DATA SHEET

FortiToken One-Time Password Token

Available in:

Cloud

Enable two-factor authentication with FortiToken Mobile (FTM) One-Time Password (OTP) Application with Push Notifications or a Hardware Time-Based OTP Token

Overview

Fortinet FortiToken Mobile (FTM) and hardware OTP Tokens are fully integrated with FortiClient, protected by FortiGuard, and leverage direct management and use within the FortiGate and FortiAuthenticator security platforms. Fortinet two-factor authentication solutions are easy to manage and easy to use.

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 200B/200BCD

FortiToken 200B 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 200B generates and displays a secure one-time password every 60 seconds. The password verifies user identity for access to critical networks and applications. The LCD big screen of the rugged FortiToken 200B is much easier to read than other OTP tokens. There is an indicator on the screen displaying the time left until the next OTP generation. FortiToken 200BCD tokens are shipped with an encrypted activation CD for the ultimate in OTP token seed security.

FortiToken 220

The FortiToken 220 OTP token form factor is a mini credit card that fits into a wallet. The card is also shipped with a pre-cut hole for a keyring.

HIGHLIGHTS

Convenient, Strong Authentication

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

Alternatively, hardware-based OTP tokens can be used to prevent users' passwords from being stolen via phishing, dictionary, and brute-force attacks.

Ultra-Secure Token Provisioning

FortiToken Mobile is simple to use and administer and provision for the system administrator. 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 a phone, take pictures or video, record or transmit audio, or read or send emails. Further, it cannot see browser history, and it requires permission to send notifications or to change any settings.

Additionally, FortiToken Mobile cannot remotely wipe a phone. Any visibility FortiToken Mobile requires is to verify the OS version to determine app version compatibility.

While FortiToken Mobile cannot change any settings without 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
- Access to the internet for communication to activate tokens and receive push notifications
- "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

Leverages Existing Fortinet Platforms

Besides offering out-of-the-box interoperability with any time-based OATH compliant authentication server such as FortiAuthenticator, FortiToken can also be used directly with FortiGate Next-Generation Firewalls, including with high availability configurations.

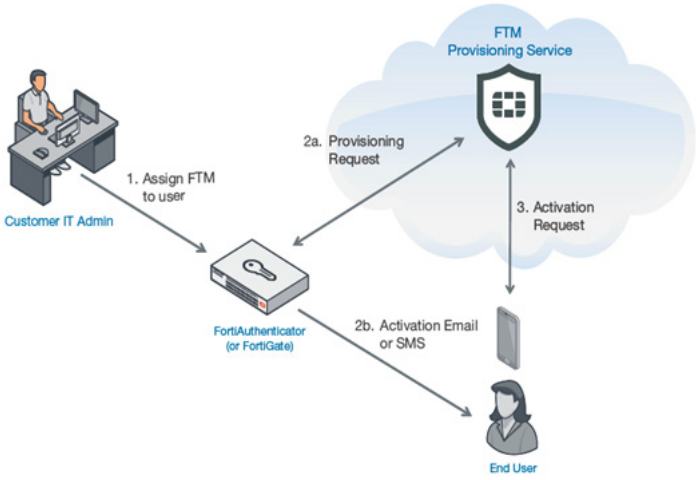
FortiGate has an integrated authentication server for validating the OTP as the second authentication factor for SSL VPN, IPsec VPN, captive portal, and administrative login. This eliminates the need for the external RADIUS server that is typically required when implementing two-factor solutions.

Online Activation with FortiGuard®

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

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 an 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
- Mobile Application Security Certified (v3.1) for Android and iOS devices
- 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
- Battery Life Indicator
- OTP Timer

SUPPORTED PLATFORMS

FortiToken Mobile

- 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 200B/ 200BCD	FORTITOKEN 220
Onboard Security Algorithm	OATH-TOTP (RFC6238)	OATH-TOTP (RFC6238)
OTP Spec	60 seconds, SHA-1	60 seconds, SHA-1
Component	6-digit high contrast LCD display	6-digit flexible display
Dimensions (Length x Width x Height)	61.6 × 28.6 × 8.9 mm	64 × 38 × 1 mm
Hardware Certification	RoHS, CE, FCC, ICES, UKCA Compliant	RoHS, CE, FCC, ICES, UKCA
Operating Temperature	50°-104°F (10°-40°C)	50°-104°F (10° - 40°C))
Storage Temperature	14°-113°F (-10°-45°C)	14° - 113°F (-10°C - 45°C)
Water-Resistant	IP67 (Ingress Protection)	IP68 (Ingress Protection)
Casing	Hard Molded Plastic (ABS) Tamper-Evident	ABS Multi-layer laminated Tamper-Evident
Secure Storage Medium	Static RAM	Static RAM
Battery Type	Standard Lithium Battery (non-rechargeable)	Lithium Battery (non-rechargeable)
Battery Lifetime	Minimum 3 Years	Minimum 3 years
Customization Available*	Casing Color, Company Logo, Faceplate Branding	Casing Color, Company Logo, Faceplate Branding

* Customizations are quantity-based

	FORTITOKEN MOBILE
Onboard Security Algorithm	OATH time and event based OTP generator
OTP Spec	RFC 6238, RFC 4226
Supported Platforms	iOS (iPhone, iPod Touch, iPad, iWatch), Android, Windows Phone 8/8.1, Windows 10 and Windows Universal Platform
Over-the-Air Token Activation	WiFi-only devices supported
One-Tap Approval	Login details pushed to phone
PIN/Fingerprint/Facial Security	✓
Serial Number Display	✓
Token and App Management	✓
Self-Erase Brute-Force Protection	✓

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 200B	FTK-200B-5	5 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-10	10 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-20	20 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-50	50 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-100	100 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-200	200 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-500	500 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-1000	1000 pieces, one-time passwork token, time-based password generator. Perpetual license.
	FTK-200B-2000	2000 pieces, one-time passwork token, time-based password generator. Perpetual license.
FortiToken 200BCD	FTK-200BCD-10	FortiToken OTP hardware generator shipped with CD containing encrypted seed file — 10-pack.
	FTK-200BCD-20	20 pieces one-time password token, time-based password generator shipped with encrypted seed file on CD. Perpetual license.
	FTK-200BCD-50	FortiToken OTP hardware generator shipped with CD containing encrypted seed file — 50-pack.
	FTK-200BCD-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 © 2022 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 is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).

FTK-OTP-DAT-R18-20220516