IXM WEB Integration with WIN-PAK by Honeywell

Installation Instructions

V4.0

P/N XAD-TPI-006-04G

Table of Contents

List of Figures

List of Tables

1. Introduction

Purpose

This document outlines the process of configuring the software integration between WIN-PAK by Honeywell and Invixium's IXM WEB.

Description

IXM Link, a licensed module in IXM WEB, is required to synchronize the user database between IXM WEB (where biometric enrollment for users is performed) and WIN-PAK 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 WIN-PAK.

Acronyms

Acronym	Description
ACPCS	Access Control Panel Configuration Software
API	Application Programming Interface
IXM	Invixium

Field Mappings

The following are the Honeywell WIN-PAK fields that are mapped to IXM WEB:

WIN-PAK Field	IXM Field	Notes
First name	First Name	
Last name	Last Name	
Card Number (Card)	Number (Card)	
Issue (Card)	Issue Level (Card)	
Activation Date (Card)	Activation Date (Card)	
Expiration Date (Card)	Expiry Date (Card)	
Photo/Badge (Card Biometrics)	Employee Photo	
Status (Card)	Status (Card)	Active is mapped with the card's Active status in IXM WEB. Lost/Stolen is mapped with the Lost status of the card in IXM WEB. Others will be inactive in IXM WEB.
Access Level	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 Honeywell WIN-PAK will be added to this created employee group andwill be used for automatic transfer to IXM Devices.

Note: Multiple Cards – Honeywell WIN-PAK 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**
Honeywell WIN-PAK	V4.9+
Invixium IXM WEB	3.0.2536.0
Operating Systems	Windows 11 Pro Windows 10 Professional Version Windows Server 2016 StandardWindows 10 Professional Version Windows 11 Pro Windows Server 2016 Standard Windows Server 2019
Microsoft .NET Framework	.NET Framework 4.8
Database Engine	SQL Server 2016+ Supported but not recommended: (legacy) SQL server 2014 Express Edition (Default Installation)
Internet Information Services (IIS)	Microsoft® Internet Information Services version 10.0
Web Browser	Google Chrome Mozilla Firefox Microsoft Edge (Internet Explorer not recommended)

Other Requirements

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

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

Compatibility Matrix for IXM WEB & WIN-PAK Integration:

IXM WEB version	WIN-PAK version	Compatible
IXM WEB 2.2.252.0	V4.9	Yes
IXM WEB 2.2.330.0	V4.9	Yes
IXM WEB 2.3.2.0	V4.9	Yes
IXM WEB 3.0.36.0	V4.9	Yes
IXM WEB 3.0.25.0	V4.9	Yes

Table 1: Compatibility Matrix for IXM WEB & Honeywell WIN-PAK Integration

3. Checklist

Item List	Interface
Prerequisites For IXM WEB Installation	Invixium
Installation Of IXM WEB	Invixium
Email Configuration in IXM WEB	Invixium
IXM WEB And IXM Link Activation	Invixium
Configure IXM Link for Honeywell WIN-PAK	Invixium
Configure Invixium Reader	Invixium
Configure Note Field for Email (Optional)	Honeywell WIN-PAK
Configuration for Integration when IXM WEB and Honeywell WIN-PAK are installed on different servers	

4. Task List Summary

Task	IXM WEB Application Task List using IXM WEB	Honeywell WIN-PAK Task List using WIN-PAK
1	Activate IXM WEB and IXM Link for Honeywell WIN-PAK.	Create a cardholder. Assign Card and Access Level to the cardholder.
2	Configure IXM Link for WIN-PAK.	Create a Note Field in WIN-PAK for email configuration.
3	Register the IXM Device and configure settings as per the requirement.	
4	Configure Weigand or OSDP settings on the device as per the requirement.	
5	Assign a specific Device Group to the device.	

Table 2: Task List Summary

1. Prerequisites for Installing Invixium IXM WEB Software

Acquiring an 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/.

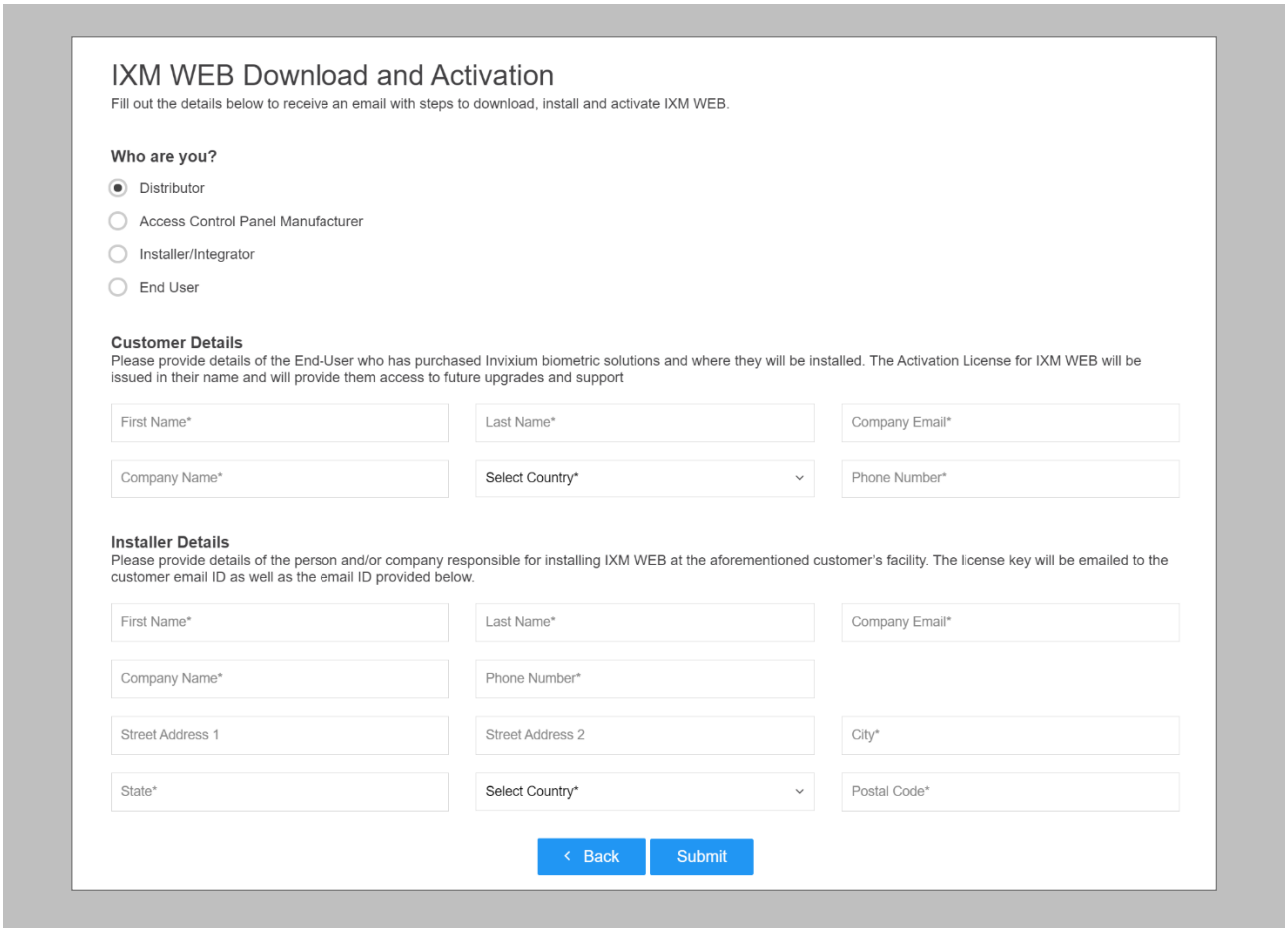
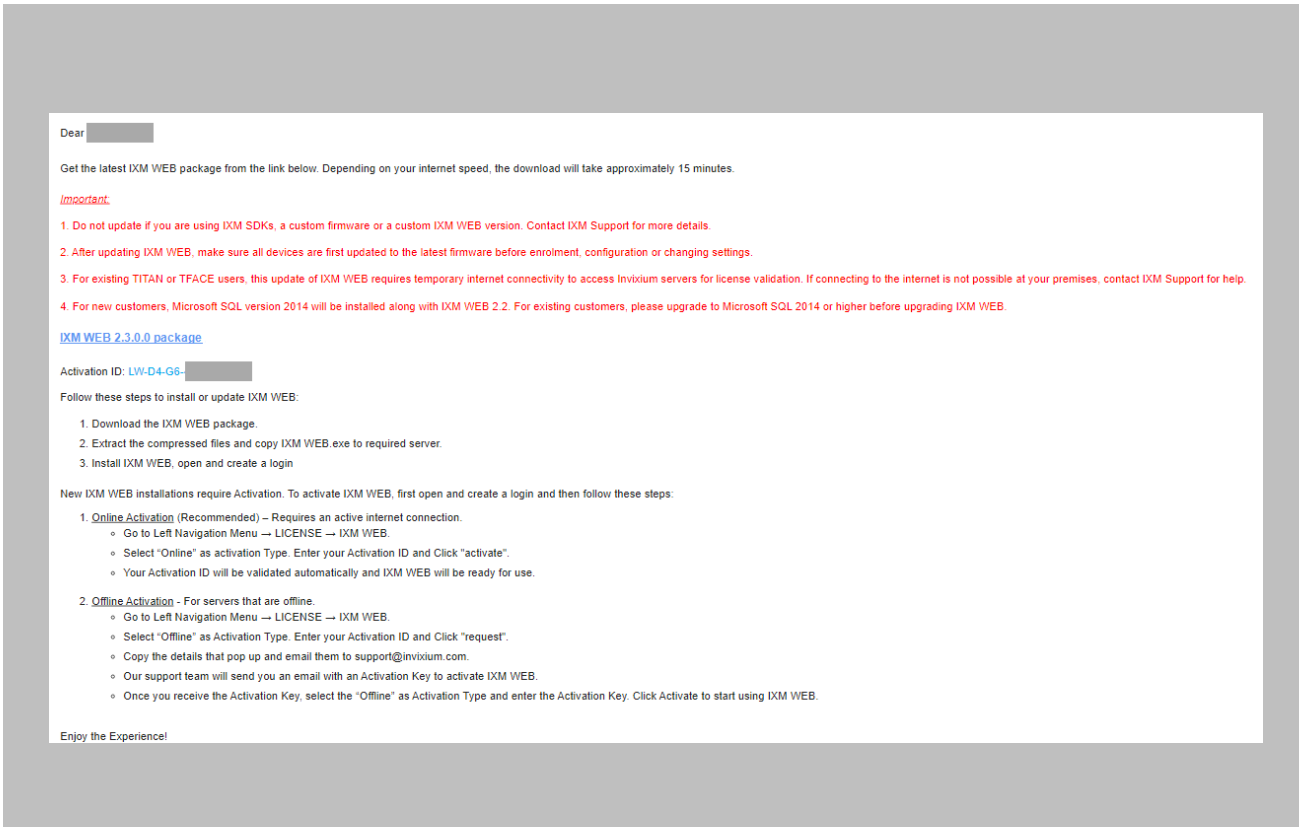


Figure 1: IXM WEB Online Request Form

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

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 Installation 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

Table 4: Port Information

2. Installing IXM WEB

Software Install

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator).

Select **Advanced.**

Figure 3: IXM WEB Installer

STEP 2

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

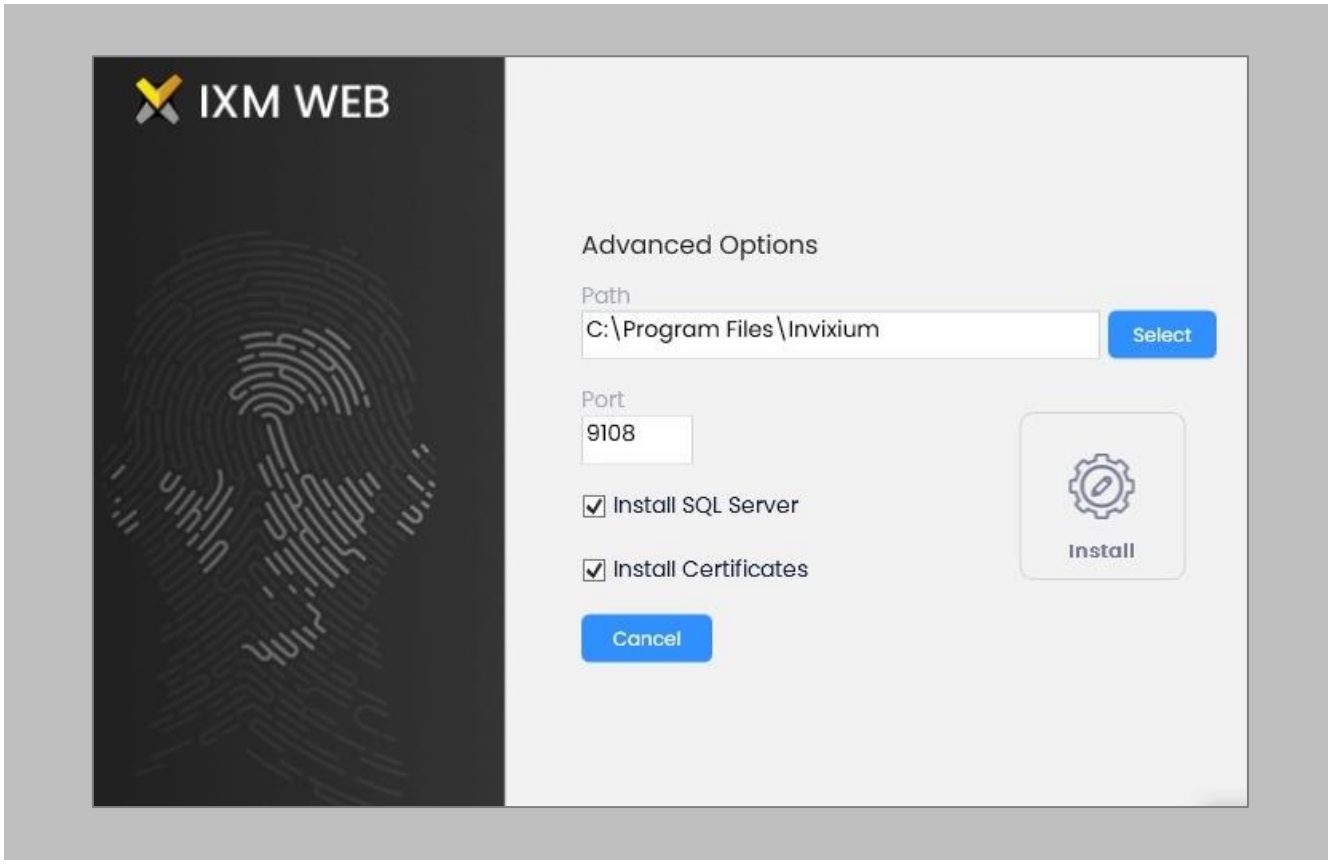


Figure 4: Advanced Options in IXM WEB Installer

STEP 3

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

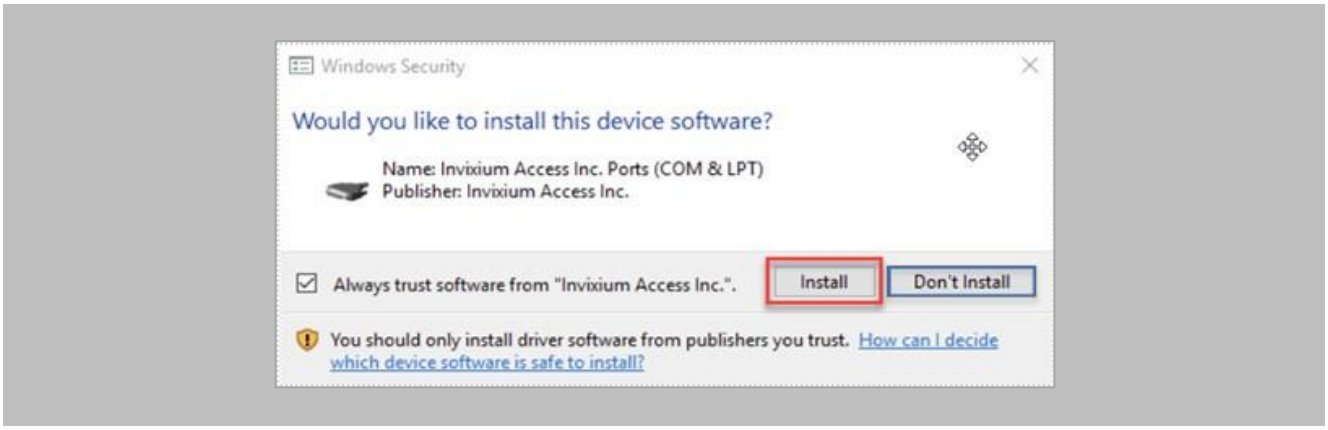


Figure 5: Invixium Fingerprint Driver Installation Message

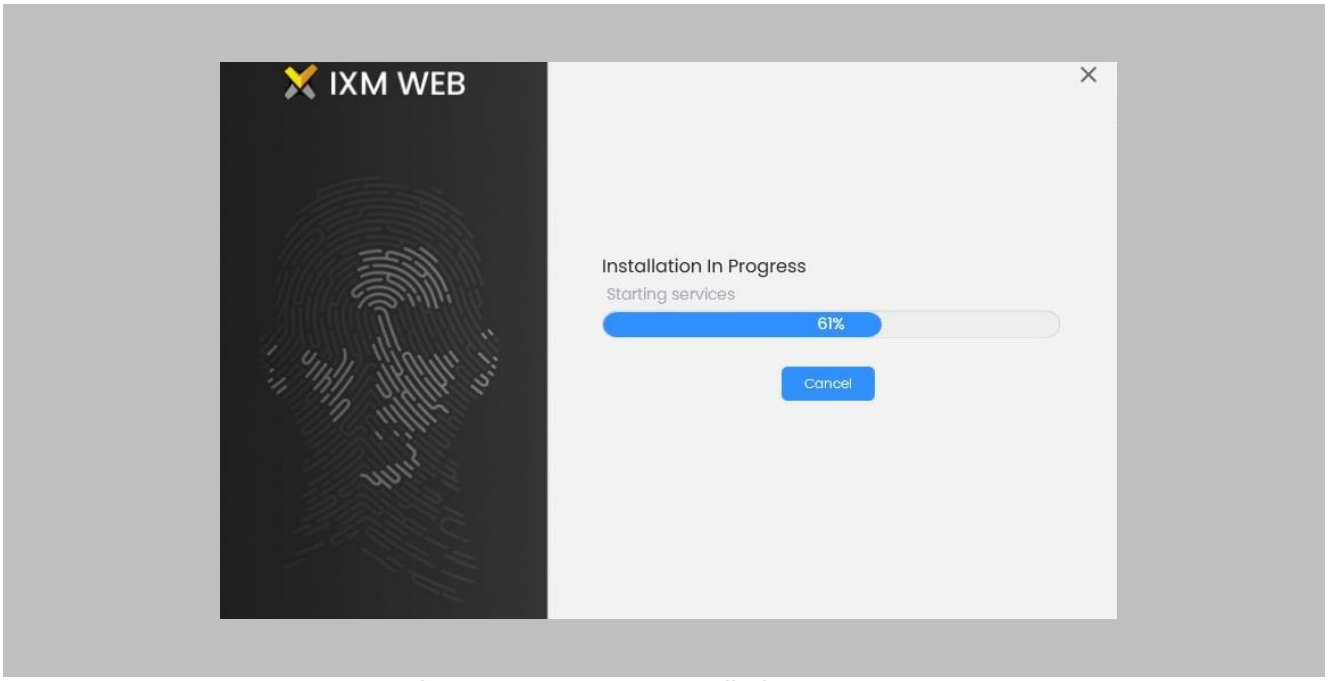


Figure 6: IXM WEB Installation Progress

STEP 4

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

Figure 7: 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 8: IXM WEB Icon - Desktop Shortcut

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

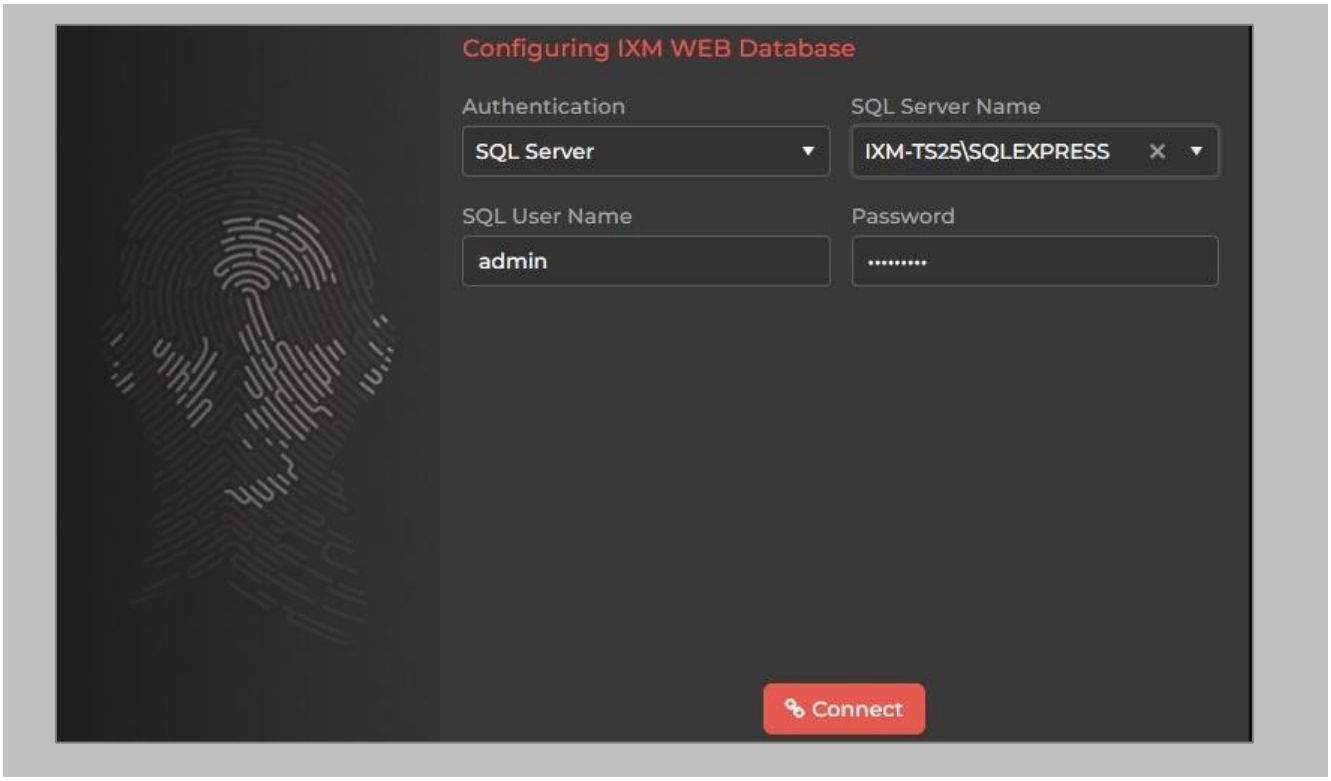


Figure 9: IXM WEB Database Configuration

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.

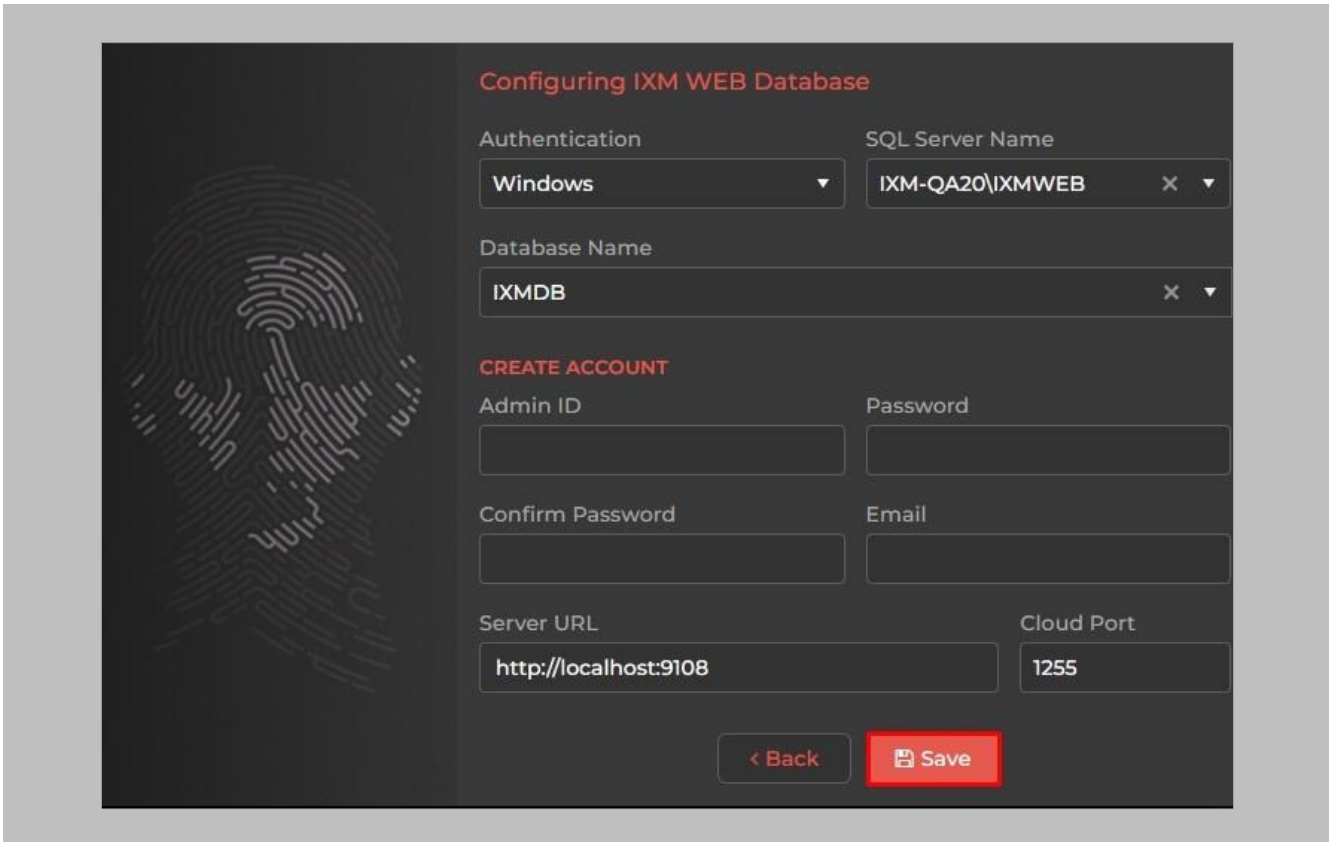


Figure 10: IXM WEB Administrator User Configuration

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:

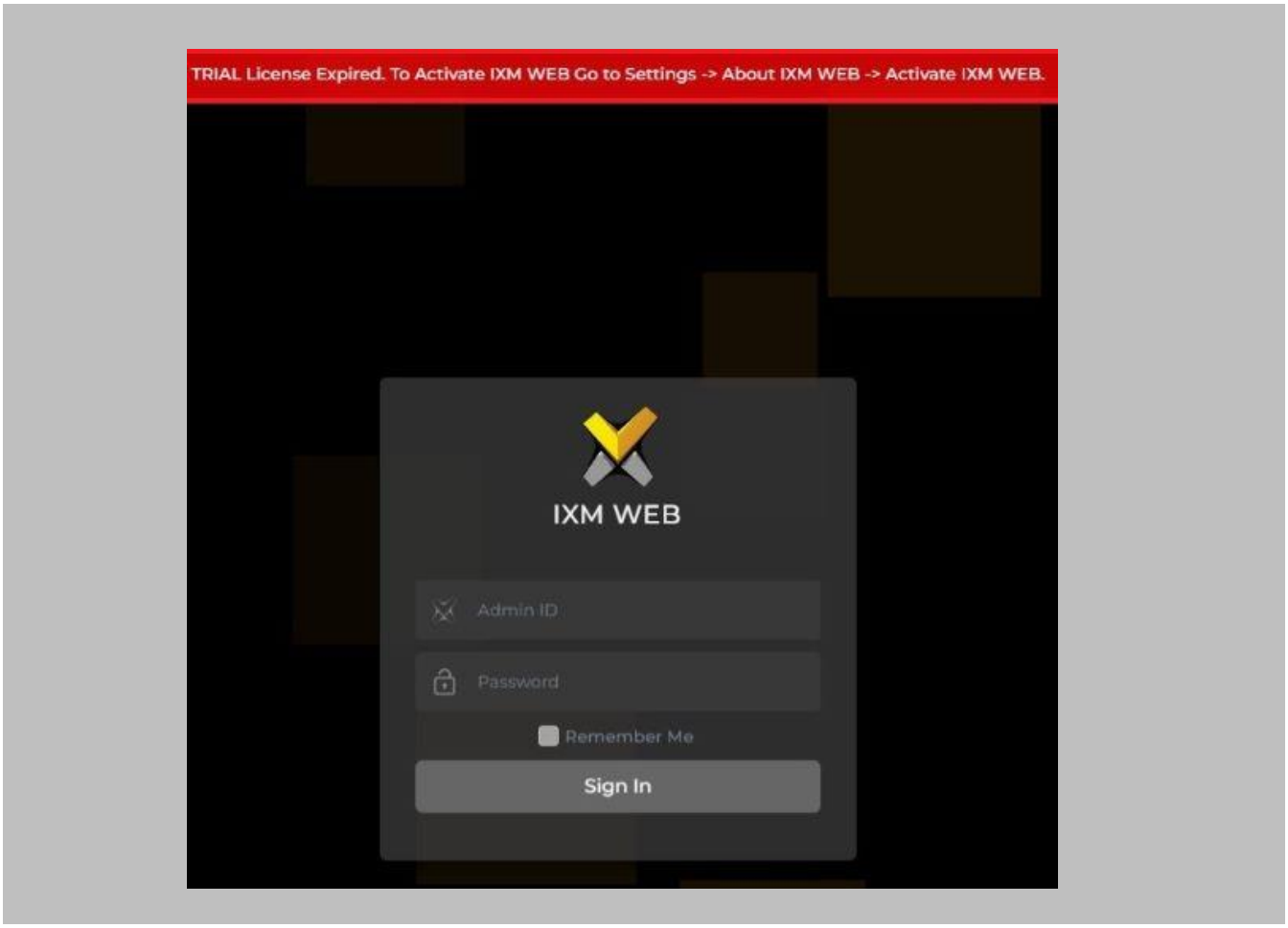


Figure 11: IXM WEB Login Page

Note: During an upgrade of IXM WEB from any previous release to 3.0.25.0, 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.

