IXM WEB Integration with ACRE Security Access It!

Installation Instructions

V1.0

Table of Contents

1. Introduction 8
Purpose 8
Summary of key features related to this IXM WEB and Access It! Integration 8
Description 8
Acronyms 8
Field Mappings 8

2. Compatibility 10
Invixium Readers 10
Software Requirements 10
Other Requirements 12
Compatibility Matrix for IXM WEB & Access It! Integration 12

3. Checklist 13

4. Task List Summary 13

5. Prerequisites for Installing Invixium IXM WEB Software 14
Acquiring IXM WEB Activation Key 14
Setting Up SQL instance 16
Minor Checklist and Considerations 20

6. Installing IXM WEB 21
Software Install 21

7. Configuring Email Settings using IXM WEB 30
Email Setting Configuration 30

8. Software and Module Activation 34
IXM WEB Activation 34
Access It Module Activation 37

9. Configuring IXM Link for ACRE Security 40

10. Create System User(s) for Biometric Enrollment 44
Creating System User(s) for Biometric Enrollment 44

11. Add and Configure Invixium Readers 48

Adding an Invixium Reader in IXM WEB 48

12. Adding an Invixium Device to a Device Group 53
Configuring Wiegand Format to Assign Invixium Readers 54
Assign Wiegand to Invixium Readers 57
Configuring Panel Feedback with ACRE Security 60
Configuring Thermal Settings 62
Thermal Calibration 65
Test Calibration Options 68
Change Temperature Unit Settings 69
Configuring Mask Authentication Settings 71

13. Fingerprint Enrollment using Access It sofware 74

14. Enrollment Best Practices 81
Fingerprint Enrollment Best Practices 81
Avoid Poor Fingerprint Conditions 81
Fingerprint Image Samples 82
Fingerprint Imaging Do's and Don'ts 83
Finger Vein Enrollment Best Practices 84
Face Enrollment Best Practices 85

15. Appendix 86
Installing Invixium IXM WEB with Default Installation using SQL Server 2014 86
Pushing Configuration to Multiple Invixium Readers 91
Configuring for OSDP Connection 93
Wiring and Termination 98
Wiring 99
Wiegand Connection 101
Wiegand Connection with Panel Feedback 102
OSDP Connections 103

16. Troubleshooting 104
Reader Offline from the IXM WEB Dashboard 104
Elevated Body Temperature Denied Access but Granted Access in Access It 106
Logs in IXM WEB Application 107
Unable to connect to the Access It Server 109

17. Support 111

18. Disclaimer and Restrictions 111

List of Figures

Figure 1: IXM WEB Online Request Form 14
Figure 2: Sample Email After Submitting Online Request Form 15
Figure 3: SQL New Login 17
Figure 4: SQL Login Properties 18
Figure 5: SQL Server Roles 19
Figure 6: IXM WEB Installer 21
Figure 7: Advanced Options in IXM WEB Installer 22
Figure 8: Invixium Fingerprint Driver Installation Message 23
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 29
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 - Forgot Password 33
Figure 20: IXM WEB - Enter Login Credentials 34
Figure 21: IXM WEB - License Setup 35
Figure 22: IXM WEB - Online Activation 36
Figure 23: IXM WEB – Request Link License 37
Figure 24: ACRE Security License Key Email 38
Figure 25: IXM WEB - Activate ACRE Security Link License 39
Figure 26: IXM WEB - Enable ACRE Security Link Module 40
Figure 27: IXM WEB - Sync Activities 42
Figure 28: IXM WEB - Create System User 44
Figure 29: IXM WEB - Add New System User 45
Figure 30: IXM WEB - New System User 46
Figure 31: Employee and Employee Group Rights 47

Figure 32: IXM WEB - Save System User 47
Figure 33: IXM WEB - Devices Tab 48
Figure 34: IXM WEB - Search Device Using IP Address 49
Figure 35: IXM WEB - Register Device 50
Figure 36: IXM WEB - Device Registration Complete 51
Figure 37: IXM WEB - Dashboard, Device Status 52
Figure 38: IXM WEB - Assign Device Group 53
Figure 39: IXM WEB - Create Wiegand Format 54
Figure 40: IXM WEB - Create Custom Wiegand Format 55
Figure 41: IXM WEB - Custom Wiegand Format 55
Figure 42: IXM WEB – Custom Wiegand Format Created 56
Figure 43: IXM WEB - Upload Wiegand Format 56
Figure 44: IXM WEB - Navigate to Access Control Tab 57
Figure 45: IXM WEB - Wiegand Output 58
Figure 46: IXM WEB - Save Output Wiegand 59
Figure 47: IXM WEB - Panel Feedback 60
Figure 48: IXM WEB - Configuring Panel Feedback in IXM WEB 61
Figure 49: IXM WEB - Save Panel Feedback 61
Figure 50: IXM WEB - Thermal Settings 62
Figure 51: IXM WEB - Save Thermal Settings 64
Figure 52: IXM WEB - Thermal Calibration Settings 65
Figure 53: IXM WEB - Save Thermal Calibration Settings 66
Figure 54: IXM WEB - Capture Thermal Data 66
Figure 55: IXM WEB - Save Captured Thermal Data 67
Figure 56: IXM WEB - Test Thermal Calibration 68
Figure 57: IXM WEB - Option to Change Temperature Unit 69
Figure 58: IXM WEB - Save Temperature Unit Setting 70
Figure 59: IXM WEB - Mask Authentication Settings 71
Figure 60: IXM WEB - Save Mask Settings 73
Figure 61: ACRE Security - System 74
Figure 62: ACRE Security – Workstations 75
Figure 63: ACRE Security – Edit Workstation 76
Figure 64: Edit Workstation – Encode / Enroll 76
Figure 65: Encode/Enroll – Add New 77
Figure 66: Add new Device 78
Figure 67: Newly created device 79
Figure 68: IXM WEB – Biometric Enrollment 80

Figure 69: Fingerprint Enrollment Best Practices 81
Figure 70: Fingerprint Images Samples 82
Figure 71: Finger Vein Enrollment Best Practices 84
Figure 72: Face Enrollment Best Practices 85
Figure 73: Install IXM WEB 86
Figure 74: Loading SQL Express & Installation Progress 87
Figure 75: IXM WEB - Shortcut Icon on Desktop 88
Figure 76: IXM WEB - Configuring IXM WEB Database 88
Figure 77: IXM WEB - Select Database Name 89
Figure 78: IXM WEB - Broadcast Option 91
Figure 79: IXM WEB - Broadcast Wiegand Output Settings 91
Figure 80: IXM WEB - Broadcast to Devices 92
Figure 81: IXM WEB - OSDP Settings 93
Figure 82: IXM WEB - Save OSDP Settings 96
Figure 83: IXM WEB - Edit Device Options 96
Figure 84: IXM WEB - Disable Panel Feedback 97
Figure 85: Earth Ground Wiring 98
Figure 86: IXM TITAN – Top & Bottom Connector Wiring 99
Figure 87: Power, Wiegand & OSDP Wires 100
Figure 88: IXM TITAN - Wiegand 101
Figure 89: IXM TITAN - Panel Feedback 102
Figure 90: IXM TITAN - OSDP Connections 103
Figure 91: IXM WEB - Server URL Setting 104
Figure 92: IXM WEB - Server URL Setting from General Settings 105
Figure 93: IXM WEB - Thermal Authentication Wiegand Output Event 106
Figure 94: IXM WEB - Enable Device Logs 107
Figure 95: Save Device Log File 107
Figure 96: IXM WEB - Licence Module 109
Figure 97: ACRE Security – Access It Web API 109

List of Tables

Table 1: Compatibility Matrix for IXM WEB & ACRE Security Integration 12
Table 2: Task List Summary 13
Table 3: System Related Checklist 20
Table 4: Port Information 20
Table 5: IXM WEB - OSDP Configuration Options 95
Table 6: IXM WEB - OSDP Text Options 95
Table 7: Logs Folder Location 108

1. Introduction

Purpose

This document outlines the process of configuring the software integration between ACRE Security Access It! and Invixium's IXM WEB.

Summary of key features related to this IXM WEB and Access It! Integration

- 'Sync All' feature to resynchronize the database from Access It! to IXM WEB
- Multiple card support upto 10

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 ACRE Security Access It 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 Access It by using ACRE Security Access It API to import and export cardholders.

Acronyms

Acronym	Description
ACPCS	Access Control Panel Configuration Software
AI	ACRE Security Access It!
IXM	Invixium

Field Mappings

The following are the Access It fields that are mapped to IXM WEB:

Access It Field	IXM Field	Notes
First name	First Name	
Last name	Last Name	

Cardholder Status	Suspend User	IXM WEB has two values of Cardholder Status - ACTIVE and INACTIVE while AI has three statuses - Inactive, Active, and Date based. ACTIVE of AI is mapped to INACTIVE. INACTIVE of AI is mapped to ACTIVE as Suspend User in IXM WEB. The Date field is mapped to the Start Date & End Date of IXM WEB.
Cardholder Status Date is Active (Cardholder Status - Date based)	Start Date	AI doesn't allow a value less than 1/1/1970.
Cardholder Status Date is expired (Cardholder Status - Date based)	End Date	AI doesn't allow a value greater than 31/12/2035.
Department	Department	
Card number	Prox ID	
Facility Code	Facility Code	
PIN Number	PIN	ACRE Security has a PIN at the card level which is mapped to a PIN at the user level since IXM WEB supports only one card per user. The rationale is that the user remembers their PIN which can be used on Invixium devices for authentication. In ACRE Security, the default value for PIN Number is 0. If the PIN Number is 0 then it is considered empty in IXM WEB.
Card status	"No equivalent"	Prox ID, Facility Code, and PIN are set when the Card Status is not Inactive. Inactive card statuses are not transferred to IXM WEB.
Active (Card Status - Date based) &	"No equivalent"	If an active date is less than or equal to the current date, and the expiry date is greater than or equal to the current date then Prox ID, Facility Code, and PIN are transferred to IXM WEB.

Expire (Card Status - Date based)		
Photo	User Image	Upon syncing, IXM WEB fetches all the user's profile pictures from AI. Users need to ensure that photos have a valid size (it should not be 0 bytes).

Note: Multiple Cards – Access It can have multiple cards per user but IXM WEB imports cards up to 10 only.

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
ACRE Security Access It!	v10.2.0
Invixium IXM WEB	3.0.36.0
Operating Systems	Windows Server 2016 Standard Windows Server 2019 Windows 11 Pro Windows 10 Professional Version
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 & Access It! Integration

IXM WEB version	Access It version	Compatible
IXM WEB 2.2.57.0	v4.5	Yes
IXM WEB 2.2.57.0	v5.0	Yes
IXM WEB 2.2.224.0	v4.5	Yes
IXM WEB 2.2.224.0	v5.0	Yes
IXM WEB 2.2.252.0	v5.0	Yes
IXM WEB 2.2.252.0	v5.5	Yes
IXM WEB 2.2.330.0	v5.0	Yes
IXM WEB 2.2.330.0	v5.5	Yes
IXM WEB 2.3.0.0	v10.2	Yes
IXM WEB 2.3.0.0	v10.2	Yes
IXM WEB 3.0.36.0	v10.2	Yes
IXM WEB 3.0.36.0	v10.2	Yes

Table 1: Compatibility Matrix for IXM WEB & ACRE Security Integration

3. Checklist

Item List	Interface
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 ACRE Security Access It	Invixium
Configure Invixium Reader	Invixium
Face or Finger Enrollment	Invixium

4. Task List Summary

Task	IXM WEB Application Task List using IXM WEB	ACRE Security Access It Task List using Access It
1	Activate IXM WEB and IXM Link for Access It	Fingerprint Enrollment from ACRE Security
2	Configure IXM Link for Access It	
3	Register IXM Devices and configure settings as per the requirement	
4	Configure Weigand or OSDP in the device for integration with ACRE Security	
5	Assign a specific Device Group to the device	

Table 2: Task List Summary

5. 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/.

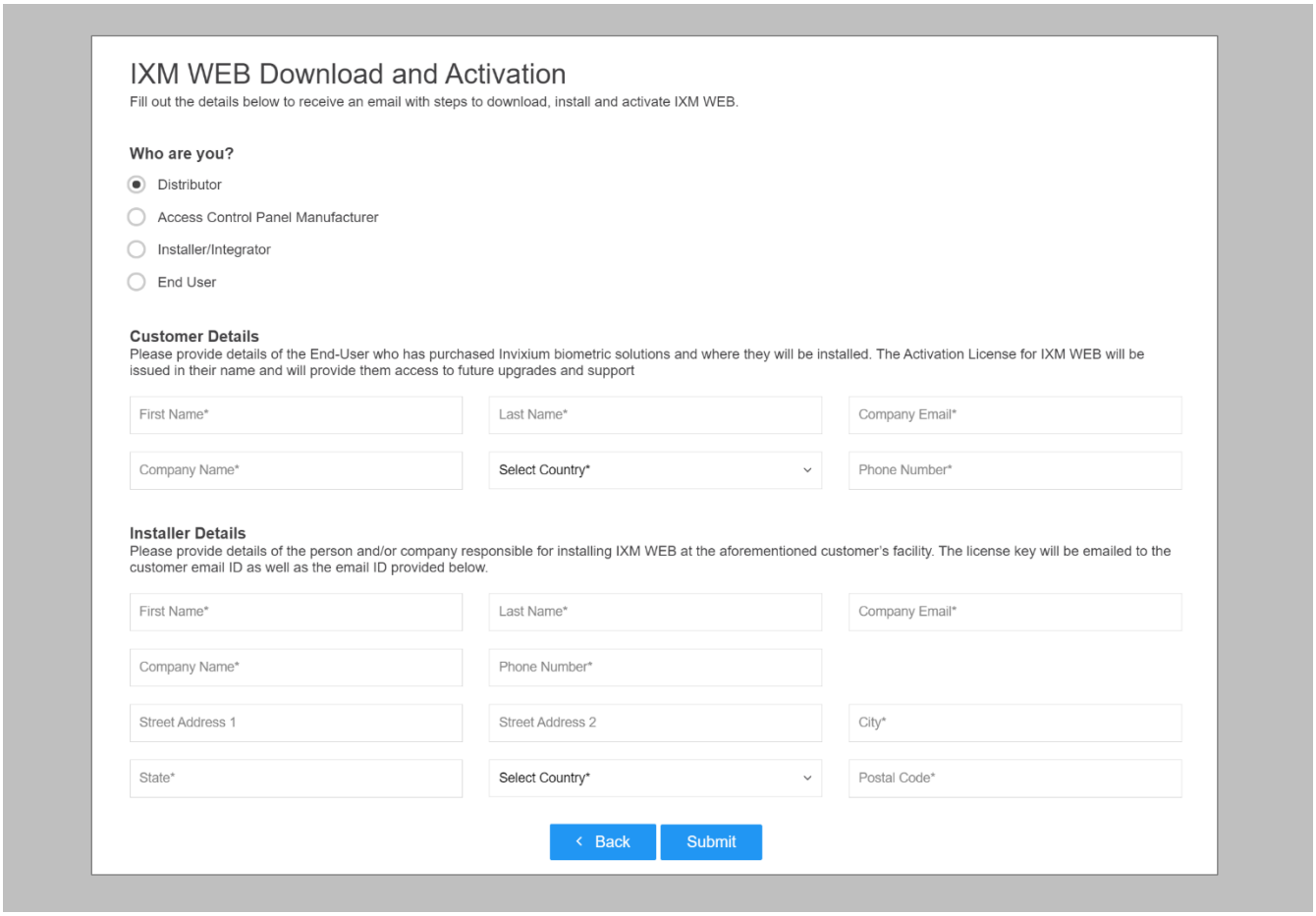
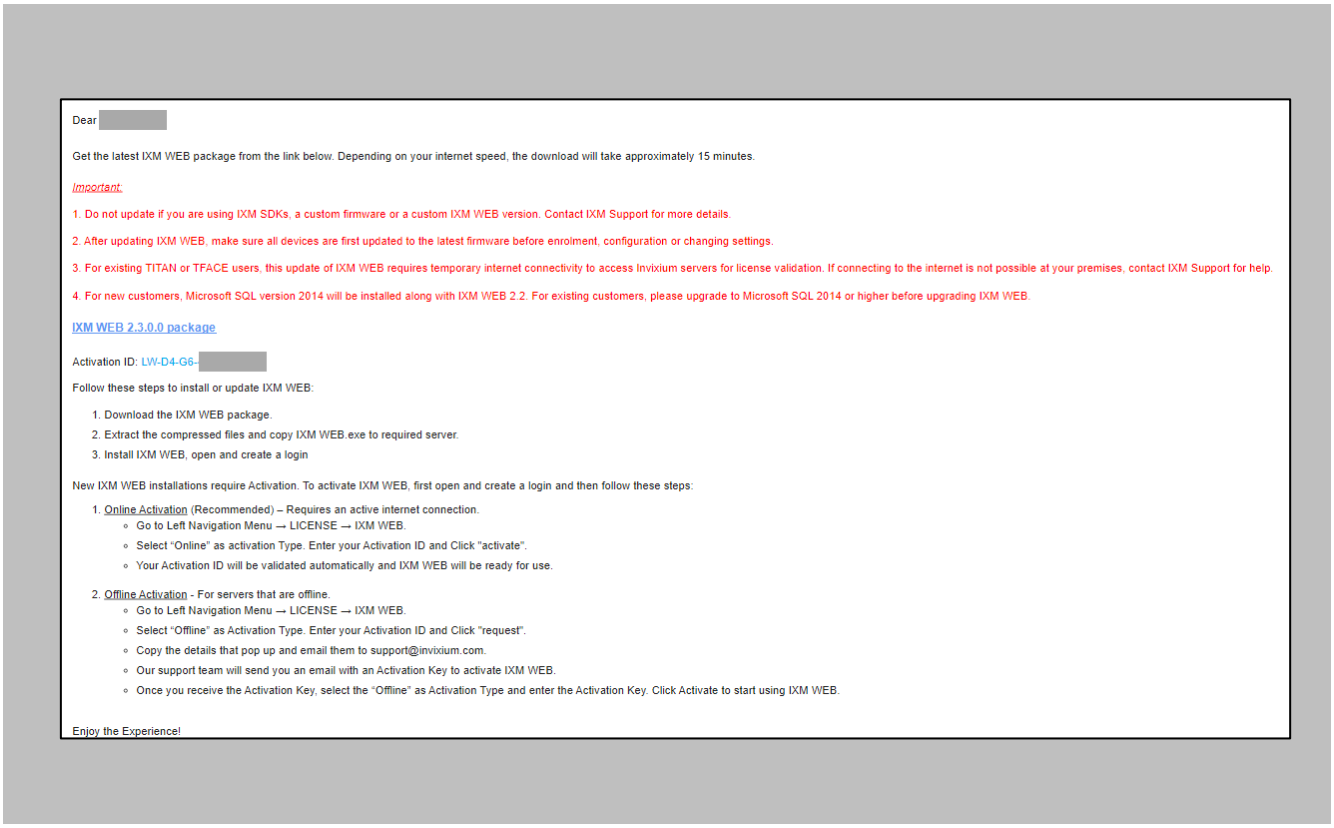


Figure 1: IXM WEB Online Request Form

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.



Dear [redacted]

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

Important:

1. Do not update if you are using IXM SDKs, a custom firmware or a custom IXM WEB version. Contact IXM Support for more details.
2. After updating IXM WEB, make sure all devices are first updated to the latest firmware before enrolment, configuration or changing settings.
3. For existing TITAN or TFACE users, this update of IXM WEB requires temporary internet connectivity to access Invixium servers for license validation. If connecting to the internet is not possible at your premises, contact IXM Support for help.
4. For new customers, Microsoft SQL version 2014 will be installed along with IXM WEB 2.2. For existing customers, please upgrade to Microsoft SQL 2014 or higher before upgrading IXM WEB.

IXM WEB 2.3.0.0 package

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

Follow these steps to install or update IXM WEB:

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

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

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

Enjoy the Experience!

Figure 2: Sample Email After Submitting Online Request Form

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.

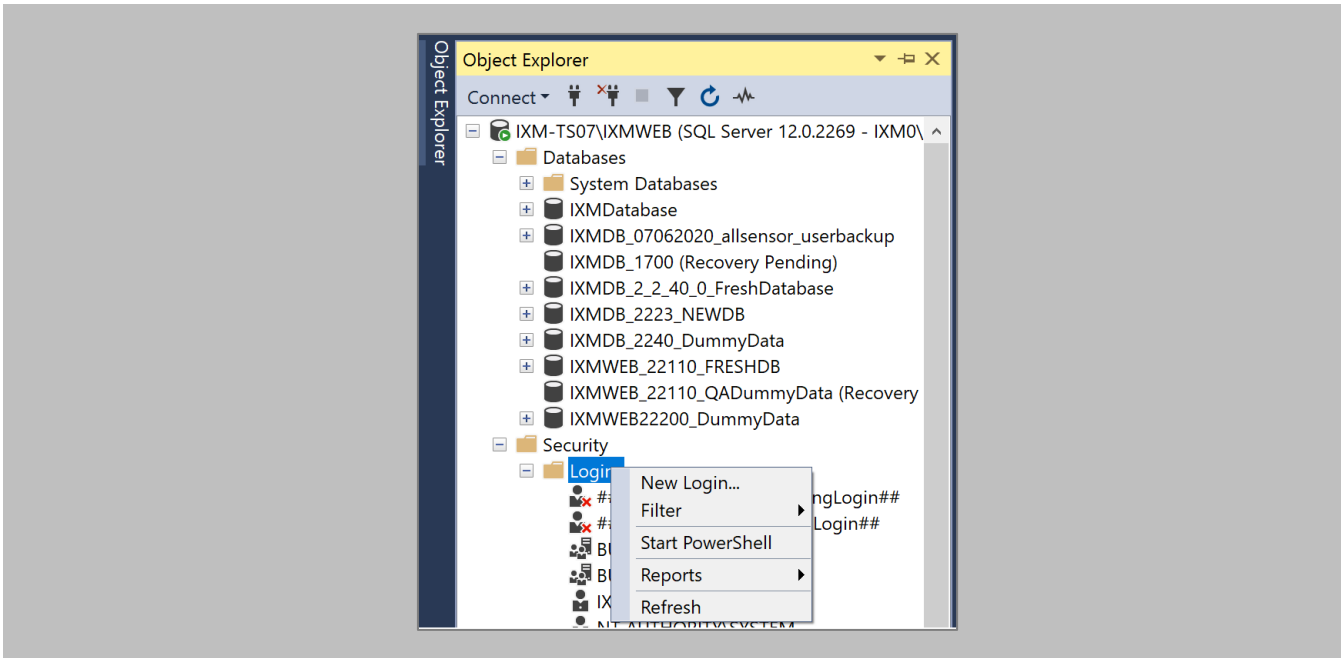


Figure 3: SQL New Login

STEP 6

Select **SQL Server authentication.**

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

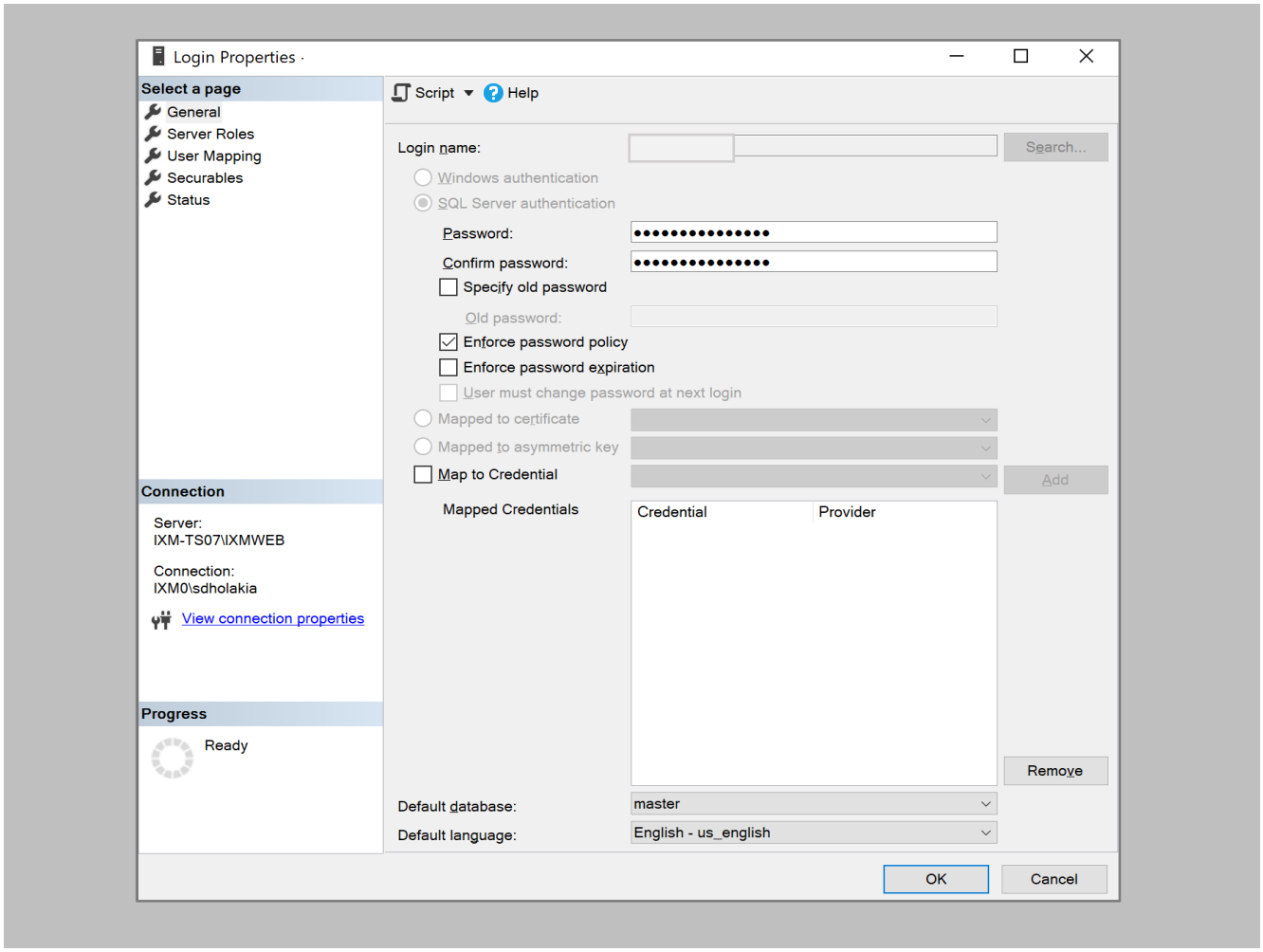


Figure 4: SQL Login Properties

STEP 7

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

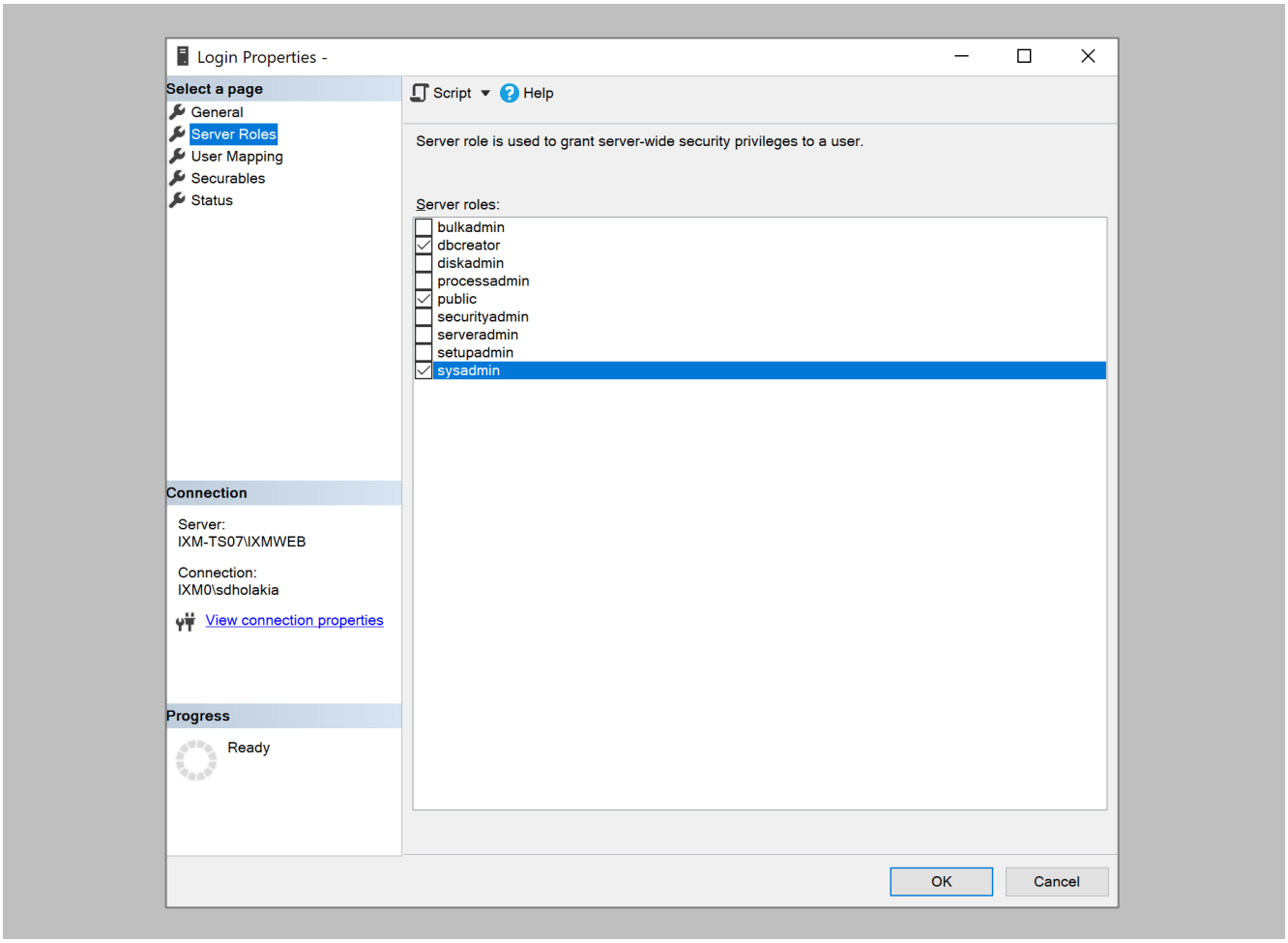


Figure 5: SQL Server Roles

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

Table 3: System Related Checklist

Port Assignment	**Port**
Inbound HTTP Port	9108
TCP	1433
Port to communicate between IXM WEB & Devices	9734
Inbound Port	1255
Access It Web Service API Port	8732 (default)

