



IXM WEB Integration with SIEMENS SiPort

Installation Instructions

V3.0



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	10
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	31
Email Setting Configuration	31
9. Software and Module Activation	35
IXM WEB Activation	35
SiPort Module Activation	38
10. Configuring IXM Link for SIEMENS	41
11. Create System User(s) for Biometric Enrollment	45



Creating System User(s) for Biometric Enrollment	45
12. Add and Configure Invixium Readers.....	49
Adding an Invixium Reader in IXM WEB	49
13. Adding an Invixium Device to a Device Group.....	54
Configuring Wiegand Format to Assign Invixium Readers	55
Assign Wiegand to Invixium Readers	58
Configuring Panel Feedback with SIEMENS	61
Configuring Thermal Settings	63
Thermal Calibration.....	66
Test Calibration Options.....	68
Change Temperature Unit Settings	70
Configuring Mask Authentication Settings	72
14. Enrollment Best Practices	75
Fingerprint Enrollment Best Practices.....	75
Avoid Poor Fingerprint Conditions	75
Fingerprint Image Samples	76
Fingerprint Imaging Do's and Don'ts	77
Finger Vein Enrollment Best Practices	78
Face Enrollment Best Practices	79
15. Appendix	80
Installing Invixium IXM WEB with Default Installation using SQL Server 2014	80
Pushing Configuration to Multiple Invixium Readers	85
Configuring for OSDP Connection	87
Configuring MIFARE DESFire Custom Cards	92
Wiring and Termination	95
Wiring	96
Wiegand Connection.....	98
Wiegand Connection with Panel Feedback	99
OSDP Connections	100
16. Troubleshooting.....	101
Reader Offline from the IXM WEB Dashboard	101
Elevated Body Temperature Denied Access but Granted Access in SiPort.....	103
Logs in IXM WEB Application	104
Unable to connect to the SiPort Server.....	106



17. Support	109
18. 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	25
Figure 10: IXM WEB Installation Completed	26
Figure 11: IXM WEB Icon - Desktop Shortcut	27
Figure 12: IXM WEB Database Configuration	27
Figure 13: IXM WEB Administrator User Configuration	28
Figure 14: IXM WEB Login Page	30
Figure 15: Configure Email	32
Figure 16: IXM WEB - SMTP Settings.....	32
Figure 17: IXM WEB - Save Email Settings	33
Figure 18: IXM WEB – Test Connection.....	33
Figure 19: IXM WEB - Forgot Password	34
Figure 20: IXM WEB - Enter Login Credentials	35
Figure 21: IXM WEB - License Setup.....	36
Figure 22: IXM WEB - Online Activation.....	37
Figure 23: IXM WEB – Request Link License.....	38
Figure 24: SIEMENS License Key Email.....	39
Figure 25: IXM WEB - Activate SIEMENS Link License	40
Figure 26: IXM WEB - Enable SIEMENS Link Module	41
Figure 27: IXM WEB - Sync Activities	43
Figure 28: IXM WEB - Create System User	45
Figure 29: IXM WEB - Add New System User.....	46
Figure 30: IXM WEB - New System User.....	47



Figure 31: Employee and Employee Group Rights	48
Figure 32: IXM WEB - Save System User	48
Figure 33: IXM WEB - Devices Tab	49
Figure 34: IXM WEB - Search Device Using IP Address	50
Figure 35: IXM WEB - Register Device	51
Figure 36: IXM WEB - Device Registration Complete	52
Figure 37: IXM WEB - Dashboard, Device Status	53
Figure 38: IXM WEB - Assign Device Group	54
Figure 39: IXM WEB - Create Wiegand Format	55
Figure 40: IXM WEB - Create Custom Wiegand Format	56
Figure 41: IXM WEB - Custom Wiegand Format	56
Figure 42: IXM WEB – Custom Wiegand Format Created.....	57
Figure 43: IXM WEB - Upload Wiegand Format	57
Figure 44: IXM WEB - Navigate to Access Control Tab	58
Figure 45: IXM WEB - Wiegand Output.....	59
Figure 46: IXM WEB - Save Output Wiegand.....	60
Figure 47: IXM WEB - Panel Feedback.....	61
Figure 48: IXM WEB - Configuring Panel Feedback in IXM WEB.....	62
Figure 49: IXM WEB - Save Panel Feedback.....	62
Figure 50: IXM WEB - Thermal Settings	63
Figure 51: IXM WEB - Save Thermal Settings	65
Figure 52: IXM WEB - Thermal Calibration Settings.....	66
Figure 53: IXM WEB - Save Thermal Calibration Settings.....	67
Figure 54: IXM WEB - Capture Thermal Data	67
Figure 55: IXM WEB - Save Captured Thermal Data	68
Figure 56: IXM WEB - Test Thermal Calibration	69
Figure 57: IXM WEB - Option to Change Temperature Unit	70
Figure 58: IXM WEB - Save Temperature Unit Setting.....	71
Figure 59: IXM WEB - Mask Authentication Settings.....	72
Figure 60: IXM WEB - Save Mask Settings	74
Figure 61: Fingerprint Enrollment Best Practices	75
Figure 62: Fingerprint Images Samples	76
Figure 63: Finger Vein Enrollment Best Practices	78
Figure 64: Face Enrollment Best Practices	79
Figure 65: Install IXM WEB	80
Figure 66: Loading SQL Express & Installation Progress	81
Figure 67: IXM WEB - Shortcut Icon on Desktop	82



Figure 68: IXM WEB - Configuring IXM WEB Database.....	82
Figure 69: IXM WEB - Select Database Name.....	83
Figure 70: IXM WEB - Broadcast Option.....	85
Figure 71: IXM WEB - Broadcast Wiegand Output Settings.....	85
Figure 72: IXM WEB - Broadcast to Devices.....	86
Figure 73: IXM WEB - OSDP Settings	87
Figure 74: IXM WEB - Save OSDP Settings	90
Figure 75: 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 - Server URL Setting.....	101
Figure 86: IXM WEB - Server URL Setting from General Settings	102
Figure 87: IXM WEB - Thermal Authentication Wiegand Output Event	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: SIEMENS – SiPort Web Service	107



List of Tables

Table 1: Compatibility Matrix for IXM WEB & SIEMENS Integration.....	Error! Bookmark not defined.
Table 2: Task List Summary	Error! Bookmark not defined.
Table 3: System Related Checklist	21
Table 4: Port Information	21
Table 5: IXM WEB - OSDP Configuration Options	89
Table 6: IXM WEB - OSDP Text Options	89
Table 7: 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 the 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 the First Name in IXM WEB. If the Last Name is also null, then the Card Number will be considered as the First Name in IXM WEB.
Last name	Last Name	
ValidTo	Employee End Date	The start date for IXM WEB will be the date and time of import.
Gender	Gender	
Status	Suspend	An employee who is “Inactive” in SiPort will be marked as suspended in IXM WEB.
Cards	Prox ID	Multiple cards will be imported using a card array if they exists 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 the 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	3.0.36.0
Operating Systems	Windows 10 Professional Version Windows 11 Pro Windows Server 2016 Standard Windows Server 2019
Microsoft .NET Framework	.NET Framework 4.8
Database Engine	SQL Server 2016+ Supported but not recommended: (Legacy) SQL Server 2014 Express Edition (Default Installation)
Internet Information Services (IIS)	Microsoft® Internet Information Services version 10.0
Web Browser	Google Chrome Mozilla Firefox Microsoft Edge (Internet Explorer not recommended)

Other Requirements

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

Note: Server requirements mentioned are ideal for 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 2.3.2.0	v3.1.4.286	Yes
IXM WEB 3.0.36.0	v3.1.4.286	Yes

Table 1: Compatibility Matrix for IXM WEB & SIEMENS Integration



3. Checklist

Item List	Interface
SiPort API	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 SiPort	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 the 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.

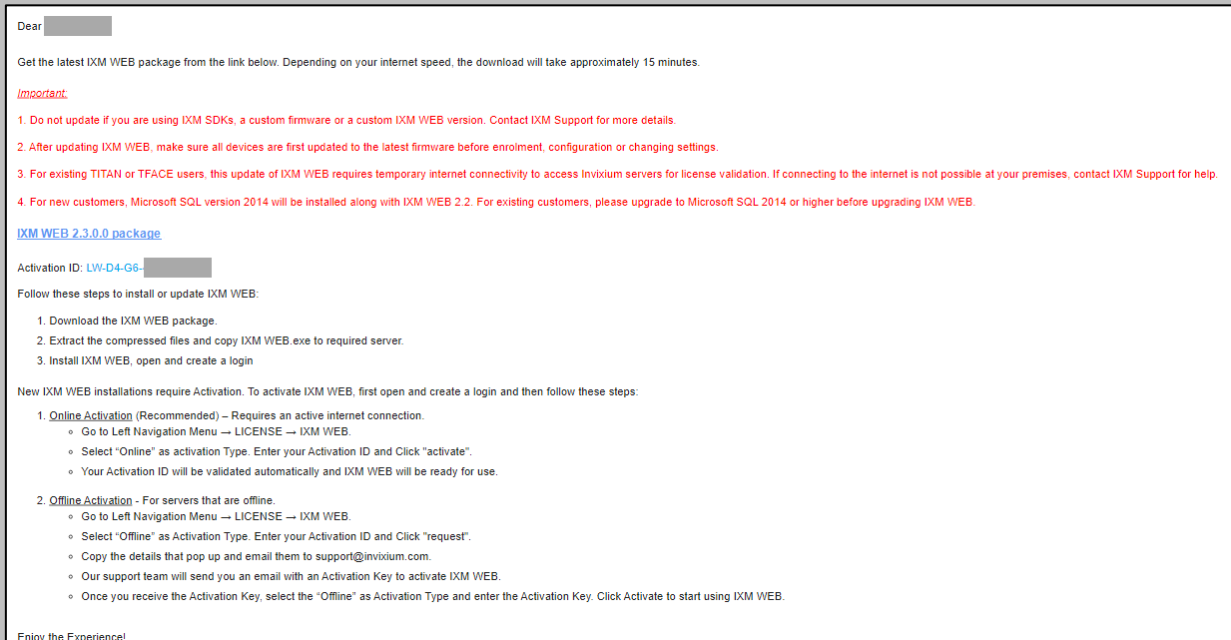



Figure 2: Sample Email After Submitting Online Request Form

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 Command Centre 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.

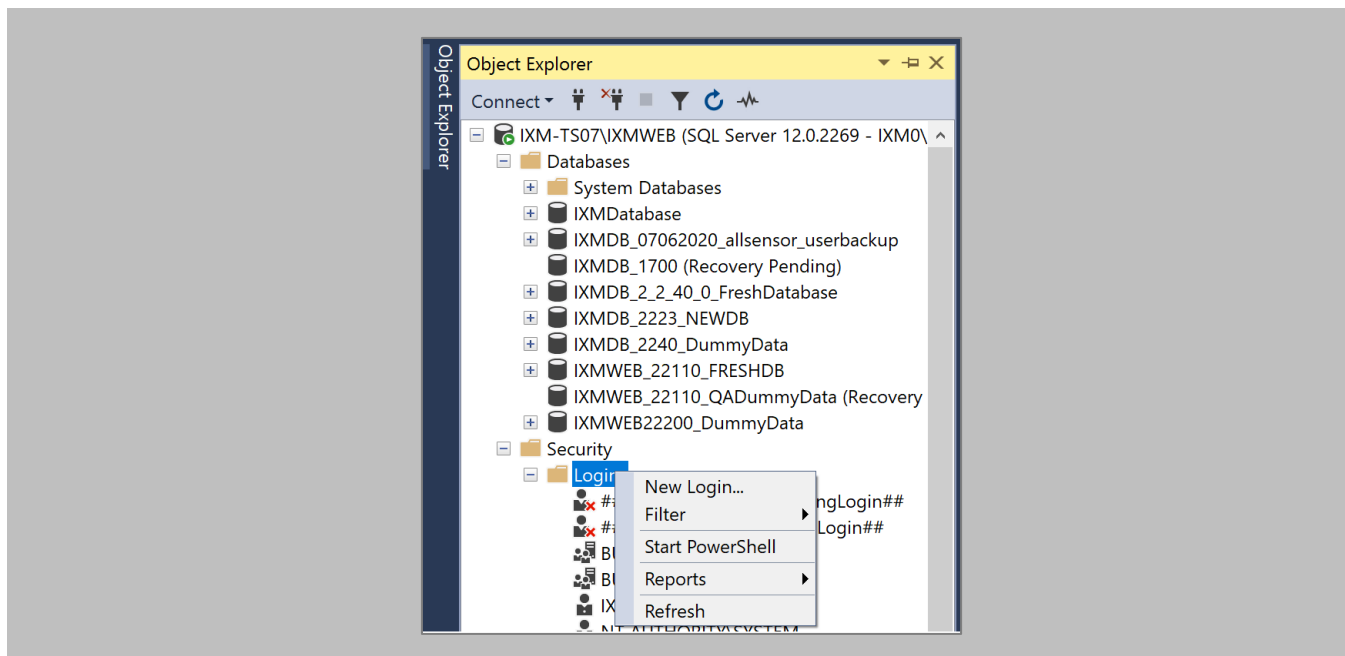



Figure 3: SQL New Login

STEP 6

Select **SQL Server authentication**.

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

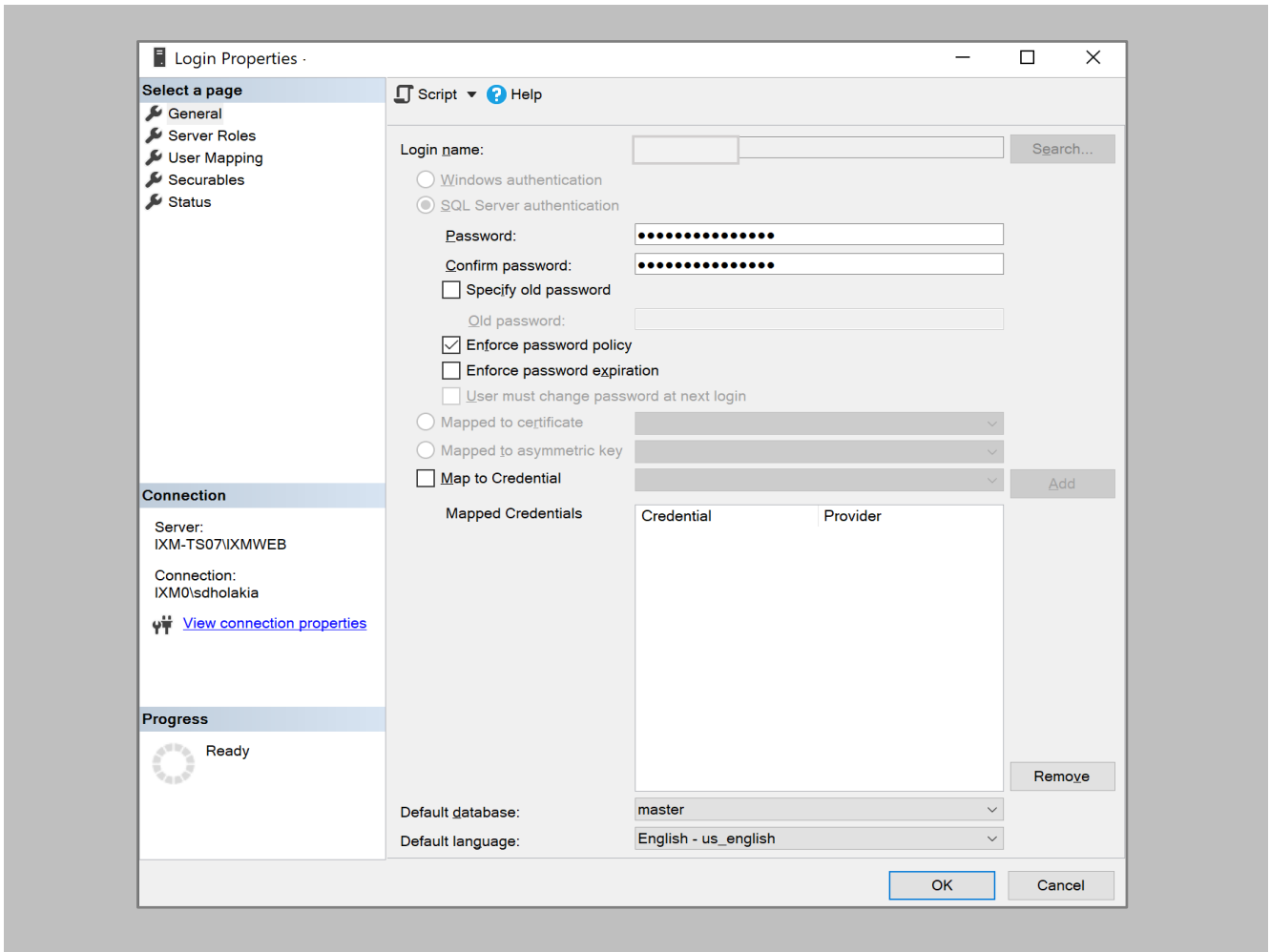


Figure 4: SQL Login Properties

STEP 7

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

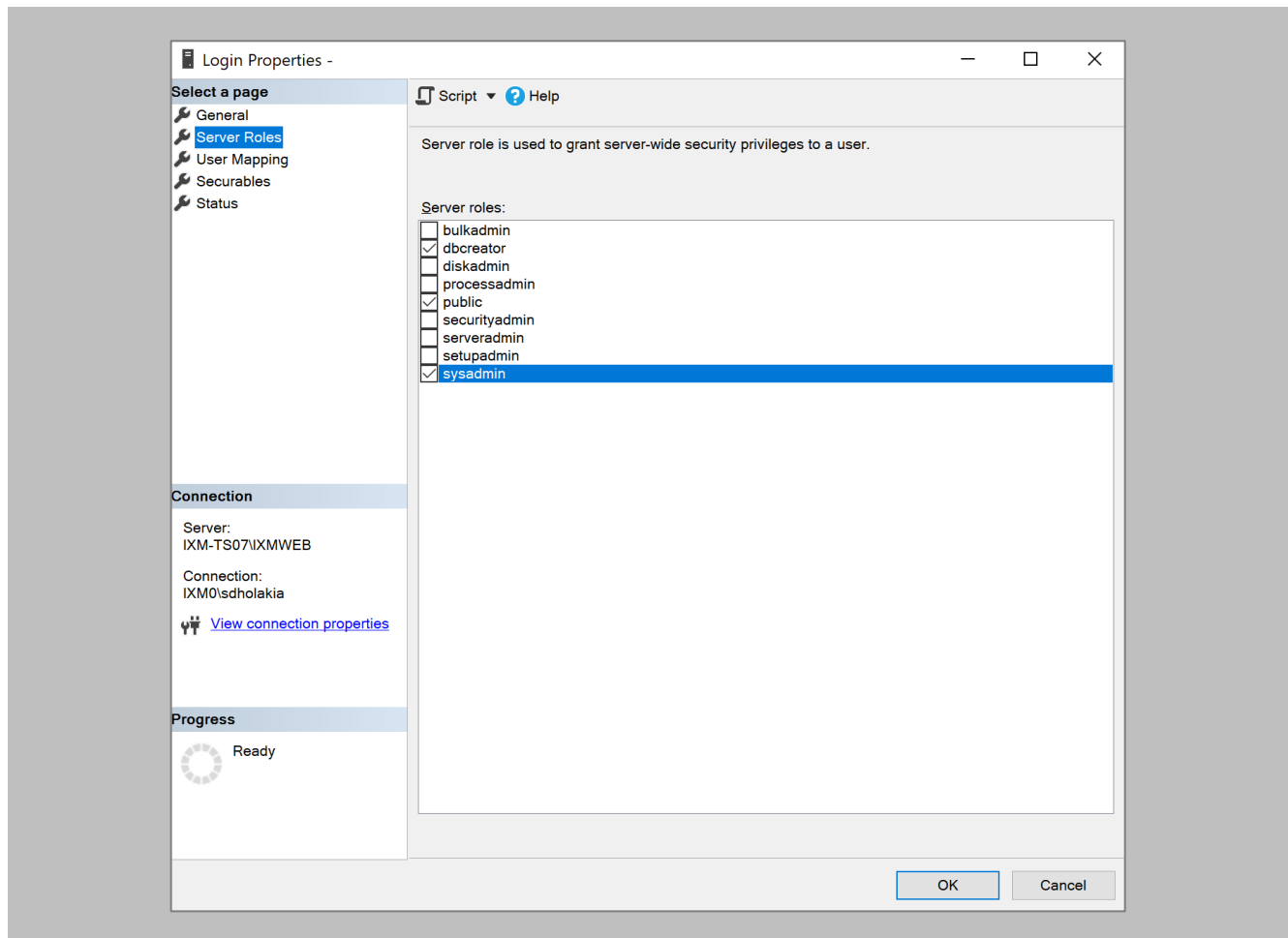


Figure 5: SQL Server Roles

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 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**.

