IXM WEB Integration with Gallagher Command Centre

Installation Instructions

V4.0

Table of Contents

1. Introduction 9

Purpose 9

Summary of key features related to this IXM WEB and GCC Integration 9

Description 9

Acronyms 9

Field Mappings 10

2. Compatibility 11

Invixium Readers 11

Software Requirements 11

Other Requirements 12

Compatibility Matrix for IXM WEB & Command Centre Integration 12

3. Checklist 13

4. Task List Summary 14

5. Prerequisites for GCC and IXM WEB Integration 15

URL Enrollment PDF (Personal Data Field) 15

Enrollment Status PDF (Personal Data Field) 19

Cardholder Access Group 22

Enabling the Invixium License for IXM WEB in Command Centre 24

REST API Client 28

6. Prerequisites for Installing Invixium IXM WEB Software 29

Acquiring IXM WEB Activation Key 29

Setting Up SQL instance 31

Minor Checklist and Considerations 35

7. Installing IXM WEB 36

Software Install 36

8. Configuring Email Settings using IXM WEB 45

Email Setting Configuration 45

9. Software and Module Activation 49

IXM WEB Activation 49

Command Centre Module Activation 52

10. Configuring IXM Link for Gallagher 55

11. Create System User(s) for Biometric Enrollment 60
Creating System User(s) for Biometric Enrollment 60

12. Add and Configure Invixium Readers 64
Adding an Invixium Reader in IXM WEB 64

13. Adding an Invixium Device to a Device Group 69
Configuring Wiegand to Assign Invixium Readers 70
Assign Wiegand to Invixium Readers 73
Configure UCF on Configuration Client 77
Configuring Panel Feedback with Gallagher 78
Configuring Thermal Settings 80
Thermal Calibration 83
Test Calibration Options 85
Change Temperature Unit Settings 87
Configuring Mask Authentication Settings 89
Pre-configuration for Enrollment 92

14. Enrollment from Gallagher Command Centre 95

15. Enrollment Best Practices 96
Fingerprint Enrollment Best Practices 96
Avoid Poor Fingerprint Conditions 96
Fingerprint Image Samples 97
Fingerprint Imaging Do's and Don'ts 98
Finger Vein Enrollment Best Practices 99
Face Enrollment Best Practices 100

16. Send Logical Events to Command Centre 101

17. Appendix 104
Installing Invixium IXM WEB with Default Installation using SQL Server 2014 104
Pushing Configuration to Multiple Invixium Readers 109
Configuring for OSDP Connection 111
Configuring MIFARE DESFire Custom Cards 117
Wiring 121
Wiegand Connection 123
Wiegand Connection with Panel Feedback 124

OSDP Connections 125

18. Troubleshooting 126

Reader Offline from the IXM WEB Dashboard 126

Elevated Body Temperature Denied Access but Granted Access in GCC 128

Logs in IXM WEB Application 129

19. Support 131

20. Disclaimer and Restrictions 131

List of Figures

Figure 1: GCC - Personal Data Field 1 Properties 15
Figure 2: GCC - Gallagher Invixium Properties 17
Figure 3: GCC - Cardholder Access Group Properties 18
Figure 4: GCC - Personal Data Field 1 Properties – Enrollment Status 19
Figure 5: GCC – Enrollment Status Properties 20
Figure 6: GCC - Cardholder Access Group Properties 21
Figure 7: GCC - Invixium Access Group Properties 22
Figure 8: GCC – Invixium License for IXM WEB 25
Figure 9: GCC - Restart GCC Services 26
Figure 10: GCC – C12873Invixium License Enabled 27
Figure 11: IXM WEB Online Request Form 29
Figure 12: Sample Email After Submitting Online Request Form 30
Figure 13: SQL New Login 32
Figure 14: SQL Login Properties 33
Figure 15: SQL Server Roles 34
Figure 16: IXM WEB Installer 36
Figure 17: Advanced Options in IXM WEB Installer 37
Figure 18: Invixium Fingerprint Driver Installation Message 38
Figure 19: IXM WEB Installation Progress 39
Figure 20: IXM WEB Installation Completed 40
Figure 21: IXM WEB Icon - Desktop Shortcut 41
Figure 22: IXM WEB Database Configuration 41
Figure 23: IXM WEB Administrator User Configuration 42

Figure 24: IXM WEB Login Page 44
Figure 25: Configure Email 46
Figure 26: IXM WEB - SMTP Settings........ 46
Figure 27: IXM WEB - Save Email Settings 47
Figure 28: IXM WEB – Test Connection........ 47
Figure 29: IXM WEB - Forgot Password 48
Figure 30: IXM WEB - Enter Login Credentials 49
Figure 31: IXM WEB - License Setup........ 50
Figure 32: IXM WEB - Online Activation........ 51
Figure 33: IXM WEB – Request Link License........ 52
Figure 34: Gallagher License Key Email 53
Figure 35: IXM WEB - Activate Gallagher Command Center Link License........ 54
Figure 36: IXM WEB - Enable Gallagher Link Module........ 55
Figure 37: GCC - REST Client Certificate Thumbprint 56
Figure 38: IXM WEB - Map Access Group to User Group........ 57
Figure 39: IXM WEB - Sync Direction 57
Figure 40: IXM WEB - Auto Transfer Employees 58
Figure 41: IXM WEB - Sync Activities 58
Figure 42: IXM WEB - Create System User 60
Figure 43: IXM WEB - Add New System User........ 61
Figure 44: IXM WEB - New System User........ 62
Figure 45: Employee and Employee Group Rights 63
Figure 46: IXM WEB - Save System User........ 63
Figure 47: IXM WEB - Devices Tab 64
Figure 48: IXM WEB - Search Device Using IP Address........ 65
Figure 49: IXM WEB - Register Device 66
Figure 50: IXM WEB - Device Registration Complete 67
Figure 51: IXM WEB - Dashboard, Device Status........ 68
Figure 52: IXM WEB - Assign Device Group........ 69
Figure 53: IXM WEB - Create Wiegand Format 70
Figure 54: IXM WEB - Create Custom Wiegand Format 70
Figure 55: IXM WEB - Custom Wiegand........ 71
Figure 56: IXM WEB – Custom Wiegand Format Created........ 72
Figure 57: IXM WEB - Upload Wiegand Format........ 72
Figure 58: IXM WEB - Navigate to Access Control Tab 73
Figure 59: IXM WEB - Wiegand Output........ 74
Figure 60: IXM WEB - Save Output Wiegand........ 75

Figure 61: IXM WEB - Configure Universal Card Formats 77
Figure 62: IXM WEB - Panel Feedback 78
Figure 63: IXM WEB - Configuring Panel Feedback in IXM WEB 79
Figure 64: IXM WEB - Save Panel Feedback 79
Figure 65: IXM WEB - Thermal Settings 80
Figure 66: IXM WEB - Save Thermal Settings 82
Figure 67: IXM WEB - Thermal Calibration Settings 83
Figure 68: IXM WEB - Save Thermal Calibration Settings 84
Figure 69: IXM WEB - Capture Thermal Data 84
Figure 70: IXM WEB - Save Captured Thermal Data 85
Figure 71: IXM WEB - Test Thermal Calibration 86
Figure 72: IXM WEB - Option to Change Temperature Unit 87
Figure 73: IXM WEB - Save Temperature Unit Setting 88
Figure 74: IXM WEB - Mask Authentication Settings 89
Figure 75: IXM WEB - Save Mask Settings 91
Figure 76: GCC - Cardholder Viewer General Configuration 92
Figure 77: GCC - Enrollment Viewer 93
Figure 78: GCC - URL Tile Configuration 94
Figure 79: Enrollment Viewer 95
Figure 80: Fingerprint Enrollment Best Practices 96
Figure 81: Fingerprint Images Samples 97
Figure 81: Finger Vein Enrollment Best Practices 99
Figure 82: Face Enrollment Best Practices 100
Figure 83: GCC - Gallagher External Event Type Configuration Utility 102
Figure 84: GCC - Cardholder’s Notes 103
Figure 86: Install IXM WEB 104
Figure 87: Loading SQL Express & Installation Progress 105
Figure 88: IXM WEB - Shortcut Icon on Desktop 106
Figure 89: IXM WEB - Configuring IXM WEB Database 106
Figure 90: IXM WEB - Select Database Name 107
Figure 91: IXM WEB - Broadcast Option 109
Figure 92: IXM WEB - Broadcast Wiegand Output Settings 109
Figure 93: IXM WEB - Broadcast to Devices 110
Figure 94: IXM WEB - OSDP Settings 111
Figure 95: IXM WEB - Save OSDP Settings 114
Figure 96: IXM WEB - Edit Device Options 114
Figure 97: GCC - Device ID 115

Figure 98: GCC - Setup OSDP reader 115
Figure 99: IXM WEB - Disable Panel Feedback.. 116
Figure 100: IXM WEB - MIFARE DESFire Configuration 117
Figure 101: IXM WEB - MIFARE DESFire Sample Configuration... 119
Figure 102: Earth Ground Wiring 120
Figure 103: IXM TITAN – Top & Bottom Connector Wiring 121
Figure 104: Power, Wiegand & OSDP Wires 122
Figure 105: IXM TITAN - Wiegand 123
Figure 106: IXM TITAN - Panel Feedback 124
Figure 107: IXM TITAN - OSDP Connections 125
Figure 108: IXM WEB - Server URL Setting.. 126
Figure 109: IXM WEB - Server URL Setting from General Settings 127
Figure 110: IXM WEB - Thermal Authentication Wiegand Output Event 128
Figure 111: IXM WEB - Enable Device Logs.. 129
Figure 112: Save Device Log File 129

List of Tables

Table 1: Compatibility Matrix for IXM WEB & Gallagher Integration 12
Table 2: Task List Summary 14
Table 3: System Related Checklist 35
Table 4: Port Information 35
Table 5: IXM WEB - OSDP Configuration Options 113
Table 6: IXM WEB - OSDP Text Options 113
Table 7: IXM WEB – MIFARE DESFire Configuration Options... 119
Table 7: Logs Folder Location.. 130

1. Introduction

Purpose

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

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

- C12873Invixium license instead of REST API to support GCC integration
- Enrollment status PDF
- Temperature unit selection for sending alarm events to GCC
- 'Sync All' feature to resynchronize the database from GCC to IXM WEB
- MIFARE DESFire custom layout to support Gallagher access card

Description

IXM Link, a licensed module in IXM WEB, is required to synchronize the user database between IXM WEB (where biometric enrollment for users is performed) and Gallagher Command Centre Software (where access rules for the users and the organization are managed).

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

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

Acronyms

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

Field Mappings

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

GCC Field	IXM Field	Notes
First name	First Name	
Last name	Last Name	
Division	Department	This is mandatory when adding or editing users from IXM WEB.
Authorized	Suspend Employee	
Number (CardholderCards Tile)	Number (Card)	This is mandatory when adding users to GCC from IXM WEB.
Issue (CardholderCards Tile)	Issue Level (Card)	This is mandatory when adding or editing users from IXM WEB. Max issue-level value supported by GCC is 15.
Card Type (CardholderCards Tile)	Card Type (Card)	This is mandatory when adding or editing users from IXM WEB. Not able to change card type while editing user from IXM WEB.
Facility Code(Card Type)	Facility Code (Card)	This will be disabled by default. When you select card type from IXM WEB, the Facility Code will populate automatically. From Card Type, only the Facility Code is imported to IXM WEB. Region Code is not imported from Card Type.
From	Activation Date (Card)	
Until	Expiry Date (Card)	
Status	Status (Card)	Active, Lost, and Stolen states are mapped with IXM WEB. Others will be inactive in IXM WEB. Not Yet Activated in GCC will display as active with future dates in IXM WEB.
Access Group	User Group / Device Group / Sync Group	Setting Map Access Group to YES in configuration will create an employee group, device group, and sync group in IXM WEB. Further employees imported from GCC will be added to this created employee group and will be used for automatic transfer to IXM devices. Refer to separate Feature Description Documents (FDDs) accessible from Invixium Customer Portal for details on Employee/Device/Sync Groups.

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

2. Compatibility

Invixium Readers

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

Software Requirements

Application	**Version**
Gallagher Command Centre	v9.0
Invixium IXM WEB	3.0.36.0
Operating Systems	Windows Server 2016 Standard Windows Server 2019 Windows 11 Pro Windows 10 Professional Version
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 & Command Centre Integration

IXM WEB version	Command Centre version	Compatible
IXM WEB 2.2.57.0	v8.40	Yes
IXM WEB 2.2.57.0	v8.50	Yes
IXM WEB 2.2.224.0	v8.40	No
IXM WEB 2.2.224.0	v8.50	No
IXM WEB 2.2.224.0	v8.50 (with patch*)	Yes
IXM WEB 2.2.224.0	v8.60	Yes
IXM WEB 2.2.230.0	v8.60	Yes
IXM WEB 2.2.252.0	v8.60	Yes
IXM WEB 2.2.330.0	v8.60	Yes
IXM WEB 2.3.2.0	v8.60	Yes
IXM WEB 2.3.2.0	v8.80	Yes
IXM WEB 3.0.36.0	v9.0	Yes

Table 1: Compatibility Matrix for IXM WEB & Gallagher Integration

3. Checklist

Item List	Interface
URL Enrollment PDF and Access Group	Gallagher
REST API Client	Gallagher
IXM WEB Activation ID	Invixium
SQL Instance on SQL Server 2016+	Invixium
Install IXM WEB Application	Invixium
IXM WEB and IXM Link Activation	Invixium
Configure IXM Link to Gallagher	Invixium
Configure Invixium Reader	Invixium
Configure Logical Events	Gallagher
Face or Finger Enrollment	Invixium

4. Task List Summary

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

Table 2: Task List Summary

5. Prerequisites for GCC and IXM WEB Integration

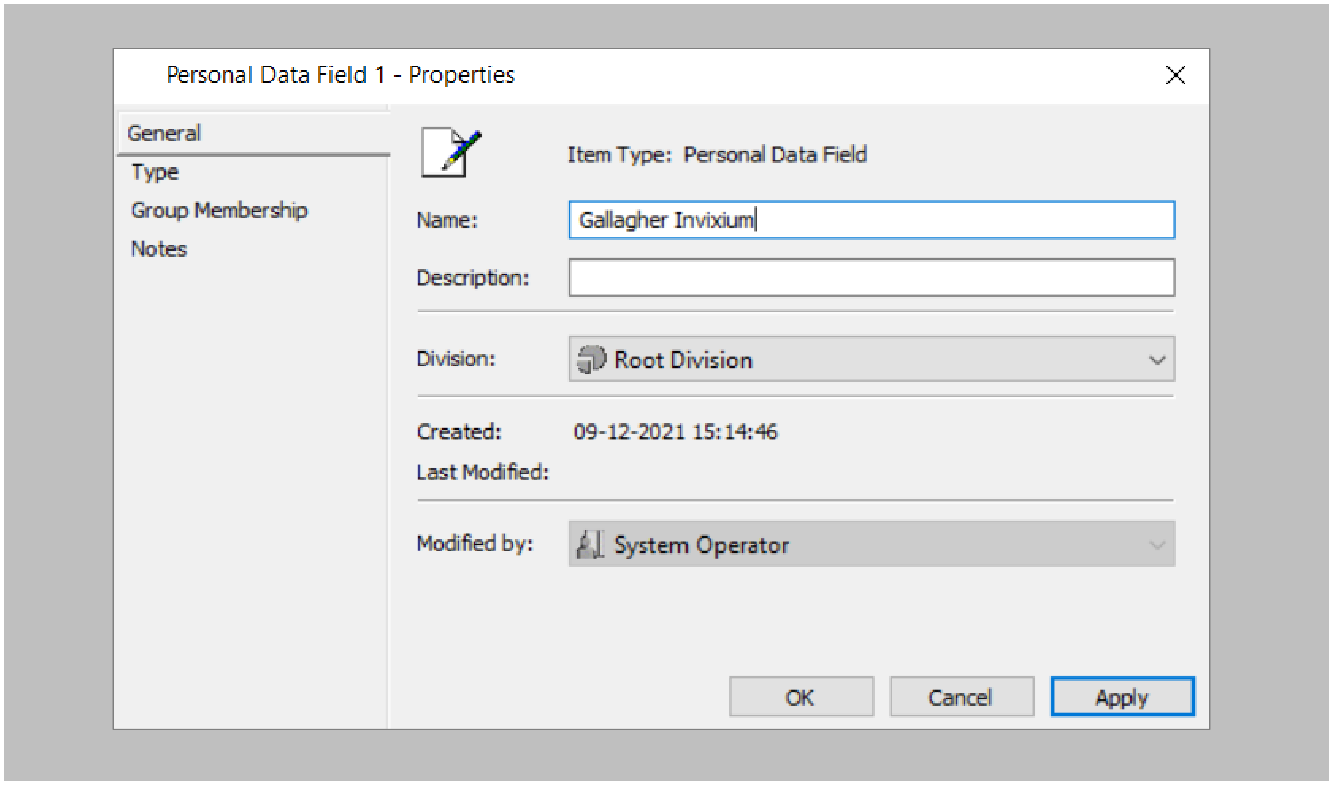
URL Enrollment PDF (Personal Data Field)

Procedure

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

STEP 1

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


Personal Data Field 1 - Properties

Item Type: Personal Data Field

Name: Gallagher Invixium

Description:

Division: Root Division

Created: 09-12-2021 15:14:46

Last Modified:

Modified by: System Operator

Figure 1: GCC - Personal Data Field 1 Properties

STEP 2

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

STEP 3

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

STEP 4

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

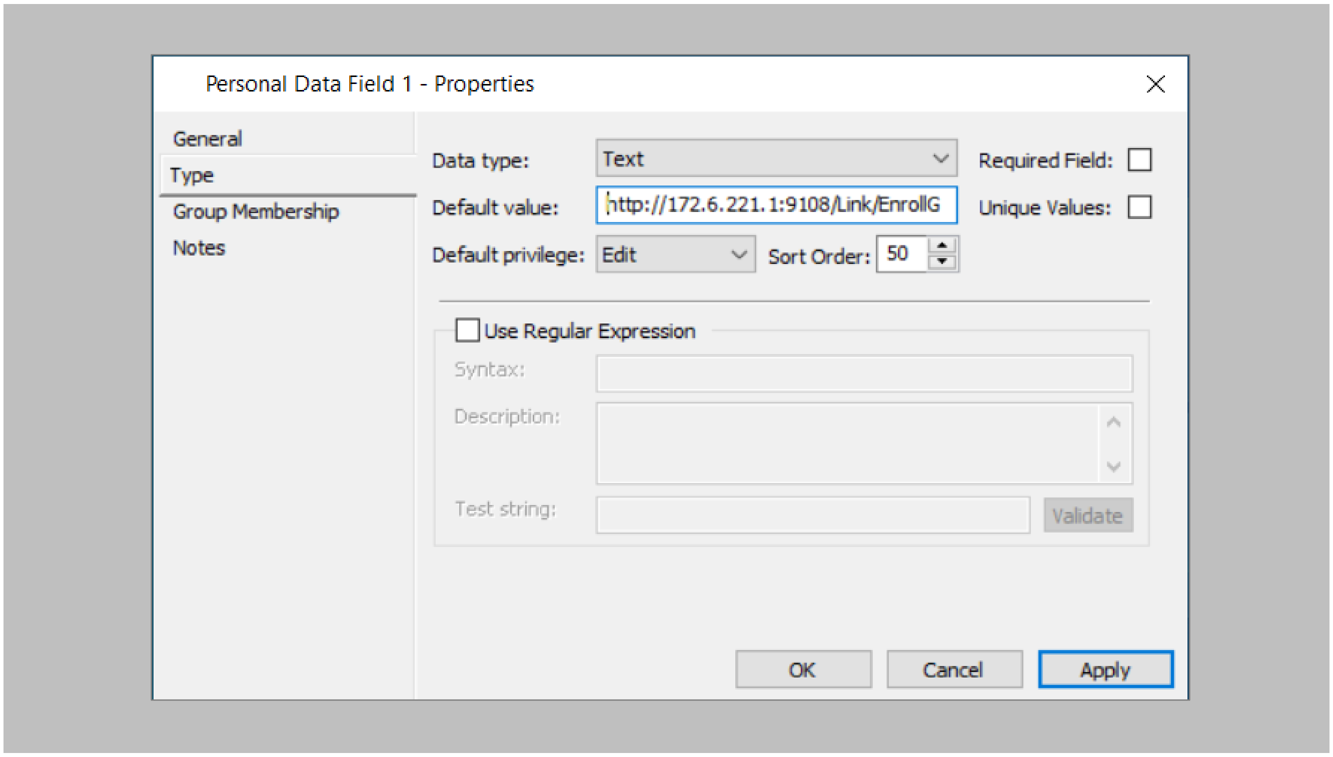
http://[IXM WEB Server IP:Port]/Link/EnrollGallagherUser/

For example:

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

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

Enable the **Required Field** checkbox.



Personal Data Field 1 - Properties

Data type: Text

Default value: http://172.6.221.1:9108/Link/EnrollG

Default privilege: Edit

Sort Order: 50

Required Field: □

Unique Values: □

□ Use Regular Expression

Syntax:

Description:

Test string:

Figure 2: GCC - Gallagher Invixium Properties

STEP 5

Click **OK.**

STEP 6

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

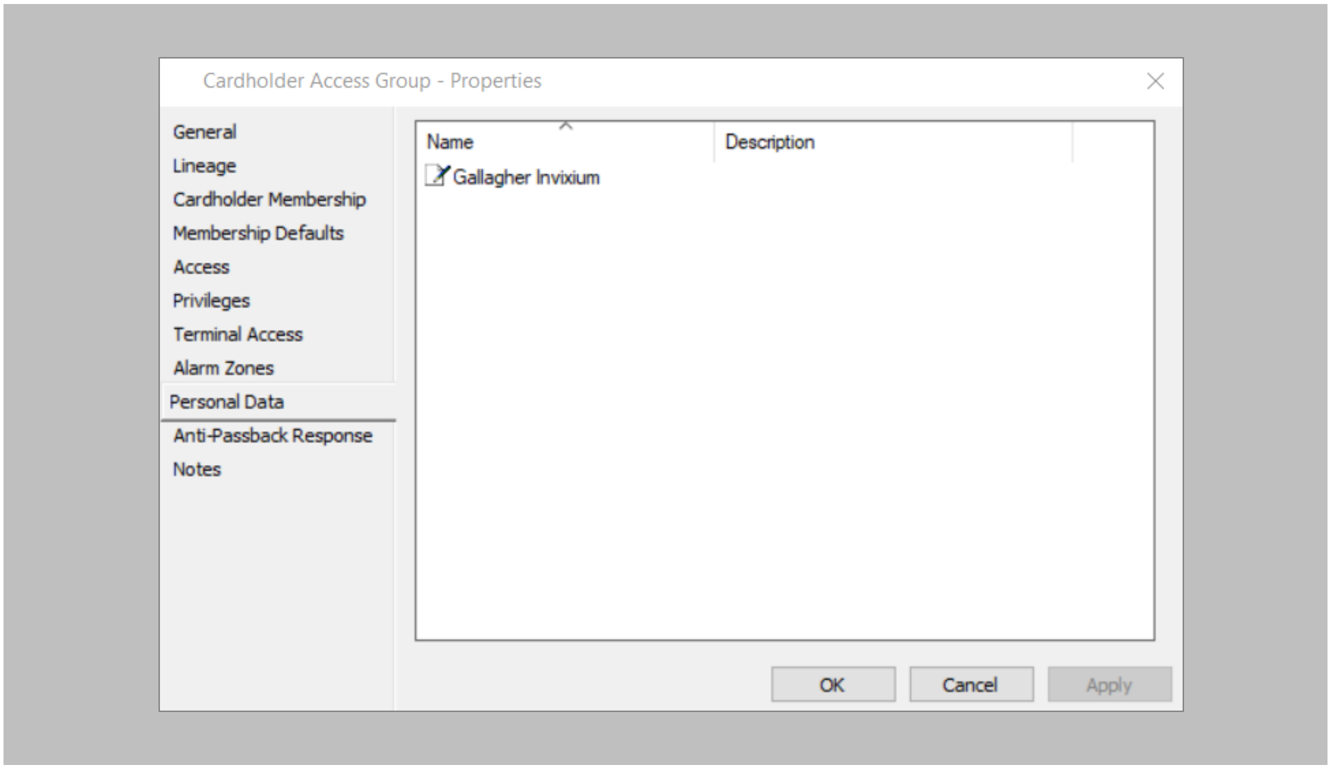


Figure 3: GCC - Cardholder Access Group Properties

STEP 7

Click **OK.**

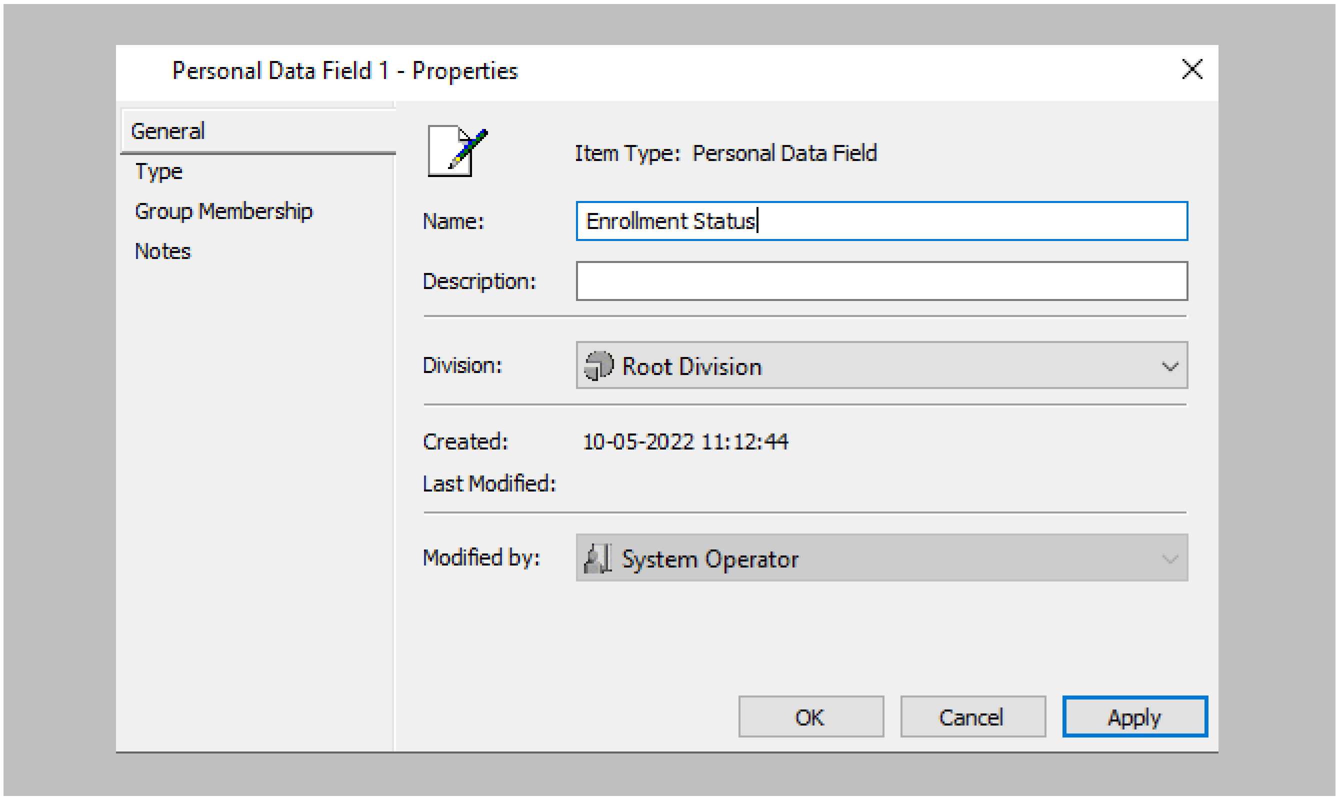
Enrollment Status PDF (Personal Data Field)

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

Procedure

STEP 1

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



Personal Data Field 1 - Properties

Item Type: Personal Data Field

Name: Enrollment Status

Description:

Division: Root Division

Created: 10-05-2022 11:12:44

Last Modified:

Modified by: System Operator

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

STEP 2

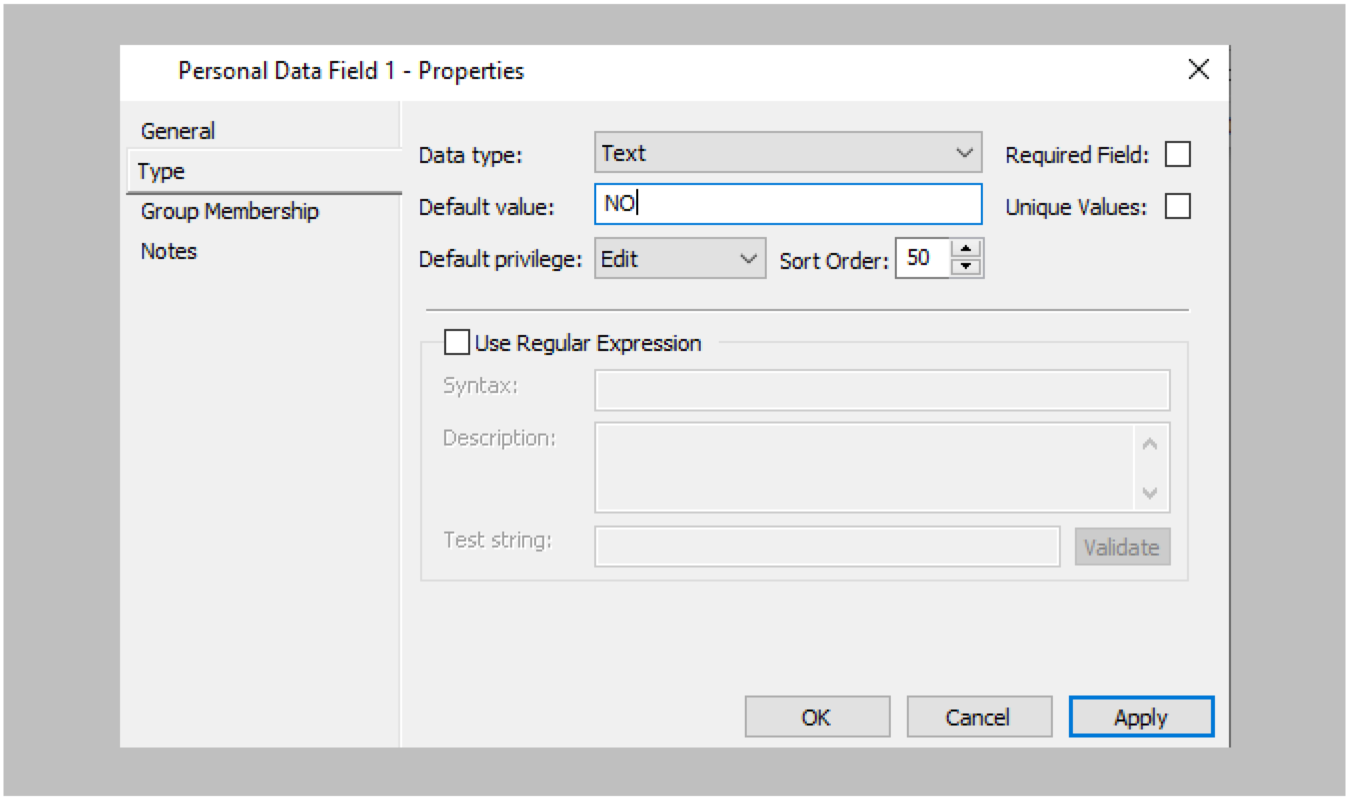
Enter a **Name** and **Description** (optional).

STEP 3

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

STEP 4

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



Personal Data Field 1 - Properties

Data type: Text

Default value: NO

Default privilege: Edit

Sort Order: 50

Required Field: □

Unique Values: □

□ Use Regular Expression

Figure 5: GCC – Enrollment Status Properties

STEP 5

Click **OK.**

STEP 6

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

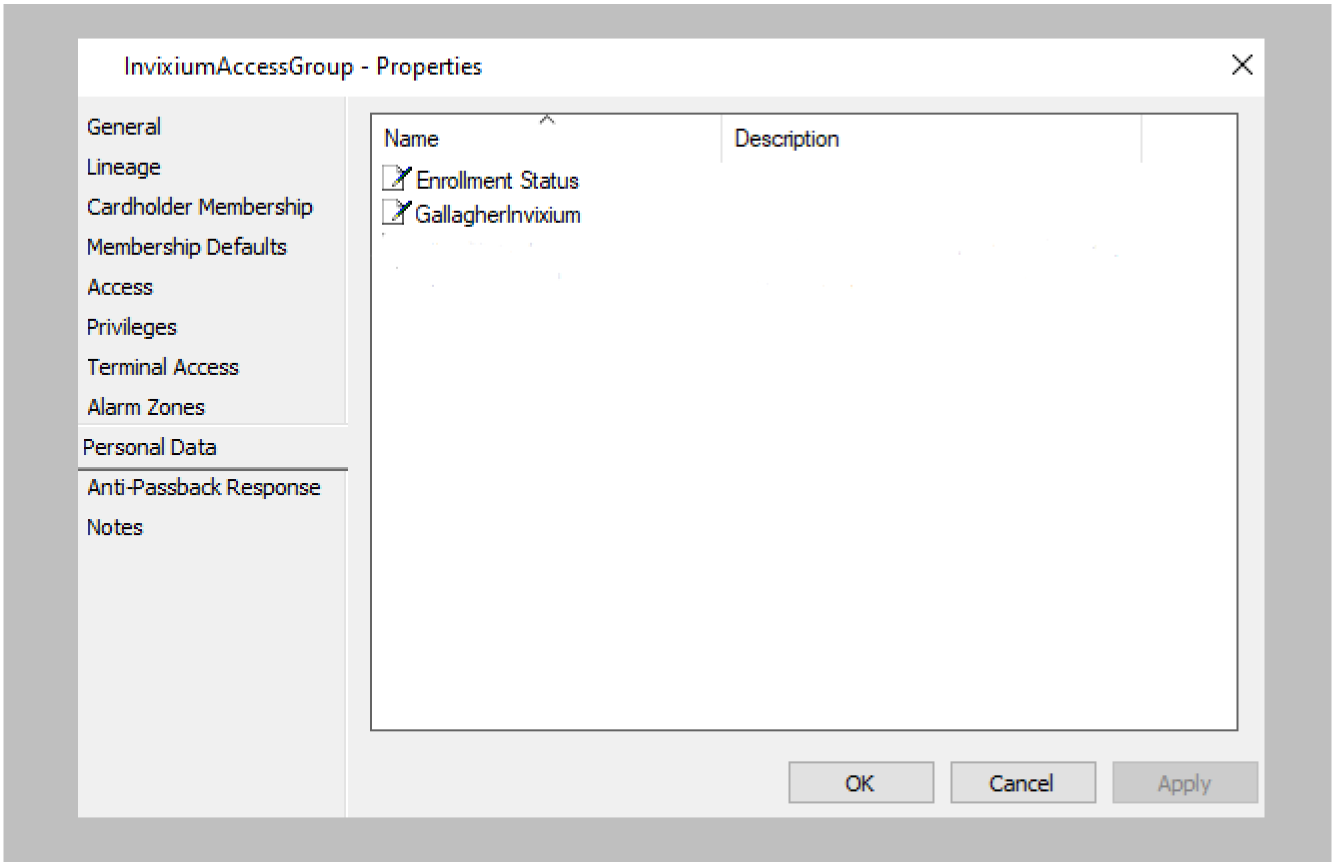


Figure 6: GCC - Cardholder Access Group Properties

STEP 7

Click **OK.**

Cardholder Access Group

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

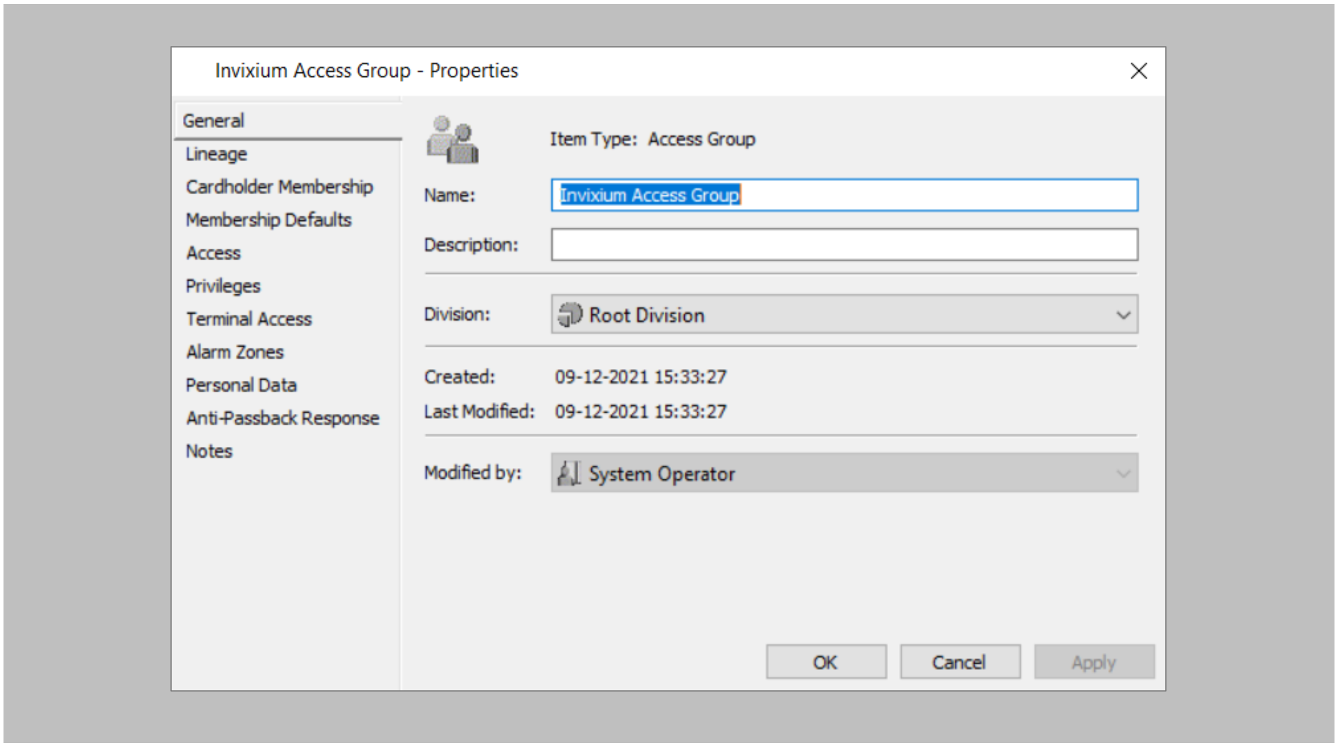
Procedure

STEP 1

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

STEP 2

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



Invixium Access Group - Properties

Item Type: Access Group

Name: Invixium Access Group

Description:

Division: Root Division

Created: 09-12-2021 15:33:27

Last Modified: 09-12-2021 15:33:27

Modified by: System Operator

Figure 7: GCC - Invixium Access Group Properties

STEP 3

Click **OK.**

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

Enabling the Invixium License for IXM WEB in Command Centre

What you will need:

- **C12873Invixium**
- REST API String

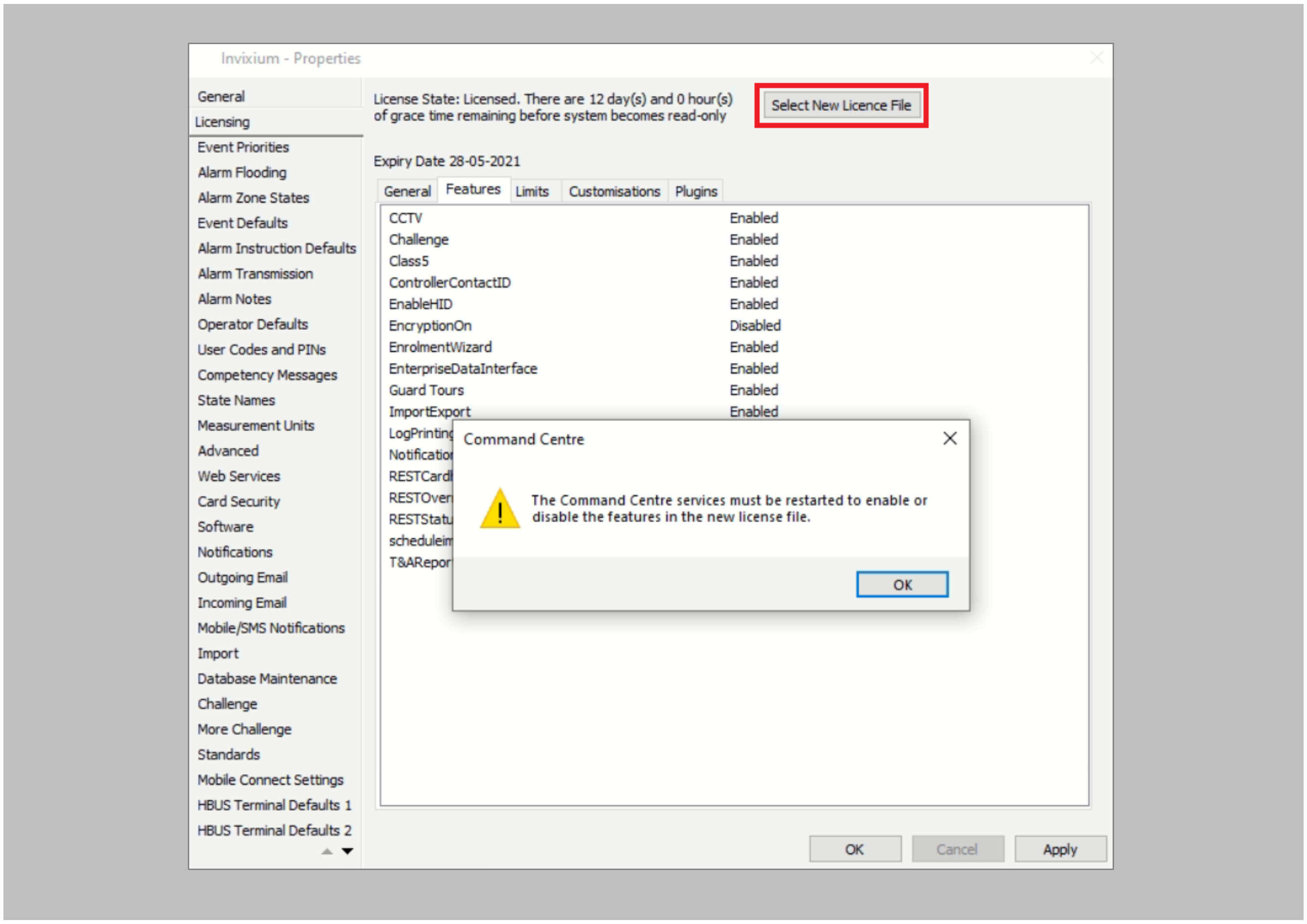
Note: C12873 is the Gallagher License required for integration with IXM WEB v2.2.224.0 onwards.

