

# SafeNet MobilePASS for Windows Phone User Guide



THE  
DATA  
PROTECTION  
COMPANY

## Document Information

<b>Product Version</b>	8.4
<b>Document Part Number</b>	007-012867-001, Rev A
<b>Release Date</b>	6 January 2015

## 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	Contact Information
<b>Mail</b>	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
<b>Email</b>	<a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a>

# Contents

<b>CHAPTER 1 Overview</b> .....	<b>4</b>
What is a SafeNet MobilePASS Token? .....	4
How does SafeNet MobilePASS protect me? .....	4
How do I generate an OTP on my mobile device? .....	4
How do I get started with SafeNet MobilePASS? .....	4
I have not received an enrollment email, what should I do? .....	4
For how long will my token continue to operate? .....	5
What is self-enrollment? .....	5
What are the benefits of using the token? .....	5
How do I protect my security PIN? .....	5
What if I forget my PIN? .....	5
What if my token is locked? .....	5
What should I do if I can't log on using my token? .....	5
<b>CHAPTER 2 Enrolling MobilePASS</b> .....	<b>6</b>
Downloading the MobilePASS Application .....	6
Enrolling a MobilePASS Token .....	6
Automatic Enrollment .....	7
Enrolling by Copying and Pasting the Activation String .....	9
Creating a New Token .....	13
<b>CHAPTER 3 Creating and Changing a Token PIN</b> .....	<b>15</b>
Creating a Token PIN .....	15
Changing a Token PIN .....	16
<b>CHAPTER 4 Generating Passcodes</b> .....	<b>18</b>
Generating a Passcode with Time-Based Tokens .....	18
Generating Passcodes with Challenge-Response Tokens .....	19
<b>CHAPTER 5 Renaming, Deleting and Activating a Token</b> .....	<b>20</b>
Renaming a Token .....	20
Deleting a Token .....	21
Deactivating a Token .....	22
<b>CHAPTER 6 Viewing Token and Phone Information</b> .....	<b>23</b>
Viewing Token Information .....	23
Viewing Windows Phone Application Information .....	23
<b>CHAPTER 7 Security Enhancements</b> .....	<b>24</b>
Event-Based Token Security Enhancements .....	24
Time-Based Token Security Enhancements .....	24

# CHAPTER 1

## Overview

As a SafeNet MobilePASS for Windows Phone user, you can generate One Time Passcodes (OTP) on your Windows Phone device, and use those passcodes to authenticate to SafeNet-protected corporate and web-based applications.

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

This document provides information on how to install and run the SafeNet MobilePASS token.

### What is a SafeNet MobilePASS Token?

---

A SafeNet MobilePASS Token is an application that generates an OTP to use for secure remote access to corporate and web-based applications. It works independently of mobile network connectivity.

### How does SafeNet MobilePASS protect me?

---

Password theft is the method used most frequently by thieves and hackers to steal identities and gain unauthorized access to computer networks. While they have many ways to steal a password, success depends on the stolen password being valid, in much the same way that credit card theft relies on the card being usable until you report it missing. SafeNet MobilePASS prevents the stolen password being used to log 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 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.

### How do I generate an OTP on my mobile device?

---

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

### How do I get started with SafeNet MobilePASS?

---

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

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

---

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

## For how long will my token continue to operate?

---

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

## What is self-enrollment?

---

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

## What are the benefits of using the token?

---

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

## How do I protect my security PIN?

---

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

## What if I forget my PIN?

---

If your SafeNet MobilePASS token is configured to use a PIN and you forget it, contact your company's help desk. They will verify your identity and reset your PIN.

## What if my token is locked?

---

This indicates that there has been an attempt to generate OTPs using an incorrect PIN. Contact your help desk.

## What should I do if I can't log on using my token?

---

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

# CHAPTER 2

## Enrolling MobilePASS

### Downloading the MobilePASS Application

---

Download and install the application from the Windows Phone Store.

Once installed, the MobilePASS application will be visible on the Windows Phone menu.



