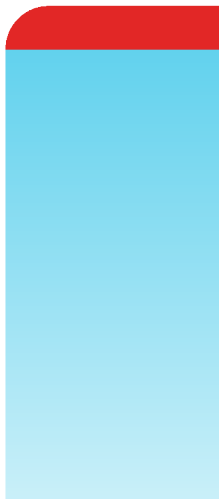


Admin Guide

FortiToken Cloud 22.2.d



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 30, 2022

FortiToken Cloud 22.2.d Admin Guide

TABLE OF CONTENTS

Introduction	9
Main features	9
Compatible Fortinet applications	10
Supported browsers	11
Important notes	11
Credit-based licenses no longer available for purchase	11
Transfer auth clients	11
Use of non-officially supported FOS	12
The same token for the same user on multiple auth clients	12
FOS 6.2.3 and 6.4.0 CLI differences	12
Admin accounts and realms	12
Supported hard tokens	13
No SMS MFA with FAC as LDAP server	13
A single FTC user in multiple auth clients	13
FAC users' name issues on FTC GUI	13
How to use FortiClient	14
Local vs. global disable/delete	14
Product documentation and support	15
Release history	17
22.2.d	17
22.2.c	17
22.2.b	17
22.2.a	17
21.4.d	18
21.4.a	18
21.3.d	18
21.3.c	18
21.3.b	18
21.3.a	18
21.2.d	19
21.2.c	19
21.2.a	19
21.1.a	19
20.4.d	20
20.4.c	20
20.4.a	20
20.3.e	20
20.3.d	20
20.2.c	21
20.1.b	21
20.1.a	21
4.4.c	21
4.4.b	21

4.3.a	22
4.2.d	22
4.2.c	22
4.2.b	22
Licensing	23
Time-based subscriptions	23
Time-based SKUs and their services	23
Stackable co-termed licenses	24
SKUs vs. auth clients and realms supported	24
Transition to time-based subscriptions	25
Replace credit-based license with time-based license	25
Free time-based trial licenses	25
Credit-based subscriptions	26
Credit-based SKUs and their services	27
Credits vs. users supported	27
SMS licensing	28
FortiTrust Identity	28
Licensing options	28
Account disablement and closure	29
Getting started—FGT-FTC users	30
Register your FTC subscription	30
Upgrade FortiOS	31
Log in to the FortiToken Cloud portal	31
Activate FGT VDOMs for FTC service	32
Add an admin user for FTC service	32
Add a local user for FTC service	32
Add remote FortiGate users for FTC service	33
Getting started—FAC-FTC users	35
Register your FTC subscription	35
Upgrade FortiAuthenticator OS	36
Log in to the FortiToken Cloud portal	36
Activate FAC for FTC service	37
Add an admin user for FTC service	37
Add a local user for FTC service	37
FOS CLI commands for FortiToken Cloud	39
Global system configuration	39
Access FTC management commands	39
Configure admin users	40
Configure local users	41
Configure local LDAP users for FTC service	42
Configure wildcard LDAP users for FTC service	42
Configure local RADIUS users for FTC service	43
Migrate FTM tokens to FortiToken Cloud	43
Procedures	44
Verification	44

Diagnose FortiToken Cloud	45
FortiToken Cloud GUI	47
Launch FortiToken Cloud	49
Log in as a regular FTC user	49
Log in as an IAM user	49
FortiCloud	50
The FortiCloud Logo	50
Your FortiCloud account	50
Services	51
Support	52
Dashboard	53
Last 10 authentication attempts in 30 days	54
Administrators	54
Create a sub-admin group	55
Delete a sub-admin group	56
Users	57
Get a new FTM token	58
Auto-assign FTKs to selected users	59
Add user aliases	59
Hide/Show full FortiAuthenticator username	59
View a user's auth clients	59
Edit a user	59
Enable Auto-alias by Email	60
Realms	61
Create a custom realm	61
Edit a realm	62
View realm permission	62
Delete a realm	62
View realm settings	63
FortiProducts	63
Assign an auth client to a realm	64
Edit an auth client	64
Viewing additional information about an auth client	64
Delete an auth client	64
Web Apps	65
Add an auth client	65
Regenerate the API credentials	66
Edit a web app as auth client	66
Delete a web app as auth client	66
Devices (HA)	66
Search for a standalone device	66
Search for a standalone device	67
Validate device ownership	67
Transfer devices	67
Add devices to cluster	69
Remove devices from a cluster	69
Move a device between clusters	69

Mobile Tokens	70
Hardware Tokens	70
Add hard tokens manually	71
Batch-upload hard tokens	72
Assign a hard token to a user	72
Delete hard tokens	72
Usage	73
View usage data	73
View current user count and user quota	74
Licenses	74
Settings	74
Global	75
Realm	77
Templates	82
Adaptive authentication	84
View adaptive authentication policies	85
Create an adaptive authentication policy	86
Edit an adaptive auth policy	87
Delete an adaptive auth policy	87
View adaptive auth profiles	87
Create an adaptive authentication profile	88
Edit an adaptive auth profile	88
Delete an adaptive authentication profile	88
Apply adaptive authentication profiles	88
Logs	89
Authentication	89
Management	91
SMS	93
FortiToken Mobile	94
Supported FortiToken Mobile apps	94
Activate FTM tokens	95
Activate third-party tokens	95
Use FTM tokens	95
FAQs	97
Licenses	97
Credit-based	97
Time-based	97
Free trial	98
SMS	99
FortiTrust Identity	99
General	100
Accounts	103
What should I do if I am not able to access to ftc.fortinet.com ?	103
What should I do if I receive "Unauthorized (Your account cannot be found)" message?	103
If I switch to FortiCloud Premium after enabling FTC trial, will my FTC trial quota be updated to 25?	104

Does an FTC time-based trial account support user quota allocation?	104
Administrators	104
Why a newly created sub-account cannot see FTC end-users from FTC portal but the master account and other sub-accounts can?	104
Settings	105
Global settings	105
Realm settings	105
Realms	105
What is realm? And what does it do?	105
How to add a FortiGate to a ftc.fortinet.com realm?	106
How come my old VPN token stops working after I add a new one?	106
Auth clients	106
FortiProducts	106
Web Apps	107
Users	108
How to create an aliased user?	108
Why can't I add end-users to a new realm when I haven't reached the maximum user quota?	108
Device transfer	108
How do I transfer my FortiGate to a new FortiCloud account and keep using FTC service with the left-over quota?	108
Tokens	110
What does the status of the FortiToken Cloud (FTC) token mean?	110
How to provision FortiToken Cloud?	110
Are FortiToken and FortiToken Cloud the same?	111
If I have 100 users with 100 mobile or hard tokens, can I assign them to 10 FortiGate auth clients?	112
Why can't I issue a new FortiCloud token to a new admin user?	112
Is it possible to use one token on multiple FortiGate HA systems?	112
Can I use the same FortiToken Cloud token for users with different usernames on different FGT serial numbers?	113
FTC LDAP	113
Does FortiGate support FTC AD-wildcard 2FA if cnid=sAMAccountName?	113
How to configure FortiGate for LDAP authentication?	113
How to prevent LDAP users from bypassing 2FA?	114
Can I import wildcard LDAP users directly from the FTC portal if somehow some LDAP users cannot sync over to FTC?	114
FortiOS FTC CLI	115
How does FortiOS support FortiToken Cloud?	115
What is 'fortitoken-cloud show' command for?	127
How to add SMS configuration on FortiGate to activate FortiToken-Cloud 2FA via VPN SSL?	128
What is the 'execute fortitoken-cloud sync' command for?	128
FortiOS Admin	129
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?	129
FortiAuthenticator	129

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?	129
Miscellaneous	130
When trying to access FortiAnalyzer Cloud, it prompts me for a mobile token. Can you help?	130
Technical support	131
Prepare for technical support	131
How to get your Fortinet product serial number	131
Customers on time-based licenses	131
Customers on credit-based licenses	132
Customers with FTM Tokens migrated from FortiGate to FTC	132
Create a technical support ticket	134
Change log	135

Introduction

Thank you for choosing FortiToken Cloud (FTC)!

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

Main features

FortiToken Cloud (FTC) offers the following main features:

- **Multi-factor authentication (MFA) for FGT and FAC devices**—FTC provides a cloud-based MFA solution for all your Fortinet products (such as FortiGate (FGT) and FortiAuthenticator (FAC) and 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-users to bypass MFA and request new tokens on behalf of their end-users easily from the GUI.
- **Automatic lockout of users for excessive MFA failures**—FTC automatically locks out users when they have breached their specified MFA failure threshold, ensuring security and integrity of your account.
- **Secure, cross-platform token transfer**—You can securely transfer your FTC and third-party tokens between iOS and Android devices using the FortiToken Mobile (FTM) app.
- **User synchronization from FGT and/or FAC to FTC**—The admin user can synchronize their end-users from FGT or FAC to FTC from the FGT Console or FAC GUI. The user base of record is always the Auth Client (i.e., FGT or FAC), and trumps the user base that exists in FTC (if different) prior to running the sync command.
- **Support for remote FortiGate users**—You can configure FortiGate wildcard LDAP users to use FTC for MFA.
- **Auth client delete function from FTC**—The admin user is able to delete from the FTC portal auth clients that are no longer in use.
- **Auto log-out**—FTC automatically logs out a user when the GUI has been idle for more than ten minutes, safeguarding the security and integrity of your asset on FTC.
- **Real-time usage statistics**—The administrator can view daily, monthly, and current usage data easily from the GUI.
- **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.
- **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.)
- **FortiCloud SSO**—Integration with FortiCloud provides unified single sign-on (SSO) access to all your Fortinet cloud service offerings.
- **Authentication and Management logs**—FTC provides comprehensive authentication and management logs to keep you informed of all authentication and management events that have happened in your account.
- **Support for FGT HA clusters**—FTC supports FGT and FAC HA cluster configuration. You can view your FGT and/or FAC devices in any cluster from the Auth Clients page.