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

Procedure

STEP 1

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



License State: Licensed. There are 12 day(s) and 0 hour(s) of grace time remaining before system becomes read-only

Expiry Date 28-05-2021

CCTV	Enabled
Challenge	Enabled
Class5	Enabled
ControllerContactID	Enabled
EnableHID	Enabled
EncryptionOn	Disabled
EnrolmentWizard	Enabled
EnterpriseDataInterface	Enabled
Guard Tours	Enabled
ImportExport	Enabled
LogPrinting	
Notificatio	
RESTCard	
RESTOver	
RESTStatu	
scheduleim	
T&ARepor	

Command Centre

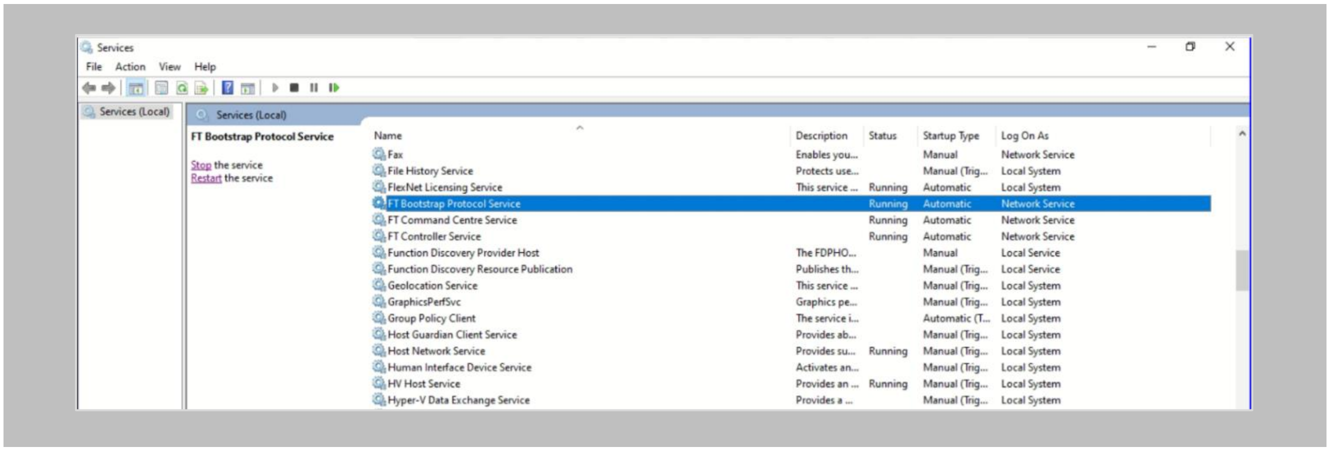
The Command Centre services must be restarted to enable or disable the features in the new license file.

OK

Figure 8: GCC – Invixium License for IXM WEB

STEP 2

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

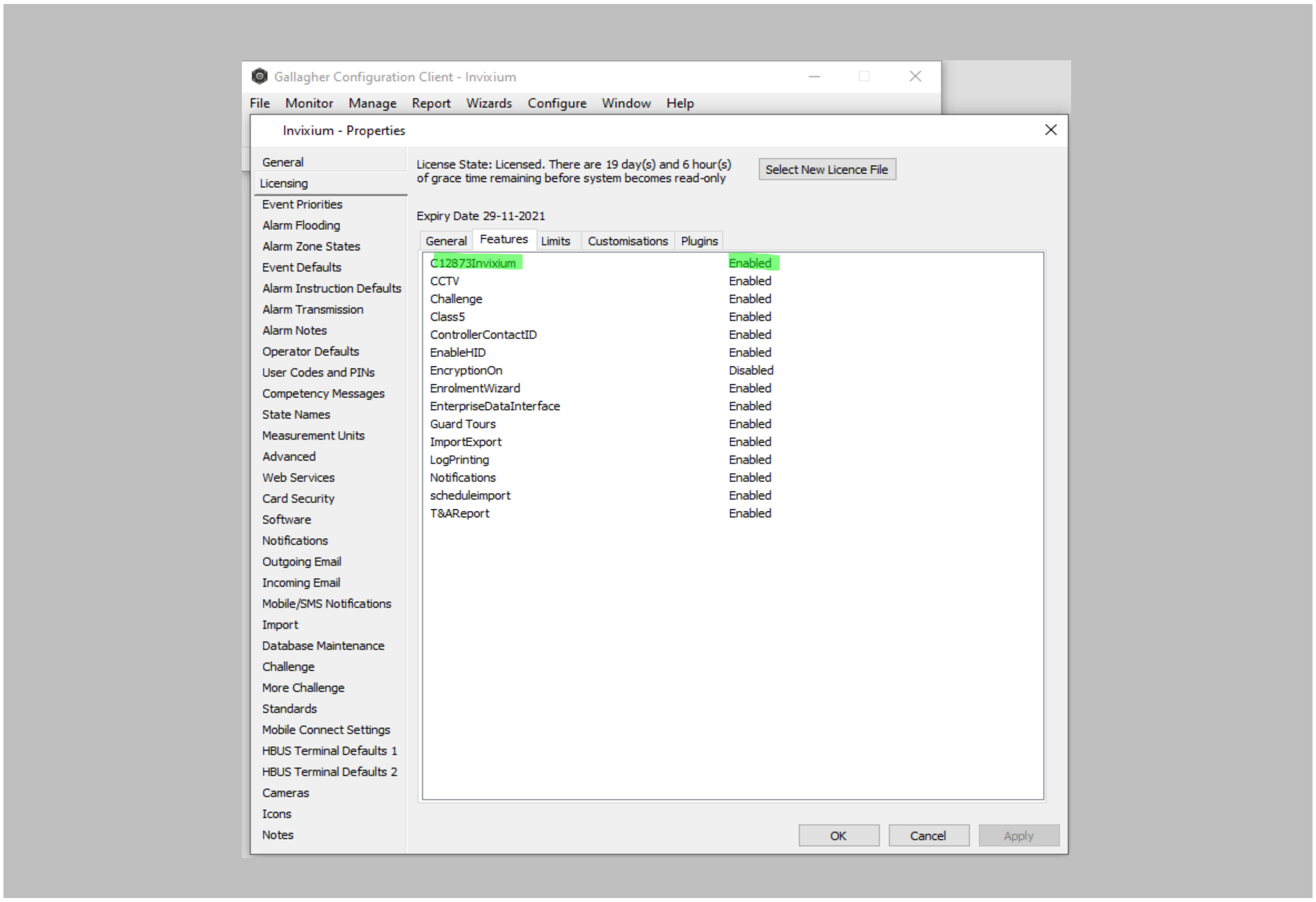


FT Bootstrap Protocol Service

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Fax	Enables you...		Manual	Network Service
File History Service	Protects use...		Manual (Trig...	Local System
FlexNet Licensing Service	This service ...	Running	Automatic	Local System
FT Bootstrap Protocol Service		Running	Automatic	Network Service
FT Command Centre Service		Running	Automatic	Network Service
FT Controller Service		Running	Automatic	Network Service
Function Discovery Provider Host	The FDPHO...		Manual	Local Service
Function Discovery Resource Publication	Publishes th...		Manual (Trig...	Local Service
Geolocation Service	This service ...		Manual (Trig...	Local System
GraphicsPerfSvc	Graphics pe...		Manual (Trig...	Local System
Group Policy Client	The service i...		Automatic (T...	Local System
Host Guardian Client Service	Provides ab...		Manual (Trig...	Local System
Host Network Service	Provides su...	Running	Manual (Trig...	Local System
Human Interface Device Service	Activates an...		Manual (Trig...	Local System
HV Host Service	Provides an ...	Running	Manual (Trig...	Local System
Hyper-V Data Exchange Service	Provides a ...		Manual (Trig...	Local System

Figure 9: GCC - Restart GCC Services



License State: Licensed. There are 19 day(s) and 6 hour(s) of grace time remaining before system becomes read-only

Expiry Date 29-11-2021

C12873Invixium	Enabled
CCTV	Enabled
Challenge	Enabled
Class5	Enabled
ControllerContactID	Enabled
EnableHID	Enabled
EncryptionOn	Disabled
EnrolmentWizard	Enabled
EnterpriseDataInterface	Enabled
Guard Tours	Enabled
ImportExport	Enabled
LogPrinting	Enabled
Notifications	Enabled
scheduleimport	Enabled
T&AReport	Enabled

Figure 10: GCC – C12873Invixium License Enabled

REST API Client

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

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

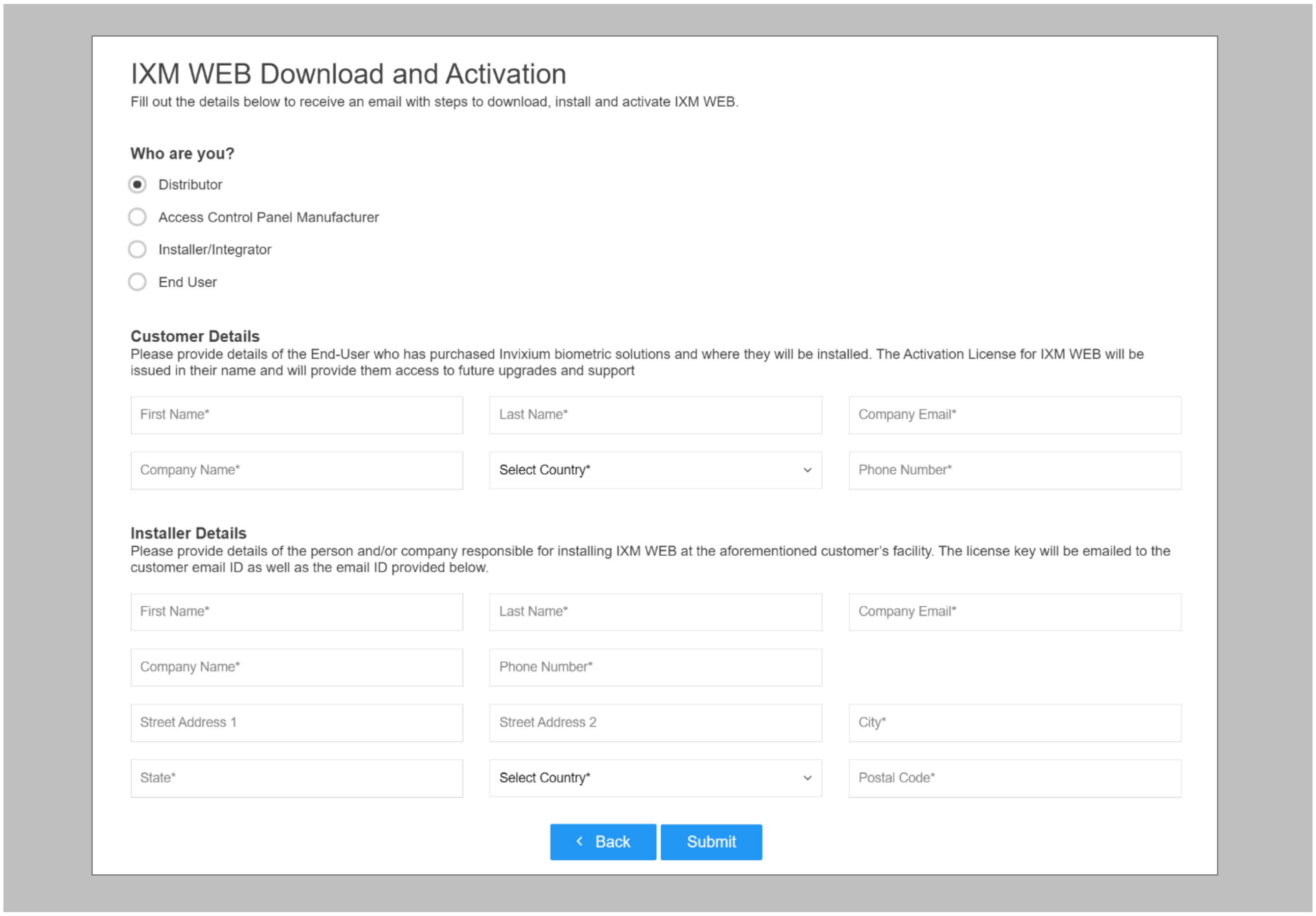
6. Prerequisites for Installing Invixium IXM WEB Software

Acquiring IXM WEB Activation Key

Procedure

STEP 1

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



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.

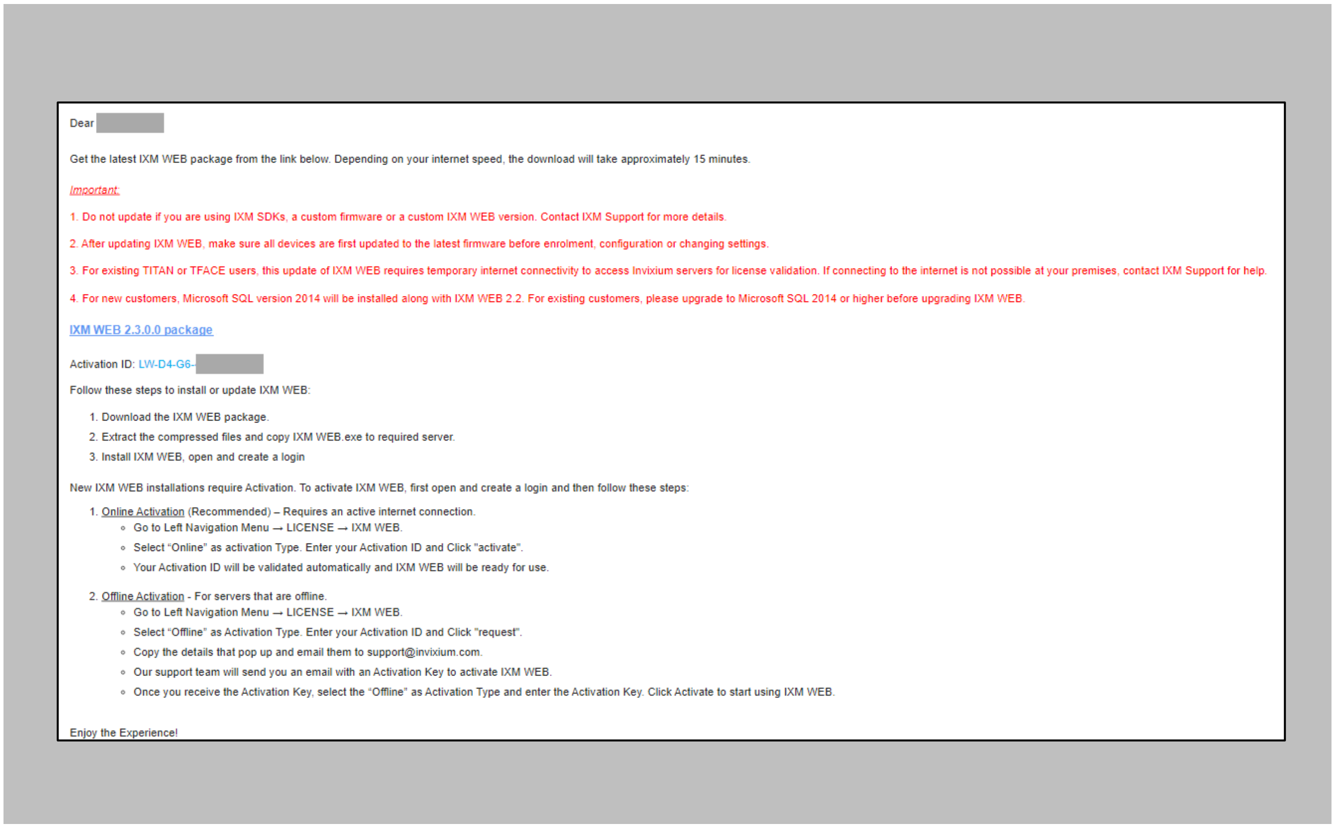
First Name*	Last Name*	Company Email*
Company Name*	Phone Number*	
Street Address 1	Street Address 2	City*
State*	Select Country*	Postal Code*

Figure 11: IXM WEB Online Request Form

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

Please ensure to check the spam or junk folder.

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



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 12: Sample Email After Submitting Online Request Form

Setting Up SQL instance

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

Procedure

STEP 1

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

STEP 2

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

STEP 3

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

STEP 4

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

STEP 5

Log into the new instance and create a new user.

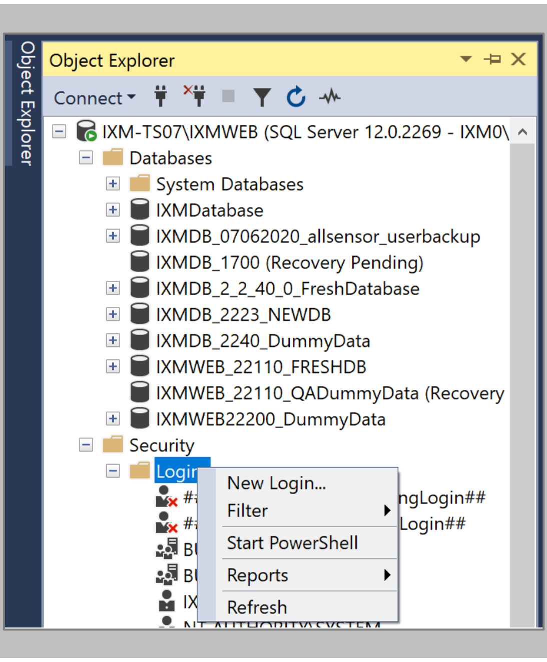
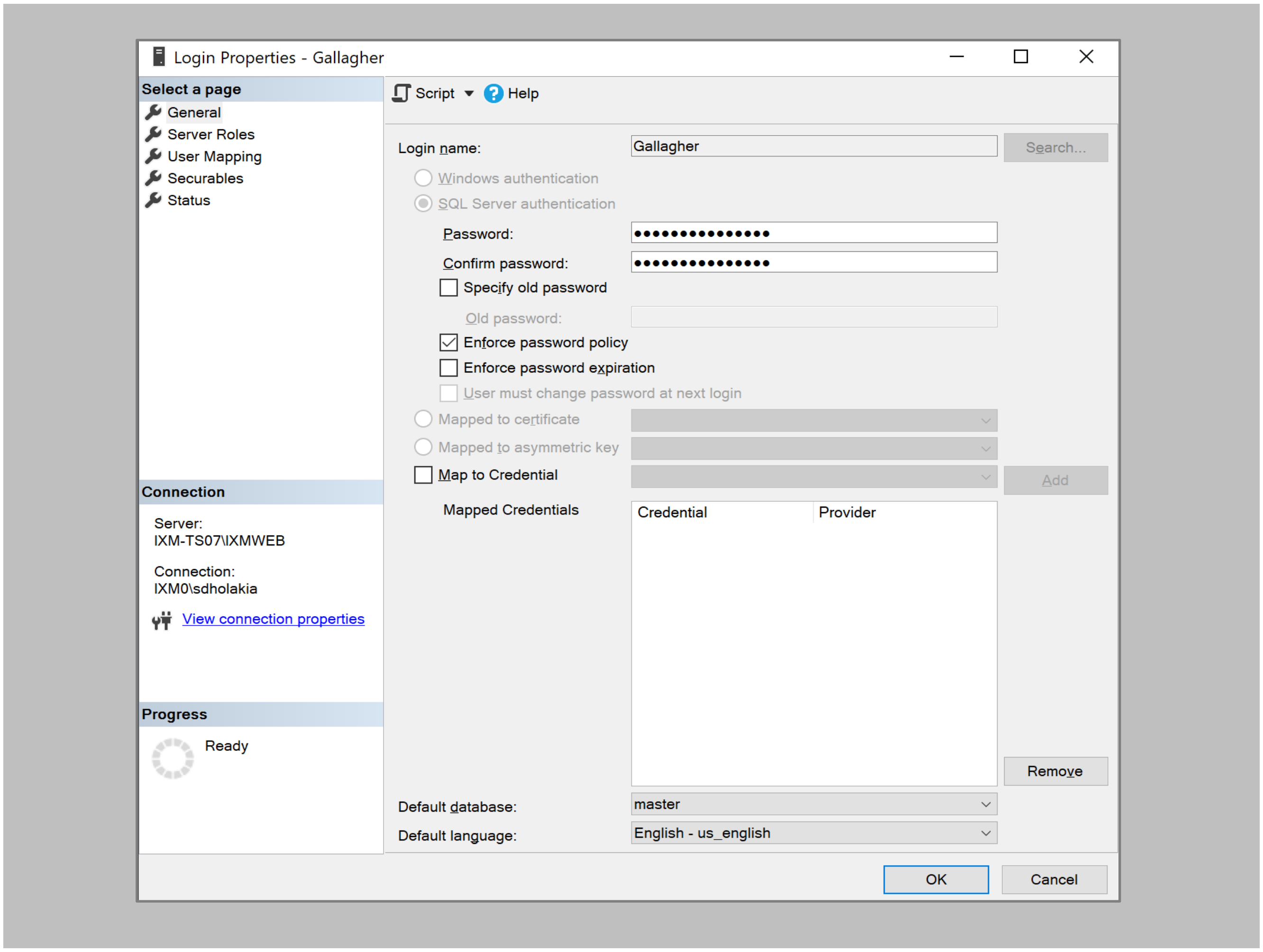


Figure 13: SQL New Login

STEP 6

Select **SQL Server authentication.**

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



Login Properties - Gallagher

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Script ▾ Help

Login name: Gallagher [Search...]

○ 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 [Add]

Mapped Credentials

Credential	Provider

[Remove]

Default database: master

Default language: English - us_english

Connection

Server:
IXM-TS07\IXMWEB

Connection:
IXM0\sdholakia

View connection properties

Progress

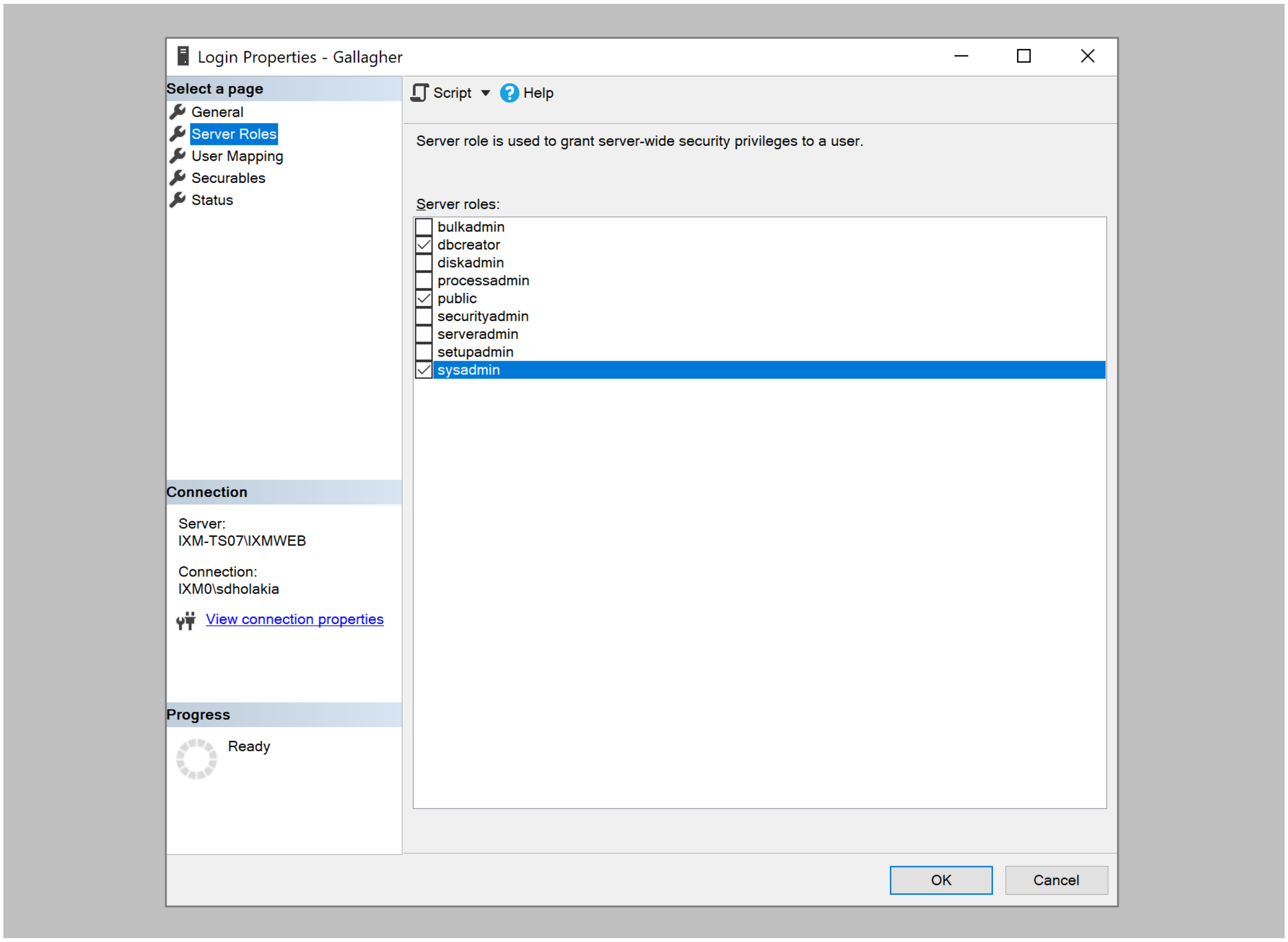
Ready

[OK] [Cancel]

Figure 14: SQL Login Properties

STEP 7

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



Login Properties - Gallagher

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Script ▾ Help

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

Server roles:

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

Connection

Server:
IXM-TS07\IXMWEB

Connection:
IXM0\sdholakia

View connection properties

Progress

Ready

Figure 15: SQL Server Roles

RESULT

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

Minor Checklist and Considerations

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

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

Table 3: System Related Checklist

Port Assignment	**Port**
Inbound HTTP Port	9108
TCP	1433
Port to communicate between IXM WEB & Devices	9734
Inbound Port	1255
GCC REST API Port	8904 (default)

Table 4: Port Information

7. Installing IXM WEB

Software Install

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator).

Select **Advanced.**

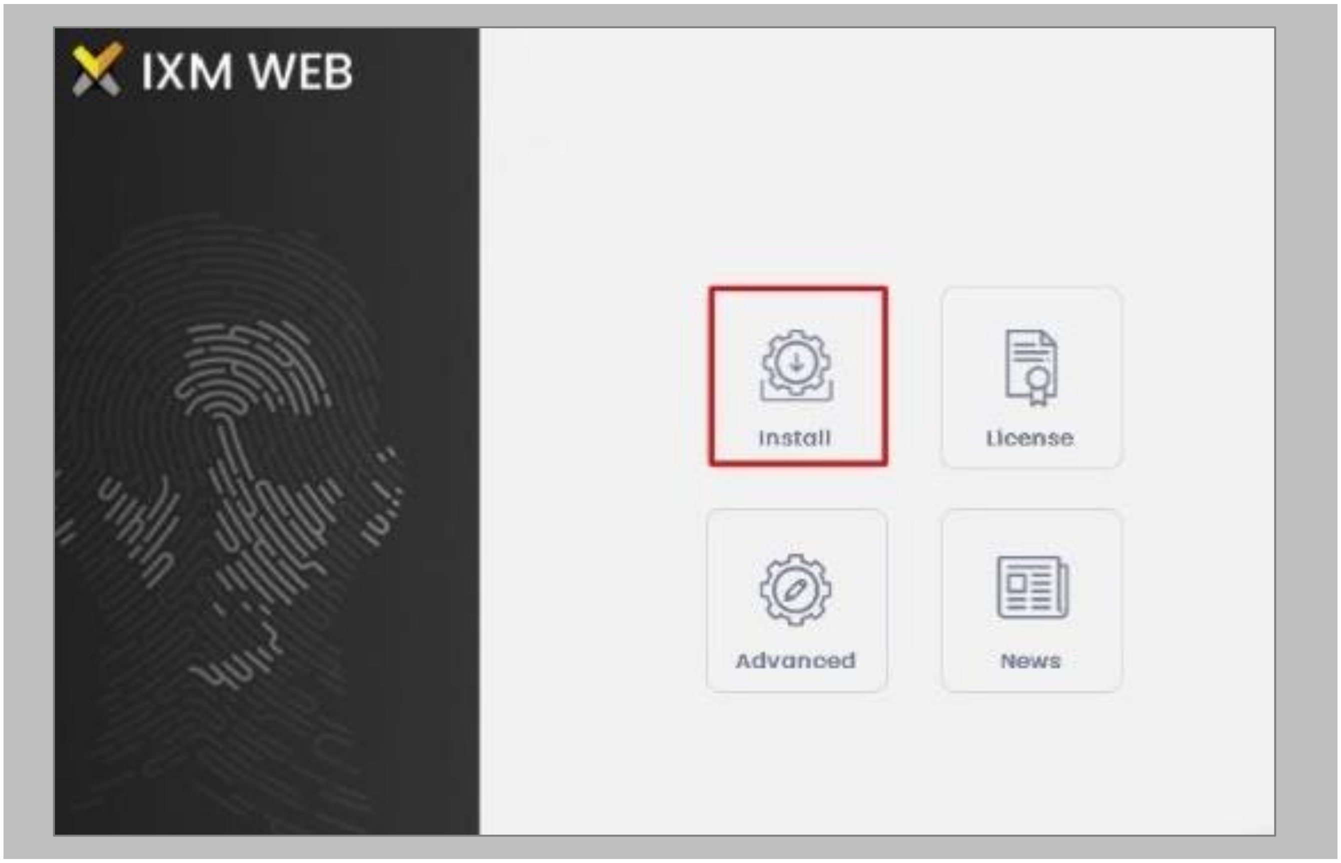
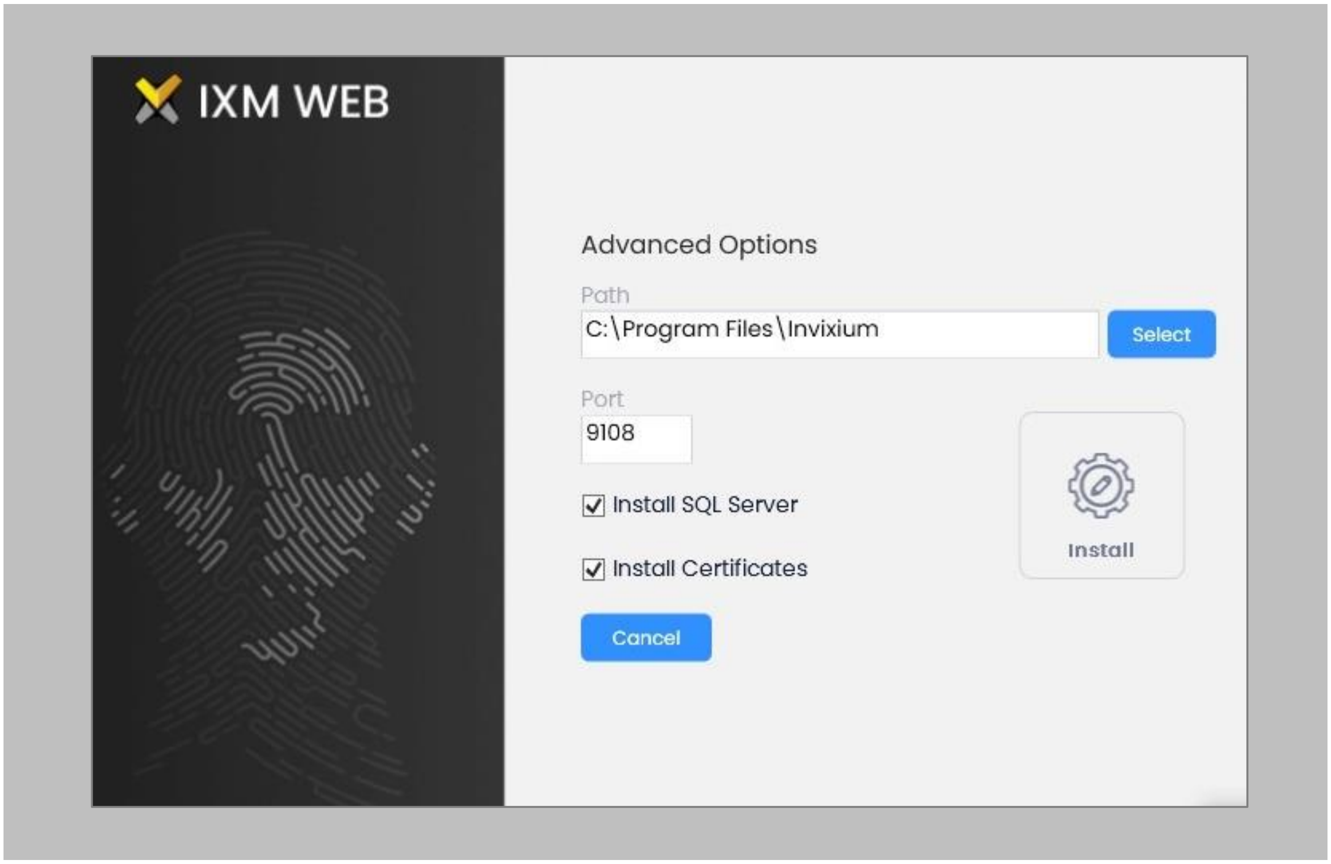


Figure 16: IXM WEB Installer

STEP 2

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



Advanced Options

Path

C:\Program Files\Invixium

Port

9108

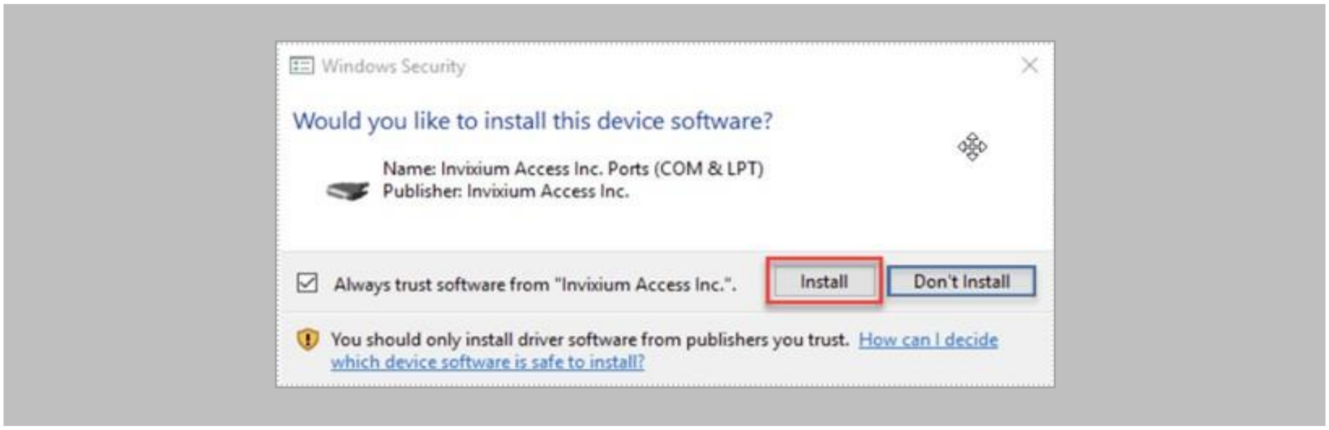
☑ Install SQL Server

☑ Install Certificates

Figure 17: Advanced Options in IXM WEB Installer

STEP 3

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



Windows Security

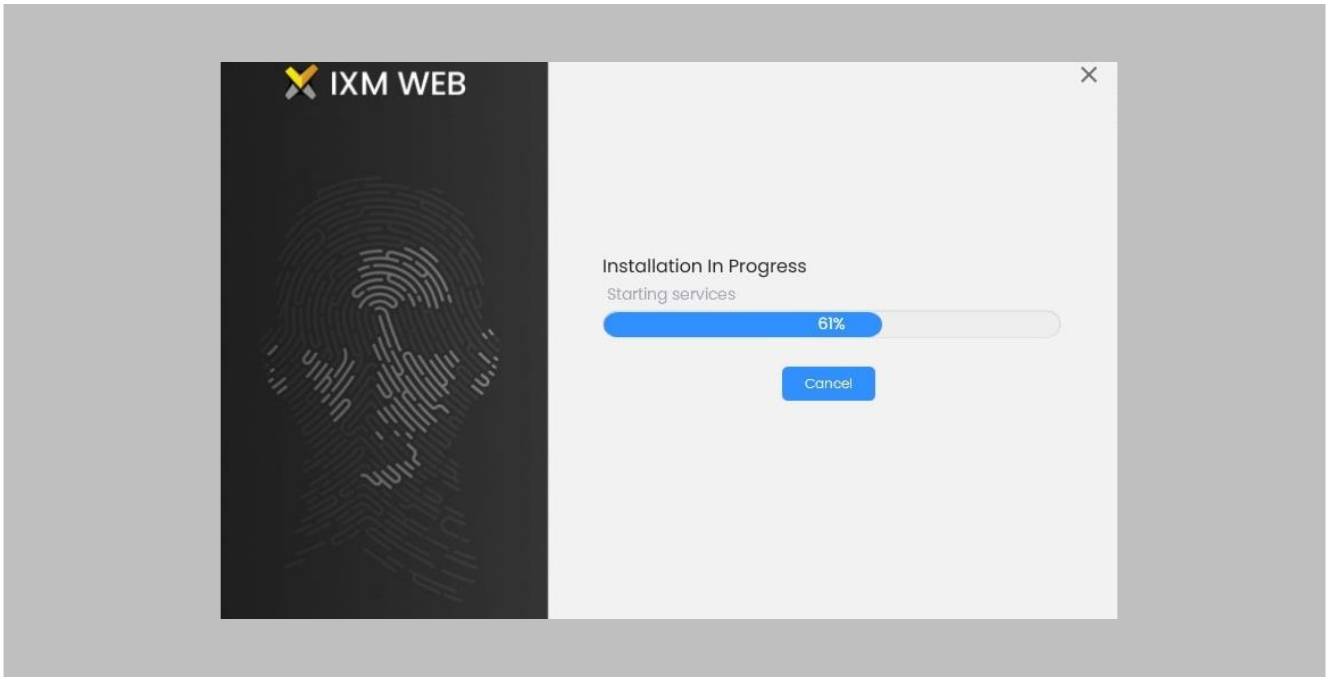
Would you like to install this device software?

