IXM WEB Integration with OnGuard by LenelS2

Installation Instructions

V5.0

P/N XAD-TPI-003-05G

Table of Contents

1. Introduction 9
Purpose 9
Description 9
Acronyms 9
Field Mappings 10

2. Compatibility 11
Invixium Readers 11
Software Requirements 11
Other Requirements 12
Compatibility Matrix for IXM WEB & OnGuard Integration: 12

3. Checklist 13

4. Task List Summary 14

5. Prerequisites for Installing Invixium IXM WEB Software 15
Getting an IXM WEB activation key 15
Minor Checklist and Considerations 17

6. Installing IXM WEB 18
Software Installation 18

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

8. Software and Module Activation 34
IXM WEB Activation 34
OnGuard by LenelS2 Module Activation 37

9. Configuring IXM Link for OnGuard by LenelS2 40

10. Create API System Users for Biometric Enrollment 45
Creating API System Users for Biometric Enrollment 45

11. Configure Readers in OnGuard 48

12. Add and Configure Invixium Readers 58

Adding Invixium Readers in the IXM WEB application 58

13. Adding Invixium Device to a Device Group 61
Assign Wiegand to Invixium Readers 62
Configuring Panel Feedback with Lenel 65
Configuring Thermal Settings....67
Thermal Calibration 70
Test Calibration Options....73
Change Temperature Unit Settings 74
Configuring Mask Authentication Settings 76
Pre-Configuration for Enrollment 79

14. Enrollment from LenelS2 System Administration 86
Biometric Enrollment from the OnGuard Enrollment Add-On 88
Access Rules Configuration from the OnGuard Enrollment Add-On 94
Save User Records on Cards from the OnGuard Enrollment Add-On 96

15. Enrollment Best Practices 97
Fingerprint Enrollment Best Practices....97
Avoid Poor Fingerprint Conditions 97
Fingerprint Image Samples 98
Fingerprint Imaging Do's and Don'ts 99
Finger Vein Enrollment Best Practices 100
Face Enrollment Best Practices 101

16. Send Logical Events to OnGuard 102

17. Configure Custom PIN Fields in OnGuard 112

18. Appendix 116
Pushing Configuration to Multiple Invixium Readers 116
Configuring for OSDP Connection 119
Wiring and Termination 125
Wiring 126
Wiegand Connection 128
Wiegand Connection with Panel Feedback 129
OSDP Connections 129

19. Troubleshooting....130
Reader Offline from the IXM WEB Dashboard 130

Elevated Body Temperature Denied Access but Granted Access in OnGuard 133
Logs in IXM WEB Application 134

20. Support 136

21. Disclaimer and Restrictions 136

List of Figures

Figure 1: IXM WEB Online Request Form 15
Figure 2: Sample Email After Submitting Online Request Form 16
Figure 3: IXM WEB Installer 18
Figure 4: Advanced Option in IXM WEB Installer 19
Figure 5: IXM WEB Installation 21
Figure 6: IXM WEB Installation Completed 22
Figure 7: IXM WEB Icon - Desktop Shortcut 23
Figure 8: IXM WEB Database Configuration 23
Figure 9: SQL Database Configuration 24
Figure 10: IXM WEB Database Name 25
Figure 11: IXM WEB Administrator User Configuration 26
Figure 12: Save Database Configuration 28
Figure 13: IXM WEB Login Page 29
Figure 14: Configure Email 30
Figure 15: IXM WEB - SMTP Settings 31
Figure 16: IXM WEB - Save Email Settings 32
Figure 17: IXM WEB - Test Connection 32
Figure 18: IXM WEB - Enter Email ID 33
Figure 19: IXM WEB - Forgot Password 33
Figure 20: IXM WEB - Enter Login Credentials 34
Figure 21: IXM WEB - License Setup 35
Figure 22: IXM WEB - Online Activation 36
Figure 23: IXM WEB – OnGuard by LenelS2 Link Activation 37
Figure 24: OnGuard License Key Email 38
Figure 25: IXM WEB - Activate LenelS2 Link License 39
Figure 26: IXM WEB - Link Menu 40

Figure 27: IXM WEB - Enable Lene-S2 Link Module 41
Figure 28: IXM WEB - Map Access Level to User Group 42
Figure 29: IXM WEB - Auto Transfer No 42
Figure 30: IXM WEB - Auto Transfer Yes 42
Figure 31: IXM WEB - Sync Activities 43
Figure 32: IXM WEB - Create API User 45
Figure 33: IXM WEB - Add New API User 46
Figure 34: IXM WEB - New API User 47
Figure 35: IXM WEB - Save API User 47
Figure 36: OnGuard - Access Panel 48
Figure 37: OnGuard - Add Access Panel 49
Figure 38: OnGuard - Readers and Doors 50
Figure 39: OnGuard - Add New Reader 50
Figure 40: OnGuard - Reader Configuration 51
Figure 41: OnGuard – Facility Code 52
Figure 42: OnGuard - Access Level 53
Figure 43: OnGuard - Add New Access Level 54
Figure 44: OnGuard - Add Reader to Access Level 55
Figure 45: OnGuard - Access Level Configuration 56
Figure 46: OnGuard - New Access Level 57
Figure 47: IXM WEB - Devices Tab 58
Figure 48: IXM WEB - Search Device using IP Address 58
Figure 49: IXM WEB - Register Device 59
Figure 50: IXM WEB - Device Registration Complete 60
Figure 51: IXM WEB - Dashboard, Device Status 60
Figure 52: IXM WEB - Assign Device Group 61
Figure 53: IXM WEB – Navigate to Access Control Tab 62
Figure 54: IXM WEB - Wiegand Output 63
Figure 55: IXM WEB - Save Output Wiegand 64
Figure 56: IXM WEB - Panel Feedback 65
Figure 57: IXM WEB - Configuring Panel Feedback in IXM WEB 66
Figure 58: IXM WEB - Save Panel Feedback 66
Figure 59: IXM WEB - Thermal Settings 67
Figure 60: IXM WEB - Save Thermal Settings 69
Figure 61: IXM WEB - Thermal Calibration Settings 70
Figure 62: IXM WEB - Save Thermal Calibration Settings 71
Figure 63: IXM WEB - Capture Thermal Data 71

Figure 64: IXM WEB - Save Captured Thermal Data 72
Figure 65: IXM WEB - Test Thermal Calibration 73
Figure 66: IXM WEB - Option to change Temperature unit. 74
Figure 67: IXM WEB - Save Temperature Unit Setting 75
Figure 68: IXM WEB - Mask Authentication Settings 76
Figure 69: IXM WEB - Save Mask Settings 78
Figure 70: IXM WEB - Download Enrollment Add-On 79
Figure 71: IXM WEB - Download Add-On Zip File 79
Figure 72: IXM WEB - OnGuard Add-On Enrollment.exe 80
Figure 73: OnGuard - Workstation 80
Figure 74: OnGuard - Modify Workstation 81
Figure 75: OnGuard - Partner Connector 82
Figure 76: OnGuard - Add UDF 83
Figure 77: OnGuard - Add Partner Connector 84
Figure 78: OnGuard - Enroll Button 85
Figure 79: OnGuard - Click Enroll 86
Figure 80: OnGuard - Enrollment Add-on Configuration 87
Figure 81: OnGuard – Fingerprint Device Selection 88
Figure 82: OnGuard - Fingerprint Enrollment 89
Figure 83: OnGuard - Face Enrollment 90
Figure 84: OnGuard – Finger Vein Device Selection 91
Figure 85: OnGuard – Finger Vein Enrollment 92
Figure 86: OnGuard – IXM WEB Save Enrollment 93
Figure 87: OnGuard – IXM WEB Save Access Rules Settings 95
Figure 88: OnGuard - IXM WEB Save User Record on Card 96
Figure 89: OnGuard – IXM WEB User Record Saved on Card 96
Figure 90: Fingerprint Enrollment Best Practices 97
Figure 91: Fingerprint Images Samples 98
Figure 92: Finger Vein Enrollment Best Practices 100
Figure 93: Face Enrollment Best Practices 101
Figure 94: OnGuard - Add New Logical Source 102
Figure 95: OnGuard – Logical Source 103
Figure 96: OnGuard - Add New Logical Source 104
Figure 97: OnGuard - Save Logical Source 105
Figure 98: OnGuard - Logical Source Monitor Zone 106
Figure 99: OnGuard - Logical Sources List 106
Figure 100: OnGuard - Logical Device 107

Figure 101: OnGuard - Logical Device Configuration 108
Figure 102: OnGuard - Save Logical Device 109
Figure 103: OnGuard - Logical Devices List 110
Figure 104: OnGuard - Mask and Thermal Events 110
Figure 105: OnGuard - View Associated Text 111
Figure 106: OnGuard - View Associated Text 111
Figure 107: OnGuard - Custom Pin 112
Figure 108: OnGuard - Badge Custom Pin 112
Figure 109: OnGuard - Add Numeric Field 113
Figure 110: OnGuard - Design Numeric Field 113
Figure 111: OnGuard - Save Numeric Field 114
Figure 112: OnGuard - Add Label 114
Figure 113: OnGuard - Save Label 115
Figure 114: OnGuard - IXM WEB Custom Pin 115
Figure 115: IXM WEB - Broadcast Option 116
Figure 116: IXM WEB - Wiegand Output Selection in Broadcast 116
Figure 117: IXM WEB - Broadcast Wiegand Output Settings 117
Figure 118: IXM WEB - Broadcast to Devices 118
Figure 119: IXM WEB - OSDP Settings 119
Figure 120: IXM WEB - Save OSDP Settings 122
Figure 121: IXM WEB - Edit Device 122
Figure 122: IXM WEB - Edit Device Options 123
Figure 123: OnGuard - Add OSDP Reader 123
Figure 124: OnGuard - OSDP Reader 124
Figure 125: IXM WEB - Disable Panel Feedback 124
Figure 126: Earth Ground Wiring 125
Figure 127: IXM TITAN – Top & Bottom Connector Wiring 126
Figure 128: Power, Wiegand & OSDP Wires 127
Figure 129: IXM TITAN - Wiegand 128
Figure 130: IXM TITAN - Panel Feedback 129
Figure 131: IXM TITAN - OSDP Connections 129
Figure 132: IXM WEB - Device Communication Settings 130
Figure 133: IXM WEB - Server URL Setting 131
Figure 134: IXM WEB - Server URL Setting from General Settings 132
Figure 135: IXM WEB - Thermal Authentication Wiegand Output Event 133
Figure 136: IXM WEB - Enable Device Logs 134
Figure 137: Save Device Log File 134

List of Tables

Table 1: Compatibility Matrix for IXM WEB & OnGuard 12
Table 2: Task List Summary 14
Table 3: System Related Checklist 17
Table 4: Port Information 17
Table 5: IXM WEB - OSDP Configuration Options 121
Table 6: IXM WEB - OSDP Text Options 121
Table 7: Logs Folder Location 135

1. Introduction

Purpose

This document outlines the process of configuring the software integration between OnGuard by LenelS2 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 LenelS2 OnGuard 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 OnGuard by using "Open Access API" to import and export cardholders.

Acronyms

Acronym	Description
API	Application Programming Interface
IXM	Invixium
LS2	LenelS2
OAAP	OpenAccess Alliance Program

Field Mappings

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

OnGuard Field	IXM Field	Notes
First name	First Name	This is mandatory for adding users to IXM WEB from OnGuard.
Last name	Last Name	
Badge ID (Badge)	Number (Card)	This is mandatory for adding users to IXM WEB from OnGuard.
Issue Code (Badge)	Issue Level (Card)	
Activate (Badge)	Activation Date (Card)	
Deactivate (Badge)	Expiry Date (Card)	
Status (Badge)	Status (Card)	Cards with “Active” status in OnGuard are only synchronized to IXM WEB. In case of other status, cards will be deleted from IXM WEB
<<Custom Field>>	Pin	To synchronize PINs from OnGuard to IXM WEB, users have to configure a custom field in OnGuard and provide the name of the custom field on the IXM Link configuration page.
Photo	Photo	
Access Levels	Employee Group / DeviceGroup / 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 with respective Access Levels from OnGuard will be automatically added to the employee group in IXM WEB.

Note: Multiple Cards - OnGuard can have multiple badges (cards) per cardholder, and IXM WEB supports a maximum of 10 cards per employee.

2. Compatibility

Invixium Readers

TITAN	TFACE	TOUCH2	SENSE2	MERGE2	MYCRO
All models	All models	All models	All models	All models	All models

Note: Invixium devices with the OnGuard category will only be registered in IXM WEB if they have the OnGuard license activated.

Software Requirements

Application	Version
OnGuard	v7.6 / v8.0
IXM WEB	2.3.0.0
Operating Systems	Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows 10 Professional Version Windows Server 2016 Standard Windows Server 2019
Microsoft .NET Framework	.NET Framework 4.8
Database Engine	SQL Server 2014 or higher
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 small to medium business installations. For large enterprise installation server requirements, contact support@invixium.com.

Compatibility Matrix for IXM WEB & OnGuard Integration:

IXM WEB version	OnGuard version	Compatible
IXM WEB 2.2.57.0	v7.6	Yes
IXM WEB 2.2.57.0	v8.0	Yes
IXM WEB 2.2.224.0	v7.6	Yes
IXM WEB 2.2.224.0	v8.0	Yes
IXM WEB 2.2.230.0	v8.0	Yes
IXM WEB 2.2.252.0	v8.0	Yes
IXM WEB 2.2.252.0	v8.1	Yes
IXM WEB 2.2.330.0	v8.0	Yes
IXM WEB 2.2.330.0	v8.1	Yes
IXM WEB 2.3.0.0	v8.0	Yes
IXM WEB 2.3.0.0	v8.1	Yes

Table 1: Compatibility Matrix for IXM WEB & OnGuard

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 LenelS2	Invixium
Creation of API Users in IXM WEB	Invixium
Configure Readers in OnGuard	LenelS2
Configure Invixium Readers	Invixium
Face, Fingerprint or Finger Vein Enrollment	LenelS2
Configure Logical Events	LenelS2
Configure Custom PINs (Optional)	LenelS2

4. Task List Summary

Task	IXM WEB Task List	OnGuard Task List
1	Activate IXM WEB and IXM Link for LenelS2 OnGuard	Add a reader with the same name as an IXM reader present in IXM WEB
2	Configure IXM Link for OnGuard	Create an Access Level and add a reader to it
3	Add a new API System User in IXM WEB for enrollment	Create Cardholders, Assign Badges and Assign Access Levels to cardholders
4	Register an IXM Device and configure settings as per the requirement	Configure Partner Connector Workstations for Enrollment
5	Configure Weigand or OSDP settings in device for integration with Access Panels	Enroll cardholder biometrics (Face, fingerprint, finger vein) from the enrollment addon
6	Download the Add-on for enrollment from the Link Configuration page	Add logical devices with the same name as an IXM reader present in IXM WEB for Temperature and Mask Events using OnGuard
7		Monitor Events and Generate Reports

Table 2: Task List Summary

5. Prerequisites for Installing Invixium IXM WEB Software

Getting an IXM WEB activation key

Procedure

Complete the online form to receive instructions on how to download IXM WEB: https://www.invixium.com/download-ixm-web/

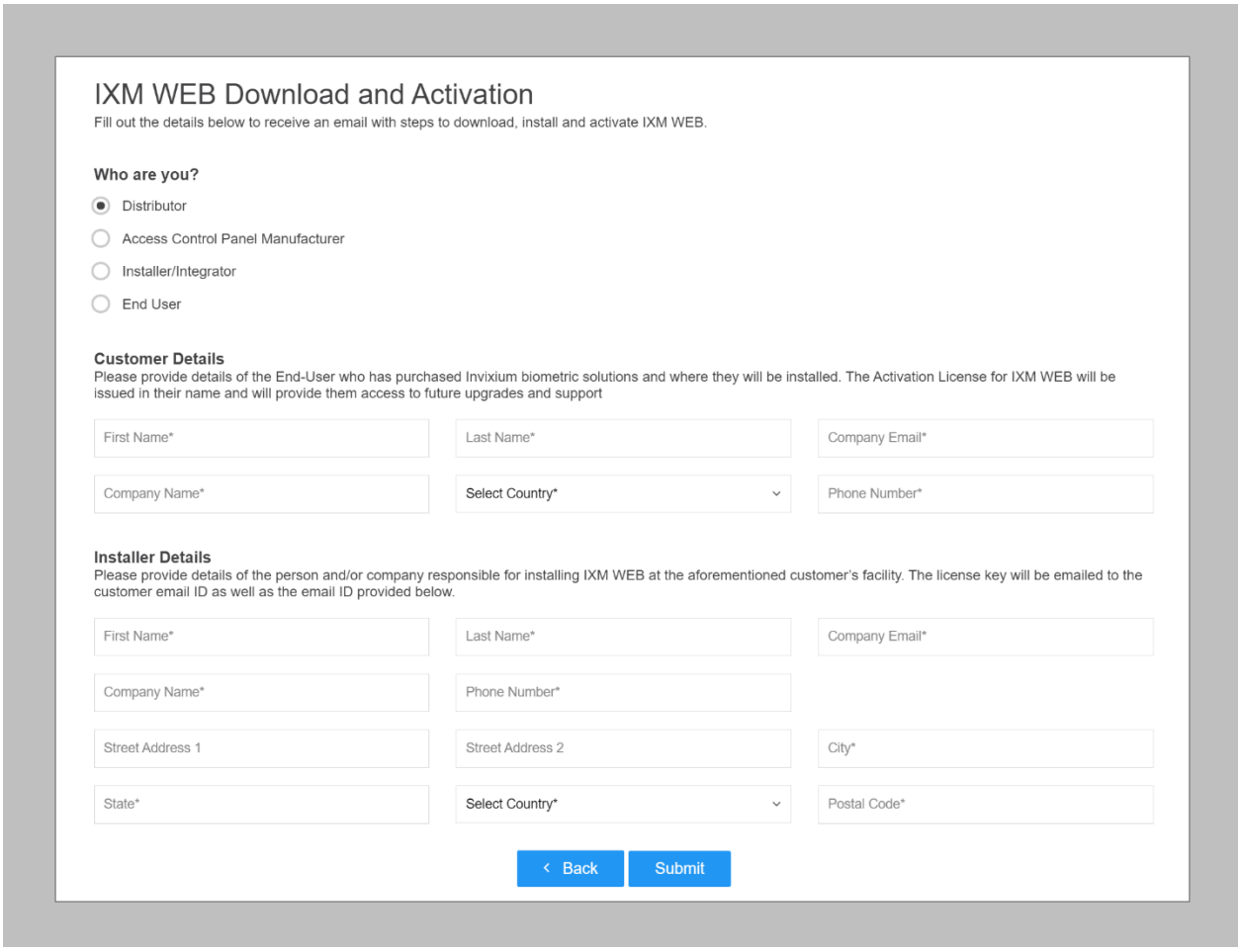
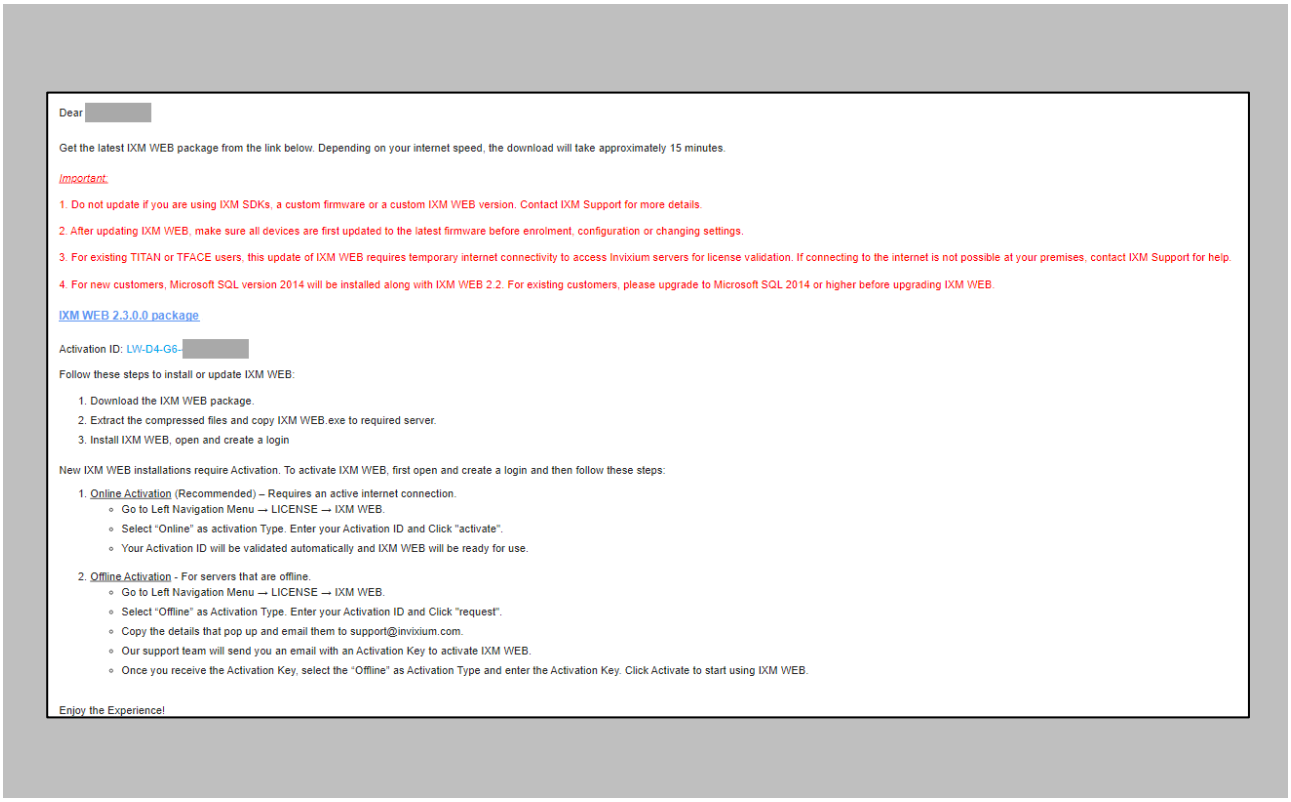


Figure 1: IXM WEB Online Request Form

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 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 conducted 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 the 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
LenelS2 Open Access API Port	8080

Table 4: Port Information

6. Installing IXM WEB

Software Installation

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator), then click **Install**. It will display a popup window to accept the **License Agreement**.

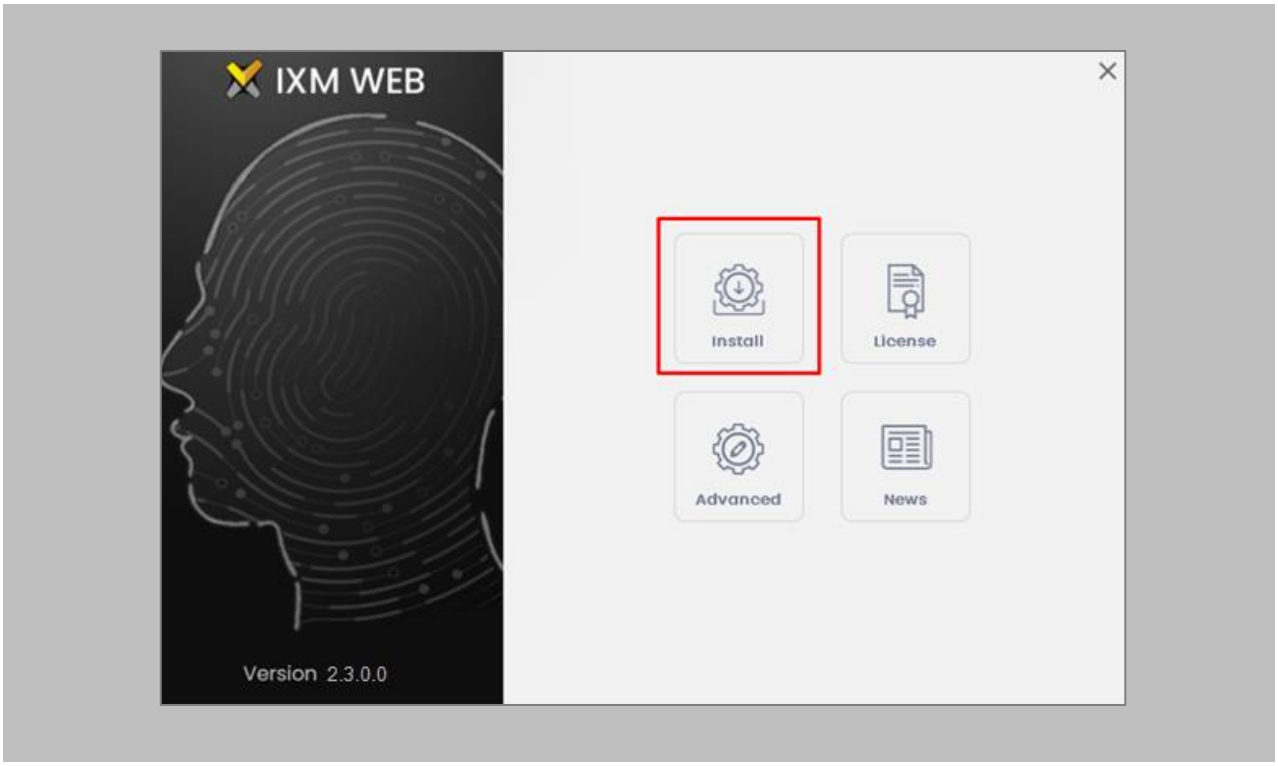


Figure 3: IXM WEB Installer

STEP 2

Click **'Yes'** in the popup window. The IXM WEB installer will start a basic installation process.

STEP 3

By default, IXM WEB performs basic installation and installs software to the default location with the default port number. If the user wants to, they can change the installation path and choose a port number that communicates with the IIS server. Click **Advance**.

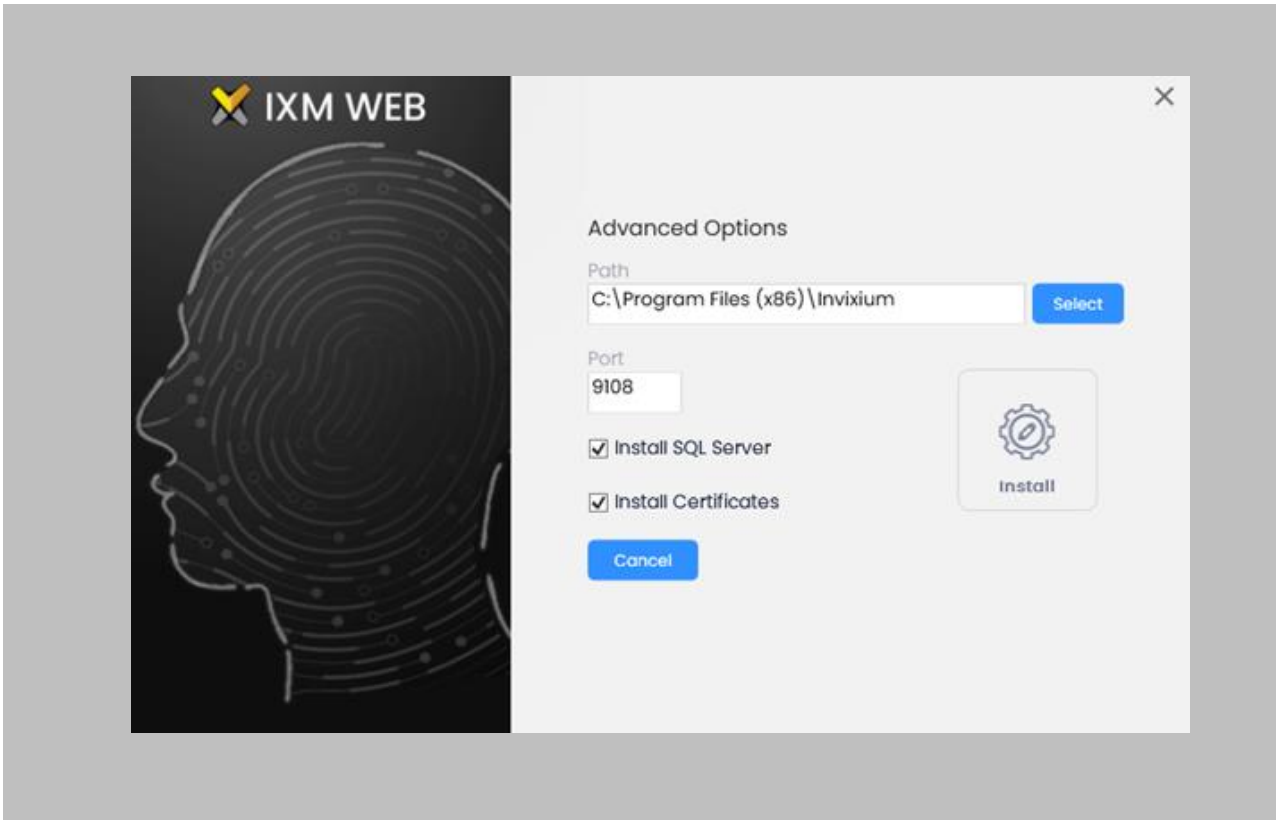


Figure 4: Advanced Option in IXM WEB Installer

STEP 4

In the **Advanced** installation section, the user can change the following options:

- **Installation Path:** In basic installations, the default path is – "***C:\Program Files (x86)\Invixium***". By changing the path, users can determine the new physical path on the machine where the IXM WEB package will be extracted.

- **Port Number:** By default, the port number is "**9108**". Users can change the port number that is generally used to communicate between the WEB Server (Internet Information Services) and IXM WEB.

- **Install SQL Server:** By default, this field is always selected. It means that IXM WEB will install **SQL Server 2014 Express Edition** along with the IXM WEB application. Users can uncheck this field if any other version of SQL Server will be used or if a different machine will be used as a Database Server.

- **Install Certificates:** By default, the IXM WEB installer installs all the necessary certificates that are used in SSL communication. It also installs specific certificates used for communication when configured through the cloud. Users can uncheck this field to prevent IXM WEB from installing all the necessary certificates. Invixium does not recommend deselecting this field.

STEP 5

Once the user completes the changes, click **Install**. IXM WEB packages will continue to install on the machine, and it will display the progress when any component is installed in the background.

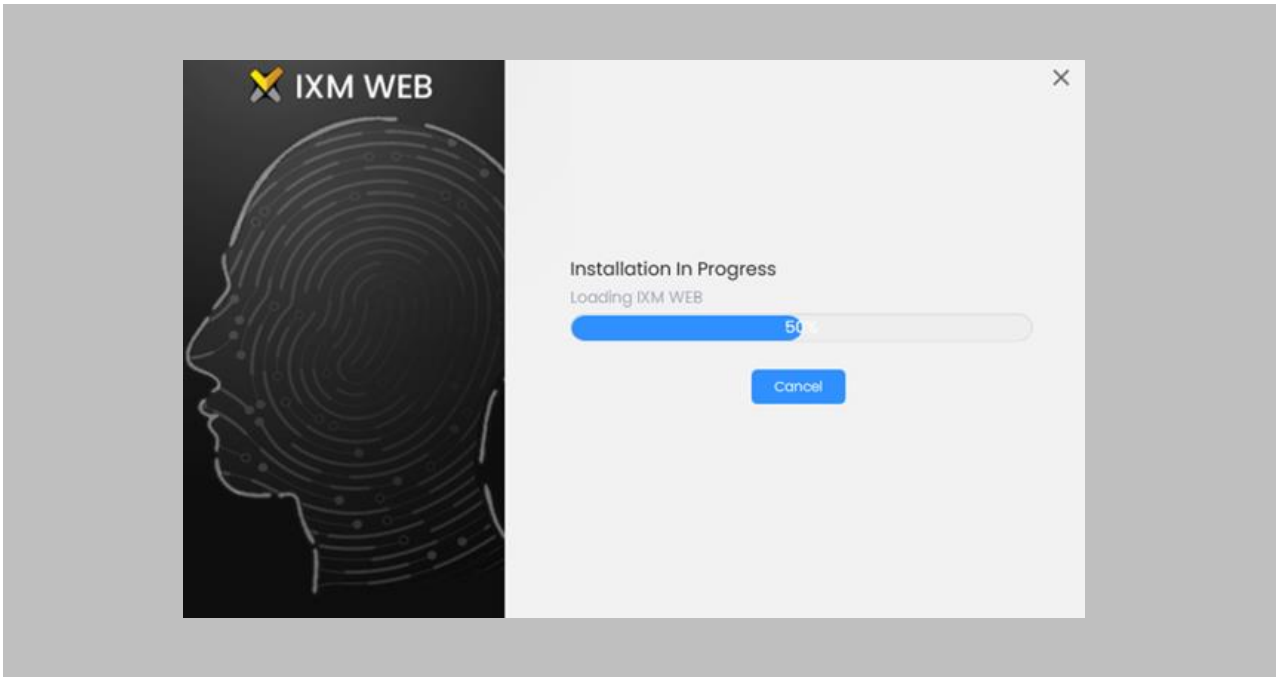


Figure 5: IXM WEB Installation

STEP 6

Once the installation process completes, the user can click **Complete** to finish.

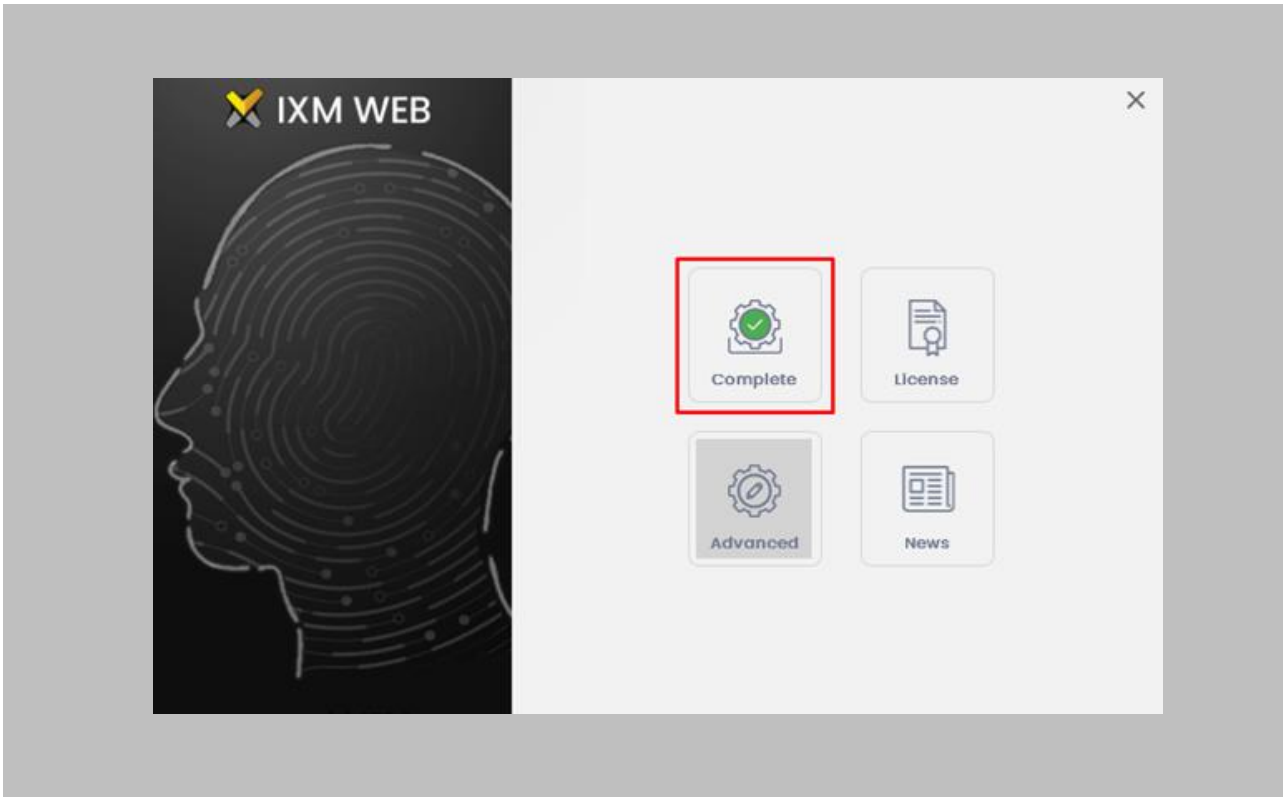


Figure 6: IXM WEB Installation Completed

STEP 7

The IXM WEB package will create a **shortcut icon** on the desktop after the process.

Figure 7: IXM WEB Icon - Desktop Shortcut

STEP 8

Double click on the shortcut icon from the desktop to open **IXM WEB** in the default browser. Users can also open a browser and run the IXM WEB application.

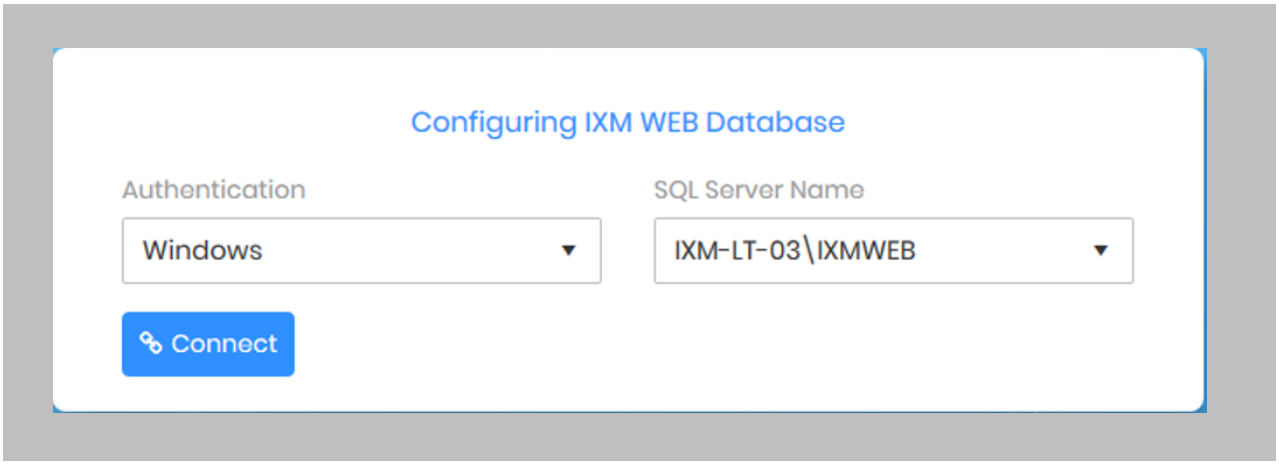


Figure 8: IXM WEB Database Configuration

STEP 9

IXM WEB will populate the default SQL Server name and SQL Server instance.

STEP 10

If the user wants to configure a database that is installed on another machine, then select the **'SQL Server'** option from the Authentication field. By selecting the **'SQL Server'** option, the

user will have to add credentials (SQL User Name and Password) to connect to the Database Server machine.

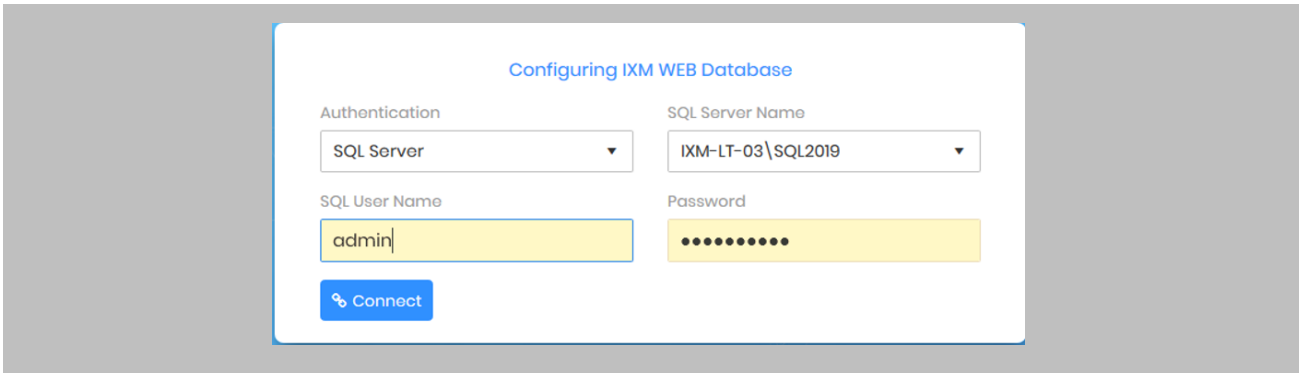


Figure 9: SQL Database Configuration

STEP 11

If a user wants to use the same database instance on the same machine, then click connect to verify if the connection is established with the SQL Instance.

STEP 12

Enter a new **Database** name if there is no previously set up database available.

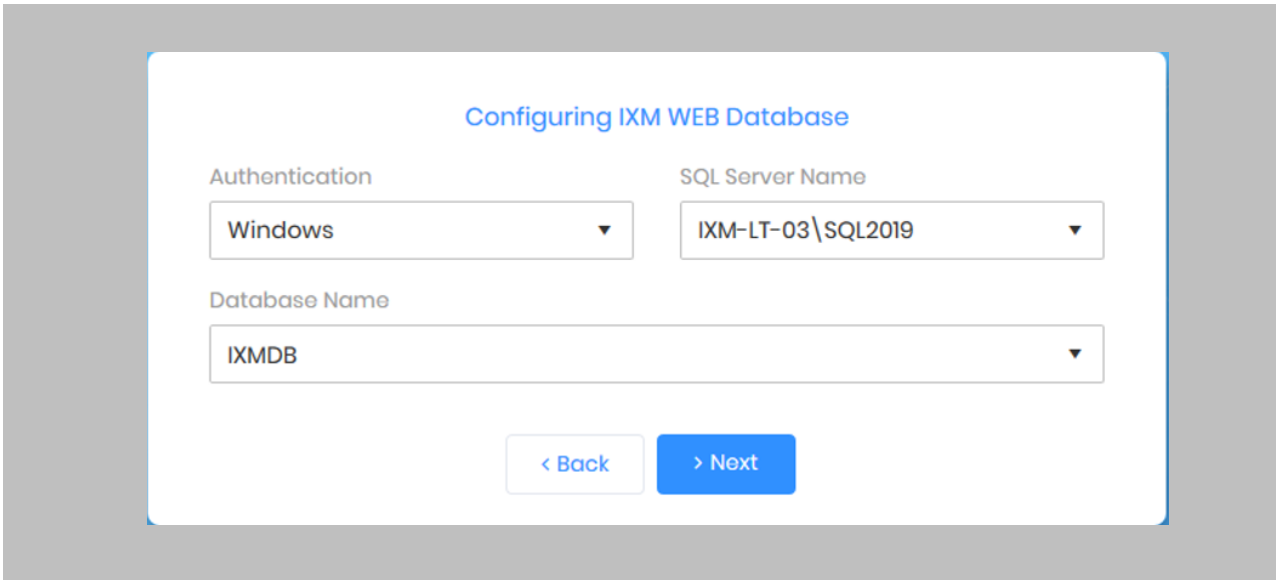


Figure 10: IXM WEB Database Name

STEP 13

Click **Next**.

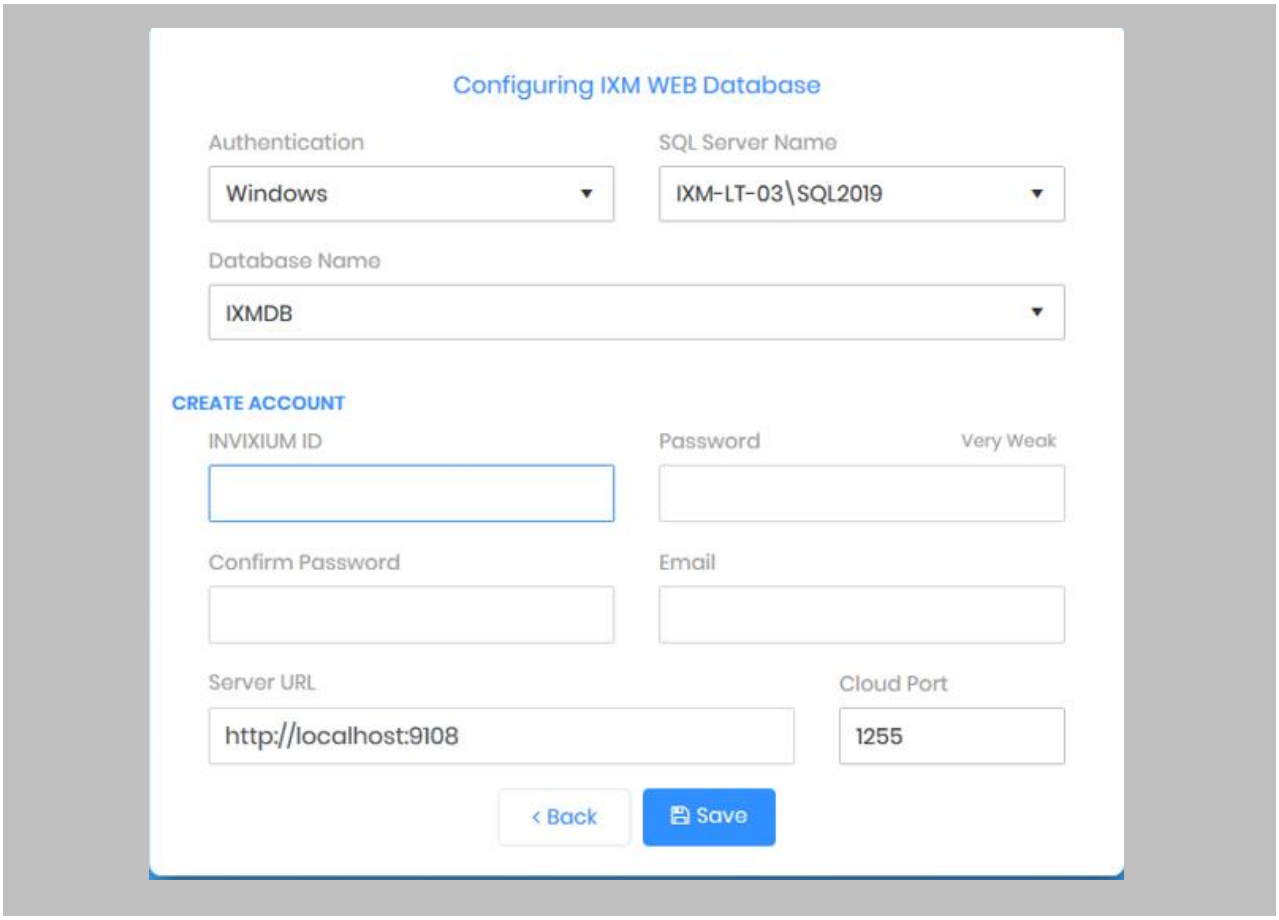


Figure 11: IXM WEB Administrator User Configuration

STEP 14

Users can provide the necessary values to all the fields displayed under the **'Create Account'** section.

STEP 15

The fields and their functions are mentioned below:

- **Invixium ID:** Users can add a username that will have all the rights to access any settings within IXM WEB. This Invixium ID should have a minimum of 5 characters. This Invixium ID configuration will have administrator rights.

- **Password:** The user can set a password. While typing the password, IXM WEB will also display the strength of the entered value to determine how secure the password field is.
- **Confirm Password:** Enter the password value once again. Users need to enter the same password that they entered in the password field.

- **Email:** Set an administrator email address, IXM WEB will use this email address in the future in case the password needs to be reset, or to send any type of email notification.

- **Server URL:** Users can set a Web URL or an IP Address on the machine where IXM WEB is installed along with the port number. By default, the port number is 9108. Format: **http://IP_IXMServer:9108**

- **Cloud Port:** If a user wants to configure the devices over WEB Cloud, then a specific port number needs to be mentioned in the Cloud Port field. By default, the Cloud Port value is 1255.

STEP 16

Once the user is done providing all the values, click **Save**.

