



Biometric Fingerprint Platform

User Guide

Bayometric
1743 Park Avenue,
San Jose, CA 95126,
Phone: 877-917-3287, +1-408-940-3955,
Email: sales@bayometric.com

The software contains proprietary information of Bayometric; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information is subject to change without notice. The information and intellectual property contained herein is confidential between Bayometric and the client and remains the exclusive property of Bayometric. If you find any problems in the documentation, please report them to us in writing. Bayometric does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying and recording or otherwise without the prior written permission of Bayometric.

All the product names mentioned in this Guide are trademarks or registered trademarks of their respective owners. Bayometric acknowledges any and all rights of the trademarked companies.

Table of Contents

[Requirements](#)

[Installation instructions](#)

[Server Setup](#)

[Configuration Wizard](#)

[Client Setup](#)

[Firewall configuration](#)

[Step 1 - Start Firewall Configuration](#)

[Step 2 - Add Exceptions](#)

[Using Auto Discovery](#)

[Administration Tool](#)

[Accessing the tool](#)

[Main screen](#)

[User Management](#)

[Manage Roles](#)

[Adding a new privileged user](#)

[Backup Settings](#)

[Fingerprint Settings](#)

[Status and Reports](#)

This document aims to guide the user on how to prepare a development environment to use Bayometric Fingerprint Solution.

Requirements

Following are hardware and software requirements to install Bayometric Fingerprint Platform:

- Hardware
 - 2GB of RAM
 - 300MB of free space
- Software
 - Server
 - Server 2012/2008 R2 (recommended)
 - Windows 7 (minimum)
 - .net Framework 4.0
 - Client
 - Windows 7, 8.1
 - .net Framework 4.0
- Compatible fingerprint scanner

Installation instructions

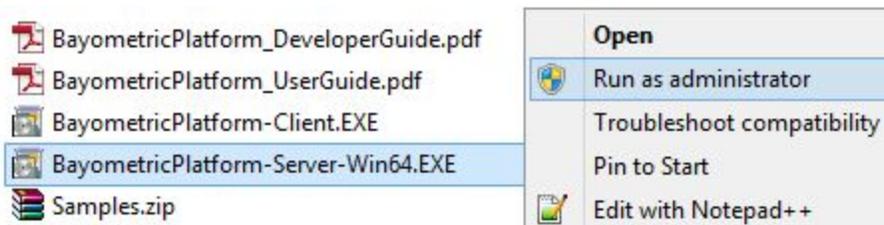
Platform installation package is a zip file that contains the following files:

- BayometricPlatform-Server-Win64.exe
 - Server installation package, this package installs services and tools required to host the Biometric server as well as administration tools.
- BayometricPlatform-Client.exe
 - Client redistribution package. This package installs client software and SDK required for applications to interface with the platform. It also installs a Client Configuration tool that helps user finding server location.
- Samples.zip
 - This zip file contains sample applications in C#.NET, Java and C++, with source code, that demonstrate usage of SDK and API.
- BayometricPlatform_UserGuide.pdf (this document)
- BayometricPlatform_DeveloperGuide.pdf
 - Guide document for developers.

Server Setup

Pre-requisites: Please make sure the computer does not have any previous installation of Bayometric Platform, OR MySQL database prior to installing this software. If any version of MySQL is installed, platform setup will not succeed. Also make sure that no folder named MySQL is present in C:\Program Data folder.

Install Platform by executing BayometricPlatform-Server-Win64.exe as administrator on a clean machine. To install as administrator, right click on the BayometricPlatform-Server-Win64.exe, select “Run as administrator”.



If the option “Run as Administrator” is not used, installer will not be able to start the service.

This setup will install MySQL server, setup database, install Bayometric Platform Services and Administration Tools.

During the steps below, when firewall settings are configured by the tool, consider that it only works for Windows Firewall. If the computer is protected by other solutions, check item “Firewall configuration” below in order to find which ports must be enabled.

Configuration Wizard

After setup finishes installing all necessary services and tools, Bayometric Configuration Wizard will appear. First screen, figure below, shows services status. If the installation was successful, all 3 services must be with status “Available”. If this is not the case, close the wizard and reinstall the platform.

