FortiToken Cloud - Admin Guide

Version 21.2.d

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/support-and-training/training.html

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

JJune 28, 2021
FortiToken Cloud 21.2.d Admin Guide

TABLE OF CONTENTS

Introduction

Thank you for choosing FortiToken Cloud (FTC)!

FTC is an Identity and Access Management as a Service (IDaaS) cloud service offering by Fortinet. It enables FortiGate (FGT) and FortiAuthenticator (FAC) customers to add multi-factor authentication (MFA) for their respective users, with no additional hardware or software required. It protects local and remote FGT and FAC administrators as well as firewall and VPN users.

Main features

FortiToken Cloud (FTC) offers the following main features:

- **Multi-factor authentication (MFA) for FGT and FAC devices**—FTC provides a cloud-based MFA solution for all your FortiGate (FGT) and FortiAuthenticator (FAC) devices.
- **Integration with FOS 6.2**—FTC works seamlessly with FortiOS (FOS) 6.2.x.
- **Support for MFA bypass and new token request**—FTC admin users can allow end-uses to bypass MFA and request new tokens on behalf of their end-users easily from the GUI.
- **Automatic lockout of users for excessive MFA failures**—FTC automatically locks out users when they have breached their specified MFA failure threshold, ensuring security and integrity of your account.
- **Secure, cross-platform token transfer**—You can securely transfer your FTC and third-party tokens between iOS and Android devices using the FortiToken Mobile (FTM) app.
- **User synchronization from FGT and/or FAC to FTC**—The admin user can synchronize their end users from FGT or FAC to FTC from the FGT Console or FAC GUI. The user base of record is always the Auth Client (i.e., FGT or FAC), and trumps the user base that exists in FTC (if different) prior to running the sync command.
- **Support for remote FortiGate users**—You can configure FortiGate wildcard LDAP users to use FTC for MFA. See Configure wildcard LDAP users for FTC service on page 29 for details.
- **Auth client delete function from FTC**—The admin user is able to delete from the FTC portal auth clients that are no longer in use.
- **Auto log-out**—FTC automatically logs out a user when the GUI has been idle for more than ten minutes, safeguarding the security and integrity of your asset on FTC.
- **Real-time usage statistics**—The admin user can view up-to-date usage data for the current month easily from the GUI.
- **Subscription-based MFA service**—FTC uses a flexible SKU-based subscription mechanism to enable you to subscribe and scale your FTC MFA service with ease.
- **Free trial offer**—FTC offers a 24-credit free trial subscription to enable potential customers to try it out before purchase.
- **FortiCloud SSO**—Integration with FortiCloud provides unified single sign-on (SSO) access to all your Fortinet cloud service offerings.
- **Authentication and Management logs**—FTC provides comprehensive authentication and management logs to keep you informed of all authentication and management events that have happened in your account.
- **Support for FGT HA clusters**—FTC supports FGT and FAC HA cluster configuration. You can view your FGT and/or FAC devices in any cluster from the Auth Clients page.

- **Support for custom logo**—The admin user can upload custom logo images to replace the default Fortinet banner at the bottom of the FTM app on your end-users' mobile devices.
- **FTM token activation/transfer notification by SMS**—FTC is able to send FTM token activation or transfer notifications to end-user mobile devices by SMS.
- **Access to all accounts by admin users**—The admin user is able to access all FTC accounts belonging to his/her own organization, choose which of your accounts to open upon login, and switch to any of your other accounts during a session.
- **Global administrator and sub-admin support**—FTC now enables the global admin to create sun-admin account to better allocate and manage resources across all the accounts under management.
- **Realm support**—FTC enables admin users to create realms to effectively allocate resources and better manage their end users.
- **Support for multiple MFA options**—FTC offers four MFA methods: FTM (FortiToken Mobile), email, SMS, and FTK (FortiToken, which is a hardware token).
- **Auto-alias by email**—You can attribute different usernames with the same email address to the same user so that only one token needs to be assigned to a single user. See Enable Auto-alias by Email for details.
- **Time-based license model**—FortiToken Cloud (FTC) now features a new annual subscription model with license options for customers to choose from based on the number of FTC end users on their account per year. The new license model allows for SMS messages in the amount of 100 multiplied by the total number of users your license can support for the year. *(Applicable to time-based annual subscriptions only.)*
- **Realm-based user quota**—The administrator of a customer with time-based license now can allocate user quota to each realm to effectively manage their assets and end users. *(Applicable to time-based annual subscriptions only.)*
- **Export of logs in .CSV**—You can now export FTC authentication and management logs in .CSV format for record keeping and sharing.

Licensing

FTC is a subscription-based cloud service. Upon purchasing your service subscription, you receive a License Certificate in .pdf format with a license code in it. *Be sure to register your FTC license under the same FortiCloud (FC) account where your FortiGate or FortiAuthenticator is registered.*

FC manages FTC service licensing using SKUs, which come at different credit levels. Credits are consumed based on the number of MFA cloud service user-months in your FTC account. One credit equals to one user-month. Each SKU has an expiration date, and you must use your credits before they expire. You can add more credits to your subscription through an in-app purchase of new SKUs. The FTC portal keeps track of your user-months and reports your monthly usage data to FC. For more information, see Usage on page 57.

Your license is valid only for one year after the date of purchase. Be sure to activate your license within one year of purchase. Your license will be invalid once it has expired. Licenses that have expired cannot Un-used credits will expire one year after activation.

The following table shows the license options that FTC offers.

SKU	Number of FTC credits
FTC-LIC-120	120

SKU	Number of FTC credits
FTC-LIC-1200	1,200
FTC-LIC-12K	12,000
FTC-LIC-120K	120,000

Compatible Fortinet applications

FortiToken Cloud 21.2.d works in tandem with the following Fortinet applications:

- FortiOS 6.2.3 or later, and FortiOS 6.4.0 or later
- FortiClient 6.2.2 or later
- FortiAuthenticator 6.0.1 or later
- FortiSandbox 3.2.0 or later
- FortiADC 6.0 or later
- FortiToken Mobile (FTM) iOS 4.5.3 or later
- FortiToken Mobile (FTM) Android 4.6.0 or later

- FortiToken Cloud works best with FortiOS 6.2.3 or later. If you have to use FortiOS 6.2.0, we strongly recommend that you turn off the multi-realm mode and move your auth clients to the default realm.
- For the time being, FortiToken Cloud does NOT support OTP via email or SMS as an MFA method for end users with FortiAuthenticator as the auth client.

Supported browsers

FortiToken Cloud 21.2.d supports the latest versions of the following web browsers:

- Google Chrome
- Mozilla Firefox

Other web browsers may work as well, but have not been rigorously tested.

Important notes

This section discusses some subtle but important credits regarding the use of FTC.

- Transferring auth clients on page 10
- Use of non-officially supported FOS on page 10

Transferring auth clients

You can transfer your auth clients from one FTC account to another. However, before transferring an auth client, we strongly recommend that you delete all data on the auth client. FortiToken Cloud or the Fortinet Support is unable to automatically delete old user data left on transferred auth clients.

Use of non-officially supported FOS

FOS 6.2.1 is not officially supported by FTC. Although it is still possible to enable FTC MFA for users on that platform, using FTC with FOS 6.2.1 may introduce a security risk that allows SSL VPN users to log in without a second factor when the second factor is configured from FTC.

DO NOT use FTC with FOS 6.2.1!

The same token for the same user on multiple auth clients

FortiToken Cloud allows the same end user created on two or more auth clients to use the same FortiToken Mobile (FTM) or FortiToken (FTK) token for FortiToken Cloud services, as long as the following conditions are met:

- The auth clients must be FortiGate VDOMs only.
- The same user created on the auth clients must bear the same username.
- The auth clients must be assigned to the same realm in FortiToken Cloud.

FOS 6.2.3 and 6.4.0 CLI differences

Starting with FOS 6.4.0, the "local" and "remote" options are added to the following CLI commands:

```
execute fortitoken-cloud sync {<Enter> | all | local | remote}
```

```
diag fortitoken-cloud sync {<Enter> | all | local | remote}
```

These two options apply to FOS 6.4.0 only, and do not apply to FOS 6.2.3 which does not distinguish between local and remote users.

Admin accounts and realms

Starting from its 20.1.a release, FortiToken Cloud (FTC) has introduced the following major behavior change which will impact all FTC customers, including existing customers:

Upon upgrading to 20.1.a or later, the first FTC account of your organization that has logged in to the FTC portal originally and/or your master account in FortiCloud will be automatically assigned the FTC global admin role; all accounts under your FortiCloud master account will be assigned the sub-admin role by default, with no realm assigned (including the default Realm) to them, and therefore will not be able to see any FTC data. The global admin must create admin groups and map the sub-admins with the realms in order for them to view and manage realm resources.

For more information, refer to the FTC Admin Guide and online Help.

Supported hard tokens

For the current release, FortiToken Cloud only supports FortiToken (FTK) FTK200 and FTK220 hardware tokens. The FTK200CD (with token serial number prefix FTK211) is NOT supported.

No SMS MFA with FAC as LDAP server

FortiToken Cloud (FTC) does not support SMS MFA authentication for end users configured on FortiAuthenticator as a native LDAP server, because a FortiAuthenticator native LDAP server does not allow FTC to query the users' phone numbers. Therefore, FTC does support SMS MFA for FortiAuthenticator end users configured as remote users in a remote LDAP server.

A single FTC user in multiple auth clients

A given FTC user can be in two or more auth clients (FGT or FAC devices), resulting in a so-called "single-user-in-multiple-auth-clients" situation. For example, User-1 can be in FGT-1 and FGT-2. An FTC admin user is able to see all auth clients (FGTs) for a given user on the FTC portal.

You must keep the following two important credits in mind when handling such a situation:

(1) When you disable (remove) User-1 from FGT-1, it still exists in FGT-2. As a result, User-1 still remains in FTC. The only way to remove User-1 from FTC is to remove it from both FGT-1 and FGT-2.

(2) Suppose you have enabled User-1 for FTC in FGT-1 and FGT-2, and the end user of User-1 has a token from FTC. You disable User-1 in FGT-1, but leave it still enabled in FGT-2 so that it still exists in FTC. Later on, if you enable User-1 again without assigning it a new FTC token, User-1 will continue to use the same FTC token it used before.

Now suppose, instead of enabling User-1 again in FGT-1, you assign SMS from FGT-1 (an FGT internal feature that is not available in FTC) as the MFA method for User-1. This is what is going to happen: If User-1 attempts to log into FGT-1, the user will get an SMS from FGT-1; but if User-1 attempts to log into FGT-2, the user will have to use the FTC token.

Starting with its version 20.1.a release, FortiToken Cloud has introduced the multi-realm concept. As a result, two identical end users can co-exist on two different auth clients assigned to two different realms.

FAC users' name issues on FTC GUI

Names of FTC users created on FortiAuthenticator (FAC) show up with prefixed and suffixed characters in corner brackets, on the FTC GUI and in email notifications. This is due to the fact that FAC differentiates the same username populated by multiple user sources to FAC. The development team is aware of this issue and is working to resolve it in a future release.

How to use FortiClient

FortiToken Cloud supports FortiClient 6.2.1 and later for both auto push and manual OTP.

Use auto push

Upon entering your username and password, you do the following:

1. On FortiClient, log in with your username and password.
2. On your mobile device, press the **Approve** button.
3. Wait for FortiClient to complete the remote access login.

"Notification" must be enabled on the mobile device for auto push to work.

Use OTP

Upon entering your username and password, do the following:

1. In the Token window on FortiClient, enter the OTP obtained from your mobile device.
2. On your mobile device, do not press the **Approve** or **Deny** button.
3. Wait for FortiClient to complete the remote access login.

Product documentation and support

The following are the FortiToken Cloud product documentation and support information:

- For information about the current release, see the Release Notes.
- For detailed information about product features, click the (Help) on the GUI or see Admin Guide.
- For product API, see REST API.
- For frequently asked questions, see FAQs.
- For SSL VPN configuration instructions, see SSL VPN Configuration Guide.
- For product licensing, see Purchasing Guide.
- For terms of service, see Service Descriptions.
- For product support issues, click FortiToken Cloud Support (fortitokencloud-support@fortinet.com).

Acronyms and abbreviations

The table below lists the acronyms and/or abbreviations used in this document and/or on the FTC portal.

Acronym/Abbreviation	Terminology
2FA	Two-factor authentication **Note:** This term is used in FortiGate/FortiOS. It carries the same meaning as "MFA" (listed below) used in FortiToken Cloud.
MFA	Multi-factor authentication.
Auth	Authentication
FAC	FortiAuthenticator
FC	FortiCloud
FGT	FortiGate
FOS	FortiOS
FTC	FortiToken Cloud
FTK	FortiToken (hardware token)
FTM	FortiToken Mobile (software token)
OTP	One-time password
SMS	Short message service
SSO	Single sign-on
TOTP	Time-based one-time password
UTC	Universal Time Coordinated (or Coordinated Universal Time)

Release history

This section highlights the major feature changes or updates in each of the releases of FortiToken Cloud since its GA release. For a complete list of product features, see Main features on page 7.

21.2.d

- **Time-based license model**—FortiToken Cloud (FTC) now features a new annual subscription model with license options for customers to choose from based on the number of FTC end users on their account per year. The new license model allows for SMS messages in the amount of 100 multiplied by the total number of users your license can support for the year. *(Applicable to the new time-based annual subscription only.)*
- **Realm-based user quota**—The administrator of a customer with time-based license now can allocate user quota to each realm to effectively manage their assets and end users. *(Applicable to the new time-based annual subscription only.)*
- **Export of logs in .CSV**—You can now export FTC authentication and management logs in .CSV format for record keeping and sharing.

21.2.c

FortiToken Cloud 21.2.c is a patch release only; no new feature or enhancement has been implemented in this release.

21.2.a

FortiToken Cloud 21.2.a offers the following new features and enhancements:

- New API to query credit balance with single request.
- Upgrade to FortiGuard access and authentication method.
- Read and write access to all settings, regardless of realm 2FA method.
- Custom OTP and token activation/transfer notification templates.
- FortiCloud IAM support (including new APIs).
- Dashboard Notification when free-trial credits are used.
- New logo for FC premium customers.
- Miscellaneous GUI updates.

21.1.a

FortiToken Cloud 21.1.a is a patch release, with the following enhancements:

- The word "point(s)" has been replaced with "credit(s)" in FortiToken Cloud and its documentation.
- The Dashboard has been updated with the following changes:
  - The "Realms/Max Realms" meter has been relocated to the same row as the "Users/Max Users"and "Clients/Max Clients" meters.
  - The "Clients/Max Clients" meter has been renamed to "Auth Clients/Max Auth Clients"

20.4.d

FortiToken Cloud 20.4.d is a patch release only; no new feature or enhancement has been implemented in this release.

20.4.c

- **Commercial API**—Enables admin users to add web applications as FTC auth clients and serve their end users.
- **API for generic auth clients**—The Auth Clients page now shows auth client type, auth client name, user count, and realm name.
- **Revamped GUI**—The Auth Clients page now has three sub-pages, with the FortiProducts sub-page showing auth client alias, auth client type, auth client name, user count, and realm name.
- **FortiToken Cloud RESTful API Specifications**—The document, available in the Docs Library, provides detailed information of the APIs and instructions on how to use them.

20.4.a

FortiToken Cloud 20.4.a is a patch release only; no new feature or enhancement has been implemented in this release.

20.3.e

FortiToken Cloud 20.3.e is a patch release only; no new feature or enhancement has been implemented in this release.

20.3.d

- **Token management made easy**—This release has added the Auth Devices menu to the main menu. It has two sub-menus: Mobile Devices and Hard Tokens. It consolidates soft tokens and hard tokens in one place, enabling the user to view and manage mobile devices and hard tokens more efficiently.
- **HA cluster management**—A Devices menu has been added to the main menu. Not only can you view standalone devices and clusters of auth clients on the same page, but add devices to or remove them from a cluster as well.
- **User Alias**—The **Settings>Realms** page now has an "Auto-alias by Email" option. When it is enabled, all usernames with the same email address and are in the same realm are automatically set as aliases under the

same username (on the Users page). In this way, FTC only needs to assign one token to the same user. When "Auto-alias by Email" is enabled in a realm, you can use the Users page to manually create aliases, modify, merge, or delete aliases.

