

SafeNet MobilePASS+ for Android

User Guide

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Product Version: 1.3.1 Android

Document Part Number: 007-013317-003, Rev. B

Release Date: 5 May 2017

Contents

1	Preface	5
	Difference between SafeNet MobilePASS+ App and Token	5
	SafeNet MobilePASS+ App	5
	SafeNet MobilePASS+ Token	5
	Who Should Read this Document	5
	Support Contacts	6
2	Installing the SafeNet MobilePASS+ App	7
	Supported Platforms	7
	Downloading the SafeNet MobilePASS+ Application	7
3	Enrolling SafeNet MobilePASS+ Token	8
	Methods to Enroll a SafeNet MobilePASS+ Token	8
	Automatic Enrollment	9
	Enrolling by Scanning QR Code	14
	Enrolling by Copying and Pasting the Activation String	19
	Creating a New Token	23
4	Authenticating with a Biometric PIN	24
	Introduction to Biometric Authentication	24
	Activating and Deactivating the Biometric PIN Feature	25
	Accessing a Token Using a Biometric PIN	26
5	Generating Passcodes	27
	Generating a Passcode with Time-based Tokens	28
	Generating a Passcode with Event-based Tokens	29
	Generating Passcodes with Challenge-Response Tokens	30
6	Using Push OTP	31
	Introduction to Push OTP	31
	Activating and Deactivating Push OTP	32
	Logging in with Push OTP	33
7	Changing a Token PIN	37
	Changing a Token PIN	37
8	Renaming and Deleting a Token	39
	Renaming a Token	39
	Deleting a Token	40
9	Viewing Token, App, and Log Information	41
	Viewing Token Information	41

Viewing SafeNet MobilePASS+ App Information	42
Viewing Help Topics	43
Viewing Token Enrollment Log	45
10 Frequently Asked Questions	47
What is a SafeNet MobilePASS+ Token?	47
How does SafeNet MobilePASS+ protect me?	47
How do I generate a passcode on my mobile device?	47
How do I get started with SafeNet MobilePASS+?	48
I have not received an enrollment email, what should I do?	48
For how long will my token continue to operate?	48
What is self-enrollment?	48
What are the benefits of using the token?	48
How do I protect my security PIN?	48
What should I do if I cannot log in using my token?	48
What is Push OTP?	49
How do I use Push OTP?	49
11 Terminology	50
12 References	52
Related Documents	52
SafeNet MobilePASS+	52

SafeNet MobilePASS+ is a mobile client application that enables you to access corporate and web-based resources securely. It eliminates the need to remember complex passwords. SafeNet MobilePASS+ is a cost-effective way for businesses to leverage the security of One Time Passwords (OTP) using mobile phones. Associated with SafeNet Authentication Service- Cloud Edition, the MobilePASS+ application is a perfect combination of security and convenience. It offers a simple user experience for token activation and authentication using the Push OTP mechanism.



NOTE: SafeNet MobilePASS+ can generate passcodes independently of mobile network connectivity.

Difference between SafeNet MobilePASS+ App and Token

The SafeNet MobilePASS+ solution includes both the SafeNet MobilePASS+ app and SafeNet MobilePASS+ tokens. The following description clarifies the terms.

SafeNet MobilePASS+ App

The SafeNet MobilePASS+ app is an application that turns your mobile phone into a two-factor authentication device, removing the need to carry an additional hardware token.

As a SafeNet MobilePASS+ user, you can generate passcodes on your mobile device, and use those passcodes to authenticate to protected corporate and web-based applications.

SafeNet MobilePASS+ Token

A SafeNet MobilePASS+ token is related to an account and its associated parameters, such as name, user PIN, enrolled keys, and PIN policy. Each SafeNet MobilePASS+ app can manage multiple SafeNet MobilePASS+ tokens. For example, a user may require several tokens, each one related to a different web service.

Who Should Read this Document

This document is intended for end-users who will be using the SafeNet MobilePASS+ app. This document provides information on how to install and run the SafeNet MobilePASS+ token.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com

Installing the SafeNet MobilePASS+ App

Supported Platforms

SafeNet MobilePASS+ for Android runs on Android versions 4.0 and later.

Android 6 or later is required for the Biometric PIN feature.

Downloading the SafeNet MobilePASS+ Application

Download and install SafeNet MobilePASS+ from Google Play.

Once installed, the SafeNet MobilePASS+ application icon will be visible on your device:



Enrolling SafeNet MobilePASS+ Token

Methods to Enroll a SafeNet MobilePASS+ Token

Before you can use SafeNet MobilePASS+ to generate passcodes, you must enroll a SafeNet MobilePASS+ token on your device.



Note: Additional SafeNet MobilePASS+ tokens can be added later. See “Creating a New Token” on page 23.

You can enroll your SafeNet MobilePASS+ token using one of the following methods:

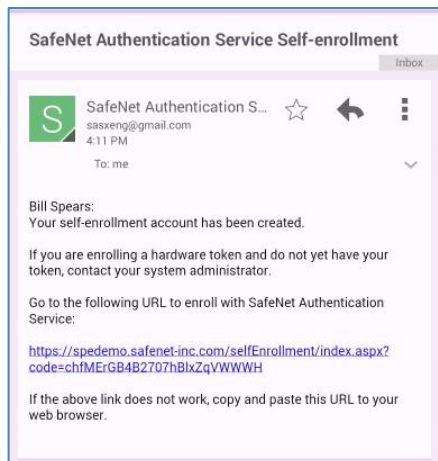
- **Automatic Enrollment** - Automatically copy and paste the activation code into the Auto Enrollment window by clicking the Enroll your SafeNet MobilePASS+ token link on the notification email.
- **QR Code Enrollment** - Scan a QR Code to enroll your SafeNet MobilePASS+ token. This is recommended when you cannot receive email or open self-enrollment from the target device.
- **Copy and Paste Activation String into the Automatic Enrollment Window** - This is recommended when you have difficulties with Automatic Enrollment. For example, if the registration link in the device does not work or the browser in use does not support opening an external application.

Automatic Enrollment

After your system administrator assigns you a token, you will receive a notification email.

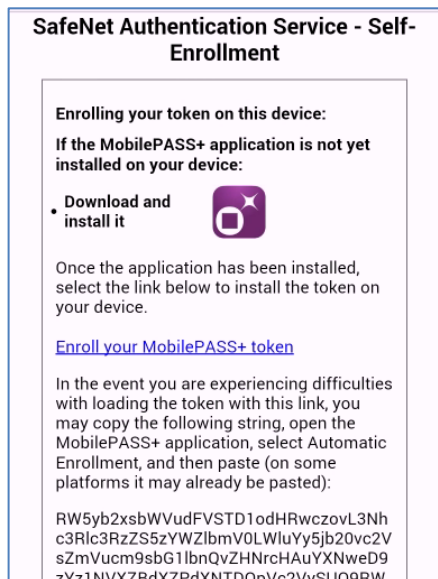
To enroll SafeNet MobilePASS+ token automatically:

1. Tap the https:// link in the email.



The **SafeNet Authentication Service Self-Enrollment** webpage opens.

2. Click **Enroll your SafeNet MobilePASS+ token**.





NOTE: Your token can be configured by your system administrator to work with Token PIN, Server PIN, or no PIN.

If configured for no PIN, you will not be prompted to enter a PIN.

3. If your token is PIN protected, you are prompted to enter a PIN.
 - a. If your token is user-selected PIN protected, the **TOKEN PIN** window opens. Enter a PIN in the Token PIN field and enter again in the Confirm PIN field, and tap **SUBMIT**.
-



NOTE: The type and number of characters required for the PIN is displayed on the screen above the **Submit** button.

TOKEN PIN

Set and confirm your PIN.

Token PIN

Confirm Token PIN

The PIN should contain 4 numeric characters.

SUBMIT

- b. If your token is server-side PIN protected, the **SERVER PIN** window opens. Enter a Server PIN, confirm and tap **SUBMIT**.
-



NOTE: The type and number of characters required for the PIN is displayed on the screen above the **Submit** button.

SERVER PIN

Set and confirm your PIN.

