IXM WEB Integration with Genetec Security Center

Installation Instructions

V4.0

Table of Contents

List of Figures

List of Tables

1. Introduction

Purpose

This document outlines the process of configuring the software integration between Genetec Security Center (GSC) and Invixium's IXM WEB.

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

- Setting Web-based SDK
- 'Sync All' feature to resynchronize the database from GSC to IXM WEB
- 'IXM WEB AddOn' facility for Biometric Enrollment from GSC
- Multiple Card Support upto 10 cards (default card formats of GSC)
- RIO Integration for wireless connection

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 Genetec Security Center 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 Security Center by using Genetec Web-based SDK.

Acronyms

Acronym	Description
ACPCS	Access Control Panel Configuration Software
GSC	Genetec Security Center
IXM	Invixium

Field Mappings

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

GSC Field	IXM Field	Notes
First name	First Name	
Last name	Last Name	
Status	Suspend User	
Activation	Start Date	
Expiration	End Date	
Card Number	Prox ID/Smart Card ID	Prox ID is given priority during export
Facility Code	Facility Code	
Email Address	Email	
Bypass antipassback rules	Anti-passback	

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

2. Compatibility

Invixium Readers

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

Software Requirements

Application	Version
Genetec Security Center	v5.12
Invixium IXM WEB	3.0.36.0
Operating Systems	Windows 11 Pro Windows 10 Professional Version Windows Server 2016 Standard Windows Server 2019
Microsoft .NET Framework	.NET Framework 4.8

Database Engine	SQL Server 2016+ Supported but not recommended: (legacy) SQL server 2014 Express Edition (Default Installation)
Internet Information Services (IIS)	Microsoft® Internet Information Services version 10.0
Web Browser	Google Chrome Mozilla Firefox Microsoft Edge (Internet Explorer not recommended)

Other Requirements

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

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

Compatibility Matrix for IXM WEB & Security Center Integration

IXM WEB version	GSC version	Compatible
IXM WEB 2.2.57.0	v5.9.1	Yes
IXM WEB 2.2.57.0	v5.10.3	Yes
IXM WEB 2.2.224.0	v.5.9.1	Yes
IXM WEB 2.2.224.0	v5.10.3	Yes
IXM WEB 2.2.252.0	v5.10.3	Yes
IXM WEB 2.2.330.0	v5.10.3	Yes
IXM WEB 2.3.2.0	v5.10.3	Yes
IXM WEB 2.3.2.0	v5.12	Yes
IXM WEB 3.0.36.0	v5.12	Yes

Table 1: Compatibility Matrix for IXM WEB & Genetec Integration

3. Checklist

Item List	Interface
Create Web-based SDK	Genetec
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 Genetec	Invixium
Configure Invixium Reader	Invixium
Face or Finger Enrollment	Invixium

4. Task List Summary

Task	IXM WEB Application Task List using IXM WEB	Genetec Security Center Task List using GSC
1	Activate IXM WEB and IXM Link for GSC	Create Web-based SDK
2	Configure IXM Link for GSC	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 or RIO settings in device for integration with Genetec Synergies appliance	Configuring door for RIO integration
5	Assign a specific Device Group to the device	Monitor Events and Generate Report

Table 2: Task List Summary

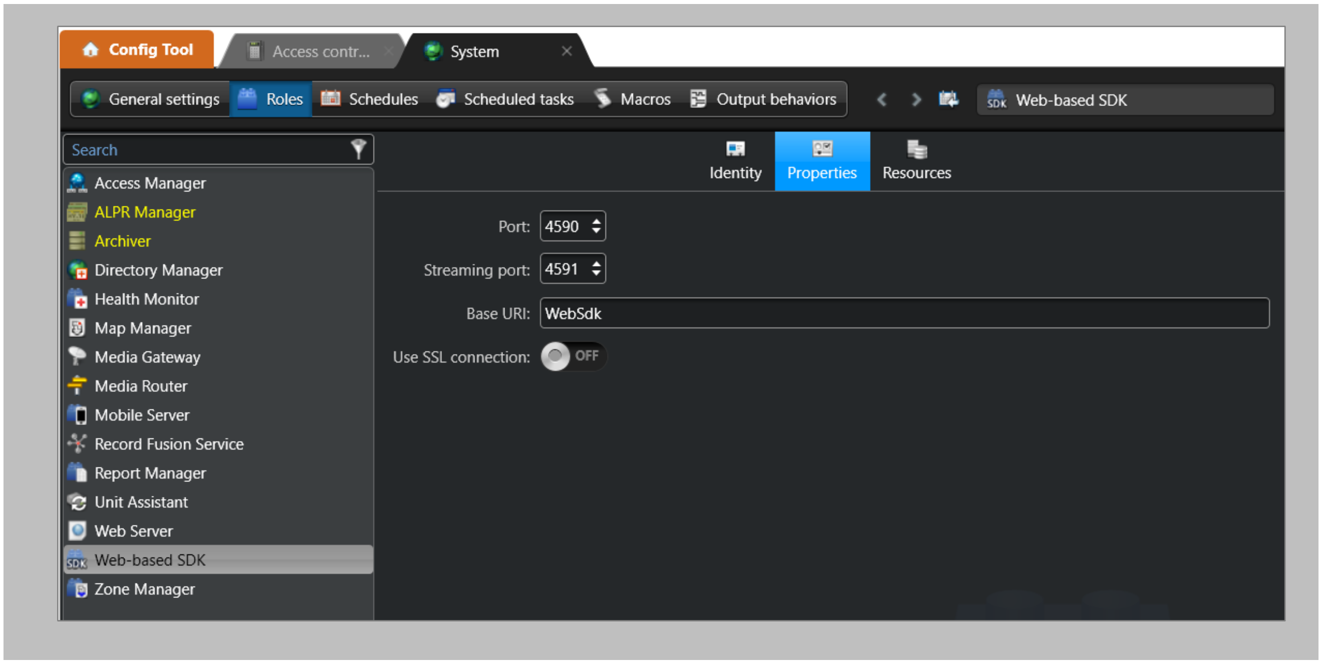
5. Prerequisites for GSC and IXM WEB Integration

Setting up Web-based SDK

Procedure

STEP 1

Navigate to **System** → **Roles** → Click **Web-based SDK**



Port: 4590

Streaming port: 4591

Base URI: WebSdk

Use SSL connection: OFF

Figure 1: GSC – Setting up Web-Based SDK

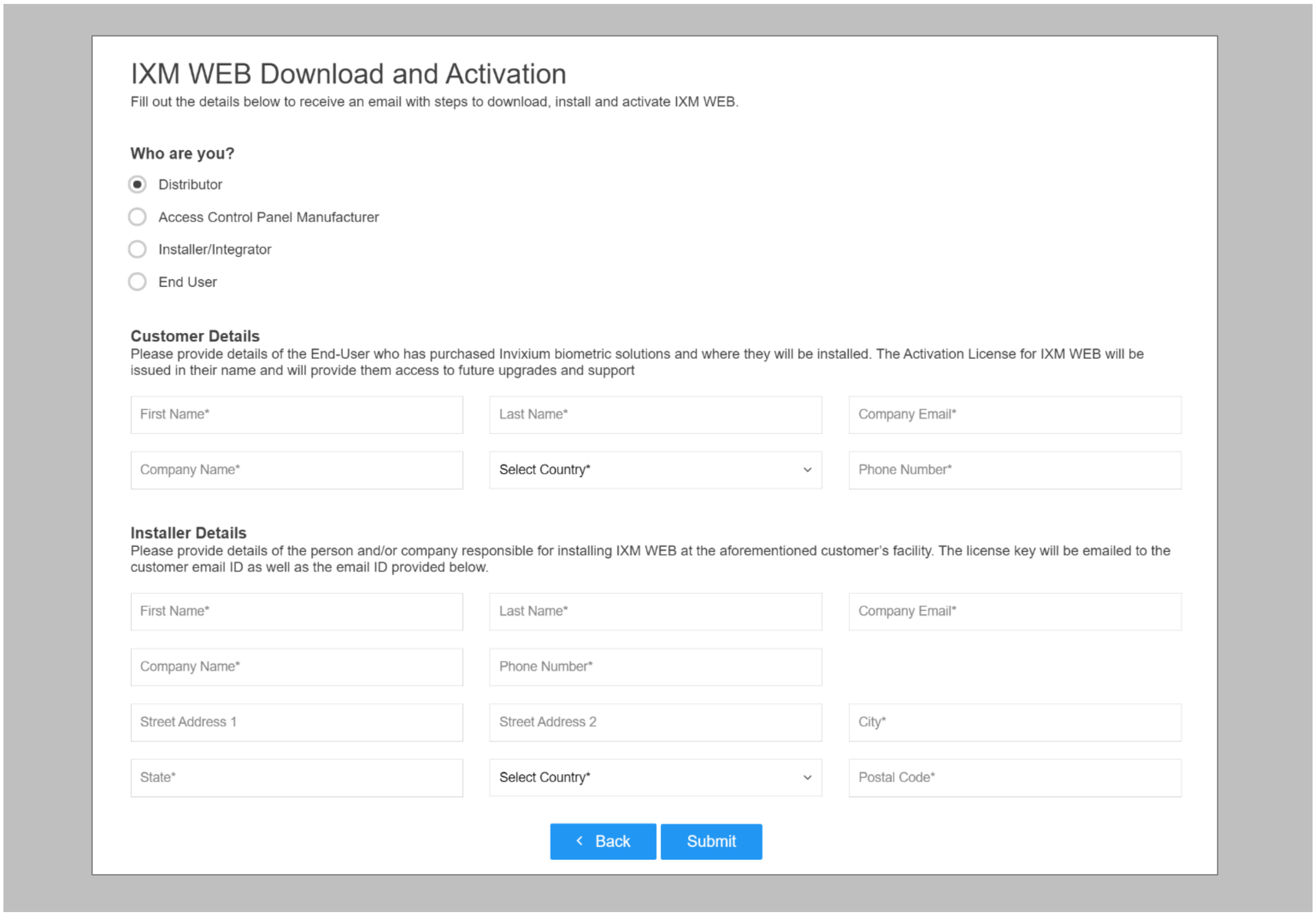
6. Prerequisites for Installing Invixium IXM WEB Software

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*	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.

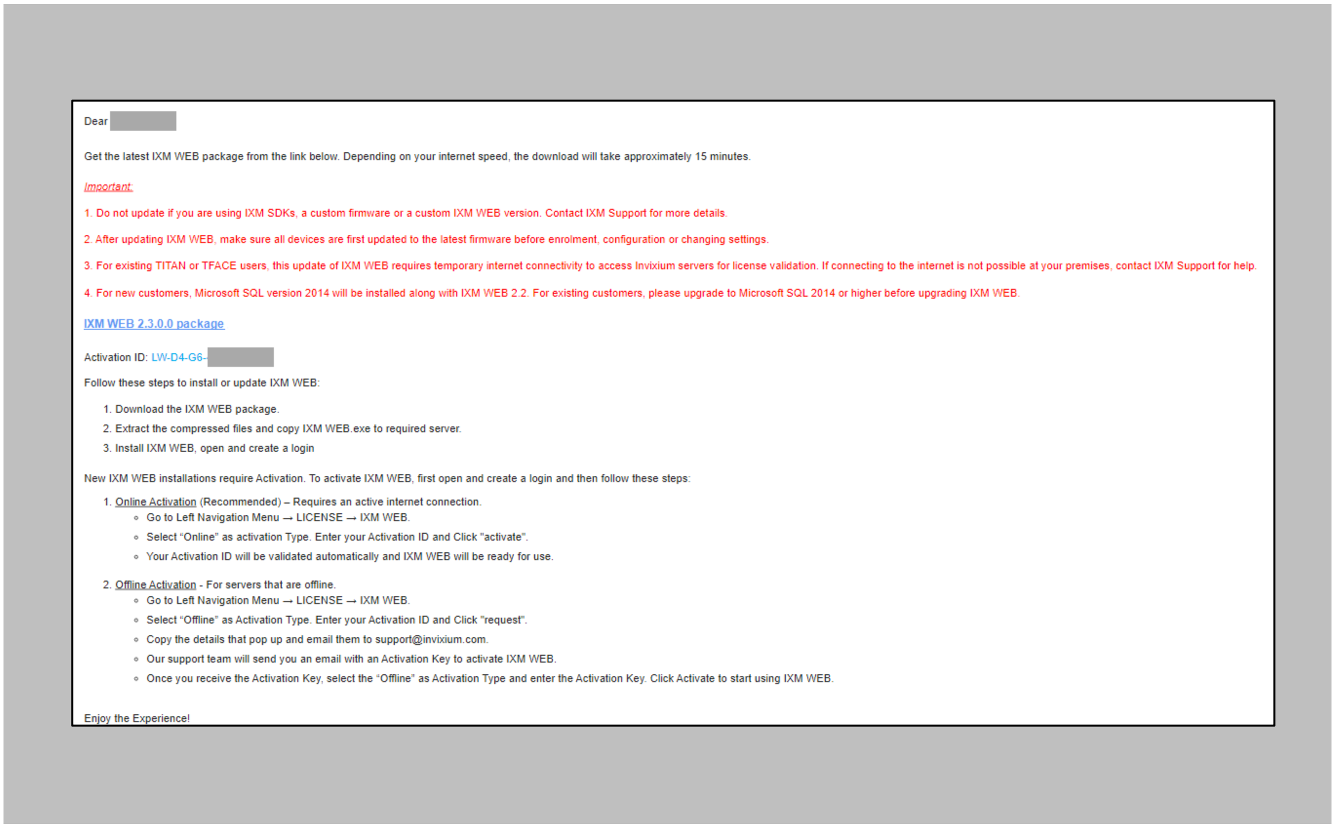
First Name*	Last Name*	Company Email*
Company Name*	Phone Number*	
Street Address 1	Street Address 2	City*
State*	Select Country*	Postal Code*

Figure 1: IXM WEB Online Request Form

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

Please ensure to check the spam or junk folder.

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



Dear [redacted]

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

Important:

1. Do not update if you are using IXM SDKs, a custom firmware or a custom IXM WEB version. Contact IXM Support for more details.

2. After updating IXM WEB, make sure all devices are first updated to the latest firmware before enrolment, configuration or changing settings.

3. For existing TITAN or TFACE users, this update of IXM WEB requires temporary internet connectivity to access Invixium servers for license validation. If connecting to the internet is not possible at your premises, contact IXM Support for help.

4. For new customers, Microsoft SQL version 2014 will be installed along with IXM WEB 2.2. For existing customers, please upgrade to Microsoft SQL 2014 or higher before upgrading IXM WEB.

IXM WEB 2.3.0.0 package

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

Follow these steps to install or update IXM WEB:

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

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

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

Enjoy the Experience!

Figure 2: Sample Email After Submitting Online Request Form

Setting Up SQL instance

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

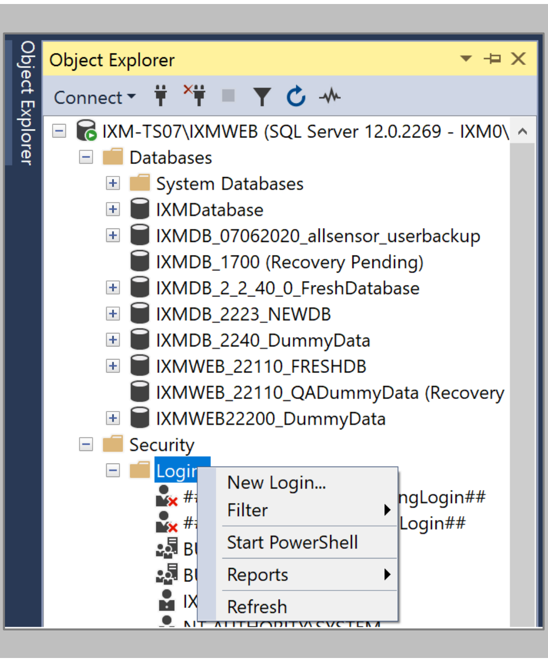
Select mixed mode: SQL Authentication and Windows Authentication for secure logins. Leave everything else as default.

STEP 4

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

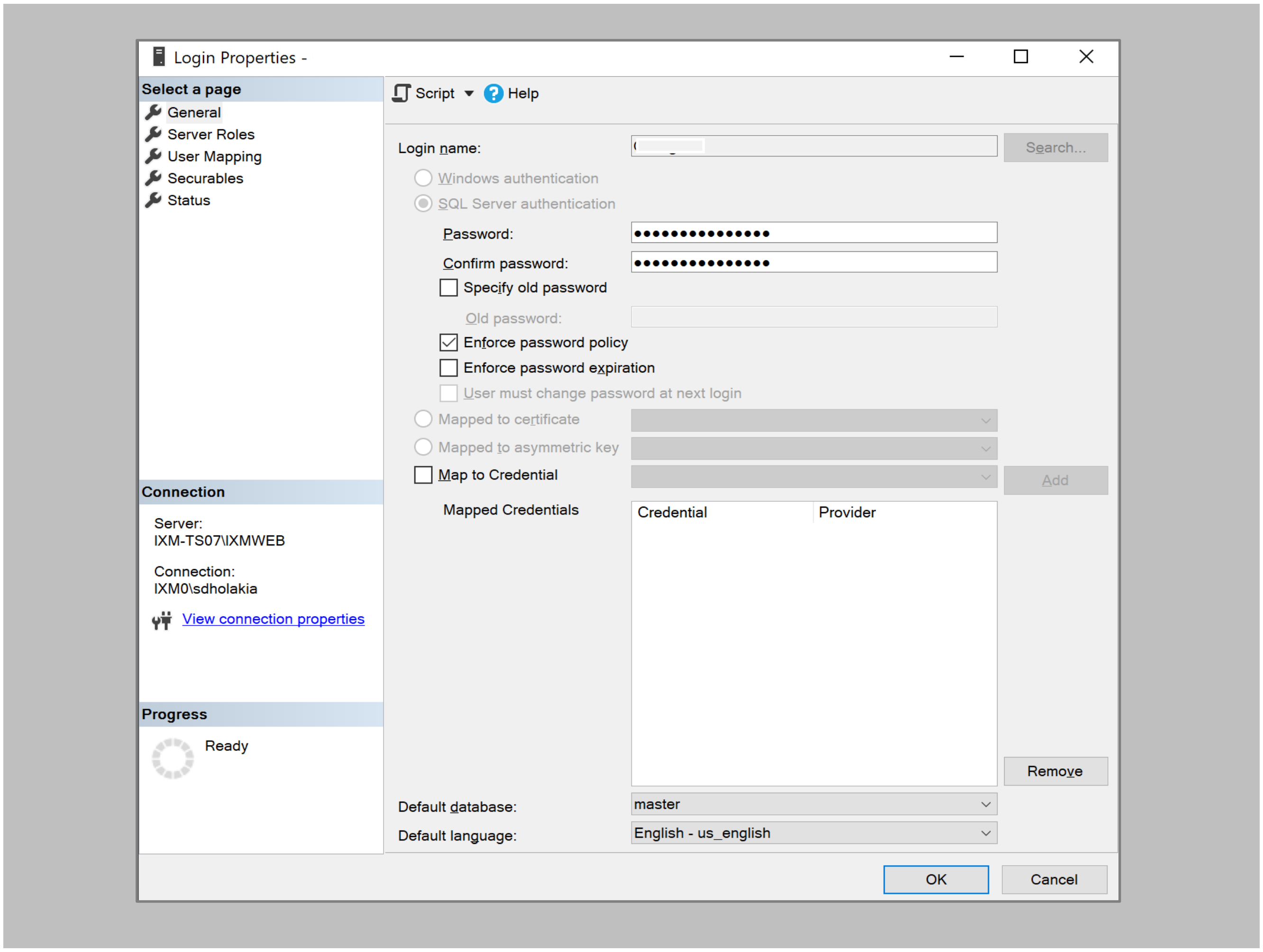
STEP 5

Log into the new instance and create a new user.



IXM-TS07\IXMWEB (SQL Server 12.0.2269 - IXM0\
Databases
System Databases
IXMDatabase
IXMDB_07062020_allsensor_userbackup
IXMDB_1700 (Recovery Pending)
IXMDB_2_2_40_0_FreshDatabase
IXMDB_2223_NEWDB
IXMDB_2240_DummyData
IXMWEB_22110_FRESHDB
IXMWEB_22110_QADummyData (Recovery
IXMWEB22200_DummyData
Security
Logins
##...ngLogin##
##...Login##
BU
BU
IX
NT AUTHORITY\SYSTEM

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



Login Properties -

Login name: [redacted]

○ Windows authentication

● SQL Server authentication

Password: •••••••••••••••

Confirm password: •••••••••••••••

□ Specify old password

Old password:

☑ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

Default language: English - us_english

Connection

Server:
IXM-TS07\IXMWEB

Connection:
IXM0\sdholakia

View connection properties

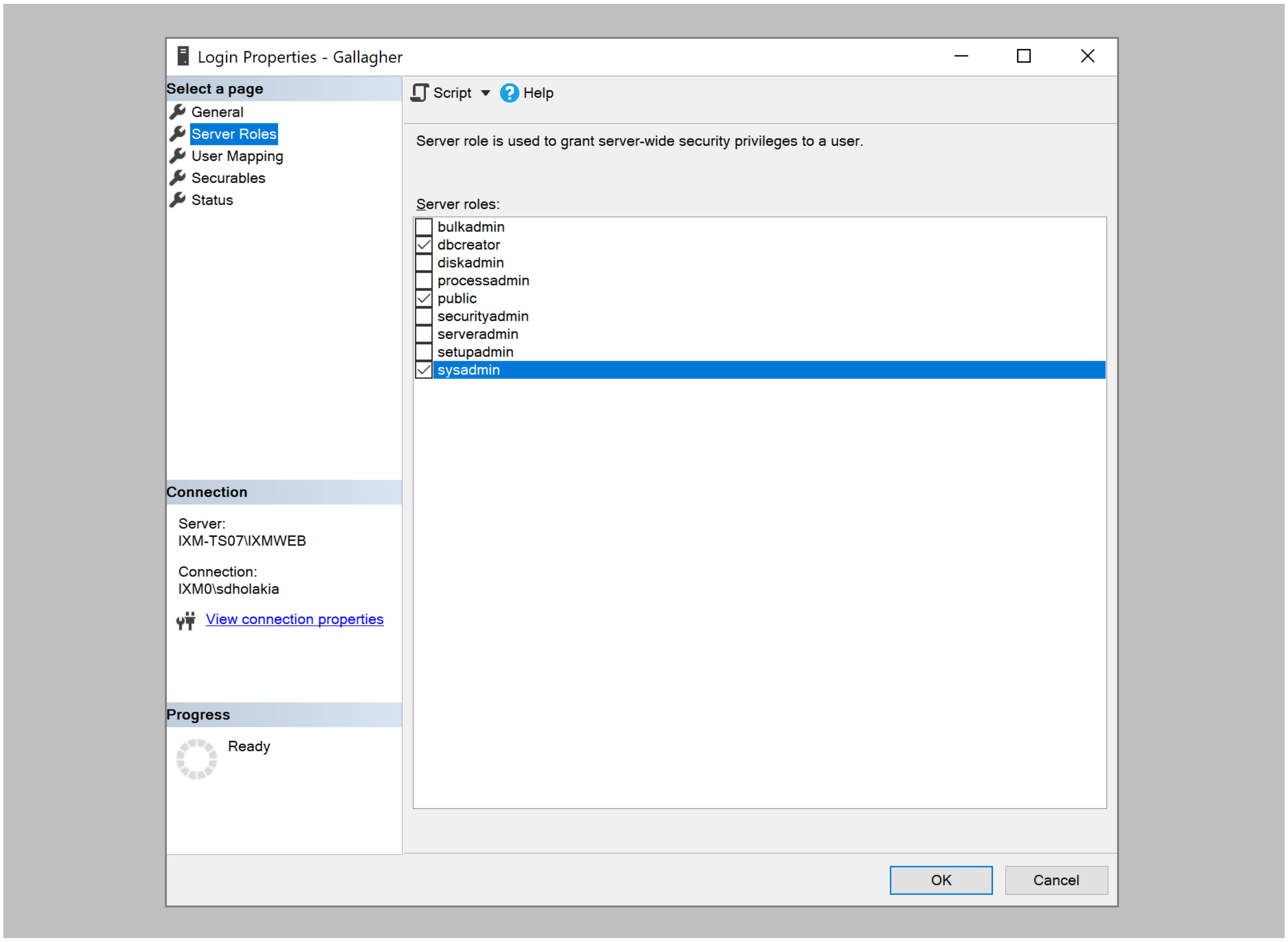
Progress

Ready

Figure 4: SQL Login Properties

STEP 7

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



Login Properties - Gallagher

Server role is used to grant server-wide security privileges to a user.

Server roles:

- ☐ bulkadmin
- ☑ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☑ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☑ sysadmin

Server:
IXM-TS07\IXMWEB

Connection:
IXM0\sdholakia

Figure 5: SQL Server Roles

RESULT

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

Minor Checklist and Considerations

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

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

Table 3: System Related Checklist

Port Assignment	**Port**
Inbound HTTP Port	9108
TCP	1433
Port to communicate between IXM WEB & Devices	9734
Inbound Port	1255
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.**

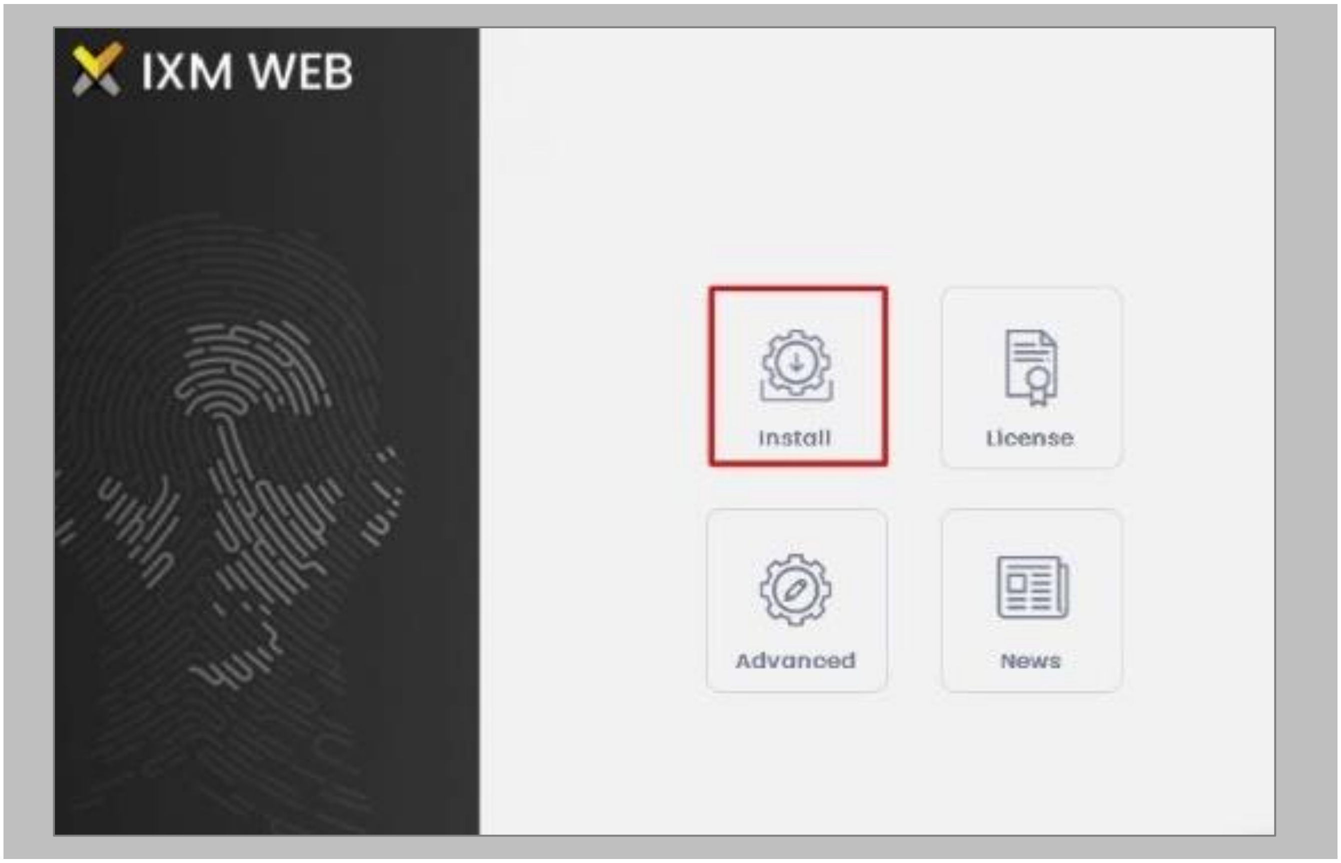
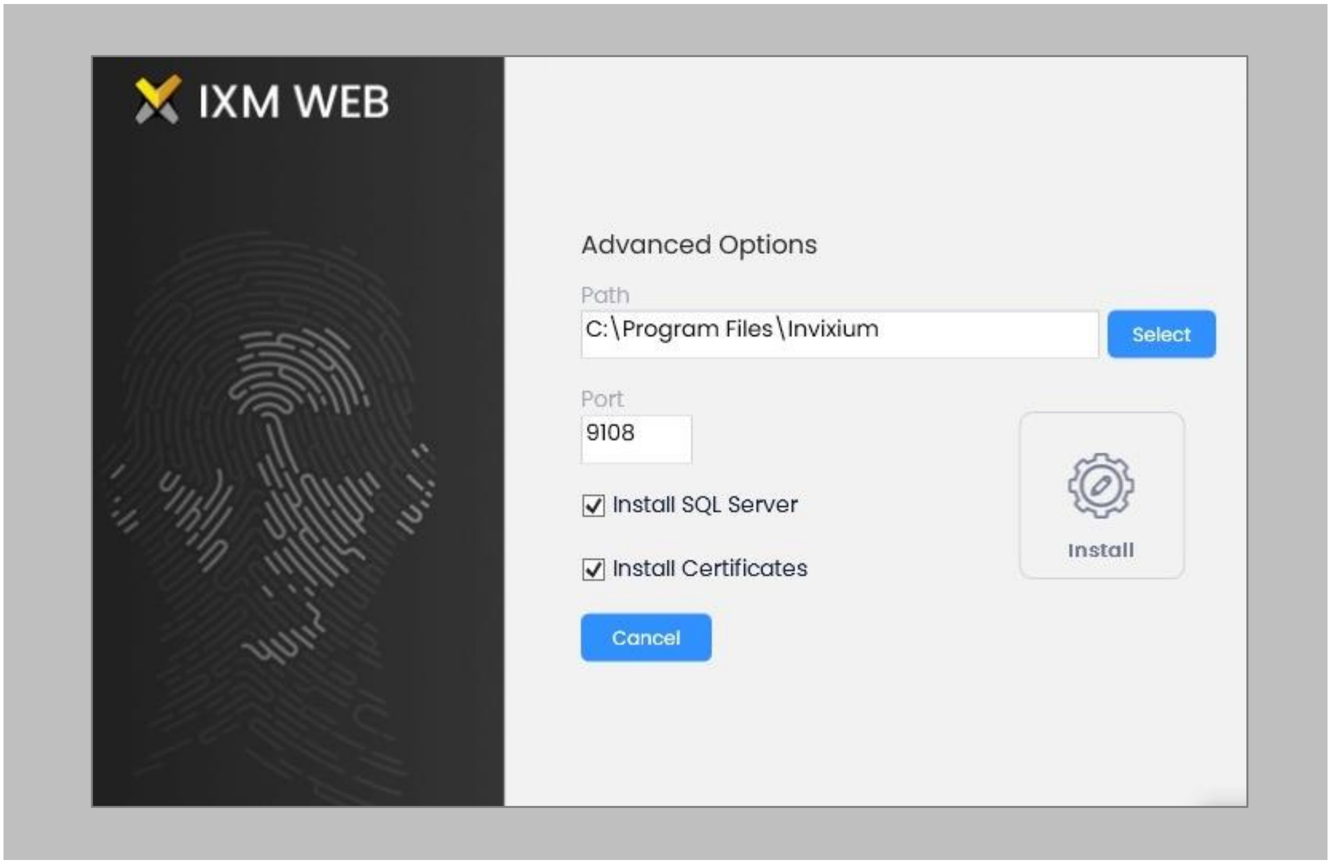


Figure 6: IXM WEB Installer

STEP 2

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



Advanced Options

Path

C:\Program Files\Invixium

Port

9108

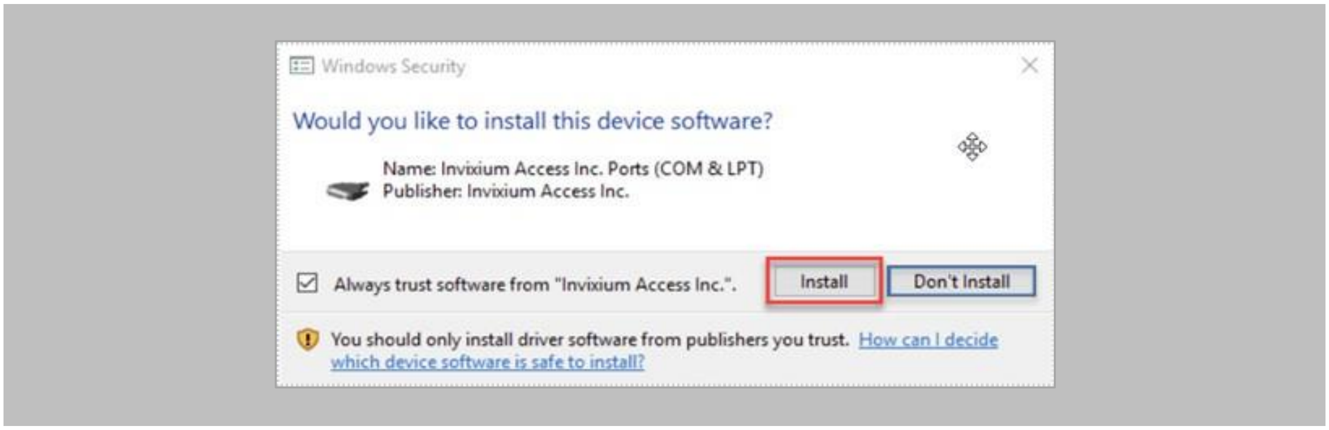
☑ Install SQL Server

☑ Install Certificates

Figure 7: Advanced Options in IXM WEB Installer

STEP 3

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



Windows Security

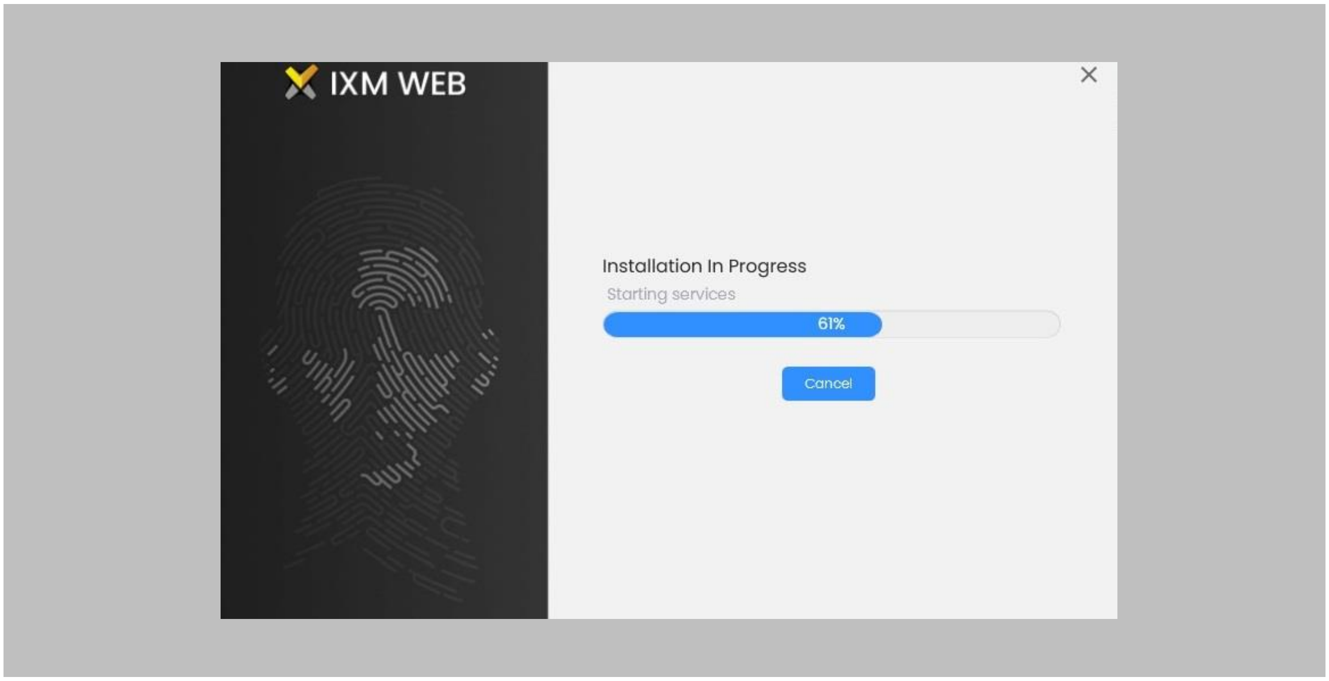
Would you like to install this device software?

Name: Invixium Access Inc. Ports (COM & LPT)
Publisher: Invixium Access Inc.

☑ Always trust software from "Invixium Access Inc.".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

Figure 8: Invixium Fingerprint Driver Installation Message



Installation In Progress

Starting services

61%

Figure 9: IXM WEB Installation Progress

STEP 4

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

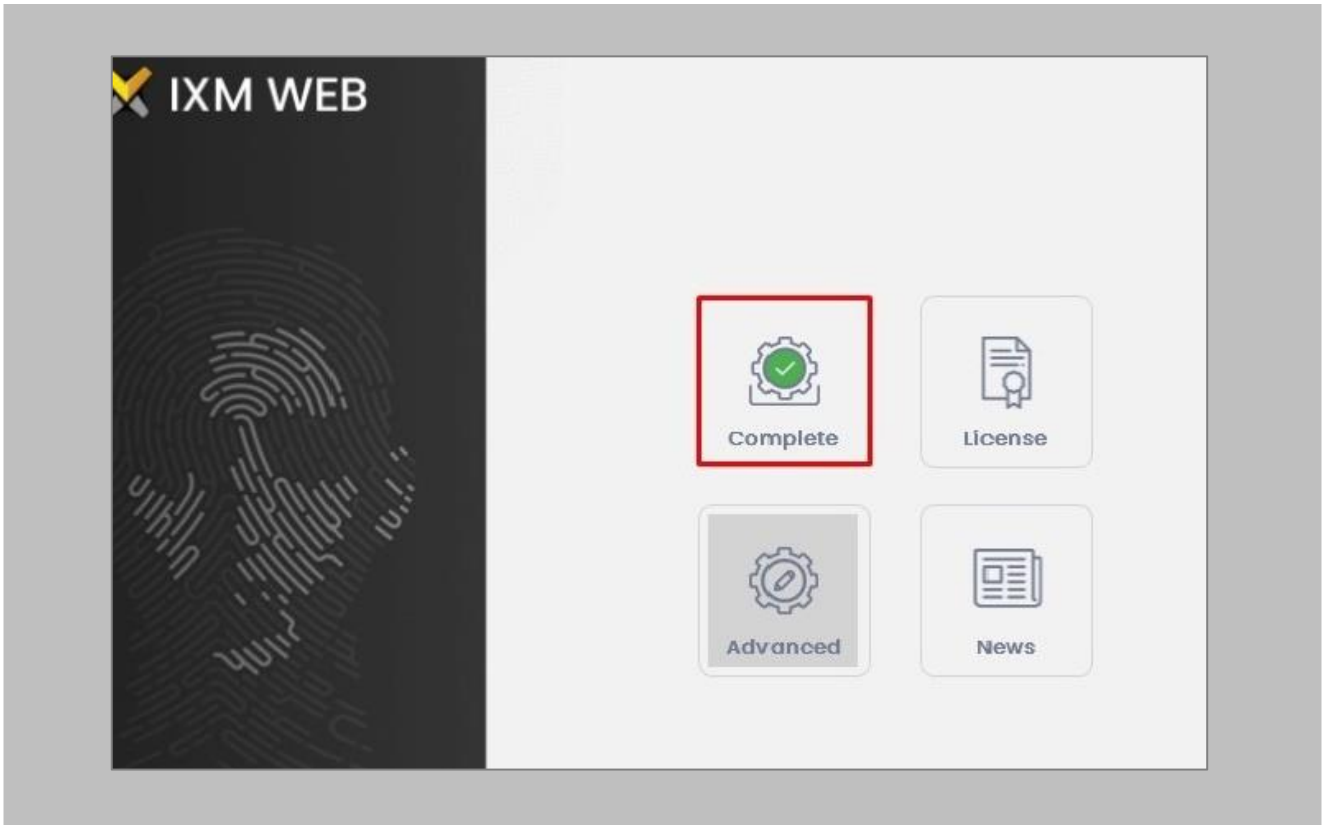


Figure 10: IXM WEB Installation Completed

Click on the **X** in the upper right corner to close.

