IXM WEB Integration with Gallagher Command Centre

Installation Instructions

V2.0

P/N XAD-TPI-001-02G

Table of Contents

List of Figures

List of Tables

1. Introduction

Purpose

This document outlines the process of configuring the software integration between Gallagher Command Centre (GCC) and Invixium's IXM WEB.

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

- C12873Invixium license instead of REST API to support GCC integration
- Enrollment status PDF
- Temperature unit selection for sending alarm events to GCC
- 'Sync All' feature to resynchronize the database from GCC to IXM WEB
- MIFARE DESFire custom layout to support Gallagher 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 Gallagher Command Centre Software (where access rules for the users and the organization are managed).

Note: To activate IXM Link within IXM WEB, the installer must contact Invixium Support at support@invixium.com to obtain the activation key.

The following sections will describe how to set up and configure IXM Link to keep IXM WEB users in sync with Command Centre by using Gallagher Cardholder "REST API" to import and export cardholders.

Acronyms

Acronym	Description
API	Gallagher Cardholder REST API
ACPCS	Access Control Panel Configuration Software
GCC	Gallagher Command Centre
IXM	Invixium

Field Mappings

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

GCC Field	IXM Field	Notes
First name	First Name	
Last name	Last Name	
Division	Department	This is mandatory when adding or editing users from IXM WEB.
Authorized	Suspend Employee	
Number (CardholderCards Tile)	Number (Card)	This is mandatory when adding users to GCC from IXM WEB.
Issue (CardholderCards Tile)	Issue Level (Card)	This is mandatory when adding or editing users from IXM WEB. Max issue-level value supported by GCC is 15.
Card Type (CardholderCards Tile)	Card Type (Card)	This is mandatory when adding or editing users from IXM WEB. Not able to change card type while editing user from IXM WEB.
Facility Code(Card Type)	Facility Code (Card)	This will be disabled by default. When you select card type from IXM WEB, the Facility Code will populate automatically. From Card Type, only the Facility Code is imported to IXM WEB. Region Code is not imported from Card Type.
From	Activation Date (Card)	
Until	Expiry Date (Card)	
Status	Status (Card)	Active, Lost, and Stolen states are mapped with IXM WEB. Others will be inactive in IXM WEB. Not Yet Activated in GCC will display as active with future dates in IXM WEB.
Access Group	User Group / Device Group / 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 GCC 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 Invixium Customer Portal for details on Employee/Device/Sync Groups.

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

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**
Gallagher Command Centre	v8.60 (MR1)+
Invixium IXM WEB	2.2.252.0
Operating Systems	Windows 10 (Build 1709+) Professional Version Windows Server 2016 Standard Windows Server 2019 Supported but not recommended: (legacy) *Windows 8.1* *Windows Server 2012 R2* *Windows Server 2012*
Microsoft .NET Framework	.NET Framework 4.7.2
Database Engine	SQL Server 2016+ Supported but not recommended: (legacy) SQL server 2014 Express Edition (Default Installation)
Internet Information Services (IIS)	Microsoft® Internet Information Services version 7.5 or higher
Web Browser	Google Chrome Mozilla Firefox Microsoft Edge (Internet Explorer not recommended)

Other Requirements

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

Note: Server requirements mentioned are ideal for 10-15 devices registered with 500 employees or fewer. For large enterprise installation server requirements, contact support@invixium.com.

Compatibility Matrix for IXM WEB & Command Centre Integration

IXM WEB version	Command Centre version	Compatible
IXM WEB 2.2.57.0	v8.40	Yes
IXM WEB 2.2.57.0	v8.50	Yes
IXM WEB 2.2.224.0	v8.40	No
IXM WEB 2.2.224.0	v8.50	No
IXM WEB 2.2.224.0	v8.50 (with patch*)	Yes
IXM WEB 2.2.224.0	v8.60	Yes
IXM WEB 2.2.230.0	v8.60	Yes
IXM WEB 2.2.252.0	v8.60	Yes

Table 1: Compatibility Matrix for IXM WEB & Gallagher Integration

3. Checklist

Item List	Interface
URL Enrollment PDF and Access Group	Gallagher
REST API Client	Gallagher
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 Gallagher	Invixium
Configure Invixium Reader	Invixium
Configure Logical Events	Gallagher
Face or Finger Enrollment	Invixium

4. Task List Summary

Task	IXM WEB Application Task List using IXM WEB	Gallagher Command Centre Task List using GCC
1	Activate IXM WEB and IXM Link for GCC	Create Cardholder. Assign Card and Access Group to cardholder
2	Configure IXM Link for GCC	Define Enrollment URL PDF and create custom Enrollment viewer
3	Register IXM Devices and configure settings as per the requirement	Enroll cardholder biometric (Face, fingerprint, finger vein)
4	Configure Weigand or OSDP settings in device for integration with Gallagher Controller 6000	Create External Events for Temperature and Mask Event using Gallagher External Event Type Configuration Utility
5	Assign a specific Device Group to the device	Define Reader and Door in GCC for integration with Controller 6000 on Weigand or OSD
6		Create Event and Response for associated Temperature and Mask Events
7		Monitor Events and Generate Report

Table 2: Task List Summary

5. Prerequisites for GCC and IXM WEB Integration

URL Enrollment PDF (Personal Data Field)

Procedure

Configure a **Personal Data Field (PDF)** for URL Enrollment in Configuration Client in Command Centre.

STEP 1

From Configuration Client, create a new **Personal Data Field.**

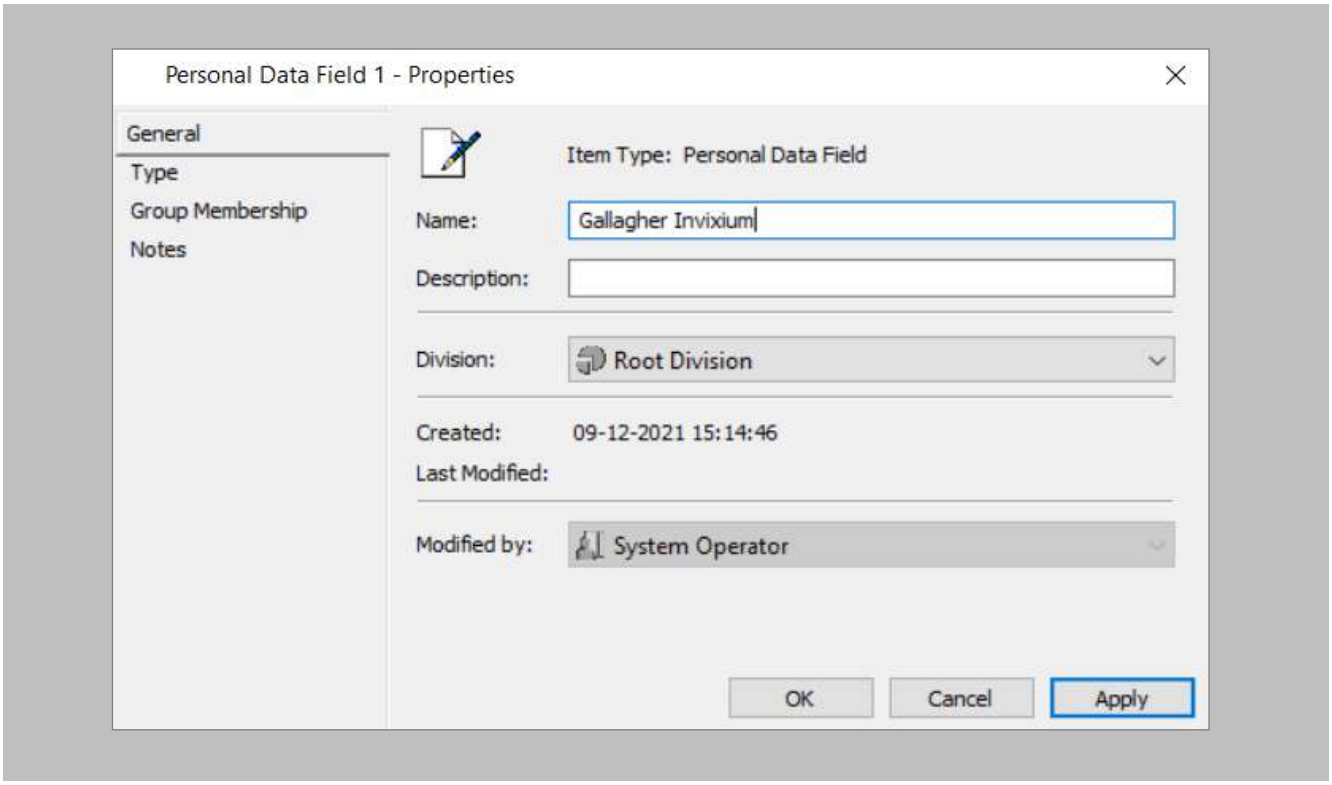


Figure 1: GCC - Personal Data Field 1 Properties

STEP 2

Enter a **Name** and **Description** (optional).

STEP 3

In the **Type** tab, set the **Data Type** to **Text.**

STEP 4

Enter the Enrollment URL link in the **Default Value** field.

http://[IXM WEB Server IP:Port]/Link/EnrollGallagherUser/

For example:

If the IXM WEB Server IP address is 192.168.1.100 and running on default port:9108, then specify URL for Default Value as the following:

http://192.168.1.100:9108/Link/EnrollGallagherUser/

Enable the **Required Field** checkbox.

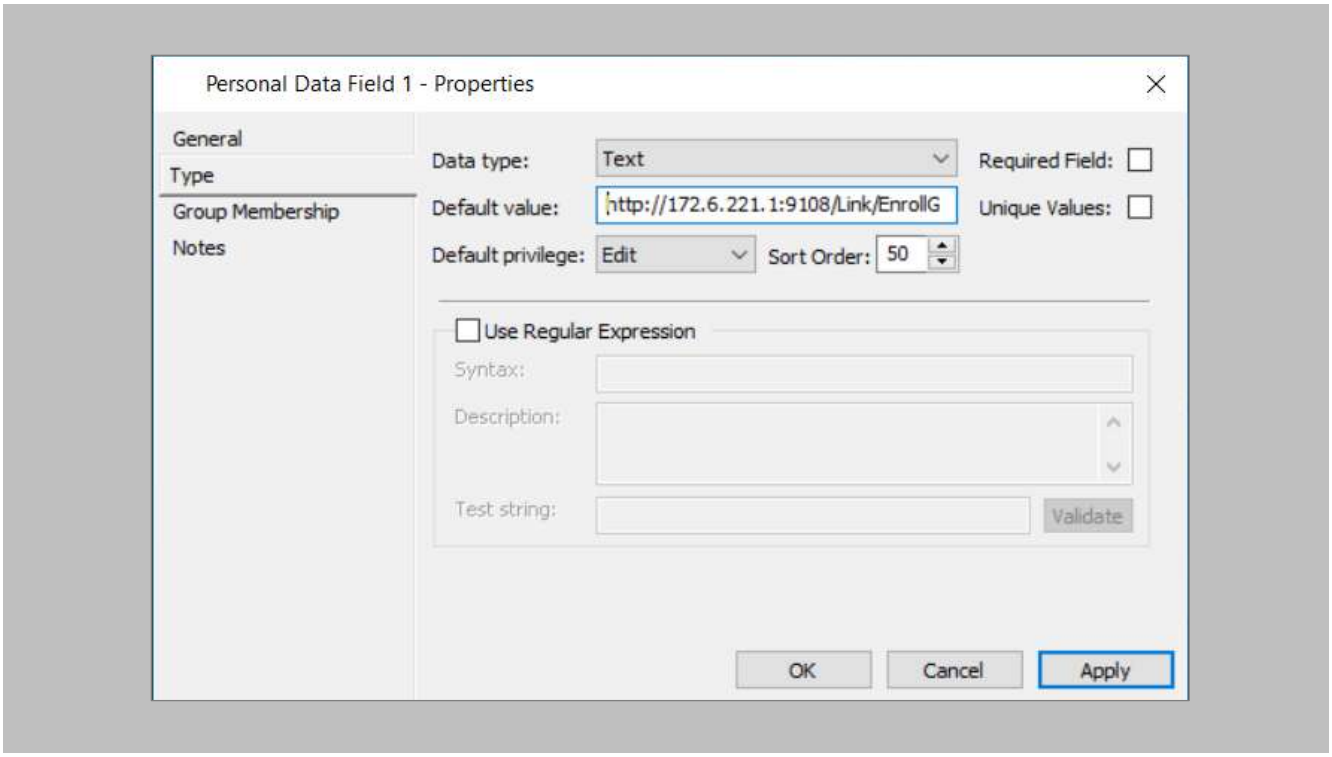


Figure 2: GCC - Gallagher Invixium Properties

STEP 5

Click **OK.**

STEP 6

Create a **Cardholder Access Group** and assign the URL Enrollment PDF.

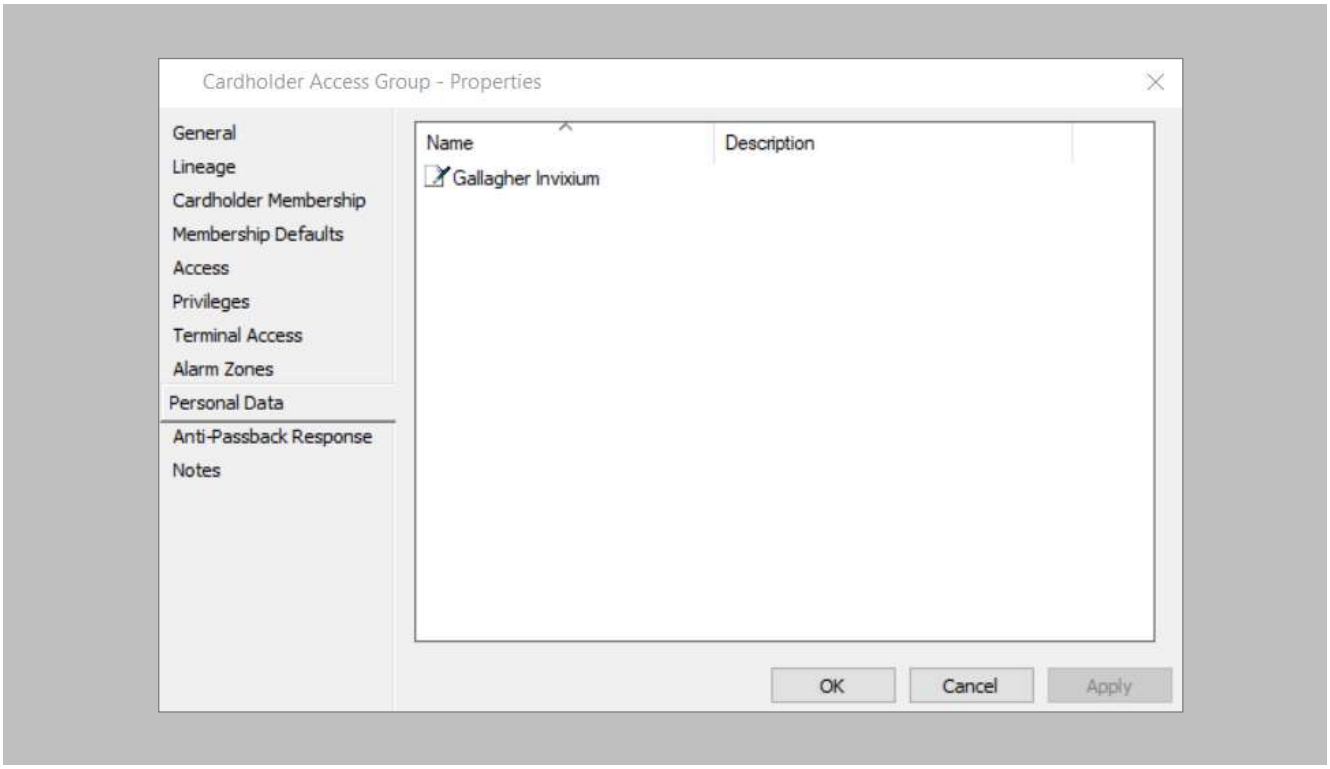


Figure 3: GCC - Cardholder Access Group Properties

STEP 7

Click **OK.**

Enrollment Status PDF (Personal Data Field)

Configure **Personal Data Field (PDF)** for Enrollment status in the Configuration Client in Command Centre.

Procedure

STEP 1

From Configuration Client, create a new **Personal Data Field.**

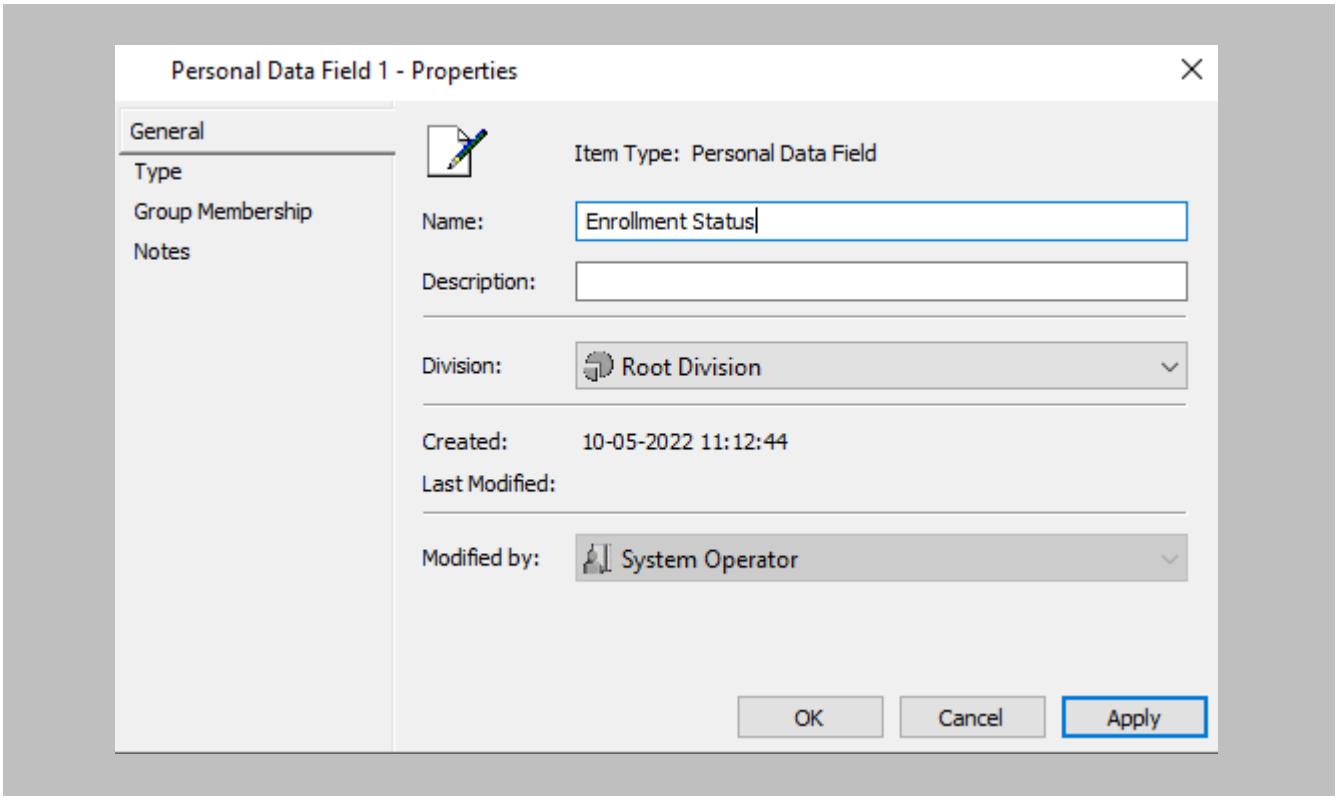


Figure 4: GCC - Personal Data Field 1 Properties – Enrollment Status

STEP 2

Enter a **Name** and **Description** (optional).

STEP 3

In the **Type** tab, set the **Data Type** to **Text.**

STEP 4

Enter NO in the **Default Value** field.

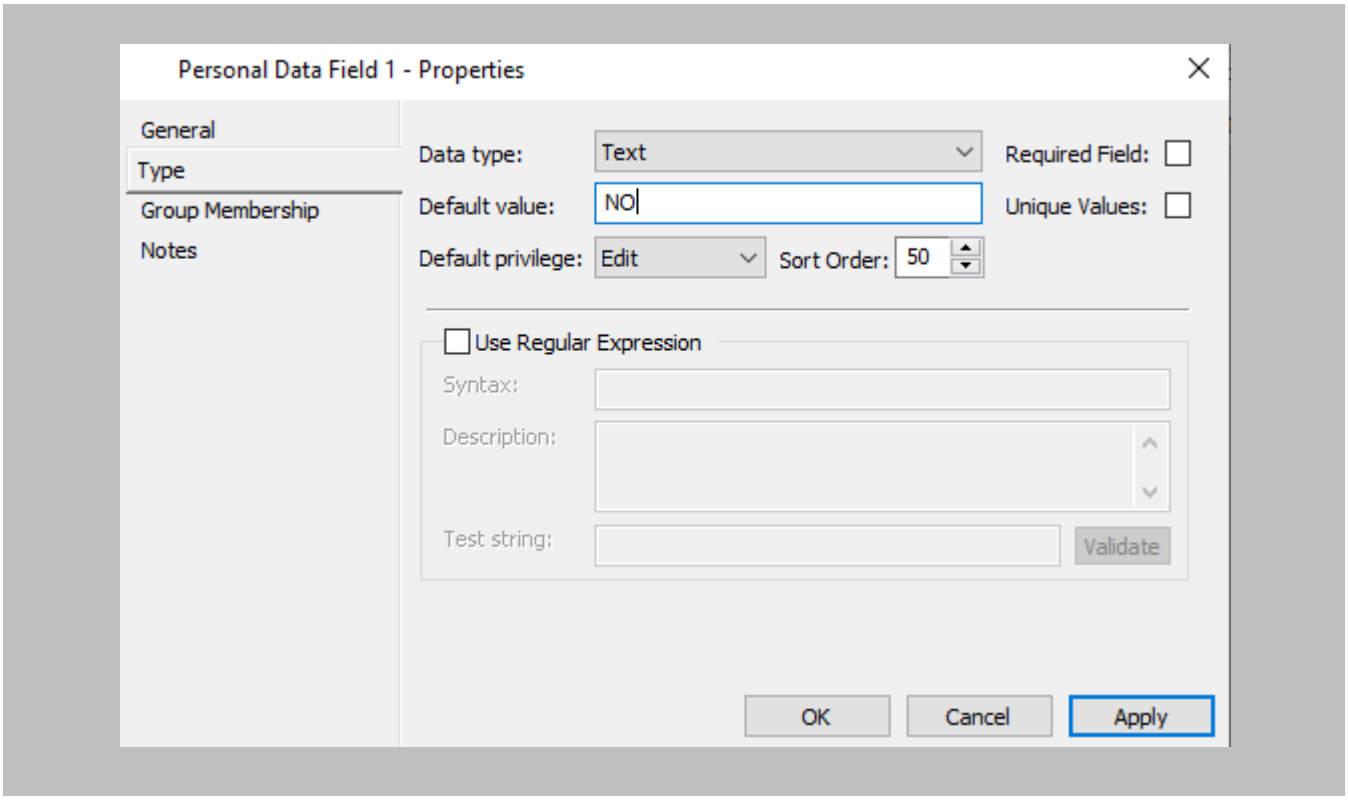


Figure 5: GCC – Enrollment Status Properties

STEP 5

Click **OK.**

STEP 6

Create a **Cardholder Access Group** and assign the Enrollment Status PDF.

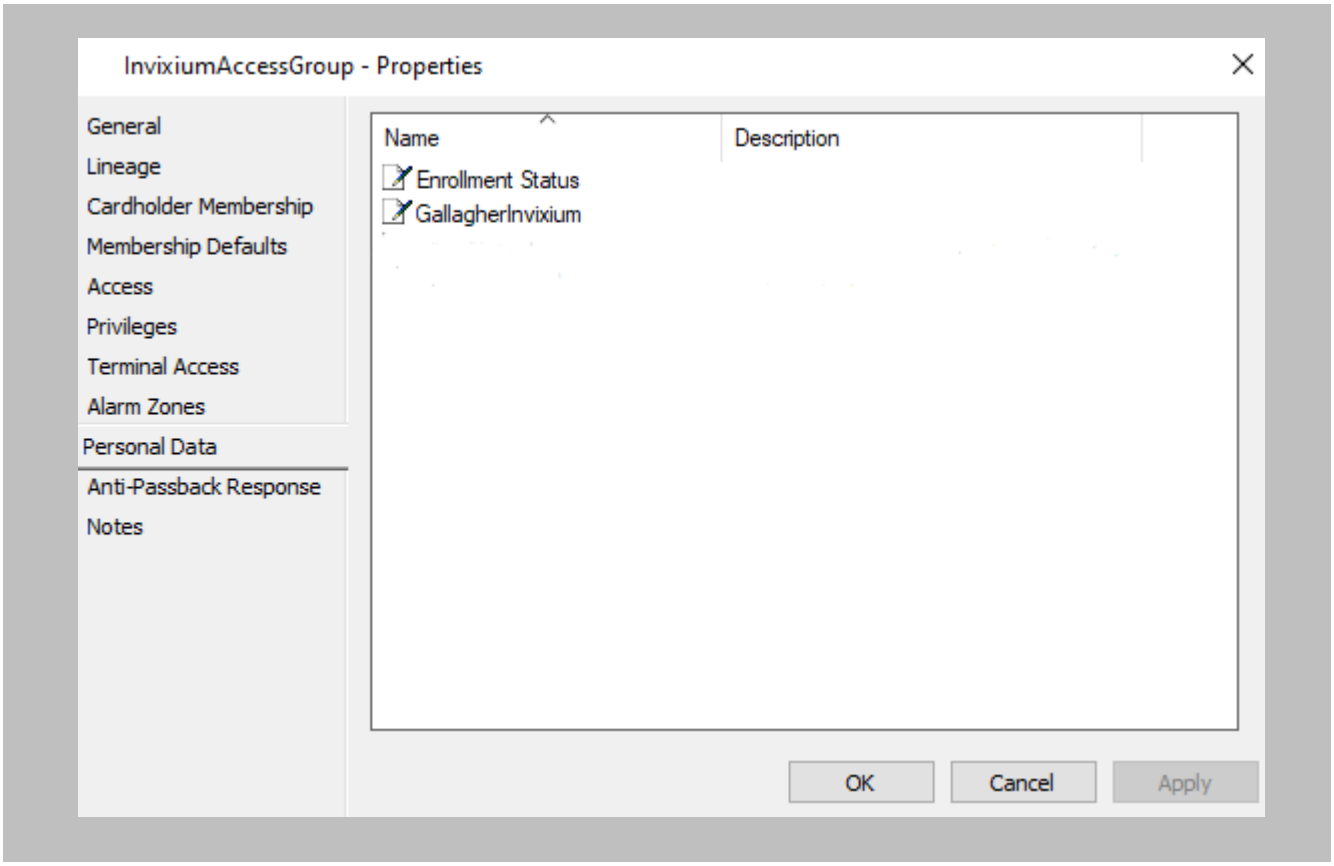


Figure 6: GCC - Cardholder Access Group Properties

STEP 7

Click **OK.**

Cardholder Access Group

Cardholders belonging to the access group created below will be allowed to use the reader for door access.

Procedure

STEP 1

Create an **Access Group** to assign Invixium Readers.

STEP 2

From the Configuration Client, create an **Access Group**.

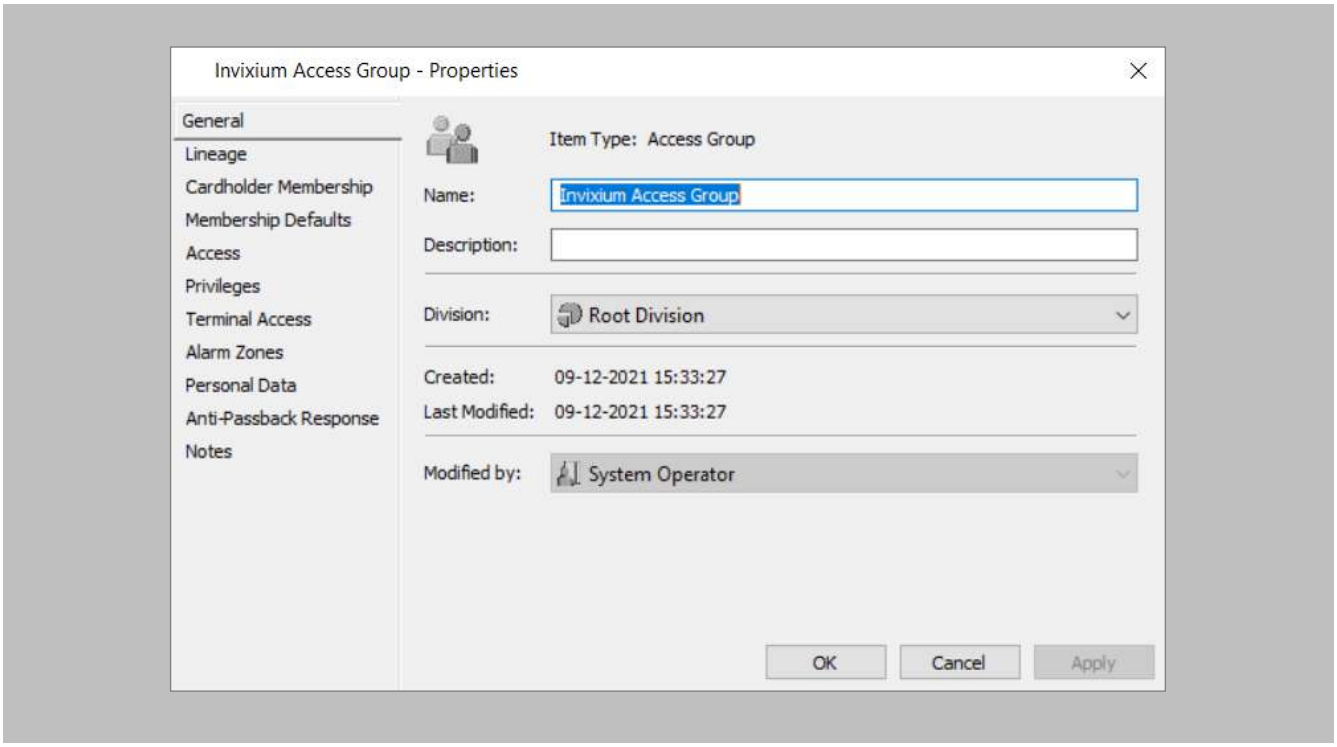


Figure 7: GCC - Invixium Access Group Properties

STEP 3

Click **OK.**

Note: You need to have at least one user assigned within this access group to make it selectable.

Enabling the Invixium License for IXM WEB in Command Centre

What you will need:

- **C12873Invixium**
- REST API String

Note: C12873 is the Gallagher License required for integration with IXM WEB v2.2.224.0 onwards.

Contact your local Gallagher Team/Sales to obtain a CommandCentre.lic file inclusive of the IXM WEB integration license.

Procedure

STEP 1

Go to the Licensing tab in CC. Click on **Select New License File** to upload the CommandCentre.lic file.

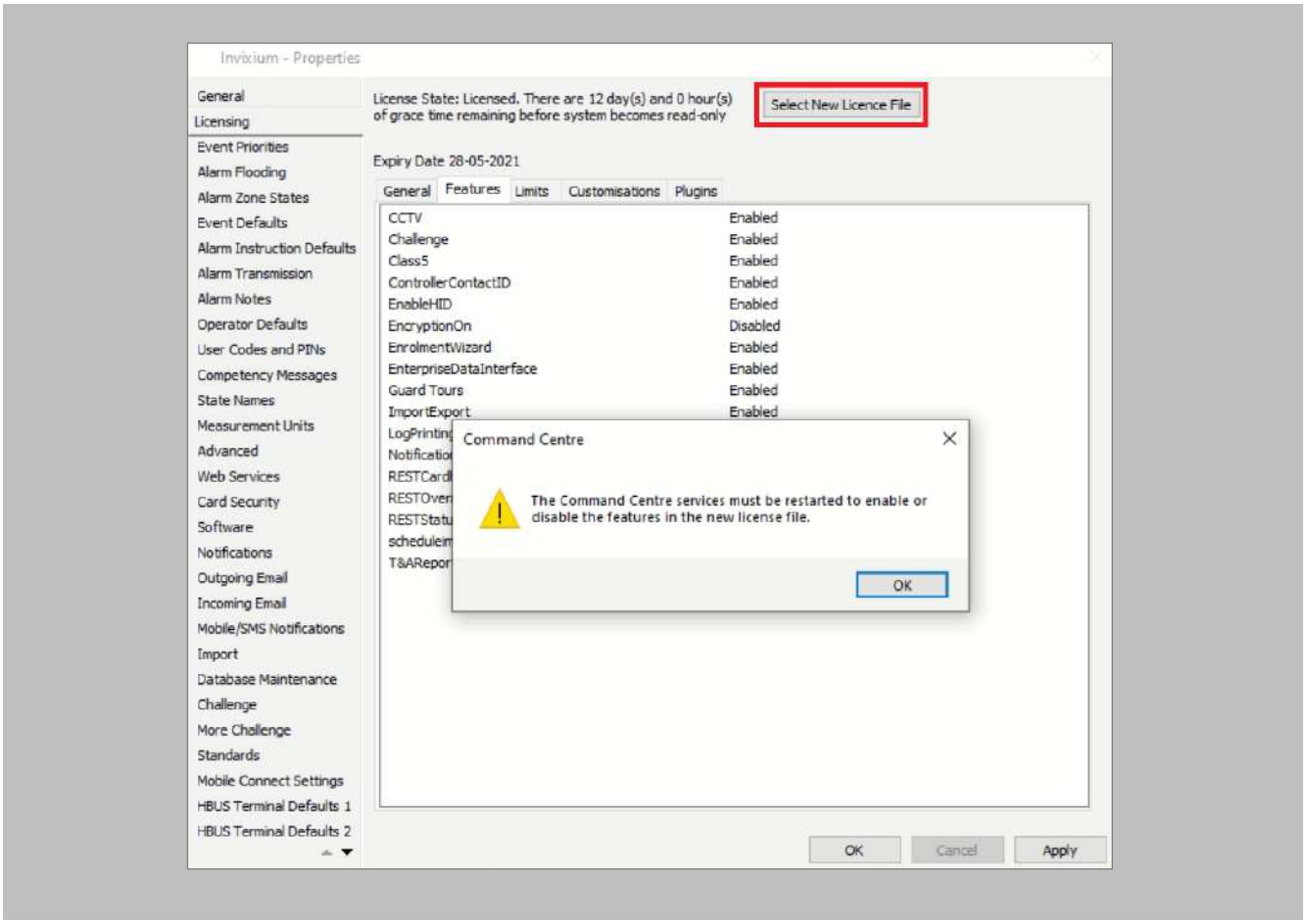


Figure 8: GCC – Invixium License for IXM WEB

STEP 2

Restart all GCC-related services (i.e. services starting with “FT”) to enable the IXM WEB integration.

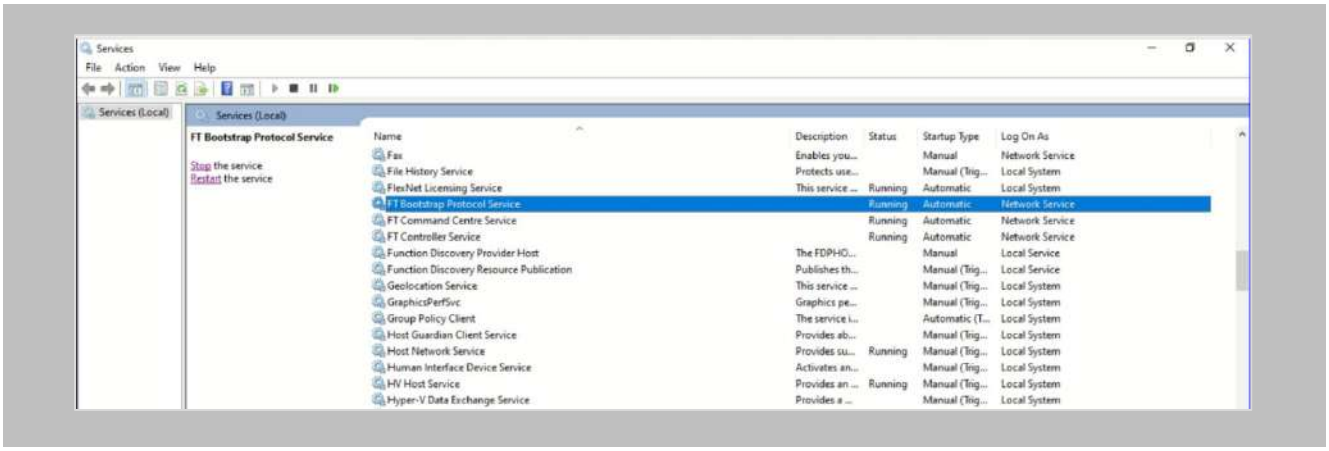


Figure 9: GCC - Restart GCC Services

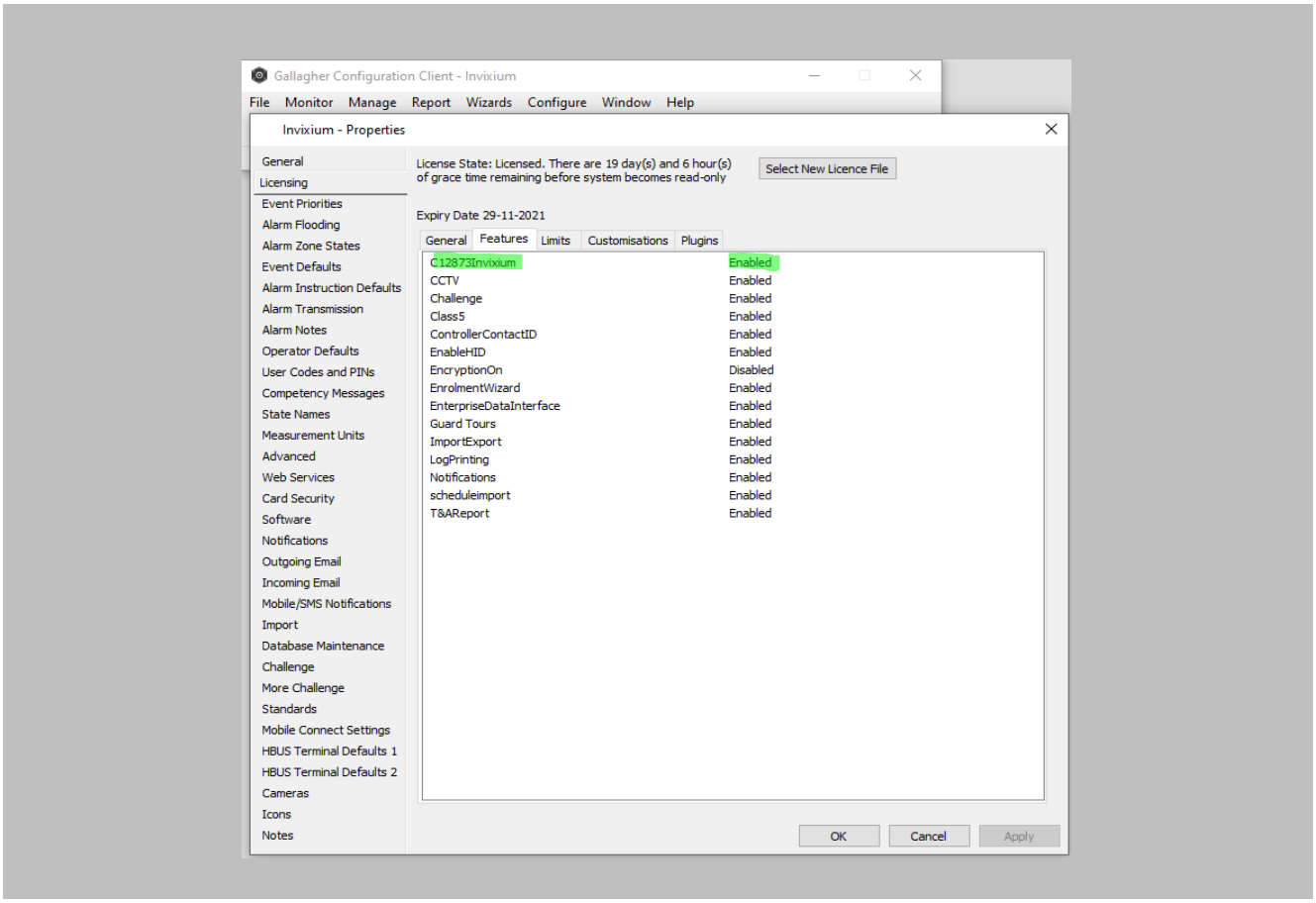


Figure 10: GCC – C12873Invixium License Enabled

REST API Client

Setup of the REST Client within Command Centre is configured through the Services and Workstations window from within the Configuration menu.