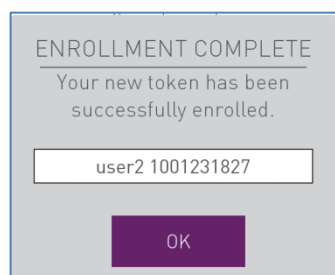
Server PIN

Confirm Server PIN

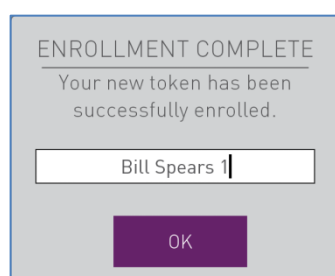
The PIN should contain 3 to 8 numeric characters.

SUBMIT

The **ENROLLMENT COMPLETE** screen opens.



4. In the **ENROLLMENT COMPLETE** screen, do one of the following:
 - a. To accept the default token name, tap **OK**.
 - b. To edit the Token Name, type the required changes into the **TOKEN NAME** field and tap **OK**.

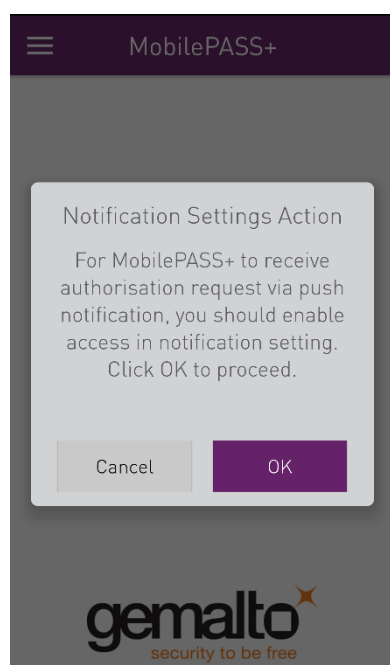


The new SafeNet MobilePASS+ token is displayed in the SafeNet MobilePASS+ app.

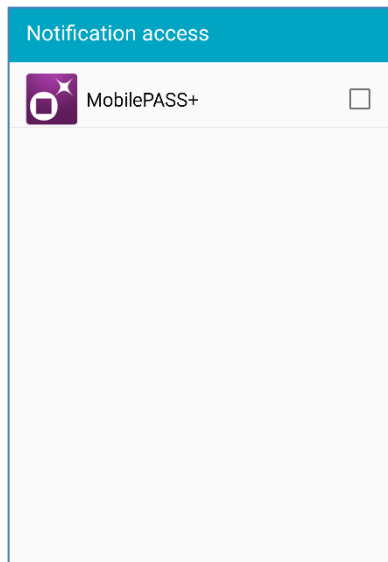
5. If prompted, to enable the Push Notification feature, in the **Notification Settings Action** window tap **OK**.



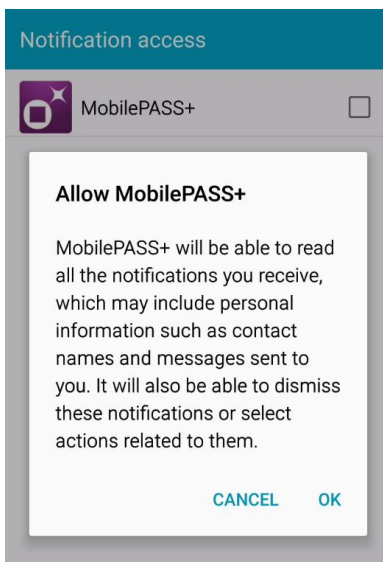
NOTE: Push Notification is available only if this feature has been activated by your system administrator.



6. In the **Notification Access** Window, tap on the checkbox.

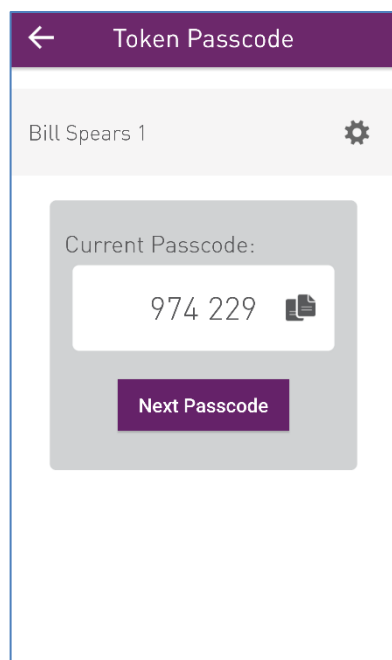


7. In the **Allow MobilePASS+** window, tap **OK** to confirm.



The new SafeNet MobilePASS+ token is displayed with the generated passcode.

This example below shows an Event Based Token. The token can also be Time-Based or Challenge-Response. For details see “Generating Passcodes” on page 27.



Enrolling by Scanning QR Code



NOTE: Enrollment by scanning QR code is available if your token has been configured to include this feature.

After your system administrator assigns you a token, you will receive a notification email.

To enroll SafeNet MobilePASS+ by scanning the QR Code:

1. Tap the <https://> link in the email *on a different device* to the one on which you want to install the SafeNet MobilePASS+ token

The **SafeNet Authentication Service Self-Enrollment** webpage opens.

2. Select **Android** from the drop-down list of supported devices.

The QR code is displayed.

To enroll your token on another device

Please select a supported device below, and follow the instructions.


Android

If the MobilePASS+ application is not yet installed on your device:

- Locate it on Google Play Store



- Download and install it




Open this page on your selected device, and follow the instructions shown on the page.

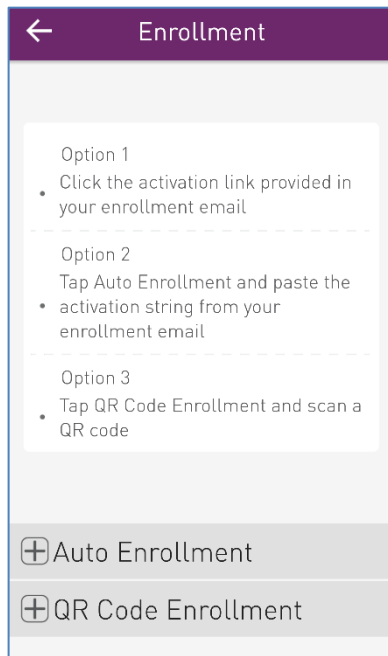
- To enroll your token on your device using QR code, scan the code to the right using downloaded MobilePASS+ application on your device.



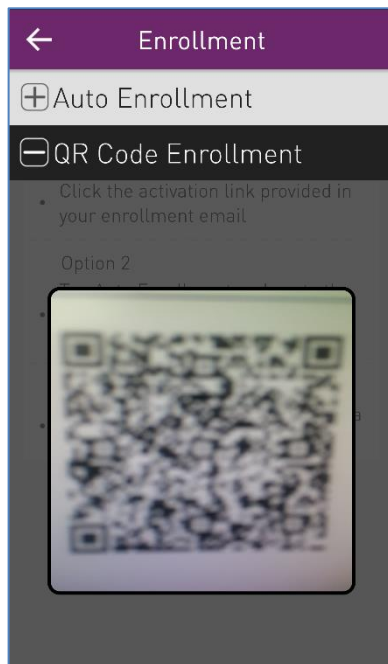
After completing token enrollment, close the browser window.

3. On your device, open the SafeNet MobilePASS+ application, tap **Get Started** (if you have not yet enrolled a token), or tap the **Add** icon .

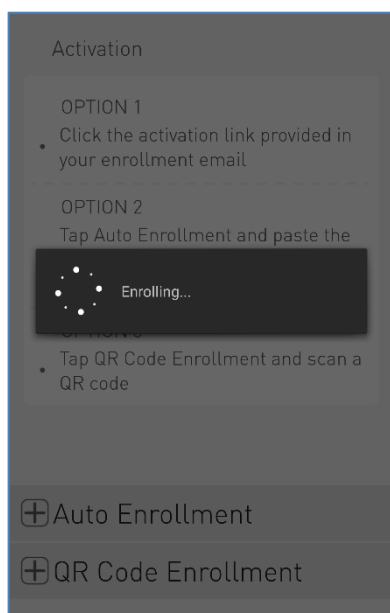
4. In the **Activation** window, tap **QR Code Enrollment**.



5. Point the camera to the QR Code on the **SafeNet Authentication Service Self-Enrollment** webpage.



The camera scans the QR Code and begins enrollment.



NOTE: Your token can be configured by your system administrator to work with Token PIN, Server PIN, or no PIN.

If configured for no PIN, you will not be prompted to enter a PIN.

