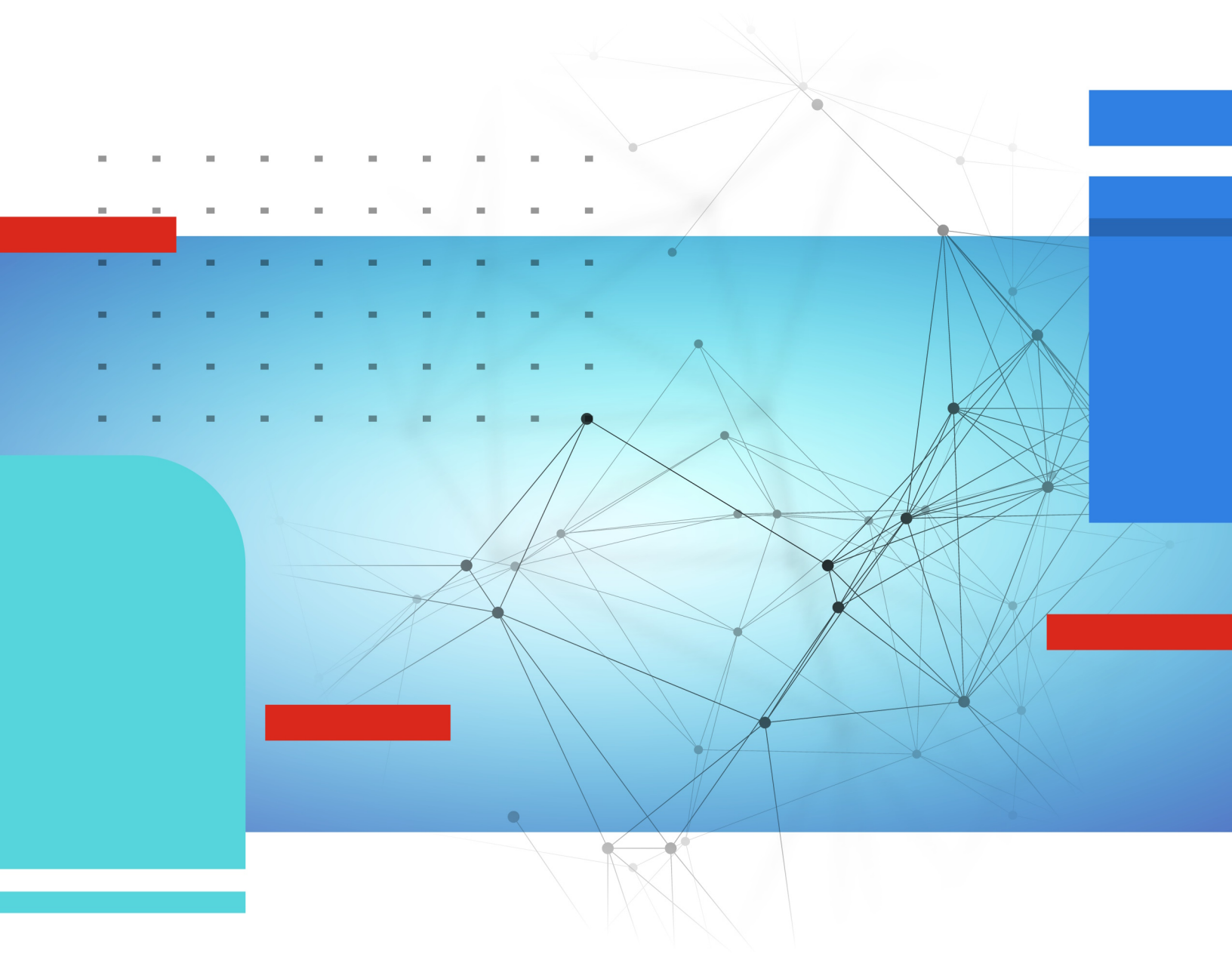




# Admin Guide

FortiToken Cloud 25.2.a



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 9, 2025

FortiToken Cloud 25.2.a Admin Guide

---

# TABLE OF CONTENTS

<b>Introduction</b>	<b>10</b>
<b>Licensing and availability</b>	<b>11</b>
Subscription licensing	11
Time-based SKUs and their services	11
SKUs vs. applications and realms supported	12
Stackable co-termed licenses	12
Resource rules	12
Free trial license	13
SMS licensing	14
Email notification on license balance status	14
<b>Architecture</b>	<b>16</b>
<b>Acronyms and abbreviations</b>	<b>17</b>
<b>Quickstart guide</b>	<b>18</b>
Step 1: Register FortiProduct (FortiGate)	18
Step 2: Get FTC license	19
Option 1: Trial license	19
Option 2: Paid license	20
Step 3: Configure SSL VPN and a local user on FGT with FortiToken Cloud enabled for MFA	20
Step 4: Activate the local user on FTM app	20
Step 5: Configure FortiClient on the login server	21
Step 6: User login authentication	21
Getting started—FGT-FTC users	21
Register your FTC subscription	21
Upgrade FortiOS	22
Log in to the FortiToken Cloud portal	22
Activate FGT VDOMs for FTC service	23
Add an admin user for FTC service	23
Add a local user for FTC service	24
Add remote FortiGate users for FTC service	24
Getting started—FAC-FTC users	25
Register your FTC subscription	25
Upgrade FortiAuthenticator OS	26
Log in to the FortiToken Cloud portal	26
Activate FAC for FTC service	27
Add an admin user for FTC service	27
Add a local user for FTC service	28
Enable FTC service for remote users	28
<b>Main features</b>	<b>30</b>
<b>Compatibility</b>	<b>36</b>
Compatible Fortinet applications	36
Supported browsers	37

<b>Important notes</b>	<b>38</b>
Trial account API request limit	38
Auth clients to applications	38
The same token for the same user on multiple applications	39
A single FTC user in multiple applications	39
Admin accounts and realms	39
Supported OTP hard tokens	40
Supported FIDO security key	40
No SMS MFA with FAC as LDAP server	40
FAC users' name issues on FTC GUI	40
How to use FortiClient	41
Use auto push	41
Use OTP	44
Enabling/Disabling FTC end-users on FortiGate	44
New public IP for FTC	44
Account disablement and closure	45
<b>FortiToken Mobile</b>	<b>46</b>
Supported FortiToken Mobile apps	46
Activate FTM tokens	47
Activate third-party tokens	47
Use FTM tokens	47
<b>Use cases</b>	<b>49</b>
One Token shared by different applications	49
Change separate tokens to a single token	50
Independent token	52
Auto-Alias features—Use the same email address	53
Split user quota to different realms	56
FTC account lockout (2FA)	60
Manage access to FTC	62
Admin Group	62
Add an admin group	63
Add realms to an admin group	65
Control risky conditions	65
Adaptive Authentication	65
Create adaptive authentication policy	66
Create adaptive authentication profile	66
Apply adaptive authentication profile to an application	67
Apply adaptive authentication profile to a realm	68
Migrate FTM tokens to FortiToken Cloud	70
Migrate FTM tokens from FortiGate	71
Migrate FTM tokens from FortiAuthenticator	72
Synchronize LDAP remote users in wildcard user group from FortiGate	74
Transfer devices on FTC	75
ZTNA HTTPS access proxy with FTC MFA	77
Add FTC MFA to remote access IPsec VPN	78



Create users .....	78
Create a user group .....	79
Configure FTC as Microsoft Entra external authentication service provider .....	79
Enable FortiSASE VPN users to use FTC MFA .....	85
Configuration On FTC: .....	85
Configuration on FortiSASE .....	86
FortiToken Cloud as OIDC provider .....	87
Configure FTC as an OIDC provider .....	88
End-user experience .....	90
<b>Applications .....</b>	<b>93</b>
Create FortiProduct applications .....	93
Transfer application (FC account logout) .....	93
Replace an old FortiGate with a new one .....	94
Applications in HA mode .....	94
Configuring the primary FortiGate .....	95
Configuring a backup FortiGate .....	96
Applications for third-party usage .....	97
<b>Maintenance .....</b>	<b>98</b>
Add, sync, and delete users .....	98
Add, sync, and delete applications (FortiProducts) .....	99
Service debug .....	99
<b>FortiToken Cloud GUI .....</b>	<b>100</b>
Launch FortiToken Cloud .....	102
Log in as a regular FTC user .....	102
Log in as an IAM user .....	103
Log into an OU account .....	103
FortiCloud .....	104
The FortiCloud Logo .....	104
Your FortiCloud account .....	104
Services .....	105
Support .....	106
Dashboard .....	107
Last 10 authentication attempts in 30 days .....	107
Monitor FTC status .....	108
Pagination for accounts with multiple sub-admin users .....	109
Refresh button for premium trial and extending premium trial .....	109
Manage admin groups .....	110
Create a sub-admin group .....	111
Delete a sub-admin group .....	113
Manage realms .....	113
Create a custom realm .....	114
Edit a realm .....	114
Delete a realm .....	115
View realm permission .....	115
Remove sub-admin groups from a realm access list .....	115
View realm settings .....	115

Manage users .....	115
Batch-add users .....	117
Enable Auto-alias by Email .....	118
Add user aliases .....	119
Auto-assign FTKs to selected users .....	119
Get a new FTM token .....	119
Hide/Show full FortiAuthenticator username .....	119
View a user's applications .....	120
Use a temporary token .....	120
Edit a user .....	120
Delete users from FTC .....	121
Manage user groups .....	121
Add a user group .....	122
Edit a user group .....	122
View user group information .....	122
Delete a user group .....	122
FortiProducts .....	123
Assign an application to a realm .....	124
Edit an application .....	124
Viewing additional information about an application .....	124
Delete an application .....	124
Web Applications .....	125
Add a web app .....	125
Regenerate API credentials .....	126
Edit a web app .....	126
Delete a web app .....	126
SCIM client integration .....	126
Management Applications .....	146
Use SSO applications .....	146
Use Cases .....	147
Example 1: Google SAML as IdP and FortiGate SSL VPN as SP .....	148
Example 2: Azure as SAML IdP and FortiGate as SP .....	158
Example 3: Google OIDC as IdP .....	160
Example 4: Azure OIDC as IdP .....	165
Example 5: FortiGate IPsec as SP .....	169
Example 6: ZTNA application gateway with SAML as SP .....	176
Configure domain mapping .....	180
Attribute Mapping .....	181
Login hint .....	181
Configure user source .....	182
Manage end-user portals .....	183
Configure End-user Portals .....	183
Configure IdP user source .....	185
Keep SSO applications off end-user portals .....	185
Manage device ownership .....	193
Validate device ownership .....	194
Transfer devices .....	194
Transfer devices on FTC .....	195

Manage device transfer .....	197
Perform factory reset .....	198
Manage HA clusters .....	198
Add devices to a cluster .....	198
Move a device between clusters .....	199
Remove devices from a cluster .....	199
Search for a standalone device .....	199
Use mobile tokens .....	200
Use hardware tokens .....	200
Add hard tokens manually .....	201
Batch-upload hard tokens .....	202
Assign a hard token to a user .....	202
Delete hard tokens .....	203
Use passkeys .....	203
Use Case .....	203
Register FortiToken 410 USB key in Windows devices .....	204
Steps to register a USB passkey for an end-user: .....	205
Authenticate with the USB passkey in IDP proxy .....	208
Steps to Register phone Passkeys for a Enduser: .....	211
Authentication with a Phone Passkey in IDP proxy .....	215
Logs for Passkeys .....	218
Delete PassKey .....	220
Usage .....	222
View usage data .....	222
View current user count and user quota .....	222
Licenses .....	223
License search bar .....	223
Manage global settings .....	224
Multi-realm Mode .....	224
Auto-create an application .....	225
Share-quota Mode .....	225
Username Case & Accent Sensitive .....	225
Account Disable/Delete Notification .....	226
Manage realm settings .....	226
General settings .....	226
FTM MFA settings .....	229
Email MFA settings .....	231
SMS MFA settings .....	231
Use templates .....	232
Add a template .....	232
Edit a template .....	233
Delete a template .....	233
Apply templates .....	234
Manage custom branding .....	235
Create an SSO application branding theme .....	235
Create an end-user portal branding theme .....	235
Delete a branding scheme configuration .....	236
Apply custom branding theme to SSO application .....	236

Apply custom branding theme to end-user portals .....	237
Manage certificates .....	237
Adaptive authentication .....	237
View adaptive authentication policies .....	238
Create an adaptive authentication policy .....	238
Edit an adaptive auth policy .....	239
Delete an adaptive auth policy .....	240
View adaptive auth profiles .....	240
Create an adaptive authentication profile .....	240
Apply adaptive authentication profiles .....	241
Edit an adaptive auth profile .....	241
Delete an adaptive authentication profile .....	241
Create a last-login policy .....	242
Create an impossible-to-travel policy .....	242
Alarms .....	243
Configure receivers .....	243
Configure receiver groups .....	243
Create an SMS credit balance alarm event .....	243
Create a user quota alarm event .....	244
Logs .....	244
Authentication .....	244
Management .....	246
SMS .....	248
<b>FOS CLI commands for FortiToken Cloud .....</b>	<b>250</b>
Global system configuration .....	250
Access FTC management commands .....	250
Configure admin users .....	251
Configure local users .....	252
Configure local LDAP users for FTC service .....	253
Configure wildcard LDAP users for FTC service .....	253
Configure local RADIUS users for FTC service .....	254
Migrate FTM tokens to FortiToken Cloud .....	255
Diagnose FortiToken Cloud .....	255
Show user ldap .....	256
<b>Product documentation and support .....</b>	<b>258</b>
<b>Release history .....</b>	<b>259</b>
25.2.a .....	259
25.1.a .....	259
24.3.a .....	259
24.2.a .....	260
23.4.b .....	260
23.4.a .....	260
23.3.b .....	260
23.3.a .....	260
23.1.a .....	261

22.4.a	261
22.3.a	262
22.2.d	262
22.2.c	262
22.2.b	262
22.2.a	262
21.4.d	263
21.4.a	263
21.3.d	263
21.3.c	263
21.3.b	263
21.3.a	264
21.2.d	264
21.2.c	264
21.2.a	264
21.1.a	265
20.4.d	265
20.4.c	265
20.4.a	265
20.3.e	265
20.3.d	266
20.2.c	266
20.1.b	266
20.1.a	266
4.4.c	267
4.4.b	267
4.3.a	267
4.2.d	267
4.2.c	267
4.2.b	268
<b>Technical support</b>	<b>269</b>
Prepare for technical support	269
How to get your Fortinet product serial number	269
Licensed customers	269
Customers with FTM tokens migrated from FortiGate to FTC	269
Create a technical support ticket	270
<b>Change log</b>	<b>272</b>

# Introduction

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

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

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

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

# Licensing and availability

- [Subscription licensing on page 11](#)
- [Free trial license on page 13](#)
- [SMS licensing on page 14](#)
- [Email notification on license balance status on page 14](#)

## Subscription licensing

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



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

- [Time-based SKUs and their services on page 11](#)
- [SKUs vs. applications and realms supported on page 12](#)
- [Stackable co-termed licenses on page 12](#)

## Time-based SKUs and their services

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

SKU	Number of FTC end-users supported
FC1-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 25 users, including 3,125 SMS credits and FortiCare Premium Support, per year.
FC2-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 100 users, including 12,500 SMS credits and FortiCare Premium Support, per year.
FC3-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 500 users, including 62,500 SMS credits and FortiCare Premium Support, per year.
FC4-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 2,000 users, including 250,000 SMS credits and FortiCare Premium Support, per year.
FC5-10-TKCLD-445-01-DD	FortiToken Cloud subscription for up to 10,000 users, including 1,250,000 SMS credits and FortiCare Premium Support, per year.

## SKUs vs. applications and realms supported

The following table highlights the number of applications 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 222](#).

## 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 the new license will be prorated so that it expires on August 1, 2022; it will have the same expiration date as the original 500-user license, but with a new limit of 525 users.

In the first case, the new license is independent of the original license, which can be purchased based on its SKU. In the second case, you will have to reach out to our license renewal team ([renewals@fortinet.com](mailto:renewals@fortinet.com)) for assistance.

For more information, see [Time-based SKUs and their services on page 11](#) and [SKUs vs. applications and realms supported](#) in the Admin Guide.

## Resource rules

For a licensed account, when the total purchased user quota is  $x$  among the licenses, the related resource quota is calculated as follows:



Resource	Quota
Users	x
Realms	If $x \leq 500$ , then x; if $x > 500$ , then $500 + x/10$
Web Applications & Mgmt Applications	Maximum (x/10, 5)
SAML Applications	Maximum (x/10, 5)
User Sources	Maximum (x/10, 5)
Certificates	Maximum (x/10, 5)
Brandings	Maximum (x/10, 5)
Domains	Maximum (x/10, 5)
User Groups	Maximum (x/10, 5)
Profile	100
Policies	200



- x/10 will truncate any decimal places if the result is not an integer. For example, if  $x = 49$ , x/10 is counted as 4.
- For realms, if the total purchased user quota is x and x is equal to or less than 500, the maximum number of realms allowed is also x; if the total purchased user quota is greater than 500, the maximum number of realms allowed is  $500 + x/10$ . For example, if user quota is 400, the maximum number of realms allowed is 400; if user quota is 600, the maximum number of realms allowed is 560.
- For maximum (x/10, 5), if the total purchased user quota is x, the maximum number of the target resource is the greater value between x/10 and 5. For example, if user quota is 40, the maximum number of the target resource is 5; if user quota is 60, the maximum number of the target resource is 6.

## Free trial license

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



You will receive a welcome email after activating the free trial license. The email includes, among other things, the expiration date of the free trial license and instructions on how to purchase a paid license.

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

---



You will receive another welcome email when activating a paid license. The email shows, among other things, the user quota and expiration date of your license.

---

FTC also offers a free three-user licenses that can be activated from the UI of supported Fortinet devices, such as FortiGate and FortiAuthenticator, as long as the device has a valid support contract in FortiCare. Neither the free license nor the 30-day free trial includes SMS quota.

The free three-user license include three realms and IdP proxy for unlimited downstream Fortinet devices and 1 upstream remote IdP. The free three-user license expires at the same time as the support contract of the device does.

If trial is enabled from the FortiToken Cloud portal, it allocates a quota of five users and five realms for non-premium account and 25 users and 25 realms for premium accounts only for 30 days. If the account has a supported device with a valid contract, the free three-user license can be activated after the 30-day trial ends.

## SMS licensing

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

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

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

## Email notification on license balance status

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

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

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

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

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

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

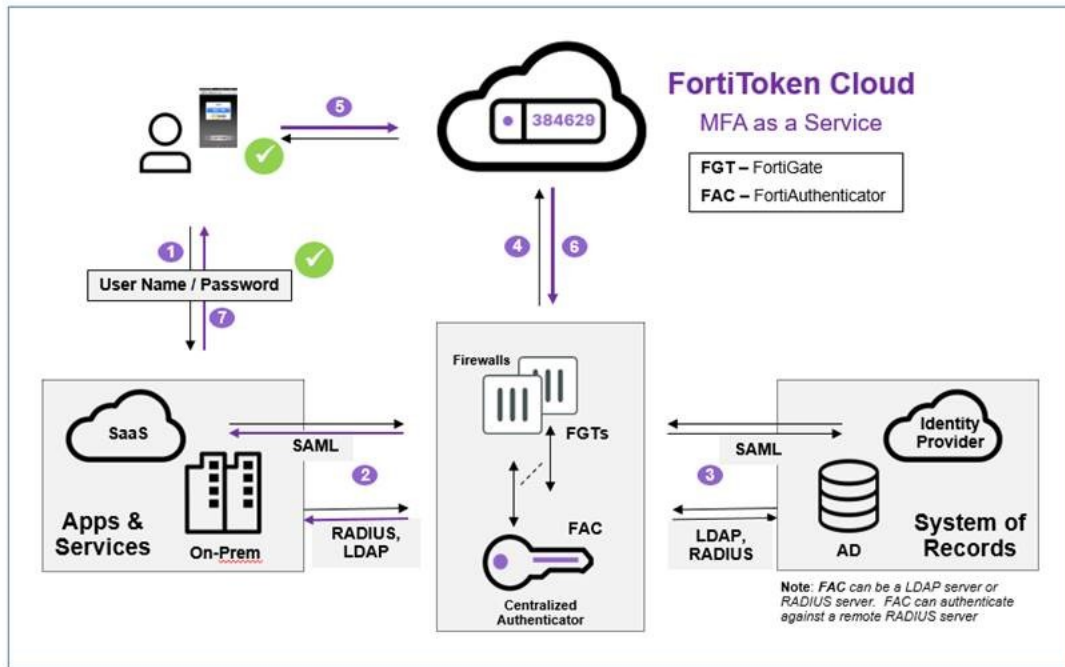
FTC also provides a switch button for enabling/disabling email notifications at *Settings > Global > Account Disable/Delete Notification*. The default setting of this feature is to receive all email notifications.

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

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

# Architecture

The following topology highlights the network architecture of the FortiToken Cloud end-to-end solution.



The following describes the workflow of the FTC MFA authentication process:

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

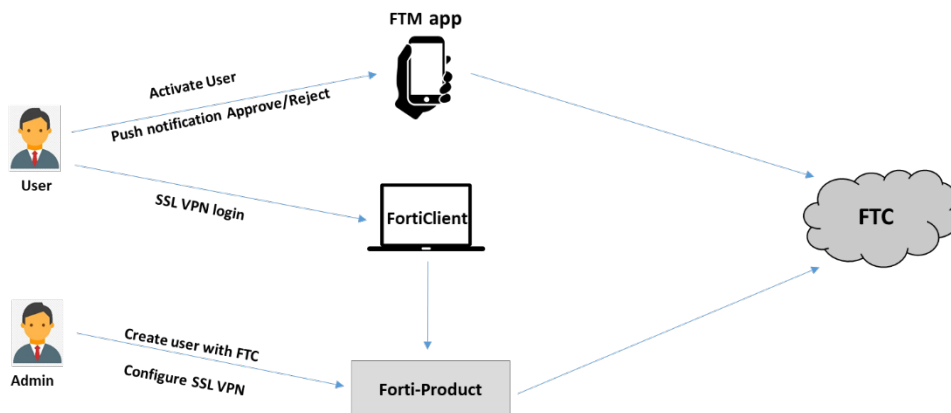
# Acronyms and abbreviations

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

Acronym/Abbreviation	Terminology
2FA	Two-factor authentication <b>Note:</b> 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)
IdP	Identity Provider
OIDC	OpenID Connect
OU	Organizational Unit
OTP	One-time password
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SMS	Short message service
SP	Service Provider
SSO	Single sign-on
TOTP	Time-based one-time password
UTC	Universal Time Coordinated (or Coordinated Universal Time)

# Quickstart guide

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

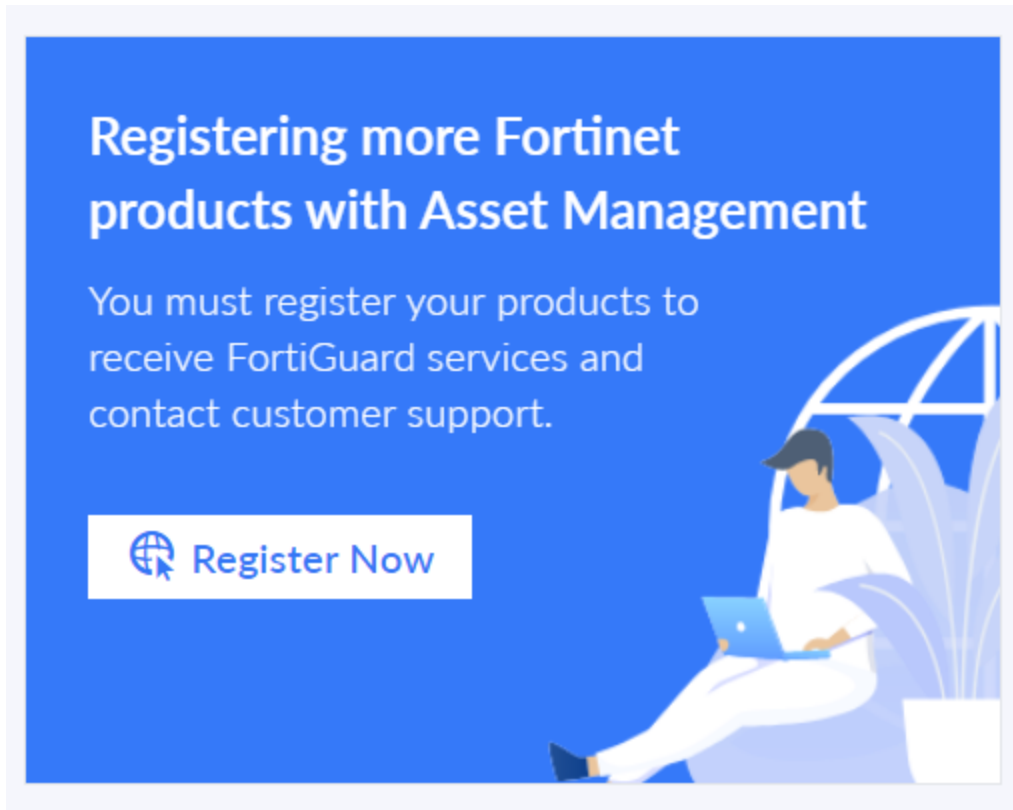


What you need:

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

## Step 1: Register FortiProduct (FortiGate)

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



## Step 2: Get FTC license

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

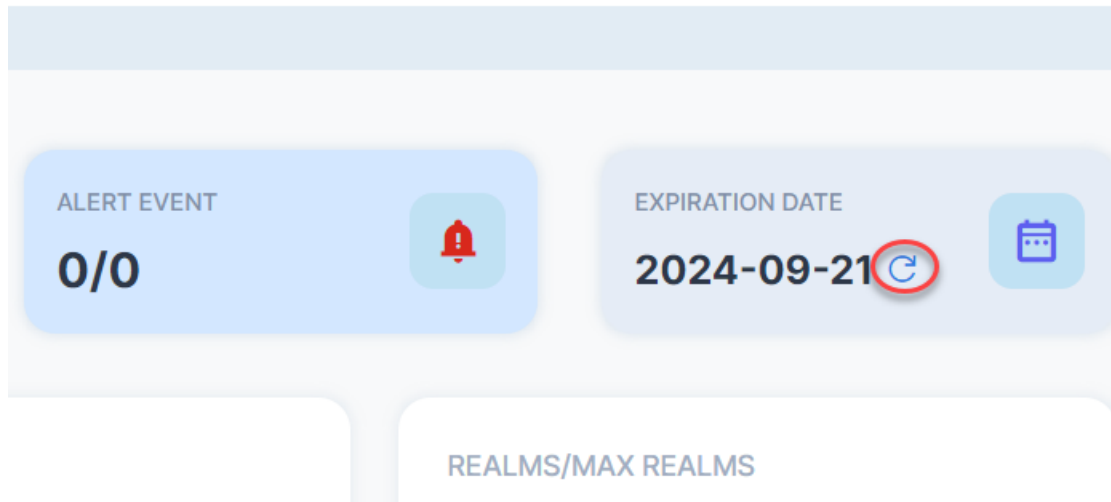
### Option 1: Trial license

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



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

ftc.device.migration2@gmail.c



## Option 2: Paid license

- [How to purchase FTC licenses](#)
- [How to register your FTC license](#)

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

Configure SSL VPN and a local user on FGT. See [SSL VPN setting up on FGT](#).

## Step 4: Activate the local user on FTM app

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

- [FortiToken Mobile on page 46](#)
- [Supported FortiToken Mobile apps on page 46](#)
- [Activate FTM tokens on page 47](#)
- [Activate third-party tokens on page 47](#)
- [Use FTM tokens on page 47](#)



## Step 5: Configure FortiClient on the login server

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

Link: [Connecting from FortiClient to SSL VPN](#)

## Step 6: User login authentication

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

## Getting started—FGT-FTC users



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

FTC supports up to four MFA methods, namely FTM, FTK, SMS, and email. The MFA method is set on a per-realm basis. The default method is FTM, but the admin user can change it to another method if needed. Sub-admins can then further change the MFA methods for end-users in their assigned realms to something other than the default (i.e., FTM). See [Manage users on page 115](#) for MFA methods used by end-users.

---

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

1. [Register your FTC subscription on page 21.](#)
2. [Upgrade FortiOS on page 22.](#)
3. [Log in to the FortiToken Cloud portal on page 22.](#)
4. [Activate FGT VDOMs for FTC service on page 23.](#)
5. [Add a local user for FTC service on page 24.](#)
6. [Add an admin user for FTC service on page 23.](#)

## Register your FTC subscription

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



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

---

### To register your FTC subscription:

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

## Upgrade FortiOS



This FTC release requires upgrading your FortiGate (FGT) firmware to FortiOS (FOS) version 6.4.0 or later.

---

### 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 6.4.x.
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 (FGT) users to take advantage of the MFA feature provided by FortiToken Cloud, you must make sure that FTC service is enabled on the FGT device.