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 18: Invixium Fingerprint Driver Installation Message



Installation In Progress

Starting services

Figure 19: IXM WEB Installation Progress

STEP 4

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

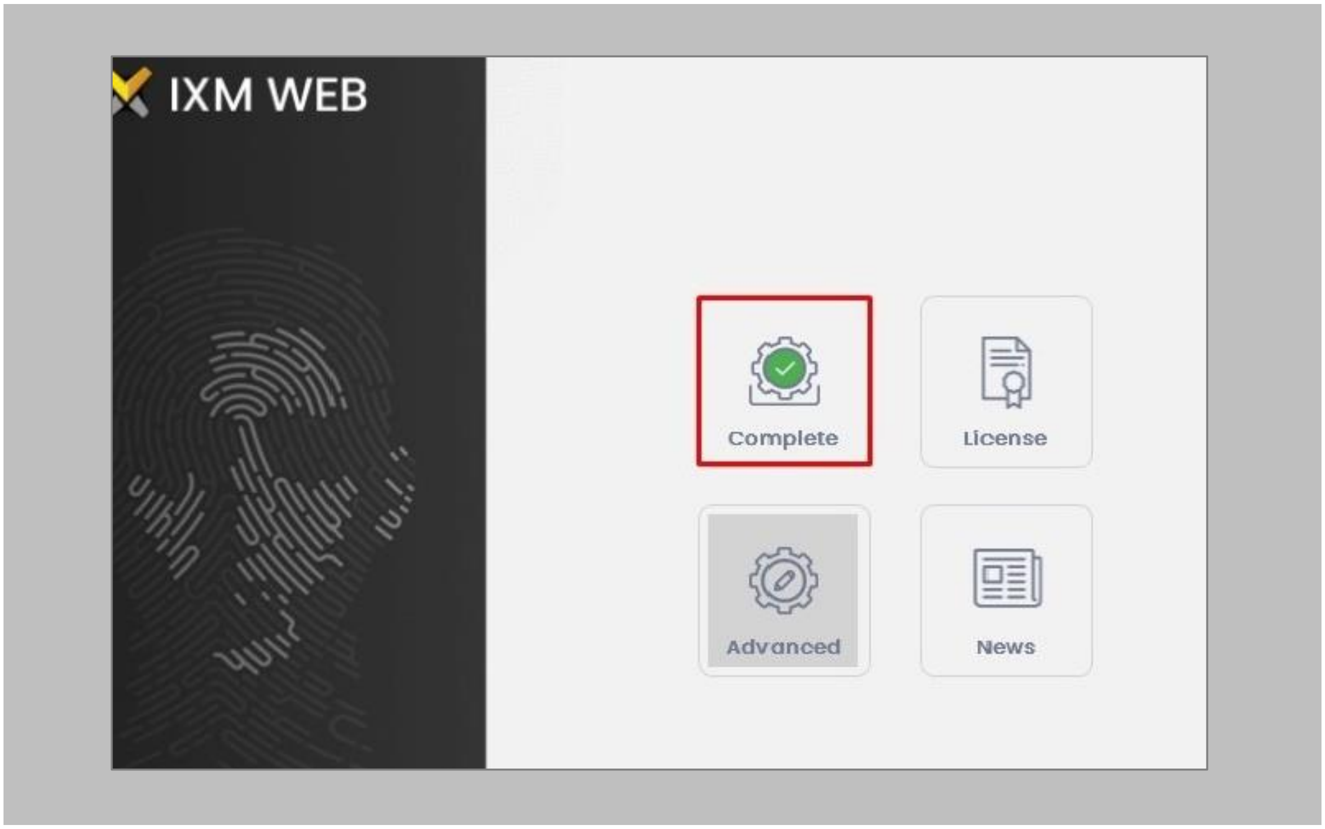


Figure 20: IXM WEB Installation Completed

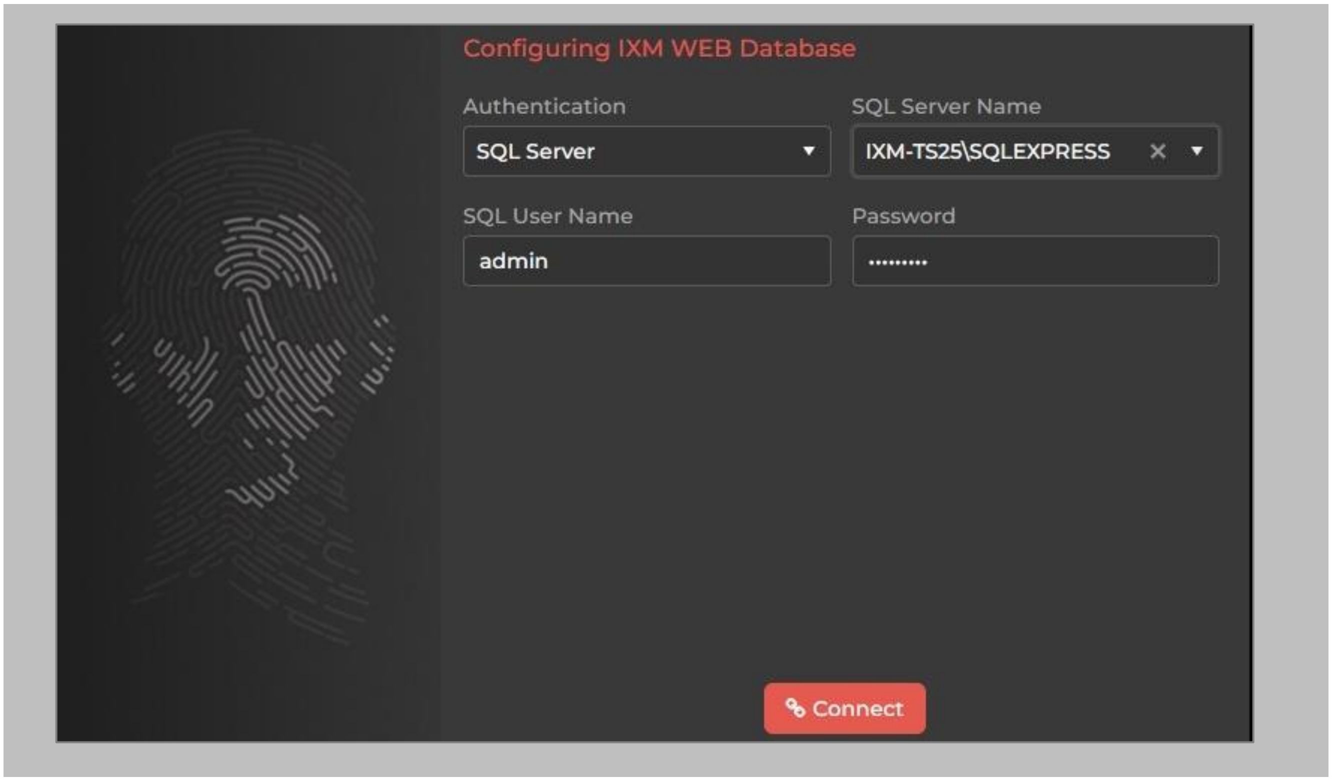
Click on the **X** in the upper right corner to close.

STEP 5

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

Figure 21: IXM WEB Icon - Desktop Shortcut

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



Configuring IXM WEB Database

Authentication: SQL Server

SQL Server Name: IXM-TS25\SQLEXPRESS

SQL User Name: admin

Password: •••••••••

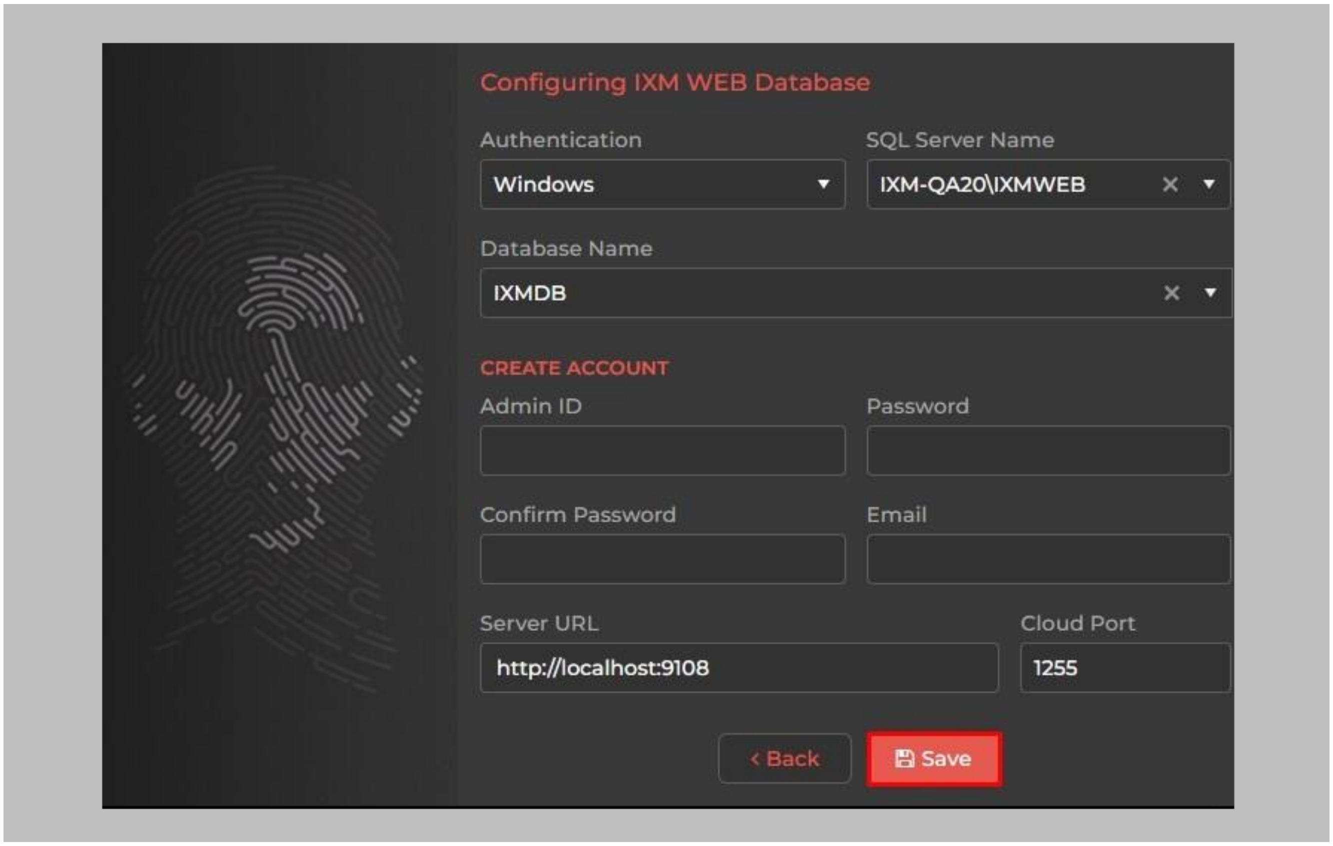
Figure 22: IXM WEB Database Configuration

STEP 6

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

STEP 7

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



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 23: IXM WEB Administrator User Configuration

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

STEP 8

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

STEP 9

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

For example:

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

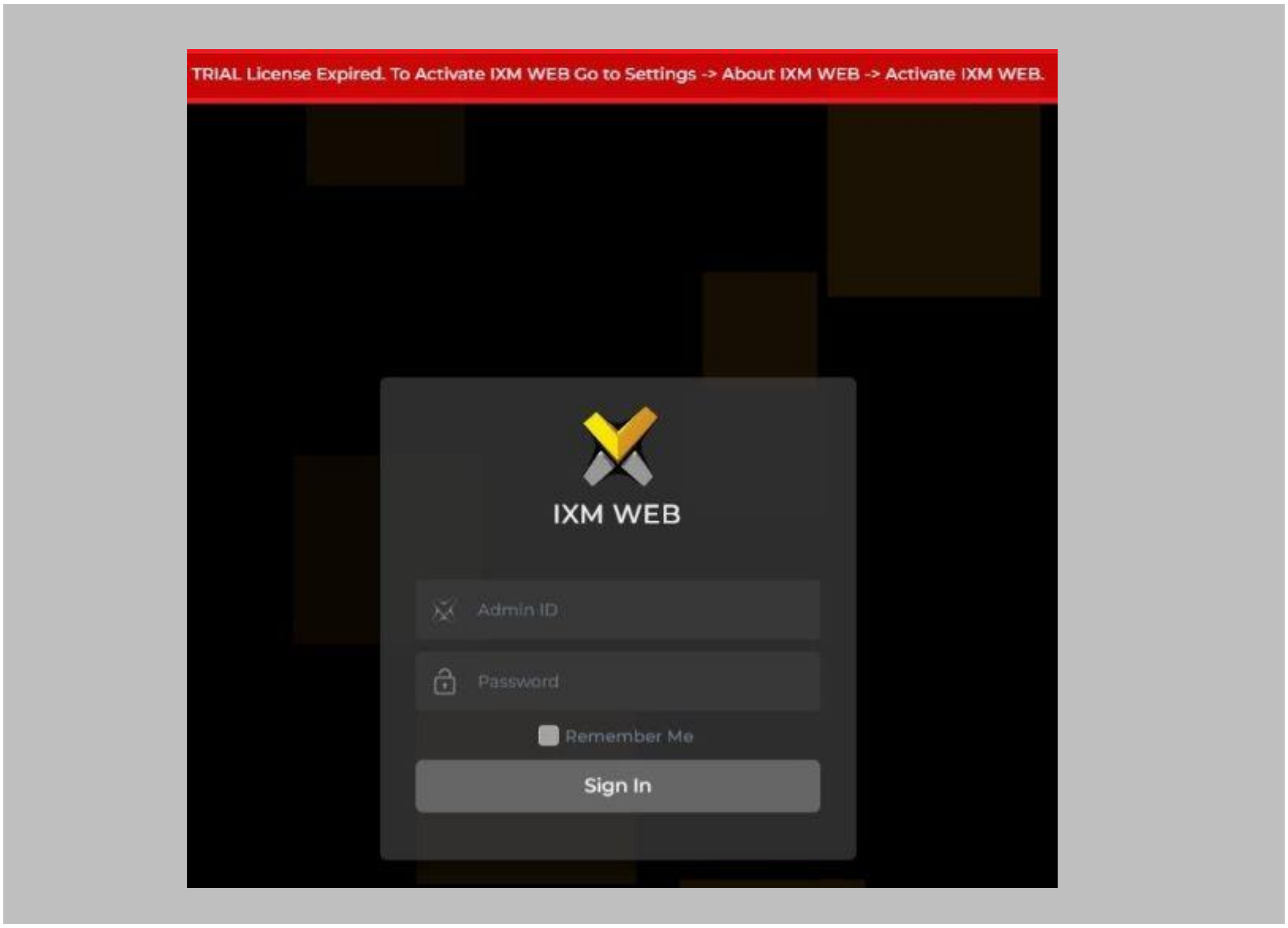
http://192.168.1.100:9108

STEP 10

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

STEP 11

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



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

Figure 24: 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

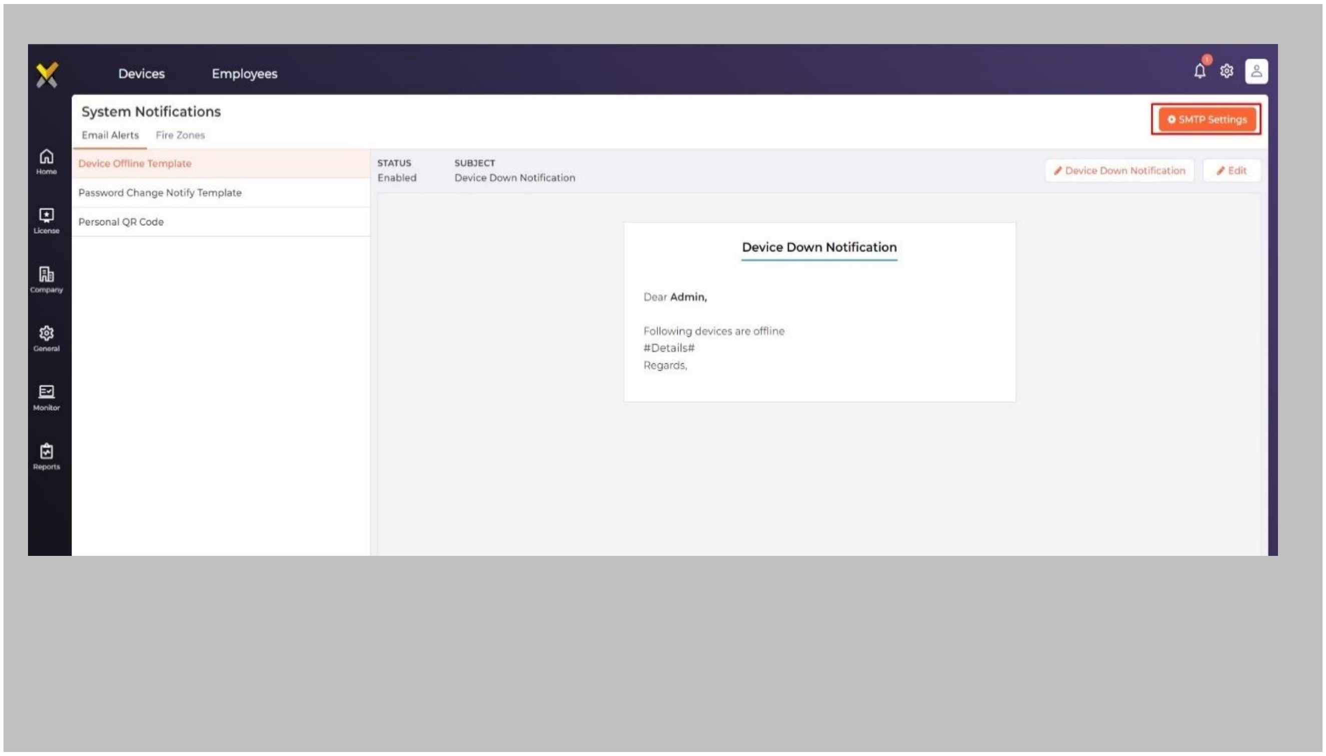
Configuring Email settings is highly recommended as one of the first steps after installing IXM WEB. Email configuration settings will help the admin retrievie the password for IXM WEB in case it is forgotten. In addition, having email settings configured also makes activation and license key requests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

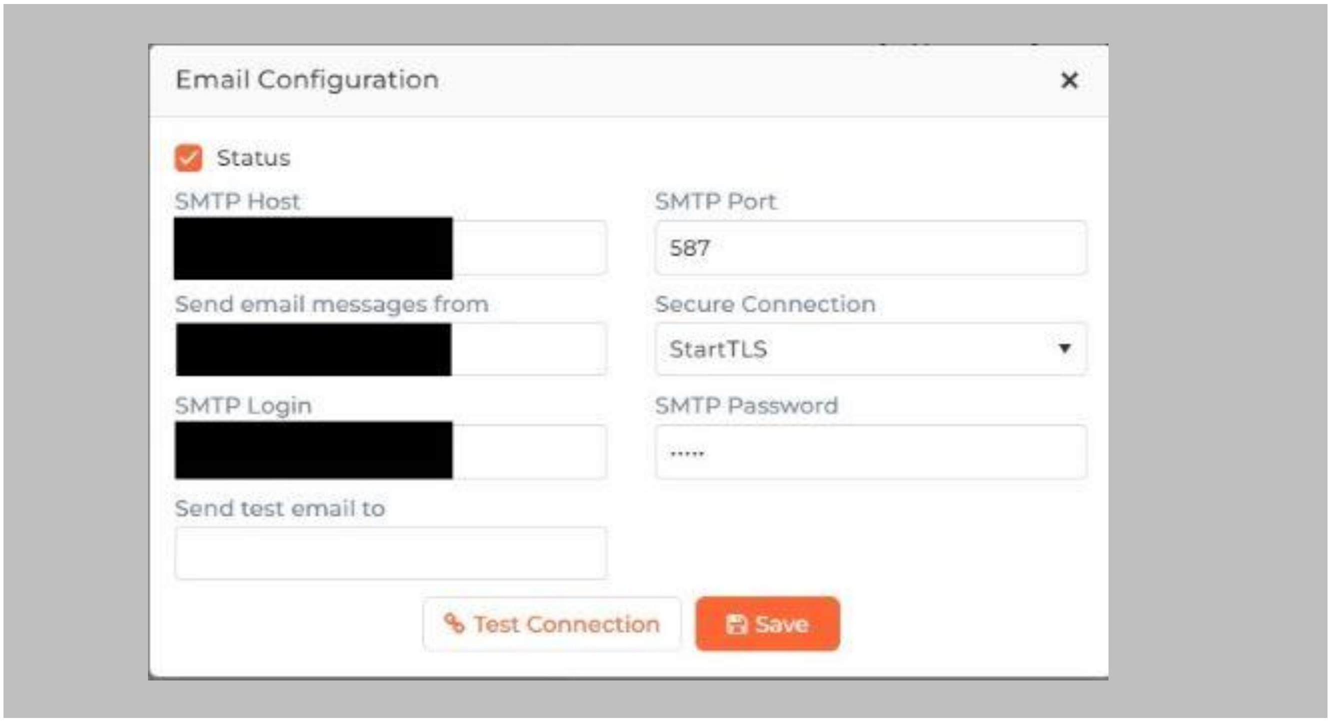
Dear **Admin,**

Following devices are offline
#Details#
Regards,

Figure 25: 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: •••••

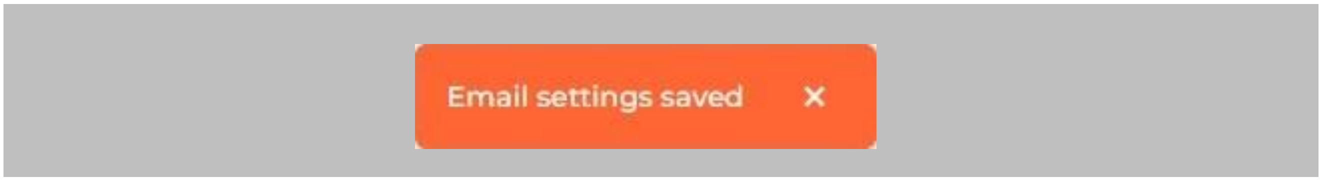
Send test email to:

Figure 26: IXM WEB - SMTP Settings

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

STEP 3

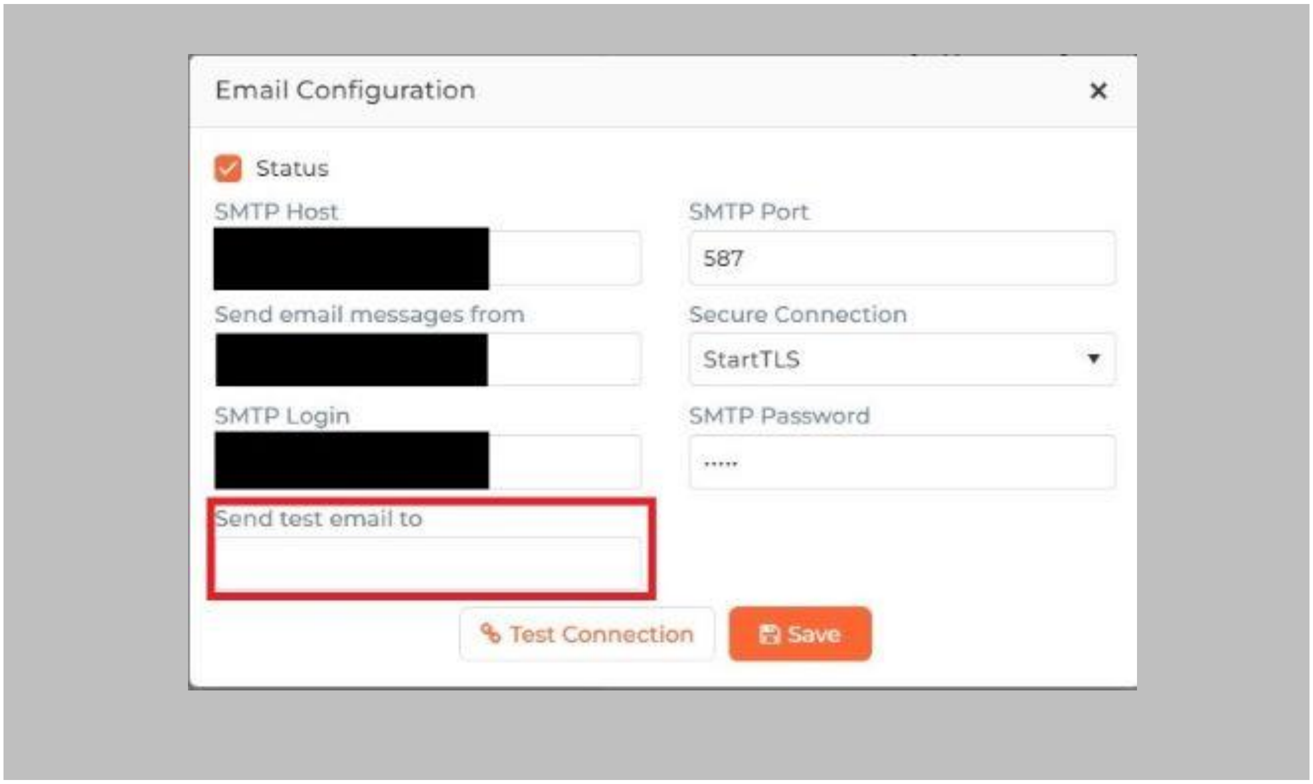
After entering the values, click **Save** to save the SMTP Settings on the IXM WEB database.



Email settings saved ✕

Figure 27: 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 28: 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.

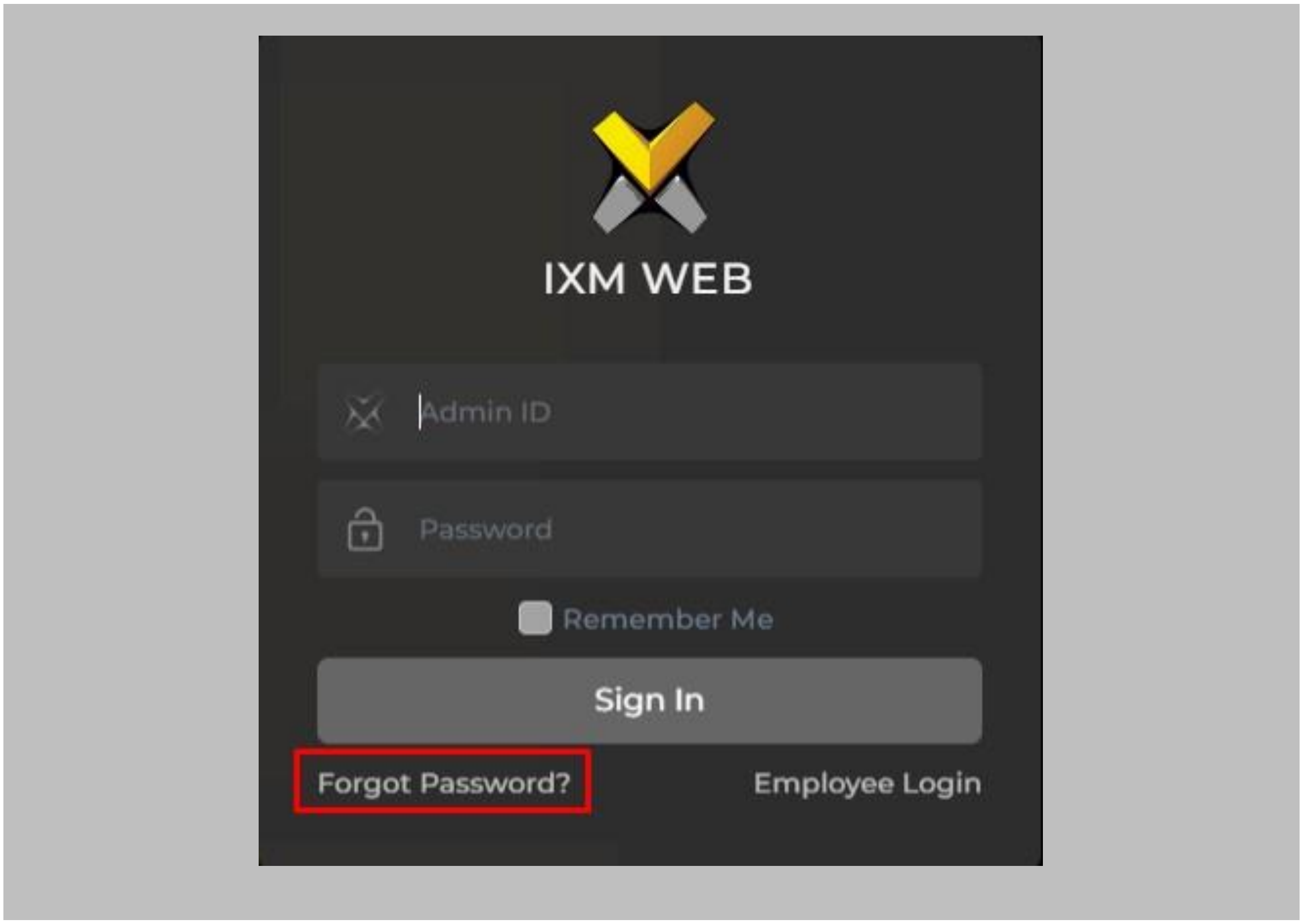


Figure 29: IXM WEB - Forgot Password

9. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

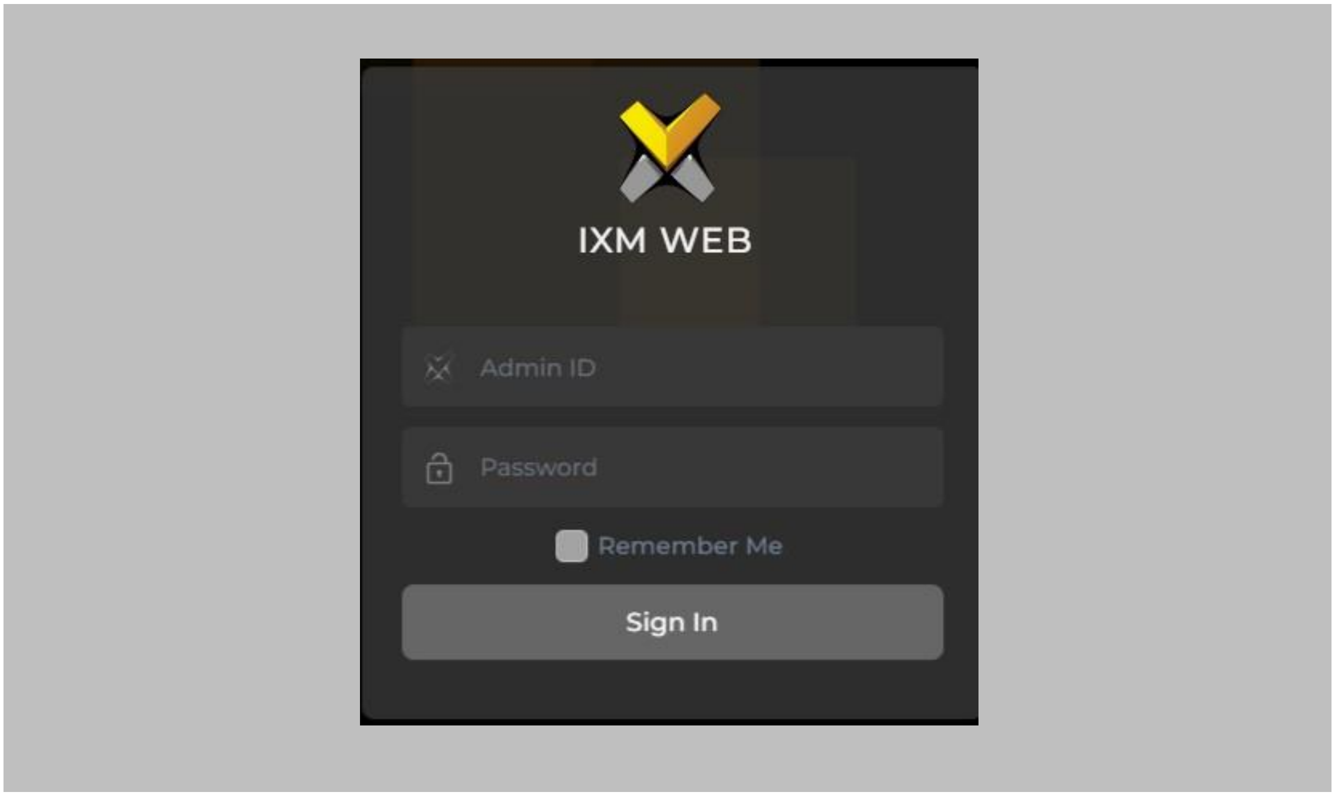
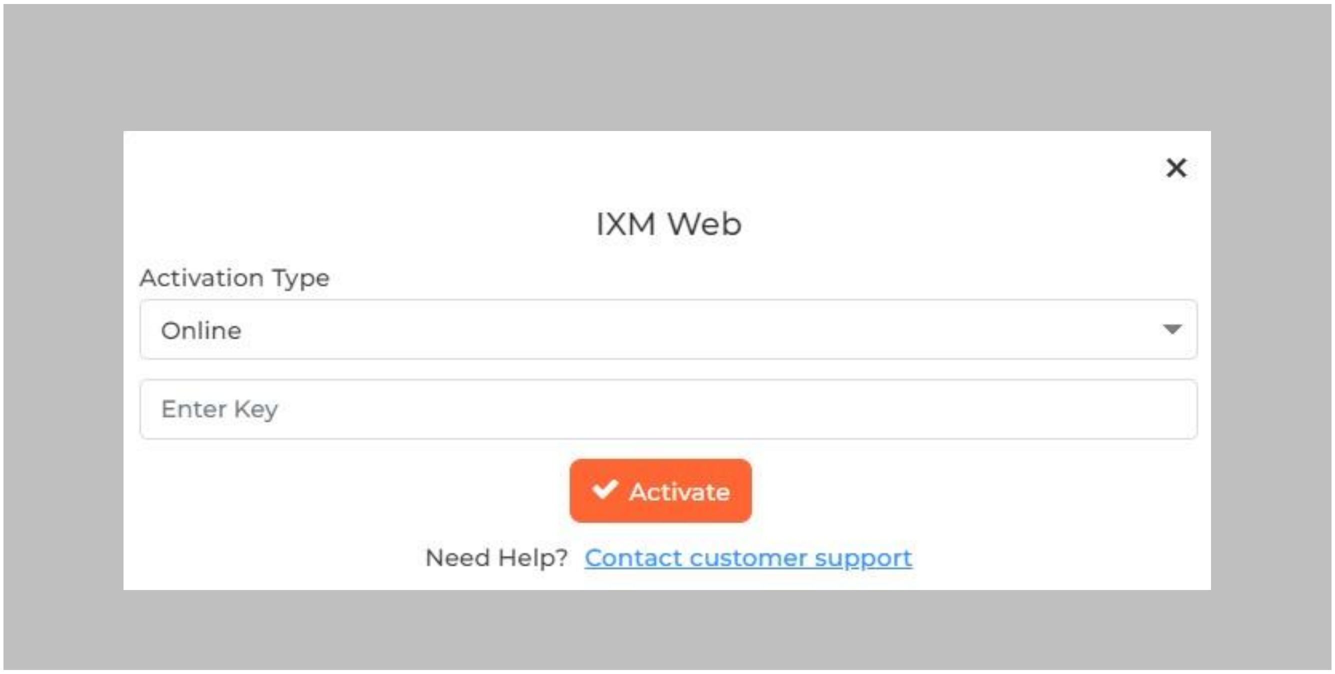