Table 4: Port Information

6. 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.**

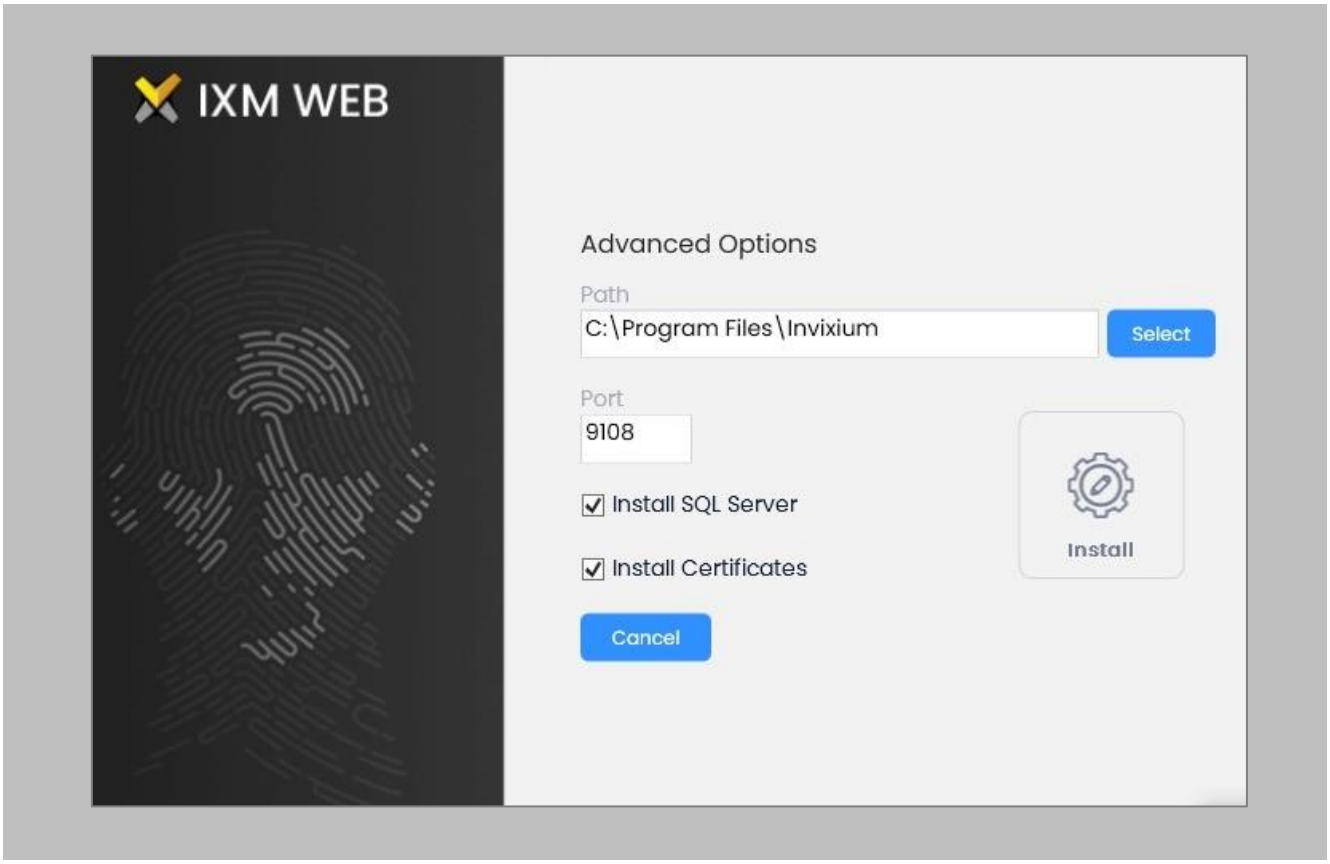


Figure 7: Advanced Options in IXM WEB Installer

STEP 3

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

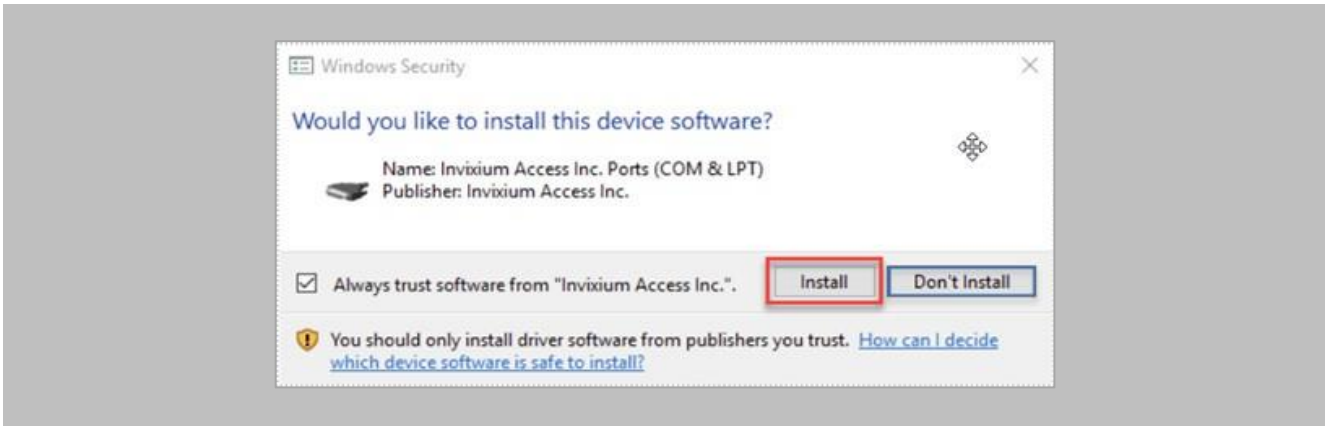


Figure 8: Invixium Fingerprint Driver Installation Message

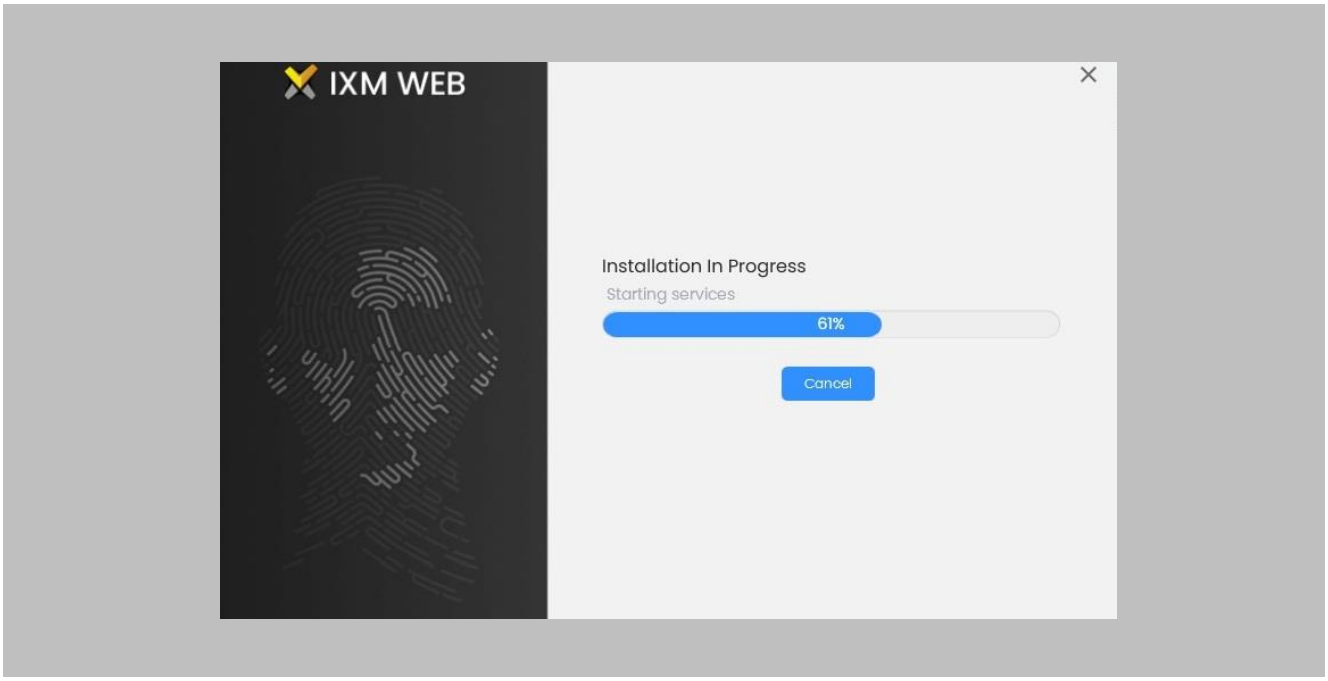


Figure 9: IXM WEB Installation Progress

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).

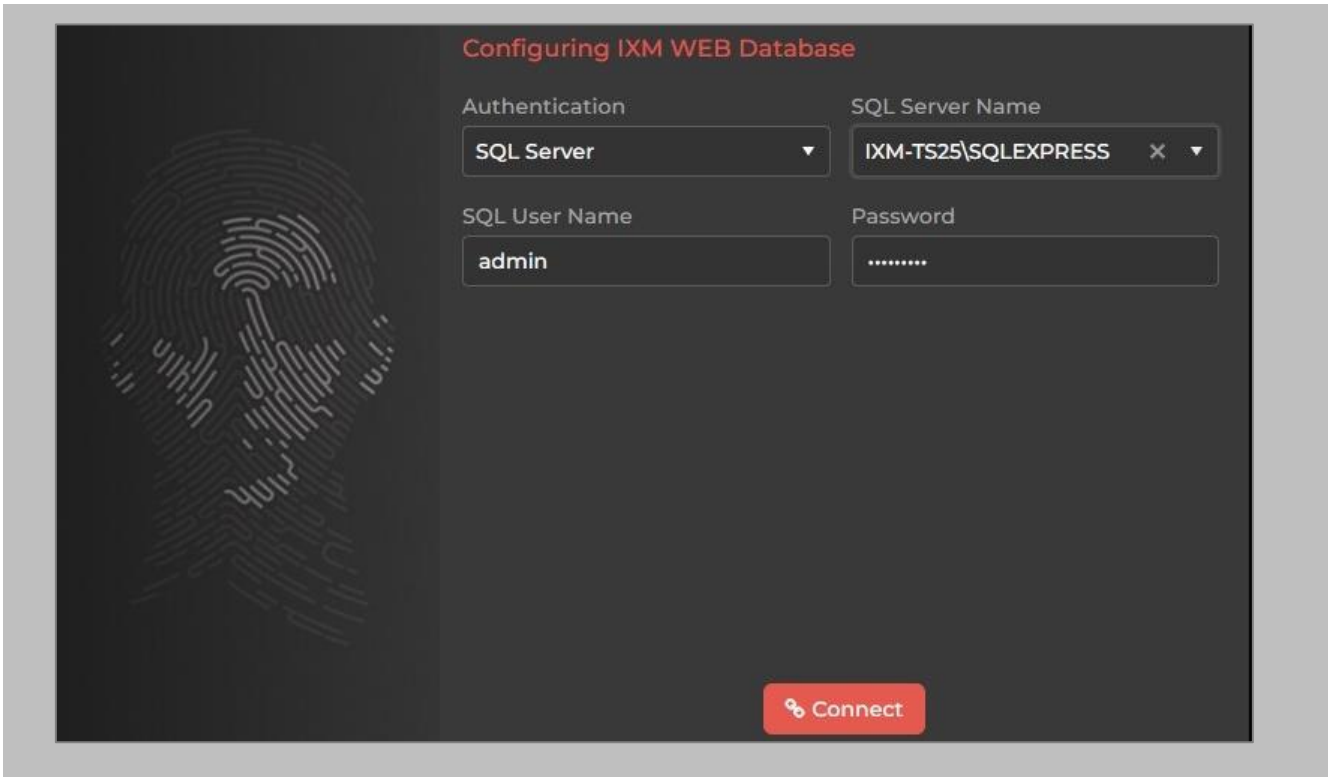


Figure 12: IXM WEB Database Configuration

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.

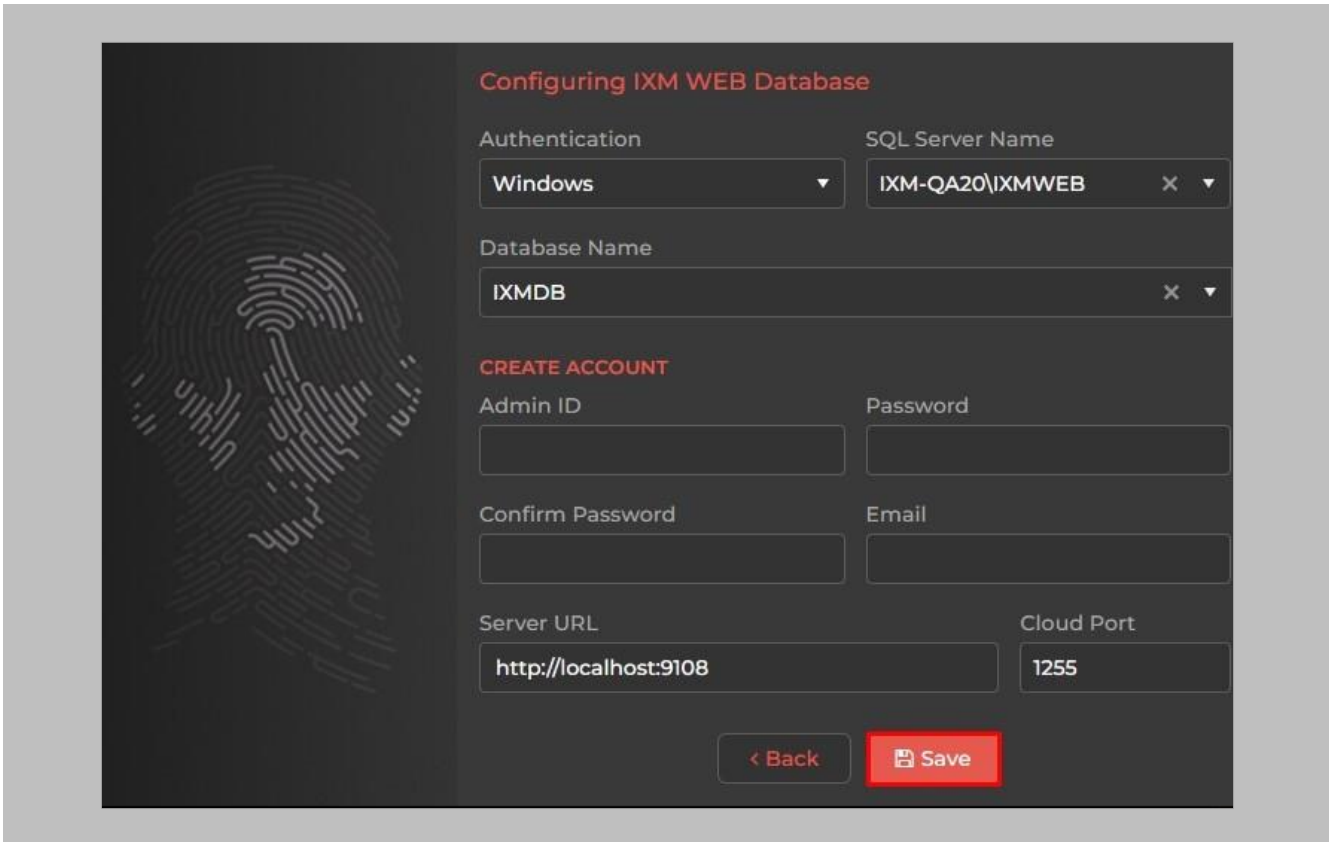


Figure 13: IXM WEB Administrator User Configuration

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:

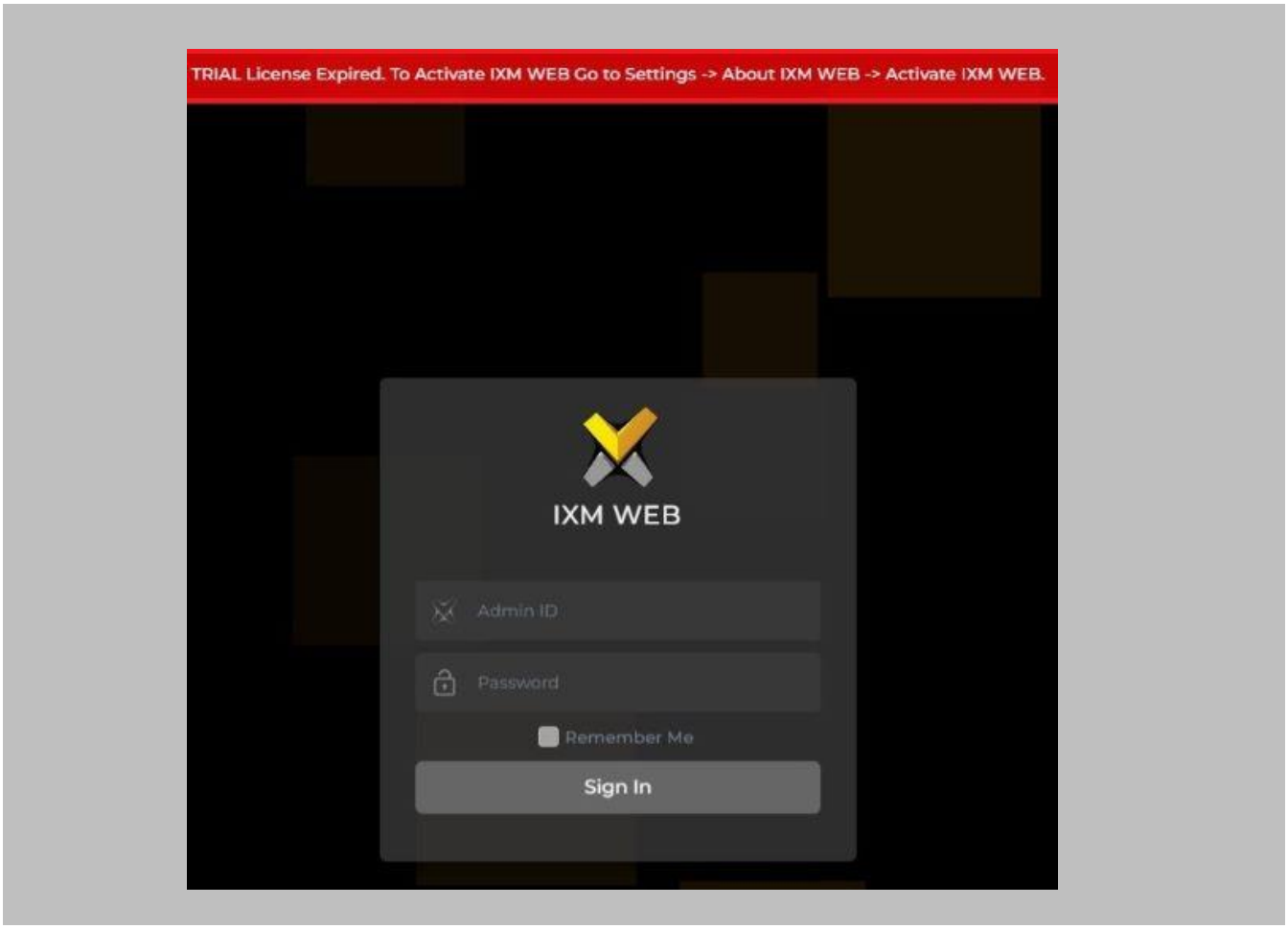


Figure 14: IXM WEB Login Page

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.

7. Configuring Email Settings using IXM WEB

Configuring Email settings is highly recommended as one of the first steps after installing IXM WEB. Email configuration settings will help the admin retrievie 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.**

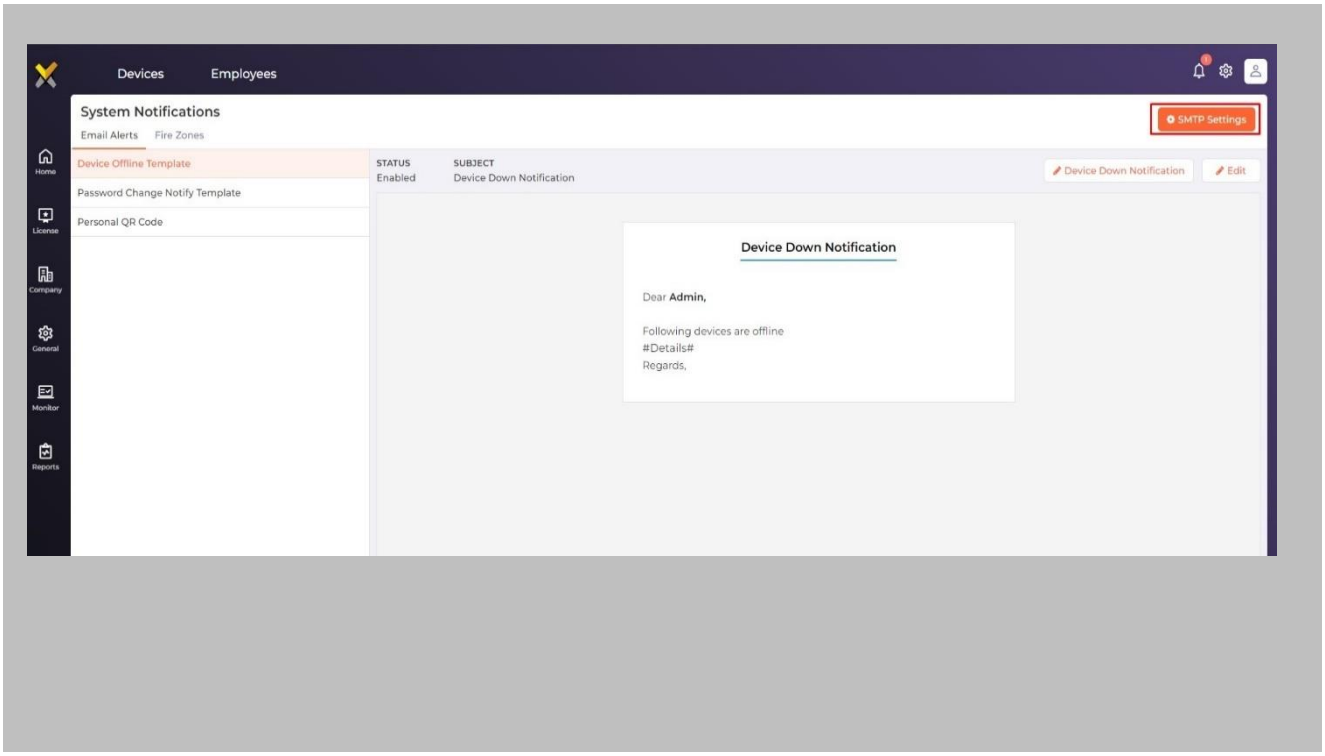


Figure 15: Configure Email

STEP 2

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

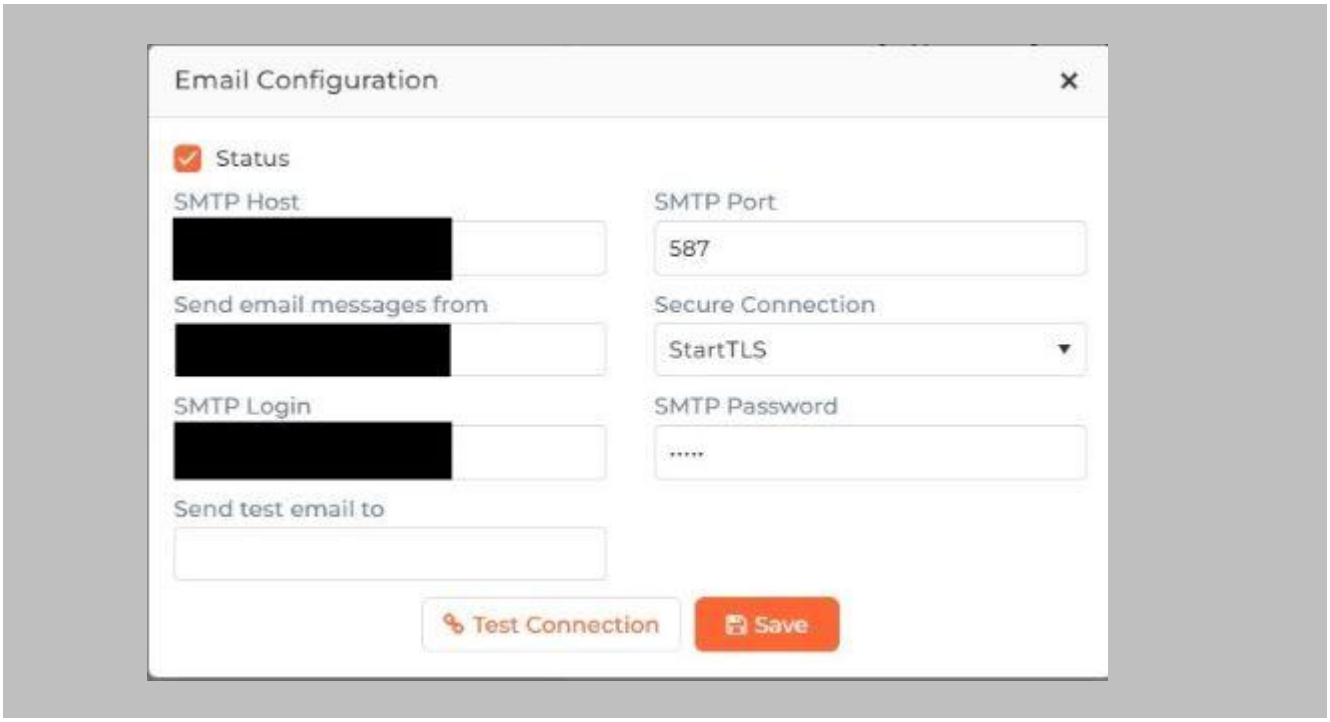


Figure 16: IXM WEB - SMTP Settings

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.

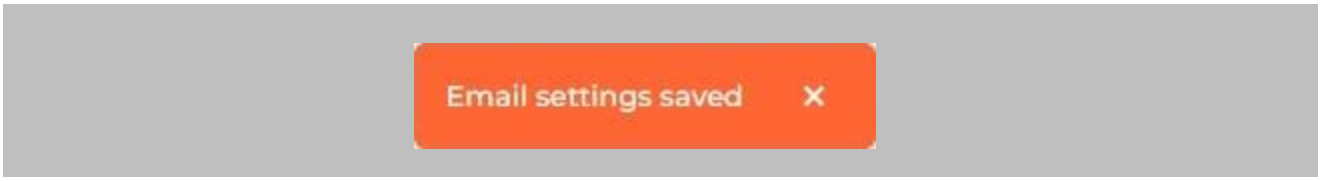


Figure 17: IXM WEB - Save Email Settings

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.

