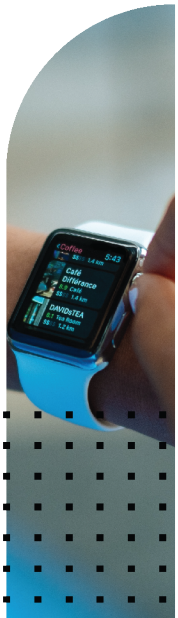
User Guide

FortiToken Mobile 5.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 23, 2022
FortiToken Mobile 5.4 User Guide
33-540-665753-20221123

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-07-14	Initial release.
2022-09-06	Updated Introduction on page 5.
2022-10-11	Updates to content throughout.
2022-11-23	Updated supported languages in Introduction on page 5 and FortiToken Mobile settings view on page 14.

Introduction

FortiToken Mobile allows you to generate one-time password (OTP) values on your mobile device for use in two-factor authentication. Once your token is activated, you will not need any network access to generate OTPs on your device.

Overview

The FortiToken Mobile application supports three platforms: iOS, Android, and Windows.

FortiToken Mobile for iOS and FortiToken Mobile for Android support localization in English, simplified Chinese, traditional Chinese, Japanese, and French (France and Canada). FortiToken Mobile for Windows is only available in English.

After installing FortiToken Mobile on your device, you will need to activate a token. Once activated, you can immediately generate OTPs on your device. You can manually enter the OTP or approve or deny the remote access login request from push notifications.

If an old mobile device doesn't work or is lost, you can transfer the activated token to a new device without activation of a new token.

Supported Versions and Devices

FortiToken Mobile for iOS can be installed on iPad, iPod Touch and iPhone, iWatch with iOS from 9 to latest 13.

FortiToken Mobile for Android can be installed on all Android devices with Android OS from 7 to latest 13.

FortiToken Mobile for Windows can be installed on Windows 10 PCs and Windows 10 Mobile devices.

No cellular network is required. If cellular service is not available, use Wi-Fi access.

There are differences in the interface for each of these versions. Menus and options may vary slightly depending on the platform you are using.

Installing FortiToken Mobile

To install FortiToken Mobile on your device, visit the appropriate app store.

Downloading for Apple iOS

Go to the Apple app store to download the free FortiToken Mobile for iOS application.

Downloading for Google Android

Go to the Google Play store to download the free FortiToken Mobile for Android application.

Downloading for Microsoft Windows

Go to Microsoft store to download the free FortiToken Mobile for Windows application.

Before the app is installed, make sure the device has the correct date and time.

Token Activation

FortiToken Mobile allows you to install tokens that are issued from FortiGate, FortiAuthenticator, and FortiToken Cloud, as well as third-party tokens such as those used for two-step verification by Dropbox, Google, Amazon, and Microsoft.

FortiToken activation email or SMS message

After your system administrator assigns a token to you, you will receive a notification with an activation code and an activation expiration date by which you must activate your token.

Depending on which option your system administrator has chosen, you will receive the activation notification by SMS, email, or both.

The activation message includes the activation code and the activation expiration date. If you do not activate your token by the indicated expiration date, you must contact your system administrator so that your token can be re-assigned for activation.

If the message is sent as an email it also contains a scannable QR code.

The activation notification looks like this for tokens issued from FortiGate, FortiAuthenticator, and FortiToken Cloud:

```
Welcome to FortiToken Mobile - One-Time-Password software token.

Please visit https://docs.fortinet.com/fortitoken/ for instructions on how to install your
FortiToken Mobile application on your device and activate your token.

You must use FortiToken Mobile version 2 or above to activate this token.

Your Activation Code, which you will need to enter on your device later, is

"xxxxxxxxxxxxxxx"

Alternatively, use the attached QR code image to activate your token with the "Scan Barcode"
feature of the app.

You must activate your token by:

Monday December 14, 2020 20:39 UTC(+0000), after which you will need to contact your system
administrator to re-enable your activation.
```

Activating Your Token

You can activate your token on FortiToken Mobile for iOS, Android, and Windows after you receive an activation code via email or SMS.

Before you begin, make sure your device is set to the correct time and you have internet access.

Tokens may have `enforced-pin`, `required (optional)`, and `not-required` PIN policy on FortiAuthenticator and FortiToken Cloud. PINs need to be set before activating tokens for two cases:

1. If `enforced-pin` policy is selected by system administrator
2. If `required (optional)` PIN policy is selected by system administrator and no mobile device PIN is set.

Once you have created and confirmed your PIN, you can add your tokens by using the activation code received via email or SMS. You can either enter the activation code manually or scan a QR code.

Scan Barcode

If your device supports QR code recognition, you can simply tap *SCAN BARCODE* in the FortiToken Mobile home screen and point your device camera at the QR code attached to the activation email.

Note: QR code images are not provided using the SMS activation message, only with the email activation message.

Enter Manually

1. Tap *ENTER MANUALLY*, then select the type of token from the list.
   a. For FortiToken, select *Fortinet*.
   b. For third-party tokens, select *Other*.
2. Enter a name for this token and the activation code exactly as it appears in your activation message, either by typing or copying and pasting.