STEP 5

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

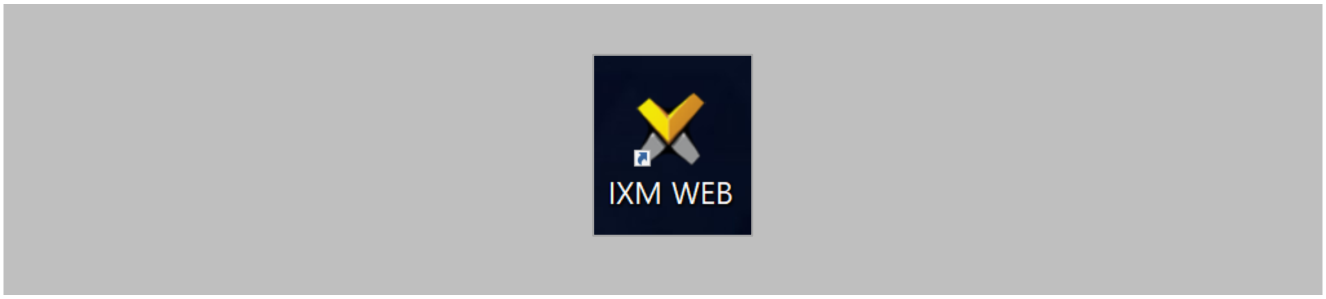
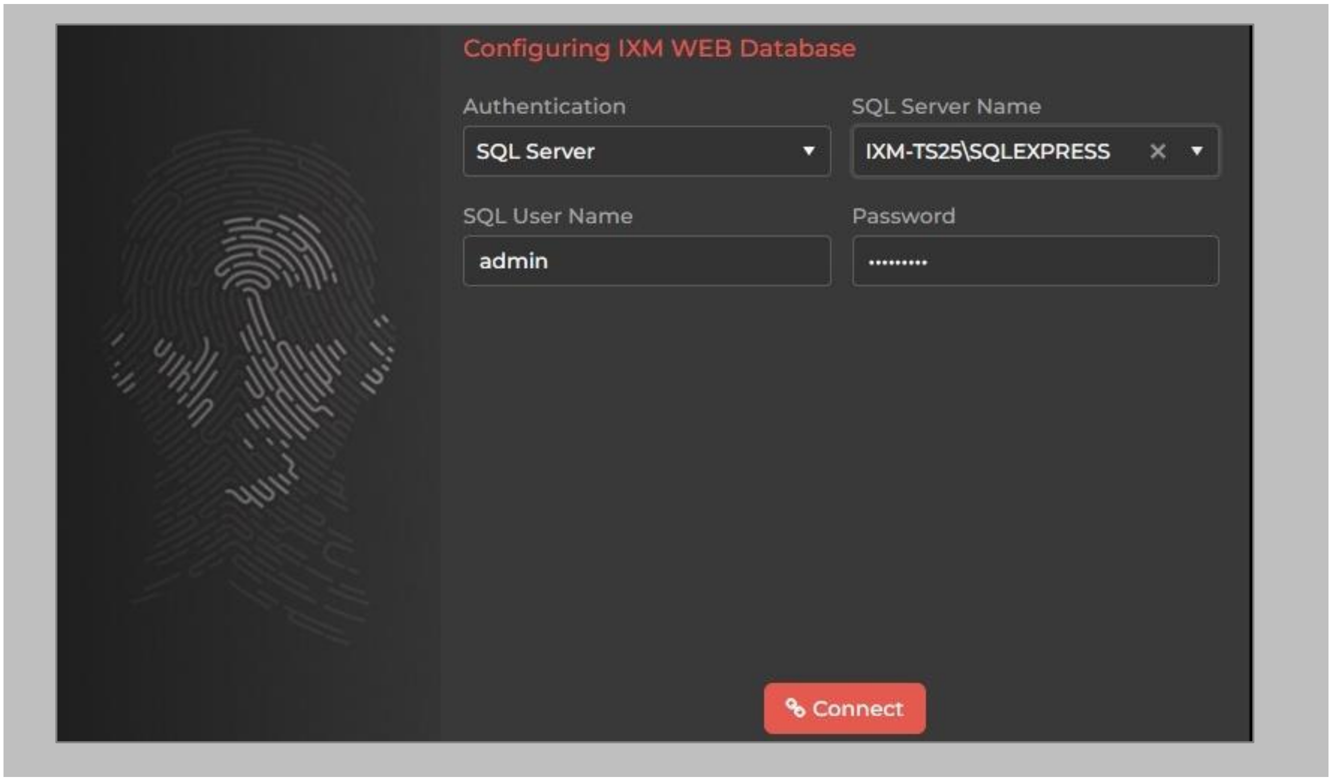


Figure 11: IXM WEB Icon - Desktop Shortcut

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


Configuring IXM WEB Database

Authentication: SQL Server

SQL Server Name: IXM-TS25\SQLEXPRESS

SQL User Name: admin

Password: •••••••••

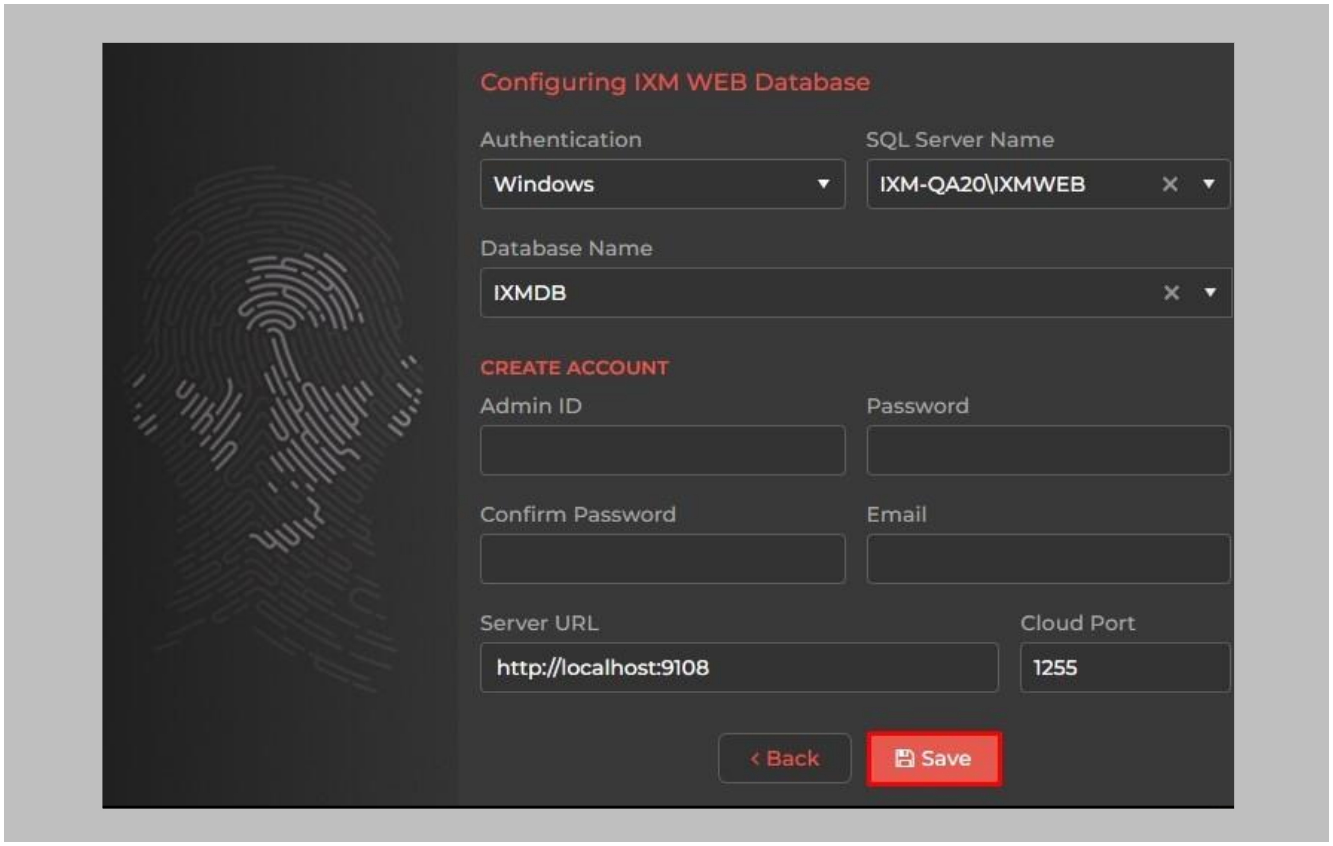
Figure 12: IXM WEB Database Configuration

STEP 6

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

STEP 7

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



Configuring IXM WEB Database

Authentication: Windows

SQL Server Name: IXM-QA20\IXMWEB

Database Name: IXMDB

CREATE ACCOUNT

Admin ID:

Password:

Confirm Password:

Email:

Server URL: http://localhost:9108

Cloud Port: 1255

Figure 13: IXM WEB Administrator User Configuration

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

STEP 8

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

STEP 9

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

For example:

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

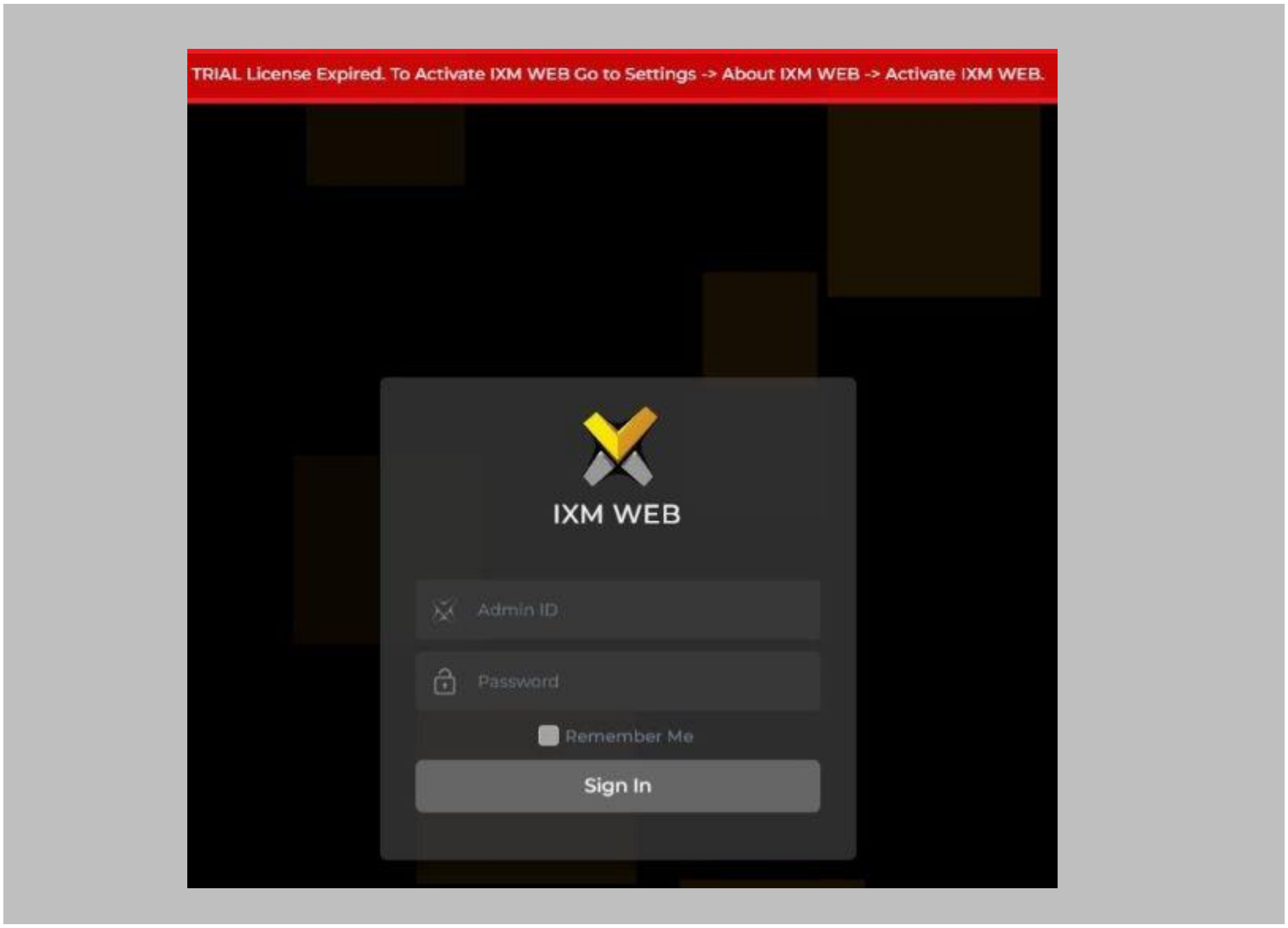
http://192.168.1.100:9108

STEP 10

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

STEP 11

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



TRIAL License Expired. To Activate IXM WEB Go to Settings -> About IXM WEB -> Activate IXM WEB.

Figure 14: IXM WEB Login Page

Note: During an upgrade of IXM WEB from any previous release to 3.0.36.0, an internet connection is required for license validation. As this new version includes a face algorithm update, it will automatically convert templates without the need for re-enrollment of faces.

8. Configuring Email Settings using IXM WEB

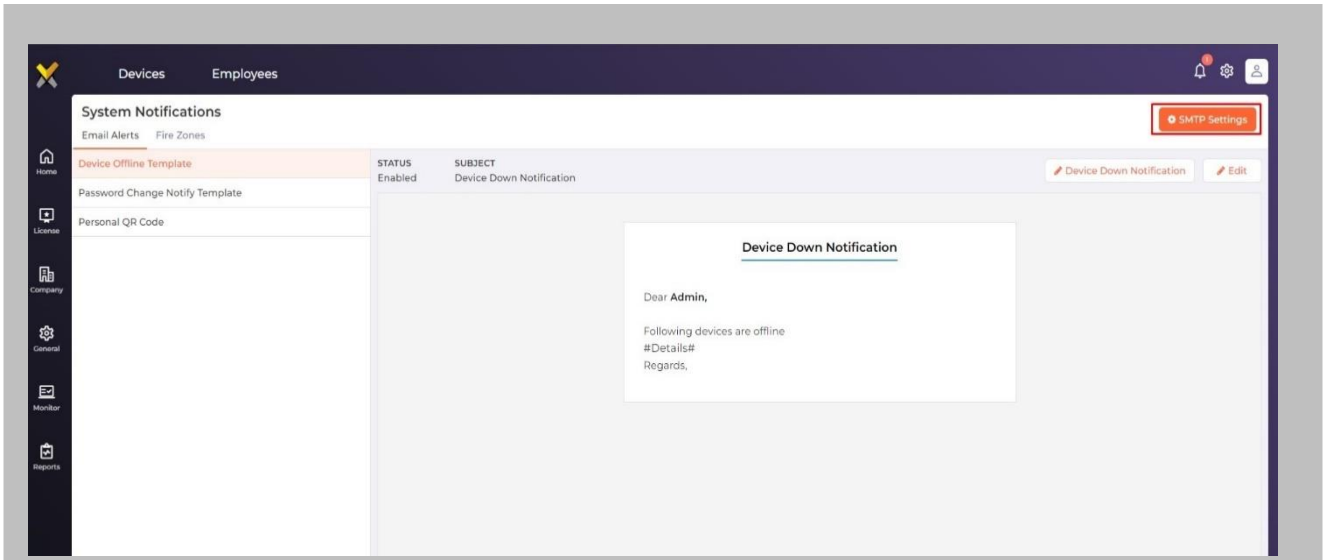
Configuring Email settings is highly recommended as one of the first steps after installing IXM WEB. Email configuration settings will help the admin retrievie the password for IXM WEB in case it is forgotten. In addition, having email settings configured also makes activation and license key requests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

Email Setting Configuration

Procedure

STEP 1

Login and navigate to **Settings** icon on top right of the page → **System Notifications** → Click on **SMTP Settings.**



STATUS Enabled

SUBJECT Device Down Notification

Device Down Notification

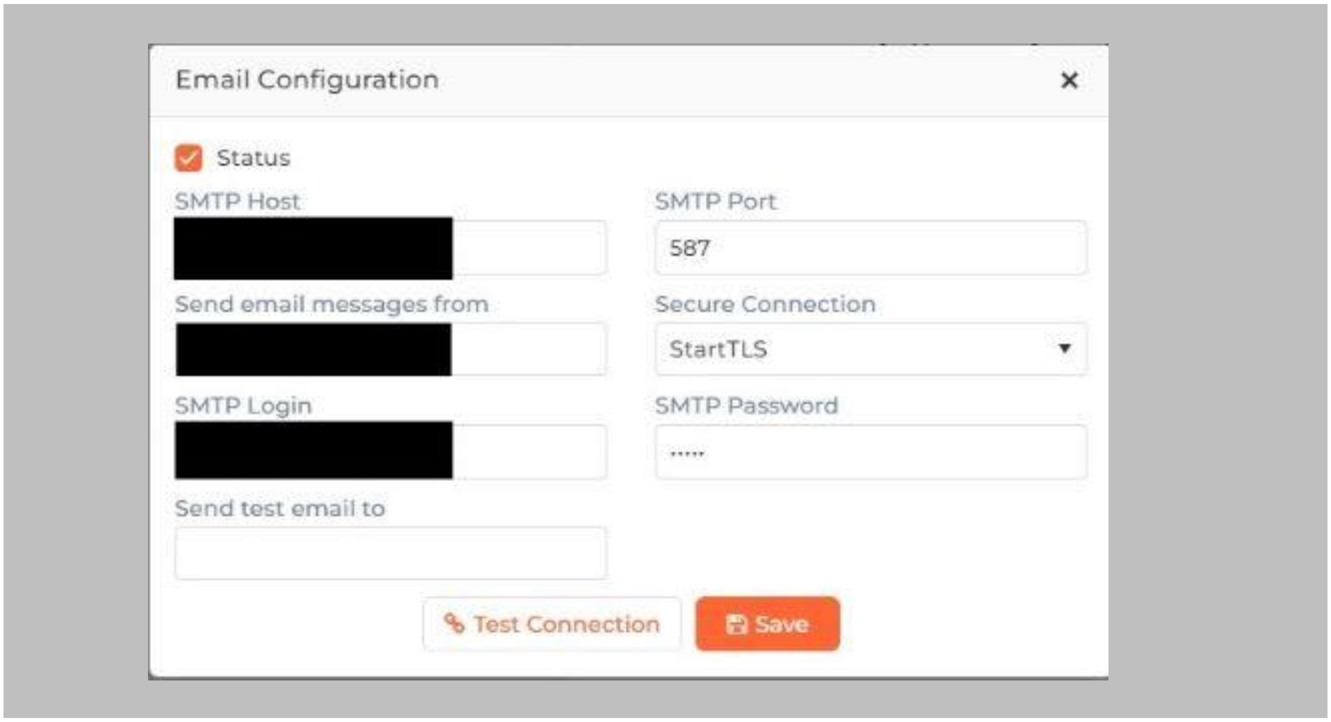
Dear **Admin,**

Following devices are offline
#Details#
Regards,

Figure 15: Configure Email

STEP 2

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



Email Configuration

☑ Status

SMTP Host: [redacted]

SMTP Port: 587

Send email messages from: [redacted]

Secure Connection: StartTLS

SMTP Login: [redacted]

SMTP Password: •••••

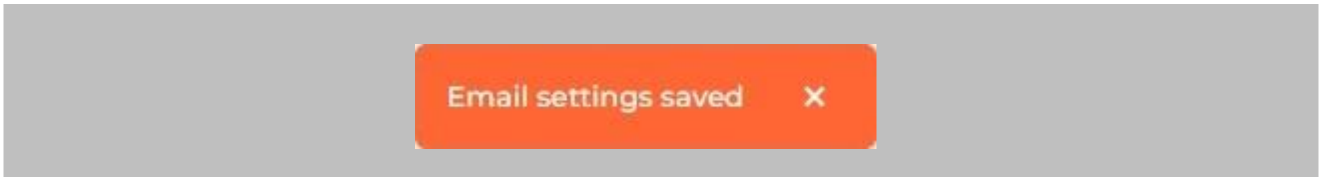
Send test email to:

Figure 16: IXM WEB - SMTP Settings

Note: If Gmail/Yahoo/MSN etc. email servers are used for “SMTP Host” then “SMTP Login” and “SMTP Password” values need to be provided. Also in this case, “Secure Connection” needs to be set to either SSL or SSL/StartTLS.

STEP 3

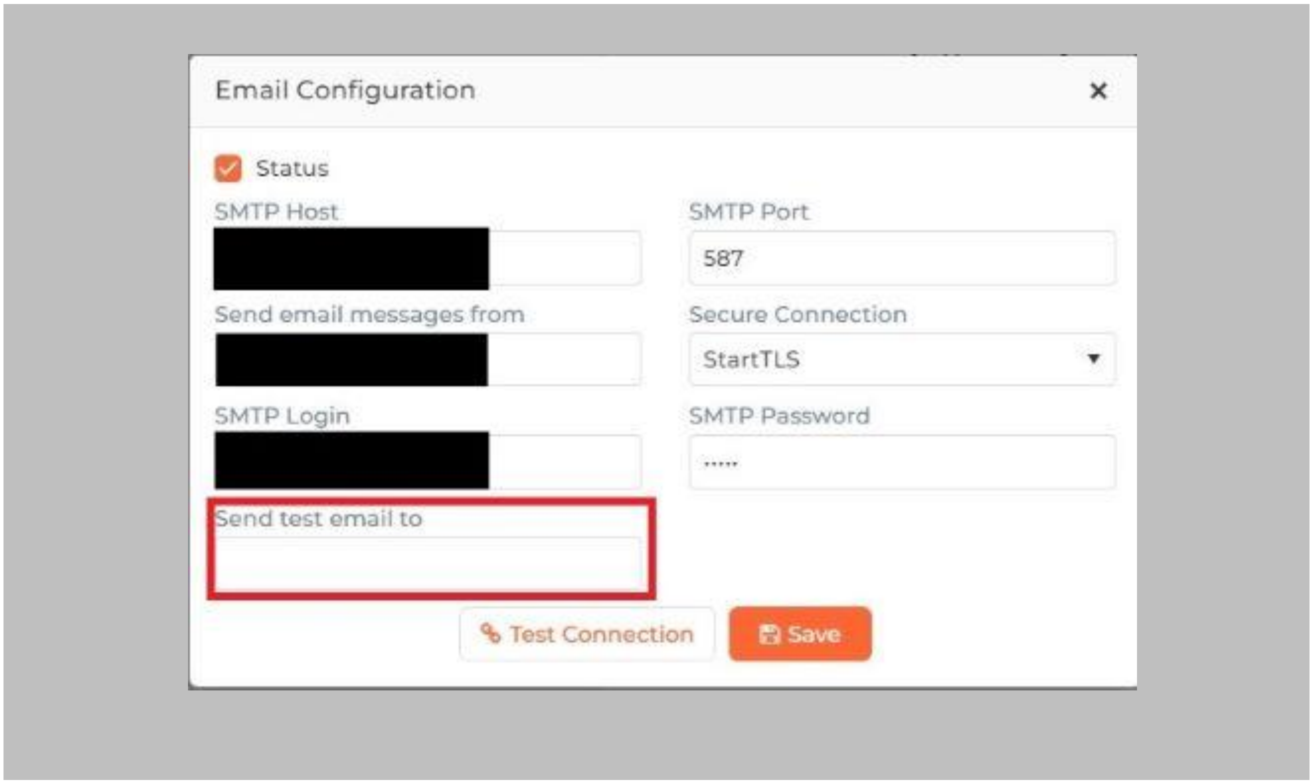
After entering the values, click **Save** to save the SMTP Settings on the IXM WEB database.



Email settings saved ×

Figure 17: IXM WEB - Save Email Settings

To test the settings, navigate to **Settings** icon on top right of the page → **System Notifications** → Click on **SMTP Settings.** Provide a valid email address under **Send test email to** >> Click the **Test Connection** button.



Email Configuration ×

☑ Status

SMTP Host: [redacted]

SMTP Port: 587

Send email messages from: [redacted]

Secure Connection: StartTLS ▾

SMTP Login: [redacted]

SMTP Password: •••••

Send test email to

Figure 18: IXM WEB – Test Connection

STEP 4

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

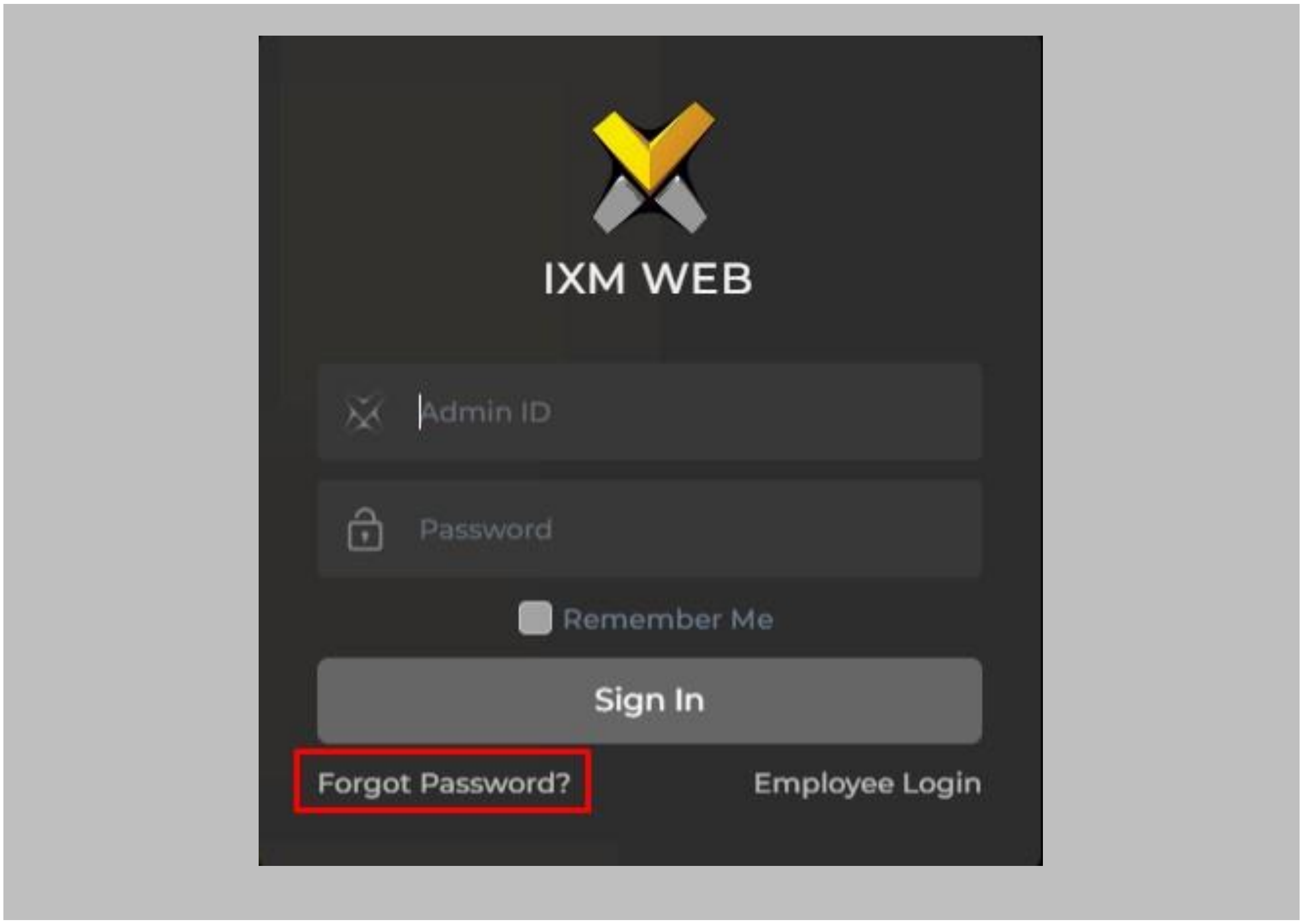


Figure 19: IXM WEB - Forgot Password

9. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

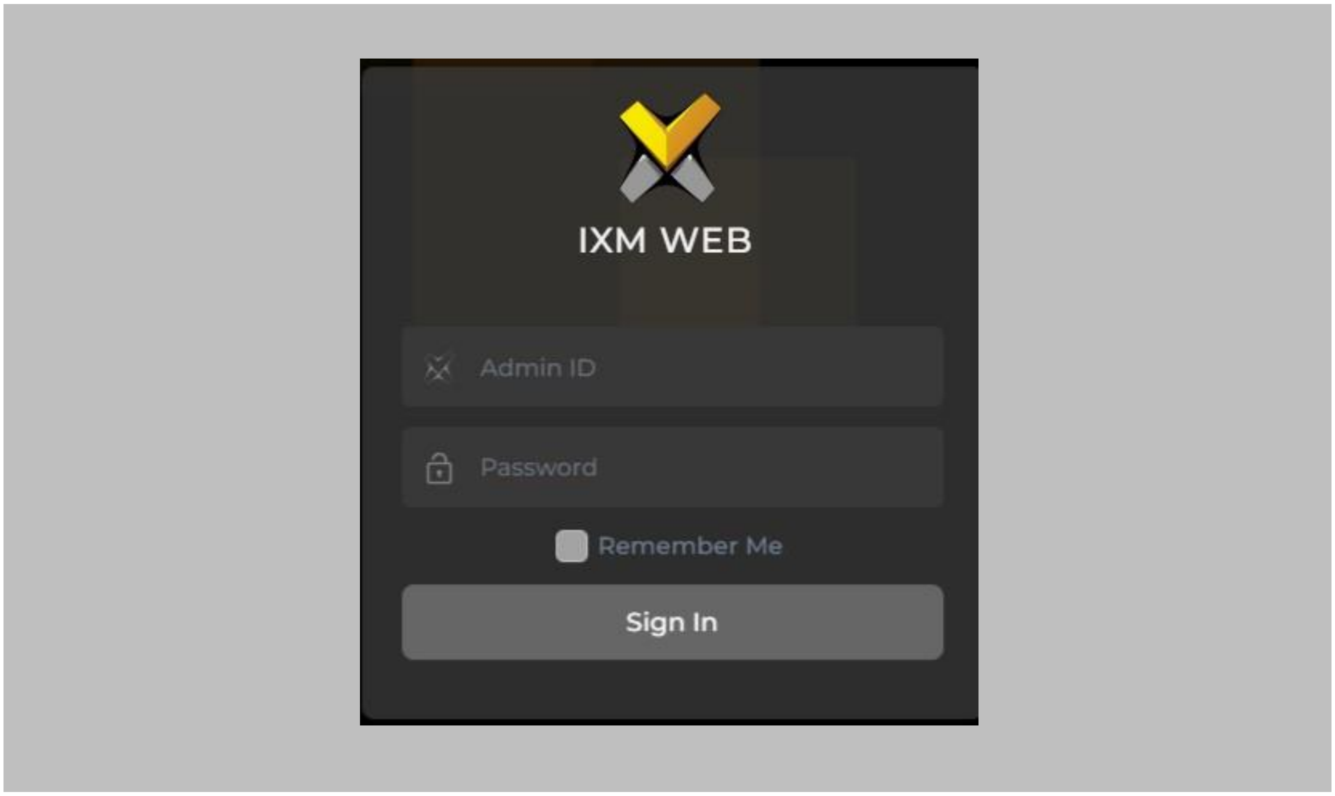
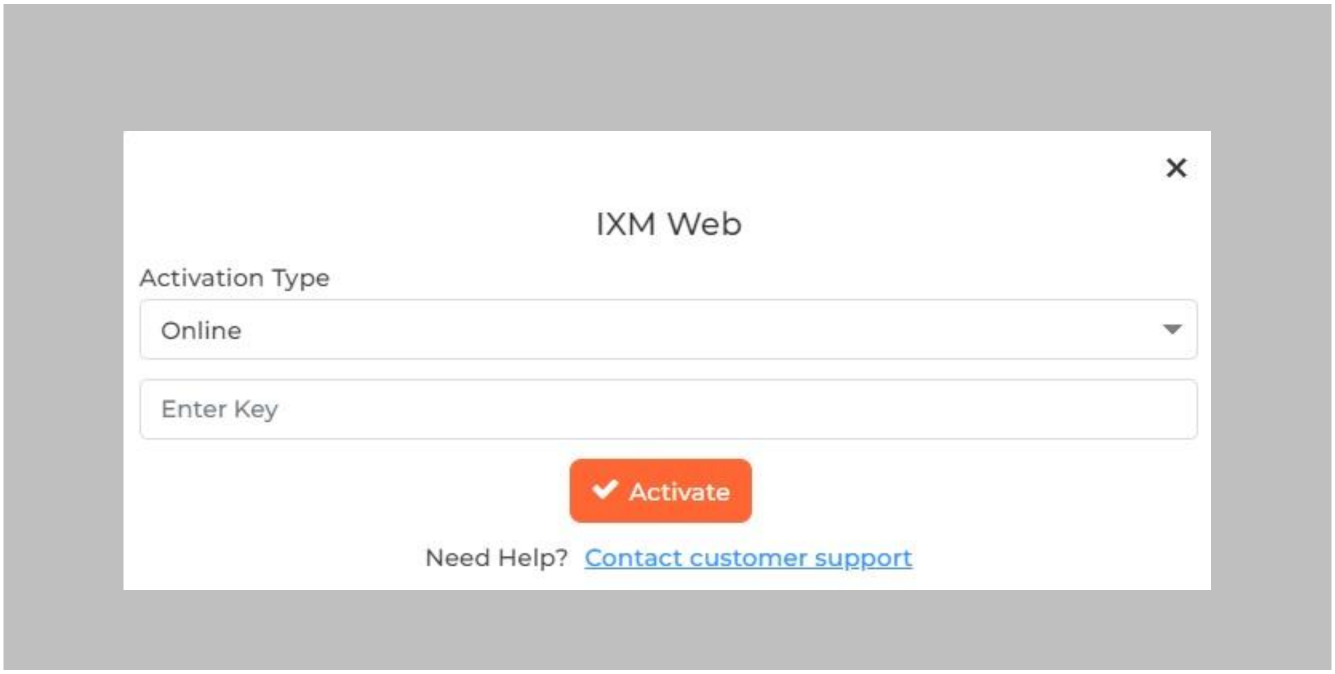


Figure 20: IXM WEB - Enter Login Credentials

STEP 2

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



IXM Web

Activation Type

Online

Enter Key

Figure 21: IXM WEB - License Setup

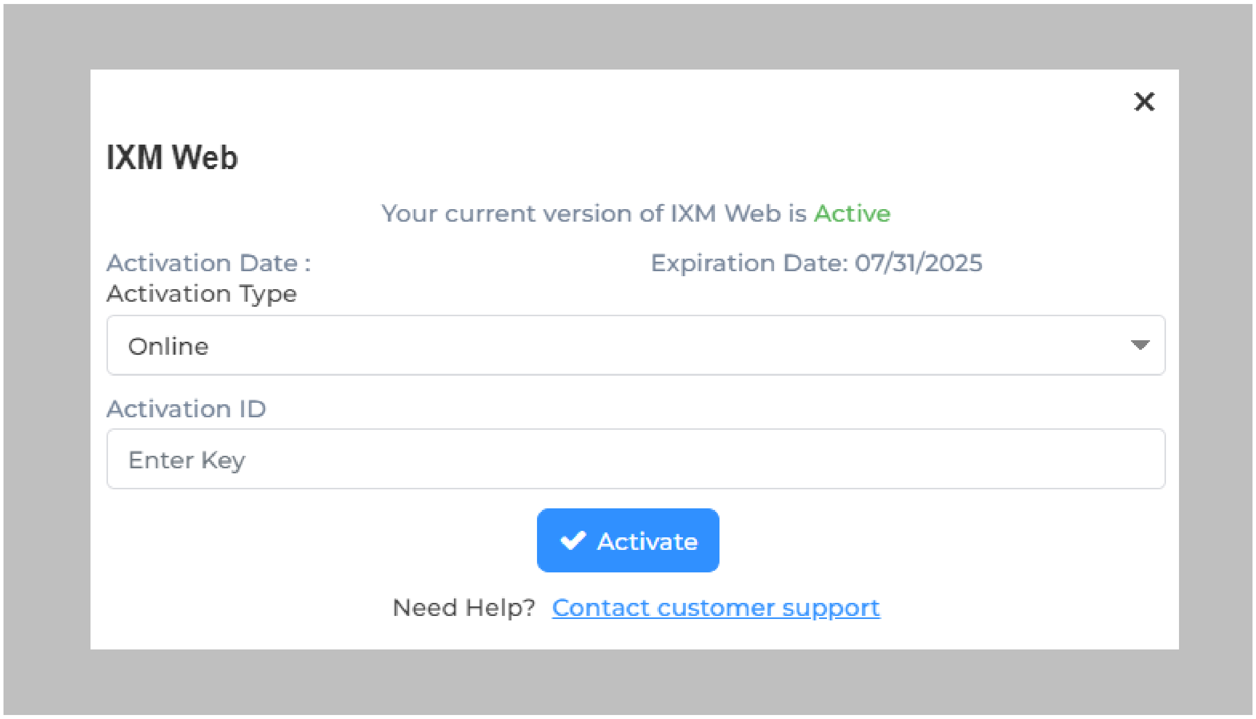
STEP 3

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

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

STEP 4

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



IXM Web

Your current version of IXM Web is Active

Activation Date :

Expiration Date: 07/31/2025

Activation Type

Online

Activation ID

Enter Key

Need Help? Contact customer support

Figure 22: IXM WEB - Online Activation

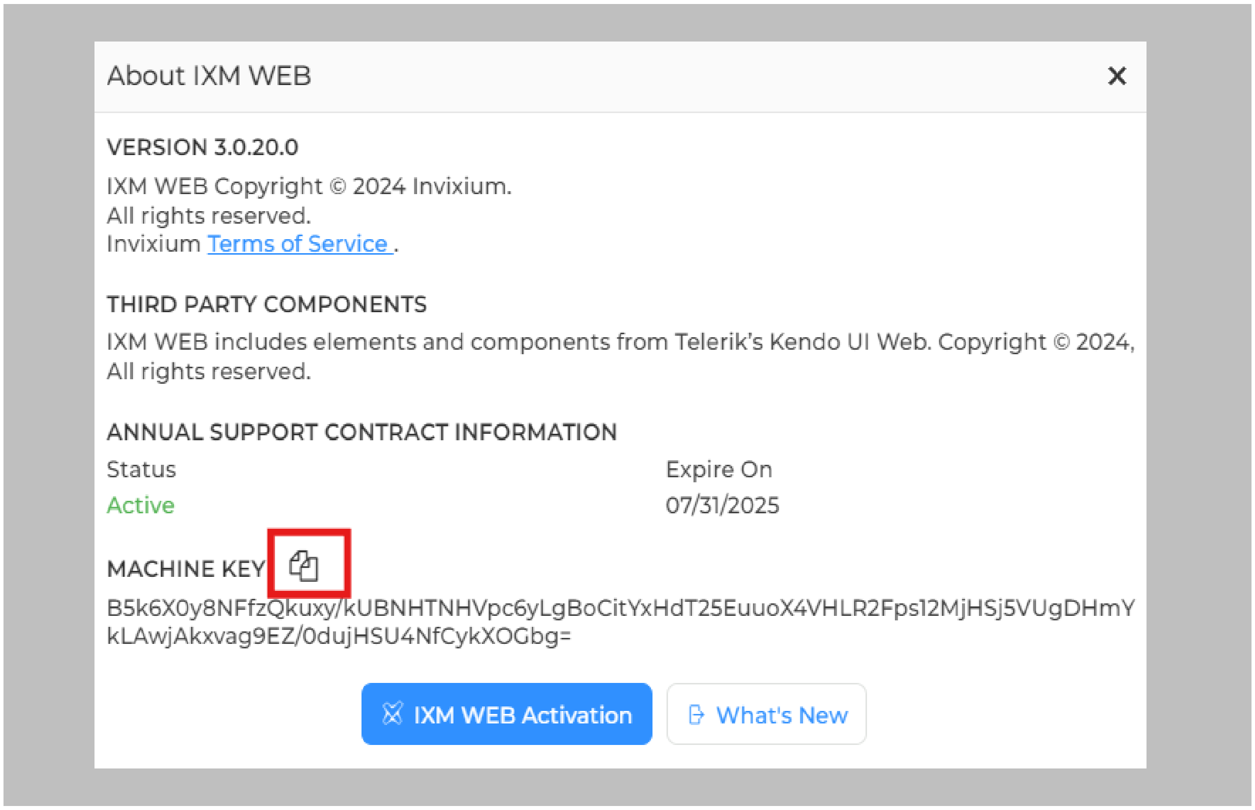
Security Center Module Activation

The option to activate a Genetec Security Center License is available under the **License** tab.

STEP 1

Select **Settings** icon on top right of the page >> Click on **About IXM WEB** >> Click on **copy to clipboard** button next to **MACHINE KEY.**

Request a **License** by sending email to support@invixium.com. Paste the copied machine key in the email.



About IXM WEB

VERSION 3.0.20.0

IXM WEB Copyright © 2024 Invixium.
All rights reserved.
Invixium Terms of Service .

THIRD PARTY COMPONENTS

IXM WEB includes elements and components from Telerik's Kendo UI Web. Copyright © 2024, All rights reserved.

