

IXM WEB Integration with ACRE Security Access It!

Installation Instructions

V1.0





Table of Contents

1.	Introduction	
	Purpose	
	Summary of key features related to this IXM WEB and Access It! Integration	
	Description	
	Acronyms	
	Field Mappings	8
2.	Compatibility	10
	Invixium Readers	10
	Software Requirements	
	Other Requirements	
	Compatibility Matrix for IXM WEB & Access It! Integration	12
3.	Checklist	
4.	Task List Summary	13
5	Draraguisitas for Installing Invivium IVM WED Software	4.4
ວ.	Prerequisites for Installing Invixium IXM WEB Software	
	Acquiring IXM WEB Activation Key	
	Setting Up SQL instance	
	Minor Checklist and Considerations	20
6.	Installing IXM WEB	21
	Software Install	21
7.	Configuring Email Settings using IXM WEB	30
••	Email Setting Configuration	
8.	Software and Module Activation	
	IXM WEB Activation	
	Access It Module Activation	
9.	Configuring IXM Link for ACRE Security	40
10.	Create System User(s) for Biometric Enrollment	44
	Creating System User(s) for Biometric Enrollment	
11.	Add and Configure Invixium Readers	



Adding an Invixium Reader in IXM WEB	48
12. Adding an Invixium Device to a Device Group	53
Configuring Wiegand Format to Assign Invixium Readers	54
Assign Wiegand to Invixium Readers	
Configuring Panel Feedback with ACRE Security	60
Configuring Thermal Settings	62
Thermal Calibration	65
Test Calibration Options	68
Change Temperature Unit Settings	69
Configuring Mask Authentication Settings	71
13. Fingerprint Enrollment using Access It sofware	74
14. Enrollment Best Practices	81
Fingerprint Enrollment Best Practices	
Avoid Poor Fingerprint Conditions	81
Fingerprint Image Samples	
Fingerprint Imaging Do's and Don'ts	
Finger Vein Enrollment Best Practices	
Face Enrollment Best Practices	85
15. Appendix	86
Installing Invixium IXM WEB with Default Installation using SQL Server 2014	
Pushing Configuration to Multiple Invixium Readers	
Configuring for OSDP Connection	
Wiring and Termination	
Wiring	
Wiegand Connection	
Wiegand Connection with Panel Feedback	
OSDP Connections	
16. Troubleshooting	104
Reader Offline from the IXM WEB Dashboard	
Elevated Body Temperature Denied Access but Granted Access in Access It	
Logs in IXM WEB Application	
Unable to connect to the Access It Server	109
17. Support	111



3. Disclaimer and Restrictions

List of Figures

Figure 1: IXM WEB Online Request Form	. 14
Figure 2: Sample Email After Submitting Online Request Form	. 15
Figure 3: SQL New Login	. 17
Figure 4: SQL Login Properties	. 18
Figure 5: SQL Server Roles	. 19
Figure 6: IXM WEB Installer	. 21
Figure 7: Advanced Options in IXM WEB Installer	. 22
Figure 8: Invixium Fingerprint Driver Installation Message	. 23
Figure 9: IXM WEB Installation Progress	. 24
Figure 10: IXM WEB Installation Completed	. 25
Figure 11: IXM WEB Icon - Desktop Shortcut	. 26
Figure 12: IXM WEB Database Configuration	. 26
Figure 13: IXM WEB Administrator User Configuration	
Figure 14: IXM WEB Login Page	. 29
Figure 15: Configure Email	. 30
Figure 16: IXM WEB - SMTP Settings	. 31
Figure 17: IXM WEB - Save Email Settings	. 32
Figure 18: IXM WEB – Test Connection	. 32
Figure 19: IXM WEB - Forgot Password	. 33
Figure 20: IXM WEB - Enter Login Credentials	
Figure 21: IXM WEB - License Setup	. 35
Figure 22: IXM WEB - Online Activation	. 36
Figure 23: IXM WEB – Request Link License	. 37
Figure 24: ACRE Security License Key Email	. 38
Figure 25: IXM WEB - Activate ACRE Security Link License	. 39
Figure 26: IXM WEB - Enable ACRE Security Link Module	. 40
Figure 27: IXM WEB - Sync Activities	. 42
Figure 28: IXM WEB - Create System User	. 44
Figure 29: IXM WEB - Add New System User	. 45
Figure 30: IXM WEB - New System User	. 46
Figure 31: Employee and Employee Group Rights	. 47



Figure 32: IXM WEB - Save System User	47
Figure 33: IXM WEB - Devices Tab	48
Figure 34: IXM WEB - Search Device Using IP Address	49
Figure 35: IXM WEB - Register Device	50
Figure 36: IXM WEB - Device Registration Complete	51
Figure 37: IXM WEB - Dashboard, Device Status	52
Figure 38: IXM WEB - Assign Device Group	53
Figure 39: IXM WEB - Create Wiegand Format	54
Figure 40: IXM WEB - Create Custom Wiegand Format	55
Figure 41: IXM WEB - Custom Wiegand Format	55
Figure 42: IXM WEB – Custom Wiegand Format Created	56
Figure 43: IXM WEB - Upload Wiegand Format	56
Figure 44: IXM WEB - Navigate to Access Control Tab	57
Figure 45: IXM WEB - Wiegand Output	58
Figure 46: IXM WEB - Save Output Wiegand	59
Figure 47: IXM WEB - Panel Feedback	60
Figure 48: IXM WEB - Configuring Panel Feedback in IXM WEB	61
Figure 49: IXM WEB - Save Panel Feedback	61
Figure 50: IXM WEB - Thermal Settings	62
Figure 51: IXM WEB - Save Thermal Settings	64
Figure 52: IXM WEB - Thermal Calibration Settings	65
Figure 53: IXM WEB - Save Thermal Calibration Settings	66
Figure 54: IXM WEB - Capture Thermal Data	66
Figure 55: IXM WEB - Save Captured Thermal Data	67
Figure 56: IXM WEB - Test Thermal Calibration	68
Figure 57: IXM WEB - Option to Change Temperature Unit	69
Figure 58: IXM WEB - Save Temperature Unit Setting	70
Figure 59: IXM WEB - Mask Authentication Settings	71
Figure 60: IXM WEB - Save Mask Settings	73
Figure 61: ACRE Security - System	74
Figure 62: ACRE Security – Workstations	75
Figure 63: ACRE Security – Edit Workstation	76
Figure 64: Edit Workstation – Encode / Enroll	76
Figure 65: Encode/Enroll – Add New	77
Figure 66: Add new Device	78
Figure 67: Newly created device	79
Figure 68: IXM WEB – Biometric Enrollment	



Figure 69: F	Fingerprint Enrollment Best Practices	81
Figure 70: F	Fingerprint Images Samples	82
Figure 71: F	Finger Vein Enrollment Best Practices	84
	Face Enrollment Best Practices	
Figure 73: Ir	nstall IXM WEB	86
Figure 74: L	.oading SQL Express & Installation Progress	87
Figure 75: I>	XM WEB - Shortcut Icon on Desktop	88
Figure 76: I>	XM WEB - Configuring IXM WEB Database	88
Figure 77: I>	XM WEB - Select Database Name	89
Figure 78: I>	XM WEB - Broadcast Option	91
Figure 79: I>	XM WEB - Broadcast Wiegand Output Settings	91
Figure 80: I>	XM WEB - Broadcast to Devices	92
Figure 81: I>	XM WEB - OSDP Settings	93
Figure 82: I>	XM WEB - Save OSDP Settings	96
Figure 83: I>	XM WEB - Edit Device Options	96
Figure 84: I>	XM WEB - Disable Panel Feedback	97
Figure 85: E	Earth Ground Wiring	98
Figure 86: I>	XM TITAN – Top & Bottom Connector Wiring	99
Figure 87: P	Power, Wiegand & OSDP Wires1	00
Figure 88: I>	XM TITAN - Wiegand1	01
Figure 89: I>	XM TITAN - Panel Feedback 1	02
Figure 90: I>	XM TITAN - OSDP Connections1	03
Figure 91: I>	XM WEB - Server URL Setting1	04
Figure 92: I>	XM WEB - Server URL Setting from General Settings1	05
Figure 93: I>	XM WEB - Thermal Authentication Wiegand Output Event 1	06
Figure 94: I>	XM WEB - Enable Device Logs1	07
Figure 95: S	Save Device Log File 1	07
Figure 96: I>	XM WEB - Licence Module1	09
Figure 97: A	ACRE Security – Access It Web API 1	09



List of Tables

Table 1: Compatibility Matrix for IXM WEB & ACRE Security Integration	12
Table 2: Task List Summary	13
Table 3: System Related Checklist	20
Table 4: Port Information	20
Table 5: IXM WEB - OSDP Configuration Options	95
Table 6: IXM WEB - OSDP Text Options	95
Table 7: Logs Folder Location	108



1. Introduction

Purpose

This document outlines the process of configuring the software integration between ACRE Security Access It! and Invixium's IXM WEB.