3. 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.**

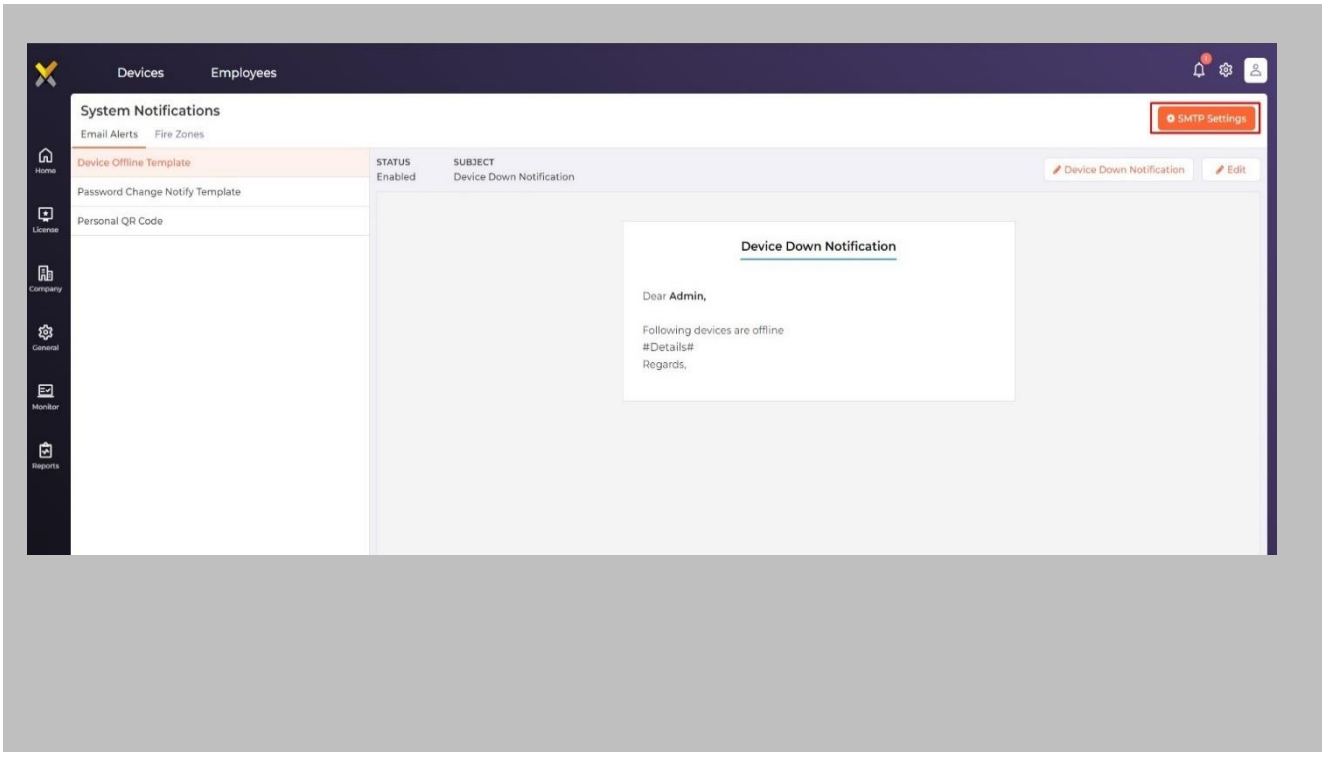


Figure 12: Configure Email

STEP 2

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

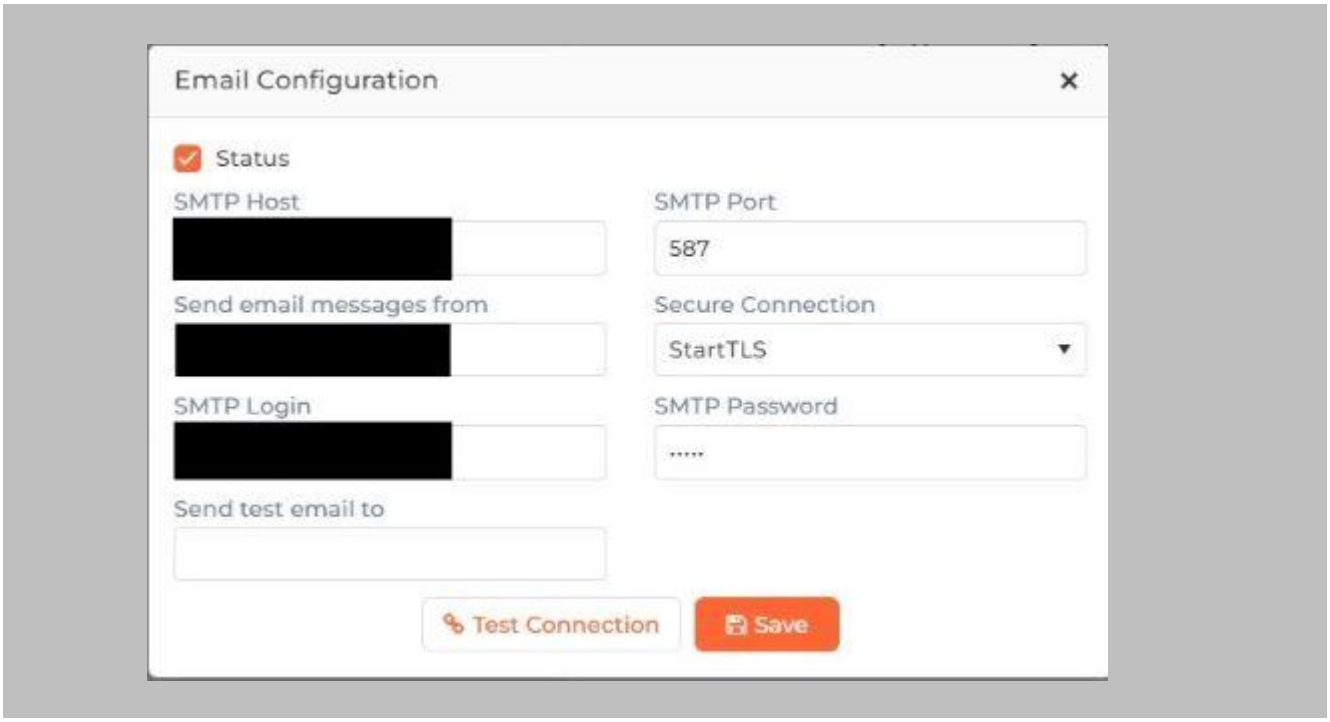


Figure 13: IXM WEB - SMTP Settings

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.

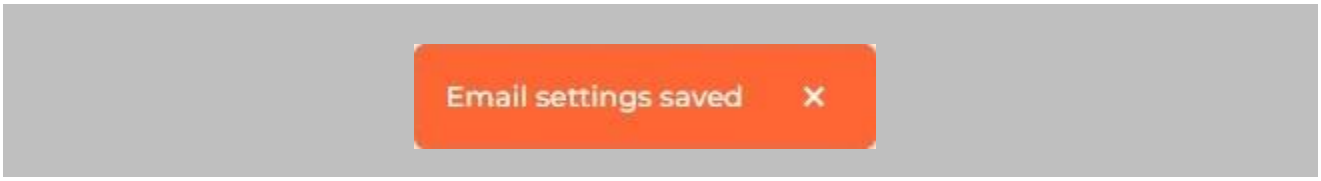


Figure 14: IXM WEB - Save Email Settings

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.

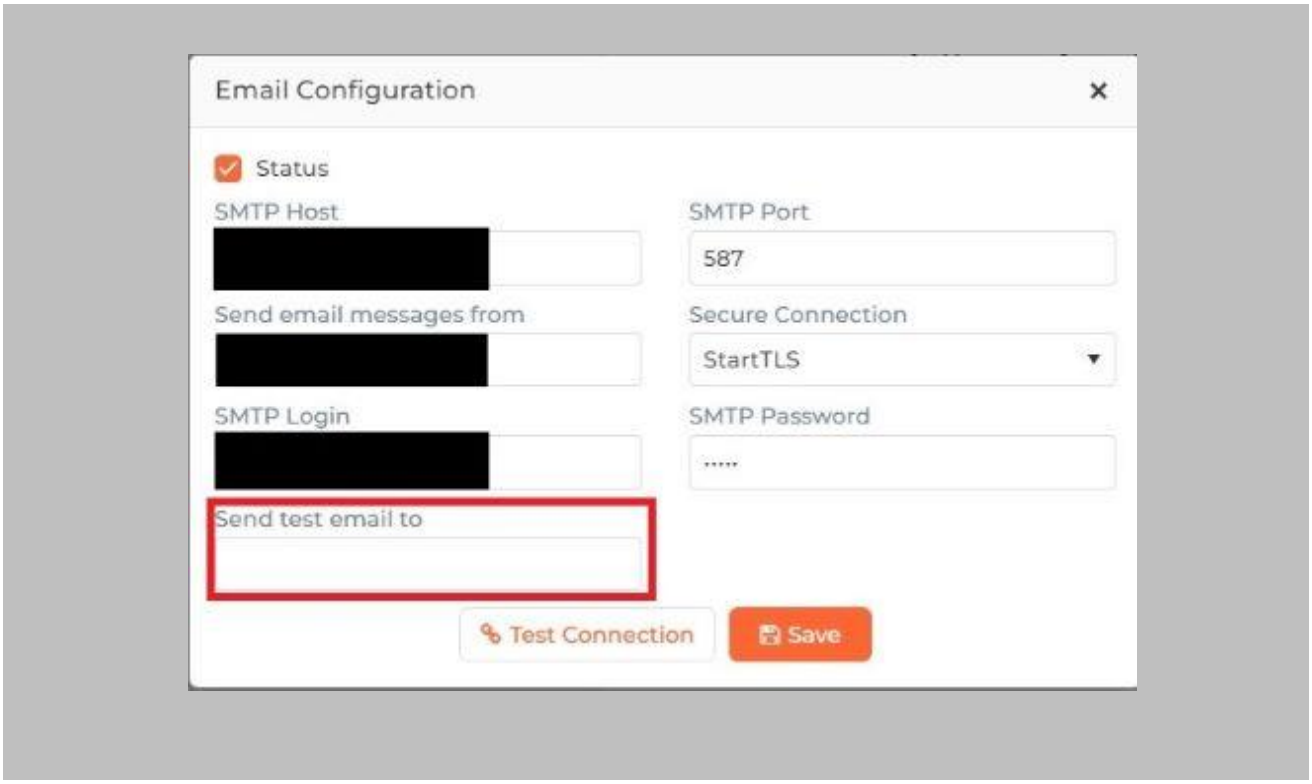


Figure 15: IXM WEB – Test Connection

STEP 4

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

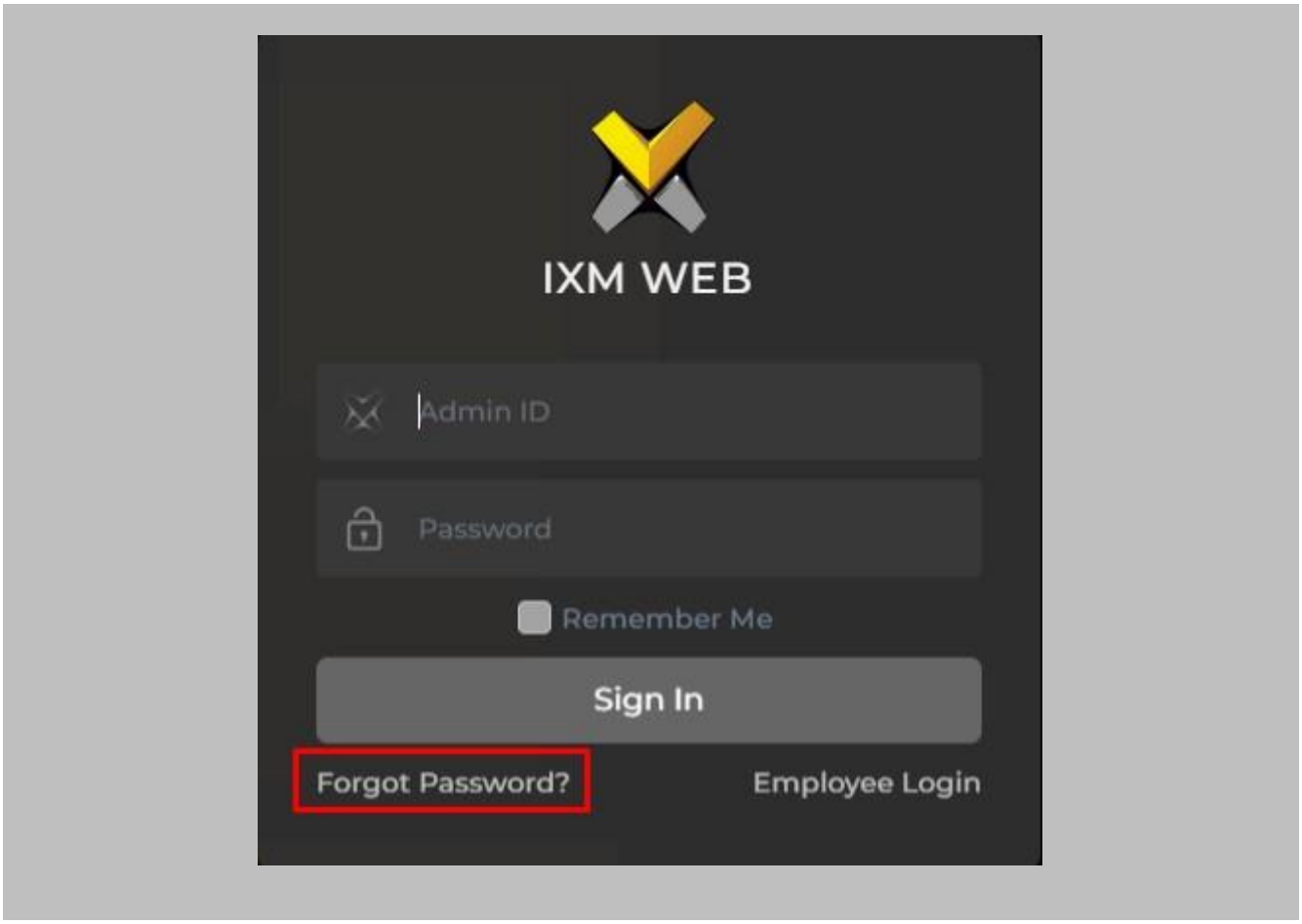


Figure 16: IXM WEB - Forgot Password

4. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

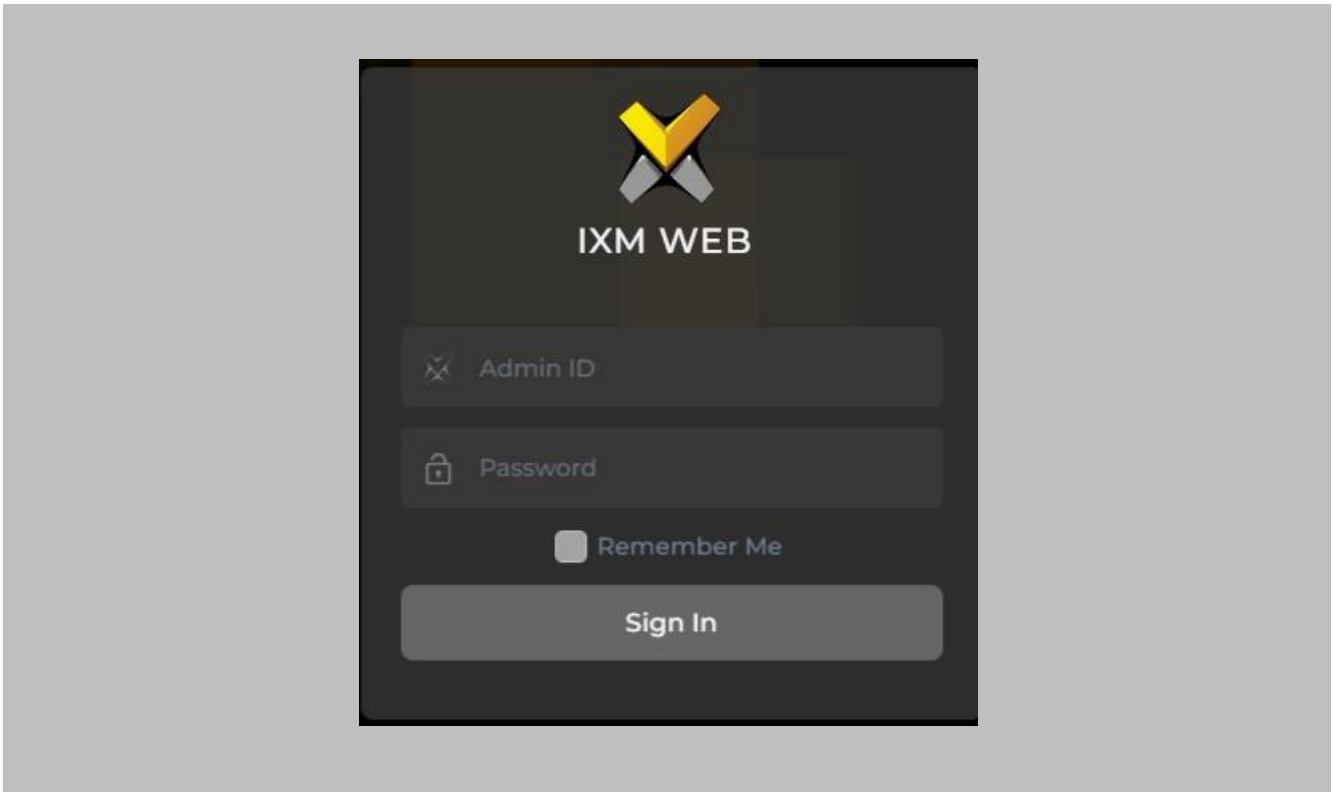


Figure 17: IXM WEB - Enter Login Credentials

STEP 2

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

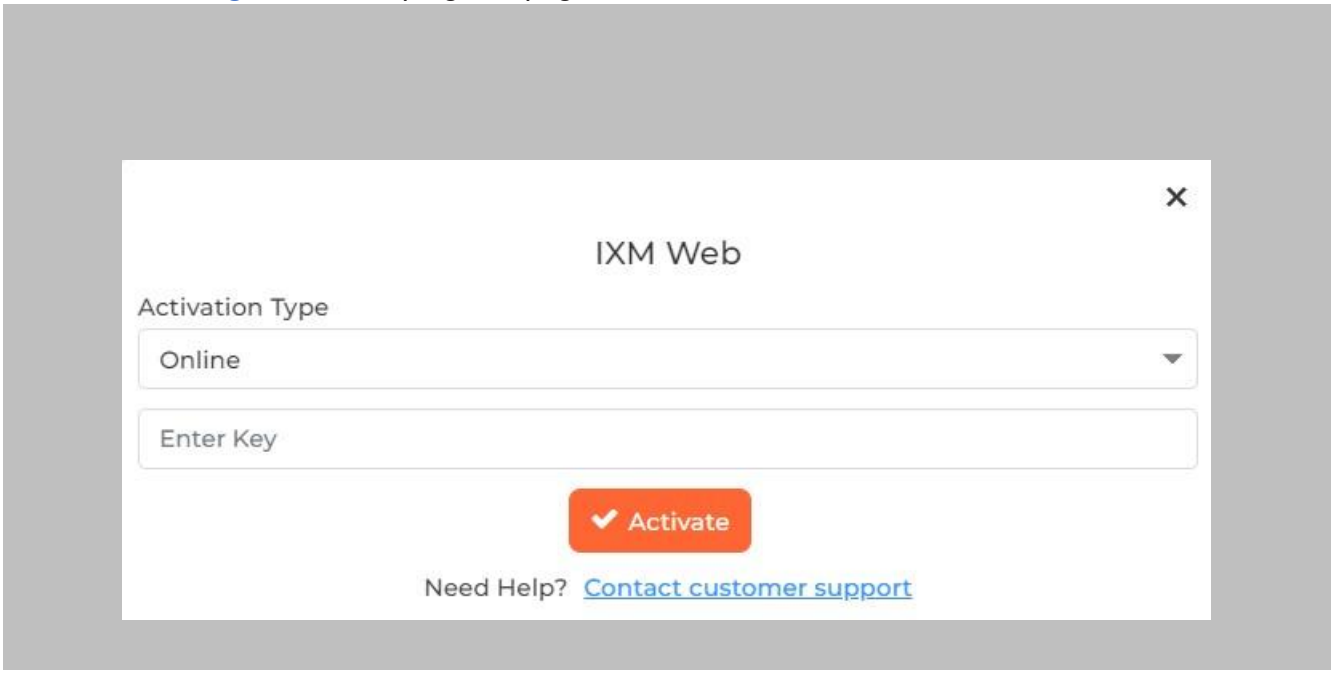


Figure 18: IXM WEB - License Setup

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**.

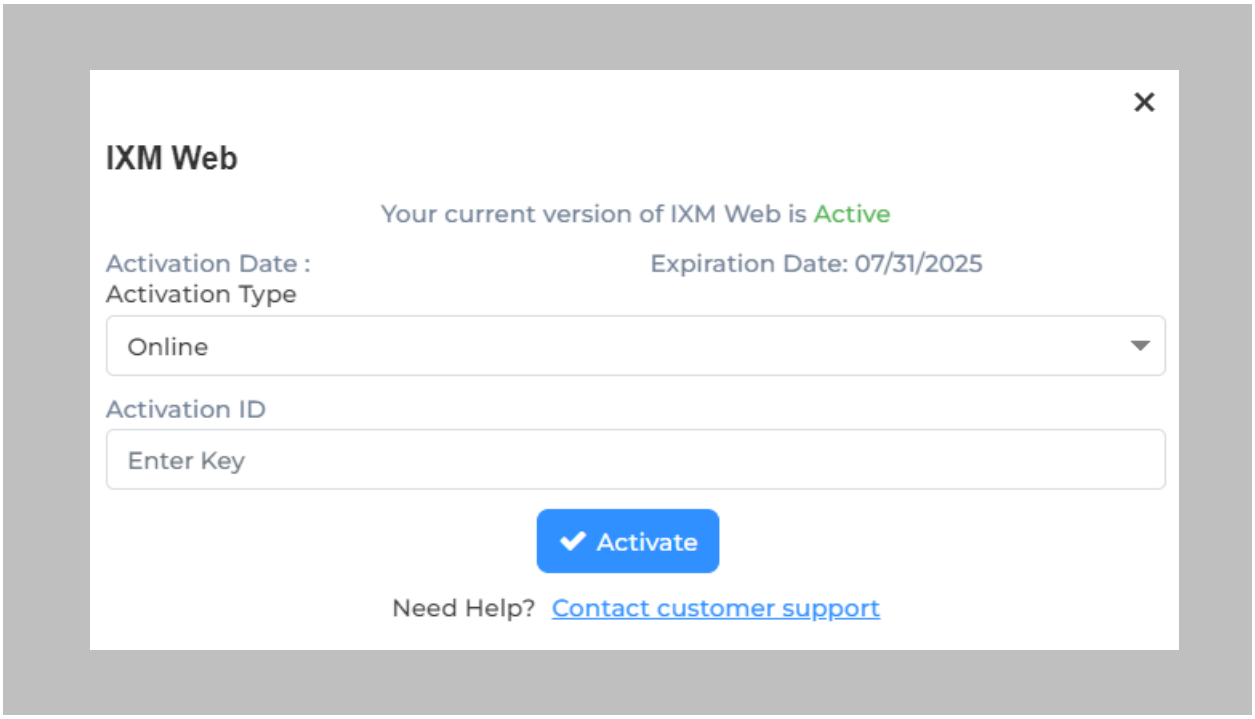


Figure 19: IXM WEB - Online Activation

WIN-PAK Module Activation

The option to activate a Honeywell WIN-PAK 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.

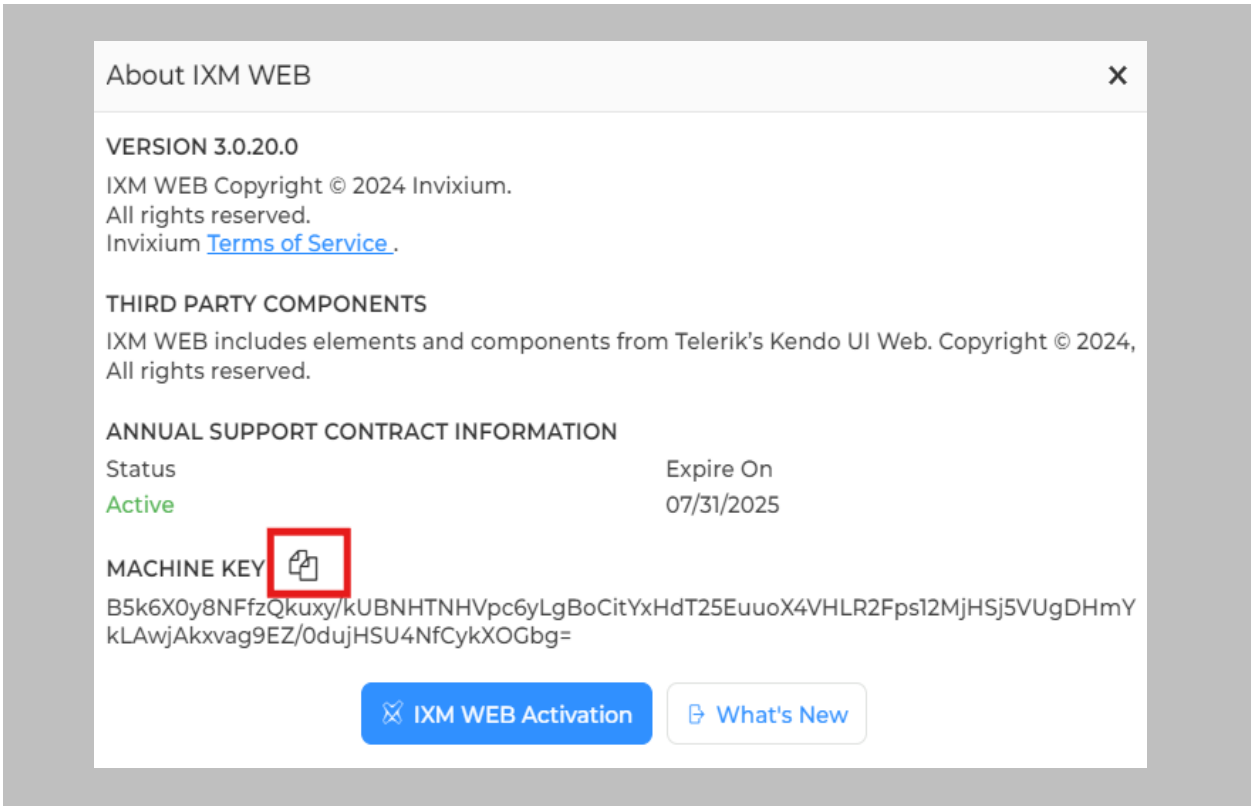


Figure 20: IXM WEB – Request Link License

STEP 2

You will receive an email from Invixium Support containing a license key for the Honeywell WIN-PAK Activation.

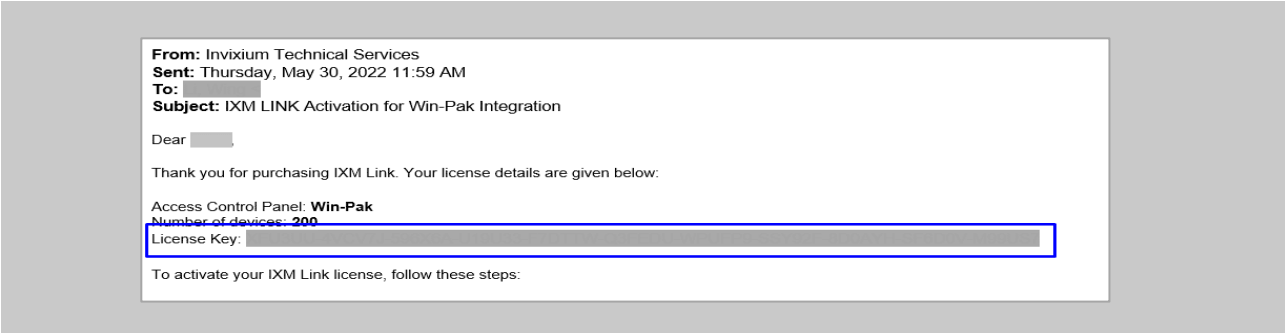


Figure 21: WIN-PAK License Key Email

STEP 3

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

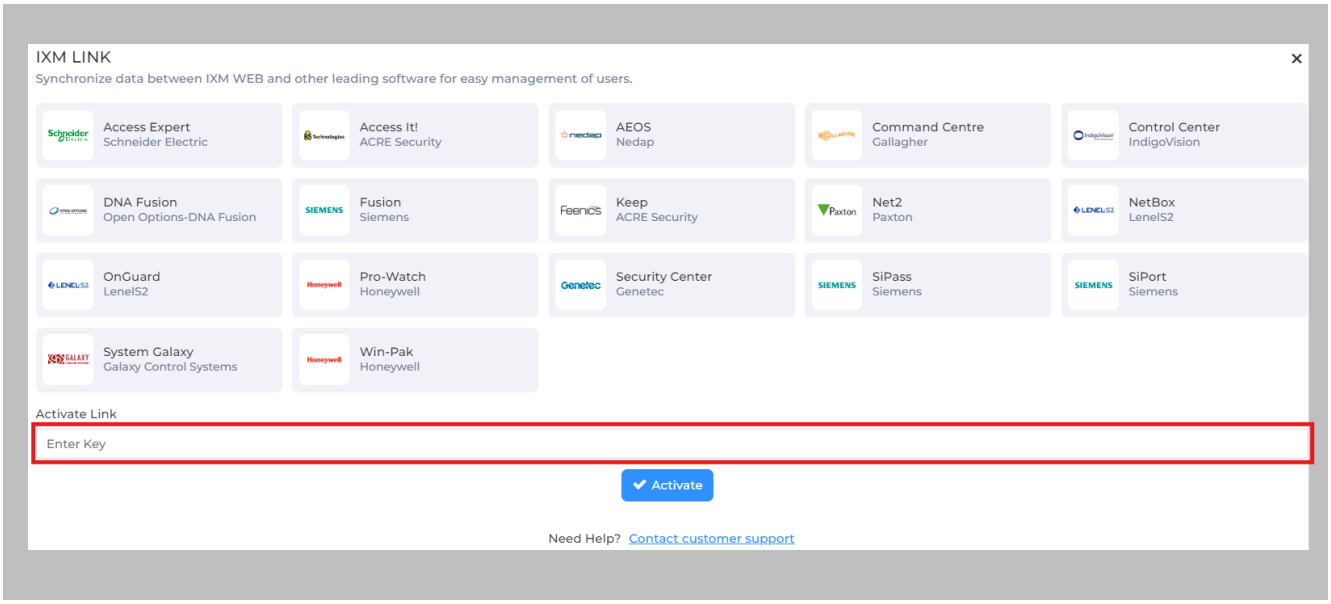


Figure 22: IXM WEB – WIN-PAK Link Activation

RESULT

IXM WEB is now licensed for use with WIN-PAK and configuration can begin.

5. Configuring IXM Link for WIN-PAK

Procedure

STEP 1

From the **Link** → click the **WIN-PAK (Honeywell)** icon.

Toggle the **Status** switch to enable.

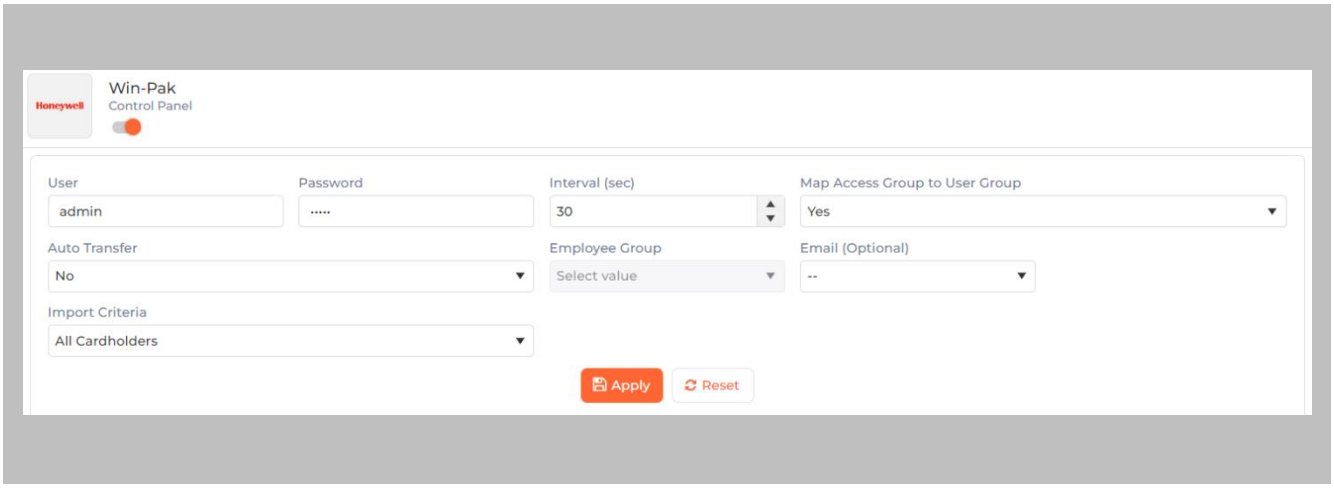


Figure 23: IXM WEB - Enable WIN-PAK Link Module

STEP 2

Enter the **User and Password** of the WIN-PAK user to log in.