For setup instructions, refer to the REST API help file within Command Centre.

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/.

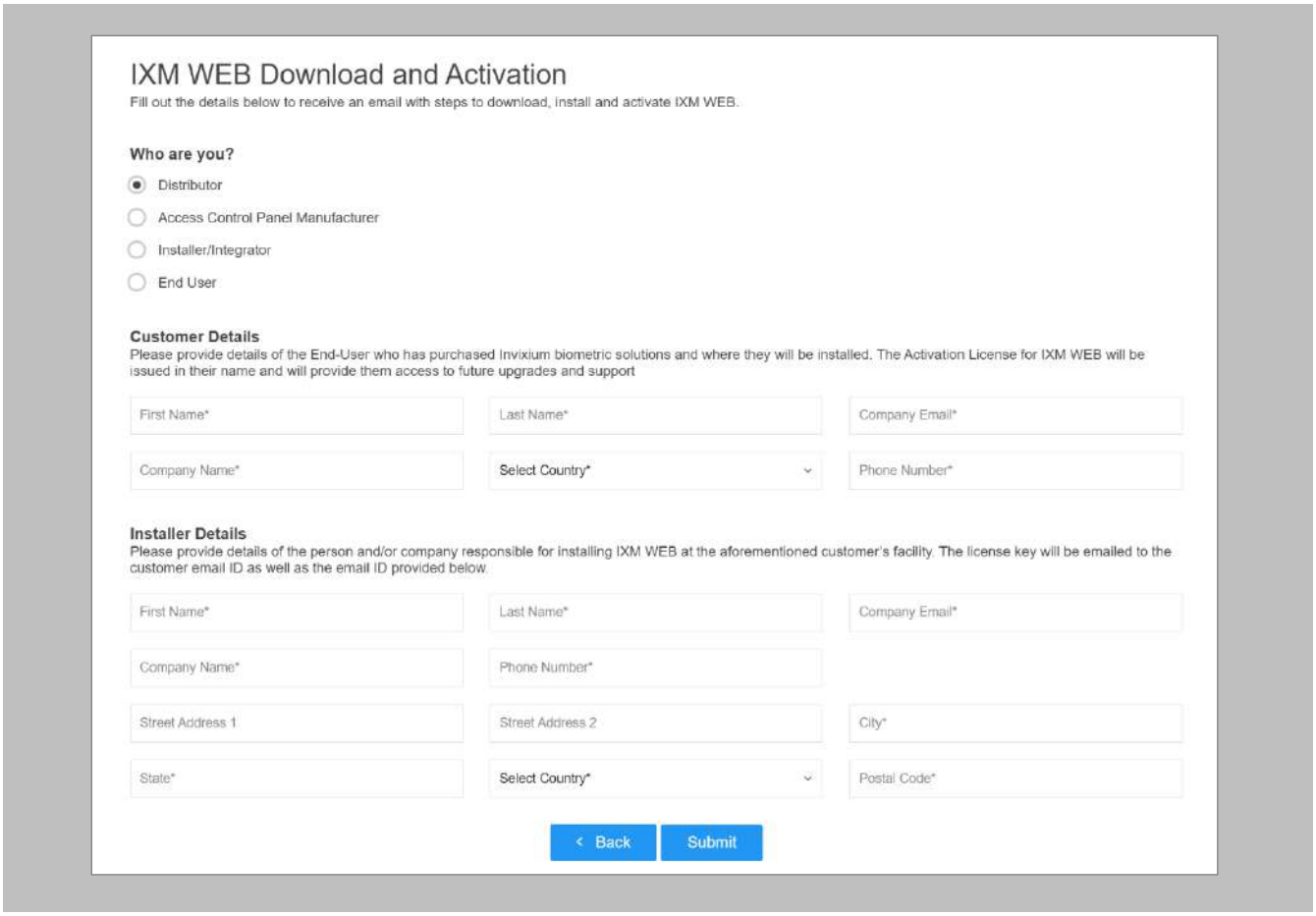
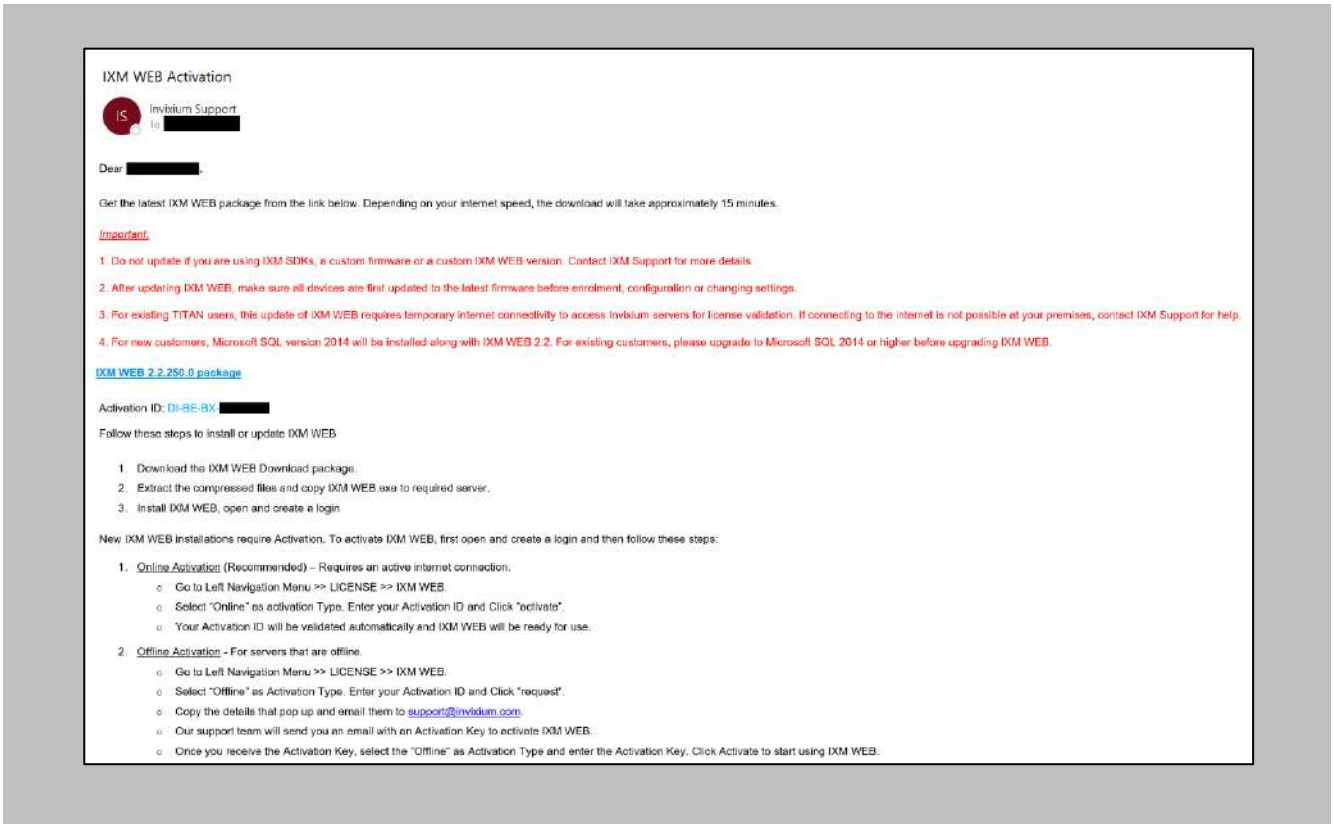


Figure 11: IXM WEB Online Request Form

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.



IXM WEB Activation

IS Invixium Support
to [redacted]

Dear [redacted],

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

Important:

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

IXM WEB 2.2.250.0 package

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

Follow these steps to install or update IXM WEB:

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

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

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

Figure 12: 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.

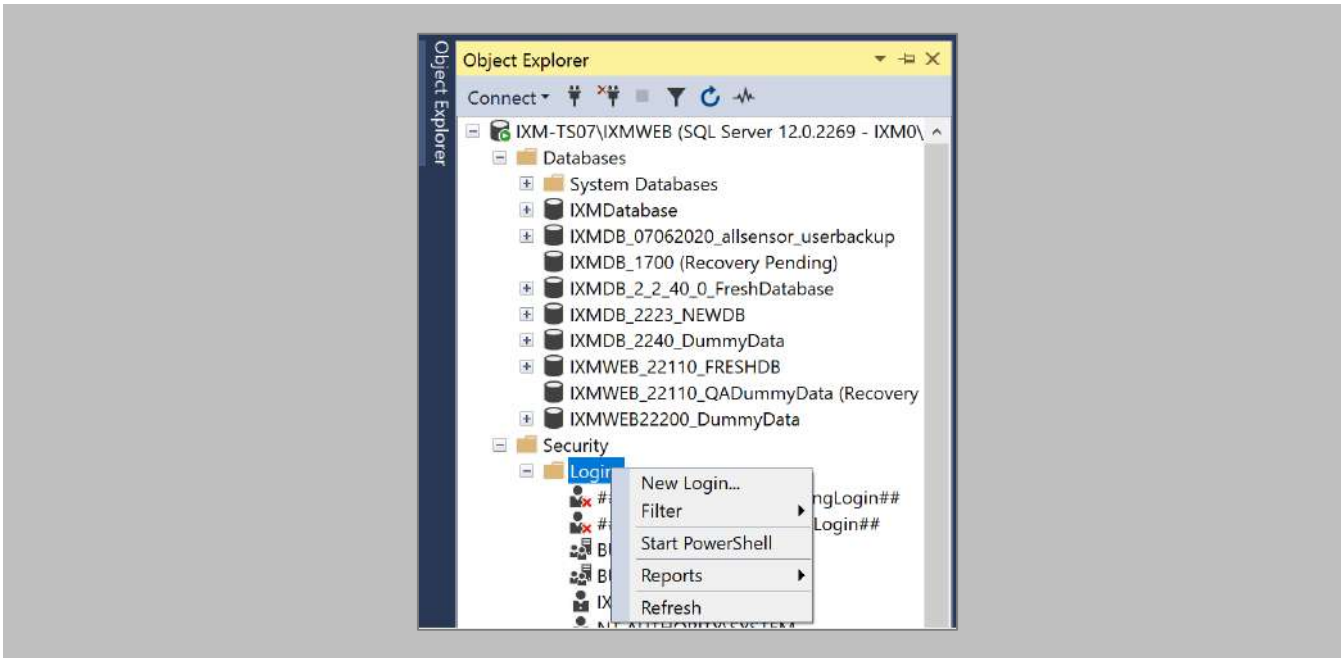


Figure 13: SQL New Login

STEP 6

Select **SQL Server authentication.**

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

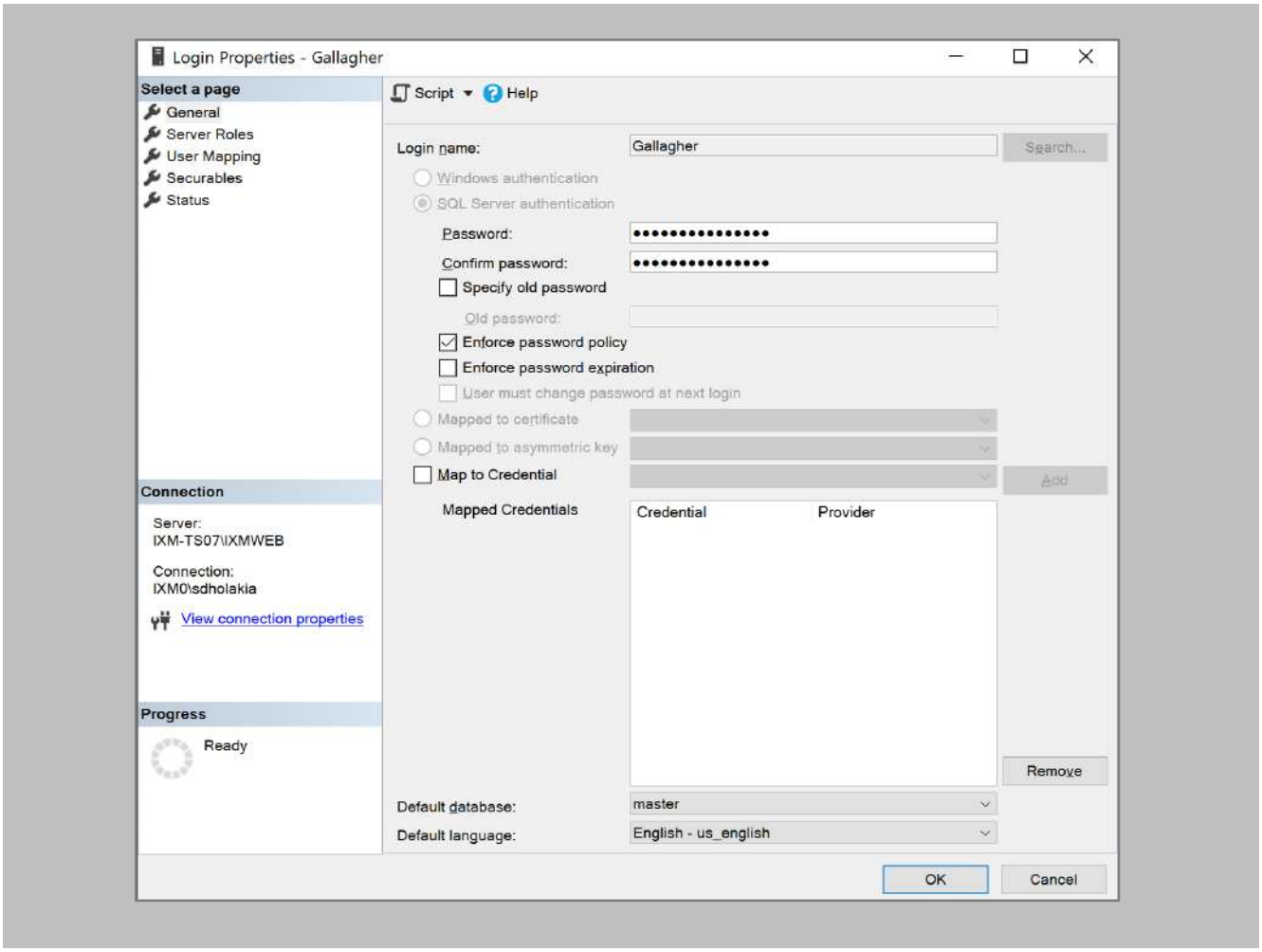


Figure 14: SQL Login Properties

STEP 7

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

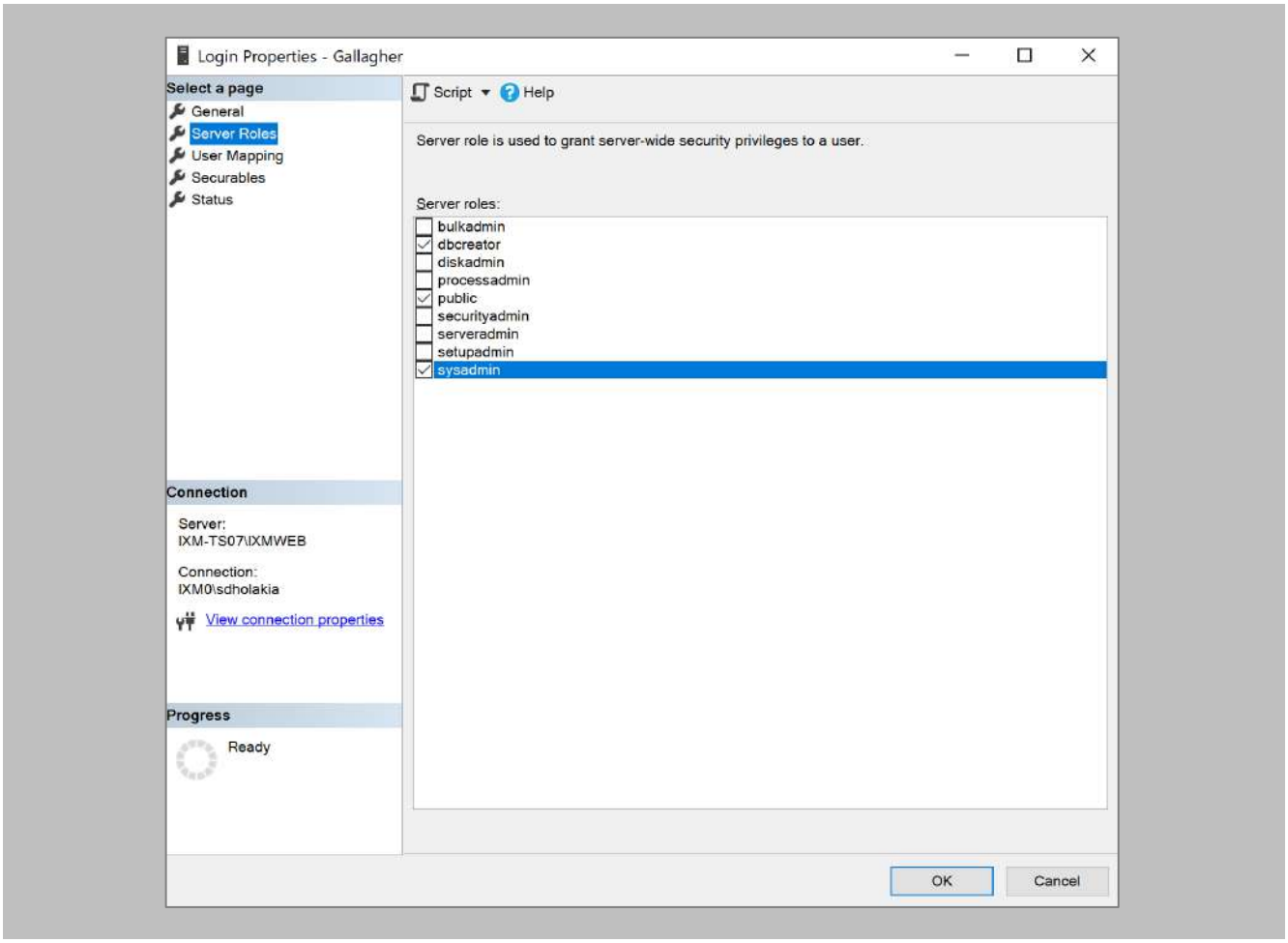


Figure 15: SQL Server Roles

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
GCC REST API Port	8904 (default)

Table 4: Port Information

7. Installing IXM WEB

Software Install

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator).

Select **Advanced.**

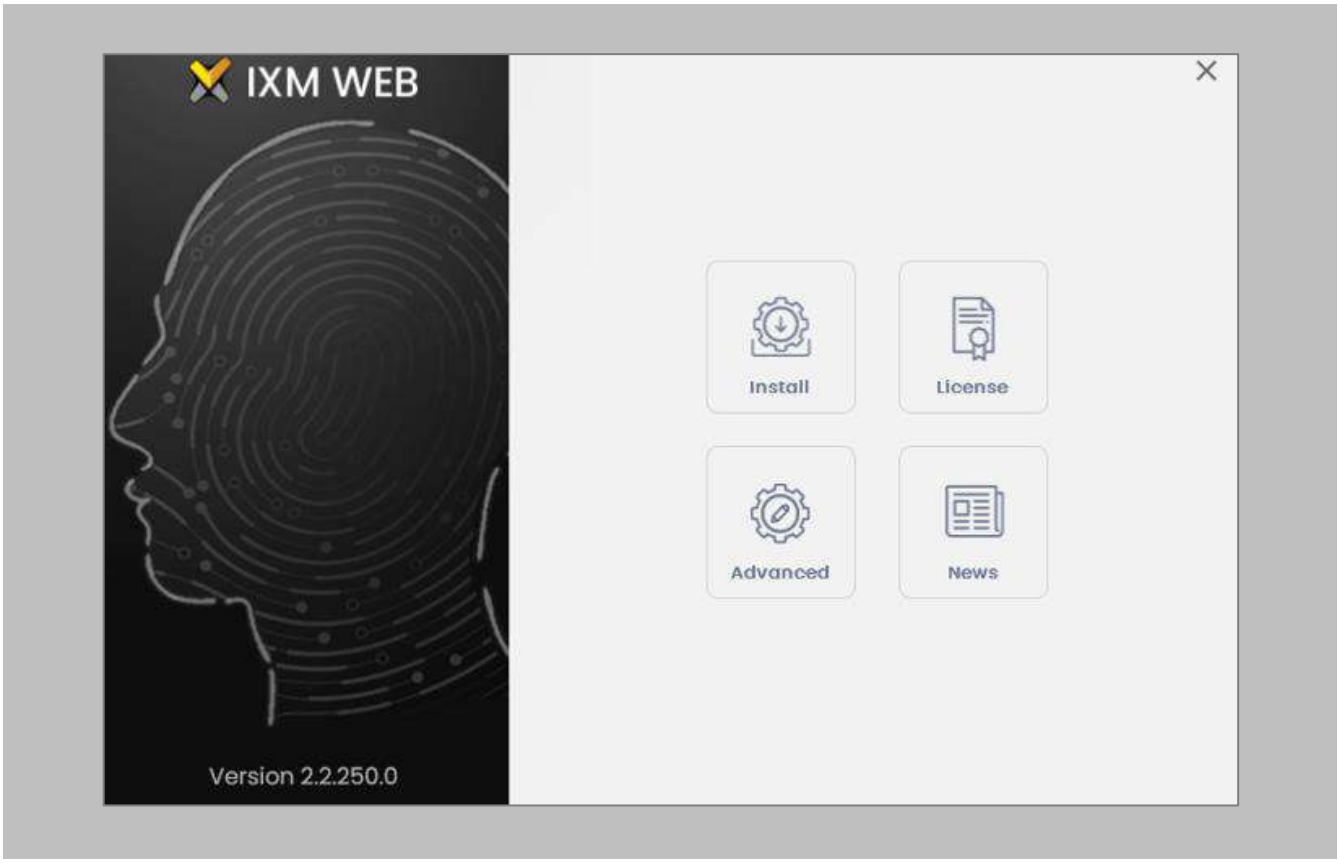


Figure 16: IXM WEB Installer

STEP 2

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

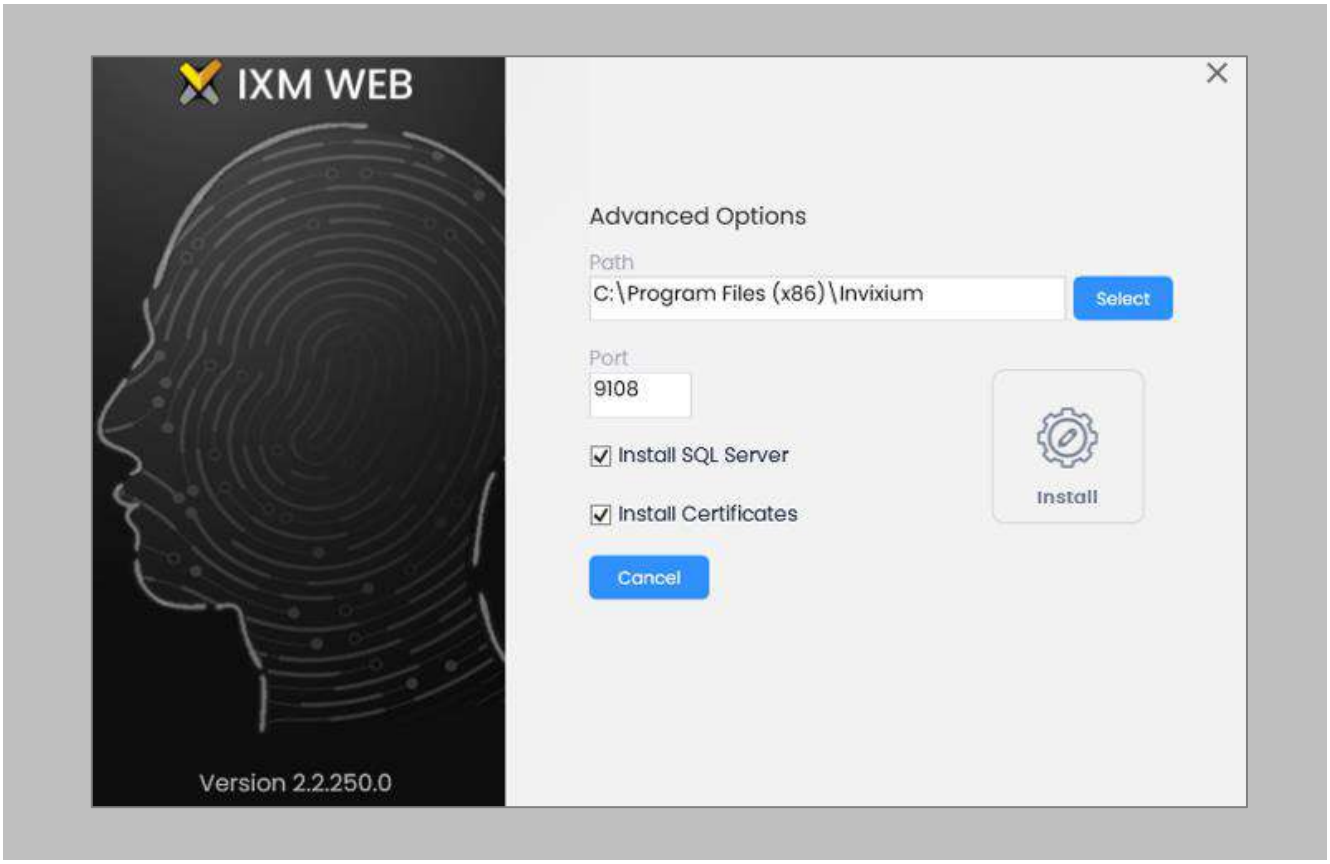


Figure 17: Advanced Options in IXM WEB Installer

STEP 3

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

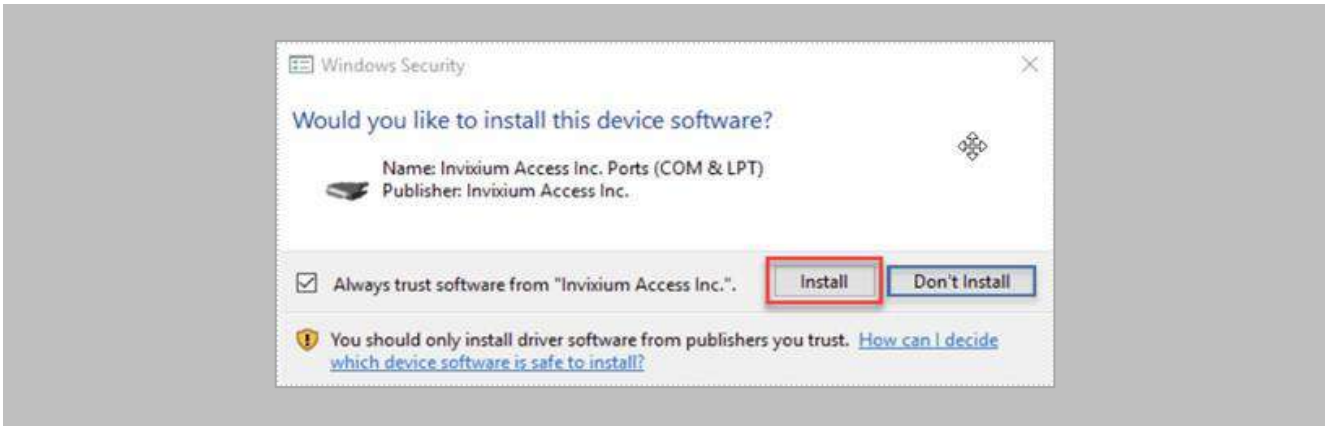


Figure 18: Invixium Fingerprint Driver Installation Message

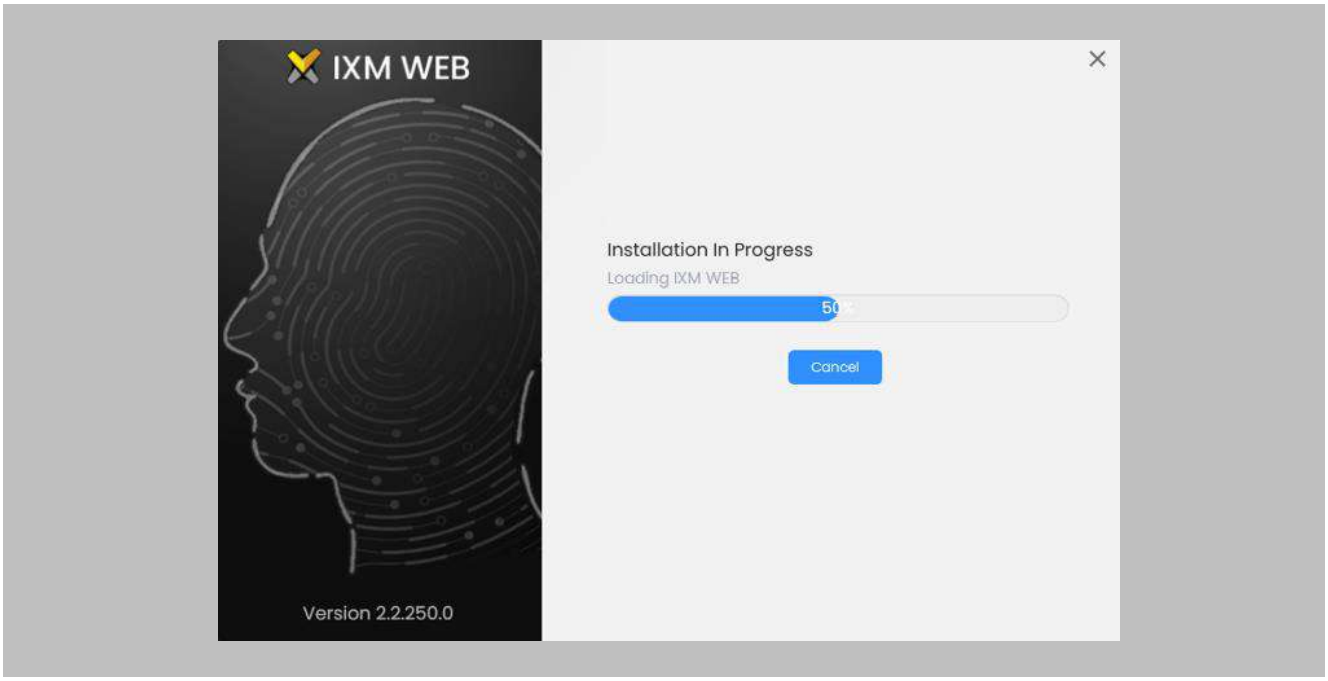


Figure 19: IXM WEB Installation Progress

STEP 4

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

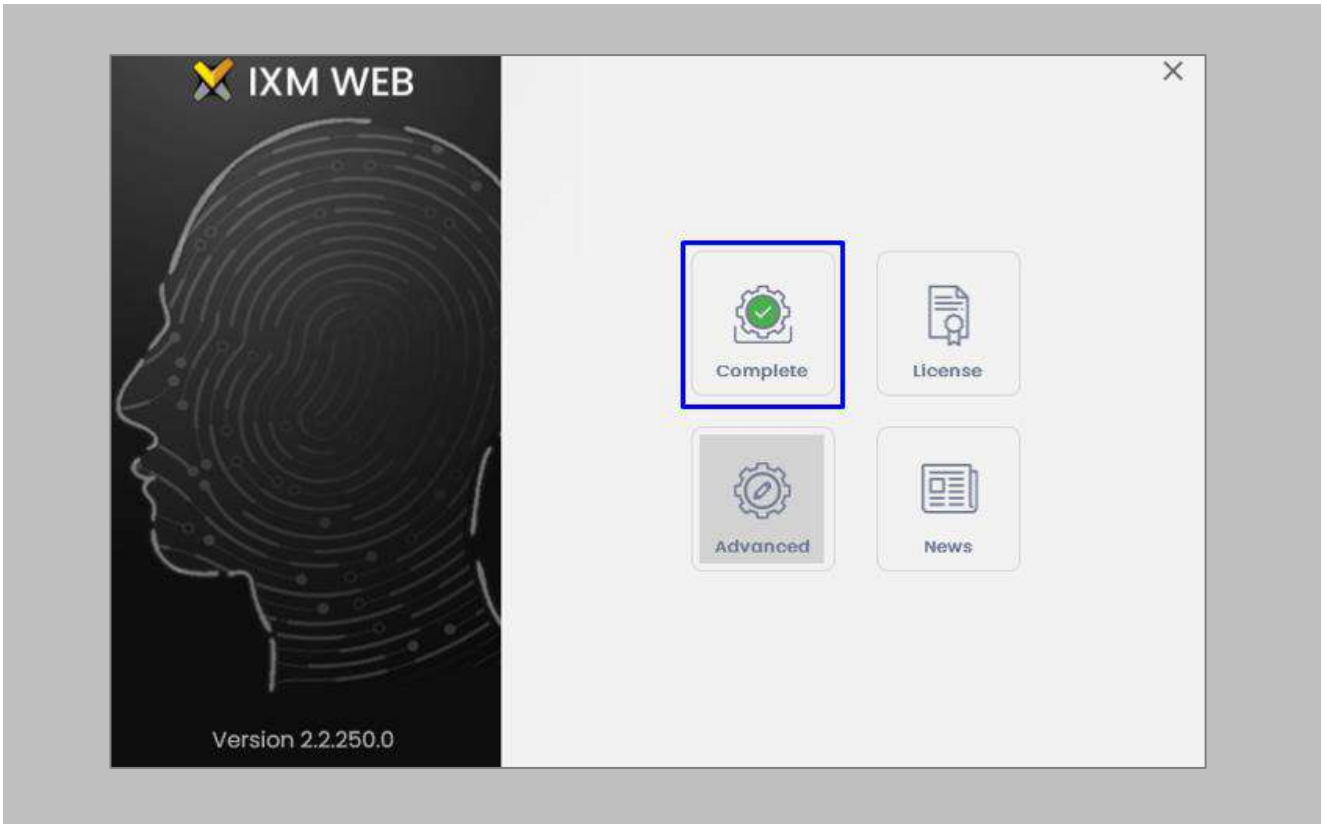


Figure 20: IXM WEB Installation Completed

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 21: IXM WEB Icon - Desktop Shortcut

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

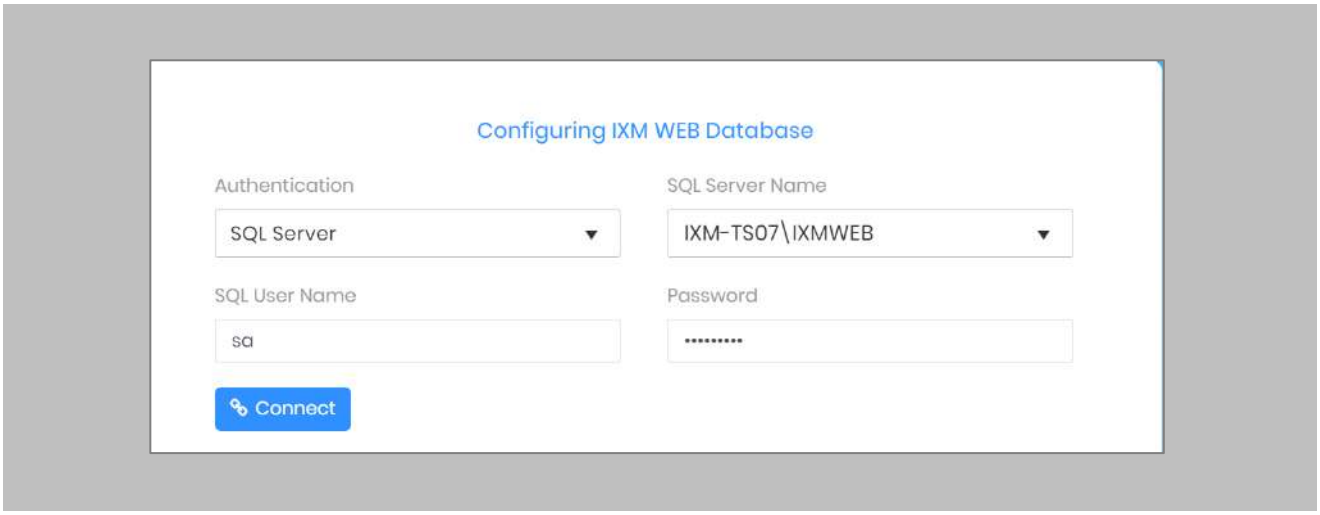


Figure 22: IXM WEB Database Configuration

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.