Summary of key features related to this IXM WEB and Access It! Integration

- 'Sync All' feature to resynchronize the database from Access It! to IXM WEB
- Multiple card support upto 10

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 ACRE Security Access It Software (where access rules for the users and the organization are managed).

Note: To activate the IXM Link within IXM WEB, the installer must contact Invixium Support at <u>support@invixium.com</u> 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 Access It by using ACRE Security Access It API to import and export cardholders.

Acronyms

Acronym	Description		
ACPCS	Access Control Panel Configuration Software		
AI	ACRE Security Access It!		
IXM	Invixium		

Field Mappings

The following are the Access It fields that are mapped to IXM WEB:

Access It Field	IXM Field	Notes	
First name	First Name		
Last name	Last Name		



Cardholder Status	Suspend User	IXM WEB has two values of Cardholder Status - ACTIVE and INACTIVE while AI has three statuses - Inactive, Active, and Date based. ACTIVE of AI is mapped to INACTIVE. INACTIVE of AI is mapped to ACTIVE as Suspend User in IXM WEB. The Date field is mapped to the Start Date & End Date of IXM WEB.
Cardholder Status Date is Active (Cardholder Status - Date based)	Start Date	Al doesn't allow a value less than 1/1/1970.
Cardholder Status Date is expired (Cardholder Status - Date based)	End Date	Al doesn't allow a value greater than 31/12/2035.
Department	Department	
Card number	Prox ID	
Facility Code	Facility Code	
PIN Number	PIN	ACRE Security has a PIN at the card level which is mapped to a PIN at the user level since IXM WEB supports only one card per user. The rationale is that the user remembers their PIN which can be used on Invixium devices for authentication. In ACRE Security, the default value for PIN Number is 0. If the PIN Number is 0 then it is considered empty in IXM WEB.
Card status	"No equivalent"	Prox ID, Facility Code, and PIN are set when the Card Status is not Inactive. Inactive card statuses are not transferred to IXM WEB.
Active (Card Status - Date based) &	"No equivalent"	If an active date is less than or equal to the current date, and the expiry date is greater than or equal to the current date then Prox ID, Facility Code, and PIN are transferred to IXM WEB.



Expire (Card Status - Date based)		
Photo	User Image	Upon syncing, IXM WEB fetches all the user's profile pictures from AI. Users need to ensure that photos have a valid size (it should not be 0 bytes).

Note: Multiple Cards – Access It can have multiple cards per user but IXM WEB imports cards up to 10 only.

2. Compatibility

Invixium Readers

TITAN	TFACE	TOUCH2	SENSE2	MERGE2	MYCRO
All models					

Software Requirements

Application	Version
ACRE Security Access It!	v10.2.0
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 & Access It! Integration

IXM WEB version	Access It version	Compatible
IXM WEB 2.2.57.0	v4.5	Yes
IXM WEB 2.2.57.0	v5.0	Yes
IXM WEB 2.2.224.0	v4.5	Yes
IXM WEB 2.2.224.0	v5.0	Yes
IXM WEB 2.2.252.0	v5.0	Yes
IXM WEB 2.2.252.0	v5.5	Yes
IXM WEB 2.2.330.0	v5.0	Yes
IXM WEB 2.2.330.0	v5.5	Yes
IXM WEB 2.3.0.0	v10.2	Yes
IXM WEB 2.3.0.0	v10.2	Yes
IXM WEB 3.0.36.0	v10.2	Yes
IXM WEB 3.0.36.0	v10.2	Yes

Table 1: Compatibility Matrix for IXM WEB & ACRE Security Integration



3. Checklist

Item List	Interface
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 ACRE Security Access It	Invixium
Configure Invixium Reader	Invixium
Face or Finger Enrollment	Invixium

4. Task List Summary

Task	IXM WEB Application Task List using IXM WEB	ACRE Security Access It Task List using Access It
1	Activate IXM WEB and IXM Link for Access It	Fingerprint Enrollment from ACRE Security
2	Configure IXM Link for Access It	
3	Register IXM Devices and configure settings as per the requirement	
4	Configure Weigand or OSDP in the device for integration with ACRE Security	
5	Assign a specific Device Group to the device	

Table 2: Task List Summary



5. 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: <u>https://www.invixium.com/download-ixm-web/.</u>

 Distributor 			
Access Control Panel Manufacturer			
Installer/Integrator			
O End User			
issued in their name and will provide them acces	Last Name*		Company Email*
First Name*	Last Name*		Company Email*
Company Name*	Select Country*	~	Phone Number*
Installer Details Please provide details of the person and/or comp customer email ID as well as the email ID provid	pany responsible for installing IXM WEB at the a ed below.	aforementioned cust	omer's facility. The license key will be emailed to the
			Company Email*
First Name*	Last Name*		
First Name* Company Name*	Last Name* Phone Number*		
			City*

Figure 1: IXM WEB Online Request Form



After submitting the completed form, an email will be sent with instructions from <u>support@invixium.com</u> 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	
Get the	latest IXM WEB package from the link below. Depending on your internet speed, the download will take approximately 15 minutes.
Importa	
1. Do no	n 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 e	visting TITAN or TFACE users, this update of IXM WEB requires temporary internet connectivity to access Invikium servers for license validation. If connecting to the internet is not possible at your premises, contact IXM Support for
4. For n	ew 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 WE	B 2.3.0.0 package
Activatio	In ID: LW-D4-66-
Follow t	hese steps to install or update IXM WEB:
1. D	ownload the IXM WEB package.
2. E	xtract the compressed files and copy IXM WEB.exe to required server.
3. Ir	stall IXM WEB, open and create a login
New IXI	I WEB installations require Activation. To activate IXM WEB, first open and create a login and then follow these steps:
1. <u>O</u>	n <u>Ilne Activation</u> (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. 0	ffline 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 th	e Experience!

Figure 2: Sample Email After Submitting Online Request Form



Setting Up SQL instance

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

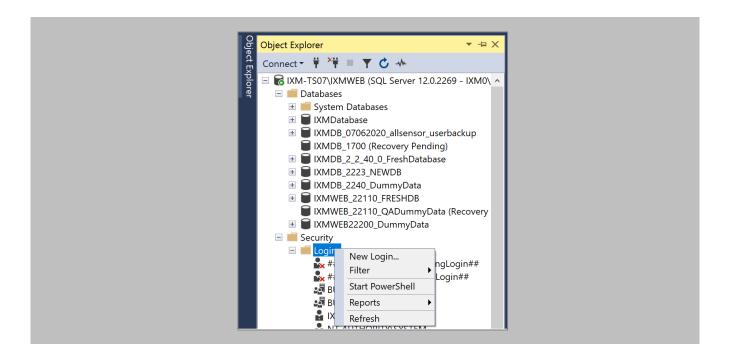
Select mixed mode: SQL Authentication and Windows Authentication for secure logins. Leave everything else as default.

STEP 4

Install SQL Management Studio on the server.



Log into the new instance and create a new user.





STEP 6

Select SQL Server authentication.

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



Select a page	🖵 Script 🔻 😯 Help				
 General Server Roles 					
Ser Mapping	Login <u>n</u> ame:				Search
Securables	◯ <u>W</u> indows authentication				
🔑 Status	SQL Server authentication				
	Password:	•••••			
	<u>C</u> onfirm password:	•••••			
	Specify old password				
	<u>O</u> ld password:				
	Enforce password polic	у			
	Enforce password expir	ation			
	User must change pass	word at next login			
	O Mapped to certificate			\sim	
	O Mapped <u>t</u> o asymmetric key			\sim	
	Map to Credential			\sim	Add
Connection	Mapped Credentials	Credential	Provider		
Server: IXM-TS07\IXMWEB		Credential	TTOVIDEI		
Connection:					
IXM0\sdholakia					
View connection properties					
Progress					
Ready					
ALL A					Remo <u>v</u> e
	Default <u>d</u> atabase:	master		\sim	
	Default language:	English - us_english		\sim	

Figure 4: SQL Login Properties



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

Login Properties -		_		×
Select a page	🖵 Script 🔻 😯 Help			
 General Server Roles User Mapping Securables 	Server role is used to grant server-wide security privileges to a user.			
🗲 Status	Server roles:			
	bulkadmin ✓ dbcreator diskadmin processadmin ✓ public securityadmin serveradmin stypadmin sysadmin			
Connection				
Server: IXM-TS07\IXMWEB				
Connection: IXM0\sdholakia				
₩ <u>View connection properties</u>				
Progress				
Ready				
		ОК	Can	

Figure 5: SQL Server Roles

RESULT

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



Minor Checklist and Considerations

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

Other Minor Checklist	
	Windows Operating system needs to be up to date.
Windows Updates	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
ТСР	1433
Port to communicate between IXM WEB & Devices	9734
Inbound Port	1255
Access It Web Service API Port	8732 (default)

Table 4: Port Information



6. Installing IXM WEB

Software Install

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator).