SERVER INSTALLATION

Step 1 of 4



Service State

If any of the following services are 'Unavailable', please re-install the software.

Core Service	Available
Authentication Service	Available
Client Service	Available

Next

After clicking "NEXT", following screen should appear. On this screen, it is possible to allow Bayometric Wizard to set firewall rules necessary to run the platform. Please note that this wizard only creates rules on Windows Firewall.

Two firewall settings are available:

- **Mandatory Settings:** this item must always be configured, so, click SET to create the rules on Windows Firewall.
- **Auto Discovery Settings:** this item must be configured if auto discovery will be used by client machines to find server location. Click set to have the tool to configure Windows Firewall.

**SERVER INSTALLATION**

Step 2 of 4

**Configure Settings**

Click 'Next' to allow the Software to Configure the Windows Firewall Settings

Add TCP Port exception for Server Access Add UDP Port exception for Auto-Discovery

Back

Next

After configuration is done, click “NEXT”, and, if no license is installed on server, the following screen will show up.

**SERVER INSTALLATION**

Step 3 of 4

**Mail Server ID**Mail the below server ID to license@touchngo.com**63D2 - FG27 - 4521 - 6YT2 - 23DS**

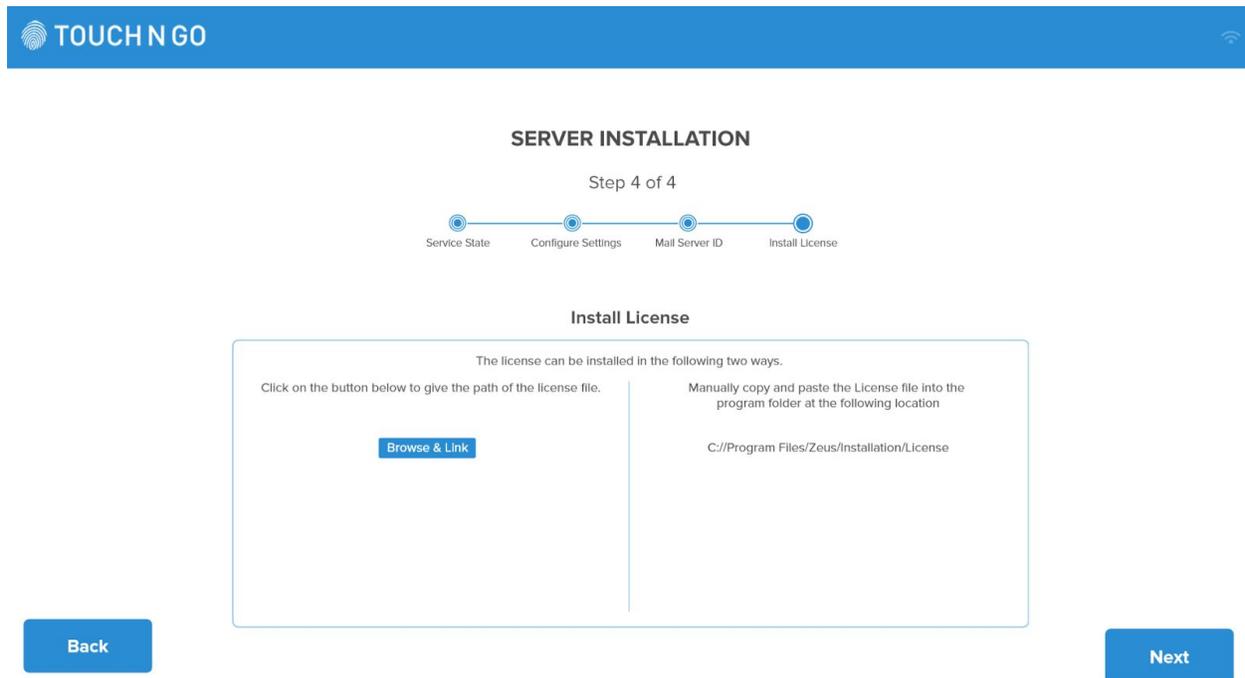
Back

Next

This screen shows a Machine ID, that is the machine identification that must be sent to Bayometric in order to acquire a license.