Figure 30: IXM WEB - Enter Login Credentials

STEP 2

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



IXM Web

Activation Type

Online

Figure 31: IXM WEB - License Setup

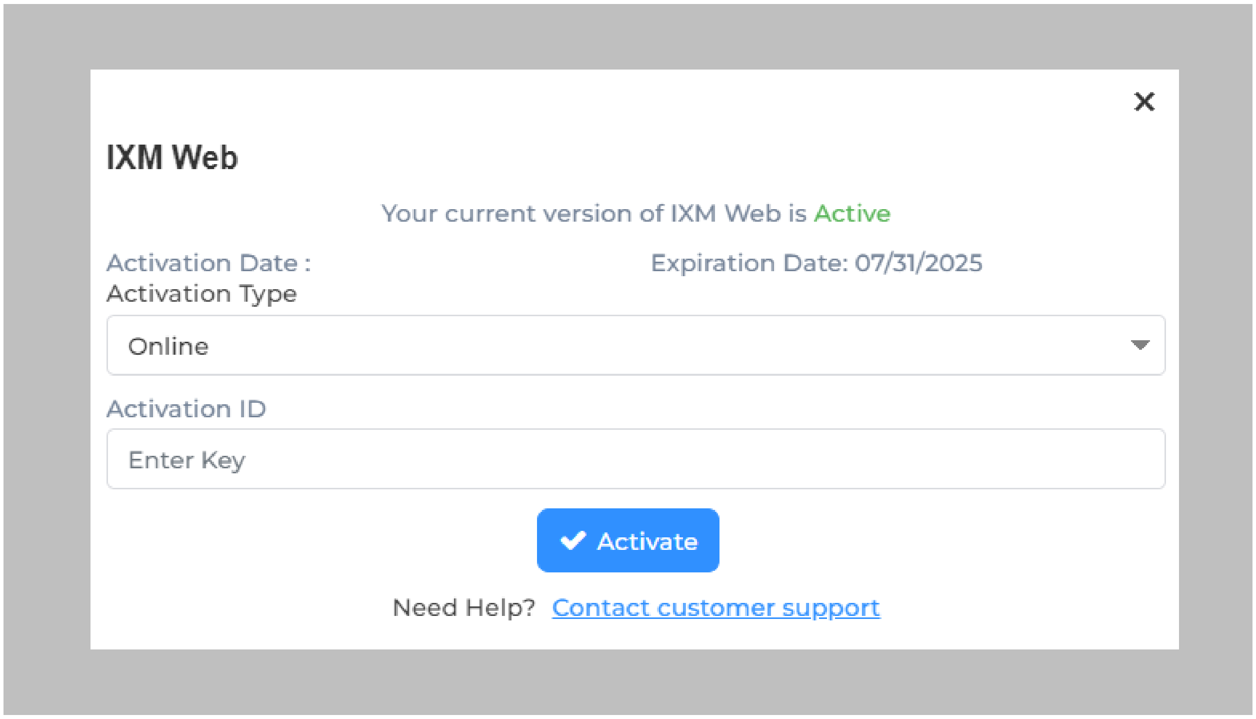
STEP 3

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 32: IXM WEB - Online Activation

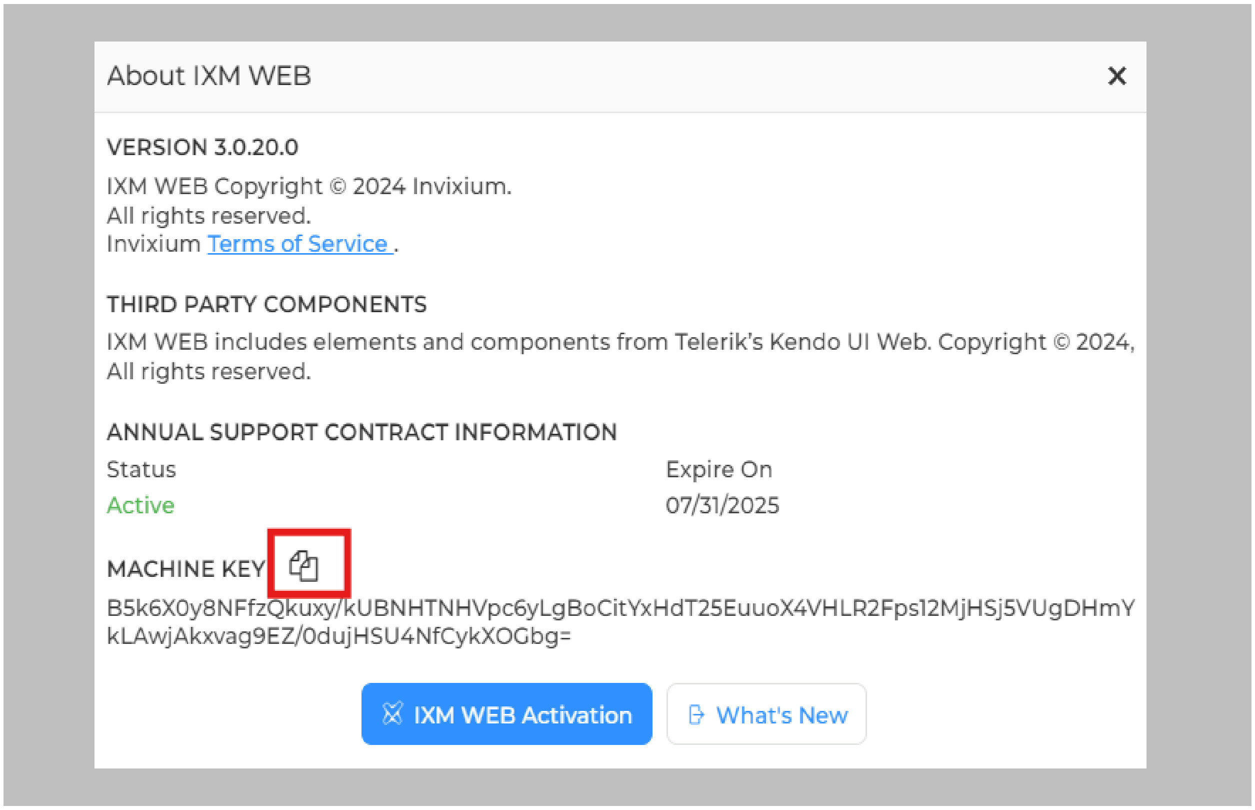
Command Centre Module Activation

The option to activate a Gallagher Command Centre 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

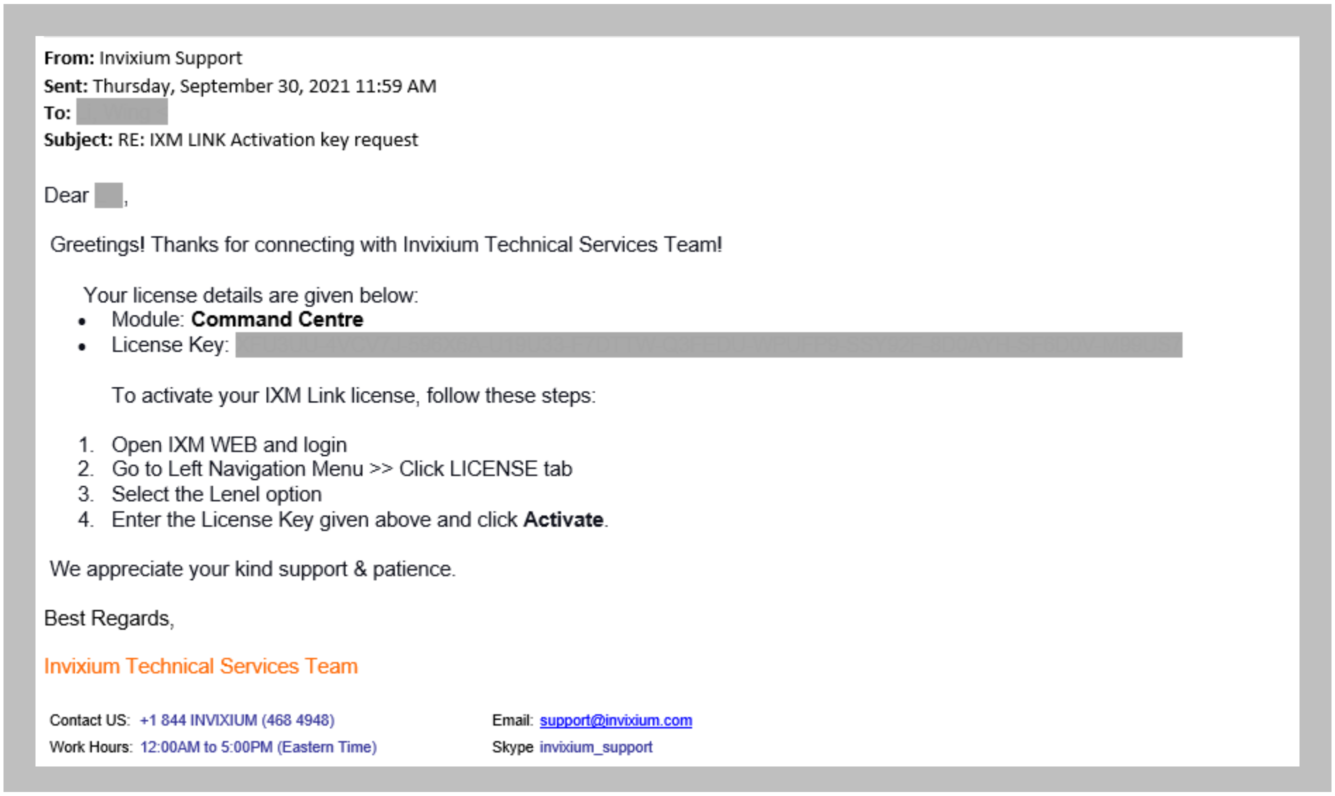
MACHINE KEY

B5k6X0y8NFfzQkuxy/kUBNHTNHVpc6yLgBoCitYxHdT25EuuoX4VHLR2Fps12MjHSj5VUgDHmYkLAwjAkxvag9EZ/0dujHSU4NfCykXOGbg=

Figure 33: IXM WEB – Request Link License

STEP 2

You will receive an email from Invixium Support containing a license key for the Gallagher Command Centre 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: **Command Centre**
- 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,

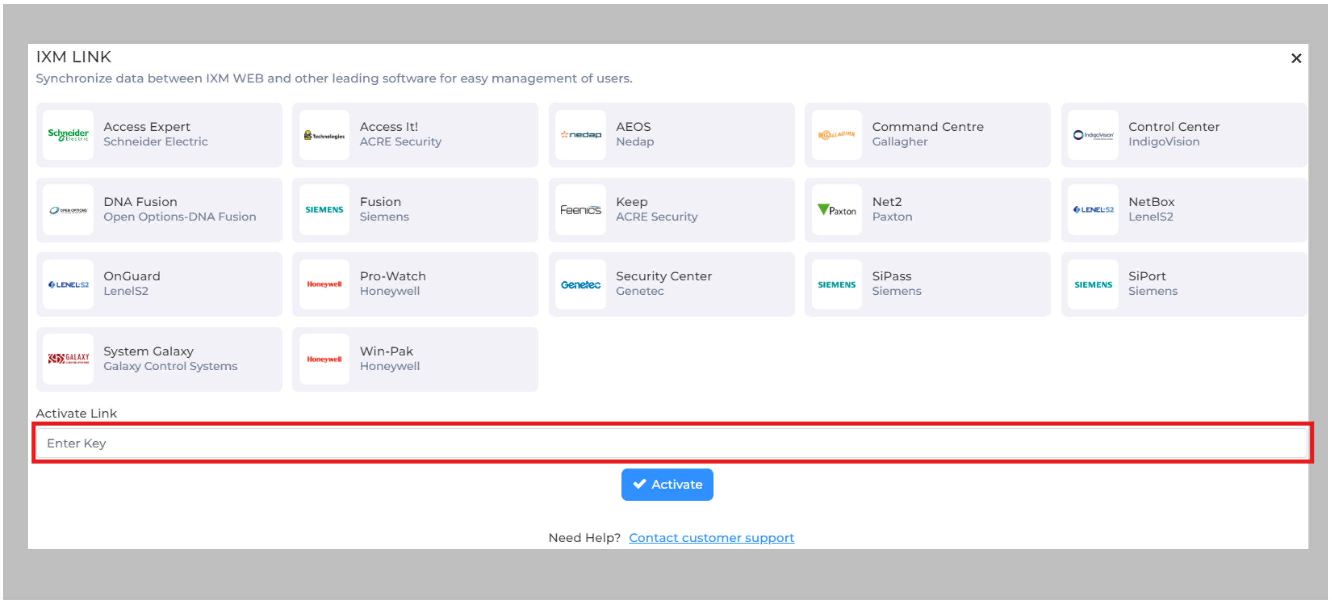
Invixium Technical Services Team

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

Figure 34: Gallagher 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 35: IXM WEB - Activate Gallagher Command Center Link License

RESULT

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

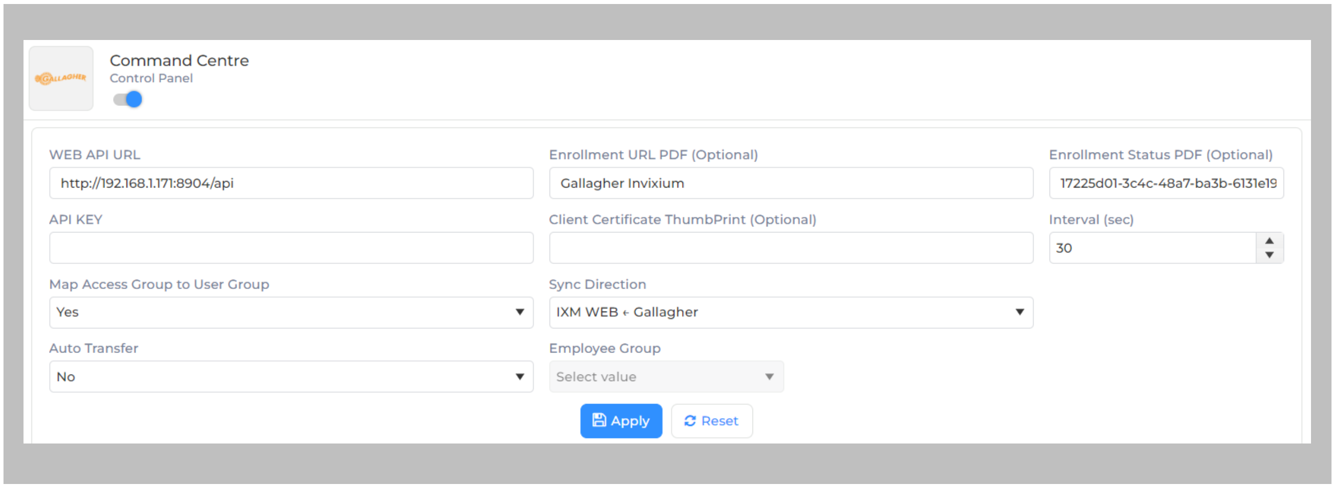
10. Configuring IXM Link for Gallagher

Procedure

STEP 1

From the **Link** → click the **Command Centre (Gallagher)** icon.

Toggle the **Status** switch to enable.



Command Centre
Control Panel

WEB API URL: http://192.168.1.171:8904/api

Enrollment URL PDF (Optional): Gallagher Invixium

Enrollment Status PDF (Optional): 17225d01-3c4c-48a7-ba3b-6131e19

API KEY:

Client Certificate ThumbPrint (Optional):

Interval (sec): 30

Map Access Group to User Group: Yes

Sync Direction: IXM WEB ← Gallagher

Auto Transfer: No

Employee Group: Select value

Figure 36: IXM WEB - Enable Gallagher Link Module

STEP 2

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

STEP 3

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

STEP 4

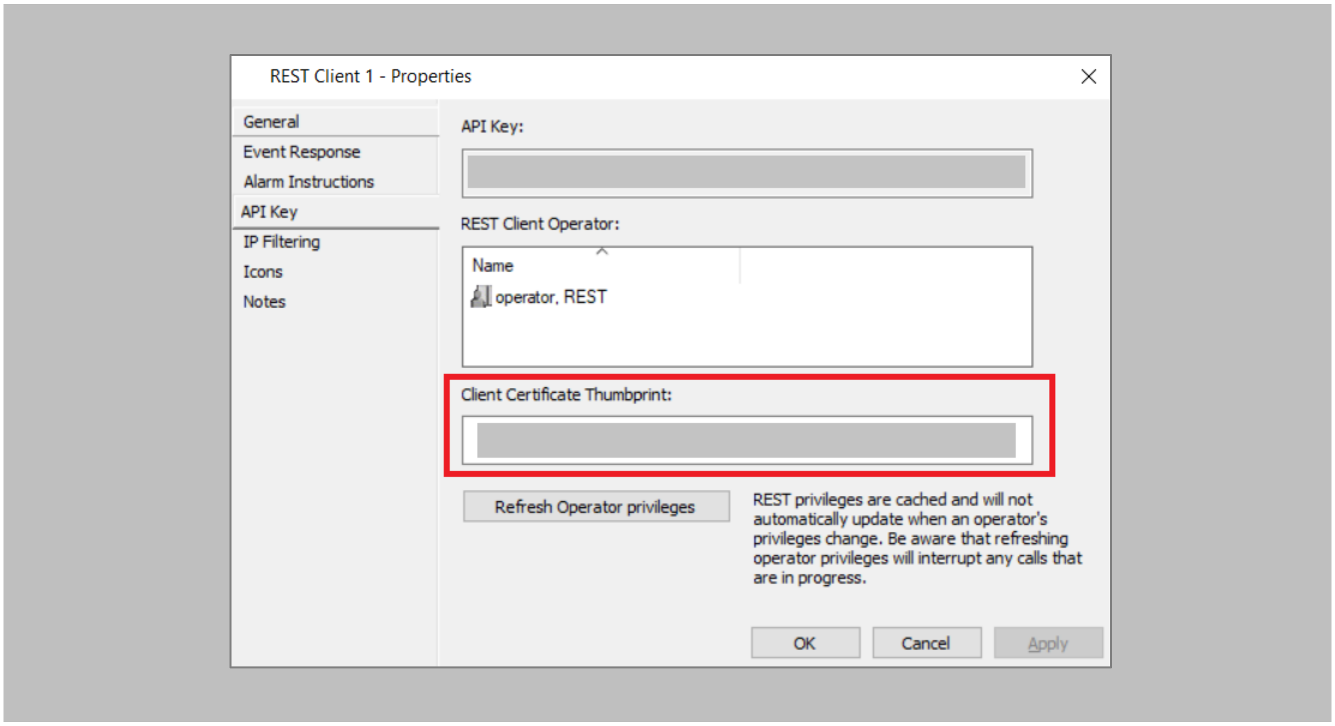
Copy the Enrollment status name created **'ENROLLMENT STATUS'** (refer to Enrollment Status PDF (Personal Data Field)).

STEP 5

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

STEP 6

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



REST Client 1 - Properties

API Key: [redacted]

REST Client Operator:

Name: operator, REST

Client Certificate Thumbprint: [redacted]

REST privileges are cached and will not automatically update when an operator's privileges change. Be aware that refreshing operator privileges will interrupt any calls that are in progress.

Figure 37: GCC - REST Client Certificate Thumbprint

STEP 7

Specify in seconds how often sync should take place.

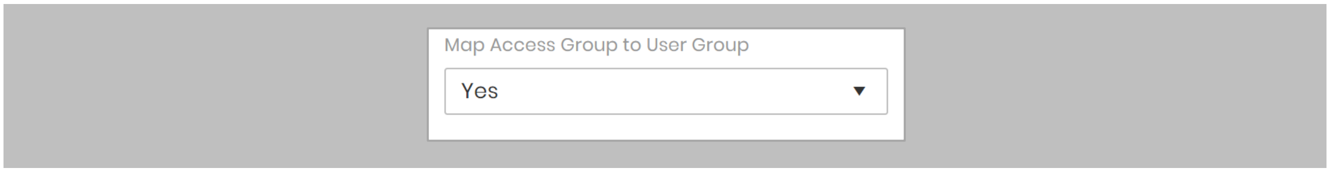
STEP 8

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

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

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

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



Map Access Group to User Group

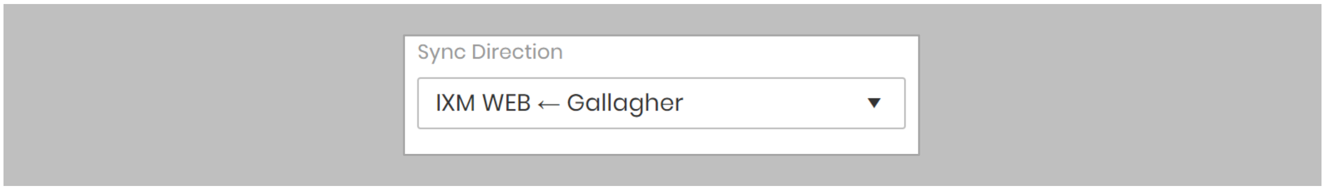
Yes

Figure 38: IXM WEB - Map Access Group to User Group

STEP 9

Select **Sync Direction.**

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



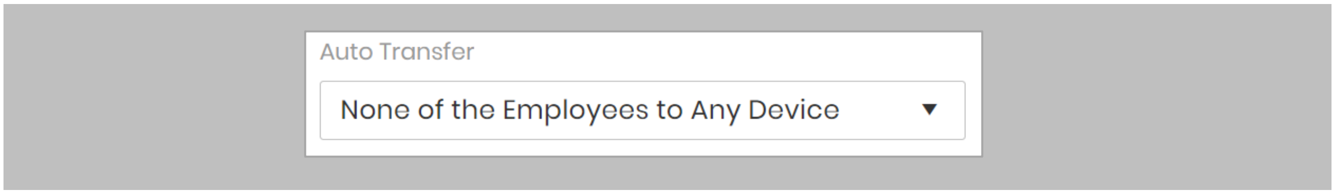
Sync Direction

IXM WEB ← Gallagher

Figure 39: IXM WEB - Sync Direction

STEP 10

Select **Auto Transfer.**



Auto Transfer

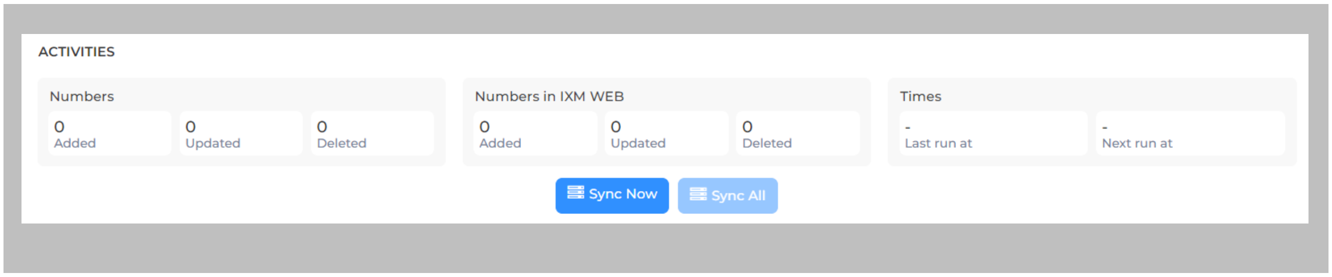
None of the Employees to Any Device ▼

Figure 40: IXM WEB - Auto Transfer Employees

STEP 11

Click **Apply.**

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



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 41: IXM WEB - Sync Activities

STEP 12

Clicking **Sync Now** immediately starts synchronizing pending data. This is useful when you do not want to wait until the next scheduled run shown by “Next Run At”.

STEP 13

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

STEP 14

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

RESULT

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

11. Create System User(s) for Biometric Enrollment

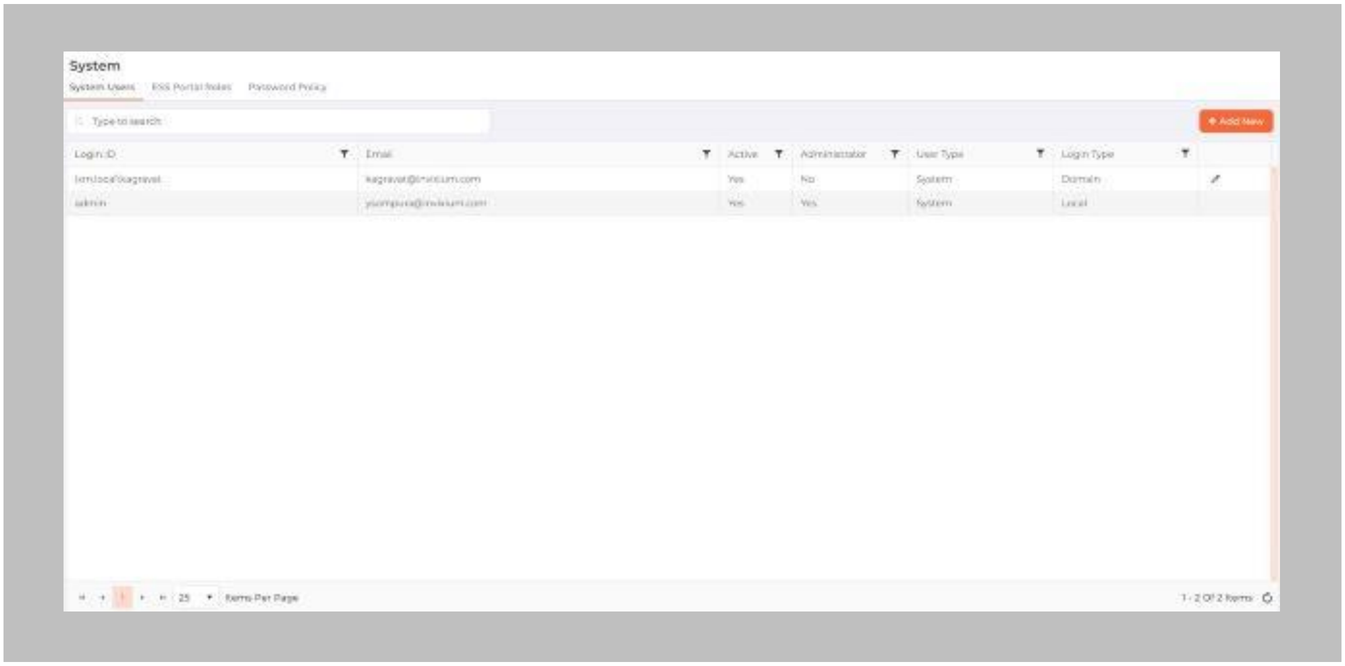
Creating System User(s) for Biometric Enrollment

Procedure

STEP 1

Log into IXM WEB.

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

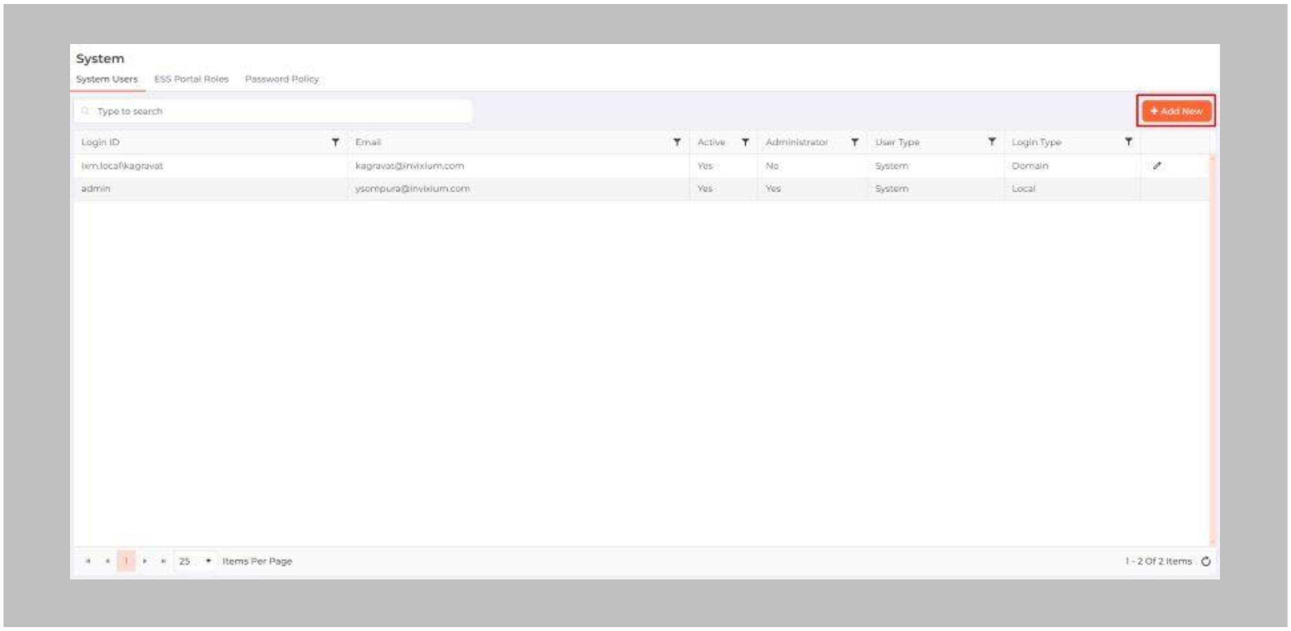


Login ID	Email	Active	Administrator	User Type	Login Type
ixmlocal\kagrawal	kagrawal@invixium.com	Yes	No	System	Domain
admin	ysompura@invixium.com	Yes	Yes	System	Local

Figure 42: 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	

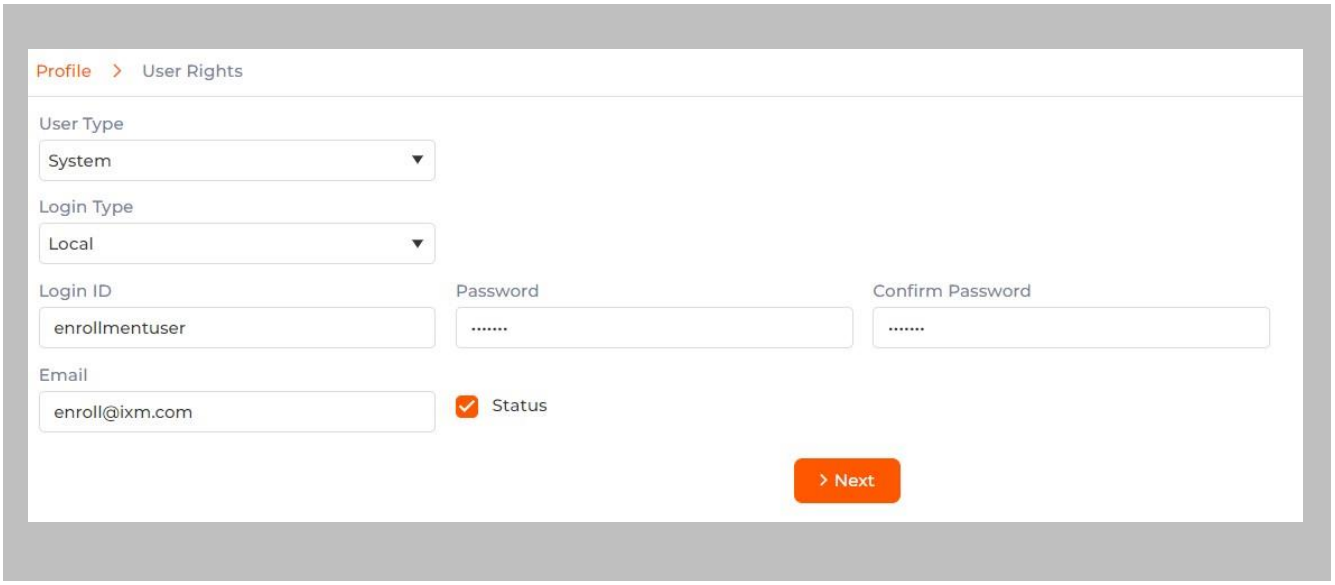
Figure 43: IXM WEB - Add New System User

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

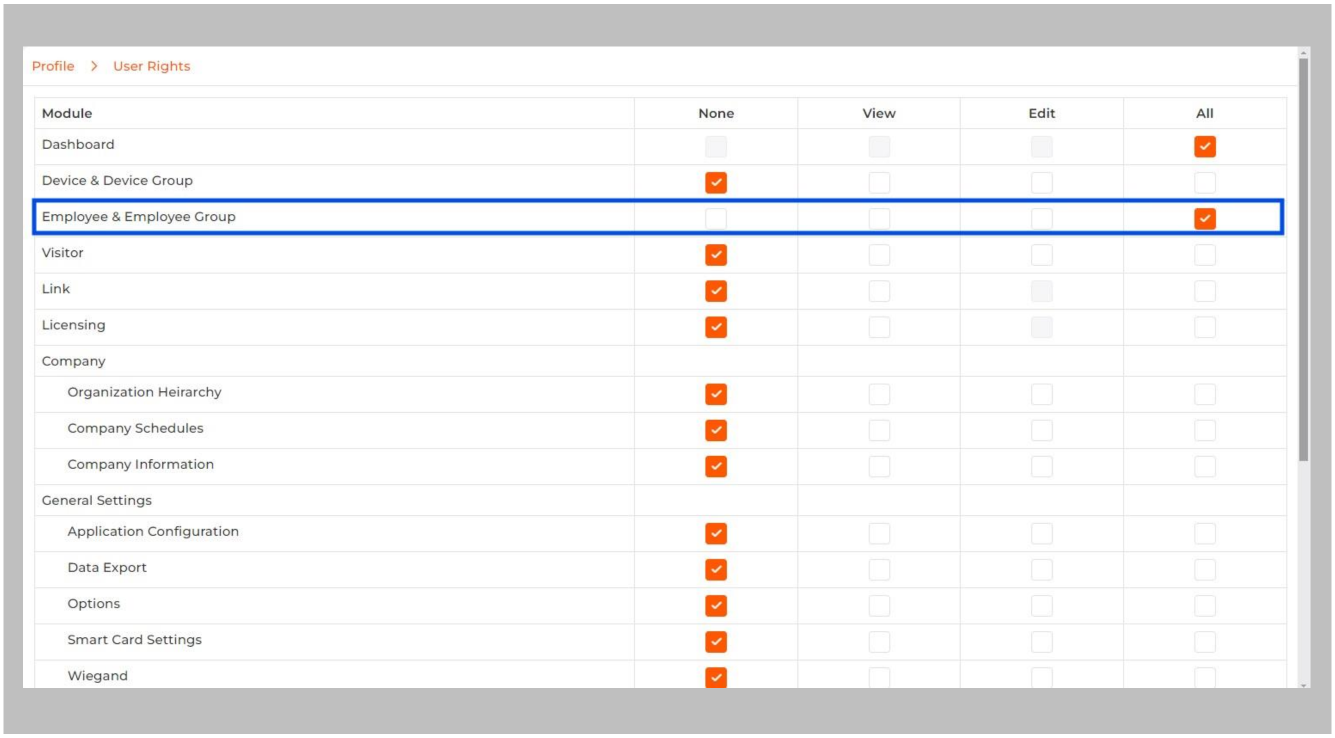
☑ Status

Figure 44: IXM WEB - New System User

STEP 4

Add an email address.

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



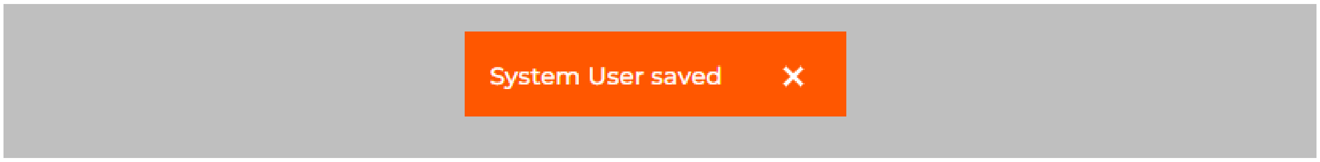
Profile > User Rights

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 45: Employee and Employee Group Rights

STEP 5

Click **Save**.



System User saved ✕

Figure 46: IXM WEB - Save System User

12. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

Click the **Devices** tab.

