SafeNet MobilePASS for Windows Desktop

User Guide

gemalto
security to be free

Product Version: 8.4.4

Document Part Number: 007-013228-001, Rev. B

Release Date: 23 May 2016

Contents

1 Overview 4
About SafeNet MobilePASS 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
Product Documentation 5
Support Contacts 6

2 Installation 7
Installing SafeNet MobilePASS 8.4.4 for Windows Desktop 7

3 Creating and Enrolling SafeNet MobilePASS 10
Enrollment Options 10
Automatic Enrollment (SAS) 11
Token Assignment 11
Auto-Enrolling SafeNet MobilePASS by Copying and Pasting the Activation String Automatically 11
Auto-Enrolling SafeNet MobilePASS by Copying the Activation String Manually 14
Automatic Enrollment (SAM, SAMx, SPA) 18
Manual Enrollment (SAM, SAMx, SPA) 21

4 Creating and Changing the Token PIN 25
Creating a Token PIN 25
Changing a Token PIN 27

5 Generating Passcodes 30
Generating a Passcode with Time-based Tokens 30
Generating Passcodes with Challenge-Response Tokens 31

6 Deleting, Deactivating and Renaming a Token 32
Renaming a Token 32
Renaming a Token on Windows 8/8.1 33
Deleting a Token 35
Deactivating a Token 36

7 Viewing Token Information 37
Viewing Token Information 37

8 Security Features 39
Time-based Security Enhancement Scenario 39

CHAPTER 1

Overview

About SafeNet MobilePASS

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 Windows Desktop 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 or deactivated after exceeding the permitted number of failed login attempts.

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.

Product Documentation

The following documentation is associated with this release:

- *SafeNet MobilePASS for Windows Desktop 8.4.4 Customer Release Notes (CRN)*

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.

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.

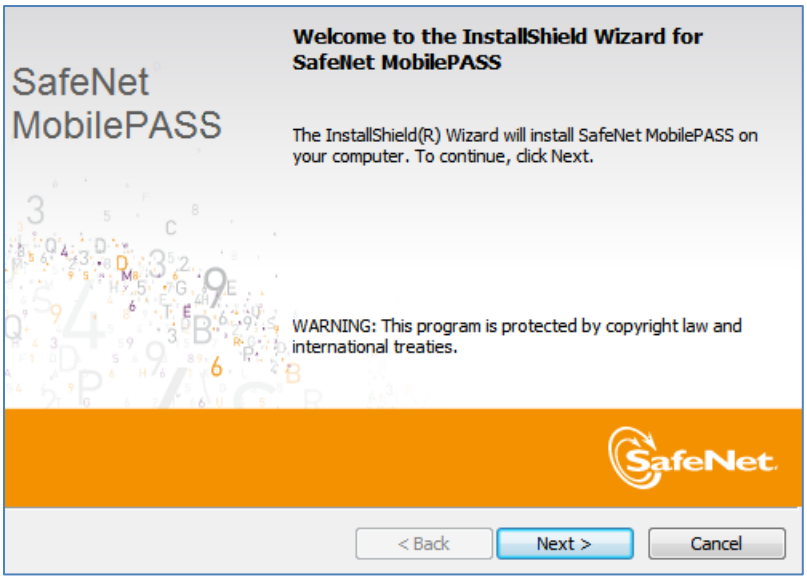
Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

CHAPTER 2

Installation

Installing SafeNet MobilePASS 8.4.4 for Windows Desktop

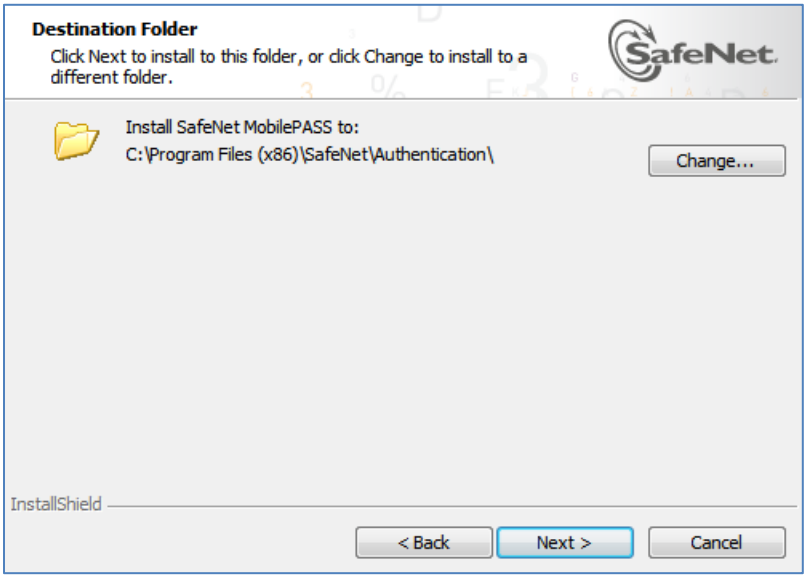
1. Double-click **SafeNet MobilePASS.msi**. The SafeNet MobilePASS Installation Wizard opens.



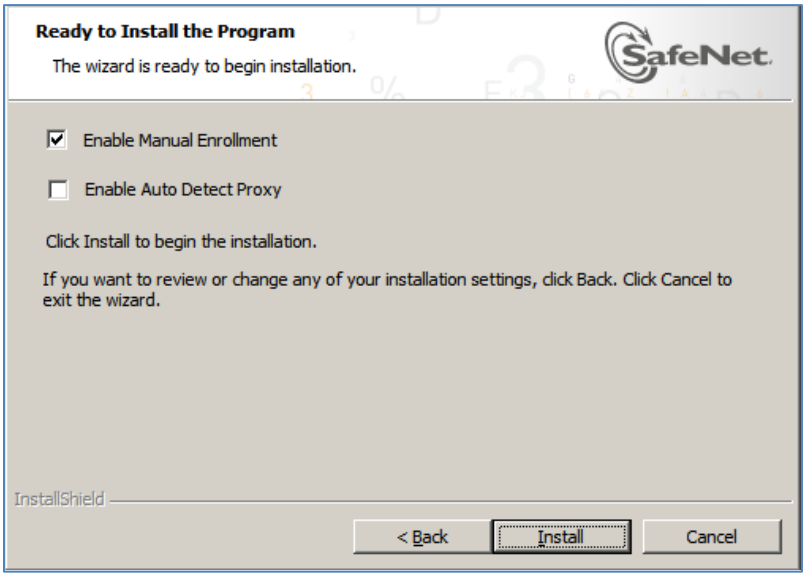
2. Click **Next**. The **License Agreement** window opens.

3. Read the license agreement carefully, select **I accept the license agreement**, and click **Next**.

   The **Destination Folder** window opens, displaying the path to the installation folder.