- **Auto-create Auth Client**—The **Settings>Global** page now has added an "Auto-create Auth Client" option, which enables the global admin user to enable or disable (default) the auto-creation of auth clients. It applies to FortiGate VDOMs only, and offers global admin users an option to control over the auto-create-auth-client function for FortiGate VDOMs to prevent unintended auth clients from consuming credits.
- **Administrators page enhancements**—The Administrators page has gone through some enhancements. You are now able to select multiple realms to add to an admin group, and to view all accounts associated with a customer ID by clicking the Member Count in the Administrators page.
- **Export to CSV**—The Usage page now has an option to enable you to export usage data in .csv file format.
- **Contact Support**—The main menu now has an "Contact Support" menu, which enables you to contact Fortinet support team by email directly from the FTC portal.

20.2.c

FortiToken Cloud 20.2.c is a patch release only; no new feature or enhancement is implemented in this release.

20.1.b

- Differentiation of user data for local and remote auth client users.
- Support for FTM Windows provisioning and activation.

20.1.a

- **Hard Tokens**—FTC now supports FortiToken (FTK) which is a hardware token. See Hardware Tokens on page 54.
- **Global administrator and sub-admins**—FTC now enables the global administrator to create sub-admins and allocate resources to them. See Administrators on page 39.
- **Multi-realm support**—FTC now allows the global admin to create realms. See Realms on page 41.
- **More MFA methods**—This release adds support for e-mail, SMS, and FTK (FortiToken, which is a hardware token) as options for MFA. See Settings on page 61.

4.4.c

FortiToken Cloud 4.4.c is a patch release only; no new feature or enhancement is implemented in this release.

4.4.b

- **FortiAuthenticator as authentication client**—FortiToken Cloud now supports FortiAuthenticator as an authentication client, in addition to FortiGate.
- **FortiToken Cloud enabled on FortiGate**—FortiToken Cloud now is enabled on FortiGate by default.

4.3.a

- **Custom logo**—Enables admin users to upload custom logo images to replace the default Fortinet logo at the bottom of the FTM app screen on end users' devices. See Settings on page 61 for more information.
- **FTM token activation/transfer notification by SMS**—Enables admin users to let end users receive FTM token activation or transfer notifications by SMS. See Settings on page 61 for more information.
- **Access to all accounts by admin users**—FTC admin users are able to access all FTC accounts belonging to their own organization. They can choose which of their accounts to open upon login, and switch to any of their other accounts during a session.

4.2.d

FortiToken Cloud 4.2.d is a patch release in support of FortiCloud upgrade, along with some bug fixes; no new feature or enhancement is implemented in this release.

4.2.c

FortiToken Cloud 4.2.c is a patch release only; no new feature or enhancement is implemented in this release.

4.2.b

FortiToken Cloud 4.2.b is the FortiToken Cloud GA release, which offers many of the major features of the product. For more information, see Main features on page 7.

Getting started—FGT-FTC users

FTC service is enabled on FGT VDOMs by default. So an FGT VDOM with a valid FTC license automatically becomes an auth client of FTC the moment it is created.

FTC supports up to four MFA methods, namely FTM, FTK, SMS, and email. The MFA method is set on a per-realm basis. The default method is FTM, but the admin user can change it to another method if needed. Sub-admins can then further change the MFA methods for end users in their assigned realms to something other than the default (i.e., FTM). The Users on page 44 page shows the MFA methods used by individual end users.

If you use FGT as an authentication client of FTC, you may complete the following steps to get started with FTC:

1. Register your FTC subscription on page 18.
2. Upgrade FortiOS on page 19.
3. Log in to the FortiToken Cloud portal on page 19.
4. Activate FGT VDOMs for FTC service on page 20.
5. Add a local user for FTC service on page 20.
6. Add an admin user for FTC service on page 20.

Register your FTC subscription

Upon purchasing your FTC service subscription, you'll receive via email a license certificate (a .PDF file) with a registration code in it. Your first step is to register your FTC subscription on FortiCloud.

Be sure to register your FTC subscription to the same FortiCloud (FC) account where your FGT is registered.

To register your FTC subscription

1. Have your FTC license certificate ready.
2. Launch your web browser.
3. Log into FortiCloud with your FortiCloud username and password.
4. On the FortiCloud banner across the top of the page, click **Services** to open the drop-down menu.
5. Click **Asset Management** to open the Asset Management page.
6. From the side menu, click **Register Product.**
7. Follow the prompts onscreen to complete the registration.

Upgrade FortiOS

This FTC release requires upgrading your FortiGate (FGT) firmware to FortiOS (FOS) version 6.2.3

To upgrade your FortiOS

1. Log into your FGT device.
   The FGT GUI opens.
2. From the menu (on the left), click **System>Firmware**.
3. Click **Browse** to browse for FOS version 6.2.3.
4. Follow the instructions onscreen to complete upgrading your FOS.

Log in to the FortiToken Cloud portal

All FortiCloud (FC) registered users can access the FTC portal. If your organization has multiple FTC accounts, you'll see a list of your FTC accounts after you sign in on FortiCloud. You can then select an account to open it on the FTC portal. During a session, you can switch from one account to another using the Account drop-down menu in the upper-right corner of the GUI.

Access to FTC is managed by FortiCloud SSO authentication via FortiAuthenticator (FAC). Upon receiving your login request, the system redirects you to FortiCloud which is the FortiCloud (FC) SSO page. From there, you must use your FC master account username and password to log in. After authenticating your identity using multi-factor authentication (MFA), the system grants you access to the FTC portal.

To log in to the FTC portal

1. Open your web browser, point to https//ftc.fortinet.com, and press the **Enter** key on your keyboard.
   The FortiToken Cloud page opens.
2. In the upper-right corner of the page, click **LOGIN**.
   The FortiToken Cloud Login page opens.
3. Enter your FC master account username and password, and press **LOGIN**.
   Once you've logged in, the FortiToken Cloud landing page opens, showing your FTC account (or a list of accounts if your organization has multiple FTC accounts).
4. Click your account or one of your accounts to open it.
   The FTC Dashboard page opens by default.

Activate FGT VDOMs for FTC service

In order for your FortiGate users to take advantage of the MFA feature provided by FortiToken Cloud, you must make sure that FTC service is enabled on the FortiGate device.

Because 21.2.d requires FOS 6.2.3 or FOS 6.4.0 which has FortiToken Cloud service enabled by default, you normally do not need to manually enable FTC on your FGT running FOS 6.2.3. However, if for some reason, FTC is not enabled on the FortiGate, you must manually enable it to proceed.

Only an FGT global admin user can activate FTC service on a per-FGT device basis, not by specific VDOMs.

To activate FGT VDOMs for FTC service

```
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system global
FortiGate-VM64 (global) # set fortitoken-cloud enable
FortiGate-VM64 (global) # end
```

`set fortitoken-cloud enable` is a "local" command and does not trigger communication with the FTC server. It simply enables FGT VDOM admin users to manage FTC users locally using the FGT CLI.

Add an admin user for FTC service

You can add FGT VDOM admin users for FTC service using the following commands:

```
config system admin
   edit <admin_username>
      set accprofile <super_admin>
      set vdom root
      set two-factor fortitoken-cloud
      set email-to <admin_user@fortinet.com>
      set password ENC SH2aEArTfqHbNJ8E2O87zSFAYqak8t14t+AiQxH+XWhZMKJQMfoPZS002MDPCo=
   next
end
```

For more information, see Configure admin users on page 27.

Add a local user for FTC service

Once you are sure that your FTC service is enabled on your FGT device, you can add VDOM users and enable them for FTC service using the following commands:

```
config user local
    edit <username>
        set type password
        set two-factor fortitoken-cloud
        set email-to <user@abc.com>
        set passwd-time 2018-05-15 08:41:35
        set passwd ENC
51sXDNIDYqPgRvahKx6jh+HACElPinhC+yXCDva6ytEaH+bHM5G0+AFkwFVJdEpidKBIY0xn2LlLPpvSmWRhXhAFAP77Oo
fUdFSs9eydatFw/BY/4WgCimfir1EOLdtTRjVO9oaCj6LTPBYzZJsyrImmKx7benWG1tTOXWgmktUy88WR02rdUB8ZZdBT
fDfDoBAL2Q==
    next
end
```

As an option for two-factor authentication, “fortitoken-cloud” becomes available only when FTC service is enabled on FGT.

Upon execution of the above commands, a local FGT user is created and is set to use FTC for MFA authentication. Information about the user automatically appears on the Users page of the FTC portal. If the user is the first user of the FGT VDOM that you've added for FTC service, the VDOM appears on the Auth Clients page as well.

For more information, see Configure local users on page 28.

Add remote FortiGate users for FTC service

Your can use the following commands to configure FortiGate wildcard LDAP users to use FortiToken Cloud for MFA.

```
config user ldap
     edit "EngLDAP"
          set server "xxx.xx.xxx.xx"
          set cnid "uid"
          set dn "dc=srv,dc=world"
          set type regular
          set two-factor fortitoken-cloud
          set username "cn=Manager,dc=srv,dc=world"
          set password ENC LWdyb+/k6e4TtSk070tODaCZAcbgEGKohA==
     next
end
```

Wildcard LDAP users are those of a remote LDAP server user group, whose user configuration is unknown to FortiGate. For FortiGate to find them on the remote LDAP server, FortiOS requires that each user be configured with "uid" for "cnid" under "ou=People" in the dn and have the following attributes configured on the LDAP server:

- mail: user_email_address (e.g., mail: user1@abc.com)
- mobile: user_phone_number (e.g., mobile: +14080123456)

- In FortiOS, the "mail" attribute is mandatory and required of each user, while the "mobile" attribute is optional.
- FTC requires that the phone number be in the format of " +(country_code)(areacode_ number)".

See Configure wildcard LDAP users for FTC service on page 29 for more information.

Getting started—FAC-FTC users

- Tasks such as creating FAC users and enabling them for FTC service can and must be performed on the FAC GUI only; no FAC Console commands are available for such operations.
- FTC supports token activation via SMS and synchronization of mobile numbers for end users with FortiAuthenticator as the auth client. FortiAuthenticator 6.2 or later is required.
- For the time being, FTC does NOT support OTP via email or SMS as an MFA method for end users with FAC as the auth client.

If you use FAC as an authentication client of FTC, you can complete the following steps to get started with FTC:

1. Register your FTC subscription on page 22.
2. Upgrade FortiAuthenticator OS on page 23.
3. Log in to the FortiToken Cloud portal on page 23.
4. Activate FAC for FTC service on page 24.
5. Add an admin user for FTC service on page 24.
6. Add a local user for FTC service on page 24.

Register your FTC subscription

Upon purchasing your FTC service subscription, you'll receive via email a license certificate (a .PDF file) with a registration code in it. Your first step is to register your FTC subscription on FortiCloud.

Be sure to register your FTC subscription to the same FortiCloud (FC) account where your FortiAuthenticator (FAC) is registered.

To register your FTC subscription

1. Have your FTC license certificate ready.
2. Launch your web browser.
3. Log into FortiCloud with your FortiCloud username and password.
4. On the FortiCloud banner across the top of the page, click **Services** to open the drop-down menu.
5. Click **Asset Management** to open the Asset Management page.
6. From the side menu, click **Register Product.**
7. Follow the prompts onscreen to complete the registration.

Upgrade FortiAuthenticator OS

The FTC 4.4.c release requires upgrading your FortiAuthenticator (FAC) to FAC version 6.0.1.

To upgrade your FAC OS

1. Log into your FAC device.
   The FAC GUI opens.
2. From the menu (on the left), click **System>Firmware**.
3. Click **Browse** to browse for FAC version 6.0.1.
4. Follow the instructions onscreen to complete upgrading your FAC OS.

Log in to the FortiToken Cloud portal

All FortiCloud (FC) registered users can access the FTC portal. If your organization has multiple FTC accounts, you'll see a list of your FTC accounts after you sign in on FortiCloud. You can then select an account to open it on the FTC portal. During a session, you can switch from one account to another using the Account drop-down menu at the bottom of the main menu.

Access to FTC is managed by FortiCloud SSO authentication via FortiAuthenticator (FAC). Upon receiving your login request, the system redirects you to FortiCloud which is the FortiCloud (FC) SSO page. From there, you must use your FC master account username and password to log in. After authenticating your identity using multi-factor authentication (MFA), the system grants you access to the FTC portal.

To log in to the FTC portal

1. Open your web browser, credit to https//ftc.fortinet.com, and press the **Enter** key on your keyboard.
   The FortiToken Cloud page opens.
2. In the upper-right corner of the page, click **LOGIN**.
   The FortiToken Cloud Login page opens.
3. Enter your FC master account username and password, and press **LOGIN**.
   Once you've logged in, the FortiToken Cloud landing page opens, showing your FTC account (or a list of accounts if your organization has multiple FTC accounts).
4. Click your account or one of your accounts to open it.
   The FTC Dashboard page opens by default.

Activate FAC for FTC service

In order for your FortiAuthenticator (FAC) users to take advantage of the MFA feature provided by FortiToken Cloud, you must make sure that FTC service is enabled on your FAC devices.

Because FTC requires FAC 6.0.1 which has FortiToken Cloud service enabled by default, you normally do not need to manually enable FTC on your FAC. However, if for some reason, FTC is not enabled on the FAC, you must manually enable it to proceed.

Only the FAC admin user can activate FTC service on FAC devices.

Add an admin user for FTC service

You may add an FAC admin user for FTC service using the following procedures:

1. From the FAC menu, click **Authentication>User Management>Local Users**.
2. From the top of the page, click **Create New** to open the Create New Local User page.
3. Specify a unique username.
4. For Role, select the **Administrator** radio button.
5. Click **Full permission** to enable it.
6. Click **OK.**The page refreshes.
7. On the Change local user page, select **Token-based authentication>FortiToken>FortiToken Cloud.**
8. Click **User Information.**
9. Enter the user's first name and last name.
10. Enter the user's email address.
11. Click **OK.**

Names of FTC users created on FAC show up on the FTC GUI and in email notifications with some unwanted characters in corner brackets before and after them.

Add a local user for FTC service

Once you are sure that your FTC service is enabled on your FAC device, you can create local FAC users and enable them for FTC service using the following procedures:

1. From the FAC menu, click **Authentication>User Management>Local Users**.
2. From the top of the page, click **Create New** to open the Create New Local User page.
3. Specify a unique username.
4. For Role, select the **User** radio button.

5. Click **OK.**The page refreshes.
6. On the Change local user page, select **Token-based authentication>FortiToken>FortiToken Cloud.**
7. Click **User Information.**
8. Enter the user's first name and last name.
9. Enter the user's email address.
10. Click **OK.**

Once a user is created on FAC, information about the user automatically appears on the Users page of the FTC portal. If the user is the first user of the FAC that you've added for FTC service, the FAC appears on the Auth Clients page as well.

FAC supports local and remote users. FAC remote users are those imported into FAC form an LDAP/AD or RADIUS server. They are stored in FAC without their passwords (which are still kept in the remote directory). Such imported users are stored in FAC as Remote Users, and are unique per directory.

Names of FTC users created on FAC show up on the FTC GUI and in email notifications with some unwanted characters in corner brackets before and/or after them.

FOS CLI commands for FortiToken Cloud

This section discusses the FOS (version 6.2.3 and later, and version 6.4.0 and later) CLI commands supported in the FTC 21.2.d release.

Global system configuration

FortiOS comes with a "config system global" command, which enables the FortiGate admin to enable or disable FTC service on the FortiGate. If FTC is disabled, all APIs to FTC will be disabled, except the `"show"` command under `"execute fortitoken-cloud ?"`. This provides a way to control the communication between the whole FortiGate device so that individual auth clients (VDOMs) will not be able to set up their connections and communicate with the remote FTC server.

By default, FTC is enabled in FortiOS. If it is disabled, you won't have the option of FTC service as a MFA method when configuring a user.

```
config system global
    set alias "FG101ETK18002806"
    set hostname "FG101ETK18002806"
    set fortitoken-cloud enable
    set switch-controller enable
    set timezone 04
end
```

This global configuration does not invoke any FortiGate-FortiToken Cloud API.