6. If your token is PIN protected, do one of the following:

- a. If your token is token PIN protected, the **TOKEN PIN** window opens. Enter a PIN in the **Token PIN** field and enter again in the **Confirm Token PIN** field, and tap **SUBMIT**.



NOTE: The type and number of characters required for the PIN is displayed on the screen above the **Submit** button.

- b. If your token is server-side PIN protected, the **SERVER PIN** window opens. Enter a PIN in the **Server PIN** field and enter again in the **Confirm Token PIN** field, and tap **SUBMIT**.



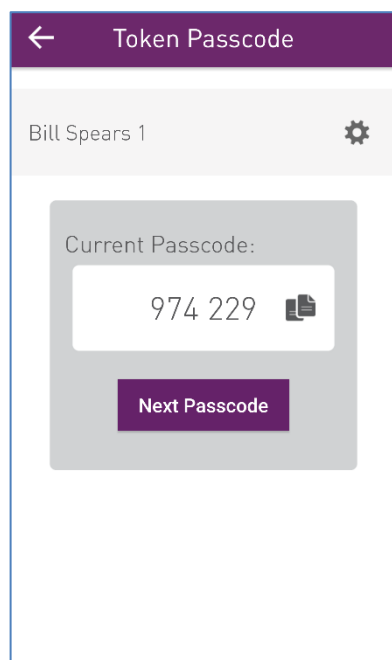
NOTE: The type and number of characters required for the PIN is displayed on the screen above the **Submit** button.

7. In the **ENROLLMENT COMPLETE** screen, do one of the following:
- To accept the default token name, tap **OK**.
 - To edit the Token Name, type the required changes into the **TOKEN NAME** field and tap **OK**.

- c. The new SafeNet MobilePASS+ token is displayed in the SafeNet MobilePASS+ app.

The new SafeNet MobilePASS+ token is displayed with the generated passcode.

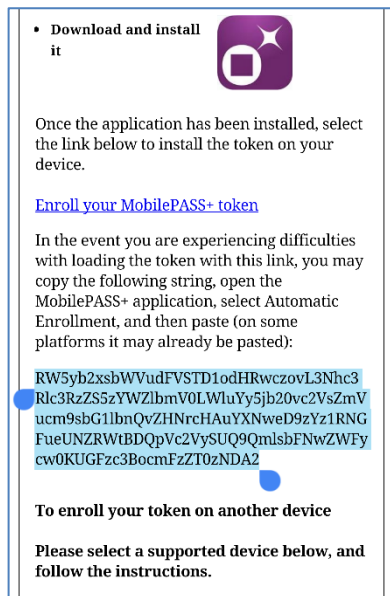
This example below shows an Event Based Token. The token can also be Time-Based or Challenge-Response. For details see “Generating Passcodes” on page 27.



Enrolling by Copying and Pasting the Activation String

To enroll SafeNet MobilePASS+ by copying and pasting the activation string:

1. Copy the activation string from the webpage.

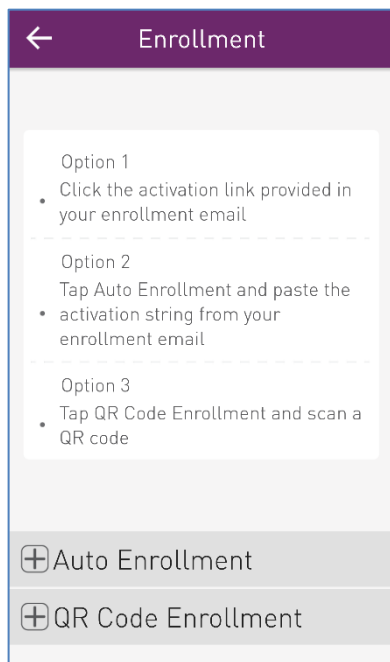


TIP: To copy the activation string:

1. Long-tap on the activation string.
2. Drag the set of bounding handles to include the whole activation string.
3. Tap the selected text again to copy the activation string to the clipboard.

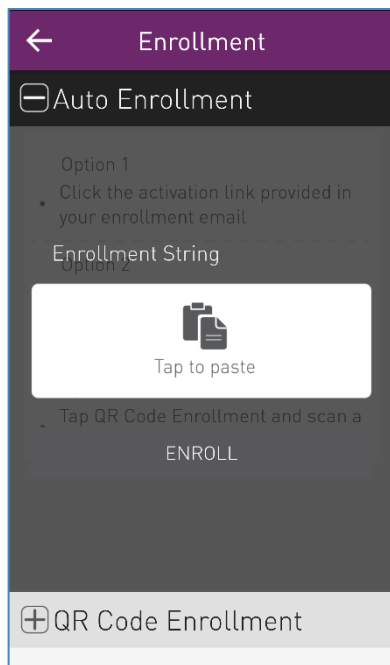
2. Open the SafeNet MobilePASS+ application and tap **Get Started** or tap the **Add** icon .

3. Tap **Auto Enrollment**.

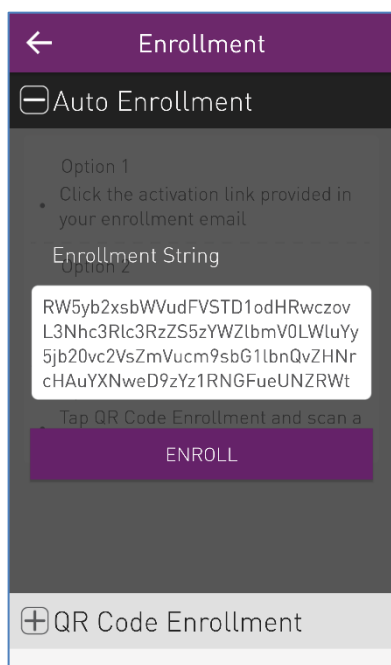


4. To paste the activation string:

a. Tap **Tap to paste**.



- b. Tap **ENROLL**.



5. To enter, or edit, the activation string from the keyboard:

- Double tap the **Enrollment String** box.
- Use the keyboard to type in, or edit, the Activation String:



NOTE: Your token can be configured by your system administrator to work with Token PIN, Server PIN, or no PIN.

If configured for no PIN, you will not be prompted to enter a PIN.

6. If your token is PIN protected, do one of the following:

- If your token is token PIN protected, the **TOKEN PIN** window opens. Enter a PIN in the **Token PIN** field and enter again in the **Confirm Token PIN** field, and tap **SUBMIT**.



NOTE: The type and number of characters required for the PIN is displayed on the screen above the **Submit** button.

- b. If your token is server-side PIN protected, the **SERVER PIN** window opens. Enter a PIN in the **Token PIN** field, enter again in the **Confirm PIN** field, and tap **SUBMIT**.



NOTE: The type and number of characters required for the PIN is displayed on the screen above the **Submit** button.

7. In the **ENROLLMENT COMPLETE** screen, do one of the following:
- To accept the default token name, tap **OK**.
 - To edit the Token Name, type the required changes into the **TOKEN NAME** field and tap **OK**.

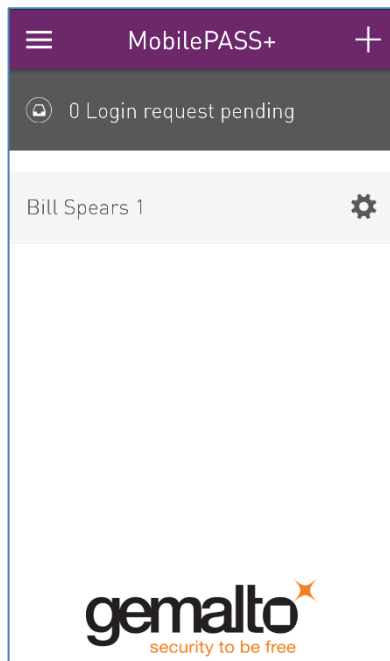
8. Tap **OK**.


The new SafeNet MobilePASS+ token is displayed on the SafeNet MobilePASS+ app.

Creating a New Token

To create a new token:

1. Open the SafeNet MobilePASS+ application.



2. Tap the Add icon .
3. Enroll a new token (see “Methods to Enroll a SafeNet MobilePASS+ Token” on page 8).

Authenticating with a Biometric PIN

Introduction to Biometric Authentication



Biometric Authentication is a generic term used to describe the use of a human characteristic to perform authentication. In MobilePASS+, the human characteristic in question is a fingerprint, which can be used to access the app and tokens. This is a convenient alternative to entering a PIN manually, and is often referred-to as a Biometric PIN. To perform Biometric Authentication with MobilePASS+ for Android, the fingerprint is scanned by a Nexus Imprint fingerprint sensor on the device.