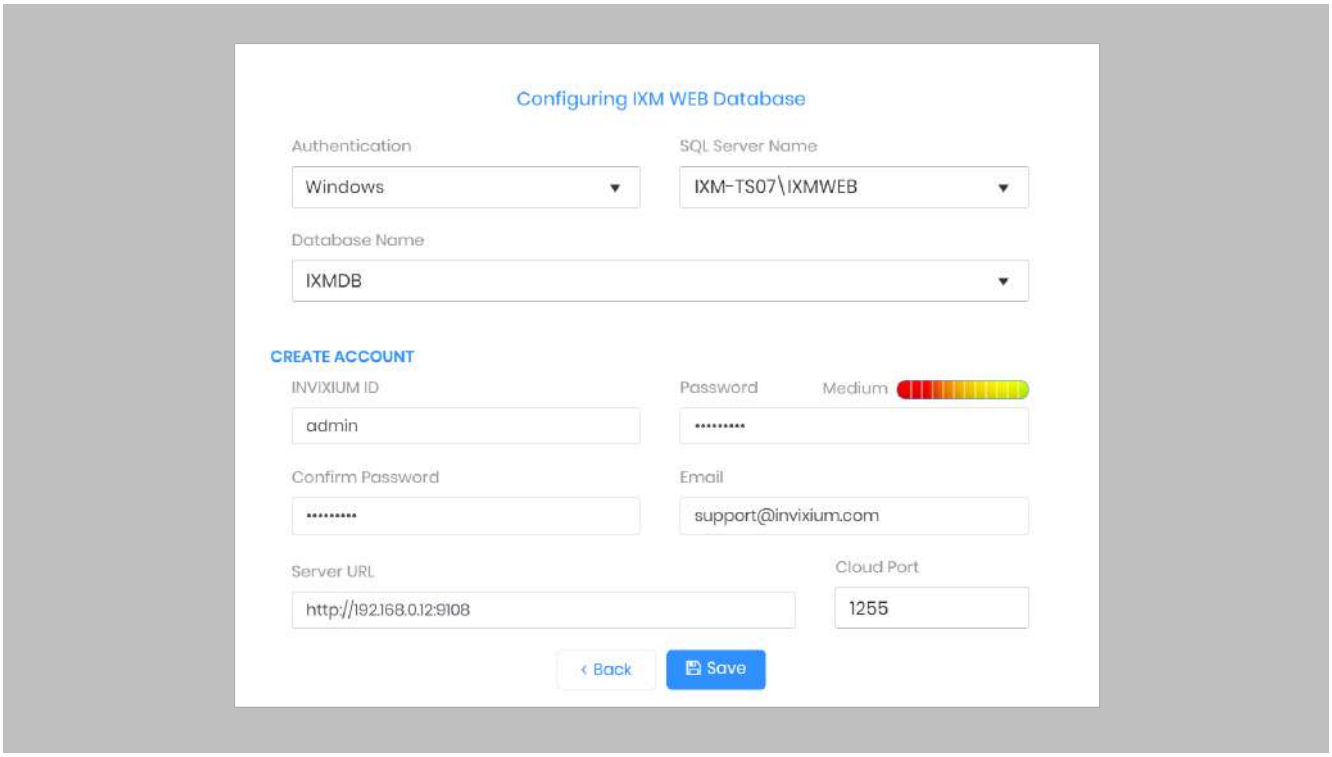


Figure 23: IXM WEB Administrator User Configuration

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:

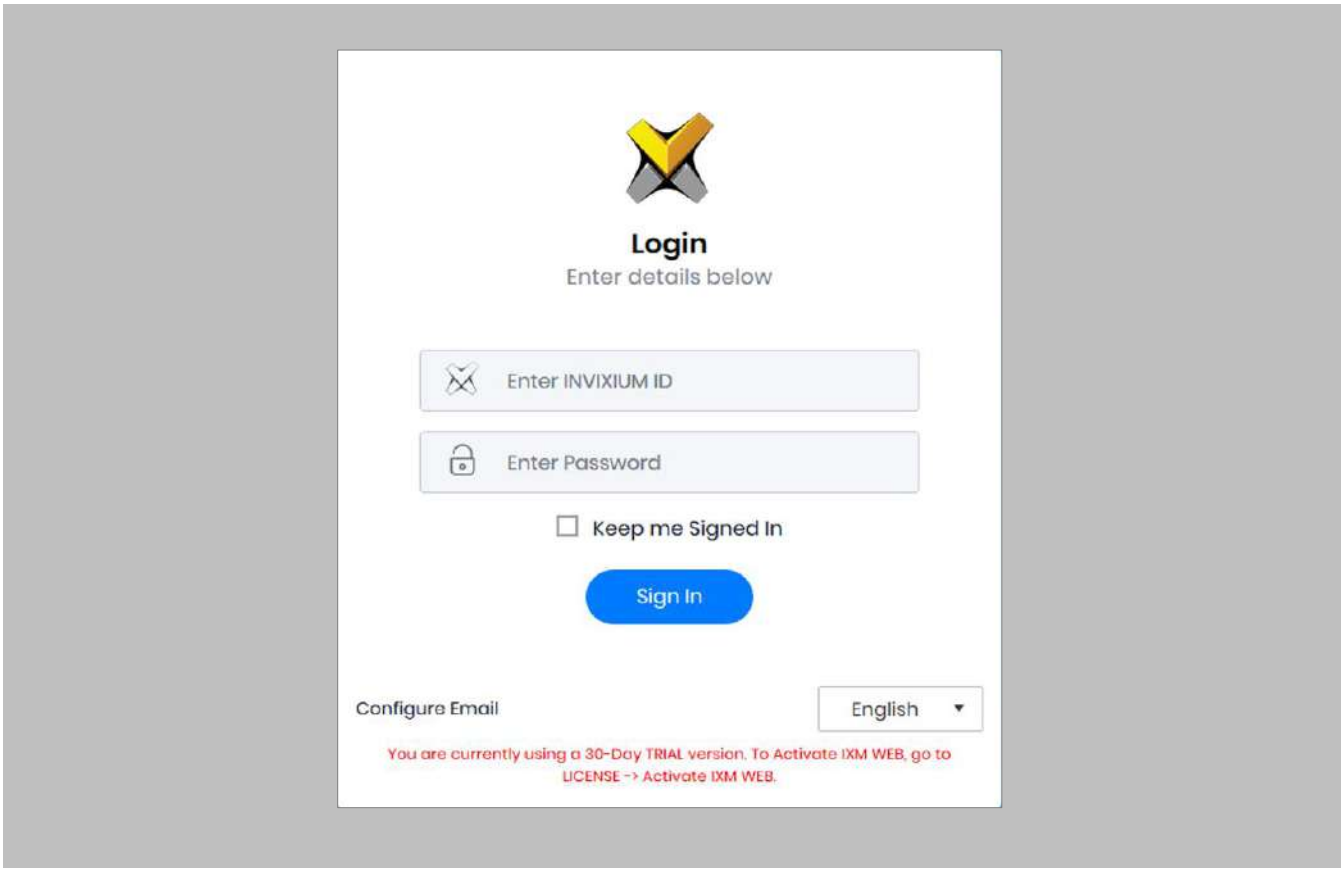


Figure 24: IXM WEB Login Page

Note: During an upgrade of IXM WEB from any previous release to 2.2.252.0, 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 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

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

OR

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

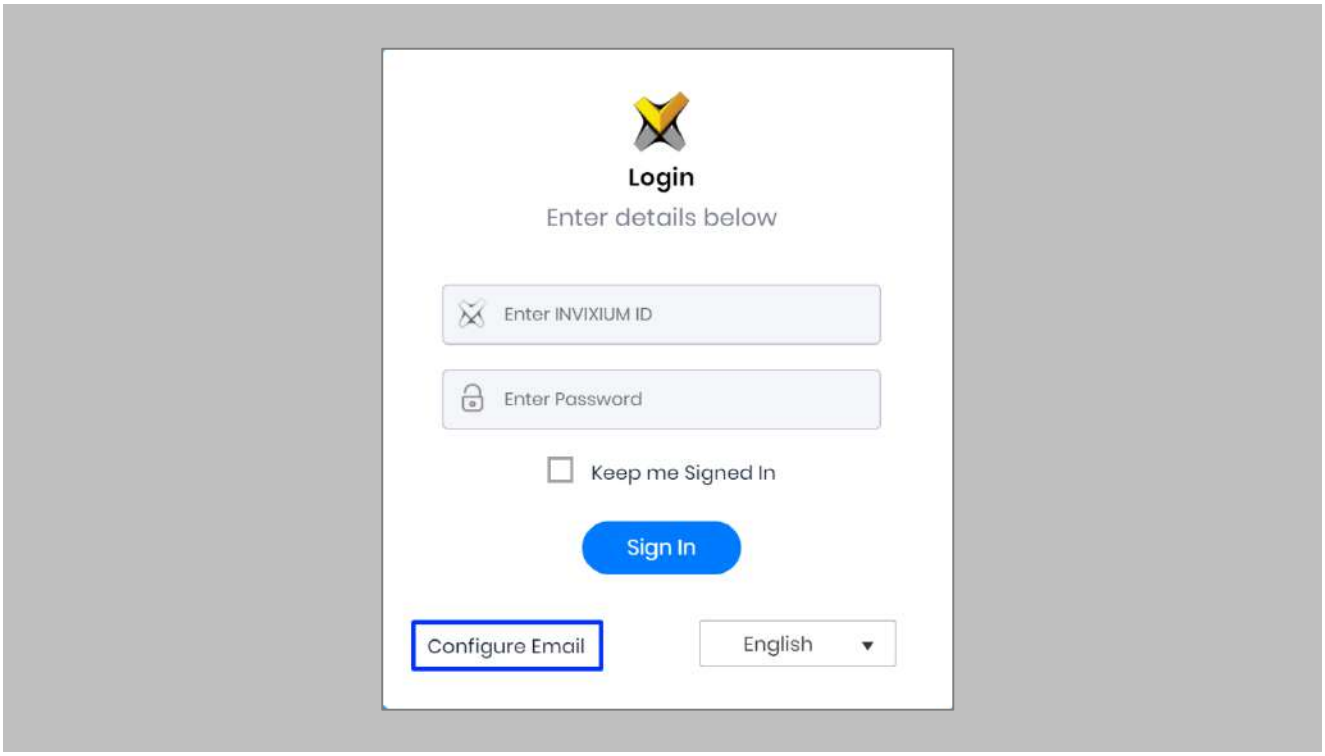


Figure 25: Configure Email

STEP 2

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

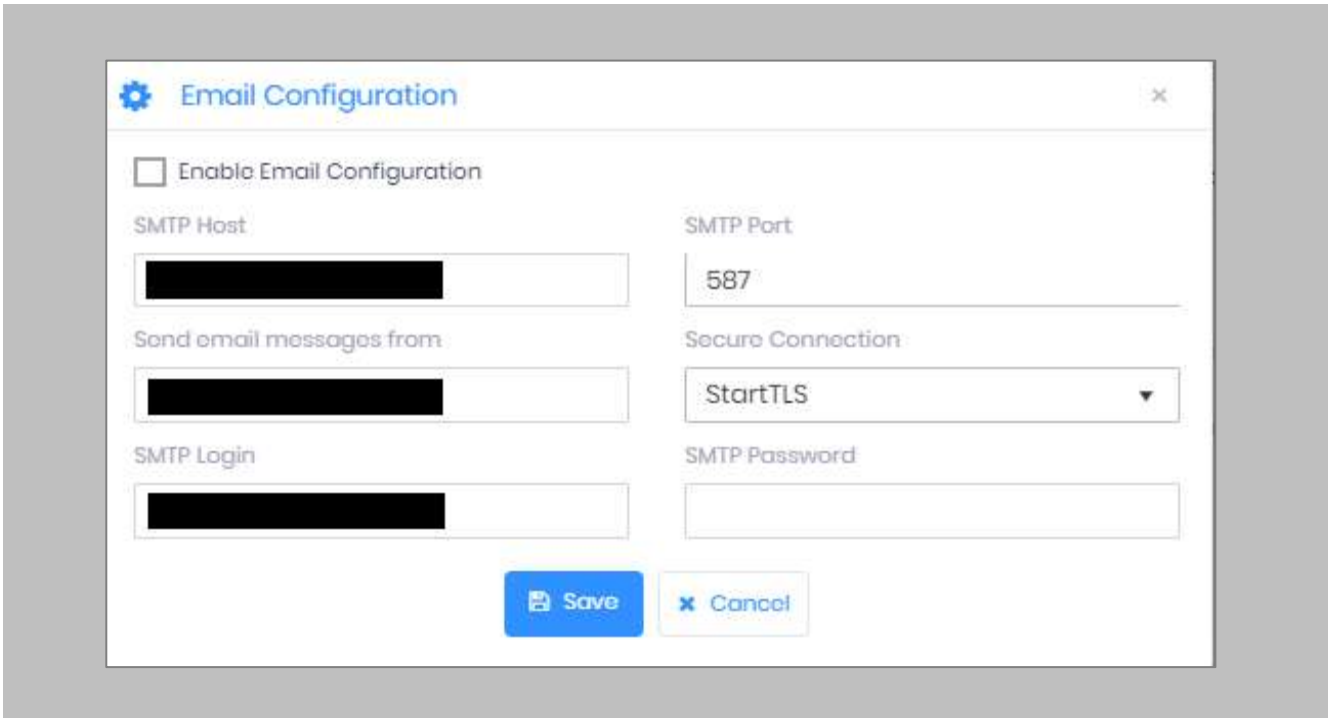


Figure 26: IXM WEB - SMTP Settings

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.

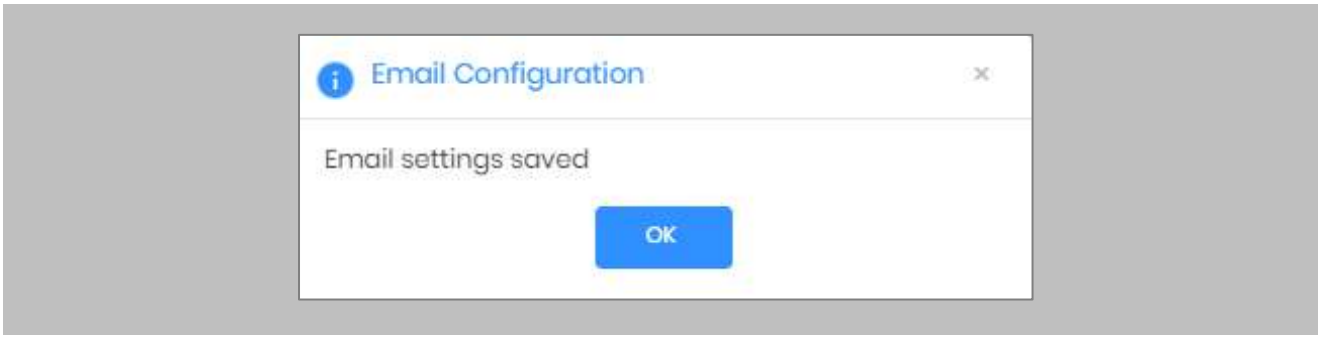


Figure 27: IXM WEB - Save Email Settings

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

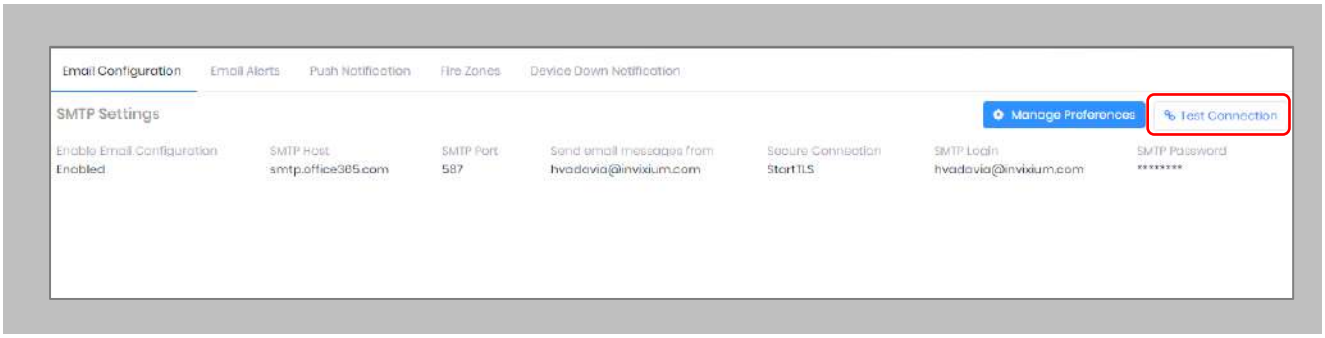


Figure 28: IXM WEB - Test Connection

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

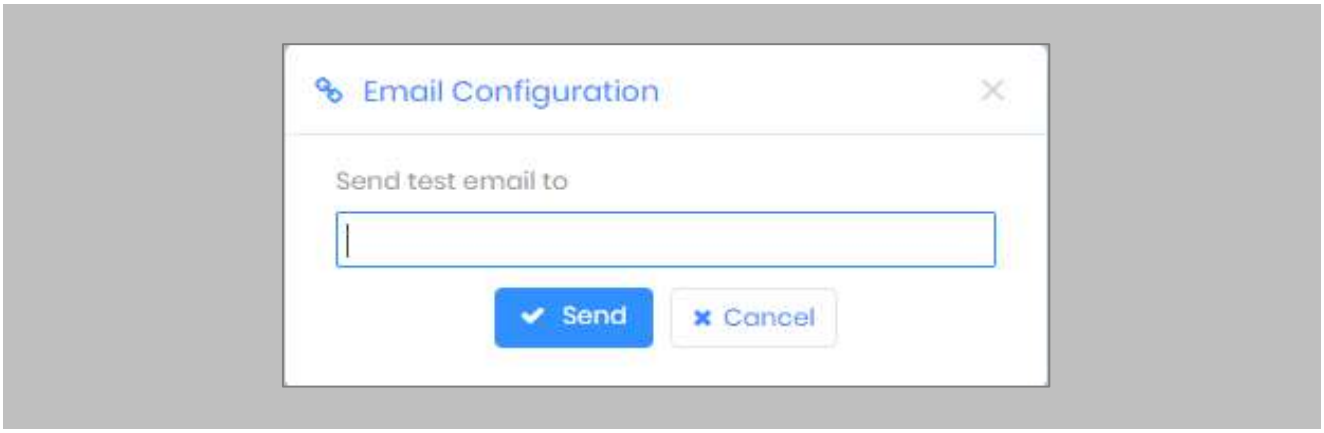


Figure 29: IXM WEB - Enter Email ID

STEP 4

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

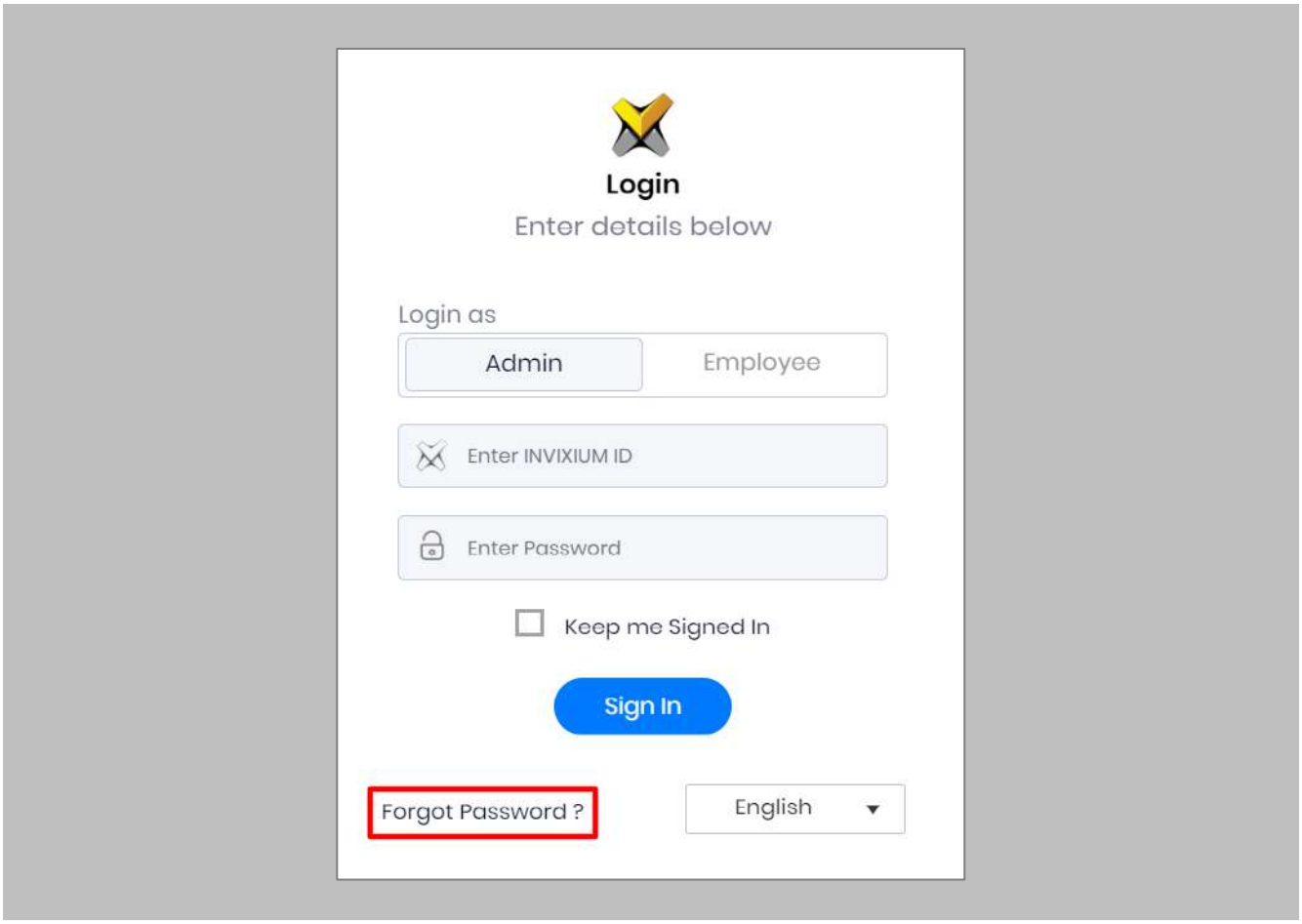


Figure 30: IXM WEB - Forgot Password

9. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

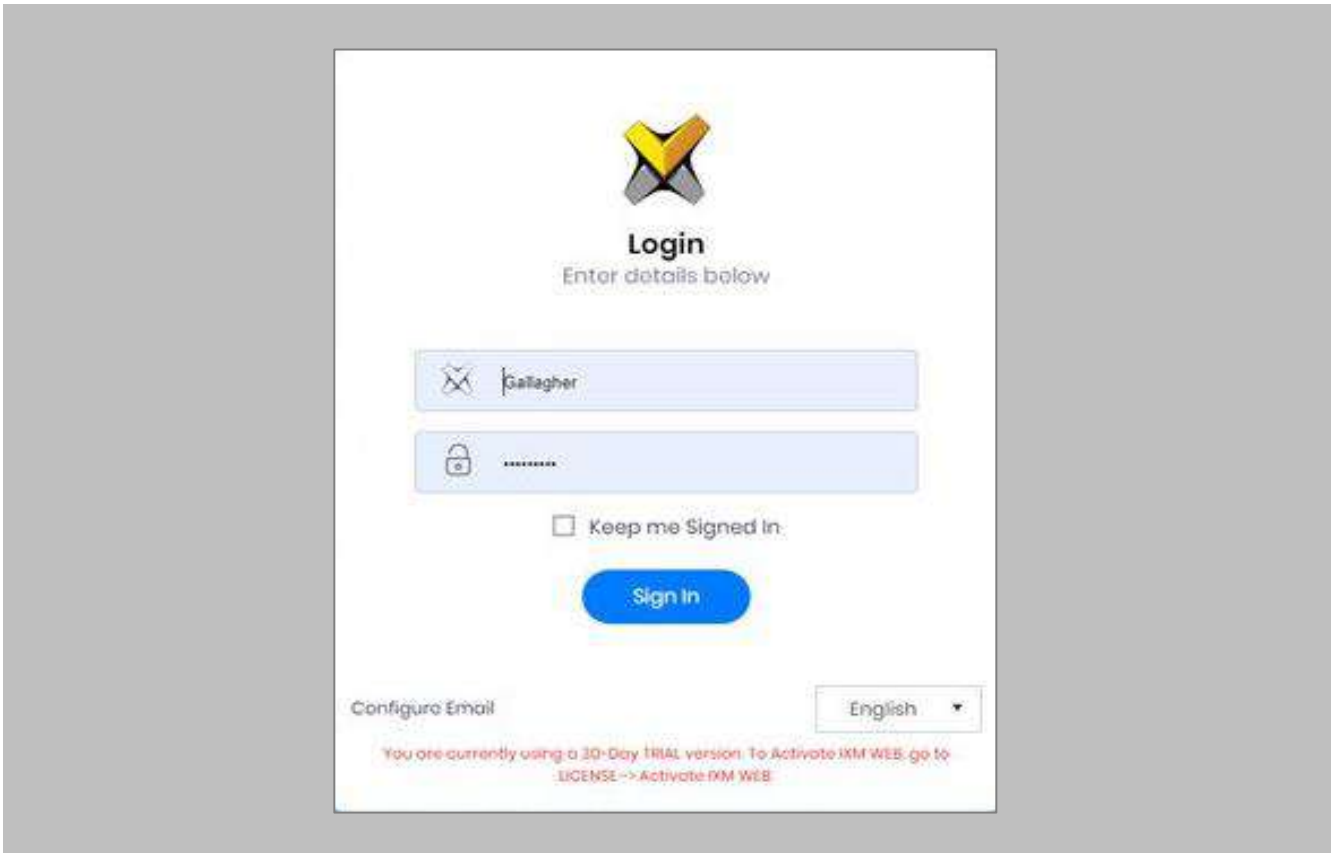


Figure 31: IXM WEB - Enter Login Credentials

STEP 2

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

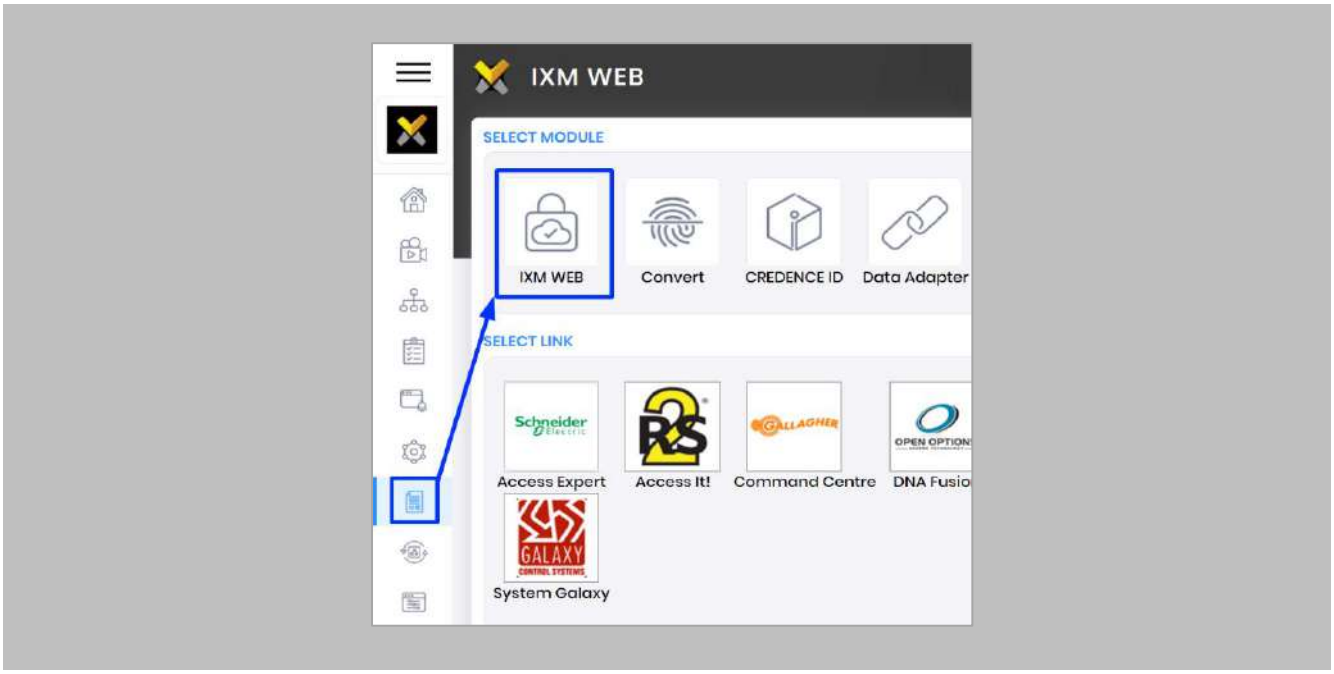


Figure 32: IXM WEB - License Setup

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**.

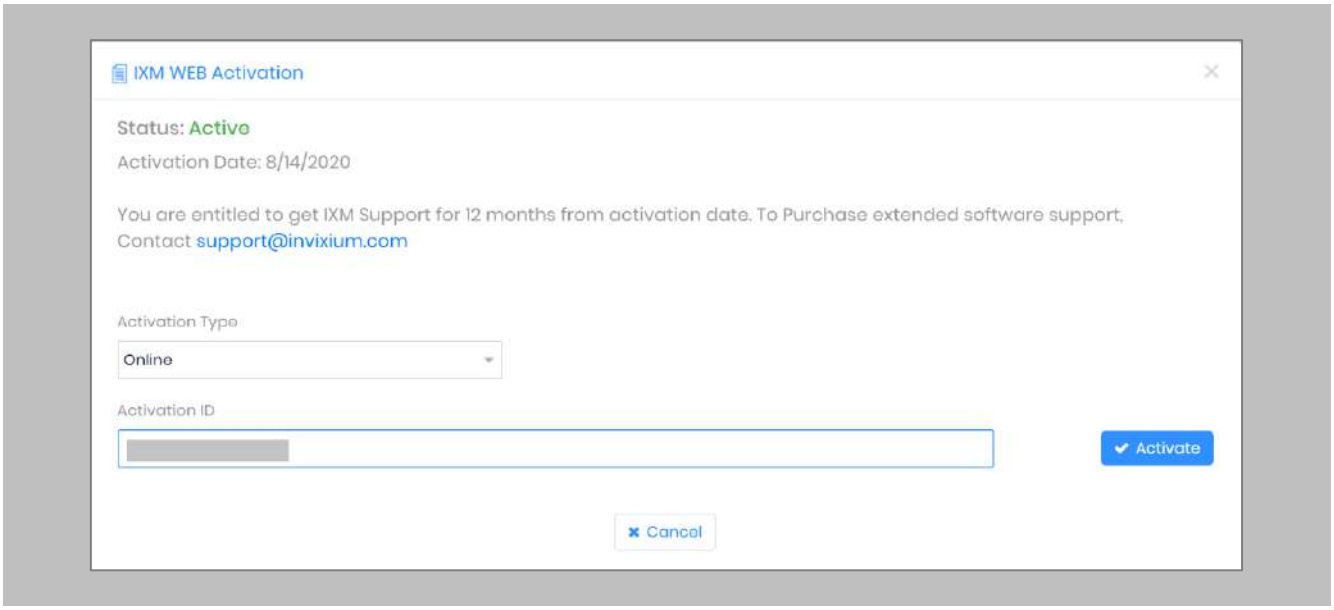


Figure 33: IXM WEB - Online Activation

Command Centre Module Activation

The option to request a Gallagher Command Centre License is available under the **License** tab.

STEP 1

Request a **License**.

STEP 2

From **Home**, expand the **Left Navigation Pane**, Go to the **License** tab. Click on **Command Centre (Gallagher).**

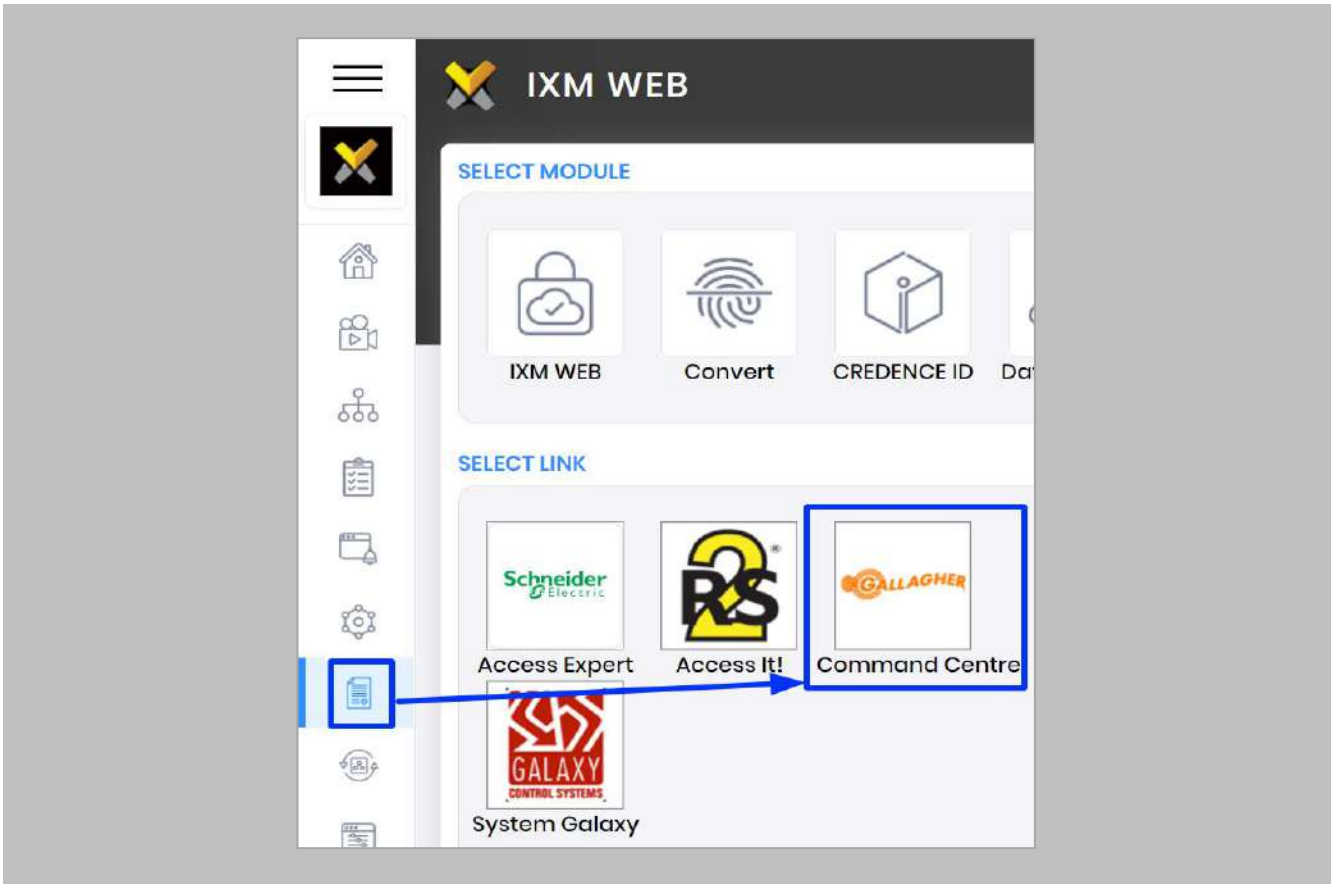


Figure 34: IXM WEB - Gallagher Link Activation

STEP 3

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

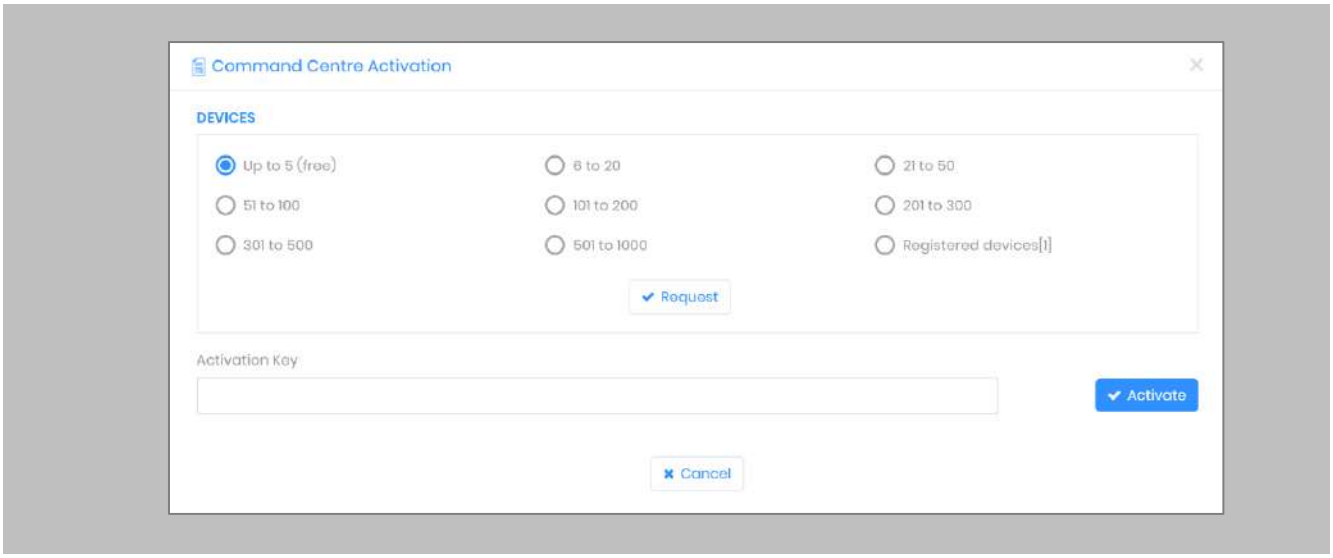


Figure 35: IXM WEB - Device Selection for Gallagher License Request

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

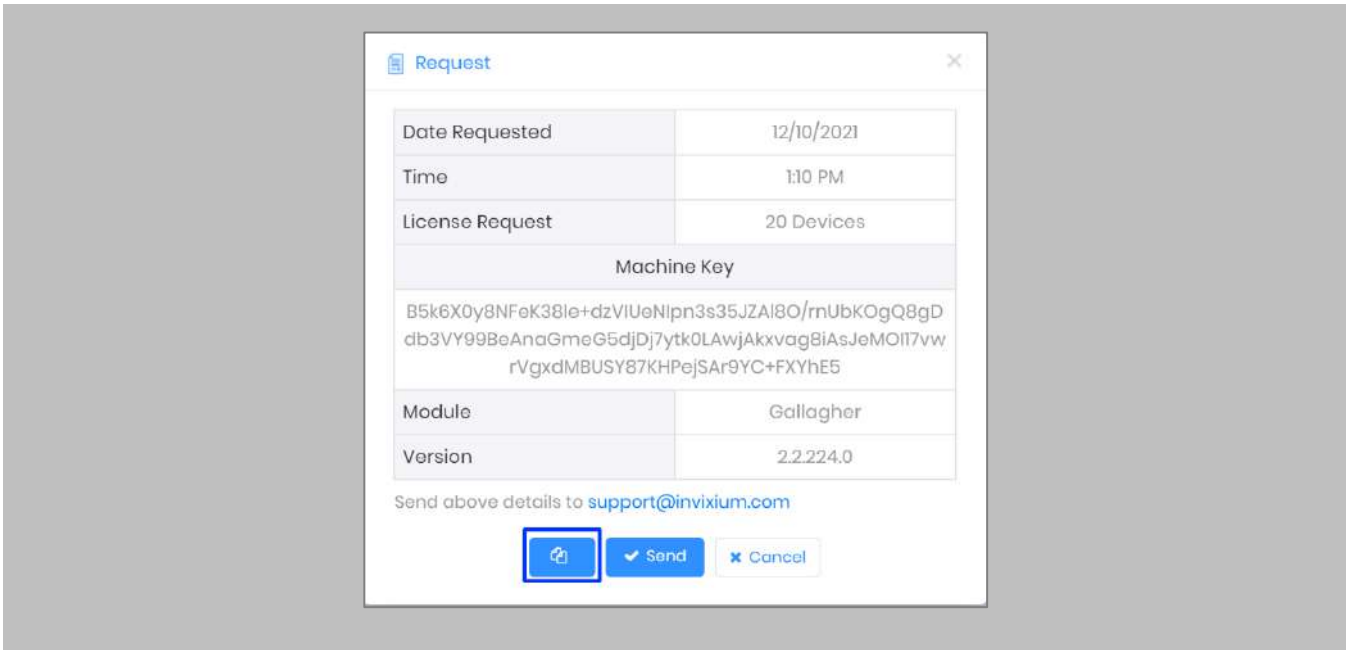


Figure 36: IXM WEB - Gallagher License Request

STEP 4

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

You will receive an email from Invixium Support containing a license key for the Gallagher Command Centre Activation.

