# Document Information

<table>
<thead>
<tr>
<th>Product Version</th>
<th>SafeNet MobilePASS 8.4 for Mac OS X by Gemalto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Part Number</td>
<td>007-013049-001, Rev. B</td>
</tr>
<tr>
<td>Release Date</td>
<td>19 July 2015</td>
</tr>
</tbody>
</table>

## Trademarks

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, Inc.

## Disclaimer

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 or organization of any such revisions or changes.

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.

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 or email below.

## Contact Method

<table>
<thead>
<tr>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mail</strong></td>
</tr>
<tr>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td><strong>Email</strong></td>
</tr>
<tr>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
## Contents

### CHAPTER 1 Overview
- About SafeNet MobilePASS by Gemalto .......................................................... 4
- Getting Started with SafeNet MobilePASS ....................................................... 4
- Benefits of Using SafeNet MobilePASS .......................................................... 4
- Protecting Your Security PIN ......................................................................... 5
- Unlocking a Locked Token .............................................................................. 5
- Token Logon Issues ....................................................................................... 5

### CHAPTER 2 Downloading and Installing SafeNet MobilePASS
- Prerequisites ..................................................................................................... 6
- Removing SafeNet MobilePASS 8.4 for Mac OS X, Customer Preview .......... 6
- Downloading and Installing SafeNet MobilePASS 8.4 for Mac OS X ........... 6

### CHAPTER 3 Creating and Enrolling SafeNet MobilePASS
- Enrollment Options .......................................................................................... 7
- Automatic Enrollment (SAS) ........................................................................... 8
  - Token Assignment ........................................................................................ 8
    - Auto-Enrolling SafeNet MobilePASS by Copying and Pasting the Activation String Automatically 8
    - Auto-Enrolling SafeNet MobilePASS by Copying the Activation String Manually .......................... 10
- Automatic Enrollment (SAM, SAMx, SPA) .................................................... 14
- Manual Enrollment (SAM, SAMx, SPA) ......................................................... 17

### CHAPTER 4 Creating and Changing the Token PIN
- Creating a Token PIN ...................................................................................... 21
- Changing a Token PIN ................................................................................... 22

### CHAPTER 5 Generating Passcodes
- Generating a Passcode with Time-based Tokens ........................................ 25
- Generating Passcodes with Challenge-Response Tokens .......................... 26

### CHAPTER 6 Deleting, Deactivating and Renaming a Token
- Opening Settings Window ............................................................................. 27
- Renaming a Token ......................................................................................... 29
- Deleting a Token ............................................................................................ 30
- Deleting all Tokens ....................................................................................... 30
- Deactivating a Token .................................................................................... 31

### CHAPTER 7 Token Information and Log Settings
- Viewing Token Information .......................................................................... 32
- Configuring Log Settings ............................................................................. 33

### CHAPTER 8 Security Features
- Time-based Security Enhancement Scenario .............................................. 34
 CHAPTER 1

Overview

About SafeNet MobilePASS by Gemalto

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 on 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 one-time passcode (OTP) stops being valid. Any attempt to logon by reusing the OTP will fail, and will alert your network security professionals to the possibility that your identity has been stolen.

SafeNet MobilePASS allows secure remote access to corporate and web-based applications. As a SafeNet MobilePASS for Mac OS X user, you can generate one-time passcodes (OTPs) on your computer and use those passcodes to authenticate to SafeNet-protected applications.

An integrated support feature allows your company’s system administrator to manage SafeNet MobilePASS directly from an authentication management system.

Getting Started with SafeNet MobilePASS

You must complete the self-enrollment process before you can use your SafeNet MobilePASS token. Self-enrollment is the process of activating your token. You will receive a self-enrollment email from your company that contains a link to the SafeNet MobilePASS self-enrollment website, along with instructions for installing, enrolling, and activating your MobilePASS token.

If you have not received your self-enrollment email, contact your system administrator.

After installing MobilePASS on your computer, you can use the application to generate an OTP. You may be required to enter a PIN before generating the OTP.

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

Benefits of Using SafeNet MobilePASS

SafeNet MobilePASS enables you to access corporate and web-based resources securely. It will also reduce or eliminate the need to remember or periodically change you logon passwords, as your token will do this for you.
Protecting Your 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 anyone. 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.