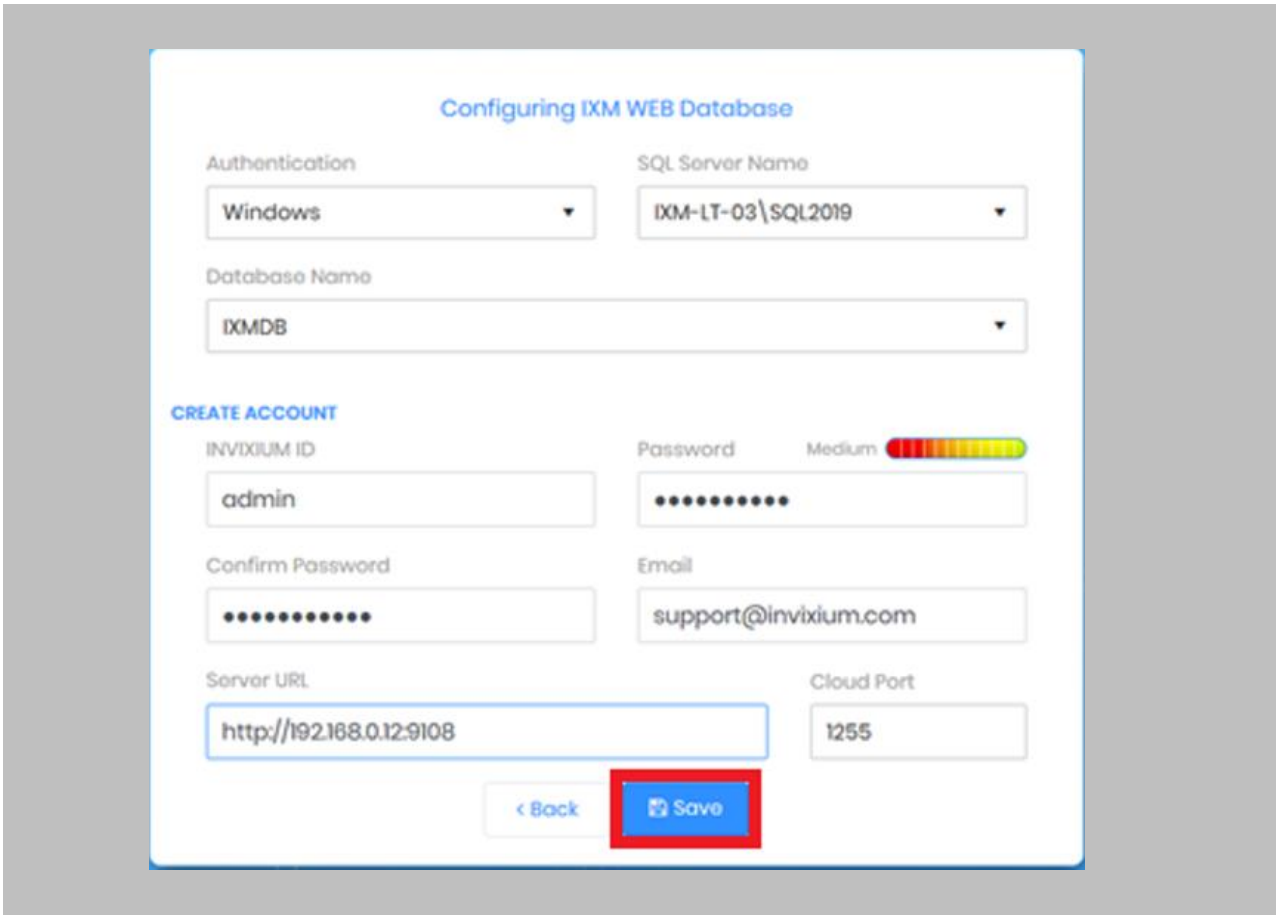


Figure 12: Save Database Configuration

STEP 17

Using the provided values, IXM WEB will create a database and, upon success, the user will be redirected to the **Login Page**.

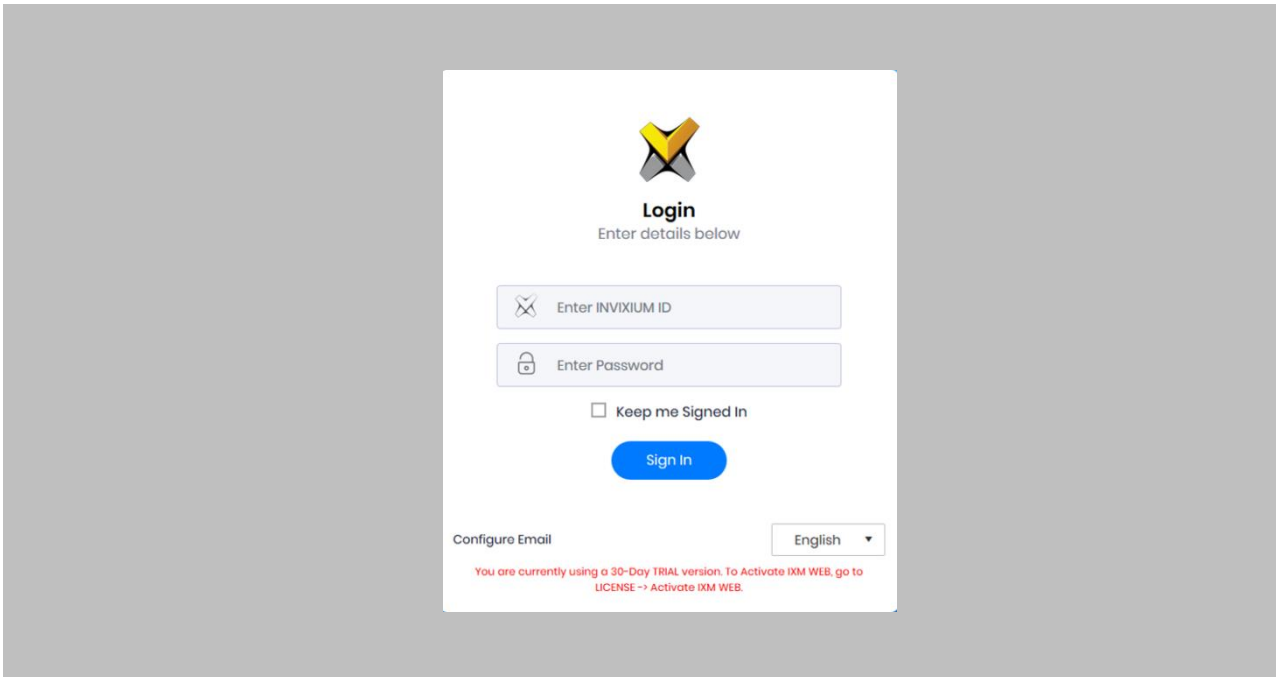


Figure 13: IXM WEB Login Page

7. Configuring Email Settings Using IXM WEB

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

Email Setting Configuration

Procedure

STEP 1

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

OR

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

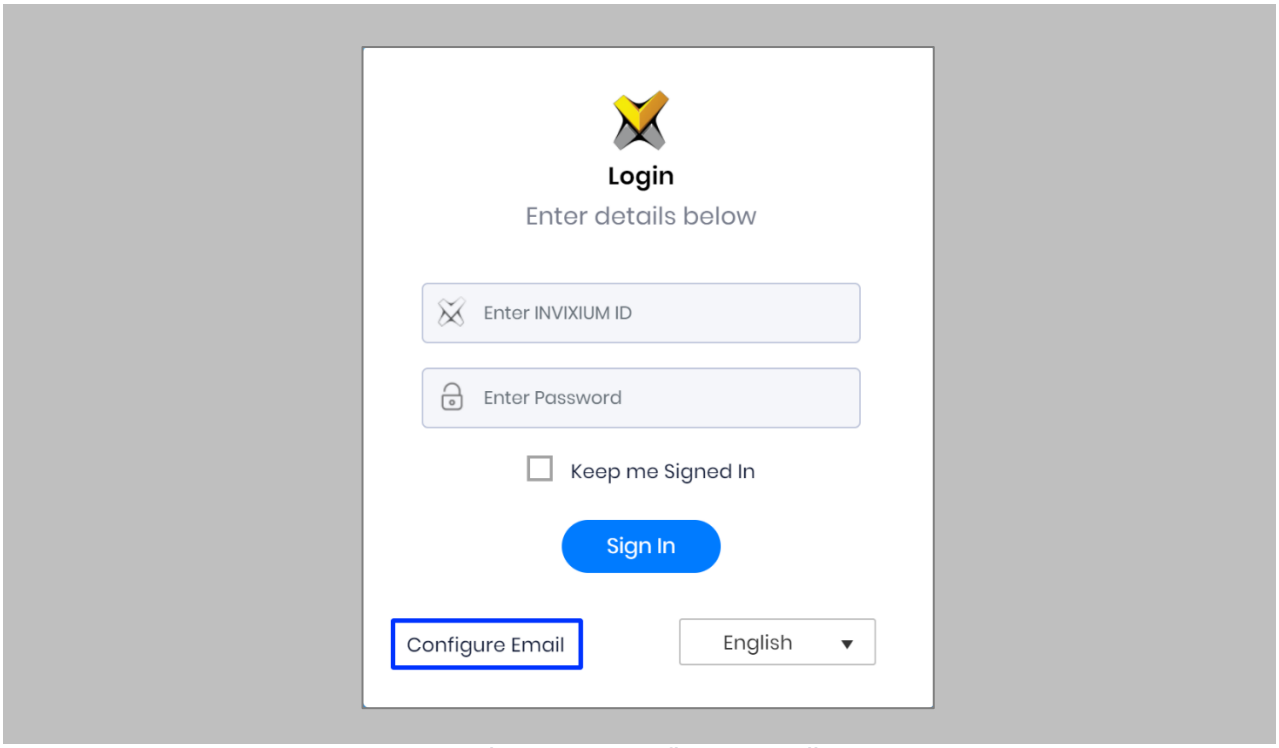


Figure 14: Configure Email

STEP 2

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

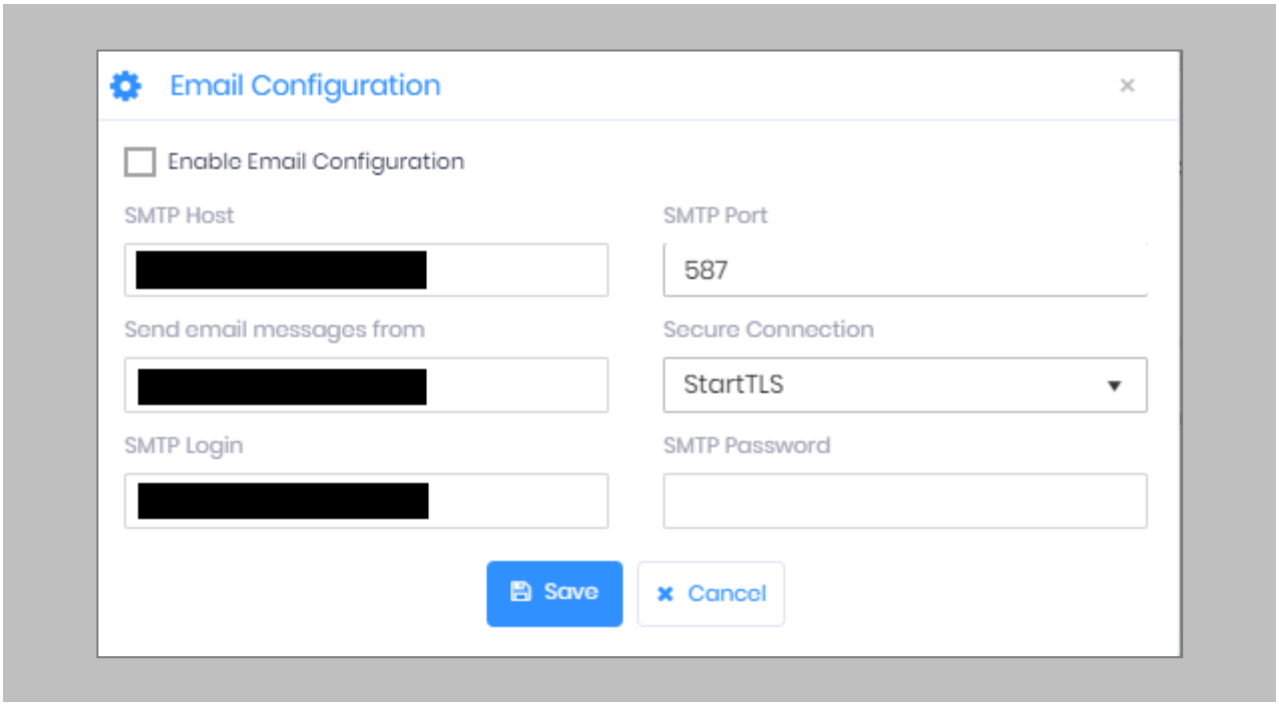


Figure 15: IXM WEB - SMTP Settings

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.

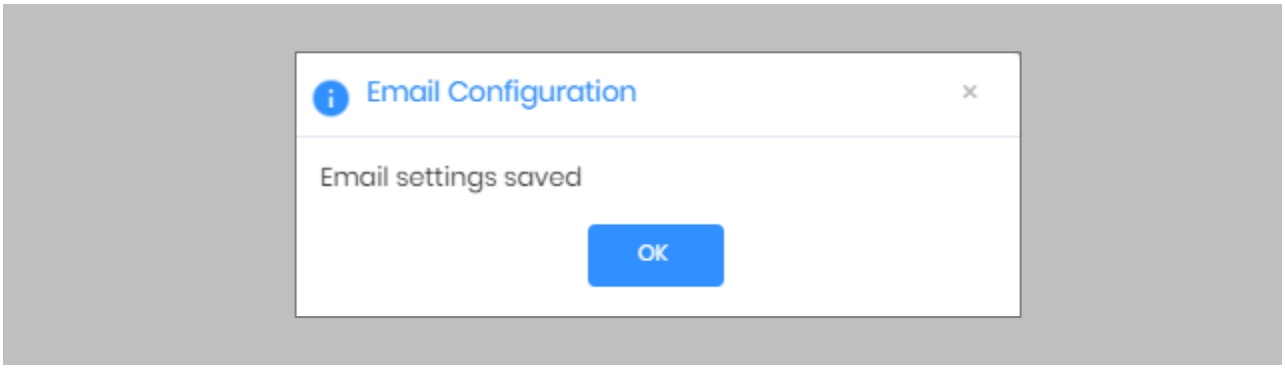


Figure 16: IXM WEB - Save Email Settings

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.

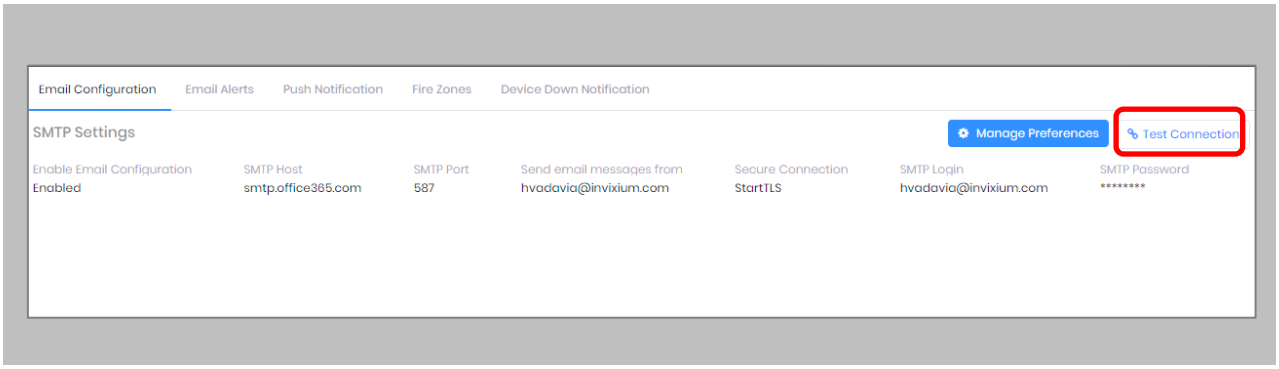


Figure 17: IXM WEB - Test Connection

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

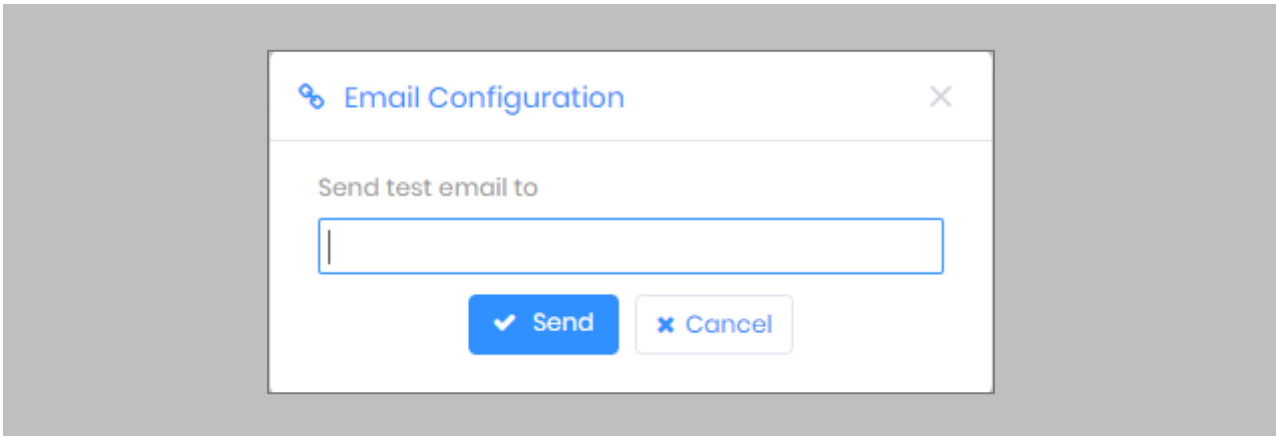


Figure 18: IXM WEB - Enter Email ID

STEP 4

Once Email Configuration is completed, a **Forgot Password** link will appear on the Sign In page in its place.

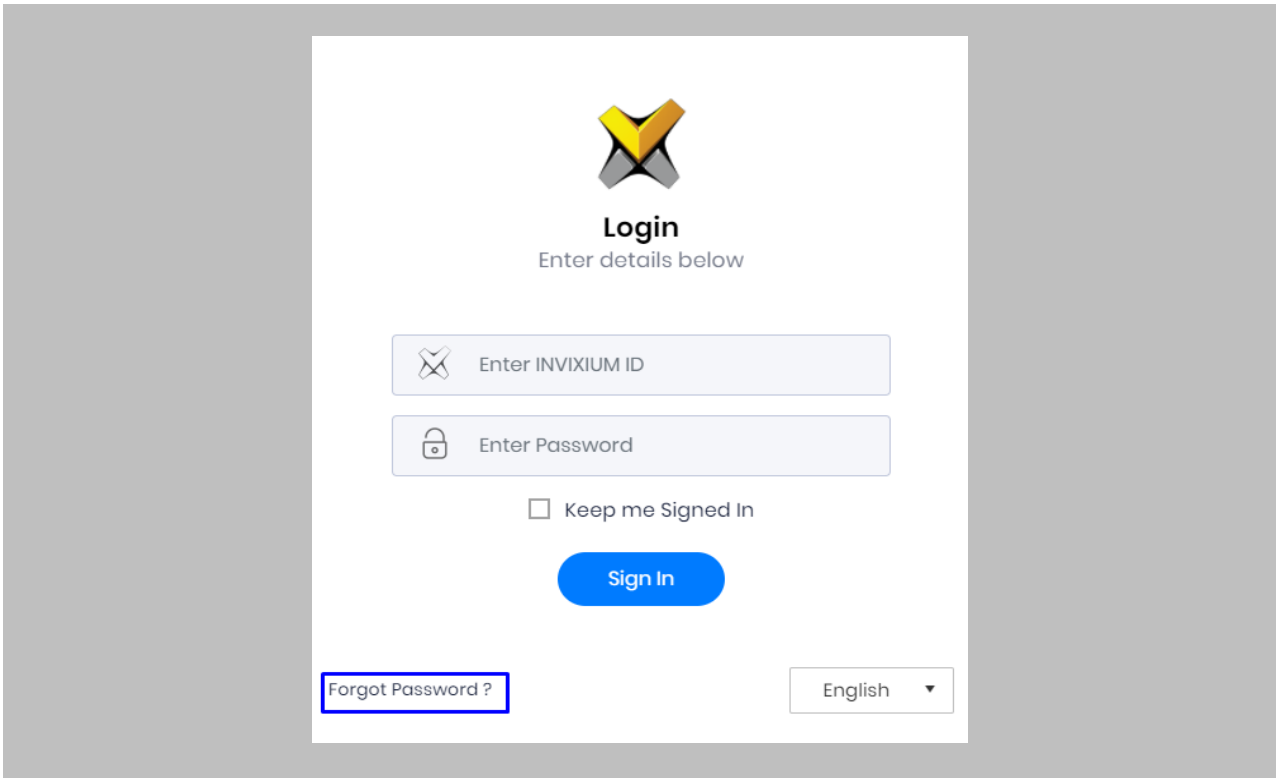


Figure 19: IXM WEB - Forgot Password

8. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

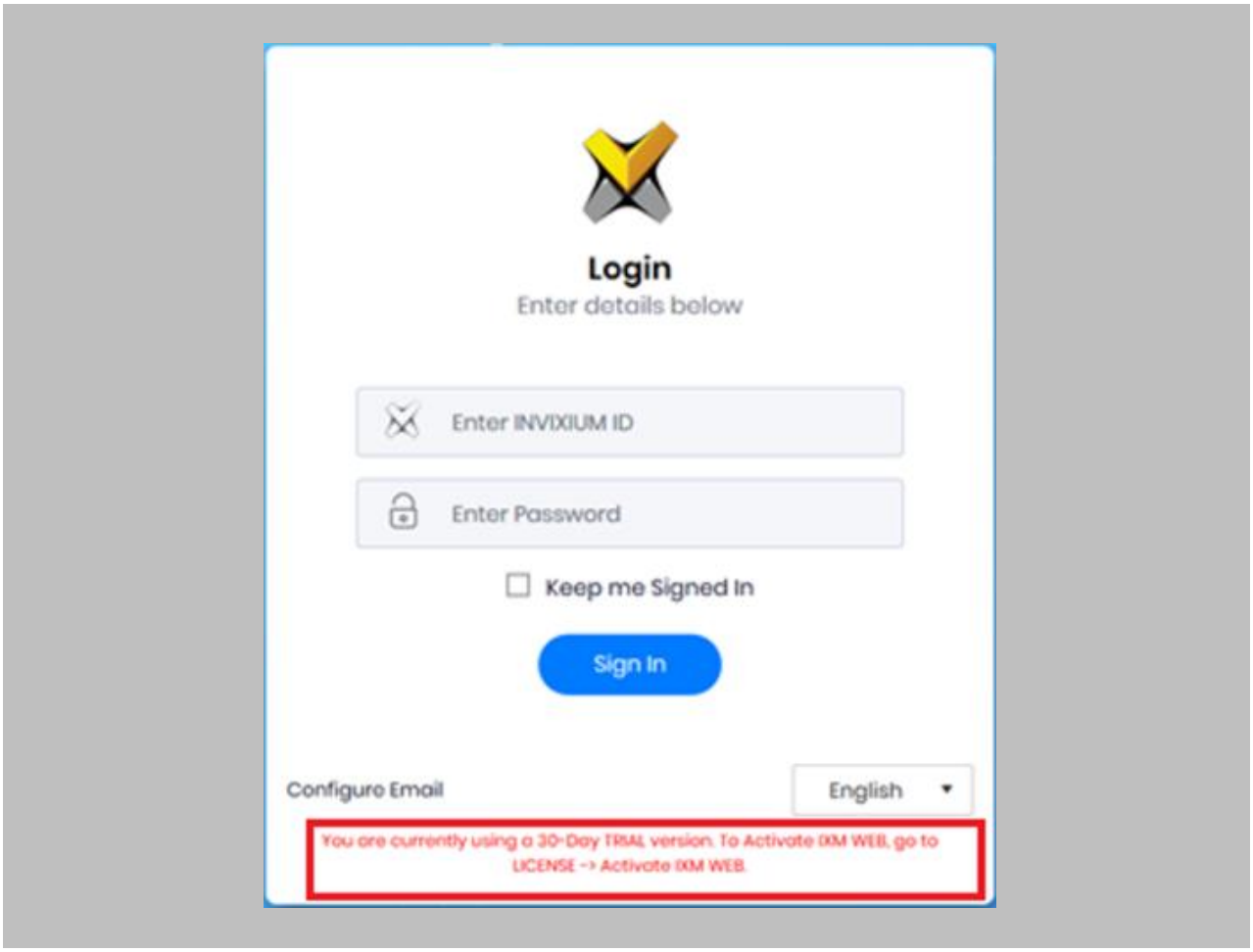


Figure 20: IXM WEB - Enter Login Credentials

STEP 2

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

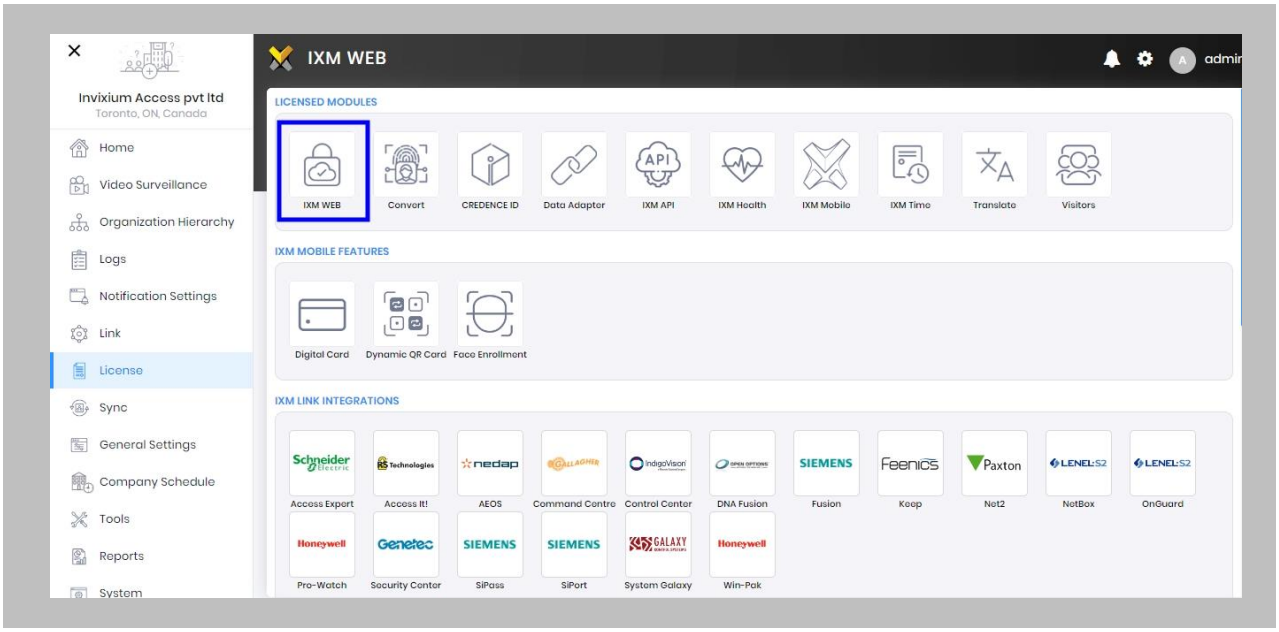


Figure 21: IXM WEB - License Setup

STEP 3

Request an **activation key online** or via **Offline Activation Options.**

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

STEP 4

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

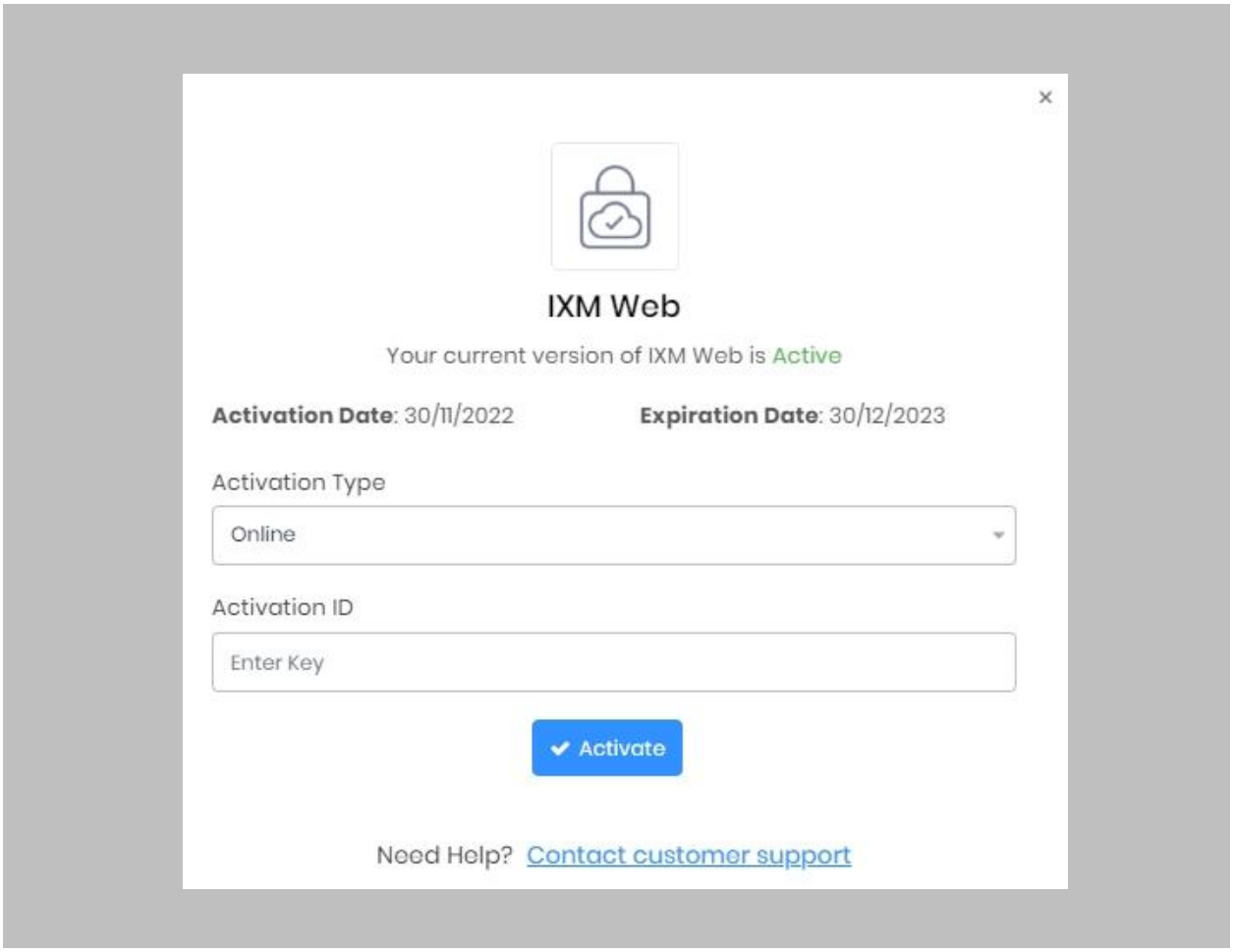


Figure 22: IXM WEB - Online Activation

OnGuard by LenelS2 Module Activation

The option to request an OnGuard License is available under the **License** tab.

STEP 1

Request a **License**.

STEP 2

From **Home**, expand the **Left Navigation Pane**, and go to the **License** tab. Click on OnGuard **(LenelS2).**

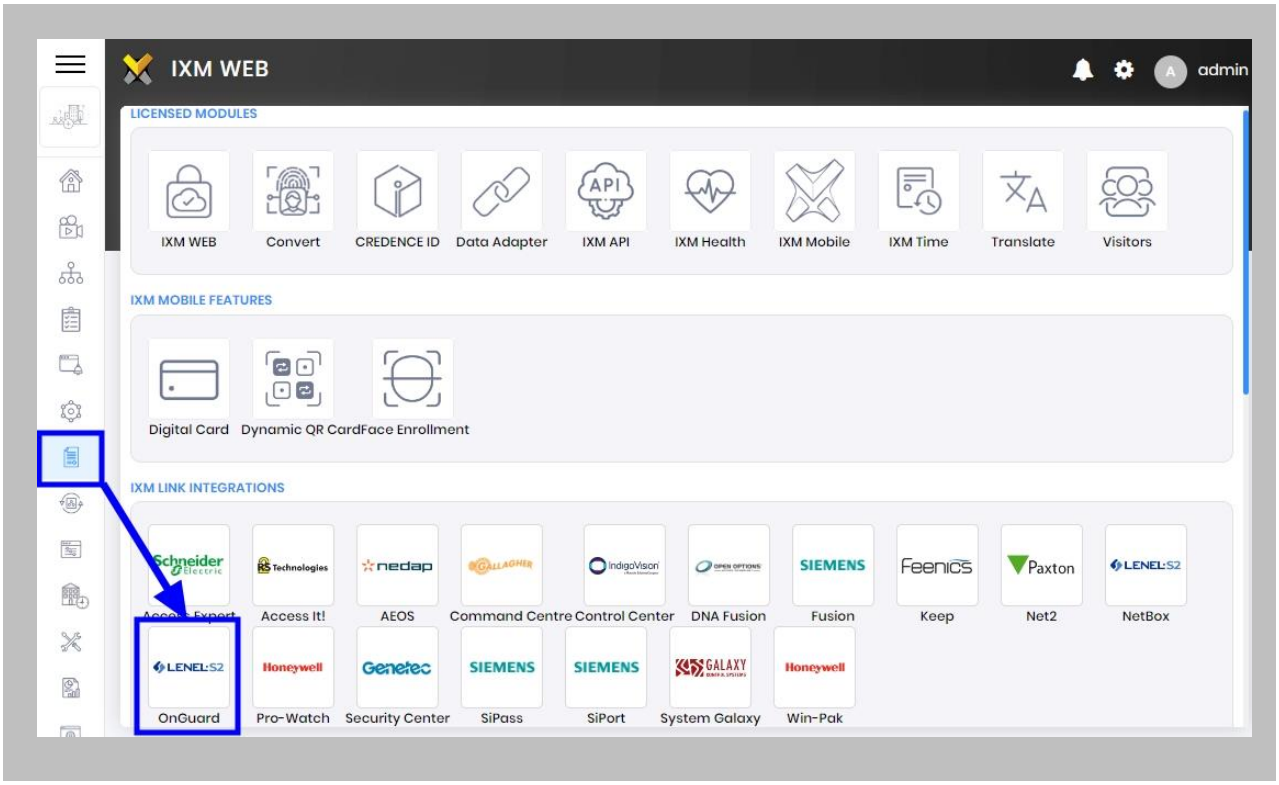
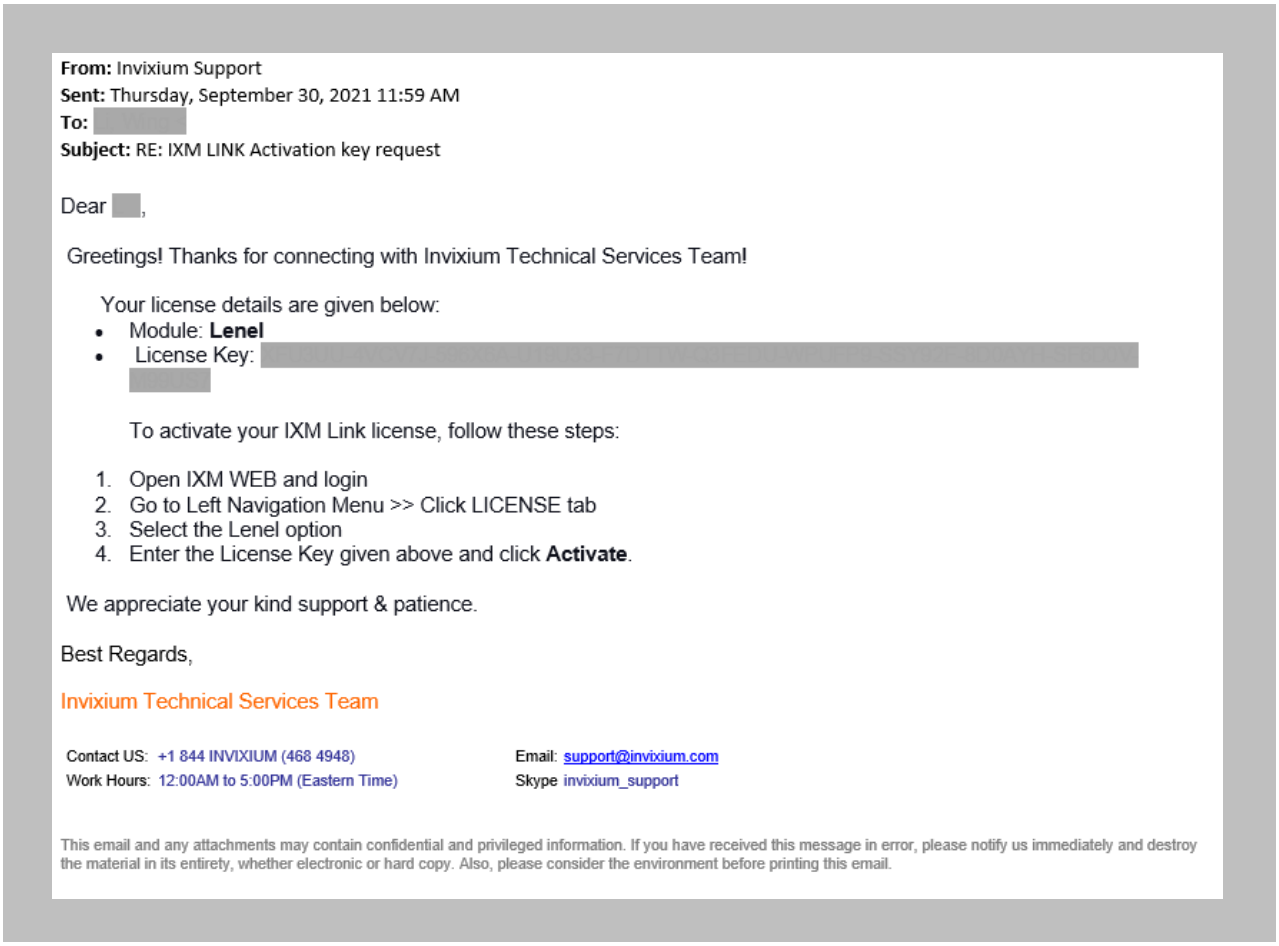


Figure 23: IXM WEB – OnGuard by LenelS2 Link Activation

STEP 3

You will receive an email from **Invixium Support** with a license key for the OnGuard Activation.



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

Dear [redacted],

Greetings! Thanks for connecting with Invixium Technical Services Team!

Your license details are given below:

- Module: **Lenel**
- License Key: [redacted]

To activate your IXM Link license, follow these steps:

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

We appreciate your kind support & patience.

Best Regards,

Invixium Technical Services Team

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

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

Figure 24: OnGuard License Key Email

STEP 4

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

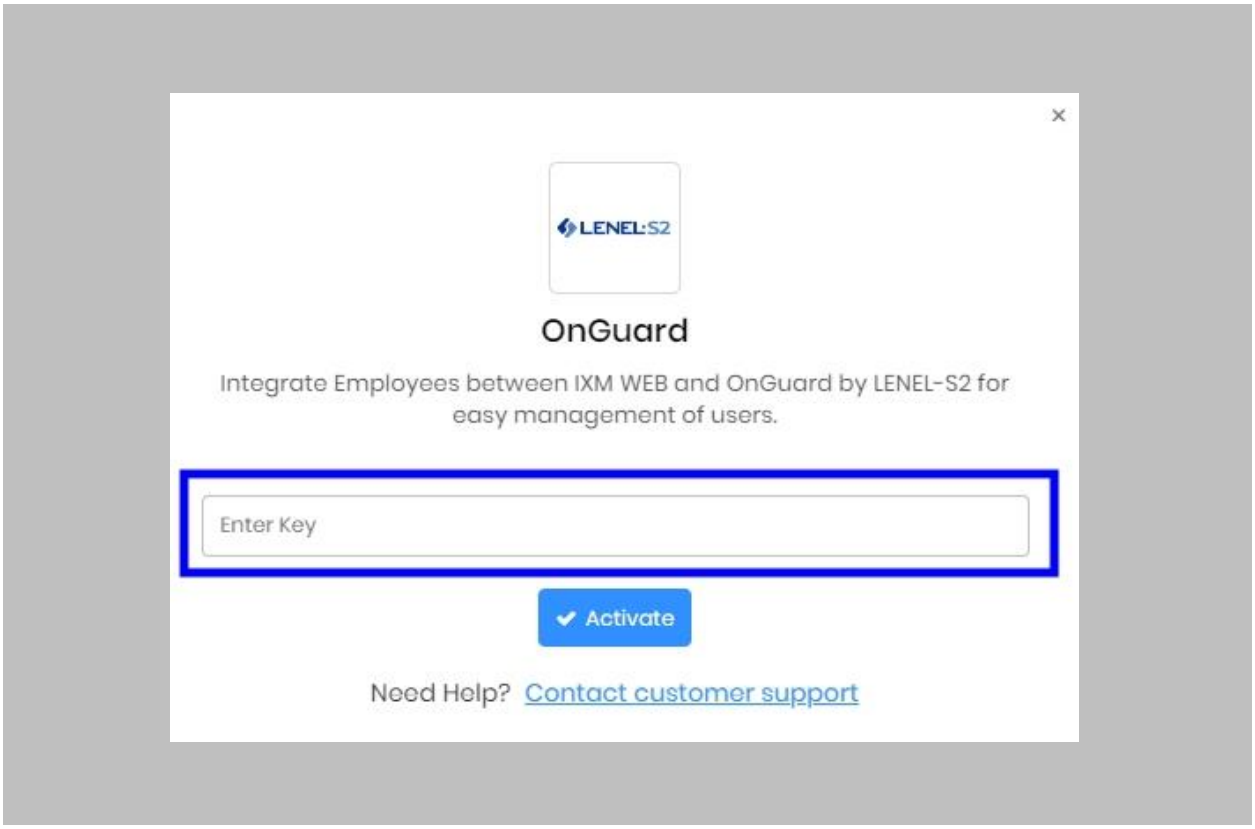


Figure 25: IXM WEB - Activate LenelS2 Link License

RESULT

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

9. Configuring IXM Link for OnGuard by LenelS2

Procedure

STEP 1

From the **Left Navigation Pane** → **Link** → click the red **OnGuard (Lenel-S2)** icon.

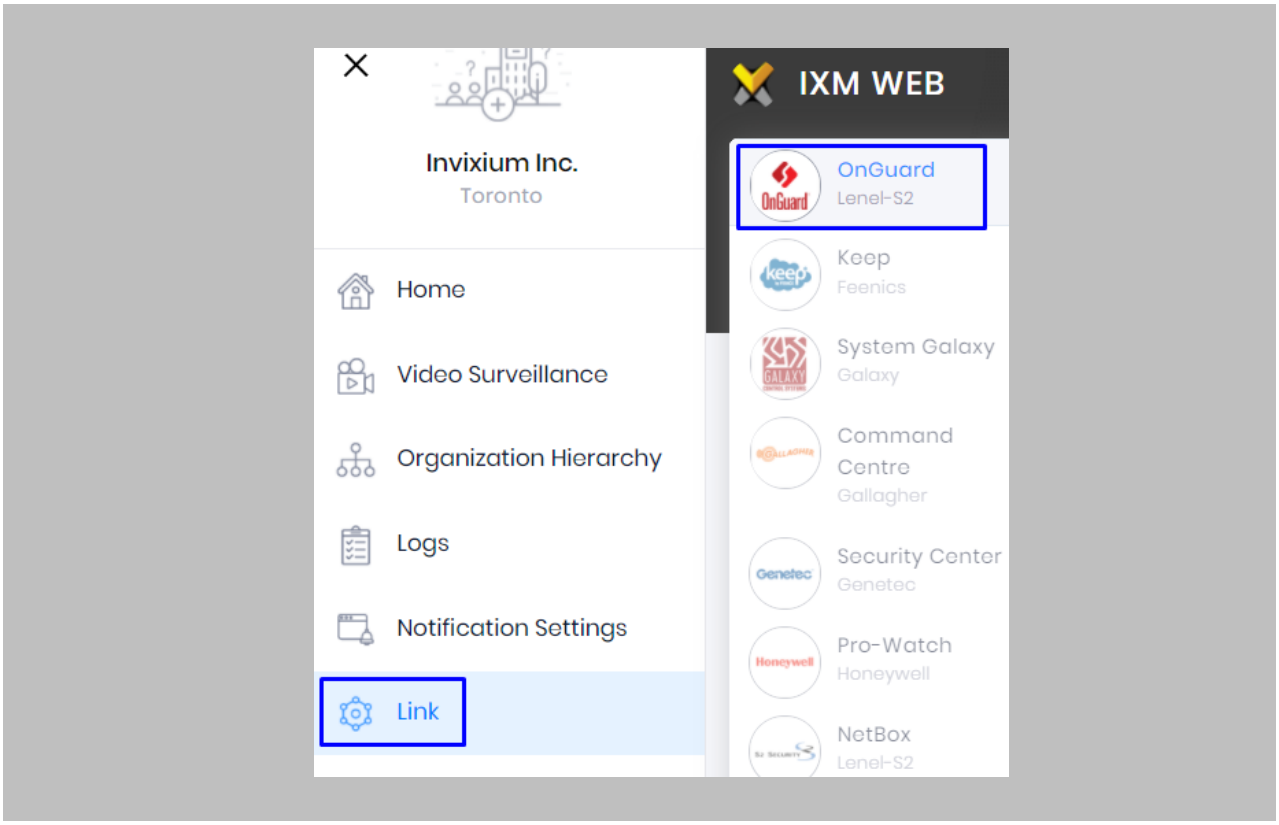


Figure 26: IXM WEB - Link Menu

STEP 2

Toggle the **Status** switch to enable.

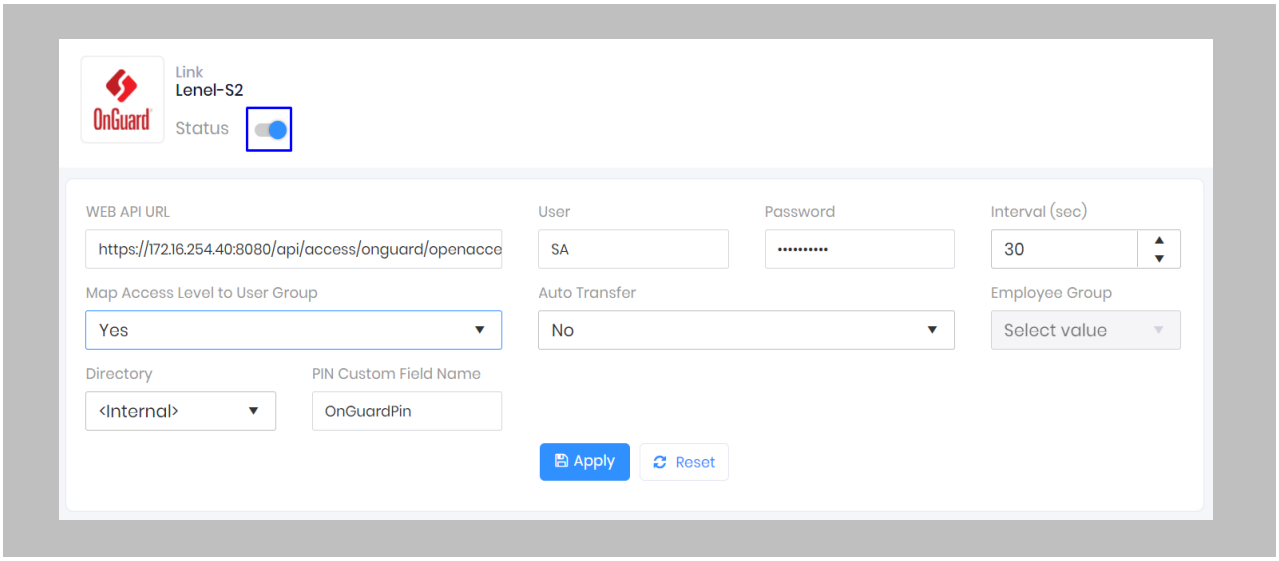


Figure 27: IXM WEB - Enable Lene-S2 Link Module

STEP 3

Enter the **OnGuard Open Access API URL**. For example:
https://172.16.254.40:8080/api/access/onguard/openaccess/

STEP 4

Enter your **Username and Password** for accessing Open Access API.

STEP 5

Specify in seconds how often **sync** should take place.

STEP 6

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 OnGuard 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.