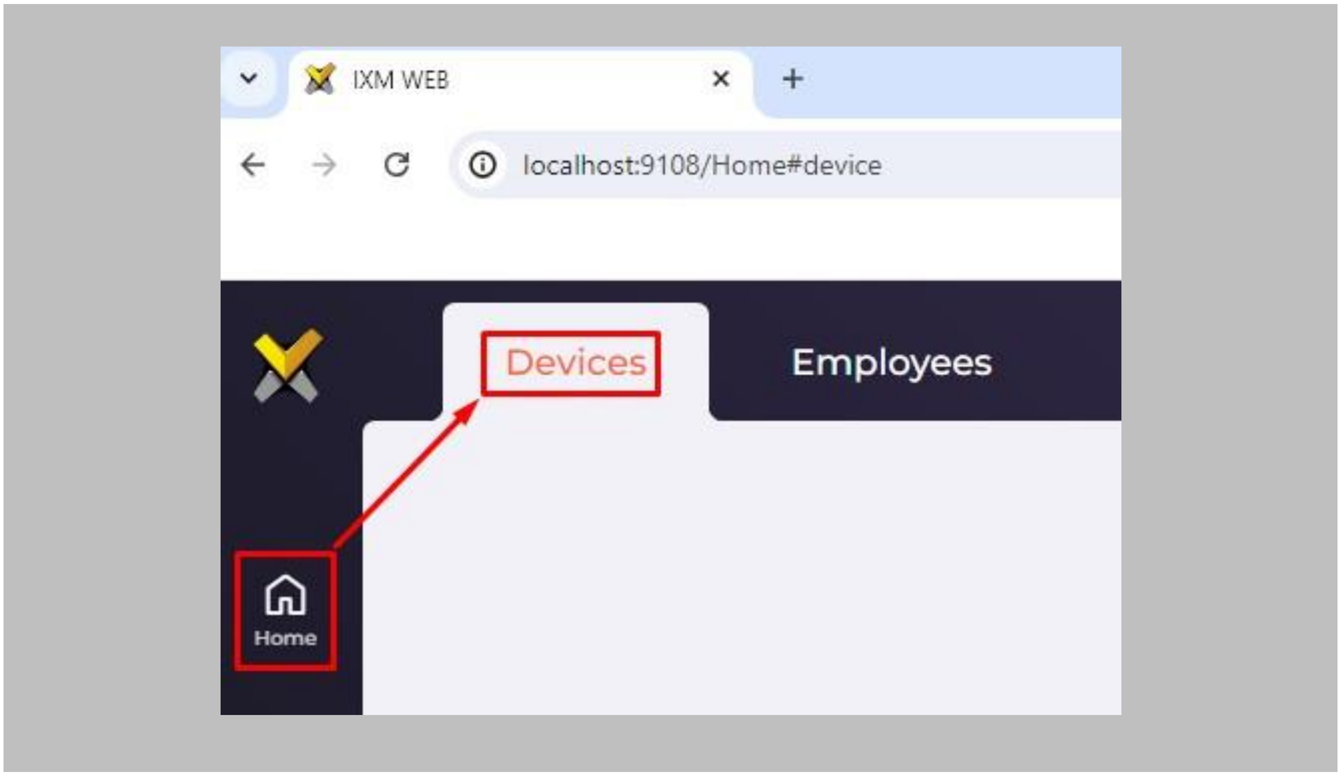
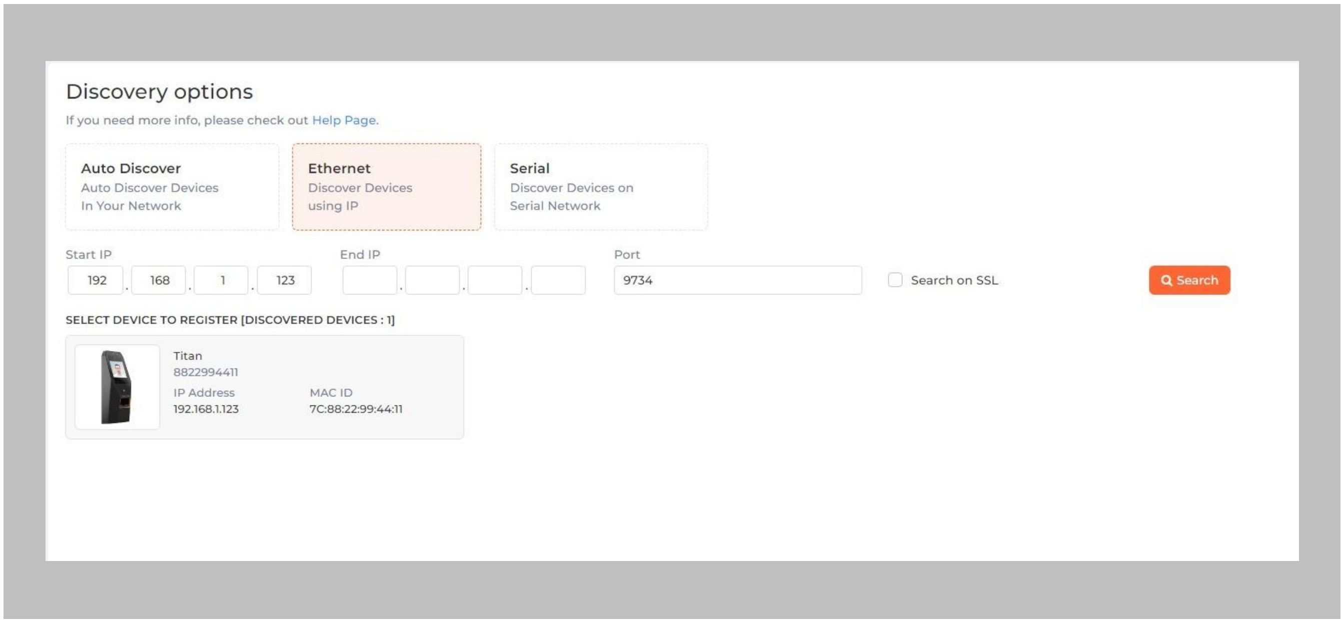


Figure 47: IXM WEB - Devices Tab

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

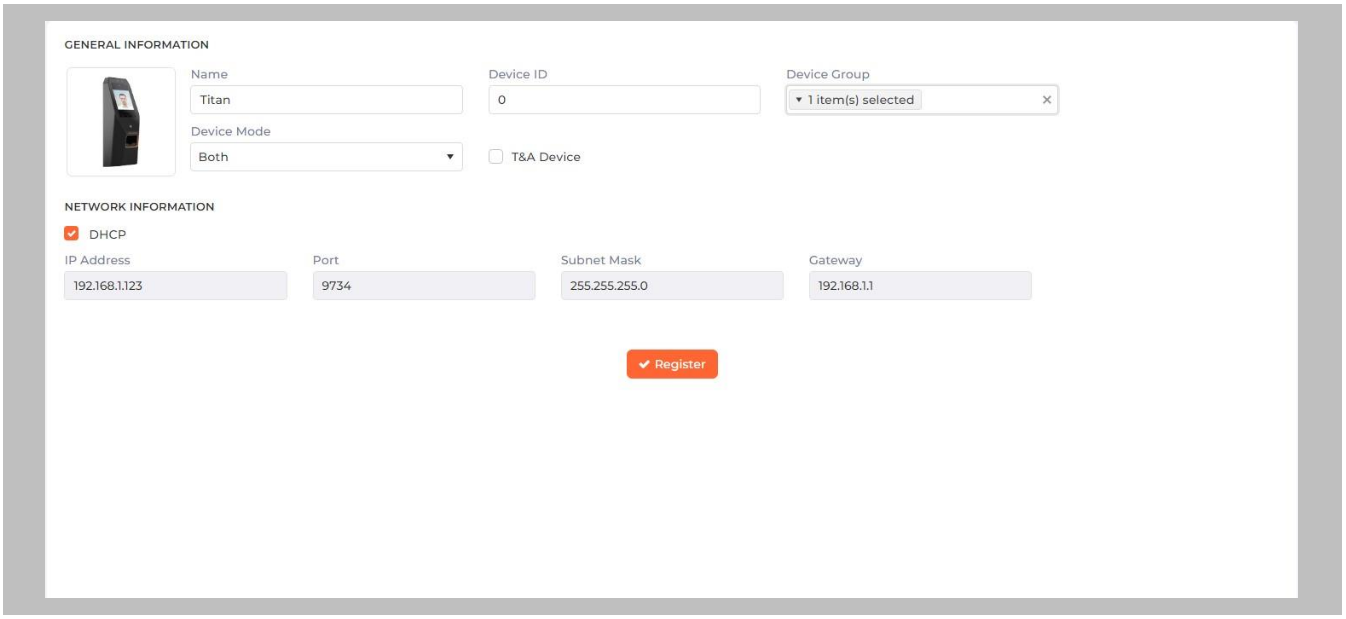
IP Address: 192.168.1.123

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

Figure 48: 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 49: IXM WEB - Register Device

STEP 4

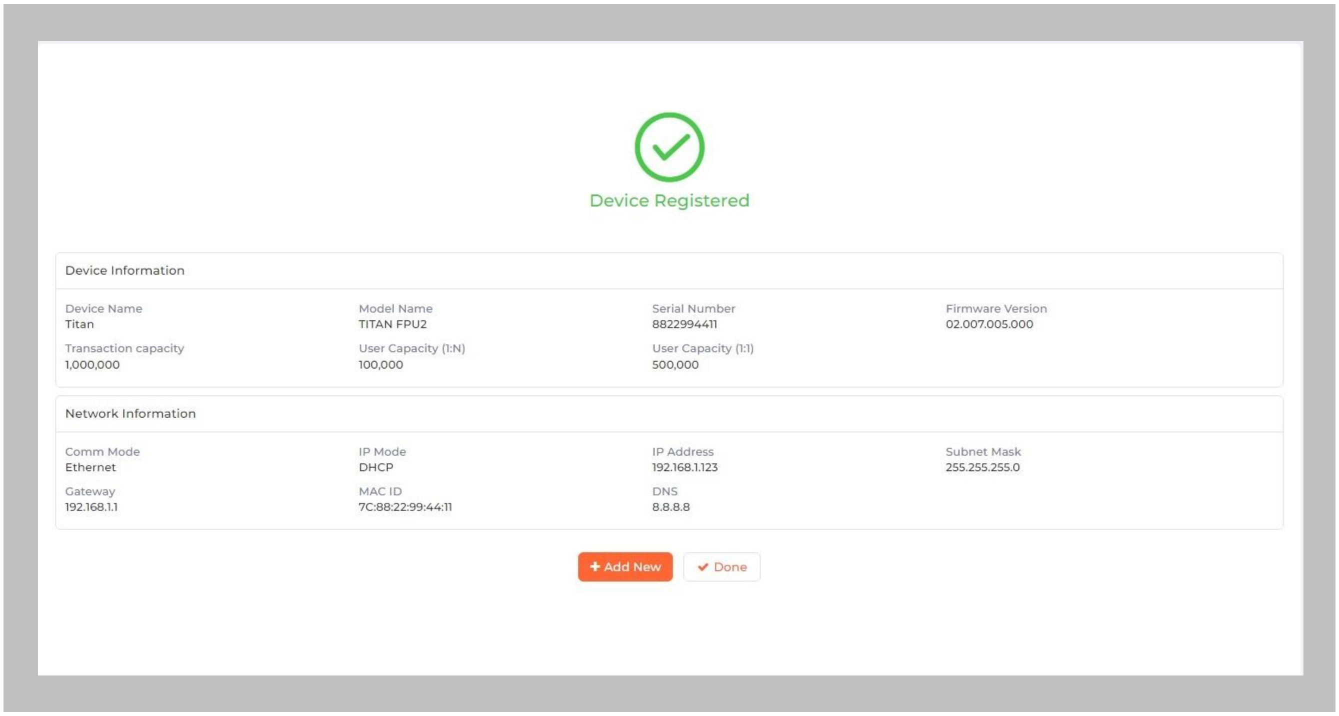
Name the **device** exactly as the name of the door it will be used for.

Device Mode: select accordingly.

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

STEP 5

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



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

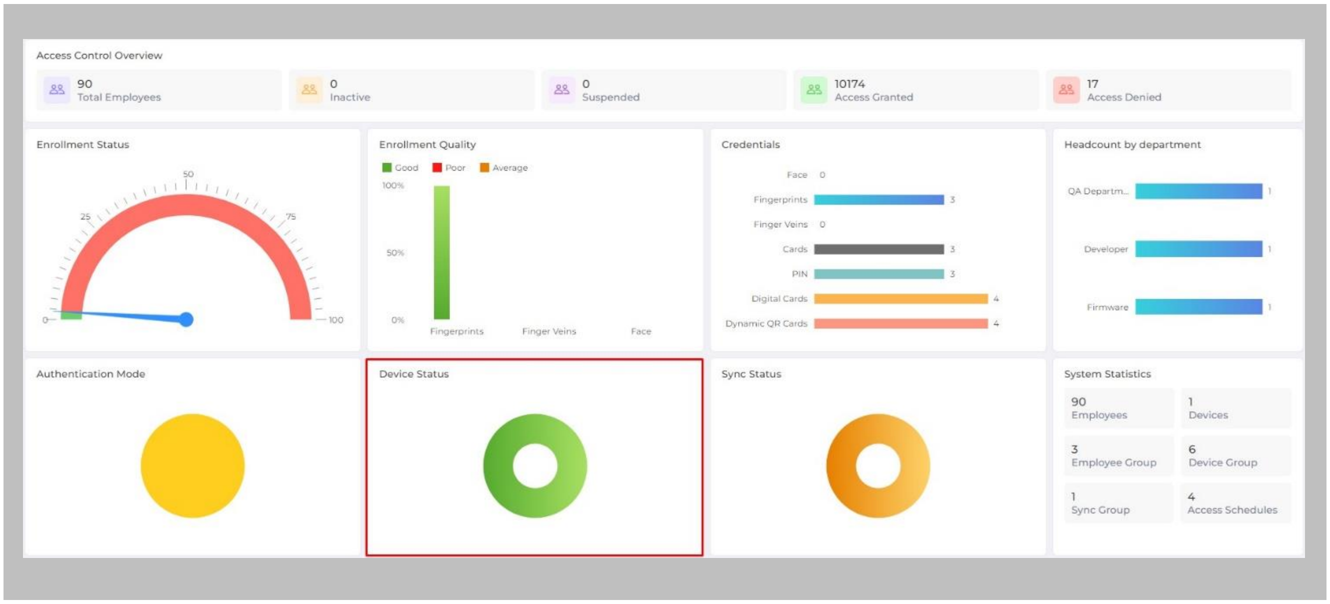
Gateway
192.168.1.1

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

DNS
8.8.8.8

Figure 50: 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 51: IXM WEB - Dashboard, Device Status

13. Adding an Invixium Device to a Device Group

Procedure

STEP 1

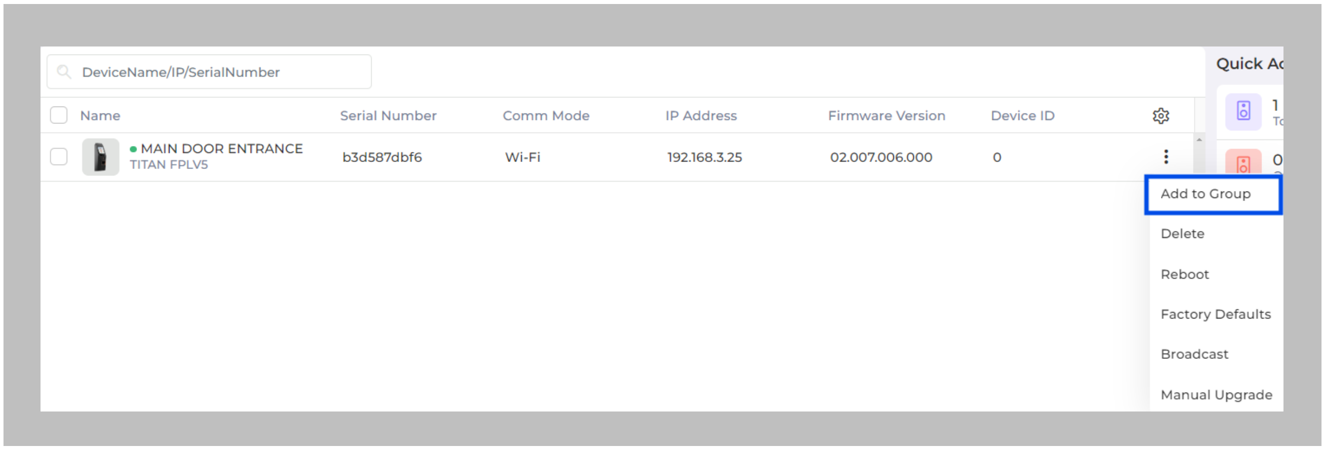
Any of below methods can be used to add device to device group.

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

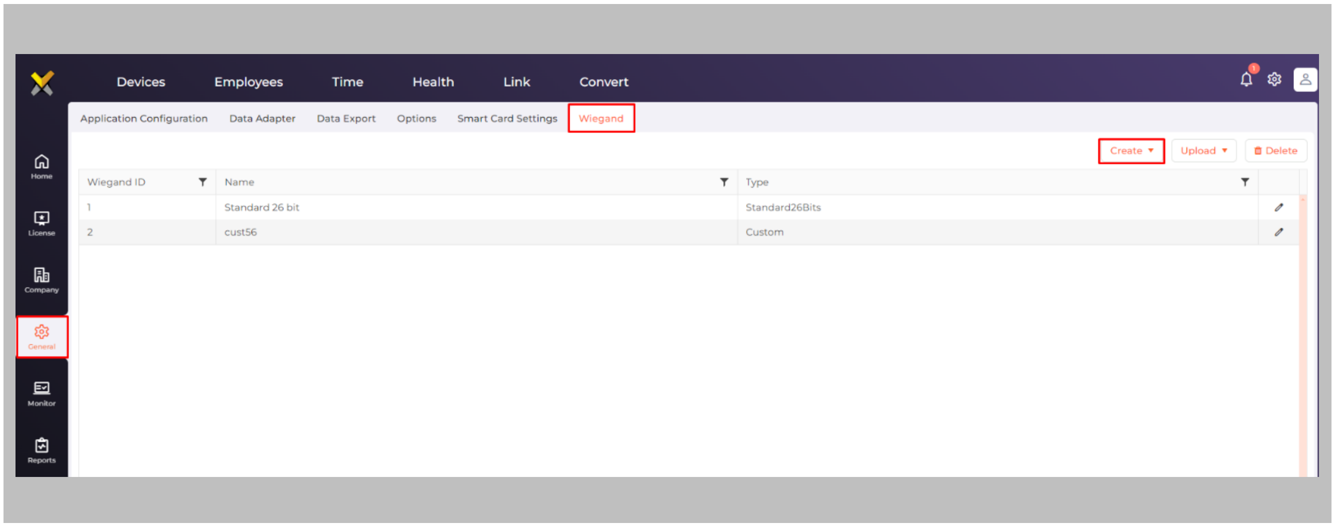
Figure 52: IXM WEB - Assign Device Group

Configuring Wiegand to Assign Invixium Readers

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

STEP 1

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

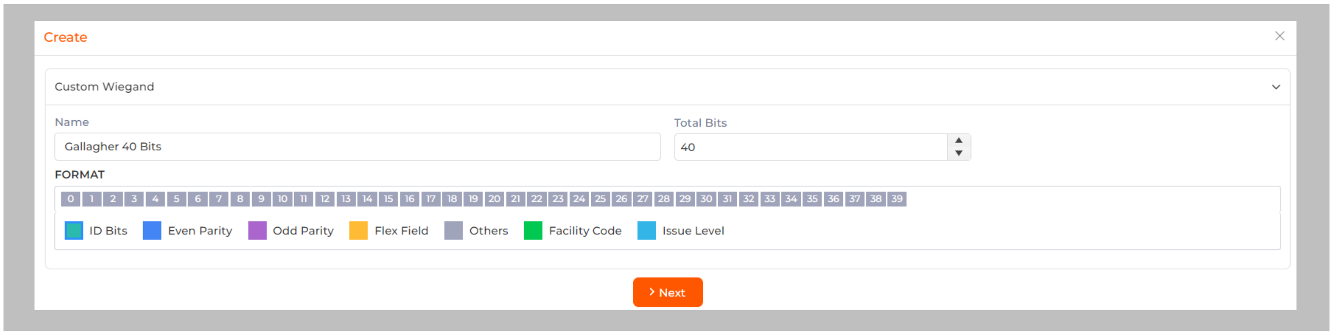


Wiegand ID	Name	Type
1	Standard 26 bit	Standard26Bits
2	cust56	Custom

Figure 53: IXM WEB - Create Wiegand Format

STEP 2

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



Custom Wiegand

Name: Gallagher 40 Bits

Total Bits: 40

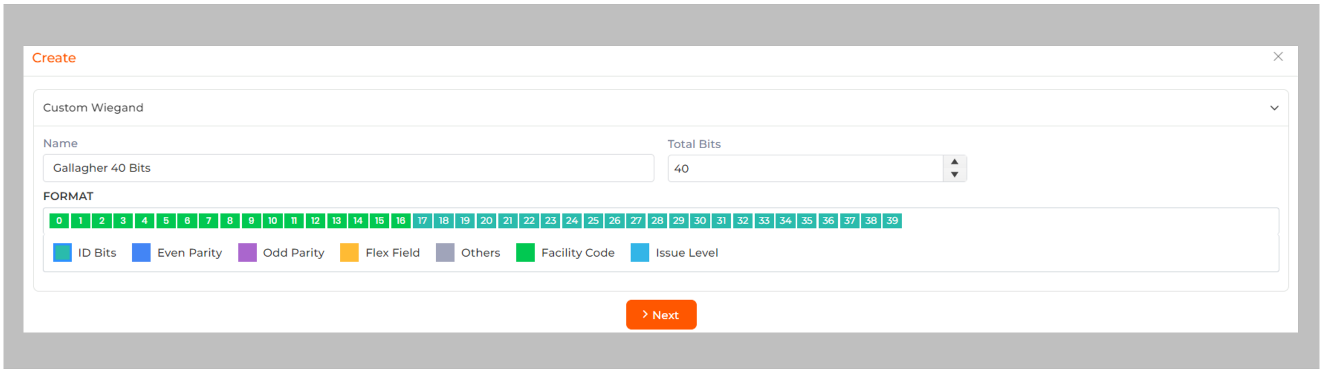
Figure 54: IXM WEB - Create Custom Wiegand Format

STEP 3

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

Facility Code: 0 to 16 bits

ID Bits: 17 to 39 bits



Create

Custom Wiegand

Name: Gallagher 40 Bits

Total Bits: 40

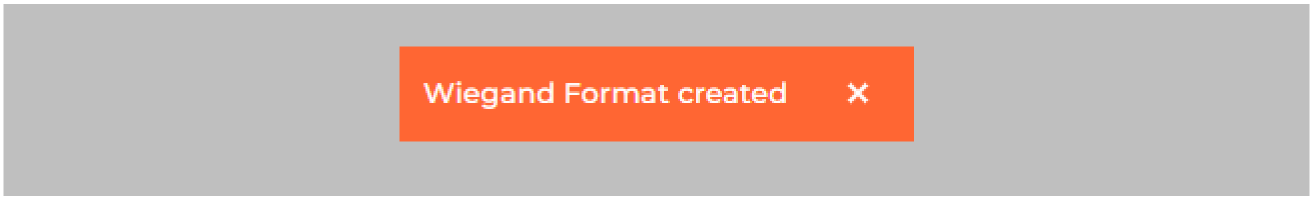
FORMAT

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39

Figure 55: IXM WEB - Custom Wiegand

STEP 4

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

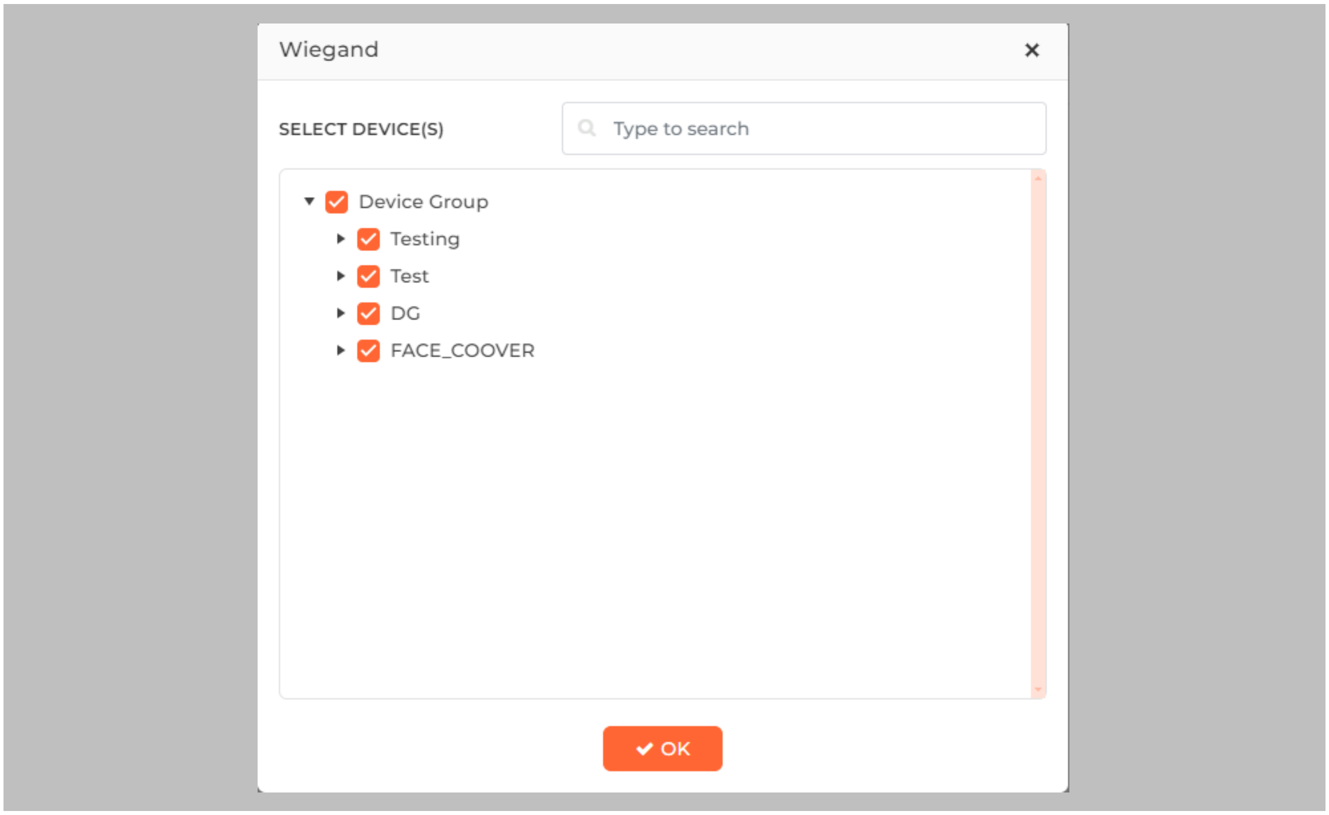


Wiegand Format created ✕

Figure 56: 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 57: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invixium Readers

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

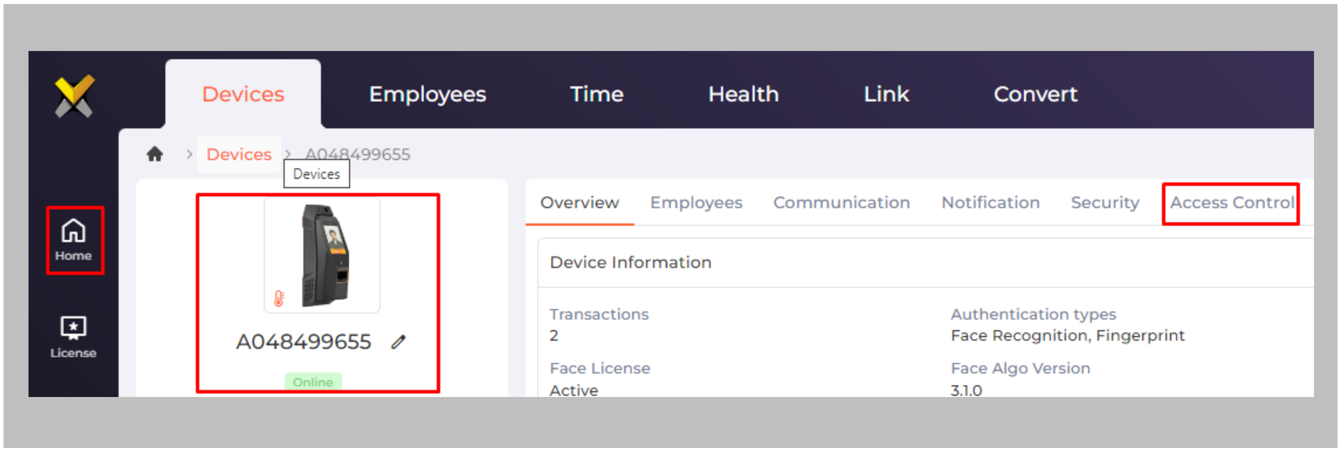
The created Wiegand will be used to define which output format will be sent to GCC.

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.



Device Information

Transactions
2

Authentication types
Face Recognition, Fingerprint

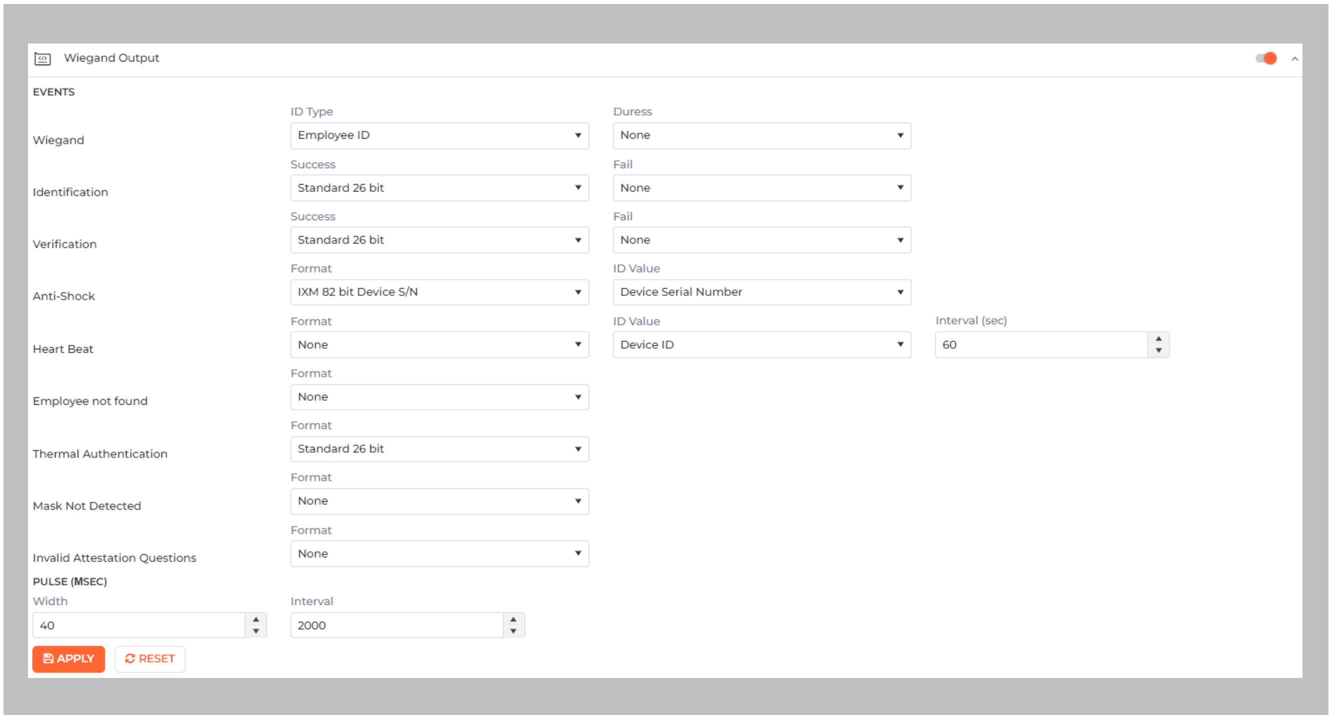
Face License
Active

Face Algo Version
3.1.0

Figure 58: 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 59: 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 GCC, select either Default Card or Actual Card.

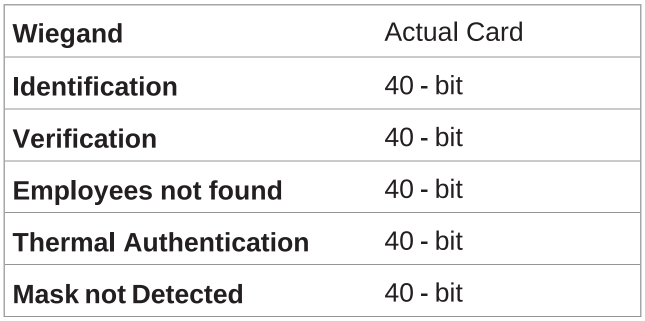
Actual Card: when more than one card is assigned to the cardholder, and you want to generate Wiegand output data for the same card which is presented on the Invixium device.

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

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

STEP 4

Set the **items**:



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

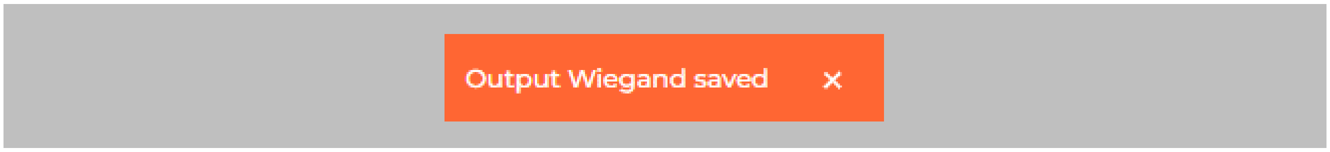
Empoyee ID: This is auto generated ID by IXM WEB for an imported cardholder in Gallagher.

STEP 5

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

STEP 6

Click **Apply.**



Output Wiegand saved ×

Figure 60: IXM WEB - Save Output Wiegand

RESULT

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

ⓘ Note:

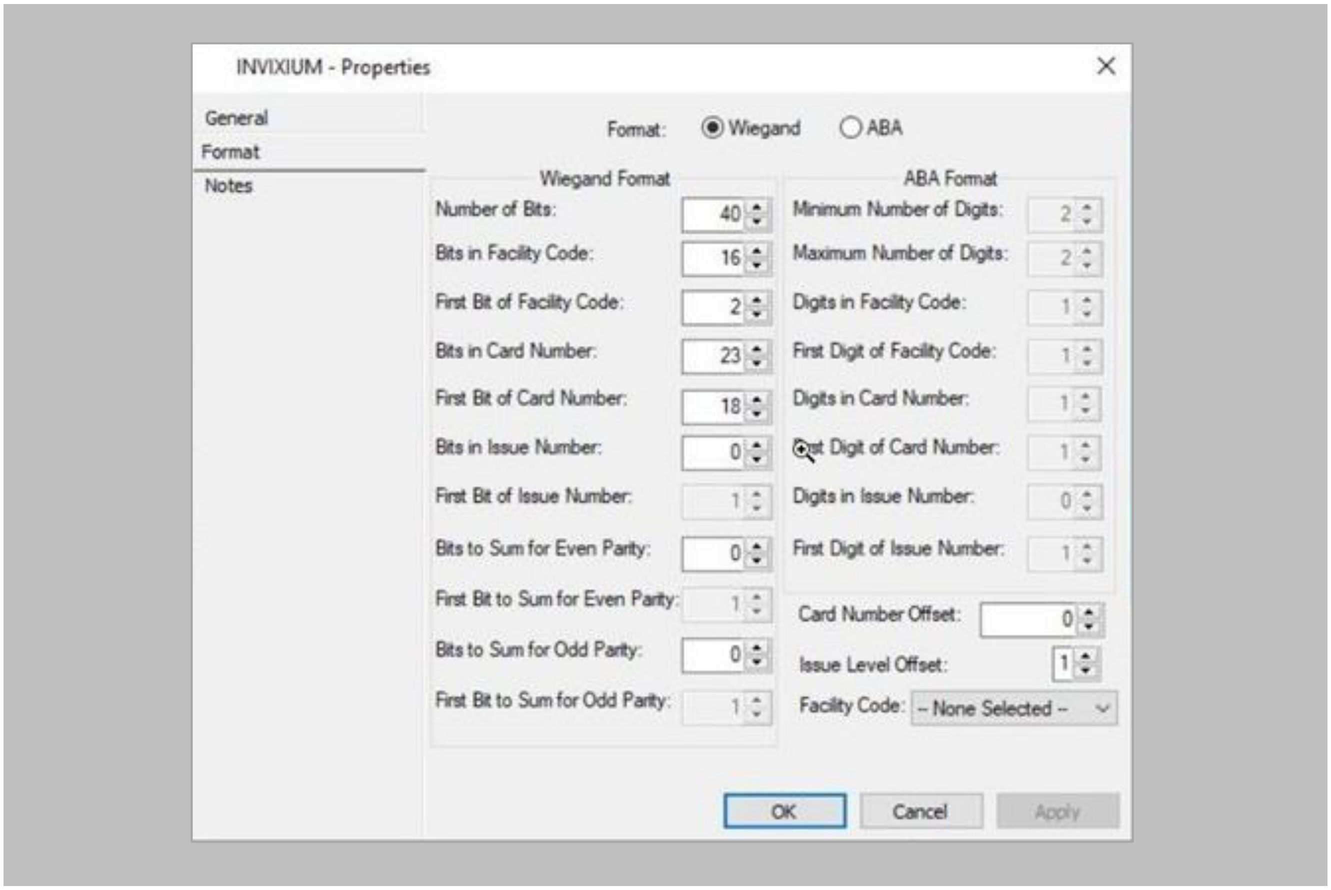
- If you have more devices, follow the next steps to copy all Wiegand settings to all devices simultaneously. Note: This copies all Wiegand output settings. See Appendix C for more information.
- If the cardholder was assigned multiple cards, the first assigned card will be the 'default' selected card.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

Configure UCF on Configuration Client

Procedure

STEP 1

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



INVIXIUM - Properties

General
Format
Notes

Format: ● Wiegand ○ ABA

Wiegand Format	
Number of Bits:	40
Bits in Facility Code:	16
First Bit of Facility Code:	2
Bits in Card Number:	23
First Bit of Card Number:	18
Bits in Issue Number:	0
First Bit of Issue Number:	1
Bits to Sum for Even Parity:	0
First Bit to Sum for Even Parity:	1
Bits to Sum for Odd Parity:	0
First Bit to Sum for Odd Parity:	1

ABA Format	
Minimum Number of Digits:	2
Maximum Number of Digits:	2
Digits in Facility Code:	1
First Digit of Facility Code:	1
Digits in Card Number:	1
First Digit of Card Number:	1
Digits in Issue Number:	0
First Digit of Issue Number:	1

Card Number Offset: 0

Issue Level Offset: 1

Facility Code: -- None Selected --

Figure 61: IXM WEB - Configure Universal Card Formats

STEP 2

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

Configuring Panel Feedback with Gallagher

Procedure

STEP 1

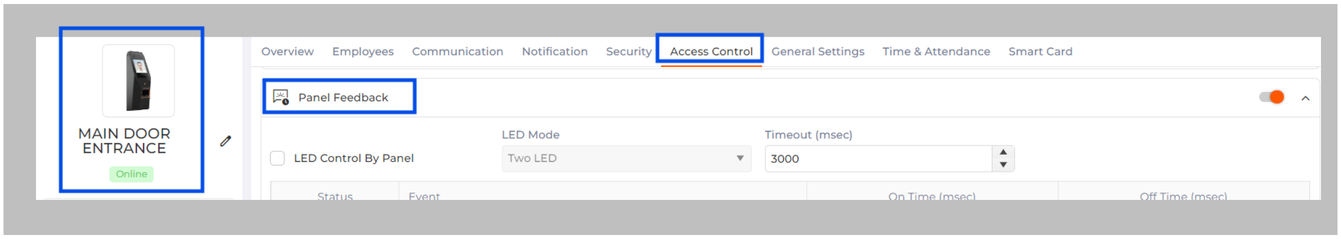
Connect Wiegand Data D0 of the Gallagher Panel with **WDATA_OUT0** of the IXM device, Wiegand Data D1 of the Gallagher Panel with WDATA_OUT1, and Wiegand Ground of the Gallagher Panel with WGND of the IXM Device.

STEP 2

Connect the **LED** of the Gallagher Panel with **ACP_LED1** of the IXM device.

STEP 3

On the **Devices** tab, select the required device and navigate to the **Access Control** tab. Scroll down and click on **Panel Feedback**.



□ LED Control By Panel

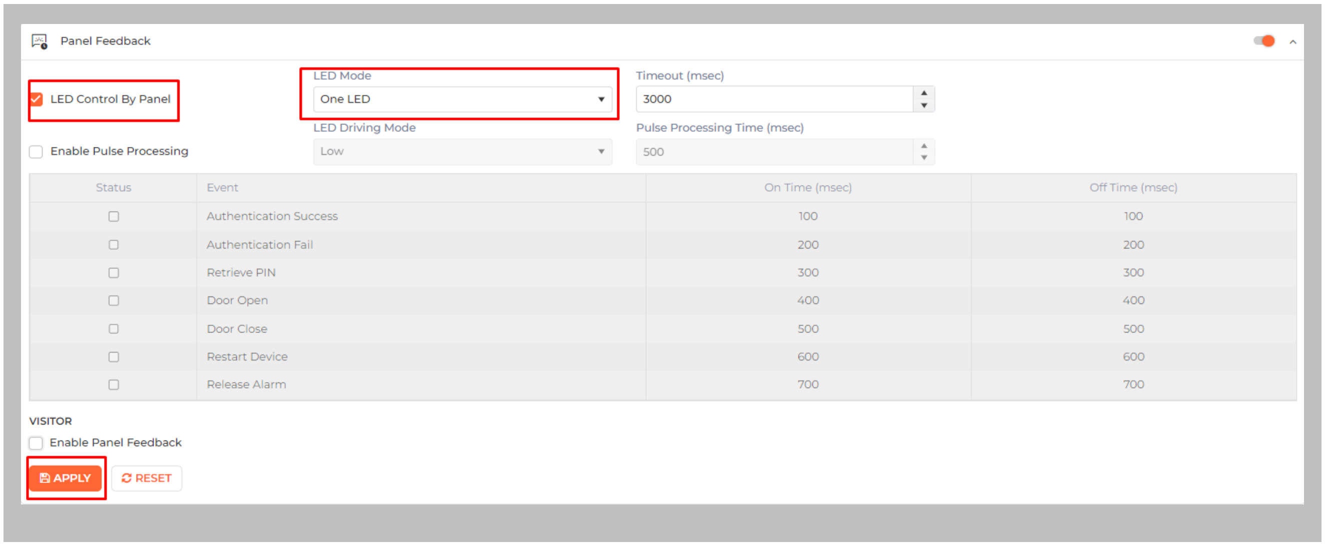
LED Mode: Two LED

Timeout (msec): 3000

Figure 62: 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

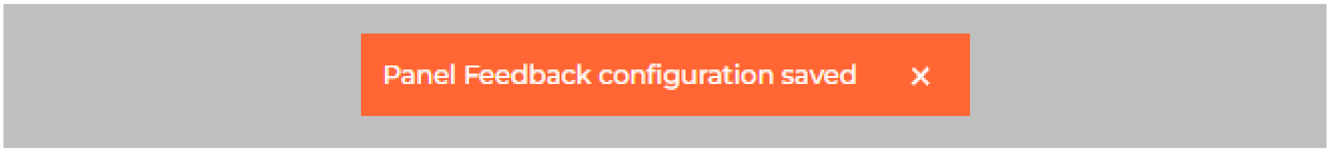
VISITOR

☐ Enable Panel Feedback

Figure 63: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.