Select Advanced.

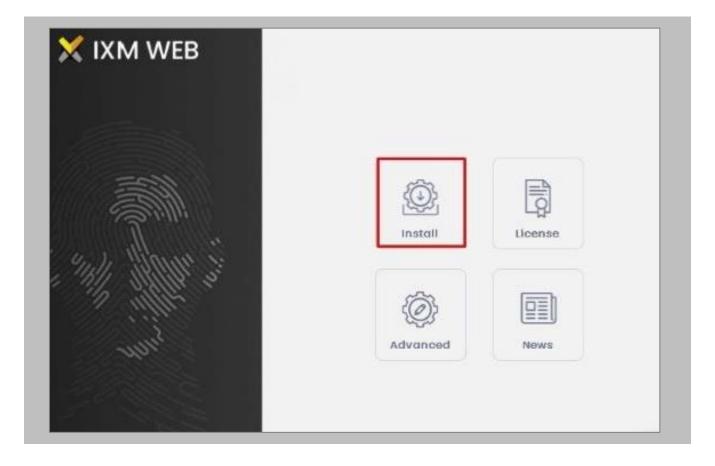


Figure 6: IXM WEB Installer



Deselect Install SQL Server and select Install.

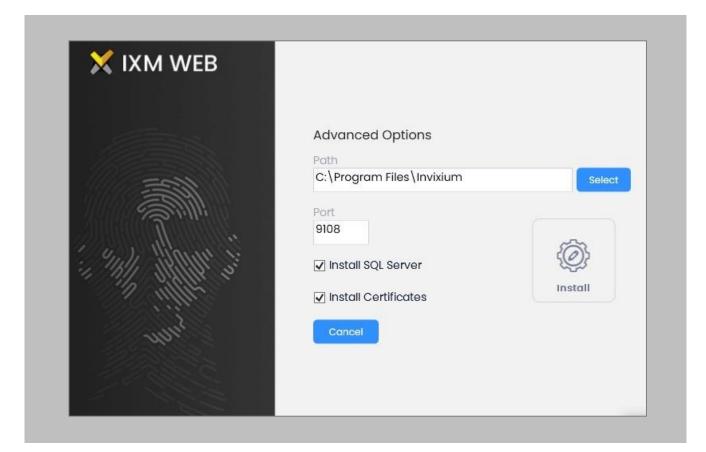


Figure 7: Advanced Options in IXM WEB Installer



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

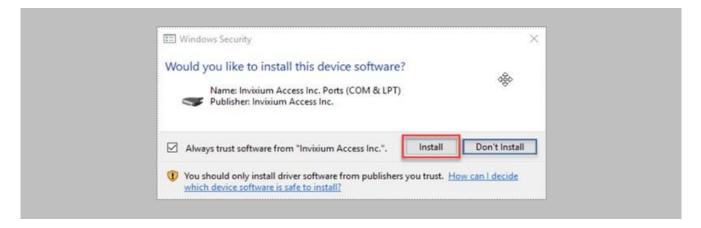


Figure 8: Invixium Fingerprint Driver Installation Message



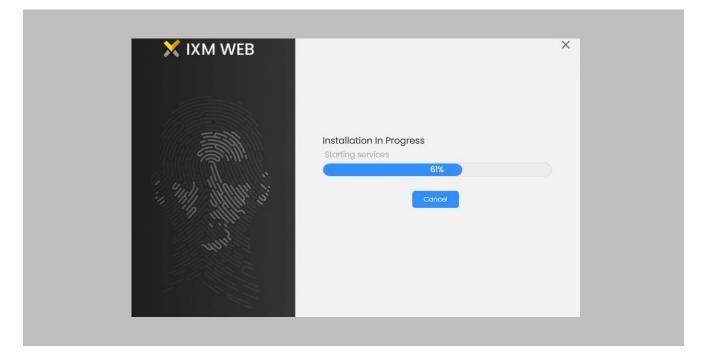


Figure 9: IXM WEB Installation Progress



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



Figure 10: IXM WEB Installation Completed

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



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



Figure 11: IXM WEB Icon - Desktop Shortcut

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

Authentication	SQL Server Name
SQL Server	▼ IXM-TS25\SQLEXPRESS × ▼
 SQL User Name	Password
admin	





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.

	Authentication	SQL Server Name	
	Windows	▼ IXM-QA20\IXMWEB	× •
	Database Name		
	IXMDB		× •
" " " "	CREATE ACCOUNT		
in White Ballin is	Admin ID	Password	
Sulley-	Confirm Password	Email	
	Server URL	Cloud P	ort
	http://localhost:9108	1255	
			ort

Figure 13: IXM WEB Administrator User Configuration

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



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.



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

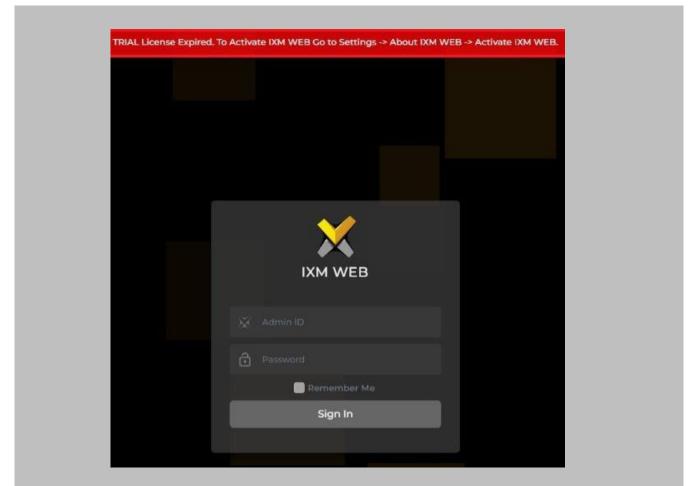


Figure 14: IXM WEB Login Page

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



7. 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 \rightarrow **System Notifications** \rightarrow Click on **SMTP Settings**.

Device Offline Template SHUESE Device Down Notification Password Change Notify Template Personal QR Code Device Down Notification	Email Alerts Fire Zones		• SMTP Setting
Device Down Notification Dear Admin, Following devices are offline #Details#		on	Device Down Notification P Ed
	iersonal QR Code	Dear Admin, Following devices are offline #Details#	

Figure 15: Configure Email



ň

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

Email Configuration		×
Status		
SMTP Host	SMTP Port	
	587	
Send email messages from	Secure Connection	
	StartTLS	•
SMTP Login	SMTP Password	
Send test email to		
% Test Cor	nnection	

Figure 16: IXM WEB - SMTP Settings

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



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

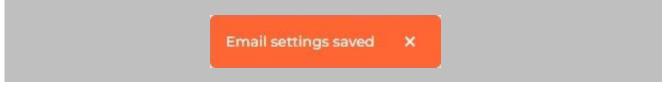


Figure 17: IXM WEB - Save Email Settings

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

🛃 Status		
SMTP Host	SMTP Port	
	587	
Send email messages from	Secure Connection	
	StartTLS	
SMTP Login	SMTP Password	
Send test email to		
% Test Con	nection 🛛 🗃 Save	

Figure 18: IXM WEB – Test Connection



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

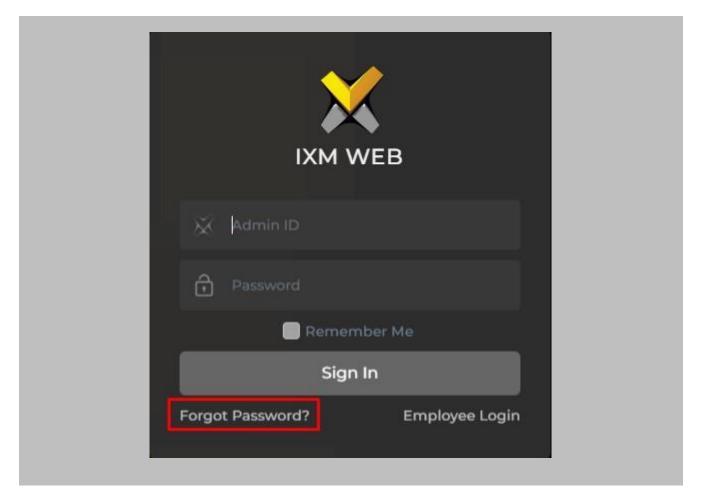


Figure 19: IXM WEB - Forgot Password



8. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.



Figure 20: IXM WEB - Enter Login Credentials



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

	×
IXM	Web
Activation Type	
Online	•
Enter Key	
- Act	ivate
Need Help? Contac	t customer support

Figure 21: IXM WEB - License Setup

STEP 3

Request Activation Key Online or via Offline Activation Options.

