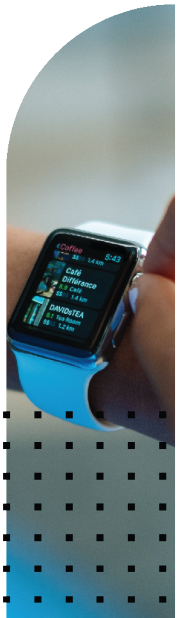
Comprehensive Guide

FortiToken 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

March 27, 2023
FortiToken 5.4 Comprehensive Guide
33-540-412648-20230327

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-03-24	Initial release. This release combines previous related FortiToken documentation into a single resource.
2016-05-12	Added video link to the configuration example "Captive portal WiFi access with FortiToken-200".
2016-06-06	Added video link to the configuration example "IPsec VPN two-factor authentication with FortiToken-200".
2016-06-01	Added information in Reference section regarding FortiToken provisioning with FortiAuthenticator REST API.
2016-07-18	Added information regarding FortiToken deployment in an HA cluster with multiple FortiGate/FortiAuthenticator units.
2016-08-22	Clarified CLI command information regarding activation code expiry.
2016-10-04	Added information regarding FortiToken authentication with no Internet.
2016-12-15	Added FortiToken Mobile 4.0 new feature information: PUSH notifications and Touch ID.
2017-08-15	FortiToken is a Windows Universal Platform (UWP) application, and therefore supports Windows 10.
2017-08-11	Added extra details to previously added encryption information and updated Introduction section.
2017-08-08	Added FortiToken encryption information under Considerations.
2018-01-04	Update to FortiToken-200CD information regarding simultaneous token registration.
2020-09-18	Updated the url for Drift adjustment on page 24.
2022-12-12	Updated Configuration examples on page 14 section. Updated Reference on page 23 section.
2023-03-15	Updated Introduction on page 5.
2023-03-27	Updated FortiToken platform scalability on page 23.

Introduction

FortiTokens are security tokens used as part of a two-factor authentication system on FortiGate/FortiOS and FortiAuthenticator devices. The token produces a temporary six or eight digit (configurable) code that is used to prove one's identity electronically as a prerequisite for accessing network resources. There are many types of hardware and software based tokens, sometimes referred to as dongles, key fobs, authentication tokens, USB tokens, and cryptographic tokens.

FortiToken is available as either a physical or a mobile token, as described below.

Physical token

- **FortiToken-200**: These physical tokens display their code on the device itself, and provide two-factor authentication for RADIUS, LDAP, and 802.1X wireless authentication, as well as Fortinet single sign-on (FSSO). This kind of two-factor authentication improves security by moving away from use of static passwords.

  To transfer FortiToken-200 tokens from one FortiGate or FortiAuthenticator device to another, visit the Fortinet Support website.

  When contacting customer support, you must provide the FortiToken serial number as well as the FortiGate or FortiAuthenticator serial number to which the token is assigned.

- **FortiToken-200CD**: These tokens provide the same authentication properties as FortiToken-200 devices, however they come with an activation CD. The CD contains the token seed files which are installed to the FortiGate or FortiAuthenticator, and is used to easily import multiple FortiTokens at once.

  With FortiToken-200CD, the tokens can be installed on as many FortiGate and FortiAuthenticator devices as the customer wants, simultaneously, from the same seed file.
- **FortiToken-220-Edge**: These tokens provide the same authentication properties as FortiToken-200 devices, however they come in a convenient mini credit card form factor.

Mobile token

- **FortiToken Mobile**: These tokens produce their codes in an application you can download to your Android or iOS device that is used just like a FortiToken-200 but without the need for a physical token. FortiToken Mobile uses push technology to send login attempt notifications to a user's smartphone or tablet where they can verify the login with a single tap.

  Users can download their free FortiToken Mobile application from the iTunes App Store or Google Play.

Administrator guide

The following sections demonstrate how to set up FortiToken support for your end users with FortiGate or FortiAuthenticator.

Setting up FortiToken Hardware

The following steps are required to add FortiToken two-factor authentication to a user on FortiGate or FortiAuthenticator:

1. Register FortiToken-200/200CD/220-Edge
2. Assign the FortiToken to the user

FortiGate must also have a FortiGuard subscription to support FortiToken.

Register a FortiToken

The following steps show how to register a FortiToken-200, FortiToken-200CD, and FortiToken-220-Edge on FortiGate or FortiAuthenticator.

On FortiGate

For FortiToken-200 and FortiToken-220-Edge

1. Go to *User & Authentication* > *FortiTokens* and click *Create New*.
2. Set *Type* to *Hard Token*, enter the FortiToken serial number in the *Serial Number* field, and then click *OK*.

If you have several FortiTokens to add at once, you can list their serial numbers in a text file and select *Import*. Each serial number must be listed individually per line of text.

3. Wait for FortiGuard to validate your FortiToken serial number. When you first enter the serial number, its status is listed as *Pending*. When FortiGuard validates the serial number, the status changes to *Available*.

For FortiToken-200CD

1. Insert the activation CD labeled *FortiToken-200 Activation File*.
2. On FortiGate, go to *User & Authentication* > *FortiTokens* and click *Create New*. Set *Type* to *Hard Token* and click *Import*.
3. Select *Seed File* and click *Upload*.

4. Browse to the CD and select the .FTK file, then click *OK*.
   Each FortiToken is installed and activated.

On FortiAuthenticator

For FortiToken-200 and FortiToken-220-Edge

1. Go to *Authentication* > *User Management* > *FortiTokens* and click *Create New*.
2. Set *Token type* to *FortiToken hardware*, enter the FortiToken serial number in the *Serial numbers* field, and then click *OK*.

If you have several FortiTokens to add at once, you can select *Import Multiple* and import by *Serial number file*, *Seed file*, or *FortiGate configuration file*.

For FortiToken-200CD

1. Insert the activation CD labeled *FortiToken-200 Activation File*.
2. Go to *Authentication* > *User Management* > *FortiToken* and select *Import*. Set *File type* to *Seed file*, select the .FTK file on the CD, and then click **OK**.
   Each FortiToken will be installed and activated.

Assign a FortiToken to a user

The following steps show how to assign a FortiToken to a user on FortiGate and FortiAuthenticator.

On FortiGate

1. Go to *User & Authentication* > *User Definition* and edit the user.
2. Enable *Two-factor Authentication*.
3. select the *Authentication Type* and select the appropriate FortiToken from the list
4. Enter the user's *Email Address* or enable *SMS* and enter the *Phone Number*.
5. Click *OK*.
6. Go to *User & Authentication* > *FortiTokens* to confirm that the FortiToken is assigned to the correct user.

On FortiAuthenticator

1. Go to *Authentication* > *User Management* > *Local Users* and edit the user.
2. Enable *Token-based authentication*, select *FortiToken*, select the FortiToken from the dropdown menu, and then click *OK*.
3. Go to *Authentication* > *User Management* > *FortiTokens* to confirm that the FortiToken is assigned to the correct user.

Registering and provisioning FortiToken Mobile tokens

To deploy FortiToken Mobile for your end users, you must first register the tokens on FortiGate or FortiAuthenticator. After registering the tokens, you can assign them to your end users.