Panel Feedback configuration saved

Figure 64: IXM WEB - Save Panel Feedback

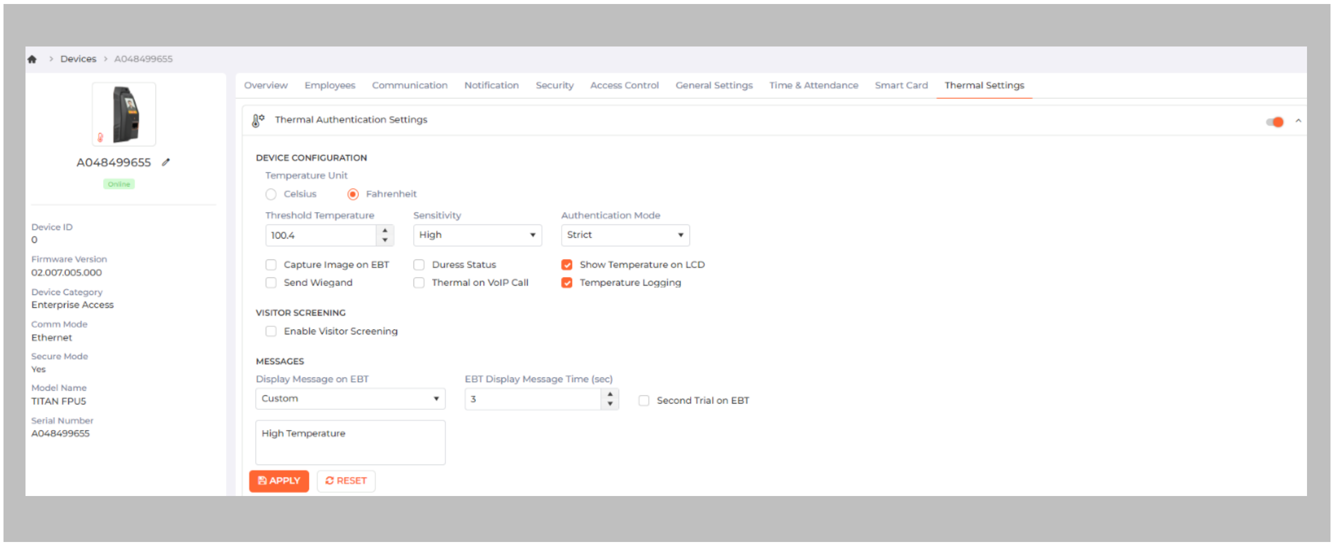
Configuring Thermal Settings

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.



Devices > A048499655

A048499655
Online

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
□ Duress Status
☑ Show Temperature on LCD
□ Send Wiegand
□ Thermal on VoIP Call
☑ 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 65: 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.

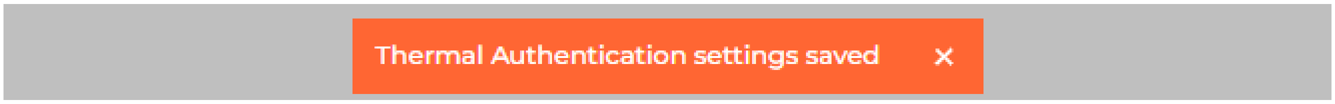
- **Visitor Message Display Time (sec):** Users can configure the length of time that the visitor screening message stays on the screen. The default time is 3 seconds.

- **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**.



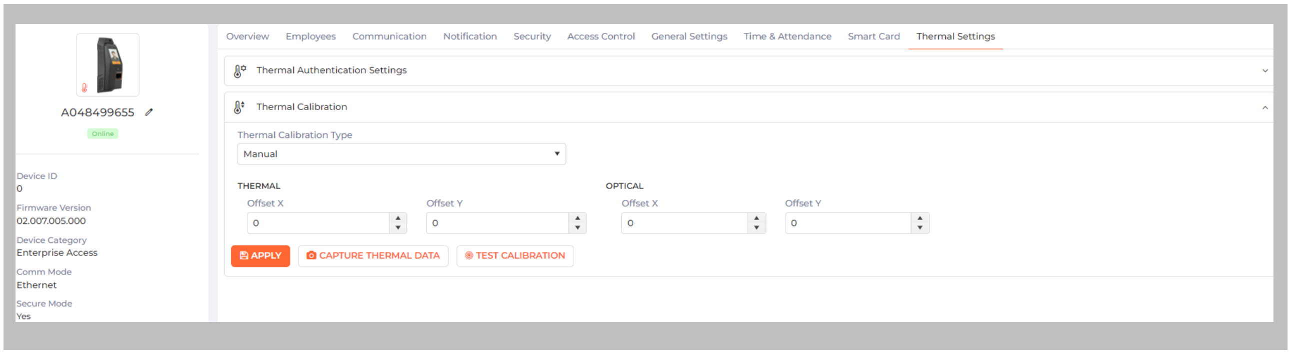
Thermal Authentication settings saved ×

Figure 66: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

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



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 67: 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.

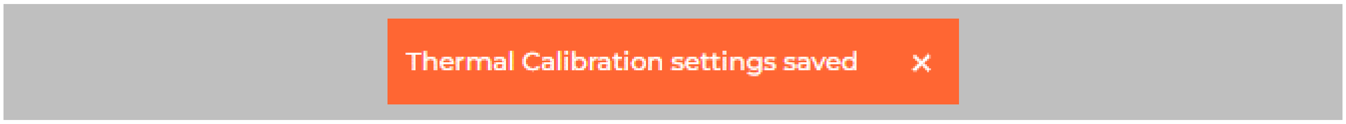
- **Offset Y (Thermal Section):** Users can set the value for the offset Y coordinate of the TIR camera.

- **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

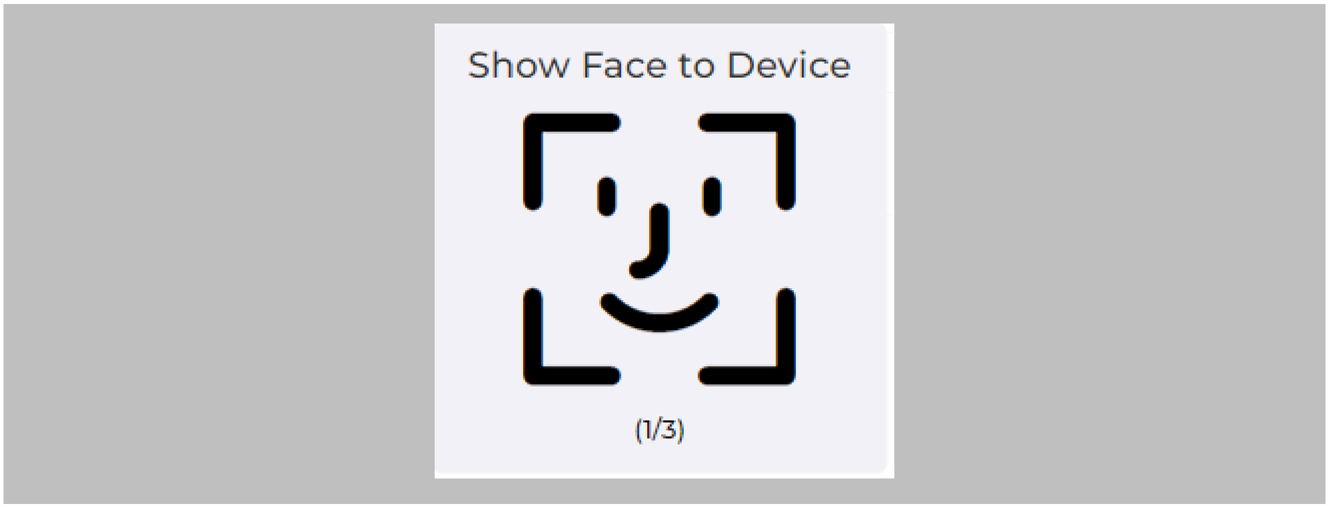
Once all the settings have been configured, click **Apply**, then click **OK**.



Thermal Calibration settings saved ×

Figure 68: 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.



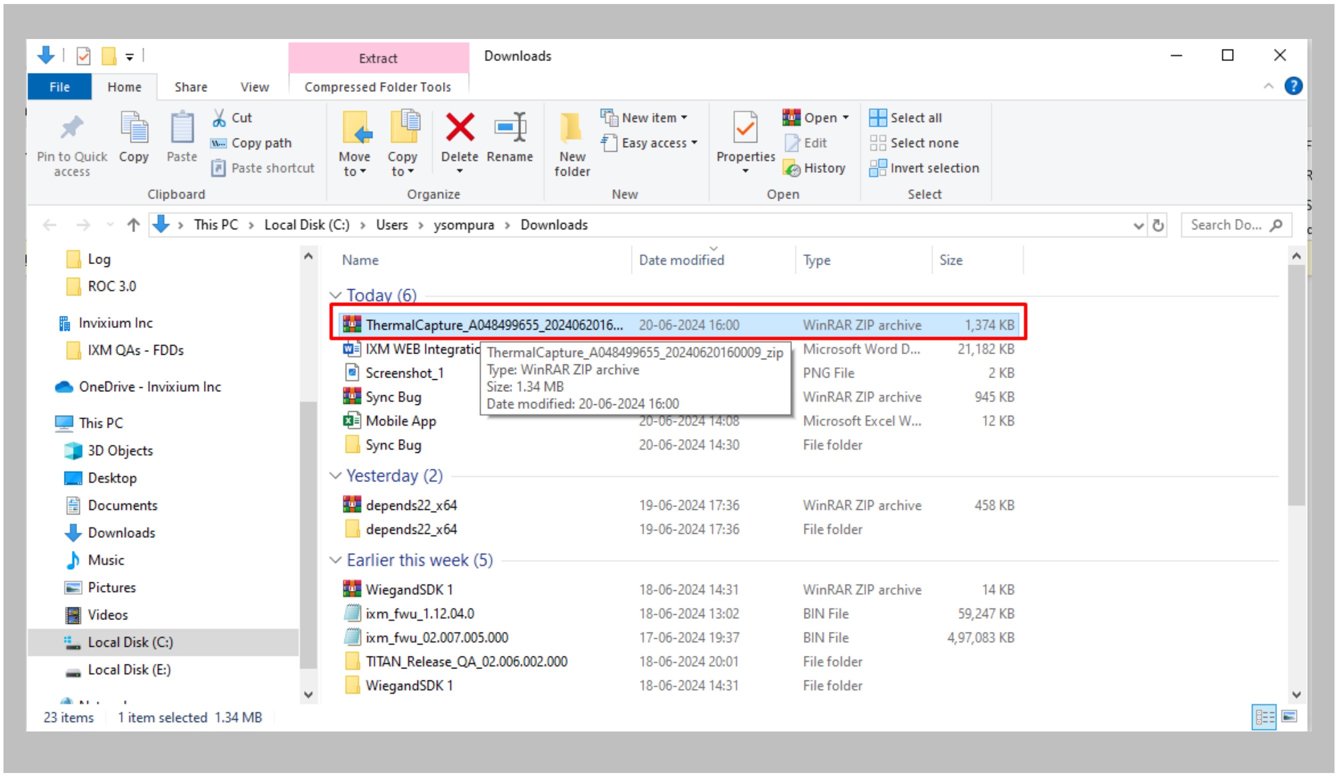
Show Face to Device

(1/3)

Figure 69: 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 70: IXM WEB - Save Captured Thermal Data

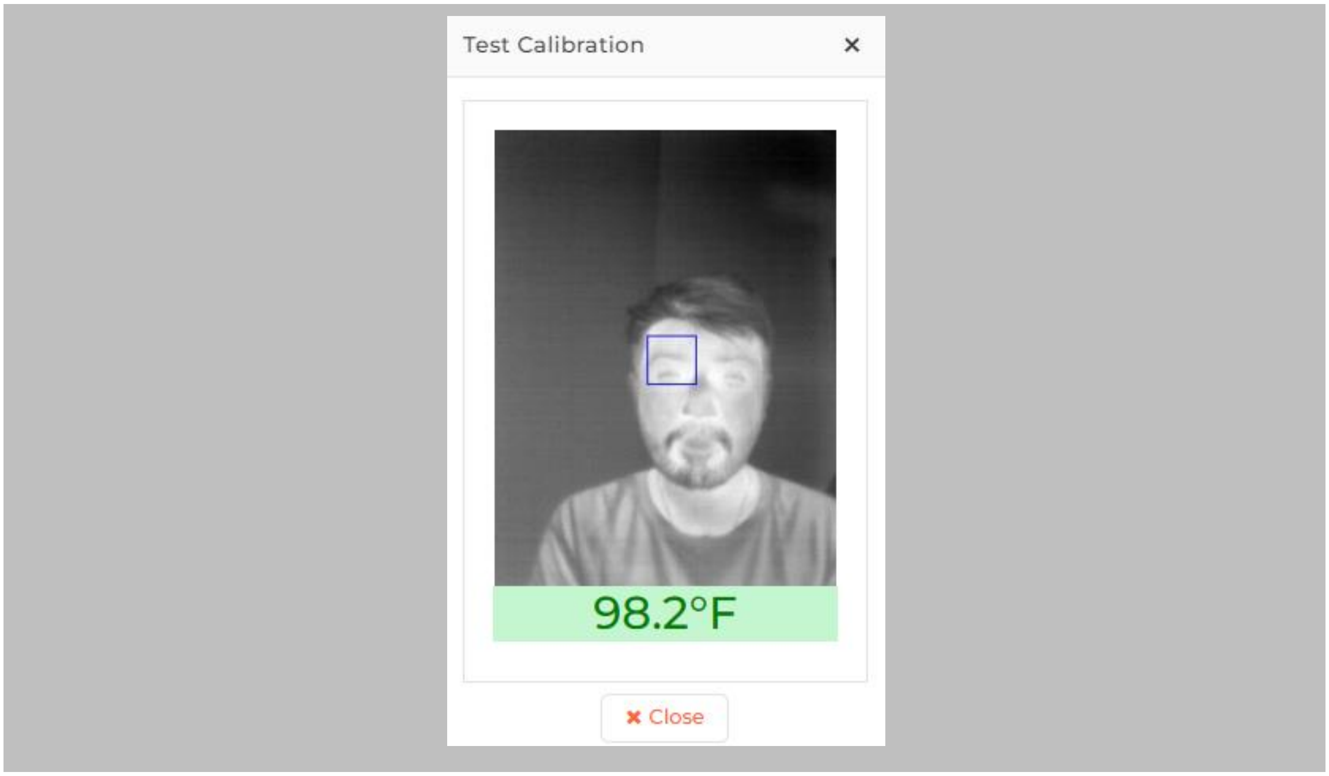
STEP 5

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**.


Test Calibration

98.2°F

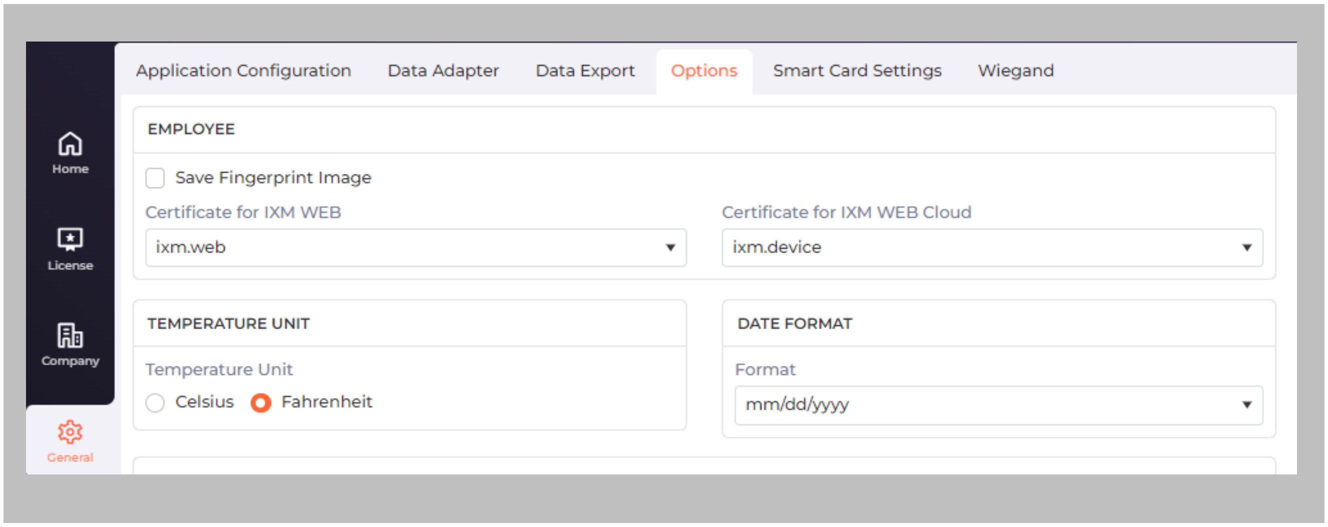
Figure 71: IXM WEB - Test Thermal Calibration

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

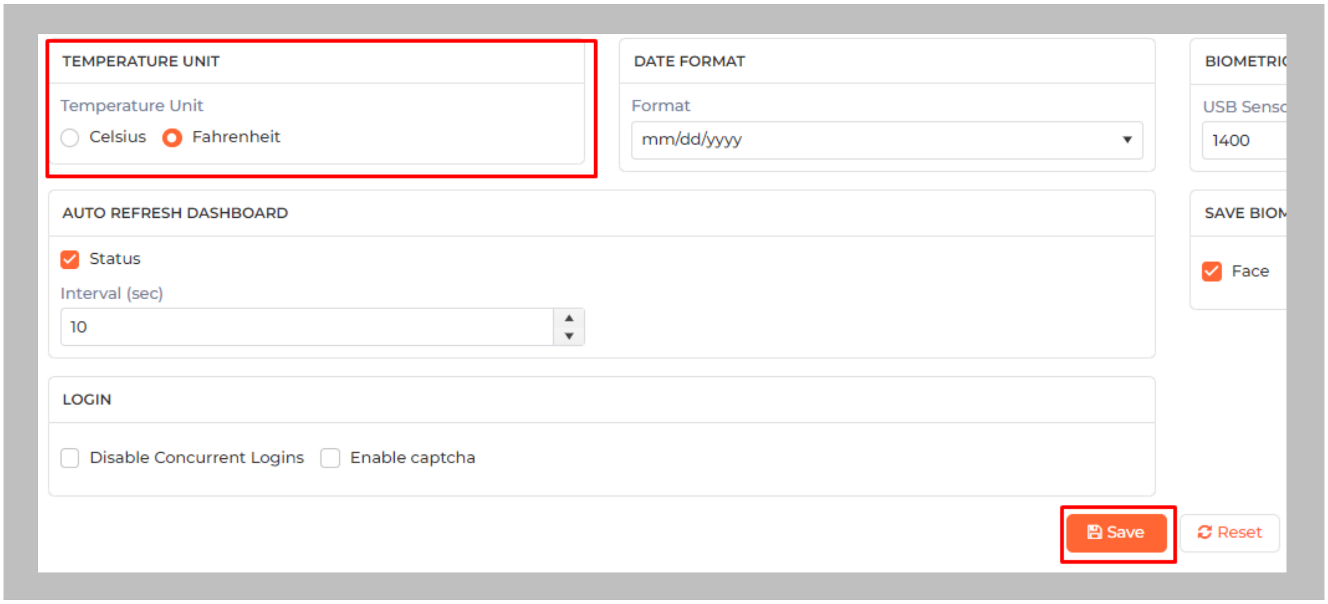
DATE FORMAT

Format: mm/dd/yyyy

Figure 72: 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 ▾

BIOMETRI

USB Senso

1400

AUTO REFRESH DASHBOARD

☑ Status

Interval (sec)

10

SAVE BIOM

☑ Face

LOGIN

☐ Disable Concurrent Logins ☐ Enable captcha

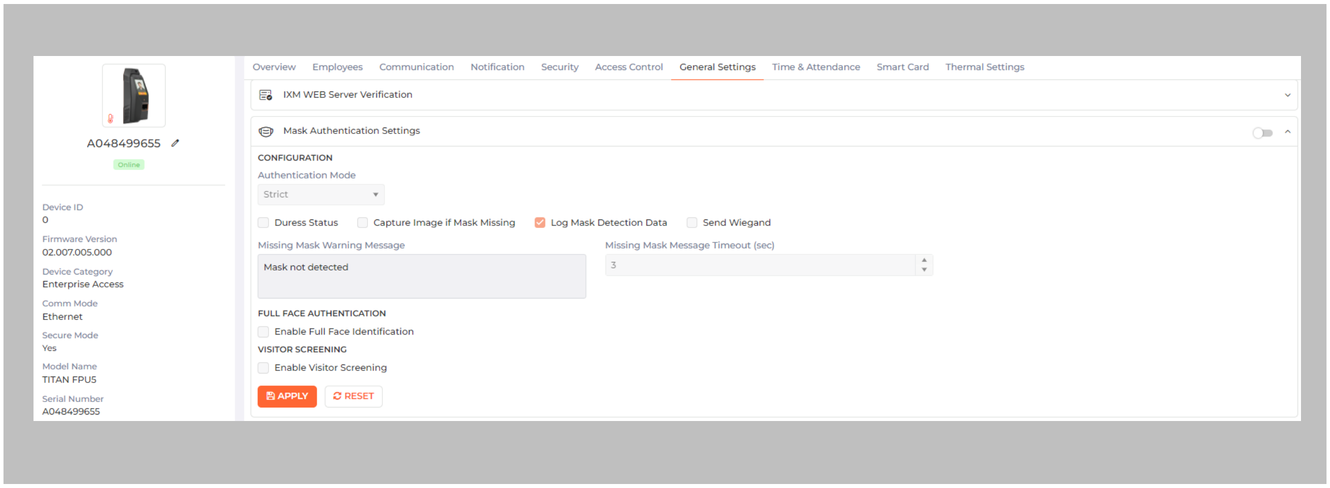
Figure 73: IXM WEB - Save Temperature Unit Setting

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

Configuring Mask Authentication Settings

STEP 1

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



A048499655

Online

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

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 74: 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**.

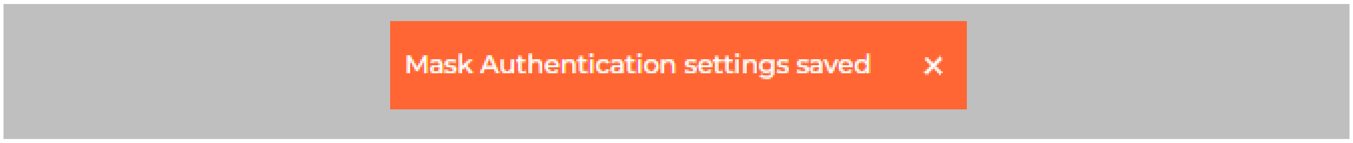
- **Visitor Screening Message:** Set a message that will be displayed when a visitor is showing their face. Messages can be up to 50 characters.

- **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 75: IXM WEB - Save Mask Settings

Pre-configuration for Enrollment

Procedure

STEP 1

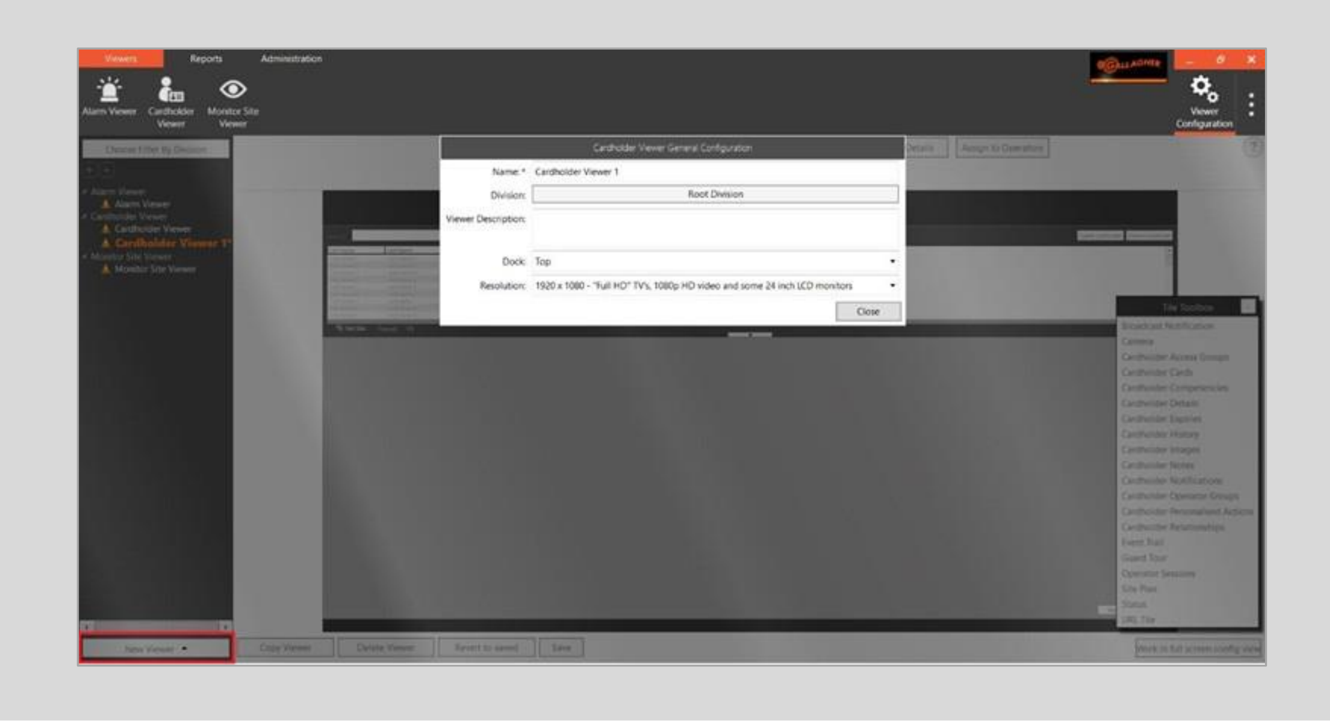
Click **Viewers**, then click **New Viewers** under the **Cardholder Viewers** section.

STEP 2

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

STEP 3

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



Cardholder Viewer General Configuration

Name:* Cardholder Viewer 1

Division: Root Division

Viewer Description:

Dock: Top

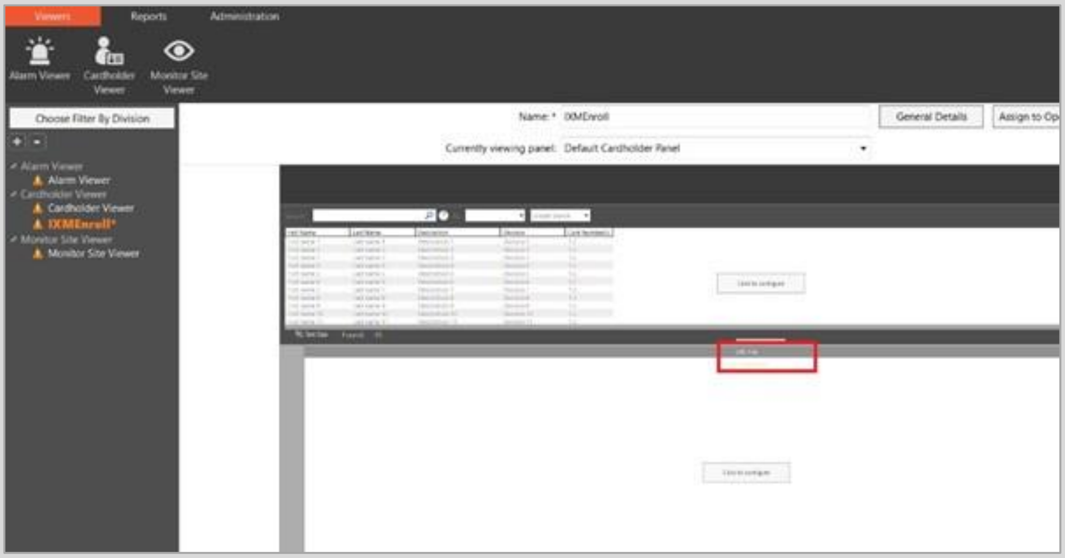
Resolution: 1920 x 1080 - "Full HD" TV's, 1080p HD video and some 24 inch LCD monitors

Close

Figure 76: GCC - Cardholder Viewer General Configuration

STEP 4

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



Name: * IXMEnroll

Currently viewing panel: Default Cardholder Panel

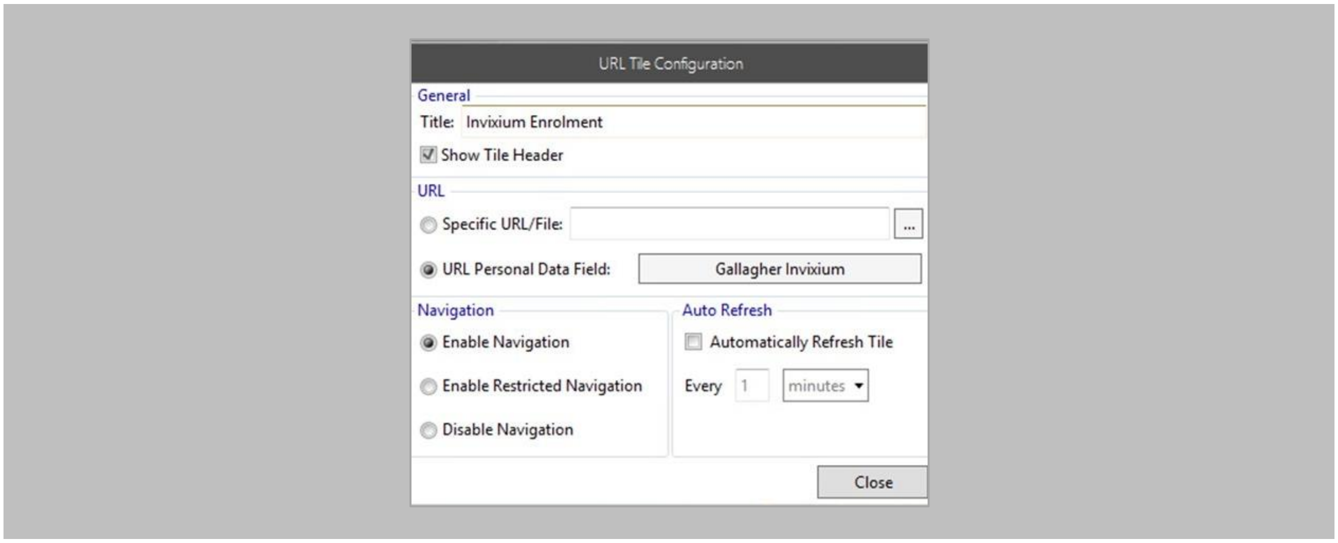
Figure 77: GCC - Enrollment Viewer

STEP 5

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

STEP 6

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



URL Tile Configuration

General

Title: Invixium Enrolment

☑ Show Tile Header

URL

○ Specific URL/File:

● URL Personal Data Field: Gallagher Invixium

Navigation

● Enable Navigation

○ Enable Restricted Navigation

○ Disable Navigation

Auto Refresh

☐ Automatically Refresh Tile

Every 1 minutes

Close

Figure 78: GCC - URL Tile Configuration

STEP 7

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

STEP 8

Click **Save**.

14. Enrollment from Gallagher Command Centre

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

Procedure

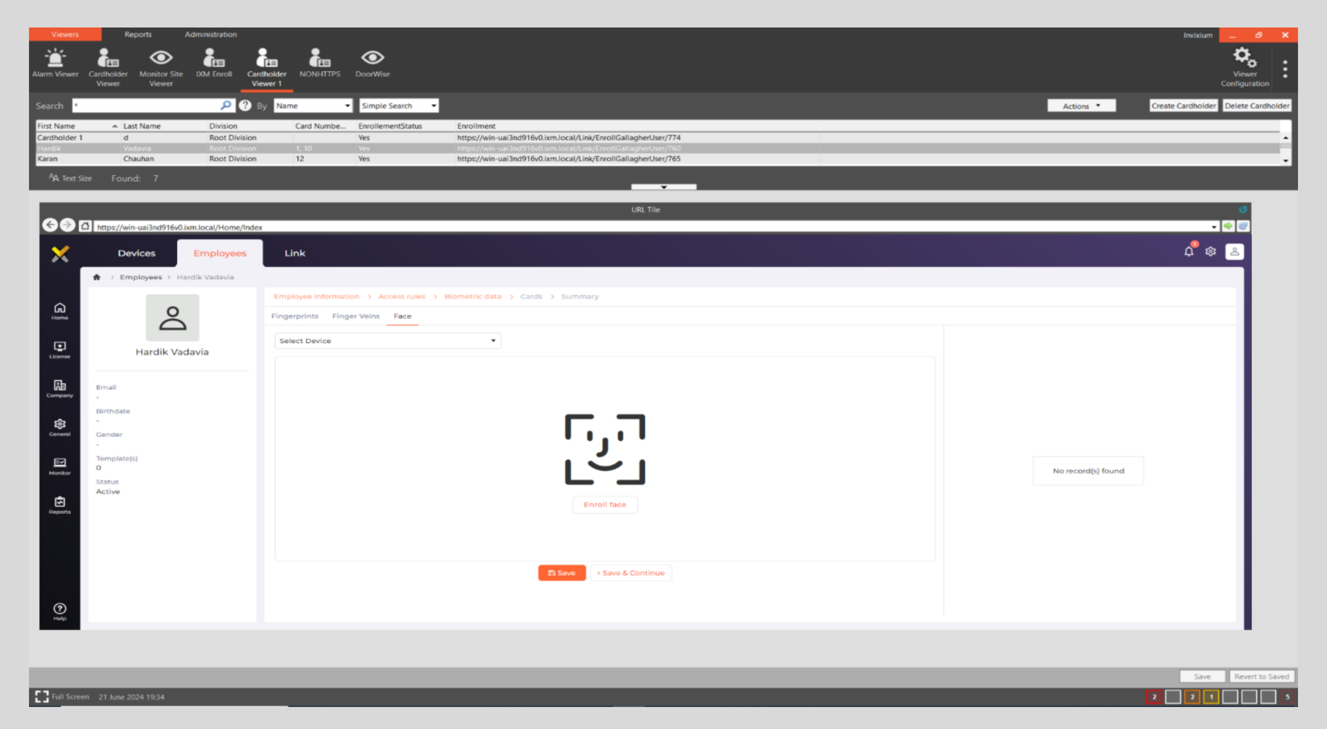
STEP 1

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

Perform enrollment from this viewer option.

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

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



First Name	Last Name	Division	Card Numbe...	EnrollementStatus	Enrollment
Cardholder 1	d	Root Division		Yes	https://win-uai3nd916v0.ixm.local/Link/EnrollGallagherUser/774
Hardik	Vadavia	Root Division	1, 10	Yes	https://win-uai3nd916v0.ixm.local/Link/EnrollGallagherUser/760
Karan	Chauhan	Root Division	12	Yes	https://win-uai3nd916v0.ixm.local/Link/EnrollGallagherUser/765

https://win-uai3nd916v0.ixm.local/Home/Index

Hardik Vadavia

Email
-
Birthdate
-
Gender
-
Template(s)
0
Status
Active

Figure 79: Enrollment Viewer

15. Enrollment Best Practices

Fingerprint Enrollment Best Practices

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

Avoid Poor Fingerprint Conditions

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

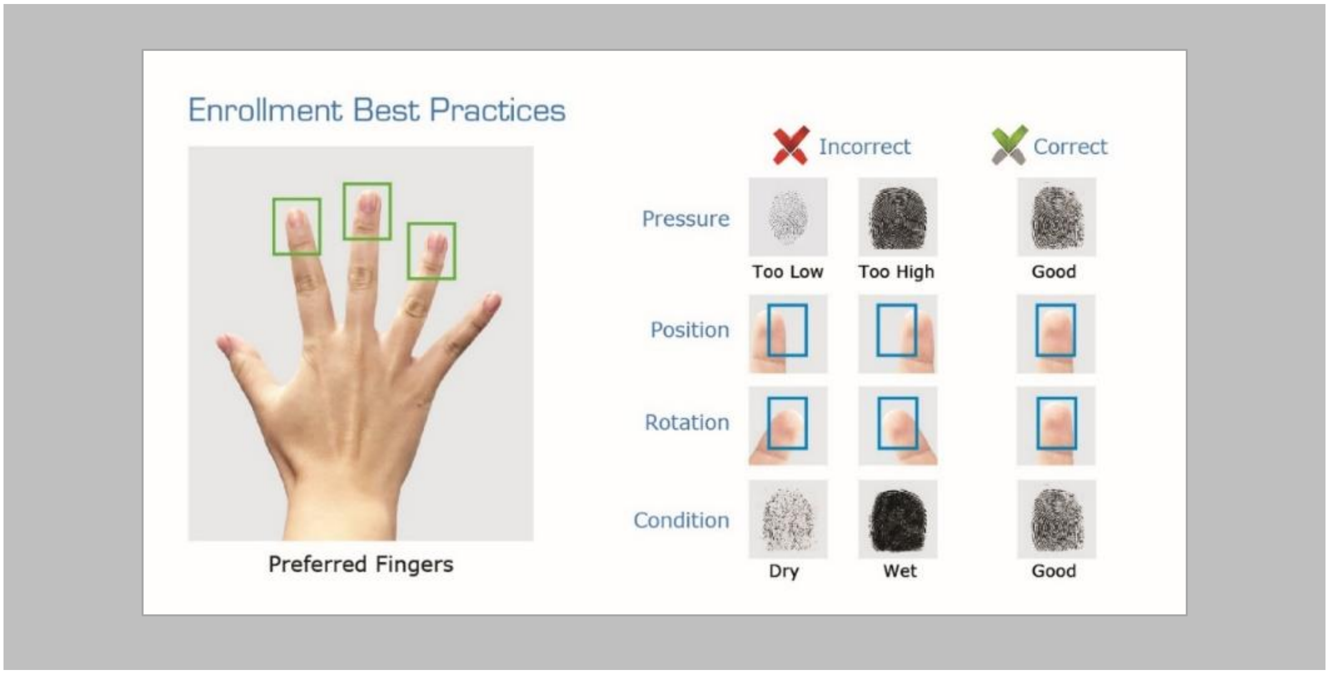


Figure 80: Fingerprint Enrollment Best Practices

Fingerprint Image Samples

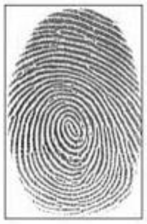
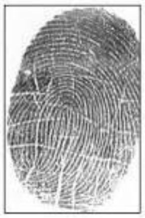
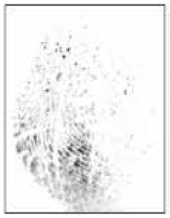
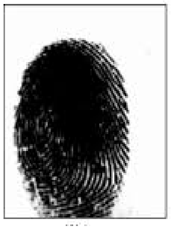
Fingerprint Sample	Result	Recommendation
	Good Fingerprint	Always try and get a good fingerprint like this for a good enrollment score
	Fingerprint with cuts	Invixium recommends using Card + Biometrics or Card + PIN
	Dry finger	Moisten finger and re-enroll for better results
	Wet/Sweaty finger	Rub finger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

Figure 81: 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.