Access FTC management commands

This global command enables you to access the following command options to manage FTC service on your FortiGate.

```
FG101ETK18002806 #  execute fortitoken-cloud ?
new       Send new activation code for a user.
show      Show service status of this FortiGate.
```

```
sync      Synchronize users to FortiToken Cloud.
trial     Activate free trial.
update    Update VDOM list to FortiToken Cloud.

FG101ETK18002806 #  execute fortitoken-cloud new ?
<user name>    User name for new token.

FG101ETK18002806 #  execute fortitoken-cloud sync ?
<user type>    {Enter <return> | all | local | remote}

FG101ETK18002806 #  execute fortitoken-cloud trial ?
<Enter>

FG101ETK18002806 #  execute fortitoken-cloud update
<Enter>
```

The `# execute fortitoken-cloud show` command yields the FTC service status of the FortiGate, which can be one of the following:

- Licensed—The FortiGate has a valid FTC service license.
- Service ready—The FortiGate is ready for FTC service.
- Service balance—The remaining FTC account balance in terms of credits, for example, 11474.40 credits.

The "local" and "remote" options for the `execute fortitoken-cloud sync` command apply to FOS 6.4.0 only. They do not apply to FOS 6.2.3 which does not distinguish between local and remote users.

The `execute fortitoken-cloud update` command sends an updated list of VDOM names to FortiToken Cloud so that they can be assigned to realms on the FortiToken Cloud portal.

Configure admin users

Use the following commands to add an admin user account.

```
config system admin
    edit "admin1"
        set accprofile "super_admin"
        set vdom "root"
        set two-factor fortitoken-cloud
        set email-to "admin1@fortinet.com"
        set sms-phone "+14150123456"
        set password ENC SH2w9YIyuuKUMy+xmpxksgsJ9CfAMIjG8ZOVu8yGDk=
   next
end
```

Command	Description
`config system admin`	Starts the configuration of a system admin user.
`edit <username>`	Specify the admin username.
`set accprofile`	Specify the admin account profile name. For example, `super_admin`.
`set vdom`	Specify the VDOM name. For example, `root`.

Command	Description
`set two-factor`	Select an MFA method: • `disable` —No MFA. • `fortitoken`—FortiToken (FTK) or FortiToken Mobile (FTM). • `email`—Email. • `sms`—Simple message service. This option requires an SMS server and SMS phones. • `fortitoken-cloud`—FortiToken Cloud. **Note:** FortiToken Cloud is the default MFA method.
`set email-to`	Specify the email address to which FTC sends MFA activation codes.
`set sms-phone`	Specify the mobile phone number for receiving SMS messages.
`set password`	A system-generated password.

Configure local users

Use the following commands to add a local user.

```
config user local
   edit "user1"
      set type password
      set two-factor fortitoken-cloud
      set email-to "user1@fortinet.com"
      set sms-phone "+14080123456"
      set passwd-time 2019-06-14 16:38:12
      set passwd ENC EKhmlTBu1hmHUokESNTkNjxV8mBQ+AgyRPlInw==
   next
end
```

Command	Description
`config user local`	Starts the configuration of a local user.
`edit <username>`	Create the username.
`set type password`	Set type to password (authentication).
`set two-factor`	Select the MFA method: • `disable`—No MFA. • `fortitoken`—FortiToken (FTK) or FortiToken Mobile (FTM). • `email`—Email. • `sms`—Simple message service. **Note:** This option requires an SMS server and SMS phones. • `fortitoken-cloud`—FortiToken Cloud. **Note:** FTC is the default MFA method.
`set email-to <email address>`	Specify the email address to which the authentication code is sent.

Command	Description
`set sms-phone`	Set the mobile phone number for receiving SMS messages.
`set passwd-time`	Set the time the password is created.
`set passwd`	Set the password .

Configure local LDAP users for FTC service

Your can use the following commands to configure FortiGate local LDAP users to use FortiToken Cloud for MFA. In this case, verification of the LDAP user passwords verification is done through the LDAP server EngLDAP, but the other settings are the same as those of a regular local user.

```
config user local
   edit "ldap-user1"
      set type ldap
      set two-factor fortitoken-cloud
      set email-to "ldap-user1@fortinet.com"
      set sms-phone "+14080123456"
      set ldap-server "EngLDAP"
      set passwd ENC EKhmlTBu1hmHUokESNTkNjxV8mBQ+AgyRPlInw==
   next
end
```

Configure wildcard LDAP users for FTC service

Your can use the following commands to configure FortiGate wildcard LDAP users to use FortiToken Cloud for MFA.

```
   config user ldap
        edit "EngLDAP"
             set server "xx.xxx.xx.xx"
             set cnid "uid"
             set dn "dc=srv,dc=world"
             set type regular
             set two-factor fortitoken-cloud
             set username "cn=Manager,dc=srv,dc=world"
             set password ENC LWdyb+/k6e4TtSk070tODaCZAcbgEGKohA==
        next
   end
```

Wildcard LDAP users are those of a remote LDAP server user group, whose user configuration is unknown to FortiGate. For FortiGate to find them on the remote LDAP server, FortiOS requires that each user be configured with "uid" for "cnid" under "ou=People" in the dn and have the following attributes configured on the LDAP server:

- mail: user_email_address (e.g., mail: user1@abc.com)
- mobile: user_phone_number (e.g., mobile: +14080123456)

- In FortiOS, the "mail" attribute is mandatory and required of each user, while the "mobile" attribute is optional.
- FTC requires that the phone number be in the format of " +(country_code)(areacode_ number)".

During user configuration, the FortiGate-FTC user APIs are called for add-user, delete-user, modify-user with the following information in each API:

- Username
- VDOM name
- FortiGate serial number (SN)
- HA cluster membership information (if it's part of an HA configuration)

If an API requires the user ID, e.g., the delete-user API, FortiOS must use the GET API to retrieve the user ID from FTC.

Configure local RADIUS users for FTC service

Your can use the following commands to configure FortiGate local RADIUS users to use FortiToken Cloud for MFA. In this case, verification of the RADIUS user passwords verification is done through the RADIUS server EngRadius, but the other settings are the same as those of a regular local user.

```
config user local
         edit  "radius-user1"
               set type radius
               set type password
               set two-factor fortitoken-cloud
               set email-to "radius_user1@anycompany.com"
               set sms-phone "+14081234567"
                set radius-server  "EngRadius"
               set passwd-time 2020-02-18 16:00:59
               set passwd ENC M27kJaZ3I3VeHjQun8yqSHWvA
           next
 end
```

Diagnose FortiToken Cloud

Use the following commands to diagnose and troubleshoot FTC issues.

```
FG100D3G13804897 (global) # diag fortitoken-cloud {debug | ...}
debug       Enable or disable debug output.
server      Display FTC server IP address, port number, and https.
show        Display diagnostics information.
delete      Delete a user.
set-http    Set HTTP status return code for diagnostics only.
clear       Clear server connection settings for diagnostics.
sync        Synchronize user information with FortiToken Cloud.
```

Examples

```
FG100D3G13804897 (global) # diag fortitoken-cloud debug {enable | disable}

FG100D3G13804897 (global) # diag fortitoken-cloud server

FG100D3G13804897 (global) # diag fortitoken-cloud show {server | realm | users | user
<username> <VDOM>}

FG100D3G13804897 (global) # diag fortitoken-cloud delete <username>

FG100D3G13804897 (global) # diag fortitoken-cloud set-http <number>

FG100D3G13804897 (global) # diag fortitoken-cloud clear <Enter>

FG100D3G13804897 (global) # diag fortitoken-cloud sync { <Enter> | all | local | remote }
```

The `diag fortitoken-cloud sync` command requires you to specify the type of user to sync to FortiToken Cloud:

```
diagnose fortitoken-cloud sync ?
<user type> {Enter <return> | all | local | remote}
```

The "local" and "remote" options for the above command apply to FOS 6.4.0 only. They do not apply to FOS 6.2.3 which does not distinguish between local and remote users.

FortiToken Cloud GUI

- Only the global admin and sub-admin users can access the FortiToken Cloud portal. However, sub-admin users will not be able to see any data until the global admin has delegated some realms to them.
- The global admin is the first account from a customer organization that has logged in to the FTC portal. The master FortiCloud account of a customer organization is the de facto FTC global admin.

The FTC GUI has nine main pages, as listed in the main menu along the left-hand side of the GUI:

Menu	Description
Dashboard	Shows the number of auth clients, users, current month usage, and current balance (credits remaining) on your account. For more information. See Dashboard on page 37.
Administrators	(Accessible by the global admin only) enables the global admin to create sub-admin groups and assign realms to them. See Administrators on page 39.
Realms	Shows realms assigned to a sub-admin and provides tools for adding and deleting realms, viewing realm permission, and viewing or changing realm settings. See Realms on page 41.
Users	Shows information of all your FTC end users. For more information. See Users on page 44.
Auth Clients	Shows information about all your authentication clients which include the following types: • FortiProducts • Web Apps on page 50 • Devices (HA)
Tokens	Shows the tokens in two groups: • Mobile—Shows mobile tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See Mobile Tokens on page 53. • Hardware—Shows hardware tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See Hardware Tokens on page 54.
Usage	Shows daily usage data for the current month. See Usage on page 57.
Licenses	Shows all the licenses in your account. See Licenses on page 61. **Note:** This menu is visible to customers of the newly introduced time-based subscriptions only. Customers of credit-based subscriptions will not see this menu.
Settings	Opens the Settings page which has two variants:

Menu	Description
	• Global—Allows the global administrator to enable or disable "Auto-create Auth Client" and/or "Multi-reaml Mode" feature for all account under management. See Global on page 61. • Realm—Enables both the global admin and sub-admins to view and manage the settings of the selected realm. See Settings on page 61. • Templates—Opens the Templates page where you can add or delete templates.
Logs	Shows FTC logs which are categorized in two groups: • Authentication logs on page 71 • Management logs on page 73 See Logs on page 71.
Help	Opens the FortiToken Cloud Help page, which provides following resources and documentation: • **Contact Support** • **Purchasing Guide** • **Online Help** • **FAQs**
The bottom of the main menu shows the following information about the realm/account you are looking at:	
Users	Shows the number of users in your realm or account. See the note for Account below.
Auth Clients	Shows the number of auth clients in your realm or account. See the note for Account below.
Account	Shows your account number and the name of your company. **Note:** • If you have more than one FTC account, you can click the down arrow to view all your accounts in the drop-down list. You can then select any of the other accounts to switch to it. • For a global admin, this part of the page shows the consolidated user and auth client counts of all the sub-admin accounts under administration; for a sub-admin, it shows the user and auth client counts of the delegated sub-admin account only.

Launch FortiToken Cloud

The FortiToken Cloud (FTC) portal is a powerful, yet easy to use tool for administrators to manage their FTC assets and end users. Once you have your FTC account created, you can log on to the portal anywhere in the world using a supported web browser and your login credentials.

Log in as a regular FTC user

Admin users created on FortiProducts (e.g., FortiGate, FortiAuthenticator, etc.) are regular FTC users.

To log in as a regular FTC user:

1. Start your web browser.
2. Point to https://ftc.fortinet.com, and press **Enter** on your keyboard.
3. In the upper-right corner of the FortiToken Cloud landing page, click **LOGIN.**
4. On the FTC login page, enter your FTC email address and password.
   Note: The email address used when creating your FTC account is your FTC username or account name. Be sure to use the same email address when logging into the FTC portal.
5. Click **LOGIN.**

Log in as an IAM user

The Identity and Access Management (IAM) portal is an advanced feature of FortiCloud, which is accessible only to customers with FortiCloud Premium Subscription.

An IAM user is one created by the super-admin of a premium FortiCloud account. IAM users of FTC can only assume the role of a sub-admin on the FTC portal.

To log in as an IAM user of FTC:

1. Start your web browser.
2. Point to https://ftc.fortinet.com, and press **Enter** on your keyboard.
3. In the upper-right corner of the FortiToken Cloud landing page, click **LOGIN.**
4. At the bottom of the FTC login page, click **Sign in as IAM user (BETA).**
5. Enter your Account ID/Alias, username (email address), and password.
6. Click **LOGIN.**

FortiCloud

As part of FortiCloud (the umbrella of Fortinet's Cloud service offerings), the top of the FortiToken Cloud portal provides a one-stop access to all services and resources available on FortiCloud as well as tools for managing your FortiCloud account, as shown in the screen capture below.

The FortiCloud Logo

The FortiCloud logo has two variants: one with the word "PREMIUM" and the other without it. The FortiCloud logo that you see on the FortiCloud portal reflects the level of FortiCloud service you have subscribed: if you are a premium FortiCloud customer, the word "PREMIUM" always appears under the logo; if you are basic FortiCloud customer, you will see the logo only. A premium FortiCloud account requires a premium FortiCloud license and entitles your to more features and services. If you are interested in getting FortiCloud premium services, contact your Fortinet sales representative for more information.

Your FortiCloud account

As shown in the image above, the upper-right corner of the FTC portal shows your FortiCloud account ID, which typically is the email address that you've registered on FortiCloud (FC). Clicking your account ID or the down arrow next to it opens a drop-down menu with a list of options for managing your FortiCloud account, as described in the following table.

Tools for managing your FortiCloud account

Menu	Description
My Account	Opens your FortiCloud Account page with the following tools: • **Account Profile**—View and edit your account profile. • **Change Account ID (Email)**—Change your account ID. • **Manage User**—Add users to your account.
User Information (Applicable to IAM users only)	Opens the User Information page with the following tools: • **User Profile**—View and edit your user profile. • **Change Email**—Change your email address. • **Permissions**—Manage IAM permissions.
Security Credentials	Opens the FortiCloud page with the following tools: • **Change Password**—Change/update your account password. • **2FA Settings**—Manage your account's two-factor authentication settings. • **Subscriptions**—Manage your subscriptions to (1) Weekly FortiGuard update and/or (2) Quarterly product update (Introduction & EOS).
Subscriptions	Opens the FortiCloud page where you can manage your subscriptions to (1) Weekly FortiGuard update and/or (2) Quarterly product update (Introduction & EOS).
Logout	Logs out of FortiCloud (including FortiToken Cloud).

Services

This Services tab opens a drop-down menu which provides easy access to all Cloud services that Fortinet offers.

Menu	Description
IAM	Click this link to navigate to the IAM portal where you can take advantage of FortiCloud IAM service. **Note:** This menu is accessible to FortiCloud Premium customers only. For more information, contact your Fortinet sales representative or an authorized Fortinet reseller in your region.
Asset Management	Click this link or the icon to navigate to the **FortiCloud>Asset Management** page, where you can • Register your Fortinet products • View your Fortinet products and their status • Renew your product or service subscriptions • View your account services
Cloud Management	Click any of the following icons (links) to manage the Fortinet product over FortiCloud.
FortiGate	FortiGate Cloud.
FortiExtender	FortiExtender Cloud
FortiAnalyzer	FortiAnalyzer Cloud
FortiSwitch	FortiSwitch Cloud
FortiAP	FortiAP Cloud
FortiManager	FortiManager Cloud
FortiClient	FortiClient Cloud
Cloud Services	Click any of the icons (links) to launch the FortiCloud serice. **Note:** You must have a valid license to access any of the following Cloud services.
FortiPresence	FortiPresence Cloud
FortiCASB	FortiCASB
FortiToken	FortiToken Cloud
FortiMail	FortiMail Cloud
FortiPhish	FortiPhish Cloud
FortiInsight	FortiInsight Cloud
FortiGSLB	FortiGSLB
FortiConverter	FortiConverter Cloud
FortiVoice (Beta)	FortiVoice Cloud
FortiPenTest	FortiPenTest Cloud
FortiSandbox	FortiSandbox Cloud

Menu	Description
FortiWeb	FortiWeb Cloud
OCVPN-Portal	OCVPN-Portal Cloud
FortiCWP	FortiCWP Cloud
FortiIPAM	FortiIPAM Cloud

Support

This tab opens a drop-down menu which provides easy access to Fortinet product and support:

Menu	Description
DOWNLOADS	Click any of the following the link to download. • Firmware Download • Service Updates • HQIP Images • Firmware Image Checksum • VM Images
RESOURCE	Click this tab to open the FortiCloud>Resources page, where enables you to access a slew of resources to Fortinet products and services.
FORTICARE	Click one of the following links for the support service you need: • Create a Ticket • Manage Active Tickets • Manage Tickets • Ticket Survey • Contact Support • Technical Web Chat

Dashboard

By default, the Dashboard page opens upon log-in. You can also navigate to this page from any of the other pages by clicking **Dashboard** on the main menu.