Platforms that support FortiToken Mobile:

Platform	Device and Firmware support
Android	• Smartphones and tablets • Firmware version Jellybean 4.1+
iOS	• iPhone, iPad, and iPod Touch • Firmware version iOS 6.0+
Windows	• Windows 10 and later (desktop and mobile), Windows Phone 8.1, and Windows Phone 8. Note that FortiToken Mobile is a Windows Universal Platform (UWP) application. To download FortiToken Mobile for Windows desktop and mobile platforms, see FortiToken Windows on the Microsoft Store.

You will need a certificate to register FortiToken Mobile. There are two options for getting FortiToken Mobile certificates for use on your authentication server:

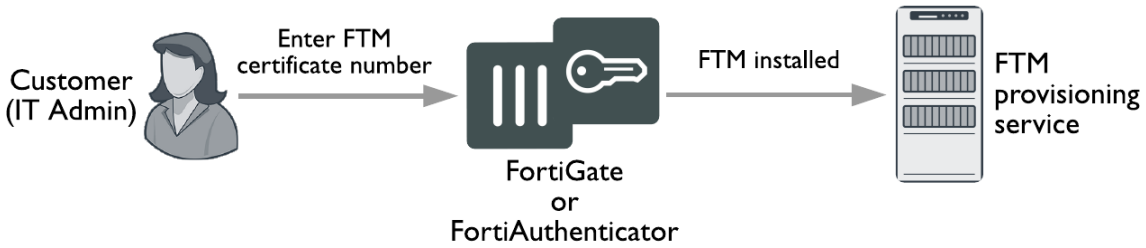
- FortiToken Mobile Redemption Certificate
- FortiToken Mobile Free Trial “virtual” certificate

For each FortiToken Mobile purchase, you receive a physical redemption certificate. Scratch off the designated area of the redemption certificate to reveal the 20-digit activation code.

Each FortiGate or FortiAuthenticator also comes with a trial license for two free tokens. The device must be registered with FortiCare to retrieve the tokens. The certificate code to use for the free trial FortiToken Mobile tokens is 0000-0000-0000-0000-0000.

The registration process is the same for both options:

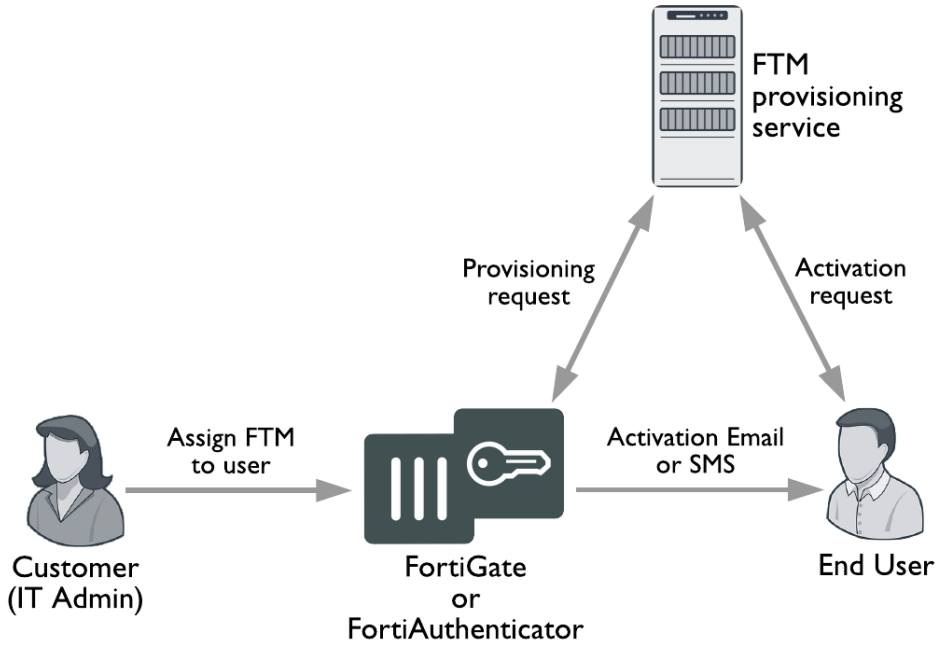
1. The authentication server administrator enters the certificate activation code from the redemption certificate.
2. The authentication server sends the activation code to the FortiToken Mobile provisioning server, which validates the request, registers the FortiToken Mobile license, and sends the FortiToken Mobile serial numbers back to the authentication server.



The provisioning process includes the following steps:

1. An authentication server administrator assigns a FortiToken Mobile token to the user.
2. The authentication server notifies the provisioning server that the token has been assigned for activation and receives an activation code to forward to the end user.
3. The end user receives an activation notification via email or SMS, depending on how the authentication server is configured.

After activating the FortiToken Mobile token on their mobile device the application begins generating authentication codes.



Push notifications

FortiToken Mobile supports push notifications and Touch ID as an optional choice over using a PIN, allowing an extra layer of security.

Push notifications are used to send alerts to the end user's device each time a login request is made. The alert contains information about the login attempt, for example the IP address of the system from which the attempt originated.

The user taps to approve or deny the request, optionally using Touch ID. If approved, a code is sent by FortiToken Mobile to authenticate the end user in the background. If denied, FortiToken Mobile logs the attempt.

The manual OTP authentication method is still available in case the end user cannot or does not wish to use push notifications.

When upgrading, users will see a request to allow notifications. This is required for push notifications to work.

Registering FortiToken Mobile

The following steps show how to register FortiToken Mobile tokens on FortiGateand FortiAuthenticator.

On FortiGate

1. Locate the 20-digit code on the redemption certificate.
2. Go to *User & Authentication* > *FortiTokens* and click *Create New*.
3. Select *Mobile Token* and enter the 20-digit certificate code in the *Activation Code* field.
4. Click *OK*.

On FortiAuthenticator

1. Locate the 20-digit code on the redemption certificate.
2. Go to *Authenticaton* > *User Management* > *FortiTokens* and click *Create New*.
3. Select *FortiToken Mobile* and enter the 20-digit certificate code in the *Activation codes* box.
4. Click *OK*.

Provisioning FortiToken Mobile

To ensure that messaging functions properly, you must configure the messaging server, configure users to receive messages from the server by email or SMS, and use the FortiToken Mobile token.

The following steps show how to provision FortiToken Mobile for a user on FortiGate and FortiAuthenticator.

On FortiGate

1. Go to *System* > *Advanced*.
2. Configure the server under *Email Service* as required (note that port 25 is the default port).
3. Go to *User & Authentication* > *User Definition*.
4. Edit the user you wish to assign the FortiToken Mobile token to.
5. Enable *Two-factor Authentication*, set *Authentication Type* to *FortiToken* and select the appropriate FortiToken Mobile token in the *Token* field.
6. Enter an *Email Address* or *SMS*, enter the user's contact information, and then click *OK*.
   The user will receive the activation code by the method or methods specified.

Activation expiration

The activation code will expire after a configurable time period. To configure this time period for FortiToken Mobile tokens (in hours), use the FortiGate CLI.