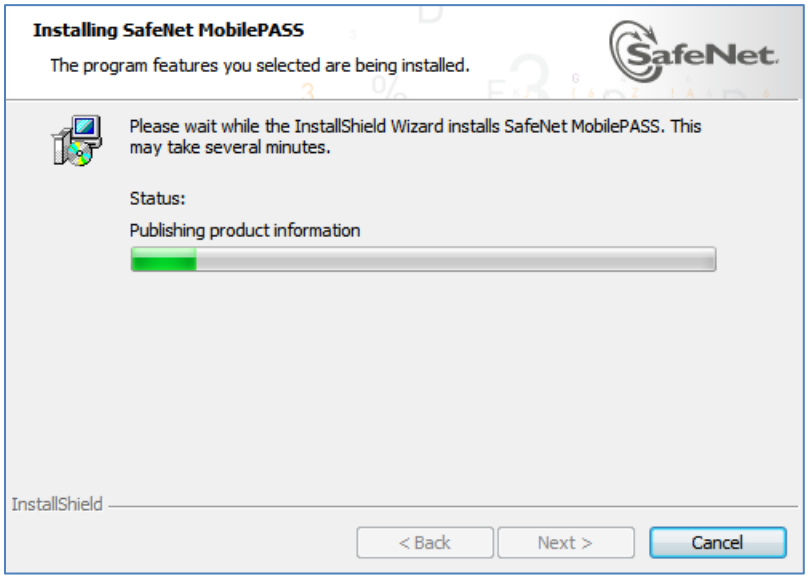
4. If necessary, click **Browse** to select a different destination folder, and then click **Next**. The **Ready to Install the Program** window opens.



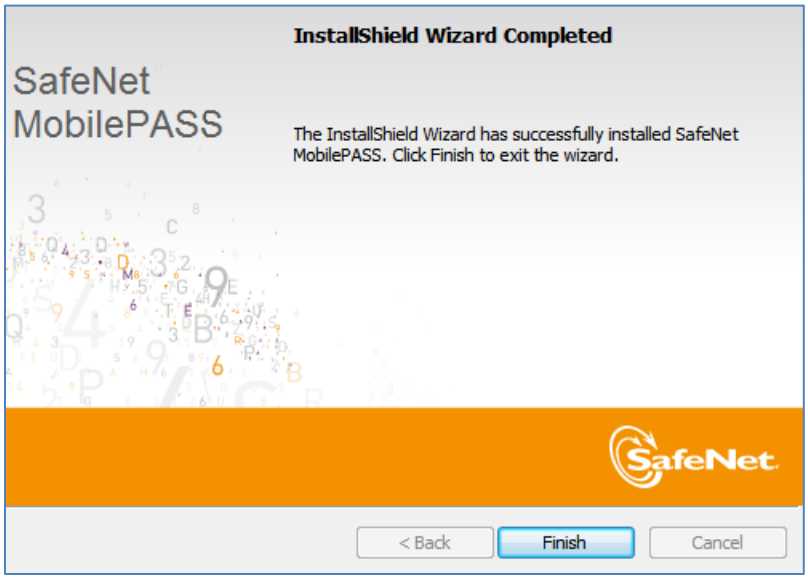
5. To activate manual enrollment, select **Enable Manual Enrollment**. If not selected, you will be able to use automatic enrollment only.
6. If required, select **Enable Auto Detect Proxy** – the client will look for a proxy on the network, in addition to searching locally.

> **NOTE:** The Manual Enrollment and Auto Detect Proxy setting can also be changed by running the Repair setup.

7. Click **Install**. The installation process starts.



On completion of the installation process, the **InstallShield Wizard Complete** window opens.



8. Click **Finish** to complete the process.

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 11
- Gemalto's SafeNet Authentication Service (SAS) PCE/SPE - see Automatic Enrollment (SAS) on page 11
- Gemalto's SafeNet Authentication Manager (SAM) - see Automatic Enrollment (SAM, SAMx, SPA) on page 18
- Gemalto's SafeWord Premier Access (SPA) - see Automatic Enrollment (SAM, SAMx, SPA) on page 18
- Gemalto's SafeNet Authentication Manager Express (SAMx) - see Automatic Enrollment (SAM, SAMx, SPA) on page 18

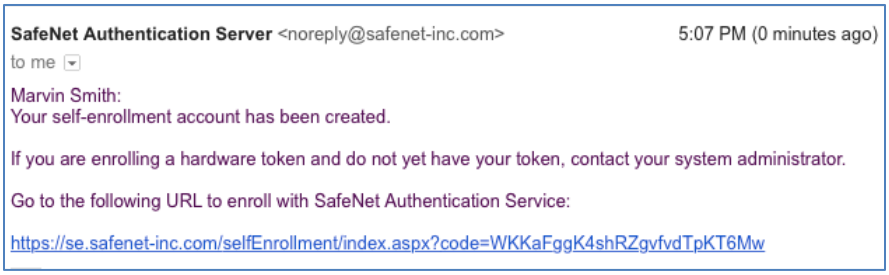
Manual enrollment:

- Gemalto's SafeNet Authentication Manager (SAM) - see Manual Enrollment (SAM, SAMx, SPA) on page 21
- Gemalto's SafeWord Premier Access (SPA) - see Manual Enrollment (SAM, SAMx, SPA) on page 21
- Gemalto's SafeNet Authentication Manager Express (SAMx) - see Manual Enrollment (SAM, SAMx, SPA) on page 21

Automatic Enrollment (SAS)

Token Assignment

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



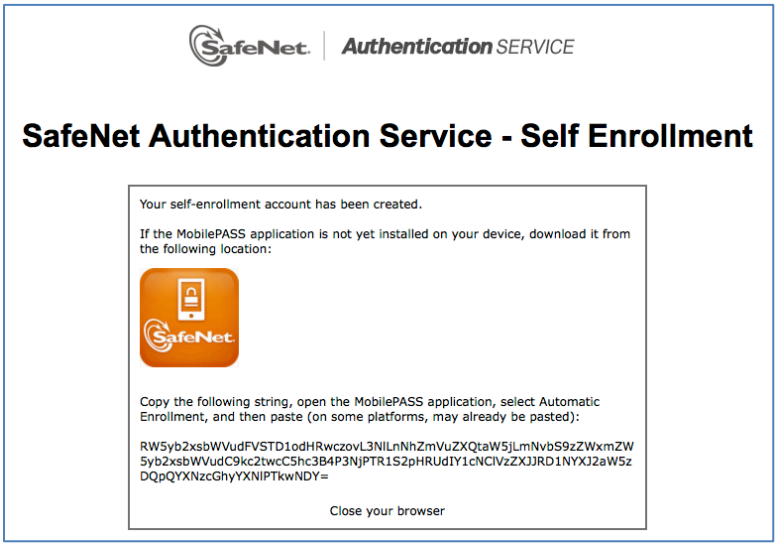
You can perform Automatic Enrollment using one of the following two methods:

- 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 11.
- **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 14.**

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

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

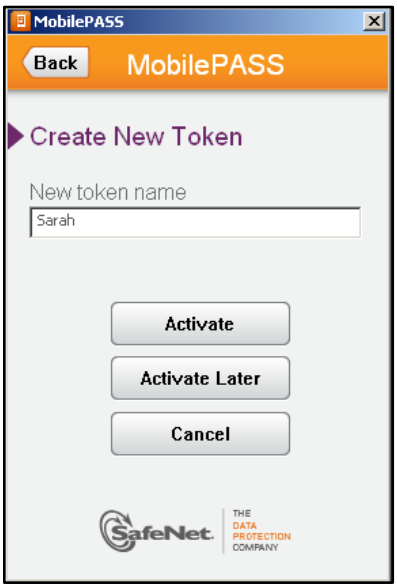
1. Click the https:// link in the email. The Self-Enrollment page is displayed.



2. If you have not downloaded **SafeNet MobilePASS for Windows Desktop**, click the icon to download and install.
3. Click the **Enroll your MobilePASS** token link.

