

## IXM-WEB Invixium Biometric Solution

Installation • Activation • Setup • Biometric Enrollment

- ◆ System Integration Requirements
- ◆ How to Install and Activate IXM-WEB
- ◆ How to Publish Database and Sign-in to IXM-WEB
- ◆ How to Configure IXM-WEB
- ◆ How to Upgrade Reader Firmware in IXM-WEB
- ◆ How to Enroll Biometric Fingers within System Galaxy
- ◆ Hardware Installation and Wiring Tech Notes.

JAN 2021 | SG 11.7.0 thru Current



# System Galaxy

## Quick Guide

**Invixium Readers  
& IXM-WEB Enrollment**

**2<sup>ND</sup> Edition**

Revision 2.6

**Galaxy Control Systems**

3 North Main Street

Walkersville MD 21793

**[www.galaxysys.com](http://www.galaxysys.com)**

Information in this document is subject to change without notice.

Therefore, no claims are made as to the accuracy or completeness of this document. However, every effort is made to achieve the most accurate information available at the time this manual is written and published.

Galaxy Control Systems makes no claims on the requirements or limitations of software or devices of 3<sup>rd</sup> Party Manufacturers. Every effort is made to include all known requirements and capabilities as they relate to integration with System Galaxy. Information herein may not supersede requirements of 3<sup>rd</sup> party manufacturers.

**Copyright © 2020 ♦ Galaxy Control Systems ♦ All rights reserved**

No part of this document may be reproduced, copied, adapted, or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written consent of Galaxy Control Systems. Copyright protection claims include all forms and matters of copyrighted material and information, including but not limited to, material generated from the software programs, which are displayed on the screen such as icons, look and feel, etc.

### Trademarks

Trademarks herein follow the rule of first mention.

Microsoft®, Windows®, Windows NT®, and SQL Server™ are registered trademarks of Microsoft Corporation in the U.S. and other countries.

Trademarks for Invixium, IXM, IXM-WEB products are the property of Invixium, Inc in the U.S. and other countries.

MIFARE® and MIFARE DESFire® are registered trademarks of NXP Semiconductors. In this guide, these are generally understood to be the *technology type* supported.

HID®, Corporate 1000®, and Lumidigm® are registered trademarks of HID Global Corporation in the U.S. and/or other countries. In this guide, these are generally understood to be the *technology type* supported.

Adobe® and Acrobat® are registered trademarks of Adobe Systems, Inc.

## Table of Contents

<b>System Galaxy Integration with IXM-WEB .....</b>	<b>5</b>
Compatibility Overview.....	5
SOFTWARE .....	5
HARDWARE .....	5
SYSTEM INTEGRATION DIAGRAM.....	5
INTEGRATION REQUIREMENTS .....	6
REQUIREMENTS:.....	6
<b>Start the Installation Process .....</b>	<b>7</b>
Verifying System Galaxy Setup.....	7
Verifying GCS Web API Service .....	8
Verify of IIS Server Installation .....	8
Installing IXM-Web Application on the Galaxy Server.....	9
INSTALLING IXM-WEB.....	9
CREATE DATABASE ON FIRST LAUNCH.....	11
ACTIVATE THE IXM-WEB LICENSE .....	13
REQUEST THE DEVICE LINK LICENSE FOR READERS .....	15
ACTIVATE THE GALAXY DEVICE LINK.....	17
CONFIGURING THE LINK TO IXM-WEB.....	19
ADDING THE READER DEVICE TO THE SYSTEM.....	20
UPGRADING THE READER FIRMWARE.....	23
CONFIGURE READER FOR ACCESS CONTROL .....	26
CREATING AN EMPLOYEE GROUP.....	28
CREATE A SYNC GROUP.....	29
<b>Enrolling Cardholders in System Galaxy.....</b>	<b>30</b>
CARDHOLDER ENROLLMENT STIPULATIONS.....	30
PRE-ENROLLING A NEW ACCESS CARD .....	30
ENROLLING BIOMETRIC CREDENTIALS IN SYSTEM GALAXY .....	31
Quick Enroll for Biometric-Only Credentials .....	31
<b>Appendixes .....</b>	<b>35</b>
INVIXIUM READER INSTALL REQUIREMENTS: .....	35
Invixium Biometric IXM Reader - Cable Specs & Wiring Pinout .....	35
Full Integration Requirements Checklist.....	36
Glossary of Terms.....	38

## History Table - Document and Features

Date	Edition	Description
JULY 2020	SG 11.6.0  2nd Edition	<p><b>VERSION RANGE:</b> These instructions are published at the release of <i>System Galaxy</i> (SG v11.6.0) and IXM-WEB v2.2.</p> <p><b>SCOPE:</b> This is an integration guide that covers the integration between System Galaxy and IXM-WEB. This guide covers requirements, installation, functionality, and features specifically related to the biometric integration and enrollment. General functionality or other features that are outside the scope of this guide are not discussed herein.</p> <p><b>LIFE CYCLE:</b> These instructions are considered <i>current</i> and applicable to this integration until a future version introduces a major change or redesign that makes these instructions no longer valid as a whole, at which time a <i>new edition</i> of this guide will be published, and this <i>existing edition</i> will be given a cut-off version. When minor changes are discovered, the <i>existing edition</i> will be revised, its revision number incremented, and the affected instructions will be updated with a <i>versioned annotation</i> that describes the new change.</p> <p>You can check with <i>customer service</i> to confirm compatibility of a newer version of SG or IXM-WEB.</p>

## Table of Supporting Documents

Document	Descriptions
System Galaxy User Guide	<i>The main System Galaxy software user manual.</i>
System Galaxy System Specifications Guide	<i>The consolidated list of system requirements and specifications for SG.</i>
600-635 Hardware Install Guide	<i>The main hardware installation guide for 635 &amp; 600-series hardware</i>

# System Galaxy Integration with IXM-WEB

System Galaxy integrates with Invixium's IXM-Web application using *IIS Server* and Galaxy's *Web-API Service*. The IXM database can be published on Galaxy's SQL instance.

All *Invixium Biometric Readers* are supported and licensed through IXM-WEB (*link activation*). The *access decision* is controlled by the Galaxy panel, therefore the IXM Reader '*Voice Command*' should be configured to "follow panel decision".

Biometric enrollment is performed from the *SG Cardholder screen* where the **IXM-WEB Enrollment module**. The biometric credential is assigned to an *IXM Employee Group* during enrollment and then downloaded to the reader based on the associated Sync Group.

## Compatibility Overview

At the time this guide is written, the following features are supported.

### SOFTWARE

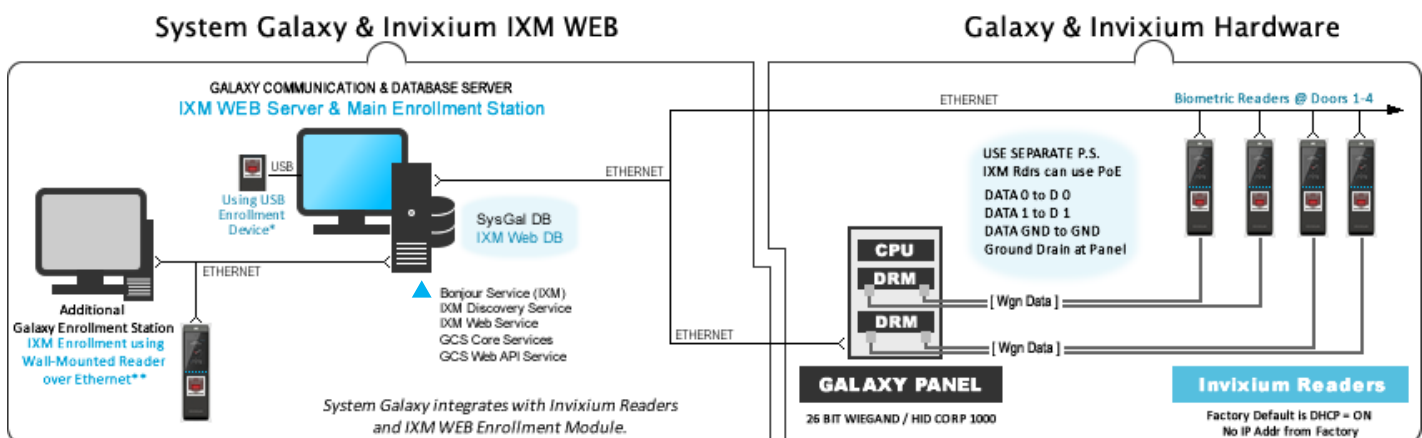
- 1) System Galaxy v11.6.0 (or higher)
- 2) IXM-WEB 2.2
- 3) Data Synchronization: "unidirectional-downstream data-sync" (SG to IXM) (recommended).
- 4) Authentication Types: Biometric Only, Prox + Biometric; *plus types listed in IXM* (see Invixium Documentation or current Invixium Specifications, which may vary based on the reader model).

### HARDWARE

- 5) Galaxy Hardware: 508i-series and 635-series Access Control Panel with 635-series DRM Boards. Also
- 6) Card Technology: 26-bit Wiegand, HID Corporate 1000, MIFARE, DESFire (contact Customer Service information on additional supported technology types).
- 7) See [Reader Wiring Requirements](#)

## SYSTEM INTEGRATION DIAGRAM

Invixium can be installed on the same computer with the System Galaxy installation.



## INTEGRATION REQUIREMENTS

This covers the basic requirements for installing, license/activations, software configuration, compatibilities and dependencies for readers and software. For enrollment requirements, see the Enrollment section of this guide.

★ **NOTICE • REQUEST THE IXM-WEB ‘Download Link’ and ‘Web Activation Key’. This request is not immediate!**

Create an account and complete an [Online Request Form](#) to get the *Download Link* and *Web Activation Key* by email.

★ **NOTICE • You must also send a ‘Link Activation Request’ that covers the number of readers you are installing.**

This *Link Activation Request* is launched from within the IXM configuration screen, after the IXM-WEB software is installed. Once the Link Activation is done, you can connect to the readers and upgrade firmware. See instructions in this guide.

### REQUIREMENTS:

- a. Start the installation procedure. The assumption is that the System Galaxy software has already been correctly installed and registered.
- b. If System Galaxy software is not yet installed, refer to the [System Installation QRS](#) for system installation.
- c. If System Galaxy software is installed, refer to [Verifying System Galaxy Setup](#) in this guide.
- d. The enrollment PC must have a dedicated USB port for a finger capture device (if used) and a valid Browser.

See [IXM-WEB 2.2](#) list of compatible browsers for. Scroll to the bottom of web page and click **[+more]**.

**Edge** v40 or higher

**Chrome** v70 or higher

**IE 11** or higher

**Firefox** v70 or higher

# Start the Installation Process

This section covers performing the necessary system validation and then performing the IXM-WEB Installation.

1. [Verifying System Galaxy Setup](#)
2. [Verifying the GCS Web API Service](#)
3. [Verifying the IIS/Web Service](#)
4. [Installing the IXM-WEB Application](#)

## Verifying System Galaxy Setup

*This procedure verifies that System Galaxy is configured for biometric support, and that you can enroll a test card.*

2. Sign-in to System Galaxy using a master-level login to begin verification steps.
3. Open SG Operator screen ([Configure > System > Operators](#)) and verify that the *Web API Login and Password* have been added as a master operator. The name and password must exactly match what you made during Step-3 of the installation. You must set this credential to be a *master operator* that *never expires*.
4. Open System Registration screen ([Configure > Options > Registration > System](#)) and verify *System Galaxy* is registered for “Biometric Support” option and the IXM reader count must be included in the *total reader count*, but not in the *biometric reader count*. IXM readers will be licensed under the IXM-WEB software link license.
5. Open *System Settings* screen ([Configure > Options > System Settings](#)) verify Biometric System and Server URL are configured correctly.
  - a. Biometric System field = “Invixium Access”
  - b. Invixium Enrollment checkbox option = checked/enabled.
  - c. Invixium Server URL is correct  
( “http://localhost:9108/Link/EnrollGalaxyUser/” is the default; edit as needed).
6. Open Loop/Cluster Properties screen ([Configure > Hardware > Loops](#)) and select the LED Options tab:
  - a. verify Door Locked = Steady High
  - b. verify Door Unlocked = Steady Low
7. Open Reader Properties screen ([Configure > Hardware > Readers](#)) verify the Reader Type field should be “Wiegand Standard”.
8. Open the SG Cardholder screen ([Configure > Cards > Cardholder](#)), verify you can create a simple test credential.
  - a. Enter the First and Last Name, a valid Card ID, add the appropriate Authorized Loop, and assign access privileges that are valid (such as ‘unlimited access’ or a valid custom access group).
  - b. Save the *test card* by clicking APPLY, which will add a Common ID to the record.
  - c. Reselect the cardholder and click EDIT and verify that the [Launch IXM WEB] button is unlocked.  
NOTE: You will not be able to enroll fingers until after the Invixium is correctly installed and configured.

## Verifying GCS Web API Service

*This procedure verifies GCS Web API Service.*

- d. The GCS Web API Service must be running on the System Galaxy Main Communication Server.
- e. Open a web browser on the Comm Server. Enter the Swagger URL into the browser address field to verify you can reach the default *Swagger* page.
  - <http://localhost:8000/swagger> (enter this in the browser on the SG Comm Server)
  - <http://X.X.X.X:8000/swagger> (where 'X' is the raw IP Address of the SG Comm Server)

## Verify of IIS Server Installation

*This procedure verifies your IIS Server Installation will support the IXM-WEB application.*

1. Open a web browser on the computer that is hosting your IIS Server.
2. Enter the default IIS Server URL to verify you can reach the default ISS Host webpage
  - <http://localhost> (enter this in the browser on the SG Comm Server)

NOTE: you can install the IIS Server from the *Galaxy IIS Install Helper utility* by clicking the "Install IIS Web Server" link from the splash-screen of the System Galaxy Installation Media (USB/ISO) *Galaxy Installer App*.