### Enrolling a MobilePASS Token

---

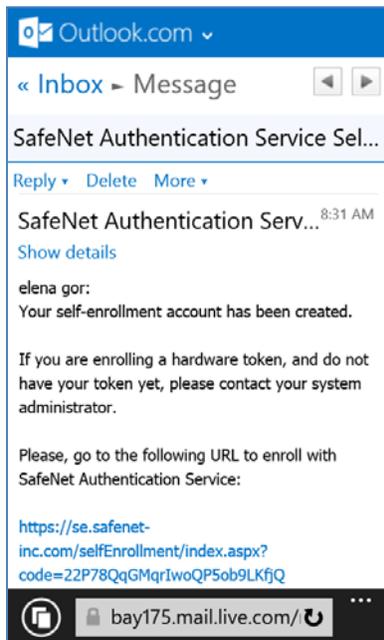
Enroll a MobilePASS token to generate an OTP on your mobile device without the need for a physical token. The token works independently of mobile network connectivity.

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

- **Automatic Enrollment** - Automatically copy and paste the activation code into the Auto Enrollment window by clicking the **Enroll your MobilePASS token** link on the notification email (see **Enrolling MobilePASS**, page 6)
- **Copy and Paste Activation String into the Automatic Enrollment Window** – If your company is using SafeNet Authentication Manager (SAM), or if you experience difficulties with the Automatic Enrollment, copy the activation string into the Auto Enrollment window (See **Enrolling by Copying and Pasting the Activation String**, page 9).

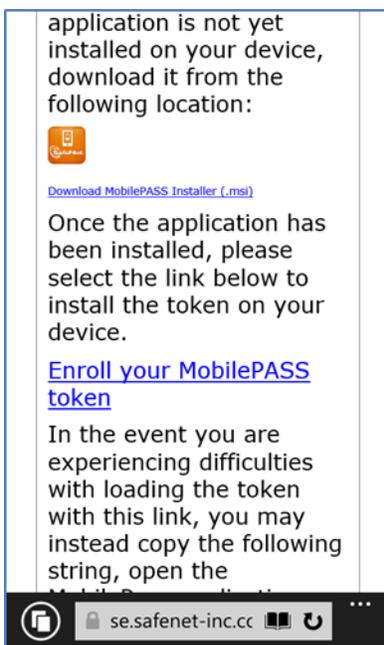
## Automatic Enrollment

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



### To Enroll MobilePASS Automatically:

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



2. If you have not downloaded **SafeNet MobilePASS for Windows Phone**, tap the icon to download and install.

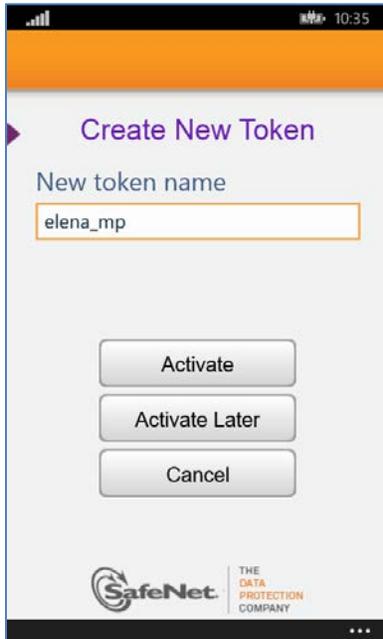


3. Tap the **Enroll your MobilePASS token** link.



**NOTE:** The default token name is displayed in the **Create New Token** window as it has not yet been enrolled. If your default token was previously enrolled, the window appears with a blank display, enabling you to create and then enroll a new token.