Because FortiToken Cloud requires FOS 6.4.0 or later which has FortiToken Cloud service enabled by default, you normally do not need to manually enable FTC on your FGT. However, if for some reason, FTC is not enabled on your FGT, 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 SH2aEArTfqHbNJ8E2087zSFAYqak8t14t+AiQxH+XWhZMKJQMfoPZS002MDPCo=
  next
end
```

For more information, see [Configure admin users on page 251](#).

## 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+AFkwFVJdEpidKBIY0xn2L1LPpvSmWRhXhAFAP770ofUdF
Ss9eydatFw/BY/4WgCimfir1E0LdtTRjV09oaCj6LTPBYzZJsyrImmKx7benWG1tTOXWgmktUy88WR02rdUB8ZZdBTfDfDoBAL
2Q==
    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 applications page as well.

For more information, see [Configure local users on page 252](#).

## 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+/k6e4TtSk070t0DaCZAcbgEGKohA==
  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 253](#) 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 application. 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 application, as long as the realm associated with the FAC (or end-user) MFA method is provisioned properly.

---

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

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

## Register your FTC subscription

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



---

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

---

### To register your FTC subscription:

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

## Upgrade FortiAuthenticator OS



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

---

### To upgrade your FAC OS:

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

## Log in to the FortiToken Cloud portal



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

---

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

### To log in to the FTC portal:

1. Open your web browser, credit to <https://ftc.fortinet.com>, and press the **Enter** key on your keyboard.  
The FortiToken Cloud page opens.
2. In the upper-right corner of the page, click **LOGIN**.  
The FortiToken Cloud Login page opens.

3. Enter your FC master account username and password, and press **LOGIN**.  
Once you've logged in, the FortiToken Cloud landing page opens, showing your FTC account (or a list of accounts if your organization has multiple FTC accounts).
4. Click your account or one of your accounts to open it.  
The FTC Dashboard page opens by default.

## Activate FAC for FTC service

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

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



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

---

## Add an admin user for FTC service

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

1. From the FAC menu, click **Authentication>User Management>Local Users**.
2. From the top of the page, click **Create New** to open the Create New Local User page.
3. Specify a unique username.
4. For Role, select the **Administrator** radio button.
5. Click **Full permission** to enable it.
6. Click **OK**. The page refreshes.
7. On the Edit User page (depending on your FAC version), do the following:
  - a. 6.0, select Token-based authentication > FortiToken > FortiToken Cloud.
  - b. 6.1, select Token-based authentication > FortiToken > Cloud.
  - c. 6.2–6.3, select Token-based authentication > FortiToken > Cloud > Choose Email or SMS.
  - d. 6.4 and later, select One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS if Mobile was chosen.
8. Click **User Information**.
9. Enter the user's email address or SMS information as needed based on the option you chose earlier.
10. Click **OK**.



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

---

## Add a local user for FTC service

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

1. From the FAC menu, click **Authentication>User Management>Local Users**.
2. From the top of the page, click **Create New** to open the Create New Local User page.
3. Specify a unique username.
4. For Role, select the **User** radio button.
5. Click **OK**. The page refreshes.
6. On the Edit User page (depending on your FAC version), do the following:
  - a. 6.0, select Token-based authentication > FortiToken > FortiToken Cloud.
  - b. 6.1, select Token-based authentication > FortiToken > Cloud.
  - c. 6.2–6.3, select Token-based authentication > FortiToken > Cloud > Choose Email or SMS.
  - d. 6.4 and later, select One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS if Mobile was chosen.
7. Click **User Information**.
8. Enter the user's first name and last name.
9. Enter the user's email address or SMS information as needed based on the option you chose earlier.
10. Click **OK**.

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

---

## Enable FTC service for remote users

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

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

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



- d. 6.4 and later, select One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS if Mobile was chosen.
5. Click User Information.
6. Enter the user's email address or SMS information as needed based on the option you chose earlier.
7. Click OK.

# Main features

## FortiCloud SSO

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

## Free trial licenses

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

## Time-based annual subscriptions

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

## Authentication and Management logs

FTC provides comprehensive authentication and management logs to keep you informed of all authentication and management events that have happened in your account.

## Global administrator and sub-admin support

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

## Access to all accounts by admin users

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

## Realm support

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

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

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

## Integration with FOS

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

## Temporary token

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

## Disabling MFA after account disabled

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

## Secure, cross-platform token transfer

You can securely transfer your FTC and third-party tokens between iOS and Android devices using the FortiToken Mobile (FTM) app.

## Support for remote FortiGate users

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

## Auto log-out

FTC automatically logs out a user when the GUI has been idle for more than ten minutes, safeguarding the security and integrity of your asset on FTC.

## Real-time usage statistics

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

## Support for HA clusters

FTC supports FGT and FAC HA cluster configuration. You can add or remove auth devices to or from the FTC portal. You can view your FGT and/or FAC devices in any cluster from the applications page.

## Support for custom logo

The admin user can upload custom logo images to replace the default Fortinet banner at the bottom of the FTM app on your end-users' mobile devices.

## Support for multiple MFA options

FTC offers four MFA methods: FTM (FortiToken Mobile), email, SMS, and FTK (FortiToken, which is a hardware token).

## Auto-alias by email

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

## Realm-based user quota

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

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

## Export of logs in .CSV

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

## SMS usage

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

## Migration of FTM licenses to FTC

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

## Device ownership transfer

FTC enables you to transfer device ownership with or without migrating device data.

## Replay protection

FTC provides three (high, medium, and low) levels of MFA replay protection for admin users to choose from when configuring realm settings.

## Effective end-user management

FTC enables admin users to effectively monitor and manage their end-users from its portal.

## Support for pagination

FTC has implemented pagination to limit the number of records returned in each API request. This ensures that the system can respond to API requests faster, and present information in a more organized and user-friendly manner. For more information, refer to the FortiToken Cloud API.

## SMS usage restriction

FTC has implemented a mechanism that prevents users from using its SMS function if the destination is a restricted country by law. Once implemented, FTC will automatically pop up a message on its GUI, informing users of the restriction when it detects the SMS messages that are being sent to a restricted country. (**Note:** For this release, UAE is the only country that has such a restriction.)

## IdP Proxy

Identity Provider Proxy (IdP) combines the capability of both an IdP and Service Provider (SP) in one. With FortiToken Cloud providing the SAML and OIDC interface, applications can be part of the FTC SaaS service and take full advantage of the existing SSO protocol to integrate with not only the Forti-ecosystem, but third-party applications and IdPs as well.

## Passkeys

FTC has been implemented support for passkeys using Webauth, which is a core component of FIDO Alliance's FIDO2 set of specifications. The web-based API allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms. This enables end-users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

## SCIM

SCIM provides a standardized, secure methodology for exchanging information between IT systems. It ensures interoperability across domains without expensive custom integrations. SCIM auto-provisioning can free up valuable IT resources for critical tasks while boosting productivity across the entire organization.

## Migrate FTM tokens from FortiGate and FortiAuthenticator

FortiGate and FortiAuthenticator (FAC) administrators can migrate their FTM tokens from FAC to FTC. Upon completion of migration, FTC automatically generates a one-year free transfer license for the migrated account to cover the number of end-users corresponding to the total number of FTM tokens that have been transferred.

## Batch-add User

This features enables admin users to batch-add end-users from different realms manually or by importing end-user information in .csv files.

## User group

This feature enables admin users to set up authorization groups of users, grant different access rights to users by user group.

## Integration with Microsoft Entra ID

FTC now can be configured as an Entra MFA external authentication method (EAM) method provider. See [Configure FTC as Microsoft Entra external authentication service provider on page 79](#).

## End-user Portals

Introduced in FTC 25.1.a, this feature offers end users the capability to change or update their profiles, phone numbers, and MFA methods and register FIDO tokens on their own based on the permissions granted by the administrator. See [Manage end-user portals on page 183](#).

## FortiSASE VPN user SSO through FortiToken Cloud

Working in tandem with FortiClient, this feature enables customers to use FTC MFA to manage their FortiSASE VPN users SSO. See [Enable FortiSASE VPN users to use FTC MFA on page 85](#).

## Allow end users to use additional MFA methods

This feature provides additional MFA methods other than the default set in their realm to authenticate, especially when they are unable to access or use the default MFA method, for example, mobile phones. If email is chosen as an additional MFA method, FTC will automatically switch from SMS to email when SMS service becomes unavailable (for instance, due to no or inadequate SMS quota or geographical limitation or restrictions). See [General settings on page 226](#).

## Support for Local IdP

FortiToken Cloud's local IdP feature enables end users to log into their End-user Portal and applications using their user identity (username and password) local to FortiToken Cloud rather than any external identity provider, such as Google, Azure, etc. For more information, see [Local IdP](#).

## Support for OIDC Provider

FortiToken Cloud can be configured as an OpenID Provider (OP) for authenticating users and issuing tokens to a Relying Party (RP). When configured in tandem with its local IdP, FTC can be the authentication source as well and provide end-to-end OP functionality. For more information, see [FortiToken Cloud as OIDC provider on page 87](#).

## Allow rooted device

This features enables administrators to effectively manage rooted devices in their environment. For more information, see [General settings on page 226](#).

## Support for subdomain for End-user Portal

This feature enables you to create the End-user Portal using your custom URL rather than the URL generated by FortiToken Cloud. For more information, see [Configure End-user Portals on page 183](#).

# Compatibility

- [Compatible Fortinet applications on page 36](#)
- [Supported browsers on page 37](#)

## Compatible Fortinet applications

FortiToken Cloud 25.2.a works in tandem with the following Fortinet applications:

Fortinet Application	Application Version
FortiOS	<ul style="list-style-type: none"><li>• 7.0.0 or later</li><li>• 7.2.0 or later</li><li>• 7.6.0 or later</li></ul>
FortiClient for Windows	<ul style="list-style-type: none"><li>• 7.0.0 or later</li></ul>
FortiClient for MacOS	<ul style="list-style-type: none"><li>• 7.0.0 or later</li></ul>
FortiClient for Linux	<ul style="list-style-type: none"><li>• 7.0.0 or later</li></ul>
FortiAuthenticator	<ul style="list-style-type: none"><li>• 6.4.0 or later</li><li>• 6.5.0 or later</li></ul>
FortiSandbox	<ul style="list-style-type: none"><li>• 3.2.0 or later</li></ul>
FortiADC	<ul style="list-style-type: none"><li>• 7.1.3 or later</li><li>• 7.2.1 or later</li><li>• 7.4.0 or later</li><li>• 7.6.0 or later</li></ul>
FortiManager	<ul style="list-style-type: none"><li>• 7.2.2 or later</li><li>• 7.4.0 or later</li></ul>
FortiAnalyzer	<ul style="list-style-type: none"><li>• 7.2.2 or later</li><li>• 7.4.0 or later</li><li>• 7.6.0 or later</li></ul>
FortiPortal	<ul style="list-style-type: none"><li>• 7.0.0 or later</li></ul>
FortiPAM	<ul style="list-style-type: none"><li>• 1.2 or later</li><li>• 1.3.0 or later</li><li>• 1.4.0 or later</li></ul>
FortiToken Mobile for iOS	<ul style="list-style-type: none"><li>• 5.5.1 or later</li></ul>



Fortinet Application	Application Version
FortiToken Mobile for Android	<ul style="list-style-type: none"><li>• 5.4.1 or later</li></ul>
FortiToken Mobile for Windows	<ul style="list-style-type: none"><li>• 5.0 or later</li></ul>



- FortiToken Cloud does not work well with FortiOS 7.0.2. We recommend upgrading to FortiOS 7.0.5 or later for best performance.
- Using IPsec with FortiClient as a SAML application with FTC is not supported on FortiClient versions 7.2 and earlier.

## Supported browsers

FortiToken Cloud supports the latest versions of the following web browsers:

- Google Chrome
- Mozilla Firefox



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

# Important notes

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

- [Trial account API request limit on page 38](#)
- [Auth clients to applications on page 38](#)
- [The same token for the same user on multiple applications on page 39](#)
- [A single FTC user in multiple applications on page 39](#)
- [Admin accounts and realms on page 39](#)
- [Supported OTP hard tokens on page 40](#)
- [Supported FIDO security key on page 40](#)
- [No SMS MFA with FAC as LDAP server on page 40](#)
- [FAC users' name issues on FTC GUI on page 40](#)
- [How to use FortiClient on page 41](#)
- [Enabling/Disabling FTC end-users on FortiGate on page 44](#)
- [New public IP for FTC on page 44](#)
- [Account disablement and closure on page 45](#)

## Trial account API request limit

Starting from FTC 24.3.a release, FTC offers limited access to its REST APIs for its trial customers. Trial customers now can test out FTC's Web application APIs and IdP-related APIs for free as long as they abide by the following restrictions:

- Each trial account can make up to 60 API requests with a 5-minute period.
- Any request exceeding the aforementioned limit will be rejected. In such a case, the user will get a "429 Too Many Requests HTTP" error, along with the message "Trial request limit exceeded. Please retry after 5 minutes."
- Trial users who exceed 240 API requests within a 5-minute period risk having their accounts disabled altogether.

## Auth clients to applications

Starting with FortiToken Cloud 24.2.a release, "Auth Clients" in the main menu has been renamed to "Applications". As a result, all references to auth clients or Auth Clients have been changed to applications or Applications.

## The same token for the same user on multiple applications

FortiToken Cloud allows the same end-user created on two or more applications to use the same FortiToken Mobile (FTM) or FortiToken (FTK) token for its services, as long as:

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



The same end-user created on the applications can be of different usernames. For more detailed information, see [A single FTC user in multiple applications on page 39](#).

---

## A single FTC user in multiple applications

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

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

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

(2) Suppose you have enabled User-1 for FTC in FGT-1 and FGT-2, and User-1 has a token from FTC. You disable User-1 in FGT-1, but leave it still enabled in FGT-2 so that it still exists in FTC. Later on, if you enable User-1 again without assigning a new FTC token to it, User-1 will continue to use the same FTC token that it has used before. Now suppose, instead of enabling User-1 again in FGT-1, you assign SMS from FGT-1 (an FGT internal feature that is not available in FTC) as the MFA method for User-1. This is what is going to happen: If User-1 attempts to log into FGT-1, the user will get an SMS from FGT-1; but if User-1 attempts to log into FGT-2, the user will have to use the FTC token.



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

---

## Admin accounts and realms

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

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

For more information on how to create admin groups and grant permissions to sub-admins, see [Manage admin groups on page 110](#).

## Supported OTP hard tokens

FortiToken Cloud only supports FortiToken (FTK) FTK-200B and FTK-210 OTP hard tokens. The FTK-200CD tokens (with token serial number prefix FTK-211) are NOT supported.

## Supported FIDO security key

FortiToken 410 (FTK-410) is required for use with Passkey. For more information about FTK-410, visit [FortiToken 410](#).

## No SMS MFA with FAC as LDAP server

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

## FAC users' name issues on FTC GUI


Names of FTC end-users created on FortiAuthenticator (FAC) earlier than v.6.6.0 show up with prefixed and suffixed characters in corner brackets on the FTC GUI and in email notifications. This is because FAC differentiates the same username populated by multiple user sources to FAC. To remove the prefix and the suffix from a FAC username, select the FAC username and click the *Hide Full FAC username* button.

 Services ▼


 Support ▼

 New FTM Token

 Delete

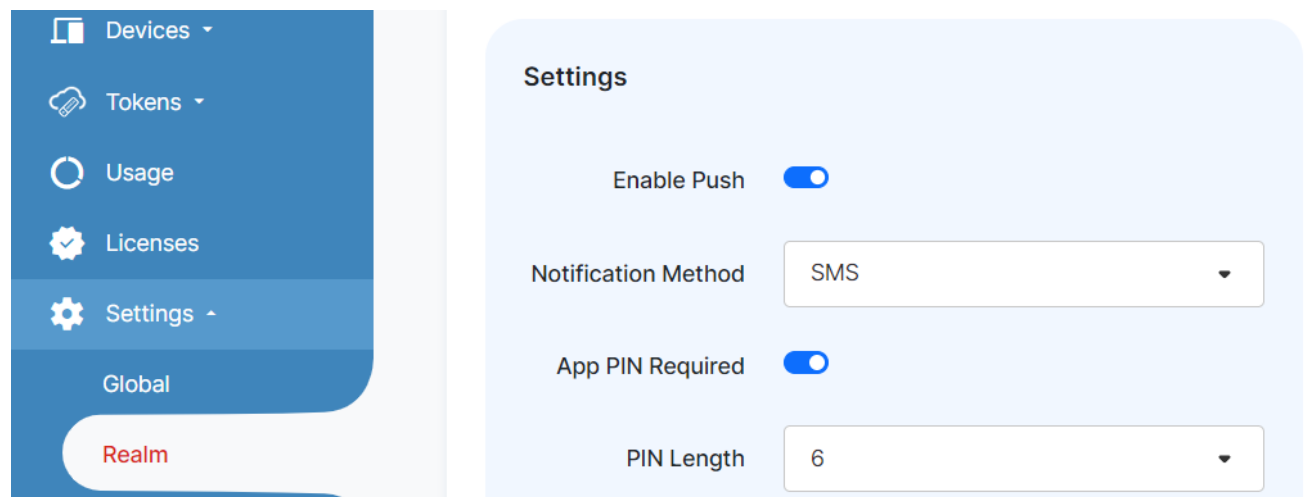
 Auto-assign FTK

 Add User Alias

 Hide Full FAC Username

## How to use FortiClient

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



## Use auto push

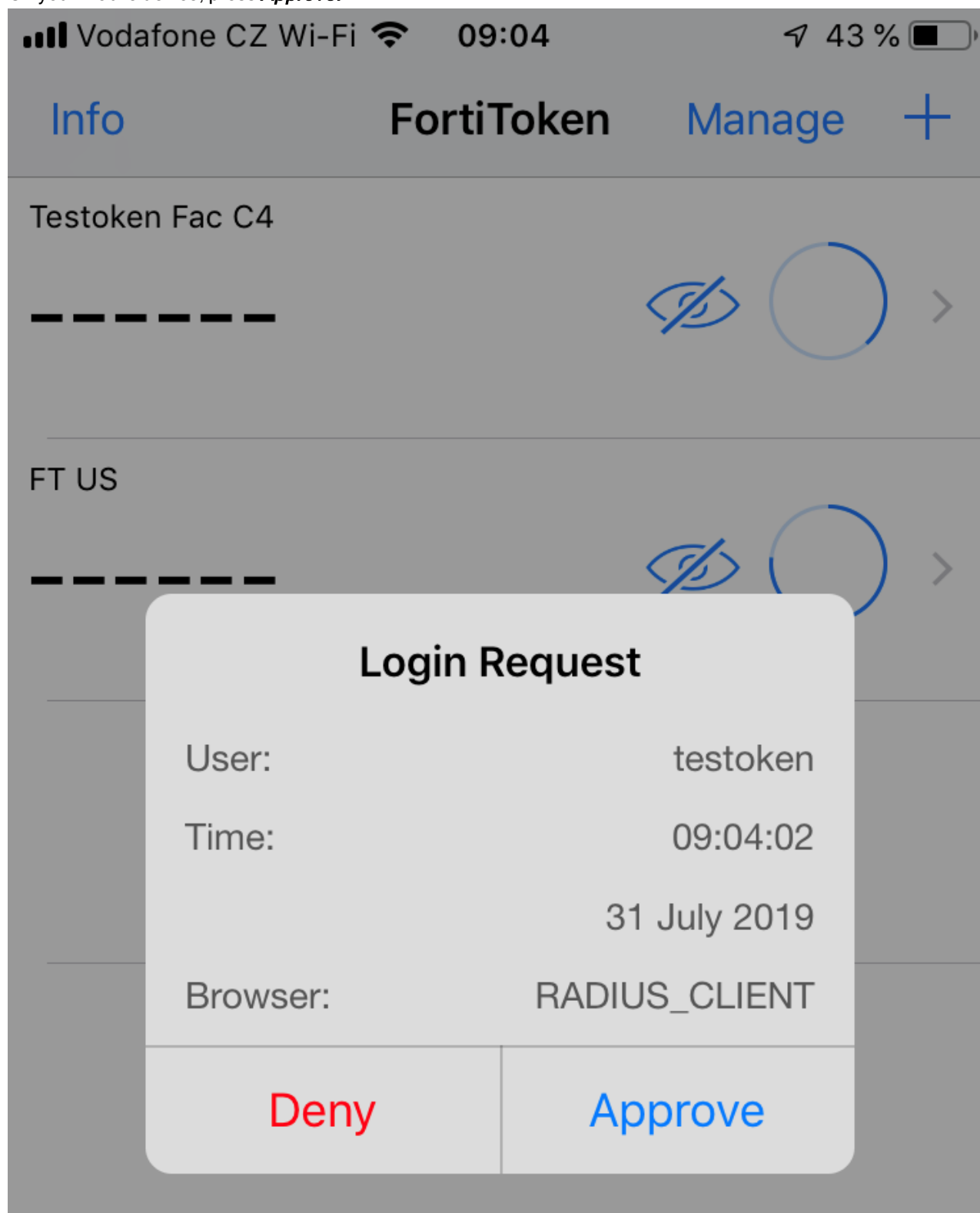
Upon entering your username and password, do the following:

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



VPN Name	<input type="text" value="test"/>	⌵	≡
Username	<input type="text" value="test_user"/>		
Password	<input type="password" value="....."/> ⦿		
<input type="button" value="Connect"/>			

2. On your mobile device, press **Approve**.

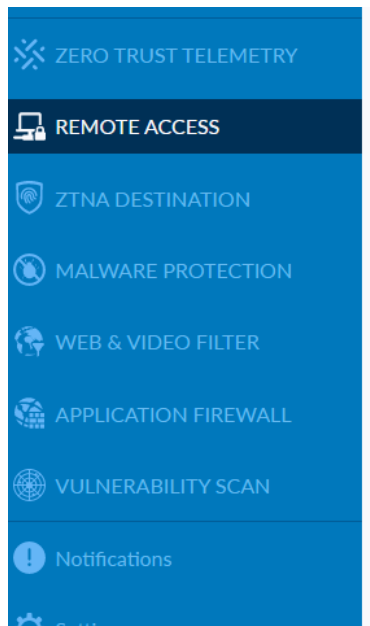


3. Wait for FortiClient to complete the remote access login.

## Use OTP

Upon entering your username and password, do the following:

1. In the Token window on FortiClient, enter the OTP obtained from your mobile device.



Enter token code or no code to send a notification to your FortiToken Mobile

VPN Name: US Sunnyvale (Backup Full Tunne)

Username: [Redacted]

Password: [Redacted]

Token: [Empty input field]

OK Cancel

2. Wait for FortiClient to complete the remote access login.

## Enabling/Disabling FTC end-users on FortiGate

If you have end-users with FortiToken Cloud for 2FA enabled on a FortiGate, they will remain on the FTC portal if you disable them on the FortiGate because FTC keeps a record of its end-users regardless of their status on FGT. If you want to remove the end-users from the FTC portal, you must do one of the following:

- Delete the end-users from the FGT.
- Revoke the tokens from the end-users.
- Delete the end-users from the FTC portal (**Note:** This method does not delete the end-users on the FGT, so it is best to delete them from the FGT.)

## New public IP for FTC

On September 7, 2024, the FortiToken Cloud primary data center will move to a new public IP address: 69.167.109.248. This is in place of 173.243.137.31. IP address 206.47.184.22 will remain unchanged.



If you have a firewall policy that manages traffic to [ftc.fortinet.com](https://ftc.fortinet.com), please ensure that this new public IP is allowed as a destination. Additionally, verify that connectivity from all subnets that require access to [ftc.fortinet.com](https://ftc.fortinet.com) is functioning properly.

To verify connectivity from a FortiOS device, you can run `execute ping`.



For more information about running ping from a FortiOS device, refer to [Running ping and traceroute](#) in the *FortiOS Administration Guide*.

---

If you need more assistance or clarification, please contact our support team. For more information on how to contact the support team, refer to [Technical support](#).

## 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 before it expires.

# 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 46.](#)
- [Activate FTM tokens on page 47.](#)
- [Activate third-party tokens on page 47.](#)
- [Use FTM tokens on page 47.](#)

## 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 5.4.3 and later	Apple iOS 12 and later	iPhone and iPad
FortiToken Mobile for Android 5.3.2 and later	Google Android 10 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. Search for **FortiToken Mobile**.
4. Download and install the app.

#### To get FTM for Android:

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

#### To get FTM for Windows:

1. Start your Windows device.
2. Go to **Microsoft Store**.
3. Search 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 via SMS or email depending on the option your system administrator has chosen.

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

The following guide can be referenced for more details about activating FTM tokens: [Activating FortiToken Mobile on a mobile phone](#).

## Activate third-party tokens

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

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

## Use FTM tokens

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

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

**To use an FTM token:**

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

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

For more information on FTM Push with CLI configuration for FortiGate, please refer to:

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/927108/fortitoken-mobile-push>.

# Use cases

- [One Token shared by different applications on page 49](#)
- [Change separate tokens to a single token on page 50](#)
- [Independent token on page 52](#)
- [Auto-Alias features—Use the same email address on page 53](#)
- [Split user quota to different realms on page 56](#)
- [FTC account lockout \(2FA\) on page 60](#)
- [Manage access to FTC on page 62](#)
- [Control risky conditions on page 65](#)
- [Migrate FTM tokens to FortiToken Cloud on page 255](#)
- [Synchronize LDAP remote users in wildcard user group from FortiGate on page 74](#)
- [Transfer devices on FTC on page 195](#)
- [ZTNA HTTPS access proxy with FTC MFA on page 77](#)
- [Add FTC MFA to remote access IPsec VPN on page 78](#)
- [Configure FTC as Microsoft Entra external authentication service provider on page 79](#)
- [Enable FortiSASE VPN users to use FTC MFA on page 85](#)
- [FortiToken Cloud as OIDC provider on page 87](#)

## One Token shared by different applications

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

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

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



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

---

1. Create a user “user1” in the application “client1”, which is assigned under the realm “realm1”. For more information on creating a user under application for FTC, refer to <https://docs.fortinet.com/document/fortitoken-cloud/latest/admin-guide/367002/add-a-local-user-for-ftc-service>.
2. Activate the token in the FortiToken Mobile.
3. Create a user with the same username “user1” in another application “client2”, which is also assigned under the same realm “realm1”. Note that if you are trying to assign the token on the FortiGate, there may be a warning message that says that you don’t have enough resources to add the new user. This is a false negative and you should still click “OK” after editing the user.
4. The activated token will also be assigned to the newly created user in “client2” which can use MFA login.

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

### Auth Client Count

1

2

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

Auth Client List for User: ttt

<input type="checkbox"/>	USERNAME	EMAIL	MOBILE NUMBER	NAME	SERIAL NUMBER	VDOM	CLUSTER ID
<input type="checkbox"/>	ttt	jgenie@fortinet.com	+1925-247-247	FSA5HF1C00000... 247-root	FSA5HF1C00000...	root	

Rows per page: 10

1-1 of 1

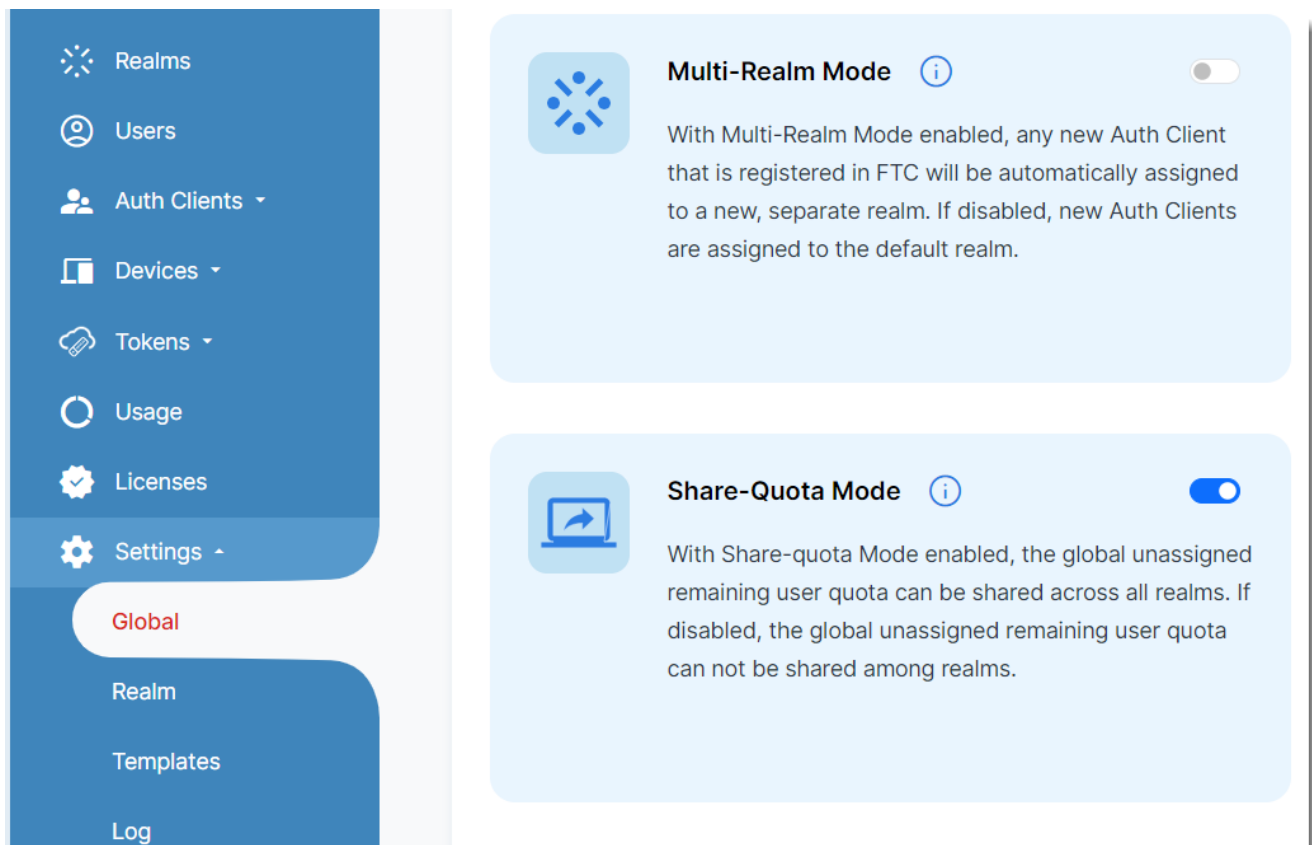
<< < > >>

Close

Remove Alias

## Change separate tokens to a single token

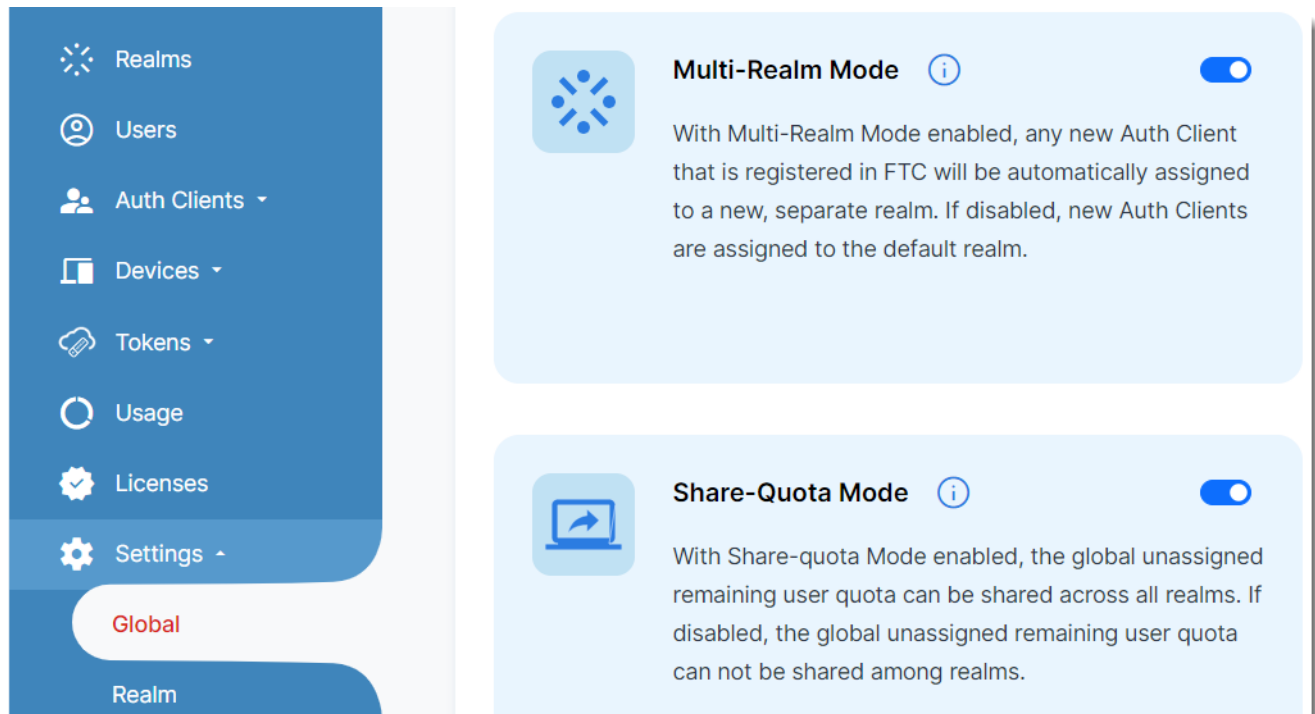
When you change the Multi-realm Mode from "enable" to "disable", your FTC will be changed so that the same user in different client applications (even with different usernames) will use the same token.



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

# Independent token

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



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

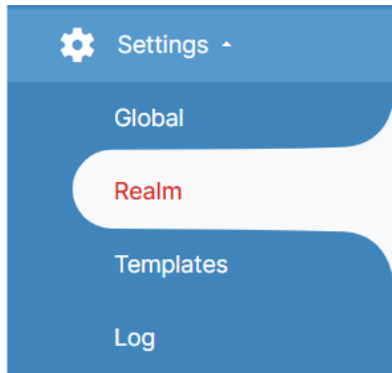


## Auto-Alias features—Use the same email address

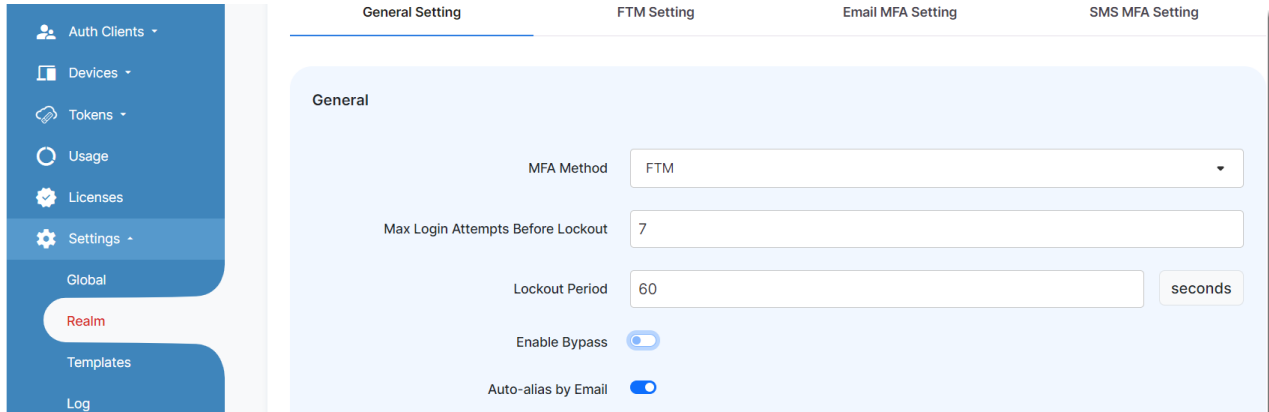
Many FTC end-users with the same email address have different usernames in different applications and different domains. For the same token, a single FTC user may have different usernames in different FTC applications. FTC allows for different usernames to be attributed to the same user (i.e., same person)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

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

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



2. Scroll down until you see the Auto-alias by Email option near the bottom of the page.
3. Click the Auto-alias by Email button to enable it.

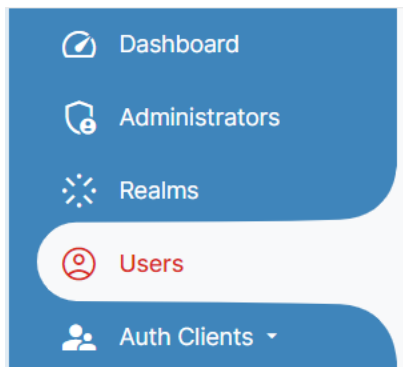


Once the Auto-alias by Email feature is enabled, all newly created usernames with the same email address are automatically set as an alias under the same username. The existing usernames with the same email address will not be grouped into an alias, but you can manually set up alias users. See [Manage users on page 115](#).

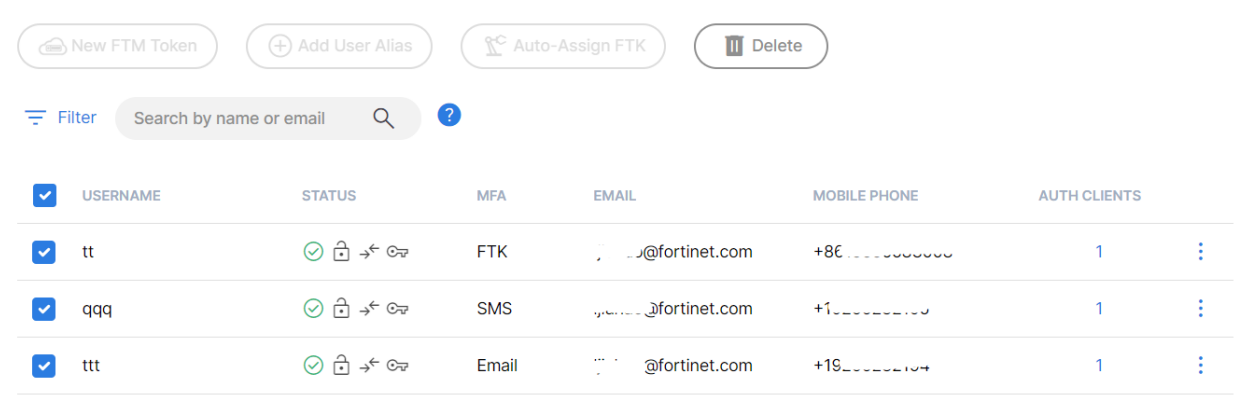
It is important to note that aliased users must be in the same realm. Usernames with the same email address are still set as unique users if they are in different realms, even when the auto-alias feature is enabled.

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

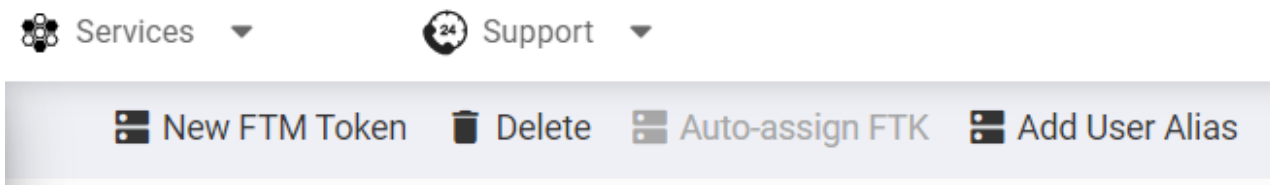
1. On the side menu, click Users to navigate to the Users page.



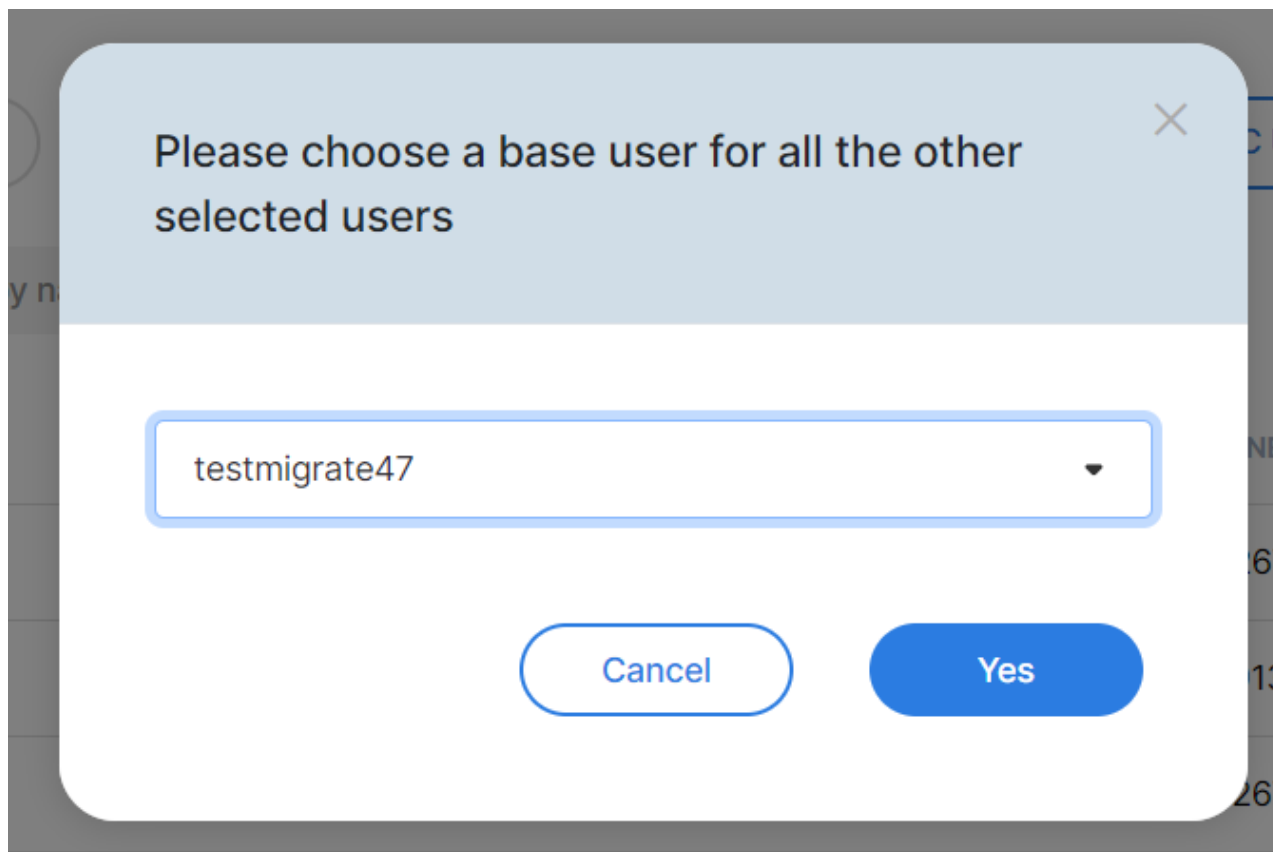
2. Select any number of users in the same realm by clicking the checkbox in the first column.



3. Click the Add User Alias button in the top bar which should be enabled if the users are in the same realm.



4. Select the base username which will be displayed in the Users page, and click Next>Confirm.



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

<input type="checkbox"/>	<b>testmigrate1</b>	   	Email	test@fortinet.com
--------------------------	---------------------	---	-------	-------------------

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

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

AUTH CLIENTS ▼

2

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

## Auth Client List for Use

☐

USERNAME

☐

testmigrate1

☒

testmigrate5

3. Click the Remove Alias button.

Rows per page: 10 1-2 of 2 |< < > >|

Close

Remove Alias

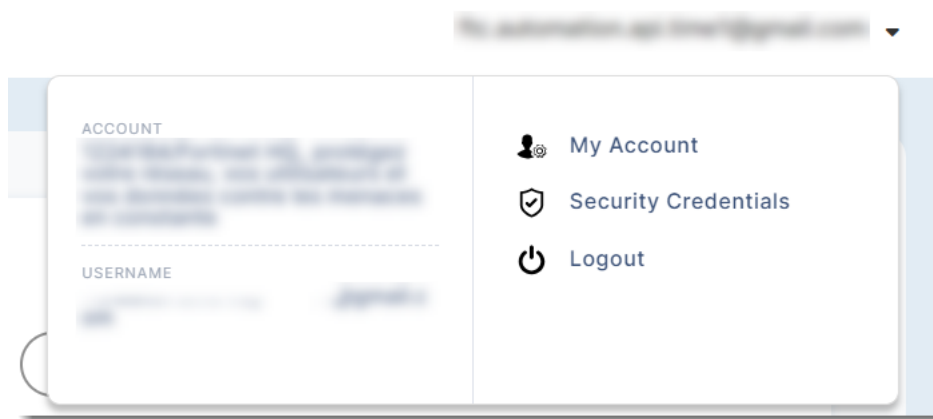
To remove the User Aliases that have the same email address, be sure to disable the Auto-Alias feature first in the Realm setting page. Once the auto-alias feature is disabled, the steps are the same as before.

## Split user quota to different realms

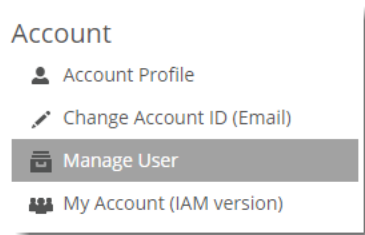
FortiToken Cloud enables you to split out user quota to sub-accounts. Sub-accounts can also use functions like MFA, bypass, block, and realm configuration. This is the so-called “Managed Security Service Provider” capability. The host account holder can create sub-accounts and assign a user quota to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

**To create a sub-account:**

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



3. The browser will be navigated to [support.fortinet.com](https://support.fortinet.com) automatically.
4. Click "Manage User" in the left sidebar to open the sub-users list.



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



6. Enter the sub-user client information, including "User Name", "Email (Account ID)", and "Telephone". Additionally, enter some details, such as "purchased 10 user quotas", in the Description field.
7. Select "Limit Access", which allows you (the host account holder) to assign specific devices to this sub-user, like a FortiGate for creating users.
8. Click **Save**.

Account

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

### Add User

#### User Information

User Name: \*
Telephone: \*

Email (Account ID): \*
Confirm Email (Account ID): \*

Description:

#### Permissions

☒ Customer Service  
☒ RMA/DOA  
☒ Technical Assistance  
☐ Notify the master account of ticket updates  
☒ Send renewal notices  
☒ Can create user  
☒ Full Access ☐ Limit Access

You are about to create a sub-account for Fortinet, Inc. By doing so, you agree to share visibility for this account, including ticket history and asset management, as per the settings that you have defined. You agree to assure that sharing visibility does not breach any confidentiality obligations or applicable data protection legislation.

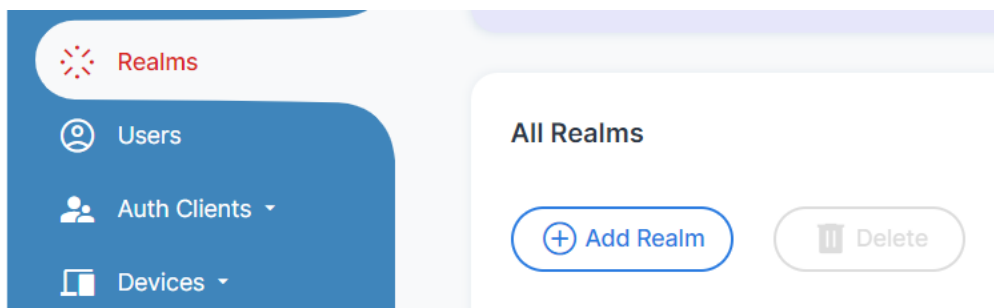
**Note:** If you have another account same email address, those accounts will be consolidated into one login account. Your original connection between email and accounts (master account or sub account) will be kept, you will use one login user ID/ password to access those accounts.

Save
Cancel

9. The sub-user clients will receive an email, asking them to create their own passwords for logging into [ftc.fortinet.com](https://ftc.fortinet.com).
10. After sub-users are created, the host account holder can assign resources to sub-users, including user quotas, realms, and applications. For more details of assigning resources, see [Manage admin groups on page 110](#).

The following steps show how to use this feature:

1. The host account holder creates a sub-user “subuser1” by using the provided client’s email. Clients can use their own email and password to log into [ftc.fortinet.com](https://ftc.fortinet.com), and can see the user quota assigned to them by the host account holder.
2. The host account holder can assign a user quota to a client in the Realms page.
  - a. Navigate to the Realms page, and click Add Realm to add a new realm.



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

<input checked="" type="checkbox"/>	jz_test	0	NA	Documentation	0	<a href="#">Edit</a>
<input type="checkbox"/>	FMGVMSTM22003726-FMG-FAZ	0	NA	generated by FortiToken Cloud when		<a href="#">Refresh Realm</a>
<input type="checkbox"/>	FGVMULTM21001705-13_27_1	0	NA	generated by FortiToken Cloud when		<a href="#">Show Permission</a>
<input type="checkbox"/>	FGVMULTM21001705-root	0	NA	generated by FortiToken Cloud when		<a href="#">Settings</a>
<input type="checkbox"/>	FAD3HFTA19000037-root	0	NA	generated by FortiToken Cloud when		<a href="#">Delete</a>

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

Edit Realm

Name

jz\_test

Description

Documentation

Allocated User Quota:

4010

Min Value: 0

Max Value: 7248

Cancel

Save

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

- a. Navigate to the Administrator page and click Add Admin Group.

Dashboard

Administrators

Realms

Users

Auth Clients

Administrators

+ Add Admin Group

Delete

Search

<input type="checkbox"/>	NAME	DESCRIPTION	LEVEL	MEMBER COUNT
<input type="checkbox"/>	global_admin	2222222	global_admin	2

- b. Edit the admin group by clicking the new group name.
- c. Assign to this group the sub-account in Admins in Group and the realm in Managed Realms which are created

in Step 2, and click Close.

4. The host account holder can assign application to the client by selecting applications>FortiProducts.
5. The client can see the users created by the host on the assigned FortiProduct, for example, FortiGate.

<input type="checkbox"/>	blah	FGVMULTM22003890-rootr	FortiGateVM	0	⋮
<input type="checkbox"/>	FGVMULTM22003890-rootr	FGVMULTM22003890-rootr	FortiGateVM	0	⋮
<input type="checkbox"/>	blah	FGVMULTM22003890-rootr	FortiGateVM	0	⋮

## FTC account lockout (2FA)

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

1. For example, Jack is an FTC admin and manages two FortiGates FGT1 and FGT2. He has enabled MFA for FGT admin login. When the FTC account is validated, everything is working fine.
2. By missing the disabled email notification sent by FTC, Jack's FTC account is disabled.
3. In this situation, the MFA login function is blocked. The behavior is that MFA login automatically fails after the user enters the correct username/password.
4. Jack can't log into the FGT admin portal to see users who are enabled for MFA login authentication.
5. Jack is allowed to log into his account and perform some limited activities, including enable bypass, setup bypass for users, and delete auth devices.
6. Log into the FTC portal, [ftc.fortinet.com](https://ftc.fortinet.com), navigate to Settings>Realm, find the Realm which contains the users for whom Jack wants to set up bypass, and click "Enable Bypass".



The screenshot shows the FortiToken Cloud administration interface. On the left is a blue sidebar with navigation links: Devices, Tokens, Usage, Licenses, Settings (selected), Global, Realm (selected), Templates, Log, Adaptive Auth, Alarm, Logs, Help, and Users (3). The main content area is titled 'General' and contains the following settings:

- MFA Method: FTM (dropdown)
- Max Login Attempts Before Lockout: 7 (text input)
- Lockout Period: 60 (text input) with a 'seconds' label
- Enable Bypass: ☒ (toggle)
- Bypass Expiration Time: 3600 (text input) with a 'seconds' label
- Auto-alias by Email: ☐ (toggle)
- Adaptive Auth Profile: -- None -- (dropdown)

An 'Apply Changes' button is located at the bottom right of the settings panel.

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

Edit User

Name

tt


Auth Method

FTK


Token SN

FTK\_-----





Email

 fortinet.com

Mobile Phone

 +86 138 0000 0000

Status

Created At

9/12/2023, 11:43:01 AM

Cancel

Apply

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

## Manage access to FTC

### Admin Group

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

**Edit Admin Group**

**Group Information**

Group Name: global\_admin

Group Description: 2222222

Group ID: 43c746bc-54e4-421a-b067-b9d3988ce633

Cancel Save

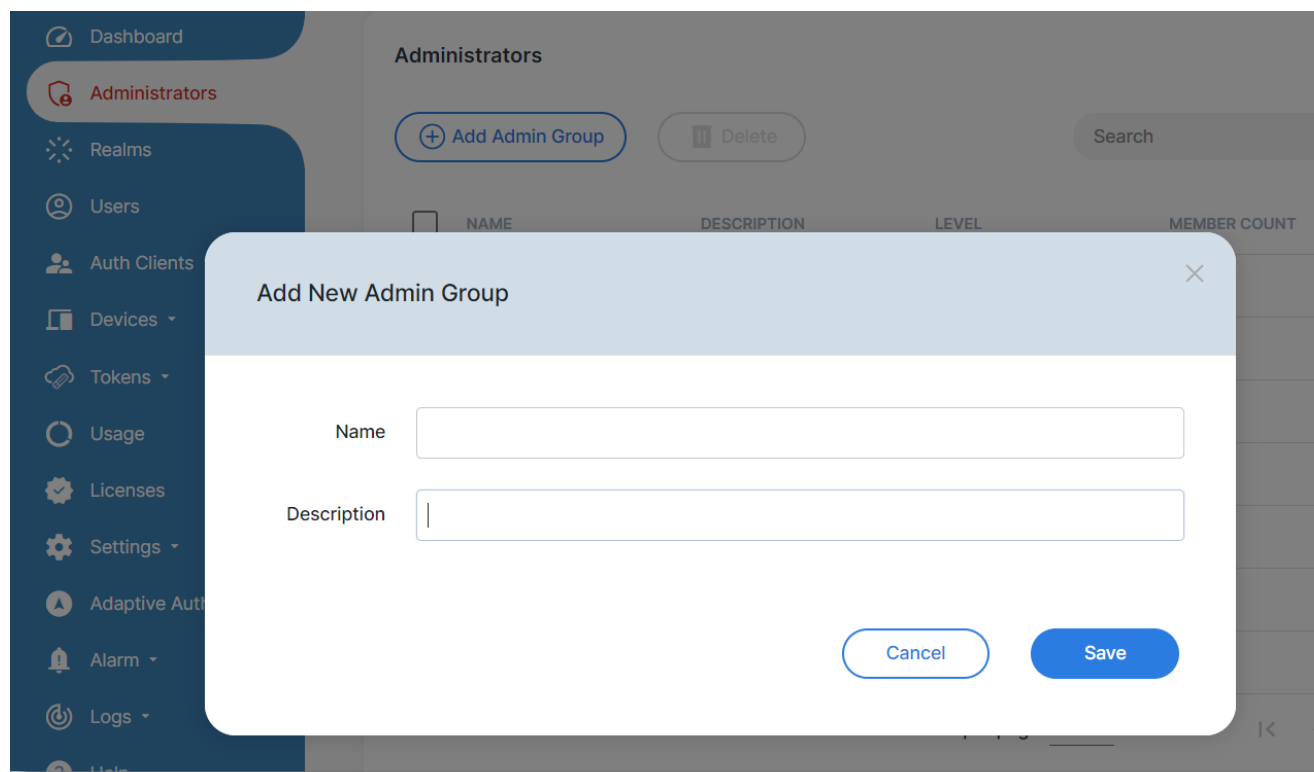
**Admins in Group** Manage Admin

NAME	EMAIL
Solutions QA	ftcmanualtest2@hotmail.com

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

## Add an admin group

On the Administrators page, click Add Admin Group to open the Add New Admin Group dialog.

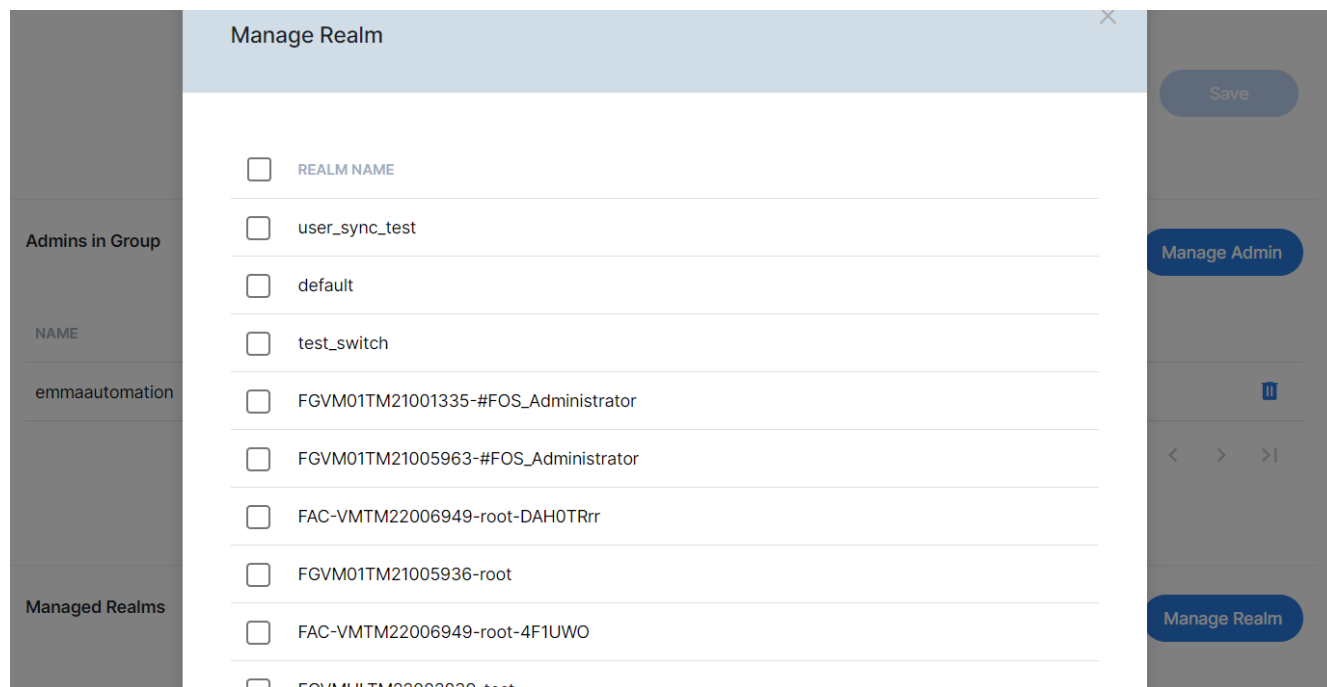


1. Specify the group name.
2. (Optional) Enter a brief description of the group.
3. Click OK.



The group name can only contain lower-case letters from "a" to "z" and/or numeric values from "0" to "9", and underscore "\_" and/or hyphen "-". It must be between 3 and 36 characters in length.

## Add realms to an admin group



1. Scroll down the Edit Admin Group dialog, and click Manage Realm to open the Manage Realm dialog.
2. Select the realm(s) of interest and click Apply.

## Control risky conditions

### Adaptive Authentication

You can bypass OTP verification of MFA under certain “safer” conditions and deny such attempts under some otherwise “risky” conditions. You can pre-configure OTP verification of MFA based on trusted subnet/geo-location and time of day/day of week. For more details about how to configure it, go to [Adaptive authentication on page 237](#).

## Create adaptive authentication policy

**Policies**

[+ Add Policy](#) [Delete](#)

<input type="checkbox"/>	NAME	ACTION	PROFILE REFERENCES	LAST UPDATE	
<input type="checkbox"/>	test5	Multi-factor Authentication	0	11/9/2023, 1:34:06 PM	⋮
<input type="checkbox"/>	tst1	Multi-factor Authentication	4	10/3/2022, 11:00:23 PM	⋮
<input type="checkbox"/>	test6	Multi-factor Authentication	1	9/12/2023, 1:46:38 PM	⋮
<input type="checkbox"/>	test99	Multi-factor Authentication	0	9/20/2023, 3:45:09 PM	⋮
<input type="checkbox"/>	test3	Multi-factor Authentication	0	9/11/2023, 3:05:05 PM	⋮
<input type="checkbox"/>	test1	Bypass	0	9/12/2023, 1:46:01 PM	⋮
<input type="checkbox"/>	test2	Multi-factor Authentication	0	9/12/2023, 9:54:49 AM	⋮
<input type="checkbox"/>	ddd	Multi-factor Authentication	0	9/23/2022, 9:51:55 AM	⋮

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

## Create adaptive authentication profile

**Profiles**

[+ Add Profile](#) [Delete](#)

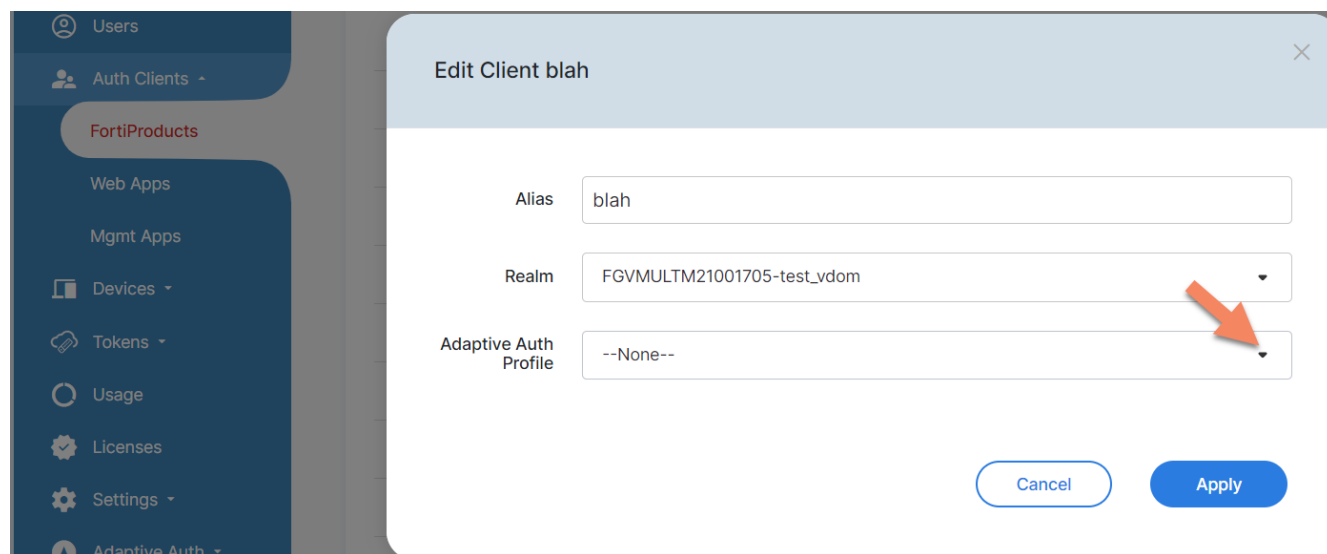
<input type="checkbox"/>	NAME	ACTION	REALM REFERENCES	CLIENT REFERENCES	
<input type="checkbox"/>	test1	Multi-factor Authentication	0	7	⋮
<input type="checkbox"/>	a	Multi-factor Authentication	0	2	⋮
<input type="checkbox"/>	a1	Multi-factor Authentication	0	0	⋮

Rows per page: 10 1-3 of 3 |< < > >|

1. Click Adaptive Auth > Profile to open the Profile page.
2. On top of the page, click Add Profile to open the Add New Profile dialog.

3. Make the entries and/or selections.
4. Click Save.

## Apply adaptive authentication profile to an application



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

## Apply adaptive authentication profile to a realm

The screenshot displays the 'Realm Settings' interface. On the left is a navigation menu with options: Dashboard, Administrators, Realms, Users, Auth Clients, Devices, Tokens, Usage, Licenses, Settings (selected), Global, Realm (highlighted), Templates, Log, Adaptive Auth, Alarm, and Logs. The main content area is titled 'Realm Settings' and shows a dropdown for the realm ID 'FGVMULTM21001705-test\_vdom 0a4fe6f9-fe71-4871-b1c8-57b0f141e7c6'. Below this are four tabs: 'General Setting' (active), 'FTM Setting', 'Email MFA Setting', and 'SMS MFA Setting'. The 'General' section contains several settings: 'MFA Method' set to 'FTM', 'Max Login Attempts Before Lockout' set to '7', 'Lockout Period' set to '60' seconds, 'Enable Bypass' toggleed on, 'Bypass Expiration Time' set to '3600' seconds, 'Auto-alias by Email' toggleed off, and 'Adaptive Auth Profile' set to '-- None --'. A red arrow points to the 'Adaptive Auth Profile' dropdown menu.

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

## Last login

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



### To enable the Last Login feature in Adaptive Authentication Policy:

Filters ☒ Subnet Filter ☐ Location Filter ☐ No Source Filter

Schedule ☒

**Subnet Filter** Please click [?](#) to check supported devices.

Subnets  [+](#)

No IP ☐

**Schedule**

All Days ☐

Days ☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Timezone

All day ☐

Start Time  [🕒](#)

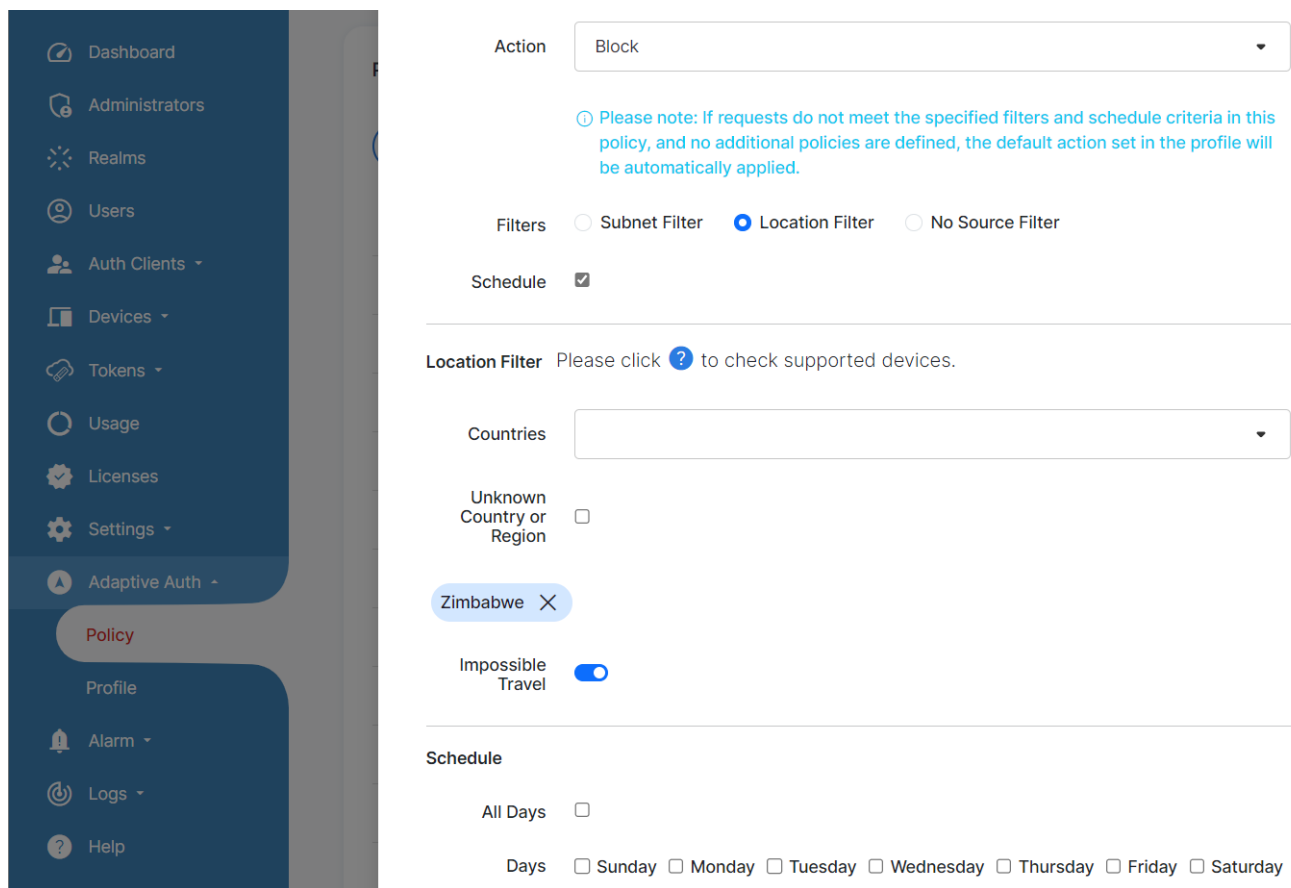
End Time  [🕒](#)

1. Add the new policy by click Add Policy in Adaptive Auth > Policy page.
2. Specify a unique name and select Bypass MFA in Action section, and select Subnet Filter.
3. Enter the IP or subset in Subnets section, and click Enter to confirm (Note: The IP or Subnet must be supported by the FortiProducts).
4. Click Last Login and specify a reasonable MFA Interval time period (Note: The range of this period is from 1 to 72 hours.)
5. Select a schedule configuration set in Schedule section
6. Click confirm.
7. Add the newly created policy to a profile and select the same action, i.e., Bypass MFA.
8. Apply the newly created profile to any applications (including FortiProducts and Web Apps) and any realms whose users are going to use those trusted IPs or Subnets.

## Impossible travel

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

### To enable the Impossible Travel feature in Adaptive Authentication Policy:



The screenshot shows the FortiGate Adaptive Authentication Policy configuration interface. On the left is a navigation menu with options: Dashboard, Administrators, Realms, Users, Auth Clients, Devices, Tokens, Usage, Licenses, Settings, Adaptive Auth, Policy (selected), Profile, Alarm, Logs, and Help. The main configuration area is divided into sections:

- Action:** A dropdown menu set to "Block".
- Filters:** Radio buttons for "Subnet Filter", "Location Filter" (selected), and "No Source Filter".
- Schedule:** A checkbox that is checked.
- Location Filter:** A section with a note: "Please click ? to check supported devices." It includes a "Countries" dropdown menu, an "Unknown Country or Region" checkbox (unchecked), and a tag for "Zimbabwe" with an "X" to remove it.
- Impossible Travel:** A toggle switch that is turned on (blue).
- Schedule:** A section with an "All Days" checkbox (unchecked) and a row of checkboxes for each day of the week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday (all unchecked).

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

## 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. An FTC account administrator can migrate FTM token to FTC from any FTC-supported FortiProducts. The following sections show to;

- Migrate FTM tokens from FortiGate on page 71
- Migrate FTM tokens from FortiAuthenticator on page 72

## Migrate FTM tokens from FortiGate

The FortiGate administrator can migrate FTM tokens to FTC themselves using the following command:

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

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



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

---

### Procedures

1. Ensure that the FTM license has already been imported into the FortiGate. (The Token serial number under the FTM license may or may not have been assigned to users.)
2. Submit a FTM migration request (using the command 'set FTM migration tag request') to Customer Support (<https://www.fortinet.com/support/contact>) by providing the FGT serial number and the FTM license serial number. The CS team then confirms the pre-authentication from the customer and sets up the 'FTM migration tag'.
3. Once the tag has been set up, run the `execute fortitoken-cloud migrate-ftm <FortiToken mobile license number> <vdom>` command on the FortiGate. The command will transfer all end-users with FTM token authentication under the FTM license to FTC authentication. You can find the FTM license number in the output of the `show user fortitoken` command, which has `set license <FTM license number>`.
4. The FTM tokens under the migrated license are then removed from the FGT GUI, and all end-users that have been migrated show up on the FTC GUI.
5. Once the migration CLI command is completed, user log-in authentication should work without any token data change.
6. Upon completion of the migration, FTC sends out email to CS asynchronously 24 hours. The email notifies CS to invalidate the FTM license and to 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 Licenses page of the FTC portal.
- The migrated MFA end-users show up on the Users page of the FTC portal.
- 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).



- Before starting the migration process, be sure to back up your FortiGate configuration .
- Once the FTM license and tokens are successfully migrated to FortiToken Cloud, they cannot be reversed.
- The original FTM license is invalidated once the migration is completed.
- FTM token migration requests can be initiated by an FGT administrator only.
- 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 end-users, be sure to set the FGT CLI Console timeout value long enough to cover the entire migration 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.

## Migrate FTM tokens from FortiAuthenticator

An FortiAuthenticator (FAC) administrator can migrate FTM tokens from FAC to FTC using the following command:  
`execute fortitoken-cloud ftm-migrate <FTM 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 are required to purchase an FTC license to continue using the service.

## Procedures

1. Ensure that the FTM license has already been imported into the FAC. (The Token serial number under the FTM license may or may not have been assigned to users.)
2. Submit an FTM migration request (using the command, `set ftm migration tag request`) to Customer Support (<https://www.fortinet.com/support/contact>) by providing your FAC serial number and 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 migration tag has been set up, run the `execute fortitoken-cloud ftm-migrate <FTM license number>` command on the FAC. The command transfers all end-users with FTM token authentication under the

FTM license to FTC authentication method. You can find the FTM license number in the output of the `show user fortitoken` command, which has `set license <FTM license number>`.

4. All the FTM tokens under the migrated license are then removed from the FAC GUI, and all end-users that have been migrated show up on the FTC GUI.
5. Once the migration CLI command is completed, user log-in 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 `request(set FTM migration tag 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 FAC portal:

- All end-users with FTM token auth under the migrated FTM license are updated to FortiToken Cloud on the FAC portal (Authentication>User Management).
- The migrated FTM license is removed from the FAC 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 Licenses page of the FTC portal.
- 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 log-in authentication process).



- Before starting the migration process, be sure to back up your FortiAuthenticator configuration.
- 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 FAC administrator.
- FTM token migration is supported for trial accounts.
- FTM token migration is not supported for credit-based accounts.
- Before migrating your FTM license with a large number of end-users, be sure to set the FAC CLI Console timeout value long enough to cover the entire migration process. If the Console times out while the migration is in progress, you can open another Console window and run the 'execute fortitoken-cloud ftm-migrate-status <FTM license number>' command to check the migration status.
- If for some reason you want to abort a migration operation that is in progress, you can do so using the command 'execute fortitoken-cloud ftm-migrate-abort <FTM license number>'

## Synchronize LDAP remote users in wildcard user group from FortiGate

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

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

### User case



This feature is supported on FortiGate devices running on FOS 7.4.5 or later, or FOS 7.6.0 or later.

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

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