To configure the activation period, use this CLI command:

```
config system global
   set two-factor-ftm-expiry <1-168>
end
```

The CLI command above should be used instead of `set activation-expire` under `config user fortitoken`.

The CLI command `set activation-code`, under `config user fortitoken`, cannot be used or set by the administrator.

On FortiAuthenticator

1. Go to *System* > *Administration* > *FortiGuard*.
2. Under *FortiToken Mobile Provisioning*, ensure that the *Activation timeout* period is set. This is the time period in hours (1 to 168) in which the end user must activate the token before having to re-provision the token.
3. Go to *Authentication* > *User Management* > *Local Users* and select *Create New*.
4. In the *Password creation* dropdown menu, select *No password, FortiToken authentication only*, and select *OK*.
   Note: Only after you select *OK* can you specify a token and enter contact information for the user.
5. Once created, the user account will become disabled. You must associate a FortiToken and re-enable it.
   Deselect the *Disabled* radio, and select *Token-based authentication*. Choose to deliver the token by *FortiToken* and select an available *FortiToken Mobile* token from the dropdown menu.
6. Under *User Information*, enter the user's *Email address*. You may also enter their *Mobile number*.
7. Click *OK*.
   The user will receive the activation code by the method specified.

End user token activation

To activate the FortiToken in the FortiToken Mobile app:

1. Open the FortiToken Mobile application and go to *Add account* > *Enter Manually* > *Fortinet*.
2. Enter your email address, enter the activation code you received, and tap *Add account*.
   Your token will activate and start generating codes.

Alternatively, use the attached QR code if your activation code is sent to you by email. Activate the token in FortiToken Mobile with the *Scan Barcode* option instead of *Enter Manually*.

Deactivating a FortiToken

You can deactivate a FortiToken by removing the token from the user it is assigned to.

On FortiGate

1. Go to *User & Authentication* > *User Definition* and edit the appropriate user.
2. Disable *Enable Two-factor Authentication* and click *OK*.

   The token is removed from the user's *Two-factor authentication* column. The user is also removed from the token's *User* column in *User & Authentication* > *FortiTokens*.

On FortiAuthenticator

1. Go to *Authentication* > *User Management* > *Local Users* and edit the appropriate user.
2. Disable *Token-based authentication* and click*OK*.

   The token is removed from the user's *Token* column. The user is also removed from the token's *User* column in *Authentication* > *User Management* > *FortiTokens*.

Considerations

The following information clarifies a few factors regarding different FortiToken deployments.

FortiToken encryption

FortiToken uses OATH algorithms, in compliance with algorithms for both HOTP and TOTP (see RFCs 4226 and 6238).

In addition, AES 256 CBC is used to encrypt the seeds for storage (see below for more information on FortiToken seed files). The encryption key for the seed is a device-unique ID that is generated each time the seed needs to be accessed so that, if the seed is copied to another device, it will not decrypt and yield invalid OTPs.

The seeds are passed to the mobile device using TLS (HTTPS) and encrypted within the TLS tunnel using the key derived from the device ID. In this way, the seed is effectively double-encrypted.

FortiToken authentication with no internet

The following consideration is applicable to FortiOS 5.0 and later.

FortiTokens (excluding FortiToken-200CD) store their encryption seed files in the FortiGate or FortiAuthenticator they are assigned to. Their FortiTokens will continue to generate token codes. Therefore, FortiGate and FortiAuthenticator units can validate token codes and provide two-factor authentication even if they have lost access to the internet.

Note that FortiToken Mobile needs access to FortiGuard for all management changes (such as token assignment to users). Once assigned, these tokens will work even if the FortiGate or FortiAuthenticator has no internet access. However, FortiToken-200 user assignment without internet access is possible.

FortiToken seed files

A FortiToken Mobile token can only be registered to a single FortiGate or FortiAuthenticator unit at a time. However, physical FortiToken-200 tokens can be registered on multiple FortiGates or FortiAuthenticators. To register physical

tokens on multiple FortiGate or FortiAuthenticator units, visit the Fortinet Support website. Token activation locks need to be reset on FortiGuard before being activated on a different unit.

FortiToken-200CD seed files are stored on the CD. These tokens are designed to be used in "walled-garden" scenarios, with no internet access. Because of this, these tokens can be used on multiple devices.

High availability clustering with FortiToken

When setting up a high availability (HA) cluster with multiple FortiGate or FortiAuthenticator units, you must register and apply any FortiToken Mobile licenses to the primary unit. This can be done either before or after configuring the unit for HA operation. After HA is configured, all tokens are replicated across cluster members. Because of this, you only need one FortiToken Mobile license per HA cluster.

To learn more about HA clustering, see the FortiOS High Availability guide.

Native iOS VPN client with FortiToken authentication

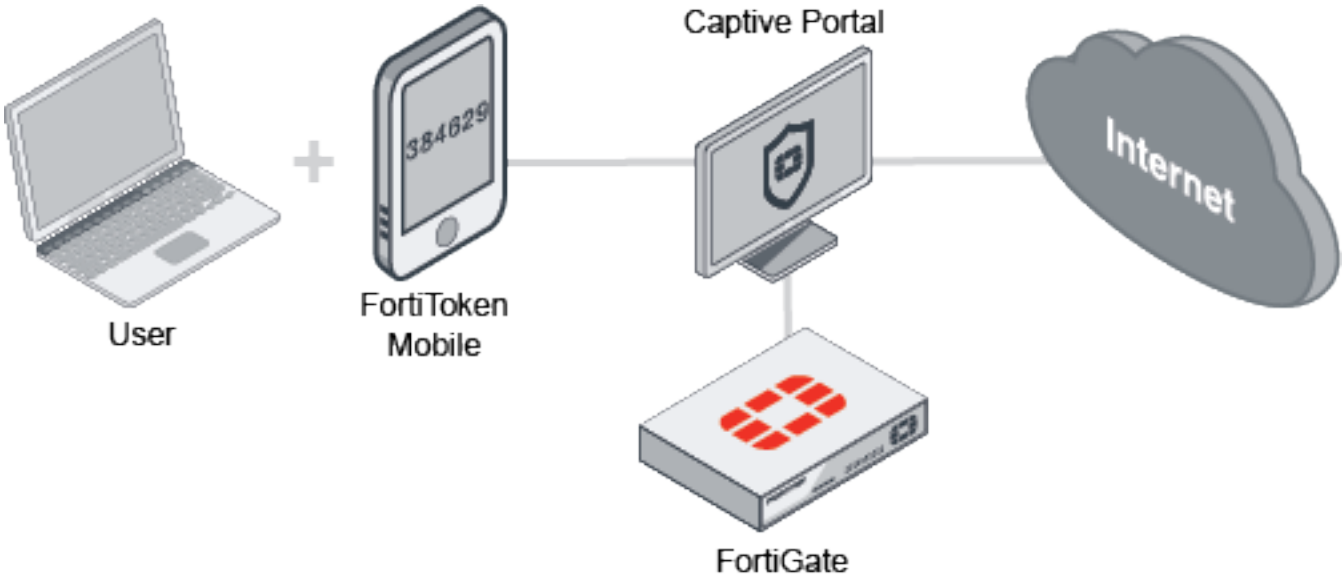
Unlike other VPN instances that typically require a username, password, and the OTP provided by FortiToken, the native iOS VPN client requires the OTP to be combined with the user's password. For example, if the user's password was `fortinet`, and the OTP was `123456`, the combined password for authentication would be `fortinet123456`.