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



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

IXM Web	
Your cu	irrent version of IXM Web is Active
Activation Date : Activation Type	Expiration Date: 07/31/2025
Online	
Activation ID	
Enter Key	
	✓ Activate
Need	Help? Contact customer support

Figure 22: IXM WEB - Online Activation



Access It Module Activation

The option to activate a ACRE Security Access It 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 Invixio	um.	
All rights reserved. Invixium <u>Terms of Service</u> .		
invixium <u>remis of service</u> .		
THIRD PARTY COMPONENTS		
IXM WEB includes elements and of All rights reserved.	components from Telerik's Kendo UI Web	. Copyright © 2024,
ANNUAL SUPPORT CONTRACT IN	FORMATION	
Status	Expire On	
Active	07/31/2025	
B5k6X0y8NFfzQkuxy/kUBNHTNH kLAwjAkxvag9EZ/0dujHSU4NfCyk	Vpc6yLgBoCitYxHdT25EuuoX4VHLR2Fps1 kXOGbg=	2MjHSj5VUgDHmY
🛛 🖾 IXM V	VEB Activation 🕒 What's New	

Figure 23: IXM WEB - Request Link License



You will receive an email from Invixium Support containing a license key for the ACRE Security Access It Activation.

Sent: To:	Invikium Support Thursday, September 30, 2021 11:59 AM at: RE: IXM LINK Activation key request
Dear	
Gree	tings! Thanks for connecting with Invixium Technical Services Team!
:	our license details are given below: Module: Access It License Key: To activate your IXM Link license, follow these steps: Construction MMER and here
2. 3.	Open IXM WEB and login Go to Left Navigation Menu >> Click LICENSE tab Select the Lenel option Enter the License Key given above and click Activate .
We a	ppreciate your kind support & patience.
Best I	Regards,
Invixi	um Technical Services Team
	LUS: ~1 844 (NVXXXXI/L) (468 4948) Email: <u>support(@invixium.com</u> Isour: 12 200AN to 5 00FW (Eastern Time) Skype Invixium_support
This see	all and any attachments may contain confidential and privileged information. If you have received this message in error, please notify us immediately and destroy the material in its entirety whether electronic or hard copy. Also, please consider the environment helpse potentian this emaintent of the environment helpse potentian.

Figure 24: ACRE Security License Key Email



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

ichneider Hettre	Access Expert Schneider Electric	🔒 Technologies	Access It! ACRE Security	*nedap	AEOS Nedap	Queen	Command Centre Gallagher	OindigoWassi	Control Center IndigoVision
	DNA Fusion Open Options-DNA Fusion	SIEMENS	Fusion Siemens	Feenics	Keep ACRE Security	Paxton	Net2 Paxton	ØLENELS2	NetBox LenelS2
LENELS2	OnGuard LenelS2	Honeywell	Pro-Watch Honeywell	Genetec	Security Center Genetec	SIEMENS	SiPass Siemens	SIEMENS	SiPort Siemens
GALAXY	System Galaxy Galaxy Control Systems	Honeywell	Win-Pak Honeywell						
tivate I Enter K									

Figure 25: IXM WEB - Activate ACRE Security Link License

RESULT

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



9. Configuring IXM Link for ACRE Security

Procedure

STEP 1

From the Link \rightarrow click the Access It (ACRE Security) icon.

Toggle the Status switch to enable.

Authentication	abole	Server				User		Password
SQL	•	IXM-QA06\AIUNIV	ERSAL,1435		× •	sa		
Database		Interval (sec)		Sync Direction				
AlUniversal	× •	30	*	IXM WEB ← RS2			•	
Auto Transfer				Employee Group				
Yes			•	Select value	•			
ACTIVITIES				🖺 Apply 😂	Reset			
Numbers			Numbers	in IXM WEB			Times	
		0	29406	48	29334		25 Jun, 2024 12:35 PM	25 Jun, 2024 12:36 PI

Figure 26: IXM WEB - Enable ACRE Security Link Module

Authentication Mode:

Select "Windows" or "SQL Server" as an authentication mode from the dropdown list.

Server:

Enter the Name or IP of SQL Server Instance where ACRE Security database is installed.

User:

Enter the name of the authorized user to log into SQL Server to access database.

Password:

Enter the Password of the authorized user to log into SQL Server to access database.



Database:

Select the AIUniversal database from the dropdown list.

Interval (Sec):

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

Sync Direction:

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

• IXM WEB - ACRE Security

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

Note: This is the recommended option.

• IXM WEB → ACRE Security

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

• IXM WEB ← → ACRE Security

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

Auto Transfer:

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

Click on either 'Yes' or 'No'.

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



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

Employee Group:

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

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

Click **Apply**. The transfer of data between ACRE Security and IXM WEB is possible only after successful connection.

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

Numbers			Numbers in IXI	M WEB		Times	
0 Added	0 Updated	0 Deleted	29406 Added	48 Updated	29334 Deleted	25 Jun, 2024 12:32 PM Last run at	25 Jun, 2024 12:33 PM Next run at
	A COMPANY			l formats Sync			

Figure 27: IXM WEB - Sync Activities

Numbers

The first two colums display the number of records added, updated and deleted in ACRE Security and IXM WEB respectively after each data transfer.

Times

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



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

STEP 2

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 3

The Sync All feature allows resynchronization of database from Access It to IXM WEB. This will reimport missing cardholders or updated cardholders from Access It to IXM WEB. Also, it will delete IXM WEB employee records according to cardholders available in Access It.

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

STEP 4

Clicking on **Sync card formats** immediately synchronizes card formats from Access It to IXM WEB. This will re-import card formats available in Access It to IXM WEB.

RESULT

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



10. 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 \rightarrow Click Users. The application will redirect to the System Users window.

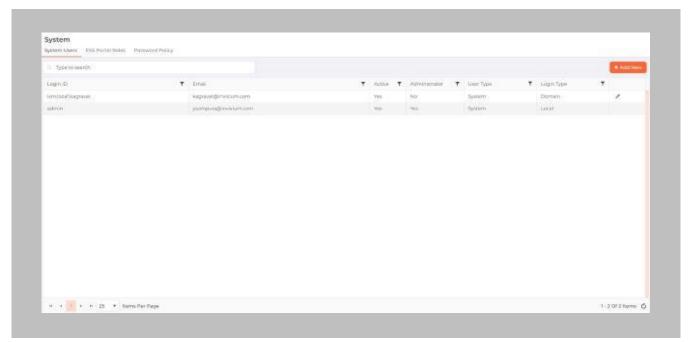


Figure 28: IXM WEB - Create System User



Click Add New.

Login ID							+ Add
	🕈 Email		T Active	▼ Adminis	trator 🔻 User 1	ype 🔻 Lo	ogin Type 🕴
km.localikagravat	kagravas@mv	ixium.com	Yes	No	Syster	n Di	omain d
admin	ysompura@in	vixium.com	Yes	Yes	System	n Lo	scal

Figure 29: 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



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

Jser Type		
System		
login Type		
Local	•	
ogin ID	Password	Confirm Password
enrollmentuser		
Email		
enroll@ixm.com	Status	

Figure 30: IXM WEB - New System User



Add an email address.

Apply for permission as "All" for **Employee & Employee Group** module.

lodule	None	View	Edit	All
Dashboard				~
Device & Device Group				
Employee & Employee Group				~
Visitor				
Link				
Licensing				
Company				
Organization Heirarchy				
Company Schedules				
Company Information	2			
General Settings				
Application Configuration				
Data Export				
Options	2			
Smart Card Settings	Image: A start and a start			
Wiegand				

Figure 31: Employee and Employee Group Rights

STEP 5

Click Save.



Figure 32: IXM WEB - Save System User



11. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

Click the **Devices** tab.

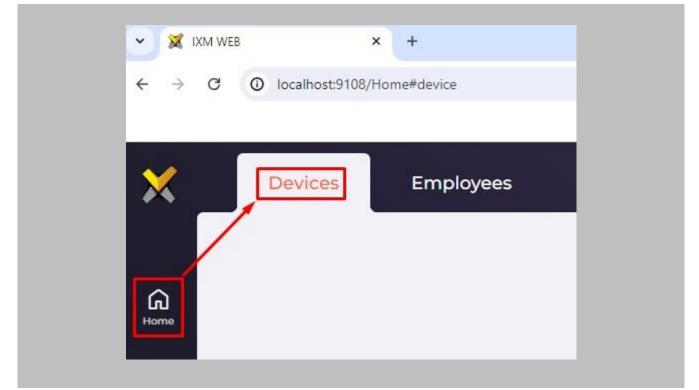


Figure 33: IXM WEB - Devices Tab



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.

Auto Discover Auto Discover Devices In Your Network	Ethernet Discover Devices using IP	Serial Discover Devices on Serial Network		
tart IP	End IP	Port		
192 . 168 . 1 .	123		Search on SSL	Q Search
ELECT DEVICE TO REGISTER [DIS	COVERED DEVICES : 1]			
Titan 8822994411				
IP Address	MAC ID			
192.168.1.123	7C:88:22:99:44:11			

Figure 34: IXM WEB - Search Device Using IP Address



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

- Andrews	Name	Device ID	Device Group
	Titan	0	▼ 1 item(s) selected ×
	Device Mode		
	Both 🔻	T&A Device	
ETWORK INFORM	MATION		
DHCP			
Address	Port	Subnet Mask	Gateway
92.168.1.123	9734	255.255.255.0	192.168.1.1
		✓ Register	

Figure 35: 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.