Starting with its 21.2.d release, FortiToken Cloud has introduced a time-based annual subscription model which will eventually replace the current credit-based subscription.

If you are a customer of the credit-based subscription, you are still able to continue using your existing subscription until it expires. You can then continue your FTC service byIf you arto switch to the new time-based subscription

The top of the Dashboard page shows the following data about your account:

- **Days to Expire**—The number of days remaining before your current FTC subscription expires. (*This applies to time-based subscriptions only.)*
- **Current Month Usage**—The number of credits that your account has consumed so far for the current month. (*This applies to credit-based subscriptions only.)*
  Note: Clicking the numeric value on the tab opens the Usage on page 57 page.
- **Current Balance**—The number of credits that currently remains on your account. *(This applies to credit-based subscriptions only.)*
  Note: Clicking the numeric value takes you to the FortiCloud Customer Service & Support website, where you can purchase more FTC credits to add to your account, provided that you've already purchased a new license (more credits).

The second row of the Dashboard shows the following data in your account:

- **FortiProducts**—The number of Fortinet products (e.g., FortiGate, FortiGate VM, and FortiAuthenticator, etc.) that function as authentication clients of FortiToken Cloud in your account.
  Note: There is no limit to the number of Fortinet products that your account can accommodate. Clicking the numeric value on the tab opens the FortiProducts on page 48 page.
- **Web Apps/Max Web Apps**—The number of Web apps currently function as authentication clients in your account and the maximum number of Web apps that your account can support.
  Note: Clicking the numeric value on the tab opens the FortiProducts on page 48 page.
- **Users/Max Users**—The number of users currently in your account and the maximum number of users that your account can support.
  Note: Clicking the numeric values on the tab opens the Users on page 44 page.
- **Realms/Max Realms**—The number of realms currently created in your account and the maximum number of realms that your account can support.
  Note: Clicking the numeric values on the tab opens the Realms on page 41 page.
- **Remaining SMS**—The number of SMS messages available for use. (*This applies to credit-based subscriptions only.)*
  Note: The time-based subscription allows for SMS messages in the amount of 100 multiplied by the total number of end users your license can support for the year.

Last 10 authentication attempts in 30 days

The lower part of the Dashboard is a table, which shows the 10 most recent authentication attempts over the past 30 days. Each row represents an event.

Column	Description
Timestamp	The date and time of the authentication event. **Note:** FTC captures the time of the event in UTC time, and then converts it to the client browser's local time which is the time shown in the timestamp.
Username	The username of the FTC user who requested authentication.
Auth Client	The authentication client that made the request.
Action	Type of authentication action.
Result	The outcome of an authentication request, which can be either of the following: • Success

Column	Description
	• Failed
Message	A system-generated message about the authentication request.

FTC extracts the aforementioned data from its Authentication logs. You can sort the logs by clicking the column headers (except for the Result column) of the table.

Administrators

Only admin users can access the FortiToken Cloud (FTC) portal. There are two types of administrator accounts: the global administrator (global_admin) and sub-administators (sub_admin). Anyone from your organization with a valid user account on FortiCloud (FC) can log in to the FTC portal using his or her FC username and password. By default, the FC account holder from your organization who logs in to the FTC portal first automatically becomes the global administrator of your FTC account. The master FC account holder of your organization is the de facto global administrator of your FTC account.

The Administrators menu is accessible to the global admin user only. Sub-admin users will not be able to see this menu.

The Administrators page provides the tools for the global admin to create and manage sub-admin groups. It also shows all the sub-admin groups that the global admin has created.

You (the global admin) can access the Administrators page by click **Administrators** on the main menu.

The following table highlights the information of sub-admin group configuration shown on the Administrators page.

Column Header	Description
Name	The name of an admin group.
Description	The description of a group. Not required.
Level	The level of administration of a group: • global_admin—The highest level of administration. **Note:**The global_admin group is the default admin account, and cannot be deleted. • sub_admin—Any admin group that the global admin has added. Users in a sub-admin group are all sub-admin users. They can only access the realms assigned to their group, and manage the auth clients in those realms and the users on those auth clients .
Member Count	The number of sub-admins in a group.

Column Header	Description
	Note: The numeric value indicates the number of users (sub-admins) in a given admin group. Clicking the value opens a pop-up window that shows the usernames, email addresses, and user IDs of those users.
Tool bar	The tool bar slides in from the right end of the row the moment you mouse over an entry in the table. It shows the following tools: • **Edit**—Edits the administrator group. • **Delete**—Deletes the administrator group.

The following paragraphs discuss the tasks the global admin can do.

Create a sub-admin group

To create a sub-admin group:

1. On the Administrators page, click **Add Admin Group.**
   The Add New Admin Group dialog opens.
2. Specify the group name.
   Note: The group name can only contain lower-case letters from "a" to "z" and/or numeric values from "0" to "9", and underscore "_" and/or hyphen "-". It must be between 3 and 36 characters in length.
3. (Optional) Enter a brief description of the group.
4. Click **OK.**
   Note: The name of the sub-admin group you've just created appears in the Add Admin Group table. Your next steps are to add sub-admin users and assign realms to the group, as discussed in the following sections.

Add users to a group

You must have sub-admin users already in your account in order to add them to a sub-admin group.

To add sub-admins to a admin group:

1. In the Add Admin Group table, click the name of the group of interest to open the Edit Admin Group dialog.
2. To add admins to the group, click **Add Admin** to open the Manage Admins dialog.
3. Under Admins not in Group, select the admins to be added, click **Add To**, and click **Close** to close the dialog.

Add realms to a group

Once you have added sub-admins to a group, you need to assign realms to the group to enable the sub-admins to manage the auth clients and FTC end users in those realms.

- You must have realms created first before assigning them to a sun-admin group. See Realms on page 41.
- Sub-admin users cannot see any data on the FTC portal until/unless the global admin has assigned realms to their group.

To add realms to a group:

1. Click **Add Realm.**
   The Manage Realm dialog opens.
2. Under Not Managed by Group, select the realm(s) of interest and click **Add To**, and click **Close** to close the dialog.

Edit admin group configuration

You can edit an admin group by changing its name and description, and/or by adding or deleting of sub-admins and realms in the group.

To edit an admin group:

1. On the Administrators page, identify the group of interest and mouse over it.
2. From the slide-in tool bar, click the **Edit** button to open the Edit Admin Group dialog.
3. To change the group name, highlight the **Group Name** and type a new name over it.
4. To modify the description of the group, highlight the **Group Description**, and type a new one over it.
5. To add more sub-admins to the group, click **Add Admin.** See Create a sub-admin group on page 40.
6. To delete a sub-admin, identify the admin and click **x (Delete)**.
7. To add more realms to the group, click **Add Realm.** See Add realms to a group on page 40.
8. To delete a realm, identify the realm and click **x (Delete).**
9. Click **Close.**

Delete a sub-admin group

The global admin can delete any sub-admin group, except the default 'global_admin" group. Also, when deleting a sub-admin group with sub-admins in it, you must delete the sub-admin users from the group first in order to delete the group. See Edit admin group configuration on page 41.

To delete a sub-admin group:

1. On the Administrators page, identify the admin group of interest, and mouse over it.
2. From the slide-in tool bar, click the **Delete** button.

Realms

You can open the Realms page by click **Realms** on the main menu.

The Realms page shows information about the realms in your account. If you are a global admin, you will see all realms across all sub-admin accounts under your administration; if you are a sub-admin user, you will see the realms assigned to your sub-admin group only.

Starting with the 21.2.d release, the following three tabs *visible to customers of time-based subscriptions only* have been added to the top of the Realms page:

- **Current Realm**—The number of the realms currently created in your account.
- **Max Realms**—The maximum number of realms that your subscription can support.
- **Remaining User Quota**—The number of end user quota left in your account.

The following table highlights the information on the Realms page.

Column header	Description
Check box	Enables you to select a realm. **Note:** The **Delete** button above the table becomes activated when a realm is selected. You can click the button to delete the realm. Alternatively, you can delete a realm by clicking the corresponding **Delete** icon in the Actions column. For more information, see Delete a realm on page 43.
Name	The name of a realm.
Description	A brief description about the realm that the global admin added when creating the realm.
Client Count	The number of auth clients assigned to a realm.
Tool bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It has the following tools: • **Edit Realm**—Edits the name and/or description of the selected realm. • **Show Permission**—Opens a dialog which shows the sub-admin groups that have access to the realm. You can also remove sub-admin groups from the access list by deleting them. • **Settings**—Opens the Settings page which shows the settings of the realm. See Settings on page 61. • **Delete**—Deletes the realm. See Delete a realm on page 43.

Create a custom realm

FTC comes with a default realm. It also enables you to create your custom realms.

To create a realm:

1. On the Realms page, click **Add Realm.**
   The Add New Realm dialog opens.
2. Specify a realm name.
3. (Optional) Enter a brief description.
4. Click **OK.**

Edit a realm

You can edit a realm by changing its name.

To edit a realm:

1. On the Realms page, identify the realm of interest and mouse over it.
2. In the slide-in tool bar, click the **Edit Realm** button to open the Edit Realm dialog.
3. Make the desired changes.
4. Click **OK.**

View realm permission

When the global admin user creates a sub-admin group, he or she adds the sub-admins to the group and assign realms to them. As a result, all sub-admins in the group have access to the realms assigned to that group. See Administrators on page 39 for more information.

The Realms page provides a tool to enable you view the sub-admin groups who have access to a realm.

To view the access list of a realm:

1. On the Realms page, identify the realm of interest and mouse over it.
2. In the slide-in tool bar, click the **Show Permission** button.
3. The Access List for Realm dialog opens, showing all the sub-admin groups who have access to the realm.

To close the Access list for realm dialog, click the **Close** button at the bottom of it or anywhere outside the dialog.

Remove sub-admin groups from a realm access list

To remove sub-admin groups from the access list of a realm:

1. On the Realms page, identify the realm of interest.
2. In the Actions column, click the **Show Permission** button to open the Access list for realm dialog.
3. Identify the sub-admin group of interest, and click the corresponding **x (Delete)** icon.

Delete a realm

To delete a realm:

1. On the Realms page, identify the realm of interest and mouse over it.
2. In the slide-in tool bar, click the **Delete** button.

- You cannot delete the default realm.
- If a realm has auth clients assigned to it, you must delete the auth clients from the realm before deleting the realm.

View realm settings

The Realms page also provides a tool for you to look up the settings of a realm. Once you have open the Settings page for that realm, you can also edit the settings of the realm from there as well.

To view the settings of a realm:

1. On the Realms page, identify the realm of interest and mouse over it.
2. In the slide-in tool bar, click the **Settings** icon.
3. The Realm Settings page opens. The upper-right corner of the page shows the name of the realm, and the page shows the settings of the realm,
4. You can make any changes to the settings if you like. See Settings on page 61 for more information.
5. To go back to the Realms page, click the **Back** button at the bottom of the Realm Settings page.

Users

You can open the Users page by clicking **Users** on the main menu.

The term "users" refers to end users of FortiToken Cloud. The Users page displays the following information about FTC end users in your account.

Column	Description
Checkbox	This checkbox only applies to users who use FTM for MFA. You can use the checkbox to select a user, and then click the **NEW FTM TOKEN** button to request a new FTM token for the user. See Get a new token.
Username	The username of an FTC end user.
Status	The status of a user, which can be a combination of any of the following: •  **(active)**—The user is enabled. **Note:** By default, all new users are enabled to use FTC for MFA. The FTC administrator can click this button to quickly deactivate a user when necessary. See below. •  **(disabled)**—This button enables the administrator to temporarily stopped the user from using FTC. **Note:** If a user is disabled, FTC cannot provide MFA for the user because it will deny all log-in requests from the user. It must be noted that disabling a user only stops the user from using FTC, but does not remove the user from your FTC account. FTC will continue charging you credits for the user until

Column	Description
	you remove the user from your account. An admin user can click this button to re-enable a disabled user. •  **(locked)**—The user is locked out. **Note:** FTC locks a user out when he or she has exceeded the specified maximum number of log-in attempts allowed. See Settings on page 61. •  **(unlocked)**—The user is unlocked. **Note:** FTC automatically unlocks users based on their lockout settings. The FTC admin user can also manually unlock a locked user by clicking the  **(locked)** button. •  **(pending)**—A token assigned to the user has not been activated yet. •  **(expired)**—The user's token activation code has expired. •  **(bypass)**—The user is allowed to bypass MFA. •  **(no bypass)**—The user is not allowed to bypass MFA. **Note:** The admin user can enable MFA bypass on a user from here only if **Enable Bypass** is enabled on the Settings page. See Settings on page 61. Otherwise, when you click the  **(no bypass)** icon, a tool tip will appear asking you to turn on **Enable Bypass** on the Settings page first.
MFA Method	The user's MFA method, which can be one of the following: • FTM (soft token) • Email • SMS • FTK (FortiToken, a hardware token)
Token SN	The serial number of a token. **Note:** A serial number that starts with "FTC" indicates that it is a FortiToken Cloud token, whereas a serial number that starts with "FTK" indicates that it is a FortiToken.
Notification Method	The method by which FTC sends FTM token activation/transfer notifications to an end user, which can be either of the following: • Email—FTC sends FTM token activation/transfer notification to the user's email address. • SMS—FTC sends FTM token activation/transfer notification by SMS to the user's mobile phone. **Note:** If the user's notification method is set to SMS, you must make sure that the mobile phone number in the system is valid, and that you have enough credits in your account to send OTPs by SMS. For more information, see Settings on page 61.
Email	A user's email address. **Note:** An admin user is able to edit users' email addresses.

Column	Description
Mobile Phone	The user's mobile phone number, if available. **Note:** The phone number is in the format of "+ Country Code Area Code Phone Number", e.g., +1 4082221234. An admin use can edit an end user's mobile phone numbers.
Auth Client Count	The number of auth clients.
Create Date	The date on which the user was added.
Tool Bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It has an **Edit** tool button that enables you to make changes to the user's settings.

Get a new FTM token

You can request a new FTM token for an end user only if the user's current MFA method is FTM.

To get a new FTM token for an end user,

1. On the Users page, select the user of interest.
2. On top of the table, click **NEW FTM TOKEN**.
3. Follow the prompts onscreen to request a new FTM token for the user.

Auto-assign FTKs to selected users

The **Auto-assign FTK** button enables FTC to automatically assign available FTKs to selected users.

To let FTC automatically assign FTKs to end users,

1. Select the users of interest.
2. Click the **Auto-assign FTK** button.

Add user aliases

On top of the Users page is the Add User Alias button, which becomes Auto-alias by Email is enabled in Settings page of a realm. It enables you to select users of interest on the Users page, and group them together using an alias.

To add an alias:

1. Select the users of interest.
2. Click Add User Alias.
3. Follow the prompts onscreen to create an alias.

The alias now appears in the table in bold font.

Hide/Show full FortiAuthenticator username

By default, the usernames of FTC users created on FortiAuthenticator (FAC) show up with prefixed and suffixed characters in corner brackets on the FTC GUI. This is due to the fact that FAC differentiates the same username populated by multiple user sources to FAC. The Users page provides an option to let you toggle between showing and hiding those extra characters.

To hide/show the extra characters in the usernames of users added on FAC, click **Hide/Show Full FAC Username**.

View a user's auth clients

1. On the Users page, identify the user of interest.
2. Click the numeric value in the Auth Client Count column.
   A window opens, showing the auth client(s) on which the user is on.
3. Click **Close** to close the window.

Edit a user

You can edit a user by making changes to the user's settings.

To edit a user:

1. On the Users page, identify the user of interest, and mouse over it.
   The Edit User dialog appears.
2. Make the desired changes as described in the following table, and click **Apply** when done.

Field	Description
Auth Method	Click the down arrow, and select a desired authentication method from the drop-down list menu: • FTM • Email • SMS (**Note:** You must provide a valid mobile phone number to use SMS authentication.) • FTK
Notification Method	**Note:** This field applies only when you set Auth Method to FTM. See above.
Token SN	*Read only*.
Email	Make the desired changes to the email address.
Mobile Phone	Click the down arrow to select the country code, and then enter a valid phone number. **Note:** This field is required when Auth Method and/or Notification Method is set to SMS, as stated above.