STEP 4

Specify in seconds how often sync should take place.

STEP 5

Select **Map Access Level** to Employee Group.

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

As per the WIN-PAK Access Level selected in the cardholder section, that cardholder will be assigned to the IXM WEB Employee Group. It will be assigned to the Invixium devices mapped with that Employee Group.

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

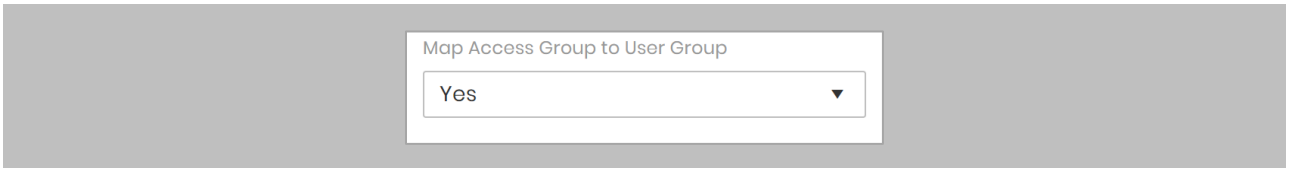


Figure 24: IXM WEB - Map Access Group to User Group

STEP 6

Auto Transfer

No: Employees synchronized from WIN-PAK will not be automatically added to any of the employee groups present in IXM WEB.

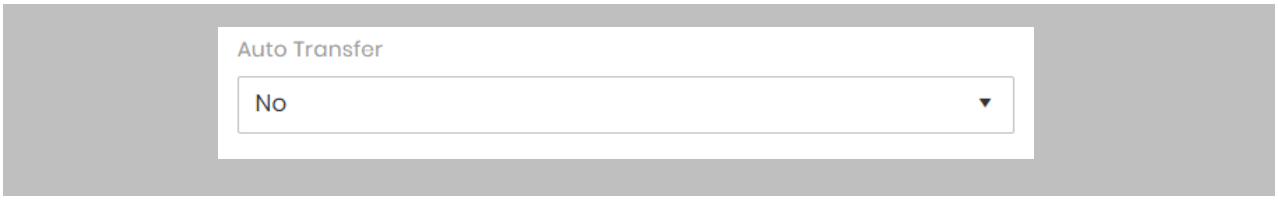


Figure 25: IXM WEB - Auto Transfer No

Yes: By selecting 'Yes' for Auto Transfer, the employee group selection dropdown enables, which displays all the employee groups present in IXM WEB. All the employees synchronized from WIN-PAK will be automatically added to the employee group selected on Link Configuration Page.

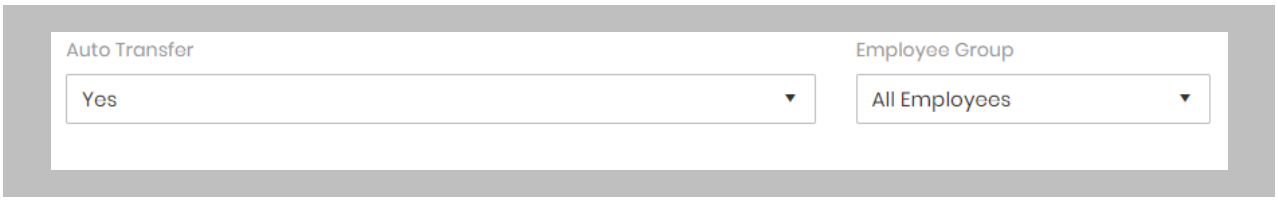


Figure 26: IXM WEB - Auto Transfer Yes

STEP 6

Copy the note field name created for **'Email'** (refer to Configure Note Field for Email in WIN-PAK)

STEP 7

Import Criteria

All Cardholders: All the cardholders from WIN-PAK will be synced to IXM WEB.

Cardholders With Active Card: Only those cardholders with at least 1 active card in WIN-PAK will be synced to IXM WEB.

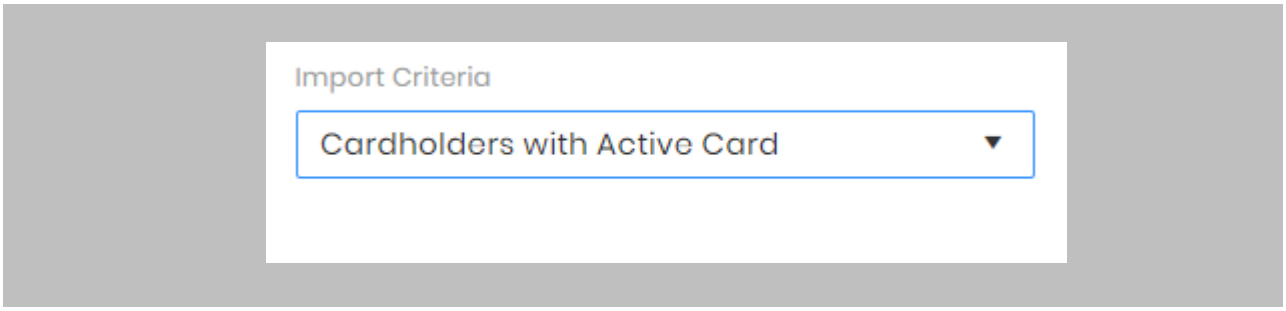


Figure 27: IXM WEB – Import Criteria

STEP 8

Click **Apply.**

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

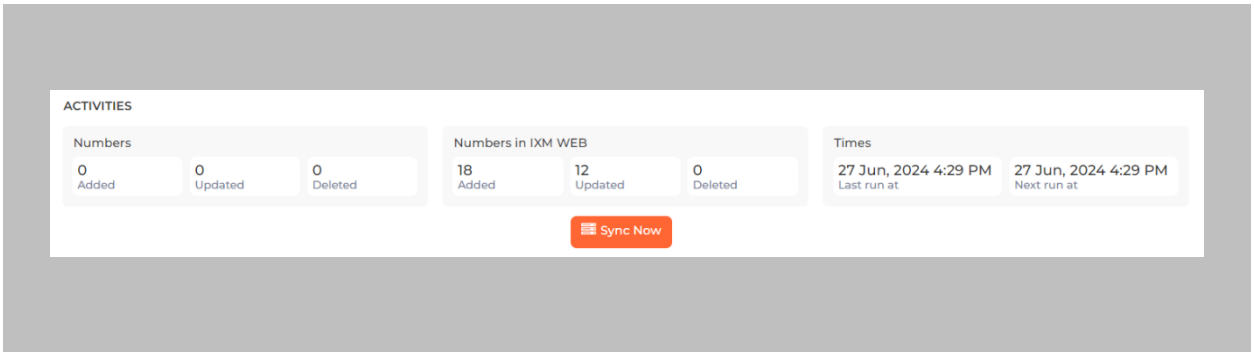


Figure 28: IXM WEB - Sync Activities

STEP 9

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”.

RESULT

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

6. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

Click the **Devices** tab.

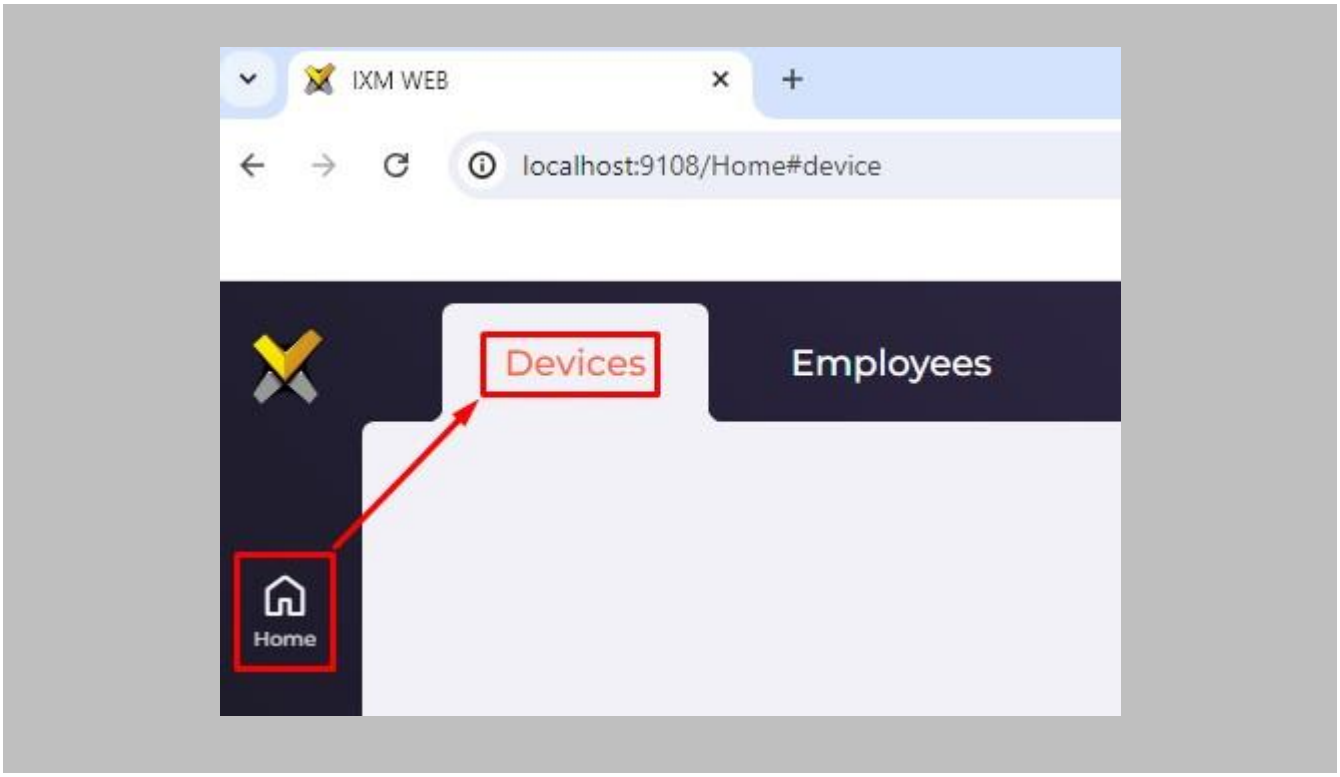


Figure 29: IXM WEB - Devices Tab

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.

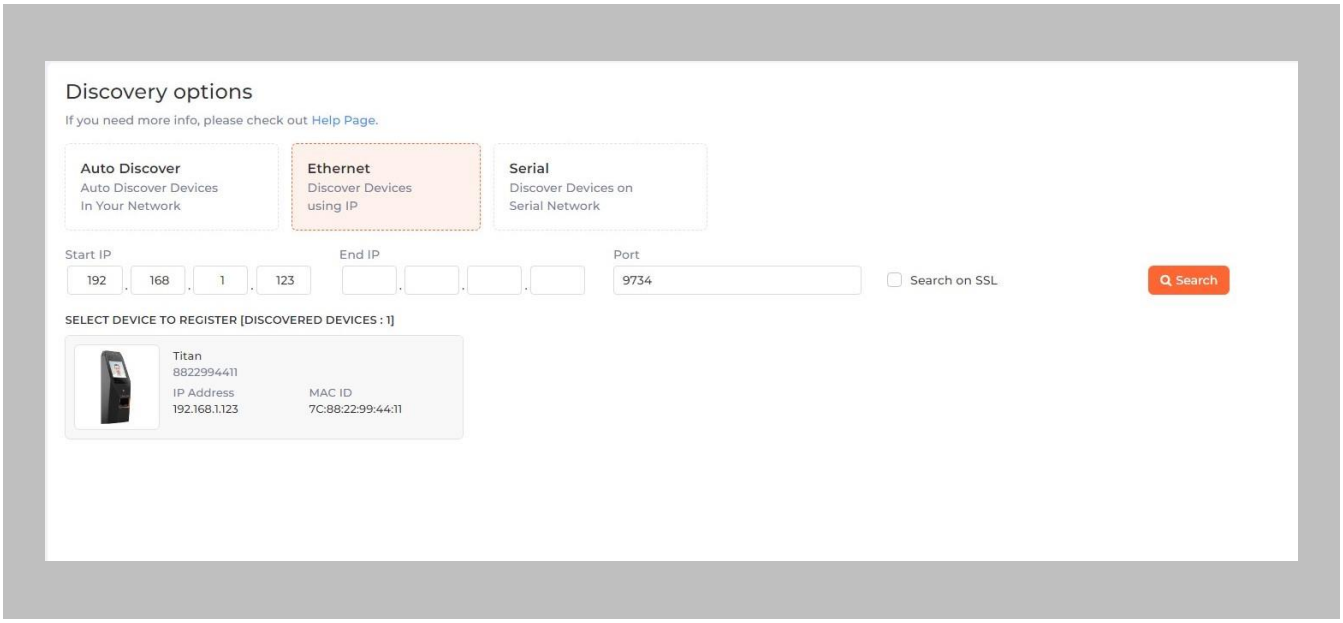


Figure 30: IXM WEB - Search Device Using IP Address

STEP 3

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

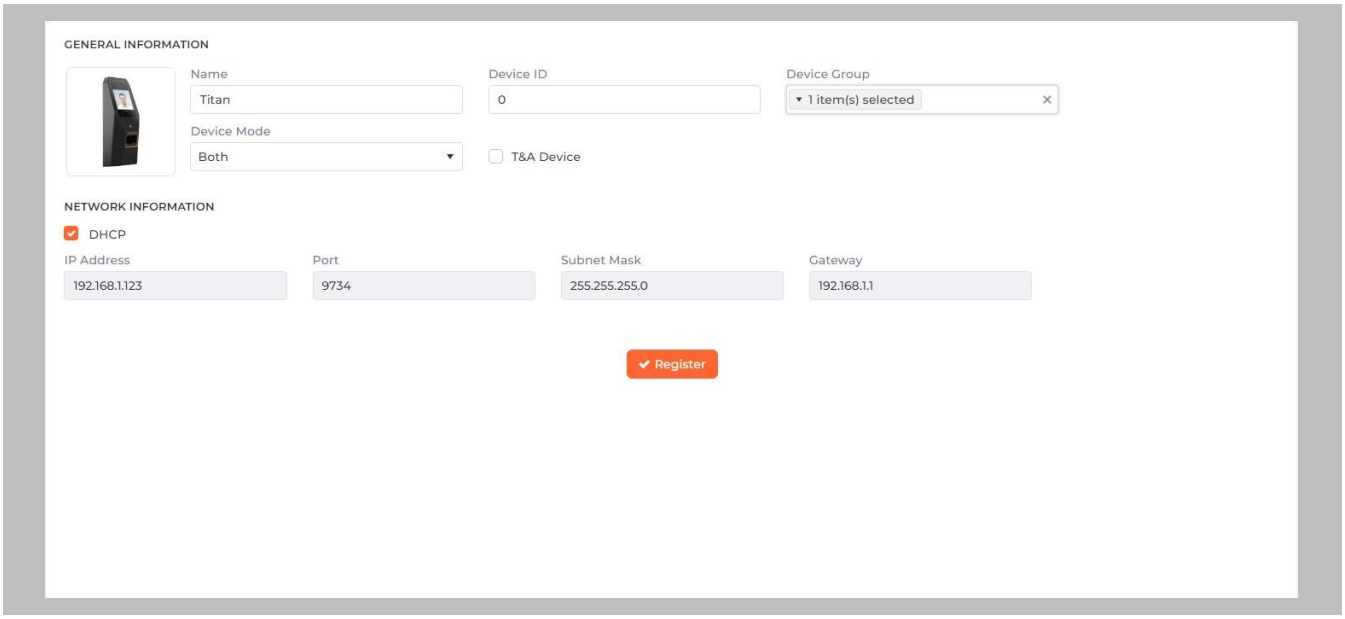


Figure 31: IXM WEB - Register Device

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**.

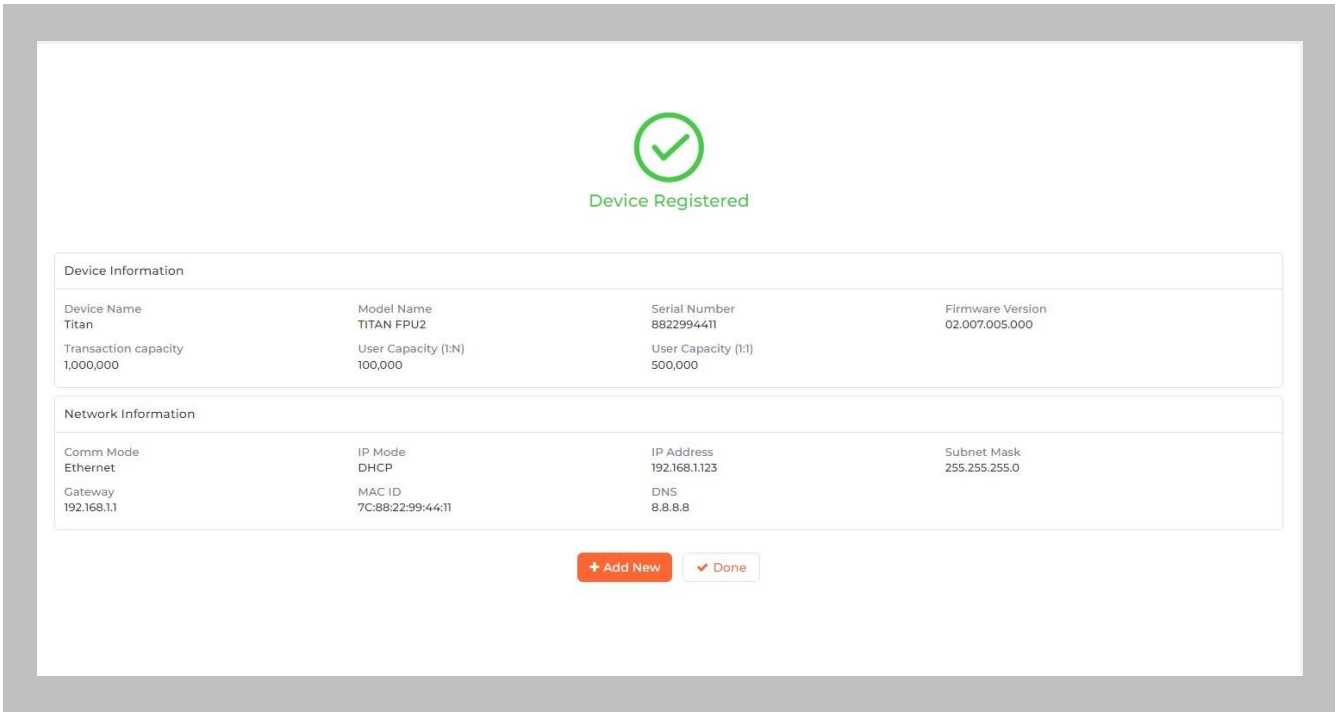


Figure 32: IXM WEB - Device Registration Complete

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).

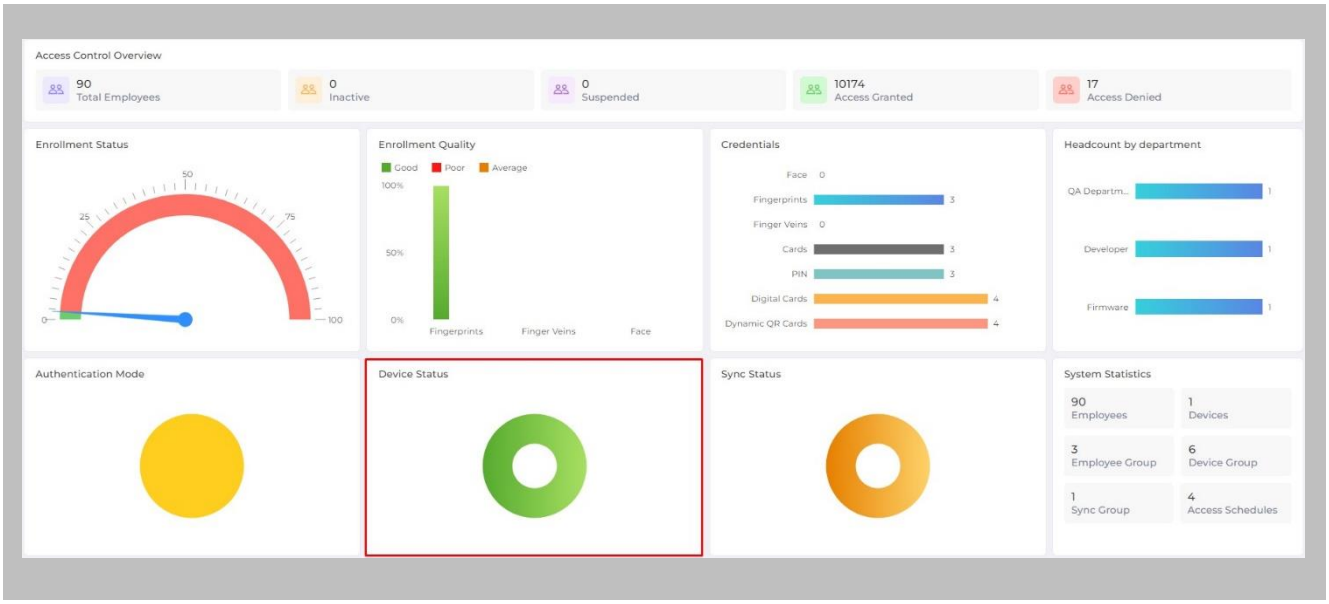


Figure 33: IXM WEB - Dashboard, Device Status

7. 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**.

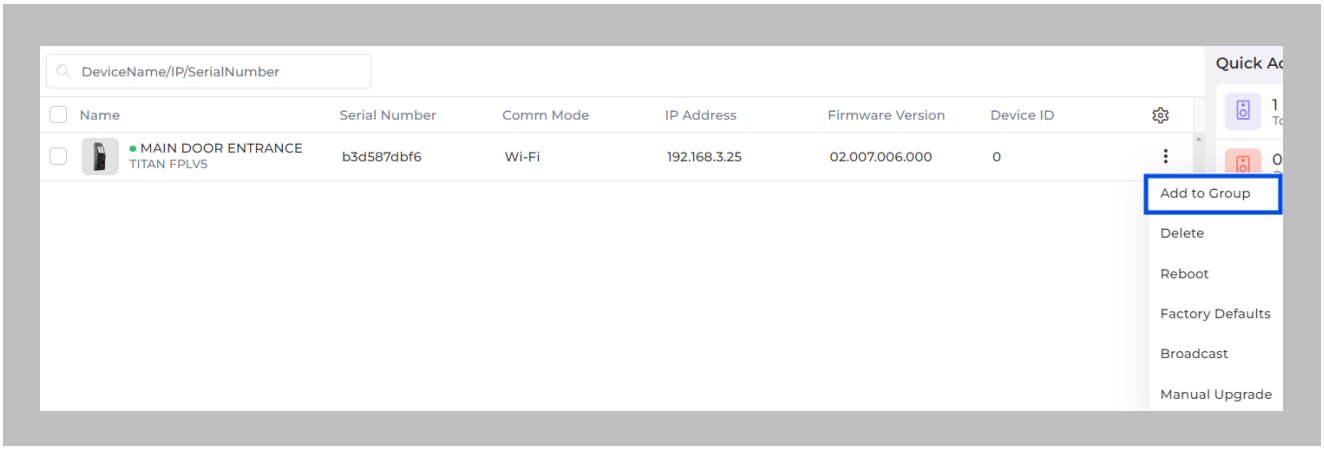


Figure 34: IXM WEB - Assign Device Group

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.**

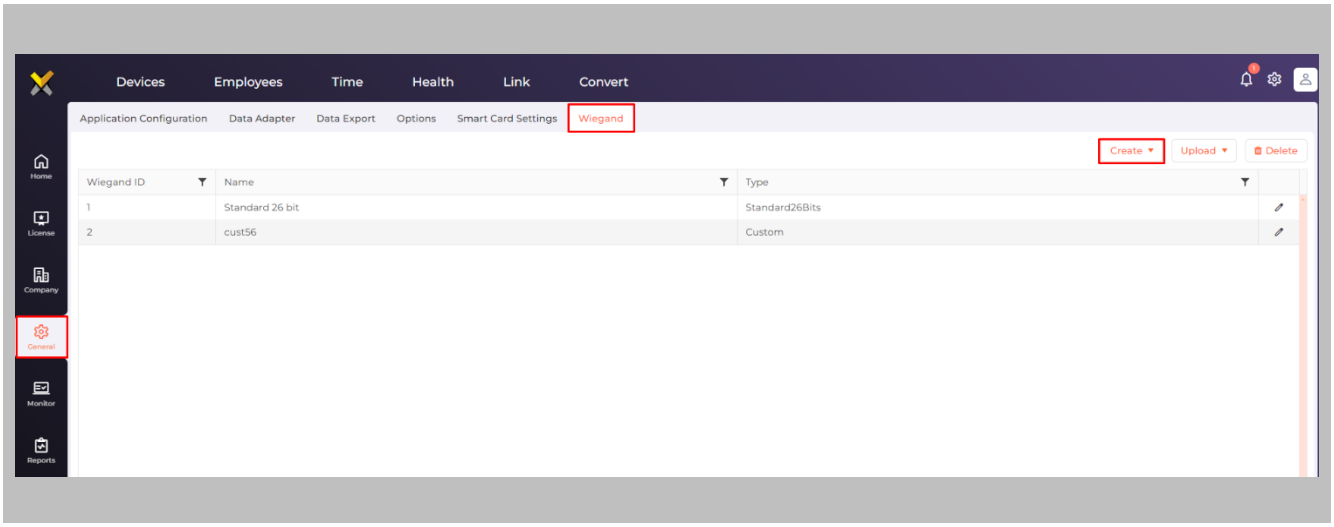


Figure 35: IXM WEB - Create Wiegand Format

STEP 2

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

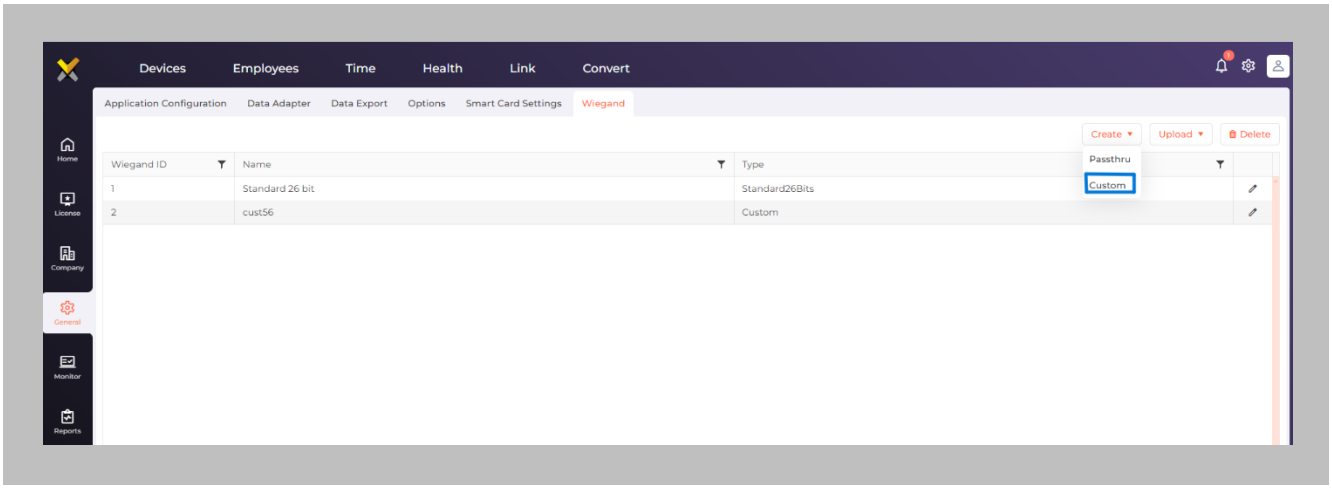


Figure 36: IXM WEB - Create Custom Wiegand Format

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.

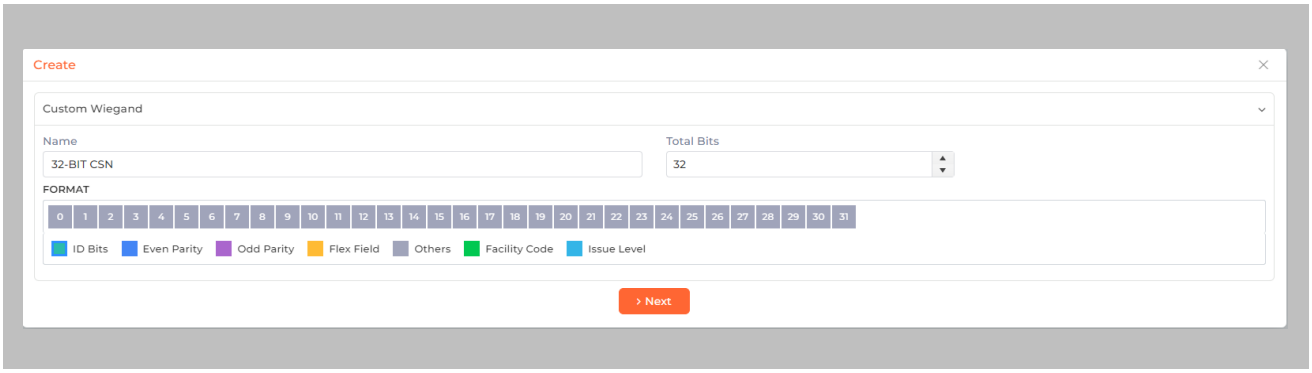


Figure 37: IXM WEB - Custom Wiegand Format

STEP 4

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

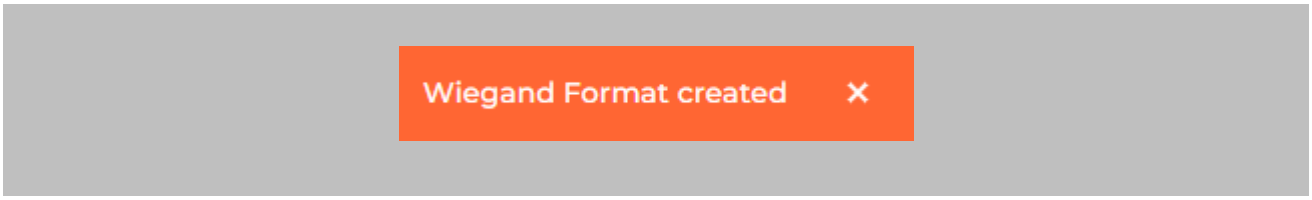


Figure 38: IXM WEB – Custom Wiegand Format Created

STEP 5

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

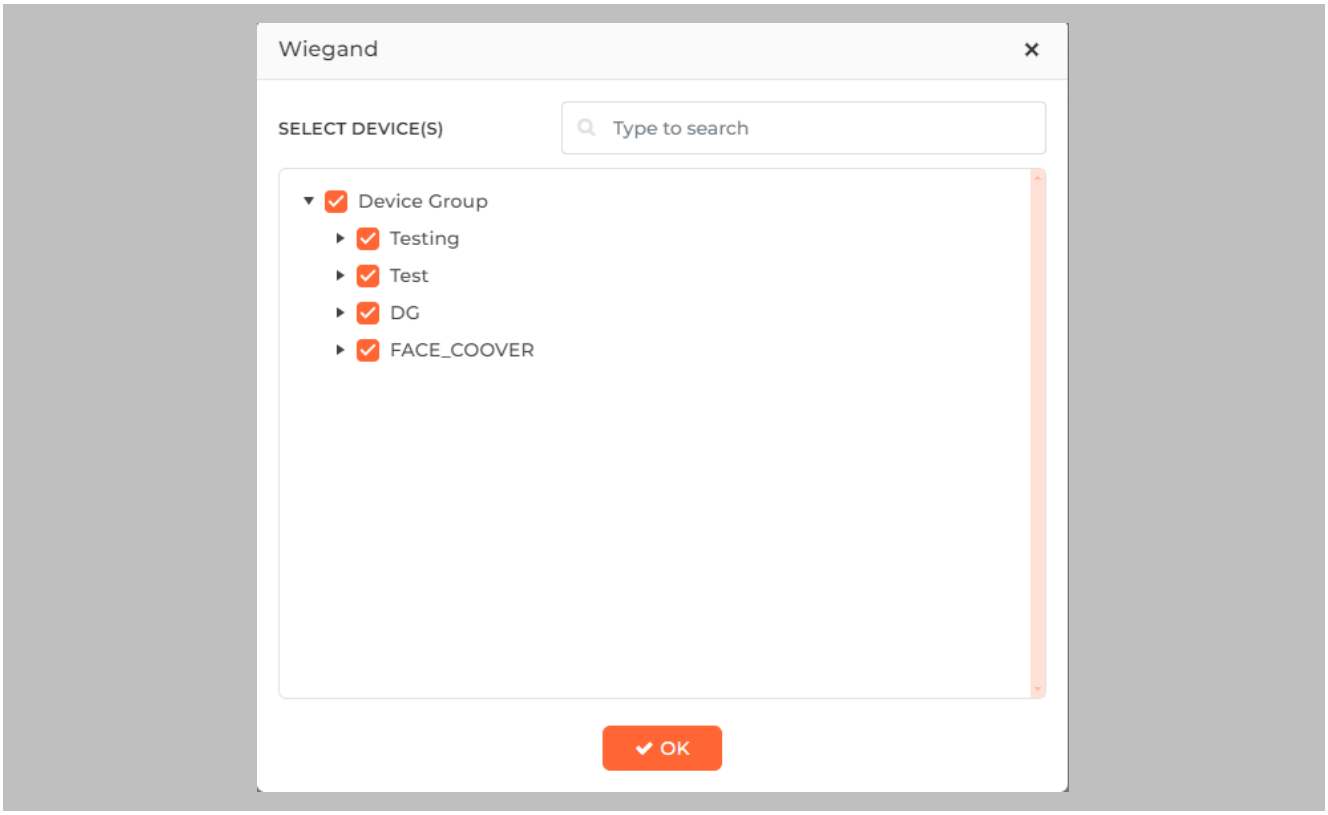


Figure 39: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invixium Readers

Note: Face and finger will always give a Wiegand output based on the initial card that was synced from WIN-PAK to IXM WEB.