Configuration examples

This section presents the following FortiToken configuration examples:

- Example: Two-factor authentication with captive portal
- Example: IPsec VPN two-factor authentication with FortiToken-200
- Example: Captive portal WiFi access with FortiToken-200
- Example: FortiToken two-factor authentication with RADIUS on a FortiAuthenticator
- Example: Third-party token activation with Google

Example: Two-factor authentication with captive portal



In this scenario, you will set up a FortiGate to require users on an internal network to use two-factor authentication with FortiToken Mobile to access the Internet through a captive portal.

The captive portal will be added to the FortiGate internal interface and you will customize the portal by changing the login page appearance and adding a new image.

This scenario assumes that you have already added an internet access policy, that you have added FortiToken Mobile to the FortiGate, and the `elainemarley` user is a member of the FortiToken user group named `FTK-users`.

1. Enable FortiToken for `elainemarley`:
   a. Go to *User & Authentication* > *User Definition* and edit `elainemarley`.
   b. Enable *Two-factor Authentication*, set *Authentication Type* to *FortiToken* and select the appropriate FortiToken Mobile token in the *Token* field.
   c. Enter an *Email Address* or *SMS*, enter the user's contact information, and then click *OK*.
   The user will receive the activation code by the method or methods specified.

2. 2. Add a user account to FortiToken Mobile on your mobile device:
   - Add the account manually:

     Open FortiToken Mobile and go to *Add account* > *Enter Manually* > *Fortinet*, enter your email address and the activation code you received, and then tap *ADD ACCOUNT*.
   - Add the account by scanning a QR code:

     Open FortiToken Mobile and go to *Add account* > *SCAN BARCODE* to scan an attached QR code.

     The token activates and begins generating codes.
3. 3. Edit the internal interface:
   a. Go to *Network* > *Interfaces* and edit the internal interface.
   b. Under *Network*, enable *Security mode* and set it to *Captive Portal*.
   c. Set *Authentication Portal* to *Local*, set *User access* to *Restricted to Groups*, and set *User groups* to `FTK-users`.
4. 4. Customize the captive portal login page:
   a. Go to *System* > *Replacement Messages*. Under *Authentication*, edit *Login Page*.Two panels will open showing the login page that users will see when attempting to browse the Internet and the HTML format. Customize the login page using the HTML panel. When finished, click *Save*.
   b. Click *Manage Images* and then *Create New*.
   c. Enter a name for the new replacement image and upload an image file of your choice (in this example, `Mêlée-Island.png`).

      Note that your image must be 24 KB or less.
   d. In the HTML editing panel for *Login Page*, scroll down to the logo and configure the HTML as follows:

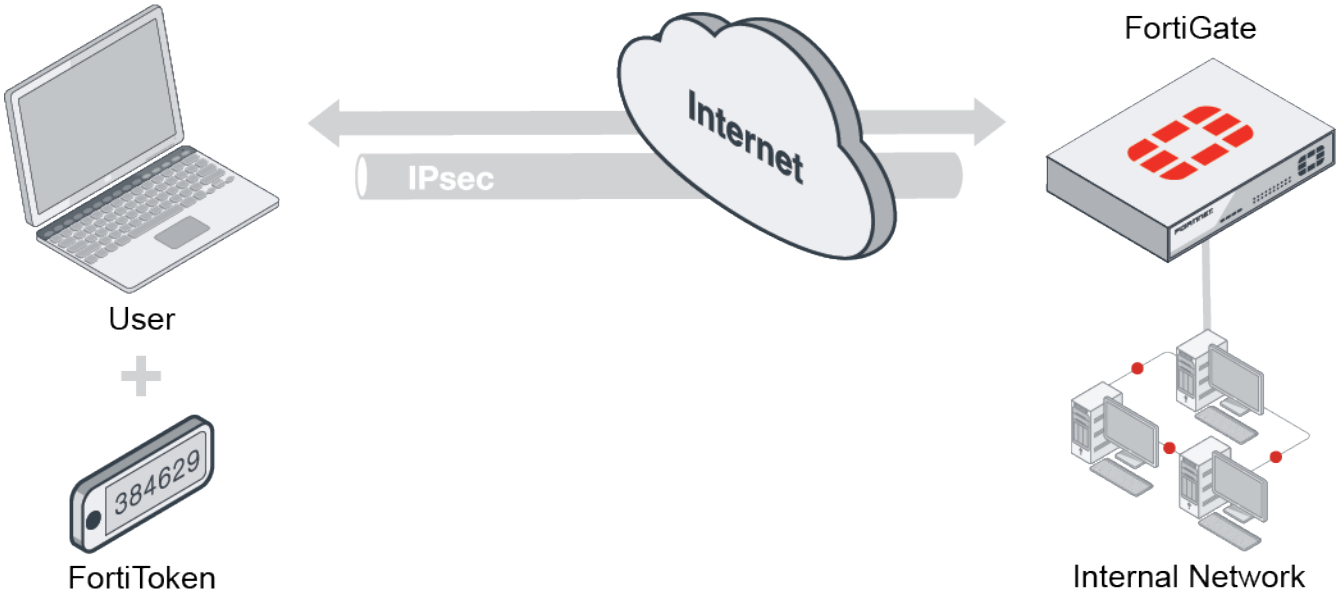
      ```
      .logo {
        background:#eee center 5px url(%%IMAGE:Example%%) no-repeat;
        padding-top:110px;
      }
      ```

      Make any other changes you wish.

      The new logo will replace the old image on the login page.
   e. Under *Authentication*, select *FortiToken Page* and make the same customization changes made for the login page.
5. 5. Check your results:

   Internal network users are redirected to the captive portal login page when attempting to browse the Internet.
   a. Enter the user's credentials. You are prompted to enter a FortiToken code. Enter the code from FFortiToken Mobile and click *Continue*.
   b. The user is successfully authenticated and has access to the internet.
   c. To verify the user's connection, go to *Monitor* > *FortiClient Monitor*.

Example: IPsec VPN two-factor authentication with FortiToken-200



In this scenario, you will configure two-factor authentication using a FortiToken-200 for IPsec VPN connections.

This configuration assumes that you have already created a user (`elainemarley`) and a user group (`FTK-users`). You will add a FortiToken-200 to FortiGate, assign the token to the user, and add the user to the group. You will then use create an IPsec VPN tunnel that allows FortiToken-200 users to securely access an internal network and the Internet. You will test the setup by having the user access the VPN from a remote device, using FortiClient.