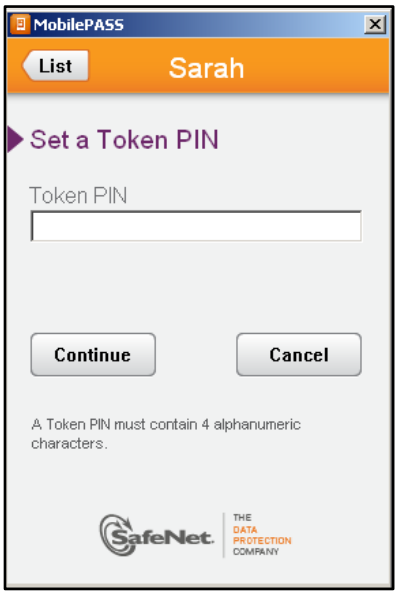
> **NOTE:** The default token name is displayed in the **Create New Token** window, as it has not yet been enrolled. For the first token enrollment, the token name is derived from your SAS user name.

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

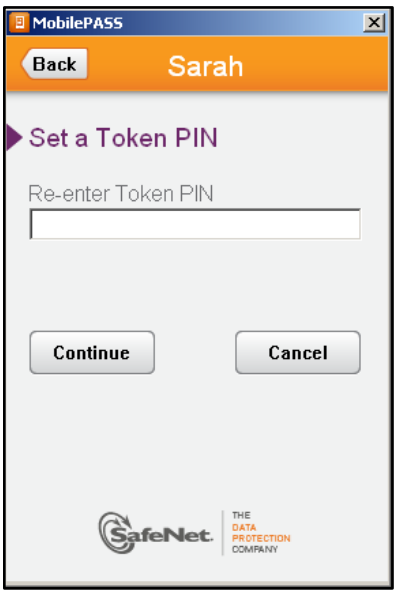


5. If your token is PIN protected, the **Set a Token PIN** window appears. Enter the PIN and click **Continue**.

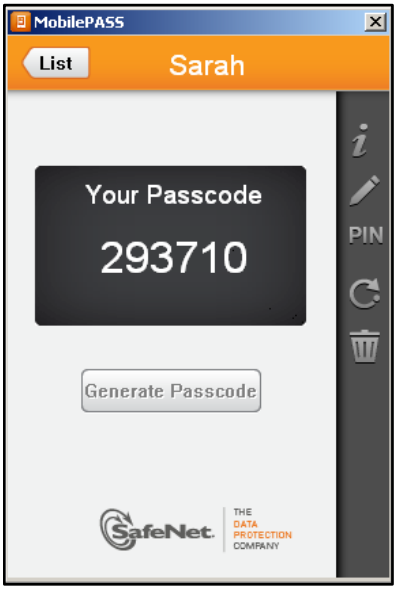
> **NOTE:** The required number and type of characters required for the PIN depends on the configuration of your system.



6. Re-enter the PIN and click **Continue**.



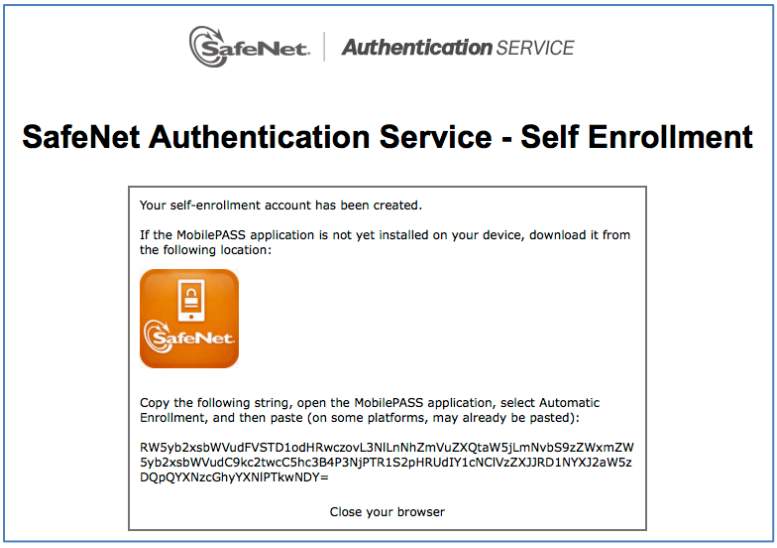
Your Passcode is displayed on your SafeNet MobilePASS window.



Auto-Enrolling SafeNet MobilePASS by Copying the Activation String Manually

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

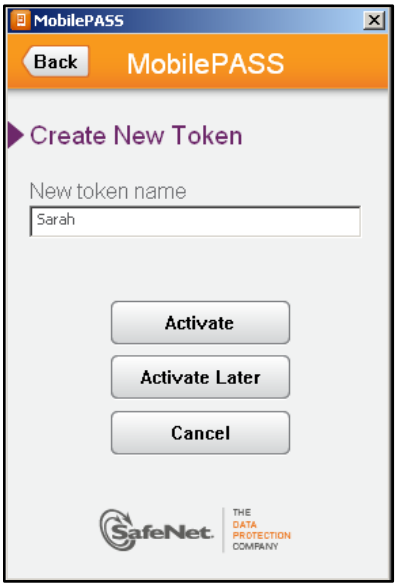
1. Click the https:// link in the email.
2. The SafeNet Authentication Service – Self Enrollment page opens.



3. If you have not downloaded **SafeNet MobilePASS for Windows Desktop**, click the icon to download and install.
4. Copy the activation string

> **NOTE:** Ensure that you select the entire string.

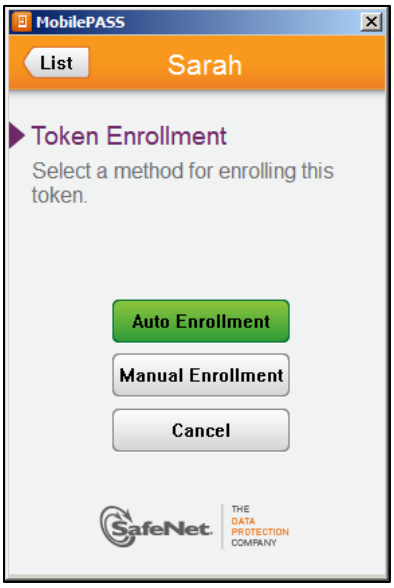
5. Run the SafeNet MobilePASS application.
6. On the Welcome screen click Add 
7. In the **Create New Token** window, enter a token name of more than four characters and click **Activate**.



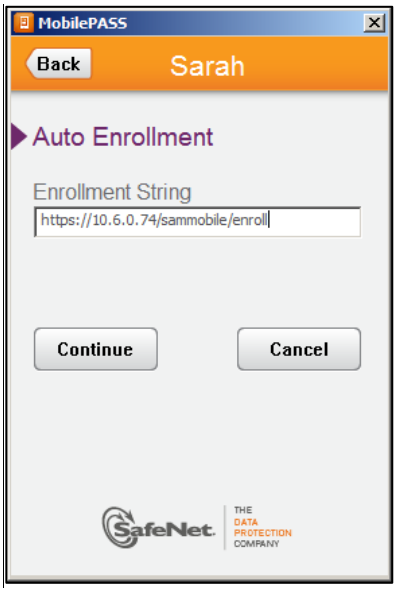
8. If your token is PIN protected, the **Set a Token PIN** window appears. Enter the PIN and click **Continue**.