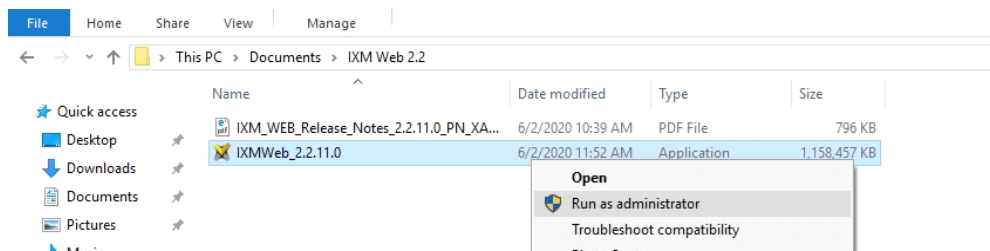
# Installing IXM-Web Application on the Galaxy Server

This section describes installing Invixium's IXM-WEB application on the IIS Web Server.

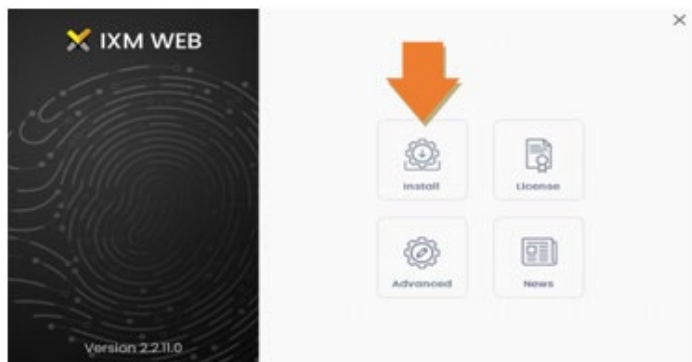
- The install tech must have already obtained the IXM *Download Link* and *Web License key* from Invixium at <https://ixmweb.invixium.com/Web/IXMWEB> .
- You must run the IXM Installer (.EXE file) "as administrator".
- IXM-WEB default port is 9108.

## INSTALLING IXM-WEB

1. When you launch the IXM installer, you must "run as administrator".



2. Click on the **Install** button to begin the install.

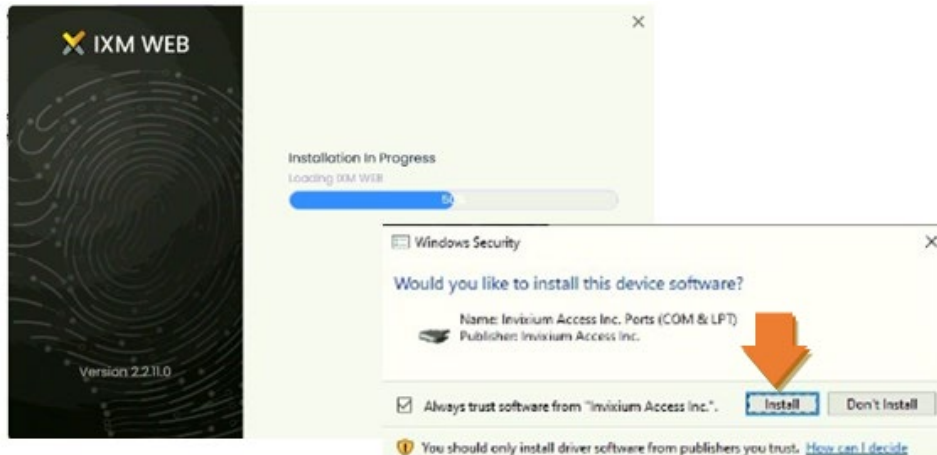


3. Click **YES** to accept the license agreement

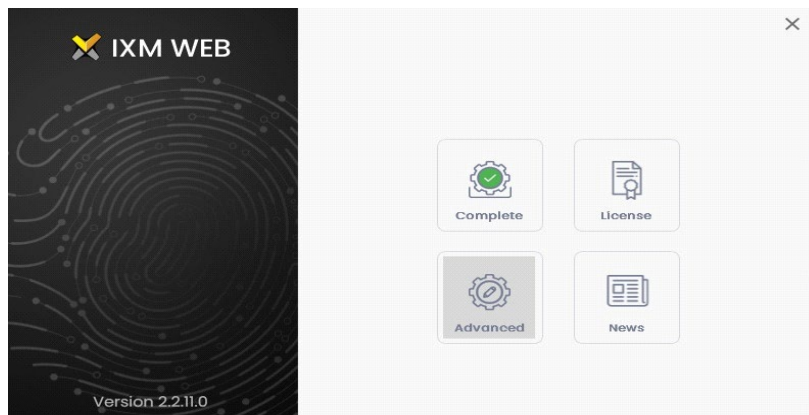


- During the install you will be prompted to install drivers for fingerprint capture and com ports.

NOTE: Also, if IIS is not properly installed you will not get past this point. If the progress bar seems to hang up or stall about halfway through, be sure you have properly installed IIS. Use the Galaxy [\*IIS Install Helper Utility\*](#) that can be launched from the System Galaxy installer splash screen.



- When the install is complete you will see this. Close [X] to exit this screen.



- You should see the IXM Web desktop shortcut.



## CREATE DATABASE ON FIRST LAUNCH

This topic covers installing the Invixium database on the Galaxy SQL Instance “GCSSQLEXPRESS”, which was created when you ran Step-2 of the System Galaxy installer.

### REQUIREMENTS:

- System Galaxy databases and SQL Server Instance must already be installed and online.
- You must create the Invixium database and a login account.
- Remember to use the **Windows Authentication**, select the Galaxy SQL instance GCSSQLEXPRESS.

1. Launch the IXM WEB from the desktop shortcut.



2. Click the **Connect** button to proceed.

A screenshot of the 'Configuring IXM WEB Database' window. It has a title bar and a light blue header. Below the header, there are two dropdown menus: 'Authentication' set to 'Windows' and 'SQL Server Name' set to 'DEV1\GCSSQLEXPRESS'. A blue 'Connect' button with a white icon is at the bottom left.

3. Click **Next** button to create an account to access the IXM database. When the database is created you will be redirected to the sign-in screen.

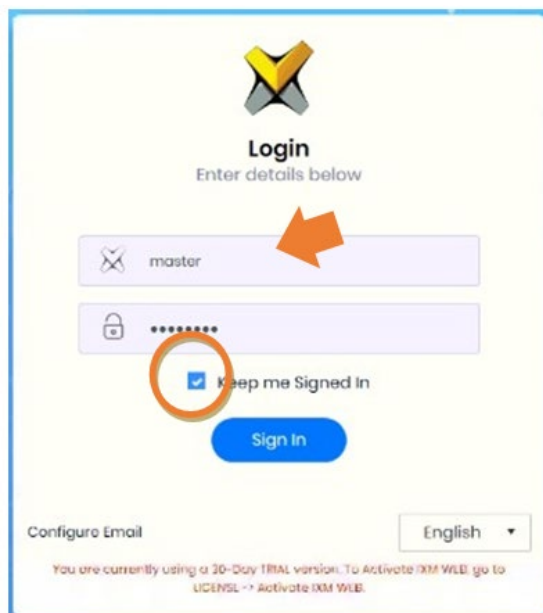
A screenshot of the 'Configuring IXM WEB Database' window, showing the next step. It has the same title bar and header. Below the header, there are three dropdown menus: 'Authentication' set to 'Windows', 'SQL Server Name' set to 'DEV3C4\GCSSQLEXPRESS', and 'Database Name' set to 'IXMDB'. At the bottom, there are two buttons: '< Back' and '> Next'.

4. In the Create Account section, enter a unique login credentials here.
5. Click the **Save** button.



6. In the Login screen, enter the login credentials you just created. This is the login credential for the Invixium database.
7. Check the '**Keep me Signed in**' option.

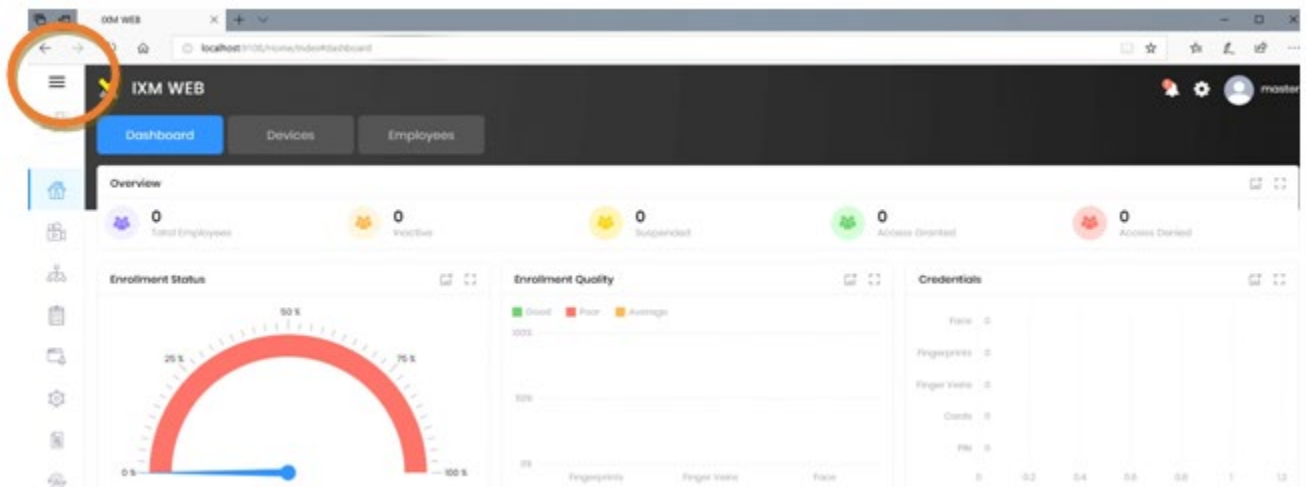
IMPORTANT: This option must be checked if you don't want the Galaxy operator to need to sign-in to the Invixium Enrollment Web Module every time they click the [Launch IXM] button to enroll fingerprints. If you did not check this option now you can simply sign out of Invixium at the Web browser and sign back in to get to this option again.



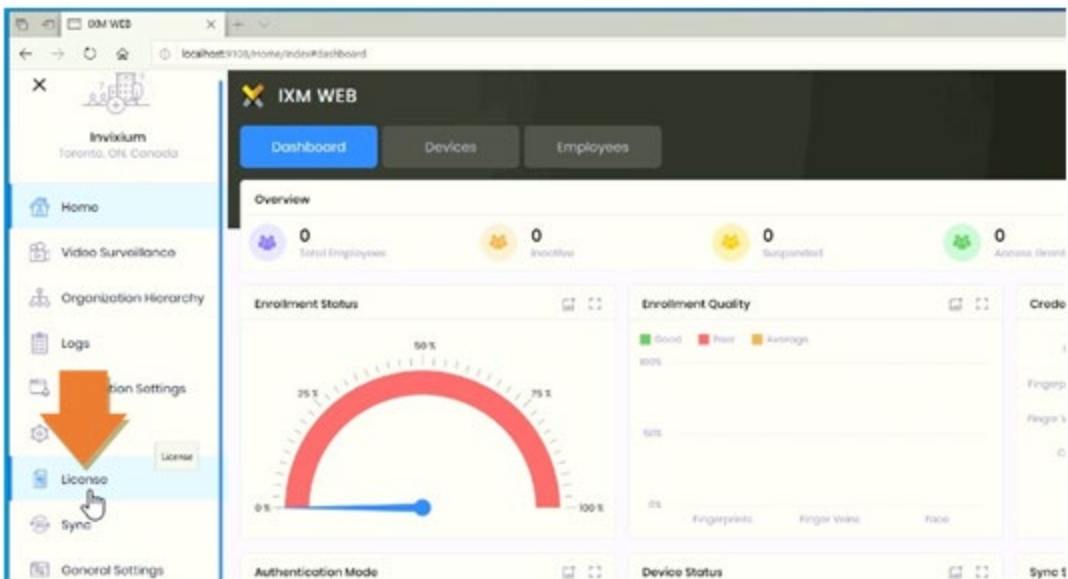
8. Click the **Sign In** button.

