Admin Guide

FortiToken Cloud 23.1.a

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

FORTINET TRAINING 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

TABLE OF CONTENTS

Introduction

Many of today's most damaging security breaches could have been prevented by the use of multi-factor authentication (MFA). FortiToken Cloud solves this by offering a secure, easy-to-use, MFA-as-a-service for users of Fortinet products such as FortiGate (FGT) and FortiAuthenticator (FAC) as well as third-party web applications.

From provisioning to revocation, FortiToken Cloud offers a robust platform to manage your multi-factor authentication deployment. Its intuitive dashboard is available anywhere over the internet. It's a highly available platform that can scale support from organizations with a single FortiGate to managed service providers managing hundreds of FortiProducts and/or third-party Web apps.

FortiToken Cloud is easily deployed without additional hardware, software, or ACL changes, and expands as your needs grow. FortiToken Cloud is a subscription service available through the purchase of time-based licenses, where all licenses are stackable with co-termed renewal options.

FortiToken Cloud has many innovative features to proactively reduce the risk of data breach while making it convenient and simple for your end-users to use.

Licensing and availability

Free trial license

If you have registered under FortiCloud on support.fortinet.com, FortiToken Cloud (FTC) automatically enables your 30-day free trial license when you log into the FTC portal (ftc.fortinet.com) for the first time. There are two types of FTC time-based trial licenses depending on your FortiCloud account status: premium vs. non-premium trial. For FortiCloud premium accounts, the FTC free trial license can support up to 25 end-users and up to 25 realms; for FortiCloud non-premium accounts, the free trial license can only support up to five end-users and five realms. Neither free trial license offers SMS support.

If, at the end of your free trial, you want to continue using FTC service, you can purchase a license (SKU) that best fits your needs to take full advantage of FTC MFA cloud service offerings. For license information, see Licensing options.

Time-based subscriptions

FortiToken Cloud is a subscription-based MFA cloud service. To take advantage of the service, you must subscribe by purchasing a license (i.e., SKU) based on the number of FTC service end-users in your account for the year. Refer to Time-based SKUs and their services on page 11 for more information.

> - Your FTC license is valid for one year only, and must be activated within one year after the date of purchase.
> - Licenses that are not activated automatically expire one year after the date of purchase.

Time-based SKUs and their services

The following table lists licensing options of the time-based subscriptions by SKU.

SKU	Number of FTC end-users supported
FC1-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 25 users, including 3,125 SMS credits and FortiCare Premium Support, for one year.

SKU	Number of FTC end-users supported
FC2-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 100 users, including 12,500 SMS credits and FortiCare Premium Support, for one year.
FC3-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 500 users, including 62,500 SMS credits and FortiCare Premium Support, for one year.
FC4-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 2,000 users, including 250,000 SMS credits and FortiCare Premium Support, for one year.
FC5-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 10,000 users, including 1,250,000 SMS credits and FortiCare Premium Support, for one year.

SKUs vs. auth clients and realms supported

The following table highlights the number of auth clients (Fortinet products and Web apps) and realms that each of the FortiToken Cloud SKUs supports.

SKU	Fortinet Products	Web Apps (API)	Realms
FC1-10-TKCLD-445-01-DD	Unlimited	5	25
FC2-10-TKCLD-445-01-DD	Unlimited	10	100
FC3-10-TKCLD-445-01-DD	Unlimited	50	500
FC4-10-TKCLD-445-01-DD	Unlimited	200	700
FC5-10-TKCLD-445-01-DD	Unlimited	1,000	1,500

For usage data, see .

Credit-based subscriptions

Credit-based licenses are no longer available for purchase, and hence are no longer applicable to FTC unless you have one that has not yet been activated and the activation window has not yet expired.

Starting from its v.21.2.d release, FortiToken Cloud is phasing out credit-based subscriptions, and replacing them with time-based subscriptions. If you started FTC service with a credit-based subscription and would like to renew your service upon expiration of your subscription, we will help convert your account to a time-based subscription at the time of renewal. Contact the FortiToken Cloud team for how to transition your FTC service from credit-based to time-based subscriptions. For information about the time-based subscriptions, refer to Time-based subscriptions on page 11.

FTC is a subscription-based cloud service. Upon purchasing your service subscription, you receive a License Certificate in .pdf format with a license registration 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. For more information, see Usage on page 119.

Each SKU has an expiration date. 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. Credits that are not used expire on the day when your license expires. So be sure to use up all your credits before your license expires.

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.

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 date 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. Once your credit-based license has expired, you MUST purchase a new time-based license to continue using FTC service. For information on how to transition to a time-based license, see Transition to time-based subscriptions on page 14.
- When your account credit balance is running low, Fortinet will notify you of the situation and prompt you to purchase a new time-based license to continue using your FTC service. For more information, see Transition to time-based subscriptions on page 14.

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 (once 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. You can only view usage data in the account or accounts which you are authorized to log into.

Transition to time-based subscriptions

The time-based annual subscriptions provide a better customer and sales experience, and will replace the old credit-based subscriptions in due time. During the transition to time-based subscriptions, FortiToken Cloud will continue to support existing customers of credit-based subscriptions until their licenses have expired or their credits have been exhausted, whichever comes earlier.

So, if you are an existing customer of a credit-based subscription, you can continue using your current FTC service until your subscription has expired or you have exhausted all the credits in your account. At that point, the FortiToken Cloud team will assist you to switch to a time-based subscription that fits your needs, if you want to renew your FTC service.

As the credits in your credit-based subscription are running low, FortiToken Cloud will alert you of the situation and encourage you to renew your subscription with a time-based subscription. Your SMS service will be stopped once your credit balance has dropped to zero. We highly recommend that you renew your service with a time-based subscription sooner.

Once your credit-based subscription has expired or all credits in your credit-based account have been used up, you'll have a 30-day grace period to renew your service by purchasing a time-based subscription. During the grace period, you are able to use FTC to authenticate your *existing* end-users, but you won't be able to use SMS messaging. Your account will be disabled if you do not renew your subscription 30 days after your license has expired.

You cannot apply a time-based subscription to your existing credit-based subscription if it still has some remaining credits. You must contact FortiCare (FC) to have the remaining credit-based license removed before you can register and activate your new time-based license.

FortiTrust-identity licensing

Starting with its 22.1.a release, FTC supports the IDENTITY user bands license which is part of the FortiTrust framework. As such, FTC will serve all the tokens for FTM.

Licensing options

SKU	Description
FC2-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription, including FortiCare Premium Support for 100-499 users
FC3-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription, including FortiCare Premium Support for 500-1,999 users

SKU	Description
FC4-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription, including FortiCare Premium Support for 2,000-9,999 users
FC5-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription, including FortiCare Premium Support for 10,000+ users

For questions about FortiTrust Identity, see FAQs on page 142.

SMS licensing

Starting with its 22.1.a release, FTC will switch to credits-based SMS accounting. All existing licensed customers will receive a total SMS credit equivalent to their existing SMS balance x 125.

Each time-based license (SKU) allows for 125 SMS credits for each end-user annually. You can view your SMS credit balance on the Dashboard page.

The number of credits that FTC charges for SMS use varies, depending on where the end-user's phone number is registered. For more information, see SMS Rate Card.

Email notification on license balance status

For time-based accounts, once the user count in FTC becomes greater than the user quota, the account will be marked as an expired account.

After the account expires, FTC offers a 30-day grace period. During the 30-day grace period, you (the FTC admin) still have full admin access to the FTC portal, your existing FTC end-users will still be authenticated by FTC, and your account usage will continue to be calculated, but you will not be able to add more end-users to your account.

After the 30-day grace period, if there is no new license applied, the expired account will be marked as disabled, and the existing users will not be able to get authenticated by FTC.

After 90 days of being disabled, the disabled account will be deleted from the FTC system if there is no license applied.

FTC will send out email reminders to the account at 30-, 14-, and 1-day intervals to remind you that the account is going to be disabled.

FTC will send out email reminders to the account at 30-, 14-, and 1-day intervals to remind you that the account is going to be deleted.

FTC also provides a switch button for enabling/disabling email notifications at *Settings > Global > Account Disable/Delete Notification*. The default setting of this feature is to receive all email notifications.

When a credit-based account is going to run out of credits in 30 days, FTC will send out an email to the customer based on the current existing users in FTC.

For credit-based accounts, once the account credit is less than 0, the account is marked as an expired account.

Architecture

The following topology highlights the network architecture of the FortiToken Cloud end-to-end solution.
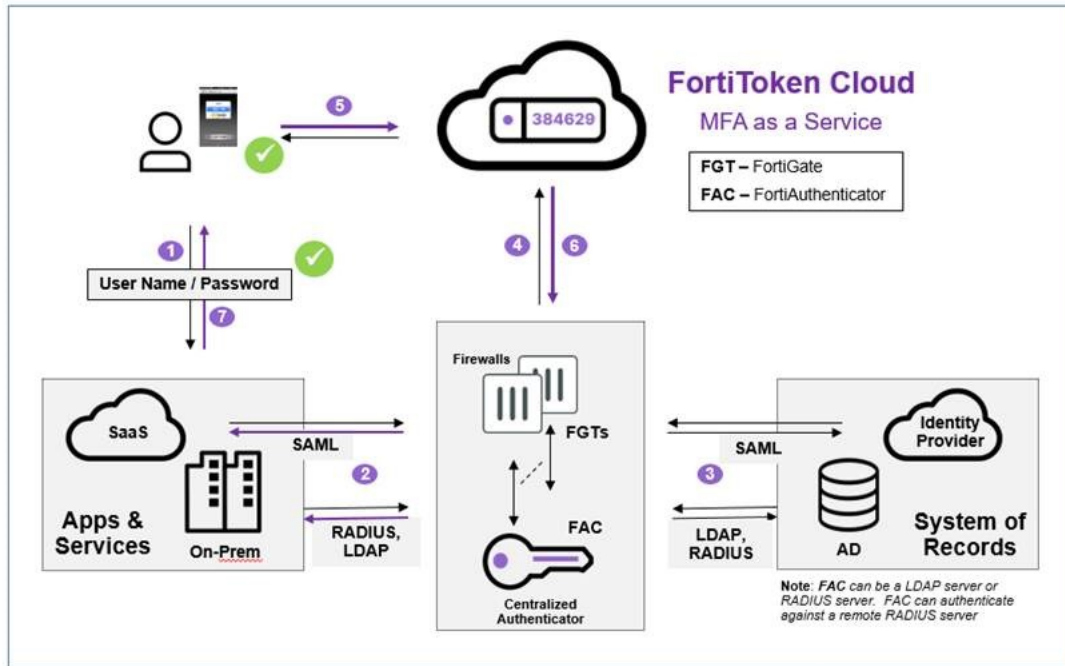
The following describes the workflow of the FTC MFA authentication process:

1. The user enters their username and password which will be first sent over to the connected apps and services.
2. The apps and services will then relay the credentials to the connected Fortinet devices.
3. The Fortinet devices will then consult the connected system of records (e.g., SAML, LDAP, or RADIUS servers) to verify the credentials.
4. Upon successful verification, a FortiToken Cloud code will be sent to the user.
5. Once the user enters the code either manually or via push notification, FTC will verify the code.
6. If the code verification is successful, the Fortinet devices will be notified.
7. At this point, the authentication process is completed, and the user should be able to successfully log into their apps and services.

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)
OU	Organizational Unit
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)

Quickstart guide

This quickstart guide shows how to configure an auth client to use FTC service for end-to-end authentication. The instructions are for configuring a local FortiGate SSL VPN user to log in using MFA with FTC push notification.
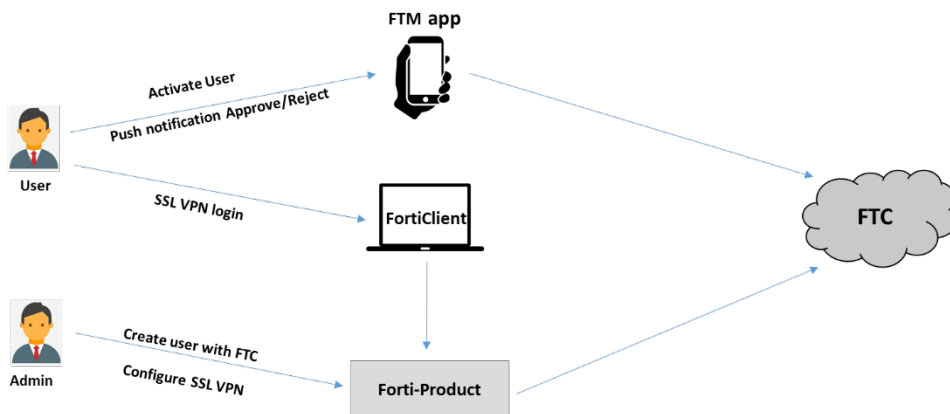
What you need:

- FortiProduct, e.g., FortiGate or FortiAuthenticator (FOS version 7.0.5)
- FortiClient
- FortiToken Mobile app

Step 1: Register FortiProduct (FortiGate)

Register the FortiGate (FGT) under your FortiCloud (FC) account. If you don't have an FC account, go to https://support.fortinet.com/ to register a new FortiCloud account. Register your FGT license under your FC account, and then, if a license file is required for you to use your device (e.g., FortiGate VM), you can download the license file from https://support.fortinet.com/.
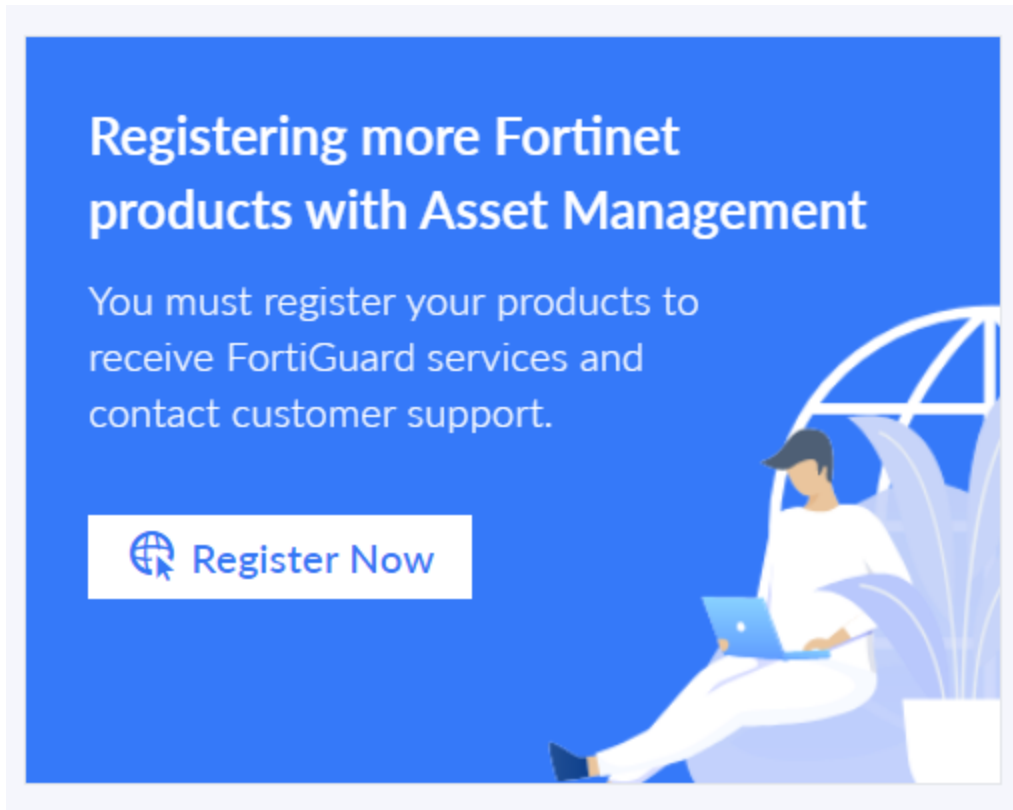
Step 2: Get FTC license

FTC provides free trial licenses and paid licenses. You can choose one based on your preference. The following instructions show you how to get a license:

Option 1: Trial license

If you have registered under FortiCloud from support.fortinet.com, FortiToken Cloud (FTC) automatically enables your 30-day free trial license when you log into the FTC portal (ftc.fortinet.com) for the first time. There are two types of FTC time-based trial licenses: premium trial and non-premium trial. For FortiCloud premium accounts, the FTC free trial license can support up to 25 end-users and up to 25 realms; for FortiCloud non-premium accounts, the free trial license can only support up to five end-users and five realms. Neither of the free trial licenses offers SMS support. This applies to all FTC-supported auth devices.

> If you are a FortiCare Premium customer, you'll notice a Refresh button on the dashboard of the trial mode of FTC. It says either "Update your trial to Premium" or "Extend your premium trial", depending on your account's situation. You can click the button to update your user quota status if you're noticing that the current quota is inconsistent with your FortiCloud subscription.

Web Apps/Max Web Apps

0/0

N/A

Users/Max Users

0/0

N/A

N/A

SMS Credits

0

Expiration Date

October 20, 2022

↻ Update Your Trial to Premium

Web Apps/Max Web Apps

0/0

N/A

Users/Max Users

0/25

0%

N/A

SMS Credits

0

Expiration Date

December 12, 2023

↻ Extend Your Premium Trial
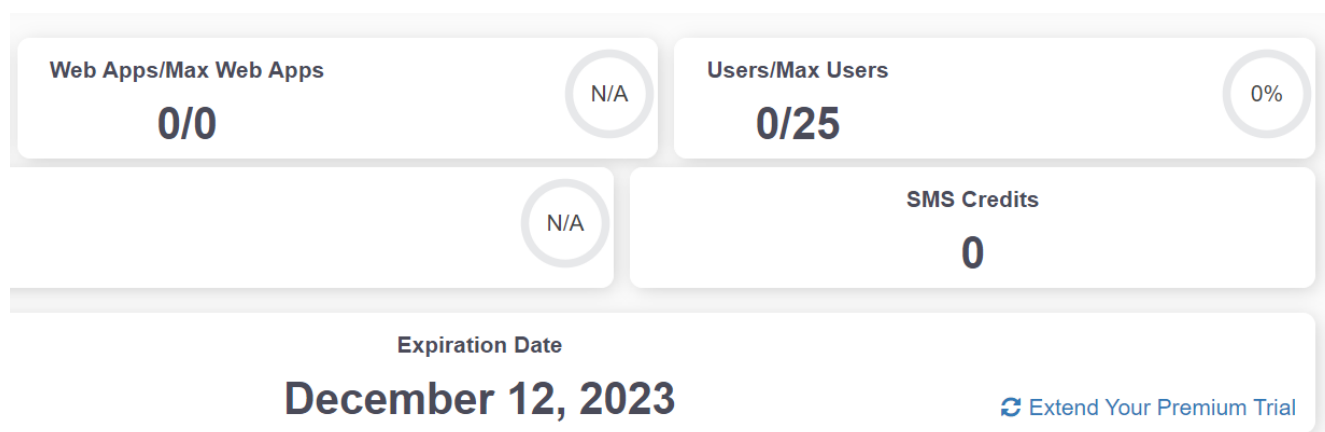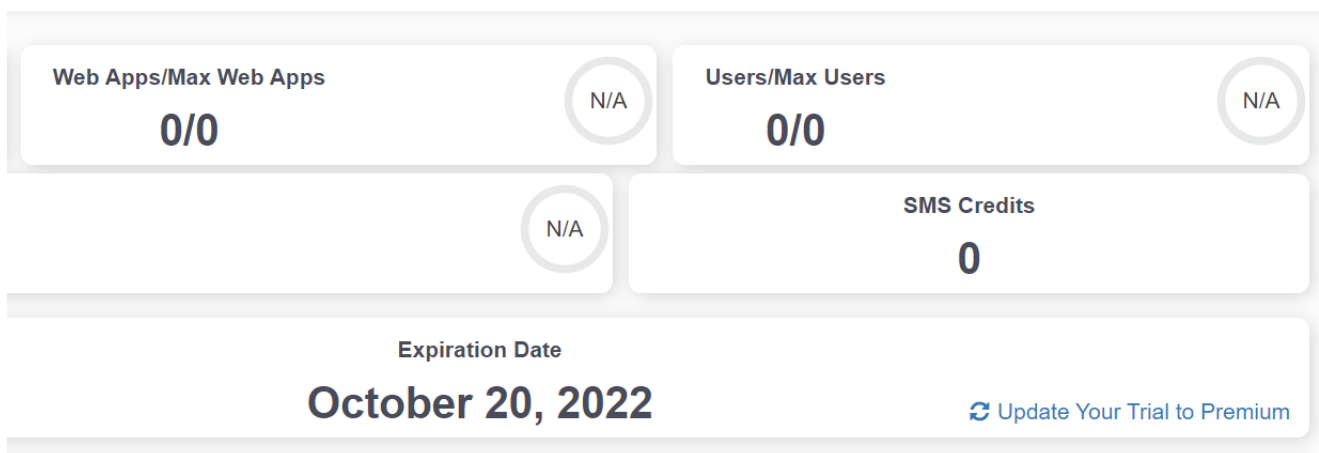
Option 2: Paid license

- How to purchase FTC licenses
- How to register your FTC license

Step 3: Configure SSL VPN and a local user on FGT with FortiToken Cloud enabled for MFA

Configure SSL VPN and a local user on FGT. See SSL VPN setting up on FGT.

Step 4: Activate the local user on FTM app

Install the FTM app on your phone, and activate the user created by scanning the activation code in the email that the user sent with the FTM app. Please make sure system notifications have been enabled for FTM phone (this is used for

receiving notifications).

- FortiToken Mobile on page 41
- Supported FortiToken Mobile apps on page 41
- Activate FTM tokens on page 42
- Activate third-party tokens on page 42
- Use FTM tokens on page 42

Step 5: Configure FortiClient on the login server

Install FortiClient on the server that you are going to use for logging in the user. Configure the SSL VPN tunnel which connects to the FGT from FortiClient.

Link: Connecting from FortiClient to SSL VPN

Step 6: User login authentication

The user logs in with FortiClient on the server. After entering the username and password, you will receive a notification from the FTM app on your phone. Click *Approve*, and then you can log into the system via SSL VPN.

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). See Users on page 100 for MFA methods used by 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 22.
2. Upgrade FortiOS on page 22.
3. Log in to the FortiToken Cloud portal on page 22.
4. Activate FGT VDOMs for FTC service on page 23.
5. Add a local user for FTC service on page 24.
6. Add an admin user for FTC service on page 23.

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 at https://support.fortinet.com/ 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 23.1.a 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 .

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+AFkwFVJdEpidKBIY0xn2LlLPpvSmWRhXhAFAP77
OofUdFSs9eydatFw/BY/4WgCimfir1EOLdtTRjVO9oaCj6LTPBYzZJsyrImmKx7benWG1tTOXWgmktUy88WR02rdUB8Z
ZdBTfDfDoBAL2Q==
    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 .

.

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. Each end-user should 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)".
> - All end-users under the "dn" on LDAP server are synchronized to FTC, which could be a large number. Setting "dn" to a proper level of the LDAP directory can manage the number of users who have FTC enabled.

See Configure wildcard LDAP users for FTC service on page 137 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.
> - FTC supports OTP via email or SMS as an MFA method for end-users with FAC as an auth client, as long as the realm associated with the FAC (or end-user) MFA method is provisioned properly.

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 25.
2. Upgrade FortiAuthenticator OS on page 26.
3. Log in to the FortiToken Cloud portal on page 26.
4. Activate FAC for FTC service on page 27.
5. Add an admin user for FTC service on page 27.
6. Add a local user for FTC service on page 28.
7. Enable FTC service for remote users on page 28

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 at https://support.fortinet.com/ 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 Edit User page (depending on your FAC version), do the following:
   a. 6.0, select Token-based authentication > FortiToken > FortiToken Cloud.
   b. 6.1, select Token-based authentication > FortiToken > Cloud.
   c. 6.2—6.3, select Token-based authentication > FortiToken > Cloud > Choose Email or SMS.
   d. 6.4 and later, select One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS if Mobile was chosen.
8. Click **User Information.**
9. Enter the user's email address or SMS information as needed based on the option you chose earlier.
10. 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 Edit User page (depending on your FAC version), do the following:
   a. 6.0, select Token-based authentication > FortiToken > FortiToken Cloud.
   b. 6.1, select Token-based authentication > FortiToken > Cloud.
   c. 6.2—6.3, select Token-based authentication > FortiToken > Cloud > Choose Email or SMS.
   d. 6.4 and later, select One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS if Mobile was chosen.
7. Click **User Information.**
8. Enter the user's first name and last name.
9. Enter the user's email address or SMS information as needed based on the option you chose earlier.
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.

Enable FTC service for remote users

If you already have some remote users configured, you can also enable FTC service for those remote users (e.g., remote LDAP, RADIUS and SAML users).

For more detailed configuration instructions regarding remote servers and users, refer to the FAC cookbook https://docs.fortinet.com/document/fortiauthenticator/6.4.0/cookbook.

1. From the FAC menu, click Authentication>User Management>Remote Users.
2. On the top right, select the type of user (e.g., LDAP, RADIUS, SAML, etc.).
3. Click in the row of the user you wish to edit.
4. On the Edit User page (depending on your FAC version), do the following:
   a. 6.0, select Token-based authentication > FortiToken > FortiToken Cloud.
   b. 6.1, select Token-based authentication > FortiToken > Cloud.
   c. 6.2-6.3, select Token-based authentication > FortiToken > Cloud > Choose Email or SMS.

      d. 6.4 and later, select One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS if Mobile was chosen.