ANNUAL SUPPORT CONTRACT INFORMATION

Status	Expire On
Active	07/31/2025

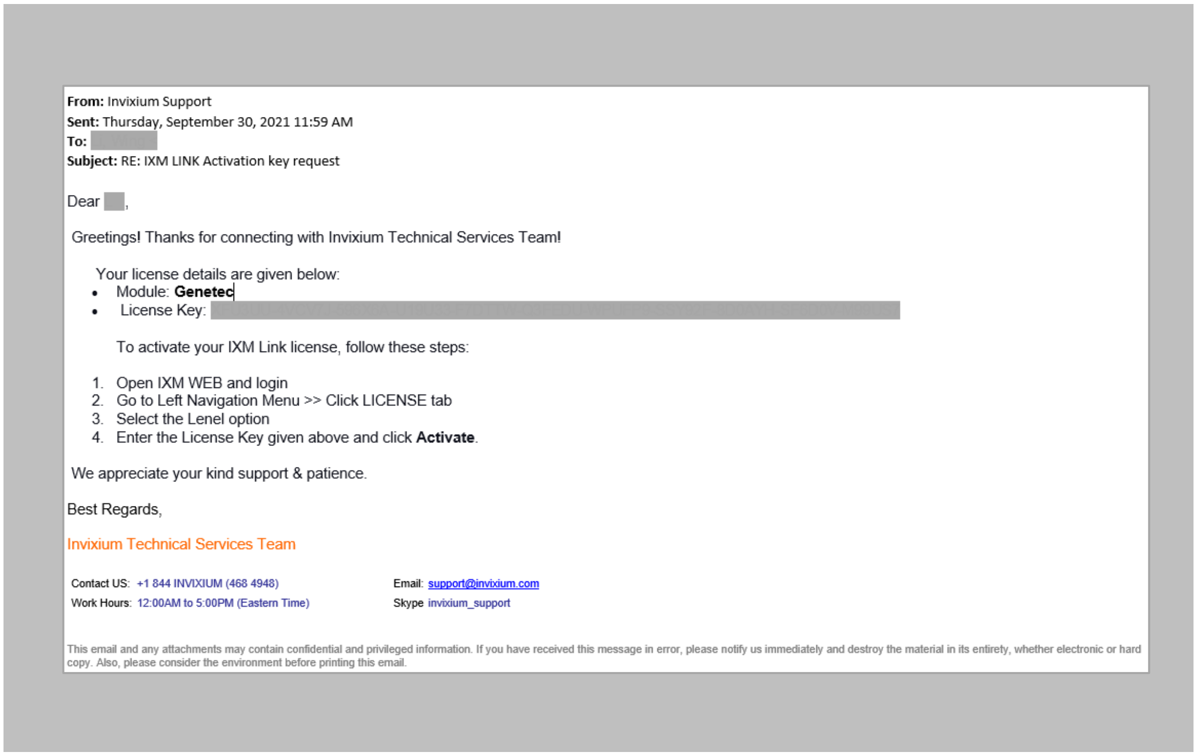
MACHINE KEY

B5k6X0y8NFfzQkuxy/kUBNHTNHVpc6yLgBoCitYxHdT25EuuoX4VHLR2Fps12MjHSj5VUgDHmYkLAwjAkxvag9EZ/0dujHSU4NfCykXOGbg=

Figure 23: IXM WEB – Request Link License

STEP 2

You will receive an email from Invixium Support containing a license key for the Genetec Security Center 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: **Genetec**
- License Key: [redacted]

To activate your IXM Link license, follow these steps:

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

We appreciate your kind support & patience.

Best Regards,

Invixium Technical Services Team

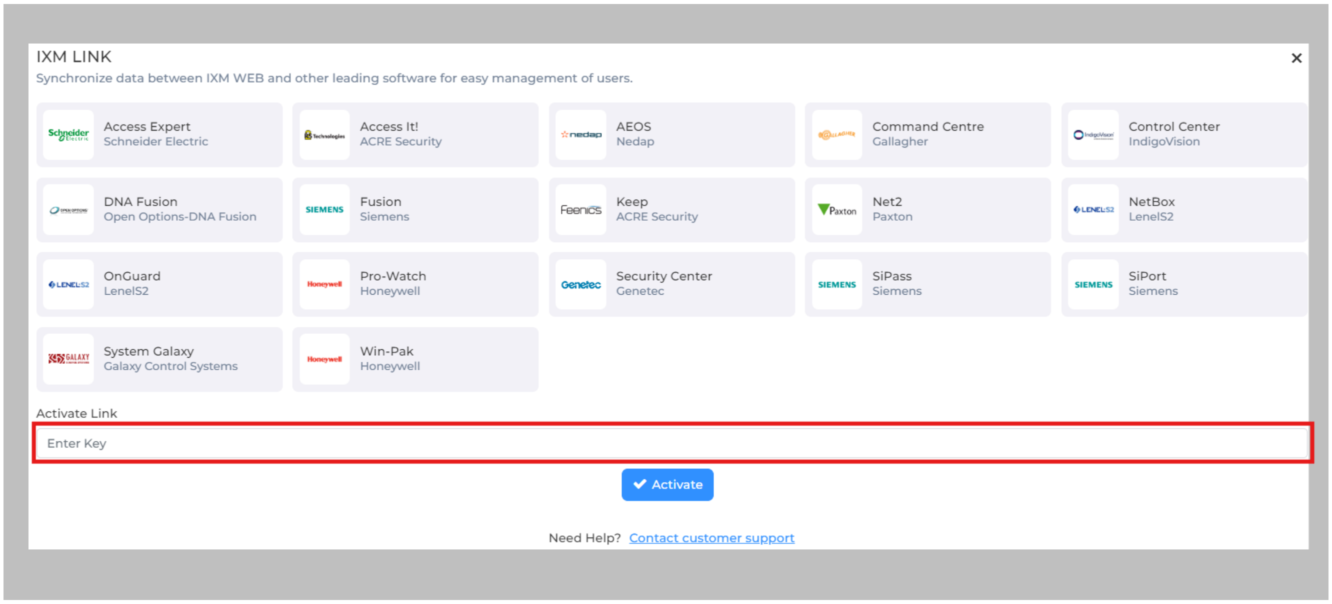
Contact US: +1 844 INVIXIUM (468 4948) Email: support@invixium.com
Work Hours: 12:00AM to 5:00PM (Eastern Time) Skype invixium_support

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

Figure 24: Genetec License Key Email

STEP 3

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



IXM LINK ×

Synchronize data between IXM WEB and other leading software for easy management of users.

Access Expert Schneider Electric	Access It! ACRE Security	AEOS Nedap	Command Centre Gallagher	Control Center IndigoVision
DNA Fusion Open Options-DNA Fusion	Fusion Siemens	Keep ACRE Security	Net2 Paxton	NetBox LenelS2
OnGuard LenelS2	Pro-Watch Honeywell	Security Center Genetec	SiPass Siemens	SiPort Siemens
System Galaxy Galaxy Control Systems	Win-Pak Honeywell			

Activate Link

Enter Key

Need Help? Contact customer support

Figure 25: IXM WEB - Activate Genetec Security Center Link License

RESULT

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

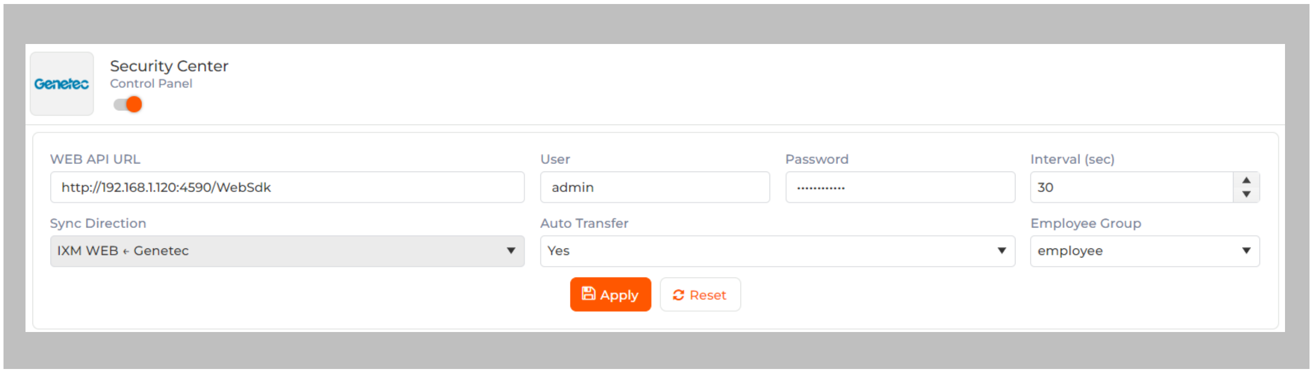
10. Configuring IXM Link for Genetec

Procedure

STEP 1

From the **Link** → click the **Security Center (Genetec)** icon.

Toggle the **Status** switch to enable.



Security Center
Control Panel

WEB API URL: http://192.168.1.120:4590/WebSdk

User: admin

Password: ············

Interval (sec): 30

Sync Direction: IXM WEB ← Genetec

Auto Transfer: Yes

Employee Group: employee

Figure 26: IXM WEB - Enable Genetec Link Module

Web API URL:

Enter the GSC WEB API URL. For example: https://localhost:4590/WebSdk

User:

Enter the name of the authorized user to connect to the Web SDK of Genetec Security Center.

Password:

Enter the Password of the authorized user to connect to the WEB SDK of Genetec Security Center

Interval (Sec):

Enter the duration of interval for data transfer between Genetec 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 ← Genetec

  Choosing this option will transfer data in one direction only, ie, from Genetec to IXM WEB. Genetec 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 → Genetec

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

- IXM WEB ↔ Genetec

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

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 Genetec 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:

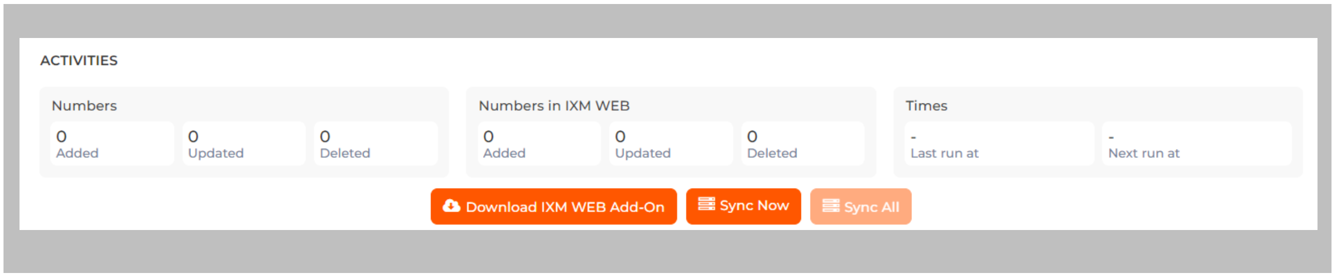
- This option will be enabled only when ‘Auto Transfer’ is set as ‘Yes’. Otherwise it will remain disabled.

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 Genetec and IXM WEB is possible only after successful connection.

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:



ACTIVITIES

Numbers			Numbers in IXM WEB			Times	
0 Added	0 Updated	0 Deleted	0 Added	0 Updated	0 Deleted	- Last run at	- Next run at

Figure 27: IXM WEB - Sync Activities

Numbers

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

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

RESULT

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

STEP 5

The **Download IXM WEB Add-On** feature allows to download and set up installation on each machine where Config Tool is available for enrollment of biometric templates from LINK view.

11. Installing IXM WEB Add-On

Download IXM WEB Add-On exe

Procedure

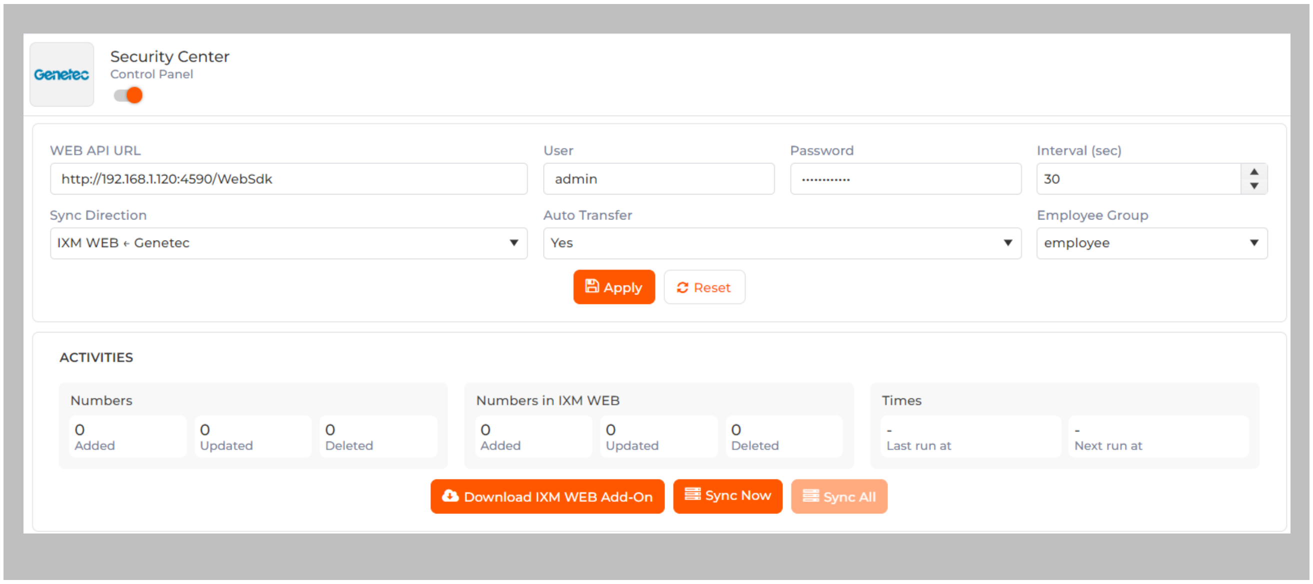
STEP 1

Log into IXM WEB and click on **Link** tab.

Click on **Security Center (Genetec).**

STEP 2

Click **Download IXM WEB Add-On** to download the executable file.



Security Center
Control Panel

WEB API URL: http://192.168.1.120:4590/WebSdk
User: admin
Password: ············
Interval (sec): 30
Sync Direction: IXM WEB ← Genetec
Auto Transfer: Yes
Employee Group: employee

ACTIVITIES

Numbers: 0 Added, 0 Updated, 0 Deleted
Numbers in IXM WEB: 0 Added, 0 Updated, 0 Deleted
Times: - Last run at, - Next run at

Figure 28: IXM WEB – Download IXM WEB Add-On

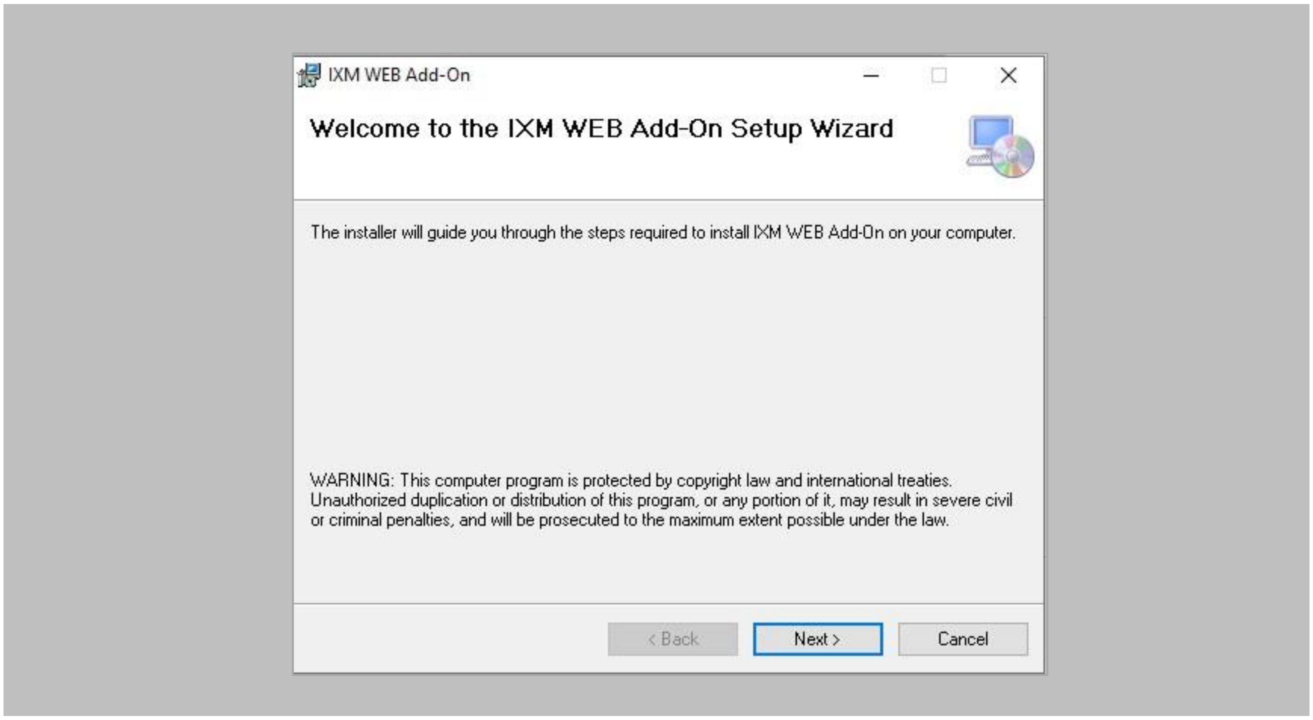
Note: The executable file should be downloaded on the same path as that of Genetec server.

Install IXM WEB Add-On

Procedure

STEP 1

Double click on the downloaded IXM WEB Add-On file in its path to start the Setup Wizard.



Welcome to the IXM WEB Add-On Setup Wizard

The installer will guide you through the steps required to install IXM WEB Add-On on your computer.

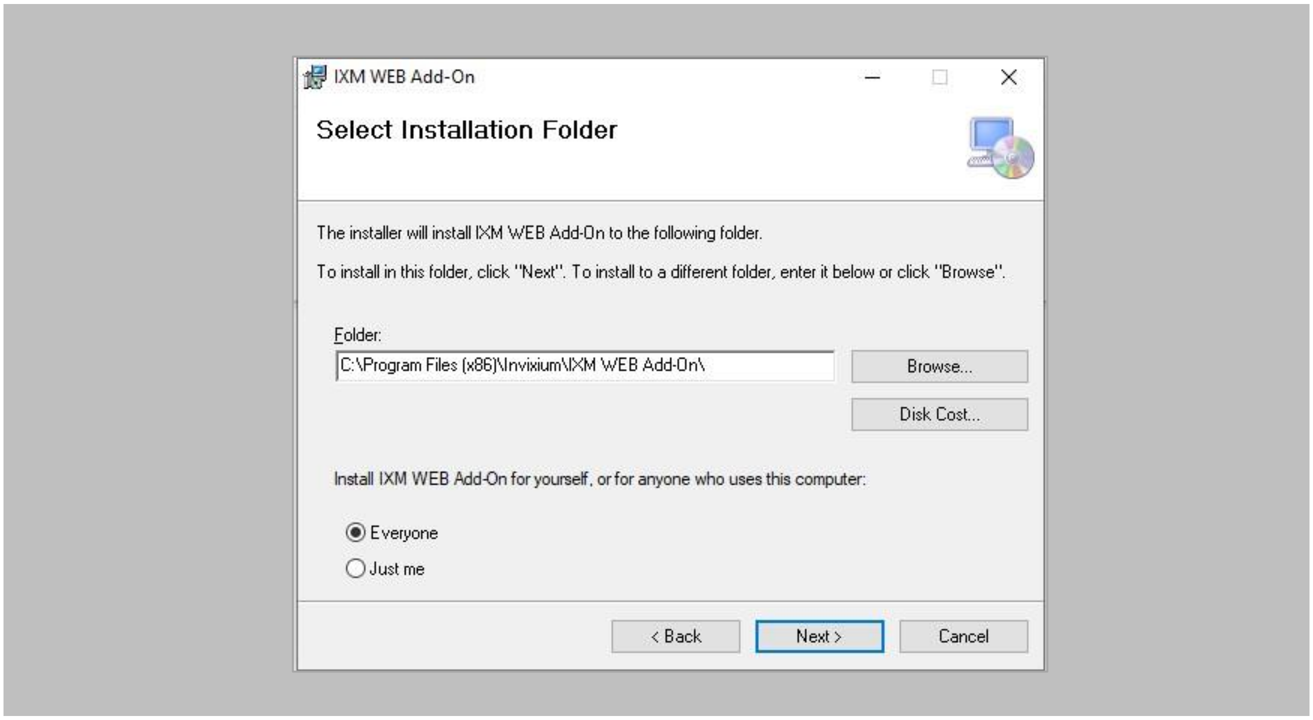
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 29: IXM WEB – Add-On Setup Wizard

Click **Next**.

STEP 2

The installer will install IXM WEB Add-On to the default folder. To install to a different folder, enter the path or click ‘Browse’.



Select Installation Folder

The installer will install IXM WEB Add-On to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\Invixium\IXM WEB Add-On\

Install IXM WEB Add-On for yourself, or for anyone who uses this computer:

● Everyone

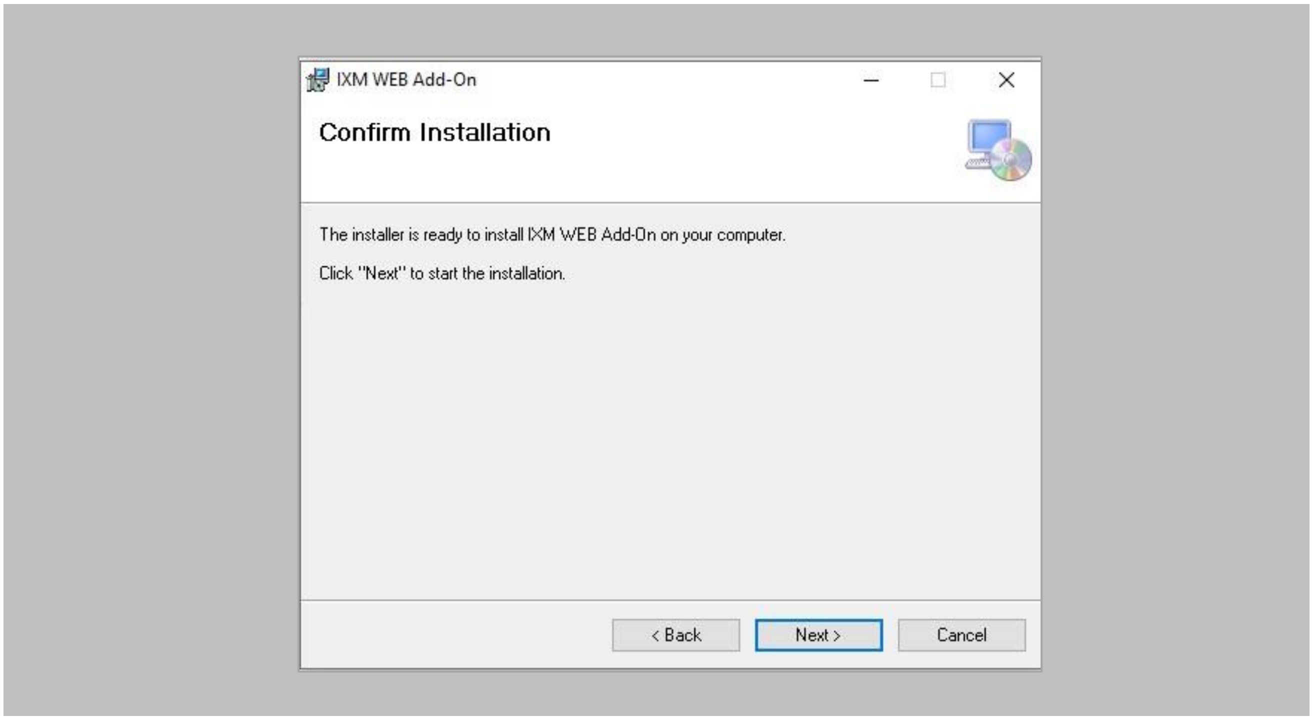
○ Just me

Figure 30: IXM WEB – Select Installation Folder

Click **Next.**

STEP 3

The installer is ready to install IXM WEB Add-On on the given path.



Confirm Installation

The installer is ready to install IXM WEB Add-On on your computer.

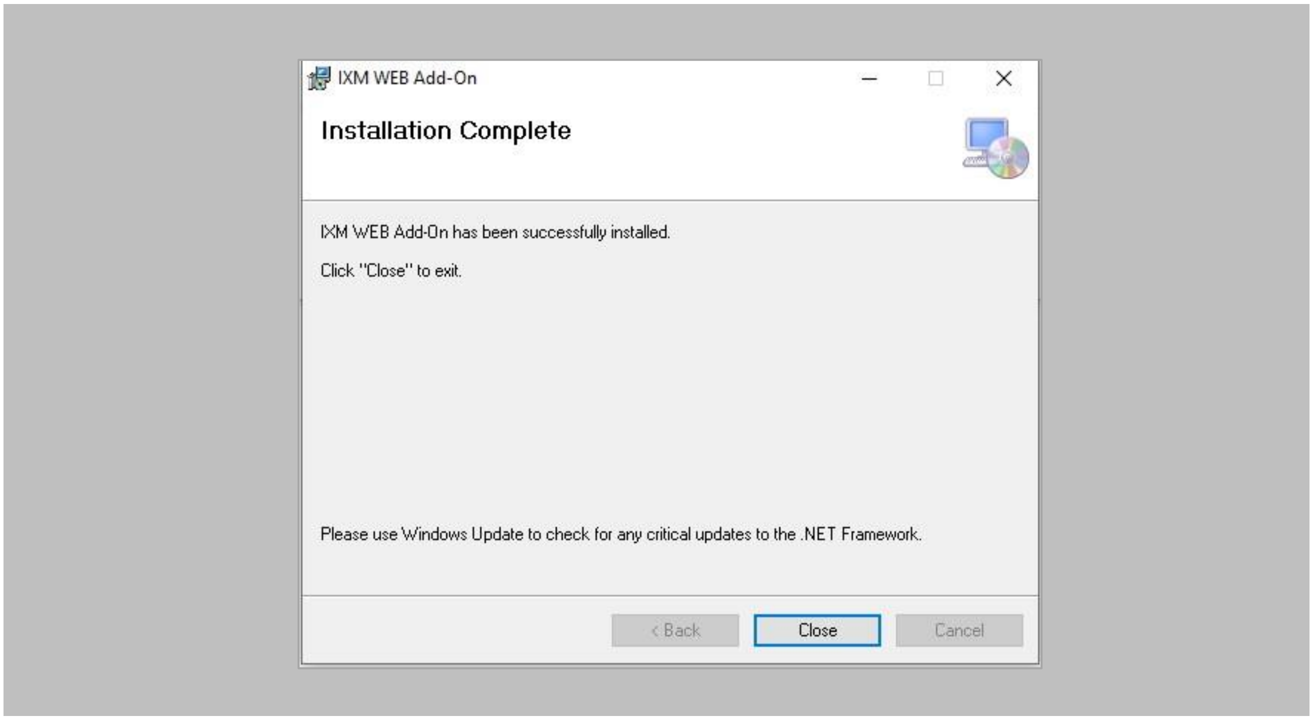
Click "Next" to start the installation.

Figure 31: IXM WEB – Confirm Installation

Click **Next.**

STEP 4

Installation of IXM WEB Add-On is complete.



Installation Complete

IXM WEB Add-On has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

Figure 32: IXM WEB – Add-On Installation Complete

Click **Close**.

12. Create System User(s) for Biometric Enrollment

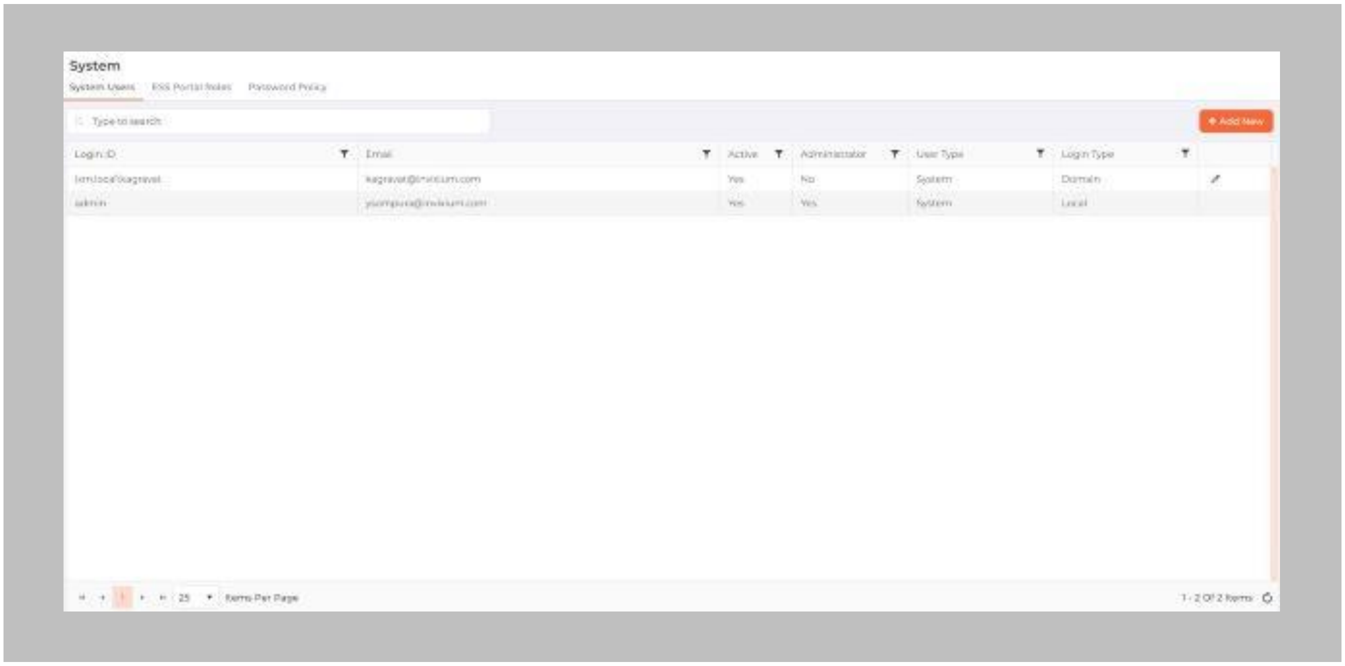
Creating System User(s) for Biometric Enrollment

Procedure

STEP 1

Log into IXM WEB.

On the top right of default page, click on the **User Menu** → Click **Users**. The application will redirect to the System Users window.



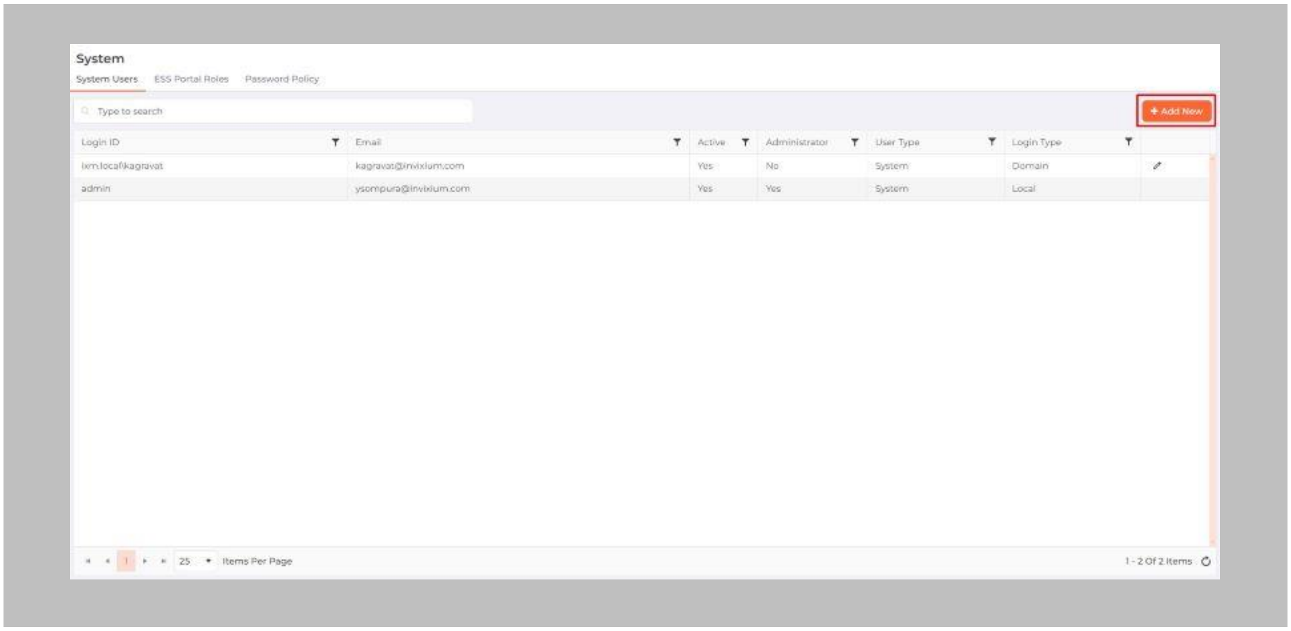
System

Login ID	Email	Active	Administrator	User Type	Login Type
ixmlocal\kagravat	kagravat@invixium.com	Yes	No	System	Domain
admin	ysompura@invixium.com	Yes	Yes	System	Local

Figure 33: IXM WEB - Create System User

STEP 2

Click **Add New**.



Login ID	Email	Active	Administrator	User Type	Login Type	
ixm.local\kagravat	kagravat@invixium.com	Yes	No	System	Domain	
admin	ysompura@invixium.com	Yes	Yes	System	Local	

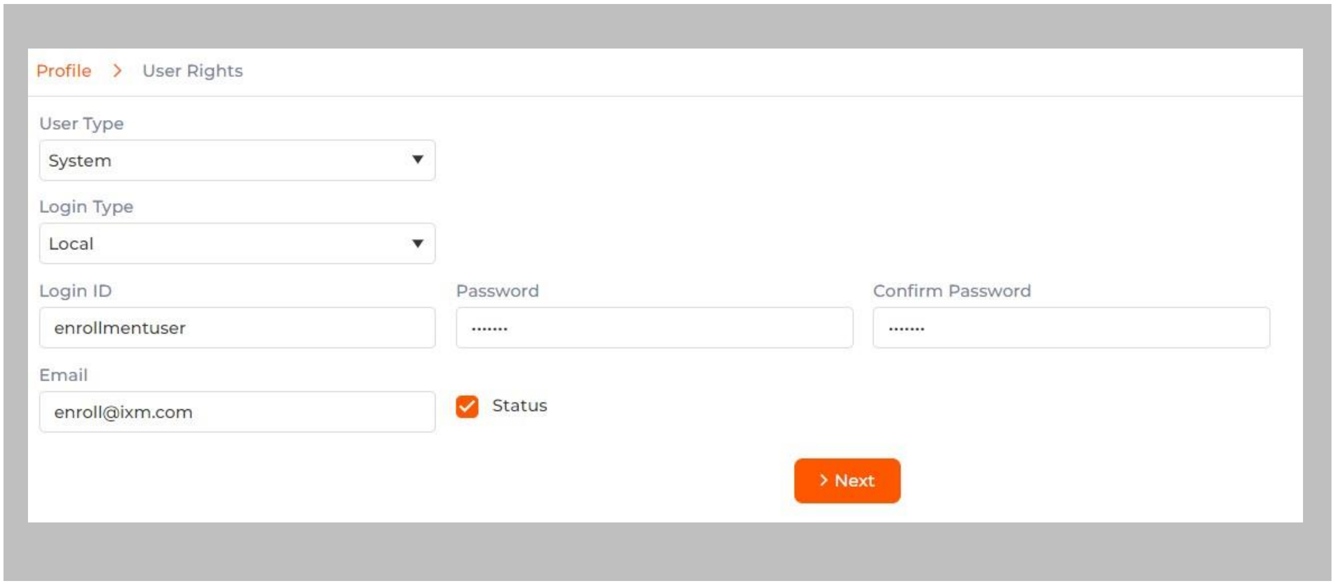
Figure 34: IXM WEB - Add New System User

Creating a system user requires the following details:

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

STEP 3

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



User Type: System

Login Type: Local

Login ID: enrollmentuser

Password: •••••••

Confirm Password: •••••••

Email: enroll@ixm.com

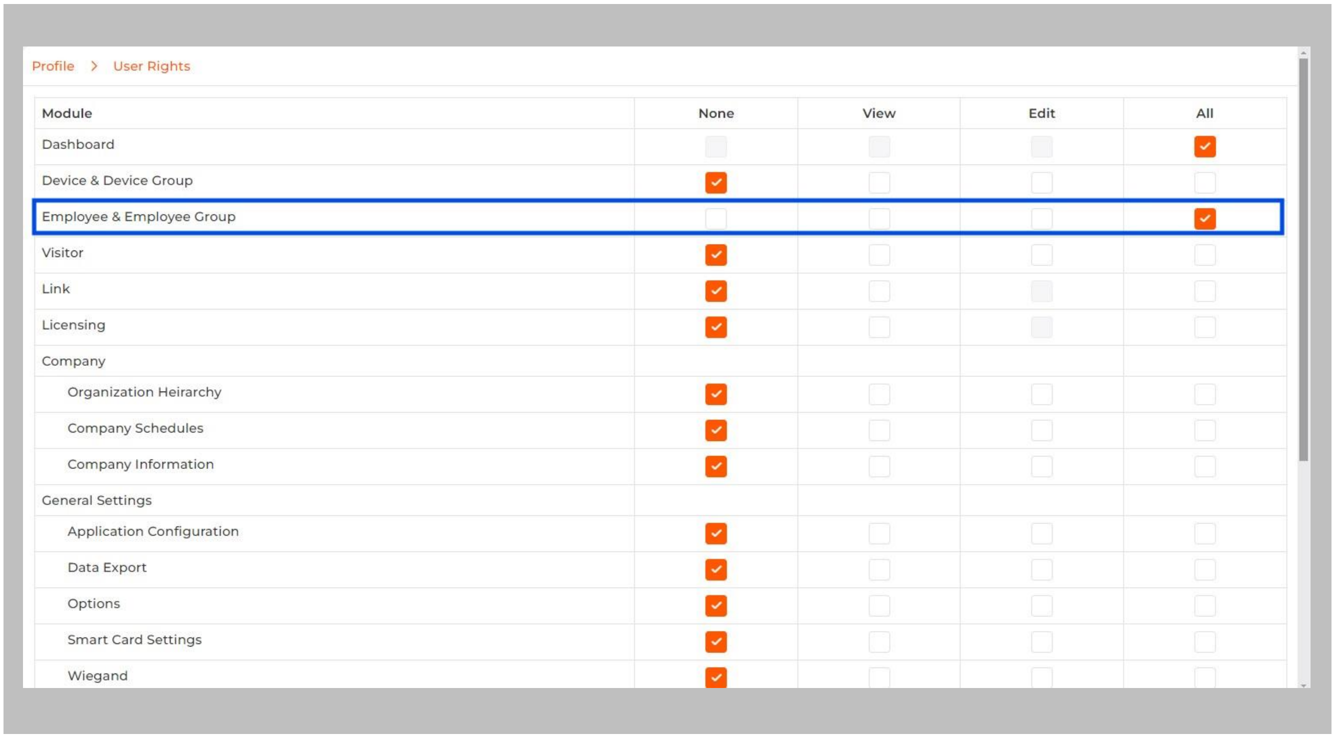
☑ Status

Figure 35: IXM WEB - New System User

STEP 4

Add an email address.

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



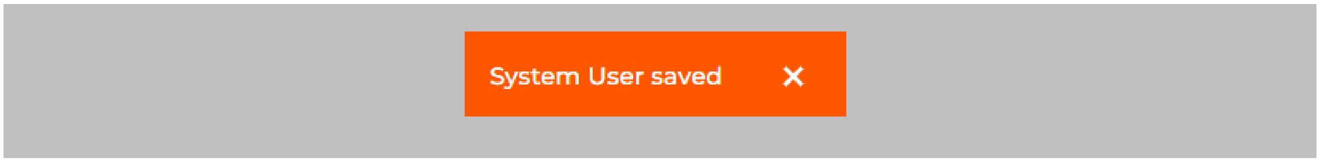
Profile > User Rights

Module	None	View	Edit	All
Dashboard	□	□	□	☑
Device & Device Group	☑	□	□	□
Employee & Employee Group	□	□	□	☑
Visitor	☑	□	□	□
Link	☑	□	□	□
Licensing	☑	□	□	□
Company				
Organization Heirarchy	☑	□	□	□
Company Schedules	☑	□	□	□
Company Information	☑	□	□	□
General Settings				
Application Configuration	☑	□	□	□
Data Export	☑	□	□	□
Options	☑	□	□	□
Smart Card Settings	☑	□	□	□
Wiegand	☑	□	□	□

Figure 36: Employee and Employee Group Rights

STEP 5

Click **Save**.



System User saved ✕

Figure 37: IXM WEB - Save System User

13. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

Click the **Devices** tab.