```
FGVMULTM00000000 (root) # show user ldap
config user ldap
  edit <string>
    set server <ip address>
    set cnid <string>
```

```

set dn <string>
set type {Simple | Anonymous | Regular}
set two-factor <fortitoken-cloud>
set two-factor-filter <string>
set username <string>
set password <string>
next
end

```

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

```

FGVMULTM000000000 (root) # show user ldap
config user ldap
edit "ad-136"
set server "00.000.00.0"
set cnid "sAMAccountName"
set dn "DC=cloudsolutionsqa,DC=com"
set type regular
set two-factor fortitoken-cloud
set two-factor-filter "(&(objectClass=user)(memberOf=Cn=ftc-ops,ou=QA,dc=cloudsolutionsqa,dc=com))"
set username "ldapadmin"
set password *****
next
end

```

When a group filter is not used, all users in Active Directory with a valid email or mobile number will be retrieved; when a group filter is used, only users in that group will be filtered. In the example above, the group filter is `ftc-ops`.

For more syntax and diagnostic details, please check FortiOS Release Notes at [Administration Guide | FortiGate / FortiOS 7.0.7 | Fortinet Documentation Library](#).

## Transfer devices on FTC

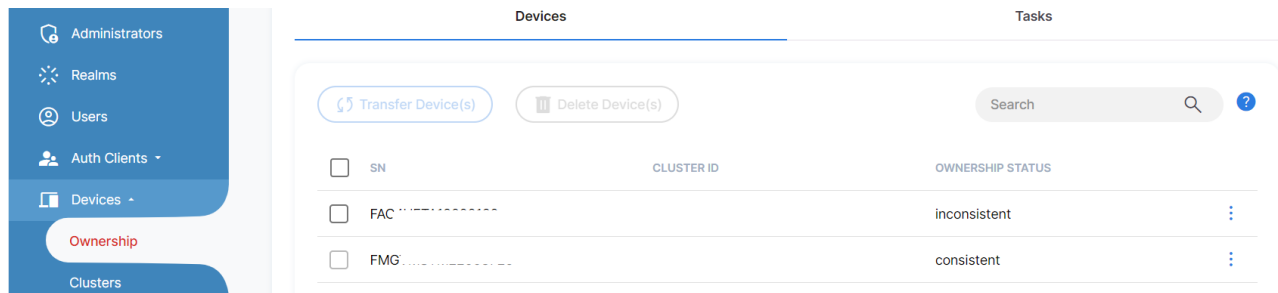
You can transfer devices from one FTC account to another using the FTC portal. While the transfer is being processed, your end-users should not notice any changes in their user experience with FTC. For example, if they have logged in through VPN, they can continue using VPN while the device is being transferred.



FortiToken Cloud approves device transfer requests automatically if the source account has been removed or merged into another account in FortiCare. We strongly recommend that you check and clear any sensitive user data off the device before removing it from the source account or merging it with another FortiCare account.

**To transfer a device with data:**

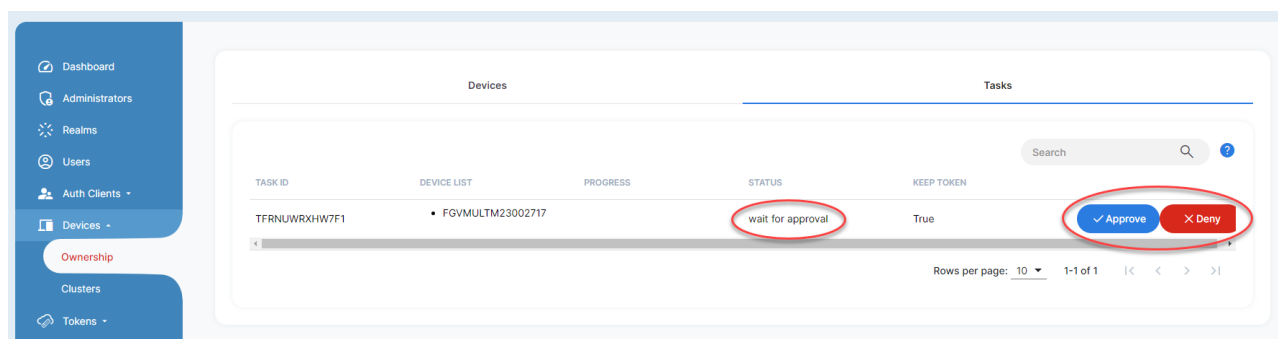
1. Submit a device ownership transfer ticket in FortiCare.
2. Wait until after the ticket is processed and the ownership is transferred to the new owner in FortiCare. For example, Account A is the original owner and Account B is the new owner.
3. Now the owner of either Account A or B can start the device transfer by selecting *applications>Devices (HA)>Manage Device Ownership>Devices*.
4. Locate the device (whose Ownership Status should be "Inconsistent").



5. On the right side of the row, click the three dots to open the menu, and then click *Transfer* to start transferring the device ownership.
6. If you are NOT the owner of the new account who has initiated the device ownership transfer, click *Devices (HA)>Ownership>Tasks*, locate the transfer task, and click "Approve".



- Device ownership transfer tasks are viewable by both parties involved in the transfer process.
- A device ownership transfer task cannot be initiated and approved by the same party. If you have initiated a device ownership transfer task, you must wait for the other party to approve it.



7. Wait until the *Progress* column shows "100%" and the *Status* column shows "Complete". By then, the ownership of the device should have been transferred to the new owner, and any old data left on the device should have been wiped out.





Transfer tasks will remain on the page for 24 hours and will be deleted automatically thereafter.

### To transfer a device without data:

If all data related to the old account has been removed from the device, FTC can automatically transfer the device ownership to the new owner. However, the device will not appear in the new account's *applications* or *Devices (HA)>Manage Device Ownership* pages of the FTC portal.

To establish a new connection between the FTC portal and the application (FortiGate for this case), you must log in to the FortiGate device and run the CLI command "execute fortitoken-cloud update".

## ZTNA HTTPS access proxy with FTC MFA

1. Configure a ZTNA HTTPS access proxy on FortiGate by following the instructions in [ZTNA HTTPS access proxy example](#).
2. Configure FTC MFA for end-users. If you use LDAPS to authenticate end-users on an internal Microsoft AD, you can set up FTC MFA by referring to the instructions in [ZTNA session-based form authentication](#).

# Add FTC MFA to remote access IPsec VPN

This use case shows how to add FTC multi-factor authentication (MFA) to a FortiClient dialup VPN configuration (see [FortiClient as dialup client](#)).

## Create users

### To create users from the GUI:

1. Select *User & Device > User Definition*.
2. Select *Create New*.
3. Select *Local User*, and click *Next*.
4. Name the user "test-ipsec".
5. Enable the *User Account Status*.
6. Enter a unique password for the user.
7. Enter the user's email address.
8. Enable two-factor Authentication, and set the *Authentication Type* to *FortiToken Cloud*.
9. Click *OK*.
10. Repeat Steps 1 through 9 to create another user named "testipsec2".

### To create users from the Console:

```
config user local
  edit "test-ipsec"
    set type password
    set passwd <user-password>
    set two-factor fortitoken-cloud
    set email-to <user@abc.com>
  next
end

config user local
  edit "testipsec2"
    set type password
    set passwd <user-password>
    set two-factor fortitoken-cloud
    set email-to <user@abc.com>
  next
end
```

## Create a user group

To create a user group from the GUI:

1. Select *User & Device > User Groups*.
2. Click *Create New*.
3. Name the user group "ipsecgrp".
4. Set *User Group Type* to *Firewall*.
5. Click the + sign (*Add*) in the Member box to add users "test-ipsec" and "testipsec2" to the user group.
6. Click *OK*.

To create a user group from the Console:

```
config user group
  edit "ipsecgrp"
    set member "test-ipsec" "testipsec2"
  next
end
```

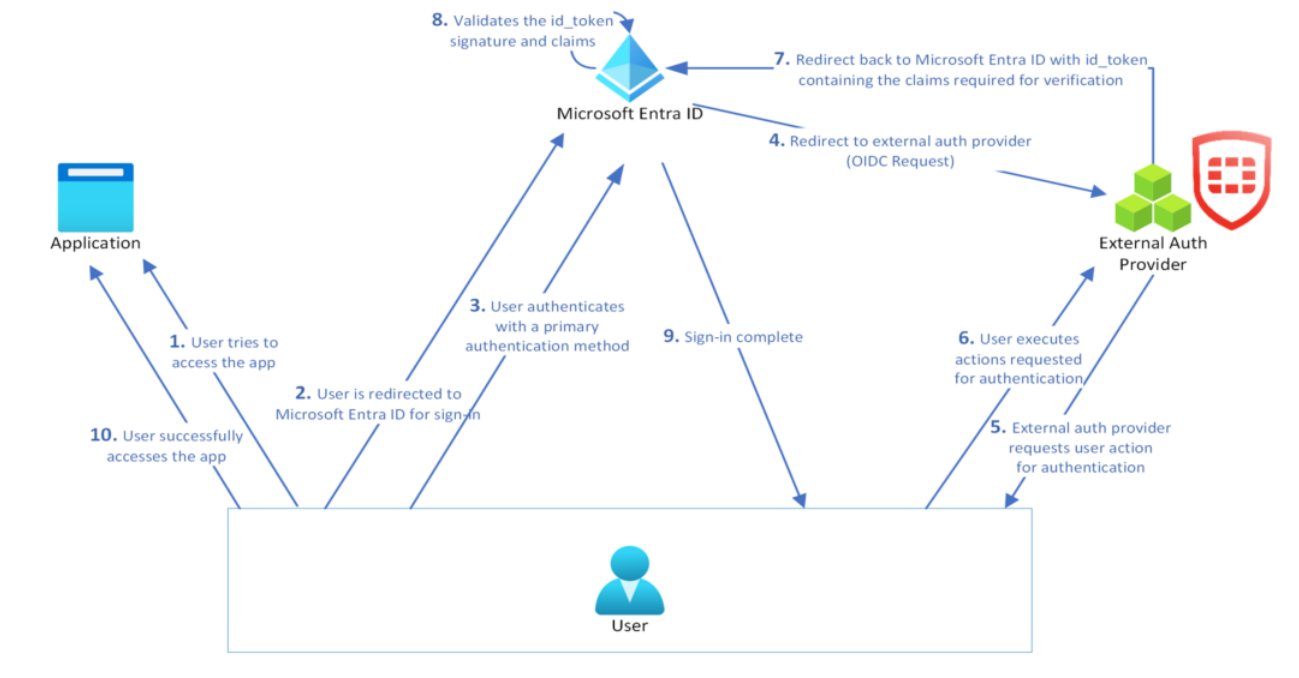
## Configure FTC as Microsoft Entra external authentication service provider

In May 2024, Microsoft introduced Entra ID external authentication method provider feature. An external authentication provider can integrate with Entra ID tenants as an external authentication method (EAM) provider, which can satisfy the second factor of the MFA requirement.

An EAM must be implemented on top of Open ID Connect (OIDC). This implementation requires at least three public facing endpoints:

- An OIDC discovery endpoint
- A valid OIDC authentication endpoint
- The public certificates of the EAM provider

The following diagram shows the network topology of the configuration:



### Step 1: Add FTC app on Entra admin center

Microsoft Entra admin center

Search resources, services, and docs (G+)

Home > App registrations >

## Register an application

**Name**

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Fortinet only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

By proceeding, you agree to the [Microsoft Platform Policies](#)

[Register](#)

1. Log onto Microsoft Entra admin center.
2. Select *Applications > App registrations*.
3. Enter a unique name for the app.
4. For Redirect URL (optional), select None. (**Note:** The redirect URL will be generated on the FTC portal later.)
5. Click *Register*.



Upon successful registration, you will receive the Application (client) ID that Microsoft generated. Be sure to save the Application (client) ID as you will need it later in the configuration.

## Step 2: Create the Microsoft app on FTC portal

Realm\* Select Realm

Interface\* OIDC (Azure)  
SAML 2.0  
OIDC (Azure)

Adaptive Auth Profile

Custom Branding ⓘ Default Branding

Default Permission Allow

Interface Detail ^

IdP Signing Cert ⓘ Default Certificate

IdP Metadata

Discovery Endpoint ⓘ https://

Authorization Endpoint ⓘ https://

RP Metadata

Audience ID ⓘ Azure OIDC requires an Audience ID to function

Redirect URI ⓘ https://login.

1. On the FTC portal, select *Applications > SSO Applications*.
2. Click *Add SSO Application*.
3. Name the Microsoft app.
4. For *Realm*, select the realm on which the end users of the Microsoft app reside.

5. For *Audience ID*, enter the Application (client) ID that you have saved on Microsoft Entra admin center.
6. For *Redirect URI*, enter the default Microsoft URI.
7. Make the other entries and/or selections on the page.
8. Click *Save* when done.



- Once the Microsoft app has been created, you will receive the FTC App ID, the discovery endpoint, and the authorization endpoint.
- If no Signing Cert is provided, the application will use the default certificate for authentication.

### Step 3: Update the FTC app on Entra admin center

The screenshot shows the Microsoft Entra admin center interface. The breadcrumb navigation is: [Conditional Access | Overview](#) > [Policies](#) > [ftc](#) > [Conditional Access | Overview](#) > [Policies](#) > [ftc](#) > [App registrations](#) > [eam\\_sp](#). The left sidebar shows the 'Overview' tab selected. The main content area displays the 'Essentials' section for the application 'eam\_sp'. The 'Client credentials' section is circled in red, showing '1 certificate, 0 secret'. Other visible fields include Display name, Application (client) ID, Object ID, Directory (tenant) ID, Supported account types, Redirect URIs, Application ID URI, and Managed application in local directory.

1. On Microsoft Entra admin center, select *Applications* > *App registrations* > *All Applications*.
2. Locate the FTC app, click to open it, and make the desired updates to its Client credentials and redirect URI.
3. To add client credentials, go to *Certificates* and upload the public key downloaded from the FTC portal.
4. To add redirect URI, go to Redirect URI, click *Add a platform*, choose Web Applications, and enter the authorization endpoint generated from the FTC portal.

## Step 4: Register FTC as Entra MFA external method provider

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > App registrations > token2-user | Authentication > Authentication methods | Policies >

### Add external method (Preview)

Authentication Methods

#### Method Properties

Your provider will give you the name, client ID, discovery endpoint, and app ID for the external authentication method.

Name \*

*The name cannot be changed once this method is saved.*

Client ID \*

Discovery Endpoint \*

App ID \*

Request admin consent

#### Enable and target

Enable ☐ Off

1. On Microsoft Entra admin center, select *Protection* -> *Authentication methods* -> *Policies* -> *Add external method (Preview)*.
2. For Client ID, enter the Application ID generated from the FTC portal.
3. For Discovery Endpoint, enter the discovery endpoint generated from FTC portal.
4. For App ID, enter the Application (client) ID generated from Microsoft.
5. Upon securing the permission, enable *Enable and target*.



- Up to this point, FTC should have been successfully set up as the EMA. With this configuration, all apps in your Microsoft account will use FTC for MFA.
- If you prefer using MFA methods other than FTC for your different Microsoft apps, you can take advantage of Microsoft's custom authentication strengths feature. For more information, visit <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strength-advanced-options>. Keep in mind that "Password + Software AUTH token" is the MFA setting that you should pick when configuring custom authentication strength in Microsoft that corresponds to the type of MFA that Microsoft considers FTC to be in this case.

## Step 5: Set Conditional Access policy to assign users to EMA

The screenshot shows the Microsoft Entra admin center interface. The left navigation pane is expanded to 'Protection' > 'Conditional Access'. The main pane shows the configuration for a Conditional Access policy named 'ftc'. The 'Assignments' section is highlighted with a red circle, showing 'Users' with 'Specific users included' selected. The 'Access controls' section is also highlighted with a red circle, showing 'Grant' with '1 control selected'. The right pane, titled 'Grant', shows the 'Grant access' radio button selected, with 'Require multifactor authentication' checked. Other options like 'Require authentication strength', 'Require device to be marked as compliant', 'Require Microsoft Entra hybrid joined device', and 'Require approved client' are unchecked. A warning message states: '"Require authentication strength" cannot be used with "Require multifactor authentication"'. At the bottom, the 'Enable policy' toggle is set to 'On'.

1. Select *Protection* -> *Conditional Access* -> *Policies*.
2. Create a new policy and assign users to Target resources: Select Cloud apps and then select the FTC application that you have created.
3. For Access Controls, select *Grant access* > *Require multifactor authentication*.
4. Set *Enable policy* to *On*.



Make sure to create a new user in FTC with the same username as the preferred username for the target user on Microsoft Entra admin center for identification.



# Enable FortiSASE VPN users to use FTC MFA

## Scenario

This use case presents a scenario in which a customer has both FortiSASE and FortiToken Cloud in their network ecosystem. They would like end users in their Google user base to be able to log into VPN through SSO. They also would like to control their end users MFA with FTC when they are logging into VPN using FortiSASE VPN with FortiClient configuration.

Enabling FortiSASE VPN users to use FortiToken Cloud for MFA involving configurations on both FortiToken Cloud and FortiSASE, as discussed in the following sections.

## Configuration On FTC:

### Step 1: Set up the authentication user source from Google.

1. Create a realm. See [Manage realms](#).
2. Navigate to Authentication and choose the realm created above and create an Authentication source.
3. Provide your Google SAML app details for the Identity Provider (IdP).
4. In your google SAML app, make sure that this FTC authentication source is configured as the SP.

### Step 2: Set up the SSO application

1. Navigate to *Applications > SSO Applications > Create a new SSO Application*.
2. Make sure that the application is in the same realm where the end users reside.
3. For *SP Metadata*, provide the metadata from the FortiSASE VPN User SSO configuration file.
4. For *Authentication > User Source*, select the Google authentication source configured in Step 1.
5. (Optional), if you want to let your end users change their MFA methods, do the following:
  - Select *Settings > Realm* and choose your realm from the drop-down list.
  - For *Allow Additional MFA Methods*, select the alternative MFA methods that you would like the end users to use.

### Step 3: Enable End-user Portals

FTC offers the *End-user Portals* function which the administrators can enable or disable from the FTC portal. Once enabled, the feature gives the end users the freedom to use MFA methods other than the one configured on the realm, and make changes or updates to their profiles according to the permissions granted by their administrator.

1. Navigate to *Applications > End-user Portals > Add User Portal* to create end-user portals.
2. For Realm, be sure to select the same realm which was used in Steps 1 through 2 above.
3. Create a custom branding theme, if you like.
4. Click *Save*.

# Configuration on FortiSASE

## Step 1: Configure the FTC SSO application as IdP for FortiSASE VPN user SSO

1. On the FortiSASE portal, select *VPN User SSO* to configure a VPN user SSO.
2. For *Identity Provider Configuration*, make the required entries or selections as highlighted in the following screen shot.

portal.prod.fortisase.com/ui-pro/configuration/user/saml-server

FortiSASE Services

VPN USER SINGLE SIGN ON (SSO)

Service Provider Configuration

Portal (Sign On) URL <https://turbo-rzichjd9.edge.prod.fortisase.com/i>

Identity Provider Configuration

IdP Entity ID <https://auth.fortinet.com/saml/>

IdP Single Sign-On URL <https://auth.fortinet.com/saml/>

IdP Single Log-Out URL <https://auth.fortinet.com/saml/>

SAML Claims Mapping

Username username

Group Name group

IdP Certificate [REMOTE\\_Cert\\_1](#)

Service Provider Certificate [FortiSASE Default Certificate](#)

Digest Method SHA-256

[Onboard Users](#)

Create a [User Group](#) in FortiSASE to map to any user group that exists on your remote authentication source. User Groups can be used within Policies to explicitly allow or deny traffic for subsets of users.

Test SSO Configuration

SSO configuration can be tested end-to-end by logging into a user account configured on your SSO server. The test will time out if FortiSASE does not get a successful login response from your IdP within a minute. Navigating to another page will cancel the test.

[Start Test](#)

Useful Links

[Single Sign On Configuration](#)

[FortiSASE with Okta](#)

Back Submit Delete

3. Click *Submit*.
4. Then, click the *Onboard Users* button on the right (highlighted above) to help the end users to download and install FortiClient on their devices.



You can let your end users to download FortiClient using any of the following options (highlighted in the following screen shot):

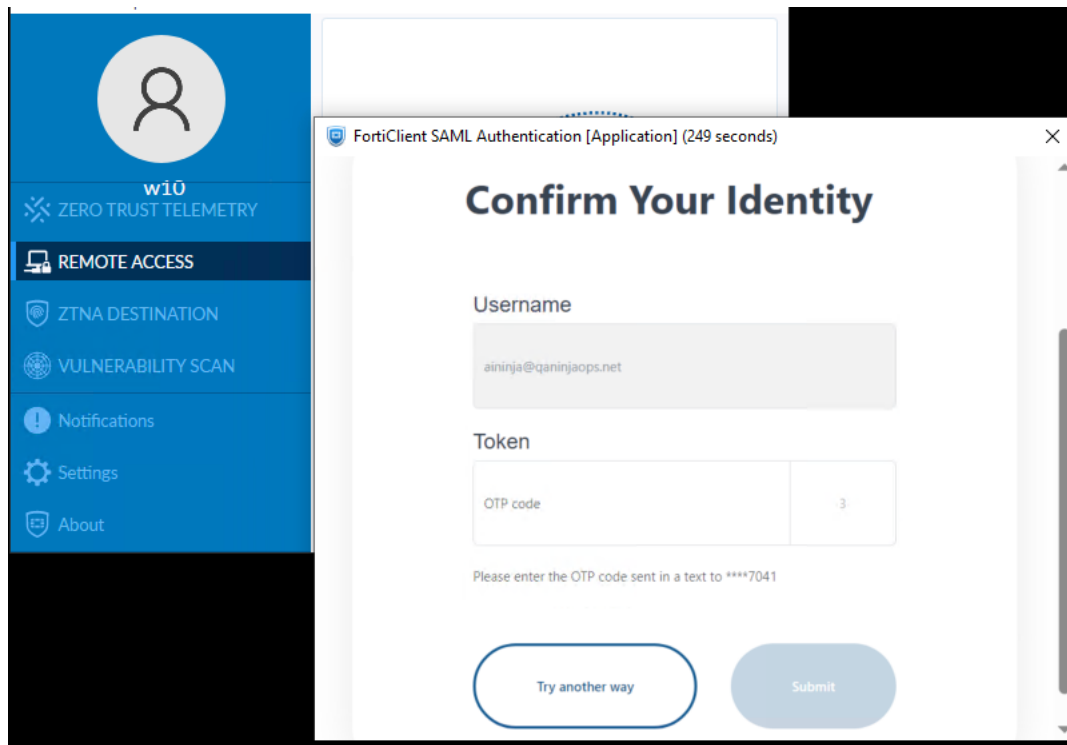
- Download installer
- Send link to users
- Send Invitation code

Refer to FortiSASE documentation for instructions on how to use each of these options.

5. Click *Close* when done.

## FortiSASE VPN end-user SSO experience with FTC MFA

Upon successful installation of FortiClient, the users can access the VPN server anytime from FortiClient. Each time, their requests will trigger FTC authentication with the default MFA method set by the administrator.



If you (the FTC admin) have enabled the End-user Portals function on FTC for the end-users (as mentioned earlier in Configurations on FTC), they will have the ability to access their own FTC end-user portal where they can change or update their mobile phone numbers, MFA methods, and so on based on the permissions that you have granted them. For more information, see [Manage end-user portals](#).

## FortiToken Cloud as OIDC provider

Starting from its 25.2.a release, FortiToken Cloud (FTC) can be configured as an OpenID Provider (OP) for authenticating users and issuing tokens to a Relying Party (RP). When configured in tandem with its local IdP, FTC can be the authentication source as well and provide end-to-end OP functionality.

Keep in mind that Local IdP is only a beta feature in FTC 25.2.a release and must be enabled by an FTC admin. For instructions on how to enable Local IdP, see [Enable local IDP beta feature](#).

You may also configure other third-party IdP providers as authentication user sources based on the your environment. For configurations supported by FTC as OIDC OP, refer to the `./well-known/opened-configuration` generated by FTC once the configuration is complete.



While Implicit grant type is supported, we do not recommend using it unless there is no other alternative for your application.

## Configure FTC as an OIDC provider

In the following example, we demonstrate the steps to configure FTC as an OIDC OP and a test on-prem grafana setup as RP. We also use FTC Local IdP as the user source for the first factor authentication.

1. Navigate to Applications > SSO. Click Add SSO Application.
2. Make sure to choose Interface as OIDC and provide the other necessary details as in the following sample.

The screenshot shows the 'Create' page for a new SSO application in the FortiToken Cloud interface. The left sidebar contains navigation links: Dashboard, User Management, Applications, FortiProducts, Web, Management, SCIM, SSO (selected), End-User Portals, Authentication, Security Devices, Log and Report, Customization, Settings, Licenses, and Help. The main content area is titled 'Applications > SSO > Create' and has four tabs: General Information, Interface Detail, Authentication, and Attribute Mapping. The 'General Information' tab is active, showing the following fields:

- Name\*: ftc-op
- Logo URL: (empty)
- Display Logo: F
- Realm\*: OIDC-OP
- Interface\*: OIDC
- Adaptive Auth Profile: Select Profile
- Custom Branding: Default Branding
- Session Timeout: 15 minutes
- Login URL: (empty)
- Default Permission: Allow
- Login Hint: (empty)

At the bottom right of the form are 'Cancel' and 'Next' buttons.

3. Click Next.

In the Interface Detail tab, the IdP metadata will be generated by FTC and will be displayed as in the following screenshot.



For the Redirect URI, ensure to provide a valid Redirect URI as documented by your RP. In this sample we use an on-prem grafana setup and the redirect URI provided by grafana is `https://<grafana ip>:<grafana port>/login/generic_oauth`. Make sure to click the '+' button to have the redirect URI added.

The screenshot shows the 'Interface Detail' tab of the SSO application configuration. It displays the generated IdP metadata and the RP metadata. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Applications > SSO > Create' and has four tabs: General Information, Interface Detail (selected), Authentication, and Attribute Mapping. The 'Interface Detail' tab shows the following metadata:

- IdP Metadata:**
  - Issuer: https://auth.fortinet.com/oidc/
  - Discovery Endpoint: https://auth.fortinet.com/oidc/.well-known/openid-configuration
  - Authorization Endpoint: https://auth.fortinet.com/oidc/authorize/
  - UserInfo Endpoint: https://auth.fortinet.com/oidc/userinfo/
  - Token Endpoint: https://auth.fortinet.com/oidc/token/
- RP Metadata:**
  - Redirect URI: (empty)

At the bottom right of the form are 'Back' and 'Next' buttons.

4. Click Next, and choose an appropriate user source under Authentication>User Sources.

In this example, we use a Local IdP source which is a beta feature to demonstrate the capability for FTC to act as an OIDC provider along with local user source.

The screenshot shows the 'Create' page for SSO in the FortiToken Cloud interface. The left sidebar contains a navigation menu with options like Dashboard, User Management, Applications, FortiProducts, Web, Management, SCIM, SSO (selected), End-User Portals, Authentication, Security Devices, Log and Report, Customization, and Settings. The main content area is titled 'Applications > SSO > Create' and has four tabs: General Information, Interface Detail, Authentication (active), and Attribute Mapping. In the Authentication tab, there is a 'User Source' dropdown menu with a plus icon, and a 'Default User Source' field with a plus icon. A dropdown menu is open for 'User Source', showing 'Select User Source' and 'LocalIDP'. At the bottom right of the form are 'Back' and 'Next' buttons.

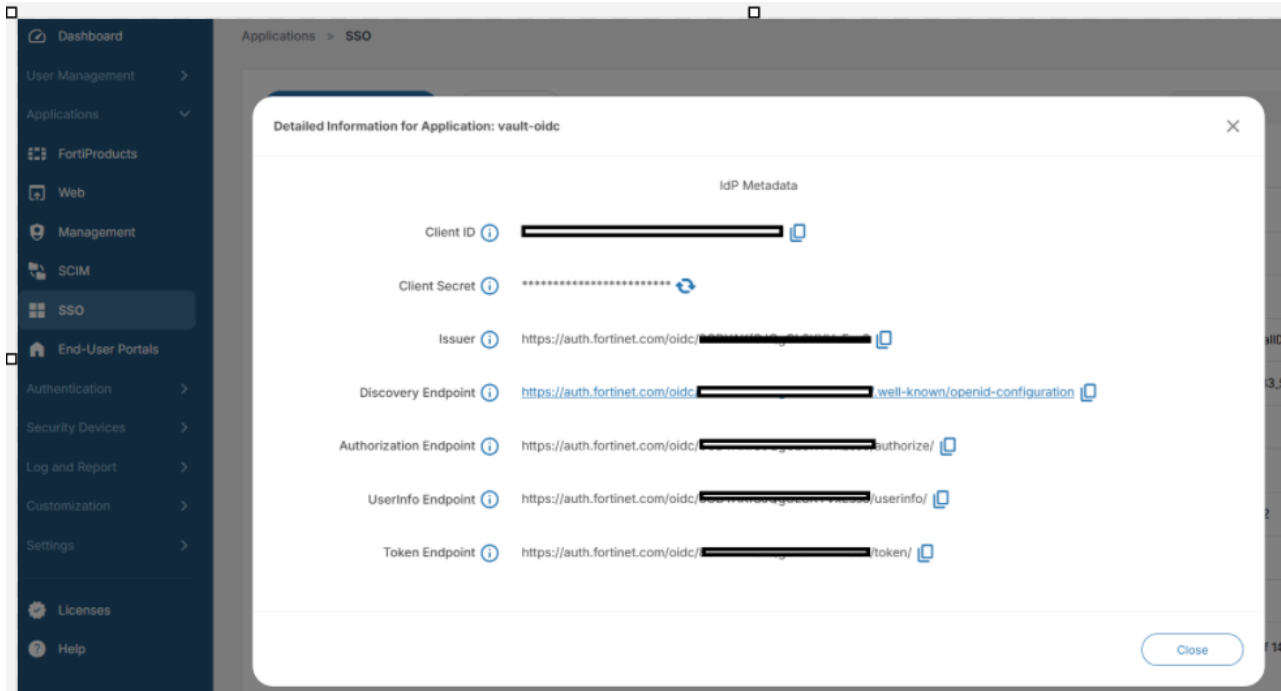
5. Click *Next*.

6. Add any attribute mapping that might be needed by the RP, and click *Save*.

The screenshot shows the 'Interface Detail' tab of the 'Create' page. It contains two sections: 'IdP Metadata' and 'RP Metadata'. The 'IdP Metadata' section has several fields: 'Client Secret' (with a copy icon), 'Issuer' (https://auth.fortinet.com/oidc/), 'Discovery Endpoint' (https://auth.fortinet.com/oidc/...well-known/openid-configuration), 'Authorization Endpoint' (https://auth.fortinet.com/oidc/.../authorize/), 'UserInfo Endpoint' (https://auth.fortinet.com/oidc/.../userinfo/), and 'Token Endpoint' (https://auth.fortinet.com/oidc/.../token/). Each field has a copy icon. The 'RP Metadata' section has a 'Redirect URI' field with a plus icon. Below the field, there is a text box containing 'https://...login/generic\_oauth' and a close icon. At the bottom right is an 'Acknowledge' button.

7. Copy the client Secret as it will be visible only once, and click *Acknowledge*.

8. Once the configuration is completed, click the tools pop-up menu (three vertical dots) at the right of the row, and click *Details* to view all the required IdP metadata.



9. On your RP, furnish the IdP metadata from FTC as shown in the above screenshot.

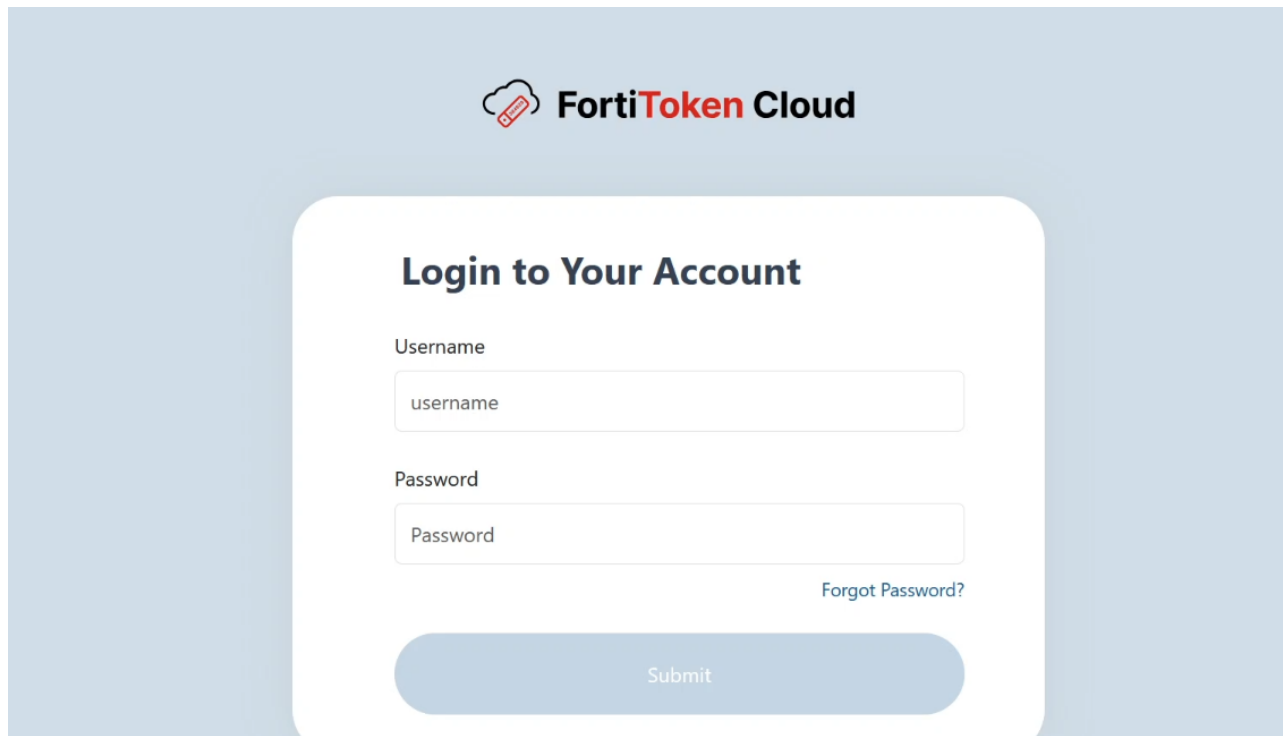
The following sample shows the configuration done for this test of on-prem grafana setup acting as RP.