5. Click User Information.
6. Enter the user's email address or SMS information as needed based on the option you chose earlier.
7. Click OK.

Main features

FortiCloud SSO

Integration with FortiCloud provides unified single sign-on (SSO) access to all your Fortinet cloud service offerings.

Free trial licenses

FTC offers 30-day free trial licenses, which can support up to five FTC end-users for FortiCloud non-premium accounts and up to 25 end-users for FortiCloud premium accounts. (SMS messages are not included.)

Time-based annual subscriptions

FTC offers time-based subscriptions that are stackable and co-termed, giving you the flexibility to scale up your FTC MFA service with ease.

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.

Global administrator and sub-admin support

FTC now enables the global admin to create sub-admin account to better allocate and manage resources across all the accounts under management.

Access to all accounts by admin users

As the global admin, you are able to access all FTC accounts belonging to your organization, choose which of your accounts to open upon login, and switch to any of your other accounts during a session.

Realm support

FTC enables admin users to create realms to effectively allocate resources and better manage their end-users.

Multi-factor authentication (MFA) for FGT and FAC devices

FTC provides a cloud-based MFA solution for all your Fortinet products, such as FortiGate (FGT) and FortiAuthenticator (FAC), and third-party web apps as auth clients.

Integration with FOS 6.2

FTC works seamlessly with FortiOS (FOS) 6.2.x and later.

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 end-users when they have breached their specified MFA failure threshold, ensuring security and integrity of your account.

Temporary token

This new feature allows you to enable your end-users to use temporary tokens for MFA authentication when they do not have their authentication devices with them, while keeping the end-users' existing authentication methods intact. If an end-user forgets to carry his/her FTM device around and needs to log into the firewall or SSLVPN using MFA, you can enable the temporary token for the user and set the expiration time. The user can log into the firewall or SSLVPN using the temporary token until it expires. The user can get temporary tokens by email or SMS.

Disabling MFA after account disabled

Starting from its 2.5 release, FortiToken Cloud can enable existing users in disabled accounts to bypass MFA. There have been many customer cases when users are locked out due to expired licenses or exceeded quotas. With this feature, you are able to delete users by performing a user sync or delete a particular user. In the portal, you are able to change user settings including bypass MFA. After MFA is bypassed, auth requests should succeed.

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.

Support for remote FortiGate users

You can configure FortiGate wildcard LDAP users to use FTC for MFA.

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 administrator can view daily, monthly, and current usage data easily from the GUI.

Support for HA clusters

FTC supports FGT and FAC HA cluster configuration. You can add or remove auth devices to or from the FTC portal. 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.

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

Many FTC end-users have different usernames in different applications and different domains. For the same token, a single FTC user may have different usernames in different FTC auth clients. FTC now allows for different usernames to be attributed to the same user (i.e., same person) so that only one token (FTM or FTK) needs to be assigned to that same user. It does this by providing an Auto-alias by Email option, which, once turned on, enables FTC to automatically put usernames into an alias if they use the same email address.

Realm-based user quota

The global admin of an account with a time-based license can allocate user quota by realm to effectively manage their assets and end-users.

If you are an MSSP (Managed Security Service Provider), you can split out your user quota to sub-accounts. Sub-account holders can create their own passwords and have their private login portal. They can use MFA, bypass, block, and realm configurations to manage their own end-users. The MSSP can manage all your sub-accounts using the FortiToken Cloud portal.

Export of logs in .CSV

You can export FTC authentication and management logs in .CSV format for record-keeping and sharing.

SMS usage

The SMS Log page enables you to view your SMS usage.

Migration of FTM licenses to FTC

Starting from FOS 7.0.5, FTM licenses and their users on FortiGate can be seamlessly migrated to FTC without any user token change.

Compatibility

Compatible Fortinet applications

FortiToken Cloud 23.1.a 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
- FortiManager 7.2.2 or later
- FortiAnalyzer 7.2.2 or later
- FortiToken Mobile (FTM) for iOS 4.5.3 or later
- FortiToken Mobile (FTM) for Android 4.6.0 or later
- FortiToken Mobile (FTM) for Windows 4.1.1

- 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.
- FortiToken Cloud does not work well with FortiOS 7.0.2. We recommend upgading to FortiOS 7.0.5 or later for best performance.
- For end-users with FortiAuthenticator 6.3.0 or later as an auth client, FortiToken Cloud supports OTP via email or SMS.

Supported browsers

FortiToken Cloud 23.1.a 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 important notes regarding the use of FTC.

Credit-based licenses no longer available for purchase

Credit-based licenses are no longer available for purchase, and hence are no longer applicable to FTC unless you have one that has not yet been activated and the activation window has not yet expired.

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 auth clients are FTC-supported auth clients, such as Fortinet products or third-party Web apps.
- The auth clients are assigned to the same realm in FortiToken Cloud.

The same end-user created on the auth clients can be of different usernames.

For more detailed information, see One Token shared by different auth clients on page 44 and A single FTC user in multiple auth clients on page 35.

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 the so-called "a-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 points 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 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 that it has 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.

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 FTC account of your organization that has logged in to the FTC portal first 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 realms in order for them to view and manage realm resources.

For more information on how to create admin groups and grant permissions to sub-admins, see Administrators on page 97.

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 users' phone numbers. Therefore, FTC does support SMS MFA for FortiAuthenticator end-users configured as remote users in a remote LDAP server.

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 because FAC differentiates the same username populated by multiple user sources to FAC. To remove the prefix and the suffix from a FAC username, first select the FAC username, and then click the **"Hide Full FAC username'** button.
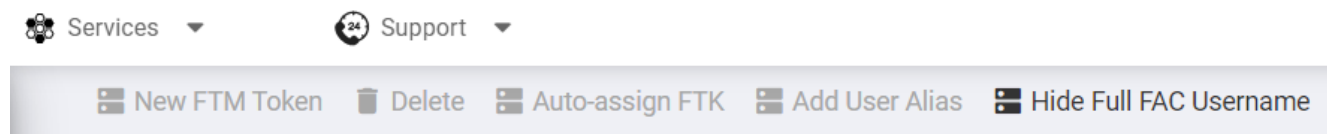
How to use FortiClient

FortiToken Cloud supports FortiClient 6.2.1 and later for both auto push and manual OTP. To use FortiClient with FortiToken Cloud, you must make sure that "Notification" is enabled on the FortiToken Mobile app on your mobile device. For auto push, you must also ensure that "push" is enabled (Enable push) in the Realm FTM Setting on the FortiToken Cloud portal.
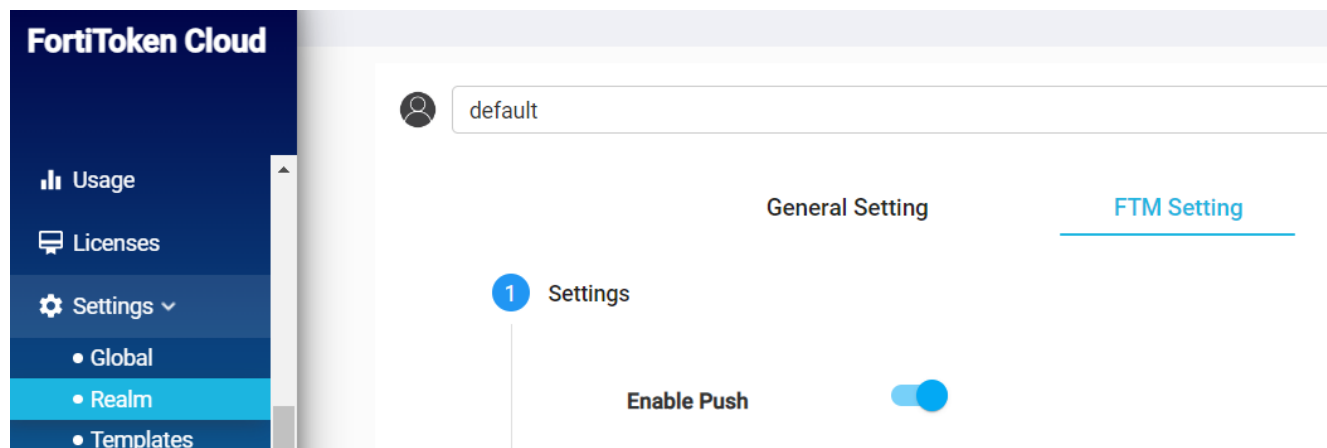
Use auto push

Upon entering your username and password, do the following:

1. On FortiClient, log in with your username and password.

2. On your mobile device, press the **Approve** button.
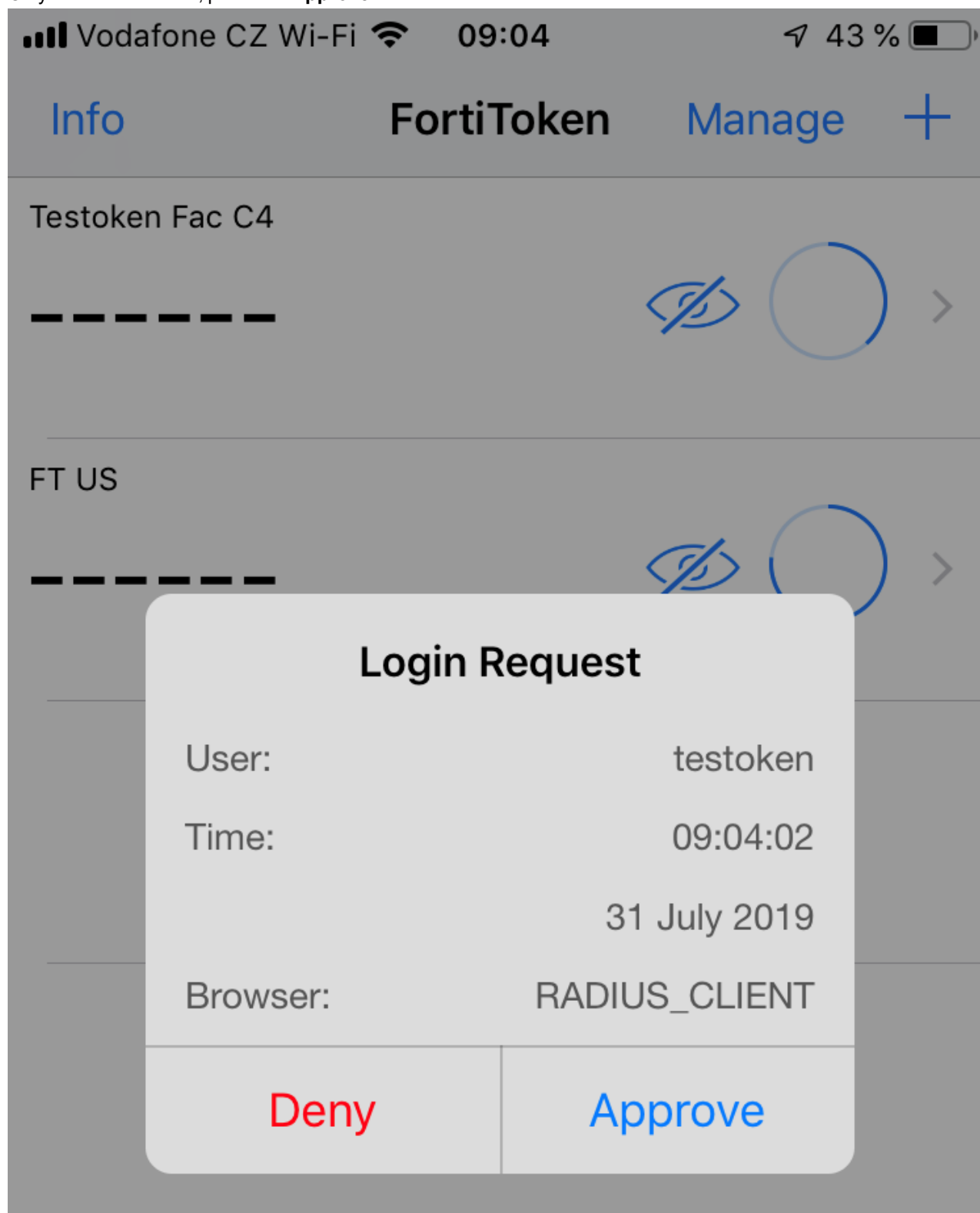
3. Wait for FortiClient to complete the remote access login.

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. Wait for FortiClient to complete the remote access login.

Enabling/Disabling users on FortiGate

If you have users with FortiToken Cloud for 2FA enabled on FortiGate, they can not be deleted from the FTC portal if you disable them on the FortiGate because FTC retains the users regardless of the their status on FGT. If you want to remove the users from FTC, you can do one of the following:

- Delete the user from FGT.
- Revoke the token from the FGT user.
- Delete the user from the FTC portal (note that this method will not delete the user on the FGT side, so it is best to perform this operation on the FGT.)

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 FortiToken Mobile apps on page 41.
- Activate FTM tokens on page 42.
- Activate third-party tokens on page 42.
- Use FTM tokens on page 42.

Supported FortiToken Mobile 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
FortiToken Mobile for iOS 4.5.3 and later	Apple iOS 9.x, 10.x, and 11.x	iPhone, iPad, and iPod Touch
FortiToken Mobile for Android 5.1.0 and later	Google Android 5.0 and later	Android phone and tablet
FortiToken Mobile for Windows 4.1.1	Windows 10 version 14393.0 or higher	Windows PC, tablet, and phone

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 for iOS:

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

To get FTM for Android:

1. Start your Android device.
2. Go to **Google Play**.

3. Browse for **FortiToken Mobile** version 5.1.0 or later.
4. Download and install the app.

To get FTM for Windows:

1. Start your Windows device.
2. Go to **Microsoft Store**.
3. Browse for **FortiToken Windows** version 4.1.1 or later.
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 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 guide can be referenced for more details about activating FTM tokens: https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/776309/activating-fortitoken-mobile-on-a-mobile-phone.

Activate third-party tokens

The steps for activating a third-party token are the same as those 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.

Please refer to our REST API quickstart guide for more information on how to create a third-party user https://docs.fortinet.com/document/fortitoken-cloud/latest/rest-api/698584/get-access-token-and-create-users-from-web-apps.

Use FTM tokens

Upon opening the FTM app on your iPhone, your token will be visible on 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 an 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 after you pass the MFA process.

For more information on FTM Push with CLI configuration for FortiGate, please refer to:
https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/927108/fortitoken-mobile-push.

Use cases

One Token shared by different auth clients

You can share the same token used by one end-user but with different auth clients. A single end-user can be defined by the same user name on different auth clients but in the same realm or the same email address on different auth clients. If multi-realm mode is enabled, the newly registered auth client will be assigned to a new realm; if multi-realm mode is disabled, the newly registered auth client will only be assigned to the "default" realm.

For example, if you have one user named "user1" with FTC MFA on FGT, you need to create a new user named "user1" with FTC MFA on FAC, "user1" can share the first token without allocating a new token for the "user1" on FAC if the auth client for FGT and FAC are under the same realm on FTC. Having the same user name is the default condition for sharing the same token between different auth clients on FTC. The same email address can be set for token-sharing from FTC as well.

This use case also applies when you have the same auth device but the auth device serial number is changed. If there are multiple users with FTC MFA on one auth client, but the auth client serial number is changed for any reason, the users can be synced to FTC with the new serial number under the same realm as the auth client with the preceding serial number. Then all users can keep the previous token without going through the re-activation process.

> If you are trying to add a new FortiGate and are having difficulties with getting the new FortiGate's auth client(s) to show up, it may help to use the `exec fortitoken-cloud update` command in the CLI on the new FortiGate.

1. Create a user "user1" in the auth client "client1", which is assigned under the realm "realm1". For more information on creating a user under auth client for FTC, refer to https://docs.fortinet.com/document/fortitoken-cloud/latest/admin-guide/367002/add-a-local-user-for-ftc-service.
2. Activate the token in the FortiToken Mobile.

3. Create a user with the same username "user1" in another auth client "client2", which is also assigned under the same realm "realm1". Note that if you are trying to assign the token on the FortiGate, there may be a warning message that says that you don't have enough resources to add the new user. This is a false negative and you should still click "OK" after editing the user.

4. The activated token will also be assigned to the newly created user in "client2" which can use MFA login.

Once you have completed the steps above, the auth client count for the user should be higher than 1 and it should look like this:

Auth Client Count

1

2

And if you click the number, you should be able to see the details about the user having more auth clients under it:

Auth Client List for User: test_ftc

Select	Username	Email	Mobile Number	Name
☐	test_ftc	●●●●●●●@fortinet.com	+1408●●●●●●●	MyAuthClient
☐	test_ftc	●●●●●●●@fortinet.com		FGVMULTM22002839-root

Change separate tokens to a single token

When you change the Multi-realm Mode from "enable" to "disable", your FTC will be changed from share-token to single token login.
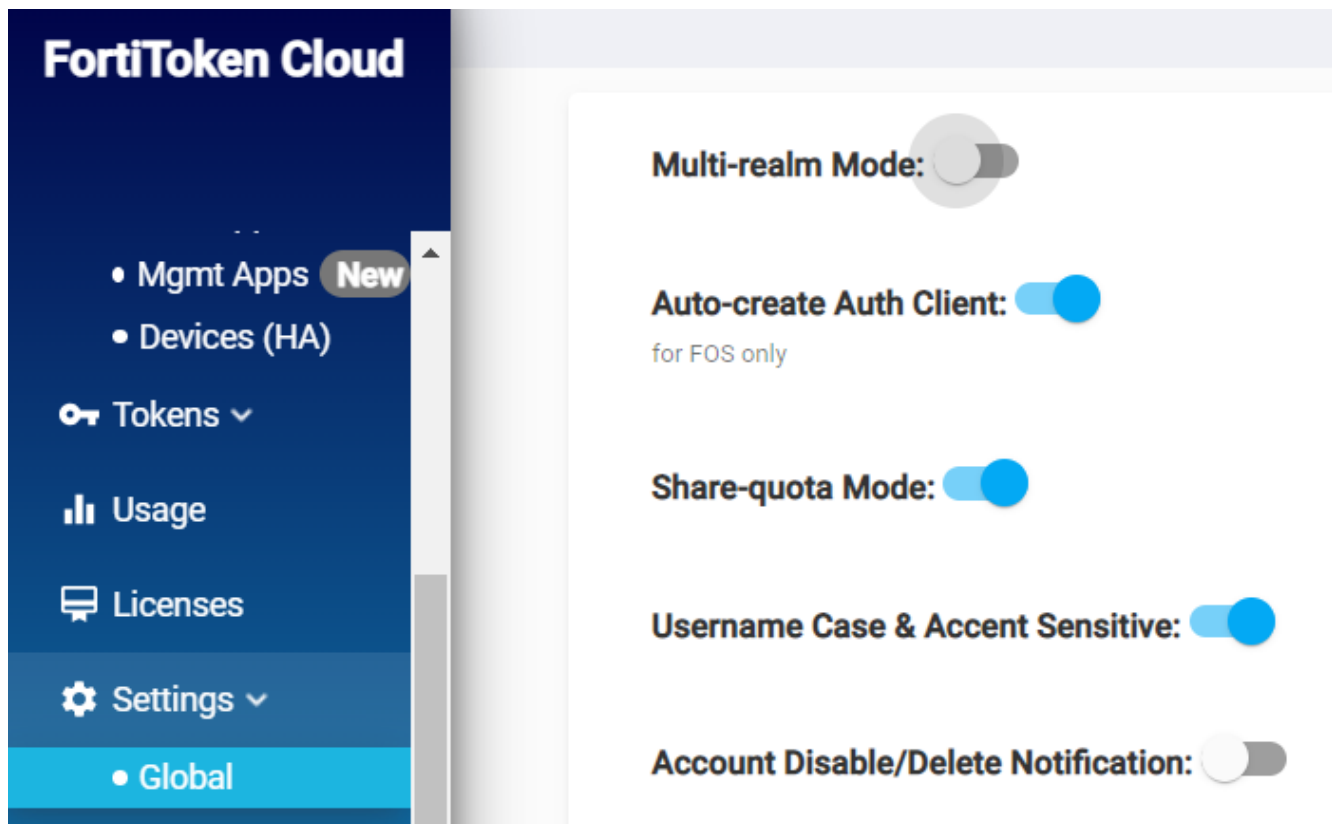
1. FortiGate1 with the serial number (FG200ETK1990xxxx) and FortiGate2 with the serial number (FG300ETK1990xxxx) are registered under the FC account (fortinet_account@gmail.com).
2. As long as the realm has enough resources, FTC will automatically create two realms: "FG200ETK1990xxxx-root" and "FG300ETK1990xxxx-root", and FGT1 and FGT2 will be assigned to those two separate realms.
3. In this case, a user created in FGT1 named "Jack Talyor" is assigned one token, and a user created in FGT2 named "Jack Talyor" is assigned a new token. They are two separate users with the same username but use separate tokens.
4. If you want to switch to one-token login mode (Users with the same username use one token only), the FTC admin can move FGT1 and FGT2 to the same realm, for example, the "default" realm, from the two realms "FG200ETK1990xxxx-root" and "FG300ETK1990xxxx-root".
5. The users will be merged on the Users page, the two users named "Jack Taylor" will be merged into one "Jack Taylor" and the auth client count will increase to "2". The same token will be shared by the two users named "Jack Taylor". By default, the token will be kept for the auth client migrated to the "default" realm first, and the token for the user in the second migrated auth client will be removed.
6. Right now, "Jack Taylor" will only need one token to log into the two FGT resources.
7. Additionally, if you want to always use one-token login mode, the FTC admin can navigate to Settings>Global and disable Multi-realm Mode. He must also move all existing auth clients to the same realm, for example the "default" realm.
8. After Step 7, the existing auth clients will use single token mode and newly assigned auth clients will also migrate to the "default" realm and use single token mode.

Independent token

When Multi-realm Mode is enabled, newly registered auth clients will be assigned to new realms. This function is very convenient for admin users who want to become an MSSP (Managed Security Service Provider).

1. FortiGate1 with serial number (FG200ETK1990xxxx) and FortiGate2 with serial number (FG300ETK1990xxxx) are registered under the FC account (fortinet_account@gmail.com).
2. As long as the realm has enough resources, FTC will automatically create two realms: FG200ETK1990xxxx-root and FG300ETK1990xxxx-root, and FGT1 and FGT2 will be assigned to those two separated realms.
3. In this case, a user created in FGT1 named "Jack Talyor" is assigned one token, and a user created in FGT2 named "Jack Talyor" is assigned a new token. They are two separate users with the same username but use separate tokens.
4. If the two "Jack Taylors" exist in two realms, some events could be confusing. For example, if "Jack Taylor" is deleted from FGT1, the "Jack Taylor" still exists in FTC. This scenario looks like "Jack Taylor" has never been deleted on FGT1. In fact, the "Jack Taylor" is no longer in FGT1, but only exists in FGT2.
5. Solution: Log into FGT2 and delete "Jack Taylor". Then execute the console command "exec fortitoken-cloud sync" in FGT. This will remove the user "Jack Taylor" in FTC. After deleting the user in FGT2, assign auth client FGT1 and auth client FGT2 to the same realm, for example, the "default" realm. This will prevent the situation from happening.

Auto-Alias features—Use the same email address

Many FTC end-users with the same email address have different usernames in different applications and different domains. For the same token, a single FTC user may have different usernames in different FTC auth clients. FTC allows for different usernames to be attributed to the same user (i.e., same person) so that only one token (FTM or FTK) needs to be assigned to that same user. It does this using its auto-alias by email option.

Auto-alias by email is disabled by default, but you can enable it using the following procedures:

1. On the side menu, click Settings>Realm to open the settings page of the current realm.

   ⚙ Settings ⌄
   • Global
   • Realm
   • Templates
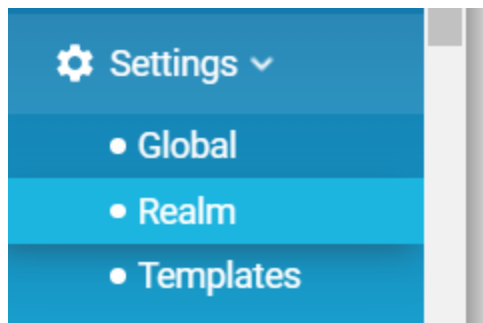
2. Scroll down until you see the Auto-alias by Email option near the bottom of the page.
3. Click the Auto-alias by Email button to enable it.

General Setting	FTM Setting

MFA Method	FTM
Max Login Attempts Before Lockout	8
Lockout Period	60
Enable Bypass	⊘
Auto-alias by Email	●
Adaptive Auth Profile	-- None --

Once the Auto-alias by Email feature is enabled, all newly created usernames with the same email address are automatically set as an alias under the same username. The existing usernames with the same email address will not be grouped into an alias, but you can manually set up alias users. See Users on page 100.

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 enabled.