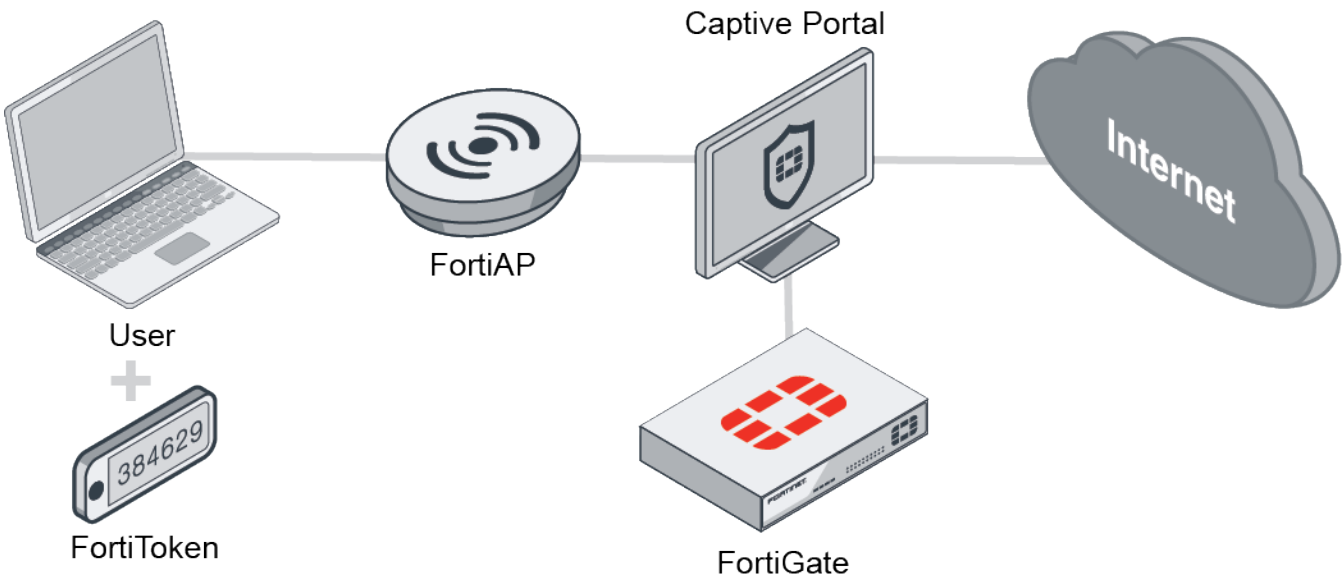
You can view a video of this configuration here.

1. 1. Add the FortiToken:
   a. In FortiGate, go to *User & Authentication* > *FortiTokens* and click *Create New*.
   b. Set *Type* to *Hard Token*, enter the FortiToken *Serial Number*, and click *OK*. The serial number, located on the back of the FortiToken device, is case sensitive. Note that the token can only be registered to one device.
2. 2. Edit the user and assign the FortiToken:
   a. Go to *User & Authentication* > *User Definition* and edit `elainemarley`.
   b. Enable *Two-factor Authentication*, set *AuthenticationType* to *FortiToken*, and select the token in the *Token* field.
   c. Enable *User Group*, select `FTK-users`, then click *OK*.
3. 3. Configure IPsec VPN using the IPsec VPN Wizard:
   a. Go to *VPN* > *IPSec Wizard*.
   b. Enter a *Name* (in this example, `FTK-VPN`).
   c. Set Template type to *Remote Access* template, set *Remote device type* to *Client-based* and *FortiClient*, and click *Next*.
   d. Set *Incoming Interface* to the internet-facing interface.
   e. Set *Authentication method* to *Pre-shared Key* and enter the key in *Pre-shared key*.
   Select the *User Group* (FTK-users) and click *Next*.
   f. Set *Local interface* to the internal interface and set *Local Address* to *all*.

g. In *Client Address Range*, enter the IP address range for VPN users. Ensure no other interfaces are using the same address range. *Subnet Mask* should already be set.
h. Click *Next*.
i. Configure additional *Client Options* as needed and click *Create*.
   A summary page appears showing the VPN configuration.

4. 4. Connect to the IPsec VPN:
   a. On your remote device, open the FortiClient application, go to *REMOTE ACCESS*, and add a new connection.
   b. Set *VPN* to *IPsec VPN*, and enter a *Connection Name*.
   c. Set *Remote Gateway* to the IP address of the FortiGate.
   d. Set *Authentication Method* to *Pre-shared key*, and enter the key.The key must match the key entered in the wizard on the FortiGate earlier.
   e. Click *Save* to add the new connection.
5. 5. Check your results:
   a. Go to *REMOTE ACCESS* and attempt to log in to the VPN as `elainemarley`.
   b. You will be prompted to enter a FortiToken code. Enter the code from the FortiToken device and click *OK*.
   c. The user is now connected to the IPsec VPN `FTK-VPN`.
   d. To verify the user's connection, go to *Dashboard* > *FortiView VPN*.
   e. You can also go to *Dashboard* > *Network* to view the IPsec tunnel status, and *Dashboard* > *Users & Devices* to view the user and device.

Example: Captive portal WiFi access with FortiToken-200



In this scenario, you will enforce two-factor authentication for WiFi users who have FortiToken-200 devices through a captive portal. FortiToken-200 users who attempt to browse the internet will be redirected to the captive portal login page and asked to enter their username, password, and six-digit authentication code.

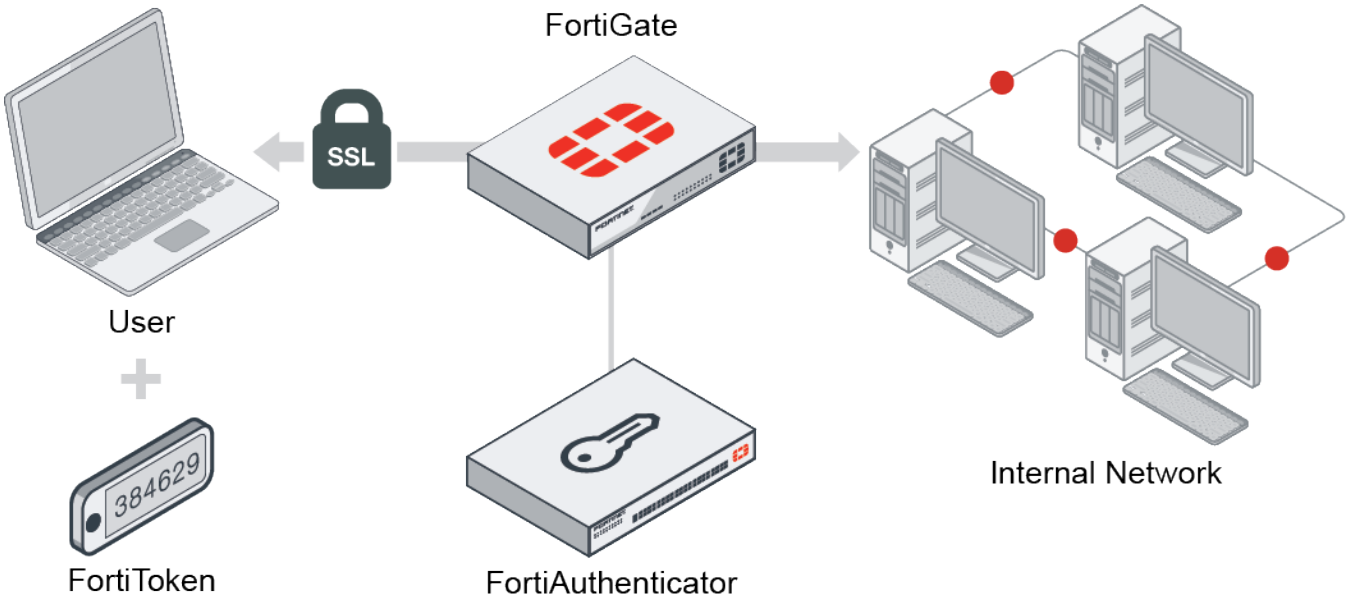
This scenario assumes that you already have a FortiAP unit connected and authorized with FortiGate, and that the SSID has been set up and configured to use captive portal.