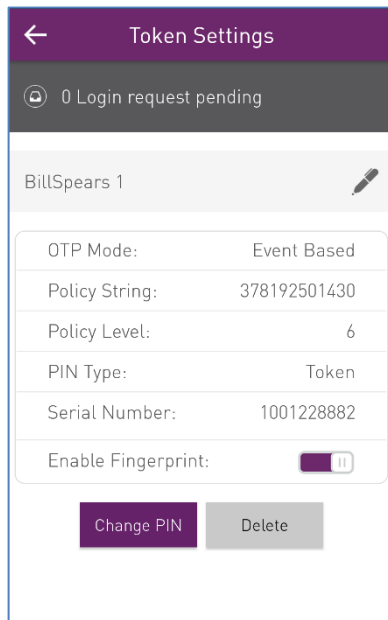
To use a Biometric PIN to access SafeNet MobilePASS+, the following requirements must be met:


- Android 6 or later must be installed on your device.
- The Nexus Imprint fingerprint sensor must be present, and activated, on your device.
- Your SafeNet MobilePASS+ token must have been configured by your system administrator to allow the use of a Biometric PIN.

Activating and Deactivating the Biometric PIN Feature

To activate/deactivate Biometric PIN on a SafeNet MobilePASS+ token:

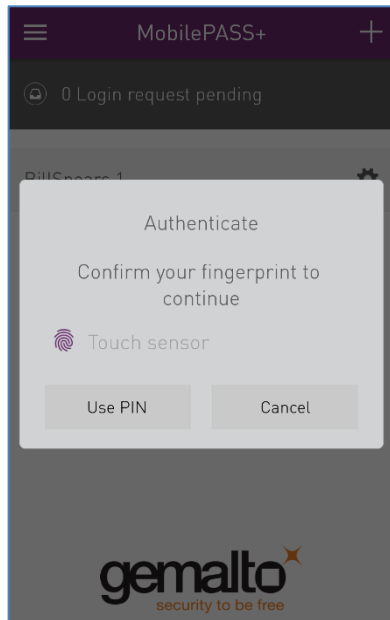
1. Open the SafeNet MobilePASS+ app and tap the **Settings** icon  next to the token.
2. Drag the **Enable Fingerprint** slider to the right. The Purple color indicates that Biometric PIN feature is activated. 



3. To deactivate the Biometric Authentication, drag the **Enable Fingerprint** slider to the left. 
The grey color indicates that Biometric PIN feature is deactivated.

Accessing a Token Using a Biometric PIN

If the token has been configured to work with Biometric PIN, each time you are required to enter a PIN you will be prompted to use your fingerprint to authenticate.

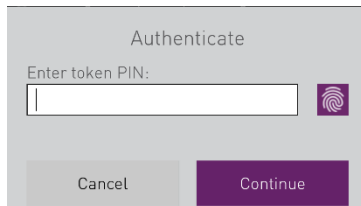



To access the token with fingerprint:

When prompted with the message, **Confirm your fingerprint to continue**, touch the device's fingerprint sensor.

To access the token with a PIN after being prompted for a fingerprint:

1. Tap **Use PIN**.
2. In the **Enter token PIN** field, enter the PIN.



3. To switch to fingerprint, tap the fingerprint icon .

5

Generating Passcodes

Your SafeNet MobilePASS+ tokens can be configured by your system administrator to generate passcodes using one of the following methods:

- Time based
- Event based
- Challenge-Response

Your SafeNet MobilePASS+ app can contain multiple SafeNet MobilePASS+ tokens, configured with different passcode generation methods.



NOTE: The number of pending logon requests is displayed at the top of the app screen.

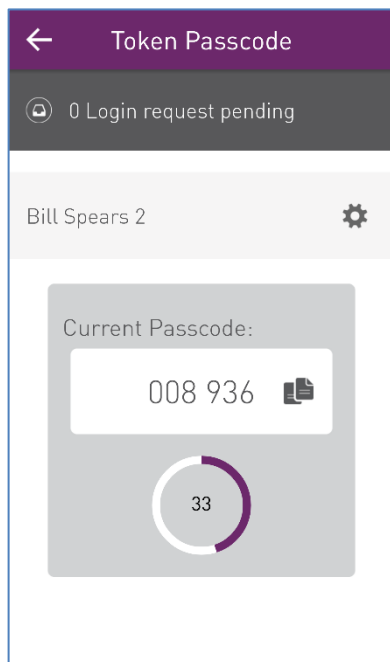
Generating a Passcode with Time-based Tokens


If you are using a time-based token, the passcode is generated automatically after the specified time interval has elapsed. When a new passcode is generated, the previous passcode is no longer valid.

To generate a passcode with a time-based token:

1. Open the SafeNet MobilePASS+ app.
2. If there is more than one token, tap the required token.
3. If your token is PIN protected, enter the PIN, or if available, use the Biometric PIN.

The passcode is displayed.



4. To copy the passcode to the clipboard, tap the Clipboard icon . A new passcode will be displayed at the end of the specified time-interval.

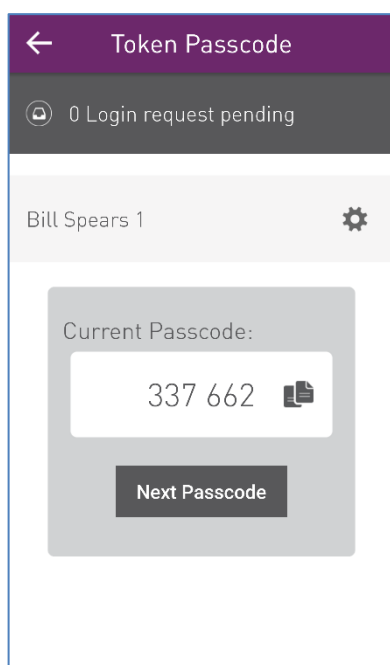
Generating a Passcode with Event-based Tokens


Event-based tokens are so-called because they require an event to generate the passcode. In SafeNet MobilePASS+, the event is the tapping of the **Next Password** button. The passcode is valid until it is used to authenticate or until another passcode is generated.

To generate a passcode with an event-based token:

1. Open the SafeNet MobilePASS+ app.
2. If there is more than one token, tap the required token.
3. If your token is PIN protected, enter the PIN, or if available, use the Biometric PIN.

The passcode is displayed.



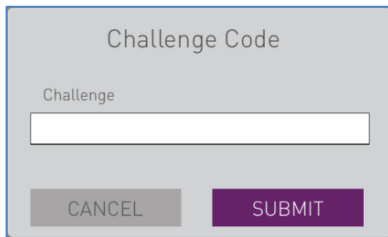
4. To copy the passcode to the clipboard, tap the clipboard icon .
5. To generate a new passcode, tap **Next Password**.

Generating Passcodes with Challenge-Response Tokens

To generate a passcode on a Challenge-Response Token, you must first receive the challenge code. To receive the challenge code, follow the procedure used in your organization.

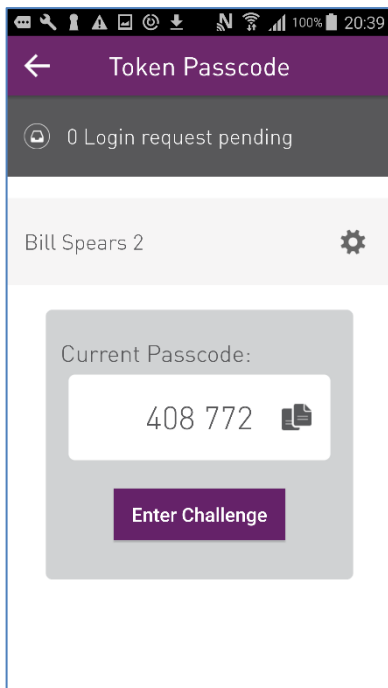
To generate a passcode with a challenge-response token:

1. Open the SafeNet MobilePASS+ app.
2. If there is more than one token, tap the required token.
3. Enter the provided challenge code in the **Challenge Code** field.

A screenshot of a mobile app screen titled "Challenge Code". It features a text input field labeled "Challenge" with a white background and a grey border. Below the input field are two buttons: a grey "CANCEL" button on the left and a purple "SUBMIT" button on the right.