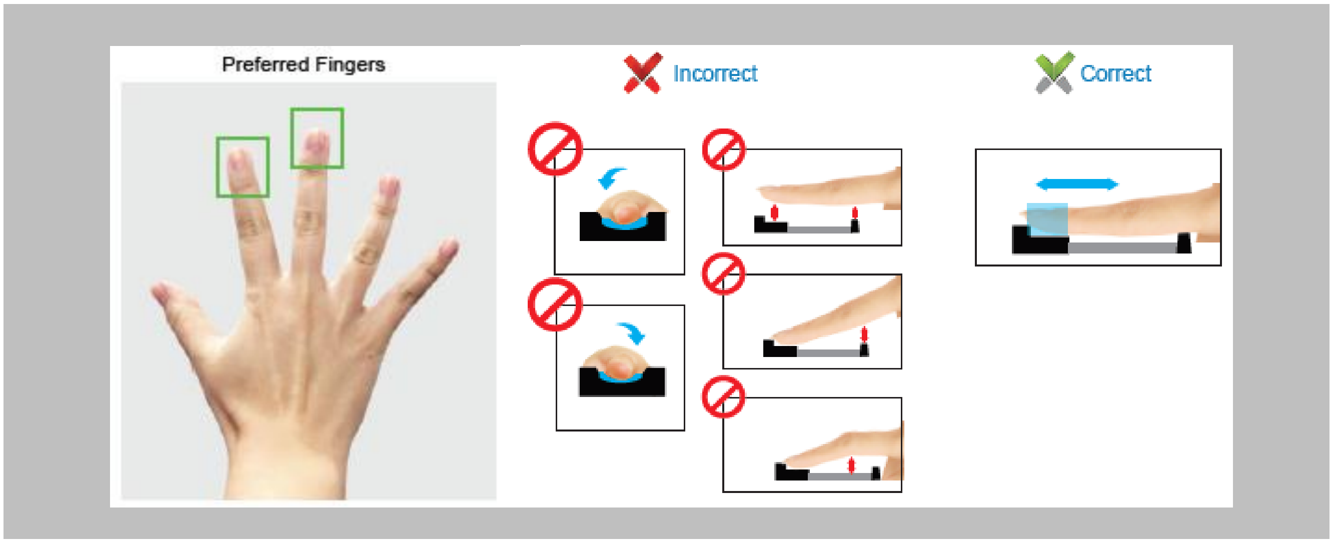


Figure 82: Finger Vein Enrollment Best Practices

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.

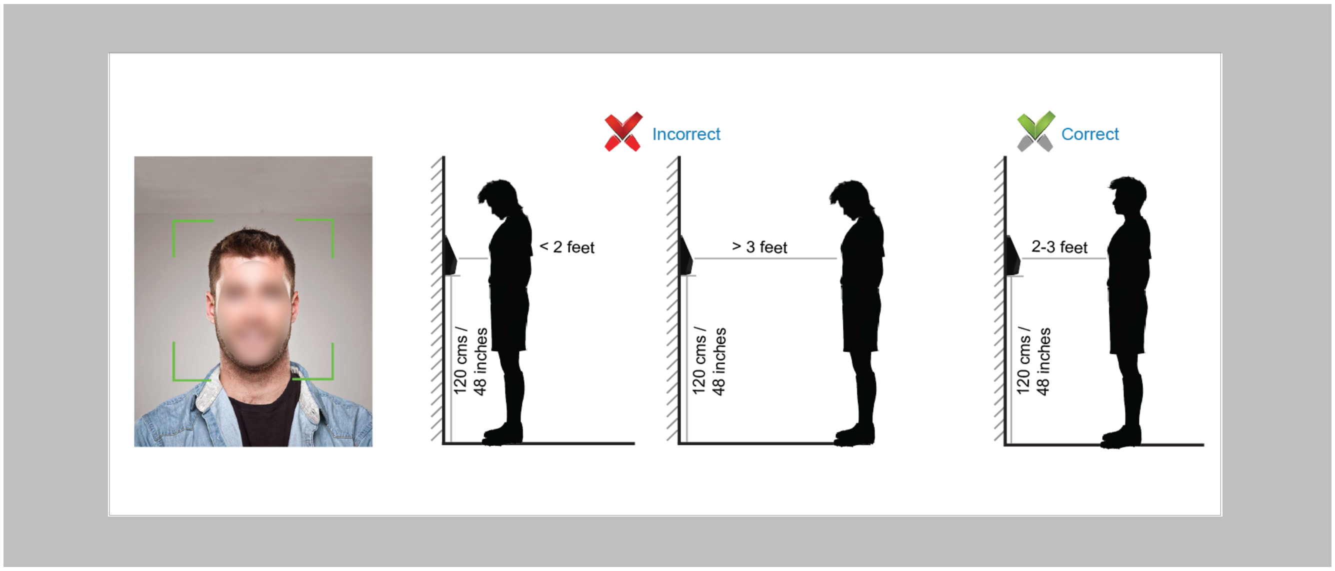


Figure 83: Face Enrollment Best Practices

16. Send Logical Events to Command Centre

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

Note:

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

Procedure

STEP 1

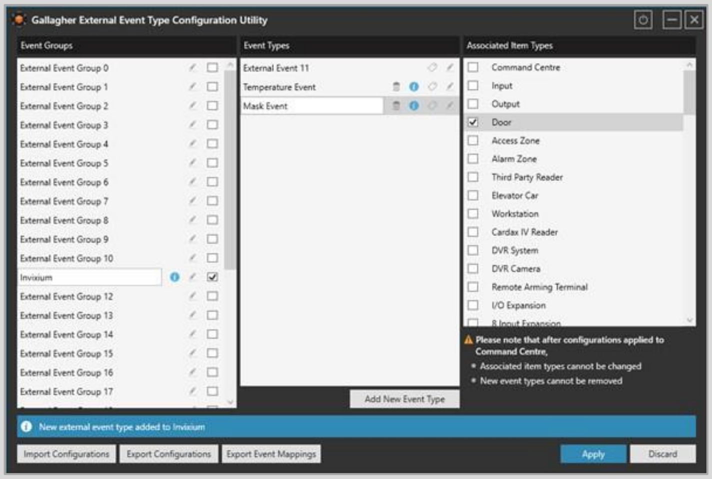
IXM WEB requires an External Event Group named Invixium to be present in Command Centre. This could be done using the event utility provided in the installation path. Invixium recommends skipping the first 10 pre-existing External Event Groups and changing the name of 11th or any other to Invixium.

STEP 2

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

STEP 3

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



Gallagher External Event Type Configuration Utility

Event Groups

- External Event Group 0 □
- External Event Group 1 □
- External Event Group 2 □
- External Event Group 3 □
- External Event Group 4 □
- External Event Group 5 □
- External Event Group 6 □
- External Event Group 7 □
- External Event Group 8 □
- External Event Group 9 □
- External Event Group 10 □
- Invixium ☑
- External Event Group 12 □
- External Event Group 13 □
- External Event Group 14 □
- External Event Group 15 □
- External Event Group 16 □
- External Event Group 17 □

Event Types

- External Event 11
- Temperature Event
- Mask Event

Associated Item Types

- □ Command Centre
- □ Input
- □ Output
- ☑ Door
- □ Access Zone
- □ Alarm Zone
- □ Third Party Reader
- □ Elevator Car
- □ Workstation
- □ Cardax IV Reader
- □ DVR System
- □ DVR Camera
- □ Remote Arming Terminal
- □ I/O Expansion
- □ 8 Input Expansion

Please note that after configurations applied to Command Centre,

- Associated item types cannot be changed
- New event types cannot be removed

New external event type added to Invixium

Figure 84: GCC - Gallagher External Event Type Configuration Utility

STEP 4

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

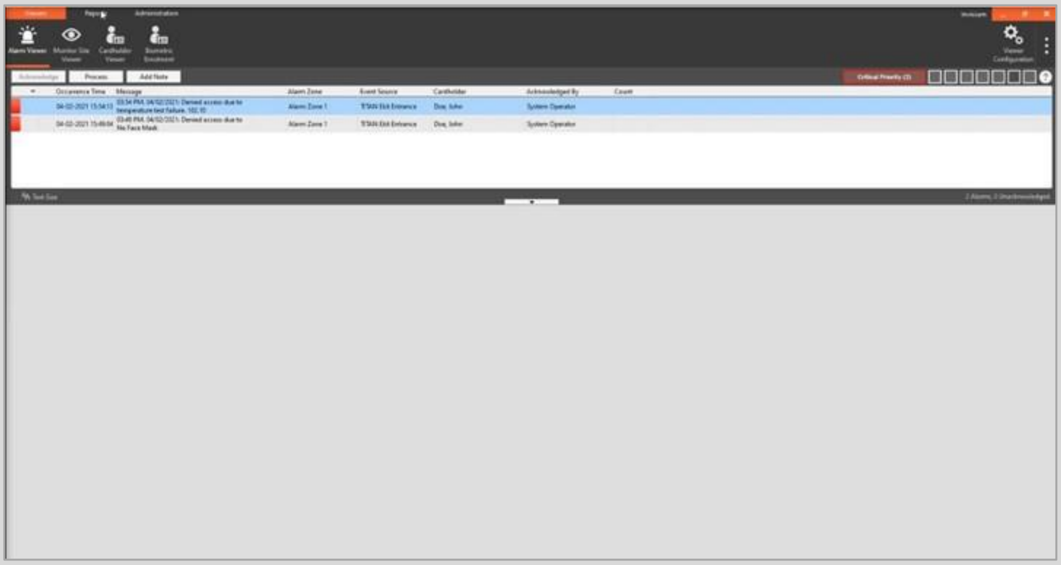
Note: If an employee violates both mask and temperature rules, then both events will be reported to Command Centre.

STEP 5

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

STEP 6

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



Occurrence Time	Message	Alarm Zone	Event Source	Cardholder	Acknowledged By	Count
04-02-2021 15:54:13	03:54 PM, 04/02/2021: Denied access due to temperature test failure. 102.10	Alarm Zone 1	TITAN Exit Entrance	Doe, John	System Operator	
04-02-2021 15:49:04	03:49 PM, 04/02/2021: Denied access due to No Face Mask	Alarm Zone 1	TITAN Exit Entrance	Doe, John	System Operator	

Figure 85: GCC - Cardholder’s Notes

17. Appendix

Installing Invixium IXM WEB with Default Installation using SQL Server 2014

Note:

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

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

Procedure

STEP 1

Run the **installer.exe**

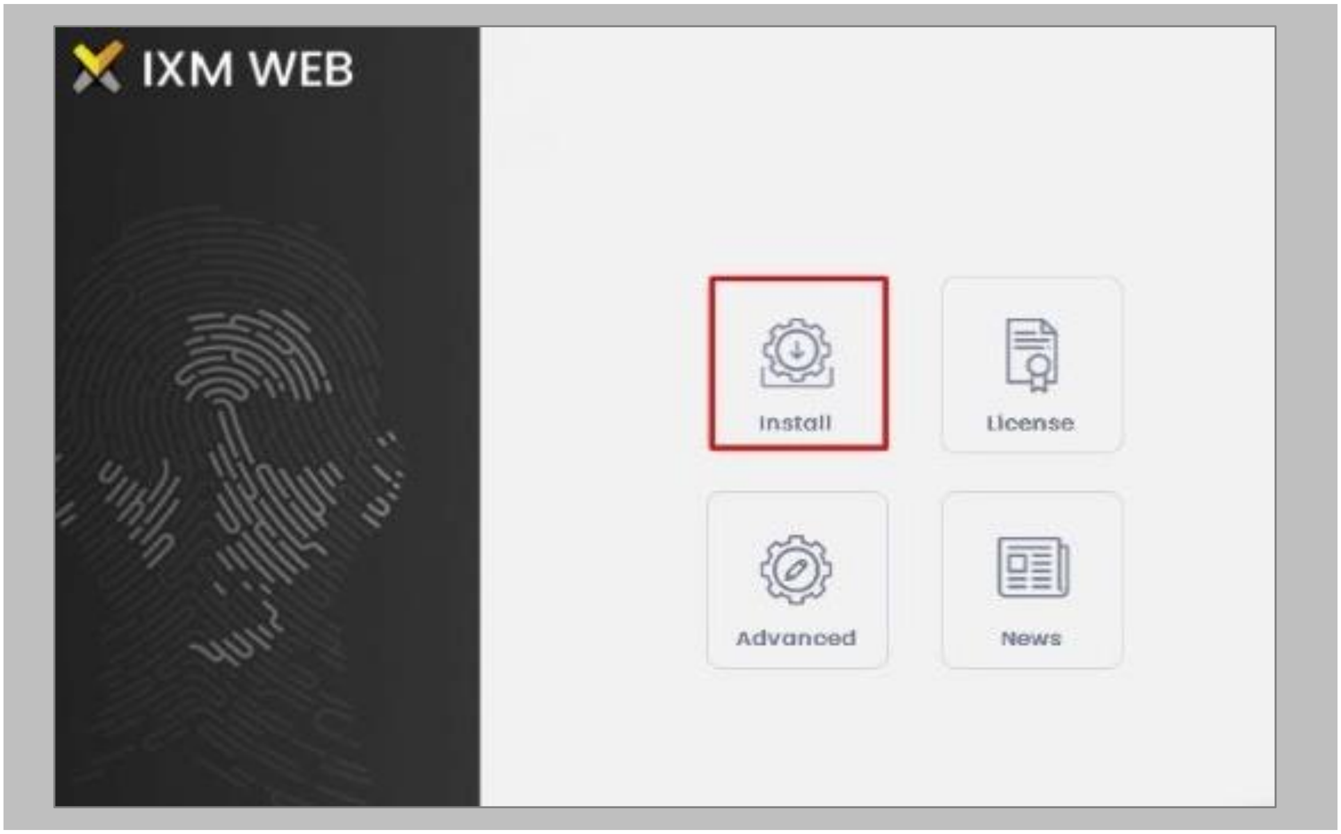
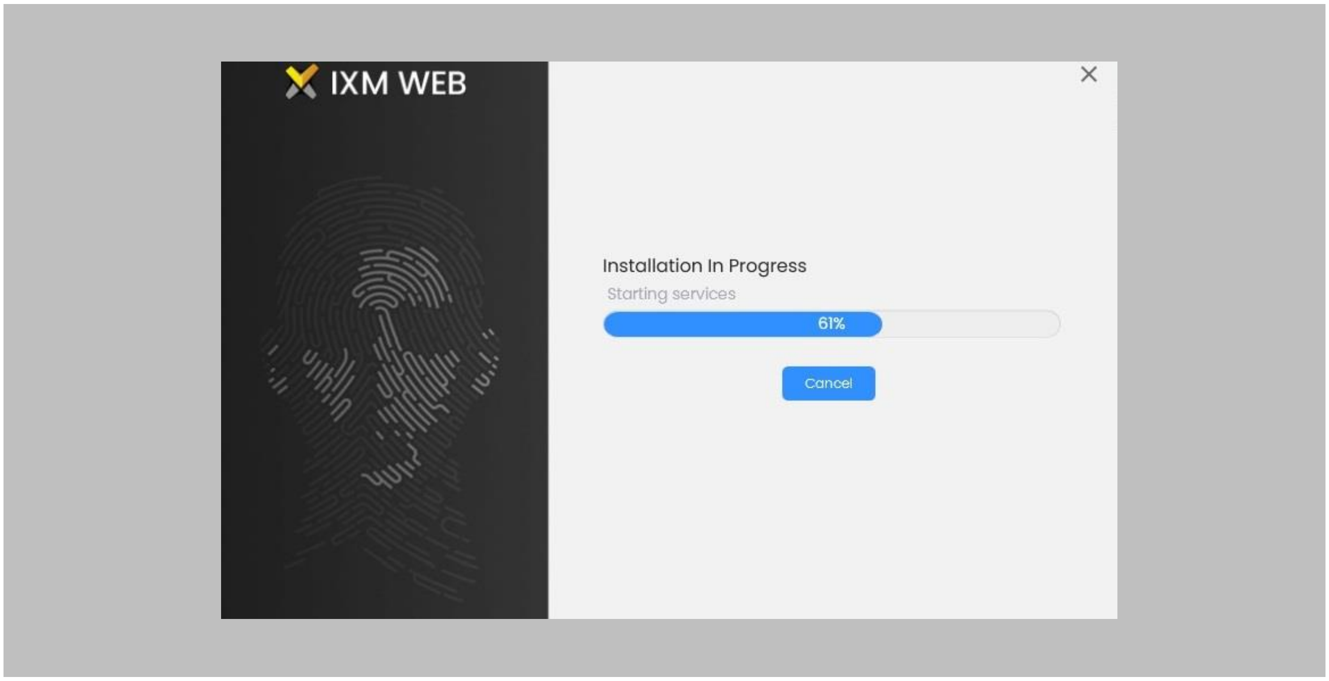


Figure 86: Install IXM WEB

Note: Installs SQL 2014 Express.



Installation In Progress

Starting services

Figure 87: 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.

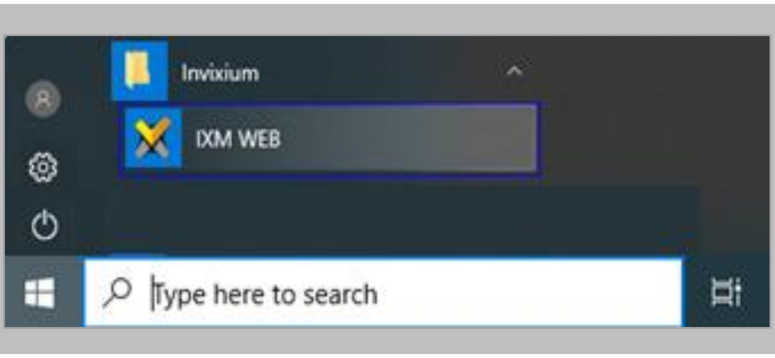
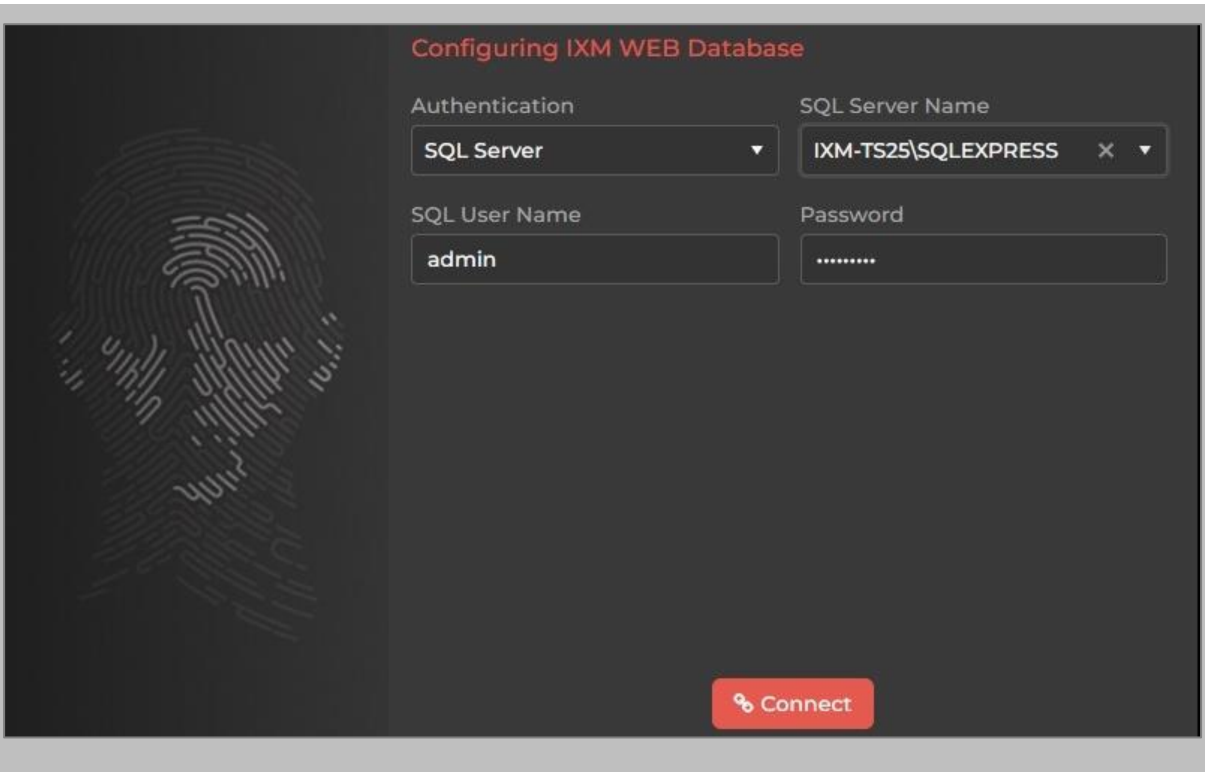


Figure 88: IXM WEB - Shortcut Icon on Desktop

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

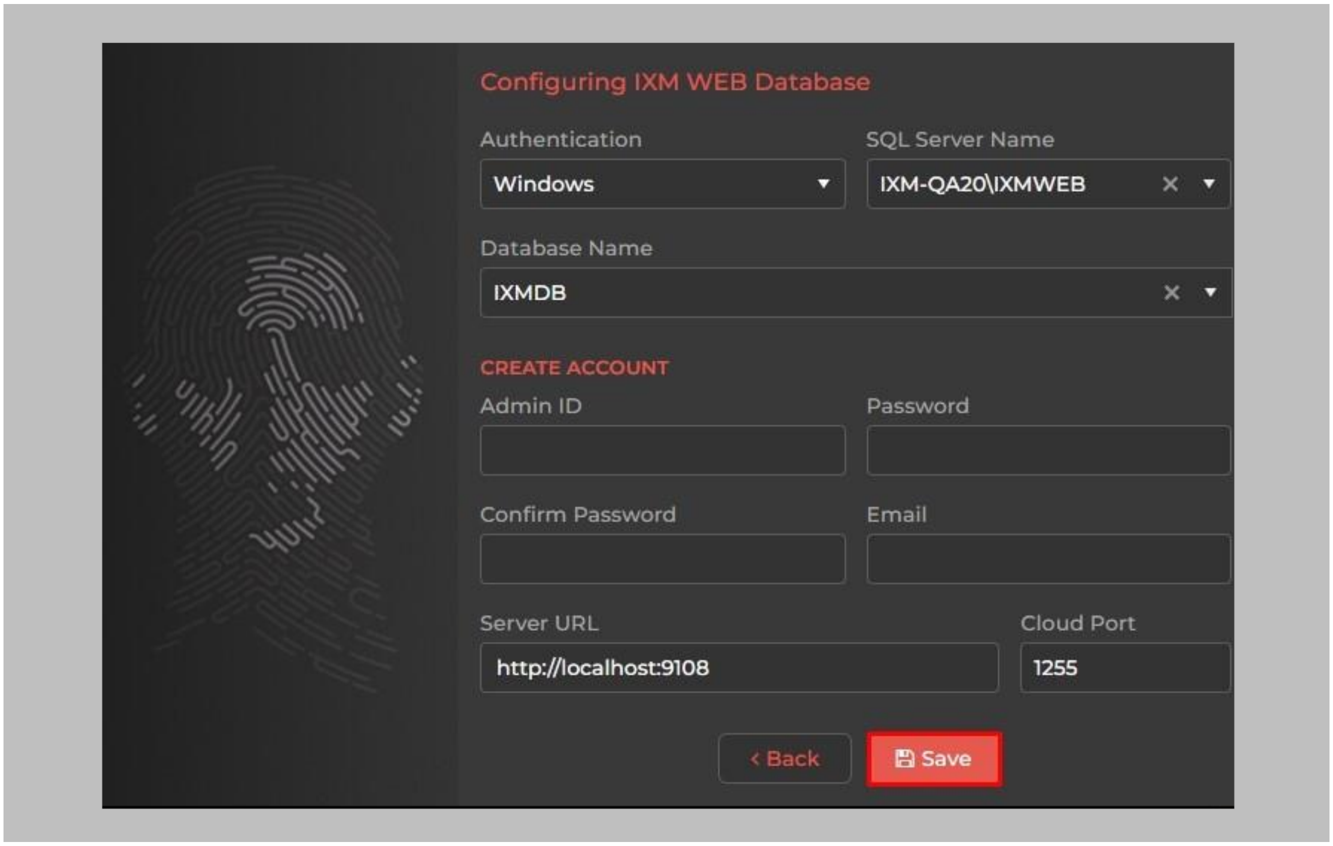
SQL User Name: admin

Password: •••••••••

Figure 89: 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 90: 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

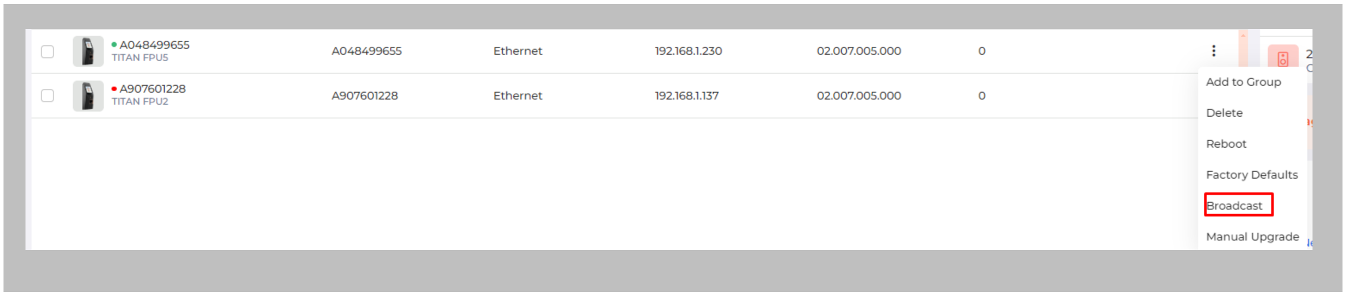
Click **Save**. The software will now create the database and continue setup. This could take several minutes.

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.

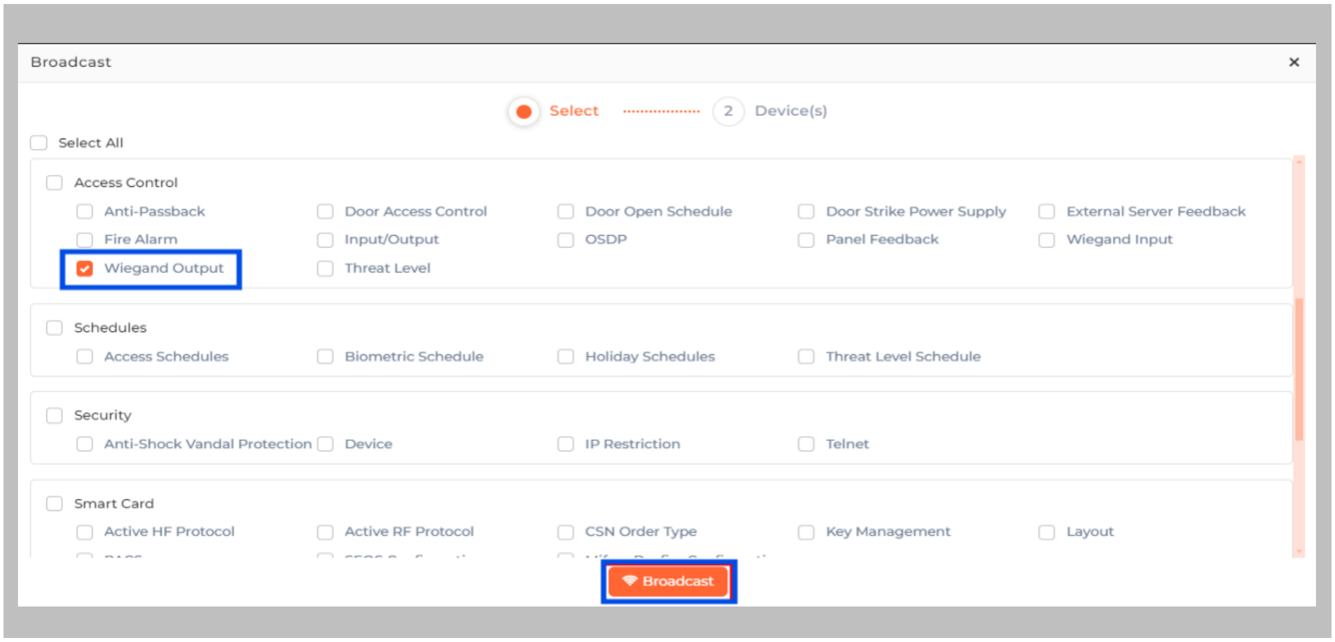


☐	A048499655 TITAN FPU5	A048499655	Ethernet	192.168.1.230	02.007.005.000	0
☐	A907601228 TITAN FPU2	A907601228	Ethernet	192.168.1.137	02.007.005.000	0

Figure 91: IXM WEB - Broadcast Option

STEP 2

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



☐ 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 92: IXM WEB - Broadcast Wiegand Output Settings

STEP 3

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

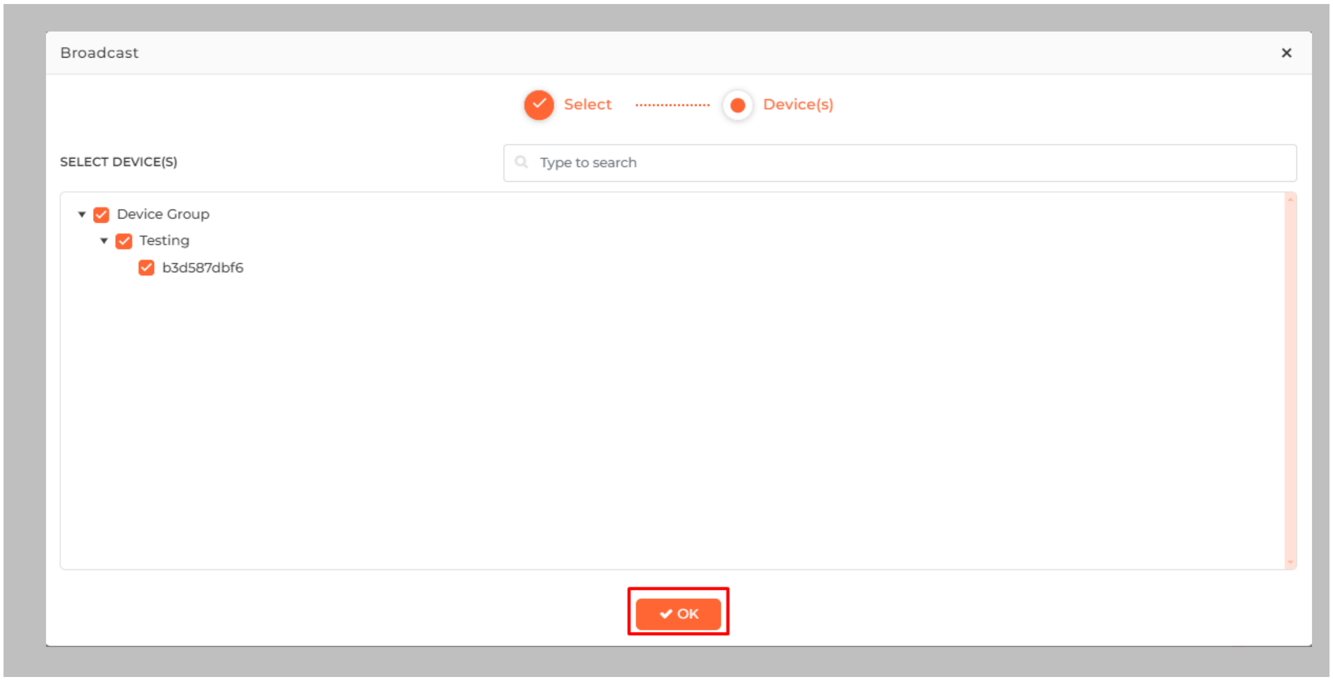


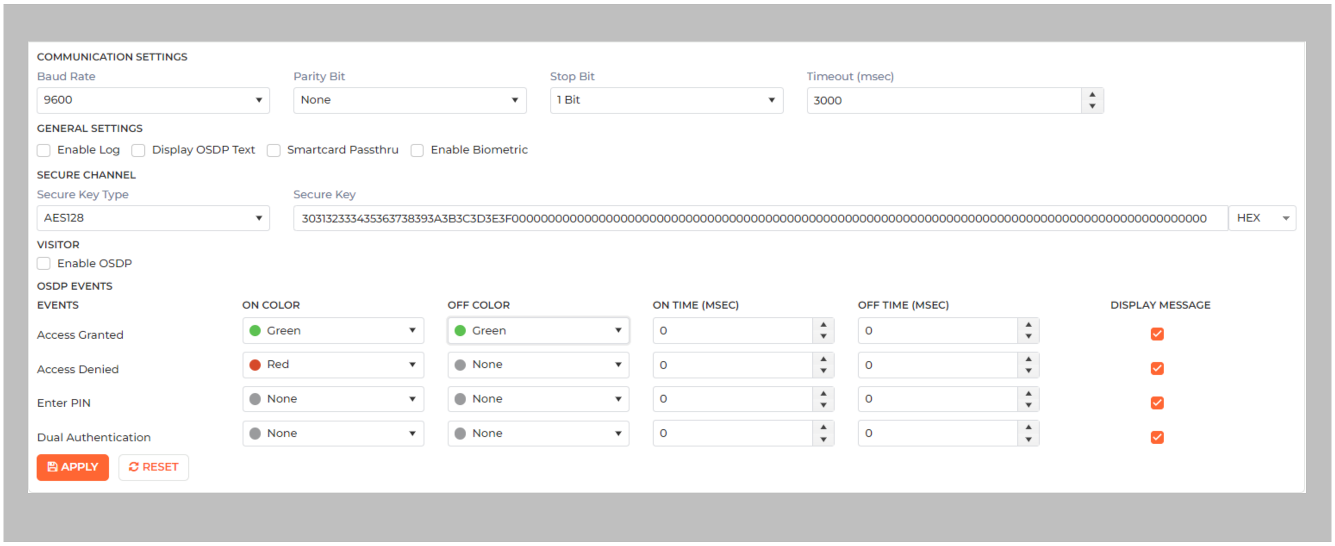
Figure 93: IXM WEB - Broadcast to Devices

Configuring for OSDP Connection

STEP 1

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

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



COMMUNICATION SETTINGS

Baud Rate: 9600

Parity Bit: None

Stop Bit: 1 Bit

Timeout (msec): 3000

GENERAL SETTINGS

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

SECURE CHANNEL

Secure Key Type: AES128

Secure Key: 303132333435363738393A3B3C3D3E3F0000000000000000000000000000000000000000000000000000000000000000 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 94: IXM WEB - OSDP Settings

STEP 2

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

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

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

Table 5: IXM WEB - OSDP Configuration Options

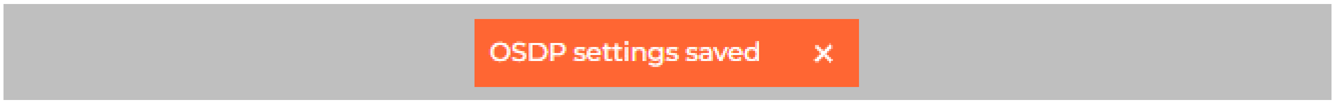
Note: Mismatches between the unit and Access Control Panel LED configuration would cause unrecognized events.

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

Table 6: IXM WEB - OSDP Text Options

STEP 3

Click **Apply** to save the settings.

