



# Feature Description Document

## Adding Employees from IXM WEB



## Purpose

This document outlines the process of adding employees from IXM WEB.

## Applies to

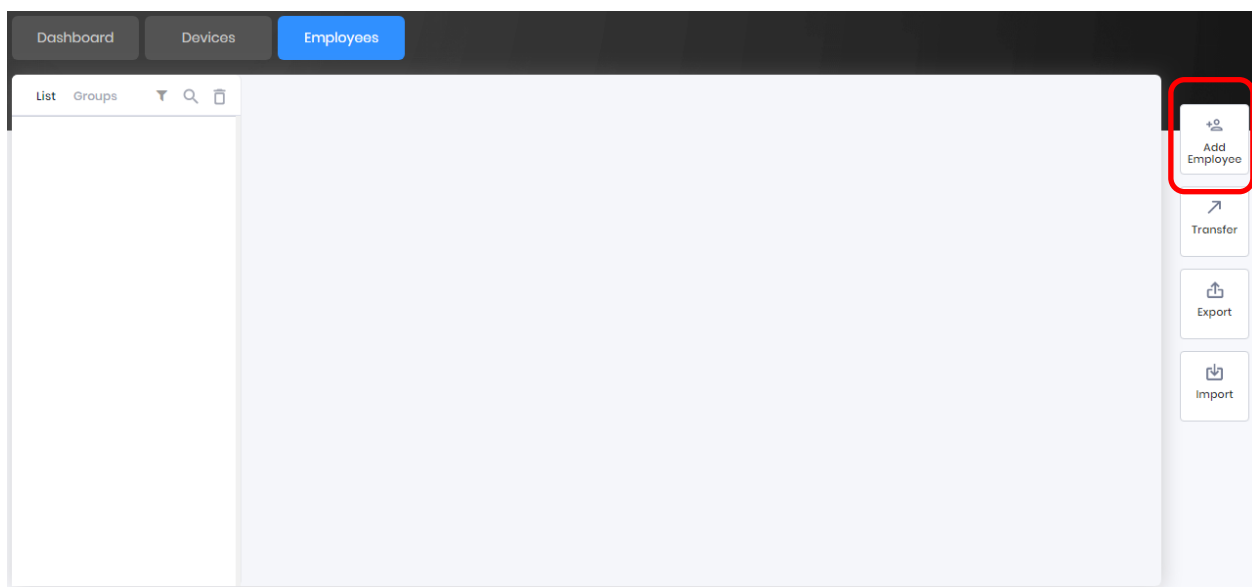
TITAN	TFACE	TOUCH 2	SENSE 2	MERGE 2	MYCRO
All Devices	All Devices	All Devices	All Devices	All Devices	All Devices

## Description

Adding employees is one of the initial and most important steps in IXM WEB.

## Add Employee

1. Click the **Employees** tab >> Click the **Add Employee** icon. The application will redirect you to the Add Employee window.



It has the following sections mentioned below.

1. Employee Information
2. Access Rules
3. Biometric Data Enrollment
4. IXM TIME (this tab will visible only if an IXM TIME license is purchased)
5. Summary



## Employee Information Section

The Employee information section is used to input personal information of employees/users such as Title, Gender, First Name, Last Name, Birth Date, and Employee ID. Among all these details First Name and User ID are mandatory fields. An administrator can input additional information about an employee/user like Address – 1, Address – 2, City, State, ZIP Code, Country, Home Phone, Office Phone, Mobile, Company, Location, Branch, Department, Designation, Section, and Email (all are optional fields).

After providing all the required details, click on **Save** to save details only in the IXM WEB database. Upon doing so, IXM WEB will display a success or failure message. Click **Save & Continue** to continue to the next section.



## Access Rules Section

The Access Rules section is used to define the access details of individuals.