This configuration is designed for a FortiToken-200 physical key generator. See step 2 for information about using FortiToken Mobile.

1. 1. Add the FortiToken:
   a. In FortiGate, go to *User & Authentication* > *FortiTokens* and click *Create New*.
   b. Set *Type* to *Hard Token*, enter the FortiToken *Serial Number*, and click *OK*. The serial number, located on the back of the FortiToken device, is case sensitive. Note that the token can only be registered to one device.
2. 2. Edit the user and assign the FortiToken:
   a. Go to *User & Authentication* > *User Definition* and edit the user (`rgreen`).
   b. Enable *Two-factor Authentication*, set *AuthenticationType* to *FortiToken*, and select the token in the *Token* field.
   c. Enable *User Group* and select the captive portal user group (`employees`).
   d. Click *OK* to save these changes.

   
   If the user has FortiToken Mobile, the user's contact information must be included so that the FortiToken code can be sent to the user via email or SMS.
3. 3. Check your results:
   a. When a user attempts to browse the internet, they are redirected to the captive portal login screen.
   b. Members of the FortiToken group must enter their username and password and are redirected to a screen requiring them to enter their token code. They retrieve the code by pressing the button on their FortiToken device. Once the code is successfully entered, the user is redirected to the URL originally requested.
   c. In FortiGate, go to *Dashboard* > *Users & Devices* to verify that the user is authenticated.

Example: FortiToken two-factor authentication with RADIUS on a FortiAuthenticator



In this scenario, you will set up FortiAuthenticator to function as a RADIUS server to allow SSL VPN users to authenticate with a FortiToken-200.

This scenario assumes that you have already added the FortiToken, assigned it to the user, and added the user to a group for FortiToken users on FortiAuthenticator.

You will configure a user, FortiToken-200, the RADIUS client on FortiAuthenticator, and FortiGate to use FortiAuthenticator as a RADIUS server. You will then create the SSL VPN tunnel.

You can view a video of this configuration here.

1. Add FortiToken to FortiAuthenticator:
   a. In FortiAuthenticator, go to *Authentication* > *User Management* > *FortiTokens*, and click *Create New*.
   b. Set *Token type* to *FortiToken Hardware* and enter the FortiToken serial number into the *Serial numbers* field. The serial number, located on the back of the FortiToken device, is case sensitive. Note that the token can only be registered to one device.
2. 2. Add the FortiToken user to FortiAuthenticator:
   a. In FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users* and click *Create New*.
   b. Enter a *Username* (`gthreepwood`), enter and confirm a password, and enable *Allow RADIUS authentication*.
   c. Click OK to access additional settings.
   d. Enable *One-Time Password (OTP) authentication*, set *Deliver token codes from* to *FortiAuthenticator*, set *Deliver token code by* to *FortiToken*, select the FortiToken added earlier from the *Token* field, and then click *OK* to save.
   e. Go to *Authentication* > *User Management* > *User Groups*, create a user group (`RemoteFortiTokenUsers`), and add `gthreepwood` to the group.
3. 3. Create the RADIUS Client on FortiAuthenticator:

   a. In FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients* and click *Create New*.
   b. Enter a name (`OfficeServer`), set *Client address* to *IP/Hostname* and enter the IP address of the FortiGate, and enter a *Secret*. The secret is a pre-shared, secure password that FortiGate will use to authenticate with FortiAuthenticator.
   c. Go to *Authentication* > *RADIUS Service* > *Policies* and click *Create New*.
   d. Enter a *Policy name* and choose the FortiGate client in the *RADIUS clients* field. Click *Next* to continue.
   e. In the *RADIUS attribute criteria* section, click *Next* to continue.
   f. In *Authentication Type*, select *Password/OTP authentication*.
   g. In *Realms*, set *Realm* to *local | Local users* and enable *Filter*. Note the *Username* input format. This is the format that the user must use to enter their username in the web portal.
   h. Edit the filter, choose the user group created earlier, click *OK*, then click *Next* to continue.
   i. Click *Next* and then click *Save and exit* to save the policy.

4. 4. Connect FortiGate to the RADIUS Server:
   a. In FortiGate, go to User & Authentication > RADIUS Servers, and click *Create New*.
   b. Enter a *Name* (`OfficeRADIUS`), set *Primary Server* > *IP/Name* to the IP of the FortiAuthenticator, and enter the *Secret* created earlier.

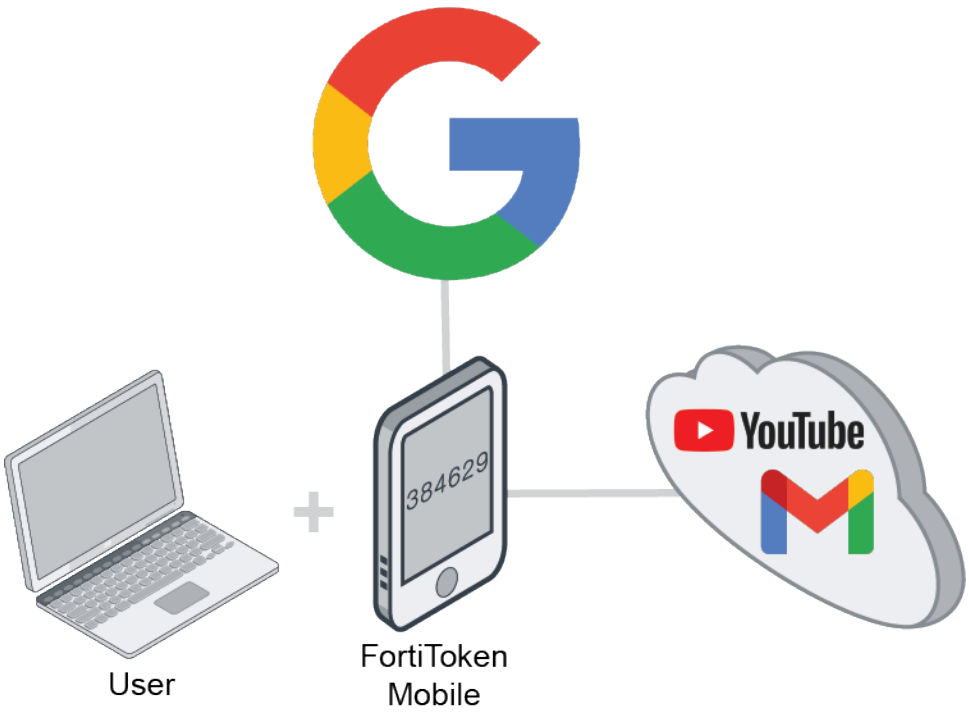
      Use the *Test Connectivity* and *Test User Credentials* buttons to verify the connection. Click *OK* to save the RADIUS server.