4. Tap **Generate Passcode**.

The passcode is displayed.

A screenshot of the "Token Passcode" screen in the SafeNet MobilePASS+ app. The screen has a purple header with a back arrow and the title "Token Passcode". Below the header is a grey bar showing "0 Login request pending". The main content area is white and shows the user name "Bill Spears 2" with a settings gear icon. A grey box contains the text "Current Passcode:" followed by a white input field displaying the passcode "408 772" and a copy icon. Below the input field is a purple button labeled "Enter Challenge".

5. To generate another passcode, tap **Enter Challenge**, and then repeat the process.

Using Push OTP

Introduction to Push OTP

Support for the Push OTP feature depends on the configuration of your SafeNet MobilePASS+ token.

Push OTP simplifies the process of accessing a protected resource, such as a webpage, cloud or VPN. A push notification is sent from the login page to your mobile device and can be viewed as follows:



- An Android locked-screen notification.
- A Pending Notification bar displayed on the SafeNet MobilePASS+ application.

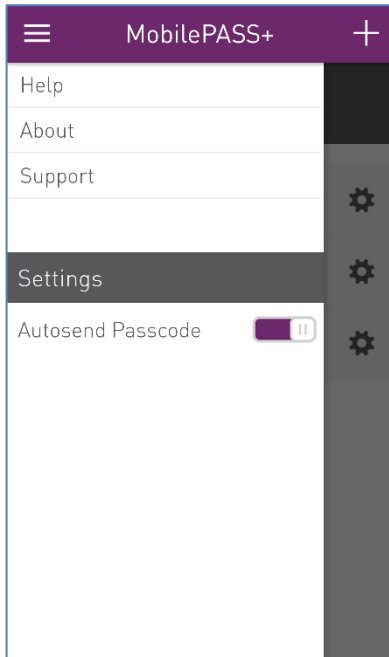
After you have approved the login request with a tap of a button, and entered a PIN (if required according to your tokens' settings), a passcode is generated by your SafeNet MobilePASS+ app and sent to the login page, logging you in automatically. This eliminates the need to generate a one-time passcode (OTP) on your mobile device or to enter it into the login page.


You may be required to enter a PIN after approving the push notification.

Activating and Deactivating Push OTP

To activate/deactivate Push OTP:

1. Tap the Menu Icon 
2. Do one of the following:
 - a. To activate Push OTP, slide the **Autosend Passcode** button to the right. The Purple color indicates the Push OTP is activated. 



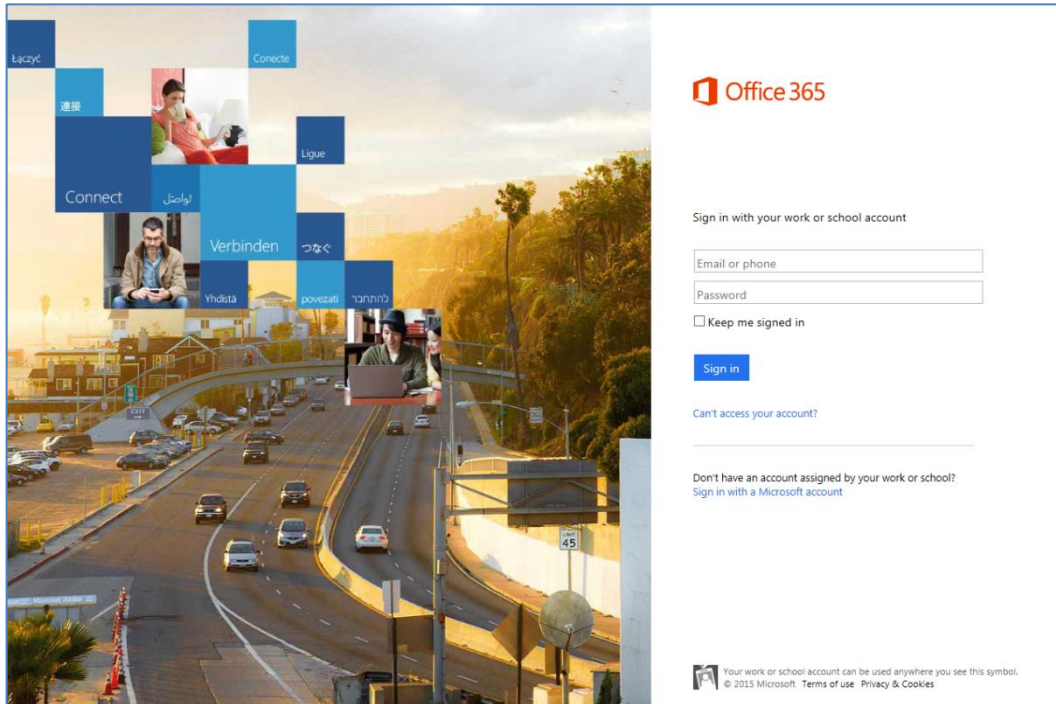
- b. To deactivate Push OTP, slide the **Autosend Passcode** button to the left.  The grey color indicates the Push OTP is deactivated.

Logging in with Push OTP

The following description uses Microsoft Office 365 as an example. The login steps may vary for other resources.

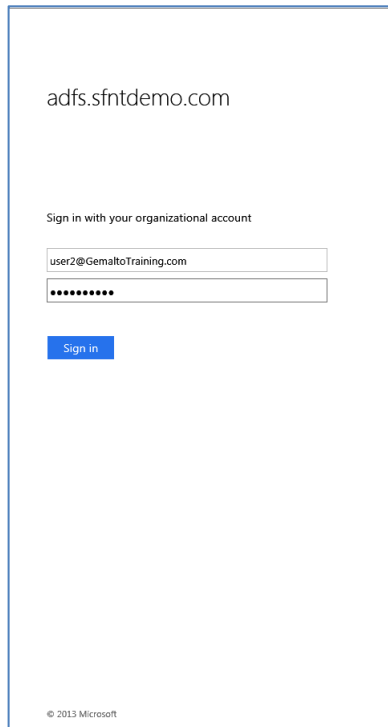
To log in with Push OTP:

1. Open the login page of the resource you wish to access and enter your organization username and password.



You are redirected to your organization's login page.

2. Enter your login credentials and click **Sign in**.



adfs.sfntdemo.com

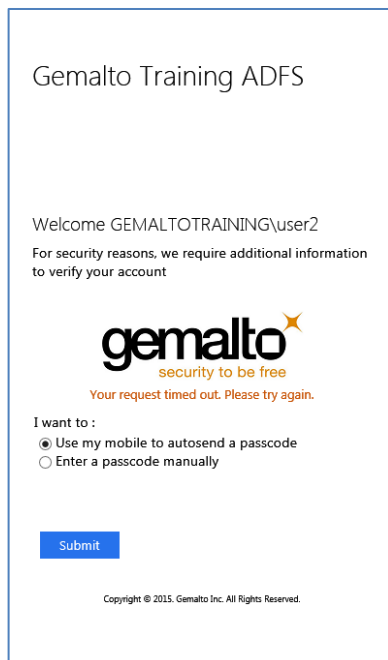
Sign in with your organizational account

user2@GemaltoTraining.com

Sign in

© 2013 Microsoft

3. Select **Use my mobile to autosend a password** and click **Submit**.



Gemalto Training ADFS

Welcome GEMALTOTRAINING\user2

For security reasons, we require additional information to verify your account

gemalto
security to be free
Your request timed out. Please try again.