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

Compatible Fortinet applications

FortiToken Cloud 22.2.d works in tandem with the following Fortinet applications:

- FortiOS 6.2.3 or later, and FortiOS 6.4.0 or later
- FortiClient 6.2.2 or later
- FortiAuthenticator 6.0.1 or later
- FortiSandbox 3.2.0 or later
- FortiADC 6.0 or later
- FortiToken Mobile (FTM) 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 updating 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 22.2.d supports the latest versions of the following web browsers:

- Google Chrome
- Mozilla Firefox



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

Important notes

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

- [Credit-based licenses no longer available for purchase on page 11](#)
- [Transfer auth clients on page 11](#)
- [Use of non-officially supported FOS on page 12](#)
- [The same token for the same user on multiple auth clients on page 12](#)
- [FOS 6.2.3 and 6.4.0 CLI differences on page 12](#)
- [Admin accounts and realms on page 12](#)
- [Supported hard tokens on page 13](#)
- [No SMS MFA with FAC as LDAP server on page 13](#)
- [A single FTC user in multiple auth clients on page 13](#)
- [FAC users' name issues on FTC GUI on page 13](#)
- [How to use FortiClient on page 14](#)

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.

Transfer auth clients

If your existing FortiCloud account (e.g., accountA@gmail.com) doesn't work for some reason, you can transfer your FortiGate devices (auth clients) to another FortiCloud account (e.g., accountB@gmail.com) of yours to be able to continue using your FTC service. If your FortiGate devices are running FOS version 6.4.1 or later, or FOS version 7.0.0 or later, you can transfer your FortiGates using the FortiOS administrator portal. If your FortiGate devices are running FOS version 6.4.0 or earlier, please contact FortiCare Technical Support fortinet.com/support/contact to request FGT account transfer via 'Live Chat' or over the phone. You must have your FortiGate device serial number(s) ready to complete the transfer process. The following steps show how to transfer your FortiGate devices using the FortiGate Administrator Portal. Below are the easy steps that you must to follow to smoothly transfer your auth clients.

1. Log in to the FOS Administrator Portal.
2. Select the global VDOM (if multi-vdom is enabled) > System > FortiGuard.
3. Under "License Information", click the "Action" button of FortiCare.
4. Select "Transfer FortiGate to Another Account".
5. On the FTC portal, click Auth Clients>FortiProducts to open the FortiProducts page, select all auth clients associated with the FGT SN registered under account, and click the 'Delete' button.
Note: If you are unable to access your old FortiCloud account any more, contact [FortiCare Technical Support](#) for assistance.
6. After your account transfer has been confirmed, execute `'exe fortitoken-cloud update'` to update the auth clients to the new account on the FGT CLI.
7. On FortiGate CLI, execute `'exe fortitoken-cloud sync'` to update the FTC users to the new account.
Note: If customer hits new-created on FGT doesn't sync over to FTC portal from Auth Client > Count is 0, customer needs to associate auth client to a realm manually on FTC portal from 'Auth Client > Edit Auth Client > select realm then apply

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.

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

FOS 6.2.3 and 6.4.0 CLI differences

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

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

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

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

Admin accounts and realms

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

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

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

Supported hard tokens

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

No SMS MFA with FAC as LDAP server

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

A single FTC user in multiple auth clients

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

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

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

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



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

FAC users' name issues on FTC GUI

Names of FTC users created on FortiAuthenticator (FAC) show up with prefixed and suffixed characters in corner brackets, on the FTC GUI and in email notifications. This is due to the fact that FAC differentiates the same username

populated by multiple user sources to FAC. 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.

Use auto push

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

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



You must make sure that “Notification” is enabled on the FortiToken Mobile app on the mobile device. You must also ensure that “push” is enabled (Enable push) on the Realm FTM Setting on the FortiToken Cloud Portal.

Use OTP

Upon entering your username and password, do the following:

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

Local vs. global disable/delete

FOS distinguishes between local and global disable/delete operations for FTC-enabled FGT users.

While a local delete operation removes the user from an FGT VDOM without affecting the user in FTC, a global delete operation removes the user in both FGT and FTC.

When you disable an FTC-enabled user locally in an FGT VDOM, the user remains unchanged in FTC; when you disable an FTC-enabled user globally in FGT, you remove the user from FTC.

The table below highlights the differences between local and global disable/delete operations.


FortiGate Operation	Disable	Enable	Delete Locally	Delete Global
User in FortiGate	Enabled->Disabled	Disabled->Enabled	Deleted	Deleted
User in FTC	Unchanged	Unchanged	Unchanged	Deleted



Since a local delete-user operation in FGT removes a user only from a specific FGT VDOM but leaves it intact in FTC, FOS warns the VDOM admin that the local delete operation does not remove the user in FTC and, therefore, usage will still be counted as long as the user remains in FTC.

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 product support issues, click [FortiToken Cloud Support](#) ().

Acronyms and abbreviations

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

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

Acronym/Abbreviation	Terminology
TOTP	Time-based one-time password
UTC	Universal Time Coordinated (or Coordinated Universal Time)

Release history

This section highlights the major feature changes or updates in each of the releases of FortiToken Cloud since its GA release. For a complete list of product features, see [Main features on page 9](#).

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 a "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 70](#).
- **Global administrator and sub-admins**—FTC now enables the global administrator to create sub-admins and allocate resources to them. See [Administrators on page 54](#).
- **Multi-realm support**—FTC now allows the global admin to create realms. See [Realms on page 61](#).
- **More MFA methods**—This release adds support for e-mail, SMS, and FTK (FortiToken, which is a hardware token) as options for MFA. See [Settings on page 74](#).

4.4.c

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

4.4.b

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

4.3.a

- **Custom logo**—Enables admin users to upload custom logo images to replace the default Fortinet logo at the bottom of the FTM app screen on end-users' devices. See [Settings on page 74](#) for more information.
- **FTM token activation/transfer notification by SMS**—Enables admin users to let end-users receive FTM token activation or transfer notifications by SMS. See [Settings on page 74](#) for more information.
- **Access to all accounts by admin users**—FTC admin users are able to access all FTC accounts belonging to their own organization. They can choose which of their accounts to open upon login, and switch to any of their other accounts during a session.

4.2.d

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

4.2.c

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

4.2.b

FortiToken Cloud 4.2.b is the FortiToken Cloud GA release, which offers many of the major features of the product. For more information, see [Main features on page 9](#).

Licensing

FortiToken Cloud (FTC) started with a credit-based annual subscription model that has been serving our early customers over the years. To provide better user and sales experience for our customers, we have started with our v.21.2.d release the transition to a time-based annual subscription model which will eventually replace the credit-based subscription model.

While we will continue to support our existing customers of the legacy credit-based subscriptions during the transition period, new customers must purchase the new time-based subscriptions to use our service.

Also, customers of credit-based subscriptions must renew their service with time-based subscriptions when their credit-based subscriptions have expired or when they have used up all the credits in their account. For more information, see

- [Time-based subscriptions on page 23](#)
- [Credit-based subscriptions on page 26](#)
- [SMS licensing on page 28](#)
- [FortiTrust Identity on page 28](#)
- [Account disablement and closure on page 29](#)

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 23](#) 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	One-year subscription for up to 25 users, including 2,500 SMS messages and 24x7 FortiCare Support.
FC2-10-TKCLD-445-01-DD	One-year subscription for up to 100 users, including 10,000 SMS messages and 24x7 FortiCare Support.
FC3-10-TKCLD-445-01-DD	One-year subscription for up to 500 users, including 50,000 SMS messages and 24x7 FortiCare Support.
FC4-10-TKCLD-445-01-DD	One-year subscription for up to 2,000 users, including 200,000 SMS messages

SKU	Number of FTC end-users supported
	and 24x7 FortiCare Support.
FC5-10-TKCLD-445-01-DD	One-year subscription for up to 10,000 users, including 1,000,000 SMS messages and 24x7 FortiCare Support.

Stackable co-termed licenses

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 your existing time-based license by requesting a co-termed license. For example, on December 1, 2021, you want to add a 25-user license and you want it to expire on the same date as your 500-user license does. In this case, the new co-termed 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.

In the first case, the new license is independent of the original license and you can purchase it the its SKU. In the second case, you will have to reach out to our license renewal team (renewals@fortinet.com) for assistance.

For more information, see [Time-based SKUs and their services on page 23](#) and [SKUs vs. auth clients and realms supported on page 24](#) in the Admin Guide.

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 [Usage on page 73](#).

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.