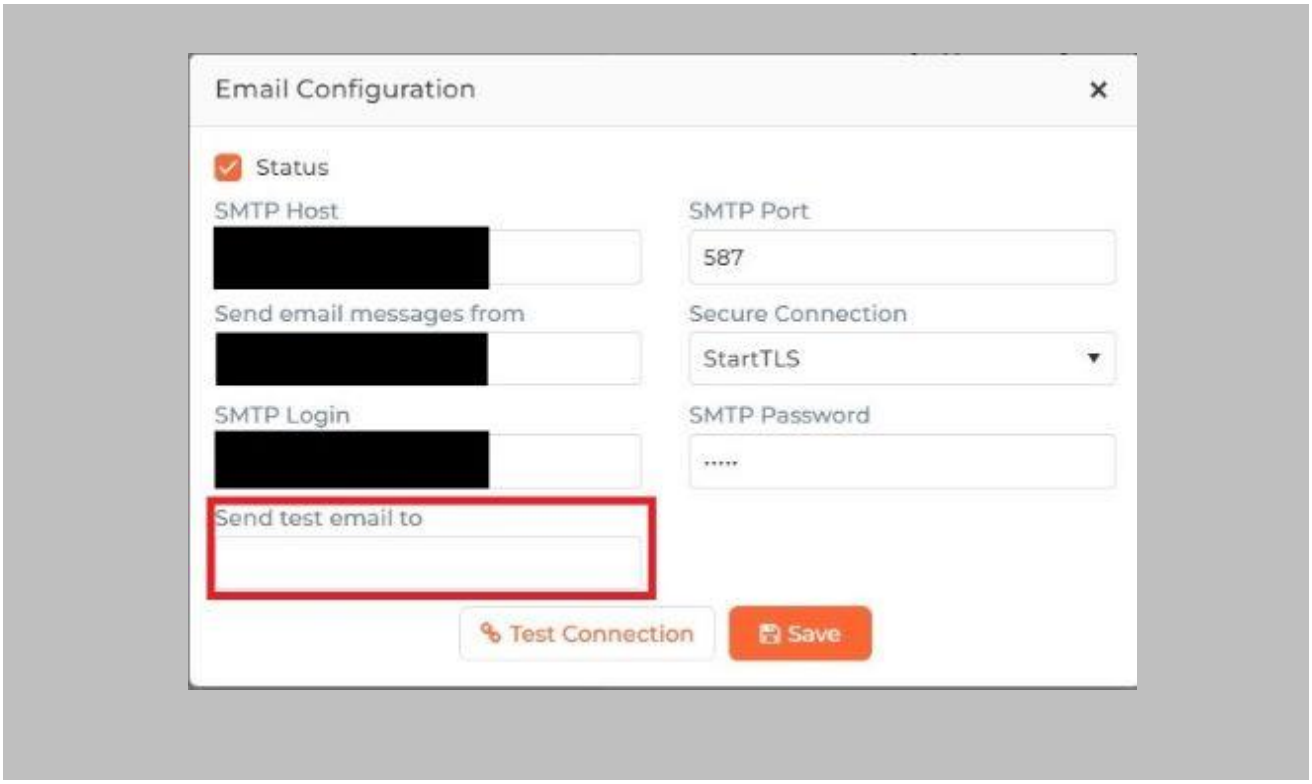


Figure 18: IXM WEB – Test Connection

STEP 4

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

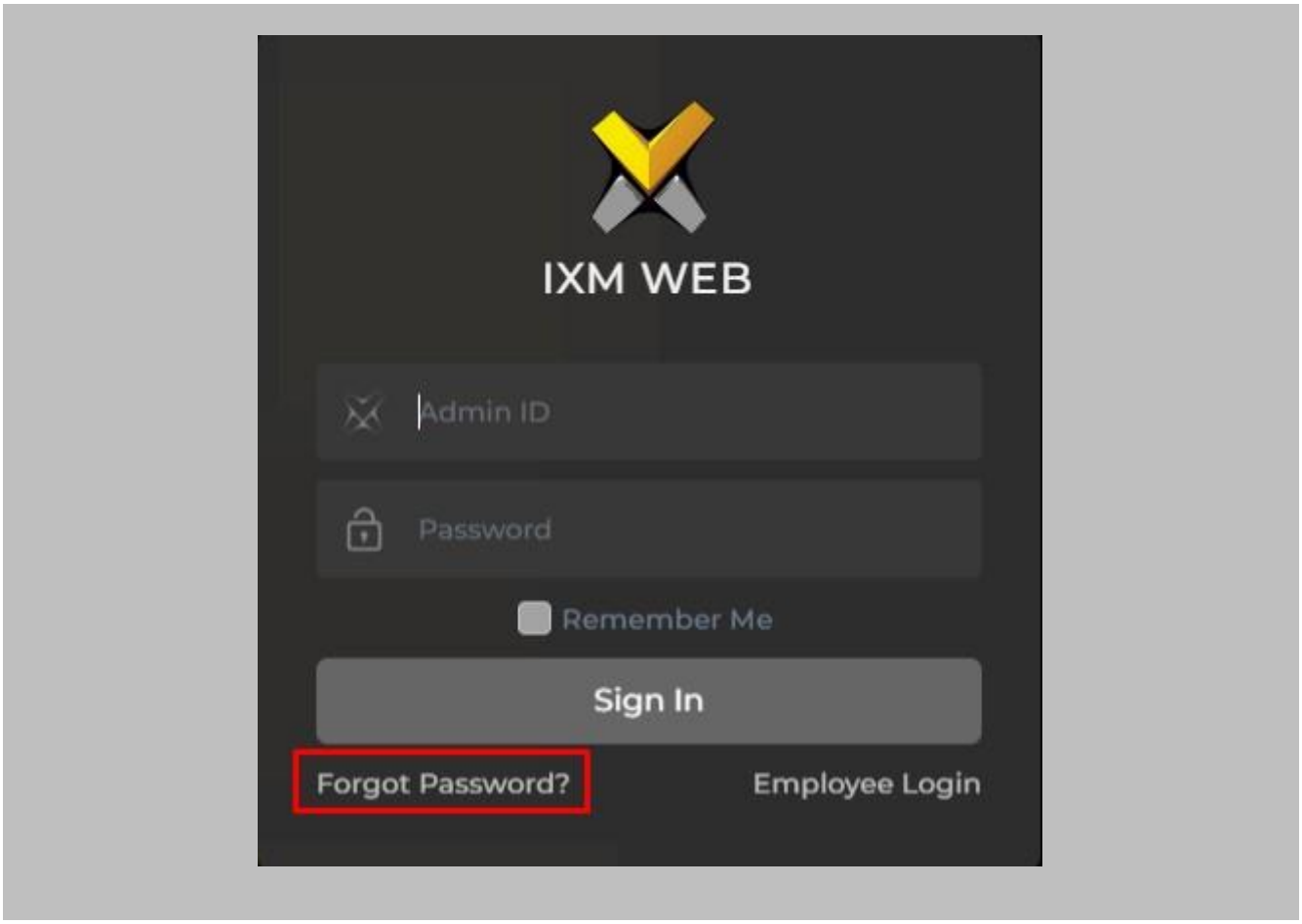


Figure 19: IXM WEB - Forgot Password

8. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

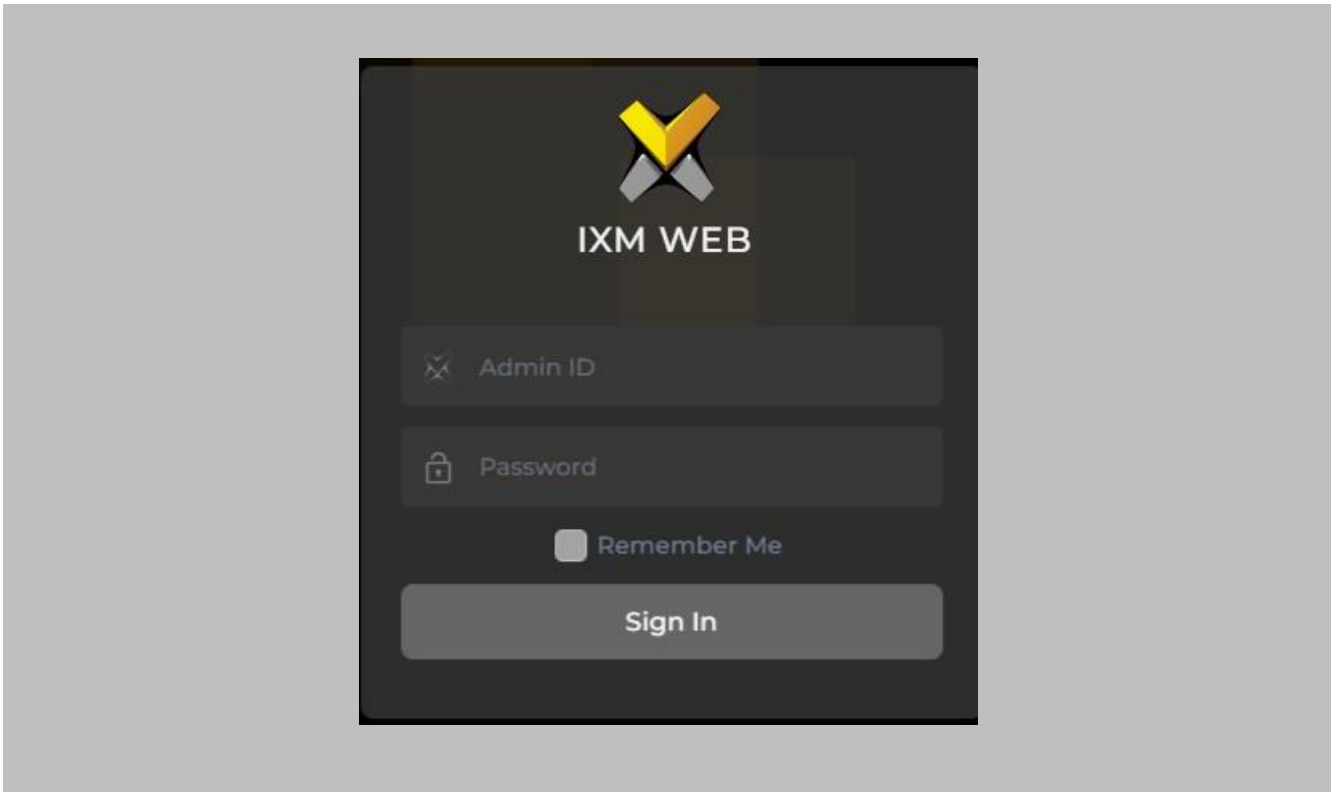


Figure 20: IXM WEB - Enter Login Credentials

STEP 2

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

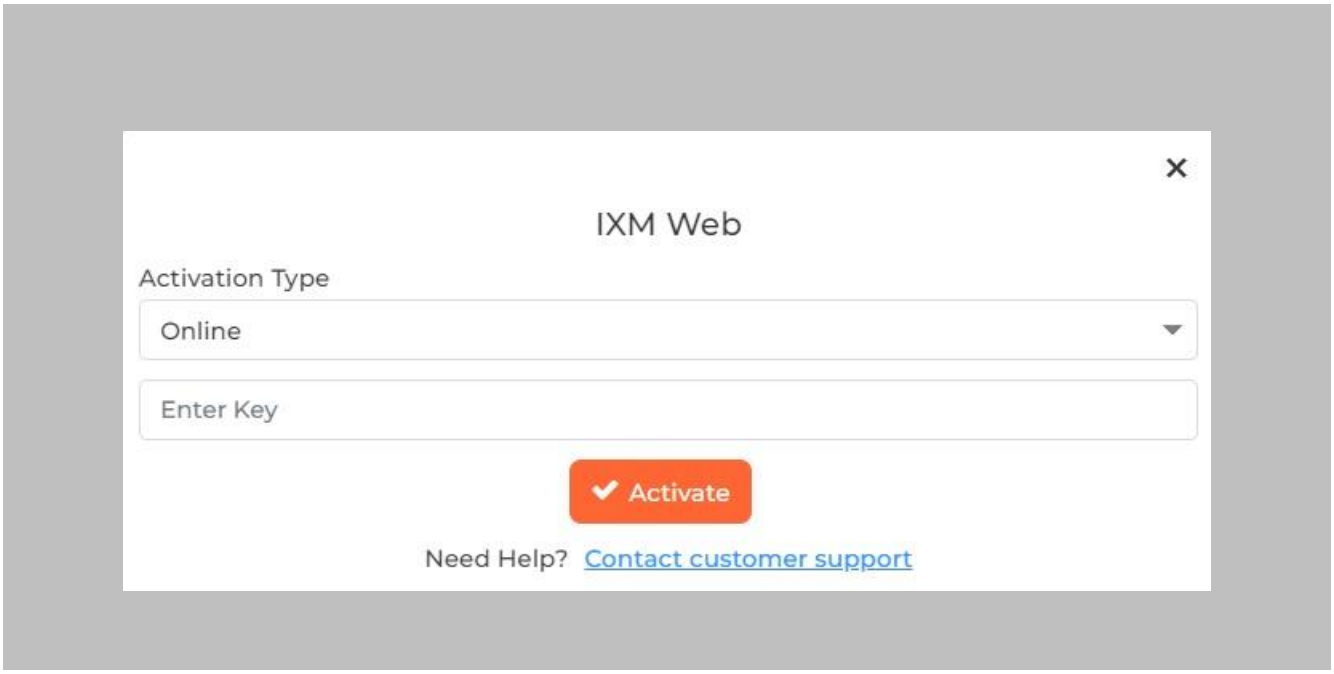


Figure 21: IXM WEB - License Setup

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**.

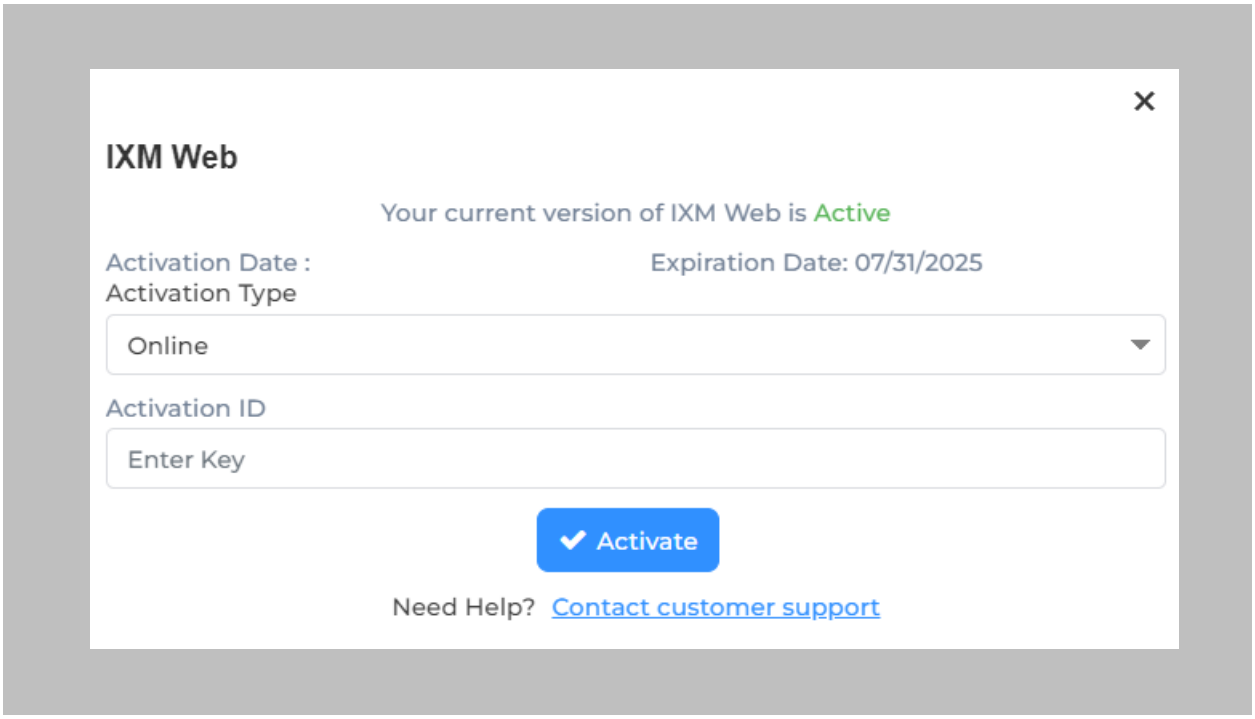


Figure 22: IXM WEB - Online Activation

Access It Module Activation

The option to activate a ACRE Security Access It 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.

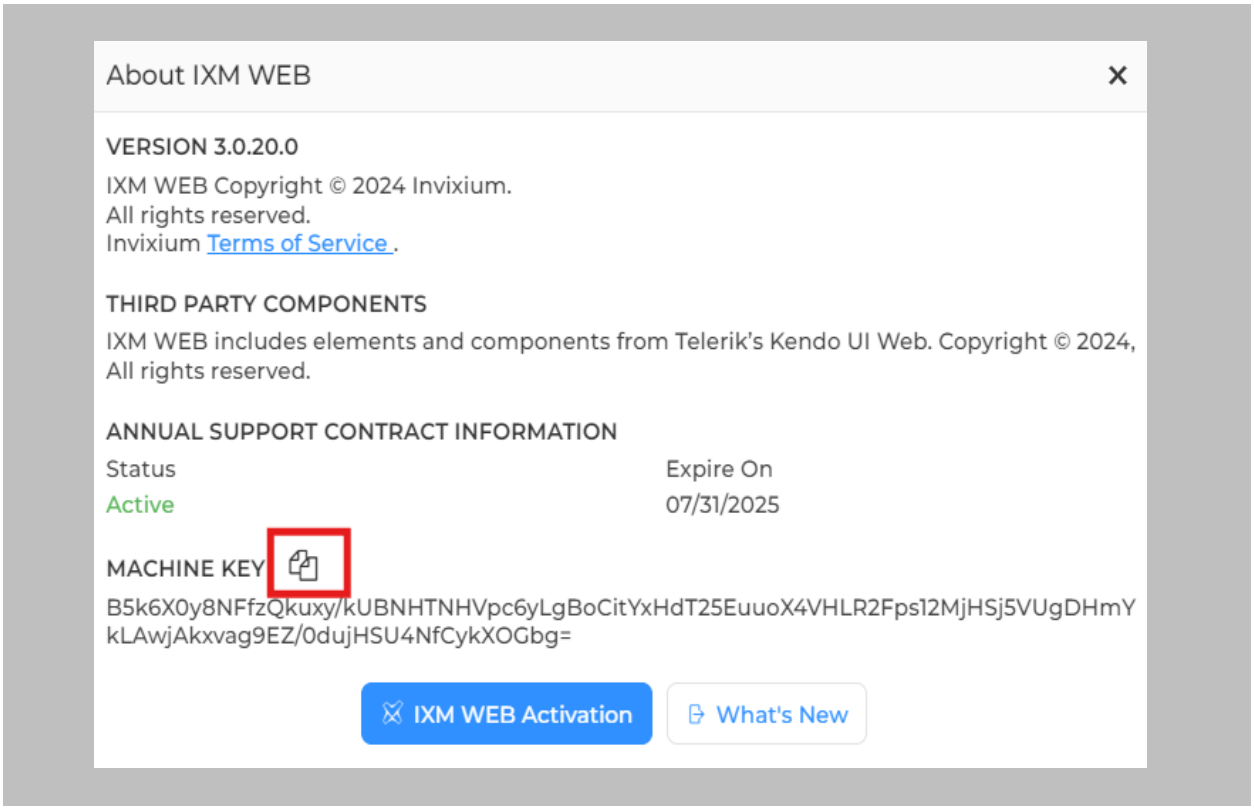


Figure 23: IXM WEB – Request Link License

STEP 2

You will receive an email from Invixium Support containing a license key for the ACRE Security Access It Activation.

From: Invixium Support
Sent: Thursday, September 30, 2021 11:59 AM
To: [redacted]
Subject: RE: IXM LINK Activation key request

Dear [redacted],

Greetings! Thanks for connecting with Invixium Technical Services Team!

Your license details are given below:

- Module: **Access It**
- License Key: [redacted]

To activate your IXM Link license, follow these steps:

1. Open IXM WEB and login
2. Go to Left Navigation Menu >> Click LICENSE tab
3. Select the Lenel option
4. Enter the License Key given above and click **Activate**.

We appreciate your kind support & patience.

Best Regards,

Invixium Technical Services Team

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

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

Figure 24: ACRE Security 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**.

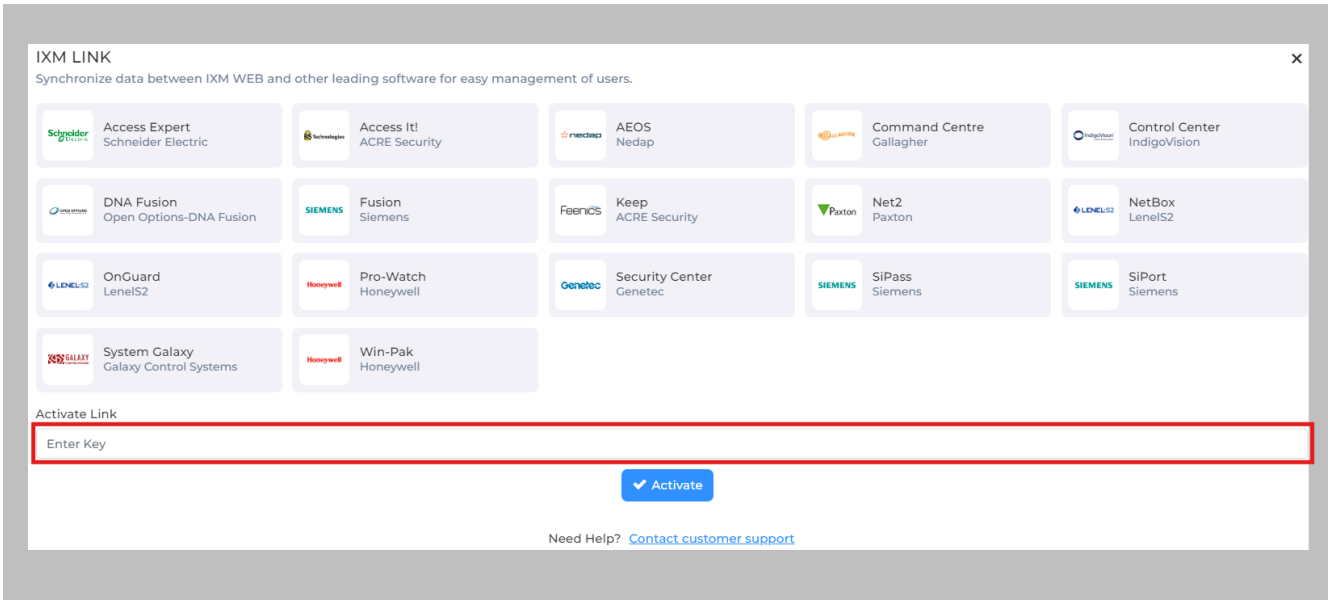


Figure 25: IXM WEB - Activate ACRE Security Link License

RESULT

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

9. Configuring IXM Link for ACRE Security

Procedure

STEP 1

From the **Link** → click the **Access It (ACRE Security)** icon.

Toggle the **Status** switch to enable.

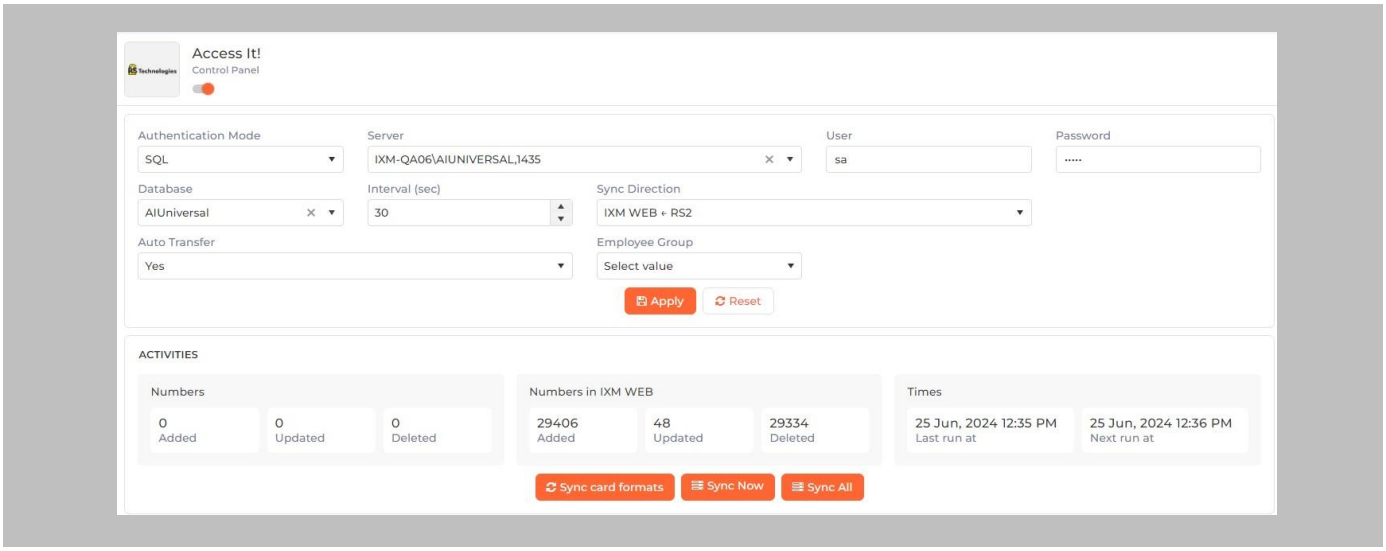


Figure 26: IXM WEB - Enable ACRE Security Link Module

Authentication Mode:
Select “Windows” or “SQL Server” as an authentication mode from the dropdown list.

Server:
Enter the Name or IP of SQL Server Instance where ACRE Security database is installed.

User:
Enter the name of the authorized user to log into SQL Server to access database.

Password:
Enter the Password of the authorized user to log into SQL Server to access database.

Database:
Select the AIUniversal database from the dropdown list.

Interval (Sec):
Enter the duration of interval for data transfer between ACRE Security and IXM WEB. The system will automatically try to establish connection after every specified interval of time and sync users.

Sync Direction:
Click on the field to select the direction of data transfer. Data can be transferred in following three ways :

- IXM WEB ← ACRE Security

  Choosing this option will transfer data in one direction only, ie, from ACRE Security to IXM WEB. ACRE Security is considered as the master data in this case and any changes made in IXM WEB data will be overwritten during transfer.

  Note:
  This is the recommended option.

- IXM WEB → ACRE Security

  Choosing this option will transfer data in one direction only, ie, from IXM WEB to ACRE Security. IXM WEB is considered as the master data in this case and any changes made in ACRE Security data will be overwritten during transfer.

- IXM WEB ↔ ACRE Security

  Choosing this option will transfer data in both the directions, ie, from ACRE Security to IXM WEB first followed by IXM WEB to ACRE Security.

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 ACRE Security 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 ACRE Security and IXM WEB is possible only after successful connection.

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

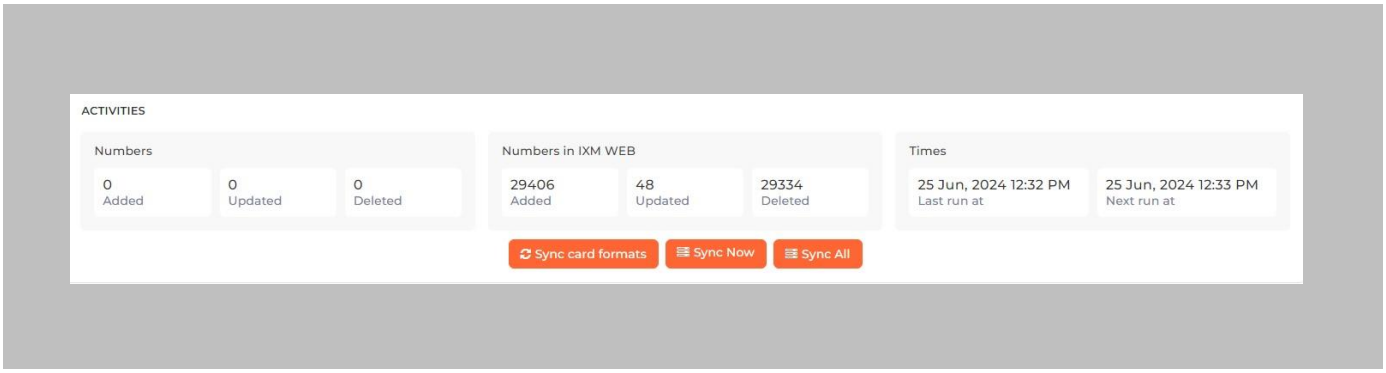


Figure 27: IXM WEB - Sync Activities

Numbers

The first two colums display the number of records added, updated and deleted in ACRE Security 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 resynchronization of database from Access It to IXM WEB. This will re-import missing cardholders or updated cardholders from Access It to IXM WEB. Also, it will delete IXM WEB employee records according to cardholders available in Access It .

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

STEP 4

Clicking on **Sync card formats** immediately synchronizes card formats from Access It to IXM WEB. This will re-import card formats available in Access It to IXM WEB.

RESULT

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

10. 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.

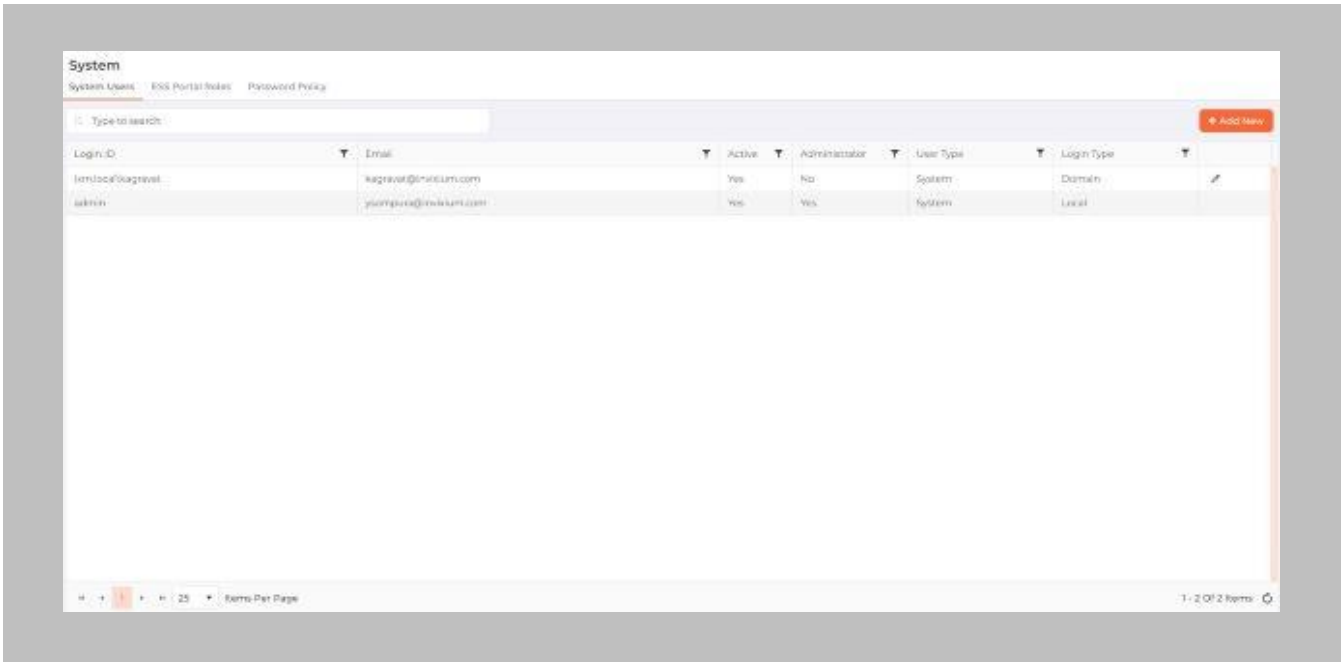


Figure 28: IXM WEB - Create System User

STEP 2

Click **Add New**.

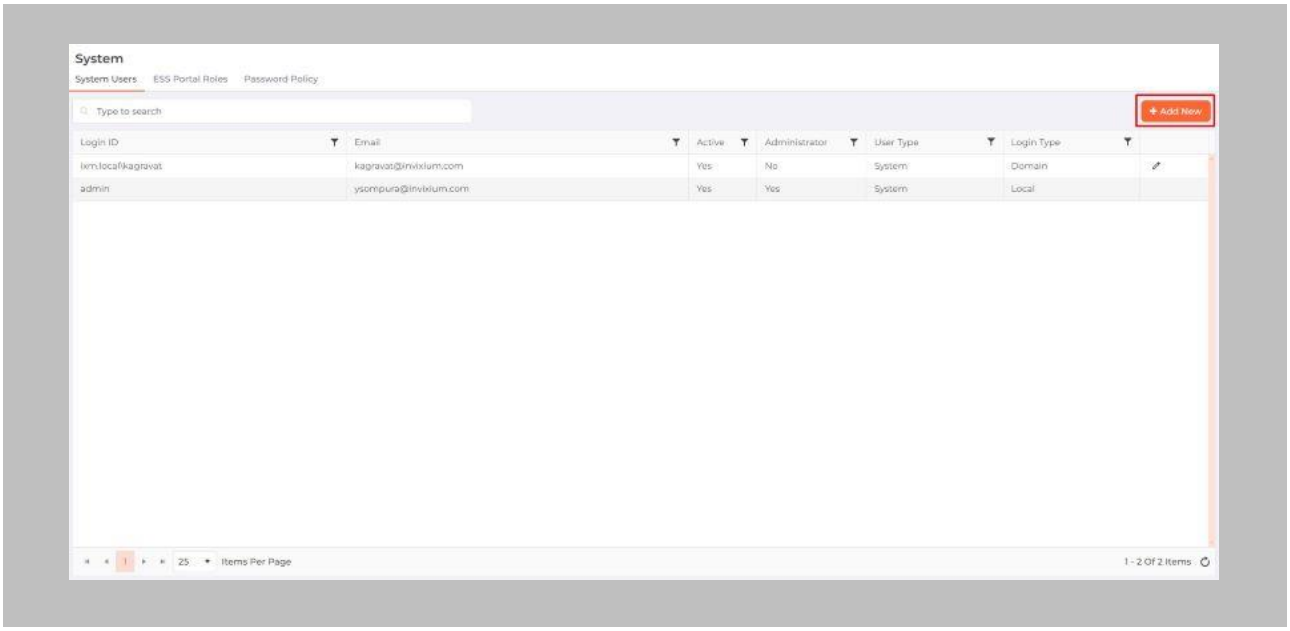


Figure 29: IXM WEB - Add New System User

Creating a system user requires the following details:

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

STEP 3

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

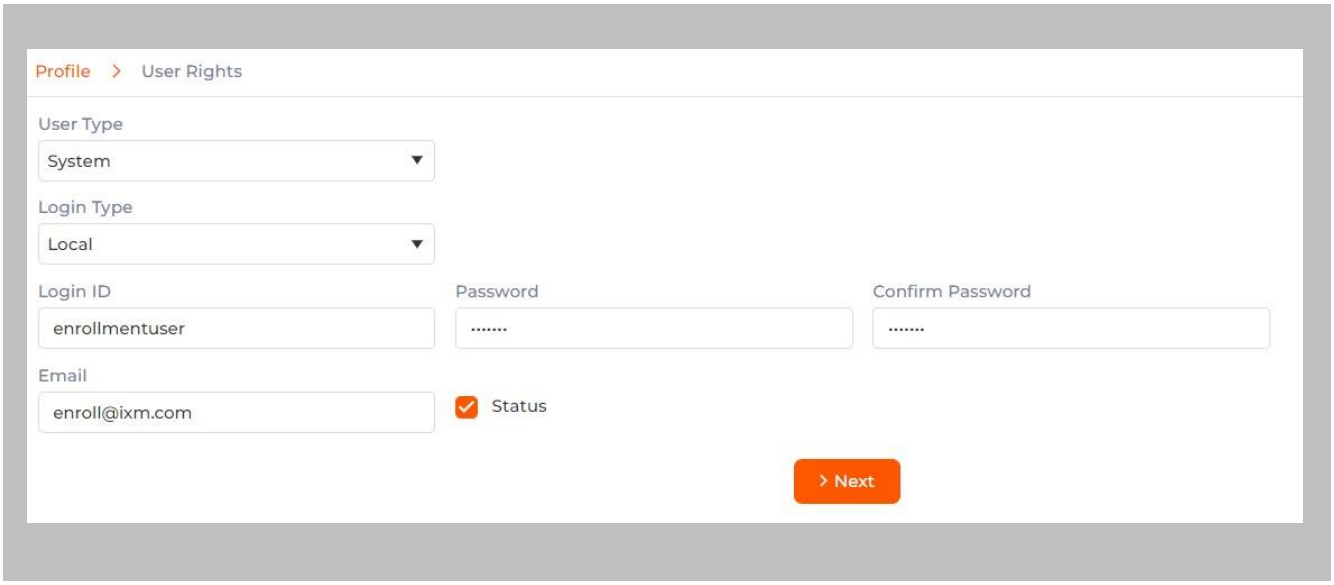


Figure 30: IXM WEB - New System User

STEP 4

Add an email address.

