FortiToken™ Mobile and FortiToken™ 210

One-Time Password (OTP) Token

Product Offerings

FortiToken Mobile

OATH compliant OTP generator application, supporting both time-based (TOTP) and event-based (HOTP) tokens

FortiToken 210

Multi-Factor Authentication, OATH compliant, TOTP. A keychain-sized device that offers real mobility and flexibility.

No client software to install. Press the button, generate and display a secure one-time password every 60 seconds. The password verifies user identity.

The LCD big screen of the rugged FortiToken 210 is easy to read. The indicator displays the time left until the next OTP generation.

Multi-Factor Authentication Offers Real Mobility

Enable Multi-Factor Authentication with FortiToken Mobile (FTM) One-Time Password (OTP) application with push notifications or a hardware time-based OTP token. Fortinet FortiToken Mobile 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 Multi-Factor Authentication solutions are easy to manage and easy to use.

Highlights

Available in

Cloud

Convenient, Strong Authentication

FortiToken is the client component of the Fortinet highly secure, simple to use and administer, and cost-effective multi-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 user 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

Highlights continued

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 method eliminates the need for the external RADIUS server that is typically required when implementing multi-factor solutions.

Online Activation with FortiGuard®

FortiToken tokens can be activated online directly from FortiGate or FortiAuthenticator using the FortiGuard Center. This process 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 Multi-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
- FTK-210 is FIPS 140-2 compliant

Supported Platforms

FortiToken Mobile

- iOS (iPhone, iPod Touch, iPad), Android, Windows (Intel, AMD, Arm)
- WiFi-only devices supported (for over-the-air token activation)

FortiToken Hardware Devices

- FortiOS 4.3 and up
- FortiAuthenticator — all versions

Specifications

	FORTITOKEN 210
Time interval	30 seconds or 60 seconds
Display	6-digit high contrast LCD
Dimensions (Length x Width x Height)	61.8 × 28.7 × 8.9 mm
Weight	12 g
Operating Temperature	50°F to 104°F (10°C to 40°C)
Storage Temperature	32°F to 113°F (0°C to 45°C)
Water-Resistance	IP65 (Ingress Protection)
Casing	Hard Molded Plastic (ABS)
Secure Storage Medium	Static RAM
Battery	Lithium (non-rechargeable); minimum 3 years lifetime
OTP standard	OATH-TOTP (RFC6238) HMAC-SHA1
Certification	RoHS, CE, FCC, ICES, UKCA
FIPS Certification	FIPS 140-2 Certificate

	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 10 and Windows 11
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

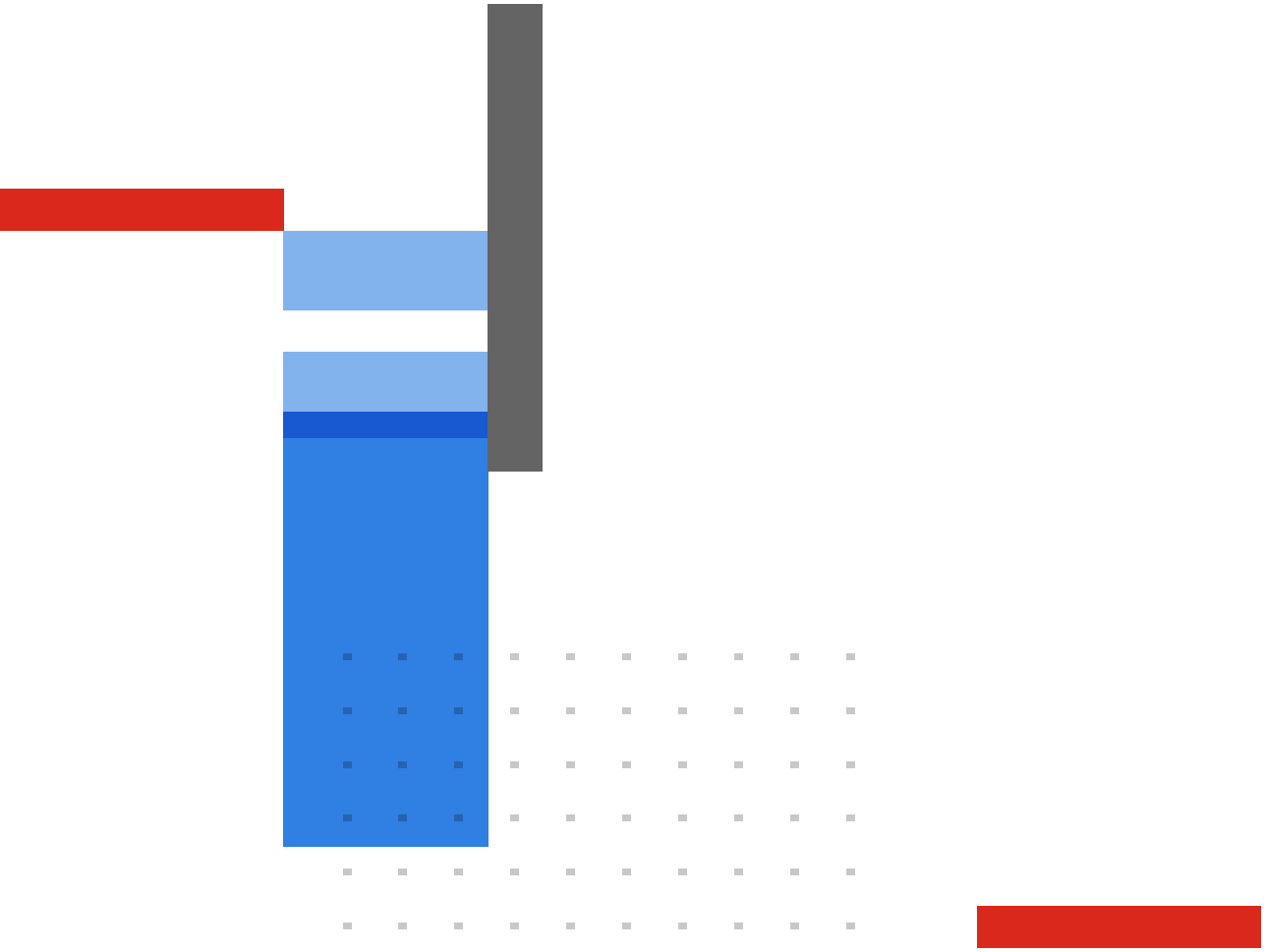
Ordering Information

Product	SKU	Description
FortiTokenMobile **Electronic license certificate**	FTM-ELIC-5	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-10	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-25	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-50	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-100	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-200	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-500	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-1000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-2000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-5000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
	FTM-ELIC-10000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for XXX users. License transfer between devices is not allowed for licenses shipped on or after August 4, 2025.
FortiToken 210 **Hardware Key FOB**	FTK-210-5	Five pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request.
	FTK-210-20	Twenty pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request.
	FTK-210-100	One hundred pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request.
	FTK-210-500	Five hundred pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request.
	FTK-210-1000	One thousand pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud. Encrypted seed file is available via customer support request.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

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 illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Copyright © 2026 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 SVP Legal and above, 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.

July 27, 2026

FTM-FTK210-DAT-R27-20260727