Replace credit-based license with time-based license

Once you have transitioned to a time-based license, you are no longer able to register or activate any credit-based license that you've purchased. In that case, you can contact FortiCare to replace the credit-based license with an equivalent time-based license.

Free time-based trial licenses

To help customers make informed purchasing decisions, we offer 30-day free trial licenses to all FortiCloud customers to test-drive our new time-based FortiToken Cloud MFA service. For FortiCloud premium customers, the trial license can support up to of 25 FTC end-users; for FortiCloud non-premium customers, the limit is 5 FTC end-users per trial license.

Please note that free trial licenses do NOT include SMS messages.

Enable FTC trial service on FTC GUI

Log on to the FortiToken GUI (<https://ftc.fortinet.com>) with your FortiCloud username and password with which the auth device is registered. The FTC trial service is enabled automatically after you have logged in for the first time. This method applies to all FTC-supported auth devices.

Enable FTC trial service on FortiGate

In addition to the enabling the trial service from the FTC GUI, you can also enable it from FGT using the following CLI command:

```
execute fortitoken-cloud trial
```

The FTC trial service is enabled after this CLI is executed successfully.



This CLI command is not supported in FOS versions 7.0.2 and 7.0.3.

Once the FTC trial service has been enabled, you can add users on FortiGate for FTC MFA service.

If, after the free trial, you decide to continue using FTC. You can purchase a license, and register it to your account. For more information, see [Register your FTC subscription on page 30](#).

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 the credit-based subscriptions, and replacing them with the new 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 23](#).

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 73](#).



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 will expire on the same day that your license expires and can no longer be used. 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 ($=30 \times 1/30$) 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 ($=(1 \times 1/30) \times 30$).



- 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 25](#).
- 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 25](#).

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.

Credit-based SKUs and their services

The following table highlights the maximum number of end-users, the maximum number of auth clients, and the maximum number of realms that each credit-based SKU supports.

SKU	Number of credits	Number of end-users	Max. number of auth clients	Max. number of realms
FTC-LIC-120	120	120	12	12
FTC-LIC-1200	1,200	1,200	120	120
FTC-LIC-12K	12,000	12,000	1,200	1,200
FTC-LIC-120K	120,000	120,000	12,000	12,000

Credits vs. users supported

FortiToken Cloud (FTC) offers SKUs for 120, 1,200, 12,000 and 120,000 credits. See [Credit-based SKUs and their services on page 27](#). FTC works in tandem with FC to enforce your maximum user limit. When you try to add more users

than the SKU limit, FTC first checks with FC to see if you have enough credits in your account to support the additional users. If you don't, FTC will prompt you to purchase more credits.

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

The following table highlights the correlation between your account credit balance and the maximum number of FTC end-users that your account can support.

Current credit balance	Maxim number of end-users supported
0–120	120
121–1,200	1,200
1,201–12,000	12,000
12,001–120,000	120,000
>120,000	1,200,000

SMS licensing

Starting with 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 10.

Each time-based license (SKU) allows for 125 SMS credits for each end-user annually. The FTC Dashboard page displays your SMS credit balance.

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](#).

FortiTrust Identity

Starting with its 22.1.a release, FTC supports IDENTITY user bands license which is part of 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](#).

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.

Getting started—FGT-FTC users



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

FTC supports up to four MFA methods, namely FTM, FTK, SMS, and email. The MFA method is set on a per-realm basis. The default method is FTM, but the admin user can change it to another method if needed. Sub-admins can then further change the MFA methods for end-users in their assigned realms to something other than the default (i.e., FTM). The [Users on page 57](#) page shows the MFA methods used by individual end-users.

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

1. [Register your FTC subscription on page 30.](#)
2. [Upgrade FortiOS on page 31.](#)
3. [Log in to the FortiToken Cloud portal on page 31.](#)
4. [Activate FGT VDOMs for FTC service on page 32.](#)
5. [Add a local user for FTC service on page 32.](#)
6. [Add an admin user for FTC service on page 32.](#)

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



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

To activate FGT VDOMs for FTC service:

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



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

Add an admin user for FTC service

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

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

For more information, see [Configure admin users on page 40](#).

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 [Configure local users on page 41](#).

Add remote FortiGate users for FTC service

You 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 42](#) 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 35.](#)
2. [Upgrade FortiAuthenticator OS on page 36.](#)
3. [Log in to the FortiToken Cloud portal on page 36.](#)
4. [Activate FAC for FTC service on page 37.](#)
5. [Add an admin user for FTC service on page 37.](#)
6. [Add a local user for FTC service on page 37.](#)

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



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

Add a local user for FTC service

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

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

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

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

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



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

FOS CLI commands for FortiToken Cloud

This section discusses the FOS (version 6.2.3 and later, and version 6.4.0 and later) CLI commands supported in the FTC 22.2.d release.

- [Global system configuration on page 39](#)
- [Access FTC management commands on page 39](#)
- [Configure admin users on page 40](#)
- [Configure local users on page 41](#)
- [Configure local LDAP users for FTC service on page 42](#)
- [Configure wildcard LDAP users for FTC service on page 42](#)
- [Configure local RADIUS users for FTC service on page 43](#)
- [Diagnose FortiToken Cloud on page 45](#)

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[REDACTED]"
    set hostname "FG[REDACTED]"
    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[REDACTED] # 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 [REDACTED] # execute fortitoken-cloud new ?
<user name>   User name for new token.

```

```

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

```

```

FG [REDACTED] # execute fortitoken-cloud trial ?
<Enter>

```

```

FG [REDACTED] # 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
<code>config system admin</code>	Starts the configuration of a system admin user.
<code>edit <username></code>	Specify the admin username.
<code>set accprofile</code>	Specify the admin account profile name. For example, <code>super_admin</code> .
<code>set vdom</code>	Specify the VDOM name. For example, <code>root</code> .

Command	Description
<code>set two-factor</code>	Select an MFA method: <ul style="list-style-type: none"> <code>disable</code>—No MFA. <code>fortitoken</code>—FortiToken (FTK) or FortiToken Mobile (FTM). <code>email</code>—Email. <code>sms</code>—Simple message service. This option requires an SMS server and SMS phones. <code>fortitoken-cloud</code>—FortiToken Cloud. Note: FortiToken Cloud is the default MFA method.
<code>set email-to</code>	Specify the email address to which FTC sends MFA activation codes.
<code>set sms-phone</code>	Specify the mobile phone number for receiving SMS messages.
<code>set password</code>	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 EKhtmlTBulhmHUokESNTkNjxV8mBQ+AgyRPlInw==
  next
end
```

Command	Description
<code>config user local</code>	Starts the configuration of a local user.
<code>edit <username></code>	Create the username.
<code>set type password</code>	Set type to password (authentication).
<code>set two-factor</code>	Select the MFA method: <ul style="list-style-type: none"> <code>disable</code>—No MFA. <code>fortitoken</code>—FortiToken (FTK) or FortiToken Mobile (FTM). <code>email</code>—Email. <code>sms</code>—Simple message service. Note: This option requires an SMS server and SMS phones. <code>fortitoken-cloud</code>—FortiToken Cloud. Note: FTC is the default MFA method.
<code>set email-to <email address></code>	Specify the email address to which the authentication code is sent.

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

Configure local LDAP users for FTC service

You 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 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 EKhm1TBulhmHUokESNTkNjxV8mBQ+AgyRPlInw==
  next
end
```

Configure wildcard LDAP users for FTC service

You 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=src,dc=world"
    set type regular
    set two-factor fortitoken-cloud
    set username "cn=Manager,dc=src,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

You 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 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>
```



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 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 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).
- 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.

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

Examples

```
FG [REDACTED] (global) # diag fortitoken-cloud debug {enable | disable}
FG [REDACTED] (global) # diag fortitoken-cloud server
FG [REDACTED] (global) # diag fortitoken-cloud show {server | realm | users | user
<username> <VDOM>}
FG [REDACTED] (global) # diag fortitoken-cloud delete <username>
FG [REDACTED] (global) # diag fortitoken-cloud set-http <number>
FG [REDACTED] (global) # diag fortitoken-cloud clear <Enter>
FG [REDACTED] (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 [REDACTED] (global) # diagnose fortitoken-cloud migrate-ftm
<string>      Enter command: show, start, abort, add-users, delete-users, ftm2ftc.
```

```
FGVM [REDACTED] (global) # diagnose fortitoken-cloud migrate-ftm show  
<string> FTM license number.
```

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

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

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

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

```
FGVM [REDACTED] (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.