FTC also allows you to set up user aliases manually. In this way, the users are not required to have the same email. To enable this feature, just follow the steps below:

1. On the side menu, click Users to navigate to the Users page.
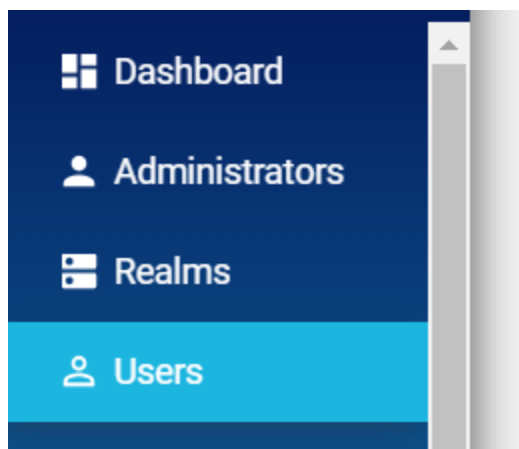
2. Select any number of users in the same realm by clicking the checkbox in the first column.
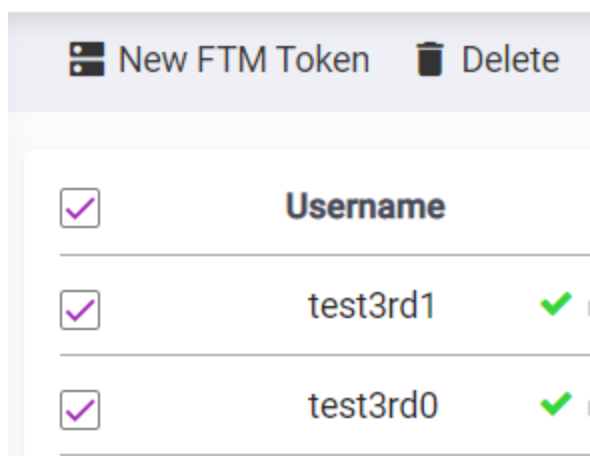
3. Click the Add User Alias button in the top bar which should be enabled if the users are in the same realm.
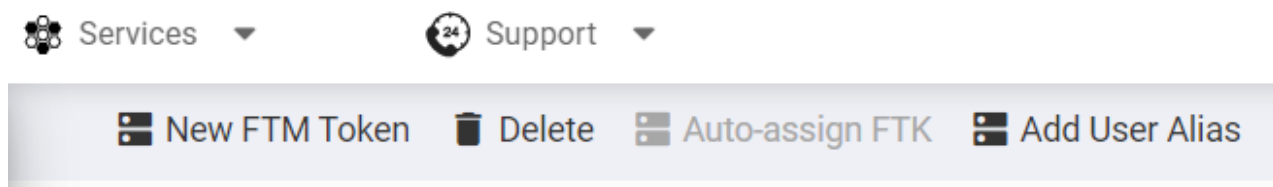
4. Select the base username which will be displayed in the Users page, and click Next>Confirm.

Please choose a base user for all the other selected users

test3rd1

| Next | Cancel |

Once the User Alias is formed, the base user's username changes to boldfaced and the Auth Client Count will be increased based on how many users are selected in the previous step.

	Username	Status	MFA Method	Token SN	Notification Method
	test3rd1	✔ 🔓 ⇄ 🔑 🕐	FTM	FTCT1TMLNEWB958D	Email

Mobile Phone	Auth Client Count	Create Date
+15556667777	2	5/4/2023, 3:21:33 PM

To remove the User Aliases that have different email addresses, just follow the steps below:

1. Find any user alias you want to remove, and click the number in the Auth Client Count column.

Auth Client Count

2

2. Select any users you want to remove from the user alias group by clicking the checkbox.

Auth Client List for User: test3rd1

Select	Username
☐	test3rd1
☑	test3rd0

3. Click the Remove Alias button.

    Remove Alias   Close

To remove the User Aliases that have the same email address, be sure to disable the Auto-Alias feature first in the Realm setting page. Once the auto-alias feature is disabled, the steps are the same as before.

Split user quota to different realms

FortiToken Cloud enables you to split out user quota to sub-accounts. Sub-accounts can also use functions like MFA, bypass, block, and realm configuration. This is the so-called "Managed Security Service Provider" capability. The host account holder can create sub-accounts and assign a user quota to those sub-accounts. Each sub-account can create its own password and has its own private login portal. The account holder is the security service provider and can manage all of the sub-accounts on the FortiToken Cloud portal.

To create a sub-account:

1. Log in to ftc.fortinet.com using the host account holder's credential.
2. Click the email username in the top-right corner, and select "My Account".

    My Account

    Security Credentials

    Logout
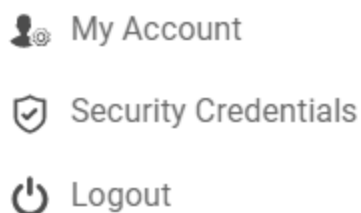
3. The browser will be navigated to support.fortinet.com automatically.
4. Click "Manage User" in the left sidebar to open the sub-users list.

    Account
       Account Profile
       Change Account ID (Email)
       Manage User
       My Account (IAM version)

    Manage User

    Current Users
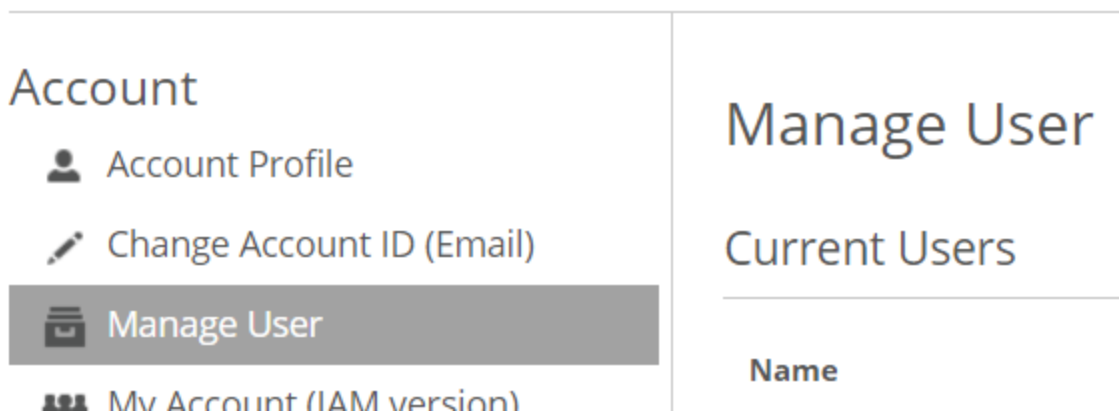
    Name

5. In the upper-right corner of the sub-users list, click the Add user button.

6. Enter the sub-user client information, including "User Name", "Email (Account ID)", and "Telephone". Additionally, enter some details, such as "purchased 10 user quotas", in the Description field.

7. Select "Limit Access", which allows you (the host account holder) to assign specific devices to this sub-user, like a FortiGate for creating users.

8. Click *Save.*

9. The sub-user clients will receive an email, asking them to create their own passwords for logging into ftc.fortinet.com.

10. After sub-users are created, the host account holder can assign resources to sub-users, including user quotas, realms, and auth clients. For more details of assigning resources, see Administrators on page 97.

The following steps show how to use this feature:

1. The host account holder creates a sub-user "subuser1" by using the provided client's email. Clients can use their own email and password to log into ftc.fortinet.com, and can see the user quota assigned to them by the host account holder.

2. The host account holder can assign a user quota to a client in the Realms page.

    a. Navigate to the Realms page, and click Add Realm to add a new realm.

    b. Mouse over the newly created realm, select Edit Realm in the tool bar on the right.

    c. Assign a user quota by entering a number or dragging the bubble point, and click OK.

3. The host account holder can assign the realms to a client in the Administrator page.

   a. Navigate to the Administrator page and click Add Admin Group.
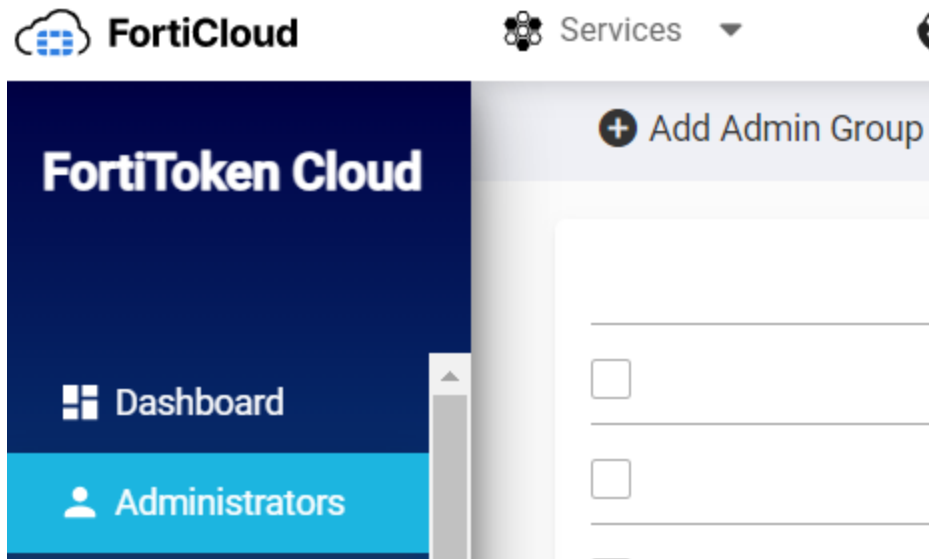
   b. Edit the admin group by clicking the new group name.

   c. Assign to this group the sub-account in Admins in Group and the realm in Managed Realms which are created in Step 2, and click Close.
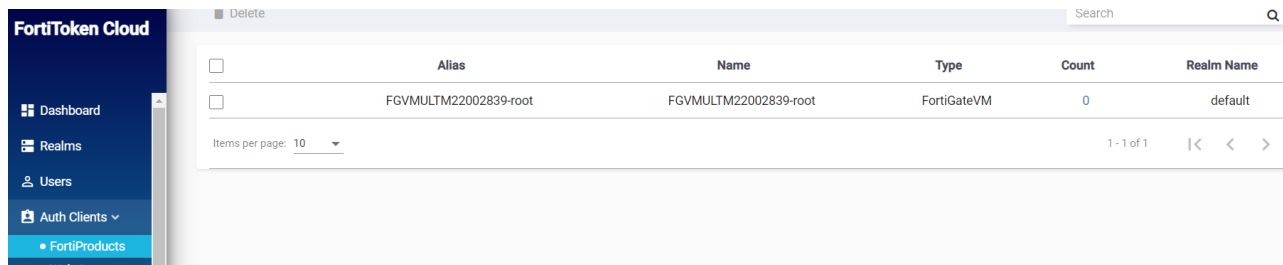
4. The host account holder can assign auth client to the client by selecting Auth Clients>FortiProducts.
5. The client can see the users created by the host on the assigned FortiProduct, for example, FortiGate.
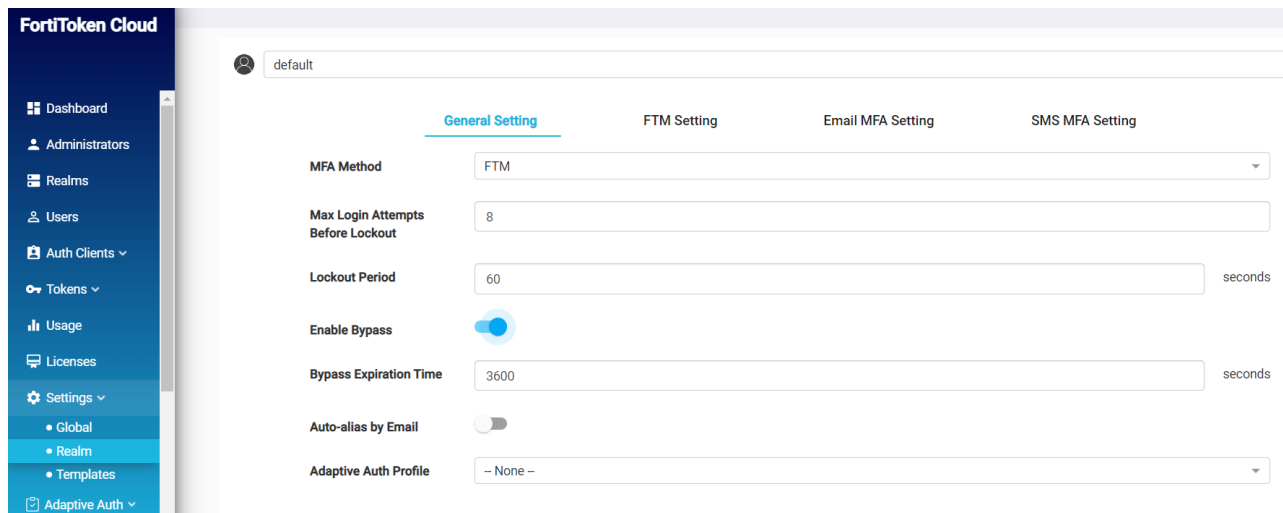
FTC account lockout (2FA)

You may find yourself unable to log in as an FGT admin.

1. For example, Jack is an FTC admin and manages two FortiGates FGT1 and FGT2. He has enabled MFA for FGT admin login. When the FTC account is validated, everything is working fine.

2. By missing the disabled email notification sent by FTC, Jack's FTC account is disabled.

3. In this situation, the MFA login function is blocked. The behavior is that MFA login automatically fails after the user enters the correct username/password.

4. Jack can't log into the FGT admin portal to see users who are enabled for MFA login authentication.

5. Jack is allowed to log into his account and perform some limited activities, including enable bypass, setup bypass for users, and delete auth devices.

6. Log into the FTC portal, ftc.fortinet.com, navigate to Settings>Realm, find the Realm which contains the users for whom Jack wants to set up bypass, and click "Enable Bypass".

7. Navigate to the Users page, find the FGT admin user, click "Edit User", and click "Enable bypass" in the "Status" row. Note that the "Enable Bypass" option for the realm you're working with from Step 6 must be turned on for FTC to allow you to turn on the bypass button on the Edit User page.

Edit User

Name	test_ftc
Auth Method	FTM
Notification Method	Email
Token SN	FTCTU2U7ST0GXX0N
Email:	test@test.com
Mobile Phone	🇺🇸 ▾ (201) 555-0123
Status	✓ 🔓 ⇄ ⚷
Last MFA	{}

Apply   Cancel

8. Now, the FGT admin is not required to use MFA to log in anymore. Jack can log into the FGT admin portal and remove the FTC setup in the admin user until he renews the license.

Manage access to FTC

Admin Group

As an FTC global administrator, you can view your associated sub-accounts and assign realms to different admin groups for better realm management. For example, you can manage your headquarters realm and several realms assigned to its local branches. You can create one sub-account for each of your branch administrators and each admin group, and then assign realms to each admin group.

1. Log into the master account which is the global administrator or the first sub-admin inside your master account. Only global administrator or the first sub-admin can edit the Administrators page.
2. On the Administrators page, identify the group of interest and mouse over it.
3. From the slide-in tool bar, click the Edit button to open the Edit Admin Group dialog.
4. To change the group name, highlight the Group Name and type a new name over it.
5. To modify the description of the group, highlight the Group Description, and type a new one over it.
6. To add more sub-admins to the group, click Add Admin.
7. To delete a sub-admin, identify the sub-admin and click x (Delete).
8. To add more realms to the group, click Add Realm.
9. To delete a realm, identify the realm and click x (Delete).
10. Click Close.

Add an admin group

On the Administrators page, click Add Admin Group to open the Add New Admin Group dialog.
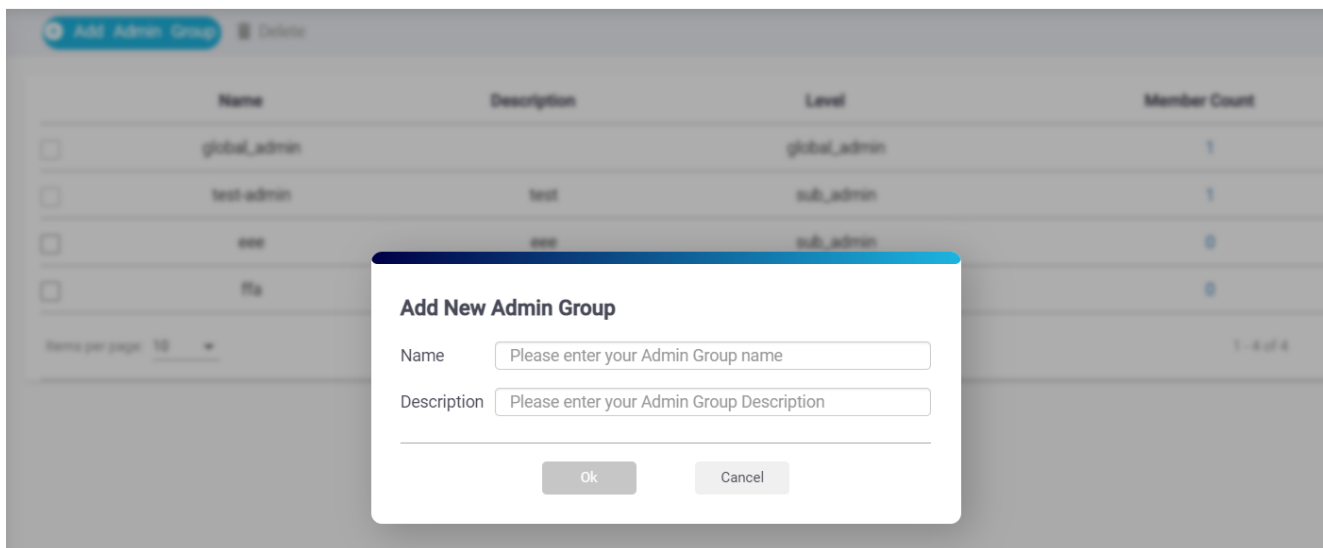
1. Specify the group name.
2. (Optional) Enter a brief description of the group.
3. Click OK.

> 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.

Add realms to an admin group
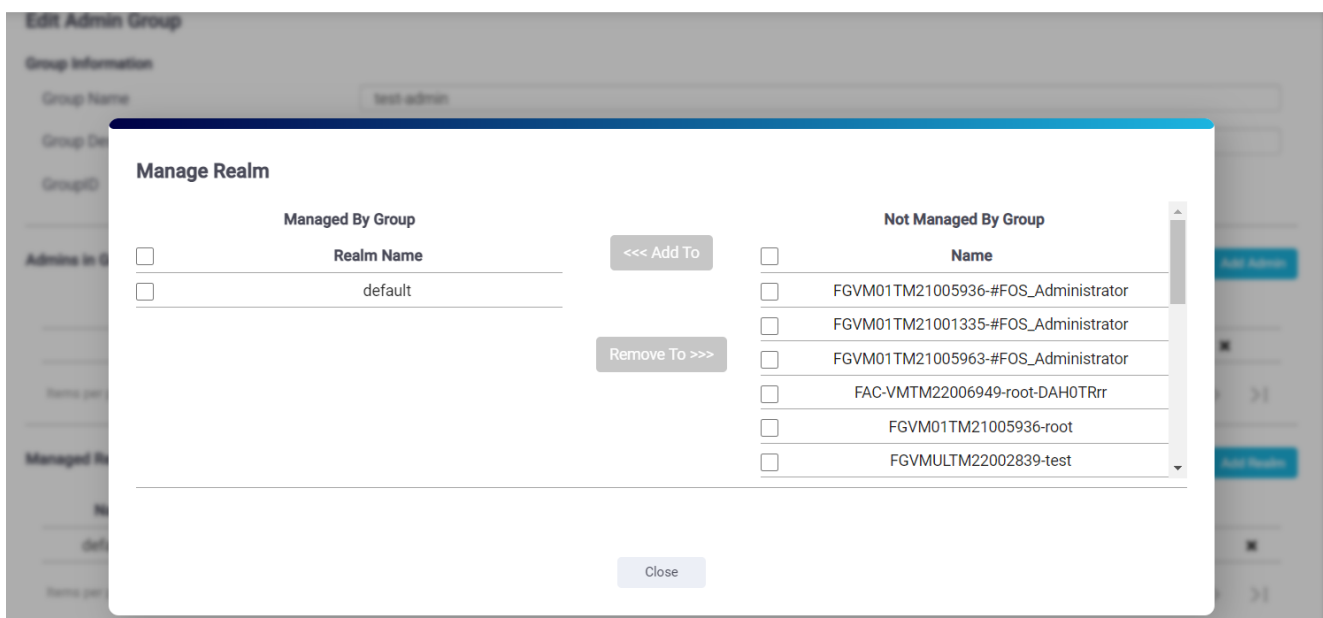
1. Click Add Realm to open the Manage Realm dialog.
2. Under Not Managed by Group, select the realm(s) of interest and click Add To.
3. Click Close.

Control risky conditions

Adaptive Authentication

You can bypass OTP verification of MFA under certain "safer" conditions and deny such attempts under some otherwise "risky" conditions. You can pre-configure OTP verification of MFA based on trusted subnet/geo-location and time of day/day of week. For more details about how to configure it, go to Adaptive authentication on page 120.

Create adaptive authentication policy

1. From the main menu, click Adaptive Auth > Policy to open the Policy page.
2. On top of the page, click Add Policy to open the Add New Policy dialog.
3. Make the desired entries and/or selections.
4. Click Confirm.

Create adaptive authentication profile

1. Click Adaptive Auth > Profile to open the Profile page.
2. On top of the page, click Add Profile to open the Add New Profile dialog.
3. Make the entries and/or selections.
4. Click Save.

Apply adaptive authentication profile to an auth client

1. From the main menu, click Auth Clients > FortiProducts.
2. Highlight the auth client of interest and click the Edit button to open the Edit Client dialog.
3. Select an adaptive auth profile.
4. Click OK.

Apply adaptive authentication profile to a realm

1. From the main menu, click Settings > Realm.
2. Ensure that the General Setting tab is selected.
3. Select an adaptive auth profile.
4. Click Apply Changes.

Last login

The Last Login feature enables you to let end-users use trusted IPs or subnets to log in by bypassing the MFA requirement within a specified time period.

To enable the Last Login feature in Adaptive Authentication Policy:

Subnet Filter Please click here to check supported devices.

Subnets ❓   IP addresses, IP ranges or CIDRs   ➕

☐ No IP ❓

8.8.8.8 ✕

Last Login ❓   ⬤

MFA Interval   8   hours

Schedule

Weekdays   ☑ **Everyday**

☑ **Monday** ☑ **Tuesday** ☑ **Wednesday** ☑ **Thursday** ☑ **Friday**
☑ **Saturday** ☑ **Sunday**

Timezone   (GMT-08:00) Pacific Time (US & Canada)

Time Range   ☑ **All day**

From 00:00 📅   **To** 23:59 📅

Confirm   Cancel

1. Add the new policy by click Add Policy in Adaptive Auth > Policy page.
2. Specify a unique name and select Bypass MFA in Action section, and select Subnet Filter.
3. Enter the IP or subset in Subnets section, and click Enter to confirm (Note: The IP or Subnet must be supported by the FortiProducts).

4. Click Last Login and specify a reasonable MFA Interval time period (Note: The range of this period is from 1 to 72 hours.)

5. Select a schedule configuration set in Schedule section

6. Click confirm.

7. Add the newly created policy to a profile and select the same action, i.e., Bypass MFA.

8. Apply the newly created profile to any auth clients (including FortiProducts and Web Apps) and any realms whose users are going to use those trusted IPs or Subnets.

Impossible travel

The Impossible Travel feature enables FTC to detect and block suspicious login attempts. Upon detecting a login request coming far away from the normal geographical location, for example, a login request from Russia for a device used by an employee who is based in the United States, FTC will block it. Using this feature, FTC can effectively identify suspicious sign-in attempts based on the distance and time elapsed between two subsequent user sign-in attempts. The feature works with IP addresses in the format that FortiProducts support.

To enable the Impossible Travel feature in Adaptive Authentication Policy:

Action	Block

Filters
- ( ) Subnet Filter ● Location Filter ( ) No Source Filter
- ☑ Schedule

Location Filter Please click here to check supported devices.

Countries or Regions

☐ Unknown Country or Region ❓

United States of America ⊗

Impossible Travel ❓ ⬤ (toggle enabled)

Schedule

Weekdays
- ☑ Everyday
- ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Timezone | (GMT-08:00) Pacific Time (US & Canada) |

Time Range
- ☑ All day
- From `00:00` To `23:59`

1. Add the new policy by clicking Add Policy in Adaptive Auth > Policy page.
2. Give a unique name and select Enforce MFA/Block in the Action section, and select Location Filter.
3. Enter the Countries or Regions for normal login location, and click Enter.
4. Click the Impossible Travel button to enable it.
5. select a schedule configuration set in the Schedule section.
6. Click Confirm.
7. Add the policy to any profile. Be sure to select the same action, .i.e., Enforce MFA/Block.
8. Apply the profile to any Auth Clients (including FortiProducts and Web Apps) and any Realms whose users are going to log in from those locations.

Switch from Fortitoken to FortiToken Cloud (FTC) lockout

You can migrate FortiToken mobile license/users to FortiToken Cloud users if they prefer to take advantage of the cloud MFA service. The migration is based on the FortiToken mobile license. After the migration, the FortiToken mobile license will be converted to a time-based license on FTC and all users under this license will be converted from FTM users to FTC users. For more information, refer to .

