SafeNet MobilePASS
Version 8.2.0, Revision B

User Guide
Preface

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person of organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

4690 Millennium Drive
Belcamp, Maryland 21017, USA

Disclaimers

The foregoing integration was performed and tested only with specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

This product contains software that is subject to various public licenses. The source code form of such software and all derivative forms thereof can be copied from the following website: http://c3.safenet-inc.com/

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Technical Support

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, please contact your supplier or SafeNet support.

SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:

Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com
# Table of Contents

Chapter 1  SafeNet MobilePASS Overview ............................................................................................................................................. 5
Chapter 2  Installing and upgrading MobilePASS for BlackBerry ........................................................................................................ 8
Chapter 3  Configuring and upgrading MobilePASS for Windows Desktop ...................................................................................... 20
Chapter 4  Configuring and upgrading MobilePASS for iOS ........................................................................................................ 32
Chapter 5  Configuring and upgrading MobilePASS for Android ................................................................................................ 41
Appendix  Troubleshooting ....................................................................................................................................................................... 51
Chapter 1  SafeNet MobilePASS Overview

This document provides instructions for installing, upgrading, and running the MobilePASS solution on your mobile device or desktop machine.

Introduction

Software tokens allow users to generate OTPs (One-Time-Passcodes) on their personal mobile devices and Desktops/Laptops. The Software tokens are compatible with SafeWord 2008, SafeNet Authentication Manager, and SafeWord Premier Access (for Solaris), and enable secure remote access to corporate and web-based applications. An integrated support feature allows administration directly from the SafeWord management interface. The MobilePASS Enrollment Portal allows users to enroll, activate, and use their tokens without administrative assistance. The MobilePASS product was integrated into SafeWord 2008 beginning in version 2.1.0.03, in SafeNet Authentication Manager 8.0 SP3, and in SafeWord PremierAccess (for Solaris) beginning in version 3.2.1.05.

What's new in this version?

MobilePASS 8.2 offers several significant new features, and an enhanced application interface:

- Superior deployment and management: MobilePASS 8.2 offers automatic one-step installation and policy-based activation, which determines the token configuration. This translates into simplified deployment processes, and reduced IT administration.
- Optimized security: Sophisticated security capabilities, including standards-based activation and dynamic seeding offer enhanced security.

New features include:

Configurable Token with Policy-based Activation

- Time-sync and event-based one-time-passcodes
- Challenge response-based one-time-passcodes
- Configurable PIN and token policy
- Multi-token support – use the same application to create and manage several tokens.

Easy to Manage Deployment Model

- Automatic one-step installation and activation – no need to activate on an external Web portal
- Policy-based activation determines token configuration
- BES one-click installation and activation (feature is available on BlackBerry devices only)

Enhanced Security

- Ability to set strong alphanumeric token PINs
- Highly secure standards-based activation
- Dynamic re-seeding means organizations control their own seed data
Workflow examples

The following are examples of the two workflows that occur when MobilePASS is launched. The first example illustrates the process that occurs when the application is launched for the first time. The second example illustrates the process upon subsequent application launches.

First application launch
Subsequent application launches

1. Launch Application
2. Single Token
   - Yes: PIN Authentication
   - No: Token List
3. Token List
   - Select Token
4. PIN Authentication
   - No: PIN Match
5. PIN Match
   - Yes: Enter Challenge
   - No: OTP Passcode Screen
6. Enter Challenge
   - Yes: C-R Token
   - No: OTP Passcode Screen
7. C-R Token
   - Yes: Token Settings
   - No: OTP Passcode Screen
8. Token Settings
   - Token Information
   - Edit Token Name
   - Change Token PIN
   - Deactivate Token
   - Delete Token
Chapter 2  Installing and upgrading MobilePASS for BlackBerry

This chapter includes sections describing how to install MobilePASS for BlackBerry and how to upgrade from an existing version.

