

FortiToken™ One-Time Password Token

Mobile (FTM) One-Time Password (OTP) Application with Push Notification
Hardware Token Time-Based OTP Form-Factors: FTK-200, FTK-200CD and FTK-220

Overview

Fortinet's FortiToken Mobile (FTM) and hardware OTP Tokens (FTK-200, FTK-200CD and FTK-220) are fully integrated with FortiClient, protected by FortiGuard and leverage direct management and use within the FortiGate and FortiAuthenticator security platforms. Secure your network with Fortinet's easy-to-manage, easy-to-use Two-Factor Authentication solutions.



PRODUCT OFFERINGS

FortiToken Mobile

FortiToken Mobile is an OATH compliant OTP generator application for the mobile device supporting both time-based (TOTP) and event-based (HOTP) tokens.



FortiToken 200/200CD

FortiToken 200 is part of Fortinet's broad and flexible two-factor authentication offering. It is an OATH compliant, TOTP. It is a small, keychain-sized device that offers real mobility and flexibility for the end-user.

There is no client software to install; simply press the button and the FortiToken 200 generates and displays a secure one-time password every 60 seconds to verify user identity for access to critical networks and applications. The big LCD screen of the rugged FortiToken 200 is much easier to read than other OTP tokens and there is an indicator on the screen displaying the time left until the next OTP generation. FortiToken 200CD tokens are shipped with an encrypted activation CD for the ultimate in OTP token seed security.



FortiToken 220

The FortiToken 220 OTP token is a mini credit card form factor token. The card is shipped with a pre-cut hole for key ring application. Its sleek and slim design fits neatly into your wallet.



HIGHLIGHTS

Strong Authentication at your Fingertips

It is the client component of Fortinet's highly secure, simple to use and administer, and extremely cost effective two-factor solution for meeting your strong authentication needs. This application makes your Android, iOS and Windows mobile devices behave like a hardware-based OTP token without the hassles of having to carry yet another device. Push notification allows you to view login details on your mobile device to approve or deny with one tap.

Alternatively, you can deploy hardware-based OTP token to prevent users' passwords from stolen, phishing, dictionary and brute-force attacks.

Ultra-Secure Token Provisioning

What makes FortiToken mobile OTP application superior to others on the market is that while being simple to use for the end user, and easy to administer and provision for the system administrator, it is actually more secure than the conventional hard token. The token seeds are generated dynamically, minimizing online exposure. Binding the token to the device is enforced and the seeds are always encrypted at rest and in motion.

Privacy and Control

FortiToken Mobile cannot change settings on your phone, take pictures or video, record or transmit audio, nor can it read or send emails. Further, it cannot see your browser history, and it requires your permission to send you notifications or to change any settings.

And, FortiToken Mobile cannot remotely wipe your phone. Any visibility FortiToken Mobile requires is to verify your OS version to determine app version compatibility. While FortiToken Mobile cannot change any settings without your permission, the following permissions are relevant to FortiToken Mobile operations:

- Access to camera for scanning QR codes for easy token activation
- TouchID/FaceID: used for app security, respectively
- Access to the Internet for communication to activate tokens and receive push notifications

Leverage Existing Fortinet Platforms

Besides offering out-of-the-box interoperability with any time-based OATH compliant authentication server, such as the FortiAuthenticator™ from Fortinet, the FortiToken can also be used directly with the FortiGate® consolidated security platform, including High Availability configurations.

FortiGate has an integrated authentication server for validating the OTP as the second authentication factor for SSL VPN, IPsecVPN, Captive Portal and Administrative login, thereby eliminating the need for the external RADIUS server ordinarily required when implementing two-factor solutions.

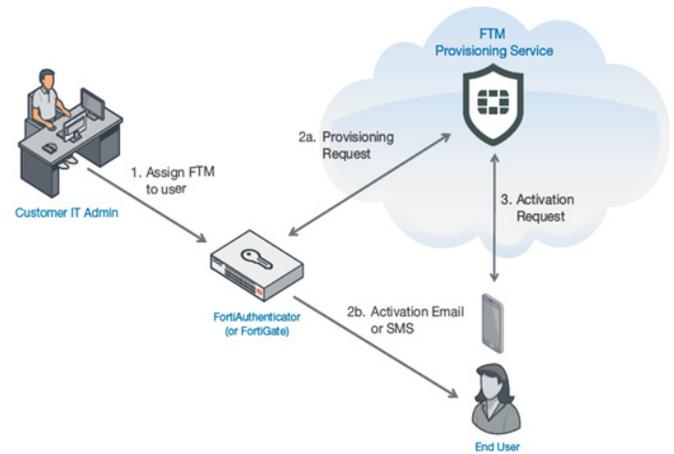
Online Activation with FortiGuard®

You can activate your FortiToken tokens online directly from FortiGate or FortiAuthenticator using the FortiGuard® Center, which maintains your token seeds in a managed service repository. Once the seeds are activated, they can no longer be accessed from FortiGuard, ensuring that your seeds are safe from compromise. Alternatively, Fortinet also offers an encrypted activation CD solution.

