



IXM WEB Integration with Lenel-S2 NetBox

Installation Instructions

V2.0



Table of Contents

1. Introduction	8
Purpose	8
Summary of key features related to this IXM WEB and NetBox Integration	8
Description	8
Acronyms	8
Field Mappings	8
2. Compatibility	10
Invixium Readers	10
Software Requirements	10
Other Requirements	10
Compatibility Matrix for IXM WEB & NetBox Integration	11
3. Checklist	12
4. Task List Summary	12
5. Prerequisites for NetBox and IXM WEB Integration	13
Enable S2 NetBox API	13
Enable Card Format	16
6. Prerequisites for Installing Invixium IXM WEB Software	18
Acquiring IXM WEB Activation Key	18
Setting Up SQL instance	20
Minor Checklist and Considerations	24
7. Installing IXM WEB	25
Software Install	25
8. Configuring Email Settings using IXM WEB	33
Email Setting Configuration	33
9. Software and Module Activation	38
IXM WEB Activation	38
NetBox Module Activation	41
10. Configuring IXM Link for Lenel-S2	44



11. Create System User(s) for Biometric Enrollment.....	49
Creating System User(s) for Biometric Enrollment	49
12. Add and Configure Invixium Readers.....	53
Adding an Invixium Reader in IXM WEB	53
13. Adding an Invixium Device to a Device Group.....	58
Configuring Wiegand to Assign Invixium Readers.....	59
Assign Wiegand to Invixium Readers	61
Configuring Panel Feedback with Lenel-S2.....	66
Configuring Thermal Settings	68
Thermal Calibration.....	72
Test Calibration Options.....	76
Change Temperature Unit Settings	77
Configuring Mask Authentication Settings	78
14. Enrollment Best Practices	82
Fingerprint Enrollment Best Practices.....	82
Avoid Poor Fingerprint Conditions	82
Fingerprint Image Samples.....	83
Fingerprint Imaging Do's and Don'ts.....	84
Finger Vein Enrollment Best Practices	85
Face Enrollment Best Practices	86
15. Appendix	87
Installing Invixium IXM WEB with Default Installation using SQL Server 2014	87
Pushing Configuration to Multiple Invixium Readers	91
Configuring for OSDP Connection	94
Wiring and Termination	100
Wiring	101
Wiegand Connection.....	103
Wiegand Connection with Panel Feedback	104
OSDP Connections	105
16. Troubleshooting.....	106
Reader Offline from the IXM WEB Dashboard	106
Elevated Body Temperature Denied Access but Granted Access in Security Center	109
Logs in IXM WEB Application	110
Unable to connect to the Lenel-S2 Server	112
Can not find cardholder(s) in IXM WEB after importing data from Netbox	114



17. Support	119
18. Disclaimer and Restrictions	119

List of Figures

Figure 1: Configuring S2 NetBox API – Site Settings	13
Figure 2: Configuring S2 NetBox API – Network Controller.....	14
Figure 3: NetBox – Enabling S2 NetBox API.....	15
Figure 4: Netbox – Configuring Card/Keypad Format.....	16
Figure 5: Netbox – Enable Card/Keypad Format.....	17
Figure 6: IXM WEB Online Request Form.....	18
Figure 7: Sample Email After Submitting Online Request Form	19
Figure 8: SQL New Login.....	21
Figure 9: SQL Login Properties.....	22
Figure 10: SQL Server Roles	23
Figure 11: IXM WEB Installer	25
Figure 12: Advanced Options in IXM WEB Installer	26
Figure 13: Invixium Fingerprint Driver Installation Message	27
Figure 14: IXM WEB Installation Progress	27
Figure 15: IXM WEB Installation Completed	28
Figure 16: IXM WEB Icon - Desktop Shortcut	29
Figure 17: IXM WEB Database Configuration	29
Figure 18: IXM WEB Administrator User Configuration	30
Figure 19: IXM WEB Login Page	31
Figure 20: Configure Email	33
Figure 21: IXM WEB - SMTP Settings.....	34
Figure 22: IXM WEB - Save Email Settings	35
Figure 23: IXM WEB - Test Connection	35
Figure 24: IXM WEB - Enter Email ID	36
Figure 25: IXM WEB - Forgot Password	37
Figure 26: IXM WEB - Enter Login Credentials	38
Figure 27: IXM WEB - License Setup.....	39
Figure 28: IXM WEB - Online Activation.....	40
Figure 29: IXM WEB – Lenel-S2 Link Activation	41
Figure 30: Lenel-S2 License Key Email	42



Figure 31: IXM WEB - Activate Lenel-S2 Link License	43
Figure 32: IXM WEB - Link Menu.....	44
Figure 33: IXM WEB - Enable Lenel-S2 Link Module	45
Figure 34: IXM WEB – Link Settings Saved	47
Figure 35: IXM WEB - Sync Activities	47
Figure 36: IXM WEB - Create System User	49
Figure 37: IXM WEB - Add New System User.....	50
Figure 38: IXM WEB - New System User.....	51
Figure 39: IXM WEB - Save System User.....	52
Figure 40: IXM WEB - Devices Tab	53
Figure 41: IXM WEB - Search Device Using IP Address.....	54
Figure 42: IXM WEB - Register Device	55
Figure 43: IXM WEB - Device Registration Complete	56
Figure 44: IXM WEB - Dashboard, Device Status	57
Figure 45: IXM WEB - Assign Device Group.....	58
Figure 46: IXM WEB - Create Wiegand Format	59
Figure 47: IXM WEB - Create Custom Wiegand Format	60
Figure 48: IXM WEB - Custom Wiegand Format.....	60
Figure 49: IXM WEB – Custom Wiegand Format Created.....	61
Figure 50: IXM WEB - Upload Wiegand Format.....	61
Figure 51: IXM WEB - Navigate to Access Control Tab	62
Figure 52: IXM WEB - Wiegand Output.....	63
Figure 53: IXM WEB - Save Output Wiegand.....	64
Figure 54: IXM WEB - Panel Feedback.....	66
Figure 55: IXM WEB - Configuring Panel Feedback in IXM WEB.....	67
Figure 56: IXM WEB - Save Panel Feedback.....	67
Figure 57: IXM WEB - Thermal Settings	68
Figure 58: IXM WEB - Save Thermal Settings	71
Figure 59: IXM WEB - Thermal Calibration Settings.....	72
Figure 60: IXM WEB - Save Thermal Calibration Settings.....	73
Figure 61: IXM WEB - Capture Thermal Data	74
Figure 62: IXM WEB - Save Captured Thermal Data	75
Figure 63: IXM WEB - Test Thermal Calibration	76
Figure 64: IXM WEB - Option to Change Temperature Unit	77
Figure 65: IXM WEB - Save Temperature Unit Setting.....	78
Figure 66: IXM WEB - Mask Authentication Settings.....	79
Figure 67: IXM WEB - Save Mask Settings.....	81



Figure 68: Fingerprint Enrollment Best Practices	82
Figure 69: Fingerprint Images Samples	83
Figure 70: Finger Vein Enrollment Best Practices	85
Figure 71: Face Enrollment Best Practices	86
Figure 72: Install IXM WEB	87
Figure 73: Loading SQL Express & Installation Progress	88
Figure 74: IXM WEB - Shortcut Icon on Desktop	89
Figure 75: IXM WEB - Configuring IXM WEB Database	89
Figure 76: IXM WEB - Select Database Name	90
Figure 77: IXM WEB - Server URL format	90
Figure 78: IXM WEB - Broadcast Option	91
Figure 79: IXM WEB - Wiegand Output Selection in Broadcast	91
Figure 80: IXM WEB - Broadcast Wiegand Output Settings	92
Figure 81: IXM WEB - Broadcast to Devices	93
Figure 82: IXM WEB - OSDP Settings	94
Figure 83: IXM WEB - Save OSDP Settings	98
Figure 84: IXM WEB - Edit Device	98
Figure 85: IXM WEB - Edit Device Options	99
Figure 86: IXM WEB - Disable Panel Feedback	99
Figure 87: Earth Ground Wiring	100
Figure 88: IXM TITAN – Top & Bottom Connector Wiring	101
Figure 89: Power, Wiegand & OSDP Wires	102
Figure 90: IXM TITAN - Wiegand	103
Figure 91: IXM TITAN - Panel Feedback	104
Figure 92: IXM TITAN - OSDP Connections	105
Figure 93: IXM WEB - Device Communication Settings	106
Figure 94: IXM WEB - Server URL Setting	107
Figure 95: IXM WEB - Server URL Setting	107
Figure 96: IXM WEB - Server URL Setting from General Settings	108
Figure 97: IXM WEB - Server URL Setting from General Settings	108
Figure 98: IXM WEB - Thermal Authentication Wiegand Output Event	109
Figure 99: IXM WEB - Thermal Authentication Wiegand Output Event	109
Figure 100: IXM WEB - Enable Device Logs	110
Figure 101: Save Device Log File	110
Figure 102: Save Device Log File	110
Figure 103: IXM WEB - Licence Module	112
Figure 104: IXM WEB – Lenel-S2 Link Module	113



Figure 105: NetBox – Enabling S2 NetBox API.....	114
Figure 106: Lenel-S2 NetBox – Personal Information	115
Figure 107: IXM WEB – Card Format	116
Figure 108: Lenel-S2 NetBox – Card Format	117
Figure 109: Lenel-S2 NetBox – Personal Information	118

List of Tables

Table 1: Compatibility Matrix for IXM WEB & NetBox Integration	11
Table 2: Task List Summary	12
Table 3: System Related Checklist	24
Table 4: Port Information	24
Table 5: IXM WEB - OSDP Configuration Options	96
Table 6: IXM WEB - OSDP Text Options	97
Table 7: Logs Folder Location.....	111



1. Introduction

Purpose


This document outlines the process of configuring the software integration between Lenel-S2 NetBox (NetBox) and Invixium’s IXM WEB.

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

- S2 NetBox API to support NetBox integration
- ‘Sync All’ feature to resynchronize the database from NetBox to 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 Lenel-S2 NetBox 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 S2 NetBox by using S2 NetBox API.

Acronyms

Acronym	Description
ACPCS	Access Control Panel Configuration Software
NetBox	Lenel-S2 NetBox
IXM	Invixium

Field Mappings

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

NetBox Field	IXM Field	Notes
ID#	User ID	NetBox allows alphanumeric & special characters in ID# while IXM WEB



		allows only alphanumeric with a maximum length of 64 characters. Hence, IXM WEB will sync only those users whose ID# value is compatible with IXM WEB.
First name	First Name	
Last name	Last Name	
Telephone2 (Another Contact tab)	Home Phone	
Telephone (Another Contact tab)	Office Phone	
Phone (Contact tab)	Mobile	
Email (Contact tab)	Email	
Activation Date/Time & Expiration Date/Time	Start Date & End Date	If both Activation and Expiration Date times are specified, then they are synced from NetBox to IXM WEB
PIN	PIN	
Hot Stamp	Prox ID	
Photo	Photo	
Location (Contact tab)	Location	
Deleted	Suspend User	NetBox does not delete users, so records deleted in IXM WEB are flagged as deleted in NetBox



Note: Multiple Cards - NetBox can have multiple cards per user but IXM WEB supports only one Prox card. Link selects one of the cards with the CARD FORMAT specified in configuration and one which is active/temporary and not expired.



2. Compatibility

Invixium Readers


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

Software Requirements

Application	Version
Lenel-S2 NetBox	V4.9
Invixium IXM WEB	2.3.0.0
Operating Systems	Windows 10 (Build 1709+) Professional Version Windows Server 2016 Standard Windows Server 2019 Supported but not recommended: (legacy) <i>Windows 8.1</i> <i>Windows Server 2012 R2</i> <i>Windows Server 2012</i>
Microsoft .NET Framework	.NET Framework 4.8
Database Engine	SQL Server 2016+ Supported but not recommended: (legacy) SQL server 2014 Express Edition (Default Installation)
Internet Information Services (IIS)	Microsoft® Internet Information Services version 7.5 or higher
Web Browser	Google Chrome Mozilla Firefox Microsoft Edge (Internet Explorer not recommended)

Other Requirements

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

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

Compatibility Matrix for IXM WEB & NetBox Integration

IXM WEB version	NetBox version	Compatible
IXM WEB 2.2.57.0	v4.9	Yes
IXM WEB 2.2.57.0	v4.9	Yes
IXM WEB 2.2.224.0	v4.9	Yes
IXM WEB 2.2.224.0	v4.9	Yes
IXM WEB 2.2.252.0	v4.9	Yes
IXM WEB 2.2.330.0	v4.9	Yes
IXM WEB 2.3.0.0	v4.9	Yes

Table 1: Compatibility Matrix for IXM WEB & NetBox Integration

3. Checklist

Item List	Interface
Enable S2 NetBox API	NetBox
IXM WEB Activation ID	Invixium
SQL Instance on SQL Server 2016+	Invixium
Install IXM WEB Application	Invixium
IXM WEB and IXM Link Activation	Invixium
Configure IXM Link to NetBox	Invixium
Configure Invixium Reader	Invixium
Face or Finger Enrollment	Invixium

4. Task List Summary

Task	IXM WEB Application Task List using IXM WEB	Lenel-S2 NetBox Task List using NetBox
1	Activate IXM WEB and IXM Link for NetBox	Enable S2 NetBox API
2	Configure IXM Link for NetBox	First time enrollment configuration
3	Register IXM Devices and configure settings as per the requirement	Enroll cardholder biometric (Face, fingerprint, finger vein)
4	Configure Weigand or OSDP settings in device for integration	Monitor Events and Generate Report
5	Assign a specific Device Group to the device	

Table 2: Task List Summary

5. Prerequisites for NetBox and IXM WEB Integration

Enable S2 NetBox API

Procedure

STEP 1

Browse Lenel-S2 server IP address.

STEP 2

Enter valid login and password for authentication.

STEP 3

Navigate to **Configuration** → **Site Settings**.

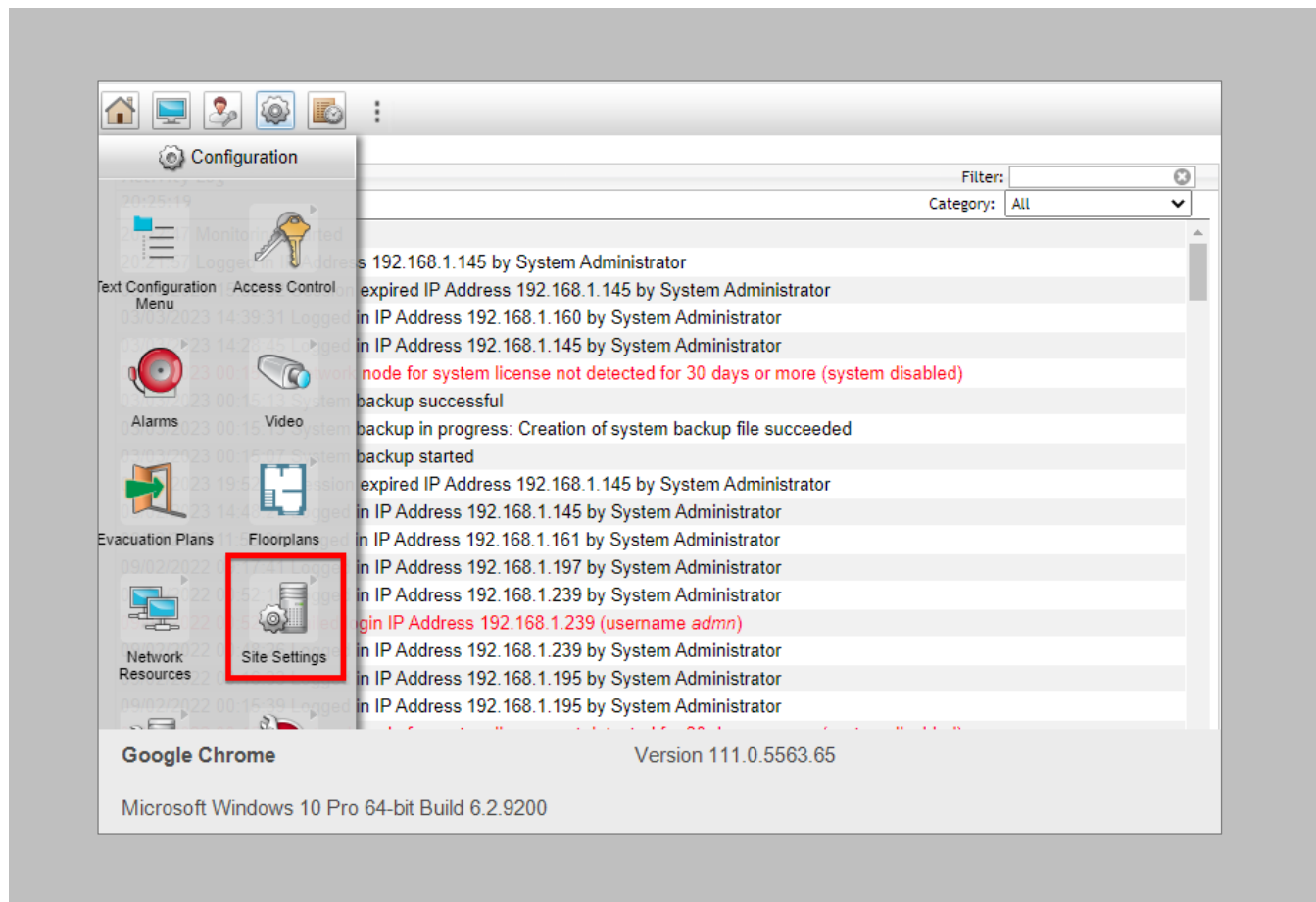


Figure 1: Configuring S2 NetBox API – Site Settings



STEP 4

Under [Site Settings](#), click on [Network Controller](#).

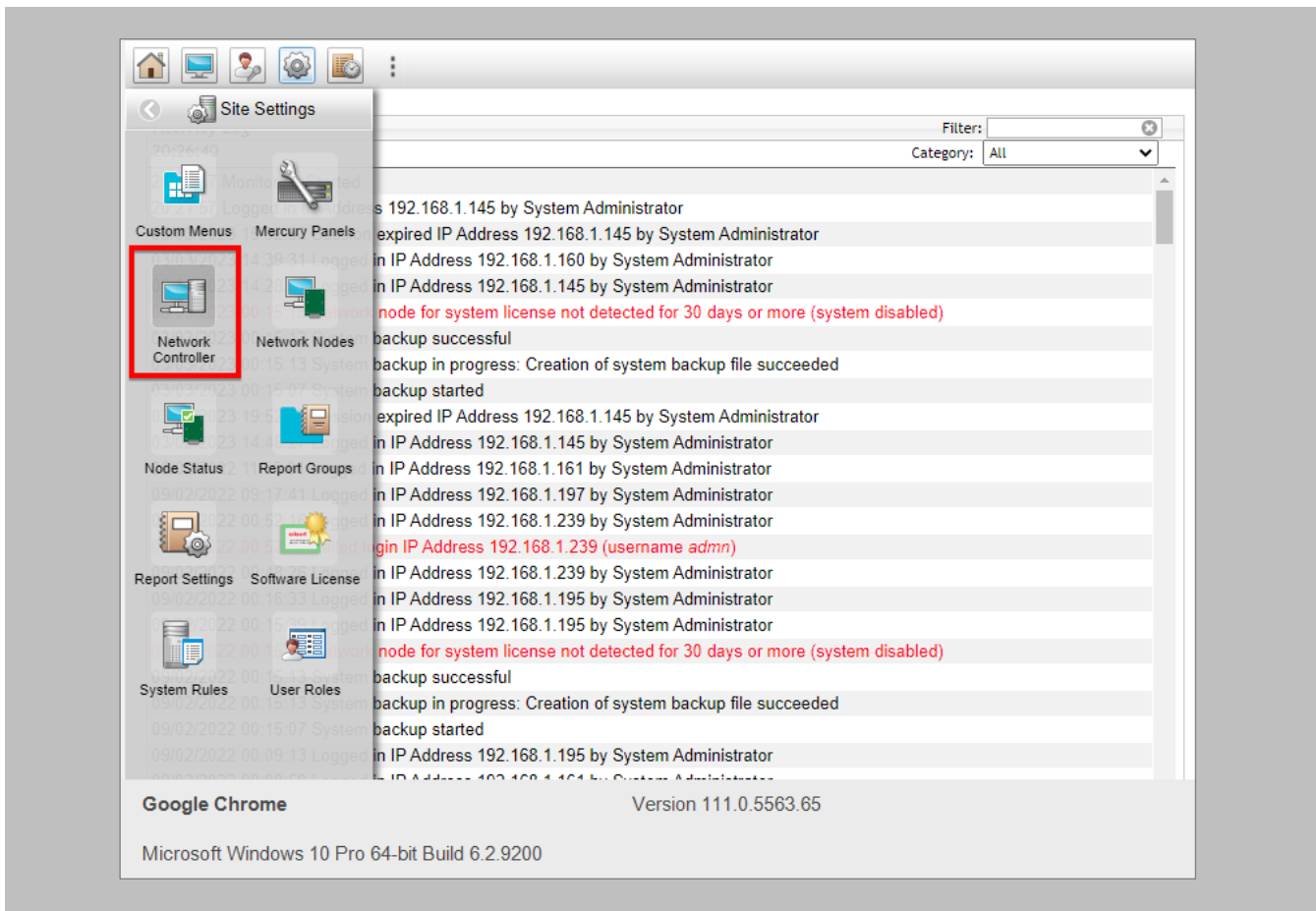


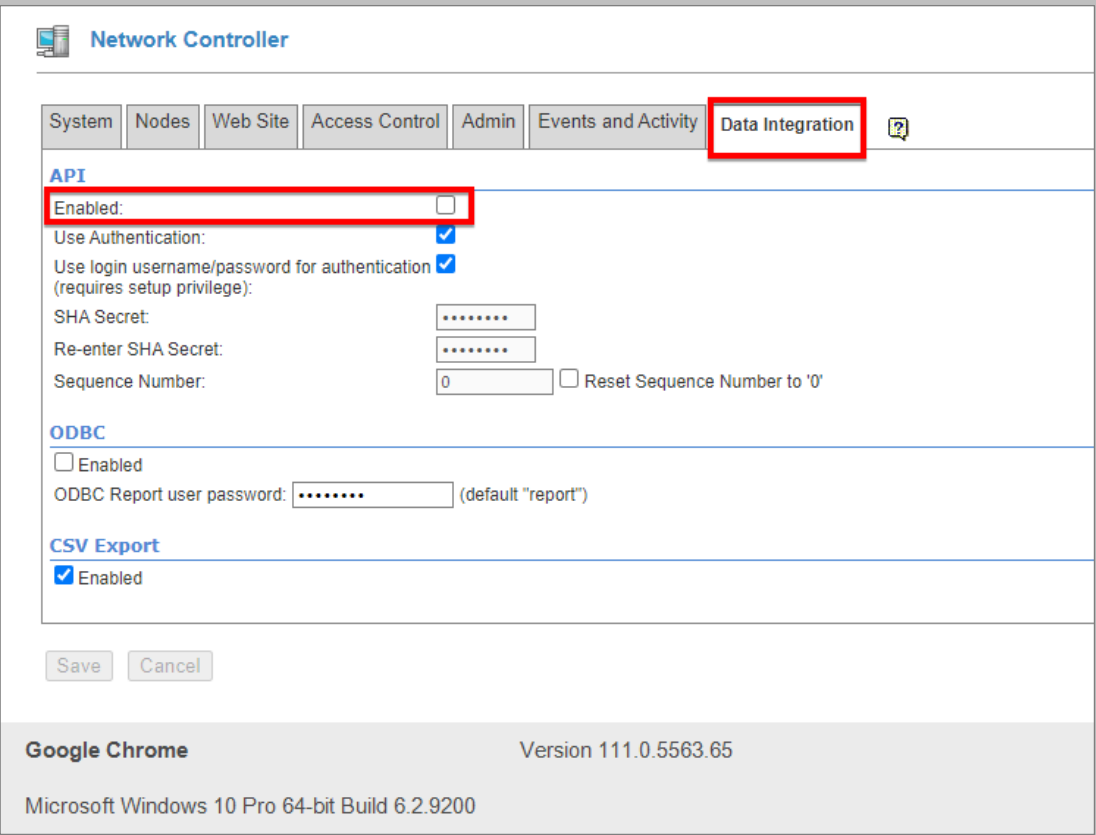
Figure 2: Configuring S2 NetBox API – Network Controller

STEP 5

Navigate to [Data Integration tab](#).

STEP 6

Under **API** section; select “Enabled” and **Save** the settings.



The screenshot shows the NetBox Network Controller interface. The 'Data Integration' tab is selected and highlighted with a red box. Under the 'API' section, the 'Enabled' checkbox is also highlighted with a red box. Other settings include 'Use Authentication' (checked), 'Use login username/password for authentication' (checked), 'SHA Secret' (masked), 'Re-enter SHA Secret' (masked), 'Sequence Number' (0), and 'Reset Sequence Number to '0'' (unchecked). The 'ODBC' section has 'Enabled' (unchecked) and 'ODBC Report user password' (masked). The 'CSV Export' section has 'Enabled' (checked). 'Save' and 'Cancel' buttons are at the bottom.

Network Controller

System | Nodes | Web Site | Access Control | Admin | Events and Activity | **Data Integration** ⓘ

API

Enabled:

Use Authentication:

Use login username/password for authentication (requires setup privilege):

SHA Secret:

Re-enter SHA Secret:

Sequence Number: Reset Sequence Number to '0'

ODBC

Enabled

ODBC Report user password: (default "report")

CSV Export

Enabled

Save Cancel

Google Chrome Version 111.0.5563.65
Microsoft Windows 10 Pro 64-bit Build 6.2.9200

Figure 3: NetBox – Enabling S2 NetBox API

Enable Card Format

Procedure

STEP 1

Navigate to **Configuration** → **Text Configuration Menu**.

STEP 2

Under **Access Control**, click on **Card/Keypad Formats**.

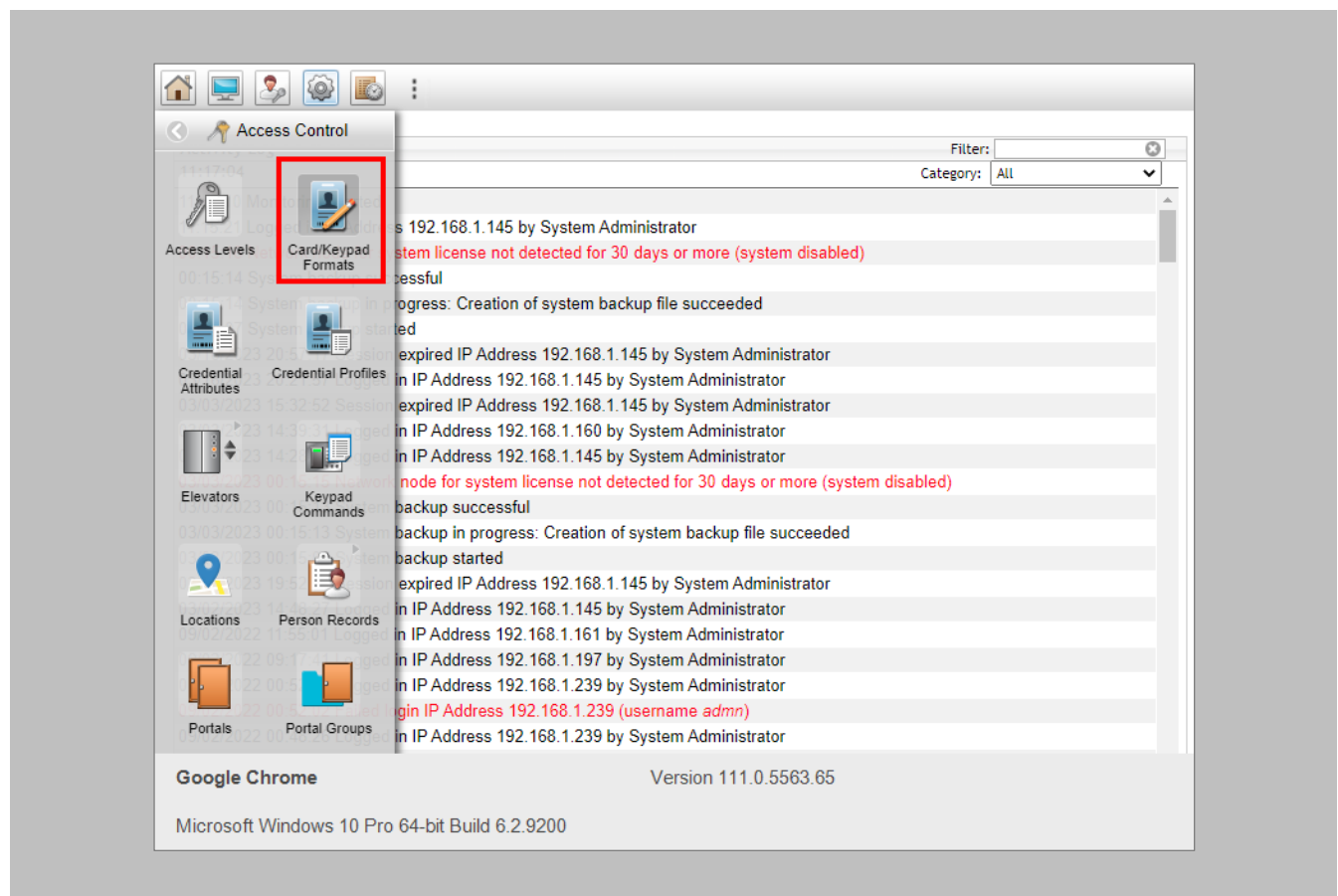


Figure 4: Netbox – Configuring Card/Keypad Format

STEP 3

Select Card /Keypad Format from the dropdown list and select “Enabled”.

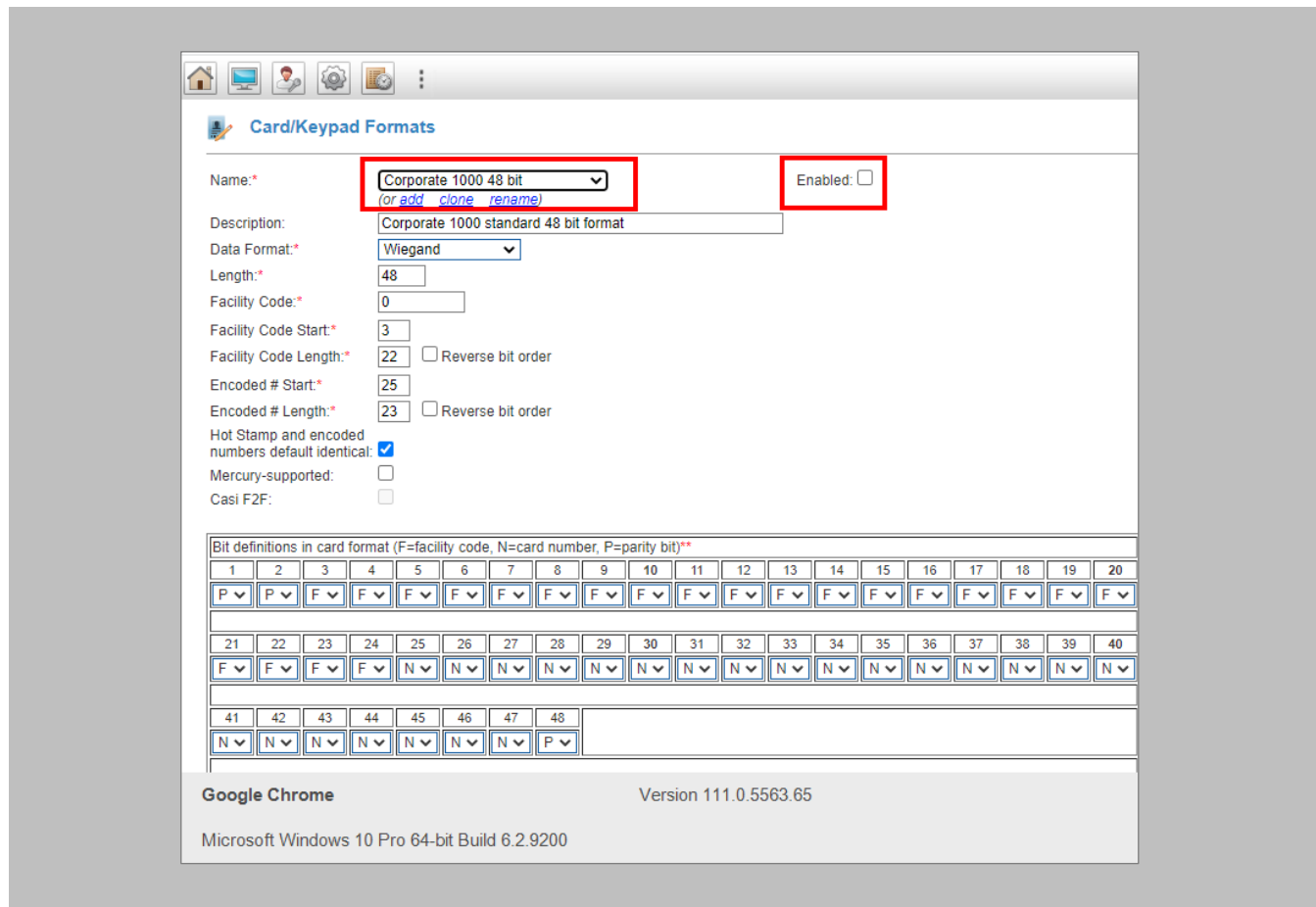


Figure 5: Netbox – Enable Card/Keypad Format

STEP 4

Save the settings.

6. Prerequisites for Installing Invixium IXM WEB Software

Acquiring IXM WEB Activation Key

Procedure

STEP 1

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

IXM WEB Download and Activation

Fill out the details below to receive an email with steps to download, install and activate IXM WEB.

Who are you?

Distributor
 Access Control Panel Manufacturer
 Installer/Integrator
 End User

Customer Details

Please provide details of the End-User who has purchased Invixium biometric solutions and where they will be installed. The Activation License for IXM WEB will be issued in their name and will provide them access to future upgrades and support

First Name*	Last Name*	Company Email*
Company Name*	Select Country* v	Phone Number*

Installer Details

Please provide details of the person and/or company responsible for installing IXM WEB at the aforementioned customer's facility. The license key will be emailed to the customer email ID as well as the email ID provided below.

First Name*	Last Name*	Company Email*
Company Name*	Phone Number*	
Street Address 1	Street Address 2	City*
State*	Select Country* v	Postal Code*

< Back
Submit

Figure 6: IXM WEB Online Request Form

After submitting the completed form, an email will be sent with instructions from support@invixium.com to the email ID specified in the form.

Please ensure to check the spam or junk folder.

See below for a sample of the email that includes instructions on how to download and install IXM WEB along with your Activation ID.

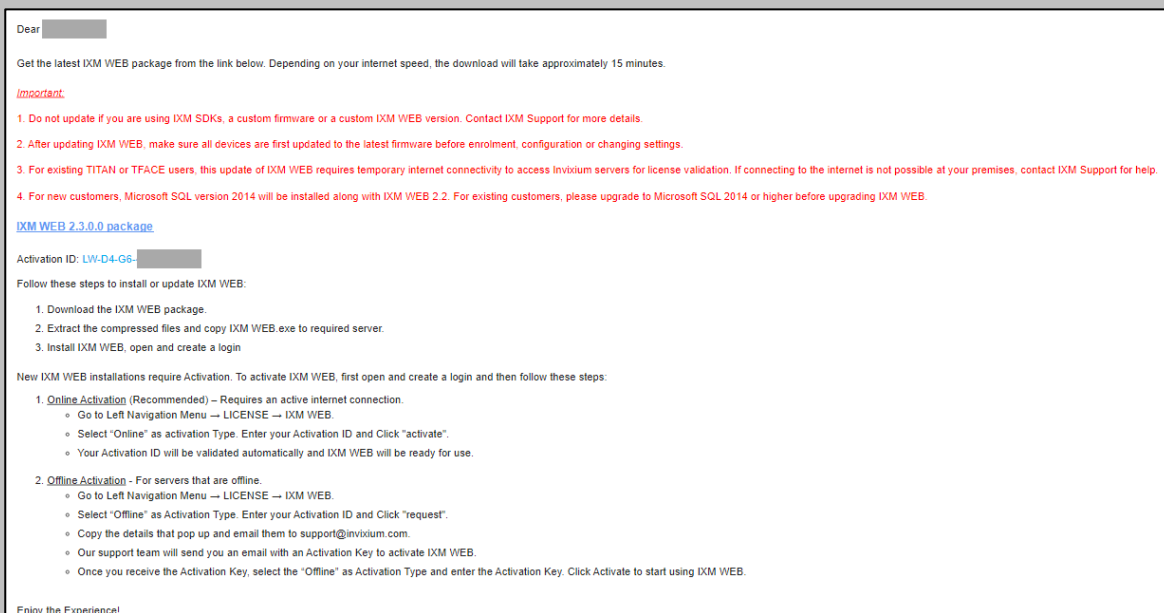



Figure 7: Sample Email After Submitting Online Request Form

Setting Up SQL instance

 Note: The following section describes the setup of a pre-created instance of SQL 2016+. Creating a new instance can be done with the use of SQL Installer within the Security Center installation media kit.