```
- name: GF_AUTH_GENERIC_OAUTH_ENABLED
  value: "true"
- name: GF_AUTH_GENERIC_OAUTH_NAME
  value: OIDC
- name: GF_AUTH_GENERIC_OAUTH_CLIENT_ID
  value: [Redacted]
- name: GF_AUTH_GENERIC_OAUTH_CLIENT_SECRET
  value: J[Redacted]
- name: GF_AUTH_GENERIC_OAUTH_AUTH_URL
  value: https://auth.fortinet.com/oidc/[Redacted]/authorize/
- name: GF_AUTH_GENERIC_OAUTH_TOKEN_URL
  value: https://auth.fortinet.com/oidc/[Redacted]/token/
- name: GF_AUTH_GENERIC_OAUTH_SCOPES
  value: openid profile email
- name: GF_AUTH_GENERIC_OAUTH_USE_PKCE
  value: "true"
- name: GF_AUTH_GENERIC_OAUTH_USE_REFRESH_TOKEN
  value: "true"
- name: GF_AUTH_GENERIC_OAUTH_DISCOVERY_URL
  value: https://auth.fortinet.com/oidc/[Redacted]/.well-known/openid-configuration
```

10. Click User Management>Users, and create users in your realm to facilitate login.  
11. Make sure that the user type is Local User for the first factor authentication to be performed by FTC.

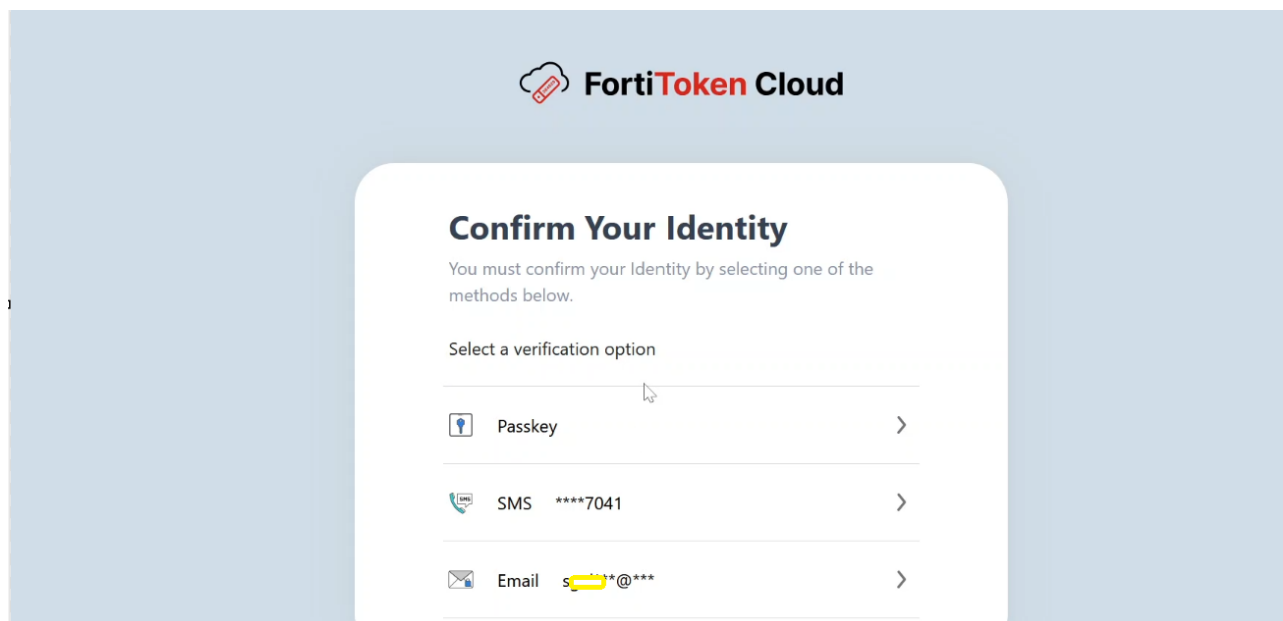
## End-user experience

- In the RP (on-prem grafana in this case), select Sign in with OIDC.  
With Local IdP beta feature enabled for this account and Local IdP configured as the user source, FTC will perform the first factor authentication.
- Observe the user gets navigated to FTC's `auth.fortinet.com` page. Enter the username and password configured on the FTC for the user.

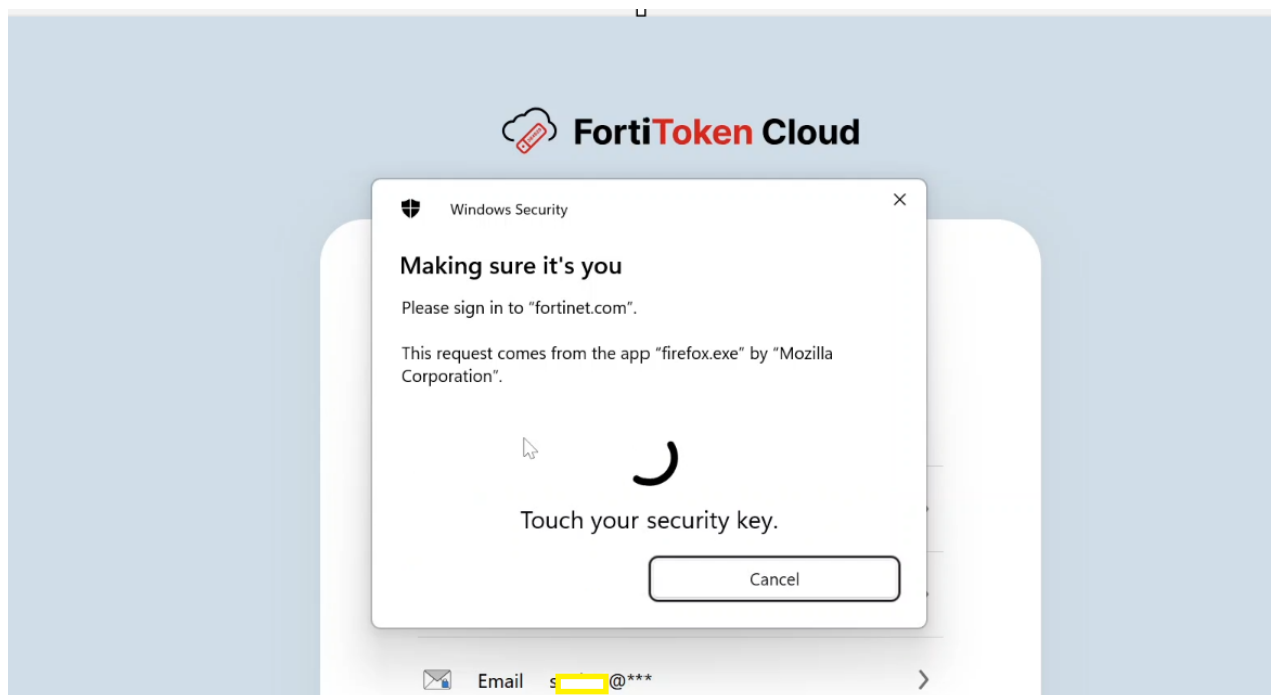


The screenshot shows the 'Login to Your Account' interface of FortiToken Cloud. At the top, the FortiToken Cloud logo is displayed. Below it, the title 'Login to Your Account' is centered. There are two input fields: 'Username' with the placeholder text 'username' and 'Password' with the placeholder text 'Password'. To the right of the password field is a link that says 'Forgot Password?'. At the bottom of the form is a large blue button labeled 'Submit'.

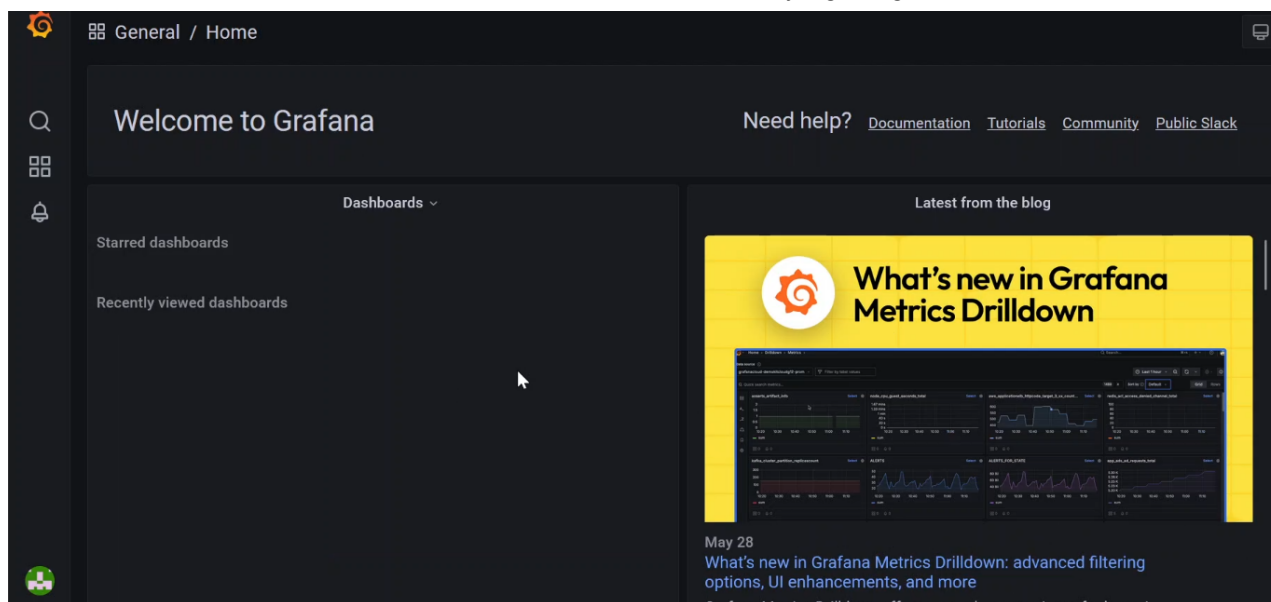
After successful first factor authentication, the user is prompted for MFA by FTC based on the users MFA method. In this example, the user has Passkey configured, so passkey will be prompted by default.



The screenshot shows the 'Confirm Your Identity' interface of FortiToken Cloud. At the top, the FortiToken Cloud logo is displayed. Below it, the title 'Confirm Your Identity' is centered. Underneath the title is a message: 'You must confirm your Identity by selecting one of the methods below.' Below this message is a label 'Select a verification option' followed by a horizontal line. Under the line are three options, each with an icon, a label, and a right-pointing chevron: 'Passkey' with a key icon, 'SMS' with a phone icon and the text '\*\*\*\*7041', and 'Email' with an envelope icon and the text 's\*\*\*\*@\*\*\*'. A mouse cursor is pointing at the 'Passkey' option.



After successful second factor authentication, the user can successfully log into grafana.



In this sample demonstrates that with FTC Local IdP for first factor and a variety of MFA methods to choose from, administrators can secure their applications by configuring FTC as the OIDC provider.



# Applications

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

- [Create FortiProduct applications on page 93](#)
- [Transfer application \(FC account logout\) on page 93](#)
- [Replace an old FortiGate with a new one on page 94](#)
- [Applications in HA mode on page 94](#)
- [Applications for third-party usage on page 97](#)

## Create FortiProduct applications

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

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

## Transfer application (FC account logout)

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

**To transfer an application to a new account:**

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

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

4. Refer to [Transfer devices on FTC on page 195](#) for instructions on how to migrate device data.

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

## Replace an old FortiGate with a new one

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

### In the FortiToken Cloud:

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

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

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

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

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

## Applications in HA mode

Applications in an HA cluster are shared by all members of the cluster. This is to ensure that the cluster members are using the same applications to preserve HA functionality. For more information about how to configure HA clusters in the GUI, see the [FortiProducts](#) section.

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

## Configuring the primary FortiGate

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

Host name

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

### Single heartbeat interface:

Mode

Device priority ⓘ

### Cluster Settings


Group name

Password .....

Session pickup ☐

Monitor interfaces

Heartbeat interfaces 

 ha

**Multiple heartbeat interfaces:**

Mode Active-Passive

Device priority ⓘ 250

**Cluster Settings**



Group name Edge-HA-Cluster

Password •••••••• Change

Session pickup ☐

Monitor interfaces +

Heartbeat interfaces

	port3	<span>×</span>
	port4	<span>×</span>
		<span>+</span>

**Heartbeat Interface Priority ⓘ**

port3		50
port4		50

## Configuring a backup FortiGate

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

Host name Edge-Backup

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

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

## Applications for third-party usage

- Web apps – <https://docs.fortinet.com/document/fortitoken-cloud/latest/rest-api/597289/web-app>
  - Management apps – <https://docs.fortinet.com/document/fortitoken-cloud/latest/rest-api/816036/management-app>
- 



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

---

# Maintenance

- [Add, sync, and delete users on page 98](#)
- [Add, sync, and delete applications \(FortiProducts\) on page 99](#)
- [Service debug on page 99](#)

## Add, sync, and delete users

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

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

### Use case

1. Create or delete users in FGT.
2. Run `"exec fortitoken-cloud sync"` on FGT to sync users with FTC auth method to FTC:
  - If syncing works well, the output will show:

```
Sync status: {"status": "complete", "msg": {"delete": {"success": 0, "failure": 0},  
"modify": {"success": 0, "failure": 0}, "create": {"success": 3, "failure": 0}}}  
User synchronization completed!
```

- If syncing failed, the output will show:

```
Sync status: {"status": "complete", "msg": {"delete": {"success": 0, "failure": 0},  
"modify": {"success": 0, "failure": 0}, "create": {"success": 0, "failure": 3}}}  
User synchronization completed!
```

- If you encounter the “failure” as shown above, check to see if this application exists in the FTC side by searching the SN in the *applications > FortiProducts* page.
  - If it does not exist, check to see if the switch *Auto-create Auch Client* is enabled in the *Settings > Global* page.
  - If it does exist, check to see if the user quota has reached the maximum, or if the realm assigned has available quota and if the *Share-quota Mode* is disabled.
- If the connection to FTC is unstable or unavailable, the output will show:

```
Cannot find FTC server!  
Cannot retrieve user information from FortiToken Cloud!  
Command fail. Return code -1
```

# Add, sync, and delete applications (FortiProducts)

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

## Use cases

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