A valid Bayometric Platform license is required for the platform to activate and respond to the application requests. If license file is already available, click “Click to add license” button, and select license file to activate platform.

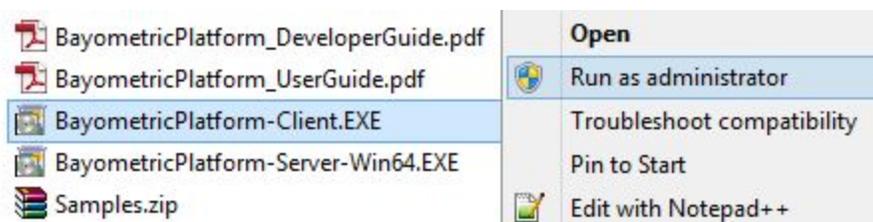
If license will be installed later place the license file “bfslic.lic” in “C:\Program Files (x86)\Bayometric\Zeus Core” folder.



After clicking next, final screen below will appear and Installation Wizard will close.

Client Setup

A remote client can be setup by installing BayometricPlatform-Client.exe. This package must be deployed with applications that use Bayometric Platform.



After running as administrator BayometricPlatform-Client.exe, as the last step of installation, Bayometric Client Configuration tool will open and the following screen will appear.

The screenshot shows the 'CLIENT CONFIGURATION' window. At the top left is the 'TOUCH N GO' logo. Below it, the title 'CLIENT CONFIGURATION' is displayed. The interface is divided into two main sections: 'Auto-Discovery' and 'Manual Configuration'. The 'Auto-Discovery' section contains a message stating that required firewall configuration is missing and provides a 'Configure Firewall' button. The 'Manual Configuration' section includes fields for 'Hostname/IP' (with 'bayometric' entered) and an unchecked 'SSL' checkbox. Below this is the 'REST API Configuration' section with an empty 'Accepted Domains' field. A 'Save' button is located at the bottom right of the window.

User will be able to see screen above if firewall settings needed to perform auto discovery are not created on the machine. In this situation, two options are available:

- Click Configure Firewall button and let Bayometric do all firewall configuration needed.
- Manually set Hostname or IP address under Bayometric Server section

If “Configure Firewall” button is clicked, the following screen will appear, and if server is properly configured to respond to auto discovery requests, server information will appear, as shown on figure below.

CLIENT CONFIGURATION

Auto-Discovery

Auto Discovery Performed		
Hostname	IP Address	Uses SSL
bayometric	169.254.115.75	False

[Refresh](#)

Manual Configuration

Hostname/IP

SSL

REST API Configuration

Accepted Domains

[Save](#)

Bayometric Server section will be updated and show correct hostname.

REST API Configuration session allows users to configure which domains are allowed to call local service from web pages. This configuration sets the “Access-Control-Allow-Origin” header on HTTP requests. All browsers expect this information to be set. Default value is empty, which means that no domain can call Bayometric service. For allowing any domain to call it, set it to “*”. For more information, HTTP headers configuration should be followed.

If everything is correct, click Save. If you see a message “Could not find Server”, then please click on Refresh.

It is important to know that auto discovery uses UDP communication between client and server. So, it is possible that some attempts to find server does not work due to packages loss. Button Refresh can be clicked to try again.

Client side of the platform is now ready to be used.

Firewall configuration

If machines running Bayometric Platform use a different firewall solution other than Windows Firewall, or if during installation firewall was not configured, firewall shall be configure to allow Bayometric Platform Clients to be able to communicate with the server over the network and also to allow client machines to find server location during platform setup. By default, firewall

would have blocked the network ports used by Bayometric Platform. This configuration is not required if firewall is turned off on the server and client where Bayometric Platform is installed. Also, please review the network configuration with your network administrator and make sure the network configuration in your organization is setup to allow Bayometric Platform Clients to be able to communicate with the server. Steps below go through configuration process on Windows Firewall. For other solutions, please check with your network administrator how to create the rules for required ports.