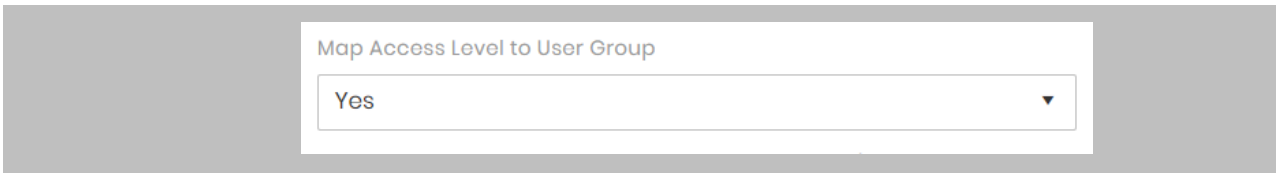


Figure 28: IXM WEB - Map Access Level to User Group

STEP 7

Auto Transfer

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

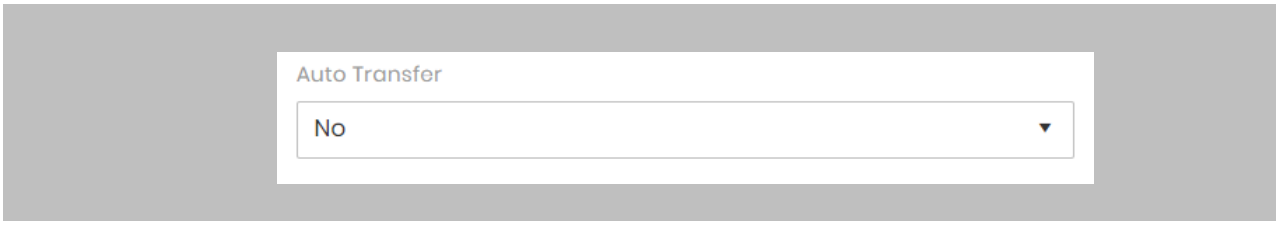


Figure 29: IXM WEB - Auto Transfer No

Yes: On selecting 'Yes' for Auto Transfer, the employee group selection dropdown enables displaying all the employee groups present in IXM WEB. All the employees synchronized from OnGuard will be automatically added to the employee group selected on the Link Configuration Page.

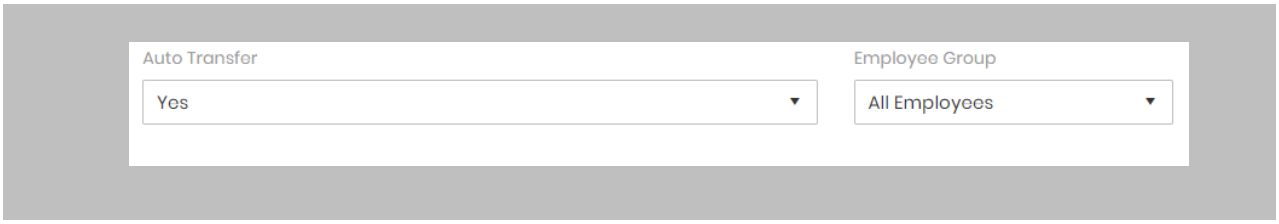


Figure 30: IXM WEB - Auto Transfer Yes

STEP 8

Select the **Directory** to which the API user belongs.

STEP 9

Copy the custom field name created for **'PIN Number'** (refer to Configure Custom PIN Field in OnGuard)

STEP 10

Click **Apply.**

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

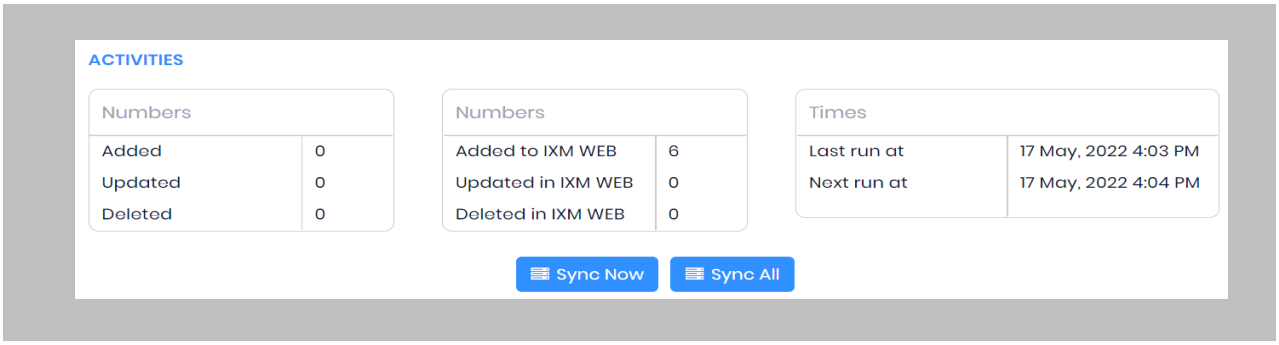


Figure 31: IXM WEB - Sync Activities

STEP 11

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 12

If the sync direction is selected as OnGuard to IXM WEB (One-way sync) then the **Sync All** button will get displayed.

STEP 13

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

RESULT

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

10. Create API System Users for Biometric Enrollment

Creating API System Users 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.

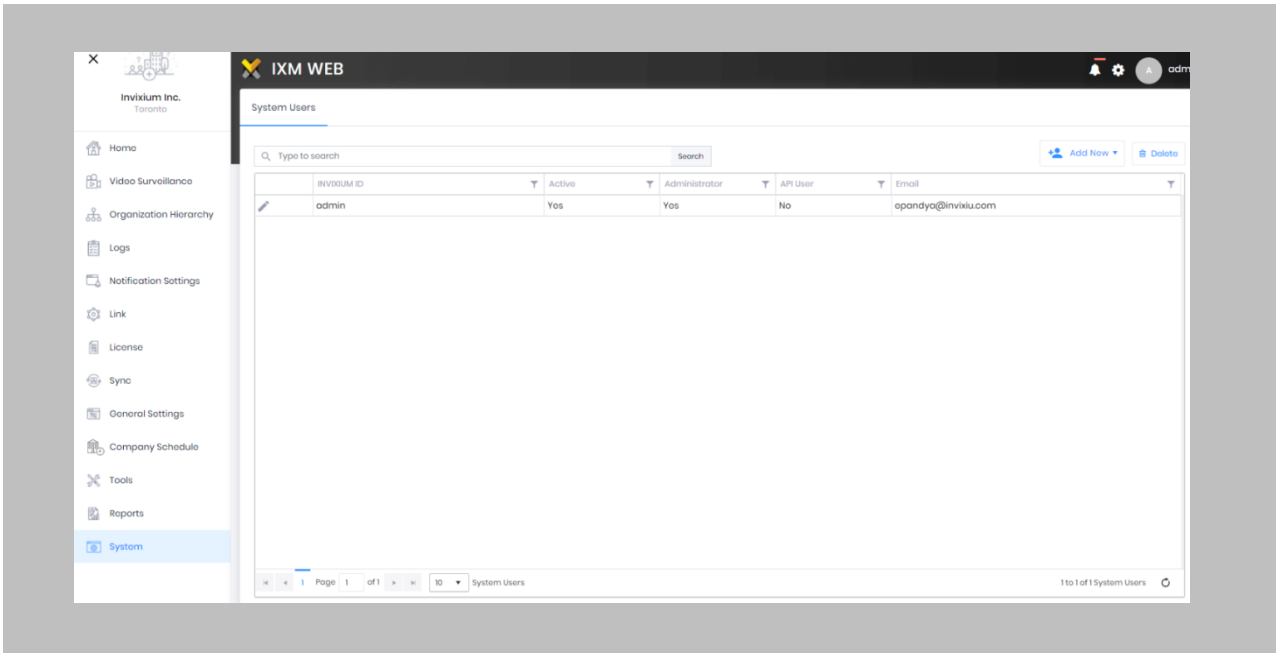


Figure 32: IXM WEB - Create API User

STEP 2

Click **Add New API User**.

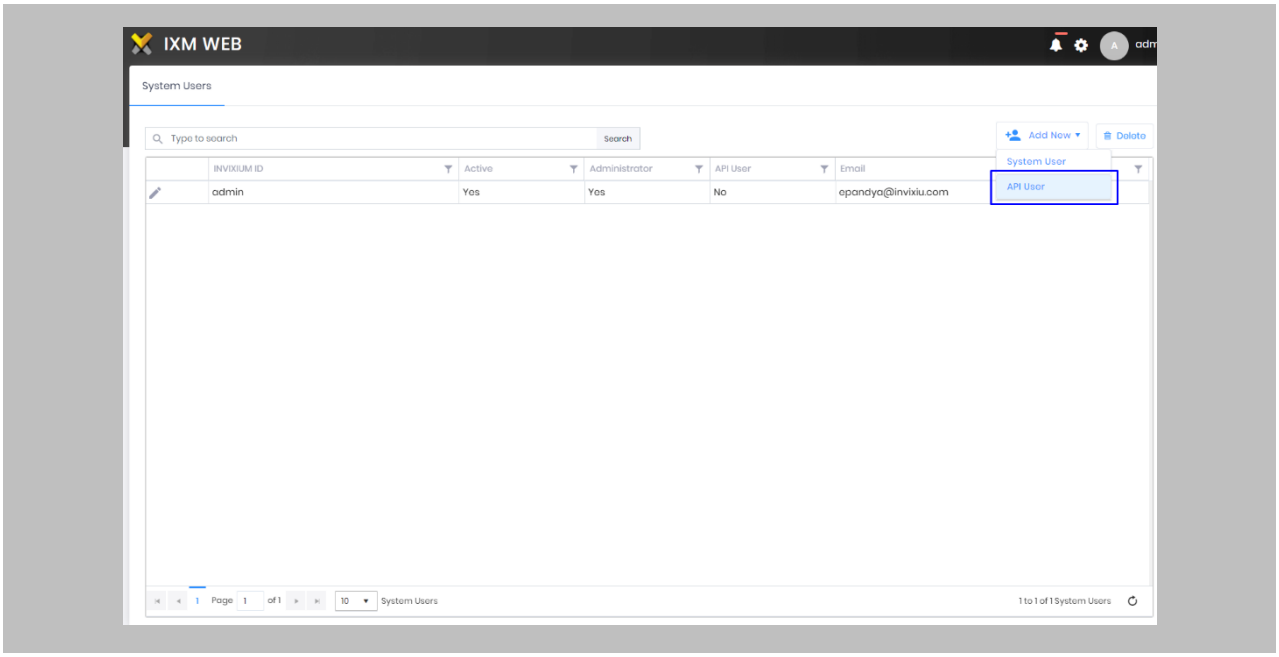


Figure 33: IXM WEB - Add New API User

Creating an API user requires the following details:

- Invixium ID (User ID)
- Password
- Confirm Password
- Email address
- Status
- Permission for modules

STEP 3

Enter the **Invixium ID and Password** for the API user.

STEP 4

Add an email address.

Apply for permission as “All” in the **Enrollment & Employee Access Rule** module.

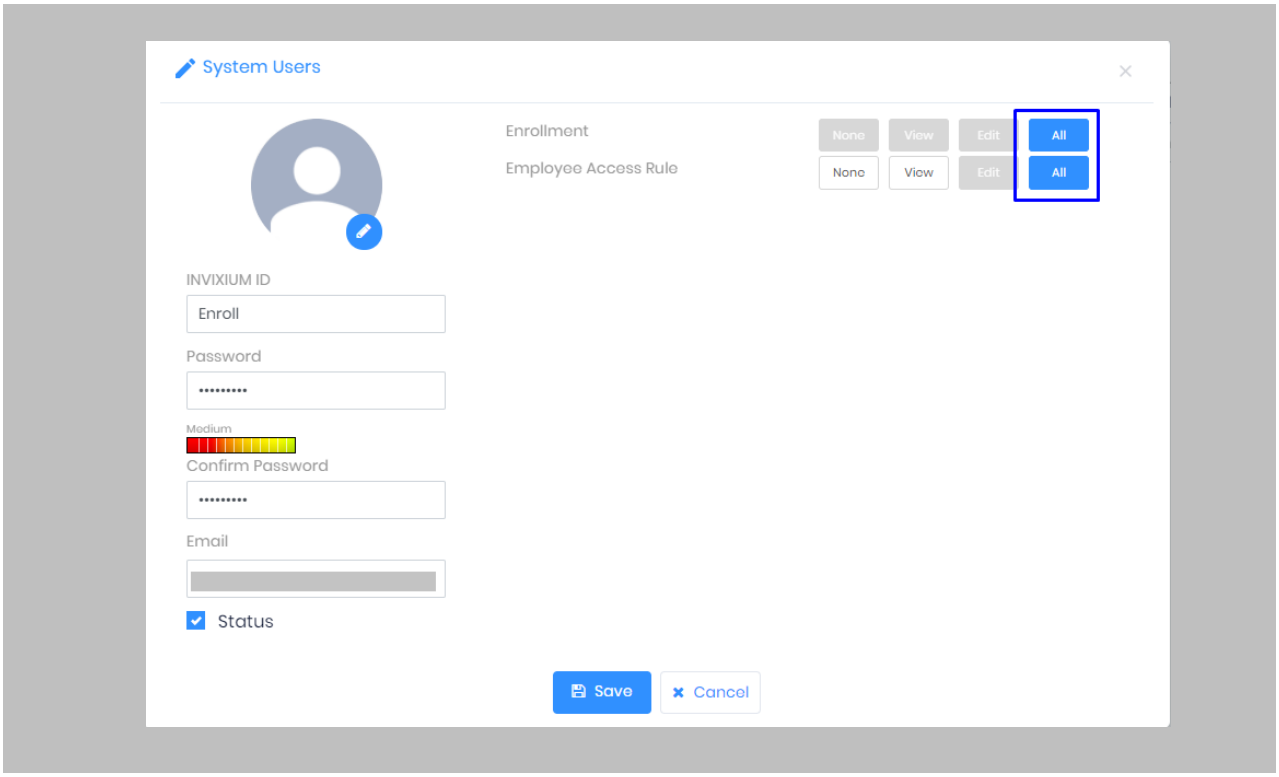


Figure 34: IXM WEB - New API User

STEP 5

Click **Save**.

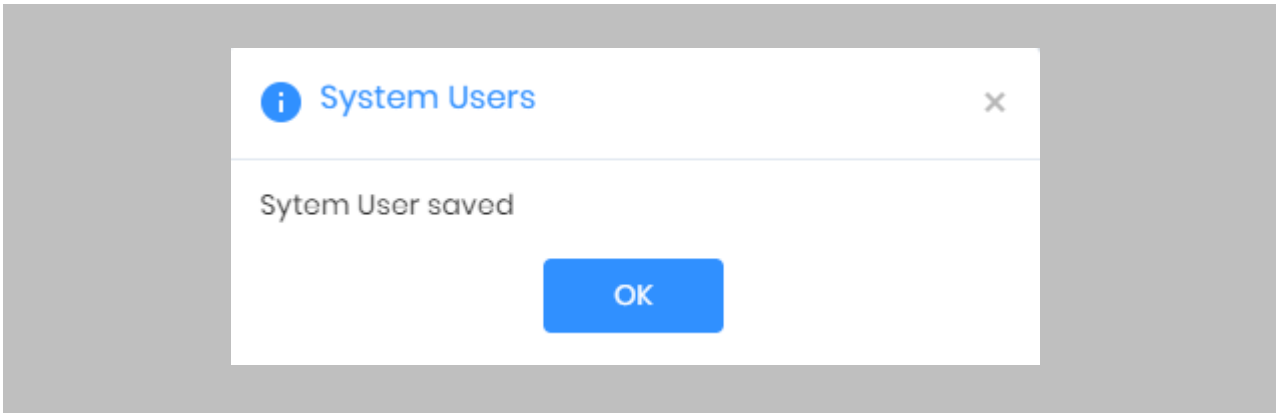


Figure 35: IXM WEB - Save API User

11. Configure Readers in OnGuard

The following settings are needed in System Administration for using the ‘Map Access Level to User Group’ feature.

Procedure

STEP 1

Open ‘System Administration’ → Click **Access Control** → **Access Panels.**

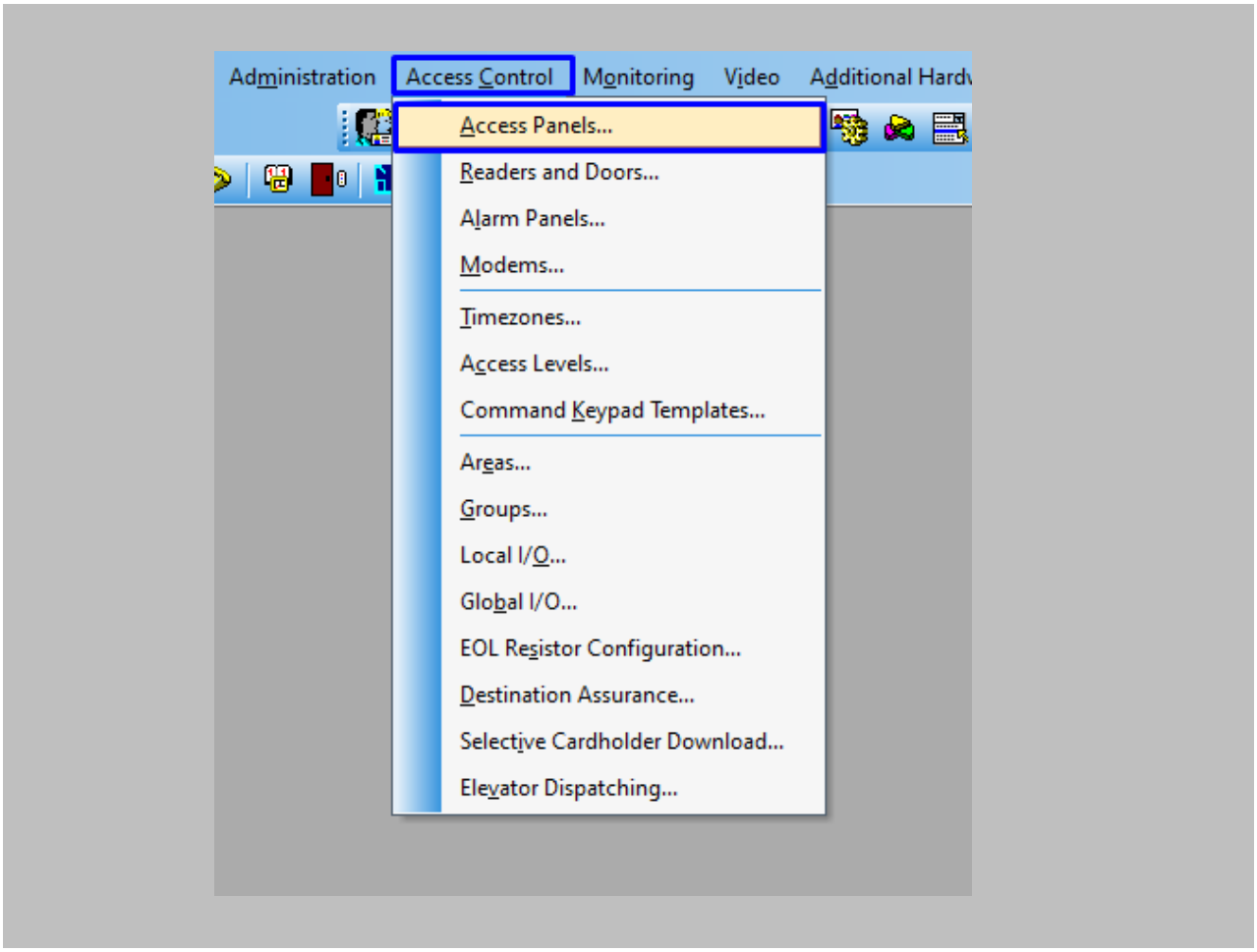


Figure 36: OnGuard - Access Panel

STEP 2

Add a new panel as per your requirement from the following screen.

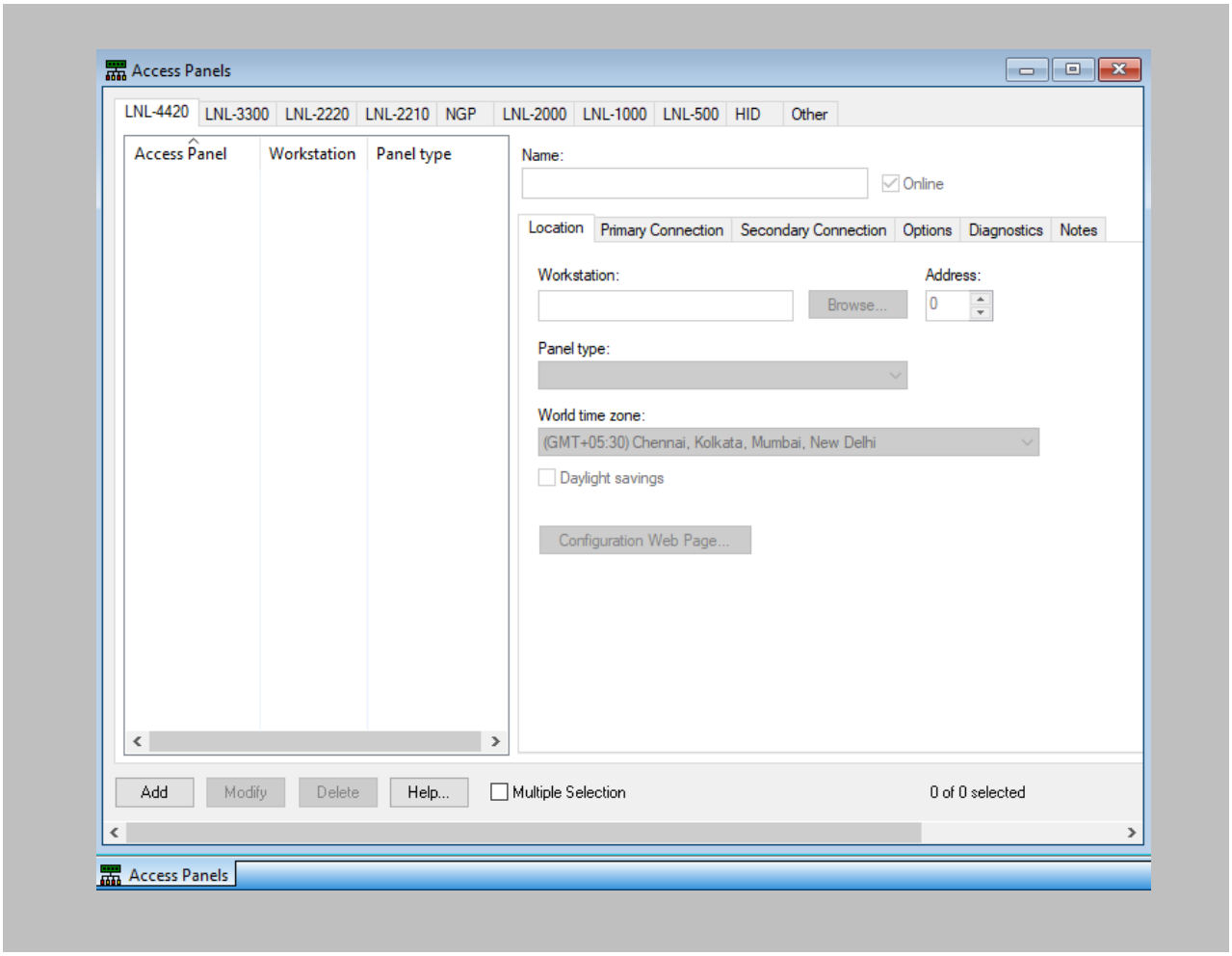


Figure 37: OnGuard - Add Access Panel

STEP 3

Click **Access Control** → **Readers and Doors**.

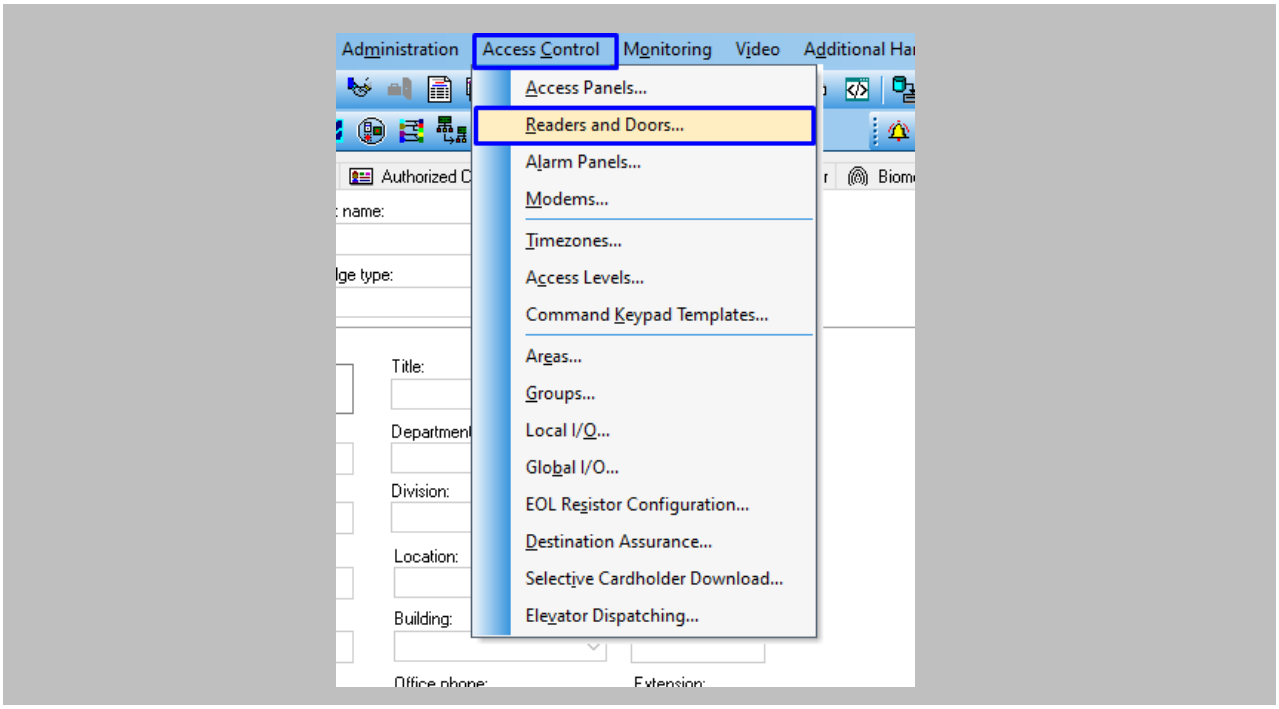


Figure 38: OnGuard - Readers and Doors

STEP 4

Click on the **Add** button.

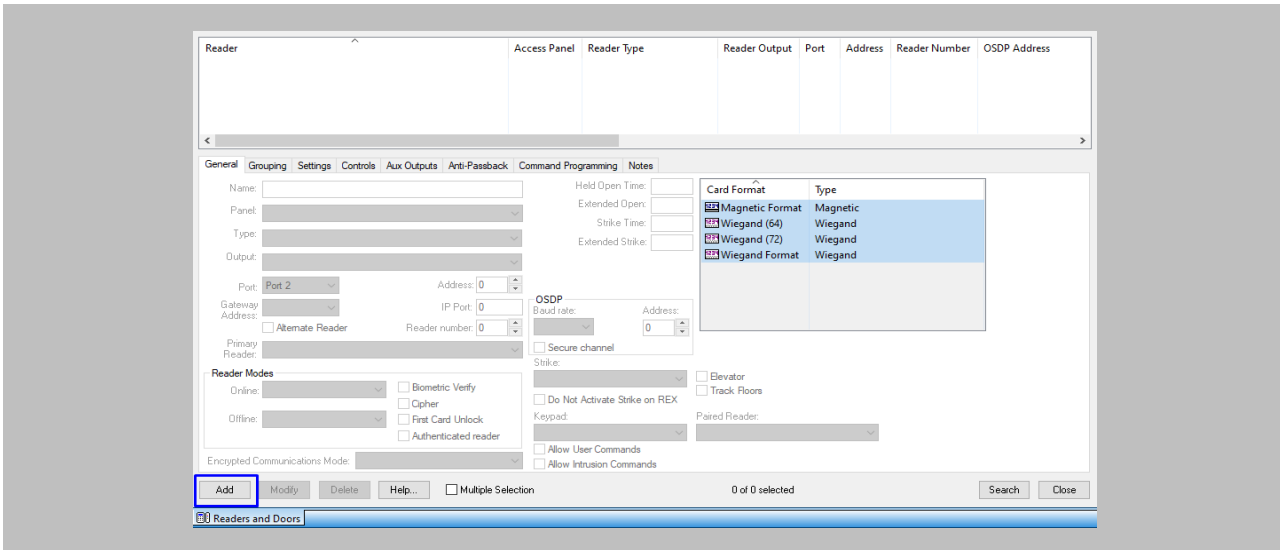


Figure 39: OnGuard - Add New Reader

STEP 5

Enter the following details:

Name: The name of the **reader** should be the same as the name of the **Invixium device** present in IXM WEB, which will automatically add the Invixium device to the device group synced from OnGuard when the 'Map Access Level To User Group' setting is enabled.

Panel: Select any of the existing OnGuard panels from the **Panel** dropdown.

Enter other mandatory details and Click **OK.**

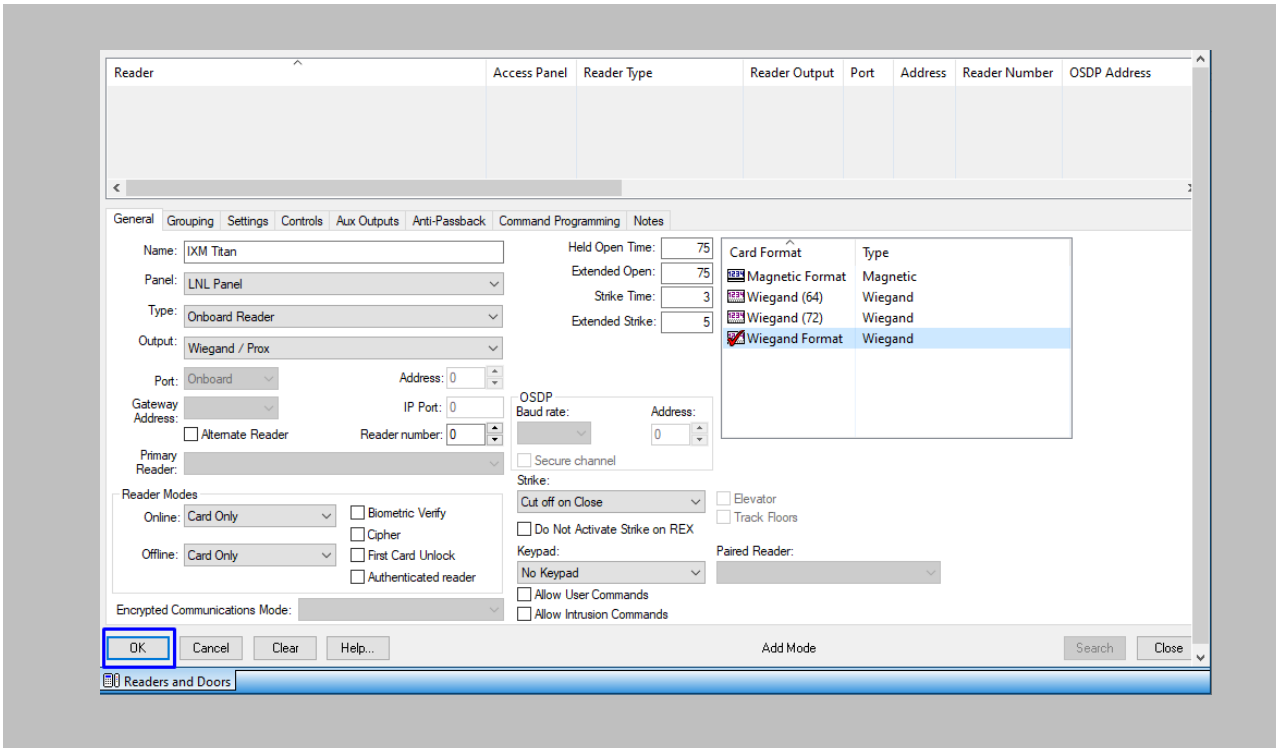


Figure 40: OnGuard - Reader Configuration

Note: Facility Code of the Card Format should be zero during Card Format configuration.

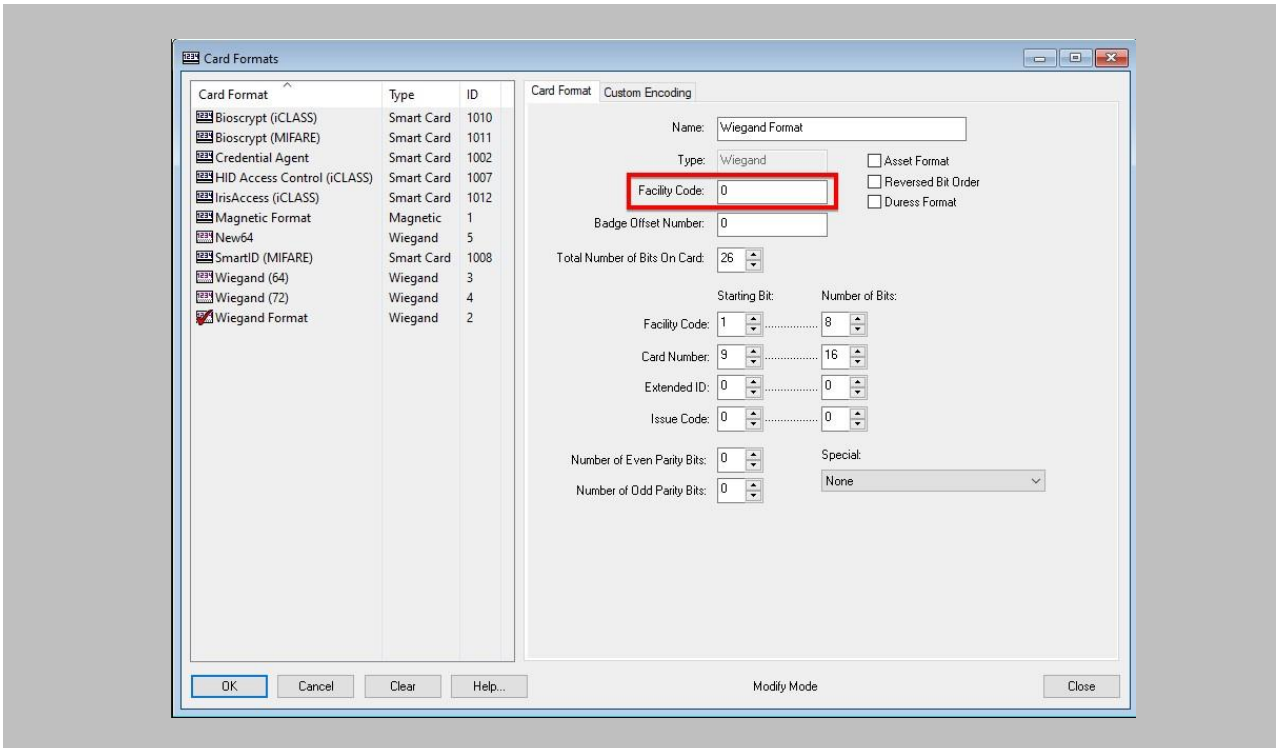


Figure 41: OnGuard – Facility Code

STEP 6

Click **Access Control** → **Access Levels.**

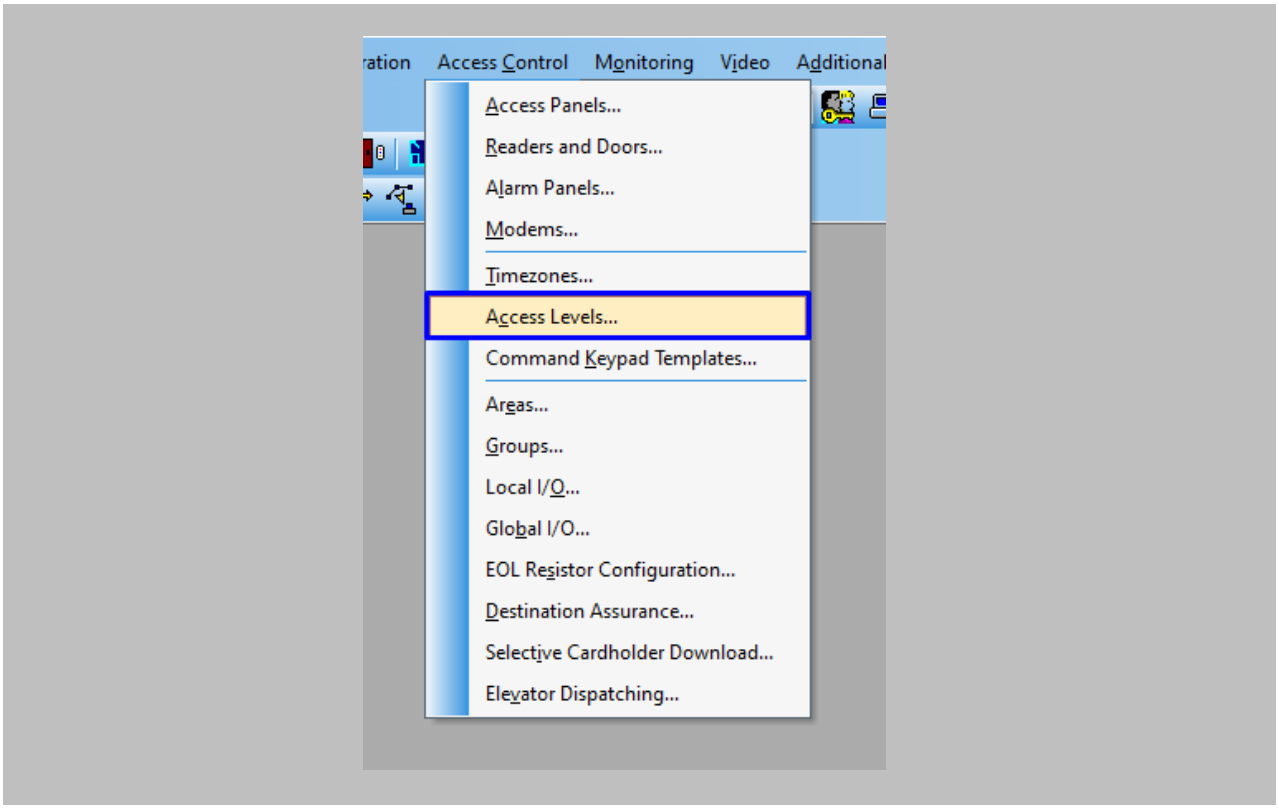


Figure 42: OnGuard - Access Level

STEP 7

Click on the **Add** button.

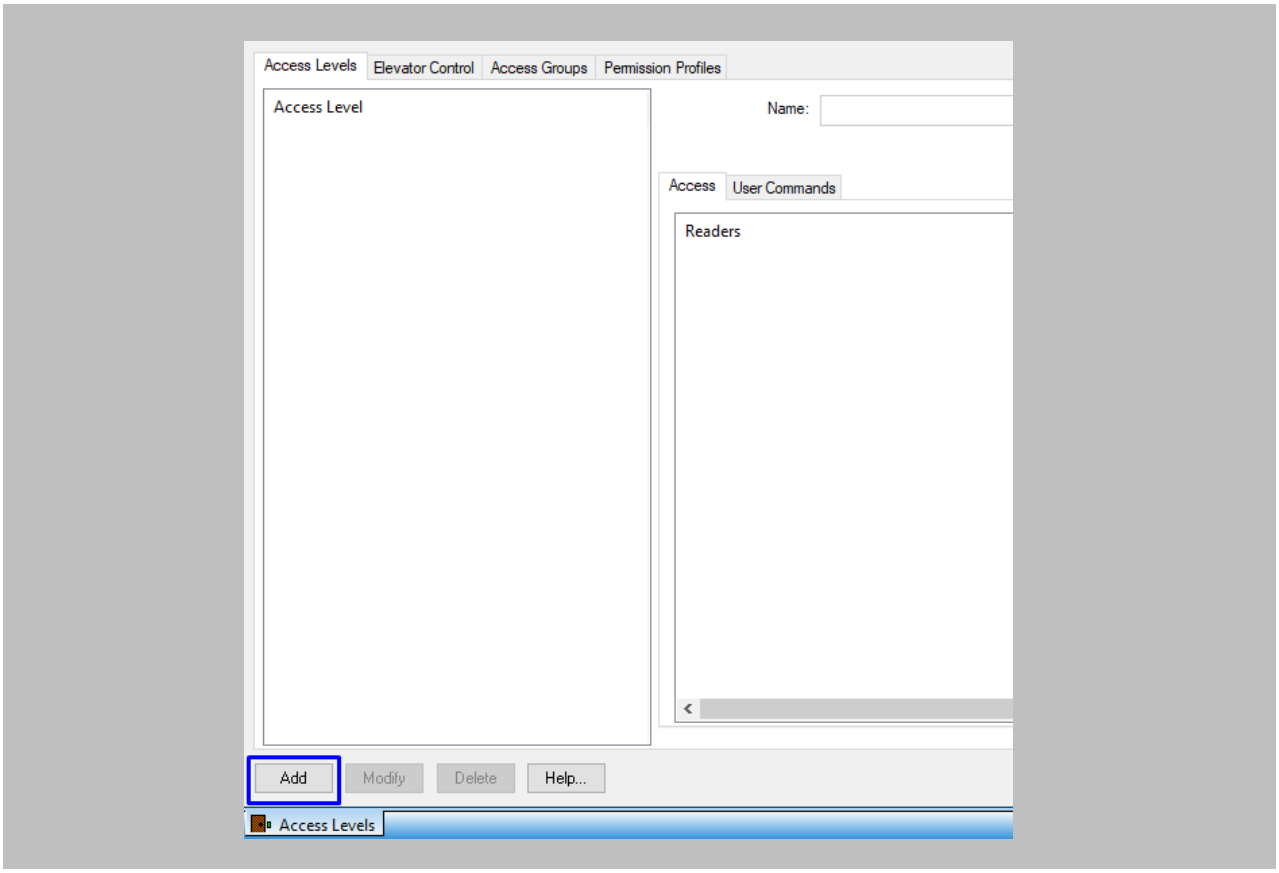


Figure 43: OnGuard - Add New Access Level

STEP 8

Define the Name of Access Level in the **'Name'** field → Select **'Reader'** and **'Timezone'** → Add to **Access Level.**

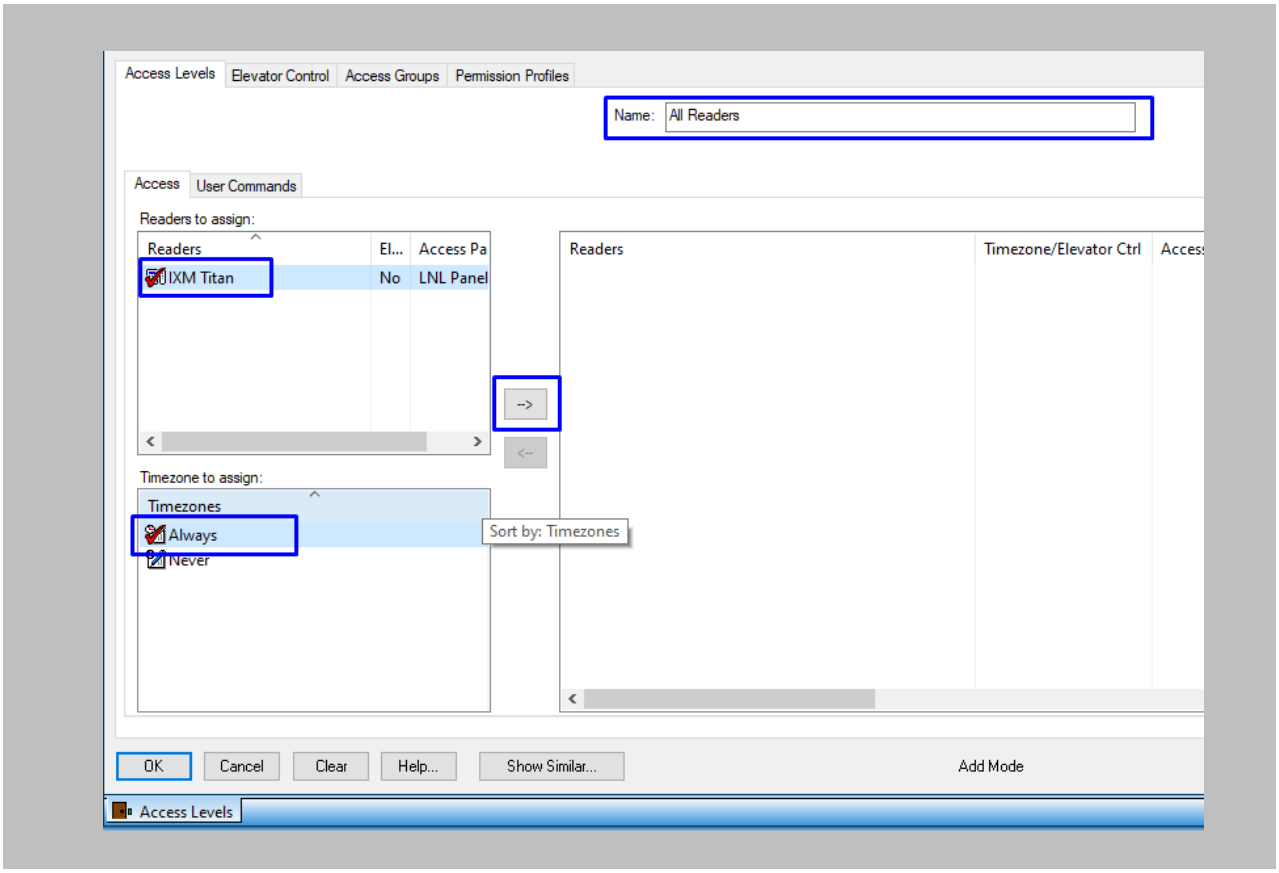


Figure 44: OnGuard - Add Reader to Access Level

STEP 9

Click **OK.**

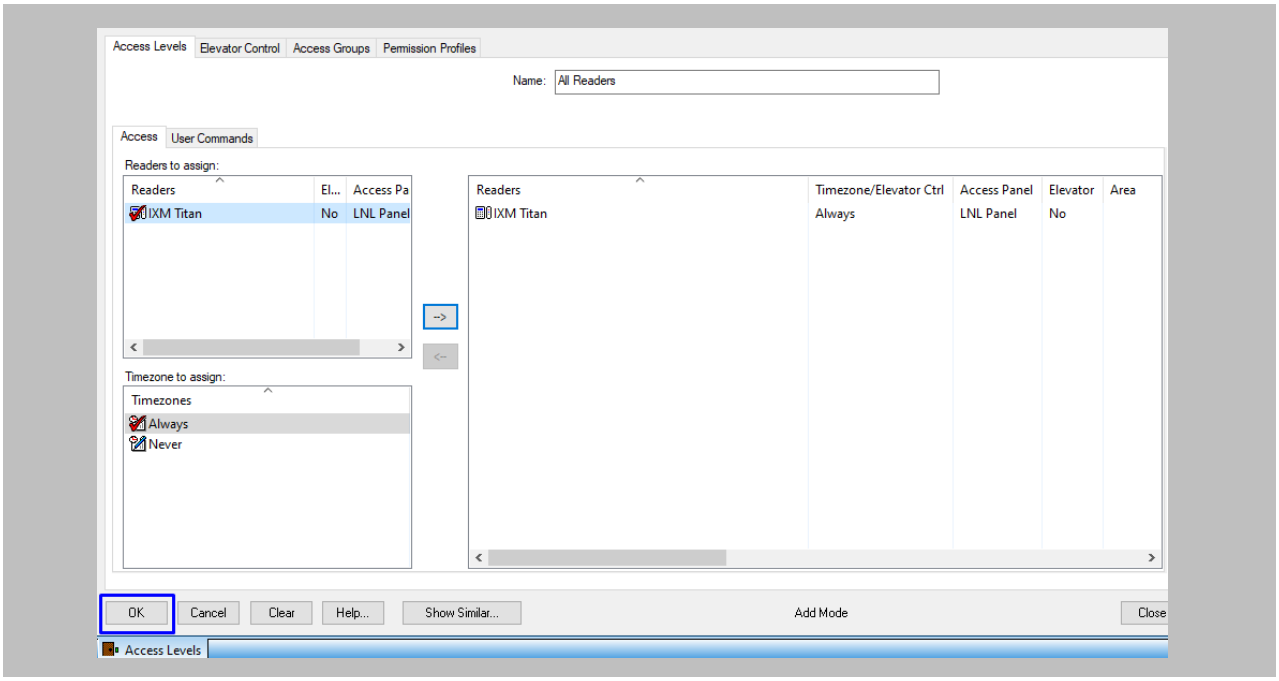


Figure 45: OnGuard - Access Level Configuration

RESULT

An Access Level will be created and the reader will be assigned to the Access Level.