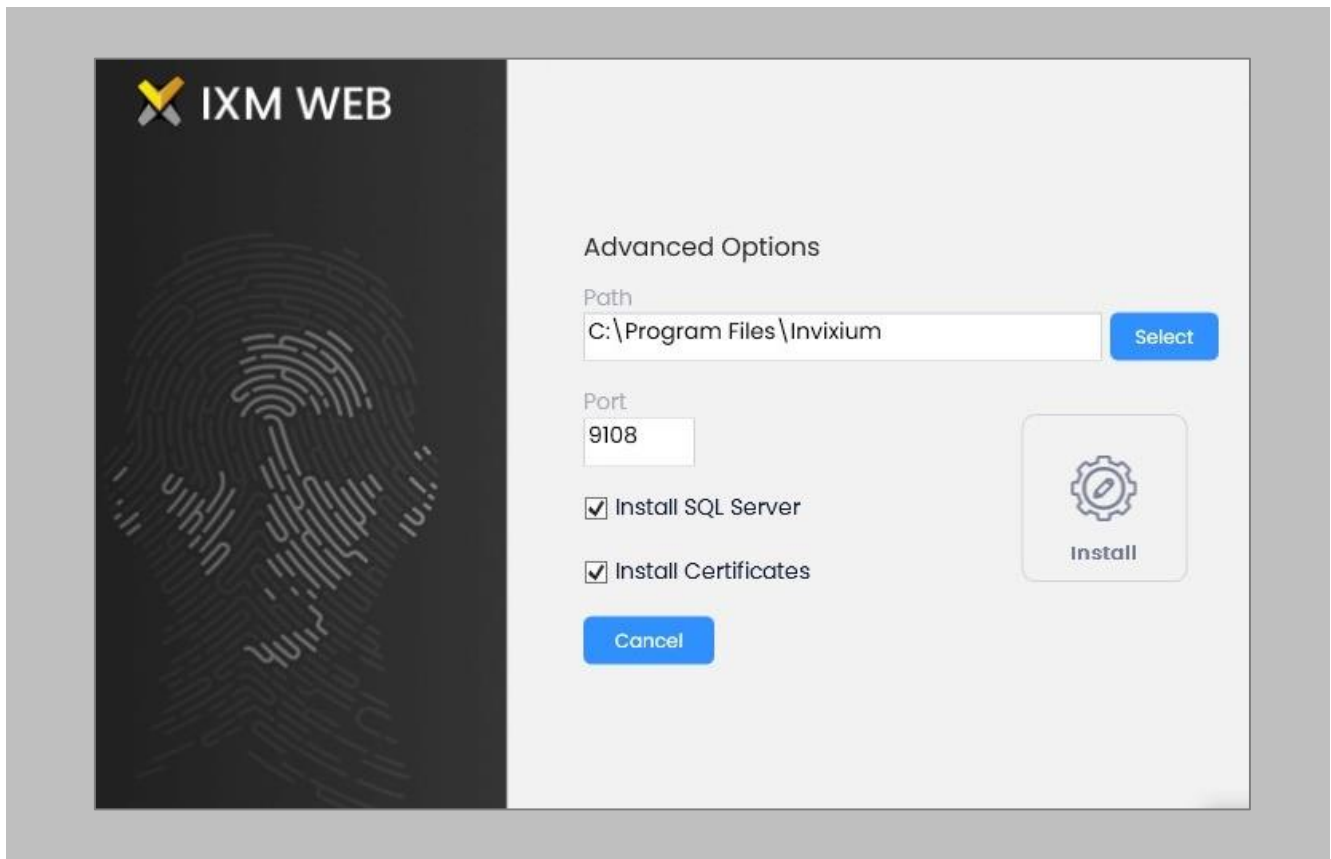


Figure 7: Advanced Options in IXM WEB Installer

STEP 3

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

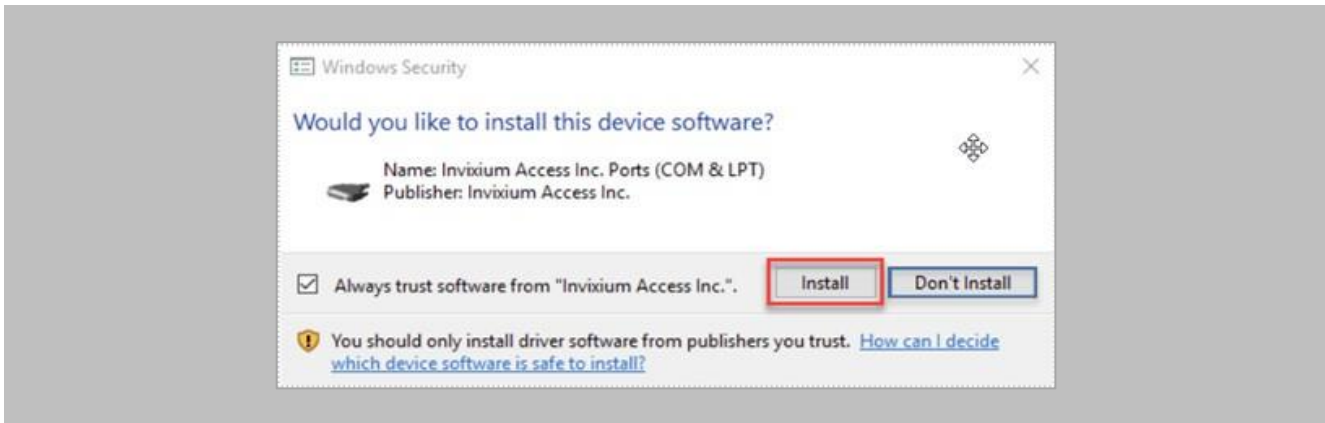


Figure 8: Inixium Fingerprint Driver Installation Message

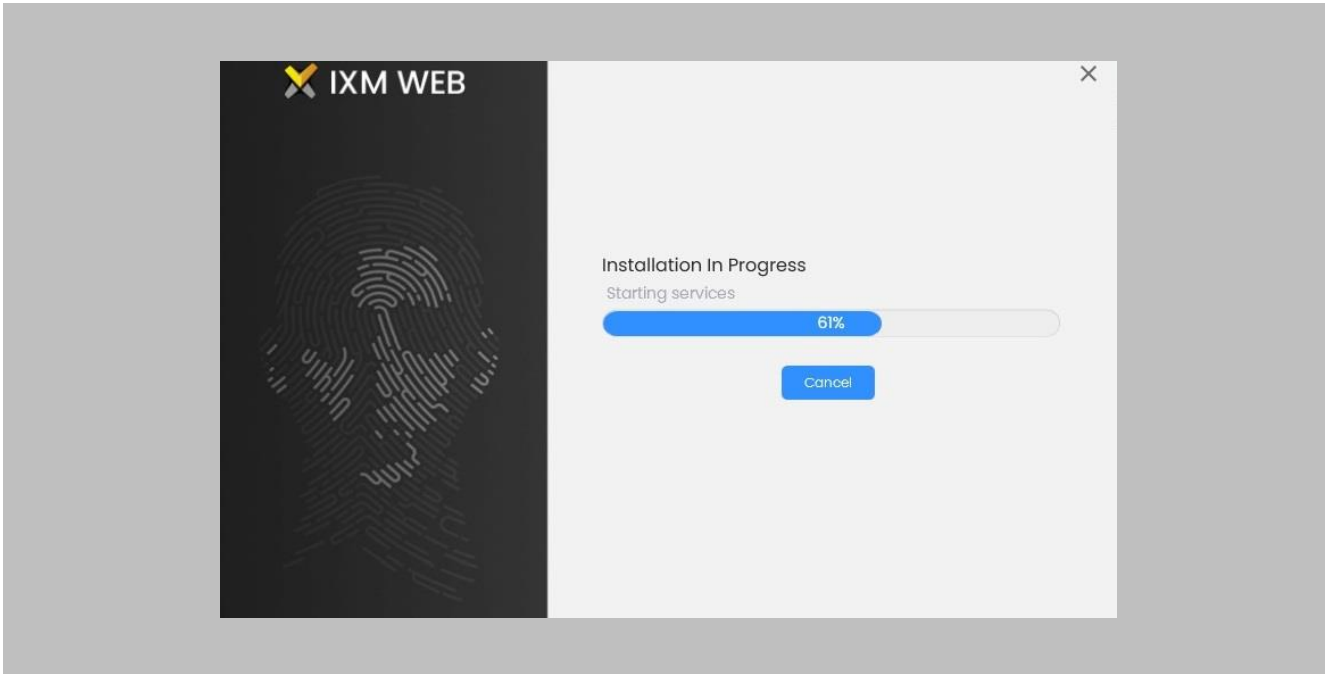


Figure 9: IXM WEB Installation Progress

STEP 4

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

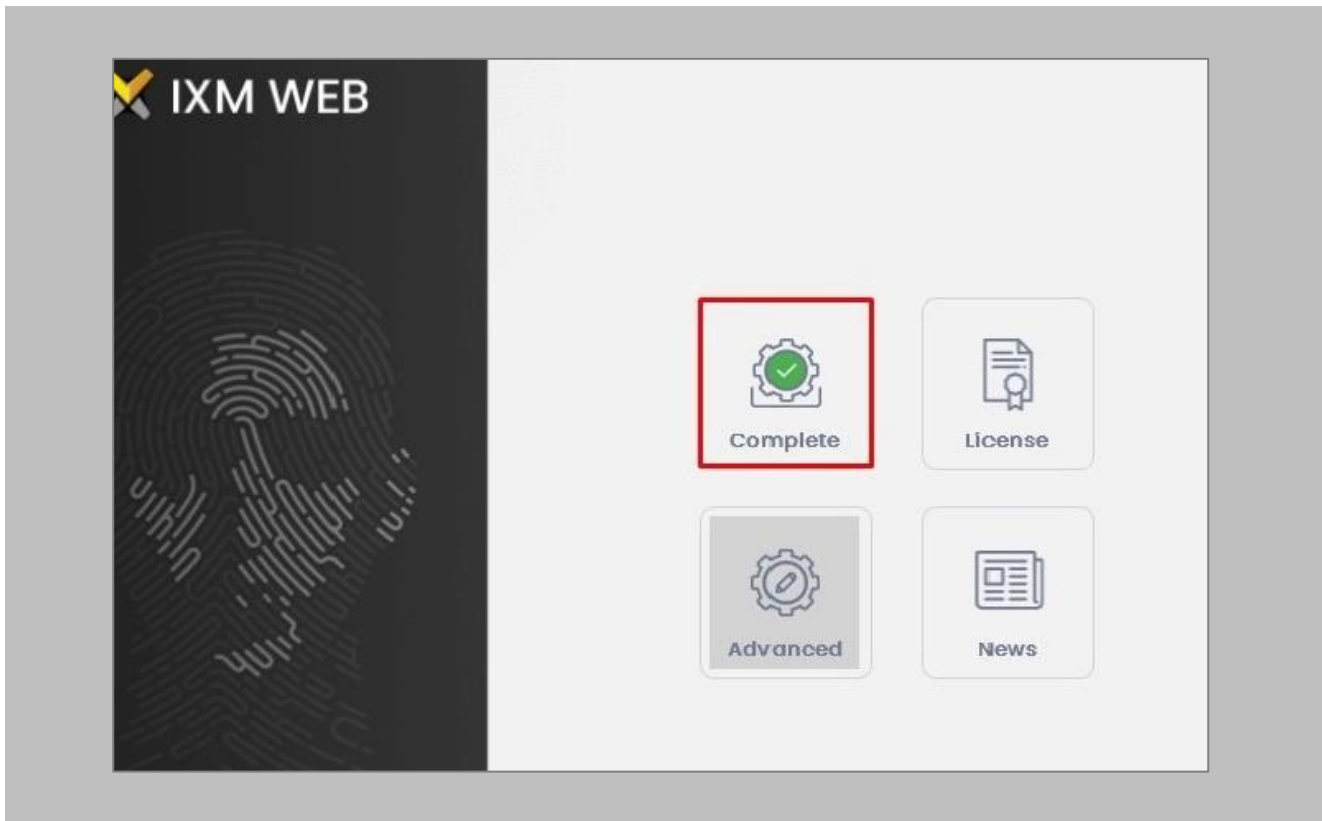


Figure 10: IXM WEB Installation Completed

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

STEP 5

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

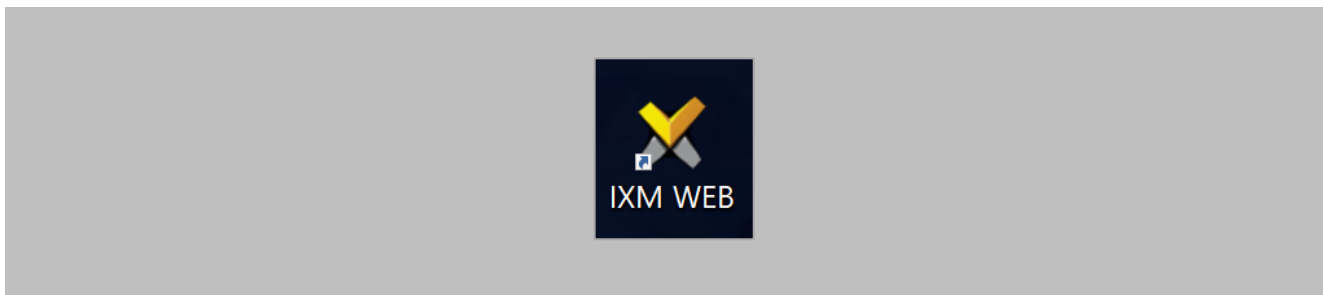


Figure 11: IXM WEB Icon - Desktop Shortcut

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

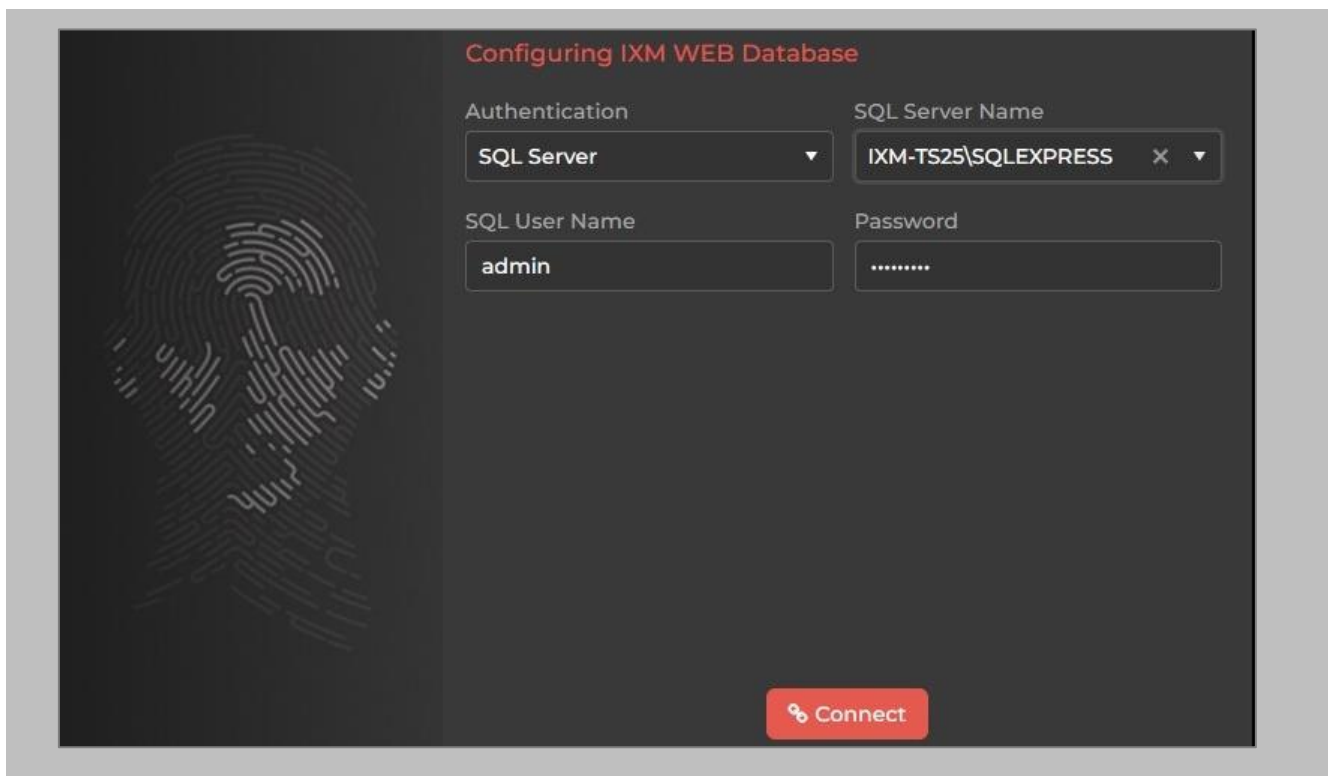


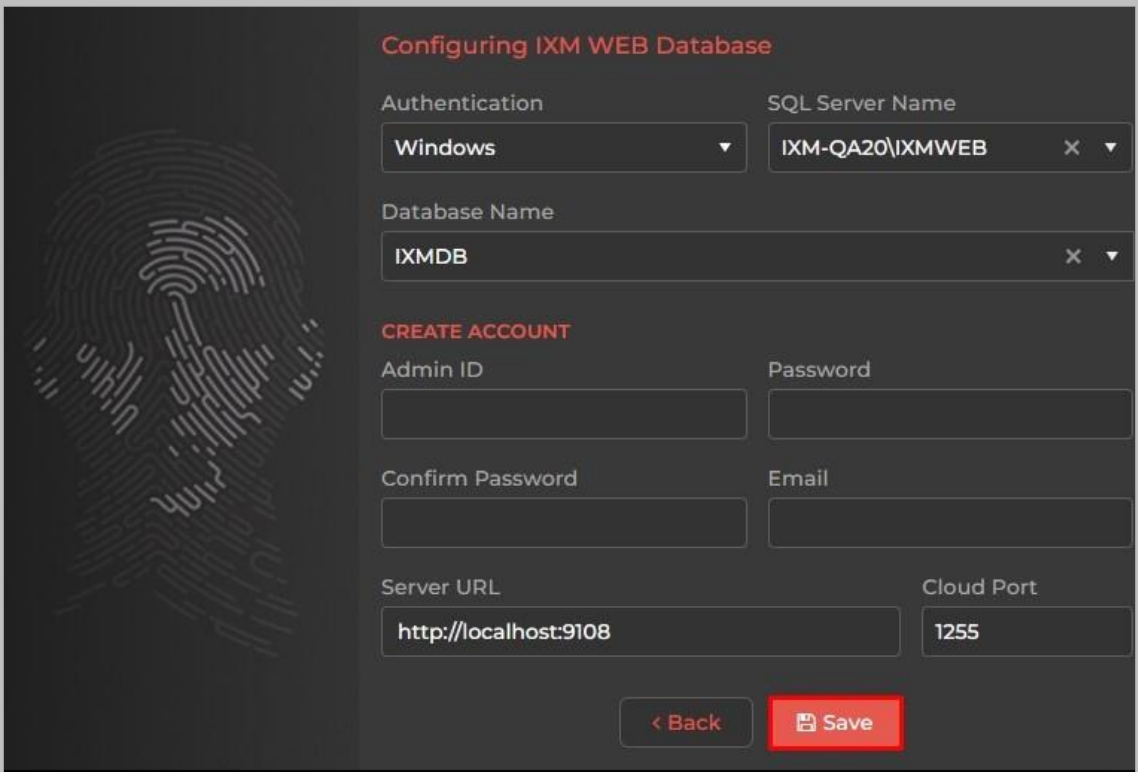
Figure 12: IXM WEB Database Configuration

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.



The screenshot shows a configuration interface for the IXM WEB Administrator. The title is "Configuring IXM WEB Database". The interface is dark-themed with a fingerprint graphic on the left. The configuration fields are as follows:

- Authentication:** Windows (dropdown)
- SQL Server Name:** IXM-QA20\IXMWEB (dropdown)
- Database Name:** IXMDB (dropdown)
- CREATE ACCOUNT:**
 - Admin ID:** (text input)
 - Password:** (text input)
 - Confirm Password:** (text input)
 - Email:** (text input)
- Server URL:** http://localhost:9108 (text input)
- Cloud Port:** 1255 (text input)

At the bottom, there are two buttons: "< Back" and "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:

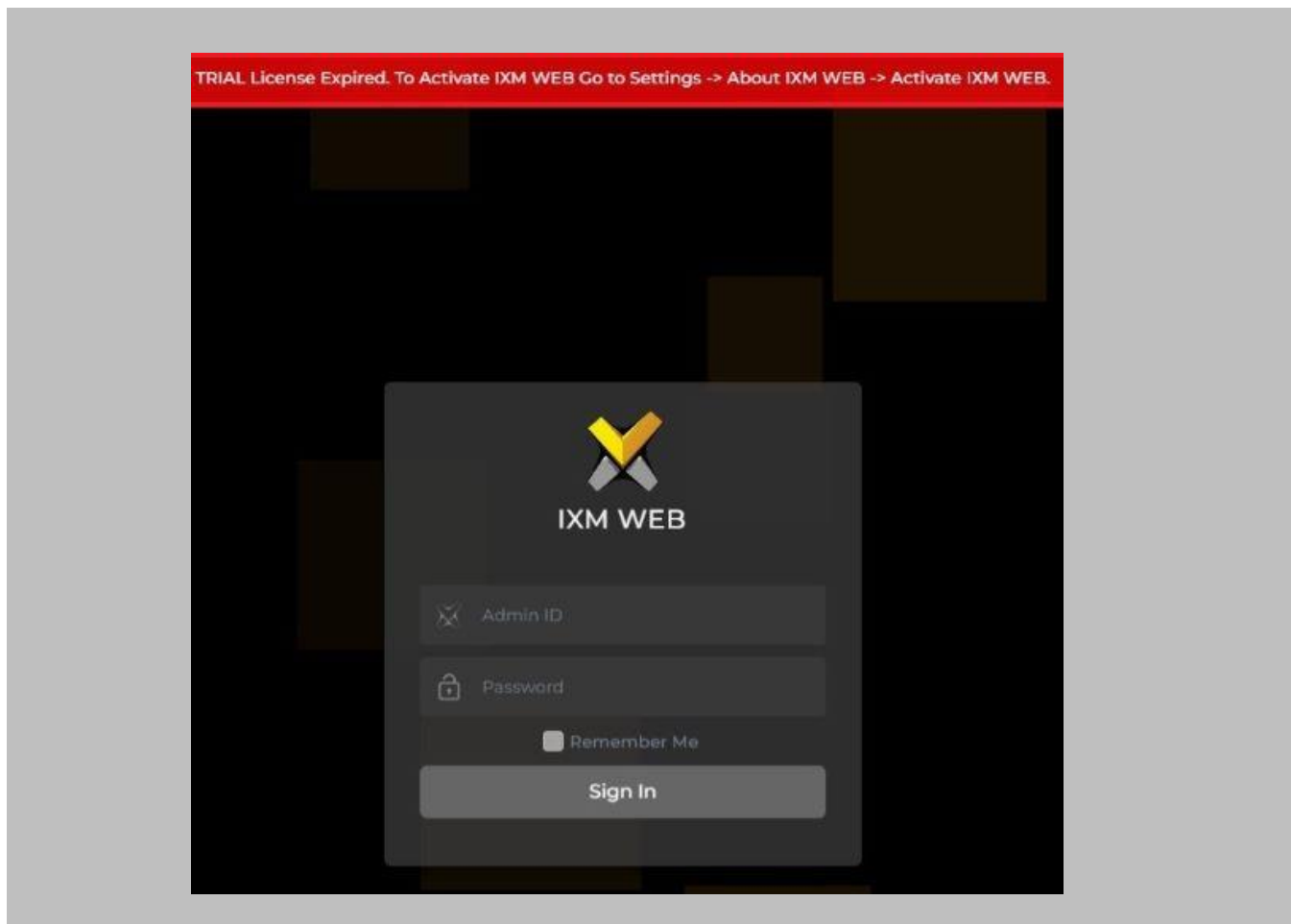



Figure 14: IXM WEB Login Page

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

8. Configuring Email Settings using IXM WEB

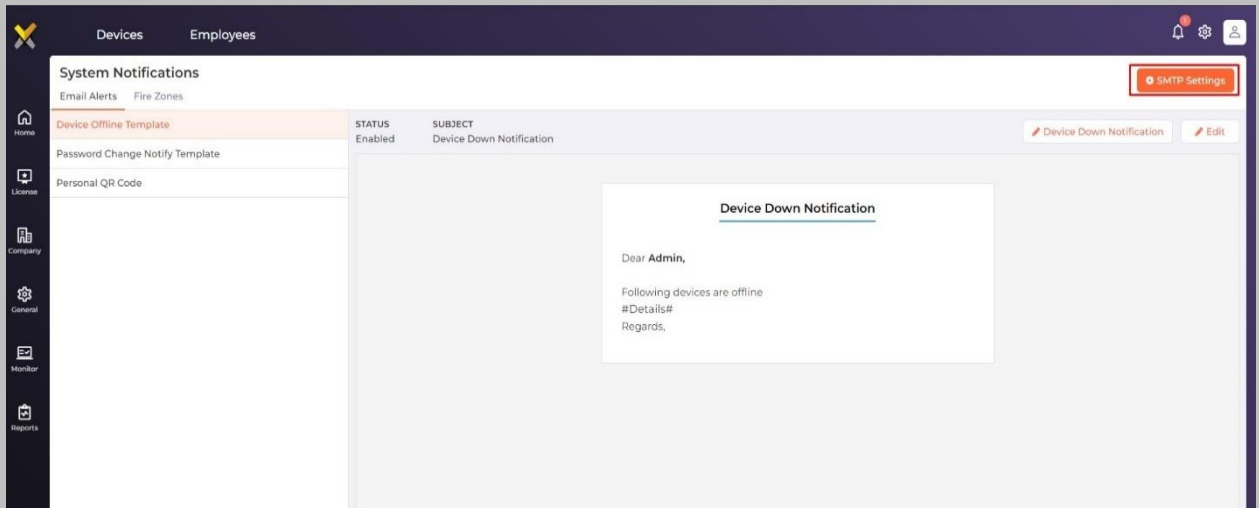
Configuring Email settings is highly recommended as one of the first steps after installing IXM WEB. Email configuration settings will help the admin retrieve the password for IXM WEB in case it is forgotten. In addition, having email settings configured also makes activation and license key requests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

Email Setting Configuration

Procedure

STEP 1

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



The screenshot displays the 'System Notifications' interface in the IXM WEB application. The top navigation bar includes 'Devices' and 'Employees' tabs, along with notification, settings, and user profile icons. A sidebar on the left contains navigation options: Home, License, Company, General, Monitor, and Reports. The main content area is titled 'System Notifications' and features a sub-menu with 'Email Alerts' and 'Fire Zones'. A table lists notification templates:

Template Name	STATUS	SUBJECT	Actions
Device Offline Template	Enabled	Device Down Notification	Device Down Notification Edit
Password Change Notify Template			
Personal QR Code			

The 'Device Down Notification' template is selected, showing a preview of the email content:

Device Down Notification

Dear Admin,

Following devices are offline
#Details#

Regards,

An orange 'SMTP Settings' button is visible in the top right corner of the notification list.

Figure 15: Configure Email

STEP 2

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

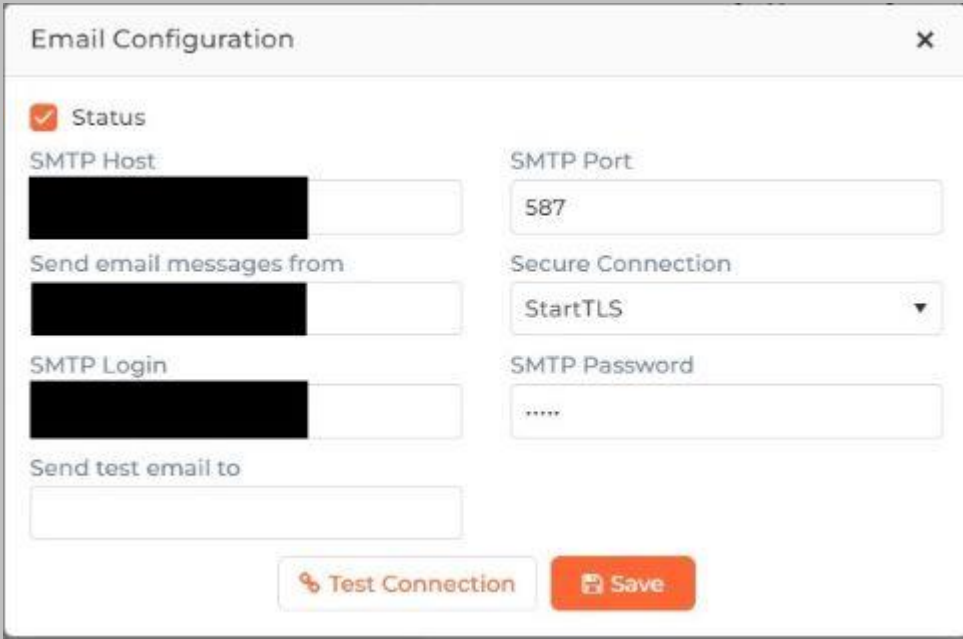


Figure 16: IXM WEB - SMTP Settings



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

STEP 3

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

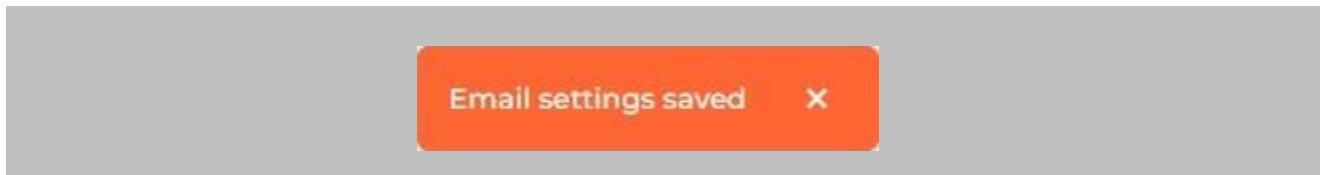


Figure 17: IXM WEB - Save Email Settings

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

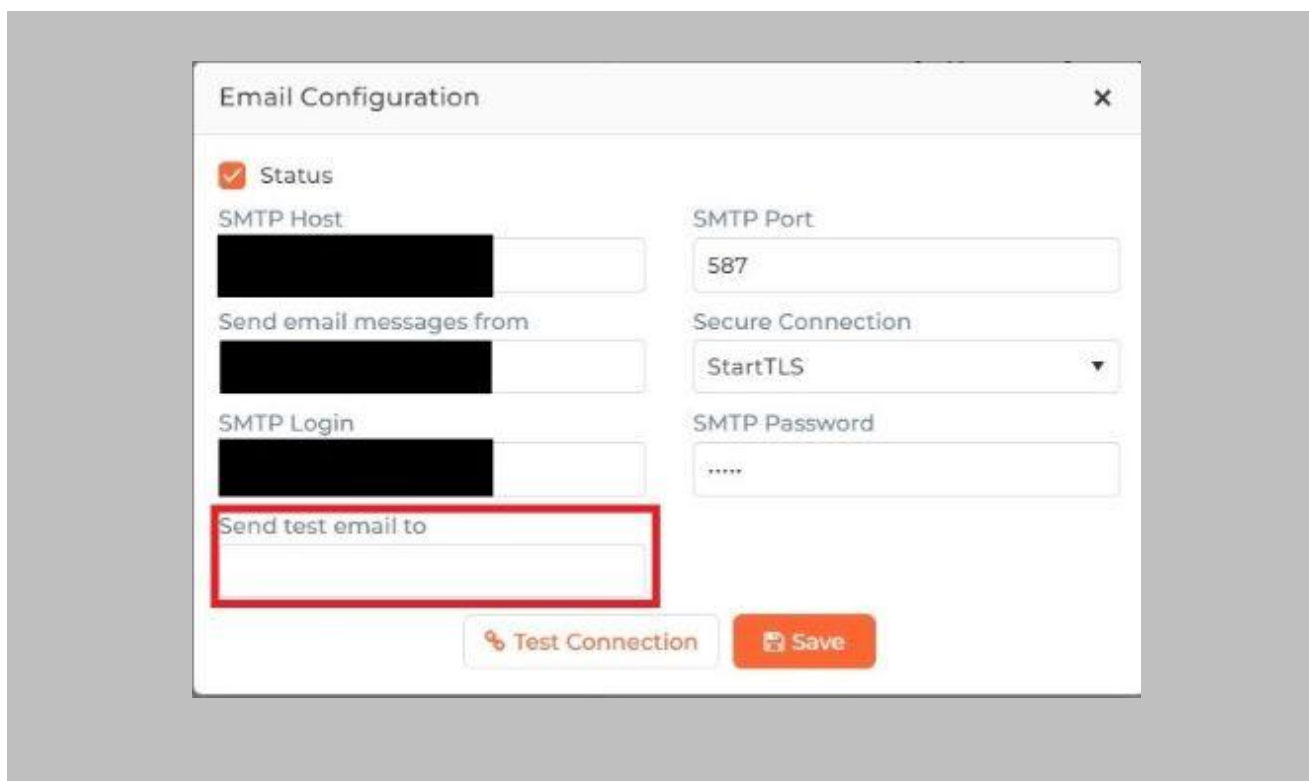


Figure 18: IXM WEB – Test Connection

STEP 4

Once email configuration is completed, a [Forgot password](#) link will appear on the Sign In page in its place.