Figure 37: Gallagher License Key Email

STEP 5

Copy and **paste** the license key into the Activation Key area in the IXM WEB Command Centre Activation, and then select **Activate**.

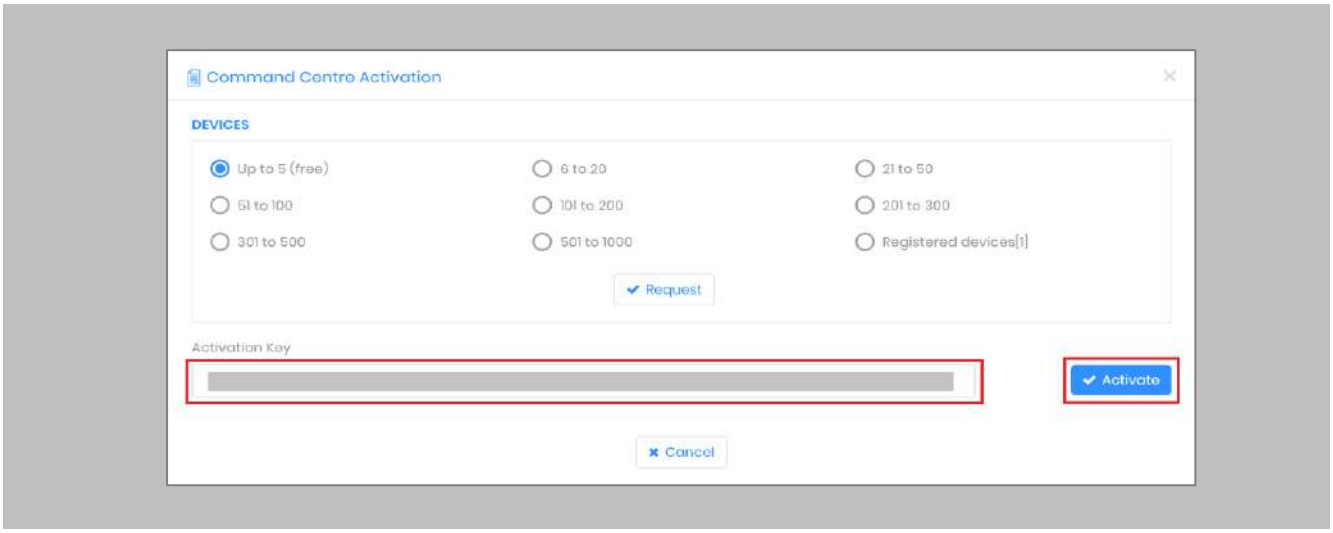


Figure 38: IXM WEB - Activate Gallagher Link License

RESULT

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

10. Configuring IXM Link for Gallagher

Procedure

STEP 1

From the **Left Navigation Pane** → **Link** → click the orange **Command Centre (Gallagher)** icon.

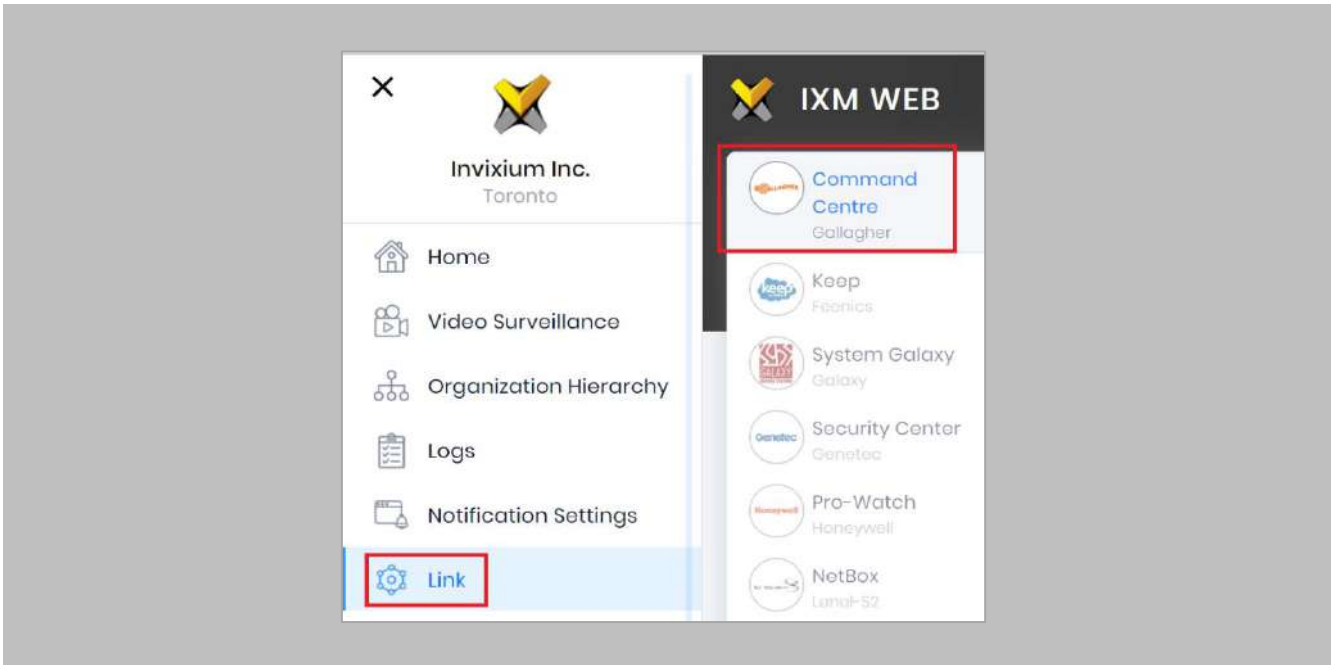


Figure 39: IXM WEB - Link Menu

STEP 2

Toggle the **Status** switch to enable.

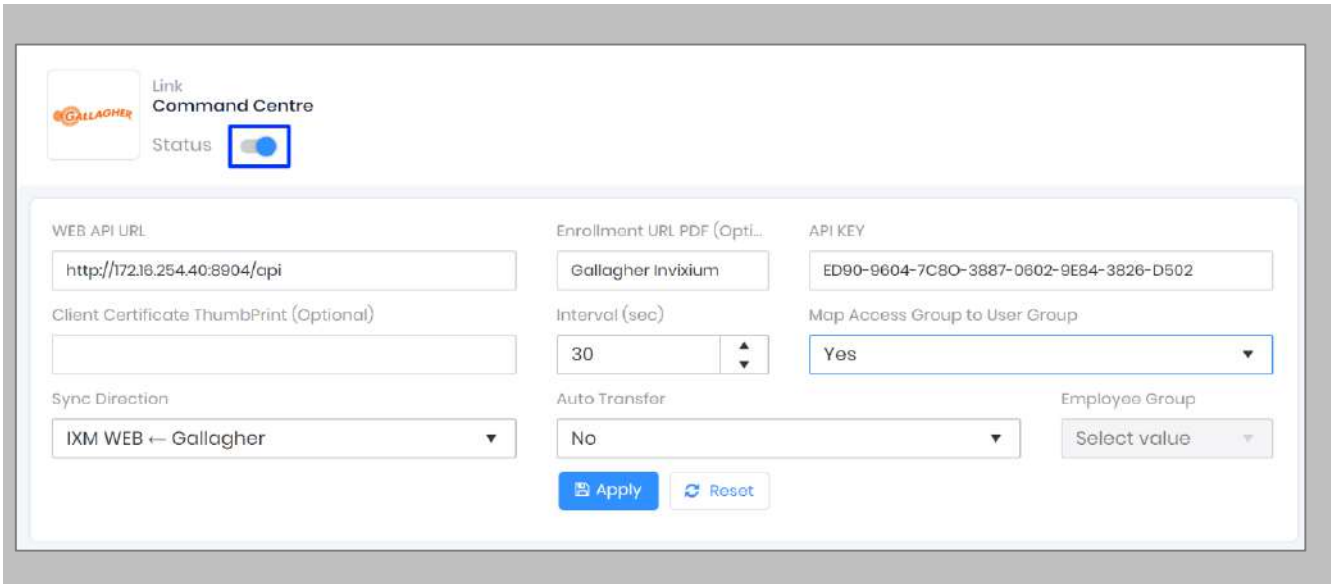


Figure 40: IXM WEB - Enable Gallagher Link Module

STEP 3

Enter the **GCC REST API URL**. For example: **https://172.16.254.40:8904/api/.**

STEP 4

Copy the PDF's name created for **'Enrollment URL PDF'** (refer to URL Enrollment PDF (Personal Data Field)).

STEP 5

Copy the Enrollment status name created **'ENROLLMENT STATUS'** (refer to Enrollment Status PDF (Personal Data Field)).

STEP 6

Enter the **API key** for basic authentication API as indicated.

STEP *7*

Refer to the **REST Client Certificate** thumbprint found within the REST API.

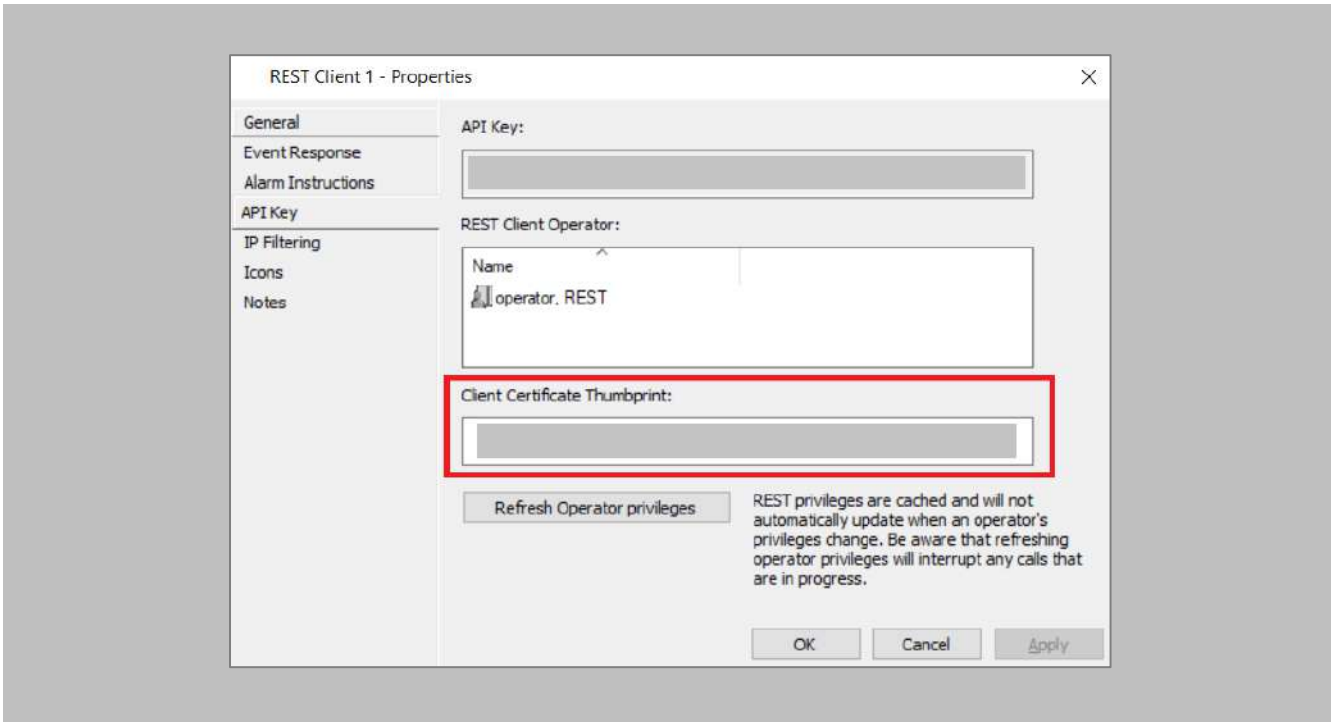


Figure 41: GCC - REST Client Certificate Thumbprint

STEP 7

Specify in seconds how often sync should take place.

STEP 8

Select **Map Access Group** to User Group.

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

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

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

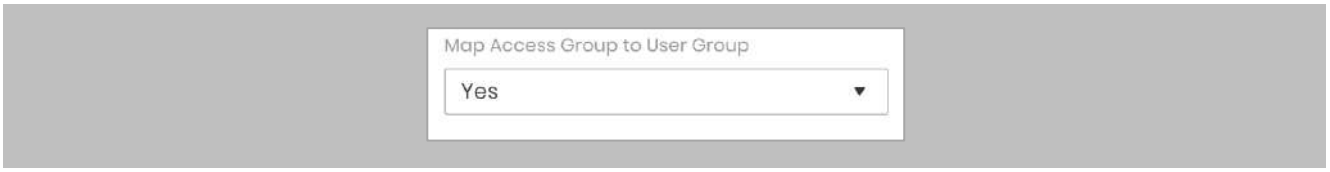


Figure 42: IXM WEB - Map Access Group to User Group

STEP 9

Select **Sync Direction.**

Select one-way sync direction IXM WEB ← Gallagher to import cardholders from Gallagher to IXM WEB.

Figure 43: IXM WEB - Sync Direction

STEP 10

Select **Auto Transfer.**

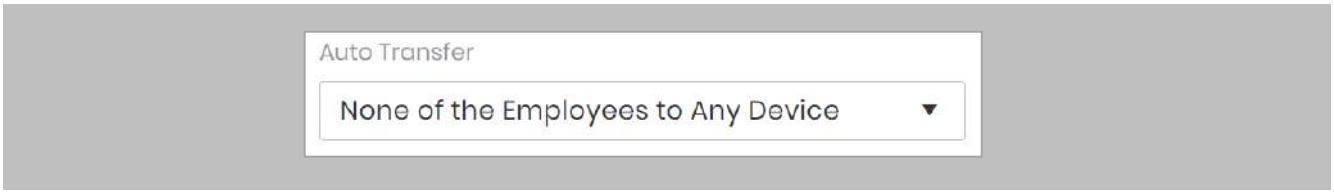


Figure 44: IXM WEB - Auto Transfer Employees

STEP 11

Click **Apply.**

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

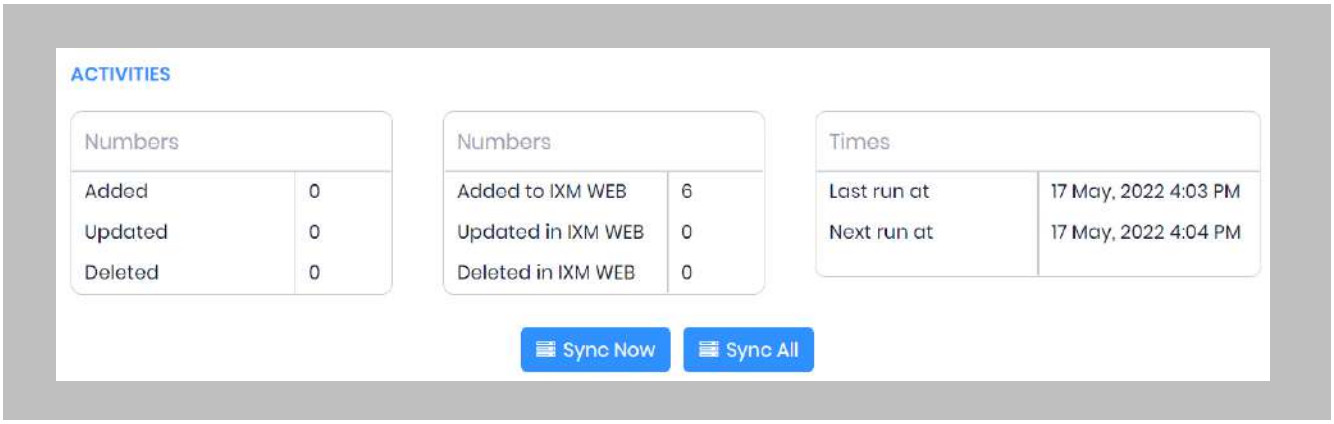


Figure 45: IXM WEB - Sync Activities

STEP 12

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 13

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

STEP 14

The **Sync All** feature allows a resynchronization of the database from GCC to IXM WEB. This will re-import missing cardholders or updated cardholders from GCC to IXM WEB. Also, it will delete IXM WEB employee records according to cardholders available in GCC.

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

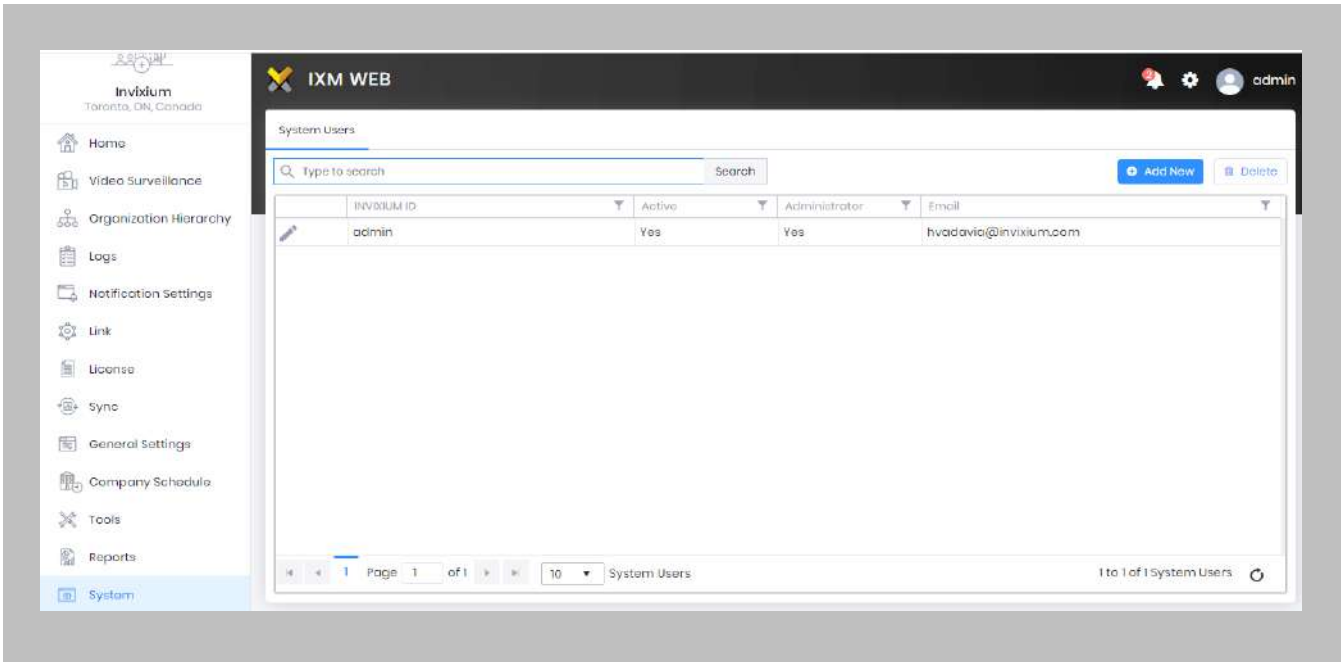


Figure 46: IXM WEB - Create System User

STEP 2

Click **Add New**.

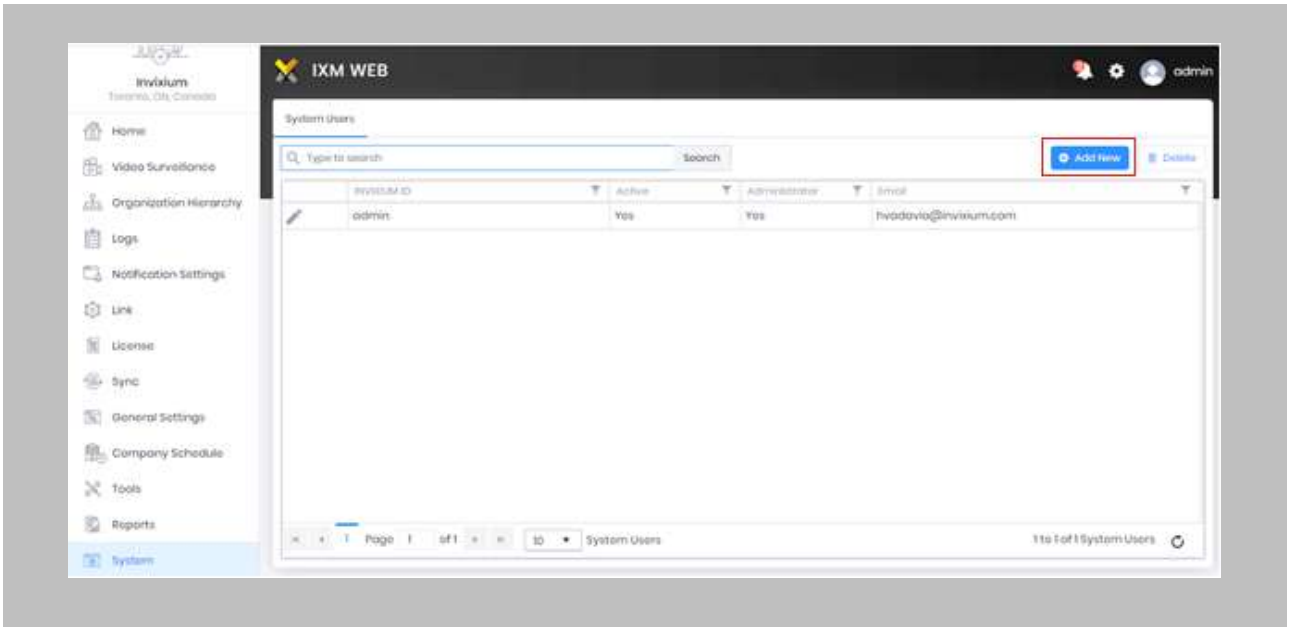


Figure 47: IXM WEB - Add New System User

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.

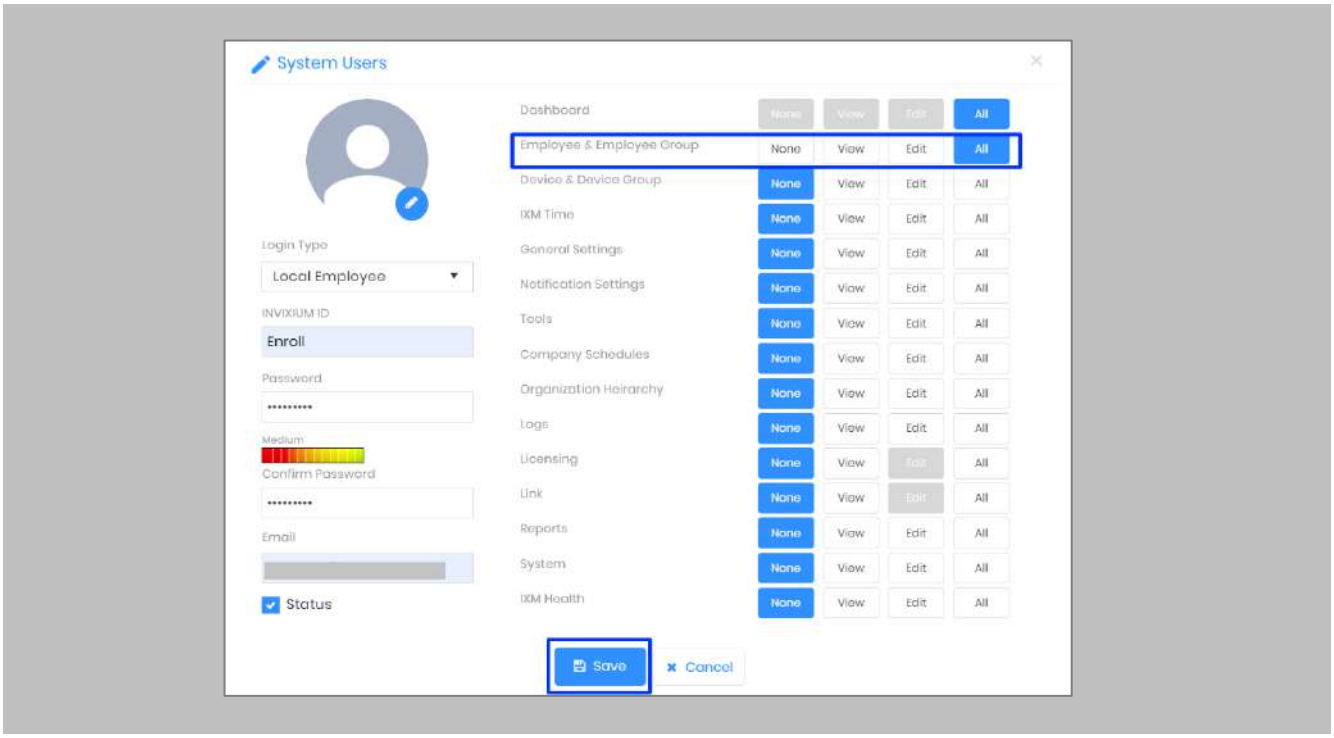


Figure 48: IXM WEB - New System User

STEP 4

Add an email address.

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

Click **Save**.

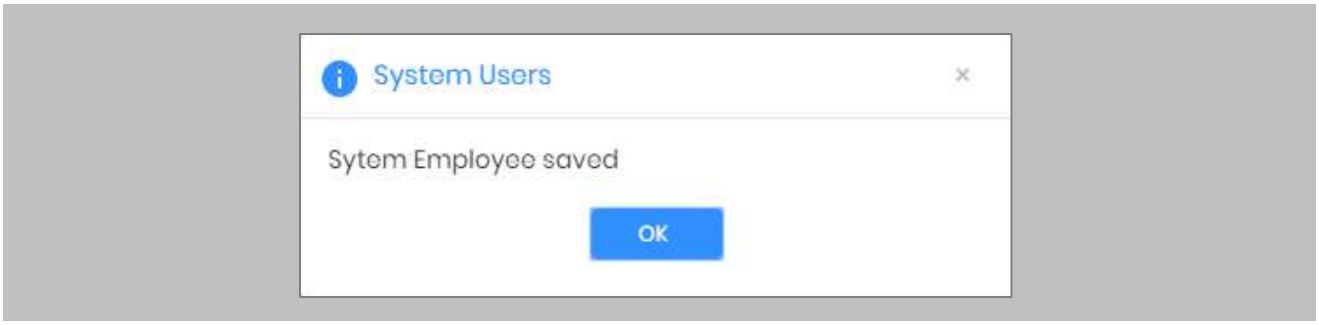


Figure 49: IXM WEB - Save System User

12. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

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

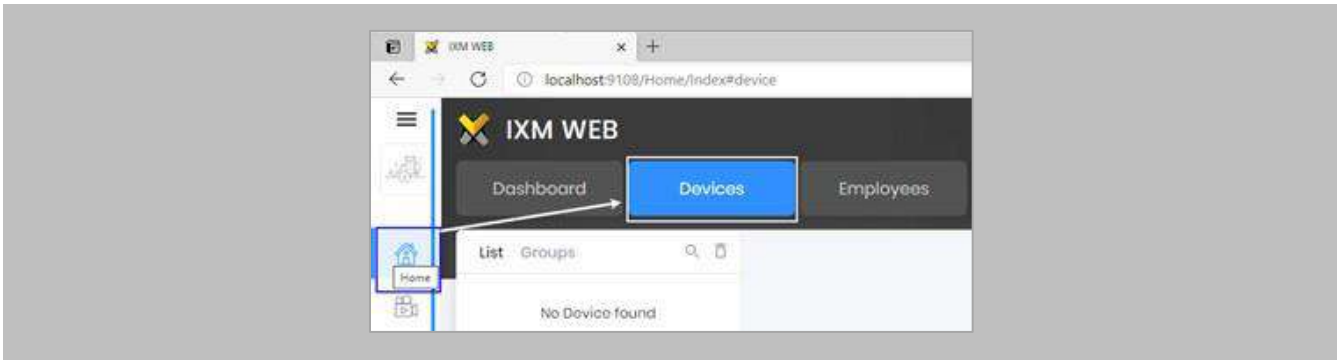


Figure 50: IXM WEB - Devices Tab

STEP 2

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

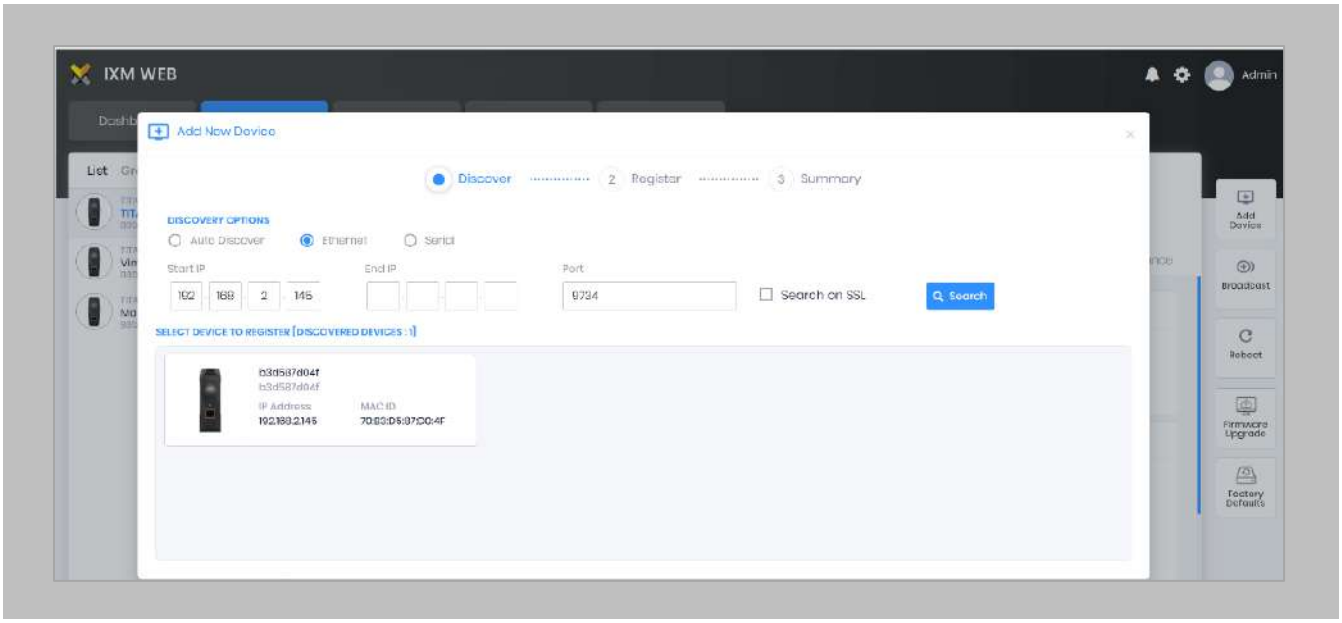


Figure 51: IXM WEB - Search Device Using IP Address

STEP 3

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

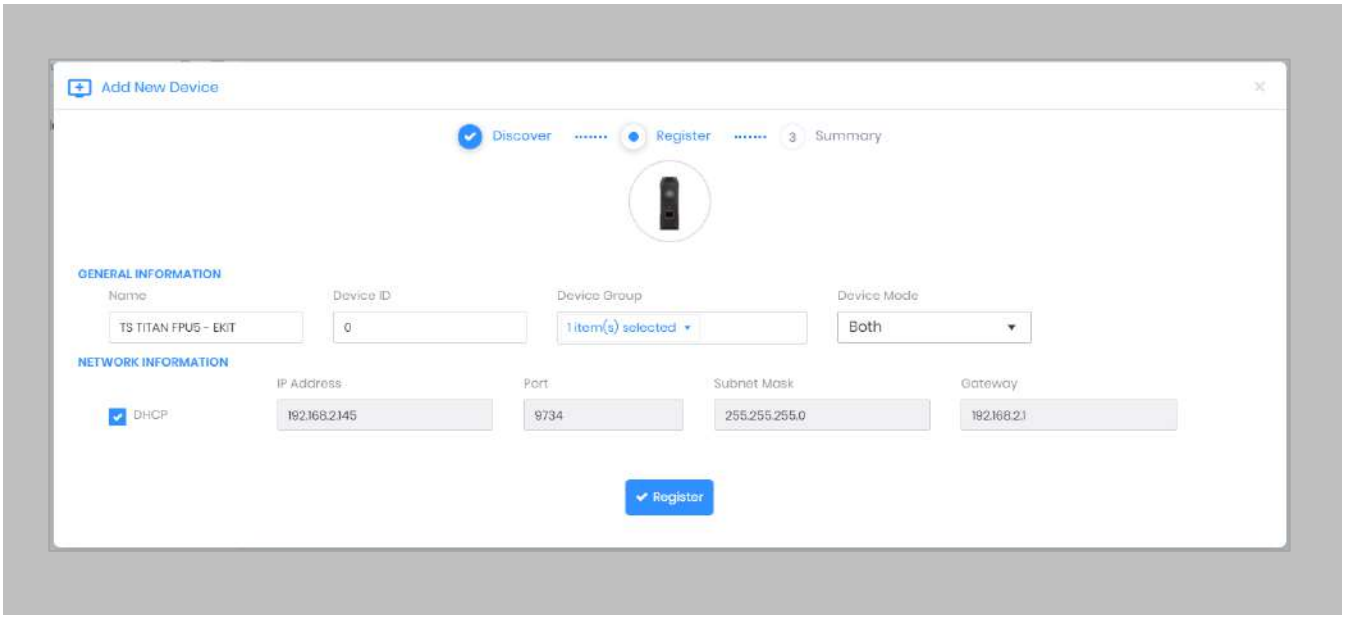


Figure 52: IXM WEB - Register Device

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**.

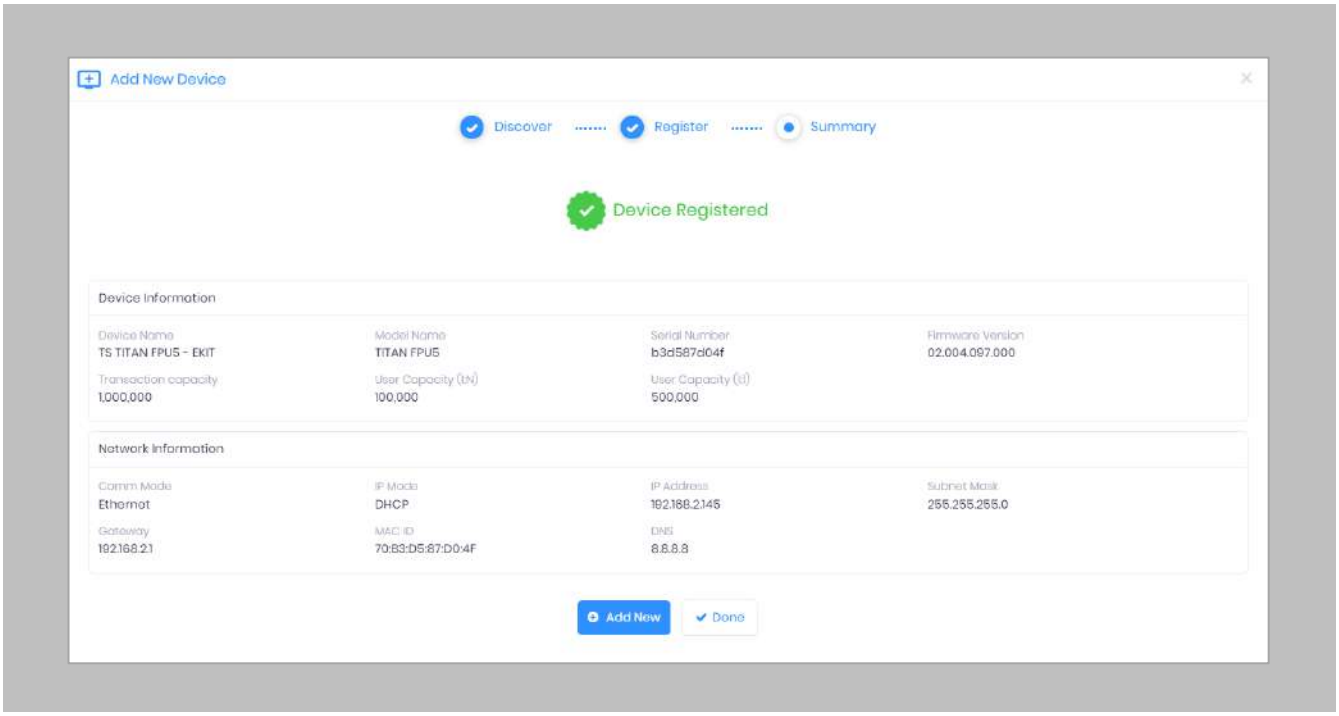


Figure 53: IXM WEB - Device Registration Complete

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).

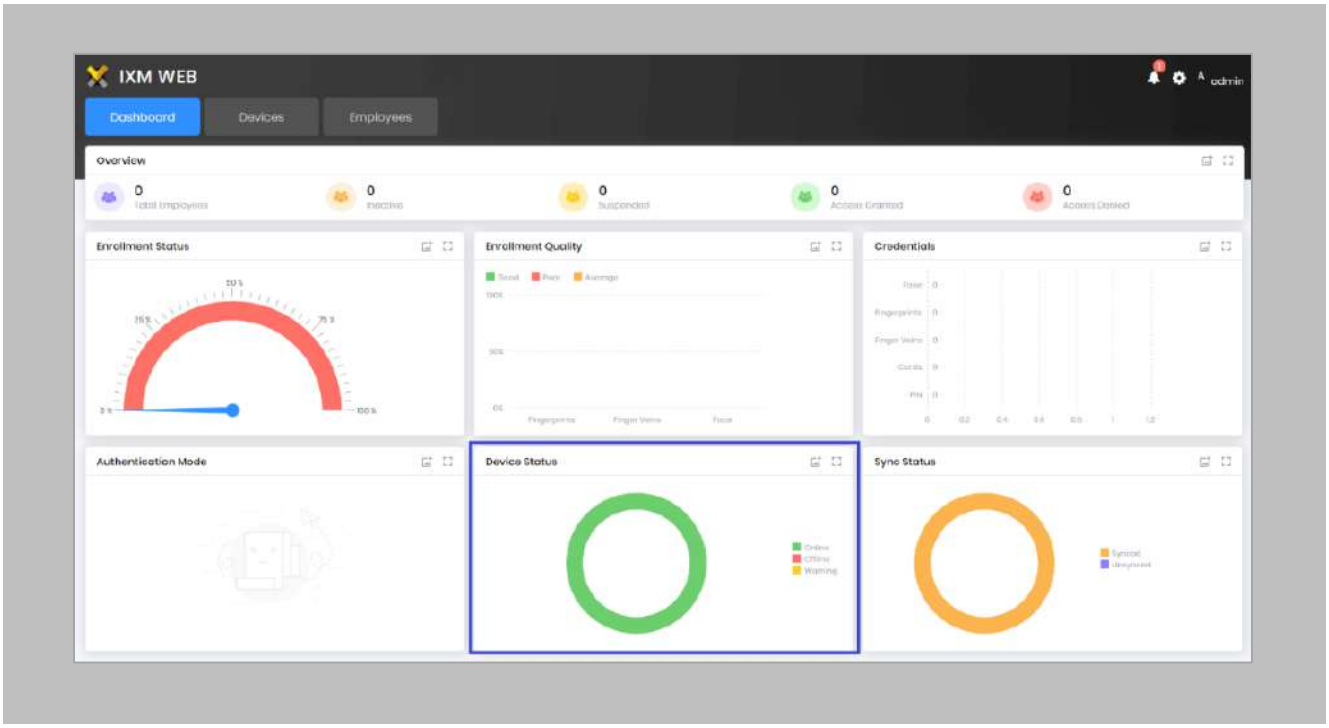


Figure 54: IXM WEB - Dashboard, Device Status

13. Adding an Invixium Device to a Device Group

Procedure

STEP 1

Go to **Devices** → **Groups**.