Procedure

STEP 1

Make sure to **Create** a new SQL instance on the server.

STEP 2

Set the instance name as IXM WEB (default) or Invixium.

STEP 3

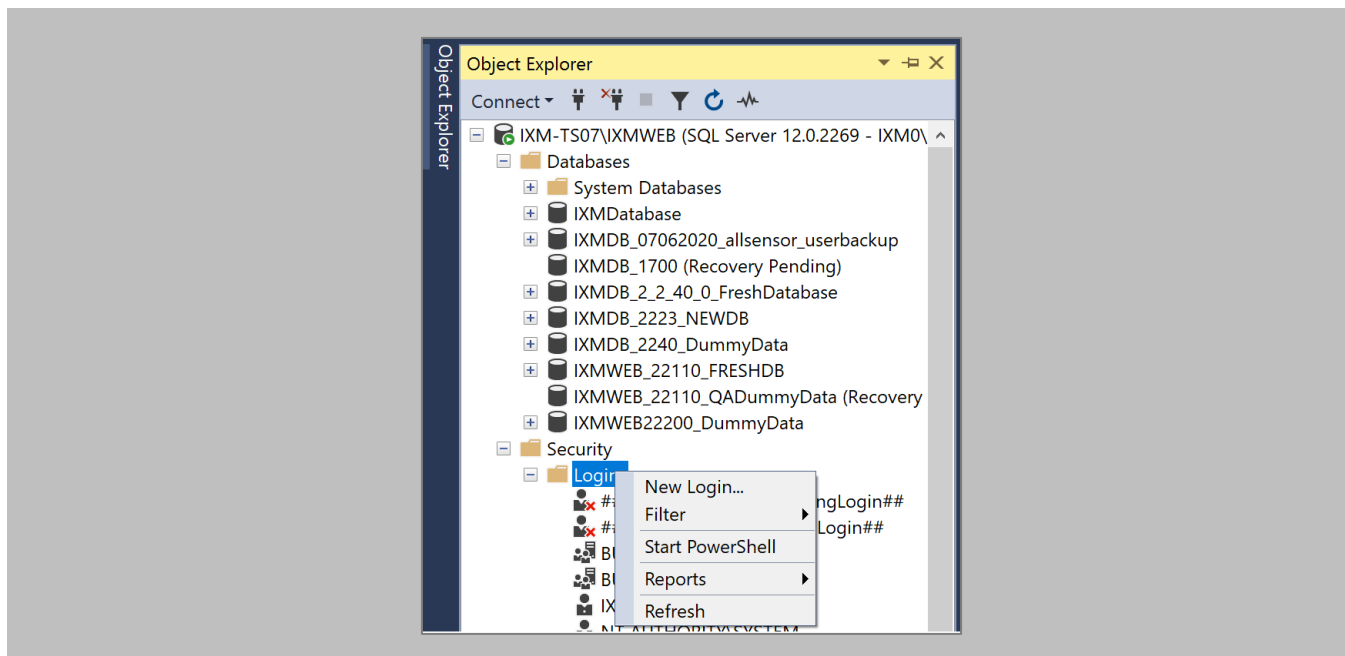
Select mixed mode: SQL Authentication and Windows Authentication for secure logins. Leave everything else as default.


STEP 4

Install **SQL Management Studio** on the server.

STEP 5

Log into the new instance and create a new user.



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

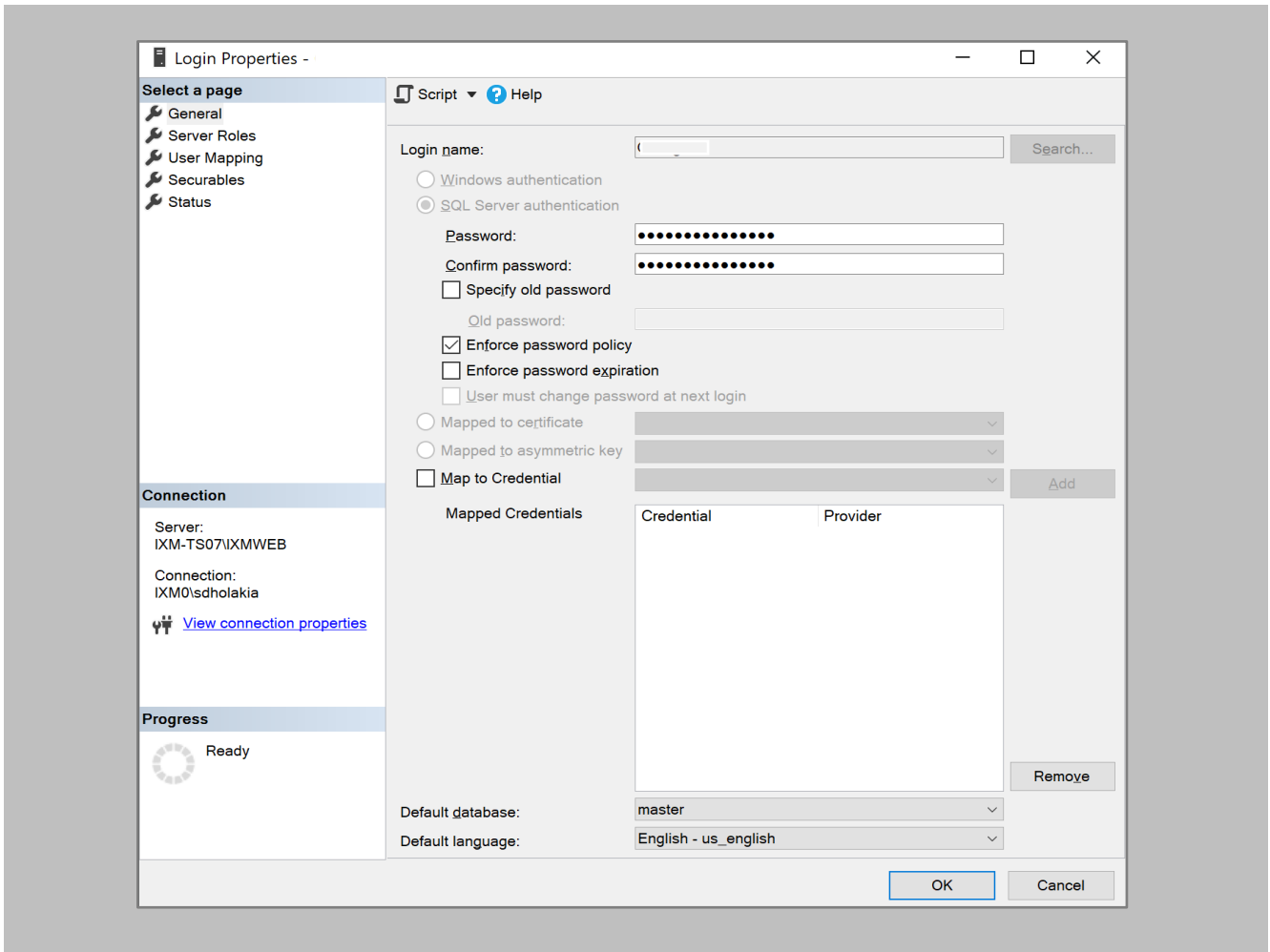


Figure 9: SQL Login Properties

STEP 7

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

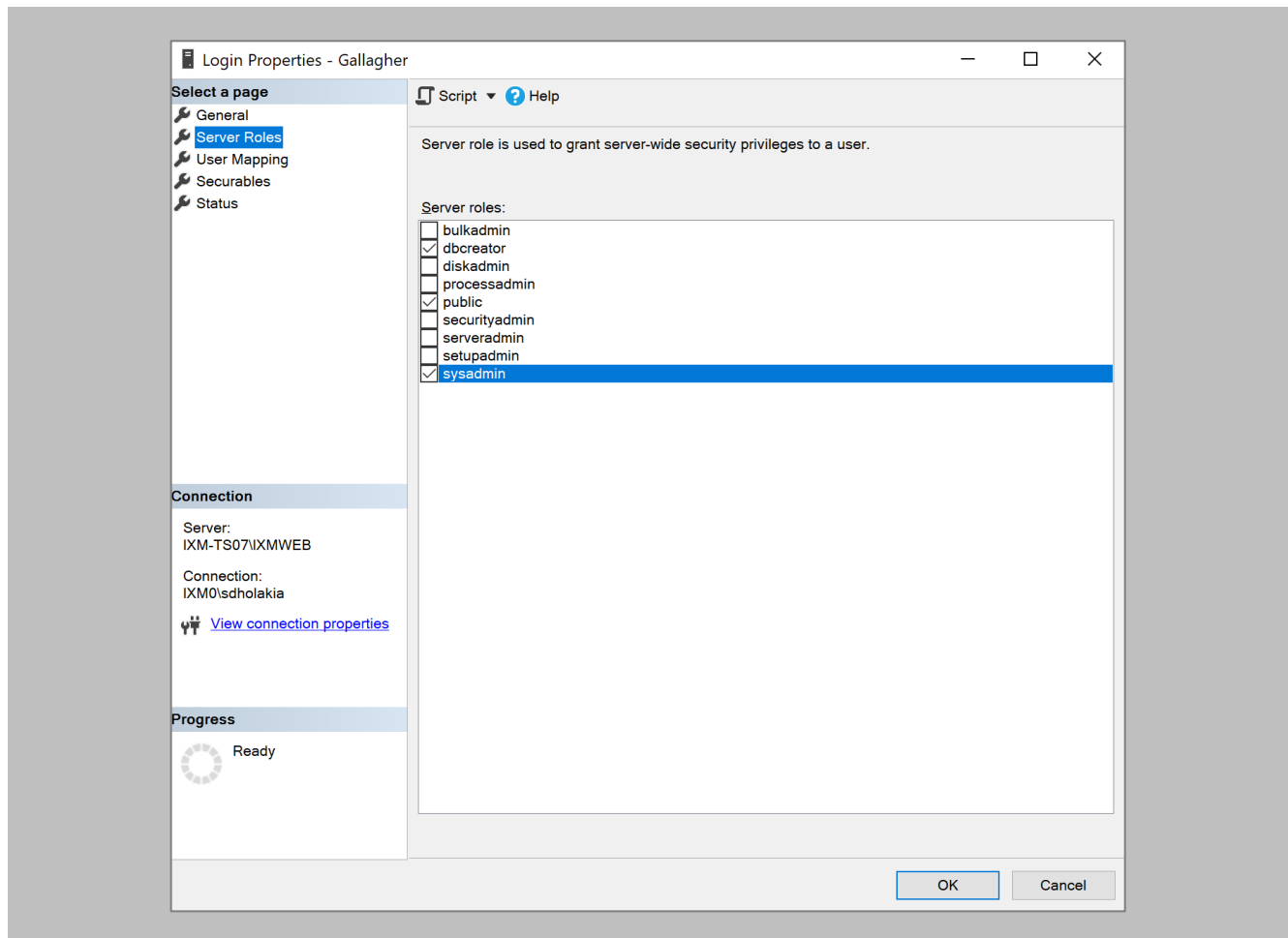


Figure 10: SQL Server Roles

RESULT

These privileges will be used later in the installation process to create the database.

Minor Checklist and Considerations

Use these tables to verify that you have carried out all required steps.

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

Table 3: System Related Checklist

Port Assignment	Port
Inbound HTTP Port	9108
TCP	1433
Port to communicate between IXM WEB & Devices	9734
Inbound Port	1255
GSC Web SDK Port	4590 (default)

Table 4: Port Information

7. Installing IXM WEB

Software Install

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator).

Select **Advanced**.

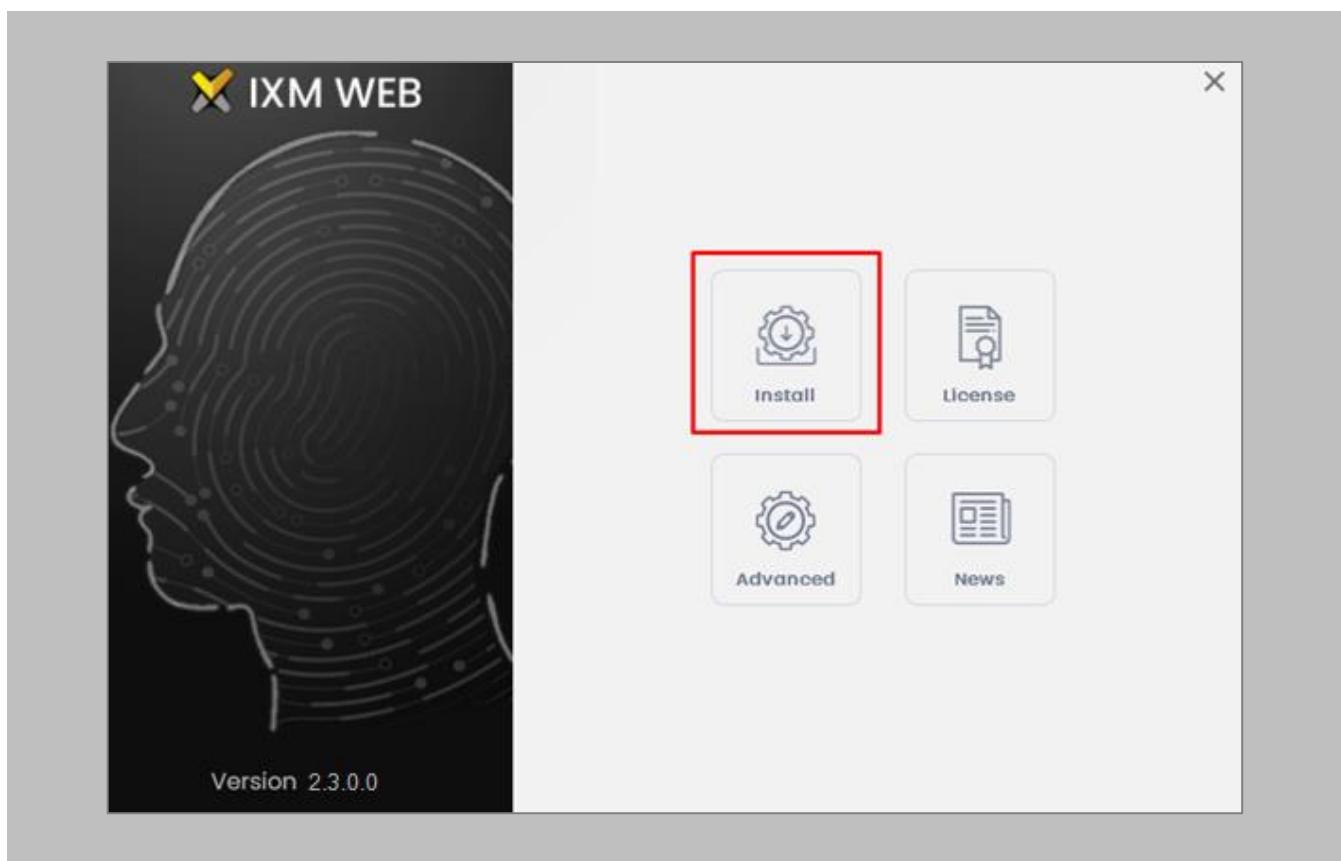


Figure 11: IXM WEB Installer

STEP 2

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

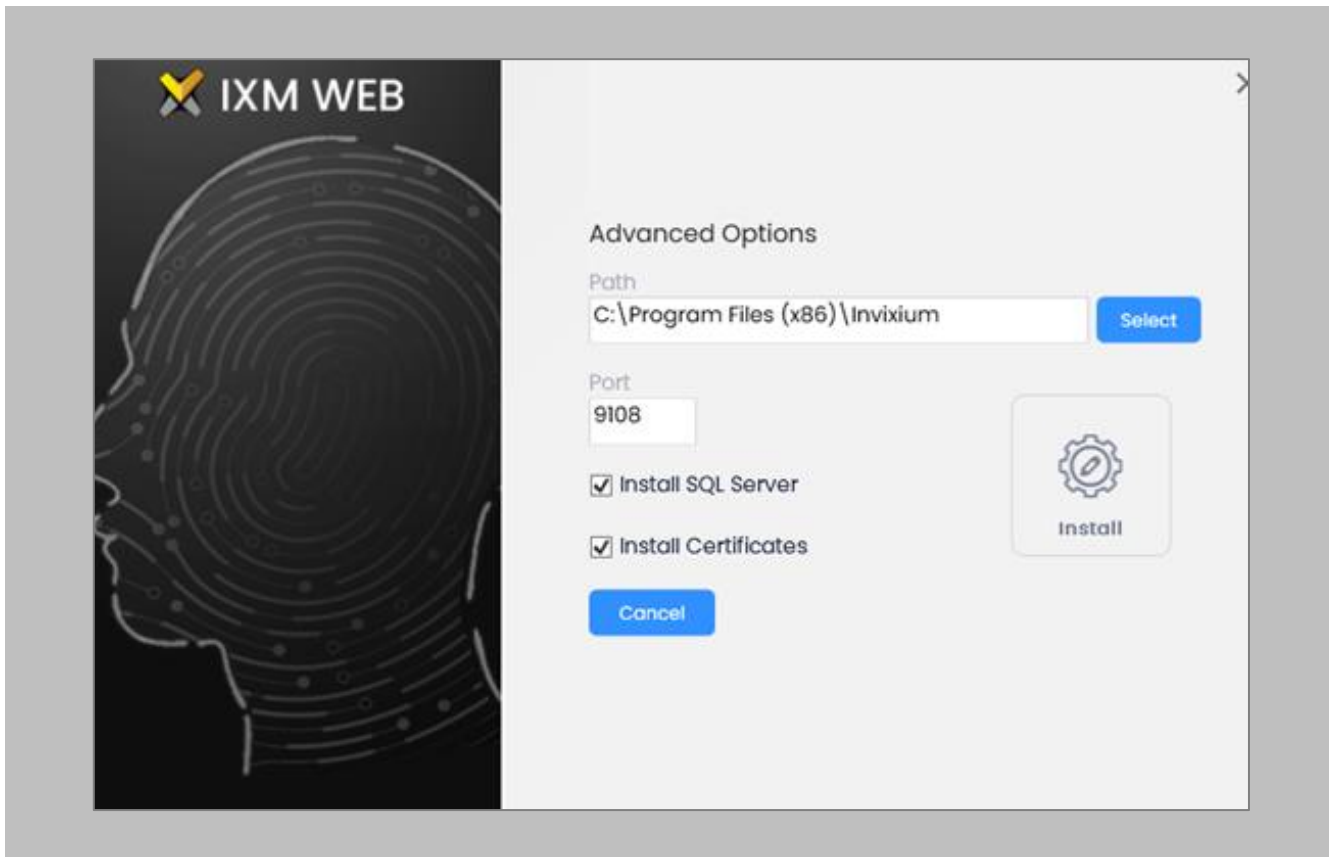


Figure 12: Advanced Options in IXM WEB Installer

STEP 3

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

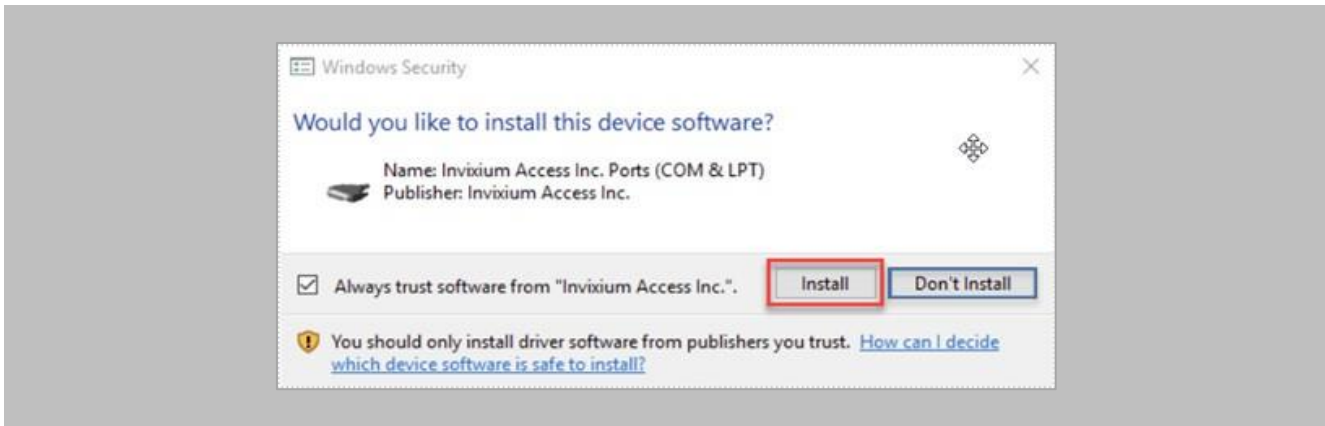


Figure 13: Invidia Fingerprint Driver Installation Message

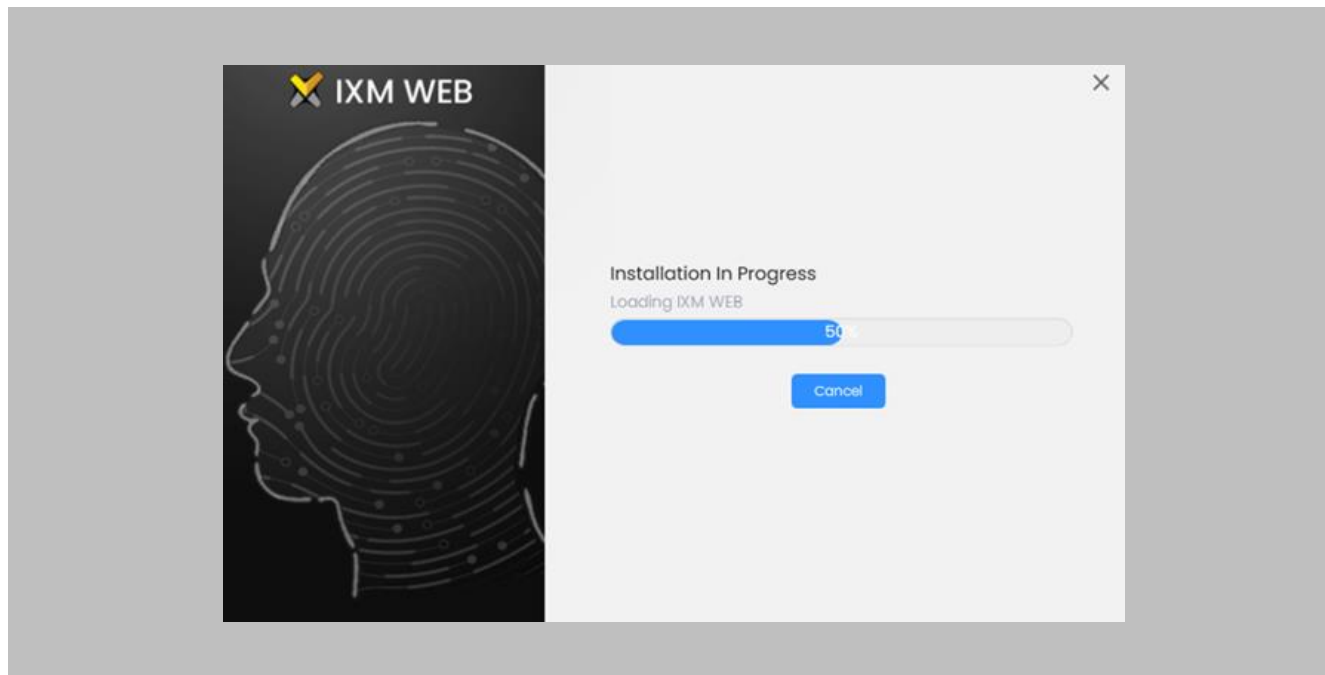


Figure 14: IXM WEB Installation Progress

STEP 4

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

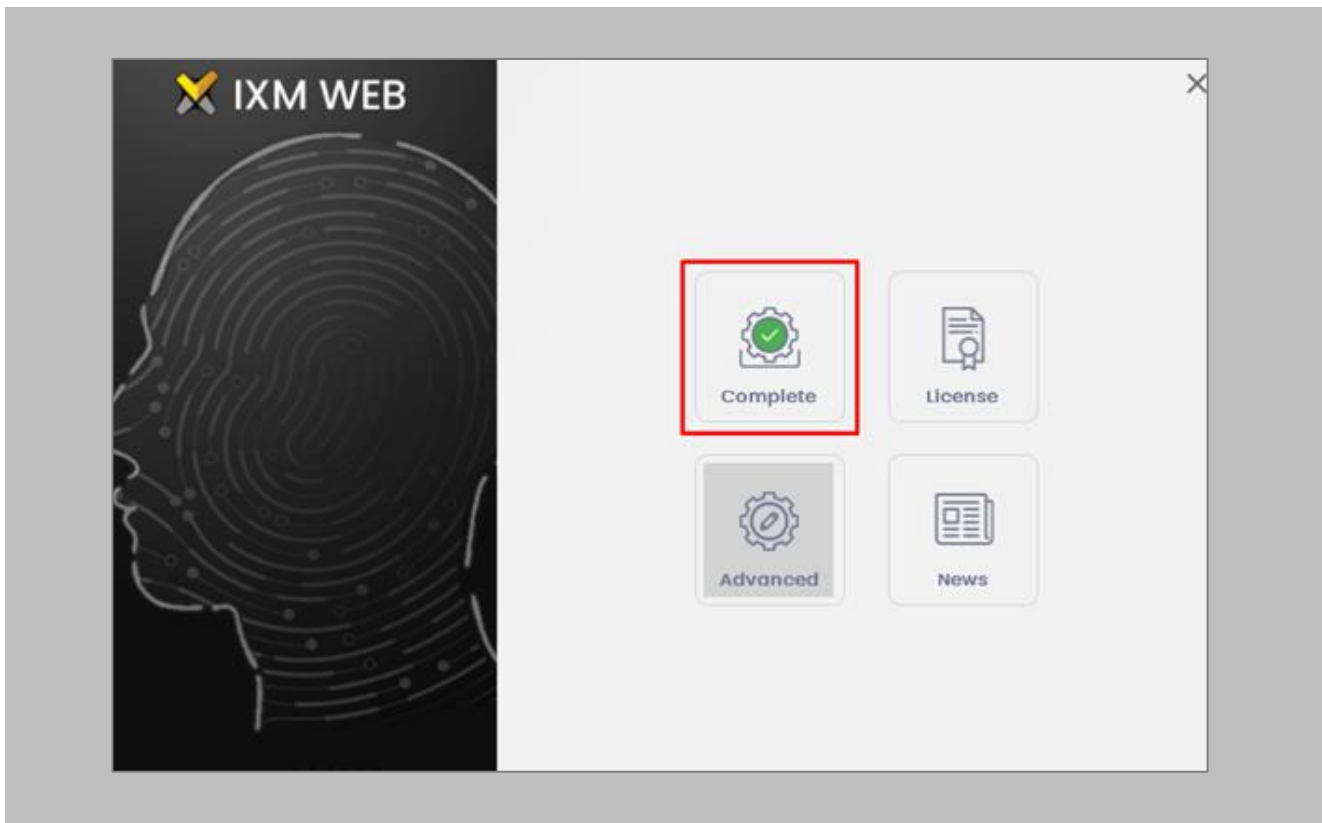


Figure 15: IXM WEB Installation Completed

STEP 5

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

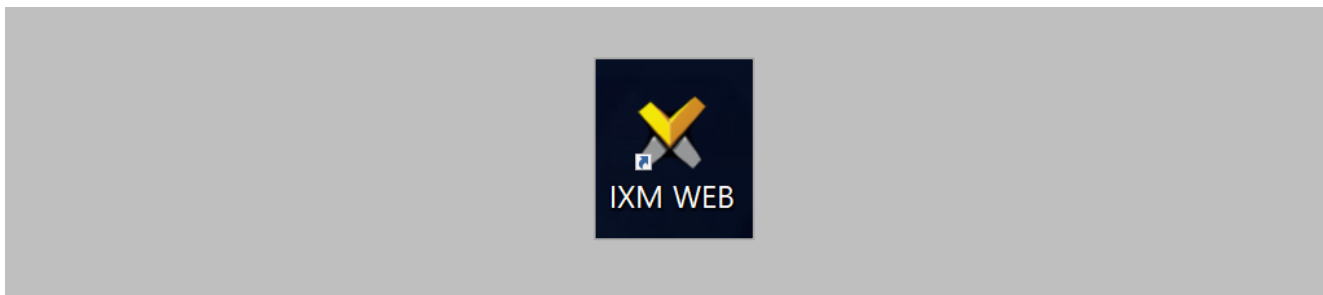


Figure 16: IXM WEB Icon - Desktop Shortcut

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

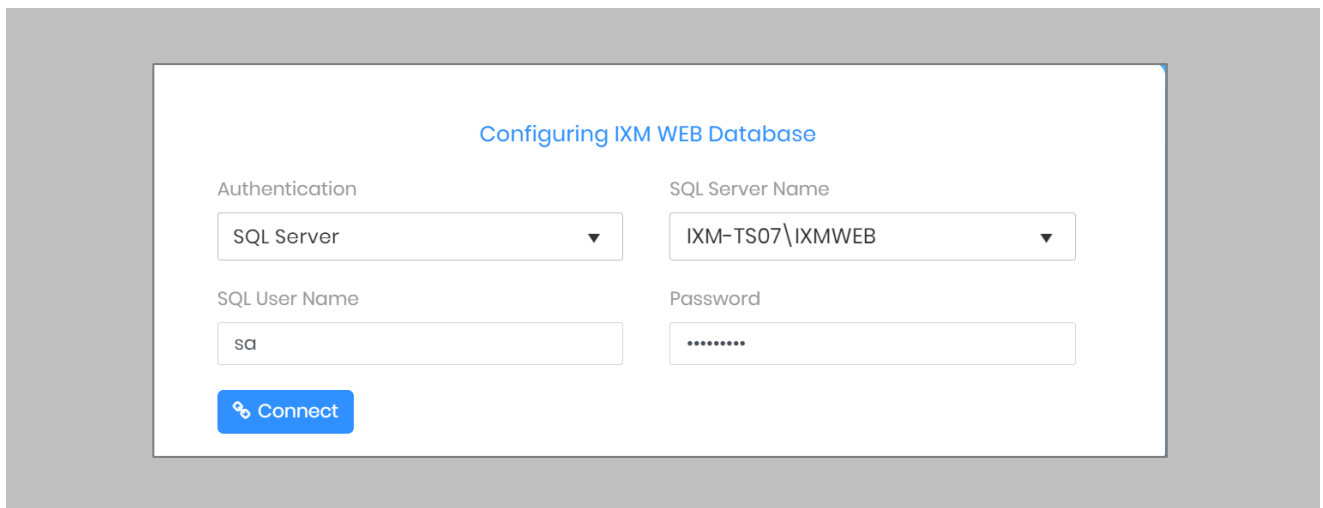


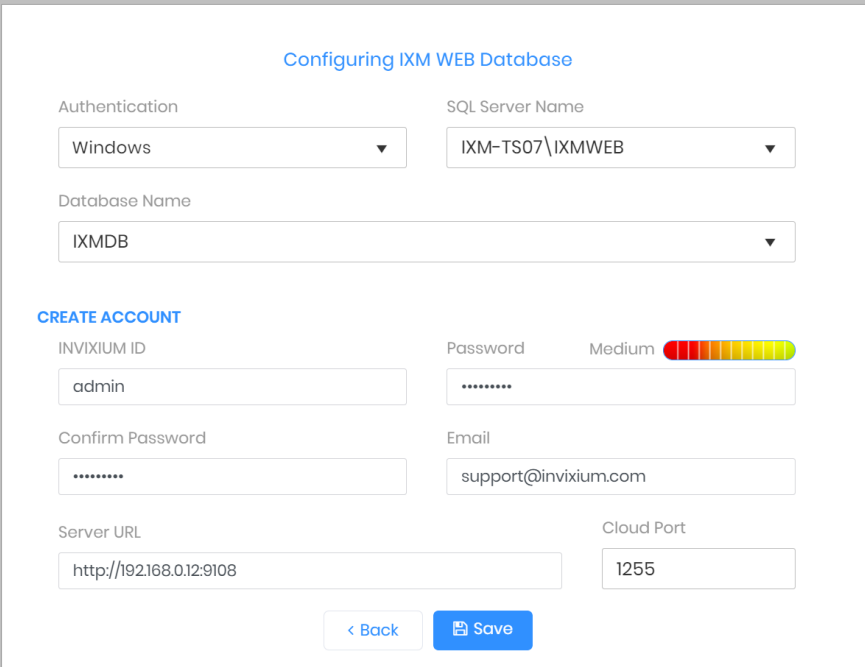
Figure 17: IXM WEB Database Configuration

STEP 6

Select the **SQL Server** authentication and the **Server Name** from the drop-down options. If it does not appear, enter it manually.

STEP 7

Enter the user credentials created above and leave **IXMDB** as the database name.



Configuring IXM WEB Database

Authentication: Windows | SQL Server Name: IXM-TS07\IXMWEB

Database Name: IXMDB

CREATE ACCOUNT

INVIXIUM ID: admin | Password: Medium (strength indicator) | Confirm Password: | Email: support@invixium.com

Server URL: http://192.168.0.12:9108 | Cloud Port: 1255

< Back | Save

Figure 18: IXM WEB Administrator User Configuration

Now comes the step to create the user account for Invixium to access the database itself.

STEP 8

Create a **user account** (this is different from the identity used to connect to the SQL instance at the top of the page). The status bar will indicate the strength of the chosen password.

STEP 9

Change **http://localhost:9108** to **http://[IP address of server]:9108**

For example:

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

http://192.168.1.100:9108

STEP 10

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

STEP 11

When IXM WEB is finished installing, you should be prompted with the following screen:

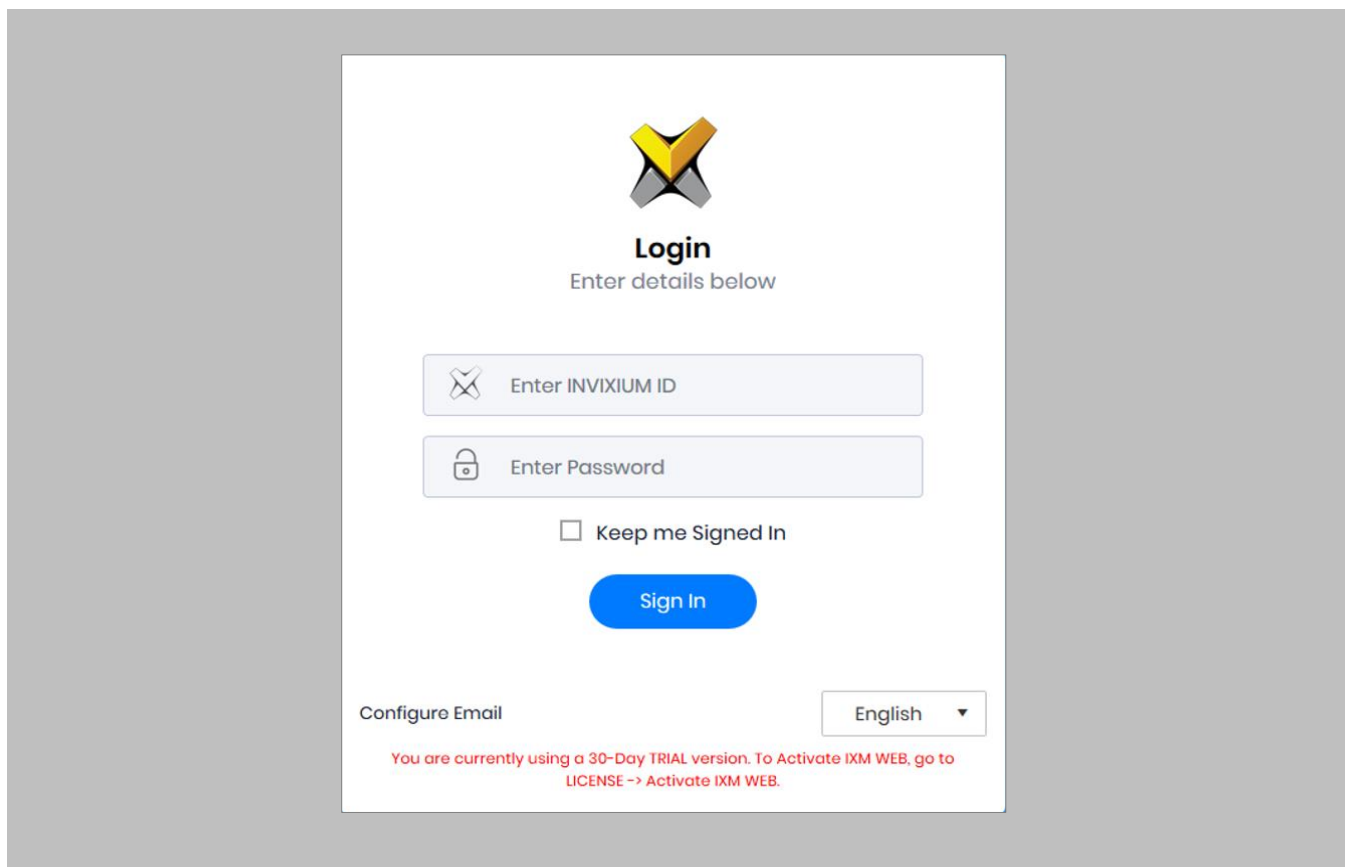



Figure 19: IXM WEB Login Page



 Note: During an upgrade of IXM WEB from any previous release to 2.3.0.0, an internet connection is required for license validation. As this new version includes a face algorithm update, it will automatically convert templates without the need for re-enrollment of faces.