The created Wiegand will be used to define which output format will be sent to WIN-PAK.

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.

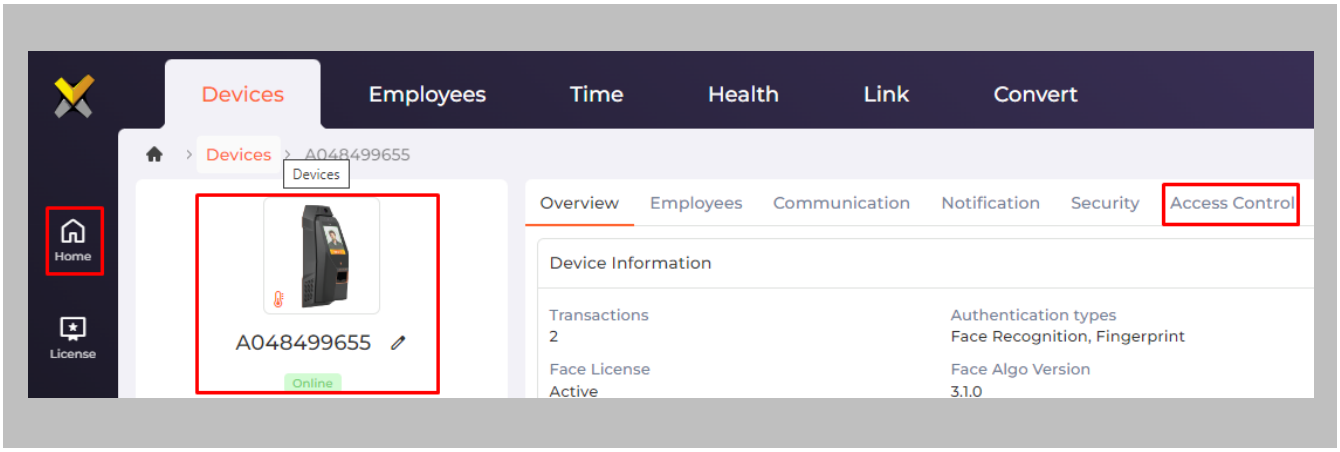


Figure 40: IXM WEB - Navigate to Access Control Tab

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.

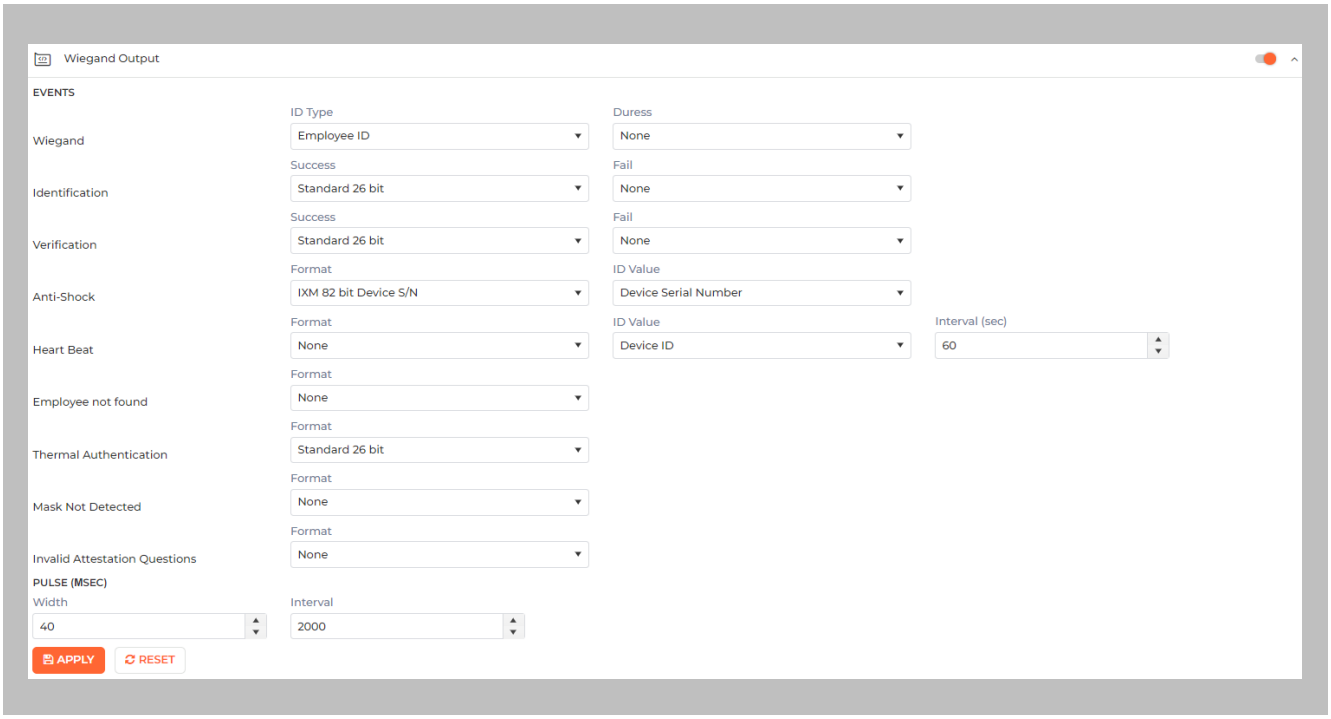


Figure 41: IXM WEB - Wiegand Output

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 WIN-PAK, select either Default Card or Actual Card.

Empoyee ID: This is auto generated ID by IXM WEB for an imported cardholder in WIN-PAK.

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.**

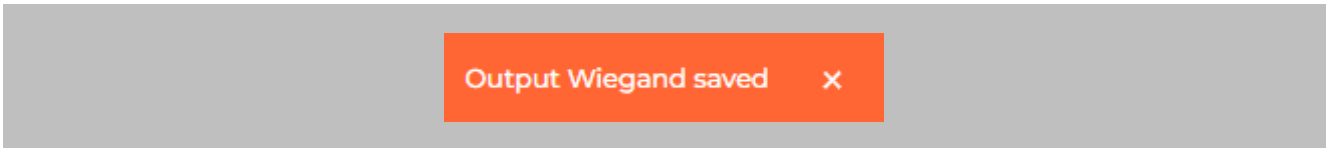


Figure 42: IXM WEB - Save Output Wiegand

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

Configuring Panel Feedback with WIN-PAK

Procedure

STEP 1

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

STEP 2

Connect the **LED** of the WIN-PAK 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**.

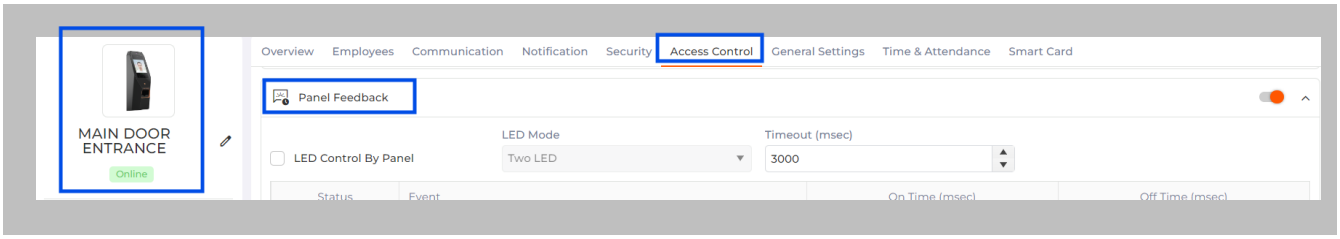


Figure 43: IXM WEB - Panel Feedback

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**.

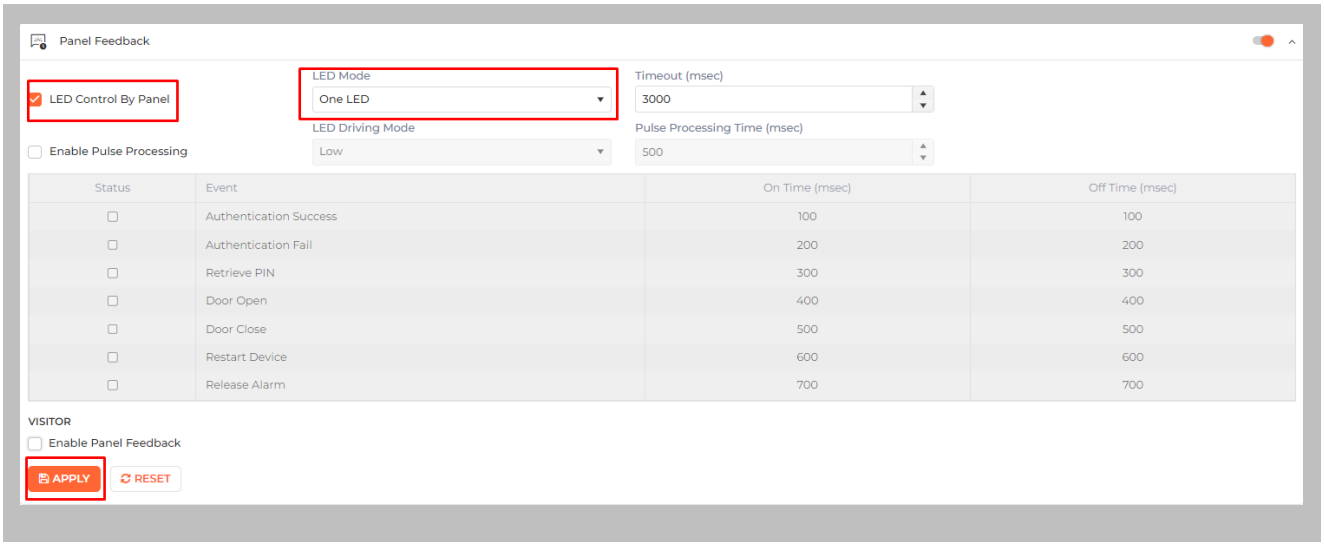


Figure 44: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.

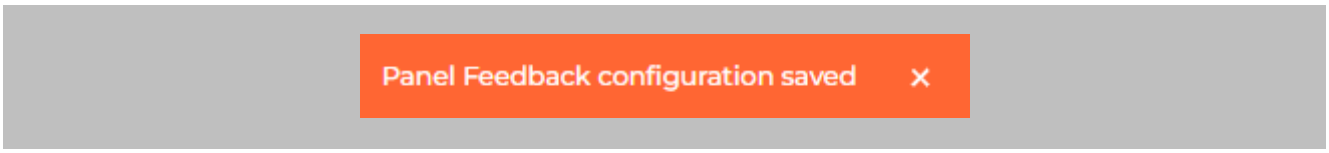


Figure 45: IXM WEB - Save Panel Feedback

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.

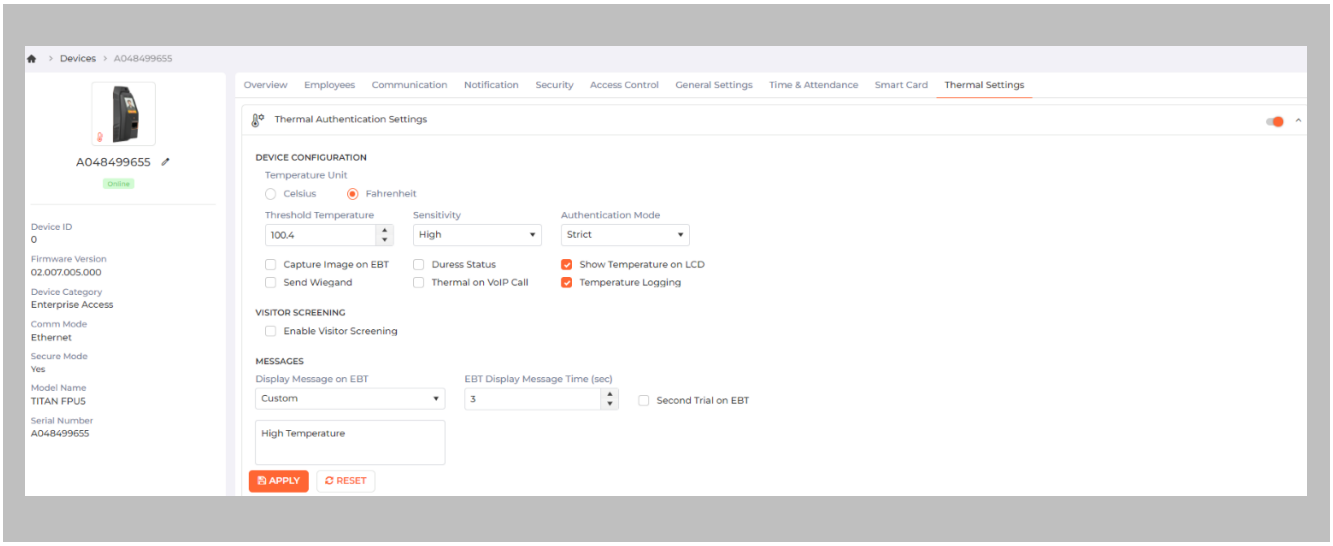


Figure 46: IXM WEB - Thermal Settings

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**.

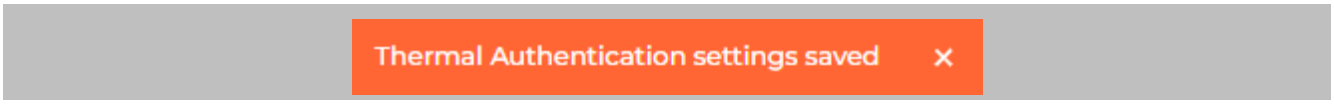


Figure 47: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

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

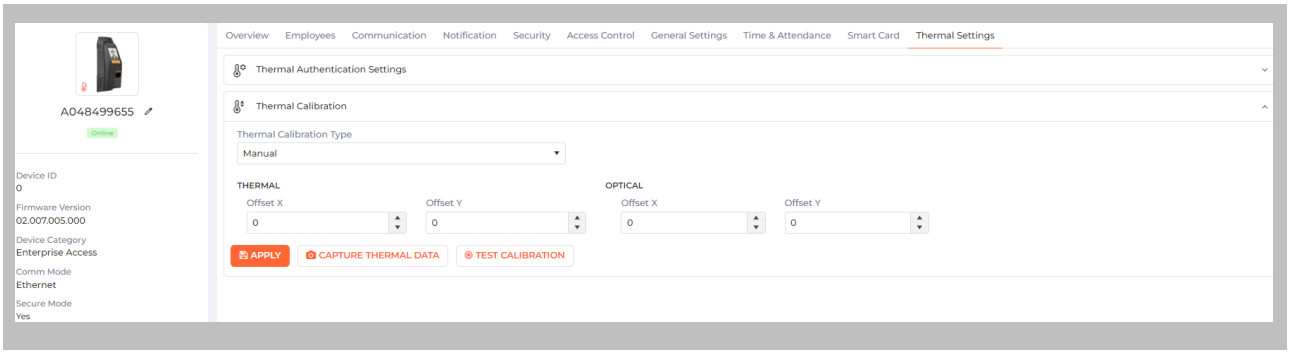


Figure 48: IXM WEB - Thermal Calibration Settings

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**.

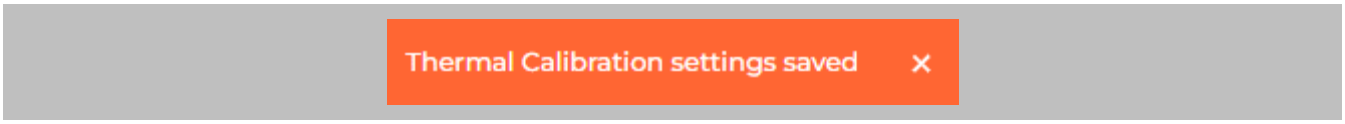


Figure 49: IXM WEB - Save Thermal Calibration Settings

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.

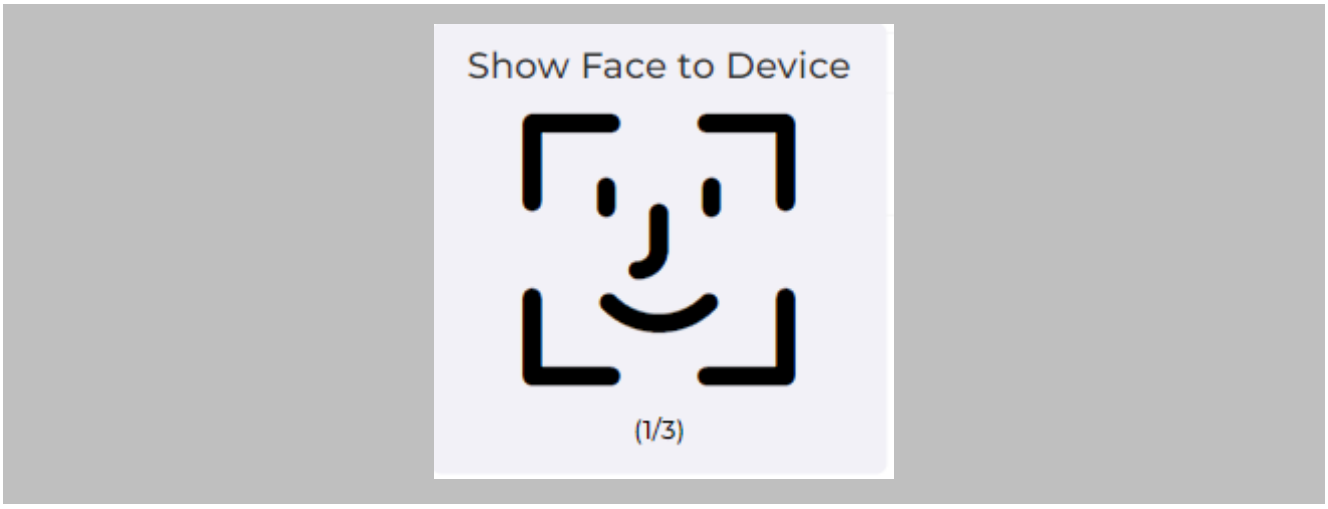


Figure 50: IXM WEB - Capture Thermal Data

STEP 4

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

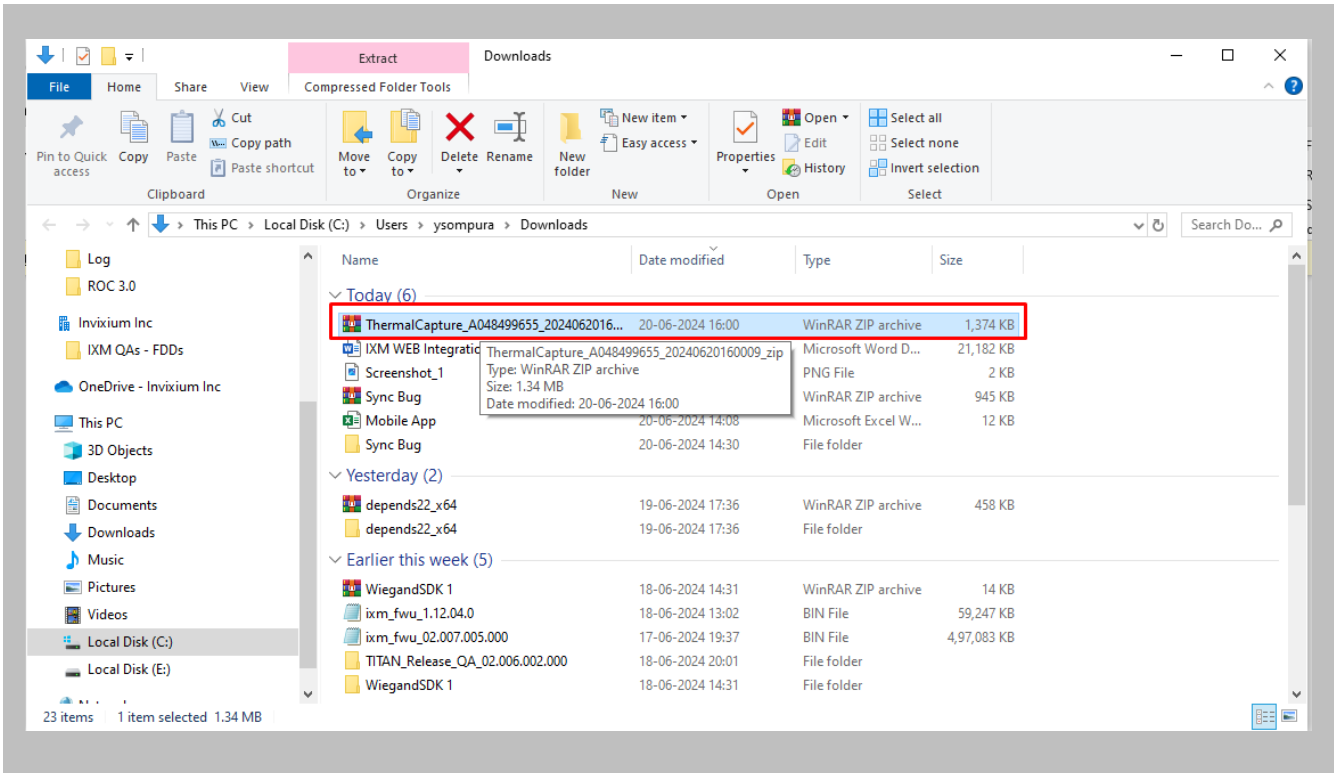


Figure 51: IXM WEB - Save Captured Thermal Data

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**.

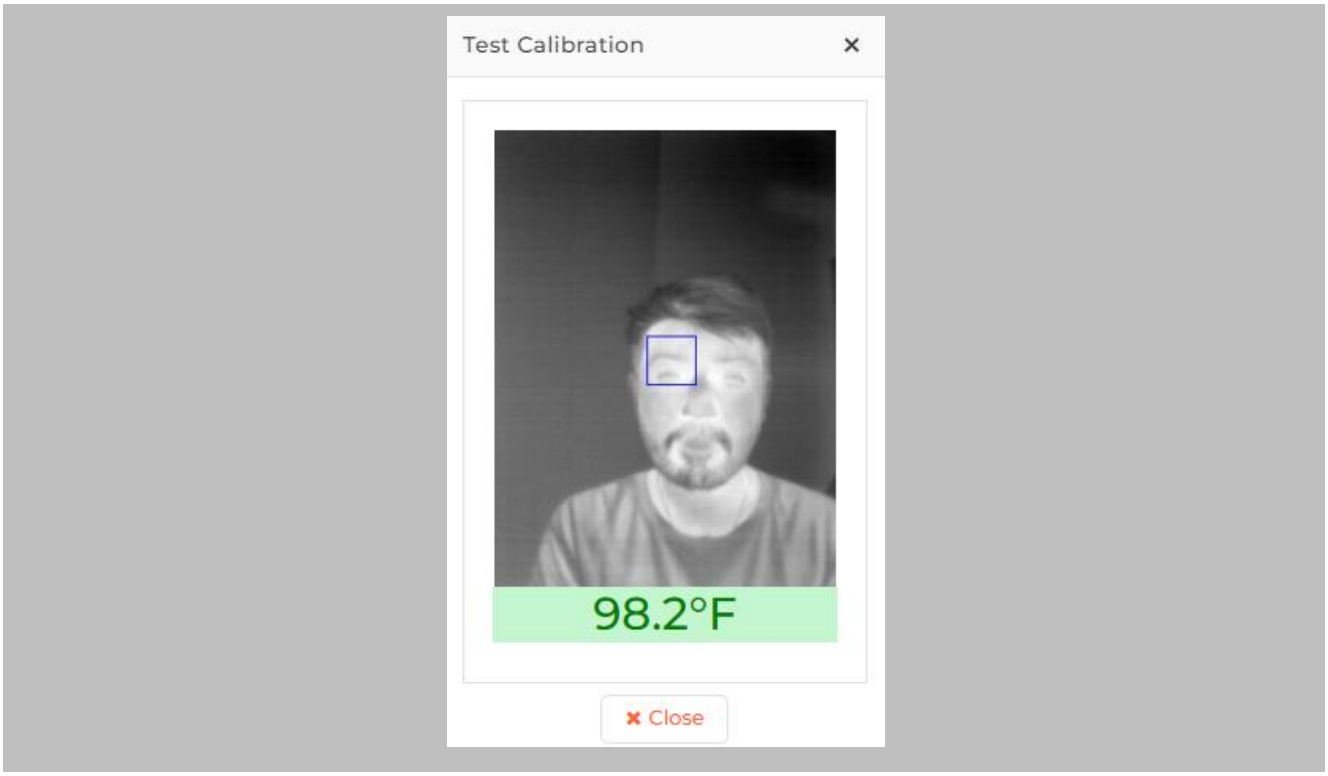


Figure 52: IXM WEB - Test Thermal Calibration

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**.

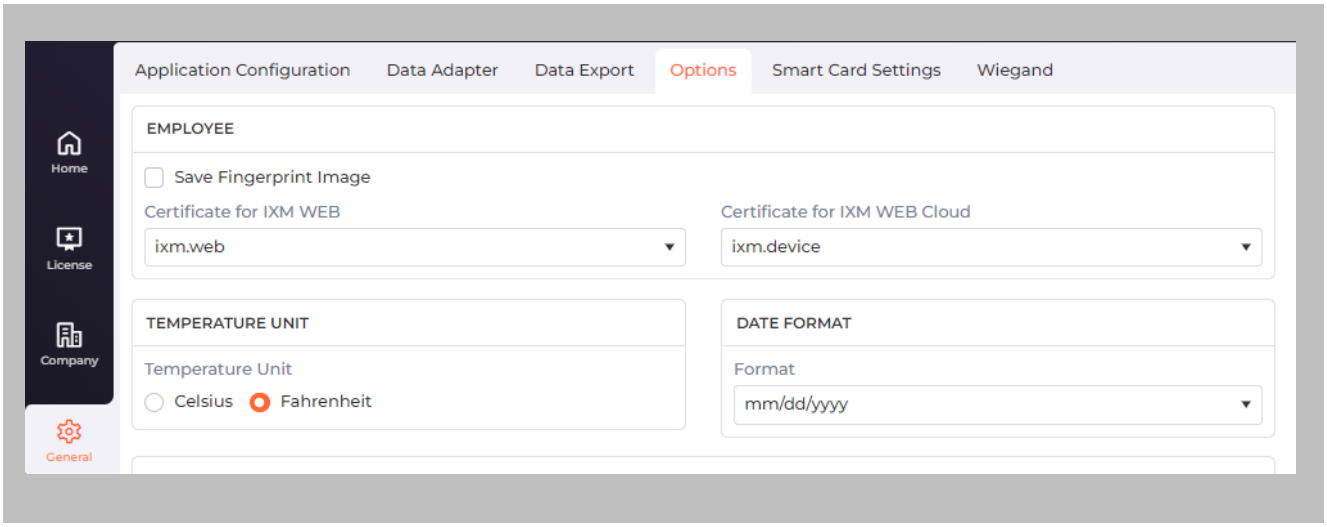


Figure 53: IXM WEB - Option to Change Temperature Unit

STEP 2

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

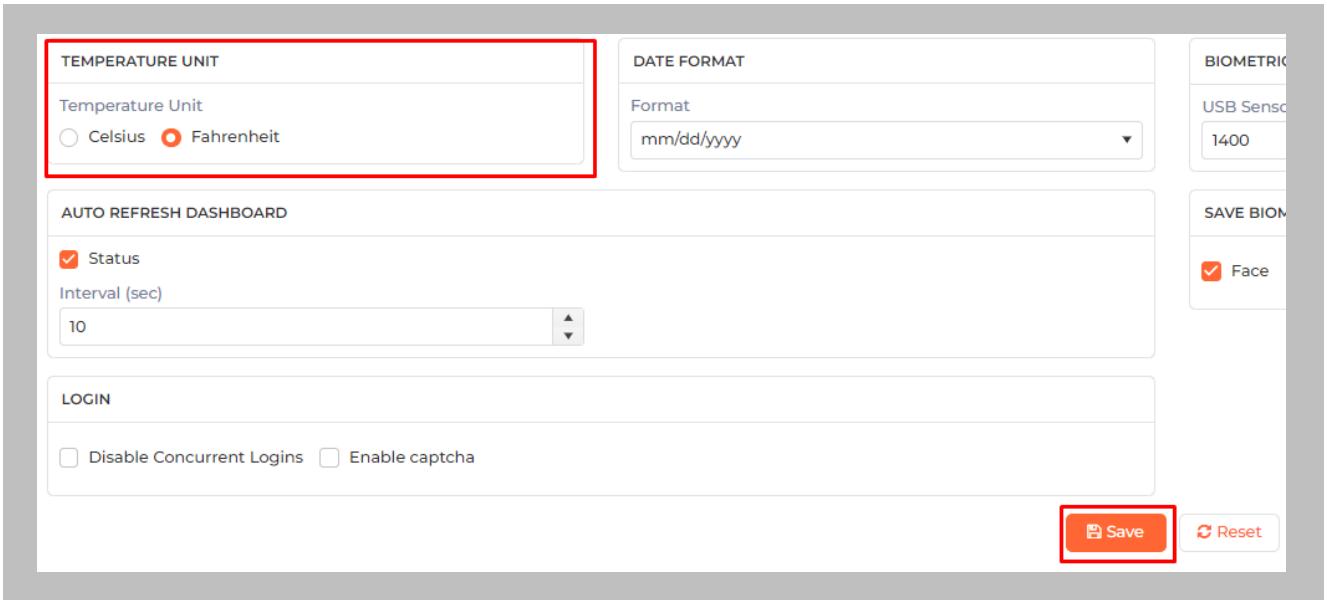


Figure 54: IXM WEB - Save Temperature Unit Setting

Configuring Mask Authentication Settings

STEP 1

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

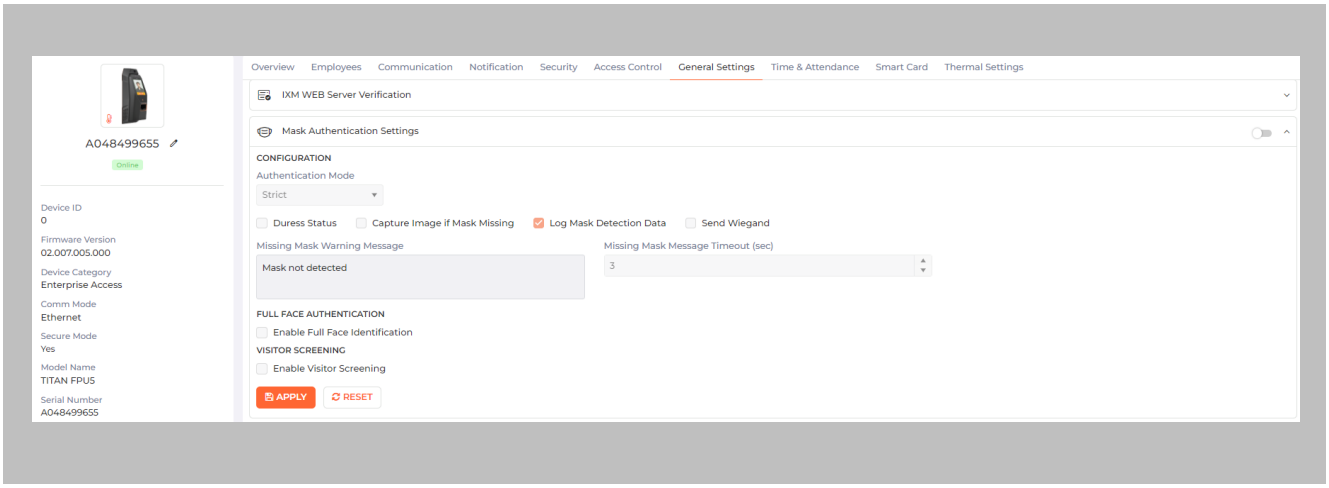


Figure 55: IXM WEB - Mask Authentication Settings

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**.