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

		\bigcirc		
		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		
		+ Add New Vone		

Figure 36: 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).

890 Total Employees	0 Inactive	88 0 Suspended	Access Granted	Access Denied	
nrollment Status	Enrollment Qual		Credentials	Headcount by depar	tment
25 111111111111111111111	Good Pool 100%	Average	Face 0 Fingerprints	3 QA Departm	1
1	50%		Finger Veins 0 Cards PIN	3 Developer	1
		rints Finger Veins Face	Digital Cards	4 Firmware	1
thentication Mode	Device Status		Sync Status	System Statistics	
				90 Employees	1 Devices
				3 Employee Group	6 Device Group
				1 Sync Group	4 Access Schedule

Figure 37: IXM WEB - Dashboard, Device Status



12. 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** \rightarrow click on **Manage Device Group**. Add the device by clicking vertical ellipses button of respective Device Group \rightarrow click on **Add Device** \rightarrow Search for device \rightarrow click **Add** button.

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

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

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

Q DeviceName/IP/SerialNumber						Quick
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	:
						Add to Group
						Delete
						Reboot
						Factory Default
						Broadcast
						Manual Upgrad

Figure 38: IXM WEB - Assign Device Group



Configuring Wiegand Format to Assign Invixium Readers

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

STEP 1

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

×	Devices	Employees	Time	Health	Link	Convert				L	û ⁰ 🎄 😕
	Application Configuration	Data Adapter	Data Export	Options	Smart Card Settings	Wiegand					
â									[Create 🔻 Upload 🔻	Delete
Home	Wiegand ID	Name					т	Туре			T
	1	Standard 26 bit						Standard26Bits			0
License	2	cust56						Custom			1
Company											
र्ट्र General											
ET Monitor											
Reports											

Figure 39: IXM WEB - Create Wiegand Format



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

	Application Configuratio	n Data Adapter	Data Export	Options	Smart Card Settings	Wiegand				
ଇ									Create 🔻 Up	load 🔻 📋 Delet
Home	Wiegand ID	T Name					Ŧ	Type	Passthru	Ŧ
Ţ.	1	Standard 26 bit						Standard26Bits	Custom	1
icense	2	cust56						Custom		0
ieneral										
ET Aonitor										

Figure 40: IXM WEB - Create Custom Wiegand Format

STEP 3

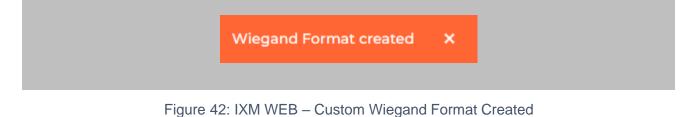
Enter **Name** of the custom Wiegand and assign **Bits**. Lets say we name the Wiegand as '32-BIT CSN' and define Total Bits as 32 bits where all the 32 bits are ID bits.

ate				
ustom Wiegand				
ame		Total Bits		
32-BIT CSN		32	*	
DRMAT				
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 2	9 30 31	
ID Bits Even Parity Odd Parity Flex Fie	Id 📃 Others 📄 Facility Code	Issue Level		

Figure 41: IXM WEB - Custom Wiegand Format



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



STEP 5

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

SELECT DEVICE(S) Device Group Testing Test DG FACE_COOVER 	Wiegand		×
 Testing Test DG 	SELECT DEVICE(S)	Q Type to search	
	 ✓ Testing ✓ Test ✓ DG 	VER	

Figure 43: 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 ACRE Security to Invixium.

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

STEP 1

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

STEP 2

Navigate to the Access Control tab.

×	Devices	Employees	Time	Heal	th Link	Conve	rt
	♠ > Devices > A04 Devices	8499655					
ŵ			Overview E	mployees	Communication	Notification	Security Access Control
Home			Device Inform	nation			
±.			Transactions			Authenticatio	
License	A0484996	655 🧷	2			Face Recognit	tion, Fingerprint
	Online		Face License			Face Algo Ver	sion
			Active			3.1.0	

Figure 44: IXM WEB - Navigate to Access Control Tab



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							
	ID Type		Duress				
Wiegand	Employee ID	•	None	•			
	Success		Fail				
Identification	Standard 26 bit	•	None	•			
	Success		Fail				
Verification	Standard 26 bit	•	None	•			
	Format		ID Value				
Anti-Shock	IXM 82 bit Device S/N	•	Device Serial Number	•			
	Format		ID Value		Interval (sec)		
Heart Beat	None	•	Device ID	•	60	*	
	Format						
Employee not found	None	•					
	Format						
Thermal Authentication	Standard 26 bit	•					
	Format						
Mask Not Detected	None	•					
	Format						
Invalid Attestation Questions	None	•					
PULSE (MSEC)							
Width	Interval						
40 *	2000						

Figure 45: 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 Access It, select either Default Card or Actual Card.

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



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

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

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

STEP 4

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

STEP 5

Click Apply.

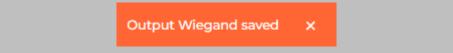


Figure 46: IXM WEB - Save Output Wiegand

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



Configuring Panel Feedback with ACRE Security

Procedure

STEP 1

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

STEP 2

Connect the LED of the ACRE Security 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**.

		Overview Employees Communi	cation Notification	Security Access Control	General Settings	Time & Attendance	Smart Card	
		Panel Feedback						(
MAIN DOOR	0		LED Mode		Timeout (msec)			
Online		LED Control By Panel	Two LED	v	3000		+	
or mine		Status Event				On Time (msec)		Off Time (msec)

Figure 47: IXM WEB - Panel Feedback



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**.

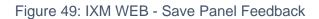
ED Control By Pane	One LED	▼ 3000	* *	
	LED Driving Mode	Pulse Processing		
nable Pulse Process	Low	▼ 500	▲ ▼	
Status	Event		On Time (msec)	Off Time (msec)
	Authentication Success		100	100
	Authentication Fail		200	200
	Retrieve PIN		300	300
	Door Open		400	400
	Door Close		500	500
	Restart Device		600	600
	Release Alarm		700	700
OR				
nable Panel Feedba	ack			



STEP 5

Click Apply.

Panel Feedback configuration saved



×



Configuring Thermal Settings

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

Procedure

STEP 1

Click the Devices tab \rightarrow Select Device \rightarrow Select Thermal Settings \rightarrow Thermal Authentication Settings to view default settings.

♠ > Devices > A048499655	Overview Employees Communication Notification Security Access Control Ceneral Settings Time & Attendance Smart Card Thermal Settings
8	R ^o Thermal Authentication Settings
A048499655 /	DEVICE CONFIGURATION
Online	Temperature Unit
	Celsius 🖲 Fahrenheit Threshold Temperature Sensitivity Authentication Mode
Device ID 0	Transition or provide the second sec
Firmware Version 02.007.005.000 Device Category Enterprise Access Comm Mode Ethernet	Capture Image on EBT Duress Status Show Temperature on LCD Send Wiegand Thermal on VolP Call Temperature Logging
Secure Mode Yes	MESSACES
Model Name TITAN FPU5 Serial Number	Display Message on EBT EBT Display Message Time (sec) Custom
A048499655	High Temperature

Figure 50: 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.

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

Thermal Authentication settings saved 💦 🗙

Figure 51: IXM WEB - Save Thermal Settings



Thermal Calibration

STEP 1

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

	Overview Employees Communication Notification Security Access Control General Settings Time & Attendance Smart Card Thermal Settings
R.	80 Thermal Authentication Settings
A048499655 /	Thermal Calibration
Online	Thermal Calibration Type
	Manual 🔹
ce ID	THERMAL OPTICAL
nware Version	Offset X Offset Y Offset Y Offset Y
07.005.000	
ce Category rrprise Access	CAPPURE THERMAL DATA © TEST CALIBRATION
im Mode ernet	
ire Mode	

Figure 52: IXM WEB - Thermal Calibration Settings

STEP 2

The settings along with their functions are:

- Thermal Calibration Type:
 - o Manual
 - o 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.