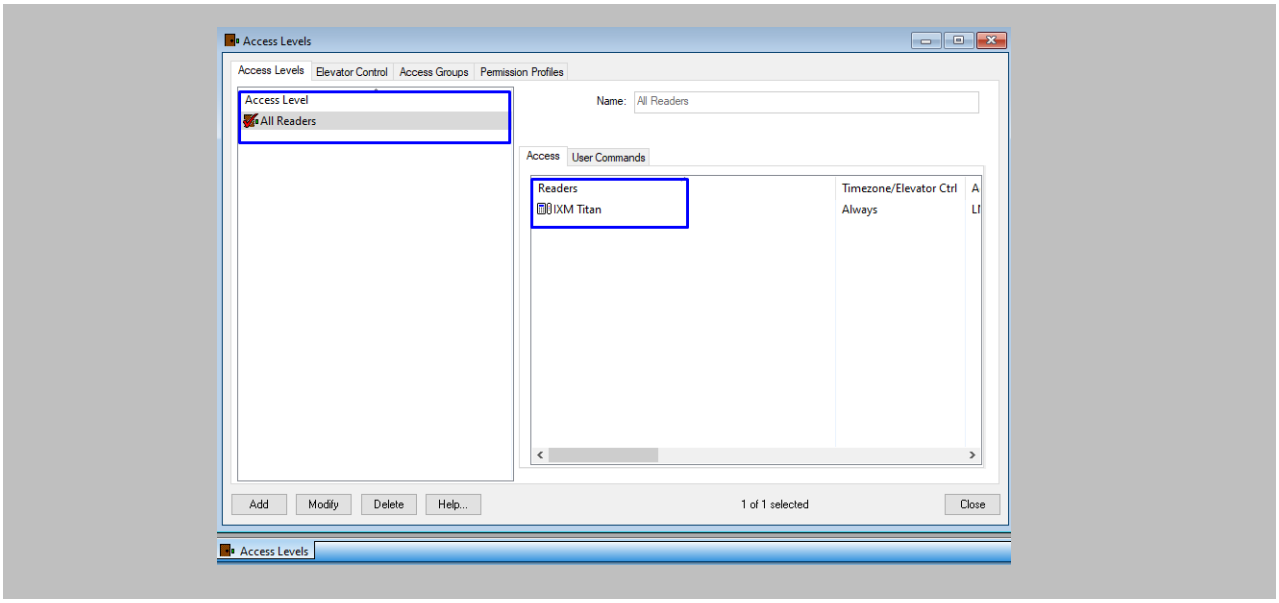


Figure 46: OnGuard - New Access Level

12. Add and Configure Invixium Readers

Adding Invixium Readers in the IXM WEB application

Note: Only Invixium devices with the 'Lenel OnGuard' category can be registered in IXM WEB.

Procedure

STEP 1

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

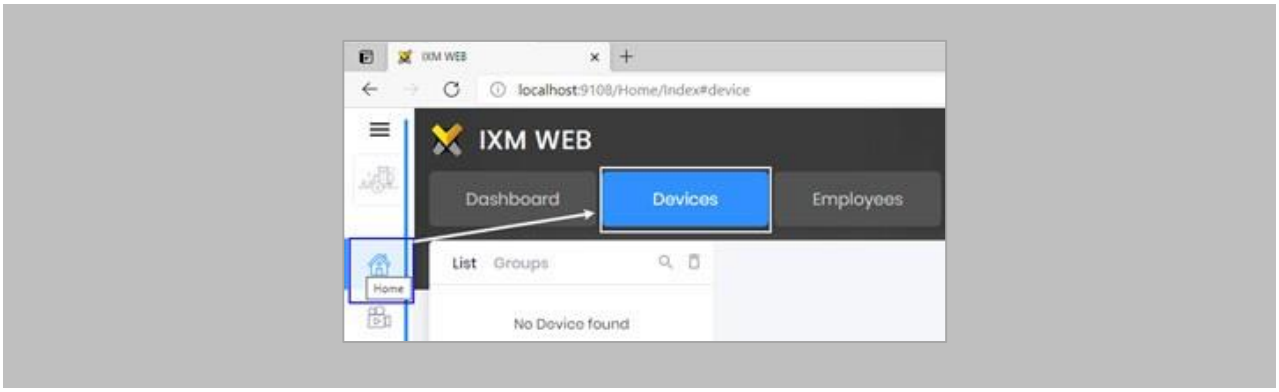


Figure 47: IXM WEB - Devices Tab

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.

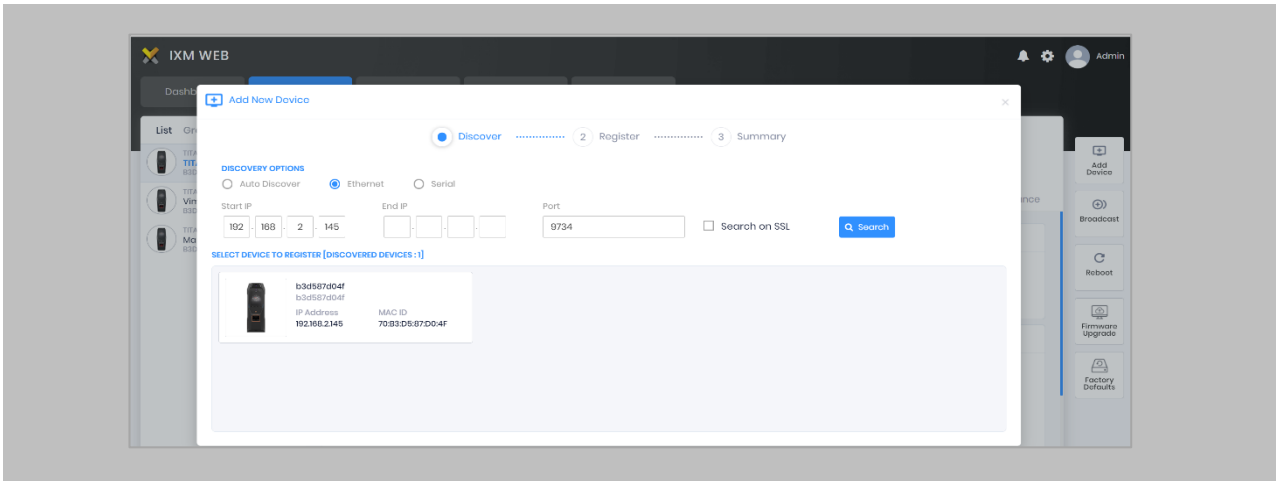


Figure 48: IXM WEB - Search Device using IP Address

STEP 3

Once the device is found, click on it. Enter the following details:

- **Device Name:** The name of the **device** in IXM WEB should be exactly the same as the name of the 'Reader' defined in '**System Administration'.** This will automatically add the device to the device group in IXM WEB based on Access Level mapping in **'System Administration'.**
- **Device Group:** Create a **'Default'** device group and select it.
- **Device Mode:** Select device mode as 'Entry', 'Exit', or 'Both' (Based on requirement).

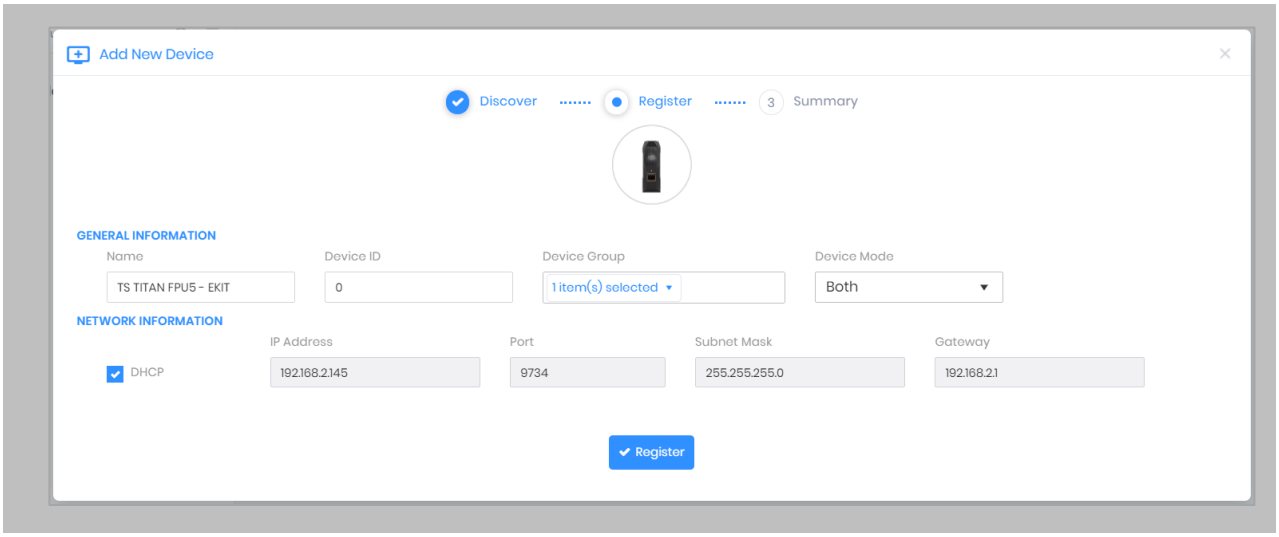


Figure 49: IXM WEB - Register Device

STEP 4

Click **Register**.

STEP 5

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

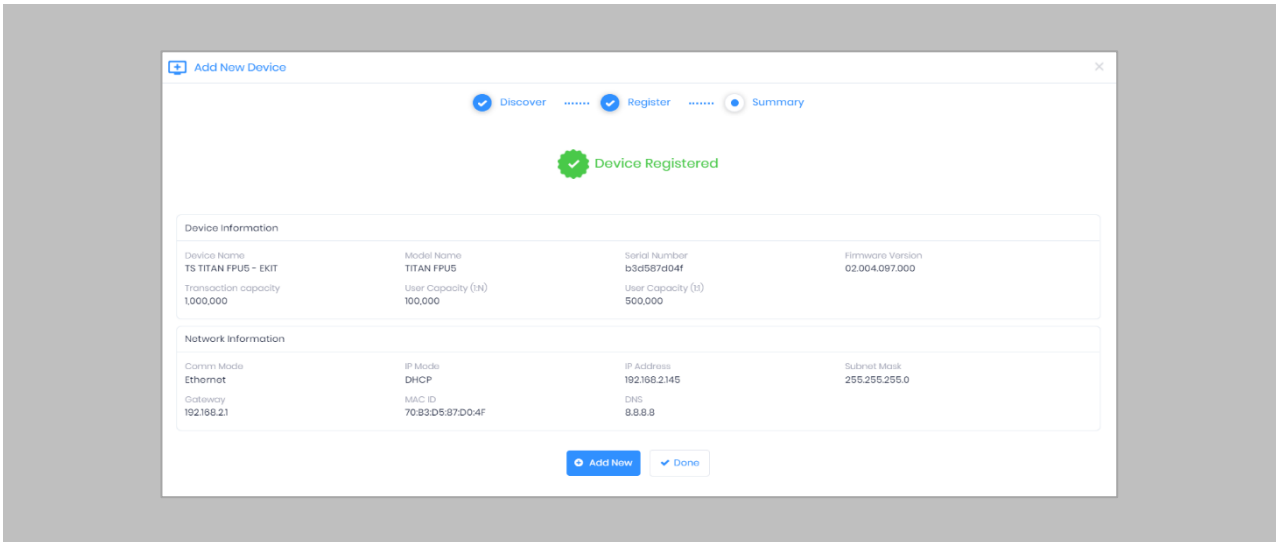


Figure 50: IXM WEB - Device Registration Complete

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

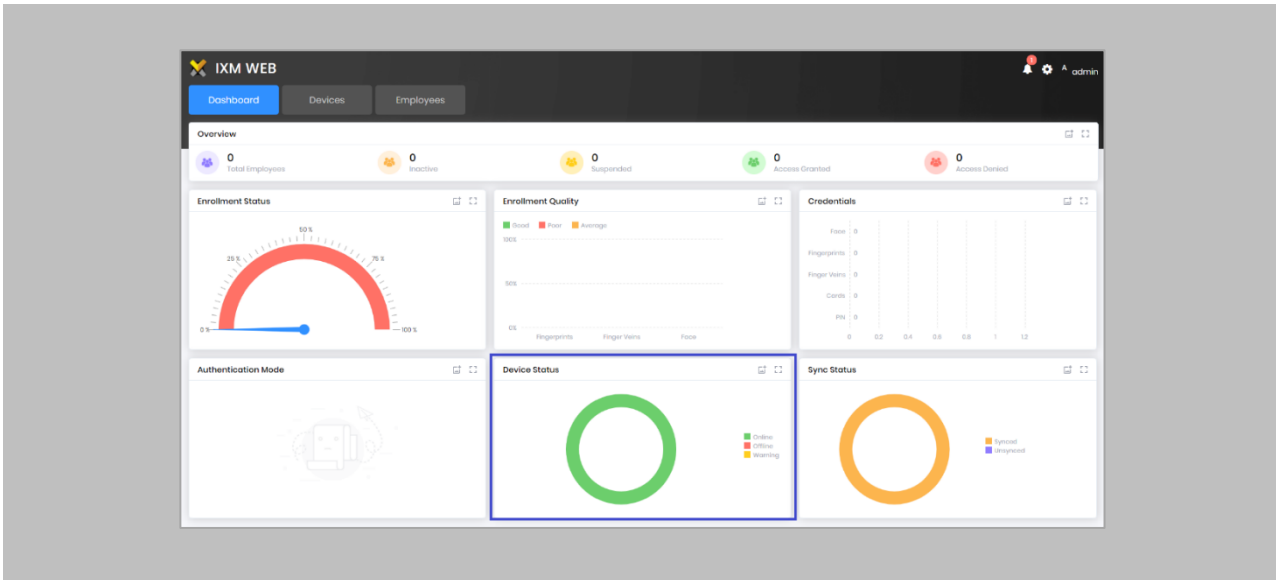


Figure 51: IXM WEB - Dashboard, Device Status

13. Adding Invixium Device to a Device Group

Note: Turn OFF the ‘Map Access Level To User Group’ setting from the Link Configuration page to use this feature.

Procedure

STEP 1

Go to **Devices** → **Groups**.

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

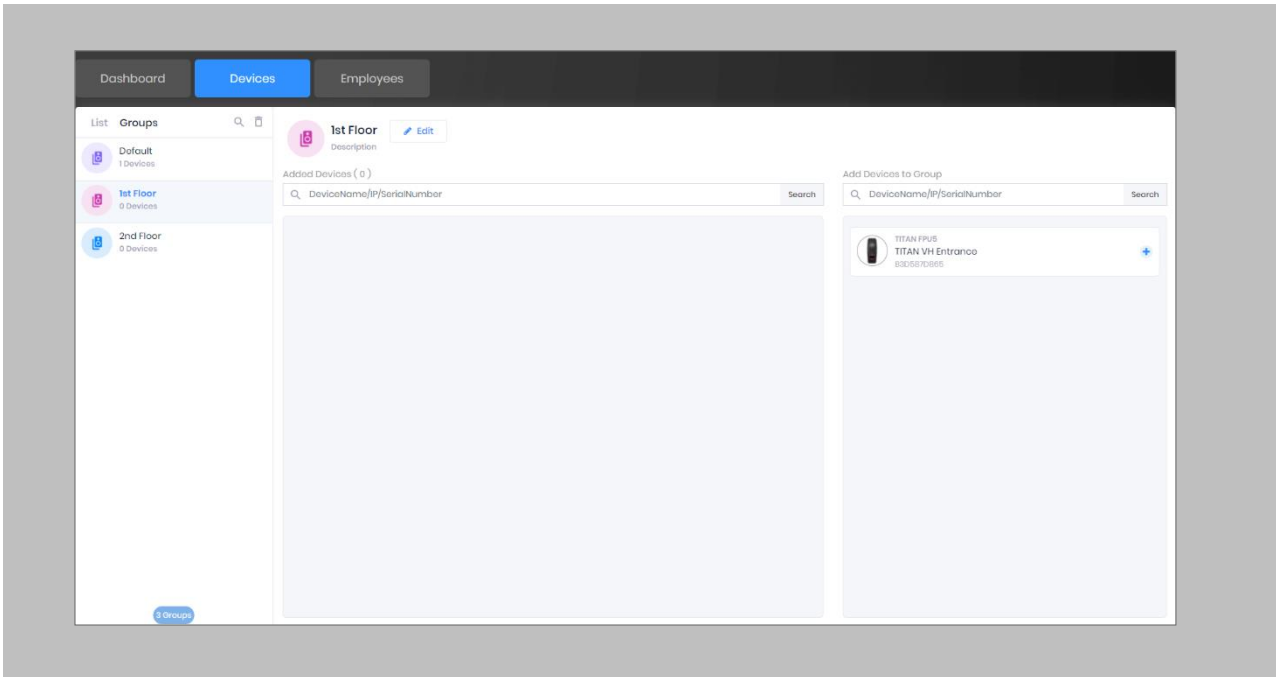


Figure 52: IXM WEB - Assign Device Group

Assign Wiegand to Invixium Readers

Note: Face and finger will always give a Wiegand output based on the initial card that was synced from LenelS2 to Invixium.

The Standard 26 Bit Wiegand will be used to define which output format will be sent to OnGuard.

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.

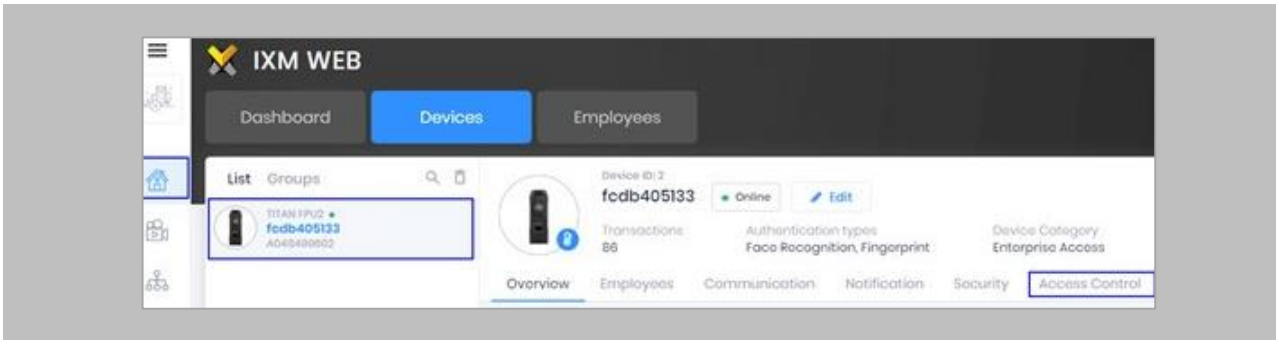


Figure 53: IXM WEB – Navigate to Access Control Tab

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.

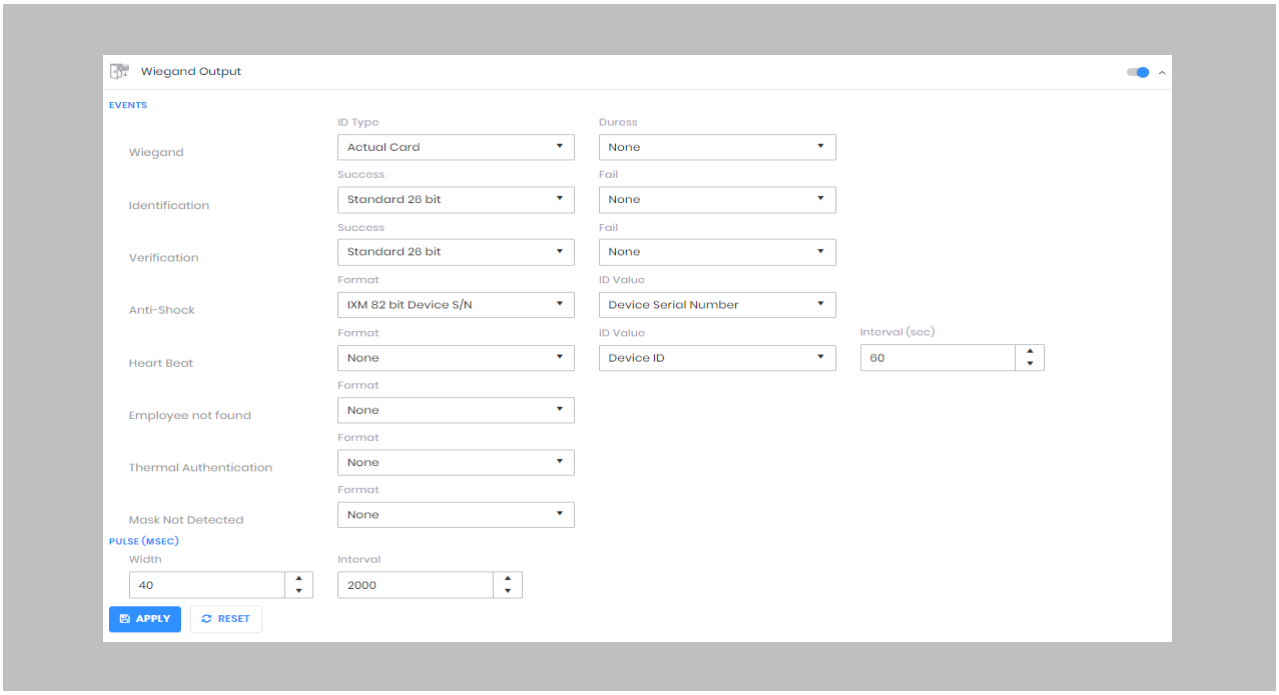


Figure 54: IXM WEB - Wiegand Output

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 OnGuard, 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 Invixium Device.

Default Card: It will generate Wiegand output data for the default card marked in IXM WEB.

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

STEP 4

Set the **items**:

Wiegand	Actual Card
Identification	26 - bit
Verification	26 - bit

STEP 5

Click **Apply.**

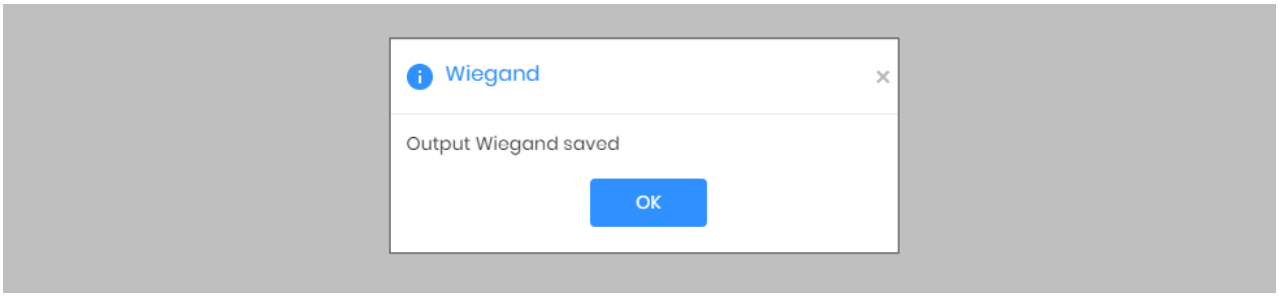


Figure 55: IXM WEB - Save Output Wiegand

RESULT

The Wiegand Output settings of the device selected 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 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 OnGuard Panel.

Configuring Panel Feedback with Lenel

Procedure

STEP 1

Connect Wiegand Data D0 of LenelS2 Panel with **WDATA_OUT0** of IXM device, Wiegand Data D1 of LenelS2 Panel with **WDATA_OUT1** & Wiegand Ground of LenelS2 Panel with WGND of the IXM Device.

STEP 2

Connect the **LED** of LenelS2 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**.

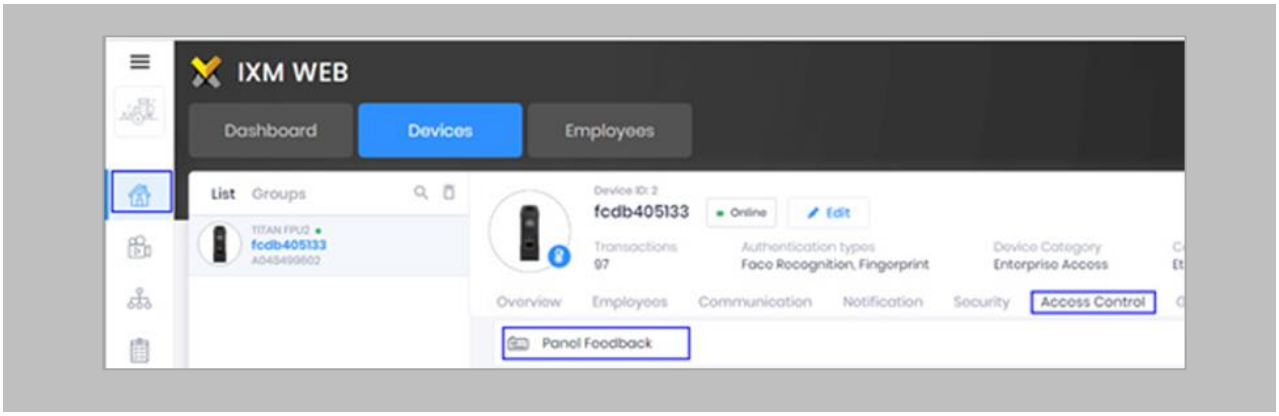


Figure 56: IXM WEB - Panel Feedback

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**.

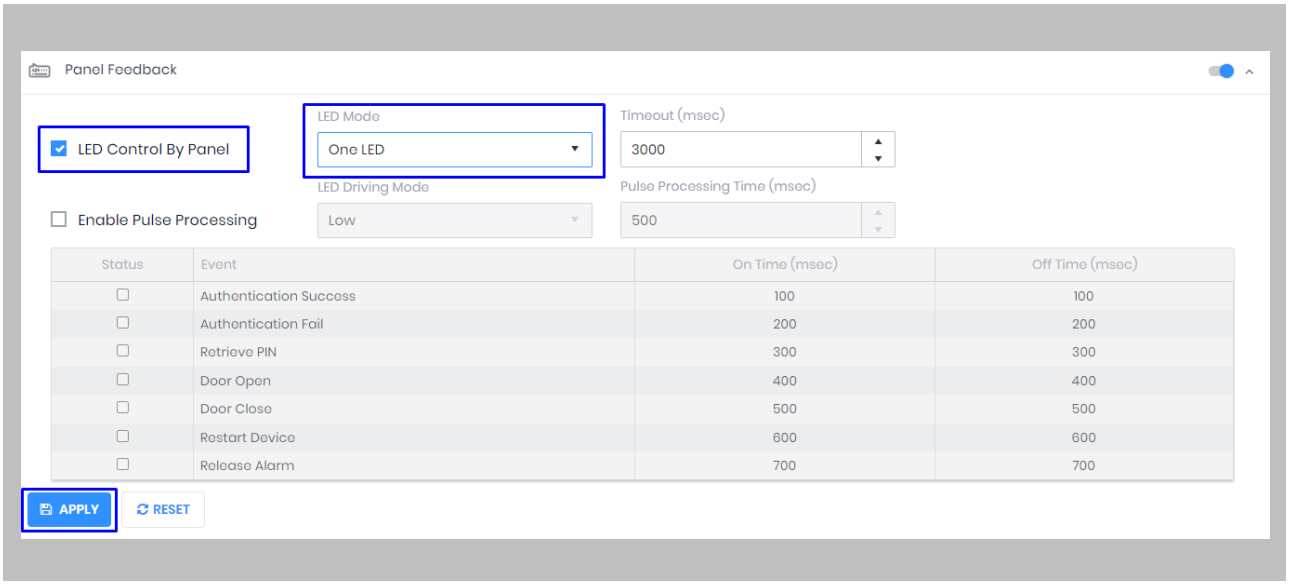


Figure 57: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.

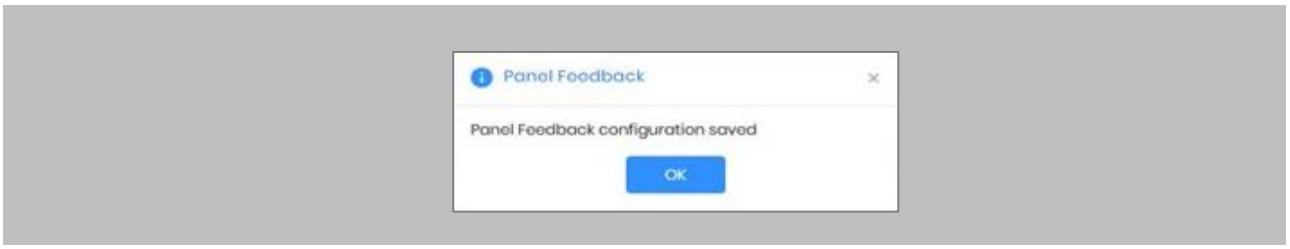


Figure 58: IXM WEB - Save Panel Feedback

Configuring Thermal Settings

Note: Confirm if 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.

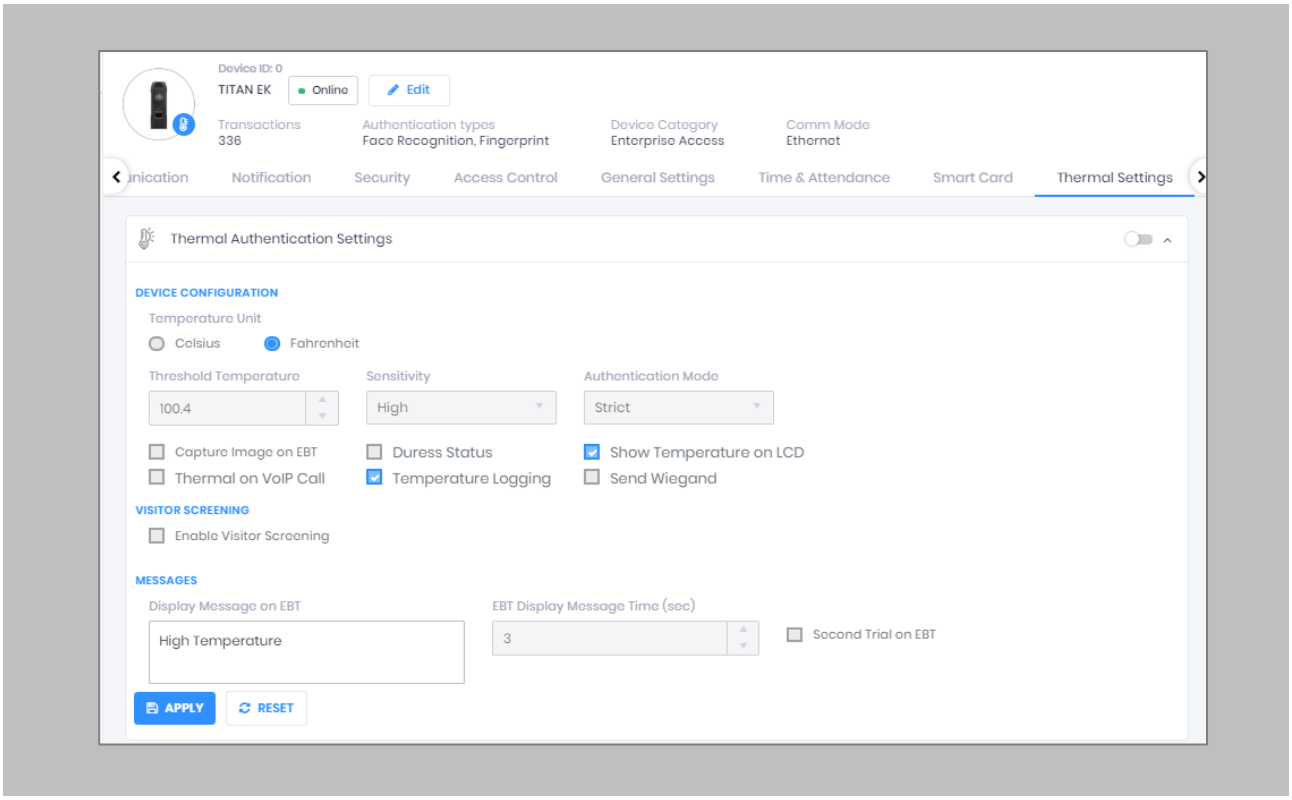


Figure 59: IXM WEB - Thermal Settings

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 choice will be Fahrenheit.

- **Threshold Temperature:** Users can set a threshold temperature. Elevated Body Temperature (EBT) workflows will trigger when any user'stemperature 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:** Users will have two options for the mode of authentication, Soft orStrict. This mode of authentication is used to control the access of the user if a fever is detected. The default mode of authentication is Strict.

    - **Soft:** Access will be granted to the end-user even after a 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:** Enabling this setting gives users a notification to retry after EBT detection. If this setting is enabled, the 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 stays disabled.
- **Visitor Screening Message:** Users can set a message that will be displayed when a visitor is showing their face. A maximum of 50 characters is allowed.
- **Visitor Screening Message on EBT:** Users can set a message that will be displayed when a 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 stays disabled.
- **Temperature Logging:** This setting keeps logsof detected temperature in the Transaction Log. By default, this field stays enabled. Users can disable this feature using IXM WEB only. Enable/Disable this setting is not available on the LCD.

STEP 3

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

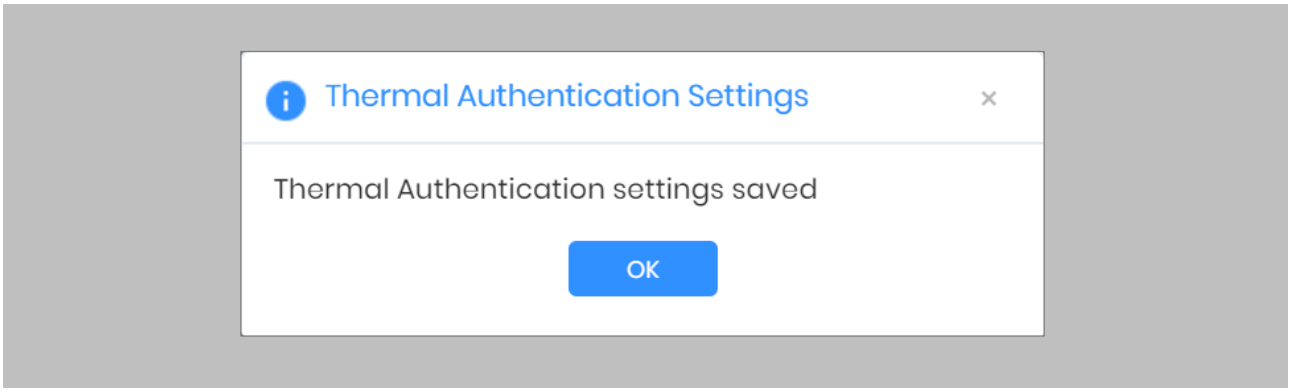


Figure 60: IXM WEB - Save Thermal Settings

Thermal Calibration

Procedure

STEP 1

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

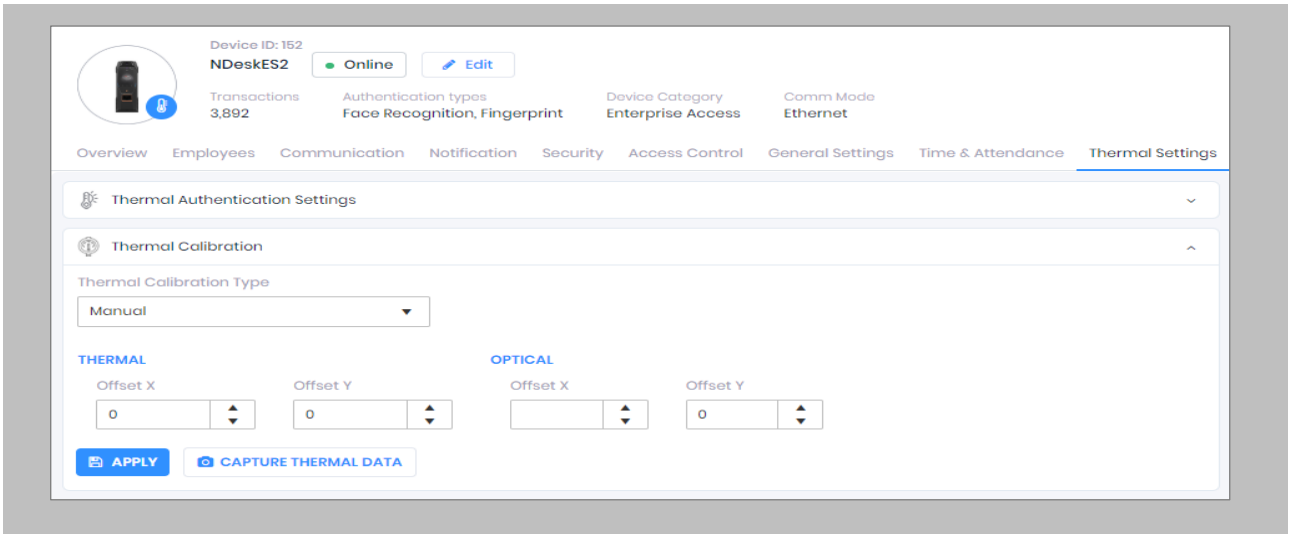


Figure 61: IXM WEB - Thermal Calibration Settings

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**.

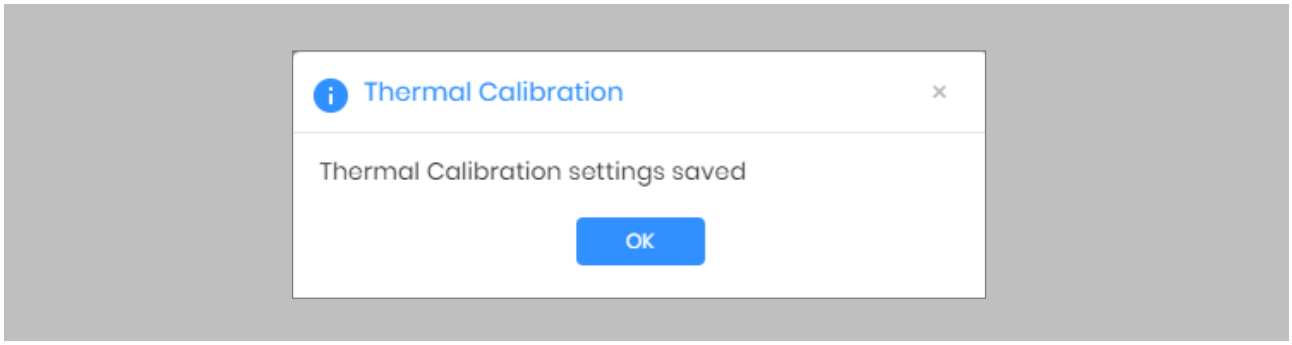


Figure 62: IXM WEB - Save Thermal Calibration Settings

To provide 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.

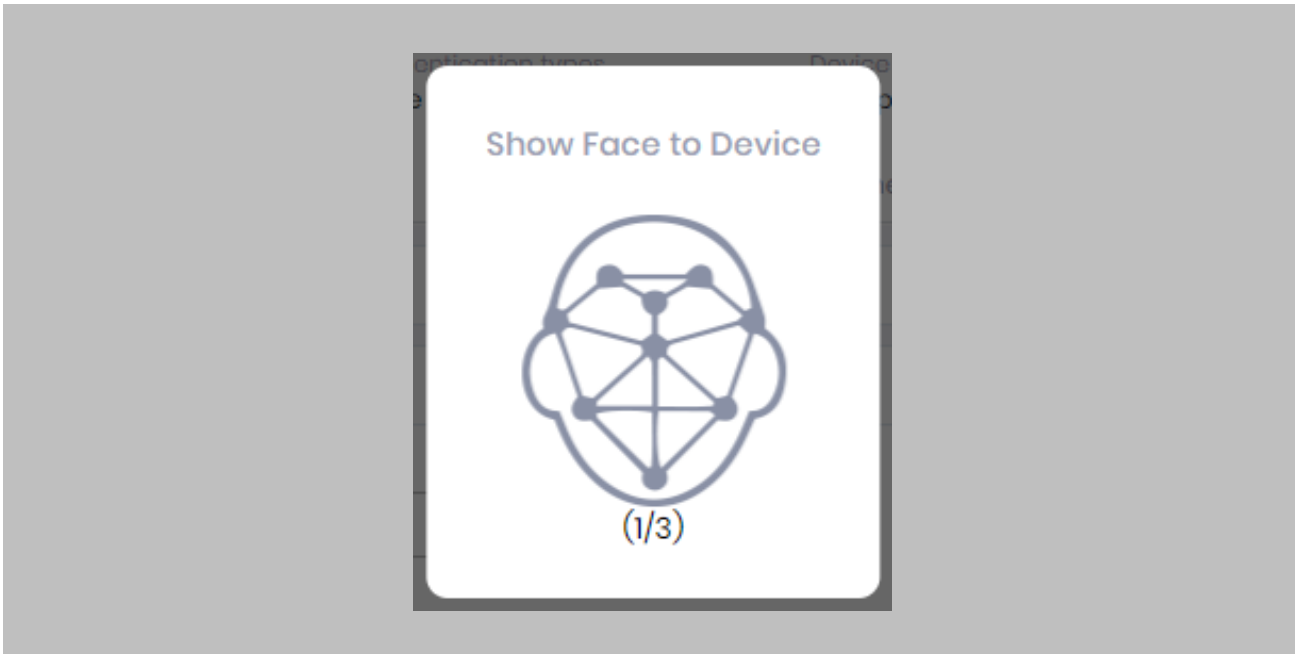


Figure 63: IXM WEB - Capture Thermal Data

STEP 4

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

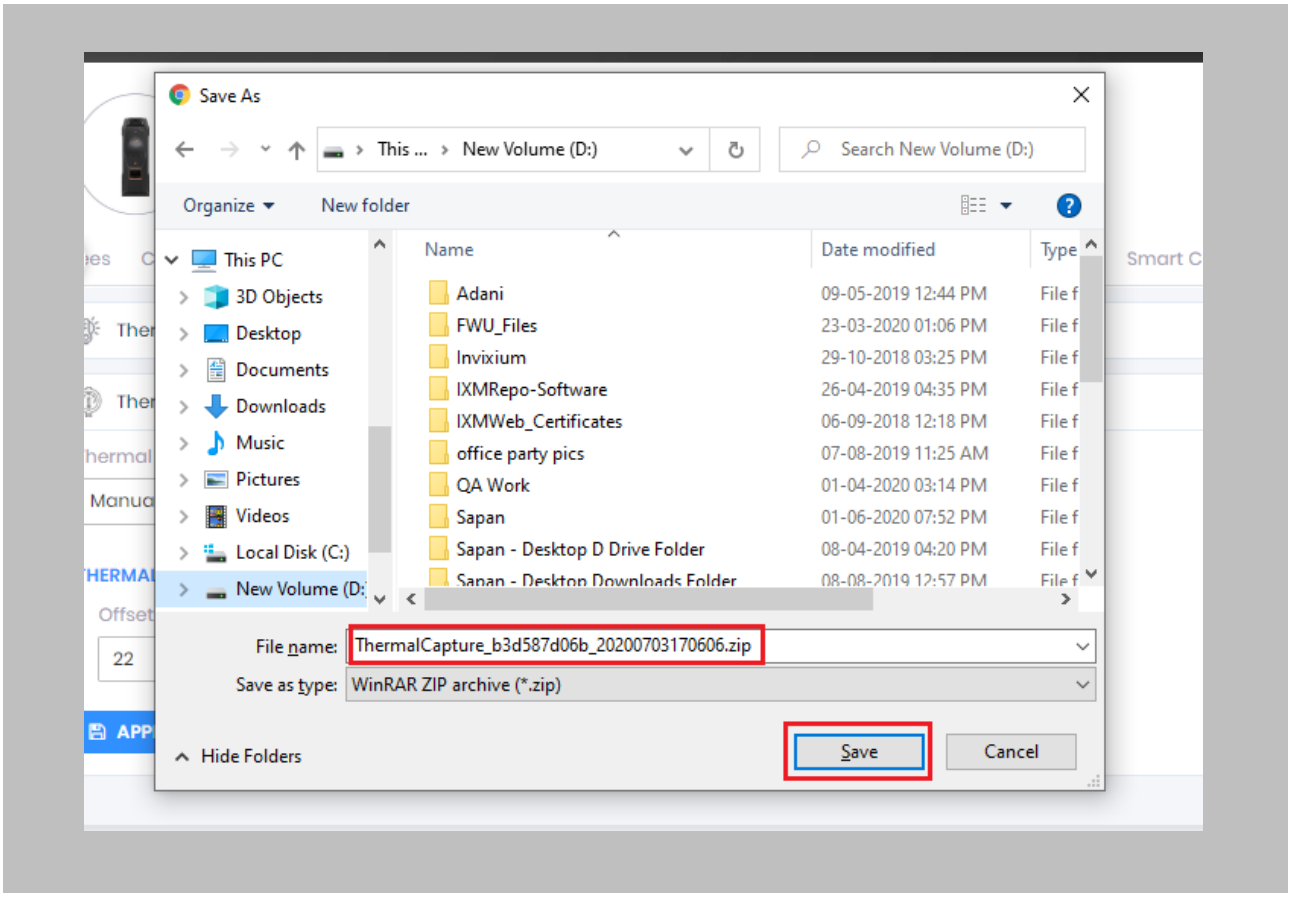


Figure 64: IXM WEB - Save Captured Thermal Data

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's camera.

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

Test Calibration Options

To test Thermal Calibration click Test Calibration.

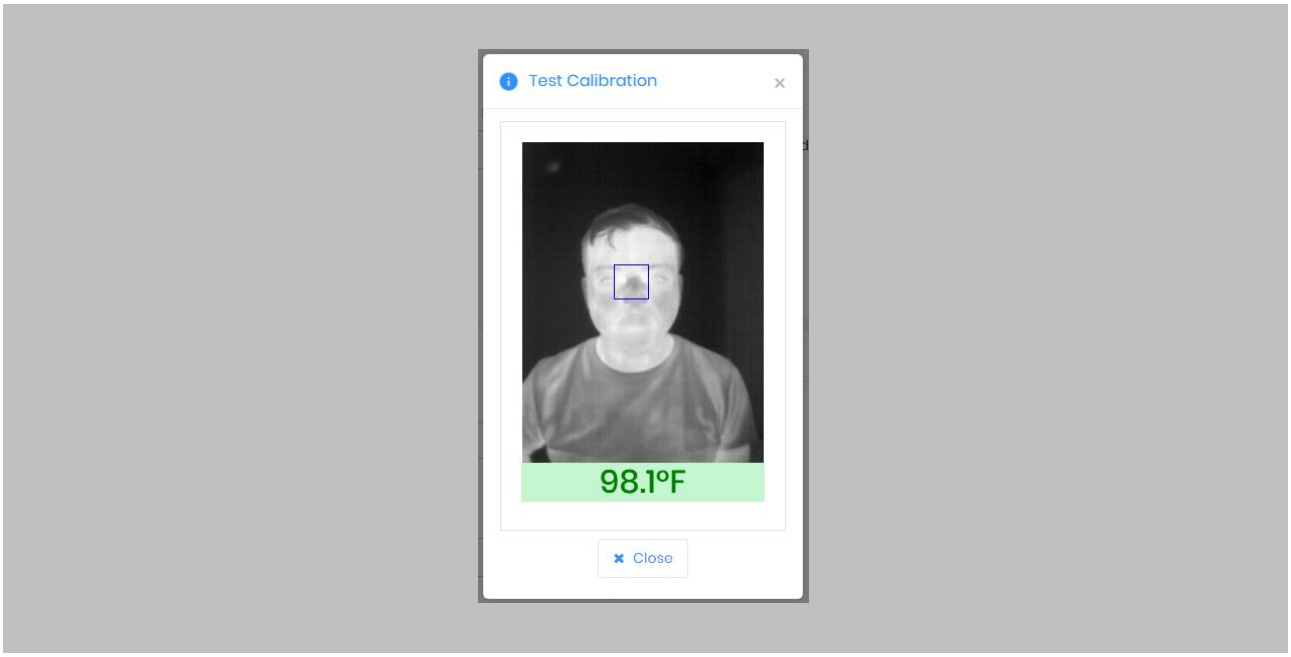


Figure 65: IXM WEB - Test Thermal Calibration

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 Celcius to Fahrenheit and vice-versa, click **Tools** → **Options** → **Manage Preferences**.