8. Configuring Email Settings using IXM WEB

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

Email Setting Configuration

Procedure

STEP 1

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

OR

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

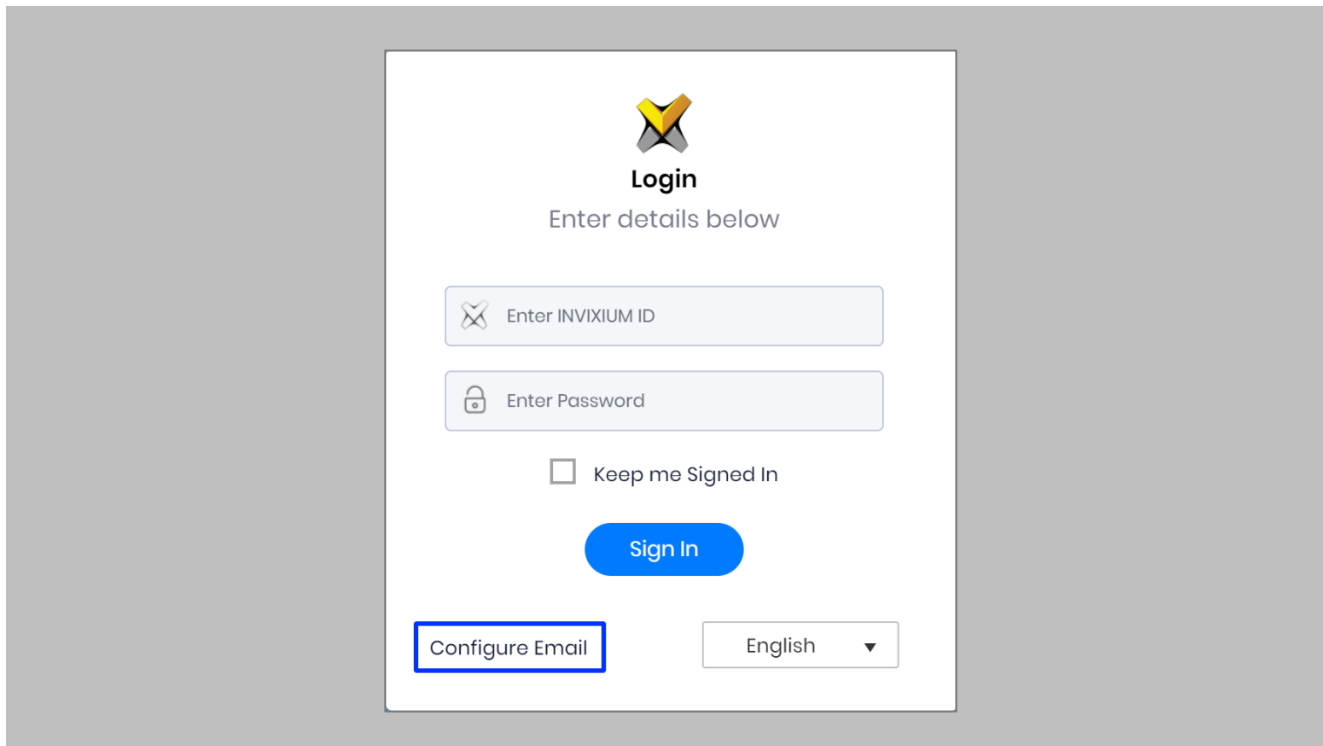


Figure 20: Configure Email

STEP 2

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

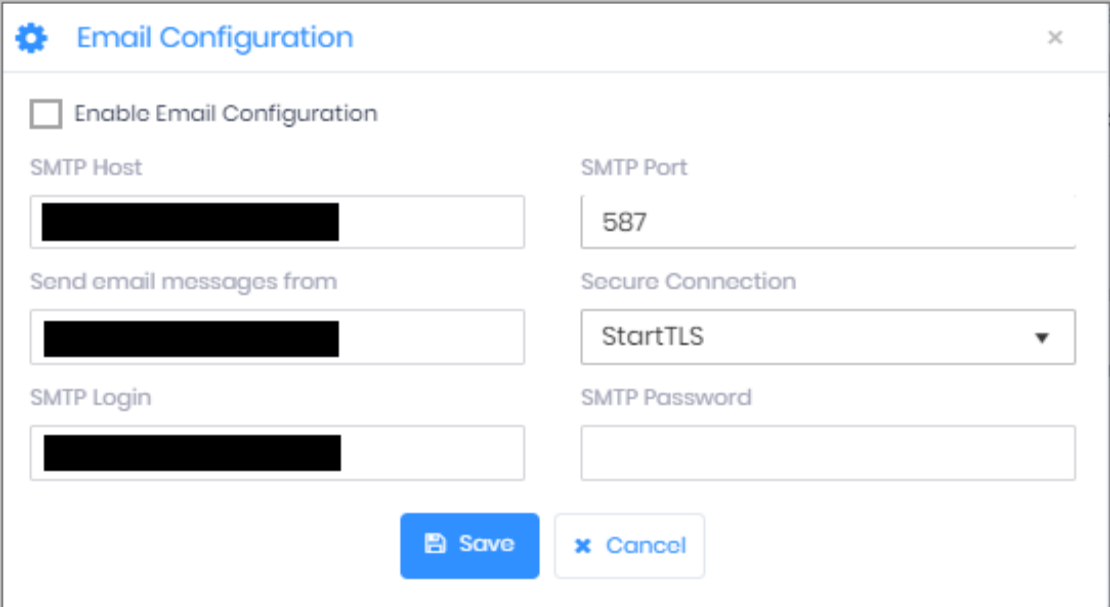



Figure 21: IXM WEB - SMTP Settings

 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.

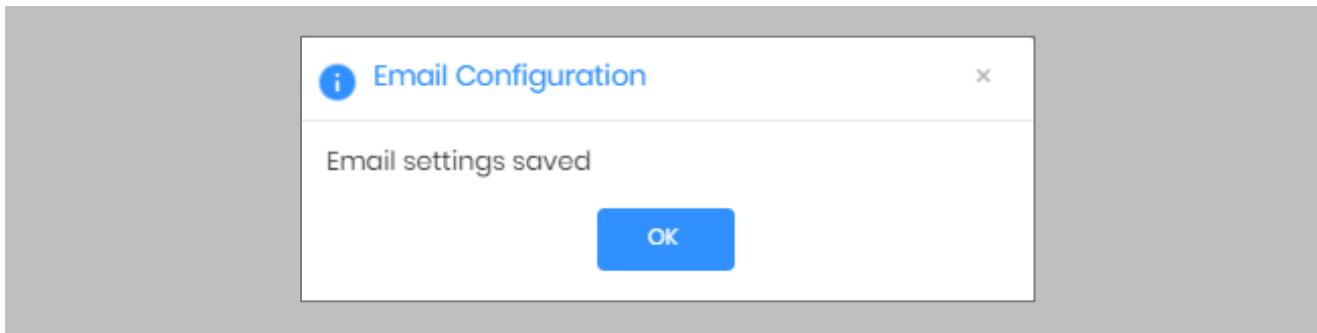


Figure 22: IXM WEB - Save Email Settings

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.

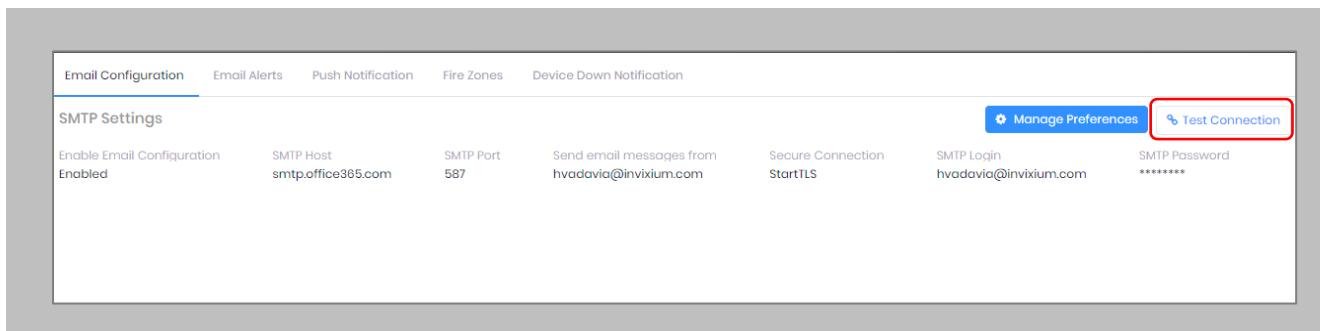


Figure 23: IXM WEB - Test Connection

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

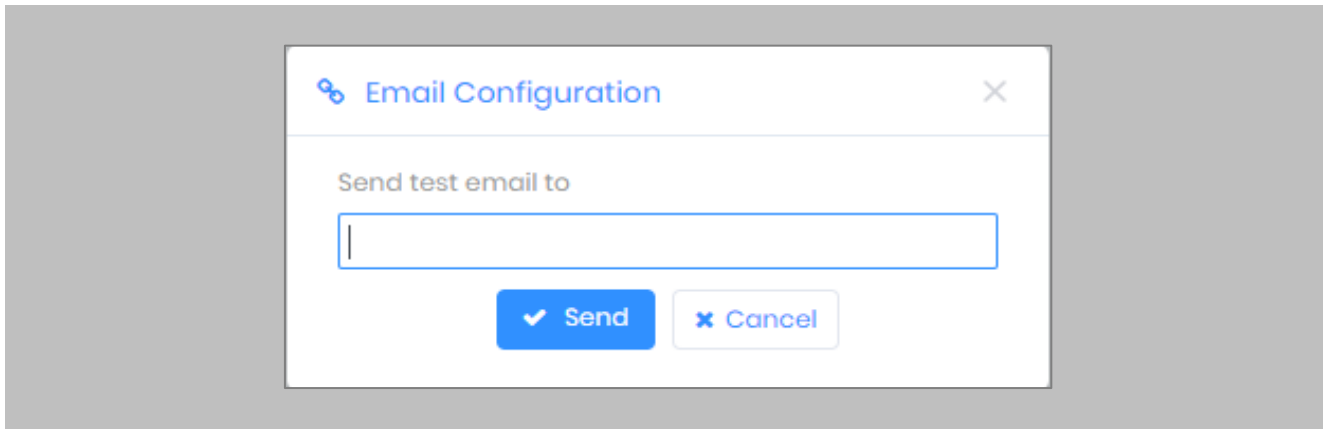
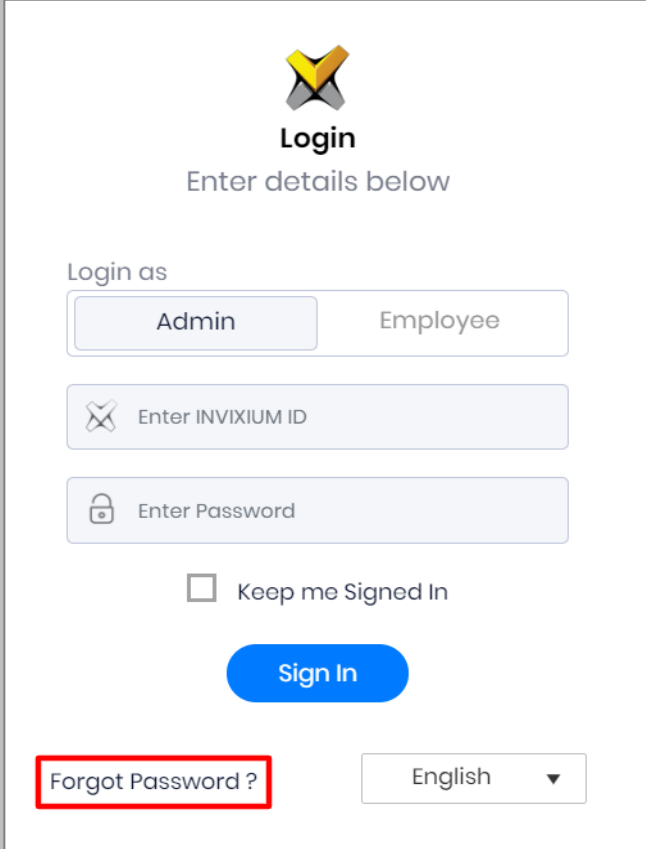


Figure 24: IXM WEB - Enter Email ID

STEP 4

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



INVIXIUM

Login
Enter details below

Login as

Admin Employee

Enter INVIXIUM ID

Enter Password

Keep me Signed In

Sign In

Forgot Password ? English

Figure 25: IXM WEB - Forgot Password

9. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

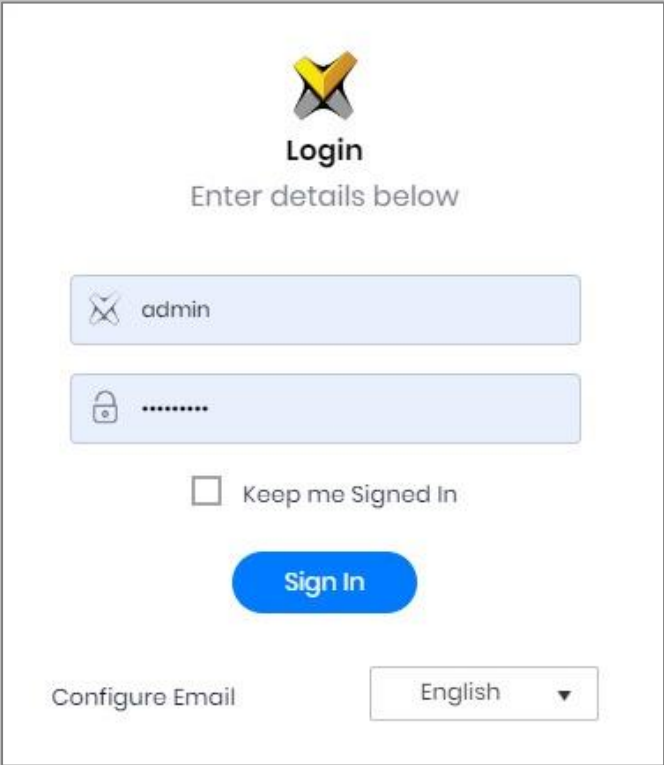


Figure 26: IXM WEB - Enter Login Credentials

STEP 2

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

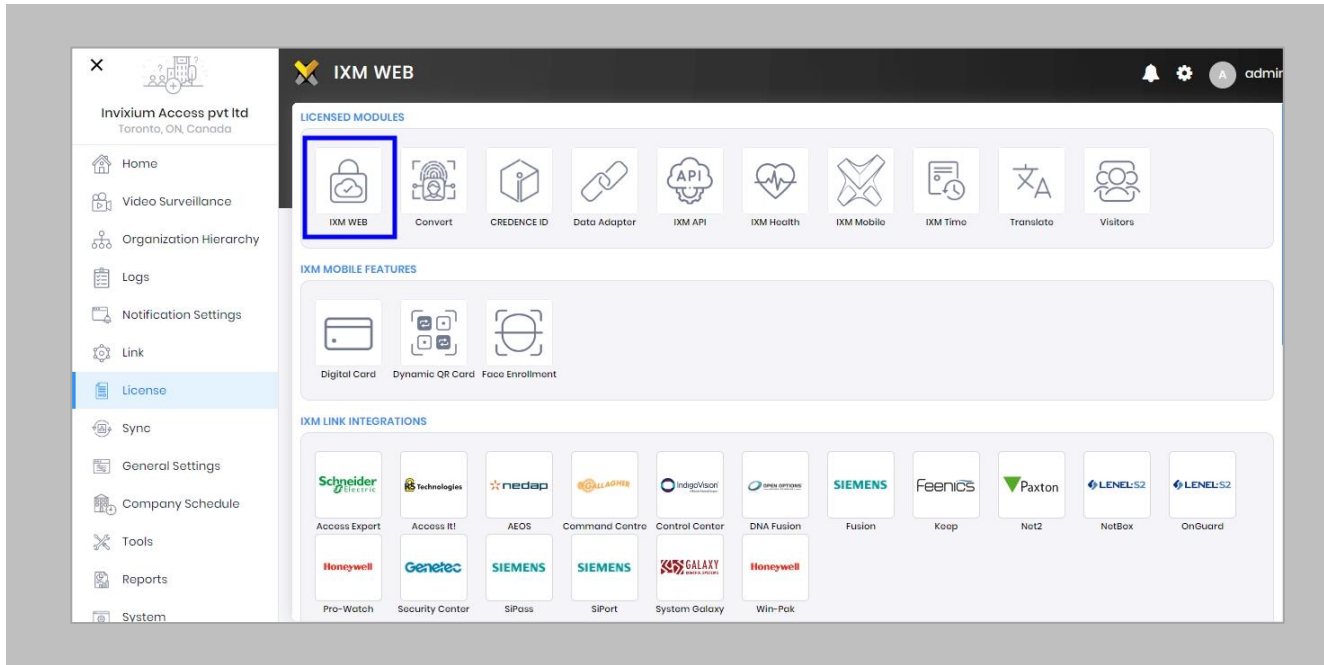



Figure 27: IXM WEB - License Setup

STEP 3

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

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

STEP 4

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

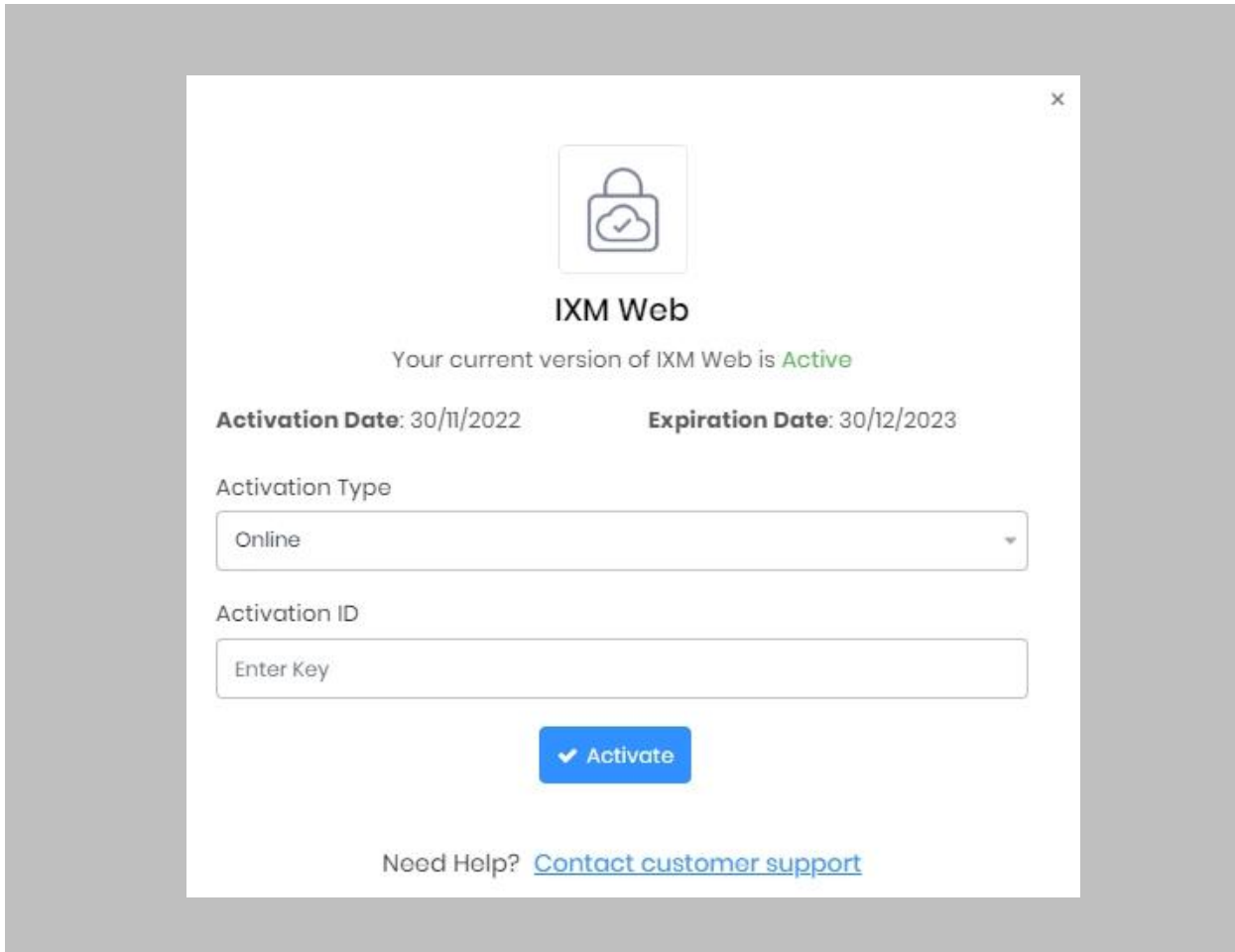


Figure 28: IXM WEB - Online Activation

NetBox Module Activation

The option to request a Lenel-S2 NetBox License is available under the **License** tab.

STEP 1

Request a **License**.

STEP 2

From **Home**, expand the **Left Navigation Pane**, Go to the **License** tab. Click on **NetBox (Lenel-S2)**.

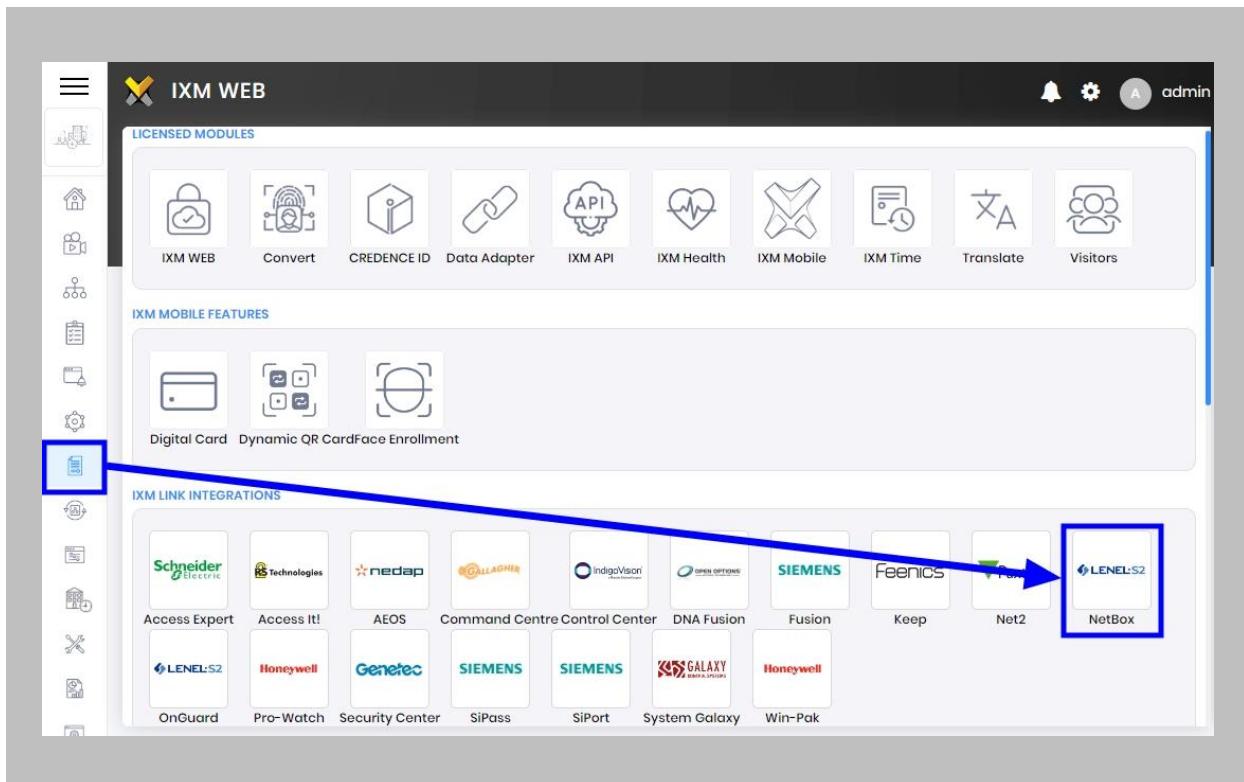


Figure 29: IXM WEB – Lenel-S2 Link Activation

STEP 3

You will receive an email from Invixium Support containing a license key for the Lenel-S2 NetBox Activation.

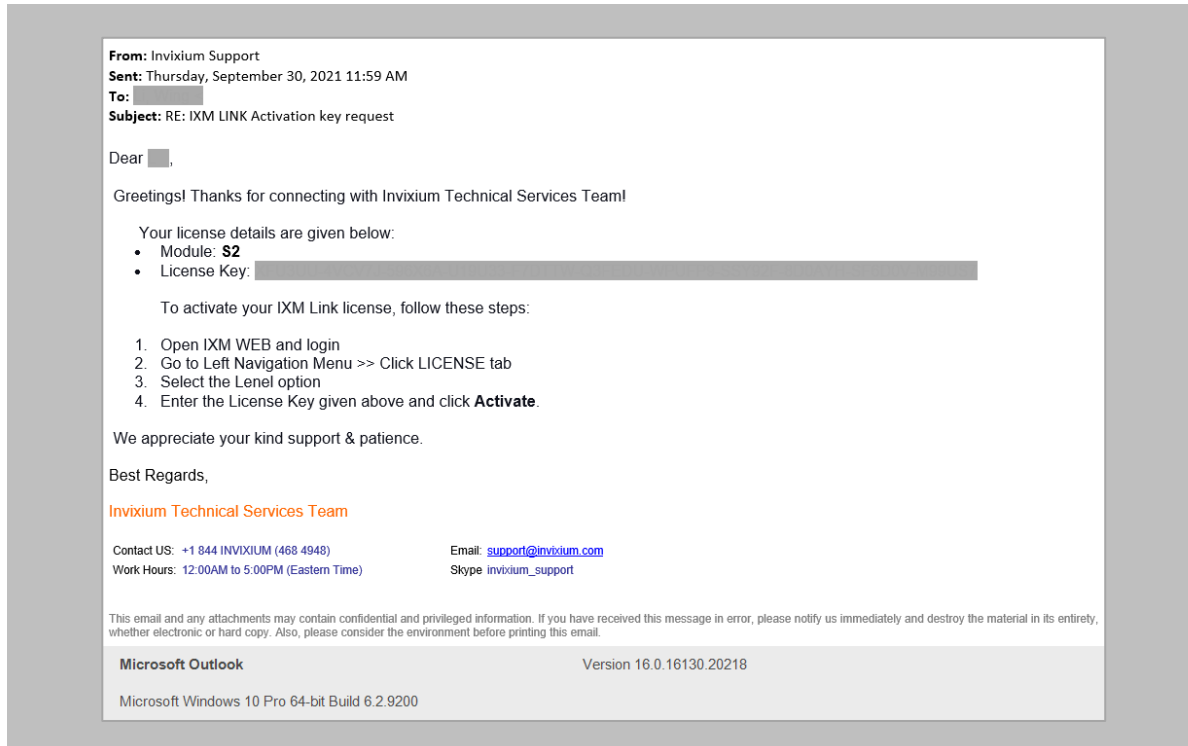


Figure 30: Lenel-S2 License Key Email

STEP 4

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

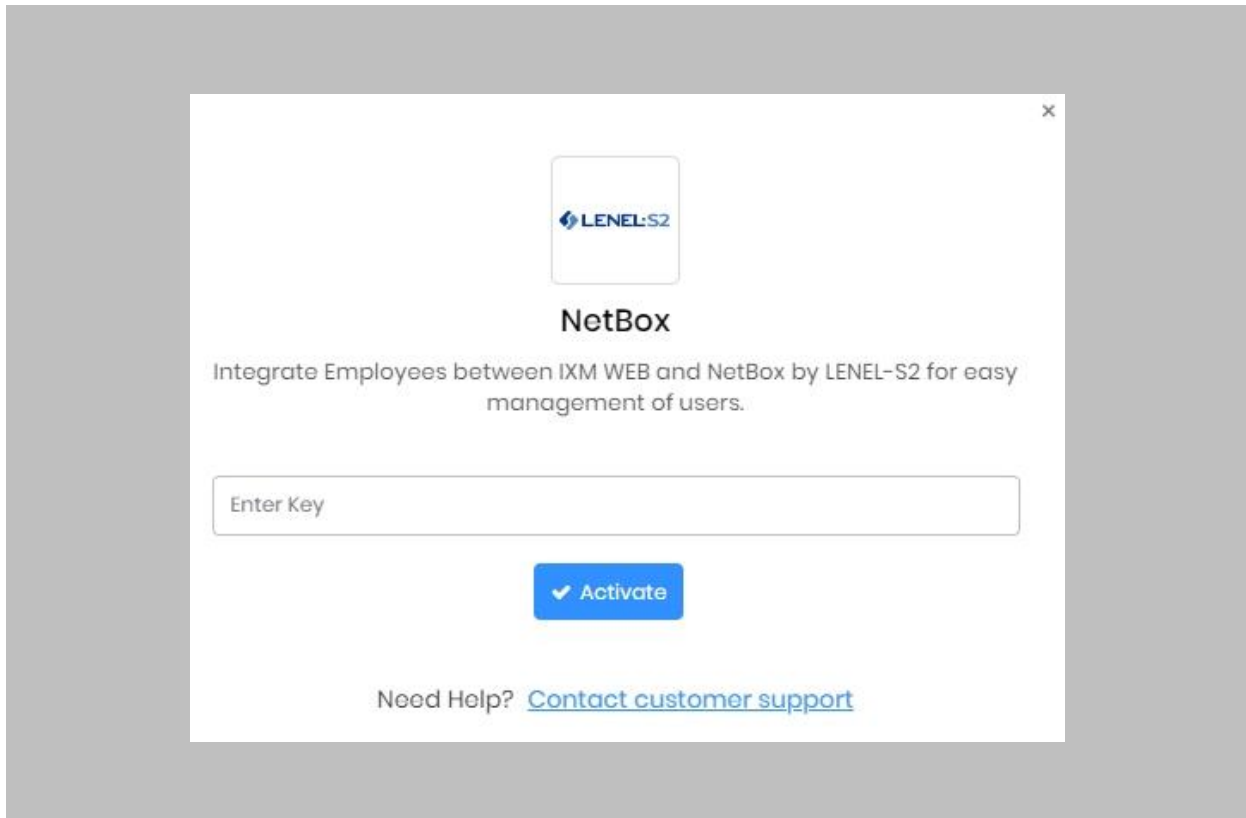


Figure 31: IXM WEB - Activate Lenel-S2 Link License

RESULT

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

10. Configuring IXM Link for Lenel-S2

Procedure

STEP 1

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

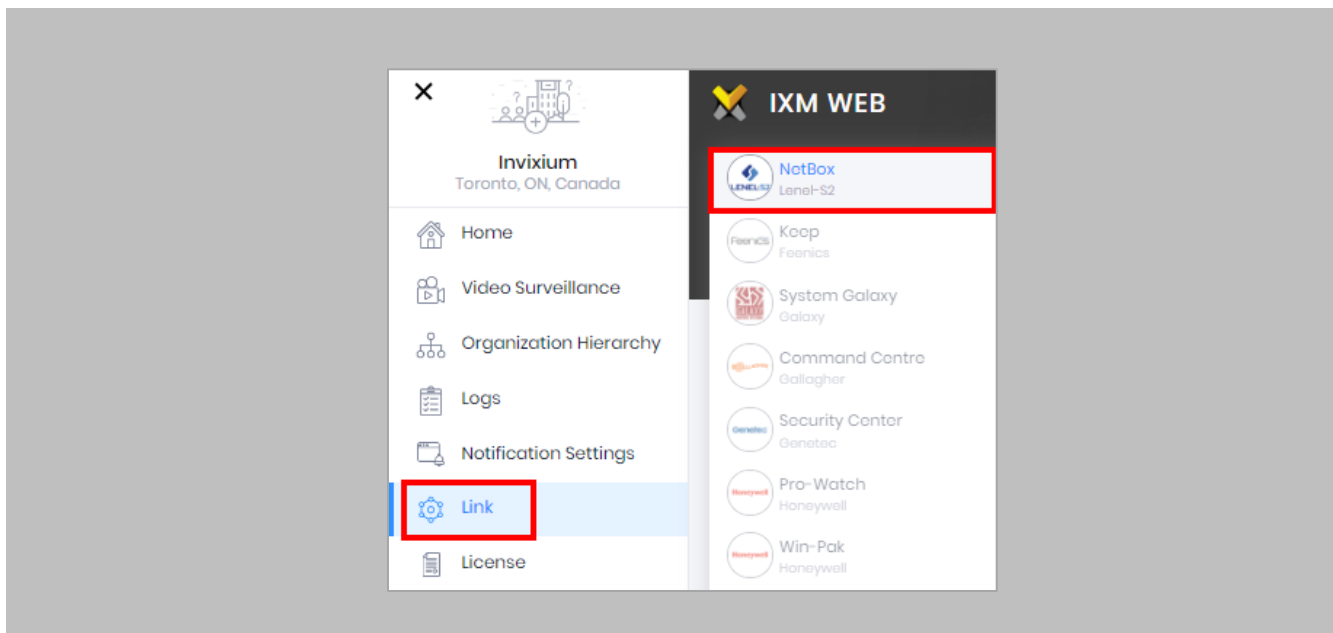


Figure 32: IXM WEB - Link Menu

STEP 2

Toggle the **Status** switch to enable.

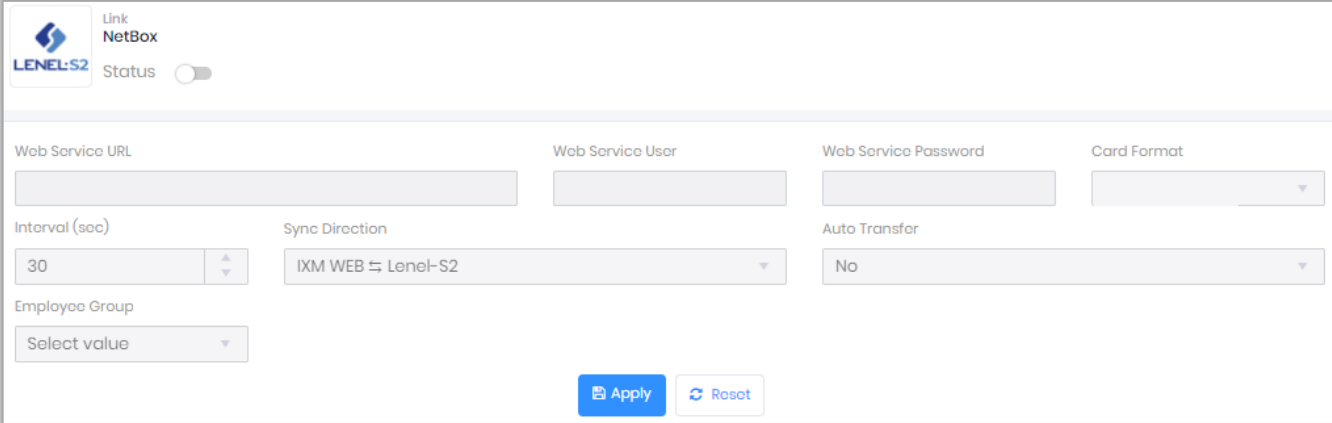


Figure 33: IXM WEB - Enable Lenel-S2 Link Module

Web Service URL:

Enter the S2 NetBox API URL. For example: `http://192.168.1.111/goforms/nbapi`

Web Service User:


Enter the name of the authorized user to connect to the Web Service of Lenel-S2 NetBox.

Web Service Password:

Enter the Password of the authorized user to connect to the Web Service of Lenel-S2 NetBox.