Changes that you've made here become effective when you click **Apply**. A error message will pop up if the system encounter a when validating the changes. In that case, you must correct the error and try to apply the changes again.

FortiProducts

The FortiProducts page shows information about all Fortinet products that function as auth clients in your FTC account. You can open the FortiProducts page by clicking **Auth Clients>FortiProducts** on the main menu.

The following table highlights the information on the FortiProducts page.

Column	Description
Checkbox	Unchecked by default. If checked, the auth client becomes selected and the **DELETE** button is enabled. You can then click the **DELETE** button to remove the selected auth client. For more information, see Delete an auth client on page 49. **Note:** You can select all the auth clients at once by checking the checkbox in the column header.
Alias	The alias of an auth client.
Name	The name of an auth client.
Type	The type of auth client, which can be any of the following: • FortiAuthenticator • FortiGate • FortiGateVM • FortiSandbox **Note:** FTC assigns the auth client type based on the product serial number and model.
Count	The number of FTC end users on an auth client. **Note:** Clicking the numeric value opens a dialog which shows the list of FTC end users on the auth client, along with some basic information about each of the users.
Realm Name	The name of the realm to which an auth client is assigned.
Tool Bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It provides the following tools: • **Edit**—Change certain settings of auth client. • **Details**—Shows some detailed information of the auth client. • **Delete**—Deletes the auth client.

- FTC is able to detect an FortiGate device as soon as the FTC API activates it for FTC, and populates the Auth Clients page with information of the device.
- You can sort the table by clicking any of the column headers.

Assign an auth client to a realm

An auth client must be assigned to a realm. Otherwise, you cannot add or sync users from the auth client. For more information, see Realms on page 41.

The Auth Clients page enables you to change the realm assignment of your auth clients.

To assign an auth client to another realm:

1. On the main menu, click **Auth Clients>FortiProducts** to open the FortiProducts page.
2. In the table, locate the auth client of interest.
3. Click in the Realm Name column (which should show the word "None", meaning the auth client has not been assigned to any realm yet).
   A drop-down list menu appears, showing all the realms you can choose from.
4. Select a realm of interest. A message pops up.
5. Be sure to read the message.
6. Click **Yes.**
   The name of the newly selected realm now appears in that column, meaning that the auth client now is assigned to this realm.

Edit an auth client

To edit an auth client:

1. On the FortiProducts page, identify the auth client of interest, and mouse over it.
   The tool bar slides in from the right end of the row.
2. Click **Edit.**
   The Edit Client dialog opens.
3. Make the desired changes, and click **Ok.**

Viewing additional information about an auth client

To view additional information about an auth client:

1. On the FortiProducts page, identify the auth client of interest, and mouse over it.
   The tool bar slides in from the right end of the row.
2. Click **Details**.
   The Detailed Information for Auth Client dialog opens, showing some more information about the auth client.

Delete an auth client

Deleting an auth client removes all FTC end users from it unless a user is also on another auth client.

To delete an auth client:

1. On the **Auth Clients>FortiProducts** page, identify the auth client of interest, and mouse over it.
   The tool bar slides in from the right end of the row.
2. Click **Delete.**
   The Delete Auth Clients alert pops up.
3. Be sure to read the message.
4. Click **Yes.**

Web Apps

The Web Apps page enables you to manage web applications as FTC auth clients that are Web apps. You can open the Web Apps page by clicking Auth Clients>Web Apps on the main menu.

The table below highlights the information on the Web Apps page.

Parameter	Description
Name	The name of an auth client.
Client ID	A unique ID that FTC has generated for the auth client. **Note:** The Client ID cannot be edited.
Count	The number of FTC end users on the auth client.
Realm Name	The name of the realm to which the auth client is assigned.
Secret	Part of the secret. **Note:** Clicking the button regenerates the secret for the auth client.
Last Update	The time when the auth client was last updated.
Tool Bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It provides the following tools: • **Edit**—Edits the settings of a web app as auth client • **Delete**—Deletes the web app as auth client.

Add an auth client

You can create a new auth client for your Web app using the Auth Clients>Web Apps page. When a new auth client is added, FortiToken Cloud assigns it the default name "MyAuthClient" which can be edited. If you add more auth clients of the same type, FortiToken Cloud will append a sequence number starting with "1" to the subsequent auth client names, e.g., MyAuthClient1, MyAuthClient2, and so on.

You need to select a realm from the list of realms in your account and assigns the new auth client to it. Otherwise, the auth client will be assigned to the default realm. You must assign the auth client to a custom realm in order to add end users to it.

When creating an auth client, FortiToken Cloud will generate a unique, non-editable ID. It will also generate the API credentials which the auth client needs when accessing the FortiToken Cloud API server. With this release, use of the API is limited to licensed accounts only; it is not available for free trial accounts.

To create an auth client for your web app:

1. In the upper-left corner of the Auth Clients>Web Apps page, click **Add Auth Client** to open the Add New Auth Client dialog.
2. Type a unique name over the default name.
3. Select a realm, or leave it to the default.
4. Click **Add.** A window pops up, showing the information of the newly added auth client, including its ID and Secret.
5. Click **OK**. The auth client is now added to the Auth Client>Web Apps page.

Regenerate the API credentials

To regenerate the API credentials:

1. On the Auth Clients>Web Apps page, locate the auth client.
2. In the Secret column, click the **regenerate secret** button.
3. In the Regenerate Secret dialog, select either of the following:
   - **Display on portal**—Shows the secret on the GUI.
   - **Send to email**—Sends the secret to the email address you have specified. You must open the email to retrieve it. The email message contains instructions on how to use the secret.
4. Click **OK.**

Edit a web app

To edit a web app as auth client:

1. On the **Auth Clients>Web Apps** page, locate the web app of interest and mouse over it. The tool bar slides in from the right end of the row.
2. Click **Edit.**
3. Make the desired changes, and click **OK.**

Delete a web app

To delete a web app:

1. On the **Auth Clients>Web Apps** page, locate the web app of interest and mouse over it. The tool bar slides in from the right end of the row.
2. Click **Delete.**

Devices (HA)

The Devices page enables you to view and manage HA clusters using authentication clients that use FTC for MFA. You can access the Devices page by clicking **Auth Clients>Devices** on the main menu.

The Devices page has two parts (left and right). On the left is the Standalone Devices panel which shows authentication devices that are standalone (not part of any HA cluster); on the right is the Clusters panel which shows the HA clusters and the authentication clients in each of the clusters.

Search for a standalone device

On the top of the Standalone Devices panel is a Search by SN tool, which enables you to search for standalone devices by serial number (SN). It comes in handy when you are trying to locate a standalone device and add it to an existing cluster on the right.

- The search tool applies to standalone devices only.
- You can search for a device by any part of its serial number (SN). However, the more specific your entry, the more accurate your search result.

To search for a standalone device:

1. In the upper-left corner of the Standalone panel, click **Search by SN**.
2. Type in any part of the serial number of device of interest.
3. Press the **Enter** key on your keyboard.

The device or devices that match your entry now show up in the table below.

Add devices to cluster

You can add any device in the Standalone Devices panel to any cluster in the Clusters panel. Once a standalone device is added to a cluster, it becomes part of the cluster and will not show up in the Standalone Devices panel.

Before adding a standalone device to a cluster, you must make sure that the change you are going to make to the cluster is consistent with its actual configuration.

To add a standalone device to a cluster:

1. In the Clusters panel, locate the cluster of interest.
2. In the Standalone Devices panel, locate the standalone device of interest. See Search for a standalone device on page 52.
3. Click the device, and drag and drop it to the cluster on the right.
4. When the Device Management alert pops up , be sure to read the message, and click **OK** to continue.

The device is now added to the cluster.

Remove devices from a cluster

You can remove a device from any cluster in the Clusters panel. Once a standalone device is removed from a cluster, it becomes standalone and shows up in the Standalone Devices panel.

Before removing a device from a cluster, you must make sure that the change you are going to make to the cluster is consistent with its actual configuration.

To remove a device to a cluster:

1. In the Clusters panel, locate the cluster of interest.
2. Click the down arrow to view the devices in the cluster.
3. Highlight the device of interest, and click Moved Out. The Device Management dialog opens.
4. Read the message, and click **OK** to continue.

The device is now removed from the cluster, and appears in the Standalone Devices panel.

Move a device between clusters

You can also move devices between clusters in the Clusters panel.

Before moving a device from one cluster to another, you must make sure that the change you are going to make to the clusters is consistent with the actual configurations of your network.

To move a device from one cluster to another:

1. In the Clusters panel, locate the clusters of interest.
2. In one of the clusters, identify the device you want to relocate.
3. Drag and drop it to the other cluster. The Device Management dialog opens.
4. Be sure to read the message, and click **OK** to continue.

The device now is removed from one cluster and added to the other cluster.

Mobile Tokens

The term "mobile" refers to FortiToken Mobile (FTM) for mobile devices. The **Soft Tokens** page is read-only and shows all FTMs used by end users in your FTC account.

You can access the **Mobile** page by clicking **Tokens**>**Mobile** on the main menu. The following table describes the information on the **Tokens**>**Mobile** page.

Column	Description
Serial Number	The serial number of an FTM.
Username	The username of the FTC user to whom an FTM has been assigned.
Realm	The realm to which the user of the FTM has been assigned. **Note:** The field shows "default" if the auth clients associated with the user has not been assigned to any realm.
Platform	The mobile platform of a soft token, which can be either of the following: • Android • iOS
Algorithm	The algorithm of time-based one-time password authentication used on a soft token supported by FTC: • TOTP
Registration ID	The ID under which a soft token is registered.

Hardware Tokens

The term "hardware" refers to FortiToken (FTK), which is the only hardware token that FTC supports in the current release. The **Hardware** page shows all FortiTokens used by end users in your FTC account. It also offers tools for adding and deleting FTKs.

You can access the **Hardware** page by clicking **Tokens** on the main menu. The following table describes the information on the **Hard Tokens** page.

Column	Description
Checkbox	Unchecked by default. If checked, the corresponding hard token becomes selected and the **Delete** button enabled. You can then click the button to delete that hard token. For more information, see Delete hard tokens on page 56. **Note:** You can also check the checkbox in the column header to select all the hard tokens and delete them all at once.
Serial Number	The serial number of a FortiToken.
Model	The models of supported hard tokens, which can be one of the following: • FTK200 • FTK220 • Other
Algorithm	The algorithm of time-based one-time password authentication used on the hard token. • TOTP (default)
Username	The username of the FTC user to whom a FortiToken has been assigned. **Note:** If this field is blank, it means that the FortiToken has not been assigned to any user yet.

Column	Description
Last Update	The date and time of the most recent update of the hard token.

The **Import Tokens** button enables you to add hard tokens to your account. You can either manually add serial numbers of hard tokens one by one or batch-upload them by importing a .csv file which contains the serial numbers of the hard tokens you want to add to your account. See Batch-upload hard tokens on page 55.

FortiToken Cloud only supports FTK200 and FTK220 hardware tokens. The FTK200CD (with the serial number prefix FTK211) is NOT supported.

Add hard tokens manually

If FTK is set as the default MFA method in the settings of a realm, you can select users on the Users page and let FTC automatically assign FTKs to them by clicking the **Auto-assign FTK** button. See Users on page 44.

To add hard tokens manually:

1. On the Hard Tokens page, click the **Import Tokens** button.
   The **Import Hard Tokens** dialog opens.
2. Click where it says "**Token SN***", and enter the serial number of a hard token.
3. Click the **Add New Token** button (if you want to add more than one hard tokens).
4. Repeat Steps 2 through 3 above to add as many hard tokens as you have available.
5. Click **OK.**
   The **Import Hard Token** dialog closes, and a message pops up in the upper-right corner of the Hard Tokens page, informing you how many hard tokens have been successfully added and how many have failed (if any) to be added. You can either click **OK** to dismiss the message, or wait for a few seconds to let it automatically close itself. The serial numbers of the hard tokens that are successfully added now appear on the **Hard Tokens** page.

Batch-upload hard tokens

You can also batch-upload all the hard tokens you want to add at once if you have access to a .csv file that contains the serial numbers of the hard tokens to be added.

Be sure to have the .csv file ready before starting the following procedures.

To batch-upload hard tokens:

1. On the **Tokens** > **Hardware** page, click the **Import Tokens** button.
   The **Import Hard Tokens** dialog opens.
2. In the upper-right corner of the dialog, click the **Upload CSV file** button.
   The typical Windows **File Upload** dialog opens.
3. Locate the .csv file in your file system, and click **Open.**
   The Windows Upload File dialog closes, and all the serial numbers of the hard tokens in the .csv file are now added to the Import Hard Tokens dialog.
4. Click **OK.**
   The **Import Hard Token** dialog closes, and a message pops up in the upper-right corner of the **Hard Tokens** page, informing you how many hard tokens have been successfully added and how many have failed (if any) to be added. You can either click **OK** to dismiss the message, or wait for it to automatically close itself in a few seconds. The serial numbers of the hard tokens that are successfully added now appear on the **Hardware** page.

Assign a hard token to a user

A hardware token shown on the Hard Tokens page without a username means that it is free or has not been assigned to any user yet. You can assign it to any user in your FTC account.

To assign a free hard token to a user:

1. On the main menu, click **Users.**
   The **Users** page opens. See Users on page 44.
2. Identify the user of interest and click the **MFA Method** column.
   A pop-up list appears showing all the MFA methods that FTC supports.
3. Select **FTK.**

Delete hard tokens

The Hard Tokens page provides tools to delete hard tokens that are no longer needed. You can delete one, multiple, or all the hardware tokens at once.

Only free (unassigned) FTK tokens can be deleted.

To delete individual hardware tokens:

1. Identify the hard token(s).
2. Select the corresponding checkbox(es).
3. Click the **Delete**button.
   The Delete Hard Tokens warning message appears.
4. Click **Yes.**

To delete all hardware tokens:

1. Select the checkbox in the header of the checkbox column.
2. Click the **Delete Hard Tokens** button.
   The Delete Hard Tokens warning message appears.
3. Click **Yes.**

Usage

The Usage page enables you to view your daily FTC usage data for a given day or month. You can open the Usage page by clicking the **Usage** tab on the main menu.

View usage data

The usage graph shows the number of credits consumed by user and by SMS, respectively. If you want to view usage by user only, click SMS to turn SMS usage data off, and vice verse.

1. Click in the **Realm** drop-down, and select a realm of interest.
2. On top of the Usage page, select either **Daily** or **Monthly.**
3. Click in the **From** box, and set the start date or month of the year.
4. Click in the **To** box, and set the end date or month of the year.
5. Click **Filter.**
   The usage bar graph appears. Each bar represents a month within the time window that you have specified.
6. If you've select Daily (in Step 2 above), you click the **Usage Type** drop-down menu and then select either **Count** or **Credit.**
   Note: The **Usage Type** drop-down menu applies only to customers who have converted to a time-based subscription after their credit-based subscription has expired. Its purpose is to aid customers for a smooth transition. **Count** enables you to view usage data in terms of the number of end users and the number of SMS messages sent within the specified time period, whereas **Credit** shows the number of FTC credits used for end users and SMS messages. If you are using a credit-based subscription or have started your FTC service with a time-based subscription, you will not see the menu.
7. At the bottom of the usage chart, click SMS and/or Users to show or hide usage data by user or by SMS.
8. Mouse over a bar to view the total number of credits or user/SMS counts for the given time period.
9. While in Daily View, click **View Usage Details** to view detailed daily usage data, or click **Export CSV** to export the usage data to a .csv file.

View current user count and user quota

This section apply to customer of time-based subscriptions only.

Customers of a time-based subscription will see the "Current" tab across the top of the Usage page. Clicking that tab opens a page that shows the current user count and the allocated user quota for the selected realm or realms.

Credits

FortiToken Cloud charges its customers credits for its service. An FTC credit is defined as one FTC user-month, which means that one FTC credit can support one FTC end user for a month of service. The number of days in a user-month is determined by the number of days in the *current* month. For example, it's 30 for November, and 31 for December.

Flexible credit-based usage model

FTC calculates your daily credit consumption and charges your account accordingly using the following formula:

Daily credit usage = (Total number of FTC users on a given day) x (1/Number of days in the current month)

FTC uses a flexible credit-based licensing model and allows any combination of users and days of use. One FTC credit can either be used by one FTC end user for one month, or by 30 users for one day if the current month is June.

