



# **Feature Description Document**

Understanding Biometric Configuration in IXM WEB



### **Purpose**

This document outlines the process of Biometric Configuration in IXM WEB.

### **Applies to**

TITAN	TFACE	TOUCH 2	SENSE 2	MERGE 2	MYCRO
All Devices					

### Description

Biometric Configuration is configured in IXM WEB's Biometric Settings. The following sections can be changed:

- Security Level Fingerprints.
- Device Mode.
- Access Rule.
- Security Settings.

Using these options, users can troubleshoot biometric issues and easily identify the current biometric configuration on the device.



## **Configure the Biometric setting from IXM WEB**

1. From Home >> Click the Devices tab on the top >> Select Device >> Click General Settings >> Biometric.

Biometric		^
SECURITY LEVEL FINGERPRINT Low Medium High Very High Moximum 1:1 Security	DEVICE MODE Device Type Identification	Time Out (sec)
Low Medium High Very High Maximum 1 : N Security	Biometric Access Biometric + Face + PIN D Access	Card Access Card + Biometrics Face Access
FACE Low Medium High Very High Maximum 1:1 Security Low Medium High Very High Maximum	ID + Face + Finger   SECURITY SETTINOS  Private Authentication Disable Biometric in Verificatio Disable PIN	Face Only       Disable Identification       On     Access Schedule in Duress
1: N Security		

- 2. The following are the sections of Biometric Configuration:
  - Security Level Fingerprints:
    - o 1:1 Security: 1:1 Security operates in Verification mode. Accuracy of user verification can be set to "Low", "Medium", "High", of "Very High". "Medium" is the default accuracy.
    - o 1:N Security: 1:N Security operates in Identification mode. Accuracy of user identification can be set to "Low", "Medium", "High", of "Very High".
       "Medium" is the default accuracy.

**NOTE:** When users will select a TIAN or TOUCH 2 Face device, Face Level Security options will also be available.

- Device Mode:
  - o **Verification:** This option enables card-only authentication.
    - To change the device mode, click on the device type and change the mode from Identification to Verification.

INVIXIUM



ECURITY	LEVEL				DEVICE MODE
INGERPRI	INT				Device Type Time Out (sec)
Low	Medium	High	Very High	Maximum	Identification To
		1:1Security			Acc Verification
	0				Identification Card Access
.ow	Medium	High	Very High	Maximum	Biometric + Face + PIN  Card + Biometrics
		1: N Security			
ACE	~				ID + Face + Finger   Face Only
ow	Medium	High	Very High	Maximum	SECURITY SETTINGS
		1:1Security			Private Authentication
					Disable Biometric in Verification
low	Medium	High	Very High	Maximum	Disable PIN
		1: N Security			

• After the changing device mode to verification, click **Apply**.





o **Identification:** In Identifiation mode, the device will use multiple authentication modes based on its model.

re, ponero	^
SECURITY LEVEL DEVICE MODE FINGERPRINT Device Type Time Out (sec) Low Medium High Very High Moximum	
1:1 Security     ACCESS RULE       Low     High       Very High     Moximum       1:N Security     ID Access   Card Access Card Access Card + Biometrics Card + Biometrics	
FACE     ID + Face + Finger     Face Only       Low     Medium     High     Very High       1:1Security     Private Authentication     Disable Identification	
Disable Biometric in Verification     Access Schedule in Dure     Low Medium High VeryHigh Maximum     Disable PIN     1: N Security	55

• **Time Out (Sec):** Edit the amount of time before authentication times out between 3 and 60 seconds. By default, authentication times out after 10 seconds.

