FortiToken Mobile for iOS - Release Notes

Version 5.0.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

10/07/2019
FortiToken Mobile for iOS 5.0.2 Release Notes
33-502-586107-201901007

TABLE OF CONTENTS

Change log

Date	Change Description
2019-10-03	Initial release.

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 5.0.2, build 0004.

FortiToken Mobile is an OATH compliant, time-based one-time password (OTP) generator application for mobile devices. FortiToken Mobile produces its 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, visit FortiToken | Fortinet Documentation Library

What's new

FortiToken Mobile for iOS version 5.0.2 includes the following new features and enhancements:

- Bug Fixes

Product support

iOS devices and version support

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

FortiOS and FortiAuthenticator support

FortiToken Mobile for iOS is supported by FortiOS 5.2.11 GA and later, and by FortiAuthenticator 4.3.2 GA and later.

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.

FortiGate Models	Max. FortiTokens
30D / 30E / 50E / 60D / 60E / 70D / 80D / 80E / 90D / 90E	500
100D / 100E / 140D / 140E / 200D / 200E / 300D / 300E / 400D / 500D / 500E / 600D / 800D / 900D	5,000
1000D / 1200D / 1500D / 2000E / 2500E / 3000D / 3100D / 3200D / 3600E / 3601E / 3700D / 3800D / 3810D /3815D /3960E /3980E / 5100D / 5100E VMware / Xen / AWS / AWS on Demand / KVN / Hyper V	20,000

FortiAuthenticator Models	Max. FortiTokens
200E	1000
400E	4,000
1000D	20,000
2000E	40,000
3000D / 3000E	80,000
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 FortiGate and FortiAuthenticator devices.

On the FortiGate device

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 device

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 FortiAuthenticator devices.

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

For more information see the FortiToken Mobile Data Sheet.

Resolved issues

There are no resolved issues with this release.

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

For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
3502378	Fixed issue where Registration ID ended with an extra character '}' in FortiToken Mobile
3481504	Fixed issue where FortiToken Mobile would briefly show tokens before authentication is prompted.

Known issues

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

For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
	No new known issues

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 FortiToken Mobile 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.