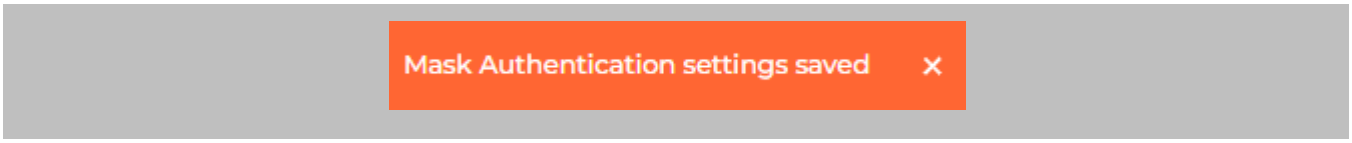


Figure 56: IXM WEB - Save Mask Settings

8. 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.

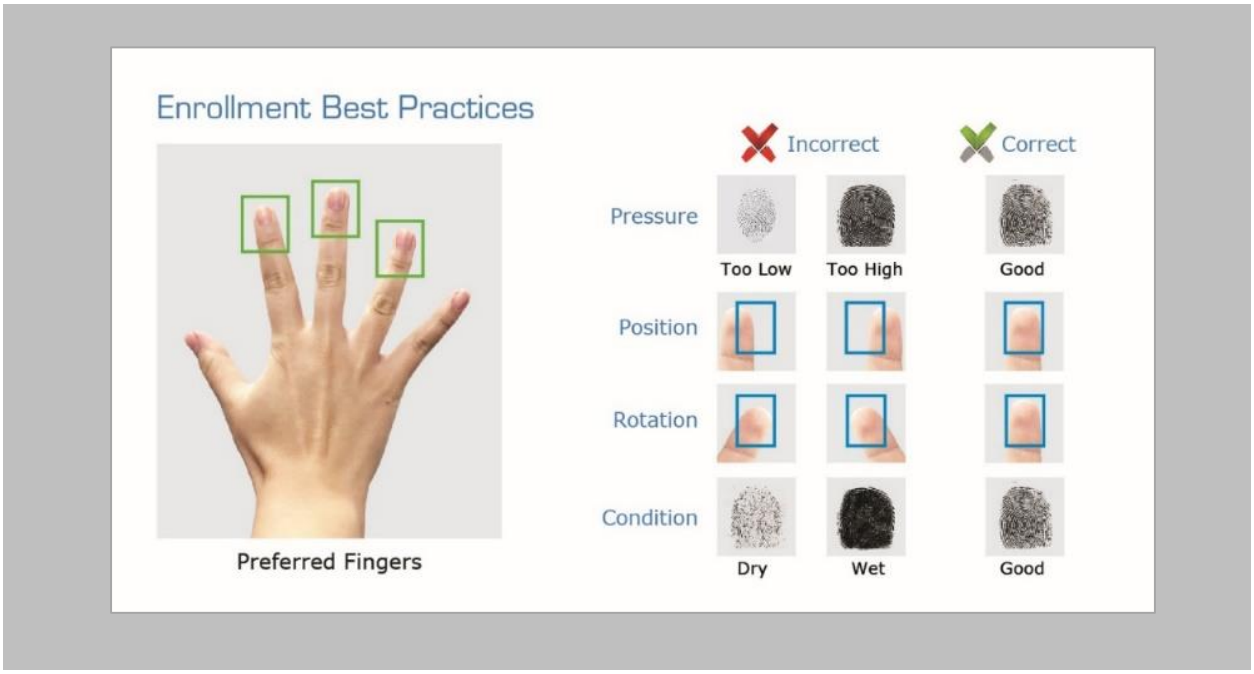


Figure 57: Fingerprint Enrollment Best Practices

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 58: 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.

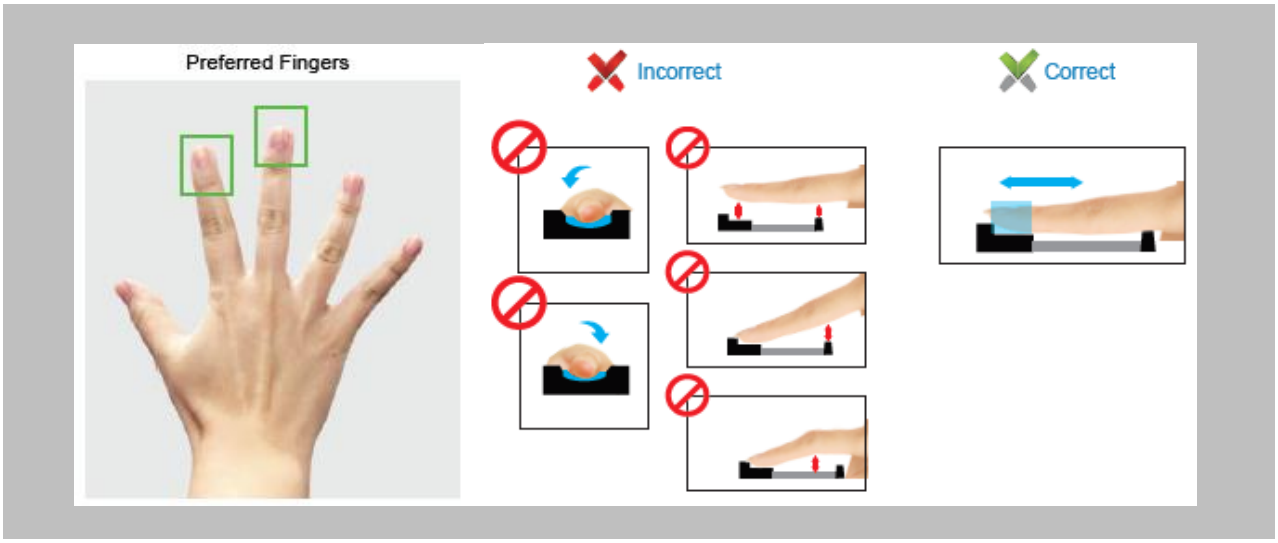


Figure 59: Finger Vein Enrollment Best Practices

Face Enrollment Best Practices

- Invixium recommends standing at least 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.

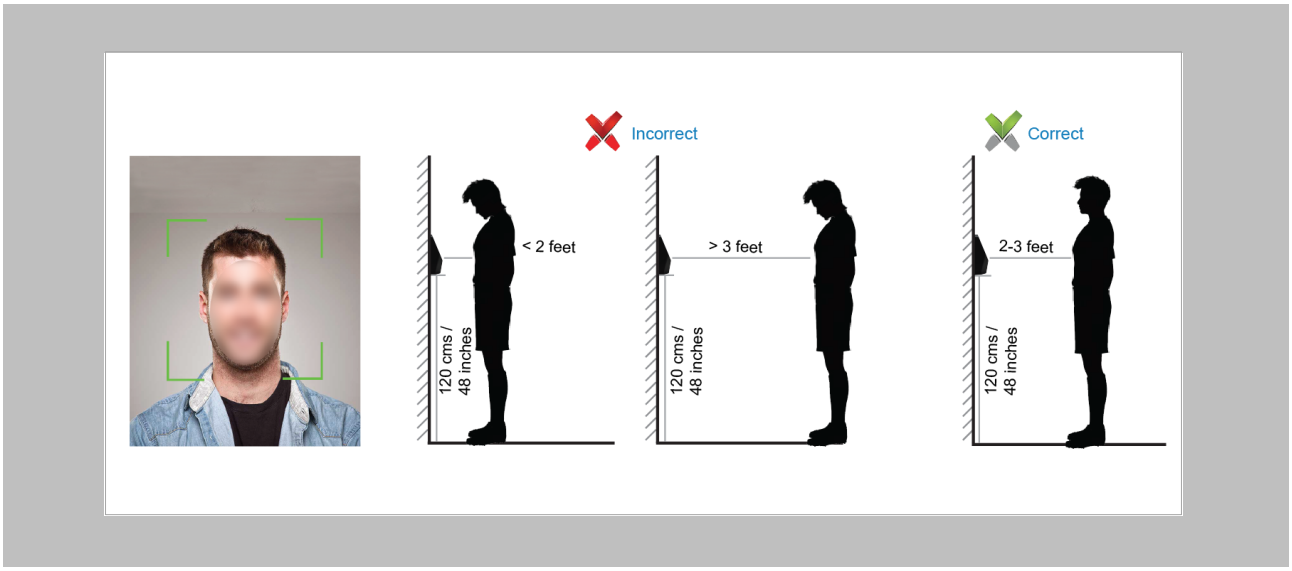


Figure 60: Face Enrollment Best Practices

9. Configure Note Field for Email in WIN-PAK

The following settings are required in WIN-PAK to synchronize the email address of the cardholder from WIN-PAK to IXM WEB.

Procedure

STEP 1

Login to **WIN-PAK User Interface** → Go to **Configuration** → **Card Holder** → **Note Field Template.**

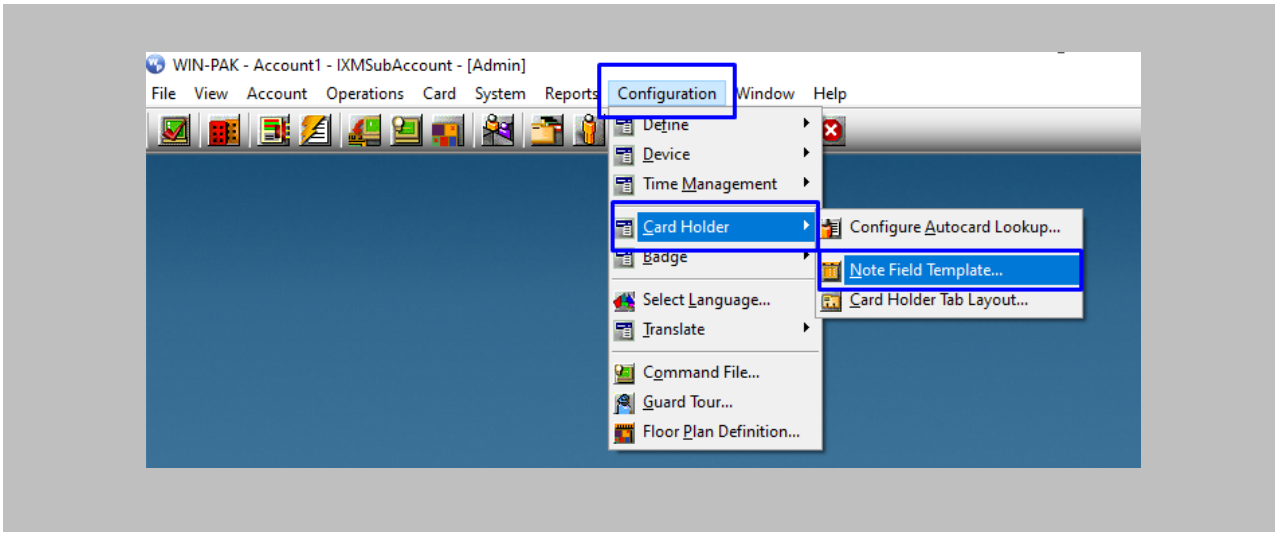


Figure 61: WIN-PAK Note Field Template

STEP 2

On the **Note Field Template** Window click on **Add**.

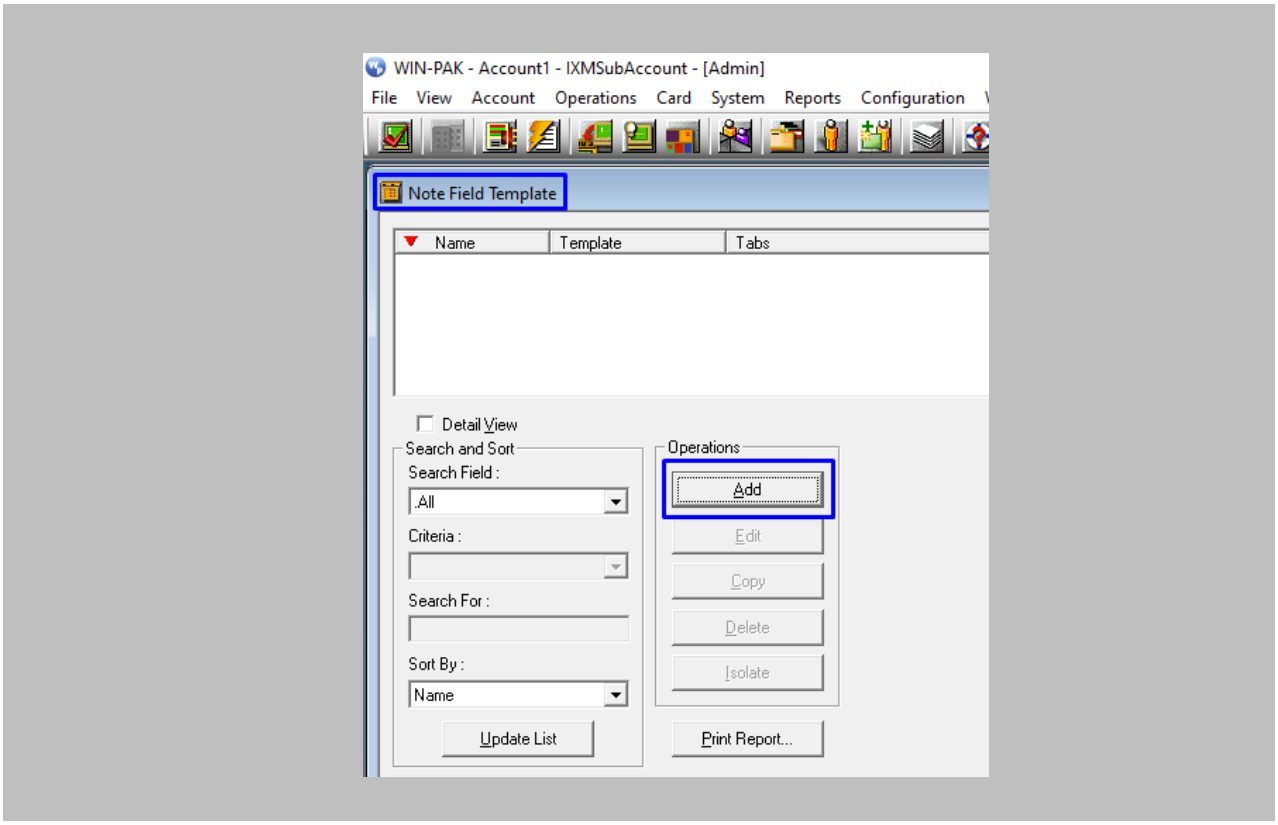


Figure 62: WIN-PAK Add New Note Field

STEP 3

Enter the **Name** of the note field → Click on the **OK** button

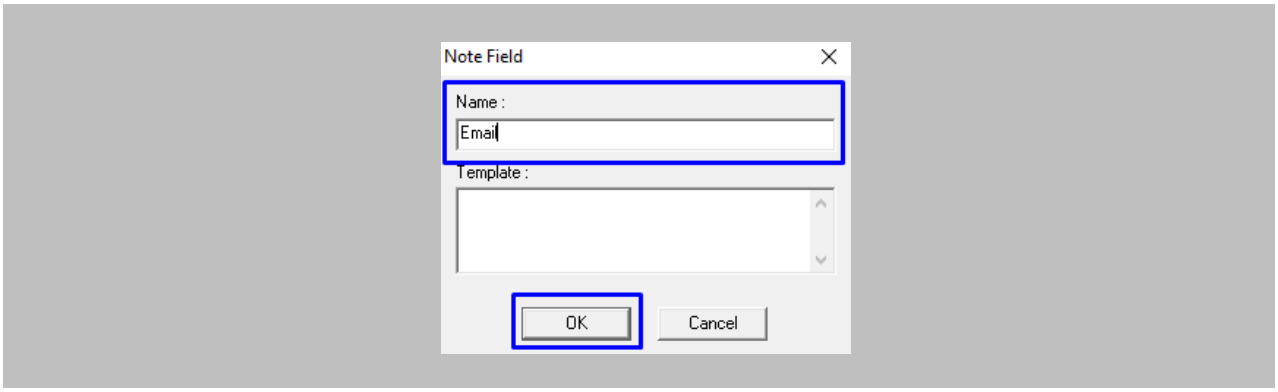


Figure 63: WIN-PAK Create Note Field

STEP 4

Go to **Configuration** → **Card Holder** → **Card Holder Tab Layout.**

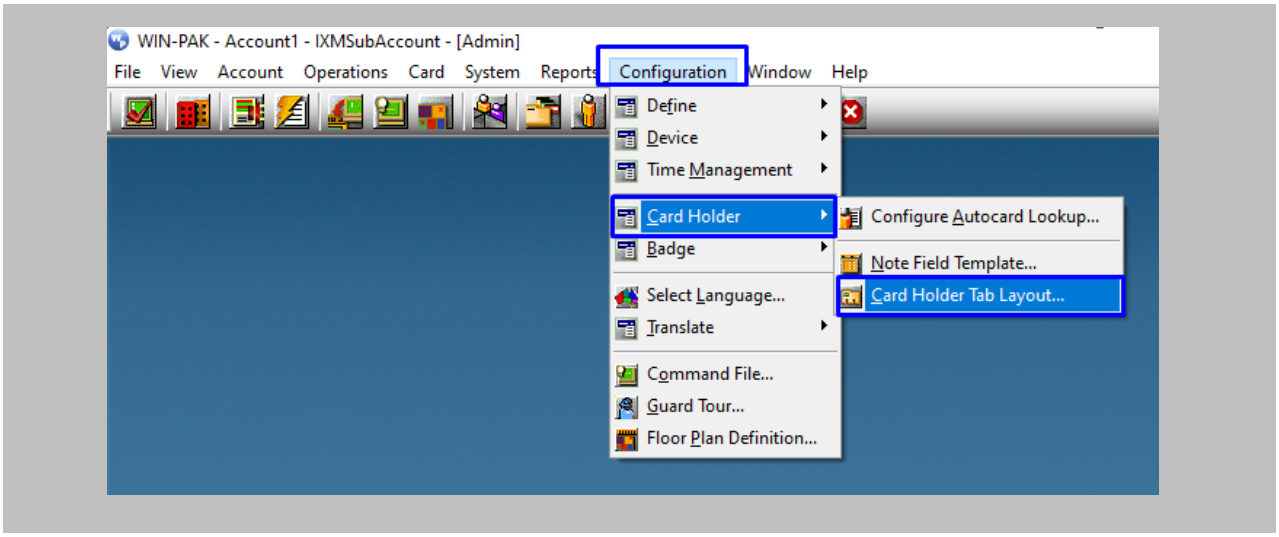


Figure 64: WIN-PAK Card Holder Tab Layout

STEP 5

On the **Card Holder Tab Layout** Window, click on **Add**.

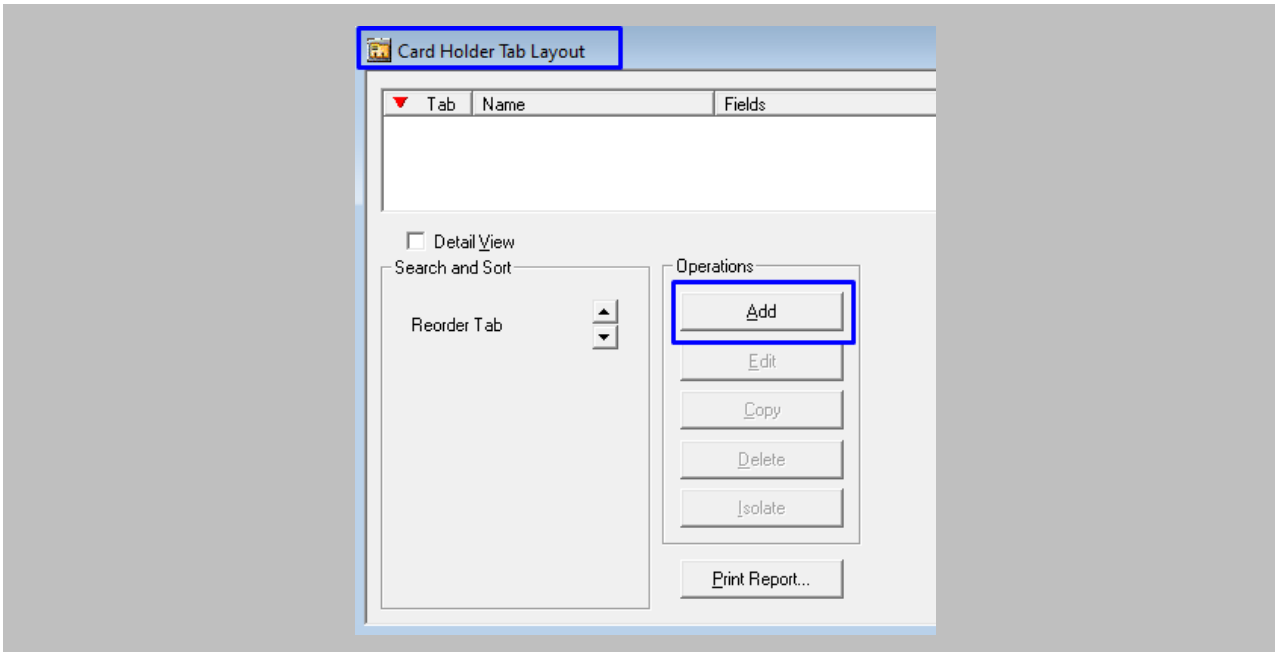


Figure 65: WIN-PAK Add New Card Holder Tab Layout

STEP 6

Enter the **Tab Name** → Select the note field from the list of **Available Note Fields** → Click on **Add** button.

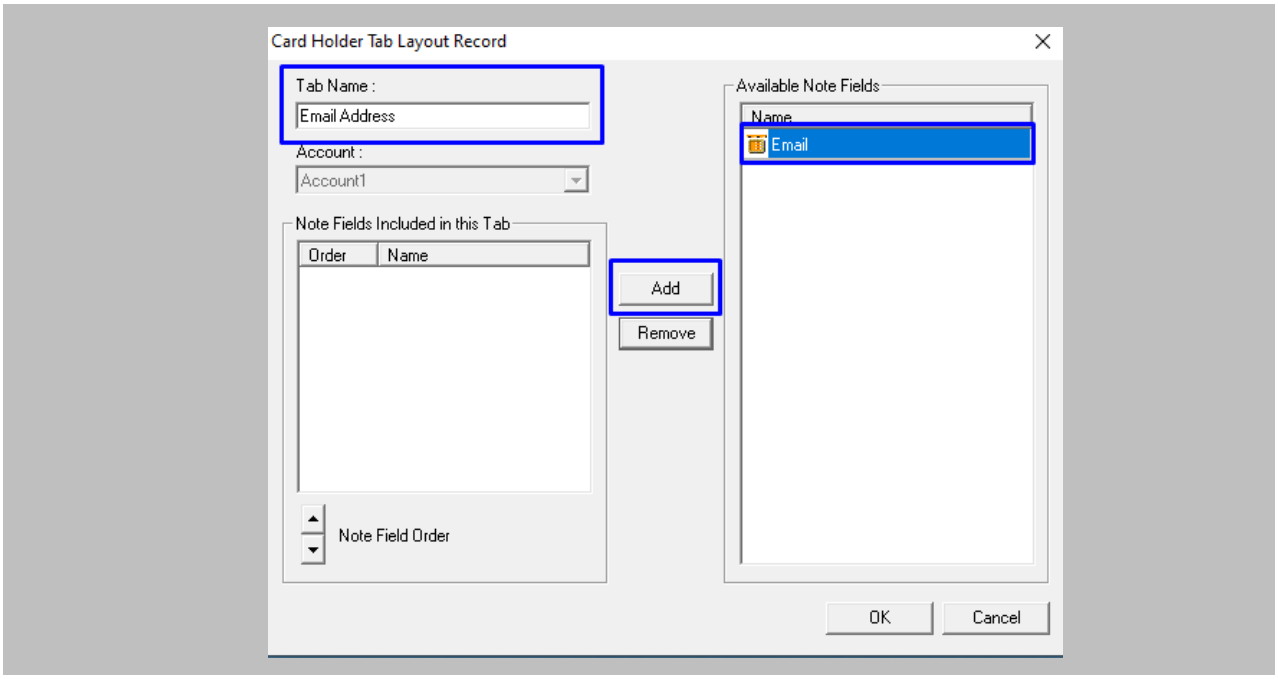


Figure 66: WIN-PAK Add Note Field to Card Holder Tab

STEP 7

Click on **OK**.

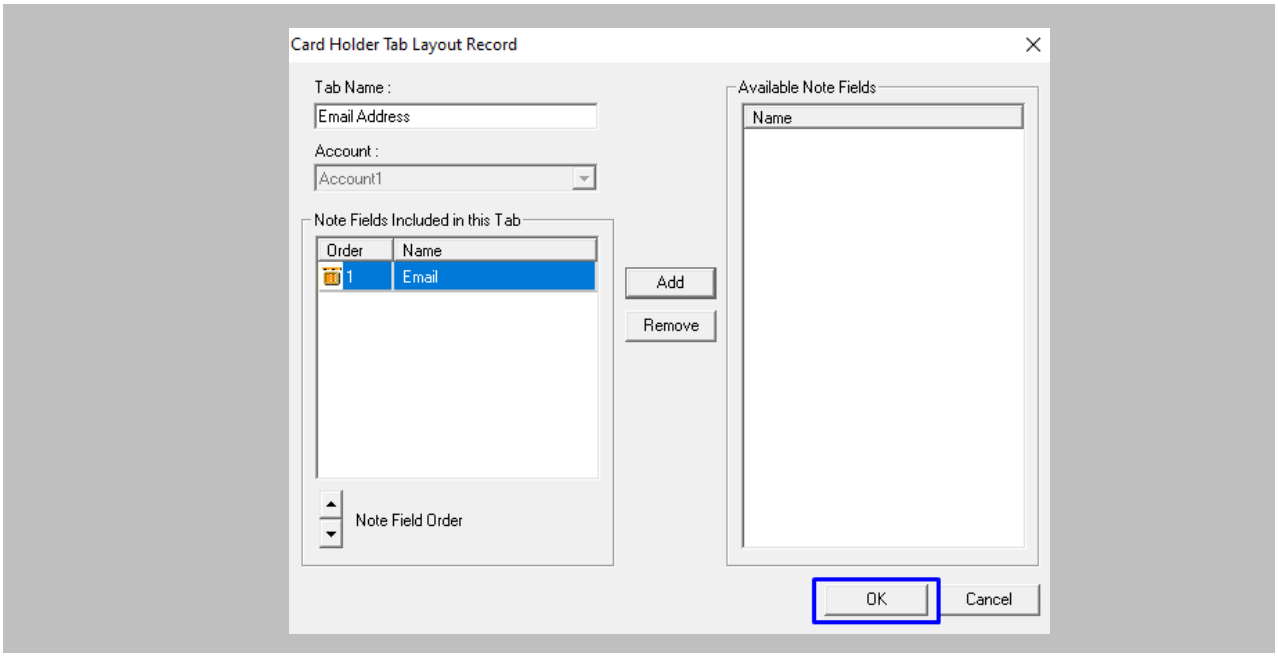


Figure 67: Save Card Holder Tab Layout

The custom **Note** field will be visible on the **Card Holder** window as below.