## ACTIVATE THE IXM-WEB LICENSE

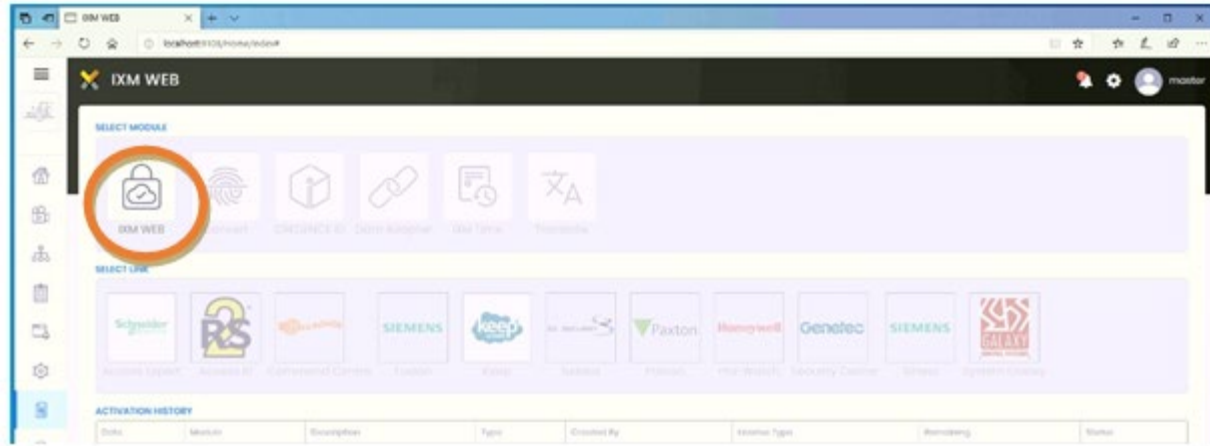
1. The **Dashboard screen** will open in your browser.  
You can **expand the left side-menu** by clicking the **hamburger symbol** in the top left corner. Expanding the side-menu allows you to see the text-labels of each menu option.



2. To activate the IXM WEB license, you must enter the Web Activation key that you received from Invixium.
3. Click on the **License** menu option in the side menu.



4. Click the **IXM-WEB** module.



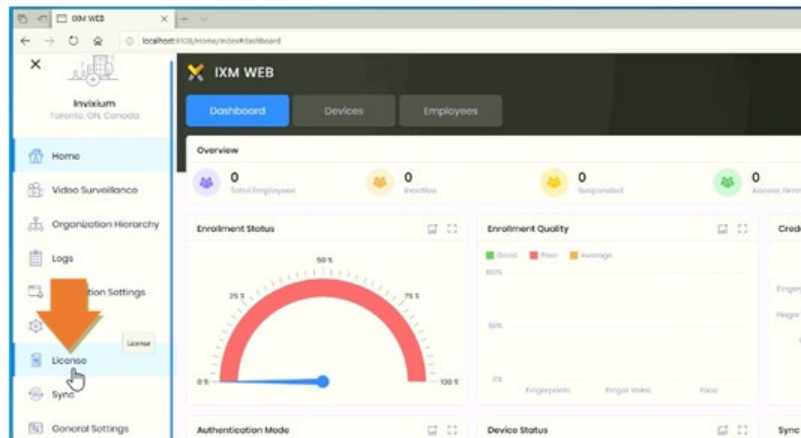
5. Select the “**Online**” option in the Activation Type droplist and **enter the Web Activation key** .
6. Click the **Activate** button – you must have a public internet connection to complete this process.

A screenshot of the 'IXM WEB Activation' dialog box. It features a title bar with the text 'IXM WEB Activation' and a close button. The dialog contains two main input sections. The first section, labeled 'Activation Type', has a dropdown menu currently showing 'Online'. The second section, labeled 'Activation ID', has a text input field containing the alphanumeric string 'YC-4F-FF-RL-F2-MW'. To the right of this field is a blue button with a checkmark and the text 'Activate'. Below the input fields is a light blue button with a cross icon and the text 'Cancel'.

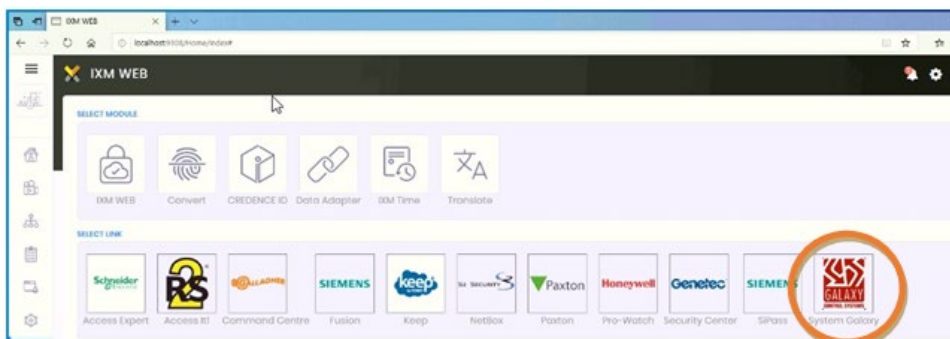
NOTE – optionally you can switch to an offline request, which will display a REQUEST button that you click open a request popup dialog that you enter the activation ID and then click the copy button it will copy the machine key and other info that you will paste into an email to get another license key.

## REQUEST THE DEVICE LINK LICENSE FOR READERS

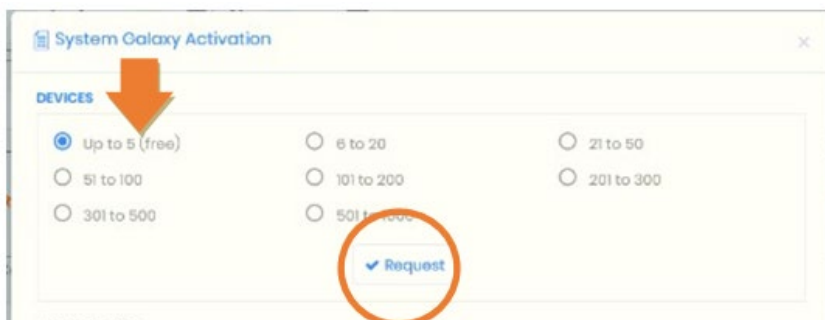
1. Refresh the browser IXM web page (click F5)
2. Click on the **License** menu option in the menu sidebar.



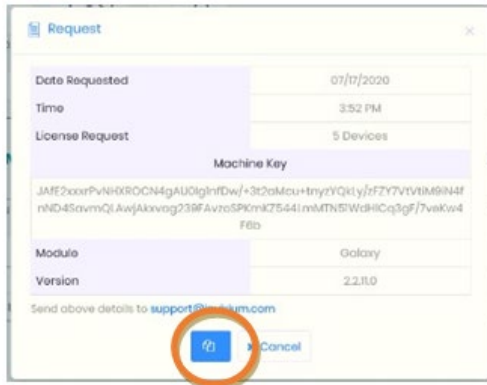
3. The **Galaxy module** will be enabled.



4. Click the **Galaxy module** to open the Galaxy Device Link Activation window.
5. Click the **number of devices** you want to purchase a license for, and click the **REQUEST** button,



6. In the *Request window*, click the **COPY** button to capture the machine key to your PC clipboard.



The screenshot shows a 'Request' window with the following details:

Date Requested	07/17/2020
Time	3:52 PM
License Request	5 Devices
Machine Key	
JAF2xxrPvN+0ROCN4gAU0gInFDw/+3t2oMou+tnyzYQkly/fZY7YV1IM9IN4F nND4SavmQlAwjAkkvvg239FAvraSPKmk27544InbMTN5IWdHCo3gf/7vskw4 F6b	
Module	Galaxy
Version	2.2.11.0

Send above details to [support@invixium.com](mailto:support@invixium.com)

At the bottom, there is a blue button with a copy icon (two sheets of paper) and a 'Cancel' button. The copy button is circled in red.

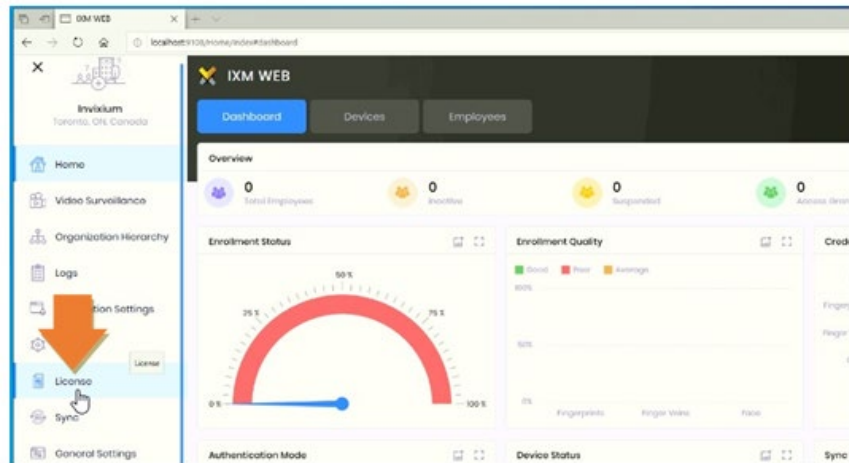
7. Paste the information into your email and send the request to Invixium at [support@invixium.com](mailto:support@invixium.com). You should receive an email with your activation key.
8. Exit the request screen for now.



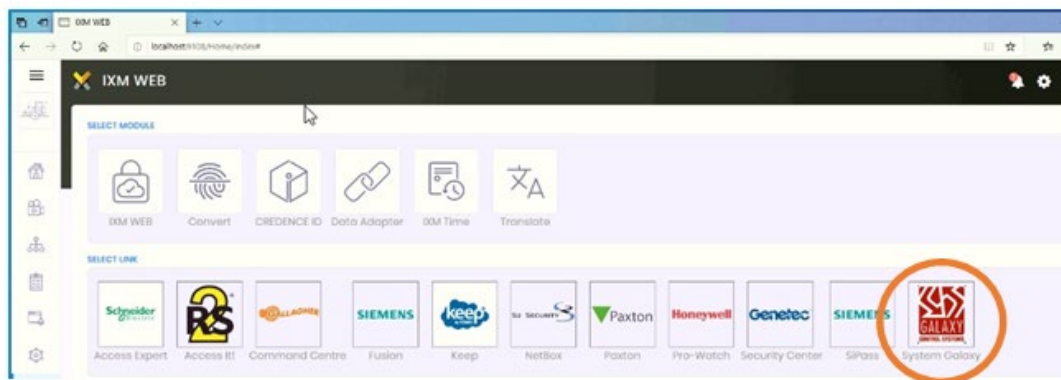
## ACTIVATE THE GALAXY DEVICE LINK

- You must choose the same reader *number range* that you requested.
- You may need to refresh the web page (F5) and open the License page.

1. Refresh the browser IXM web page (F5)
2. Click the **License** menu option in the menu sidebar.



3. Click the **Galaxy module** to open the *Galaxy Device Link Activation* window if needed.



4. Click the same **number of devices** you requested the license for.
5. Enter your Link Activation Key in the appropriate field.
6. Then click the **ACTIVATE** button. Click the **OK** button to close the confirmation message.

The screenshot shows a 'System Galaxy Activation' dialog box. It has a title bar with a close button. The main area is divided into sections. The first section is titled 'DEVICES' and contains a grid of radio buttons for selecting the number of devices: 'Up to 5 (free)', '51 to 100', '301 to 500', '6 to 20', '101 to 200', '501 to 1000', '21 to 50', and '201 to 400'. An orange arrow points to the 'Up to 5 (free)' option. Below this grid is a 'Request' button. The second section is titled 'Activation Key' and contains a text input field with a long alphanumeric string and a clear button. To the right of this field is an 'Activate' button, which is circled in orange. At the bottom of the dialog is a 'Cancel' button.

## CONFIGURING THE LINK TO IXM-WEB

Now that the link has been activated, it needs to be configured.

- You must know the GCS Web API Login credentials to complete this part.
- You must have already added and activated the Link Activation Key (in previous section).

1. Click on the **Link** menu option on the left menu sidebar.
2. Set the Link **Status** (blue) toggle button to 'ON'.
  - a. Enter the **IP address** and use **port 8000** to the Galaxy PC that hosts the **GCSWeb API service**,
  - b. Enter the **User Name** and **Password** for the GCSWeb.Api service.
  - c. Select the **Card Type** you will be using,
  - d. Set the Synch Direction the (**IXM ← Galaxy**) unidirectional option.
  - e. Set Auto Transfer field to “**All Employees to All Devices**”.
  - f. Click **Apply**.

The screenshot shows the IXM WEB interface in a web browser. The left sidebar contains a menu with various system options. The main content area displays the configuration for 'Link System Galaxy'. The 'Status' toggle is turned on, indicated by a blue circle and an orange arrow. The configuration fields are as follows:

Field	Value
Web Service URL	http://192.168.0.10:8000
Web Service User	master
Web Service Password	*****
Card Type	26 Bit Wiegand
Interval (sec)	30
Sync Direction	IXM WEB ← Galaxy
Auto Transfer	All Employees to All Devices
Sync Card code With	Prox ID

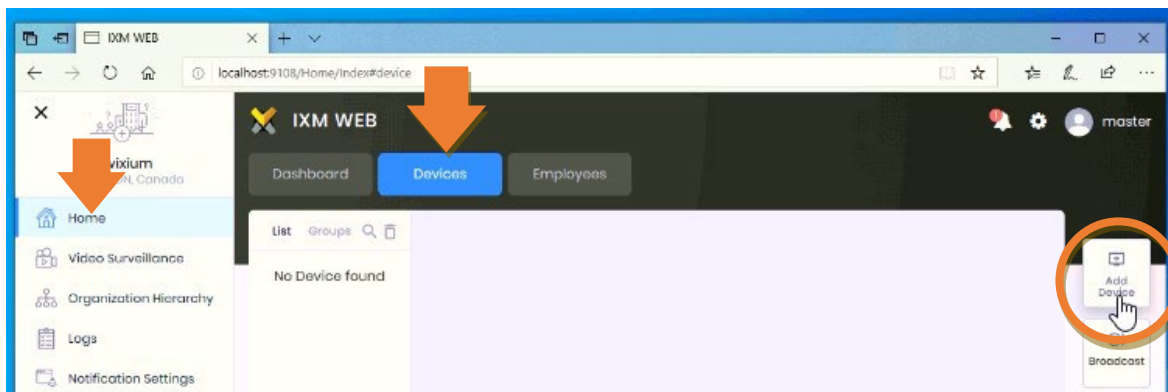
At the bottom, there is a link to the Galaxy website for more information and two buttons: 'Apply' and 'Reset'.