Installing MobilePASS for BlackBerry

MobilePASS for BlackBerry allows users to automatically activate and enroll their software tokens over Wi-Fi and wireless networks using the MobilePASS application. MobilePASS for BlackBerry can be downloaded and installed directly to devices running BlackBerry OS version 4.6 and higher. MobilePASS for BlackBerry software tokens can be deployed:

- Over-the-air OTA via the SafeNet-hosted server
- OTA via your own internally-hosted server (providing for version control)
- Via the BlackBerry Desktop Manager

The BES policy configuration is not available when deploying with Desktop Manager.

- Via BlackBerry Enterprise Server (BES) application push.

The Automatic Authentication feature is only available for BES deployments.

The MobilePASS application is available at http://www.safenet-inc.com/GetMP. The zipped file includes folders for OTA, Desktop and BES packages. The MobilePASS for BlackBerry zip consists of a combination of the following files:

- MobilePASS.cod
- MobilePASS.jad
- MobilePASS.alx.

Files are combined based on how the software will be installed on the BlackBerry device. If installing OTA, the MobilePASS.cod file and the MobilePASS.jad file should be used. If installing via the Desktop Manager, the MobilePASS.cod file and the MobilePASS.alx file should be used. To distribute MobilePASS for BlackBerry, do the following:

1. Determine how BlackBerry device users will download the MobilePASS for BlackBerry application to their device.
2. Configure the appropriate files and/or policies if users will automatically enroll with the automatic authentication feature on or off with their tokens.
3. Post the appropriate files to a location where users can access them, and then inform your MobilePASS for BlackBerry users that the software is available for downloading and installing.

Administrators may install the MobilePASS for BlackBerry software onto the device themselves, and then distribute the device to the user. This method is convenient when there are a small number of users.

Once installed, the MobilePASS application will be visible on the BlackBerry device as seen in the screenshots below.
Enrolling your token

MobilePASS 8.2 can be enrolled via automatic or manual enrollment. MobilePASS 8.2 retains the enrollment parameters previously supported in earlier 3.2.1.x, 8.x versions of MobilePASS. For more details, refer to Chapter 2 of the SafeNet MobilePASS Software Administration Guide.

To enroll and activate your token with MobilePASS 8.2:

1. Open the MobilePASS application on your device.
2. Tap the “Continue” button after reading the welcome message.
3. Enter a token name, and then press “Activate”.
4. Choose automatic or manual enrollment. If you select automatic enrollment, continue the next step. If you select manual enrollment, proceed to step 6.

5. For automatic enrollment, do the following:
   a. Enter the MobilePASS Enrollment Portal URL using the following format: https://<servername:port>/portal/enroll.
   b. Press the “Continue” button.
c. Enter your User ID and Password, and then press “Continue”.

d. Upon successful automatic enrollment, the Create a PIN window appears. If you are using a PIN with this token, continue to the step 7. If no PIN is required, skip to step 9.
6. When manual enrollment is selected, the Token Policy String window appears. Enter the policy provided by your administrator, and then press “Continue”. If no policy was provided, press “Continue”.

   a. The Confirm Activation window appears displaying the activation code. Enter the activation code onto the MobilePASS Enrollment Portal to complete enrollment.

   b. Press “Continue” on the device.

   c. If you are using a PIN with this token, continue to the next step. If no PIN is required, skip to Generating one-time-passcodes.

**Defining a protection PIN**

7. If your administrator has chosen to require a protection PIN with this token, do the following:

   a. Enter a four, six, or eight digit numeric or alphanumeric PIN to use with this token into the Token PIN field, and then press “Continue”.

   b. Re-enter the same PIN in the Re-enter Token PIN field, and then press “Continue”. Your one-time-passcode appears.
Generating one-time-passcodes

Your token is now activated. To generate another passcode, press “Generate Passcode”.

Generating passcodes with challenge-response tokens

1. If you are using a challenge-response token, enter the challenge provided on the Enrollment Portal into the Challenge Code field.
2. Press “Generate Passcode”. The passcode appears.
Generating passcodes with time-based tokens

If you are using a time-based token, the one-time-passcode is automatically generated after the specified time interval has elapsed.
Upgrading MobilePASS for BlackBerry

Install MobilePASS 8.2 via OTA, BES, or the BlackBerry Desktop Manager. When the upgrade is complete, MobilePASS displays on the device or desktop with the upgraded icon.

