



# QuickStart Guide

FortiToken 210

FTK-210

# The Essentials

FortiToken 210 is a small hardware one time password (OTP) generator that fits on a keychain. Press the button on the FortiToken 210 to display a secure OTP that you enter along with your regular password for secure authentication and access to critical applications and sensitive data.

The time remaining is shown on a graph in 10-second increments. After 60 seconds, the OTP expires and the FortiToken display turns off.

## Comprehensive Guide

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

## FortiGate

For more information about FortiToken management through FortiGate, refer to the FortiGate Administration Guide: <https://docs.fortinet.com/product/fortigate>.

## FortiAuthenticator

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

## FortiToken Cloud

For more information about FortiToken management through FortiToken Cloud, refer to the FortiToken Cloud Administration Guide: <https://docs.fortinet.com/product/fortitoken-cloud>.

## Customer Service

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



This guide covers: FortiToken 210

March 20, 2024

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.

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>

33-210-1009894-20240320

# Package Contents

## FortiToken 210 FTK-210



FortiToken 210



QuickStart Guide

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

**Note:** There is no CD version of FortiToken 210. To request a token seed file, contact FortiCare.

# Activating the FortiToken

Before you can use the FortiToken 210, it must be activated on a FortiGate or FortiAuthenticator or with FortiToken Cloud.

On FortiOS, FortiToken identifiers must be entered into the FortiGate unit, which then contacts FortiGuard servers to verify the information before activating them.

On FortiAuthenticator, the FortiAuthenticator unit acts as a repository for all FortiToken devices used on your network. It is a single point of registration and synchronization for easier installation and maintenance.

## Activation on FortiGate or FortiAuthenticator

### Prerequisites

- The FortiGate or FortiAuthenticator is configured to synchronize with a network time protocol (NTP) server.
- The FortiGate or FortiAuthenticator is able to access the FortiGuard Distribution Network (FDN).

### To add and activate on FortiGate:

1. In *User & Authentication > FortiTokens*, click *Create New*.
2. Set *Type* to *Hard Token*, enter the FortiToken serial number, and click *OK*.

**Note:** Alternatively, add or activate the FortiToken through the FortiGate CLI.

### To add and activate on FortiAuthenticator:

1. In *Authentication > User Management > FortiTokens*, click *Create New*.
2. Set *Token type* to *FortiToken hardware*, enter the FortiToken serial number, and click *OK*.

## Activation with FortiToken Cloud

### To activate with FortiToken Cloud (FTC):

1. In a web browser, log in to FortiToken Cloud.
2. In *Tokens > Hardware*, click *Import Tokens*.
3. Enter the FortiToken serial number and click *Add New Token*.
4. Click *OK*.

# Assigning the FortiToken to a user

To use token authentication, a user account must be configured to use two-factor authentication and assigned the serial number of an activated FortiToken device. The serial number cannot be shared by multiple users.

## To assign the FortiToken to a user on FortiGate:

1. Edit the user or administrator account.
2. Enable *Two-factor Authentication*, select the FortiToken, and click *OK*.

## To assign the FortiToken to a user on FortiAuthenticator:

1. Edit the user account.
2. Enable *Token-based Authentication*, select the FortiToken, and click *OK*.

## To assign the FortiToken to a user with FortiToken Cloud:

1. In a web browser, log in to FortiToken Cloud.
2. In *Users*, select the user and click *MFA Method*. then select the FortiToken.



# Logging in with FortiToken

When prompted, press the *Start* button of your FortiToken unit and enter the generated OTP into the appropriate field on the login page. You must do this within 60 seconds while the token password is still valid.

### Please Login

**Name:**

**Password:**

**FortiToken Code:**

