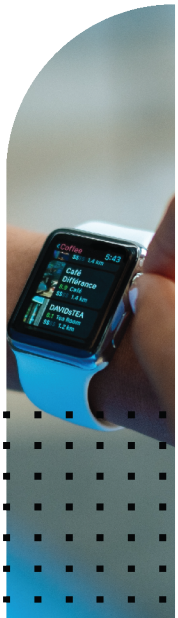
FAQs

FortiToken Cloud 21.2.d



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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 5, 2021
FortiToken Cloud 21.2.d FAQs

FAQs

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

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

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

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

How to configure FortiGate for LDAP authentication?

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

Step 1: Configure LDAP server in FortiGate via CLI

```
config user ldap
    edit "ldap_1"
        set server "xx.xxx.xx.xxx" (ldap-server-ip)
        set source-ip xx.xxx.xx.xx (fgt-ip)
        set cnid "cn"                <<< cnid
        set dn "DC=FIS,DC=local"
        set type regular
        set two-factor fortitoken-cloud  -> enable 2fa ftc
        set username "CN=admin,CN=Users,DC=FIS,DC=local"
        set password ENC  ----
>YmplY+eec9Wi1qmxYnZvrf3QSxJ8Bui73VwAo+ngLSf3ynkLF4So9AmAn6zNqbRHqQOEwSM5jP1p2BNNdnpCHJlo06u
FwQmySdvUm6CYhXsD/zNB3T4XkTIDqTy5g43/Fq0CavX7sXtI485chKKaAU5HRO6xf+/0+2ZeBj2qlHxOxO7Qz1j2Wkq
kN+bRyAGkVUDOkw==
    next
```

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

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

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

```
exe fortitoken-cloud sync
```

Step 4: Verify all LDAP users on FTC portal

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

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

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

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

Single auth status checking by auth id

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

Batch auth query

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

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

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

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

How to Configure SNMP server on FortiOS

Configuring an SNMP sever on FortiOS requires the following steps:

Step 1: Configure the SMTP server

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

Step 2: Configure SMS service on FortiGate

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

Step 3: Configure SMS service on SMS provider

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

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

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

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

How does FortiOS support FortiToken Cloud?

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

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`set-http`— Set HTTP status return code for diagnostics purposes. `clear`— Clear server connection settings for diagnostics. `sync`— Synchronize user information with FortiToken Cloud.
6.2.1	FTM	No	No	No	No	No. FTC must be enabled manually `config system global`	`execute fortitoken-cloud sync-user`— Synchronize users to the FortiToken Cloud	`diagnose ftk-cloud debug`— Enable/disable debug output.

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

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

6.2.2	FTM	No	No	`config user ldap`
				`edit "L"`
				`set server "xx.xxx.xx.xxx"`
				`set cnid "uid"`
				`set dn "dc=srv,dc=world"`
				`set type regular`
				`set two-factor fortitoken-cloud`
					No	No. FTC must be enabled manually
						`config system global`
						`set fortitoken-cloud-service {enable | disable}`
							`exe fortitoken-cloud new` — Send new activation code for a user.
							`show` — Show service status of this FortiGate.
							`sync` — Synchronize users to FortiToken Cloud.
							`trial`— Activate free trial.
							`update` — Update VDOM list to FortiToken Cloud.
								`diagnose ftk-cloud debug`—Enable/disable debug output.
								`server` — Display FTC server IP address, port number, and https.
								`show`— Display diagnostics information.
								`delete` — Delete a user (name).

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

6.2.3	FTM, Email, SMS	No	No	`config user ldap`
				`edit "L"`
				`set server "xx.xxx.xx.xxx"`
				`set cnid "uid"`
				`set dn "dc=srv,dc=world"`
				`set type regular`
					No	Yes	`exe fortitoken-cloud show` — Show service status of this FortiGate.
							`sync` — Synchronize users to FortiToken Cloud.
							`trial` — Activate free trial.
								`diagnose ftk-cloud debug`— Enable/disable debug output.

FOS Version	2FA	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
				`set two-factor forti token-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	Multi-realm	Auto-create Auth	Open LDAP wildcard Remote	Send VDOM List	FTC Enabled by Default	FTC execute command	FTC Diagnose Command
								`sync`—Synchronize user information with FortiToken Cloud.

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

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

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

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

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

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

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

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

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

How to prevent LDAP users from bypassing 2FA?

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

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

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

Check 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 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, eg., accountA@gmail.com, doesn't work, you can transfer your FGT to a different FortiCloud account, e.g., accountB@gmail.com, to continue using FTC service. Just follow these steps:

Step 1: Transfer the FortiGate using the FortiOS Administrator portal.

For FOS version 6.4.1 or later and FOS version 7.0.0 or later.

1. Log into 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"**.

For FOS version 6.4.0 or earlier, please contact FortiCare Technical Support at fortinet.com/support/contact to request FortiGate account transfer via 'Live Chat' or Call. You must have your FortiGate serial number ready to complete the account.

Step 2: Manually delete existing auth clients from the old FortiCloud account form 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.**

Note: If you cannot access your old FortiCloud account any more, contact the Fortitoken Cloud support team via email fortitokencloud-support@fortinet.com.

Step 3: 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 4: Update FTC user to new account using the FortiGate CLI.

```
execute 'exe fortitoken-cloud sync
```

Note: 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**, and 2) Select the realm, and then click Apply.