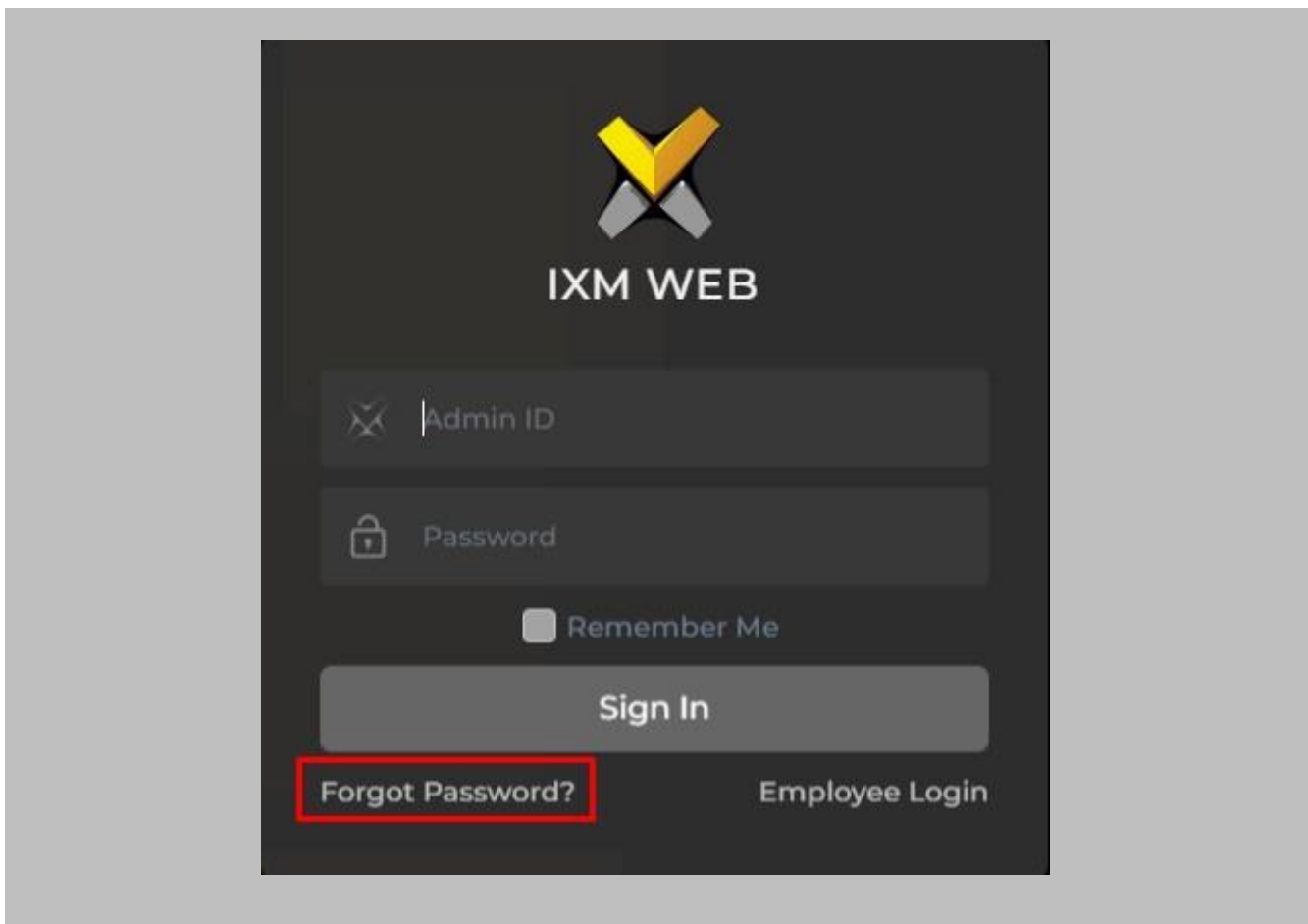


Figure 19: IXM WEB - Forgot Password

9. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

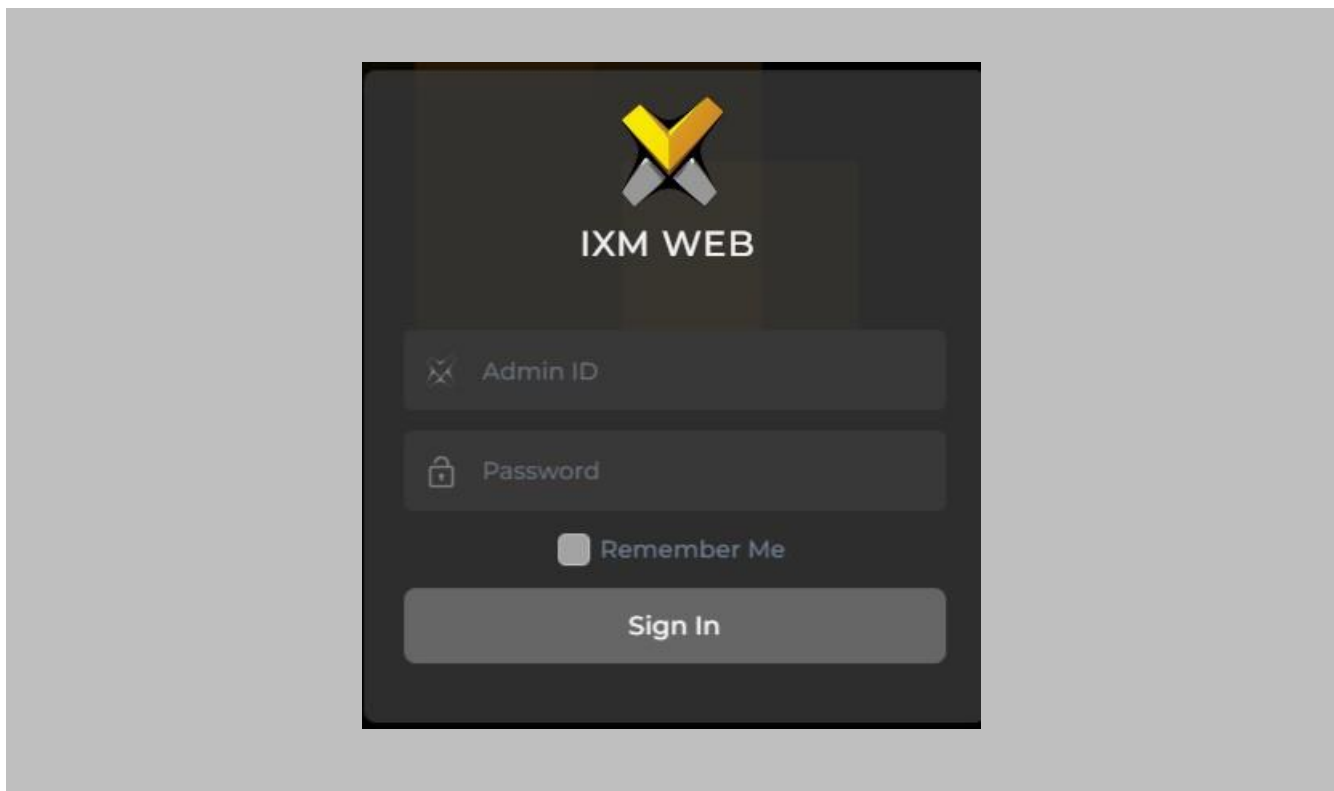


Figure 20: IXM WEB - Enter Login Credentials

STEP 2

Select the [Settings Icon](#) on top right of page then click [About IXM WEB](#).

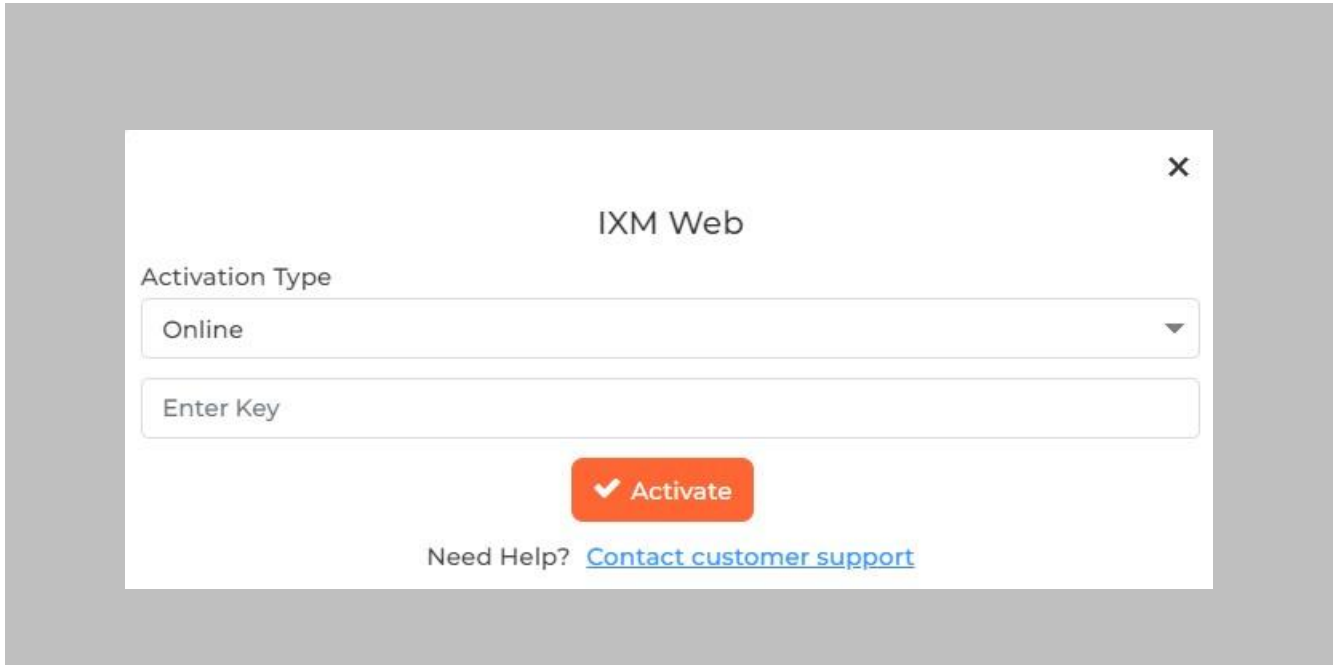



Figure 21: IXM WEB - License Setup

STEP 3

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

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

STEP 4

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

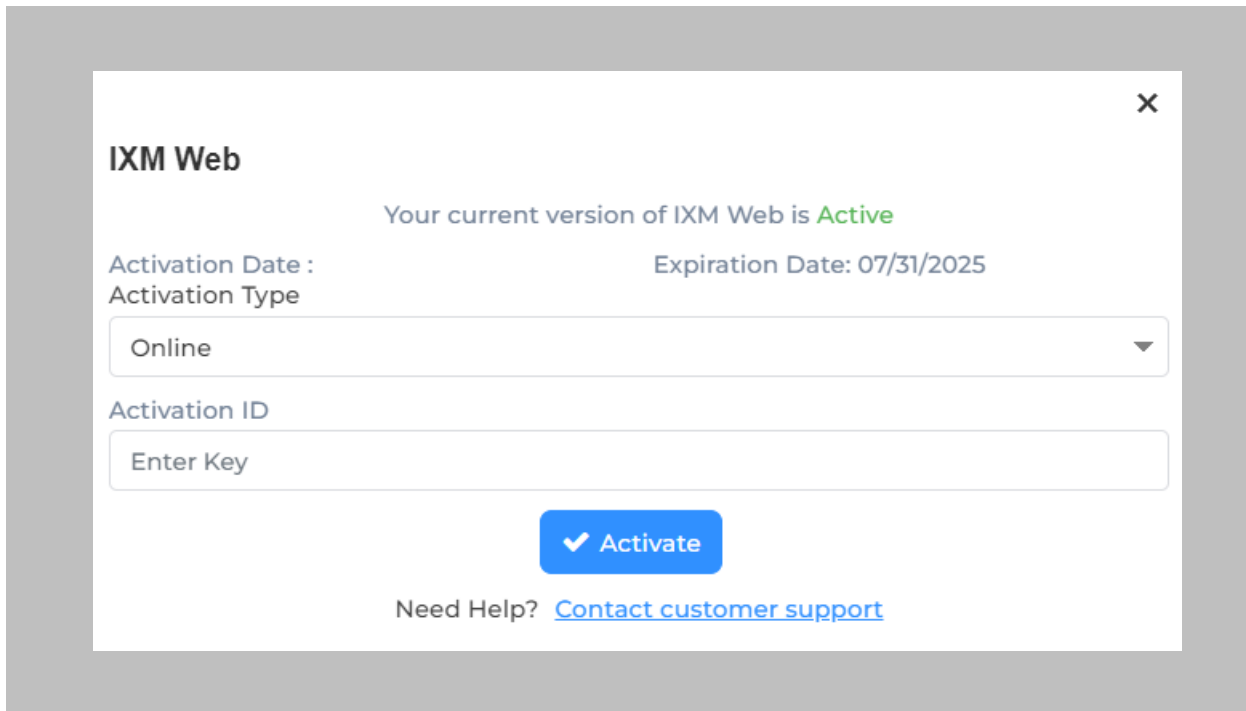


Figure 22: IXM WEB - Online Activation

SiPort Module Activation

The option to activate a SIEMENS SiPort License is available under the **License** tab.

STEP 1

Select **Settings** icon on top right of the page >> Click on **About IXM WEB** >> Click on **copy to clipboard** button next to **MACHINE KEY**.

Request a **License** by sending email to support@invixium.com. Paste the copied machine key in the email.

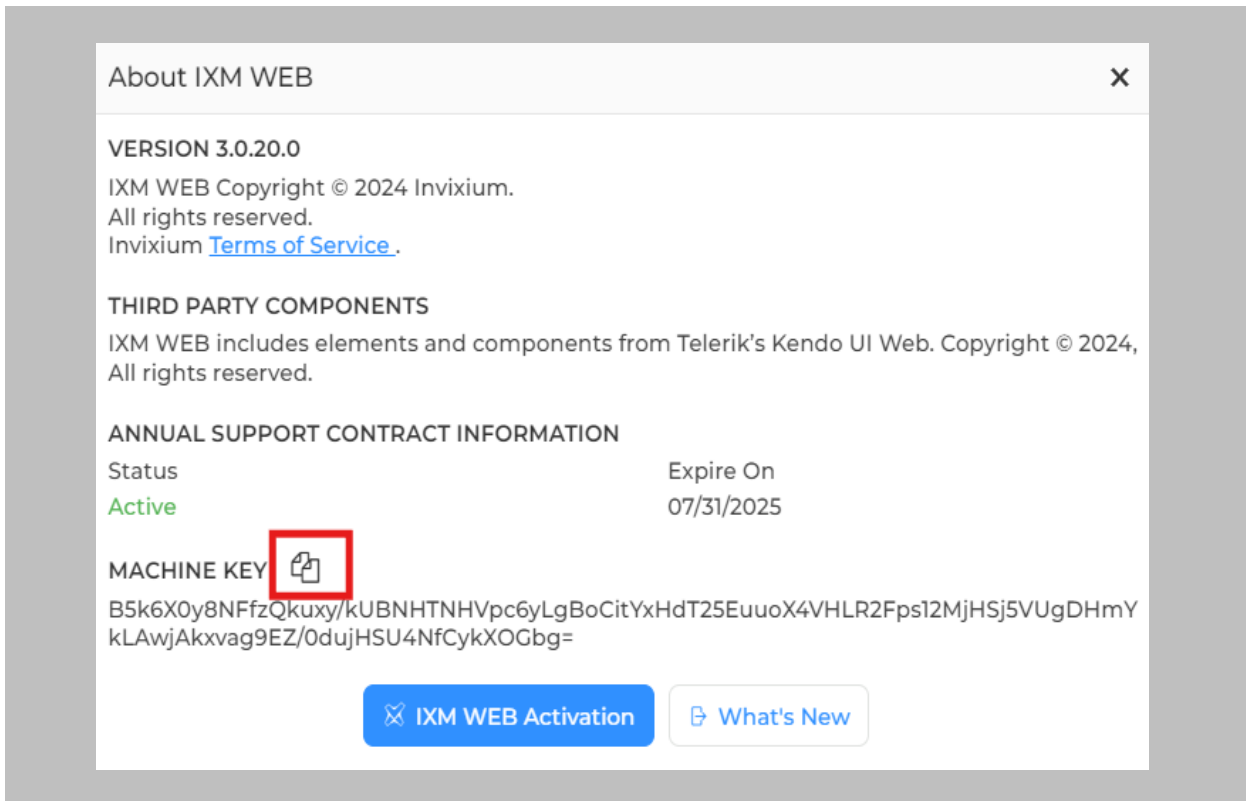


Figure 23: IXM WEB – Request Link License

STEP 2

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

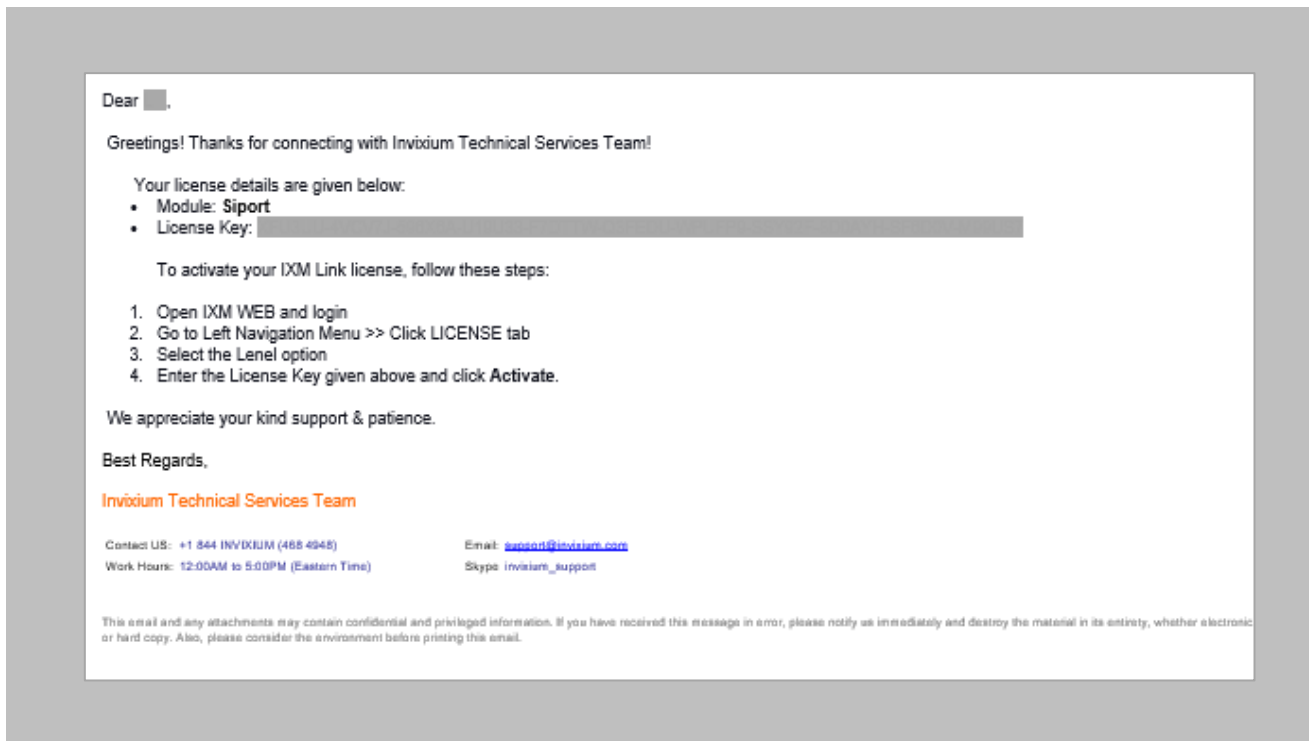


Figure 24: SIEMENS License Key Email

STEP 3

Navigate to **License** → Click on **IXM LINK** → **Copy** and **paste** the License Key in the box provided, and then select **Activate**.

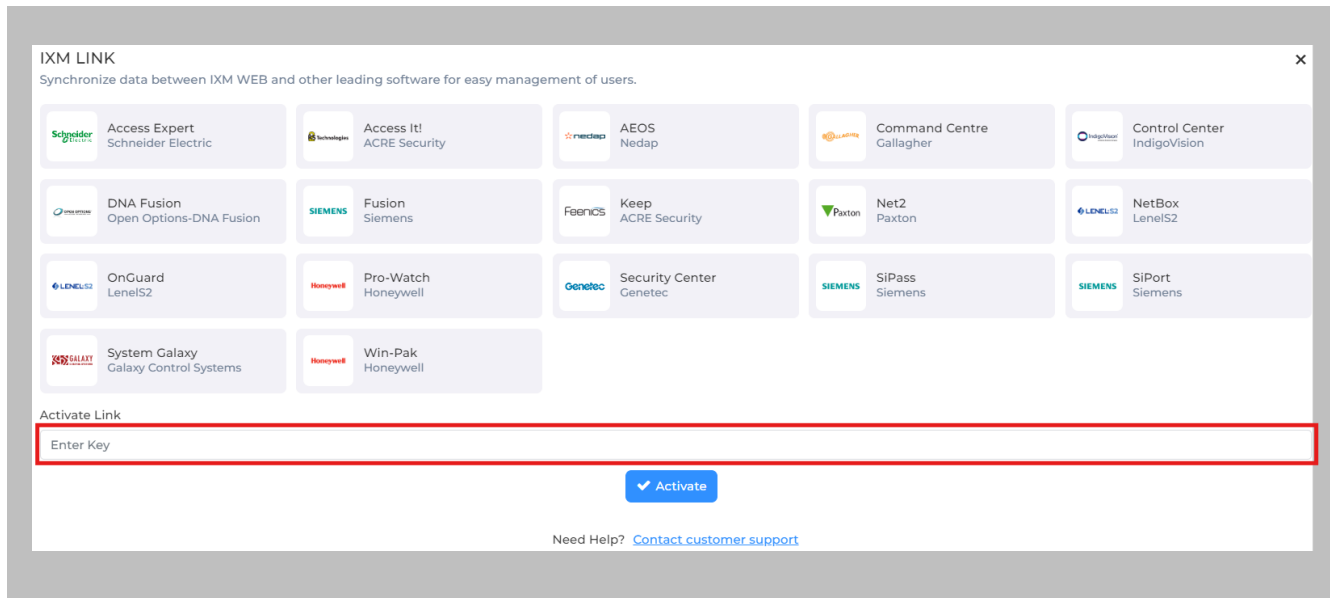


Figure 25: IXM WEB - Activate SIEMENS Link License

RESULT

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

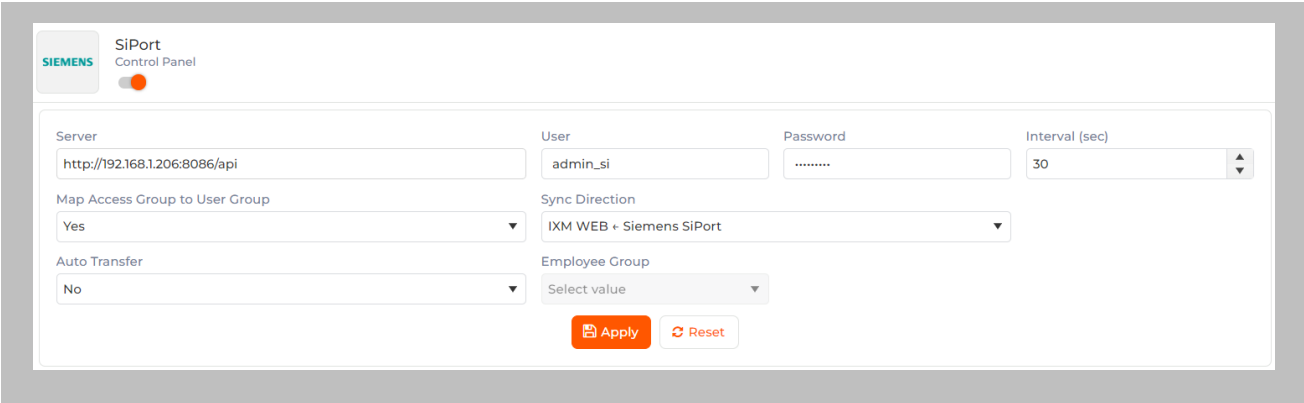
10. Configuring IXM Link for SIEMENS

Procedure

STEP 1

From the **Link** → click the **SiPort (SIEMENS)** icon.

Toggle the **Status** switch to enable.



The screenshot shows the 'SiPort Control Panel' configuration page. At the top left, there is a 'SIEMENS' logo and a status switch that is currently turned off. Below this, there are several configuration fields:

- Server:** A text input field containing 'http://192.168.1.206:8086/api'.
- User:** A text input field containing 'admin_si'.
- Password:** A text input field with masked characters '.....'.
- Interval (sec):** A dropdown menu showing '30'.
- Map Access Group to User Group:** A dropdown menu showing 'Yes'.
- Sync Direction:** A dropdown menu showing 'IXM WEB ← Siemens SiPort'.
- Auto Transfer:** A dropdown menu showing 'No'.
- Employee Group:** A dropdown menu showing 'Select value'.

At the bottom of the configuration area, there are two buttons: 'Apply' (orange) and 'Reset' (white with a red border).

Figure 26: 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 interval for data transfer between SIEMENS 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-on-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.

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 β 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.

Auto Transfer:

This option provides facility to add employee 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 and IXM WEB is possible only after 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:

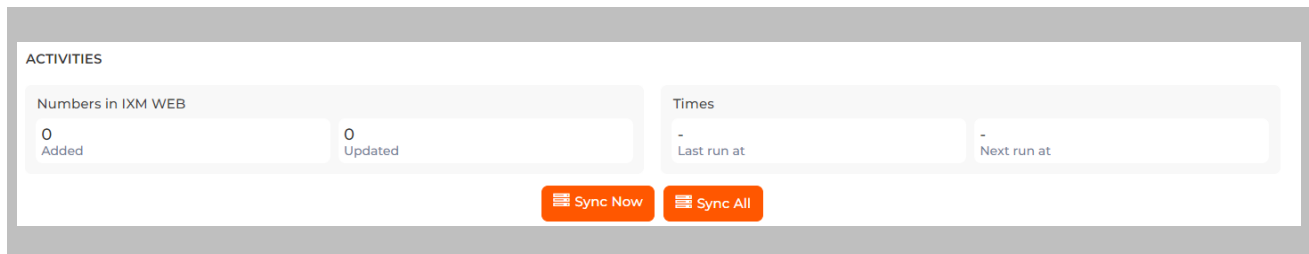


Figure 27: IXM WEB - Sync Activities

Numbers

The first two columns display the number of records added and updated in SIEMENS 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 2

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 3

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.

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

RESULT

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

11. Create System User(s) for Biometric Enrollment

Creating System User(s) for Biometric Enrollment

Procedure

STEP 1

Log into IXM WEB.