Card Format:

Select the valid Card format which allows syncing of cards between NetBox and IXM WEB from the dropdown list.

 Note: There can be multiple cards per user in Netbox, but while syncing the data, IXM WEB will import only those users that have the same Card Format specified here.

Interval (Sec):

Enter the duration of interval for data transfer between Lenel-S2 and IXM WEB. The system will automatically try to establish connection after every specified interval of time and sync users.

Sync Direction:

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

- IXM WEB ← Lenel-S2

Choosing this option will transfer data in one direction only, ie, from Lenel-S2 to IXM WEB. Lenel-S2 is considered as the master data in this case and any changes made in IXM WEB data will be overwritten during transfer.

Note:

This is the recommended option.

- IXM WEB → Lenel-S2

Choosing this option will transfer data in one direction only, ie, from IXM WEB to Lenel-S2. IXM WEB is considered as the master data in this case and any changes made in Lenel-S2 data will be overwritten during transfer.

- IXM WEB ↔ Lenel-S2

Choosing this option will transfer data in both the directions, ie, from Lenel-S2 to IXM WEB first followed by IXM WEB to Lenel-S2.

Auto Transfer:

This option provides facility to add employee into Employee Groups in IXM WEB. For example, if there is an Employee Group called 'Default Group' in IXM WEB, then all the employees from Lenel-S2 will be added directly to the 'Default Group'.

Click on either 'Yes' or 'No'.

Yes: Selection of User Group is mandatory to use Auto Transfer. Users will be transferred to IXM Devices based on Sync Group configuration for selected Employee Group.

No: Users will not be transferred to the IXM Devices.

Employee Group:

- This option will be enabled only when 'Auto Transfer' is set as 'Yes'. Otherwise it will remain disabled.

A list of existing Employee Groups created in IXM WEB is displayed. Click on the Employee Group to which employees should be transferred automatically.

Click **Apply**. The transfer of data between Lenel-S2 and IXM WEB is possible only after successful connection.

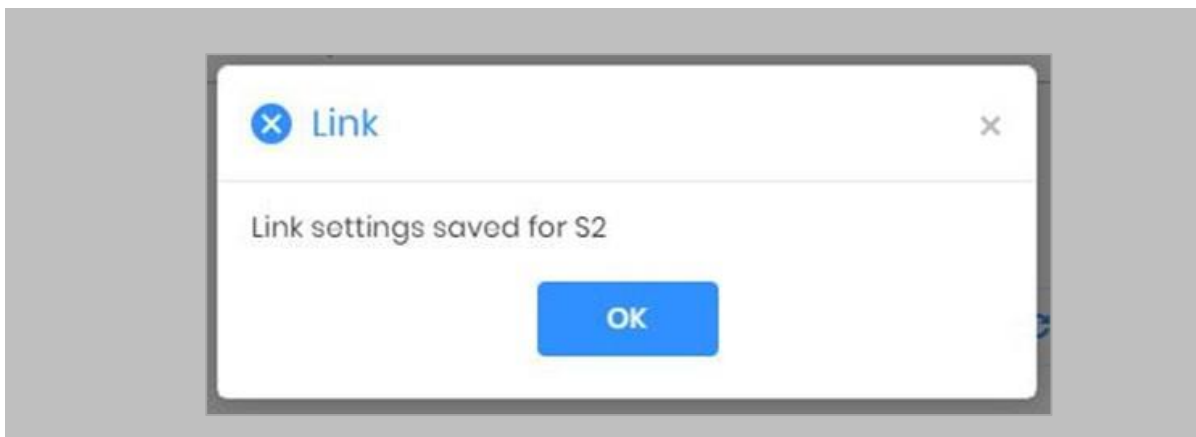


Figure 34: IXM WEB – Link Settings Saved

In case of unsuccessful connection, please refer to the *Troubleshooting* section.

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

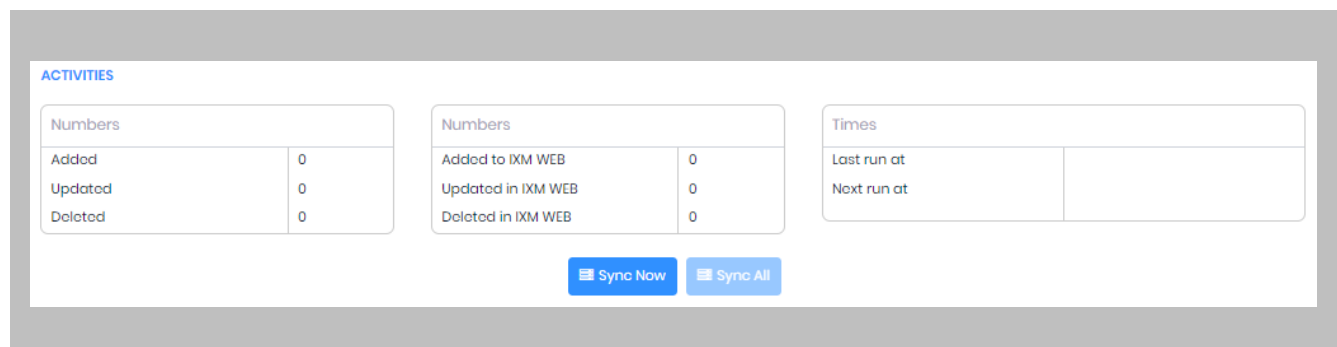


Figure 35: IXM WEB - Sync Activities





Numbers

The first two columns display the number of records added, updated and deleted in Lenel-S2 and IXM WEB respectively after each data transfer.

Times

The last column displays the time when the data was transferred last.

It also shows the time when the data will be transferred next. It is calculated as per the specified Interval.

STEP 3

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 4

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

- The **Sync All** button will be visible only when the sync direction is selected as Lenel-S2 to IXM WEB (One-way sync).

RESULT

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

11. Create System User(s) for Biometric Enrollment

Creating System User(s) for Biometric Enrollment

Procedure

STEP 1

Log into IXM WEB.

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

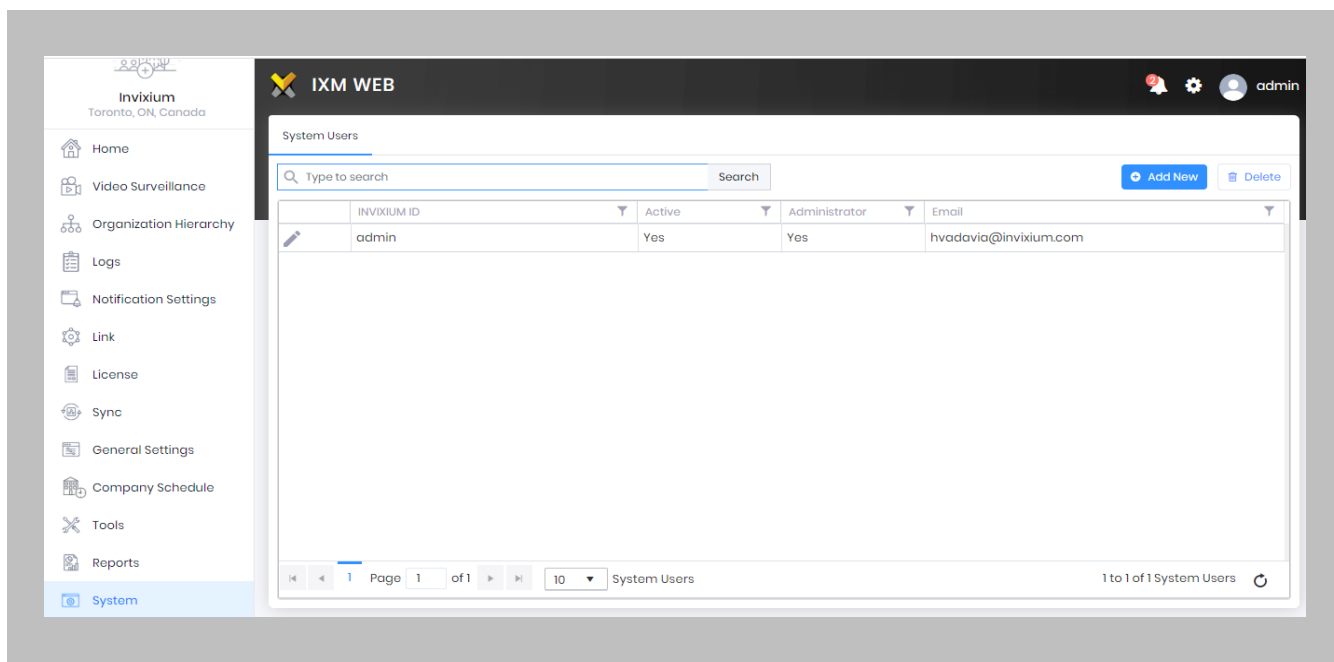


Figure 36: IXM WEB - Create System User

STEP 2

Click **Add New**.

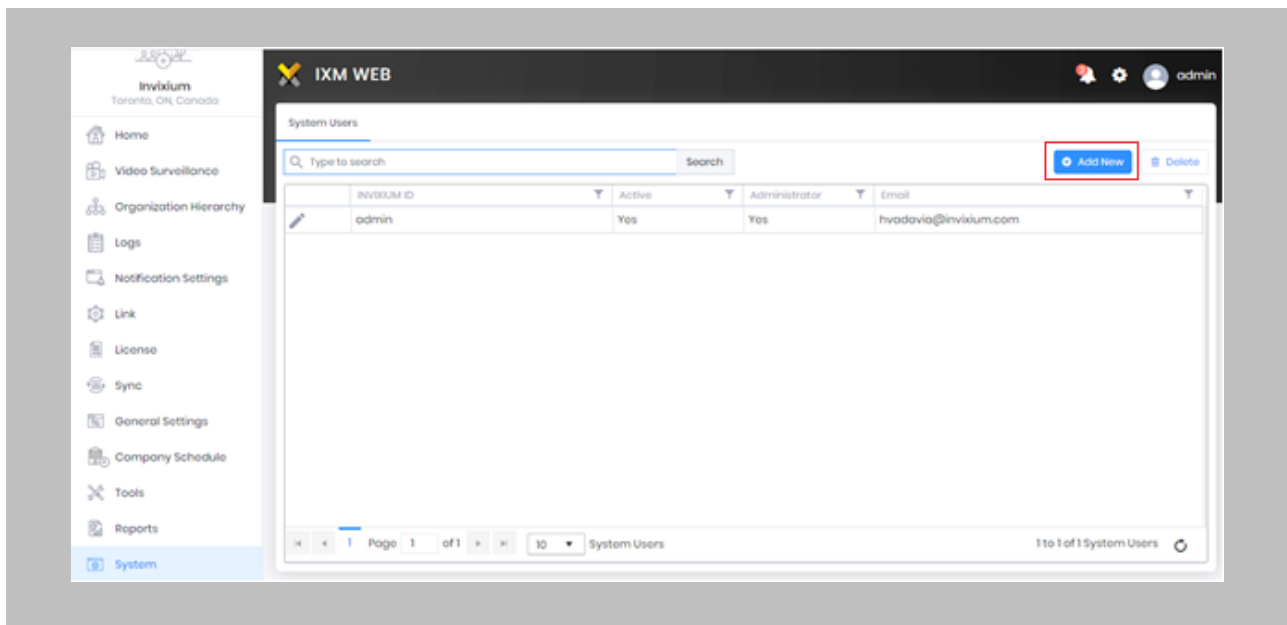


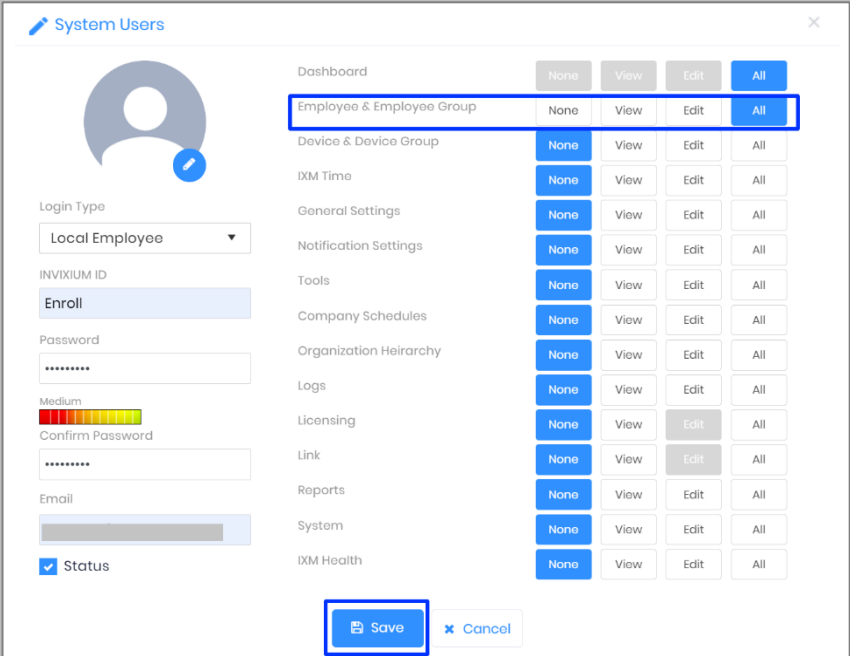
Figure 37: IXM WEB - Add New System User

Creating a system user requires the following details:

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

STEP 3

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



	None	View	Edit	All
Employee & Employee Group	None	View	Edit	All
Device & Device Group	None	View	Edit	All
IXM Time	None	View	Edit	All
General Settings	None	View	Edit	All
Notification Settings	None	View	Edit	All
Tools	None	View	Edit	All
Company Schedules	None	View	Edit	All
Organization Hierarchy	None	View	Edit	All
Logs	None	View	Edit	All
Licensing	None	View	Edit	All
Link	None	View	Edit	All
Reports	None	View	Edit	All
System	None	View	Edit	All
IXM Health	None	View	Edit	All

Figure 38: IXM WEB - New System User

STEP 4

Add an email address.

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

Click **Save**.

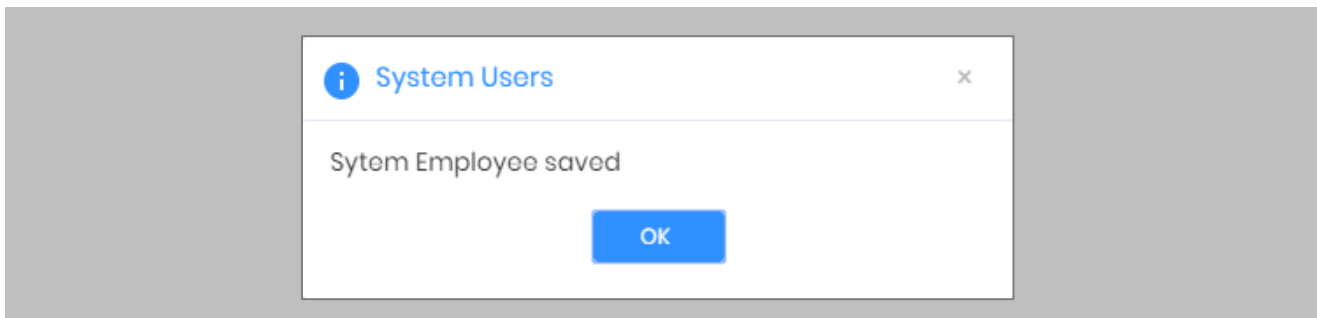


Figure 39: IXM WEB - Save System User

12. Add and Configure Invoxium Readers

Adding an Invoxium Reader in IXM WEB

Procedure

STEP 1

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

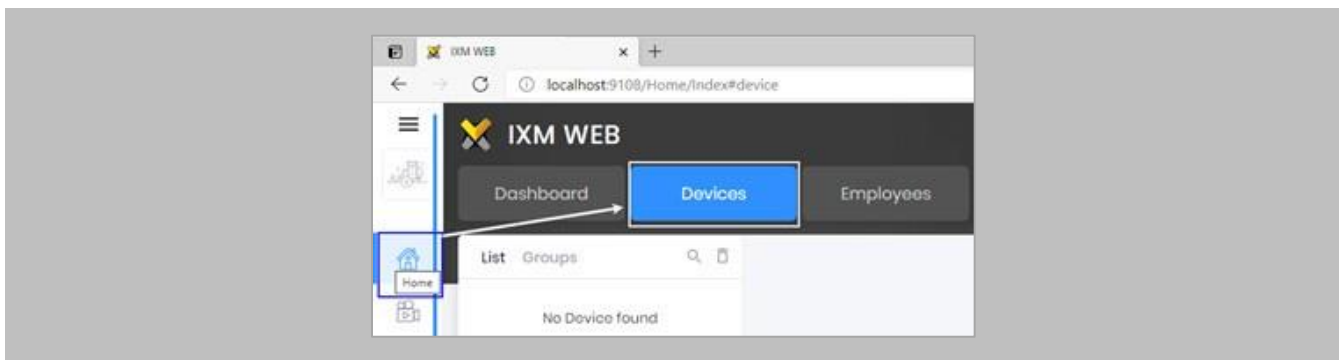


Figure 40: IXM WEB - Devices Tab

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.

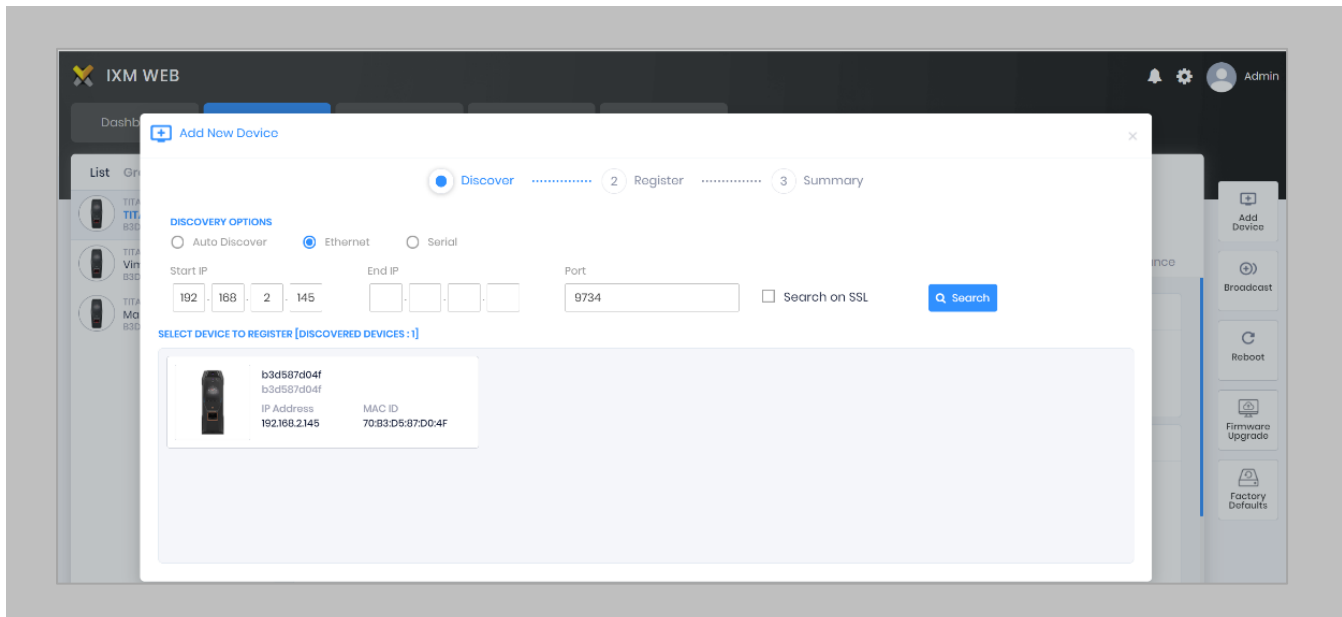


Figure 41: IXM WEB - Search Device Using IP Address

STEP 3

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

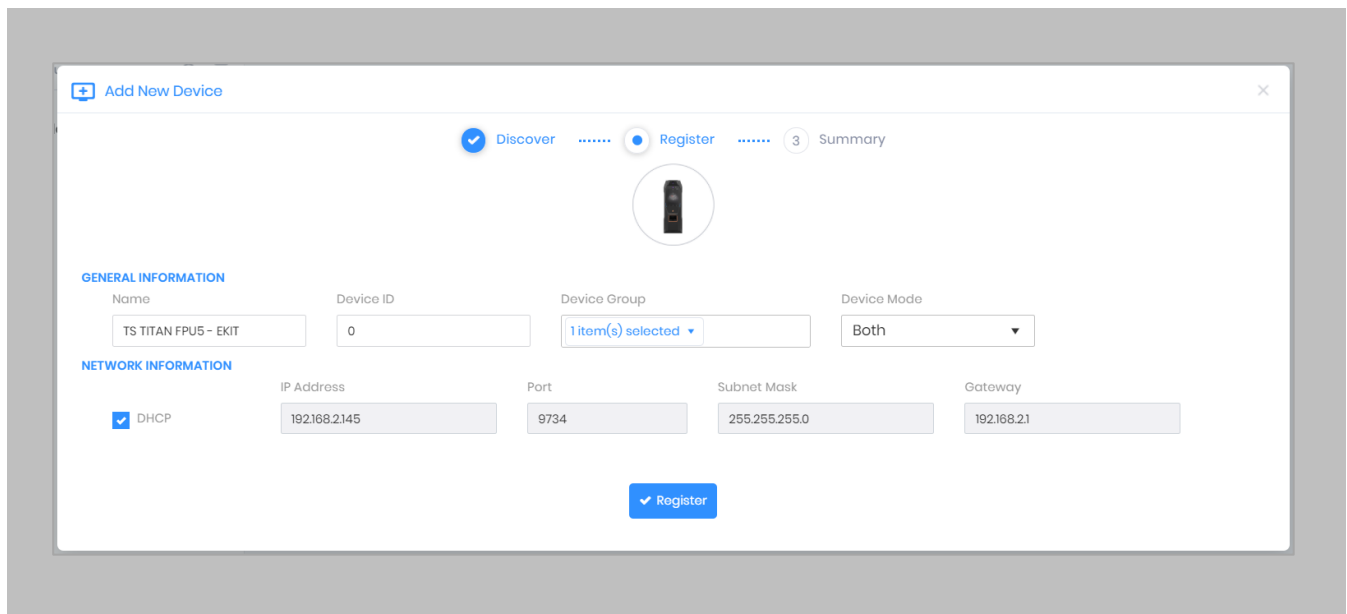


Figure 42: IXM WEB - Register Device

STEP 4

Name the **device** exactly as the name of the door it will be used for.

Device Mode: select accordingly.

Device Group: select the Access Group to which the reader will be assigned.

STEP 5

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

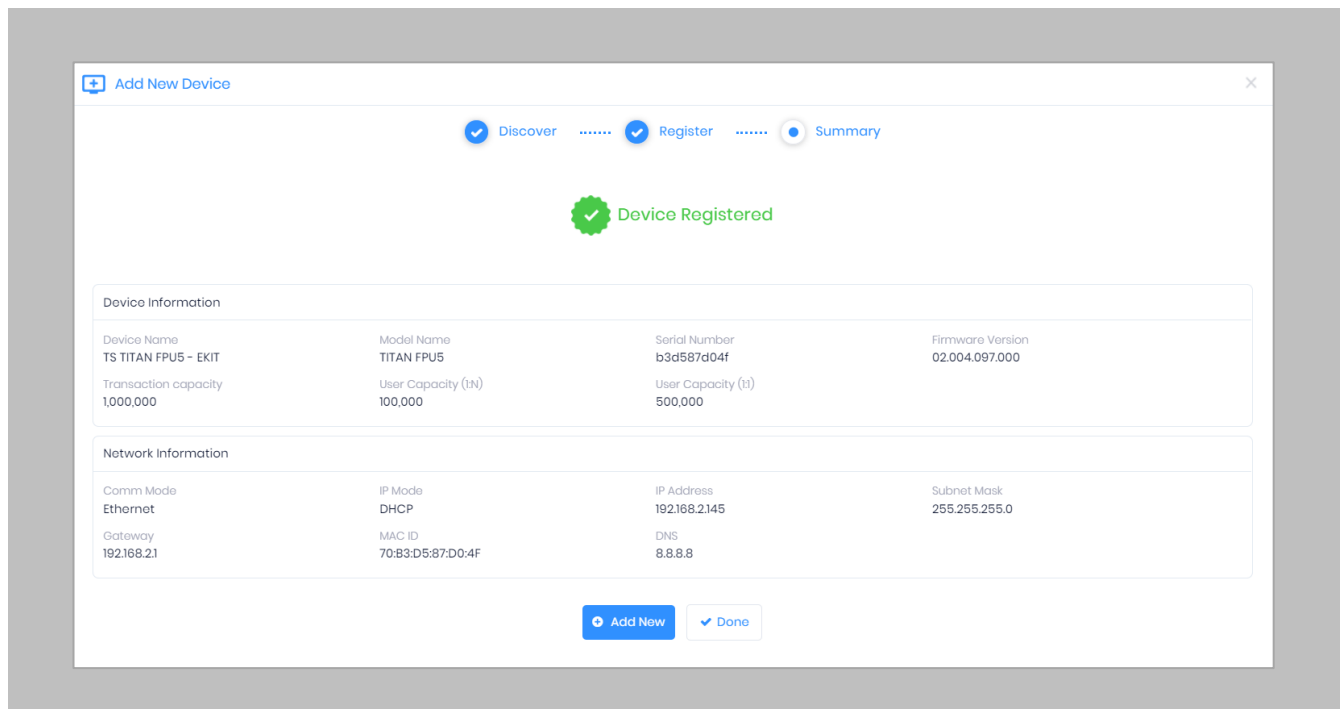


Figure 43: IXM WEB - Device Registration Complete

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

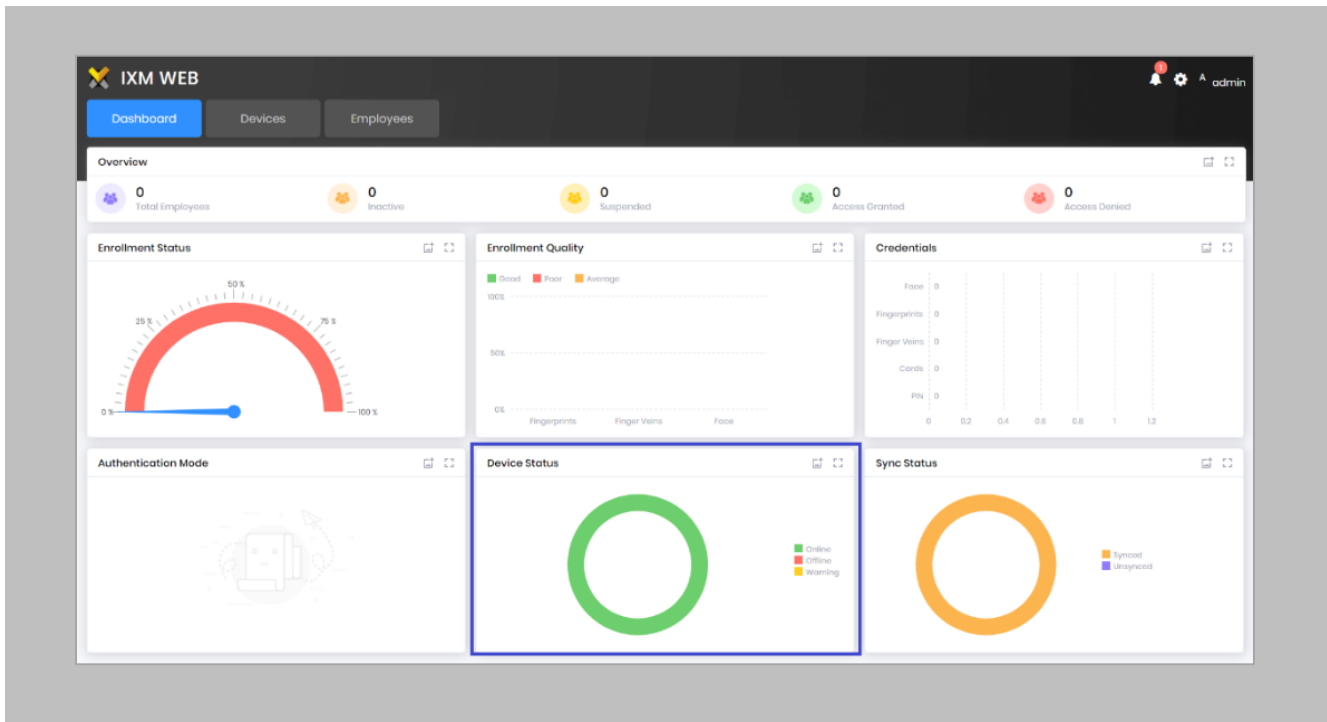


Figure 44: IXM WEB - Dashboard, Device Status

13. Adding an Invixium Device to a Device Group

Procedure

STEP 1

Go to **Devices** → **Groups**.

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

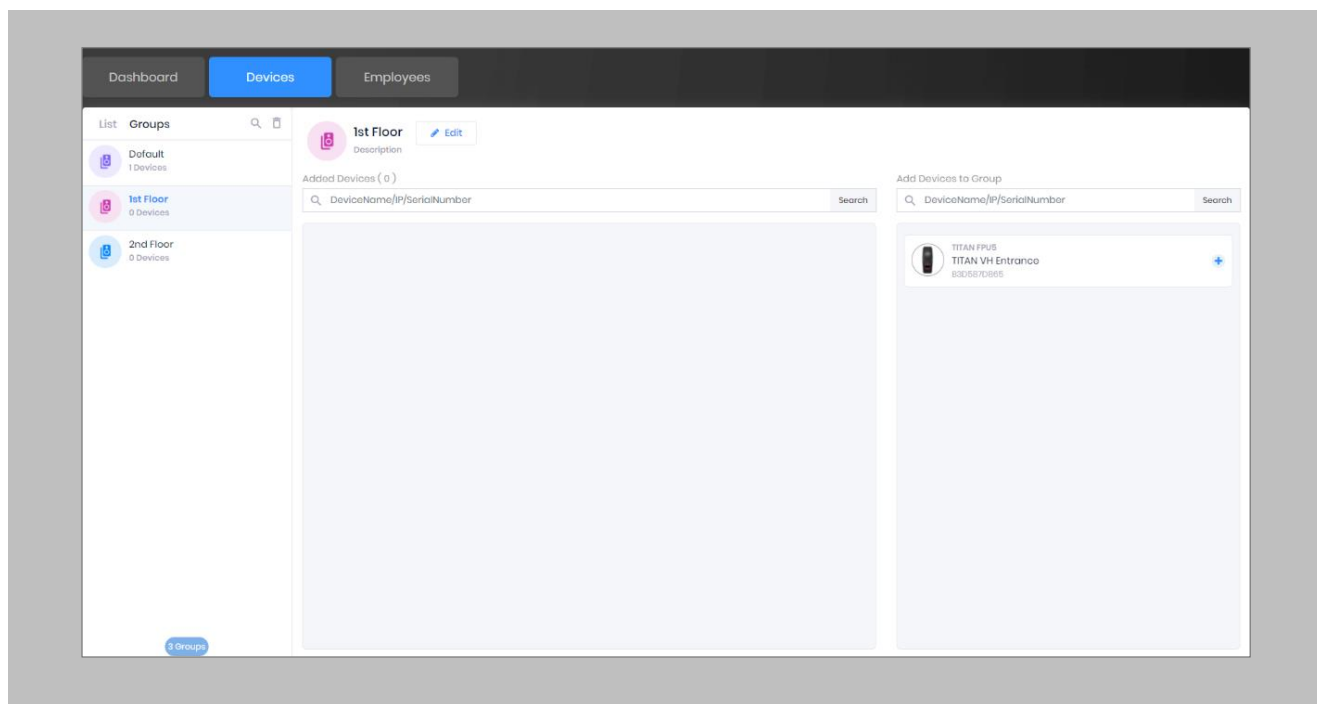



Figure 45: IXM WEB - Assign Device Group

Configuring Wiegand to Assign Invixium Readers

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

STEP 1

From Home >> Expand the Left Navigation Pane >> Navigate to the **General Settings** tab >> Click the **Wiegand** app to open the Wiegand Format settings.

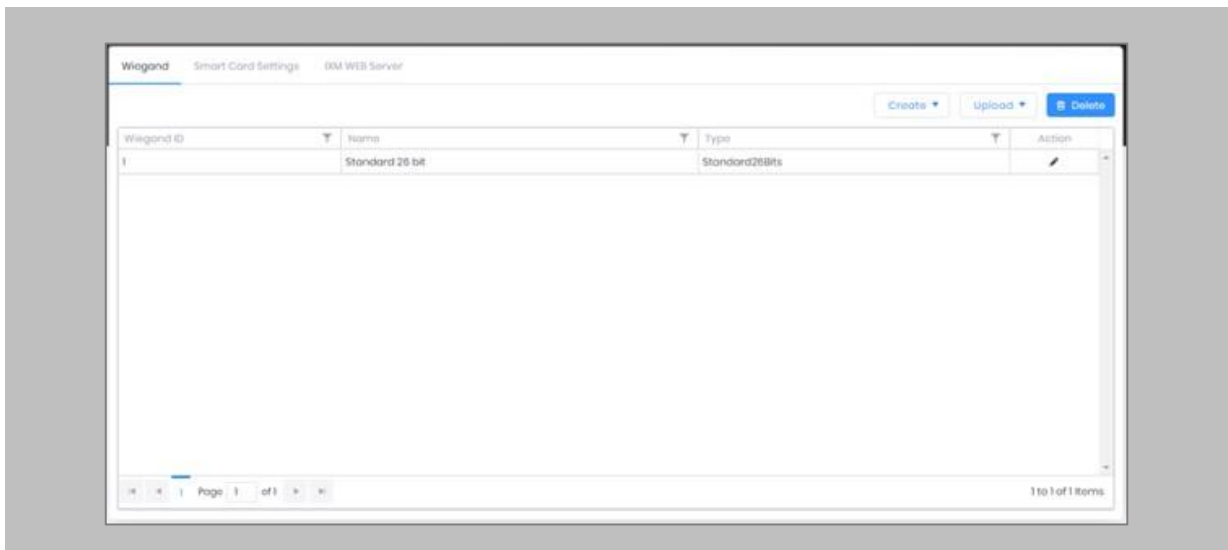


Figure 46: IXM WEB - Create Wiegand Format

STEP 2

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

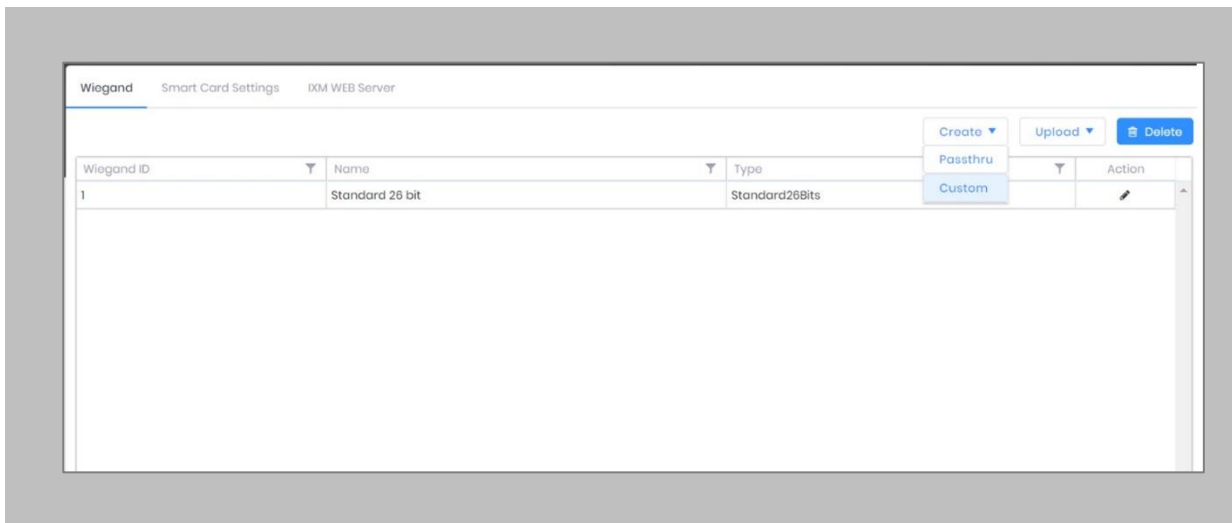


Figure 47: IXM WEB - Create Custom Wiegand Format

STEP 3

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

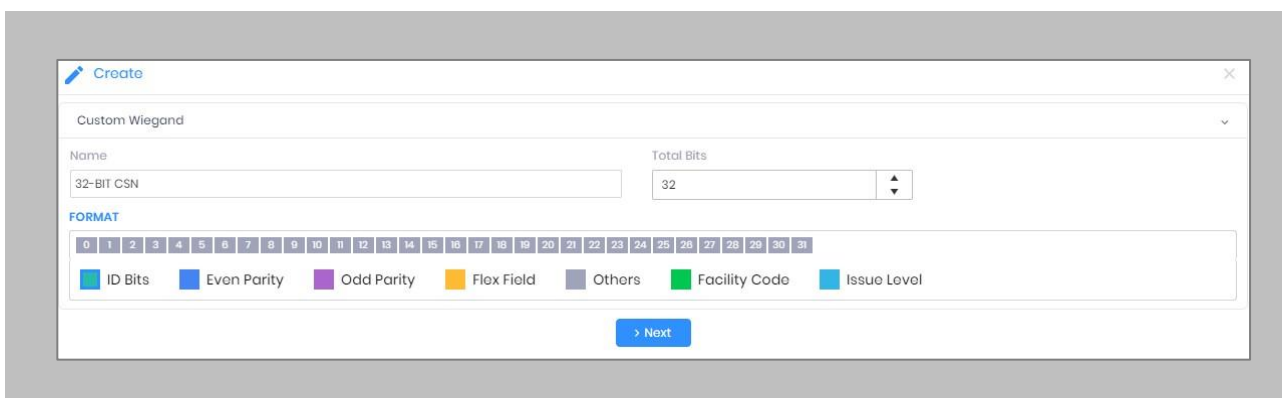


Figure 48: IXM WEB - Custom Wiegand Format

STEP 4

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

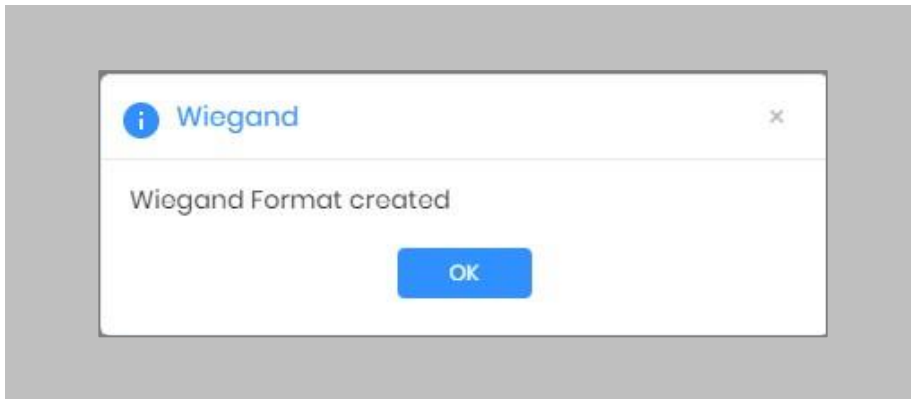


Figure 49: IXM WEB – Custom Wiegand Format Created

STEP 5

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

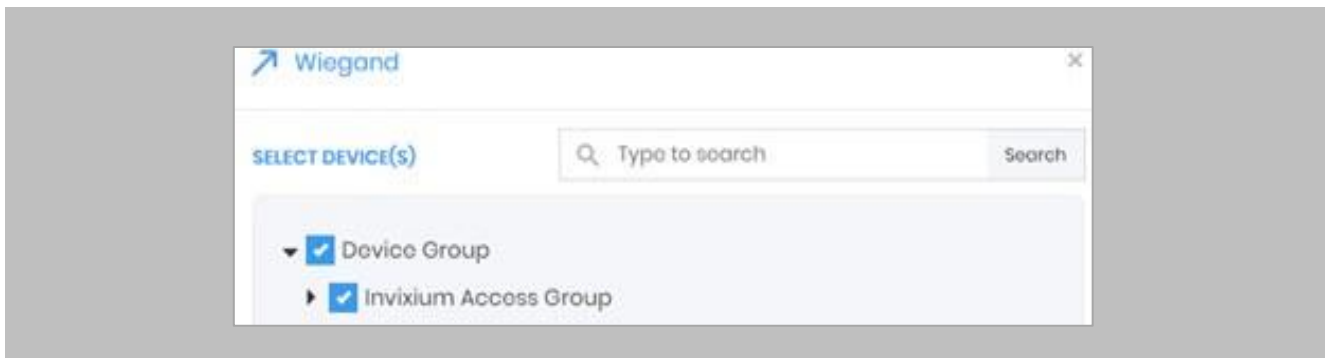


Figure 50: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invisium Readers

Note: Face and finger will always give a Wiegand output based on the initial card that was synced from Lenel-S2 to Invisium.

