DATA SHEET

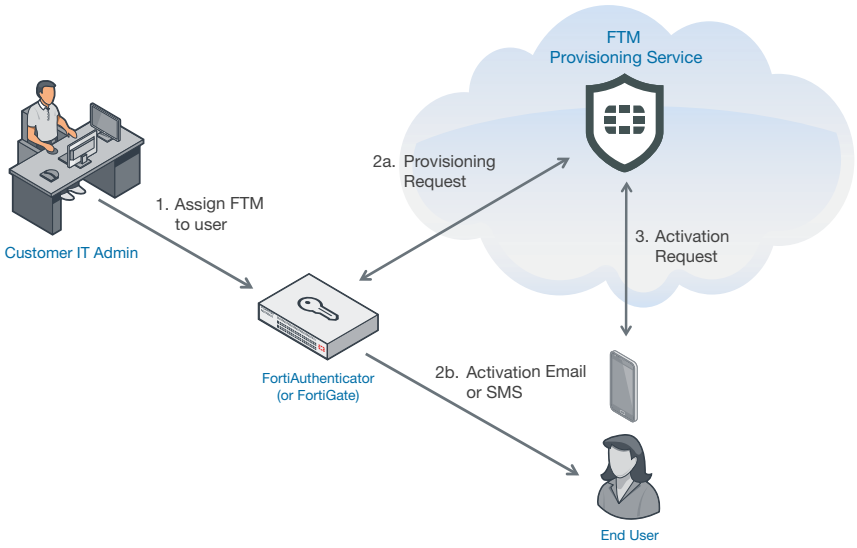
FortiToken™ Mobile

One-Time Password Application with Push Notification

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

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.



Highlights

FortiToken Mobile Advantages

- Unique token provisioning service via FortiGuard™ minimizes provisioning overhead and ensures maximum seed security
- Perpetual token license and unlimited device transfers eliminates 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

HIGHLIGHTS

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, IPsec VPN, Captive Portal and Administrative login, thereby eliminating the need for the external RADIUS server ordinarily required when implementing two-factor solutions.

Ultra-Secure Token Provisioning

What makes this mobile OTP application superior to others on the market is that while being simple to use for the enduser, 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;
- “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.

FortiToken Main Features

- OATH time- and event-based OTP generator
- Login details pushed to phone for one-tap approval
- 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

Supported Platforms

- 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)

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 license certificate.
	FTM-ELIC-10	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10 users. Electronic license certificate.
	FTM-ELIC-20	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 20 users. Electronic license certificate.
	FTM-ELIC-50	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic license certificate.
	FTM-ELIC-100	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic license certificate.
	FTM-ELIC-200	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 200 users. Electronic license certificate.
	FTM-ELIC-500	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 500 users. Electronic license certificate.
	FTM-ELIC-1000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 1,000 users. Electronic license certificate.
	FTM-ELIC-2000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2,000 users. Electronic license certificate.
	FTM-ELIC-5000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5,000 users. Electronic license certificate.
	FTM-ELIC-10000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10,000 users. Electronic license certificate.

FTM Redemption Certificate containing one license code for the number of token instances ordered will be issued. Enter license code into FortiGate or FortiAuthenticator to retrieve the tokens. Requires FortiOS 5.0 and up or FortiAuthenticator 1.4 and up.