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



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

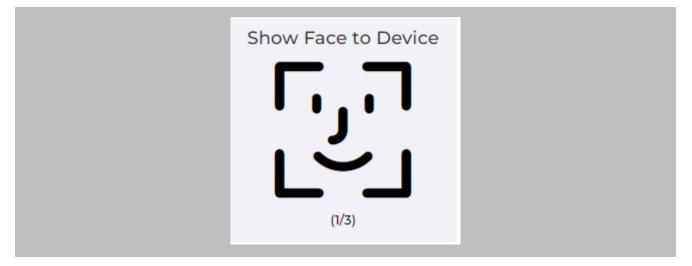


Figure 54: IXM WEB - Capture Thermal Data



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

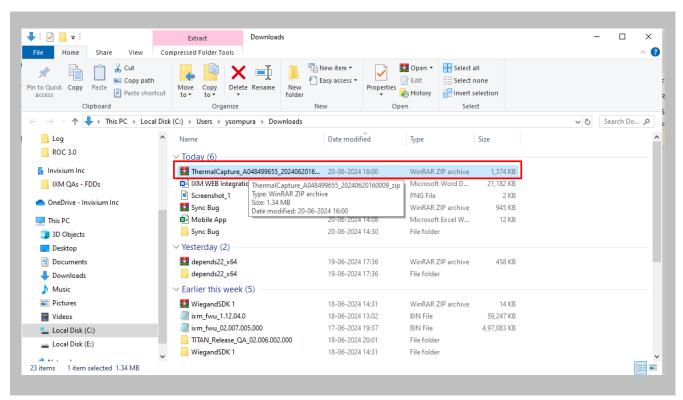


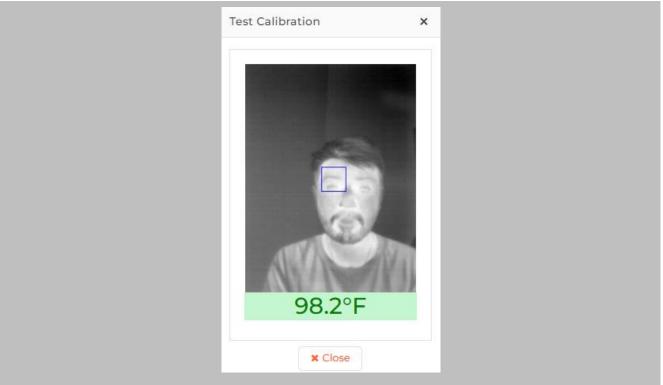
Figure 55: IXM WEB - Save Captured Thermal Data



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

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

Test Calibration Options



To test Thermal Calibration, click Test Calibration.

Figure 56: 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 \rightarrow Options \rightarrow Temperature Unit.

Application Configuration	Data Adapter	Data Export	Options	Smart Card Settings	Wiegand
EMPLOYEE					
Save Fingerprint Image	9				
Certificate for IXM WEB			Ce	rtificate for IXM WEB Clou	d
ixm.web			• i	km.device	
TEMPERATURE UNIT			C	DATE FORMAT	
Temperature Unit			F	ormat	
🔵 Celsius 🚺 Fahrenhei	t			mm/dd/yyyy	

Figure 57: IXM WEB - Option to Change Temperature Unit



Select required temperature unit. Click Save.

TEMPERATURE UNIT	DATE FORMAT	BIOMETRIC
Temperature Unit	Format	USB Senso
🔾 Celsius 🗿 Fahrenheit	mm/dd/yyyy	▼ 1400
AUTO REFRESH DASHBOARD		SAVE BION
Status		V Face
Interval (sec)		
10		
LOGIN		
Disable Concurrent Logins Enable captcha		
		Save

Figure 58: IXM WEB - Save Temperature Unit Setting



Configuring Mask Authentication Settings

STEP 1

Click the Devices tab \rightarrow Select Device \rightarrow Select General Settings \rightarrow Mask Authentication Settings to view default settings.

	Overview Employees Communication Notification Security Access Control General Settings Time & Attendance Smart Card Thermal Settings	
	E IXM WEB Server Verification	
A048499655 /	Mask Authentication Settings	0
Online	CONFIGURATION Authentication Mode	
evice ID	Strict •	
	📄 Duress Status 📄 Capture Image if Mask Missing 🦉 Log Mask Detection Data 📄 Send Wiegand	
rmware Version 2.007.005.000	Missing Mask Warning Message Missing Mask Message Timeout (sec)	
avice Category hterprise Access	Mask not detected 3 *	
mm Mode hernet	FULL FACE AUTHENTICATION	
cure Mode	Enable Full Face Identification	
s	VISITOR SCREENING	
ran FPU5	Enable Visitor Screening	
rial Number)48499655	B APPLY C RESET	

Figure 59: 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.

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

Mask Authentication settings saved 💦 🗙

Figure 60: IXM WEB - Save Mask Settings



13. Fingerprint Enrollment using Access It sofware

Procedure

STEP 1

Log in to the Access It application. Click the System tab on the left-hand menu.

	3
Main Cardholders Cards Macros Alarms Events Tracking Mustering Maps	
Hardware Configuration	
System	

Figure 61: ACRE Security - System



Select Workstations.

Navigation
Main Hardware Configuration System
Servers Sites Workstations Diagnostics System Status

Figure 62: ACRE Security – Workstations



Edit the workstation from which entrollment has to be done.

Workstation Name	Drag a column here to group by this column. Workstation Description	
BHAVESH-PC		
DOM-8M-01		
DIM-QAS		
D DKM-QAS-HARSH		
DIM-QA-TC)		
QA-PC4		



STEP 4

Select the Encode/Enroll tab.

Edit Workstation			- • ×
📕 Save 🗙 Close 🚺			
Workstation name:	DOM:QASHHARSH		
Workstation descrip	tion		
	ation Cardholder Enrollment Enrollment Readers	Encode/Enroll Auditing	· · ·
Attachments			
Location			Select.
Compression factor:	25		(Jentin)
Receive TCP events			
			_





Click New.

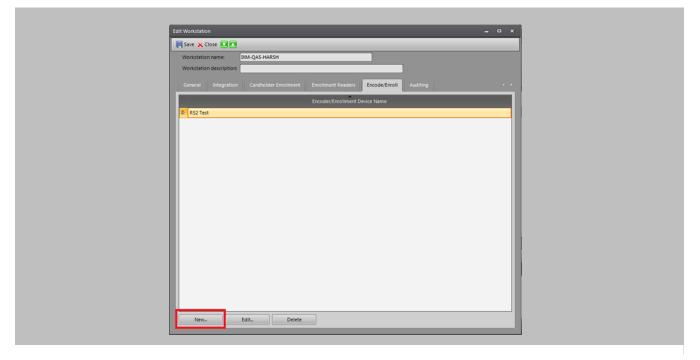


Figure 65: Encode/Enroll – Add New



Enter IXM WEB details as follows:

1	
	Edit Encoder/Enrollment Device
	Device name: RS2 Demo
	Device type: Invixium
	Invixium Enrollment URL
	http://192.168.1.45:9108/Link/EnrolIRS2User/
	OK Cancel

Figure 66: Add new Device

Devide name:

Enter the name of the device.

Device type:

Select "Invixium" from the dropdown list.

Once done, click **OK** button.

Close and reopen the Access It software.



Go to Main >> Cardholder >> Select user >> click on Card Number. This will show the newly created device name.

Nor Main Ver	Convet for Vario		
Card Clubbard Commands	Pret Site hiter Guery results: 7 items (1 currently selected).	Search for	holders) 💁 🚮
Catholden Cosh Cash Cash Cash Cash Cash Cash Cash Ca	Loss hume Pick hume Fig. Proc hume F	Creg a column here to group by the column. Monitor Show	
	• Disense Trites Carls Stat Connector Stree Connector		
DeleTine Site None	Card Number Facility Code C	Benoglan Benoglan	Location

Figure 67: Newly created device



Click on the device name to launch IXM WEB using the "Invixium Enrollment URL" with the cardholder ID appended for enrollment.

C 🛛 N 192.168.1.164:9108	/Home/Index#employee	☆ ♡ (
Devices Employees	Link	ب
♠ > Employees > WEB card		
	Employee information \rightarrow Access rules \rightarrow Biometric data \rightarrow Cards \rightarrow Summary	
Ô	Fingerprints Finger Veins Face	
WEB card	Select Device	
Email -		
Birthdate -		
Gender -	l i i i i	
Template(s) O		
Status Active		No record(s) found
	Enroll face	no neos das round
	법 Save → Save & Continue	

Figure 68: IXM WEB – Biometric Enrollment



14. Enrollment Best Practices

Fingerprint Enrollment Best Practices

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

Avoid Poor Fingerprint Conditions

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

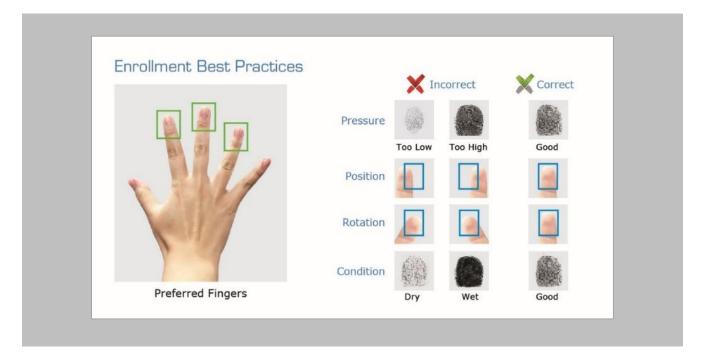


Figure 69: Fingerprint Enrollment Best Practices



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 70: 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.