Using your previously-activated token

Your previously-activated token is automatically imported when the MobilePASS software is upgraded. The token is renamed SafeNet MobilePASS. This name can be changed at any time by choosing the “Edit Token” option in the MobilePASS application.
Using your previously-set token PIN

Your MobilePASS token starts automatically when you open the MobilePASS application. When the application opens, you are prompted to enter your token PIN.

1. Enter the token PIN you used with the previous version of MobilePASS, and then press “Continue”.

2. Your new passcode appears. To generate another passcode, press “Generate Passcode”.
For Challenge Response tokens:

1. For a challenge-response-type token, enter the challenge provided on the Enrollment Portal into the Challenge Code field.
2. Press “Generate Passcode”. The passcode appears.

If you are using time-based token, the one-time-passcode is automatically generated after the time interval has elapsed.
Using the new navigation controls

Viewing application information

To view the application information:

1. Open the MobilePASS application on the device.
2. Select “Information” from the menu options. The application information appears.

Viewing token information

To view token information:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN to authenticate.
3. Select “Token Information” from the menu options. The token information appears.
Changing token PIN

To change your PIN, ensure that the token is activated, and then do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change PIN” from the menu options.
4. Enter your current PIN and press “Continue”. The Enter your new PIN window appears.
5. Enter and confirm the new PIN that you will use with the token. You have successfully reset the PIN.

The Attack-Lock feature will deactivate your token as per the token policy on entering the wrong PIN consecutively. When the token is deactivated, you will need to reactivate it.

Changing the token name

To change the token name, do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change Token Name” from the menu options.
4. Enter your new token name and then press “Continue”. You have successfully changed the token name.

The token name change is not permitted if token has been activated using auto-enrollment.

Deactivating the token

There will be instances when you will need to deactivate your token back to its original state.

Before deactivating tokens, contact your administrator. Unless re-enrollment privileges are enabled, you cannot reenroll your token until the administrator removes the token from your record.

To deactivate the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Deactivate Token” from the menu options.
4. Read the warning, and then press “Deactivate”. You have successfully deactivated your MobilePASS token.

Deleting the token

There will be instances when you will need to delete your token. To delete the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Delete Token” from the menu options.
4. Read the warning, and then press “Delete”. You have successfully deleted your MobilePASS token.
Chapter 3 Configuring and upgrading MobilePASS for Windows Desktop

This chapter describes configuring and upgrading MobilePASS for Windows Desktop.

Configuring MobilePASS for Windows Desktops

Configuring MobilePASS for Windows Desktop for the first time

The MobilePASS for Windows Desktop application works with Windows XP, Windows Vista, and Windows 7. It is available at http://www.safenet-inc.com/GetMP. Once downloaded, the MobilePASS application will be visible on the Windows Desktop. Double-click the icon to open the application. The Welcome window appears.

1. Click “Continue”. The Create a New Token window appears.

2. Enter a name for the token, and then click “Activate”.

Welcome to MobilePASS
Press 'Continue' to create, enroll, and activate a new token.

Continue
Cancel

Create New Token
New token name
Demo

Activate
Activate Later
Cancel
3. Select the Auto Enrollment button or the Manual Enrollment button. If you select automatic enrollment, continue to the next step. If you select manual enrollment, proceed to step 5.

4. For automatic enrollment, do the following:
   a) Enter the MobilePASS Enrollment Portal URL using the following format: https://<servername:port>/portal/enroll.
   b) Click the "Continue" button.
c. Enter your User ID and Password, and then click “Continue”.

d. Upon successful automatic enrollment, the Create a PIN window appears. If you are using a PIN with this token, continue to “Defining a protection PIN”. If no PIN is required, skip to step 6.

5. When manual enrollment is selected, the Token Policy String window appears. Enter the policy provided by your administrator, and then click “Continue”. If no policy was provided, click “Continue”.