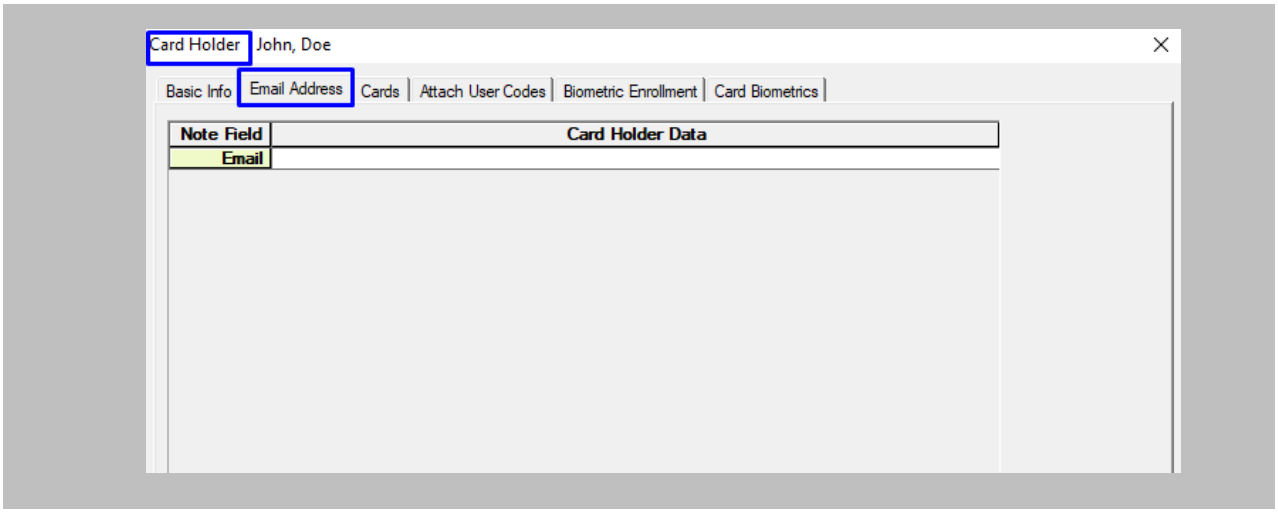


Figure 68: Add Card Holder Window

10. Prerequisites for Integration when IXM WEB and Honeywell WIN-PAK are Installed on Different Servers

Configuration Of Group Policy

Procedure

STEP 1

Open **Run** on the machine where WIN-PAK is installed → Enter **'gpedit.msc'.**

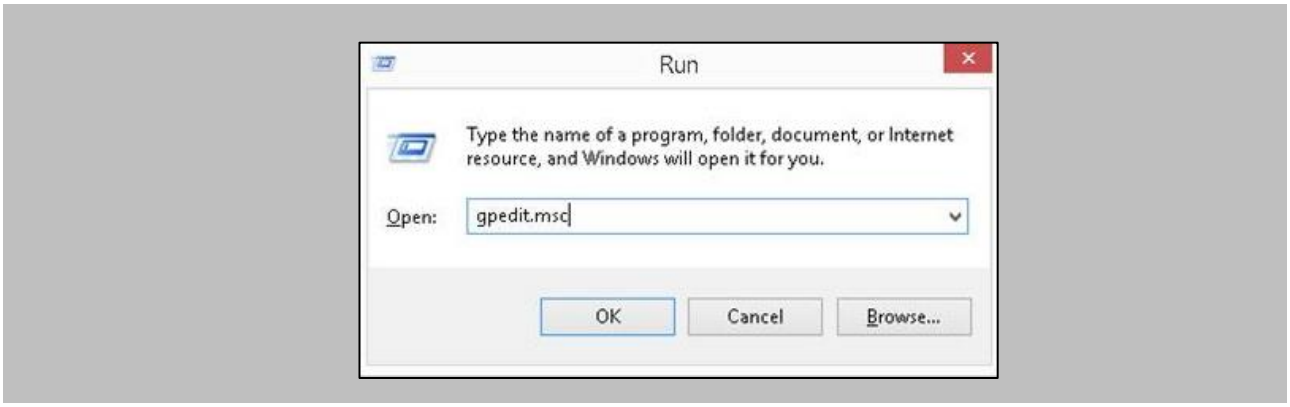


Figure 69: WIN-PAK Open Group Policy Editor

STEP 2

Navigate to the **Local Computer policy** → **Computer Configuration** → **Windows Settings** → **Security Settings** → **Local Polices** → **Security Options.**

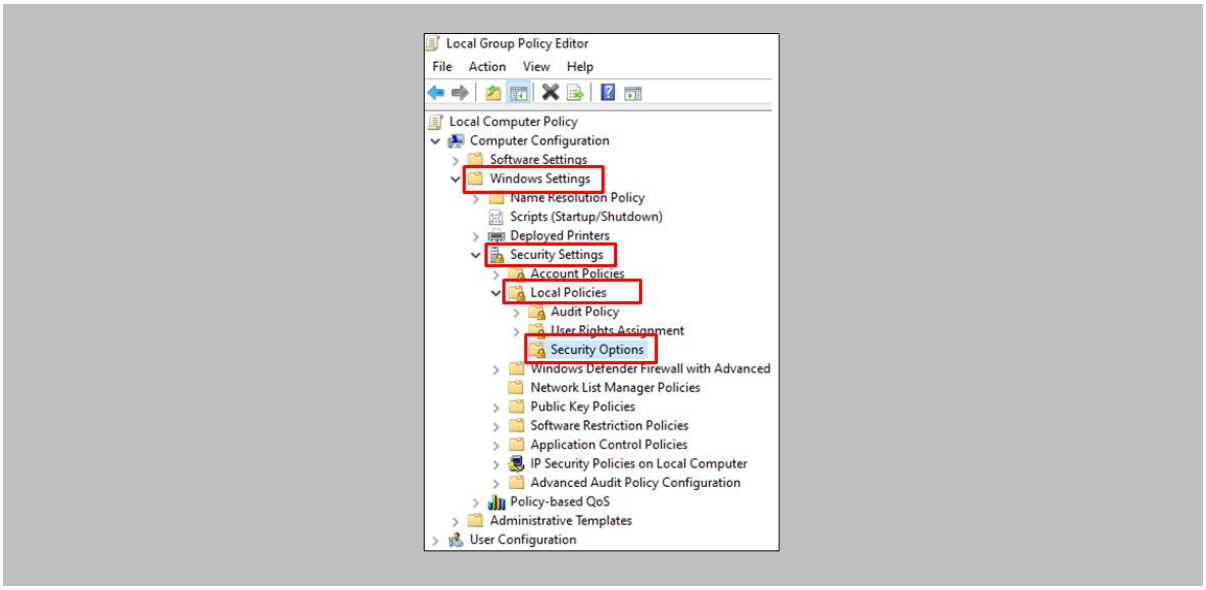


Figure 70: WIN-PAK Security Options

STEP 3

From the list of policies, select **DCOM Machine Access Restriction in Security Description Definition Language (SDDL) syntax** → Right click and click on **Properties**.

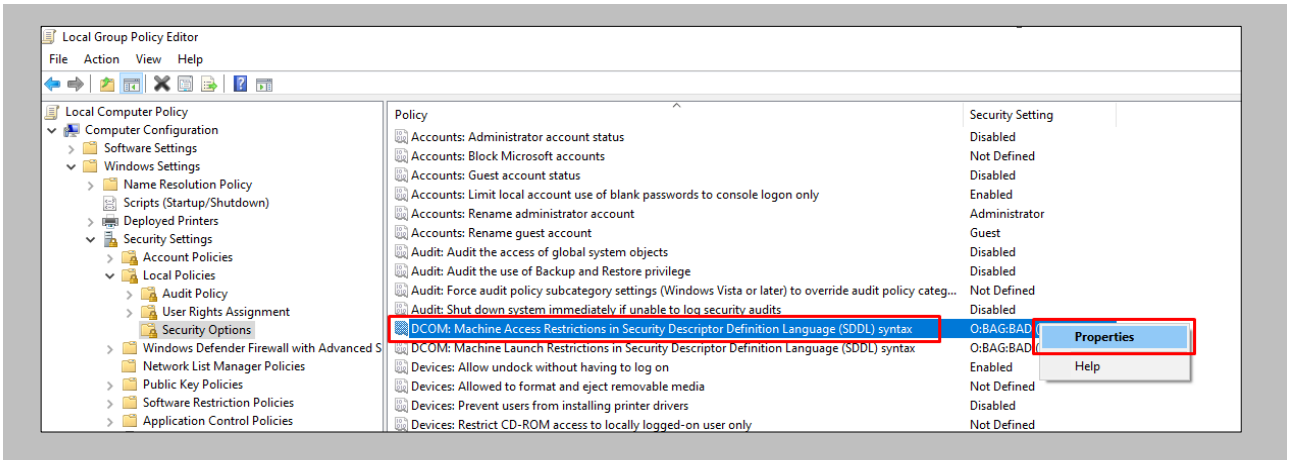


Figure 71: WIN-PAK DCOM SDDL Syntax

STEP 4

Click on **Edit Securities.**

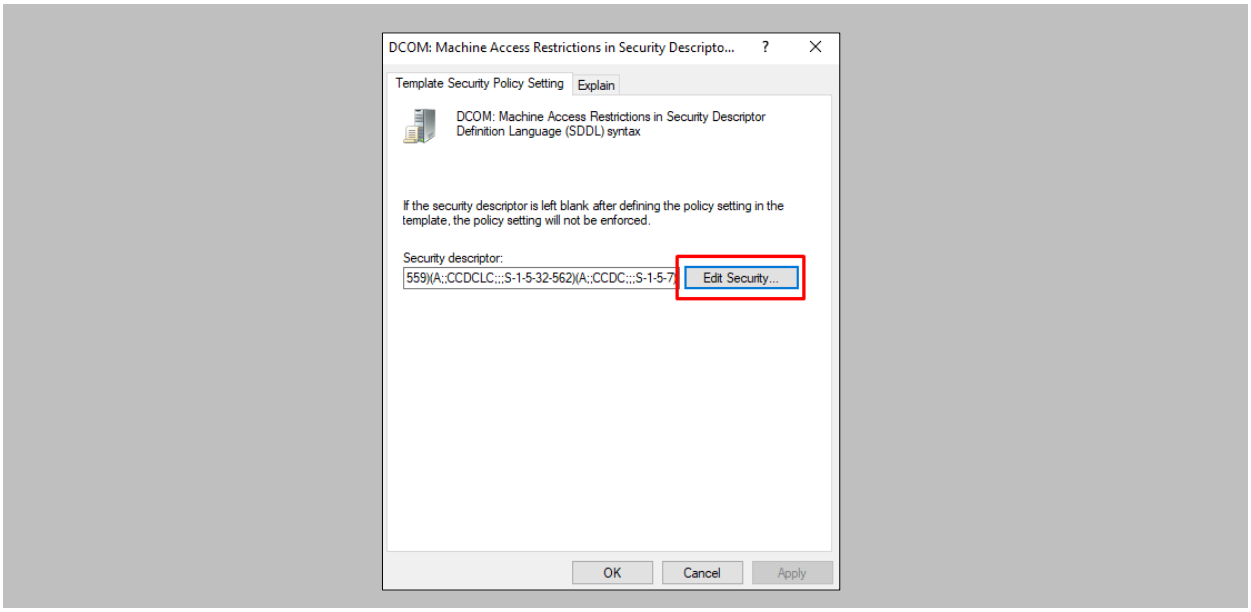


Figure 72: WIN-PAK DCOM Access Restrictions - Edit Securities

STEP 5

Give **'Local Access'** and **'Remote Access'** permissions for the below groups or usernames.

- Distributed COM Users
- All APPLICATION PACKAGES
- Performance Log User
- Everyone

Click on **OK** once permissions are assigned.

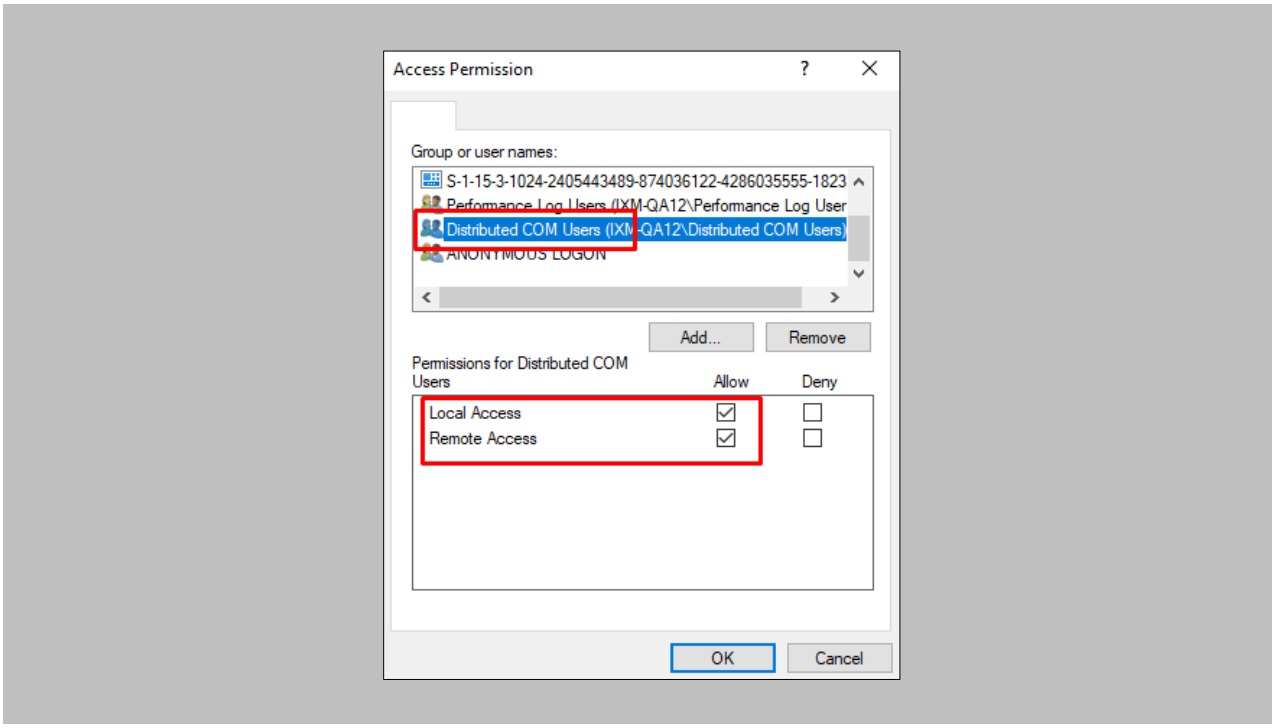


Figure 73: WIN-PAK Access Permissions for DCOM Users

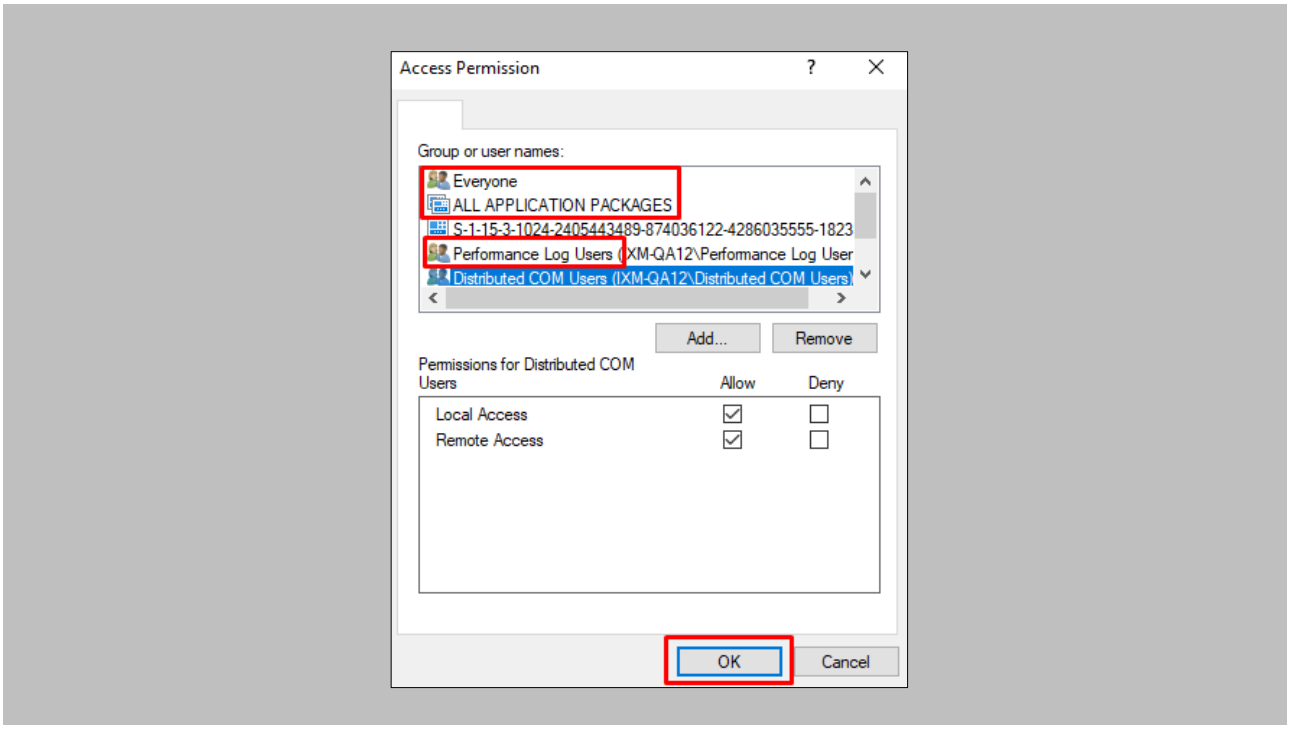


Figure 74: WIN-PAK Access Permissions for Users and Groups

STEP 6

From the list of policies, select **DCOM Machine Launch Restriction in Security Description Definition Language (SDDL) syntax** → Right click and click on **Properties** → Click on **Edit Securities**.

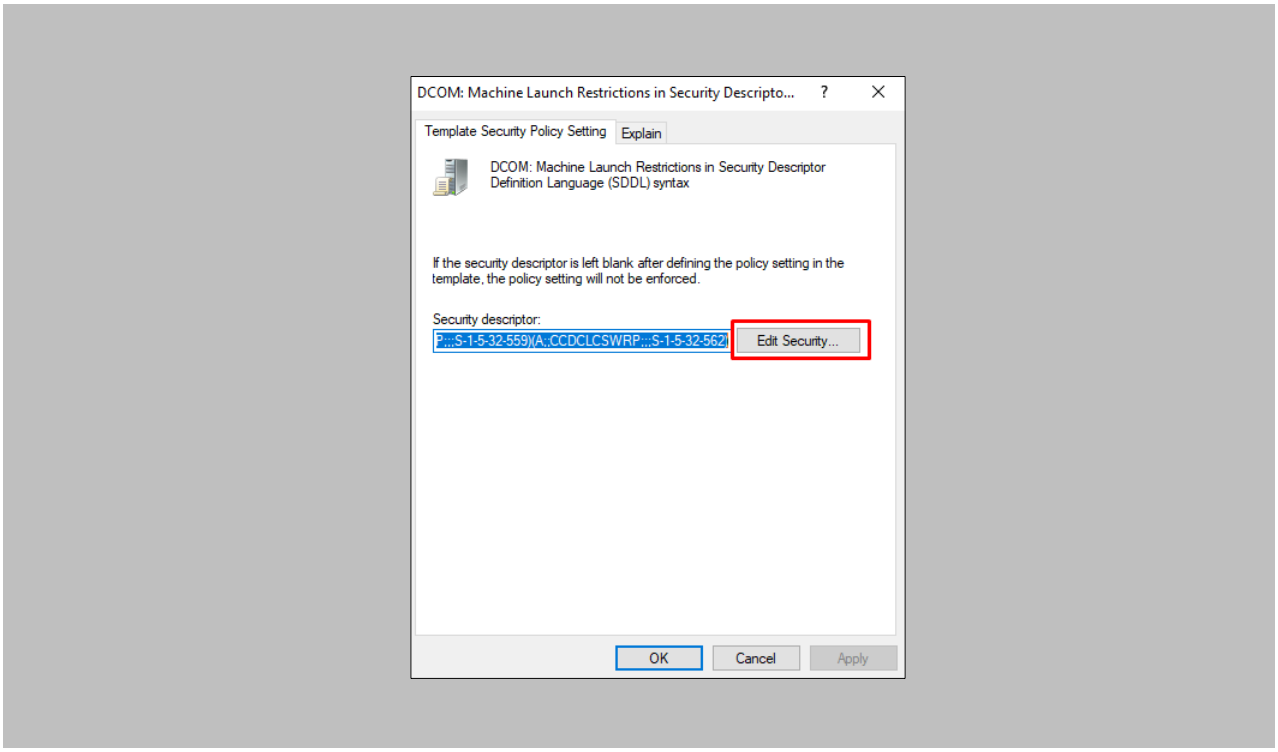


Figure 75: WIN-PAK DCOM Launch Restrictions - Edit Securities

STEP 7

Give **'Local Launch'**, **'Remote Launch'**, **'Local Activation',** and **'Remote Activation'** permissions for the below groups or usernames:

- Distributed COM Users
- All APPLICATION PACKAGES
- Performance Log User
- Everyone

Click on **OK** once permissions are assigned.

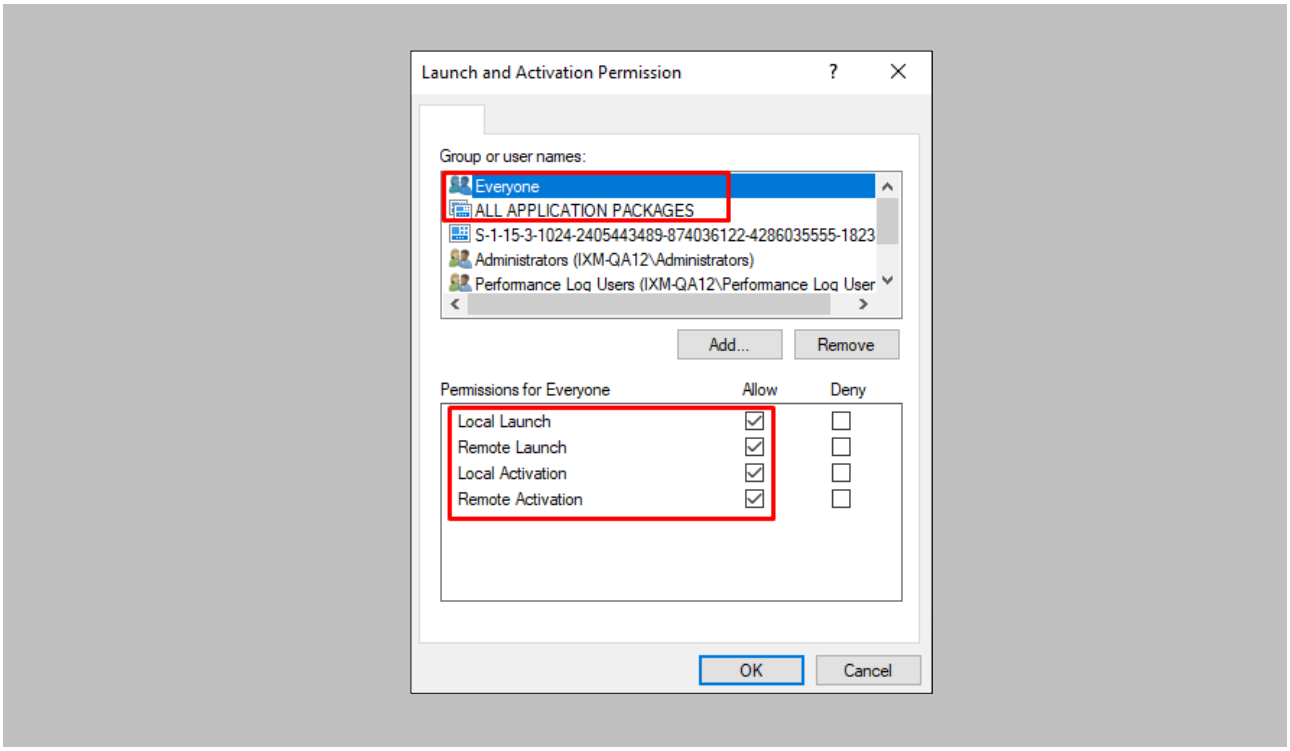


Figure 76: WIN-PAK Launch Permissions for Users and Groups

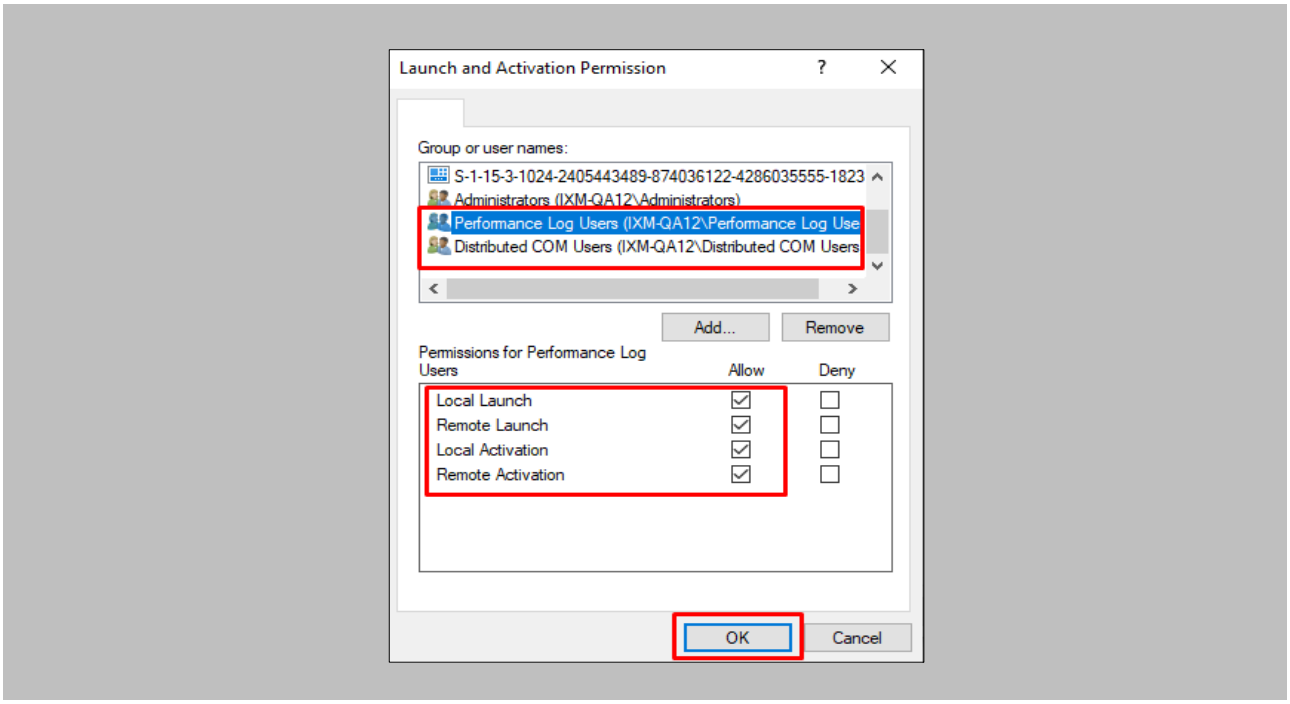


Figure 77: WIN-PAK Launch Permissions for Users

STEP 8

Open **Command Prompt** → Write **gpupdate /force** → Click on **Enter.**

These settings will connect the WIN-PAK API Client from the Client machine where the WIN-PAK API proxy is installed.

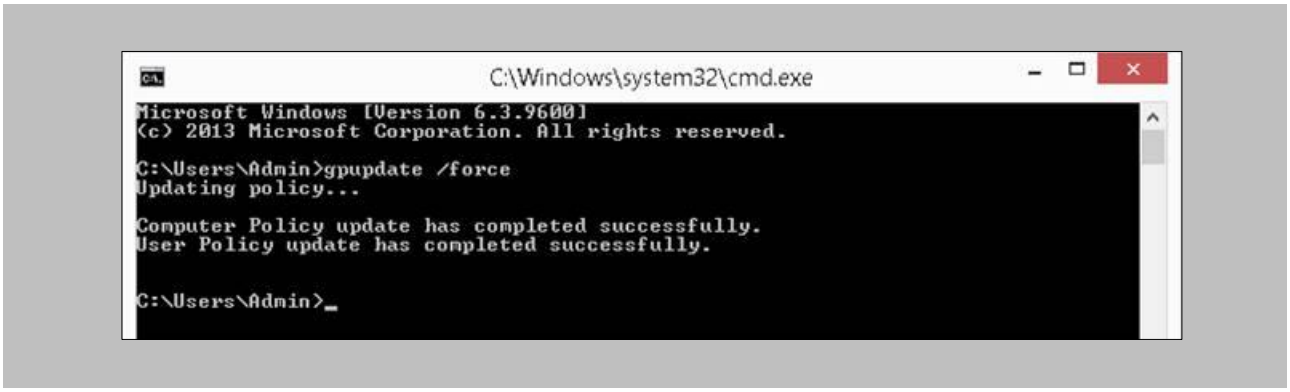


Figure 78: WIN-PAK Group Policy Update

Exporting Proxy from Server Machine

Procedure

STEP 1

Open the **Control Panel** → Navigate to **Administrative Tools** → **Component Services.**

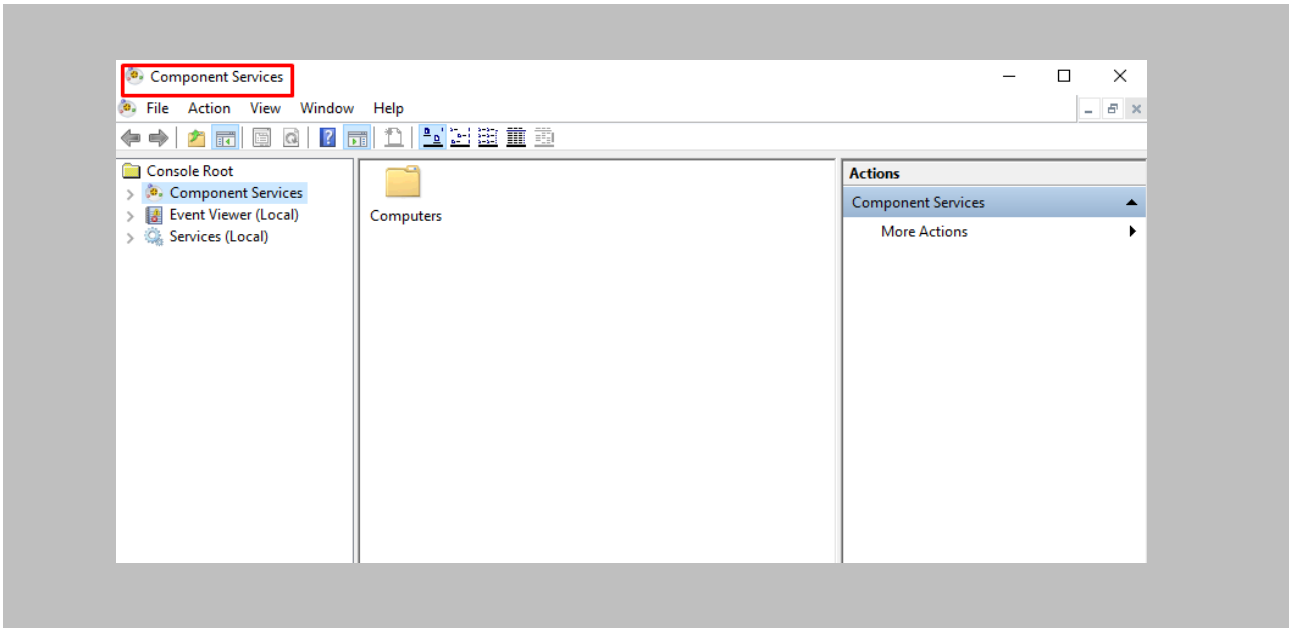


Figure 79: WIN-PAK Component Services

STEP 2

Go to **Component Services** → **Computers** → **My Computer** → **COM+ Applications.**