I want to :

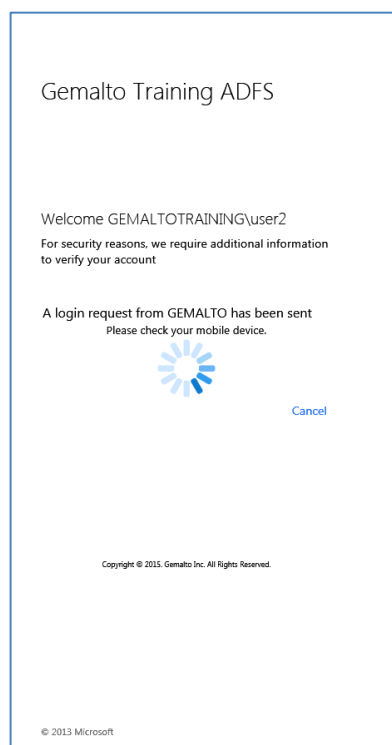
☒ Use my mobile to autosend a passcode

☐ Enter a passcode manually

Submit

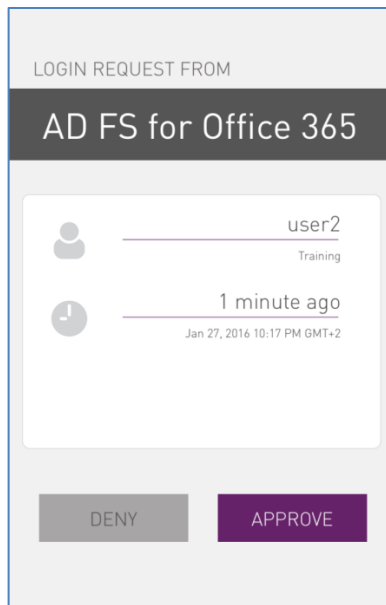
Copyright © 2015. Gemalto Inc. All Rights Reserved.

A notification of the login request is sent to your mobile device.



4. When the login request notification arrives on your mobile device, you can respond in one of the following ways:

Notification Location	Action to approve the Push OTP login request
Android Locked Screen	<p>Do one of the following:</p> <ul style="list-style-type: none"> Swipe the notification from right to left to expand it, and tap APPROVE. Single tap on the notification to open the login request in SafeNet MobilePASS+, review the login request information, and tap APPROVE.
SafeNet MobilePASS+ Application	<ol style="list-style-type: none"> Tap the Pending Notification bar. <div data-bbox="532 1409 919 1495" data-label="Image"> </div> Tap APPROVE. <p>Note: If there are multiple login requests pending, tapping the Pending Notification bar will prompt the user to approve or deny the most recent notification. Earlier notifications will remain in the bar.</p>

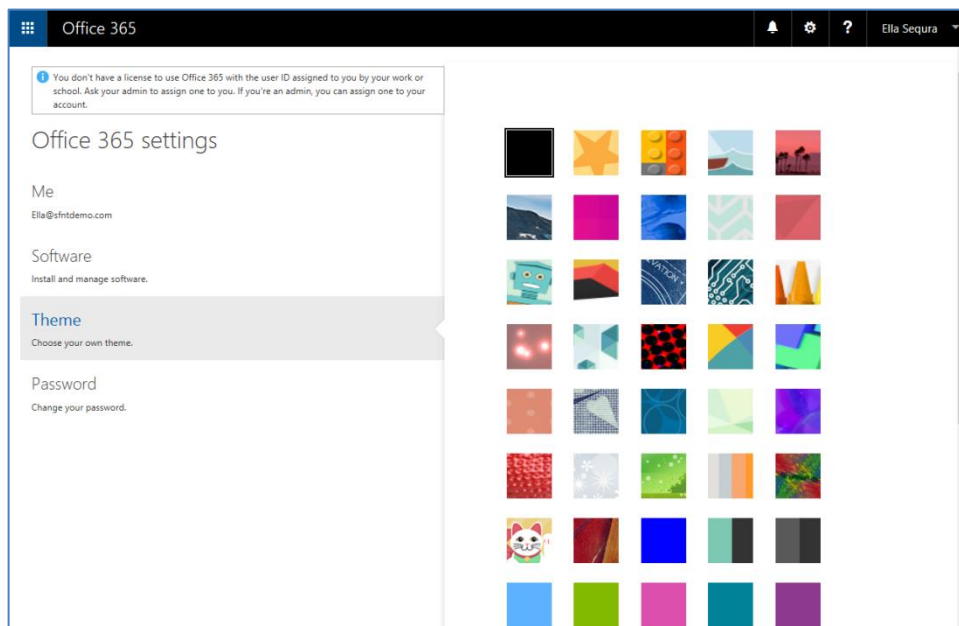


NOTE: If you receive an unexpected request, tap **DENY**, and then tap **'It wasn't me!'** This will send a notification of the unauthorized login attempt to your organization's authentication management system.

3. If prompted, enter the SafeNet MobilePASS+ PIN and tap **Continue**.

SafeNet MobilePASS+ sends a passcode to the login page.

You are now logged in.



Changing a Token PIN

Changing a Token PIN




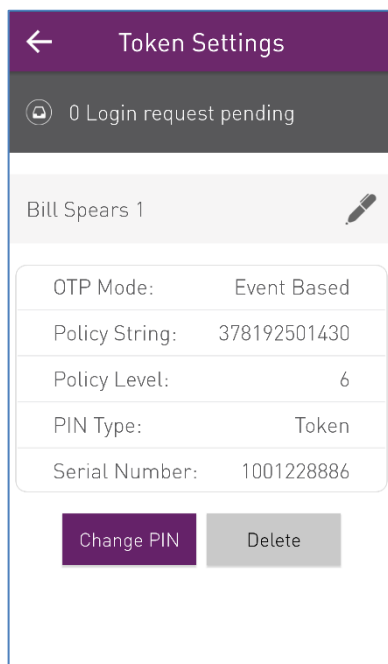
NOTE: The **Change Token PIN** option is available only if your SafeNet MobilePASS+ token has been configured for user-selected PIN protection.

You are allowed only a certain number of attempts to enter the correct PIN (depending on how many permitted retries your administrator has defined). If you exceed the number of allowed retries, your token must be re-enrolled.

The PIN entered must be in accordance with the policy set by your system administrator. For example, the minimum length and character types required.

To change the PIN:

1. Open SafeNet MobilePASS+ app.
2. Tap the Settings icon .
3. Tap **CHANGE PIN**.



4. In the **CHANGE TOKEN PIN** screen, enter the **Current PIN**.
5. Enter the new PIN in the **NEW PIN** field, enter again in **Confirm new PIN**, and then tap **SUBMIT**.

Change Token PIN

Current PIN

New PIN

Confirm new PIN

Cancel Submit

PIN Type: Token




1	2	3
4	5	6
7	8	9
	0	⬅ X

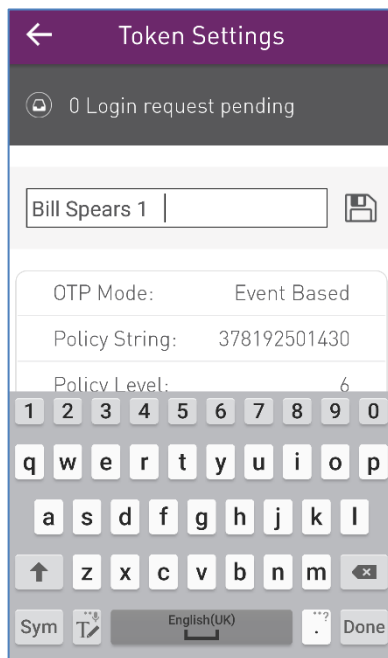
The token PIN has been changed.

Renaming and Deleting a Token

Renaming a Token


To rename a token:

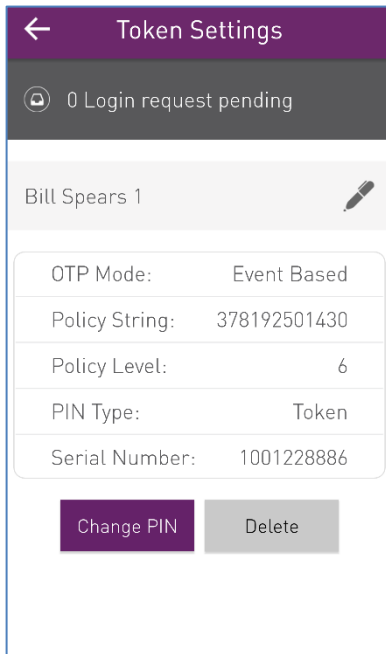
1. Open the SafeNet MobilePASS+ app.
2. Tap the Configuration icon  next to the token you want to rename.
3. Click the Edit icon , type in the new name and click the Save icon .