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

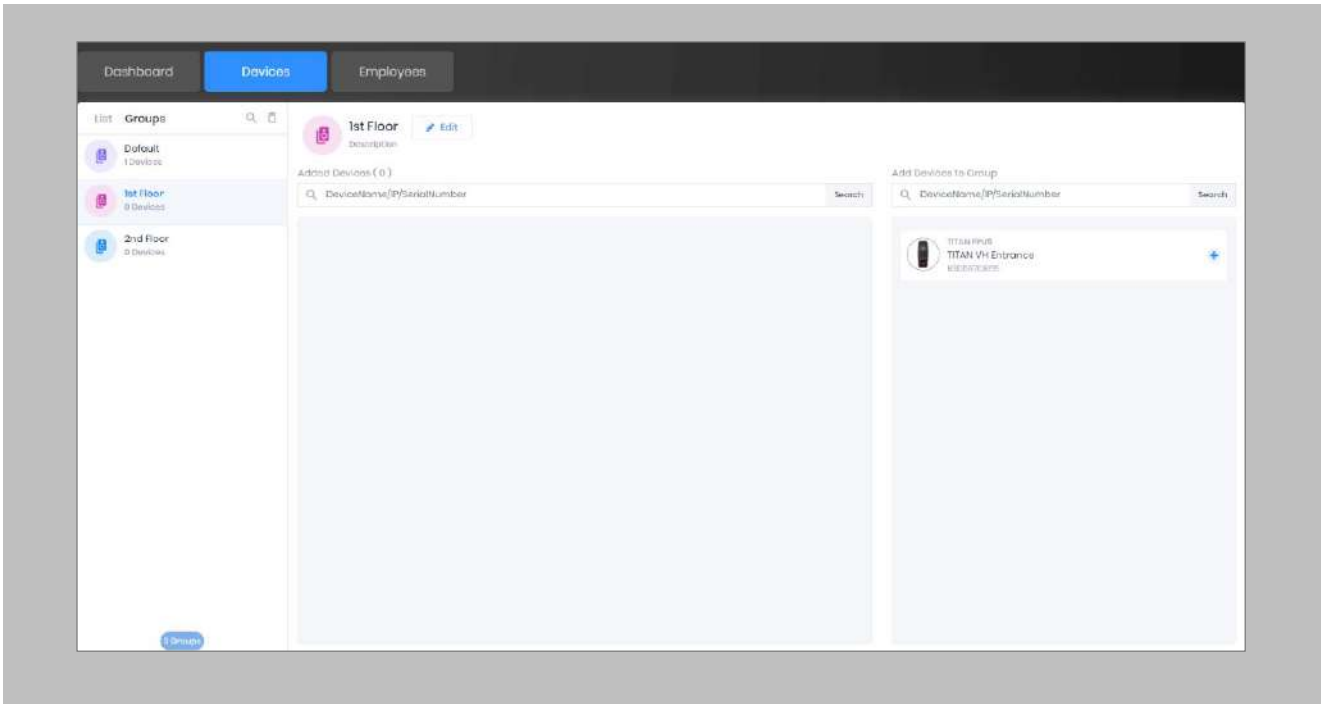


Figure 55: IXM WEB - Assign Device Group

Configuring Wiegand to Assign Invixium Readers

Note: This is based on 17/23 bits for facility code/card number format allowing facility codes up to 65535 and card numbers from 1 to 8,388,607.

STEP 1

Click **General Settings** and **Create Custom.**

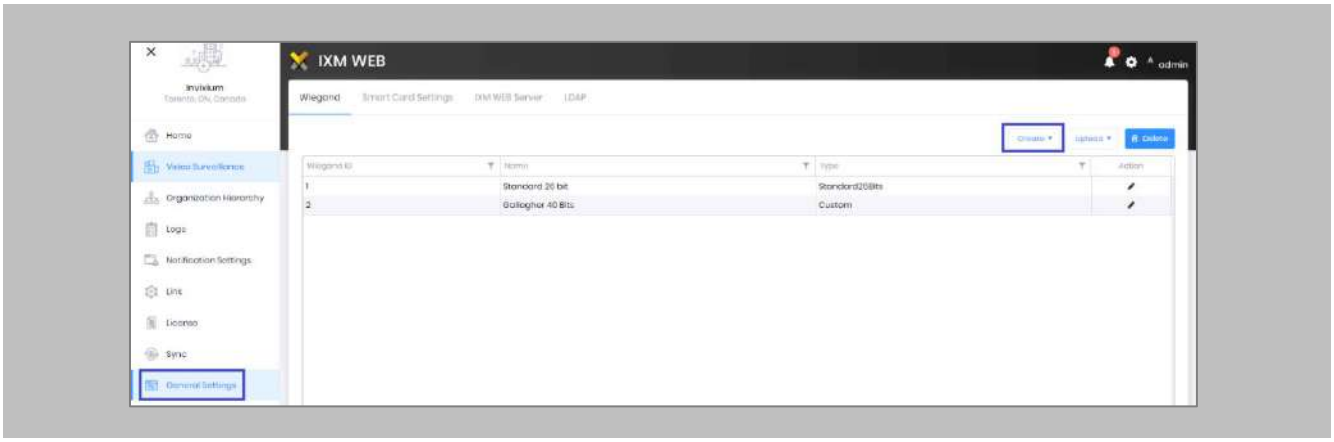


Figure 56: IXM WEB - Create Wiegand Format

STEP 2

Click **Name** & Assign **40-bit**.

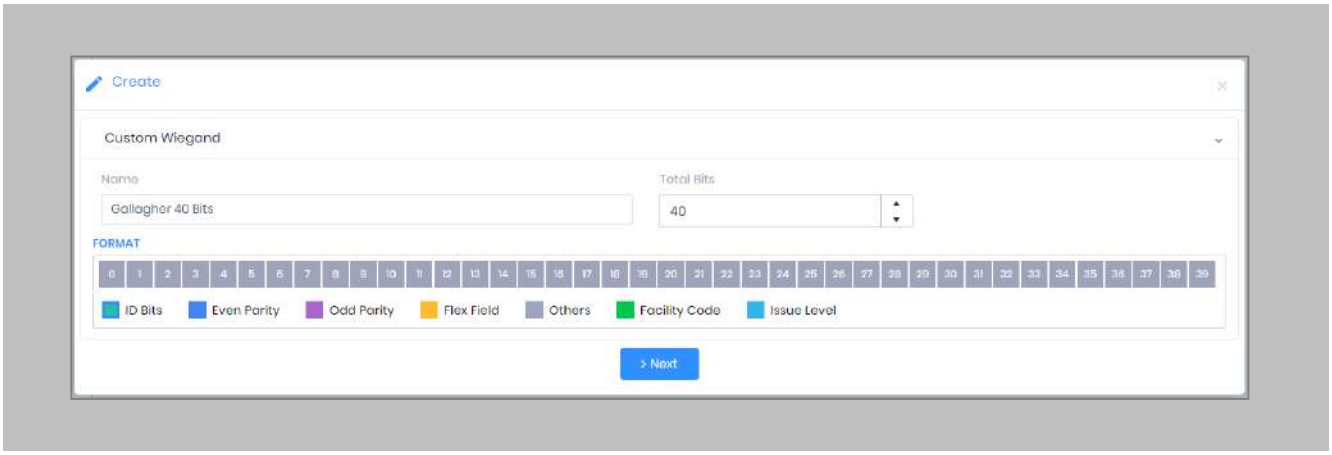


Figure 57: IXM WEB - Create Custom Wiegand Format

STEP 3

Click **Next** and **Highlight** as shown:

Facility Code: 0 to 16 bits

ID Bits: 17 to 39 bits

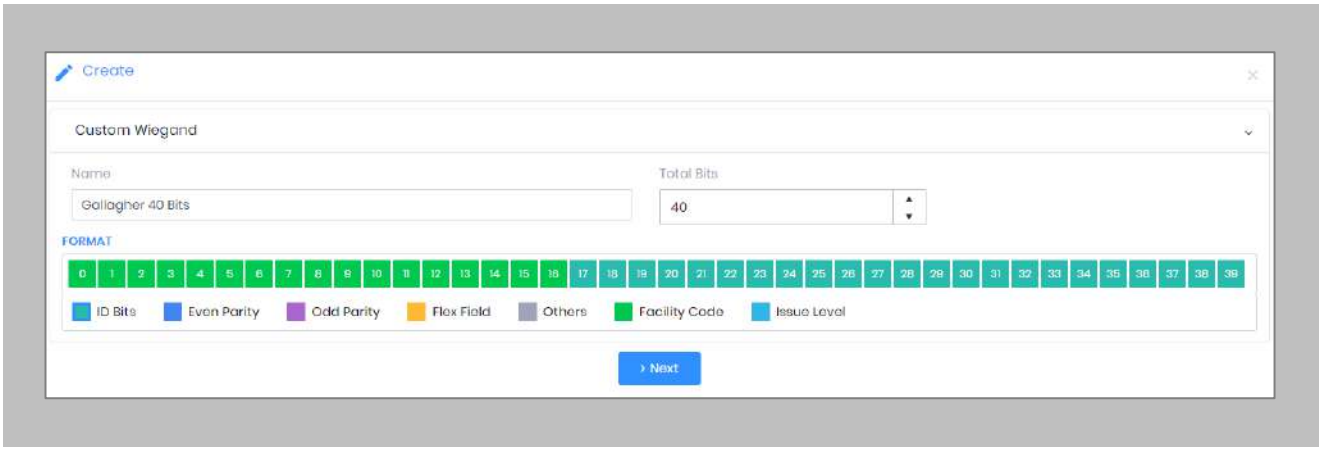


Figure 58: IXM WEB - Custom Wiegand

STEP 4

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

STEP 5

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

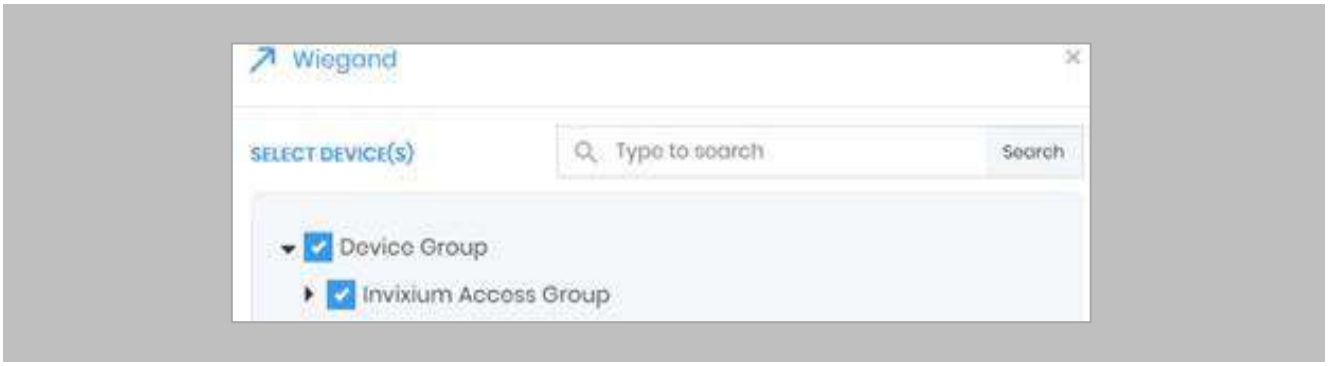


Figure 59: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invixium Readers

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

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

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.

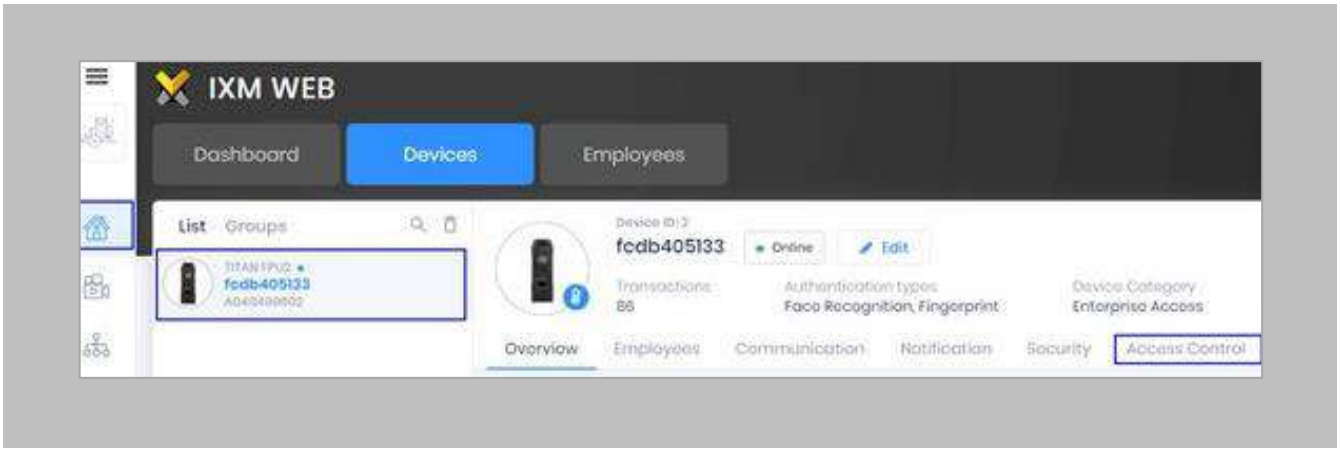


Figure 60: IXM WEB - Navigate to Access Control Tab

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.

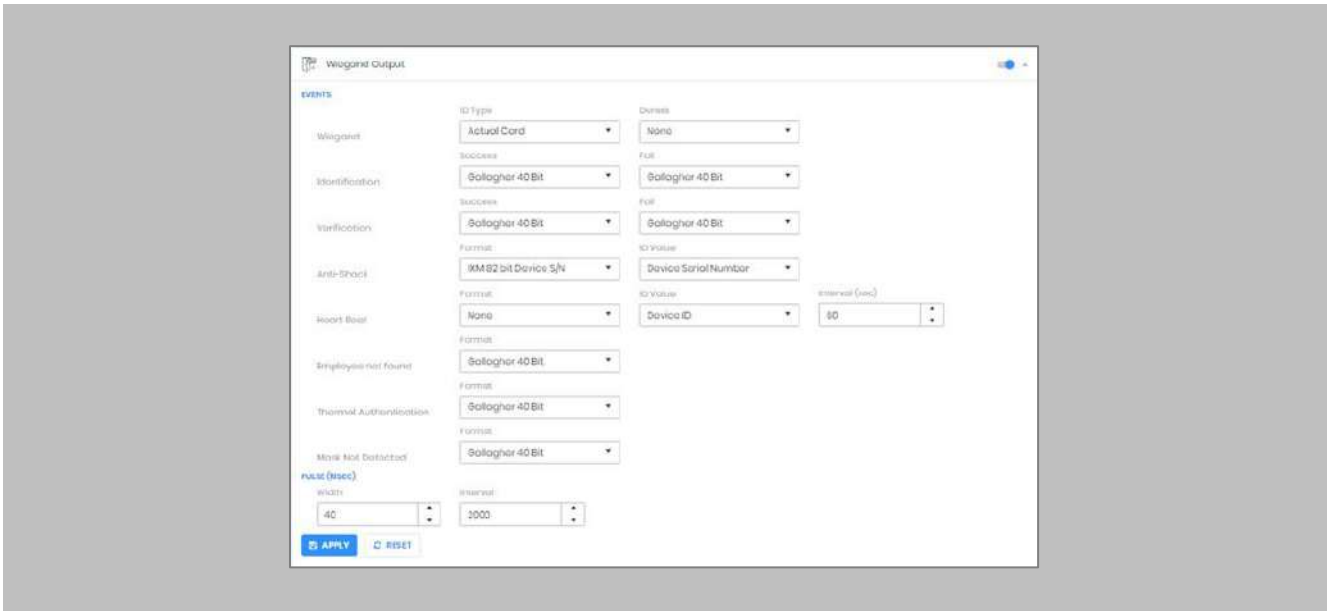


Figure 61: IXM WEB - Wiegand Output

ID types for Wiegand output are as follows:

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

By default, Employee ID is selected in Wiegand Event.

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

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

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

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

STEP 4

Set the **items**:

Wiegand	Actual Card
Identification	40 - bit
Verification	40 - bit
Employees not found	40 - bit
Thermal Authentication	40 - bit
Mask not Detected	40 - bit

STEP 5

Click **Apply.**

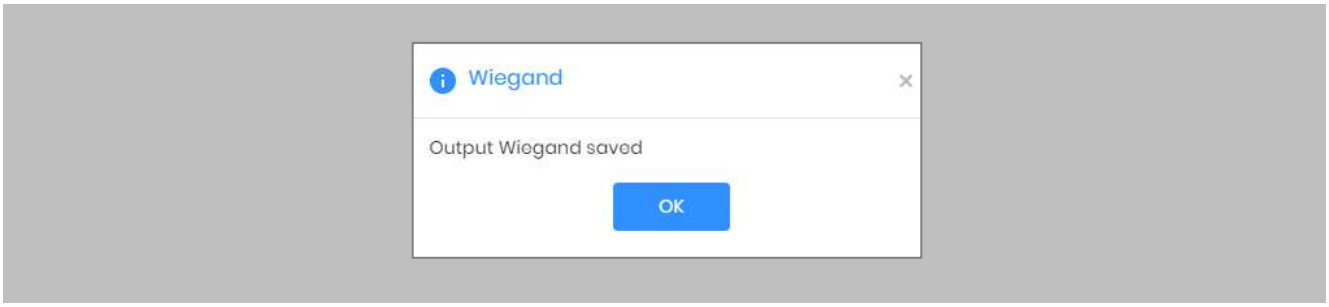


Figure 62: IXM WEB - Save Output Wiegand

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 Gallagher Controller.

- To make this Wiegand output work on Gallagher, you will need to create a UCF (Universal Card Format) for use on the controllers talking to the Invixium reader (by Wiegand or OSDP).

Configure UCF on Configuration Client

Procedure

STEP 1

From the Configuration Client Menu Bar, go to **Configure** → **Universal Card Formats** and create a new UCF as indicated below:

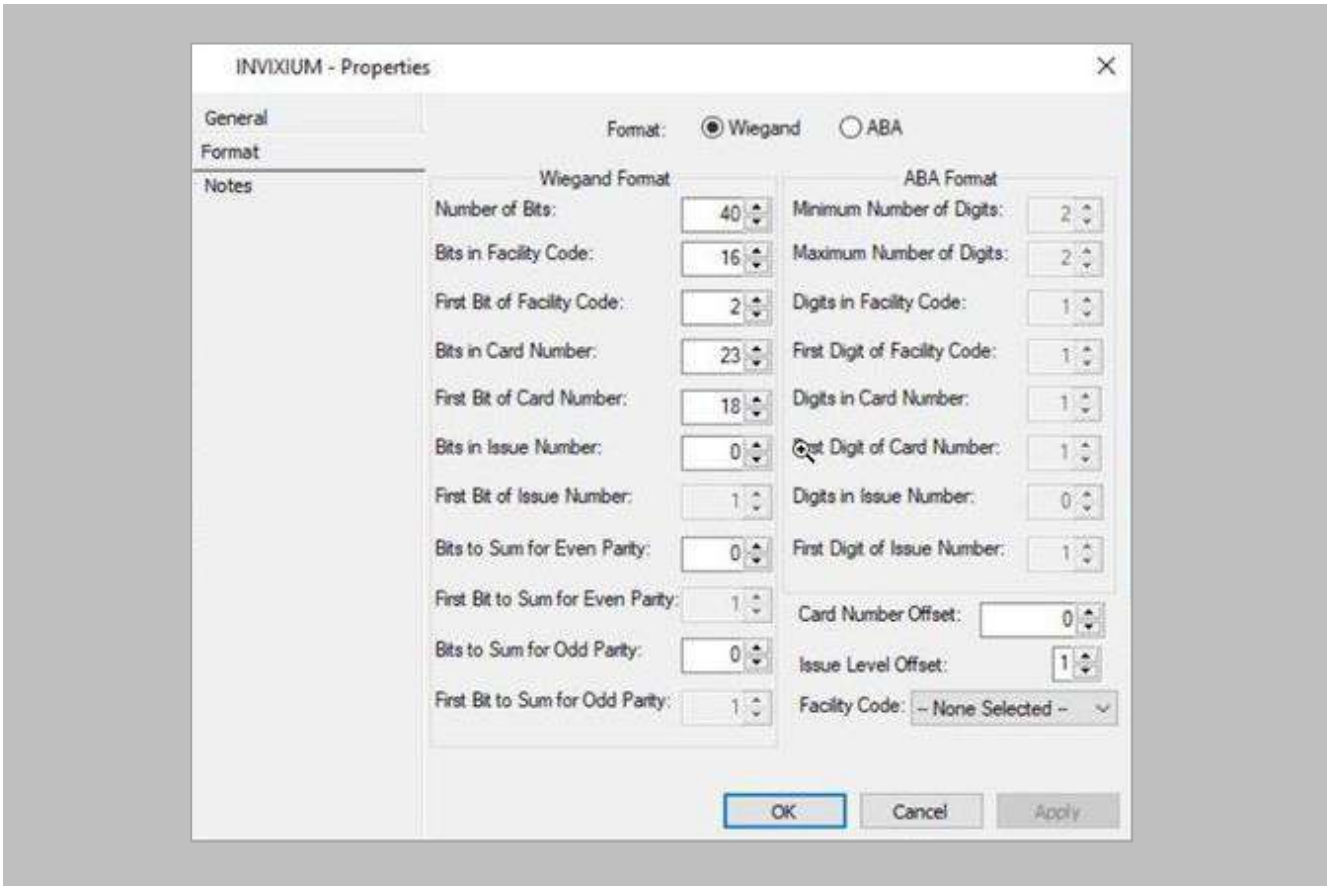


Figure 63: IXM WEB - Configure Universal Card Formats

STEP 2

Click **Apply** and apply to the controller(s) connected to the Invixium reader(s).

Configuring Panel Feedback with Gallagher

Procedure

STEP 1

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

STEP 2

Connect the **LED** of the Gallagher 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**.

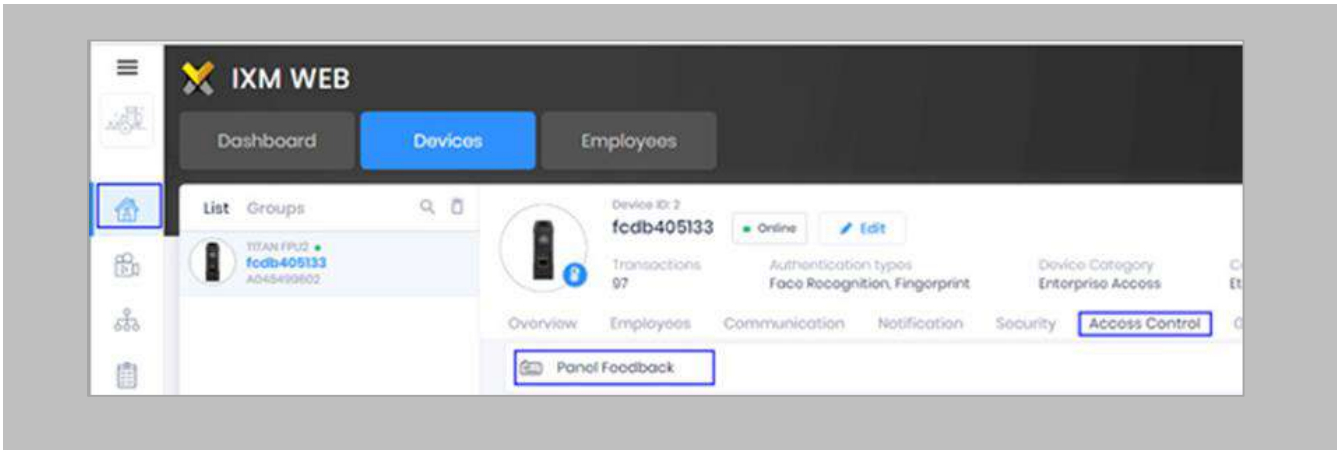


Figure 64: IXM WEB - Panel Feedback

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**.

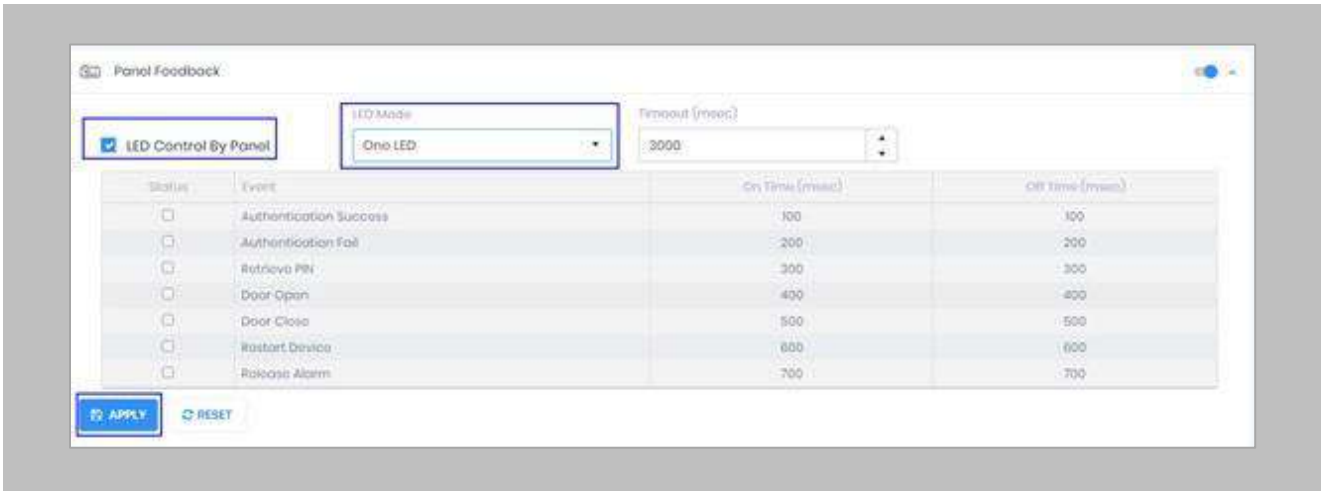


Figure 65: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.

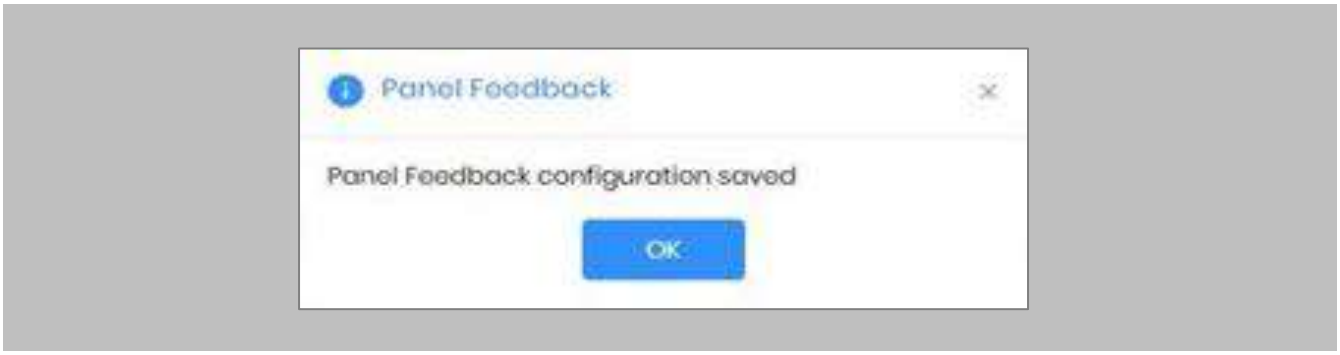


Figure 66: IXM WEB - Save Panel Feedback

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.

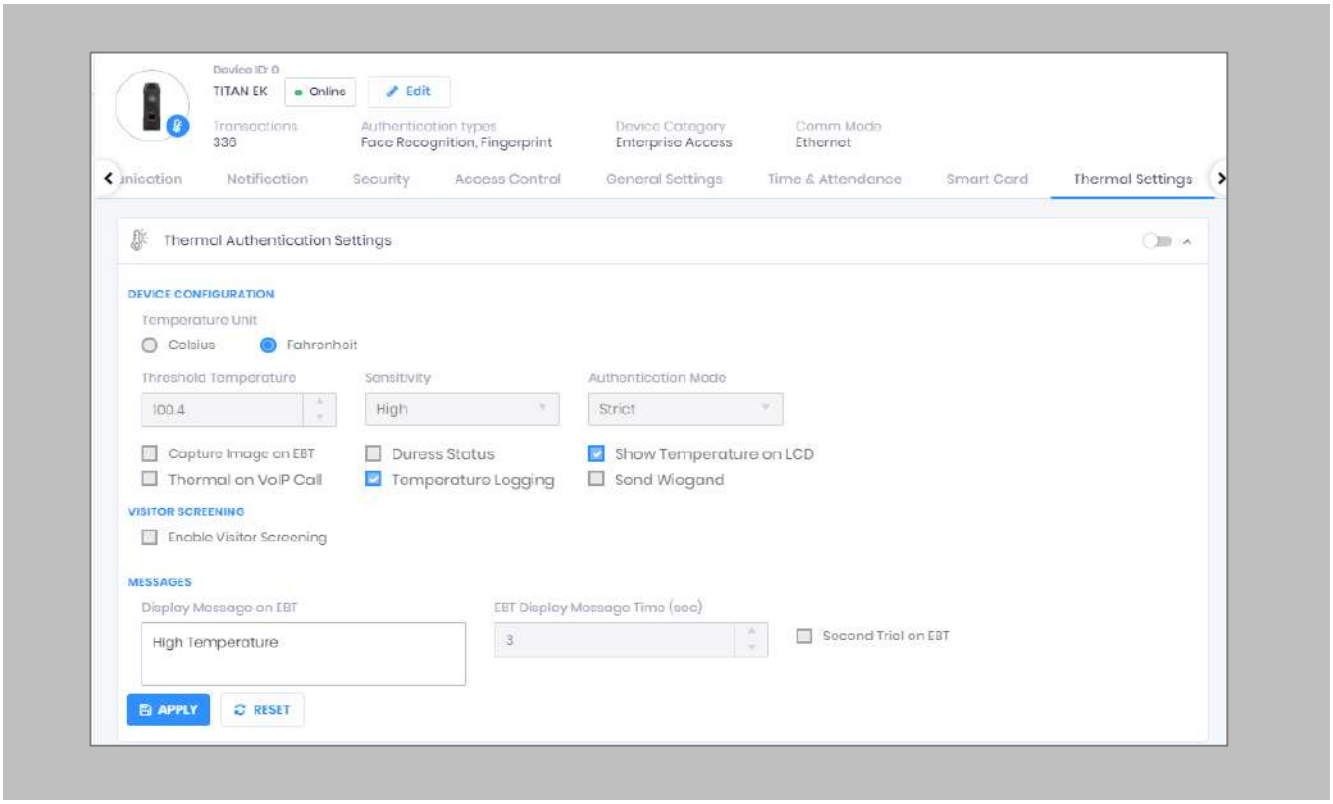


Figure 67: IXM WEB - Thermal Settings

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**.

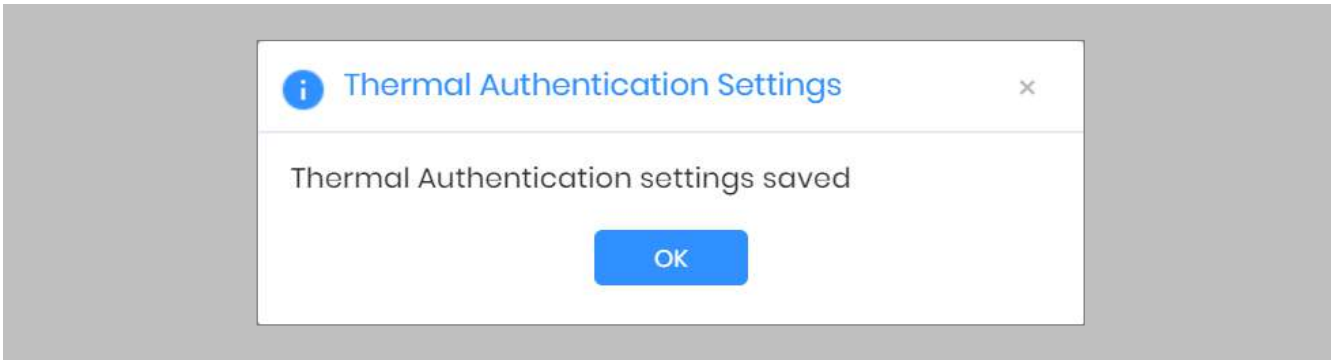


Figure 68: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

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

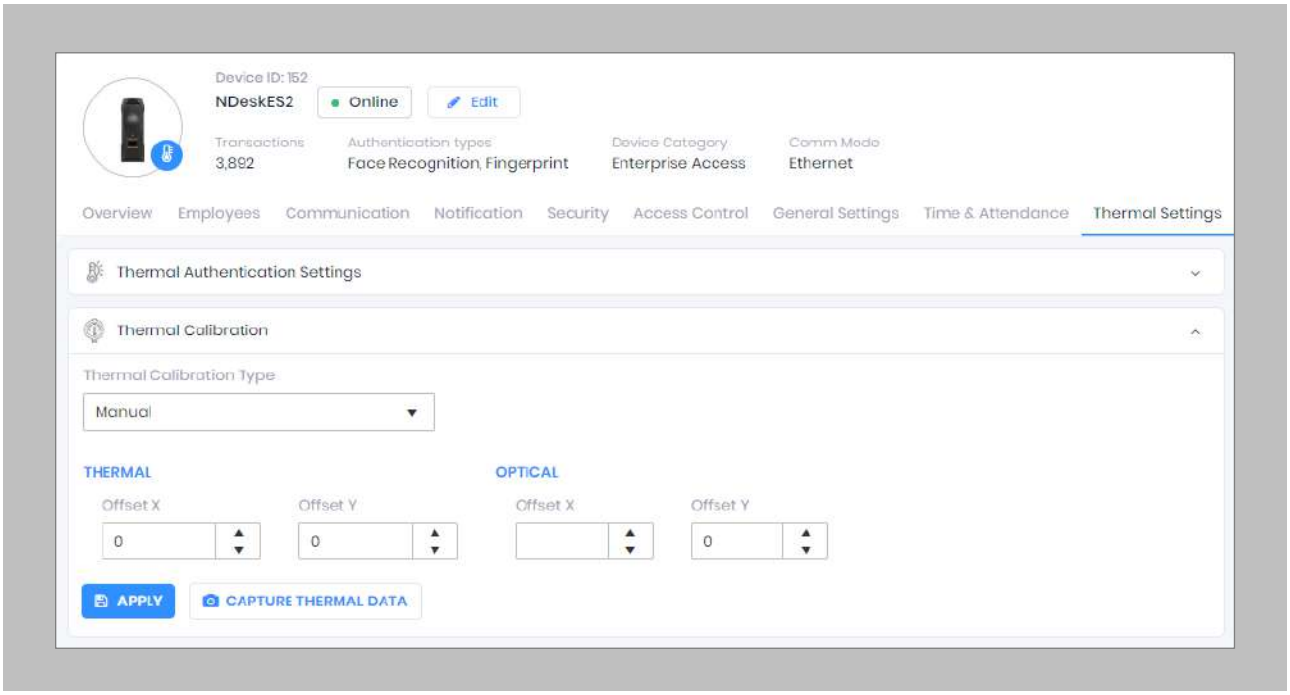


Figure 69: IXM WEB - Thermal Calibration Settings

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**.