> **NOTE:** The required number and type of characters required for the PIN depends on the configuration of your system.

9. On the Token Enrollment window, click **Auto Enrollment**.

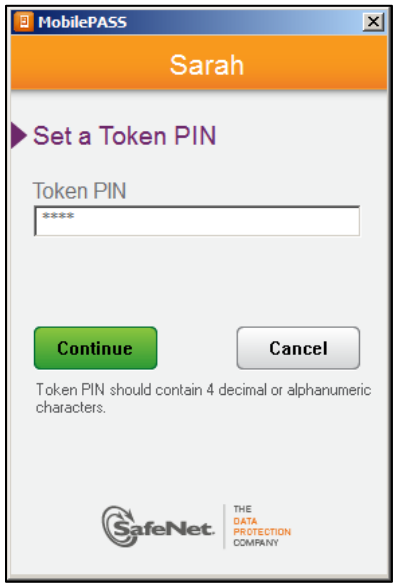


10. On the **Auto Enrollment** window, the copied Activation String is automatically pasted into the **Enrollment String** field.



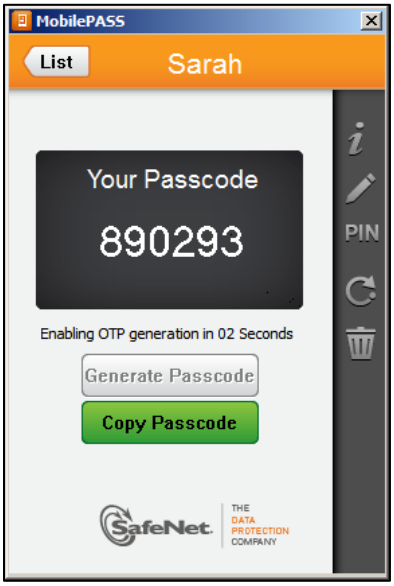
11. Click **Continue.**

12. If your token is PIN protected, the **Set a Token PIN** window is displayed. Enter the PIN in the **Token PIN** field, confirm 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.

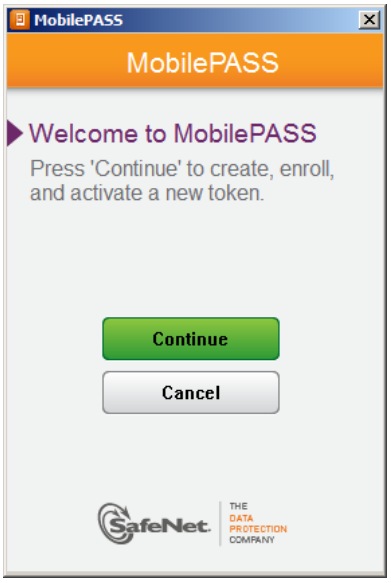
Your passcode is displayed in the SafeNet MobilePASS window.



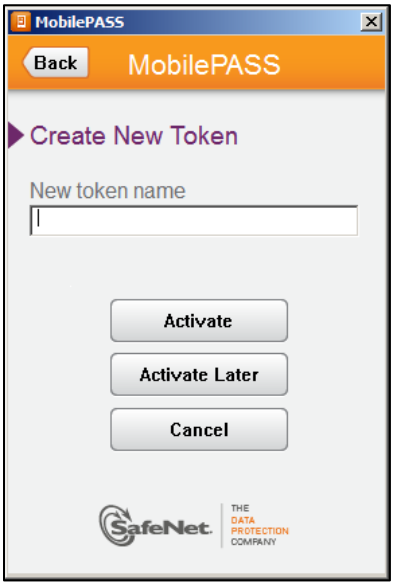
Automatic Enrollment (SAM, SAMx, SPA)

To Enroll SafeNet MobilePASS automatically:

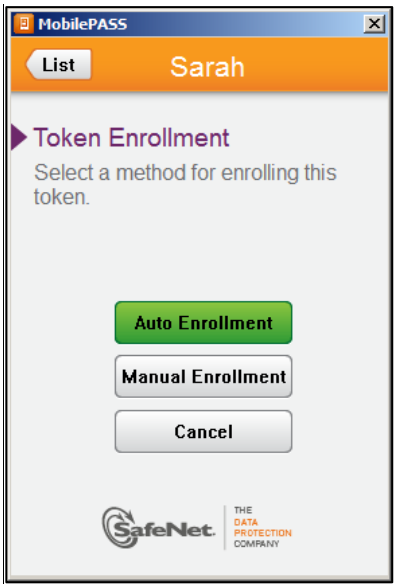
1. Open the SafeNet MobilePASS application.
2. **On the Welcome to MobilePASS screen, click Continue.**



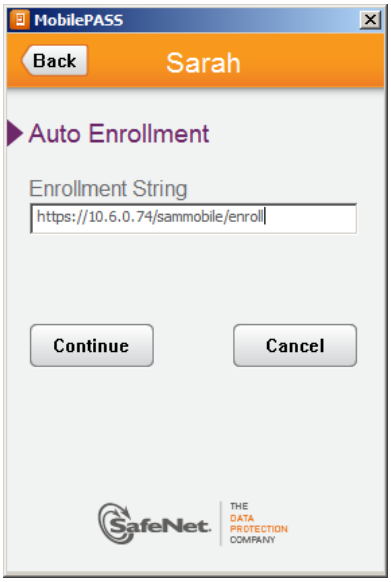
3. In the **Create New Token** window, enter a token name of more than four characters and click **Activate**.



4. Click **Auto Enrollment**

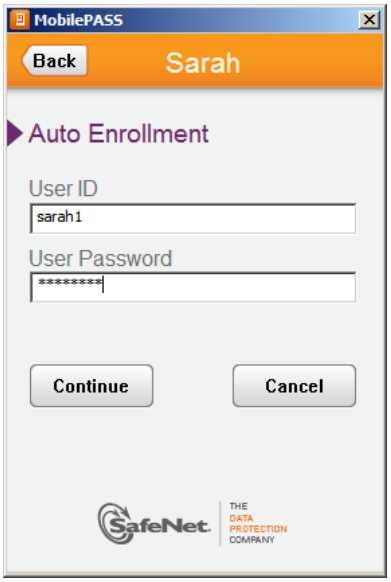


5. Enter the URL of your authentication management system portal (SAS, SAMx, or SPA) and click **Continue.**

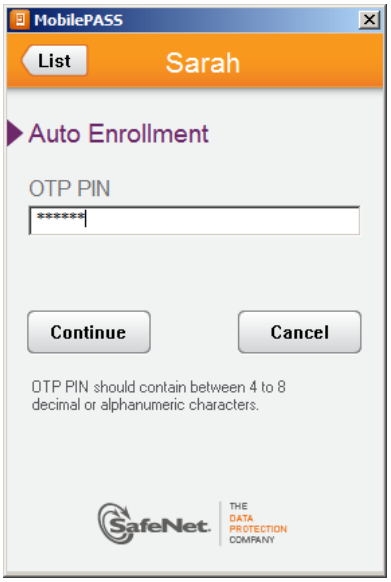


6. In the **User ID** field, enter the username you use to log on to your authentication management platform (SAM, SAMx, SPA)
7. In the **User Password** field, enter your enrollment password and click **Continue**.

> **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, enter PIN in the **OTP PIN** field, and then click **Continue**.

