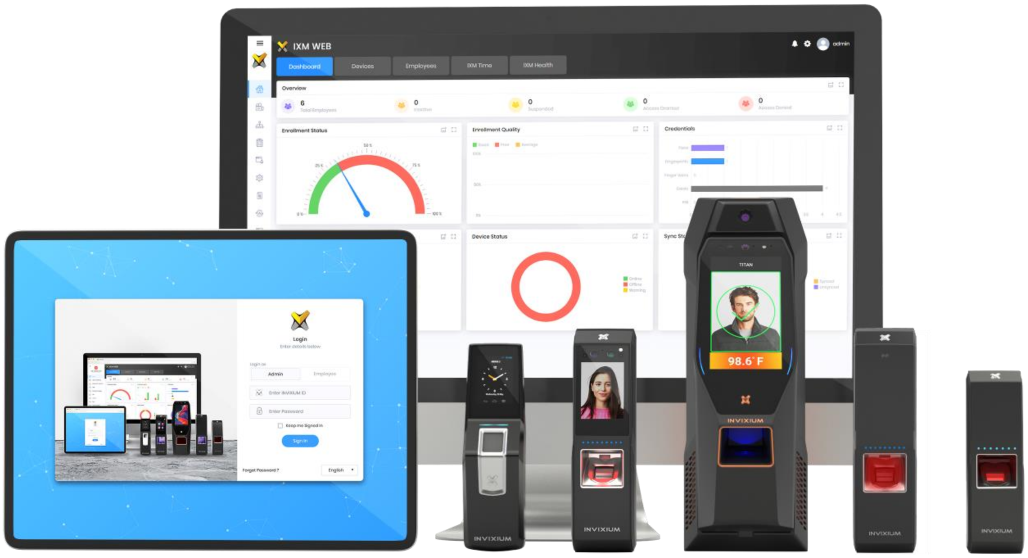


# Feature Description Document

## Understanding Multi-User Authentication Settings

## Purpose

This document outlines the process to configure the Multi-User Authentication settings 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

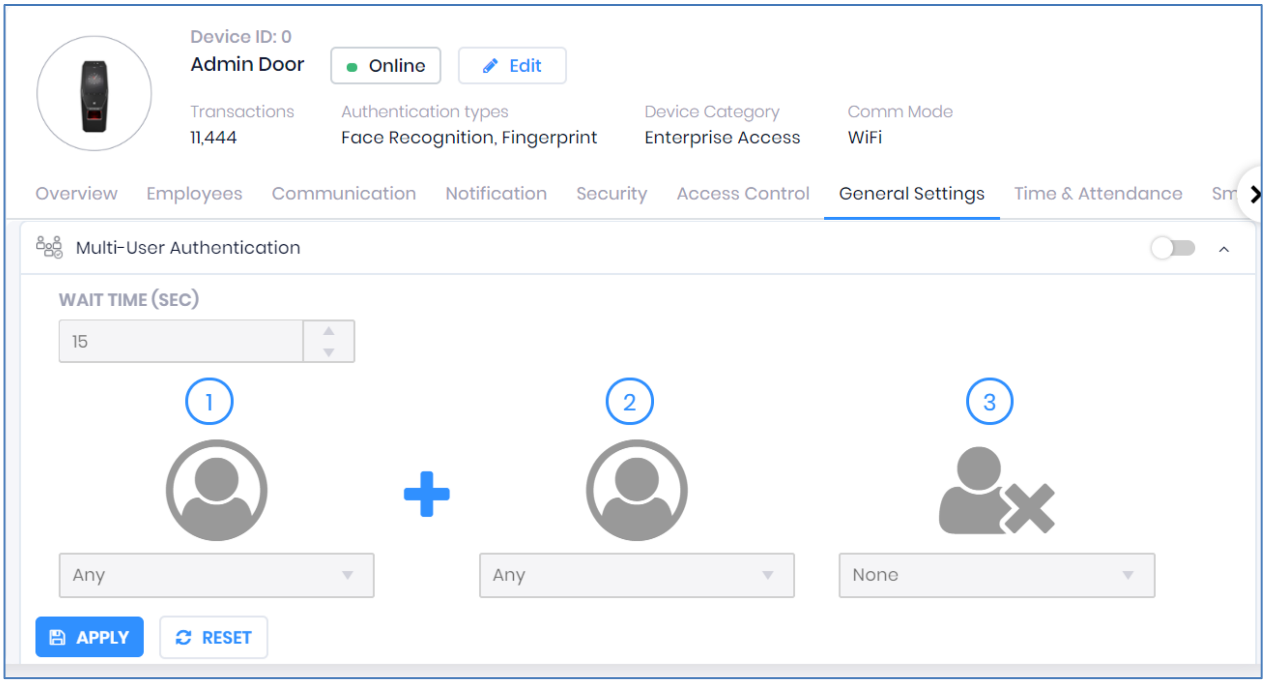
This specification will enable end-users to run the device in “Two-Man Rule” mode which is a control mechanism designed to achieve a high level of security, especially for critical materials or operations. The presence of two authorized persons is always required for all access and actions.