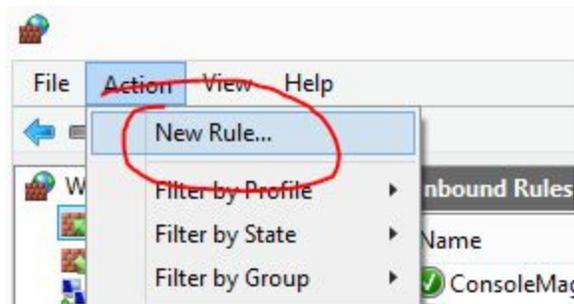
Step 1 - Start Firewall Configuration

Start Firewall Configurator on the computer where Bayometric Platform is installed. Select “Advanced Settings” to start advanced firewall configuration.



Step 2 - Add Exceptions

Click on “Inbound Rules” and select “Action->New Rule...” from the menu



On the rules below, UDP port configuration is only needed if client will use Auto Discovery feature to find server.

Add the following rules for “Port Exception”:

1. TCP port **22960**
2. TCP port **22961**
3. UDP port **22965**

Now, if client machines will use Auto Discovery to locate server, on previous screen, click on “Outbound Rules” and select “Action->New Rule...” from the menu.

Add the following rules for “Port Exception”:

1. UPD port **22964**

Using Auto Discovery

Bayometric supplies a Client Configuration tool that can be ran on client machines in order to allow auto location of server.

If this is the case, client machines firewall must also be configured. Add the following Port Exception rules on each client machine if Auto Discovery is used:

Add the following Inbound rule for “Port Exception”:

1. UDP port **22964**

And also add the following Outboud rule for “Port Exception”:

1. UDP port **22965**

Administration Tool

Bayometric Administration tool helps bootstrap the platform by enrolling the first administrator. A fingerprint scanner is required to enroll the first administrator, so please have the scanner connected before launching the admin tool.

Launch **Bayometric Administration** software under Bayometric folder on Start Menu.

Running the tool from the same machine server is installed is called Local Mode. Running from a different machine is called Remote mode.

When running the tool for first time (when no administrator is registered), two situations are possible. In local mode, the following screen will show.

The screenshot shows the 'SOFTWARE SETUP' interface. At the top, there is a blue header with the 'TOUCH N GO' logo and a help icon. Below the header, the title 'SOFTWARE SETUP' is centered, followed by 'Step 1 of 4'. A progress bar with four steps is shown: 'Create Initial Administrator' (active), 'Register Administrator Fingerprints', 'Set Mandatory Fingerprints', and 'Configure other fingerprint logging-in settings'. The main content area is titled 'Create Initial Administrator' and contains the instruction 'Enter details to create the initial administrator.' Below this are three input fields: 'User ID', 'Password', and 'Confirm Password'. A blue 'Submit' button is positioned below the 'Confirm Password' field. To the right of the main form area, there is a 'Next' button.

This screen allows IT Administrator to enroll a new admin or the configure the server.

Fill-in ID, Password fields in the form, and click Submit. Fingerprint capture wizard screen will guide you to enroll fingerprints for administrator.

When enrollment GUI opens, it is in “automatic mode”, this means that this is already waiting for the first finger to be placed on fingerprint reader.

Mandatory fingers are marked with a black lines. These fingers must be captured before submitting captured information. Current finger being captured is marked with pink background.

For each finger to be captured, user should place his finger up to 7 times on the the fingerprint scanner depending on the fingerprint quality. This number guarantees that the quality of the enrollment is good and recognition performance will be high.

After capturing all mandatory fingers, Submit button will be enabled. Upon submission (click on the Submit button), the identity will be registered.

If person being enrolled does not have a mandatory finger or is not able to capture that finger, select Mark Exception. A Mark Exception Window will open. Please select the reason for exception. After an exception is set, finger is considered to be captured. Once an exception is marked, please select the next finger to be registered by clicking on the finger.

If for any reason user needs to switch to “manual mode”, just click “Manual Mode” button. On manual mode, to start capturing a finger, just click on desired finger.