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

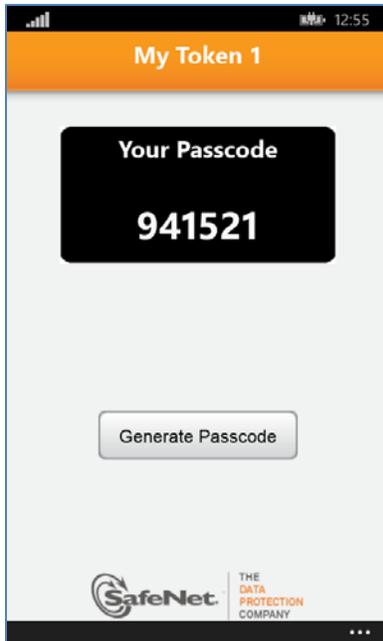


5. If your token is PIN protected, the **Enter a Token PIN** window appears. Enter the PIN and tap **Continue**.



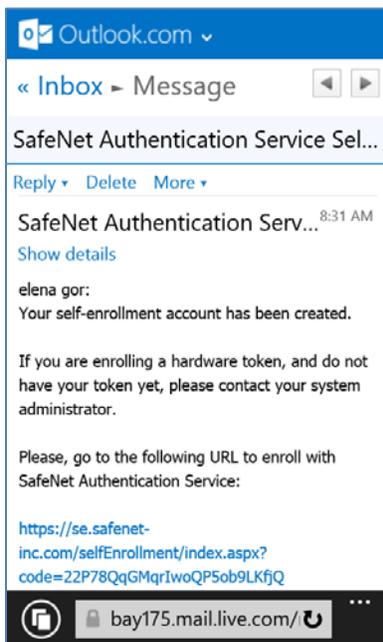
**NOTE:** The required number and type of characters required for the PIN depends on the configuration of your system. The requirement could be for four, six or eight digits, either numeric or alphanumeric.

6. Your Passcode is displayed on your MobilePASS window.



## Enrolling by Copying and Pasting the Activation String

Your system administrator will assign you a token and you will be sent a notification email.

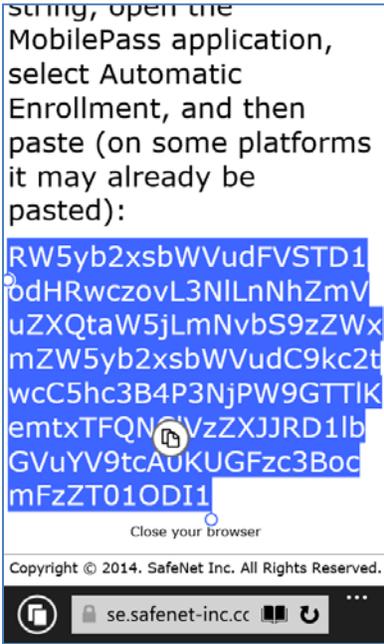


### To Enroll MobilePASS by copying and pasting the activation string:

1. Tap the **https://** link in the email.
2. In the **SafeNet Authentication Service Self-Enrollment** page, copy the activation string, ensuring that you select the entire string. The last character "=" can be ignored during the copy operation.

### To copy the activation string:

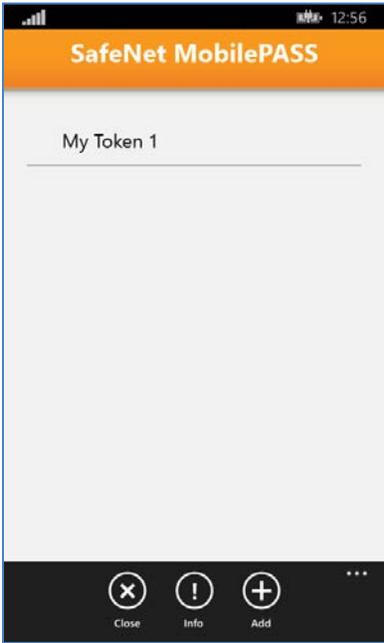
- a. Tap a word in the activation string.
- b. Drag the circles at each end of the highlighted text to include the first and last words you want to copy.



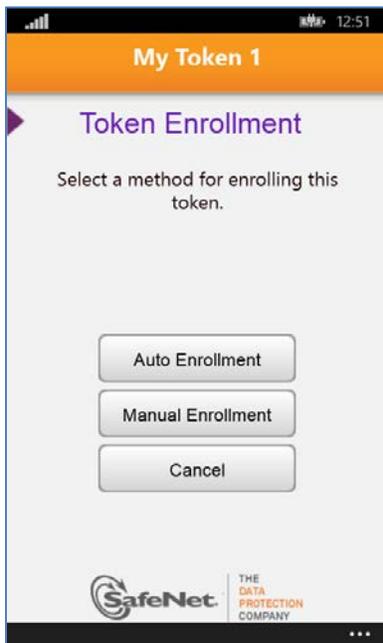
- 3. If you have not downloaded the SafeNet MobilePASS for Windows Phone, tap the icon to download and install.