```
List of VDOMs updated to FortiToken Cloud.
```

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

## How to debug

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

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

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

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

# Service debug

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

# FortiToken Cloud GUI



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

The FTC GUI has the following main pages:

Menu	Description
Dashboard	Provides some key statistics about your account. The content of the page varies, depending on the type of license you are using. For more information, see <a href="#">Dashboard on page 107</a> .
Administrators	(Accessible to the global admin only) enables the global admin to create sub-admin groups and assign realms to them. See <a href="#">Manage admin groups on page 110</a> .
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 <a href="#">Manage realms on page 113</a> .
Users	Shows information of all your FTC end-users. For more information, see <a href="#">Manage users on page 115</a> .
Applications	Shows information about all your authentication clients which include the following types: <ul style="list-style-type: none"><li>• <a href="#">FortiProducts on page 123</a></li><li>• <a href="#">Web Applications on page 125</a></li><li>• <a href="#">Management Applications on page 146</a></li><li>• <a href="#">Use SSO applications on page 146</a></li></ul>
Tokens	Shows the tokens in two groups: <ul style="list-style-type: none"><li>• <i>Mobile</i>—Shows mobile tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See <a href="#">Use mobile tokens on page 200</a>.</li><li>• <i>Hardware</i>—Shows hardware tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See <a href="#">Use hardware tokens on page 200</a>.</li></ul>
Usage	Shows usage data of your account. See <a href="#">Usage on page 222</a> .
Licenses	Shows all the licenses in your account. See <a href="#">Licenses on page 223</a> . <b>Note:</b> This menu is visible to users of time-based subscriptions only, and is not available to users of credit-based subscriptions.



Menu	Description
<b>Settings</b>	<p>Opens the <i>Settings</i> menu which has the following options:</p> <ul style="list-style-type: none"> <li>• <i>Global</i>—Allows the global administrator to enable or disable some settings at the system level. See <a href="#">Manage global settings on page 224</a>.</li> <li>• <i>Realm</i>—Enables both the global admin and sub-admins to view and manage the settings of the selected realm. See <a href="#">Multi-realm Mode on page 224</a>.</li> <li>• <i>Templates</i>—Opens the Templates page where you can add or delete templates. See <a href="#">Use templates on page 232</a>.</li> </ul>
<b>Adaptive Auth</b>	<p>Opens the <i>Adaptive Auth</i> menu which has the following options:</p> <ul style="list-style-type: none"> <li>• <i>Policy</i>—Creates and manage adaptive auth policies.</li> <li>• <i>Profile</i>—Creates and manager adaptive auth profiles.</li> </ul> <p>See <a href="#">Adaptive authentication on page 237</a>.</p>
<b>Logs</b>	<p>Shows the <i>Logs</i> menu which has the following options:</p> <ul style="list-style-type: none"> <li>• <a href="#">Authentication on page 244</a></li> <li>• <a href="#">Management on page 246</a></li> <li>• <a href="#">SMS on page 248</a></li> </ul> <p>See <a href="#">Logs on page 244</a>.</p>
<b>Help</b>	<p>Opens the <i>Help</i> menu which has the following options:</p> <ul style="list-style-type: none"> <li>• <a href="#">Contact Support</a></li> <li>• <a href="#">Purchasing Guide</a></li> <li>• <a href="#">SMS Rate</a></li> <li>• <a href="#">Online Help</a></li> <li>• <a href="#">FAQ</a></li> <li>• <a href="#">Status Monitoring</a></li> </ul>
The bottom of the main menu shows the following information about the realm/account you are looking at:	
<b>Users</b>	Shows the number of users in your realm or account. See the note for <i>Account</i> below.
<b>applications</b>	Shows the number of applications in your realm or account. See the note for <i>Account</i> below.
<b>Account</b>	<p>Shows your account number and the name of your company.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• For a global admin, this part of the page shows the consolidated user and application counts of all the sub-admin accounts under administration; for a sub-admin, it shows the user and application counts of the delegated sub-admin account only.</li> </ul>

# Launch FortiToken Cloud

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

## Log in as a regular FTC user

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

### To log in as a regular FTC user:







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



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

**Welcome to Your Dashboard**

Search

	Account ID 775111 Email <a href="#">[redacted]</a> Company Fortinet Status Free Trial		Account ID 1050546 Email <a href="#">[redacted]</a> Company Fortinet Status Licensed		Account ID 1063530 Email <a href="#">[redacted]</a> Company Fortinet Status Licensed <b>Master</b>
	Account ID 1224184 Email <a href="#">[redacted]</a> Company Fortinet Status Licensed		Account ID 1257532 Email <a href="#">[redacted]</a> Company Fortinet Status Licensed		Account ID 1560106 Email <a href="#">[redacted]</a> Company Fortinet Status Licensed

## Log in as an IAM user

The Identity and Access Management (IAM) portal is an advanced feature of FortiCloud, and is accessible only to FortiCloud Premium customers. An IAM user is one created by the super-admin of a FortiCloud Premium account. IAM users of FTC can only assume the role of a sub-admin on the FTC portal.

### To log in as an IAM user of FTC:

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

## Log into an OU account

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

For more information about Organizations and OUs, see the [Organization Portal Guide](#).

For more information on IAM, see the [Identity & Access Management Guide](#).

### To access Organizational Unit accounts with IAM user credentials:

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

### To access Organizational Unit accounts with external IdP credentials:

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

# 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
<b>My Account</b>	Opens your FC Account page with the following tools: <ul style="list-style-type: none"> <li>• <i>Account Profile</i>–View and edit your account profile.</li> <li>• <i>Change Account ID (Email)</i>–Change your account ID.</li> <li>• <i>Manage User</i>–Add users to your account.</li> <li>• <i>My Account (IAM version)</i></li> </ul>
<b>User Information</b> (Applicable to IAM users only)	Opens the User Information page with the following tools: <ul style="list-style-type: none"> <li>• <i>User Profile</i>–View and edit your user profile.</li> <li>• <i>Change Email</i>–Change your email address.</li> <li>• <i>Permissions</i>–Manage IAM permissions.</li> </ul>
<b>Security Credentials</b>	Opens the FortiCloud page with the following tools: <ul style="list-style-type: none"> <li>• <i>Change Password</i>–Change/update your account password.</li> <li>• <i>2FA Settings</i>–Manage your account's two-factor authentication settings.</li> </ul>

Menu	Description
	<ul style="list-style-type: none"> <li><i>Subscriptions</i>—Manage your subscriptions to (1) Weekly FortiGuard update and/or (2) Quarterly product update (Introduction &amp; EOS).</li> </ul>
<b>Subscriptions</b>	Opens the FortiCloud page where you can manage your subscriptions to (1) Weekly FortiGuard update and/or (2) Quarterly product update (Introduction & EOS).
<b>Logout</b>	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
<b>IAM</b>	<p>Click this link to navigate to the <i>IAM</i> portal where you can take advantage of FortiCloud IAM service.</p> <p><b>Note:</b> 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.</p>
<b>Asset Management</b>	<p>Click this link or the icon to navigate to the <i>FortiCloud &gt; Asset Management</i> page, where you can</p> <ul style="list-style-type: none"> <li>Register your Fortinet products</li> <li>View your Fortinet products and their status</li> <li>Renew your product or service subscriptions</li> <li>View your account services</li> </ul>
<b>Cloud Management</b>	Click any of the following icons (links) to manage the Fortinet product over FC.
FortiGate	FortiGate Cloud
FortiExtender	FortiExtender Cloud
FortiAnalyzer	FortiAnalyzer Cloud
FortiSwitch	FortiSwitch Cloud
FortiAP	FortiAP Cloud
FortiManager	FortiManager Cloud
FortiClient	FortiClient Cloud
<b>Cloud Services</b>	<p>Click any of the icons (links) to launch the FC service.</p> <p><b>Note:</b> You must have a valid license to access any of the following cloud services.</p>
FortiPresence	FortiPresence Cloud

Menu	Description
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
<b>Downloads</b>	Click any of the following links to download. <ul style="list-style-type: none"> <li>• <i>Firmware Download</i></li> <li>• <i>VM Images</i></li> <li>• <i>Service Updates</i></li> <li>• <i>HQIP Images</i></li> <li>• <i>Firmware Image Checksum</i></li> </ul>
<b>Resources</b>	Click this tab to open the <i>FortiCloud &gt; Resources</i> page, where enables you to access a slew of resources to Fortinet products and services.
<b>FortiCare</b>	Click one of the following links for the support service you need: <ul style="list-style-type: none"> <li>• <i>Create a Ticket</i></li> <li>• <i>Manage Active Tickets</i></li> <li>• <i>Manage Tickets</i></li> <li>• <i>Ticket Survey</i></li> <li>• <i>Contact Support</i></li> <li>• <i>Technical Web Chat</i></li> </ul>

# Dashboard

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



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

If you are a customer of a credit-based subscription, you can continue using your existing subscription until it expires. You can then decide whether you want to continue your FTC service by purchasing a time-based subscription.

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

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

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

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

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

## Last 10 authentication attempts in 30 days

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

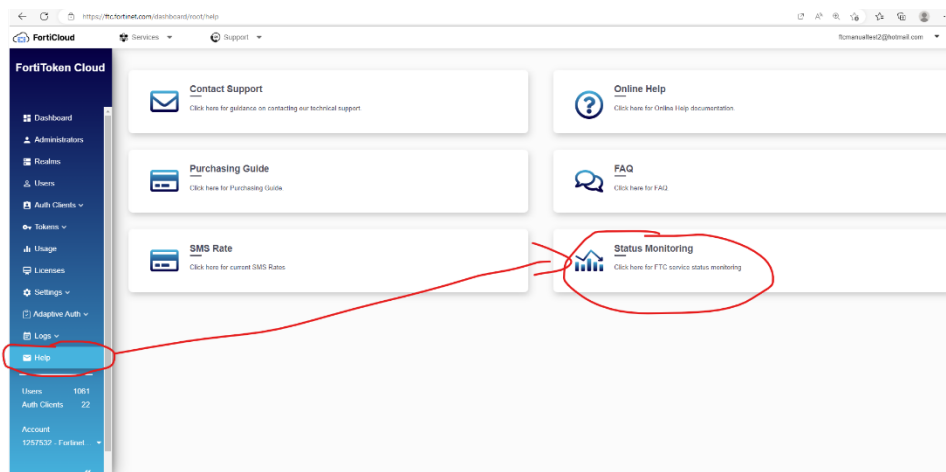
Column	Description
Timestamp	The date and time of the authentication event. <b>Note:</b> FTC captures the time of the event in UTC time, and then converts it to the client browser's local time which is the time shown in the timestamp.
Username	The username of the FTC end-user who requested authentication.
application	The authentication client that made the request.
Action	The type of authentication action.
Result	The outcome of the authentication request, which can be either of the following: <ul style="list-style-type: none"> <li>• <i>Success</i></li> <li>• <i>Failed</i></li> </ul>
Message	A system-generated message about the authentication request.



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

## Monitor FTC status

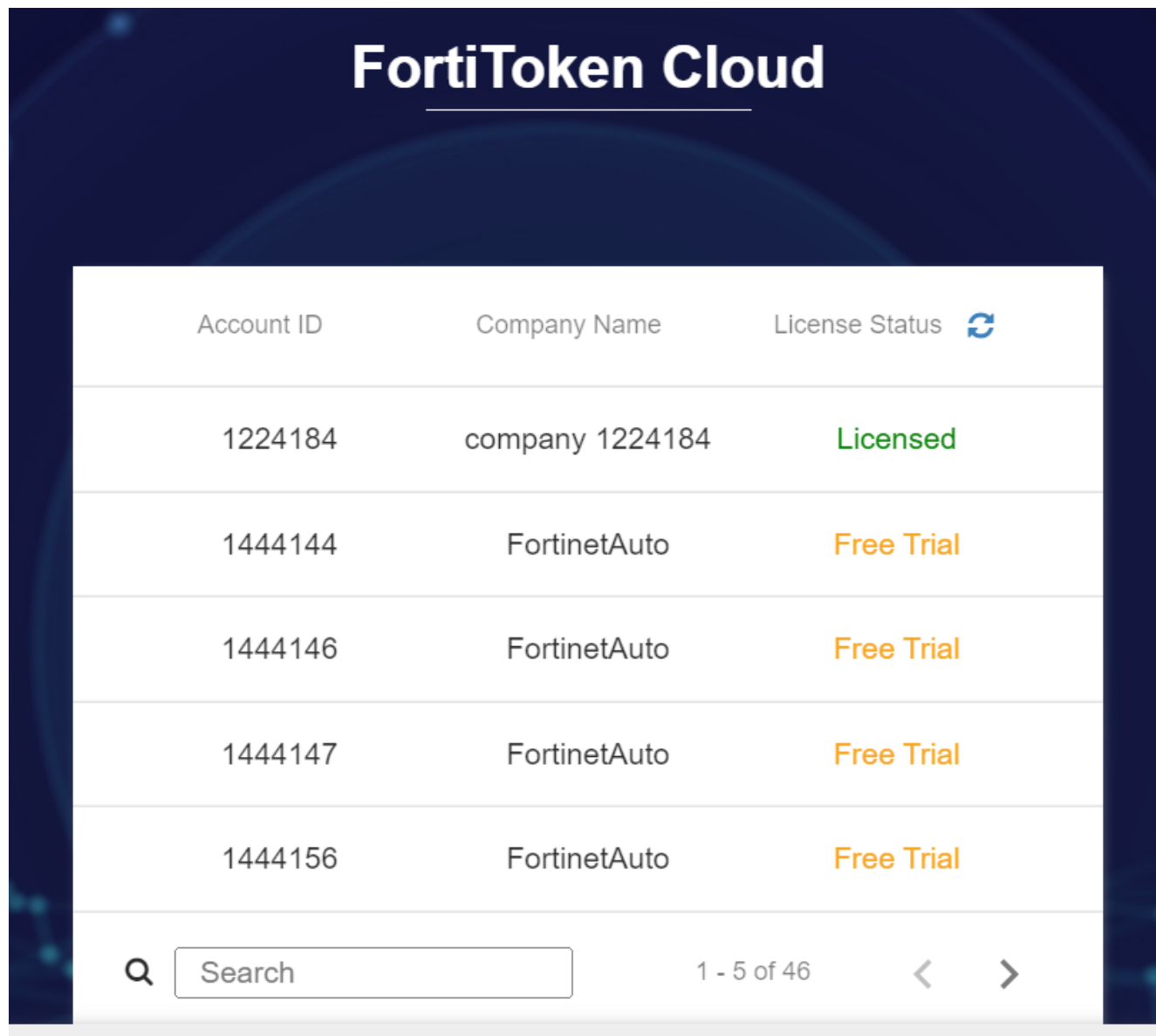
FortiToken Cloud provides the monitor system for FTC's core service, includes API Services, Portal, FortiCloud Login, MFA, Email, SMS and FTM push. The monitor page shows the health status of those services in the past one month and current status. If customers have met any unexpected behaviors, both FortiToken Cloud team or customers can come to check the health status history. Based on the case, FTC team can do more investigation or customers can be notified of what happened in that period. The location of the hyperlink is: Help -> Status Monitoring; moreover, the page is accessible directly by typing [ftc.fortinet.com/status](https://ftc.fortinet.com/status).









## Pagination for accounts with multiple sub-admin users

To avoid taking too long to query multiple sub-users within a master account all at once when logging in, a new design was implemented where we paginate the list of accounts by 5 per page. This allows for the accounts to be loaded in 5 at a time, which should be more user-friendly.



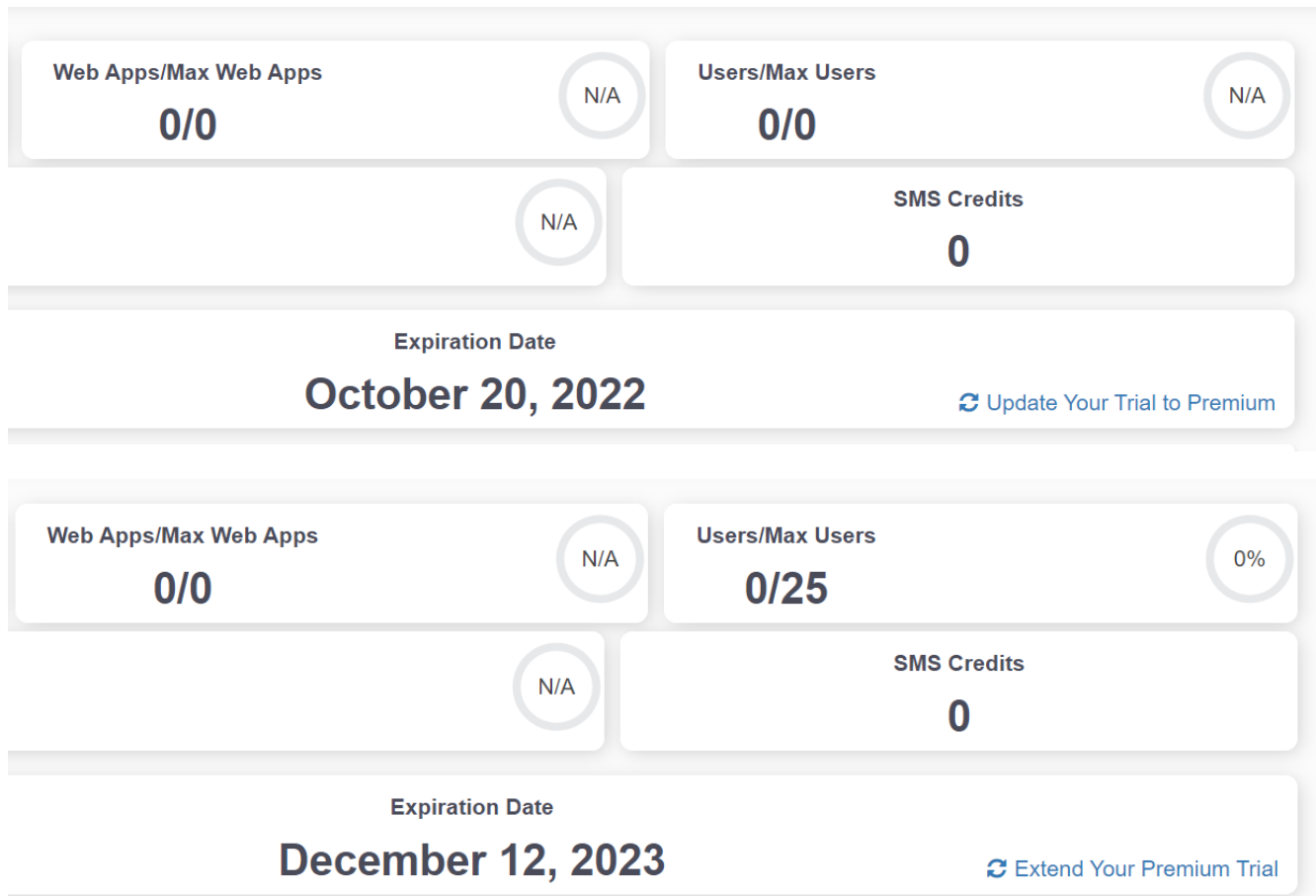
The screenshot shows the FortiToken Cloud interface. At the top, the title "FortiToken Cloud" is displayed. Below it is a table with three columns: "Account ID", "Company Name", and "License Status". The table contains five rows of data. At the bottom of the table, there is a search bar with a magnifying glass icon and the text "Search". To the right of the search bar, it says "1 - 5 of 46". Further right are navigation arrows: a left arrow and a right arrow.

Account ID	Company Name	License Status 
1224184	company 1224184	Licensed
1444144	FortinetAuto	Free Trial
1444146	FortinetAuto	Free Trial
1444147	FortinetAuto	Free Trial
1444156	FortinetAuto	Free Trial

  1 - 5 of 46  

## Refresh button for premium trial and extending premium trial

This button on the Dashboard page is for users who have premium FortiCare and are in trial mode for FTC. The button will either say "Update your trial to Premium" or "Extend your premium trial" depending on the account's situation.



## Manage admin groups

FortiToken Cloud has two levels of admins: `global_admin` (global administrator) and `sub_admin` (sub-administrator). Anyone from a customer organization with a valid user account on FortiCloud (FC) can log on to the FTC portal using their FC username and password. By default, the FC account holder from your organization who logs onto the FTC portal first automatically becomes the `global_admin` of your FTC account. In addition, the main FC account holder of your organization is the de facto `global_admin` of your FTC account.



The *Administrators* menu is accessible to `global_admin` users only; `sub_admin` users will not be able to see this menu.

The *Administrators* page shows all the admin groups that the `global_admin` has created. It also provides the tools for the `global_admin` to manage admin groups. By default, all admins created by the `global_admin` become `sub_admins`.

You (the `global_admin`) can access the *Administrators* page by clicking *Administrators* on the main menu.

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

Column Header	Description
<b>Name</b>	The name of an admin group.
<b>Description</b>	The description of the group. (Optional)
<b>Level</b>	<p>The level of administration of the group:</p> <ul style="list-style-type: none"> <li><i>global_admin</i>—The highest level of administration. <b>Note:</b> The <i>global_admin</i> group is the default admin account, and cannot be deleted.</li> <li><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 applications in those realms and the users on those applications .</li> </ul>
<b>Member Count</b>	<p>The number of sub-admins in the group.</p> <p><b>Note:</b> 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>
<b>Tool bar</b>	<p>The tool bar slides in from the right end of the row when you mouse over the entry in the table. It shows the following tools:</p> <ul style="list-style-type: none"> <li><i>Edit</i>—Edits the administrator group.</li> <li><i>Delete</i>—Deletes the administrator group.</li> </ul>

## Create a sub-admin group

### To create a sub-admin group:

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

## Add users to the group



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

**To add sub-admins to an admin group:**

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

## Add realms to the group

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



- Only the global admin can add realms to an admin group.
- You must have realms created first before assigning them to a sub-admin group. See [Manage realms on page 113](#).
- 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 111](#).
6. To delete a sub-admin, identify the sub-admin and click X (*Delete*).
7. To add more realms to the group, click *Add Realm*. See [Add realms to the group on page 112](#).
8. To delete a realm, identify the realm and click X (*Delete*).
9. Click *Close*.

## Delete a sub-admin group

The global admin can delete any sub-admin group, except the default *'global\_admin'* group. Also, when deleting a sub-admin group with sub-admins in it, you must delete the sub-admin users from the group first before deleting the group. See [Edit sub-admin group configuration on page 112](#).

### 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.

## Manage realms

In FortiToken Cloud, a realm is a container that has a set of users that can be referenced to other users in the same realm and can be controlled by the same realm settings, including MFA method and adaptive auth profile. With realms, admin users can control settings such as user quota and MFA method. FTC comes with a default realm for your convenience.

The *Realms* page shows information about the realms under your management. It also provides tools for managing realms. If you are a global admin, you can see all realms assigned to all sub-admin groups in your account; if you are a sub-admin user, you can see the realms assigned to your sub-admin group only.

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

The following table highlights the information on the Realms page.

Parameter	Description
Check box	Enables you to select a realm. <b>Note:</b> 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 <a href="#">Manage realms on page 113</a> .
Name	The name of a realm.
User Count	The number of end-users in the realm.
Allocated User Quota	The number of end-user quota allocated to the realm.
Description	A brief description about the realm that the global admin added when creating the realm.
Client Count	The number of applications assigned to the realm.
Tool bar	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It has the following tools: <ul style="list-style-type: none"><li>• <i>Refresh Realm</i>—Refreshes the entry to get the latest data about the realm.</li><li>• <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</li></ul>

Parameter	Description
	<p>quota allocation to the selected realm within the set value range.</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Settings</i>—Opens the Settings page which shows the settings of the realm. See .</li> <li>• <i>Delete</i>—Deletes the realm. See <a href="#">Manage realms on page 113</a>.</li> </ul>

- [Create a custom realm on page 114](#)
- [Edit a realm on page 114](#)
- [Delete a realm on page 115](#)
- [View realm permission on page 115](#)
- [Remove sub-admin groups from a realm access list on page 115](#)
- [View realm settings on page 115](#)

## Create a custom realm

1. On the *Realms* page, click *Add Realm*.  
The *Add New Realm* dialog opens.
2. Specify the name of the realm.
3. (Optional) Enter a brief description.
4. Click *OK*.
5. On the *Realms* page, locate the realm that you have just created.
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*.

## Delete a realm

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



- The default realm cannot be modified or deleted.
  - If a realm has applications assigned to it, you must delete the applications from the realm before deleting the realm.
- 

## 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 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. On the toolbar, click the *Show Permission* button to open the *Access List for Realm* dialog.
3. Identify the sub-admin group of interest, and click the corresponding **x** (*Delete*) icon.

## 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.

## Manage 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 <a href="#">Get a new FTM token on page 119</a> .
USERNAME	The username of the end-user.
STATUS	<p>The status of the user, which can be a combination of any of the following:</p> <ul style="list-style-type: none"> <li>  <b>(active)</b>—The user is enabled.  <b>Note:</b> 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. </li> <li>  <b>(disabled)</b>—This button enables the administrator to temporarily stop the user from using FTC.  <b>Note:</b> If a user is disabled, FTC will deny all log-in requests from the user. It must be noted that disabling a user only prevents the user from using FTC, but does not remove the user from your account. FTC will continue counting it toward your user quota for the user until the user is removed from your account. The admin user can also click this button to enable the user if the user is disabled. </li> <li>  <b>(locked)</b>—The user is locked out.  <b>Note:</b> FTC locks a user out when the user has exceeded the specified maximum number of log-in attempts allowed. See <a href="#">Manage realm settings on page 226</a>. </li> <li>  <b>(unlocked)</b>—The user is unlocked.  <b>Note:</b> FTC automatically unlocks users based on their lockout settings. The admin user can also manually unlock a locked user by clicking the  <b>(locked)</b> button. </li> <li>  <b>(Temporary token deactivated)</b>—Temporary token is deactivated.   <b>(Temporary token activated)</b>—Temporary token is activated. </li> <li>  <b>(pending)</b>—A token assigned to the user has not been activated yet. </li> <li>  <b>(expired)</b>—The user's token activation code has expired. </li> <li>  <b>(bypass)</b>—The user is allowed to bypass MFA. </li> <li>  <b>(no bypass)</b>—The user is not allowed to bypass MFA.  <b>Note:</b> 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 <a href="#">Manage realm settings on page 226</a>. Otherwise, when you click the  <b>(no bypass)</b> icon, a tool tip will appear asking you to turn on <i>Enable Bypass on the Settings</i> page. </li> </ul>
MFA	The MFA method used by the user, which can be one of the following:



Column	Description
	<ul style="list-style-type: none"> <li>• <i>FTM</i> (soft token)</li> <li>• <i>Email</i></li> <li>• <i>SMS</i></li> <li>• <i>FTK</i> (FortiToken, a hardware token)</li> </ul>
NOTIFICATION	<p>The method by which FTC sends FTM token activation/transfer notifications to the user, which can be either of the following:</p> <ul style="list-style-type: none"> <li>• <i>Email</i>—FTC sends FTM token activation/transfer notifications to the user's email address.</li> <li>• <i>SMS</i>—FTC sends FTM token activation/transfer notifications by SMS to the user's mobile phone.</li> </ul> <p><b>Note:</b> 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 <a href="#">Manage realm settings on page 226</a>.</p>
EMAIL	<p>The user's email address.</p> <p><b>Note:</b> The admin user is able to edit users' email addresses.</p>
MOBILE PHONE	<p>The user's mobile phone number, if available.</p> <p><b>Note:</b> The phone number must be in the format of "+ <u>Country Code</u> <u>Area Code</u> <u>Phone Number</u>", e.g., +1 4082221234. You can edit an end-user's mobile phone numbers.</p>
REF COUNT	The number of Ref clients for the user.
LAST LOGIN	The timestamp of the user's last successful login.
Tool Bar	<p>The tool bar slides in from the right end of the row when you hover the cursor over an entry. It has the following options:</p> <ul style="list-style-type: none"> <li>• <i>Edit</i>—Edits the user's settings.</li> <li>• <i>Delete</i>—Deletes the user.</li> </ul>

- [Enable Auto-alias by Email on page 118](#)
- [Add user aliases on page 119](#)
- [Auto-assign FTKs to selected users on page 119](#)
- [Get a new FTM token on page 119](#)
- [Hide/Show full FortiAuthenticator username on page 119](#)
- [View a user's applications on page 120](#)
- [Use a temporary token on page 120](#)
- [Edit a user on page 120](#)
- [Delete users from FTC on page 121](#)

## Batch-add users

1. On the *Users* page, click the *Batch Add* button to open the *Batch Add Users* dialog.
2. Select a realm.

3. Enter the username, Email, and mobile phone number.
4. Click *Add New User* and repeat Step 3 to add as many users as needed.
5. Click *Save* when done.

All users you have entered are added to the Users page at once.

Alternatively, you can add multiple users all at once by downloading the `Users_template.csv` file, filling it out with the required user information, and then uploading it to FTC.

### To batch-add users using the `Users_template`:

1. In the Batch Add Users dialog, click *Download CSV Template*.
2. Open the `Users_template.csv` file, and fill it up with the username, email address, and mobile phone number of each of the users to be added.
3. Save the file.
4. On the Users page, click *Upload CSV file*. All users in the `Users_template.csv` file are added to the Batch Add Users dialog.
5. Click *Save*. The uses are now added to the *Users* page.

## 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 applications. For example, John Doe II may have the following usernames:

- user1 in VPN
- user\_one in a web app
- u1 as a system admin
- user1@company.com on an email server

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

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

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

Once the *Auto-alias by Email* feature is enabled, all usernames with the same email address are automatically set as an alias under the same username.

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

## Add user aliases



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

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

## Auto-assign FTKs to selected users



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

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

## Get a new FTM token



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

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

## Hide/Show full FortiAuthenticator username

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

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

## View a user's applications

1. On the *Users* page, identify the user of interest.
2. Click the numeric value in the *REF COUNT* column.  
A window opens, showing the Ref Client List for the user.
3. Click *Close* to close the window.

## Use a temporary token

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

### To assign a temporary token to a user:

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

## Edit a user

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

Field	Description
Name	The username of the end-user. ( <b>Note:</b> This field is read only.)
Auth Method	Click the down arrow, and select a desired authentication method from the drop-down menu: <ul style="list-style-type: none"><li>• <i>FTM</i></li><li>• <i>Email</i></li><li>• <i>SMS</i> (<b>Note:</b> This option requires a valid mobile phone number.)</li><li>• <i>FTK</i></li></ul>
Notification Method	<b>Note:</b> This field applies only when you set <i>Auth Method</i> to <i>FTM</i> . See above.
Token SN	The serial number of the token.

Field	Description
	<b>Note:</b> This field is read only. 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.
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. <b>Note:</b> This field is required when <i>Auth Method</i> and/or <i>Notification Method</i> is set to <i>SMS</i> , as stated above.
Status	Displays the user's status in icons applicable to the user.
Created at	The times when the end-user was created.

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

## Delete users from FTC



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

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

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

## Manage user groups

The User Groups page shows all the user groups that the admin has created. It also provides tools for managing user groups.

- [Add a user group on page 122](#)
- [View user group information on page 122](#)

- [Edit a user group on page 122](#)
- [Delete a user group on page 122](#)

## Add a user group

1. From the top of the *User Groups* page, select *Add User Group* to open the *Create New User Group* dialog.
2. Click the *General* tab (if it has not yet been opened), specify a user group name, add a brief description, and select a realm.
3. Click the *Users* tab and select the users to be added to the group. To add all users to the group, select the checkbox in the upper-left corner of the table; to add some users to the group, select the users and select *Selected Users Only* in the upper-right corner of the table.
4. Click the *Application* tab, and in the *CUSTOMIZED PERMISSION* column, click the down arrow and select the appropriate permission for each of the applications.
5. Click *Save*.

## Edit a user group

1. On the *User Groups* page, locate the user group.
2. Click the tool button, and select *Edit* to open the *Edit User Group* dialog.
3. Make desired changes.
4. Click the *User Groups* sub-menu to refresh the page.

## View user group information

The *User Groups* page contains the following information:

Parameter	Description
NAME	Name of the user group.
DESCRIPTION	(Optional) Description of the group.
REALM	Realm the user group is associated with.
USER COUNT	Number of end-users in the group.
Tool button	<ul style="list-style-type: none"><li>• Edit. See <a href="#">Edit a user group on page 122</a>.</li><li>• Delete. See <a href="#">Delete a user group on page 122</a>.</li></ul>

## Delete a user group



To delete a user group, you must remove all users from the user group first.

1. On the *User Groups* page, locate the user group.
2. Click the tool button, and select *Edit* to open the *Edit User Group* dialog.
3. Click *Manage User* to open the *Manage Users* dialog.
4. Deselect all the selected users to remove them from the user group, and click *Apply*.
5. On the *User Groups* page, click the tool button and select *Delete*.
6. In the *Delete User Group* dialog, click *Yes*.

## FortiProducts

The *FortiProducts* page shows information about all Fortinet products as applications in your FTC account. You can open the *FortiProducts* page by clicking *applications > FortiProducts* on the main menu.

The following table highlights the information on the *FortiProducts* page.

Column	Description
<b>Checkbox</b>	<p>Unchecked by default. If checked, the application becomes selected and the <i>DELETE</i> button is enabled. You can then click the <i>DELETE</i> button to remove the selected applications. For more information, see <a href="#">Delete an application on page 124</a>.</p> <p><b>Note:</b> You can select all the applications at once by checking the checkbox in the column header.</p>
<b>Alias</b>	The alias of the application.
<b>Name</b>	The name of the application.
<b>Type</b>	<p>The type of application, which can be any of the following:</p> <ul style="list-style-type: none"> <li>• <i>FortiAuthenticator</i></li> <li>• <i>FortiGate</i></li> <li>• <i>FortiGateVM</i></li> <li>• <i>FortiSandbox</i></li> </ul> <p><b>Note:</b> FTC assigns applications type based on the serial number and model of the product.</p>
<b>Count</b>	<p>The number of FTC end-users on the applications.</p> <p><b>Note:</b> Clicking the numeric value opens a dialog which shows the list of FTC end-users on an applications, along with some basic user information.</p>
<b>Realm Name</b>	The name of the realm to which the applications is assigned.
<b>Tool Bar</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• <i>Edit</i>—Change certain settings of the application.</li> <li>• <i>Details</i>—Shows some detailed information of the application.</li> <li>• <i>Delete</i>—Deletes the applications.</li> </ul>



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

## Assign an application to a realm



An application must be assigned to a realm. Otherwise, you cannot add or sync users from the application. For more information, see [Manage realms on page 113](#).

---

1. On the main menu, click *applications > FortiProducts* to open the *FortiProducts* page.
2. In the table, locate the unassigned application, and mouse over it to bring out the toolbar.
3. Click the *Edit Fortiprod* button to open the Edit dialog.
4. Click the *Realm* drop-down menu, and select a realm of interest.
5. Read the message.
6. Click *OK*.  
The name of the newly selected realm now appears in that column, meaning that the application now is assigned to this realm.

## Edit an application

1. On the *FortiProducts* page, identify the application 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 application

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

## Delete an application



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

---

1. On the *Applications > FortiProducts* page, identify the application 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 Applications

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

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

Parameter	Description
<b>Name</b>	The name of a web app.
<b>Client ID</b>	A unique, read-only ID that FTC has generated for an application.
<b>Count</b>	The number of FTC end-users on the application.
<b>Realm Name</b>	The name of the realm to which the application is assigned.
<b>Secret</b>	Part of the secret. <b>Note:</b> Click the icon to regenerate the secret for the application.
<b>Last Update</b>	The time when the application was last updated.
<b>Tool Bar</b>	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"><li>• <i>Edit</i>—Edits the settings of a web app as application</li><li>• <i>Delete</i>—Deletes the web app as application.</li></ul>

## Add a web app

When a new application is added, FTC assigns it the default name "*MyAuthClient*" which can be edited. If you add more applications of the same type, FTC will append a sequence number starting with "1" to the subsequent application 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 application to it. Otherwise, the application will be assigned to the default realm. You must assign the application to a custom realm to add end-users to it.

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



Paid customers have full access to FortiToken Cloud APIs; trial customers only have limited access to the APIs with certain restrictions. For more information, refer to [Trial account API request limit on page 38](#).

1. In the upper-left corner of the *applications > 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 application.
6. Click *OK*.

## Regenerate API credentials

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

## Edit a web app

1. On the *applications > 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

1. On the *applications > 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*.

## SCIM client integration

Starting with its 24.2.a release, FortiToken Cloud has integrated with SCIM client applications. SCIM, which stands for System for Cross-domain Identity Management, is an open standard for cloud-based user provisioning. The greatest benefit of SCIM is that it provides a standardized, secure methodology for exchanging information between IT systems or identity domains. This ensures interoperability across domains without expensive custom integrations. SCIM auto-provisioning increases productivity across the entire organization. Besides freeing up IT resources to focus on more mission-critical tasks. SCIM, in tandem with access management systems, can reduce the time needed to grant access to backend infrastructure and boost employee productivity at the same time. Together, these benefits can greatly improve the return on investment (ROI) on IT infrastructure while reducing the total cost of ownership (TCO).

- [Features and benefits on page 127](#)
- [Use case on page 128](#)
- [Supported SCIM client applications on page 128](#)
- [Integrate FTC with SCIM clients on page 129](#)
- [Demo configurations on page 130](#)
- [Known issues and special notes on page 145](#)

## Features and benefits

FTC and SCIM client integration offers the following features and benefits:

### User provisioning

Automated creation of user accounts in target systems based on changes in the identity provider (IdP). When a new user is added to the IdP or updates are made to existing user attributes, the SCIM server communicates these changes to the connected applications or services, ensuring that user accounts are consistently provisioned across the ecosystem.

### User deprovisioning

When a user is deactivated or removed from the identity provider, the SCIM server ensures that corresponding actions are taken in connected systems to deactivate or delete the user account.

### Attribute synchronization

Synchronize user attributes (such as name, email, group memberships, roles, etc.) between the identity provider and connected systems. Changes made to user attributes in one system are propagated to other systems, ensuring consistency and accuracy of user data across the organization's IT infrastructure.

### Group management

Manage user groups and their memberships across different systems. Group-provisioning and deprovisioning functionalities enable organizations to efficiently manage access permissions by automatically updating group memberships based on changes in the identity provider.

### Security

Implement security measures such as authentication, authorization, and secure communication protocols (e.g., HTTPS) to ensure the confidentiality, integrity, and availability of sensitive identity data exchanged between systems.

### Standards compliance

SCIM is built on standard web protocols such as HTTP and JSON, making it interoperable with and widely supported by various identity management solutions, cloud services, and applications. A SCIM server streamlines identity management processes, reduces manual effort, enhances security, and improves the efficiency of user lifecycle management in organizations with complex IT environments. Compliance with SCIM specifications ensures seamless integration and compatibility with other SCIM-compliant systems.

## Supported SCIM client applications

FTC and SCIM integration involves configuration of FTC as the SCIM server and one or more SCIM-compliant cloud-based applications as SCIM clients. For current release, FTC has been fully tested with the following SCIM client applications:

- Okta
- Azure
- FortiAuthenticator



FortiToken Cloud is fully compliant with SCIM specifications and, therefore, can work with any SCIM client application on the market.

---

## Use case

Imagine a large multinational corporation with offices spread across the globe. Each office has its own identity management system, handling employee accounts, permissions, and access to resources. However, managing user identities across these disparate systems is not an easy task. This is where SCIM comes in handy.

In this scenario, the corporation decides to implement SCIM to streamline the management of user identities across all its offices. Here's how it works:

- Centralized identity management – With SCIM, the corporation can establish a central identity management system that serves as the authoritative source of user identities. The system contains a master user directory where all employee identities are stored.
- Automated user provisioning – Whenever a new employee joins the company, their information is entered into the central identity management system. SCIM allows for automated provisioning, meaning that user accounts can be automatically created in the various office-specific identity systems without manual intervention.
- Consistent user data – SCIM ensures that user data remains consistent across all systems. If an employee updates their profile information (such as changing their job title or contact details), those changes are automatically propagated to all relevant systems via SCIM.
- Simplified access management – With SCIM, access permissions can be managed centrally. When an employee leaves a company or changes roles in the company, access privileges are updated in real time across all the systems, reducing the risk of unauthorized access.
- Interoperability – SCIM provides a standardized way for different identity management systems to communicate with each other. This ensures interoperability between systems from different vendors, allowing the corporation to use the best-in-class solutions for each office while still maintaining a cohesive identity management strategy.
- Audit trail and compliance – SCIM provides a comprehensive audit trail, allowing administrators to track changes to user identities and access permissions. This is crucial for compliance purposes because it ensures that the corporation meets regulatory requirements related to data security and privacy.

Overall, by implementing SCIM, the corporation can achieve greater efficiency, consistency, and security in managing user identities across its distributed infrastructure

## Integrate FTC with SCIM clients

Suppose your organization is using Okta, Azure, and/or FortiAuthenticator to manage user identity, you must integrate these applications with FTC and sync their users or user groups to FTC. In so doing, you are turning FTC into a SCIM server and those applications SCIM clients. The integration enables end-users of those applications to authenticate themselves through FTC – the SCIM server.

FTC-SCIM client integration requires the following two major steps:

1. Configure FTC as the SCIM server.
2. Configure one or more SCIM client applications (i.e., Okta, Azure, or FortiAuthenticator) as SCIM client(s).

For detailed steps for configuring the SCIM server and SCIM clients, refer to the following sections:

- [Configure FTC as SCIM server on page 129](#)
- [Configure Okta as SCIM client on page 129](#)
- [Configure Azure as SCIM client on page 129](#)
- [Configure FortiAuthenticator as SCIM client on page 130](#)

### Configure FTC as SCIM server

1. Go to <https://ftc.fortinet.com>.
2. From the main menu, select *Applications > Web Apps*.
3. Select *Add SCIM Client*.
4. Copy the secret.

### Configure Okta as SCIM client

1. Log into your Okta admin account.
2. Select Application > Browse App Catalog, search for SCIM 2.0 Test App ( Header Auth), and add the application.
3. Select Add Integrations > Provisioning > Enable API integration.
  - a. Base URL: <https://ftc.fortinet.com:9696/api/v2/scim/>
  - b. API Token: (Bearer+space-Copied Secret)
  - c. Click Test API Credentials
4. Assignments
  - a. Add the users (Tom/Mike ) or group.
  - b. Remove the users or group

### Configure Azure as SCIM client

1. Go to <https://portal.azure.com>, and log into your corp account.
2. Click Enterprise Applications > New Applications to create a new application.
3. Upon creation of the new application, click Provisioning > Select Automatic > Admin Credentials.
  - a. Tenant URL: <https://ftc.fortinet.com:9696/api/v2/scim/>
  - b. Secret Token: Copied Secret
  - c. Test Connection
4. Manage users and groups:

- a. To add a user or group, click Add user/group, select the user or group, and click Assign.
- b. To remove a user, select the user and remove the assignment.

## Configure FortiAuthenticator as SCIM client

1. Log into your FAC admin account.
2. Click Authentication > SCIM > Service Provider > Create New.
3. In the Create New SCIM Service Provider window, do the following:
  - a. Name: test-scim
  - b. SCIM endpoint: <https://ftc.fortinet.com:9696/api/v2/scim/>
  - c. Access Token: copied secret
4. Click Sync to automatically add exiting users to the SCIM server.

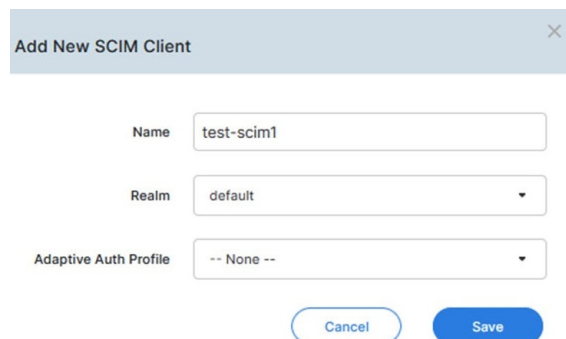
## Demo configurations

This sections provides sample configurations for FTC and SCIM client integration.

- [Demo: Configure FTC as the SCIM server on page 130](#)
- [Demo: Configure Okta as SCIM client on page 131](#)
- [Demo: Configure Azure as SCIM client on page 135](#)
- [Demo: Configure FortiAuthenticator as SCIM client on page 142](#)

## Demo: Configure FTC as the SCIM server

1. Go to <http://ftc.fortinet.com> and log in.
2. Click Applications>Web Apps>Add SCIM Client.



- Name: test-scim1, for example
  - Realm : <default>
  - Adaptive Auth Profile: --None--
3. Click Save. The following page opens.

Web App test-scim1

Name: test-scim1

Realm: default

Adaptive Auth Profile: -- None --

ID: 650

Secret: ey b3

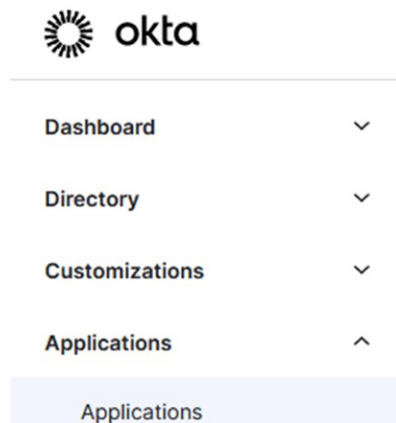
Copy to clipboard

OK

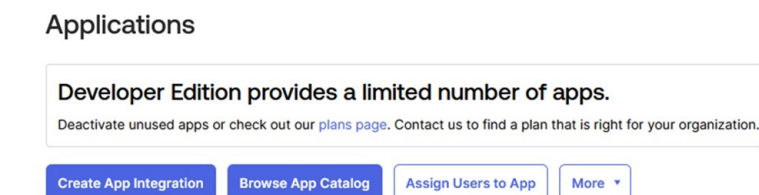
4. Copy the secret. Be sure to apply the secret to the SCIM clients (i.e., Okta, Azure, or FortiAuthenticator) you are going to configure.

## Demo: Configure Okta as SCIM client

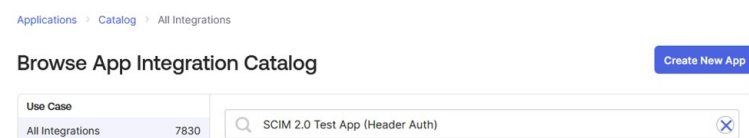
1. Go to <http://okta.com>, and log in with your Corp account.



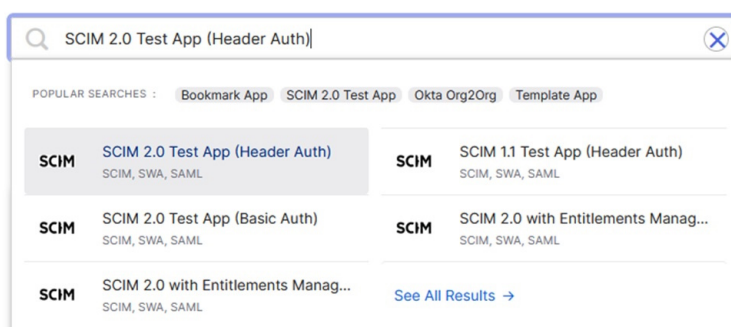
2. Click Applications > Browse App Catalog.



3. Search SCIM 2.0 Test App (Header Auth).



#### 4. Click SCIM 2.0 Test App (Header Auth) and Add Integration.



#### 5. Okta Add SCIM Provisioning.

- After your integration is created, click the General tab.
- Click Edit.
- In the Provisioning section, select SCIM and click Save.

#### Add SCIM 2.0 Test App (Header Auth)

1 General Settings

2 Sign-On Options

### General settings Required

Application label

SCIM 2.0 Test App (Header Auth)

This label displays under the app on your home page

Application Visibility

☐ Do not display application icon to users
   
☐ Do not display application icon in the Okta Mobile App

Browser plugin auto-submit

☒ Automatically log in when user lands on login page

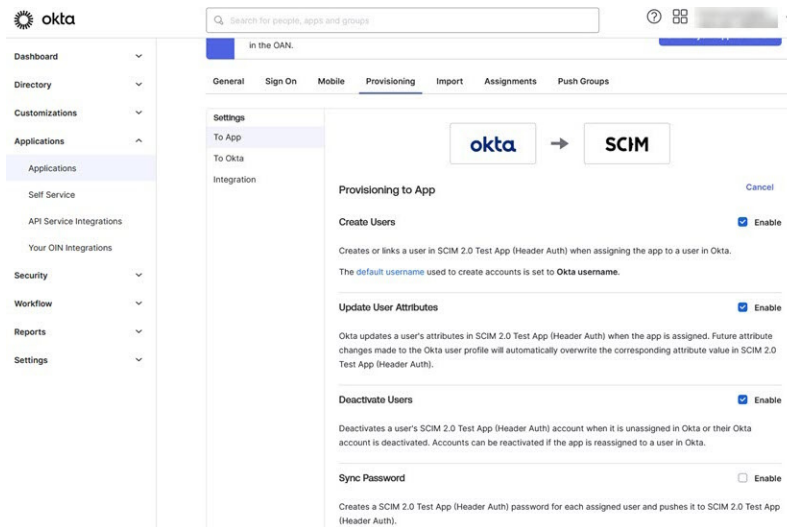
Cancel

Next

#### 6. Choose Provisioning options

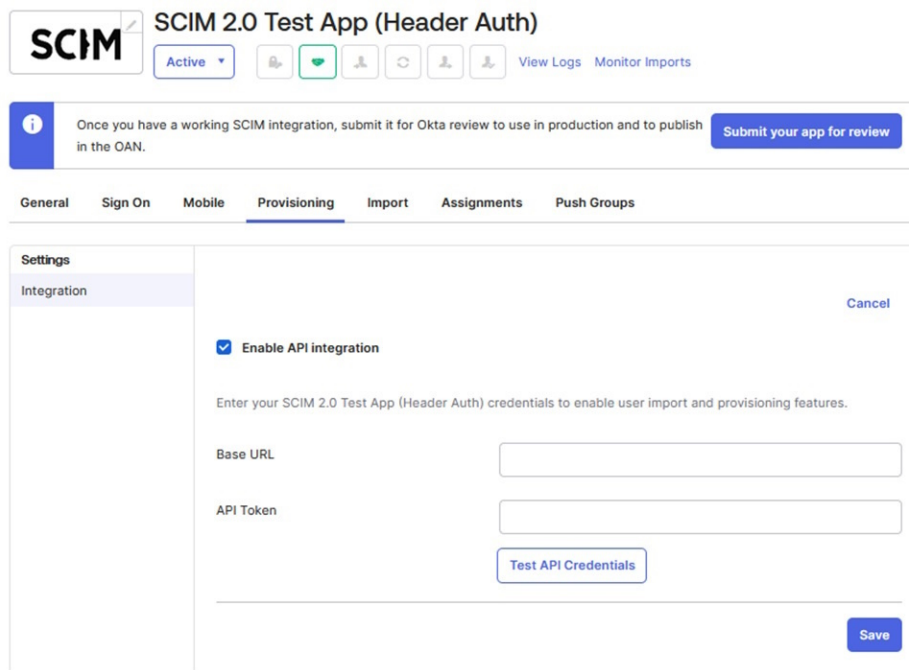
- From the integration settings page, choose the **Provisioning** tab. The SCIM connection settings appear under Settings Integration.





## 7. Click **Edit**.

- Specify the SCIM connector base URL and the field name of the unique identifier for your users on your SCIM server.



Base URL: `https://ftc.fortinet.com:9696/api/v2/scim/`

API Token: (Bearer+space-Copied Secret)

## 8. Assign the users to the applications, go to the Applications > Assignments > Assign to People, and Assign.

**SCIM 2.0 Test App (Header Auth)**

Active | View Logs | Monitor Imports

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN. [Submit your app for review](#)

General | Sign On | Mobile | Provisioning | Import | **Assignments** | Push Groups

Assign | Convert assignments | Search... | People

Assign to People | Assign to Groups

Type
01101110
01101111
01101111

REPORTS

- Current Assignments
- Recent Unassignments

9. Add the users:

- Create the Okta new user and add the email id field.

**Assign SCIM 2.0 Test App (Header Auth) to People**

Search...

devops ninja devopsninja22@...l.com	Assign
testuser15-03 testuser15-03 whateverba4@...l.com	Assign
ai ninj aininja@qaninjaops.net	Assign

Done

10. Add the groups:

- Create the okta new group and add the user to the group
- Assign the users to the applications , go to the Applications --> Assignments --> Assign to group and Assign

**Assign SCIM 2.0 Test App (Header Auth) to Groups**

Search...

Everyone All users in your organization	Assign
ftc-scim-15 ftc scim mar15 2024	Assign
ftc-scimgrp	Assign

Done

11. Remove the users and groups from the app:
  - a. Click the X button remove the user or group.

**SCIM** SCIM 2.0 Test App (Header Auth)

Active

Once you have a working SCIM integration, submit it for Okta review to use in production and to pu in the OAN.

General Sign On Mobile Provisioning Import **Assignments** Push Groups

Assign Convert assignments Search... People

Filters	Person	Type	
People	devops ninja devopsninja22@.com	Individual	X
Groups	testuser15-03 testuser15-03 whateverba4@.com	Group	X

## Demo: Configure Azure as SCIM client

1. Go to <https://portal.azure.com>.
2. Click **Enterprise Applications**.

Azure services

Create a resource Enterprise applications View

3. Click **Create your Own applications**.

Microsoft Azure

Home > Enterprise applications

Enterprise applications | All applica

Default Directory - Microsoft Entra ID

<< + New application


Overview

Browse Microsoft Entra Gallery

+ Create your own application | Got feedback

The Microsoft Entra App Gallery is a catalog of thousand

## Create your own application

 Got feedback?

If you are developing your own application, using Application Proxy, or wait for an application that is not in the gallery, you can create your own application here.

What's the name of your app?


ftc-scim-test2

What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premise application.  
☐ Register an application to integrate with Microsoft Entra ID (App you're developing).  
☒ Integrate any other application you don't find in the gallery (Non-gallery application).

Create

### 4. Review the application that you've just created.

 ftc-scim-test2 | Overview ...

Overview
Provision on demand
Manage
Provisioning
Monitor
Provisioning logs
Audit logs
Insights
Troubleshoot
New support request

Automate identity lifecycle management with Microsoft Entra ID.

Automatically create, update, and delete accounts when users join, leave, and move.

Get started

What is provisioning? Plan an application deployment.

### 5. Click **Provisioning** and Select Automatic Provisioning Mode.

**Provisioning** ...

 Save  Discard

Provisioning Mode

Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in ftc-scim-test2 based on user and group assignment.

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to ftc-scim-test2's API and synchronize user data.

Tenant URL \*

https://ftc.fortinet.com:9696/api/v2/scim/

Secret Token

Test Connection

### 6. Add the users to the applications:

- a. Go to the applications and click the newly created the application ftc-scim-test2.

Home > Enterprise applications | All applications > ftc-scim-test2

## ftc-scim-test2 | Users and groups

Enterprise Application

« + Add user/group | Edit assignment

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

The application will appear for assigned users with

Assign users and groups to app-roles for your app

First 200 shown, to search all users & gr...

Display Name

No application assignments found

- b. Click **Add user/group**, Select and Assign

Home > Enterprise applications > ftc-scim-test2

## Add Assignments

Default Directory

Groups are not available for this application.

Users

None Selected

Select a role

User

### Users

Try changing or adding filters if you don't see what you're looking for.

Search

4 results found

	Name	Type	Details
<input type="checkbox"/>	devops ninja	User	devopsninja22@... .com
<input type="checkbox"/>	randy	User	randy@r... .com
<input type="checkbox"/>	sunnyvaleninja	User	hqninja@... .com
<input type="checkbox"/>	yahooninja1	User	yahooninjaops@... .com

- c. Add to the assignment and click assign

[Home](#) > [Enterprise applications](#) | [All applications](#) > [ftc-scim-test2](#) | [Users and groups](#) >

## Add Assignment

Default Directory



Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

### Users

1 user selected.

Select a role

User

Assign

[Home](#) > [Enterprise applications](#) | [All applications](#) > [ftc-scim-test2](#) | [Provisioning](#) >

## ftc-scim-test2 | Overview

Overview

Provision on demand

Manage

Provisioning

Users and groups

Expression builder

Monitor

Provisioning logs

Audit logs

Insights

Troubleshoot

New support request

Start provisioning

Stop provisioning

Restart provisioning

Edit provisioning

Provision on demand

Refresh

Current cycle status

Initial cycle not run.

0% complete

View provisioning logs

Statistics to date

View provisioning details

View technical information

Manage provisioning

Update credentials

Edit attribute mappings

Add scoping filters

Provision on demand

FortiToken Cloud 25.2.a Admin Guide  
Fortinet Inc.

138

## Provisioning:

### a. Click Provisioning and Restart

Home > Enterprise applications | All applications > ftc-scim-test2 | Provisioning >

**ftc-scim-test2 | Overview** ...

Overview | Provision on demand | Manage | Provisioning | Users and groups | Expression builder | Monitor | Provisioning logs | Audit logs | Insights | Troubleshoot | New support request

Start provisioning ☐ Stop provisioning Restart provisioning Edit provisioning Provision on demand Refresh

**Current cycle status**

Initial cycle not run. 0% complete

View provisioning logs

**Statistics to date**

View provisioning details  
View technical information

**Manage provisioning**

Update credentials  
Edit attribute mappings  
Add scoping filters  
Provision on demand

**Overview** ...

Start provisioning ☐ Stop provisioning Restart provisioning Edit provisioning Provision on demand Refresh

**Restart provisioning**

Are you sure you want to restart provisioning?

OK Cancel

View technical information

View provisioning logs

**Restart provisioning**

Provisioning is scheduled to restart.

**Remove User:**[All applications](#) > [ftc-scim-test2](#)**Users and groups** ...

« [+ Add user/group](#) | [Edit assignment](#) | **Remove** | [Update credentials](#)

**i** The application will appear for assigned users within My Apps. Set 'visible to users?' to no i

Assign users and groups to app-roles for your application here. To create new app-role

First 200 shown, to search all users & gr...

Display Name	Object Type
<input checked="" type="checkbox"/> <b>DN</b> devops ninja	User

« [+ Add user/group](#) | [Edit assignment](#) | [Remove](#) | [Update credentials](#) | [Columns](#) | [Got feedback?](#)

**Do you want to remove these assignments?**  
Selected application assignments will be removed

First 200 shown, to search all users & gr...

Display Name	Object Type	Role assi
<input checked="" type="checkbox"/> <b>DN</b> devops ninja	User	User

**✓ Application assignments removed**  
1 application assignments have been removed

**On-Demand Provision:**

Go to Enterprise Applications>All Applications>your-Applications>Provisioning>Provision on demand.  
Example.



a. Search and select the user or group.

[Home](#) > [Enterprise applications](#) | [All applications](#) > [ftc-scim-apr23](#) | [Provisioning](#) > [ftc-scim-apr23](#)

## ftc-scim-apr23 | Provision on demand ...

«

[Learn More](#) | [Got feedback?](#)

Overview

Provision on demand

Manage

Provisioning

Users and groups

Provision on-demand for a subset of users or groups before rolling it out broadly to your organization members at a time.

No user or group will be provisioned on-demand that would not have been provisioned through the regular provisioning process.

Select a user or group

b. For groups, select the members.

## ftc-scim-apr23 | Provision on demand ...

«

[Learn More](#) | [Got feedback?](#)

Overview

Provision on demand

Manage

Provisioning

Users and groups

Expression builder

Monitor

Provisioning logs

Audit logs

Insights

Troubleshoot

New support request

Provision on-demand for a subset of users or groups before rolling it out broadly to your organization members at a time.

No user or group will be provisioned on-demand that would not have been provisioned through the regular provisioning process.

Selected group

Selected users

☒ View members only

☐ View all users

1 selected

Provision


c. Click Provision





| All applications &gt; ftc-scim-apr23 | Provisioning &gt; ftc-scim-apr23

## | Provision on demand ...

[Learn More](#) | [Technical details](#) | [Got feedback?](#)

Group


**azure-rc11-grp9**  
d10b2720-551a-43fd-914b-7d5999431e83

- 1. Import group**  
This step shows the group retrieved from the source system and the properties of the group in the source system.  
 Success | [View details](#)
- 2. Determine if group is in scope**  
This step shows the scoping conditions that were evaluated and which ones the group passed or failed.  
 Success | [View details](#)
- 3. Match group between source and target system**  
This step shows whether the group was found in the target system as well as the properties of the group in the target system.  
 Success | [View details](#)
- 4. Perform action**  
This step shows the action that was performed in the target application, such as creating a group or updating a group.  
 Success | [View details](#)

[Retry](#)
[Provision another object](#)

## Perform action

[Group details](#) | [Group membership operations](#) | [User operations](#) | [Data flow](#)

Group 'azure-rc11-grp9' was updated in customappsso

Target attribute name	Source attribute value	Expression	Origin:
externalid	d10b2720-551a-43fd-914b-7...	[objectId]	

## d. Check the Provision logs:

Home &gt; Enterprise applications | All applications &gt; ftc-scim-apr23 | Provisioning &gt; ftc-scim-apr23

## ftc-scim-apr23 | Provisioning logs ...

[Overview](#)
[Download](#)
[Learn more](#)
[Refresh](#)
[Columns](#)
[Got feedback?](#)

[Identity Name or ID](#)
[Date: Last 24 hours](#)
[Show dates as: Local](#)
[Status: All](#)
[Action: All](#)
[Application contains 29faa7fc-2284-43d2-ac23-568a6a884cfd](#)
[Add filters](#)

Date	Identity	Action	Source System	Target System	Status
4/30/2024, 10:47:21 AM	Display Name azure-rc11user24 Source ID d0059065-2637-4ed6-9f05-abdefb Target ID 792db20e-b3ee-4ded-a925-10e33	Other	Microsoft Entra ID	customappsso	Skipped
4/30/2024, 10:47:21 AM	Display Name azure-rc11-grp9 Source ID d10b2720-551a-43fd-914b-7d5999 Target ID d7e9aabb4-9b34-4b3a-ad19-3b059	Update	Microsoft Entra ID	customappsso	Success
4/30/2024, 2:54:14 AM	Display Name azure-rc10-user16 Source ID fece1dc3-a0ec-4a38-b8aa-a012f5 Target ID a7771289-10e1-439e-8af4-7ea9a71	Disable	Microsoft Entra ID	customappsso	Failure
	Display Name azure-rc11user23				

## Demo: Configure FortiAuthenticator as SCIM client



- This demo is conducted using FortiAuthenticator VM v6.6.1, Build 1660 (GA) release.
- For more information about FortiAuthenticator, visit <https://docs.fortinet.com/document/fortiauthenticator/6.6.0/administration-guide/684814/service-providers>.

## Configure the SCIM service provider

1. From the main menu, click *Authentication>SCIM>Service Provider>Create New*. The Create New SCIM Service Provider page opens.

2. Make the entries and/or selections as described in the following table, and click **Save**.

## Edit Service Provider

Parameter	Description
Name	Enter the name of the SCIM service provider (SP).
SCIM endpoint	Enter the SCIM SP IP address.
Access token	Enter the SCIM SP access token.

## Users/Groups To Synchronize

Parameter	Description
Remote auth. server	From the drop-down, select a remote authentication server (LDAP, RADIUS, or SAML) or select local users.
Synchronization set	Select from the following two options to synchronize users/groups: <ul style="list-style-type: none"> <li>All users/groups (default)</li> <li>Custom (<b>Note:</b> If selected, you must select the user groups from the Available Groups list and move them to the Chosen Groups list. Only selected user groups and members of those user groups are synced. For remote LDAP servers, only groups with the list of users are included. These are groups without LDAP filter.)</li> </ul>

## User Attributes Mapping

Parameter	Description
User name	Enter the user name. The default value is <code>userName</code> .
First name	Enter the user's first name. The default value is <code>name.givenName</code> .
Last name	Enter the user's last name. The default value is <code>name.familyName</code> .
Email	Enter the user's email address. The default value is <code>emails[type eq "work"].value</code> .
Phone number	Enter the user's phone number.
Mobile number	Enter the user's mobile number. The default value is <code>phoneNumbers[type eq "mobile"].value</code> .
User display name	Enter the user's display name. The default value is <code>displayName</code> .
Company	Enter the user's company name. The default value is <code>organization</code> .
Department	Enter the user's department. The default value is <code>department</code> .
Title	Enter the user's title. The default value is <code>title</code> .
Active	Enter the user status. The default value is <code>active</code> . Custom fields configured in <i>Authentication&gt;User Account Policies&gt;Custom User Fields</i> .

## Group Attributes Mapping

Parameter	Description
Group display name	Enter the group's display name. The default value is <code>displayName</code> .
Group members	Enter the group's members. The default value is <code>members</code> .

### Sync users/groups to FortiToken Cloud

1. From the main menu, click *Authentication > SCIM > Service Provider*.
2. Checkmark the SCIM service provider that you've just created.
3. Click *Edit* to open the Edit SCIM Service Provider page.
4. Click *Sync*.

### Add a local user

1. From the main menu, click *Authentication > User Management > Local Users > Create New*.
2. Make the required entries and selection as shown in the following screenshot.
3. Click *Save*.

Create New Local User

Username:

Password creation:

Specify a password

Password:

••••••••

Password confirmation:

☐ Allow RADIUS authentication

☐ Force password change on next logon

Role

Role:

Administrator

Sponsor

User

Account Expiration

☐ Enable account expiration

IAM

Account:

[ Please Select ]

Save

User Information

Display name:

First name:

Email:

emailid1@email-id.com



The user that you have just created is now added to FortiAuthenticator and FTC (the SCIM server).

1. Checkmark the user of interest, and click *Delete*.
2. Click the Yes I'm sure to the confirmation.



The selected user is now removed from both FortiAuthenticator and FTC.

## Known issues and special notes

### Common to all SCIM client applications:

- FTC (the SCIM server) allows no more than eight fields in a user profile to be updated at any given time.

### Okta-specific:

- For Primary Phone Type, you must specify "mobile".
- Users deactivated and deleted are not reflected on FTC.
- When deactivating and re-activating a user, you must assign the user to the application again.
- Users disabled on ftc and its not removed from the group.
- Users added to exiting groups do not show up on FTC.
- Users removed from one group and then assigned to another are not reflected on FTC.

### Azure-specific:

Because Azure auto-provisioning happens once every 40 minutes, the following operations carried out on Azure are not reflected on FTC in real time:

- Removing users from a group.
- Re-assigning users to a group.
- Adding new users to exiting groups.
- Removing users from one group and assigning them to other groups

### FortiAuthenticator-specific:

- Assigning users to or removing them from a user group
- Re-assigning users to another group
- Removing user groups
- Adding users to an exiting group
- Moving users between groups

## Management Applications

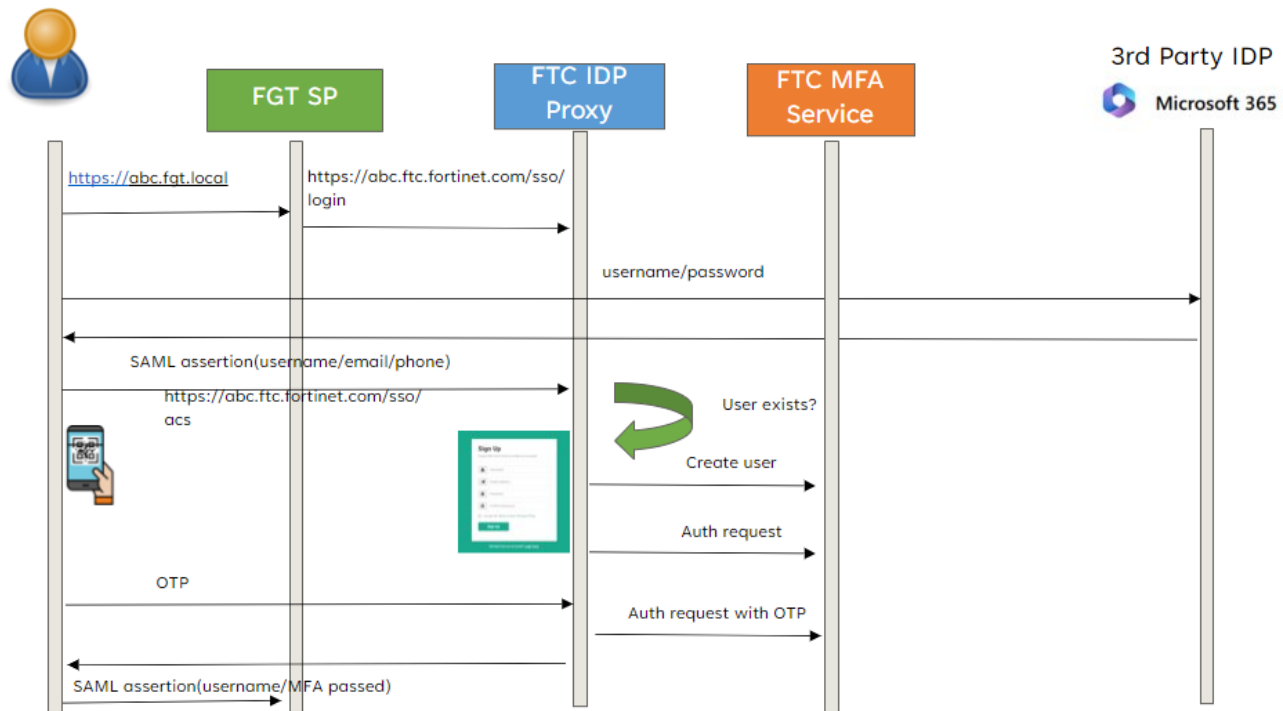
Starting with its 23.1.a release, FortiToken Cloud introduces the management applications as a special type of web application. It is a solution for remote API access and management of customer resources, such as realms, applications, users, and tokens, etc.

You can access the feature by selecting *Applications > Mgmt Applications*, where you can view/create/edit/delete management applications.

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

## Use SSO applications

An SSO application serves as a bridge or gateway between a federation of SAML IdPs and a federation of SAML SPs, as illustrated in the following diagram:



To an SP, an IdP Proxy looks like an ordinary IdP. Likewise, to an IdP, an IdP Proxy looks like an SP. Thus an IdP Proxy has the combined capability of both an IdP and an SP.

With FTC providing the SAML and OIDC IdP interface, we can move the application into the scope of FTC SaaS service and make use of existing SSO protocol to integrate with the Fortinet ecosystem, which already supports SAML log-in. This relieves Fortinet devices from private integration with FTC, as long as they use SAML SP for authentication. FTC can introduce new features such as FIDO and adaptive authentication without downstream support.

Furthermore, customers no longer need to worry about device serial numbers and FTC license ownership.

## Use Cases



- Most IdP vendors require a subscription for full access to their services. Be sure to check with your IdP and SPs vendors to see if a premium subscription is required to access their services.
- This feature is only available to FTC customers with a full subscription. It is not available to trial customers.

One example would be that a customer already has a setup with an IdP and multiple SPs, but doesn't have MFA. Let's say that they're using Google as the IdP to provide the user source and SSL VPN through a FortiGate to be the SP. With their current setup, if their end-users try to log in through SSL VPN, they will be directed to the Google login page, where once they input their username and password, they will immediately be let into SSL VPN. With FTC's IdP Proxy setup, the end-users will experience following instead:

Google login > FTC 2FA OTP page > FGT SSL VPN

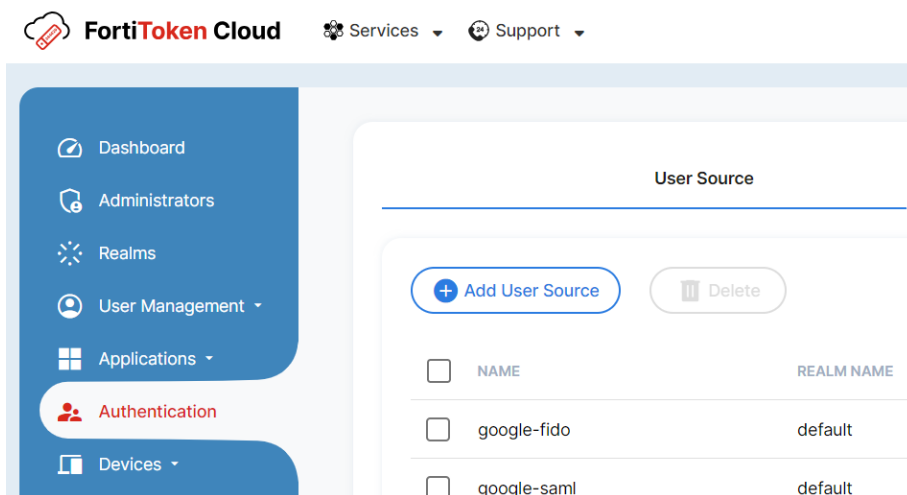
- Example 1: Google SAML as IdP and FortiGate SSL VPN as SP on page 148
- Example 2: Azure as SAML IdP and FortiGate as SP on page 158
- Example 3: Google OIDC as IdP on page 160
- Example 4: Azure OIDC as IdP on page 165
- Example 5: FortiGate IPsec as SP on page 169
- Example 6: ZTNA application gateway with SAML as SP on page 176

## Example 1: Google SAML as IdP and FortiGate SSL VPN as SP



The FortiGate device used in this example setup is running on FortiOS 7.4.3.

1. Go to **Authentication > User Source** and click **Add User Source**:



2. Configure general settings. Note that Google cannot use Login Hint:



## General ▾

Name*	<input type="text" value="google-saml"/>
prefix	<input type="text" value="MU"/>
Username Identity	<input type="text" value="username"/>
Favicon URL	<input type="text"/>
Login Hint ⓘ	<input type="text" value="Informing the IdP of who you would like to authenticate"/>
Realm*	<input type="text" value="default"/>
Interface*	<input type="text" value="SAML 2.0"/>
Domains	<input type="text" value="Select Domain"/> <span>+</span>

3. On [admin.google.com](https://admin.google.com), go to **Apps > Web and mobile apps**, then add a custom SAML app:

The screenshot shows the Google Admin console interface. On the left, the 'Apps' menu is expanded, and 'Web and mobile apps' is selected. The main content area shows the 'Apps (4)' list with a table of existing apps. A dropdown menu is open from the 'Add app' button, showing options to 'Add private Android app', 'Add private Android web app', and 'Add custom SAML app'. The 'Add custom SAML app' option is selected, opening a dialog titled 'Add custom SAML app'. The dialog has a blue header bar with a close button and the title. Below the header, there is a section for 'App details' with a link to 'Learn more'. The 'App name' field is filled with 'faz\_lab' and has a red squiggly underline. The 'Description' field is empty.

Admin

Search for users, groups or settings

Apps > Web and mobile apps

Apps (4) Add app Settings

+ Add a filter

	Name ↑		User access
<input type="checkbox"/>	fa	Add private Android app	
<input type="checkbox"/>	fa	Add private Android web app	ON for everyone
<input type="checkbox"/>	fp	Add custom SAML app	ON for everyone

admin.google.com/ac/apps/unified

**Add custom SAML app**

**App details**

Enter details for your custom SAML app. This information is shared with app users. [Learn more](#)

App name

faz\_lab

Description

4. Download the metadata. Then grab the certificate from this page and click continue:

✕ Add custom SAML app

✓ App details — 2 Google Identity Provider detail — 3 Service provider details — 4 Attribute mapping

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

Option 1: Download IdP metadata

[DOWNLOAD METADATA](#)

5. Provide SP metadata details from FTC (unter Interface Detail) on Google:

#### SP Metadata

Entity ID ⓘ [https://auth.fortinet.com/saml/MU\[redacted\]/proxy\\_metadata/](https://auth.fortinet.com/saml/MU[redacted]/proxy_metadata/)

ACS URL ⓘ [https://auth.fortinet.com/saml/MU\[redacted\]/proxy\\_acs/](https://auth.fortinet.com/saml/MU[redacted]/proxy_acs/)

SLO URL ⓘ [https://auth.fortinet.com/saml/MU\[redacted\]/proxy\\_logout/](https://auth.fortinet.com/saml/MU[redacted]/proxy_logout/)

✕ Add custom SAML app

**Service provider details**

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL  
[https://auth.fortinet.com/saml/MU\[redacted\]/proxy\\_acs/](https://auth.fortinet.com/saml/MU[redacted]/proxy_acs/)

Entity ID  
[https://auth.fortinet.com/saml/MU\[redacted\]/proxy\\_metadata/](https://auth.fortinet.com/saml/MU[redacted]/proxy_metadata/)

Start URL (optional)

☐ Signed response

6. In this example we map the primary email attribute to the username attribute.

✕ Add custom SAML app

**Attributes**

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with \* are mandatory. [Learn more](#)

Google Directory attributes	App attributes
Basic Information >	
Primary email	username

[ADD MAPPING](#)

7. On FTC, you can click Import Metadata and import the metadata file you downloaded earlier in step 4. Note that Google does not have a Logout URL:

## IdP Metadata

Import Metadata

Entity ID ⓘ

https://accounts.google.com/o/saml2?idpid=C0

Login URL ⓘ


<https://accounts.google.com/o/saml2/idp?idpid=C0>


Logout URL ⓘ


8. Load the certificate that you got from step 4 here in FTC, and you can click save now to save the entire user source setting:


[illegible]


- 9. On FTC, go to **Applications > SAML Applications** and then **Add SAML Application**:**


**FortiToken Cloud**


 Services


 Support


 Dashboard


 Administrators


 Realms


 User Management


 Users

 User Groups


 Applications


 FortiProducts

 Web Applications

 Mgmt Applications

SAML Applications





<input type="checkbox"/>	NAME	REALM NAME	INTERFACE
<input type="checkbox"/>	sslvpn	default	SAML
<input type="checkbox"/>	faz_107	default	SAML

- ## 10. Configure General settings:

## General ▾

Name*	sslvpn
Realm*	default ▾
Adaptive Auth Profile	Select Profile ▾
Custom Branding ⓘ	Default Branding ▾ +
Session Timeout	15 minutes
Default Permission	Allow ▾

11. On FGT, we assume you already have SSL VPN set up. Create a new single sign-on under **User & Authentication** > **Single Sign-On**:

Dashboard >

Network >

Policy & Objects >

Security Profiles >

VPN >

User & Authentication ▾

User Definition

User Groups

Guest Management

LDAP Servers

RADIUS Servers

Single Sign-On ☆

Authentication Settings

+ Create new

Edit

Delete

+ Search

Name	SP certificate	SP entity ID
testsaml		http://10.160. /remote/saml/metadata/

12. Put your SSLVPN address into the **Address** field and take note of the **Entity ID**, **Assertion consumer service URL**, and **Single logout service URL**:

New Single Sign-On

1 ————— 2

Input Service Provider Details      Input Identity Provider Details

Name

Service Provider Configuration

Address

Entity ID

Assertion consumer service URL

Single logout service URL

Certificate ☐

[Next](#) [Cancel](#)

13. Input the details into the **SP Metadata** section on FTC:

SP Metadata [Import Metadata](#)

Entity ID

ACS URL

SLO URL

14. For Interface Detail we're setting it like this in this example:

Interface Detail ▾

Signing Algorithm

IdP Signing Cert  [+](#)


Name ID Attribute


SAML request signed by SP ☐


SP Signing Cert  [⬆](#)

15. Take the IdP Metadata and input it into the next page on the FGT single sign-on wizard:

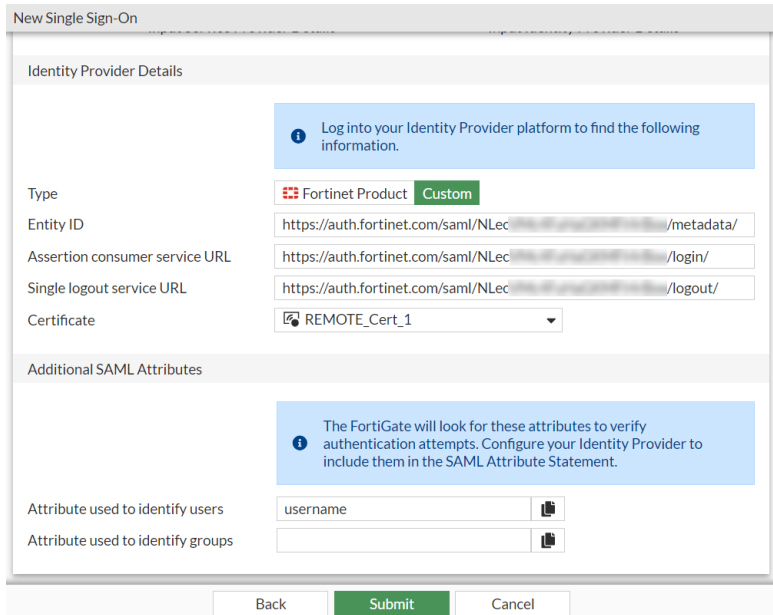
## IdP Metadata

Entity ID ⓘ [https://auth.fortinet.com/saml/NLec\[redacted\]/metadata/](https://auth.fortinet.com/saml/NLec[redacted]/metadata/) 

SSO URL ⓘ [https://auth.fortinet.com/saml/NLec\[redacted\]/login/](https://auth.fortinet.com/saml/NLec[redacted]/login/) 


SLO URL ⓘ [https://auth.fortinet.com/saml/NLec\[redacted\]/logout/](https://auth.fortinet.com/saml/NLec[redacted]/logout/) 


16. Configure as such and click **Submit**. You then need to add the SAML server that you've just created to the user group and your SSLVPN firewall policy as well.




17. To obtain the certificate, go to **Applications > SAML Applications** and then click the 3-dotted menu of your SAML application > click Details > download the signing certificate > import into FGT:

## IdP Metadata

Entity ID ⓘ [https://\[redacted\]/](https://[redacted]/) 

SSO URL ⓘ [https://\[redacted\]](https://[redacted]/) 

SLO URL ⓘ [https://\[redacted\]](https://[redacted]/) 

Signing Certificate ⓘ [Click to download the Signing Certificate](#)

18. On FTC make sure to map your new SP to the IdP you made earlier. Then you can click **Save** and now you should have both the IdP and SP parts configured:

## Authentication ▾

User Source  +
randy-azure-saml ×
fortisase-google-idp ×
randy-okta-saml ×
randy-google-saml ×
Clear All

Default User Source ⓘ

randy-google-saml ▾

Select Default User Source

randy-azure-saml

fortisase-google-idp

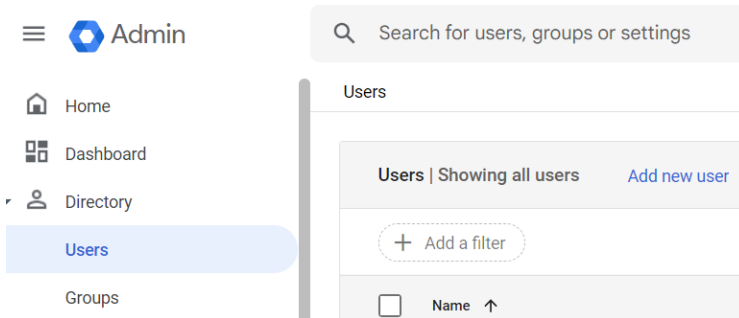
randy-okta-saml

randy-google-saml

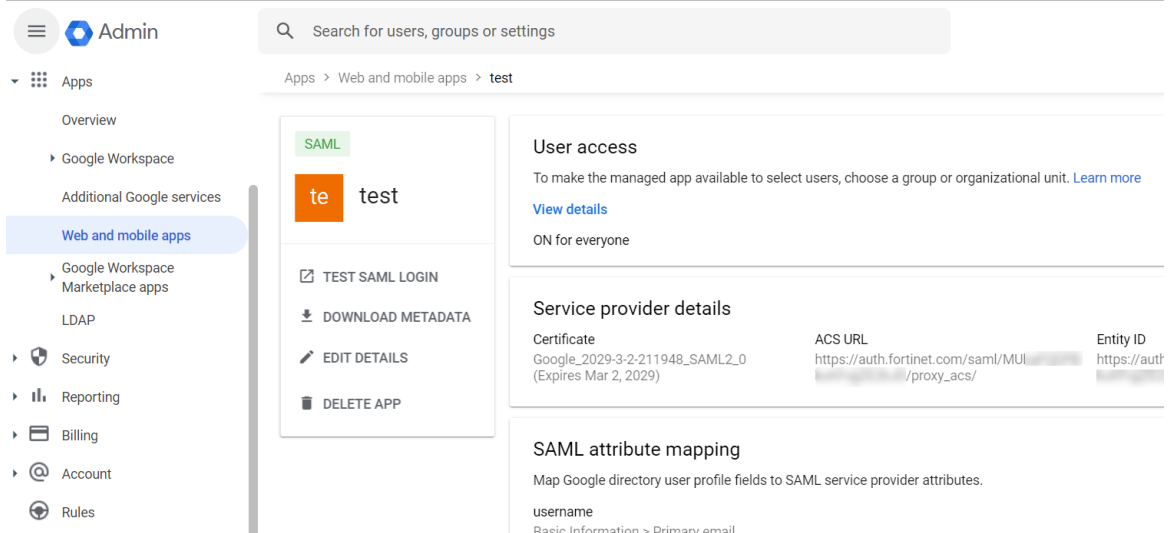
Attribute Mapping ▾

Save

19. To add users on Google, go to **Directory > Users > Add new user**:



20. You can manage user access here. In our example we've turned the access on for all users on our Google account:



21. On FTC you need to add the same user using the same username (we're using their email in our example) by going to **User Management > Users > Batch Add**:

FortiToken Cloud Services Support

Dashboard Administrators Realms User Management **Users** User Groups Applications Authentication

Users

New FTK Token Add User Alias Auto-Assign FTK Batch Add Delete

Filter Search by name or email

USERNAME	STATUS	MFA	EMAIL	MOBILE PHONE	REF COUNT
@	✓	→	Email	@	0

Batch Add Users

Download CSV Template Upload CSV file

Realm default

Users

Username Email Mobile Phone

test@ test@test.com +1

Add New User Total 1 user(s)

Cancel Save

22. Once the users are added, we now need to set up FortiClient to be used to log in to this SSLVPN setup. Firstly, we'll need to change the `remoteauthtimeout` parameter in the CLI as its default value of 5 is too short for end-users to properly login to SSLVPN this way:

```
config system global
    set remoteauthtimeout 300
end
```

In this example, we set `remoteauthtimeout` to the maximum value of 300. But feel free to set it to a lower value to suit your needs as long as it gives your end-users enough time to go through the login process.

23. In FortiClient, create a new VPN connection as shown in the following illustration. You can choose to use FortiClient's internal browser or your own computer's default browser if you select "Use external browser as user-agent for saml user authentication."



### Edit VPN Connection

VPN SSL-VPN IPsec VPN XML

Connection Name

Description

Remote Gateway  ✕  
+Add Remote Gateway

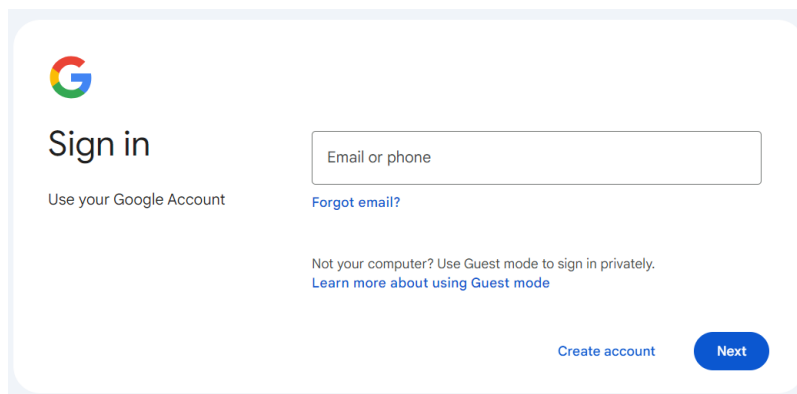
☒ Customize port

Single Sign On Settings ☒ Enable Single Sign On (SSO) for VPN Tunnel  
☐ Use external browser as user-agent for saml user authentication  
☐ Enable auto-login with Azure Active Directory

Client Certificate None ▼  
☐ Enable Dual-stack IPv4/IPv6 address

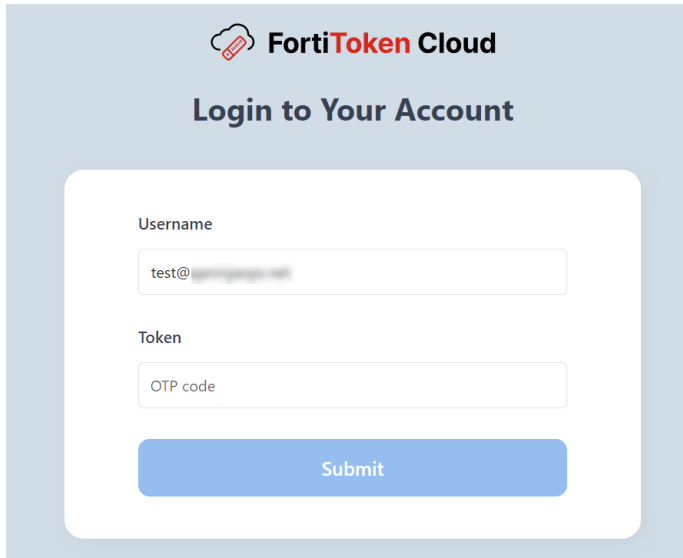
Cancel Save

24. Click **Save**. You will be taken to the following Google's sign-in page when trying to connect to the VPN:



The image shows the Google sign-in page. It features the Google logo at the top left, followed by the text "Sign in". Below this is a text input field labeled "Email or phone". To the left of the input field is the text "Use your Google Account". Below the input field is a link "Forgot email?". At the bottom, there is a link "Create account" and a blue button labeled "Next".

25. Log in, and you are now taken to the OTP page:



**FortiToken Cloud**

### Login to Your Account

Username

test@

Token

OTP code

Submit

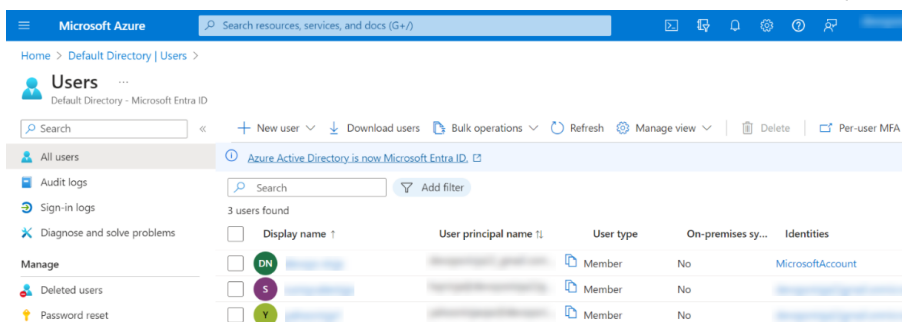
26. Verify the token using your selected MFA method of choice from when you created the user on FTC earlier. Now it should let the end-user log in to the SSLVPN through FortiClient.

## Example 2: Azure as SAML IdP and FortiGate as SP



The FortiGate device used in this example setup is running on FortiOS 7.4.3.

1. Create users on Azure on [portal.azure.com](https://portal.azure.com). Go to **Home > Default Directory > Users > All users > New user**:



2. Create a single sign-on app in **Home > Enterprise Application**. Here is also where you will be pasting in your SP metadata just like with the Google example:

Microsoft Azure Search resources, services, and docs (G+)

Home > idp-test

## idp-test | SAML-based Sign-on

Enterprise Application

Upload metadata file Change single sign-on mode Test this application Got feedback?

### Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating idp-test.

**1 Basic SAML Configuration** Edit

Identifier (Entity ID)	https://auth.fortinet.com/saml/QH
Reply URL (Assertion Consumer Service URL)	https://auth.fortinet.com/saml/QH
Sign on URL	/proxy_acs/
Relay State (Optional)	Optional
Logout Url (Optional)	https://auth.fortinet.com/saml/QH
	/proxy_logout/

**2 Attributes & Claims** Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname

3. While creating the app, add a claim for the username. In our example we'll set it like this:

Home >

## Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname
username	SAML	user.userprincipalname

4. Here is the example FTC config for Azure as the IdP. Note that the Login Hint should be "login\_hint" for Azure:

## General ▾

Name*	<input type="text" value="azure-saml"/>
prefix	<input type="text" value="QH"/>
Username Identity	<input type="text" value="username"/>
Favicon URL	<input type="text"/>
Login Hint ⓘ	<input type="text" value="login_hint"/>
Realm*	<input type="text" value="default"/>
Interface*	<input type="text" value="SAML 2.0"/>
Domains	<input type="text" value="Select Domain"/> <span>+</span>

## IdP Metadata

[Import Metadata](#)

Entity ID ⓘ	<input type="text" value="https://sts.windows.net/a0"/>
Login URL ⓘ	<input type="text" value="https://login.microsoftonline.com/a0"/>
Logout URL ⓘ	<input type="text" value="https://login.microsoftonline.com/a0"/>

5. Click **Save** after you're finished. For the rest of the setup, the SP config should be the exact same as the other example with Google. See [Example 1: Google SAML as IdP and FortiGate SSL VPN as SP on page 148](#).

## Example 3: Google OIDC as IdP



In this example, the SP can be any supported Fortinet application. For a complete list of supported Fortinet applications, see [Compatible Fortinet applications on page 36](#).

1. In order to set up OIDC for Google you need to create a new project (i.e., Pick a project name and click on CREATE) in your Google Cloud Platform console:

Google Cloud Platform

New Project

You have 10 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name \*

Quarkus Renarde Todo

Project ID: quarkus-renarde-todo. It cannot be changed later. [EDIT](#)

Location \*

No organisation [BROWSE](#)

Parent organisation or folder

[CREATE](#) [CANCEL](#)

- Now make sure you select your project in the top selector, and click on the left-hand bar menu on APIs and Services > OAuth consent screen:

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Azure Active Directory

Azure Active Directory | App registrations

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Enterprise applications

Devices

App registrations

New registration

Refresh

Download

Preview features

Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Lib security updates but we will no longer provide feature updates. Applications will need to be upgraded to Mic

Start typing a name or Application ID to filter these results

Display name

Application

- Select **External** to authorize any Google user to log in to your application and press **CREATE**:

Google Cloud Platform

Quarkus Renarde Todo

oauth

APIs and services

OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

☐ Internal

Only available to users within your organisation. You will not need to submit your app for verification. [Learn more about user type](#)

☒ External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

[CREATE](#)

- Now you can fill in your application name, your support email, your developer contact information and press **SAVE AND CONTINUE**:

**APIs & Services**

- Enabled APIs & services
- Library
- Credentials
- OAuth consent screen**
- Page usage agreements

**Edit app registration**

User support email \*

For users to contact you with questions about their consent. [Learn more](#)

**App logo**

This is your logo. It helps people recognize your app and is displayed on the OAuth consent screen.

After you upload a logo, you will need to submit your app for verification unless the app is configured for internal use only or has a publishing status of "Testing". [Learn more](#)

Logo file to upload [BROWSE](#)

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

**App domain**

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

**Authorized domains**

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

[+ ADD DOMAIN](#)

**Developer contact information**

Email addresses \*

5. Do not add any scopes on the next page, and press **SAVE AND CONTINUE**:

**Google Cloud Platform** Quarkus Renarde Todo oauth

**APIs and services**

- Dashboard
- Library
- Credentials
- OAuth consent screen**
- Domain verification
- Page usage agreements

**Edit app registration**

OAuth consent screen — **Scopes** — Test users — Summary

Scopes express the permissions that you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

[ADD OR REMOVE SCOPES](#)

**Your non-sensitive scopes**

API ↑	Scope	User-facing description
No rows to display		

**Your sensitive scopes**

Sensitive scopes are scopes that request access to private user data.

API ↑	Scope	User-facing description
No rows to display		

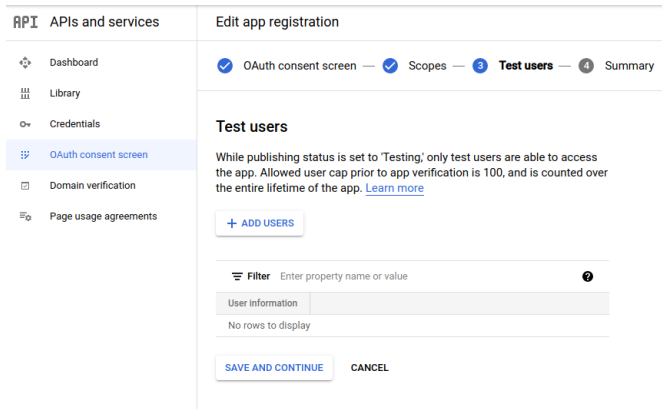
**Your restricted scopes**

Restricted scopes are scopes that request access to highly sensitive user data.

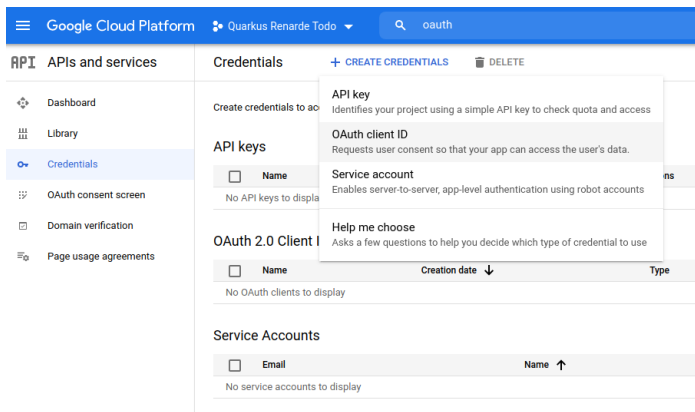
API ↑	Scope	User-facing description
No rows to display		

[SAVE AND CONTINUE](#) [CANCEL](#)

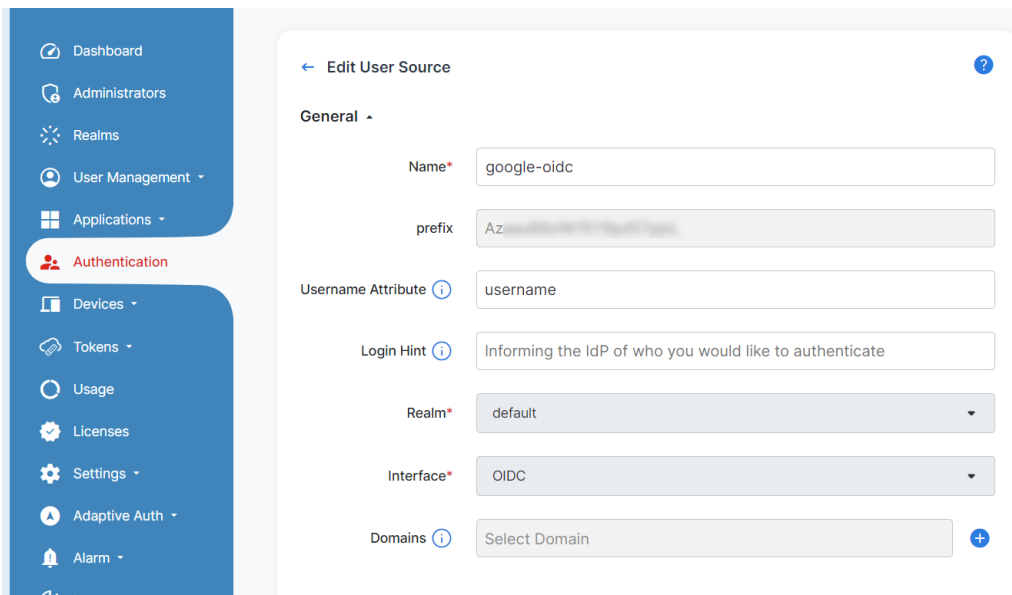
6. Add some test users on the next page if you'd like, and press **SAVE AND CONTINUE**:



7. Click on the top menu **CREATE CREDENTIALS > OAuth client ID**:



8. Now before we continue to the next page, on FTC, create a new user source and set the **Interface** to **OIDC**:



9. Take note of the **Callback URL** in the following image:

## Interface Detail ▾

## Callback Info

Callback URL ⓘ <https://auth.fortinet.com/oidc/Az-.../callback/> ⓘLogout Redirect URI ⓘ <https://auth.fortinet.com/oidc/Az-.../logout/> ⓘ

## OpenID Configuration

[Import Client Secret Configuration](#)

10. Select **Web application** as **Application type**, and add the Callback URL in the **Authorized redirect URIs** list, then press **CREATE**:

API

APIs & Services

Enabled APIs & services

Library

Credentials

OAuth consent screen

Page usage agreements

←

Create OAuth client ID

1

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ⓘ

For use with requests from a browser

+ ADD URI

Authorized redirect URIs ⓘ

For use with requests from a web server

URIs 1 \*

<https://auth.fortinet.com/oidc/Az-.../callback/>

+ ADD URI

Note: It may take 5 minutes to a few hours for settings to take effect

CREATE

CANCEL

11. Then copy your **Client ID** and **Client Secret** and fill out the rest of the fields like this:

OpenID Configuration

[Import Client Secret Configuration](#)

Issuer ⓘ

<https://accounts.google.com>

Auth URI ⓘ

<https://accounts.google.com/o/oauth2/auth>

Token URI ⓘ

<https://oauth2.googleapis.com/token>

User Info URI ⓘ

<https://openidconnect.googleapis.com/v1/userinfo>

Logout URI ⓘ

Client ID ⓘ

10...apps.googleusercontent.com

Client Secret ⓘ

\*\*\*\*\*

Attribute Mapping ▾

username

email

ⓘ



In the example above, we are mapping the "username" attribute to "email" because we're identifying the users on Google via email, and the attribute we're using to identify the users is "username."



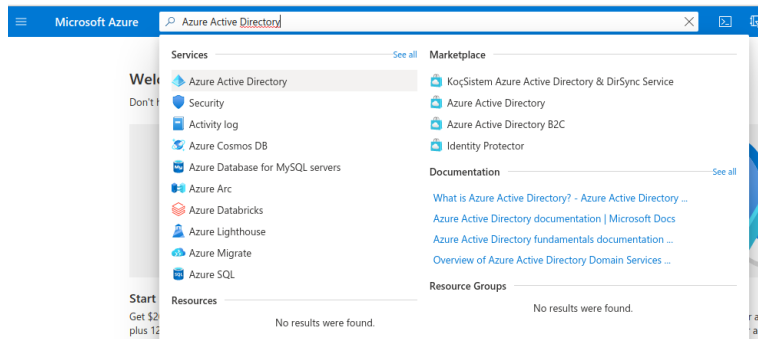
- When you're done, click **Save**. This should work with the existing SPs that you've set up on FTC.

## Example 4: Azure OIDC as IdP

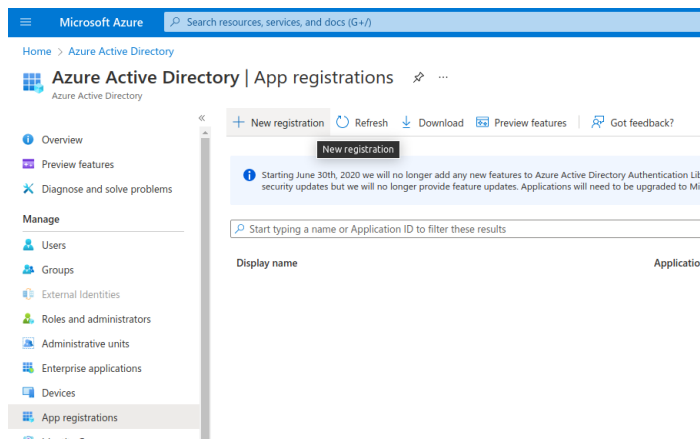


In this example, the SP can be any supported Fortinet application. For a complete list of supported Fortinet applications, see [Compatible Fortinet applications on page 36](#).

- In order to set up OIDC for Microsoft you need to go to your Microsoft Azure Portal, and search for Azure Active Directory, then click on it:



- Once there, on the left side under **Manage**, click on **App registrations** then click on **New registration**:



- On FTC, create a new user source and set the Interface to OIDC just like in the Google OIDC example. Take note of the callback URL. Then, on the next page in Azure, fill in your application name, select **Accounts** in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) to allow anyone to log in, and add a Web Redirect URI with the callback URL from FTC. Then click on **Register**:

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory | App registrations >

## Register an application

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (Default Directory only - Single tenant)  
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)  
☒ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

4. On that resulting page, copy the **Client Id** (under Application (client) ID), then click on **Add a certificate or secret**:

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory | App registrations >

## OIDC

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Essentials

Display name : [OIDC](#)

**Application (client) ID** : [\[redacted\]](#)

Object ID : [\[redacted\]](#)

Directory (tenant) ID : [\[redacted\]](#)

Supported account types : [Multiple organizations](#)

Client credentials : [0 certificate, 1 secret](#)

Redirect URIs : [1 web, 0 spa, 0 public client](#)

Application ID URI : [api://\[redacted\]](#)

Managed application in L... : [OIDC](#)

5. Now, under **Client secrets (0)**, click on **New client secret**:

Search (Ctrl+F)

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

**Certificates & secrets**

Token configuration

API permissions

Expose an API

Owners

Manifest

Credentials enable confidential applications to identify themselves to the authentication scheme. For a higher level of assurance, we recommend using a certificate (instead of a secret string) that the application uses to prove its identity when requesting a token.

Application registration certificates and secrets can be found in the tabs below.

Certificates (0) **Client secrets (0)**

A secret string that the application uses to prove its identity when requesting a token.

**+ New client secret**

Description	New client secret	Expires	Value
No client secrets have been created for this application.			

6. Click on **Add** in that dialog without changing anything:

### Add a client secret

Description

Expires

**Add** **Cancel**

7. On the resulting page, copy your **Secret Value**:

Home > Default Directory | App registrations > OIDC

**OIDC | Certificates & secrets**

Search << Got feedback?

Overview  
Quickstart  
Integration assistant

**Manage**  
Branding & properties  
Authentication  
**Certificates & secrets**  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
test	4/18/2026	hsT*****	9*****

8. Going back to the FTC configuration, note that if your users do not have any email set on them in Azure, then you'll need to configure a custom username attribute. In our example, we didn't have any email configured on our Azure users so we're configuring the username attribute with Microsoft Azure's "preferred\_username" field in order for FTC to be able to identify the username from the access token. You can read up more in Microsoft's documentation about which fields are included their OIDC access tokens if you wish to use different fields:

← Edit User Source ?

**General**

Name\* azure-oidc

prefix C\*\*\*\*\*

Username Attribute ⓘ preferred\_username

Login Hint ⓘ Informing the IdP of who you would like to authenticate

Realm\* default

Interface\* OIDC

Domains ⓘ Select Domain +

9. And here is what we are going to put in the OpenID Configuration section for our example:

OpenID Configuration Import Client Secret Configuration

Issuer i

Auth URI i

Token URI i

User Info URI i

Logout URI i

Client ID i

Client Secret i

10. If you used "preferred\_username", make sure to configure the attribute mapping as well:

Attribute Mapping ^

username  II

Add your customized attribute  +

Save

11. You already got the client and the secret from earlier. If you need to reference the other fields, you can get it from here in Azure by clicking Endpoints in the Overview page of your app:

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Overview' page for an 'OIDC' application is visible, with the 'Endpoints' tab selected. The 'Endpoints' panel on the right lists the following endpoints:

- OAuth 2.0 authorization endpoint (v2): <https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize>
- OAuth 2.0 token endpoint (v2): <https://login.microsoftonline.com/organizations/oauth2/v2.0/token>
- OAuth 2.0 authorization endpoint (v1): <https://login.microsoftonline.com/organizations/oauth2/authorize>
- OAuth 2.0 token endpoint (v1): <https://login.microsoftonline.com/organizations/oauth2/token>
- OpenID Connect metadata document: <https://login.microsoftonline.com/organizations/v2.0/.well-known/openid-configuration>
- Microsoft Graph API endpoint: <https://graph.microsoft.com>
- Federation metadata document: <https://login.microsoftonline.com/a0.../federationmetadata/2007-06/federationmetadata.xml>
- WS-Federation sign-on endpoint: <https://login.microsoftonline.com/a0.../wsfed>
- SAML-P sign-on endpoint: <https://login.microsoftonline.com/a0.../saml2>

The 'Essentials' section on the left shows the following details:

- Display name: [OIDC](#)
- Application (client) ID: 37...
- Object ID: f2...
- Directory (tenant) ID: a0...
- Supported account types: [Multiple organizations](#)

12. After clicking Save in FTC, this Azure OIDC IdP should be ready to be added into your FTC IdP proxy setup.

## Example 5: FortiGate IPsec as SP

1. On the FTC portal, click *Applications > SAML Applications > Add SAML Application*.
2. In the *General* and *Interface Detail* sections, make the required entries and selections.

← Edit Application

General ▾

Name\*

Realm\*

Adaptive Auth Profile

Custom Branding ⓘ  +

Session Timeout

Default Permission

Interface Detail ▾

Signing Algorithm

IdP Signing Cert ⓘ  +

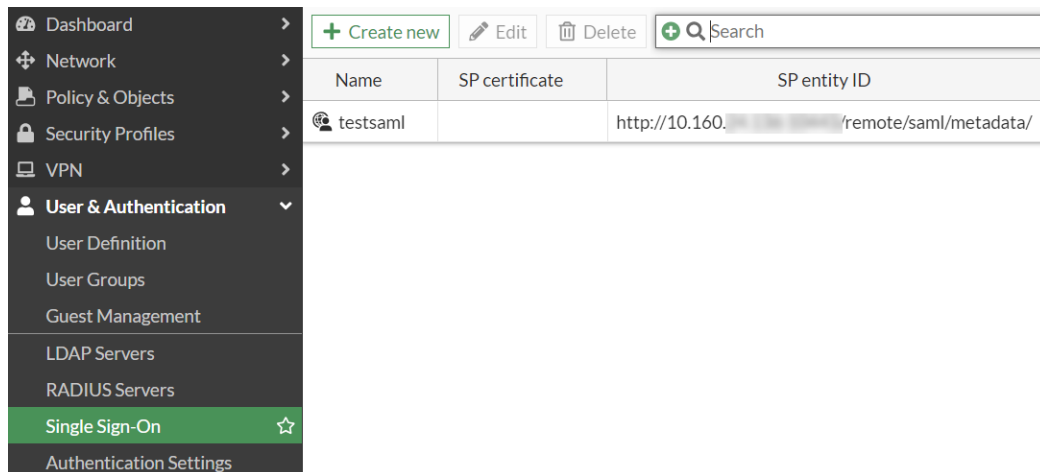
Name ID Attribute ⓘ

SAML request signed by SP ☐

SP Signing Cert ⓘ 

⬆

3. Leave the FTC GUI page open, launch the FortiGate GUI, and click *User & Authentication > Single Sign-On* to create a new single sign-on instance.



- In the *Address* field, enter the IPsec address that you want to use. In this example, we use Port 9443 for the `auth-ike-saml-port`, so make sure to append the port number to the address. Then take note of the Entity ID, Assertion consumer service URL, and Single logout service URL, and copy and paste them into the *SP Metadata* section in the FTC SAML app that you are adding in Steps 1 through 2.

The screenshot shows the 'New Single Sign-On' configuration window. It has a progress bar at the top with two steps: 1 (active) and 2. The main section is titled 'Input Service Provider Details'. It contains the following fields:

- Name:
- Service Provider Configuration section:
  - Address:
  - Entity ID:
  - Assertion consumer service URL:
  - Single logout service URL:
- Certificate: ☐

At the bottom are 'Next' and 'Cancel' buttons.

- Click *Next*.
- Then go back to the FortiGate GUI, copy the Entity ID, SSO URL, and SLO URL from the IdP Metadata section on FTC to the Identity Provider Details section on FortiGate.

7. Go back to the FTC portal to complete configuring the SAML app that you left off in Step 2 by clicking *Applications > SAML Applications > Authentication* to configure its authentication settings, (optionally) add any customized attribute that you may want, and click *Save*.
8. Click *Applications > SAML Applications*, locate the SAML application that you have created. Then click the 3-dot menu on the far-right side and select *Details*, download the signing certificate to your local machine.

9. Go back to the FortiGate GUI (Step 4 above), and import the certificate to the FortiGate, and click *Submit*.
10. Now on the FortiGate, launch the Console interface and start configuring the IPsec VPN using the following CLI command:

```
config system global
    set auth-ike-saml-port 9443
end
```

11. The `ike-saml-server` setting enables a configured SAML server to listen on a FortiGate interface for SAML authentication requests from FortiClient remote access IPsec VPN clients. Currently, this setting can only be configured in the CLI as follows. Here, "vpnsaml" is the name we gave the single sign-on setting we configured earlier:

```
config system interface
    edit <name>
        set ike-saml-server vpnsaml
```

```

    next
end

```

12. Next, configure the IPsec VPN certificate either from the FortiGate GUI or Console interface.

To configure the IPsec VPN certificate from the GUI:

- a. Go to *User & Authentication > Authentication Settings*, and select the certificate from the Certificate drop-down menu.
- b. Import the certificate on the FortiGate by following the procedures in [Import a certificate](#).

To configure the IPsec VPN certificate in the CLI:

- a. Make sure that the certificate (i.e., VPN-Certificate) has been imported to the FortiGate.
- b. Execute the following commands:

```

config user setting
    set auth-cert "VPN_Certificate"
end

```

13. Configure IPsec VPN on the FortiGate with FortiClient as the dial-up client:

- a. Go to *VPN > IPsec Tunnels*.
- b. Click *Create New > IPsec Tunnel*.  
The *VPN Creation Wizard* is displayed.
- c. Enter the *Name* as *FCT\_SAML*.  
**Note:** This example does not use the VPN wizard for the IPsec tunnel configuration, but configures a *Custom* IPsec tunnel instead.
- d. Configure the *Template* type as *Custom*.
- e. Click *Next*.
- f. Configure the following options:

Parameter	Description
Name	<i>FCT_SAML</i>
Comments	(Optional)
Network	
IP Version	<i>IPv4</i>
Remote Gateway	<i>Dialup User</i>
Interface	<i>port1</i> Select the IPsec tunnel gateway interface.
Mode Config	<i>Enable</i>
Use system DNS in mode config	(Optional) Enable FortiClient to use the host's DNS server after it connects to VPN.
Assign IP From	<i>Enable</i> Select Address/Address Group from the dropdown list.
IPv4 mode config	



Parameter	Description
Client Address Range	<i>VPN_Client_IP_Range</i> <i>VPN_Client_IP_Range</i> is configured from <i>10.212.134.1</i> to <i>10.212.134.200</i> . If it is not already created, select <i>Create &gt; Address</i> from the dropdown menu to create a new address object. See <a href="#">Subnet</a> for more information.
Subnet Mask	<i>255.255.255.255</i>
DNS Server	<i>8.8.8.8</i>
Authentication	
Method	<i>Pre-shared key</i>
Pre-shared key	Enter the pre-shared key of at least six characters.
IKE	
Version	<i>2</i>
Peer Options	
Accept Types	<i>Any peer ID</i>
Phase 1 Proposal	
Encryption	<i>AES128</i>
Authentication	<i>SHA256</i> Select the desired Encryption and Authentication algorithms that should also match with Phase1 Proposals configured on FortiClient. See <a href="#">Configuring IPsec VPN profile on FortiClient</a> .

- g. Keep the other settings as default.
- h. Click *OK*. The newly created IPsec tunnel should now be visible under *VPN > IPsec Tunnels*.
- i. Because IKEv2 uses EAP for user authentication, enable EAP using the following CLI command inside the configured IPsec tunnel for user authentication:


```
config vpn ipsec phase1-interface
  edit "FCT_SAML"
    set eap enable
    set eap-identity send-request
  next
end
```



For advanced custom configurations as per your requirement, see [Remote access](#).

14. Configure firewall policies using the following steps:
  - a. Go to *Policy & Object > Firewall Policy*.
  - b. Click *Create New*.

- c. Make the following entries:

Parameters	Description
Name	<i>IPsec to DMZ</i> Enter the desired name.
Incoming Interface	<i>FCT_SAML</i> Select the configured IPsec tunnel.
Outgoing Interface	<i>DMZ</i> Select the interfaces that FortiClient needs access to when it connects to VPN.
Source	Under <i>Address</i> , select <i>VPN_Client_IP_Range</i> . Under <i>User</i> , select <i>vpnsaml</i> .
 The group under <i>User</i> is the SAML user group configured in the earlier steps. You need to add the single sign-on server you made into a user group and then add that user group to this policy.	
Destination	<i>DMZ subnet</i> Click <i>Create</i> if it is not already created. See <a href="#">Subnet</a> for more information.
Service	<i>ALL</i>

- d. Click *OK*.
- e. Because the IPsec tunnel is configured as a full-tunnel, create another policy to allow traffic from IPsec to Internet and to allow FortiClient to access Internet through IPsec tunnel.

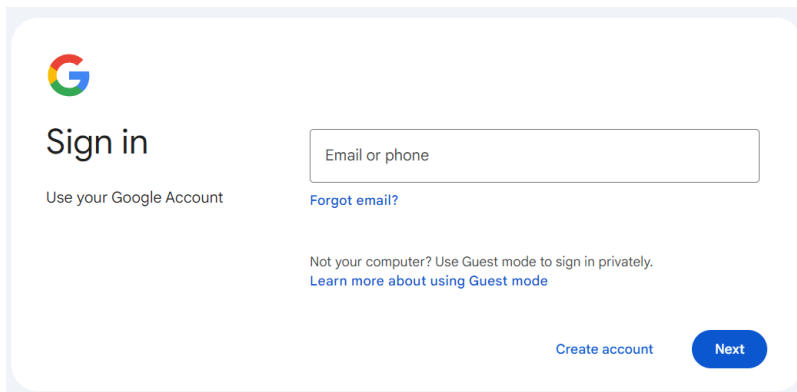
15. Configure the IPsec VPN profile on FortiClient:

- a. In FortiClient, go to *Remote Access > Configure VPN* or *Add a new connection*.
- b. Configure the following settings to set up an IPsec IKEv2 profile on FortiClient:

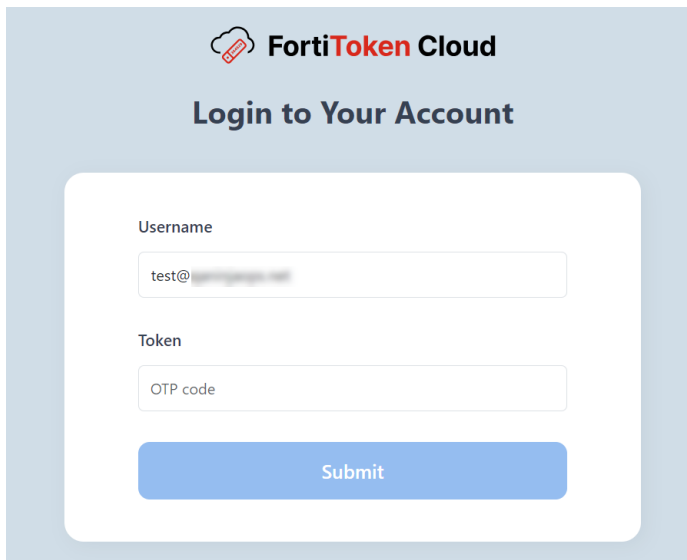
Parameter	Description
Connection Name	<i>VPN-Tunnel</i>
Remote Gateway	<i>&lt;VPN Gateway FQDN&gt; or &lt;VPN Gateway IP&gt;</i>
Authentication Method	<i>Pre-shared key with Enable Single Sign On (SSO) for VPN Tunnel enabled.</i>
Customize port	<i>9443</i>
Advanced Settings > VPN Settings	
IKE	<i>Version 2</i>
Options	<i>Mode Config</i>

To explore additional custom options to configure IPsec VPN profile, see [Configuring an IPsec VPN connection](#).

16. After clicking *Save*, if you try to connect to the VPN, you'll now be taken to your IdP's sign-in page:

A screenshot of the Google Sign in interface. It features the Google 'G' logo at the top left. Below it, the text 'Sign in' is displayed, followed by 'Use your Google Account'. To the right, there is a text input field labeled 'Email or phone'. Below this field is a link that says 'Forgot email?'. Further down, a smaller line of text reads 'Not your computer? Use Guest mode to sign in privately.' with a link 'Learn more about using Guest mode'. At the bottom right, there are two buttons: 'Create account' and 'Next'.

17. Log in, and you should be taken to the OTP page:

A screenshot of the FortiToken Cloud login page. The header shows the FortiToken Cloud logo. Below the logo, the text 'Login to Your Account' is centered. The main content area contains a white box with two input fields. The first field is labeled 'Username' and contains the text 'test@'. The second field is labeled 'Token' and contains the text 'OTP code'. Below these fields is a blue button labeled 'Submit'.

18. Verify the token using the MFA method you selected when creating the user on FTC earlier. Now the end user should be able to log in to the IPsec VPN through FortiClient, as shown in the following illustration.



VPN Name sslvpn  
IP Address   
Username   
Duration 00:02:59  
Bytes Received 0 KB  
Bytes Sent 59.18 KB

Disconnect

## Example 6: ZTNA application gateway with SAML as SP

1. Complete the initial setup by following the instructions in [Configure ZTNA HTTPS access proxy](#).
2. Create a new SAML user/server on FortiGate GUI:
  - a. On the FortiGate, click *User & Authentication > Single Sign-On*.
  - b. Click *Create New*.
  - c. Set *Address* to `webserver.ztnademo.com:9443`.

**Note:** The *Entity ID*, *Assertion consumer service URL*, and *Single logout service URL* will be updated.
  - d. Take note of the aforementioned updates, for you will be prompted to enter them into FTC.
  - e. Enable *Certificate*, and select the certificate used for the client.

In this example, the `ztna-wildcard` certificate is a local certificate that is used to sign SAML messages that are exchanged between the client and the FortiGate SP.

- f. Click *Next*.
- g. Use the settings from FTC to fill the custom *Identity Provider Details*. On FTC, go to *Applications > SAML Applications > Add SAML Application*, you can get the IdP Metadata details from the creation page there:
  - Where the REMOTE\_Cert\_1 certificate is a remote certificate that is used to identify the IdP. You'll want to use the certificate you get from after you create the FTC SAML Application if you click the 3-dotted-menu > Details > Click to download the Signing Certificate
  - In the meantime, on FTC you can fill out the SP Metadata fields with the Entity ID, Assertion consumer service URL and Single logout service URL:

- h. Set *Attribute used to identify users* to username. (**Note:** Attributes to identify users and groups are case-sensitive.)

New Single Sign-On

Identity Provider Details

Log into your Identity Provider platform to find the following information.

Type: Fortinet Product Custom

Entity ID: https://auth.fortinet.com/saml/NLec.../metadata/

Assertion consumer service URL: https://auth.fortinet.com/saml/NLec.../login/

Single logout service URL: https://auth.fortinet.com/saml/NLec.../logout/

Certificate: REMOTE\_Cert\_1

Additional SAML Attributes

The FortiGate will look for these attributes to verify authentication attempts. Configure your Identity Provider to include them in the SAML Attribute Statement.

Attribute used to identify users: username

Attribute used to identify groups:

Back Submit Cancel

- i. Click *Submit* to save the settings.
3. Create a user group for the SAML user object, using the following steps:
  - a. Click *User & Authentication > User Groups > Create New*.
  - b. Set *Name* to *ztna-saml-users*.
  - c. Under *Remote Groups*, click *Add*.
  - d. For *Remote Server*, select *ZTNA-FAC-SAML*.
  - e. Click *OK*.
  - f. Click *OK* again to save the settings.
4. Apply the SAML sever to proxy authentication:
  - a. Go to *Policy & Objects > Authentication Rules*.
  - b. Click *Create New > Authentication Scheme*.
  - c. Set *Name* to *ZTNA-SAML-scheme*.
  - d. Set *Method* to *SAML*.
  - e. Set *SAML SSO server* to *ZTNA-FAC-SAML*.
  - f. Click *OK*.
  - g. Go to *Policy & Objects > Authentication Rules*.
  - h. Click *Create New > Authentication Rule*.
  - i. Set *Name* to *ZTNA-SAML-rule*.
  - j. Set *Source Address* to *all*.
  - k. Set *Incoming Interface* to *port3*.
  - l. Set *Protocol* to *HTTP*.
  - m. Enable *Authentication Scheme* and select *ZTNA-SAML-scheme*.
  - n. Set *IP-based Authentication* to *Disable*.
  - o. Click *OK*.
5. Configure the active authentication scheme and captive portal:
  - a. Go to *User Authentication > Authentication Settings*.
  - b. Enable *Authentication scheme*.
  - c. Select *ZTNA-SAML-scheme*.

- d. Set *Captive portal type* to *FQDN*.
  - e. Enable *Captive Portal*.
  - f. Select the firewall address *webserver.ztnademo.com*. (**Note:** Choose this firewall address if you have not already done so.)
  - g. Click *Apply* to save the configuration.
6. Configure a ZTNA application gateway to allow SAML authentication requests to the SP:
- a. Configure the ZTNA server:
    - i. Go to *Policy & Objects > ZTNA > ZTNA Servers > Create New*.
    - ii. Configure the following:

Parameter	Description
Name	ZTNA-access
Interface	Any
IP	10.0.3.10
Port	9443
SAML	Enabled
SAML SSO Server	ZTNA-FAC-SAML
Default certificate	ztna-wildcard

- iii. Click *OK*.
- b. Define the full ZTNA policy to allow access to the ZTNA server:
    - i. Go to *Policy & Objects > Proxy policy > Create New*.
    - ii. Configure the following:

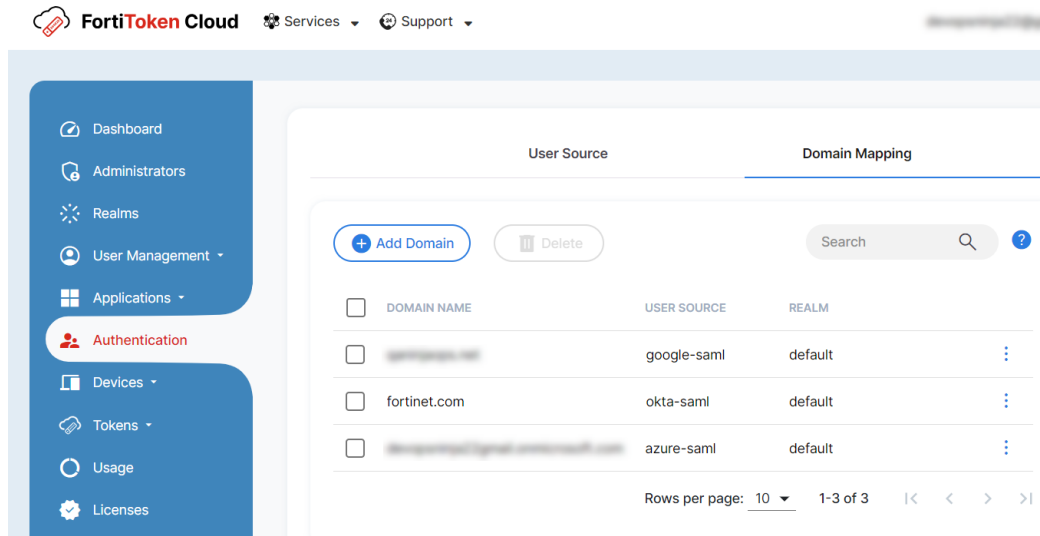
Parameter	Description
Name	ZTNA-Rule
Type	ZTNA
Incoming Interface	port3
Source (Address)	all
Source (User)	ztna-saml-users
Destination	all
ZTNA Server	ZTNA-access
Action	Accept
Log Allowed Traffic	All Sessions

- iii. Click *OK*.

Once all of the aforementioned configurations are completed on your FGT and the SAML application and User Source(s) are set up on FTC, end-users should be able to start going through the FTC SAML login process when trying to access web servers through ZTNA.

## Configure domain mapping

1. To configure a domain mapping, go to **Authentication > Domain Mapping**:



Following is an example for our Google IdP that we configured in the other example.

Domain Name

Realm

User Source

2. Now when the end-user tries to log into the SP, they get prompted with a screen that asks for their username first:

The screenshot shows the FortiToken Cloud login screen. It has a light blue background with the FortiToken Cloud logo at the top. Below the logo, it says 'Enter username to continue'. There is a white box containing a 'Username' label and a text input field. Below the input field is a blue 'Submit' button.

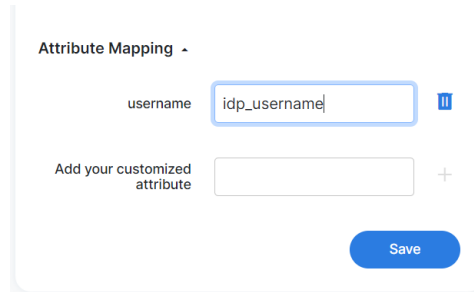
3. Upon inputting their username, the end-user is automatically directed to the Google sign-in page *if the domain of their username matches the configuration*.




## Attribute Mapping

Both IdPs and SPs can have different attributes configured which are different than the examples we gave where all attributes are just simply "username" for everything. Let's suppose our IdP used "idp\_username" as the attribute to identify usernames and then our SP used "sp\_username" to identify usernames. Then in this case we would need to make a mapping on both our IdP and our SP setting. This is how you would configure the attribute mapping according to this example in this case:

### IdP (user source):



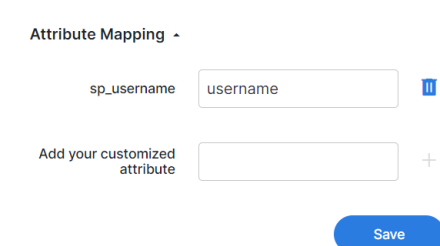
Attribute Mapping -

username  


Add your customized attribute  +

[Save](#)

### SP (SAML application):



Attribute Mapping -

sp\_username  

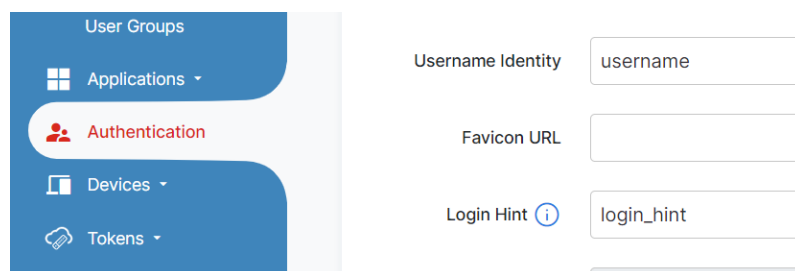
Add your customized attribute  +

[Save](#)

## Login hint

The login hint setting is used so that when an end user inputs their username from the "Enter username to continue" page. It is automatically populated in the username field once they are redirected to the IdP login page. For example, with our Azure example from earlier where we set login hint to "login\_hint," this is what it would look like:

### Login Hint setting:




User Groups

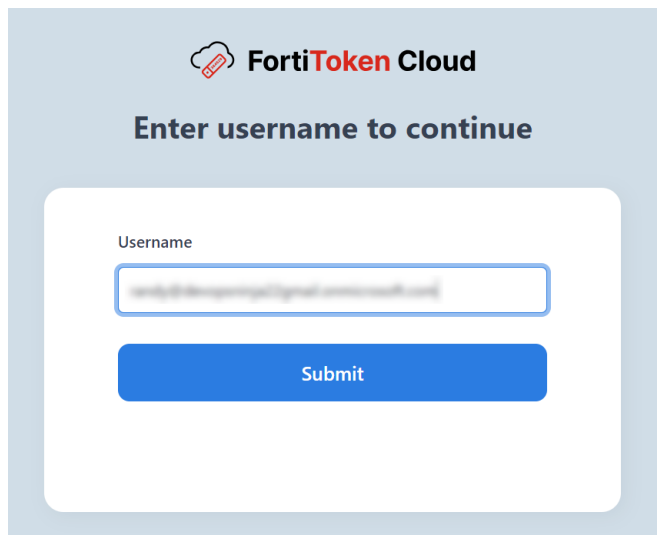
- Applications
- Authentication**
- Devices
- Tokens

Username Identity

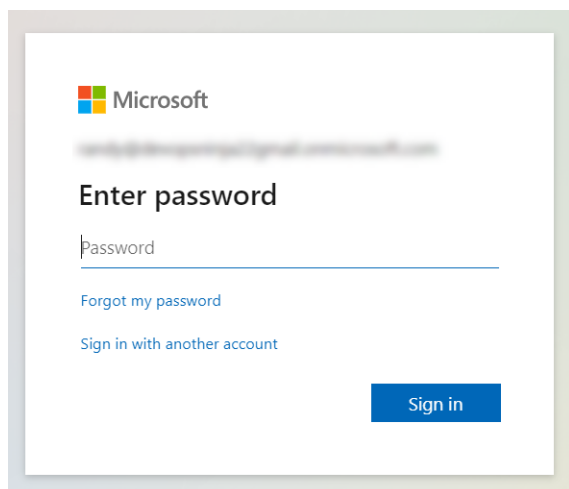
Favicon URL

Login Hint 

Input username into "Enter username to continue" page when a domain mapping is configured:



Username is automatically populated:



Some IdP vendors, such as Google, do not have a logout URL for you to configure into the IdP metadata field. In this case, logging out of the SP does not fully log the end user out.

## Configure user source

User source is an important component in any SAML application. For more information, see [Configure domain mapping on page 180](#) and [Use SSO applications on page 146](#)

# Manage end-user portals

End-user portals enable FTC end users to manage their own settings according to the permissions granted by their administrator.

End-user portals are realm-specific and must be implemented by the administrator on a per-realm basis. Before starting to configure end-user portals on a realm, ensure that the realm has already had a functioning IdP user source configured on it. For information about IdP user source configurations, refer to [Configure IdP user source on page 185](#). Your end users in the IdP user source are able to authenticate and log into their end-user portals once you have enabled the End-user Portals function on the realm.

Similar to SSO applications, the look and feel of end-user portals can be customized to align with your company's corporate theme and style. For more information, refer to [Create an end-user portal branding theme on page 235](#) and [Apply custom branding theme to end-user portals on page 237](#).




End users' mobile phone numbers and email addresses are validated through verification codes when they are trying to log into their portals and then saved to the FTC database upon successful validation. After logging into their end-user portals, end users are able to update their mobile phone numbers if the administrator grants them the permission to do so when enabling the end-users portals.

- [Configure End-user Portals on page 183](#)
- [Configure IdP user source on page 185](#)
- [Keep SSO applications off end-user portals on page 185](#)

## Configure End-user Portals

1. From the main menu, click *Applications>End-user Portals*.
2. Click *Add New User Portal*.
3. Make the entries and/or selections as described in the following table.
4. Click *Save* to enable the end-user portal.

Parameter	Description
<b>General</b>	
Name	Specify a name for the end-user portal to be created.
Subdomain	Enter your subdomain.  This feature enables users of the End-user Portal to access the portal using your custom URL rather than the URL generated by FortiToken Cloud.

Parameter	Description
	After entering your subdomain, click the (!) icon to validate it. If the domain is available, the validation will succeed. Otherwise, choose another domain and try again.
Realm	Select the realm to which the end-user portal is to be added.
Custom Branding	Click the down arrow to select a branding theme from the drop-down list or click the + (Add) to add a new one. For more information, see <a href="#">Create an end-user portal branding theme on page 235</a> and <a href="#">Apply custom branding theme to end-user portals on page 237</a> .
Session Duration	Set the length of time (in minutes) each portal session lasts before it times out. <b>Note:</b> This setting is not visible on end-user portals, and cannot be modified by end users.
<b>User-customizable Settings</b>	<div>  <p>When End-user Portals are created, all the end-users will inherit the existing settings of their realm. You can use the following radio buttons to allow/disallow the end users to customize their portal settings after they have logged into their end-user portals.</p> </div>
Profile	Allow/Disallow end users to update their profiles.
Passkey	Allow/Disallow end users to set or delete their passkeys.
Token Renewal	Allow/Disallow end users to renew their FTM tokens.

Parameter	Description
MFA Method	Allow/Disallow end users to change their MFA methods.
<b>Authentication</b>	Select the following authentication settings:
User Source	The IdP user source from the same realm. Users from the IdP user source will be able to log into the end user portals.
Default User Source	If selected, this user source will be by default if multiple user sources are available.

## Configure IdP user source

An end-user portal is automatically enabled and ready to use by the end users in the realm when it is created by the administrator. However, before starting to creating an end-user portal, you must ensure that the realm has already had an IdP user source configured on it.

Following are examples of how to configure user sources for an end-user portal:

- [Example 1: Google SAML as IdP and FortiGate SSL VPN as SP](#)
- [Example 2: Azure as SAML IdP and FortiGate as SP](#)
- [Example 3: Google OIDC as IdP](#)
- [Example 4: Azure OIDC as IdP](#)

## Keep SSO applications off end-user portals

SSO applications that are configured in the same realm where the end-user portals are enabled automatically show up under the *Applications* menu on the end-user portals. The end users can then launch the SSO apps directly from the portals by clicking the shortcuts to the apps after they have successfully logged into the end-user portals.

To prevent end users from accessing the SSO apps from the end-users portals, you must remove the login URLs of the SSO applications from the SSO application configurations on the FTC portal.

### To keep the SSO app off the end-user portals:

1. From the main menu, click *Applications>SSO Applications*.
2. Locate the SSO app, click the drop-down menu at the end of the row, and select *Edit*.
3. In the General setting of the Edit Application page, locate the Login URL field, and remove the URL.
4. Click *Save*.



- Once you have saved the change, the SSO application becomes inaccessible to the end users and will not show up as a shortcut on the end-users portals.
  - Removing the login URL in the configuration of an SSO application only removes end-users' direct access to it from the end-user portals, but has no impact on the function of the SSO application.
  - Repeat the steps mentioned above to remove all the login URLs
-















end-user portals

## Manage device ownership

The *Devices>Ownership* page shows all devices under your management. It also provides tools for managing the ownership of devices.

Column	Description
SN	The serial number of the device.
Cluster ID	The ID of the HA cluster to which the device belongs.
Ownership Status	The status of the device ownership: <ul style="list-style-type: none"><li>• Consistent – The ownership of the device belongs to the current account.</li><li>• Inconsistent – The ownership of the device does not belong to the current account and some data from the old account still remains on the device.</li></ul>
Toolbar	The slide-in toolbar provides the following tools: <ul style="list-style-type: none"><li>• Validate – Refresh the ownership status of the device. See <a href="#">Validate device ownership on page 194</a>.</li><li>• Delete – (1) Remove all user and application data that the preceding owner has left on the device. (2) Remove the device information from the <i>Manage Device Ownership&gt;Devices</i> table on both the preceding owner's and the</li></ul>