The Next Step is to Login using the Fingerprint that you just registered. Please place your registered finger on the scanner to log into the Admin Panel



SOFTWARE SETUP

Step 2 of 4



Register Administrator Fingerprints



Once you have logged in you will be guided through initial Software Settings.

In the screen below, you can select the fingerprints that are mandatory fingerprints for the user registration. Mandatory Fingers allows administrators to set which fingers are mandatory when enrolling a new user. After saving, it will be used on all client machines on the next enrollment.



SERVER INSTALLATION

Step 3 of 4



Set Mandatory Fingers



Using the next screen you are able to set the following 3 parameters -

Max finger samples: Defines the maximum amount of samples of the same finger the platform will capture to try to get maximum quality. Bayometric suggests to keep this number as 7. The minimum value is 3 the lower the number the higher the risk to face problems during recognition.

Session Duration: Defines for how long a session will be active on the platform.

Save failed authentication: Defines if failed attempts to create session (fingerprint not found) will store images on server for future auditing.

The screenshot shows the 'SERVER INSTALLATION' interface for 'TOUCH N GO'. The top navigation bar includes the logo and 'Welcome admin' with a close button. The main heading is 'SERVER INSTALLATION' and the current step is 'Step 4 of 4'. A progress bar shows four steps: 'Create Initial Administrator', 'Register Administrator Fingerprints', 'Set Mandatory Fingerprints', and 'Configure other fingerprint logging-in settings'. The active step is 'Configure other fingerprint logging-in settings'. The configuration form includes a title, a subtitle 'Set up the limit for maximum tries and session duration.', and three input fields: 'Maximum scans allowed' (value: 7), 'Session Duration (seconds)' (value: 480), and 'Save failed authentication' (checkbox). A 'Submit' button is located below the fields. A note at the bottom states: 'Note: Changes done here, will not affect already registered users. The new users henceforth will be affected.' A 'Next' button is positioned to the right of the form.

This is the final Step in the initial Software Setup.

The screenshot shows the TOUCH N GO logo on the left and 'Welcome admin' on the right of a blue header bar. Below the header, the text 'SERVER INSTALLATION' is centered. Underneath, it says 'All steps completed' above a progress bar with four steps: 'Create Initial Administrator', 'Register Administrator Fingerprints', 'Set Mandatory Fingerprints', and 'Configure other fingerprint logging-in settings'. A 'Congratulations' section follows, containing a message: 'Software setup completed successfully. Administrator has been created. Now you will be redirected to the administrator panel'. A 'Next' button is located at the bottom right.

On the following sections all operations available on the tool will be explained.

Accessing the tool

The screenshot shows the TOUCH N GO logo on the left and a close button on the right of a blue header bar. The main content area is a white box titled 'LOGIN'. It contains two input fields: 'Username:' and 'Password:'. Below these fields are two buttons: a blue 'LOGIN' button and a blue 'LOGIN by FINGERPRINT' button.

To access the platform either fingerprints or username and password must be supplied. Due to security reasons, Username + Password authentication will only be available in Local Mode. To access the platform via Fingerprint. Please click on the button LOGIN by Fingerprint.