- **Access Rule:** The device will authorize users based on the access rule applied to the user. If it is specified as “None”, then it will take device level authorization which is specified in Selected **Device >> General Settings >> Biometric** Section.
- **Access Schedule:** The device will authorize users based on the Access Schedule applied to the user. Access Schedule will be applied to the user if Access Schedule is enabled in **Device >> Access Control >> Access Schedule** Section.
- **Holidays:** If a holiday has been assigned for any Access Schedule, then this option decides whether it applies to the end-user or not.
- **1:1 Security:** 1:1 Security specifies the security level at the time of the verification process. Invixium recommends keeping it set to “Medium”.
- **1: N Security:** 1: N Security specifies the security level at the time of the identification process. Invixium recommends keeping it set to “Medium”.



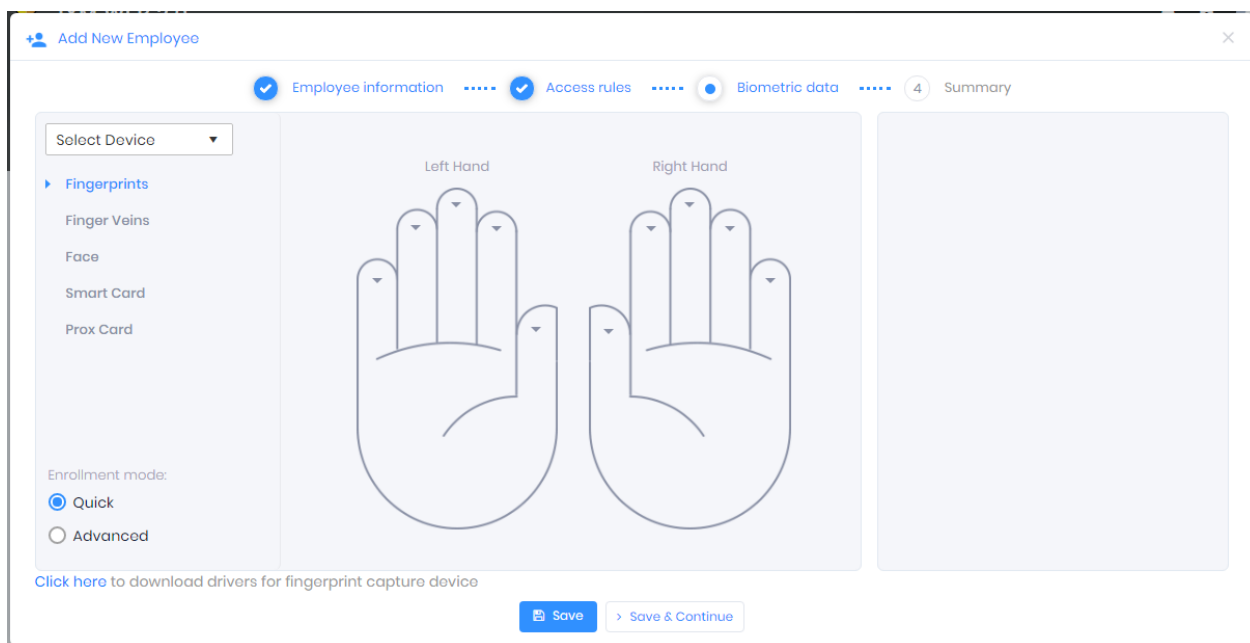
- **1:1 Face Security:** 1:1 Face Security specifies the security level at the time of the face verification process. Invixium recommends keeping it set to “Medium”.
- **1: N Face Security:** 1: N Face Security specifies the security level at the time of the face identification process. Invixium recommends keeping it set to “Medium”.
- **Open Time:** Device will keep the door open for the specified time (in seconds) after the authorization of a user on the device. If it is disabled at the time of enrollment, the device will consider the door open time that is specified in Individual **Device >> Access Control >> Door Open Time** Section.
- **Start Date and Time:** After this start date and time, the device will start authorizing the user on the device. If it is set to blank, then the device will not consider any start date and time for that user.
- **End Date and Time:** Till this end date and time, the device will authorize the user on the device. Once this date passes, the device will deny access to the user. If it is set to blank, then the device will not consider any end date and time for that user.
- **Suspend User:** If a user is suspended, then that user will not be able to get access via the device.
- **PIN:** The user needs to specify this PIN if the PIN access rule is set for the user.
- **User Type:** If a user requires access to the applications present on the LCD of TITAN, TOUCH 2, TFACE, or MERGE then the user needs to be specified as an “Administrator” user.
- **Anti-Passback:** If Anti-Passback needs to be applied to the user, then Anti-Passback settings need to be enabled. Anti-Passback will be applied to a user if Anti-Passback is enabled from **Device >> Access Control >> Anti-Passback** Section.