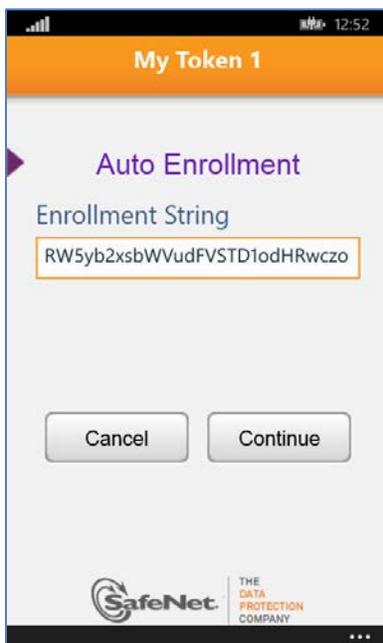
If there is not yet a token in the application, a default token named 'My Token 1' is created automatically.



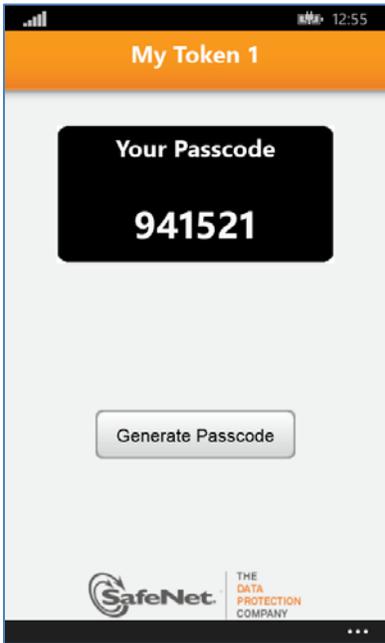
4. Tap the required token.
5. In the *Token Enrollment* window tap **Auto Enrollment**.



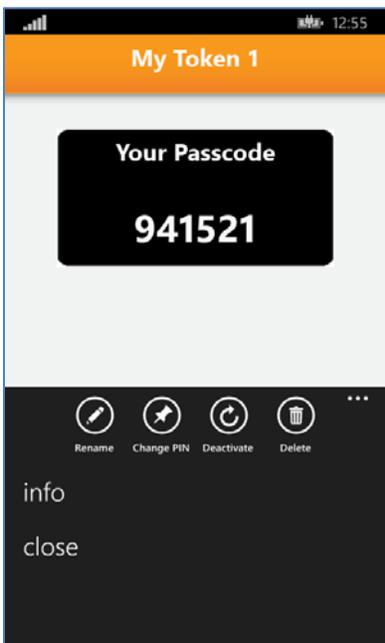
6. In the **Auto Enrollment** window, the copied Activation String is automatically pasted into the **Enrollment String** field.



7. Tap **Continue**.
8. If your token is PIN protected, the **Enter a Token PIN** window appears. Enter a four, six or eight digit numeric or alphanumeric PIN into the Token PIN field (as configured for your token), and tap **Continue**.  
Your Passcode is displayed on your MobilePASS window.



9. You can now perform other tasks such as **View Token Information**, **Change Token Name**, **Deactivate Token**, or **Delete Token**. On some devices you are required to tap the **Menu** button 