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	<p>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 53.</p> <p>If you are using a credit-based license, you'll see:</p> <ul style="list-style-type: none"> • <i>Current Month Usage</i> — The number of credits that has been used for the current month. • <i>Current Balance</i> — The current credit balance (number of credits remaining). • <i>FortiProducts</i> — The number of Fortinet products as auth clients. • <i>Web Apps</i> — The number of Web apps as auth clients. • <i>Users</i> — The number of FTC end-users. • <i>Realms</i> — The number of realms. • <i>Last 10 authentication attempts in 30 days</i> <p>If you are using a time-based license, you'll see:</p> <ul style="list-style-type: none"> • <i>FortiProducts</i> — The number of FortiProducts as auth clients in your account. • <i>Web Apps/Max Webb Apps</i> — The current number of Web apps as auth clients in your account and the maximum number of Web apps that your license can support. • <i>Users/Max Users</i> — The current number of users in your account and the maximum number of users that your license can support. • <i>Realms/Max Realms</i> — The current number of realms in your account vs. the maximum number of realms that your license can support, • <i>Remaining SMS</i> — The number of SMS messages available for use. • <i>Expiration Date</i> — The date when your current license expires. • <i>Last 10 authentication attempts in 30 days</i>
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 54 .
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

Menu	Description
	Realms on page 61.
Users	Shows information of all your FTC end-users. For more information, see Users on page 57 .
Auth Clients	Shows information about all your authentication clients which include the following types: <ul style="list-style-type: none"> • FortiProducts • Web Apps on page 65 • Devices (HA)
Tokens	Shows the tokens in two groups: <ul style="list-style-type: none"> • <i>Mobile</i>—Shows mobile tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See Mobile Tokens on page 70. • <i>Hardware</i>—Shows hardware tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See Hardware Tokens on page 70.
Usage	Shows usage data of your account. See Usage on page 73 .
Licenses	Shows all the licenses in your account. See Licenses on page 74 . 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 <i>Settings</i> menu which has the following options: <ul style="list-style-type: none"> • <i>Global</i>—Allows the global administrator to enable or disable some settings at the system level. See Share-quota mode on page 76. • <i>Realm</i>—Enables both the global admin and sub-admins to view and manage the settings of the selected realm. See Settings on page 74. • <i>Templates</i>—Opens the Templates page where you can add or delete templates. See Templates on page 82.
Adaptive Auth	Opens the <i>Adaptive Auth</i> menu which has the following options: <ul style="list-style-type: none"> • <i>Policy</i>—Creates and manage adaptive auth policies. • <i>Profile</i>—Creates and manager adaptive auth profiles. See Adaptive authentication on page 84 .
Logs	Shows the <i>Logs</i> menu which has the following options: <ul style="list-style-type: none"> • Authentication on page 89 • Management on page 91 • SMS See Logs on page 89 .
Help	Opens the <i>Help</i> menu which has the following options: <ul style="list-style-type: none"> • Contact Support • Purchasing Guide • Online Help • FAQs

Menu	Description
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 <i>Account</i> below.
Auth Clients	Shows the number of auth clients in your realm or account. See the note for <i>Account</i> below.
Account	<p>Shows your account number and the name of your company.</p> <p>Note:</p> <ul style="list-style-type: none"> • 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*.

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*.

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: <ul style="list-style-type: none">• <i>Account Profile</i>—View and edit your account profile.• <i>Change Account ID (Email)</i>—Change your account ID.• <i>Manage User</i>—Add users to your account.• <i>My Account (IAM version)</i>

Menu	Description
User Information (Applicable to IAM users only)	Opens the User Information page with the following tools: <ul style="list-style-type: none"> <i>User Profile</i>—View and edit your user profile. <i>Change Email</i>—Change your email address. <i>Permissions</i>—Manage IAM permissions.
Security Credentials	Opens the FortiCloud page with the following tools: <ul style="list-style-type: none"> <i>Change Password</i>—Change/update your account password. <i>2FA Settings</i>—Manage your account's two-factor authentication settings. <i>Subscriptions</i>—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 <i>IAM</i> 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 <i>FortiCloud > Asset Management</i> page, where you can <ul style="list-style-type: none"> 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

Menu	Description
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.
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. <ul style="list-style-type: none"> • <i>Firmware Download</i> • <i>VM Images</i> • <i>Service Updates</i> • <i>HQIP Images</i> • <i>Firmware Image Checksum</i>
Resources	Click this tab to open the <i>FortiCloud > Resources</i> page, where enables you to access a slew of resources to Fortinet products and services.

Menu	Description
FortiCare	<p>Click one of the following links for the support service you need:</p> <ul style="list-style-type: none"> • <i>Create a Ticket</i> • <i>Manage Active Tickets</i> • <i>Manage Tickets</i> • <i>Ticket Survey</i> • <i>Contact Support</i> • <i>Technical Web Chat</i>

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 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*

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 Web 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,
- *Remaining SMS* — The number of SMS messages available for use.
- *Expiration Date* — The date when your current license expires.
- *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 an authentication request, which can be either of the following: <ul style="list-style-type: none"> • <i>Success</i> • <i>Failed</i>
Message	A system-generated message about the authentication request.



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

Administrators

Only admin users can access the FortiToken Cloud (FTC) portal. There are two types of administrator accounts: the global administrator (global_admin) and sub-administrators (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 a group. (Optional)
Level	<p>The level of administration of a group:</p> <ul style="list-style-type: none"> <i>global_admin</i>—The highest level of administration. Note: The <i>global_admin</i> group is the default admin account, and cannot be deleted. <i>sub_admin</i>—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	<p>The number of sub-admins in a group.</p> <p>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.</p>
Tool bar	<p>The tool bar slides in from the right end of the row when you mouse over an entry in the table. It shows the following tools:</p> <ul style="list-style-type: none"> <i>Edit</i>—Edits the administrator group. <i>Delete</i>—Deletes the administrator group.

Create a sub-admin group

To create a sub-admin group:

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

Add users to a group



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

To add sub-admins to an admin group:

- In the *Add Admin Group* table, click the name of the group of interest to open the *Edit Admin Group* dialog.
- 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 a 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.



- You must have realms created first before assigning them to a sub-admin group. See [Realms on page 61](#).
 - 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 55](#).
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 a group on page 56](#).
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 to delete the group. See [Edit sub-admin group configuration on page 56](#).

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 <i>NEW FTM TOKEN</i> button to request a new FTM token for the user. See Get a new token .
Username	The username of an FTC end-user.
Status	<p>The status of a user, which can be a combination of any of the following:</p> <ul style="list-style-type: none">  (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. An admin user can also click this button to re-enable a disabled user.  (locked)—The user is locked out. Note: FTC locks a user out when he or she has exceeded the specified maximum number of log-in attempts allowed. See Settings on page 74.  (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.  (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 <i>Enable Bypass</i> is enabled on the <i>Settings</i> page. See Settings on page 74. Otherwise, when you click the  (no bypass) icon, a tool tip will appear asking you to turn on <i>Enable Bypass</i> on the <i>Settings</i> page.

Column	Description
MFA Method	The user's MFA method, which can be one of the following: <ul style="list-style-type: none"> • <i>FTM</i> (soft token) • <i>Email</i> • <i>SMS</i> • <i>FTK</i> (FortiToken, a hardware token)
Token SN	The serial number of a token. Note: A serial number that starts with "FTC" indicates that it is a FortiToken Cloud token; 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: <ul style="list-style-type: none"> • <i>Email</i>—FTC sends FTM token activation/transfer notifications to the user's email address. • <i>SMS</i>—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 Settings on page 74 .
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 "+ <u>Country Code Area Code Phone Number</u> ", e.g., +1 4082221234. An admin user can edit an end-user's mobile phone numbers.
Auth Client Count	The number of auth clients.
Create Date	The date on which the user 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 an <i>Edit</i> tool button that enables you to make changes to the user's settings.

Get a new FTM token



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

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

Auto-assign FTKs to selected users



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

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

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 bold font on the *Users* page.

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

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.

Edit a user

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

Field	Description
Auth Method	Click the down arrow, and select a desired authentication method from the drop-down menu: <ul style="list-style-type: none"> • <i>FTM</i> • <i>Email</i> • <i>SMS</i> (Note: This option requires a valid mobile phone number.) • <i>FTK</i>
Notification Method	Note: This field applies only when you set <i>Auth Method</i> to <i>FTM</i> . See above.
Token SN	<i>This field is read only, and cannot be edited.</i>
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 <i>Auth Method</i> and/or <i>Notification Method</i> is set to <i>SMS</i> , as stated above.

Changes that you've made here become effective when you click *Apply*. A 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.

Enable Auto-alias by Email

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

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

FTC now allows for different usernames to be attributed to the same user (i.e., same person) so that only one token (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.

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 aliases under the same username.

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.

Realms

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 <i>Delete</i> 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 <i>Delete</i> icon in the Actions column. For more information, see Delete a realm on page 62 .
Name	The name of a realm.
Description	A brief description about the realm that the global admin added when creating the realm.
Client Count	The number of auth clients assigned to a realm.
Tool bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It has the following tools: <ul style="list-style-type: none"> • <i>Edit Realm</i>—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. • <i>Show Permission</i>—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. • <i>Settings</i>—Opens the Settings page which shows the settings of the realm. See Settings on page 74. • <i>Delete</i>—Deletes the realm. See Delete a realm on page 62.

Create a custom realm

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

4. Click *OK*.
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 *Actions* column, click the *Show Permission* button to open the *Access list for realm* dialog.
3. Identify the sub-admin group of interest, and click the corresponding **x** (*Delete*) icon.