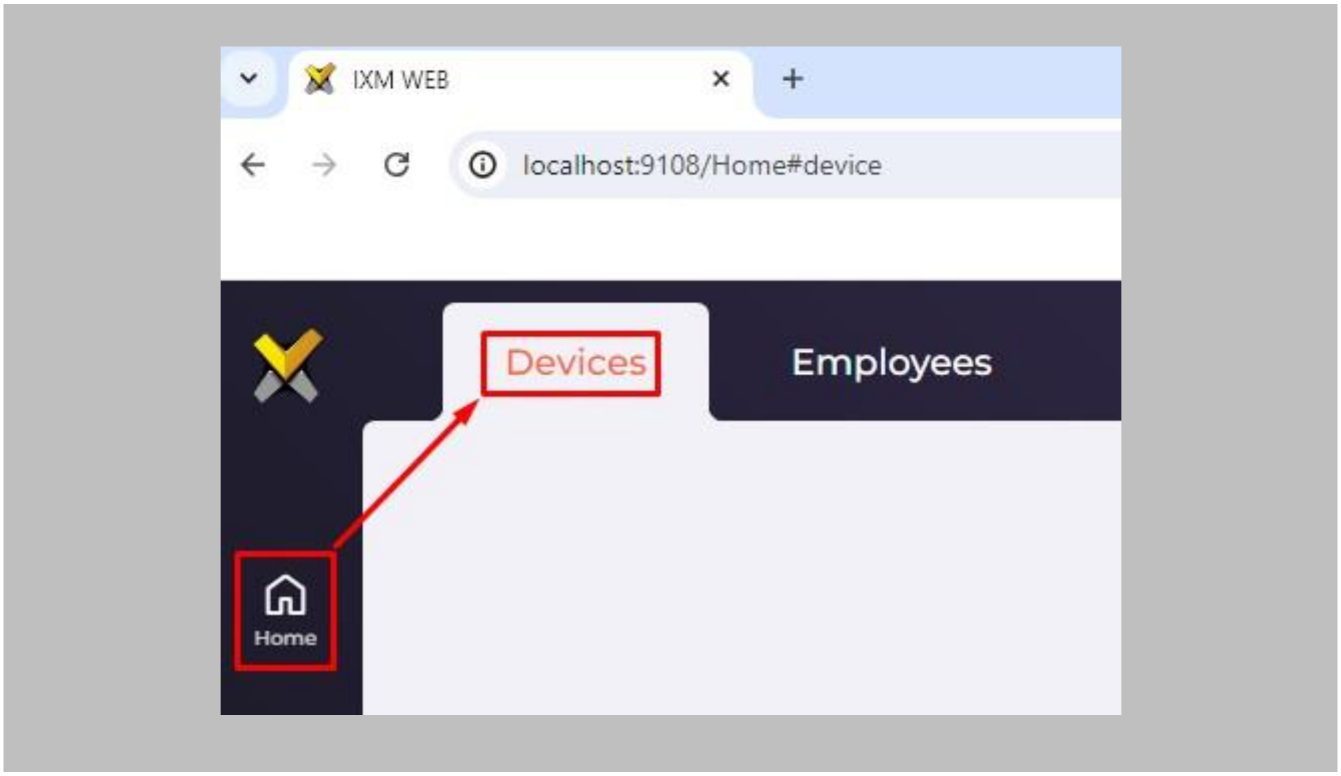
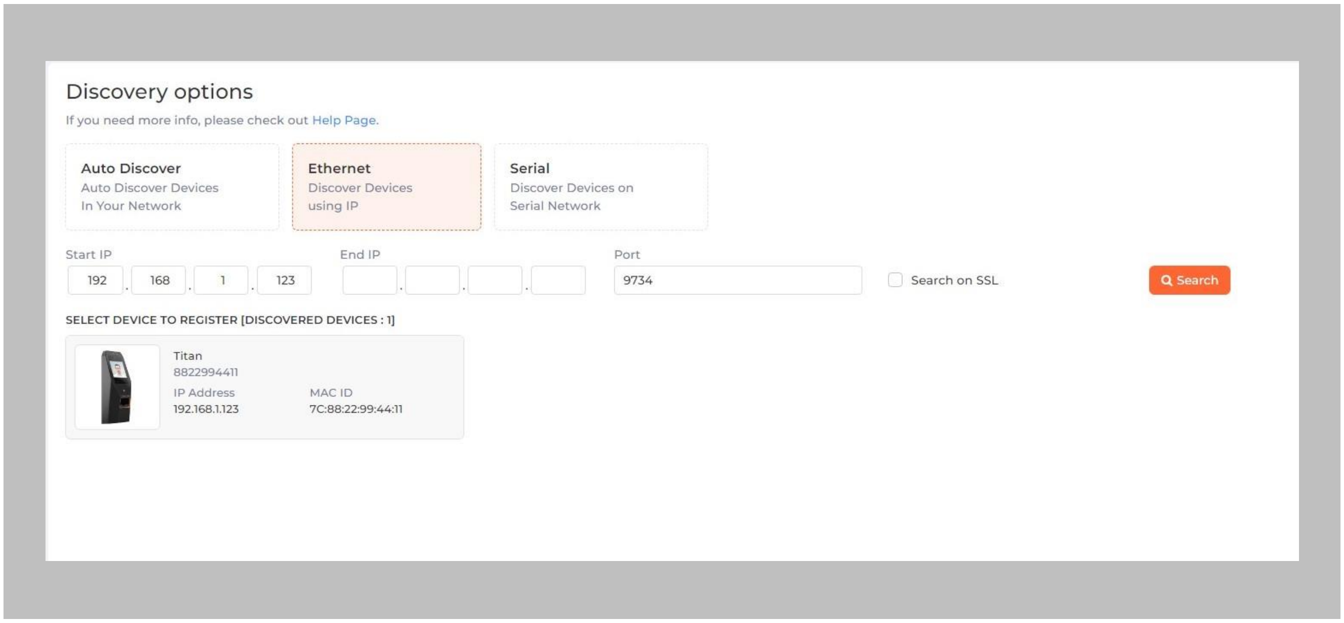


Figure 38: IXM WEB - Devices Tab

STEP 2

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



Discovery options

If you need more info, please check out Help Page.

Auto Discover
Auto Discover Devices In Your Network
Ethernet
Discover Devices using IP
Serial
Discover Devices on Serial Network

Start IP: 192 . 168 . 1 . 123

End IP: . . .

Port: 9734

□ Search on SSL

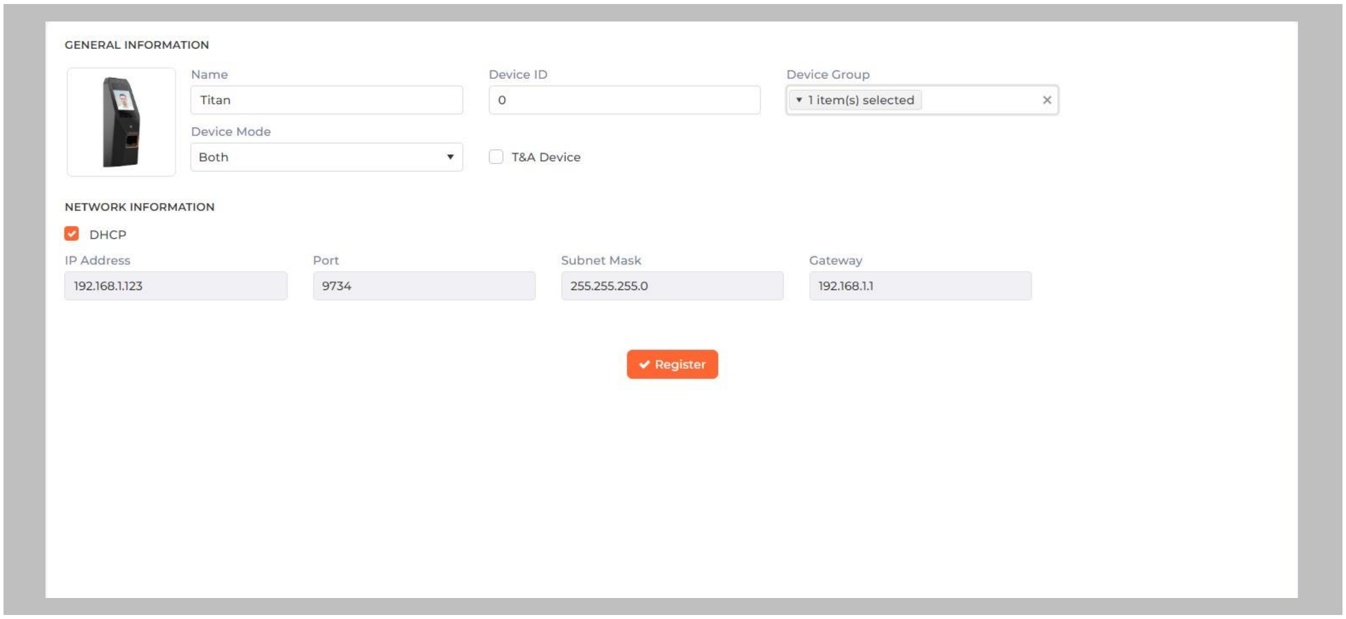
SELECT DEVICE TO REGISTER [DISCOVERED DEVICES : 1]

Titan
8822994411
IP Address: 192.168.1.123
MAC ID: 7C:88:22:99:44:11

Figure 39: IXM WEB - Search Device Using IP Address

STEP 3

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



GENERAL INFORMATION

Name: Titan

Device ID: 0

Device Group: 1 item(s) selected

Device Mode: Both

□ T&A Device

NETWORK INFORMATION

☑ DHCP

IP Address	Port	Subnet Mask	Gateway
192.168.1.123	9734	255.255.255.0	192.168.1.1

Figure 40: IXM WEB - Register Device

STEP 4

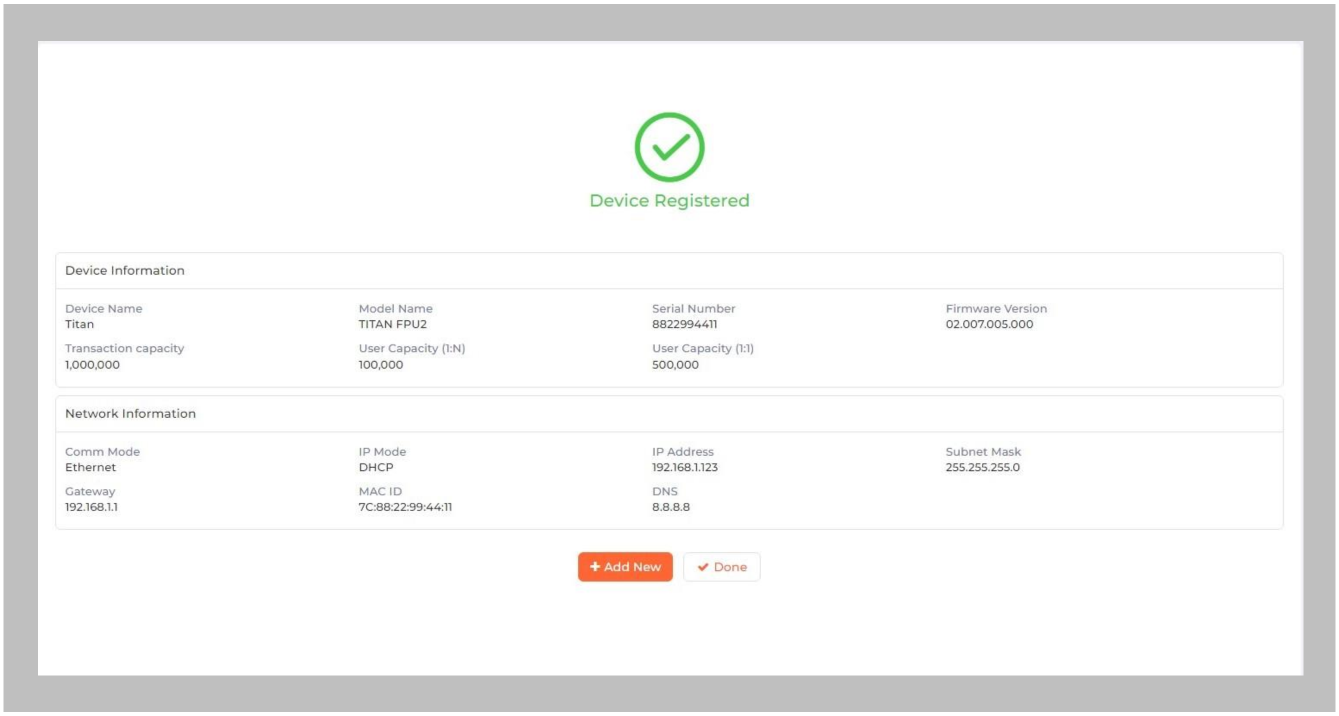
Name the **device** <u>exactly as the name of the door</u> it will be used for.

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**.



Device Registered

Device Information

Device Name
Titan

Model Name
TITAN FPU2

Serial Number
8822994411

Firmware Version
02.007.005.000

Transaction capacity
1,000,000

User Capacity (1:N)
100,000

User Capacity (1:1)
500,000

Network Information

Comm Mode
Ethernet

IP Mode
DHCP

IP Address
192.168.1.123

Subnet Mask
255.255.255.0

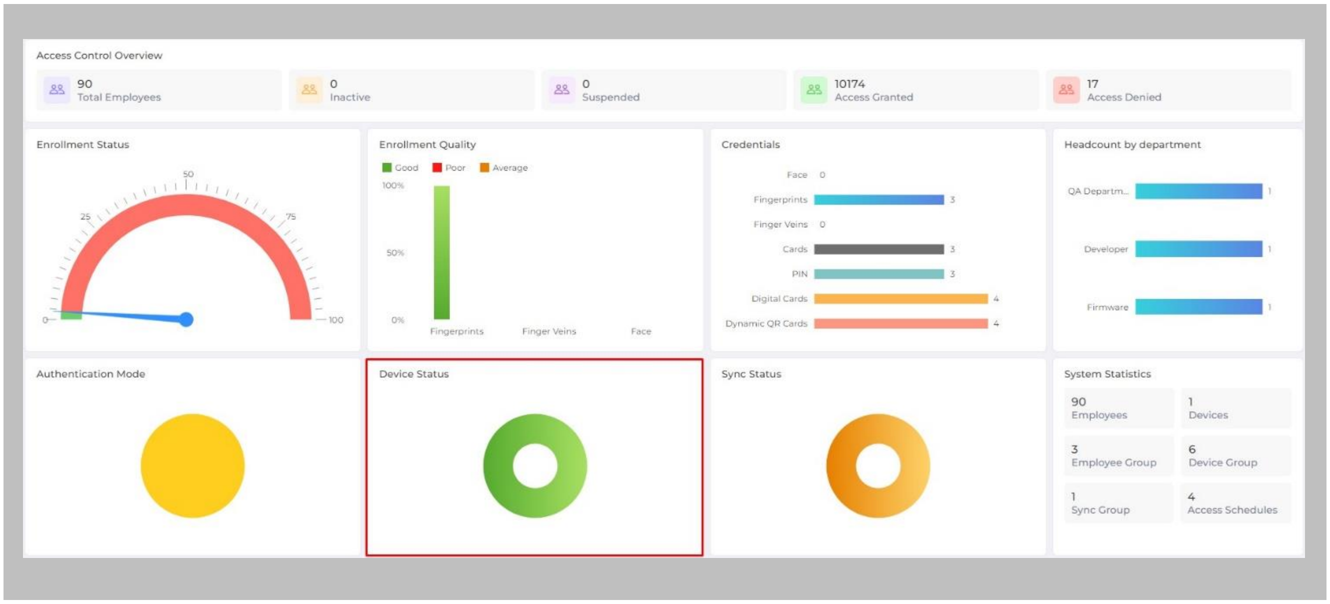
Gateway
192.168.1.1

MAC ID
7C:88:22:99:44:11

DNS
8.8.8.8

Figure 41: 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).



Access Control Overview

90 Total Employees

0 Inactive

0 Suspended

10174 Access Granted

17 Access Denied

System Statistics

90 Employees

1 Devices

3 Employee Group

6 Device Group

1 Sync Group

4 Access Schedules

Figure 42: IXM WEB - Dashboard, Device Status

14. Adding an Invixium Device to a Device Group

Procedure

STEP 1

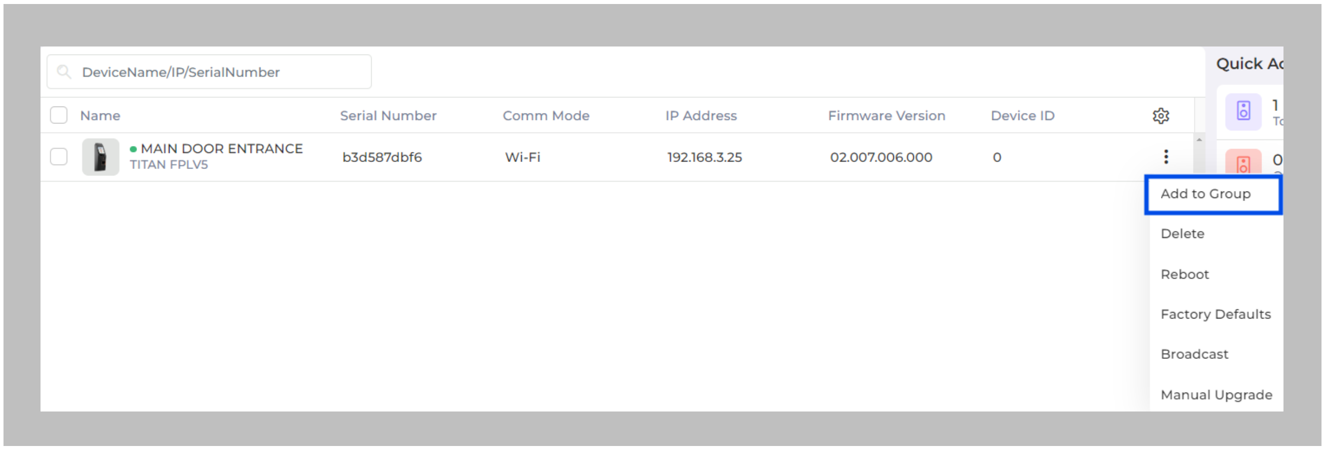
Any of below methods can be used to add device to device group.

METHOD 1: Go to **Devices** → click on **Manage Device Group**. Add the device by clicking vertical ellipses button of respective Device Group → click on **Add Device** → Search for device → click **Add** button.

METHOD 2: Go to **Devices** → click on **Manage Device Group**. Click on Device Group Name → click on **Add Device** button. Search for device → click **Add** button.

METHOD 3: On Device list page, click on vertical ellipses button of device → click on **Add to Group** → Search and select required group name → Click **Add**.

METHOD 4: On Device list page, select single or multiple device(s) → click on **Add to Group** icon visible next to search box → Search and select required group name → Click **Add**.



Name	Serial Number	Comm Mode	IP Address	Firmware Version	Device ID
● MAIN DOOR ENTRANCE TITAN FPLV5	b3d587dbf6	Wi-Fi	192.168.3.25	02.007.006.000	0

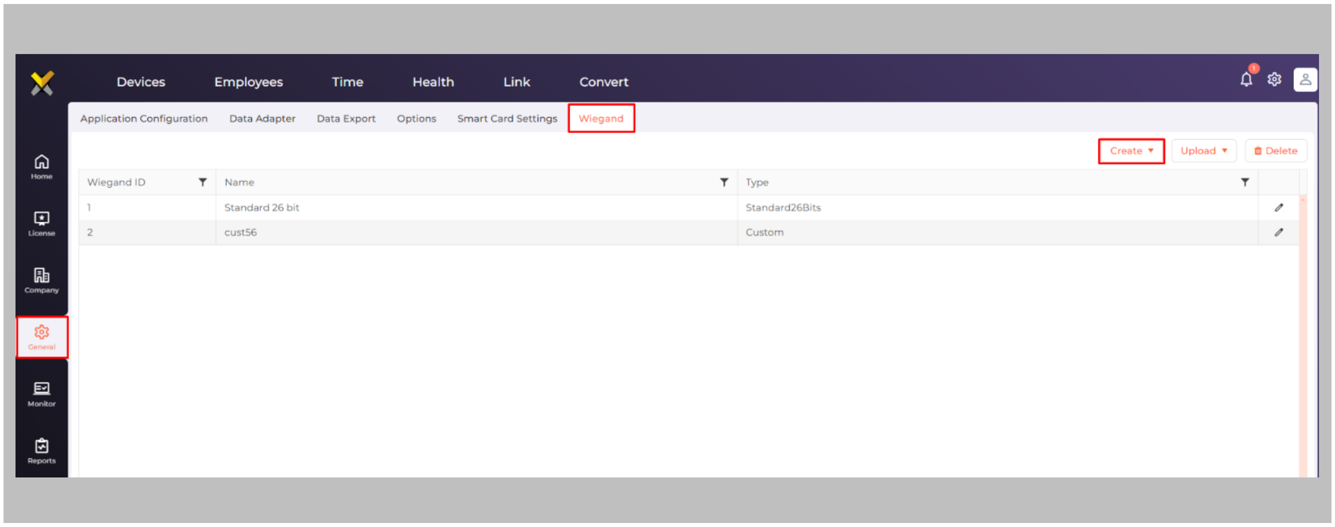
Figure 43: IXM WEB - Assign Device Group

Configuring Wiegand Format to Assign Invixium Readers

Note: Invixium devices support upto 512 bit long Wiegand format. Accordingly, you can create a Wiegand format as per your requirement.

STEP 1

Click **General** and Navigate to **Wiegand** → **Create.**

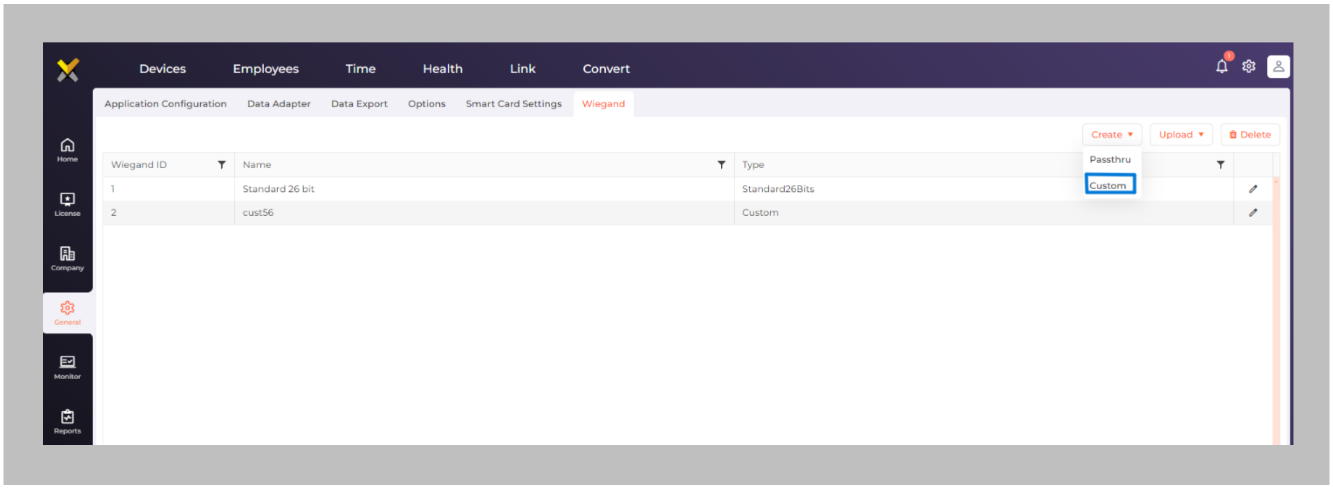


Wiegand ID	Name	Type
1	Standard 26 bit	Standard26Bits
2	cust56	Custom

Figure 44: IXM WEB - Create Wiegand Format

STEP 2

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

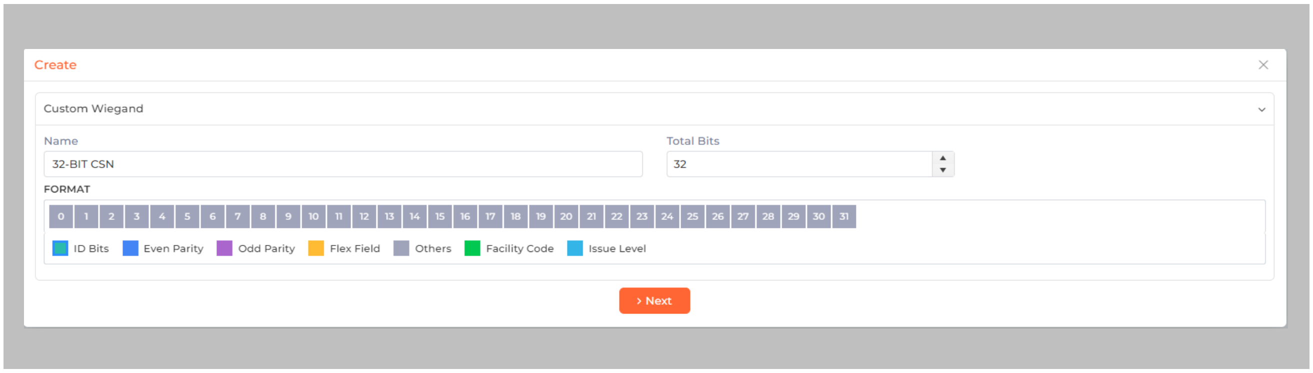


Wiegand ID	Name	Type
1	Standard 26 bit	Standard26Bits
2	cust56	Custom

Figure 45: 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.



Create

Custom Wiegand

Name: 32-BIT CSN

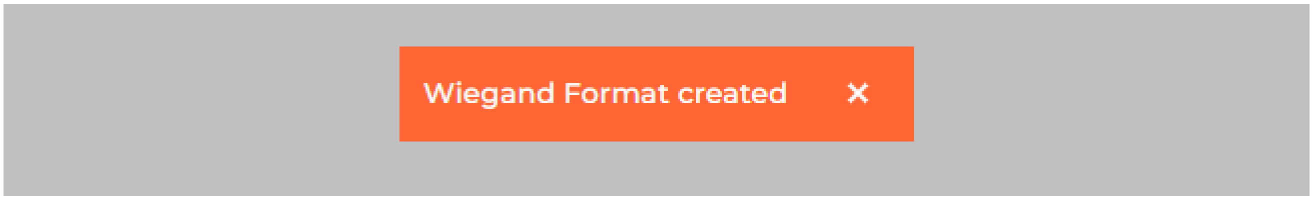
Total Bits: 32

FORMAT

Figure 46: IXM WEB - Custom Wiegand Format

STEP 4

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

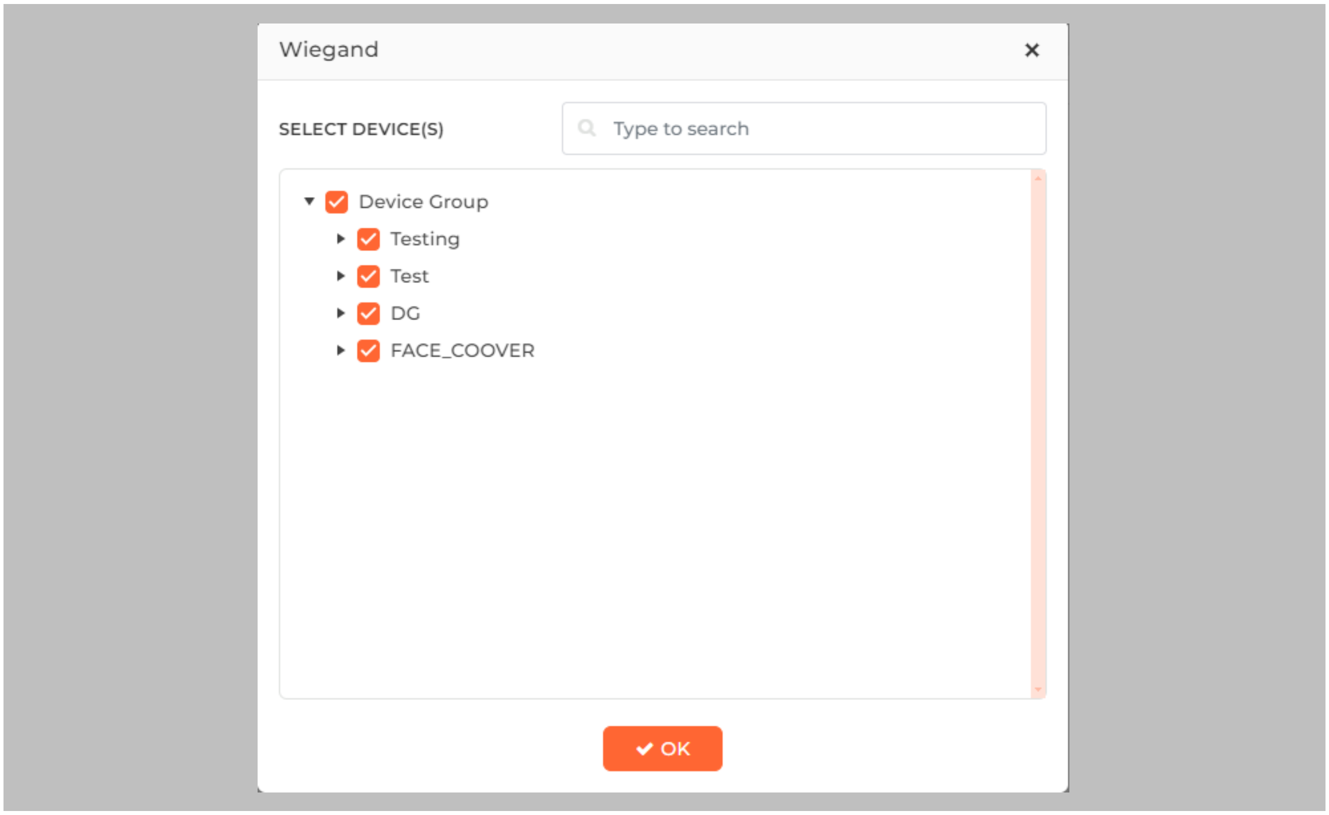


Wiegand Format created ✕

Figure 47: IXM WEB – Custom Wiegand Format Created

STEP 5

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



Wiegand ×

SELECT DEVICE(S) | Type to search

- ☑ Device Group
  - ☑ Testing
  - ☑ Test
  - ☑ DG
  - ☑ FACE_COOVER

Figure 48: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invixium Readers

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

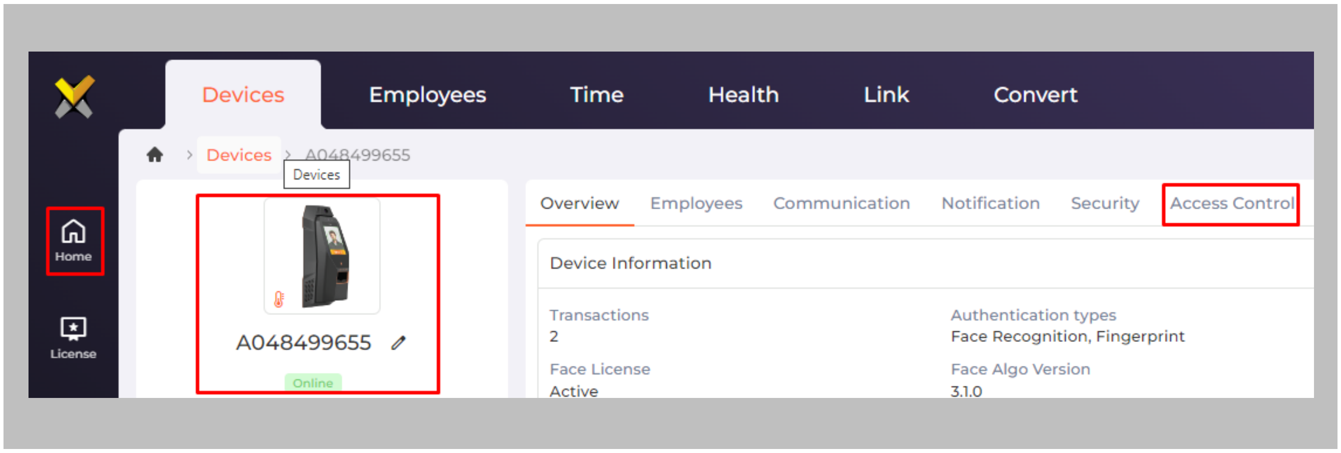
The created Wiegand will be used to define which output format will be sent to GSC.

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.



Device Information

Transactions
2

Authentication types
Face Recognition, Fingerprint

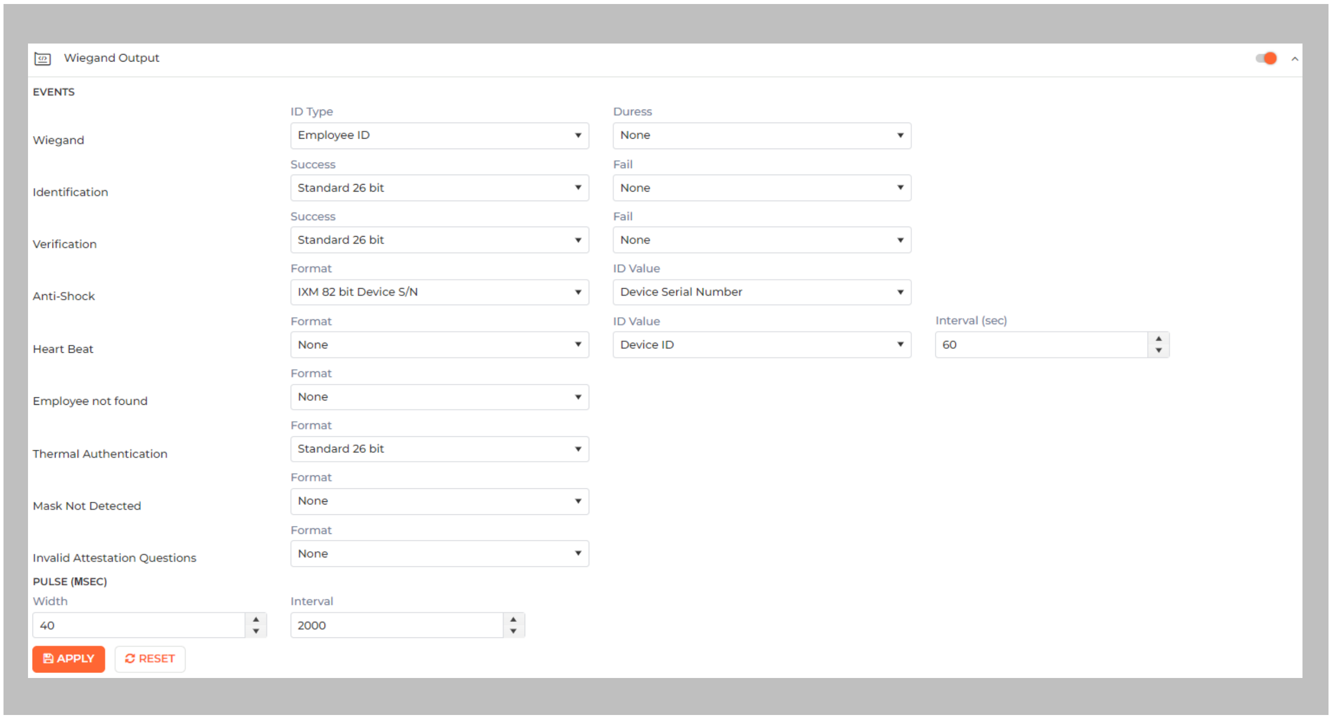
Face License
Active

Face Algo Version
3.1.0

Figure 49: 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.



Wiegand Output

EVENTS

Wiegand	ID Type: Employee ID	Duress: None	
Identification	Success: Standard 26 bit	Fail: None	
Verification	Success: Standard 26 bit	Fail: None	
Anti-Shock	Format: IXM 82 bit Device S/N	ID Value: Device Serial Number	
Heart Beat	Format: None	ID Value: Device ID	Interval (sec): 60
Employee not found	Format: None		
Thermal Authentication	Format: Standard 26 bit		
Mask Not Detected	Format: None		
Invalid Attestation Questions	Format: None		

PULSE (MSEC)

Width: 40	Interval: 2000

Figure 50: 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 Genetec, select either Default Card or Actual Card.

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

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.

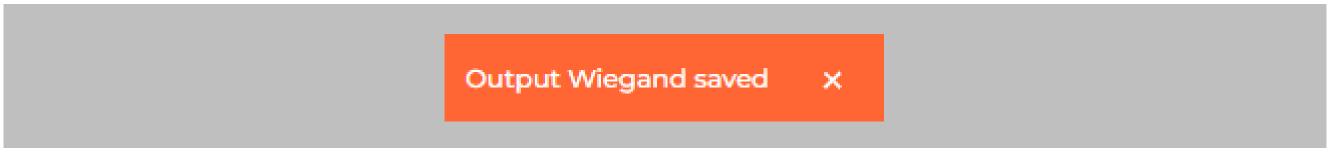
Note: For fingerprint and face access, default card Wiegand output data will be generated.

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.**



Output Wiegand saved ×

Figure 51: 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 GSC controller.
- To make this Wiegand output work on Genetec, you will need to make sure the Wiegand format is available in Genetec for use on the controllers talking to the Invixium reader (by Wiegand or OSDP).

Configuring Panel Feedback with Genetec

Procedure

STEP 1

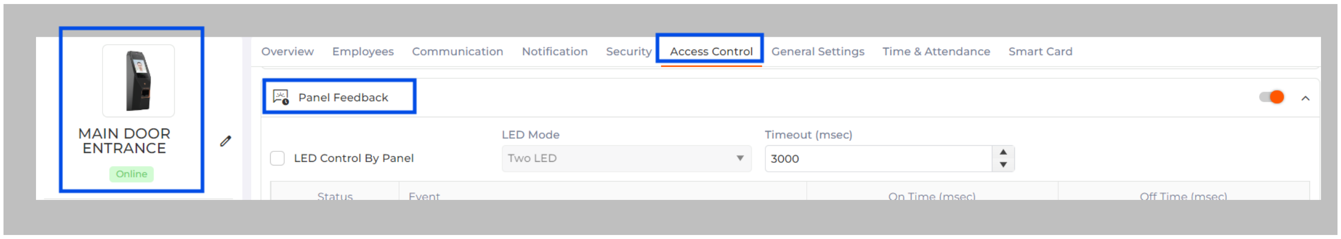
Connect Wiegand Data D0 of the Genetec Panel with **WDATA_OUT0** of the IXM device, Wiegand Data D1 of the Genetec Panel with WDATA_OUT1, and Wiegand Ground of the Genetec Panel with WGND of the IXM Device.

STEP 2

Connect the **LED** of the Genetec 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**.



□ LED Control By Panel

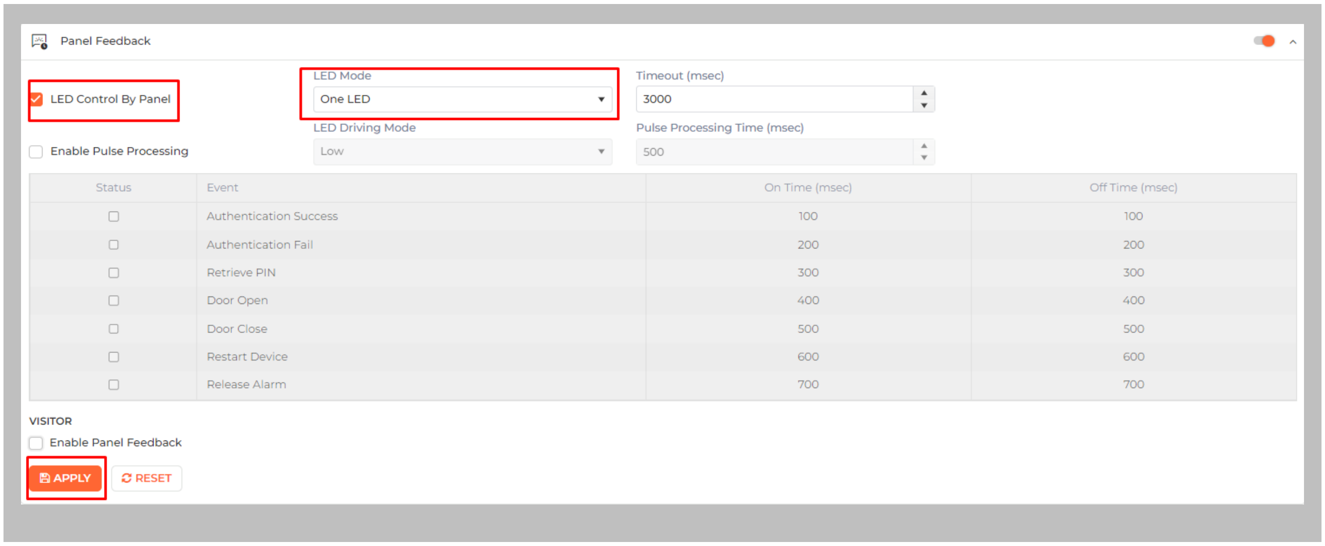
LED Mode: Two LED

Timeout (msec): 3000

Figure 52: 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**.



Panel Feedback

☑ LED Control By Panel

LED Mode: One LED

Timeout (msec): 3000

☐ Enable Pulse Processing

LED Driving Mode: Low

Pulse Processing Time (msec): 500

Status	Event	On Time (msec)	Off Time (msec)
☐	Authentication Success	100	100
☐	Authentication Fail	200	200
☐	Retrieve PIN	300	300
☐	Door Open	400	400
☐	Door Close	500	500
☐	Restart Device	600	600
☐	Release Alarm	700	700

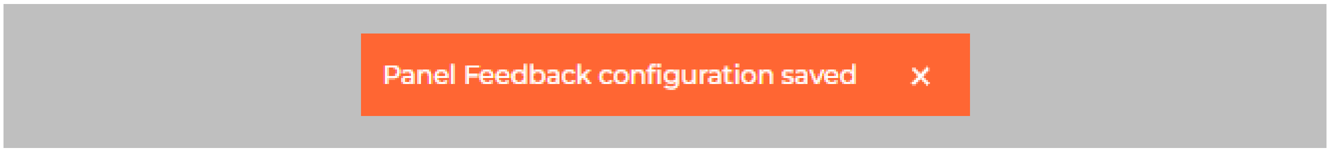
VISITOR

☐ Enable Panel Feedback

Figure 53: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.