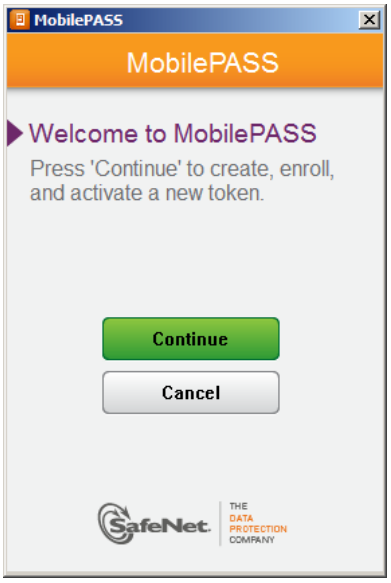


Your SafeNet MobilePASS token is enrolled.

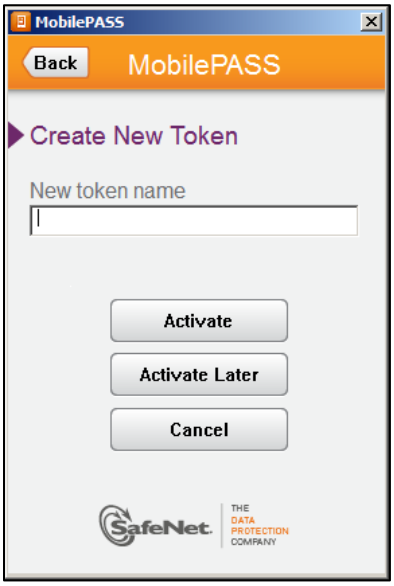
Manual Enrollment (SAM, SAMx, SPA)

To enroll SafeNet MobilePASS manually:

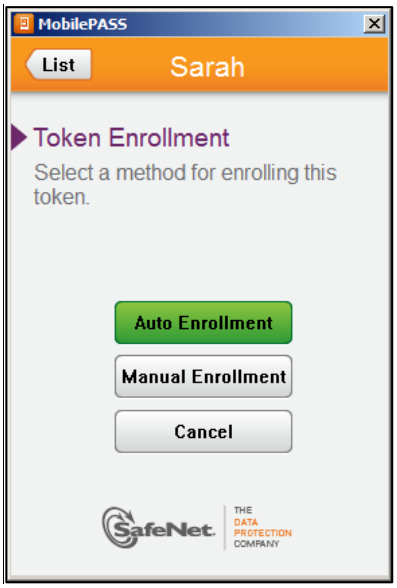
1. Open the SafeNet MobilePASS application.
2. On the Welcome to MobilePASS screen, click Continue.



3. In the **Create New Token** window, enter a token name of more than four characters and click **Activate**.

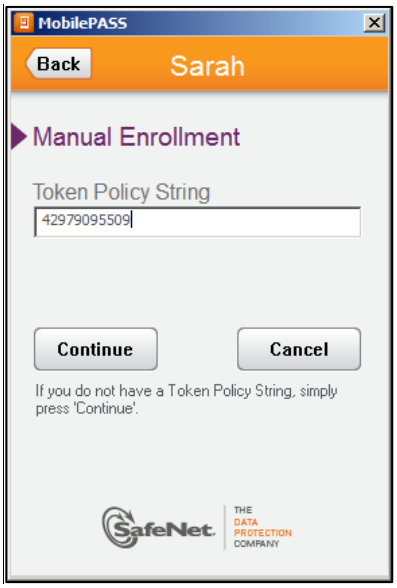


4. In the **Token Enrollment** window, **click Manual Enrollment**.



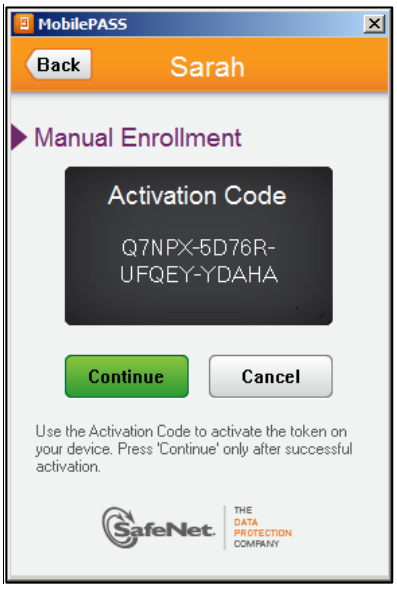
5. In the **Management Enrollment** window, enter your **Token Policy String**.

> **NOTE:** Obtain the Token Policy String form your SAM, SAMx or SPA portal.

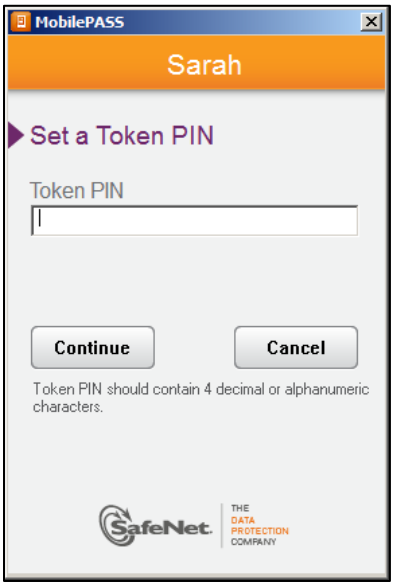


6. If your token is PIN protected, the **Enter a Token PIN** window is displayed. Enter the PIN in the **Token PIN** field, and then click **Continue**.

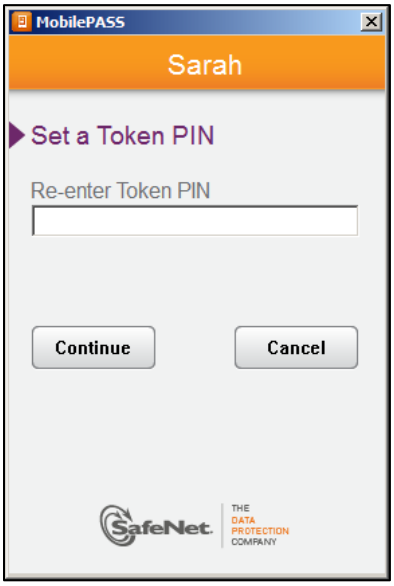
   The Activation Code is displayed.



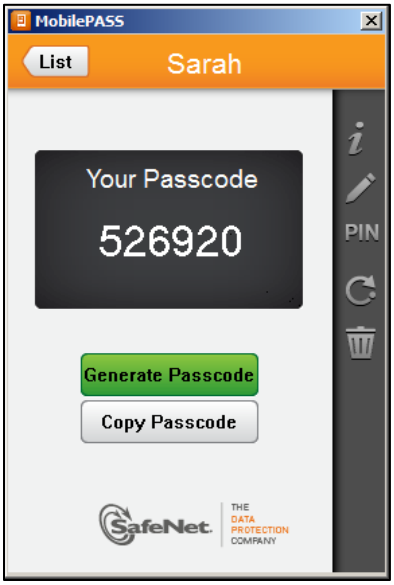
7. Enter the **Activation Code** in the portal of your authentication management platform (SAM, SAMx, or SPA).
8. If required enter the Token PIN, click **Continue**.