Deleting a Token

To delete a token:

1. Open the SafeNet MobilePASS+ app.
2. Tap the Configuration icon .
3. Tap **DELETE**.



4. When prompted to confirm the removal of the token, tap **DELETE**.

Viewing Token, App, and Log Information


Viewing Token Information

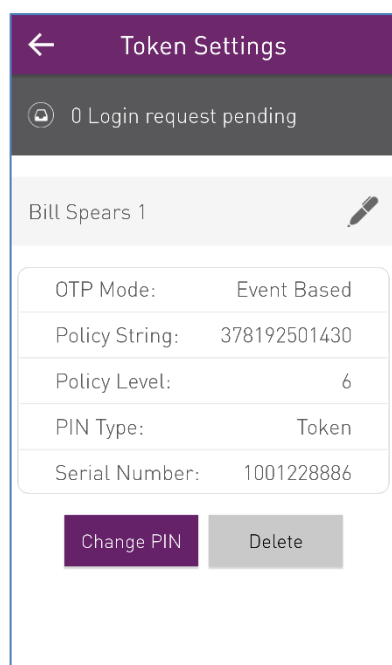


NOTE: You may be asked to supply token information by Help Desk or IT staff when dealing with a support request.

To view token information:

1. Open the SafeNet MobilePASS+ app.

2. Tap the Configuration icon .




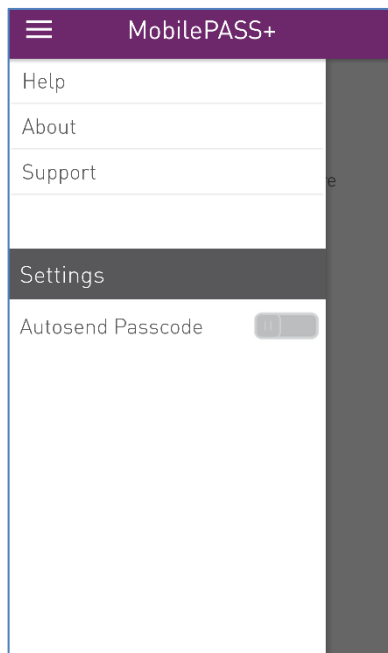
The following token information is displayed:

- **OTP Mode** - displays the system for passcode generation (Time-based or Event-Based).
- **Policy String** - identifies the SafeNet MobilePASS+ policy.
- **Policy Level** - represents the token generation, reflecting changes in the token structure and characteristics.
- **PIN Type** - indicates the type of PIN (None/Token/Server)
- **Serial Number** - a unique identifier for the token

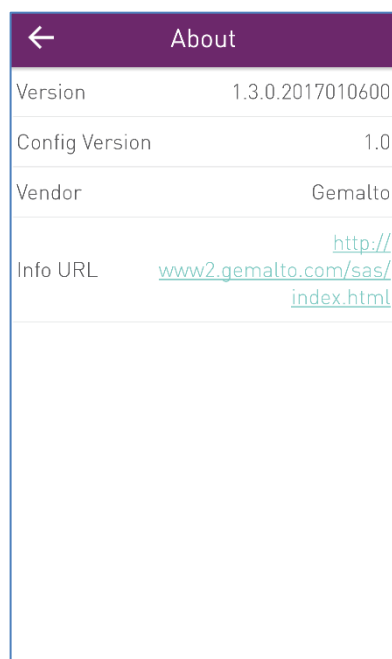
Viewing SafeNet MobilePASS+ App Information

To view SafeNet MobilePASS+ app Information:

1. Select the Menu icon 
2. Tap **About**.




Information about the SafeNet MobilePASS+ app is displayed.

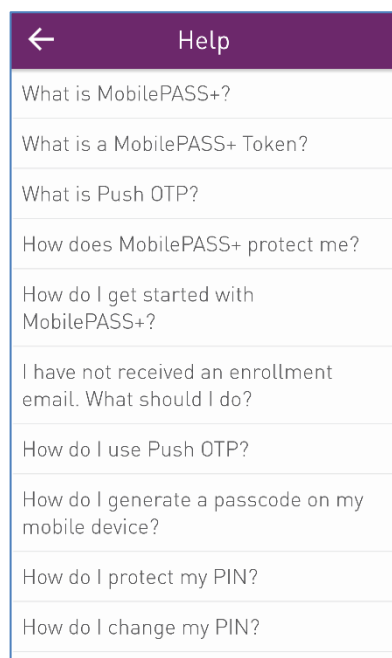


Viewing Help Topics

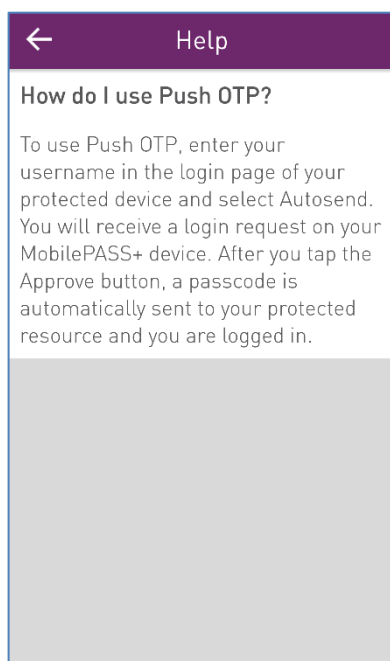
To view Help topics:

1. Tap the Menu icon .
2. Tap **Help**.

A list of help topics describing the use of the SafeNet MobilePASS+ app and token are displayed.




3. Tap on the required topic. The information is displayed.

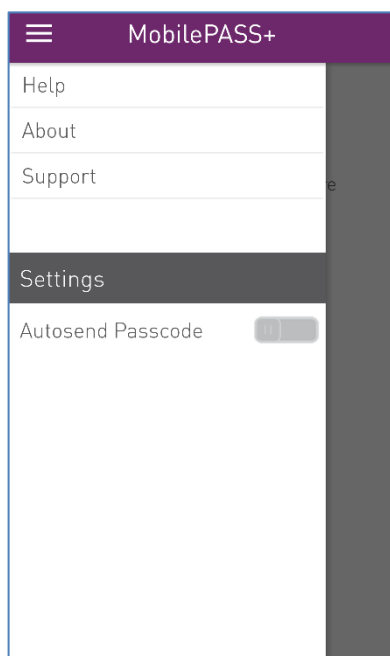


Viewing Token Enrollment Log

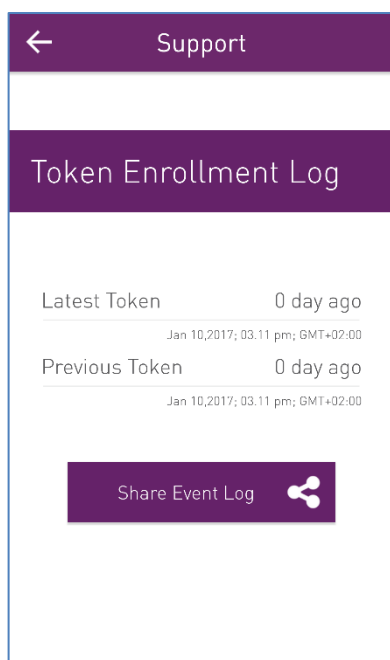
You can view a log of SafeNet MobilePASS+ events, and can send a file of the log to a recipient. This may be requested by your Help Desk to assist in resolving an issue.

To view the Token Enrollment Log:

1. Open the SafeNet MobilePASS+ app and tap the **Menu Icon** 
2. Tap **Support**.



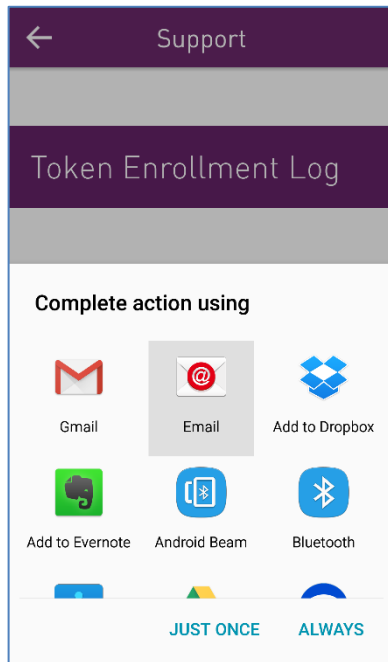
3. To share the log, click **Share Event Log**.



4. Select an email application.

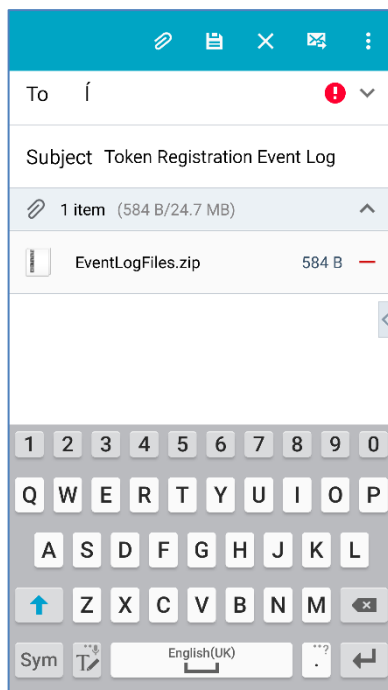


NOTE: Use an email application to send the log file. Other types of applications are not supported for this purpose.