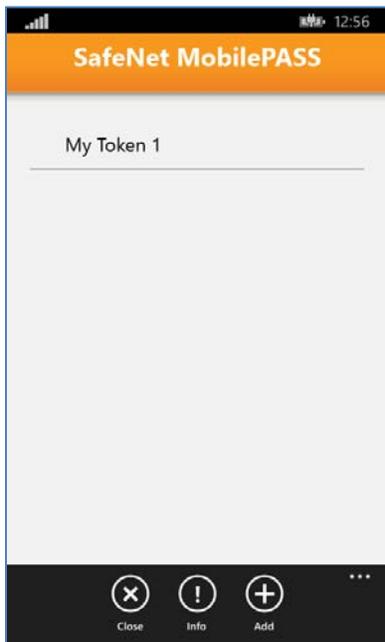


## Creating a New Token

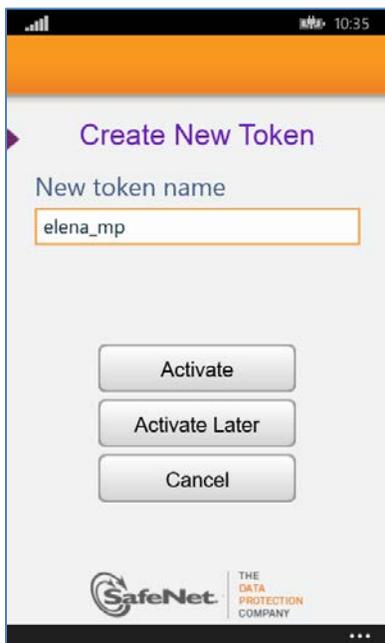
**To create a new token:**

1. Open the MobilePASS application on the device.

2. Tap **Menu**  and then tap **Add** .



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





**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**.

---

The Auto Enrollment window opens.

4. Perform enrollment as describe in **Enrolling MobilePASS**, page 6.

# Creating and Changing a Token PIN

## Creating a Token PIN

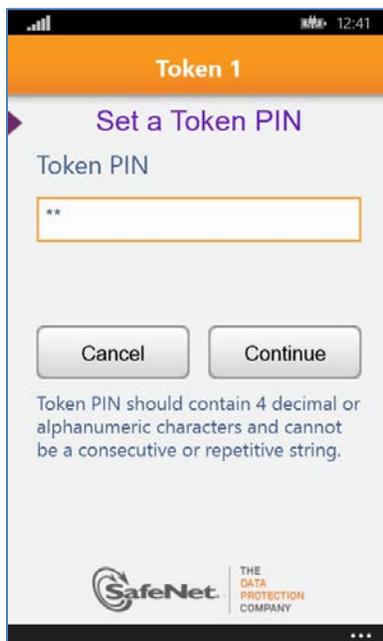


**NOTE:** The **Creating a Token PIN** option is available only if your SafeNet MobilePASS token has been configured for PIN protection.

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. In the **Set a Token PIN** window, enter a four, six or eight digit numeric or alphanumeric PIN in the **Token PIN** field (dependent on the configuration of your token).



2. Re-enter the PIN in the **Re-enter Token PIN** field.

## Changing a Token PIN

---

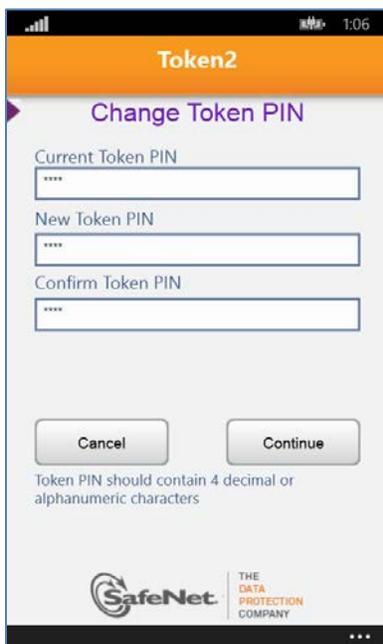


**NOTE:** The **Change Token PIN** option is available only if your SafeNet MobilePASS token has been configured for PIN protection.

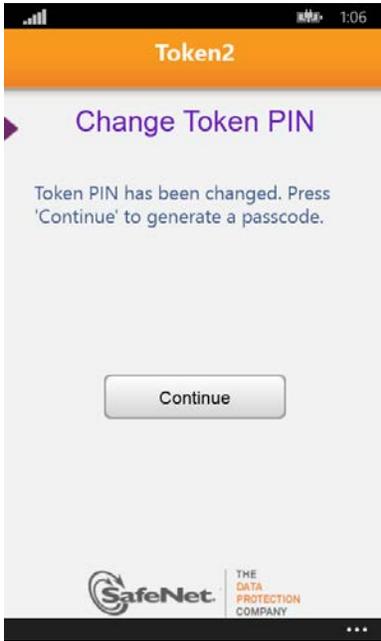
---

### To change the PIN:

1. Select the token name from the token list, and then enter your PIN to authenticate.
2. Tap **Change Token PIN** from the menu.
3. In the **Change Token PIN** window, enter the **Current Token PIN**, then enter the **New Token PIN** and confirm.



The **Change Token PIN** is displayed.