Delete a realm

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 <i>DELETE</i> button is enabled. You can then click the <i>DELETE</i> button to remove the selected auth client. For more information, see Delete an auth client on page 64 . Note: You can select all the auth clients at once by checking the checkbox in the column header.
Alias	The alias of the users on an auth client.
Name	The name of an auth client.
Type	The type of auth client, which can be any of the following: <ul style="list-style-type: none"> • <i>FortiAuthenticator</i> • <i>FortiGate</i> • <i>FortiGateVM</i> • <i>FortiSandbox</i> Note: FTC assigns auth client type based on the serial number and model of the product.
Count	The number of FTC end-users on an auth client. Note: Clicking the numeric value opens a dialog which shows the list of FTC end-users on an auth client, along with some basic user information.
Realm Name	The name of the realm to which an auth client is assigned.
Tool Bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It provides the following tools: <ul style="list-style-type: none"> • <i>Edit</i>—Change certain settings of the auth client. • <i>Details</i>—Shows some detailed information of the auth client. • <i>Delete</i>—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 61](#).

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 Yes.
The name of the newly selected realm now appears in that column, meaning that the auth client now is assigned to this realm.

Edit an auth client

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 some more information about the auth client.

Delete an auth client



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

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.

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: Clicking the button regenerates the secret for the auth client.
Last Update	The time when the auth client was last updated.
Tool Bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It provides the following tools: <ul style="list-style-type: none">• <i>Edit</i>—Edits the settings of a web app as auth client• <i>Delete</i>—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* button.
3. In the *Regenerate Secret* dialog, select either of the following:
 - *Display on portal*—Shows the secret on the GUI.
 - *Send to email*—Sends the secret to the email address 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 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 *Delete*.
3. In the confirmation dialog, click *Yes*.

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.

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.

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

Starting 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 Fortinet products

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](https://www.fortinet.com/support/contact) 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.
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, “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, you can transfer the device back to the original account using the instructions in [Transfer devices from Fortinet products on page 68](#). You can also contact FortiCare for assistance, if needed.

Add devices to cluster

You can add any device in the *Standalone Devices* panel to any cluster in the *Clusters* panel. Once a standalone device is added to a cluster, it becomes part of the cluster and will 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 [Search for a standalone device on page 66](#).
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. Be sure to read the message, and click *OK*.

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 realm.
Platform	The mobile platform of an FTM, which can be either of the following: <ul style="list-style-type: none">• <i>Android</i>• <i>iOS</i>
Algorithm	The algorithm of time-based one-time password authentication used on the token: <ul style="list-style-type: none">• <i>TOTP</i>
Registration ID	The ID under which the FTM is registered.

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 <i>Delete</i> button enabled. You can then click the button to delete that hard token. For more information, see Delete hard tokens on page 72 .

Column	Description
	Note: You can also check the checkbox in the column header to select all the hard tokens and delete them all at once.
Serial Number	The serial number of a FortiToken.
Model	The models of supported hard tokens, which can be one of the following: <ul style="list-style-type: none"> • <i>FTK200</i> • <i>FTK220</i> • <i>Other</i>
Algorithm	The algorithm of time-based one-time password authentication used on the hard token. <ul style="list-style-type: none"> • <i>TOTP (default)</i>
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 [Batch-upload hard tokens on page 72](#).



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

Add hard tokens manually



If FTK is set as the default MFA method in the settings of a realm, you can select users on the *Users* page and let FTC automatically assign FTKs to them by clicking the *Auto-assign FTK* button. See [Users on page 57](#).

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 Tokens* button.
The *Import Hard Tokens* dialog opens.
2. In the upper-right corner of the dialog, click the *Upload CSV file* button.
The typical Windows *File Upload* dialog opens.
3. Locate the .csv file in your file system, and click *Open*.
The *Windows Upload File* dialog closes, and all the serial numbers of the hard tokens in the .csv file are now added to the *Import Hard Tokens* dialog.
4. Click *OK*.
The *Import Hard Token* dialog closes, and a message pops up in the upper-right corner of the *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 hardware 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 [Users on page 57](#).
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 hardware tokens:

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

To delete all hardware tokens:


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

Usage

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

View usage data



The usage graph shows the number of 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 versa.

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 23](#).

The *Licenses* page shows all valid time-based licenses in your account. The table below describes the information about the licenses listed 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	The maximum number of SMS messages that the license can support.
Remaining SMS	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.

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 [Share-quota mode 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 77](#).
- *Templates*—Provides tools for managing message templates. For more information, see [Templates on page 82](#).



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

Global



This feature is accessible to global admin users only.

The *Settings>Global* menu enables the global admin to make system-wide changes that affect all realms in their account. It has the following options:

- [Multi-realm mode on page 75](#)
- [Auto-create Auth Client on page 76](#)
- [Share-quota mode on page 76](#)
- [Username case & accent sensitive on page 76](#)
- [Account Disable/Delete Notification on page 77](#)

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.

By design, *Multi-realm Mode* is enabled for new FTC customers, but disabled for customers who started their FTC service before the FOS 6.2.3 release. When *Multi-realm Mode* is disabled, new auth clients 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.

While there is no need for new customers to enable *Multi-realm Mode*, existing customers must enable it to take advantage of its benefits. When *Multi-realm Mode* is enabled, you can create custom realms and assign auth clients to them. You must assign an auth client to a custom realm to add users to and sync users from it. Otherwise, it will be assigned to the default realm where you cannot assign users to or sync users from it.



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

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*.

Disable Multi-realm Mode

While *Multi-realm Mode* is enabled, you can click the *Multi-realm Mode* button to disable it. For more information on realms, see [Realms on page 61](#).

Auto-create Auth Client



This feature applies to FortiGate/FortiOS VDOMs only.

Normally, the FortiGate administrator can add a VDOM to FTC as an auth client by enabling the first user on the VDOM for FTC (if the VDOM has not already been assigned to a realm). So when FTC receives a VDOM list from FortiOS with a new VDOM with a user enabled for FTC service, it automatically adds that VDOM as an auth client. This may inadvertently allow unintended auth clients to consume your FTC quotas or credits. To prevent this from happening, FTC has introduced the *Auto-create Auth Client* option to make the "add-auth-client-on-creation-of-first-user" feature optional in its global settings.

Disable Auto-create Auth Client

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

1. On the 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*.

Enable Auto-create Auth Client

If *Auto-create Auth Client* is disabled, you can enable it by clicking the *Auto-create Auth Client* button.

Share-quota mode



The *Share-quota Mode* option applies to paid time-based subscriptions only; it is not available to credit-based subscriptions or time-based trial accounts.

When *Share-quota Mode* is enabled (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.

Username case & accent sensitive

By default, the *Username Case & Accent Sensitive* option is enabled in both FortiOS and FTC, but you can disable it in FGT and FTC, respectively. To use this feature, you must ensure that they are set in the same way in both FortiOS and FTC, whether they are "enabled" or "disabled". If they are different, the setting in the FortiOS overrides the one in FTC.

When *Username Case & Accent Sensitive* is disabled, FTC ignores case and accent variations in usernames when processing login requests; when enabled, FTC checks the case and accent conformity in a username and approves the login request only when it matches exactly what is in the database.



This feature only applies to individually imported LDAP users with `set username-case-sensitivity enable/disable`; it does not apply to wildcard LDAP users.

Account Disable/Delete Notification

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

By default, *Account Disable/Delete Notification* is turned on, but you can disable it by turning the button off.

Realm

Realm

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

- [General Setting on page 77](#)
- [FTM Setting on page 79](#)
- [Email MFA Setting on page 81](#)
- [SMS MFA Setting on page 81](#)

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 Setting

Parameter	Default value
MFA Method	<p>Select the method that FTC uses to further authenticate your end-users upon receiving their login credentials (i.e., username and password).</p> <ul style="list-style-type: none"> • <i>FTM</i> (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. • <i>SMS</i>—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

Parameter	Default value
	<p>page to gain access to the auth client.</p> <p>Note: To use this option, FTC must have the end-users' valid smart phone numbers in its database.</p> <ul style="list-style-type: none"> <i>Email</i>—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). <i>FTK</i>—FTC requires end-users to provide the OTP generated by their FortiToken (hardware token) for MFA. <p>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 70. 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 <i>Auto-assign FTK</i> button on the <i>Users</i> page. See Users on page 57.</p>
Max Login Attempts Before Lockout	<p>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.</p> <p>Note: FTC does not allow locked users to authenticate. Instead, it displays the message "Locked, please try again in <lockout interval> minutes."</p>
Lockout Period	<p>Click above the horizontal line and specify a lockout period, which ranges from 60 to 7,200 seconds. The default is 60 seconds.</p>
Enable Bypass	<p>Enable or disable bypass.</p> <ul style="list-style-type: none"> <i>Enable</i>—End-users can bypass MFA. If enabled, you must also set the <i>Bypass Expiration Time</i>, as described below. <i>Disable</i> (default)—End-users cannot bypass MFA. <p>Note: If <i>Enable Bypass</i> is disabled on the <i>Settings</i> page, the admin user can not enable bypass for FTC end-users on the <i>Users</i> page. See Users on page 57.</p>
Bypass Expiration Time	<p>(Available only when <i>Enable Bypass</i> 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).</p>
Auto-alias by Email	<p>Enable or disable the <i>Auto-alias by Email</i> feature.</p> <p>Note: The feature is disabled by default. For more information, see Enable Auto-alias by Email on page 78.</p>
Adaptive Auth Profile	<p>Select an adaptive auth profile.</p>

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	<p>From the drop-down menu, select either of the following:</p> <ul style="list-style-type: none"> • <i>Email</i>—Token activation/transfer codes are sent to users' email addresses. • <i>SMS</i>—Token activation/transfer codes are sent by SMS to users' mobile phone numbers. <p>Note: When <i>Notification Method</i> is set to <i>SMS</i>, 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 <i>Users</i> page. See Users on page 57.</p> <p>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.</p>
App PIN Required	<p>Click the button to enable or disable this feature.</p> <ul style="list-style-type: none"> • <i>Disabled</i> (default)—No app PIN is required. • <i>Enable</i>—If enabled, you must select a PIN Length and PIN Required Mode, as described below.
PIN Length	<p>Click the down arrow and, from the drop-down menu, select one of the following:</p> <ul style="list-style-type: none"> • 4 • 6 (default) • 8 <p>Note: PIN length refers to the number of digits contained in an app PIN.</p>
PIN Required Type	<p>Click the down arrow and, from the drop-down menu, select either of the following:</p> <ul style="list-style-type: none"> • <i>Anytime</i>—App PIN is required all the time.