If you forget your PIN, contact your company’s help desk. They will verify your identity and reset your PIN.

Unlocking a Locked Token

A token is locked when there have been attempts to generate OTPs using an incorrect PIN. Contact your help desk to unlock a locked token.

Token Logon Issues

The most common cause of failed token logon is entering an incorrect OTP. Ensure that you enter the code exactly as displayed on the token, including any punctuation, uppercase and lowercase letters. Never attempt to reuse an OTP. Your account will automatically lock for a period if you exceed the allowed number of consecutive failed logon attempts. You must wait the required period before your account becomes active again. Contact your company’s help desk to resolve logon issues.
CHAPTER 2

Downloading and Installing SafeNet MobilePASS

Prerequisites

Removing SafeNet MobilePASS 8.4 for Mac OS X, Customer Preview

If you ran SafeNet MobilePASS 8.4 for Mac OS X, Customer Preview, remove it before installing the SafeNet MobilePASS 8.4 for Mac OS X general availability (GA) release.

To remove SafeNet MobilePASS 8.4 for Mac OS X, Customer Preview:

1. Delete the SafeNet MobilePASS application as follows:
   a. Right click the MobilePASS.app file and select Move to Trash.
   b. Right click the Trash icon and select Empty Trash.

2. Delete the container as follows:
   a. Select [User]>Library>Containers
   b. Right click on com.safenet.mobilepass.mac and select Move To Trash
   c. Right click the Trash icon and select Empty Trash.

   **NOTE:** If attempting to empty the trash fails, restart the computer and attempt to empty the trash again.

Downloading and Installing SafeNet MobilePASS 8.4 for Mac OS X

SafeNet MobilePASS 8.4 for Mac OS X is installed from the Mac App Store

To install SafeNet MobilePASS 8.4 for Mac OS X from the Mac App Store:

1. Find MobilePASS 8.4 for Mac OS X in the Mac App Store.
2. Install and follow the prompt to sign in to the Mac App Store with your Apple ID.
3. MobilePASS 8.4 for Mac OS X begins downloading and appears in your Launchpad and /Applications folder. Download and installation take place in a single step.
4. Run the application from the Launchpad.
CHAPTER 3
Creating and Enrolling SafeNet MobilePASS

Enrollment Options

After creating your SafeNet MobilePASS token, you are required to enroll your SafeNet MobilePASS token. The enrollment procedure varies according to which authentication management platform your company uses.

Automatic enrollment:

• Gemalto’s SafeNet Authentication Service (SAS) Cloud - see Automatic Enrollment (SAS) on page 8
• Gemalto’s SafeNet Authentication Service (SAS) PCE/SPE - see Automatic Enrollment (SAS) on page 8
• Gemalto’s SafeNet Authentication Manager (SAM) - see Automatic Enrollment (SAM, SAMx, SPA) on page 14
• Gemalto’s SafeWord Premier Access (SPA) - see Automatic Enrollment (SAM, SAMx, SPA) on page 14
• Gemalto’s SafeNet Authentication Manager Express (SAMx) - see Automatic Enrollment (SAM, SAMx, SPA) on page 14

Manual enrollment:

• Gemalto’s SafeNet Authentication Manager (SAM) - see Manual Enrollment (SAM, SAMx, SPA) on page 17
• Gemalto’s SafeWord Premier Access (SPA) - see Manual Enrollment (SAM, SAMx, SPA) on page 17
• Gemalto’s SafeNet Authentication Manager Express (SAMx) - see Manual Enrollment (SAM, SAMx, SPA) on page 17
Automatic Enrollment (SAS)

Token Assignment

Your system administrator will assign you a token and you will receive a self-enrollment notification email.

You can perform Automatic Enrollment using one of the following two methods:

- Automatically copy and paste the Activation String into the Auto Enrollment window by clicking the Enroll your MobilePASS token link on the notification email. See “Auto-Enrolling SafeNet MobilePASS by Copying and Pasting the Activation String” on page 8.

- Copy the Activation String manually. Use this option if you experience difficulties with the automatic copy and paste. See “Auto-Enrolling SafeNet MobilePASS by Copying the Activation String Manually” on page 10.

Auto-Enrolling SafeNet MobilePASS by Copying and Pasting the Activation String Automatically

To Enroll SafeNet MobilePASS by copying and pasting the activation string automatically:

1. Click the https:// link in the email. The Self-Enrollment page is displayed.
2. If you have not downloaded SafeNet MobilePASS for Mac OS X, click the icon to download and install.