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

STEP 1

From [Home](#) > click the [Devices](#) tab. Select any device.

STEP 2

Navigate to the [Access Control](#) tab.

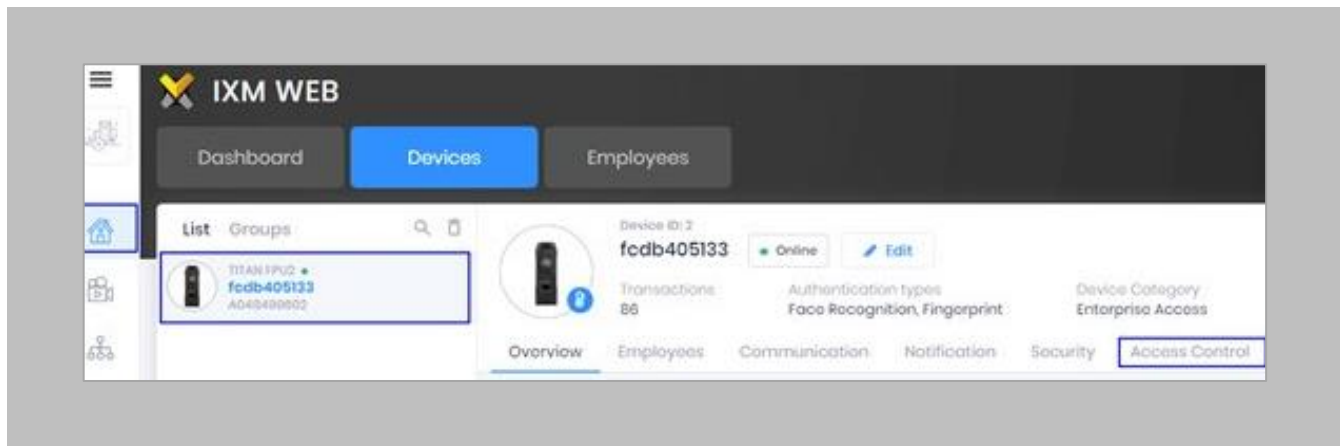


Figure 51: IXM WEB - Navigate to Access Control Tab

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.

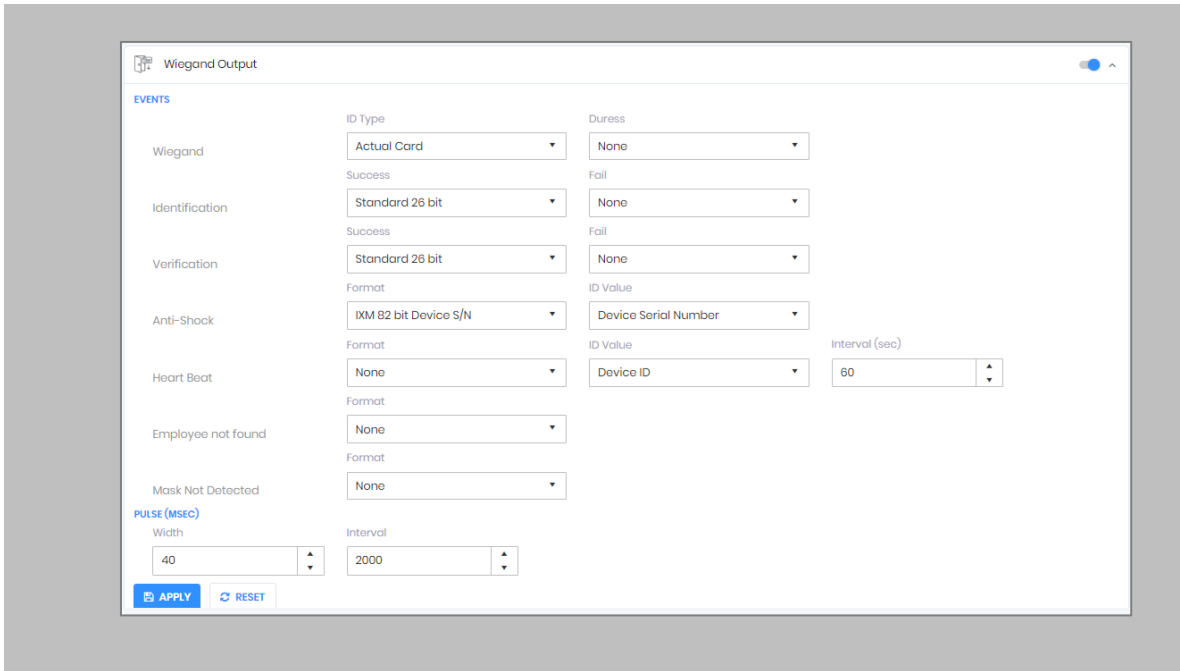


Figure 52: IXM WEB - Wiegand Output

ID types for Wiegand output are as follows:

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


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

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

Employee ID: This is auto generated ID by IXM WEB for an imported cardholder in Lenel-S2.

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

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

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

STEP 4

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

STEP 5

Click **Apply**.

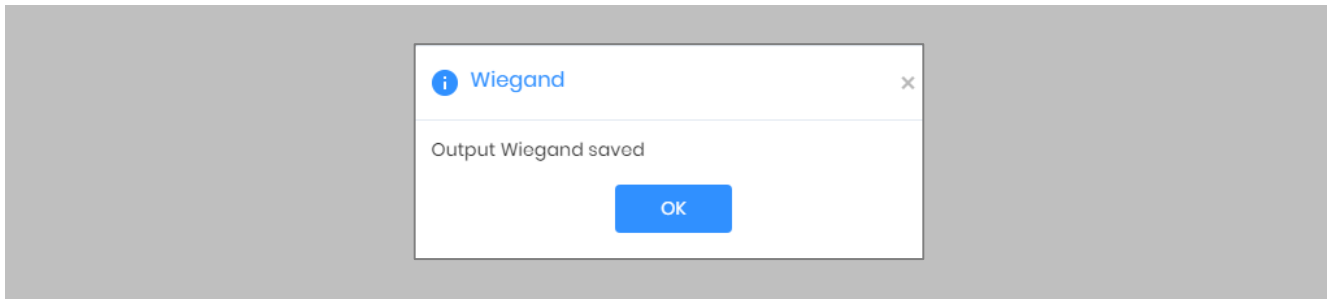


Figure 53: IXM WEB - Save Output Wiegand

RESULT

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



Note:

- If you have more devices, follow the next steps to copy all Wiegand settings to all devices simultaneously. Note: This copies all Wiegand output settings. See Appendix C for more information.
- If the cardholder was assigned multiple cards, the first assigned card will be the 'default' selected card. The details of the card will be sent as the Wiegand bits input to Lenel-S2 Controller.
- To make this Wiegand output work on Lenel-S2, you will need to make sure the Wiegand format is available in Lenel-S2 for use on the controllers talking to the Invixium reader (by Wiegand or OSDP).

Configuring Panel Feedback with Lenel-S2

Procedure

STEP 1

Connect Wiegand Data D0 of the Lenel-S2 Panel with **WDATA_OUT0** of the IXM device, Wiegand Data D1 of the Lenel-S2 Panel with WDATA_OUT1, and Wiegand Ground of the Lenel-S2 Panel with WGND of the IXM Device.

STEP 2

Connect the **LED** of the Lenel-S2 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**.

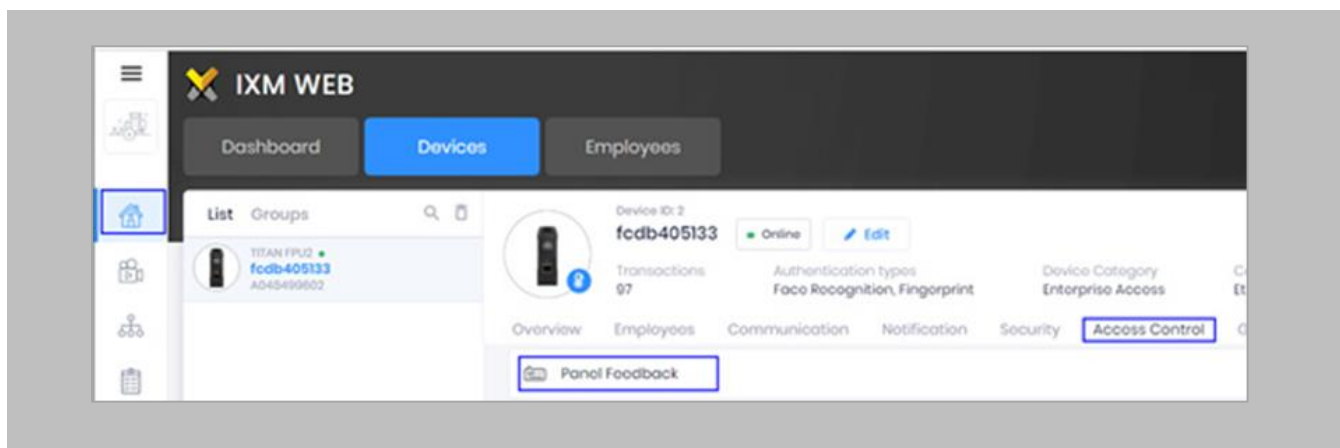


Figure 54: IXM WEB - Panel Feedback

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**.

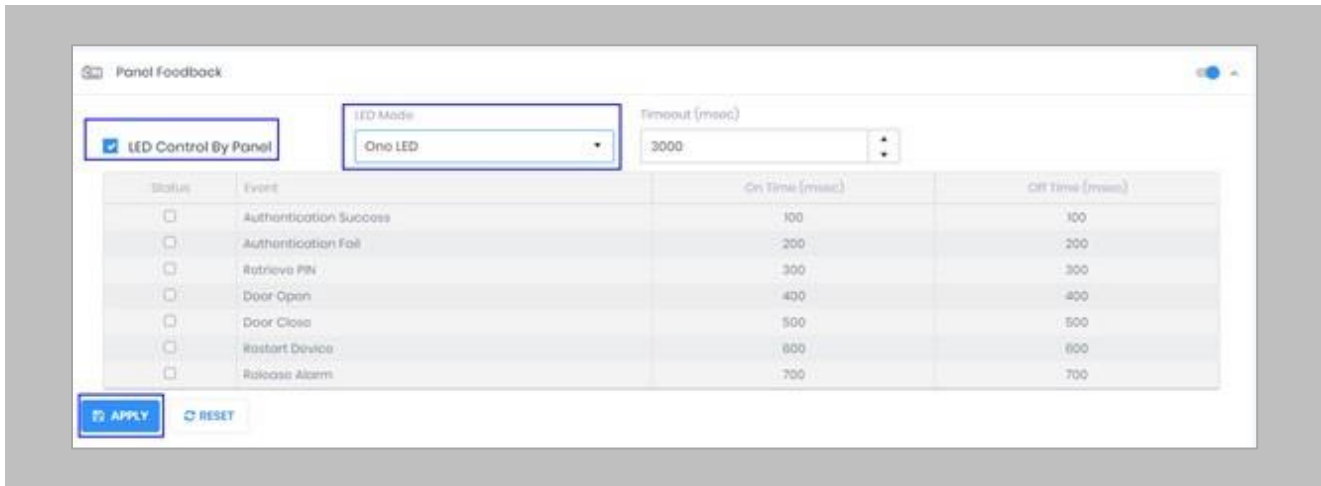


Figure 55: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.

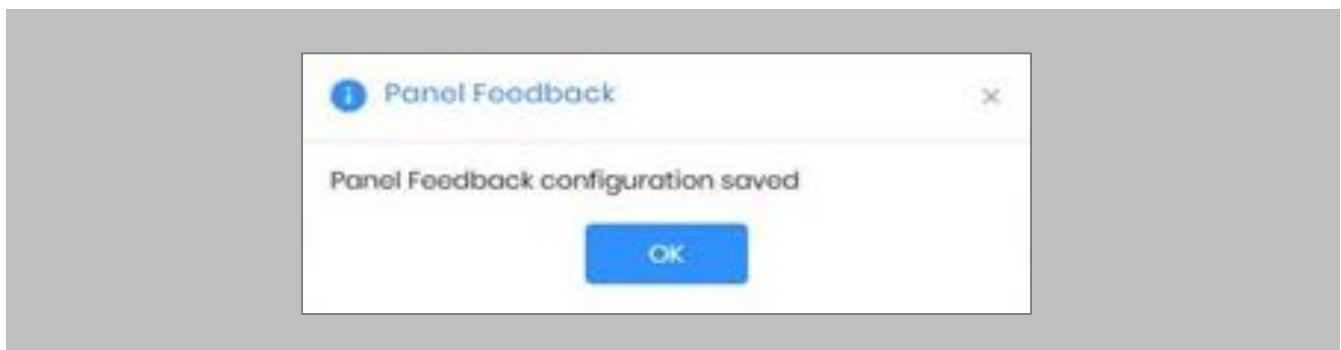


Figure 56: IXM WEB - Save Panel Feedback

Configuring Thermal Settings



Note: confirm your device is capable of temperature screening first.

Procedure

STEP 1

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

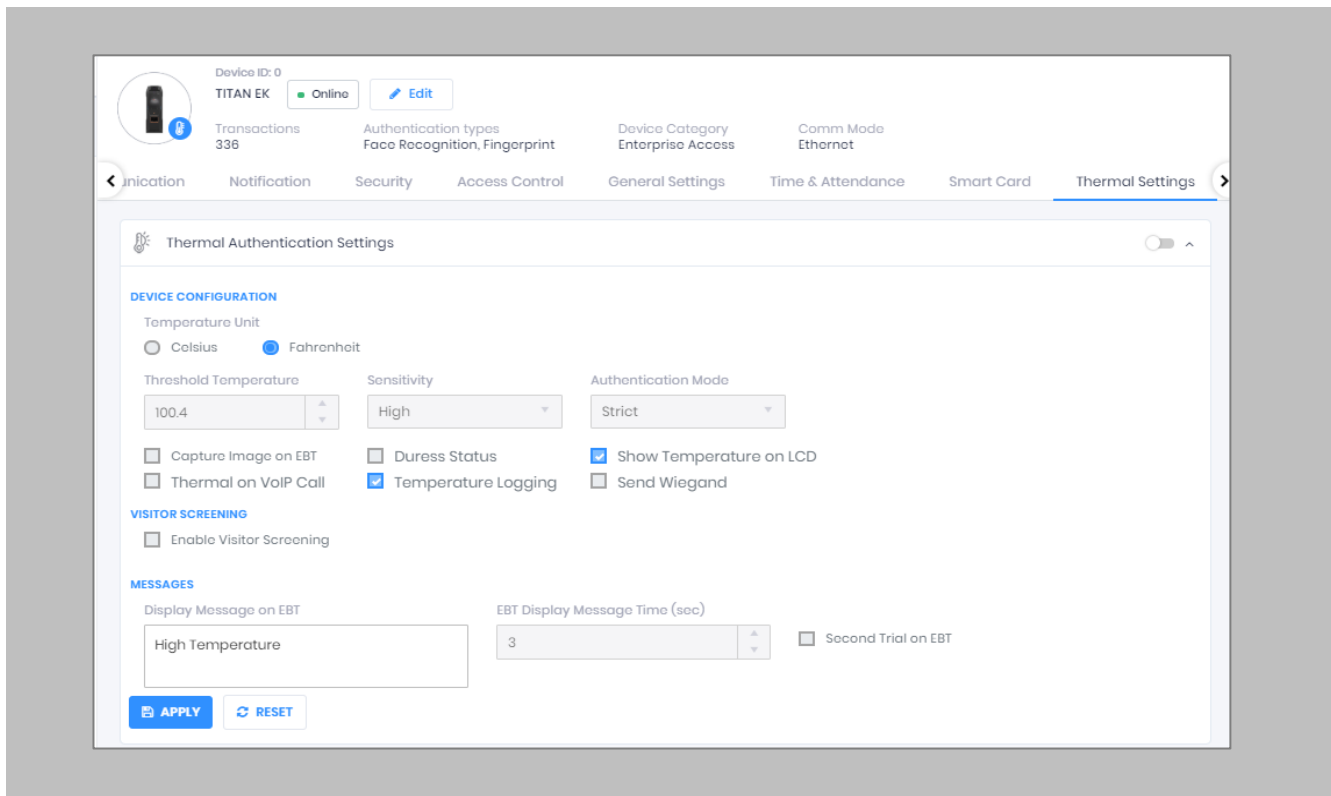


Figure 57: IXM WEB - Thermal Settings

STEP 2

The list of settings along with their functions are:



-
- **Temperature Unit:** IXM WEB supports Celsius and Fahrenheit temperature units. By default, the selected option will be Fahrenheit.
 - **Threshold Temperature:** Users can set a threshold temperature. Elevated Body Temperature (EBT) workflows will trigger when any user whose temperature is above the threshold value. The default threshold temperature is 100.4 degrees Fahrenheit.
 - **Sensitivity:** Users can set Thermal Sensitivity to low or high.
 - **Authentication Mode:** The user will have two options for the Mode of authentication Soft / Strict, this mode of authentication is used to control the access of the user if fever is detected. The default mode of authentication is Strict.
 - **Soft:** Access will be granted to the End-user even after the fever is detected.
 - **Strict:** Access will be denied if the fever is detected.
 - **Send Wiegand:** This setting will be visible only if the user selects the “Strict” Authentication Mode. Enabling this setting will generate Wiegand whenever “High Face Temperature” is detected in the authentication process.
 - **Capture Image on EBT:** Enable this setting to capture the image of the user if EBT is detected. By default, this setting will remain disabled. The same image will be used for sending email notifications from IXM WEB.
 - **Duress Status:** Enabling this setting will allow access to the user even after detecting EBT if the user authenticates using their pre-programmed duress finger. The default setting is disabled.
 - **Show Temperature on LCD:** By enabling this setting, TITAN will display the screened temperature upon authentication. By default, this setting is disabled.
 - **Display Message on EBT:** Users can set a message to display after detecting EBT. Users can set a message up to a maximum of 50 characters.
 - **EBT Display Message Time (sec):** Users can configure the length of time that the EBT message stays on the screen. The default time is 3 seconds.

-
- **Second Trial on EBT:** By enabling this setting, users will get a notification to retry after EBT detection. If this setting is enabled, Display Message for Second Trial, Second Trial Wait Time after EBT (mins), and Display Message Time After Second Trial (sec) fields will be visible.
 - **Display Message for Second Trial:** Users can set a message to display after the second trial if EBT is detected. This message can be a maximum of 50 characters.
 - **Second Trial Display Message Time (sec):** Users can configure the length of time that the second trial message stays on the screen. The default time is 3 seconds.
 - **Enable Visitor Screening:** Enable this setting to start screening temperatures for visitors. By default, this field remains disabled.
 - **Visitor Screening Message:** Users can set a message that will be displayed when a visitor is showing their face. Maximum 50 characters allowed.
 - **Visitor Screening Message on EBT:** Users can set a message that will be displayed when the visitor has an EBT. Maximum 50 characters allowed.
 - **Visitor Message Display Time (sec):** Users can configure the length of time that the visitor screening message stays on the screen. The default time is 3 seconds.
 - **Thermal on VoIP Call:** Enable this setting to start screening temperatures for a user when a VoIP call is going on. By default, this field remains disabled.
 - **Temperature Logging:** This setting keeps logging detected temperature in the Transaction Log. By default, this field remains enabled. Users can disable this feature using IXM WEB only. Enable/Disable this setting is not available in LCD.

STEP 3

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

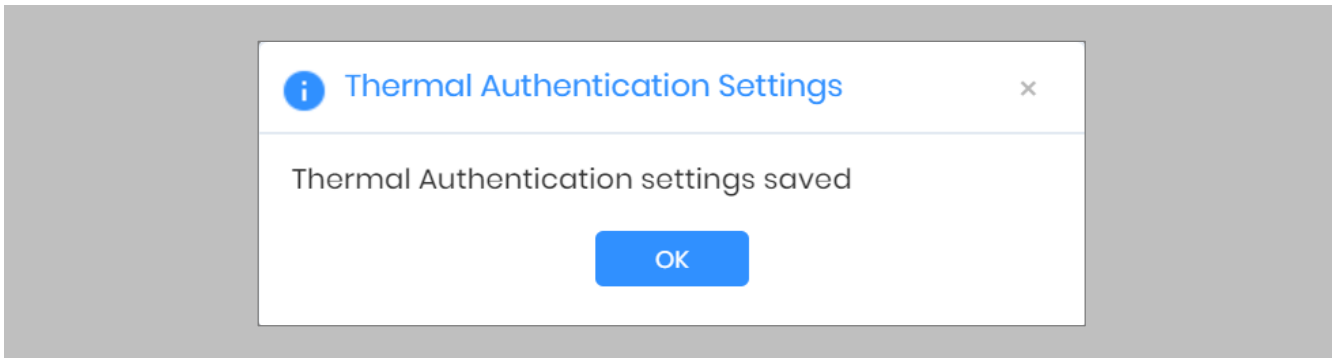


Figure 58: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

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

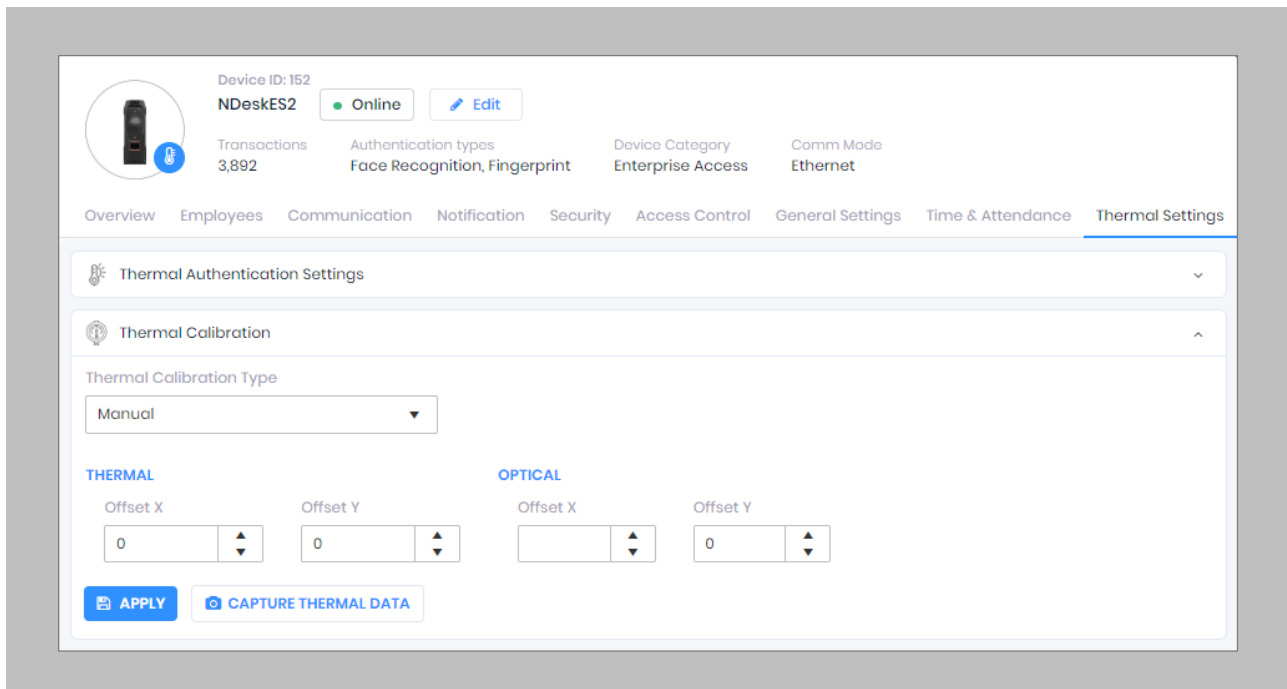


Figure 59: IXM WEB - Thermal Calibration Settings

STEP 2

The settings along with their functions are:

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

Invizium 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**.

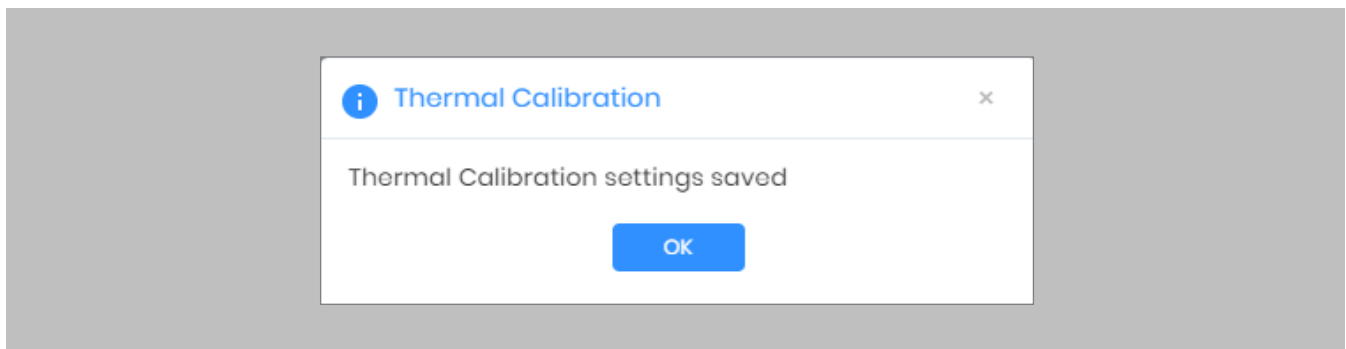


Figure 60: IXM WEB - Save Thermal Calibration Settings

To provide the Thermal Data to the Invixium Technical Services team using IXM WEB, the user needs to click [Capture Thermal Data](#). It will open the popup window and ask the user to show their face 3 times.



Figure 61: IXM WEB - Capture Thermal Data

STEP 4

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

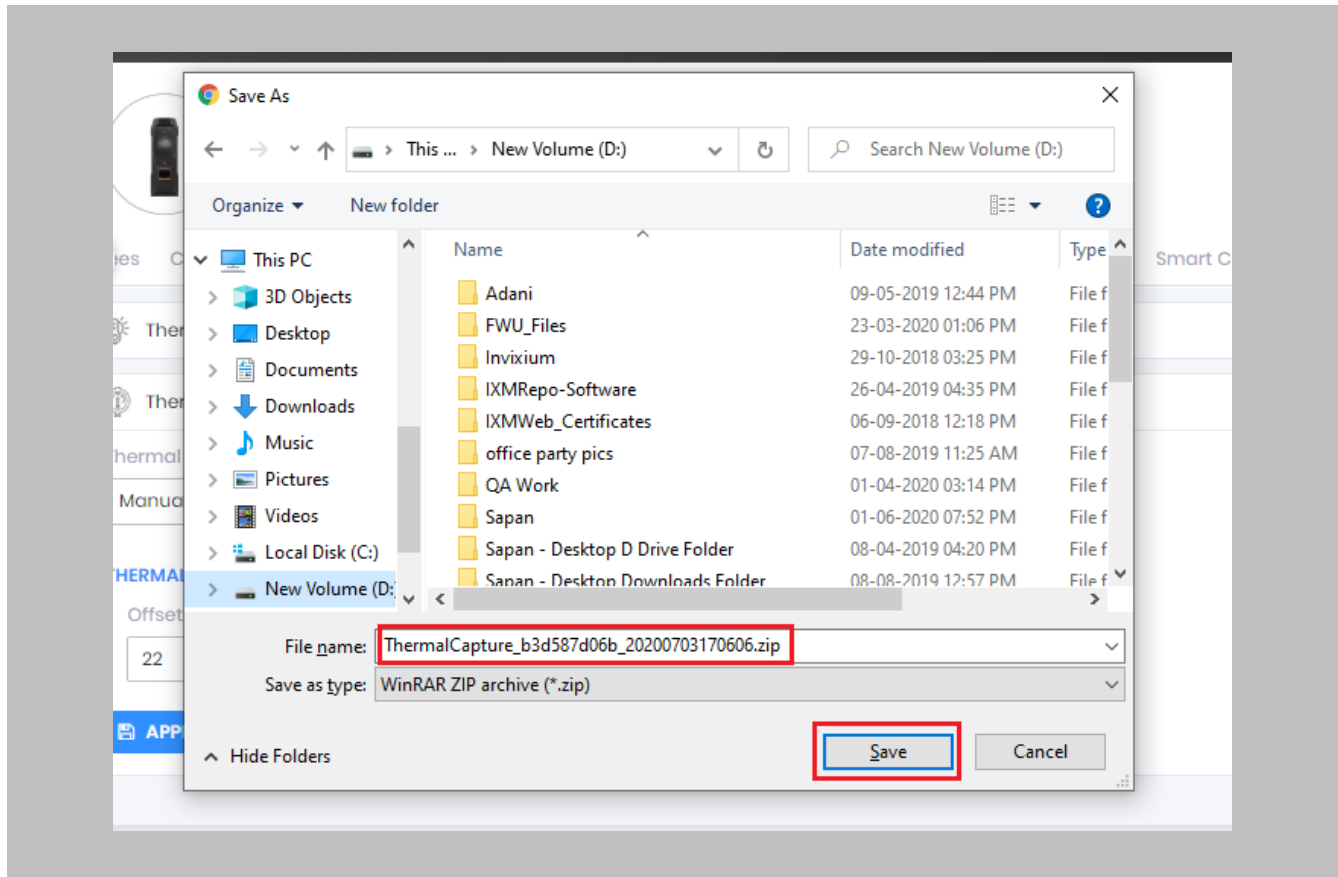



Figure 62: IXM WEB - Save Captured Thermal Data

STEP 5

Click **Save** to store the zip file, then send this file to support@invixium.com. Invixium's Technical Services team will process this file and respond to the user with calibrated values for “X” & “Y” coordinates for the TIR camera and TITAN camera.

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

Test Calibration Options

To test Thermal Calibration, click [Test Calibration](#).

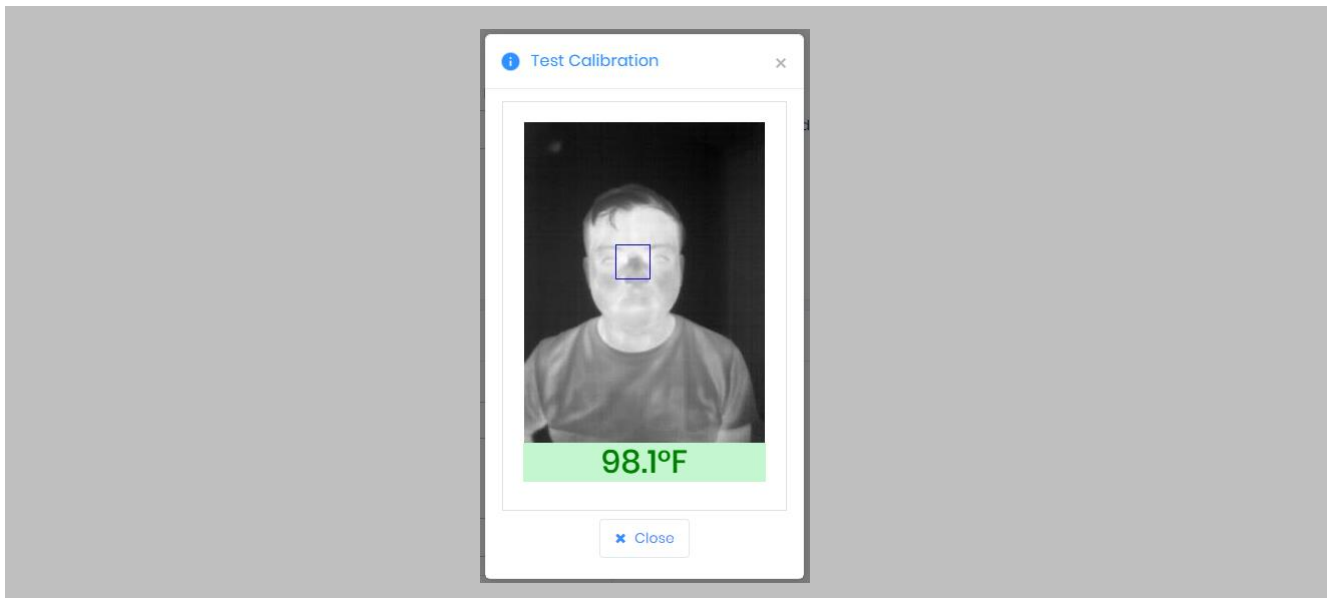



Figure 63: IXM WEB - Test Thermal Calibration

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

Change Temperature Unit Settings

STEP 1

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

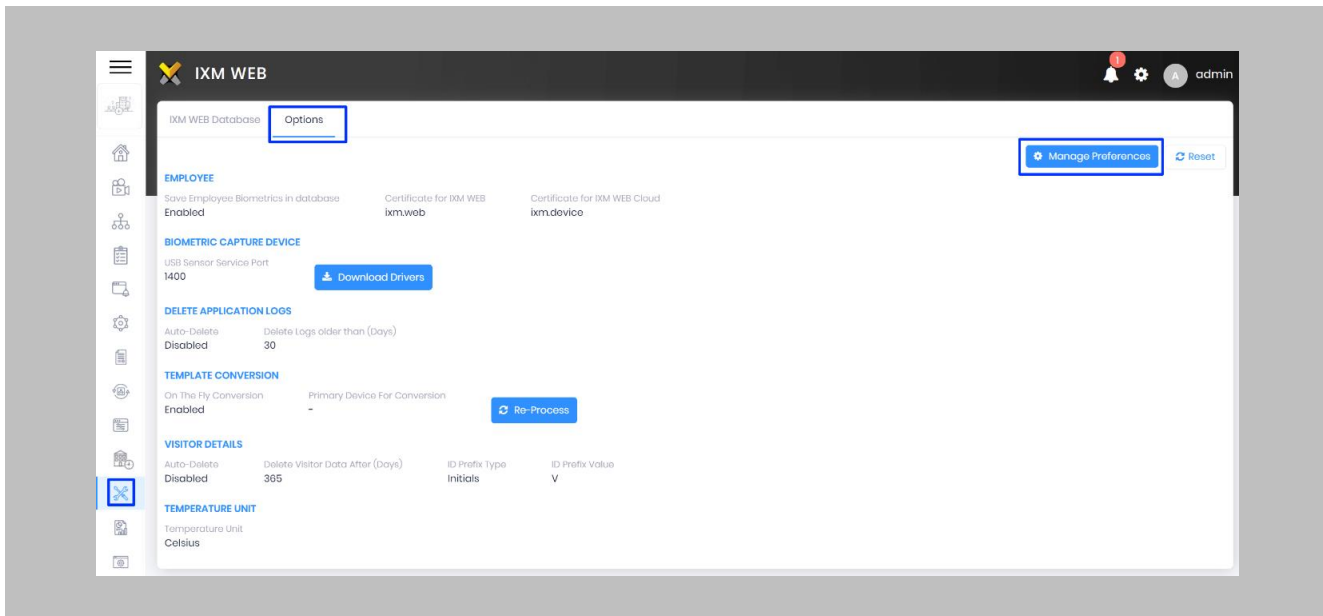


Figure 64: IXM WEB - Option to Change Temperature Unit

STEP 2

Click **Save**.



