



MobilePASS for BlackBerry OS 10

CUSTOMER RELEASE NOTES

Version: 8.4
Build: 84
Issue Date: 25 March 2015
Document Part Number: 007-012937-001, Rev. B

Contents

Product Description	2
Release Description.....	2
New Features and Enhancements.....	2
BES 10 and BES 12 support.....	2
Improved User Interface	2
Management Platform Support	2
Cryptographic Security.....	2
Default Token Name	2
Event-based Security Features.....	3
Time-based Security Features.....	3
Known Issues	5
Compatibility and Upgrade Information.....	6
Interoperability	6
BlackBerry Devices	6
Authentication Management Systems.....	6
Download and Installation.....	6
Upgrade	6
Product Documentation	6
Support Contacts	7

Product Description

SafeNet's MobilePASS family of one-time password (OTP) software authentication solutions combines the security of proven two-factor strong authentication with the convenience, simplicity, and ease of use of OTPs generated on personal mobile devices. By turning a mobile phone into a two-factor authentication device, organizations save significantly on hardware and deployment costs, while users benefit by not having to carry an additional hardware token.

Release Description

The MobilePASS 8.4 for BlackBerry OS 10 release enables BlackBerry customers using BlackBerry Enterprise Server (BES) 10 or 12 to deploy MobilePASS from their mobile device management (MDM) system.

To learn about using BlackBerry Enterprise Server (BES) 10 and 12, refer to BlackBerry documentation: <http://docs.blackberry.com/en/admin/?userType=2>



NOTE: This version of MobilePASS for BlackBerry OS 10 is available only as a standalone .bar file.

New Features and Enhancements

BES 10 and BES 12 support

MobilePASS 8.4 for BlackBerry OS 10 can be deployed by the BlackBerry Enterprise Server (BES) 10 or 12 to BlackBerry OS 10 devices.

Improved User Interface

MobilePASS 8.4 for BlackBerry OS 10 improves the user experience with an enhanced user interface.

Management Platform Support

SafeNet Authentication Service (Cloud) and SafeNet Authentication Manager are supported, offering full featured activation and policy management capabilities.

Cryptographic Security

BlackBerry FIPS 140-2 Level 1 cryptographic libraries are supported.

Default Token Name

The MobilePASS default token name for the first token is taken from the user name as configured in SAS. After activation, the default token name includes the user name.

Event-based Security Features

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

Time-based Security Features

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

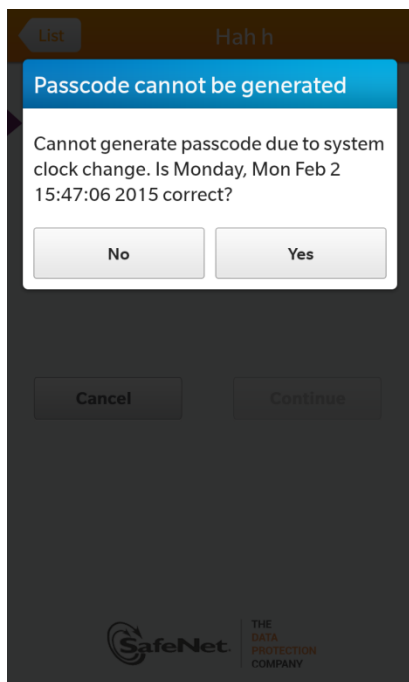
Time-based Security Enhancement Scenario

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.

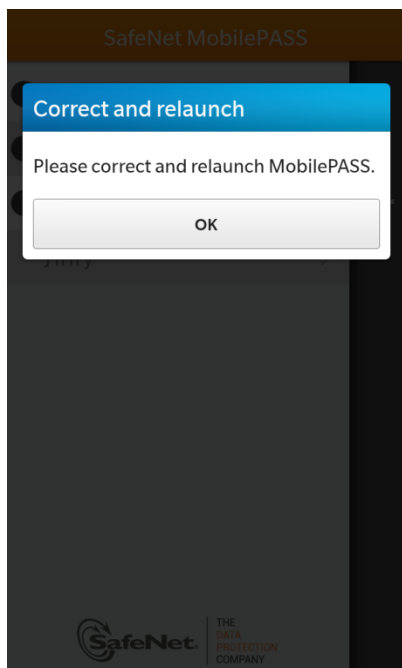
With the time-hacking countermeasures, SafeNet MobilePASS is able to detect that the device was manipulated and alerts the user to the possibility of such an attack.