3. Click the Enroll your MobilePASS token link.

   NOTE: The default token name is displayed in the Create New Token window, as it has not yet been enrolled. For the first token enrollment, the token name is derived from your SAS user name.

4. In the Create New Token window, enter a token name of more than three characters and click Activate.

5. If your token is PIN protected, the Set a Token PIN window appears. Enter the PIN and click Continue.

   NOTE: The required number and type of characters required for the PIN depends on the configuration of your system.
6. Your Passcode is displayed on your SafeNet MobilePASS window.

Auto-Enrolling SafeNet MobilePASS by Copying the Activation String Manually

To auto-enroll SafeNet MobilePASS by copying the activation string manually:

1. Click the https:// link in the email.
2. The SafeNet Authentication Service – Self Enrollment page opens.

3. If you have not downloaded SafeNet MobilePASS for Mac OS X, click the icon to download and install.
4. Copy the activation string

**NOTE:** Ensure that you select the entire string.
5. Run the SafeNet MobilePASS application.

![Image of SafeNet MobilePASS application](image)

**NOTE:** If there is not yet a token in the application, a token with a default name (My Token 1) is created automatically.

6. Click the required token.

7. On the **Token Enrollment** window, click **Auto Enrollment**.
8. On the **Auto Enrollment** window, the copied Activation String is automatically pasted into the **Enrollment String** field.

![Auto Enrollment Window](image)

9. Click **Continue**.

10. If your token is PIN protected, the **Enter a Token PIN** window is displayed. Enter the PIN in the **Token PIN** field, and then click **Continue**.

---

**NOTE:** The required number and type of characters required for the PIN depends on the configuration of your system. The requirement could be between four and eight digits, and be either numeric or alphanumeric.
Your passcode is displayed in the SafeNet MobilePASS window.
Automatic Enrollment (SAM, SAMx, SPA)

To Enroll SafeNet MobilePASS automatically:

1. Open the SafeNet MobilePASS application.

2. To Create a new token, click Add.
3. In the **Create New Token** window, enter a token name of more than three characters and click **Activate**.

4. Click **Auto Enrollment**

5. Enter the URL of your authentication management system portal (SAS, SAMx, or SPA) and click **Continue**.
6. In the **User ID** field, enter the username you use to log on to your authentication management platform (SAM, SAMx, SPA)

7. In the **User Password** field, enter your enrollment password and click **Continue**.

---

**NOTE:** The enrollment password is provided by your system administrator via email or SMS message. It can be used only once.
8. If your token is PIN protected, the **Enter a Token PIN** window is displayed. Enter the PIN in the **Token PIN** field, and then click **Continue**.

You SafeNet MobilePASS token is enrolled.

---

**Manual Enrollment (SAM, SAMx, SPA)**

**To enroll SafeNet MobilePASS manually:**

1. Open the SafeNet MobilePASS application.

2. To create a new token, Click **Add**

![Image of the SafeNet MobilePASS application interface showing the option to add a new token.](image-url)
3. On the **Create New Token** window, enter a new token name of more than three characters, and then click **Activate**.

![Create New Token Window](image)

**NOTE:** If you select **Activate Later**, you are returned to the **Token List** window. Your token is displayed but will not be enrolled until you select **Activate**.

4. In the **Token Enrollment** window, click **Manual Enrollment**.

![Token Enrollment Window](image)
5. In the Management Enrollment window, enter your Token Policy String.

**NOTE:** Your system administrator will send you the Token Policy String.
6. If your token is PIN protected, the **Enter a Token PIN** window is displayed. Enter the PIN in the **Token PIN** field, and then click **Continue**. The **Activation Code** is displayed.

![Activation Code](image)

7. Enter the **Activation Code** in the portal of your authentication management platform (SAM, SAMx, or SPA).
CHAPTER 4
Creating and Changing the Token PIN

Creating a Token PIN

NOTE: The Creating a Token PIN option is available only if your SafeNet MobilePASS token has been configured for PIN protection.

SafeNet MobilePASS supports both simple numeric protection PINs and more complex, stronger alphanumeric protection PINs. The numeric keypad is the default keyboard option.