Parameter	Default value
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> TOTP (default). No action is needed.
OTP Time Step	<p>Click the down arrow and, from the drop-down menu, select either of the following:</p> <ul style="list-style-type: none"> 30 (default) 60 <p>Note: <i>OTP Time Step</i> 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.</p>
OTP Validation Window	<p>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.</p>
OTP Display Length	<p>Click the down arrow and, from the drop-down menu, select either of the following:</p> <ul style="list-style-type: none"> 6 (default) 8 <p>Note: OTP Display Length refers to the number of digits contained in a token activation/transfer code.</p>
Activation Expiration Time	<p>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.</p> <p>Note: An FTM Token code must be activated within the set <i>Activation Expiration Time</i>. Otherwise, it will expire and you must request a new token.</p>
FTM Logo	<p>This enables admin users to choose logo image displayed at the bottom of the FTM app screen on their end-users' mobile devices.</p> <ul style="list-style-type: none"> 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 81. 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.



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*.

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 on page 85](#)
- [Create an adaptive authentication policy on page 86](#)
- [Edit an adaptive auth policy on page 87](#)
- [Delete an adaptive auth policy on page 87](#)
- [View adaptive auth profiles on page 87](#)
- [Create an adaptive authentication profile on page 88](#)
- [Edit an adaptive auth profile on page 88](#)
- [Delete an adaptive authentication profile on page 88](#)
- [Apply adaptive authentication profiles on page 88](#)

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	<p>The action specified in the policy, which can be one of the following:</p> <ul style="list-style-type: none">• <i>Multi-factor Authentication</i> (default)• <i>Block</i>• <i>Bypass</i> <p>Note: The FTC server takes the specified action when an authentication request matches the policy.</p>

Parameter	Description
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	<p>Select one of the following:</p> <ul style="list-style-type: none"> • <i>Enforce MFA</i> — By default, the FTC server will require login attempts from the specified source to use MFA. • <i>Block</i> — The FTC server will block login attempts from the specified source. • <i>Bypass MFA</i> — The FTC server will let the login attempts from the specified source bypass the MFA requirement. <p>Note: The FTC server takes the specified action when an authentication request matches the policy settings.</p>
Filters	<p>Select the filter</p> <ul style="list-style-type: none"> • <i>Subnet Filter</i> — See <i>Subnet Filter</i> below. • <i>Location Filter</i> — See <i>Location Filter</i> below. • <i>No Source Filter</i> — Select this option if you do not want to use any filter. • <i>Schedule</i> — Check the checkbox to enable scheduling. See <i>Schedule</i> below for details.
Subnet Filter	<p>Note: This option is available only when <i>Subnet Filter</i> is selected in the <i>Filters</i> field above.</p> <p>Specify the subnet in one of the following formats:</p> <ul style="list-style-type: none"> • 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 <p>Note: The <i>No IP</i> 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.</p>
Location Filter	<p>Note: This option is available only when <i>Location Filter</i> is selected in the <i>Filters</i> field above.</p> <ul style="list-style-type: none"> • Use the list menu to select the countries or regions of interest. • Select Unknown Country or Region if the location is unknown.

Parameter	Description
Schedule	<p>Note: This option becomes available only when <i>Schedule</i> is selected in the <i>Filters</i> field above. Set the schedule using the following parameters:</p> <ul style="list-style-type: none"> • <i>Weekdays</i> — Select the days of the week. • <i>Timezone</i> — 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. • <i>Time Range</i> — Select either <i>All day</i> (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	<p>The action specified in the policy, which can be one of the following:</p> <ul style="list-style-type: none"> • <i>Multi-factor Authentication</i> (default) • <i>Block</i> • <i>Bypass</i> <p>Note: The FTC server takes the specified action when an authentication request matches the profile.</p>
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: <ul style="list-style-type: none"> • <i>Multi-factor Authentication</i> (default) • <i>Block</i> • <i>Bypass</i> (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)

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*.

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*.

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 89](#)
- [Management on page 91](#)
- [SMS on page 93](#)

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.

Column	Description
	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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> <i>Success</i> <i>Failed</i>

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: <ul style="list-style-type: none">• <i>Auth Client</i>• <i>FTC portal</i>
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: <ul style="list-style-type: none">• The serial number of FGT if the request was made from FGT.• The username of the FTC user if the request was made from the FTC portal.
Action	The action of the request, which can be one of the following: <ul style="list-style-type: none">• <i>Create</i>• <i>Get</i>• <i>Modify</i>
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

This 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.

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.

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 94.](#)
- [Activate FTM tokens on page 95.](#)
- [Activate third-party tokens on page 95.](#)
- [Use FTM tokens on page 95.](#)

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**.
4. Download and install the app.

Activate FTM tokens

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

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

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

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

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

Activate third-party tokens

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

Use FTM tokens

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

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

To use a FTM token:

1. From your iPhone, start the **FortiToken Mobile** app.
2. On the home screen, press and hold on an OTP code, and tap **Copy**.
3. From your iPhone, start FTC.
4. Log in with your username and password.
5. Paste the OTP code when prompted.

You should be able to log into FTC if you pass the MFA process.

FAQs

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 125 SMS credits for each end-user annually. The number of credits that FTC charges varies, depending on where the end-user's phone number is registered. For more information, see [SMS Rate](#)

Card.

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](https://partnerportal.fortinet.com/directory/) or go to <https://partnerportal.fortinet.com/directory/>

Is the SMS quota shared by all users? What happens if we've reached the 2,500-message 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 "[time-based 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](#).

I still have SMS quota available in my account. What happens to my current outstanding SMS quota after transition to credit-based SMS accounting?

After switching to credits-based SMS accounting, all existing licensed customers will receive a total SMS credit equivalent to their existing SMS balance x 10.

Do I need to take any actions to transition to SMS credits from messages?

No, you don't need to take any actions to transition to SMS credits from messages.

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](#) and [SKUs vs. auth clients and realms supported](#) 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 Feb 2020 and the new license was in Jun 2021. So for the four months between Feb 2021 when the old license expires and Jun 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 $X \leq 120$, User Quota = 120
- If $120 < X \leq 1,200$, User Quota = 1,200
- If $1,200 < X \leq 12,000$, User Quota = 12,000
- If $12,000 < X \leq 120,000$, User Quota = 120,000
- If $X > 1,200,000$, User Quota = 1,200,000
- Realm Quota = $\min(\text{User Quota}/10, 120,000)$
- 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.

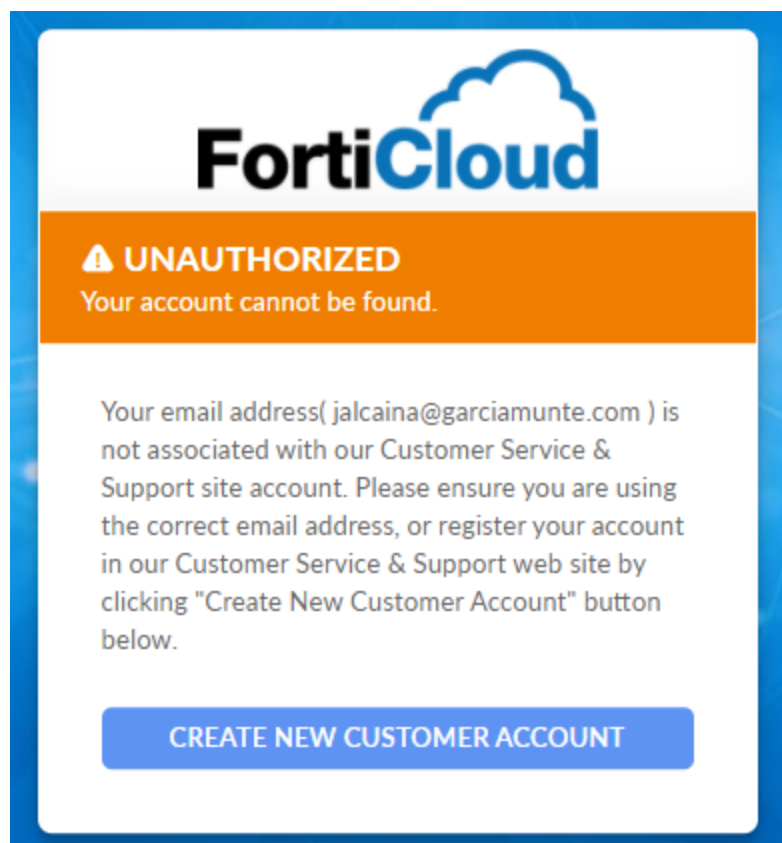
Accounts

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 77](#).