## ADDING THE READER DEVICE TO THE SYSTEM

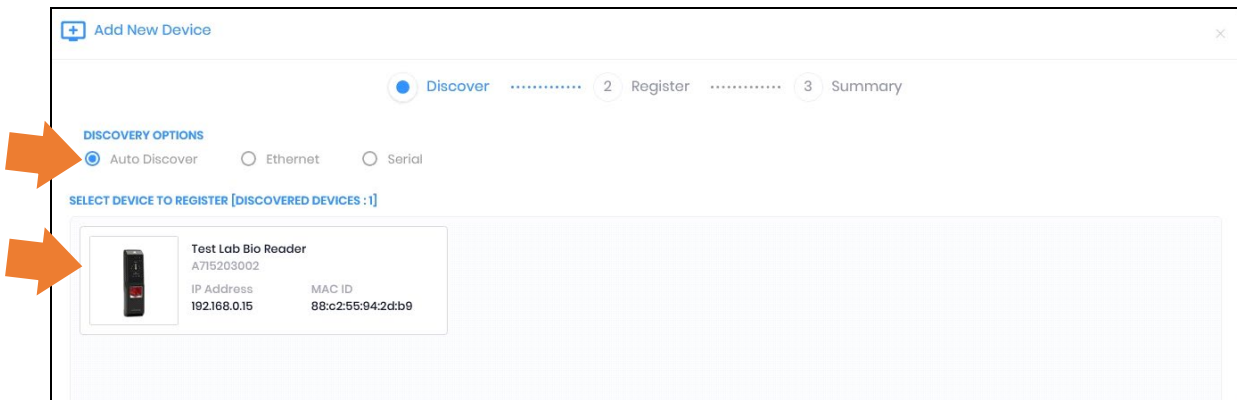
This step describes adding IXM readers to the IXM-WEB software by using Auto-Discovery option in the Add Device wizard.

- Before you can add a reader to IXM software, the reader must already be installed, powered on, and connected to the Ethernet/LAN.
- If the IXM **auto-discovery option** cannot auto-detect the reader, you can use the default password to manually reset the reader to factory default. Optionally, you can manually configure a valid IP Address into the reader.
- See [Reader Wiring Requirements](#) in the Appendix as needed.

1. Go to the *Home page* and click the blue **Devices** button on the top of the webpage.
2. Click the **Add Device** tile on the right-side tilebar.



3. Select the **Auto Discover** option and the reader(s) should appear.  
*NOTICE: If a reader is not detected, program/reset the reader from its touch screen using the default password is "0000".*
4. Click on the **Reader Tile** to open the *Add New Device* screen.



5. Enter a **name** for the reader.  
*Note that the DEVICE ID field is IXM's system ID – it is generated when the record is saved.*
6. Set IP Parameters as appropriate.
7. In the **Device Group** field, you will type a device group name into the field. And press the ENTER key to commit your name to the system. This will create the device group name on-the-fly.  
*NOTICE: it may be advisable to put all readers in the same device group for simplicity of managing the synchronization of finger data (users).*
8. Click the **Register** button without leaving or tabbing away from the field.

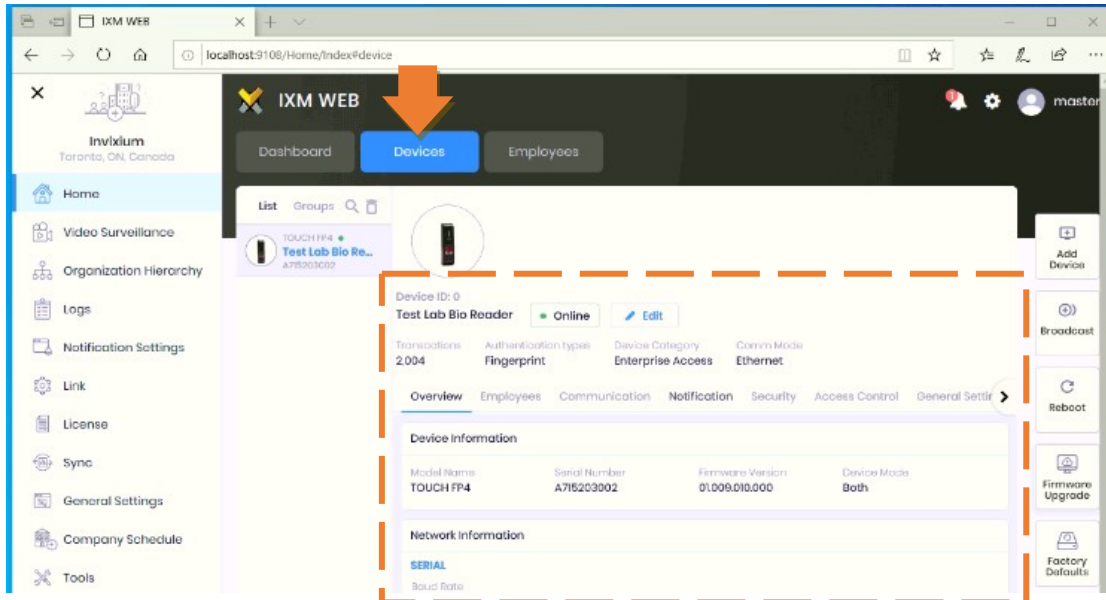
The screenshot shows the 'Add New Device' window with the 'Register' tab selected. The 'GENERAL INFORMATION' section includes fields for Name, Device ID, Device Group, and Device Mode. The 'NETWORK INFORMATION' section includes a checkbox for DHCP and fields for IP Address, Port, Subnet Mask, and Gateway. An orange box highlights the network information fields, and an orange arrow points to the 'Register' button.

9. The “Device Registered” message will display.
10. Click **Done**. (Optional – you can click Add New button and repeat these steps to add another reader).

The screenshot shows the 'Add New Device' window with the 'Register' tab selected. A green checkmark icon and the text 'Device Registered' are displayed. Below, the 'Device Information' and 'Network Information' sections are shown. The 'Device Information' section includes fields for Device Name, Model Name, Serial Number, and Firmware Version. The 'Network Information' section includes fields for Comm Mode, IP Mode, IP Address, Subnet Mask, Gateway, and MAC ID. An orange arrow points to the 'Done' button.

11. The reader(s) appears in the *Devices* screen after it is successfully added and you clicked Done.

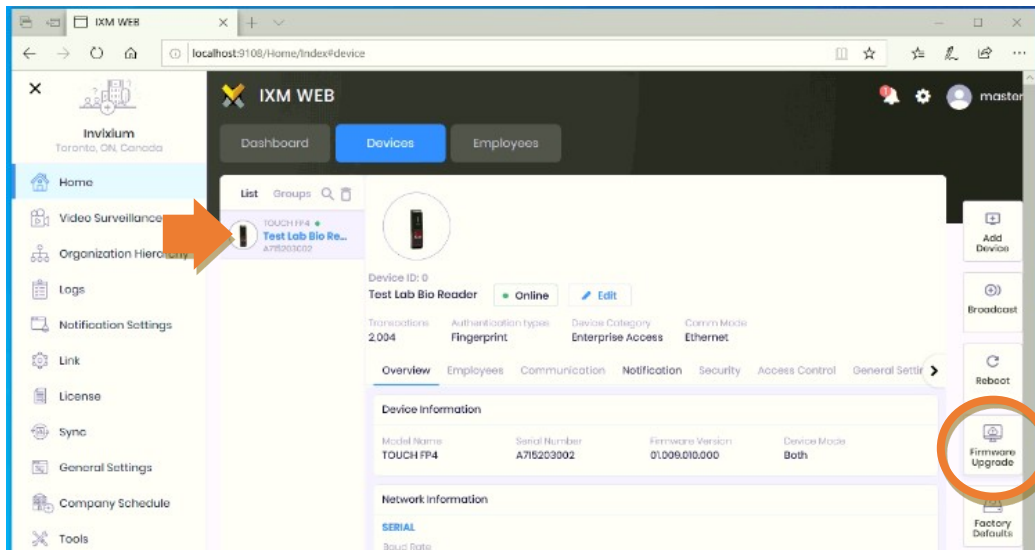
- You can still *add another reader* by returning to the beginning of this section and clicking Add Device.
- You can *upgrade firmware* or *confirm your firmware* as needed – see the next section.



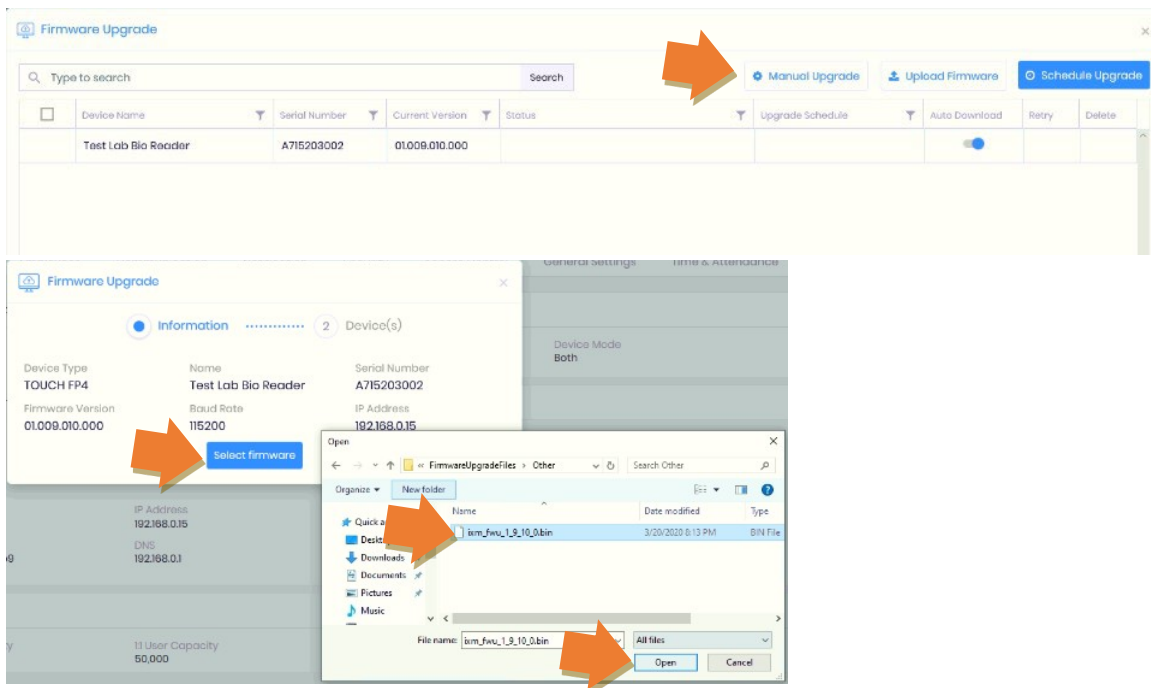
## UPGRADING THE READER FIRMWARE

Once a device is online, you need to verify your firmware and upgrade firmware as needed.

1. From the Home page, click the **DEVICES** button on top of the Home screen.
2. Select the reader you want to upgrade.
3. Click the **Upgrade Firmware** tile that is on the right-side tilebar.



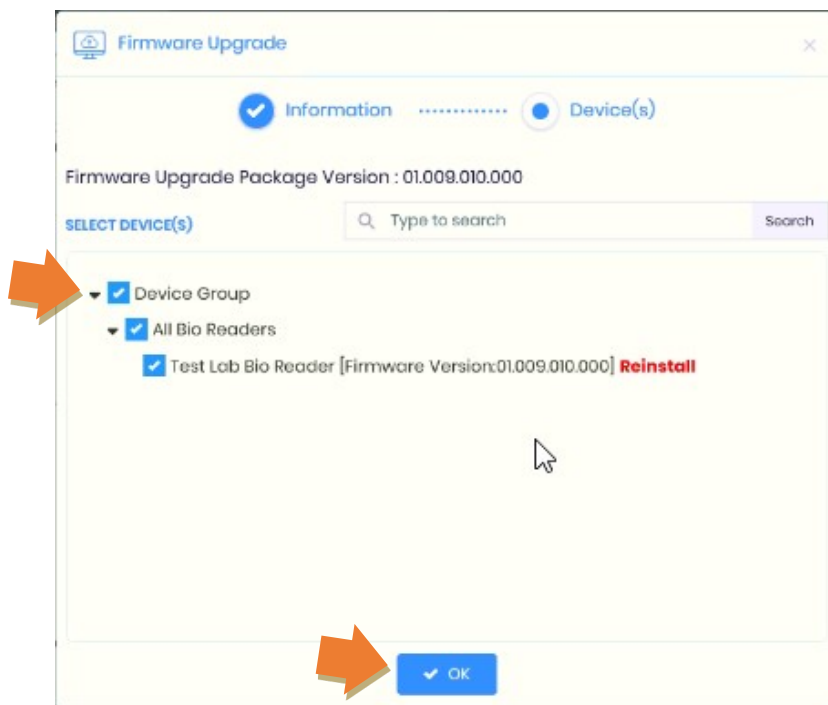
4. Click the **Manual Upgrade** button and navigate to the firmware file location.  
Program Files(x86)\Invisium\IXM WEB\FirmwareUpgradeFiles\Other (depending upon the reader model you have).



