Release Notes

FortiToken Mobile for Android 6.5.0

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

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

June 12, 2026
FortiToken Mobile for Android 6.5.0 Release Notes
33-650-1297919-20260612

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-06-12	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 Android, version 6.5.0, build 0028.

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 Google Play store to download the free FortiToken Mobile for Android application.

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

What's new

FortiToken Mobile for Android version 6.5.0 includes the following enhancements:

- Separate token value displayed in the app for improved readability
- App PIN: Security Requirements and Invariants
- App PIN: Per-Issuer Policy Tracking with Deletion Recalculation
- App PIN: Migrate Password Hashing to Argon2id
- App PIN: Migrate Auth Data to Hardware-Backed Storage
- Request Camera Permission On Demand

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, visit the FortiCare portal website.

Bug ID	Description
1264132	App PIN: Lack of salt in FTK PIN generation.
1264131	App PIN: PIN bypass due to lack of encryption in `shared_prefs`.
1284175	OTP Exfiltration via SSRF.
1284163	FortiToken PIN bypass.
1288694	App PIN validation can be bypassed via Password Manager autofill.

Product support

Android device and version support

Android version 10 and later is supported.

FortiOS and FortiAuthenticator support

FortiToken Mobile for Android is supported by FortiOS 5.2.11 and higher, and by FortiAuthenticator 4.3.2 and higher.

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 / 40F / 60F / 70F / 80F	500
100D / 100E / 140D / 140E / 200D / 200E / 300D / 300E / 400D / 400E / 500D / 500E / 600D / 600E / 800D / 900D	5,000
1000D / 1200D / 1500D / 2000E / 2500E / 3000D / 3100D / 3200D / 3400E / 3600E / 3601E / 3700D / 3800D / 3810D /3815D /3960E /3980E / 5001E / 5100D / 5100E / 6300F / 6500F / 7030E / 7040E / 7060E / 2600F / 3000F / 3300F / 3400E / 3500E / 4400F / 6300F / 6500F / 7121F/-2 VMware / Xen / AWS / AWS on Demand / KVN / Hyper V	20,000

FortiAuthenticator Models	Max. FortiTokens
200E	1000
300F	3,000
400E	4,000
800F	16,000
1000D	20,000
2000E	40,000

FortiAuthenticator Models	Max. FortiTokens
3000D / 3000E	80,000
3000F	480,000
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 & Authentication > FortiTokens* and click *Create New*.
3. Select *Mobile Token* and enter the 20-digit certificate code in the *Activation Code* field.
4. Click *OK*.

On the FortiAuthenticator

1. Locate the 20-digit code on the redemption certificate.
2. Go to *Authenticaton > User Management > FortiTokens* and click *Create New*.
3. Select *FortiToken Mobile* and enter the 20-digit certificate code in the *Activation codes* field.
4. Click *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 or FortiAuthenticator.

For more information on how to provision FortiToken Mobile for a user on FortiGate and FortiAuthenticator, see the FortiToken Comprehensive Guide.

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

www.fortinet.com