Click **Save & Continue** to continue to the next section.

## Biometric Data Enrollment Section

The Biometric Data section is used to capture the biometrics and access card information of individuals.

From this section, the administrator can enroll **Fingerprints**, **Finger Veins**, **Face**, **Smart Cards**, and **Prox Cards** for the selected individuals.




Click **Save & Continue** to continue, then IXM WEB will display the Summary section.

The summary section shows general information of individuals.



+ Add New Employee ×

Employee information     Access rules     Biometric data     Summary

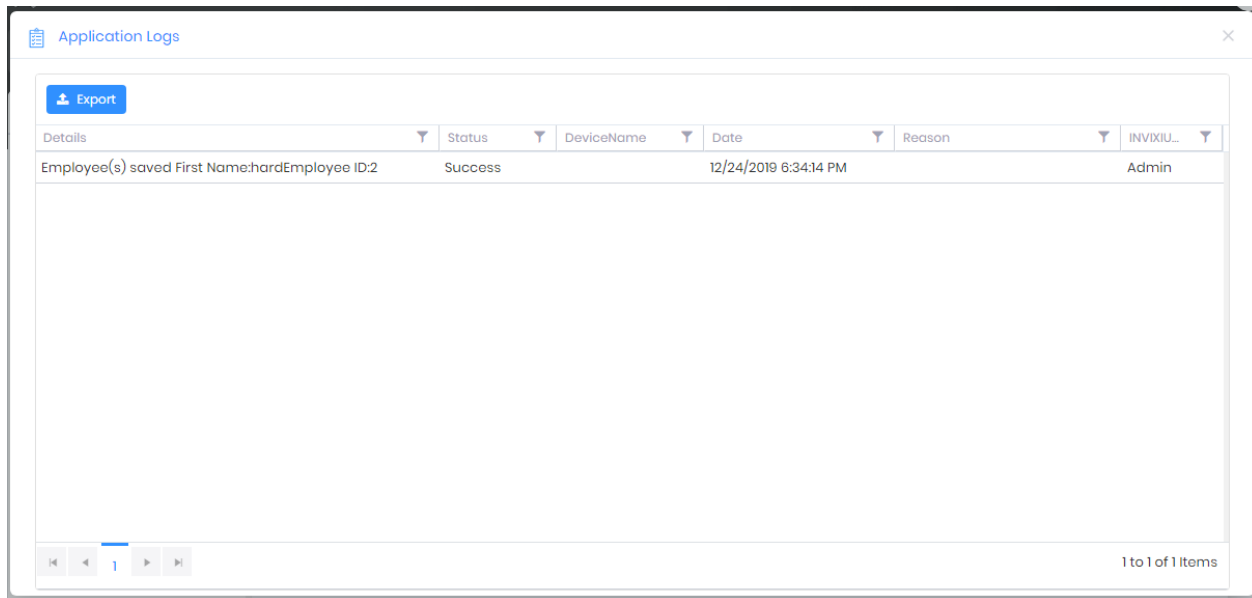
 Employee added

General Information	
Employee ID	Name
1	hardik





Click on **Add New** to add a new employee or click **Done** to complete the process and IXM WEB will display a success or failure message.