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

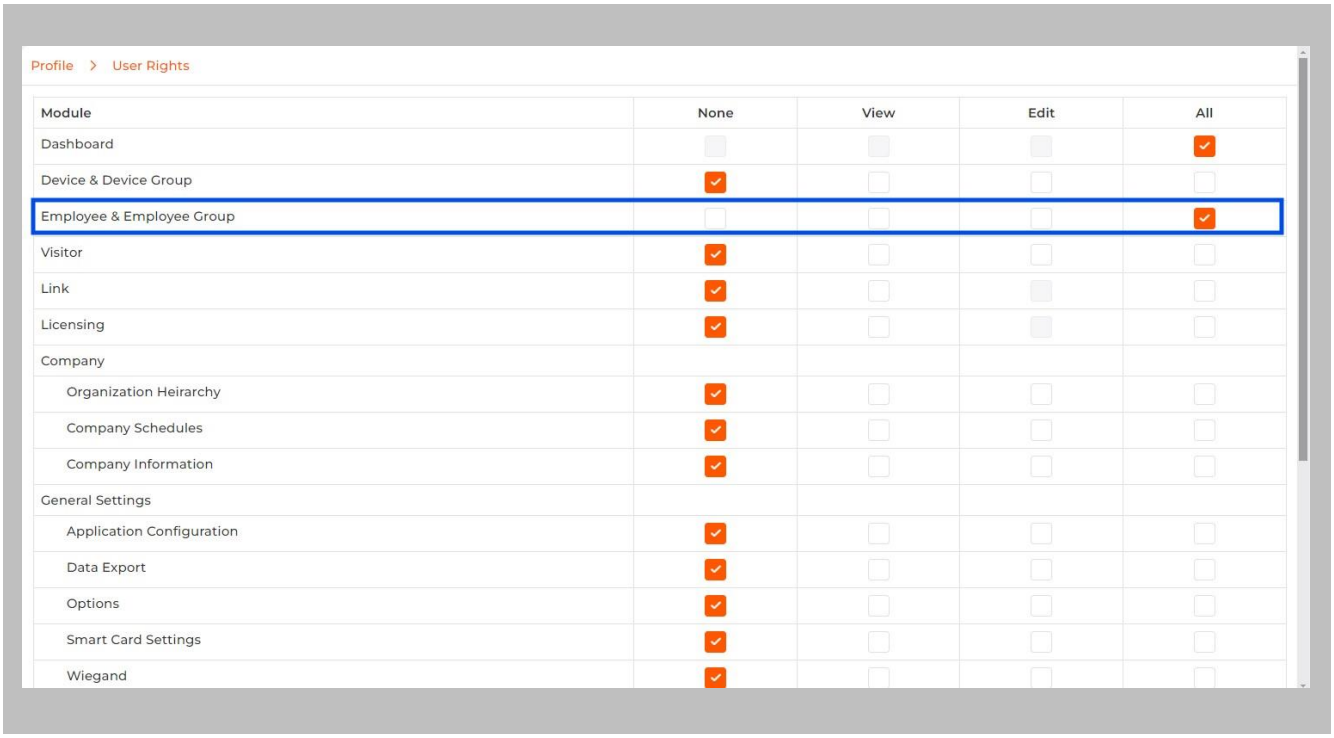


Figure 31: Employee and Employee Group Rights

STEP 5

Click **Save**.

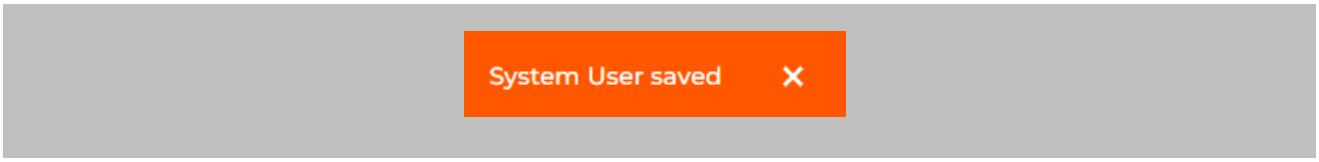


Figure 32: IXM WEB - Save System User

11. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

Click the **Devices** tab.

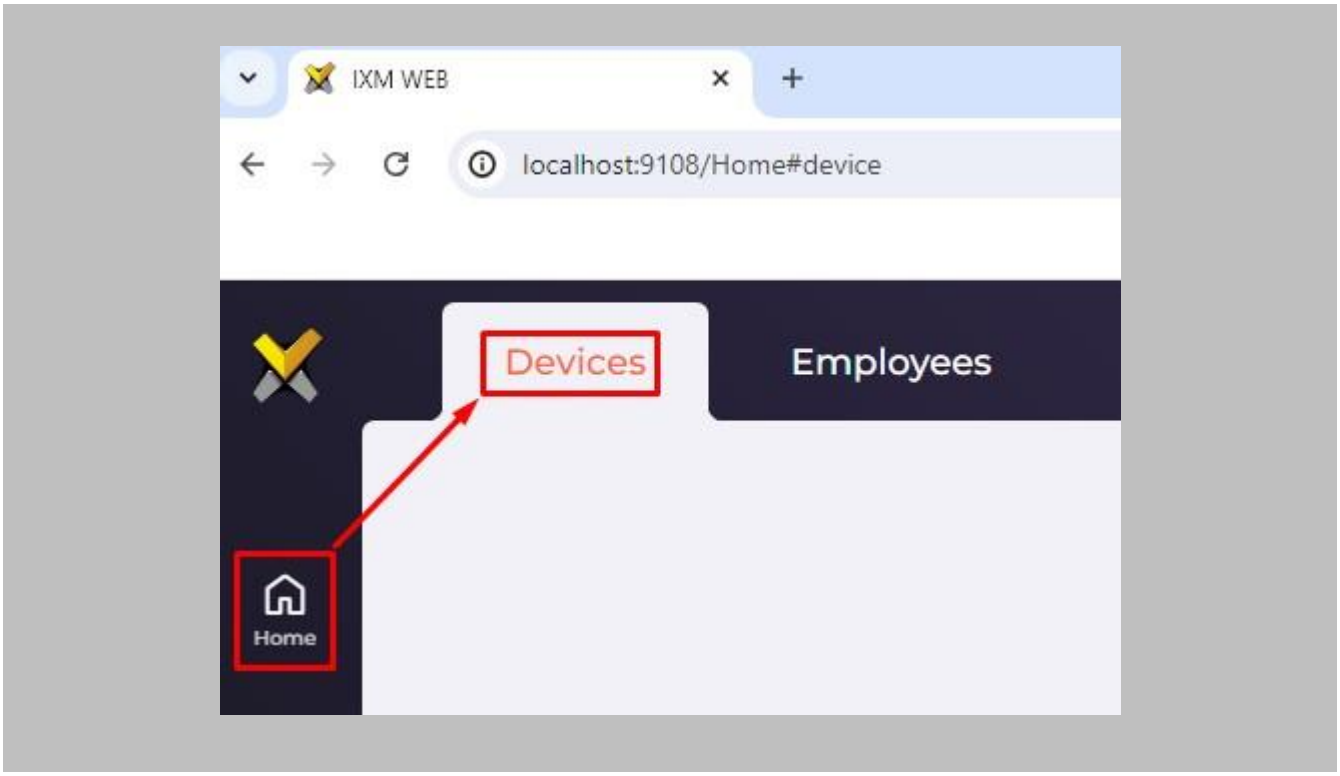


Figure 33: IXM WEB - Devices Tab

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.

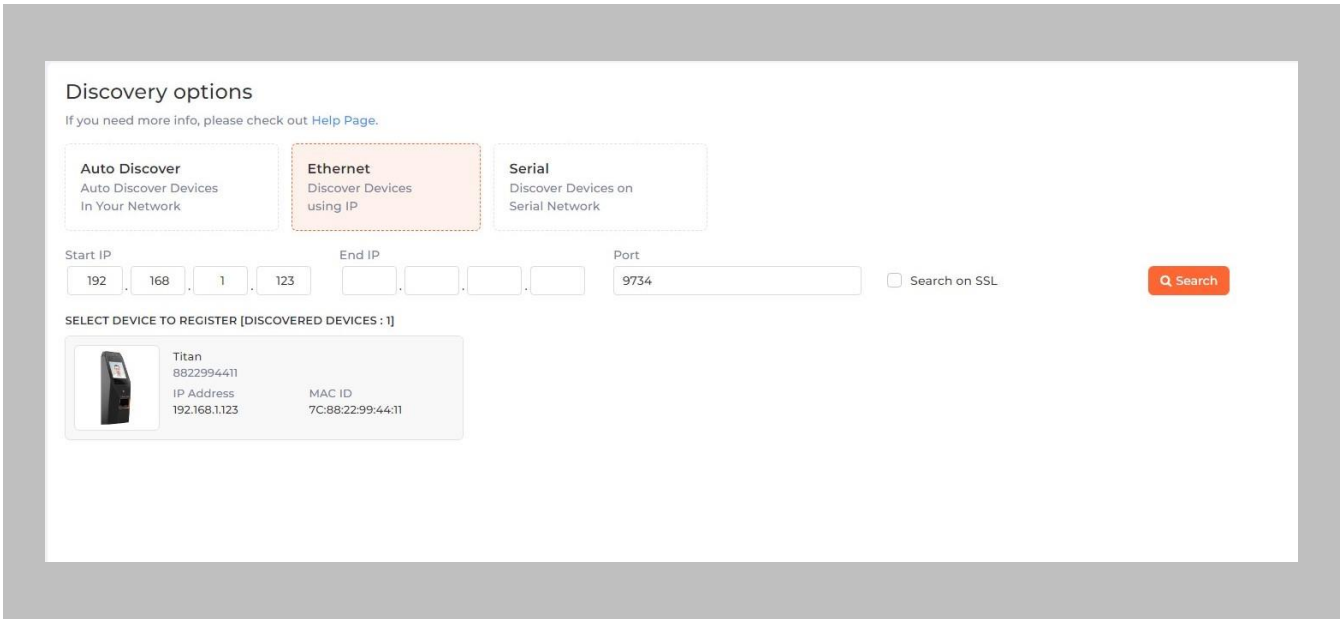


Figure 34: IXM WEB - Search Device Using IP Address

STEP 3

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

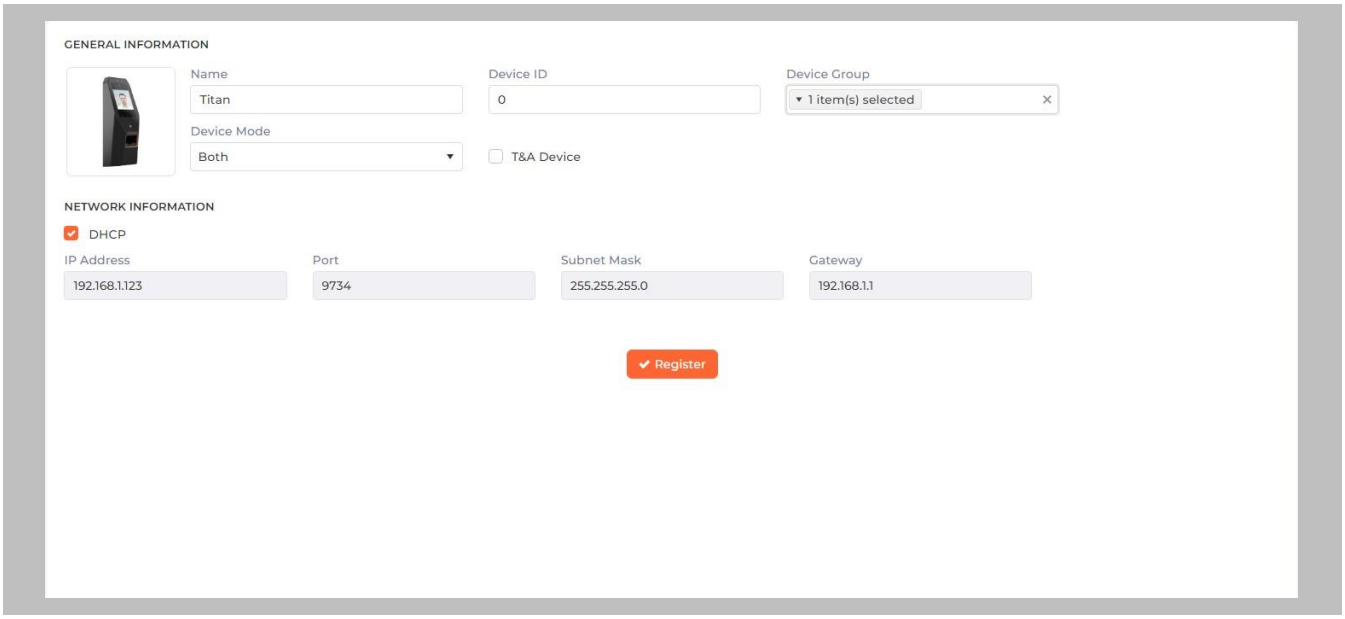


Figure 35: IXM WEB - Register Device

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**.

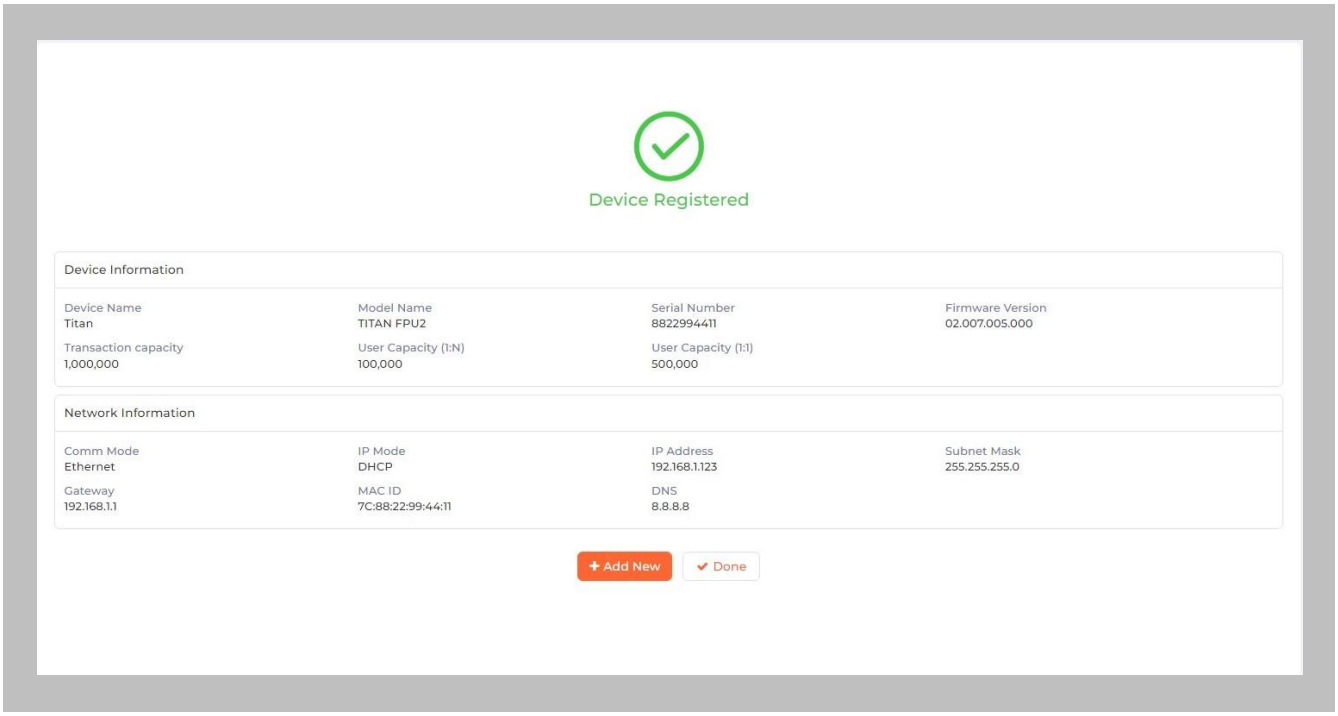


Figure 36: IXM WEB - Device Registration Complete

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).

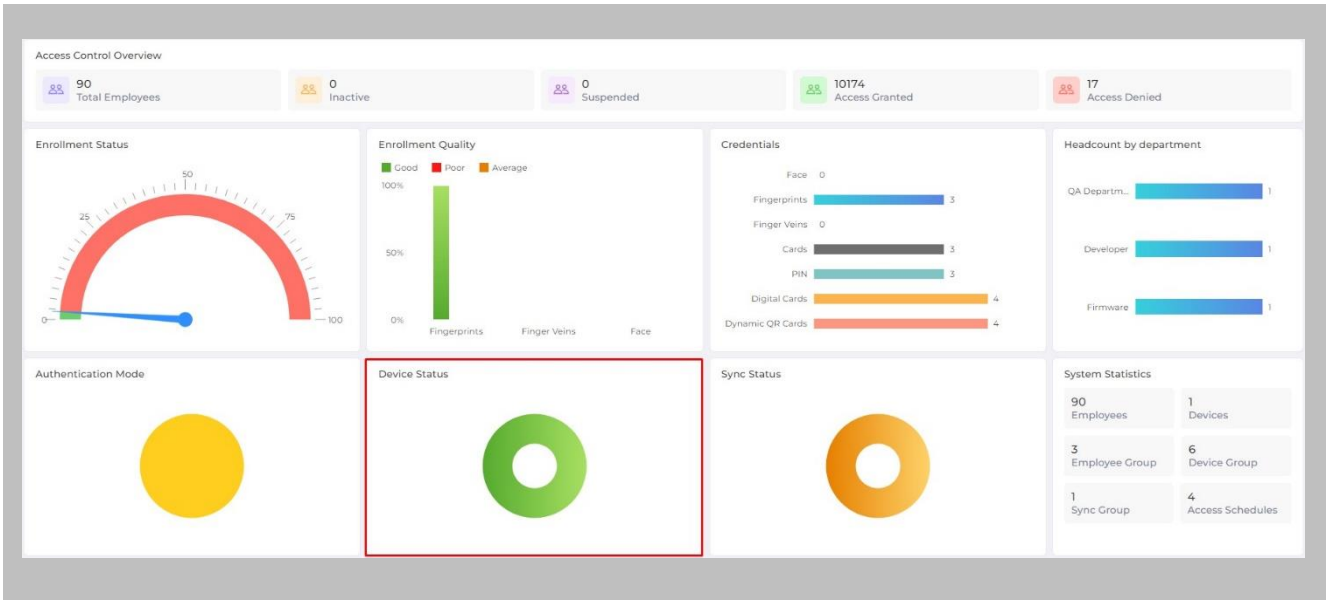


Figure 37: IXM WEB - Dashboard, Device Status

12. 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**.

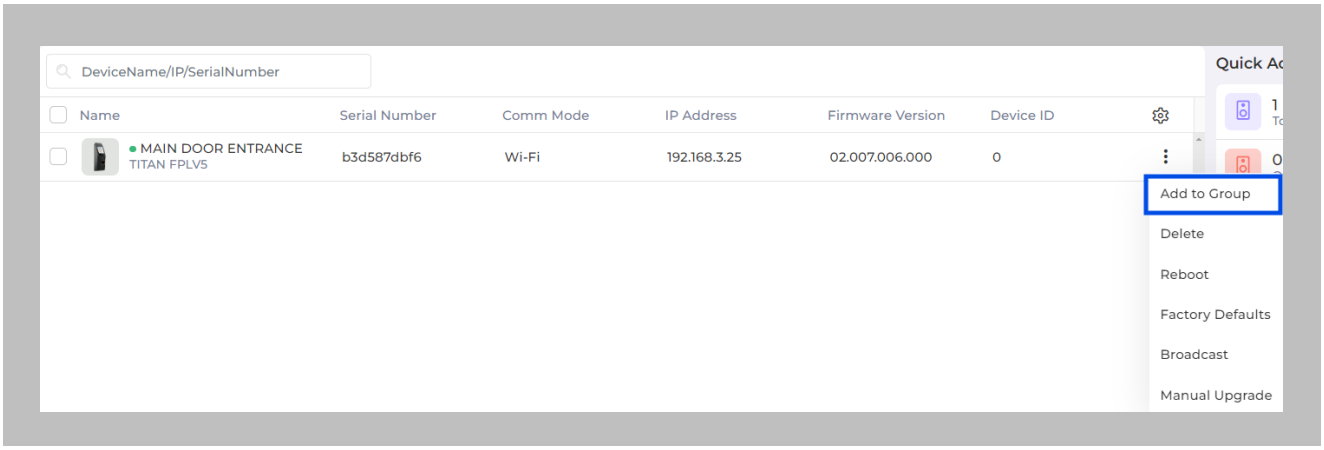


Figure 38: IXM WEB - Assign Device Group

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.**

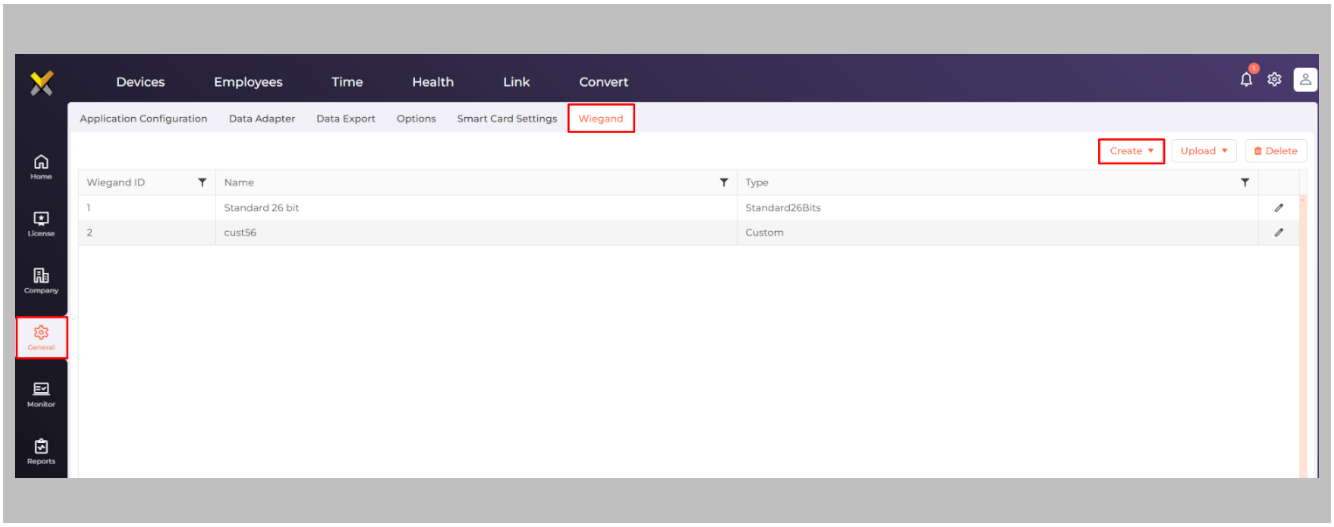


Figure 39: IXM WEB - Create Wiegand Format

STEP 2

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

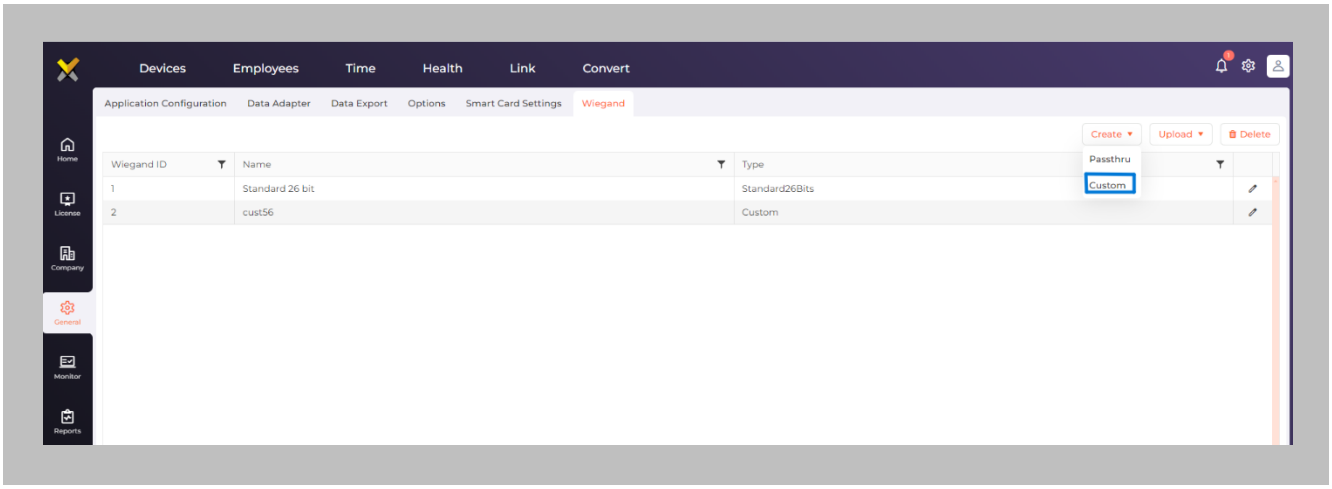


Figure 40: IXM WEB - Create Custom Wiegand Format

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.

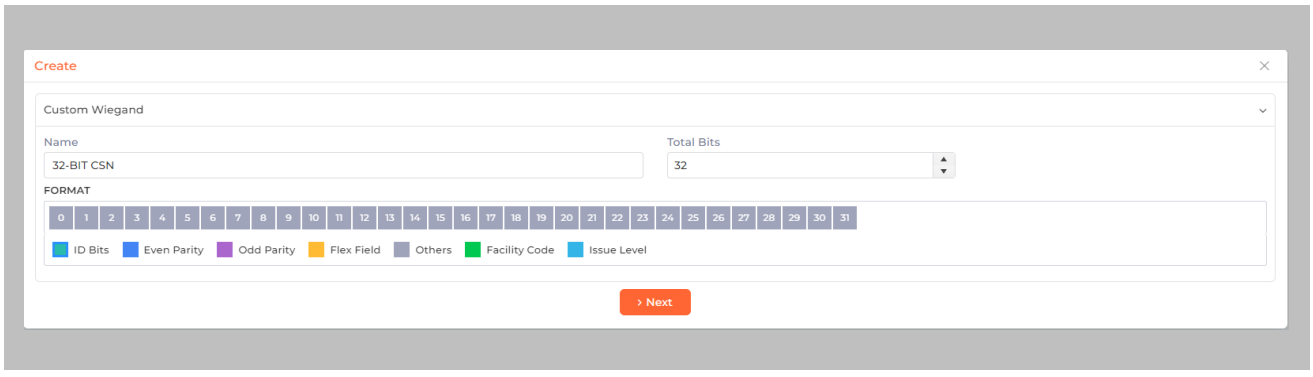


Figure 41: IXM WEB - Custom Wiegand Format

STEP 4

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

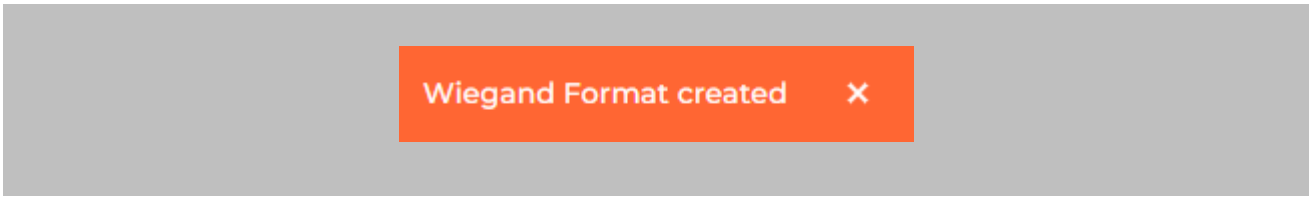


Figure 42: IXM WEB – Custom Wiegand Format Created

STEP 5

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

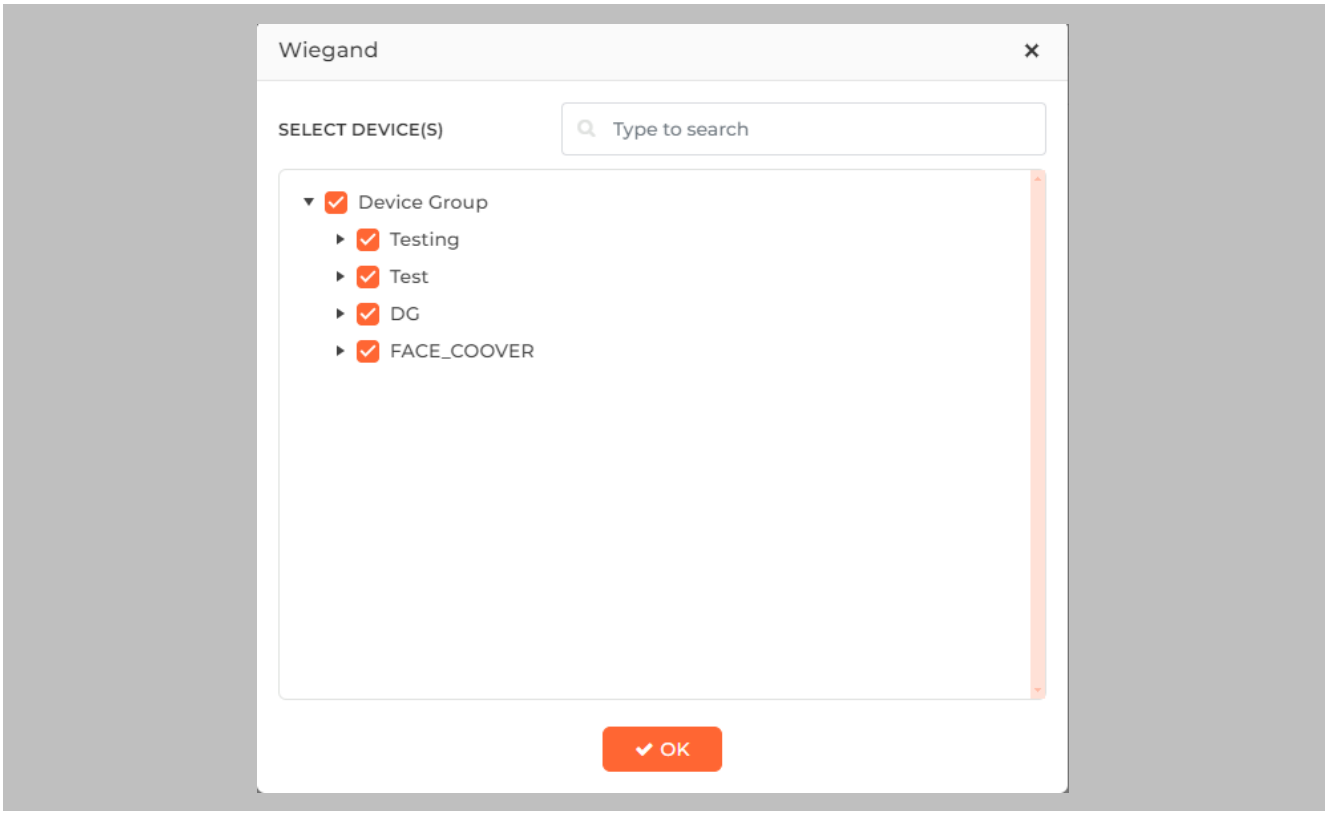


Figure 43: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invixium Readers

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

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

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.