FortiToken Mobile will automatically convert lower case to upper case letters so there is no need to use the *Shift* key when typing.

3. Tap *ADD ACCOUNT*.
   FortiToken Mobile communicates with the secure provisioning server to activate your token. The one-time password is now displayed in the token list view.

Third Party Token Activation

Many cloud and online applications offer the option to turn on two-step verification (also known as two-factor authentication) for added security. FortiToken Mobile provides a simple means to install tokens from cloud services providers, including Dropbox, Google, Amazon, and Microsoft.

Follow the provider's instructions for turning on two-step verification. They will provide an activation code with options to scan a QR code or enter the code manually if you cannot scan the bar code.

If you use the option to scan the barcode and no token name is entered, the token name will default to what is encoded in the QR code image for the account name. The token name can be edited.

FortiToken Mobile allows you to choose a third-party provider. If your provider is not listed, you can still add a token if the activation code is presented in Base32 format.

Push Notifications

Push notifications provide an alternative to entering a one-time password for remote access login.

Push notification is supported on FortiToken Mobile for both IOS and Android.FortiToken Mobile for Windows doesn't support push notifications.

FortiToken Mobile can receive push notifications even when your mobile device is locked or on the home screen as well as when FortiToken Mobile app is open. You can choose to approve or deny the login request. Once action is taken on the login request, the message "Request sent successfully" displays for 1.5 seconds.

Note:

FortiToken Mobile validates the server certificate when responding to login push notifications and transfer token requests. This only applies to tokens issued from older versions of FortiAuthenticator (6.3.1 and earlier). In some cases, you may need to enable *Allow connection to an unverified server* to make sure the push and token transfer features work properly.

Allow connection to an unverified server is disabled by default in FortiToken Mobile (iOS and Android) *Settings*.

You may need to enable this setting to approve login from push notifications in these cases:

- The token was issued by FortiAuthenticator 6.3.1 or lower.
- You are transferring a token that was issued by FortiAuthenticator 6.3.2/6.4.0 or lower and the default server certificate is not being used.

Please check with your system administrator if these conditions apply.

FortiToken Mobile home view

Generating OTPs

Two types of one-time passwords (OTPs) display in FortiToken Mobile:

- **HOTP (Event-based or HMAC-based)**: The token passcode is generated using an event trigger and a secret key. Tap *Next OTP* to display a new OTP value.
- **TOPT (Time-based)**: Tap the eye icon to hide or show the OTP. The timer bar next to the eye icon shows how much time is left before a new OTP value will be displayed. The token OTP changes every 60 or 30 seconds. The time is configured by the token administrator.

Note:

- FortiToken Mobile for iOS, Android, and Windows all support both TOTP and HOTP.
- FortiAuthenticator supports HOTP and TOTP.
- FortiGate and FortiToken Cloud only support TOTP.

Copying OTPs

Your OTP can be copied to your clipboard. This is useful in situations such as when you are using a VPN client on a mobile device and need to enter the OTP as the second factor for logging in.

To copy an OTP:

1. Tap and hold on the displayed OTP. The OTP is copied to your clipboard.

The OTP must be displayed (not hidden) to copy it.

Search for a token

Device	Procedure
iOS	1. From the FortiToken Mobile for iOS token list view, pull down from the top of the screen to show the search bar and pull up to hide the search bar. 2. Tap the search bar, then type letters to match to token names in the list. FortiToken

Device	Procedure
	Mobile for iOS will return a list of matched tokens. 3. Tap *back* to return to the token list with the selected token moved to the top of list.
Android	• From the FortiToken Mobile for Android token list view, tap the search icon displayed at the top right to open the search bar. • Type letters to match to tokens and tap a token to move it to the top of the list. A confirmation message is displayed.
Windows	FortiToken Mobile for Windows does not support the search feature.

Hide or show OTP

Both TOTP and HOTP display after they are activated. TOTP can be shown or hidden by tapping the eye icon. Its hidden or displayed status is retained after exiting or re-launching the app. HOTP is hidden all the time after exiting or re-launching the app. The only way to show an HOTP is by tapping *Next OTP*.

FortiToken Mobile for Windows does not support hiding TOTP.

Token detail

In the token list, tap a token to see the token's details, including an editable token name, issuer serial number, and issuer name.

Edit token name

To edit a token name:

1. In the token list, tap on a token. The token information window dispays.
2. Tap on the token name. The *Edit name* dialog displays.
3. Enter the new name and tap *Save*.

FortiToken Mobile manager view

To open the manager view to manage your tokens:

- In FortiToken Mobile for iOS, in the application header, tap *Manage*.
- In FortiToken Mobile for Android, in the application menu at the top right of the token list view, tap *Manage*.
- In FortiToken Mobile for Windows, manage tokens directly from the home view.