      The FortiGate can now log into the RADIUS client added earlier in FortiAuthenticator.
   c. Go to *User & Authentication* > *User Groups*, and click *Create New*.
   d. Enter a *Name* (`SSLVPNGroup`), set *Type* to *RADIUS Single Sign-On (RSSO)*, enter the RADIUS user group name (`RemoteFortiTokenUsers`) in the *RADIUS Attribute Value* field, then click *OK*.

5. 5. Configure the SSL VPN on FortiGate:
   a. In FortiGate, go to *VPN* > *SSL-VPN Portals*, and edit the full-access portal. Set *Split Tunneling* to *Disabled*.
   b. Go to *VPN* > *SSL-VPN Settings*.
   c. In *Connection Settings*, set *Listen on Port* to `10443`.
   d. In *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set it to `SSLVPN_TUNNEL_ADDR1`.
   e. In *Authentication/Portal Mapping*, click *Create New*. In *Users/Groups*, select the *SSLVPNGroup*, in *Portal*, select *full-access*, and click *OK*.
   f. In *Authentication/Portal Mapping*, select *All Other Users/Groups* and click *Edit*. Set *Portal* to *web-access* and click *OK*. This grants all other users access to the web portal only.
   g. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
   h. Set *Incoming Interface* to *SSL-VPN tunnel interface* and set *Outgoing Interface* to the internet-facing interface.
   i. Set *Source* to the *SSLVPNGroup* user group and set *Destination* to all.
   j. Set *Schedule* to *always*, *Service* to *ALL*, and enable *NAT*.
   k. Click *OK* to save the new policy.

6. 6. Check your results:
   a. From a remote device, open a web browser and navigate to the SSL-VPN web portal (*https://FortiGate-IP:10443*).Enter the user's credentials and click *Login*. Note that the username has to be entered in the format `realm\username`, as per the client configuration in FortiAuthenticator (in this example, `local\gthreepwood`).
   b. The user is prompted to enter their FortiToken code.
   c. Once the code is successfully entered, `gthreepwood` is successfully logged in to the SSL-VPN portal.
   d. In FortiGate, go to *Monitor* > *SSL-VPN Monitor* to confirm the user's connection.

Example: Third-party token activation with Google



In this scenario, you will enable Google's *2-Step Verification* and add the Google token to FortiToken Mobile for third-party two-factor authentication.

1. 1. Configure Google two-step verification in the browser:
   a. Open a browser and log in to your Google account at `https://accounts.google.com`.
   b. Click *Security*.
   c. In *Signing in to Google*, click *2-Step Verification* (re-enter your password if necessary), and then click *GET STARTED*.
   d. Follow the prompts to connect to your device using bluetooth and add a backup verification method.
   e. On your Google *2-Step Verification* page, click *Authenticator app*.
   f. If needed, re-enter your password.
   g. Click *Set up authenticator*. A QR code is displayed.
2. 2. Add Google 2-step verification to FortiToken Mobile:
   a. Open FortiToken Mobile on your mobile device and tap *Add Account*.
   b. Tap *SCAN BARCODE* or *ENTER MANUALLY*.If you choose to enter manually, tap *3RD PARTY ACCOUNTS* > *Other*. The account name will be your email address.
   c. Scan the QR code displayed in the *Authenticator app setup* dialog in your browser and then click *Next* in the dialog or click *Can't scan it?* to view and enter the secret key into FortiToken Mobile manually.

      FortiToken Mobile begins producing Google authentication codes.
   d. In the *Authenticator app setup* dialog, enter the 6-digit code displayed in FortiToken Mobile and click *Verify*.
3. 3. Check your results:
   a. Attempt to log in to a Google account (Gmail or YouTube, for example). You are prompted to enter your

verification code.

b. Enter the code displayed in FortiToken Mobile and click *Done*.

Reference

The following section provides additional reference information for FortiToken-200, FortiToken-200CD, and FortiToken Mobile.

FortiToken-200CD uses the serial number prefix `FTK211` on the back side of the physical token in order to distinguish it from the standard FortiToken-200, which uses the serial number prefix `FTK200`.

FortiToken Mobile uses the serial letter prefix `FTKMOB`.

FortiToken platform scalability

The following table shows the maximum number of FortiTokens that can be assigned to certain FortiGate and FortiAuthenticator models. Note that FortiToken is also supported on specific FortiWiFi models.

All data for this table was taken from the following Product Matrix datasheet.

FortiGate Models	Max. FortiTokens
30D / 30E	20
40F	500
50E / 60D / 60E / 70D / 80D / 90 series	100
60F / 70F / 80F	500
100D / 140D / 200D / 240D / 280D POE / 300D / 400D / 500D / 600D / 800C / 900D	1 000
100F / 200F / 400E / 400F / 600F	5 000
1000D / 1200D / 1500D / 3000D / 3100D / 3200D / 3700D / 3810D / 3815D / 5001D	5 000
VMware / KVM / Hyper V / Xen / AWS / AWS PAYG / Azure / Azure PAYG / Google Cloud / Google Cloud PAYG	5 000
1100E / 1000F / 1800F / 2200E / 2600E / 3700E / 3960E / 3980E / 4200E / 7060E	20 000
2600F / 3000F / 3300F / 3400E / 3500E / 4400F / 6300F / 6500F / 7121F/-2	20 000

FortiAuthenticator Models	Max. FortiTokens
200D	500
300F	3 000

FortiAuthenticator Models	Max. FortiTokens
400C	2 000
800F	16 000
1000D	10 000
3000D	40 000
3000F	480 000
VM BASE to VM-100000-UG	200 to 200 000+

Drift adjustment

If a user experiences clock drift, it may be the result of incorrect device time settings. If so, make sure that the mobile device clock is accurate by confirming the network time and correct timezone.

If the device clock is set correctly, the issue may be the result of the FortiAuthenticator unit and FortiTokens being initialized prior to setting an NTP server. This will result in a time difference that is too large to correct with the synchronize function. To avoid this, selected tokens can be manually drift adjusted.

The following procedure is intended to be used only in special cases where some FortiTokens are severely out-of-sync, for example, when a token is switched from manual configuration to NTP control.

Under normal circumstances, this is not required.

Only activated FortiTokens can be adjusted.

To perform time drift adjustment on a FortiToken:

1. In a browser, go to `https://<FortiAuthenticator-IP-Address>/admin/fortitoken/fortitokendrift/`
2. Select the FortiToken to adjust and click *Adjust Drift*.
3. Enter the required *Time adjustment* in minutes.
   Include a minus sign (**-**) for a negative value, but don't use a plus sign (**+**) for a positive value.
4. Click *OK* to adjust the token drift by the specified time.