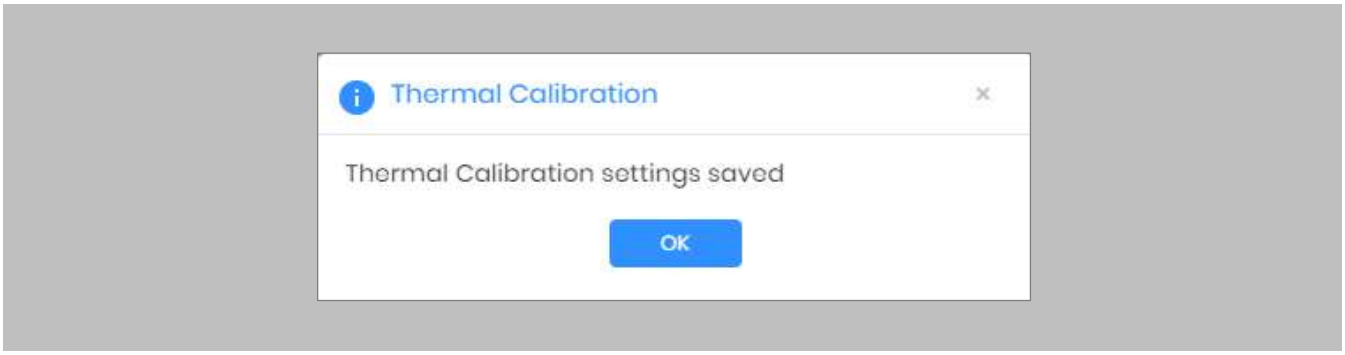


Figure 70: IXM WEB - Save Thermal Calibration Settings

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 71: IXM WEB - Capture Thermal Data

STEP 4

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

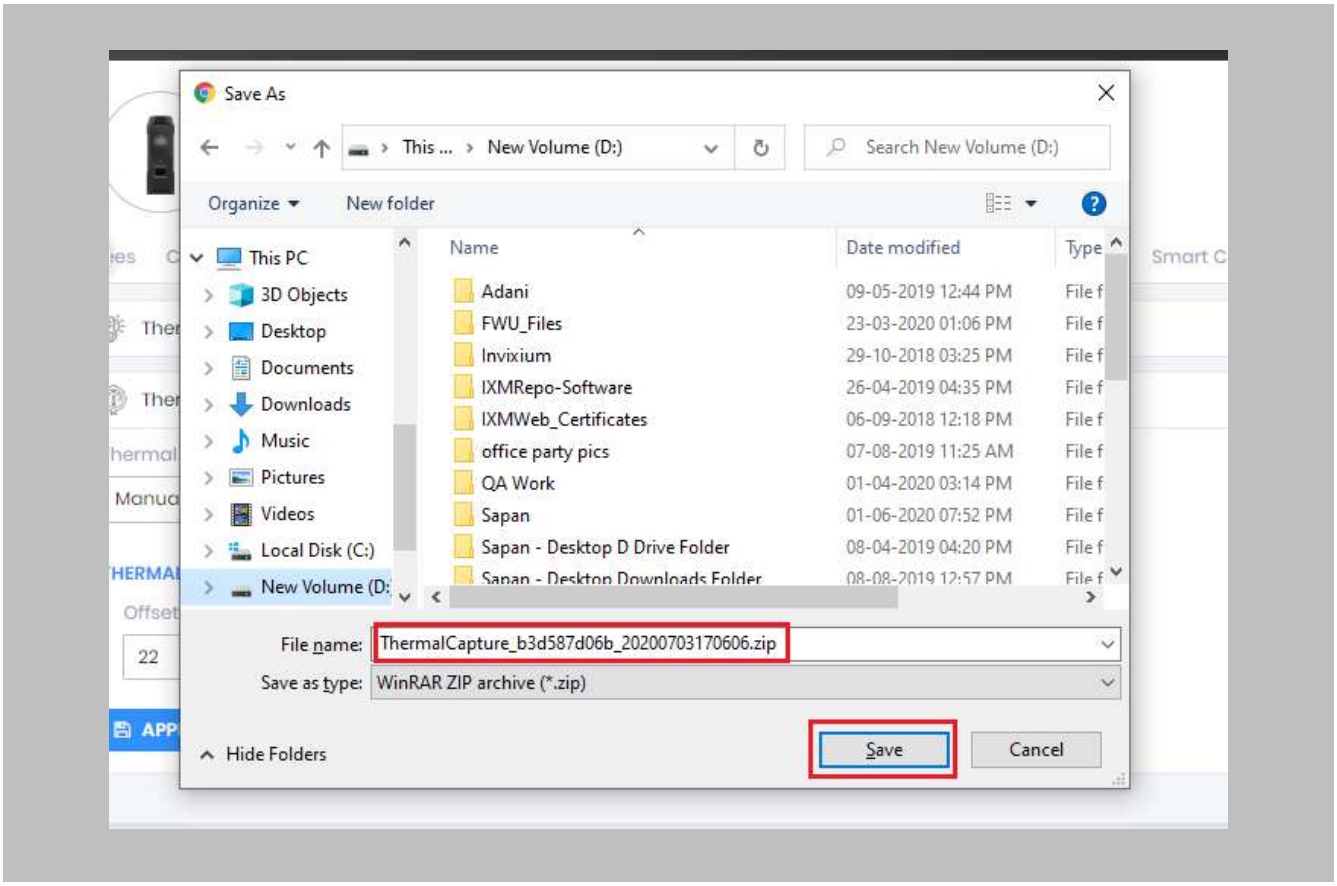


Figure 72: IXM WEB - Save Captured Thermal Data

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**.

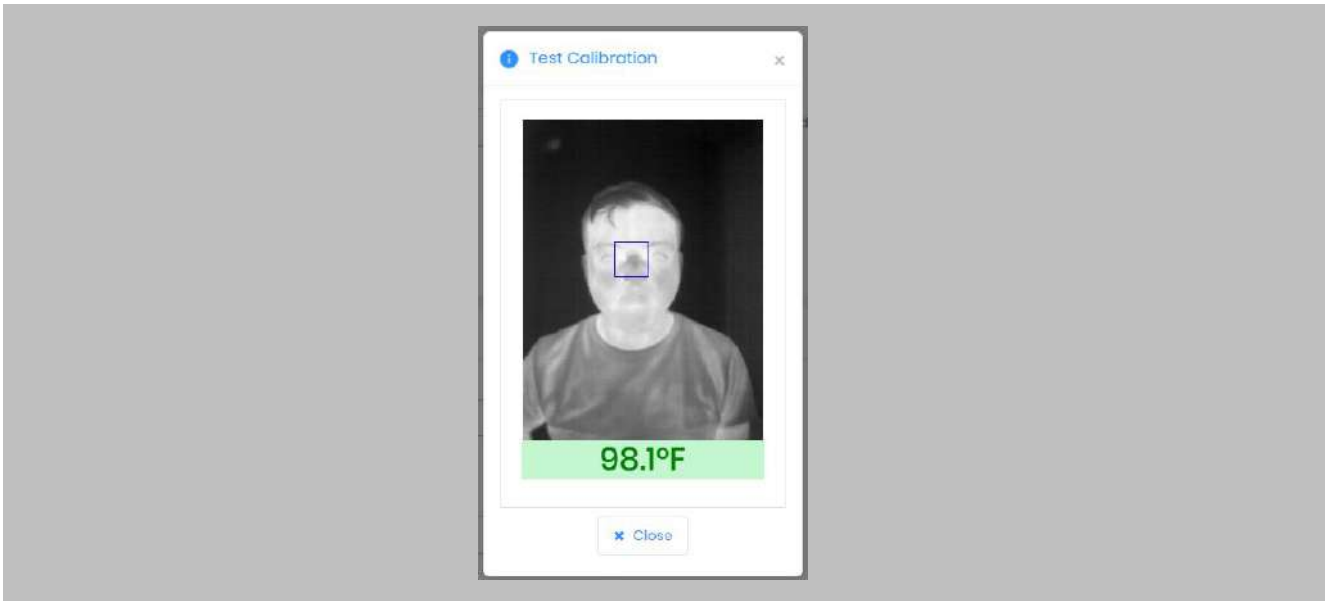


Figure 73: IXM WEB - Test Thermal Calibration

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

Change Temperature Unit Settings

STEP 1

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

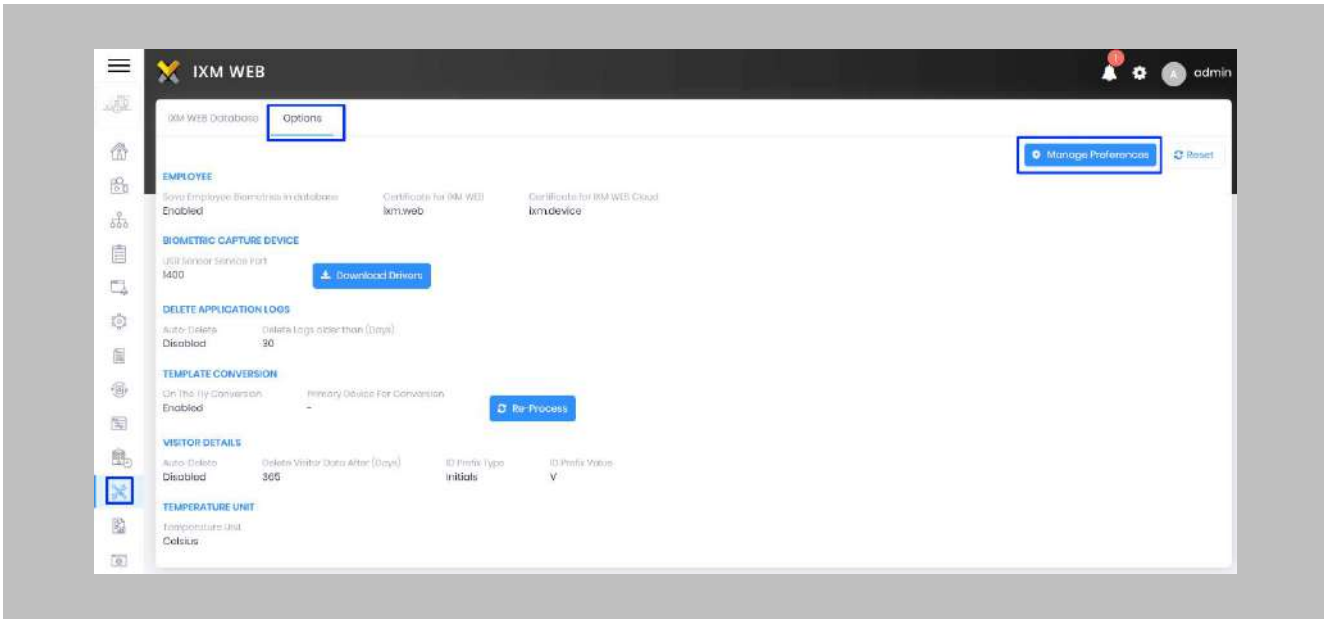


Figure 74: IXM WEB - Option to Change Temperature Unit

STEP 2

Click **Save**.

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

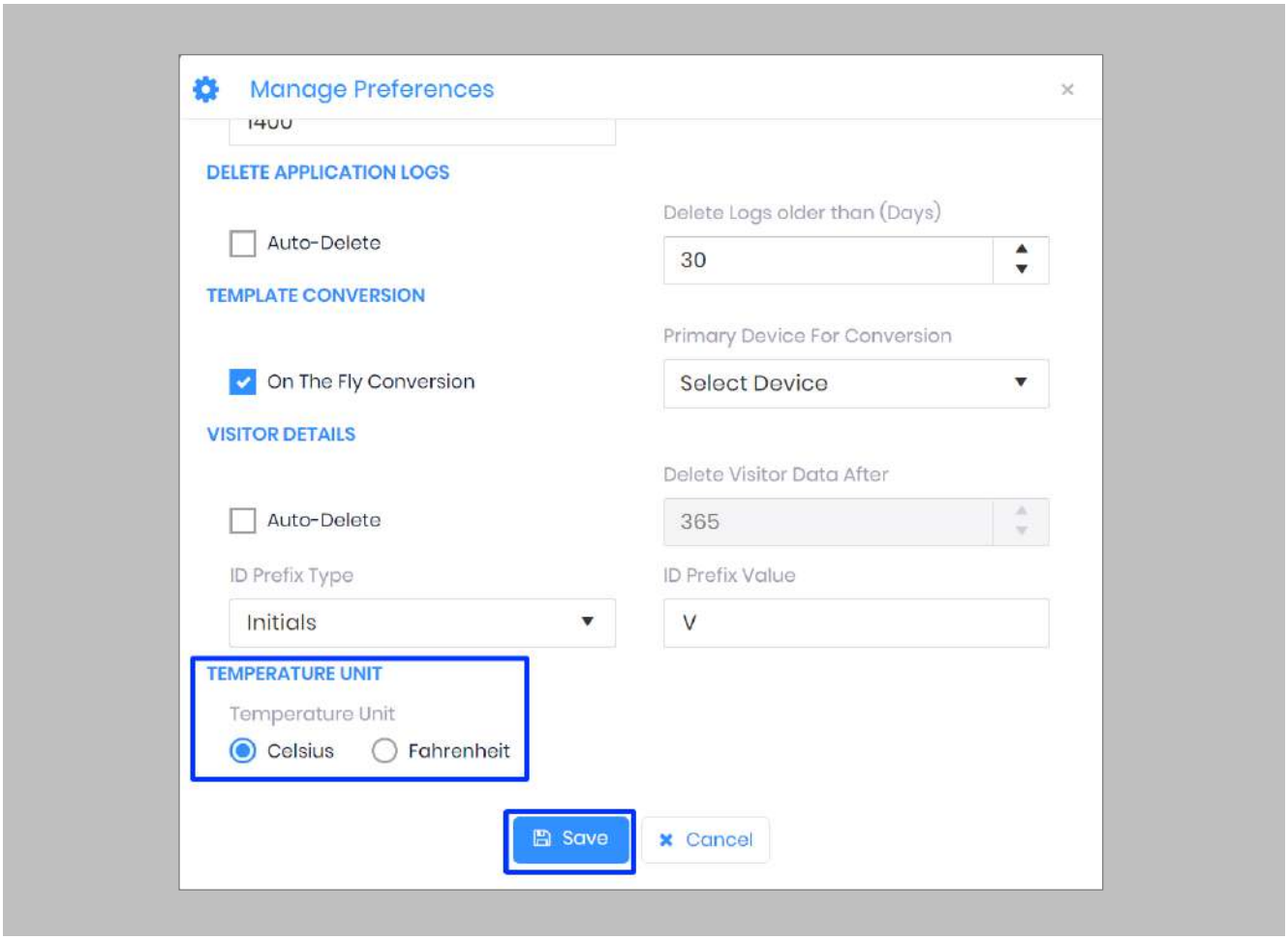


Figure 75: IXM WEB - Save Temperature Unit Setting

Configuring Mask Authentication Settings

STEP 1

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

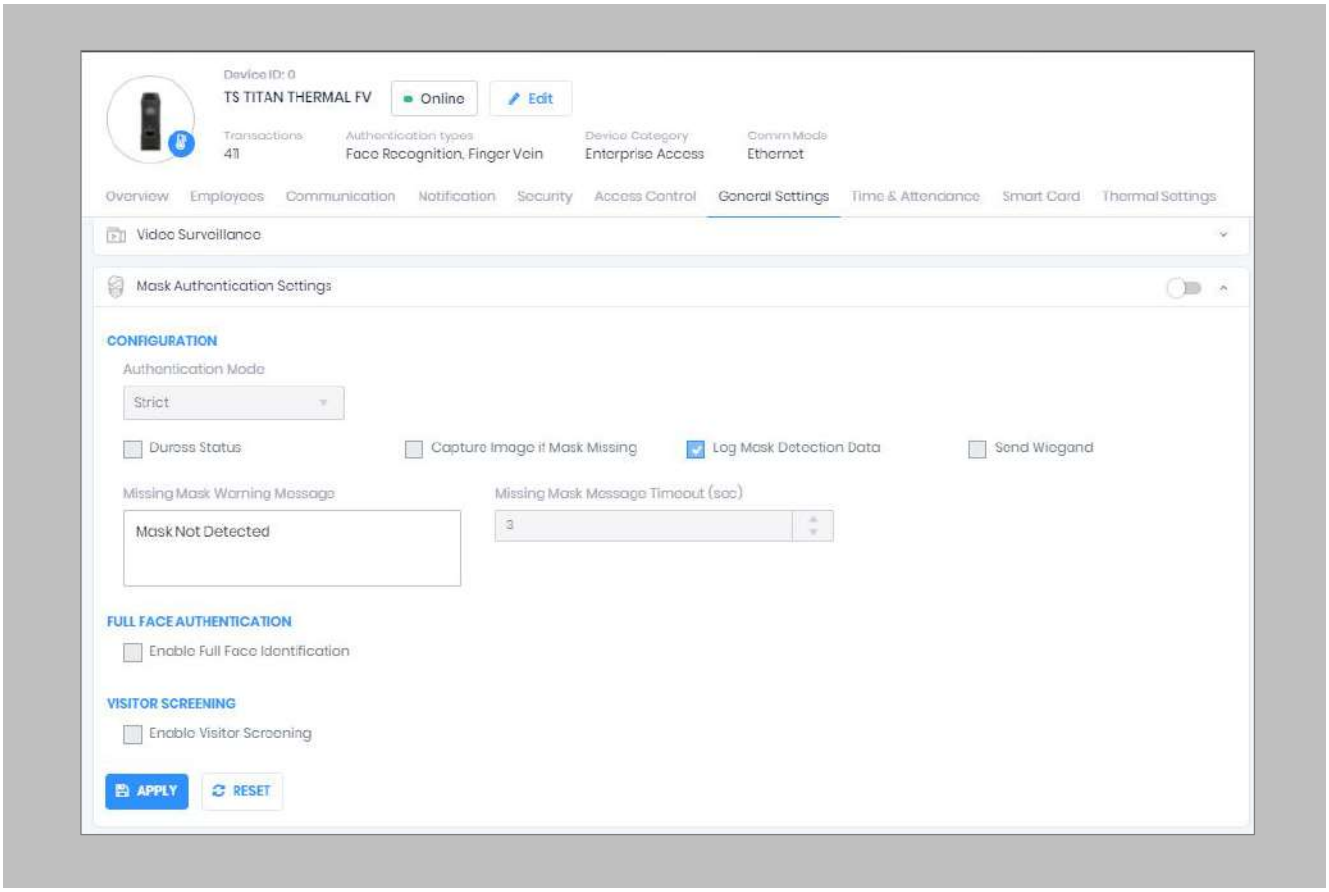


Figure 76: IXM WEB - Mask Authentication Settings

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**.

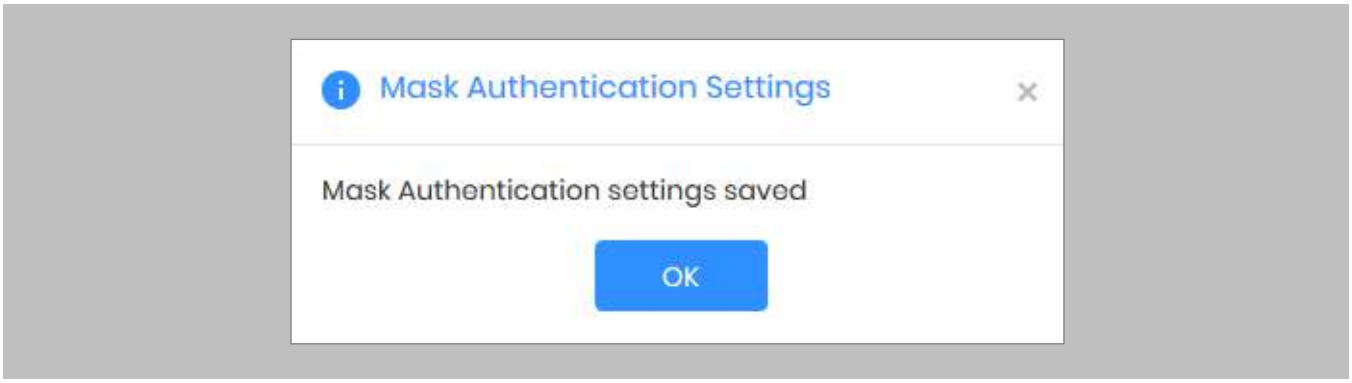


Figure 77: IXM WEB - Save Mask Settings

Pre-configuration for Enrollment

Procedure

STEP 1

Click **Viewers**, then click **New Viewers** under the **Cardholder Viewers** section.

STEP 2

Add a **Value** in the **Name** field.

STEP 3

Select **Division** and the appropriate resolution as per your monitor display settings. Click **Close.**

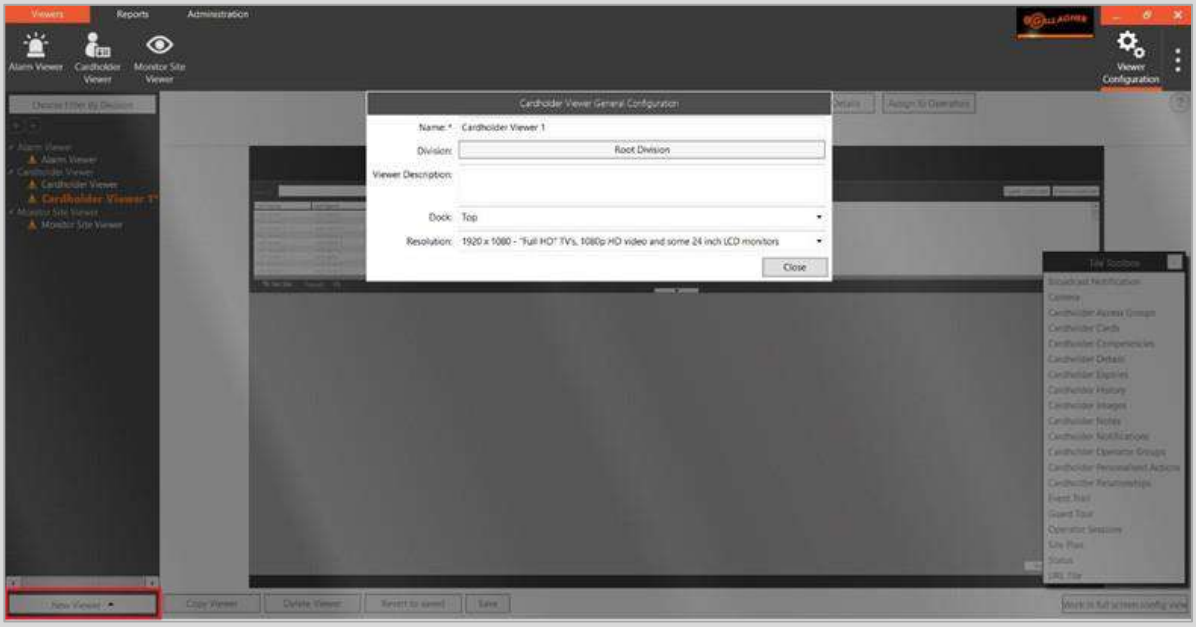


Figure 78: GCC - Cardholder Viewer General Configuration

STEP 4

Drag and drop URL Tile Configuration to **Enrollment Viewer**.

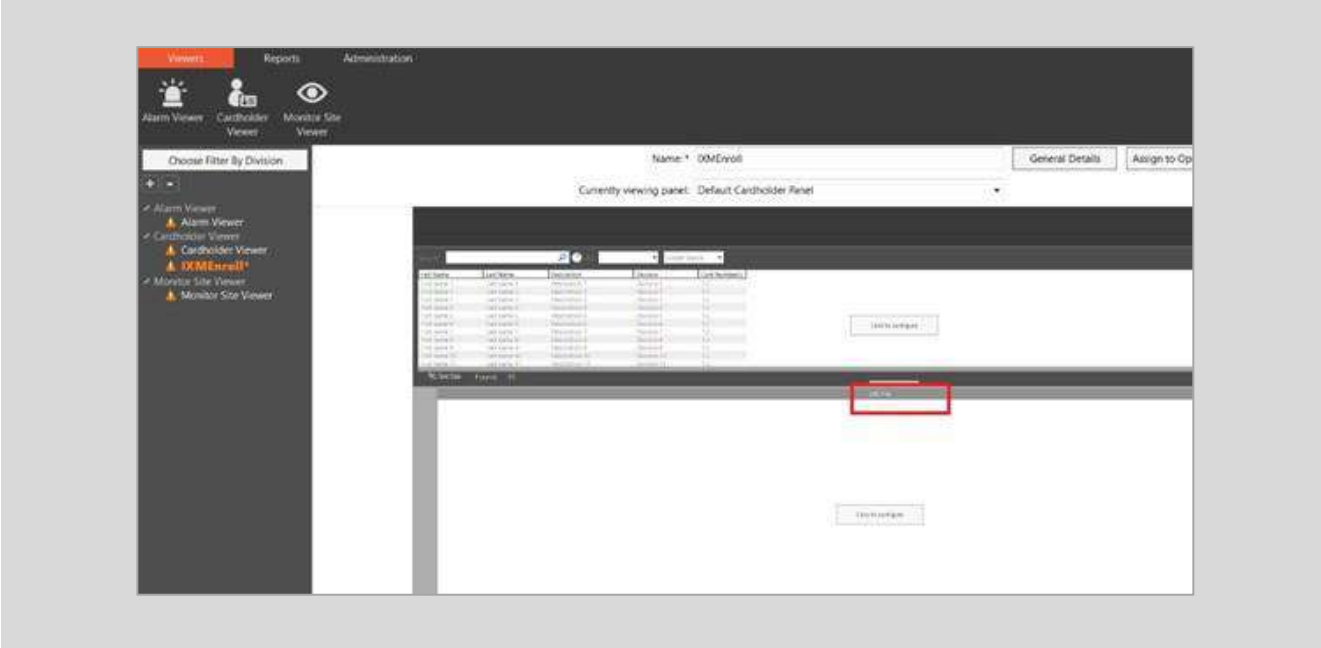


Figure 79: GCC - Enrollment Viewer

STEP 5

Click **Configure** in the URL Tile section.

STEP 6

Select Personal Data Field (PDF) from the **URL Personal Data Field**.

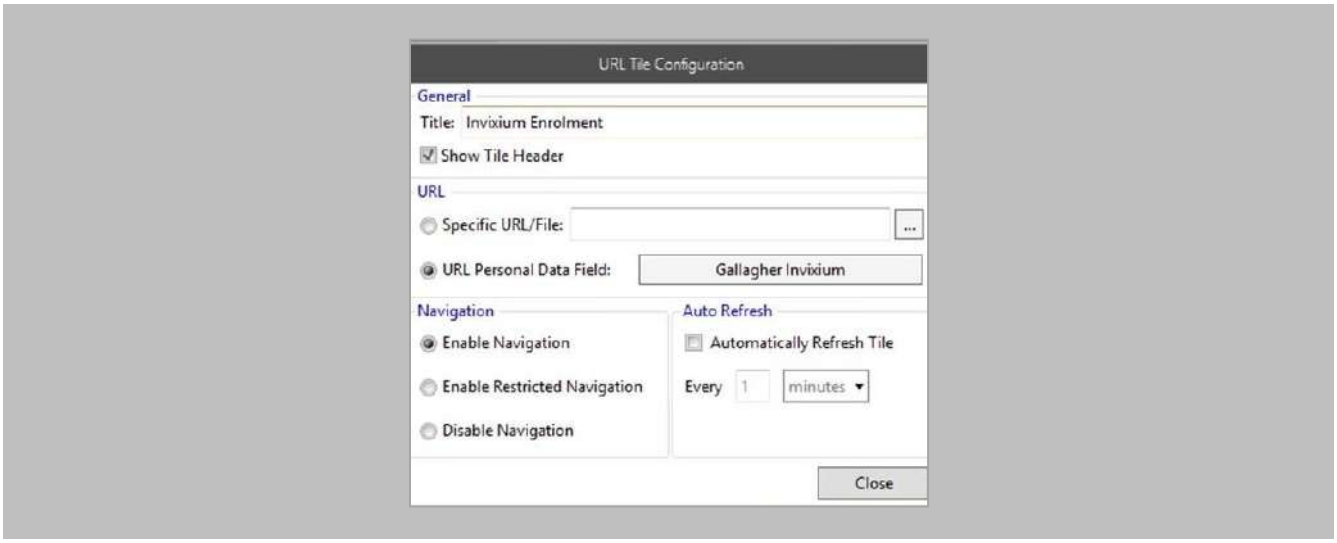


Figure 80: GCC - URL Tile Configuration

STEP 7

Click **Close** to return to the **URL Tile Configuration** view.

STEP 8

Click **Save**.

14. Enrollment from Gallagher Command Centre

When you launch the enrollment viewer for the first time, it will ask for your credentials to log in to IXM WEB. Toggle “Keep Me Signed In” to stay signed in and redirect to the Enrollment screen directly moving forward.

Procedure

STEP 1

When the Enrollment Viewer opens in Command Centre, apply your machine’s display settings to view Enrollment Viewer properly.

Perform enrollment from this viewer option.

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

Other pages of IXM WEB are not compatible to view within GCC 8.40 and 8.50 due to Internet Explorer 9 browser limitations.

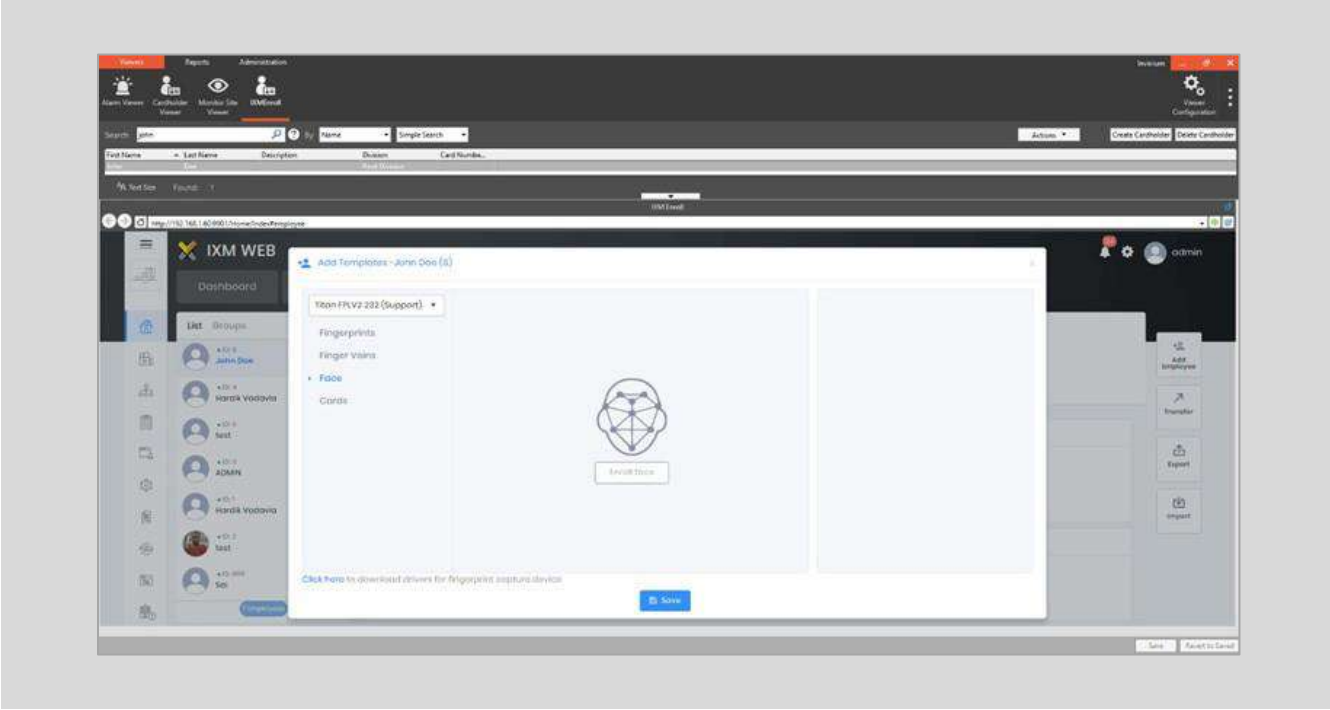


Figure 81: Enrollment Viewer

15. 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.

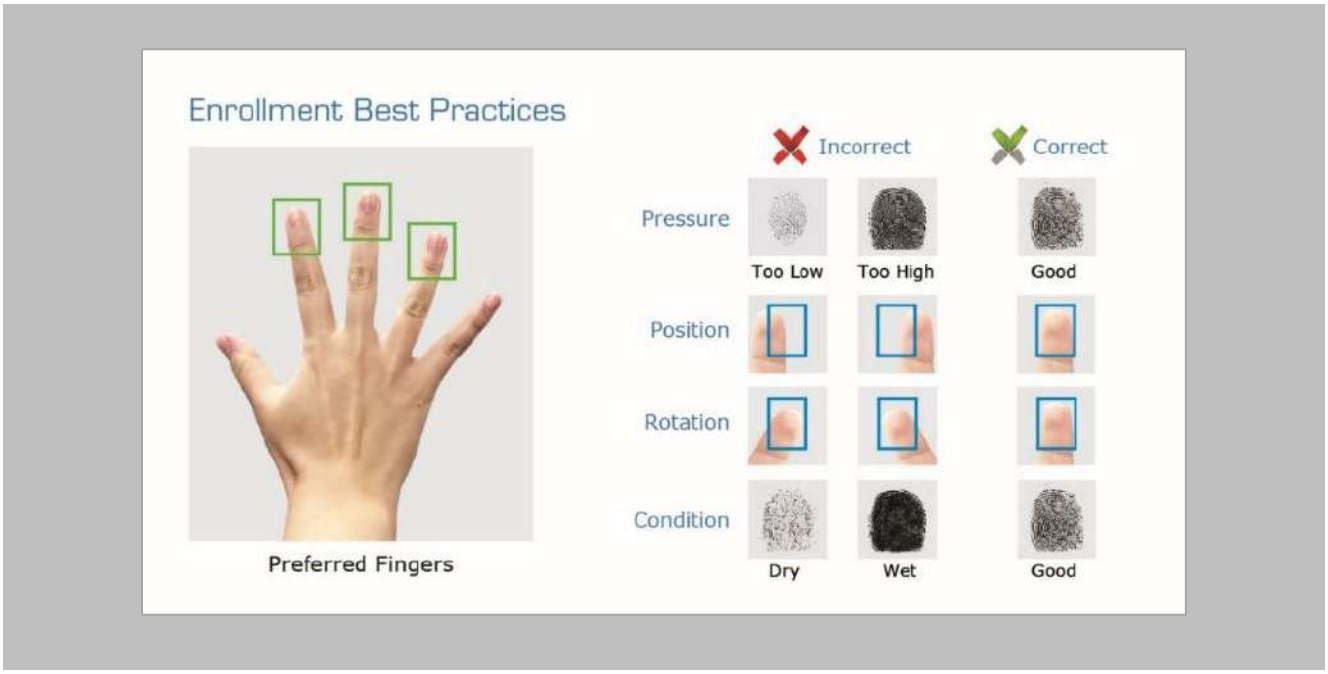


Figure 82: Fingerprint Enrollment Best Practices

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 83: 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.

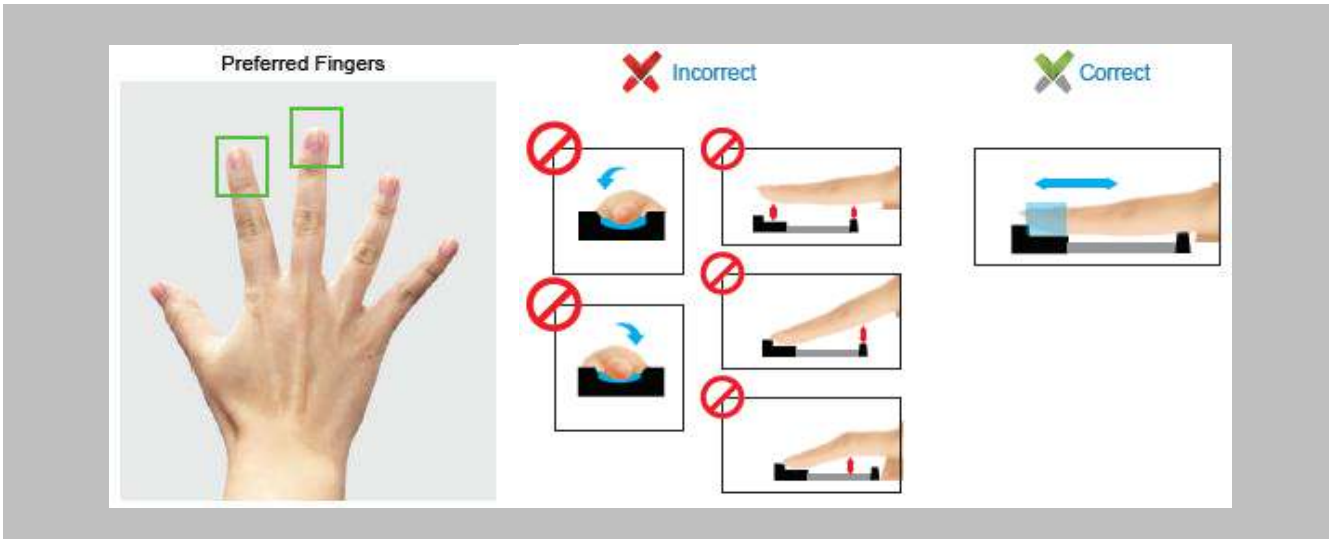


Figure 84: Finger Vein Enrollment Best Practices

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.

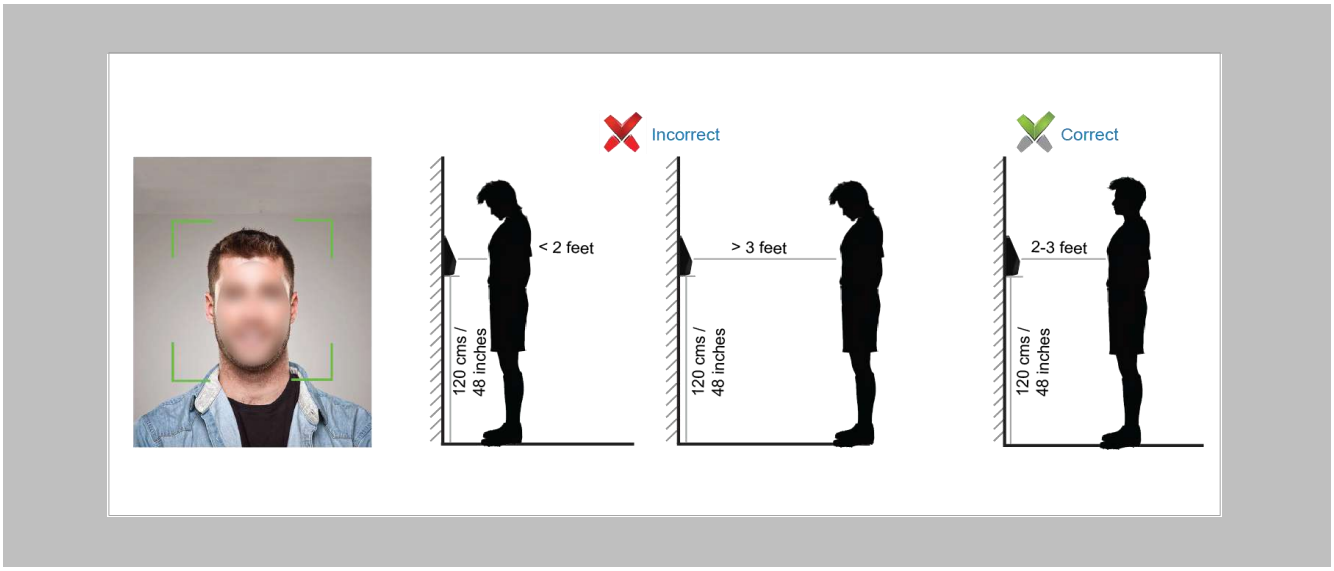


Figure 85: Face Enrollment Best Practices

16. Send Logical Events to Command Centre

The following settings are required in Command Centre to receive logical events for two events “Temperature test fail” and “No face mask” from IXM WEB.

Note:

1. Invixium and Gallagher strongly recommend performing a backup before performing this step!
2. This alarm event-response configuration is suitable for sites with one reader configured for a single door and for sites where there are more than 2 readers associated with one door. The alarm event response will only trigger for the reader with the same name as the door in GCC.

Procedure

STEP 1

IXM WEB requires an External Event Group named Invixium to be present in Command Centre. This could be done using the event utility provided in the installation path. Invixium recommends skipping the first 10 pre-existing External Event Groups and changing the name of 11th or any other to Invixium.

STEP 2

In the Invixium External Event Group, add two events named Temperature Event and Mask Event.

STEP 3

IXM WEB will report events with doors named after devices in IXM WEB. For example, if a device is named Main Entrance in IXM WEB, there should be a door named Main Entrance in Command Centre. Assign proper alarms and access zones accordingly.

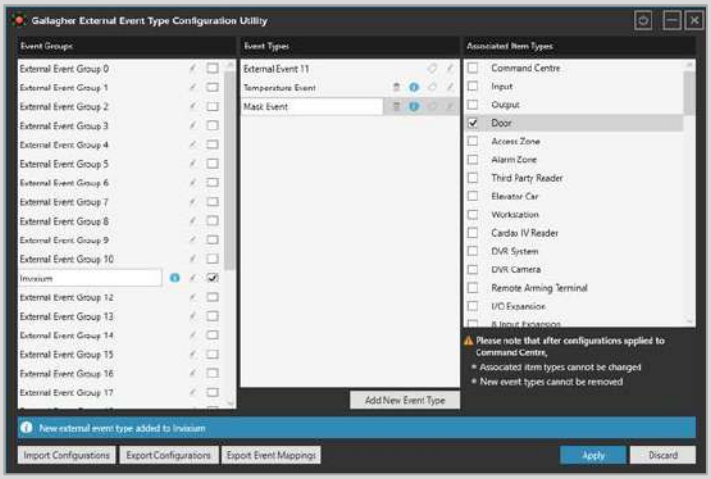


Figure 86: GCC - Gallagher External Event Type Configuration Utility

STEP 4

EBT and mask events will be picked up from **EBTEventDetails** and sent to Gallagher.