Delete a Token

To delete a token:

1. In the manager view, tap the red *X* next to the token to be deleted.
2. In the dialog tap *DELETE* to confim.

In FortiToken Mobile for Windows, delete appears as a button in the footer.

Reorder Tokens

To reorder tokens:

1. In the manager view, tap and hold the three horizontal lines at the end of token.
2. Drag the token to reorder its position, then release.

FortiToken Mobile info view

To access application information:

- In FortiToken Mobile for iOS: In the application header, tap *Info*.
- In FortiToken Mobile for Android: In the application menu (three vertical dots in the top left of the screen) tap *About*.
- In FortiToken Mobile for Windows: In the footer, tap *Settings*.

The FortiToken Mobile info view displays the following information:

Feature	Description
Version	FortiToken Mobile application version installed on your device.
Epoch Time	The universal time value that can be used to troubleshoot token synchronization issues.
Registration ID	The mobile device's ID that FortiToken Mobile uses to identify the correct device to send push notifications.
Terms and Conditions	A link to a PDF document containing the Fortinet Product License Agreement, EULA, and Warranty Terms.
Fortinet Privacy Policy	A link to the Fortinet privacy policy.

FortiToken Mobile settings view

To access application settings:

- In FortiToken Mobile for iOS: In the application header, tap *Info*.
- In FortiToken Mobile for Android: In the application menu (three vertical dots in the top left of the screen) tap *Settings*.
- In FortiToken Mobile for Windows: In the footer, tap *Settings*.

The following settings are available:

Feature	Description
Touch ID, Face ID	Enable or disable device supported security: • FortiToken Mobile for iOS: Supports *Touch ID* and *Face ID*. You must enable this feature from the device settings first, then enable it in FortiToken Mobile for iOS. • FortiToken Mobile for Android: Supports fingerprint authentication. Enable this feature in the device settings first, then enable it in FortiToken Mobile for Android.
PIN	To set a FortiToken Mobile PIN, enable PIN and either: • Enter a 4-digit PIN to create a PIN for the first time • Enter your current FortiToken Mobile PIN, then enter a new PIN. Re-enter the new PIN to confirm.
Allow connection to an unverified server	See Push Notifications on page 9 for more information.
Language	FortiToken Mobile for iOS and FortiToken Mobile for Android: Select the interface language. FortiToken Mobile for iOS and FortiToken Mobile for Android support localization in English, simplified Chinese, traditional Chinese, Japanese, and French (France and Canada). FortiToken Mobile for Windows is only available in English.

FortiToken Mobile additional features

To access additional features and settings:

- In FortiToken Mobile for iOS: In the application header, tap *Info*.
- In FortiToken Mobile for Android: In the application menu (three vertical dots in the top left of the screen) tap *Settings*.

Note: FortiToken Mobile for Windows does not support these additional features.

These additional features are available:

Feature	Description
Transfer Tokens	If a token is issued from FortiAuthenticator or FortiToken Cloud, the token can be transfered from iOS to iOS device, from Android to Android device, or between iOS and Android devices. **To transfer tokens:** Tap *Transfer Tokens*, then tap the FortiToken Cloud or FortiAuthenticator serial number with the total number of activated tokens. Tap *OK* in the *Transfer Tokens* popup. Tap *Proceed* to start the token transfer process. You will receive a transfer code via email or SMS. Scan the transfer code or enter the transfer key manually by navigating to *home screen* > + > *Enter Manually* > *Enter Transfer Code*. **Note**: • Only tokens issued from FortiAuthenticator or FortiToken Cloud can be transferred. Tokens issued from FortiGate cannot be transfered. Third party tokens issued from FortiAuthenticator or FortiToken Cloud can be transfered. • Only FortiToken Mobile for iOS and Android support token transfer. FortiToken Mobile for Windows does not support this feature. • Token transfer is supported betweenFortiToken Mobile for iOS and FortiToken Mobile for Android.
Buy Tokens	Buy tokens if tokens are used up. Only supported on FortiToken Mobile for iOS.
Purchase History	Tokens purchased will be listed under purchase history. Only supported in FortiToken Mobile for iOS.

Alerts and Troubleshooting

Activation Issues

- If you receive an error message indicating that FortiToken Mobile timed out while waiting for the server, check to make sure your device can access the Internet. If the problem persists, contact your system administrator.
- If you receive an error message indicating that FortiToken Mobile activation failed, please check your activation code and re-enter the code. If the problem persists, contact your system administrator. Please supply the error code and error message so your administrator can correct the problem.
- If a token is activated, it cannot be activated again on the same or different devices.

Synchronization Issues

If you are able to generate OTPs but your login attempts fail, please make sure your device is set to the correct time. If the problem persists, contact your system administrator.

Push Issues

If you cannot receive push notification on your mobile device, check for FortiToken Mobile under your device's settings to make sure notifications are enabled.

If you approve a push notification but remote access login fails, you can either contact your system administrator or use an OTP instead.

Application Timeout

If you do not touch your screen for 60 seconds, the application will time out and you will have to enter your PIN again to display the OTP.

www.fortinet.com