To use the time-based security feature:

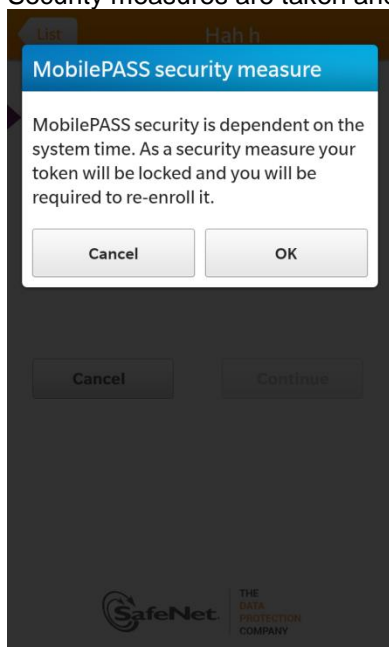
1. Open the SafeNet MobilePASS application, create a time-based token, and then generate an OTP.
2. Move the device's date and time forward, and then generate an OTP.
3. Restore the clock's date and time, and then generate another OTP.
A message is displayed indicating that an OTP could not be generated.
4. Tap **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. Tap **OK**.

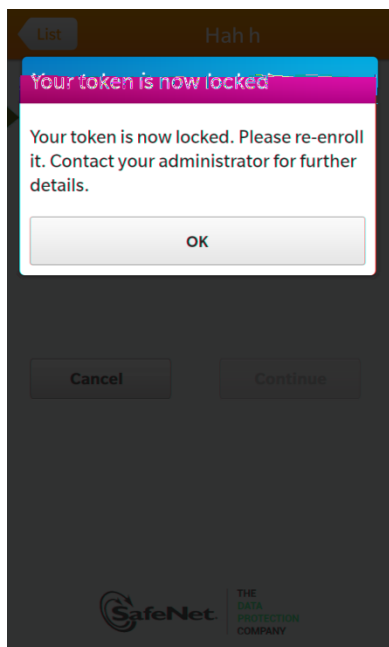


6. Security measures are taken and, if confirmed, your token will be locked. Tap **OK** to confirm.



You now need to re-enroll your token.

7. Tap **OK** to go back to the token list screen.



8. To access this token again, start the process from the beginning.

Known Issues

Issue	Synopsis
MPGA-756	<p>Summary: After generating a time-based OTP while the time stamp of the last generated OTP is later than the current system time, the user is not informed with a clear message that the error has occurred and is not prompted to update the system time to the current time.</p> <p>Workaround: Ignore message; does not affect functionality. Continue the steps as described in “Time-based Security Features” on page 3.</p>

Compatibility and Upgrade Information

Interoperability

BlackBerry Devices

MobilePASS 8.4 for BlackBerry OS 10 supports the following BlackBerry devices running OS 10.2 or higher:

- Passport
- Z10
- Z30
- Q5
- Q10

Authentication Management Systems

MobilePASS 8.4 is supported by the following SafeNet authentication platforms:

- SafeNet Authentication Service (SAS) Cloud
- SafeNet Authentication Manager (SAM) 8.2 - latest Hotfix
- SafeNet Authentication Manager Express (SAMx) 8.1

Download and Installation

MobilePASS 8.4 for BlackBerry OS 10 can be deployed through the BlackBerry Enterprise Server (BES) 10 and 12.



NOTES:

This version of MobilePASS for BlackBerry OS 10 is available only as a standalone .bar file.

To learn about using BlackBerry Enterprise Server (BES) 10 and 12, refer to BlackBerry documentation: <http://docs.blackberry.com/en/admin/?userType=2>

Upgrade

MobilePASS 8.4 for BlackBerry OS 10 does not support upgrade from earlier releases.

Product Documentation

The following product documentation is associated with this release:

- SafeNet MobilePASS 8.4 for BlackBerry OS 10 User Guide

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 SafeNet Customer Support. SafeNet 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 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.

Contact Method	Contact Information	
Address	SafeNet, Inc. 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 SafeNet Knowledge Base.	