To create a token PIN:

1. On the Set a Token PIN window, enter a PIN in the Token PIN field, and then click Continue.

   NOTE: The required number and type of characters required for the PIN depends on the configuration of your system. The requirement could be between four and eight digits, and be either numeric or alphanumeric.

2. Re-enter the PIN in the Re-enter Token PIN field, and then click Continue.
Changing a Token PIN

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

To change the PIN:

1. Select the token name from the token list, and then enter your PIN to authenticate.
2. Click Change Token PIN.

![Change Token PIN interface](image)
3. On the Change Token PIN window, enter the PIN in the Current Token PIN field, and then click Continue.

4. Enter the New Token PIN.

5. Re-enter the PIN in the Re-enter your new PIN field, and then click Continue.
6. Click **Continue** on the **Change Token PIN** window.

**NOTE:** You are allowed only a certain number of failed 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-activated.
Generating a Passcode with Time-based Tokens

If you are using a time-based token, the OTP is automatically generated after the specified time interval has elapsed.
Generating Passcodes with Challenge-Response Tokens

To generate a passcode with a challenge-response token:

1. Enter the provided challenge code in the **Challenge Code** field.

![Challenge Code Field](image)

2. Click **Generate Passcode**.
   
   The passcode is displayed.

3. To generate another passcode, click **Next Challenge**, and then repeat this process.
CHAPTER 6
Deleting, Deactivating and Renaming a Token

Opening Settings Window

To open the settings window:

1. Select the token from the list
2. If your token is PIN protected, enter your PIN when prompted.

   The **Your Passcode** window opens.

   ![Your Passcode Window]

   - Copy Passcode
   - Generate Passcode

3. Click

   The settings window opens.

   ![Settings Window]

   - Token Information
   - Change Token Name
   - PIN Change Token PIN
   - Deactivate Token
   - Delete Token
   - Log setting
   - Delete All Tokens
Renaming a Token

To change a token name:

1. Open the settings window (see “Opening Settings Window” on page 27.
2. Click Change Token Name.
3. Enter your new token name and then click Continue.
Deleting a Token

To delete a token:

1. Open the settings window (see “Opening Settings Window” on page 27.)
2. Click Delete Token.
3. Read the warning and then click Delete.

Deleting all Tokens

To delete all tokens:

1. Open the settings window (see “Opening Settings Window” on page 27.)
2. Click Delete all Tokens.
3. Read the warning and then click Continue.
Deactivating a Token

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

To deactivate a token:
1. Open the settings window (see “Opening Settings Window” on page 27.)
2. Select the token name from the token list and, if your token is PIN protected, enter your PIN.
3. Click **Deactivate Token**.
4. Read the warning and then click **Deactivate**.
CHAPTER 7

Token Information and Log Settings

Viewing Token Information

To view token information:

1. Open the settings window (see “Opening Settings Window” on page 27.)
2. Click Token Information.

   The Token Information window is displayed.
Configuring Log Settings

1. Open the settings window (see “Opening Settings Window” on page 27).
2. Click Log Settings. The Log window opens.

3. To delete the log click Clean log
4. To stop creating a log click Disable log
CHAPTER 8
Security Features

SafeNet MobilePASS provides time-hacking countermeasures to alert users to the possibility that their device has been compromised, and that OTPs have been generated that could be used in the future.

**Time-based Security Enhancement Scenario**

Your device was compromised, and the device’s date and time were changed to a future date and time. The person who took the device generates several time-based OTPs (which will be used for authentication purposes without the SafeNet MobilePASS application), and then restores the device’s time.

With the time-hacking countermeasures, SafeNet MobilePASS is able to detect that the device was tampered with, and alerts the user to the possibility of an attack.

**To use the time-based security feature:**

1. Open the SafeNet MobilePASS application, create a time-based token, and then generate an OTP.
2. Move the device’s date and time forward, and then generate an OTP.
3. Restore the clock’s date and time, and then generate another OTP.
   
   A message is displayed indicating that an OTP could not be generated.
4. Click **No** to confirm that the displayed date and time are not correct.
5. You are prompted to change the clock back to the correct date and time. Click **OK**.

![Token Alert](image1)

6. Security measures are taken and, if confirmed, your token will be locked. Click **OK** to confirm.

![Token Alert](image2)

You now need to re-enroll your token.
7. Click **OK**.
   
   Your token is now locked.