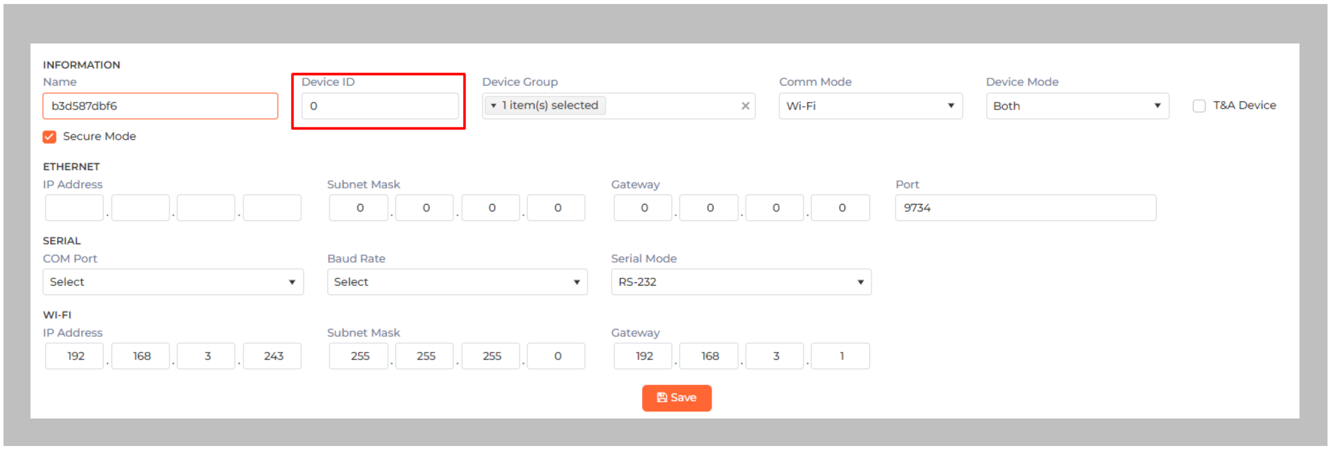


OSDP settings saved

Figure 95: IXM WEB - Save OSDP Settings

STEP 4

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



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

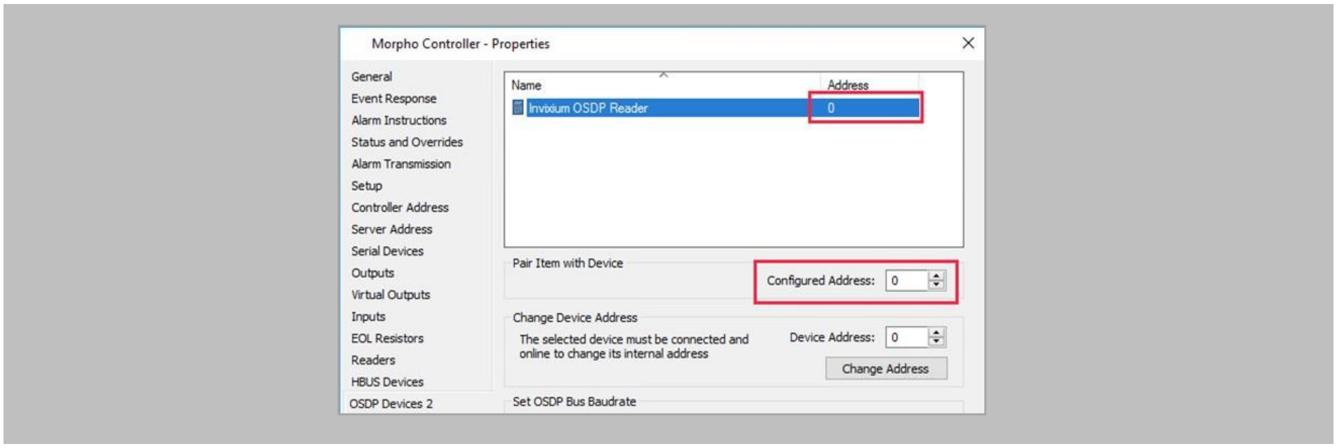
Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 3 . 1

Figure 96: IXM WEB - Edit Device Options

STEP 5

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



Morpho Controller - Properties

Name	Address
Invixium OSDP Reader	0

Pair Item with Device

Configured Address: 0

Change Device Address

The selected device must be connected and online to change its internal address

Device Address: 0

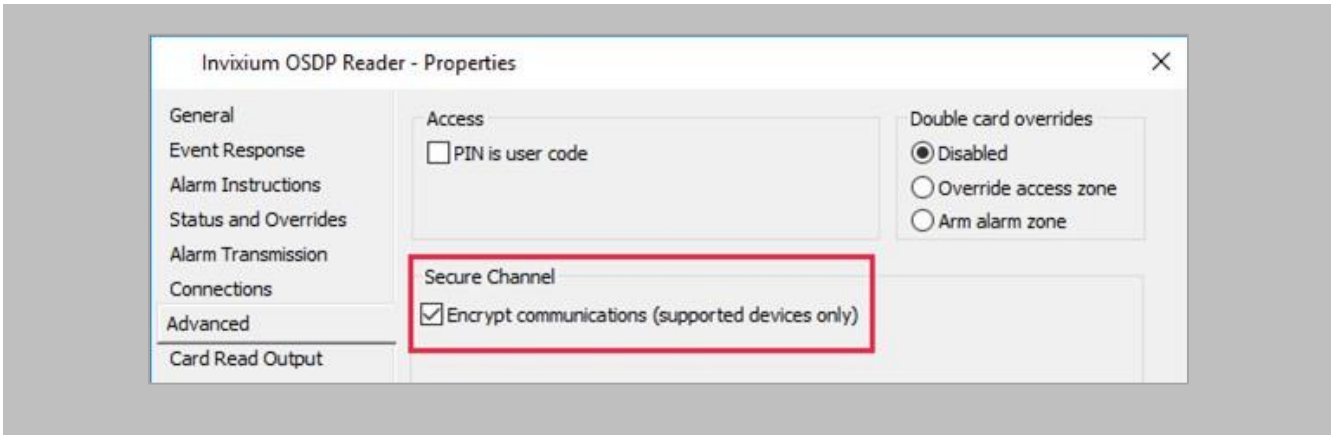
Set OSDP Bus Baudrate

Figure 97: GCC - Device ID

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

STEP 6

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



Invixium OSDP Reader - Properties

Access

□ PIN is user code

Double card overrides

● Disabled

○ Override access zone

○ Arm alarm zone

Secure Channel

☑ Encrypt communications (supported devices only)

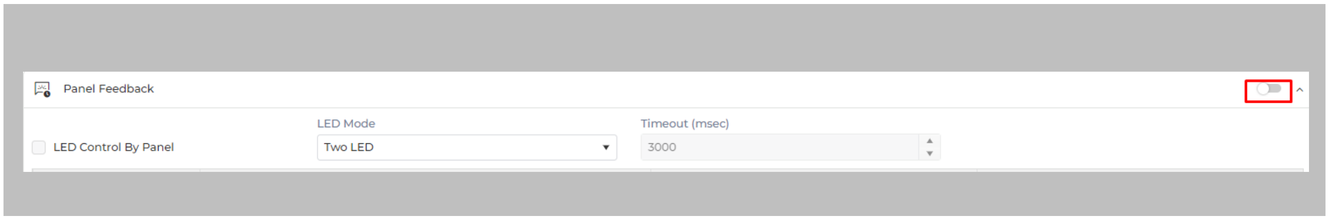
Figure 98: GCC - Setup OSDP reader

STEP 7

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

STEP 8

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



Panel Feedback

□ LED Control By Panel

LED Mode: Two LED

Timeout (msec): 3000

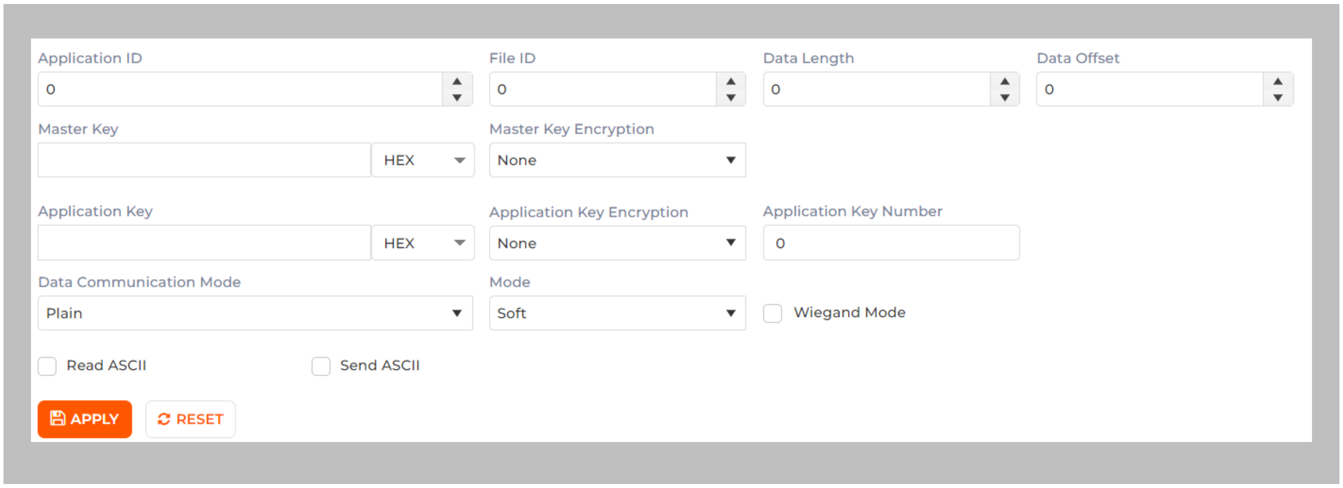
Figure 99: IXM WEB - Disable Panel Feedback

Configuring MIFARE DESFire Custom Cards

STEP 1

From the **Devices** tab. Select the required **Device** and navigate to **Smart Card**. Click **MIFARE DESFire Configuration**.

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



Application ID: 0

File ID: 0

Data Length: 0

Data Offset: 0

Master Key: HEX

Master Key Encryption: None

Application Key: HEX

Application Key Encryption: None

Application Key Number: 0

Data Communication Mode: Plain

Mode: Soft

□ Wiegand Mode

□ Read ASCII

□ Send ASCII

Figure 100: IXM WEB - MIFARE DESFire Configuration

STEP 2

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

Application ID	The application ID of the Gallagher cards.
File ID	The file ID of the Gallagher cards.
Data Length	Enter data length of Gallagher cards.
Data Offset	Enter data offset of Gallagher cards.
Master Key	Enter Master key of Gallagher cards.
Master Key Encryption	Select Master Key Encryption from the dropdown as per

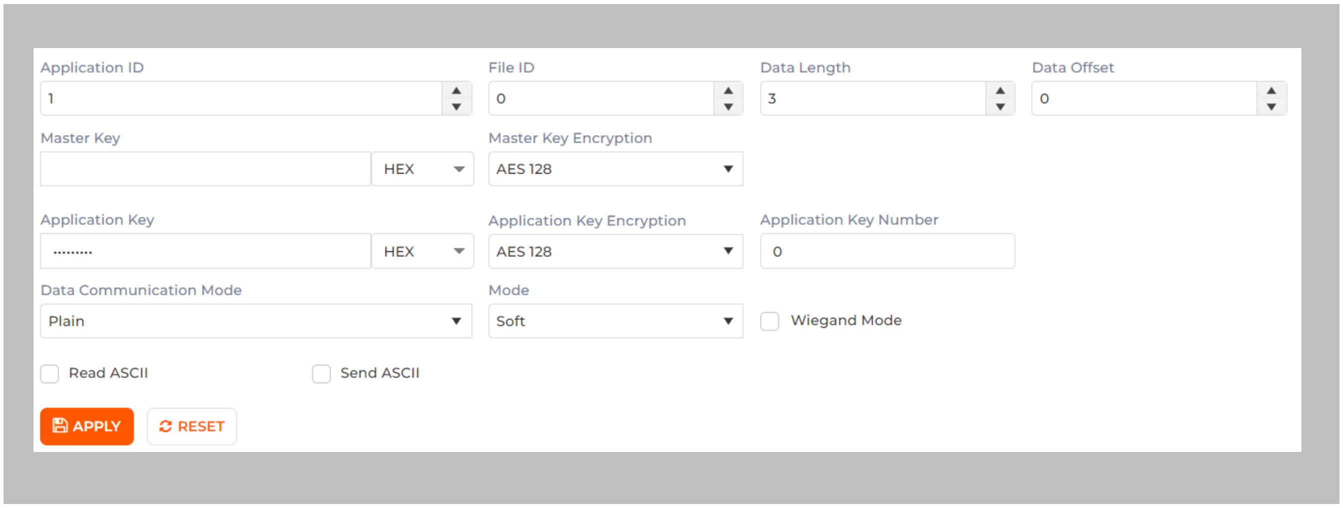
	requirement. Options are: • None • 2K 3DES • 3K 3DES • AES 128
Application Key	Enter Application key of Gallagher cards.
Application Key Encryption	Select Application Key Encryption from the dropdown as per requirement. Options are: • None • 2K 3DES • 3K 3DES • AES 128
Application Key Number	Enter Application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

Read ASCII	Enable Read ASCII so that the Device can read the ASCII data from the Smart Card as per the configuration.
Send ASCII	Enable Send ASCII so that the Device can send the ASCII raw data.

Table 7: IXM WEB – MIFARE DESFire Configuration Options

STEP 3

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



Application ID: 1

File ID: 0

Data Length: 3

Data Offset: 0

Master Key: HEX

Master Key Encryption: AES 128

Application Key: ········· HEX

Application Key Encryption: AES 128

Application Key Number: 0

Data Communication Mode: Plain

Mode: Soft

□ Wiegand Mode

□ Read ASCII

□ Send ASCII

Figure 101: IXM WEB - MIFARE DESFire Sample Configuration

Wiring and Termination

Procedure

Earth Ground

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

STEP 1

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

STEP 2

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

STEP 3

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

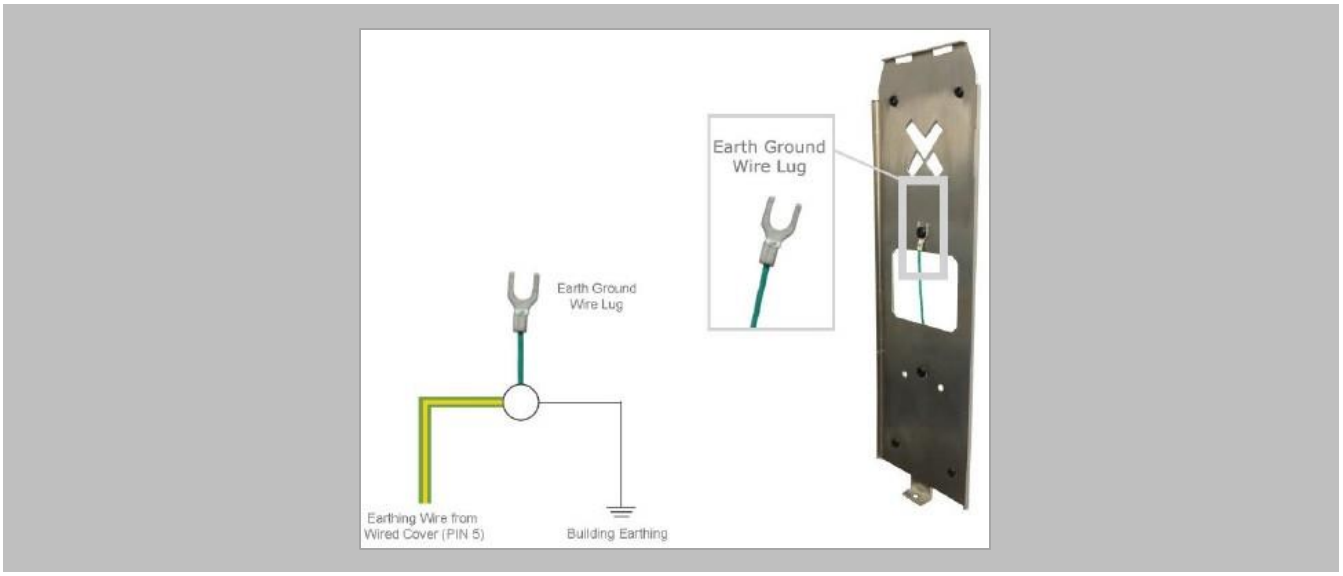


Figure 102: Earth Ground Wiring

Wiring

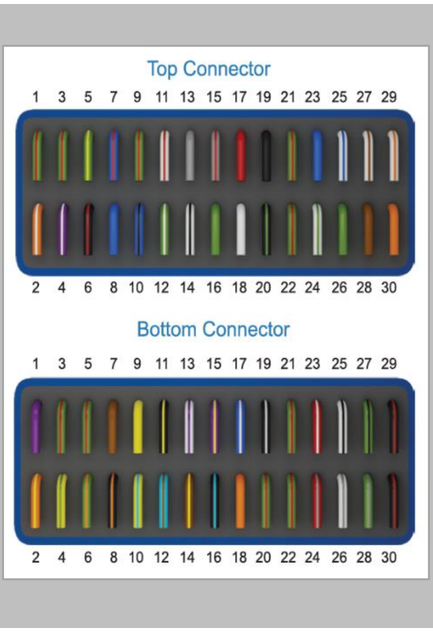
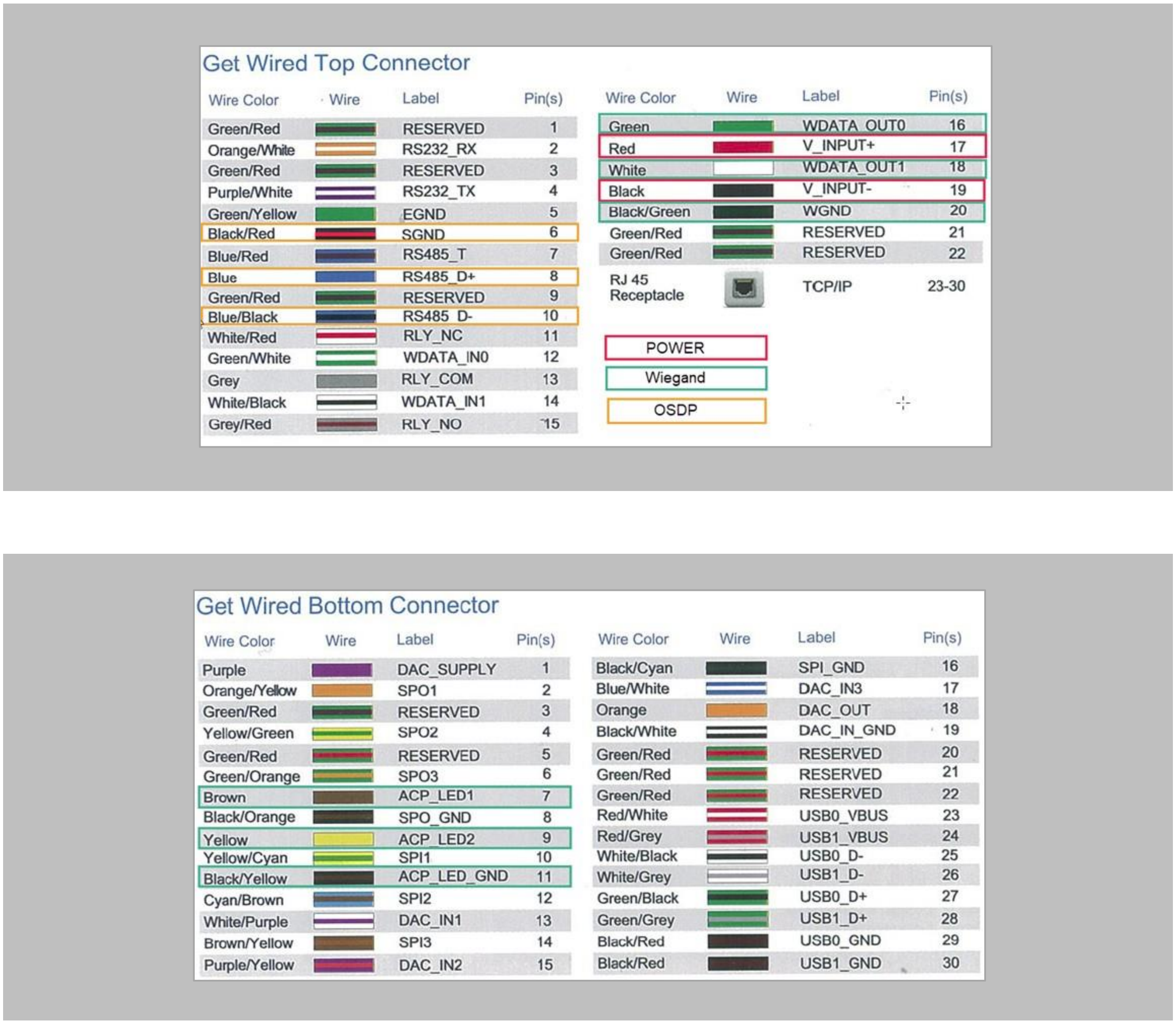


Figure 103: IXM TITAN – Top & Bottom Connector Wiring



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 104: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand and OSDP.

Invixium devices can be integrated with Gallagher Controller on:

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

Wiegand Connection

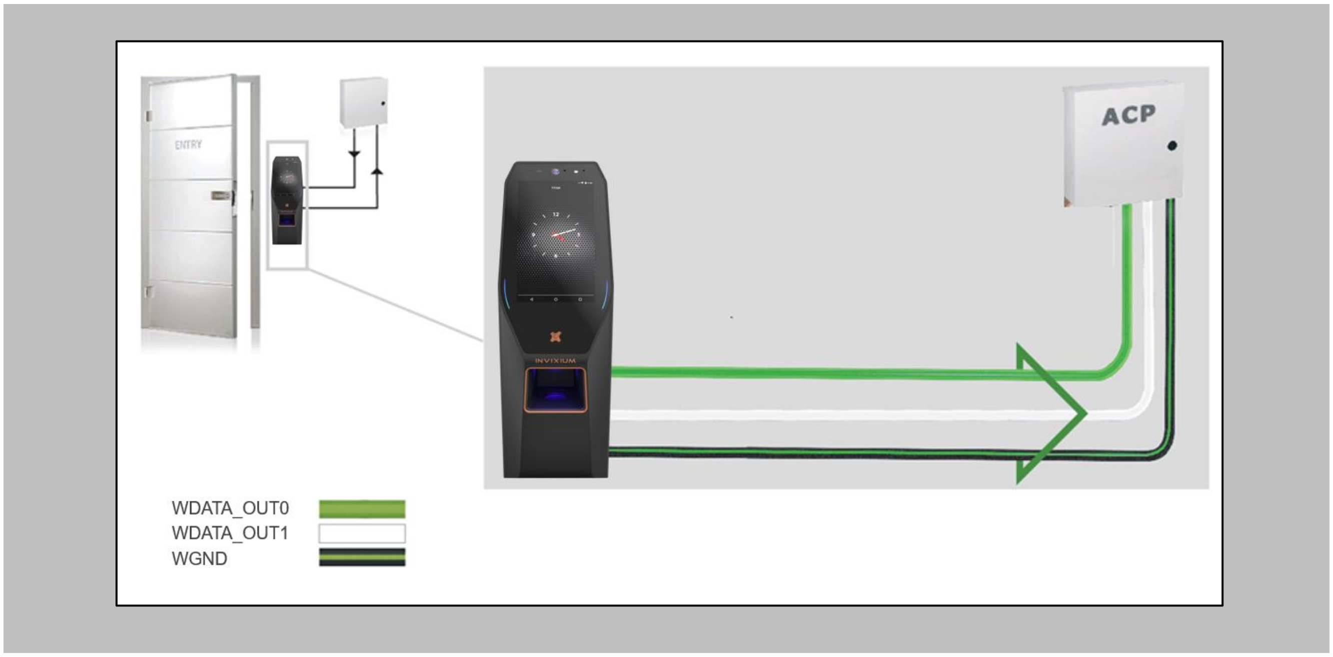
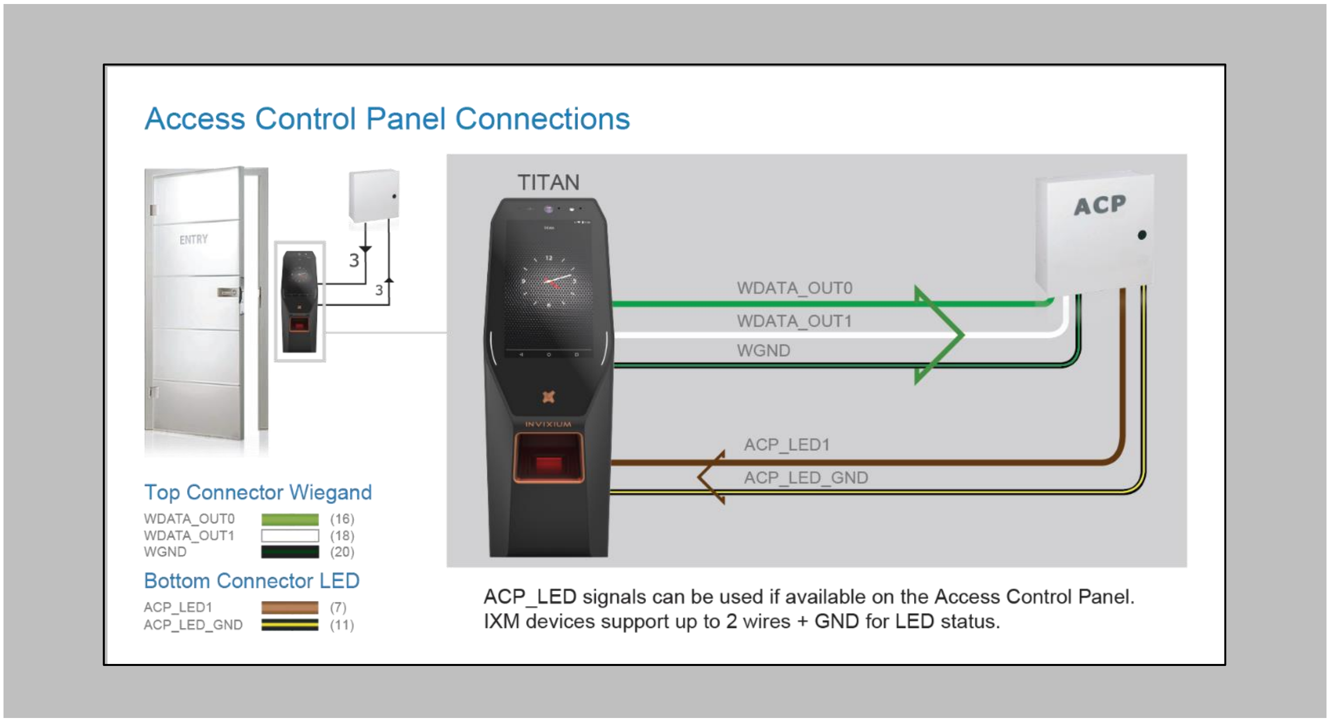


Figure 105: IXM TITAN - Wiegand

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



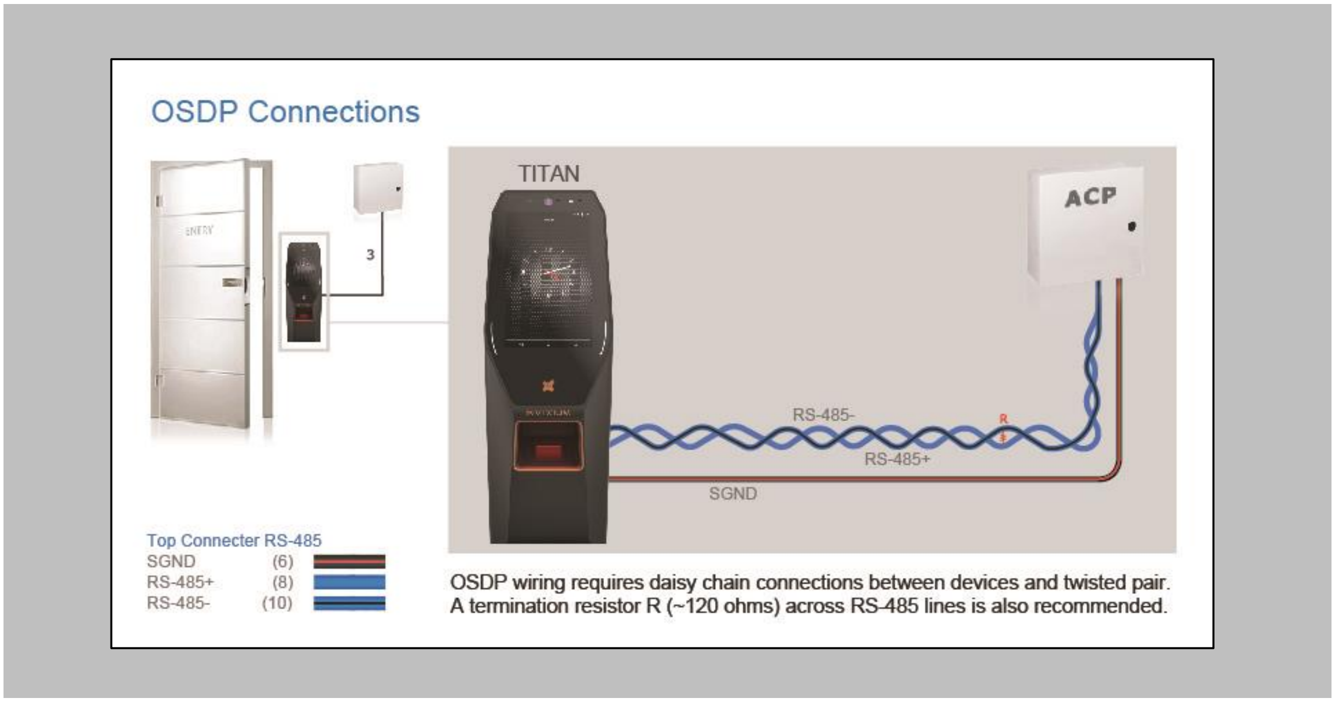
Access Control Panel Connections

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 106: 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



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 107: 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.

18. Troubleshooting

Reader Offline from the IXM WEB Dashboard

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

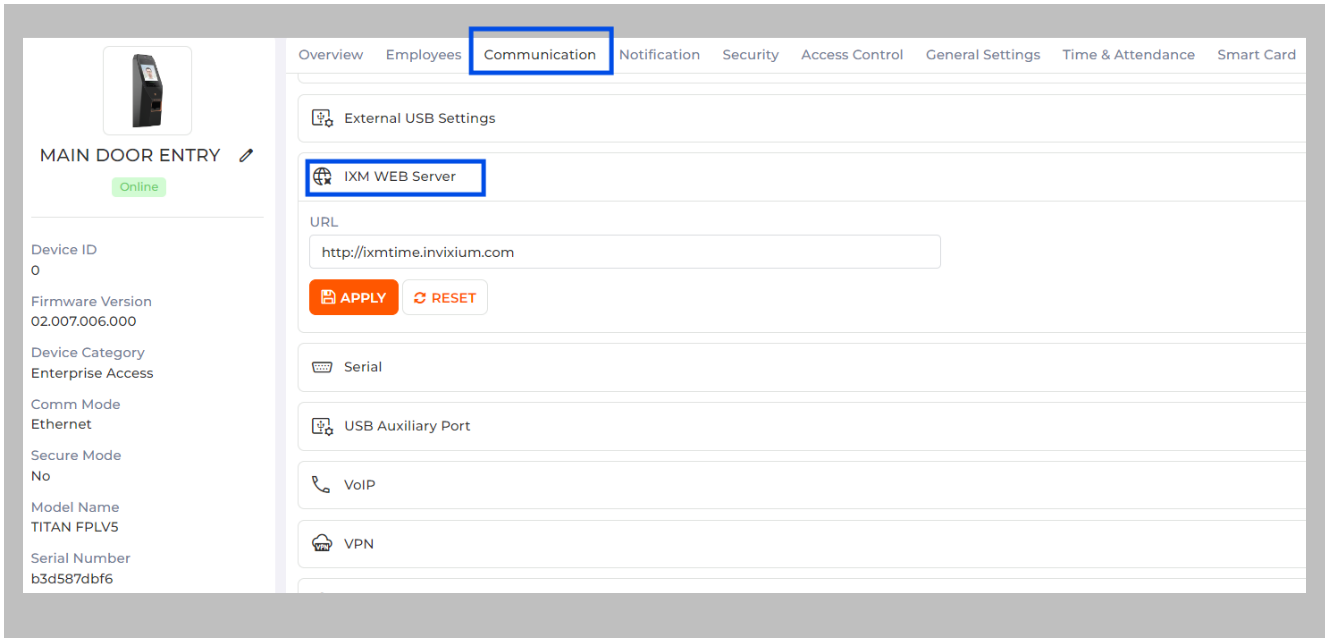
Procedure

STEP 1

From **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 108: IXM WEB - Server URL Setting

STEP 3

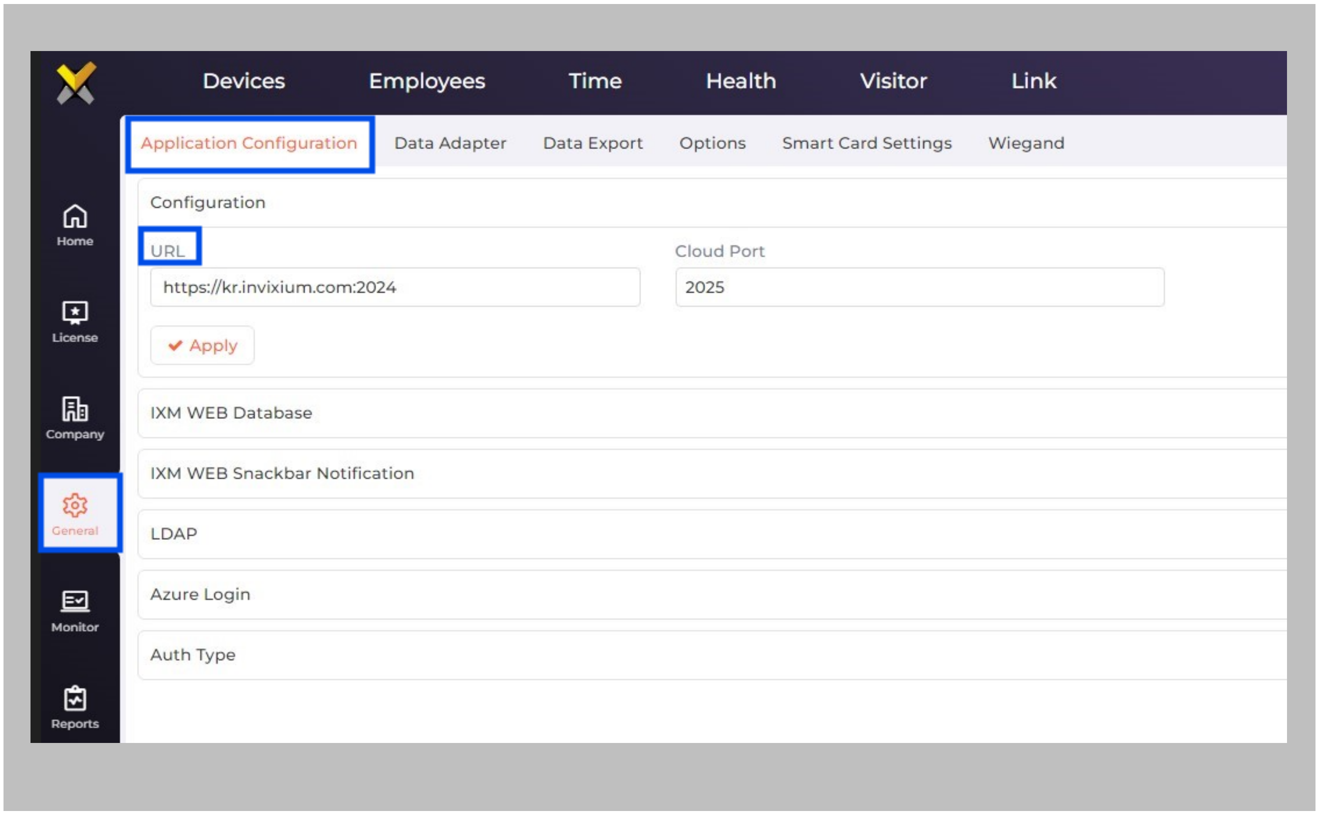
Enter the **IP address** of the Invixium server followed by **port 9108.**

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.



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

Cloud Port: 2025

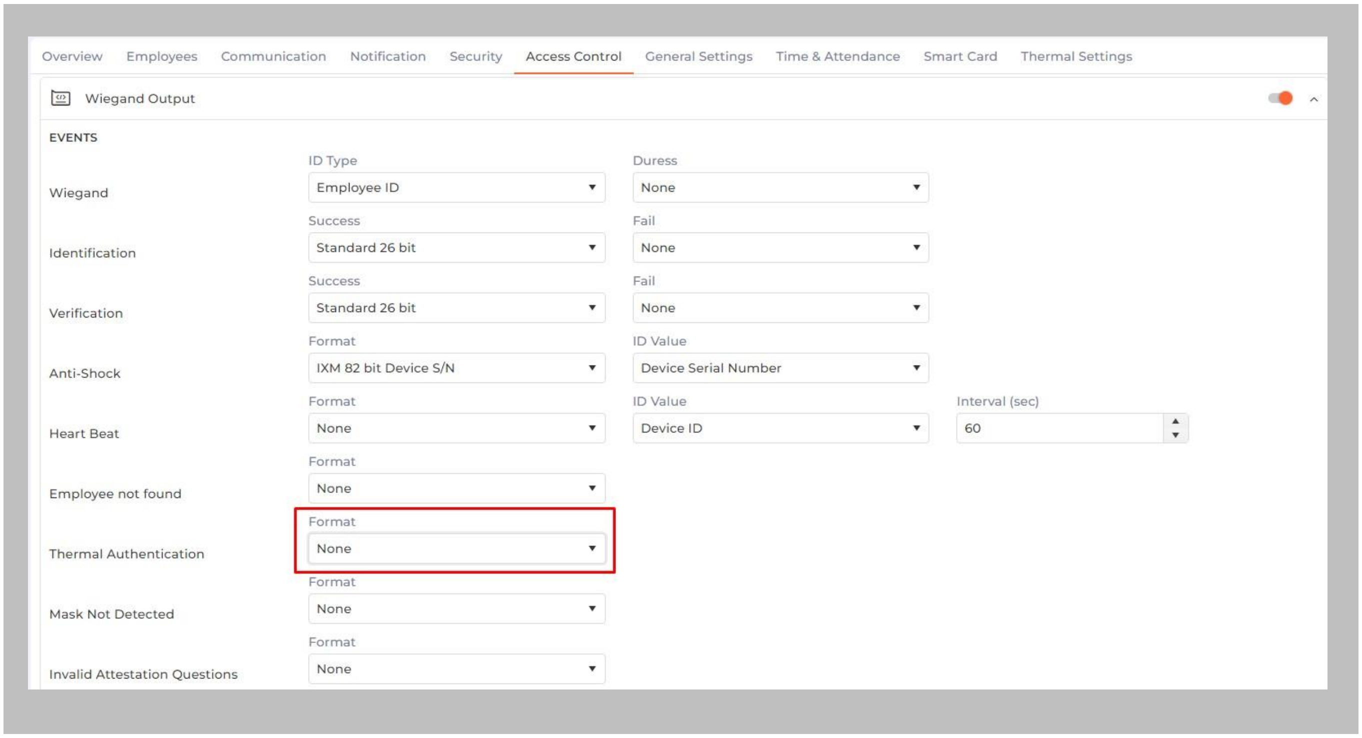
Figure 109: IXM WEB - Server URL Setting from General Settings

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		

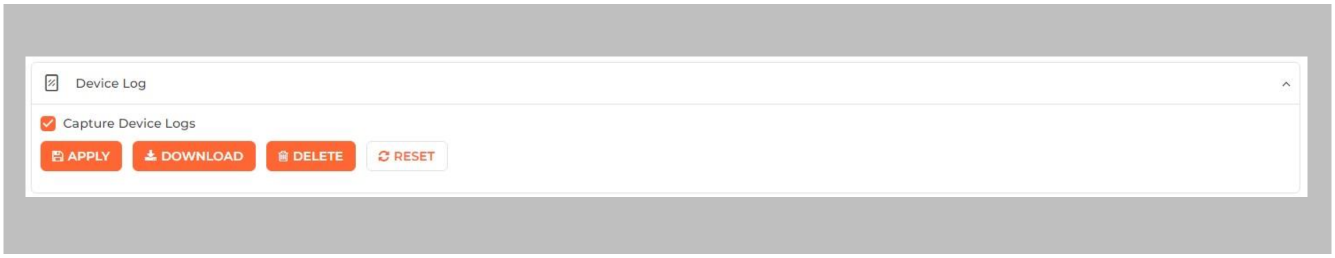
Figure 110: IXM WEB - Thermal Authentication Wiegand Output Event

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.

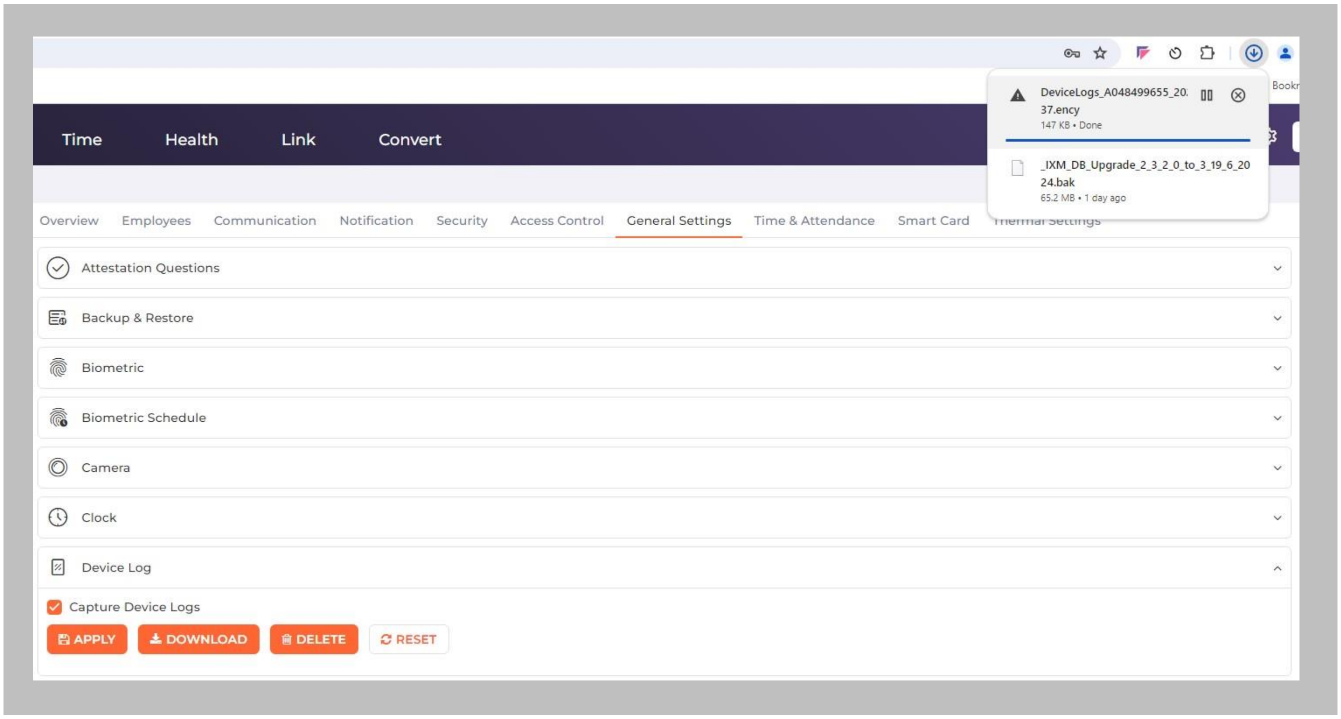


Device Log

☑ Capture Device Logs

Figure 111: 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 112: Save Device Log File

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

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

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

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

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

Logs folder location on IXM WEB Server:

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

Table 8: Logs Folder Location

19. Support

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

20. Disclaimer and Restrictions

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

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

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