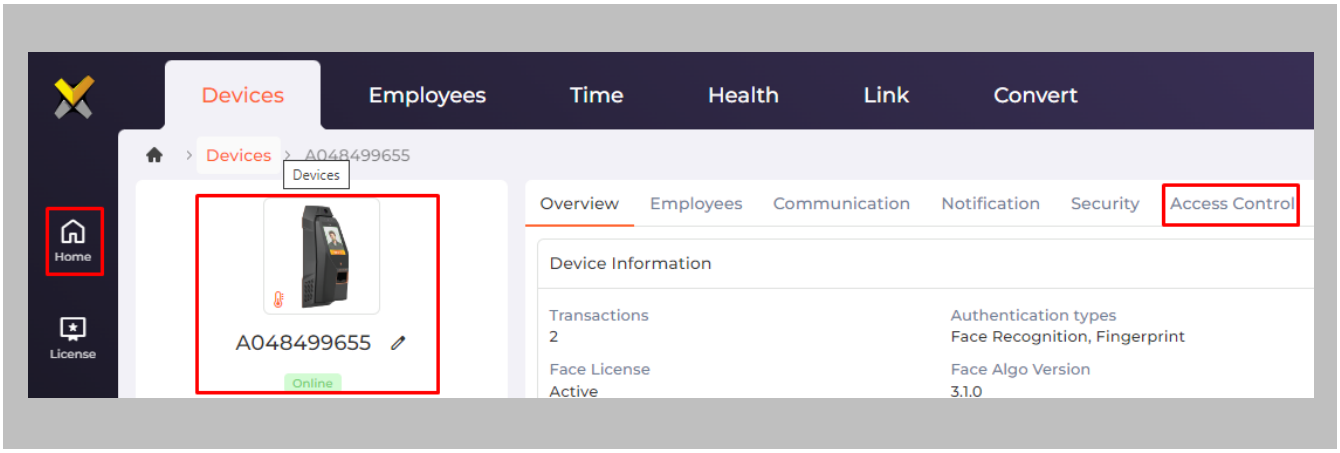


Figure 44: IXM WEB - Navigate to Access Control Tab

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.

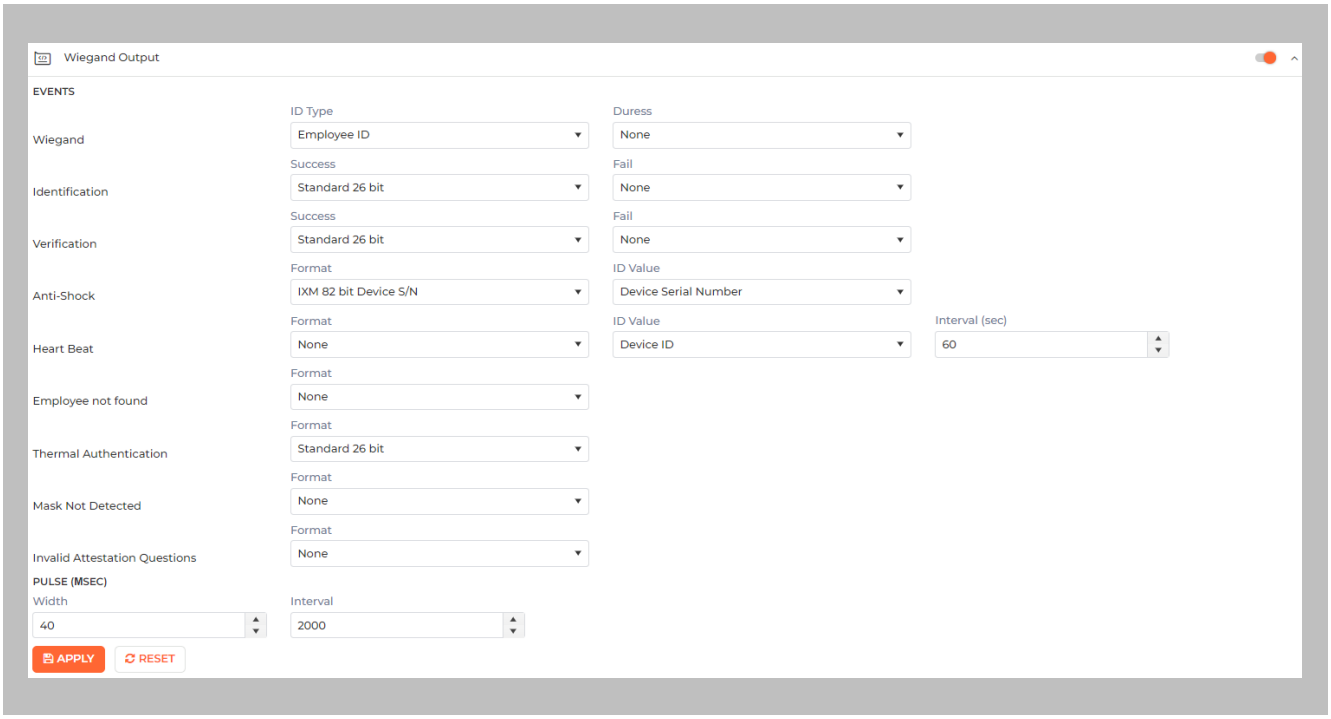


Figure 45: IXM WEB - Wiegand Output

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 Access It , select either Default Card or Actual Card.

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

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.**

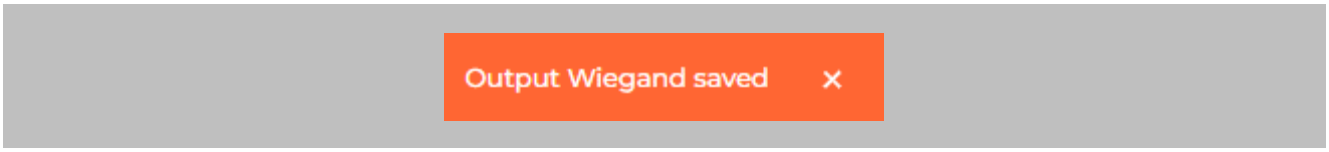


Figure 46: IXM WEB - Save Output Wiegand

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 Access It controller.
- To make this Wiegand output work on ACRE Security, you will need to make sure the Wiegand format is available in ACRE Security for use on the controllers talking to the Invixium reader (by Wiegand or OSDP).

Configuring Panel Feedback with ACRE Security

Procedure

STEP 1

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

STEP 2

Connect the **LED** of the ACRE Security 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**.

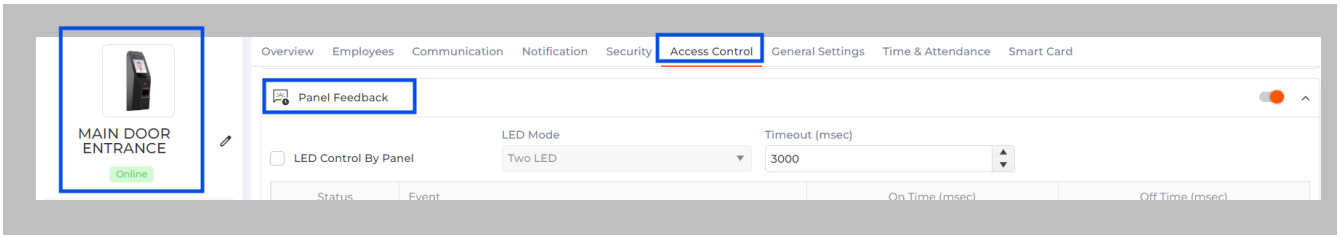


Figure 47: IXM WEB - Panel Feedback

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**.

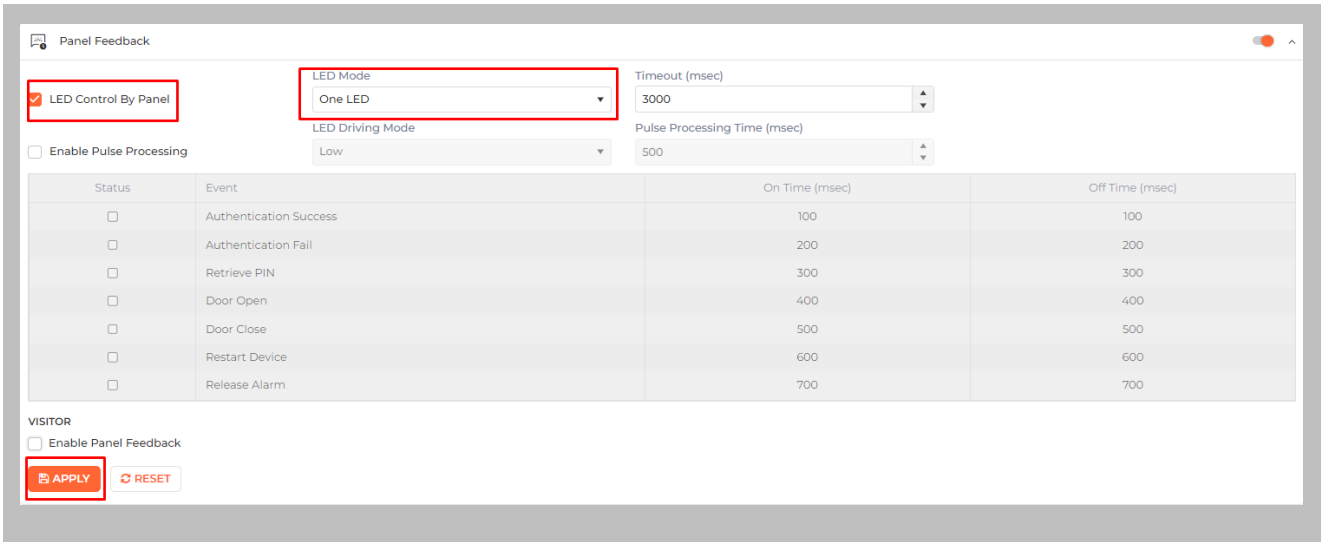


Figure 48: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.

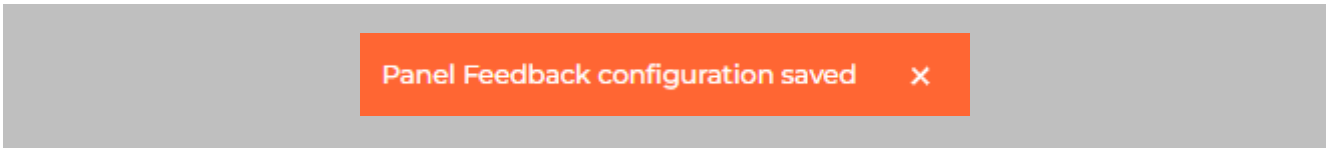


Figure 49: IXM WEB - Save Panel Feedback

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.

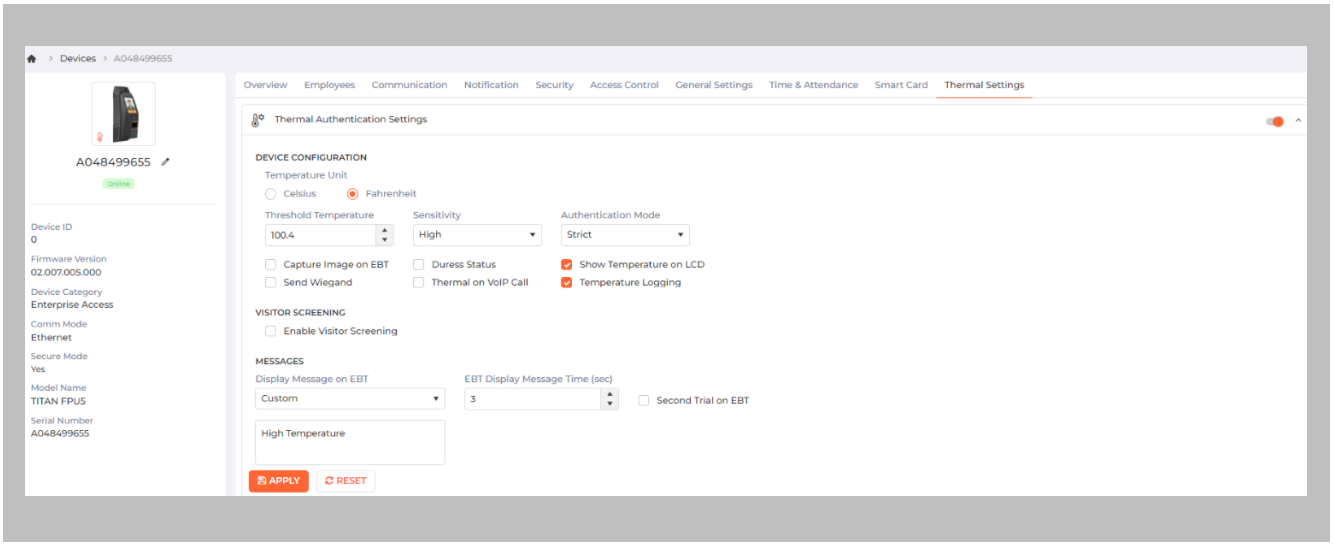


Figure 50: IXM WEB - Thermal Settings

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**.

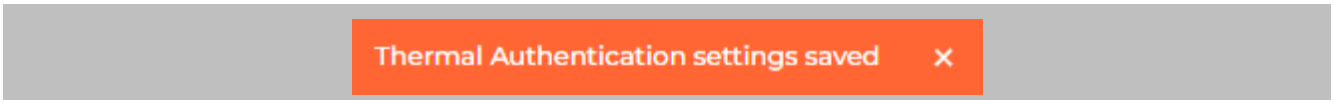


Figure 51: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

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

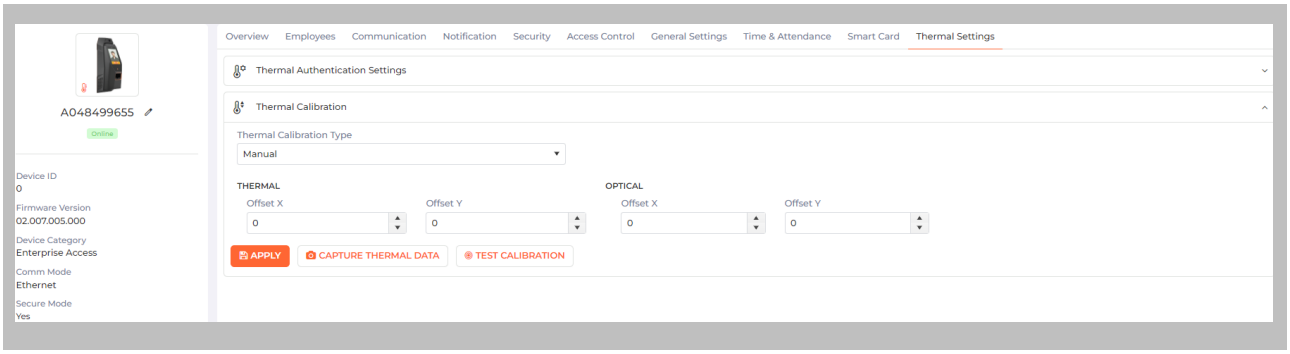


Figure 52: IXM WEB - Thermal Calibration Settings

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**.

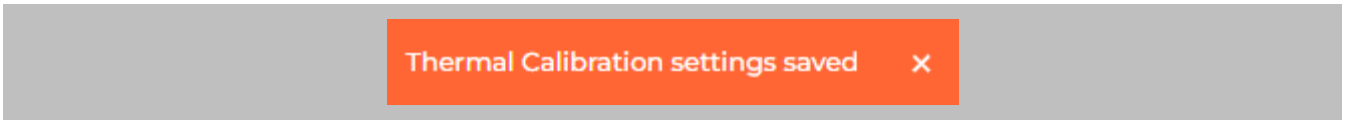


Figure 53: IXM WEB - Save Thermal Calibration Settings

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.

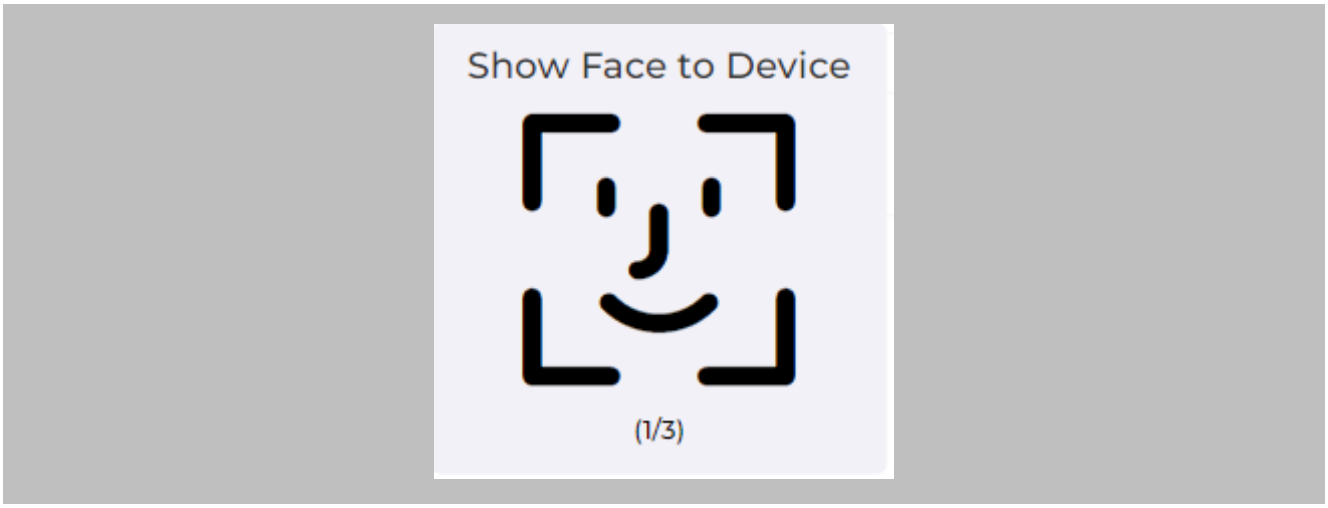


Figure 54: IXM WEB - Capture Thermal Data

STEP 4

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

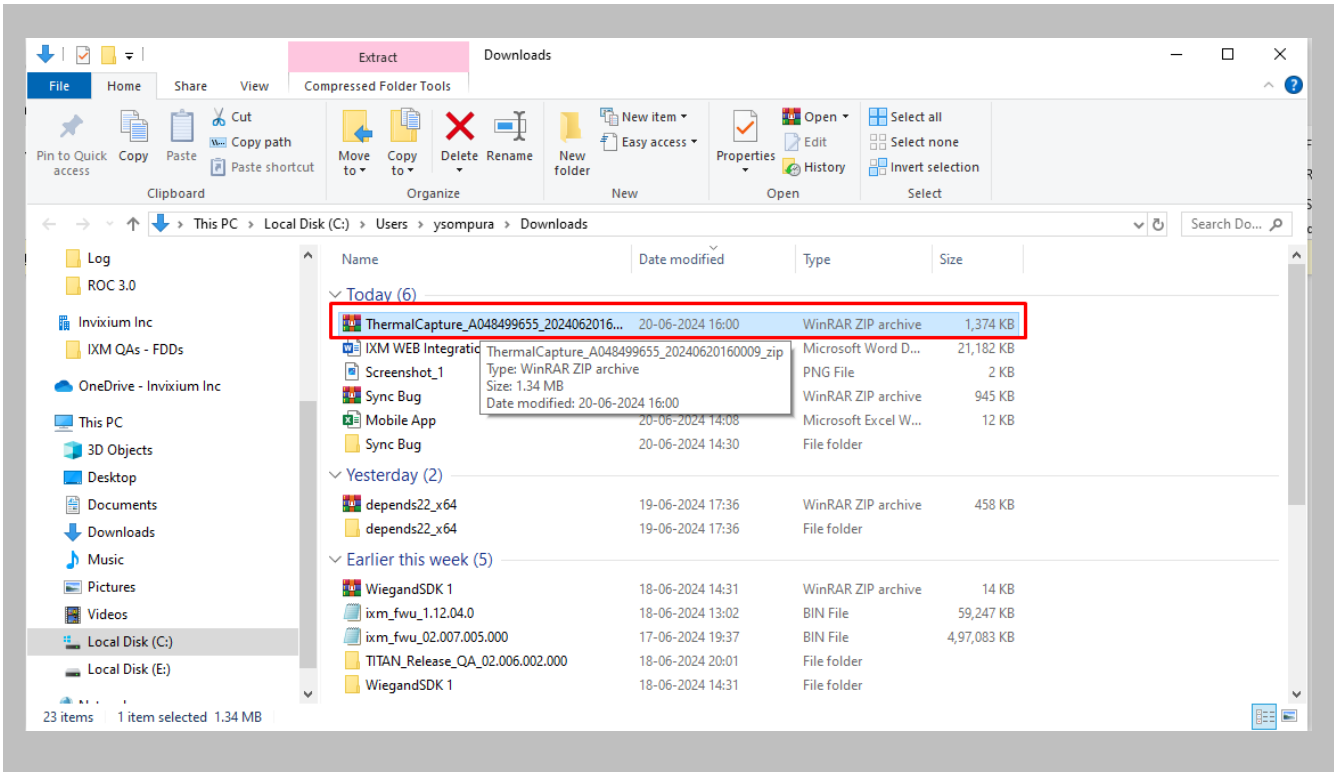


Figure 55: IXM WEB - Save Captured Thermal Data

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**.

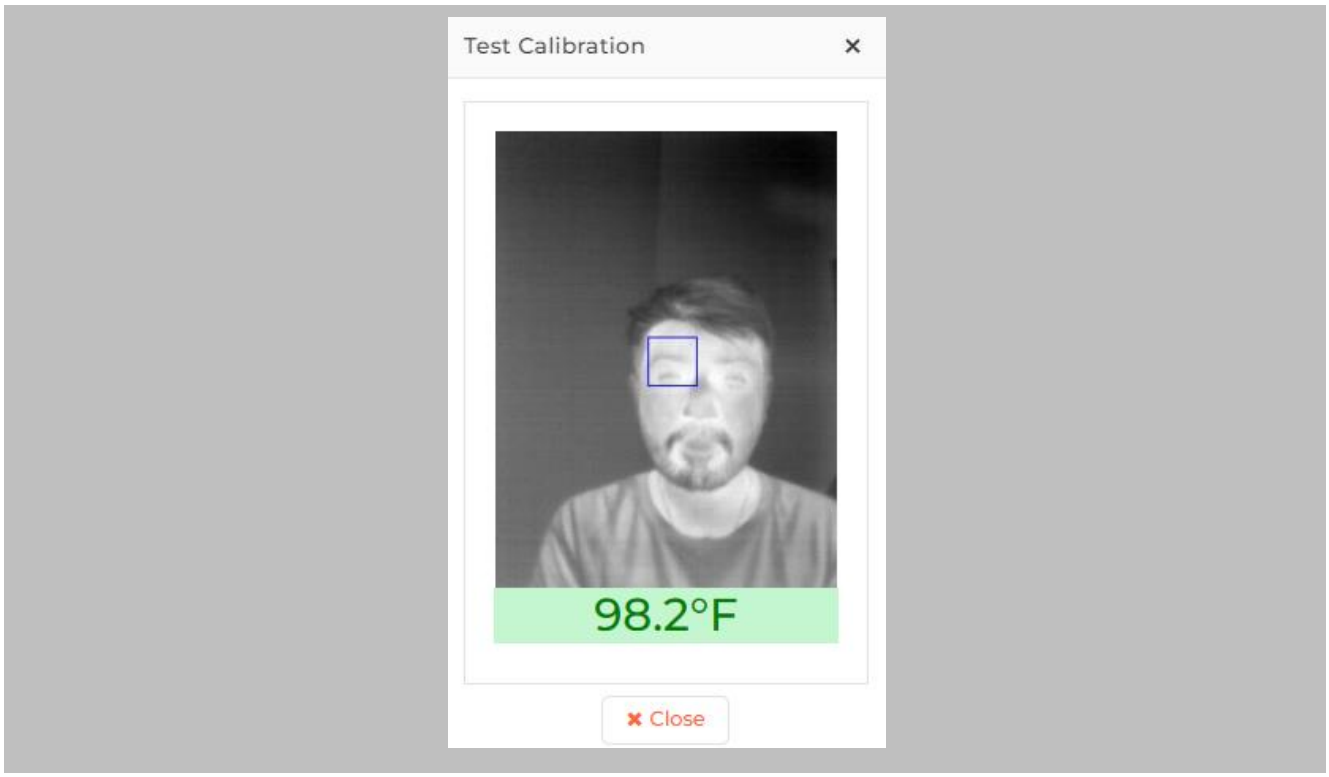


Figure 56: IXM WEB - Test Thermal Calibration

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**.

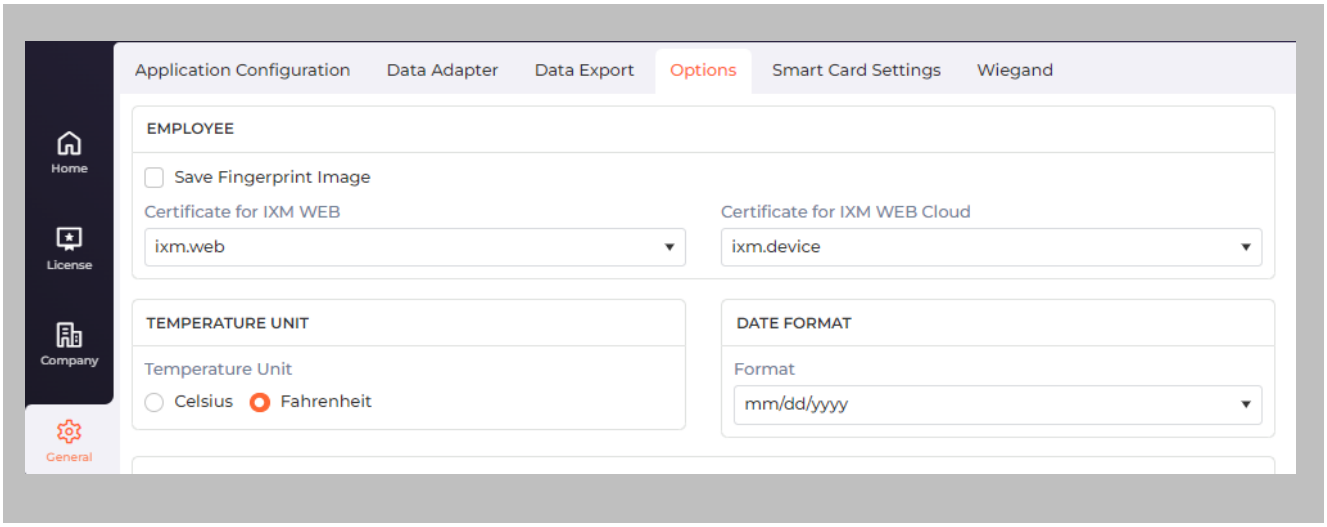


Figure 57: IXM WEB - Option to Change Temperature Unit

STEP 2

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

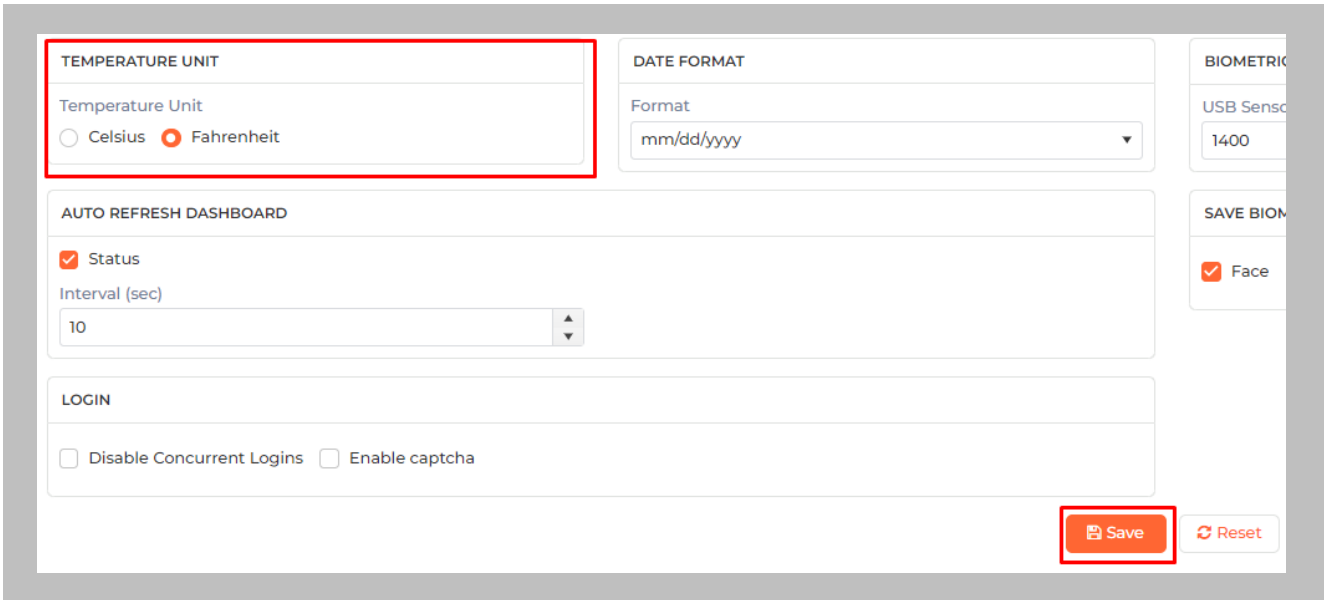


Figure 58: IXM WEB - Save Temperature Unit Setting

Configuring Mask Authentication Settings

STEP 1

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

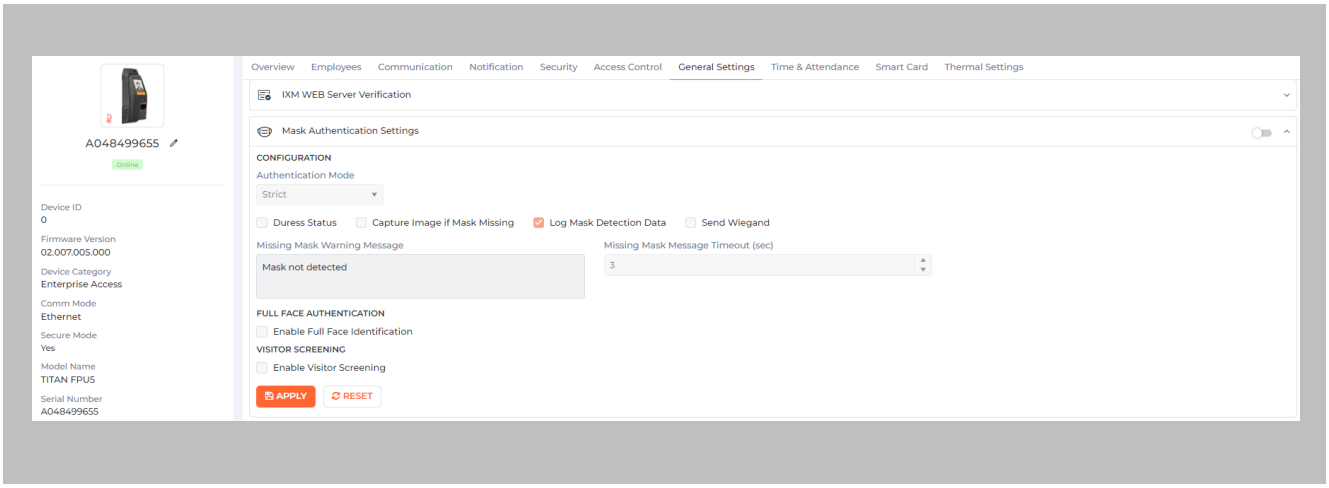


Figure 59: IXM WEB - Mask Authentication Settings

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**.