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

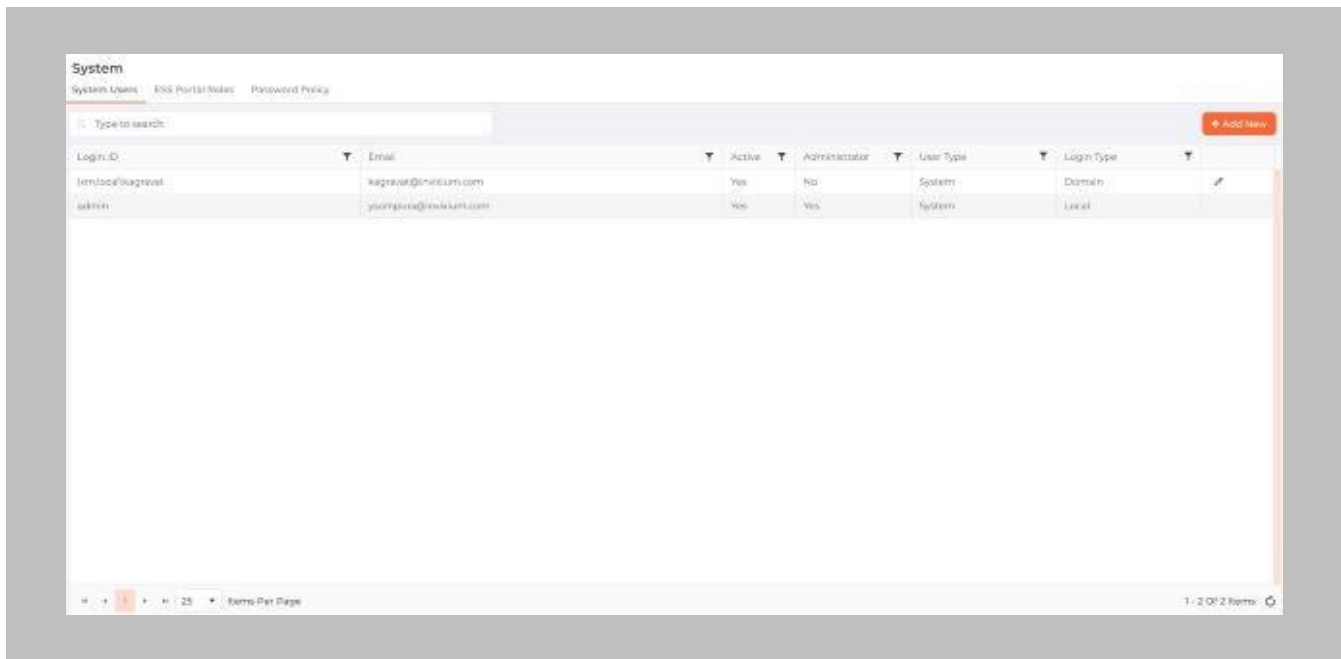


Figure 28: IXM WEB - Create System User

STEP 2

Click **Add New**.

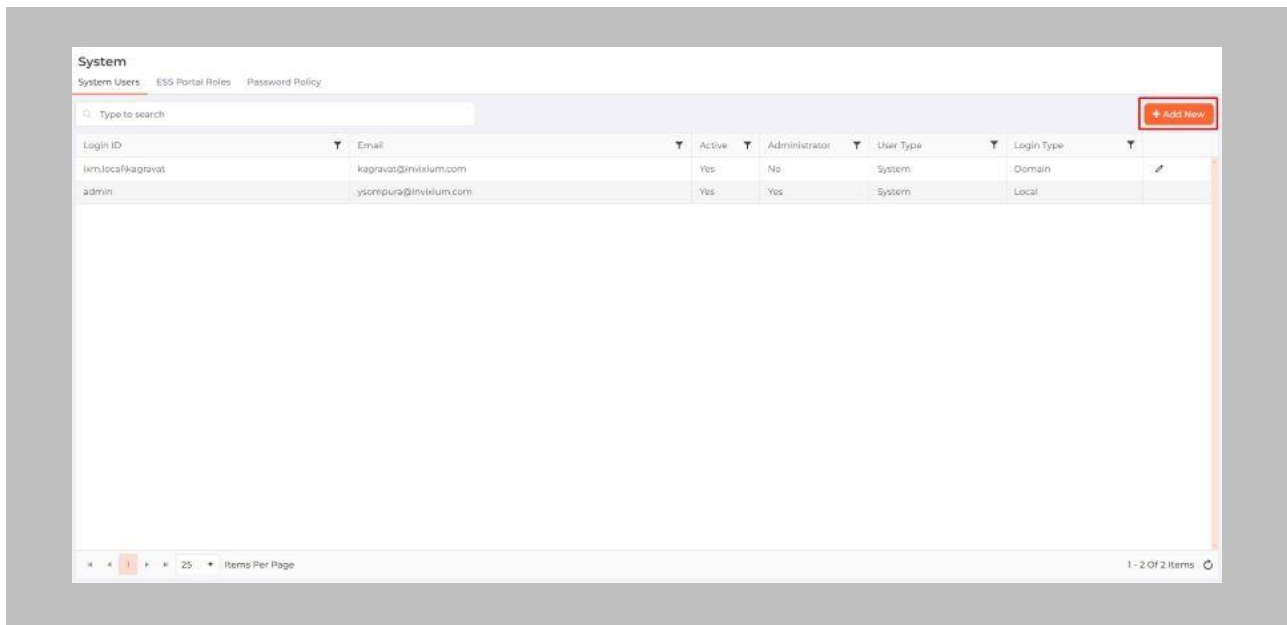


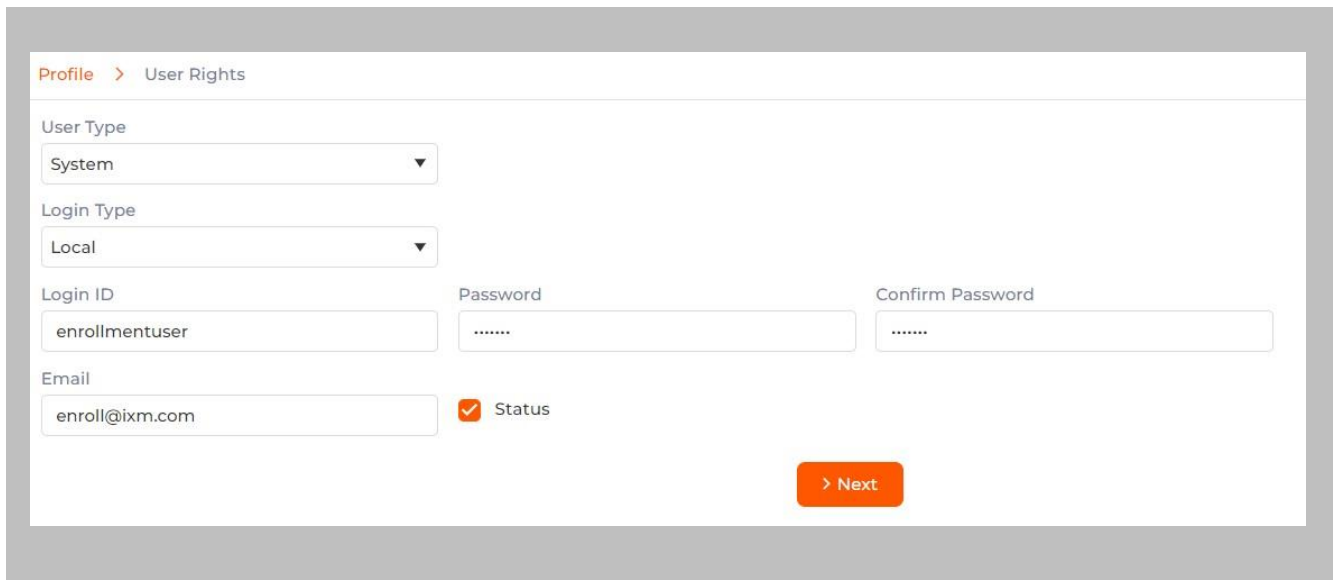
Figure 29: IXM WEB - Add New System User

Creating a system user requires the following details:

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

STEP 3

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



The screenshot shows a web form titled "Profile > User Rights". The form contains the following fields and controls:

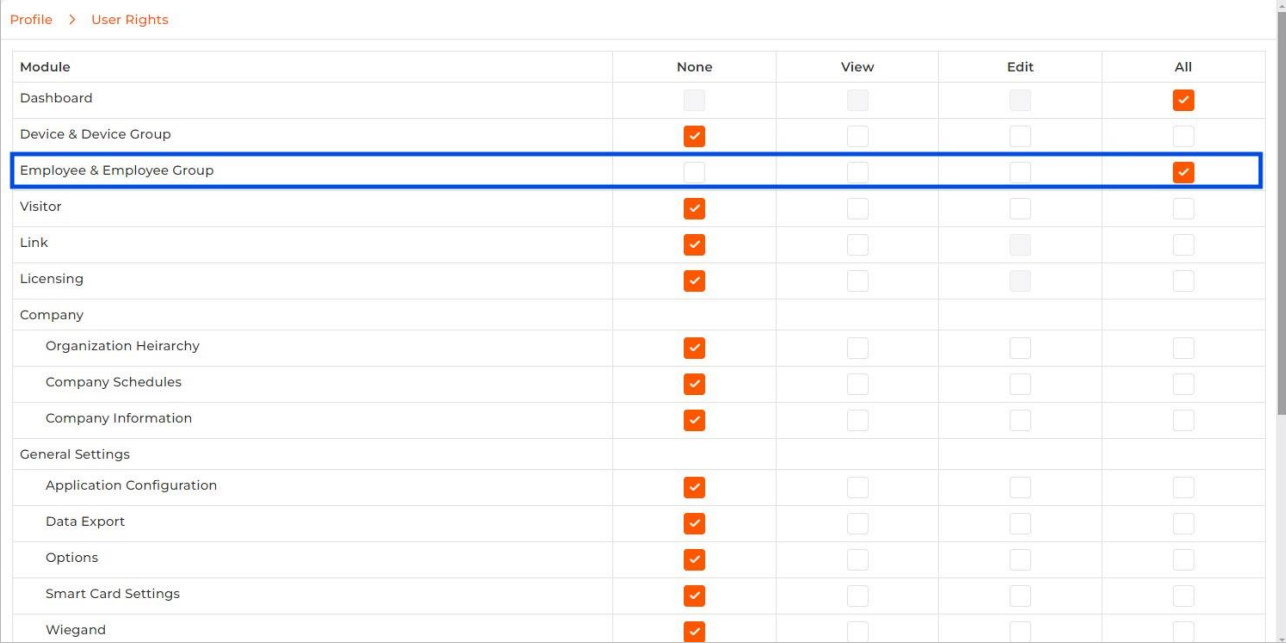
- User Type:** A dropdown menu with "System" selected.
- Login Type:** A dropdown menu with "Local" selected.
- Login ID:** A text input field containing "enrollmentuser".
- Password:** A text input field with masked characters ".....".
- Confirm Password:** A text input field with masked characters ".....".
- Email:** A text input field containing "enroll@ixm.com".
- Status:** A checkbox that is checked, labeled "Status".
- Next:** An orange button with a right-pointing chevron and the text "> Next".

Figure 30: IXM WEB - New System User

STEP 4

Add an email address.

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



Module	None	View	Edit	All
Dashboard	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Device & Device Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employee & Employee Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Visitor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Link	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Licensing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Company				
Organization Heirarchy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Company Schedules	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Company Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
General Settings				
Application Configuration	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Export	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Options	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart Card Settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wiegand	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 31: Employee and Employee Group Rights

STEP 5

Click **Save**.

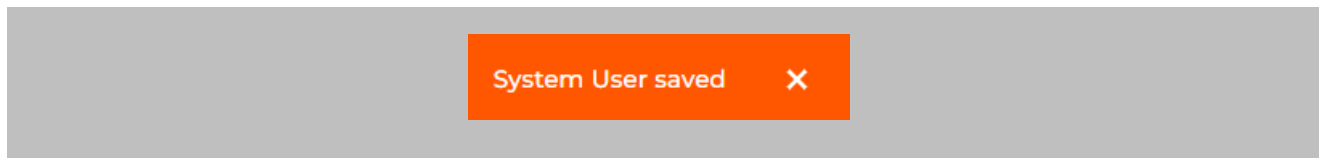


Figure 32: IXM WEB - Save System User

12. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

Click the **Devices** tab.

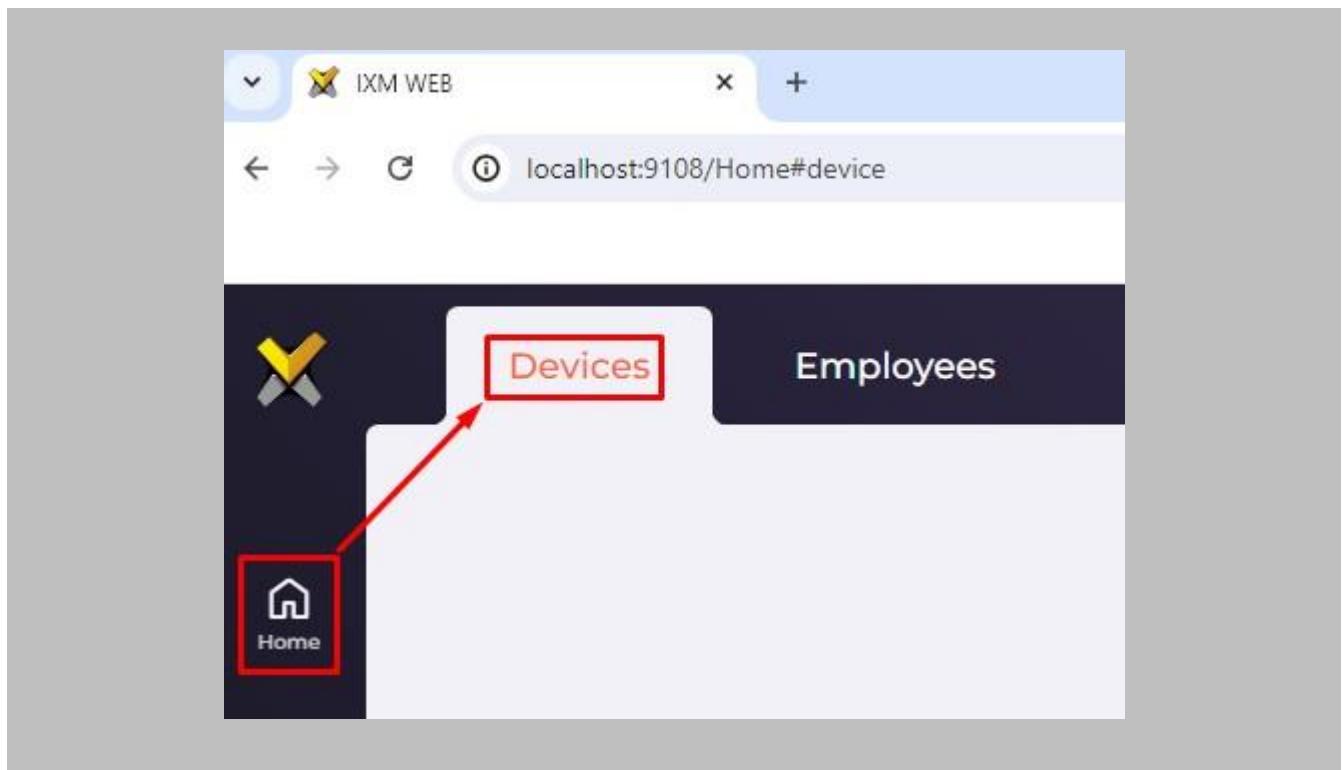
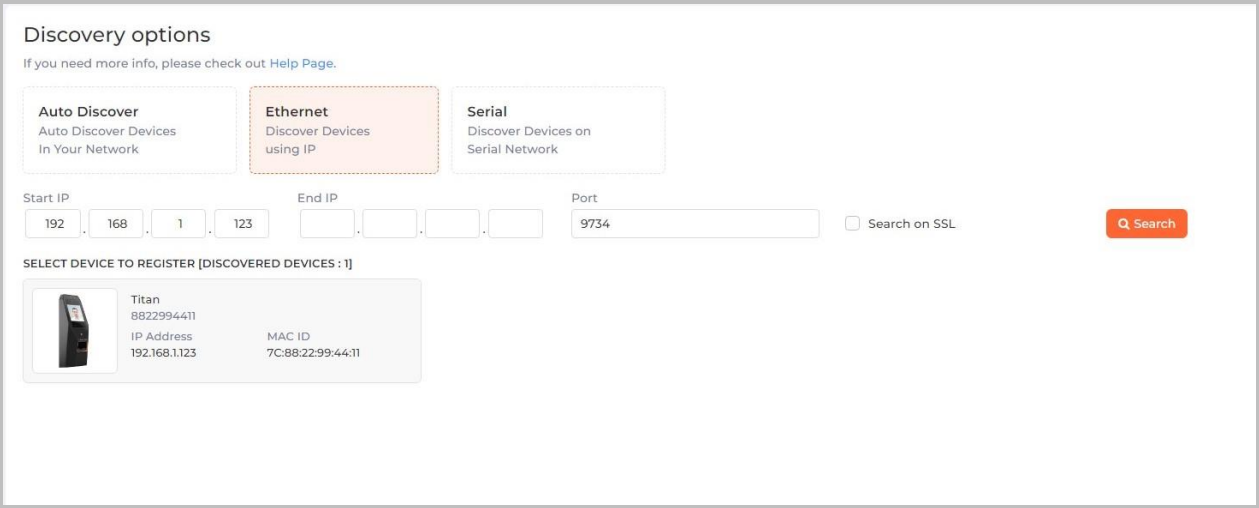


Figure 33: IXM WEB - Devices Tab

STEP 2

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



Discovery options

If you need more info, please check out [Help Page](#).

Auto Discover
Auto Discover Devices
In Your Network

Ethernet
Discover Devices
using IP

Serial
Discover Devices on
Serial Network

Start IP: 192 . 168 . 1 . 123 End IP: Port: 9734 Search on SSL **Search**

SELECT DEVICE TO REGISTER [DISCOVERED DEVICES : 1]


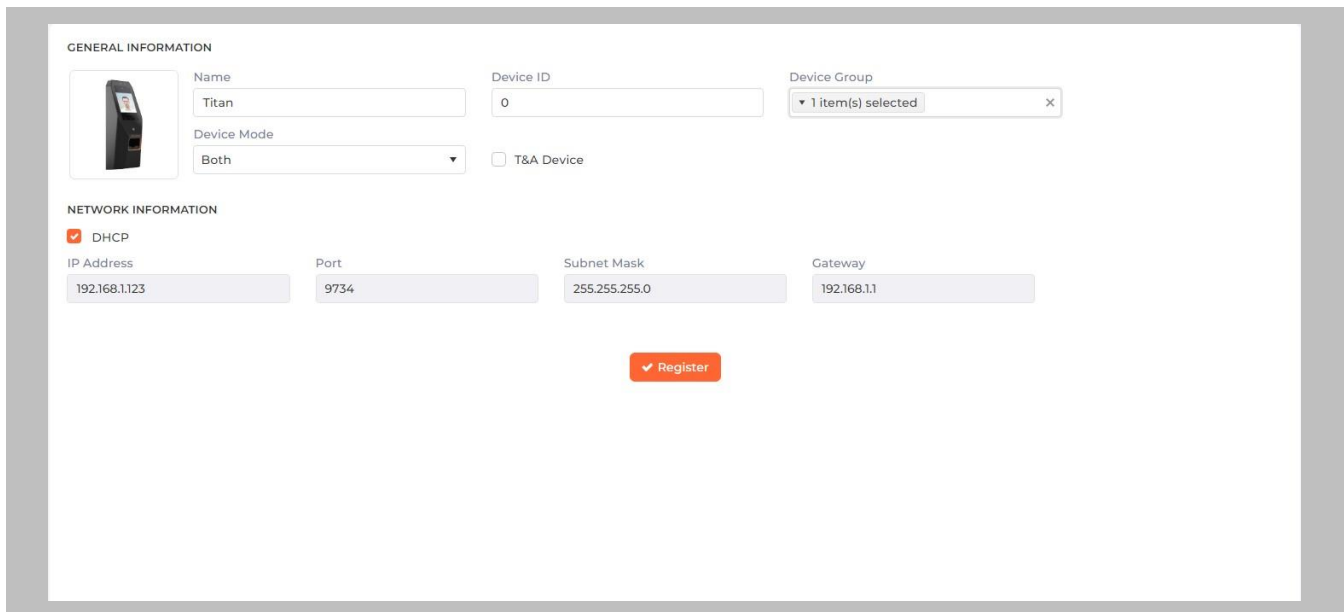
	Titan 8822994411	MAC ID
	IP Address 192.168.1.123	7C:88:22:99:44:11

Figure 34: 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 a web form for registering a device. It is divided into two main sections: GENERAL INFORMATION and NETWORK INFORMATION. In the GENERAL INFORMATION section, there is a device icon, a Name field with 'Titan', a Device ID field with '0', a Device Group dropdown menu showing '1 item(s) selected', a Device Mode dropdown menu with 'Both', and a checkbox for 'T&A Device'. In the NETWORK INFORMATION section, the DHCP checkbox is checked, and there are four input fields for IP Address (192.168.1.123), Port (9734), Subnet Mask (255.255.255.0), and Gateway (192.168.1.1). A red 'Register' button is located at the bottom center of the form.

Figure 35: 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**.

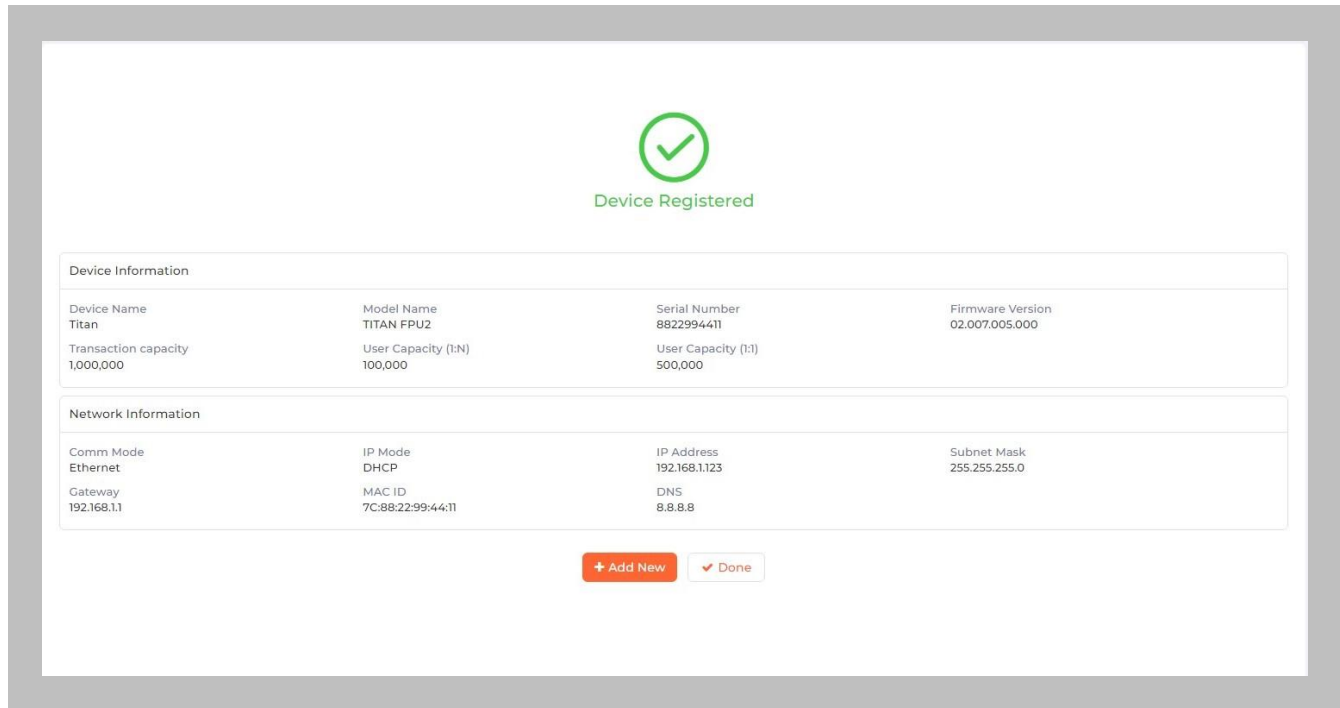


Figure 36: IXM WEB - Device Registration Complete

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).