For example, if you started your FTC service with a newly activated FTC-LIC-120 license on June 1, 2019, with 30 end users on your account, FTC would have deducted 1 credit (=30 x 1/30) from your account for that day, and the FTC Dashboard would show that your Current Month Usage was 1 (credit), and your Current Balance was 119 (=120-1).

On the other hand, if you had only one end user on your account for the entire month of June, your FTC Dashboard would have shown the same current month usage and current balance data on June 30, namely, 1 credit {=(1 x 1/30) x 30}.

- You must activate your FTC license within one year from the day of purchase. Otherwise, it will expire and cannot be activated.
- FTC credits are valid for only one year from the date of license activation. All credits that come with your license, whether used or not, expire after one year. You must purchase a new license to continue using FTC.
- When your account credit balance is running low, Fortinet will notify you of the situation and prompt you to replenish your account with more credits. We strongly recommend that you renew your subscription as soon as possible. When your balance goes to zero, you will not be able to add more users or send token activation or transfer codes by SMS, but current users will be able to continue to use the authentication service (even if the balance goes negative). *Fortinet will never block authentication service for our customers due to zero or negative credit balance.*

FTC records the time and date when you add a user to or delete a user from FTC. It also keeps track of the current calendar month, including the start and end dates of the month and the number of days in the month.

For each active user in the current month, FTC also calculates the number of days the user is active during the month. It sends the data to FC periodically (every 24 hours by default) based on the global settings that you have configured.

FTC displays the total usage data on a per-account basis. An FTC admin user can only view usage data within the account that he or she is allowed to log into.

SKUs and user limits

FTC offers SKUs for 120, 1,200, 12,000 and 120,000 credits. The table below highlights the maximum number of users that each SKU can support:

Current credit balance	Maximum number of users allowed
0–120	120
121–1,200	1,200
1,201–12,000	12,000
12,001–120,000	120,000
>120,000	1,200,000

FTC works in tandem with FC to enforce your maximum user limit.

When you try to add more users than the SKU limit, FTC first checks with FC to see if you have already added more credits to your FC account. If you haven't, FTC will prompt you to purchase more credits.

If your credit balance falls below the number for the current maximum user limit, FTC will keep the current maximum user limit. For example, if your have purchased 1,200 credits, FTC sets your maximum user limit to 1,200. If your credit balance decreases to 100, FTC still keeps the maximum user limit at 1,200. If your credit balance increases to 12,000, then FTC sets your new limit to 12,000.

Number of users vs. number of auth client and realms supported

FTC supports realm configuration. The following table highlights the correlation between the number of end users and the number of realms and auth clients that can be supported in your account.

Number of end users	Max. number of auth clients supported	Max. number of realms supported
120	12	12
1,200	120	120
12,000	1,200	1,200
120,00	12,000	12,000
1,200,000	120,00	120,000

Replenish your credit balance

FTC automatically notifies you when your account credit balance is falling. Once your credit balance drops to 0 (zero) or below, you will not be able to add new users to your account or send SMS messages to existing users on your account. To avoid service disruption, you must replenish your account by purchasing more user credits and add them to your account. You can use our SKU system to purchase more credits based on your business need.

Replenishing your account balance involves the following steps:

1. Purchase more user credits via a Fortinet-authorized reseller.
2. Add users credits to your account.

The following paragraph provides general instructions on how to purchase more user credits.

Purchase more credits

Extra user credits can be purchased through Fortinet-authorized resellers only. Do not contact Fortinet Customer Service & Support for this service.

To purchase more user credits:

1. Decide the number of extra user credits you'll need to purchase. For more information, refer FortiToken Cloud Data Sheet.
2. Contact a Fortinet-authorized reseller in your region to place an order.
3. Wait for the Fortinet FortiToken Cloud license file, which will arrive as a PDF attachment in email shortly after your order is processed.

Add credits to your account

To add the newly purchased user credits to your FTC account:

1. Open your web browser.
2. Log in to FortiToken Cloud.
3. Select the FTC account to which you want to add the newly purchased credits.
4. On the Dashboard page, locate the Current Balance tab and click the number on the tab.
   You are now taken to the Fortinet Customer Service & Support (or FortiCloud) site.
5. From the top of the web page, click **Asset>Register/Activate**.
   The Registration Wizard opens.
6. Follow the Wizard to register your FTC subscription.
   The system generates and displays a serial number when the registration is completed.
7. From the top of the page, click **Asset>Manage/View Products**.
8. Click the serial number.
   The Product Information page opens.
9. Click the **License File Download** link to download the license file.

Licenses

The Licenses page applies to customers of time-based subscriptions only.

The Licenses page shows all valid time-based licenses in your account. The table below describes the information on the Licenses page.

Column header	Description
Contract Number	The contract number of the license.
Users	The number of end users the license can support.
SMS	The number of SMS messages the license can support.
Remaining SMS	The number of SMS messages
Start Date	The date on which the license is registered for use.
End Date	The date on which

Settings

The Settings menu has three sub-menus:

- **Settings>Global** menu is accessible to the global admin user only. It opens the Settings>Global page with the tools for the global admin to make system-wide settings changes that affect all sub-admin accounts on your FTC account. For more information, see Global on page 61.
- **Settings>Realm** menu enables you to view the settings of the current realm. It also provides tools for making settings changes to the current realm. For more information, see Realm on page 63.
- **Settings>Templates** menu enables you to edit or create message templates. For more information, see Templates on page 69.

All parameters in the Settings page are centrally-managed in FTC and applied at the global level.

Global

This feature is accessible to global admin users only.

The Settings>Global menu enables global admins to make system-wide changes that affect all realms in their FTC account. it has three global menu options:

- Multi-realm Mode
- Auto-create Auth Client
- Share-quota Mode

The following paragraphs discusses how to use each of the features.

Multi-realm mode

FortiToken Cloud comes with a default realm. By enabling multi-realm mode, the global admin user can add custom realms and associate them with auth clients to better allocate and manage auth clients and end users.

By design, multi-realm mode is enabled for new FTC customers, but disabled for customers who started their FTC service before the FOS 6.2.3 release. When multi-realm mode is disabled, new auth clients will be assigned to the default realm; when multi-realm mode is enabled, new auth clients registered in FTC will be automatically assigned to a new realm.

While there is no need for new FTC customers to enable the multi-realm mode, existing customers must enable it to take advantage of the benefits that multi-realm mode offers. When multi-realm mode is enabled, you can create custom realms and assign auth clients to them. Once an auth client is assigned to a custom realm, you can add and sync users from it. Otherwise, all auth clients will be assigned to the default realm, and you cannot assign or sync users from them.

Even if your auth clients support the "pre-generated auth clients" feature and multi-realm mode is enabled on FTC, you cannot add or sync users from pre-generated auth clients until/unless the FTC global admin has associated them with a realm.

Enable Multi-realm Mode

If Multi-realm Mode has been disabled in your FTC global settings, you can enable it by taking the following steps:

1. On the side menu, click **Settings**>**Global** to open the Global Settings page.
2. On the Global Settings page, click the **Multi-realm Mode** button to turn it *on*.
   The Multi-realm Mode dialog opens, showing some important messages about the feature.
3. Read the messages, and click **OK** to proceed.
4. Click **Apply Changes.**
   The Apply Changes dialog opens.
5. Click **Confirm.**

Disable Multi-realm Mode

When Multi-realm Mode is enabled, you can disable it using almost the same procedures mentioned above. The only difference is in Step 2, where you must turn Multi-realm Mode *off* instead.

For more information on realms, see Realms on page 41.

Auto-create Authentication Client

It applies to FortiGate VDOMs only, and has no effect on other authentication clients, i.e., FortiAuthenticator and FortiSandbox.

Normally, the admin of any FortiGate VDOM can add that VDOM to FTC as an Auth Client by enabling the first user from the VDOM for FTC (if the VDOM was not already assigned to a realm). So when the FOS sends to FTC a VDOM list which contains a new VDOM with a user enabled for FTC service, FTC will automatically add that VDOM as an auth client. This may inadvertently allow unintended auth clients to consume FTC credits. To prevent this from happening, FTC has introduced the "Auto-create Auth Client" to make the "add-auth-client-on-creation-of-first-user" feature optional in its global settings.

Disable Auto-create Auth Client

By default, Auto-create Auth Client is enabled, but you can disable it using the following procedures:

1. On the side menu, click **Settings**>**Global** to open the Global Settings page.
2. On the Global Settings page, click the **Auto-create Auth Client** button to turn it *off*.
   The Auto-create Auth Client dialog opens, showing some important messages about the feature.
3. Read the messages, and click **OK** to proceed.
4. Click **Apply Changes.**
   The Apply Changes dialog opens.
5. Click **Confirm.**

Enable Auto-create Auth Client

If Auto-create Auth Client is disabled, you can enable it using almost the same procedures mentioned above. The only difference is in Step 2, where you must turn Auto-create Auth Client *on* instead.

Share-quota Mode

The "Share-quota Mode" option applies to customers of paid time-based subscriptions only; customers of credit-based subscriptions or time-based trial accounts will not see this option.

When share-quota mode is enabled (default), the remaining user quota will be shared by all realms. When share-quota mode is disabled, the remaining user quota will not be shared by realms.

Realm

Realm

The Settings>Realm menu opens the Settings>Realm page where you can set or update various settings for a selected realm. The page has the following tabs:

To configure or update the settings of a realm:

1. On menu bar, click **Settings>Realm.**
   The Settings>Realm page opens.
2. On top of the page, click the down arrow, and select a realm of interest from the drop-down list menu.
3. Click a desired tab to open the page for that setting, make the desired changes as described in the following tables, and click **Apply Changes.**
4. Repeat Step 3 above to configure or update the other settings of the realm.

General Setting

Parameter	Default value
MFA Method	Select a MFA method that FTC uses to further authenticate your end users upon receiving a username and password. The default is FTK. • FTM (default)—FTC sends a unique one-time passcode (OTP) to the FortiToken Mobile app on your end users' smart phones. **Note:** This option requires that your end users must have the FortiToken Mobile app installed on their smart phones. • SMS—FTC sends an OTP via text message to your end users' smart phones. Upon receiving the OTP, an end user must enter it on the log-in page to gain access to the auth client. **Note:** To use this option, FTC must have its end user's valid smart phone numbers in its database. Because FTC deducts one credit for every 250 SMS messages it sends, the FTC admin must ensure that the account has enough credits to use this feature. • Email—FTC sends a unique OTP to the end user's email on file. The user then has to manual copy and past the OTP to FTC to gain access to the auth client (i.e., FGT or FAC). • FTK—FTC requires end users to provide the OTP generated by their FortiToken (hardware token) for MFA. **Note:** To use this option, the FTC admin must first add the serial number of the FortiToken to FTC, and assign it to the end user. Upon receiving the user's username and password, FTC prompts the user for an OTP from the FortiToken device. The user must press the FortiToken to get the OTP, and then manually enters it. See Hardware Tokens on page 54. Also, when FTK is set as the MFA method for a realm, you can let FTC automatically assign FTKs to selected users by clicking the **Auto-assign FTK** button on the **Users** page. See Users on page 44.
Max Login Attempts Before Lockout	Click above the horizontal line and specify the number of failed login attempts allowed before lockout. Valid values range from 1 to 25. The default is 7.

Parameter	Default value
	Note: FTC does not allow locked users to authenticate. Instead, it displays the message "Locked, please try again in <lockout interval> minutes."
Lockout Period	Click above the horizontal line and specify a lockout period, which ranges from 60 to 7200 seconds. The default is 60 seconds.
Enable Bypass	Enable or disable bypass. Bypass is enabled by default. • Enable—You can let the FTC end users bypass MFA. If enabled, you must also set the Bypass Expiration Time, as described below. • Disable (default)—The admin user cannot let user bypass MFA. **Note:** If Enable Bypass is disabled on the **Settings** page, the admin user can not enable bypass for FTC end users on the **Users** page. See Users on page 44.
Bypass Expiration Time	Click above the horizontal line and specify the length of time bypass remains in effect. Valid values range from 5 minutes to 72 hours. The default is 1 hour (3600 seconds).
Auto-alias by Email	Enable or disable the Auto-alias by Email. **Note:** The feature is disabled by default. If enabled, FTC automatically alias usernames feature in the current realm. For more information, see Enable Auto-alias by Email on page 65.

Enable Auto-alias by Email

Many FTC end-users have different usernames in different applications and different domains. By the same token, a single FTC user may have different usernames in different FTC auth clients. For example, John Doe II may have the following usernames:

- `user1` in VPN
- `user_one` in a web app
- `u1` as a system admin
- `user1@company.com` on an email server

FTC now allows for different usernames to be attributed to the same user (i.e., same person) so that only one token needs to be assigned to a single person. It does this by providing an Auto-alias by Email option, which once turned on enables it to automatically add usernames as aliases when their email addresses are the same.

By default, Auto-alias by Email is disabled, you can enable using the following procedures:

1. On the side menu, click **Settings>Realm** to open the settings page of the current realm.
2. Scroll down until you see Auto-alias by Email option near the bottom of the page.
3. Click the **Auto-alias by Email** button to enable it.

Once the Auto-alias by Email feature is enabled, all usernames with the same email address are automatically set as aliases under the same username. Users with the same email address as an existing user are automatically be added as an alias.

It is important to note that aliased users must be in the same realm. Usernames with the same email address are still set as unique users if they are in different realms, even when the auto-alias feature is disabled.

FTM Setting

Parameter	Default value
1. Settings	Make the entries or selections below:
Enable Push	Click the button to enable or disable Push notification.
Notification Method	Click the down arrow and, from the drop-down menu, select either of the following: • Email—Token activation/transfer codes are sent to users' email addresses in the system. • SMS—Token activation/transfer codes are sent by SMS to users' mobile phone numbers in the system. **Note:** When Notification Method is set to SMS, make sure that the users' mobile phone numbers in the system are valid. Otherwise, you will get an error when requesting a new token for a user on the **Users** page because of invalid phone numbers. See Users on page 44. **Note:** FTC deducts one credit from your credit balance for every 250 SMS messages it sends to deliver OTPs. You may experience some problem sending OTPs by SMS when your credit balance is low, and you will get an error message when trying to send an OTP if there is no credit remaining on your account. In both cases, we strongly recommend that you purchase more credits before attempting to use this feature.
App PIN Required	Click the button to enable or disable this feature. • Disabled (default)—No app PIN is required. • Enable—If enabled, you must select a PIN Length and PIN Required Mode, as described below.
PIN Length	Click the down arrow and, from the drop-down menu, select one of the following: • 4 • 6 (default) • 8 **Note:** PIN length refers to the number of digits contained in an app PIN.
PIN Required Type	Click the down arrow and, from the drop-down menu, select either of the following: • Anytime—App PIN is required all the time. • Unlock—If selected, end users must have a PIN either on their device or FTM app to access FTC. If an end user has a PIN on the device, FTC won't ask for a PIN when using FTM; if an end user does not have a PIN on the device, FTC will ask for a PIN to use FTM.
OTP Algorithm	• TOTP (default). No action is needed.
OTP Time Step	Click the down arrow and, from the drop-down menu, select either of the following: • 30 (default) • 60

Parameter	Default value
	Note: OTP Time Step refers to the frequency in which FTM token codes are updated. For example, FTC will update FTM token codes once every 30 seconds when OTP Time Step is set to 30.
OTP Validation Window	The number of time steps the validation server takes to validate OTPs. Upon receiving an OTP from a client, the validation server computes the OTP using the shared secret key and its current timestamp (not the one used by the client) and compares the OTPs: if the OTPs are generated within the same time step, they match and the validation is successful.
OTP Display Length	Click the down arrow and, from the drop-down menu, select either of the following: • 6 (default) • 8 **Note:** OTP Display Length refers to the number of digits contained in a token activation/transfer code.
Activation Expiration Time	Click above the horizontal line and specify the length of time token activation codes remain valid. Valid values range from 1 to 336 hours. The default is 72 hours. **Note:** An FTM Token code must be activated within the set Activation Expiration Time. Otherwise, it will expire and you must request a new token.
FTM Logo	This enables admin users to choose logo image displayed at the bottom of the FTM app screen on their end users' mobile devices. • Upload Custom Logo—Click this button to upload a custom logo image to replace the default Fortinet logo. For instructions on how to use this feature, see Use a custom logo on page 67. • Restore Default Logo—Click this button to reverse to the default Fortinet logo on FTM.
2. Notification Templates	Select a desired email or SMS message template for each of the following:
Token Activation Email	An email template for FTC to send token activation notifications to your end users.
Token Transfer Email	An email template for FTC to send token transfer notifications to your end users.
Token Activation SMS	An SMS template for FTC to send token activation notifications to your end users.
Token Transfer SMS	An SMS template for FTC to send token transfer notifications to your end users.