1. Ensure that the FTM license has already been imported into the FortiGate. (The token serial number under the FTM license may or may not have been assigned to users.)
2. Submit 'set FTM migration tag request' to Customer Support (https://www.fortinet.com/support/contact) by providing the FGT serial number and the FTM license serial number. The CS team then confirms the pre-authentication from the customer and sets up the 'FTM migration tag'
3. Once the tag has been set up, run the execute fortitoken-cloud ftm-migrate < FortiToken mobile license number> command on the FGT. The command will transfer all users with FTM token auth under this FTM license to FTC auth method. You can find the FTM license number using the show user fortitoken command, which has set license <FTM license number>.
4. The tokens under the migrated license are then removed from the FOS GUI, and all users that have been migrated show up on the FTC GUI.
5. Once the migration CLI command is completed, user login authentication should work without any token data change.
6. After the migration is completed, FTC will send out email to CS asynchronously 24 hours after the migration of the account. The email is to notify CS to invalidate the FTM license and reset the migration tag. If you are migrating multiple FTM licenses, ensure that you migrate them together within 24 hours. Otherwise, you will have to re-submit the 'set FTM migration tag request' request to CS.
7. After the CS team has invalidated the FTM license and reset the migration tag, you may have to wait for up to 24 hours for the process to complete.

Migrate FTM tokens to FortiToken Cloud

Starting with FOS 7.0.4, FortiGate customers who are using FOS 2FA perpetual licenses can migrate their FTM tokens to FortiToken Cloud (FTC) by converting their FTM licenses to FTC subscription licenses. FGT admins can perform FTM token migration themselves using the following command:

```
execute fortitoken-cloud migrate-ftm <FortiToken mobile license number> <vdom>
```

where <vdom> is root, if VDOM is not enabled on the FortiGate.

	If you do not have an existing FTC license at the time of the migration, FTC will automatically generate a one-year free transfer license for you to use for the number of end-users corresponding to the total number of FTM tokens that are transferred. After one year, you will have to purchase an FTC license to continue using the service.

Procedures

1. Ensure that the FTM license has already been imported into the FortiGate. (The Token serial number under the FTM license may or may not have been assigned to users.)

2. Submit 'set FTM migration tag request' to Customer Support (https://www.fortinet.com/support/contact) by providing the FGT serial number and the FTM license serial number. The CS team then confirms the pre-authentication from the customer and sets up the 'FTM migration tag'.

3. Once the tag has been set up, run the execute fortitoken-cloud migrate-ftm <FortiToken mobile license number> <vdom> command on the FortiGate. The command will transfer all users with FTM token auth under this FTM license to FTC auth method. You can find the FTM license number with the output of the show user fortitoken command, which has set license <FTM license number>.

4. The tokens under the migrated license are then removed from the FOS GUI, and all users that have been migrated show up on the FTC GUI.

5. Once the migration CLI command is completed, user log auth should work without any token data change.

6. After the migration is completed, FTC will send out email to CS asynchronously 24 hours after the migration of the account. The email is notify CS to invalidate the FTM license and reset the migration tag. If you are migrating multiple FTM licenses, ensure that you migrate them together within 24 hours. Otherwise, you will have to re-submit the 'set FTM migration tag request' request to CS.

7. After the CS team has invalidated the FTM license and reset the migration tag, you may have to wait for up to 24 hours for the process to complete.

Verification

Check on the FOS portal:

- All users with FTM token auth under this migrated FTM license are updated to FortiToken Cloud on the FGT portal (User & Authentication>User Definition).

- The migrated FTM license is removed on the FGT portal (User & Authentication>FortiTokens). Tokens associated to the migrated FTM license will not show up in the token list.

Check on the FTC portal:

- The migrated FTM license shows up on the FTC portal (Licenses).

Contract Number	Serial Number	Category	Users	SMS Credits	Remaining SMS Credits	Status	Start Date	End Date
EFTM025130933610		FTM Migration License	25	3125	3067	active	12-13-2022	12-13-2023

- The migrated MFA users show up on the FTC portal (Users).
- The migrated FTM license quota has been added to the total FTC user quota and the assigned FTM token has been deducted from the total user quota (Dashboard).

End-user 2FA login authentication

- FTM License migration does not affect end-user 2FA login authentication with FortiToken (i.e., end-users will not notice any change in their login authentication process).

- Back up FortiGate configuration before starting the migration process.
- Once the FTM license and its tokens are successfully migrated to FortiToken Cloud, they cannot be reversed.
- The original FTM license is invalidated by the CS team once the migration is completed.
- The request can be initiated only by a FGT admin.
- FTM token migration is supported for trial accounts.
- FTM token migration is not supported for credit-based accounts.
- Before migrating an FTM license with a large number of associated users, be sure to set the FGT CLI Console timeout long enough to cover the entire process. If the Console times out while the migration is in progress, you can open another Console window and run the `diagnose fortitoken-cloud migrate-ftm show <FortiToken mobile license number>`' command to check the migration status.

Synchronize LDAP remote users in wildcard user group from FortiGate

LDAP is commonly used in user management. FortiToken Cloud supports different types of LDAP, including ADLDAP, Open LDAP, etc. In the FortiGate, for example, we can set up the filter to manage a group of users that have the same attributes, such as the same organization, the same department, or the same role.

Group filters can be used to reduce the number of the Active Directory users returned, and only synchronize the users who meet the group filter criteria. Use of LDAP filters for FortiGate and FortiAuthenticator are discussed separately below:

User case

This feature is supported on FortiGate devices running on FOS 7.2.1 and above, or FOS 7.0.7 and above, but is not supported on Series 6.x.x.

To synchronize Active Directory users and apply two-factor authentication using FortiToken Cloud, two-factor authentication must be enabled in the user LDAP object definition in FortiOS.

Two-factor authentication for LDAP group filtering can only be configured in the CLI:

```
config user ldap
    edit <name>
        set dn <string>
        set two-factor {disbale | fortitoken-cloud}
        set group-filter <string>
    next
end
```

In the following examples, a `user ldap` object is defined to connect to an Active Directory on a Windows server. The search will begin in the root of the fortinet-fsso.com directory.

```
config user ldap
    edit "ad-ldap-auth"
        set server <ip_address>
        set cnid "cn"
        set dn "dc=fortinet-fsso,dc=com"
        set type regular
        set two-factor fortitoken-cloud
        set username "cn=Administrator,cn=users,dc=fortinet-fsso,dc=com"
        set password **********
    next
end
```

When a group filter is not used, all users in Active Directory with a valid email or mobile number will be retrieved.
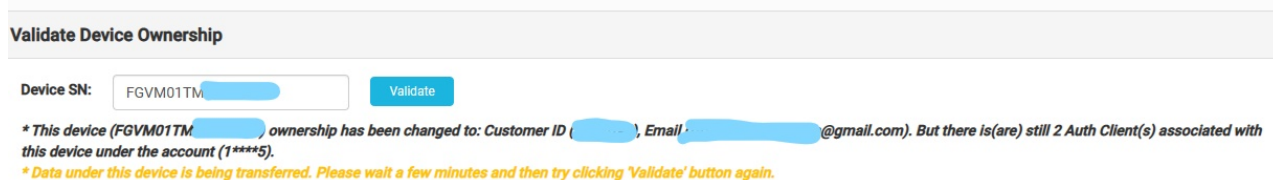
For more syntax and diagnostic details, please check FortiOS Release Notes at Administration Guide | FortiGate / FortiOS 7.0.7 | Fortinet Documentation Library.

Migrate device data on FTC

You are now able to migrate device data yourself directly from one FTC account to another on the FTC portal.

To migrate device data:

1. Request a device ownership transfer ticket in FortiCare.
2. Wait until after the ticket is processed and the ownership in FortiCare has been transferred to the new owner. For example, Account A is the original owner, and Account B is the new owner.
3. Now either Account A or Account B can start the data migration request in the FortiToken Cloud portal.
4. If Account A submits the migration request, an email notification will be sent to the owner of Account B, and vice versa.
5. Upon receiving the email notification, the owner of Account B logs into the FTC portal and confirms the data migration.
6. When the owner of Account B clicks the link in the email notification message, the browser will redirect the page to confirm device migration for Account B.
7. After Account B confirms the migration by clicking the Transfer button in the pop-up window, the transfer in process confirm window pops up..
8. The process may take a few minutes, depending on the data size (the number of users). If the following page shows, it means the migration is still in progress.

9. Wait for a few minutes before clicking the *Validate* button. If the following page shows, it means the data migration has completed.

10. The users should show up in the new owner's account, but are not longer available in the old owner's account.

Auth clients

An auth client can be hardware, software, or a third-party web application that FTC uses to perform user authentication. When creating a user, it is mandatory to have an auth client which is assigned to a realm in order for FTC to perform authentication with FortiProducts or third-party web apps. Once an auth client is created, you will be able to set the realms and adaptive auth profiles that the auth client uses. Note that by default, an auth client is automatically created when you connect your FortiGate to FTC. If you do not see the auth client (i.e., FortiGate) after connecting it to FTC, you can run the `execute fortitoken-cloud update` command which sends an updated list of VDOMs to FortiToken Cloud so that auth clients can be created for each VDOM on the FortiToken Cloud portal. Ensure that *Auto-create Auth Client* is enabled on the *Settings > Global* page. For how to get started with auth clients, see QuickStart Guide.

Create FortiProduct auth clients

While you can directly create web app and management auth clients from the FTC portal, auth clients under *Auth Clients > FortiProducts* can be created only when you successfully link your device to FortiToken Cloud (i.e., create a user on FortiGate and set its 2FA settings to be linked to FTC.)

For more information on how to setup your FortiProduct, please search and refer to the documentation for it on our main documentation site: https://docs.fortinet.com/

Transfer auth client (FC account lockout)

If one of your account owners has left your organization, the associated account will be locked out. If you still want to keep using the auth client which was registered under the locked account, you can transfer the ownership of the auth client from one FC account to another FC account.

To transfer an auth client to a new account:

1. Transfer the FortiGate to the new account by submitting a ticket (*Support > FORTICARE > Create a Ticket):* Fortinet Service & Support.
2. Log into the FTC portal with the new FC account to validate the device ownership from the Devices (HA) page.
3. Choose either of the following options:
   - Delete—Clicking the Delete button to remove all existing user information in FTC side and transfer the ownership afterward.

- Transfer—Clicking the Transfer button to migrate all existing user information in FTC side and transfer the ownership afterward.

4. Refer to Migrate device data on FTC on page 112 for instructions on how to migrate device data.

Auth client clean-up/migration may take some time, so be sure to validate the device again until the device has been transferred to the new FC account. If *Delete* is selected, all users with FTC MFA on the FGT can be synced to FTC, and the end-users need to be re-activated with a new token if you want to keep the users on the FGT. If *Transfer* is selected, all users with FTC MFA on the FGT can be migrated to the new FTC account and do not need to be re-activated.

Replace an old FortiGate with a new one

When replacing a FortiGate device, the most important thing to remember is to back up the FortiGate configuration and restore it to the new FortiGate. For backup issue, refer to Administration Guide | FortiGate / FortiOS 7.2.2 | Fortinet Documentation Library.

In the FortiToken Cloud:

1. Select *Auth Clients > FortiProducts.*
2. Find the old FGT by searching its serial number in search bar.
3. Select the device from the Auth Client list, and click *Delete.*

After the old FortiGate is removed, you can register the new FortiGate to your FC account by entering the registration code from the device or the license number if it is a VM. After the device is registered under the FC account, you can enable FortiToken Cloud on the FortiGate. This is important because you are going to restore the users who are using FortiToken Cloud as the MFA method in the next step.

Now, it's time to restore the configuration from the old FortiGate. After the basic configuration is restored, the end-users will also be restored. (Note: If the users exist in VDOMs, you need to back up/restore the VDOMs configuration.)

Finally, the users and auth clients will be updated if *Auto-create Auth Client* is enabled in the *Settings > Global* page. Otherwise, you need to run the `exec fortitioken-cloud update` command to manually update the VDOMs information from the FortiGate to FortiToken Cloud and update the users' information.

After you finish all these steps, the new FortiGate should be set up and ready to use.

Auth clients in HA mode

Auth clients in an HA cluster are shared by all members of the cluster. This is to ensure that the cluster members are using the same auth clients to preserve HA functionality. For more information about how to configure HA clusters in the GUI, see the FortiProducts section.

Before creating an HA cluster, make sure that the FortiGates are running the same version of the FortiOS and that the interfaces are not configured to get their addresses from DHCP or PPPoE. Also, switch ports are not allowed to be used as HA heartbeat interfaces. If necessary, convert switch ports to individual interfaces.

Configuring the primary FortiGate

1. On the primary FortiGate, go to *System > Settings* and change the Host name to identify it as the primary FortiGate in the HA cluster.

   Host name   Edge-Primary

2. Go to *System > HA* and set the Mode to Active-Passive. Set the Device priority to a higher value than the default (in the example, 250) to ensure that this FortiGate will always be the primary FortiGate. Also, set the group name and password.
3. Make sure you select the Heartbeat interfaces (in the example, the HA port if it exists; it does not have to use port3 or port4).

Single heartbeat interface:

Mode	Active-Passive
Device priority	250

Cluster Settings

Group name	Edge-HA-Cluster
Password	••••••••	Change
Session pickup	
Monitor interfaces	+
Heartbeat interfaces	ha ✖
	+

Multiple heartbeat interfaces:

Mode	Active-Passive ▼
Device priority ⓘ	250 ⬍

Cluster Settings

Group name	Edge-HA-Cluster
Password	•••••••• [Change]
Session pickup	⊙
Monitor interfaces	+
Heartbeat interfaces	🖥 port3 ✖
	🖥 port4 ✖
	+

Heartbeat Interface Priority ⓘ

port3	▬▬◯▬▬▬▬▬▬	50
port4	▬▬◯▬▬▬▬▬▬	50

Configuring a backup FortiGate

1. On the backup FortiGate, go to *System > Settings* and change the Host name to identify it as the backup FortiGate in the HA cluster.

Host name	Edge-Backup

2. Go to *System > HA* and set the Mode to Active-Passive. Set the Device priority to a lower value than the primary (for example, 200) to ensure that this FortiGate will always be the backup FortiGate, only to be activated when the primary FortiGate is down. Also, set the group name and password.

You can use the FTC MFA service with a cluster of auth devices. Both single and multiple auth devices in a cluster are supported. You can add or remove auth devices on the FTC portal. For example, let's say you have a system admin who maintains multiple auth devices, and some of them are FortiGate HA cluster members. The system admin has set one FortiGate cluster member to be a standalone device. The FTC system admin can check if FortiGate standalone device has been removed from the FTC device cluster. If it still shows up in the cluster due to it being out-of-sync between FortiGate and FTC, the system admin can manually take it out.

Auth clients for third-party usage

- Web app clients — https://docs.fortinet.com/document/fortitoken-cloud/latest/rest-api/597289/web-app
- Management app clients — https://docs.fortinet.com/document/fortitoken-cloud/latest/rest-api/816036/management-app

> The links above provide instructions on how to configure auth clients from the GUI and examples for how to use the auth clients with Python, Curl and Postman.

Maintenance

Add, sync, and delete users

When a user is created with FTC as the authentication method on an auth client (e.g., FortiGate), the user data is automatically added to the FTC system.

When a user with FTC as auth method on an auth client is deleted, the user data is automatically deleted from the FTC system. Deleting an auth client from the FTC portal deletes all users on the auth client. Additionally, you can delete individual users in the *Users* page of the FTC portal. You can sync user data anytime from the auth client (FortiGate in this case) to FTC by running the "`exec fortitoken-cloud sync`" command, as discussed in the following use case.

Use case

1. Create or delete users in FGT.
2. Run "`exec fortitoken-cloud sync`" on FGT to sync users with FTC auth method to FTC:
   - If syncing works well, the output will show:
     ```
     Sync status: {"status": "complete", "msg": {"delete": {"success": 0, "failure": 0},
     "modify": {"success": 0, "failure": 0}, "create": {"success": 3, "failure": 0}}}
     User synchronization completed!
     ```
   - If syncing failed, the output will show:
     ```
     Sync status: {"status": "complete", "msg": {"delete": {"success": 0, "failure": 0},
     "modify": {"success": 0, "failure": 0}, "create": {"success": 0, "failure": 3}}}
     User synchronization completed!
     ```
   - If you encounter the "failure" as shown above, check to see if this auth client exists in the FTC side by searching the SN in the *Auth Clients > FortiProducts* page.
     - If it does not exist, check to see if the switch *Auto-create Auch Client* is enabled in the *Settings > Global* page.
     - If it does exist, check to see if the user quota has reached the maximum, or if the realm assigned has available quota and if the *Share-quota Mode* is disabled.
   - If the connection to FTC is unstable or unavailable, the output will show:
     ```
     Cannot find FTC server!
     Cannot retrieve user information from FortiToken Cloud!
     Command fail. Return code -1
     ```

Add, sync, and delete auth clients (devices)

When an auth client communicates to FTC for the first time, this auth client will be added to the FTC system automatically. The first communication can be triggered by creating an FTC user on the auth client or by running some CLI commands on the auth client. The auth client can be deleted from the FTC portal by choosing Auth Clients>FortiProducts or Webapps.

Use cases

- Register a new FortiProduct, for example FortiGate, using the license or serial number of the device, create a new VDOM in FGT, or delete a VDOM.
- Run "`exec fortitoken-cloud update`" on FGT to sync VDOMs (auth clients in FTC) to FTC.
- If syncing works well, the output will show:

  `List of VDOMs updated to FortiToken Cloud.`

- After syncing, if the *Multi-realm Mode* is disabled, any new auth client will be assigned to the default realm. When *Multi-realm Mode* is enabled, any new auth client registered in FTC will be automatically assigned to a new realm.

How to debug

FortiToken Cloud has special debug mode in the FOS (ex. FortiGate) side. Before you perform any user sync/delete/add operation, the debug mode can be opened by running:

```
config global (if the multi-vdom mode is enabled)
diag fortitoken-cloud debug enable (to enable the FTC debug mode)
diagnose debug console timestamp enable (to add the timestamp to log output)
diag debug appl fnbamd -1
diag debug application httpsd 255
diag debug enable (to start the show debug message)
```

After running the CLI commands shown above, if any FTC user sync/delete/add action is triggered, the log message will show in the CLI. Or, if another CLI is open and executes "`exec fortitoken-cloud update`", the log will also display because it manually triggers the FortiToken Cloud user update in FOS (ex. FortiGate).

If you are unable to fix the error message using the aforementioned commands, the FortiToken Cloud support team is standing by to provide any assistance if needed. Just create a support ticket and submit it to our TAC team. We will respond to your service request and resolve your issue as soon as possible. It's recommended that you attach the debug log output in the ticket to enable the TAC team or the FortiToken Cloud Support Team to investigate the error faster. To contact technical support, visit Technical Support.

Service debug

You can debug the service from the FTC portal logs page if there is any auth failure or your end-users fail to receive OTP or push notifications when using the FTC service. There are two categories of logs: one is for authentication requests and responses, and the other is for management operations such as create/delete/update user. To find out if the FTC server is available, you check the Service Status (https://status.fortistatus.com/guest-portal/fortitoken/incident/overview)

Settings

The Settings menu has the following sub-menus:

- *Global* —Accessible to the global admin only, it provides tools for making system-wide settings changes to your account. For more information, see Global on page 76.
- *Realm* —Shows the settings of the current realm, and provides tools for updating the settings of the realm. For more information, see Realm on page 79.
- *Templates*—Provides tools for managing message templates. For more information, see Templates on page 84.

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

Global

Multi-realm mode

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

Multi-realm Mode is enabled for new FTC customers right now. When Multi-realm Mode is disabled, new auth clients are assigned to the default realm. When multi-realm mode is enabled, new auth clients registered in FTC are automatically assigned to a new realm. If any customers want to use multi-realm feature, it's easy to enable it from FTC GUI>Settings>Global>Multi-realm Mode.

Enable multi-realm mode

If Multi-realm Mode is 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 page.
2. Click the Multi-realm Mode button to enable it.
3. In the Multi-realm Mode dialog, read the messages and click OK to proceed.
4. Click Apply Changes.
5. Click Confirm.

Use case 1: When multi-realm mode is enabled

When Multi-realm Mode and Auto-create Auth Client are enabled, a newly registered auth client will be assigned to a new realm.

1. FortiGate1 with serial number (FG200ETK1990xxxx) and FortiGate2 with serial number (FG300ETK1990xxxx) are registered under FC account (fortinet_account@gmail.com).

2. As long as the realm resource is enough, the FTC will automatically create two realms: FG200ETK1990xxxx-root and FG300ETK1990xxxx-root, and FGT1 and FGT2 will be assigned to those two separated realms.

3. In this case, the user created in FGT1 named "Jack Talyor" is assigned one token, and user created in FGT2 named "Jack Talyor" is also assigned one new token. They are two separate users with the same username, but use separate tokens.

4. If the two "Jack Taylors" exist in two realms, some actions will be confusing somehow. For example, if one "Jack Taylor" is deleted from FGT1, and the "Jack Taylor" still exists in FTC. This scene looks like "Jack Taylor" was never deleted on FGT1, but, in fact, the "Jack Taylor" doesn't exist in FGT1 any more, but only exists in FGT2.

5. Solution: Login to FGT2 and delete "Jack Taylor", execute the console CLI command, "diag fortitoken-cloud sync" in FGT. The user "Jack Taylor" will be removed in FTC. After deleting the user in FGT2, assign the auth client FGT1 and auth client FGT2 to the same realm, for example, the "default" realm, could prevent the same situation from happening again.

Use case 2: When multi-realm mode is disabled

When Multi-realm Mode is enabled, the new registered auth client will be assigned to the "default" realm.

1. FortiGate1 with serial number (FG200ETK1990xxxx) and FortiGate2 with serial number (FG300ETK1990xxxx) are registered under FC account (fortinet_account@gmail.com).

2. The FTC will automatically assign two auth clients (FGT1 and FGT2) to the "default" realm.

3. Users with the same username will be considered as the same user and share the same token.

4. In the FTC portal, the "Jack Taylor" in the Users page will display once and the "Auth Client Count" column displays "2" which will remind administrator that "Jack Taylor" exists in two different auth clients.

Use case 3: Change Multi-realm Mode from enable to disable

When you change Multi-realm Mode from enable to disable, FTC will be changed from share-token to single token login.

1. FortiGate1 with serial number (FG200ETK1990xxxx) and FortiGate2 with serial number (FG300ETK1990xxxx) are registered under FC account (fortinet_account@gmail.com).

2. As long as the realm has enough resources, FTC will automatically create two realms: "FG200ETK1990xxxx-root" and "FG300ETK1990xxxx-root", and FGT1 and FGT2 will be assigned to those two separated realms.

3. In this case, the user created in FGT1 named "Jack Talyor" is assigned one token, and the user created in FGT2 named "Jack Talyor" is also assigned one new token. They are two separate users with the same username but use separate tokens.

4. If you want to switch to one-token login mode (same username use one token only), you can move FGT1 and FGT2 to the same realm, for example, the "default" realm, from the two realms "FG200ETK1990xxxx-root" and "FG300ETK1990xxxx-root".

5. The users will be merged in the Users page, the two "Jack Taylor" users will be merged into one "Jack Taylor" and the auth client count will increase to "2". The one token will be shared by the two "Jack Taylor" users. By default, the token will be kept for the auth client that is migrated to the "default" realm firstly, and the token of the user in the auth

client migrated later will be removed.

6. As such, the user "Jack Taylor" will only need one token to login two FGT resources.

7. Additionally, if you want to always use one-token login mode, you can navigate to Settings>Global and disable Multi-realm Mode. You must also move all existing auth clients to the same realm, e.g., the default realm.

8. After Step 7, the existing auth clients will use the one-token mode and newly assigned auth clients will also migrate to the "default" realm and uses the one-token mode.

Auto create Auth Client

By default, Auto-create Auth Client is enabled, but you can disable it using the following procedures (only when the customer doesn't need FortiToken Cloud automatically create extra auth clients, for example the MSSP customer, instead of creating manually after confirmed):

1. On the main menu, click Settings>Global to open the Global page.

2. On the Global page, click the Auto-create Auth Client button to turn it off.

3. In the Auto-create Auth Client dialog, read the messages and click OK to proceed.

4. Click Apply Changes.

5. Click Confirm.

Share-quota Mode

The Share-quota Mode option applies to paid time-based subscriptions only; it is not available to time-based trial accounts. When Share-quota Mode is enabled (by default), the remaining user quotas will be shared by all realms. When it is disabled, the remaining user quotas will not be shared among realms.

1. On the main menu, click Settings>Global to open the Global page.

2. On the Global page, click the Share-quota Mode button to turn it off.

3. In the Share-quota Mode dialog, read the messages and click OK to proceed.

4. Click Apply Changes.

5. Click Confirm.

User quota allocation by realm

Customers with time-based licenses can allocate the remaining user quota to different realms which can control the user count under each realm. The allocation can be configured in FTC GUI -> Realms -> Edit specific realm, then update the user quota amount. The customer can also define whether the remaining unallocated user quotas can be shared by all realms or not through FTC GUI -> Settings -> Global -> Share-quota Mode. The default setting has share mode enabled.

Username Case Accent Sensitive

The customer can customize the user case accent sensitive setting when they do a login auth with FTC MFA. By default, the username case accent sensitive setting is enabled. The username case accent sensitive setting can be configured from FTC GUI-> Settings->Global->Username Case&Accent Sensitive.