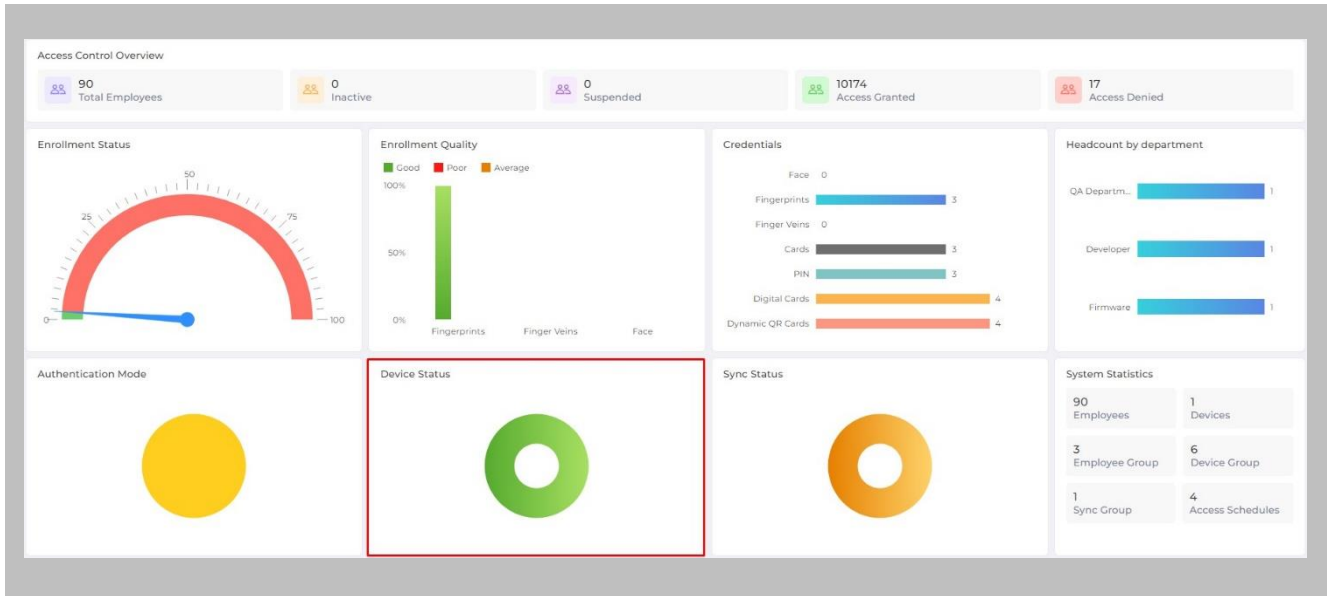


Figure 37: IXM WEB - Dashboard, Device Status

13. Adding an Invixium Device to a Device Group

Procedure

STEP 1

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

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

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

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

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

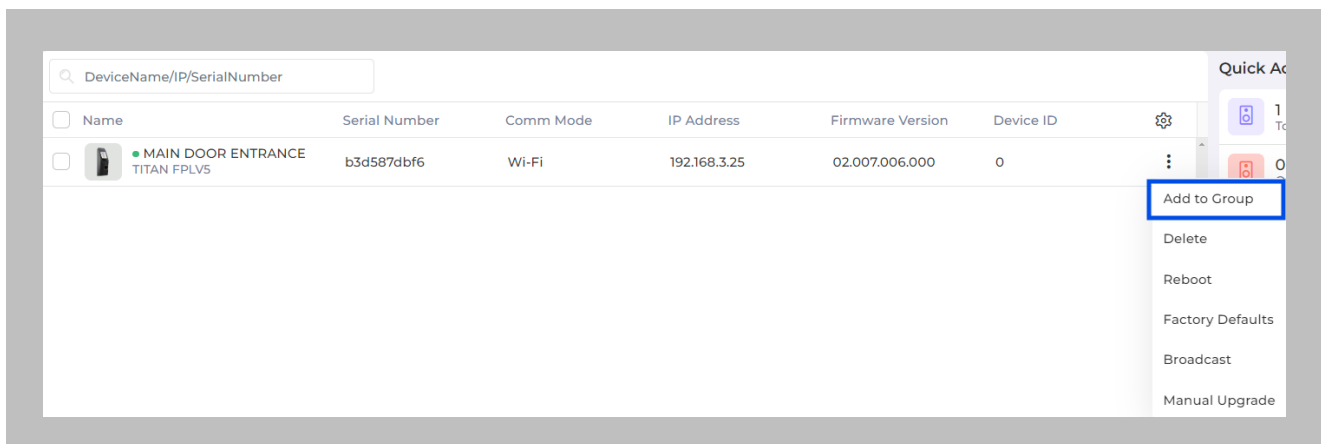



Figure 38: IXM WEB - Assign Device Group

Configuring Wiegand Format to Assign Invixium Readers

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

STEP 1

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

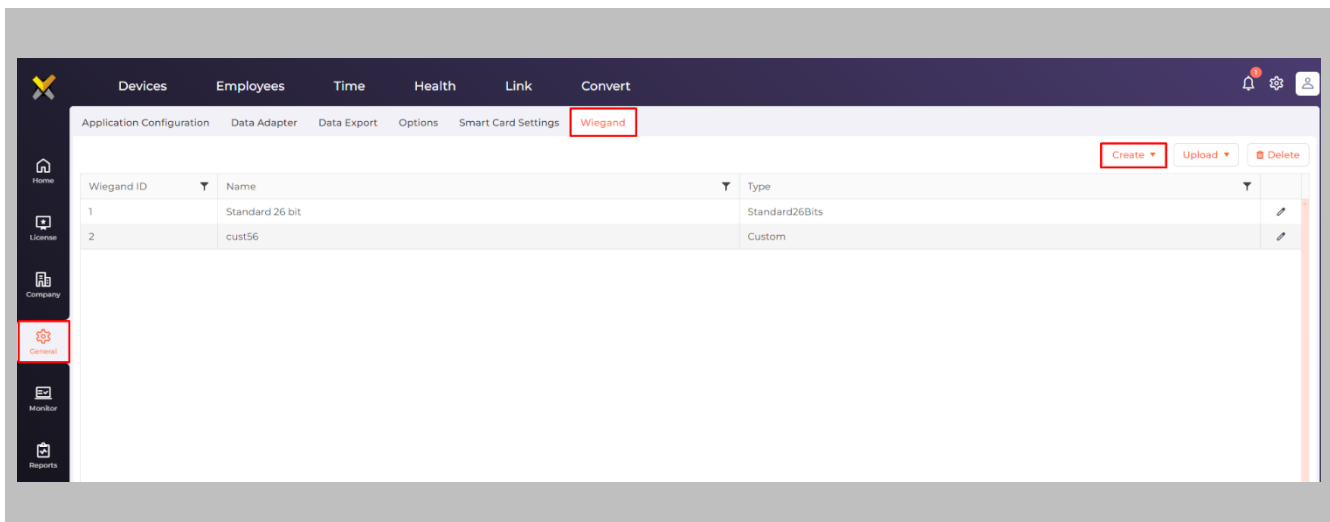


Figure 39: IXM WEB - Create Wiegand Format

STEP 2

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

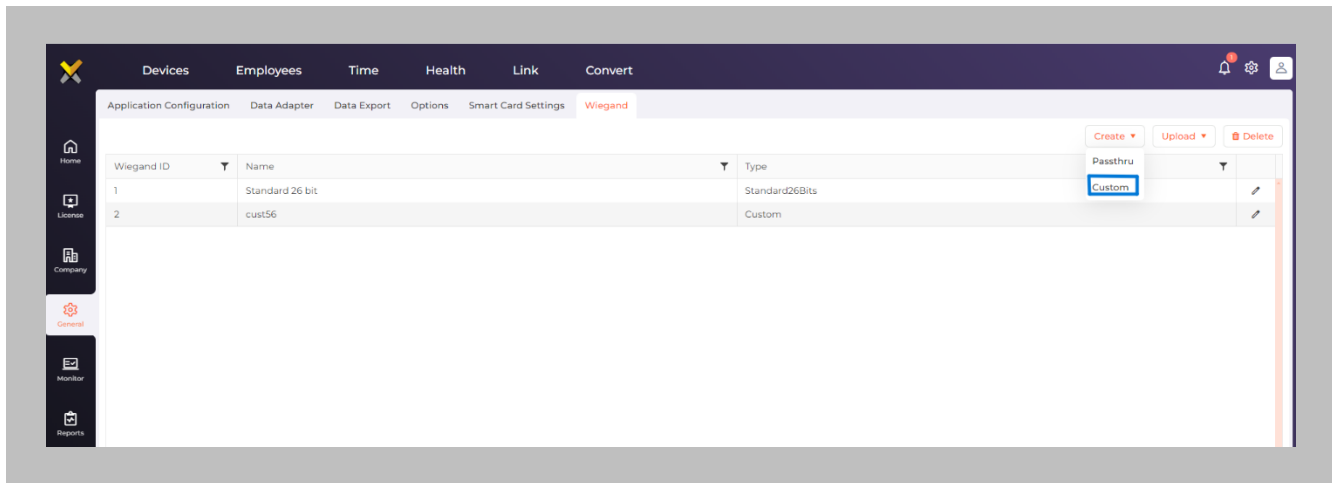


Figure 40: IXM WEB - Create Custom Wiegand Format

STEP 3

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

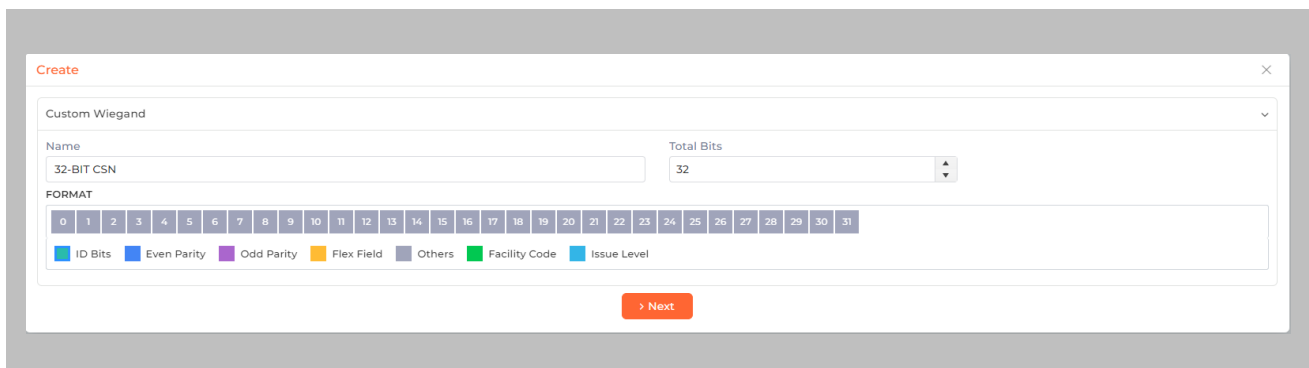


Figure 41: IXM WEB - Custom Wiegand Format

STEP 4

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

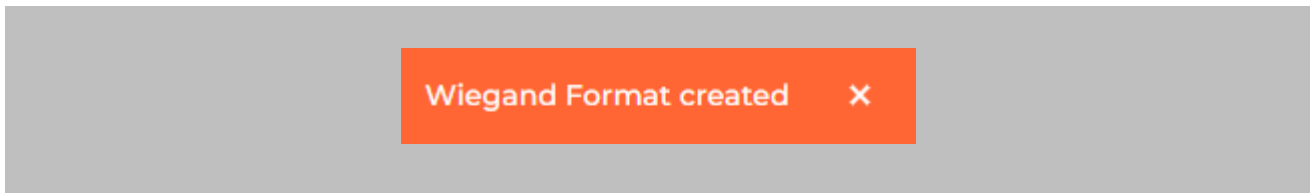


Figure 42: IXM WEB – Custom Wiegand Format Created

STEP 5

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

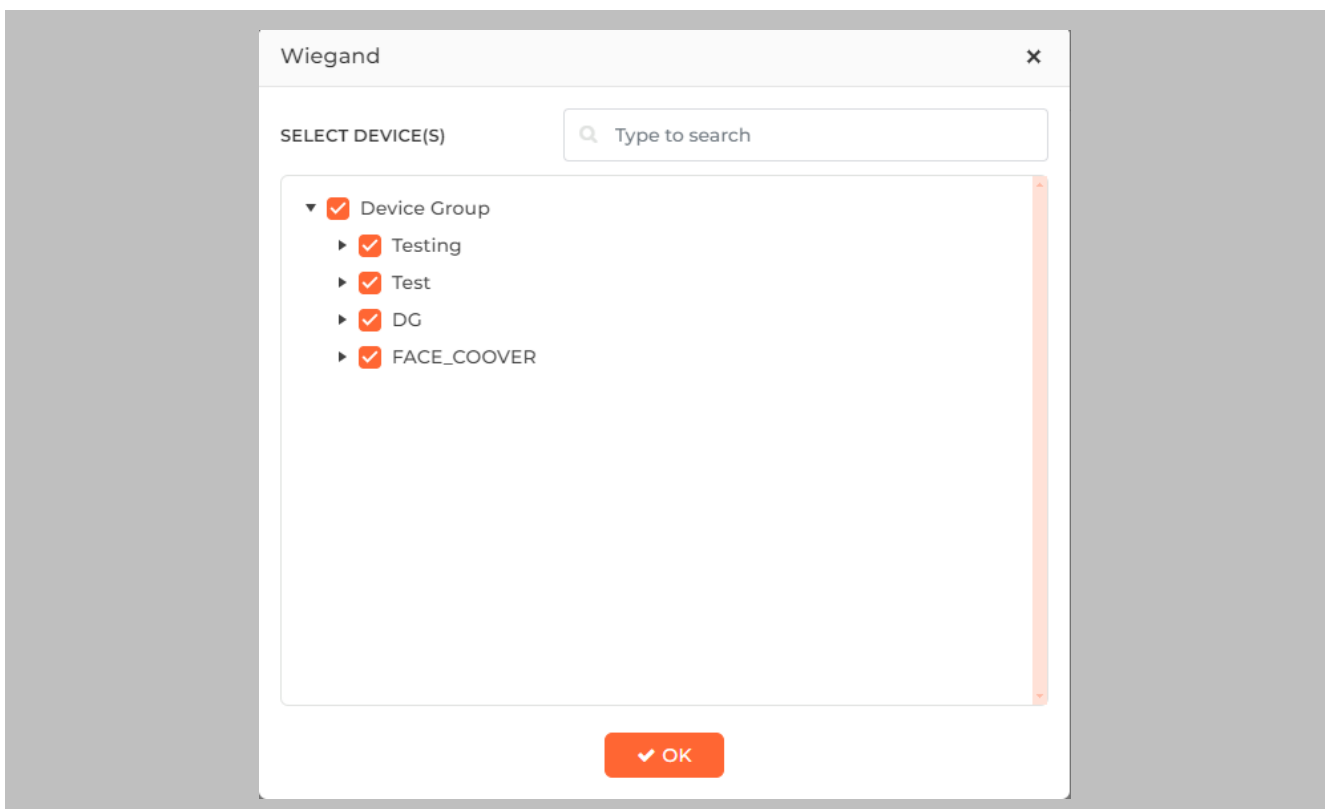


Figure 43: IXM WEB - Upload Wiegand Format

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 SiPort.

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.

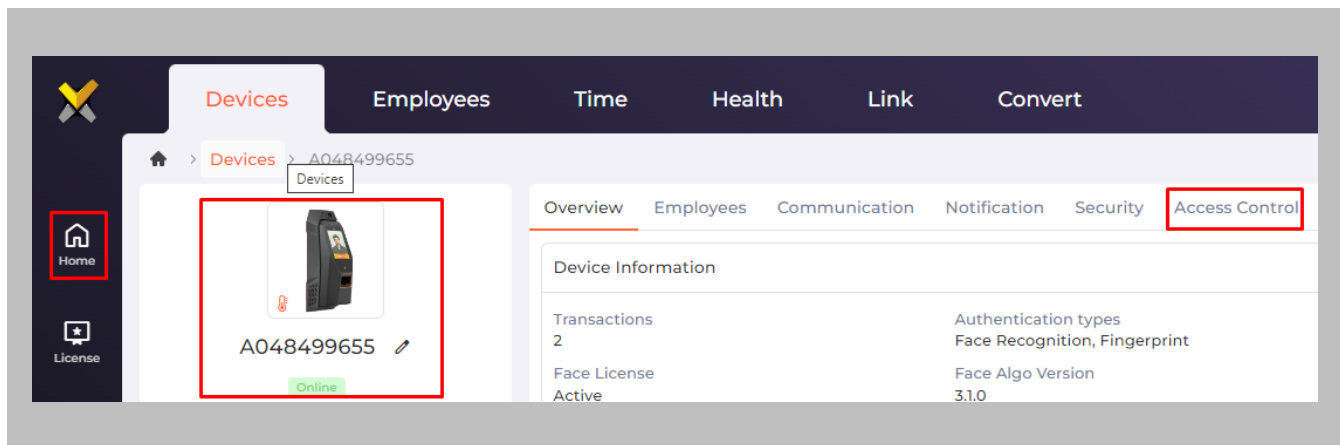


Figure 44: IXM WEB - Navigate to Access Control Tab

STEP 3

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

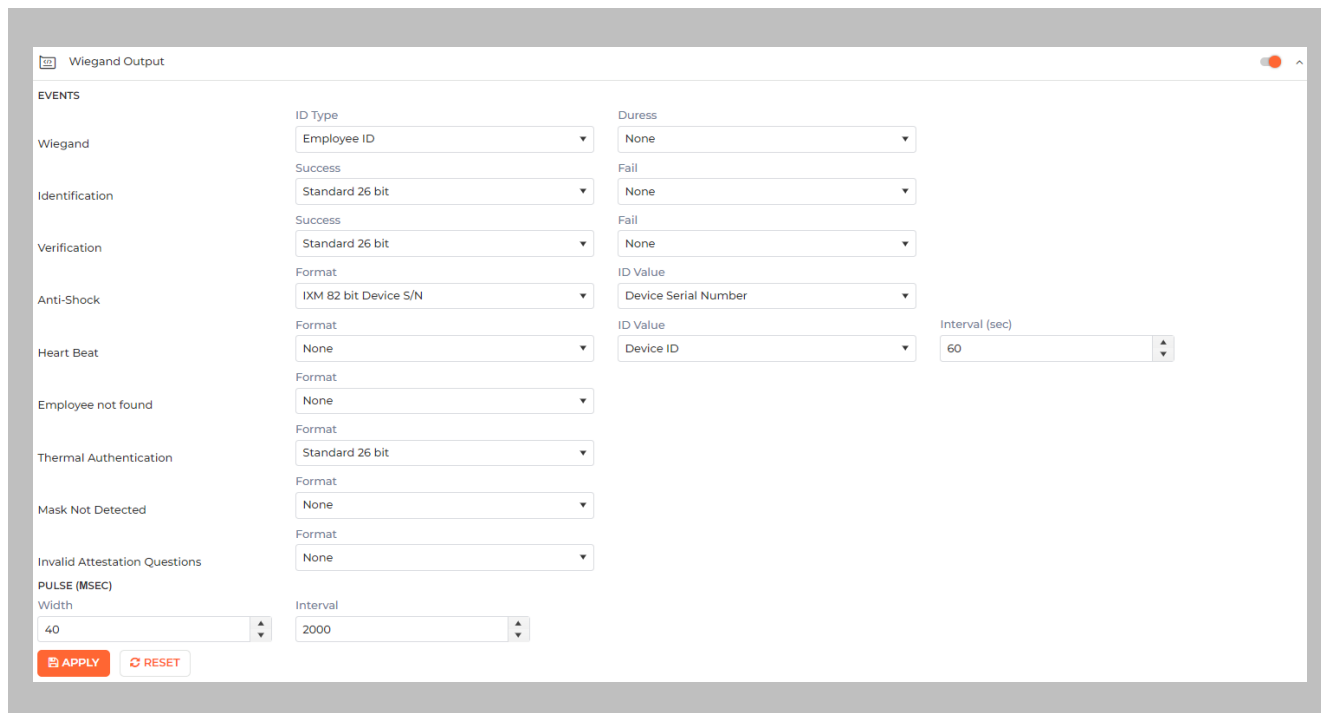


Figure 45: IXM WEB - Wiegand Output

ID types for Wiegand output are as follows:

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

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

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

Employee ID: This is auto generated ID by IXM WEB for an imported cardholder in SIEMENS.

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

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

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

STEP 4

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

STEP 5

Click **Apply**.

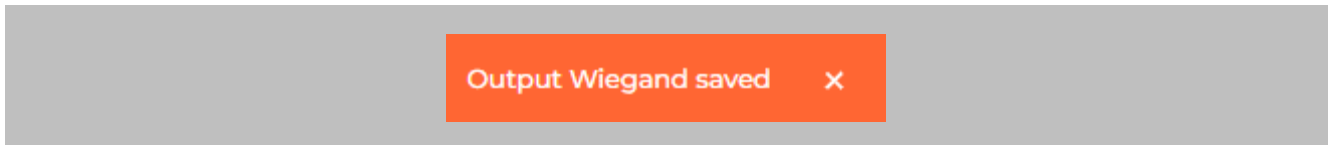


Figure 46: IXM WEB - Save Output Wiegand

RESULT

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

 **Note:**

- If you have more devices, follow the next steps to copy all Wiegand settings to all devices simultaneously. Note: This copies all Wiegand output settings. See Appendix 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 SiPort controller.
- To make this Wiegand output work on SiPort, you will need to make sure the Wiegand format is available in SiPort for use on the controllers talking to the Invixium reader (by Wiegand or OSDP).

Configuring Panel Feedback with SIEMENS

Procedure

STEP 1

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

STEP 2

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

STEP 3

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

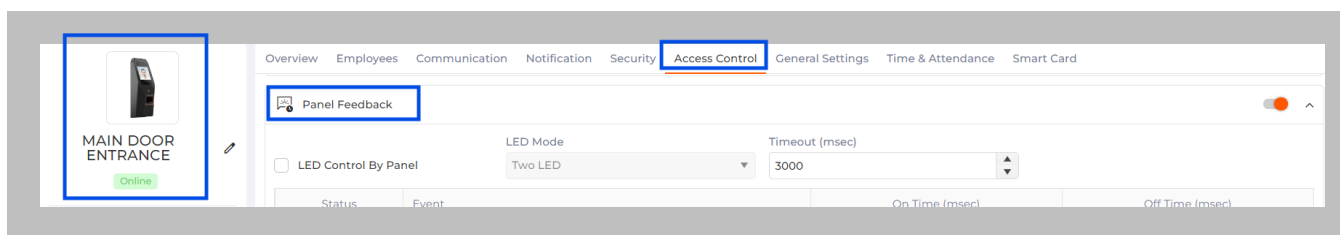
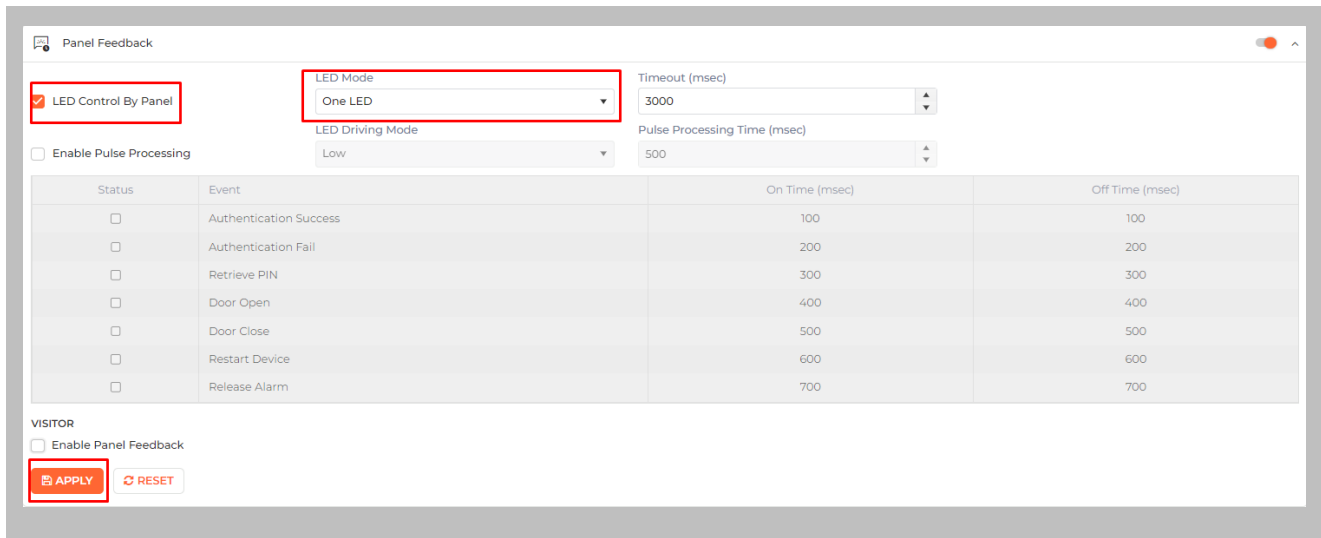


Figure 47: IXM WEB - Panel Feedback

STEP 4

By default, Panel Feedback is turned **OFF**. Toggle the Panel Feedback switch on the top right-hand 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)
<input type="checkbox"/>	Authentication Success	100	100
<input type="checkbox"/>	Authentication Fail	200	200
<input type="checkbox"/>	Retrieve PIN	300	300
<input type="checkbox"/>	Door Open	400	400
<input type="checkbox"/>	Door Close	500	500
<input type="checkbox"/>	Restart Device	600	600
<input type="checkbox"/>	Release Alarm	700	700

VISITOR

Enable Panel Feedback

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

STEP 5

Click **Apply**.

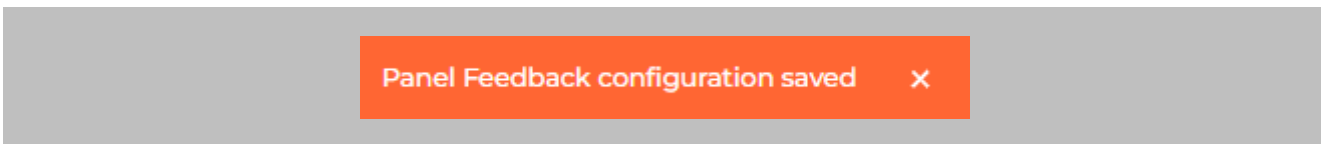


Figure 49: IXM WEB - Save Panel Feedback

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.

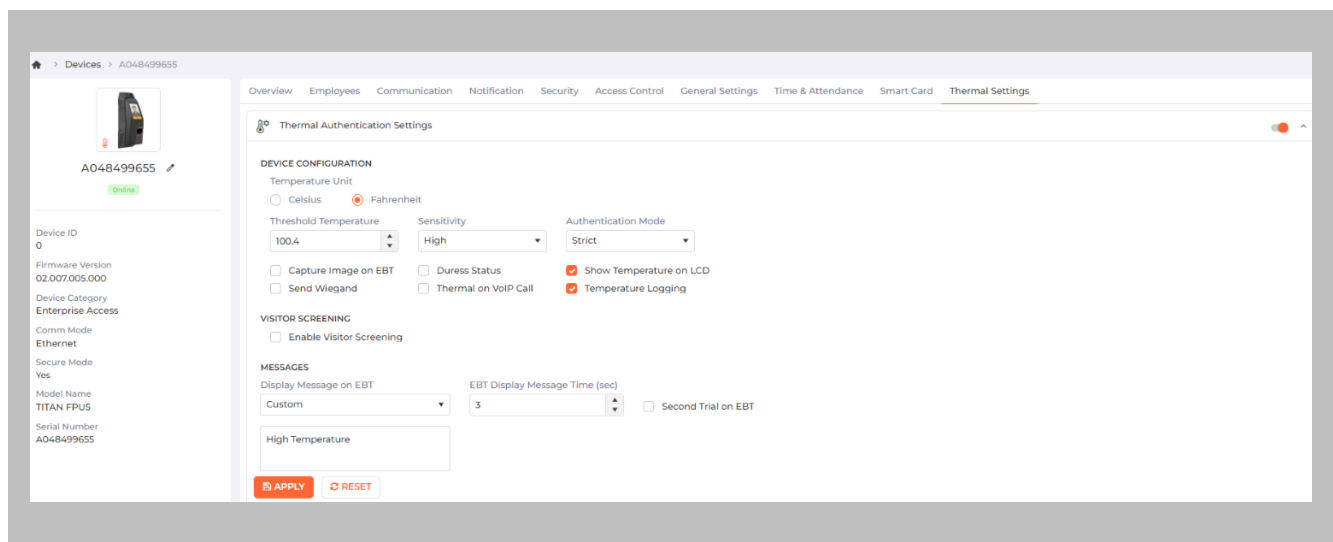


Figure 50: IXM WEB - Thermal Settings

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**.

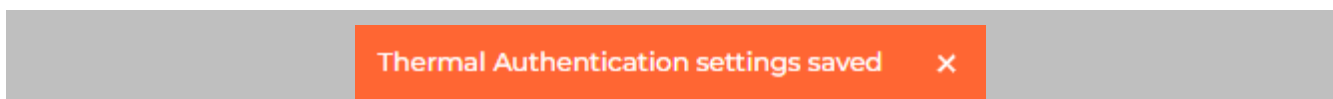


Figure 51: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

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

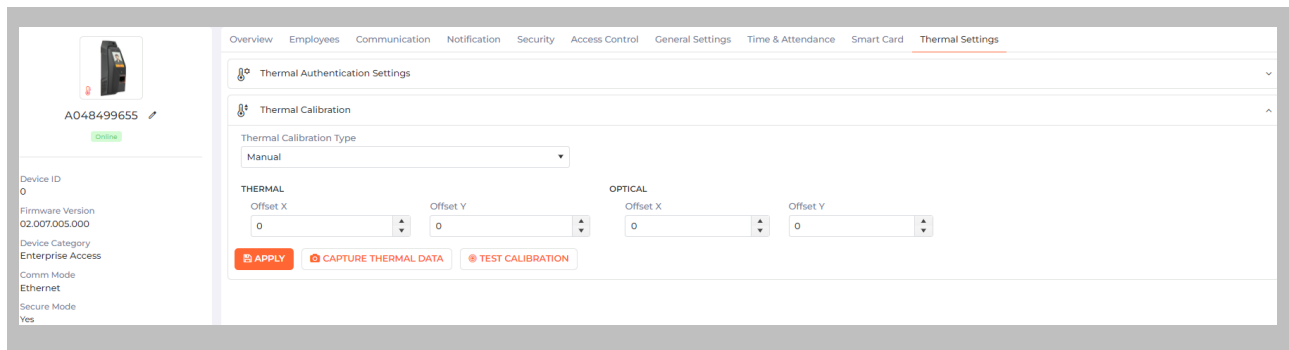


Figure 52: IXM WEB - Thermal Calibration Settings

STEP 2

The settings along with their functions are:

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

Invixium supports only Manual Thermal Calibration and does not recommend the user to 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**.