5. Click **Continue** button to open the firmware Upgrade window where you can select which reader(s) to update.



6. Click the **Device Group** checkbox or the desired reader(s) to select the target reader to be upgraded.
7. Click **OK** to continue.

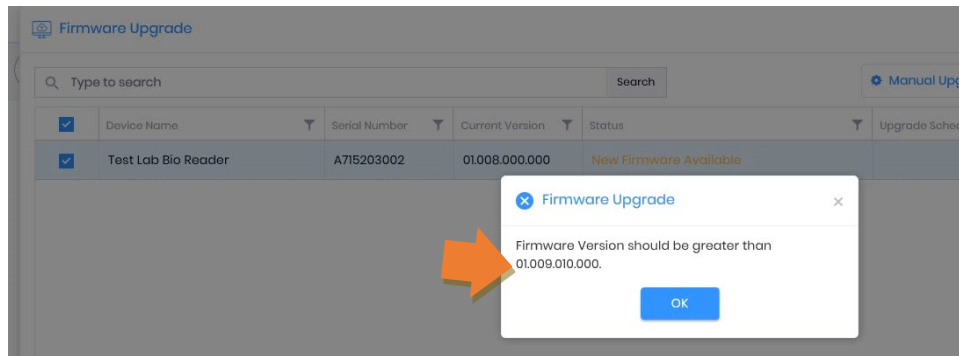




8. The Upgrade dialog box caption will show the firmware version you will get. You can see your reader's current version in the background screen.

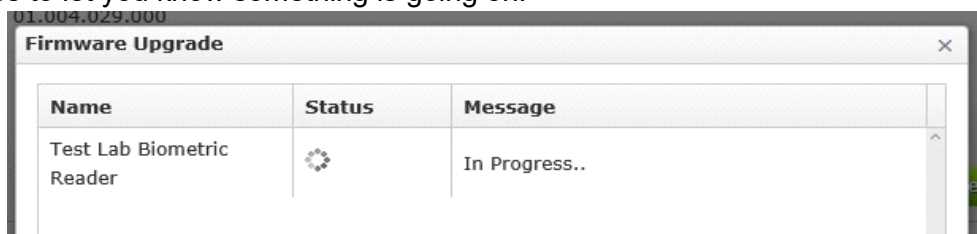
9. Click OK to proceed if appropriate.

**DO NOT CLICK OK IF YOU ARE NOT READY TO UPGRADE READERS – Notice: any fingers or user data in the reader may be reset. Reader may display a “database synching” message which means the system is restoring finger data to the reader.**

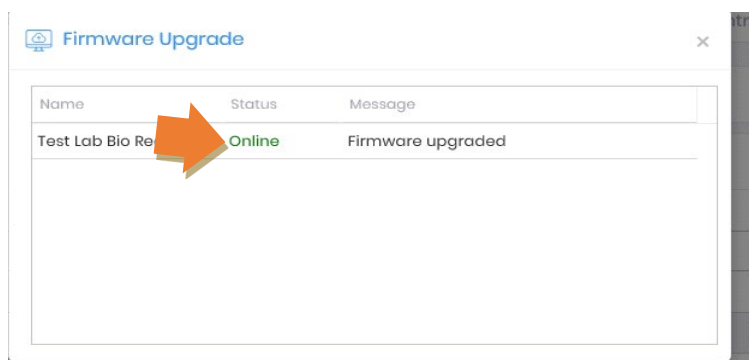


10. During the Firmware Upgrade, the “In Progress” message will display.

This could take a while, and while the firmware is being downloaded the reader will make all kinds of audibles to let you know something is going on.



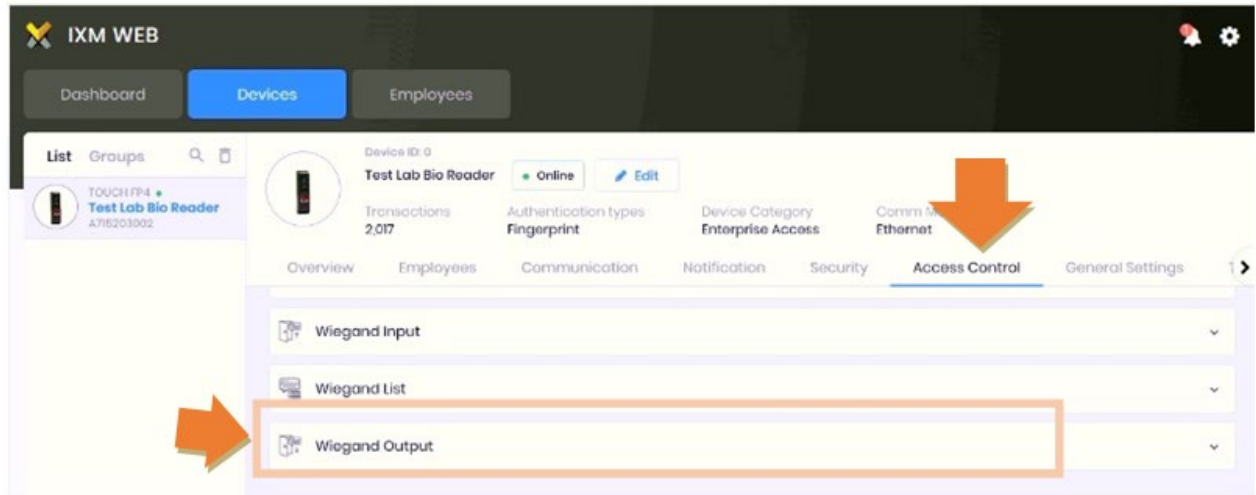
11. The Firmware Upgrade windows will display “Online” and “Firmware upgraded” when finished. Now you need to configure your reader for Access Control options in the Devices screen.



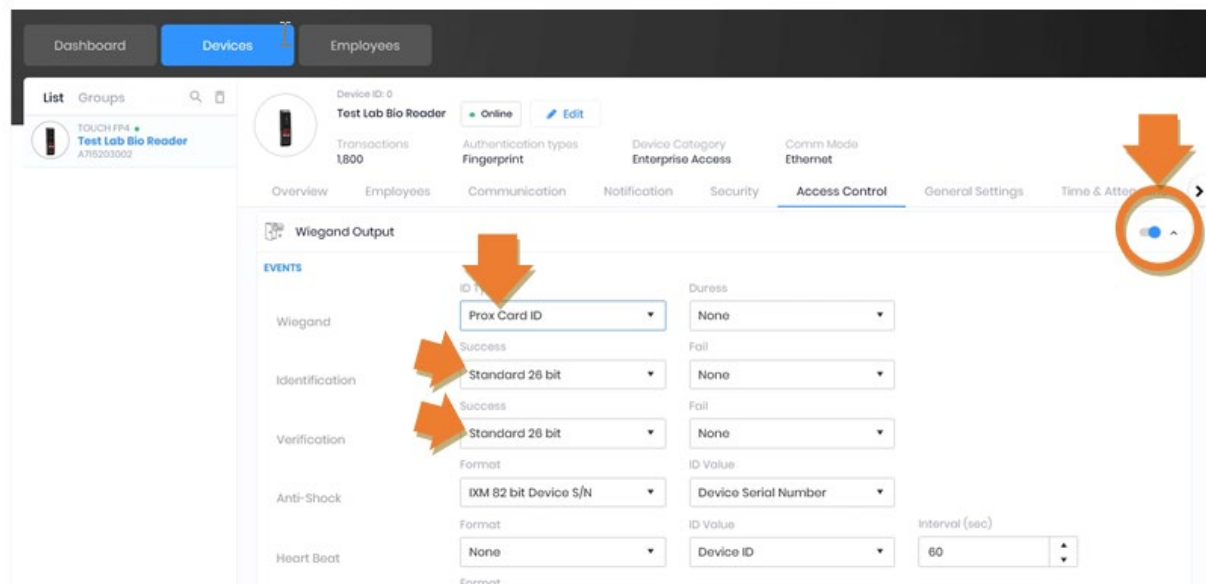
## CONFIGURE READER FOR ACCESS CONTROL

This topic covers setting the reader up for access control.

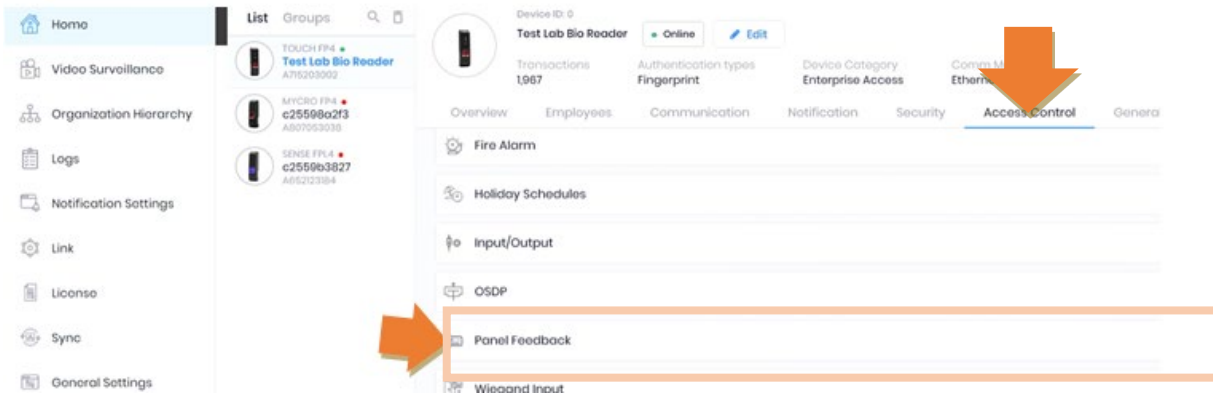
1. Click the **DEVICES** button on top of the Home screen and select the desired reader.
2. Click the **Access Control** menu option (middle of the screen).
3. Click on the **Wiegand Output** option (accordion option) to expand the Wiegand output configuration.



4. Turn **ON** the Wiegand Output by clicking the blue switch on top right side of the option bar.
5. Select **Prox Card ID** for the ID Type.
6. The Identification and Verification fields should be set to “**Standard 26 bit**” (or your appropriate format).
7. Click **Apply** and **OK** to save your changes.



8. Click on the **Panel Feedback** option (accordion option) to expand the Panel Feedback configuration.

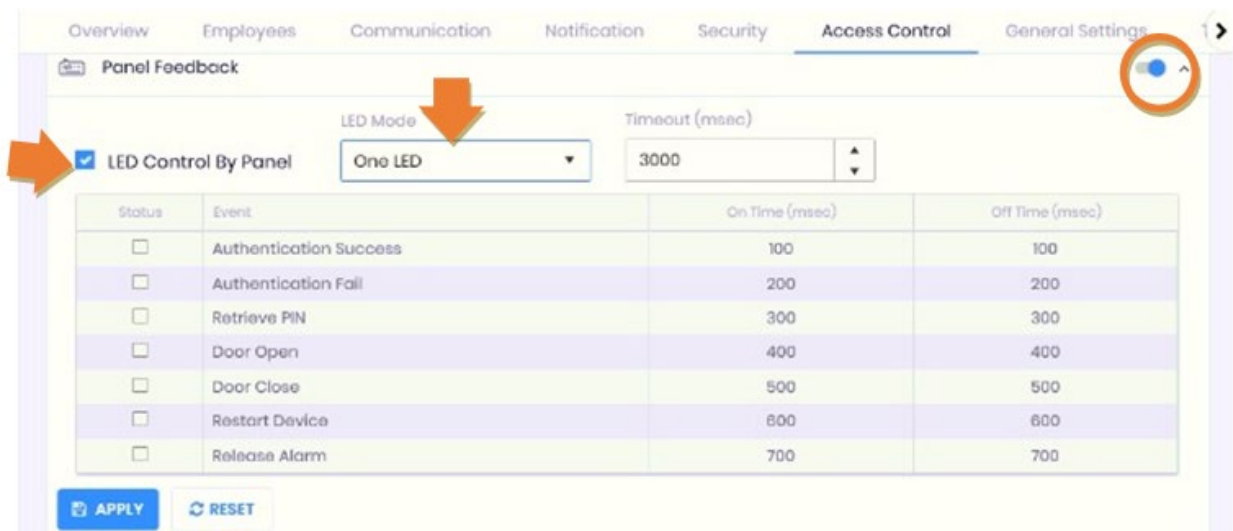


9. Turn **ON** the Panel Feedback by clicking the blue toggle switch in the upper corner of the area.

10. Check (enable) the **LED Control By Panel** option.

11. Set the LED Mode to **One LED**.

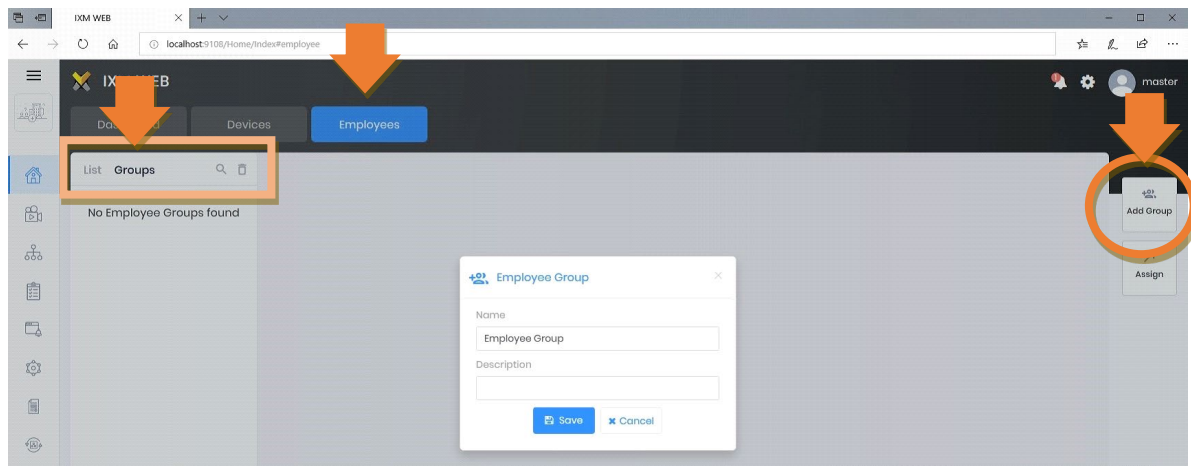
12. Click **Apply** and OK to save your changes.