Biometric				^
SECURITY LEVEL FINGERPRINT Low Med	um High VeryHigh 1:1Security um High VeryHigh	Maximum	DEVICE MODE Device Type Idontification  ACCESS RULE Biometric Access Card Access Biometric + Face + PIN Card + Biometrics	(3-60)Soc
FACE	1 : N Security	Maximum	ID Access Face Access D + Face + Finger    Face Only  SECURITY SETTINOS   Privato Authontication	▼ Disable Identification
Low Med	High Very High 1: N Security	Maximum	Disable Biometric in Verification     Disable PIN	Access Schedule in Duress



- Spoof Level (available only for Lumidigm Sensor supported devices):
   Users can set Spoof Level settings to prevent fake finger authentication.
   The following levels are available for Spoof Level settings:
  - Disable
  - Low
  - Medium
  - High
  - Very High

#### • Access Rule:

- o **Biometric Access Rule:** Users can alter the device's Biometric Access Rules. The default option is Biometric Only.
  - Biometric Only
  - Biometric + PIN (depends upon the device type)
  - Biometric + Face (available only for TITAN & TOUCH 2 Face)
  - Biometric + Face + PIN (available only for TITAN & TOUCH 2 Face)

SECURITY LEVEL		DEVICE MODE			
FINGERPRINT	1	Device Type	Time Out (sec)		
Low Medium High Very High	Maximum	Identification *	10	•	
1:1Security		ACCESS RULE			
		Biometric Access	Card Access		
Low Medium High Very High	Maximum	Biometric + Face + PIN 🔻	Card + Biometrics	•	
1:N Security		Biometric Only	Face Access		
FACE		Biometric + PIN	Face Only	•	
Low Medium High Very High	Mosimum	SED Biometric + Face			
L'ISecurity		Biometric + Face + PIN		Disable Identification	
		🔄 Disable Dismetrie in Verifie	ion	Access Schedule in Duress	
Low Medium High Very High	Maximum	Disable PIN			
1: N Security					



- Card Access: Users can select the device's Card Access Rule from one of the following. The default Card Access Rule is Card + Biometrics:
  - Card Only
  - Card + Biometrics
  - Card + PIN
  - Card + Biometric + PIN (depends upon device type)
  - Card + Face (available only for TITAN & TOUCH 2 Face)
  - Card + Face + Finger (available only for TITAN & TOUCH 2 Face)
  - Card + Face + PIN (available only for TITAN & TOUCH 2 Face)
  - Card + Face + Finger + PIN (available only for TITAN & TOUCH 2 Face)

[: Biometric		^
SECURITY LEVEL FINGERPRINT Low Medium High Very High Maximum	DEVICE MODE Device Type Identification	Time Out (sec)
1 : 1 Security Low Medium High Very High Maximum 1 : N Security	ACCESS RULE Biometric Access Biometric + Face + PIN • ID Access	Card Access Card + Biometrics Card Only
FACE Low Medium High VeryHigh Moximum 1:1Socurity	ID + Face + Finger       SECURITY SETTINGS       Private Authentication       Disable Biometric in Verification	Card + Biometrics Card + PIN Card + Biometrics + PIN Card + Biometrics + PIN Card + Face Schedule in Duress
Low Medium High VeryHigh Maximum 1:N Security	Disable PIN	Card + Face + Finger



- ID Access (available only for TITAN, TOUCH 2, and MERGE series devices): Users can select one of the following options from the device ID Access Rule. The default ID Access Rule is "ID Only":
  - ID Only
  - ID + Biometrics
  - ID + PIN
  - ID + Biometrics + Pin (depends upon device type)
  - ID + Face (available only for the TITAN & TOUCH 2 Face)
  - ID + Face + Finger (available only for the TITAN & TOUCH 2 Face)
  - ID + Face + PIN (available only for the TITAN & TOUCH 2 Face)
  - ID + Face + Finger + PIN (available only for the TITAN & TOUCH 2 Face)

[ Biometric	^
SECURITY LEVEL FINGERPRINT Law Medium High Very High Maximum	Device Type     Time Out (sec)       Identification     10
1:1Security Low Medium High VeryHigh Maximum 1:NSecurity	ACCESS RULE Biometric Access Biometric + Face + PIN Card Access Card Access Card Access Ence Access
FACE Low Medium High VeryHigh Maximum 1:1Security	ID + Face + Finger      ID + Face + Finger      ID - Plow Access      ID - Plow Acc
Low Medium High VeryHigh Maximum 1: N Security	ID + PIN ID + Biometrics + PIN ID + Face ID + Face + Finger