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

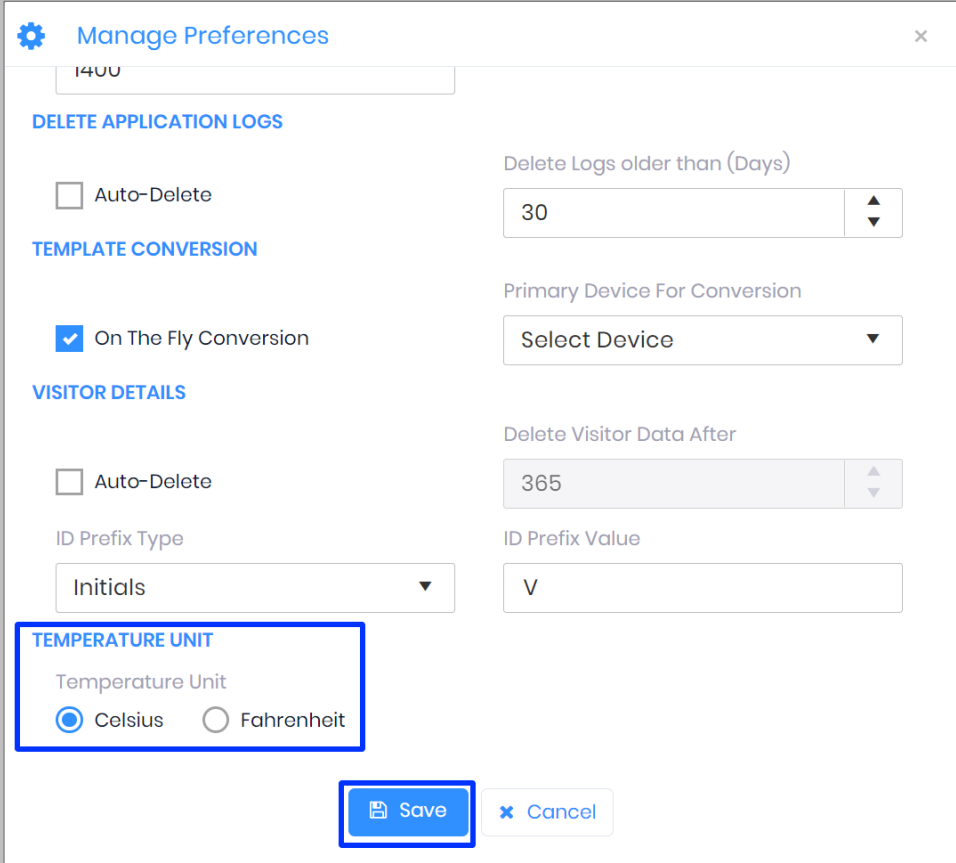


Figure 65: IXM WEB - Save Temperature Unit Setting

Configuring Mask Authentication Settings

STEP 1

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

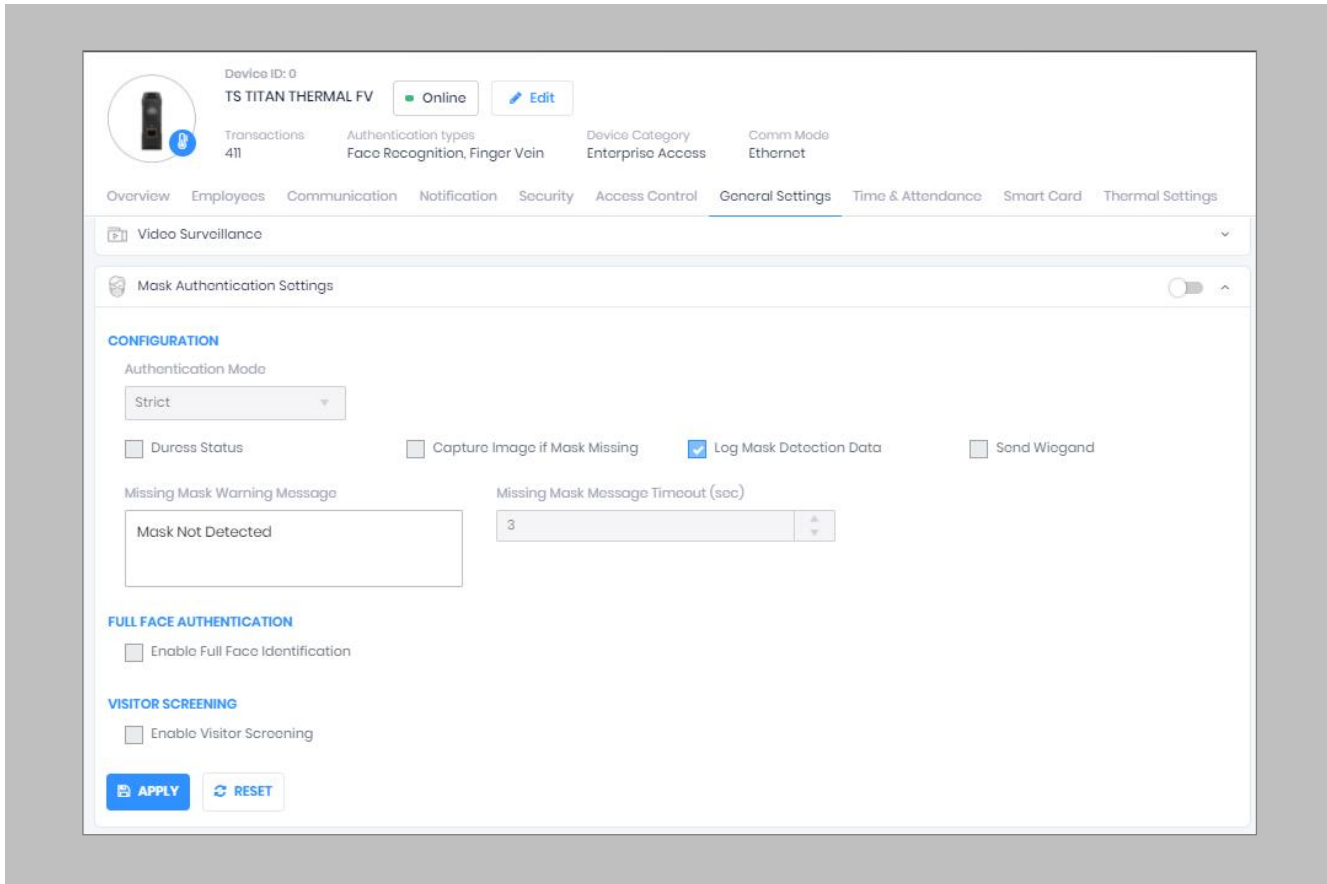


Figure 66: IXM WEB - Mask Authentication Settings

STEP 2

The list of settings is:

- **Authentication Mode:** There are two options for the mode of authentication used to control the access workflow if a mask is not detected. The default mode of authentication is strict.
 - **Soft:** Access will be granted to the user even if a mask is not detected.
 - **Strict:** Access will be denied if a mask is not detected.



-
- **Duress Status:** Enabling this setting would allow access to the user if a mask was not detected if the user authenticates using their pre-programmed duress finger. The default setting is **disabled**.
 - **Capture Image if Mask Missing:** Enable this setting to capture an image of the user if a mask is not detected. By default, this setting is **disabled**. The same image will be used for sending email notifications from IXM WEB.
 - **Log Mask Detection Data:** This setting tracks mask detection in the transaction log. By default, this setting is **enabled**. You can disable this feature using IXM WEB only, not on the device's LCD.
 - **Send Wiegand:** This setting will be visible only in "Strict" authentication mode. Enabling this setting will generate Wiegand whenever a mask is not detected in the authentication process.
 - **Missing Mask Warning Message:** Set a message to display after a mask is not detected. The message can be up to 50 characters.
 - **Missing Mask Warning Message Timeout (sec):** Configure the length of time that the mask is not detected message stays on the screen. The default time is 3 seconds.
 - **Enable Full Face Identification:** Invixium Periocular algorithms can achieve accurate identification using only the eye and eyebrow regions of the face. Full face identification is used to get more accuracy in authentication and capture a user's face without a mask in the image log. By default, this setting is **disabled**.
 - **Remove Mask Display Message:** Set a message to display after a mask is detected when Full Face Identification is enabled. Messages can be up to 50 characters.
 - **Remove Mask Display Message Time (sec):** Configure the length of time that the mask is detected message stays on the screen. The default time is 3 seconds.
 - **Enable Visitor Screening:** Enable this setting to start screening visitors for masks. By default, this field is **disabled**.
 - **Visitor Screening Message:** Set a message that will be displayed when a visitor is showing their face. Messages can be up to 50 characters.

- **Visitor Mask Missing Warning Message:** Set a message that will be displayed when a visitor is screened without a mask. Messages can be up to 50 characters.
- **Visitor Message Display Time(sec):** Configure the length of time that the visitor screening message stays on the screen. The default time is 3 seconds.

STEP 3

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

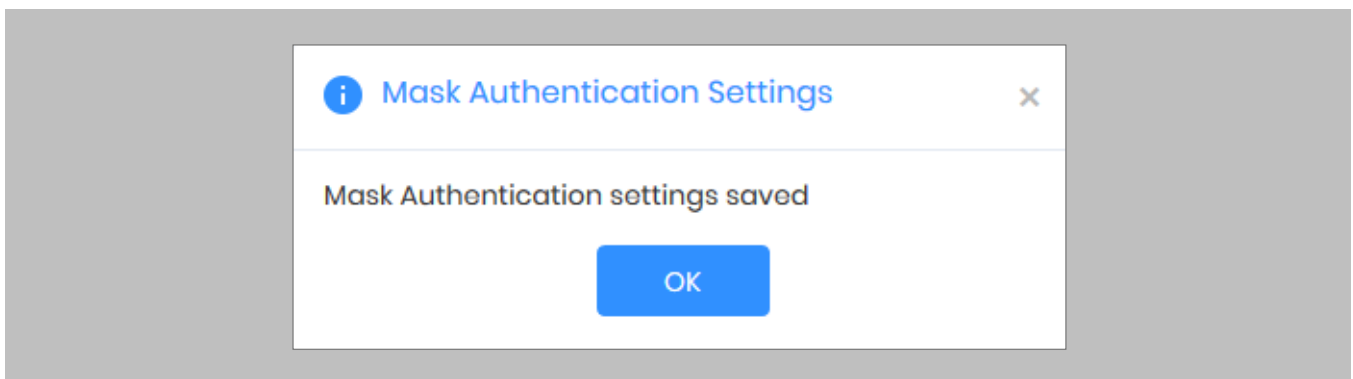


Figure 67: IXM WEB - Save Mask Settings

14. Enrollment Best Practices

Fingerprint Enrollment Best Practices

- Invixium recommends using the index, middle, and ring fingers for enrollment.
- Make sure your finger is flat and centered on the sensor scanning area.
- The finger should not be at an angle and should be straight when placed on the sensor.
- Ensure that the finger is not too dry or too wet. Moisten your finger during enrollment if required.

Avoid Poor Fingerprint Conditions

- Wet Finger: Wipe excessive moisture from the finger before placement.
- Dry Finger: Use moisturizer or blow warm breath over the finger before placement.
- Stained Finger: Wipe stains from finger before placement.

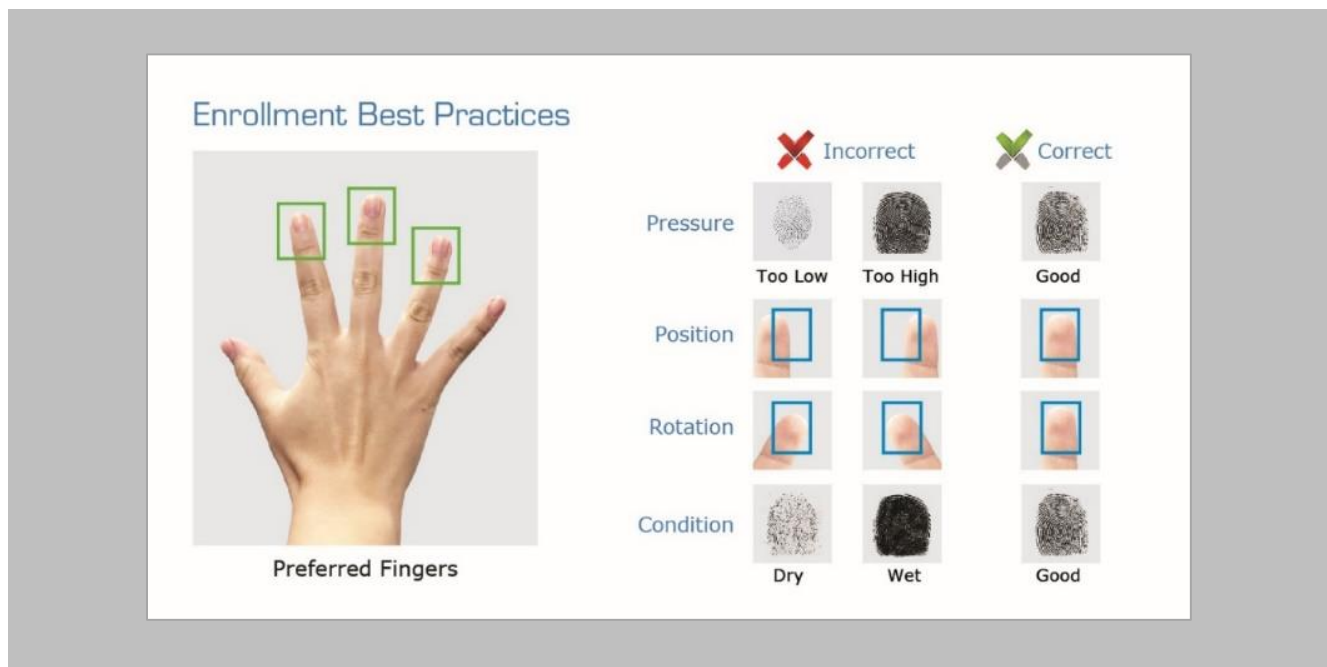


Figure 68: Fingerprint Enrollment Best Practices

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 69: 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.

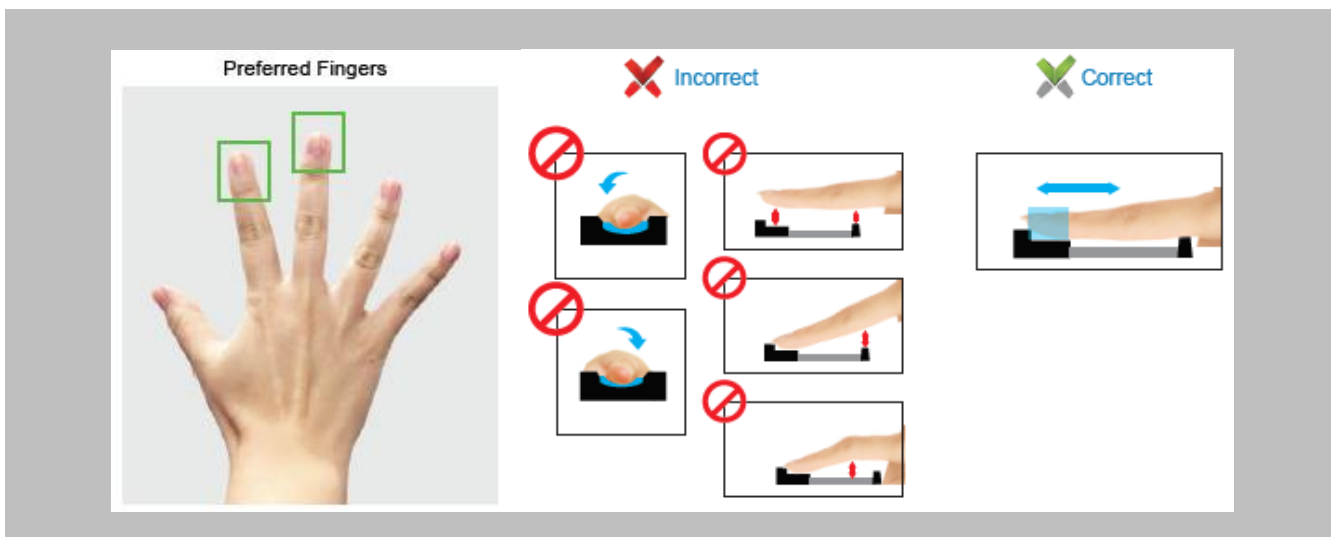


Figure 70: Finger Vein Enrollment Best Practices

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.

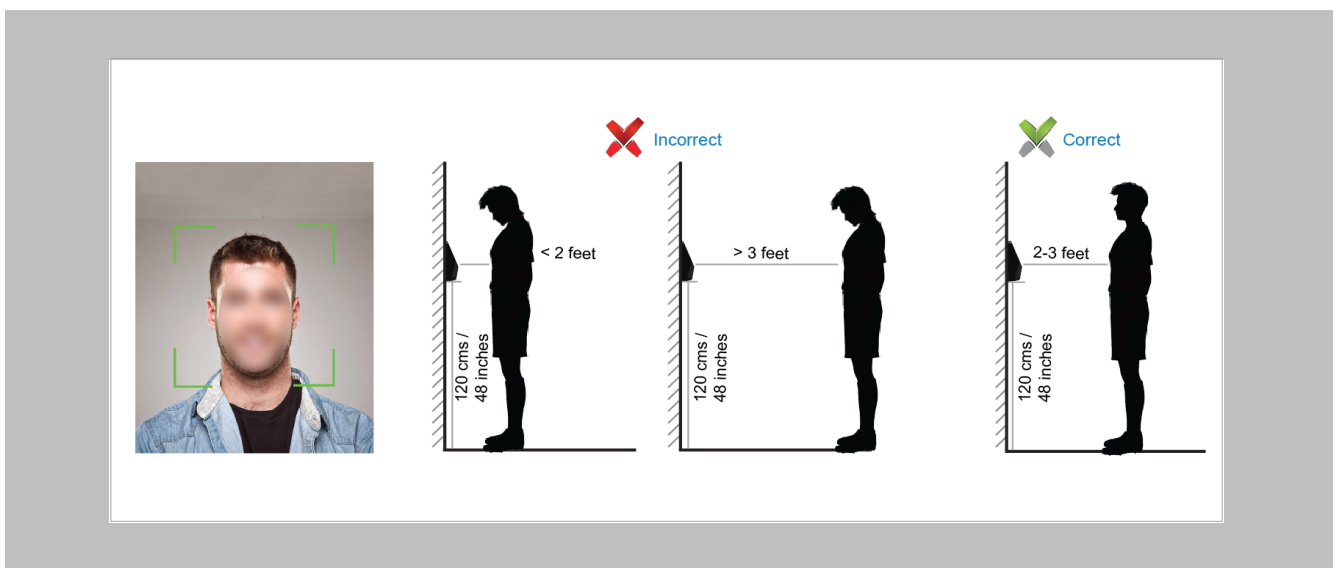


Figure 71: Face Enrollment Best Practices

15. Appendix

Installing Invixium IXM WEB with Default Installation using SQL Server 2014



Note:

- By default, the IXM WEB installer will install SQL server 2014
- It is highly recommended to use SQL server 2016 or higher

If it is intended for IXM WEB to use a non-default SQL 2014 installed instance, please refer to Installing SQL Instance.

Procedure

STEP 1

Run the [installer.exe](#)

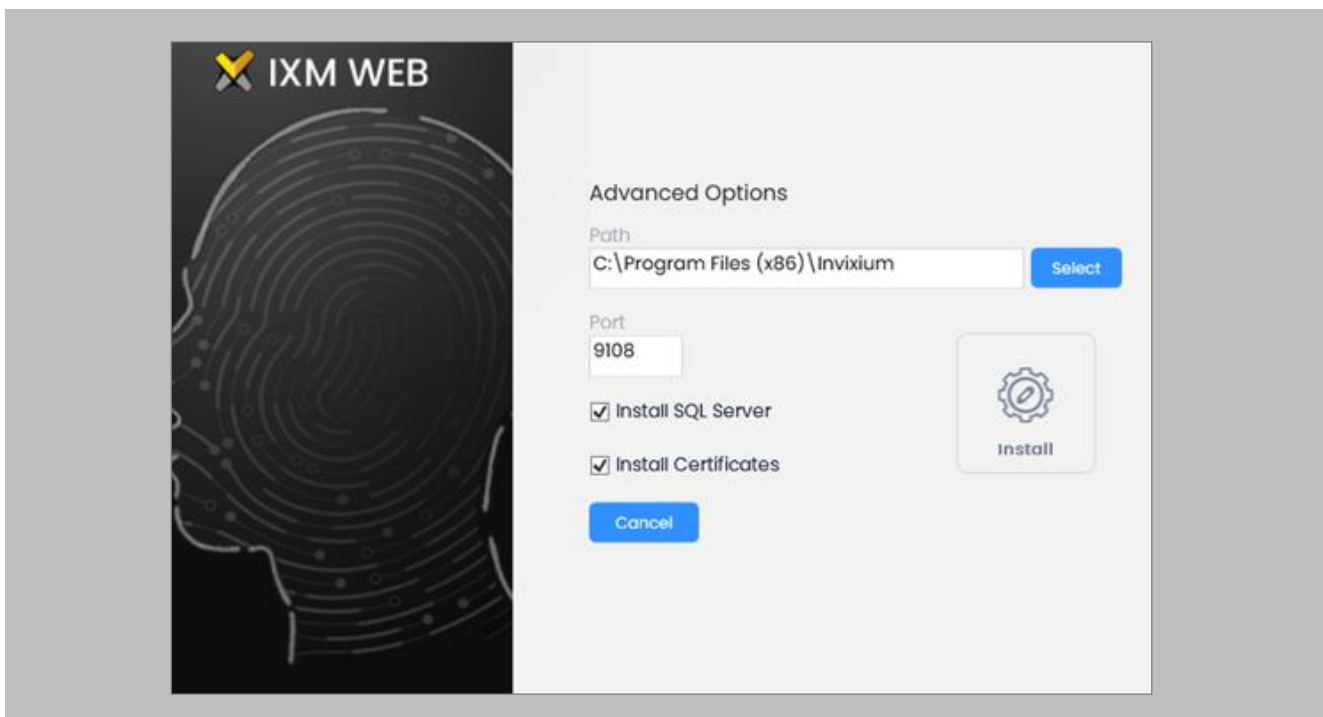


Figure 72: Install IXM WEB



Note: Installs SQL 2014 Express.

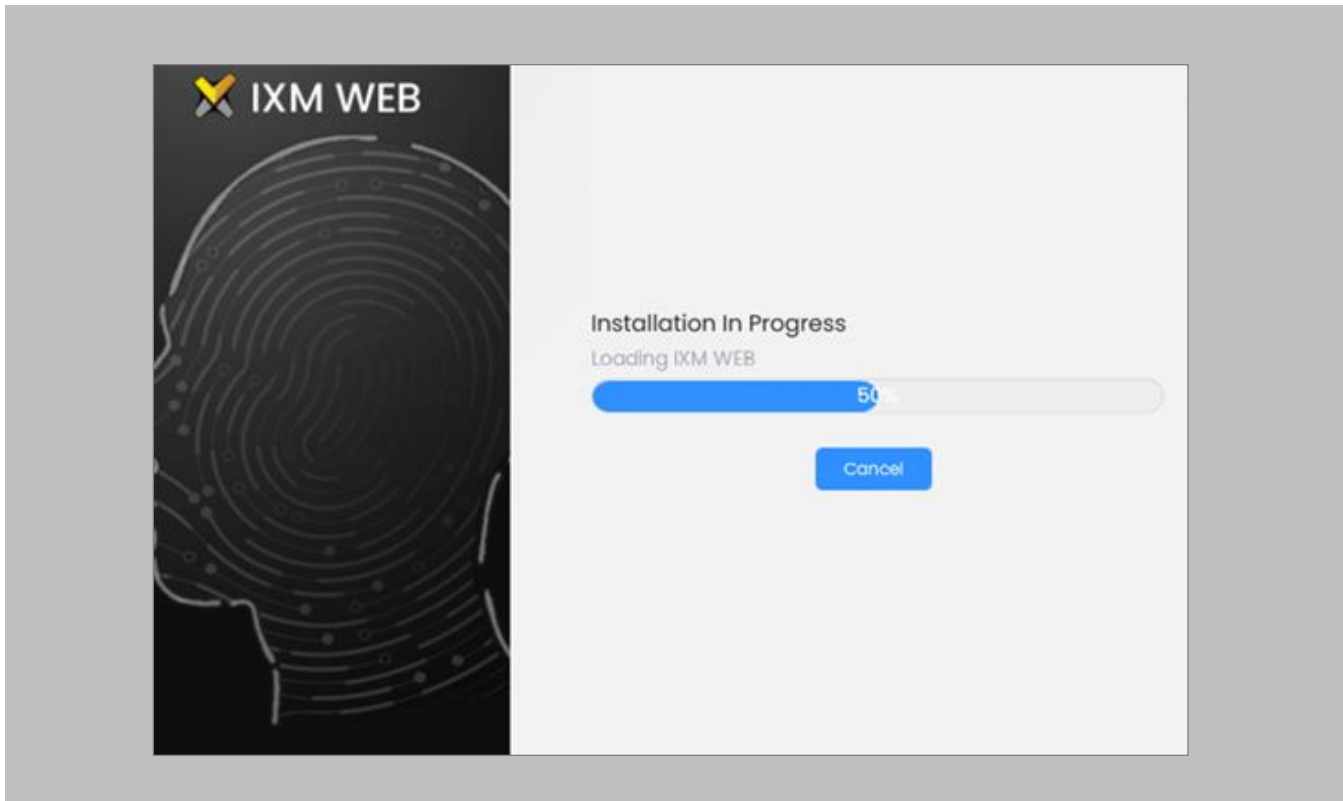


Figure 73: Loading SQL Express & Installation Progress

STEP 2

Once the installation is completed, check these services to make sure they are all running:

- Bonjour
- Invixium Device Discovery
- IXM WEB

STEP 3

Run **IXM WEB** by selecting it from the Windows Start menu or your desktop.

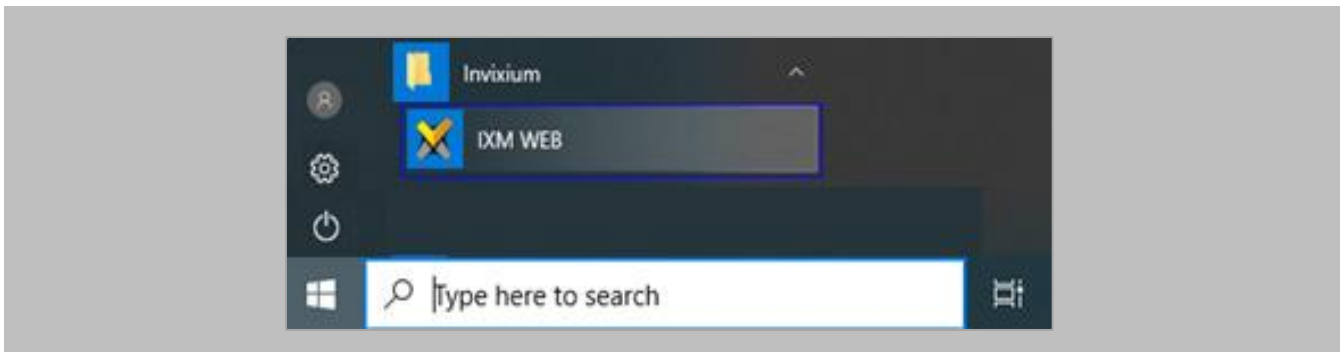


Figure 74: IXM WEB - Shortcut Icon on Desktop

STEP 4

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

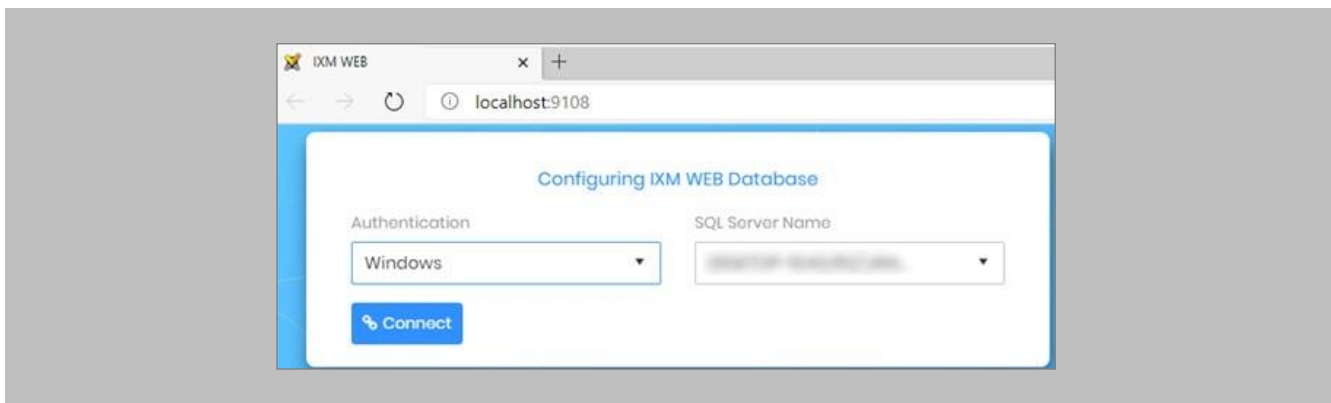
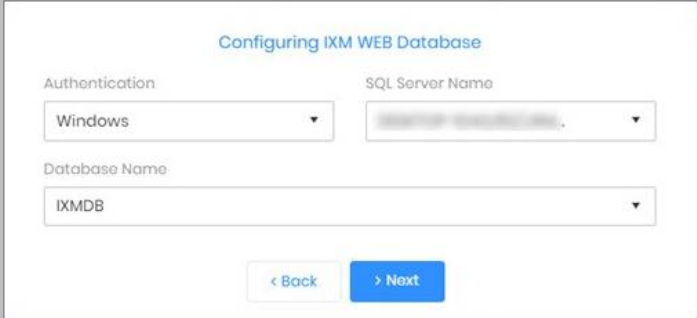


Figure 75: IXM WEB - Configuring IXM WEB Database

STEP 5

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

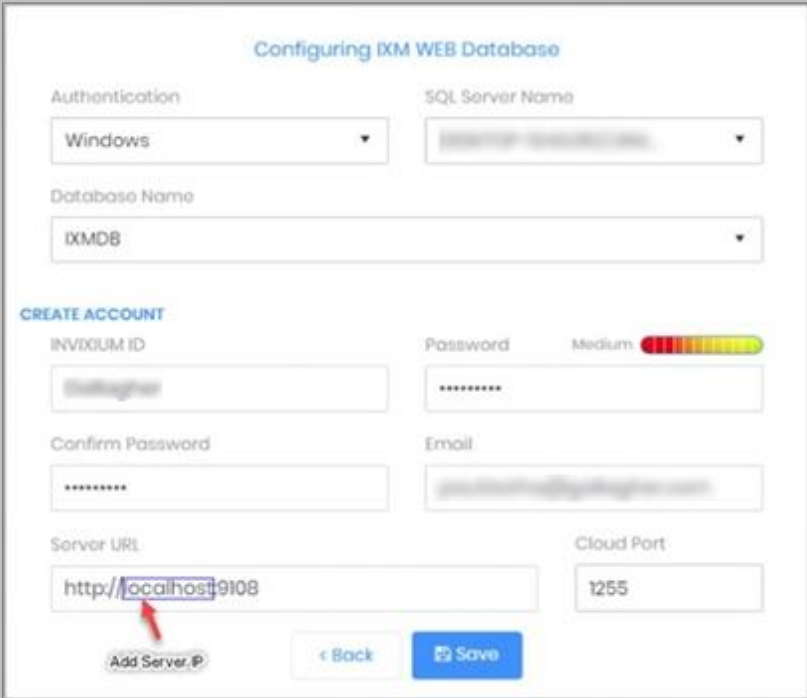


The screenshot shows a web form titled "Configuring IXM WEB Database". It contains three dropdown menus: "Authentication" set to "Windows", "SQL Server Name" set to "localhost", and "Database Name" set to "IXMDB". At the bottom, there are two buttons: "< Back" and "> Next".

Figure 76: IXM WEB - Select Database Name

STEP 6

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



The screenshot shows the "Configuring IXM WEB Database" form with the "CREATE ACCOUNT" section expanded. The fields are: "INVIXIUM ID" (filled with "test@igloo"), "Password" (filled with "*****" and a "Medium" strength indicator), "Confirm Password" (filled with "*****"), "Email" (filled with "test@igloo.com"), "Server URL" (filled with "http://localhost:9108" and a red arrow pointing to "localhost"), and "Cloud Port" (filled with "1255"). At the bottom, there are three buttons: "Add Server IP", "< Back", and "Save".

