FortiToken Mobile for iOS

Release Notes

VERSION 4.2.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

1/26/2018

FortiToken - Release Notes for iOS FortiToken Mobile 4.2.0

33-420-412648-20180126

TABLE OF CONTENTS

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions and caveats, resolved and known issues for FortiToken Mobile for iOS, version 4.2.0, build 0084.

FortiToken Mobile is an OATH compliant, time-based one-time password (OTP) generator application for mobile devices. FortiToken Mobile produces its one-time password (OTP) codes in an application that you can download to your Android, iOS, or Windows mobile device without the need for a physical token.

Go to the Apple App Store to download the free FortiToken Mobile application for iOS.

For additional documentation, please visit: http://docs.fortinet.com/fortitoken/.

What's New

Before upgrading, review the following changes for impact to your unique deployment. Note that this list is not exhaustive but highlights the major feature enhancements in this release.

- Secure token transfer — requires FortiAuthenticator 5.3 or higher.
- Support for iPhone X Face ID.
- Support for new FortiAuthenticator PIN Policy setting — no pin required, optional pin required, or enforced pin required — with FortiAuthenticator 5.2 or higher.

Product support

iOS devices and version support

iPhone and iPad for iOS version 9.0 and higher is supported.

iOS version 8 is no longer supported.

FortiOS and FortiAuthenticator support

FTM for iOS is supported by FortiOS 5.2.11 GA (build 0754), FortiOS 5.4.4 GA (build 1117), and FortiOS 5.6 GA (build 1149), and by FortiAuthenticator 4.3.2 GA (build 0222).

FortiToken platform scalability

The following table shows the maximum number of FortiTokens that can be assigned to certain FortiGate and FortiAuthenticator models. Note that FortiToken is also supported on specific FortiWiFi models.

All data for this table was taken from the following Product Matrix datasheet.

FortiGate Models	Max. FortiTokens
30E	20
50E / 60D / 60E / 70D / 80D / 90D / 90E	100
100D / 100E / 200D / 200E / 300D / 500D / 600D / 800C / 900D	1,000
1000D / 1200D / 1500D / 2000E / 2500E / 3000D / 3100D / 3200D / 3700D / 3800D / 7040E VMware / Xen / AWS / AWS on Demand / KVN / Hyper V	5,000

FortiAuthenticator Models	Max. FortiTokens
200E	500
400E	2,000

FortiAuthenticator Models	Max. FortiTokens
1000D	10,000
2000E	20,000
3000D / 3000E	40,000
VM BASE to VM-100000-UG	200 to 200,000+

Registering FortiToken Mobile

You will need a certificate to register FortiToken Mobile. There are two options for getting FortiToken Mobile certificates for use on your authentication server: FortiToken Mobile Redemption Certificate, and FortiToken Mobile Free Trial “virtual” certificate.

For each FortiToken Mobile purchase, you will receive a physical redemption certificate. Scratch off the designated area of the redemption certificate to reveal the 20-digit activation code.

The following steps show how to register FortiToken Mobile on a FortiGate and FortiAuthenticator.

On the FortiGate

1. Locate the 20-digit code on the redemption certificate.
2. Go to **User & Device > FortiTokens** and select **Create New**.
3. Select **Mobile Token**, and enter the 20-digit certificate code in the **Activation Code** box.
4. Select **OK**.

On the FortiAuthenticator

1. Locate the 20-digit code on the redemption certificate.
2. Go to **Authenticaton > User Management > FortiTokens** and select **Create New**.
3. Select **FortiToken Mobile**, and enter the 20-digit certificate code in the **Activation codes** box.
4. Select **OK**.

To ensure messaging functions properly, you must configure the messaging server, configure users to receive messages from the server by email or SMS, and provision FortiToken Mobile for the user on the FortiGate and/or FortiAuthenticator.

To see more information on how to provision FortiToken Mobile for a user on a FortiGate and FortiAuthenticator, see the FortiToken Mobile - User Instructions.

For more information see the FortiToken Mobile product datasheet available on the Fortinet web site at https://www.fortinet.com/products/identify-and-access-management/network-authentication/fortitoken-mobile.html

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release.

For inquiries about a particular bug, please Fortinet Customer Service & Support: https://support.fortinet.com.

Bug ID	Description
458770	FortiToken Mobile iOS client certificate added to approve/deny login notification on FortiGate devices.
440644, 442792	Fix bypass pin/touchID issue on FortiToken Mobile iOS.
462053	Update PIN behavior when the application is Open.
453146	Change PUSH validation message of login attempt.
442604	Fix crash when decrypting PUSH data.
436500	Fix issue where encrypted backup on iOS 9 can be restored to different iOS 10 device.

Known issues

This section lists the known issues of this release, but is not a complete list.

For inquiries about a particular bug, please Fortinet Customer Service & Support: https://support.fortinet.com.

Bug ID	Description
-	Transfer token feature will work with FortiAuthenticator (5.3), but does not work with FortiGate as the token issuer.
464780	Transfer duplicate token case.
466088	Token status is out of sync between FortiAuthenticator and FortiClient.
468079	Old device still gets “no token found” after transfer tokens were deleted.
448100	FortiToken Mobile should show warning to complete transfer token on the same device.
462556	FortiToken Mobile hasn’t translated ‘transfer token’ feature into Simplified Chinese.
468040	FortiToken Mobile still shows ‘invalid’ when hide invalid token value.
459087	Black screen issue on iPhone X when enabling FaceID for the first time (due to iOS system time delay).
-	Users will see the "Create your pin" view immediately if the FortiAuthenticator PIN required policy on a token activated from pre-5.2 FortiAuthenticator on FortiToken Mobile 4.1.1, and then upgrade to FortiToken Mobile 4.2. When the user has the device-lock enabled, and has FortiAuthenticator-enforced pin (4, 6, or 8 digits), and a token activated from pre-FortiAuthenticator 5.2 on FortiToken Mobile 4.1.1, the user can directly activate the token without creating a pin on FortiToken Mobile 4.1.1. Once FortiToken Mobile 4.2 is available, the first view users will see is the "Create your pin" view.

Special notices

This following considerations should be taken into account for this release of FortiToken Mobile for iOS.

FortiAuthenticator PIN challenge bypass

On a device with **iOS Passcode** enabled, if a token is installed that has "PIN Required" enforced on the FortiAuthenticator, and the enforced PIN length is less than or equal to six digits, the application will bypass the PIN challenge.

Restoring old tokens

If tokens were restored from a different iOS device, or if the restoration was carried out with unencrypted backups from the same device in a previous FTM version, for security reasons, you will be forced to delete all tokens from the current device and re-install them. This is the case even if you installed valid tokens after restoring old tokens.