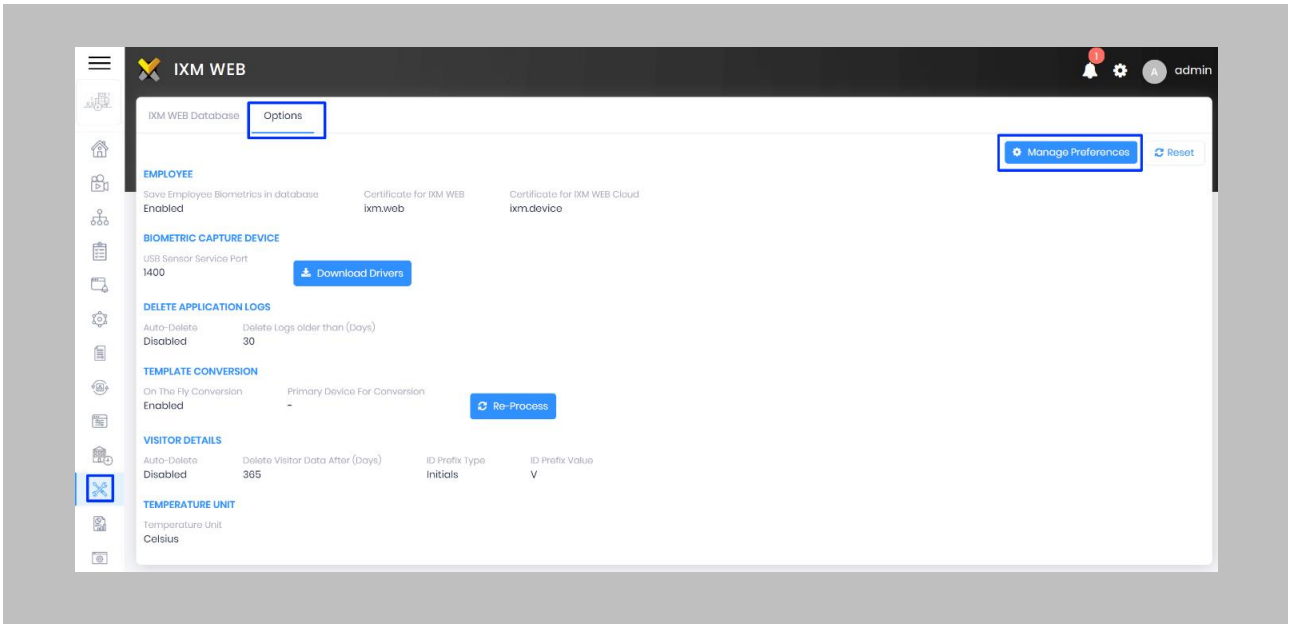


Figure 66: IXM WEB - Option to change Temperature unit.

STEP 2

Click **Save**.

Note: The Temperature Test failure event in OnGuard Alarm Monitoring will show the Temperature Value as per the Temperature Unit selection.

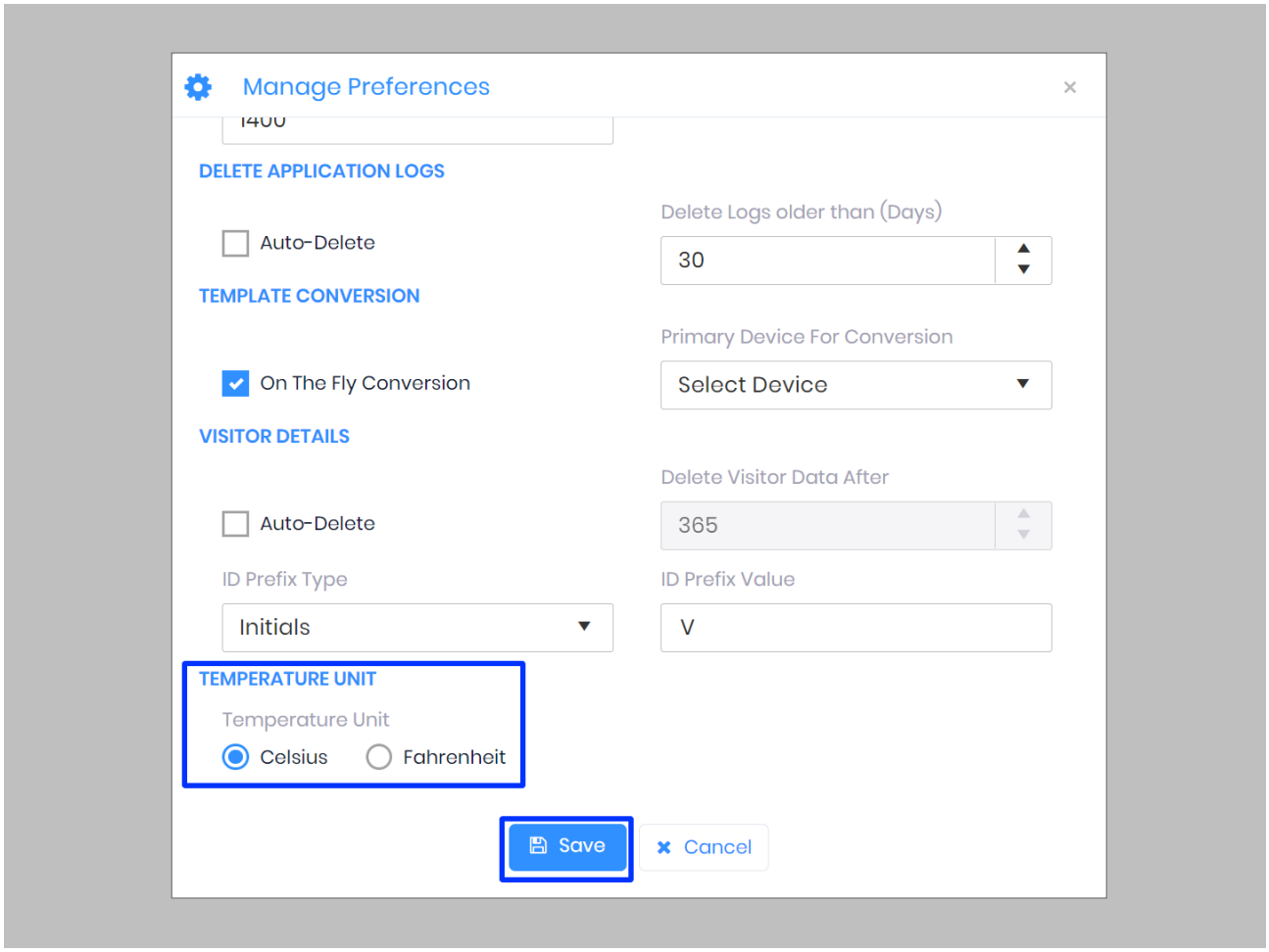


Figure 67: IXM WEB - Save Temperature Unit Setting

Configuring Mask Authentication Settings

STEP 1

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

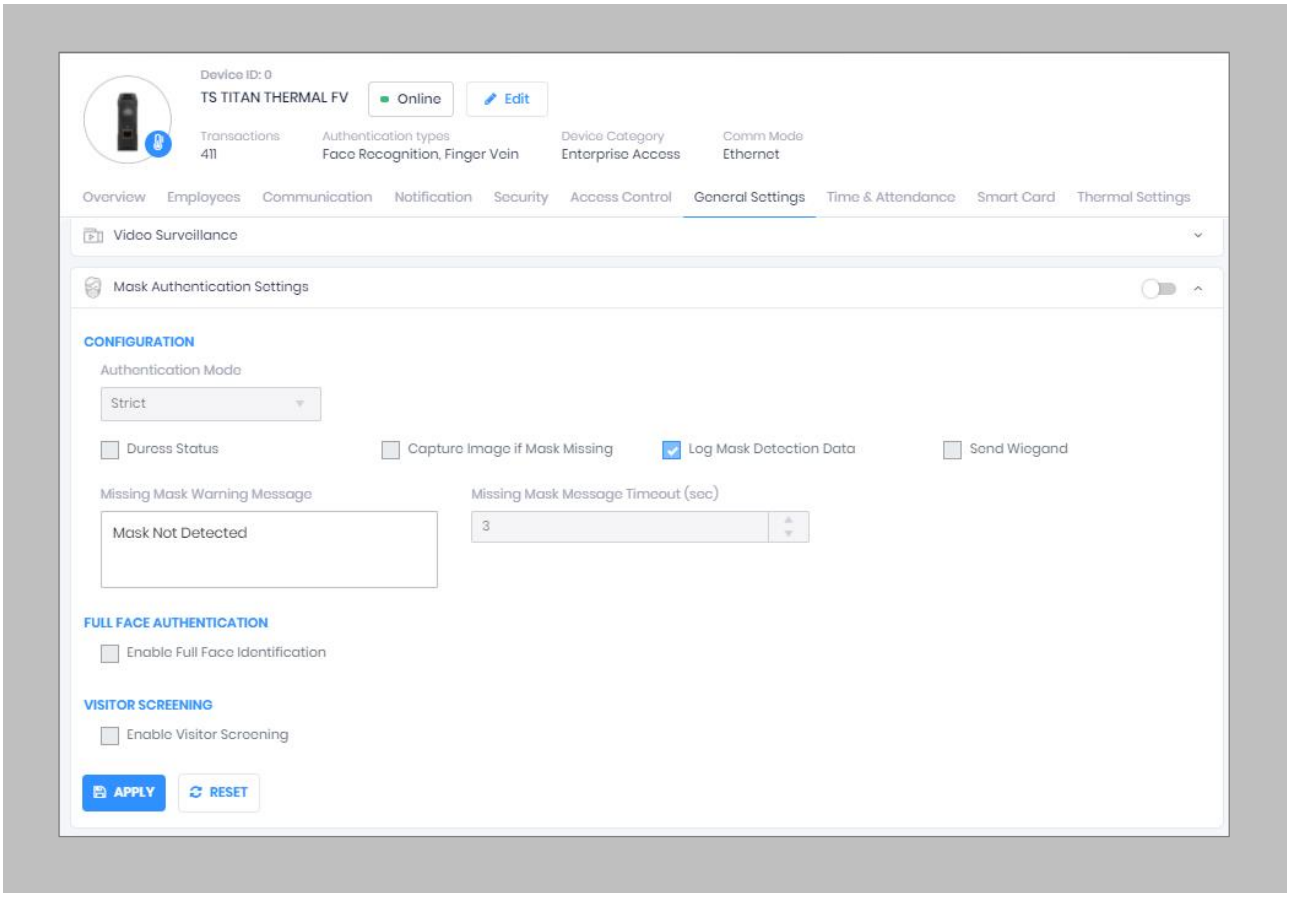


Figure 68: IXM WEB - Mask Authentication Settings

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 is 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**.

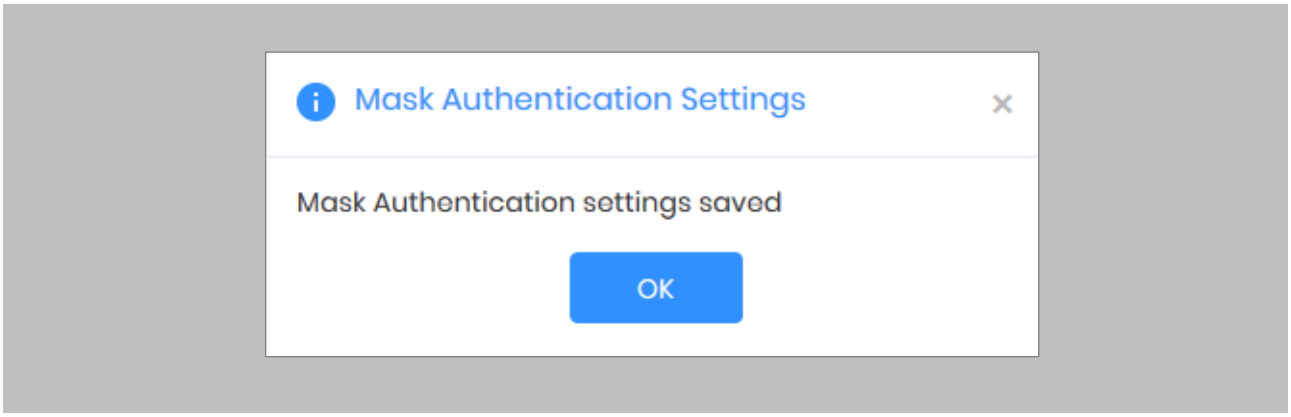


Figure 69: IXM WEB - Save Mask Settings

Pre-Configuration for Enrollment

Procedure

STEP 1

From the **Left Navigation Pane** → **Link** → click the red **OnGuard (Lenel-S2)** icon →Click **Download Add-on**

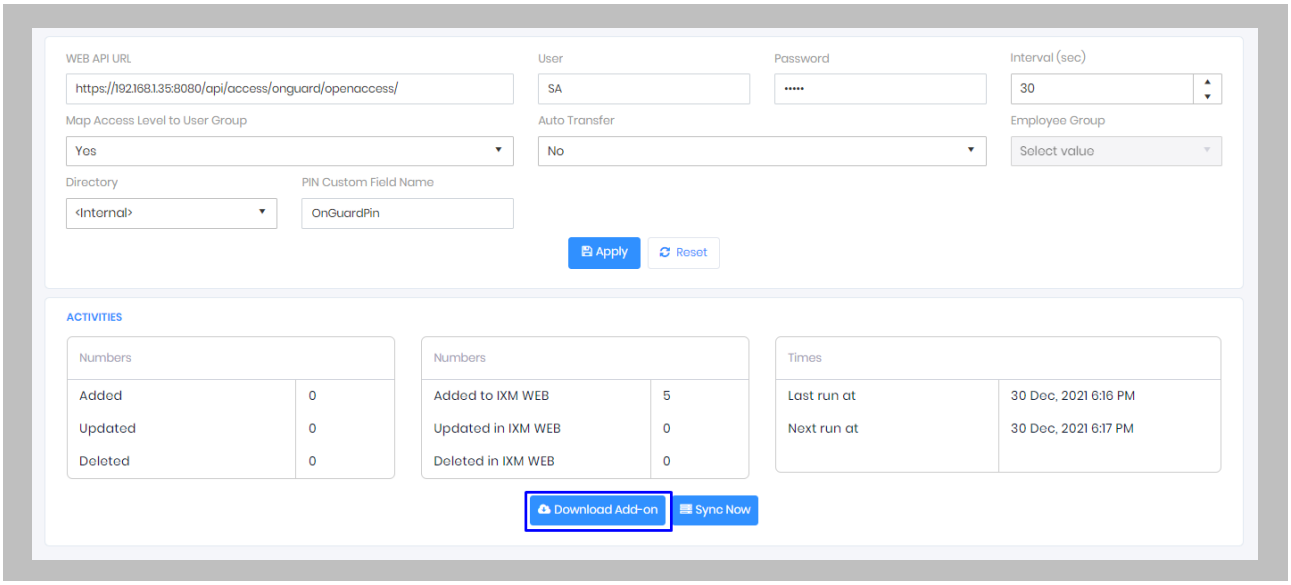


Figure 70: IXM WEB - Download Enrollment Add-On

OnGuard Add-On.zip file will be downloaded at the default download location (i.e., C:\Users\Downloads)

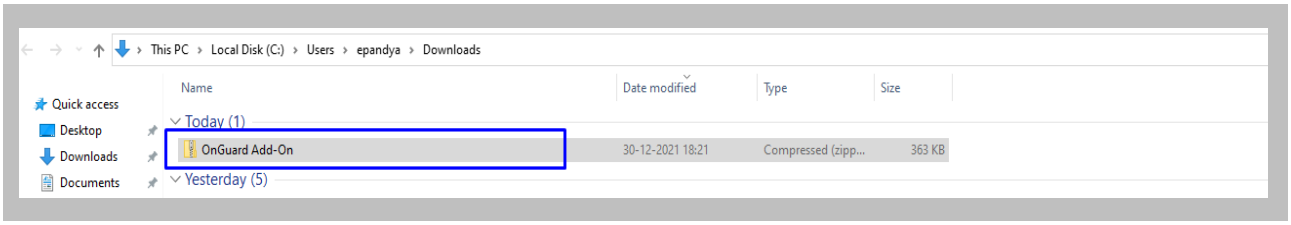


Figure 71: IXM WEB - Download Add-On Zip File

STEP 2

Extract the **OnGuard Add-On**.

STEP 3

Click on the extracted **OnGuard Add-On** folder → Copy the path of the **Enrollment.exe** file.

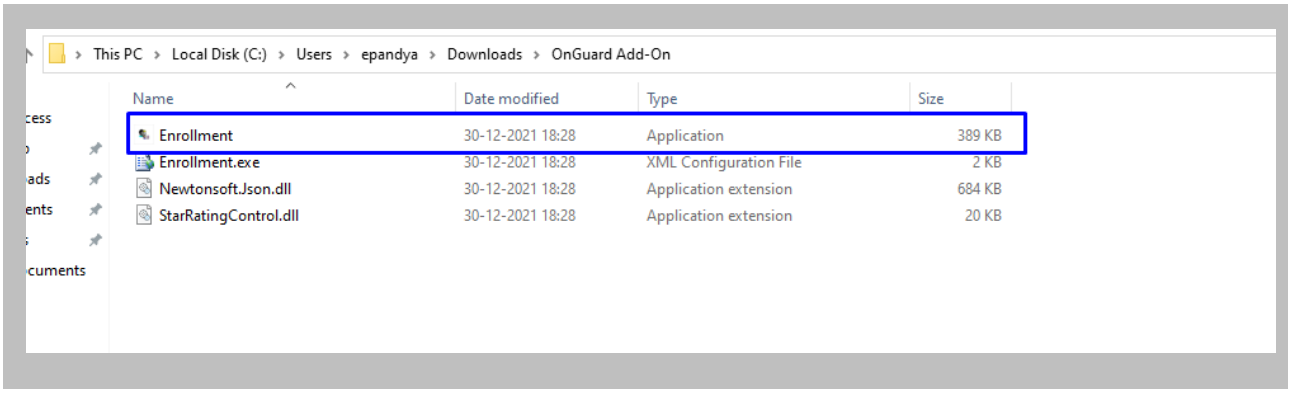


Figure 72: IXM WEB - OnGuard Add-On Enrollment.exe

STEP 4

Open **System Administration** → Click **Administration** → **Workstations.**

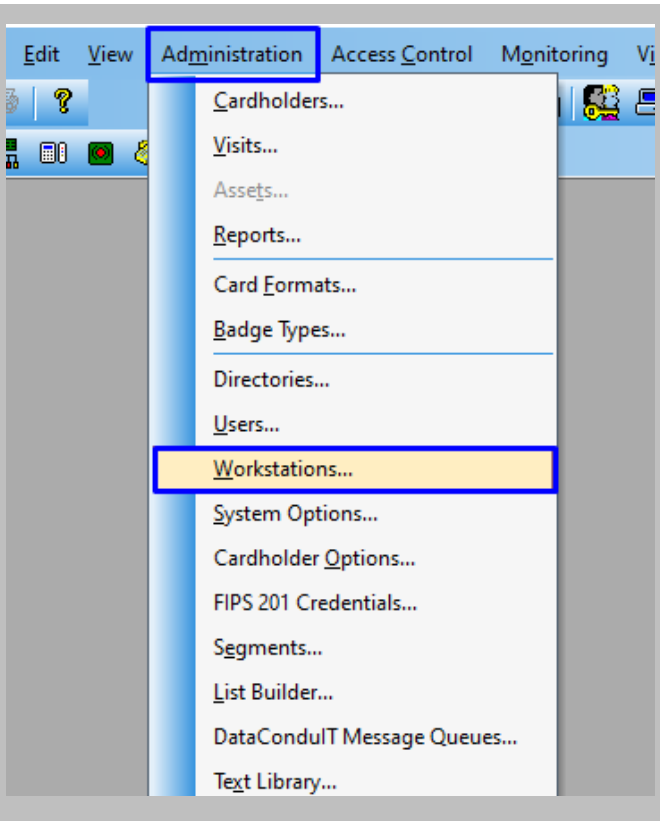


Figure 73: OnGuard - Workstation

STEP 5

Click **Modify** for the existing Workstation.

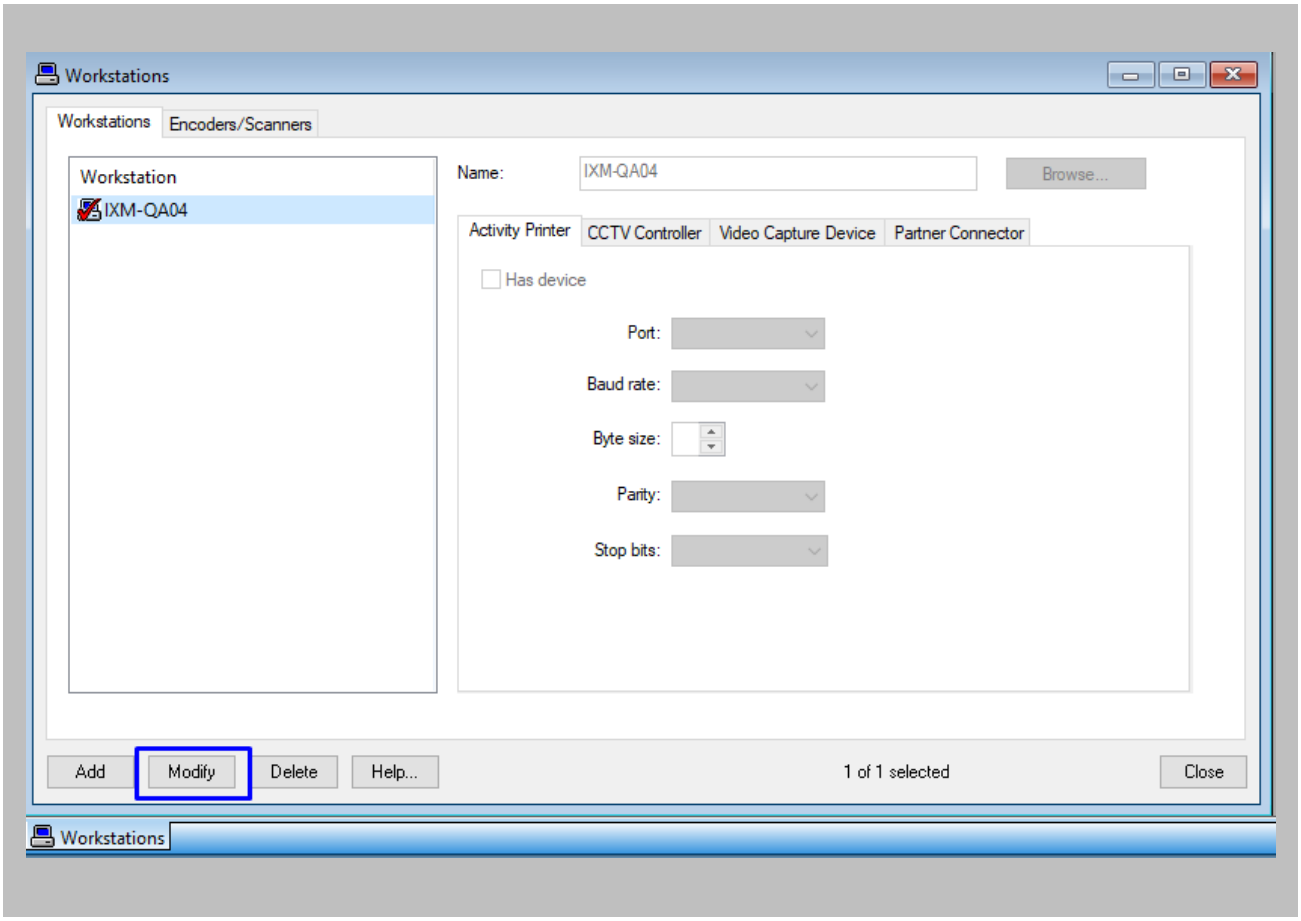


Figure 74: OnGuard - Modify Workstation

STEP 6

Click **Partner Connector.**

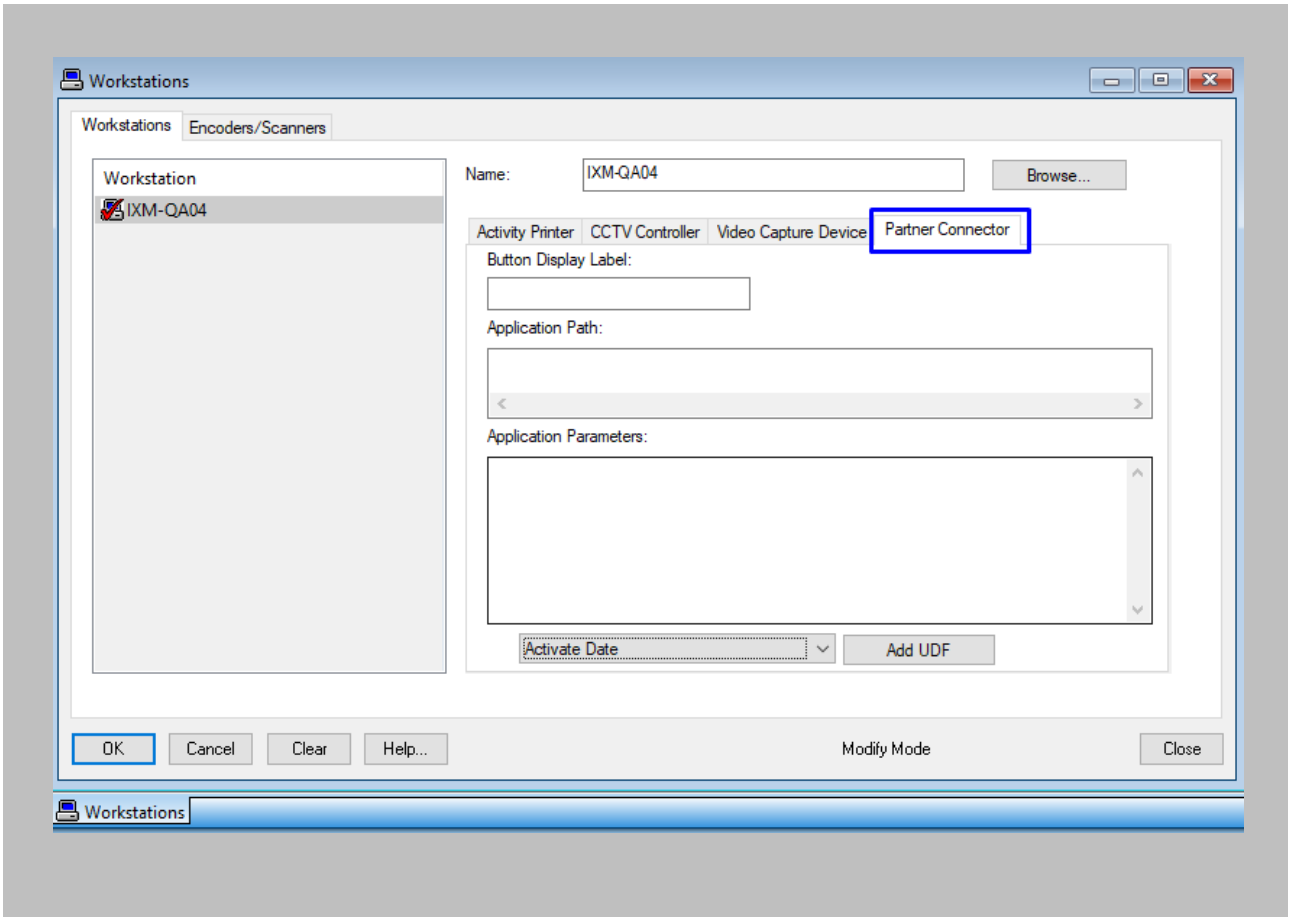


Figure 75: OnGuard - Partner Connector

STEP 7

Enter the Following Details:

- **Button Display Label:** Define the **enrollment** addon button name.
- **Application Path:** Paste the file path of **Enrollment.exe**.
- **Application Parameters:** Click on the dropdown → Find 'EMP.ID' in the list and select → Click on **Add UDF** button.

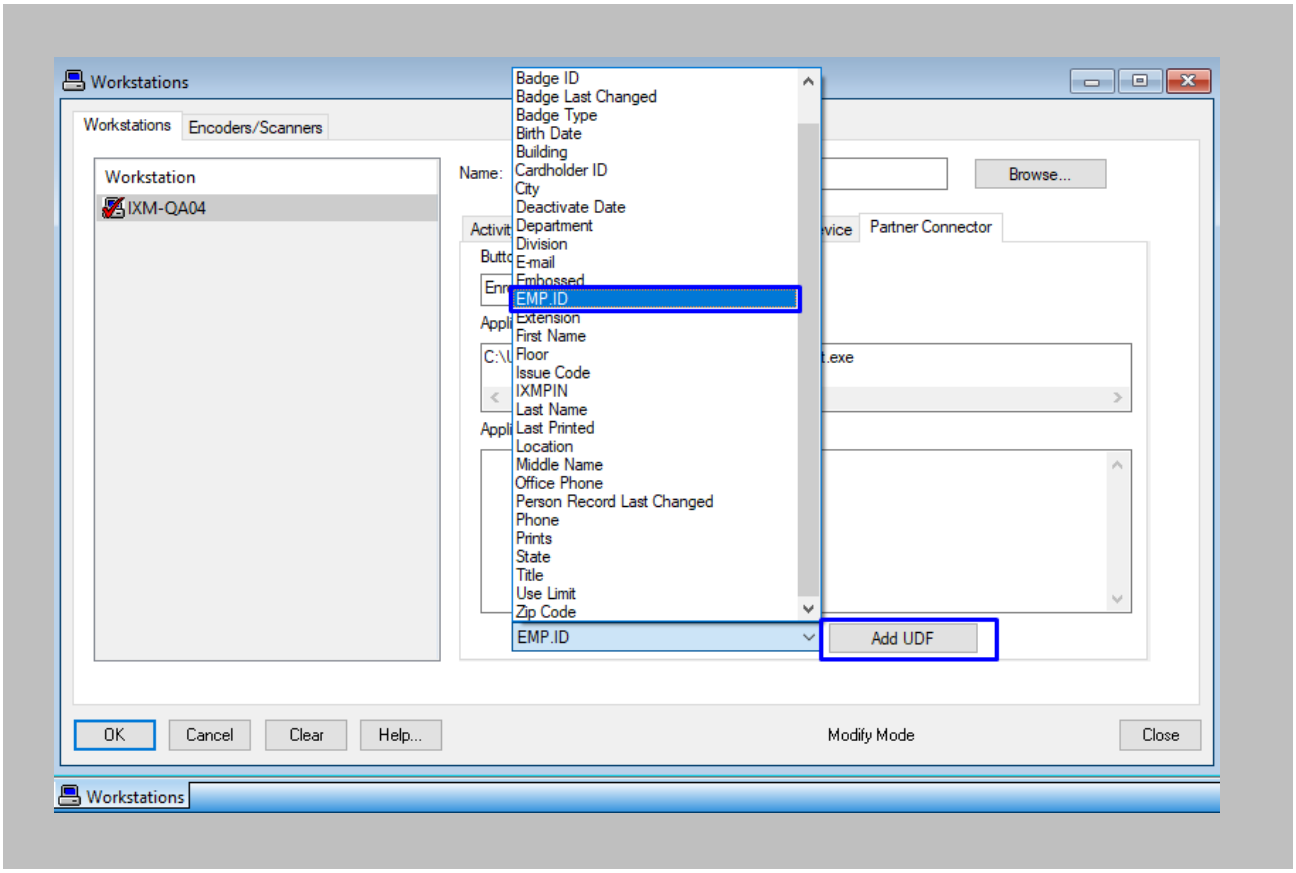


Figure 76: OnGuard - Add UDF

STEP 8

Click **OK.**

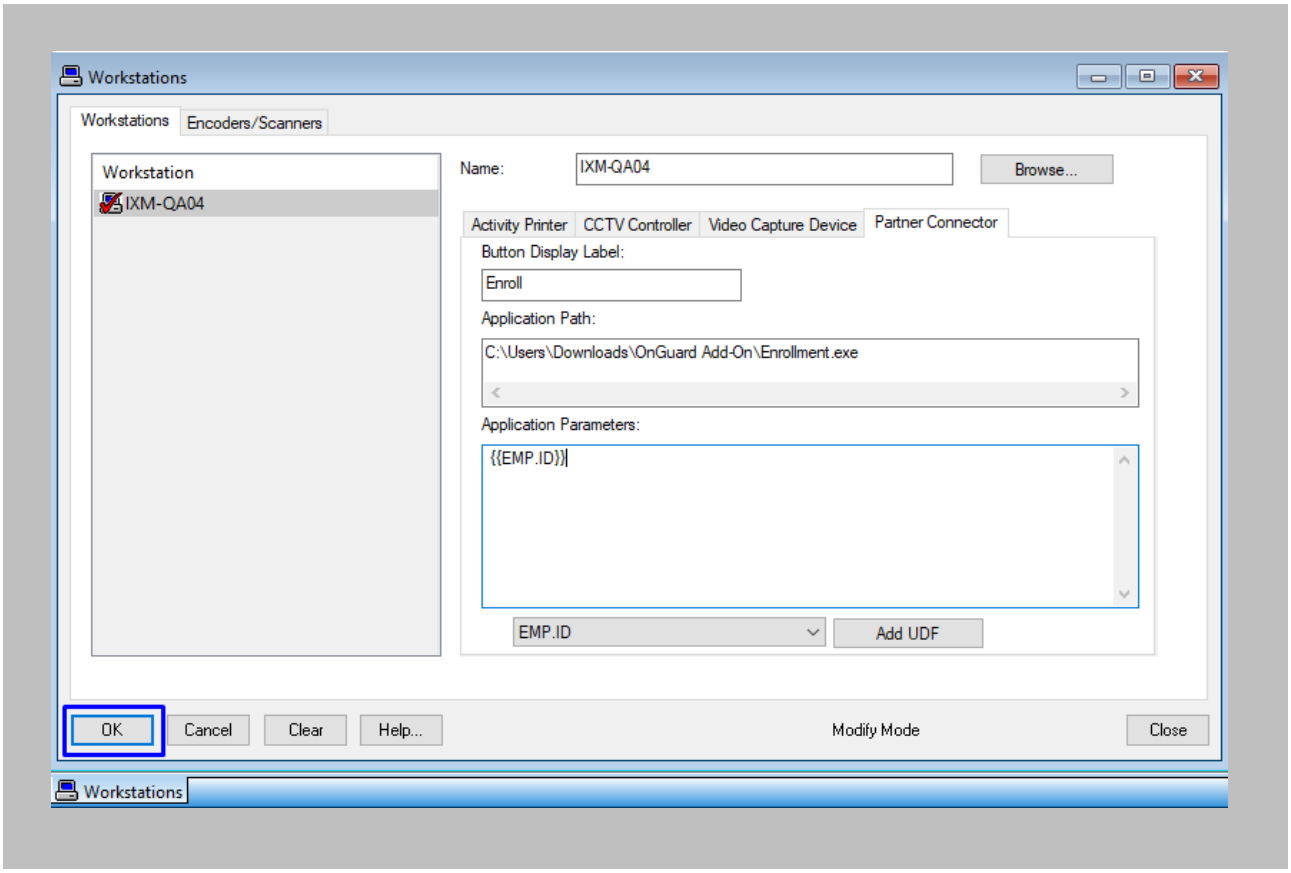


Figure 77: OnGuard - Add Partner Connector

RESULT

Once the configuration is saved the **'Enroll'** button will be displayed on the cardholder window.

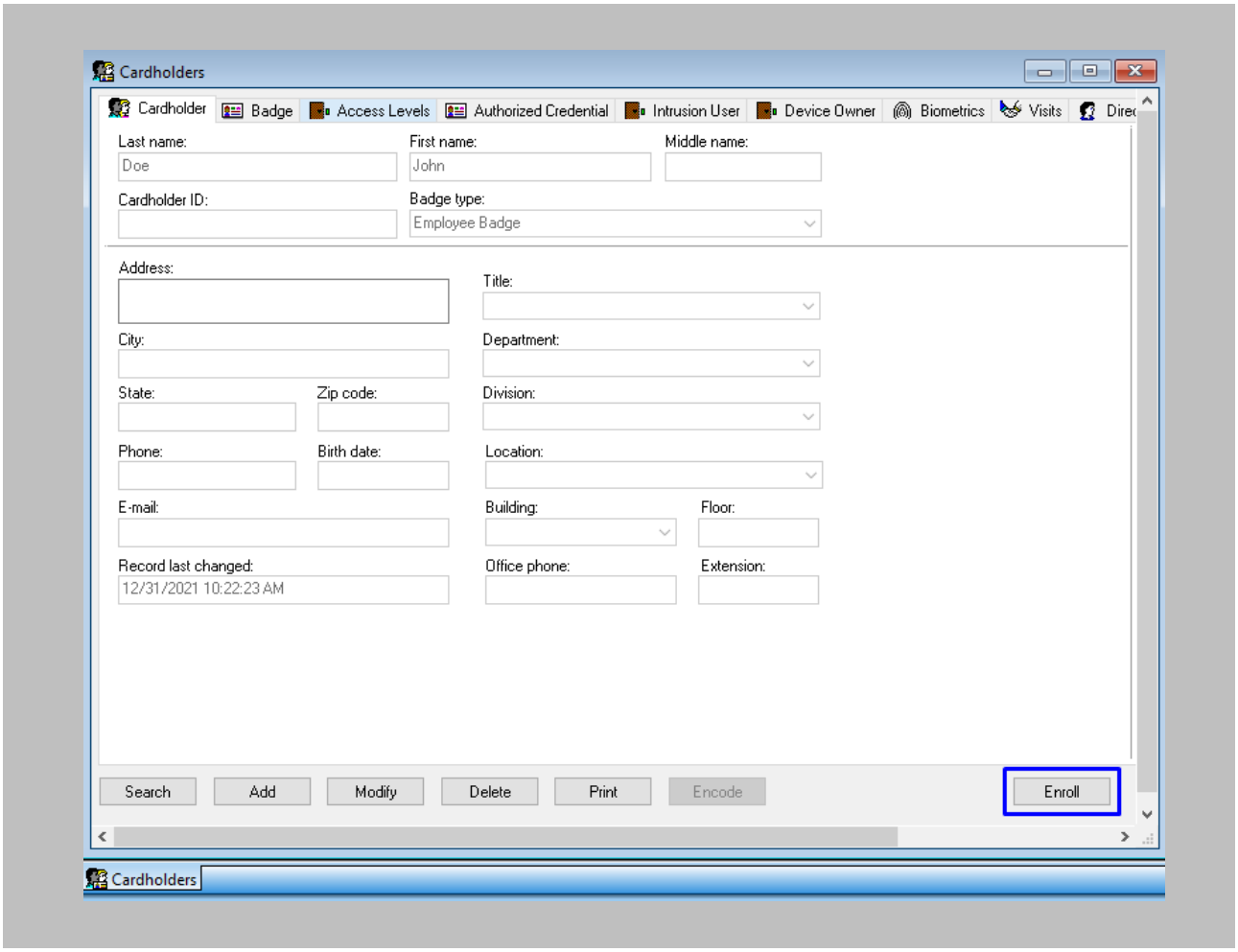


Figure 78: OnGuard - Enroll Button

14. Enrollment from LenelS2 System Administration

When you launch the enrollment application for the first time, it will ask for your API user credentials to perform enrollment.

Procedure

STEP 1

Add a new cardholder or select an existing cardholder and click on the **'Enroll'** button.

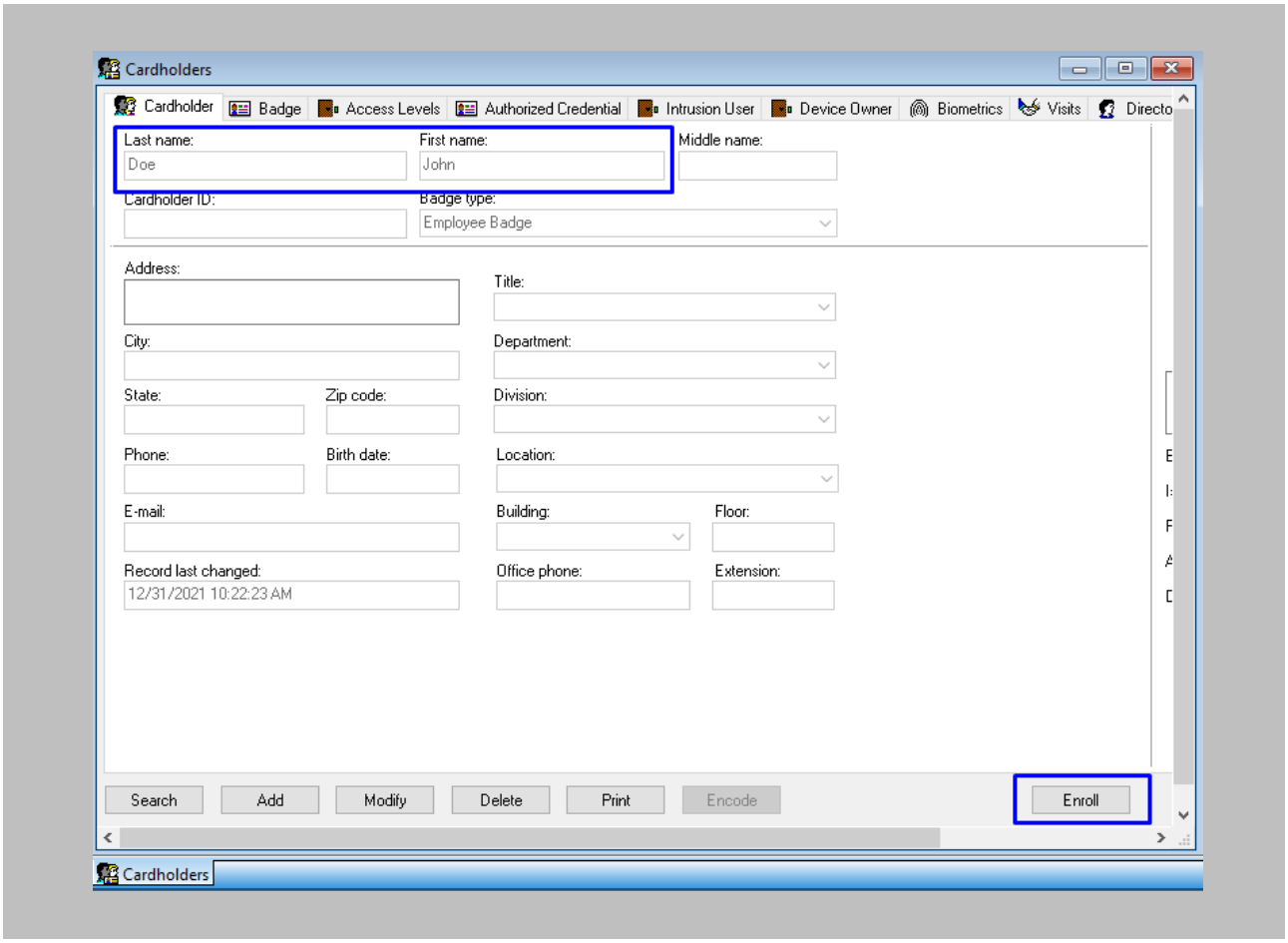


Figure 79: OnGuard - Click Enroll

STEP 2

'Server Configuration' window will appear → Enter the following details:

- **IXM WEB API:** IXM WEB server URL.

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

  http://192.168.1.100:9108/IXMAPI/1.0

- **Username**: Username of IXM WEB API system user. Refer to Creating API System User for API user creation in IXM WEB.
- **Password**: Password of IXM WEB API system user.

Click **OK**.

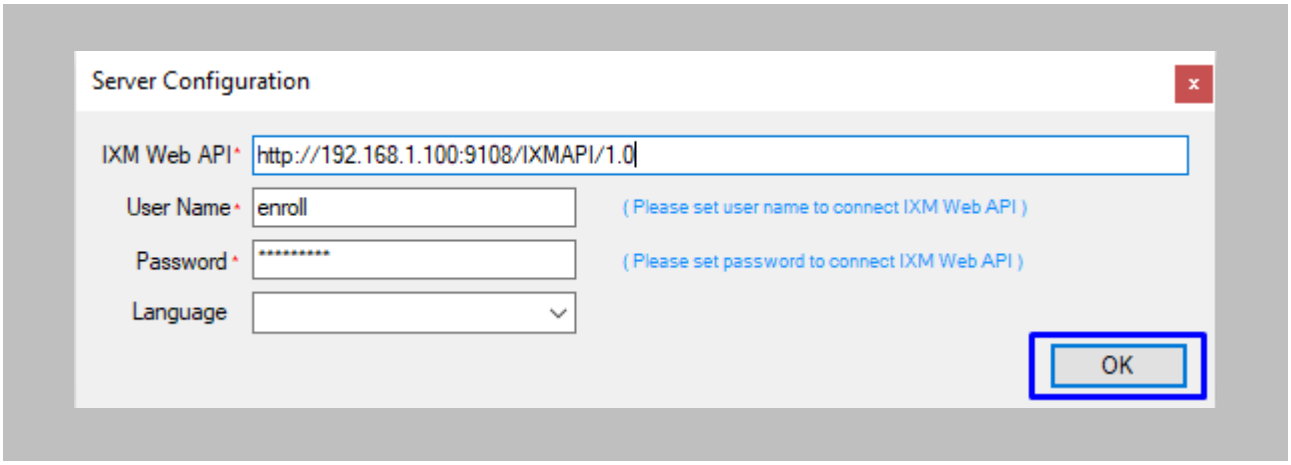


Figure 80: OnGuard - Enrollment Add-on Configuration

Biometric Enrollment from the OnGuard Enrollment Add-On

STEP 1

Click **'Open Capture'** → Select **Fingerprint** → Select **Invixium device** from Device dropdown (Device dropdown will display all fingerprint-supported Invixium devices present in IXM WEB).

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

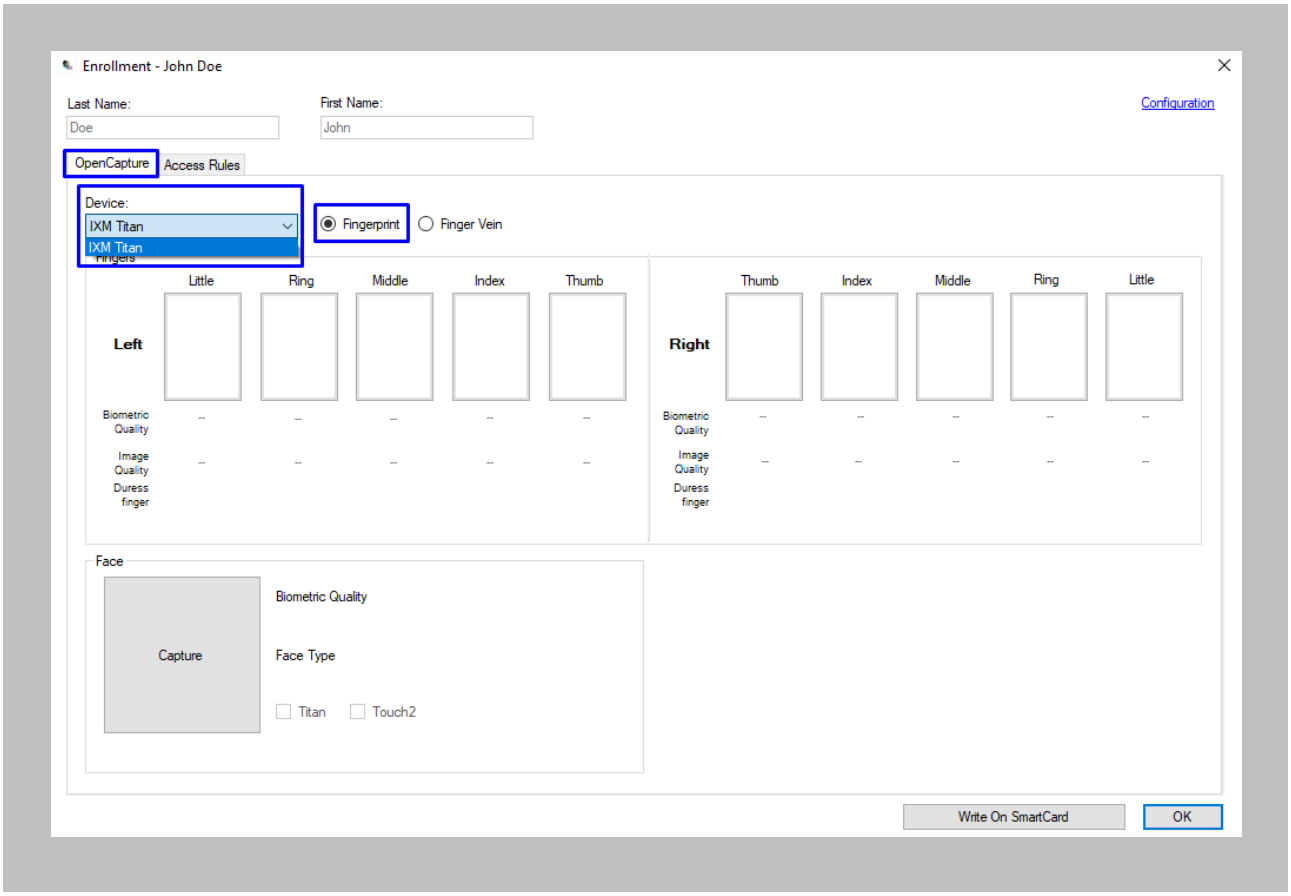


Figure 81: OnGuard – Fingerprint Device Selection

STEP 2

Click on the rectangle box drawn under name of the finger for **Fingerprint** enrollment.