9. Re-enter Token PIN and click **Continue**.



10. The **Your Passcode** window is displayed.



CHAPTER 4

Creating and Changing the Token PIN

Creating a Token PIN

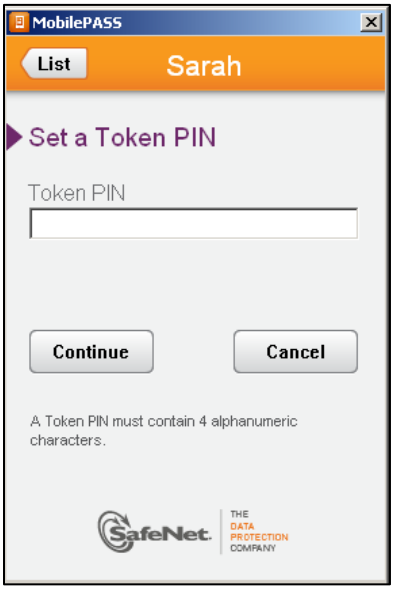
NOTE: The **Creating a Token PIN** option is available only if your SafeNet MobilePASS token has been configured for PIN protection.

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

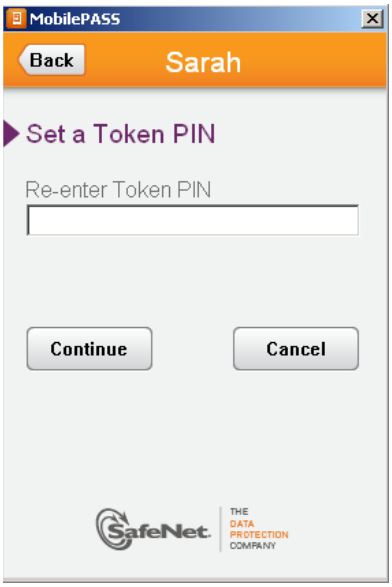
To create a token PIN:

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**.

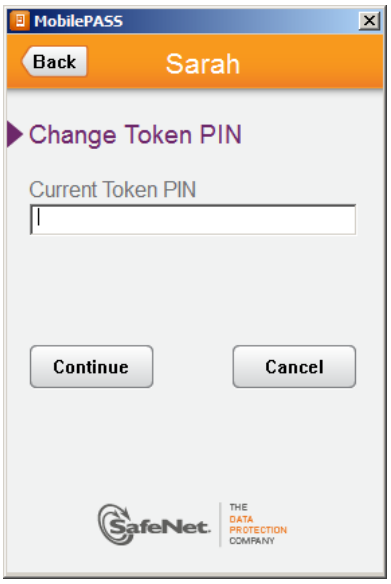


Changing a Token PIN

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

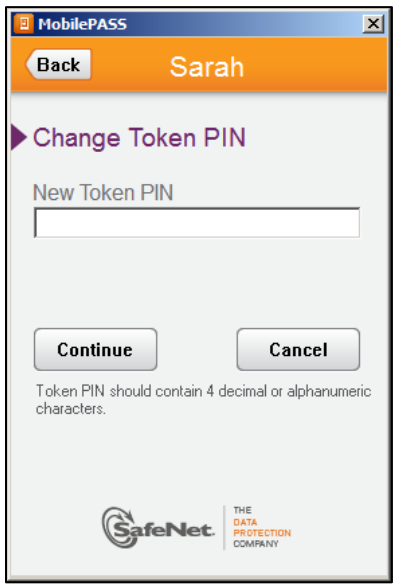
To change the PIN:

1. Select the token name from the token list, and then enter your PIN to authenticate.
2. Click Change Token PIN PIN
3. On the **Change Token PIN** window, enter the PIN in the **Current Token PIN field, and then click Continue.**

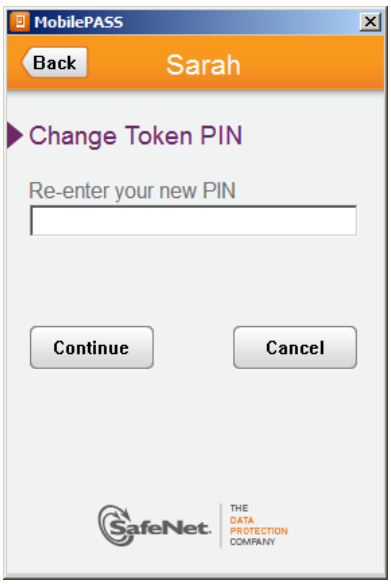


NOTE: You are allowed only a certain number of failed attempts to enter the correct PIN (depending on how many permitted retries your administrator has defined). If you exceed the number of allowed retries, your token must be re-activated.

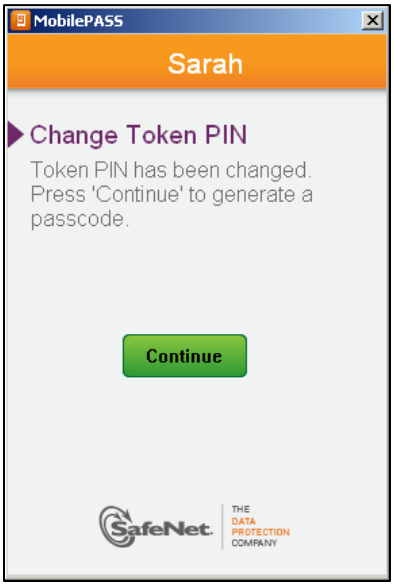
4. Enter the new token PIN.



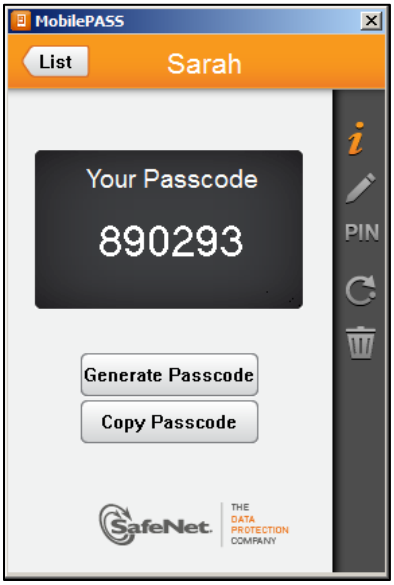
5. Re-enter the PIN in the **Re-enter your new PIN** field, and then **click Continue**.



6. Click **Continue** on the **Change Token PIN** window.



The **Your Password** window opens.

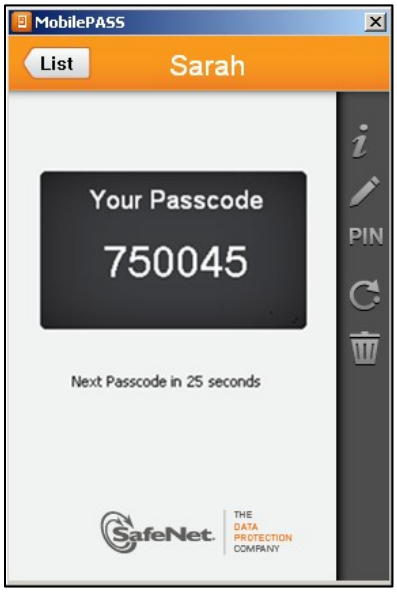


CHAPTER 5

Generating Passcodes

Generating a Passcode with Time-based Tokens

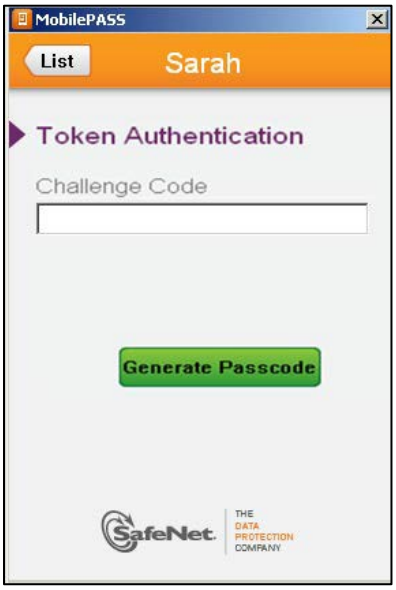
If you are using a time-based token, the OTP is automatically generated after the specified time interval has elapsed.