IXM Devices support a maximum of three authorizations to gain access, along with the following types of Multi-User Authentication:

1. **Any: –** Any user enrolled on the device can verify
2. **Employee: –** Specific employees can verify

## Configure Multi-User Authentication

1. Click the **Devices** tab >> Select **Device** >> Select **General Settings** navigation tab >> Expand **Multi-User Authentication** app.



Device ID: 0
Admin Door
● Online
Edit

Transactions
11,444

Authentication types
Face Recognition, Fingerprint

Device Category
Enterprise Access

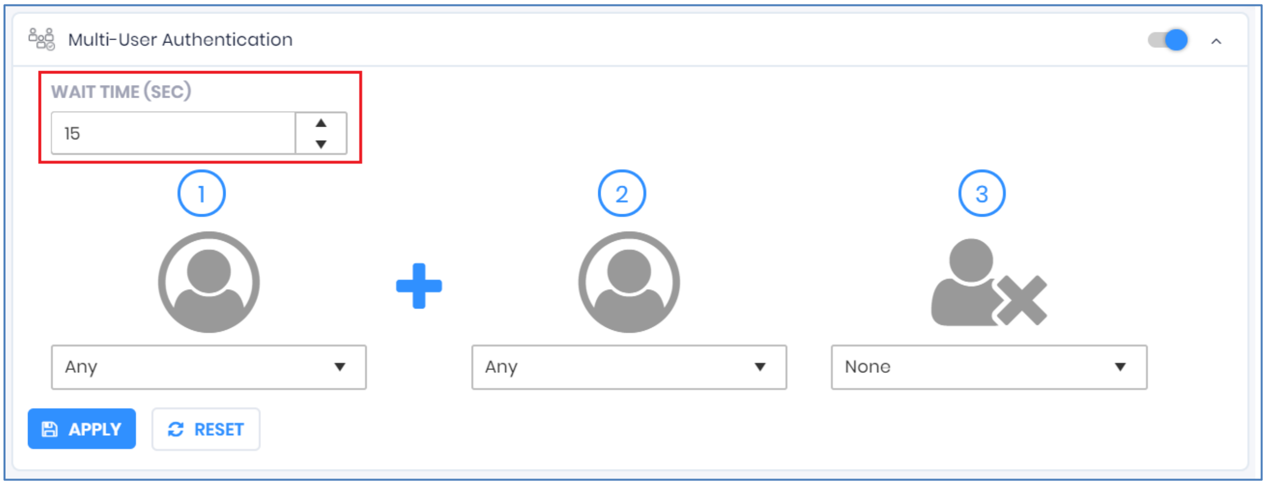
Comm Mode
WiFi

Multi-User Authentication

WAIT TIME (SEC)
15

1: Any
2: Any
3: None

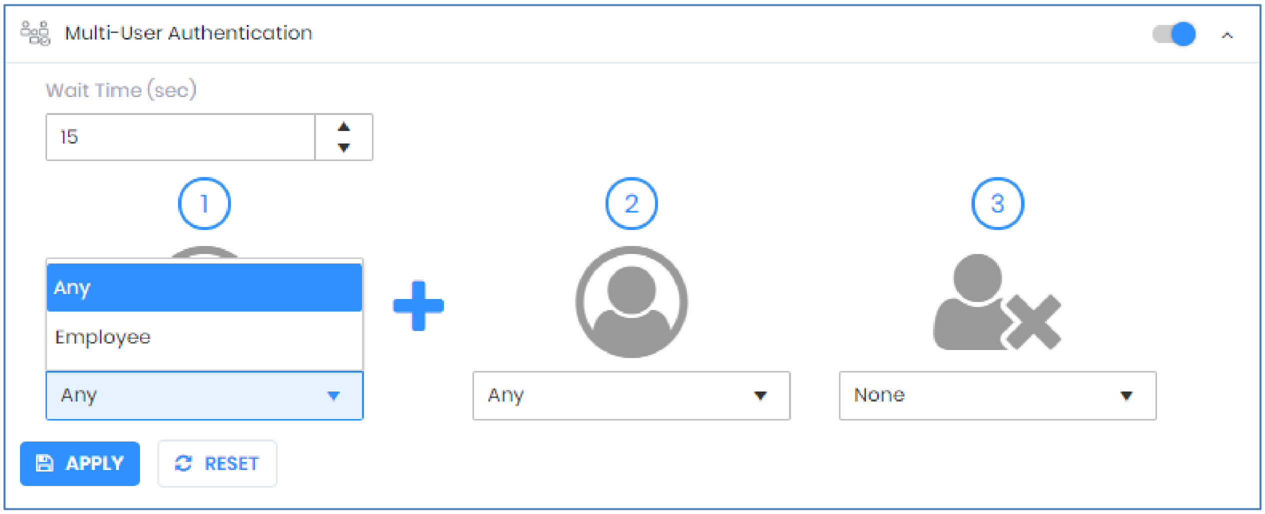
2. Toggle **ON** the Multi-User Authentication setting and enter the **“**Wait Time”, which indicates how much time the user will get between multiple-user authentication modes.



Multi-User Authentication

WAIT TIME (SEC): 15

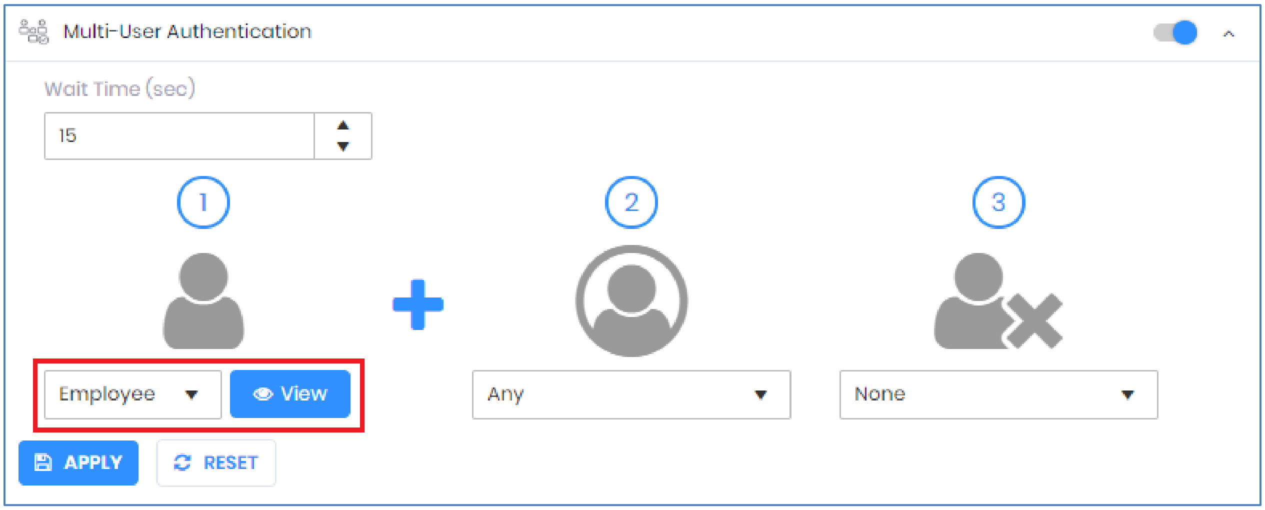
3. From the two options displayed “Any” and “Employee”, choose anyone.