Main screen

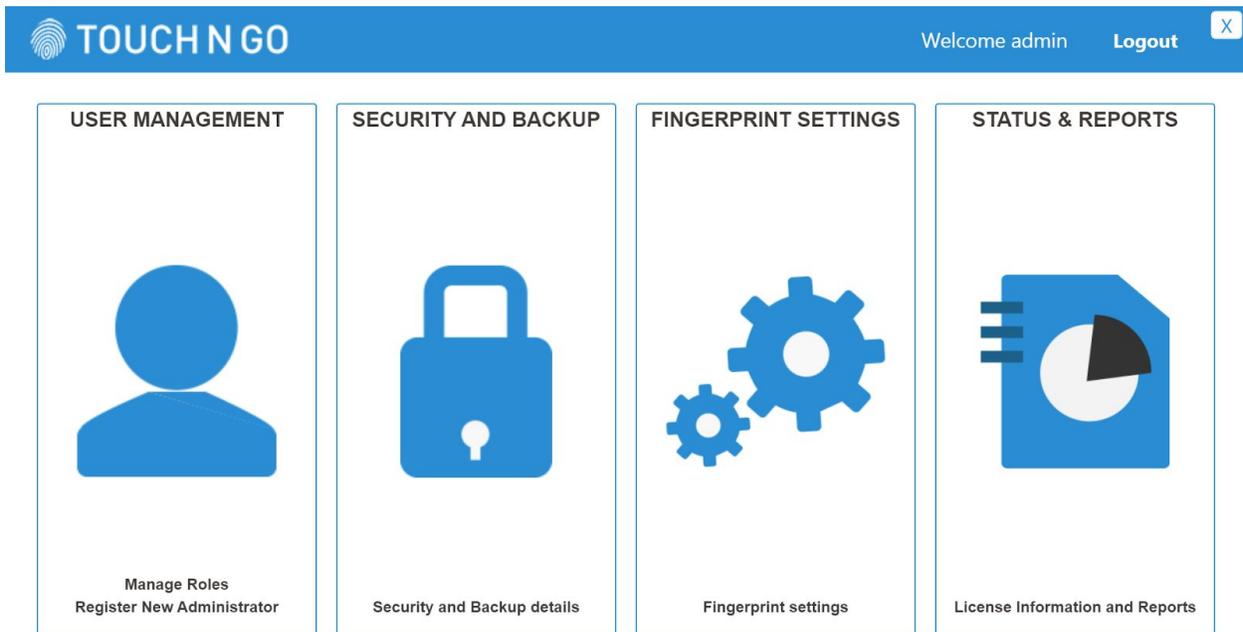


Figure above represents the main screen of Administration Tool. This is the screen that appears after a successful login. On top right corner it is possible to find the ID of the logged user (admin, in this case).

The four options available will be explained below.

User Management

This feature allows the enrollment of a new user on the platform with an Administrator role. This process is the same as the one explained during the enrollment of the first admin.

Manage Roles

TOUCH N GO Welcome admin Logout

USER MANAGEMENT

Find Create New Admin

Administrative Users

admin

User Information
User ID: admin

Edit Credentials
Password:
Confirm Password:

Assign role/permissions
Administrator
Manager

Recapture Fingerprints

Back Update

This page is responsible for user roles and data information. The list on the left shows all privileged users that are enrolled on the platform. Two roles are available:

- **Administrator:** Can perform administration operations (change platform configurations), Register and Unregister users.
- **Manager:** Can register and unregister users.

To change a user role, select user ID on left and select role on Permissions box. To change password or recapture fingerprints, User Data box options can be used.

Adding a new privileged user

There are cases where a user was registered by an application but needs to be added as a privileged user later. To do this, type user ID on top of left panel and click "ADD". If ID exists, it will appear as red on the list, just like john_smith on the figure below.

The screenshot shows the TOUCH N GO USER MANAGEMENT interface. At the top, there is a blue header with the TOUCH N GO logo, the text "Welcome admin", a "Logout" button, and a close button (X). Below the header, the "USER MANAGEMENT" section contains a search bar with "john_smith" entered and a "Find" button. A "Create New Admin" button is also present. The main content area is divided into three panels. The left panel, titled "Administrative Users", lists "admin" and "john_smith", with "john_smith" selected. The middle panel, titled "User Information", shows "User ID: johnsmith" and "Edit Credentials" with "Password:" and "Confirm Password:" fields. Below this is the "Assign role/permissions" section with checkboxes for "Administrator" and "Manager". The right panel is titled "Recapture Fingerprints" and contains a fingerprint scanner icon. At the bottom left is a "Back" button, and at the bottom right is an "Update" button. Five red text annotations with black circles and arrows point to specific elements: Step 1 points to the search bar, Step 2 points to the "john_smith" user in the list, Step 3 points to the password fields, Step 4 points to the "Administrator" checkbox, and Step 5 points to the "Update" button.