For example, if there is an FTC local user named 'test1' and they try to do an SSLVPN login auth with 'TEST1' or 'TeSt1', if Username Case Accent Sensitivity is disabled on FTC, FTC will allow the login auth to succeed and will deny the login auth if Username Case Accent Sensitivity is enabled.

1. On the main menu, click Settings>Global to open the Global page.
2. On the Global page, click the Username Case Accent Sensitive button to turn it off.
3. In the Username Case Accent Sensitive dialog, read the messages and click OK to proceed.
4. Click Apply Changes.
5. Click Confirm.

Account Disable/Delete Notification

Once your license has expired, FortiToken Cloud will periodically send notifications to your account, alerting you that your account will be disabled or closed if the license is not renewed in time.

By default, Account Disable/Delete Notification is enabled, but you can disable it by turning it off.

For more information, refer to .

1. On the main menu, click Settings>Global to open the Global page.
2. On the Global page, click the Account Disable/Delete Notification button to turn it off.
3. In the Account Disable/Delete Notification dialog, read the messages and click OK to proceed.
4. Click Apply Changes.
5. Click Confirm.

Account disablement and closure

FortiToken Cloud will disable an account 30 days after its license has expired, and close the account 90 days after it has been disabled. Before disabling or deleting the account, FTC will send out email notifications to the customer 30,14, and 1 day(s) in advance. To avoid service interruption, it is your (the customer's) responsibility to ensure that your account is in good status, and renew your license when or before it expires.

Realm

Realm

The *Settings>Realm* page provides tools for managing the settings of the selected realm. The page has the following tabs:

To configure or update the settings of the realm:

1. On the main menu, click *Settings>Realm.*
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

Parameter	Default value
MFA Method	Select the method that FTC uses to further authenticate your end-users upon receiving their login credentials (i.e., username and password). • *FTM* (default)—FTC sends a unique one-time passcode (OTP) to the FortiToken Mobile app on 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, the 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 the end-users' valid smart phone numbers in its database. • *Email*—FTC sends a unique OTP to the end-users' email addresses on file. The users then have to manually 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 numbers of the FortiTokens to FTC, and assign them to the end-users. Upon receiving an end-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 116. 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 100.
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. **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 7,200 seconds. The default is 60 seconds.
Enable Bypass	Enable or disable bypass. • *Enable*—End-users can bypass MFA. If enabled, you must also set the

Parameter	Default value
	Bypass Expiration Time, as described below. • *Disable* (default)—End-users cannot 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 100.
Bypass Expiration Time	(Available only when *Enable Bypass* is enabled.) Specify the length of time bypass remains in effect. Valid values range from 5 minutes to 72 hours. The default is 1 hour (3,600 seconds).
Auto-alias by Email	Enable or disable the *Auto-alias by Email* feature. **Note:** The feature is disabled by default. For more information, see Enable Auto-alias by Email on page 81.
Adaptive Auth Profile	Select an adaptive auth profile.

Enable Auto-alias by Email

Many FTC end-users have different usernames in different applications and domains. By the same token, the same FTC end-user may have different usernames in different auth clients. For example, a user by the name of 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 allows for different usernames to be attributed to the same user so that only one token needs to be assigned to that user. It does this by providing an *Auto-alias by Email* option, which, once turned on, enables FTC to automatically put different usernames in an alias if they use the email address.

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

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

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 *Auto-alias by Email* is enabled.

FTM Setting

Parameter	Default value
1. Settings	
Enable Push	Click the button to enable or disable push notification.
Notification Method	From the drop-down menu, select either of the following: • *Email*—Token activation/transfer codes are sent to users' email addresses.

Settings

Parameter	Default value
	• *SMS*—Token activation/transfer codes are sent by SMS to users' mobile phone numbers. **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 users on the *Users* page. See Users on page 100. **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* **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:

Parameter	Default value
	• *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 83. • *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

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

Parameter	Description
1. Settings	
OTP Expiration Time	Click the down arrow to select an OTP expiration time. **Note:** An OTP is valid only within the specified OTP expiration 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 can 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 expiration time. **Note:** An OTP is valid only within the specified OTP expiration 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 SMS template. **Note:** You can 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-users 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.

Column	Description
Default	Indicates whether the template is a default one or not.
Name	The name of the template.
Method	The way the template is used.
Type	The template type.

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

Add a template

To add a template:

1. On the main menu, click *Settings>Templates* to open the *Templates* page.
2. In the upper-left corner of the *Templates* 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-user.
4. For *Type,* click the down arrow to select a desired message template.
   Note: FTC offers three types of template, and each template is for a specific purpose. Be sure to create all the three types of template to take full advantage of this feature.
5. Click *Confirm.*
   The dialog refreshes, showing 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 the 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 *Templates* 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 *Templates* 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 *Templates* page after the page refreshes.

Apply templates

All templates are applied at the realm level.

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 *Realm* page.
4. Across the top of the *Realm* 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 templates are now applied to the realm and will be used when FTC sends token activation and/or transfer notifications to your 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 *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 *Realm* page.
4. Across the top of the *Realm* 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.*

FortiToken Cloud GUI

⚠️
- Both the global admin and sub-admin users can access the FortiToken Cloud portal, but sub-admin users will not be able to see any data until the global admin has delegated realms to them.
- The global admin is the first account from your organization that has logged in to the FTC portal. The owner/user of the main FC account of your organization is your de facto FTC global admin.

The FTC GUI has the following main pages:

Menu	Description
Dashboard	Provides some key statistics about your account. The content of the page varies, depending on the type of license you are using. For more information, see Dashboard on page 96.
Administrators	(Accessible to the global admin only) enables the global admin to create sub-admin groups and assign realms to them. See Administrators on page 97.
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 105.
Users	Shows information of all your FTC end-users. For more information, see Users on page 100.
Auth Clients	Shows information about all your authentication clients which include the following types: - FortiProducts on page 107 - Web Apps on page 113 - Devices (HA) on page 115
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 116. - *Hardware*—Shows hardware tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See Hardware Tokens on page 116.
Usage	Shows usage data of your account. See Usage on page 119.
Licenses	Shows all the licenses in your account. See Licenses on page 120. **Note:** This menu is visible to users of time-based subscriptions only, and is not available to users of credit-based subscriptions.
Settings	Opens the *Settings* menu which has the following options: - *Global*—Allows the global administrator to enable or disable some settings at

Menu	Description
	the system level. See Global on page 76. • *Realm*—Enables both the global admin and sub-admins to view and manage the settings of the selected realm. See Realm on page 79. • *Templates*—Opens the Templates page where you can add or delete templates. See Templates on page 84.
Adaptive Auth	Opens the *Adaptive Auth* menu which has the following options: • *Policy*—Creates and manage adaptive auth policies. • *Profile*—Creates and manager adaptive auth profiles. See Adaptive authentication on page 120.
Logs	Shows the *Logs* menu which has the following options: • Authentication on page 128 • Management on page 129 • SMS on page 131 See Logs on page 127.
Help	Opens the *Help* menu which has the following options: • Contact Support • Purchasing Guide • SMS Rate • Online Help • FAQ • Status Monitoring
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

After your FortiToken Cloud (FTC) account is created, you can log on to the FTC portal from anywhere using a web browser and your login credentials.

Log in as a regular FTC user

Regular FTC users are admin users that are created on FortiProducts (e.g., FortiGate, FortiAuthenticator, etc.).

To log in as a regular FTC user:

1. Start your web browser.
2. Point to https://ftc.fortinet.com, and press the *Enter* key 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 that you provided when creating your FTC account is your FTC username or account name. Be sure to use the same email address when logging in to the FTC portal.
5. Click *LOGIN.*

| | If you have five or more sub-users associated with your master account, the FTC portal shows only five accounts per page. You can scroll through your accounts by clicking the arrow buttons in the lower-right right corner of the page. |

Make a Selection to Proceed

Account ID	Email	Company	License Status	
1224184	automation.api.time1@gmail.c	company 1224184	Licensed	
1444144	:st1661805676700@qatest.cc	FortinetAuto	Free Trial	
1444146	:st1661807128640@qatest.cc	FortinetAuto	Free Trial	
1444147	:st1661807388877@qatest.cc	FortinetAuto	Free Trial	
1444156	:st1661822806528@qatest.cc	FortinetAuto	Free Trial	

1 - 5 of 42

Log in as an IAM user

The Identity and Access Management (IAM) portal is an advanced feature of FortiCloud, and is accessible only to FortiCloud Premium customers. An IAM user is one created by the super-admin of a FortiCloud Premium 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.*

Log into an OU account

You can access FTC using IAM user accounts or an Organizational Unit (OU) account when logging in with your IAM user credentials. Once the login credentials have been verified, you can then choose to proceed with an OU account. OU access is dependent on the permission profile assigned to your login credentials. Available OUs and member accounts will turn blue when you mouse over them and display the *Select* button.

For more information about Organizations and OUs, see the Organization Portal Guide.

For more information on IAM, see the Identity & Access Management Guide.

To access Organizational Unit accounts with IAM user credentials:

1. In the upper-right corner of the FTC portal, click the ftc_iam drop-down and select an OU account.
2. Enter the username and password, and click LOG IN. A list of Organizational Units and member accounts is displayed.
3. Select the access method:
   - Hover over an OU and click Select to log in to a root account.
   - Hover over an OU member account and click Select to log into the account.

To access Organizational Unit accounts with external IdP credentials:

1. Log in using your company's ID provider. The log in portal opens.
2. Select the Service Provider.
3. Select Organizations. A list of Organizational Units and member accounts is displayed.
4. Select the access method:
   - Hover over an OU and click Select to log in to a root account.
   - Hover over an OU member account and click Select to log into the account.

Log into an OU account

You can access FTC using IAM user accounts or an Organizational Unit (OU) account when logging in with your IAM user credentials. Once the login credentials have been verified, you can then choose to proceed with an OU account. OU access is dependent on the permission profile assigned to your login credentials. Available OUs and member accounts will turn blue when you mouse over them and display the *Select* button.

For more information about Organizations and OUs, see the Organization Portal Guide.

For more information on IAM, see the Identity & Access Management Guide.

To access Organizational Unit accounts with IAM user credentials:

1. In the upper-right corner of the FTC portal, click the ftc_iam drop-down and select an OU account.
2. Enter the username and password, and click LOG IN. A list of Organizational Units and member accounts is displayed.
3. Select the access method:
   - Hover over an OU and click Select to log in to a root account.
   - Hover over an OU member account and click Select to log into the account.

To access Organizational Unit accounts with external IdP credentials:

1. Log in using your company's ID provider. The log in portal opens.
2. Select the Service Provider.
3. Select Organizations. A list of Organizational Units and member accounts is displayed.
4. Select the access method:

- Hover over an OU and click Select to log in to a root account.
- Hover over an OU member account and click Select to log into the account.

FortiCloud

As part of FortiCloud (FC) — 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 FC as well as tools for managing your FC 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. It indicates the level of FC service you have subscribed: if you are a premium FC customer, the FortiCloud log will have the word "PREMIUM" beneath it; if you are a basic FC customer, you will see the logo only. A premium FC account requires a premium FC license and offers more features and services. If you are interested in getting FC 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 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 FC account, as described in the following table.

Tools for managing your FC account

Menu	Description
My Account	Opens your FC 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. • *My Account (IAM version)*
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:

Menu	Description
	• *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 FC.
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 FC service. **Note:** You must have a valid license to access any of the following cloud services.

Menu	Description
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
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 links to download. • *Firmware Download* • *VM Images* • *Service Updates* • *HQIP Images* • *Firmware Image Checksum*
Resources	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*

Menu	Description
	• *Contact Support* • *Technical Web Chat*

Dashboard

By default, the *Dashboard* page opens upon log-in. During a session, you can 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 its credit-based subscription model.
>
> If you are a customer of a credit-based subscription, you can continue using your existing subscription until it expires. You can then decide whether you want to continue your FTC service by purchasing a time-based subscription.

The content of the Dashboard varies, depending on the type of license you are using.

If you are using a time-based license, you'll see:

- *FortiProducts* — The number of FortiProducts as auth clients in your account.
- *Web Apps/Max Webb Apps* —The current number of Web apps as auth clients in your account and the maximum number of Web apps that your license can support.
- *Users/Max Users* — The current number of users in your account and the maximum number of users that your license can support.
- *Realms/Max Realms* — The current number of realms in your account vs. the maximum number of realms that your license can support,
- *SMS Credits* — The number of SMS messages available for use.
- *Expiration Date* — The date when your current license expires.
- Alert Event — The number of alert events that have been configured.
- *Last 10 authentication attempts in 30 days*

If you are using a legacy credit-based license, you'll see:

- *Current Month Usage* — The number of credits that has been used for the current month.
- *Current Balance*— The current credit balance (number of credits remaining).
- *FortiProducts* —The number of Fortinet products as auth clients.
- *Web Apps* — The number of Web apps as auth clients.
- *Users* — The number of FTC end-users.
- *Realms* — The number of realms*.*
- *Last 10 authentication attempts in 30 days*

Last 10 authentication attempts in 30 days

This section of the Dashboard shows the 10 most recent authentication attempts over the past 30 days, with the following information about each log:

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 end-user who requested authentication.
Auth Client	The authentication client that made the request.
Action	The type of authentication action.
Result	The outcome of the authentication request, which can be either of the following: • *Success* • *Failed*
Message	A system-generated message about the authentication request.

FTC extracts the 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 main 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 the group. (Optional)
Level	The level of administration of the 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 the group. **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 when you mouse over the entry in the table. It shows the following tools: • *Edit*—Edits the administrator group. • *Delete*—Deletes the administrator group.

Create a sub-admin group

To create a sub-admin group:

1. On the *Administrators* page, click *Add Admin Group* to open the *Add New Admin Group* dialog.
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 special characters such as 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 sub-admin group that you've just created appears on the Administrators page. Your then need to add sub-admin users and assign realms to the group, as discussed in the following sections.

Add users to the group

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

To add sub-admins to an 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.*
4. Click *Close*.

Add realms to the group

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

- Only the global admin can add realms to an admin group.
- You must have realms created first before assigning them to a sub-admin group. See Realms on page 105.
- 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* to open the *Manage Realm* dialog.
2. Under *Not Managed by Group,* select the realm(s) of interest and click *Add To.*
3. Click *Close*.

Edit sub-admin group configuration

You can edit an admin group by changing its name and description, and/or by adding or deleting 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 98.
6. To delete a sub-admin, identify the sub-admin and click X *(Delete)*.
7. To add more realms to the group, click *Add Realm.* See Add realms to the group on page 99.
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 before deleting the group. See Edit sub-admin group configuration on page 99.

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.

Users

The term "users" refers to end-users of FortiToken Cloud. The *Users* page displays the following information about FTC end-users in your account. You can open the *Users* page by clicking *Users* on the main menu.

Column	Description
Checkbox	This checkbox only applies to users who use FTM for MFA. It enables you 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 FTM token on page 103.
Username	The username of the end-user.
Status	The status of the 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. For more information, see the following bullet. • ✖ **(disabled)**—This button enables the administrator to temporarily stop the user from using FTC. **Note:** If a user is disabled, FTC will deny all log-in requests from the user. It must be noted that disabling a user only prevents the user from using FTC, but does not remove the user from your account. FTC will continue counting it toward your user quota for the user until the user is removed from your account. The admin user can also click this button to enable the user if the user is disabled. • 🔒 **(locked)**—The user is locked out. **Note:** FTC locks a user out when the user has exceeded the specified maximum number of log-in attempts allowed. See Realm on page 79. • 🔓 **(unlocked)**—The user is unlocked. **Note:** FTC automatically unlocks users based on their lockout settings. The admin user can also manually unlock a locked user by clicking the 🔒 **(locked)** button. • 🔑 (Temporary token deactivated)—Temporary token is deactivated. 🔑 (Temporary token activated)— Temporary token is activated.

Column	Description
	• ⏱ **(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 Realm on page 79. Otherwise, when you click the ⇄ **(no bypass)** icon, a tool tip will appear asking you to turn on *Enable Bypass on the Settings* page.
MFA Method	The MFA method used by the user, which can be one of the following: • *FTM* (soft token) • *Email* • *SMS* • *FTK* (FortiToken, a hardware token)
Token SN	The serial number of the token. **Note:** A serial number that starts with "FTC" indicates that it is a FortiToken Cloud token; 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 the user, which can be either of the following: • *Email*—FTC sends FTM token activation/transfer notifications to the user's email address. • *SMS*—FTC sends FTM token activation/transfer notifications by SMS to the user's mobile phone. **Note:** If the user's notification method is set to SMS, 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 Realm on page 79.
Email	The user's email address. **Note:** The admin user is able to edit users' email addresses.
Mobile Phone	The user's mobile phone number, if available. **Note:** The phone number must be in the format of "+ Country Code Area Code Phone Number", e.g., +1 4082221234. You can edit an end-user's mobile phone numbers.
Auth Client Count	The number of auth clients that the user uses.
Create Date	The date on which the user is 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 two options: • *Edit* —Edits the user's settings. • *Delete*—Deletes the user.

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 allows for different usernames to be attributed to the same user (i.e., same person) so that only one token (FTM or FTK) needs to be assigned to the same user. It does this by providing an Auto-alias by Email option, which, once turned on, enables FTC to automatically put usernames into an alias if they use the same email address.

Auto-alias by Email is disabled by default, but you can enable it 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 an alias under the same username.

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

Add user aliases

> The *Add User Alias* button becomes available only when *Auto-alias by Email* is enabled on the*Settings* page of a realm. It enables you to select users of interest on the *Users* page, and group them together using an alias. Aliased users show up in boldface on the *Users* page.

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

Auto-assign FTKs to selected users

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

1. On the *Users* page, select the users of interest.
2. Click the *Auto-assign FTK* button.

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.

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.

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. 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) which the user uses.
3. Click *Close* to close the window.

Use a temporary token

The temporary token feature enables end-users, who do not have their authentication devices with them, to use MFA function temporarily. The Temporary Token icon can be found in the Users page. You can activate or deactivate the feature using the Edit User button. The Temporary Token icon is greyed out when the feature is disabled, and turns green when it is enabled. When activated, the user will receive OTP for MFA authentication either by email or SMS. Temporary token is deactivated when the user is using an authentication device for MFA authentication, or when the temporary token has expired.

To assign a temporary token to a user:

1. On the *Users* page, locate the user and mouse over it to bring out the Edit User button.
2. Click the *Edit User* button to open the *EditUser* window.
3. In the *Status* field, click the grey "Temporary Token" icon to activate it. Another Edit User window opens.
4. Select Temporary Auth Method, and set the Expiration Time.
5. Click *Apply.*

Edit a user

1. On the *Users* page, identify the user of interest, and mouse over it.
2. Click the *Edit User* button to open the *Edit User* dialog.
3. Make the desired changes as described in the following table, and click *Apply*.

Field	Description
Auth Method	Click the down arrow, and select a desired authentication method from the drop-down menu: • *FTM* • *Email* • *SMS* (**Note:** This option requires a valid mobile phone number.) • *FTK*
Notification Method	**Note:** This field applies only when you set *Auth Method* to *FTM.* See above.
Token SN	*This field is read only, and cannot be edited.*
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.
Status	Displays the user's status in icons applicable to the user.
Last MFA	Displays the MFA method that the user used the last time.

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

Delete users from FTC

⚠️ • Before deleting a user, pay special attention to the confirmation message.
• Make sure that the user is really not in use any more. Deleting a user in use will result in authentication failure of the user.
• The same user may be referenced by multiple Fortinet devices. Make sure that the user is not in use by any other Fortinet devices before deleting it.

Users that are deleted from a FortiGate can still show up on the FTC portal if the two are out of sync. Running the `execute fortitoken-cloud sync` command on the FortiGate used to be the only way to solve the issue. With the FTC 23.1.a release, you can remove such users directly from the FTC portal.

1. On the menu, select *Users* to open the *Users* page.
2. Highlight the user that has already been deleted from FortiGate.
3. From the top of the *Users* page, click *Delete*.
4. Click *Yes*.

Realms

A realm in FTC is a set of users identified as valid users of one or more auth clients and can be controlled by the same adaptive auth profile in the realm settings. It is with realms that admins can control settings such as user quota and MFA method to use. FTC also comes with a default realm that you can use.

You can open the *Realms* page by clicking *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 assigned to all sub-admin groups in your account; 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 Realms*—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.

Parameter	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 107.
Name	The name of a realm.
User Count	The number of end-users on the realm.
Allocated User Quota	The number of end-user quota allocated to the 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 the 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:

Parameter	Description
	• *Refresh Realm*—Refreshes the entry to get the latest data about the realm. • *Edit Realm*—Edits the name and/or description of the selected realm. If you are on a time-based subscription, you are also able to set or change the user quota allocation to the selected realm within the set value range. • *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 76. • *Delete*—Deletes the realm. See Delete a realm on page 107.

Create a custom realm

1. On the *Realms* page, click *Add Realm.*
   The *Add New Realm* dialog opens.
2. Specify the name of the realm.
3. (Optional) Enter a brief description.
4. Click *OK.*
5. On the *Realms* page, locate the realm that you have just created. **(Note:** Steps 5 through 8 apply to time-based subscriptions only.)
6. Place the cursor over the entry to bring out the slide-in menu from the right end of the row.
7. Select the *Edit Realm* button to open the *Edit Realm* dialog.
8. Click or drag the slider to set the user quota to be allocated to the realm.
9. Click *OK.*

Edit a realm

Options for editing a realm vary, depending on the type of your FTC subscription. If you are on a credit-based subscription, you can only make changes to the name and description of the realm; if you are on a time-based annual subscription, you can also change the user quota allocated to the realm within the stated range.

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 to the realm name and the description.
4. Drag the slide bar to set or change the allocated user quota. (**Note:** This options applies to time-based subscription only.)
5. Click *OK.*

View realm permission

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 that 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

1. On the *Realms* page, identify the realm of interest.
2. In the toolbar, 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

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

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

FortiProducts

The *FortiProducts* page shows information about all Fortinet products 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 109. **Note:** You can select all the auth clients at once by checking the checkbox in the column header.
Alias	The alias of the auth client.

Column	Description
Name	The name of the auth client.
Type	The type of auth client, which can be any of the following: • *FortiAuthenticator* • *FortiGate* • *FortiGateVM* • *FortiSandbox* **Note:** FTC assigns auth client type based on the serial number and model of the product.
Count	The number of FTC end-users on the auth client. **Note:** Clicking the numeric value opens a dialog which shows the list of FTC end-users on an auth client, along with some basic user information.
Realm Name	The name of the realm to which the 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 the 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 105.

1. On the main menu, click *Auth Clients > FortiProducts* to open the *FortiProducts* page.
2. In the table, locate the unassigned auth client, and mouse over it to bring out the toolbar.
3. Click the *Edit Fortiprod* button to open the Edit dialog.
4. Click the *Realm* drop-down menu, and select a realm of interest.
5. Read the message.
6. Click *OK.*
   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

1. On the *FortiProducts* page, identify the auth client of interest, and mouse over it to bring out the slide-in toolbar.
2. Click *Edit FortiProd* to open the Edit dialog.
3. Make the desired changes.
4. Click *OK.*

Viewing additional information about an auth client

1. On the *FortiProducts* page, identify the auth client of interest, and mouse over it to bring out the slide-in toolbar.
2. Click *Details.*
   The *Detailed Information for Auth Client* dialog opens, showing 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.

1. On the *Auth Clients > FortiProducts* page, identify the auth client of interest, and mouse over it to bring out the toolbar.
2. Click *Delete.*
3. Be sure to read the message.
4. Click *Yes.*

Search for a standalone device

On the top of the *Standalone Devices* panel is a *Search by device's SN* tool. It enables you to search for standalone devices by serial number (SN). It comes in handy when you want to locate a standalone device and add it to an existing cluster.

> 💡 • 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 device's SN.*
2. Type in any part of the serial number of the device of interest.
3. Press *Enter* key on your keyboard.

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

Validate device ownership

Stating with the 21.3.c release, FTC is able to handle device ownership transfer without human intervention, automatically cleaning up user data on the transferred device from the source account.

Below are the use cases that show how FTC handles change of device ownership:

- If you move a device (e.g., FortiGate) license and the FTC license to a new account, your FTC service will continue after the transfer.
- If you move the FTC license to a new account but leave the device in the old account with no other FTC license, there will be no FTC service for the device.
- If you move the device license to a new account where there is another (new) FTC license and leave the old FTC license in the old account, usage from that device now will count against the new FTC license (not the old one).
- If you move the FTC license to a new account but leave the device in the old account, and then add a new FTC license to the old account, usage from that device will count against the new license (not the old one).

Ownership check can be performed only by clicking the *Validate* button from the GUI *[Auth Clients > Devices(HA) > Validate]*.

The *Auth Clients > Devices (HA)* page now has a *Validate Device Ownership* section, which enables you to search for devices in your account/realm and to update the device registration status in FTC in real time.

To validate the registration status of a device:

1. Click *Auth Clients > Devices (HA)*.
2. In the top of the page, enter the device serial number
3. Click *Validate.*

Transfer devices

Device transfer can be handled either directly from Fortinet products that support it or through FortiCare.

Transfer devices from FortiGate

Device transfer can be done directly from the FortiGate GUI. The same is true with some other Fortinet products that support the feature.