Panel Feedback configuration saved

Figure 54: IXM WEB - Save Panel Feedback

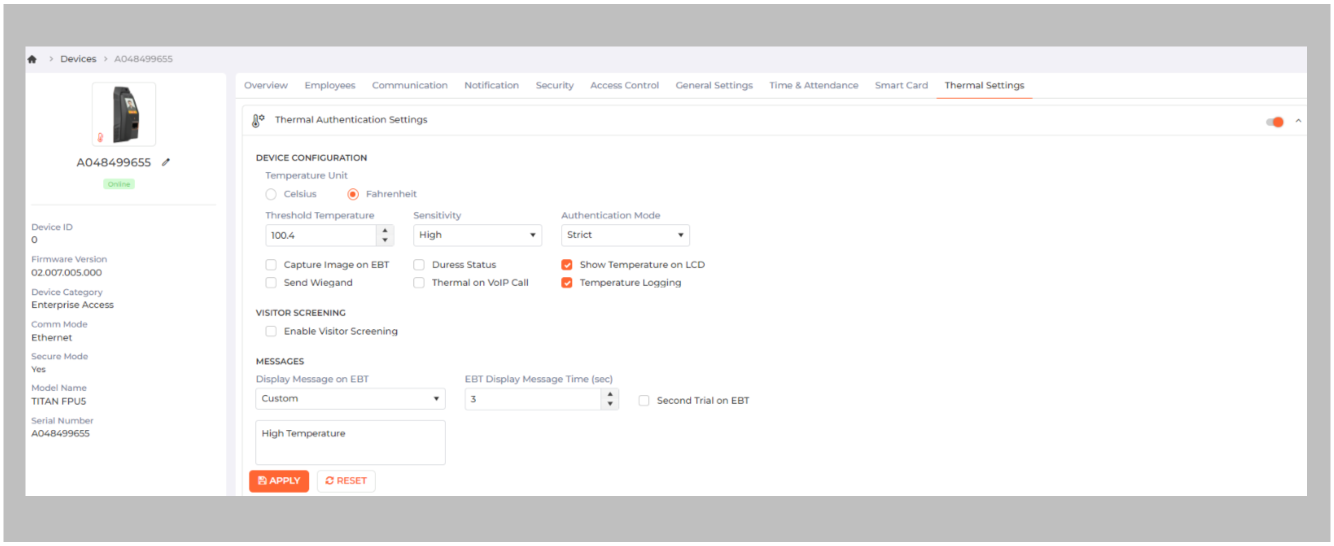
Configuring Thermal Settings

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.



A048499655

Device ID
0

Firmware Version
02.007.005.000

Device Category
Enterprise Access

Comm Mode
Ethernet

Secure Mode
Yes

Model Name
TITAN FPU5

Serial Number
A048499655

Thermal Authentication Settings

DEVICE CONFIGURATION

Temperature Unit
○ Celsius ● Fahrenheit

Threshold Temperature: 100.4
Sensitivity: High
Authentication Mode: Strict

□ Capture Image on EBT
□ Send Wiegand
□ Duress Status
□ Thermal on VoIP Call
☑ Show Temperature on LCD
☑ Temperature Logging

VISITOR SCREENING

□ Enable Visitor Screening

MESSAGES

Display Message on EBT: Custom
EBT Display Message Time (sec): 3
□ Second Trial on EBT

High Temperature

Figure 55: 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.

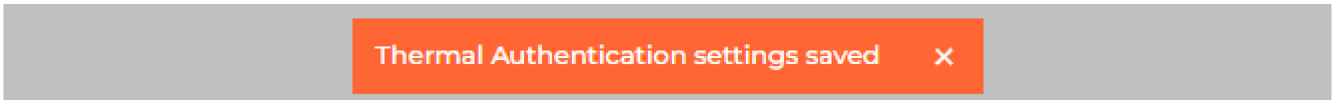
- **Visitor Message Display Time (sec):** Users can configure the length of time that the visitor screening message stays on the screen. The default time is 3 seconds.

- **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**.



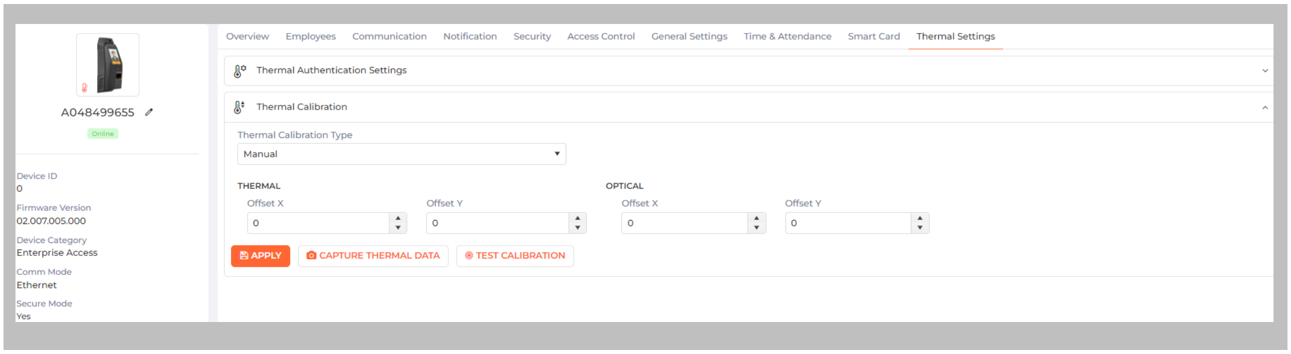
Thermal Authentication settings saved

Figure 56: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

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



A048499655

Device ID
0

Firmware Version
02.007.005.000

Device Category
Enterprise Access

Comm Mode
Ethernet

Secure Mode
Yes

Thermal Calibration Type: Manual

THERMAL
Offset X: 0
Offset Y: 0

OPTICAL
Offset X: 0
Offset Y: 0

Figure 57: 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.

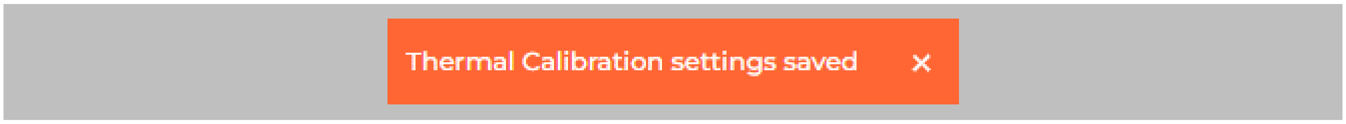
- **Offset Y (Thermal Section):** Users can set the value for the offset Y coordinate of the TIR camera.

- **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

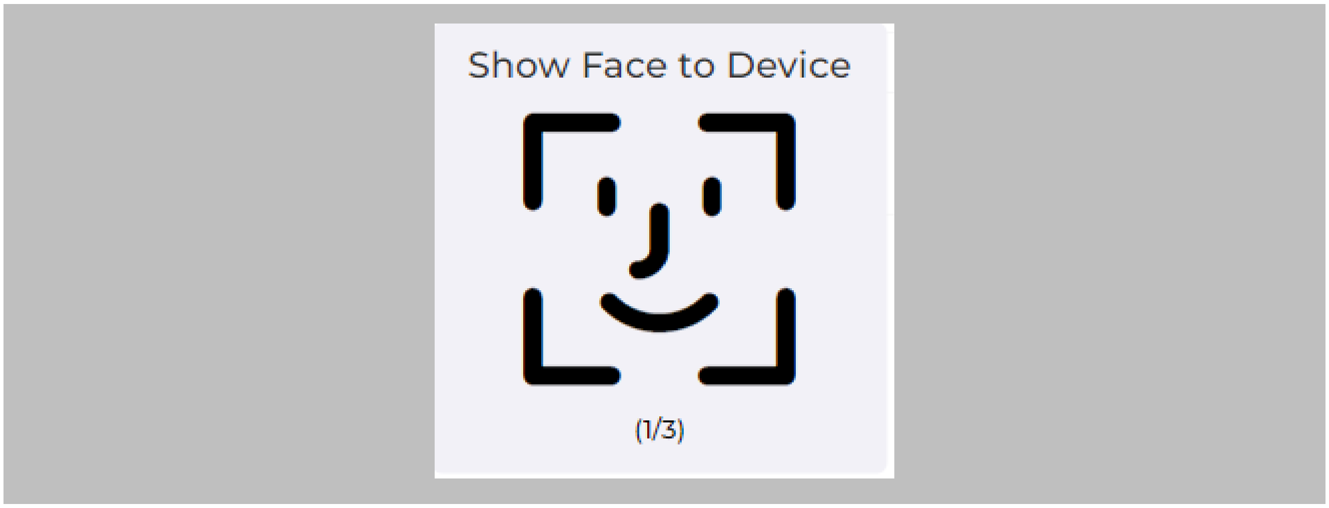
Once all the settings have been configured, click **Apply**, then click **OK**.



Thermal Calibration settings saved ×

Figure 58: 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.



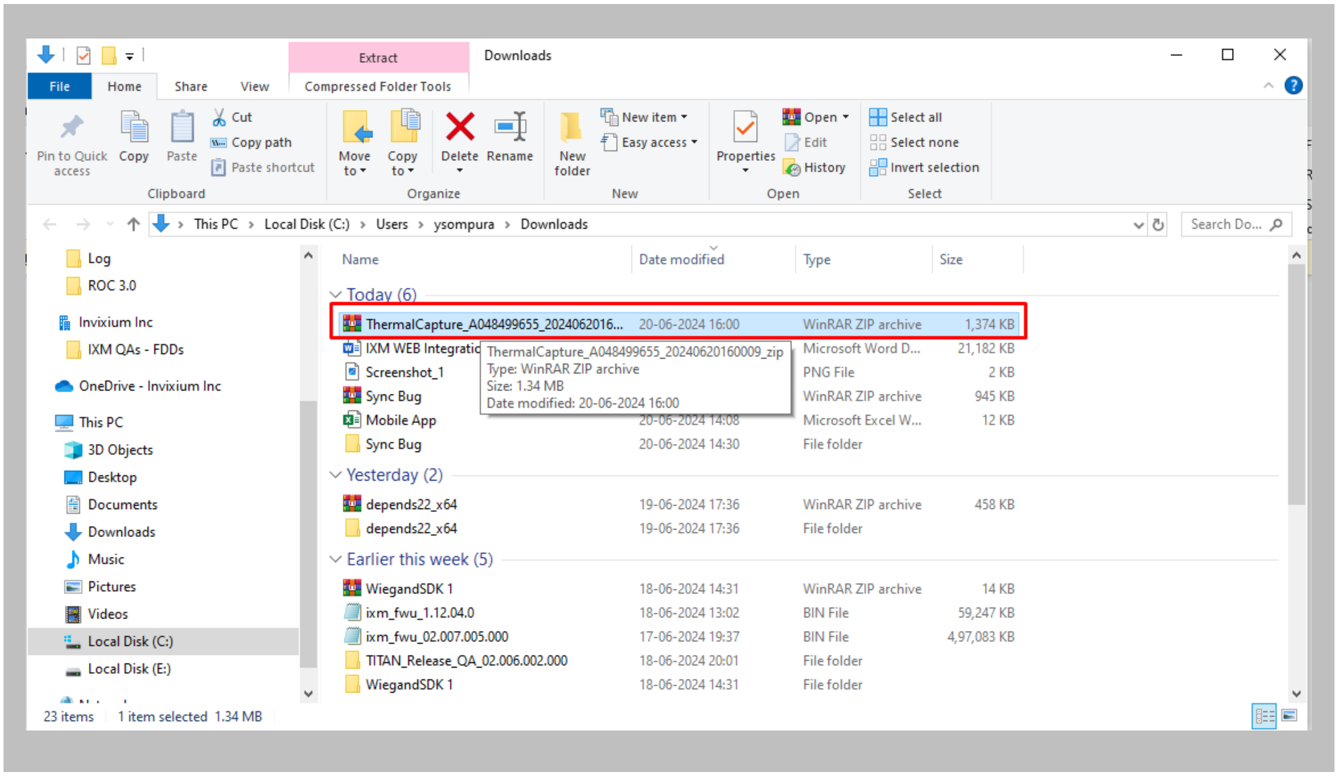
Show Face to Device

(1/3)

Figure 59: IXM WEB - Capture Thermal Data

STEP 4

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



Name	Date modified	Type	Size
Today (6)			
ThermalCapture_A048499655_2024062016...	20-06-2024 16:00	WinRAR ZIP archive	1,374 KB
IXM WEB Integratic		Microsoft Word D...	21,182 KB
Screenshot_1		PNG File	2 KB
Sync Bug		WinRAR ZIP archive	945 KB
Mobile App	20-06-2024 14:08	Microsoft Excel W...	12 KB
Sync Bug	20-06-2024 14:30	File folder	
Yesterday (2)			
depends22_x64	19-06-2024 17:36	WinRAR ZIP archive	458 KB
depends22_x64	19-06-2024 17:36	File folder	
Earlier this week (5)			
WiegandSDK 1	18-06-2024 14:31	WinRAR ZIP archive	14 KB
ixm_fwu_1.12.04.0	18-06-2024 13:02	BIN File	59,247 KB
ixm_fwu_02.007.005.000	17-06-2024 19:37	BIN File	4,97,083 KB
TITAN_Release_QA_02.006.002.000	18-06-2024 20:01	File folder	
WiegandSDK 1	18-06-2024 14:31	File folder	

ThermalCapture_A048499655_20240620160009_zip
Type: WinRAR ZIP archive
Size: 1.34 MB
Date modified: 20-06-2024 16:00

Figure 60: 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**.

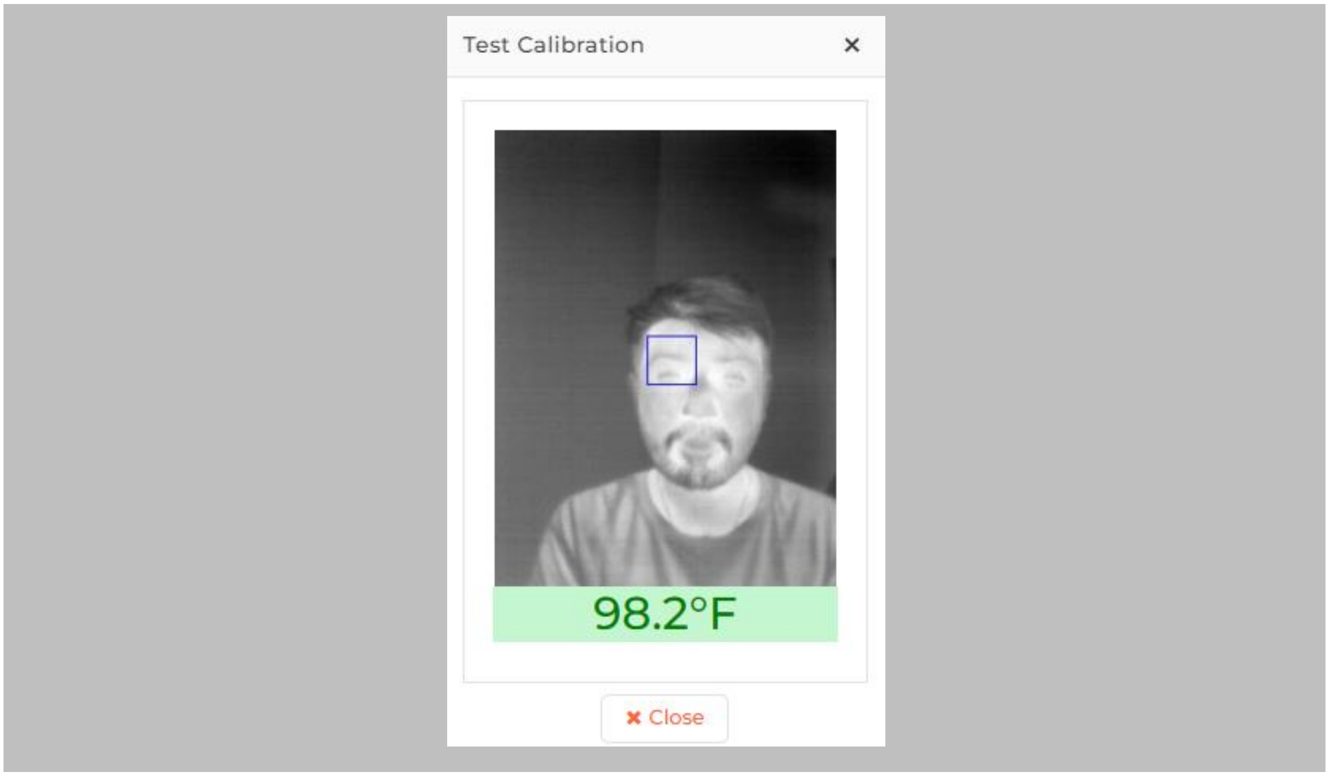


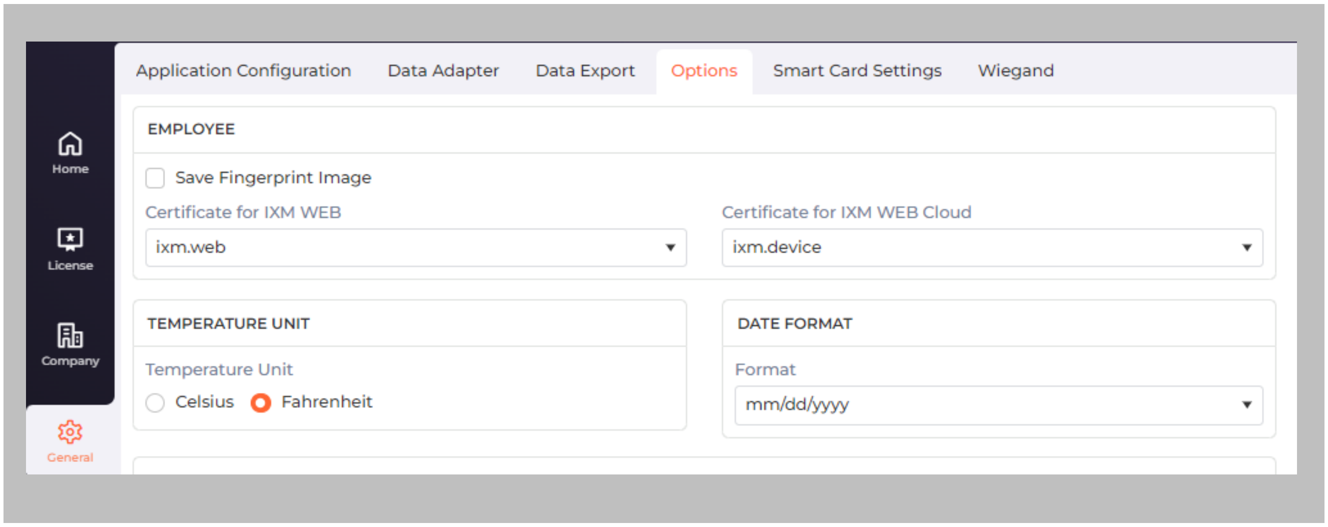
Figure 61: IXM WEB - Test Thermal Calibration

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

Change Temperature Unit Settings

STEP 1

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



EMPLOYEE

□ Save Fingerprint Image

Certificate for IXM WEB: ixm.web

Certificate for IXM WEB Cloud: ixm.device

TEMPERATURE UNIT

Temperature Unit: ○ Celsius ● Fahrenheit

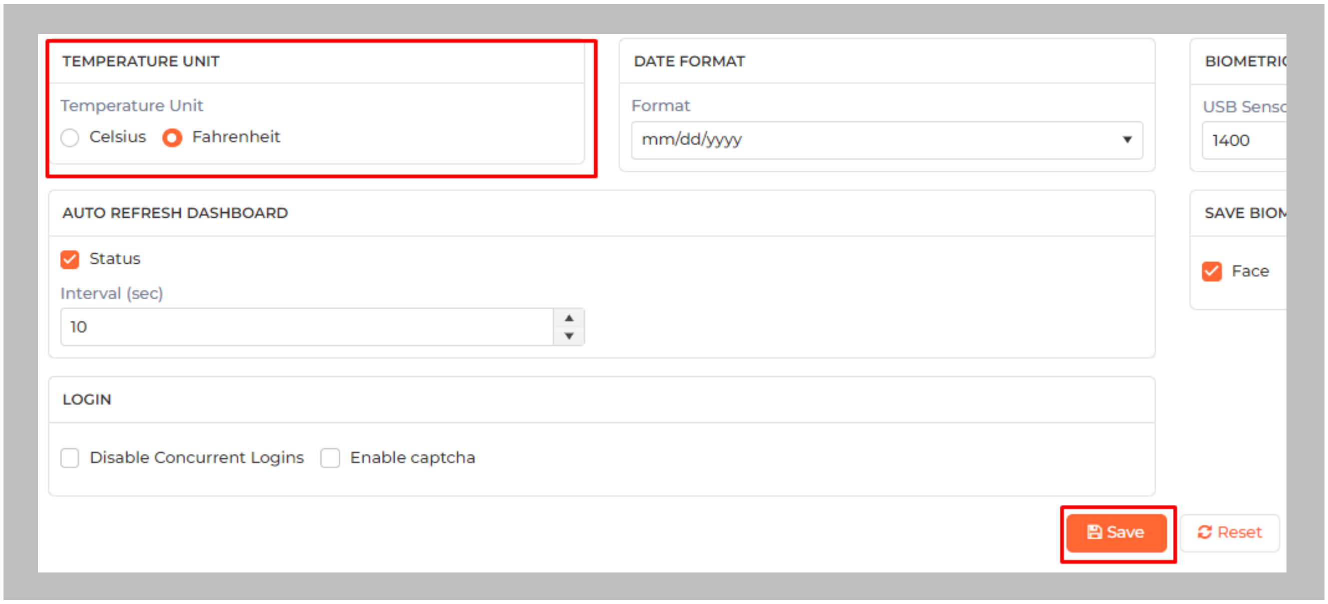
DATE FORMAT

Format: mm/dd/yyyy

Figure 62: IXM WEB - Option to Change Temperature Unit

STEP 2

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



TEMPERATURE UNIT

Temperature Unit

○ Celsius ● Fahrenheit

DATE FORMAT

Format

mm/dd/yyyy

BIOMETRIC

USB Senso

1400

AUTO REFRESH DASHBOARD

☑ Status

Interval (sec)

10

SAVE BIOM

☑ Face

LOGIN

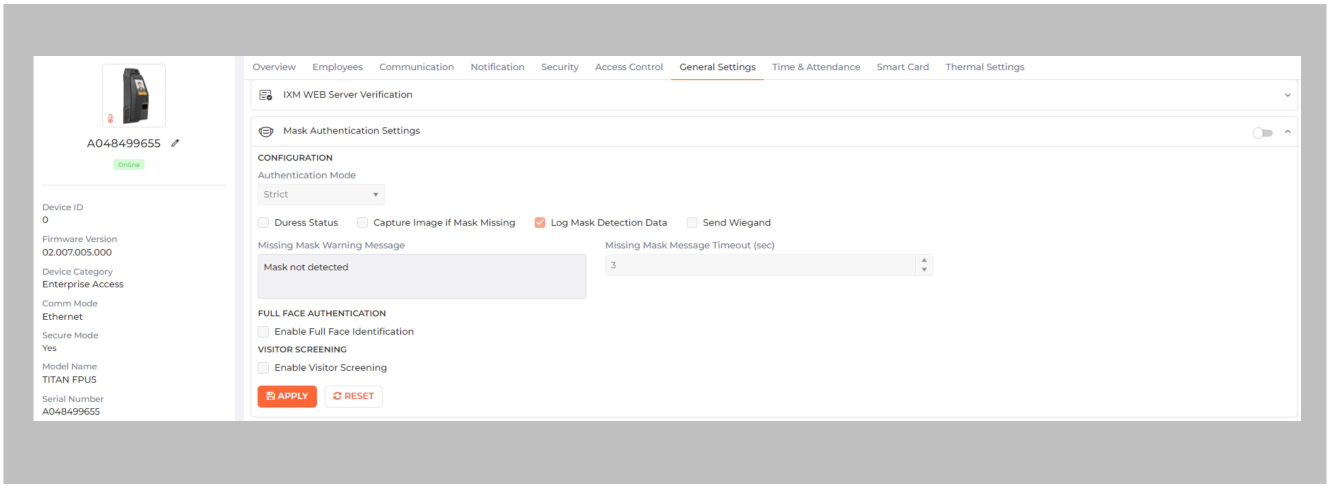
□ Disable Concurrent Logins □ Enable captcha

Figure 63: 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.



A048499655

Device ID
0

Firmware Version
02.007.005.000

Device Category
Enterprise Access

Comm Mode
Ethernet

Secure Mode
Yes

Model Name
TITAN FPU5

Serial Number
A048499655

Mask Authentication Settings

CONFIGURATION

Authentication Mode: Strict

□ Duress Status □ Capture Image if Mask Missing ☑ Log Mask Detection Data □ Send Wiegand

Missing Mask Warning Message: Mask not detected

Missing Mask Message Timeout (sec): 3

FULL FACE AUTHENTICATION

□ Enable Full Face Identification

VISITOR SCREENING

□ Enable Visitor Screening

Figure 64: 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**.

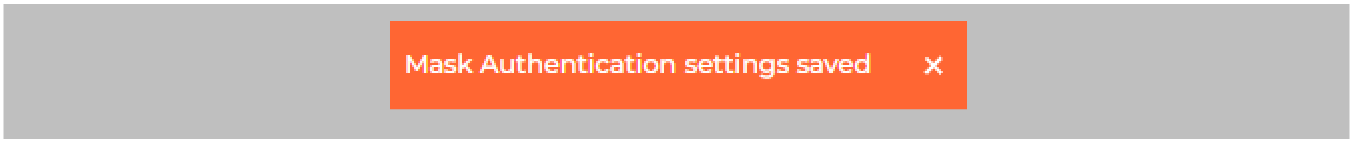
- **Visitor Screening Message:** Set a message that will be displayed when a visitor is showing their face. Messages can be up to 50 characters.

- **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**.



Mask Authentication settings saved ×

Figure 65: IXM WEB - Save Mask Settings

15. Enrollment using Genetec Config Tool

Procedure

STEP 1

Ensure that IXM WEB Add-On has been installed on the same path as that of Genetec server.

Refer *Installing IXM WEB Add-On* section.

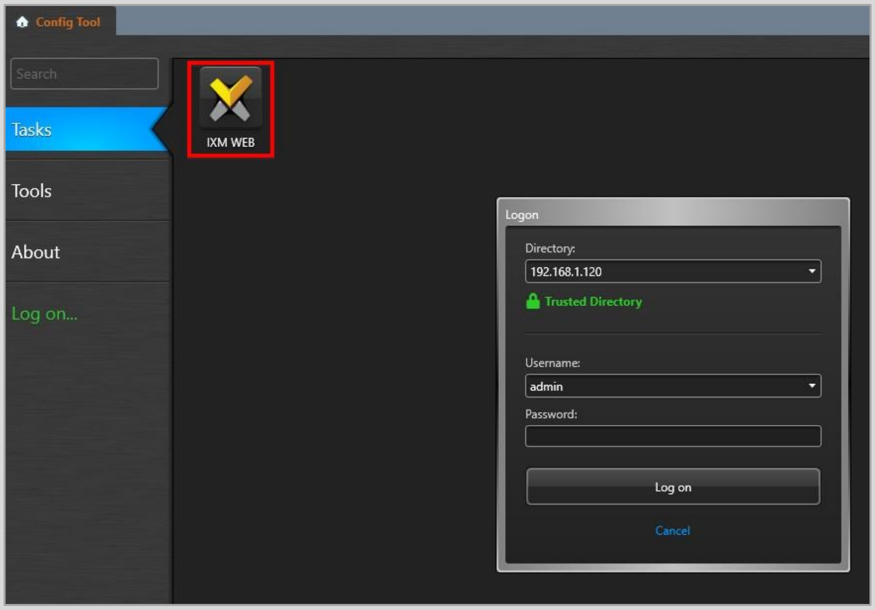
Note: Enrollment can be done using Config Tool as well as Security Desk.

STEP 2

Restart the Config Tool once installation of IXM WEB Add-On is complete. You will see the icon of IXM WEB.

STEP 3

Click **IXM WEB** and Log into Config Tool using valid credentials.



Logon

Directory: 192.168.1.120

Trusted Directory

Username: admin

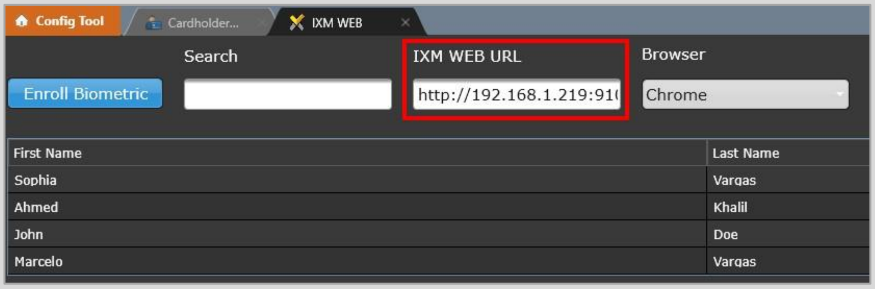
Password:

Figure 66: IXM WEB – Config Tool Logon

STEP 4

Note: IXM WEB opens in a new window with a list of Genetec Cardholders.

Enter **IXM WEB URL**. Select the **Browser**.



Search:

IXM WEB URL: http://192.168.1.219:91(

Browser: Chrome

First Name	Last Name
Sophia	Vargas
Ahmed	Khalil
John	Doe
Marcelo	Vargas

Figure 67: IXM WEB – Configure IXM WEB URL

Note:

The recommended browser is Chrome.

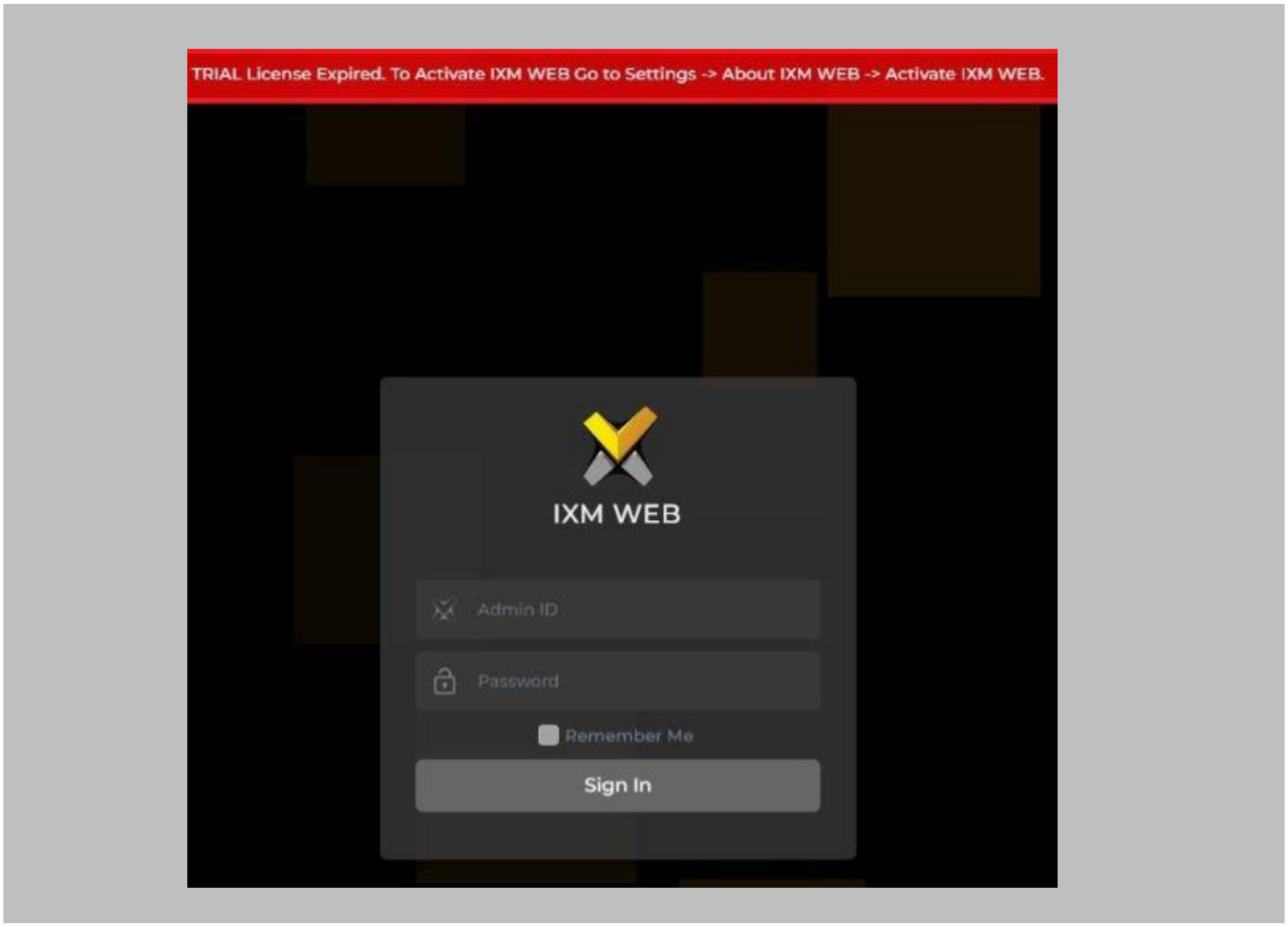
STEP 5

Select the desired Cardholder from the list. Click **Enroll Biometric**.

STEP 6

Enter credentials to log in to IXM WEB. Toggle “Remember Me” to stay signed in.

Note: Log in to IXM WEB is required only once when you launch the enrollment viewer for the first time. For subsequent enrollment, this step will be skipped as you are already signed in.



TRIAL License Expired. To Activate IXM WEB Go to Settings -> About IXM WEB -> Activate IXM WEB.

Figure 68: IXM WEB – First Time Log In

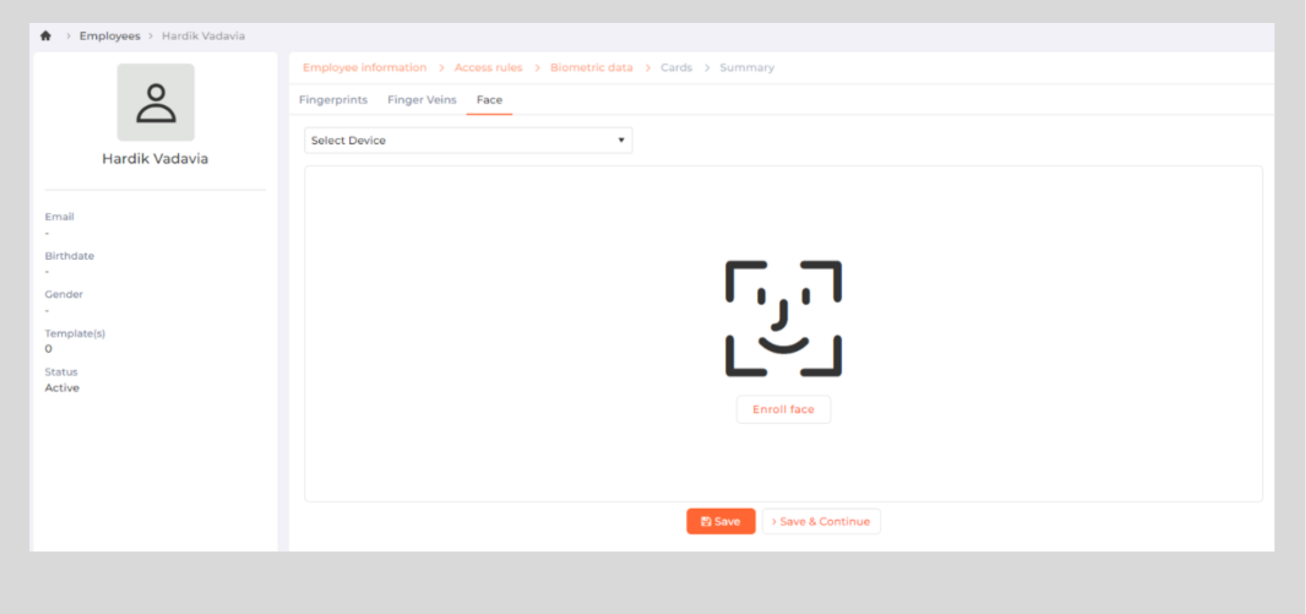
Once you are logged in, repeat STEP 5.

STEP 7

Perform Fingerprint and Face Enrollment.

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

Refer *Enrollment Best Practices* section.


Employees > Hardik Vadavia
Employee information > Access rules > Biometric data > Cards > Summary
Fingerprints
Finger Veins
Face
Select Device
Enroll face
Save
› Save & Continue

Hardik Vadavia

Email
-

Birthdate
-

Gender
-

Template(s)
0

Status
Active

Figure 69: IXM WEB – Enrollment Viewer

16. 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.

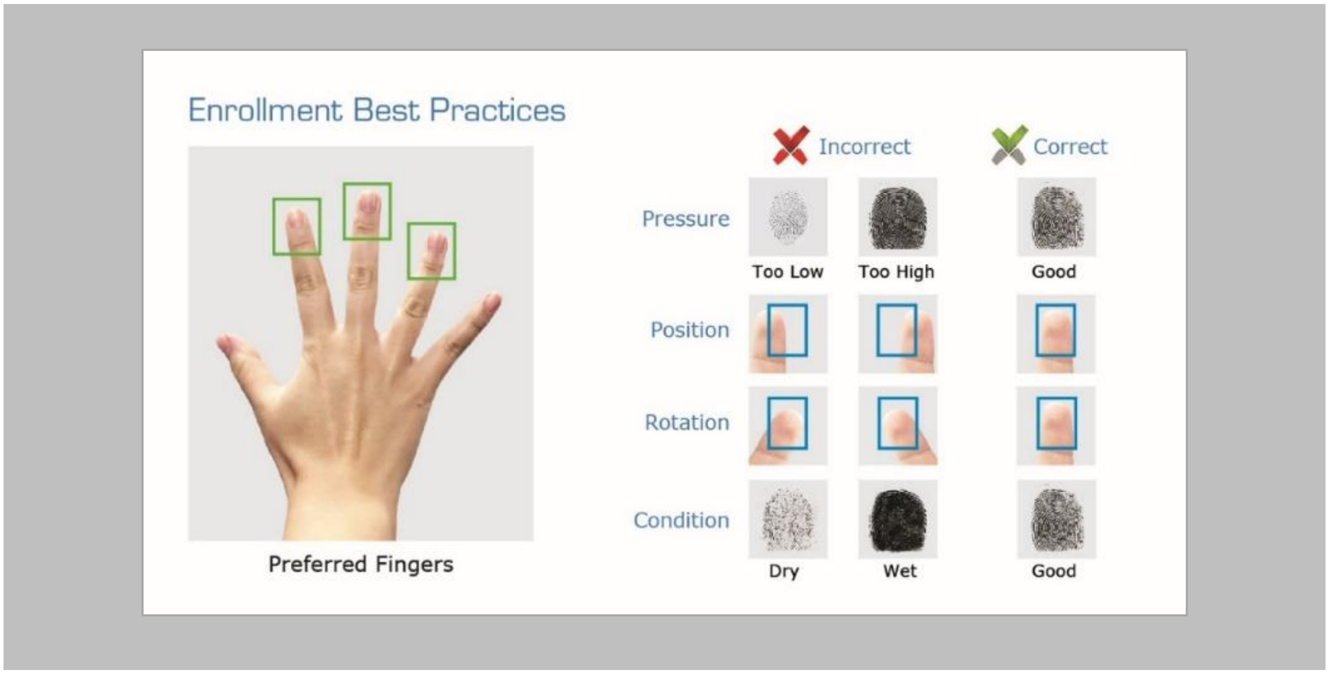


Figure 70: Fingerprint Enrollment Best Practices

Fingerprint Image Samples

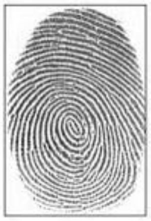
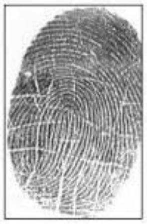
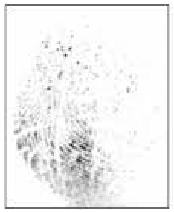
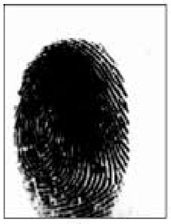
Fingerprint Sample	Result	Recommendation
	Good Fingerprint	Always try and get a good fingerprint like this for a good enrollment score
	Fingerprint with cuts	Invixium recommends using Card + Biometrics or Card + PIN
	Dry finger	Moisten finger and re-enroll for better results
	Wet/Sweaty finger	Rub finger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

Figure 71: 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.