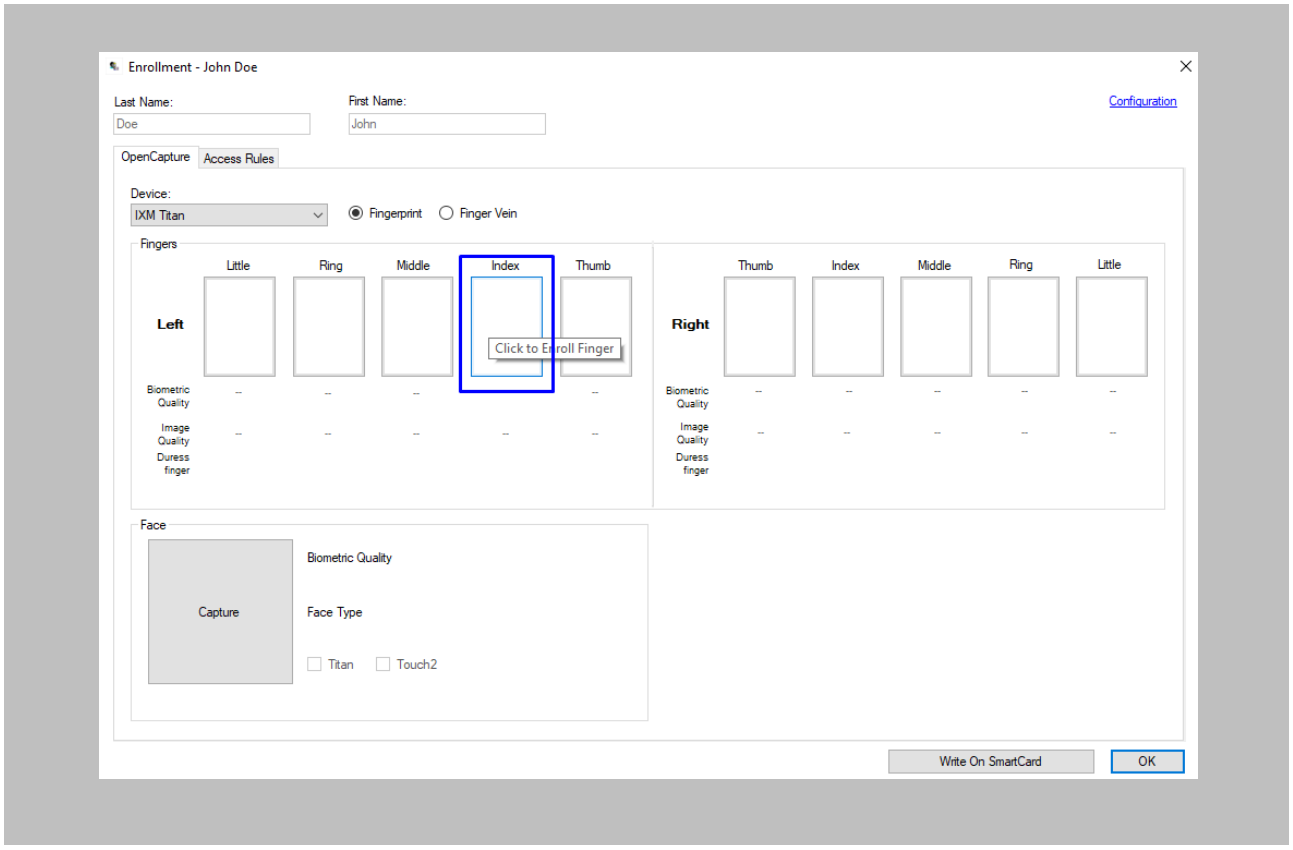


Figure 82: OnGuard - Fingerprint Enrollment

STEP 3

Click on **'Capture'** for **face** enrollment.

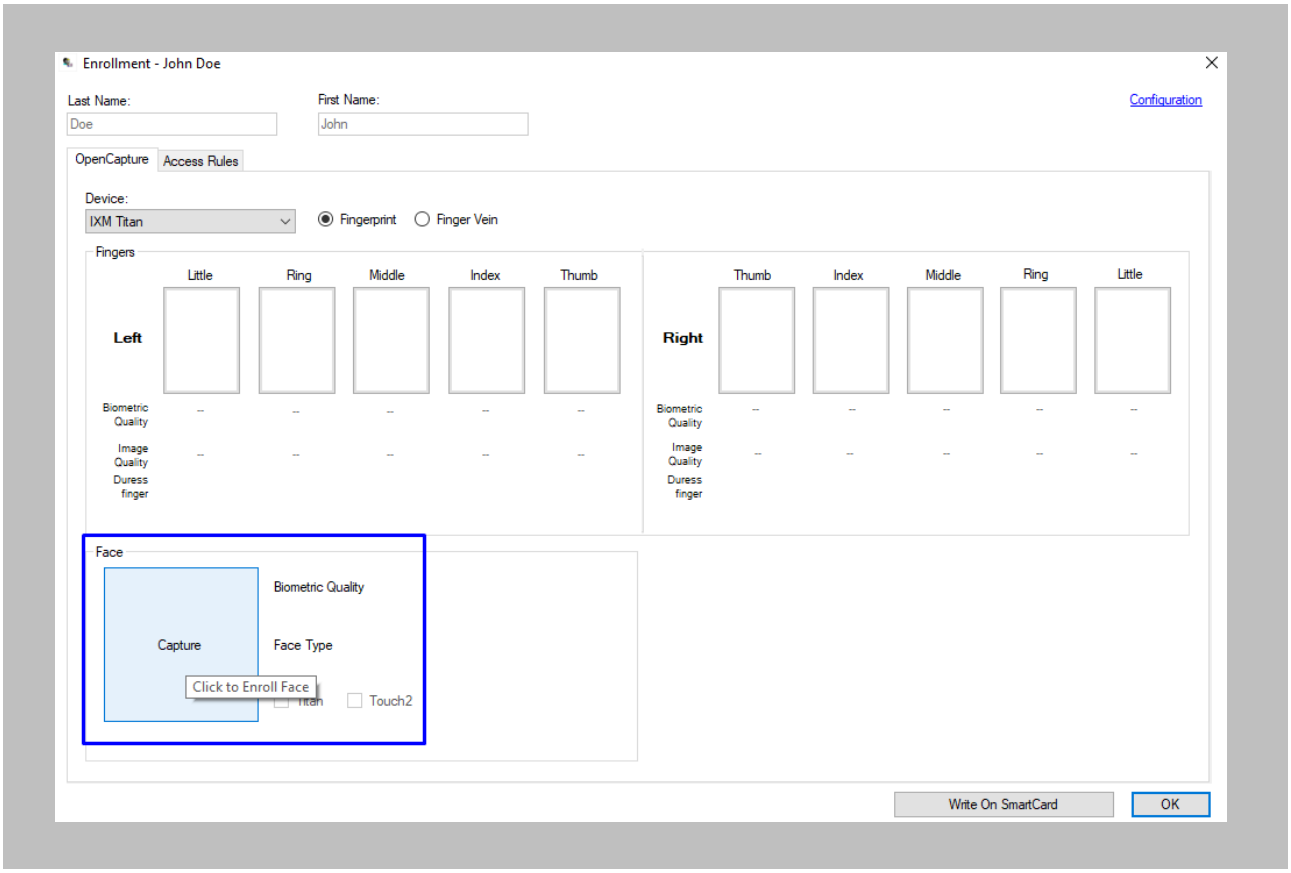


Figure 83: OnGuard - Face Enrollment

STEP 4

Select **Finger Vein** → Select the **Invixium device** from Device Dropdown (Device dropdown will display all finger vein supported Invixium devices present in IXM WEB).

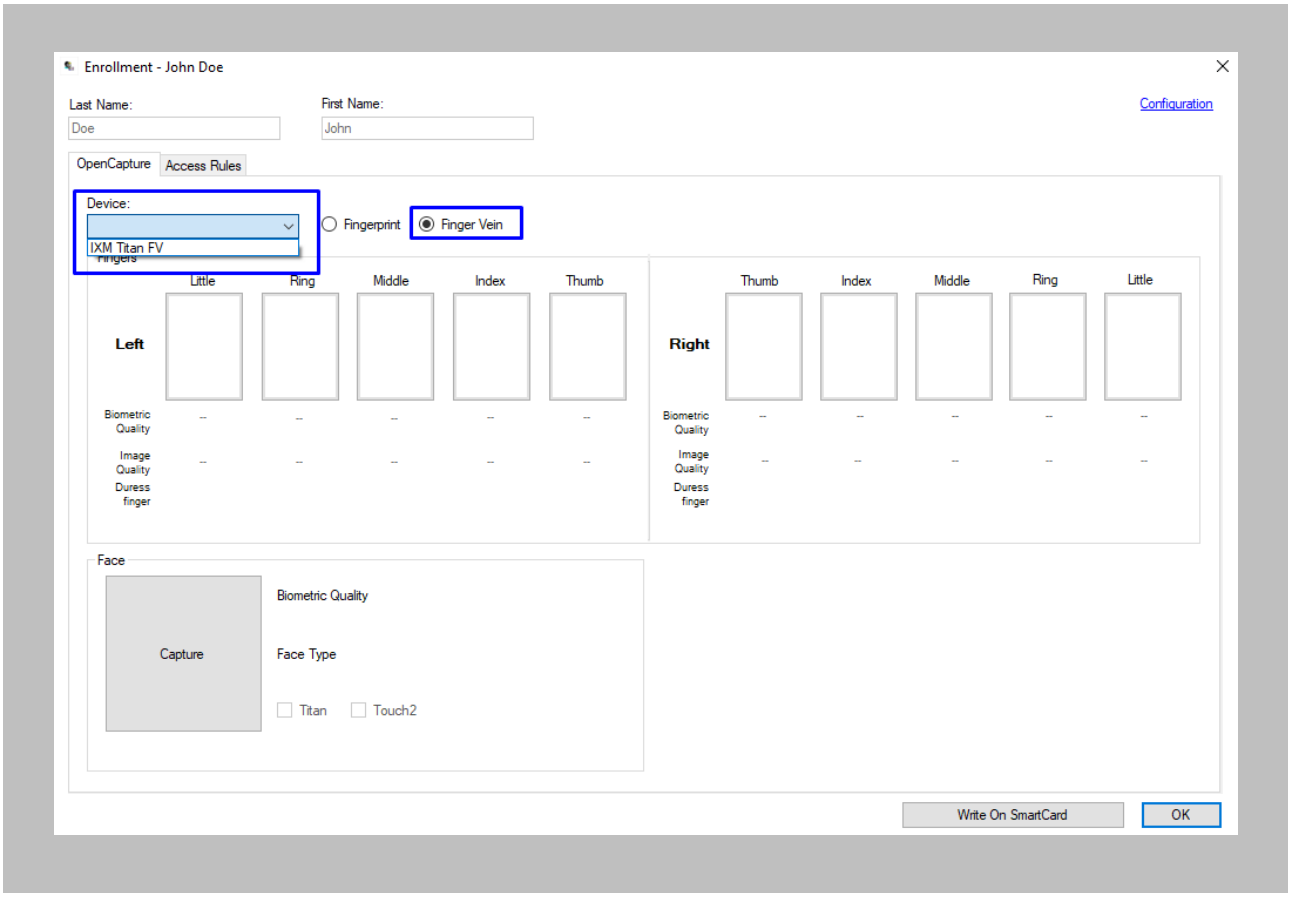


Figure 84: OnGuard – Finger Vein Device Selection

STEP 5

Click on the rectangle box drawn under name of the finger for **Finger Vein** enrollment.

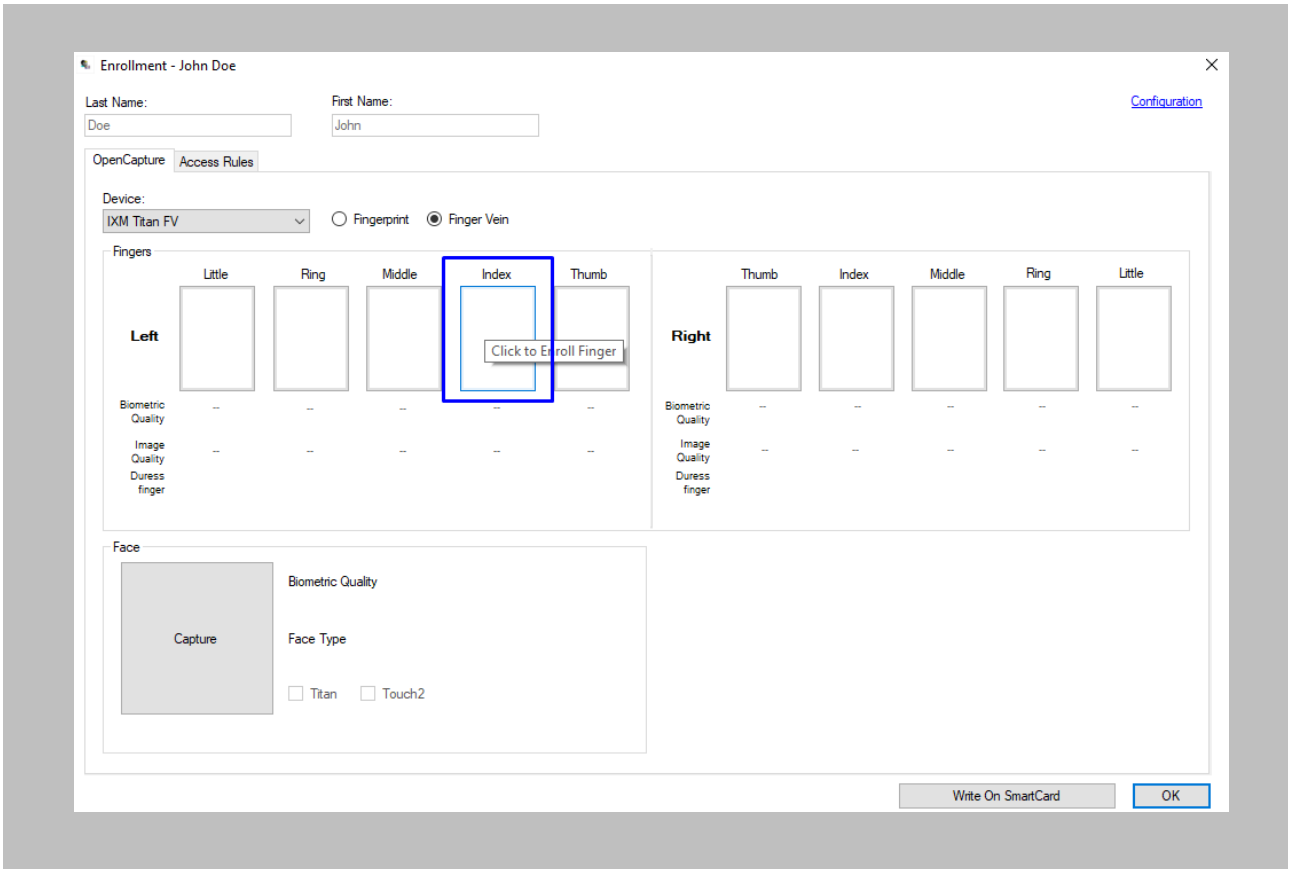


Figure 85: OnGuard – Finger Vein Enrollment

STEP 6

Click on **OK** to save enrollment.

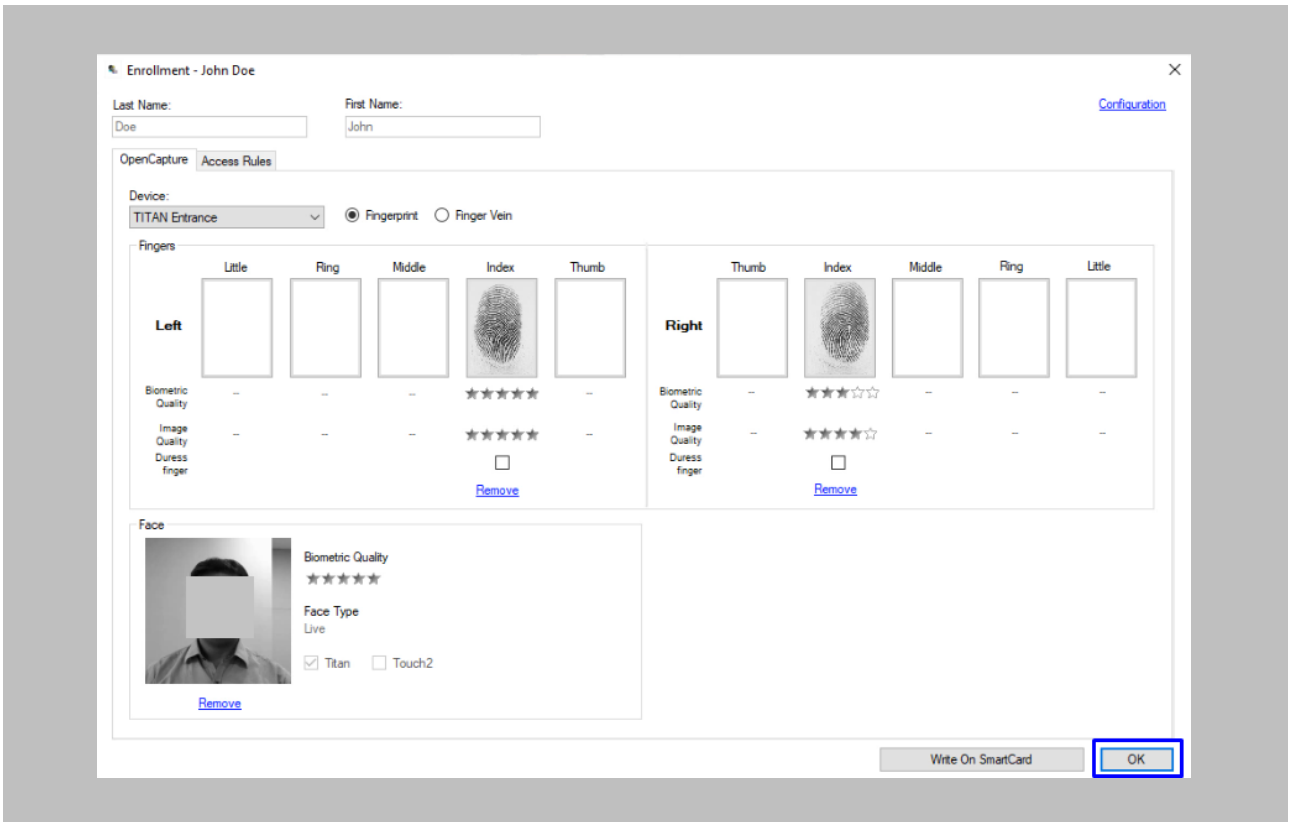


Figure 86: OnGuard – IXM WEB Save Enrollment

Access Rules Configuration from the OnGuard Enrollment Add-On

STEP 1

Click on **'Access Rules'** → Select **'Access Rules'** and **'Security Settings'** of your choice.

STEP 2

Select **'Health Access Rule'** → Select settings according to your requirements.

Note: Thermal Screening is only available if a TITAN + Enhancement Kit is installed.

Enable Mask Detection: Enable this field to allow the device to perform **mask detection**.

- **Mask Detection Rule:** Users can choose one of the following options to select which action occurs when the **Mask Detection** Rule triggers:
  - Use Device Rule
  - Allow on Fail
  - Deny on Fail

Enable Thermal Screening: Enable this field to start **Thermal Screening** during Authentication.

- **Thermal Screening Rule:** Users can choose one of the following options to select which action occurs when the **Thermal Screening** Rule triggers:
  - Use Device Rule
  - Allow on Fail
  - Deny on Fail

Attestation Questions: Enable this field to allow the device to perform **Attestation Questionaries** during Authentication.

- **Attestation Questions Rule:** Users can choose one of the following options to select which action occurs when the **Attestation Questions** Rule triggers:
  - Use Device Rule
  - Allow on Fail
  - Deny on Fail

STEP 3

Click on **OK** to save User Access Rules settings.

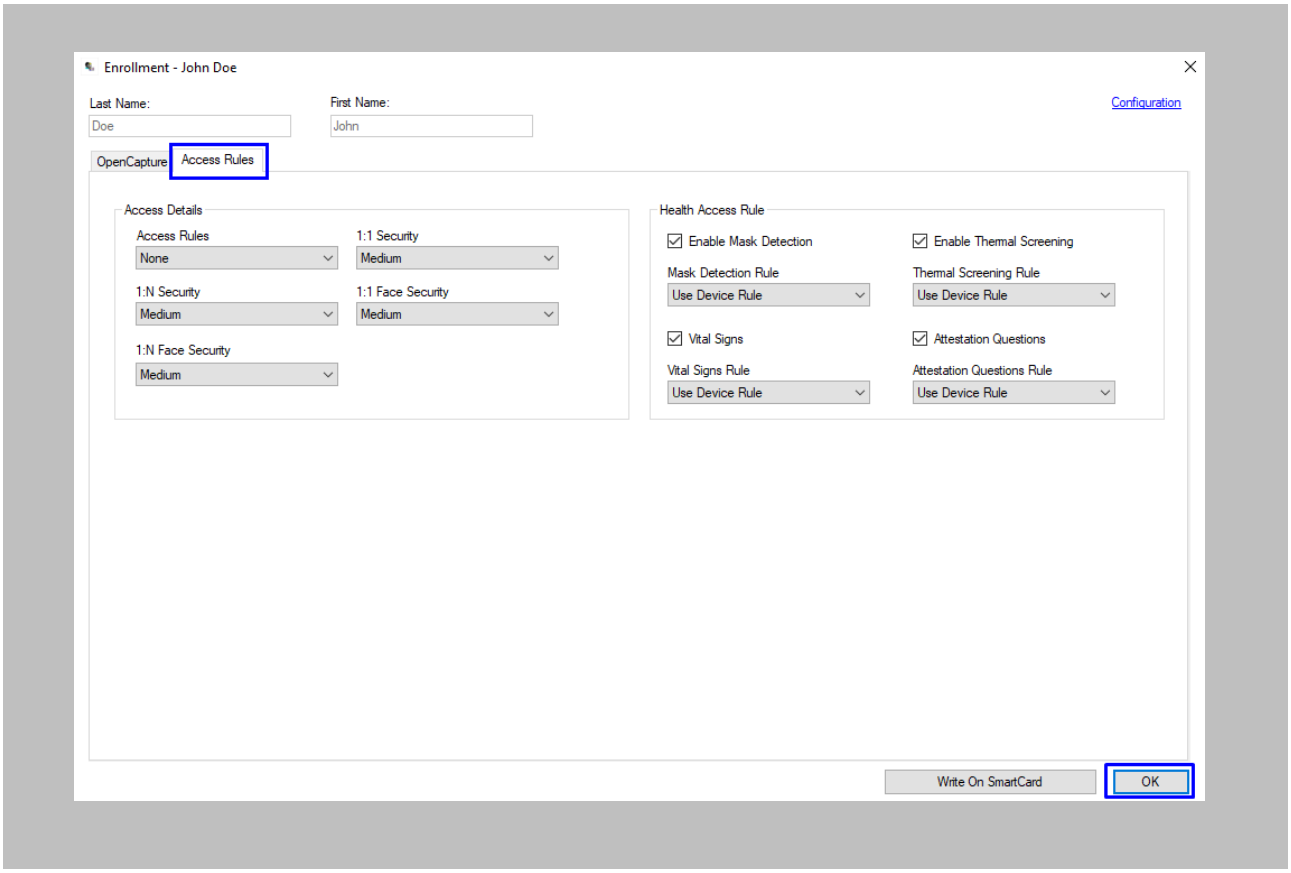


Figure 87: OnGuard – IXM WEB Save Access Rules Settings

Save User Records on Cards from the OnGuard Enrollment Add-On

STEP 1

Open the **'Enrollment'** add-on → Perform enrollment as per requirement → Click on **'Write on SmartCard'** button.

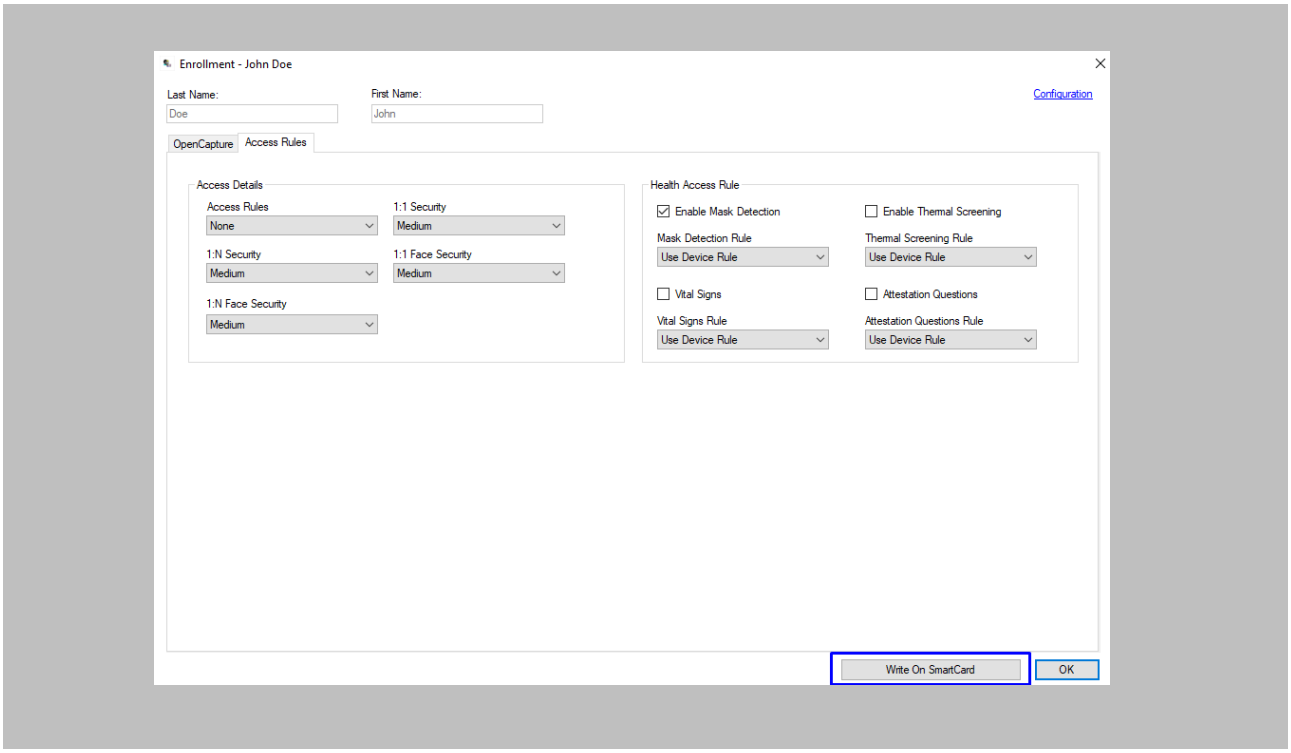


Figure 88: OnGuard - IXM WEB Save User Record on Card

RESULT

The following message will be displayed when the user record is successfully saved on the card.

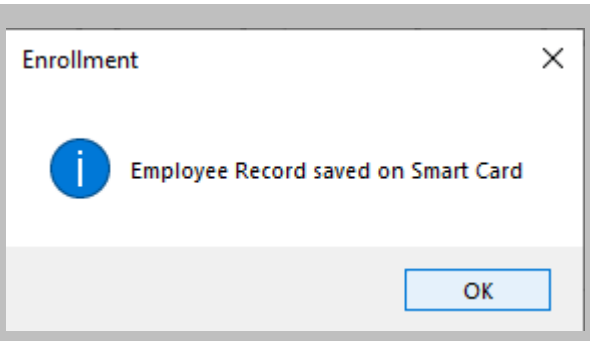


Figure 89: OnGuard – IXM WEB User Record Saved on Card

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 needed.

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 off from finger before placement.

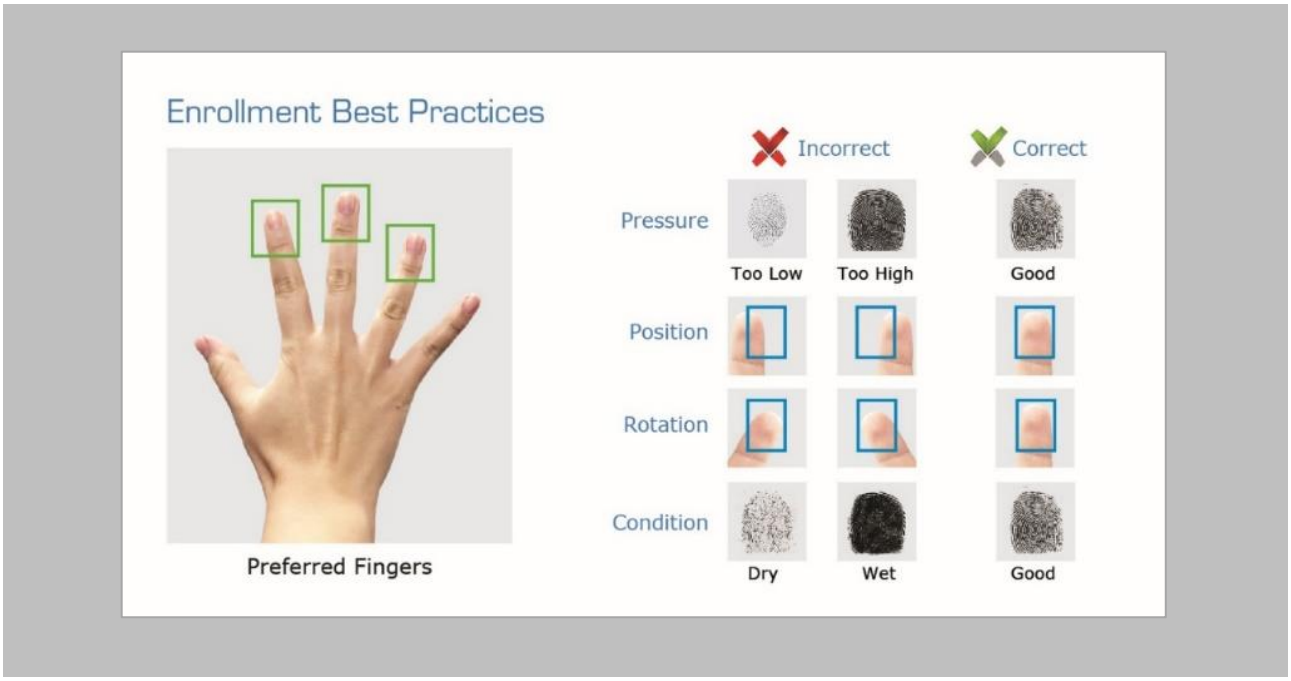


Figure 90: Fingerprint Enrollment Best Practices

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 91: 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.

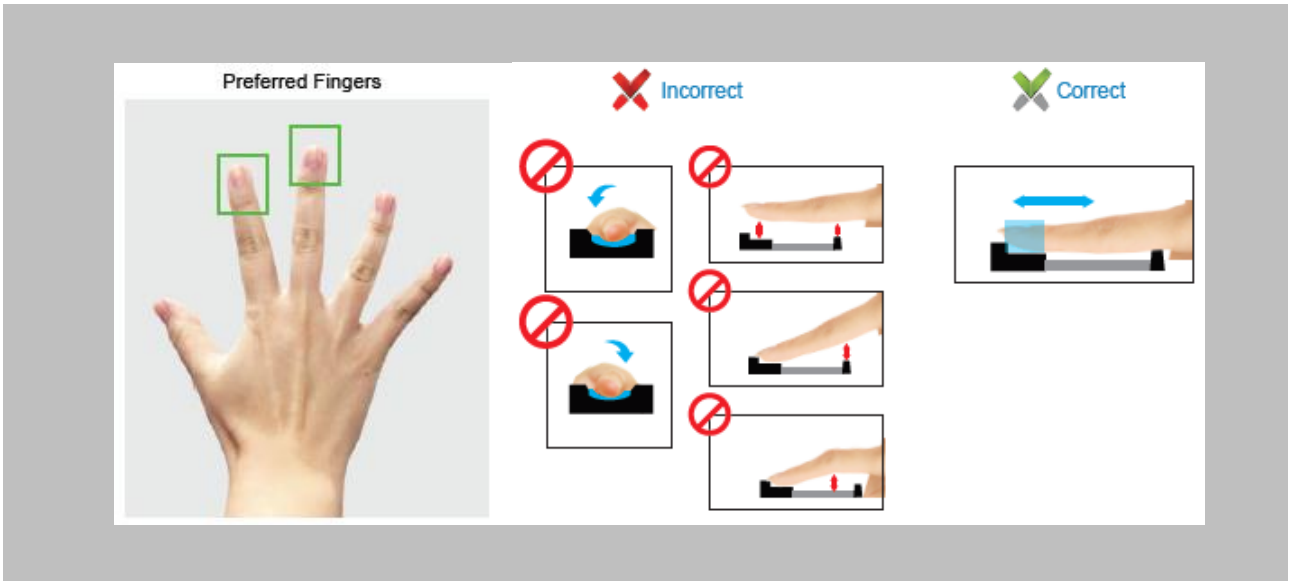


Figure 92: Finger Vein Enrollment Best Practices

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.

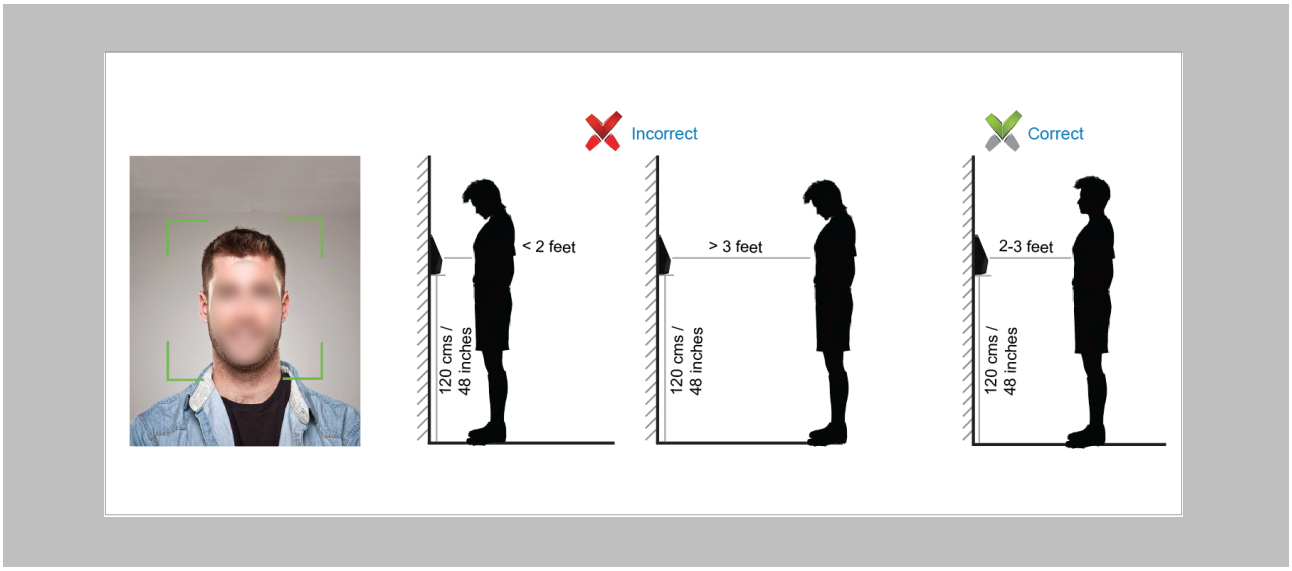


Figure 93: Face Enrollment Best Practices

16. Send Logical Events to OnGuard

The following settings are needed in System Administration to receive logical events for two events from IXM WEB.

1. Temperature
2. Mask

Procedure

STEP 1

In System Administration Click **Additional Hardware** → Select **Logical Sources.**

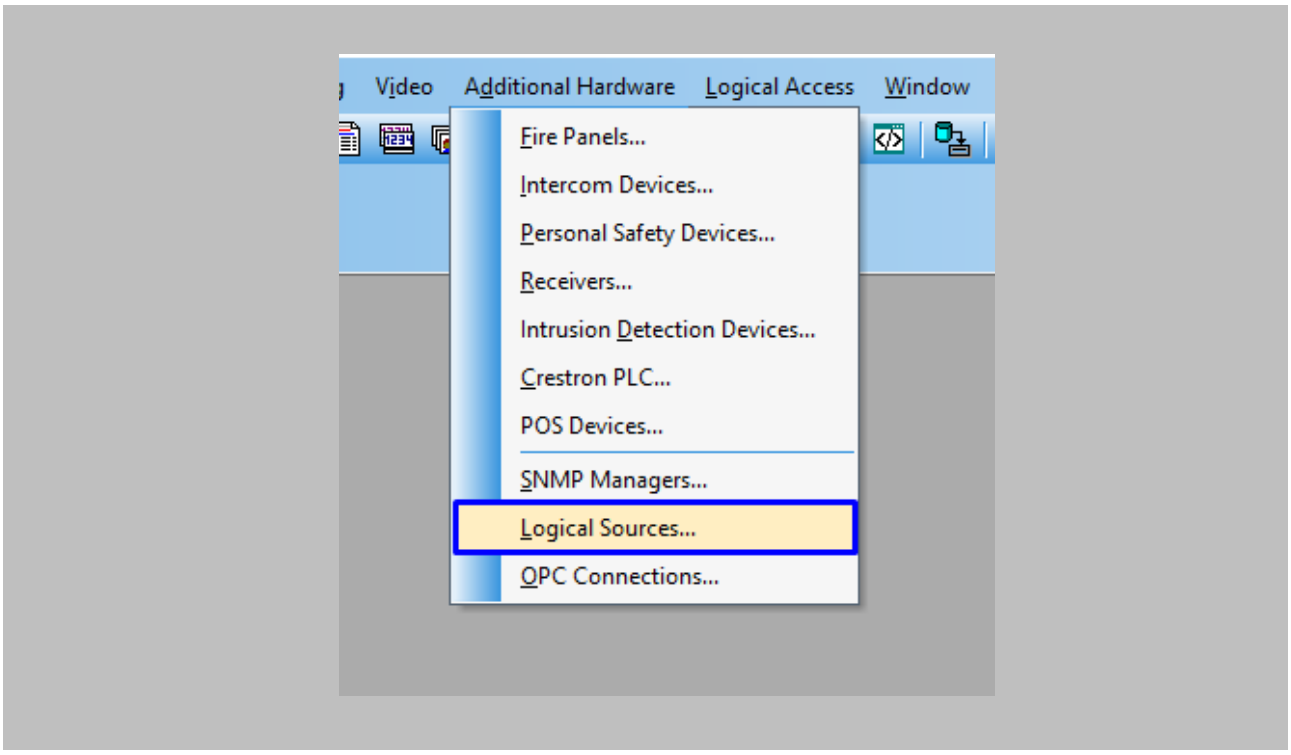


Figure 94: OnGuard - Add New Logical Source

STEP 2

Click on **Add** button.

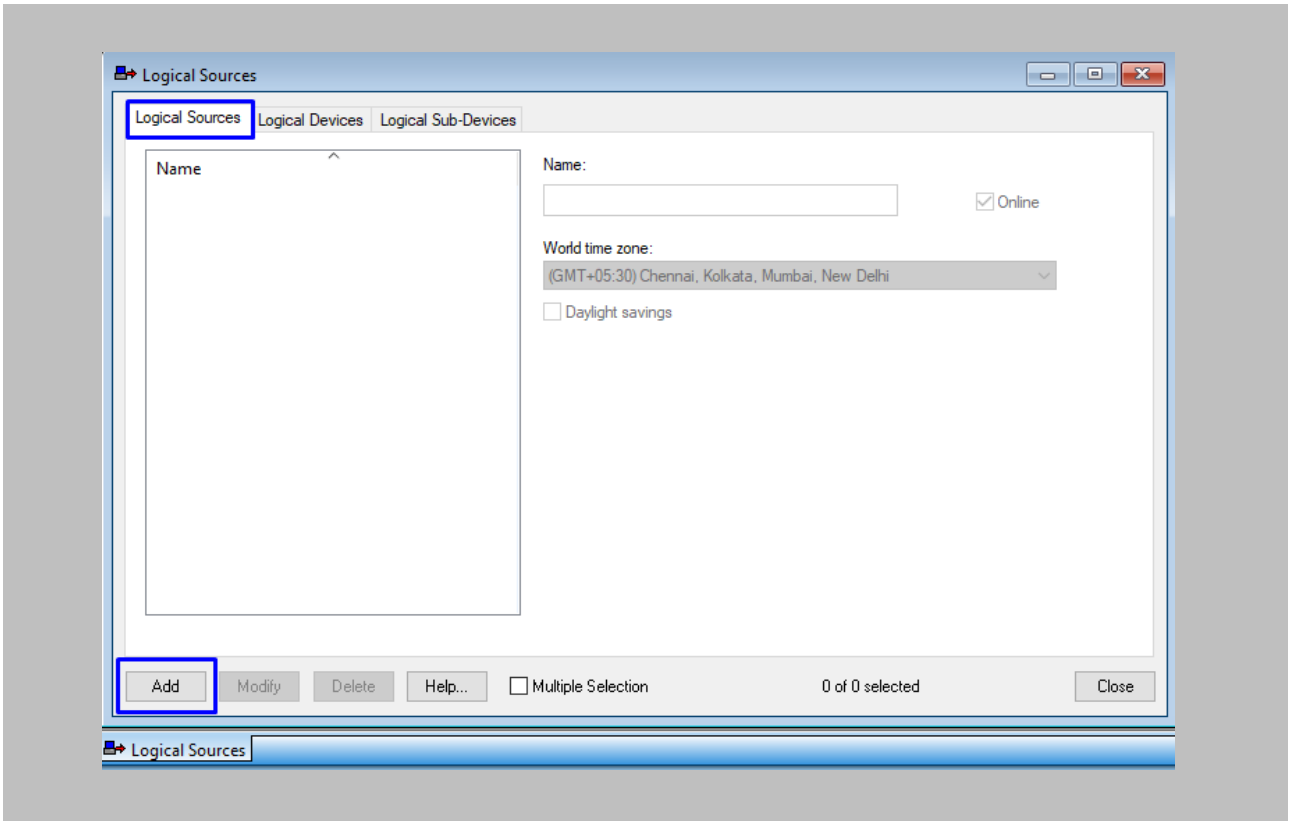


Figure 95: OnGuard – Logical Source

STEP 3

Enter the following details:

- **Name:** Define the name of **'Logical Source'**.
- **World TimeZone:** Select timezone from the **'World time zone'** dropdown.

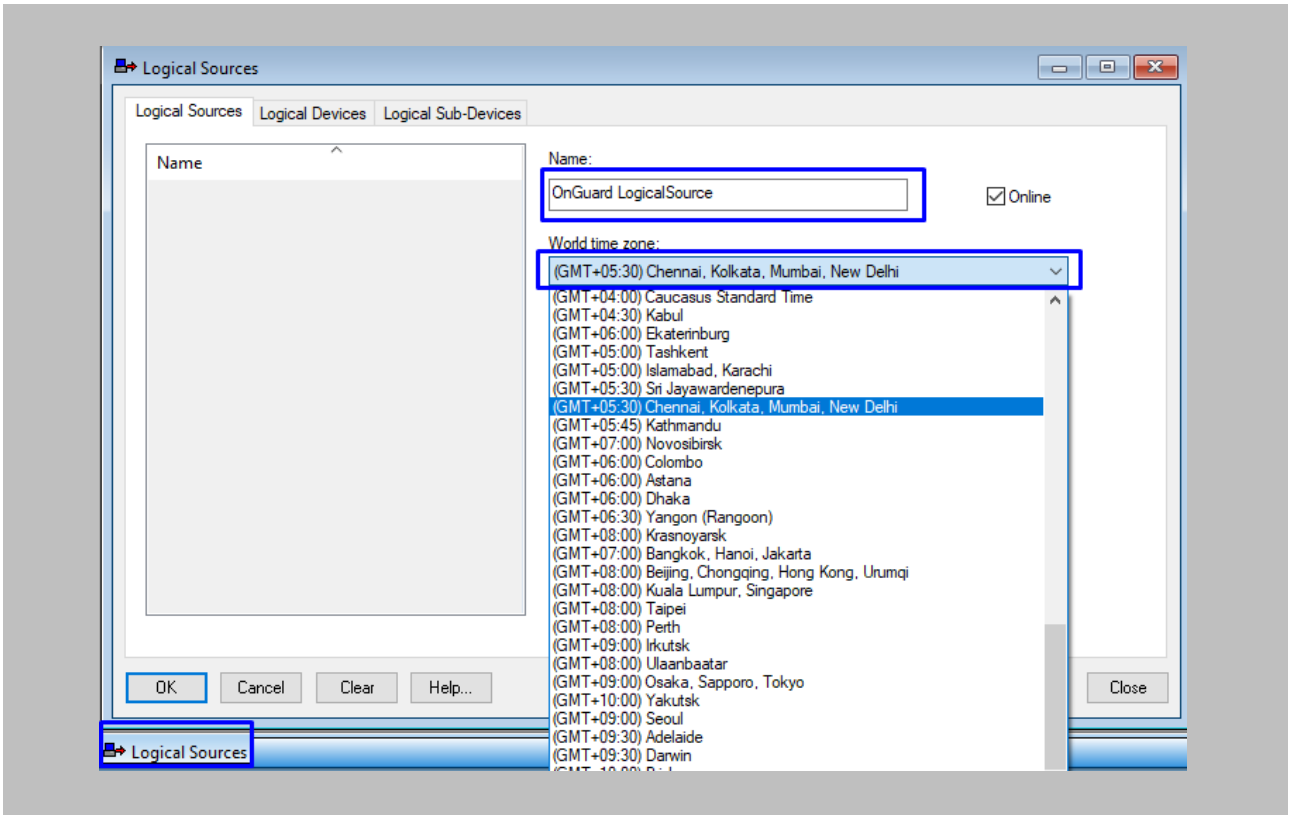


Figure 96: OnGuard - Add New Logical Source

STEP 4

Click **OK**.

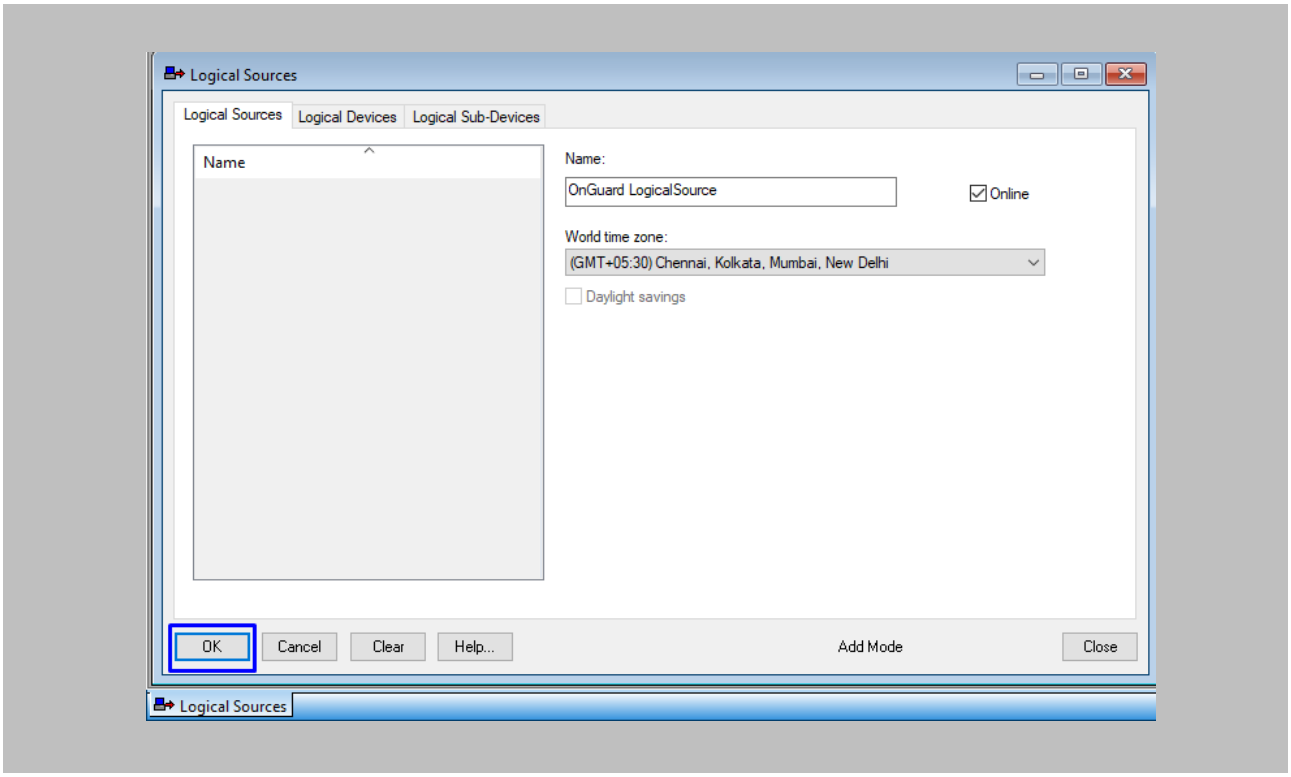


Figure 97: OnGuard - Save Logical Source

STEP 5

Select the **Monitor Zone** of your choice → Click **OK**.