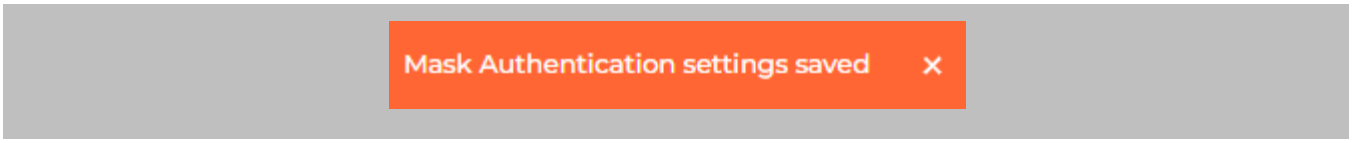


Figure 60: IXM WEB - Save Mask Settings

13. Fingerprint Enrollment using Access It sofware

Procedure

STEP 1

Log in to the Access It application. Click the **System tab** on the left-hand menu.

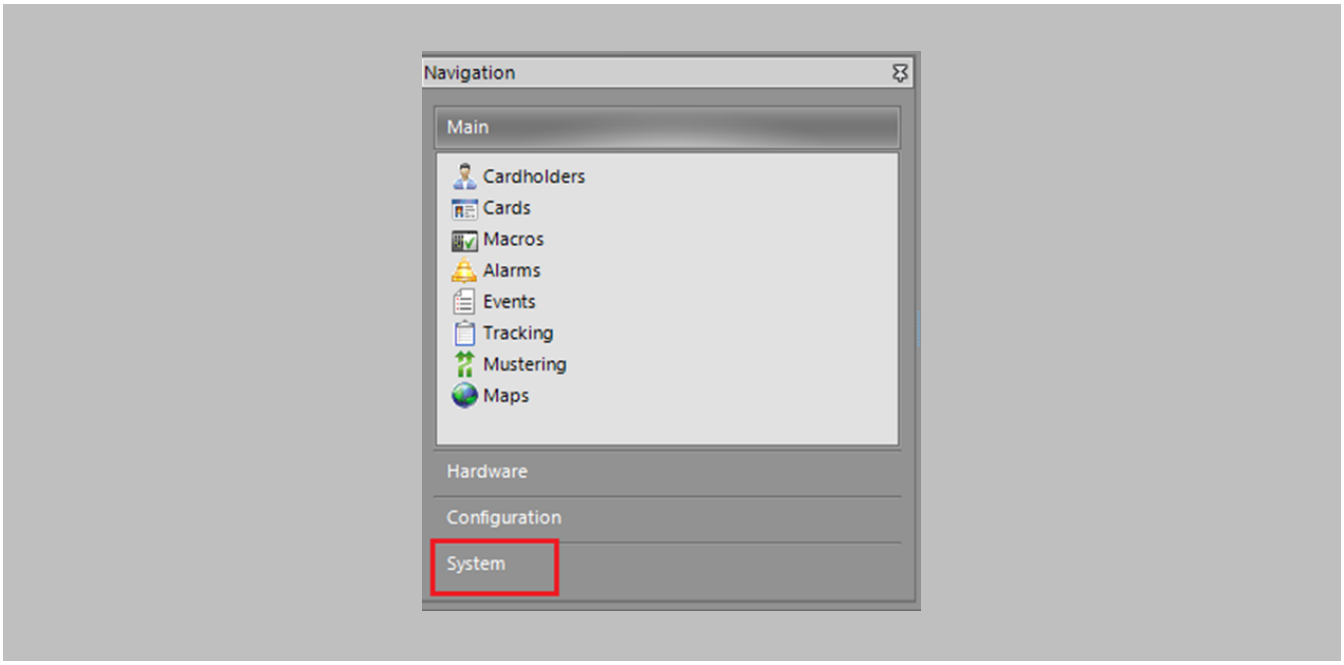


Figure 61: ACRE Security - System

STEP 2

Select **Workstations**.

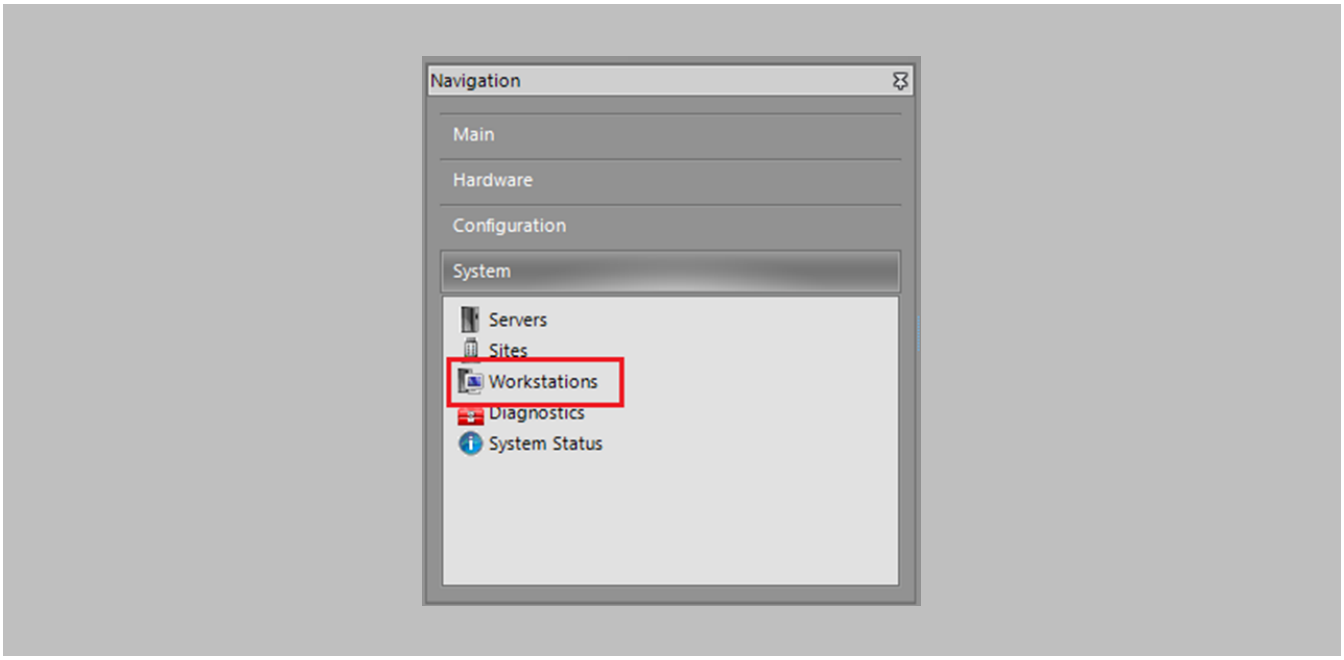


Figure 62: ACRE Security – Workstations

STEP 3

Edit the workstation from which entrollment has to be done.

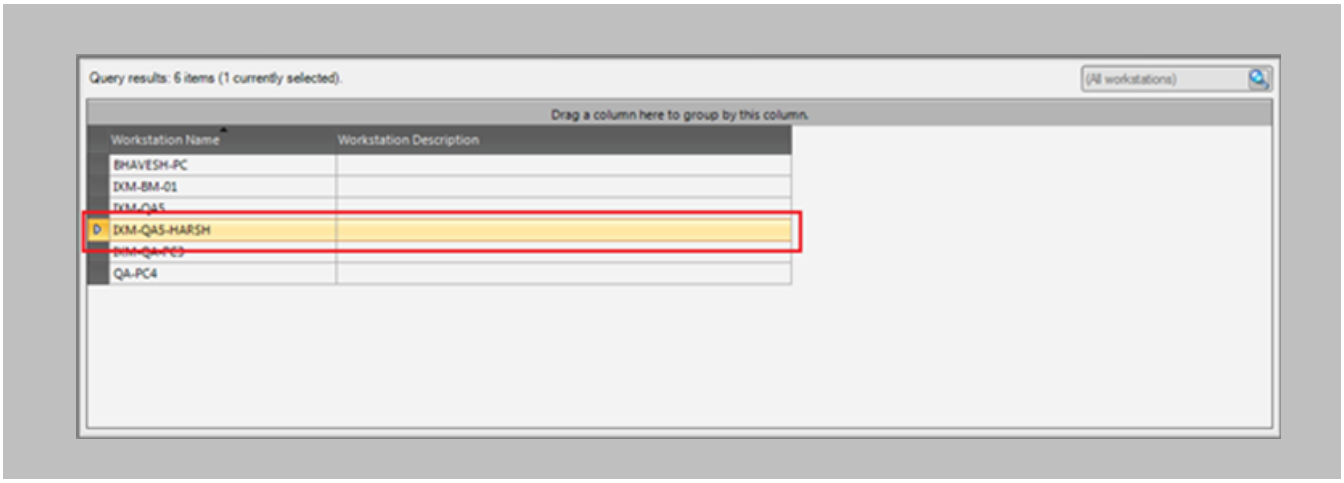


Figure 63: ACRE Security – Edit Workstation

STEP 4

Select the **Encode/Enroll** tab.

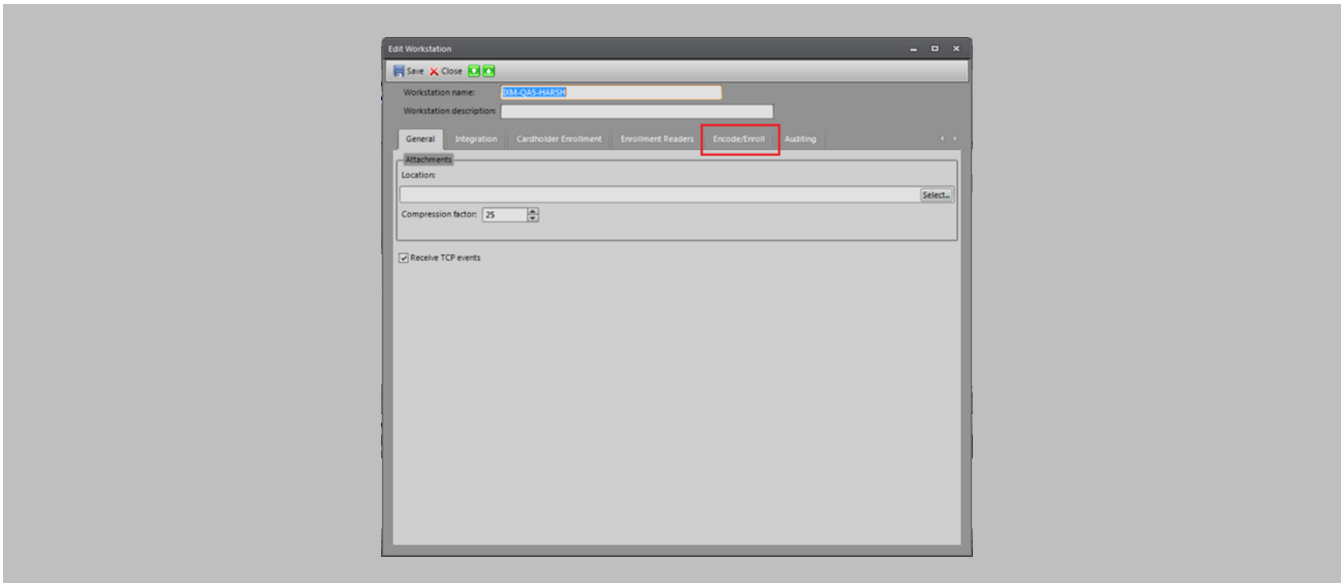


Figure 64: Edit Workstation – Encode / Enroll

STEP 5

Click **New.**

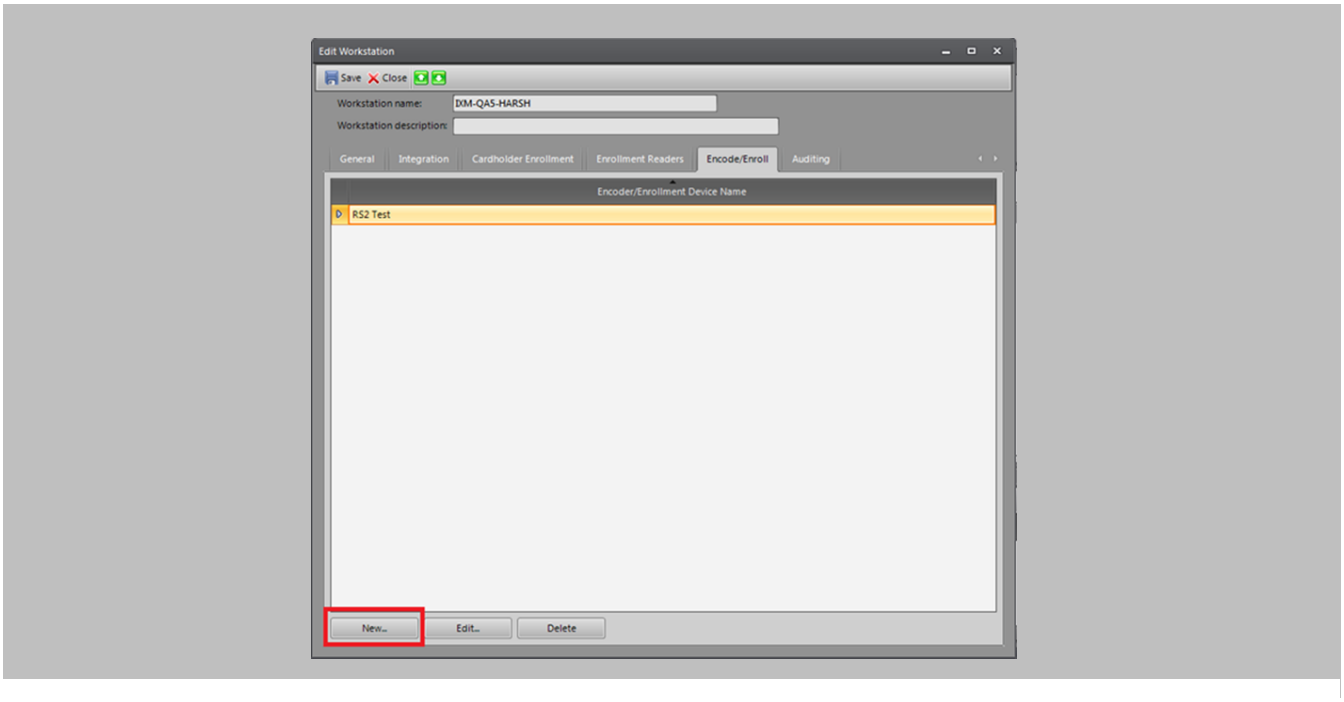


Figure 65: Encode/Enroll – Add New

STEP 6

Enter IXM WEB details as follows:

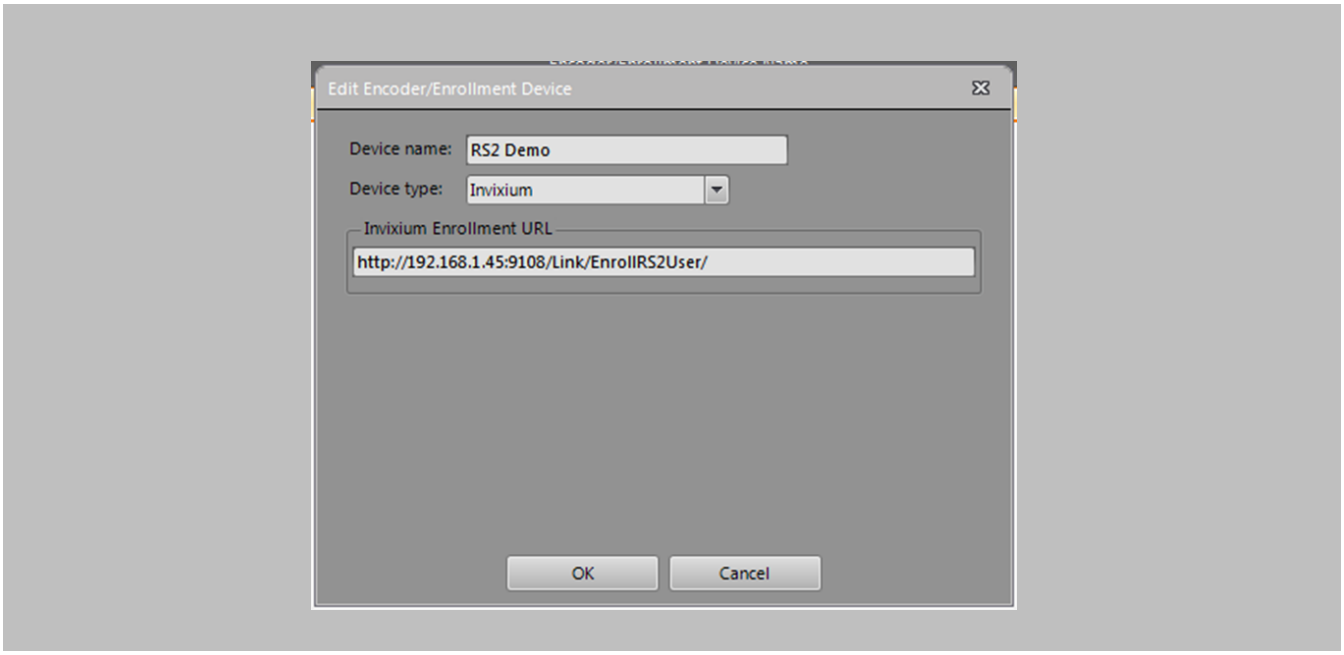


Figure 66: Add new Device

Devide name:
Enter the name of the device.

Device type:
Select “Invixium” from the dropdown list.

Once done, click **OK** button.

Close and reopen the Access It software.

STEP 7

Go to **Main >> Cardholder >> Select user >> click on Card Number**. This will show the newly created device name.

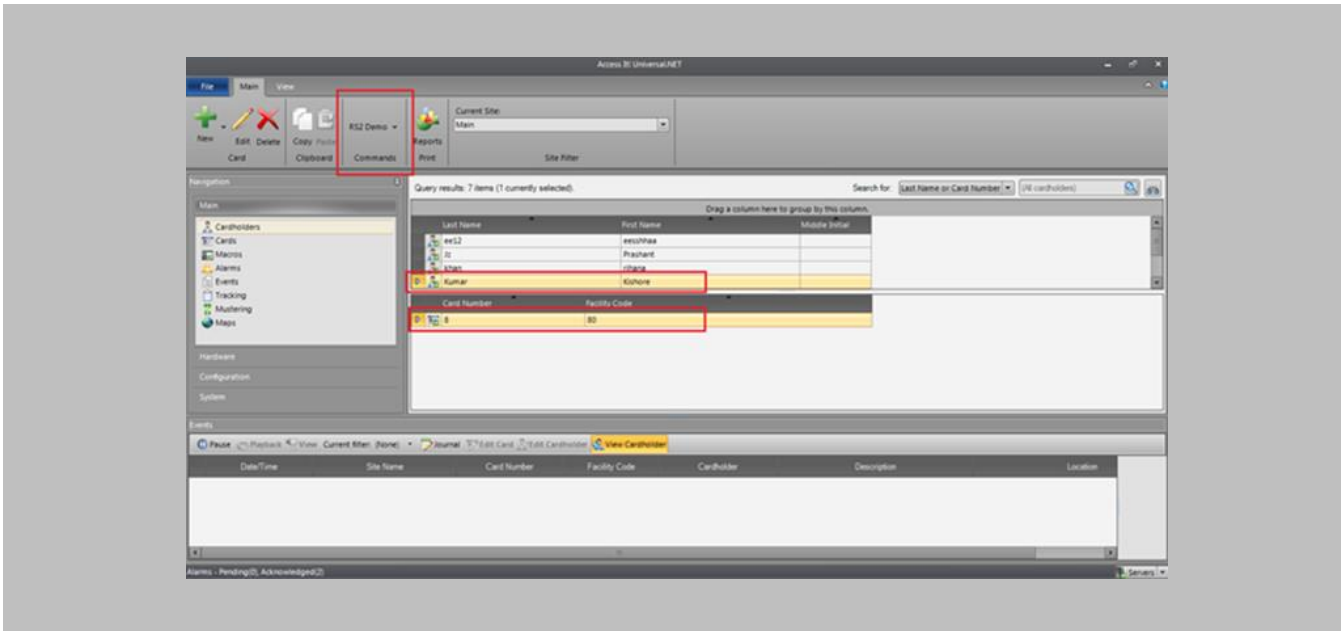


Figure 67: Newly created device

STEP 8

Click on the device name to launch IXM WEB using the “Invixium Enrollment URL” with the cardholder ID appended for enrollment.

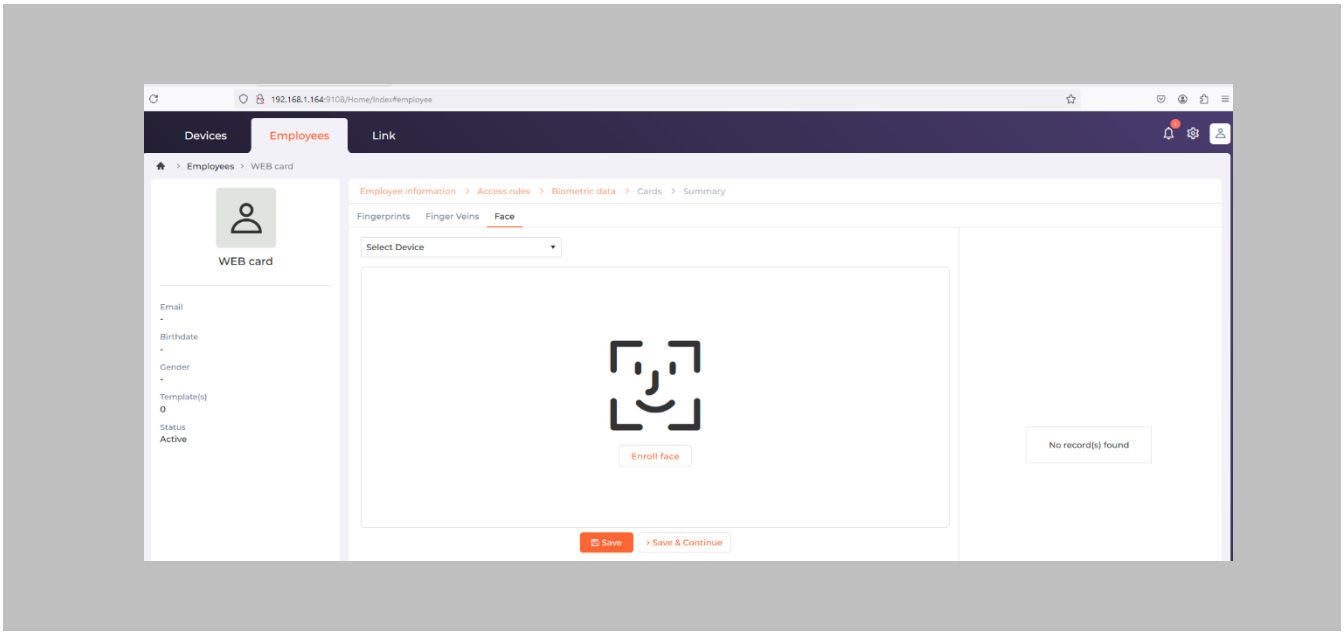


Figure 68: IXM WEB – Biometric Enrollment

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.

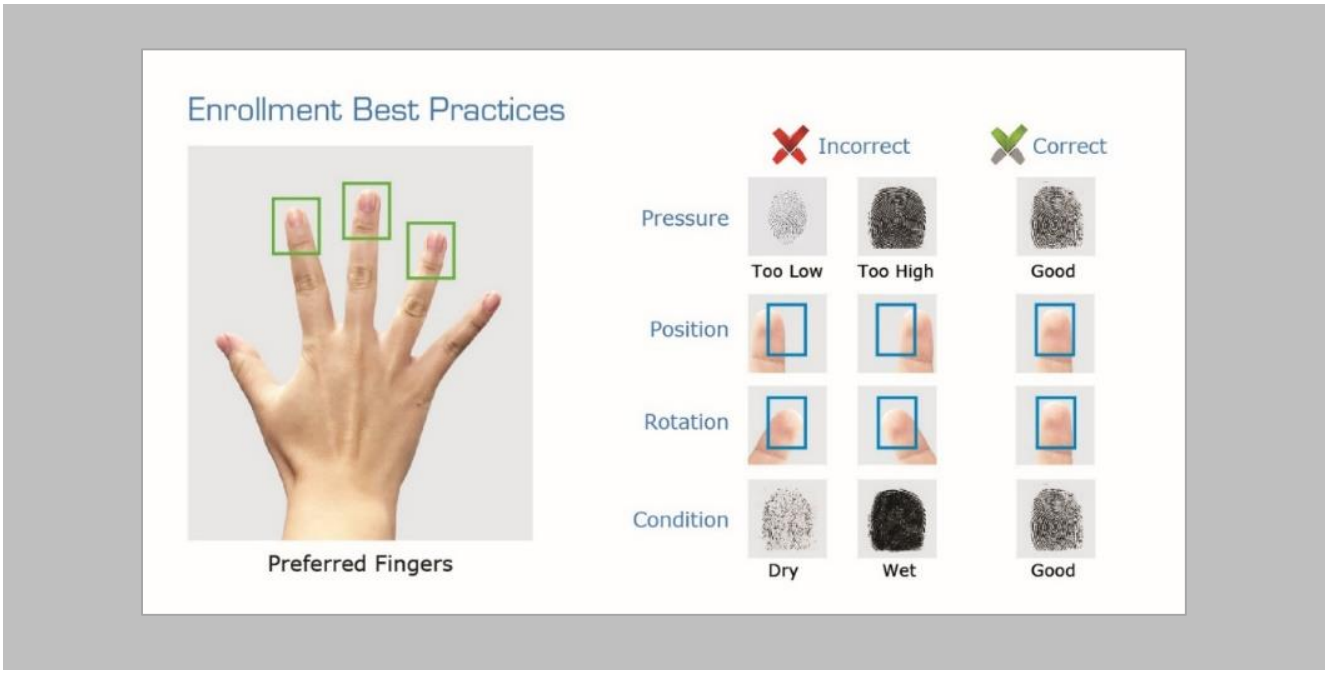


Figure 69: Fingerprint Enrollment Best Practices

Fingerprint Image Samples

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

Figure 70: 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.

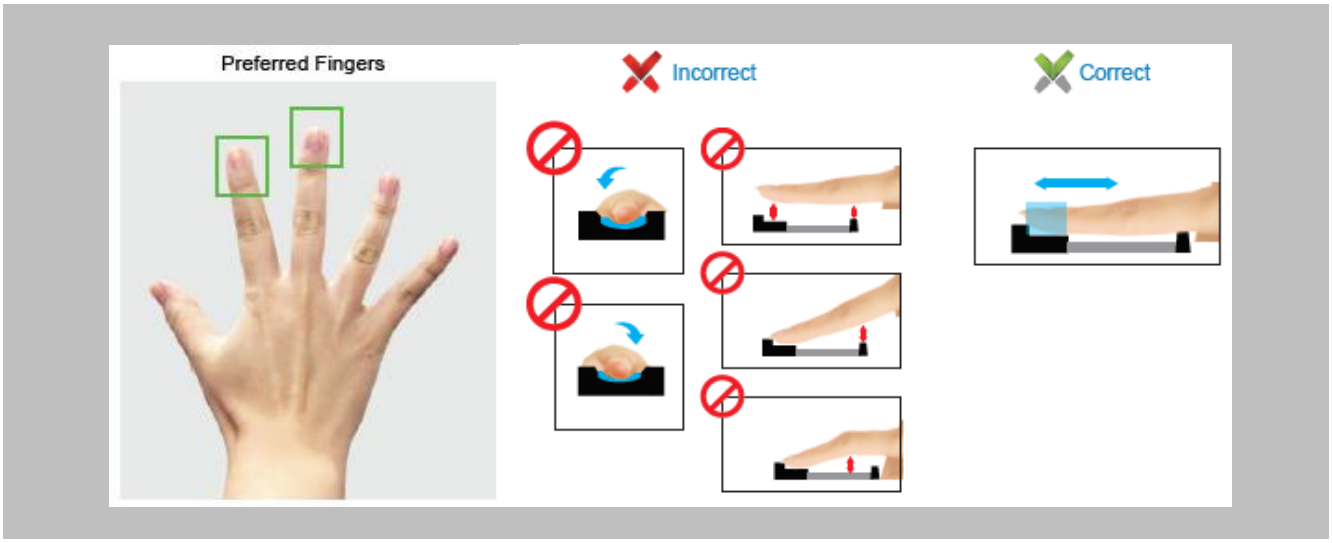


Figure 71: Finger Vein Enrollment Best Practices

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.