The screenshot shows a window titled "Application Logs" with a close button in the top right corner. Inside the window, there is an "Export" button with a download icon. Below the button is a table with the following columns: Details, Status, DeviceName, Date, Reason, and INVIXIU... The table contains one row of data: "Employee(s) saved First Name:hardEmployee ID:2", "Success", "12/24/2019 6:34:14 PM", and "Admin". At the bottom left of the table area are navigation icons (back, forward, first, last) and a page indicator showing "1". At the bottom right, it says "1 to 1 of 1 Items".

Details	Status	DeviceName	Date	Reason	INVIXIU...
Employee(s) saved First Name:hardEmployee ID:2	Success		12/24/2019 6:34:14 PM		Admin



## IXM TIME Section\* (Visible only if an IXM TIME License is purchased)

Upon clicking on the **Save & Continue** button, if an end-user does have an IXM TIME License, then IXM WEB will ask you to enter IXM TIME Data.

The IXM Time section is used to define attendance-related settings for individuals.

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

- SHIFT SETTINGS**
  - Schedule: Schedule1
  - Start Shift: SI
  - Holiday Group: IXM India
  - Leave Group: IXM Leave
  - Joining Date: 06/19/2019
  - Confirmation Date: mm/dd/yyyy
  - Attendance Policy: Default Policy
  - Late-IN Policy: Default Policy
  - Early-OUT Policy: Default Policy
  - Overtime Policy: Default Policy
  - Shift Based Access:
- IXM TIME CREDENTIALS**
  - Username: vhargunani@invixium.com
  - Password: \*\*\*\*\*
  - Reporting Group: QA

Buttons: Save, Save & Continue

- **Schedule:** Select and assign a Schedule to an employee from this field. The week off and pattern of shift will be defined based on the assigned schedule. A schedule can be created at **IXM TIME >> Shift Settings >> Schedule**.
- **Start Shift:** Select and assign a Shift to an employee from this field. Based on the Assigned shift and policies, attendance will be defined. Shifts can be created at **IXM TIME >> Shift Settings >> Shift**.
- **Holiday Group:** Select and assign a Holiday Group to an employee from this field. A holiday will be considered based on created holidays in selected groups. Holiday Groups can be created at **Home >> Company schedule >> Holiday Schedule**.
- **Leave Group:** Select and assign Leave Group to employees from this field. Applicable leave type will be decided based on the leaving group.
- **Joining Date and Confirmation Date:** Employment details.



**Attendance Policy:** Select and assign an attendance policy using this field. By default, “Default Policy” is assigned to an employee. Attendance of the day and leave transaction period are defined based on the assigned Attendance Policy and shift. Attendance Policy can be created at **IXM Time >> Policies >> Attendance.**

- **Late In Policy:** Select and assign a Late In policy using this field. By default, “Default Policy” is assigned to an employee. Late In time and duration are defined based on the assigned Late In Policy and shift. Late In Policies can be created at **IXM Time >> Policies >> Late In.**
- **Early Out Policy:** Select and assign an Early Out policy using this field. By default, “Default Policy” is assigned to an employee. Early Out time and duration are defined based on the assigned Early Out Policy. Early Out Policies can be created at **IXM Time >> Policies >> Early Out.**
- **Overtime Policy:** Select and assign an Overtime policy using this field. By default, “Default Policy” is assigned to an employee. The overtime of an individual will be calculated based on the assigned Overtime Policies and can be created at **IXM Time >> Policies >> Overtime Policy.**
- **Shift-Based Access:** By enabling it, the user will get access to the device based on allotted shifts.
- **IXM Time Credential (Username & Password):** IXM Time Credential is used to log in as an employee in IXM WEB to track individual records.
- **Reporting Group:** Selecting an individual reporting group allows the individual's reporting group manager to view employees' attendance, approve or reject attendance corrections, leave, and overtime for employees working under him.

Click **Save & Continue** to continue, IXM WEB will display the summary section.



## Support

For more information relating to this Feature Description document, please contact us at [support@invixium.com](mailto:support@invixium.com)

## Disclaimers 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 Inc. 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 Access Inc. All third-party trademarks referenced herein are recognized to be trademarks of their respective holders or manufacturers.

Copyright © 2022, INVIXIUM. All rights reserved.