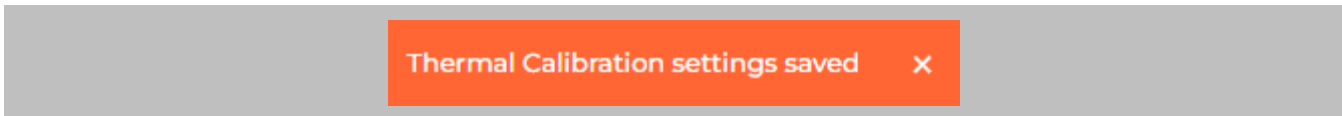


Figure 53: IXM WEB - Save Thermal Calibration Settings

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 54: IXM WEB - Capture Thermal Data

STEP 4

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

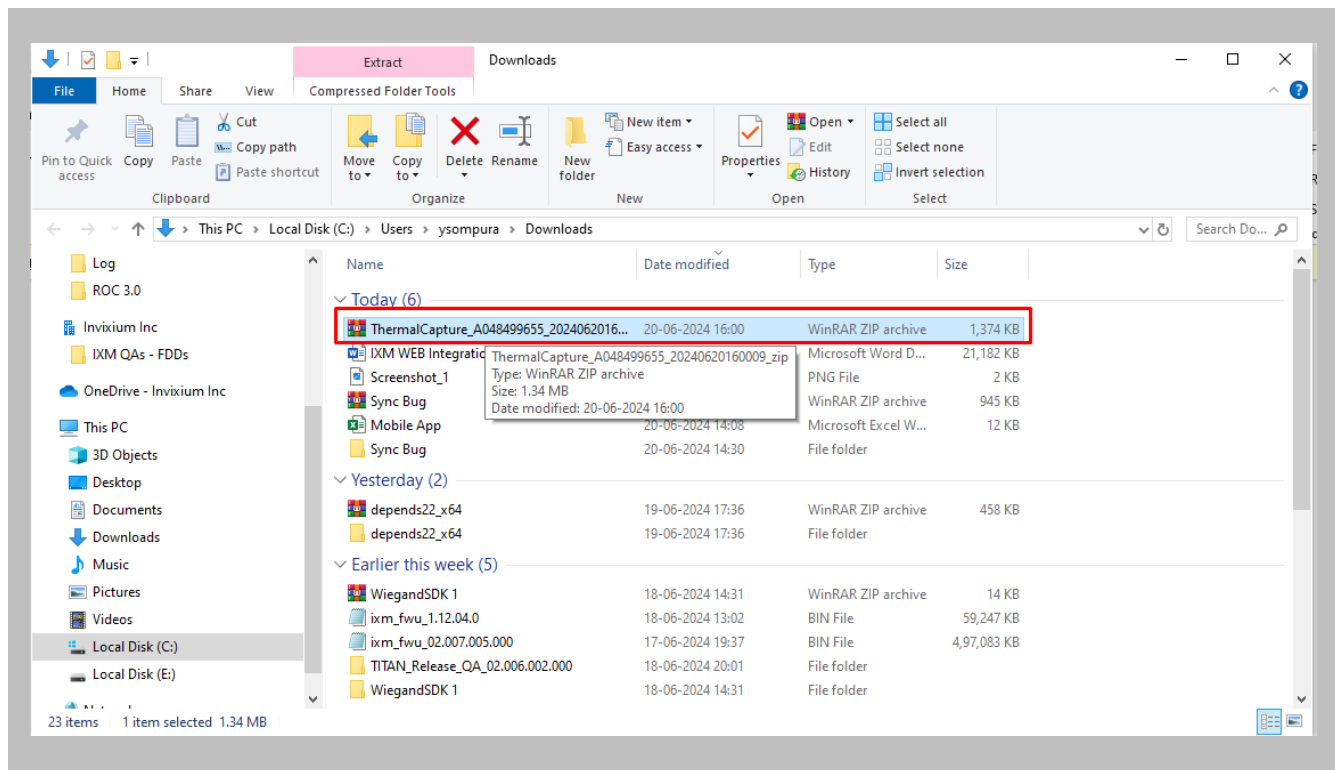



Figure 55: IXM WEB - Save Captured Thermal Data

STEP 5

Click **Save** to store the zip file, then send this file to support@invixium.com. Invixium’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](#).

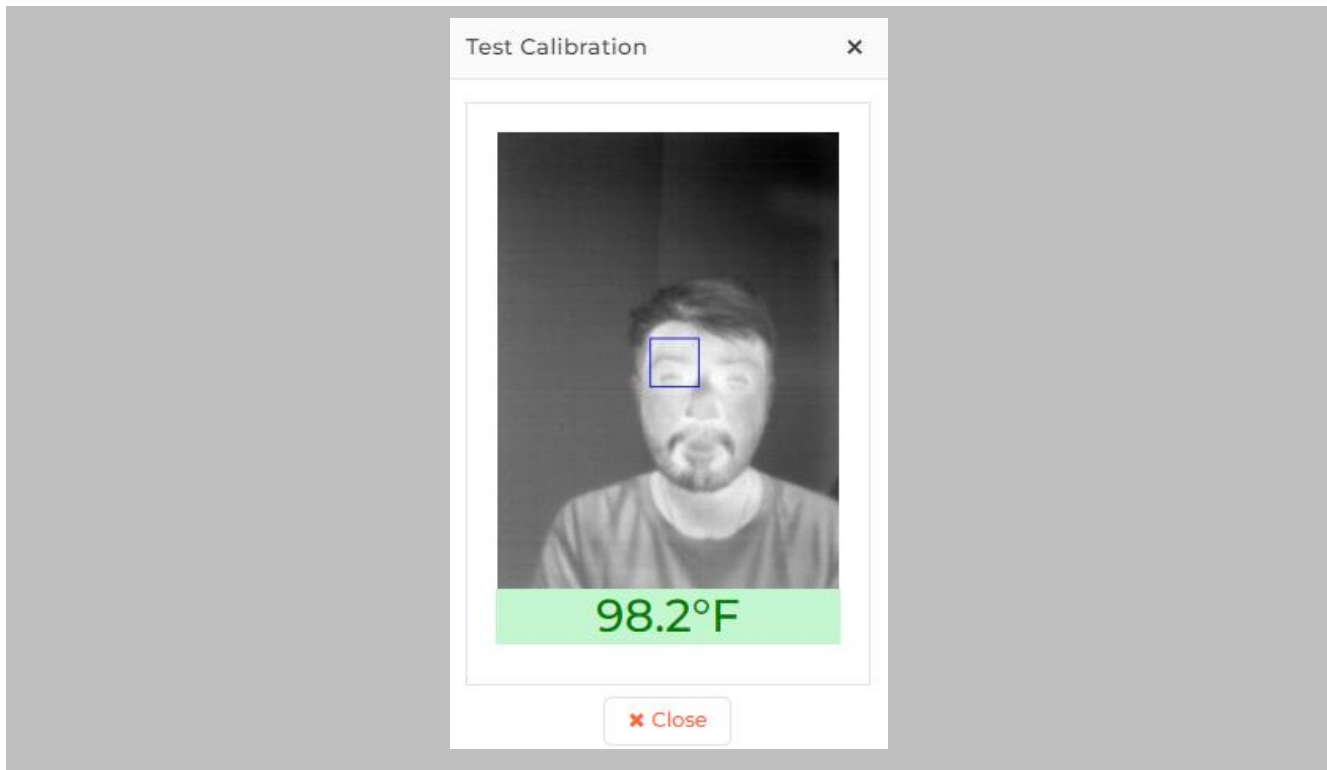



Figure 56: IXM WEB - Test Thermal Calibration

 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 **General** → **Options** → **Temperature Unit**.

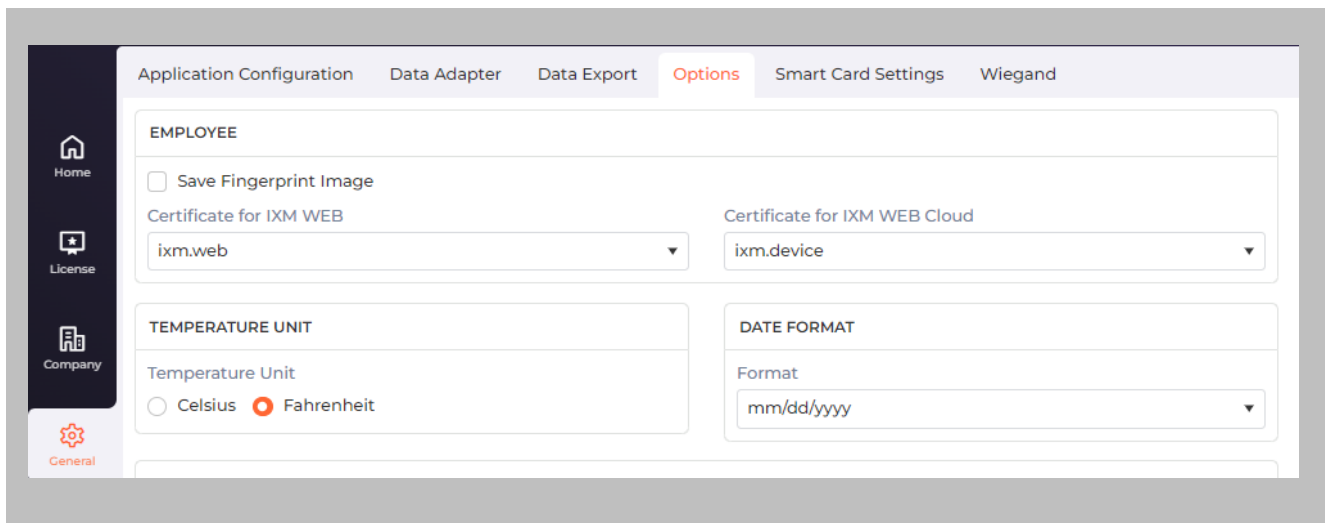
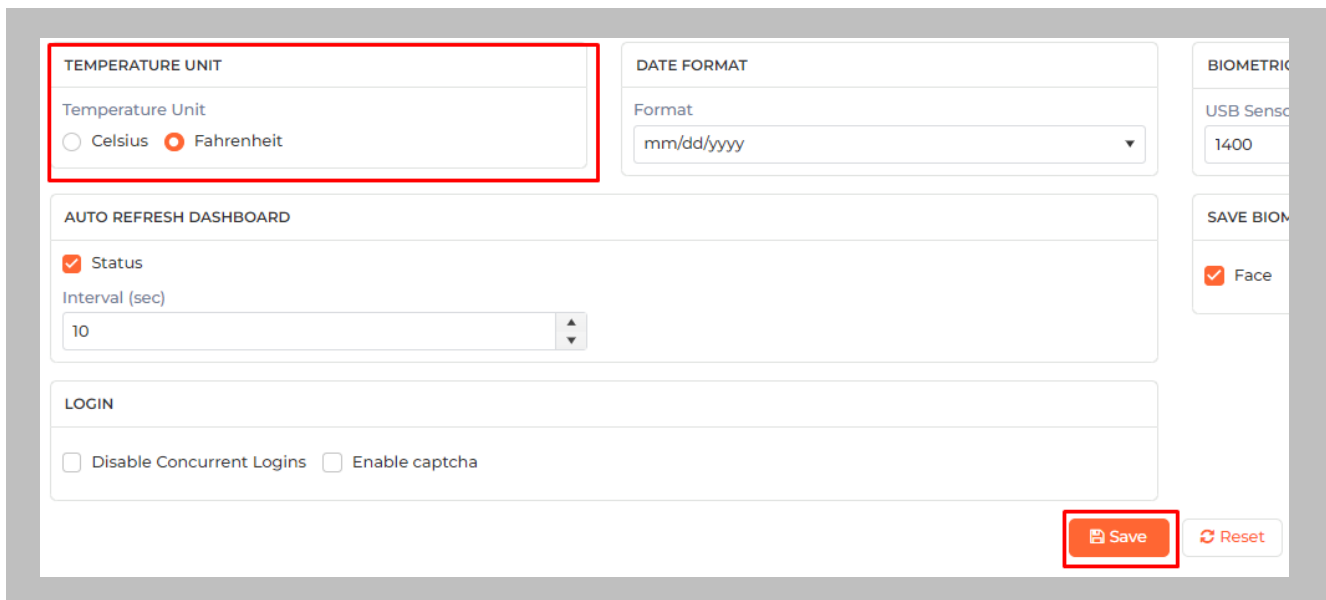


Figure 57: IXM WEB - Option to Change Temperature Unit

STEP 2

Select required temperature unit. Click **Save**.



The screenshot displays the configuration interface for the IXM WEB system. The 'TEMPERATURE UNIT' section is highlighted with a red box and contains the following elements:

- TEMPERATURE UNIT**
- Temperature Unit
- Celsius
- Fahrenheit

Other visible settings include:

- DATE FORMAT**: Format dropdown menu set to 'mm/dd/yyyy'.
- AUTO REFRESH DASHBOARD**: 'Status' checkbox is checked; 'Interval (sec)' is set to 10.
- LOGIN**: 'Disable Concurrent Logins' and 'Enable captcha' checkboxes are unchecked.
- BIOMETRIC**: 'USB SENSING' is set to 1400; 'SAVE BIOMETRIC' section has 'Face' checkbox checked.
- Buttons**: 'Save' and 'Reset' buttons are located at the bottom right, with the 'Save' button highlighted by a red box.

Figure 58: 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.

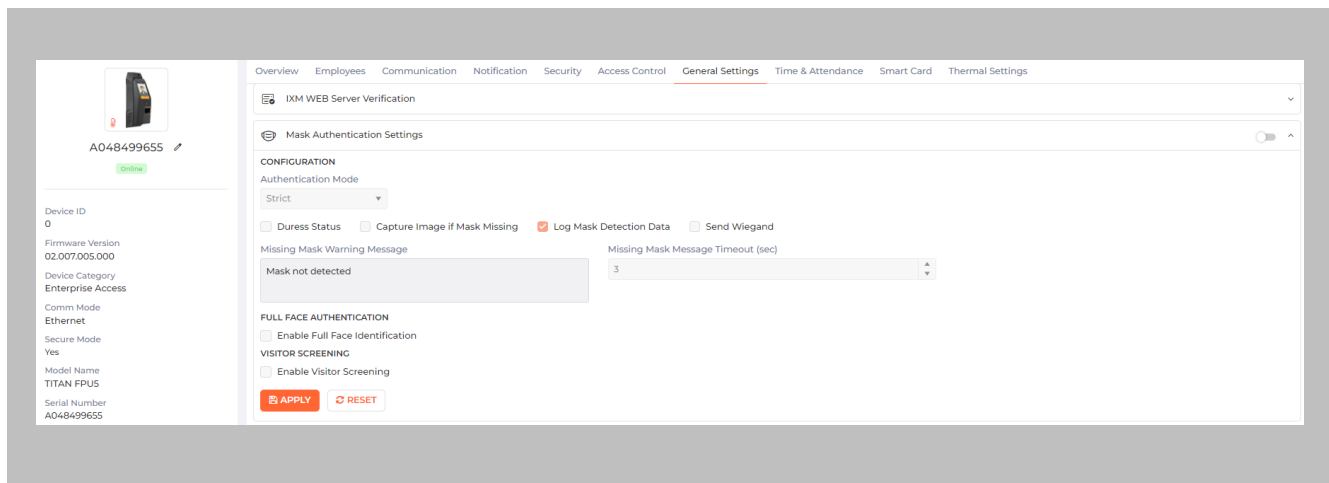


Figure 59: IXM WEB - Mask Authentication Settings

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**.

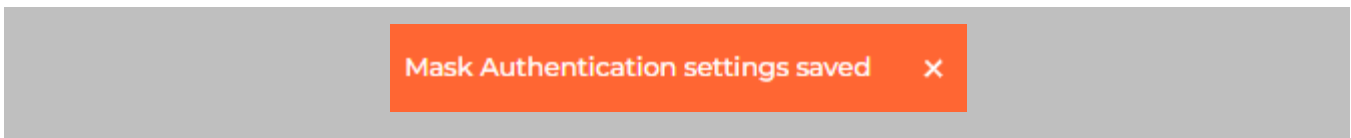


Figure 60: IXM WEB - Save Mask Settings

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 required.

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 from finger before placement.

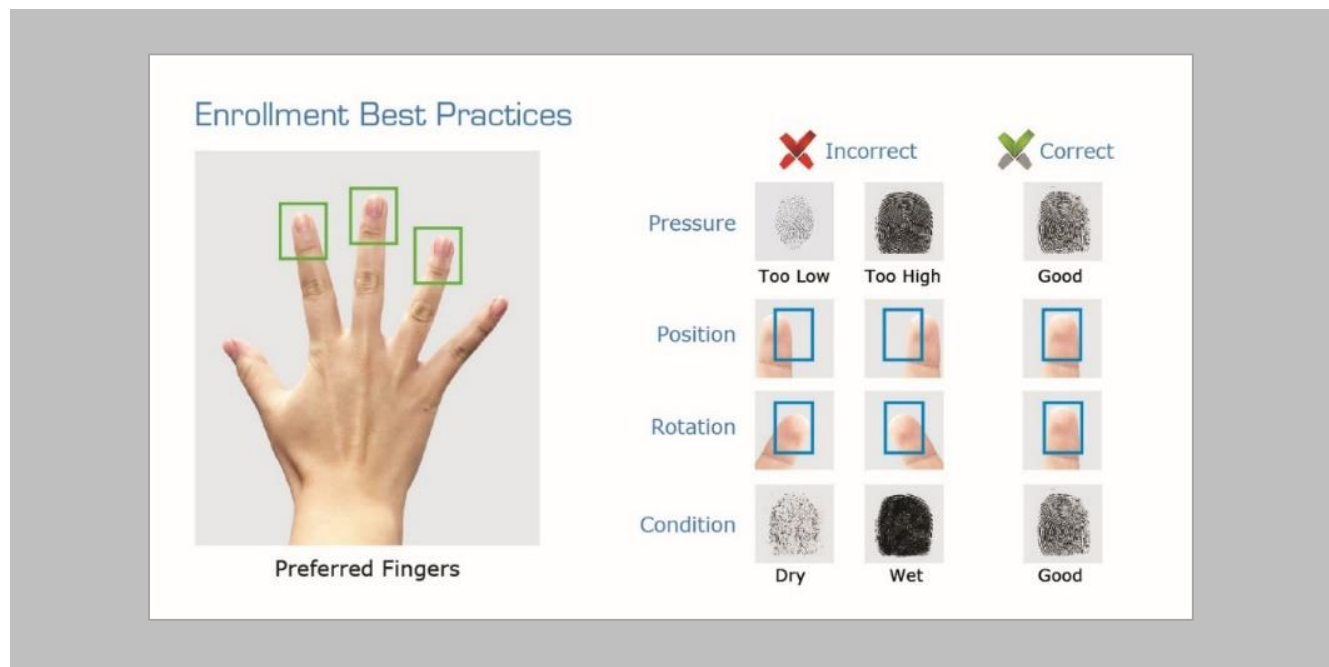


Figure 61: Fingerprint Enrollment Best Practices

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	Inxium 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.

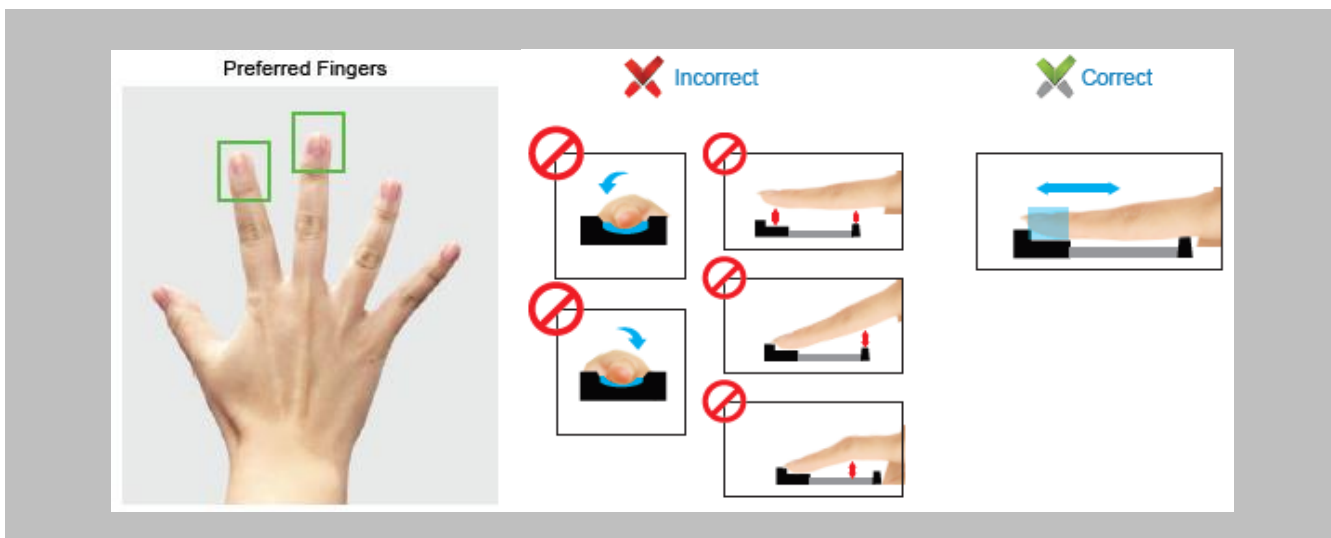


Figure 63: Finger Vein Enrollment Best Practices

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.

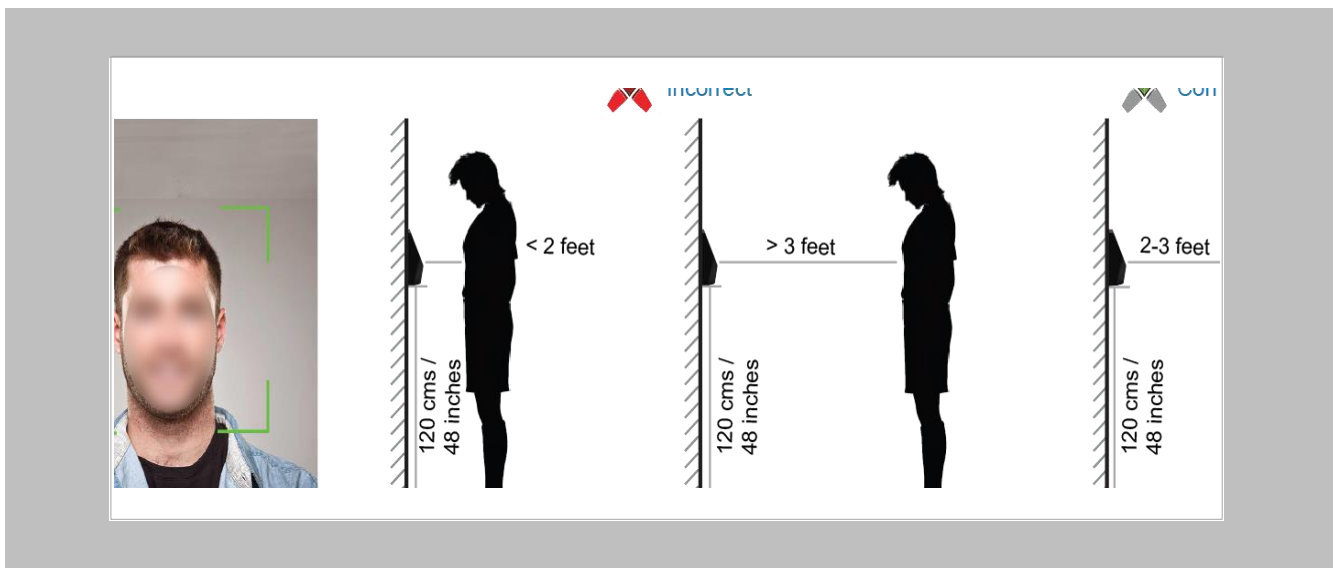


Figure 64: Face Enrollment Best Practices

15. 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 65: Install IXM WEB



Note: Installs SQL 2014 Express.

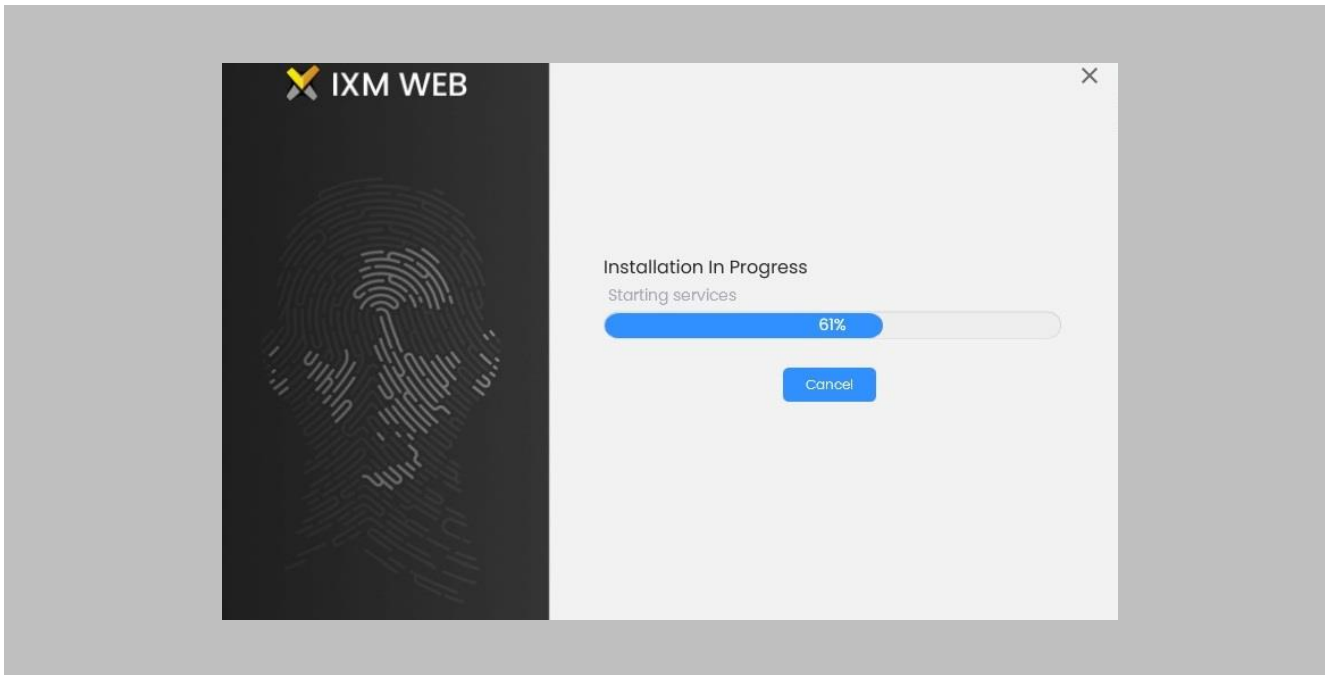


Figure 66: Loading SQL Express & Installation Progress

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 or your desktop.