User Guide
6. The Confirm Activation window appears displaying the activation code, click "Continue" to activate the token. If you are using a PIN with this token, continue to Defining a protection PIN. If no PIN is required, skip to Generating one-time-passcodes.

If you are using a PIN with this token, continue to Defining a protection PIN. If no PIN is required, skip to Generating one-time-passcodes.

Defining a protection PIN

If your administrator has chosen to require a protection PIN with this token, do the following:

1. Enter a four, six, or eight digit numeric or alphanumeric PIN to use with this token into the Token PIN field, and then click "Continue".
2. Re-enter the same PIN in the Re-enter Token PIN field, and then click “Continue”. Your one-time-passcode appears.

**Generating one-time-passcodes**

Your token is now activated. To generate another passcode, click “Generate Passcode”.
Generating passcodes with challenge-response tokens

To generate passcodes with challenge-response tokens, do the following:

1. If you are using a challenge-response type token, enter the challenge provided.
2. Click “Generate Passcode”. The passcode appears.

Generating passcodes with time-based tokens

If you are using time-based token, a new one-time-passcode is automatically generated after the specified time interval has elapsed.
Upgrading MobilePASS for Windows Desktops

To upgrade MobilePASS for Windows Desktop, download the latest version from the SafeNet Support site or from your administrator.

**Note:** MobilePASS for Windows Desktop does not have an installer. It is an application that is downloaded. If you already have MobilePASS 8.0 installed, and you then download MobilePASS 8.2, the versions can coexist. To prevent token corruption and possibly reactivating the token, we recommend users remove MobilePASS 8.0 once they begin using MobilePASS 8.2.

Using your previously-activated token

Your previously-activated token is automatically imported when the MobilePASS software is upgraded. The token is renamed SafeNet MobilePASS. This name can be changed at any time by choosing the “Edit Token” option in the MobilePASS application.
Using your previously-set token PIN

Your MobilePASS token starts automatically when you open the MobilePASS application. When the application opens, you are prompted to enter your token PIN.

1. Enter the token PIN you used with the previous version of MobilePASS, and then press “Continue”.

2. Your new passcode appears. To generate another passcode, press “Generate Passcode”.

---

**User Guide**

27
Using the new navigation controls

![MobilePASS interface]

- Application or token name
- Token tasks menu
- Application information
- Add a new token
- List of tokens

![Detailed view of a token]

- Back to previous screen or token list
- Token Information
- Change token name
- Change token PIN
- Deactivate token
- Delete token
**Viewing application information**

To view the application information:

1. Open the MobilePASS application on the device.
2. Select the Information “i” icon from the right-side menu options. The application information appears.

**Viewing token information**

To view token information:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN to authenticate.
3. Select “Token Information” from the menu options. The token information appears.
Changing token PIN

To change your PIN, ensure that the token is activated, and then do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change PIN” from the menu options.
4. Enter your current PIN and press “Continue”. The Enter your new PIN window appears.
5. Enter and confirm the new PIN that you will use with the token. You have successfully reset the PIN.

The Attack-Lock feature will deactivate your token as per the token policy on entering the wrong PIN consecutively. When the token is deactivated, you will need to reactivate it.

Changing the token name

To change the token name, do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change Token Name” from the menu options.
4. Enter your new token name and then press “Continue”. You have successfully changed the token name.

The token name change is not permitted if token has been activated using auto-enrollment.

Deactivating the token

There will be instances when you will need to reset your token back to its original state.

Before deactivating tokens, contact your administrator. Unless re-enrollment privileges are enabled, you cannot reenroll your token until the administrator removes the token from your record.

To deactivate the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Deactivate Token” from the menu options.
4. Read the warning, and then press “Deactivate”. You have successfully deactivated your MobilePASS token.
Deleting the token

There will be instances when you will need to delete your token. To delete the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Delete Token” from the menu options.
4. Read the warning, and then press “Delete”. You have successfully deleted your MobilePASS token.
Chapter 4 Configuring and upgrading MobilePASS for iOS

This chapter describes configuring and upgrading MobilePASS for iOS.