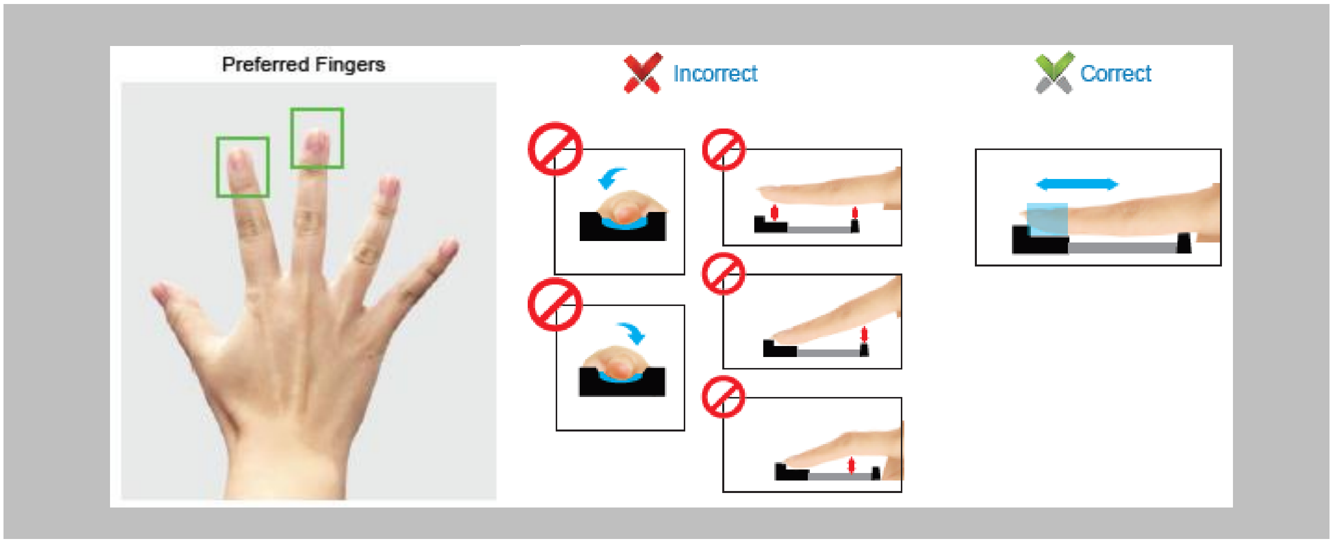


Figure 72: Finger Vein Enrollment Best Practices

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.

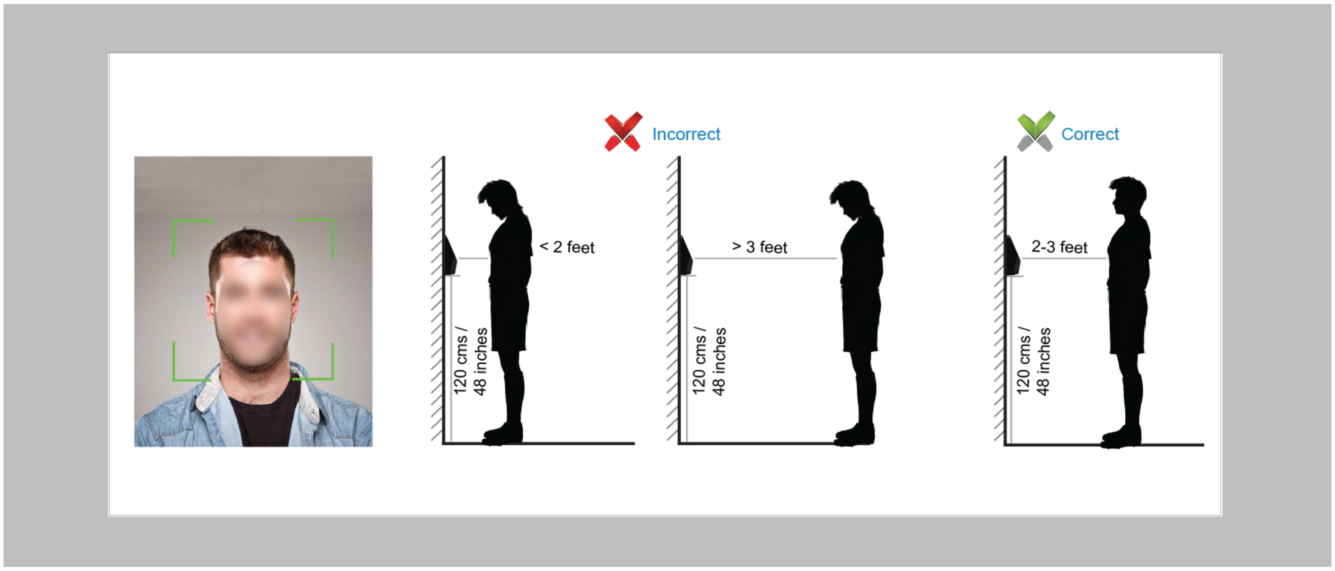


Figure 73: Face Enrollment Best Practices

17. Configuring RIO Settings

Configuring RIO in Config Tool of GSC

Procedure

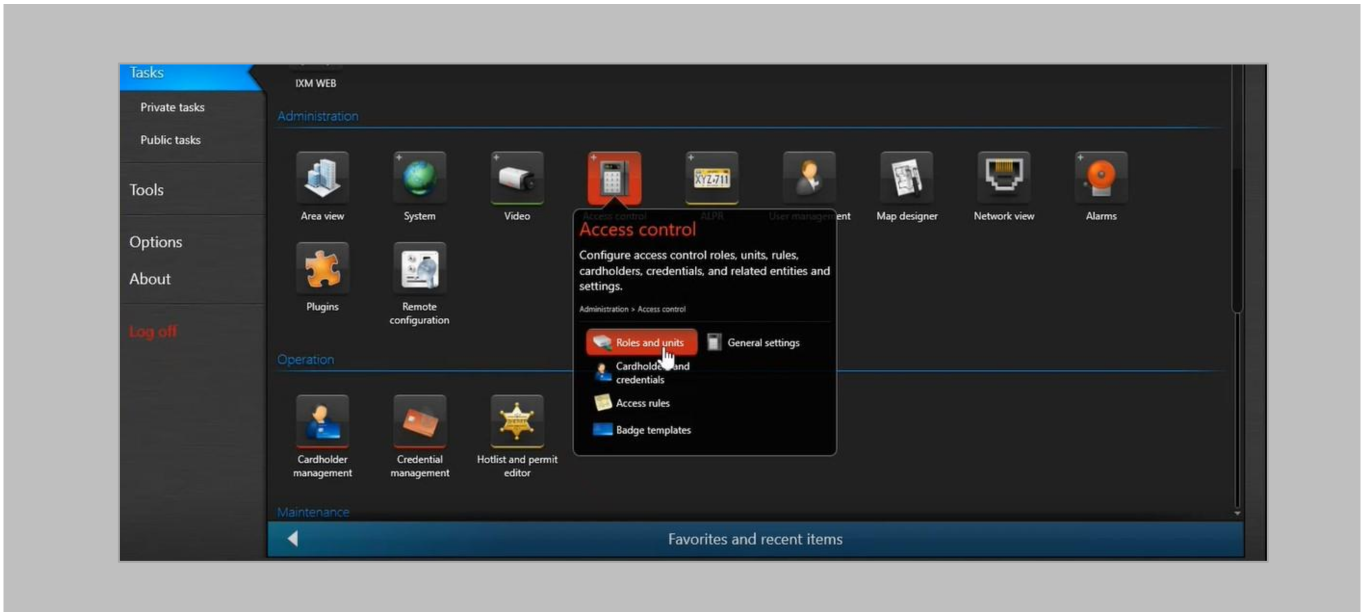
STEP 1

Log into Config Tool using valid credentials.

STEP 2

Creating Roles and Units.

Navigate to **Access Control** → **Roles and Units**



Access control

Configure access control roles, units, rules, cardholders, credentials, and related entities and settings.

Figure 74: Config Tool – Access Control

STEP 3

Create Access Manager.

Right click on server name → Click on **Add an entity** → Click on **Show all** → Click on **Access Manager**

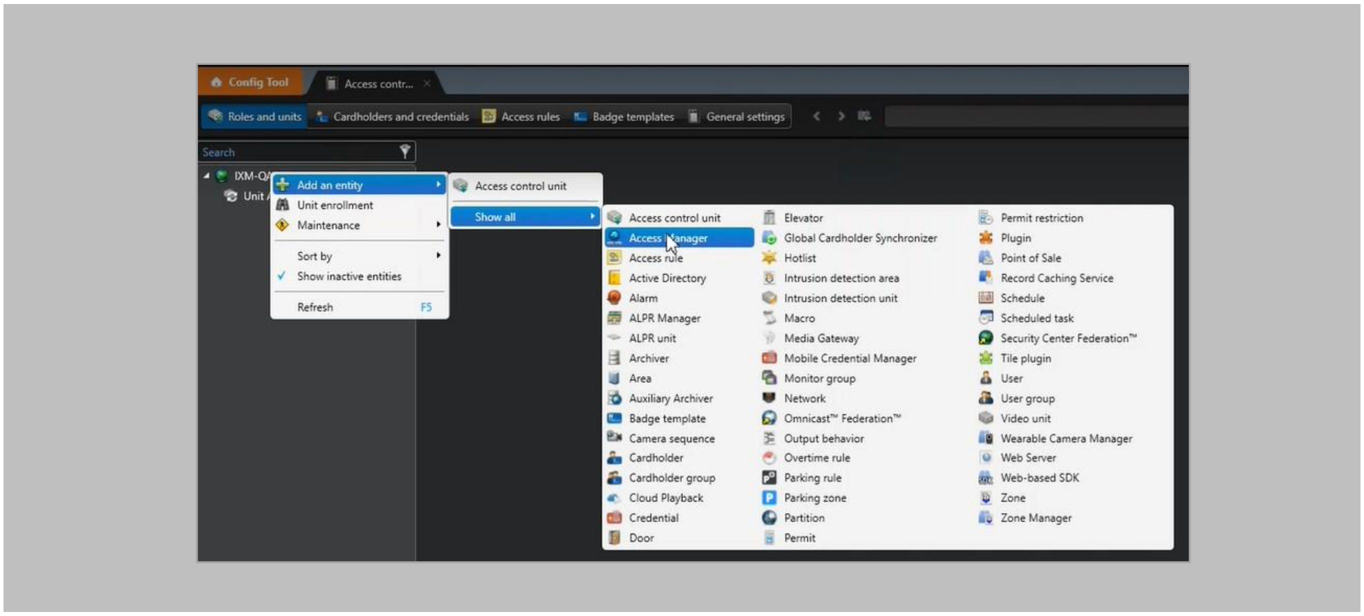
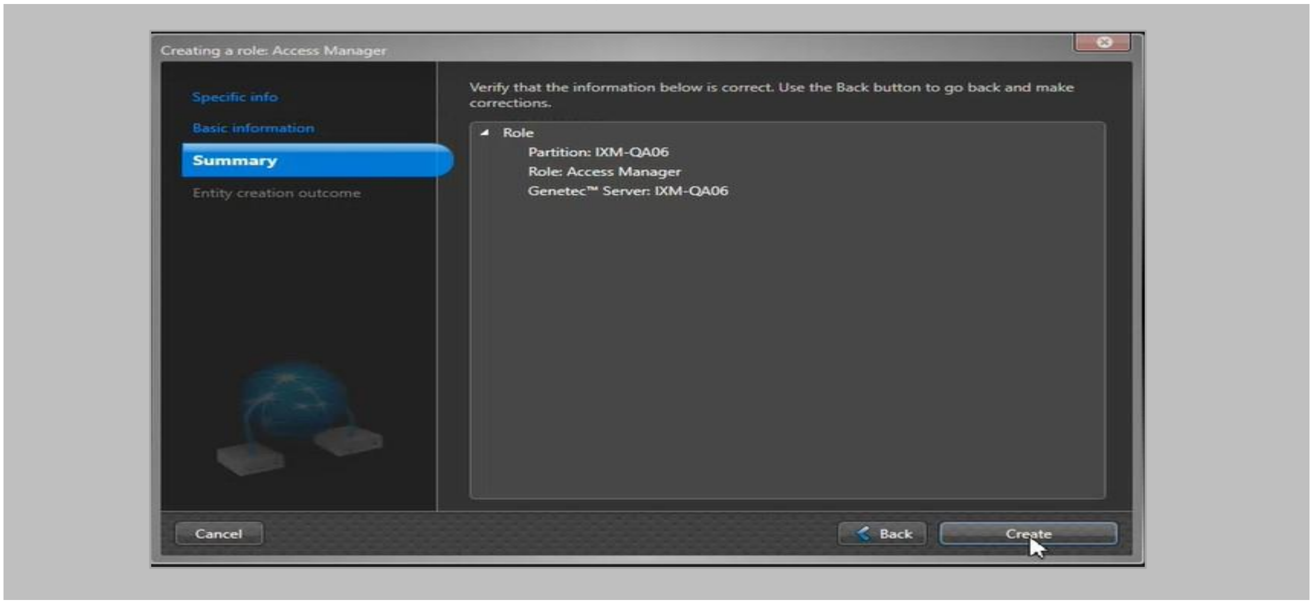


Figure 75: Config Tool – Access Manager

STEP 4

Enter required details to create **Access Manager** → click **Create.**



Creating a role: Access Manager

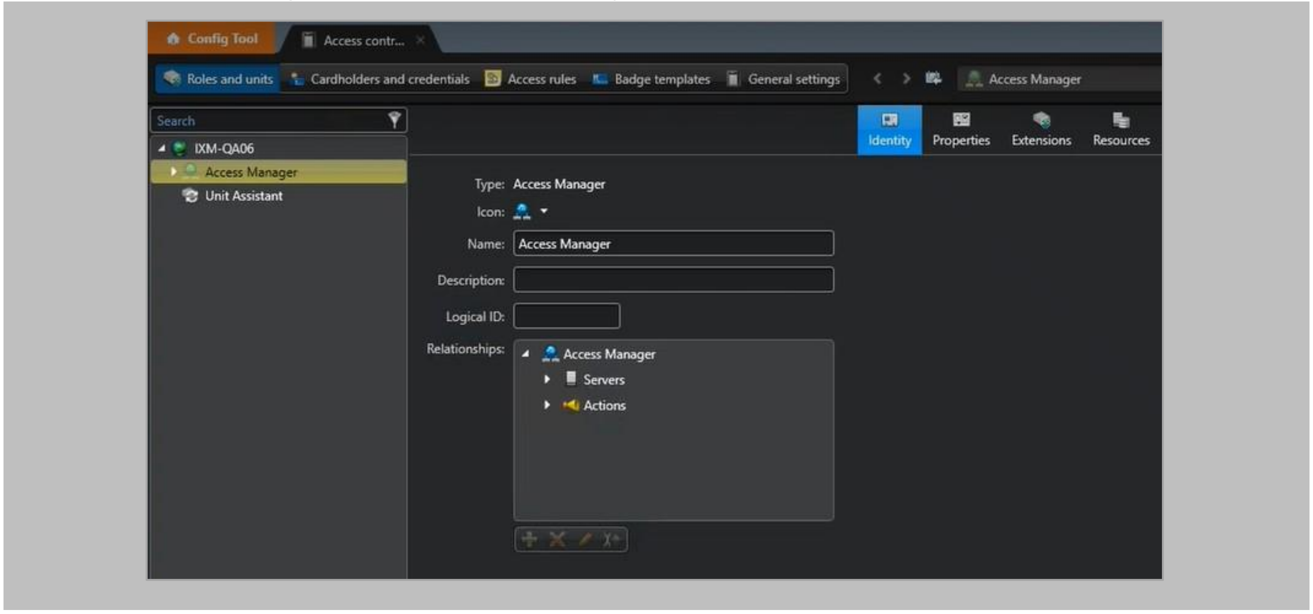
Verify that the information below is correct. Use the Back button to go back and make corrections.

- Role
  - Partition: IXM-QA06
  - Role: Access Manager
  - Genetec™ Server: IXM-QA06

Figure 76: Config Tool – Add Access Manager

STEP 5

Validate Access Manager is created successfully.



Type: Access Manager

Icon:

Name: Access Manager

Description:

Logical ID:

Relationships:

- Access Manager
  - Servers
  - Actions

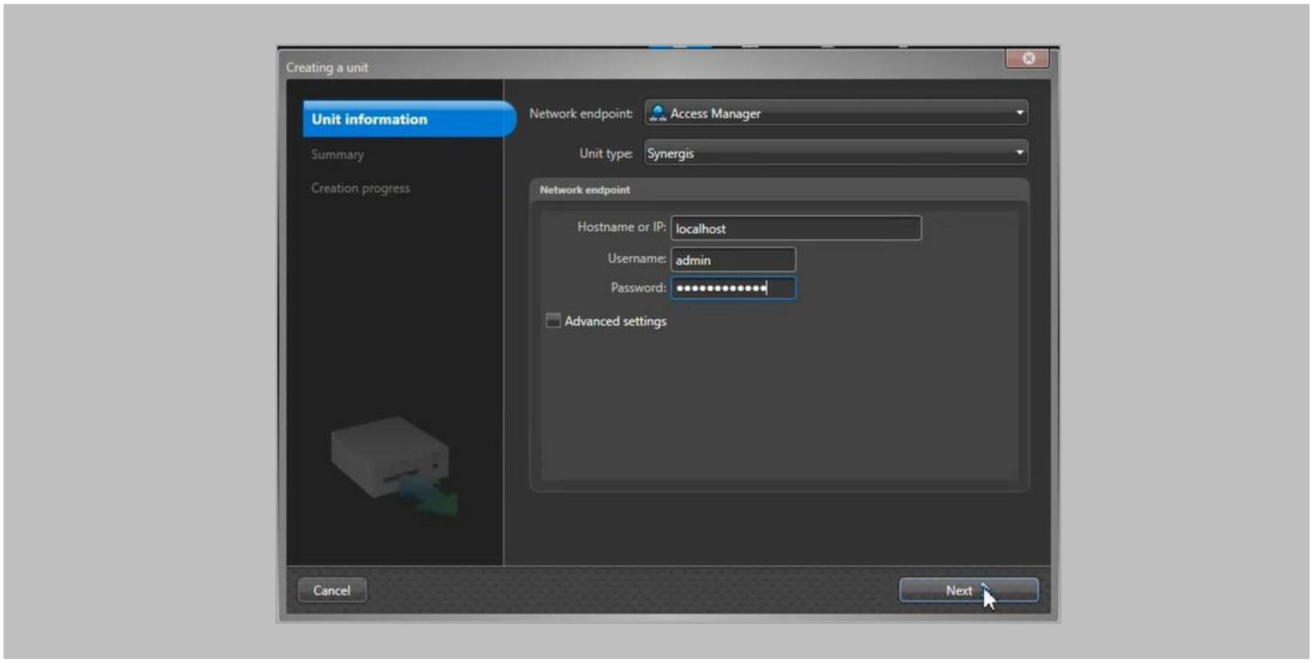
Figure 77: Config Tool – Access Manager created

Note: You need to wait till the Access Manager becomes online.

STEP 6

Create Access Control Unit.

Righ click on the **Access Manager** → **Add an entity** → **Access Control Unit**



Network endpoint: Access Manager

Unit type: Synergis

Network endpoint

Hostname or IP: localhost

Username: admin

Password: ••••••••••••

□ Advanced settings

Figure 78: Config Tool – Add Access Control Unit

Hostname or IP

Enter the value of Hostname or IP. For example: “localhost”.

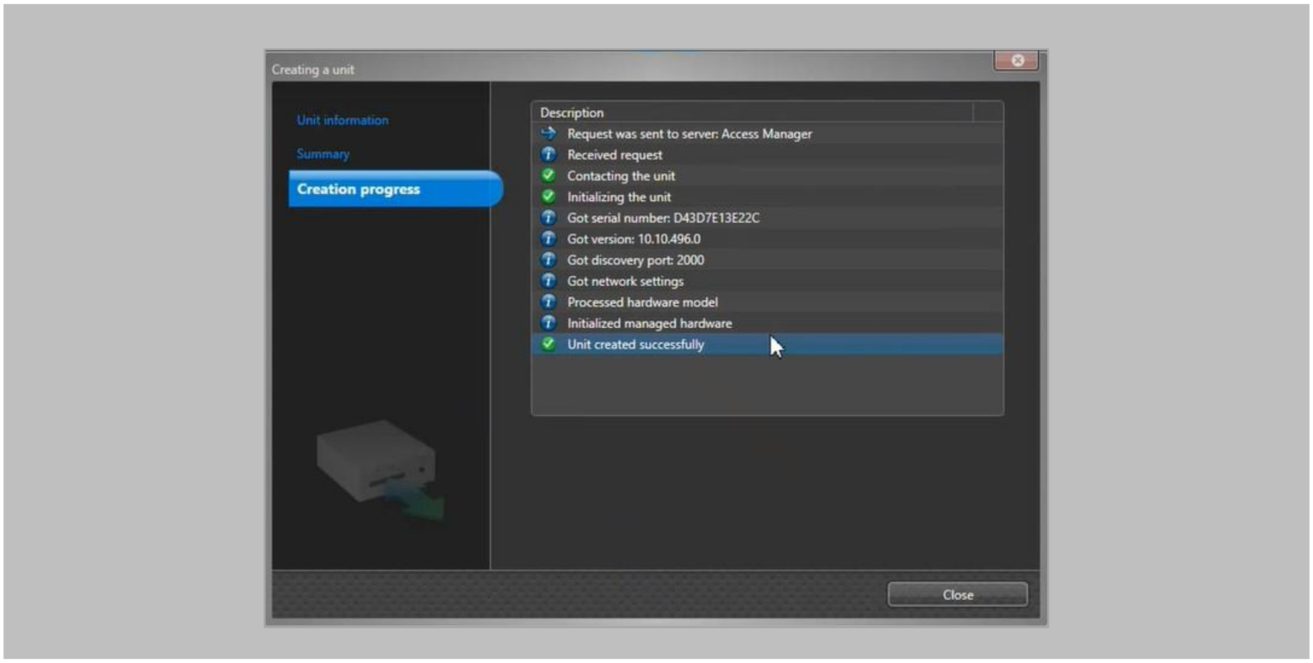
Username

Enter authorized User name to access Genetec server.

Password

Enter Password of authorized User to access Genetec server.

Click **Next** and **Create.**



Description
- Request was sent to server: Access Manager
- Received request
- Contacting the unit
- Initializing the unit
- Got serial number: D43D7E13E22C
- Got version: 10.10.496.0
- Got discovery port: 2000
- Got network settings
- Processed hardware model
- Initialized managed hardware
- Unit created successfully

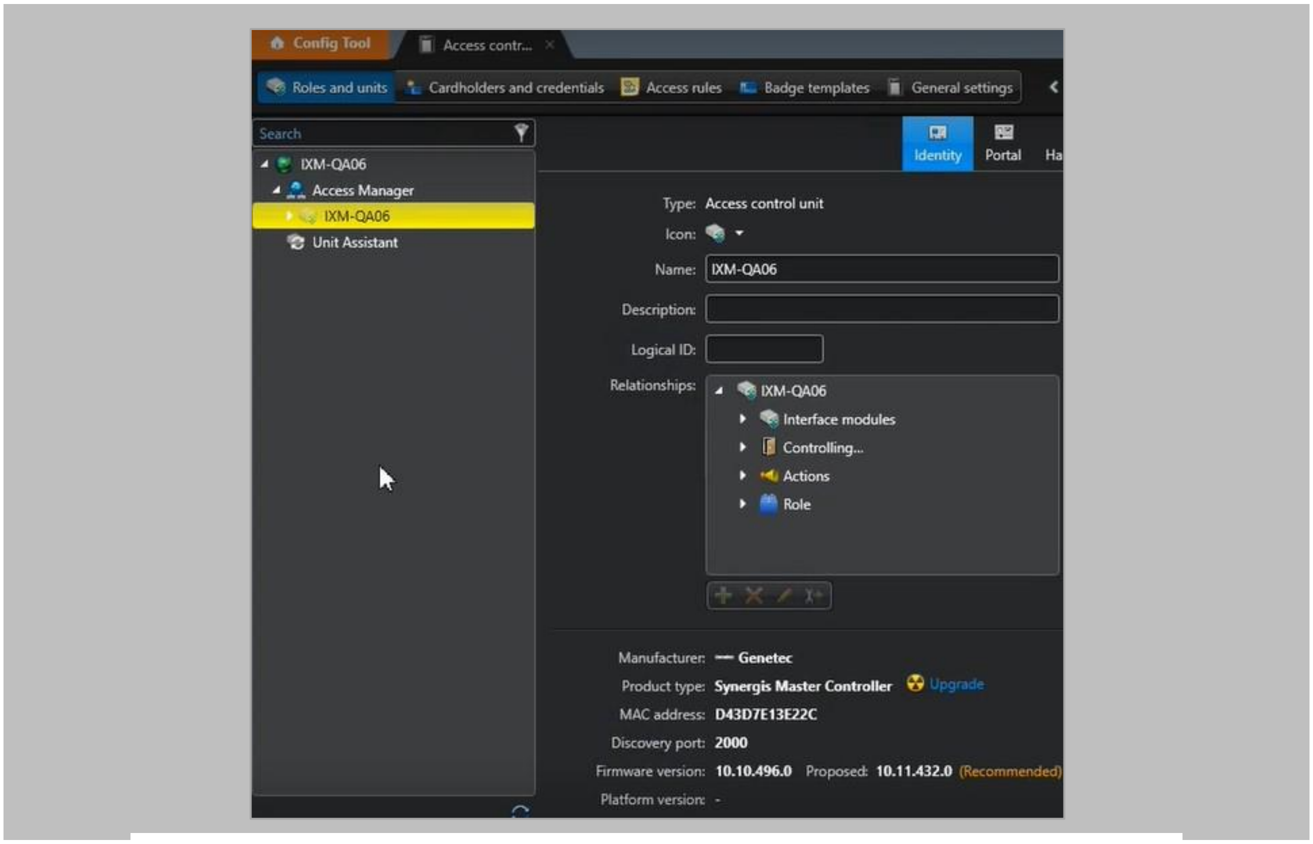
. Figure 79: Config Tool – Creating Access Control Unit

Note: Description should show “Unit created successfully”.

Click **Close**.

STEP 7

Validate Access Control Unit is added successfully.



Type: Access control unit

Icon:

Name: IXM-QA06

Description:

Logical ID:

Relationships: IXM-QA06

Manufacturer: Genetec

Product type: Synergis Master Controller

MAC address: D43D7E13E22C

Discovery port: 2000

Firmware version: 10.10.496.0 Proposed: 10.11.432.0 (Recommended)

Platform version: -

Figure 80: Config Tool – Access Control Unit created

Configuring RIO in IXM WEB

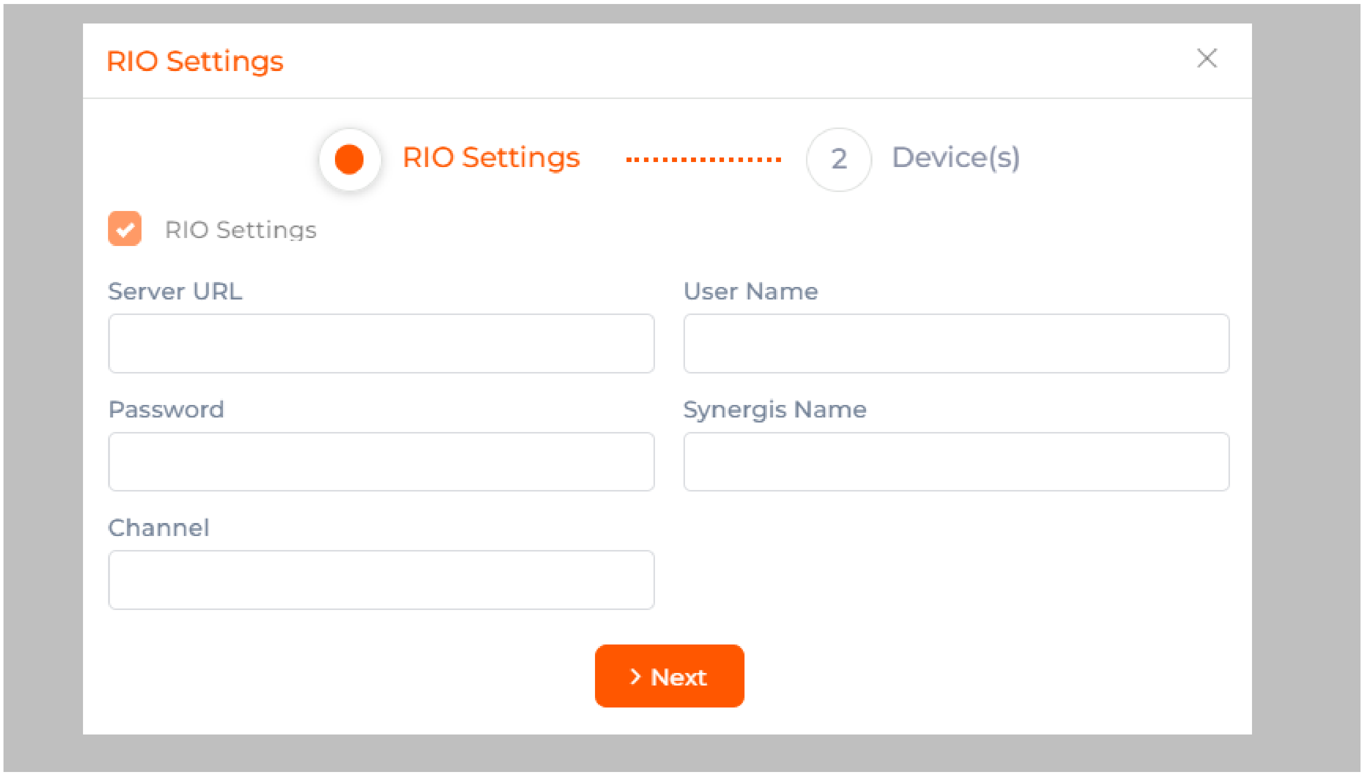
Procedure

STEP 1

Log into IXM WEB → Navigate to **Link** → click the blue **Security Center (Genetec)** icon.

STEP 2

Scroll down page to **RIO SETTINGS** → Click **Add New** button.



☑ RIO Settings

Server URL

User Name

Password

Synergis Name

Channel

Figure 81: IXM WEB – RIO Settings

RIO Setting

Click on the check box to enable wireless connection to the Control Panel.

Server URL:

Enter Address of Synergis appliance.

User Name:

Enter User name to access Synergis appliance.

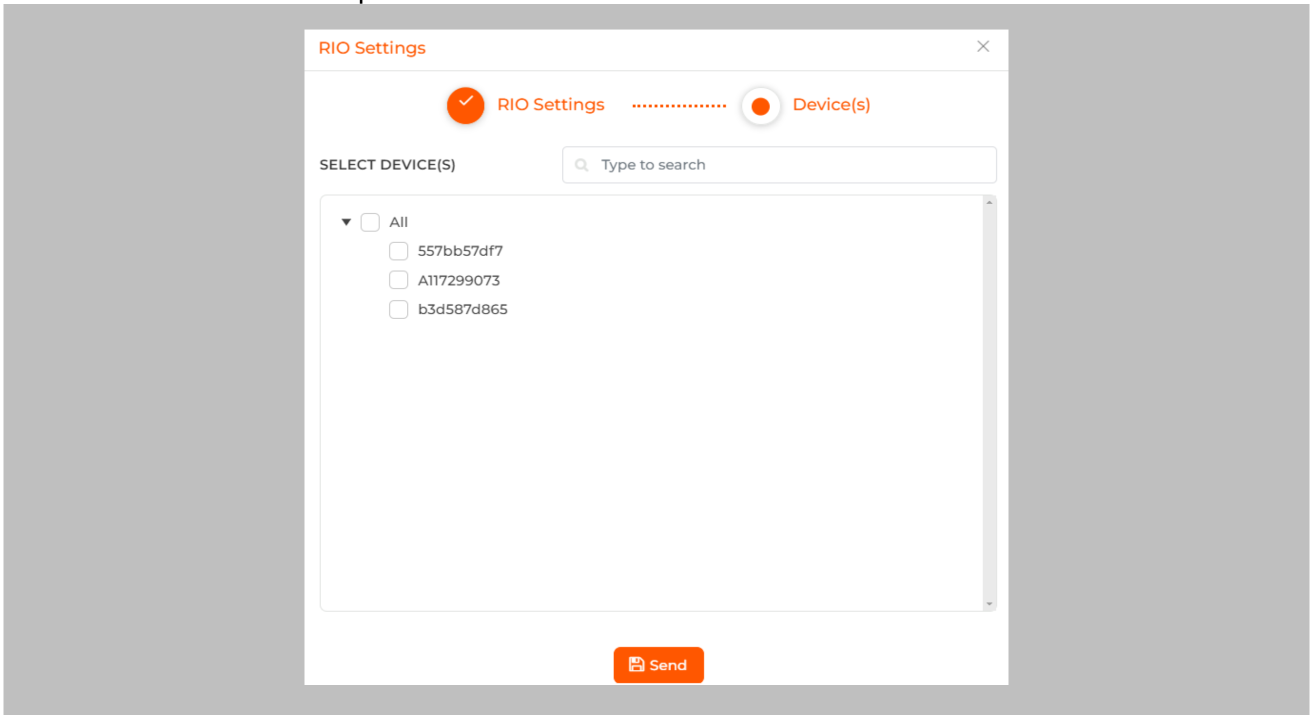
Password:

Enter Password to access Synergis appliance.

Synergis Name:

Enter Synergis Name to separate Synergis appliances for setups with multiple appliances.

Devices selected in the next step would be added to this channel on the Synergis appliance. A new channel will be created if required.



□ All
□ 557bb57df7
□ A117299073
□ b3d587d865

Figure 82: IXM WEB – Channel

Click on target sevices to select.

Click **Send.**

Note: Clicking **Send** will add each selected Invixium device as an interface on the Synergis appliance. The device name will be the name of the interface. Each interface will be given an input label, “**REX**”, an output label, “**Lock**”, and a reader label, “**Reader**”.

Configuring Invixium Device and Door in Config Tool

STEP 1

Go to Config Tool.

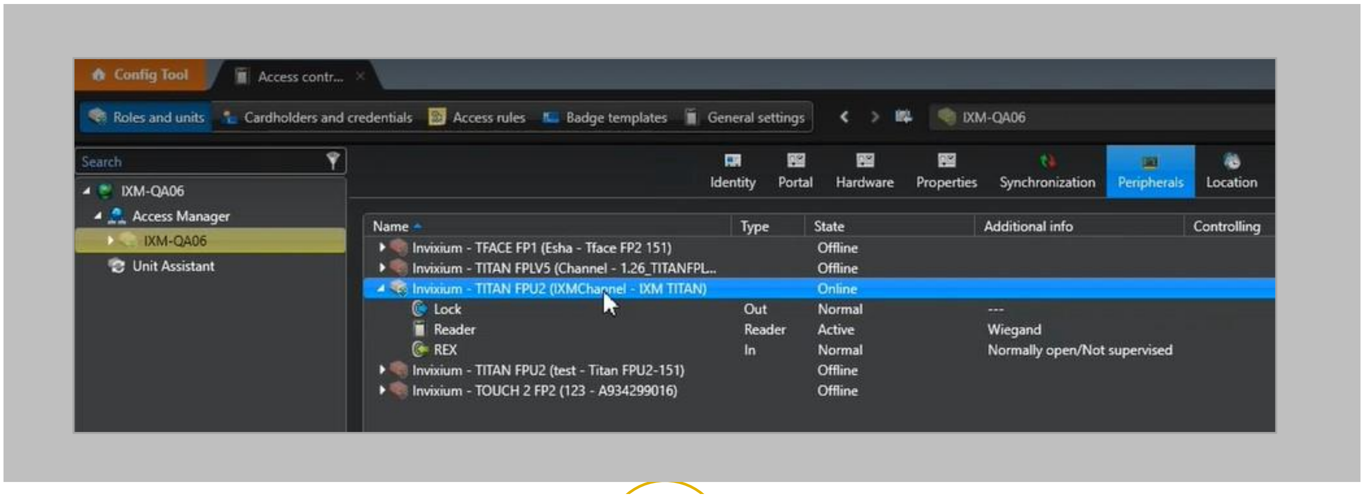
STEP 2

Navigate to **Access Manager** → Click on the created **Access Control Unit** → Click on **Peripherals** tab.

You should be able to see the name of Invixium device in the format:

Invixium – Product Type (Channel name – Invixium device name)

The State of the device should be "Online".



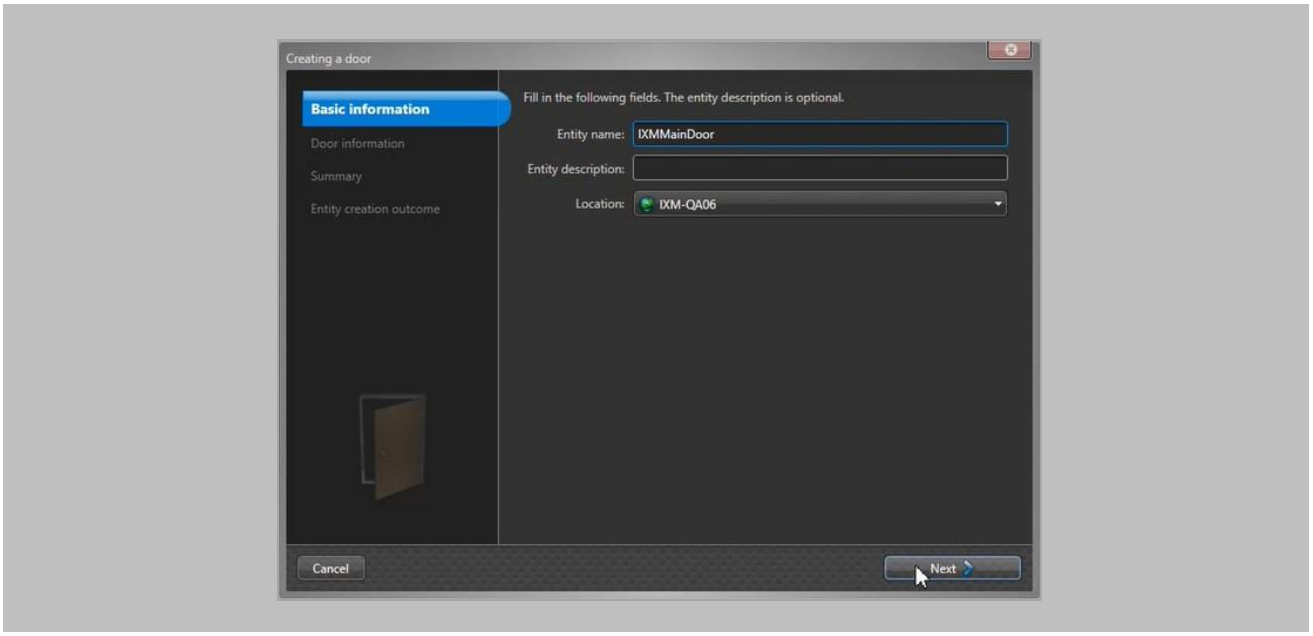
Name	Type	State	Additional info	Controlling
Invixium - TFACE FP1 (Esha - Tface FP2 151)		Offline		
Invixium - TITAN FPLV5 (Channel - 1.26_TITANFPL...		Offline		
Invixium - TITAN FPU2 (IXMChannel - IXM TITAN)		Online		
Lock	Out	Normal	---	
Reader	Reader	Active	Wiegand	
REX	In	Normal	Normally open/Not supervised	
Invixium - TITAN FPU2 (test - Titan FPU2-151)		Offline		
Invixium - TOUCH 2 FP2 (123 - A934299016)		Offline		

Figure 83: Config Tool – Peripherals

STEP 3

Create an Area or Door.

Navigate to **Area View** → Right Click on the **Server Name** → Click on **Add an entity** → Click on **Door**



Fill in the following fields. The entity description is optional.

Entity name: IXMMainDoor

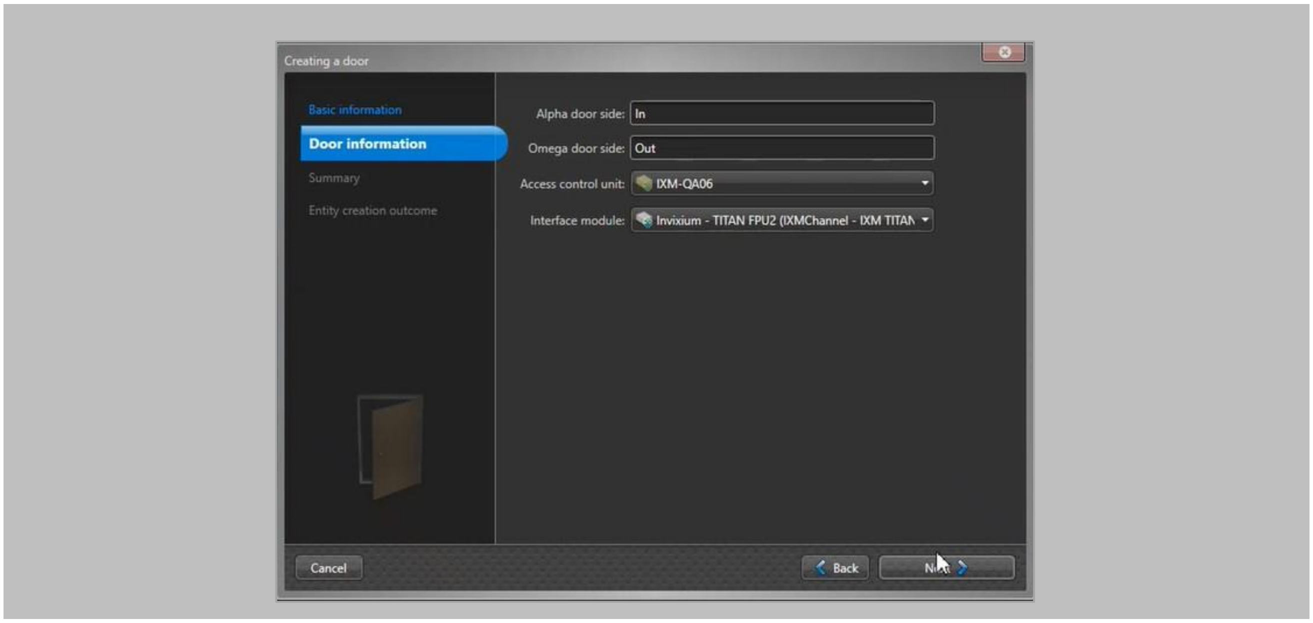
Entity description:

Location: IXM-QA06

Figure 84: Config Tool – Creating a Door

Entity name

Enter name of the Door. Click **Next**.