- "Send Feedback by Email", to automatically populate the "Sender" field
- Internally share files between applications to prepare an attachment to be sent by email for "Send Feedback by Email"
- FortiToken must keep the phone awake while it is upgrading the internal database to avoid data corruption

ADVANTAGES

- Unique token provisioning service via FortiGuard™ minimizes provisioning overhead and ensures maximum seed security
- Perpetual token license and unlimited device transfers eliminate annual subscription fees
- Scalable solution leveraging existing end-user devices offers low entry cost and TCO
- Reduces costs and complexity by using your existing FortiGate as the two-factor authentication server
- Zero footprint solution



MAIN FEATURES

FortiToken Mobile

- OATH time- and event-based OTP generator
- Login details pushed to phone for one-tap approval
- Patented Cross Platform Token Transfer
- PIN/Fingerprint protected application
- Copy OTP to the clipboard
- OTP time interval display
- Serial Number display
- Token and app management
- Self-erase brute-force protection
- Apple watch compatibility

FortiToken Hardware Devices

- Integrated with FortiClient™ and protected by FortiGuard
- OATH TOTP compliant
- Large, easy-to-read, LCD display
- Long-life Lithium battery
- Tamper-resistant/tamper-evident packaging

SUPPORTED PLATFORMS

FortiToken Mobile

- OATH time- and event-based OTP generator
- Login details pushed to phone for one-tap approval
- iOS (iPhone, iPod Touch, iPad), Android, Windows Phone 8, 8.1, Windows 10 and Windows Universal Platform
- WiFi-only devices supported (for over-the-air token activation)

FortiToken Hardware Devices

- FortiOS 4.3 and up
- FortiAuthenticator — all versions

Specifications

	FORTITOKEN 200/200CD	FORTITOKEN 220	FORTITOKEN MOBILE
Onboard Security Algorithm	OATH-TOTP (RFC6238)	OATH-TOTP (RFC6238)	OATH time and event based OTP generator
OTP Spec	60 seconds, SHA-1	60 seconds, SHA-1	RFC 6238, RFC 4226
Component	6-digit high contrast LCD display	Built-in button, 6-character LCD screen, Globally unique serial number	Supported Platforms
Dimensions (Length x Width x Height)	61.5 x 27.5 x 11.5mm	68 x 38 x 1 mm	iOS (iPhone, iPod Touch, iPad, iWatch), Android, Windows Phone 8/8.1, Windows 10 and Windows Universal Platform
Hardware Certification	RoHS Compliant	RoHS, CE, FCC (certificates pending)	Over-the-Air Token Activation
Operating Temperature	14–122°F (-10–50°C)	32–122°F (0–50°C)	WiFi-only devices supported
Storage Temperature	-4–158°F (-20–70°C)	14–140°F (-10–60°C)	One-Tap Approval
Water-Resistant	IP54 (Ingress Protection)	IP54 (Ingress Protection)	Login details pushed to phone
Casing	Hard Molded Plastic (ABS) Tamper-Evident	Hard Molded Plastic (ABS) Tamper-Evident	PIN/Fingerprint/Facial Security
Secure Storage Medium	Static RAM	Static RAM	Serial Number Display
Battery Type	Standard Lithium Battery	Standard Lithium Battery	Token and App Management
Battery Lifetime	3–5 Years	3–5 Years	Self-Erase Brute-Force Protection
Customization Available*	Casing Color, Company Logo, Faceplate Branding	Casing Color, Company Logo, Faceplate Branding	

*. Customizations are quantity-based.

PLATFORM SCALABILITY

FortiToken scalability for specific platforms can be found in the Fortinet Product Matrix located at http://www.fortinet.com/sites/default/files/productdatasheets/Fortinet_Product_Matrix.pdf

Order Information

Product	SKU	Description
FortiToken Software License Key	FTM-ELIC-5	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5 users. Electronic licence certificate.
	FTM-ELIC-10	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10 users. Electronic licence certificate.
	FTM-ELIC-20	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 20 users. Electronic licence certificate.
	FTM-ELIC-50	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic licence certificate.
	FTM-ELIC-100	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic licence certificate.
	FTM-ELIC-200	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 200 users. Electronic licence certificate.
	FTM-ELIC-500	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 500 users. Electronic licence certificate.
	FTM-ELIC-1000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 1000 users. Electronic licence certificate.
	FTM-ELIC-2000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users. Electronic licence certificate.
	FTM-ELIC-5000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5000 users. Electronic licence certificate.
	FTM-ELIC-10000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10000 users. Electronic licence certificate.
FortiToken 200	FTK-200-5	5 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-10	10 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-20	20 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-50	50 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-100	100 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-200	200 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-500	500 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-1000	1000 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200-2000	2000 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FortiToken 200CD	FTK-200CD-10
FTK-200CD-20		20 pieces one-time password token, time-based password generator shipped with encrypted seed file on CD. Perpetual license.
FTK-200CD-50		FortiToken OTP hardware generator shipped with CD containing encrypted seed file — 50-pack.
FTK-200CD-100		FortiToken OTP hardware generator shipped with CD containing encrypted seed file — 100-pack.
FortiToken 220	FTK-220-5	5 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-10	10 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-20	20 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-50	50 pieces, one-time password token, time-based password generator. Perpetual license.
	FTK-220-100	100 pieces, one-time password token, time-based password generator. Perpetual license.



www.fortinet.com

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.