Generating Passcodes with Challenge-Response Tokens

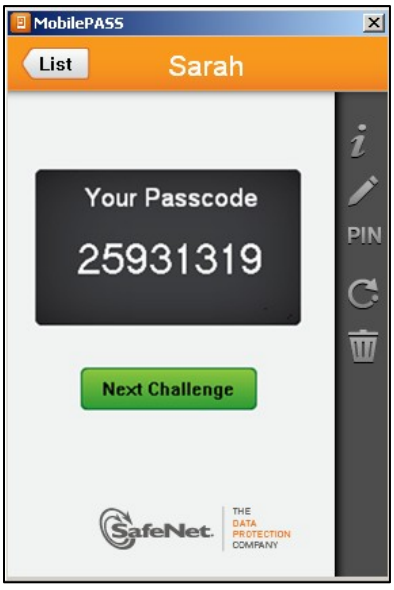
To generate a passcode with a challenge-response token:

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



2. Click **Generate Passcode**.

   The passcode is displayed.



3. To generate another passcode, click **Next Challenge**, and then repeat this process.

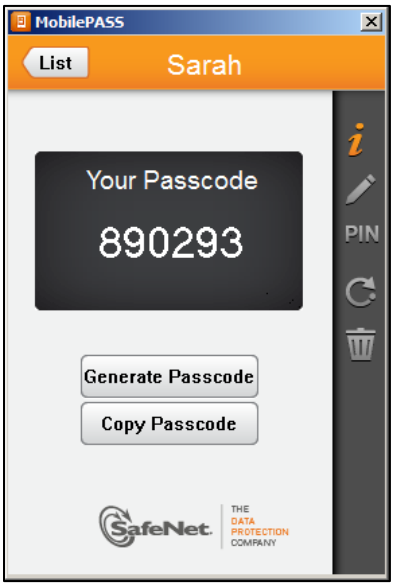
CHAPTER 6

Deleting, Deactivating and Renaming a Token

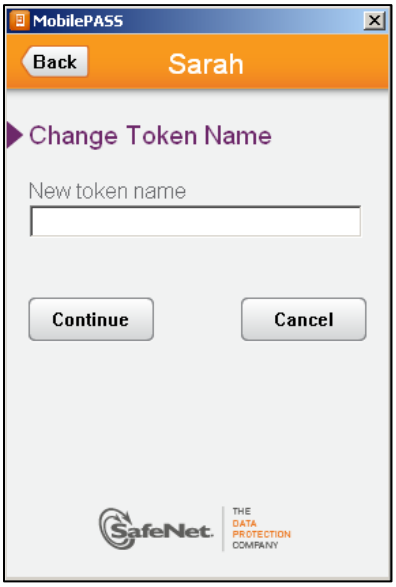
Renaming a Token

To change a token name:

1. Open MobilePASS, select the token name from the list, and if prompted, enter your PIN.
2. Click the **Change Token Name** icon 



3. Enter your new token name and then click **Continue**.



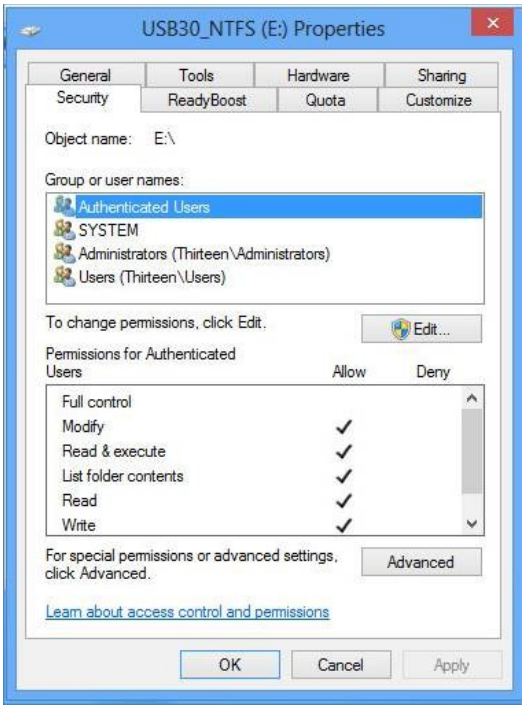
The change is confirmed.

Renaming a Token on Windows 8/8.1

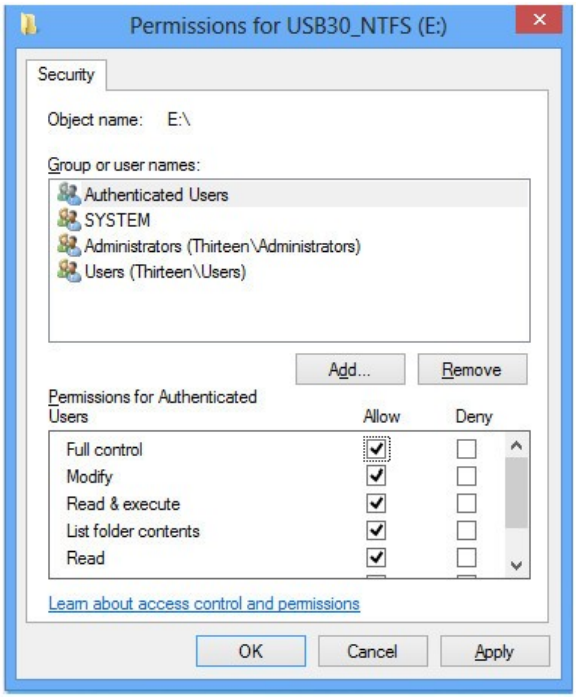
If your token is on a USB 3.0 device and your environment is Windows 8, ensure that you have “Full control” permissions to write to the device before attempting to change the token name.

To grant “Full control” permissions:

1. In Windows Explorer, right-click the USB 3.0 drive, and select **Properties**.
2. On the **Security** tab, in the **Group or user names** box, select **Authenticated Users**.



3. Click **Edit**.
4. If prompted, enter the administrator credentials.
5. In the **Permissions for Authenticated Users** box, on the **Full control** row, select **Allow**.