## CREATING AN EMPLOYEE GROUP

You must have at least one Employee Group to enroll cards into the IXM Web software.

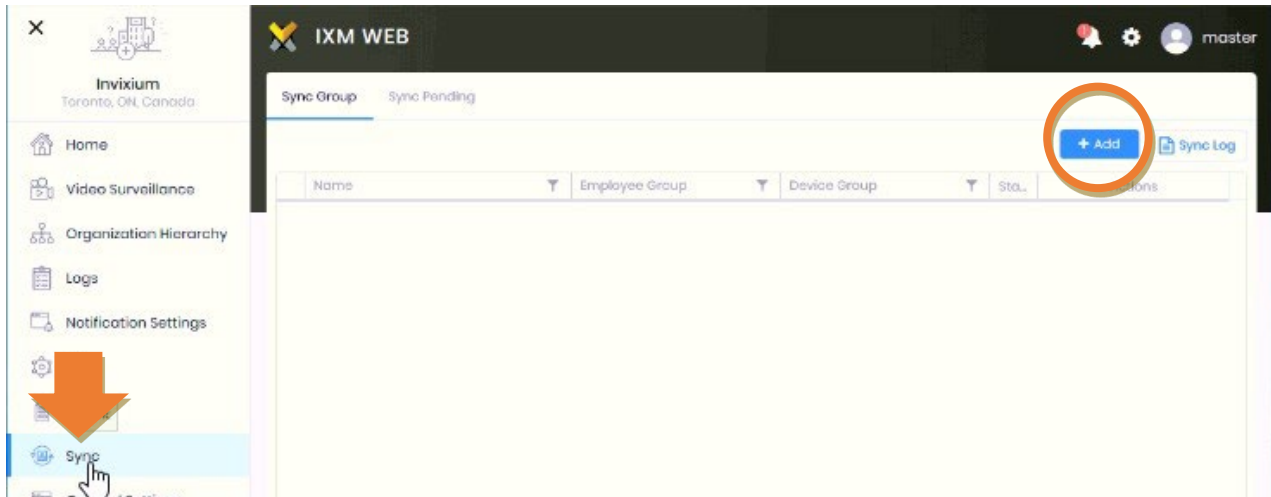
1. From the Home screen, click the **Employees** button.
2. Click the Groups tab option and then click the **Add Group** tile on right side tile-bar.
3. Enter a **name** for the Employee Group.
4. Click **Save** and OK to close the confirmation message that indicates the group was created.



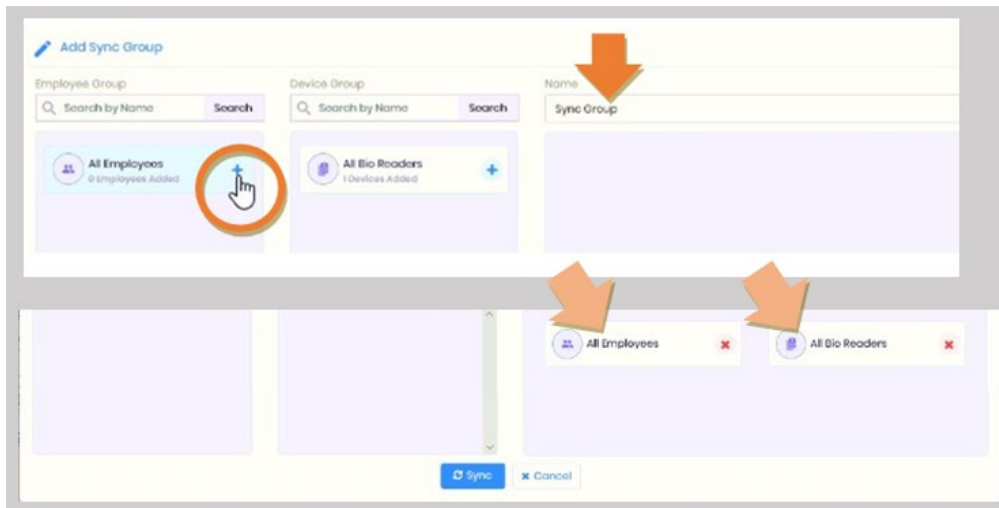
## CREATE A SYNC GROUP

You must create a **Sync Group** to link the Employee Group with a Device Group. The Sync Group is responsible for pushing finger templates into the readers. Keep Group mapping as simple as process

1. From the Home screen, click the **Sync menu** option (on the left-hand menu).
2. In the Sync Group screen, click **[+ Add]** button to open the *Add Sync Group* screen.



3. Enter a **Name** for your group in the Name field.
4. Click the **+** symbol on the *Employee Group* to move it to the Sync Group list
5. Click the **+** symbol on the *Device Group* to move it to the new Sync Group.
6. Both groups are moved to the Sync column.



7. Click **Sync** button then click OK when the sync process is finished.
8. The **Sync Group** will be added to the *Sync Group* screen with a green-checked status. *The actions column has buttons that you can click to sync the group again if you need.*

Note: when you enroll fingers in System Galaxy, you must apply the Employee Group to your credentials. The Sync Group will push your fingers to the appropriate readers based on the mapping in this screen.

# Enrolling Cardholders in System Galaxy

This section covers the two-part process of enrolling fingers in System Galaxy.

## CARDHOLDER ENROLLMENT STIPULATIONS

- DO NOT enroll users from the Invixium side. Use SG Cardholder screen.
- IXM Web only supports one biometric credential per user. Therefore, SG can only enroll one set of biometric credentials on a Cardholder, which will create the user in IXM WEB. SG can support other non-biometric credentials on the same cardholder record.
- The biometric credential must be “Card-1” on the cardholder record.
- You must pre-enroll the cardholder and card data, along with the desired loop and access permissions in the *SG Cardholder screen*. You must APPLY or save the record before the [Launch IXM WEB] button unlocks.
- After the cardholder and card are saved in SG, you must reopen/edit the record and Launch IXM to enroll fingers:
- (IXM-WEB) After the finger is saved in the IXM Enrollment Module you must assign an Employee Group to the credential. This allows the credentials to be pushed to the readers.
- Common ID will auto populate when you save the cardholder record.

## PRE-ENROLLING A NEW ACCESS CARD

You can use a pre-existing cardholder/card record provided you meet the required settings in this list of steps.

NOTE: The Common ID is a system-assigned value that is assigned when the cardholder record is saved (applied).

1. Click **Add New** button to open a blank screen.
2. Enter the **Last Name\*** and the **First Name\***
3. Select the **Card Technology\*** (26-Bit Wiegand or Corporate 1000, etc. )
4. Enter the **Card ID\*** and **FAC\*** code.
5. Assign a **Loop privileges\*** to the card.
6. Assign an **Access Group\*** to the card.
7. Configure any other settings as desired (i.e. card expiration or activation date, personal data, etc.)
8. Click **APPLY** to save the cardholder. Wait 30 seconds before proceeding with the biometric enrollment.

\* Fields with asterisks are mandatory for the pre-enrollment to unlock the Launch button.

The screenshot shows the 'SG Cardholder' interface. At the top, there's a dropdown menu with 'SG Inserted, Test Card' and buttons for 'Find Record', 'Add New' (highlighted with an orange arrow), 'Edit', 'Delete', 'Apply', and 'Cancel'. Below this are tabs: 'Personal', 'Card/Badge Settings', 'Data Fields 1', 'Data Fields 2', 'Photo Badging', 'Alarm Panel User / LCD Message', and 'Notes'. The 'Personal' tab is active. It contains fields for 'Record ID', 'Common ID' (with value '19'), 'Record Type', 'Last Name' (with value 'SG Inserted'), 'First Name' (with value 'Test Card'), and 'Middle Name'. To the right, there's a 'Select Card' dropdown with 'Card 1' selected, and buttons for 'Add New', 'Delete', and 'Add/Delete T/A Punches'. Below this are sections for 'Card Data' (including 'Card Description' with 'Card 1', 'Card Technology' with '26 Bit Wiegand', 'Facility Code' with '96', 'ID Code' with '1919', 'PIN / Card Role' with '01234' and 'Access Control'), 'Card Options' (with checkboxes for 'Card Disabled', 'Card Reversed', 'PIN Exempt', 'Duress Enabled', 'Passback Exempt', 'Active Date' with '11/14/2017', and 'Expire Date' with 'No Expiration'), and 'Loop/Cluster Settings' (with 'Authorized Loops' set to 'IXM Web Test', 'Access Profile', and 'Select Access Groups' with 'UNLIMITED ACCESS').

## ENROLLING BIOMETRIC CREDENTIALS IN SYSTEM GALAXY

This topic covers enrolling biometric credentials on an existing Cardholder/Card in SG.

- IXM only supports one credential per User and the biometric credential must be on Card-1 in SG.
- You must have pre-enrolled the Cardholder credential on Card-1. See prior section.
- After the biometric enrollment is completed you will need to save the SG Cardholder record again.

### Quick Enroll for Biometric-Only Credentials

Open the Cardholder Screen from the Configure menu or from the Toolbar.

1. Select the desired **Cardholder** (User) in SG.
2. Click **EDIT button** to open the screen
3. the [Launch IXM WEB] enrollment button should be unlocked.

If the Launch button is not unlocked, make sure to satisfy any field that is mandatory. Save and Reopen the Cardholder to continue. Once all fields are satisfied, then wait 30 seconds and retry.

4. Click [ **Launch IXM WEB button** ] to open the IXM Web Enrollment Module.  
If you are prompted to sign in to Invixium.

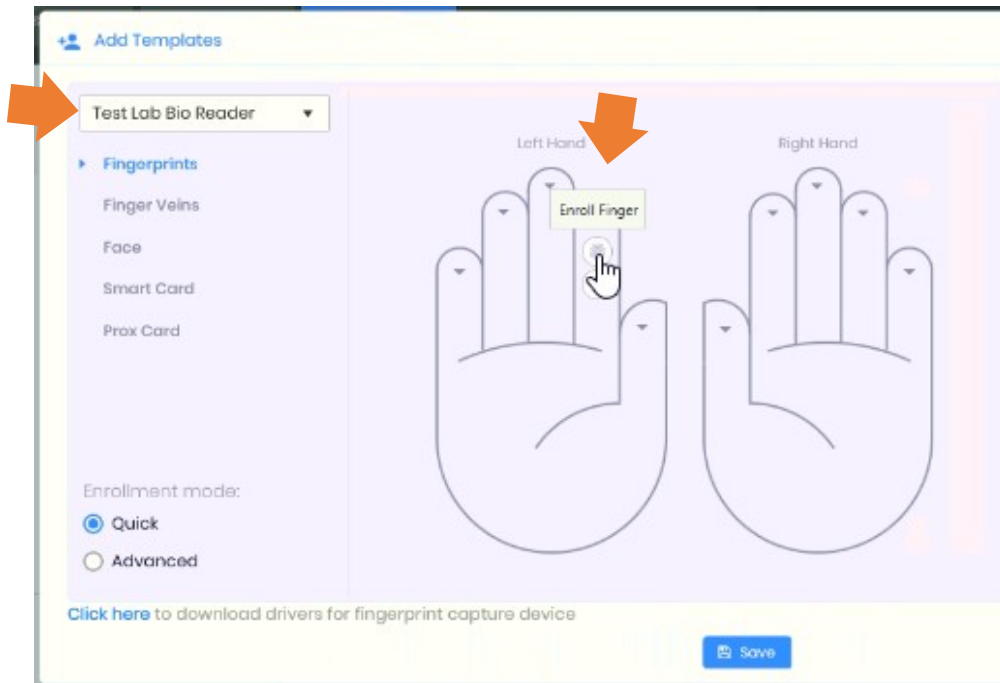
If the Invixium Dashboard opens but the finger capture screen never opens, then close all the Invixium web pages and click the [ Launch IXM Web ] button and SG again.