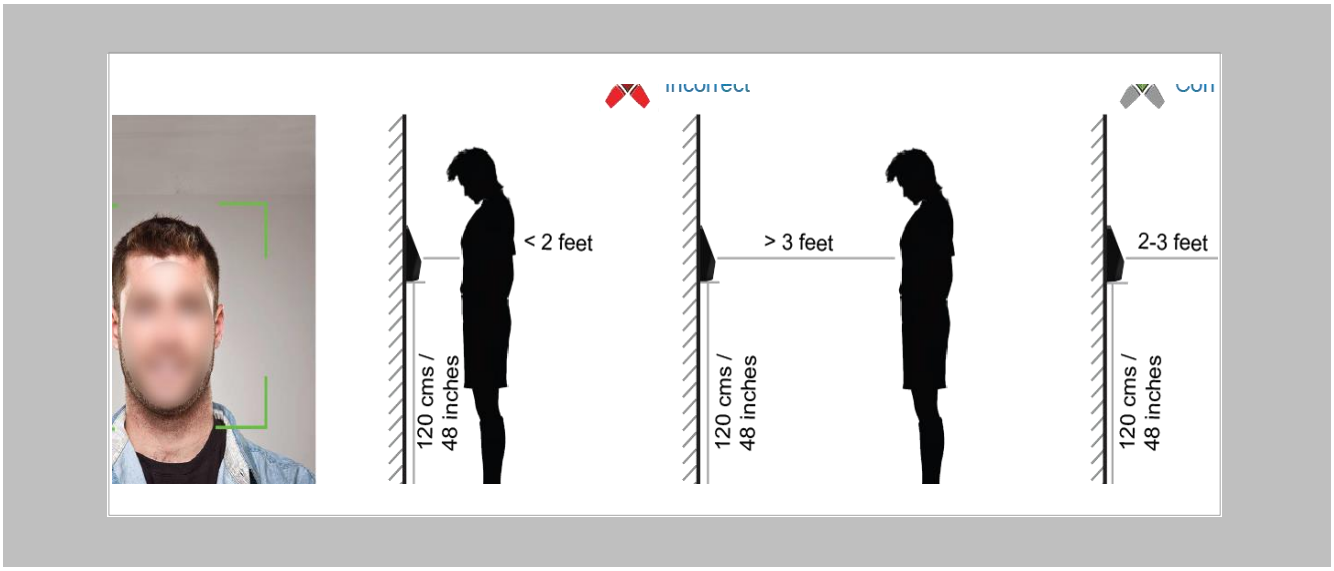


Figure 72: Face Enrollment Best Practices

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 73: Install IXM WEB

Note: Installs SQL 2014 Express.

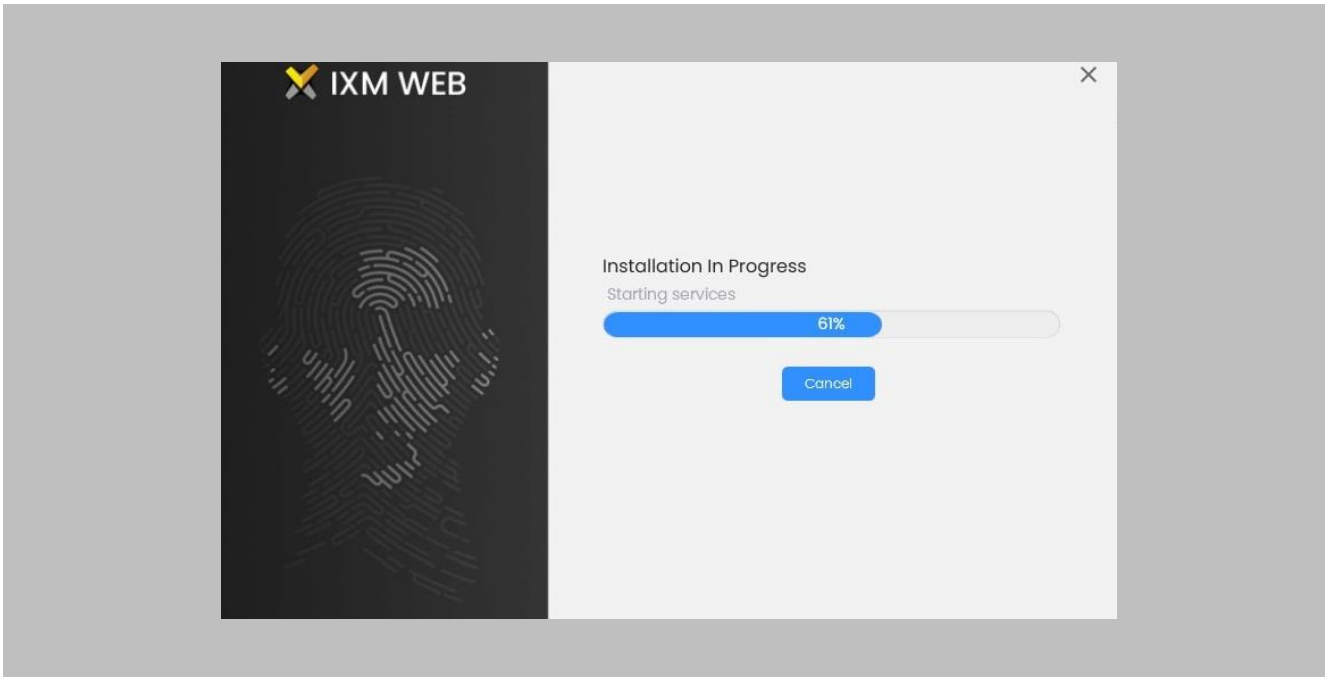


Figure 74: Loading SQL Express & Installation Progress

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.

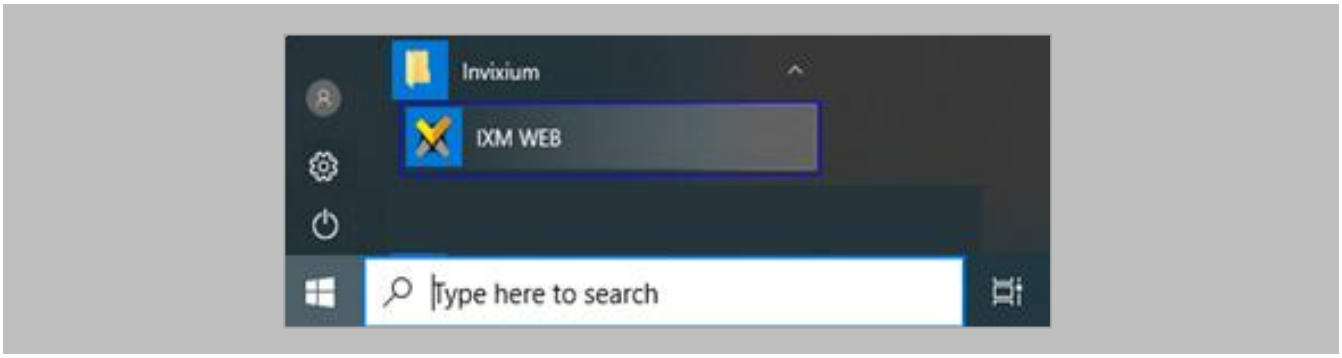


Figure 75: IXM WEB - Shortcut Icon on Desktop

STEP 4

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

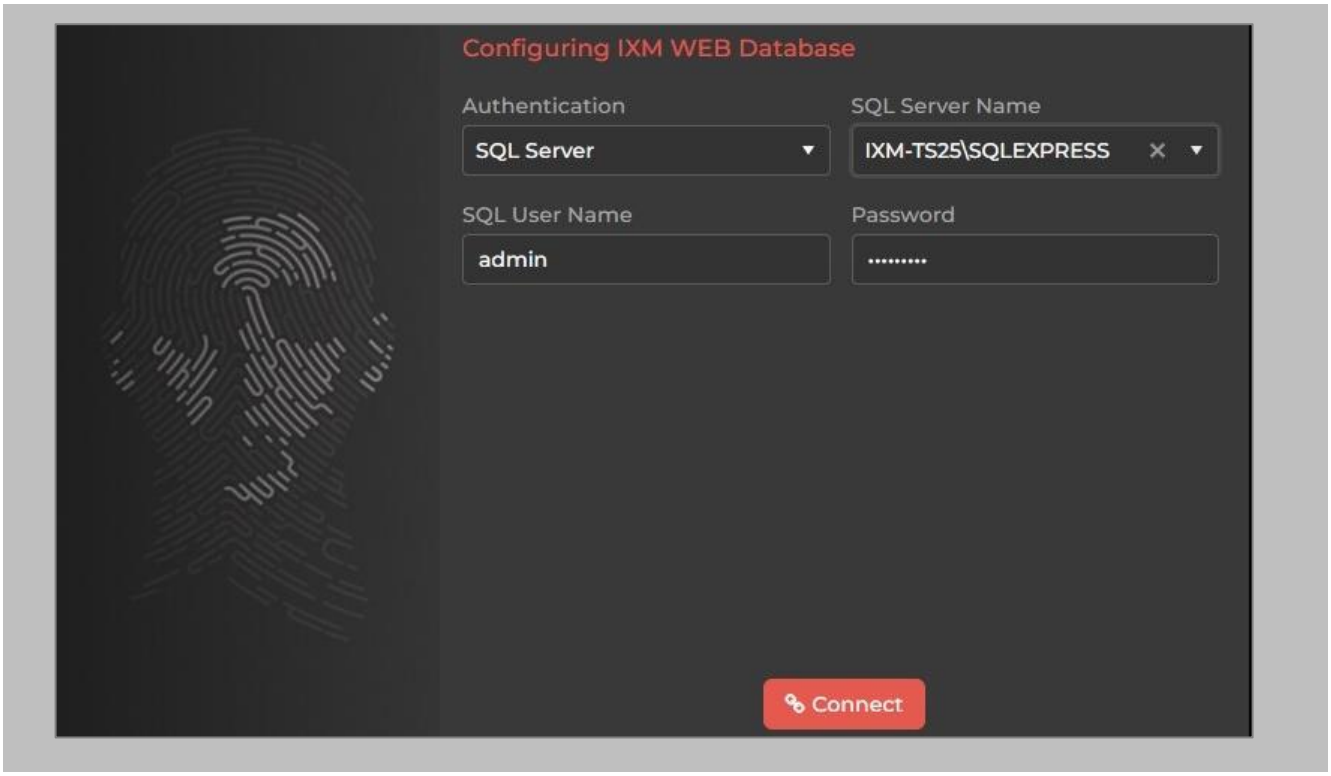


Figure 76: IXM WEB - Configuring IXM WEB Database

STEP 5

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

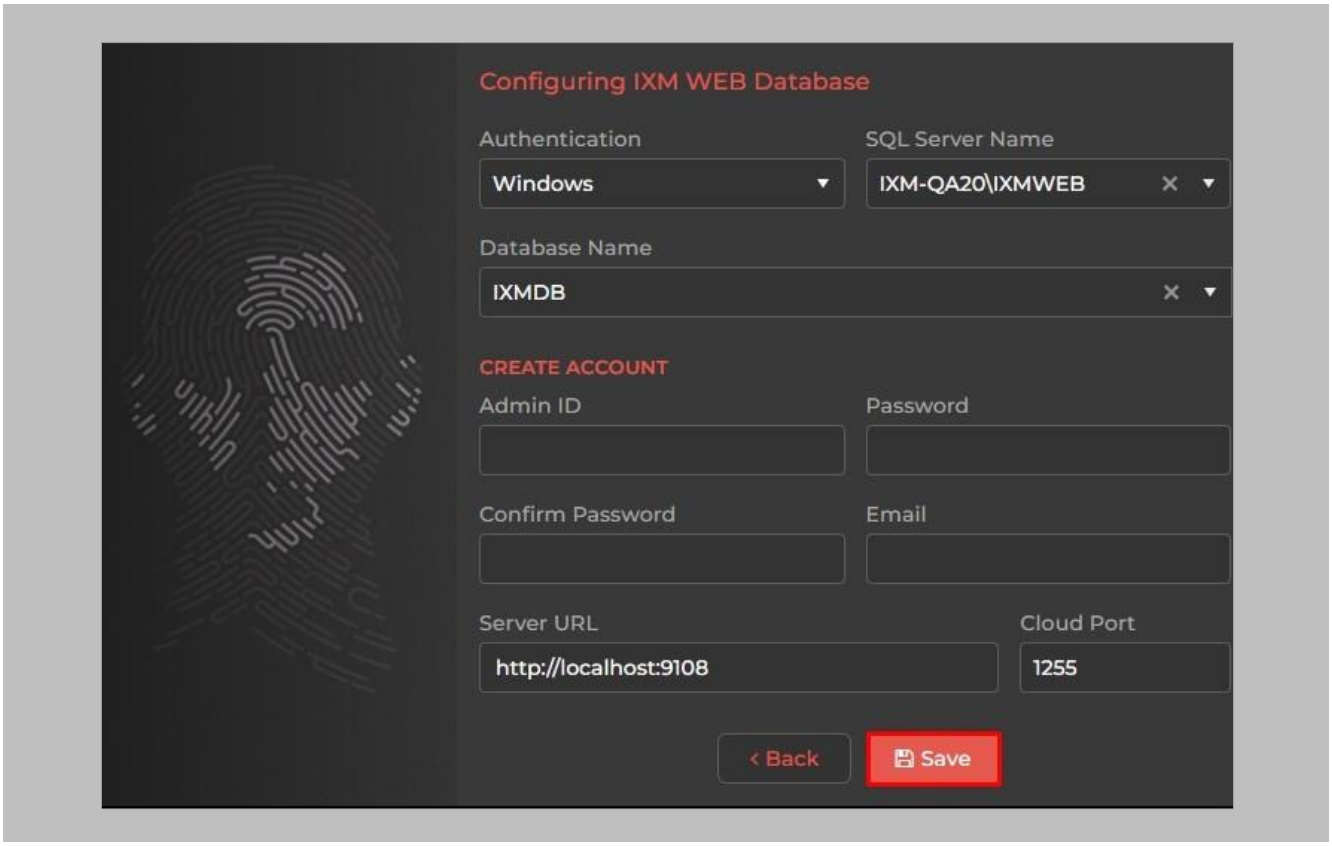


Figure 77: IXM WEB - Select Database Name

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 Invixium Readers

Procedure

STEP 1

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

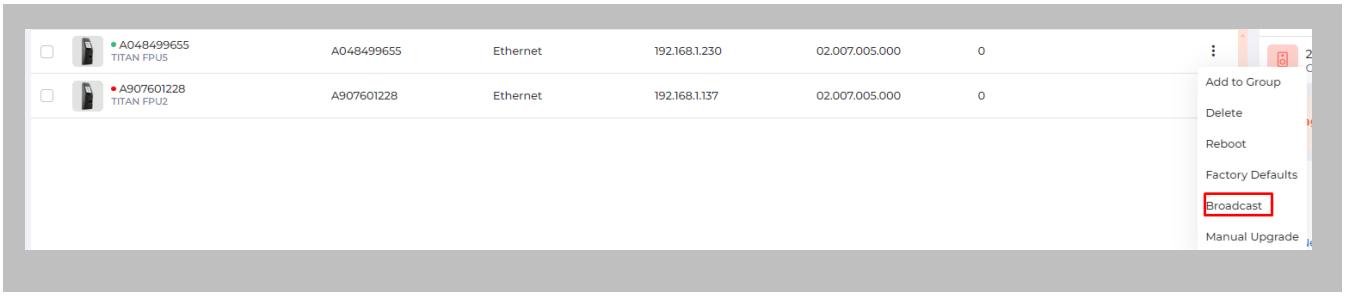


Figure 78: IXM WEB - Broadcast Option

STEP 2

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

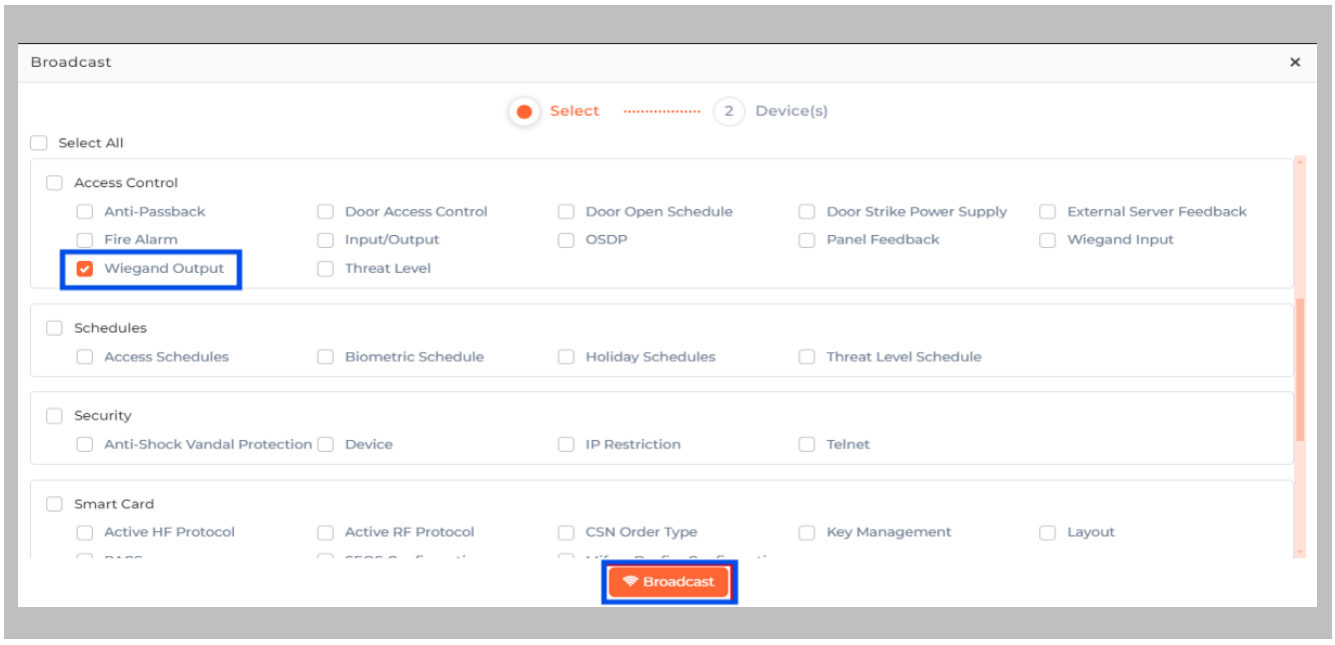


Figure 79: IXM WEB - Broadcast Wiegand Output Settings

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.

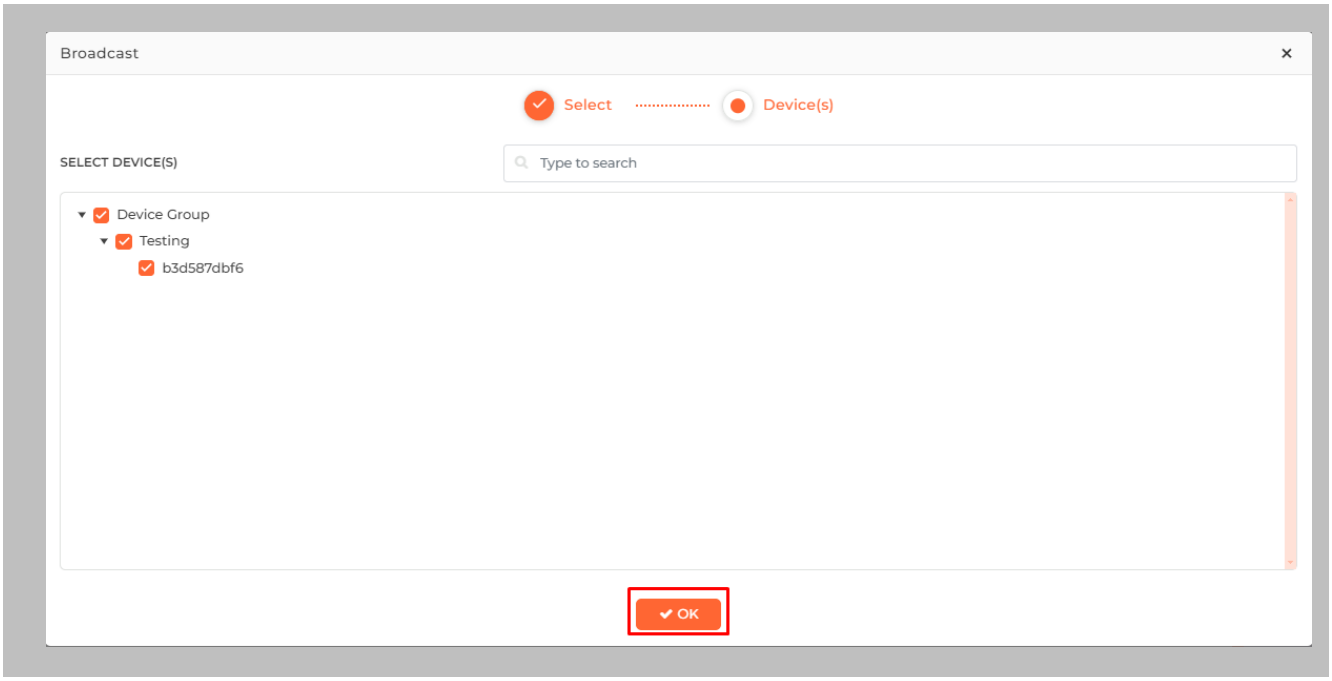


Figure 80: IXM WEB - Broadcast to Devices

Configuring for OSDP Connection

STEP 1

From the **Devices** tab. Select the required **Device** and navigate to **Access Control**. Click **OSDP**.

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

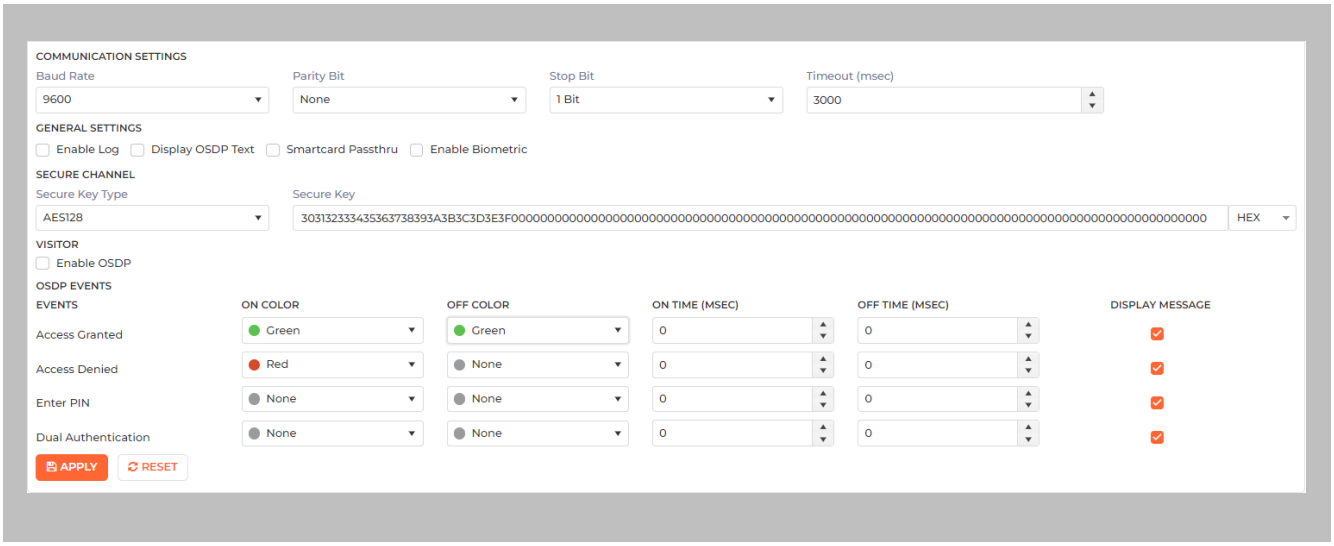


Figure 81: IXM WEB - OSDP Settings

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	The OSDP static events for panel feedback and capture pin are: Access Granted Access Denied Enter PIN Dual Authentication – It is an access mode that requires valid access by two authorized cardholders to enter an access zone within a specified time period. This feature is available only if the **Multi-User Authentication** feature is enabled and configured. To configure the Multi-User Authentication feature, from **Home**, click the **Devices** tab. Select the required Device and navigate to **General Settings**. Click on the **Multi-User Authentication** section. Upon enabling this feature, the following actions will be performed: • The Device will request the credentials of the second

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

Table 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	Notification on the device's screen. 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. If disable: Displays only the Access Control Panel notification.

Table 6: IXM WEB - OSDP Text Options

STEP 3

Click **Apply** to save the settings.

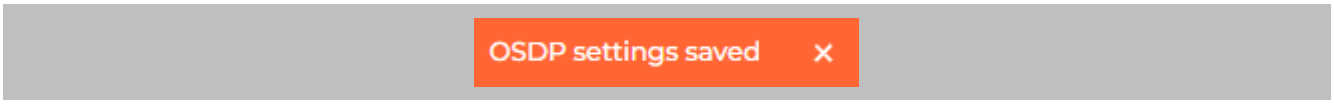


Figure 82: IXM WEB - Save OSDP Settings

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 Access It .

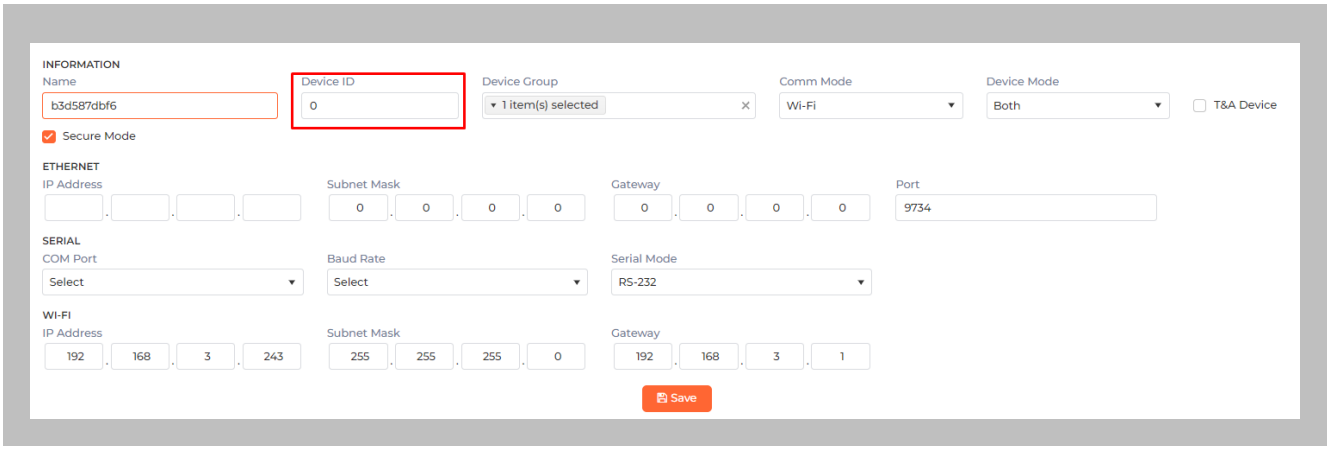


Figure 83: IXM WEB - Edit Device Options

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 Access It .

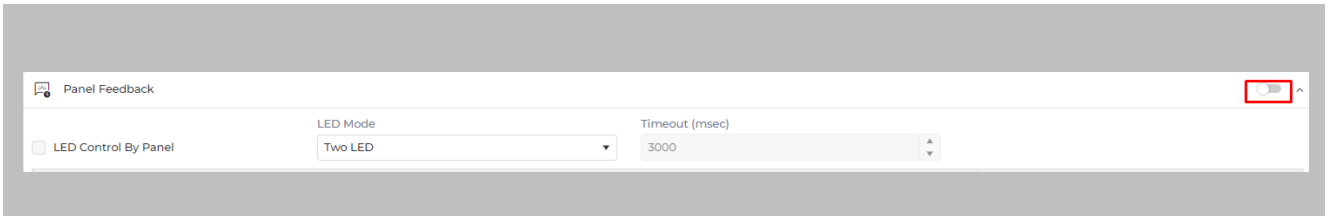


Figure 84: IXM WEB - Disable Panel Feedback

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.