Diagnosing FortiToken on FortiGate

The following diagnose command will show a list of FortiTokens, with drift and status:

```
diagnose fortitoken info

FORTITOKEN         DRIFT  STATUS
FTK200XXXXXXXXXX   0      new
```

```
FTK211XXXXXXXXXX  0      new
FTKMOBXXXXXXXXXX  0      new


Total activated token: 0
Total global activated token: 0

Token server status: reachable
```

Status outputs:

- `new`
  Newly added to FortiGate and not assigned to a user.
- `active`
  Assigned to a user. This output is for FortiToken-200 and 200 CD only.
- `provisioned`
  User has activated their token and it is assigned to them. This output is for FortiToken Mobile only.
- `provision timeout`
  The administrator assigned the token to the user, but the user did not activate the token within the timeout period. The token must be re-provisioned to the user.
- `token already activated, and seed won't be returned`
  FortiToken-200 has been added, removed, and re-added to the FortiGate. To transfer FortiToken-200 tokens from one FortiGate or FortiAuthenticator device to another, visit the Fortinet Support website.
- `activation error (token not exist in FortiGuard)`
  FortiToken-200 CD has been imported with the activation CD, but there is no contact to the FortiGuard server. In the event of this status, visit the Fortinet Support website.

When contacting customer support, you must provide the FortiToken serial number as well as the FortiGate or FortiAuthenticator serial number to which the token is assigned.

FortiToken provisioning with FortiAuthenticator REST API

The FortiAuthenticator API can be accessed (without additional cost or licensing) so that third-party user provisioning systems can confirm which FortiTokens are available to be provisioned to a user.

For the API to be accessible, a user must be granted administrator privileges so that they can log in. To view the FortiToken resource, cURL is being used to make the requests. For more information on how to do this, see the FortiAuthenticator REST API Solution Guide.

Accessing the REST API

To access the REST API resource, you browse to the following URL:

`https://[server_name]/api/[api_version]/[resource]/`

- `server_name`: Name or IP address of the FortiAuthenticator.
- `api_version`: API version to be used (currently `v1`).

- `resource`: Resource of part of config to be viewed.
  For the purposes of accessing FortiToken information, the resource is `/fortitokens/`.

To view a list of all the available resource end-points, send a request to:
`https://[server_name]/api/v1/?format=xml`

Resource: /fortitokens/

URL: `https://[server_name]/api/[api_version]/fortitokens/`

In the FortiAuthenticator GUI, this resource corresponds to *Authentication* > *User Management* > *FortiTokens*. This resource is used by third-party user provisioning systems to confirm which FortiTokens are available to be provisioned to a user.

Supported Fields

Field	Display Name	Type	Required	Other Restriction
serial	Serial number	string	No	
type	Type	string	No	Either `ftk` or `ftm`.
status	Status	string	No	Either `new`, `available`, `pending`, or `assigned`.

Allowed methods

Type	Allowed Methods	Action
List	GET	Get all FortiTokens.

Allowed filters

Field	Lookup Expressions	Values
serial	exact, iexact	
type	exact, iexact	Either `ftk` or `ftm`.
status	exact, iexact	Either `new`, `available`, `pending`, or `assigned`.

View all tokens

JSON Query

```
curl -X GET -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS
     https://192.168.0.122/api/v1/fortitokens/?format=json
```

Response

```
< HTTP/1.1 200 OK
{
   "meta": {
      "limit": 20,
      "next": null,
      "offset": 0,
      "previous": null,
      "total_count": 2
   },
   "objects": [
      {
         "resource_uri": "/api/v1/fortitokens/1/",
         "serial": "FTKMOB44142CCBF3",
         "status": "available",
         "type": "ftm"
      },
      {
         "resource_uri": "/api/v1/fortitokens/2/",
         "serial": "FTKMOB4471BB94D1",
         "status": "available",
         "type": "ftm"
      }
   ]
}
```

View subset of tokens using filters

This example shows how to obtain a list of specific tokens, for example the first available FortiToken Mobile (FTM) token.

JSON Query

```
curl -X GET -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS"
     -H 'Accept: application/json'
     "https://192.168.0.122/api/v1/fortitokens/?format=json&type=ftm&status=available&limit
     =1"
```

The URL requires additional quoting in this case, otherwise the CLI treats the "&" as an instruction to place the cURL command into the background.

Response

```
< HTTP/1.1 200 OK
{
```

```
   "meta": {
      "limit": 1,
      "next": "/api/v1/fortitokens/?status=available&type=ftm&offset=1&limit=1&format=json",
      "offset": 0,
      "previous": null,
      "total_count": 2
   },
   "objects": [
      {
         "resource_uri": "/api/v1/fortitokens/1/",
         "serial": "FTKMOB44142CCBF3",
         "status": "available",
         "type": "ftm"
      }
   ]
}
```


Authentication resource: /auth/

URL: `https://[server_name]/api/[api_version]/auth/`

The *Authentication* resouce is for validation of user credentials. Either the password, token, or both can be validated. This is useful for adding an additional factor authentication (e.g. token) to web portals where the first factor has already been locally validated (e.g. via LDAP, local DB, or a proprietary, unsupported authentication method).

To authenticate a user, POST to `https://[server_name]/api/v1/auth/` with the following key-value pair(in JSON format, but XML is also possible):

```
{
   "username": "<username>",
   "token_code": "<token_code>",
   "password": "<password>"
}
```

The `token_code` and `password` fields are optional. For example, you may validate the token only or the password only. If both token and password are specified, the password will be validated first, before the token code. If a user doesn't have two-factor authentication configured, validation for that user with any `token_code` will fail.

Supported fields

Field	Display Name	Type	Required	Other Restriction
username	Username	string	Yes	
password	Password	string	No	
token_code	Security token code	string	No	Supported token authentication: FortiToken, email token, SMS token

Allowed methods

Type	Allowed Methods	Action
List	POST	Validate user's credentials

Response codes

In addition to the general response codes, a POST request to this resource can result in the following return codes:

Code	Response Content	Description
200 OK		User is successfully authenticated.
401 Unauthorized	User authentication failed	Credentials are incorrect.
401 Unauthorized	Account is disabled	User account is currently disabled.
401 Unauthorized	No token configured	User does not have token-based authentication configured.
401 Unauthorized	Token is out of sync	The security token requires synchronization.
404 Not Found	User does not exist	The given username does not exist in the system.

To see the general response codes, see FortiAuthenticator REST API Solution Guide: General API response codes.

Validate a user password

JSON Query

```
curl -X POST -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS"
     -d '{"username":"testuser","password":"testpass"}'
     -H "Content-Type: application/json"
     https://192.168.0.122/api/v1/auth/
```

Response

```
< HTTP/1.1 200 OK
```

Validate a users token code

JSON Query

```
curl -X POST -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS"
     -d '{"username":"testuser","token_code":"893753"}'
     -H "Content-Type: application/json"
     https://192.168.0.122/api/v1/auth/
```

Response

```
< HTTP/1.1 200 OK
```

Error states

Response (incorrect password)

```
HTTP/1.1 401 UNAUTHORIZED
```

Response (incorrect token code)

```
HTTP/1.1 401 UNAUTHORIZED
```

Response (incorrect username)

```
HTTP/1.1 404 NOT FOUND
```

www.fortinet.com