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](#).

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 want 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 [Aliased users](#).

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 35](#) 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	EFTMxxxxxxxxxxxx.pdf	FASxxxxxxxxxxxx.pdf
License Serial Number Format	FTKMOBxxxxxxxx	FTCxxxxxxxxxxxx
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

Type	FortiToken	FortiToken Cloud
		(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 you 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-wildcard 2FA if cnid=sAMAccountName?

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+eec9WilqmxYnZvrf3QSxJ8Bui73VwAo+ngLSf3ynkLF4So9AmAn6zNqbRHqQOEwSM5jP1p2BNNdnpCHJl006u
FwQmySdvUm6CYhXsD/zNB3T4XkTIDqTy5g43/Fq0CavX7sXtI485chKKaAU5HRO6xf+/0+2ZeBj2qlHxOx07Qz1j2Wkq
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)" (<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

How does FortiOS support FortiToken Cloud?

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
6.2.0	FT M	No	No	No	No	No. FTC must be enabled manually config system global set for tit oke n- clo ud- ser vic e {en abl e dis abl e}	execute forti toke n- cloud sync- user- Synchronize users to the FortiToken Cloud	diagnos e ftk- cloud debug- Enable/di sable debug output.

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

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnos e Command
								sync— Synchron ize user informati on with FortiToke n Cloud.
6.2.1	FT M	No	No	No	No	No. FTC must be enabled manually config system global set for tit oke n-clo ud-ser vic e {en abl e dis abl e}	execute forti toke n-cloud sync-user— Synchronize users to the FortiToken Cloud	diagnos e ftk-cloud debug— Enable/di sable debug output. server — Display FTC server IP address, port number, and https. show— Display diagnosti cs informati on. delete — Delete a user (name).

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnos e Comma nd
								<p>set-http— Set HTTP status return code for diagnostics purposes.</p> <p>clear— Clear server connection settings for diagnostics.</p> <p>sync— Synchronize user information with FortiToken Cloud.</p>
6.2.2	FTM	No	No	<pre>config user ldap edit "L" set server "xx.xx.xx.xxx" set cnid "uid" set dn "dc=srv,dc=world" set type regular</pre>	No	No. FTC must be enabled manually config system global	<pre>exe fortitoken-cloud new — Send new activation code for a user.</pre> <p>show — Show service status of this FortiGate.</p>	<pre>diagnose ftk-cloud debug-Enable/disable debug output.</pre>

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnos e Command
				set two-factor forti token-cloud		set for tit oke n-clo ud-ser vic e {enable disable}	sync — Synchronize users to FortiToken Cloud. trial — Activate free trial. update — Update VDOM list to FortiToken Cloud.	server — Display FTC server IP address, port number, and https. show — Display diagnostics information. delete — Delete a user (name). set-http — Set HTTP status return code for diagnostics purposes. clear — Clear server connection settings for diagnostics.

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnos e Command
								sync— Synchron ize user informati on with FortiToke n Cloud.
6.2.3	FT M, Em ail, SMS	No	No	config user ldap edit "L" set server "xx.x xx.xx .xxx" set cnid "uid" set dn "dc=s rv,dc =worl d" set type regul ar set two- factor forti token- cloud	No	Yes	exe fortitoke n-cloud show— Show service status of this FortiGate. sync — Synchronize users to FortiToken Cloud. trial — Activate free trial.	diagnos e ftk- cloud debug— Enable/di sable debug output. server — Display FTC server IP address, port number, and https. show— Display diagnosti cs informati on. delete — Delete a user (name).

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnos e Comma nd
								<p>set-http— Set HTTP status return code for diagnostics purposes.</p> <p>clear— Clear server connection settings for diagnostics.</p> <p>sync— Synchronize user information with FortiToken Cloud.</p>
6.2.4	FT M, Email, SMS	Yes	No	<pre>config user ldap edit "L" set server "xx.xx.xx.xxx" set cnid "uid" set dn "dc=srv,dc=world" set type regular</pre>	<pre>execute fortitoken-cloud update</pre>	Yes	<pre>execute fortitoken-cloud new —Send new activation code for a user.</pre> <p>show — Show service status of this FortiGate.</p>	<pre>diagnose ftk-cloud debug-Enable/disable debug output.</pre>

FOS Version	2FA	Multi-real m	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
				set two-factor forti token-cloud			sync — Synchronize users to FortiToken Cloud. trial — Activate free trial. update — Update VDOM list to FortiToken Cloud.	server — Display FTC server IP address, port number, and https. show — Display diagnostics information. delete — Delete a user (name). set-http — Set HTTP status return code for diagnostics purposes. clear — Clear server connection settings for diagnostics.

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								sync— Synchron ize user informati on with FortiToke n Cloud.
6.4.0	FT M, Em ail, SMS	Yes	No	config user ldap edit "L" set server "xx.x xx.xx .xxx" set cnid "uid" set dn "dc=s rv,dc =world set type regul ar set two- factor forti token- cloud	execute fortito ken- cloud update	Yes	exe fortitoke n-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.	exe fortito ken- cloud FGT200 E-641 (globa l) # diagnos e ftk- cloud debug— Enable/di sable debug output. server — Display FTC server IP address, port number, and https. show— Display diagnosti cs informati on.

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnos e Command
								<p>delete — Delete a user (name).</p> <p>set-http— Set HTTP status return code for diagnostics purposes.</p> <p>clear— Clear server connection settings for diagnostics.</p> <p>sync— Synchronize user information with FortiToken Cloud.</p>
6.4.1	FT M, Email, SMS	Yes	Yes	<pre>config user ldap edit "L" set server "xx.xx.xx.xxx" set cnid "uid" set dn "dc=srv,dc=world"</pre>	<pre>execute fortitoken-cloud update</pre>	Yes	<pre>execute fortitoken-cloud new-activation code for a user.</pre>	<pre>diagnose ftk-cloud debug-Enable/disable debug output.</pre>

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
				set type regul ar	set two- factor forti token- cloud		show — Show service status of this FortiGate. sync — Synchronize users to FortiToken Cloud. trial — Activate free trial. update — Update VDOM list to FortiToken Cloud.	server — Display FTC server IP address, port number, and https. show — Display diagnosti cs informati on. delete — Delete a user (name). set- http — Set HTTP status return code for diagnosti cs purposes. clear — Clear server connectio n settings for diagnosti cs.

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnos e Command
								sync— Synchron ize user informati on with FortiToke n Cloud.
6.4.2	FT M, Em ail, SMS	Yes	Yes	config user ldap edit "L" set server "xx.x xx.xx .xxx" set cnid "uid" set dn "dc=s rv,dc =worl d" set type regul ar set two- factor forti token- cloud	execute fortito ken- cloud update	Yes	exe fortitoke n-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.	diagnos e fortito ken- cloud debug Enable/di sable debug output. server —IP address port number and https.

FOS Version	2FA	Mul ti-real m	Aut o-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								<p>show — Display diagnostics information.</p> <p>delete — Command to delete a user.</p> <p>set-http — Set HTTP status return code for diagnostics only.</p> <p>clear — Clear server connection settings for diagnostics.</p> <p>sync — Synchronize user information with FortiToken Cloud.</p>

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.

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

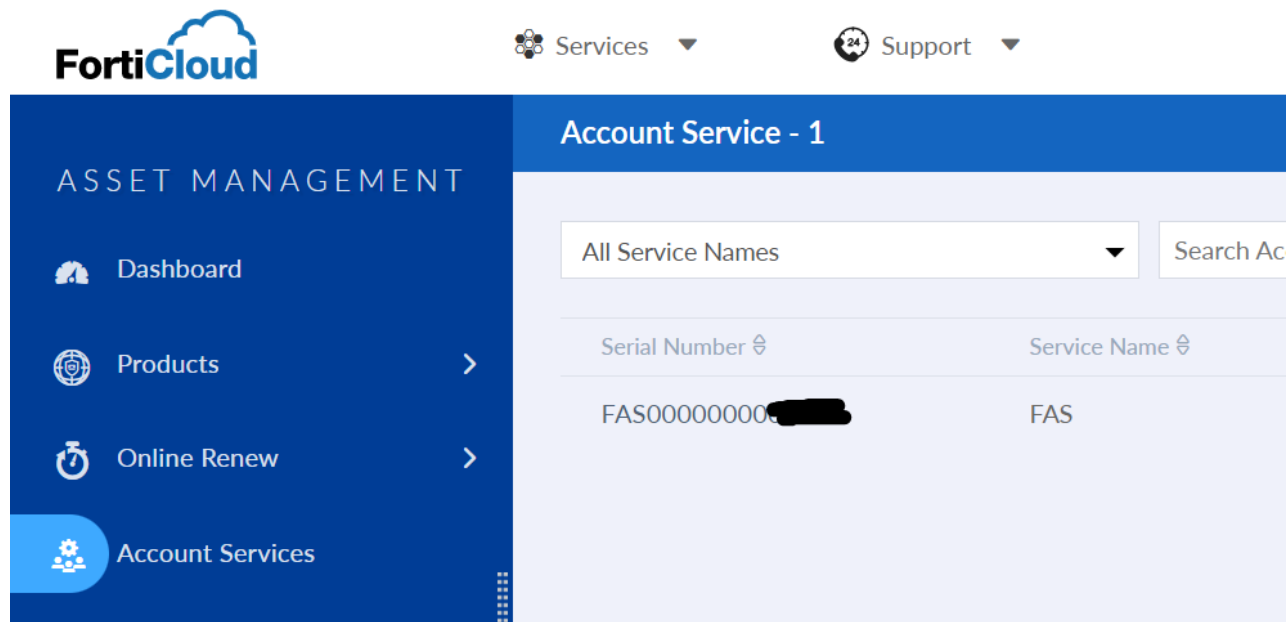
Items per page: 10 1 - 5 of 5

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:

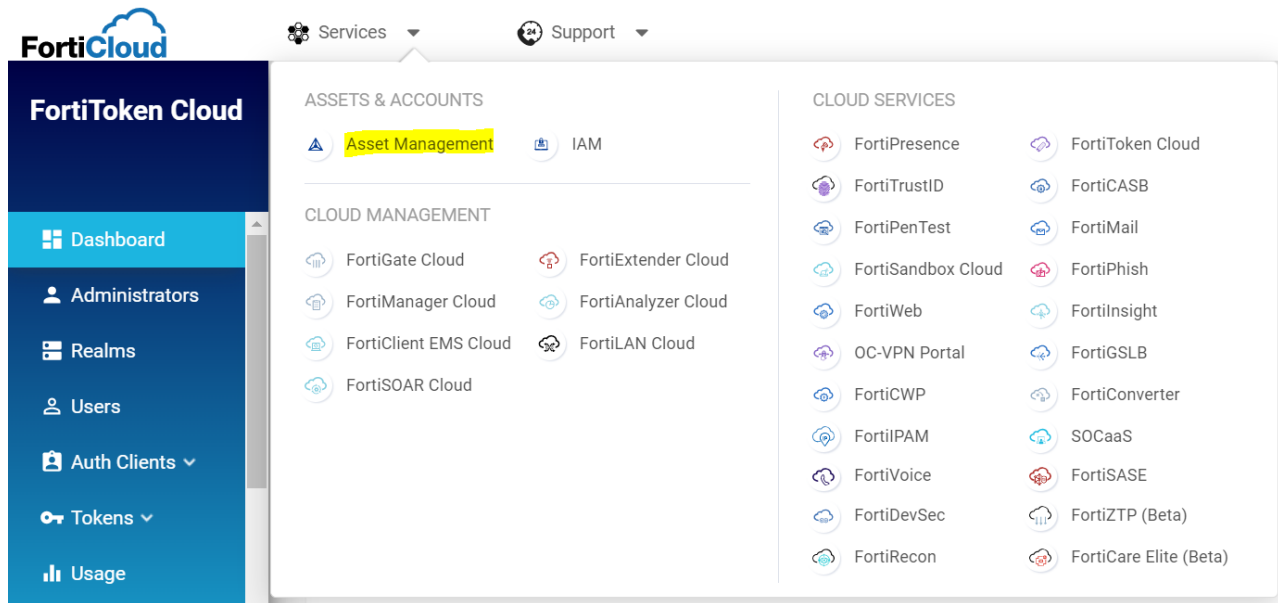
1. Go to *Services > Asset Management*.
2. Select *Account Services*.
3. Find and take note of your FAS service serial number.



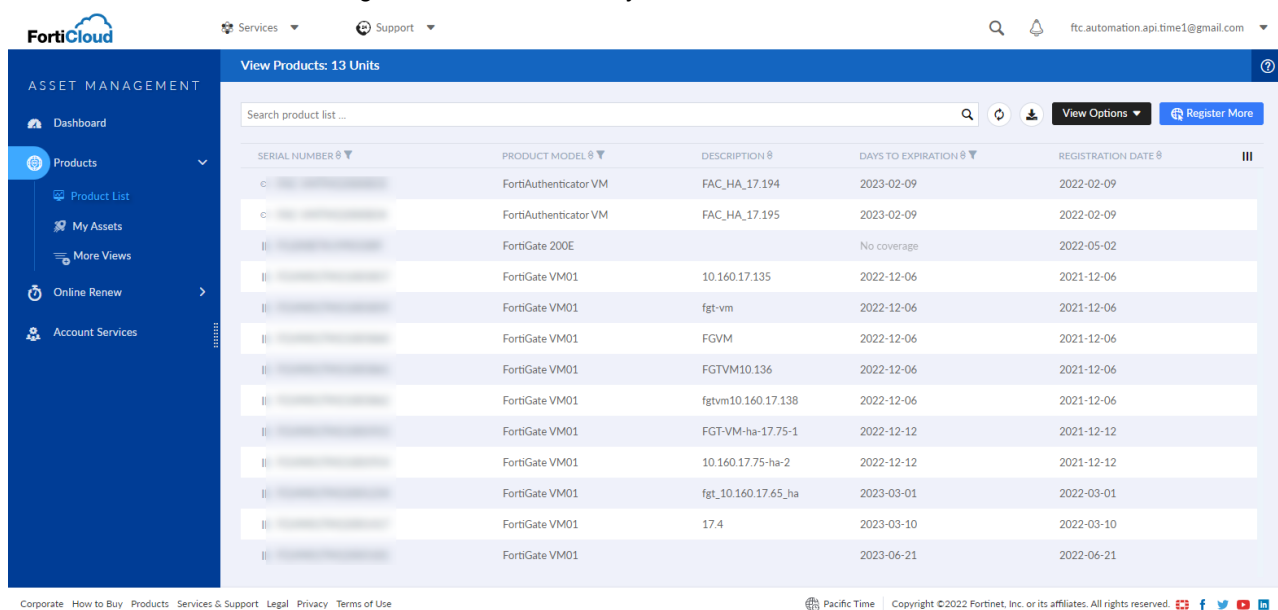
Customers with FTM Tokens migrated from FortiGate to FTC

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**.

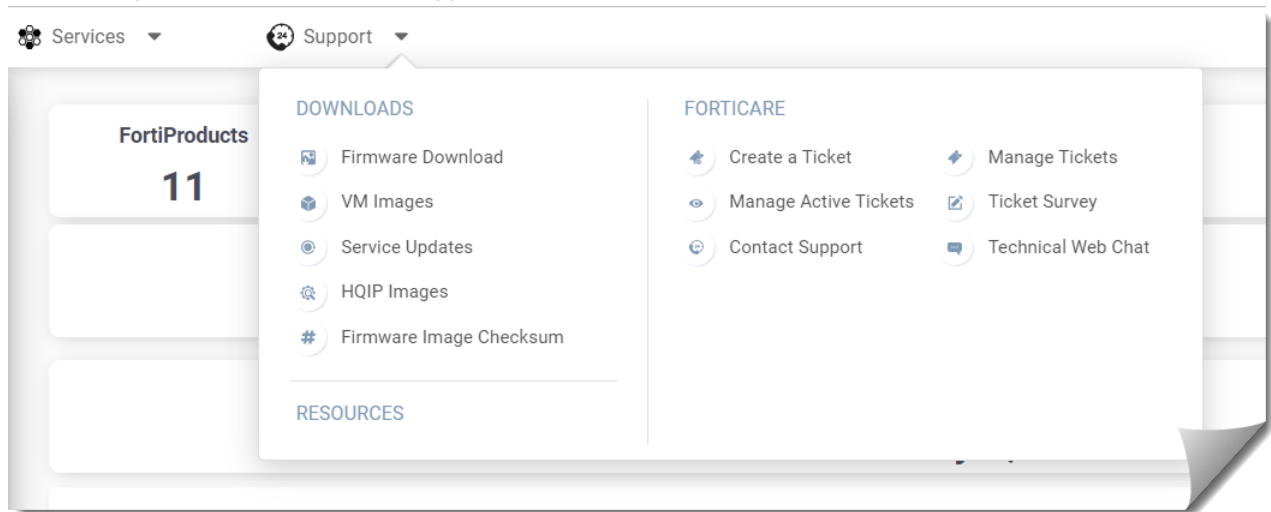


2. Click **Products > Product List** to get the serial number of your FortiGate.



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*.

Ticket Wizard

Create Ticket

1 Request Type > 2 > 3 > 4

Specify Request Ticket Type




Technical Support Ticket


You can create technical support tickets for technical issues with your Fortinet product. You require a Fortinet product with an active support contract to create this type of ticket. You will need to input the product serial number.

Serial Number: *

?




Submit Ticket




Start Web Chat

You can talk to our engineers via online web chat for general technical questions that do not require extensive troubleshooting.



Search our Knowledge Base

You can search our Knowledge Base for answers to many common questions in the use of Fortinet products.



Customer Service

You can create customer service tickets for questions related to contracts and account management.



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
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.
04/30/2019	FortiToken Cloud 4.2.d.
04/04/2019	FortiToken Cloud 4.2.b.



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.