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

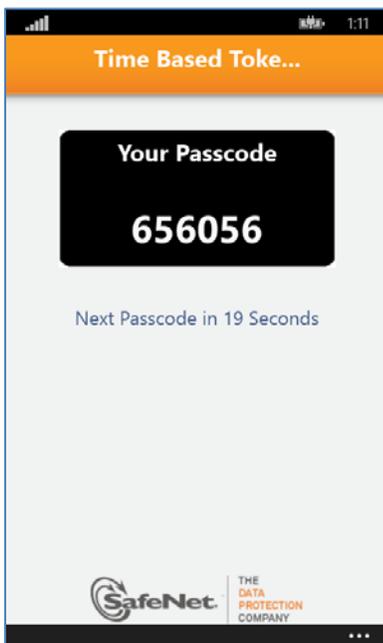
---

# CHAPTER 4

## Generating Passcodes

### Generating a Passcode with Time-Based Tokens

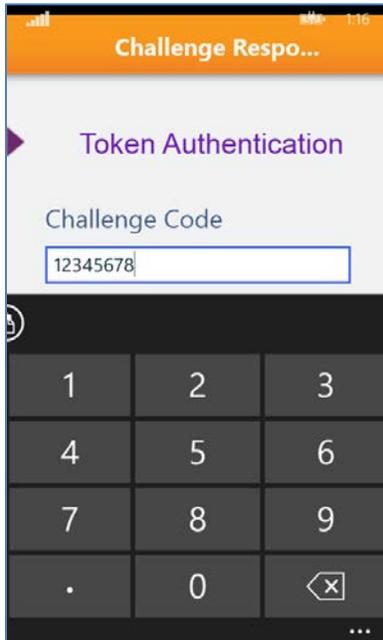
If you are using a time-based token, the One Time Passcode (OTP) is automatically generated after the specified time interval has elapsed.



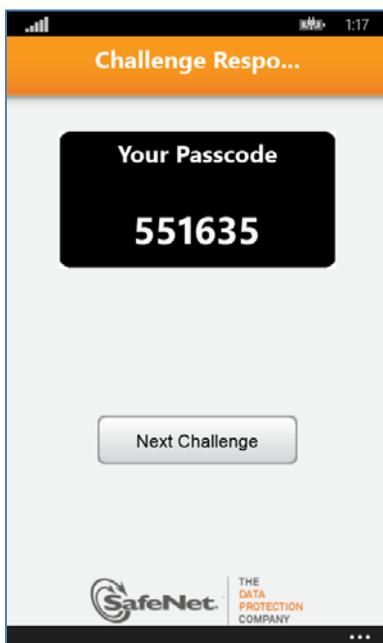
# Generating Passcodes with Challenge-Response Tokens

To generate a passcode with a challenge-response token:

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



2. Tap **Generate Passcode**. The passcode appears.
3. To generate another passcode, tap **Next Challenge**, and then repeat this process.



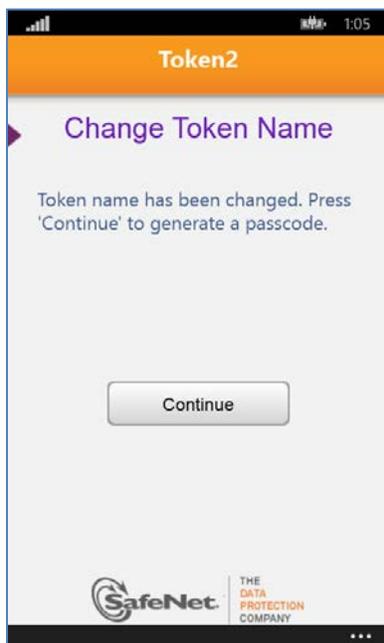
# Renaming, Deleting and Activating a Token

## Renaming a Token

---

### To change a token name:

1. Select the token name from the token list and, if your token is PIN protected, enter your PIN.
2. Tap **Rename Token**.
3. Enter your new token name and then tap **Continue**.