To transfer a device on FOS version 6.4.1 or later, or FOS version 7.0.0 or later:

1. Log into the FOS administrator portal.
2. Select the global VDOM (if the multi-VDOM feature is enabled)
3. Click *System > FortiGuard > Under License Information.*
4. Click the *Action* button of FortiCare.
5. Select *Transfer FortiGate to Another Account.*

To transfer a device on FOS version 6.4.7 or later, or FOS version 7.0.1 or later:

1. Log into the FOS administrator portal.
2. Select the global VDOM (if the multi-VDOM feature is enabled).
3. Click *Dashboard > Status >* from the *Licenses Widget.*

4. Click *FortiCare Support.*
5. Select *Transfer FortiGate to Another Account.*

Transfer devices through FortiCare

For FOS version 6.4.0 or earlier, contact FortiCare Technical Support at https://www.fortinet.com/support/contact to request FortiGate account transfer via Live Chat or over the phone. You must have your FortiGate serial number ready, and provide the source account email and the target account email to complete the account transfer. The FortiCare team will send out authorization email to each email recipient for approval. Once they have received the authorization email, they will start the transfer process and notify you when the device transfer has been completed.

Clean up user data from the source account

Clean-up of user data from the source account can be performed from the FTC portal only.

1. Log into `ftc.fortinet.com` using the source or target FC account.
2. Click *Auth Clients > Devices (HA).*
3. Enter the device serial number, and click *Validate.*
4. Read the messages onscreen.
5. Press *Delete* if you want to remove the users from the account. In the warning message, click *Delete*.

After clicking the *Delete* button, wait for a few minutes for the clean-up process to complete before clicking the *Validate* button.

If you click the *Validate* button while the clean-up is in progress, you will see the message, *"Data under this device is being deleted…."*

The clean-up process is completed if you see the *"This device ownership info is up to date...."* message after clicking *Validate* from the target account or the *"Not allowed to check the device info."* message when clicking *Validate* from the source account.

If you do not want to remove the users from the source account, your can transfer the device back to the original account using the instructions in Transfer devices from FortiGate on page 110. You can also contact FortiCare for assistance, if needed.

Add devices to a 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 be removed from the *Standalone Devices* panel.

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

1. In the *Clusters* panel, locate the cluster of interest.
2. In the *Standalone Devices* panel, locate the standalone device of interest. See Add devices to a cluster on page 111.
3. Select the device, and drag it to the cluster on the right.
4. When the *Device Management* dialog pops up, be sure to read the message, and click *OK*.

Remove devices from a cluster

You can remove a device from any cluster in the *Clusters* panel. Once a 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.

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*.

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.

1. In the *Clusters* panel, locate the clusters of interest.
2. Locate the source cluster with the device of interest.
3. Drag the device to the target cluster. The *Device Management* dialog opens.
4. Read the message, click *OK* to proceed.

Migrate device data on FTC

You are now able to migrate device data yourself directly from one FTC account to another on the FTC portal.

To migrate device data:

1. Request a device ownership transfer ticket in FortiCare.
2. Wait until after the ticket is processed and the ownership in FortiCare has been transferred to the new owner. For example, Account A is the original owner, and Account B is the new owner.
3. Now either Account A or Account B can start the data migration request in the FortiToken Cloud portal.

4. If Account A submits the migration request, an email notification will be sent to the owner of Account B, and vice versa.

5. Upon receiving the email notification, the owner of Account B logs into the FTC portal and confirms the data migration.

6. When the owner of Account B clicks the link in the email notification message, the browser will redirect the page to confirm device migration for Account B.

7. After Account B confirms the migration by clicking the Transfer button in the pop-up window, the transfer in process confirm window pops up..

8. The process may take a few minutes, depending on the data size (the number of users). If the following page shows, it means the migration is still in progress.

9. Wait for a few minutes before clicking the *Validate* button. If the following page shows, it means the data migration has completed.

10. The users should show up in the new owner's account, but are not longer available in the old owner's account.

Web Apps

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

The following table highlights the information on the *Web Apps* page.

Parameter	Description
Name	The name of a web app.
Client ID	A unique, read-only ID that FTC has generated for an auth client.
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:** Click the icon to regenerate the secret for the auth client.

Parameter	Description
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

When a new auth client is added, FTC assigns it the default name *"MyAuthClient"* which can be edited. If you add more auth clients of the same type, FTC 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 assign 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 to add end-users to it.

When creating an auth client, FTC generates a unique read-only Client ID. It also generates the API credentials which the auth client needs when accessing the FortiToken Cloud API server.

> ⚠️ FortiToken Cloud API is accessible to licensed accounts only; it is not available for free trial accounts.

1. In the upper-left corner of the *Auth Clients > Web Apps* page, click *Add Web App* to open the *Add New Web App* dialog.
2. Type a unique name over the default name.
3. Select a realm, or leave it to the default.
4. Select an adaptive auth profile.
5. Click *Add.* A window opens, showing the information of the newly added auth client.
6. Click *OK.*

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* icon.
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 that 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 as auth client

1. On the *Auth Clients > Web Apps* page, locate the web app of interest and mouse over it to bring out the slide-in toolbar.

2. From the slide-in toolbar, click *Edit.*

3. Make the desired changes, and click *OK.*

Delete a web app auth client

1. On the *Auth Clients > Web Apps* page, locate the web app of interest and mouse over it to bring out the slide-in toolbar.

2. From the slide-in toolbar, click *Delete.*

3. In the confirmation dialog, click *Yes*.

Management Apps

Starting with its 23.1.a release, FortiToken Cloud introduces the management auth client as a special type of web app auth client. It is a solution for remote API access and management of customer resources, such as realms, auth clients, users, and tokens, etc.

You can access the feature by selecting *Auth Clients > Mgmt Apps*, where you can view/create/edit/delete management auth clients.

When creating/editing management auth clients, you can set their scope for accessing the resources to the entire customer account or the realms that you specify.

Devices (HA)

The *Devices (HA)* page enables you to view and manage authentication clients that are in HA configuration. You can access the *Devices (HA)* page by clicking *Auth Clients > Devices (HA)* on the main menu.

The *Devices (HA)* 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.

This section covers discusses the following topics:

Mobile Tokens

The term "mobile" refers to FortiToken Mobile (FTM) tokens for mobile devices. The *Mobile* page is read-only and shows all FTMs used by end-users in your 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 end-user to whom the FTM has been assigned.
Realm	The realm to which the end-user of the FTM has been assigned. **Note:** The field shows "default" if the auth client associated with the end-user has not been assigned to any custom realm.
Platform	The mobile platform of the FTM, which can be either of the following: • *Android* • *iOS*
Algorithm	The algorithm of time-based one-time password authentication used by the token: • *TOTP*
Registration ID	The registration ID of the FTM.

Hardware Tokens

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

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

Column	Description
Checkbox	If checked, the corresponding hardware 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 118. **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 the hardware token.
Model	The model of the hardware token, which can be one of the following: • *FTK200* • *FTK220* • *Other*

Column	Description
Algorithm	The algorithm of time-based one-time password authentication used by the hardware 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.
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 .

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 .

To add hard tokens manually:

1. On the *Tokens > Hardware* page, click the *Import Tokens* button.
   The *Import Hard Tokens* dialog opens.
2. Enter the serial number of the hard token.
3. Click the *Add New Token* button.
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 *Hardware* 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 *Hardware* 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 Token*s 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 *Hardware* 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 hard token shown on the *Hardware* page without a username means that it has not been assigned to any end-user yet, and can be assigned to any end-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 .
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 *Hardware* page provides tools to delete hard tokens that are no longer needed. You can delete one, multiple, or all the hard tokens at once.

Only unassigned FTK tokens can be deleted.

To delete individual hard 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 hard 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 quota/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 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.
6. If you've select *Daily* (in Step 2 above), click the *Usage Type* drop-down menu and then select one of the viewing options..
   Note: If you have switched from a credit-based license to a time-based license and have some credit-based usage data left in your account, the 'User Count/SMS Credit' chart will show three data categories: Users, SMS-C (as credit-based SMS credit), and SMS-T (as time-based SMS credit), and the other is Credit chart for your credit-based licenses. For old credit-based accounts, FTC still shows the 'User Count/SMS Count' and 'Credit' charts.
7. Click the legend at the bottom of the usage chart to show or hide usage data of your choice.
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 in 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.

Licenses

The *Licenses* page applies to customers of time-based subscriptions only. For more information about the time-based subscriptions, see Time-based subscriptions on page 11.

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

Column	Description
Contract Number	The contract number of the license.
Serial Number	The serial number of the license.
Category	The license category.
Users	The maximum number of end-users that the license can support.
SMS Credits	The maximum number of SMS messages that the license can support.
Remaining SMS Credits	The number of SMS messages available for use.
Status	The status of the license.
Start Date	The date on which the license is registered for use.
End Date	The date on which the license expires.

Adaptive authentication

The adaptive authentication feature is fully supported on FOS 7.0.2.

Multi-factor authentication provides more security than password-only login, but it comes at the cost of inconvenience for end-users. The adaptive authentication feature uses the available information regarding a login attempt (for example, time of day, geo-location, and so on) to evaluate the circumstantial risk of a given login attempt. The second authentication factor is required only when that risk is higher than a predetermined threshold. Furthermore, you might choose to block an authentication attempt entirely if the circumstantial risk is deemed high enough.

FortiToken Cloud (FTC) allows end-users to bypass OTP verification of MFA under certain "safer" conditions and denies such attempts under certain otherwise "riskier" conditions. Upon receiving a request to bypass the OTP verification for MFA authentication, the FTC server assesses the situation and decides whether to deny the attempt to bypass the pre-configured OTP verification of MFA based on the following conditions:

- Trusted subnet/geo-location
- Time of day/day of week

Token bypass is allowed if the end-user meets one of the following conditions:

- End-user IP address is from a trusted subnet
- End-user IP address is from a trusted geo-location
- Time is within the expected schedule

Token bypass is denied if the end-user meets one of the following conditions:

- End-user IP address is NOT from a trusted subnet
- End-user IP address is NOT from a trusted geo-location
- Time is outside of the expected schedule

This section covers the following topics:

View adaptive authentication policies

The *Adaptive Auth > Policy* page displays all the adaptive auth policies in your account. The following table highlights the information on the page.

Parameter	Description
Name	The name of the policy.
Action	The action specified in the policy, which can be one of the following: • *Multi-factor Authentication* (default) • *Block* • *Bypass*

Parameter	Description
	Note: The FTC server takes the specified action when an authentication request matches the policy.
Profile References	The adaptive authentication profile that uses the policy.
Last Update	The date and time of the most recent update of the policy.

Create an adaptive authentication policy

1. From the main menu, click *Adaptive Auth > Policy* to open the *Policy* page.
2. On top of the page, click *Add Policy* to open the *Add New Policy* dialog.
3. Make the desired entries and/or selections, as described in the following table.
4. Click *Confirm*.

Parameter	Description
Name	Specify a unique name for the policy.
Action	Select one of the following: • *Enforce MFA* — By default, the FTC server will require login attempts from the specified source to use MFA. • *Block* — The FTC server will block login attempts from the specified source. • *Bypass MFA* — The FTC server will let the login attempts from the specified source bypass the MFA requirement. **Note:** The FTC server takes the specified action when an authentication request matches the policy settings.
Filters	Select the filter • *Subnet Filter* — See *Subnet Filter* below. • *Location Filter* — See *Location Filter* below. • *No Source Filter* — Select this option if you do not want to use any filter. • *Schedule* — Check the checkbox to enable scheduling. See *Schedule* below for details.
Subnet Filter	**Note:** This option is available only when *Subnet Filter* is selected in the *Filters* field above. Specify the subnet in one of the following formats: • IP address, e.g., 10.10.1.1 • IP range, e.g., 10.10.0.0 - 10.10.10.2 • CIDR notation, e.g., 10.10.1.0/24 **Note:** The *No IP* option is for devices that do not support subnet filtering. If enabled, the policy will be applied to auth requests that do not have IP information.
Location Filter	**Note:** This option is available only when *Location Filter* is selected in the *Filters* field above. • Use the list menu to select the countries or regions of interest.

Parameter	Description
	• Select Unknown Country or Region if the location is unknown.
Schedule	**Note:** This option becomes available only when *Schedule* is selected in the *Filters* field above. Set the schedule using the following parameters: • *Weekdays* — Select the days of the week. • *Timezone* — Select the timezone, which is the timezone of the web browser by default. When an authentication request comes in, the FTC server uses the time of this timezone to match the request. • *Time Range* — Select either *All day* (default) or a specific time frame of the day. **Note:** If the start time is less than or equal to the end time, then the time range would be start time — end time; otherwise, the time range would be 0:00 — end time, start time - 23:59.

Edit an adaptive auth policy

1. On the *Adaptive Auth > Policy* page, mouse over the policy to bring out the slide-in toolbar.
2. Click the Edit tool.
3. Make the desired changes.
4. Click *Confirm.*

Delete an adaptive auth policy

1. On the *Adaptive Auth > Profile* page, highlight the profile of interest.
2. Click *Delete*.
3. In the confirmation dialog, click *Yes.*

View adaptive auth profiles

The *Adaptive Auth > Policy* page displays all the adaptive auth policies in your account. The following table highlights the information on the page.

Parameter	Description
Name	The name of the adaptive auth profile.
Action	The action specified in the policy, which can be one of the following: • *Multi-factor Authentication* (default) • *Block* • *Bypass* **Note:** The FTC server takes the specified action when an authentication request matches the profile.
Realm References	The number of realms that are using the profile.
Client References	The number of auth clients that are using this profile.

Create an adaptive authentication profile

To create an adaptive authentication profile:

1. Click *Adaptive Auth > Profile* to open the *Profile* page.
2. On top of the page, click *Add Profile* to open the *Add New Profile* dialog.
3. Make the entries and/or selections as described in the following table.
4. Click *Save*.

Parameter	Description
Name	Specify a unique profile name.
Default action	Select a default action, which can be one of the following: • *Multi-factor Authentication* (default) • *Block* • *Bypass* (**Note:** If an authentication did not fall into any policies, FTC will take this action on the authentication request.)
Policy Sequence	Select the priority of the policies to be selected below. **Note:** The two policy fields below could be empty (no selection). If no policy is selected, the FTC server takes the default action specified above. When two policies are selected, Policy 1 takes priority over Policy 2.
Policy 1	Select a policy as Policy 1. (Optional)
Policy 2	Select a policy as Policy 2. (Optional)

Apply adaptive authentication profiles

Adaptive authentication profiles can be applied to auth clients and/or realms. A profile applied to auth clients has higher priority than a profile applied to realms. For example, an authentication from Auth Client C under Realm R. Client C has Profile A and Realm R has Profile B. In this case, Profile A is the one that is in effect.

To apply an adaptive auth profile to an auth client:

1. From the main menu, click *Auth Clients > Web App*.
2. Highlight the Web App of interest and click the *Edit* button to open the *Edit Client* dialog.
3. Select an adaptive auth profile.
4. Click *OK*.

To apply an adaptive auth profile to a realm:

1. From the main menu, click *Settings > Realm*.
2. Ensure that the *General Setting* tab is selected.
3. Select an adaptive auth profile.
4. Click *Apply Changes*.

Edit an adaptive auth profile

1. On the *Adaptive Auth > Profile* page, mouse over the profile to bring out the slide-in toolbar.
2. Click the *Edit* tool.
3. Make the desired changes.
4. Click *Save.*

Delete an adaptive authentication profile

To delete an adaptive authentication profile:

1. On the *Adaptive Auth > Policy* page, highlight the policy of interest.
2. Click *Delete*.
3. In the confirmation dialog, click *Yes.*

Create a last-login policy

The Last Login feature enables FortiToken Cloud admins to let end-users use the trusted IP or the trusted subnet login MFA bypass within a specified time period. In so doing, end-users using the trusted IP resources can use the MFA feature more easily in their daily work.

To enable the Last Login feature in an adaptive authentication policy:

1. From the side menu, select Adaptive Auth>Policy, and then select Add Policy.
2. Specify the name of the policy.
3. For Action, select Bypass MFA.
4. For Filters, select Subnet Filter.
5. For Subnet Filter>Subnets, specify the IP or subset. (Note: The IP and Subnet must be supported by FortiProducts).
6. Select the Last Login button and specify a reasonable MFA Interval time period. (Note: The valid values range from 1 to 72 hours.)
7. For Schedule, select a schedule set.
8. Click confirm.
9. Add the new policy to a profile and be sure to select the same action (Bypass MFA).
10. Add the new profile to any auth client (including FortiProducts and web apps) and any realms whose users are going to use the specified trusted IPs or subnets.

Create an impossible-to-travel policy

The Impossible Travel feature helps to improve the security level and blocks suspicious login attempts when FortiToken Cloud detects an unusual login request far away from a reasonable geographical location, for example, a login request from Russia for a device used by an employee who is living in the United States. In that case, FTC will block it. FTC is able to identify suspicious sign-in attempts based on distance and time elapsed between two subsequent user sign-in attempts. The default is 500 miles per hour. Bear in mind that the user IP must be supported by FortiProducts.

To enable the Impossible-Travel feature in an adaptive authentication policy:

1. From the side menu, select Adaptive Auth > Policy.
2. Select Add Policy.
3. Specify the policy name.

   For Action, select Enforce MFA/Block.
4. For Filters, select Location Filter.
5. For Location Filter, select the countries or regions for normal login location.
6. Select the Impossible Travel button to enable it.
7. For Schedule, select a desired schedule set.
8. Click Confirm.
9. Add the new policy into a profile, and be sure to select the same action (Enforce MFA/Block).
10. Add the new profile into any auth client (including FortiProducts and web apps) and any Realms whose users are going to login from the specified locations.

Alarm

The Alarm page enables you to configure alarm events to notify users when their consumption of user quota or SMS credits has reached the specified threshold. Alarms can be applied to your entire account or specific realms in your account. FTC sends out email messages to users specified in the alarm event configuration when the alarm is triggered.

Configuration of an alarm event starts with the configuration of receivers and receiver groups. Receivers are users who receive alert notifications.

- Configure receivers on page 126
- Configure receiver groups on page 126
- Create a user quota alarm event on page 127
- Create an SMS credit balance alarm event on page 133

Configure receivers

1. From the main menu, select *Alarm>Notification>Receiver.*
2. On top of the page, click *Add Receiver.*
3. Specify the receiver name.
4. Enter the email address of the receiver.
5. Enter a description. (Optional)
6. Click *OK.*
7. Repeat the above steps to add more receivers.

Configure receiver groups

1. From the main menu, select *Alarm>Notification>Group*
2. On top of the page, click *Add Groups.*

3. Specify the group name.

4. Enter a group description. (Optional).

5. Select the receivers.

6. Click *OK.*

7. Repeat the above steps to add more receiver groups.

Create an SMS credit balance alarm event

1. From the main menu, select *Alarm>Event.*

2. On top of the page, click *Add Alarm Event.*

3. For *Resources*, select *SMS.*

4. For *Level*, select *Realm* or *Global*. (Note: If Global is selected, the alarm will be applied to your entire account; if Realm is selected, you must select the specific realm or realms from list of realms.)

5. For *Threshold*, enter the numeric value to be used as the SMS credit threshold.

6. Enter a description of the alarm event. (Optional)

7. For *Groups*, select the receiver group(s).

8. Click *OK*.

Create a user quota alarm event

1. From the main menu, select *Alarm>Event.*

2. On top of the page, click *Add Alarm Event.*

3. For *Resources*, select *users.*

4. For *Level*, select *Realm* or *Global*. (Note: If Global is selected, the alarm will be applied to your entire account; if Realm is selected, you must select the specific realm or realms from list of realms.)

5. For *Threshold*, enter a value between 0 and 99 as a percentage.

6. Enter a description of the alarm event. (Optional)

7. For *Groups*, select the receiver group(s).

8. Click *OK*.

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 on page 128
- Management on page 129
- SMS on page 131

Authentication

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

Management logs capture management activities that have occurred on FTC.

To view management logs:

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* 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.

Column	Description
Action	The action of the request, which can be one of the following: • *Create* • *Get* • *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.

SMS

The SMS logs page shows all logs of your SMS usage. The following table shows the information about log entries.

Parameter	Description
Timestamp	The date and time the log entry was generated. Note: This is the timestamp of the web browser in which FTC is operated.
Auth Client	The auth client that sent SMS message.
Realm	The realm to which the auth client is assigned.
Action	The action that FTC took.
User	The end-user upon whom the action was performed.
Country	The country or region where the end-user's phone number is registered.
Rate	The wireless phone rate.

Filter SMS logs

1. In the upper-left corner of the *SMS* page, click the *Filters* icon.
2. Make the desired selections.
3. Click *ok*.

Filter logs by date

1. Click the *From* field and select a start date.
2. Click the *To* field and select an end date.
3. Click *Filter*.

Export SMS logs

1. In the upper-right corner of the SMS page, click the *Export CSV* button.
2. In the Download pop-up, click *Open file.*
3. Save the file on your computer or a location on your network.

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 terms of service, see Service Descriptions.

- For licensing, see Purchasing Guide.

- For SMS rates, see SMS Rate Card.

- For product support issues, click Technical Support (https://docs.fortinet.com/document/fortitoken-cloud/latest/technical-support/891133/technical-support).

Create an SMS credit balance alarm event

1. From the main menu, select *Alarm>Event.*
2. On top of the page, click *Add Alarm Event.*
3. For *Resources*, select *SMS.*
4. For *Level*, select *Realm* or *Global*. (Note: If Global is selected, the alarm will be applied to your entire account; if Realm is selected, you must select the specific realm or realms from list of realms.)
5. For *Threshold*, enter the numeric value to be used as the SMS credit threshold.
6. Enter a description of the alarm event. (Optional)
7. For *Groups*, select the receiver group(s).
8. Click *OK.*

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 23.1.a release.

Global system configuration

FortiOS comes with a "`config system global`" command which enables the FortiGate admin to enable or disable FTC service on 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 or communicate with the remote FTC server.

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

```
config system global
    set alias "FG            "
    set hostname "FG            "
    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.

```
FG            #  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.

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

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

FG████████████  #  execute fortitoken-cloud trial ?
<Enter>

FG████████████  #  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. Each end-user should 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.

- From FOS 6.2.4 and 6.4.0, wildcard LDAP users are automatically synced from the remote AD/LDAP to FTC by FOS when FOS is configured to use FTC for remote wild card users on the remote AD/LDAP server. The frequency of this auto-sync for wildcard AD/LDAP users is once every 24 hours.
- sAMAccountName as cnid is not supported before FOS 6.4.6.

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
```

Migrate FTM tokens to FortiToken Cloud

Starting with FOS 7.0.4, FortiGate customers who are using FOS 2FA perpetual licenses can migrate their FTM tokens to FortiToken Cloud (FTC) by converting their FTM licenses to FTC subscription licenses. FGT admins can perform FTM token migration themselves using the following command:

```
execute fortitoken-cloud migrate-ftm <FortiToken mobile license number> <vdom>
```

where `<vdom>` is root, if VDOM is not enabled on the FortiGate.

> If you do not have an existing FTC license at the time of the migration, FTC will automatically generate a one-year free transfer license for you to use for the number of end-users corresponding to the total number of FTM tokens that are transferred. After one year, you will have to purchase an FTC license to continue using the service.

Procedures

1. Ensure that the FTM license has already been imported into the FortiGate. (The Token serial number under the FTM license may or may not have been assigned to users.)
2. Submit `'set FTM migration tag request'` to Customer Support (https://www.fortinet.com/support/contact) by providing the FGT serial number and the FTM license serial number. The CS team then confirms the pre-authentication from the customer and sets up the 'FTM migration tag'.
3. Once the tag has been set up, run the `execute fortitoken-cloud migrate-ftm <FortiToken mobile license number> <vdom>` command on the FortiGate. The command will transfer all users with FTM token auth under this FTM license to FTC auth method. You can find the FTM license number with the output of the `show user fortitoken` command, which has `set license <FTM license number>`.
4. The tokens under the migrated license are then removed from the FOS GUI, and all users that have been migrated show up on the FTC GUI.
5. Once the migration CLI command is completed, user log auth should work without any token data change.
6. After the migration is completed, FTC will send out email to CS asynchronously 24 hours after the migration of the account. The email is notify CS to invalidate the FTM license and reset the migration tag. If you are migrating multiple FTM licenses, ensure that you migrate them together within 24 hours. Otherwise, you will have to re-submit the `'set FTM migration tag request'` request to CS.
7. After the CS team has invalidated the FTM license and reset the migration tag, you may have to wait for up to 24 hours for the process to complete.

Verification

Check on the FOS portal:

- All users with FTM token auth under this migrated FTM license are updated to FortiToken Cloud on the FGT portal (User & Authentication>User Definition).

- The migrated FTM license is removed on the FGT portal (User & Authentication>FortiTokens). Tokens associated to the migrated FTM license will not show up in the token list.

Check on the FTC portal:

- The migrated FTM license shows up on the FTC portal (Licenses).

Contract Number	Serial Number	Category	Users	SMS Credits	Remaining SMS Credits	Status	Start Date	End Date
EFTM025130933610		FTM Migration License	25	3125	3067	active	12-13-2022	12-13-2023

- The migrated MFA users show up on the FTC portal (Users).
- The migrated FTM license quota has been added to the total FTC user quota and the assigned FTM token has been deducted from the total user quota (Dashboard).

End-user 2FA login authentication

- FTM License migration does not affect end-user 2FA login authentication with FortiToken (i.e., end-users will not notice any change in their login authentication process).

- Back up FortiGate configuration before starting the migration process.
- Once the FTM license and its tokens are successfully migrated to FortiToken Cloud, they cannot be reversed.
- The original FTM license is invalidated by the CS team once the migration is completed.
- The request can be initiated only by a FGT admin.
- FTM token migration is supported for trial accounts.
- FTM token migration is not supported for credit-based accounts.
- Before migrating an FTM license with a large number of associated users, be sure to set the FGT CLI Console timeout long enough to cover the entire process. If the Console times out while the migration is in progress, you can open another Console window and run the `diagnose fortitoken-cloud migrate-ftm show <FortiToken mobile license number>`' command to check the migration status.

Diagnose FortiToken Cloud

Use the following commands to diagnose and troubleshoot FTC issues.