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.

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.

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

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

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

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

- **Pending**—The newly provisioned user initially shows up in ‘Pending’ status on the portal.
- **Active**—It changes to "Active" as soon as FortiToken Mobile is activated for the user.
- **Expired**—If the FTC token is not activated on its expiration date, the status changes to ‘Expired’.
- **No bypass/Bypass**—If bypass is enabled **(Settings>Realm>General Setting>Enable Bypass),** the newly created user in that realm shows up in ‘Bypass’ status.
- **Unlocked/Locked**—If the user's login attempts have exceeded the ‘Max Login Attempts Before Lockout’, the user's status changes to ‘Locked’.

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

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

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

Situation:

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

Solution:

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

How to create an aliased user?

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

To create an aliased user:

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

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

How to provision FortiToken Cloud?

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

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

1. Open the Console on the FortiGate device GUI.
2. Enable the **FortiToken Cloud Service** on the device:

```
config system global
   set fortitoken-cloud-service enable
end
```

   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 in the Admin Guide.

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 a unactivated credit-based license, what are my options if I want to switch to a time-based license?

You can either activate it and consume all the points before switching to a time-based subscription or contact Fortinet Support to see if they can replace your unused credit-based license with a 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 many SMS messages will I get with my new time-based license?

Each time-based license (SKU) allows for SMS messages in the amount of 100 multiplied by the total number of FTC end users that it can support for the year. For example, if you have a 25-user license (i.e., FC1-10-TKCLD-445-01-DD), you will be able to use a total of 2,500 SMS messages for the year.

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 get a free trial license?

FTC trial is auto-enabled. You just need to register your account on FortiCloud at support.fortinet.com using your business contact information.

For FortiGate users, the free trial is enabled after your first-time login to the FTC portal or creation of the first user with FTC for MFA.

See How do I register my FortiToken Cloud license to use the service? on page 29

How can I purchase a FTC license?

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

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	EFTMxxxxxxxxxxx.pdf	FASxxxxxxxxxxx.pdf
License Serial Number Format	FTKMOBxxxxxxxxxx	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 (It only displays all activated FortiToken-cCoud 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

What is "fortitoken-cloud show" command for?

On FOS 7.0.0 and 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:

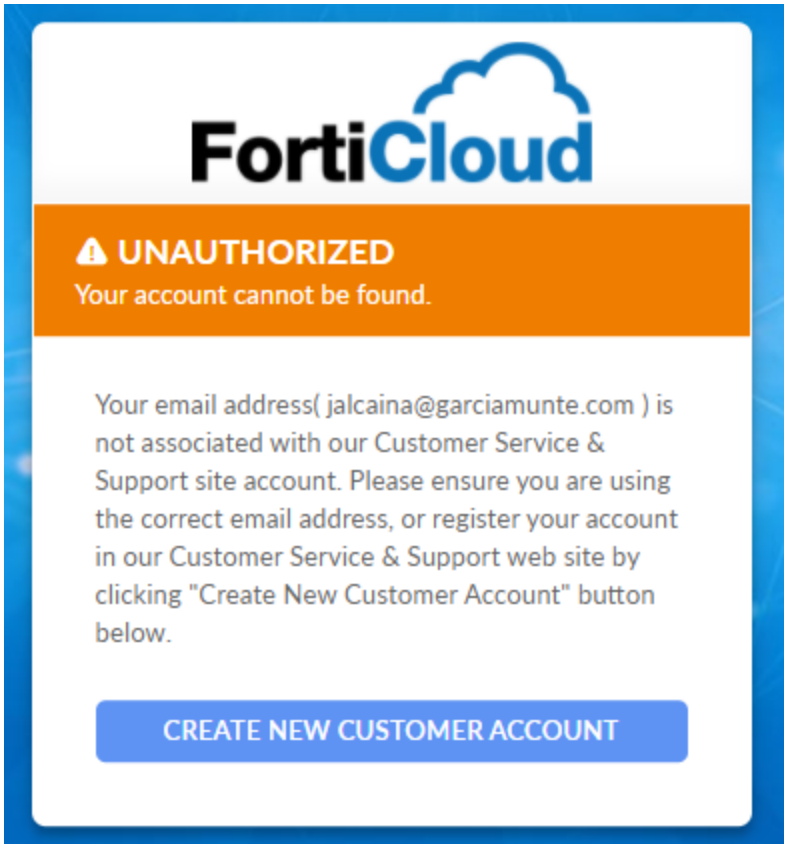
```
FGT_TEST (global) # exe fortitoken-cloud show
     FortiToken Cloud service status: licensed, service ready.
     Service balance: 36.66 points. Customer ID: 908147.
     FortiToken Cloud account number of users: 28, max number of users: 1200.
```

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 the FortiToken-Cloud team via email fortitokencloud-support@fortinet.com 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.

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.

What will happen if multi-realm mode is disable/enable?

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

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.

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 AuthClients, one for “#administrators” VDOM and another one for “root” VDOM, then the number of supported clusters will be 5."

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 +(contrycode)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.**

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

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

For more information, refer to the Purchasing Guide.

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.

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>FortiProdcuts 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.

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.

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

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

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

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.

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

Will expired licenses show on FTC Licenses page?

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

Why quota can 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.

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

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

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.

www.fortinet.com