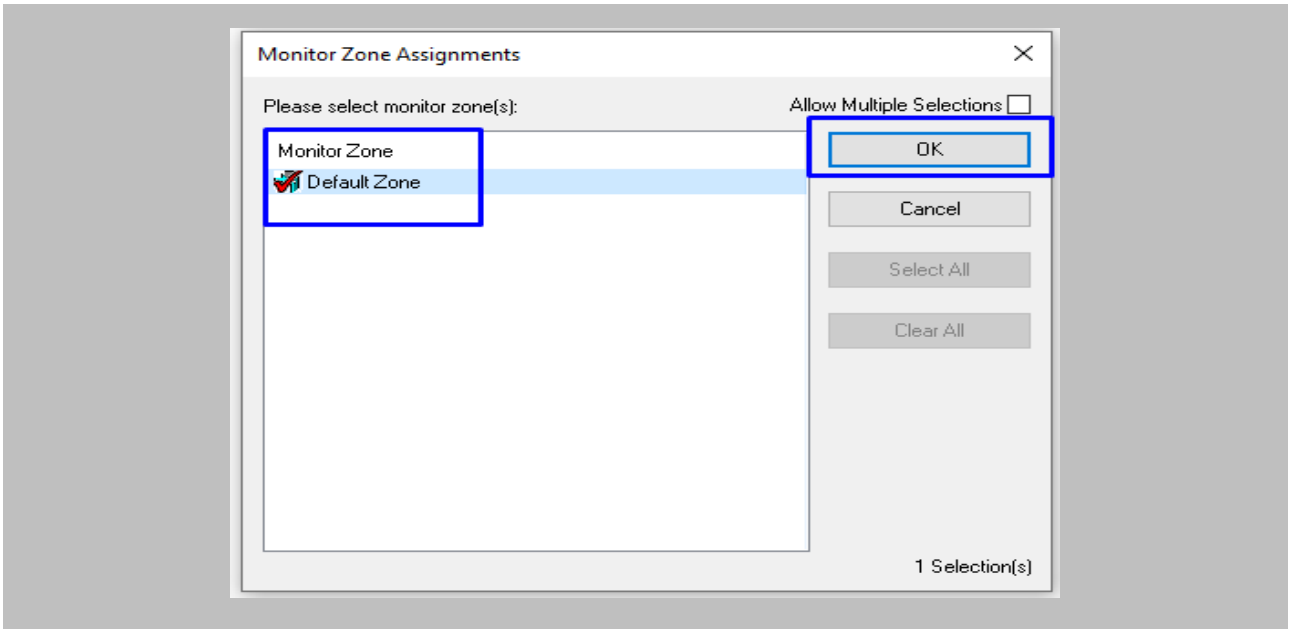


Figure 98: OnGuard - Logical Source Monitor Zone

Created **'Logical Source'** will be displayed as shown below.

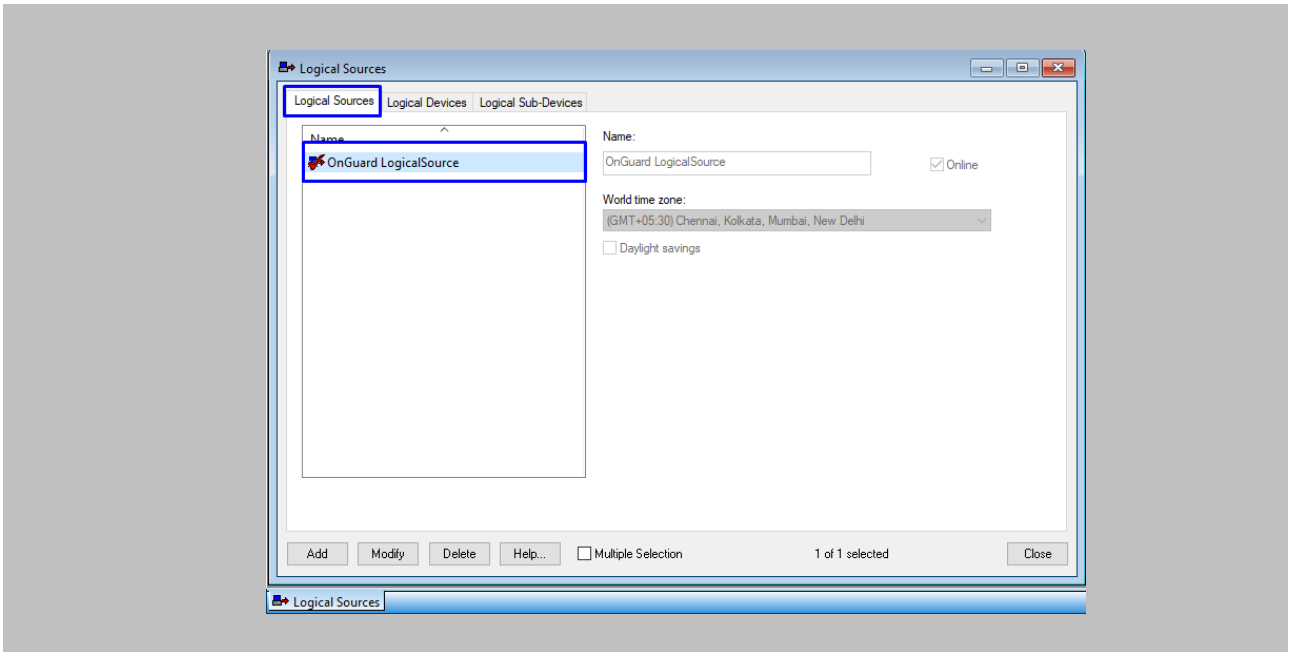


Figure 99: OnGuard - Logical Sources List

STEP 6

Click on the **'Logical Device'** tab → **Add.**

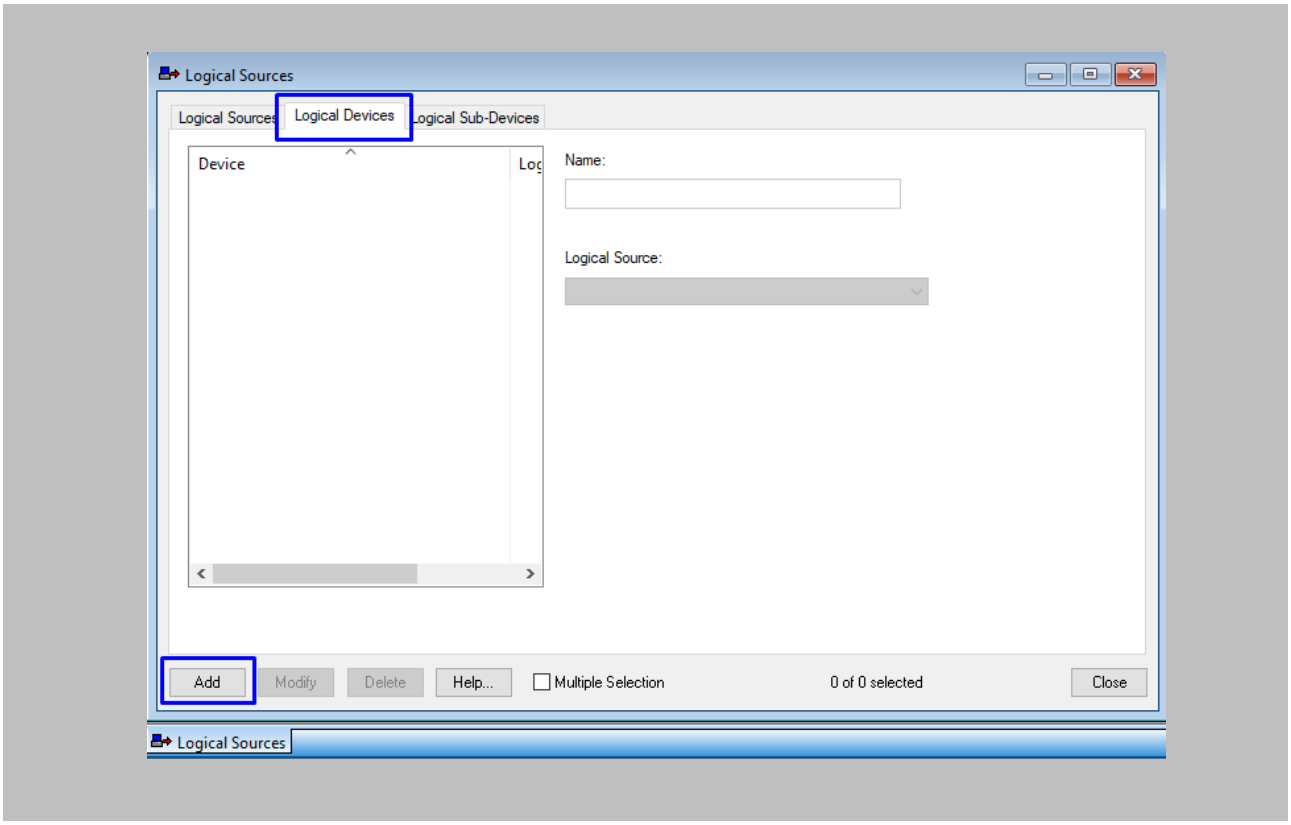


Figure 100: OnGuard - Logical Device

STEP 7

Enter the following details:

- **Name:** Define the name of **'Logical Device'** for which you want logical events.

Note: The name of 'Logical Device' should be the same as the name of the Invixium device for which you want logical events in OnGuard.

- **Logical Source:** Select **'Logical Source'** from the dropdown.

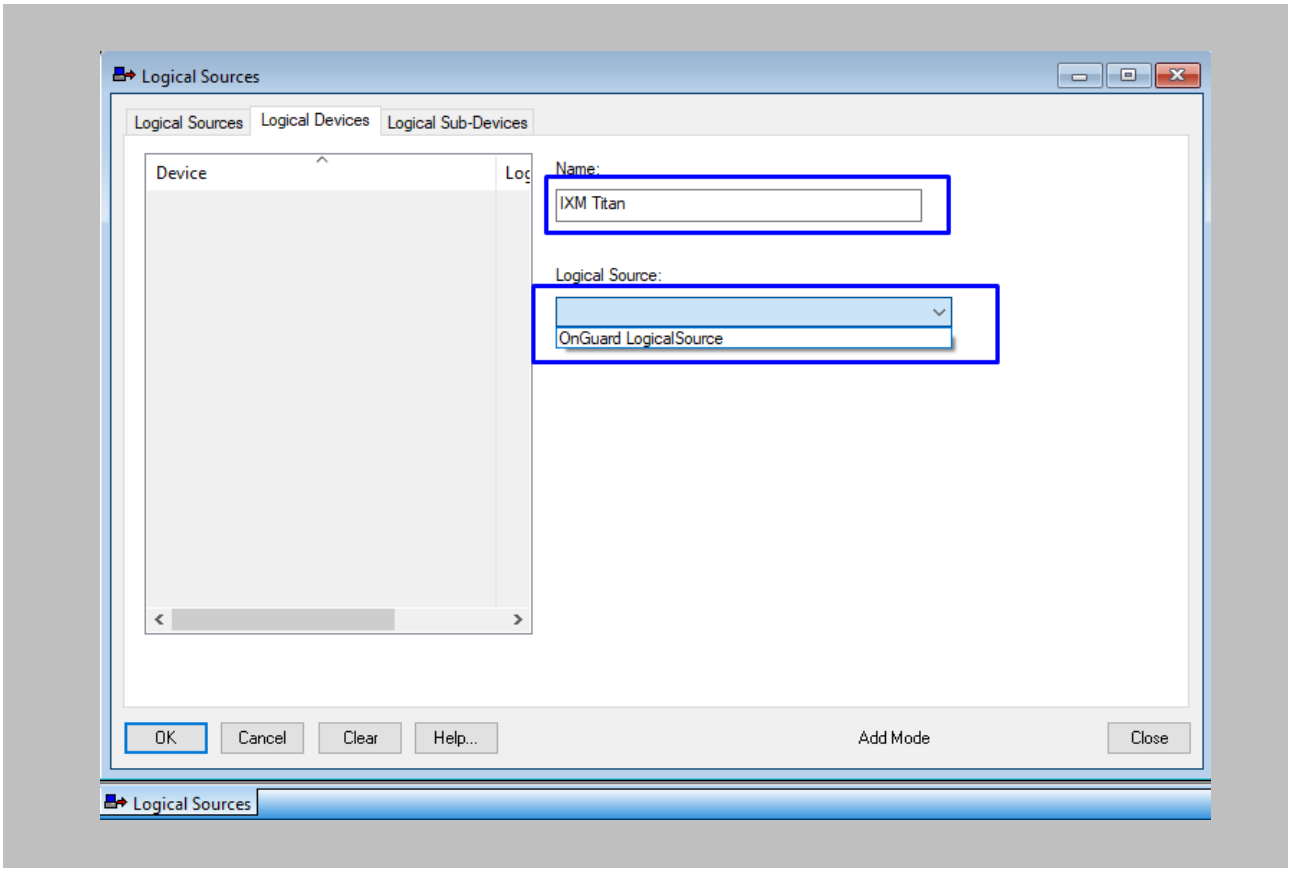


Figure 101: OnGuard - Logical Device Configuration

STEP 8

Click **OK**.

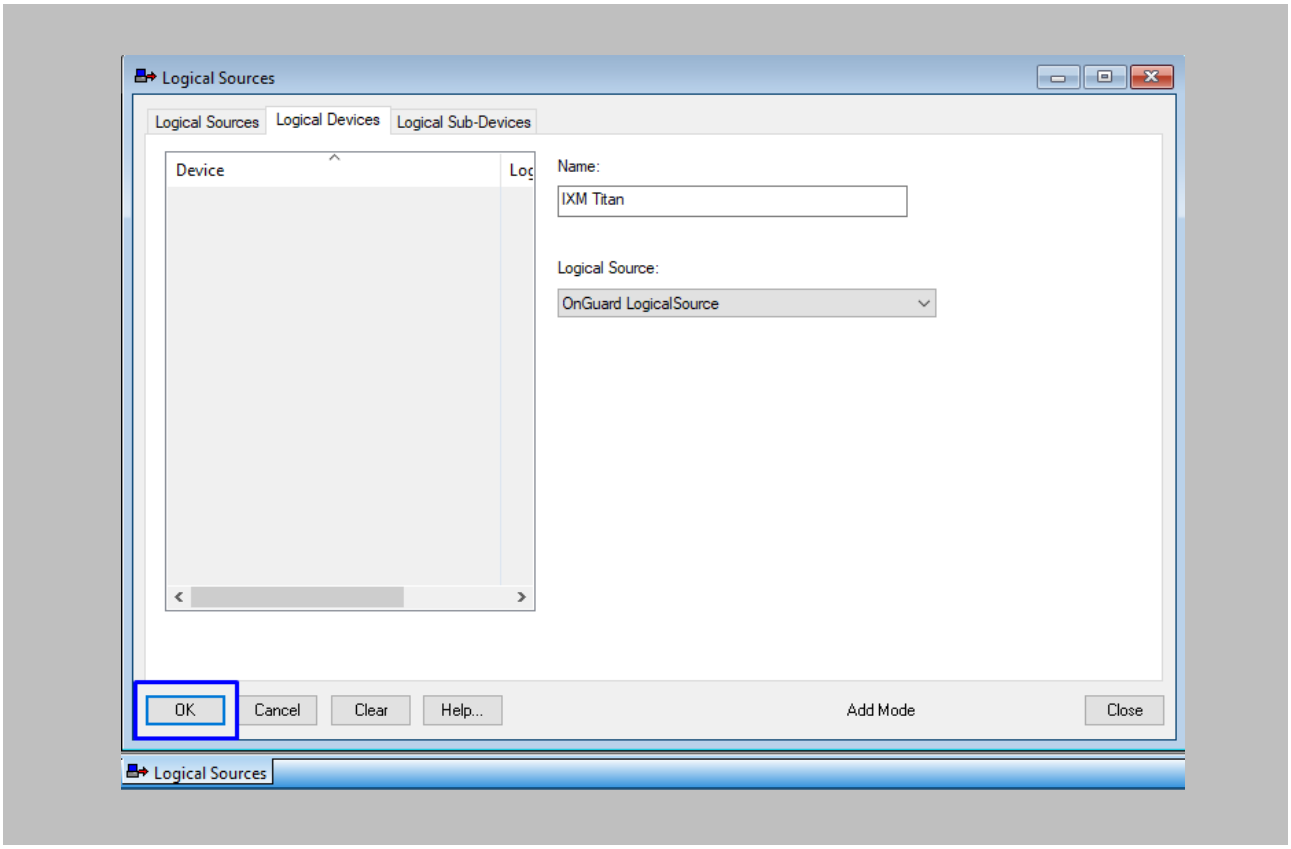


Figure 102: OnGuard - Save Logical Device

The created **'Logical Device'** will be displayed as shown below.

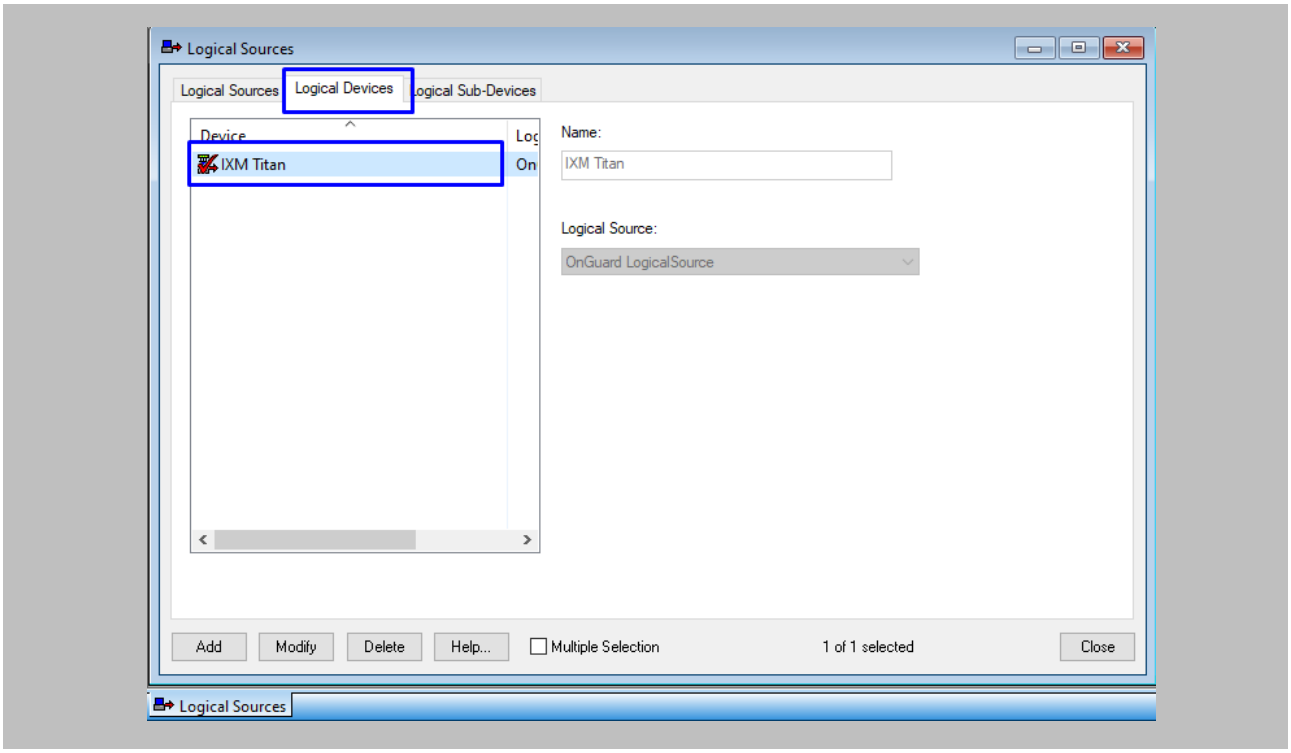


Figure 103: OnGuard - Logical Devices List

STEP 9

When **mask** and **thermal** violations are observed during authentication on the **Invixium** device, EBT and mask events will be picked up from **EBTEventDetails** and sent to OnGuard.

STEP 10

To view these events open **Alarm Monitoring**.

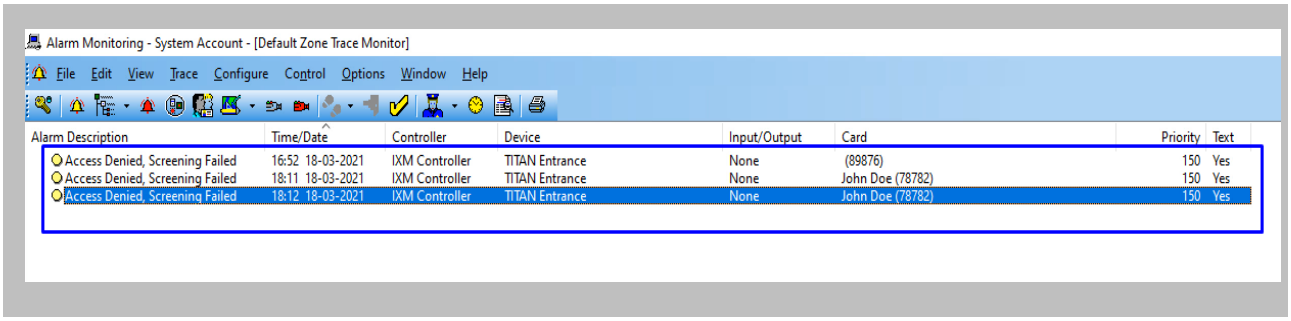


Figure 104: OnGuard - Mask and Thermal Events

STEP 11

To view the details of any event, select that **event** → Right Click → Click **View Associated Text**.

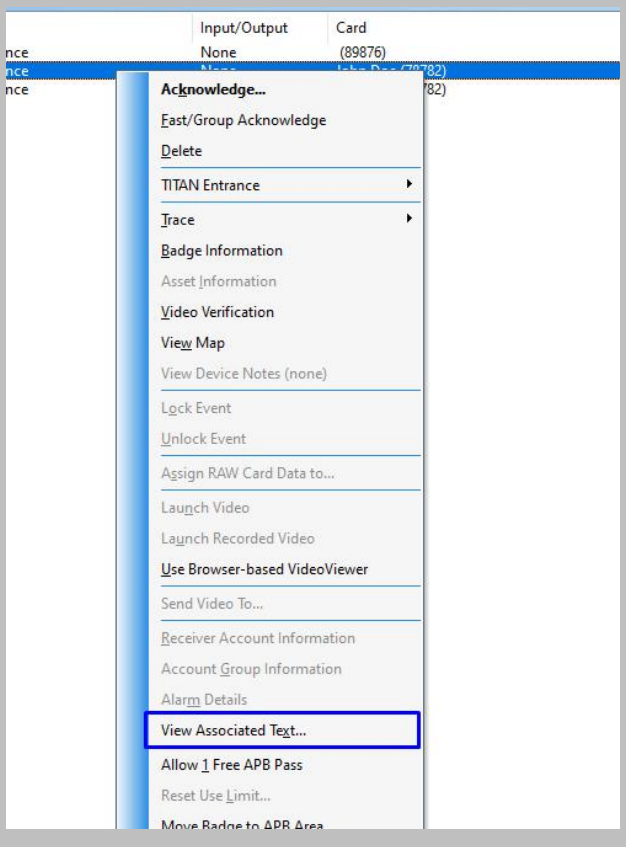


Figure 105: OnGuard - View Associated Text

The following screen will be displayed when you click on **'View Associated Text'.**

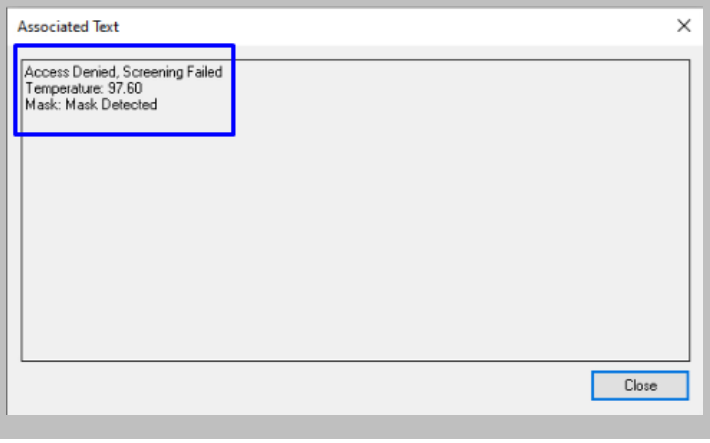


Figure 106: OnGuard - View Associated Text

17. Configure Custom PIN Fields in OnGuard

The following settings are needed in System Administration to synchronize the PIN number of the badge from OnGuard to IXM WEB.

Note: Invixium and LenelS2 strongly recommend performing a backup before performing this step!

STEP 1

Open **'Forms Designer'** → Select **'Cardholder'** → **OK.**

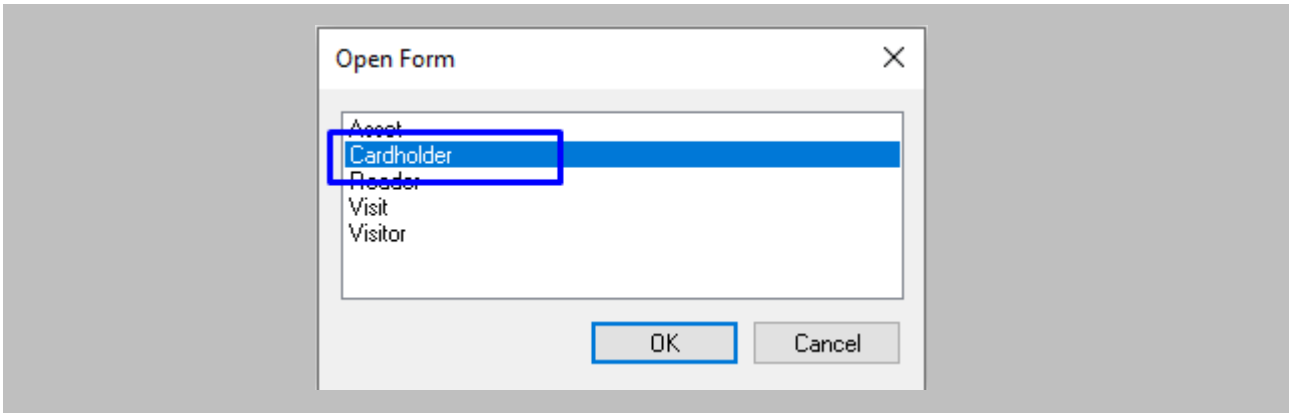


Figure 107: OnGuard - Custom Pin

STEP 2

Once the **'Cardholder'** window appears → Select the **'Badge'** tab.

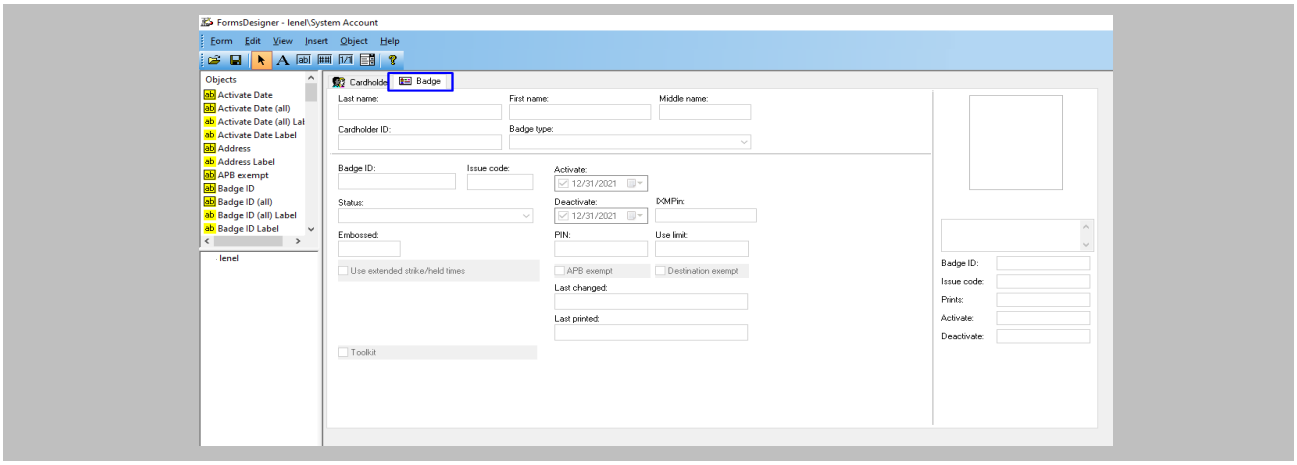


Figure 108: OnGuard - Badge Custom Pin

STEP 3

Click **Insert** → **Numeric Field** → Design **Numeric Field** at the place where you want on the **'Badge'** window.

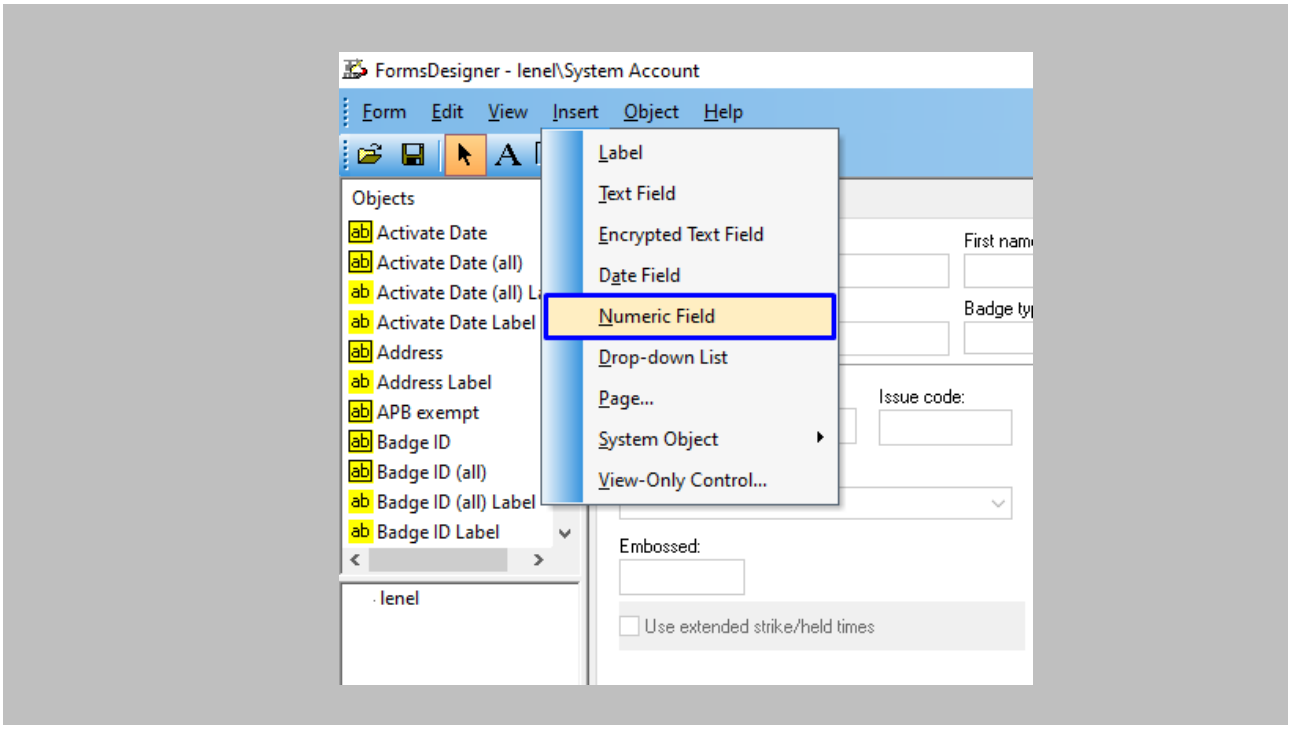


Figure 109: OnGuard - Add Numeric Field

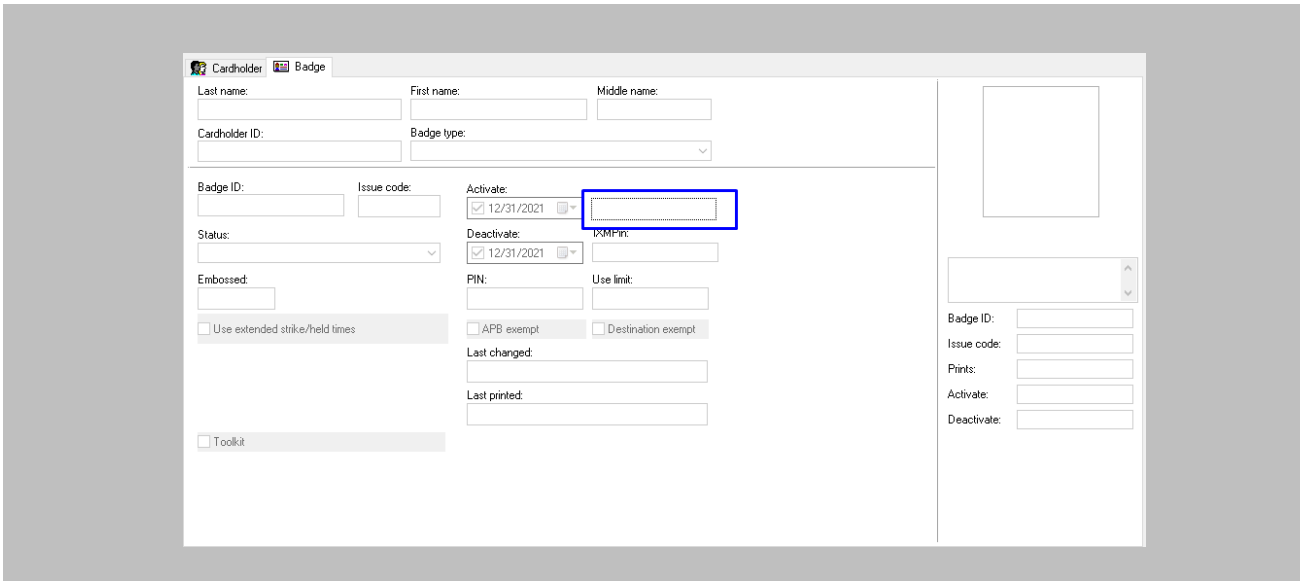


Figure 110: OnGuard - Design Numeric Field

STEP 4

Enter **'Field Name'** → **OK**.

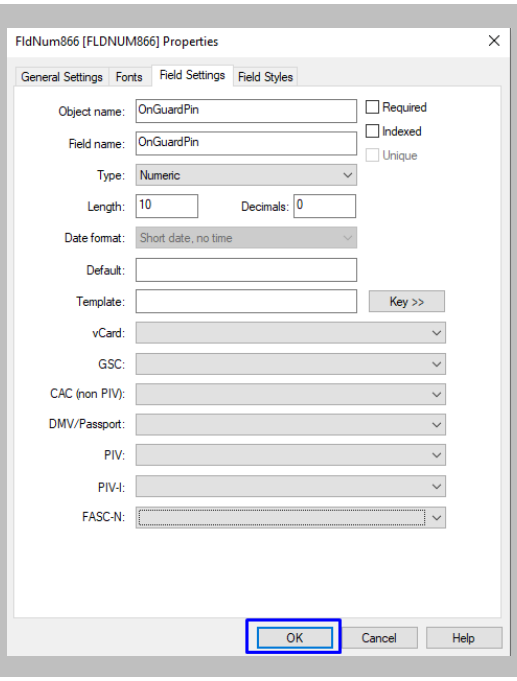


Figure 111: OnGuard - Save Numeric Field

STEP 5

Click **Insert** → **Label** → Design **Label** at the place where you want on the **'Badge'** window.

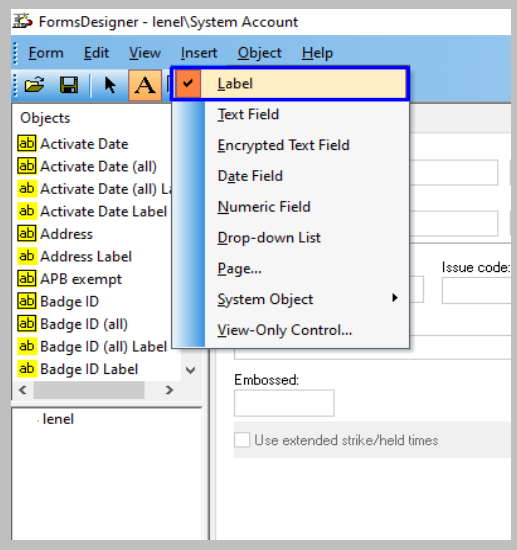


Figure 112: OnGuard - Add Label

STEP 6

Enter **'Text'** → **OK**.

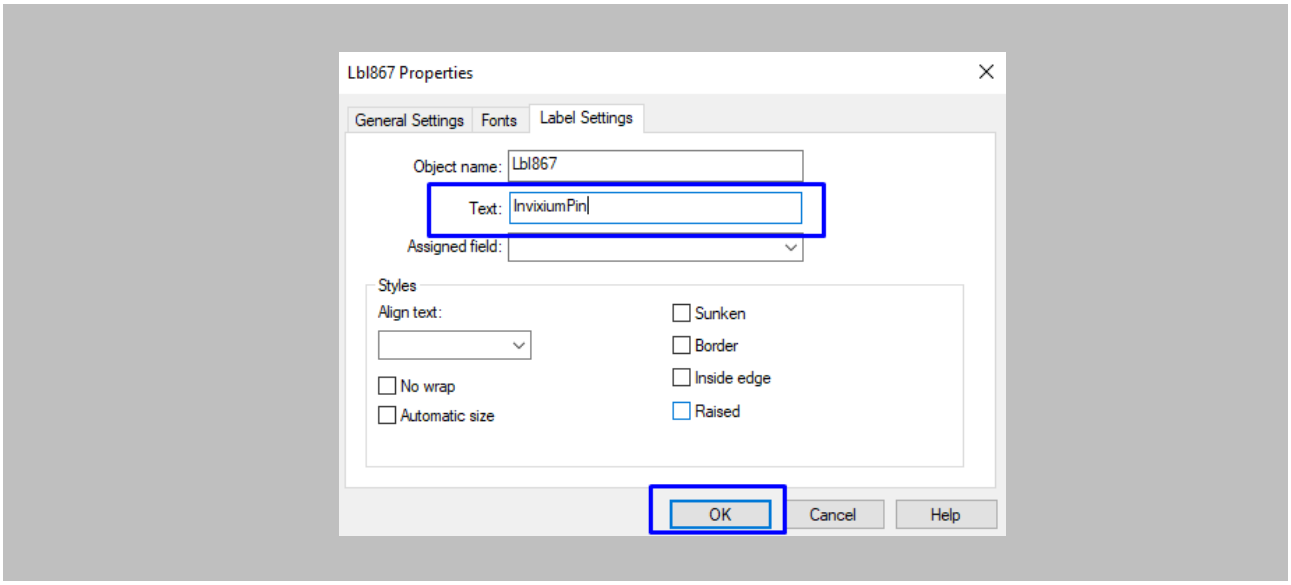


Figure 113: OnGuard - Save Label

Custom **PIN** Field will be visible on the **'badge'** window as shown below.

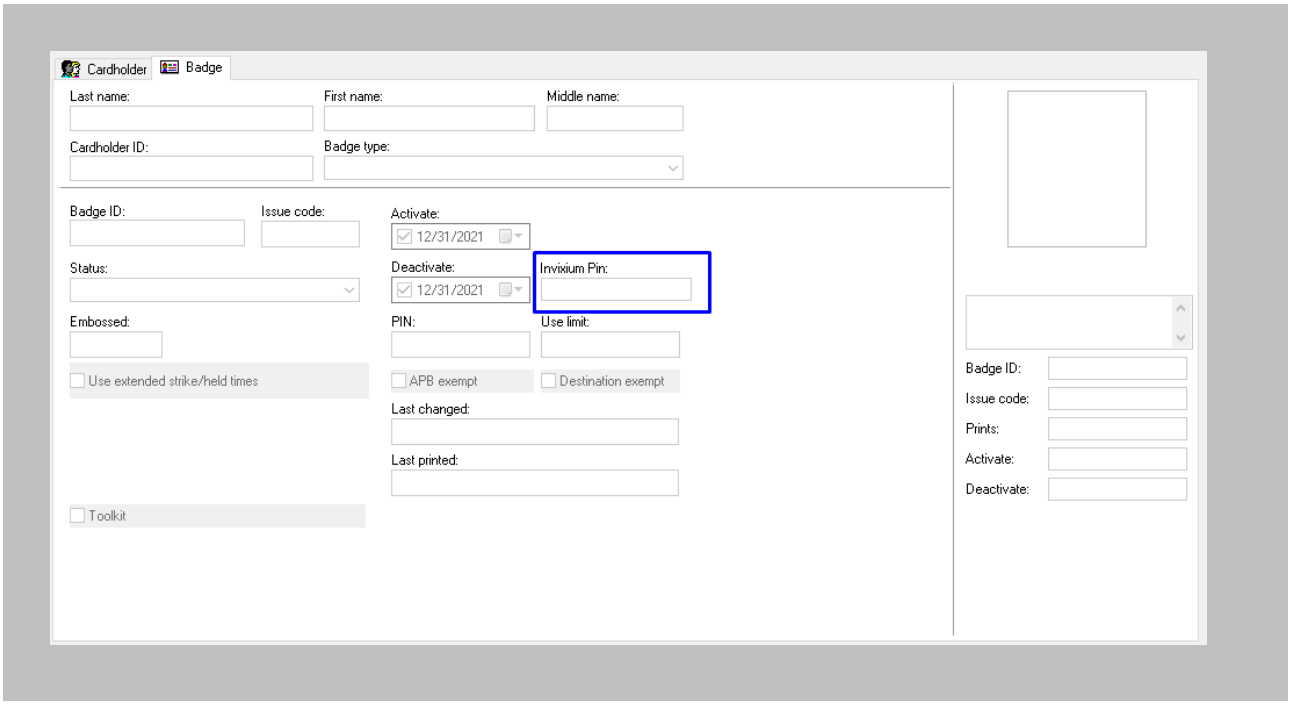


Figure 114: OnGuard - IXM WEB Custom Pin

18. 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 on the right-hand side.

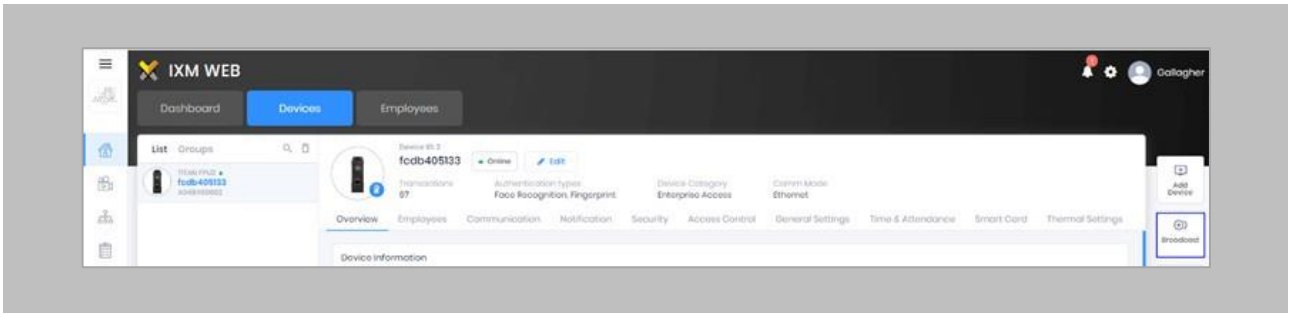


Figure 115: IXM WEB - Broadcast Option

STEP 2

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

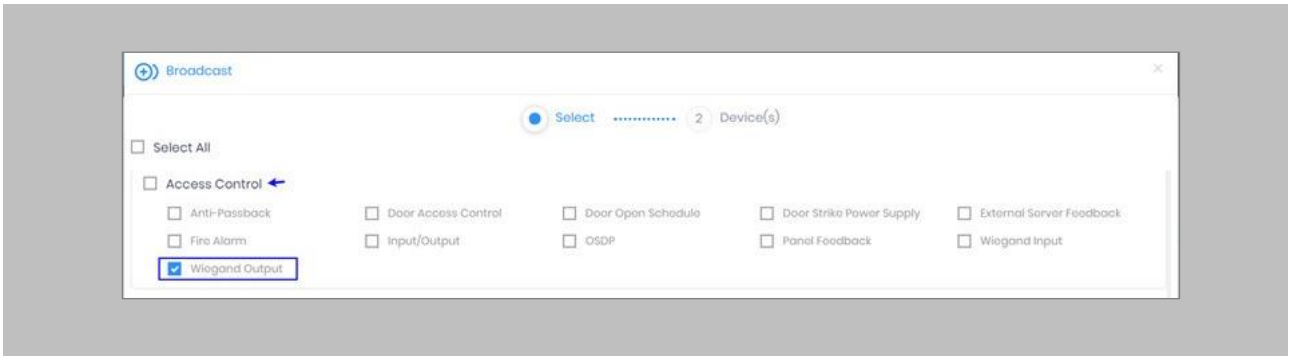


Figure 116: IXM WEB - Wiegand Output Selection in Broadcast

STEP 3

Click **Broadcast.**

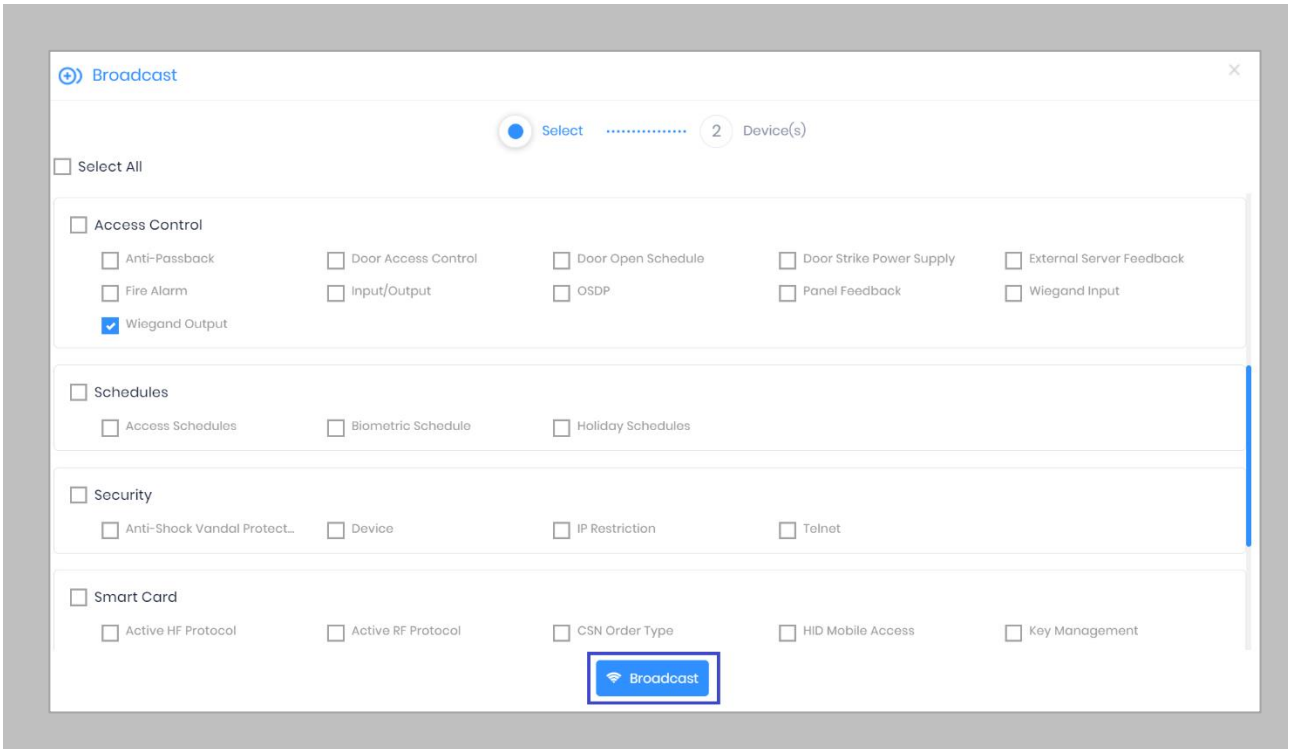


Figure 117: IXM WEB - Broadcast Wiegand Output Settings

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.