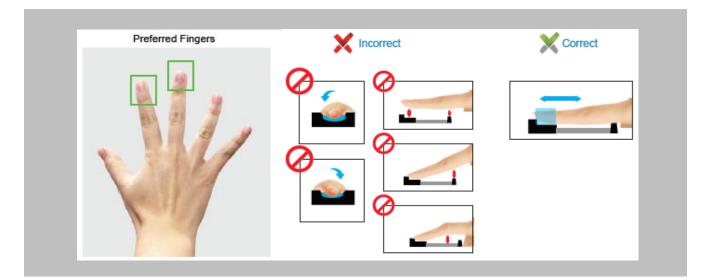


Figure 71: Finger Vein Enrollment Best Practices



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.

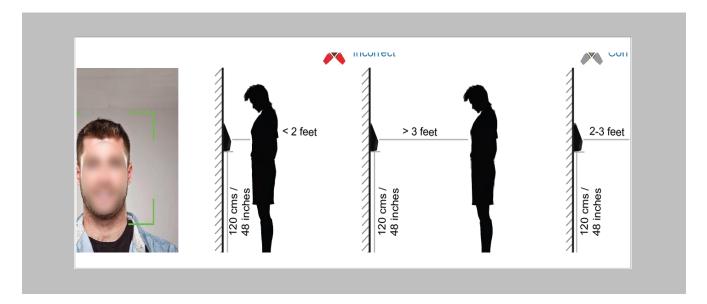


Figure 72: Face Enrollment Best Practices



15. Appendix

Installing Invixium IXM WEB with Default Installation using SQL Server 2014

Note:

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

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

Procedure

STEP 1

Run the installer.exe



Figure 73: Install IXM WEB





ñ

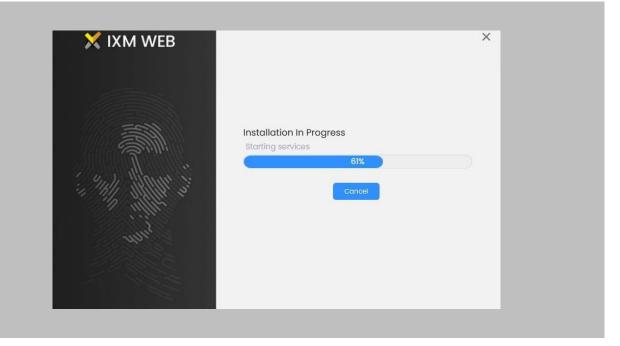


Figure 74: Loading SQL Express & Installation Progress

STEP 2

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

- Bonjour
- Invixium Device Discovery
- IXM WEB



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

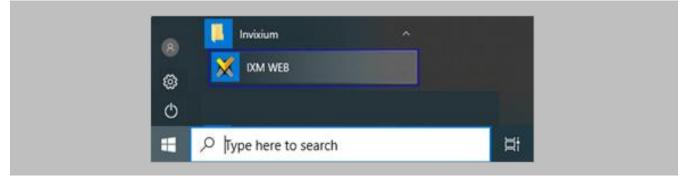


Figure 75: IXM WEB - Shortcut Icon on Desktop

STEP 4

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

Authentication	SQL Server Name
SQL Server	▼ IXM-TS25\SQLEXPRESS × ▼
 SQL User Name	Password
admin	
	% Connect

Figure 76: IXM WEB - Configuring IXM WEB Database



Select the Database Name and then click Next.

	Authentication	SQL Serv	er Name	
	Windows	▼ IXM-QA	20\IXMWEB	×
(100	Database Name			
	IXMDB			×
	CREATE ACCOUNT			
Will Willin "	Admin ID	Password	i	
aller.				
- III	Confirm Password	Email		
	Server URL		Cloud Po	rt
	http://localhost:9108		1255	

Figure 77: 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	Add to Group Delete
						Reboot
						Factory Defaults
						Broadcast Manual Upgrade

Figure 78: IXM WEB - Broadcast Option

STEP 2

Scroll down to the Access Control section \rightarrow check Wiegand Output option \rightarrow Click on Broadcast.

padcast				
	(Select 2 C	Device(s)	
Select All				
Access Control	Door Access Control	Door Open Schedule	Door Strike Power Supply	External Server Feedback
Fire Alarm	Input/Output	OSDP	Panel Feedback	Wiegand Input
Viegand Output	Threat Level			
Schedules				
Access Schedules	Biometric Schedule	Holiday Schedules	Threat Level Schedule	
Security				
Anti-Shock Vandal Protec	tion Device	IP Restriction	Telnet	
Smart Card				
Active HF Protocol	Active RF Protocol	CSN Order Type	Key Management	Layout
		♥ Broadcast		

Figure 79: IXM WEB - Broadcast Wiegand Output Settings



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.

Broadcast		
	Select Device(s)	
SELECT DEVICE(S)	Q Type to search	
🔻 🕑 Device Group		
🔻 🗹 Testing		
✓ b3d587dbf6		
	• ок	

Figure 80: 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**.

Parity Bit	Stop Bit		Timeo	ut (msec)		
▼ None	▼ 1 Bit	•	3000			×
P Text 📃 Smartcard Passthru	Enable Biometric					
Secure Key						
▼ 303132333435363	738393A3B3C3D3E3F0000000000000000	000000000000000000000000000000000000000	000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	00000000000000000000000000000000000000
ON COLOR	OFF COLOR	ON TIME (MSEC)		OFF TIME (MSEC)		DISPLAY MESSAGE
ON COLOR	OFF COLOR	ON TIME (MSEC)		OFF TIME (MSEC)		DISPLAY MESSAGE
-		0		0	•	
Red	 None 	0	v	0	÷	
None None	▼ None ▼	0	*	0	*	
None	▼ None ▼	0	*	0	*	
		None IBit DP Text Smartcard Passthru Enable Biometric Secure Key 3031322333435363738393A3B3C3D3E3F0000000000000000000000000000000000	Vone 1Bit V DP Text Smartcard Passthru Enable Blometric Secure Key 303132333435363738393A3B3C3D3E3F0000000000000000000000000000000000	None IBit 3000 OP Text Smartcard Passthru Enable Biometric Secure Key 303132333435363738393A3B3C3D3E3F0000000000000000000000000000000000	• None • IBit • 3000 >DP Text Smartcard Passthru Enable Biometric Secure Key • • 303132333435363738393A3B3C3D3E3F0000000000000000000000000000000000	• None • IBit • 3000 >DP Text. Smartcard Passthru Enable Biometric Secure Key • 303132333435363738393A3B3C3D3E3F0000000000000000000000000000000000

Figure 81: IXM WEB - OSDP Settings



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.

ñ

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



Click **Apply** to save the settings.

OSDP settings saved

Figure 82: 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 Access It.

lame	Device ID	Device Group		Comm Mode		Device Mode		
b3d587dbf6	0	▼ 1 item(s) selected	×	Wi-Fi	•	Both	•	T&A Device
Secure Mode		1						
THERNET								
P Address	Subnet Mask		Gateway		Port			
	o . o .	o . o	o . o .	οο	9734			
ERIAL								
COM Port	Baud Rate		Serial Mode					
Select	Select	•	RS-232	•				
VI-FI								
P Address	Subnet Mask		Gateway					
192 . 168 . 3 . 243	255 255	255 0	192 168	3 . 1				

Figure 83: IXM WEB - Edit Device Options

STEP 5

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



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

Panel Feedback	· · · · · · · · · · · · · · · · · · ·
LED Mode Tim	imeout (msec)
LED Control By Panel Two LED v 30	3000

Figure 84: IXM WEB - Disable Panel Feedback



Wiring and Termination

Procedure

Earth Ground

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

STEP 1

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

STEP 2

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

STEP 3

Screw the lug end of the earth ground.