```
debug           Enable/disable debug output.
server          IP address port number and https.
show            Display diagnostics information.
delete          Command to delete a user.
clear           Clear server connection settings for diagnostics.
migrate-ftm     Perform FTM license migration.
set-http        Set HTTP status return code for diagnostics only.
sync            Synchronize user information with FortiToken Cloud.
```

Examples

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

FG███████████     (global) # diag fortitoken-cloud server

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

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

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

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

FG███████████     (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 or later. They do not apply to FOS 6.2.3 which does not distinguish between local and remote users.

```
FGVM            (global) # diagnose fortitoken-cloud migrate-ftm
<string>    Enter command: show, start, abort, add-users, delete-users, ftm2ftc.
FGVM            (global) # diagnose fortitoken-cloud migrate-ftm show
<string>    FTM license number.

FGVM            (global) # diagnose fortitoken-cloud migrate-ftm start
<string>    FTM license number.

FGVM            (global) # diagnose fortitoken-cloud migrate-ftm abort
<string>    FTM license number.

FGVM            (global) # diagnose fortitoken-cloud migrate-ftm add-users
<string>    FTM license number.

FGVM            (global) # diagnose fortitoken-cloud migrate-ftm delete-users
<string>    FTM license number.

FGVM            (global) # diagnose fortitoken-cloud migrate-ftm ftm2ftc
<string>    FTM license number.
```

The above diagnose CLI command shows FTM license migration status, start migration process, abort migration process, add-users into FTC and delete-users from FTC, and force to covert two-factor authentication from FortiToken to FortiToken Cloud during the migration.

FAQs

Licenses

Credit-based

I have a credit-based license with a positive balance. The license will expire in a couple of days, but I am not able to apply a new time-based license. Can you advise how I can get my new time-based license applied to avoid an outage?

No, you cannot apply a time-based license to your credit-based FTC account that still has a positive balance. This is because FortiCare doesn't allow customer account balance to be forfeited. You can only apply a new time-based license after your credit-based account balance becomes 0 or negative.

Meanwhile, FTC offers a 30-day grace period after a credit-based license has expired. During the 30-day grace period, you (FTC admin) will still have full admin access to the FTC portal, your existing FTC end-users will still be authenticated by FTC, and your account usage will continue to be calculated, but you will not be able to add more end-users to your account.

What happens if my credit-based license expires?

- Existing FTC users with MFA auth method as FTM will not experience any difference in the 30-day grace period, and can continue using the existing token assigned to them.
- Existing FTC users cannot use SMS to receive activation codes or OTP. So FTC users with SMS notification and FTC users with SMS auth method will fall back to Email, which means the FTC activation codes or OTP codes will be sent to the users' email addresses registered on FTC.
- The FTC admin will not be able to add more FTC users.

I have a credit-based account with a positive balance when it expires. Why does my balance become negative after the expiration date?

The balance of a credit-based account becomes zero when your license has expired (one year after the license is activated). If your account has existing users, your FTC credits will keep decreasing after the expiration date. So your account will show a negative balance.

Time-based

How many SMS messages will I get with my new time-based license, and how can I use them?

Each time-based license (SKU) allows for SMS messages in the amount of 125 multiplied by the total number of FTC end-users that it can support for a year. For example, if you have a 25-user license (i.e., FC1-10-TKCLD-445-01-DD),

you will be able to use a total of 3,125 SMS messages for the year.

Your SMS quota is always shared among all your users. Allowing sharing of SMS doesn't entitle you to extra user quota, and you must make sure that you have enough user licenses to cover your existing users.

Do the time-based licenses provide the same flexibility as the credit-based ones?

Yes, time-based licenses provide the same flexibility, and you can purchase additional licenses to increase your user quota as needed. Licenses are stackable and co-termed. For co-termed licenses (e.g., adding a new license after an existing license has already been in use for 6 months), your Fortinet sales representative will apply a discount using prorated pricing for 6 months.

How can I purchase a FTC license?

Sales of FTC licenses is handled by Fortinet-authorized resellers only. You must contact a Fortinet-authorized reseller in your region to place your order. For a complete list of Fortinet-authorized resellers, click Authorized Resellers or go to https://partnerportal.fortinet.com/directory/

Is the SMS quota shared by all users? What happens if we've reached the quota limit?

Yes, your SMS quota is shared by all your end-users. If you uses up your SMS quota, any SMS notification beyond the quota limit will fail. You can either buy a new user license (which comes with free SMS) or contact FortiCare Technical Support for assistance.

Which time-based license SKU should I select?

Each FTC time-based license SKU comes with a specific end-user quota limit. Make sure that the new time-based license user quota will cover the number of your existing end-users. For example, if you currently have 32 end-users in your account, you need to purchase the FTC SKU for 50 users.

Free trial

How can I get a free trial license?

FTC trial is auto-enabled after first-time login to the FTC portal or execute CLI command on FGT: "`execute fortitoken-cloud trial`".

See Free trial license for more information.

Do I need to have an FTC license to transfer my FTM license to FTC?

No. If you have no existing FTC license when transferring your FTM license to FTC, FTC will generate a one-year free transfer license for you to use.

After one year, you'll have to purchase an FTC license to continue using the service.

SMS

Are there any guidelines on how the SMS credits are consumed?

The number of FTC credits per SMS message that FTC charges varies, depending on the country or region where the phone number is registered. For example, text messages sent to phone numbers registered in the US or Canada normally cost one (1) FTC credit per SMS message. For more information, see SMS Rate Card.

Can I upgrade or downgrade between the SMS license SKUs?

FortiCare does not support upgrade or downgrade on FortiToken Cloud (FTC) SMS licenses. FTC, however, will base the SMS quota on the number of SMS credits that are currently licensed in FortiCare.

Are these licenses stackable?

Yes, they are stackable.

Can SMS credits be co-termed when purchased at different times?

Yes, contact Fortinet Sales rep or reach out to Fortinet renewal team (renewals@fortinet.com).

FortiTrust Identity

I currently have points-based FortiToken Cloud licenses. Can I switch to FortiTrust Identity?

You can activate it and consume all the points before switching to FortiTrust Identity or contact Fortinet Support to see if they can replace your unused point-based license with a FortiTrust Identity license.

I currently have time-based FortiToken Cloud licenses. Can I switch to FortiTrust Identity?

Yes, you can simultaneously have FortiToken Cloud and FortiTrust Identity licenses.

What will happen to my existing users configured in FortiToken Cloud if I decide to switch to FortiTrust Identity?

Your existing users will continue to use MFA service without any interruptions. You will need to make sure to purchase and activate your FortiTrust Identity license within 30 days after your existing license expiration.

Do I need to purchase FortiToken licenses along with FortiTrust Identity to configure MFA?

The FortiTrust Identity license includes tokens for the FortiToken mobile application. User-friendly push technology simplifies end-user authentication experience by just requiring a swipe or click. If you prefer hardware tokens, you must purchase them separately.

General

How do FTC subscriptions work?

Currently, FortiToken Cloud offers two types of licenses: credit-based licenses and time-based licenses.

For credit-based licenses, 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 time-based licenses, FortiToken Cloud charges its user quotas for its service. Your license is consumed based on the total number of MFA cloud service end-users on your per year.

Can you give an example of FTC flexible licensing options?

FortiToken Cloud offers five time-based licenses that you can choose from based on your needs. Suppose that you start FTC service on August 1, 2021 with a 500-user license (i.e., FC3-10-TKCLD-445-01-12) which expires on August 1, 2022. On October 15, 2021, you decide to add 100 more end-users to your account, so you purchase another license for 100 end-users (i.e., FC2-10-TKCLD-445-01-12). Those two licenses are independent of each other. The 500-user license will expire on August 1, 2022, and the 100-user license will expire on October 15, 2022.

You can also renew existing time-based license by requesting a co-term license. For example, on December 1, 2021, you want to add a 25-user license which expires on the same date as the 500-user license. In this case, the new co-term license will be stacked on top of the original 500-user license. The cost of new license will be prorated so that it expires on August 1, 2022 as the original 500-user license.

For more information, see Time-based SKUs and their services on page 11 and SKUs vs. auth clients and realms supported on page 12 in the Admin Guide.

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

Check your account credit balance (if you are on a credit-based license) or your available user quota (if you are on a time-based license) to ensure that you have enough credit or user quota. The FortiToken Cloud server prevents users from issuing new FTC tokens when their account has a zero or negative credit or quota. To resolve the issue, you must purchase a new time-based license under your account ID and apply it to your account.

How do I register my FortiToken Cloud license to use the service?

Once you've set up your FortiCloud account, your account automatically becomes a trial account when you log into the FTC portal for the first time. Your FortiToken Cloud free trial will last for up to 30 days, after which you must purchase a time-based annual license to continue using FortiToken Cloud service.

For FortiCloud Premium customers, the free trial license can support up to of 25 FTC end-users; for FortiCloud Non-premium customers, the limit is five FTC end-users per trial license.

Neither free trial license offers SMS messaging service.

How can I renew with a time-based license after my credit-based license has expired or credits have been exhausted? How will the transition affect my FTC service?

You can renew your service by purchasing a time-based license and importing it into your FortiCare account. If you encounter any issue, please reach out to our FTC team who will be more than happy to assist you with a smooth transition.

Transitioning from credit-based licenses to time-based licenses will not affect your current FTC configurations at all. After the transition, your FTC service will continue operating as before, with some new features available only to time-based licenses.

I have purchased a credit-based license, but have not activated it yet. What are my options if I want to switch to a time-based license?

You can contact your Fortinet sales representative for a refund of the un-used credit-based license, and then purchase a new time-based license.

Upon activating my time-based license, I realize that I still have a credit-based license with unused credits. What can I do?

Because you have already activated your time-based license, you won't be able to use your credit-based license any more. Please contact Fortinet Support for assistance.

How come I still have a negative balance after activating a new license?

It all depends. For example, your old license expired in February 2021, but you activated a new license in June 2021 and assigned six users (one token each) from the last 15 months. You will still see a balance of -20.54 after applying the new license. This is because your first license were activated in February 2020 and the new license was in June 2021. So for the four months between February 2021 when the old license expires and June 2021, usage has to be deducted from your account with 0 balance. Because your old license expired in Feb 2021, unused quota in that license are cleared off your account in that month.

Will expired licenses show on FTC Licenses page?

No, the Licenses page only shows non-expired licenses.

How can I know that my license is going to expire?

The FTC portal will show an alert message if the license is going to be expired in 30 days.

What's the resource quota formula for licensed accounts? What will happen to my resource quota if I apply a time-based license after my credit-based license has expired or been used up?

Quota formula for credit-based accounts:

- License balance quantity = X
- If X <= 120, User Quota = 120
- If 120 < X <= 1,200, User Quota = 1,200
- If 1,200 < X <= 12,000, User Quota = 12,000
- If 12,000 < X <= 120,000, User Quota = 120,000
- If X > 1,200,000, User Quota = 1,200,000
- Realm Quota = min (User Quota/10, 120,000)
- Auth Client Quota = Realm Quota

Note: X is the total balance quantity from all the activate licenses in your account.

The following table shows some credit balances and their corresponding resource quotas.

License balance	User quota	Realm quota	Auth client quota
120	120	12	12
1,200	1,200	120	120
12,000	12,000	1,200	1,200

Quota formula for time-based accounts:

- License user pack = X
- User Quota = X
- Realm Quota = 500 + X/10 if X > 500 else = X
- API Auth Client Quota = max (X/10, 5) if X > 0 else = 0

Note: X is the total user pack from all activated licenses in your account.

The following table shows some total user packs with their corresponding resource quotas.

License user pack	User quota	Realm quota	API auth client quota	Fortinet product auth client quota
25	25	25	5	No limit
100	100	100	10	No limit
500	500	500	50	No limit
2,000	2,000	700	200	No limit
10,000	10,000	1,500	1,000	No limit

Once a time-based license has been applied after your credit-based license has expired or been used up, your resource quota will be recalculated based on the applied time-based license. For example, If you have a credit-based license and

the balance is between 120 and 1,200, you will have a 1,200-user quota, a 120-realm quota, and a 120-auth-client quota. Once the credit-based license has expired or been used up, you apply a time-based license with a 100-user pack per year, you will have new resource quotas based on the time-based license, the user quota is 100, the realm quota is 100, the API auth client quota is 10, and an unlimited auth client quota for Fortinet products.

Accounts

What should I do if I am not able to access to ftc.fortinet.com?

Sometimes, you may get "Error: Get Accountlist Failed" when trying to access the FortiToken Cloud portal. We recommend that you contact FortiCare Technical Support for assistance.

What should I do if I receive "Unauthorized (Your account cannot be found)" message?

Sometimes, you could get the "UNAUTHORIZED (Your account cannot be found.)" error when trying to log into support.fortinet.com with a valid FortiCloud account.
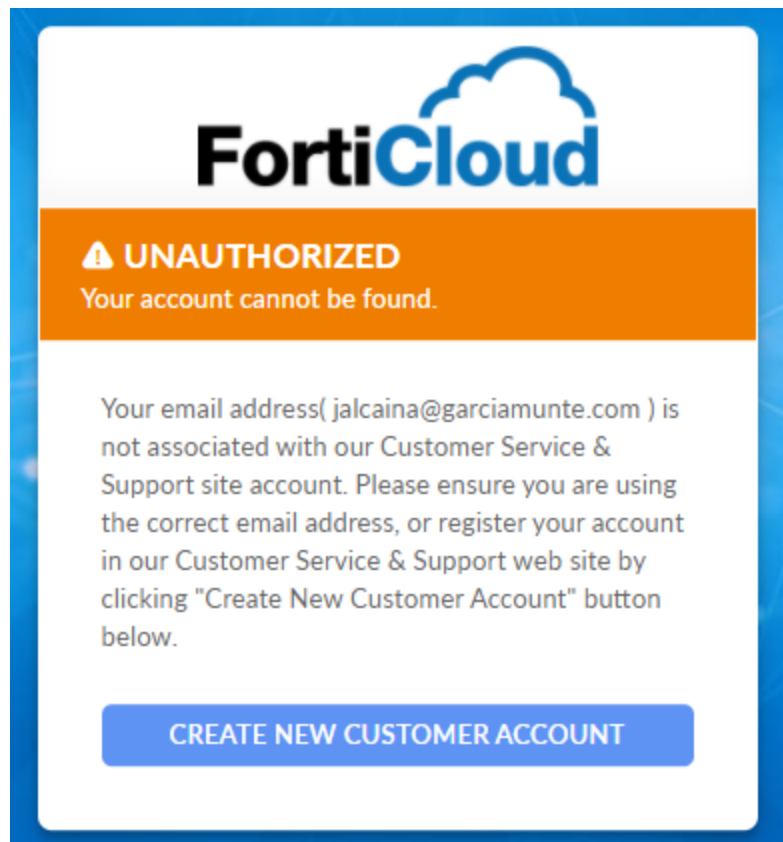
If you encounter that error, please contact our FortiCare team at https://www.fortinet.com/support/contact for assistance.

If I switch to FortiCloud Premium after enabling FTC trial, will my FTC trial quota be updated to 25?

No. FTC won't update trial account quota for users/realms if you switch to FortiCloud Premium after your FTC trial has already been enabled.

Does an FTC time-based trial account support user quota allocation?

No. Only licensed time-based account can support flexible user quota allocation for realms.

Administrators

Why a newly created sub-account cannot see FTC end-users from FTC portal but the master account and other sub-accounts can?

Sub-accounts need to be added to a group and the group needs to have realms under its management to see resources under the realm.

By default, there is a global admin group, which can see all the realms. The first account to log into FTC portal will be automatically placed in this global admin group. The master account is also by default the global admin. All other sub-accounts will have to be added to a group to manage any realms.

Depending on the intended realms for the sub-account to manage, you can add individual realms for it to manage or add the sub-account in the default global admin group so it will see all the realms as the master account does.

For more information, visit https://docs.fortinet.com/document/fortitoken-cloud/latest/admin-guide/271410/administrators

Settings

Global settings

What will happen if multi-realm mode is disabled/enabled?

When multi-realm mode is disabled, any new auth client will be assigned to the default realm; when multi-realm mode is enabled, any new auth client registered in FTC will be automatically assigned to a new realm.

Note that pre-generated auth clients pushed to FortiToken Cloud from FortiGate will not be assigned to any realm. You cannot add or sync users from those auth clients until the FTC admin has associated them to a realm

Why can quota still be allocated to realms when share-quota mode is disabled?

For time-based licenses account, the Share-quota Mode only controls the unallocated user quota that can be shared by all realms. It does not control the user quota already allocated to a realm, but has not yet been used.

Realm settings

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 79.

Realms

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 realms, view realm permission, delete realm, and view realm settings.

For more information, see Realms on page 105.

How to add a FortiGate to a ftc.fortinet.com realm?

Situation:

I have two FortiGate 500Ds which are of the same mode and configuration and registered under the same account, but are not in any HA cluster. One is up and running, and is already recognized by ftc.fortinet.com, and our users are using it for MFA. The other is currently powered down. How can I add it to the ftc.fortinet.com realm?

Here's what you need to do:

1. Power up the FortiGate, and enable Multi-Realm Mode on the FortiToken Cloud portal (Settings>Global>Multi-realm Mode if multi-realm is disabled).
2. In the FortiGate CLI, run the command `exe fortitoken-cloud update` to add it to the same realm. **Note:** This command only sends the VDOM list and creates an auth client, but does not assign it to the realm.
3. Assign the auth client corresponding to the VDOM where the users exist to Realm FGT5HDxxxxxxxxxx-root.
4. On the FortiToken Cloud portal (Auth Clients>FortiProducts), select Realm FGT5HDxxxxxxxxxx-root for the new Auth Client.
5. Make sure that there users on the FortiGate. **Note:** This FortiGate should have the same Fortitoken-Cloud users because it has the same configuration as the other FortiGate.
6. In FortiGate CLI, run the command `exec fortitoken-cloud sync` to sync users again.

How come my old VPN token stops working after I add a new one?

This may be because the auth clients are in different realms. Migrating them to the same realm can solve your issue.

Assume that you currently use FortiToken Cloud for SSL VPN. When you activate a token for VPN 2, the (already setup) VPN 1 token may stop working if the users are in different realms even though the email for both token is the same. So if you wan to use the same FortiToken on all your FortiGate devices, you must move the users and auth clients into the same realm.

Auth clients

FortiProducts

How to add a second FortiGate to a 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 VDOM 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 many auth clients can FortiToken Cloud support? What about the number of HA clusters?

The maximum number of auth clients in your account is determined by your license. You can find out that value from the FortiToken-Cloud Dashboard (https://ftc.fortinet.com/dashboard/root).

From the FTC 21.2.d release, there is no limit to the number of Fortinet Products as auth clients, and the number of Web Apps as auth clients is determined by your FTC license.

We don't set any limit to the number of clusters, but when a VDOM of a FortiProduct cluster (if no VDOM concept in the product, the default VDOM is 'root') connects to FortiToken Cloud, FortiToken Cloud will create a Auth Client for the VDOM. So the number of supported clusters is actually fewer than or equal to the number of auth clients, depending on how many VDOMs are connected to FortiToken Cloud.

Web Apps

How to check the auth status of a 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.

Users

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 on page 102.

Why can't I add end-users to a new realm when I haven't reached the maximum user quota?

Check the user quota allocation for each realm on the Realms page. If quotas have been allocated to some realms, those quotas are taken up even though no users have been created with them. In this case, you are not able to use those quotas to add users to other realms. You can resolve the problem by either taking back the allocated quotas that have not been used or deleting unused realms with allocated quotas.

Device transfer

How do I transfer my FortiGate to a new FortiCloud account and keep using FTC service with the left-over quota?

If for some reason your existing FortiCloud account, e.g., accountA@gmail.com, does not work, you can transfer your FortiGate to a different FortiCloud account, e.g., accountB@gmail.com, to continue using FTC service.

The following steps show how to transfer a FortiGate between FortiCloud accounts.

Step 1: Transfer the FortiGate using the FortiOS Administrator portal

- The following instructions apply to FOS version 6.4.1 or later and FOS version 7.0.0 or later only.
- For FOS version 6.4.0 or earlier, contact FortiCare Technical Support at fortinet.com/support/contact to request FortiGate device transfer via 'Live Chat' or by phone. You must have your FortiGate serial number ready to complete the transfer.

1. Log into the FOS administrator portal.
2. Select the global VDOM (if multi-vdom is enabled).
3. Click System>FortiGuard>Under License Information.
4. Click the Action button of FortiCare.
5. Select "Transfer FortiGate to Another Account".

Step 2: Clean up user data from the old FortiCloud account from FortiToken Cloud.

Option 1

Manually delete the existing auth clients from the old FortiCloud account from the FTC portal:

1. Click Auth Clients>FortiProducts.
2. Select all auth clients associated with the FortiGate serial number registered under the old account.
3. Click Delete.

> If you cannot access your old FortiCloud account any more, contact FortiCare Technical Support for assistance.

Option 2

Clean up user data from the FTC portal via the Validate Device Ownership page:

1. Log into ftc.fortinet.com with the source or target FC account.
2. Click Auth Clients > Devices (HA).
3. Enter the Device serial number, and click Validate.
4. Read the messages onscreen.
5. Press **Delete** to remove the users from the account.
6. In the warning message, click **Delete.**

After clicking the **Delete** button, wait for a few minutes for the clean-up process to complete before clicking the **Validate** button. If you click the **Validate** button while the clean-up is in progress, you will see the message of "Data under this device is being deleted…".

The clean-up process is completed if you see the "This device ownership info is up to date...."message after clicking **Validate** from the target account or the "Not allowed to check the device info." message when clicking **Validate** from the source account.

Step 3: Make sure the new FortiCloud account has enough license to support the users on the FortiGate.

Step 4: Upon confirmation of your account transfer, update your auth client(s) to your new FortiCloud account using the FortiGate CLI.

Execute `exe fortitoken-cloud update'

Step 5: Update FTC user to new account using the FortiGate CLI.

Execute `exe fortitoken-cloud sync'

> If you encounter the "new-created on FGT doesn't sync over to FTC portal from Auth Client > Count is 0" error, you must manually associate the auth client to a realm on the FTC portal:
> 1. Click Auth Client>Edit Auth Client.
> 2. Select the realm, and then click **Apply.**

Tokens

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'.

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
   ```
   Note: You can skip Step 2 if you are using FOS 6.2.4 or later which has Fortitoken-Cloud service enabled by default.
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 25 in the Admin Guide.

Are FortiToken and FortiToken Cloud the same?

Some customers with FortiToken licenses have enabled some users on their FortiGate to use FortiToken-Cloud MFA, but don't see those users assigned on the FortiToken Cloud portal. They are wondering if they have to do something on FortiGate to make it work.

The answer is that FortiToken licenses are different from FortiToken-cloud licenses which are issued from FortiToken-Cloud server. Only users with Fortitoken-Cloud MFA authentication are visible on the FortiToken-Cloud portal (ftc.fortinet.com).

The following table highlights the differences between FortiToken and FortiToken-Cloud licenses.

Type	FortiToken	FortiToken Cloud
License Redemption Certification Serial Number Format	EFTMxxxxxxxxxxxxx.pdf	FASxxxxxxxxxxxxx.pdf
License Serial Number Format	FTKMOBxxxxxxxxxx	FTCxxxxxxxxxxxxx
Where to Register/Import License	FortiGate Portal>User& Authentication>FortiTokens> Create New>Input registration code in License Redemption Certification .pdf file	https://support.fortinet.com > Register Product
Where to display after registration	FortiGate portal>User& Authentication>FortiTokens (It lists all imported FortiToken.)	FortiToken-Cloud portal (ftc.fortinet.com)>Tokens (It only displays all activated FortiToken-Cloud tokens.)
How to assign to admin and local user	FortiGate portal>User& Authentication>User Definition> Create New>Authentication Type: FortiToken	FortiGate portal>User& Authentication>User Definition > Create New>Authentication Type: FortiToken-Cloud
Visible on ftc.fortinet.com	No	Yes

If I have 100 users with 100 mobile or hard tokens, can I assign them to 10 FortiGate auth clients?

Yes. For FortiGate, you can use FortiToken-Cloud tokens for global admins, e.g., "#administrators" and one VDOM admins e.g. "root" VDOM, it means each cluster will use two auth clients, one for "#administrators" VDOM and another one for "root" VDOM, then the number of supported clusters will be 5."

Why can't I issue a new FortiCloud token to a new admin user?

It is because your have used up all your user quota in your current license. You must have a positive quota balance to issue a new token for the new admin. You can purchase a new FTC license using your customer ID.