Figure 77: IXM WEB - Server URL format

STEP 7

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

Pushing Configuration to Multiple Invoxium Readers

Procedure

STEP 1

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

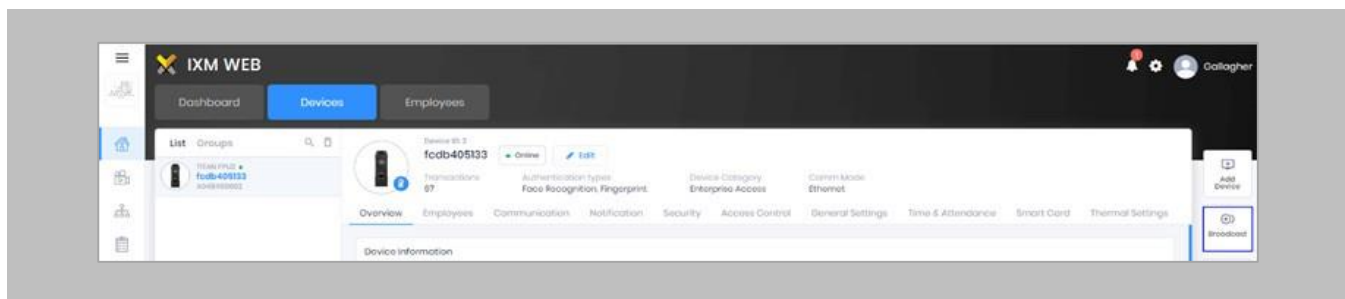


Figure 78: IXM WEB - Broadcast Option

STEP 2

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

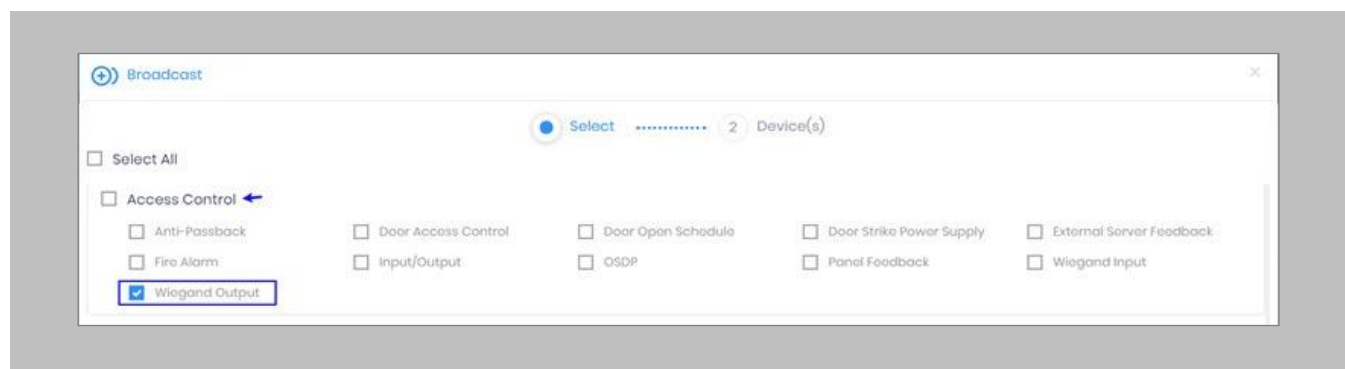


Figure 79: IXM WEB - Wiegand Output Selection in Broadcast

STEP 3

Click **Broadcast**.

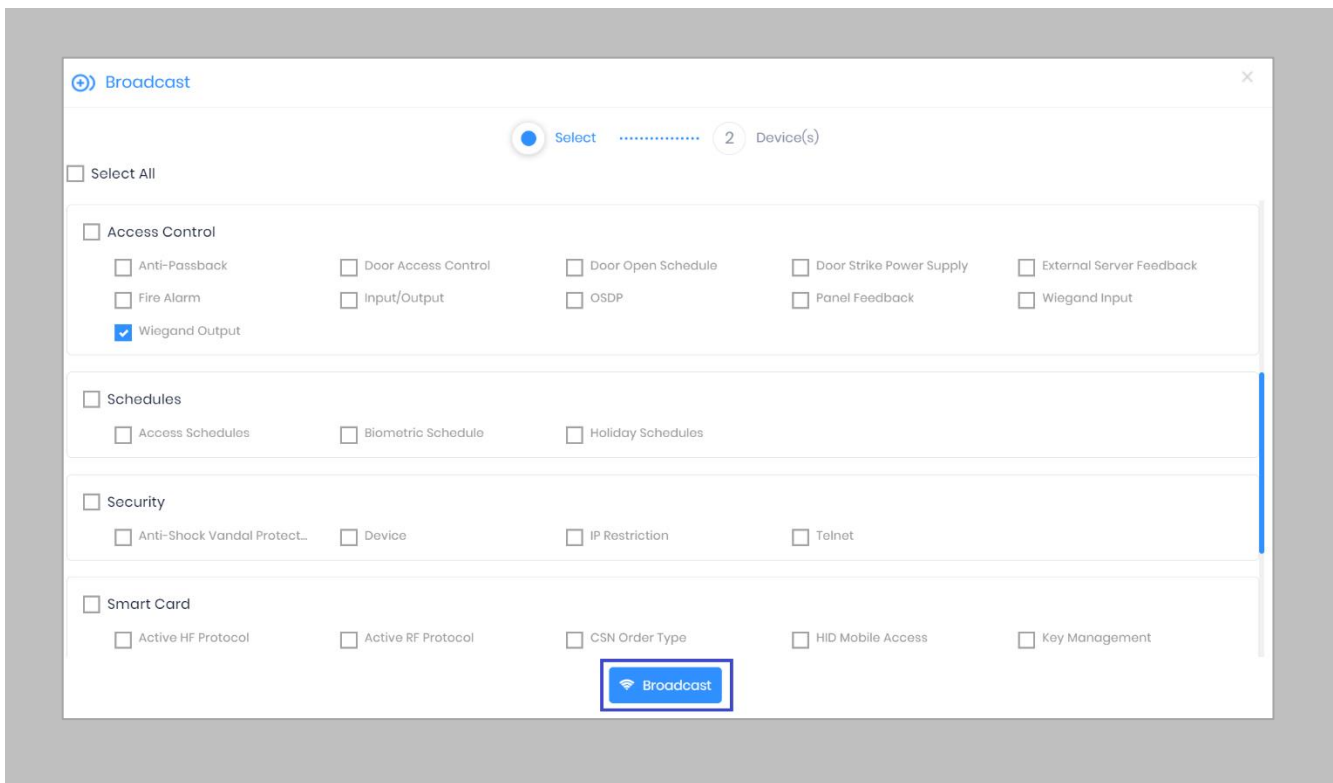


Figure 80: IXM WEB - Broadcast Wiegand Output Settings

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.

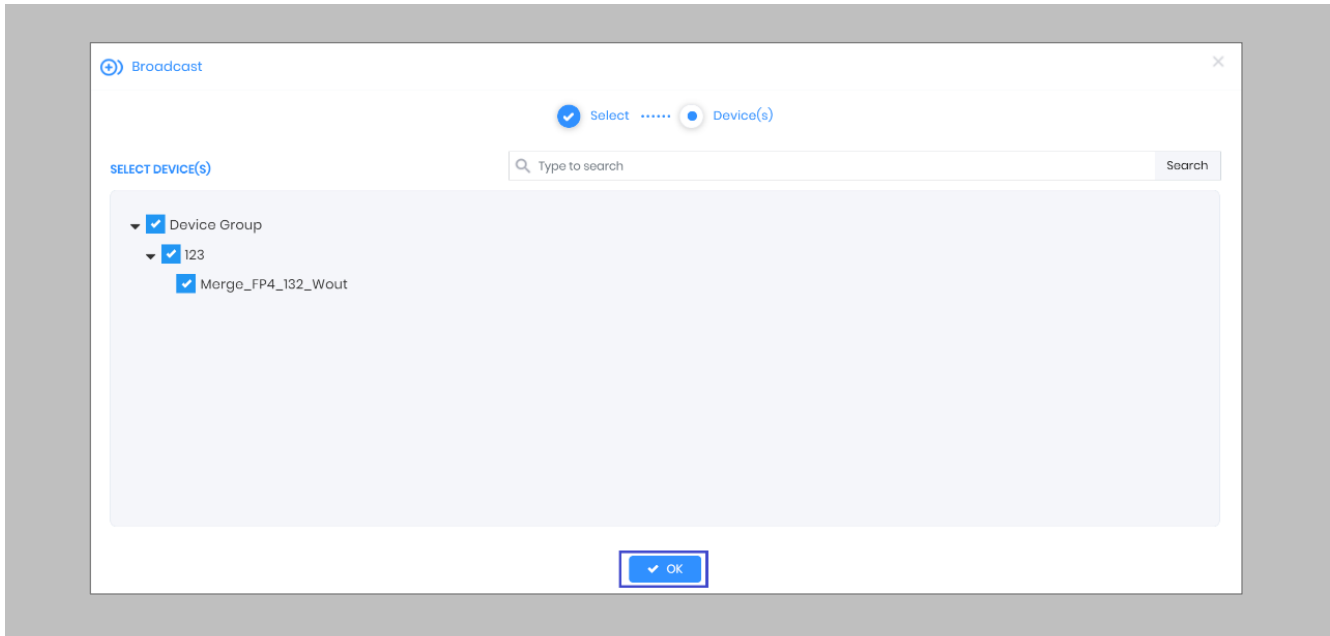


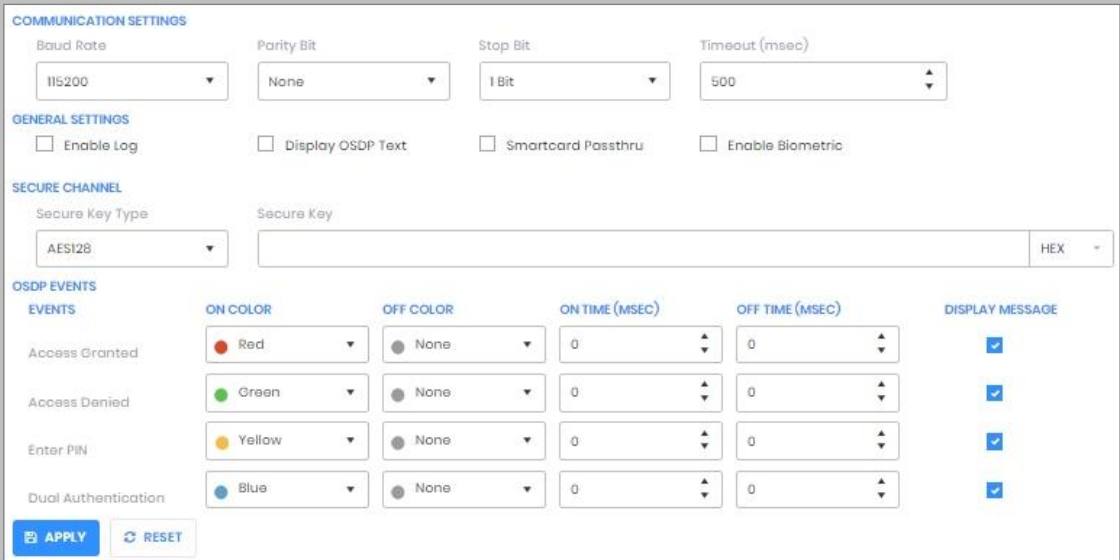
Figure 81: IXM WEB - Broadcast to Devices

Configuring for OSDP Connection

STEP 1

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

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



COMMUNICATION SETTINGS					
Baud Rate	Parity Bit	Stop Bit	Timeout (msec)		
115200	None	1 Bit	500		
GENERAL SETTINGS					
<input type="checkbox"/> Enable Log	<input type="checkbox"/> Display OSDP Text	<input type="checkbox"/> Smartcard Passthru	<input type="checkbox"/> Enable Biometric		
SECURE CHANNEL					
Secure Key Type	Secure Key				HEX
AES128					
OSDP EVENTS					
EVENTS	ON COLOR	OFF COLOR	ON TIME (MSEC)	OFF TIME (MSEC)	DISPLAY MESSAGE
Access Granted	Red	None	0	0	<input checked="" type="checkbox"/>
Access Denied	Green	None	0	0	<input checked="" type="checkbox"/>
Enter PIN	Yellow	None	0	0	<input checked="" type="checkbox"/>
Dual Authentication	Blue	None	0	0	<input checked="" type="checkbox"/>

Figure 82: IXM WEB - OSDP Settings


STEP 2

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

Baud Rate	The baud rate of the serial communication. The value must be the same as the Access Control Panel's value.
Parity Bit	The parity bit of the serial communication. The value must be the same as the Access Control Panel's value.
Stop Bit	The stop bit of the serial communication. The value must be the same as the Access Control Panel's value.
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	<p>The OSDP static events for panel feedback and capture pin are:</p> <ul style="list-style-type: none"> Access Granted Access Denied Enter PIN <p>Dual Authentication – It is an access mode 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-</p>

	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>The LED color configuration is based on panel events. The value must be the same as the Access Control Panel's value. Options are:</p> <ul style="list-style-type: none"> • Red • Green • Yellow • Blue

Table 5: IXM WEB - OSDP Configuration Options

 Note: Mismatches between the unit and Access Control Panel LED configuration would cause unrecognized events.

Display OSDP Text	Enables to display OSDP Text.
Display Message	<p>Notification on the device's screen.</p> <p>If enabled: Displays both the unit hardcoded notification and the Access Control Panel notification. IXM notification - Access Granted or Access Denied. Access Control Panel notification – Valid or Invalid.</p> <p>If disable: Displays only the Access Control Panel notification.</p>



Table 6: IXM WEB - OSDP Text Options

STEP 3

Click **Apply** to save the settings.

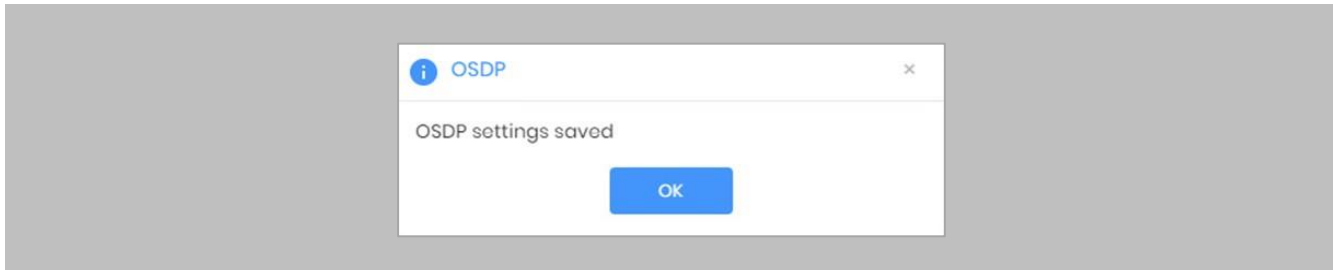


Figure 83: IXM WEB - Save OSDP Settings

STEP 4

Open the edit option on the reader and note the **Device ID**. This will be the address used in the configuration of the reader in the Security Center.

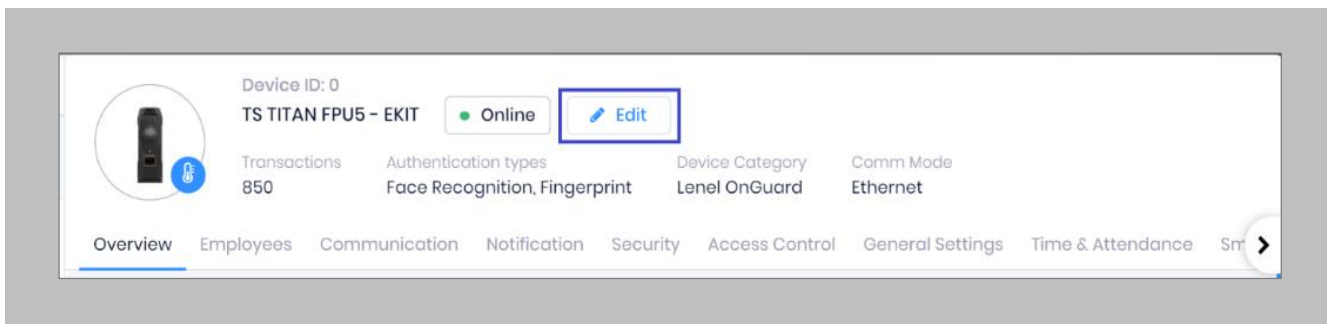


Figure 84: IXM WEB - Edit Device

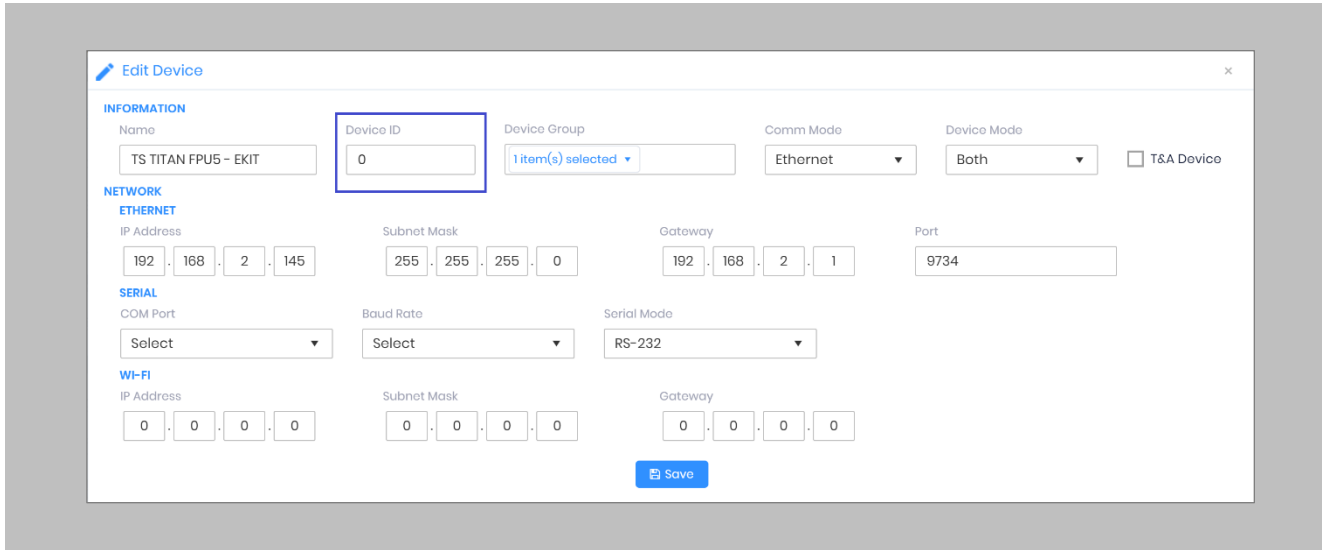


Figure 85: IXM WEB - Edit Device Options

STEP 5

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

STEP 6

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

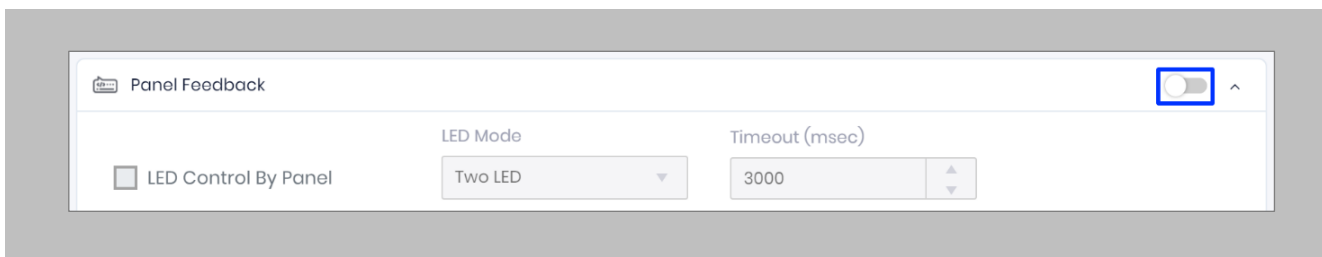


Figure 86: IXM WEB - Disable Panel Feedback

Wiring and Termination

Procedure

Earth Ground

For protection against ESD, Invixium recommends the use of a ground connection between each Invixium device to high-quality earth ground on site.

STEP 1

Connect the **green** and **yellow** earth wire from the wired back cover.

STEP 2

Connect the **open end** of the earth ground wire provided in the install kit box to the **building earth ground**.

STEP 3

Screw the **lug end** of the earth ground.

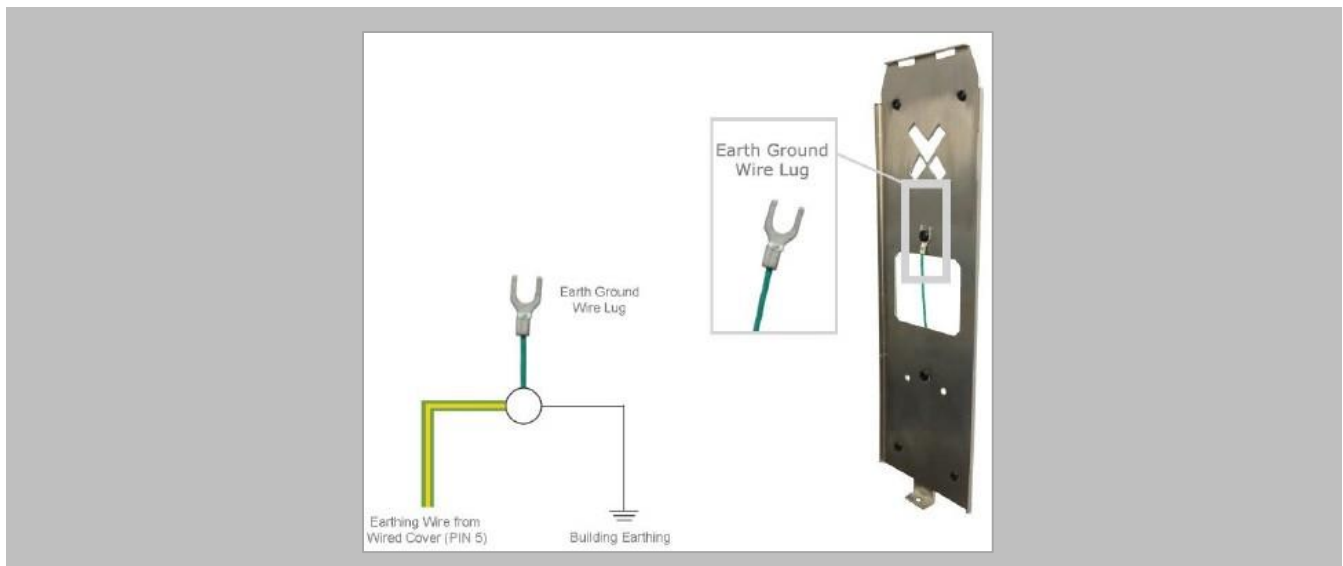


Figure 87: Earth Ground Wiring

Wiring

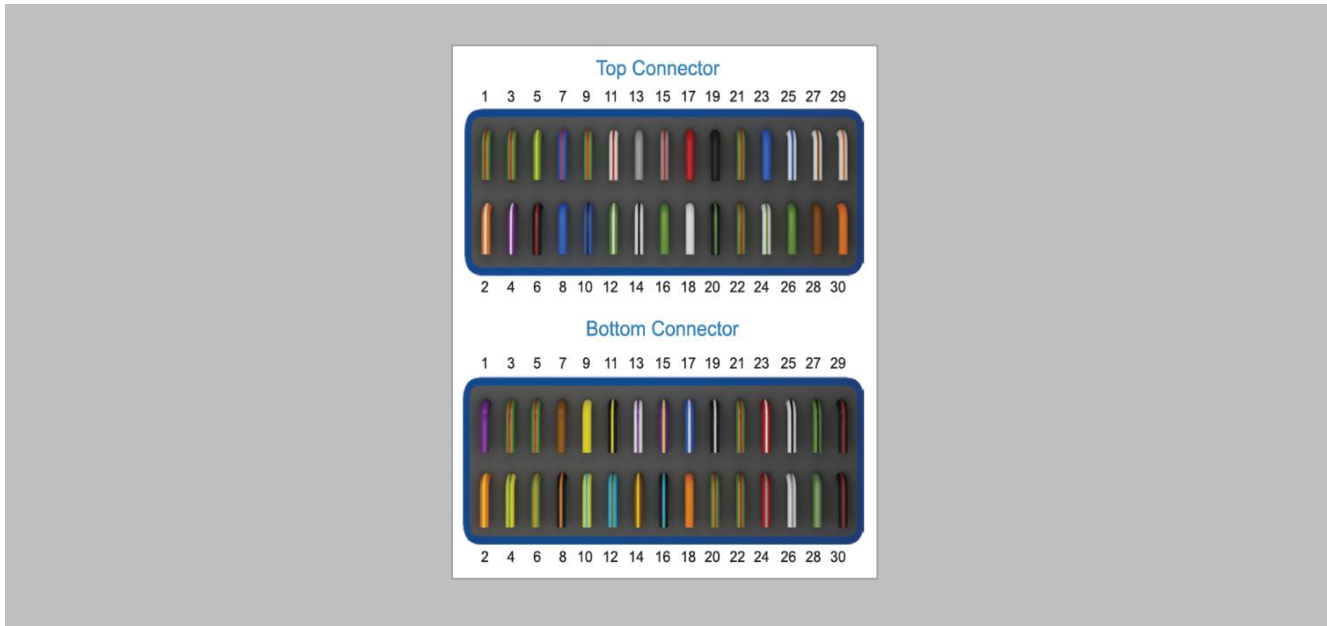


Figure 88: IXM TITAN – Top & Bottom Connector Wiring

Get Wired Top Connector

Wire Color	Wire	Label	Pin(s)	Wire Color	Wire	Label	Pin(s)
Green/Red		RESERVED	1	Green		WDATA_OUT0	16
Orange/White		RS232_RX	2	Red		V_INPUT+	17
Green/Red		RESERVED	3	White		WDATA_OUT1	18
Purple/White		RS232_TX	4	Black		V_INPUT-	19
Green/Yellow		EGND	5	Black/Green		WGND	20
Black/Red		SGND	6	Green/Red		RESERVED	21
Blue/Red		RS485_T	7	Green/Red		RESERVED	22
Blue		RS485_D+	8	RJ 45 Receptacle		TCP/IP	23-30
Green/Red		RESERVED	9	POWER			
Blue/Black		RS485_D-	10	Wiegand			
White/Red		RLY_NC	11	OSDP			
Green/White		WDATA_IN0	12				
Grey		RLY_COM	13				
White/Black		WDATA_IN1	14				
Grey/Red		RLY_NO	15				

Get Wired Bottom Connector

Wire Color	Wire	Label	Pin(s)	Wire Color	Wire	Label	Pin(s)
Purple		DAC_SUPPLY	1	Black/Cyan		SPI_GND	16
Orange/Yellow		SPO1	2	Blue/White		DAC_IN3	17
Green/Red		RESERVED	3	Orange		DAC_OUT	18
Yellow/Green		SPO2	4	Black/White		DAC_IN_GND	19
Green/Red		RESERVED	5	Green/Red		RESERVED	20
Green/Orange		SPO3	6	Green/Red		RESERVED	21
Brown		ACP_LED1	7	Green/Red		RESERVED	22
Black/Orange		SPO_GND	8	Red/White		USB0_VBUS	23
Yellow		ACP_LED2	9	Red/Grey		USB1_VBUS	24
Yellow/Cyan		SPI1	10	White/Black		USB0_D-	25
Black/Yellow		ACP_LED_GND	11	White/Grey		USB1_D-	26
Cyan/Brown		SPI2	12	Green/Black		USB0_D+	27
White/Purple		DAC_IN1	13	Green/Grey		USB1_D+	28
Brown/Yellow		SPI3	14	Black/Red		USB0_GND	29
Purple/Yellow		DAC_IN2	15	Black/Red		USB1_GND	30

Figure 89: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand, and OSDP.

Invixium devices can be integrated with Lenel-S2 Controller on:

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

Wiegand Connection

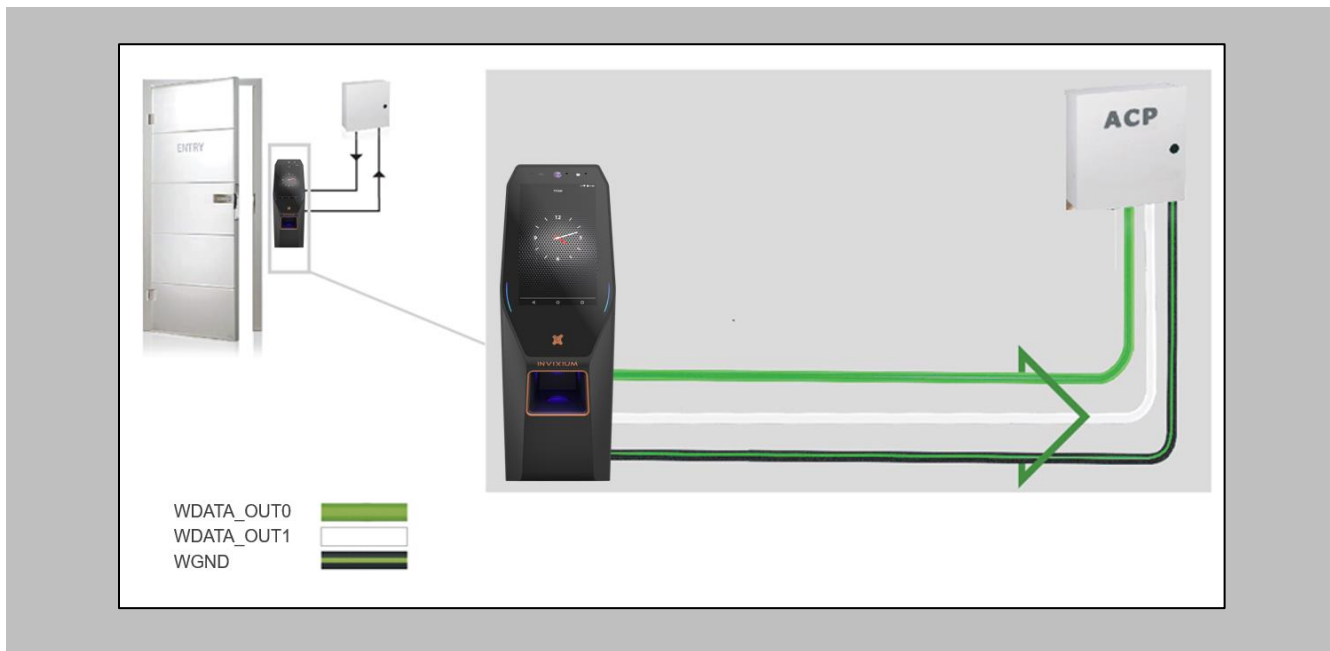



Figure 90: IXM TITAN - Wiegand

 Please refer to the INGUIDE document provided for each product on [Invixium.com](https://www.invixium.com) under the **Download** section of the **Products** menu.

Wiegand Connection with Panel Feedback

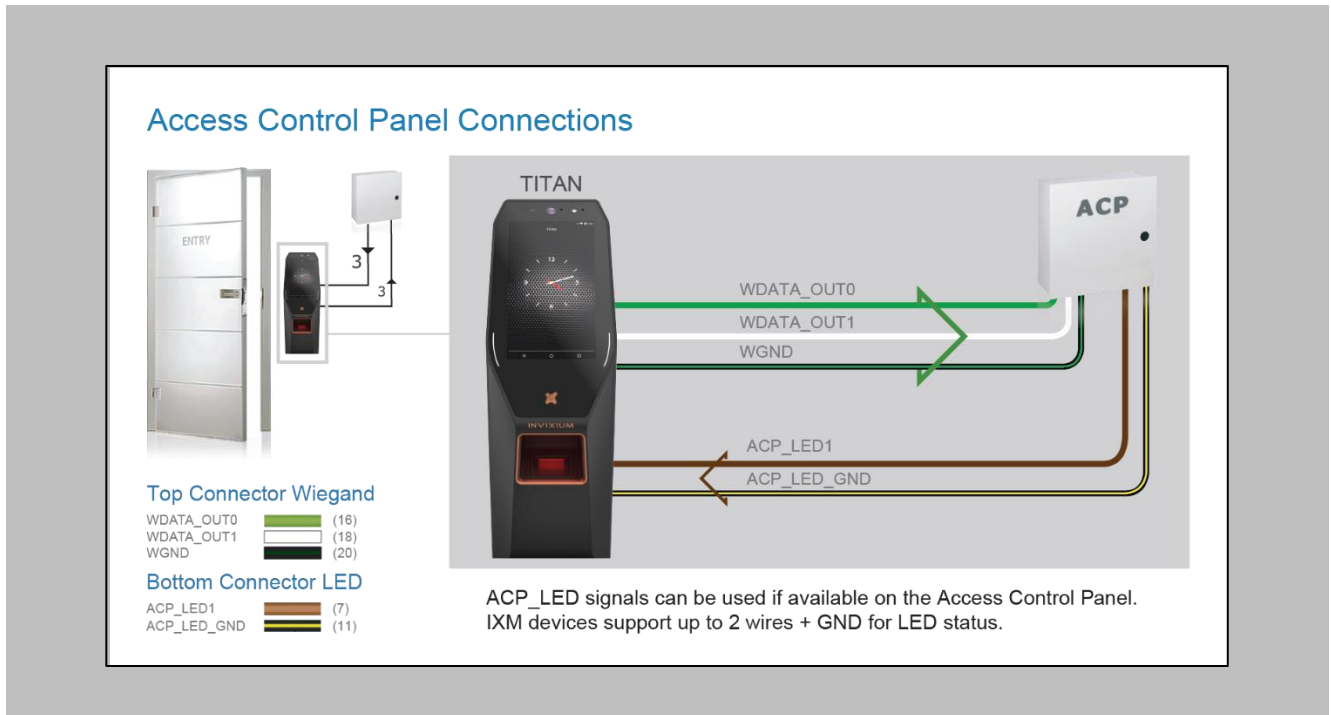



Figure 91: IXM TITAN - Panel Feedback

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

OSDP Connections

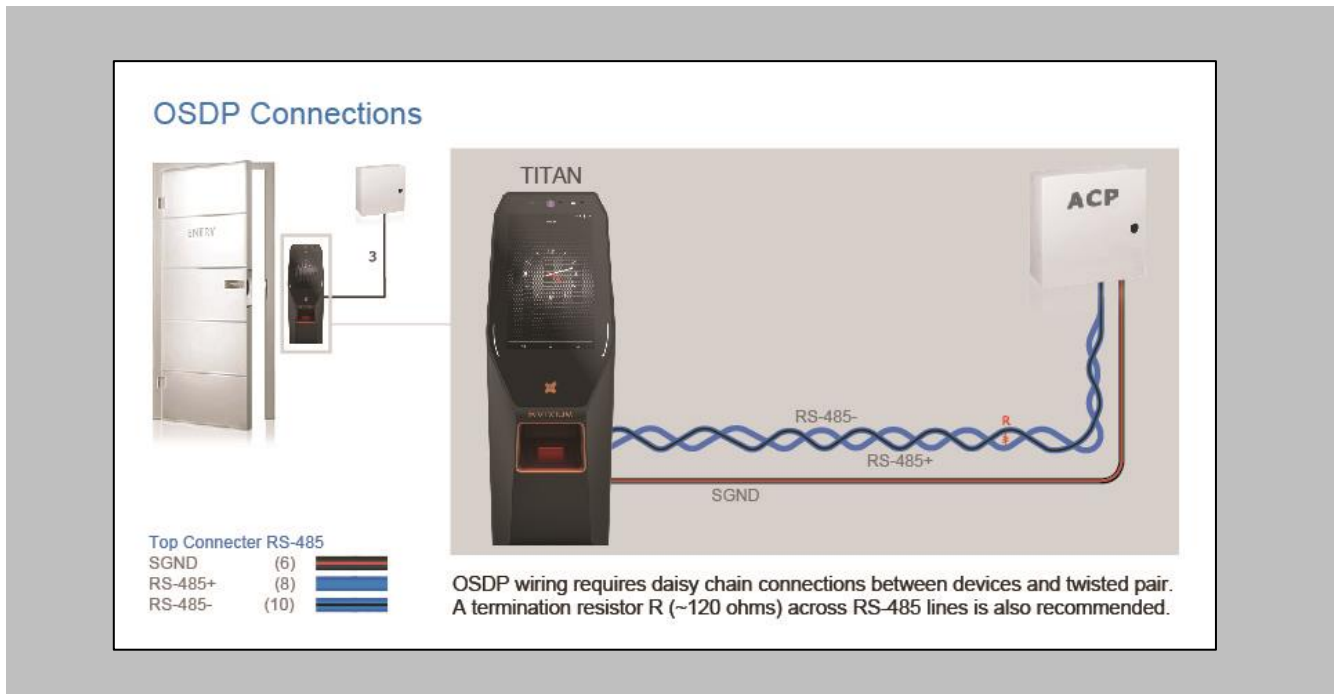




Figure 92: IXM TITAN - OSDP Connections

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

16. Troubleshooting

Reader Offline from the IXM WEB Dashboard

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

Procedure

STEP 1

From [Home](#), click the [Devices](#) tab.

STEP 2

[Select](#) any device.

STEP 3

Navigate to the [Communication](#) tab.