Alpha door side: In

Omega door side: Out

Access control unit: IXM-QA06

Interface module: Invixium - TITAN FPU2 (IXMChannel - IXM TITAN

Figure 85: Config Tool – Door Information

Access control unit

Click to select the Access control unit you created from the list.

Interface module

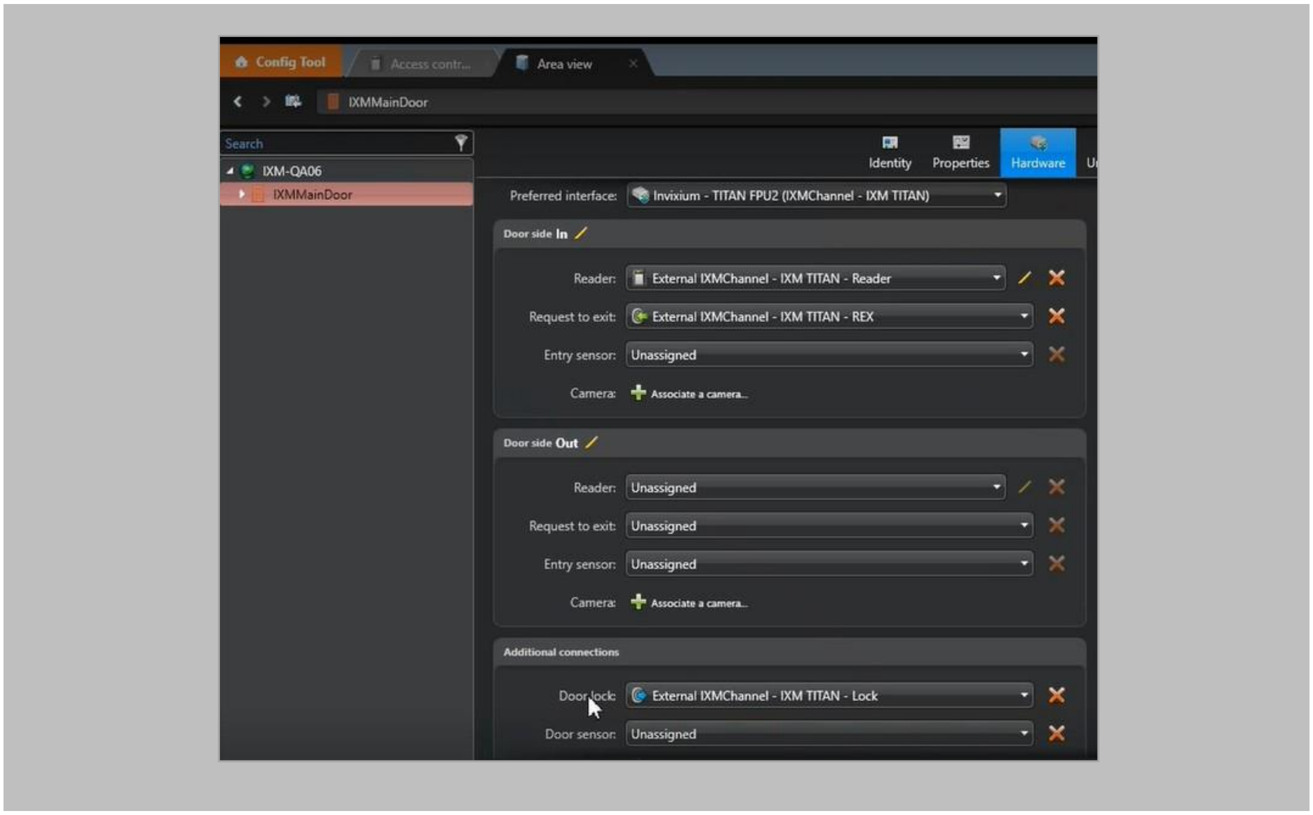
Click to select the Invixium device on which RIO settings were applied.

Click **Next** and **Create**.

STEP 4

Configure the Door.

Navigate to **Area View** → Click on the **Door** created by you → navigate to **Hardware** tab



Preferred interface: Invixium - TITAN FPU2 (IXMChannel - IXM TITAN)

Door side **In**

Reader: External IXMChannel - IXM TITAN - Reader

Request to exit: External IXMChannel - IXM TITAN - REX

Entry sensor: Unassigned

Camera: Associate a camera...

Door side **Out**

Reader: Unassigned

Request to exit: Unassigned

Entry sensor: Unassigned

Camera: Associate a camera...

Additional connections

Door lock: External IXMChannel - IXM TITAN - Lock

Door sensor: Unassigned

Figure 87: Config Tool – Configuring Door

Note: In case of single Reader, either Door Side In can be configured or Door Side Out and not both of them.

Reader

Click to select the Invixium device reader as External Reader.

Request to exit

Click to select the Invixium device as REX.

Door lock

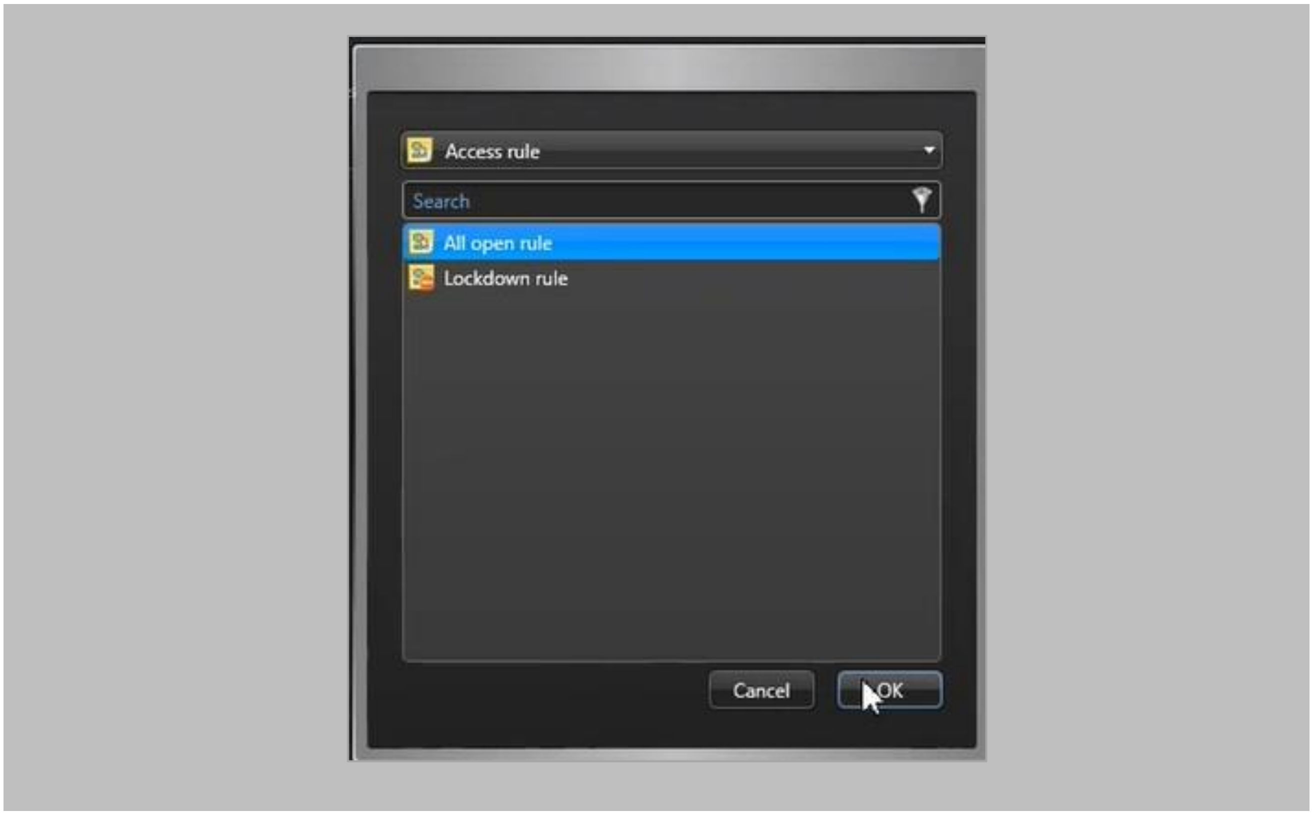
Click to select the Invixium device for Door lock.

Click **Apply**.

STEP 5

Configure the Schedule.

Select **Door** which you have created → Click on **Access Rules** tab → Click on **+** icon → Click on **All open rule**



Access rule

Search

All open rule

Lockdown rule

Figure 88: Config Tool – Access Rule

Click **OK** and **Apply**.

Monitoring Events and alarms

STEP 1

Log in to Security Desk of GSC and Navigate to **Monitoring** tab.

STEP 2

You will be able to see the Door that you have configured.

Note: The View Area is empty right now.

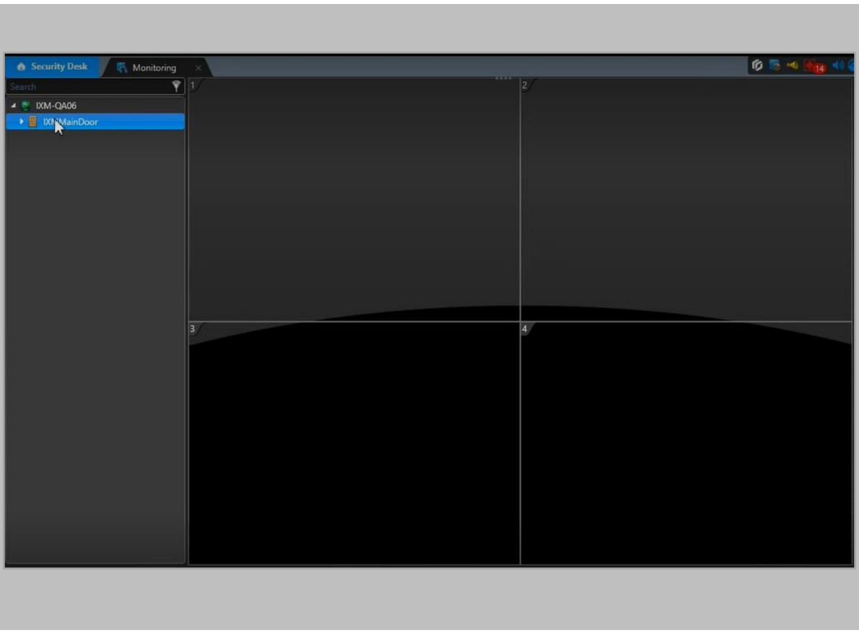


Figure 89: Security Desk – Monitoring

STEP 3

Drag and drop the Door to the View Area.

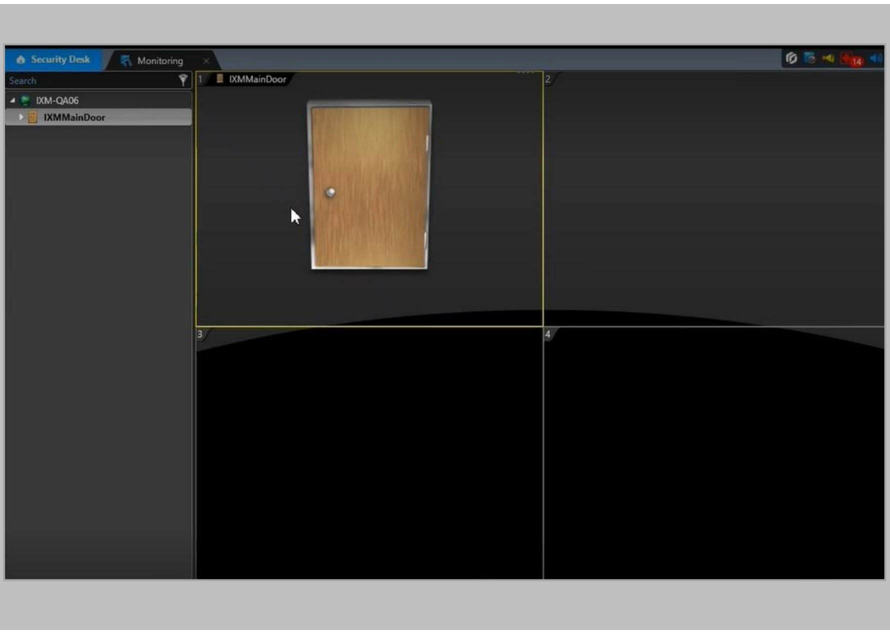
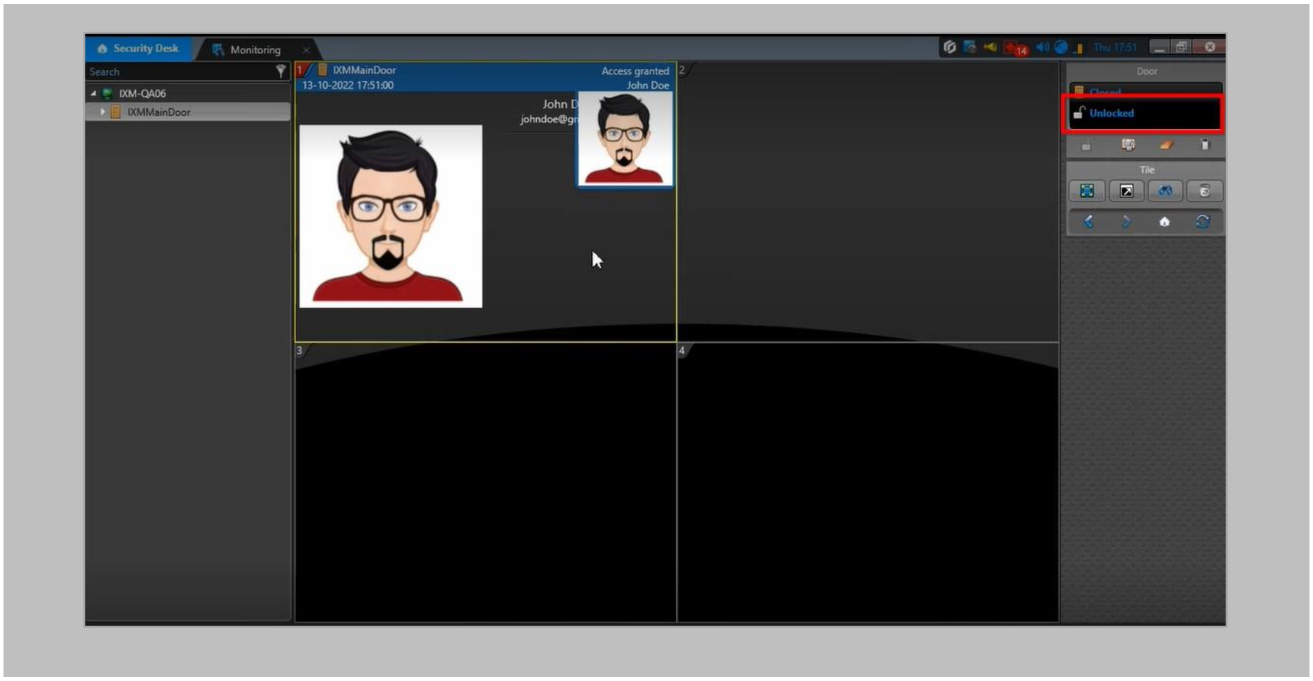


Figure 90: Security Desk – View Area

STEP 4

Perform authetification event on the device and verify the event on Genetec Desk.



1 IXMMainDoor Access granted
13-10-2022 17:51:00 John Doe

Figure 91: Security Desk – Access Granted

18. 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**

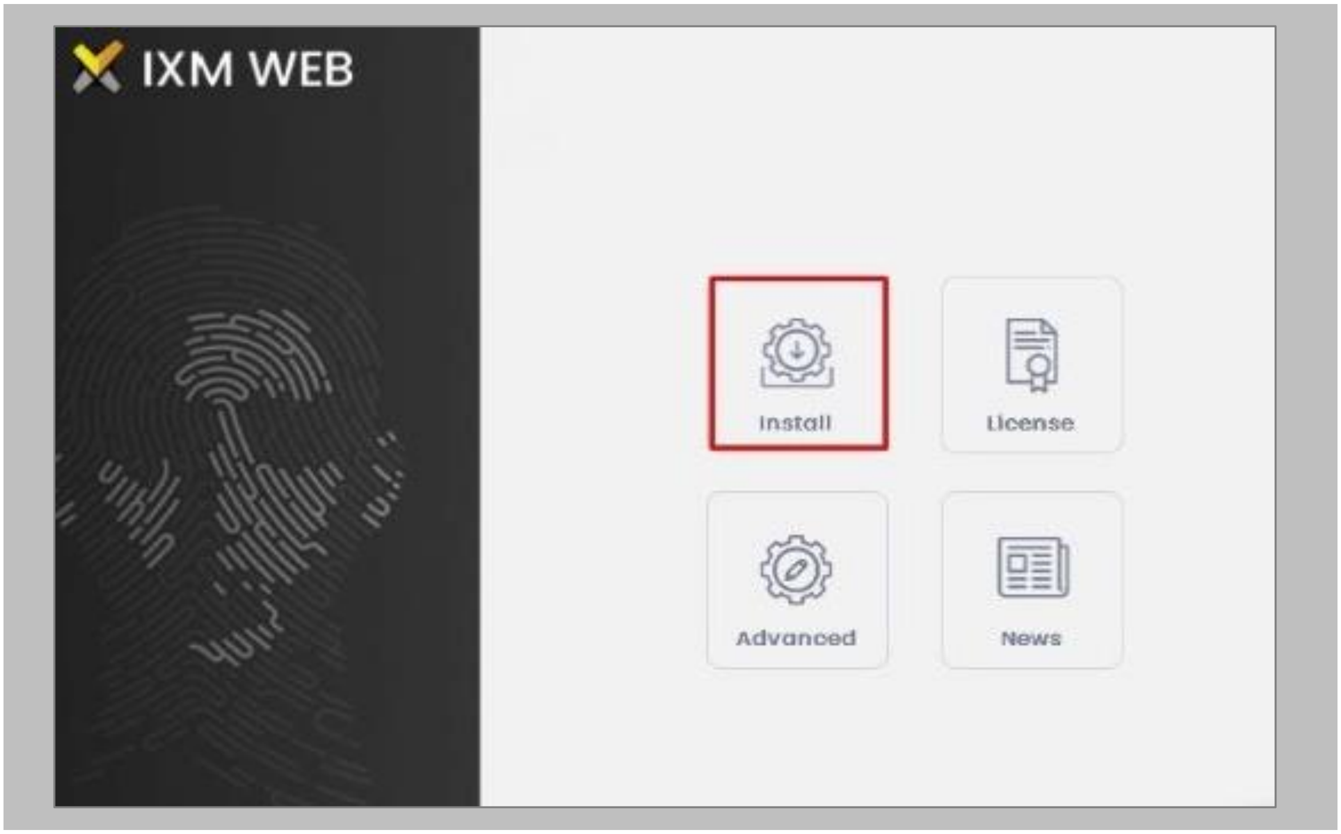
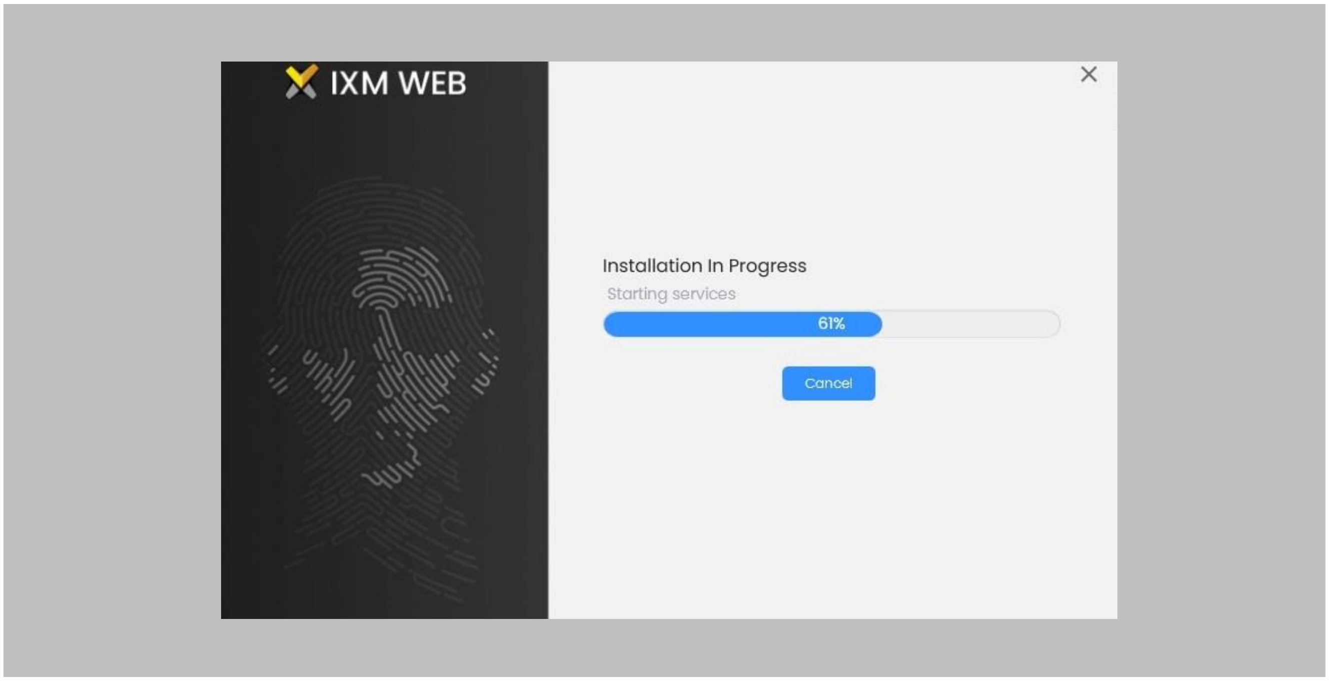


Figure 92: Install IXM WEB

Note: Installs SQL 2014 Express.



Installation In Progress

Starting services

61%

Figure 93: 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.

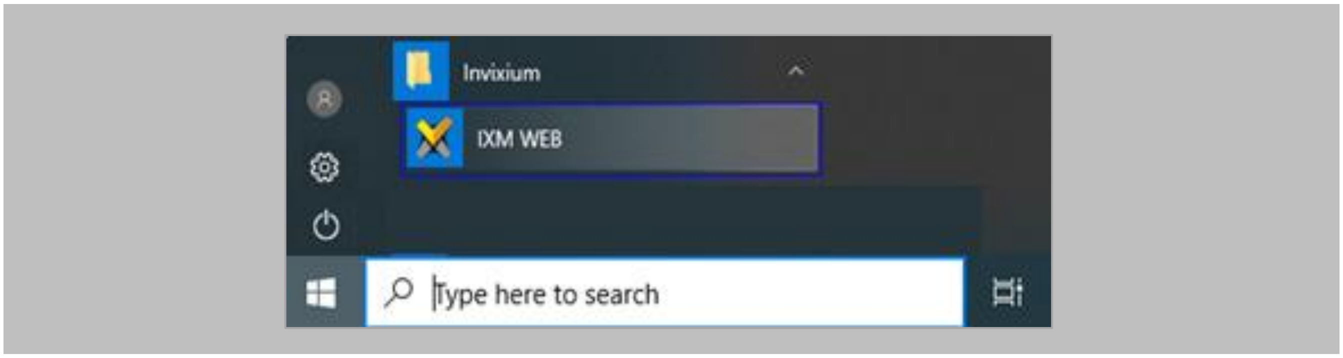
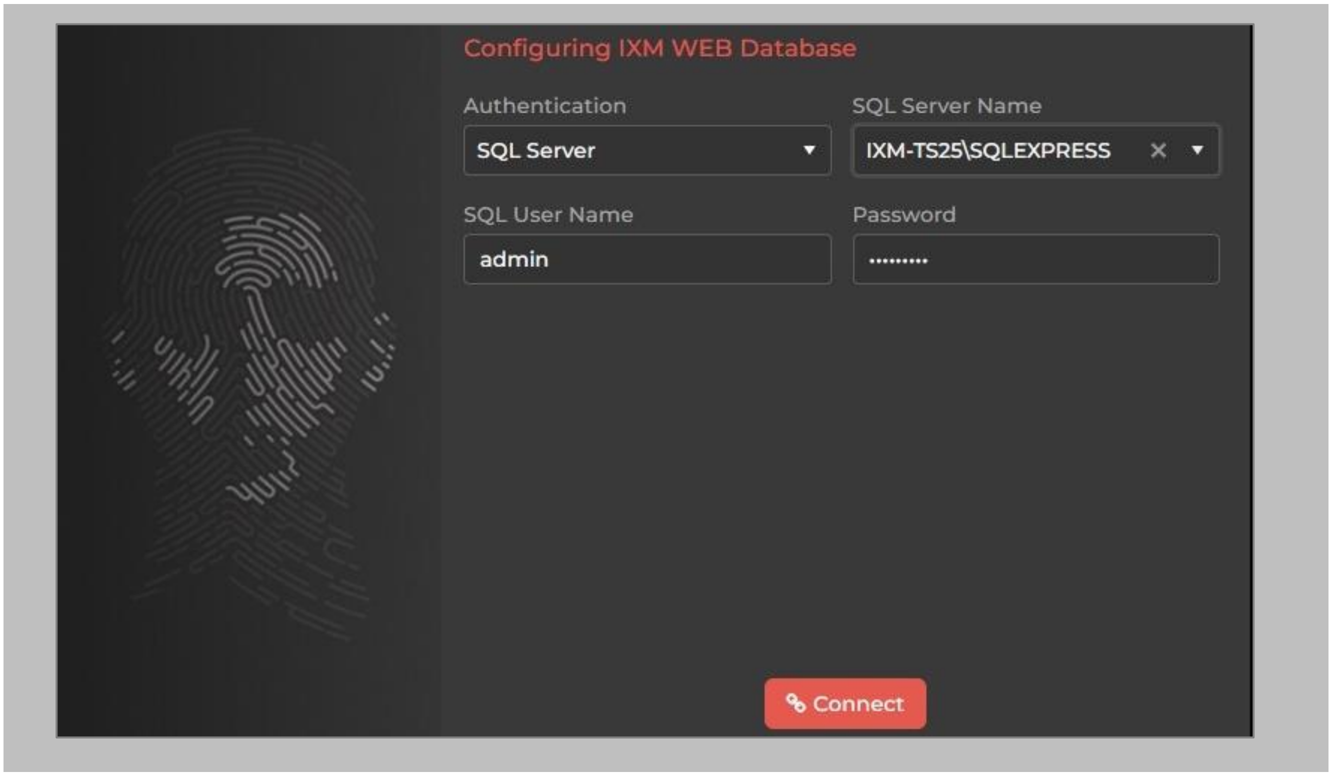


Figure 94: IXM WEB - Shortcut Icon on Desktop

STEP 4

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



Configuring IXM WEB Database

Authentication: SQL Server

SQL Server Name: IXM-TS25\SQLEXPRESS

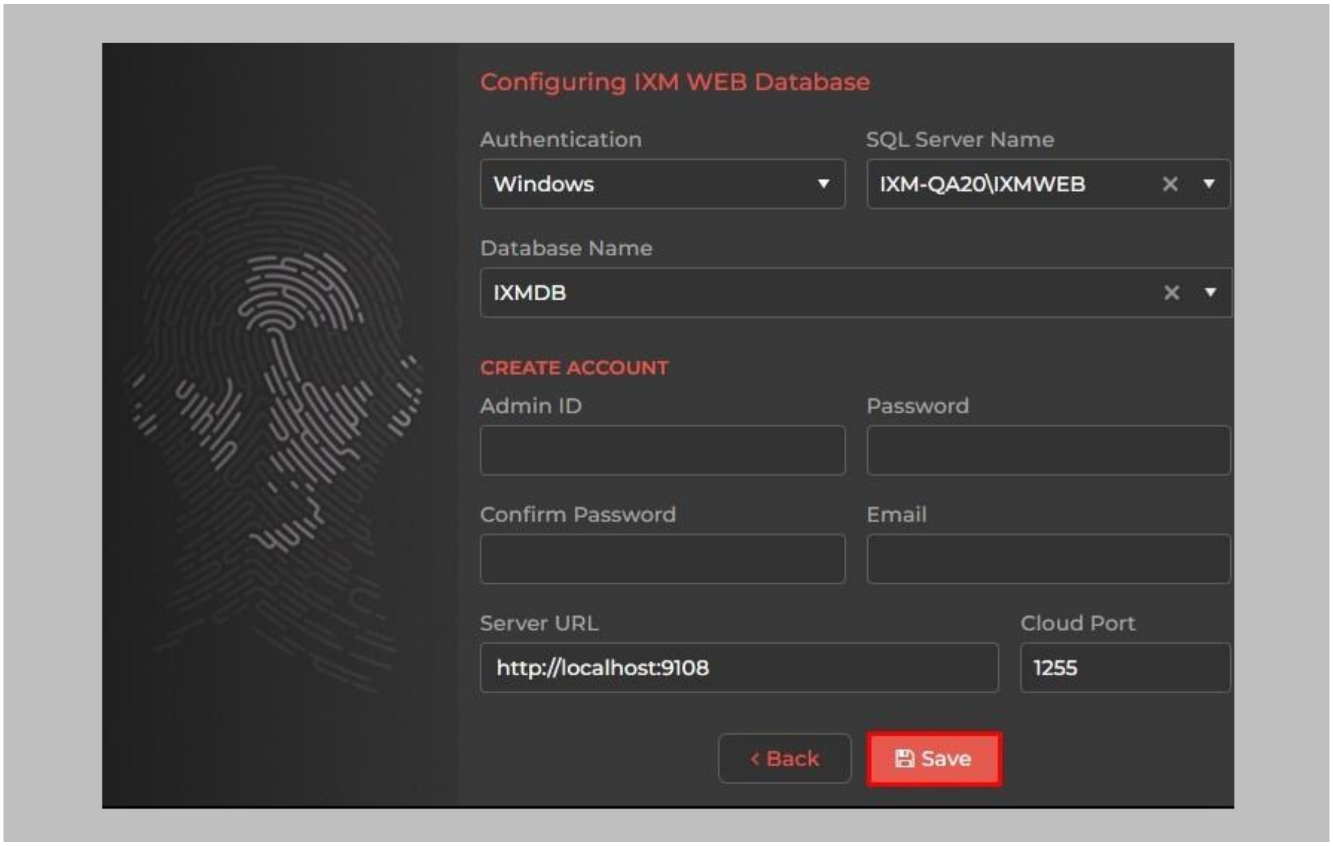
SQL User Name: admin

Password: •••••••••

Figure 95: IXM WEB - Configuring IXM WEB Database

STEP 5

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



Configuring IXM WEB Database

Authentication: Windows

SQL Server Name: IXM-QA20\IXMWEB

Database Name: IXMDB

CREATE ACCOUNT

Admin ID:

Password:

Confirm Password:

Email:

Server URL: http://localhost:9108

Cloud Port: 1255

Figure 96: IXM WEB - Select Database Name

STEP 6

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

STEP 7

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

For example:

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

http://192.168.1.100:9108

STEP 8

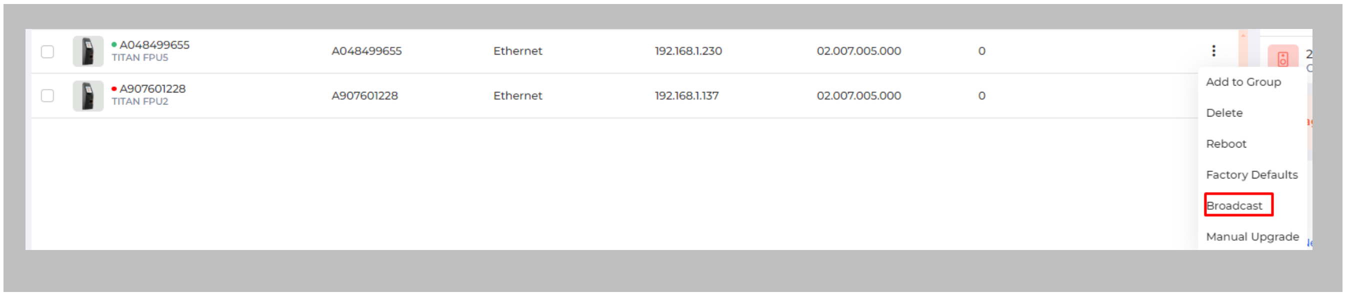
Click **Save**. The software will now create the database and continue setup. This could take several minutes.

Pushing Configuration to Multiple Invixium Readers

Procedure

STEP 1

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

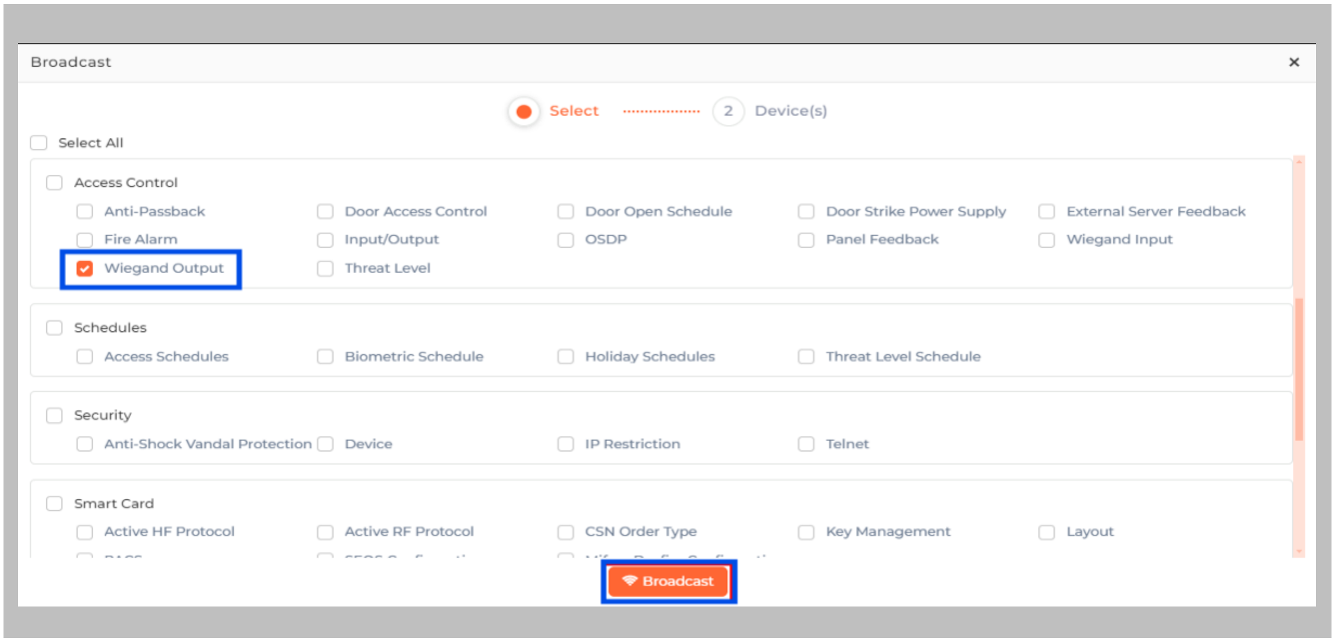


□	● A048499655 TITAN FPU5	A048499655	Ethernet	192.168.1.230	02.007.005.000	0
□	● A907601228 TITAN FPU2	A907601228	Ethernet	192.168.1.137	02.007.005.000	0

Figure 97: IXM WEB - Broadcast Option

STEP 2

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



Broadcast ×

● Select ·················· 2 Device(s)

□ Select All

□ Access Control
- □ Anti-Passback
- □ Door Access Control
- □ Door Open Schedule
- □ Door Strike Power Supply
- □ External Server Feedback
- □ Fire Alarm
- □ Input/Output
- □ OSDP
- □ Panel Feedback
- □ Wiegand Input
- ☑ Wiegand Output
- □ Threat Level

□ Schedules
- □ Access Schedules
- □ Biometric Schedule
- □ Holiday Schedules
- □ Threat Level Schedule

□ Security
- □ Anti-Shock Vandal Protection
- □ Device
- □ IP Restriction
- □ Telnet

□ Smart Card
- □ Active HF Protocol
- □ Active RF Protocol
- □ CSN Order Type
- □ Key Management
- □ Layout

Figure 98: IXM WEB - Broadcast Wiegand Output Settings

STEP 3

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

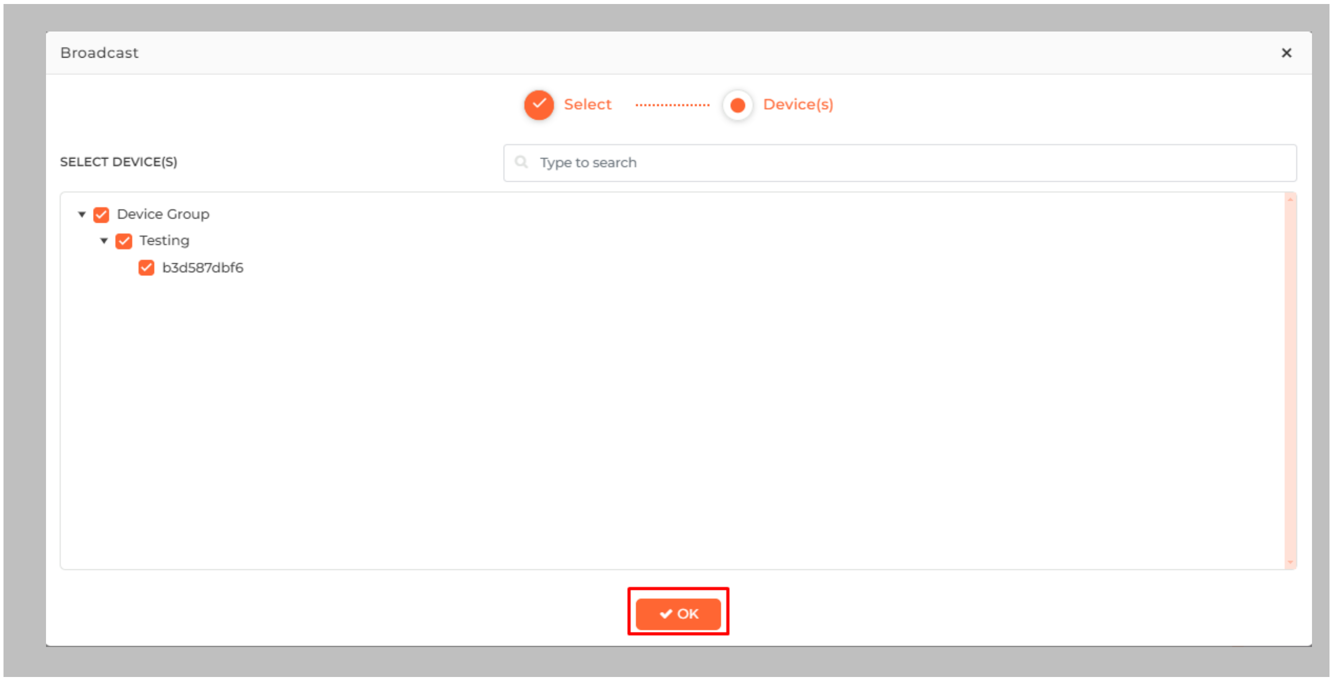


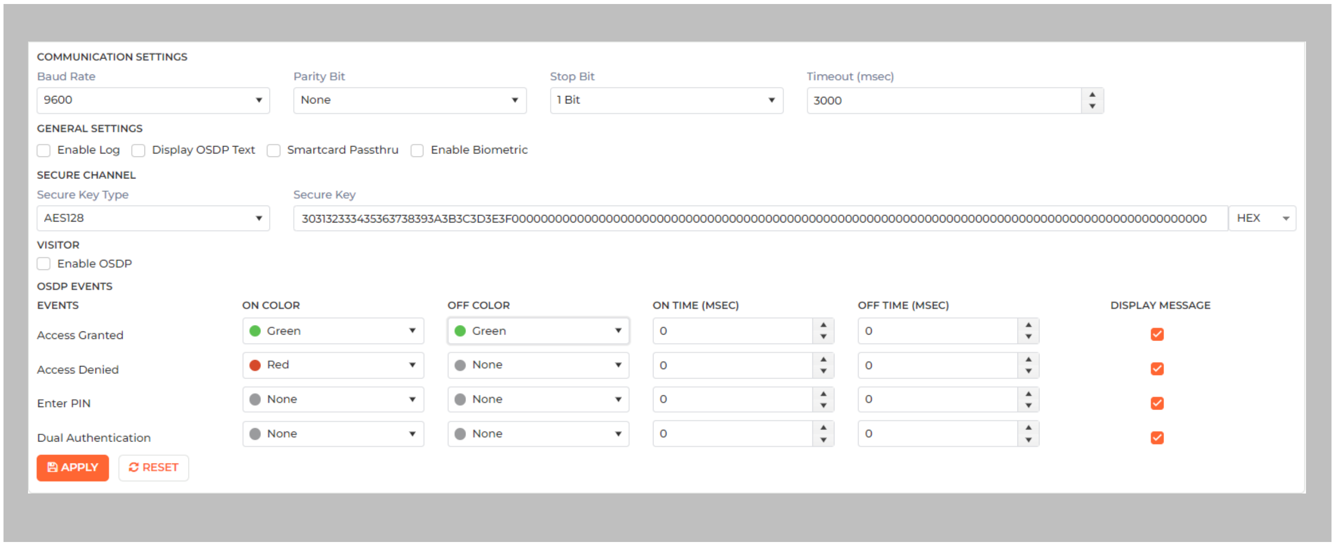
Figure 99: IXM WEB - Broadcast to Devices

Configuring for OSDP Connection

STEP 1

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

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



COMMUNICATION SETTINGS

Baud Rate	Parity Bit	Stop Bit	Timeout (msec)
9600	None	1 Bit	3000

GENERAL SETTINGS

□ Enable Log □ Display OSDP Text □ Smartcard Passthru □ Enable Biometric

SECURE CHANNEL

Secure Key Type	Secure Key	
AES128	303132333435363738393A3B3C3D3E3F000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	HEX

VISITOR

□ Enable OSDP

OSDP EVENTS

EVENTS	ON COLOR	OFF COLOR	ON TIME (MSEC)	OFF TIME (MSEC)	DISPLAY MESSAGE
Access Granted	● Green	● Green	0	0	☑
Access Denied	● Red	● None	0	0	☑
Enter PIN	● None	● None	0	0	☑
Dual Authentication	● None	● None	0	0	☑

Figure 100: IXM WEB - OSDP Settings

STEP 2

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

Baud Rate	The baud rate of the serial communication. The value must be the same as the Access Control Panel's value.
Parity Bit	The parity bit of the serial communication. The value must be the same as the Access Control Panel's value.
Stop Bit	The stop bit of the serial communication. The value must be the same as the Access Control Panel's value.
Enable Log	This logs OSDP events for support and debugging purposes. Invixium recommends disabling this feature unless needed.
SmartCard Passthru	When presenting a smart card, the device passes the smart card CSN (Card Serial Number) to the Access Control Panel without taking any other action.
Enable Biometric	Enables biometric template verification.
Secure Channel	The secure key is provided by your Access Control Panel most of the time. However, provisions for manual entry can be added as TEXT or HEX.
Event	The OSDP static events for panel feedback and capture pin are: Access Granted Access Denied Enter PIN Dual Authentication – It is an access mode that requires valid access by two authorized cardholders to enter an access zone within a specified time period. This feature is available only if the **Multi-User Authentication** feature is enabled and configured. To configure the Multi-User Authentication feature, from **Home**, click the **Devices** tab. Select the required Device and navigate to **General Settings**. Click on the **Multi-User Authentication** section. Upon enabling this feature, the following actions will be performed: • The Device will request the credentials of the second

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

Table 5: IXM WEB - OSDP Configuration Options

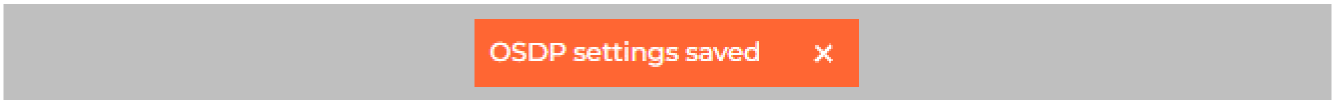
Note: Mismatches between the unit and Access Control Panel LED configuration would cause unrecognized events.