Configuring MobilePASS for iOS

Download the application from the Apple App store.

Enrolling your token

Once downloaded, the MobilePASS application will be visible on the Apple device.

Press the icon to open the application. The Token Enrollment window appears. A default token named “My Token 1” is automatically created.

1. Select the Auto Enrollment button or the Manual Enrollment button. If you select automatic enrollment, continue to the next step. If you select manual enrollment, proceed to step 3.
2. For automatic enrollment, do the following:
   a. Enter the MobilePASS Enrollment Portal URL using the following format: \texttt{https://<servername:port>/portal/enroll}.
   b. Enter your User ID and Password, and then press “Continue”.
   c. Upon successful enrollment, the Create a PIN window appears. If you are using a PIN with this token, continue to “Setting a token PIN”. If you are not using a PIN with the token, skip to “Generating one-time passcodes”.

3. For manual enrollment, the Token Policy String window appears. Enter the policy provided by your administrator, and then press “Continue”. If no policy was provided, press “Continue”. The Activation Code window appears.

4. To activate the token, do the following:
   a. Enter the activation code onto the Enrollment Portal to complete enrollment.
   b. Press “Continue” on the device.
   c. If you are using a PIN with this token, continue to the next step. If no PIN is required, skip to “Generating one-time passcodes”.
Defining a protection PIN

Tokens created with MobilePASS 8.2.0 or later version software support both simple numeric protection PINs, and more complex, stronger alphanumeric protection PINs. The numeric keypad is the default keyboard option. For stronger PIN protection, the alphanumeric keyboard option is available by selecting the ABC key on the lower left corner of the keypad.

If your administrator has chosen to require a protection PIN with this token, continue to the next step. If no PIN is required, skip to “Generating one-time-passcodes”.

1. Enter a four-, six-, or eight-digit numeric or alphanumeric PIN to use with this token into the Token PIN field.

2. Re-enter the PIN in the Re-enter Token PIN field.
Generating one-time-passcodes

Your token is now activated. To generate another passcode, press “Generate Passcode”.

Generating passcodes with challenge-response tokens

If you are using a challenge-response type token, do the following:

1. Enter the challenge provided on the Enrollment Portal into the Challenge Code field on the device.
2. Press “Generate Passcode”. The passcode appears. To generate another passcode press “Next Challenge”, and then repeat this process.
Generating passcodes with time-based tokens

If you are using a time-based token, the one-time-passcode is automatically generated after the specified time interval has elapsed.
Upgrading MobilePASS for iOS

To upgrade MobilePASS, download the latest version from the App Store. Press the SafeNet icon to install the upgrade. The upgrade is automatically installed.

Note: iOS does not have an installer. It is an application that is downloaded. If you already have MobilePASS 8.0 installed, and then you download MobilePASS 8.2, the upgrade will automatically override your older version software.

Using your previously-set token PIN

Your MobilePASS token starts automatically when you press the MobilePASS application. When the application opens, you are prompted to enter your token PIN.

1. Enter the token PIN you used with the previous version of MobilePASS, and then press “Continue”.

![Token PIN Entry Screen](image-url)
2. Your new passcode appears. To generate another passcode, press “Generate Passcode”.
Using the new navigation controls

Viewing application information
To view the application information:

1. Open the MobilePASS application on the device.
2. Select the Information “i” icon from the right-side menu options. The application information appears.

Viewing token information
To view token information:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN to authenticate.
3. Select “Token Information” from the menu options. The token information appears.
Changing token PIN

To change your PIN, ensure that the token is activated, and then do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change PIN” from the menu options.
4. Enter your current PIN and press “Continue”. The Enter your new PIN window appears.
5. Enter and confirm the new PIN that you will use with the token. You have successfully reset the PIN.

*The Attack-Lock feature will deactivate your token as per the token policy on entering the wrong PIN consecutively. When the token is deactivated, you will need to reactivate it.*

Changing the token name

To change the token name, do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change Token Name” from the menu options.
4. Enter your new token name and then press “Continue”. You have successfully changed the token name.