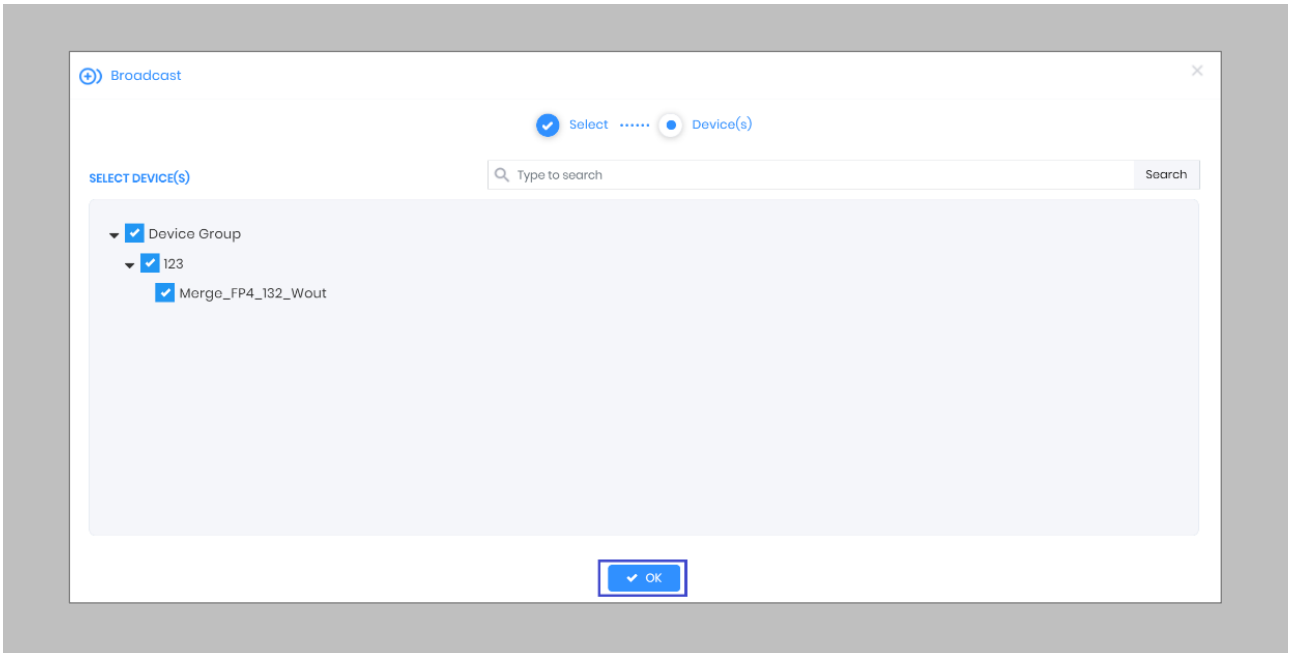


Figure 118: IXM WEB - Broadcast to Devices

Note: The popup will display devices of the same category only.

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**.

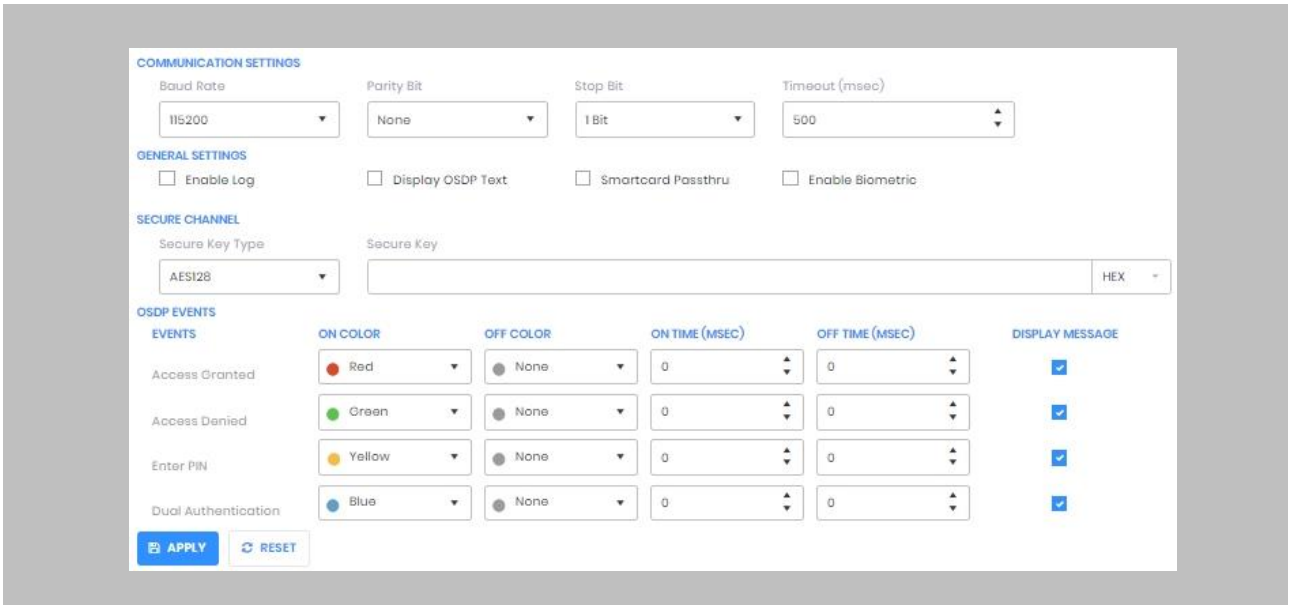


Figure 119: IXM WEB - OSDP Settings

STEP 2

Supply **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 ControlPanel's value.
Stop Bit	The stop bit of the serial communication. The value must be the same as the Access Control Panel's value.
Timeout (msec)	The time duration (500 to 10000 milliseconds) up to which the Device should keep trying to connect to the Access Control Panel. The default timeout duration is 300 milliseconds. On timeout, the Device LCD flashes "Access Denied" message and the "Application Logs" window will show a failure message.
Enable Log	This logs OSDP events for support and debugging purposes. Invixium recommends disabling this feature unless needed.
Smartcard Passthru	When presenting a smart card, the device passes the smart card CSN (Card Serial Number) to the Access Control Panel without taking any other action.
Enable Biometric	Enables biometric template verification.
Secure Channel	The secure key is provided by your Access Control Panel most of the time. However, provisions for manual entry can be added as TEXT or HEX.
Event	The OSDP static events for panel feedback and capture pin are: Access Granted Access Denied Enter Pin Dual Authenticaction – It is an access mode which requires valid access by two authorized cardholders to enter an access zone within a specified time period. This feature is available only if **Multi-User Authentication** feature is enabled and configured. To configure Multi-User Authentication feature, from **Home**, click the **Devices** tab. Select the required Device and navigate to **General Settings**. Click on **Multi-User Authentication** section. On enabling this feature, the following actions will be performed:

	• The Device will request for 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 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 hard-coded 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.

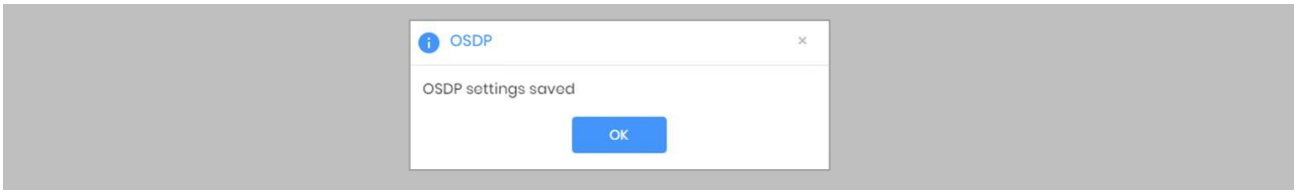


Figure 120: IXM WEB - Save OSDP Settings

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 OnGuard.

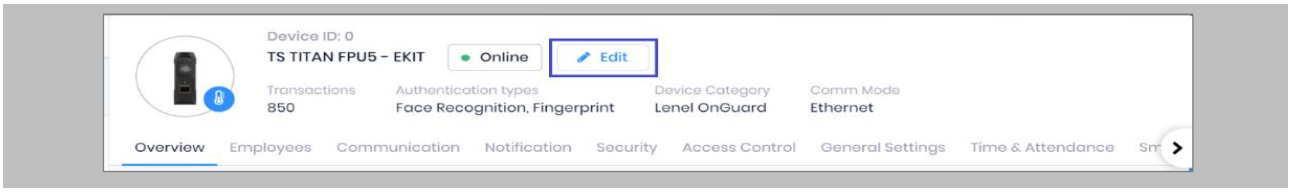


Figure 121: IXM WEB - Edit Device

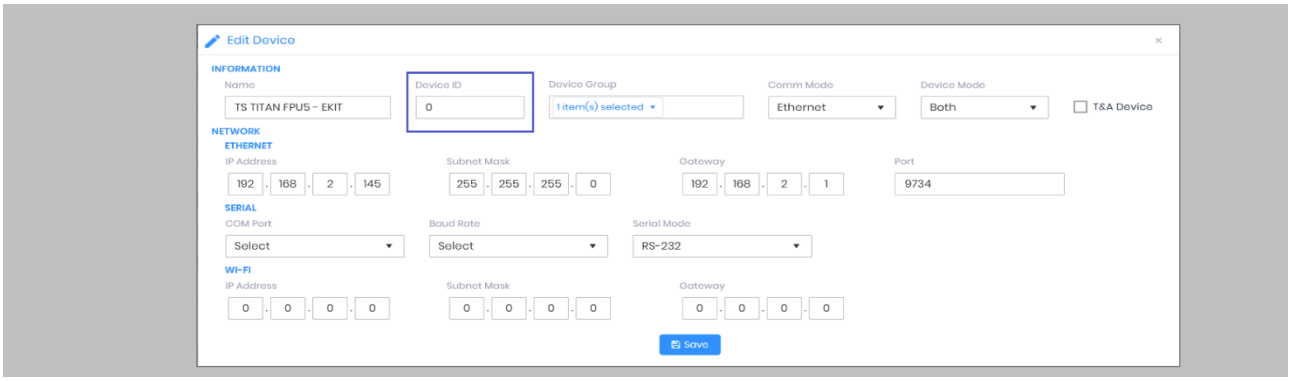


Figure 122: IXM WEB - Edit Device Options

STEP 5

Login to **'System Administration'** → Click '**Access Control**' → **'Readers and Doors'**.

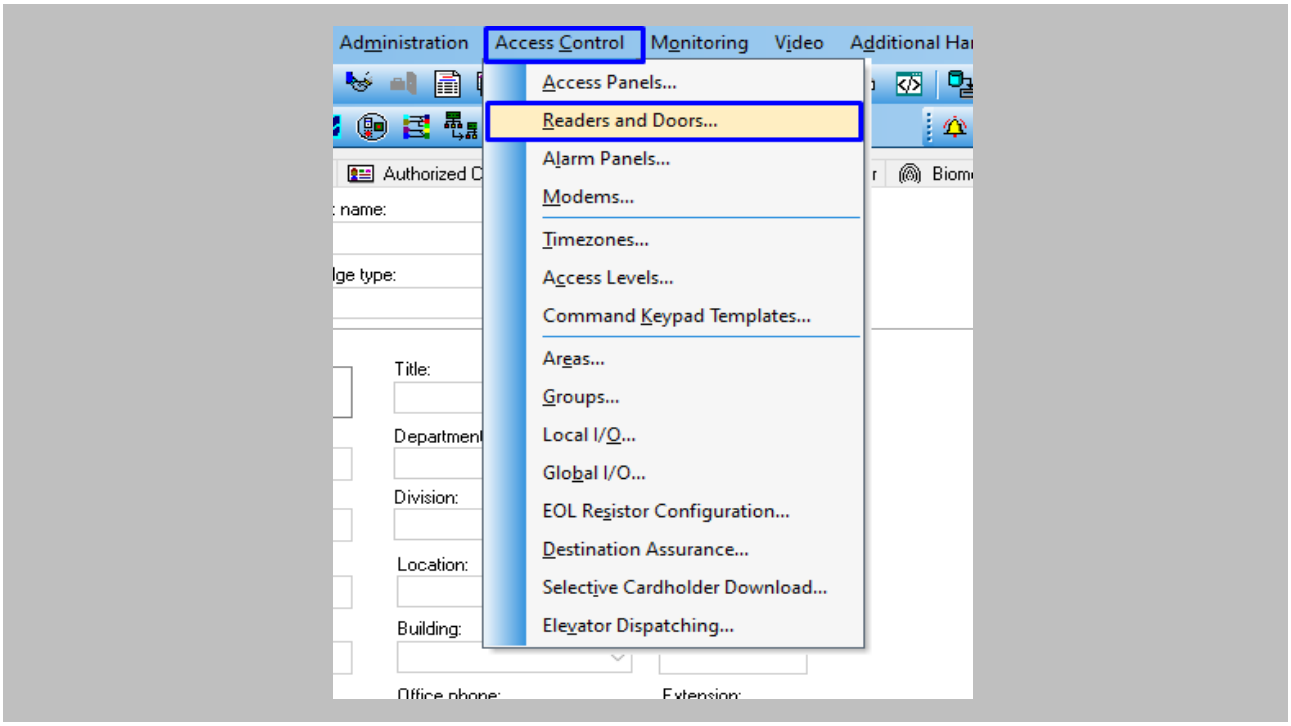


Figure 123: OnGuard - Add OSDP Reader

STEP 6

Add new **'Reader'** → Enter mandatory details → Select **'OSDP Protocol'** as output → Click **OK**.

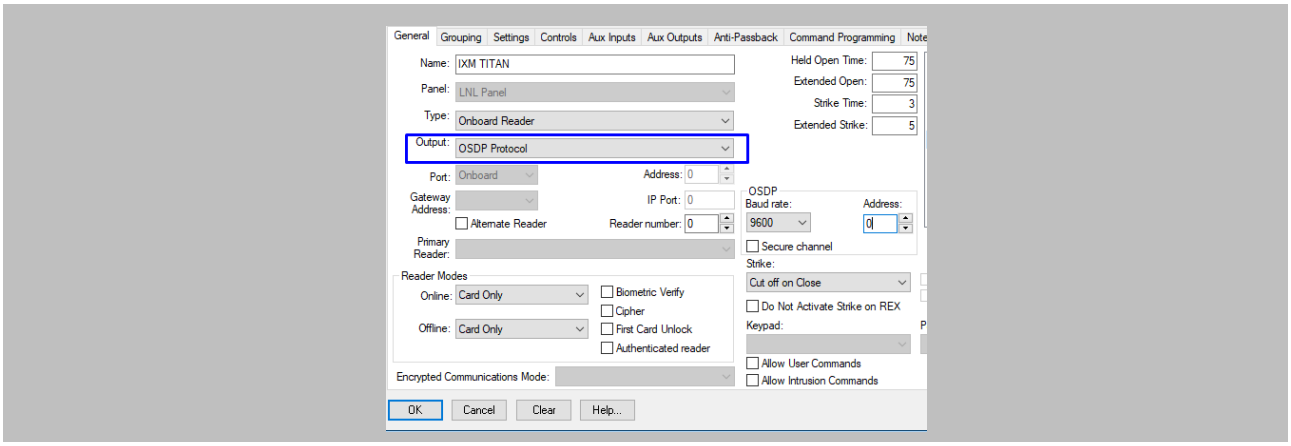


Figure 124: OnGuard - OSDP Reader

Note: The Invixium's reader address should be the same as the OSDP reader address.

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 OnGuard.

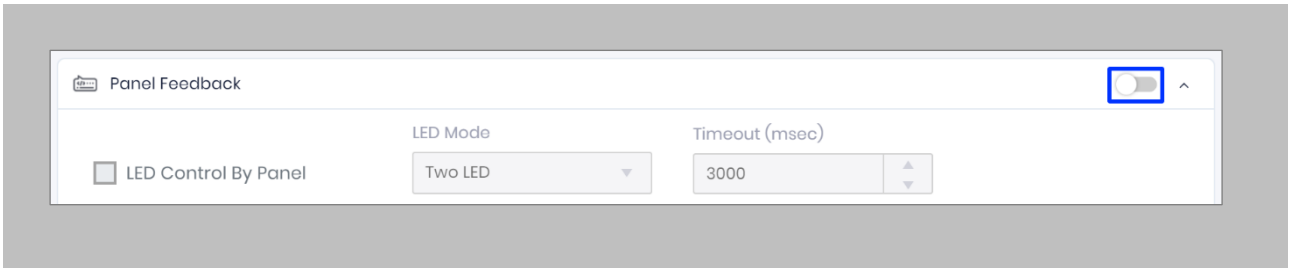


Figure 125: IXM WEB - Disable Panel Feedback

Wiring and Termination

Procedure

EARTH GROUND

For protection against ESD, Invixium recommends the use of a ground connection between each Invixium device to a 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.

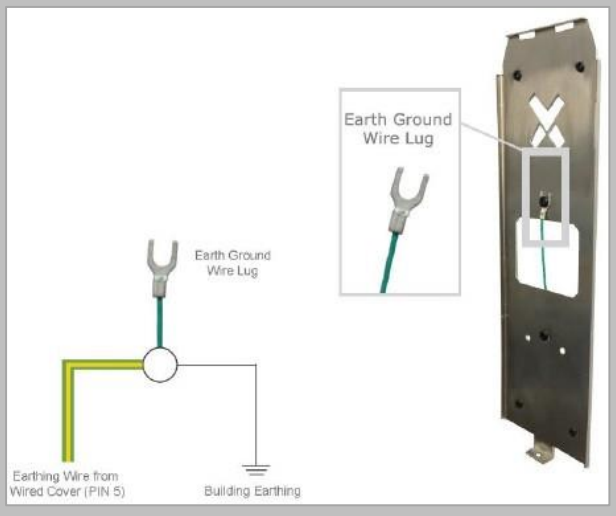


Figure 126: Earth Ground Wiring

Wiring

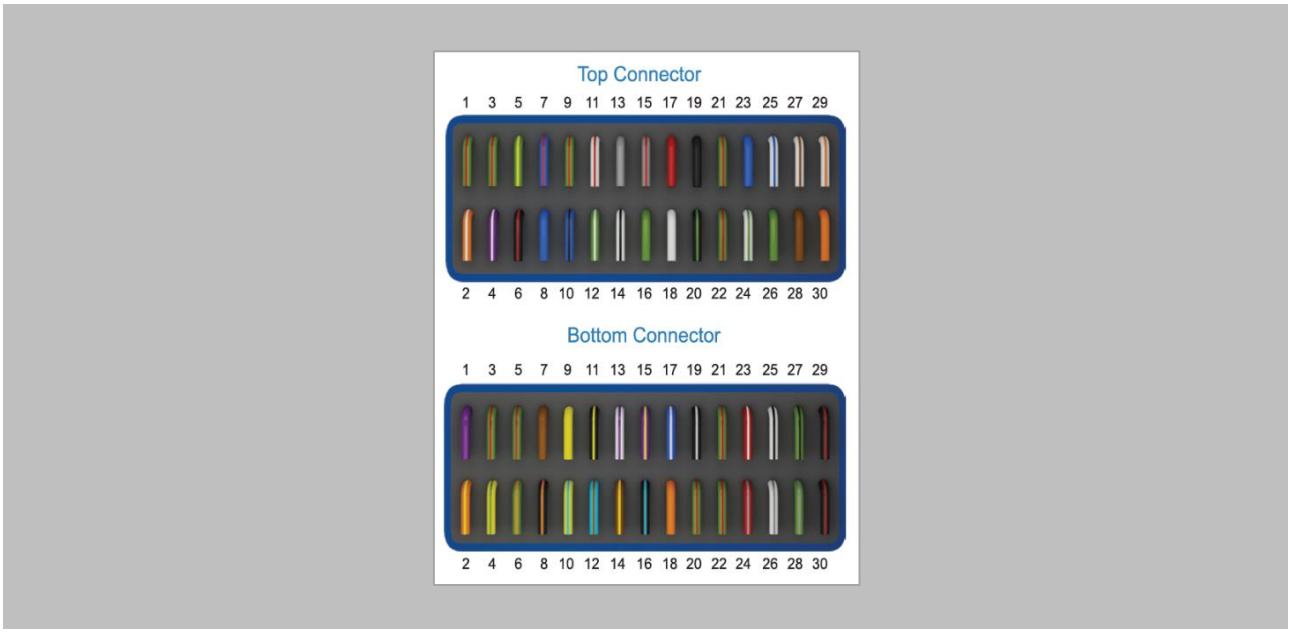
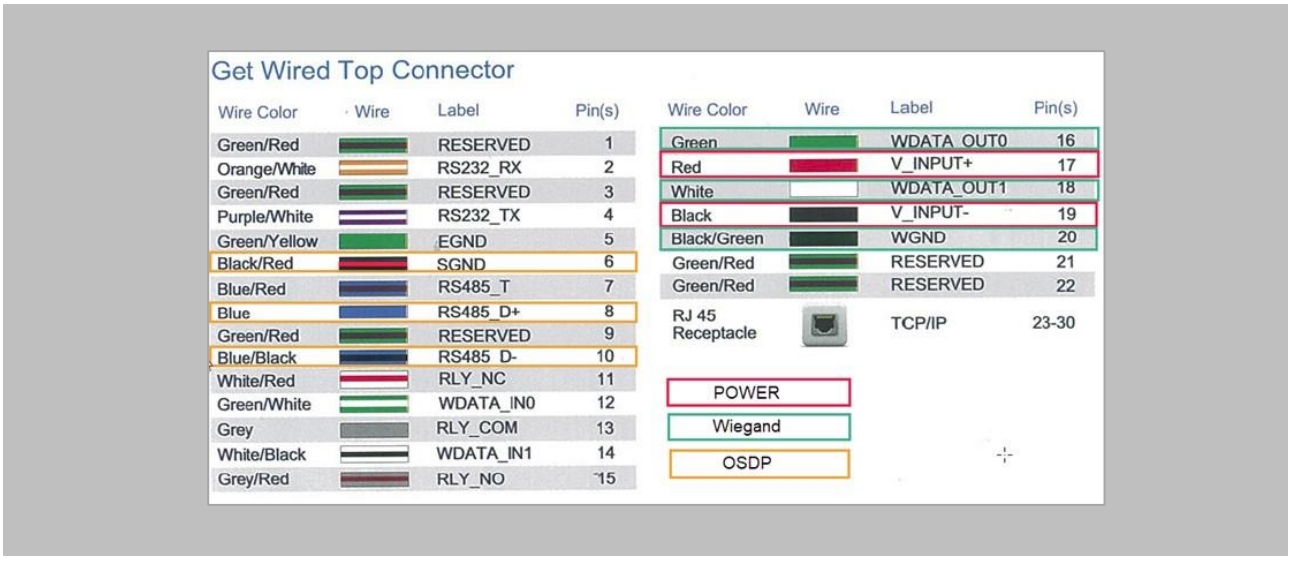


Figure 127: IXM TITAN – Top & Bottom Connector Wiring



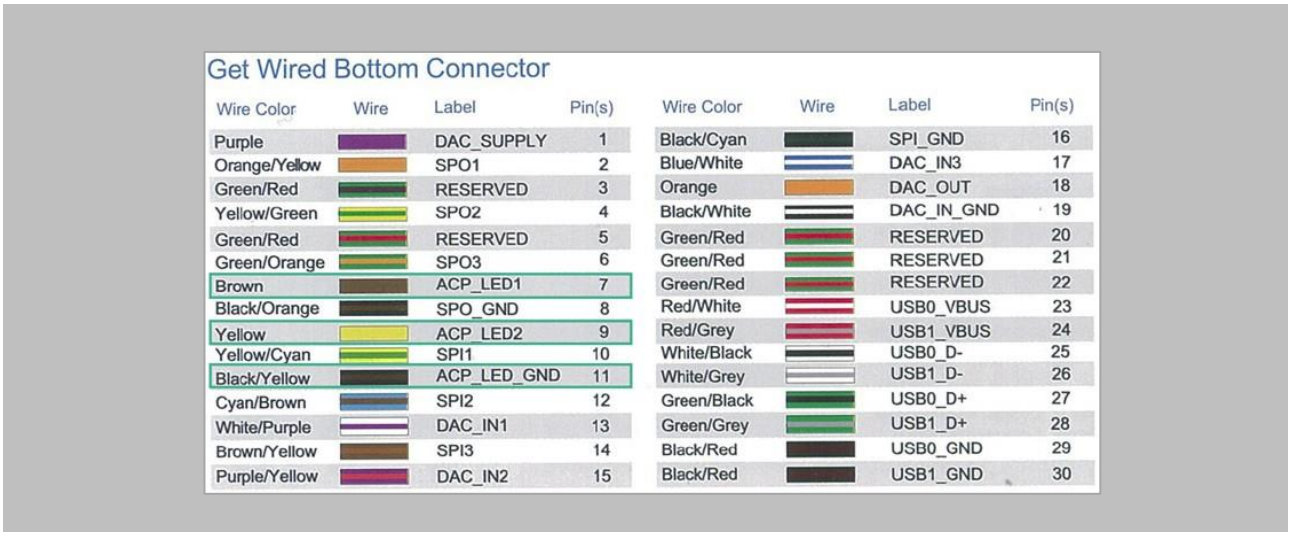


Figure 128: Power, Wiegand & OSDP Wires

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

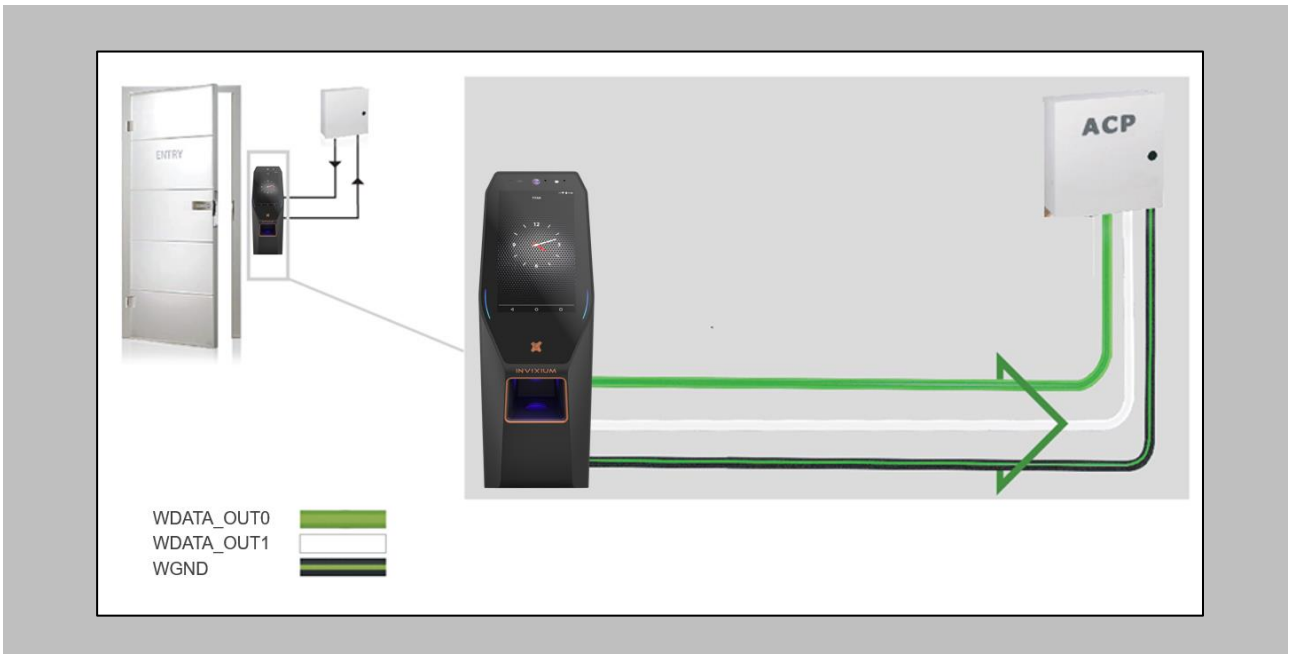


Figure 129: IXM TITAN - Wiegand

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

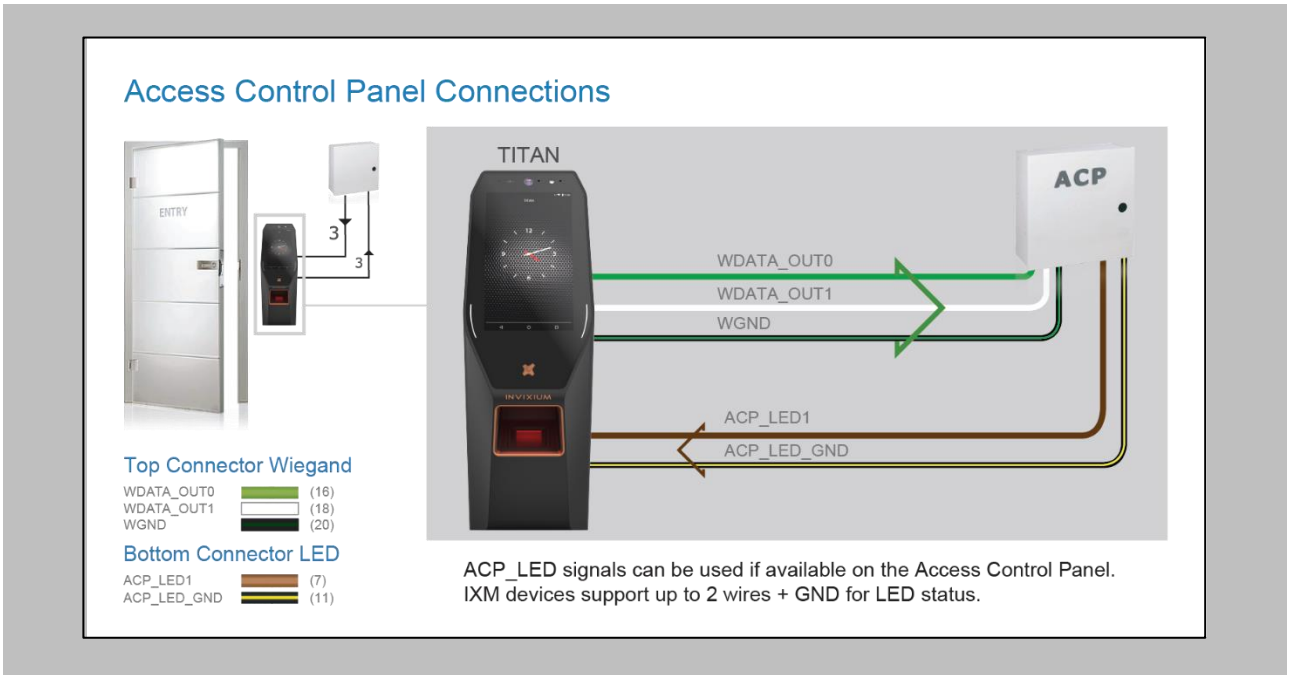


Figure 130: IXM TITAN - Panel Feedback

OSDP Connections

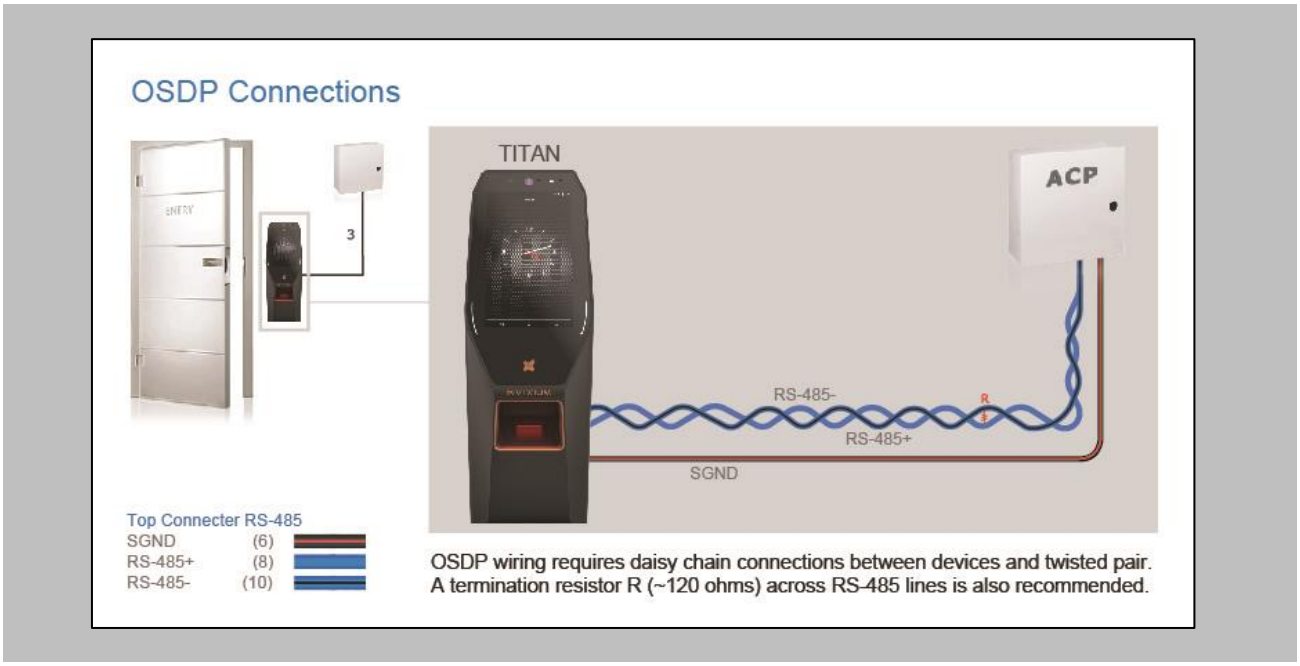


Figure 131: IXM TITAN - OSDP Connections

19. Troubleshooting

Reader Offline from the IXM WEB Dashboard

Note: Confirm Communication of IXM WEB server to Invixium reader.

Procedure

STEP 1

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

STEP 2

Select any device.

STEP 3

Navigate to the **Communication** tab.

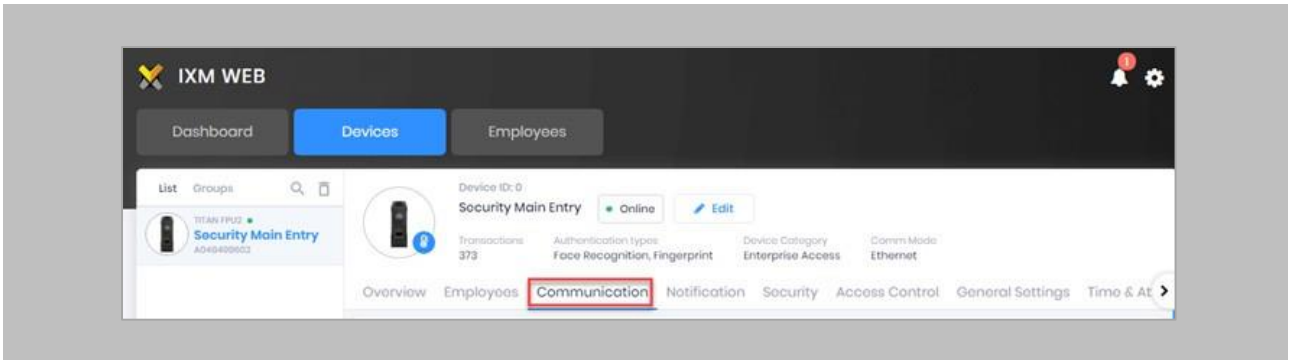


Figure 132: IXM WEB - Device Communication Settings

STEP 4

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

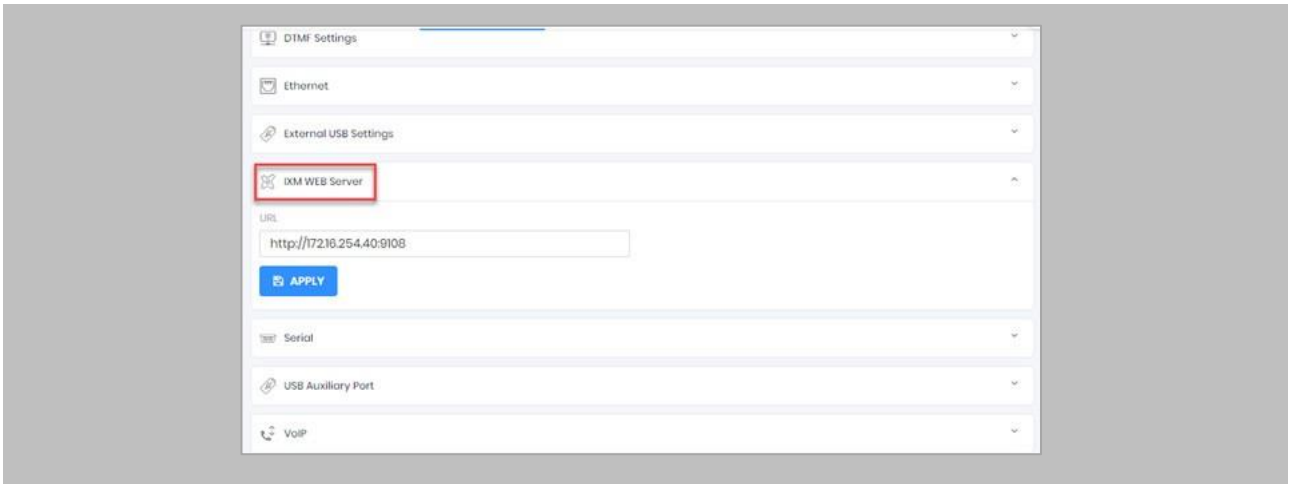


Figure 133: IXM WEB - Server URL Setting

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.

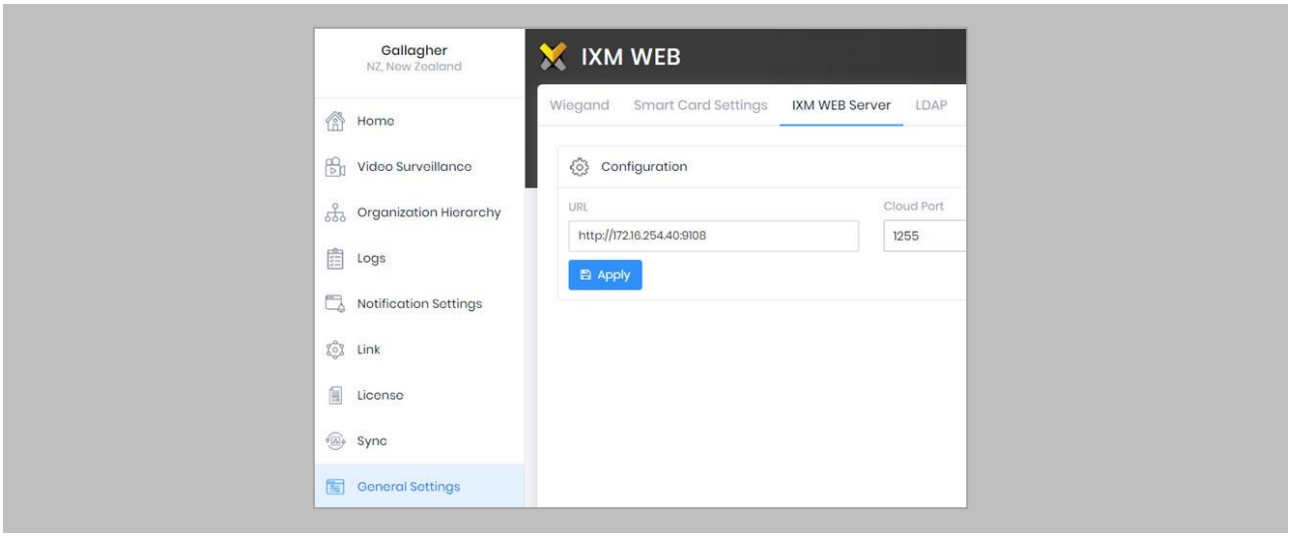


Figure 134: IXM WEB - Server URL Setting from General Settings

Elevated Body Temperature Denied Access but Granted Access in OnGuard

Procedure

STEP 1

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

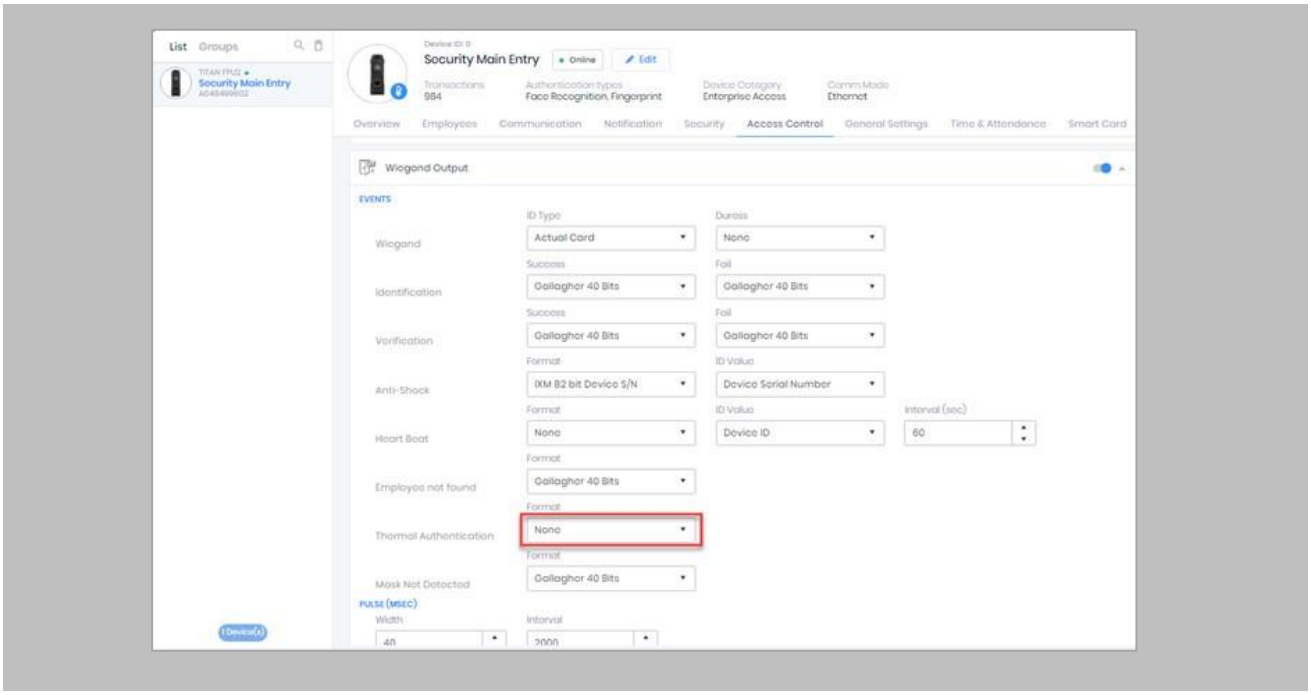


Figure 135: IXM WEB - Thermal Authentication Wiegand Output Event

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.

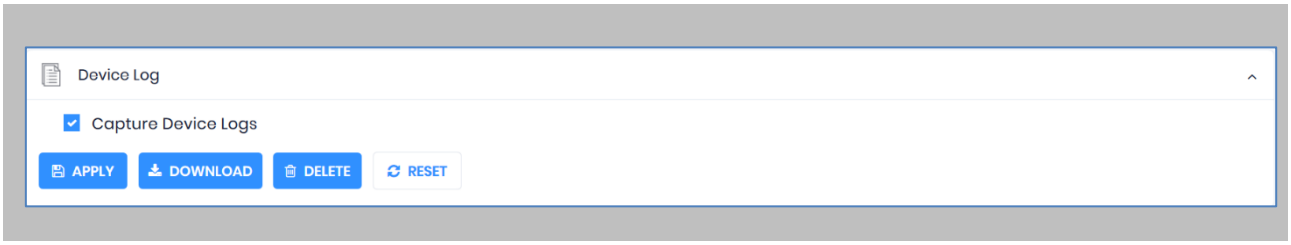


Figure 136: IXM WEB - Enable Device Logs

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

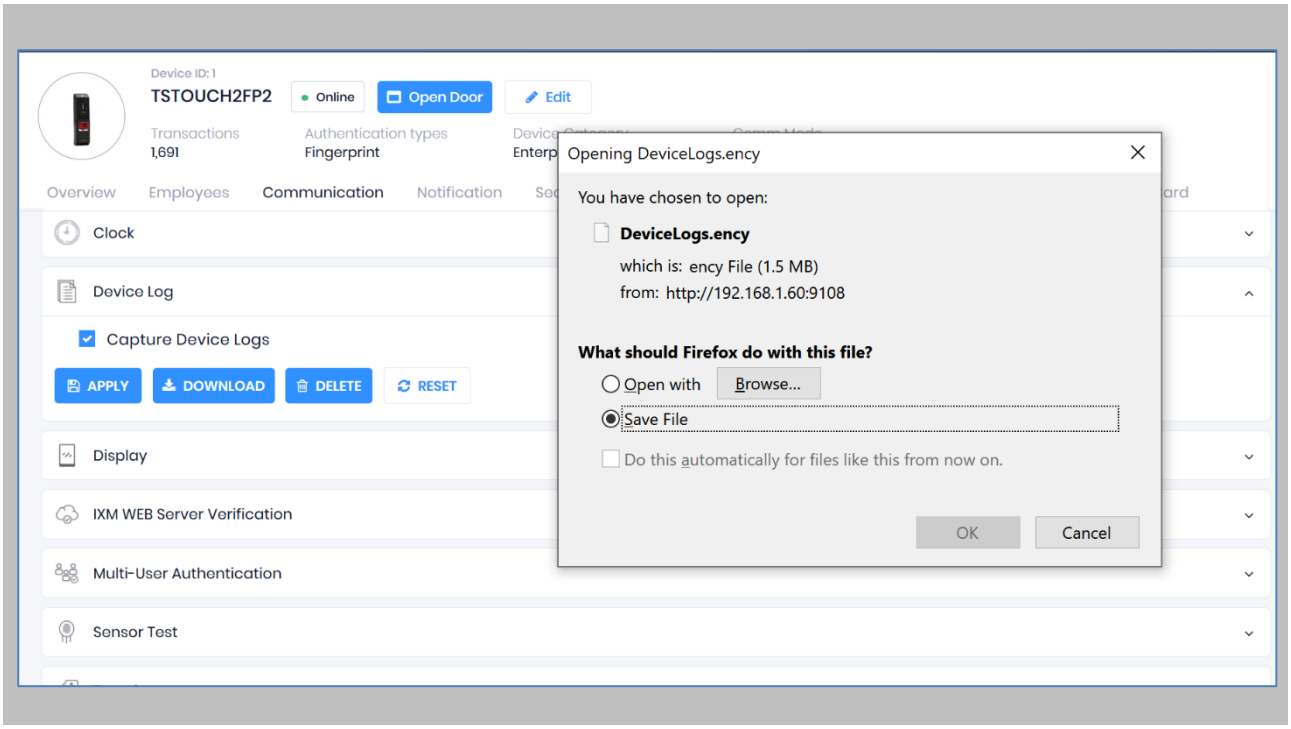


Figure 137: Save Device Log File

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. 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

20. Support

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

21. Disclaimer and Restrictions

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

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

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

Copyright © 2023 Invixium. All rights reserved.