QuickStart Guide

FortiToken 410

FTK-410

This guide covers: FortiToken 410

March 21, 2024

Regulatory Compliance: FCC Class A Part 15, / CE Mark

For Product License Agreement / EULA and Warranty Terms, visit https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf

33-410-1009890-20240321

The Essentials

FortiToken 410 is an all-in-one USB security key that can be used for multi-factor authentication (MFA) or passwordless login when using online services, device login (such as FortiGate), or network (such as VPN/ZTNA). FortiToken 410 supports FIDO U2F and FIDO2 protocols. It reduces reliance on passwords while increasing security and protecting user privacy. FIDO2 eliminates passwords entirely. During the authentication process, you will see the blinking green LED on your security key, simply enter your PIN associated with the key and press the button to sign in.

What is Fast IDentity Online or FIDO?

FIDO is an evolution of user authentication for online access. It is also known as passwordless authentication. FIDO is an open standard that was developed by the FIDO Alliance and the World Wide Web Consortium. FIDO is a lightweight approach to asymmetric public-key cryptography that extends the security benefits of public-key cryptography to a wider array of applications, domains, and devices. FIDO is designed to reduce (or remove) password usage, to avoid the sharing of secrets, and to create a path toward using a single credential for authenticating to multiple service providers such as websites and mobile services.

Comprehensive Guide

For more detailed FortiToken setup and configuration information, refer to the FortiToken Comprehensive Guide on https://docs.fortinet.com.

FortiAuthenticator

For more information about FortiToken management through FortiAuthenticator, refer to the FortiAuthenticator Administration Guide: https://docs.fortinet.com/product/fortiauthenticator.

Customer Service

For contracts, licensing, product registration and account management, contact FortiCare Support at https://www.fortinet.com/support/contact

Package Contents

FortiToken 410
FTK-410

FortiToken 410

QuickStart Guide

If any item is found missing or damaged, please contact your local reseller for replacement.

PIN Management for FortiToken 410

Windows

You can manage the PIN on your FortiToken 410 Security Key through your Windows account settings.

To set up the PIN, please use Windows with the latest updates.

1. Enter *Sign-In options* in the left-bottom search bar
2. Click *Security Key* > *Manage*.
3. Follow the on screen instructions to set the PIN for your security key.

   Follow the same steps to change or reset your PIN.

macOS and Linux

Manage the PIN on your FotiToken 410 through Chrome browser if you use macOS or Linux.

1. In Chrome browser, click the three dots next to your profile, then click *Settings*.
2. In the sidebar menu, click *Privacy and security*. Under *Privacy and Security*, click *Security*, then click *Manage security keys*.
3. Follow the on screen instructions to set the PIN for your security key.

   Follow the same steps to change or reset your PIN.

FIDO Security Key (FTK-410) Self Registration on FortiAuthenticator

Prerequsites

- An administrator has enabled FIDO for individual users.
- *FortiAuthenticator Self-Service portal* has been enabled with FIDO registration.

Note: Please refer to the FortiAuthenticator Admin Guide for futher details.

Registration

1. Obtain a FIDO KEY
2. Log in to the *FortiAuthenticator Self Service Portal* in your browser.
3. Click *FortiToken* to manage your multi-factor settings.
4. In *MFA Registration*, click *Add FIDO Key*.
5. Enter an appropriate name for your new FIDO key.
6. Click *OK* to confirm.
7. When prompted, insert your security key.
8. When the light on the security key blinks, press the button.
9. If prompted, click *OK* to continue
10. On Windows, you may get a popup for a security key PIN. Enter your Windows PIN to proceed.

You have successfully registered your FIDO key. You can see it under *Manage your FIDO keys* menu.

General Information

• You are not required to enter a PIN for google accounts because google accounts only use U2F for authentication which does not need a PIN.

• You may use the Windows Sign-on options to set a PIN value other than “888888” and try again. It should respond with a PIN error when a PIN is required.