Use a custom logo

FortiToken Cloud offers an option for admin users to upload their own logo image to replace the default Fortinet banner.

To use this feature, you must have your logo image file on your computer, and your logo image file must meet the following requirements:

- File format: Transparent PNG or JPEG
- Max image size: 150 kB, and 320 x 320 pixels

To upload your logo image

1. From the FTC GUI, select **Settings.**
2. Under FTM Logo, click **Import file.**
3. Browse for the logo image, select it, and click **Open.**
   The select image appears near the bottom of the Settings page.

If you want to restore the use of the default Fortinet logo, after uploading a custom logo image, click the **Default Logo** button.

Email MFA Setting

Once an end user is enabled for MFA, FTC sends a unique OTP to the end user's email on file. The end user must manual copy and past the OTP to FTC to gain access to the auth client (i.e., FGT or FAC).

Parameter	Description
1. Settings	
OTP Expiration Time	Click the down arrow to select an OTP (one-time password) time. **Note:** An OTP is valid only within the specified period of time, and expires beyond that. The default is 5 minutes.
OTP Display Length	Click the down arrow to select an OTP display length, which is the number of digits displayed. The default is 6.
2. Templates	
OTP Template	Click the down arrow to select an OTP email template. **Note:** You view the content of the selected template by clicking the view button on the right.

SMS MFA Setting

Once an end user is enabled for MFA, FTC sends an OTP via text message to the end users' smart phone. Upon receiving the OTP, the end user must enter it on the log-in page to gain access to the auth client.

Parameter	Description
1. Settings	
OTP Expiration Time	Click the down arrow to select an OTP (one-time password) time. **Note:** An OTP is valid only within the specified period of time, and expires beyond that. The default is 5 minutes.
OTP Display Length	Click the down arrow to select an OTP display length, which is the number of digits displayed. The default is 6.

Parameter	Description
2. Templates	
OTP Template	Click the down arrow to select an OTP SMS template. **Note:** You view the content of the selected template by clicking the view button on the right.

Templates

An FortiToken Cloud (FTC) template refers to the message template that FTC uses to send OTP and token activation or transfer notifications to its end users. FTC can notify its end user of such activities either by email or SMS, depending on your configuration. It not only offers a number of default templates that you can use out of the box, but also enables you to create your own templates on the fly.

The default templates are read-only, and cannot be altered.

Add a template

To add a template:

1. On the menu bar, click **Settings>Templates** to open the Template page.
2. In the upper-left corner of the Template page, click **Add Template.**
   The Add New Template dialog opens.
3. For Method, click the down arrow to select a notification method.
   Note: Method refers to the means that FTC uses to send OTP and token activation or transfer notifications to its end users. To use email, you must provide a valid email address; to use SMS, you must provide a valid phone number with the correct country code for each and every end users.
4. For Type, click the down arrow to select a desired message template.
   Note: FTC offers three types of templates, and each template is for a specific purposes. Be sure to create all the three types of template to take full advantage of this feature.
5. Click **Confirm.**
   The dialog refreshes, shows more fields.
6. Specify a unique name for the template.
7. Make the desired changes to the subject of the message, if you like.
8. Make desired changes to the message content, if you like.
9. Click **Preview** to review the message.
10. Click **Save.**

Edit a template

Only custom templates can be edited. Default templates are read only and cannot be edited.

To edit a template:

1. On the menu bar, click **Settings>Templates** to open the Template page.
2. On the Templates page, locate the custom template of interest and mouse over it.
   The tool bar slides in from the right end of the row.
3. Click the **Edit** tool
   A dialog opens showing the settings of the template.
4. Make the desired changes to the template.
5. Click **Preview** to review the changes to the template.
6. Click **Save.**

Delete a template

Only custom templates can be deleted. Default templates are read only, and cannot be edited or deleted.

To delete a template:

1. On the menu bar, click **Settings>Templates** to open the Template page.
2. On the Templates page, locate the custom template of interest and mouse over it.
   The tool bar slides in from the right end of the row.
3. Click the **Delete** tool
4. Click **Yes.**
5. The template is deleted from the Template page after the page refreshes.

Apply templates

All templates, regardless of their message type or communication method, are applied at the realm level. Each type of notification requires a specific notification template. For more information, see Templates on page 69

To apply a token activation and/or transfer notification template to a realm:

1. On the main menu, click **Realms**to open the Realms page.
2. On the Realms page, locate the realm of interest and mouse over it.

The tool bar slides in from the right end of the row.

3. Click the **Settings** tool to open the Settings>Realm page.
4. Across the top of the page, click the **FTM Setting** tab.
5. Scroll down the page and click **Notification Templates.**
6. In each of the field, click the down arrow and select the template of interest.
7. Click **Apply Changes.**
   The selected template is now applied to the realm and will be used when FTC sends token activation and/or transfer notifications to its end users.

To apply an email OTP template

1. On the main menu, click **Realms**to open the Realms page.
2. On the Realms page, locate the realm of interest and mouse over it.
   The tool bar slides in from the right end of the row.
3. Click the **Settings** tool to open the Settings>Realm page.
4. Across the top of the page, click the **Email MFA Setting** tab.
5. Scroll down the page and click **Templates.**
6. Click the down arrow to select the template of interest.
7. Click **Apply Changes.**

To apply an SMS OTP template

1. On the main menu, click **Realms**to open the Realms page.
2. On the Realms page, locate the realm of interest and mouse over it.
   The tool bar slides in from the right end of the row.
3. Click the **Settings** tool to open the Settings>Realm page.
4. Across the top of the page, click the **SMS MFA Setting** tab.
5. Scroll down the page and click **Templates.**
6. Click the down arrow to select the template of interest.
7. Click **Apply Changes.**

Logs

Logs capture operational and administrative events that happened on FTC. Events can be performed by an FGT VDOM admin user or FTC itself.

FTC has two types of logs:

- Authentication logs on page 71
- Management logs on page 73

Authentication logs

Authentication logs capture authentication attempts that your FTC end users have made.

To view authentication logs:

1. On the main menu, click **Logs>Authentication** to open the authentication logs page.
2. In the upper-left corner of the page, click the **Filters** button to open the Filters drop dialog.
3. Select the filters of interest.
4. Click **OK.**

Each authentication log captures the following data:

Column	Description
Timestamp	The date and time of an authentication request. **Note:** FTC captures the time of an event in UTC time, and then converts it to the client browser's local time zone, which is the time shown in the timestamp.
Username	The username of the user who made the request.
Auth Client	Shows either of the following: • The serial number and VDOM name if the Auth Client is an FGT device. • The source IP address if the Auth Client is a third-party device.
Realm	The realm ID of the realm from which the authentication request is attempted.
Action	The authentication action.
Status	The status of the authentication request expressed in standard HTTP status codes. See List of HTTP Status Codes.
Result	The outcome of an authentication request, which can be either of the following: • Success • Failed

Customize log display

The Logs > Authentication page provides a number of tools for filtering, searching for, and sorting log entries displayed on screen.

Filter logs by date and time

This option enables you to display logs for the period of time you specify.

1. In the upper-left corner of the page, choose the start date and time and the end date and time.
2. Click **Filter.**

Filter logs by user

This option enables you to filter the logs by username.

1. In the upper-left corner of the page, below the Start date and End date filter, click **user**.
2. From the drop-down menu, select a username.

Filter logs by status

This option allows you to filter logs by HTML status code.

1. In the upper-left corner of the page, below the Start date and End date filter, click **status**.
2. From the drop-down menu, select an HTML status code.

Sort the log table

You can sort the entries in the log table by clicking any of the column headers, namely:

- Timestamp
- Username
- Auth Clients
- Results

View log details

You can click a log entry to open the Log Details pop-up, which shows details of the log.

Management logs

Management logs capture management activities that have occurred on FTC.

To view managementlogs:

1. On the main menu, click **Logs>Management** to open the management logs page.
2. In the upper-left corner of the page, click the **Filters** button to open the Filters drop dialog.
3. Select the filters of interest.
4. Click **ok.**

A management log entry contains the following data:

Column	Description
Source	The source of the request, which can be either of the following: • Auth Client • FTC portal
Timestamp	The date and time of the request. **Note:** FTC captures the time of an event in UTC time, and then converts it to the client browser's local time zone, which is the time shown in the timestamp.
Administrator	The authorized entity that made the request, which can be either of the following: • The serial number of FGT if the request was made from FGT. • The username of the FTC user if the request was made from the FTC portal.
Action	The action of the request, which can be one of the following: • Create • Get

Column	Description
	• Modify
Subject	The target of an action. For example, who or what is changed? **Note:** If the subject is an FTC end user, it should also include the account to which the user belongs.
Status	The status of a management event.

Customize log display

The Logs > Management page provides a number of tools for filtering, searching for, and sorting logs displayed onscreen.

Filter logs by date and time

This option enables you to display logs for the period of time you specify.

1. In the upper-left corner of the page, choose the start date and time and the end date and time.
2. Click **Filter.**

Filter logs by user

This option enables you to filter the logs by username (email address).

1. In the upper-left corner of the page, below the Start date and End date filter, click **User**.
2. From the drop-down menu, select a username.

Filter logs by action

This option allows you to filter logs by action.

1. In the upper-left corner of the page, below the Start date and End date filter, click **Action**.
2. From the drop-down menu, select an action.

Filter logs by status

This option allows you to filter logs by status.

1. In the upper-left corner of the page, below the Start date and End date filter, click **Status**.
2. From the drop-down menu, select a status.

Filter logs by realm

This option allows you to filter logs by realm ID.

1. In the upper-left corner of the page, below the Start date and End date filter, click **Realm**.
2. From the drop-down menu, select a realm ID.

Filter logs by subject

This option allows you to filter logs by subject.

1. In the upper-left corner of the page, below the Start date and End date filter, click **Subject**.
2. From the drop-down menu, select a subject.

Filter logs by subject ID

his option allows you to filter logs by subject ID.

1. In the upper-left corner of the page, below the Start date and End date filter, click **Subject ID**.
2. From the drop-down menu, select a subject ID.

Sort the log table

You can sort the log entries in the table by clicking any of the column headers, namely:

- Source
- Timestamp
- Administrator
- Action
- Subject

View log details

You can click a log entry to open the Log Details pop-up, which shows details of the log.

FortiToken Mobile

FTM is an OATH-compliant, event- and time-based, one-time password (OTP) generator application for mobile devices. It generates OTP codes on your mobile device without the need for a physical token. It allows you to install Fortinet tokens and third-party tokens, including tokens for multi-factor authentication used by Dropbox, Google Authenticator, Amazon, Facebook, Microsoft, Yahoo, Snapchat, PayPal, eBay, and LastPass.

This section covers the following topics:

Supported FTM apps

This FTC release supports FTM for mobile devices running on the latest versions of Apple iOS or Google Android, as described below.

FTM app	Supported mobile OS	Supported devices
FTM 4.5.3 and higher for iOS	Apple iOS 9.x, 10.x, and 11.x	iPhone, iPad, and iPod Touch
FTM 4.5.0 and higher for Android	Google Android 4.4 and up	Android phones and tablets

You can download and install the app directly onto your Apple iOS or Google Android devices. No cellular network is required. If you do not have cellular service, use your WiFi access instead.

To get FTM version 4.5.3 for iOS

1. Start your iOS device.
2. Go to **App Store**.
3. Browse for **FortiToken Mobile** version 4.5.3.
4. Download and install the app.

To get FTM version 4.5.0 for Android

1. Start your Android device.
2. Go to **Google Play**.
3. Browse for **FortiToken Mobile** version 4.5.0.
4. Download and install the app.

Activate FTM tokens

After your system administrator assigns you a token, you receive a notification with an activation code and an activation expiration date via SMS or email depending on the option your system administrator has chosen.

You must activate your token by the expiration date. Otherwise, you will have to contact your system administrator for the token to be reassigned for activation.

The following instructions apply to activation of FTM token for an Apple iPhone. It is assumed that you have installed FTM version 4.5.3.x for iOS on your iPhone.

If you receive your FTM token via email, follow the steps below to activate it.

1. From your iPhone, start the FTM app.
   If this the first time you open the app, you are prompted to create a PIN for secure access to the app and tokens.
2. In the upper-right corner of the screen, tap **+** (**Add**).
   Your iPhone's camera starts so that you can scan the token's QR code. Refer to your email notification.
3. Scan the QR code.
   Once the QR code has been scanned, your token becomes provisioned and activated and starts generating token codes immediately. If you would like to view the OTP's digits, select the eye icon.

Activate third-party tokens

The steps for activating a third-party token are the same as for activating a Fortinet token. Depending on the token vendor, you may be able to activate the token by scanning the QR code as well.

Use FTM tokens

Upon opening the FTM app on your iPhone, your token will be visible in the app's home screen. The token is a 6-digit OTP which updates dynamically every 30 seconds.

If you have multiple tokens installed, they all show up on the home screen.

To use a FTM token

1. From your iPhone, start the **FortiToken Mobile** app.
2. On the home screen, press and hold on an OTP code, and tap **Copy**.
3. From your iPhone, start FTC.
4. Log in with your username and password.
5. Paste the OTP code when prompted.
   You should be able to log into FTC if you pass the MFA process.

FAQs

This section provides answers to some of the most frequently asked questions from FortiToken Cloud customers.

Does FortiGate support FTC AD-wildcad 2FA if cnid=sAMAcountName?

Yes. Starting with the FOS 6.4.6 and 7.0.0 releases, FortiGate supports FTC AD-wildcard 2FA if cnid = sAMAccountName .

Note: FortiGate also supports FTC AD-wildcard 2FA if cnid = cn.

How to configure FortiGate for LDAP authentication?

(cnid can be set either as ‘cn’ or ‘sAMAccountName’)

Step 1: Configure LDAP server in FortiGate via CLI

```
config user ldap
    edit "ldap_1"
        set server "xx.xxx.xx.xxx" (ldap-server-ip)
        set source-ip xx.xxx.xx.xx (fgt-ip)
        set cnid "cn"                <<< cnid
        set dn "DC=FIS,DC=local"
        set type regular
        set two-factor fortitoken-cloud  –> enable 2fa ftc
        set username "CN=admin,CN=Users,DC=FIS,DC=local"
        set password ENC  ----
>YmplY+eec9Wi1qmxYnZvrf3QSxJ8Bui73VwAo+ngLSf3ynkLF4So9AmAn6zNqbRHqQOEwSM5jP1p2BNNdnpCHJlo06uFw
QmySdvUm6CYhXsD/zNB3T4XkTIDqTy5g43/Fq0CavX7sXtI485chKKaAU5HRO6xf+/0+2ZeBj2qlHxOxO7Qz1j2WkqkN+b
RyAGkVUDOkw==
    next
```

Step 2: Add LDAP server as 'remote server' to the existing SSL VPN group

```
config user group
    edit "ssl_vpn_group"
        set member "ldap_1"
    next
end
```

Step 3: Search and query users from the AD-LDAP server

```
exe fortitoken-cloud sync
```

Step 4: Verify all LDAP users on FTC portal

1. Launch the FTC portal.
2. From the main menu, click Users.

All LDAP users on the remote server should appear on the Users page.

How do FTC credits work?

FortiToken Cloud charges its customers credits for its service. An FTC credit is defined as one FTC user month, which means that one FTC credit can support one FTC end user for a month of service. The number of days in a user-month is determined by the number of days in the current month.

Can you give an example of FTC flexible licensing options?

Yes. Let's assume that you would like to have 25 end users on your account for the first year. You will need 300 (=12 x 25) credits for that. So instead of buying one (1) FTC-LIC-1200 license which carries 1200 credits (more than what you need) and cost a lot more, you can just purchase three (3) FTC-LIC-120 licenses which will give you 360 credits, enough to cover all the users for one year under normal circumstances.