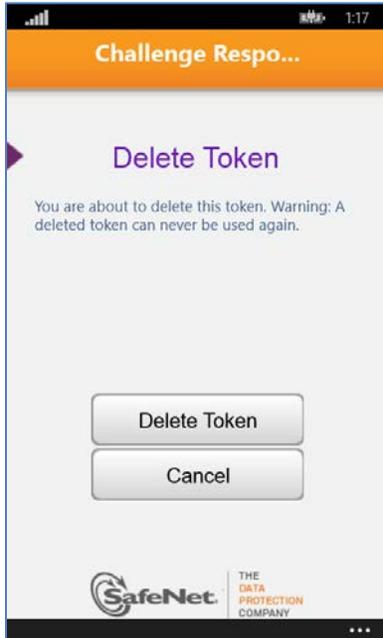


## Deleting a Token

---

### To delete a token:

1. Select the token name from the token list and if your token is PIN protected, enter your PIN.
2. Tap **Delete Token** from the menu options.



3. Read the warning, and then tap **Delete**.

## Deactivating a Token

---

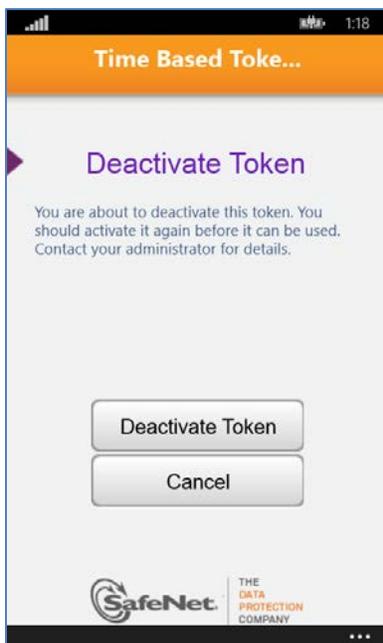


**NOTE:** Before deactivating tokens, contact your administrator. Unless re-enrollment privileges are enabled, you cannot reenroll your token until the administrator removes the token from your record.

---

### To deactivate a token:

1. Select the token name from the token list and, if your token is PIN protected, enter your PIN.
2. Tap **Deactivate Token** from the menu options.



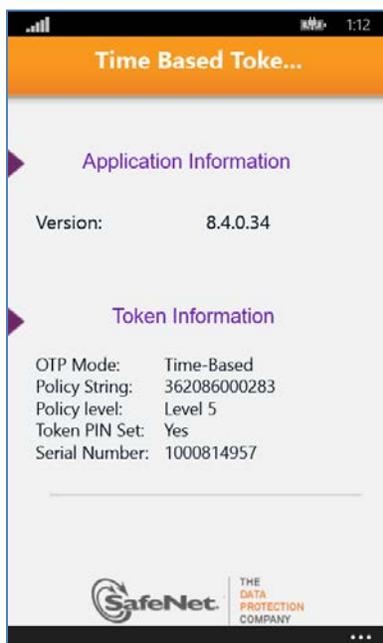
3. Read the warning, and then tap **Deactivate**.

# Viewing Token and Phone Information

## Viewing Token Information

### To view token information:

1. Select the token name from the token list, and if your token is PIN protected, enter your PIN.
2. Select Token Information from the menu options. The Token Information window appears.



## Viewing Windows Phone Application Information

You can view specific application information, as well as uninstall the application from your Windows Phone device.

To view Windows Phone application information on your Windows Phone device, tap **Settings>Apps>MobilePASS**. The *App info* window appears.

# CHAPTER 7

## Security Enhancements

### Event-Based Token Security Enhancements

---

Event-based tokens can be configured to support a delay in the pre-defined number of seconds before another OTP is generated.

### Time-Based Token Security Enhancements

---

Time hacking countermeasures have been implemented, alerting users to the possibility that their device has been compromised, and that future OTPs were generated.

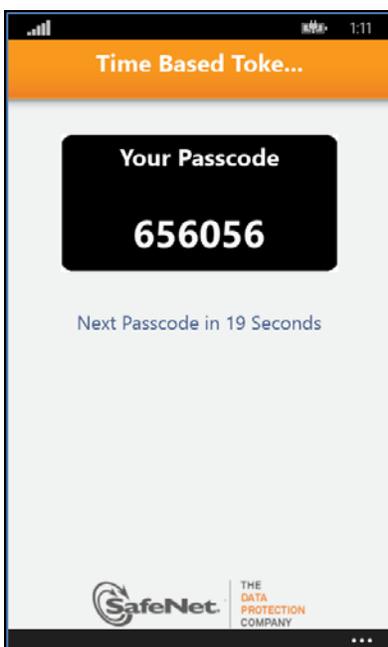
#### Time-based Security Enhancement Scenario

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

With the new security enhancement, SafeNet MobilePASS is able to detect that the device was manipulated and alerts the user to the possibility of such an attack.