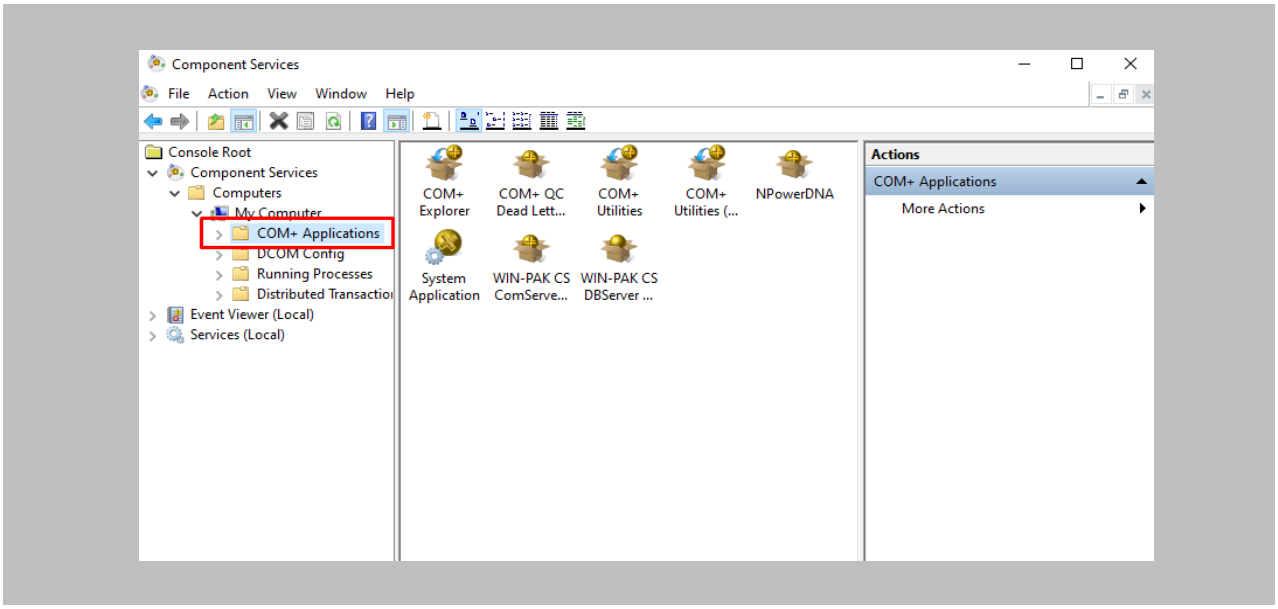


Figure 80: WIN-PAK COM+ Applications

STEP 3

Search for **WIN-PAK CS ComServer Helper** → Right click and click on **Export.**

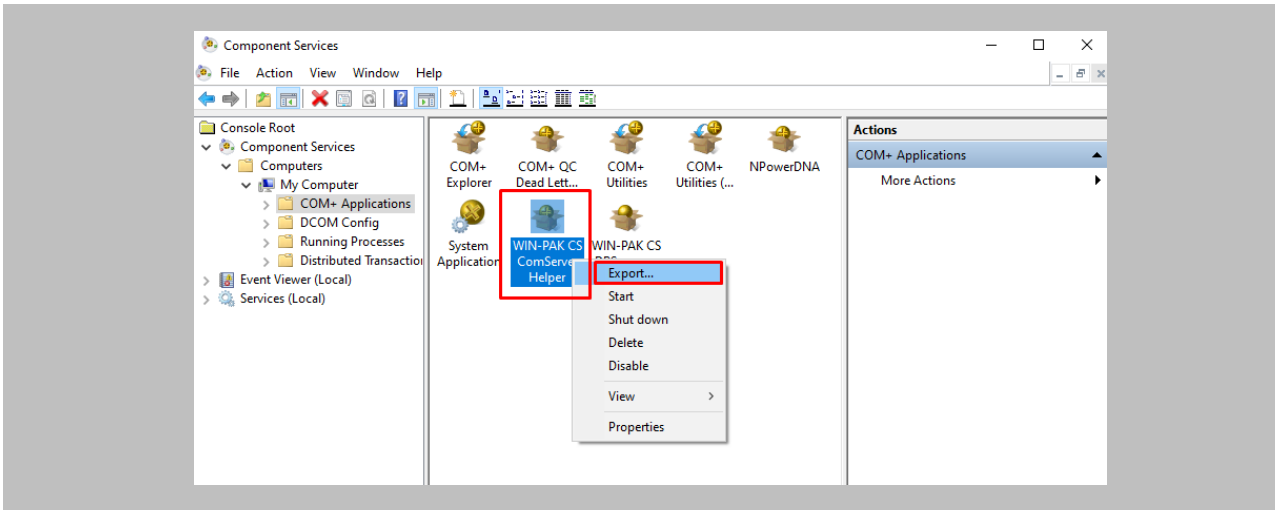


Figure 81: WIN-PAK CS ComServer Helper

STEP 4

After Cclicking Export, **Welcome to the COM+ Application Export Wizard** will open → Click on **Next.**

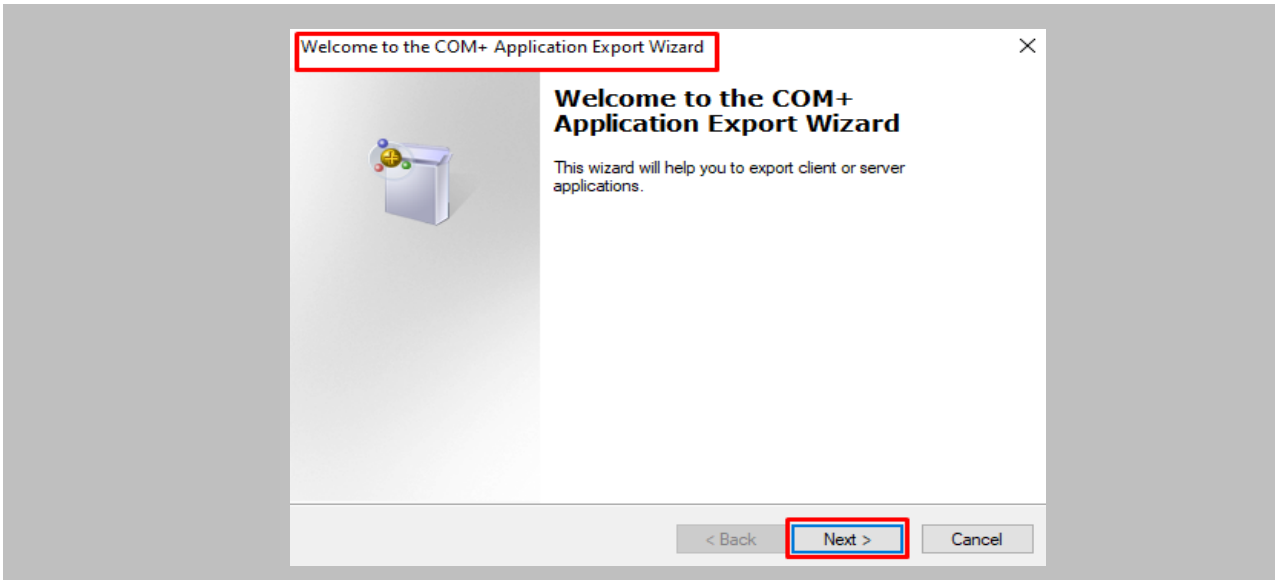


Figure 82: WIN-PAK COM+ Application Export Wizard

STEP 5

Click on **Browse** and provide a path to save the exported **Application Proxy** setup.

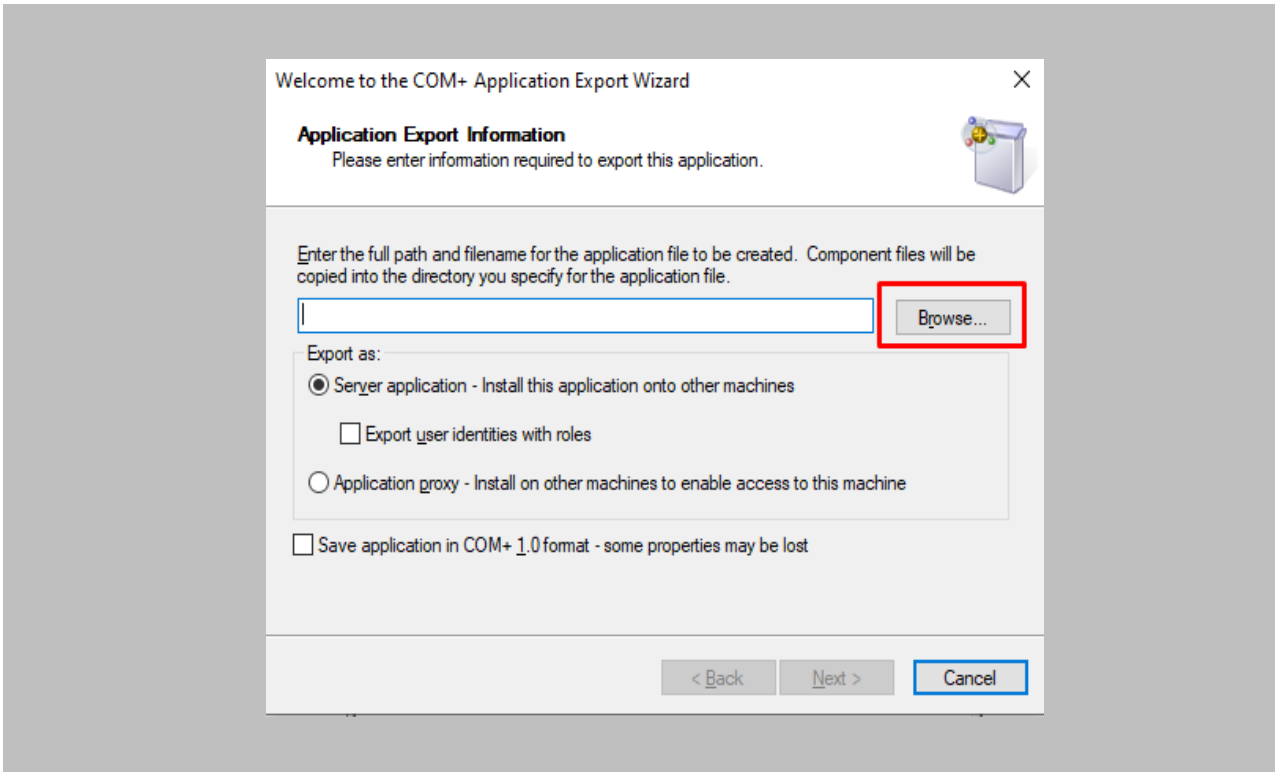


Figure 83: WIN-PAK Browse

STEP 6

Enter an appropriate name and click on **Save** → Select **Application proxy - Install on other machines to enable access to this machine** →Click on **Next**.

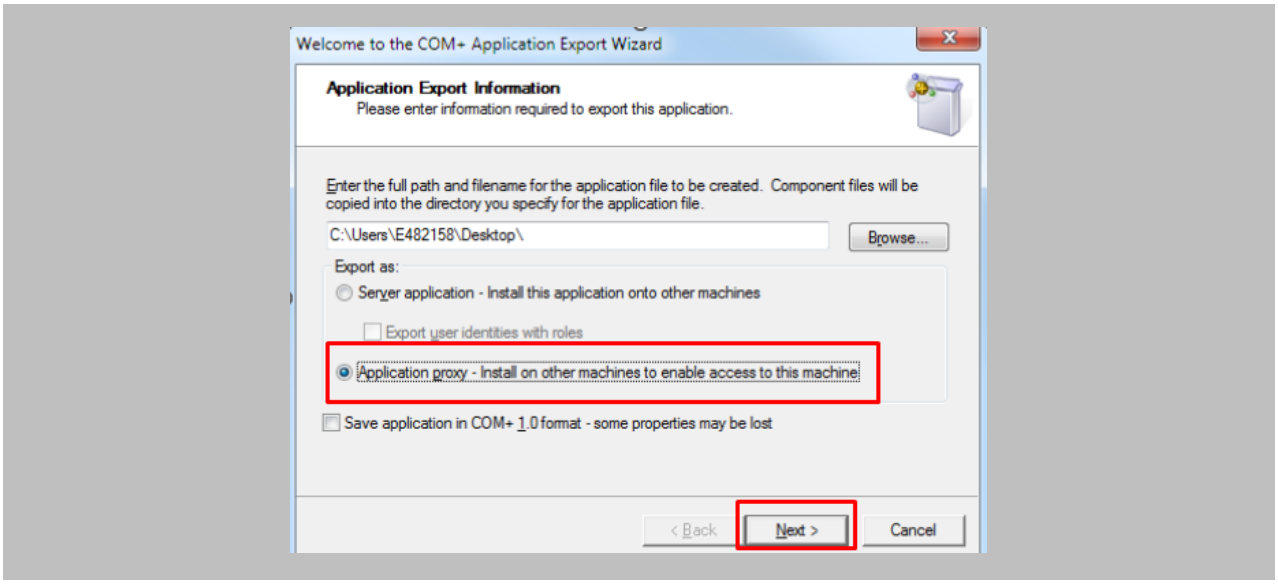


Figure 84: WIN-PAK Export Application Proxy

STEP 7

Click on **Finish.**

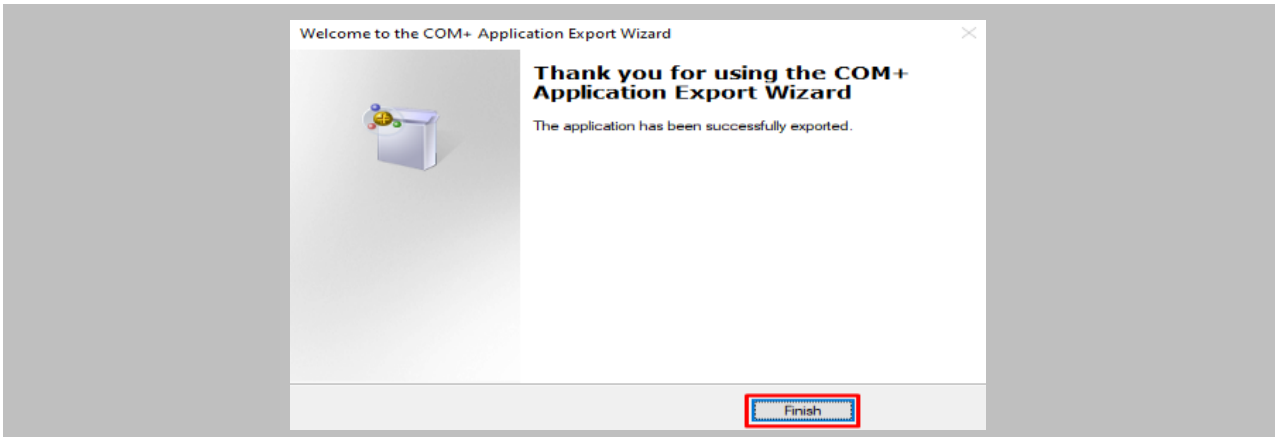


Figure 85: WIN-PAK Finish Exporting

STEP 8

Setup of **WIN-PAK Communication Server API** is created successfully. This setup consists of the **.MSI** file and the **.CAB** file.

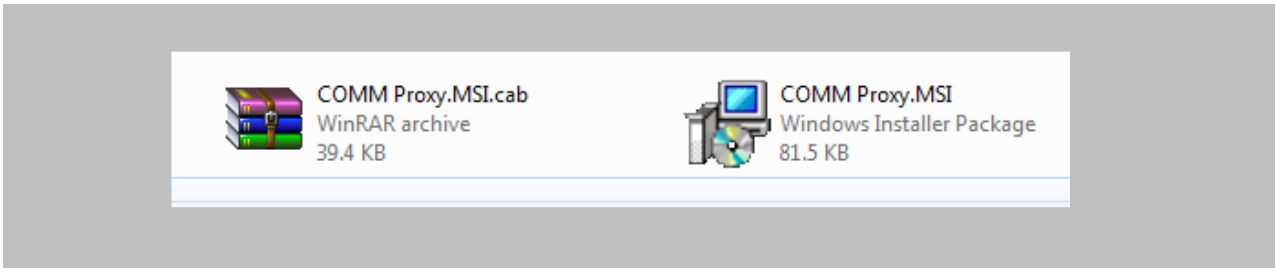


Figure 86: WIN-PAK Communication Server API Setup

STEP 9

Again go to the **Component Service** window and search for **WIN-PAK CS DBServer Helper** → Right click and click on **Export.**

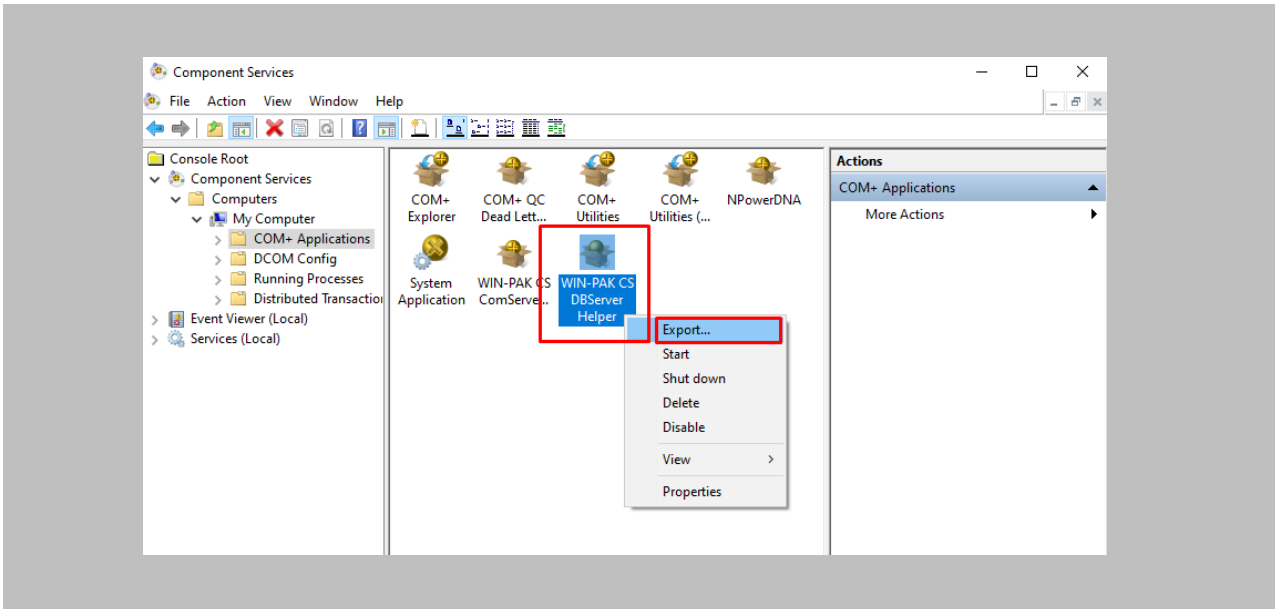


Figure 87: WIN-PAK CS DBServer Helper

STEP 10

Repeat all the steps from **Step 4** to **Step 8** for exporting the **WIN-PAK CS DBServer Helper** setup.

Installing Proxy on Client Machine

Procedure

STEP 1

Copy the previously exported proxies from the server machine to the client machine → Install both the **MSI** files.

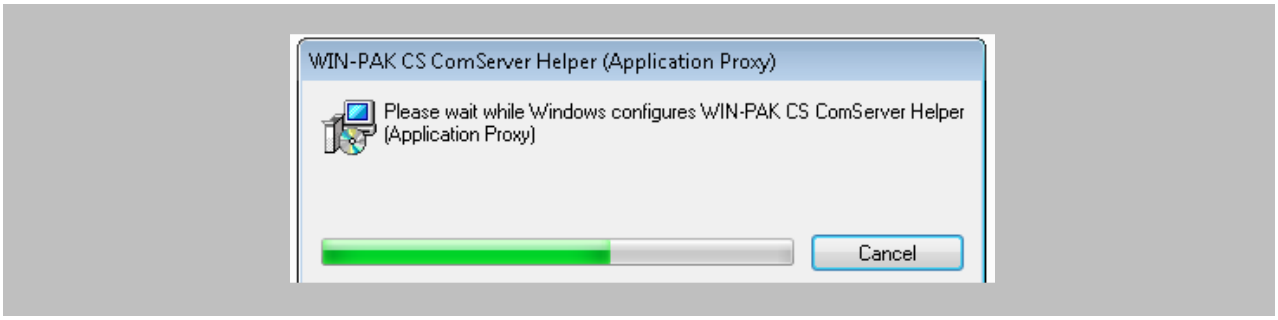


Figure 88: Installation of WIN-PAK CS CommServer Helper

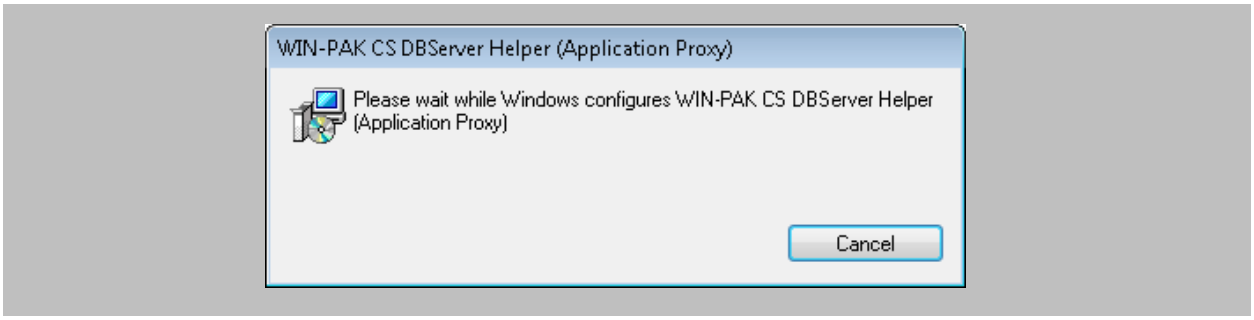


Figure 89: Installation of WIN-PAK CS DBServer Helper

STEP 2

Once installation is completed, open **Control Panel** → Navigate to **Administrative Tools** → **Component Services.**

WIN-PAK CS CommServer and **WIN-PAK CS DBServer** COM+ applications are installed with different icons.

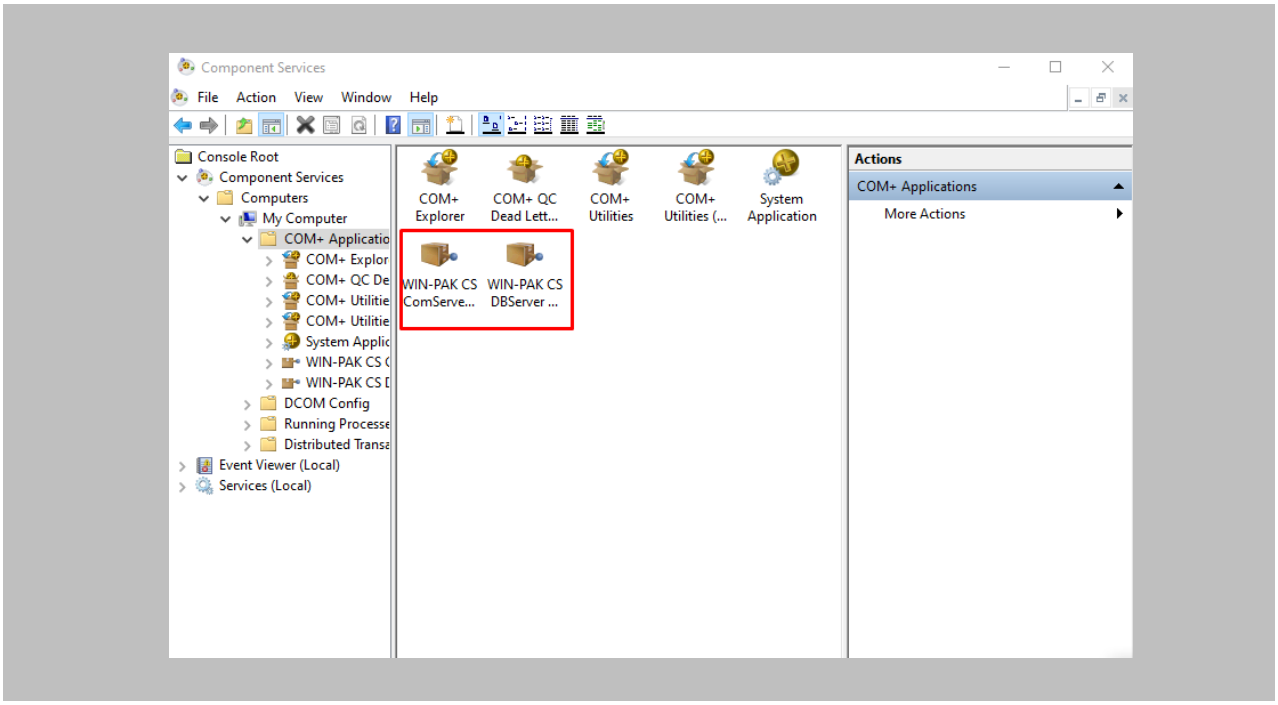


Figure 90: WIN-PAK Client COM+ Applications

11. Appendix

Pushing Configuration to Multiple Invixium Readers

Procedure

STEP 1

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

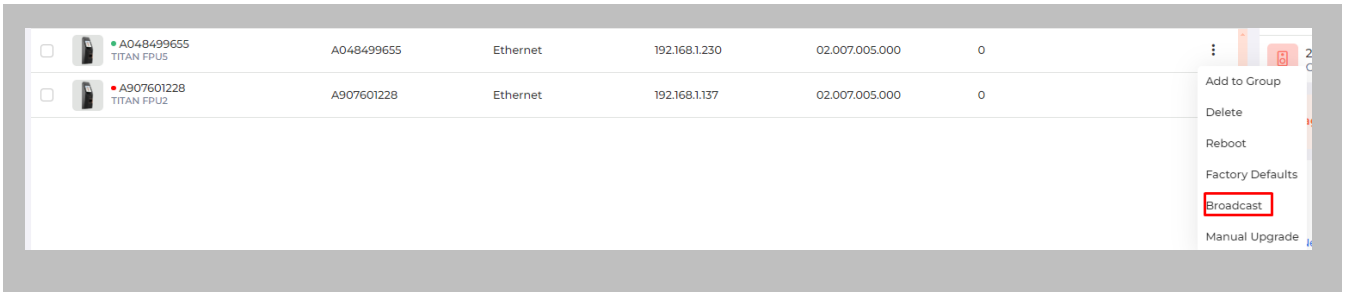


Figure 91: IXM WEB - Broadcast Option

STEP 2

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

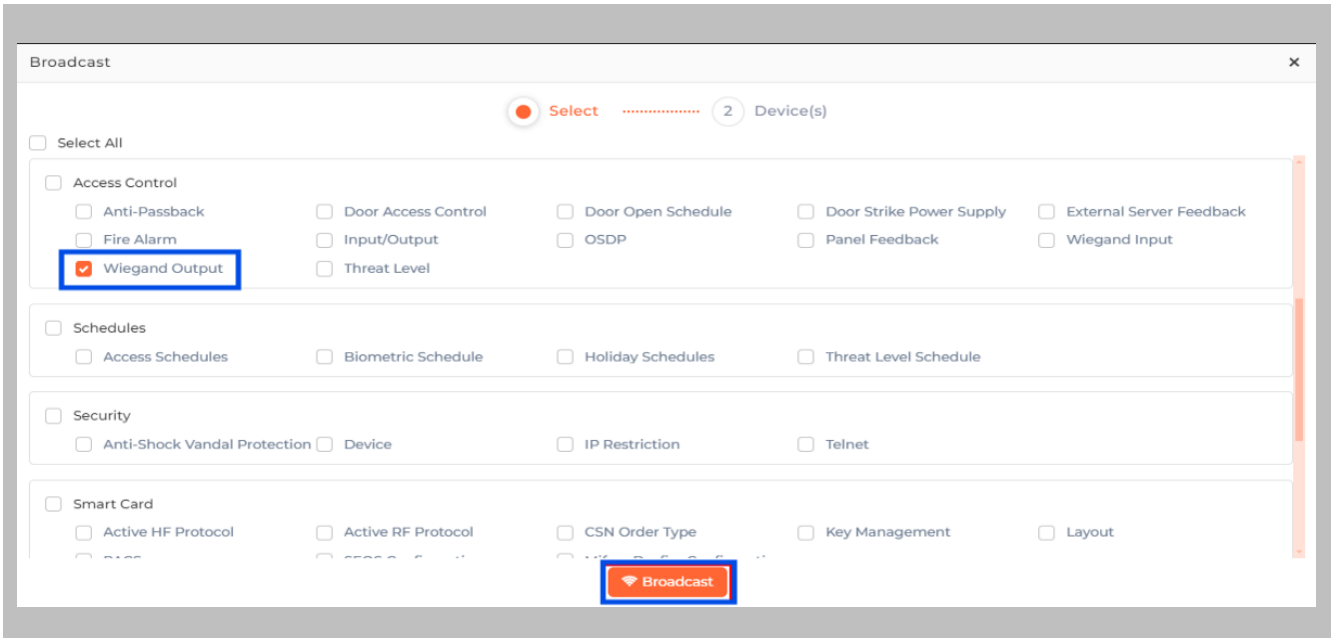


Figure 92: IXM WEB - Broadcast Wiegand Output Settings

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.

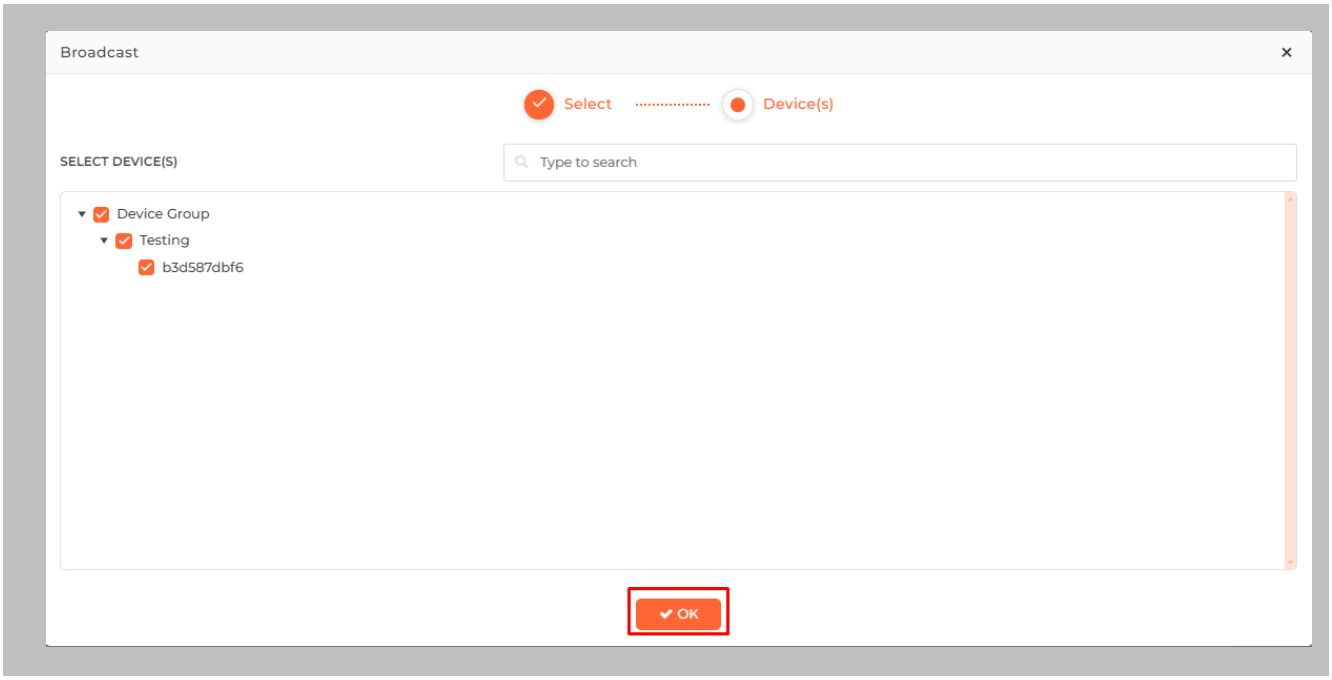


Figure 93: IXM WEB - Broadcast to Devices

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**.