*The token name change is not permitted if token has been activated using auto-enrollment.*

Deactivating the token

There will be instances when you will need to your token back to its original state.

*Before deactivating tokens, contact your administrator. Unless re-enrollment privileges are enabled, you cannot reenroll your token until the administrator removes the token from your record.*

To deactivate the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Deactivate Token” from the menu options.
4. Read the warning, and then press “Deactivate”. You have successfully deactivated your MobilePASS token.

Deleting the token

There will be instances when you will need to delete your token. To delete the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Delete Token” from the menu options.
4. Read the warning, and then press “Delete”. You have successfully deleted your MobilePASS token.
Chapter 5  Configuring and upgrading MobilePASS for Android

This chapter describes configuring and upgrading MobilePASS for Android.

Configuring MobilePASS for Android

Download the application from the Google Play store.

Enrolling your token

Once downloaded, the MobilePASS application will be visible on the Android desktop or device.

Press the icon to open the application. The Token Enrollment window appears. A default token named “My Token 1” is automatically created.

1. Select the Auto Enrollment button or the Manual Enrollment button. If you select automatic enrollment, continue to the next step. If you select manual enrollment, proceed to step 3.
2. For automatic enrollment, do the following:
   a. Enter the MobilePASS Enrollment Portal URL using the following format: https://<servername:port>/portal/enroll.
   b. Enter your User ID and Password, and then press “Continue”.
   c. Upon successful enrollment, the Create a PIN window appears. If you are using a PIN with this token, continue to “Setting a token PIN”. If you are not using a PIN with the token, skip to “Generating one-time passcodes”.

3. For manual enrollment, the Token Policy String window appears. Enter the policy provided by your administrator, and then press “Continue”. If no policy was provided, press “Continue”. The Activation Code window appears.

4. To activate the token, do the following:
   a. Enter the activation code onto the Enrollment Portal to complete enrollment.
   b. Press “Continue” on the device.
   c. If you are using a PIN with this token, continue to the next step. If no PIN is required, skip to “Generating one-time passcodes”.
Defining a protection PIN

Tokens created with MobilePASS 8.2.0 or later version software support both simple numeric protection PINs, and more complex, stronger alphanumeric protection PINs. The numeric keypad is the default keyboard option.

If your administrator has chosen to require a protection PIN with this token, continue to the next step. If no PIN is required, skip to “Generating one-time-passcodes”.

1. Enter a four-, six-, or eight-digit numeric or alphanumeric PIN to use with this token into the Token PIN field.

2. Re-enter the PIN in the Re-enter Token PIN field.
 Generating one-time-passcodes

Your token is now activated. To generate another passcode, press “Generate Passcode”.

 Generating passcodes with challenge-response tokens

If you are using a challenge-response type token, do the following:

1. Enter the challenge provided on the Enrollment Portal into the Challenge Code field on the device.
2. Press “Generate Passcode”. The passcode appears. To generate another passcode press “Next Challenge”, and then repeat this process.
Generating passcodes with time-based tokens

If you are using a time-based token, the one-time-passcode is automatically generated after the specified time interval has elapsed.
Upgrading MobilePASS for Android

To upgrade MobilePASS for Android, download the latest version from the Google Play store. Press the “Update” button to install the upgrade. The upgrade is automatic.

Change in icon after upgrade

Note: If you already have MobilePASS 8.0 installed, and then you download MobilePASS 8.2, the upgrade will automatically override your older version software.

Using your previously-set token PIN

Your MobilePASS token starts automatically when you press the MobilePASS application. When the application opens, you are prompted to enter your token PIN.

1. Enter the token PIN you used with the previous version of MobilePASS, and then press “Continue”. 
2. Your new passcode appears. To generate another passcode, press “Generate Passcode”.

![SafeNet MobilePASS](image)
Using the new navigation controls

Viewing application information

To view the application information:

1. Open the MobilePASS application on the device.
2. Press the standard Menu button on the device.
3. Select the Information “i” icon menu option. The application information appears.