TOUCH N GO Welcome admin Logout X

USER MANAGEMENT

Step 1: Type the User ID in this box and click Find

john_smith Find Create New Admin

Administrative Users

Step 2: Select the user ID from this list

admin john_smith

User Information

User ID: johnsmith

Edit Credentials

Password: Step 3: Create a new Password

Confirm Password:

Assign role/permissions

Administrator Step 4: Select the Role

Manager

Recapture Fingerprints

Back Step 5: Click on Update Update

Select the ID and no roles will be set for this user. Select a role, type and confirm password, and click Update. The user will now become a privileged user.

To remove a user from privileged users list, select it's ID and uncheck roles.

Security And Backup

This tab is only enabled in Local Mode.

SECURITY AND BACKUP

Security Settings

SSL Configuration

Use SSL Connection

Store Location

Store Name

Thumbprint

Host Configuration

Hostname / IP

Backup Settings

Generate Backup File

Import Backup File

Security Settings

On this tab, following options are available:

- **SSL Configuration:** If communication between client machines and server needs to be done through a secure channel, then configurations available on this box must be properly set.
 - **Use SSL connection:** Defines whether or not SSL will be used
 - **Store Location:** Defines Store Location of the certificate to be used
 - **Store Name:** Defines Store Name of the certificate to be used
 - **Thumbprint:** Defines thumbprint of the certificate to be used. Special attention is required while setting this field, specially when copy and past from MMC is used.
- **Hostname/IP:** When auto-discovery feature is used, this is the information that will be sent to client machines to connect to server. This field must contain the hostname/ip of the **server**

It is important to know that even if SSL configurations are correct, ports 22960 and 22961 must be properly configured with the certificate. The following command line can be used for properly configuring the ports:

```
netsh http add sslcert ipport=0.0.0.0:22960 certhash=CERTIFICATE_THUMBPRINT  
appid=APPLICATION_ID
```

```
netsh http add sslcert ipport=0.0.0.0:22961 certhash=CERTIFICATE_THUMBPRINT
appid=APPLICATION_ID
```

Please contact system administrator to guarantee that network is properly configured.

Backup Settings

Bayometric Platform allows system administrators to backup all stored information in a very simple way. Clicking “Generate Backup File” button will open a file dialog to type the file name. After choosing it, a backup file with “.bbf” extension will be created.

To import a backup file, click “Import Backup File” and choose the correct file.

Fingerprint Settings

 TOUCH N GO
Welcome admin [Logout](#) X

FINGERPRINT SETTINGS

Settings Details

Set up the limit for maximum tries and session duration.

Maximum scans allowed

Session Duration

Save failed authentication

Mandatory Fingerprint Registration

Select by clicking the fingers in the image below to make them mandatory for registration of the users.



Note
Changes done here, will not affect already registered users. The new users henceforth will be affected.

Back
Save

On this tab, following options are available:

- Mandatory Fingerprint Registration:** Allows administrators to set which fingers are mandatory when enrolling a new user. After saving, it will be used on all client machines on the next enrollment. It is not necessary to restart any service. At least 2 fingers must be set.

- **Max finger samples:** Defines the maximum amount of samples of the same finger the platform will capture to try to get maximum quality. Biometric suggests to keep this number as 7. The minimum value is 3 the lower the number the higher the risk to face problems during recognition.
- **Session Duration:** Defines for how long a session will be active on the platform.
- **Save failed authentication:** Defines if failed attempts to create session (fingerprint not found) will store images on server for future auditing.

Status and Reports

TOUCH N GO Welcome admin Logout

STATUS AND REPORTS

License Information

Information	Allowed	Current
Records	1000	1
Clients	20	2
Expiration	-	-

Backup Settings

Users IDs (.csv)

Generate File

Back

On this tab, following informations are available:

- **License information:** Shows information about license
 - **Records:** Shows maximum number of records allowed on database and current number stored.
 - **Clients:** Shows maximum number of client machines allowed to connect to server and current number
 - **Expiration:** Shows expiration date if a trial license is being used
- **Reports:** Allows generation of reports. Current version allows the generation of csv file containing all enrolled IDs on the platform.