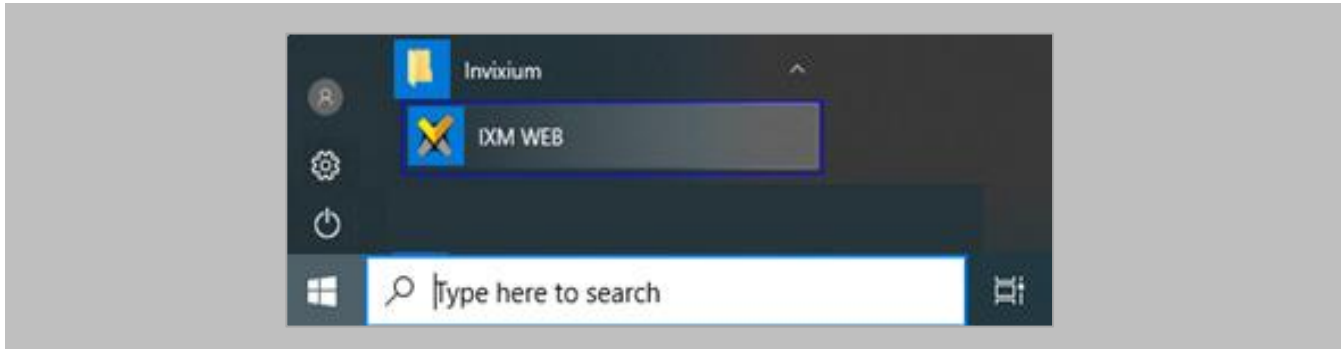


Figure 67: IXM WEB - Shortcut Icon on Desktop

STEP 4

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

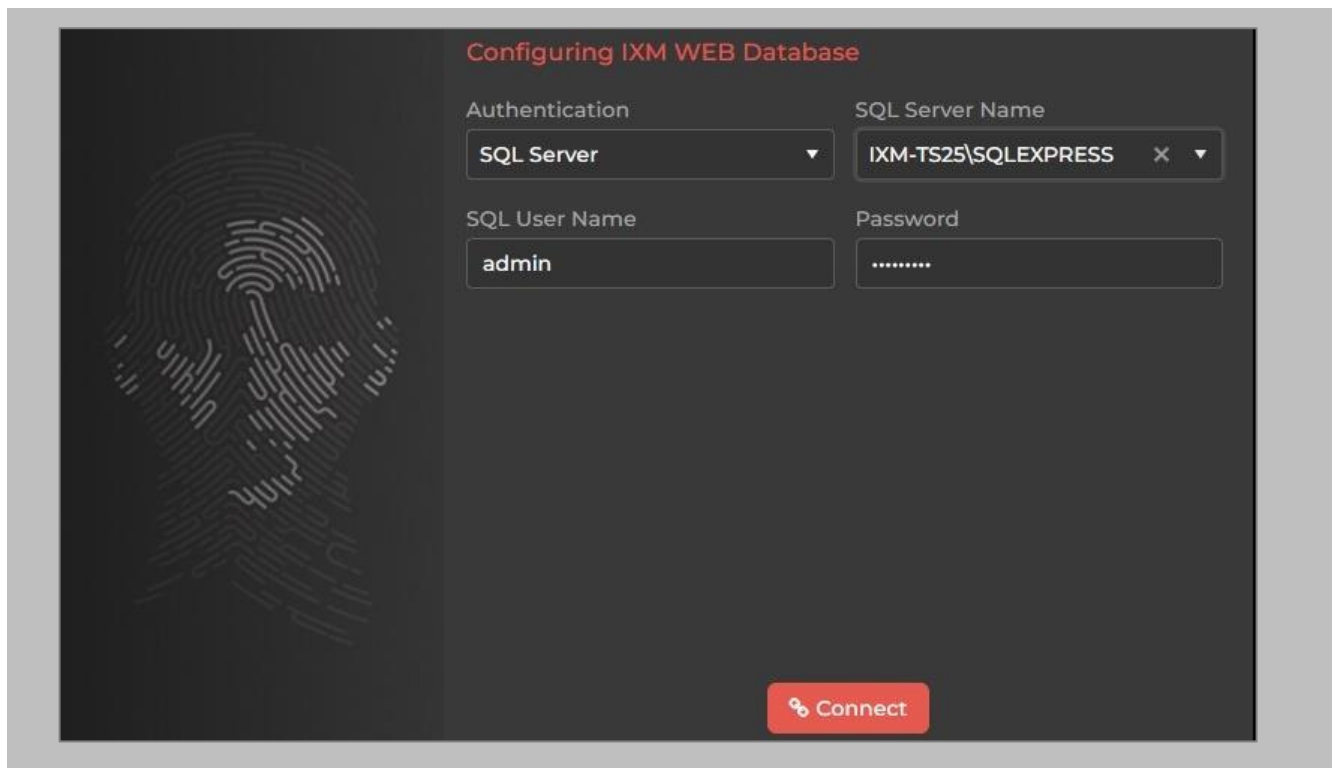


Figure 68: IXM WEB - Configuring IXM WEB Database

STEP 5

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

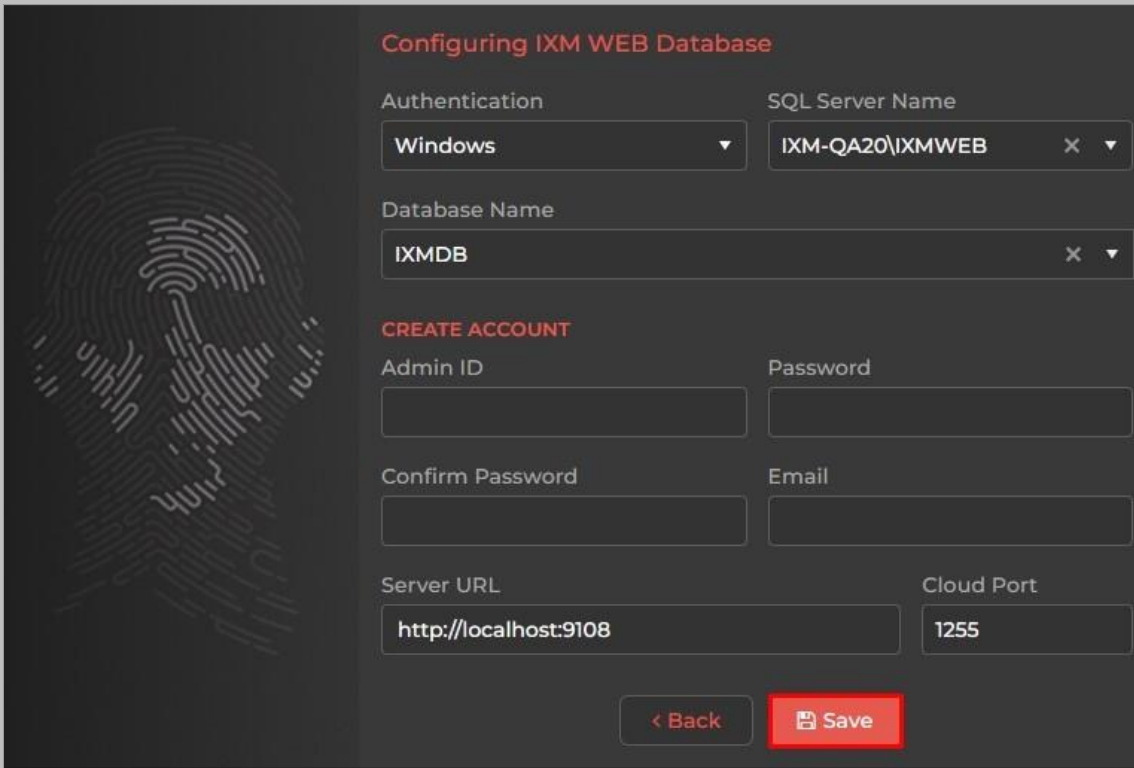


Figure 69: IXM WEB - Select Database Name

STEP 6

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 7

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 8

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

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 from vertical ellipses button.

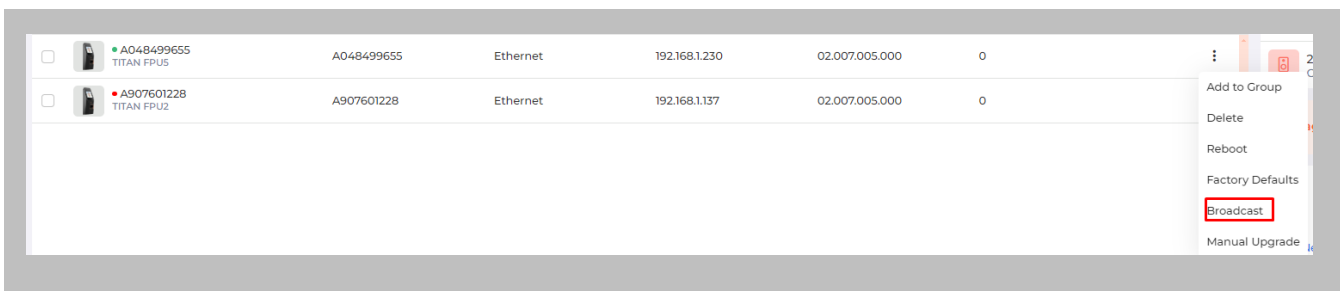


Figure 70: IXM WEB - Broadcast Option

STEP 2

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

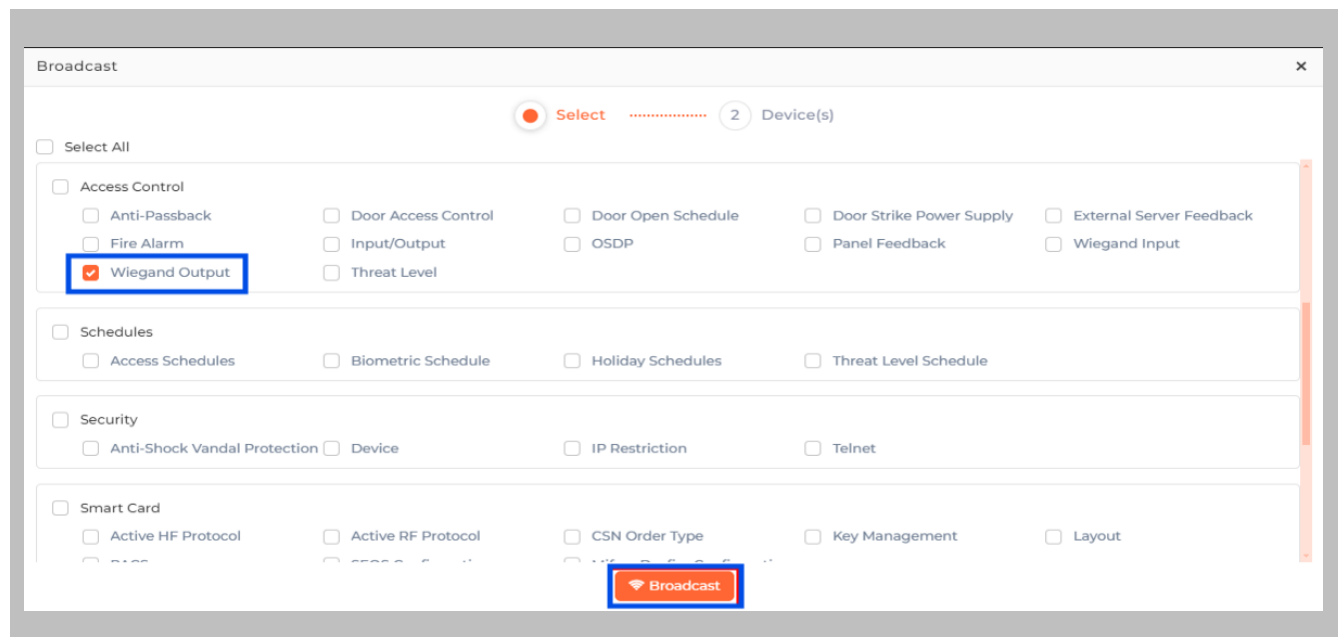


Figure 71: IXM WEB - Broadcast Wiegand Output Settings

STEP 3

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

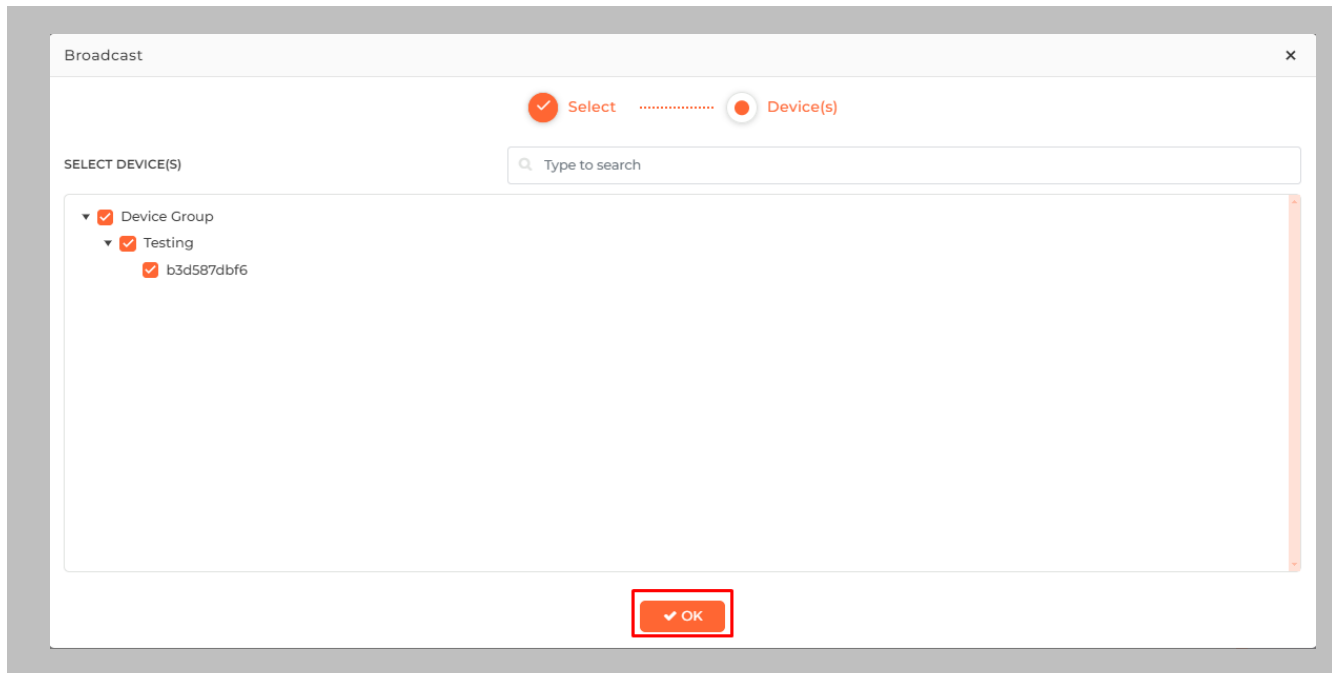


Figure 72: IXM WEB - Broadcast to Devices


STEP 2

Provide **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 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.
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	<p>The OSDP static events for panel feedback and capture pin are:</p> <ul style="list-style-type: none"> Access Granted Access Denied Enter PIN <p>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:</p> <ul style="list-style-type: none"> • The Device will request the credentials of the second

	<p>user after the first user is authenticated successfully.</p> <ul style="list-style-type: none"> • Card numbers for both, the first and the second user will be transferred to the Access Control Panel. <p>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>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
Enable VISITOR OSDP	<p>The option sends card details to ACP even if then card is not assigned to any employee on device. Based on response from ACP; device will display "Access Granted" or "Access Denied"</p>

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 disable: Displays only the Access Control Panel notification.</p>

Table 6: IXM WEB - OSDP Text Options

STEP 3

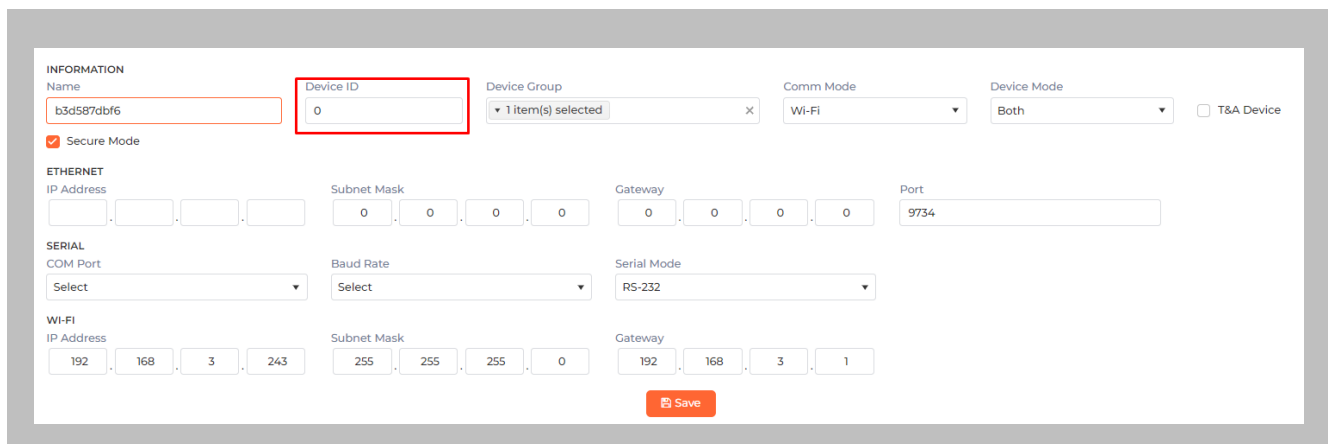
Click **Apply** to save the settings.

OSDP settings saved ×

Figure 74: 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.



The form displays configuration options for a device. The **Device ID** field is highlighted with a red box and contains the value '0'. Other fields include Name (b3d587dbf6), Device Group (1 item(s) selected), Comm Mode (Wi-Fi), Device Mode (Both), and T&A Device (unchecked). The **ETHERNET** section includes IP Address, Subnet Mask (0.0.0.0), Gateway (0.0.0.0), and Port (9734). The **SERIAL** section includes COM Port (Select), Baud Rate (Select), and Serial Mode (RS-232). The **WI-FI** section includes IP Address (192.168.3.243), Subnet Mask (255.255.255.0), and Gateway (192.168.3.1). A **Save** button is located at the bottom right.

Figure 75: IXM WEB - Edit Device Options

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 SiPort.

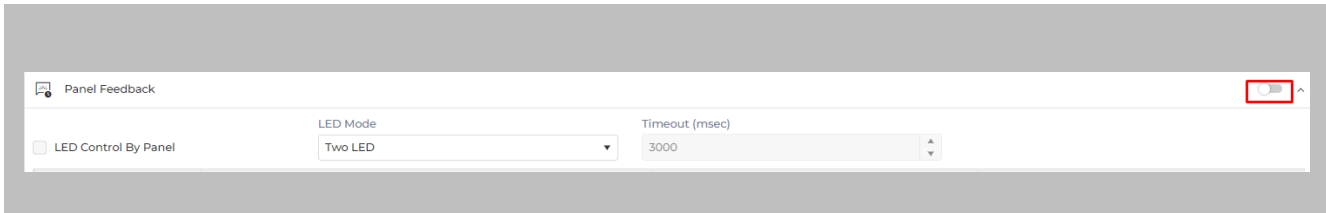


Figure 76: IXM WEB - Disable Panel Feedback

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 77: 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.

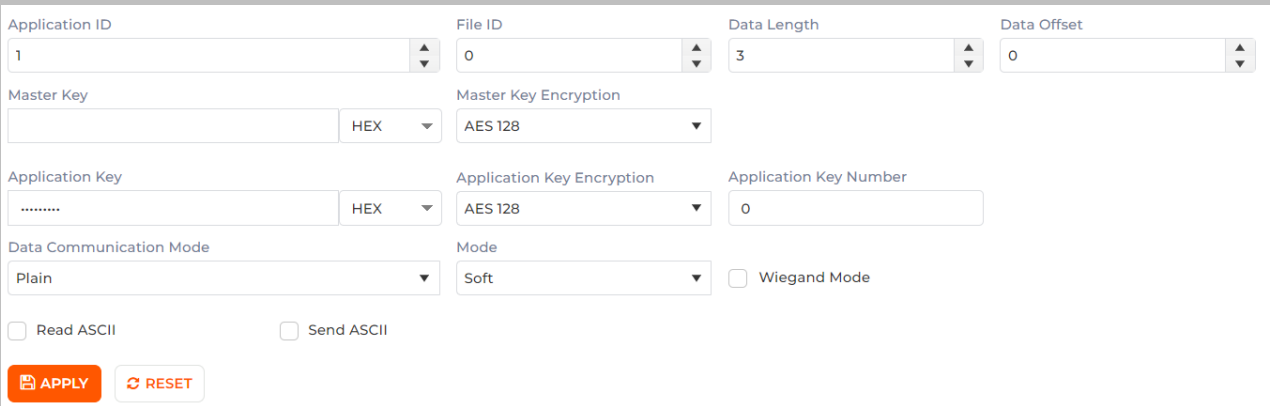
Master Key Encryption	<p>Select Master Key Encryption from the dropdown as per requirement. Options are:</p> <ul style="list-style-type: none"> • None • 2K 3DES • 3K 3DES • AES 128
Application Key	Enter the Application key of SIEMENS cards.
Application Key Encryption	<p>Select Application Key Encryption from the dropdown as per requirement. Options are:</p> <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	<p>Select Data Communication Mode from the dropdown as per requirement. Options are:</p> <ul style="list-style-type: none"> • Plain • MAC • Enciphered
Mode	<p>Select the Mode from the dropdown as per requirement. Options are:</p> <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 following configuration details:

- Application ID:** 1
- File ID:** 0
- Data Length:** 3
- Data Offset:** 0
- Master Key:** [Empty field] HEX
- Master Key Encryption:** AES 128
- Application Key:** [Dotted field] HEX
- 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 78: 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 ground.

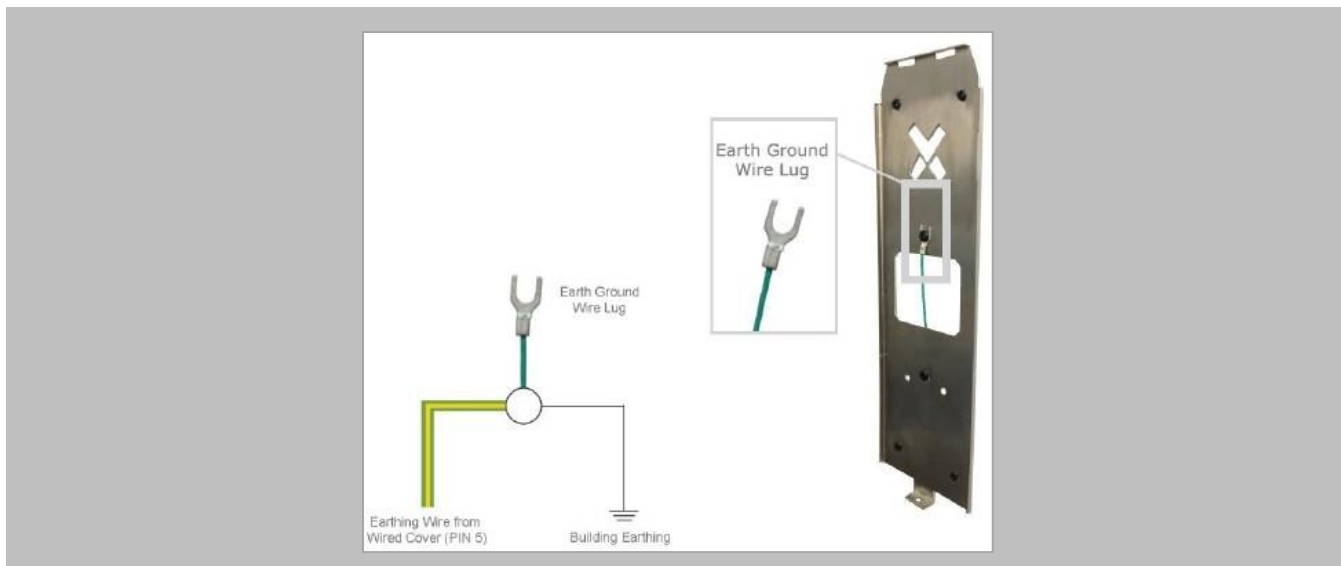


Figure 79: Earth Ground Wiring

Wiring

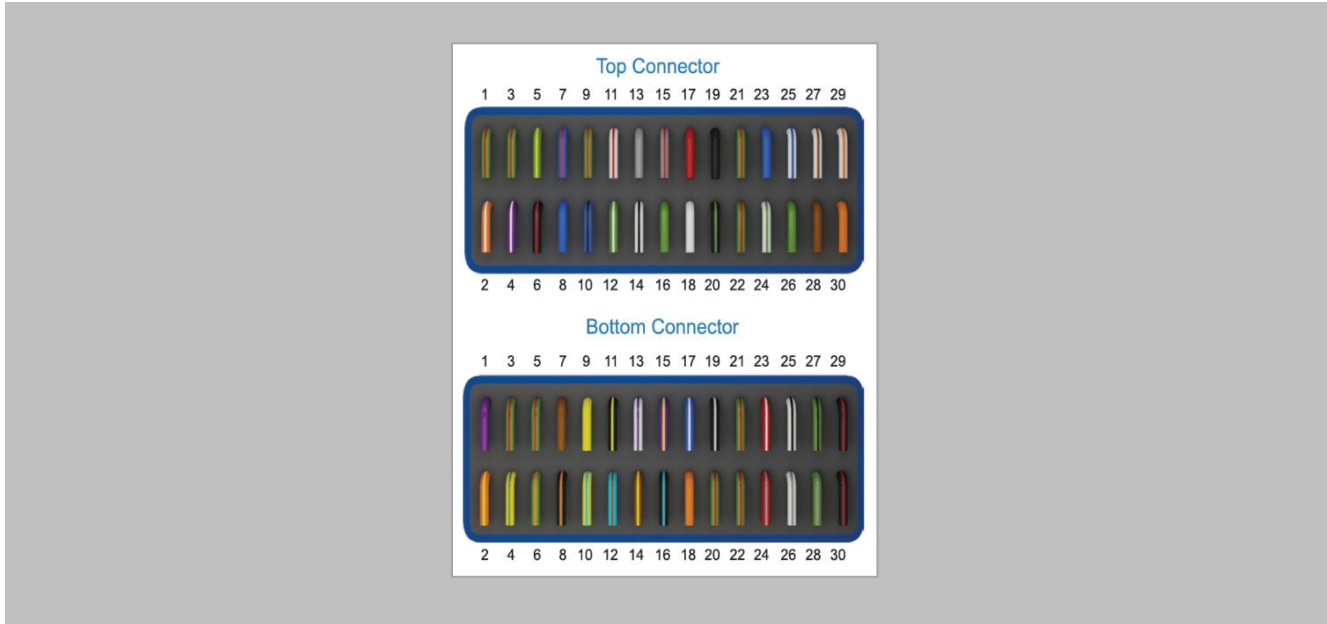


Figure 80: IXM TITAN – Top & Bottom Connector Wiring

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 81: 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