Viewing token information

To view token information:

1. Open the MobilePASS application on the device.
2. Press the standard Menu button on the device.
3. Select the token name from the token list, and then enter your PIN to authenticate.
4. Select “Token Information” from the menu options. The token information appears.
Changing token PIN

To change your PIN, ensure that the token is activated, and then do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change Token PIN” from the menu options.
4. Enter your current PIN and press “Continue”. The Enter your new PIN window appears.
5. Enter and confirm the new PIN that you will use with the token. You have successfully reset the PIN.

The Attack-Lock feature will deactivate your token as per the token policy on entering the wrong PIN consecutively. When the token is deactivated, you will need to reactivate it.

Changing the token name

To change the token name, do the following:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Change Token Name” from the menu options.
4. Enter your new token name and then press “Continue”. You have successfully changed the token name.

The token name change is not permitted if token has been activated using auto-enrollment.
Deactivating the token

There will be instances when you will need to de-activate your token back to its original state.

Before deactivating tokens, contact your administrator. Unless re-enrollment privileges are enabled, you cannot reenroll your token until the administrator removes the token from your record.

To de-activate the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Deactivate Token” from the menu options.
4. Read the warning, and then press “Deactivate”. You have successfully de-activated your MobilePASS token.

Deleting the token

There will be instances when you will need to delete your token. To delete the token:

1. Open the MobilePASS application on the device.
2. Select the token name from the token list, and then enter your PIN.
3. Select “Delete Token” from the menu options.
4. Read the warning, and then press “Delete”. You have successfully deleted your MobilePASS token.
## Appendix  Troubleshooting

1. **Auto-enrollment failure**
   - Error Message: Auto Enrollment failed. Try again, or contact your administrator for help. You can also try Manual Enrollment.
   
<table>
<thead>
<tr>
<th>Possible failure cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect server enrollment configuration or credentials provided during enrollment.</td>
<td>Re-check enrollment credentials or contact the administrator.</td>
</tr>
<tr>
<td>Enrollment portal is not accessible.</td>
<td>Check network connectivity on device or desktop.</td>
</tr>
</tbody>
</table>

2. **Invalid Policy**
   - Error Message: Token does not meet requirements.

<table>
<thead>
<tr>
<th>Possible failure cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An invalid policy was entered by the user during manual enrollment.</td>
<td>Re-enter the correct policy and press “Continue”.</td>
</tr>
</tbody>
</table>

3. **Incorrect PIN is entered during authentication**
   - Error Message: Attempts: 2/6. Invalid Token PIN. Please re-enter your PIN. After 6 unsuccessful attempts, your token will need to be activated again.

<table>
<thead>
<tr>
<th>Possible failure cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The PIN entered is incorrect</td>
<td>Re-enter the correct PIN and press on “Continue”.</td>
</tr>
</tbody>
</table>

4. **Token locked due to invalid pin attacks.**
   - Error Message: Attempt: 3/6. Your token is temporarily disabled. Try again after 1 minute. After 6 unsuccessful attempts, your token will need to be activated again.

<table>
<thead>
<tr>
<th>Possible failure cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple validation attempts were made with the wrong pin. Now the token is disabled for the time (e.g. 1,2,3… minutes) as mentioned on the screen.</td>
<td>Re-enter the correct PIN and press on “Continue” after the delay.</td>
</tr>
</tbody>
</table>

5. **Incorrect challenge**
   - Error Message: Challenge code does not meet requirements.

<table>
<thead>
<tr>
<th>Possible failure cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An invalid challenge was entered by the user.</td>
<td>Re-enter the correct challenge and press “Generate Passcode”.</td>
</tr>
</tbody>
</table>

6. **Incorrect token name**
   - Error Message: You already have a token with this name. Enter a different token name.

<table>
<thead>
<tr>
<th>Possible failure cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The token name entered by the user (while creating a new token or changing token name) is already in use.</td>
<td>Enter a different token name.</td>
</tr>
</tbody>
</table>