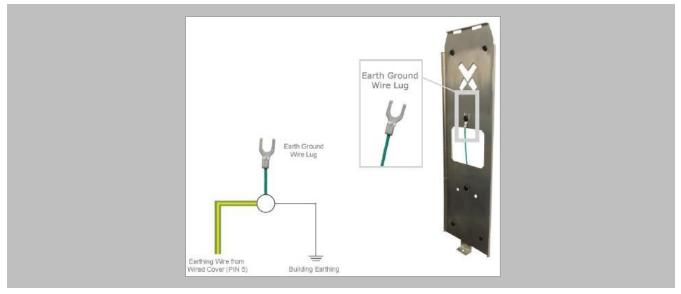


Figure 85: Earth Ground Wiring



Wiring

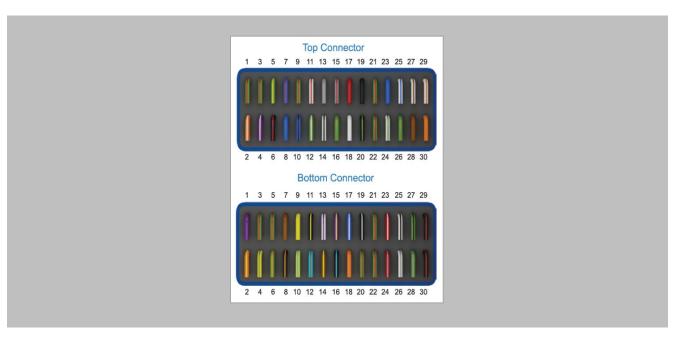
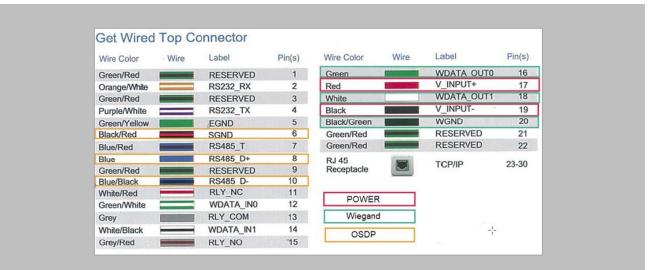


Figure 86: IXM TITAN – Top & Bottom Connector Wiring





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	Company of the Owner of the	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	Concession Services	USB0_D+	27
White/Purple		DAC_IN1	13	Green/Grey		USB1_D+	28
Brown/Yellow	State of the second second	SPI3	14	Black/Red		USB0_GND	29
Purple/Yellow	No. of Concession, name	DAC IN2	15	Black/Red		USB1 GND	30

Figure 87: Power, Wiegand & OSDP Wires



All Invixium devices support Wiegand and OSDP.

Invixium devices can be integrated with ACRE Security Controller on:

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

Wiegand Connection

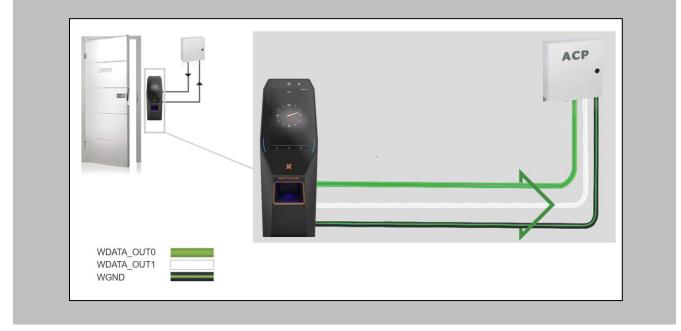


Figure 88: IXM TITAN - Wiegand

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



Wiegand Connection with Panel Feedback

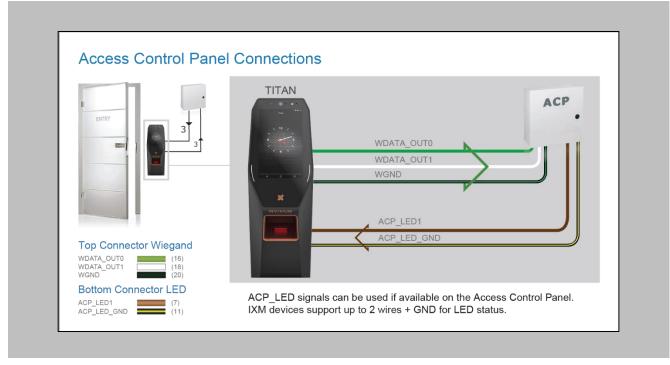


Figure 89: IXM TITAN - Panel Feedback

(1)

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



OSDP Connections

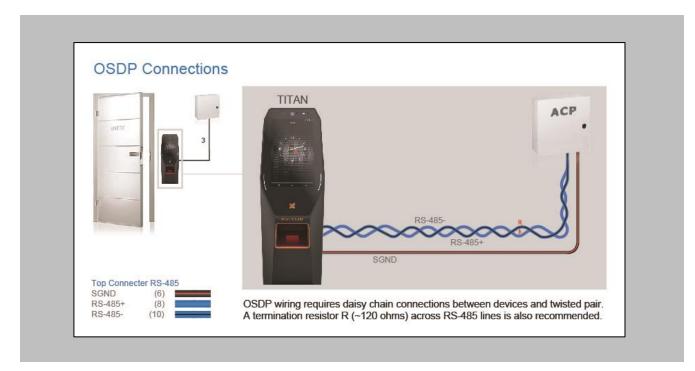


Figure 90: IXM TITAN - OSDP Connections

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



16. Troubleshooting

Reader Offline from the IXM WEB Dashboard

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

Procedure

STEP 1

From **Devices** tab select any device.

STEP 2

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

	Overview Employees Communication Notification Security Access Control General Settings Time & Attendance Smart Card
	External USB Settings
Device ID 0 Firmware Version 02.007.006.000	URL http://ixmtime.invixium.com
Device Category Enterprise Access Comm Mode	Serial
Ethernet Secure Mode No Model Name	USB Auxiliary Port
TITAN FPLV5 Serial Number b3d587dbf6	Server VPN

Figure 91: 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 \rightarrow Application Configuration and make sure that the URL is correct.

1	Devices	Employees	Time	Health	n Visitor	Link	
Applica	tion Configuratio	n Data Adapter	Data Export	Options	Smart Card Settings	Wiegand	
Config	uration						
URL				Cloud Port			
https	:://kr.invixium.com	:2024		2025			
✓ Aj	pply						
IXM W	EB Database						
IXM W	EB Snackbar Not	ification					
LDAP							
Azure	Login						
Auth T	уре						

Figure 92: IXM WEB - Server URL Setting from General Settings



Elevated Body Temperature Denied Access but Granted Access in Access It

Procedure

STEP 1

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

🖭 Wiegand Output							-
EVENTS							
	ID Type		Duress				
Wiegand	Employee ID		None				
	Success		Fail				
dentification	Standard 26 bit	•	None	•			
	Success		Fail				
/erification	Standard 26 bit	•	None	•			
	Format		ID Value				
Anti-Shock	IXM 82 bit Device S/N	•	Device Serial Number	•			
	Format		ID Value	li	nterval (sec)		
Heart Beat	None	•	Device ID	•	60	*	
	Format						
Employee not found	None	•					
	Format						
Thermal Authentication	None	•					
	Format						
Mask Not Detected	None	•					
	Format						
Invalid Attestation Questions	None						

Figure 93: 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.



Book

~

V

V

V

~

Logs in IXM WEB Application

🗹 Capture Device Logs

🖹 APPLY 📥 DOWNLOAD 🗎 DELETE 📿 RESET

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

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

Device Log	^
Capture Device Logs	
E APPLY ADOWNLOAD A DELETE CRESET	
Figure 04: IXM WER Enable Device Logo	

Figure 94: IXM WEB - Enable Device Logs

👓 🛧 투 🖄 🖸 🛛 🕑 😩 ▲ DeviceLogs_A048499655_20. □□ ⊗ 37.ency 147 KB • Done Health Link Time Convert _____IXM_DB_Upgrade_2_3_2_0_to_3_19_6_20 24.bak 65.2 MB • 1 day ago Overview Employees Communication Notification Security Access Control General Settings Time & Attendance Smart Card mermar secong Attestation Questions Backup & Restore Biometric Biometric Schedule O Camera Clock Device Log

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

Figure 95: Save Device Log File



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

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

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

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

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

Logs folder location on IXM WEB Server:

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

Table 7: Logs Folder Location



Unable to connect to the Access It Server

Procedure

STEP 1

ñ

Note: Confirm module activation

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

< _	Devices Employees	Link			ф ⁹ ф
<u>,</u>	IXM TIME		IXM LINK		IXM HEALTH
* ense	124.4		NA 4		
la Ipany	IXM MOBILE	IXM TRANSLATE	IXM API	DATA ADAPTER	CREDENCE ID
AC	CTIVATION HISTORY				
	ACCESS IT! Created By admin	Activation Date 06/25/2024 15:48:10 PM	Type Validity Volume 5000 Devices	Validity Remaining 5000 Devices	Activated

Figure 96: IXM WEB - Licence Module

STEP 2

 \parallel)Note: Confirm Access It API is up and running.

This can be checked from Windows Services (Services.msc).

Services						
File Action View Help						
Þ 🔿 📅 🧟 🖕 🚺 📷 🗠	▶ ■ II IÞ					
Services (Local)	Services (Local)					
	Name	Description	Statu	s Startup Type	Log On As	1
	Access It! Universal.NET	Access It! Universal.NET access control server service.	Runr	ing Automatic	Local System	

Figure 97: ACRE Security - Access It Web API



Note: Confirm WEB Service URL is enabled. Confirm parameters entered to connect to the ACRE Security server.

Ensure the correct **User** who is authorized to log into SQL Server to access the database is listed here. If not, **correct** and **apply**.

Ensure the correct **Password** of the user who is authorized to log into SQL Server to access the database is listed here. If not, **correct** and **apply**.

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

This file is available at the following path:

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



17. Support

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

18. Disclaimer and Restrictions

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

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

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

Copyright © 2024 Invixium. All rights reserved.