Multi-User Authentication

Wait Time (sec): 15

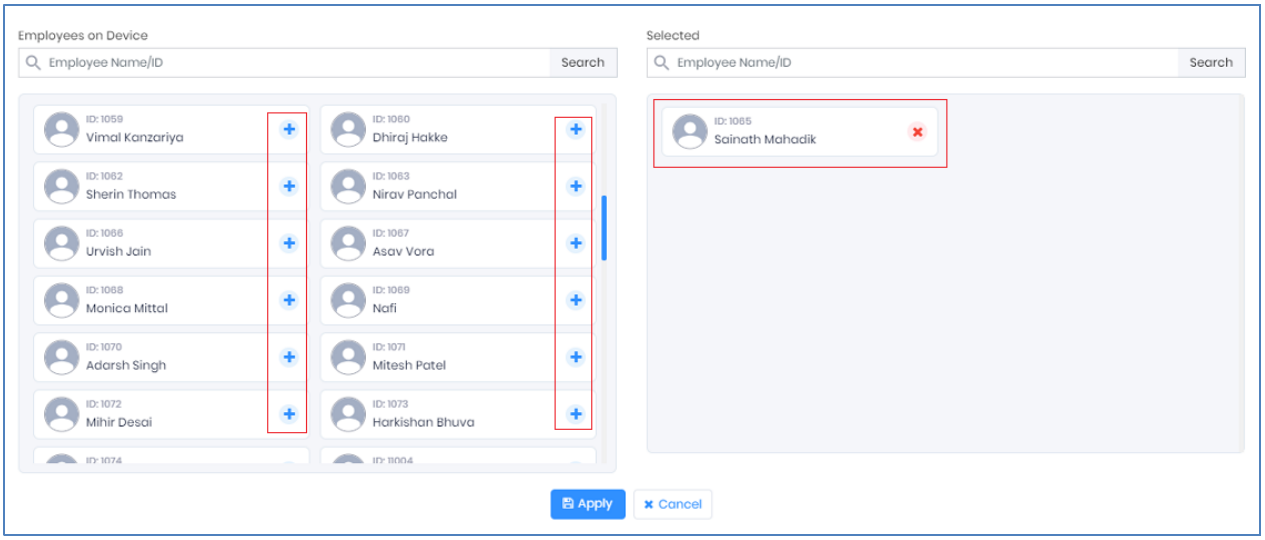
4. Upon selection, click on **View** and you will be able to see the employee list the employees which are synced to the device will be displayed.



Multi-User Authentication

Wait Time (sec): 15

5. Click on the + (add user), the user will be added for multi-user authentication on the device.



Employees on Device

- ID: 1059 Vimal Kanzariya
- ID: 1060 Dhiraj Hakke
- ID: 1062 Sherin Thomas
- ID: 1063 Nirav Panchal
- ID: 1066 Urvish Jain
- ID: 1067 Asav Vora
- ID: 1068 Monica Mittal
- ID: 1069 Nafi
- ID: 1070 Adarsh Singh
- ID: 1071 Mitesh Patel
- ID: 1072 Mihir Desai
- ID: 1073 Harkishan Bhuva
- ID: 1074
- ID: 11004

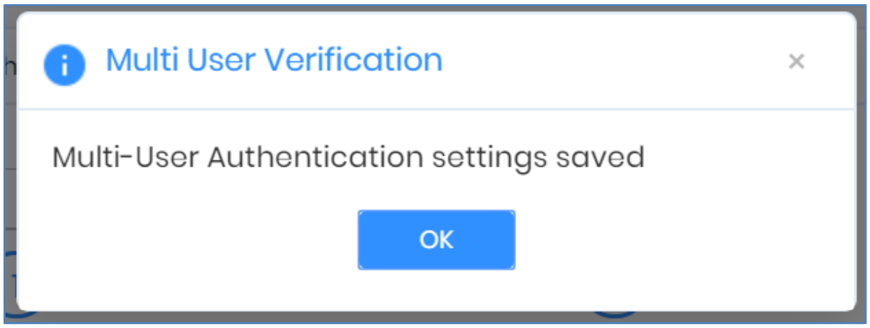
Selected

- ID: 1065 Sainath Mahadik

6. Follow the same steps for second employee authentication and make the required changes.

7. For a third user in Multi-User Authentication, by default, the option will be “None”. Select options like for the first two Multi-User Authentication modes. This selection box will remain disabled until the user selects any other option than “None”.

8. Upon process completion, click **Apply** and the settings will be saved to the IXM Device and a confirmation message will be displayed.



Multi User Verification

Multi-User Authentication settings saved

# FAQ

1. **Can both users use the same Employee ID for Multi-User Authentication?**
   No, if the user enters the same Employee ID, IXM WEB will consider it as a duplicate and a “Duplicate User ID” message will be displayed.

2. **What happens if the first and second authentications are done by the same user?**
   If the same user tries to authenticate both (first and second) times, then the IXM device will consider it as a “Duplicate User” irrespective of the settings applied for Multi-User Authentication.

3. **What are the minimum and maximum limits of Wait Time?**
   The minimum limit is 3 seconds and the maximum is 60 seconds.

## 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 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.