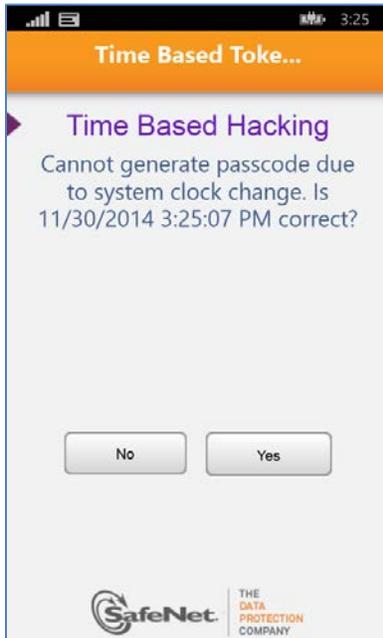
#### To use the time-based security enhancement:

1. Open the SafeNet MobilePASS application, create a time-based token, and then generate an OTP.

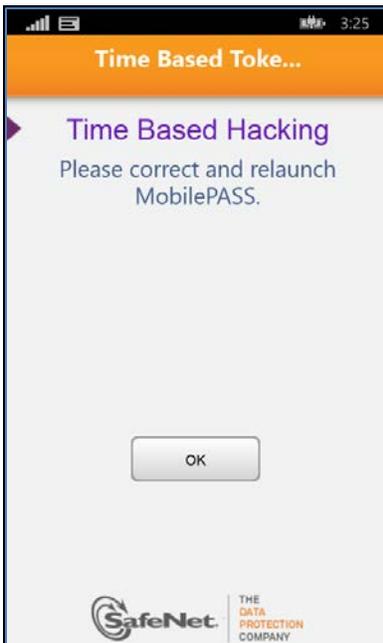


2. Move the device's date and time forward, and then generate an OTP.

- Restore the clock's date and time, and then generate another OTP.  
A message appears indicating that an OTP could not be generated.
- Tap **No**; you are prompted to change the clock back to the correct date and time.

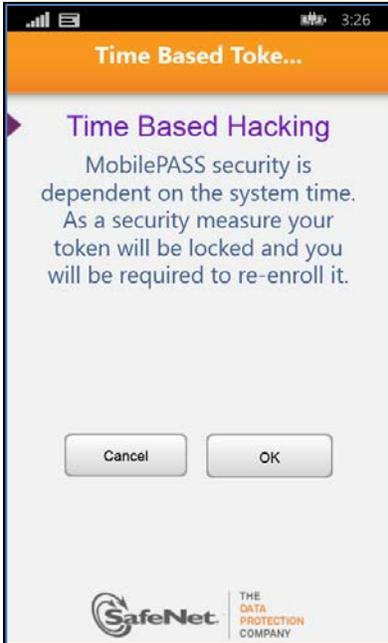


- Tap **OK**.



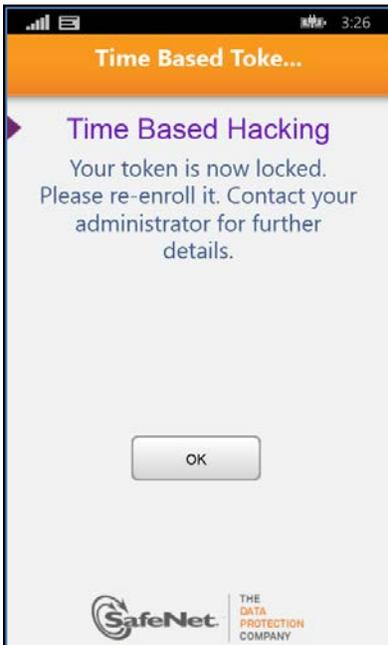
-

Security measures are taken and, if confirmed, your token will be blocked.



You now need to re-enroll your token.

7. Tap **OK** to lock your token.



8. Tap **OK** to go back to the token list screen.
9. To access this token again, start the process from the beginning.