The screenshot shows the 'Cardholder Edit' screen in System Galaxy. The top navigation bar includes 'Wallas, Mark', 'Find Record', 'Add New', 'Edit', 'Delete', 'Apply', and 'Cancel'. The main content area is divided into several sections: 'Personal' (Record ID: 1, Common ID: 1, Record Type: dropdown, Last Name: Wallas, First Name: Mark, Middle Name: dropdown, Customer: \*\* NO CUSTOMER \*\*, Phone: dropdown, Department: dropdown), 'Card/Badge Settings' (Select Card: Card 1, Card Data: Card Description: Card 1, Card Technology: 26 Bit Wiegand, Facility Code: 96, ID Code: 704, PIN / Card Role: Access Control, Card Options: Card Disabled, Card Reversed, PIN Exempt, Duress Enabled, Passback Exempt, Active Date: 2/13/2018, Expire Date: No Expiration), 'Fingerprint Data' (Launch IXM Web button, highlighted with an orange arrow), 'Badge Settings' (Badge Design: dropdown, Print Limit: 0, Print Count: 0), and 'Loop/Cluster Settings' (Authorized Loops: 635, Access Profile: dropdown, Select Access Groups: \*\* UNLIMITED ACCESS \*\*, \*\* NO ACCESS GROUP \*\*, \*\* NO ACCESS GROUP \*\*, \*\* NO ACCESS GROUP \*\*).



When the *Add Templates* window opens (capture screen), you will see two hands.  
(The two hands represent the user's right and left hand. Go by the labels on the top of the hands, not on whether you think they look like LEFT/RIGHT vs RIGHT/LEFT. )

5. Choose the enrollment reader from the droplist (top left corner).
6. Hover your *mouse pointer* over the finger you want to enroll.
7. Click on the fingerprint icon (circle hotspot) for the same hand and finger that the user will enroll.

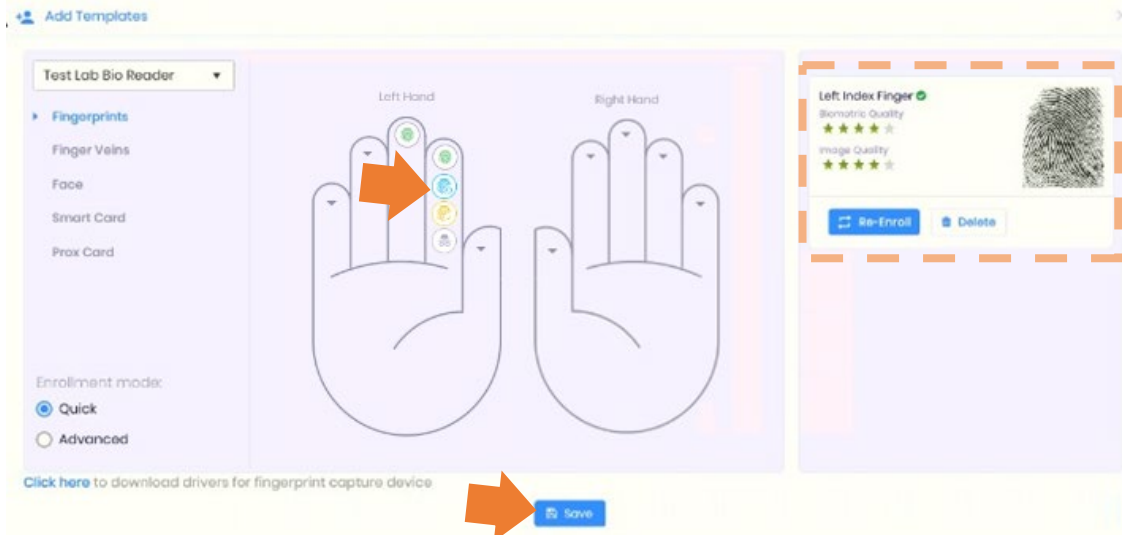


8. When you see the **Place Finger** prompt, the enrollment sensor will light up and the user can place their finger on the sensor.



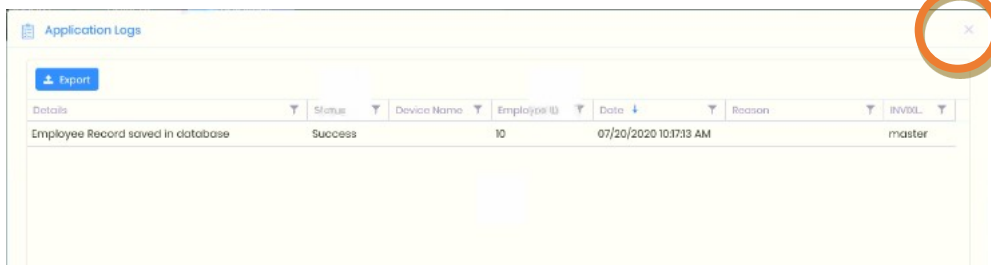


9. When the finger is captured it will display in a tile on the right side of the window. You have the option to VERIFY, RE-ENROLL, or Delete the finger as needed.



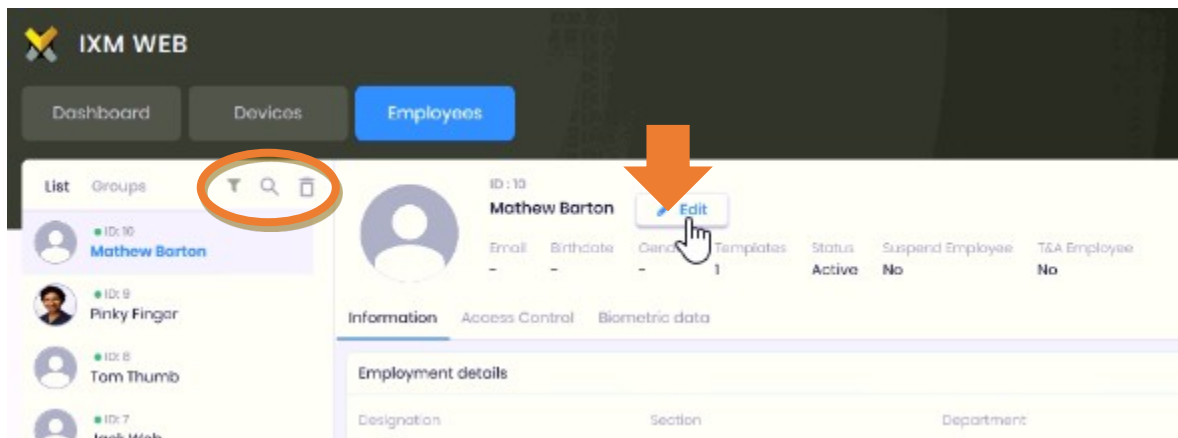
10. Click the **Save** button when you are finished enrolling (the Application Logs screen will open).

11. **Close [X]** the Application Logs screen .

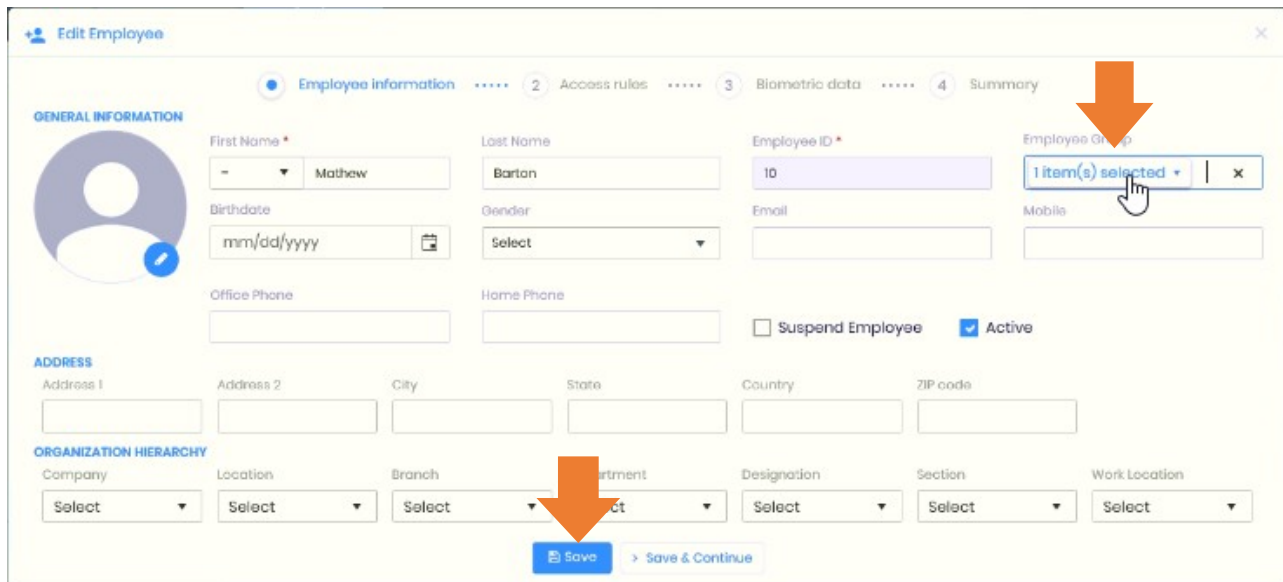


12. You should see the **Employees screen** in IXM-WEB page (browser).

13. Click the **EDIT** button on your employee record in the IXM window, it should be the top record. You can use the Search function to find your record as necessary.



14. Assign an **Employee Group** to the record.
15. Click **SAVE** and close out of the application log window again.
16. Close IXM if you are finished enrolling users.

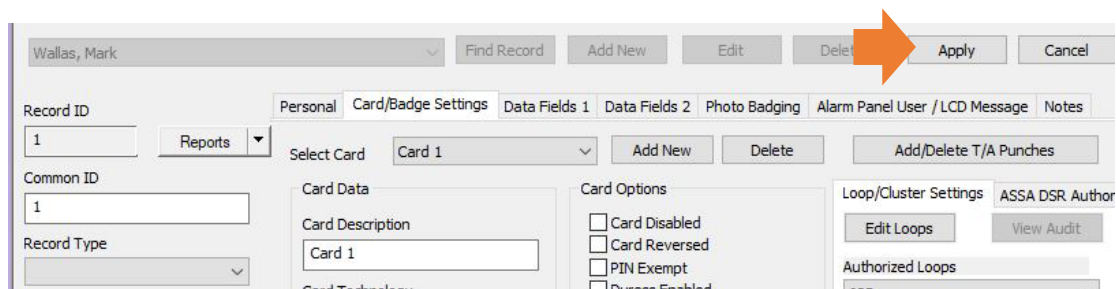


The screenshot shows the 'Edit Employee' form with the following sections and fields:

- GENERAL INFORMATION**
  - First Name: Mathew
  - Last Name: Barton
  - Employee ID: 10
  - Employee Group: 1 item(s) selected (indicated by an orange arrow pointing to the dropdown)
  - Birthdate: mm/dd/yyyy
  - Gender: Select
  - Email:
  - Mobile:
  - Office Phone:
  - Home Phone:
  - ☐ Suspend Employee ☒ Active
- ADDRESS**
  - Address 1:
  - Address 2:
  - City:
  - State:
  - Country:
  - ZIP code:
- ORGANIZATION HIERARCHY**
  - Company: Select
  - Location: Select
  - Branch: Select
  - Department: Select
  - Designation: Select
  - Section: Select
  - Work Location: Select

At the bottom, there are two buttons: **Save** (indicated by an orange arrow) and **Save & Continue**.

17. Also you must click **Apply** in the **SG Cardholder** screen to save changes there too.



The screenshot shows the 'SG Cardholder' screen with the following elements:

- Search bar: Wallas, Mark
- Buttons: Find Record, Add New, Edit, Delete, **Apply** (indicated by an orange arrow), Cancel
- Tabs: Personal, Card/Badge Settings, Data Fields 1, Data Fields 2, Photo Badging, Alarm Panel User / LCD Message, Notes
- Record ID: 1
- Common ID: 1
- Record Type:
- Select Card: Card 1
- Card Data: Card Description: Card 1
- Card Options:
  - ☐ Card Disabled
  - ☐ Card Reversed
  - ☐ PIN Exempt
  - ☐ Purse Enabled
- Loop/Cluster Settings:
  - ASSA DSR Author
  - Edit Loops
  - View Audit
- Authorized Loops:

# Appendixes

## INVIXIUM READER INSTALL REQUIREMENTS:

- Always use the *Invixium Wiring Diagram* that is shipped with the reader for correct connector/pin position and correct wire color. *Wiring specs may differ from reader to reader, even within the same model/version.*
  - IXM Readers must be powered with a separate power supply (i.e. do not power from the DRM board). Optionally, the Invixium readers are designed to use Power over Ethernet (PoE) via the LAN.
  - The Reader must be connected to the Ethernet/LAN before you can add it to IXM-WEB software.
- The IXM-WEB software will auto-discover the reader, as long as it is on the same network segment.
- If the reader is on a separate network segment, you must manually configure the static or reserved IP address into the reader from the reader keypad.
- The factory default passcode is “0000” unless it has been changed in the field. Consult *Reader Documentation* as needed. [Also see instructions this guide for details.](#)
- [See instructions in this guide for](#) verifying and upgrading reader firmware from the IXM-WEB software.
- [See instructions in this guide for](#) setting IXM Reader ‘Voice Command’ to “follow panel decision” from IXM-WEB.
- [See instructions in this guide for](#) setting LED behavior in the LED Options tab of the Loop/Cluster Properties screen in the System Galaxy software.
- [See instructions in this guide for](#) syncing readers with biometric data from the IXM-WEB software.