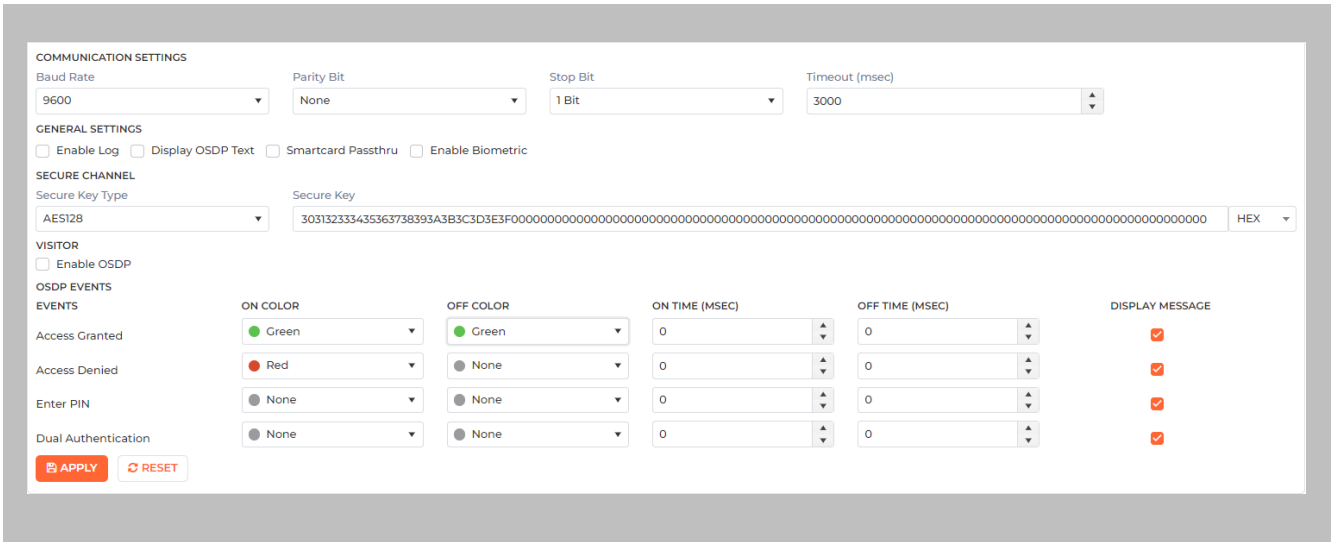


Figure 94: IXM WEB - OSDP Settings

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.

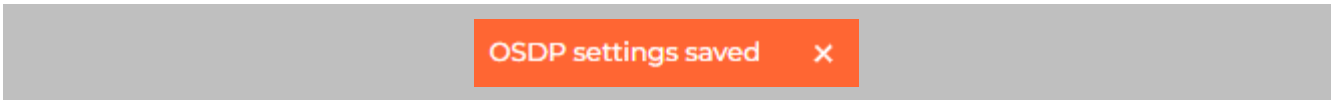


Figure 95: IXM WEB - Save OSDP Settings

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 WIN-PAK.

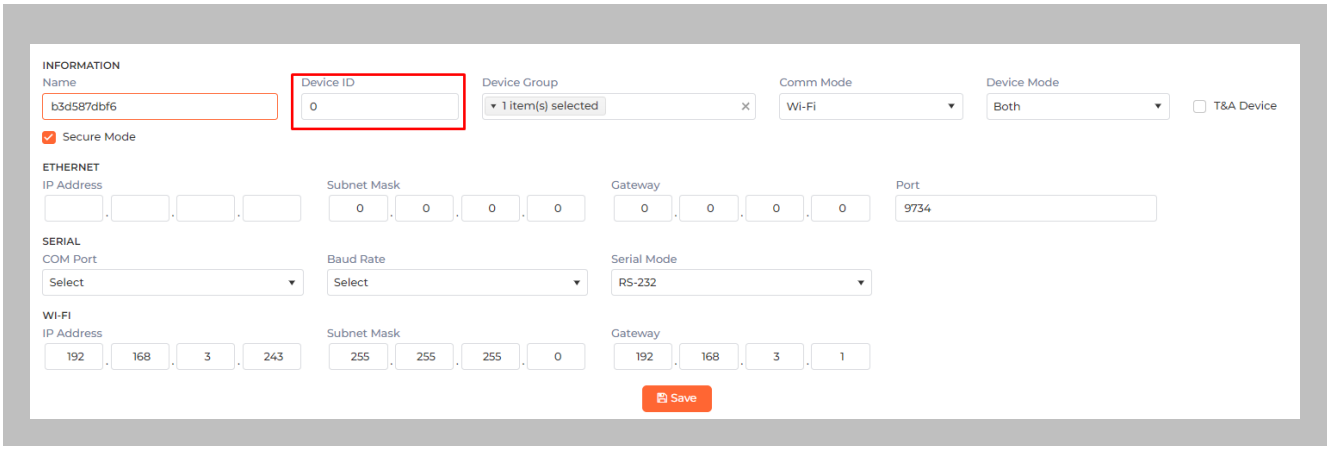


Figure 96: IXM WEB - Edit Device Options

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 WIN-PAK.

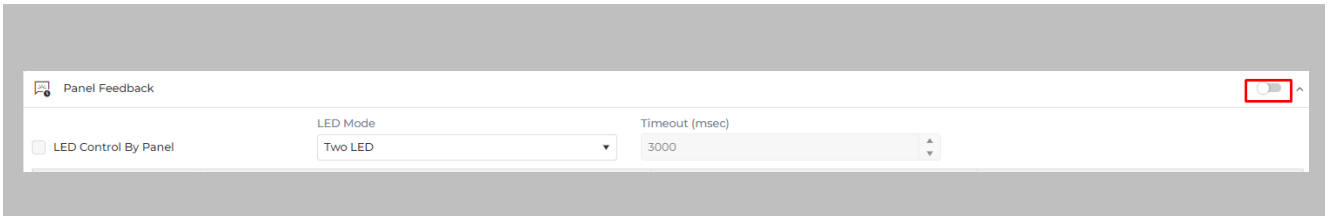


Figure 97: IXM WEB - Disable Panel Feedback

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.

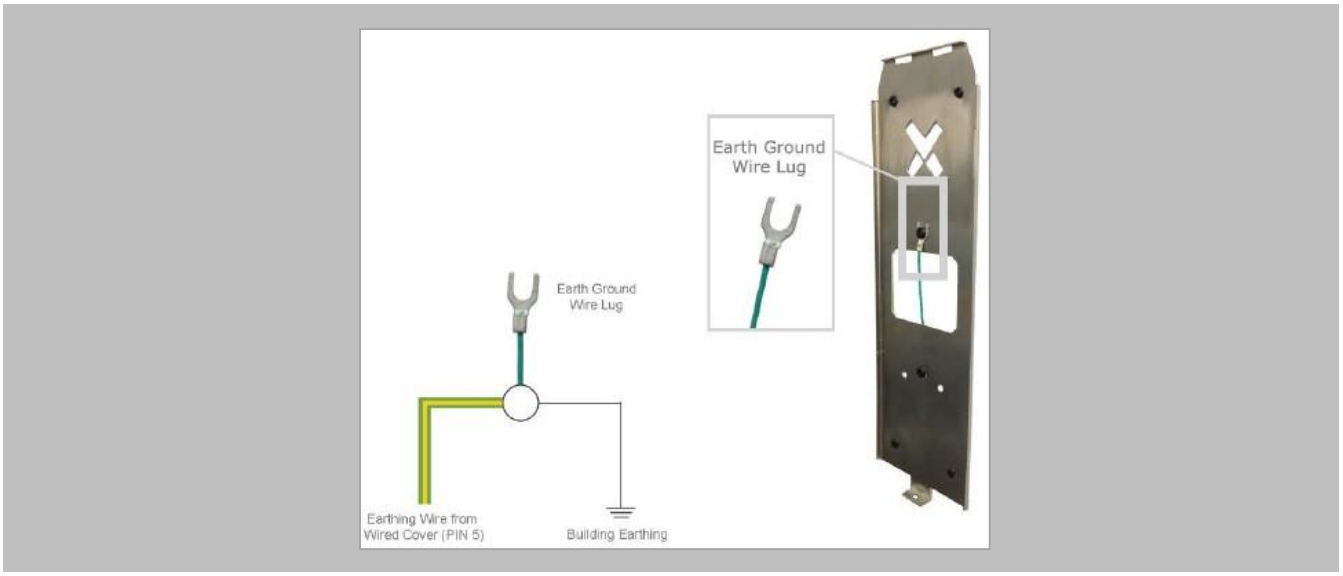


Figure 98: Earth Ground Wiring

Wiring

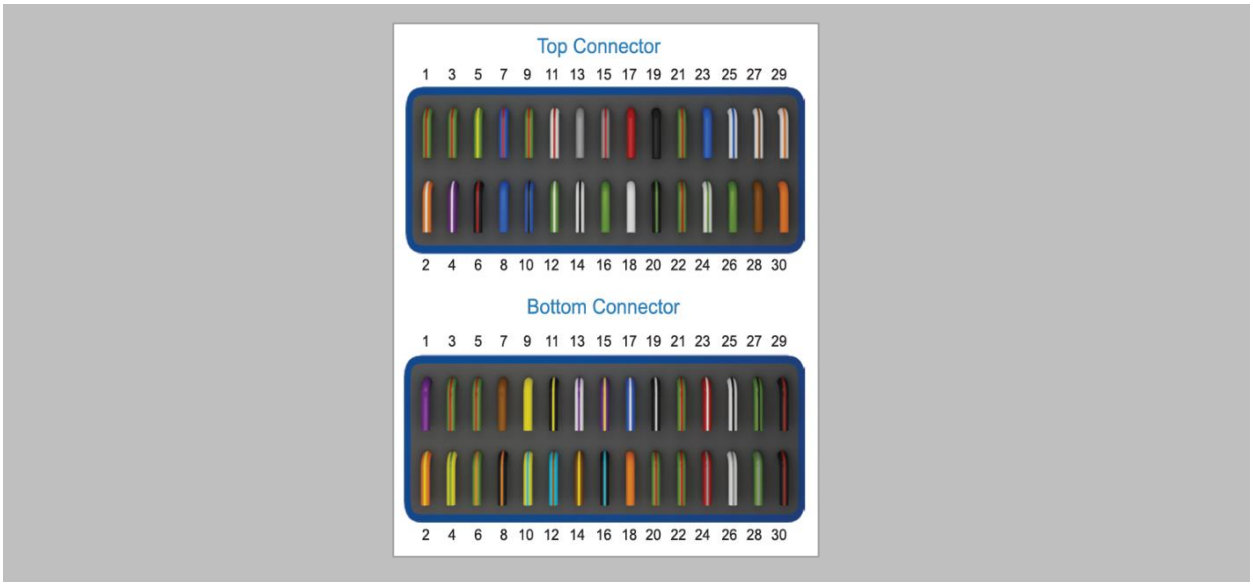
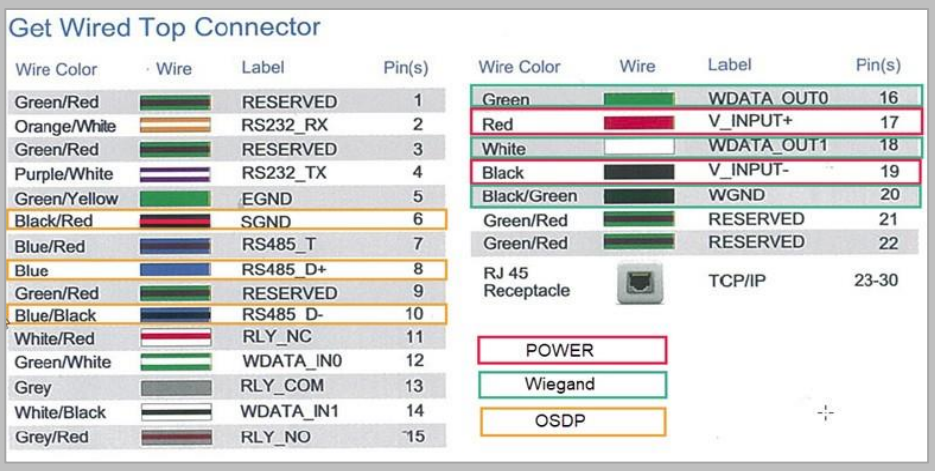


Figure 99: IXM TITAN – Top & Bottom Connector Wiring



Get Wired Top Connector

Wire Color	Label	Pin(s)
Green/Red	RESERVED	1
Orange/White	RS232_RX	2
Green/Red	RESERVED	3
Purple/White	RS232_TX	4
Green/Yellow	EGND	5
Black/Red	SGND	6
Blue/Red	RS485_T	7
Blue	RS485_D+	8
Green/Red	RESERVED	9
Blue/Black	RS485_D-	10
White/Red	RLY_NC	11
Green/White	WDATA_IN0	12
Grey	RLY_COM	13
White/Black	WDATA_IN1	14
Grey/Red	RLY_NO	15

Wire Color	Label	Pin(s)
Green	WDATA_OUT0	16
Red	V_INPUT+	17
White	WDATA_OUT1	18
Black	V_INPUT-	19
Black/Green	WGND	20
Green/Red	RESERVED	21
Green/Red	RESERVED	22
RJ 45 Receptacle	TCP/IP	23-30

POWER

Wiegand

OSDP

Get Wired Bottom Connector

Wire Color	Label	Pin(s)
Purple	DAC_SUPPLY	1
Orange/Yellow	SPO1	2
Green/Red	RESERVED	3
Yellow/Green	SPO2	4
Green/Red	RESERVED	5
Green/Orange	SPO3	6
Brown	ACP_LED1	7
Black/Orange	SPO_GND	8
Yellow	ACP_LED2	9
Yellow/Cyan	SPI1	10
Black/Yellow	ACP_LED_GND	11
Cyan/Brown	SPI2	12
White/Purple	DAC_IN1	13
Brown/Yellow	SPI3	14
Purple/Yellow	DAC_IN2	15

Wire Color	Label	Pin(s)
Black/Cyan	SPI_GND	16
Blue/White	DAC_IN3	17
Orange	DAC_OUT	18
Black/White	DAC_IN_GND	19
Green/Red	RESERVED	20
Green/Red	RESERVED	21
Green/Red	RESERVED	22
Red/White	USB0_VBUS	23
Red/Grey	USB1_VBUS	24
White/Black	USB0_D-	25
White/Grey	USB1_D-	26
Green/Black	USB0_D+	27
Green/Grey	USB1_D+	28
Black/Red	USB0_GND	29
Black/Red	USB1_GND	30

Figure 100: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand and OSDP.

Invixium devices can be integrated with Honeywell WIN-PAK panels on:

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

Wiegand Connection

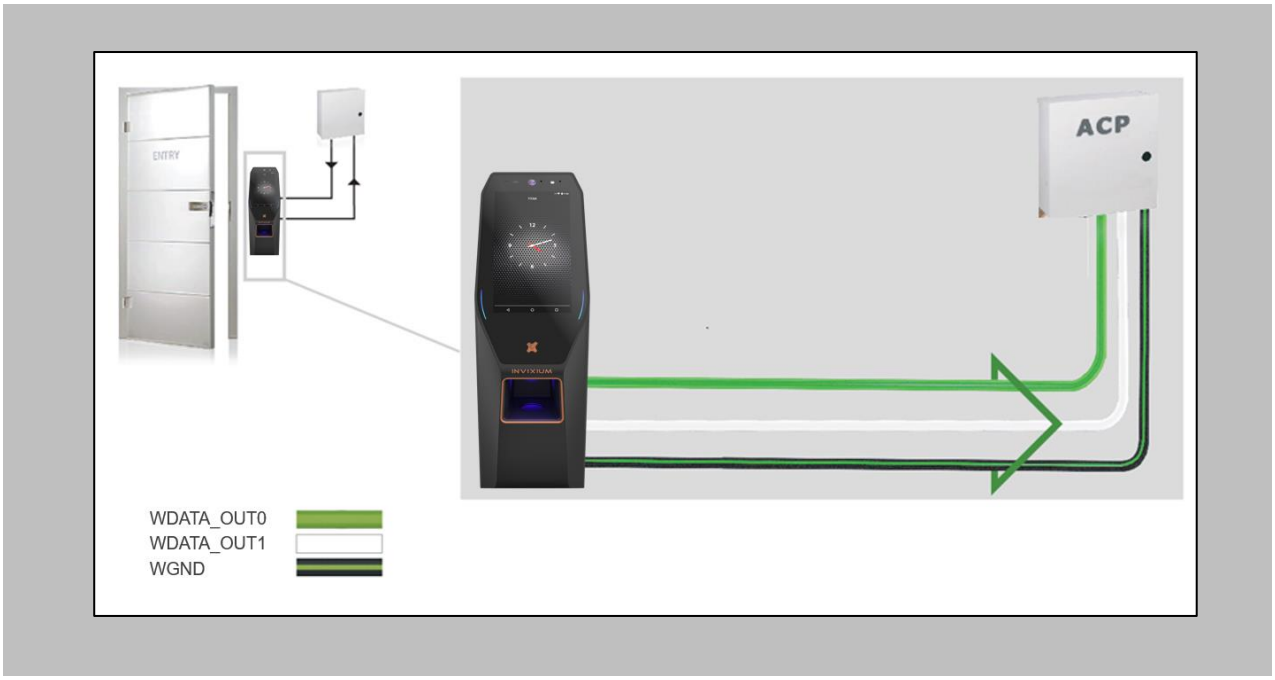


Figure 101: IXM TITAN - Wiegand

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

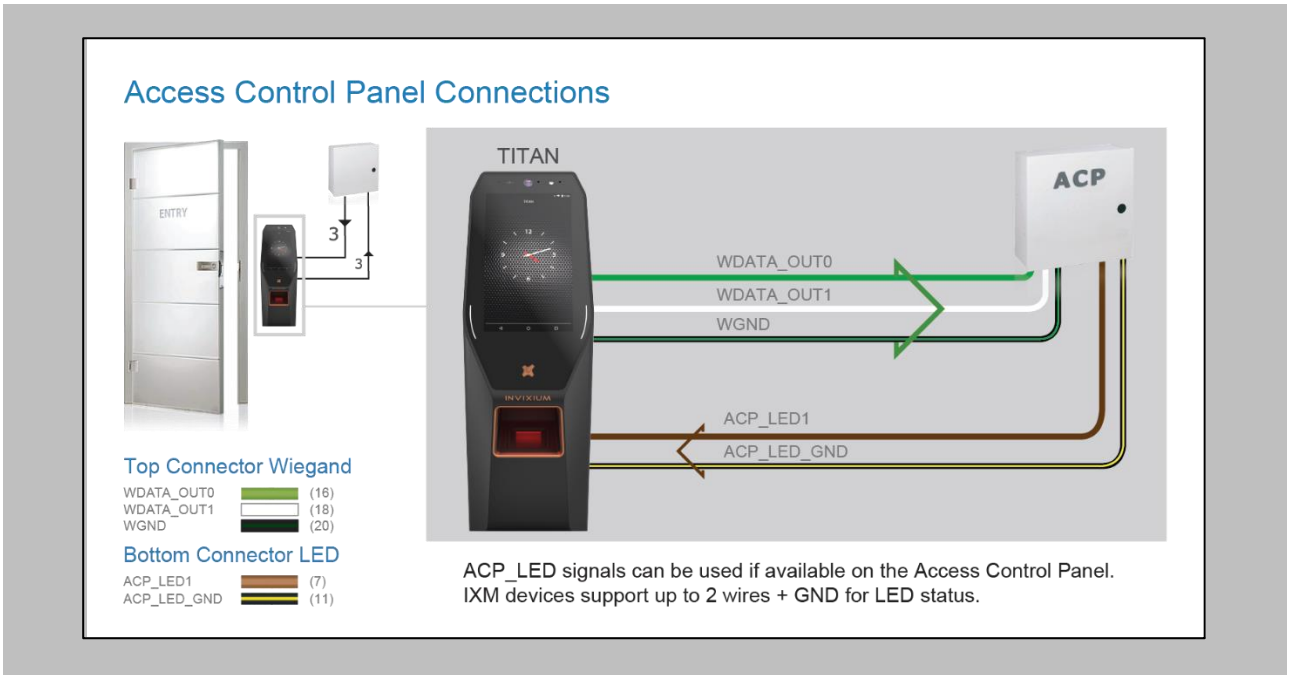


Figure 102: IXM TITAN – Panel Feedback

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

OSDP Connections

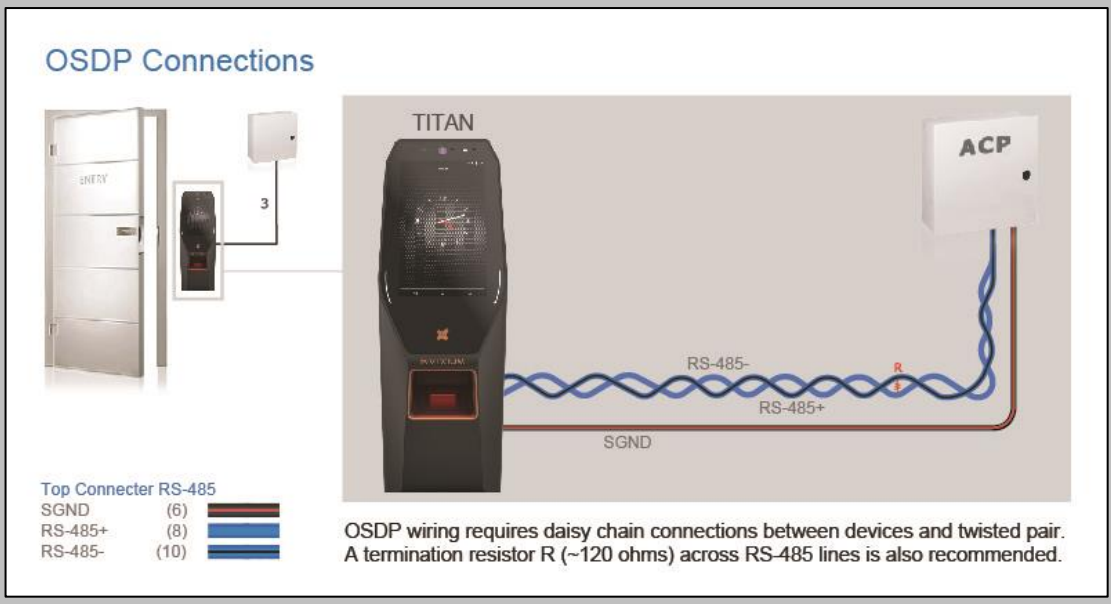


Figure 103: IXM TITAN – OSDP Connections

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

12. 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**.

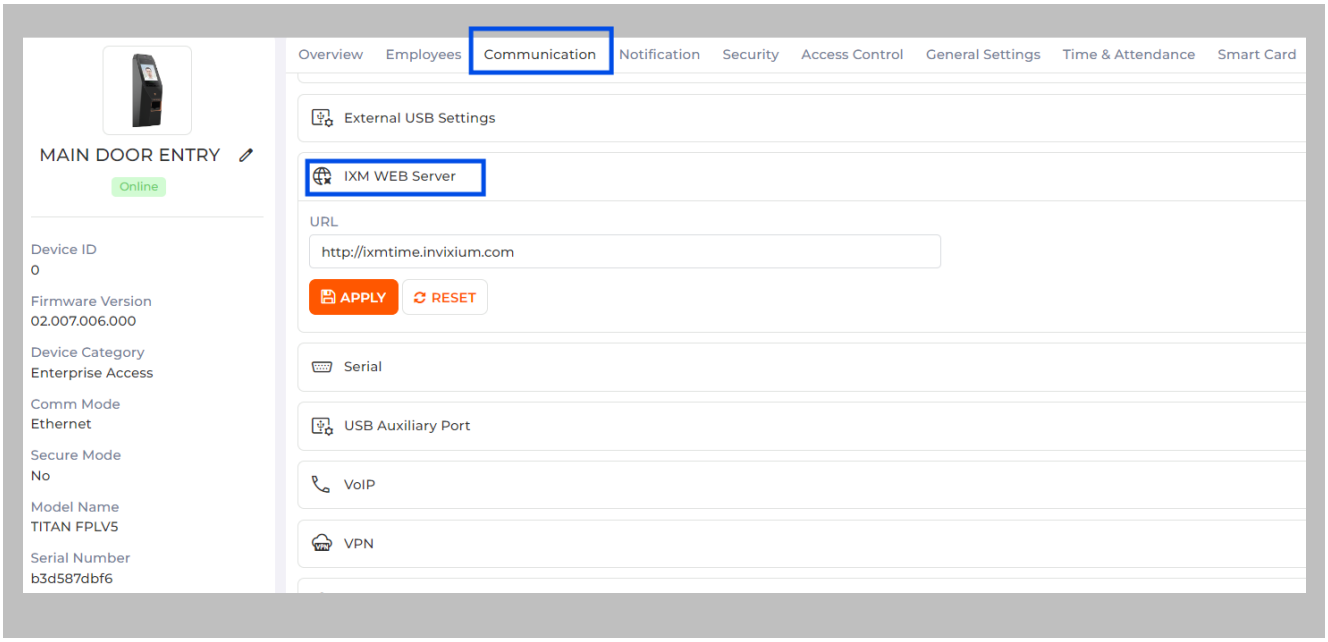


Figure 104: IXM WEB - Server URL Setting

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.

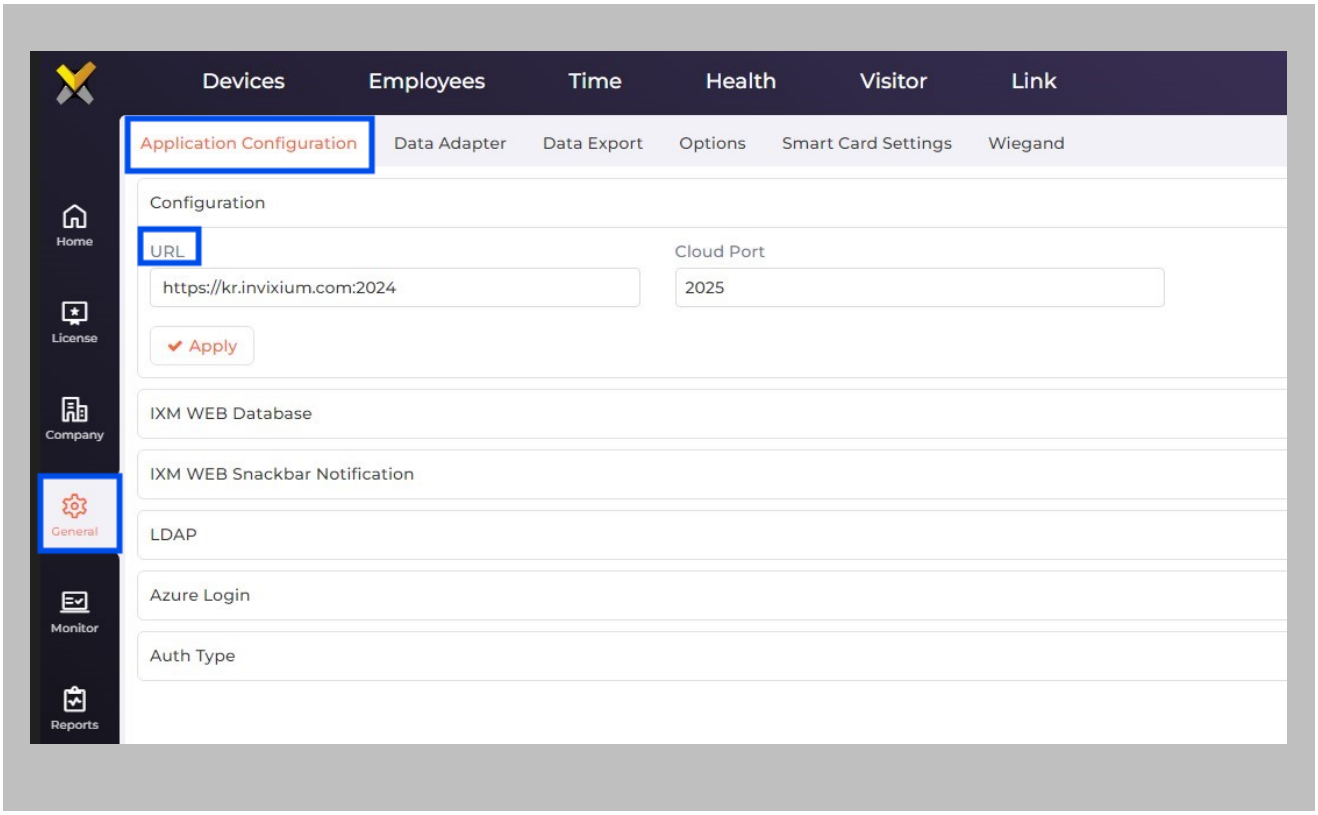


Figure 105: IXM WEB - Server URL Setting from General Settings

Logs in IXM WEB Application

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

From 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 106: IXM WEB - Enable Device Logs

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

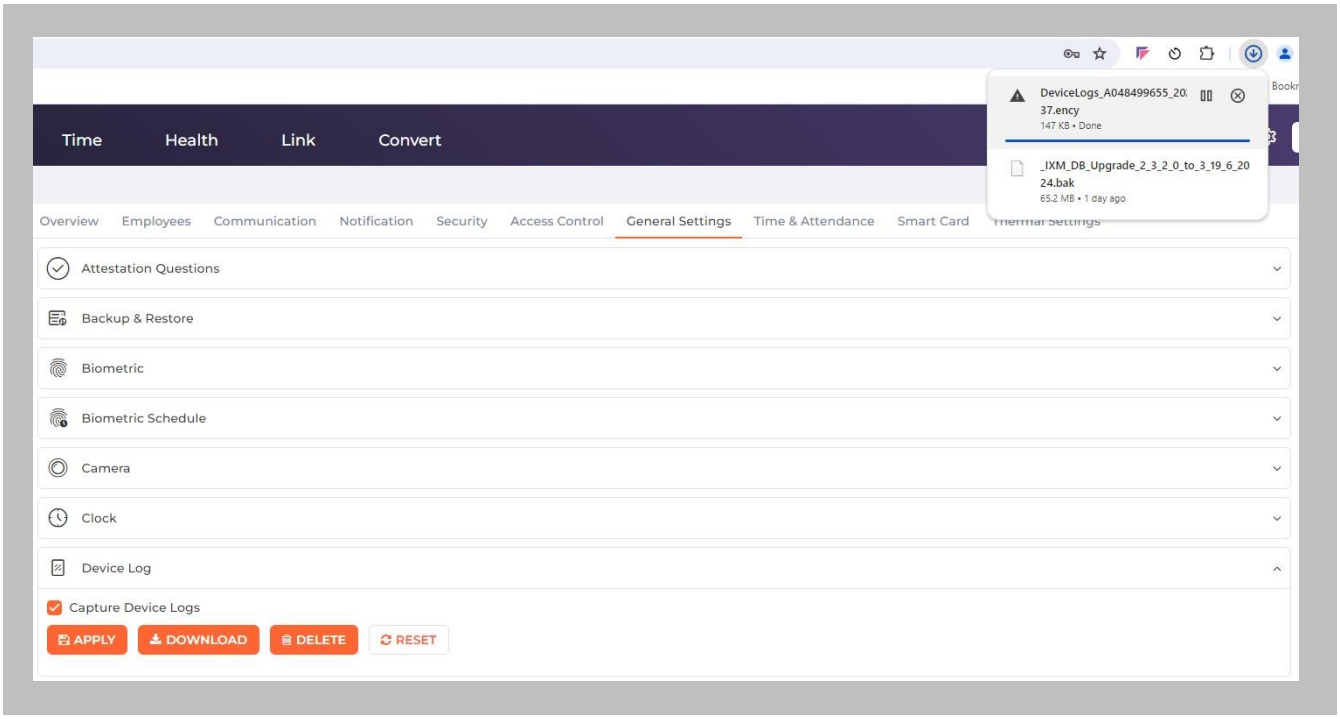


Figure 107: Save Device Log File

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

16. Support

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

17. Disclaimer and Restrictions

This document and the information described throughout are provided in their present condition and are delivered without written, expressed, or implied commitments by Invixium. and are subject to change without notice. The information and technical data herein are strictly prohibited for the intention of reverse engineering and shall not be disclosed to parties for procurement or manufacturing.

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

The trademarks specified throughout the document are registered trademarks of Invixium. All third-party trademarks referenced herein are recognized to be trademarks of their respective holders or manufacturers.