- Face Access (available only for TITAN, and TOUCH 2 Face devices): Users can select one of the following options for the device's Face Access Rule. The default Face Access Rule is "Face Only":
  - Face Only
  - Face + Finger
  - Face + PIN
  - Face + Finger + PIN

	A LEVEL RINT Medium	High	Very High	Maximum	DEVICE MODE Device Type Identification	Time Out (sec)
Low	Medium	1:1 Security High	l Very High	Maximum	ACCESS RULE Biometric Access Biometric + Face + PIN * ID Access	Card Access Card + Biometrics Face Access
Low	Medium	High 1:1Security	Very High	Maximum	ID + Face + Finger    SECURTY SETTINGS   Private Authentication	Face Only  Face Only Face + Finger Identification
Low	Medium	High	Very High	Maximum	<ul> <li>Disable Biometric in Verificat</li> <li>Disable PIN</li> </ul>	Face + PIN Schedule in Duress Face + Finger + PIN



### 3. Security Settings:

	Y LEVEL RINT Medium	l High	Very High	Maximum	Device Type     Time Out (sec)       Identification     10
Low	Medium	1:1Security High 1:NSecurity	Very High	Maximum	ACCESS RULE Biometric Access Biometric + Face + PIN  Card Access Card + Biometrics ID Access Face Access
Low	Medium	High	Very High	Maximum	ID + Face + Finger     Face Only       SECURITY SETTINGS       Private Authentication   Disable Identification
Low	Medium	High	Very High	Maximum	Disable Biometric in Verification     Disable PIN

 Private Authentication: Users can configure the Access Rule at User Level and Global (device) Level. Enabling Private Authentication means that user-based access rules will have priority during the authentication process. By disabling this setting, the Global Level access rule will overwrite the User Level access rule. This option is enabled by default.





• **Disable Identification:** If this setting is enabled, the device will not read its fingerprint sensor, e.g. if user authentication is selected as Card + Biometrics and this setting is turned on, the device will only read card authentication. By default, this option is disabled.



• **Disable Biometrics in Verification**: Biometric verification will be done only if this setting is "off". If biometrics are disabled, then during verification, the device will not ask for a finger. All other credentials will be asked as per the access rule set by the user. By default, this setting is disabled.



 Access Schedule in Duress: If an access schedule is applied on the device and a user authenticates with their pre-programmed duress credentials, access will be granted regardless of the access schedule. By default, the Access Schedule in Duress setting is disabled.

INVIXIUM

XAD-FDD-596-02G





- **Disable PIN:** It describes PIN status at the time of authentication. The PIN will be asked or bypassed as per the status set. If the PIN is disabled then during authentication, the device will not ask for the PIN. All other credentials will be asked as per the aces rule set for the user.
- 4. Once all the changes to the Biometric section have been made, click **Apply** to store all the changes on the device.





5. Click **RESET** to revert to default settings.

Biometric						^
SECURITY LEVEL FINGERPRINT Low Medium	High VeryHigh	Maximum	DEVICE MODE Device Type Identification • ACCESS RULE Biometric Access	Time Out (sec) 10 Card Access	×	
FACE	1:N Security	Moximum	Biometric + Face + PIN  ID Access ID + Face + Finger	Card + Biometrics Face Access Face Only	**	
Low Medium Low Medium	High Very High 1:1Security High Very High	Maximum Maximum	Private Authentication     Disable Biometric in Verificat     Disable PIN	tion	Disable Identification     Access Schedule in Duress	
APPLY C RES	1: N Security					

6. A confirmation popup dialog will be displayed. Click **Reset** to confirm.



7. The following confirmation message with display:



#### INVIXIUM



### FAQ

- Who can alter Biometric Configuration on the device? All IXM WEB users who have access to the Device and Device Group tab from IXM WEB.
- 2. Can I edit and update Biometric Configuration from IXM WEB? Yes, IXM WEB allows users to edit and update the Biometric Configuration.
- **3. Can I create more than one Biometric Configuration?** No, IXM WEB does not allow users to create additional Biometric Configurations.
- **4. Can I delete Biometric Configuration?** No, you can not delete the Biometric Configuration.



## Support

For more information relating to this Feature Description document, please contact us at <a href="mailto:support@invixium.com">support@invixium.com</a>

### **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.