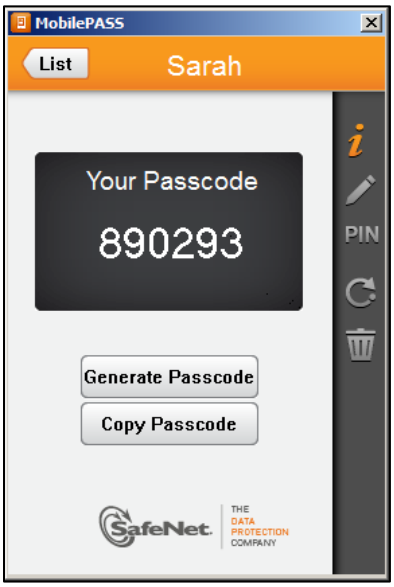


6. Click **OK** to save the changes.

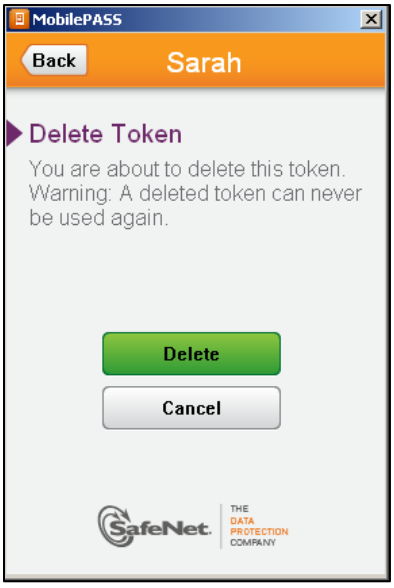
Deleting a Token

To delete a token:

1. Open MobilePASS, select the token name from the list, and if prompted, enter your PIN.
2. From the menu items, click the **Delete Token** icon 



3. Read the warning and then click **Delete**.

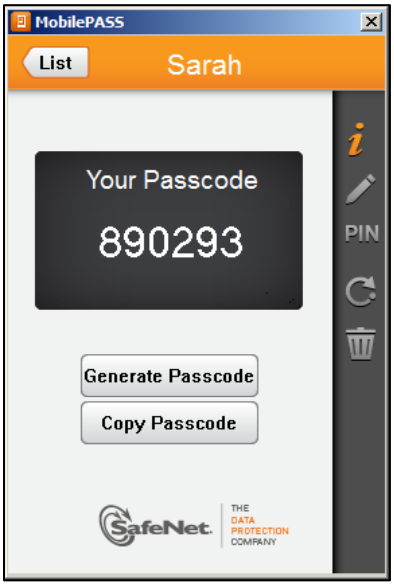


Deactivating a Token

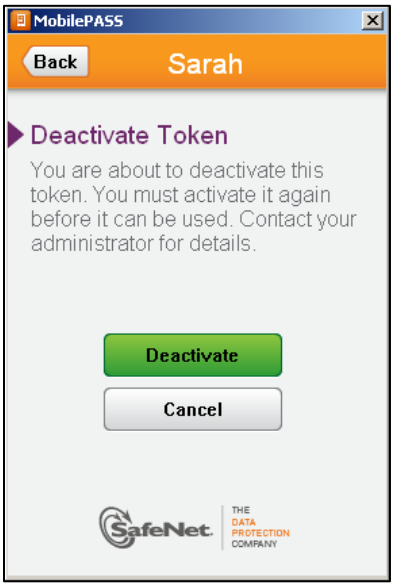
NOTE: Before deactivating tokens, contact your administrator. Unless re-enrollment privileges are enabled, you cannot re-enroll your token until the administrator removes the token from your record.

To deactivate a token:

1. Open MobilePASS, select the token name from the list, and if prompted, enter your PIN.
2. From the menu items, click the **Deactivate Token** icon 



3. Read the warning and then click **Deactivate**.



CHAPTER 7

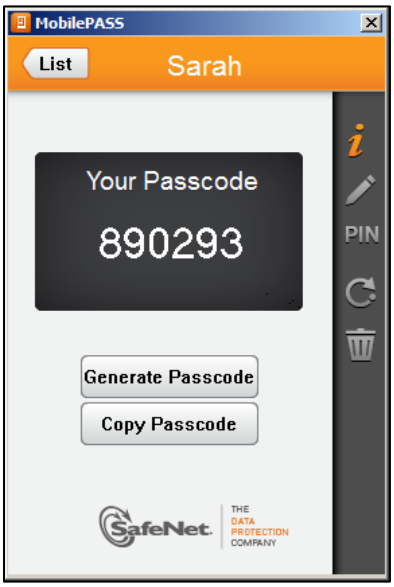
Viewing Token Information

Viewing Token Information

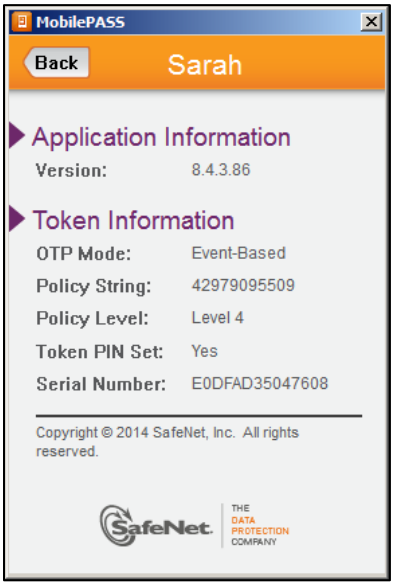
To view application and token information:

1. Open MobilePASS, select the token name from the list, and if prompted, enter your PIN.

2. From the menu items, click the **Information** icon 



The information is displayed.



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

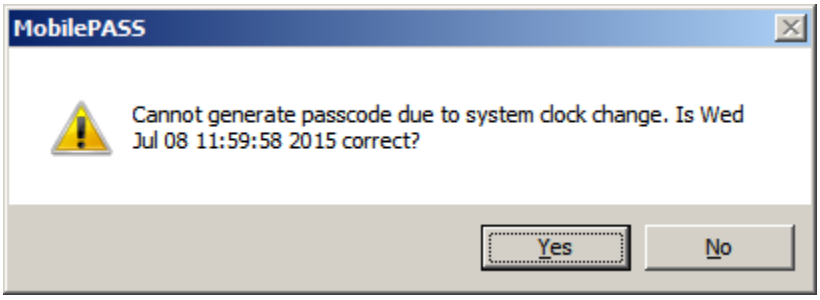
Your device was compromised, and the device's date and time were changed to a future date and time. The person who took the device generates several time-based OTPs (which will be used for authentication purposes without the SafeNet MobilePASS application), and then restores the device's time.

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.

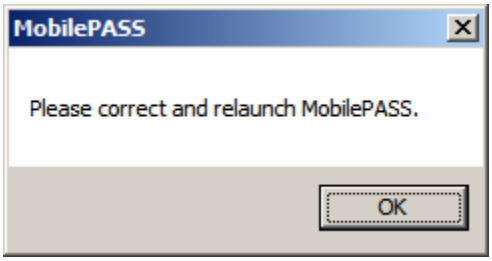
To use the time-based security feature:

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.

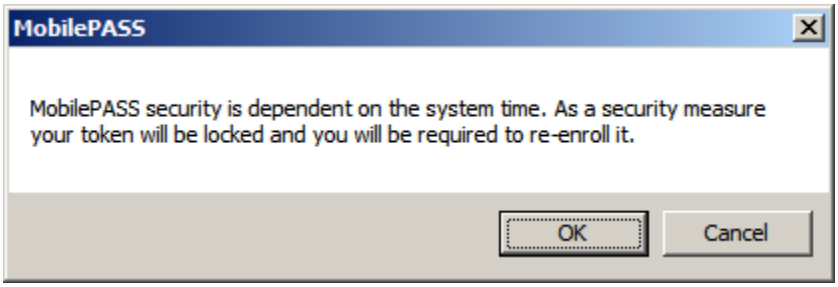
   A message is displayed indicating that an OTP could not be generated.
4. Click **No** to confirm that the displayed date and time are not correct.



5. You are prompted to change the clock back to the correct date and time. Click **OK**.



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



Your token is now locked.