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

Table 6: IXM WEB - OSDP Text Options

STEP 3

Click **Apply** to save the settings.

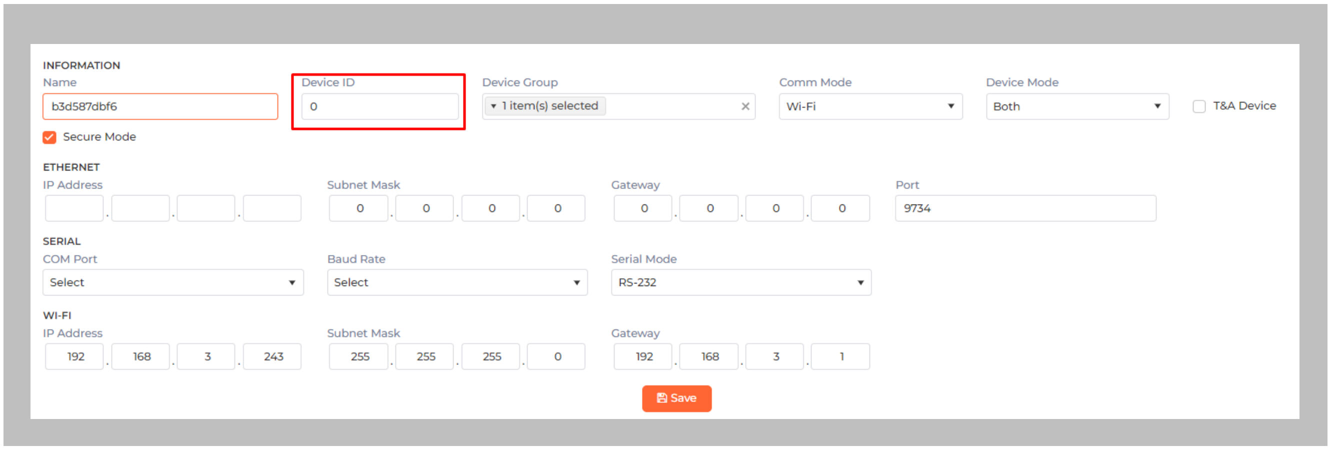


OSDP settings saved ×

Figure 101: 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 GSC.



INFORMATION

Name: b3d587dbf6

Device ID: 0

Device Group: ▾ 1 item(s) selected ×

Comm Mode: Wi-Fi ▾

Device Mode: Both ▾

☐ T&A Device

☑ Secure Mode

ETHERNET

IP Address: . . .

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Port: 9734

SERIAL

COM Port: Select ▾

Baud Rate: Select ▾

Serial Mode: RS-232 ▾

WI-FI

IP Address: 192 . 168 . 3 . 243

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 3 . 1

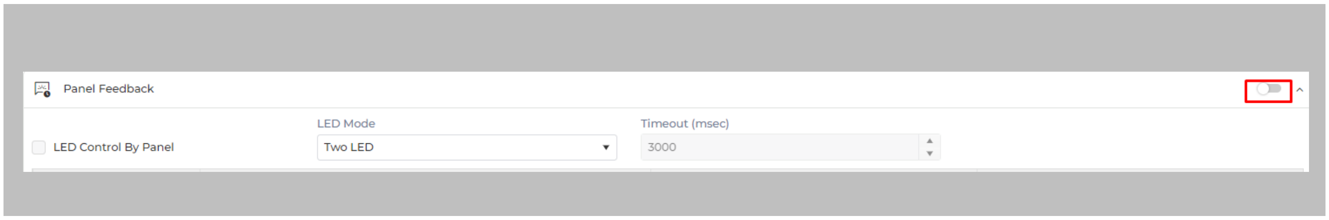
Figure 102: IXM WEB - Edit Device Options

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 GSC.



Panel Feedback

□ LED Control By Panel

LED Mode: Two LED

Timeout (msec): 3000

Figure 103: 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.

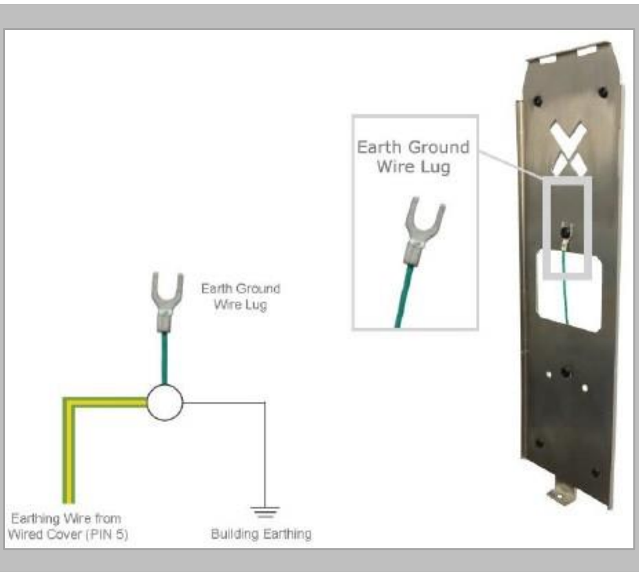


Figure 104: Earth Ground Wiring

Wiring

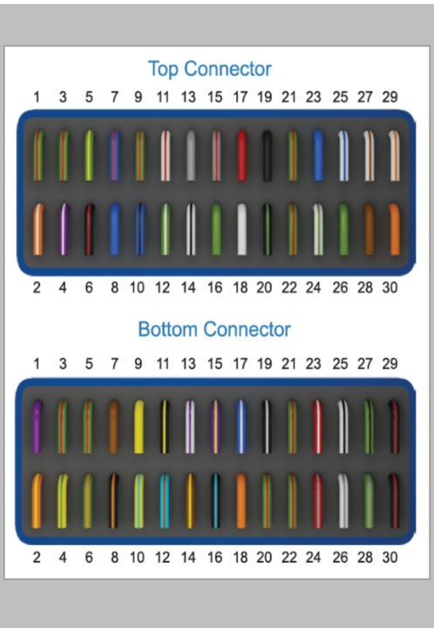
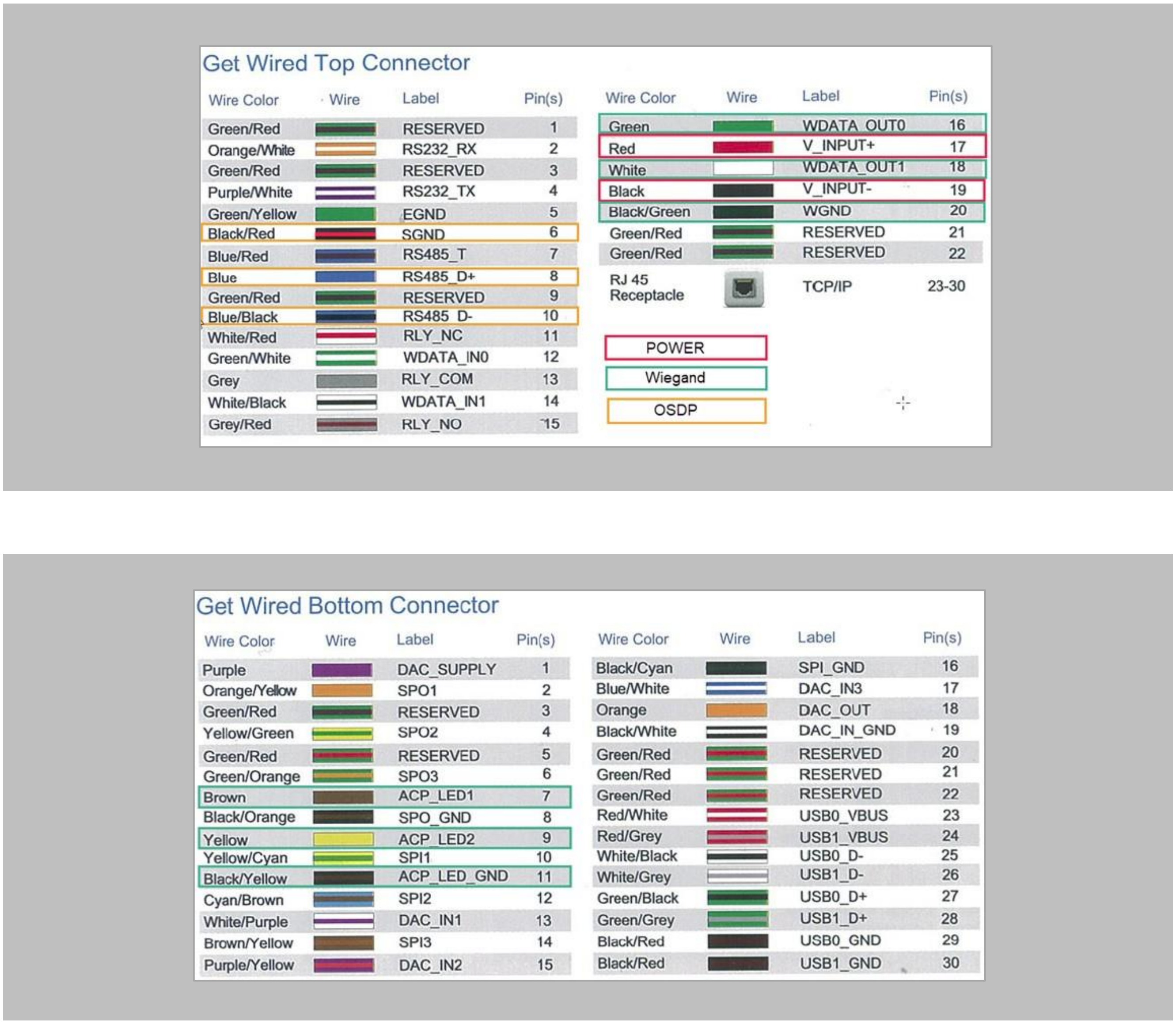


Figure 105: IXM TITAN – Top & Bottom Connector Wiring



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				
Blue/Black	🟦	RS485_D-	10				
White/Red	🟥	RLY_NC	11				
Green/White	🟩	WDATA_IN0	12				
Grey	▩	RLY_COM	13				
White/Black	⬛	WDATA_IN1	14				
Grey/Red	▩	RLY_NO	15				

POWER

Wiegand

OSDP

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 106: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand, OSDP and RIO protocol (wireless).

Invixium devices can be integrated with Genetec Controller on:

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

Wiegand Connection

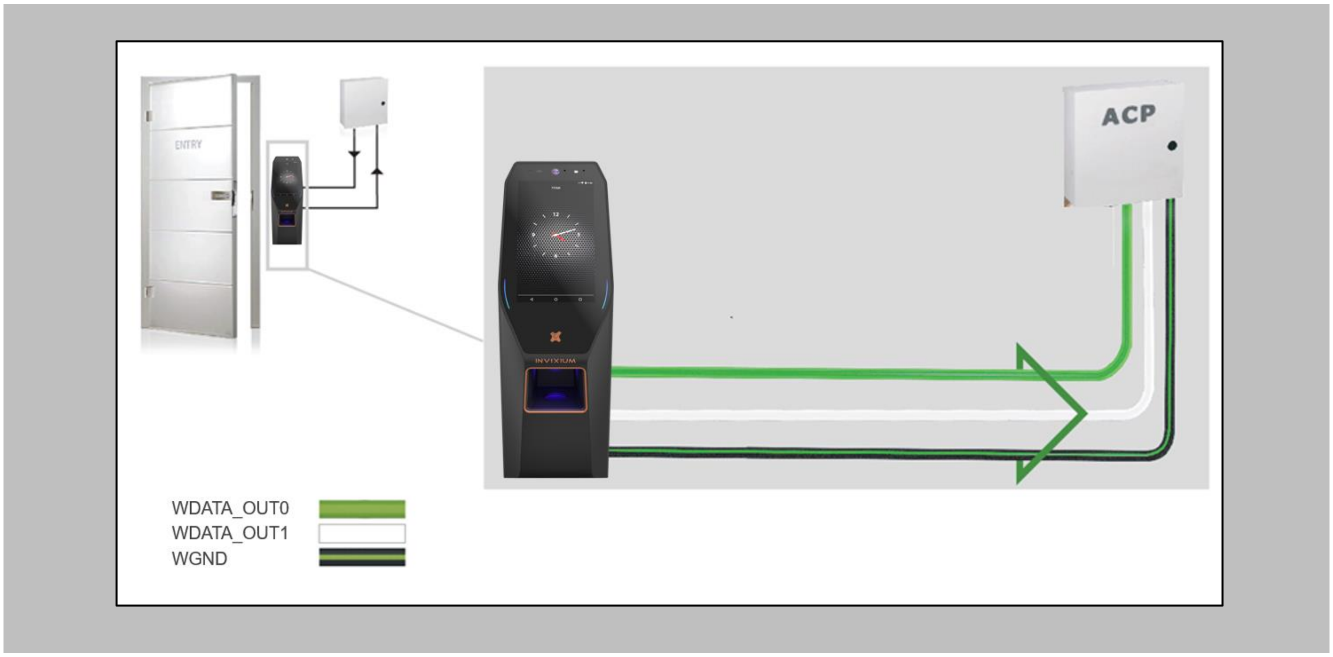
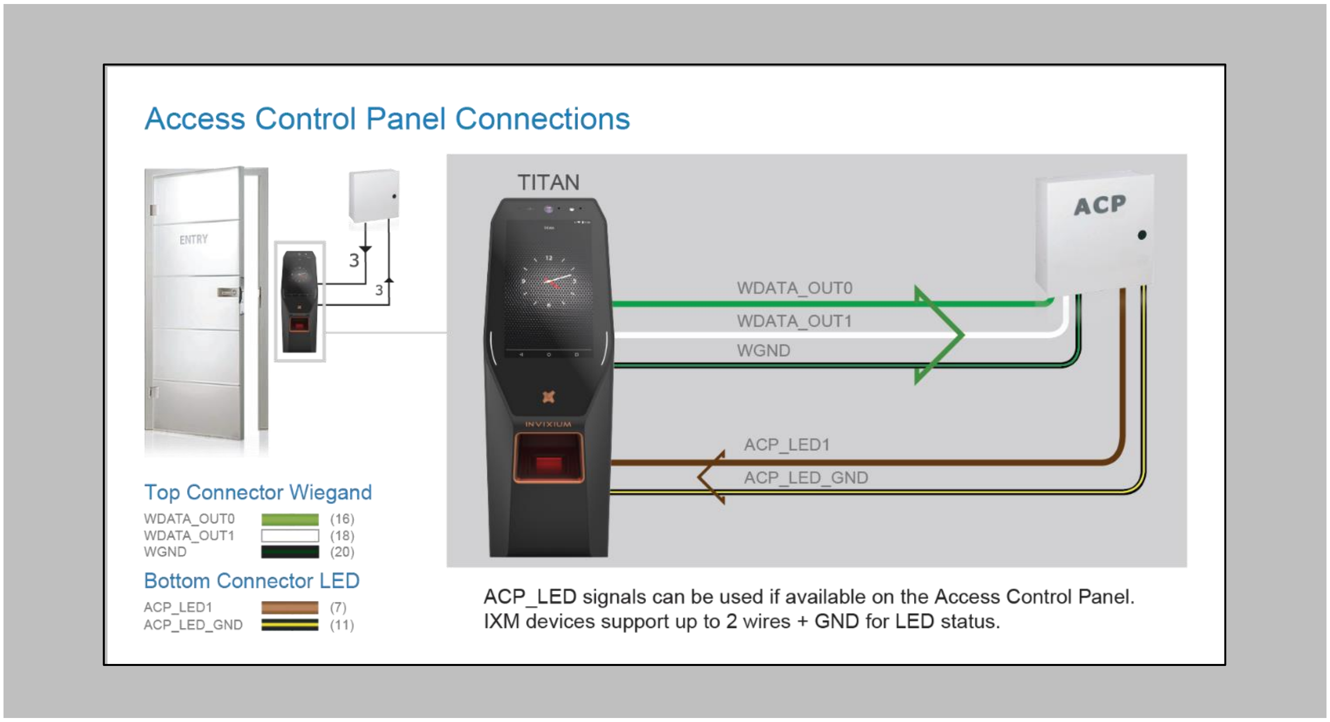


Figure 107: IXM TITAN - Wiegand

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

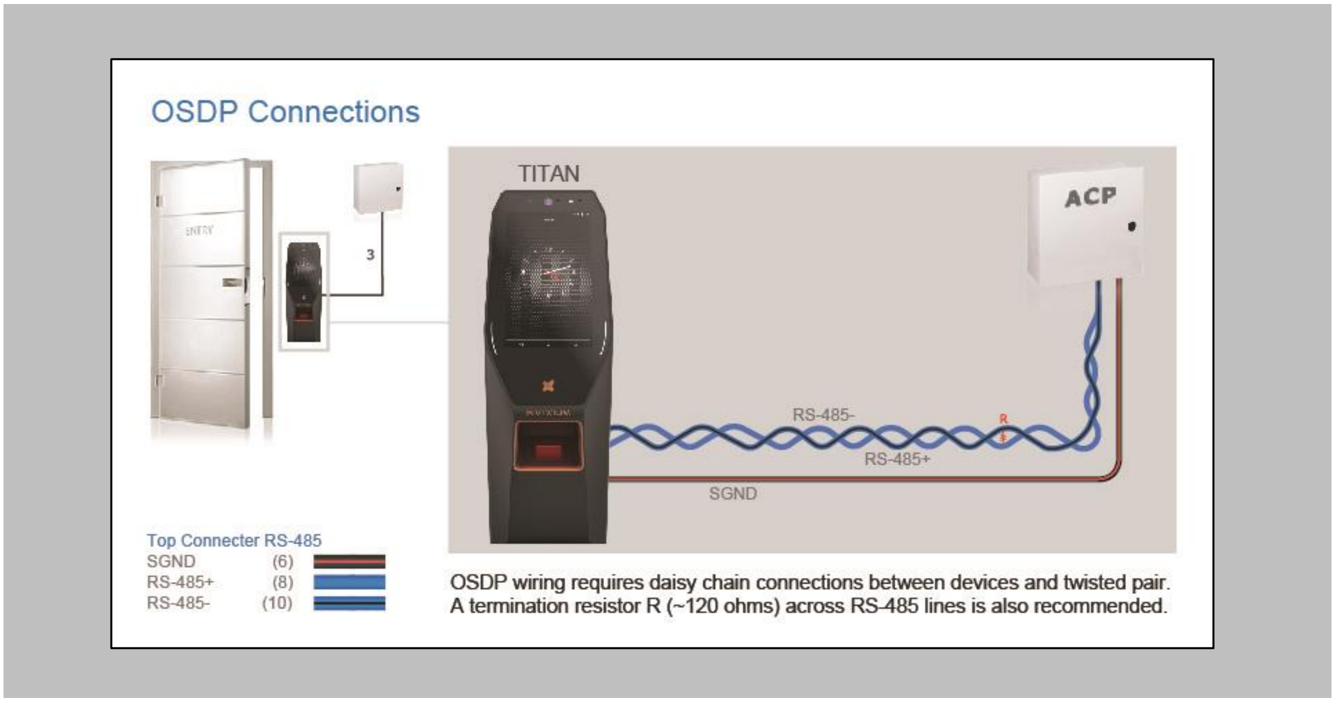

Access Control Panel Connections

ACP_LED signals can be used if available on the Access Control Panel.
IXM devices support up to 2 wires + GND for LED status.

Figure 108: 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



Top Connecter RS-485		
SGND	(6)	▬
RS-485+	(8)	▬
RS-485-	(10)	▬

OSDP wiring requires daisy chain connections between devices and twisted pair. A termination resistor R (~120 ohms) across RS-485 lines is also recommended.

Figure 109: 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.

19. Troubleshooting

Reader Offline from the IXM WEB Dashboard

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

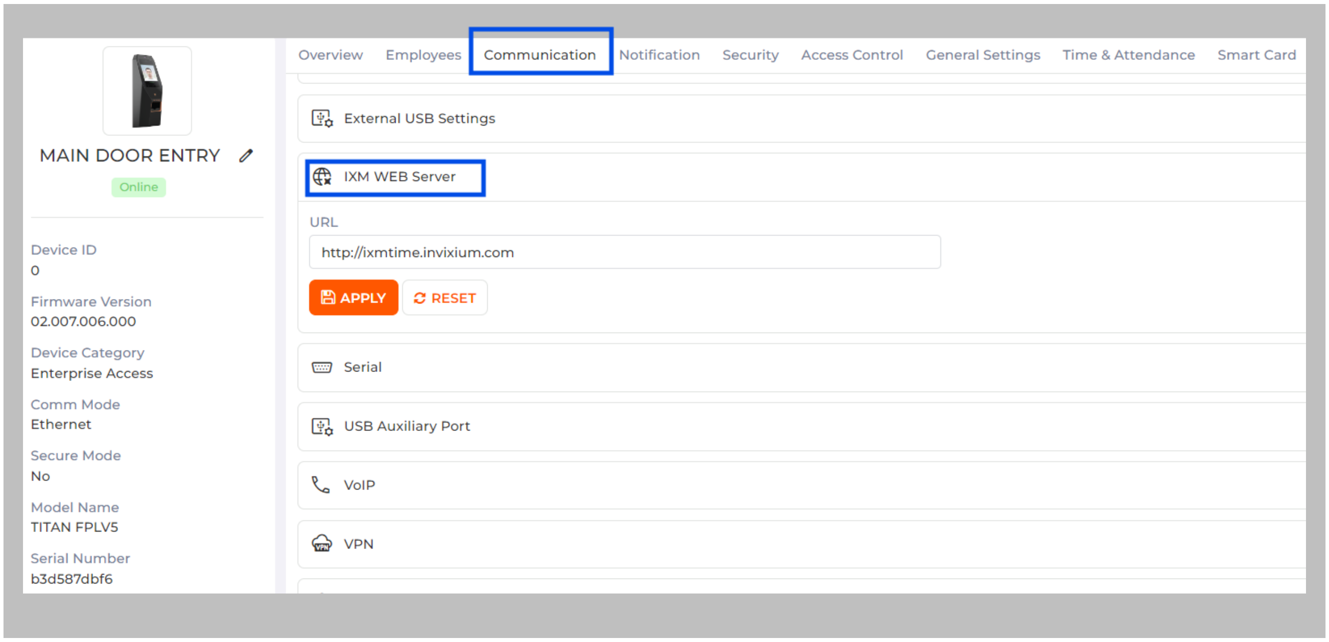
Procedure

STEP 1

From **Devices** tab select any device.

STEP 2

Navigate to the **Communication** tab. Scroll down and click on **IXM WEB Server**.



MAIN DOOR ENTRY

Online

Device ID
0

Firmware Version
02.007.006.000

Device Category
Enterprise Access

Comm Mode
Ethernet

Secure Mode
No

Model Name
TITAN FPLV5

Serial Number
b3d587dbf6

URL
http://ixmtime.invixium.com

Figure 110: IXM WEB - Server URL Setting

STEP 3

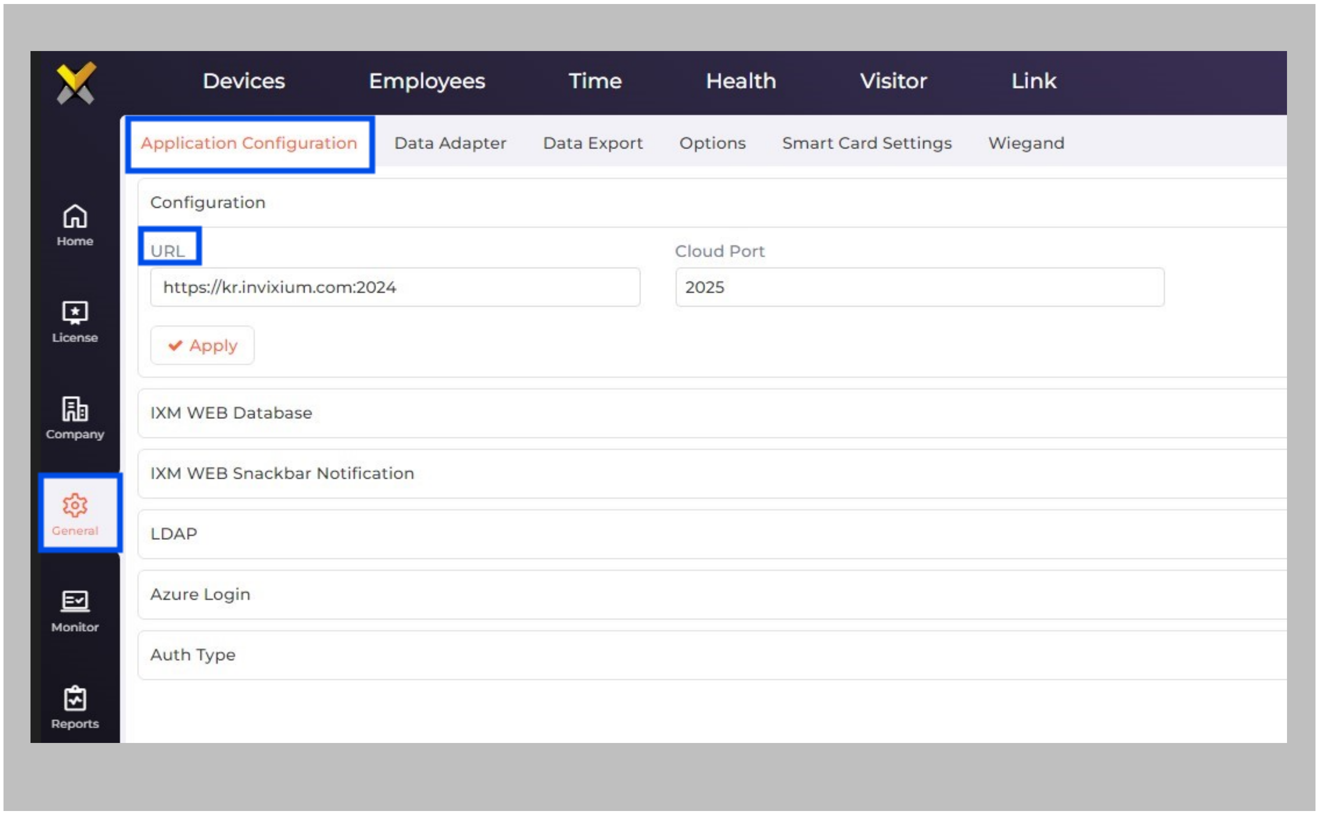
Enter the **IP address** of the Invixium server followed by **port 9108.**

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

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

In case of IP Address or URL of IXM WEB Server is changed; perform below step to update all registered device(s).

Navigate to **General** → **Application Configuration** and make sure that the **URL** is correct.



Configuration

URL: https://kr.invixium.com:2024

Cloud Port: 2025

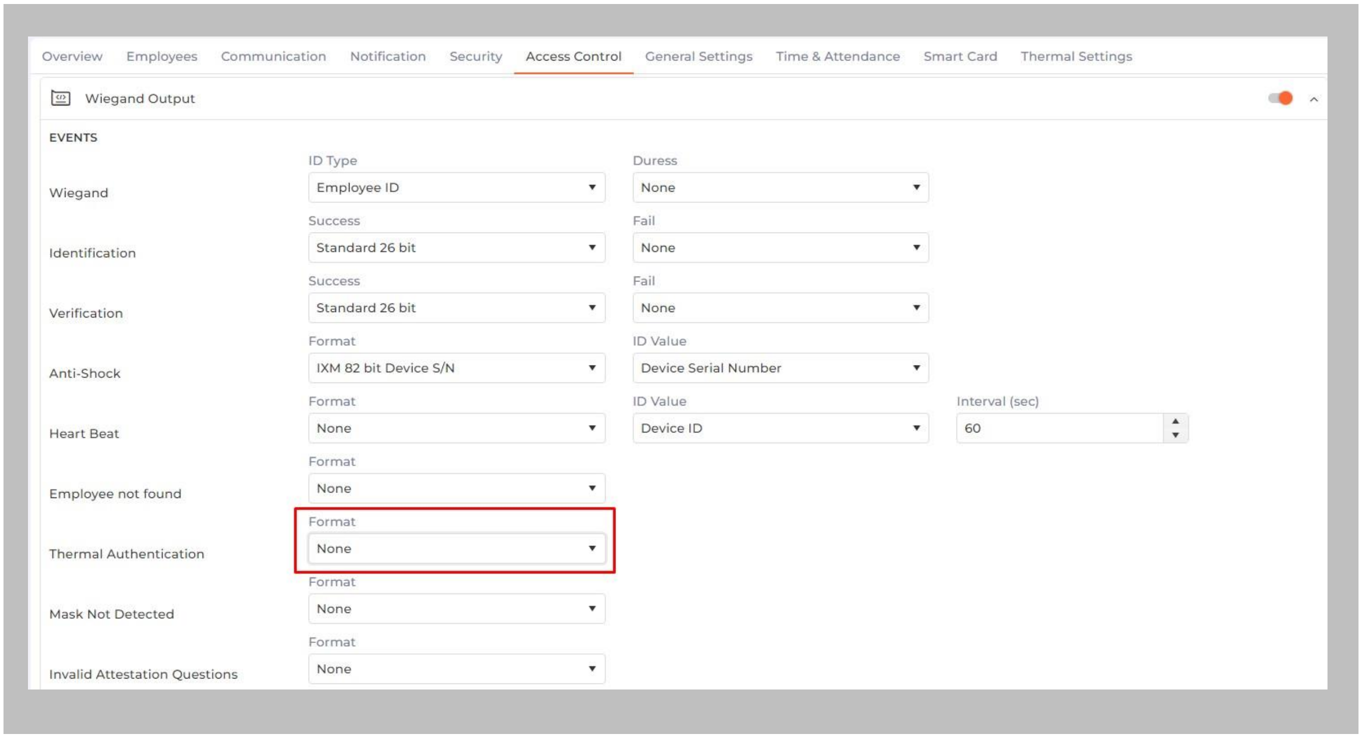
Figure 111: IXM WEB - Server URL Setting from General Settings

Elevated Body Temperature Denied Access but Granted Access in GCC

Procedure

STEP 1

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



Wiegand Output

EVENTS

Wiegand	ID Type Employee ID	Duress None	
Identification	Success Standard 26 bit	Fail None	
Verification	Success Standard 26 bit	Fail None	
Anti-Shock	Format IXM 82 bit Device S/N	ID Value Device Serial Number	
Heart Beat	Format None	ID Value Device ID	Interval (sec) 60
Employee not found	Format None		
Thermal Authentication	Format None		
Mask Not Detected	Format None		
Invalid Attestation Questions	Format None		

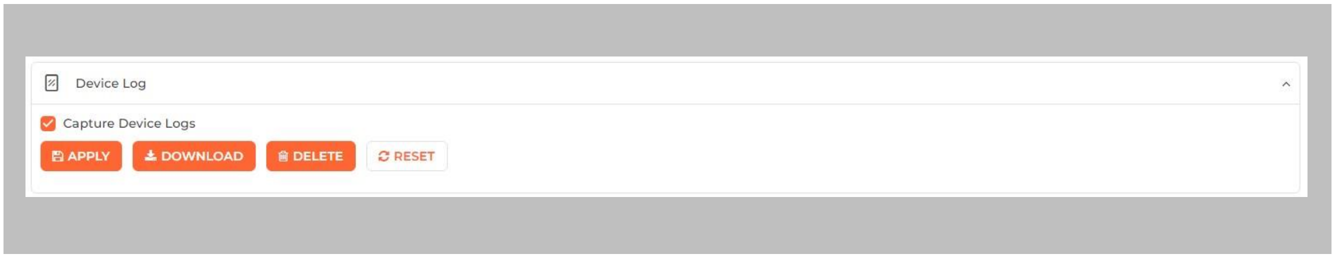
Figure 112: IXM WEB - Thermal Authentication Wiegand Output Event

Note: If Thermal Authentication events are configured for any format, it generates Wiegand output accordingly for a high-temperature event.

Logs in IXM WEB Application

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

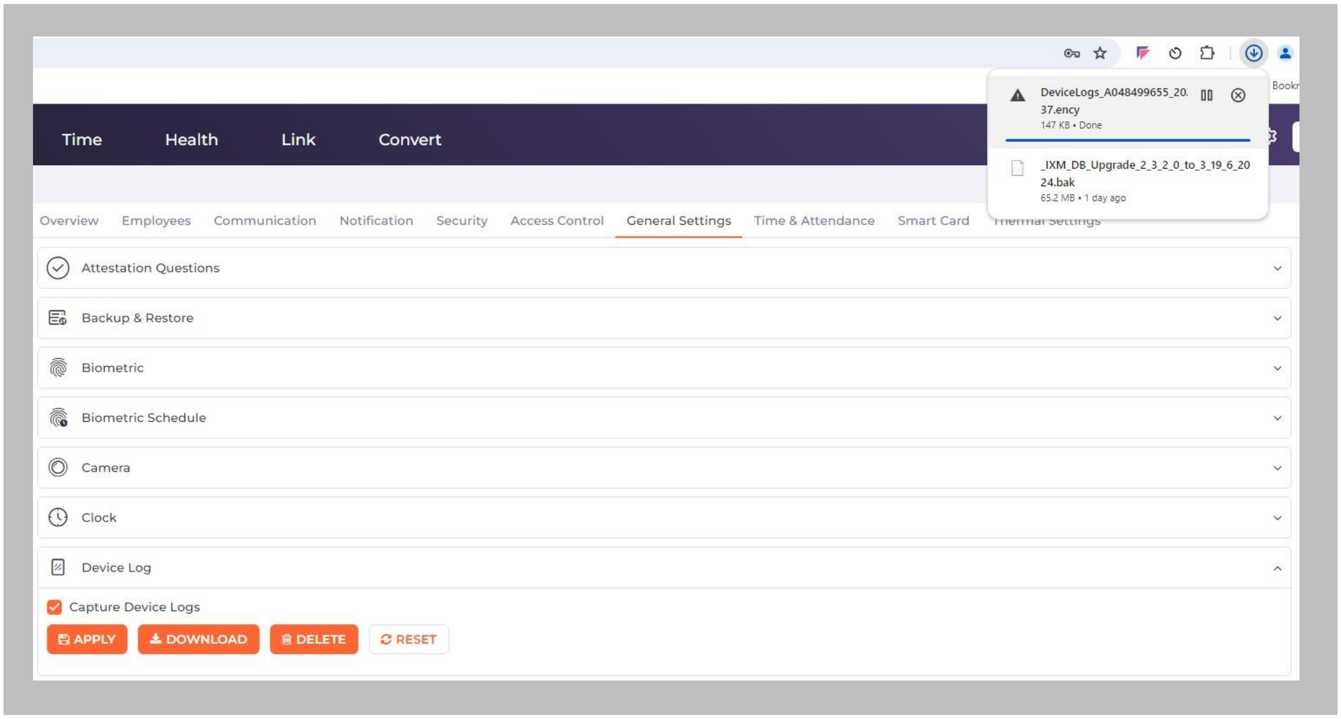
From the **Devices** Tab on the top → Select the required **Device** → Navigate to the **General Settings** tab for the device → Click on **Device Log** → **Enable** Capture Device Logs.


Device Log

☑ Capture Device Logs

Figure 113: IXM WEB - Enable Device Logs

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


DeviceLogs_A048499655_20: 37.ency
147 KB • Done

_IXM_DB_Upgrade_2_3_2_0_to_3_19_6_2024.bak
65.2 MB • 1 day ago

☑ Capture Device Logs

Figure 114: 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

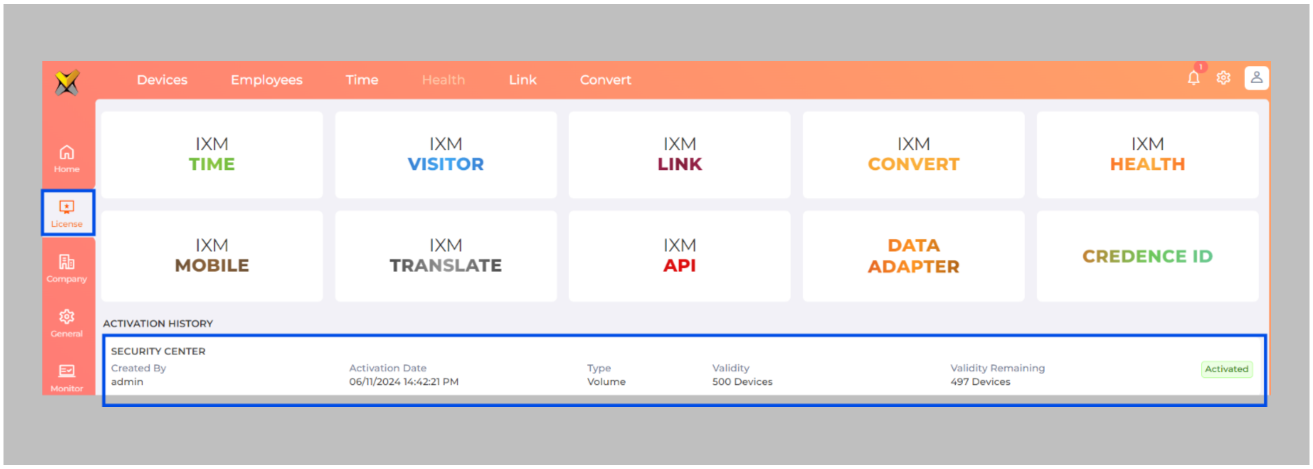
Unable to connect to the Genetec Server

Procedure

STEP 1

Note: Confirm module activation

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



ACTIVATION HISTORY

SECURITY CENTER

Created By	Activation Date	Type	Validity	Validity Remaining	
admin	06/11/2024 14:42:21 PM	Volume	500 Devices	497 Devices	Activated

Figure 115: IXM WEB - Licence Module

STEP 2

Note: Confirm WEB SDK is enabled.

This can be checked from GSC. Navigate to **System** → **Roles** → Click **Web-based SDK**

STEP 3

Note: Confirm parameters entered to connect to the Genetec server.

Ensure the correct **WEB API URL** of the server is listed. here. If not, **correct** and **apply.**

Ensure the correct **User** who is authorized to connect to the WEB SDK of Genetec Security Center is listed here. If not, **correct** and **apply.**

Ensure the correct **Password** of the user who is authorized to connect to the WEB SDK of Genetec Security Center is listed here. If not, **correct** and **apply.**

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

This file is available at the following path:

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

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.