Note: If an employee violates both mask and temperature rules, then both events will be reported to Command Centre.

STEP 5

In Command Centre, these events can be seen in **Event Monitor** and the cardholder's notes.

STEP 6

Cardholder's notes are reported for **Employees** present in **IXM WEB** and not for **Visitors**.

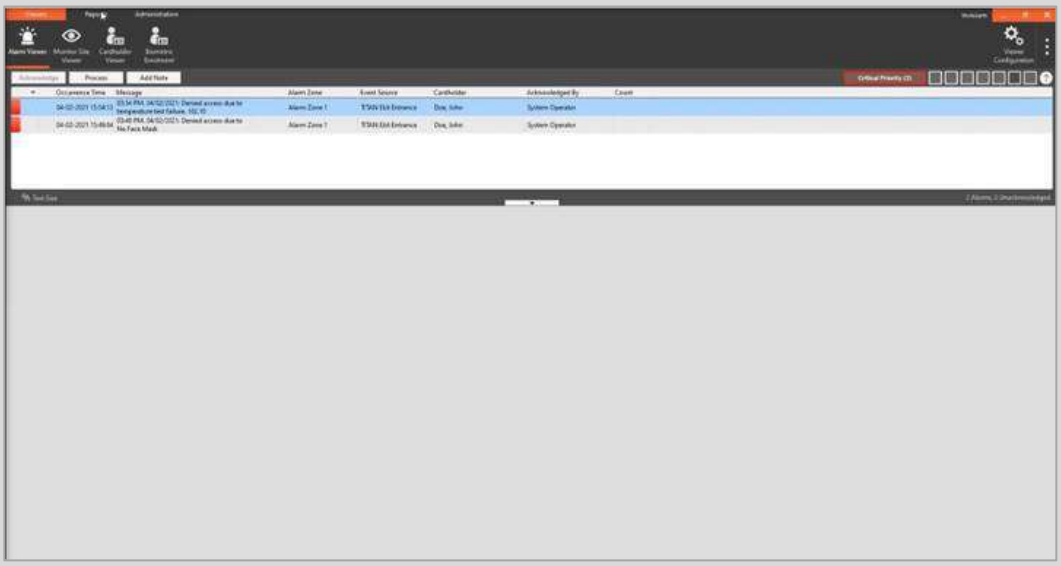


Figure 87: GCC - Cardholder’s Notes

17. 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**

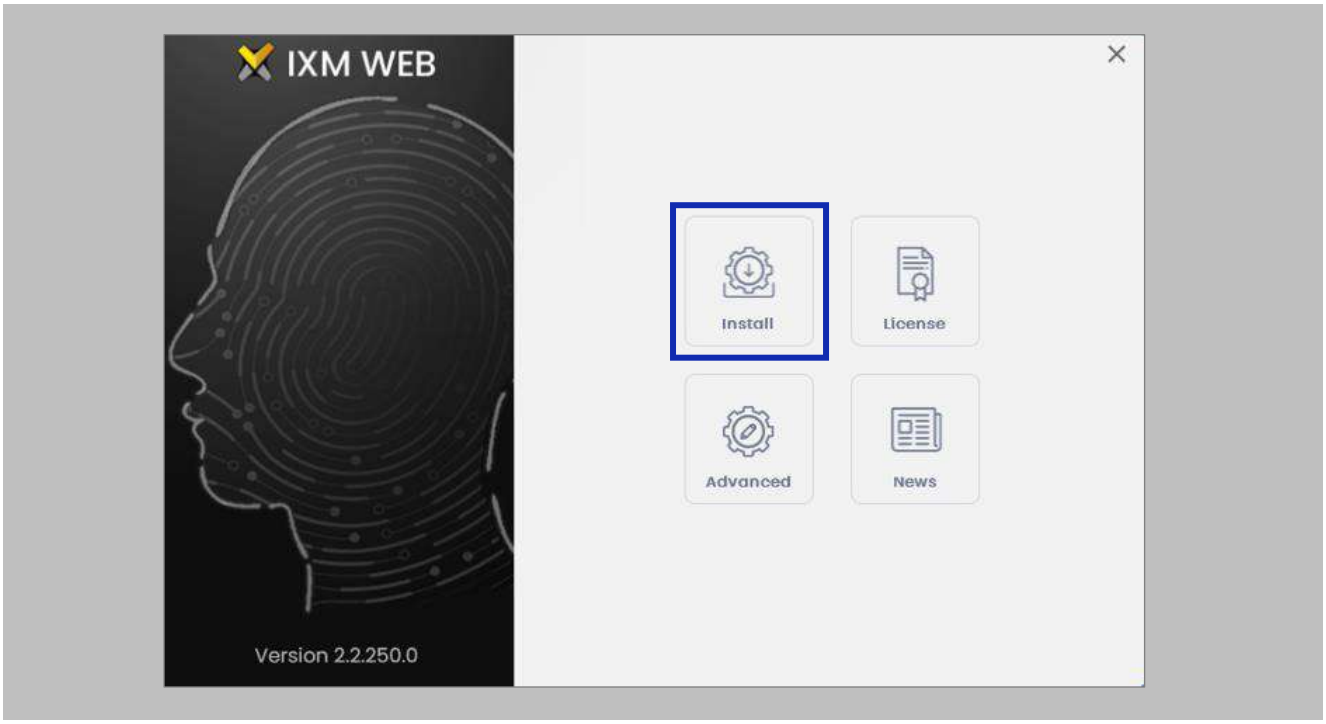


Figure 88: Install IXM WEB

Note: Installs SQL 2014 Express.

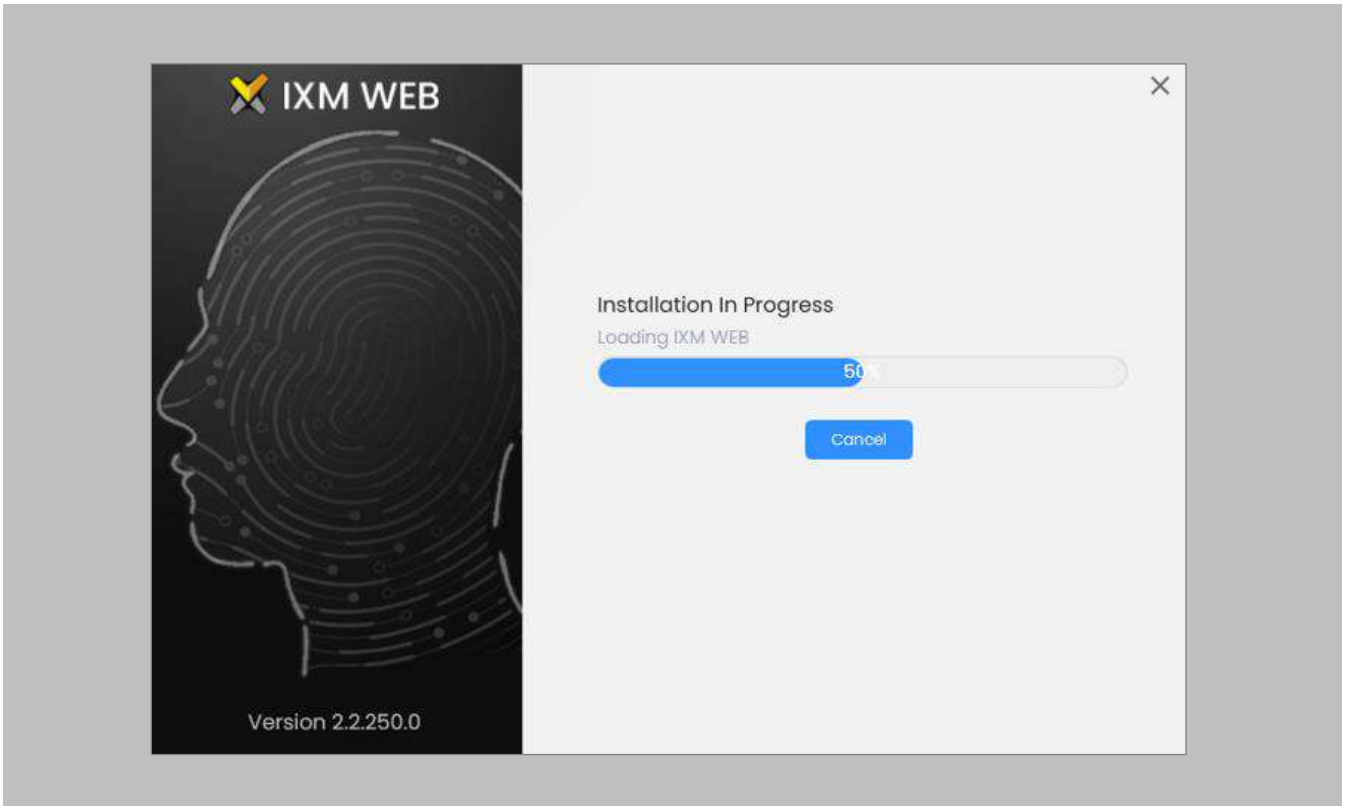


Figure 89: Loading SQL Express & Installation Progress

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.

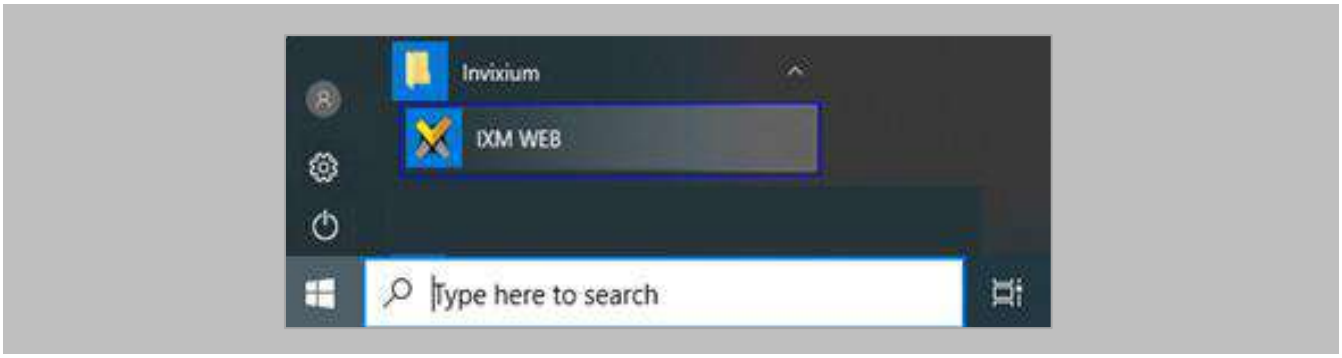


Figure 90: IXM WEB - Shortcut Icon on Desktop

STEP 4

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

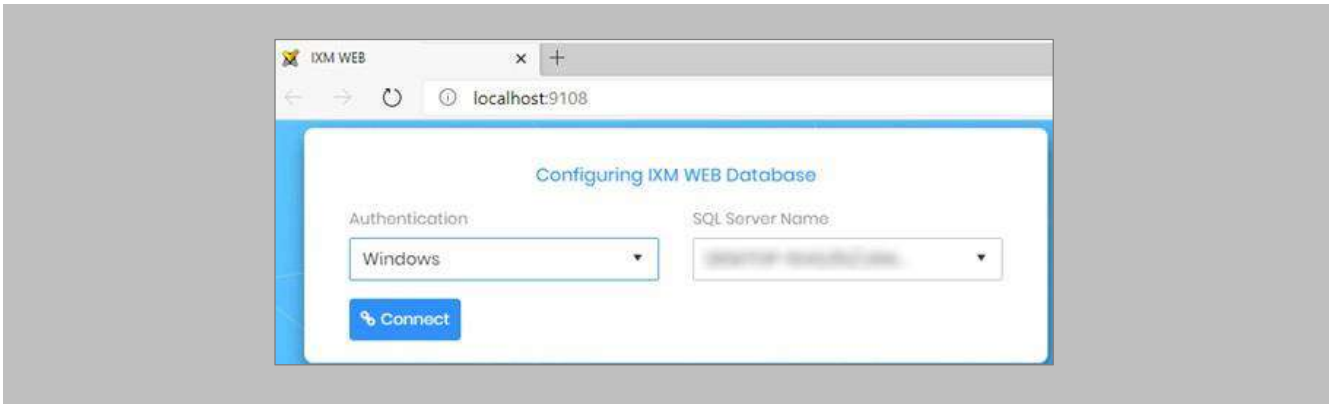


Figure 91: IXM WEB - Configuring IXM WEB Database

STEP 5

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

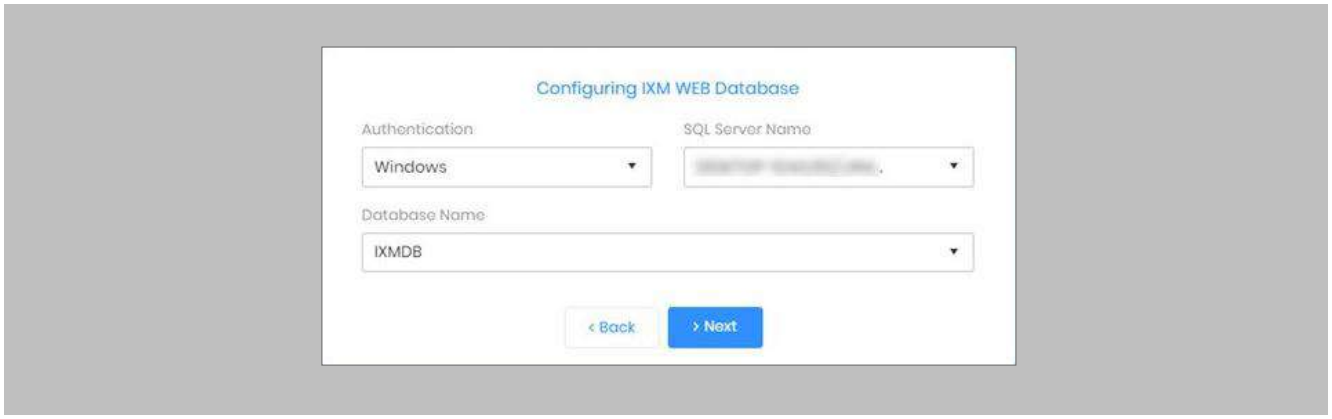


Figure 92: IXM WEB - Select Database Name

STEP 6

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

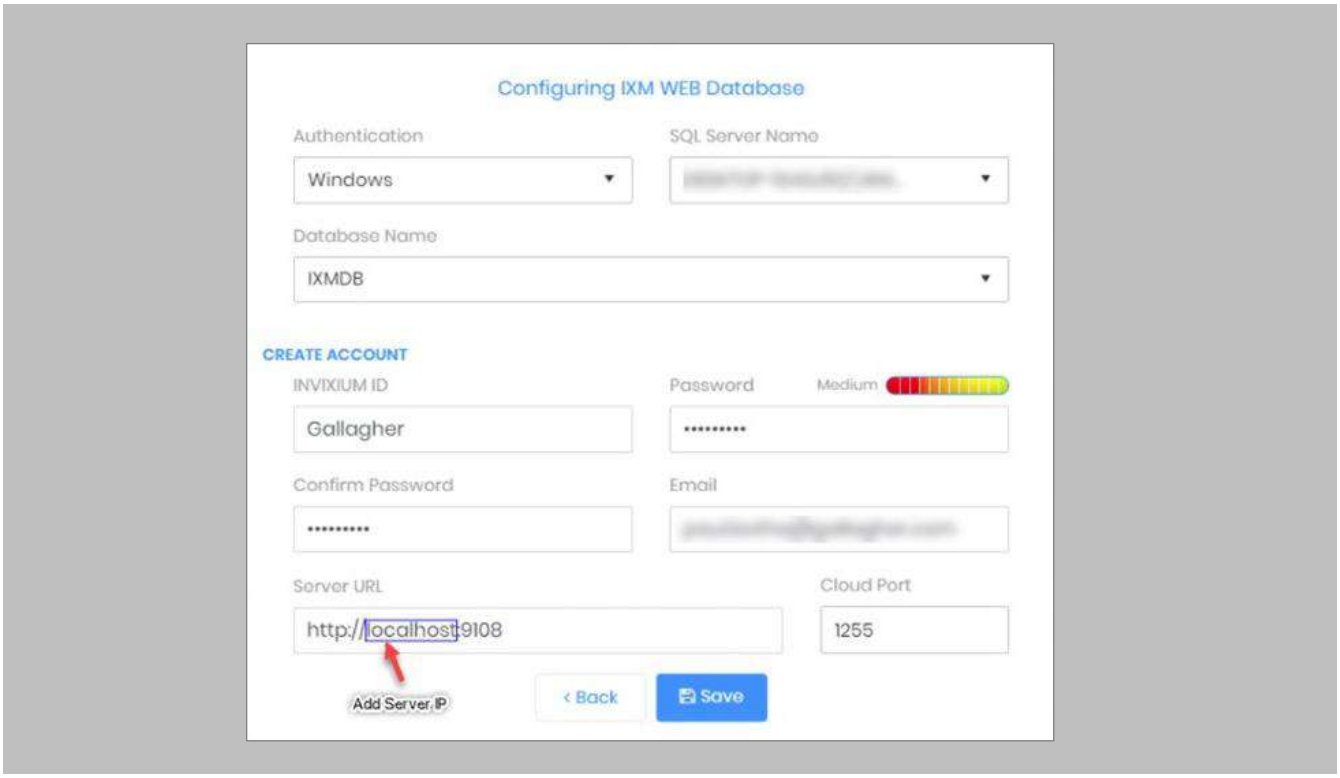


Figure 93: IXM WEB - Server URL format

STEP 7

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

Pushing Configuration to Multiple Invixium Readers

Procedure

STEP 1

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

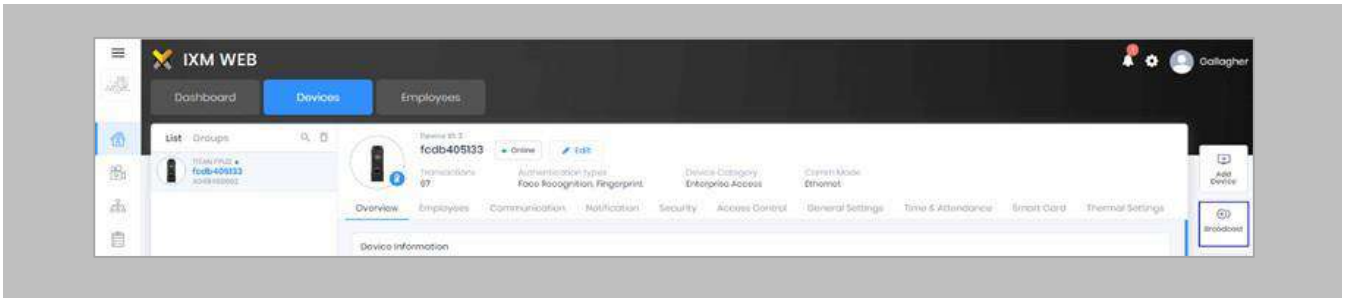


Figure 94: IXM WEB - Broadcast Option

STEP 2

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

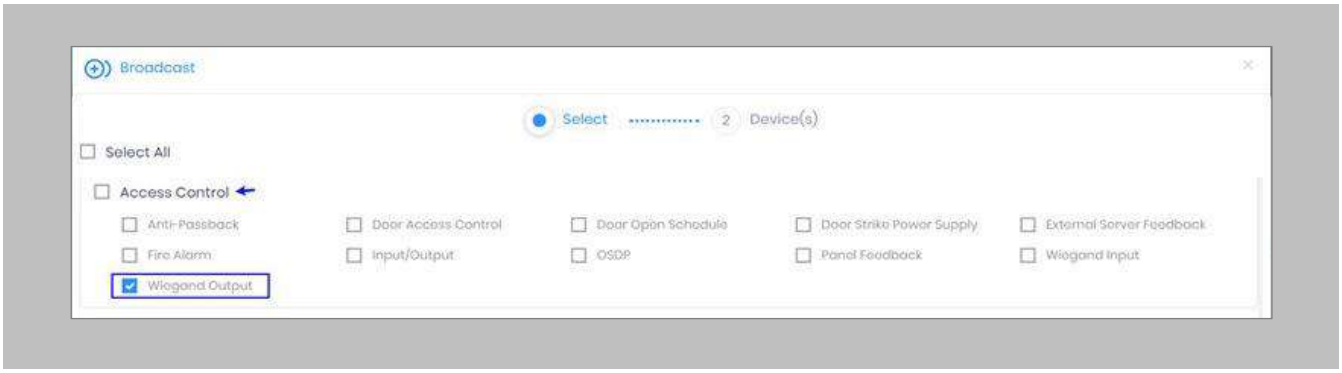


Figure 95: IXM WEB - Wiegand Output Selection in Broadcast

STEP 3

Click **Broadcast.**

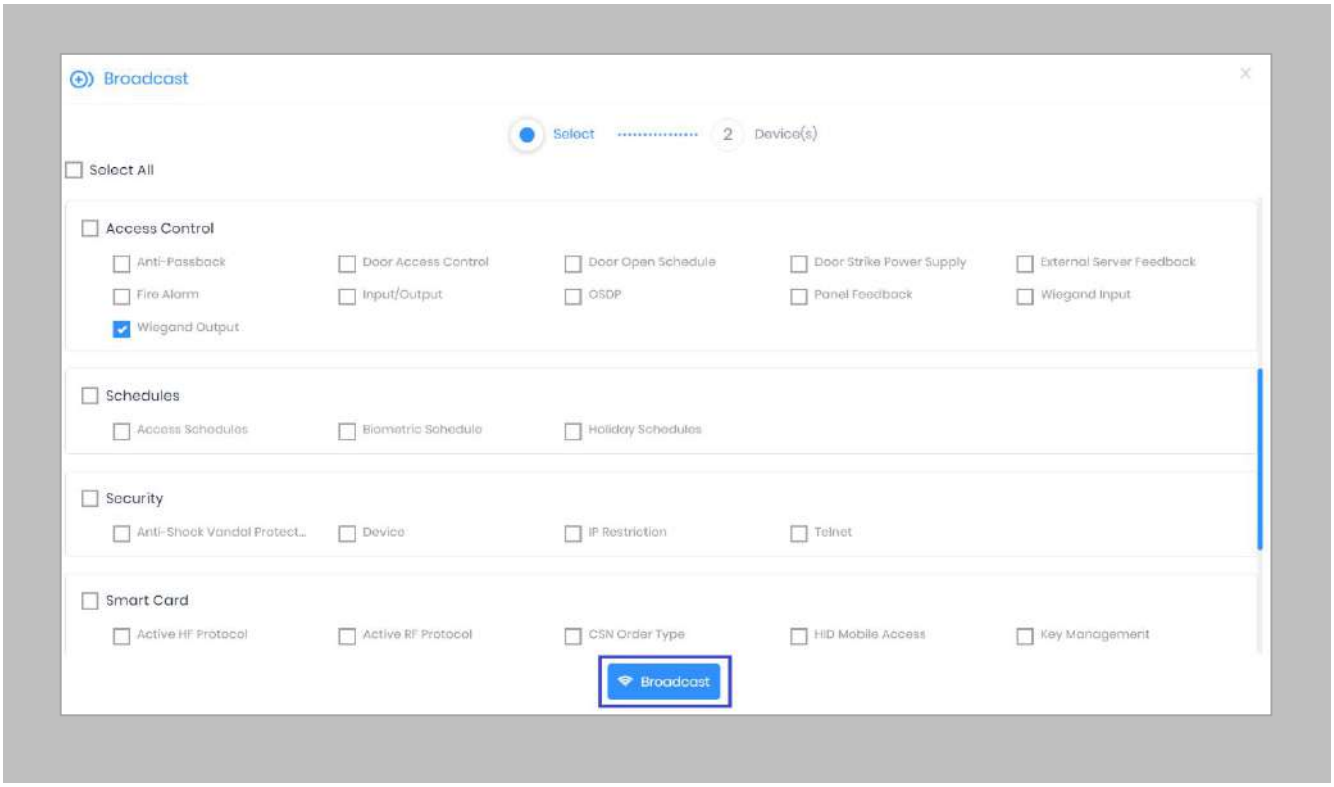


Figure 96: IXM WEB - Broadcast Wiegand Output Settings

STEP 4

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

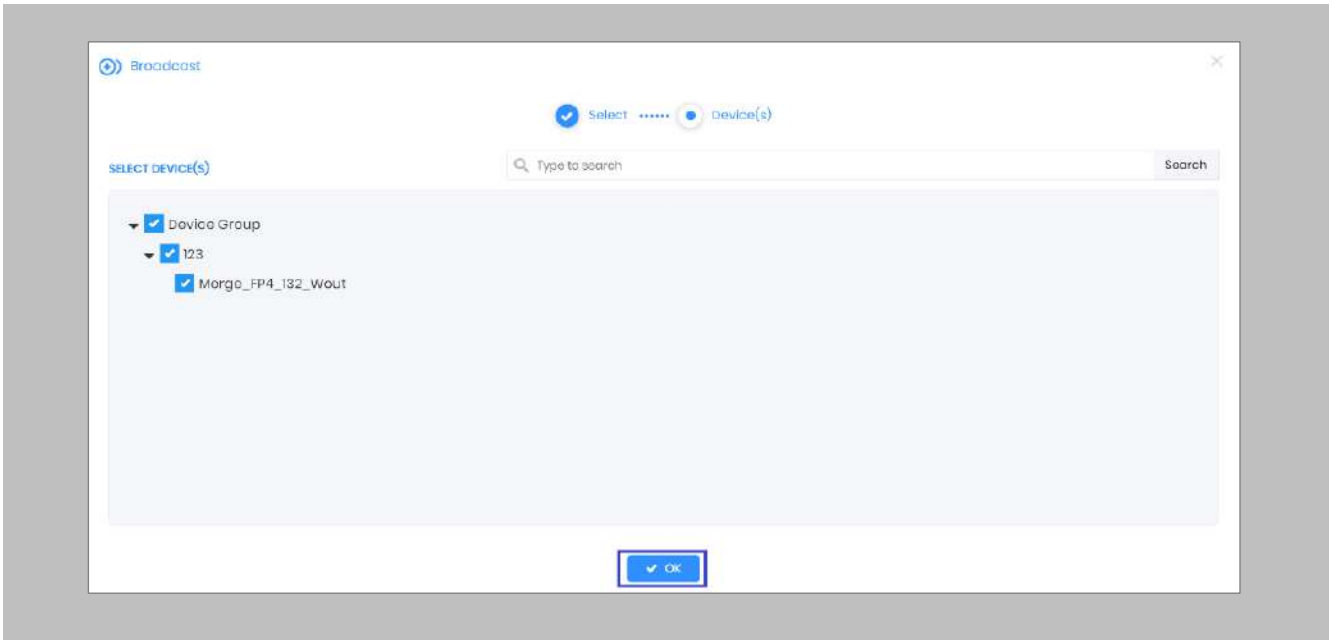


Figure 97: IXM WEB - Broadcast to Devices

Configuring for OSDP Connection

STEP 1

From **Home**, click 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**.

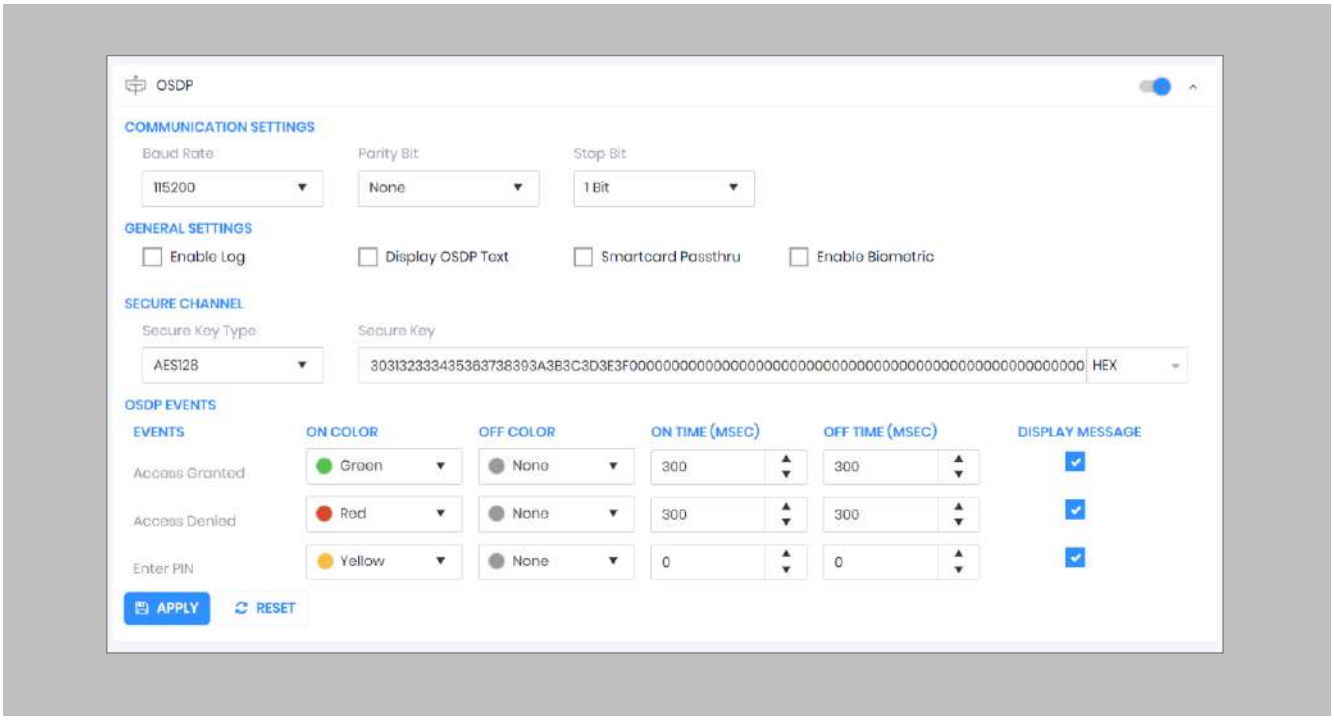


Figure 98: IXM WEB - OSDP Settings

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
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

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.

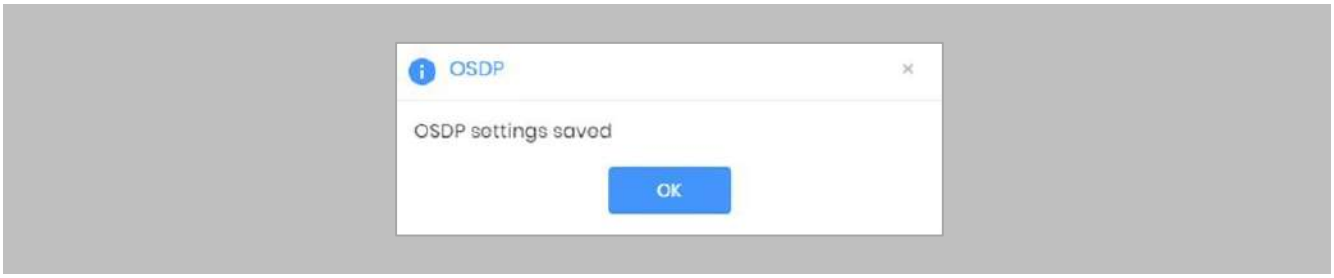


Figure 99: IXM WEB - Save OSDP Settings

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 Command Centre.

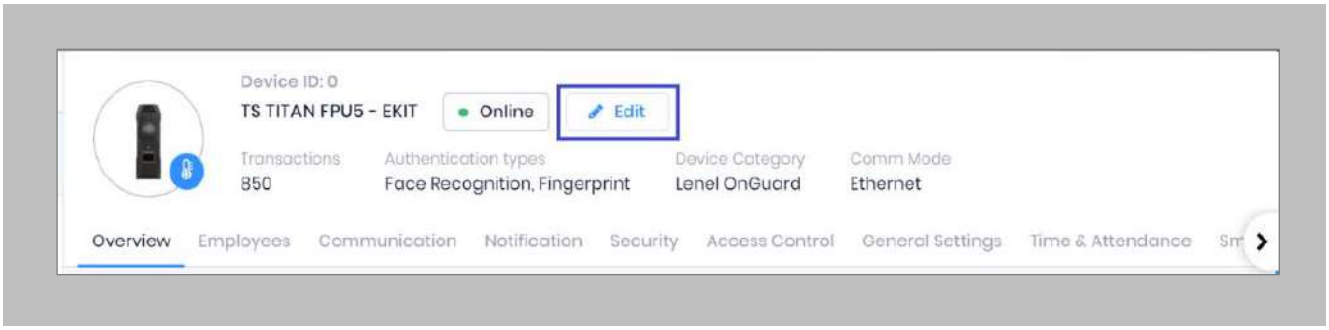


Figure 100: IXM WEB - Edit Device

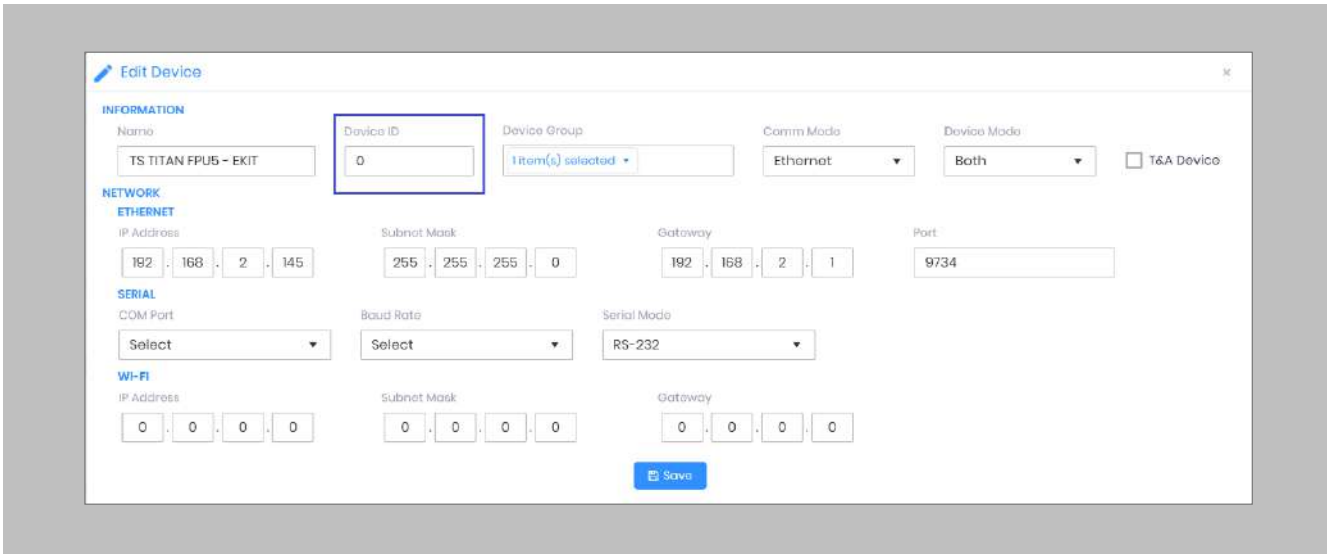


Figure 101: IXM WEB - Edit Device Options

STEP 5

Create a new **OSDP** reader in the Configuration Client. Open the properties of the controller the reader is connected to (ensuring the port the reader is connected to has been configured for OSDP). Drag the reader into the OSDP Devices tab and select the **Device ID** in the Address column. Click **Apply**.

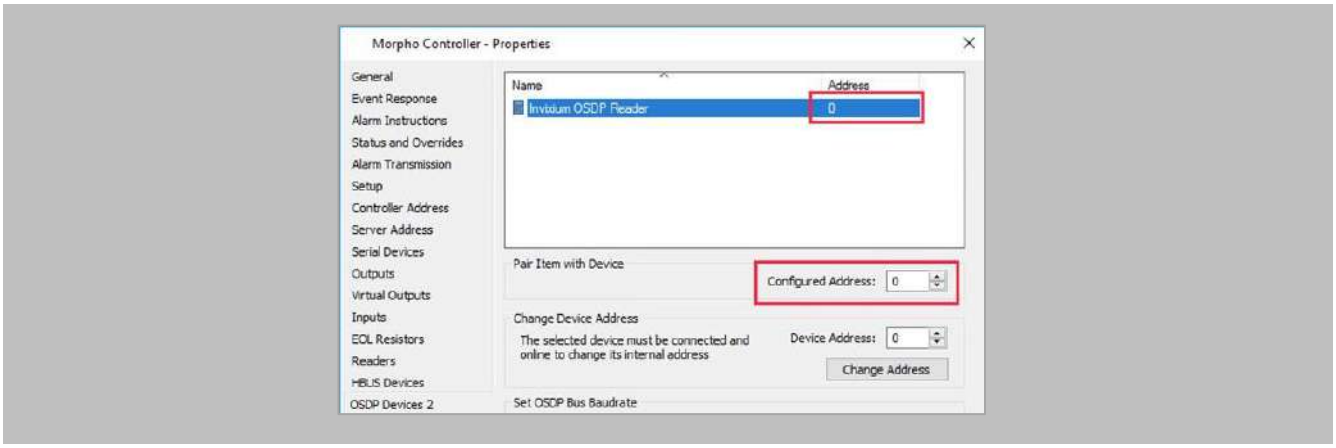


Figure 102: GCC - Device ID

Note: Change the address of the Invixium reader from within the Invixium software and not from the change address option from within Command Centre.

STEP 6

Optional: Enable encryption from the **Advanced** tab of the reader properties within Command Centre and click **Apply** - the reader will drop offline while it changes to encrypted communications.