## Invixium Biometric IXM Reader - Cable Specs & Wiring Pinout

- 3-conductor, 22 AWG, overall shielded; non-stranded; max cable distance is 500 feet.
- 2-conductor, 18 AWG for at +12vdc for 500 feet distance. Reader draws 1A at 12v .
- Cat-5e Ethernet cable for TCP/IP communication back to the server; max cable distance 300 feet.
- Separate power supply required (current draw is 1A). Must common reader's p.s. ground to controller p.s. ground.
- Ground the drain-wire at one end only - land drain wire at the DRM Board (GND).
- Refer to reader manufacturer's instructions for wiring (manufacturer's specs may supersede Galaxy specs).
- 635-DRM Board (Dual Reader Module) – PN 20-0235-10
- 635-DRM LED is used to control reader's for Voice Command when configured for “Wait for Panel Decision”.

635-DRM Terminals (Function)		Invixium Reader
<b>LED</b>	(LED control line)	<b>ACP LED1</b> (used to control Voice Command)
<b>D 1</b>	(Data 1)	<b>W DATA_OUT1</b>
<b>VDC</b>	(do not use for reader power)	
<b>GND</b>	(common ground; drain wire)	<b>VIN – (GND)</b> (bond to controller GND)
<b>D 0</b>	(Data 0)	<b>W DATA_OUT0</b>
		<b>VIN + (VDC)</b> to separate power supply
		<b>VIN – (GND)</b> to separate power supply

### NOTES:

- The IXM Reader must be configured to “follow panel decision” in the IXM-WEB software in reader configuration screen.
- Galaxy controller must be set for Door Lock = Steady-High; Door Unlock = Steady-Low in the LED Options tab of the Loop/Cluster Properties screen.

## Full Integration Requirements Checklist

This checklist covers installation, license & registration/KEYS for software and readers, and system configuration, as well as enrollment requirements. *Requirements are grouped by relevant subject and listed in a top-down sequential order to help you check things in a logical process.* This checklist is good for troubleshooting and prepping for the installation as well as troubleshooting issues; however, this list is not intended to replace the act of following the instructions.

### Software Installation Requirements:

1. **SG 11.6.0 or higher** (see the [Galaxy online documentation](#) for the latest list of documents).
2. **IXM-WEB 2.2** (contact Customer Service if you have a different version).
3. You must install System Galaxy **before** IXM WEB App. And System Galaxy must be properly registered and configured for biometric support using with Invixium, with the number of IXM readers included in the total reader count. IXM readers are not included in Galaxy biometric reader count because they are licensed through the IXM software. See the [Verification of System](#) for the full steps of validating the setup.
4. You should be able to reach the localhost/swagger page as a verification that the API is correctly installed.
5. You must install IIS Server on the PC/Server that will host IXM-WEB **before** installing IXM WEB. You should be able to reach the localhost homepage as a verification check. Use the System to check that the IIS Server has the necessary options enabled. The Galaxy [IIS Install Helper utility](#) can be launched from the splash-screen of the Galaxy Install Media (USB/ISO).
6. (IXM) You must go to the Invixium Download Portal <https://ixmweb.invixium.com/Web/IXMWEB> and submit an Online Request Form. Invixium sends the **Download Link** and **Web Activation Key** to the email you provide. The download link allows you to download the installation executable for the IXM-WEB software. The Web Activation key is the license key for the web software. You cannot configure anything until this key is activated.
7. (IXM) The IXM-WEB installation file must be “run as administrator”.
8. If you want the SG Enrollment Operator to capture fingers without having to re-login each time, you need to check the option to “keep me logged in” during the database login. If for some reason you forgot or skipped this, you can go to IXM-Web Dashboard page and click the user profile icon in the upper-right corner of the screen and logout and then log back in to invoke the sign-in screen. There you can “check” (enable) the “keep signed in”.
9. (IXM) The reader *Link Activation Key* (for the number of readers you will connect to), will be requested during the IXM configuration process. A separate email will be sent with the *link activation key*. After the link activation key is installed and activated, you can add readers, upgrade firmware, configure readers, configure the follow panel decision, and also create Device Groups, Employee Groups, and map them in the Sync Group to manage the distribution of finger credentials to the appropriate readers.

### Database Install and Connection Requirements:

1. (Recommended) Install IXM WEB database on the GCSSQLEXPRESS instance.
2. (SG) you must choose **SQL Authentication** for database connections during Part-2 Galaxy Install and provide an SA login and password.
3. (IXM)in the IXM DB-Synch settings, during Invixium configuration, you must provide that SA login and password.
4. (IXM) You must set the DB Sync to downstream “SG to IXM” & configure the scan interval = 30s (default).

### Network and Services: the following services must be running (automatic start)

1. GCS Core Services (ClientGW, CommSvr, DBWriter, Event services).
2. GCS Web API Service must be configured for automatic start up.
3. IXM Web Service, IXM Device Discovery Service and the Bonjour Service must be running.
4. Port 9108 is the default port number for IXM-WEB.

### System Registration & System Settings:

1. (SG) System Registration must be registered for 'Biometric Support'.
2. (SG) "Total Reader Count" must include the IXM Readers since they are configured in SG as Wiegand readers.
3. (SG) "Biometric Reader Count" does not need to include IXM readers since they are registered via IXM WEB.
4. (SG) System Settings 'General Tab' must be configured to use "Invixium Biometrics" system. You must also provide the URL to the Invixium Web Server – which should be installed on your localhost ISS. Port 9108 is the default port. You must check the Invixium checkbox also if your version of SG has it.

### Browser Requirements:

1. MS-Edge can be used for installing and activating **Invixium Web License** and **IXM Link License**; and for performing system configuration, adding biometric readers, device groups, etc. A list of compatible browsers for IXM-WEB 2.2 is on Invixium's site at <https://www.invixium.com/web/> Scroll to bottom and click [+more] .
2. (IXM) Some versions of IXM required Internet Explorer (IE) to support the desktop USB finger capture device.
3. If you enroll from a wall-mounted IXM Reader, you may be able to enroll with a different brand of browser.

### Cardholder Enrollment Requirements ( part-1 - the initial cardholder creation ):

1. SG integration with IXM WEB does not support enrolling users from IXM. SG operator uses the IXM Web Enrollment Module which is launched from the SG Cardholder screen.
2. During enrollment process, the SG operator must assign the captured credential to an IXM Employee Group.
3. In the IXM-WEB, the Employee Group must be mapped to a valid Sync Group. This is how the enrolled fingers are pushed to the appropriate readers. The desired reader must be a member of the correlating Device Group that the Employee Group is mapped with in the Sync Group programming screen.
4. SG Operator must be pre-enroll/pre-save the cardholder and card data, along with the desired loop and access permissions in the SG Cardholder screen.
5. SG Operator certain fields must be satisfied when the Cardholder record is saved (apply) in Galaxy before the [Launch IXM WEB] button will unlock.
6. First and Last Name, Card ID, FAC/Co Code, Loop privilege, Access Permission must be configured The Common ID is a system-assigned value at the time the cardholder is saved.
7. card formats supported are 26-bit Wiegand or Corporate 1000, MIFARE, DESFire.
8. The biometric credentials must be captured on Card-1 in Galaxy to be able to work with IXM-WEB.  
**ONE BIOMETRIC CREDENTIAL PER USER (Invixium limitation)**  
**Notice:** Since Galaxy supports multiple credentials per user record (i.e. multiple cards per cardholder), this means that you can enroll additional **non-biometric cards** on the same cardholder but the biometric card must be card-1.  
**Notice:** IF a person needs *multiple biometric credentials*, you must create separate cardholder records for each biometric credential. **The biometric credential must always be on Card-1.**
9. After the initial cardholder record is saved (applied) in SG, you must reopen (edit) the record and click the Launch IXM button to begin enrolling fingers in the IXM Enrollment Module: Also see part-2 of cardholder enrollment requirements.

## Cardholder Enrollment Requirements ( part-2 - re-edit and begin enrolling fingers ):

1. After the initial cardholder / card record is saved (applied) in SG, you must reopen (edit) the same cardholder/card and click the [ **Launch IXM** ] button to open the **IXM Enrollment Module window ...** and begin enrolling fingers:
2. the IXM Enrollment Module will open in a browser window and allow the SG operator to choose which finger to enroll. And IXM-WEB Module will prompt the user to “present finger” to the capture sensor. If the browser does not render the enrollment window, be sure you close all pre-opened browser IXM windows and retry the launch.
3. (Best practice) You should capture at least 2 fingers on different hands. If one hand is injured, you will have an alternate finger to present.
4. After the fingers are captured, the finger data **must be saved in both systems**. If you skip saving the record in in the browser (Invixium), or skip saving it in the SG Cardholder window (apply button), then the fingers will need to be re-enrolled.
  - a) First you must add the **IXM Employee Group** before you can save the user/fingers in Invixium's screen.
  - b) Then you must save (apply) the credential in the Galaxy Cardholder screen.

## Glossary of Terms

This topic covers terminology used in this guide or that is pertinent to the integration.

TERM	DEFINITION
Access Control Panel (SG) (i.e. panel)	The galaxy access control panel where the access decision is made based on the access privileges assigned to the cardholder in SG. SG access control Panel does not manage the authentication rules or store biometric data.
Access Groups (SG)	The group container for access privileges to doors and schedules that is applied to Cardholders (users) in SG. (For the sake of clarity, this guide uses the term “access privileges” to refer to SG access rules because IXM uses the term “access rules” to mean the biometric “authentication type”. See the term “Authentication Type” Multifactor Authentication for more.)
Access Panel Feedback (IXM)	The settings that allow the reader to wait for panel decision before issuing the voice response of “access granted” or “access denied”. If panel feedback is not set up, the reader could respond “access granted” yet panel decision is denied. This can happen when the reader and the IXM System does not understand the access privileges applied to the credential in the panel.
Access Privileges (SG)	The access rules that SG applies to the Cardholder in the software and enforces at the ACP Panel. These are made of Loops, doors, access groups, and calendar days & time periods (schedules). Also see Loop Privileges and Access Groups Access Profiles.
Access Profile (SG)	A group container for up-to four (4) access groups.
Access Rules (IXM)	A field that must be correctly set in the IXM WEB Enrollment Module during biometric enrollment. This field is how the Operator sets the correct authentication type for the credential – i.e. Biometric Only, Card + Print, etc.
Activation (IXM WEB)	The activation of the license key for the IXM WEB Client Software.
Activation (IXM Link)	The activation of the license key for the IXM Readers.
Authentication, Multifactor (1:N)	Multifactor Authentication (1:N) means the User must present credentials that include <i>more than one method of authentication</i> to gain access. This typically means a biometric* factor plus one or more additional forms of identity (card, PIN, BioPIN, etc.) – common types are [biometric + card], or [biometric + PIN], or [biometric + card = PIN]. (* Biometric refers to a “finger” in this guide, but biometric could generically mean any form of physical trait a reader accepts, like iris, face, or even a BioPIN in lieu of a finger ).
Authentication, single-factor (1:1)	Single-factor Authentication (1:1) means a User must present <i>only one biometric credential as a method of authentication</i> to gain access. This typically means “finger only” where the card code is stored in the device, but a physical access card is not issued.
Authentication Type, biometric	This is an industry-wide term that refers to the type of authentication (single factor vs. multi-factor) and even specifically which multifactor is set – either at the reader and/or on the Cardholder (User) credential.
Cluster (Loop)	“Cluster” always refers to the 600/635-Series Panels, which are individually connect to the LAN (not a “422 loop”) and share the same Cluster ID. “Cluster” never refers to 500i-series, which does use a 422 loop. Sometimes people use the word “loop” as a <i>generic synonym</i> to indicate the group panels – also, some of the screens, tabs, or wizards may still generically use the term “loop settings”. A cl
Controller (SG)	Same thing as an access control panel.
Department (SG)	This is an optional administrative label to allow the Cardholders (users) to be related by department. This does not affect access but may affect reports.

DB Sync (IXM)	Refers to the database synchronization that is controlled by IXM, where the IXM WEB Client scans the Access Control database for new and updated user records. Also see Sync Interval.
GCS	(acronym) Galaxy Control Systems
IE (MS browser)	A Microsoft brand of Web Browser used by IXM WEB to operate the enrollment module.
Inixium	The tradename of the Inixium biometric system.
IIS (MS)	The Microsoft localhost web service.
IXM WEB	The name of the Inixium Client software.
IXM Readers	A suite of reader models that are compatible with IXM WEB. The ISM Biometric Readers can be used to capture fingers and encode cards* (*may depend on model numbers). The reader must be counted in the IXM Link Activation for Readers.
Loop (Cluster)	The loop or cluster of panels that are grouped together. Interchangeable term in generic sense. Cluster specifically refers to a Group 600/635-series Panels, whereas Loop can specifically refer to 500i-series RS-422 Loop.
Loop Privileges (SG)	A term that refers to assigning Loops or Clusters to a Cardholder in SG.
Reader Type (SG)	This setting means the <i>Type of Reader Technology</i> that is attached to the selected Section(Port) of the DRM(DPI) – such as a “Standard Wiegand Reader”, “HID Prox”, etc. This field is in the Reader Properties screen in SG and must be set to the appropriate value to match the attached reader technology.
Services, GCS Core	GCS ClientGW Service, GCS Communication Service, GCS Event Service, GCS DBWriter Service. All these are required to be running for the Client software to operate and communicate with Panels
Service, GCS Web	GCS Web API Service – Handles transmissions between IXM WEB and System Galaxy
Services, IXM Core	The services that IXM requires to be running for this integration. Bonjour service, IXM Discovery service, IXM Web Service.
SG	(acronym) System Galaxy
Sync Interval	The interval of time (seconds) that must elapse between each DB Sync.
USB Enrollment Device/Station	A biometric enrollment device that allows the SG Operator to enroll fingers on the cardholder record.