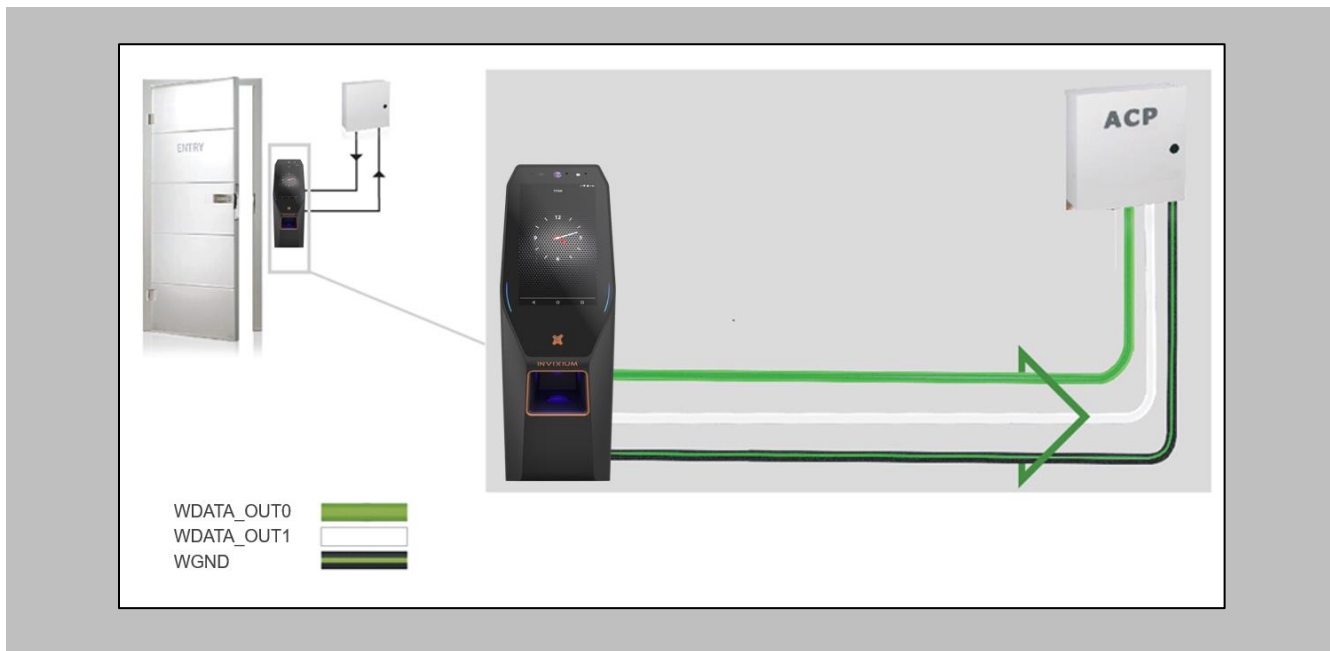



Figure 82: IXM TITAN - Wiegand

 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

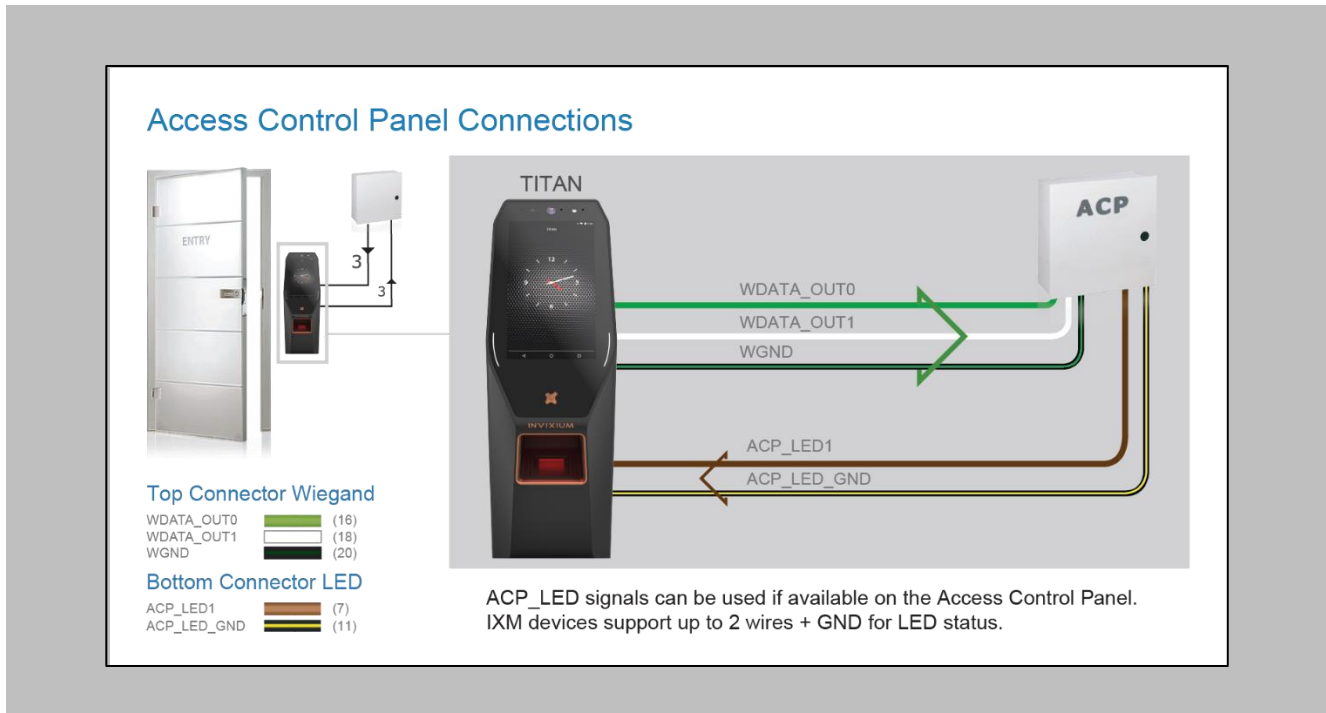



Figure 83: IXM TITAN - Panel Feedback

 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

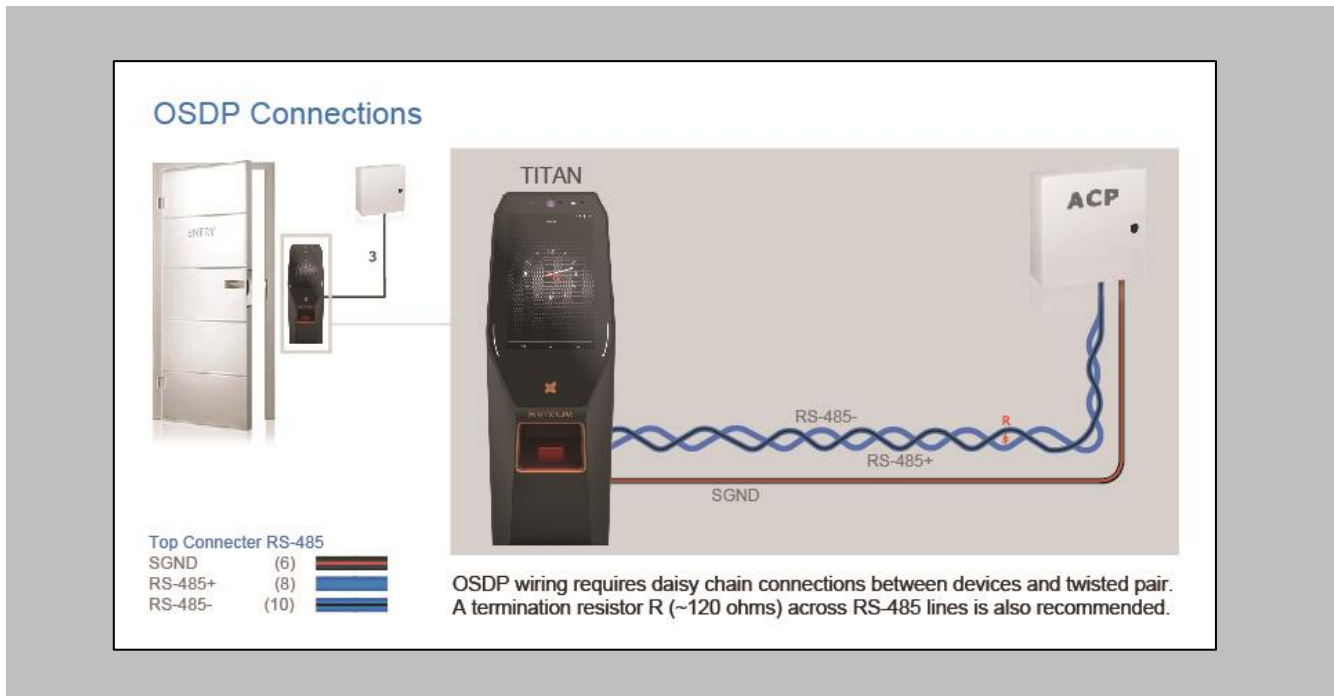



Figure 84: IXM TITAN - OSDP Connections

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

16. Troubleshooting

Reader Offline from the IXM WEB Dashboard



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

Procedure

STEP 1

From **Devices** tab select any device.

STEP 2

Navigate to the **Communication** tab. Scroll down and click on **IXM WEB Server**.

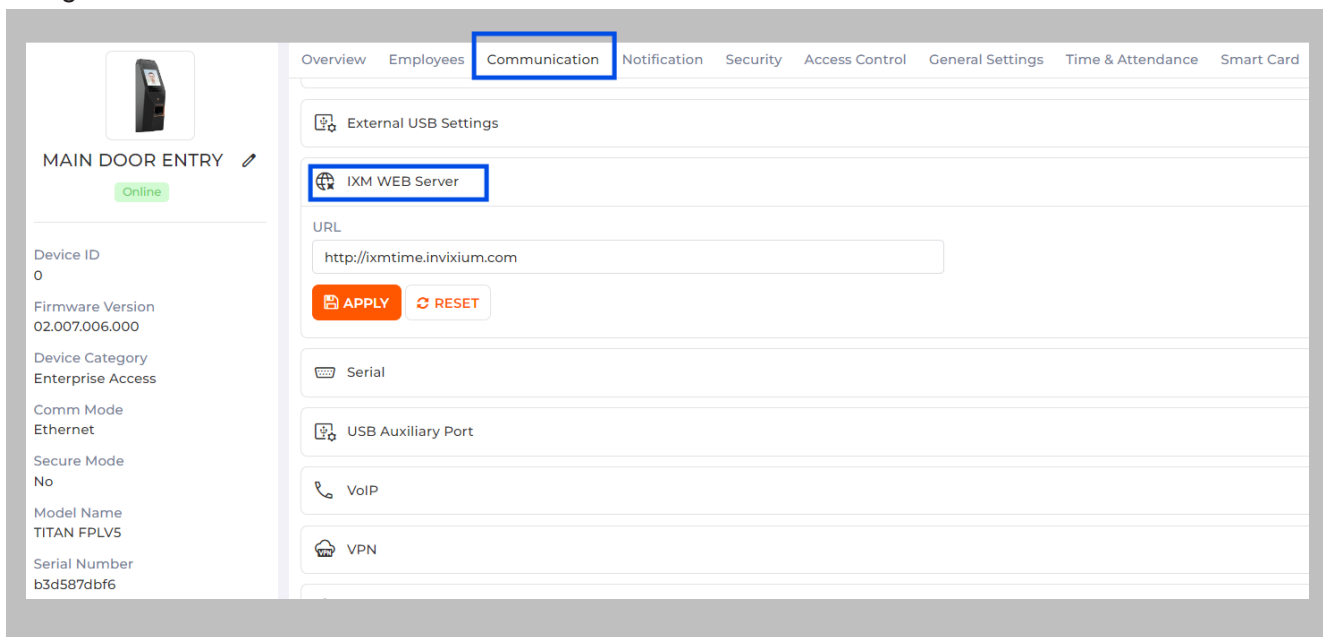


Figure 85: IXM WEB - Server URL Setting

STEP 3

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

Default Format: http://IP_IXMServer:9108

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

In case of IP Address or URL of IXM WEB Server is changed; perform below step to update all registered device(s).

Navigate to **General** → **Application Configuration** and make sure that the **URL** is correct.

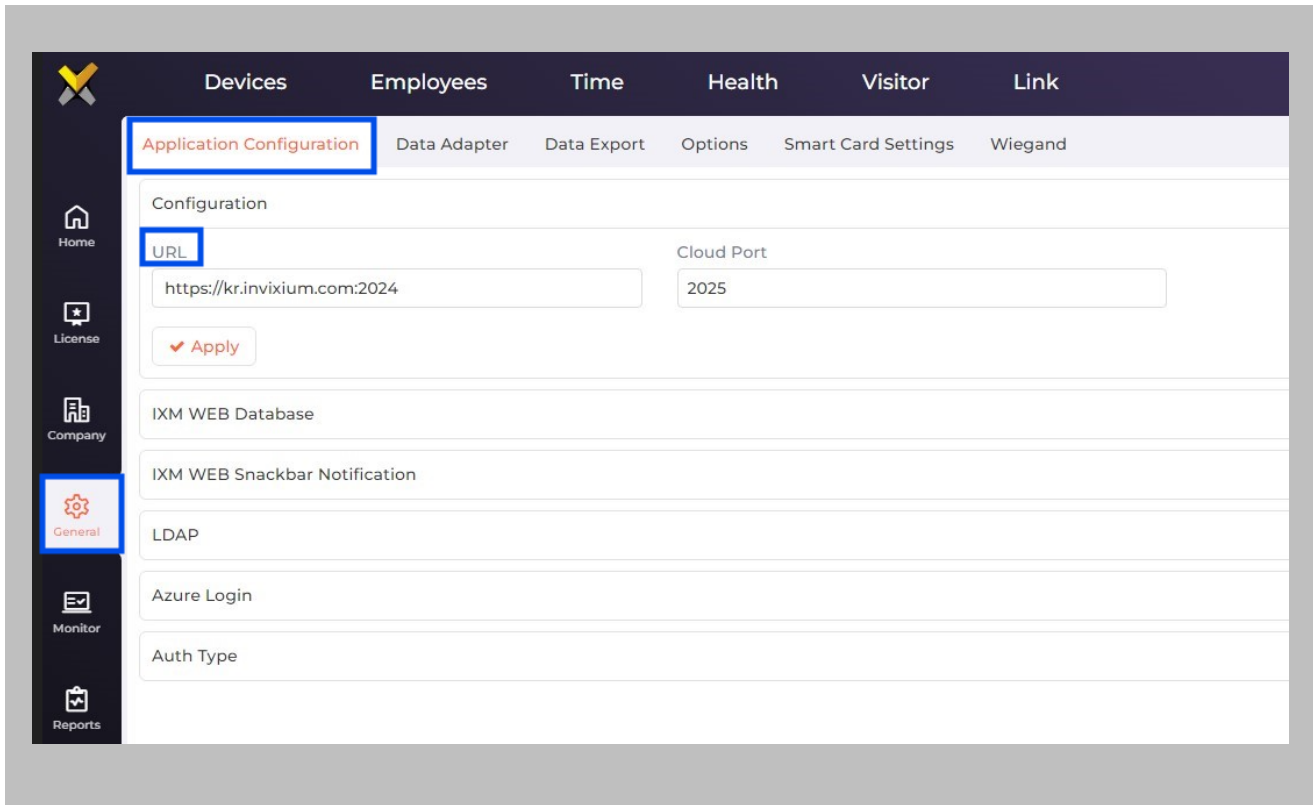


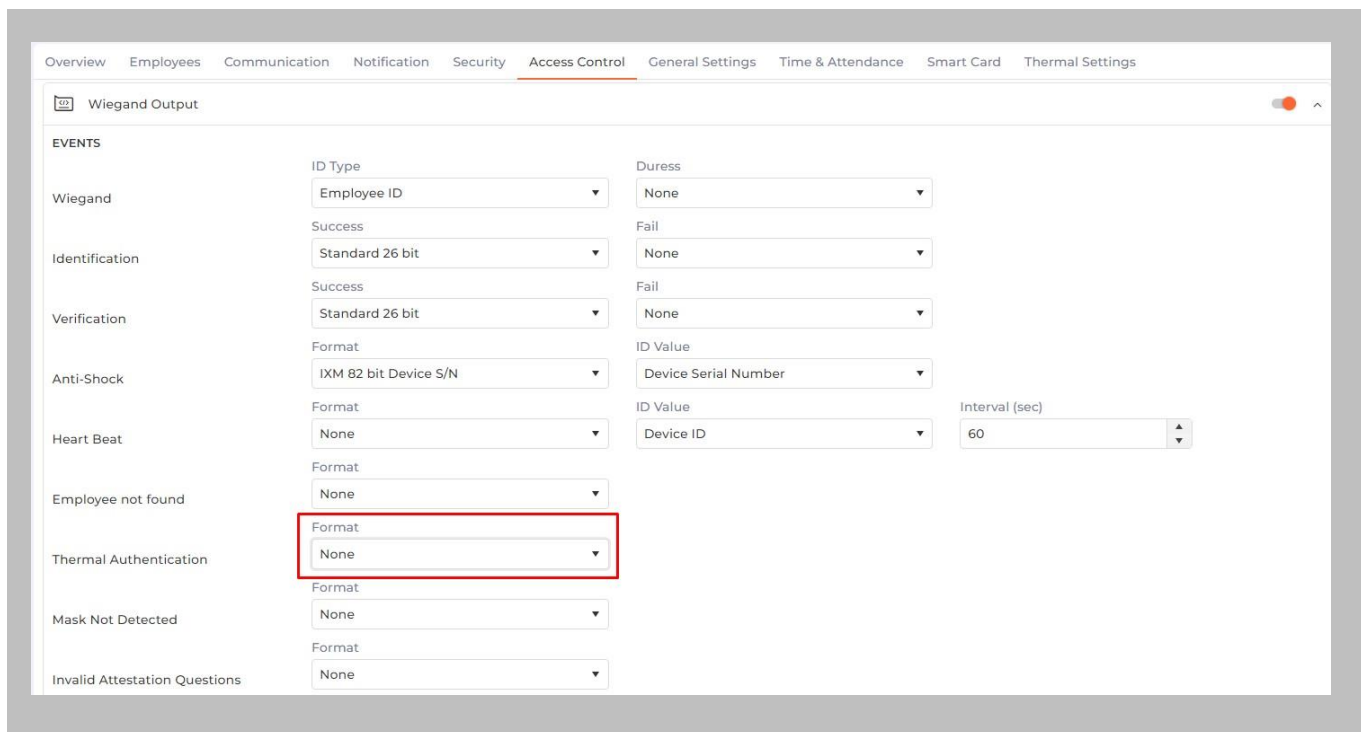
Figure 86: IXM WEB - Server URL Setting from General Settings

Elevated Body Temperature Denied Access but Granted Access in SiPort

Procedure

STEP 1


Ensure that **Thermal Authentication** is selected to none from **IXM WEB** → **Device** → **Access control settings** → **Wiegand Output**.



The screenshot shows the 'Wiegand Output' configuration page in the IXM WEB interface. The page is divided into two main sections: 'EVENTS' on the left and configuration options on the right. The 'Thermal Authentication' event is highlighted with a red box, and its 'Format' is set to 'None'.

Event	ID Type	Success	Format	Duress	Fail	ID Value	Interval (sec)
Wiegand	Employee ID	Standard 26 bit	IXM 82 bit Device S/N	None	None	Device Serial Number	60
Identification	Standard 26 bit	Standard 26 bit	None	None	None	Device ID	60
Verification	Standard 26 bit	Standard 26 bit	None	None	None	Device ID	60
Anti-Shock	IXM 82 bit Device S/N	IXM 82 bit Device S/N	None	None	None	Device ID	60
Heart Beat	None	None	None	None	None	Device ID	60
Employee not found	None	None	None	None	None	Device ID	60
Thermal Authentication	None	None	None	None	None	Device ID	60
Mask Not Detected	None	None	None	None	None	Device ID	60
Invalid Attestation Questions	None	None	None	None	None	Device ID	60

Figure 87: IXM WEB - Thermal Authentication Wiegand Output Event

 Note: If Thermal Authentication events are configured for any format, it generates Wiegand output accordingly for a high-temperature event.

Logs in IXM WEB Application

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

From 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 88: IXM WEB - Enable Device Logs

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

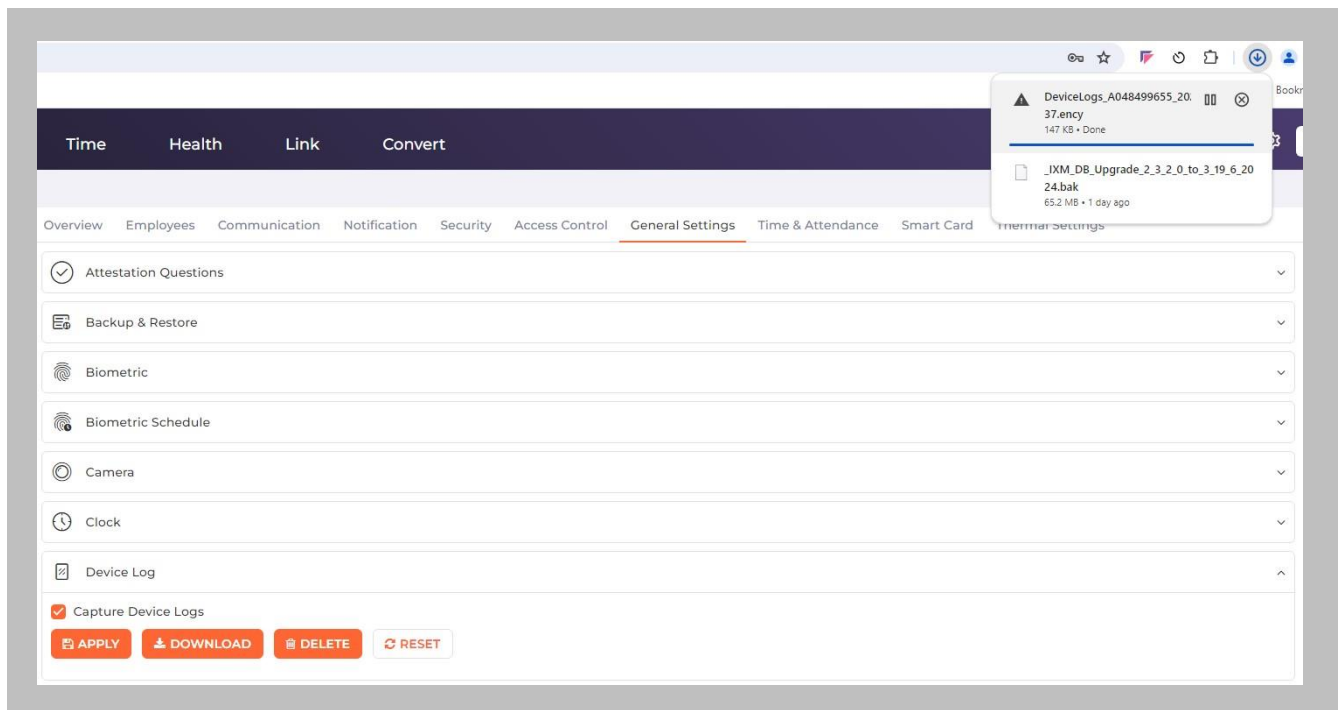


Figure 89: Save Device Log File



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 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.

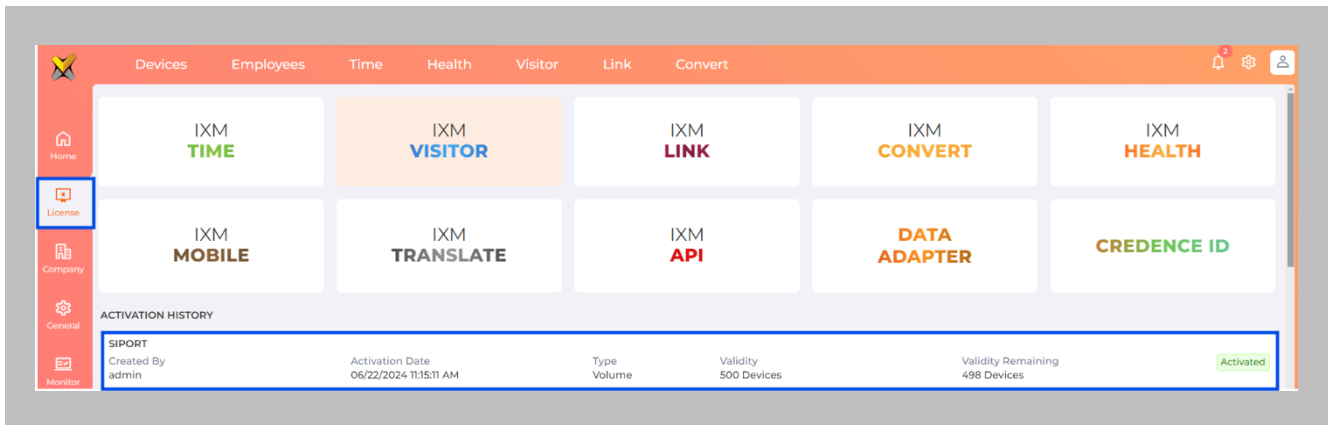



Figure 90: IXM WEB - Licence Module

STEP 2

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

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

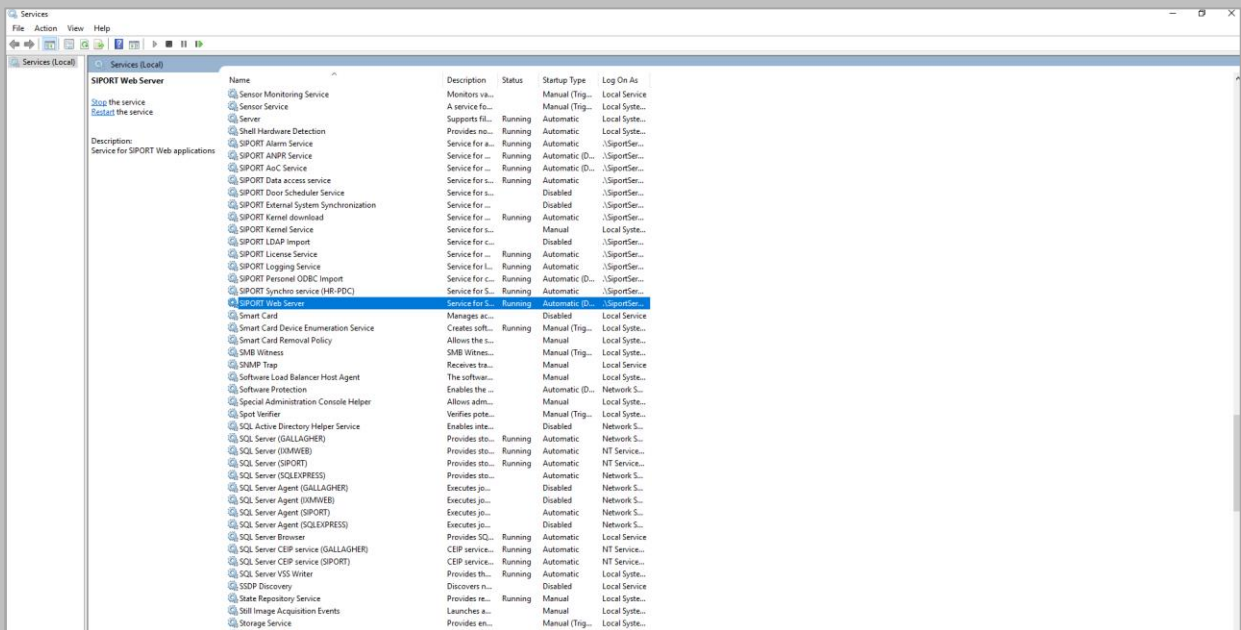



Figure 91: SIEMENS – SiPort Web Service




STEP 3

 Note: Confirm API URL is enabled. 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**.

 Note: If you are still facing problem with connection, please email **logtxt.txt** file to support@invixium.com.

This file is available at the following path:

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



17. Support

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

18. 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 © 2024 Invixium. All rights reserved.