



Feature Description Document

Access Control Information Settings



Purpose

This document outlines the process of configuring the Access Control Feature.

Applies to

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

Description

This specification will enable the users to specify their access rule through the Access Control Feature in the Add User or the Edit user option.



Access Control Feature

1. From Home >> Click the **Employees** tab on the top >> Click **Add Employee** on the right side of the window. Application will redirect to the Add New Employee window. The second step after adding Employee Information is the Access Control information.

The screenshot shows the 'Add New Employee' form at the 'Employee information' step. The progress bar at the top indicates five steps: 1. Employee information (active), 2. Access rules, 3. Biometric data, 4. IXM Time, and 5. Summary. The form is divided into several sections:

- GENERAL INFORMATION:** Includes fields for First Name, Last Name, Employee ID (with value 203), Employee Group (dropdown), Birthdate, Gender (dropdown), Email, Mobile, Office Phone, and Home Phone. There are checkboxes for 'Suspend Employee', 'Active', and 'T&A Employee'.
- ADDRESS:** Includes fields for Address 1, Address 2, City, State, Country, and ZIP code.
- ORGANIZATION HIERARCHY:** Includes dropdown menus for Company, Location, Branch, Department, Designation, and Section.

At the bottom, there are 'Save' and 'Save & Continue' buttons.

The screenshot shows the 'Add New Employee' form at the 'Access rules' step. The progress bar at the top indicates five steps: 1. Employee information, 2. Access rules (active), 3. Biometric data, 4. IXM Time, and 5. Summary. The form is divided into several sections:

- ACCESS DETAILS:** Includes dropdown menus for Access rules (None), Access Schedule (No Access), 1:1 Security (Medium), 1:N Security (Medium), 1:1 Face Security (Medium), and 1:N Face Security (Medium).
- EMPLOYMENT DETAILS:** Includes dropdown for Employee Type (Employee), and date pickers for PIN, Start Date, and End Date.
- ACCESS CONFIGURATION:** Includes checkboxes for 'Door Open Time', 'Anti-Passback', and 'Holidays' (checked).

At the bottom, there are 'Save' and 'Save & Continue' buttons.



2. Below is the complete list of information for Access Control settings:

a. **Access Rule:** Based on the access rule this device will provide access to the users. IXM WEB supports the following Access Rules:

- Biometrics Only
- Biometric + PIN
- Biometrics Only Strict
- Biometric + PIN Strict
- Card Only
- Card + Biometric
- Card + PIN
- Card + Biometric + PIN
- Card Only Strict
- Card + Biometric Strict
- Card + PIN Strict
- Card + Biometric + PIN Strict
- Card + Face
- Card + Face + Finger
- Card + Face + PIN
- Card + Face + Finger + PIN
- Card + Face Strict
- Card + Face + Finger Strict
- Card + Face + PIN Strict
- Card + Face + Finger + PIN Strict
- Face Only
- Face + Finger
- Face + PIN
- Face + Finger + PIN
- Face + Finger Strict
- Face + PIN Strict
- Face + Finger + PIN Strict
- ID Only
- ID + Biometric
- ID + PIN
- ID + Biometric + PIN
- ID Only Strict
- ID + Biometric Strict
- ID + Biometric + PIN Strict
- ID + Face
- ID + Face + Biometric
- ID + Face + PIN
- ID + Face + Biometric + PIN
- ID + Face Strict
- ID + Face + Biometric Strict
- ID + Face + PIN Strict
- ID + Face + Biometric + PIN Strict



- a. **Access Schedule:** Based on the Access Schedule, the device will decide the access of a user on a particular device. By default, IXM WEB will show “No Access” and “Full Access” for all IXM Devices. Newly created access schedules will be displayed in this section.
- b. **Holidays:** If enabled this assigns holiday(s) from the selected Access Schedule to the user.
- c. **1:1 Security:** It is used for verification purposes when a user tries to get access (using Card/ID); the device will decide based on the security level set.
- b. **1: N Security:** It is used for identification purposes when a user tries to get access (using Biometric); the device will decide based on the security level set.
- c. **1: 1 Face Security:** It is used for verification purposes when a user tries to get access (using Card/ID + Face); the device will decide based on the security level set.
- d. **1: N Face Security:** It is used for identification purposes when a user tries to get access using face; the device will decide based on the security level set.
- e. **Door Open Time:** It will overwrite the device level open time and the door will open for a given time after authorization of the user on the device.
- f. **Start Date:** It is used to specify the start date for accessing the device for the user.
- g. **End Date:** It is used to specify the end date for accessing the device for the user.
- h. **PIN:** This PIN will be used while authorizing the user on the device if a PIN related access rule is selected.
- i. **Employee Type:** Application user can specify employee types as a regular user or as an administrator. A regular employee will not be able to access IXM WEB but an administrator can access IXM WEB.



- j. **Anti-Passback:** Device-level Anti-Passback setting will be applied to a user only when this setting is ACTIVE.



Support

For more information relating to this Feature Description document, please contact us at support@invixium.com

Disclaimers and Restrictions

This document and the information described throughout are provided in its 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.