A zip file of the log is attached to the email message.

5. Enter the email address, type a message (if required), and send.



Frequently Asked Questions

As a SafeNet MobilePASS+ user, you can generate passcodes on your device, and use those passcodes to authenticate to protected corporate and web-based applications.

SafeNet MobilePASS+ allows secure remote access to corporate and web-based applications. An integrated support feature allows your company's system administrator to manage it directly from a token management application.

What is a SafeNet MobilePASS+ Token?

SafeNet MobilePASS+ is a mobile application that generates an OTP (One-Time Password), also referred to as a passcode, to use for secure remote access to corporate and web-based applications. It works independently of mobile network connectivity.

How does SafeNet MobilePASS+ protect me?

Password theft is the method used most frequently by thieves and hackers to steal identities and gain unauthorized access to computer networks. While they have many ways to steal a password, success depends on the stolen password being valid, in much the same way that credit card theft relies on the card being usable until you report it missing. SafeNet MobilePASS+ prevents the stolen password being used to log in to the protected network, even if you and your company's security professionals are unaware that it has been stolen, because immediately after logging on, the generated passcode stops being valid. Any attempt to login by reusing the passcode will fail, and will alert your network security professionals to the possibility that your identity has been stolen.

How do I generate a passcode on my mobile device?

After installing SafeNet MobilePASS+ on your mobile device, use the application to generate a passcode. You may be required to enter a PIN before generating the passcode.

How do I get started with SafeNet MobilePASS+?

After the installation of the application on your mobile, the first operation is to activate a token. There are three possible ways to do that:

Automatic self-enrolment - You will receive a self-enrollment email from your company which contains a link to the self-enrollment web site and instructions for installing, enrolling and activating your token.

QR Code Enrollment – The self-enrollment email includes a link to a webpage containing a QR Code. Scan the QR Code to enroll your SafeNet MobilePASS+ token. This is recommended when you cannot receive email or open self-enrollment from the target device.

Manual enrolment - Copy the activation code included in the self-enrollment email and paste it to your SafeNet MobilePASS+ app.

I have not received an enrollment email, what should I do?

If you have not received your self-enrollment email, contact your system administrator to arrange for a new self-enrollment email to be sent.

For how long will my token continue to operate?

Your token will be able to generate passcodes until it is revoked by your security administrator.

What is self-enrollment?

Self-enrollment is the process of activating your token. You must complete this process before using your SafeNet MobilePASS+ token to login.

What are the benefits of using the token?

SafeNet MobilePASS+ enables you to access corporate and web-based resources securely. In addition, it will reduce or eliminate the need to remember or periodically change your login passwords, as your token will do this for you.

How do I protect my security PIN?

If your SafeNet MobilePASS+ token is configured to use a PIN, protect it as you would the PIN for your credit card. Never share it with anybody. Your network security administrator and help desk will never ask for your PIN and you should never reveal it to them. Never write down your PIN.

What should I do if I cannot log in using my token?

The most common cause of failed login is entering an incorrect passcode. Ensure that you enter the code exactly as displayed on the token, including any punctuation, and upper and lower case letters. Never attempt to

reuse a passcode. Your account will automatically lock for a period if you exceed the allowed number of consecutive failed login attempts. You must wait for the required period of time before your account becomes active again. Contact your company's help desk to resolve login problems.

What is Push OTP?

The SafeNet MobilePASS+ Push OTP feature enables you to authenticate with a single tap, eliminating the need to generate manually a passcode on your mobile device, or to enter the passcode manually in the login page of your protected resource (website or network).

How do I use Push OTP?

To use Push OTP, enter your username in the login page of your protected device and select Autosend. You will receive a login request on your SafeNet MobilePASS+ app. After you tap the Approve button, a passcode is automatically sent to your protected resource and you are logged in.

11

Terminology

Term	Description
Activation String or code	The activation string is sent to the SafeNet MobilePASS+ user, who uses it to activate the application and add tokens.
Autosend	The term used to identify push notification based passcode delivery.
Biometric PIN	<p>Biometric refers to metrics as related to human characteristics. In MobilePASS+, the human characteristic in question is a fingerprint, which can be used to access the app and tokens, as an alternative to manually entering a PIN.</p> <p>See also:</p> <p>PIN (Personal Identity Number), on page 51.</p> <p>Fingerprint Sensor, on page 50.</p>
Challenge-Response or OCRA (OATH Challenge-Response Algorithm)	A family of protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated. If SafeNet MobilePASS+ is configured to work with Challenge-Response, the user is sent the challenge code. The user then enters the code into the token, taps the Challenge-Response button, and the passcode (the response) is displayed.
Enrollment	Enrollment is the process of adding a SafeNet MobilePASS+ token to the SafeNet MobilePASS+ app and making it active.
Event-Based Tokens	Event-based tokens generate passcodes when a particular event occurs; typically, when the user presses a button or taps an icon. The passcode generated by an event-based token is valid until another passcode is generated.
Fingerprint Sensor	<p>A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. MobilePASS+ utilizes a fingerprint sensor on the device when using the Biometric PIN feature.</p> <p>See also:</p> <p>Biometric PIN, on page 50</p> <p>PIN (Personal Identity Number), on page 51.</p>
SafeNet MobilePASS+ App	<p>The SafeNet MobilePASS+ application turns a mobile phone into a two-factor authentication device, removing the need to carry an additional hardware token.</p> <p>As a SafeNet MobilePASS+ user, you can generate passcodes on your mobile device, and use those passcodes to authenticate to protected corporate and web-based applications.</p>

Term	Description
SafeNet MobilePASS+ Token	A SafeNet MobilePASS+ token is related to an account and its associated parameters, such as name, user PIN, enrolled keys, and PIN policy. Each SafeNet MobilePASS+ app can manage multiple SafeNet MobilePASS+ tokens. For example, a user may require several tokens, each one related to a different web service.
OTP (One Time Password)	An OTP is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. Passcode is the preferred term in SafeNet MobilePASS+ applications and documentation, and is identical to OTP.
Passcode	The Passcode is the password generated by the SafeNet MobilePASS+ token for authenticating to a protected web or network resource. If the token is configured for a time-based OTP, the password is active for a limited period, and can be used once only, preventing access to unauthorized users, even if stolen. If the token is set up as event-based, the passcode is valid until another passcode is generated
PIN (Personal Identity Number)	If so configured, SafeNet MobilePASS+ app requires the user to enter a PIN to use the application. This provides an additional layer of protection, preventing unauthorized users from using the application.
Protected Resource	A Protected Resource is any part of a computer system or network, such as a web, cloud, or VPN, requiring authentication to enable access.
Push OTP	With Push OTP technology, when accessing a protected resource, a push notification is sent to the user's device. The user approves the request with a single tap of a button. A new OTP is automatically generated by the SafeNet MobilePASS+ app and sent to the protected resource, eliminating the need to generate manually a one-time passcode (OTP) on a mobile device or to enter the OTP passcode in the login page.
QR Code	Quick Response (QR) Code is a two dimensional barcode, a machine readable optical label. SafeNet MobilePASS+ can use the smartphone's camera as an imaging device to scan a QR Code containing the information required to perform token enrollment.
Software Token	A software token is a two-factor authentication security application that is used to authorize the use of computer services. SafeNet MobilePASS+ application is an example of a software token. By contrast, a hardware token is a physical device that needs to be connected to the computer by, for example, a USB connection, to enable authentication.
Time-Based Tokens	Time-Based tokens generate passcodes at pre-set time intervals. When a new passcode is generated, the previous passcode is no longer valid. SafeNet MobilePASS+ token can be configured to operate as a time based token.

12

References

Related Documents

The following documents contain related or additional information:

SafeNet MobilePASS+

SafeNet MobilePASS+ for Android Customer Release Notes (CRN)

SafeNet MobilePASS+ for iOS Customer Release Notes (CRN)

SafeNet MobilePASS+ for iOS User Guide