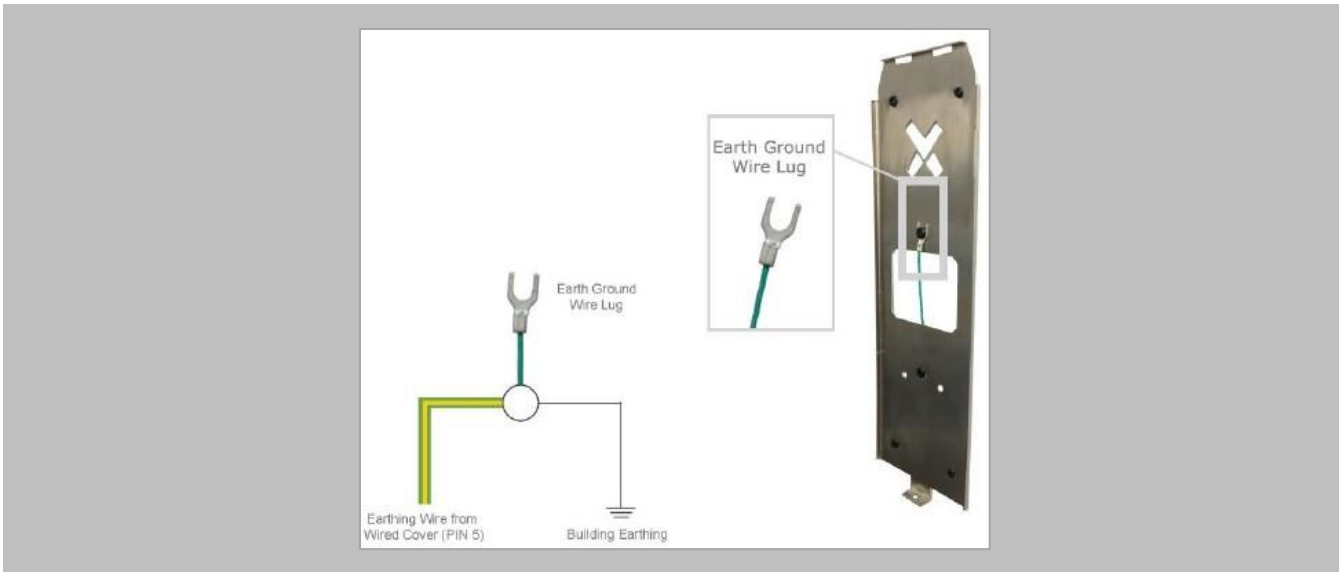


Figure 85: Earth Ground Wiring

Wiring

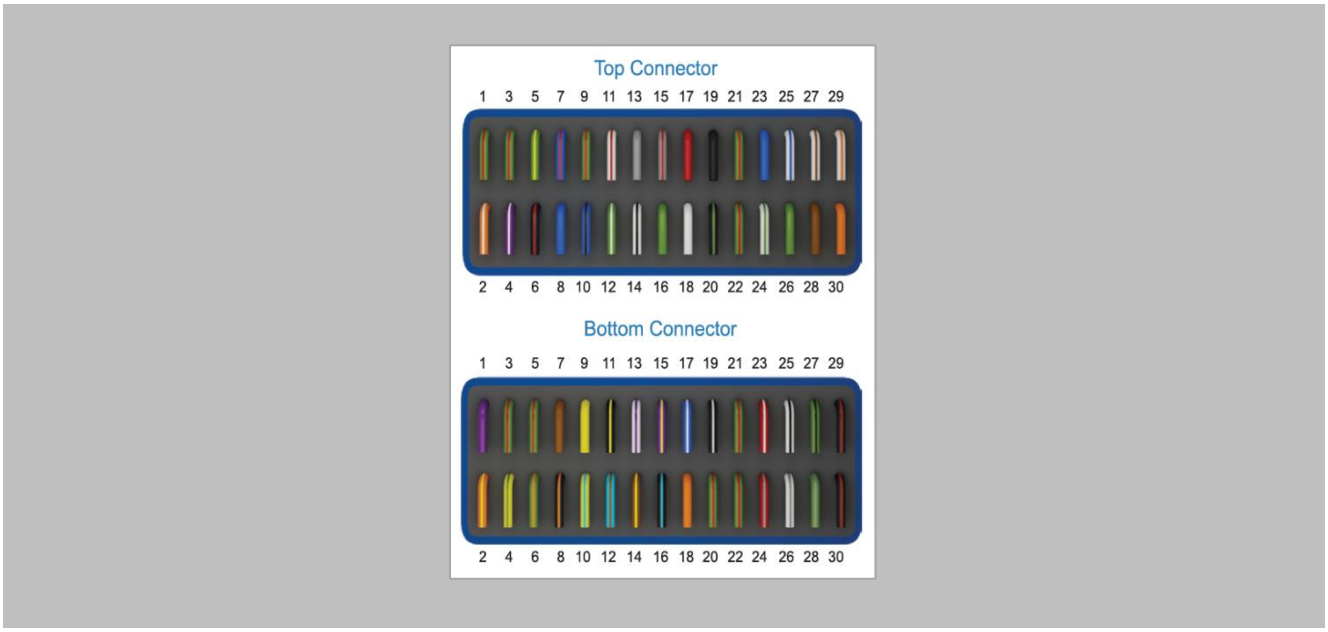
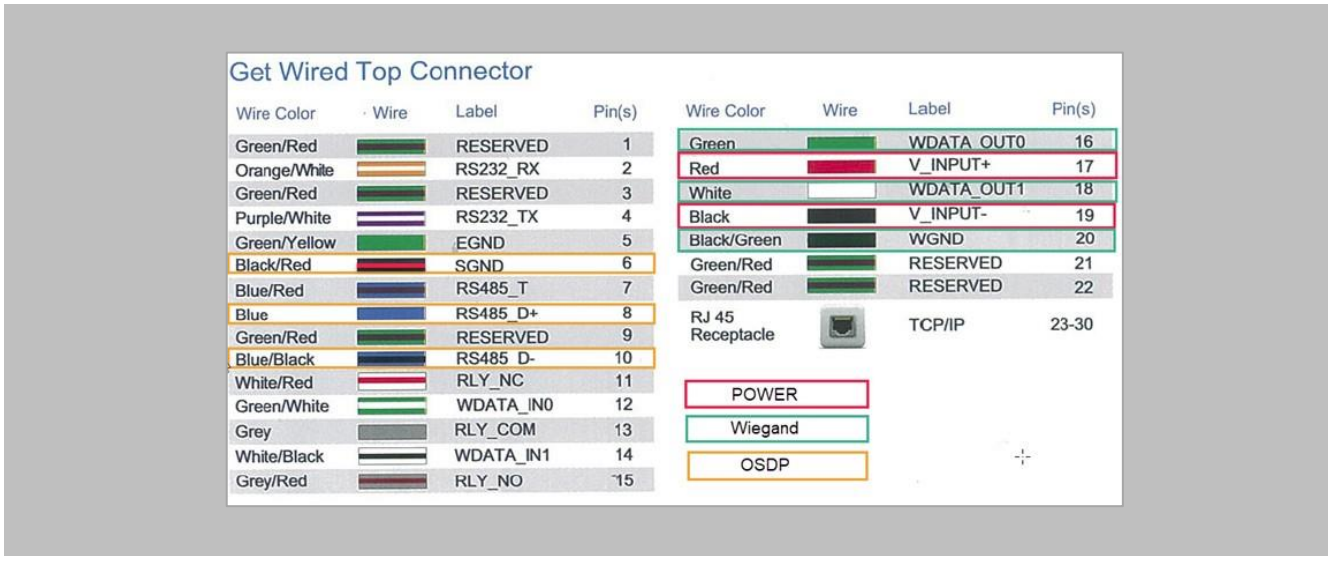


Figure 86: IXM TITAN – Top & Bottom Connector Wiring



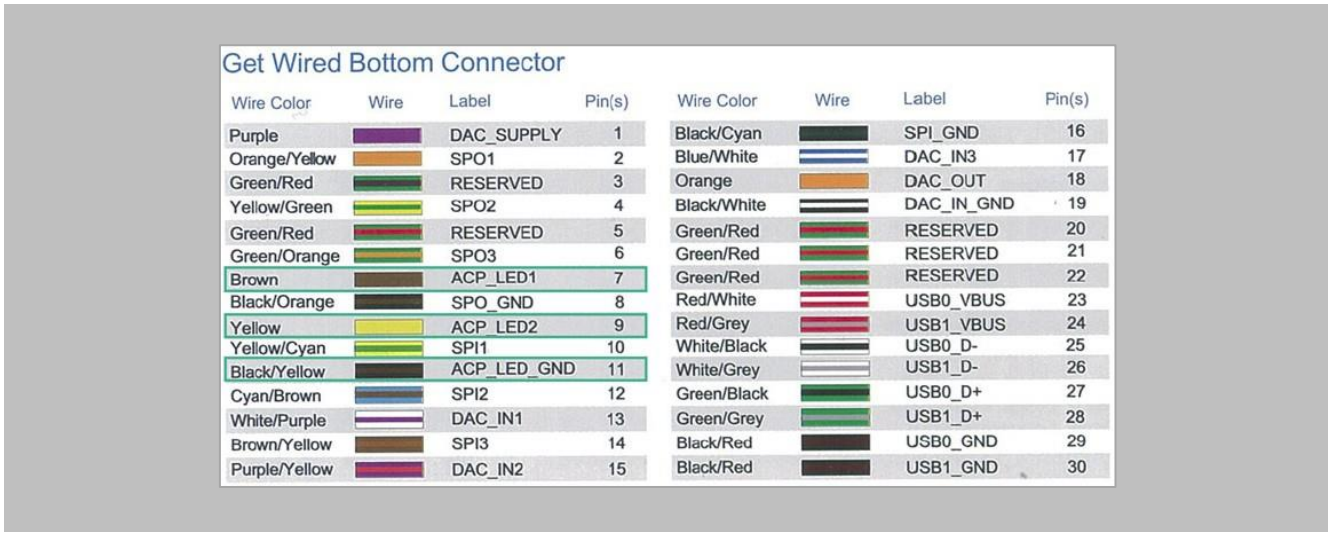


Figure 87: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand and OSDP.

Invixium devices can be integrated with ACRE Security Controller on:

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

Wiegand Connection

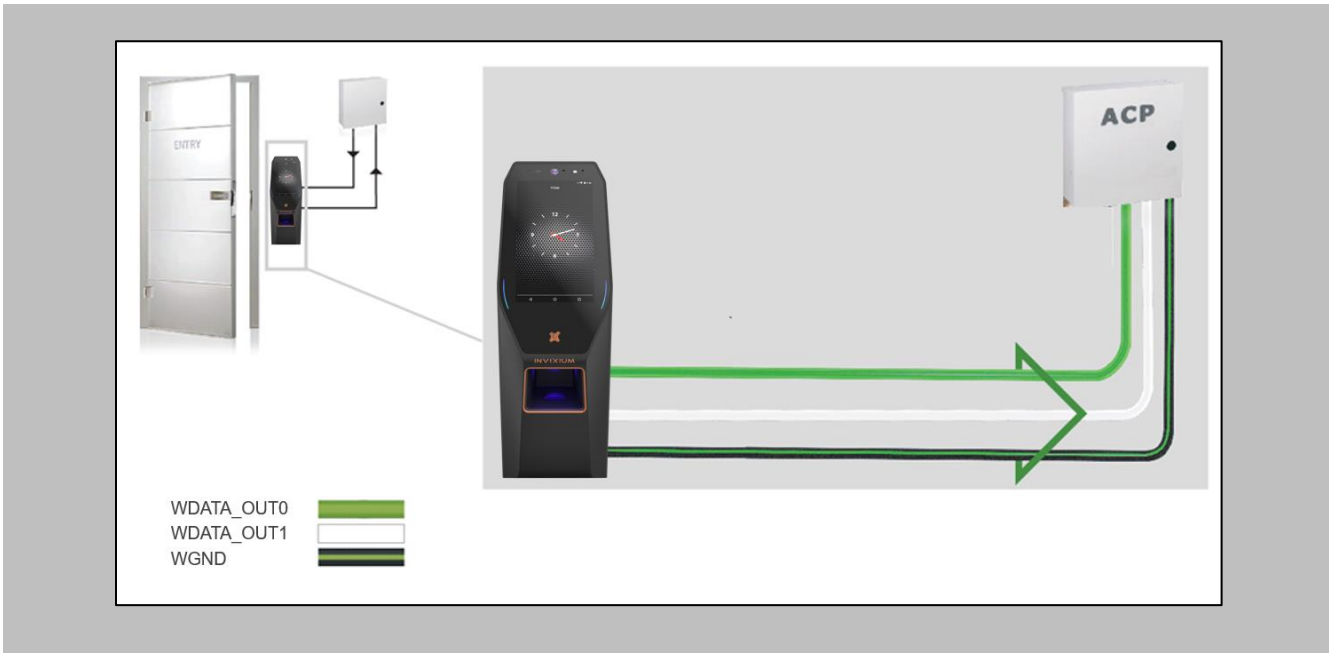


Figure 88: IXM TITAN - Wiegand

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

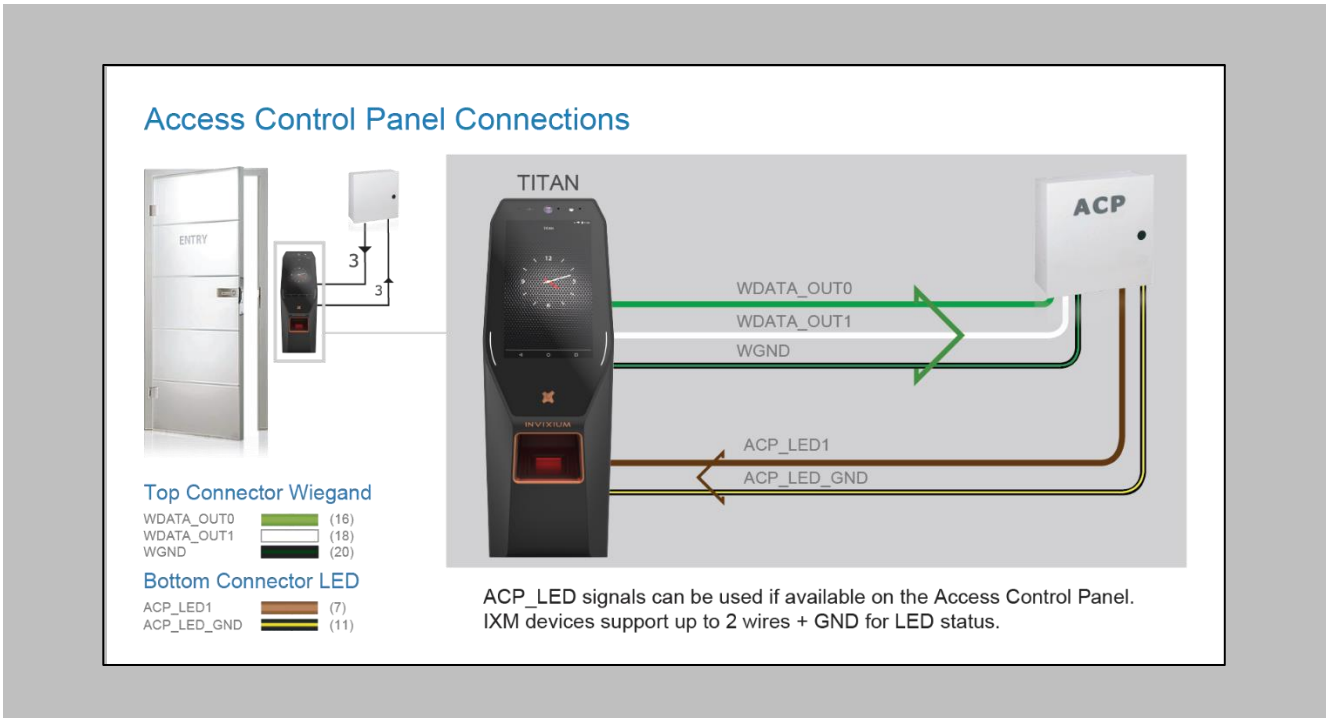


Figure 89: IXM TITAN - Panel Feedback

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

OSDP Connections

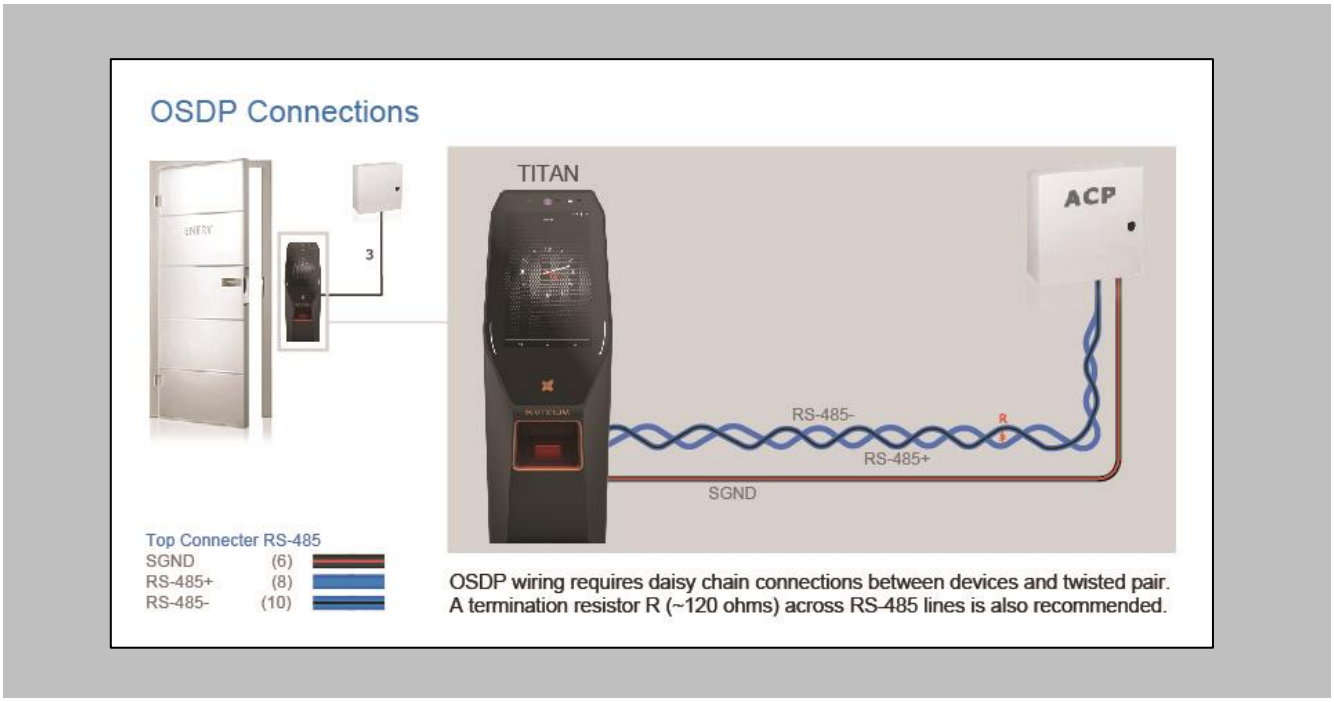


Figure 90: IXM TITAN - OSDP Connections

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 Invixium 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**.

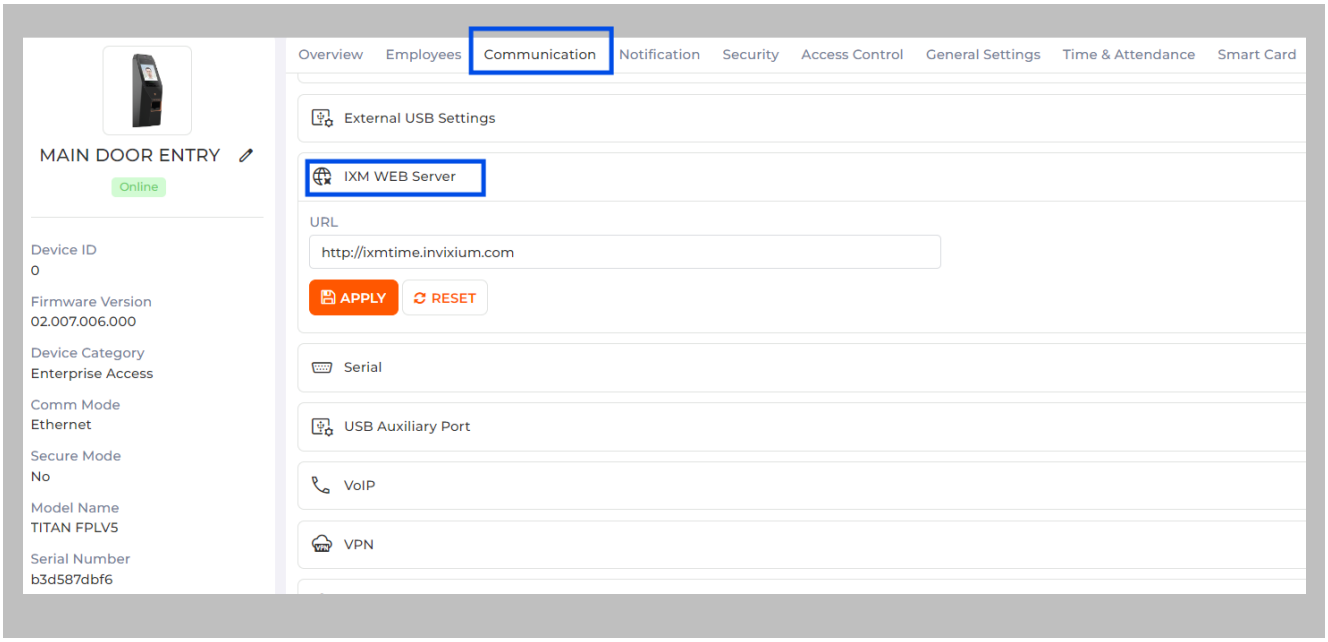


Figure 91: IXM WEB - Server URL Setting

STEP 3

Enter the **IP address** of the Invixium 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.

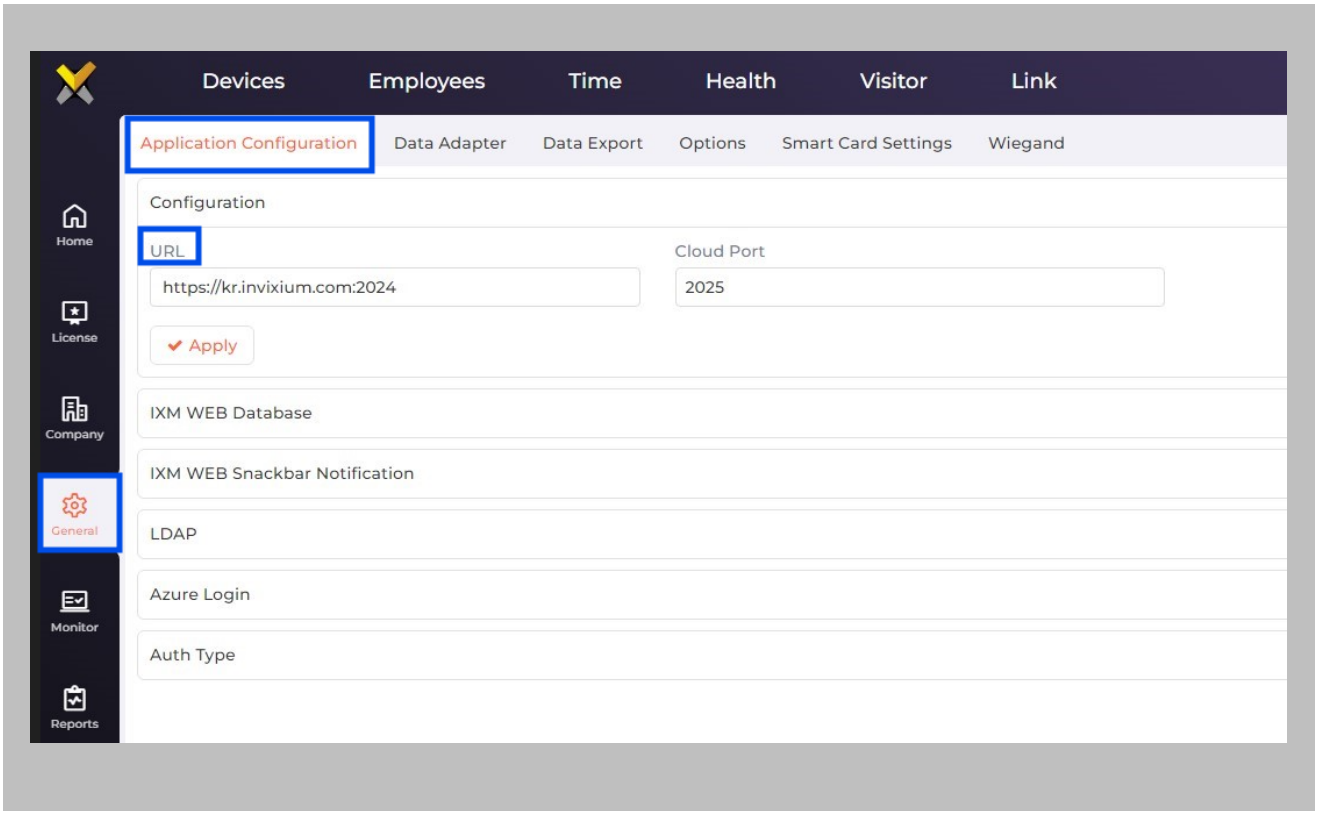


Figure 92: IXM WEB - Server URL Setting from General Settings

Elevated Body Temperature Denied Access but Granted Access in Access It

Procedure

STEP 1

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

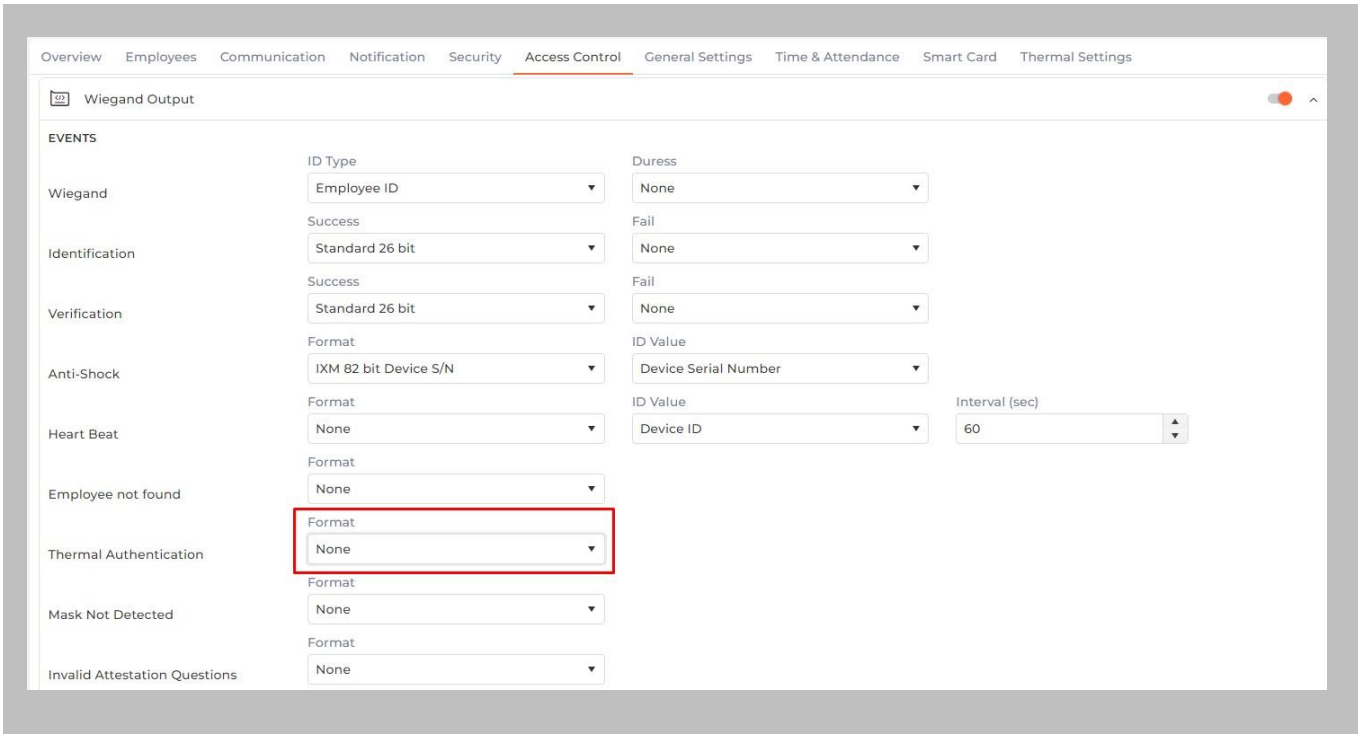


Figure 93: IXM WEB - Thermal Authentication Wiegand Output Event

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 94: IXM WEB - Enable Device Logs

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

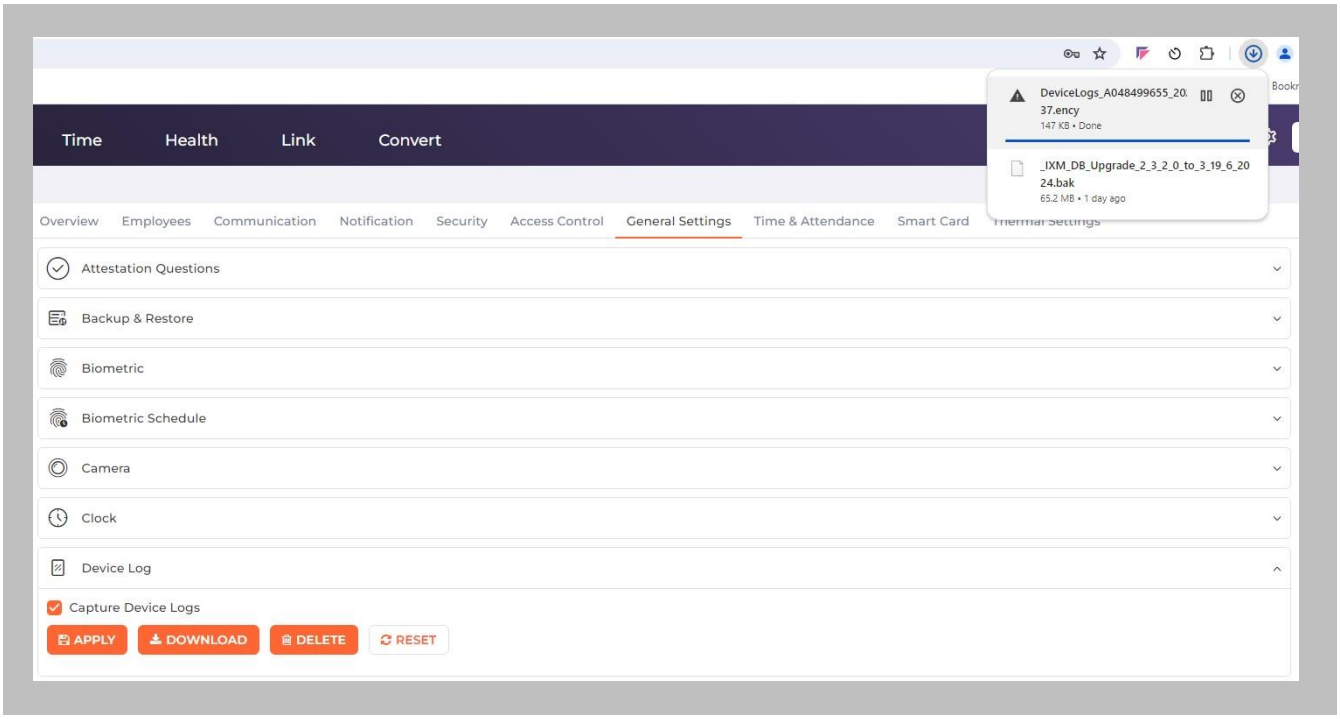


Figure 95: Save Device Log File

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 7: Logs Folder Location

Unable to connect to the Access It Server

Procedure

STEP 1

Note: Confirm module activation

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

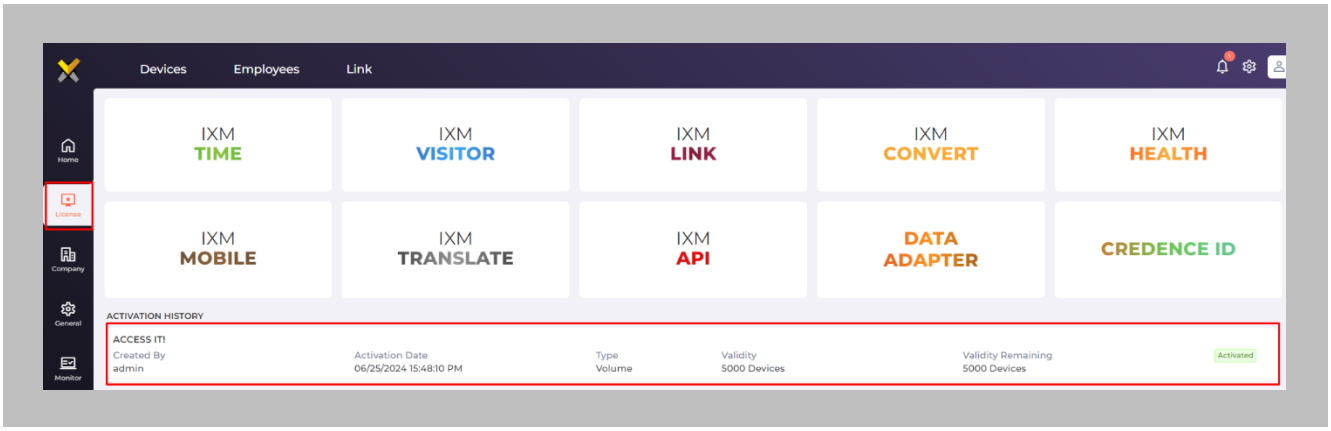


Figure 96: IXM WEB - Licence Module

STEP 2

Note: Confirm Access It API is up and running.

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

Figure 97: ACRE Security – Access It Web API

STEP 3

Note: Confirm WEB Service URL is enabled. Confirm parameters entered to connect to the ACRE Security server.

Ensure the correct **User** who is authorized to log into SQL Server to access the database is listed here. If not, **correct** and **apply.**

Ensure the correct **Password** of the user who is authorized to log into SQL Server to access the database 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.