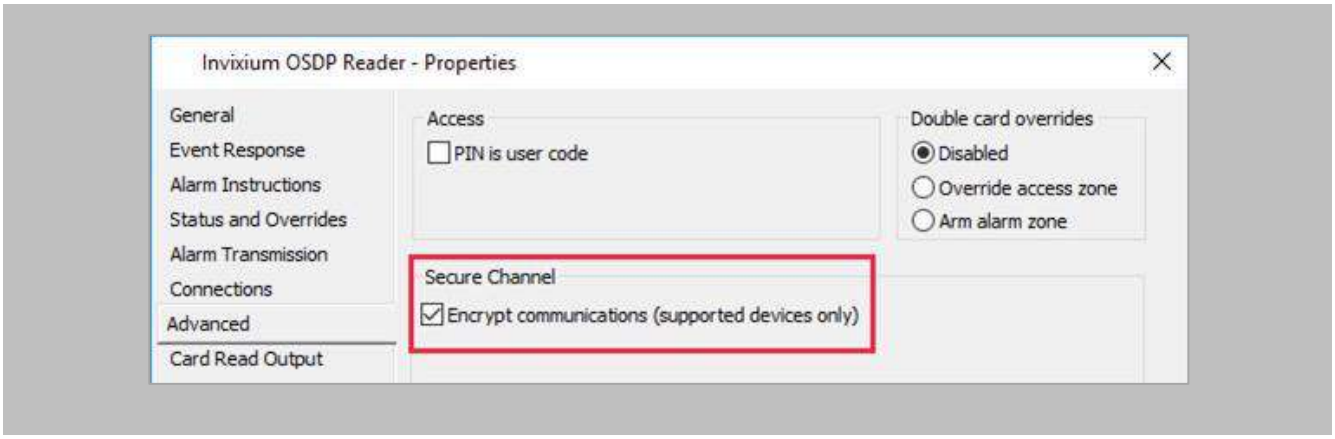


Figure 103: GCC - Setup OSDP reader

STEP 7

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

STEP 8

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

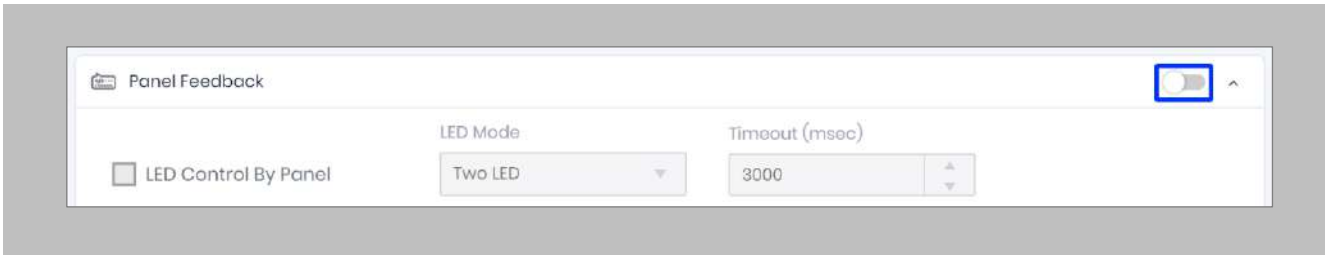


Figure 104: IXM WEB - Disable Panel Feedback

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**.

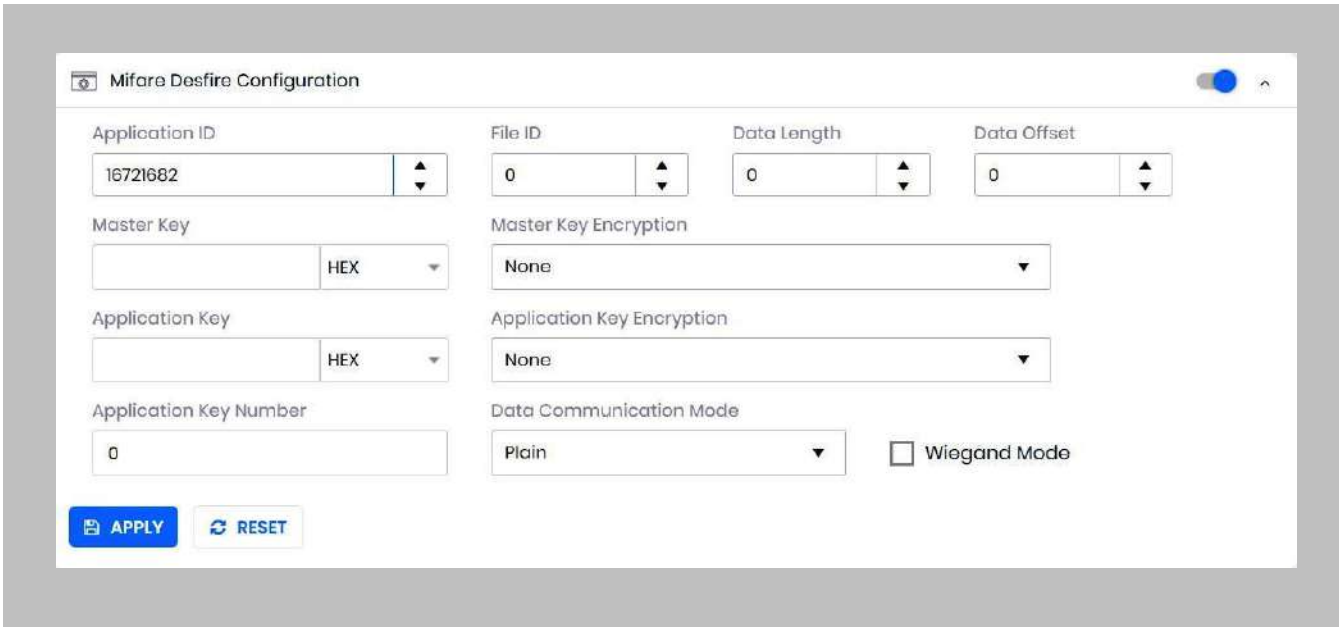


Figure 105: IXM WEB - MIFARE DESFire Configuration

STEP 2

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

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

Data Offset	Enter data offset of Gallagher cards.
Master Key	Enter Master key of Gallagher cards.
Master Key Encryption	Select Master Key Encryption from the dropdown as per requirement. Options are: • None • 2K 3DES • 3K 3DES • AES 128
Application Key	Enter Application key of Gallagher cards.
Application Key Encryption	Select Application Key Encryption from the dropdown as per requirement. Options are: • None • 2K 3DES • 3K 3DES • AES 128
Application Key Number	Enter Application key Number of Gallagher cards.
Data Communication Mode	Select Data Communication Mode from the dropdown as per requirement. Options are: • Plain • MAC • Enciphered
Wiegand Mode	Enable Wiegand mode if data is encoded in Wiegand format.

Table 7: IXM WEB – MIFARE DESFire Configuration Options

STEP 3

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

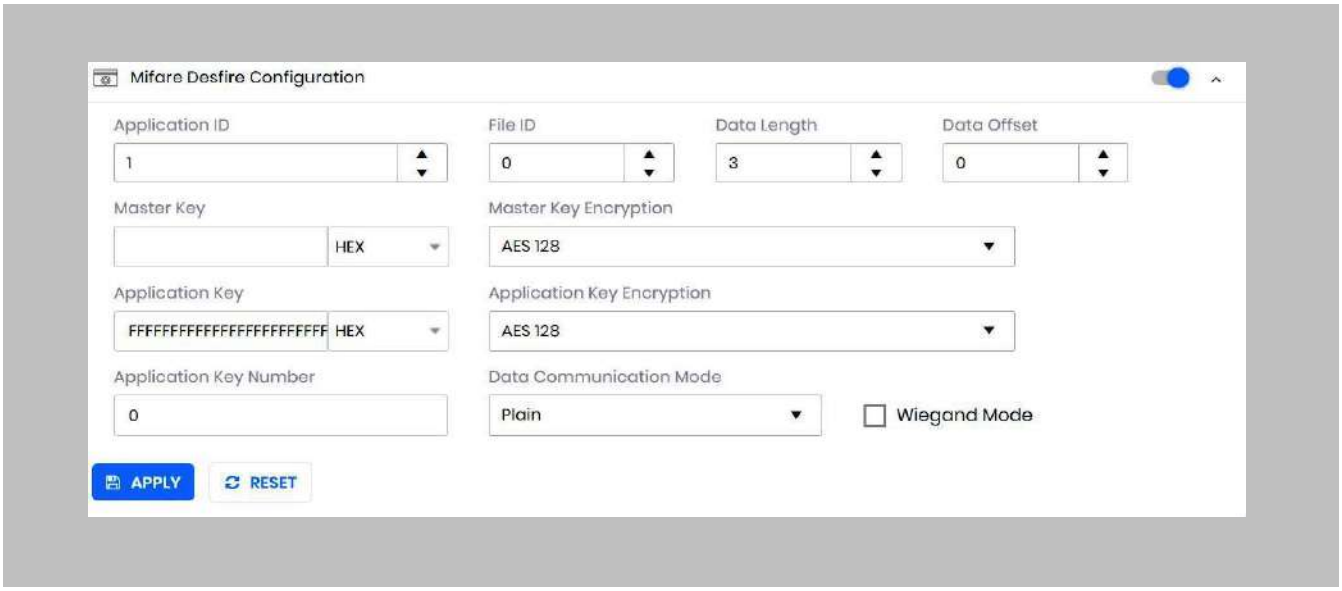


Figure 106: IXM WEB - MIFARE DESFire Sample Configuration

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.

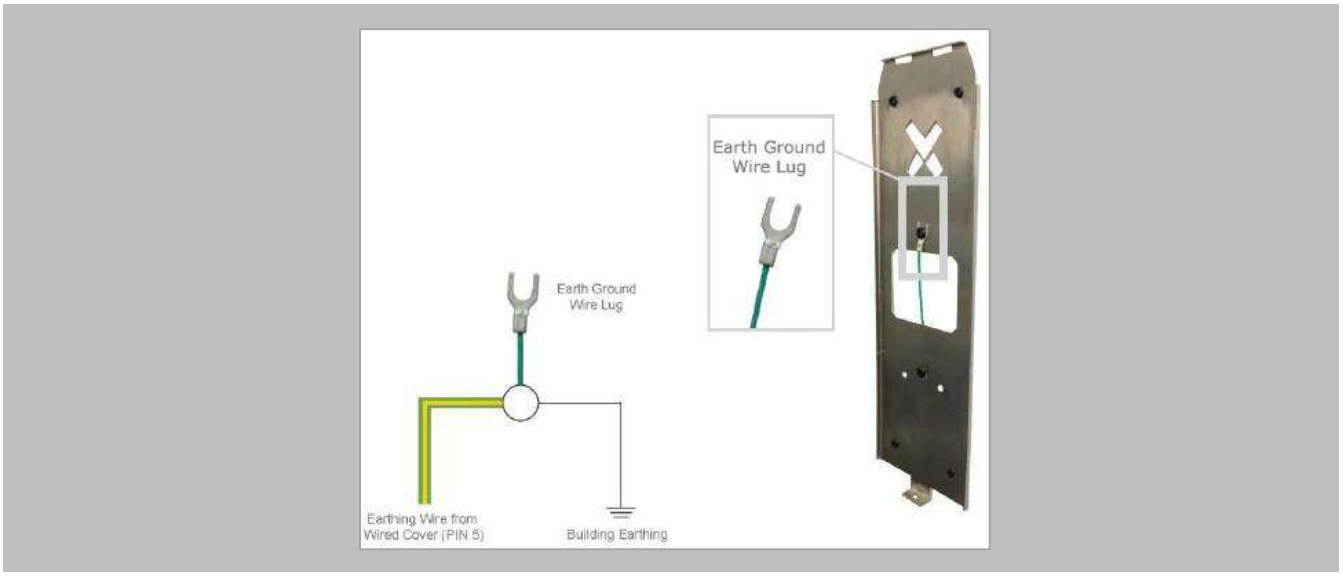


Figure 107: Earth Ground Wiring

Wiring

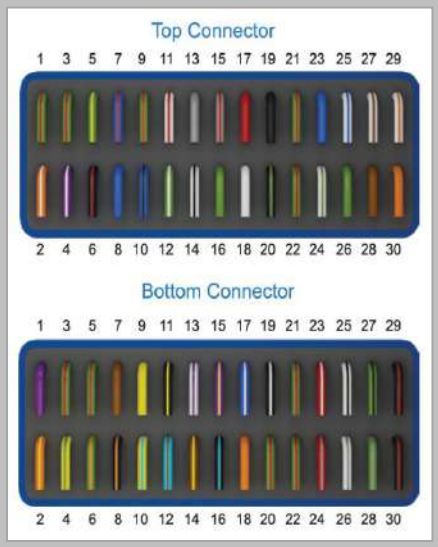
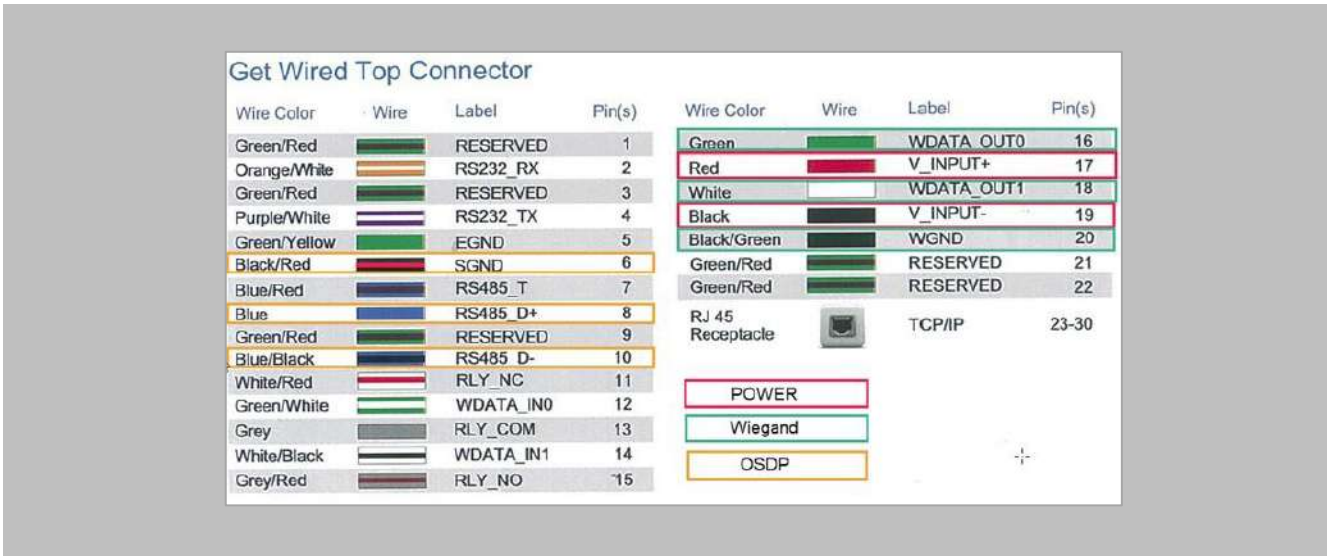


Figure 108: IXM TITAN – Top & Bottom Connector Wiring



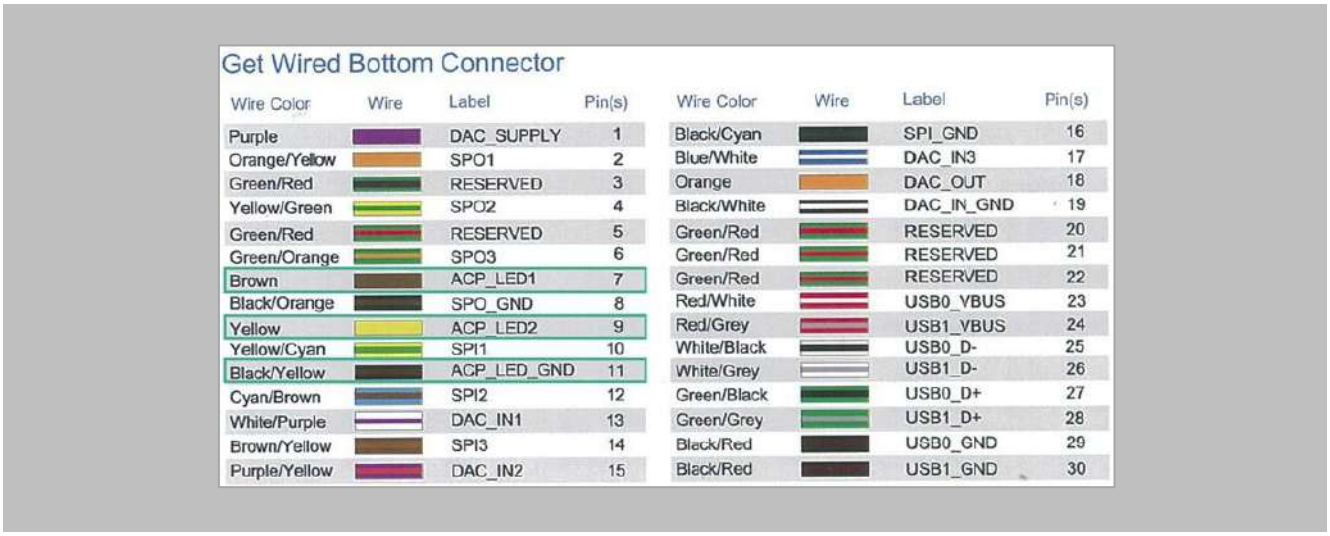


Figure 109: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand and OSDP.

Invixium devices can be integrated with Gallagher Controller on:

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

Wiegand Connection

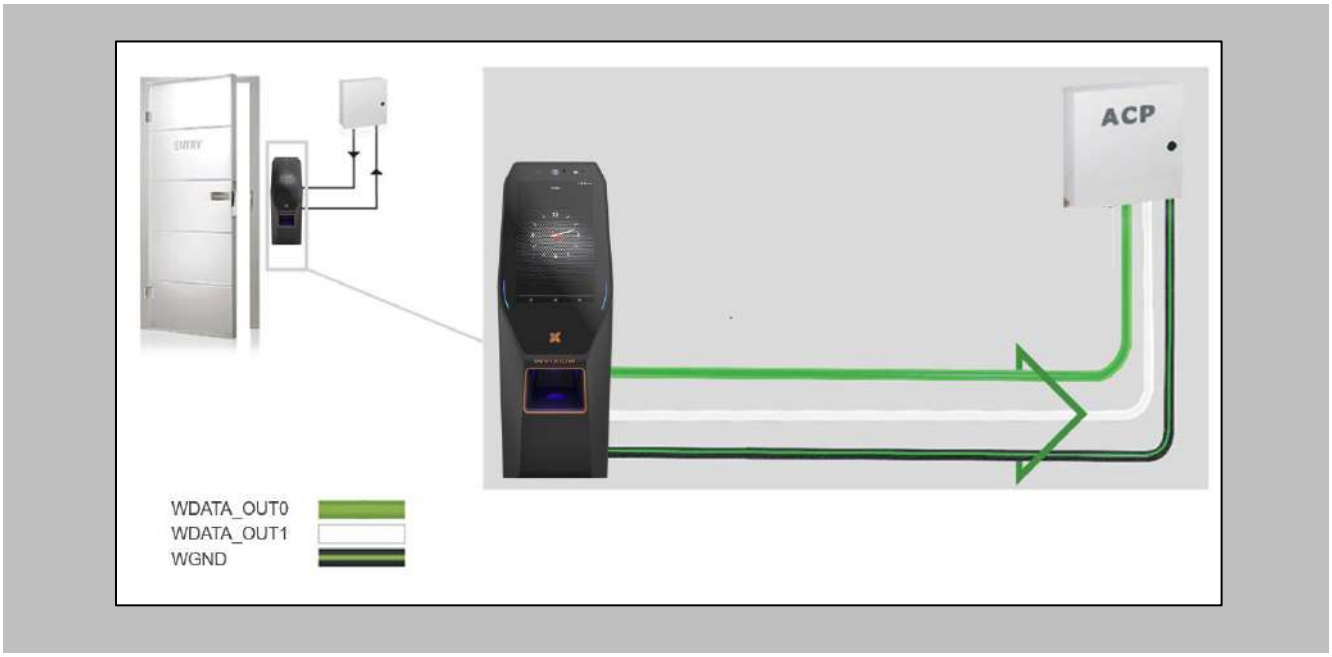


Figure 110: IXM TITAN - Wiegand

Wiegand Connection with Panel Feedback

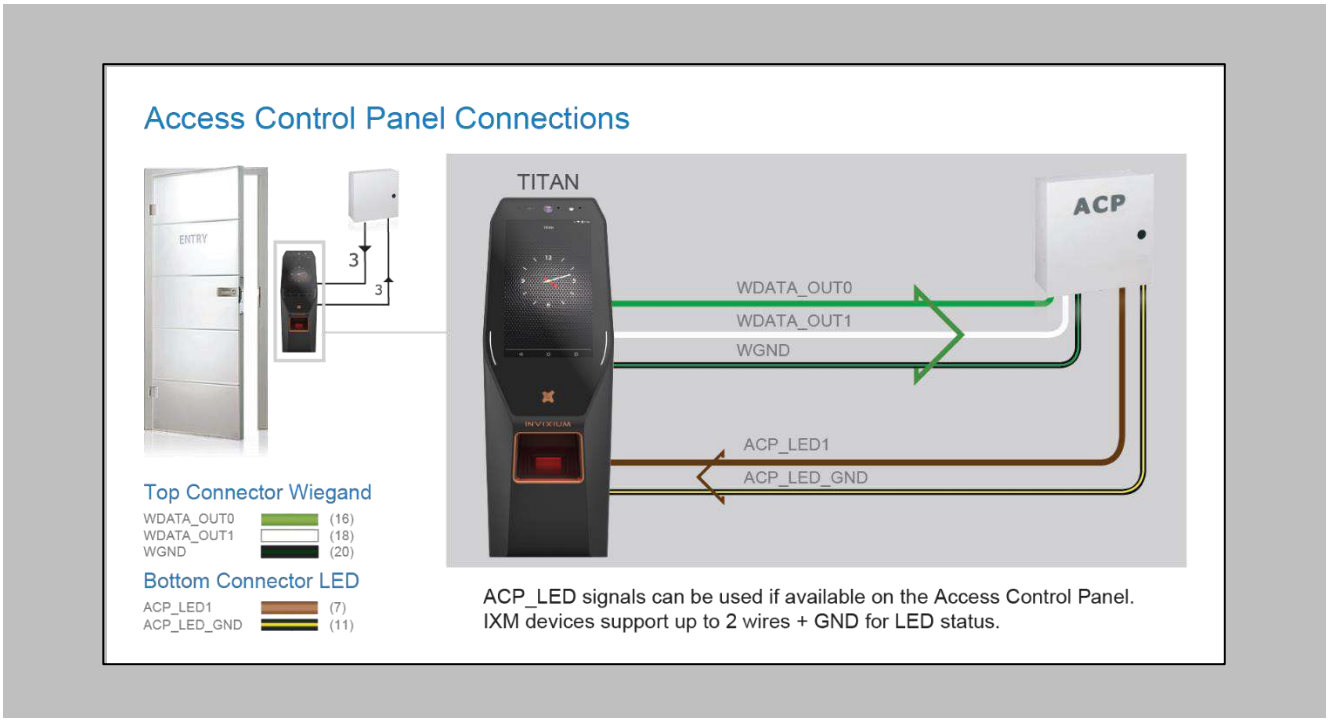


Figure 111: IXM TITAN - Panel Feedback

OSDP Connections

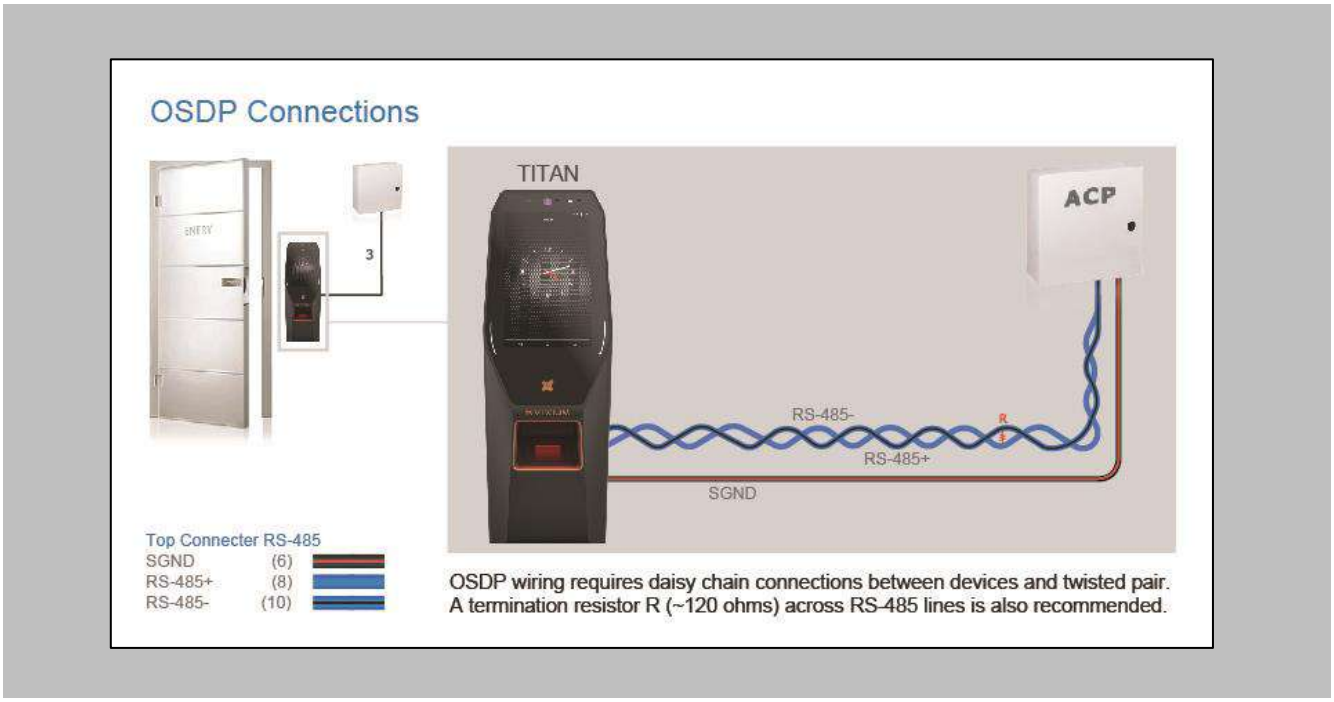


Figure 112: IXM TITAN - OSDP Connections

18. Troubleshooting

Reader Offline from the IXM WEB Dashboard

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

Procedure

STEP 1

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

STEP 2

Select any device.

STEP 3

Navigate to the **Communication** tab.

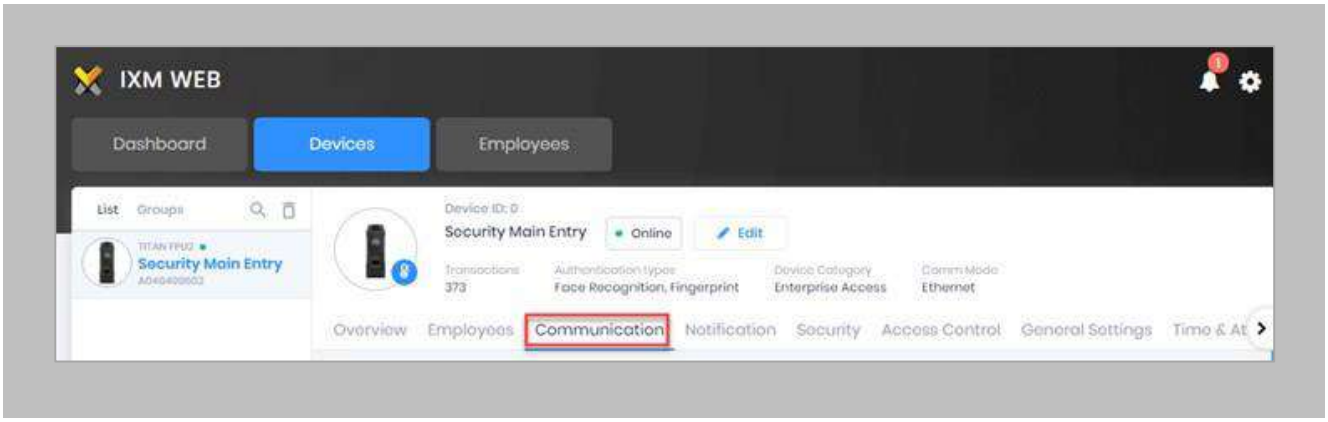


Figure 113: IXM WEB - Device Communication Settings

STEP 4

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

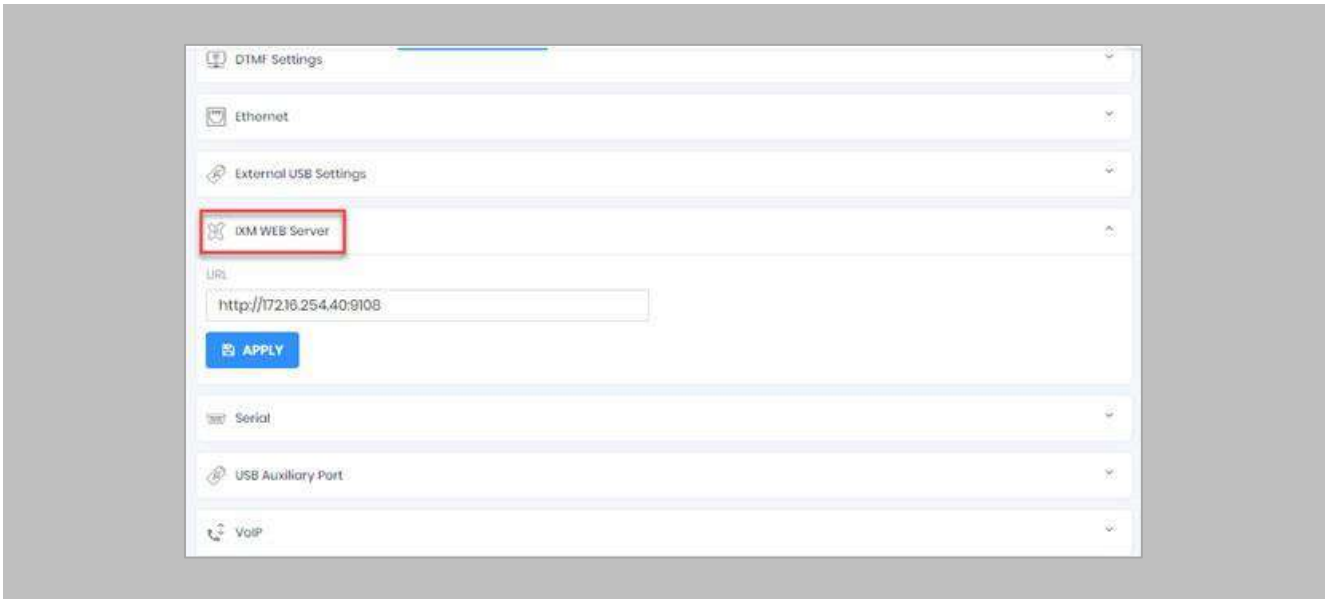


Figure 114: IXM WEB - Server URL Setting

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

STEP 5

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

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

STEP 6

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

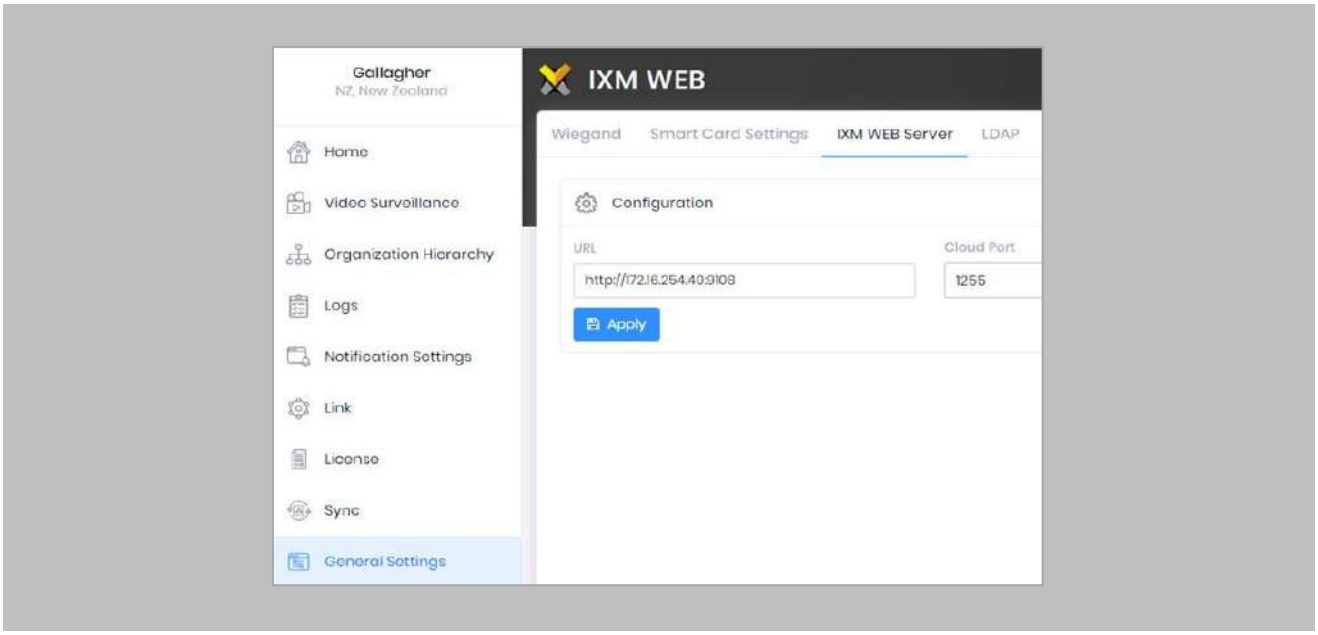


Figure 115: IXM WEB - Server URL Setting from General Settings

Elevated Body Temperature Denied Access but Granted Access in Command Centre

Procedure

STEP 1

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

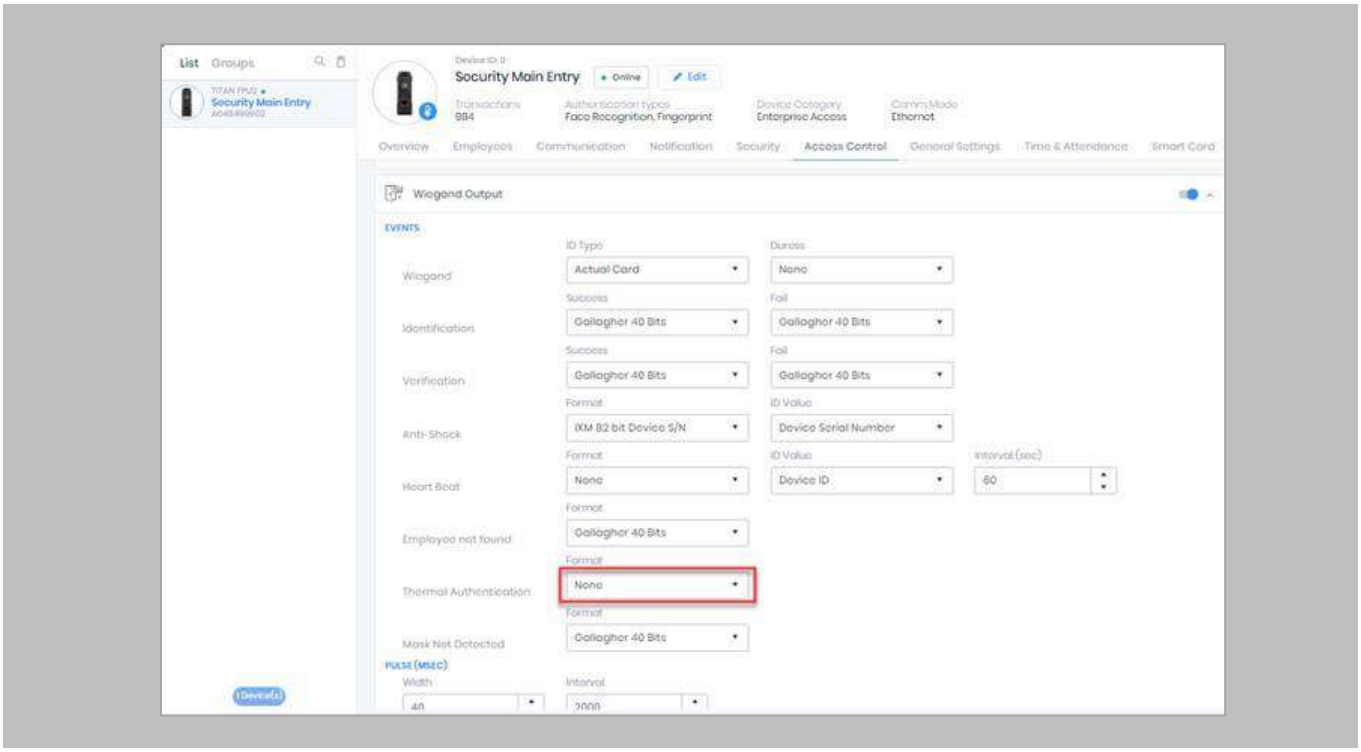


Figure 116: IXM WEB - Thermal Authentication Wiegand Output Event

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

Figure 117: IXM WEB - Enable Device Logs

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

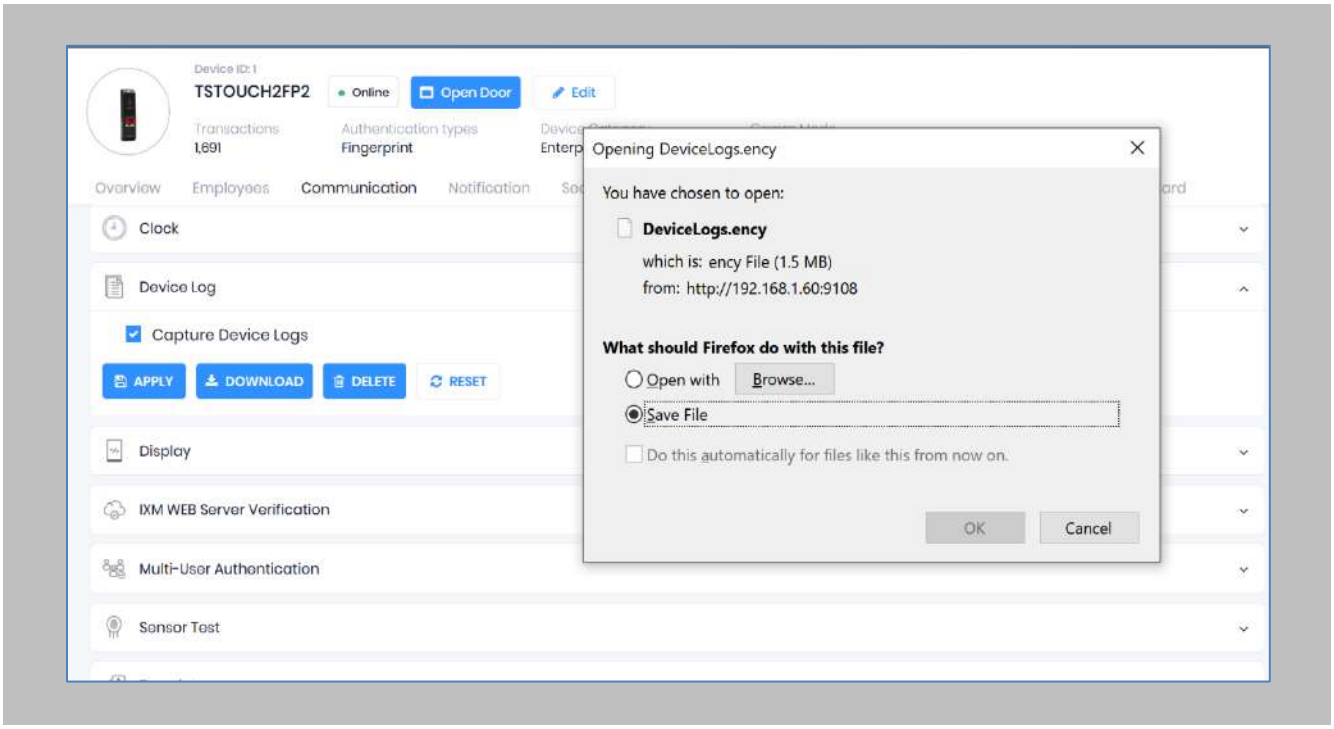


Figure 118: Save Device Log File

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

19. Support

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

20. 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.