For more information, refer to the Purchasing Guide.

Is it possible to use one token on multiple FortiGate HA systems?

Yes, FortiToken Cloud supports that. FTC treats users with the same username (by default) in the same realm as the same user and assigns one only token for that user. All you have to do is to move those auth clients with the users to the same realm so that the users with the same username will be identified as the same user.

To move auth clients to a realm, you can edit those auth clients by changing their realm assignment to the desired realm on the Auth Clients>FortiProducts page, where you can locate the auth client and then use the Edit tool to reassign it to the desired realm. This will move all the users on the auth client to the same realm, and those users can share one token.

If a user exists at Auth Client 1/Realm 1 and Auth Client 2/Realm 2, the user needs two tokens, let's say Token 1 in Realm 1 and Token 2 in Realm 2.

If you move Auth Client 2 from Realm 2 to the Realm 1, the user's Token 1 in Realm 1 will be kept and Token 2 in Realm 2 will be deleted, so the user can use Token 1 at the Auth Client 1 and Auth Client 2.

If, after moving the same users to the same realm, you have trouble identifying which token should be used, you can assign a new token for the user. This will delete Token 1 and Token 2 altogether and the user will use the new token instead.

Can I use the same FortiToken Cloud token for users with different usernames on different FGT serial numbers?

Yes. The FortiToken Cloud user alias feature is just for that purpose. You can create a user alias for a group of users with different usernames and let them share the same MFA method. Different users under the same aliased user to share the same token with the base user.

To create a aliased user:

1. On the FortiToken Cloud portal, click the **Users** menu to open the Users page.
2. Select all users whom you want to share the same token.
3. On top of the Users page, click **Add User Alias**.
4. Choose a base user for all selected users, and follow the prompts onscreen to create the user alias.

Note:

- One or more aliased users can be created for one base user.
- A newly added alias shows in black bold-faced characters on the Users page.
- The MFA method and token serial number assigned to the base user are shared by aliased user(s).
- All users to be aliased must be in the same realm.

FTC LDAP

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+ngLSf3ynkLF4So9AmAn6zNqbRHqQOEwSM5jP1p2BNNdnpCHJlo06u
FwQmySdvUm6CYhXsD/zNB3T4XkTIDqTy5g43/Fq0CavX7sXtI485chKKaAU5HRO6xf+/0+2ZeBj2qlHxOxO7Qz1j2Wkq
kN+bRyAGkVUDOkw==
    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 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.

Can I import wildcard LDAP users directly from the FTC portal if somehow some LDAP users cannot sync over to FTC?

The FTC portal doesn't support LDAP users import. You can import wildcard LDAP users from FortiGate only. Here are the steps:

Step 1: On FortiGate, disable LDAP wildcard to avoid any potential conflict or error.

```
config user ldap
        edit "your_ldap_server_name"
                unset two-factor fortitoken-cloud
        end
```

Step 2: Import LDAP user(s) by following the steps in the link below:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Importing-LDAP-user-and-applying-two-factor-email/ta-p/195678

Step 3: Configure the following settings for each LDAP user upon import.

```
config user local
        edit "your_ldap_user"
                set type ldap
                set two-factor fortitoken-cloud
                set email-to youremail@gmail.com
                set ldap-server "your_ad_ldap_server_name"
next
```

Step 4: Check to ensure that you have received new FTC activation codes for all imported LDAP users.

Step 5: Go to the FTC portal to check if the users are shown on the Users page.

FortiOS FTC CLI

What is 'fortitoken-cloud show' command for?

On FOS 7.0.0 and earlier versions, this command shows FortiToken-cloud service status, service balance, existing FTC users, and the maximum number of FTC users; on FOS 7.0.1 and later versions, it adds customer ID info.

The following is an example output of this command:

```
    FGT_TEST (global) # exe fortitoken-cloud show
```

```
FortiToken Cloud service status: licensed, service ready.
Service balance: 36.66 points. Customer ID: 908147.
FortiToken Cloud account number of users: 28, max number of users: 1200.
```

How to add SMS configuration on FortiGate to activate FortiToken-Cloud 2FA via VPN SSL?

(Note: In this case, the customer already has subscription with their SMS provider.)

Yes, you can configure it either in the FortiGate CLI or on the FortiToken-Cloud portal, but you cannot set it from FortiGate GUI. The process of setting it on the FortiToken-Cloud portal is straightforward, but setting it from the FortiGate CLI will overwrite the existing SMS settings on the FortiToken-Cloud portal.

Configure SMS on FortiGate CLI:

```
FGT-TEST (local) # edit test123
new entry 'test123' added
FGT-TEST (test123) # set two-factor fortitoken-cloud
FGT-TEST (test123) # set two-factor two-factor-authentication
FGT-TEST (test123) # set two-factor-authentication sms
FGT-TEST (test123) # set sms-custom-server [customer sms provider]
FGT-TEST (test123) # set sms-phone +(countrycode)4082357700
```

Configure SMS on FortiToken Cloud portal

1. On the main menu, click **Users** to open the Users page.
2. Select user 'test123' and click the **Edit** tool to open the Edit User dialog.
3. For **Auth Method**, select FTM.
4. For **Notification Method**, select SMS.
5. For Mobile Phone, enter +(country code) (area code) (phone number, e.g., xxx-xxxx)
6. Click **Apply.**

What is the 'execute fortitoken-cloud sync' command for?

This command compares the FTC end-users on the FTC server with those on the FortiGate and synchronizes the difference between them. If some users are deleted from FortiGate but still remain on FTC, FortiGate will issue delete request for those users; if there are users enabled for FTC on FortiGate but not on FTC, it will include user creation in the sync request.

FortiOS Admin

How can I log back into FortiGate if I (an FTC admin user) have been locked out because my FTC license has expired and/or the FGT has been removed from the FTC portal?

Even though an FGT admin user has already been removed from FTC, the user still remains in FGT with FTC MFA. So if you want to log back into FGT after you have been removed from FTC, you must first log into FGT in maintainer mode to factory-reset using the `exe factoryreset` command.

You need to provide the following information to log in in maintainer mode:

- Username: maintainer
- Password: The password is bcpb + the serial number of the firewall (Letters of the serial number are in UPPERCASE format, for example, bcpbFGT60C3G10xxxxxx.)

Then, you can log in FGT with the default admin username and password.

If you have backed up the FGT configuration file, you can edit the file and remove the line `'set two-factor fortitoken-cloud'` under admin user configuration, and then upload the modified configuration which has 2FA removed.

If you did not back up the FGT configuration file, you can factory-reset in maintainer mode and then configure the FortiGate from scratch.

> ⚠️
> - Maintainer mode doesn't support backup/restore of FGT configuration. The FGT admin can only factory-reset and set admin user password in maintainer mode.
> - Exercise caution when deleting auth clients from the FTC portal.

FortiAuthenticator

Why can't I receive email OTP, SMS OTP, FTM OTP, or FTM push notification when end-users log in to FTC through RADIUS service in FortiAuthenticator?

You must enable communication between FAC and FTC on the FAC GUI (**Authentication>RADIUS Service>Policies>Allow FortiToken Mobile push notifications**).

Miscellaneous

When trying to access FortiAnalyzer Cloud, it prompts me for a mobile token. Can you help?

Currently, FortiToken Cloud does not support FortiAnalyzer Cloud, and does not provide MFA access to other FortiCloud portals.

Please contact the FortiCare team for assistance.

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 Features and benefits.

23.1.a

Release date: March 16, 2023

- **Delete users from FTC portal** —FortiToken Cloud now allows you to delete users on the portal. (Note: Changes made on the portal will not automatically sync up with the auth clients.)
- **Process future licenses and update service notification**—FortiToken Cloud will send email alerts to customers who don't have enough user quota or whose licenses are to expire in the next 30 days. FortiToken Cloud supports and considers the purchased future co-term licenses when counting the expiration date.
- **OU login**—OU login enables OU admins to manage resources of different customer IDs that join the same organization/OU.
- **Self-service device transfer with data**—You can now transfer devices along with related data from one customer to another on the portal with the *Validate Device Ownership* button on the *Auth Client > Devices (HA)* page.
- **Management client** —FTC has introduced the new concept of management client as a special type of web app client. The management client is a solution for remote API access & management to selected or all customer's resources such as realms, auth clients, users, and tokens, etc.
- **Customized alarm based on a specific resource usage—**This feature enables you to configure alarm events to notify specified recipients when consumption of resources like user quota or SMS credits has reached the specified threshold. Alarms can be applied to your entire account or specific realms in your account.

22.4.a

Release date: November 28, 2022

FortiToken Cloud 22.4.a offers the following new feature:

- Temporary tokens for activated users
- Restricted access for disabled customers
- FortiToken Cloud services status on the monitoring page
- More information of realm/user quota usage on the Realms page
- A new button on the Realms page to show whether share-quota mode is enabled
- Last login
- Impossible to travel

22.3.a

Release date: July 19, 2022

FortiToken Cloud 22.3.a is a patch release only; no new feature or enhancement has been implemented in this release.

22.2.d

Release date: June 30, 2022

FortiToken Cloud 22.2.d is a patch release; it also offers the following new feature:

- Account Disable/Delete Notification

22.2.c

Release date: June 1, 2022

FortiToken Cloud 22.2.c is a patch release only; no new feature or enhancement has been implemented in this release.

22.2.b

Release date: May 9, 2022

FortiToken Cloud 22.2.b is a patch release only; no new feature or enhancement has been implemented in this release.

22.2.a

Release date: May 4, 2022

FortiToken Cloud 22.2.a offers the following new features and enhancements:

- Location Filter by country/region on Adaptive Auth page
- Auth client hyperlink on Users page
- FTM migration email notification enhancement
- Email notification to notify customers of the upcoming closure or removal of their accounts
- FortiTrust License support
- SMS License support
- User post/put API enhancement
- FortiAuthenticator SMS notification API

- SMS logs for time-based accounts on Logs page
- SMS usage from count to credit for time-based accounts

21.4.d

Release date: January 18, 2022

- FTM token migration from FGT to FTC

21.4.a

Release date: October 11, 2021

FortiToken Cloud 21.4.a is a patch release only; no new feature or enhancement has been implemented in this release.

21.3.d

FortiToken Cloud 21.3.d is a patch release, with the following new feature:

- Enhancement to the Validate Device Ownership page

21.3.c

- Adaptive authentication
- Validation of device ownership
- Username case and accent sensitivity (enable/disable)

21.3.b

FortiToken Cloud 21.3.b is a patch release only; no new feature or enhancement has been implemented in this release.

21.3.a

FortiToken Cloud 21.3.a is a patch release only; no new feature or enhancement has been implemented in this release.

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 116.
- **Global administrator and sub-admins**—FTC now enables the global administrator to create sub-admins and allocate resources to them. See Administrators on page 97.
- **Multi-realm support**—FTC now allows the global admin to create realms. See Realms on page 105.
- **More MFA methods**—This release adds support for e-mail, SMS, and FTK (FortiToken, which is a hardware token) as options for MFA. See Realm on page 79.

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 Realm on page 79 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 Realm on page 79 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 Features and benefits.

Technical support

We, Fortinet, provide free technical support to all our customers with valid product licenses.

Prepare for technical support

In order for us to expedite your technical support request, be sure to have the following information ready when creating the support ticket:

- Your FTC account ID, the serial number and version number of your FortiProducts (e.g., FortiAuthenticator, FortiGate), including FortiClient version if using FortiClient.
- A detailed description of your problem, including relevant background information. If the issue is about login auth failure, be sure to provide your FTC username, token serial number, and the version of the FortiToken mobile app.
- Debug log(s), error message, and/or screenshots, if available.
- Your troubleshooting steps and the result.

How to get your Fortinet product serial number

Providing your Fortinet product serial number will help use expedite your service request. How you get your Fortinet product serial number depends on your license category, as discussed in the following paragraphs.

Cusotmers on time-based licenses

If you are using a time-based FTC license, follow the steps below to locate your Fortinet product serial number before creating a technical support ticket:

1. Log into the FortiToken Cloud portal.
2. On the left-side menu, select *Licenses* to open the Licenses page.

	Contract Number	Serial Number	Category	Users	SMS	Remaining SMS	Status	Start Date	End Date
	8708SF830178	FTKCLD0000000103	FTC Subscription License	100	99937	99930	active	07-21-2021	07-21-2022
	7592RZ239356	FTKCLD0000000103	FTC Subscription License	10000	10000000	10000000	active	02-16-2022	02-16-2023
	9399WB062003	FACCLDTM22000001	FortiTrustID License	2000	0	0	active	05-03-2022	05-03-2023
	FTKMS4714167232	FTKCLD0000000103	FTC SMS License	N/A	2500	2500	active	05-03-2022	05-02-2025
	FTKMS4714167233	FACCLDTM22000001	FTC SMS License	N/A	2500	2500	active	05-03-2022	05-02-2025

Items per page: 10   1 - 5 of 5

FortiToken Cloud

- Dashboard
- Administrators
- Realms
- Users
- Auth Clients
- Tokens
- Usage
- Licenses

3. Take note of the serial number for the contract which you are having trouble with.

Customers on credit-based licenses

If you are using a credit-based license, follow the steps below to get your serial number before creating a technical support ticket:
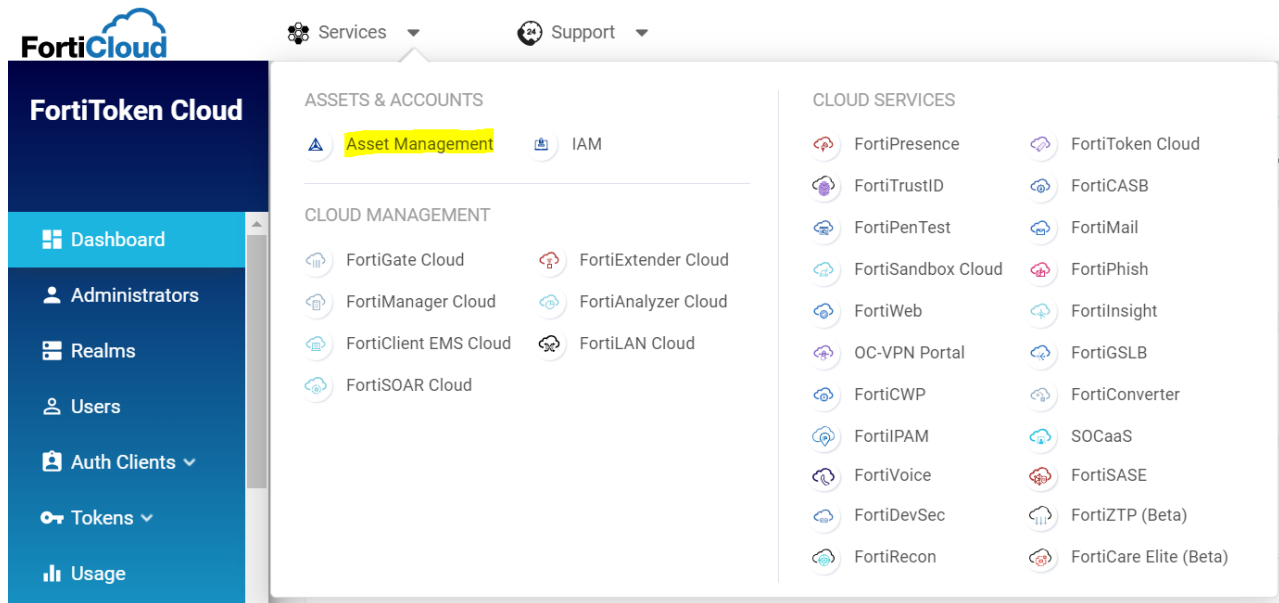
1. Go to *Services > Asset Management.*
2. Select *Account Services.*
3. Find and take note of your FAS service serial number.
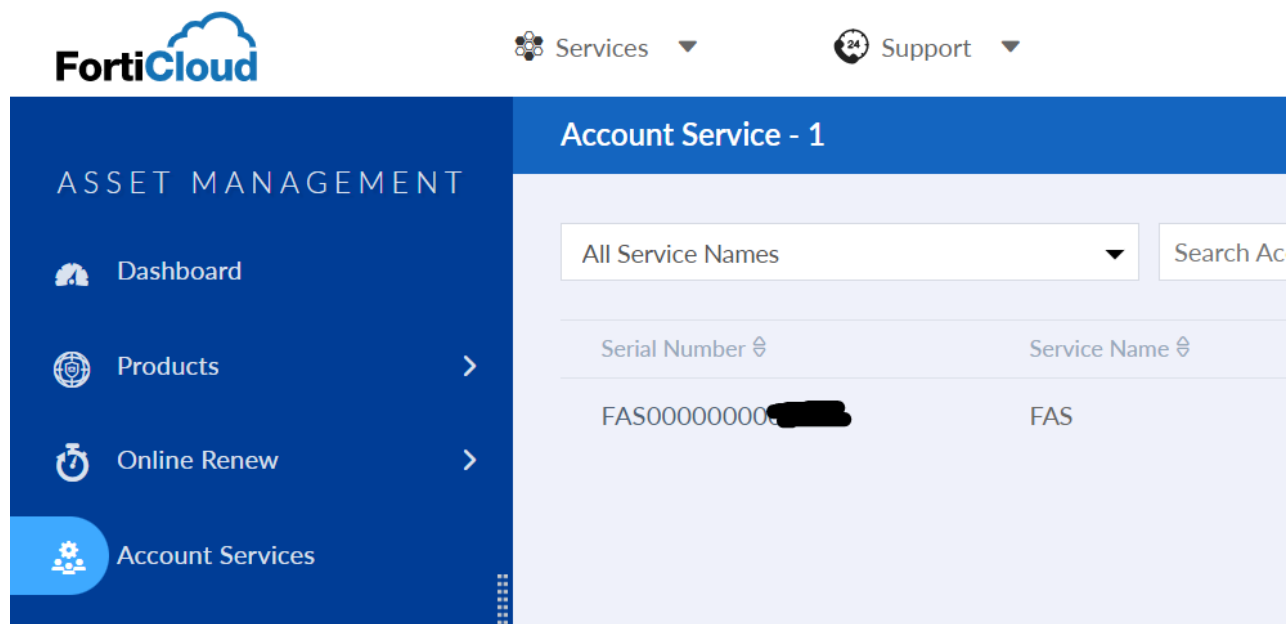
Customers with FTM Tokens migrated from FortiGate to FTC

If you have migrated your FTM tokens from FortiGate to FTC, take the following steps to get your serial number before creating a technical support ticket:

1. Got to *Services > Asset Management.*

2. Click *Products > Product List* to get the serial number of your FortiGate.
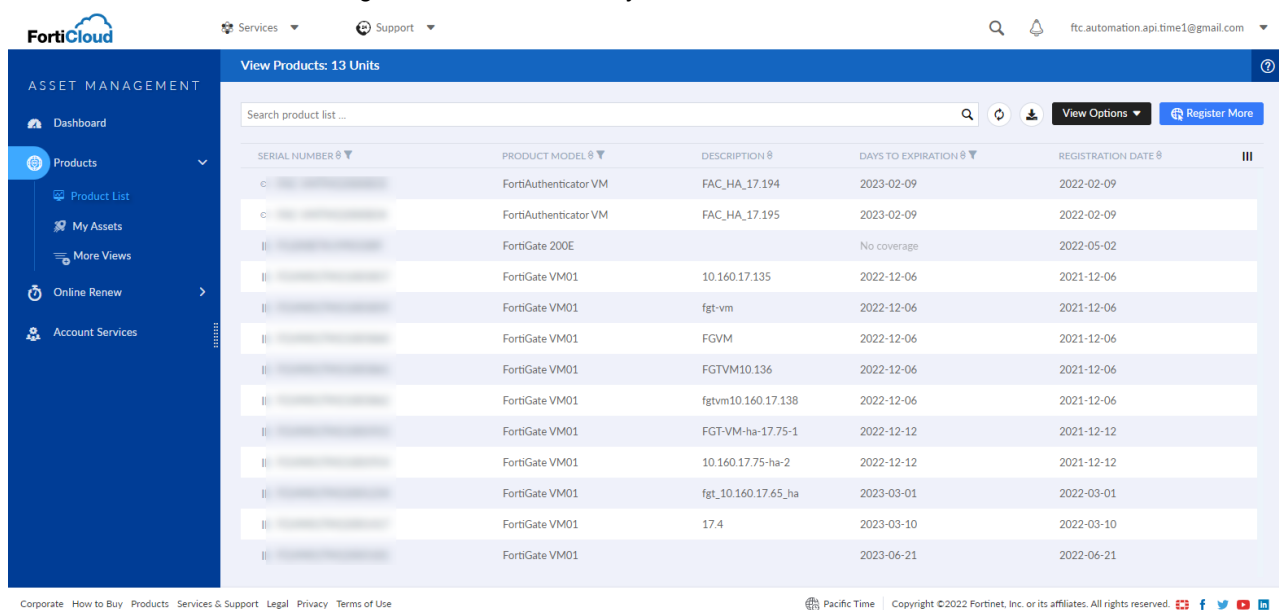
Create a technical support ticket

1. From the top of the FTC GUI, select *Support>Create a Ticket.*
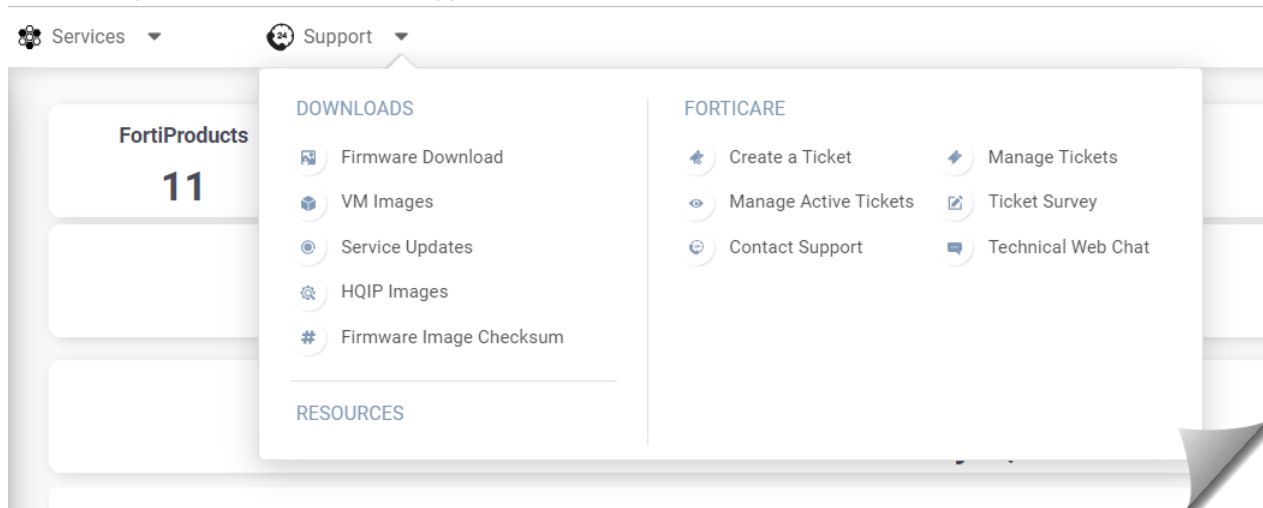
2. Select *Technical Support Ticket*, enter the serial number of your license, and click *Submit Ticket*.

⚠	The instructions above apply to paying customers with valid licenses only. If you are using a free trial version of FortiToken Cloud and have questions about contracts, licenses, and account management, please create a 'Customer Service' ticket instead.

Change log

Release Date	Product Version
03/16/2023	FortiToken Cloud 23.1.a
11/28/2022	FortiToken Cloud 22.4.a
07/19/2022	FortiToken Cloud 22.3.a
06/30/2009	FortiToken Cloud 22.2.d
06/01/2022	FortiToken Cloud 22.2.c
05/09/2022	FortiToken Cloud 22.2.b
05/04/2022	FortiToken Cloud 22.2.a.
01/18/2022	FortiToken Cloud 21.4.d.
10/11/2021	FortiToken Cloud 21.4.a.
09/30/2021	FortiToken Cloud 21.3.d.
09/16/2021	FortiToken Cloud 21.3.c.
08/13/2021	FortiToken Cloud 21.3.b.
07/26/2021	FortiToken Cloud 21.3.a.
06/09/2021	FortiToken Cloud 21.2.d.
04/15/2021	FortiToken Cloud 21.2.c.
03/01/2021	FortiToken Cloud 21.1.a.
12/02/2020	FortiToken Cloud 20.4.d.
11/30/2020	FortiToken Cloud 20.4.c.
10/07/2020	FortiToken Cloud 20.4.a.
09/01/2020	FortiToken Cloud 20.3.e.
08/05/2020	FortiToken Cloud 20.3.d.
04/24/2020	FortiToken Cloud 20.2.c.
03/25/2020	FortiToken Cloud 20.1.b.
02/12/2020	FortiToken Cloud 20.1.a.
10/25/2019	FortiToken Cloud 4.4.c.
10/02/2019	FortiToken Cloud 4.4.b.
07/02/2019	FortiToken Cloud 4.3.a.

Release Date	Product Version
04/30/2019	FortiToken Cloud 4.2.d.
04/04/2019	FortiToken Cloud 4.2.b.

FÜRTINET®