How to check the auth status for WebApp API client for push authentication?

We have two kinds of APIs for auth status checking: one is single auth status checking by auth id, the other is the batch auth query for all auth clients in current system.

Single auth status checking by auth id

GET https://ftc.fortinet.com:9696/api/v1/auth/<auth_id>. The auth status is alive for two minutes (the current production default configuration) in the system. It means that if the auth status query API reaches FTC two minutes after the push request (approves or denies), the status response will be {“status”: null}.

Batch auth query

GET https://ftc.fortinet.com:9696/api/v1/auth?sn=<auth_client_id>. This API call can get the all auth id status for the auth clients in current system. Please note that the auth status will be cleared in the system after they are returned via the batch query API. It means that there will be no any auth status back after one batch query if no any new auth arrives in the system.

API doc link: https://docs.fortinet.com/document/fortitoken-cloud/latest/rest-api, download the REST API doc, section of “User authentication” -> GET.

What are the required parameters for post auth by WebApp client?

Username is the only parameter required for post auth from the client side. The FTC server will extract the other information such as client id, realm id based on the access token.

How to Configure SNMP server on FortiOS

Configuring an SNMP sever on FortiOS requires the following steps:

Step 1: Configure the SMTP server

```
config system email-server
   set type custom
   set reply-to <reply-to string> ------{ specify the reply-to email address.
   set server <IP or domain of the SMTP Server>
   set port 25
   set source-ip 0.0.0.0
   set source-ip6 ::
   set authenticate disable
   set security none
end
```

Step 2: Configure SMS service on FortiGate

```
config system sms-server
   edit <provider> ------{ Provider Name or Any name
   set mail-server <server_name> ------{ providerdomain
end
```

Step 3: Configure SMS service on SMS provider

Configurations of SMS service on the service provider side vary, depending on the SMS provider of your chioce.

Step 4: Create a user(s) with SMS with two-factor authentication

```
config user local
edit <user> ------{ User name
   set two-factor sms
   set sms-phone "xxxxxxxxxxx"
   set sms-server custom
   set sms-custom-server <provider> ------{ configured in Step 2
end
```

- The SMTP server configured in Step 1 above is the server that the FortiGate uses to communicate to the SMS servers. This means that the SMTP server must allow the FortiGate to relay through it.
- The mail-server address in Step 2 below is the domain of the email address to which the FortiGate sends emails.
  In the example configuration above, the FortiGate sends an email to [mobile_number_of_recipient]@[providerdomain] through the server IP configured in Step 1. You can log in to the FortiGate unit using the user created in Step 4. Upon clicking 'Login', you will get the 'Token Code' request, and an SMS will be sent to your phone. You can then type in the one-time code and login to your FortiGate.

How does FortiOS support FortiToken Cloud?

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
6.2.0	FTM	No	No	No	No	No. FTC must be enabled manually `config system global set fortitoken-cloud-service {enable | disable}`	`execute fortitoken-cloud sync-user`— Synchronize users to the FortiToken Cloud	`diagnose ftk-cloud debug`— Enable/disable debug output.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`server` — Display FTC server IP address, port number, and https. `show`— Display diagnostics information. `delete` — Delete a user (name). `set-http`— Set HTTP status return code for diagnostics purposes. `clear`— Clear server connection settings for diagnostics.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`sync`—Synchronize user information with FortiToken Cloud.
6.2.1	FTM	No	No	No	No	No. FTC must be enabled manually `config system global set fortitoken-cloud-service {enable | disable}`	`execute fortitoken-cloud sync-user`—Synchronize users to the FortiToken Cloud	`diagnose ftk-cloud debug`—Enable/disable debug output. `server`—Display FTC server IP address, port number, and https. `show`—Display diagnostics information. `delete`—Delete a user (name).

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`set-http`— Set HTTP status return code for diagnostics purposes. `clear`— Clear server connection settings for diagnostics. `sync`— Synchronize user information with FortiToken Cloud.

6.2.2	FTM	No	No	`config user ldap`
				`edit "L"`
				`set server "xx.xxx.xx.xx"`
				`set cnid "uid"`
				`set dn "dc=srv,dc=world"`
				`set type regular`
				`set two-factor fortitoken-cloud`
					No	No. FTC must be enabled manually
						`config system global`
						`set fortitoken-cloud-service {enable | disable}`
							`exe fortitoken-cloud new` — Send new activation code for a user.
							`show` — Show service status of this FortiGate.
								`diagnose ftk-cloud debug`— Enable/disable debug output.
								`server` — Display FTC server IP address, port number, and https.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
							`sync` — Synchronize users to FortiToken Cloud. `trial`— Activate free trial. `update` — Update VDOM list to FortiToken Cloud.	`show`— Display diagnostics information. `delete` — Delete a user (name). `set-http`— Set HTTP status return code for diagnostics purposes. `clear`— Clear server connection settings for diagnostics. `sync`– Synchronize user information with FortiToken Cloud.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command

6.2.3	FTM, Email, SMS	No	No	`config user ldap`
				`edit "L"`
				`set server "xx.xxx.xx.xx"`
				`set cnid "uid"`
				`set dn "dc=srv,dc=world"`
				`set type regular`
				`set two-factor fortitoken-cloud`
					No	Yes	`exe fortitoken-cloud show` — Show service status of this FortiGate.
							`sync` — Synchronize users to FortiToken Cloud.
							`trial` — Activate free trial.
								`diagnose ftk-cloud debug`– Enable/disable debug output.
								`server` — Display FTC server IP address, port number, and https.
								`show`— Display diagnostics information.
								`delete` — Delete a user (name).
								`set-http`— Set HTTP status return code for diagnostics purposes.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`clear`—Clear server connection settings for diagnostics. `sync`—Synchronize user information with FortiToken Cloud.

6.2.4	FTM, Email, SMS	Yes	No	`config user ldap`
				`edit "L"`
				`set server "xx.xxx.xx.xx"`
				`set cnid "uid"`
				`set dn "dc=srv,dc=world"`
				`set type regular`
				`set two-factor fortitoken-cloud`
					`execute fortitoken-cloud update`	Yes	`exe fortitoken-cloud new` —Send new activation code for a user.
							`show` — Show service status of this FortiGate.
							`sync` — Synchronize users to FortiToken Cloud.
							`trial` — Activate free trial.
							`update` — Update VDOM list to FortiToken Cloud.
								`diagnose ftk-cloud debug`—Enable/disable debug output.
								`server` — Display FTC server IP address, port number, and https.
								`show`—Display diagnostics information.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`delete` — Delete a user (name). `set-http`— Set HTTP status return code for diagnostics purposes. `clear`— Clear server connection settings for diagnostics. `sync`– Synchronize user information with FortiToken Cloud.

6.4.0	FTM, Email, SMS	Yes	No	`config user ldap`
				`edit "L"`
				`set server "xx.xxx.xx.xx"`
				`set cnid "uid"`
				`set dn "dc=srv,dc=world"`
				`set type regular`
					`execute fortitoken-cloud update`	Yes	`exe fortitoken-cloud new` Send `new`— activation code for a user.
							`show` — Show service status of this FortiGate.
								`exe fortitoken-cloud FGT200E-641 (global) #`

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
				`set two-factor fortitoken-cloud`			`sync` — Synchronize users to FortiToken Cloud. `trial`— Activate free trial. `update` — Update VDOM list to FortiToken Cloud.	`diagnose ftk-cloud` `debug`— Enable/disable debug output. `server` — Display FTC server IP address, port number, and https. `show`— Display diagnostics information. `delete` — Delete a user (name). `set-http`— Set HTTP status return code for diagnostics purposes.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								clear—Clear server connection settings for diagnostics. sync—Synchronize user information with FortiToken Cloud.
6.4.1	FTM, Email, SMS	Yes	Yes	config user ldap edit "L" set server "xx.xxx.xx.xx" set cnid "uid" set dn "dc=srv,dc=world" set type regular set two-factor fortitoken-cloud	execute fortitoken-cloud update	Yes	exe fortitoken-cloud new Send new—activation code for a user. show—Show service status of this FortiGate. sync—Synchronize users to FortiToken Cloud. trial—Activate free trial.	diagnose ftk-cloud debug—Enable/disable debug output. server—Display FTC server IP address, port number, and https. show—Display diagnostics information.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
							`update` — Update VDOM list to FortiToken Cloud.	`delete` — Delete a user (name). `set-http`— Set HTTP status return code for diagnostics purposes. `clear`— Clear server connection settings for diagnostics. `sync`– Synchronize user information with FortiToken Cloud.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command

6.4.2	FTM, Email, SMS	Yes	Yes	`config user ldap`
				`edit "L"`
				`set server "xx.xxx.xx.xx"`
				`set cnid "uid"`
				`set dn "dc=srv,dc=world"`
				`set type regular`
				`set two-factor fortitoken-cloud`
					`execute fortitoken-cloud update`	Yes	`exe fortitoken-cloud new` Send new–activation code for a user.
							`show` — Show service status of this FortiGate.
							`sync` — Synchronize users to FortiToken Cloud.
							`trial`— Activate free trial.
							`update` — Update VDOM list to FortiToken Cloud.
								`diagnose fortitoken-cloud debug` Enable/disable debug output.
								`server` —IP address port number and https.
								`show` — Display diagnostics information.
								`delete` — Command to delete a user.
								`set-http` — Set HTTP status return code for diagnostics only.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`clear`—Clear server connection settings for diagnostics. `sync`—Synchronize user information with FortiToken Cloud.

How to prevent LDAP users from bypassing 2FA?

This question is discussed in detail in the article "CVE-2020-12812 (bypassing two-factor authentication for LDAP users) and its remedies" (https://kb.fortinet.com/kb/documentLink.do?externalID=FD49410).

It describes what CVE-2020-12812 is all about, how two-factor authentication can be bypassed in the first place, and what options FortiGate offers to prevent the vulnerability from being exploited.

How to debug ‘user is unable to issue a new FortiToken Cloud token’?

Check account credit balance. The FortiToken Cloud server prevents users from issuing new FTC tokens when their account has a zero or negative credit balance. To resolve the issue, you must purchase a new license under your account ID and apply the credits to your account. For instructions on how to purchase new licenses, refer to the Purchasing Guide at https://docs2.fortinet.com/document/fortitoken-cloud/latest/how-to-add-licenses.

How to transfer ForitiToken Cloud auth clients from one account to another?

Fortinet products like FortiGate, FortiAuthenticator, FortiSandbox and FortiADC can be FortiToken Cloud auth client. If FTC admin wants to transfer one auth client from account A to account B, admin needs to contact support.fortinet.com and use live chat feature to transfer account. FTC admin needs to provides Auth Client serial number to complete the account transferring process. If FTC account transferring is completed, the left-over balance on account A can continue use on account B.

How to register FortiToken Cloud license to start using FortiToken Cloud service?

Once your FTC trial license is registered, your account automatically becomes a trial account, with 24 FTC credits free of charge. The free trial ends when the 24 credits are exhausted.

To continue using FTC services, you must purchase a regular FTC license and register it under your account before or upon the expiration of the free trial.

For more information, see Register your FTC subscription on page 18.

What is realm? And what does it do?

FortiToken Cloud enables admin users to create realms to effectively allocate resources and better manage their end users.

FTC admin can create custom realm, view realm permission, delete realm and view realm setting.

For more information, see Realms on page 41.

What does the status of the FortiToken Cloud (FTC) token mean?

You can find out the status of FTC tokens assigned to your end users using the following procedures:

1. On the main menu, click **Users** to open the Users page.
2. Locate the user of interest.
3. Mouse over the **Status** column.

When an FTC end user is created, the FortiToken Cloud server will send an activation notification to the end user either by email or SMS depending on the user setup. The status of an FTC token can be one or more of the following:

- **Pending**—The newly provisioned user initially shows up in ‘Pending’ status on the portal.
- **Active**—It changes to "Active" as soon as FortiToken Mobile is activated for the user.
- **Expired**—If the FTC token is not activated on its expiration date, the status changes to ‘Expired’.

- **No bypass/Bypass**—If bypass is enabled **(Settings>Realm>General Setting>Enable Bypass),** the newly created user in that realm shows up in 'Bypass' status.
- **Unlocked/Locked**—If the user's login attempts have exceeded the 'Max Login Attempts Before Lockout', the user's status changes to 'Locked'.

Can FTC admin enable or disable push feature from the FortiToken Cloud portal?

Yes. Starting from FTC 21.2.a, you can enable or disable the push feature from the FortiToken Cloud portal by clicking **Settings>Realm>FTM Setting> Enable Push**. For more information, see Realm on page 63.

How to add a second FortiGate to the realm where I already have one FortiGate up running?

Situation:

I have two FortiGate devices, one is already recognized by ftc.fortinet.com and our end user are using for MFA; the other is currently powered down. I want to add the second FortiGate to the same realm as the first one, but how?

Solution:

1. Power up the second FortiGate, and make sure that it is up and running properly.
2. Open the FortiGate Console, and run the command "`exec fortitoken-cloud update`".
   The command sends the DOM list to FTC and creates an auth client, but does not assign the auth client to any realm.
3. Assign the auth client corresponding to the VDOM where the users exist to the realm FGT5HD391580xxxx-root.
4. On the Auth Clients>FortiProducts page, select the realm FGT5HD391580xxxx-root for the new auth client.
5. Make sure that the users exist on the second FortiGate. (They should have users because the two FortiGate devices have the same conMakf.)
6. On the FortiGate Console, run the command "`exec fortitoken-cloud sync`".

How to create an aliased user?

An aliased user is a number of users grouped together sharing the same MFA method used by the base user and the same token (whether it is FTM or FTK). They must also be in the same realm.

To create an aliased user:

1. Log in to the FTC portal and click the **Users** menu.
2. On the Users page, select (check) all the users you want to be in the alias.
   Note: Ensure that all the users selected are in same realm and are using the same MFA method.
3. On top of the page, click the **Add User Alias** button.

4. In the dialog, select the base user and click **Next.**
5. Click **Confirm.**

The newly added alias shows in black bold-faced letters on the Users page. All users in it will share the same MFA method used by the base user. If it is FTM or FTK, they will be sharing the same token.
For more information, refer to Enable Auto-alias by Email.

How to provision FortiToken Cloud?

To assign a FortiToken Cloud to a local or remote user using a FortiGate or FortiAuthenticator, the device must be registered on the same account as the FortiToken Cloud contracts. The following instructions show how to provision FTC on a FortiGate.

To configure FortiToken Cloud to a local or remote user using a FortiGate:

1. Open the Console on the FortiGate device GUI.
2. Enable the **FortiToken Cloud Service** on the device:
```
config system global
   set fortitoken-cloud-service enable
end
```
3. Go to **User & Authentication > User Definition**.
4. Either edit an existing user of interest or create a new user using the **Users/Groups Creation Wizard.**
5. Enable **Two-factor Authentication**.
6. Select **FortiToken Cloud for Authentication**.
7. Enter the user's email address, where the use will receive the QR code for FortiToken activation.
8. Click **OK.**

The above instructions focuses on provisioning FortiToken Cloud on FortiGate. For instructions on how to provision FortiToken Cloud on FortiAuthenticator, refer to Getting started—FAC-FTC users on page 22 in the Admin Guide.

Change log

Date	Prodcut Release
04/15/2021	FortiToken Cloud 21.2.d
03/01/2021	FortiToken Cloud 21.1.a release.
12/02/2020	FortiToken Cloud 20.4.d release.
11/30/2020	FortiToken Cloud 20.4.c release.
10/07/2020	FortiToken Cloud 20.4.a release.
09/01/2020	FortiToken Cloud 20.3.e release.
08/05/2020	FortiToken Cloud 20.3.d release.
04/24/2020	FortiToken Cloud 20.2.c release.
03/25/2020	FortiToken Cloud 20.1.b release.
02/12/2020	FortiToken Cloud 20.1.a release.
10/25/2019	FortiToken Cloud 4.4.c release.
10/02/2019	FortiToken Cloud 4.4.b release.
07/02/2019	FortiToken Cloud 4.3.a release.
04/30/2019	FortiToken Cloud 4.2.d patch release.
04/04/2019	FortiToken Cloud 4.2.b initial release.