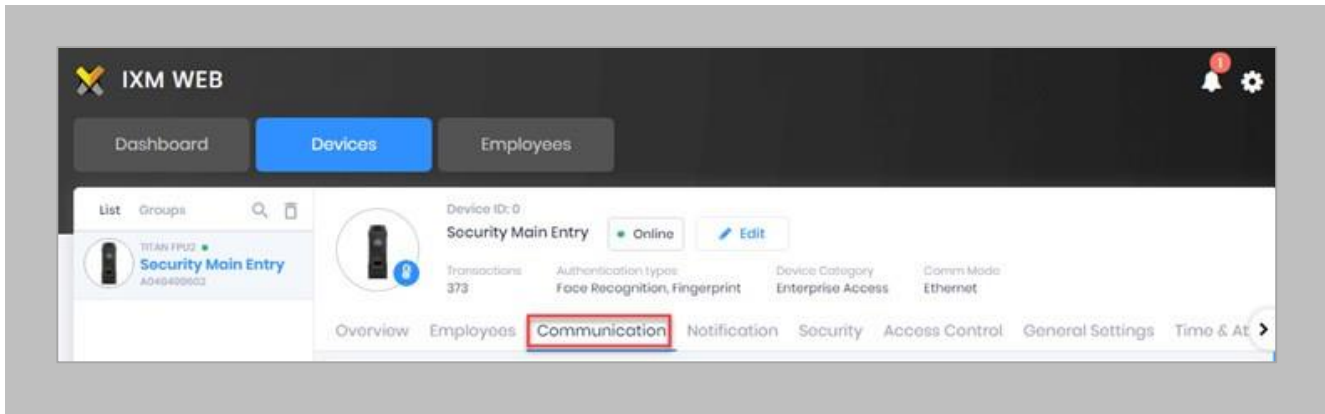


Figure 93: IXM WEB - Device Communication Settings

STEP 4

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

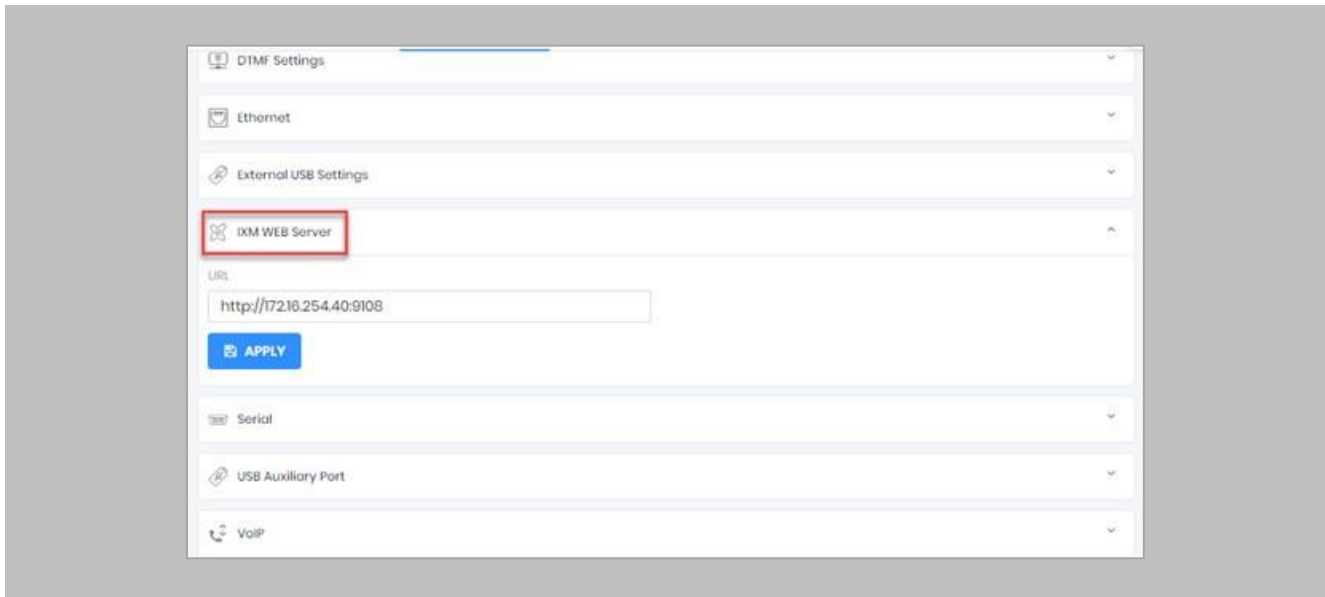


Figure 95: IXM WEB - Server URL Setting

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

STEP 5

Enter the **IP address** of the Invoxium 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.

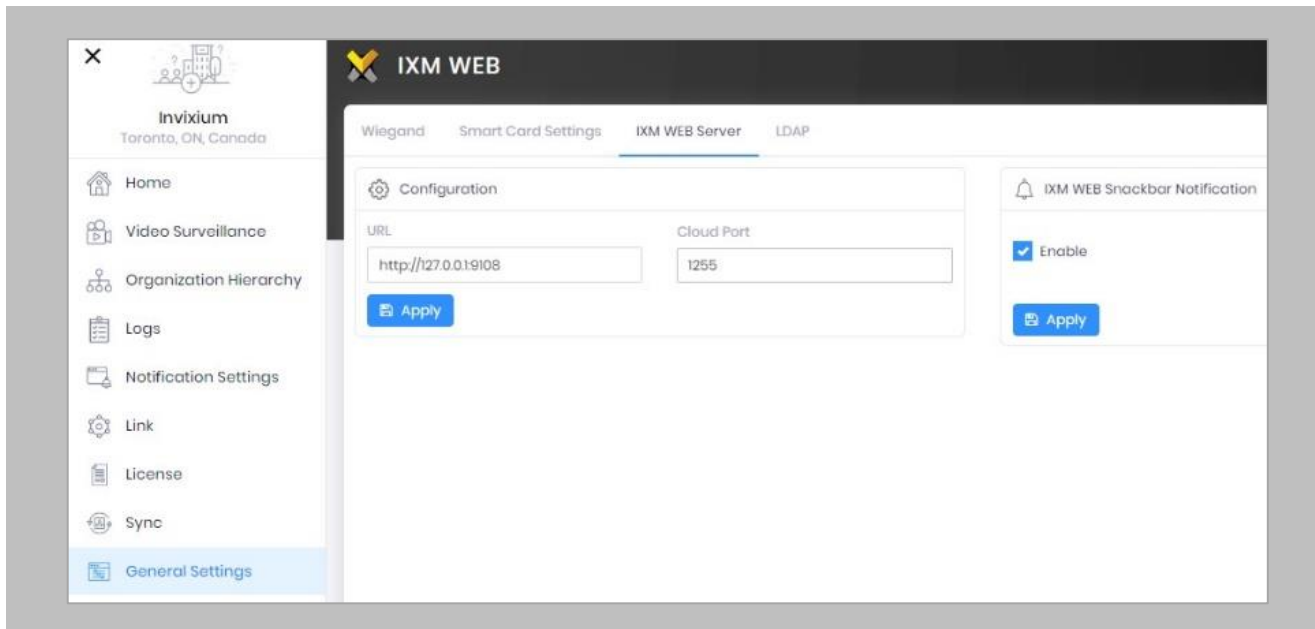


Figure 97: IXM WEB - Server URL Setting from General Settings

Elevated Body Temperature Denied Access but Granted Access in Security Center

Procedure

STEP 1

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

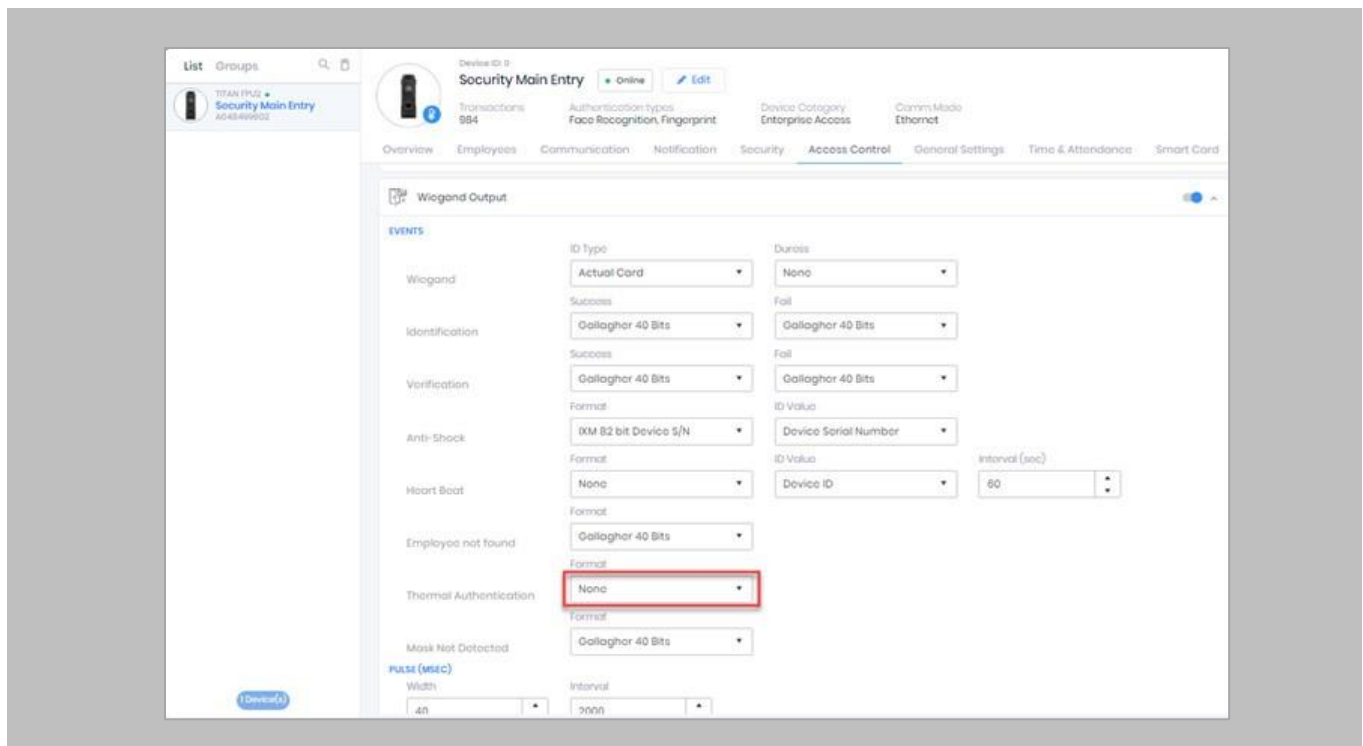



Figure 99: IXM WEB - Thermal Authentication Wiegand Output Event

 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.

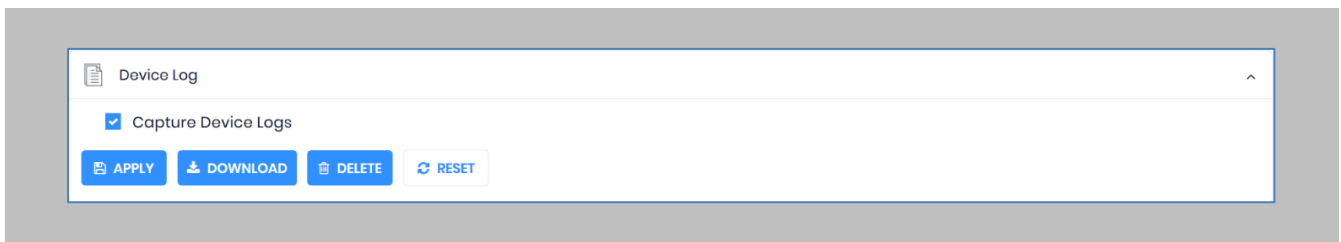


Figure 100: IXM WEB - Enable Device Logs

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

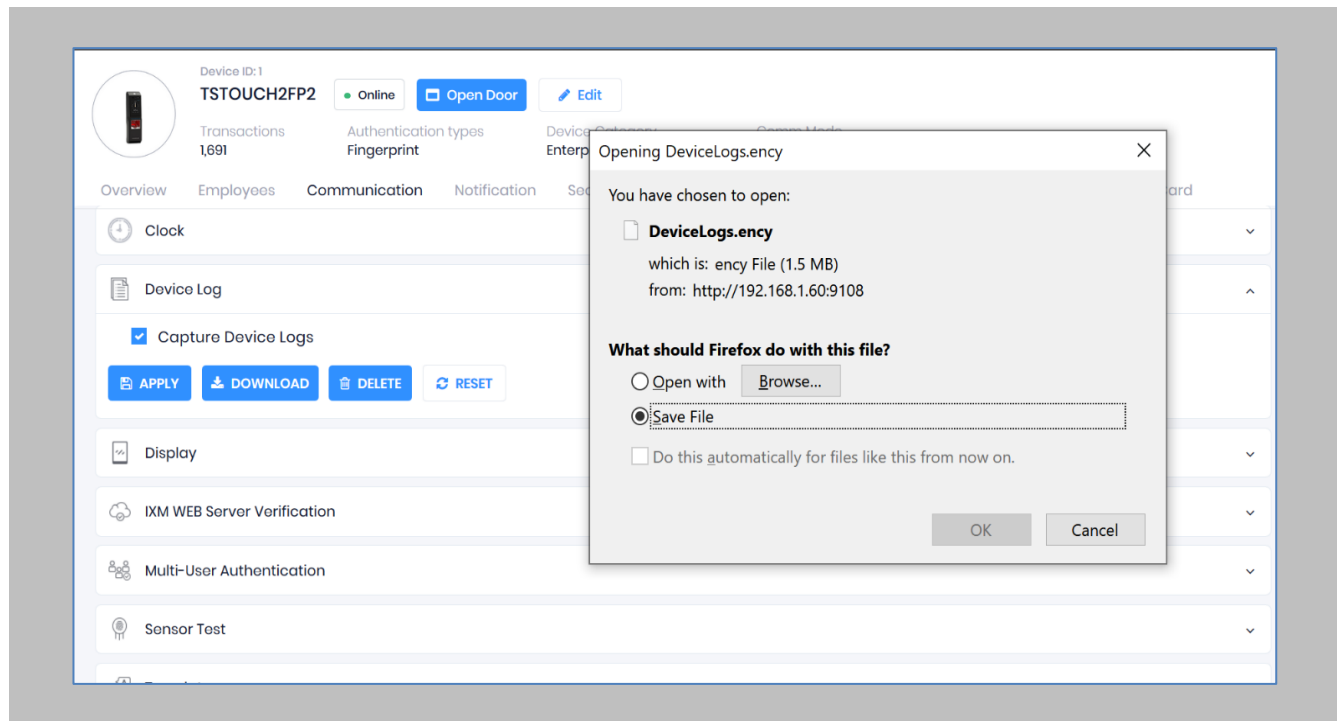


Figure 102: Save Device Log File



Select Save File and Click **OK** to store the device log file on your machine.

Transaction Logs (TLogs): Events or activities taking place on the IXM device.

- Transactions Logs can be viewed and exported from IXM WEB.
- Go to Logs in the Left Navigation pane in IXM WEB and click on Transaction Logs. A filter option is available in Transaction Logs columns.

Application Logs: Applications logs are available for any event, error, or information generated in IXM WEB.

- Applications Logs can be viewed and exported from IXM WEB.
- Go to Logs in the Left Navigation pane in IXM WEB and click on Application Logs. The filter option is available in the Application Logs columns.

Logs folder location on IXM WEB Server:


IXM WEB Logs	C:\Program Files (x86)\Invixium\IXM WEB\Log
IXM WEB Service Logs	C:\Program Files (x86)\Invixium\IXMWebService
IXM API Logs	C:\Program Files (x86)\Invixium\IXMAPI\Log

Table 7: Logs Folder Location

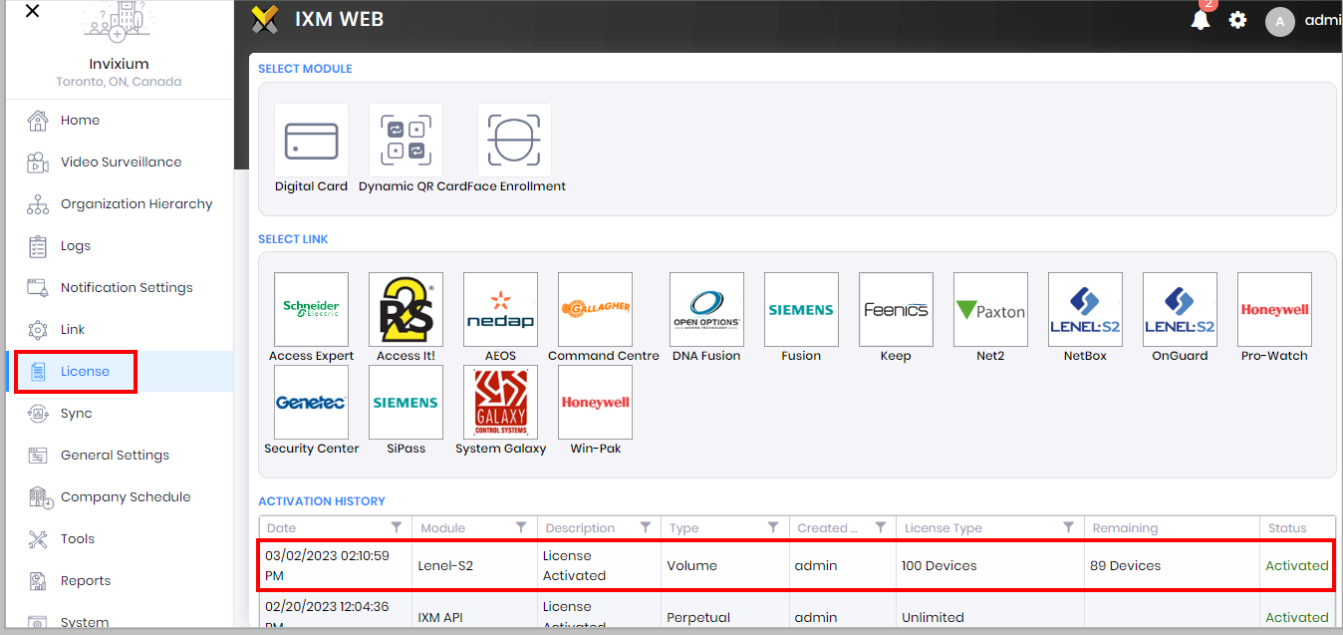
Unable to connect to the Lenel-S2 Server

Procedure

STEP 1

 Note: Confirm module activation

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



The screenshot displays the IXM WEB interface. On the left is a navigation menu with the 'License' option highlighted in red. The main content area is divided into three sections: 'SELECT MODULE' with icons for Digital Card and Dynamic QR CardFace Enrollment; 'SELECT LINK' with various vendor logos including Schneider Electric, RS, nedap, Gallagher, Open Options, Siemens, Feenics, Paxton, Net2, NetBox, OnGuard, Honeywell, Genetec, SiPass, System Galaxy, and Win-Pak; and 'ACTIVATION HISTORY' which contains a table with the following data:

Date	Module	Description	Type	Created ...	License Type	Remaining	Status
03/02/2023 02:10:59 PM	Lenel-S2	License Activated	Volume	admin	100 Devices	89 Devices	Activated
02/20/2023 12:04:36 PM	IXM API	License Activated	Perpetual	admin	Unlimited		Activated

Figure 103: IXM WEB - Licence Module

STEP 2

 Note: Confirm WEB Service URL is enabled.

From [Link](#), click the [NetBox](#) tab. Ensure the correct [WEB Service URL](#) of the server is listed. here. If not, [correct](#) and [apply](#).

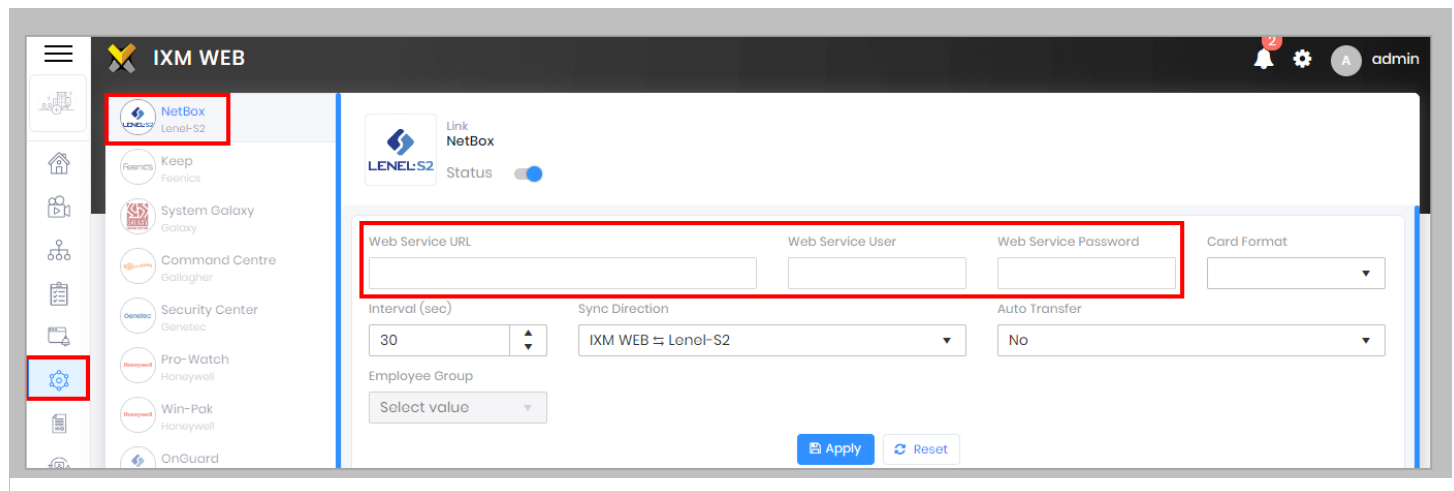


Figure 104: IXM WEB – Lenel-S2 Link Module

STEP 3

 Note: Confirm parameters entered to connect to the Lenel-S2 server.

Ensure the correct [User](#) who is authorized to connect to the API of Lenel-S2 NetBox is listed here. If not, [correct](#) and [apply](#).

Ensure the correct [Password](#) of the user who is authorized to connect to the API of Lenel-S2 NetBox is listed here. If not, [correct](#) and [apply](#).

STEP 4

 Note: Confirm S2 NetBox API is enabled in ACPCS.

Navigate to [Configuration](#) → [Site Settings](#) → [Network Controller](#) → go to [Data Integration](#) tab.

Under [API](#) section; check the status of “Enabled”. If unchecked, click on the box to enable and [Save](#) the settings.

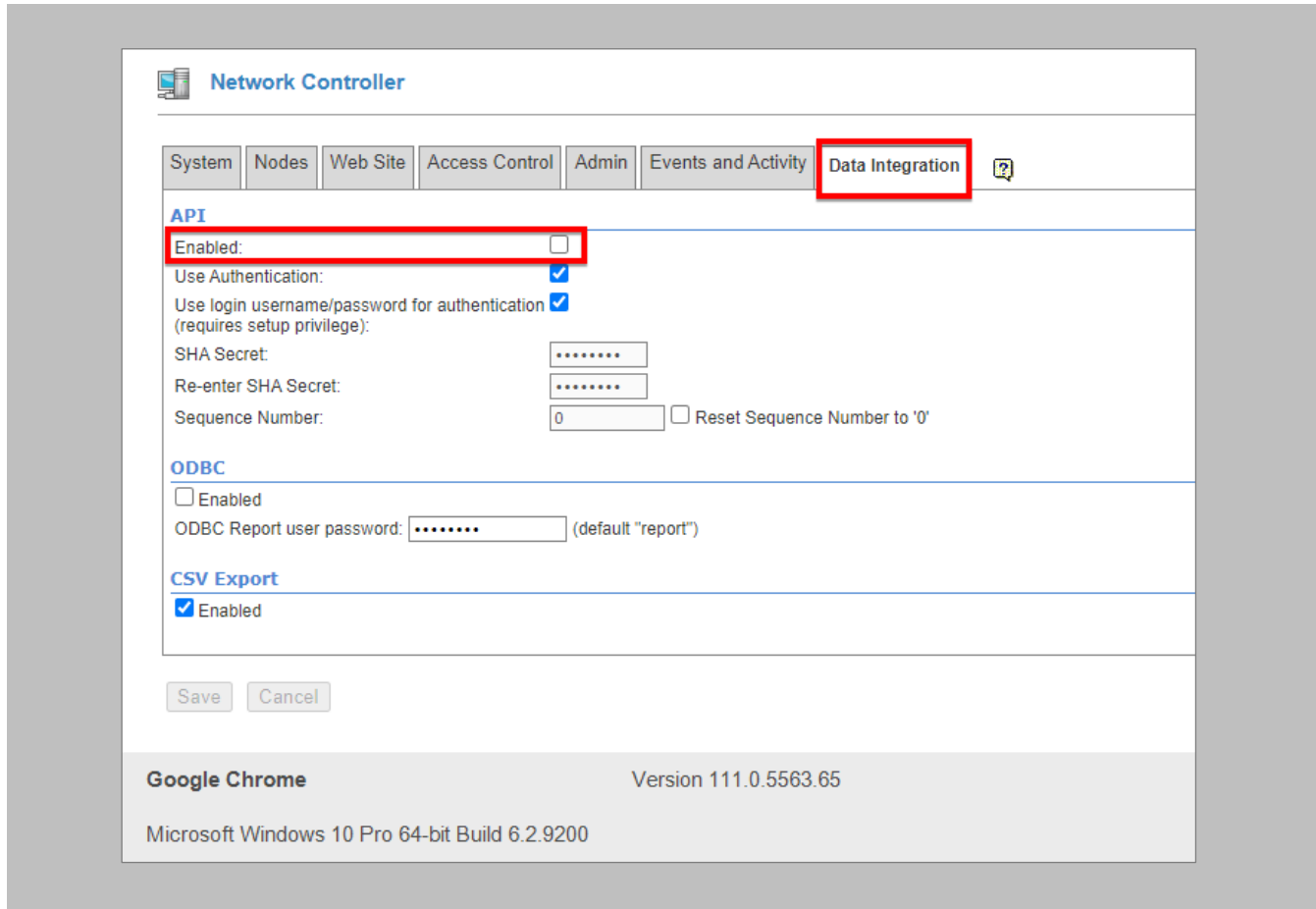



Figure 105: NetBox – Enabling S2 NetBox API

Can not find cardholder(s) in IXM WEB after importing data from Netbox

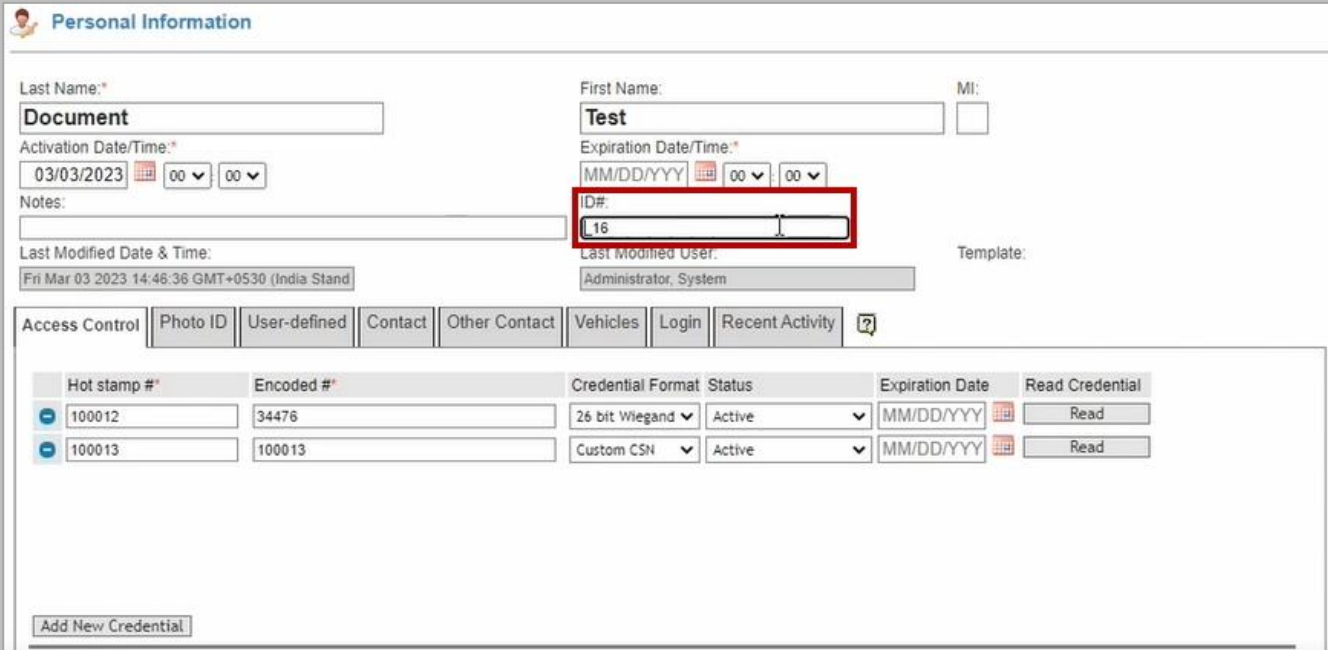
STEP 1

 Note: Confirm if correct format of User ID is entered for the cardholder in the ACPCS.

Navigate to **Administration** → **People Add** → **Personal Information**.

Ensure the format of **ID#** is entered as required in IXM WEB. If not, **correct** and **save**.

NetBox allows alphanumeric & special characters in ID# but IXM WEB allows only alphanumeric with a maximum length of 64 characters. Hence, IXM WEB will import only those users whose ID# value is compatible with IXM WEB.



Personal Information

Last Name:* First Name: MI:

Activation Date/Time:* Expiration Date/Time:*

Notes:


Last Modified Date & Time: Last Modified User: Template:

Access Control Photo ID User-defined Contact Other Contact Vehicles Login Recent Activity

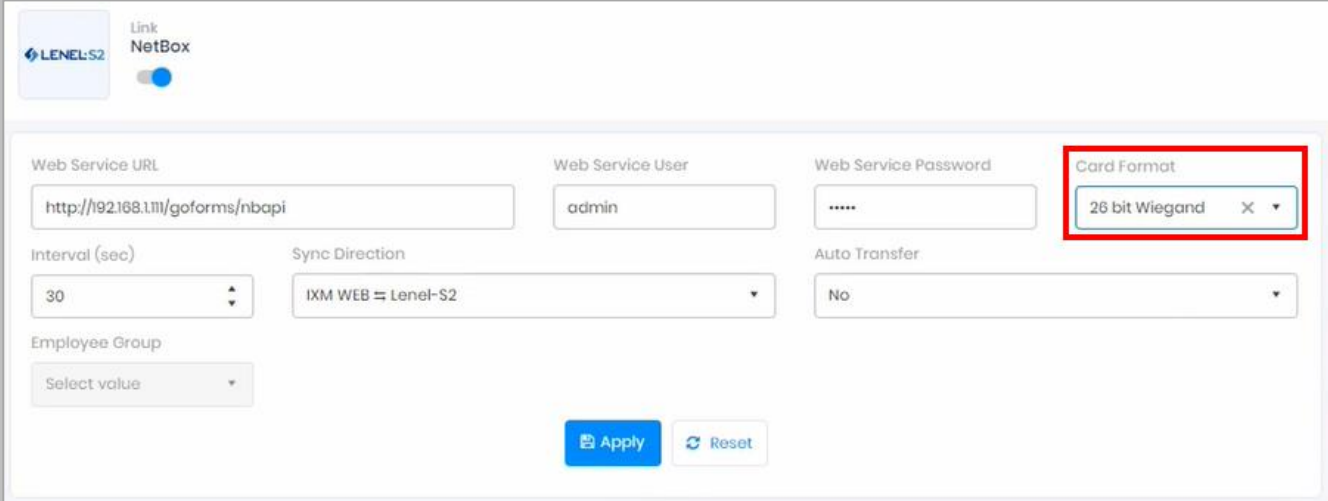
Hot stamp #*	Encoded #*	Credential Format	Status	Expiration Date	Read Credential
<input type="text" value="100012"/>	<input type="text" value="34476"/>	26 bit Wiegand	Active	MM/DD/YYYY	<input type="button" value="Read"/>
<input type="text" value="100013"/>	<input type="text" value="100013"/>	Custom CSN	Active	MM/DD/YYYY	<input type="button" value="Read"/>

Figure 106: Lenel-S2 NetBox – Personal Information

STEP 2

 Note: Ensure the Card Format selected in **IXM WEB** → **Link** is enabled in the ACPCS.

In IXM WEB, navigate to **Link** → click the blue **NetBox (Lenel-S2)** icon.



The screenshot displays the configuration interface for the Link NetBox service. At the top left, there is a 'Link NetBox' header with a toggle switch that is currently turned on. Below this, the configuration fields are organized into several sections:

- Web Service URL:** A text input field containing the URL `http://192.168.1.111/goforms/nbapi`.
- Web Service User:** A text input field containing the username `admin`.
- Web Service Password:** A text input field with masked characters (dots).
- Card Format:** A dropdown menu highlighted with a red box, currently set to `26 bit Wiegand`.
- Interval (sec):** A numeric input field set to `30`.
- Sync Direction:** A dropdown menu set to `IXM WEB ⇌ Lenel-S2`.
- Auto Transfer:** A dropdown menu set to `No`.
- Employee Group:** A dropdown menu with the placeholder text `Select value`.

At the bottom of the configuration area, there are two buttons: a blue **Apply** button and a white **Reset** button.

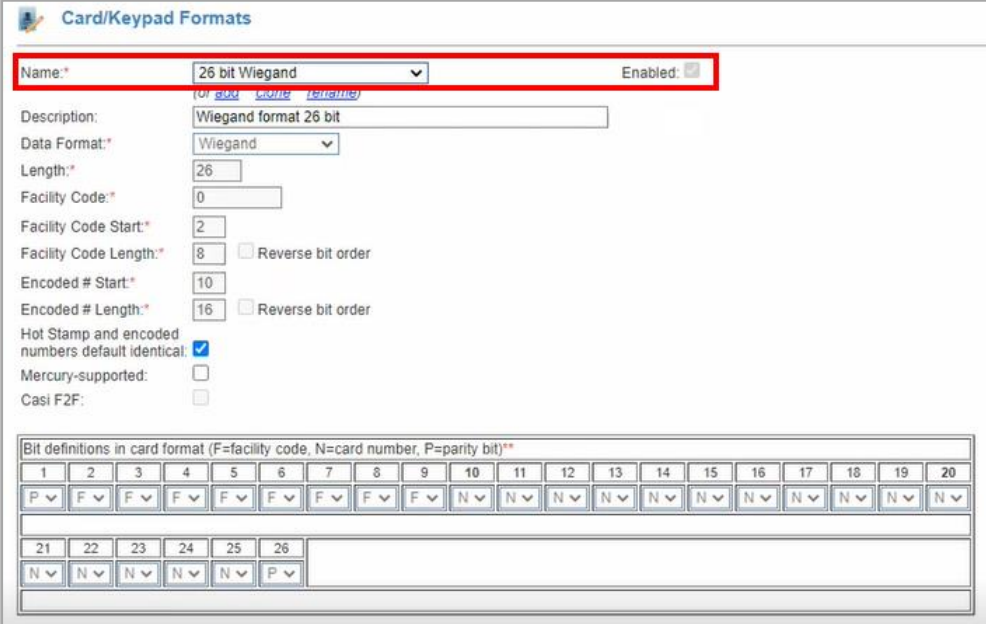
Figure 107: IXM WEB – Card Format

Note the selected **Card Format**.

In ACPCS, navigate to **Configuration** → **Access Control** → **Card/Keypad Formats**.

In **Name**, select the same Card Format from the dropdown list and check if it is **“Enabled”**.

IXM WEB will import only those cardholders that have been **“Enabled”** in the ACPCS and atleast one Employee holds that Card Format.



Card/Keypad Formats

Name:* **26 bit Wiegand** Enabled:

Description: Wiegand format 26 bit

Data Format:* Wiegand

Length:* 26

Facility Code:* 0

Facility Code Start:* 2

Facility Code Length:* 8 Reverse bit order

Encoded # Start:* 10

Encoded # Length:* 16 Reverse bit order

Hot Stamp and encoded numbers default identical:

Mercury-supported:

Casi F2F:

Bit definitions in card format (F=facility code, N=card number, P=parity bit)**																			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
P	F	F	F	F	F	F	F	F	F	N	N	N	N	N	N	N	N	N	N
21	22	23	24	25	26														
N	N	N	N	N	P														

Figure 108: Lenel-S2 NetBox – Card Format

Personal Information

Last Name:* First Name: MI:

Activation Date/Time:* Expiration Date/Time:*

Notes:

ID#:

Last Modified Date & Time: Last Modified User: Template:

Access Control | Photo ID | User-defined | Contact | Other Contact | Vehicles | Login | Recent Activity

Hot stamp #*	Encoded #*	Credential Format	Status	Expiration Date	Read Credential
<input type="text" value="100012"/>	<input type="text" value="34476"/>	26 bit Wiegand	Active	MM/DD/YYYY	<input type="button" value="Read"/>
<input type="text" value="100013"/>	<input type="text" value="100013"/>	Custom CSN	Active	MM/DD/YYYY	<input type="button" value="Read"/>

Figure 109: Lenel-S2 NetBox – Personal Information



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

This file is available at the following path:

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



17. Support

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

18. Disclaimer and Restrictions

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

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

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

Copyright © 2023 Invixium. All rights reserved.