Column	Description
	<p>current owner's sides. After the delete is completed, if the current owner wants to sync up the data for this device, they must execute the command <code>exec fortitoken-cloud update</code> from the device, for example FortiGate. (<b>Note:</b> This option is available only when the ownership status of the device is "Inconsistent".)</p> <ul style="list-style-type: none"> <li>• Transfer – Start the device transfer task which will show up under the Tasks tab. (<b>Note:</b> This option is available only when the ownership status of the device is "Inconsistent".) See <a href="#">Manage device transfer on page 197</a>.</li> </ul>

This section discusses the following topics:

- [Validate device ownership on page 194](#)
- [Transfer devices on page 194](#)
- [Transfer devices on FTC on page 195](#)
- [Manage device transfer on page 197](#)
- [Perform factory reset on page 198](#)

## 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).

### To validate the ownership of a device:

1. Click *applications > Devices (HA)*.
2. In the Manage Device Ownership section, mouse over the device of interest.
3. In the toolbar on the right, select *Validate*.
4. When the Device Ownership Info message pops up to show the ownership status of the device.
5. Click *OK*.

## Transfer devices

Device transfer must be done through the FortiCare ticket system.

If you are using FOS version 6.4.0 or earlier, contact [FortiCare Technical Support](#) at <https://www.fortinet.com/support/contact> to request FortiGate account transfer via Live Chat or over the phone. You must have your FortiGate serial number ready and provide the source account email and the target account email. The FortiCare team will send out authorization email to the email recipients for approval. Once they have received the authorization email, the FortiCare team 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. See [Transfer devices on FTC on page 195](#).

1. Log into `ftc.fortinet.com` using the source or target FC account.
2. Click *applications > Devices (HA)*.
3. In the Manage Device Ownership section, identify the device of interest.
4. Mouse over the device and click *Validate* in the tool bar.
5. Read the messages onscreen.
6. Press *Delete* if you want to remove the users from the account. In the warning message, click *Delete*.

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

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

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

## Transfer devices on FTC

You can transfer devices from one FTC account to another using the FTC portal. While the transfer is being processed, your end-users should not notice any changes in their user experience with FTC. For example, if they have logged in through VPN, they can continue using VPN while the device is being transferred.

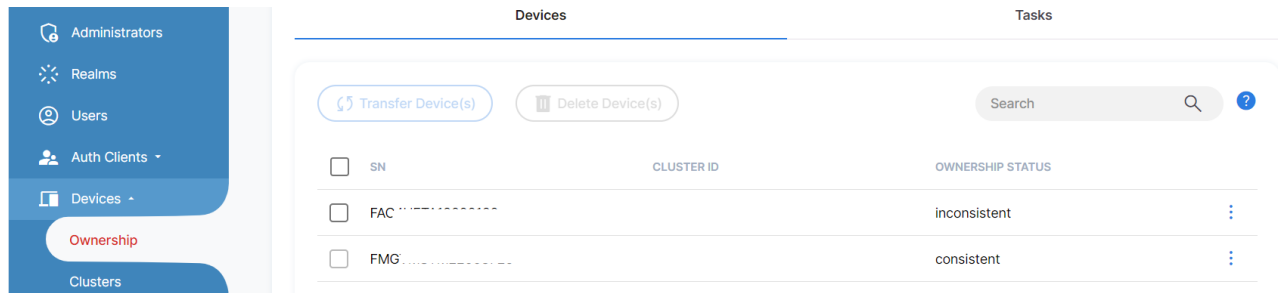


FortiToken Cloud approves device transfer requests automatically if the source account has been removed or merged into another account in FortiCare. We strongly recommend that you check and clear any sensitive user data off the device before removing it from the source account or merging it with another FortiCare account.

### To transfer a device with data:

1. Submit a device ownership transfer ticket in FortiCare.
2. Wait until after the ticket is processed and the ownership is transferred to the new owner in FortiCare. For example, Account A is the original owner and Account B is the new owner.

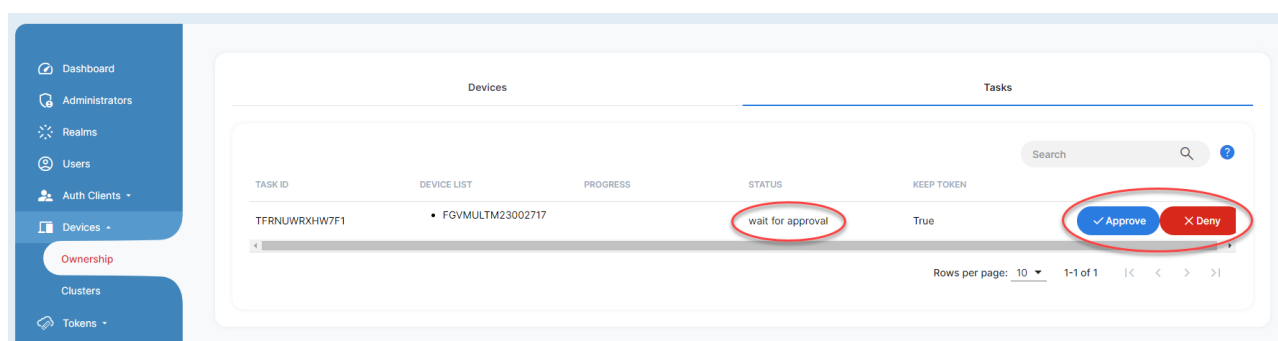
- Now the owner of either Account A or B can start the device transfer by selecting *applications>Devices (HA)>Manage Device Ownership>Devices*.
- Locate the device (whose Ownership Status should be "Inconsistent").



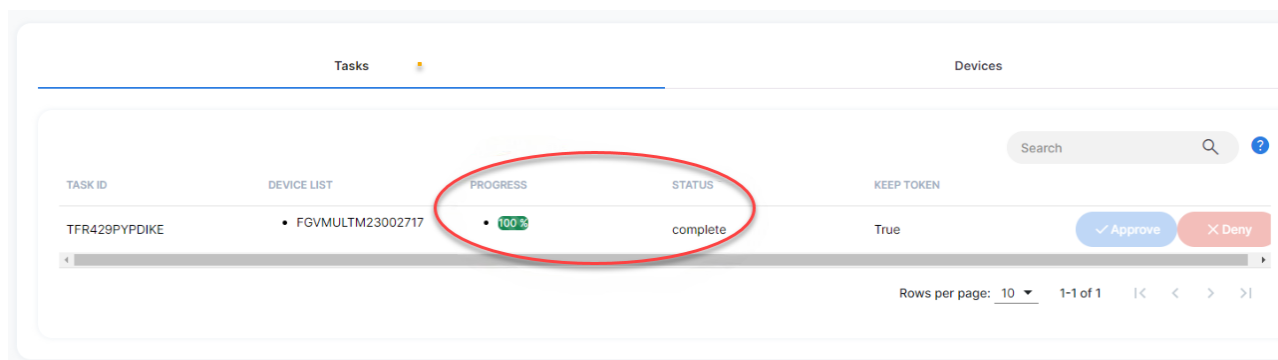
- On the right side of the row, click the three dots to open the menu, and then click *Transfer* to start transferring the device ownership.
- If you are NOT the owner of the new account who has initiated the device ownership transfer, click *Devices (HA)>Ownership>Tasks*, locate the transfer task, and click "Approve".



- Device ownership transfer tasks are viewable by both parties involved in the transfer process.
- A device ownership transfer task cannot be initiated and approved by the same party. If you have initiated a device ownership transfer task, you must wait for the other party to approve it.



- Wait until the *Progress* column shows "100%" and the *Status* column shows "Complete". By then, the ownership of the device should have been transferred to the new owner, and any old data left on the device should have been wiped out.







Transfer tasks will remain on the page for 24 hours and will be deleted automatically thereafter.

### To transfer a device without data:

If all data related to the old account has been removed from the device, FTC can automatically transfer the device ownership to the new owner. However, the device will not appear in the new account's *applications* or *Devices (HA)>Manage Device Ownership* pages of the FTC portal.

To establish a new connection between the FTC portal and the application (FortiGate for this case), you must log in to the FortiGate device and run the CLI command "execute fortitoken-cloud update".

## Manage device transfer

The *applications>Devices (HA)>Manage Device Ownership>Tasks* page provides tools for managing the transfer of devices.

Column	Description
Task ID	A system-generated identifier of the task.
Device List	The list of all devices in the transfer task.
Progress	The percentage of completion of the transfer task.
Status	The status of the transfer task, which could be one of the following: <ul style="list-style-type: none"> <li>Wait For Approve (non-clickable)</li> <li>Complete (non-clickable)</li> <li>In Progress (You can click to view the transfer result.)</li> <li>Failed (You can click to view the transfer result.)</li> </ul>
Keep Token	Shows either of the following :

Column	Description
	<ul style="list-style-type: none"> <li>• True – all users will keep their token. If selected, the new owner of the device does not need to re-activate the end-users.</li> <li>• False – If selected, the new owner of the device must reactive the end-users.</li> </ul>
Action	<p>Shows the following options:</p> <p>Approve – Approve the transfer task (This option is disabled for the party who requests the device transfer.)</p> <p>Delete – Deny and remove the device transfer task.</p>

## Perform factory reset

If you want to remove all data from a FortiGate device that uses FTC for MFA authentication before transferring or disposing the device, we strongly recommend doing the following:

1. Before performing a factory reset, remove all data on the FortiGate by executing the CLI command "execute fortitoken-cloud sync" in the Global VDOM.
2. After the factory reset, log in to the FTC portal and remove any data related to the device that still remains in the portal.

For instructions on how to delete user-related data from the FTC portal, refer to [Delete users from FTC on page 121](#) and [Delete an application on page 124](#).

## Manage HA clusters

The Devices>Clusters page provides tools for managing HA cluster configuration using devices in your account.

- [Search for a standalone device on page 199](#)
- [Add devices to a cluster on page 198](#)
- [Move a device between clusters on page 199](#)
- [Remove devices from a cluster on page 199](#)

## Add devices to a cluster

You can add any device in the *Standalone Devices* panel to any cluster in the *Clusters* panel. Once a standalone device is added to a cluster, it becomes part of the cluster and will be removed from the *Standalone Devices* panel.



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

1. In the *Clusters* panel, locate the cluster of interest.
2. In the *Standalone Devices* panel, locate the standalone device of interest. See [Search for a standalone device on page 199](#).
3. Select the device, and click *Add To Cluster*.
4. When the *Device Management* dialog pops up, be sure to read the message, and click *OK*.

## 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. Select the device of interest.
3. Click *Move out*. The *Device Management* dialog opens.
4. Read the message, click *OK* to proceed.

## 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.

## Search for a standalone device

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



- You can search for a device by any part of its serial number (SN). However, the more specific your entry, the more accurate your search result.
-

### To search for a standalone device:

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

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

## Use 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
<b>Serial Number</b>	The serial number of an FTM.
<b>Username</b>	The username of the FTC end-user to whom the FTM has been assigned.
<b>Realm</b>	The realm to which the end-user of the FTM has been assigned. <b>Note:</b> The field shows "default" if the application associated with the end-user has not been assigned to any custom realm.
<b>Platform</b>	The mobile platform of the FTM, which can be either of the following: <ul style="list-style-type: none"><li>• <i>Android</i></li><li>• <i>iOS</i></li></ul>
<b>Algorithm</b>	The algorithm of time-based one-time password authentication used by the token: <ul style="list-style-type: none"><li>• <i>TOTP</i></li></ul>
<b>Registration ID</b>	The registration ID of the FTM.

## Use 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
<b>Checkbox</b>	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 <a href="#">Delete hard tokens on page 203</a> . <b>Note:</b> You can also check the checkbox in the column header to select all the hard tokens and delete them all at once.
<b>Serial Number</b>	The serial number of the hardware token.
<b>Model</b>	The model of the hardware token, which can be one of the following: <ul style="list-style-type: none"> <li>• <i>FTK200, FTK200B, and FTK210</i></li> </ul>
<b>Algorithm</b>	The algorithm of time-based one-time password authentication used by the hardware token. <ul style="list-style-type: none"> <li>• <i>TOTP (default)</i></li> </ul>
<b>Username</b>	The username of the FTC user to whom a FortiToken has been assigned. <b>Note:</b> If this field is blank, it means that the FortiToken has not been assigned to any user yet.
<b>Last Update</b>	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 202](#).



FTK200CD and FTK200BCD (with the serial number prefix FTK211) are 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 [Manage users on page 115](#).

### 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 hard token shown on the *Hardware* page without a username means that it has not been assigned to any end-user yet, and can be assigned to any end-user in your FTC account.

### To assign a free hard token to a user:

1. On the main menu, click *Users*.  
The *Users* page opens. See [Manage users on page 115](#).
2. Identify the user of interest and click the *MFA Method* column.  
A pop-up list appears showing all the MFA methods that FTC supports.
3. Select *FTK*.

## Delete hard tokens

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



Only unassigned FTK tokens can be deleted.

---

### To delete individual hard tokens:

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

### To delete all hard tokens:

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

## Use passkeys

Support for passkeys has been implemented in FTC using Webauth. According to FIDOalliance.org ,Web Authentication (WebAuthn), a core component of FIDO Alliance's FIDO2 set of specifications, is a web-based API that allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

Passkeys are becoming the norm for enhanced protection in many sites. With passkey support, customers will be able to meet higher security standards and protect their organizations from threats like phishing.

## Use Case

For example, there are two users John and Todd in Company A. Bob is the FTC Admin for the organization. The company would like to enforce all end-users in their company to use passkeys using either the FortiToken 410 USB key or their mobile phones.

### To add the FortiToken 410 USB key as the passkey for John, the following must done:

1. Bob as the FTC admin will set a PIN for the FortiToken 410 USB key..

2. Bob will then navigate to Users , search for John and then choose Manage Passkeys .
3. Bob will add the FortiToken 410 USB key to John's profile.
4. John will then get the registered FortiToken 410 USB key from Bob and Bob will share the PIN with him.
5. John will change the PIN for the FortiToken 410 through Security key management in his computer.
6. John can now choose to use 'Login with Registered Passkey' for any SP configured with FTC's IDP Proxy and use FortiToken 410 USB as Passkey.

**To add a SmartPhone as passkey for Todd, the following must be done:**

1. Todd will need to take his phone to Bob
2. Bob as the FTC admin will navigate to Users , search for Todd and then choose Manage Passkeys
3. Bob will choose a iPhone or android device to save the Passkey and a QR code will be generated
4. Todd will then scan the QR code generated to his phone and then add the passkey to his device
5. If Todd is a new employee who gets a company provided phone, Bob can scan the QR code in Todd's company provided phone and give it to Todd.



For this release, end-users are not able to provision their passkeys by themselves. It must be done by the FTC admin. To register their SmartPhones, end-users must bring their phones to the FTC admin who can scan the QR code generated to their phones.

---

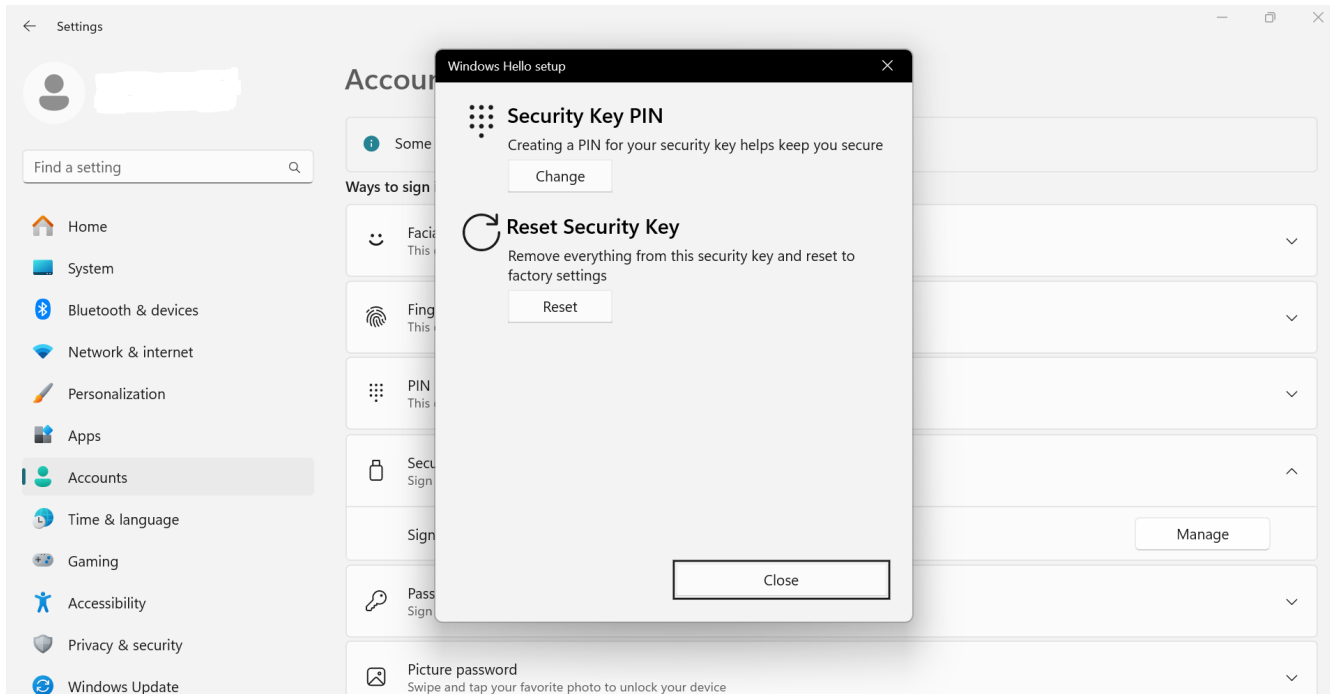
## Register FortiToken 410 USB key in Windows devices

Before registering a USB key, a PIN has to be first set up for the key. The following are the sample steps to set up the PIN for a Fortitoken 410 key in Windows 11 machine.

In the use case above, Bob , the FTC admin, needs to set a PIN for the FortiToken 410 USB key to be used by John, using the following steps:

1. After inserting the FortiToken 410 key in a USB slot in the Windows machine, search for 'Setup Security Key' in the Windows taskbar search. Then choose 'Security Key > Sign in to apps with Security key > Manage.



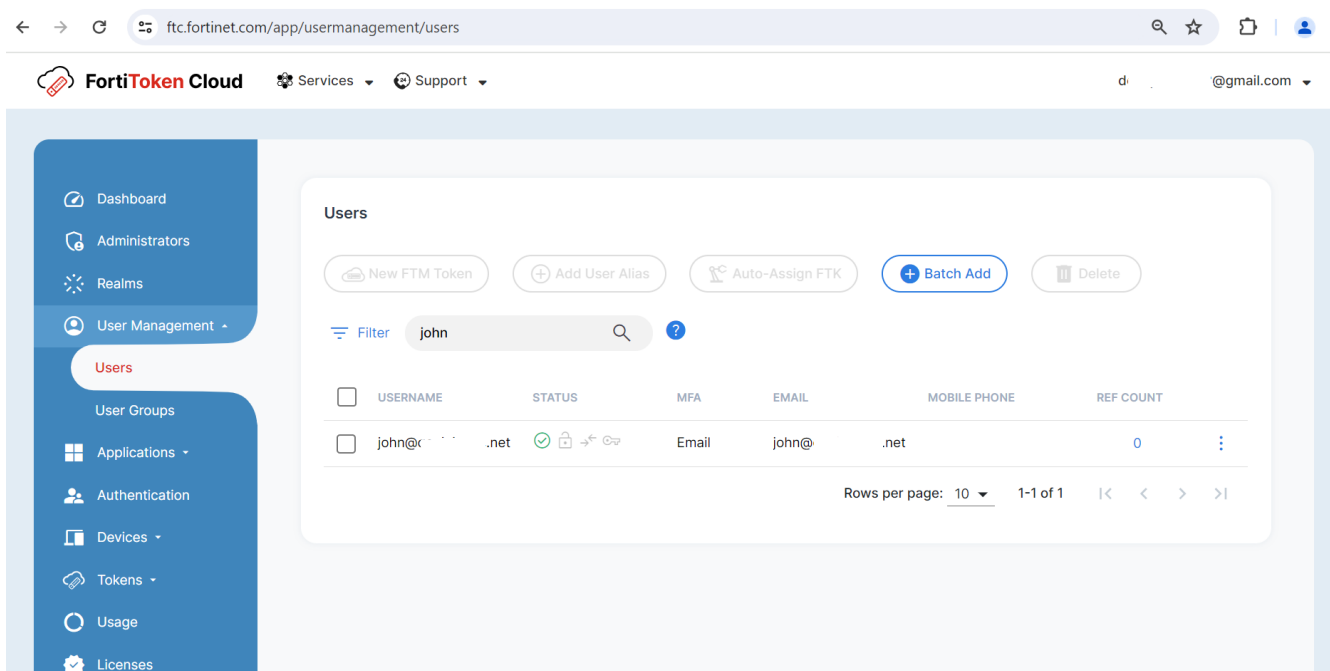


2. Choose 'Security Key PIN' and set up a PIN for the key.

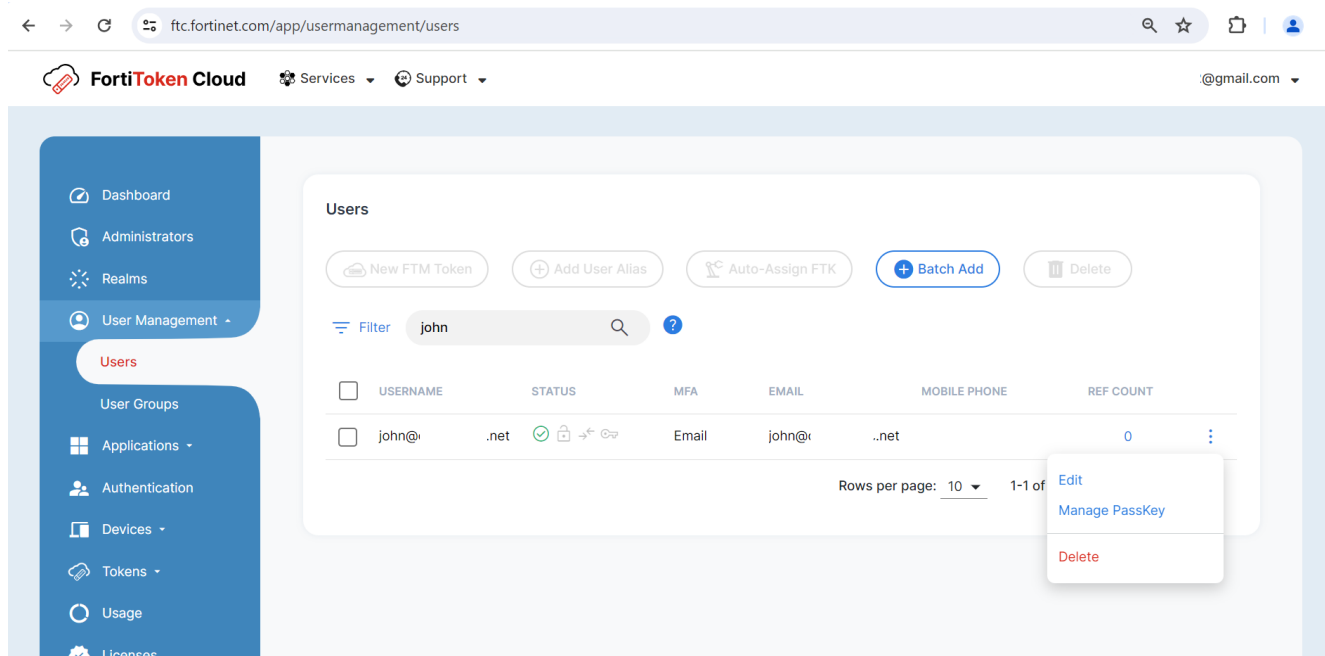
## Steps to register a USB passkey for an end-user:

For FortiToken 410 USB key to be added as Passkey for John, the FTC admin (Bob in this case) must do the following:

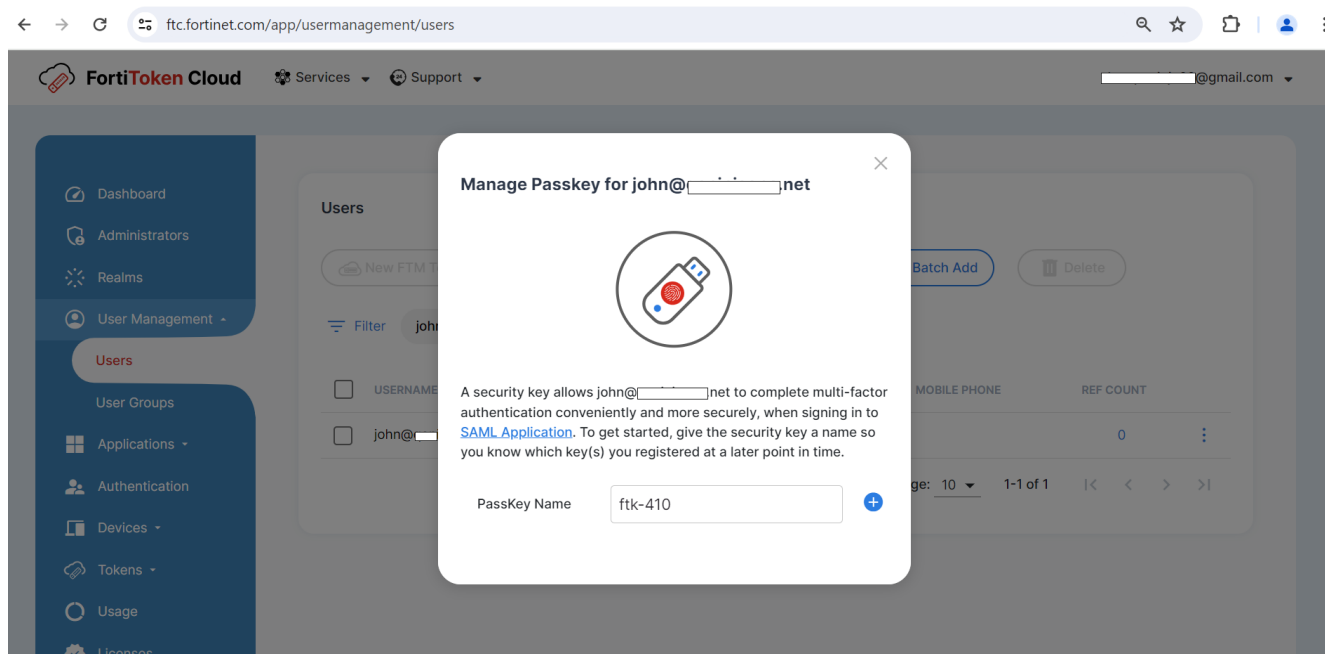
1. Navigate to Users > search for user, example John' in this case.



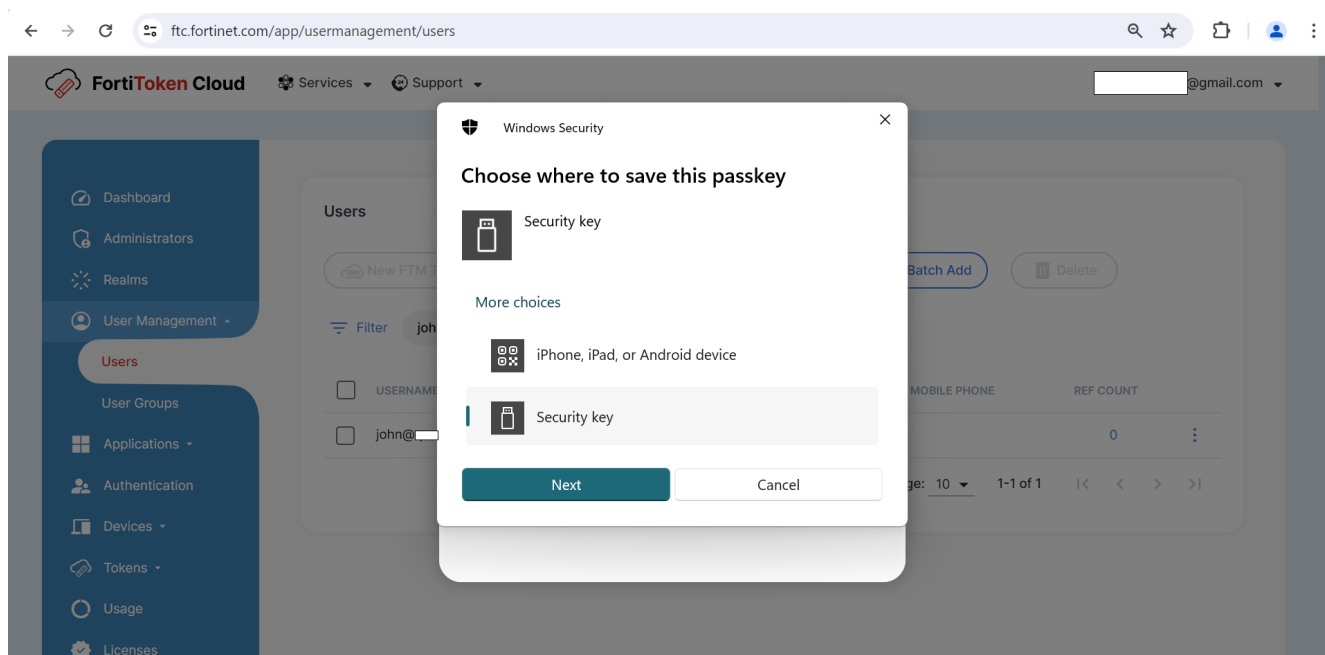
2. Click the 3 vertical dots on the right end of the row and choose 'Manage Passkey'.



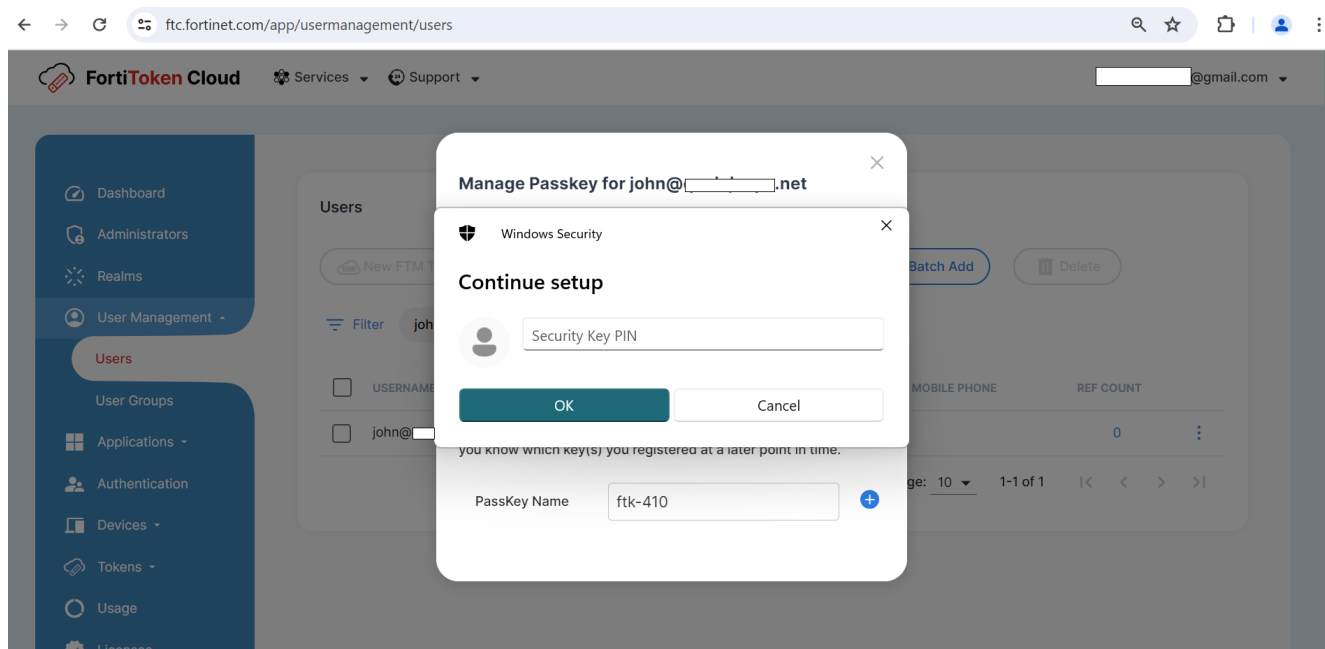
3. Provide a name for the Passkey (e.g., ftk-410 in the example shown in the following screen shot).



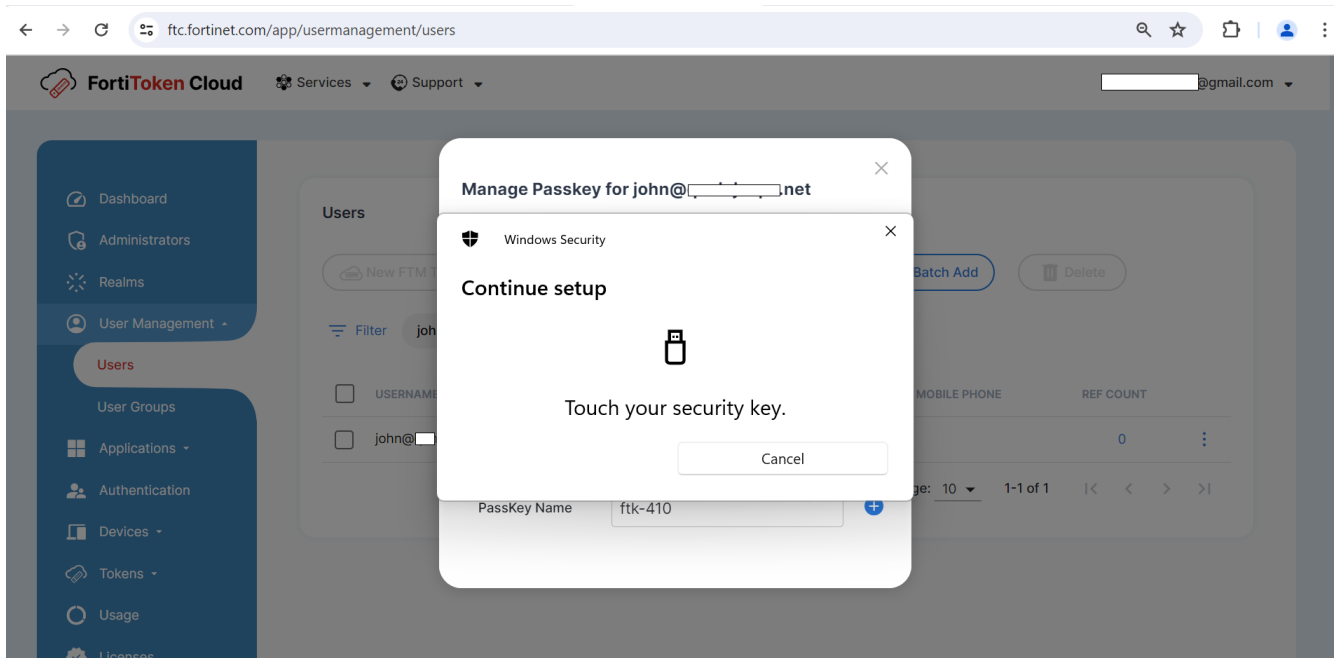
4. Choose Security Key in the Windows Prompt,



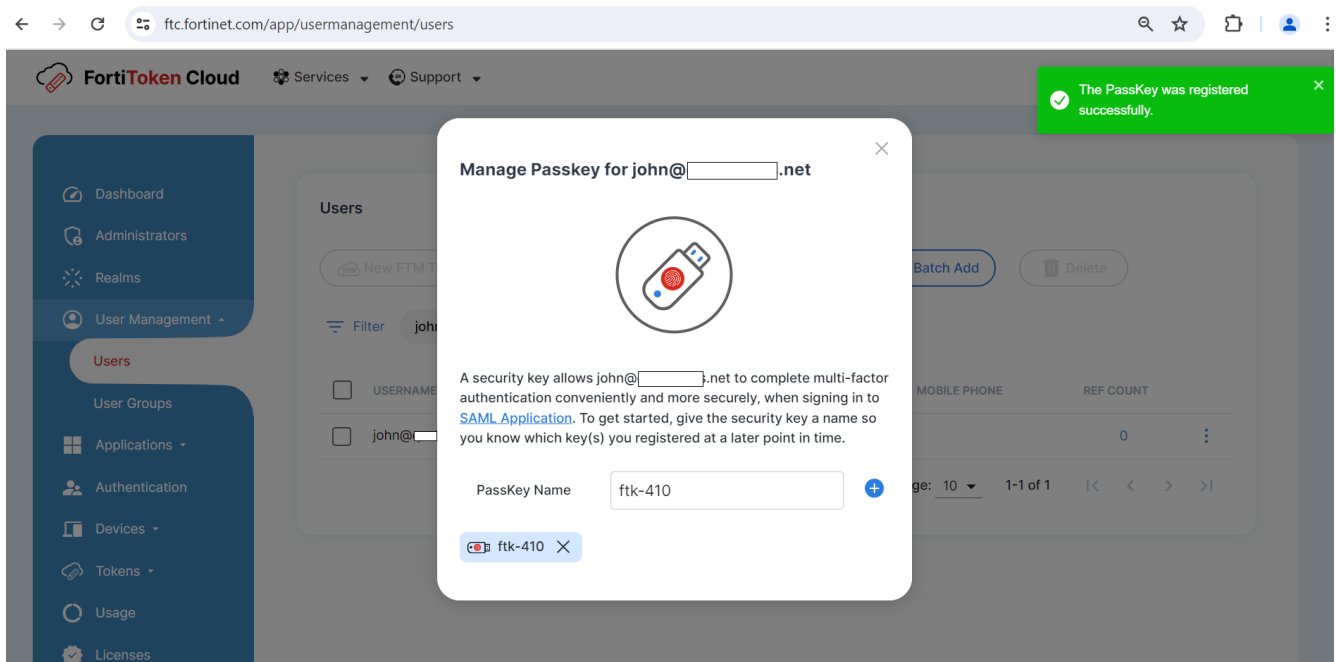
5. Provide the PIN for the FortiToken 410 configured in the section "Register FortiToken 410 USB key in Windows devices" (at the beginning of this section).



6. Once the PIN is authenticated, the system will prompt you to touch the security key. Press the button in the FortiToken 410 key.

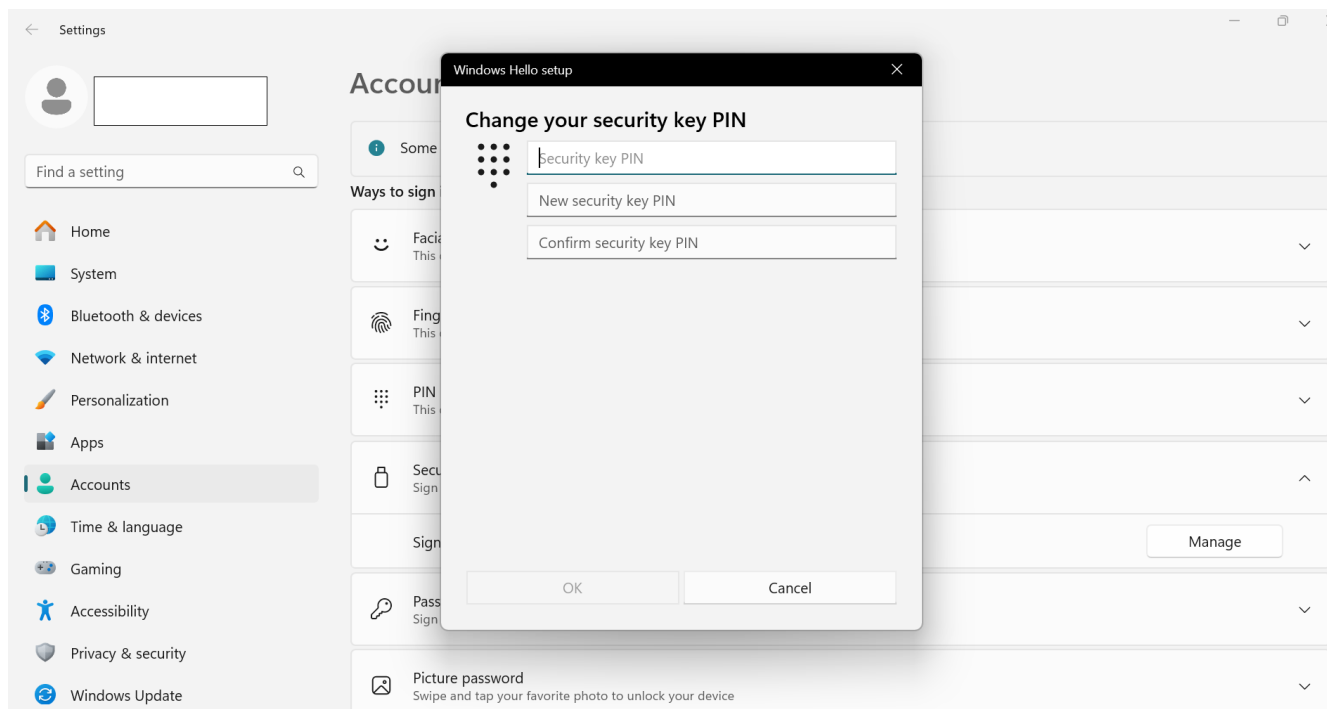


7. Once the key is successfully registered, the key appears on the screen, as illustrated in the following image.



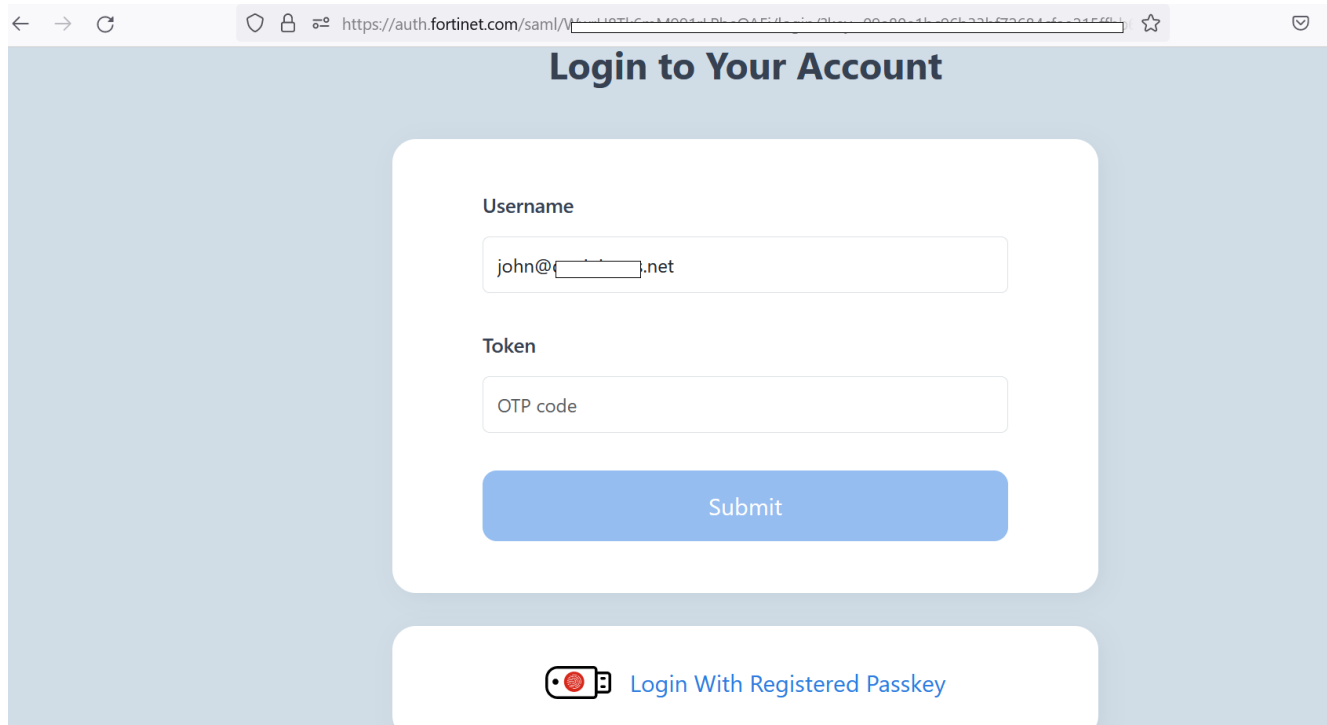
## Authenticate with the USB passkey in IDP proxy

1. Before trying to authenticate with any SP, user John will first change the PIN shared by Bob for the FortiToken 410 key. After inserting the FortiToken 410 key in a USB slot in the machine, John should search for 'Setup Security Key' in the Windows taskbar search. Then choose 'Security Key > Sign in to apps with Security key > Manage'. Provide the existing PIN that Bob shared and then update the PIN to a new one.

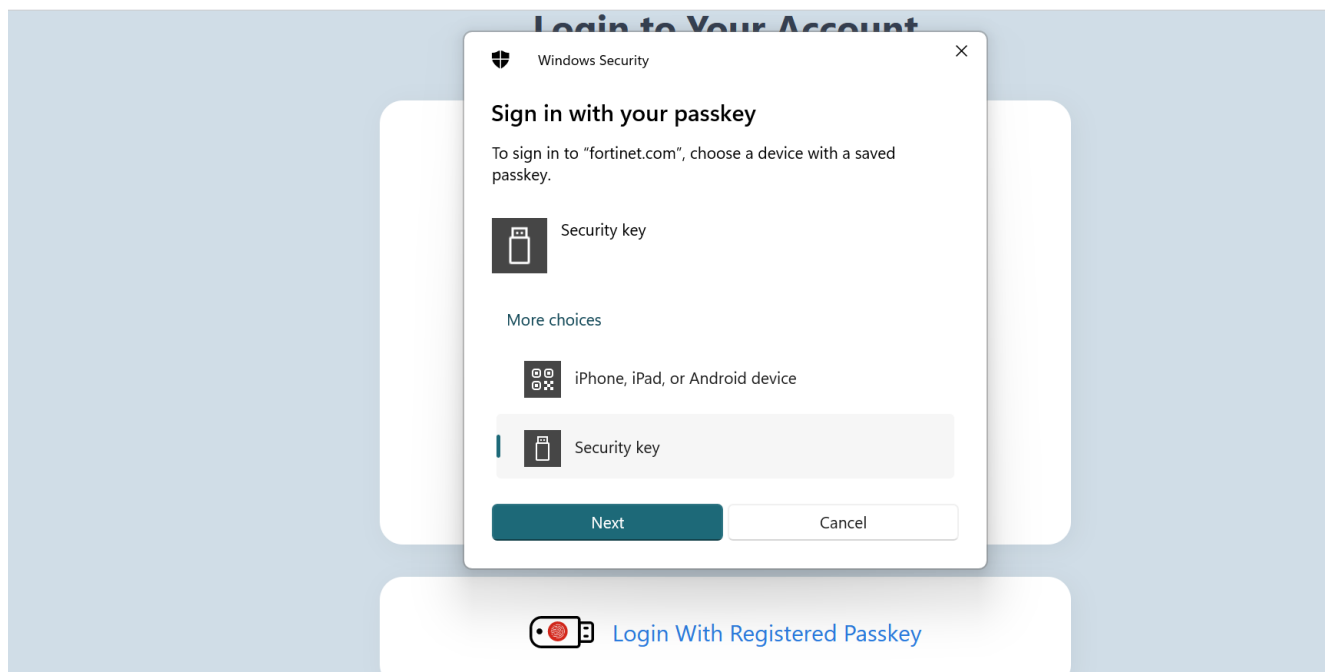


2. After successfully changing the PIN, open any SP configured with FTC's IDP proxy,

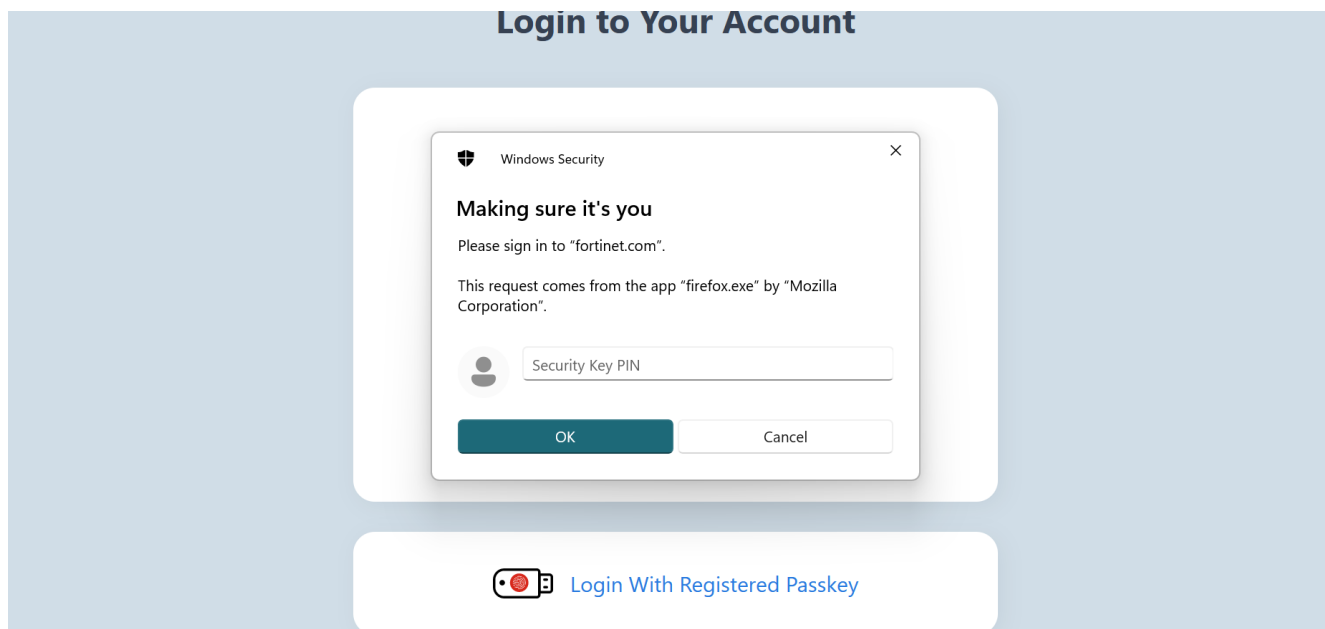
3. After successfully authenticated with the external identity provider to access a service provider, the user (John in this case) will be presented with the auth.fortinet.com page from FTC for MFA. Choose 'Login with Registered Passkey'.



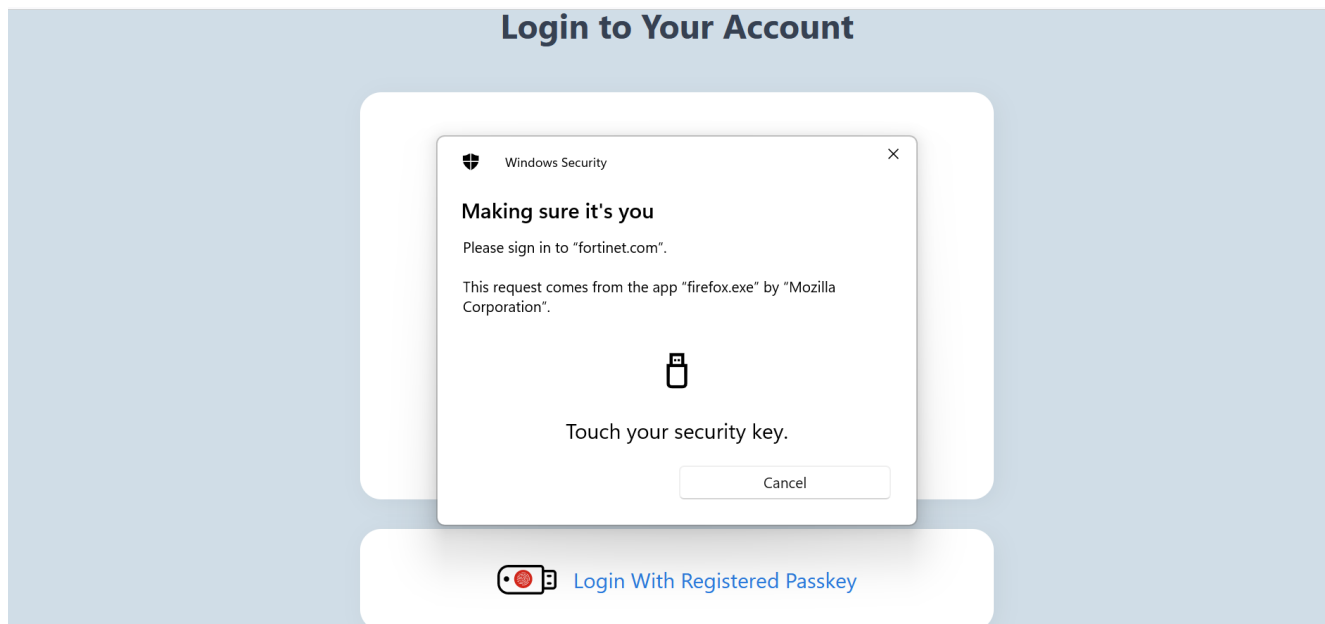
Choose 'Security key' to use the Fortitoken-410 USB pass key.



Provide the PIN for the fortitoken 410 Passkey.



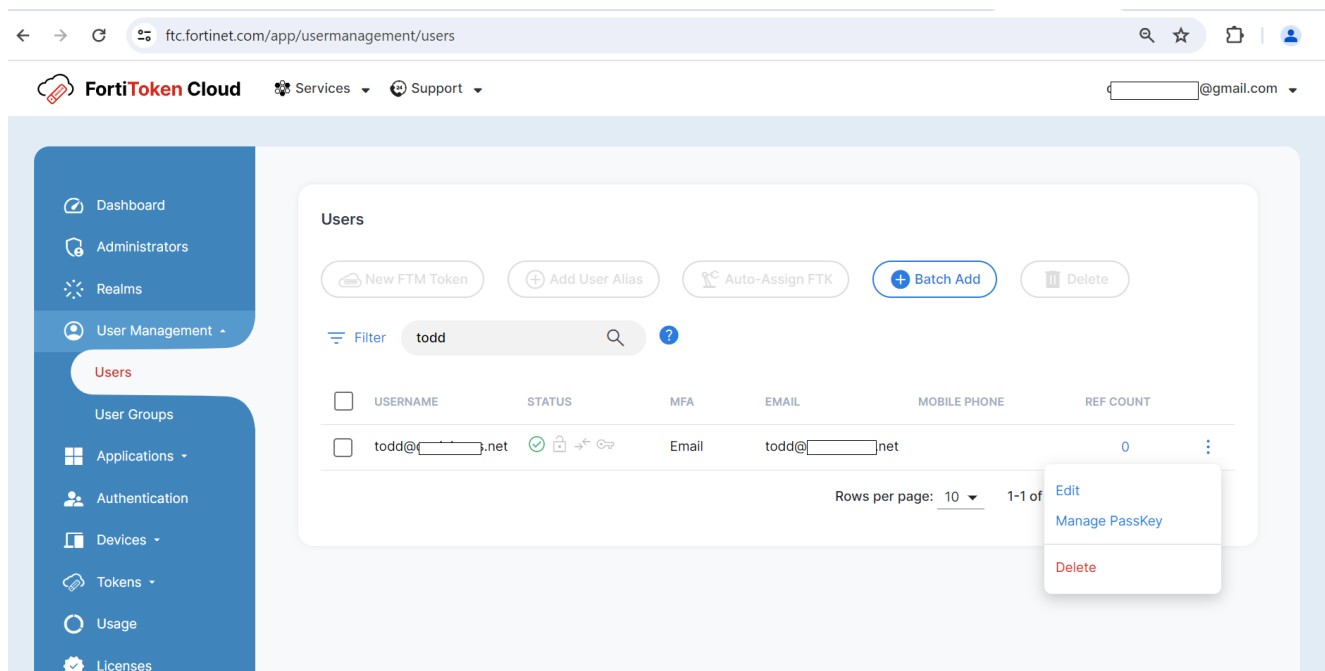
After the PIN is validated, please follow the instructions and touch the Fortitoken 410 Passkey.



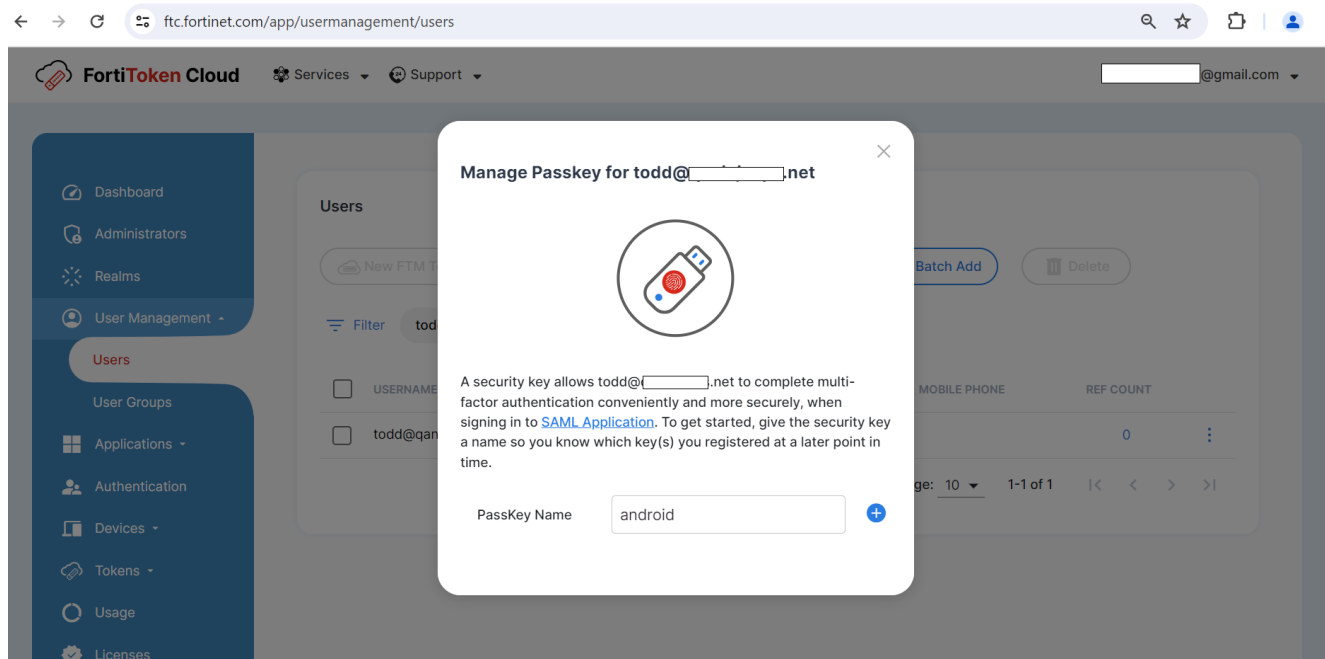
After that successful step, the user will be logged in.

## Steps to Register phone Passkeys for a Enduser:

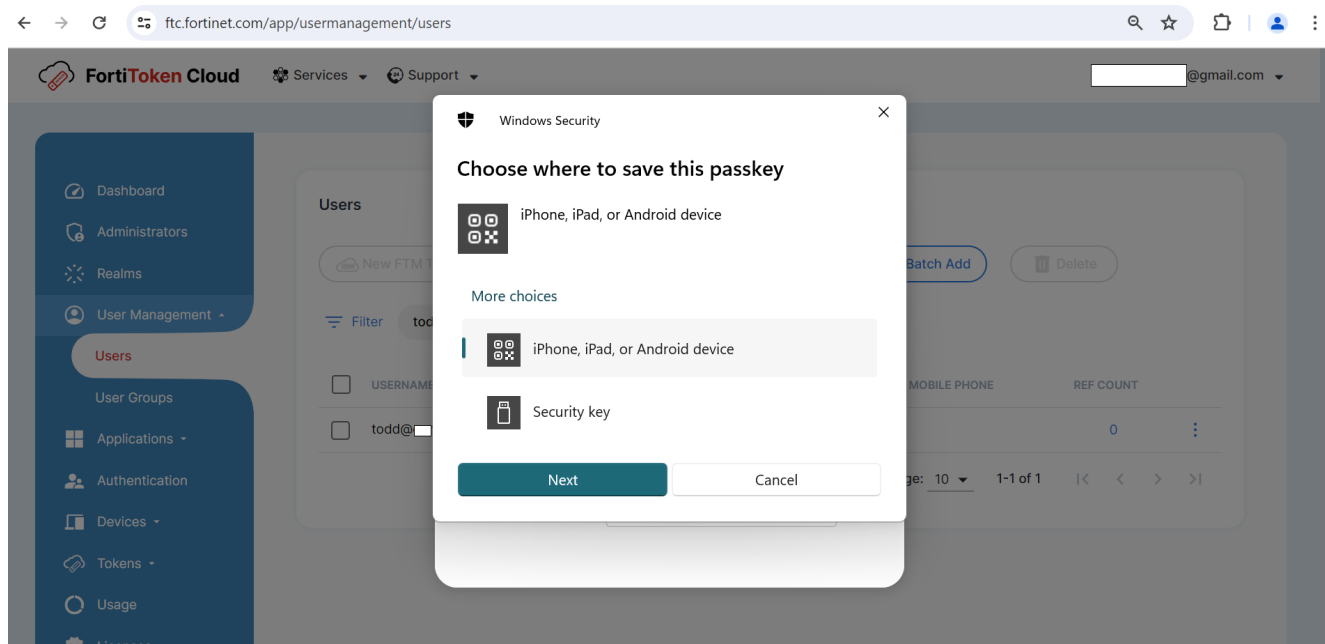
1. For a phone to be added as Passkey for user Todd the following are the steps in the GUI followed by FTC admin Bob:
2. Navigate to Users > search for user ' , example Todd in this case and choose 'Manage Passkeys'



3. Provide a name for the passkey, 'android' in the following screenshot

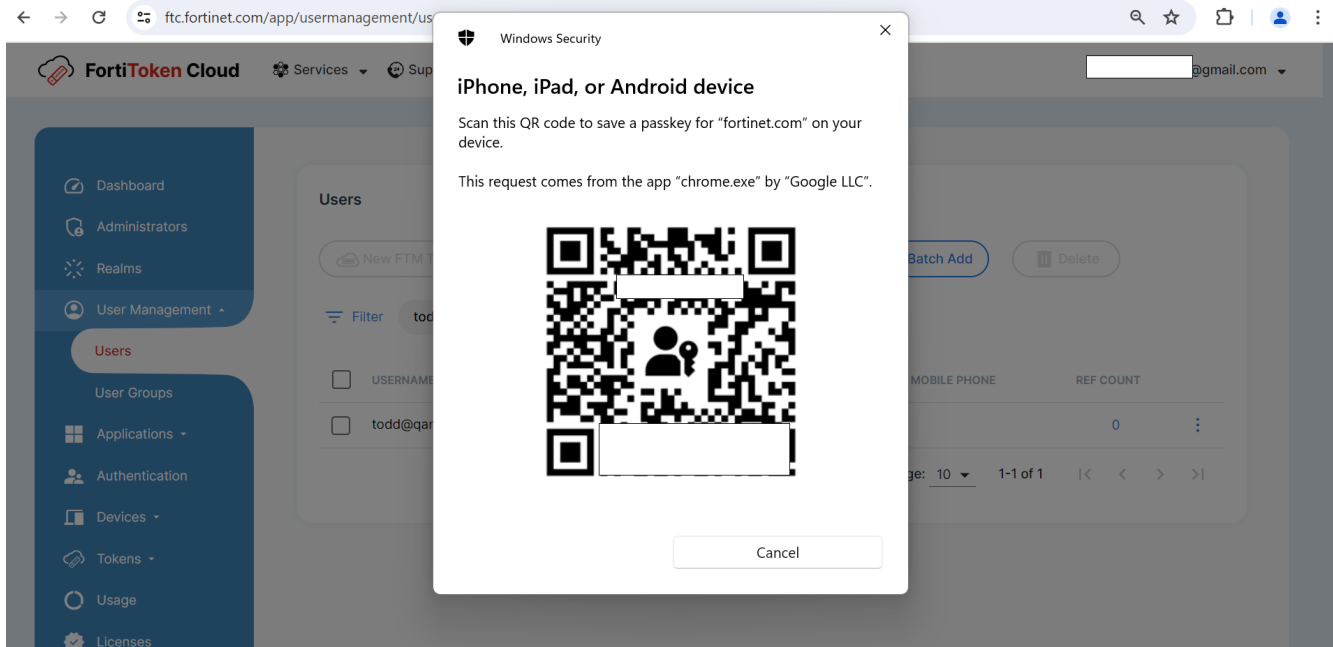


#### 4. Choose 'Iphone, Ipad or Android device' from the windows prompt

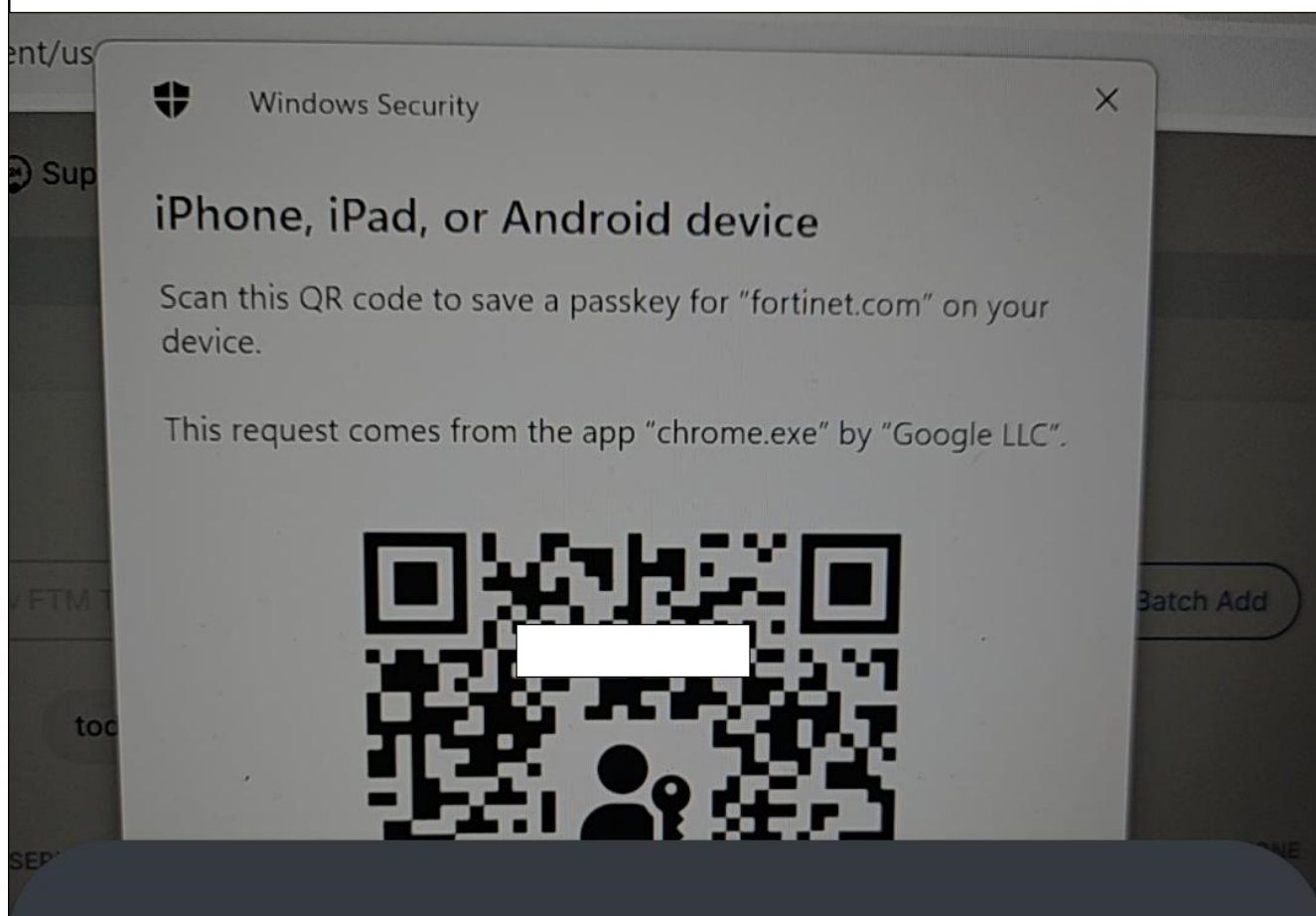
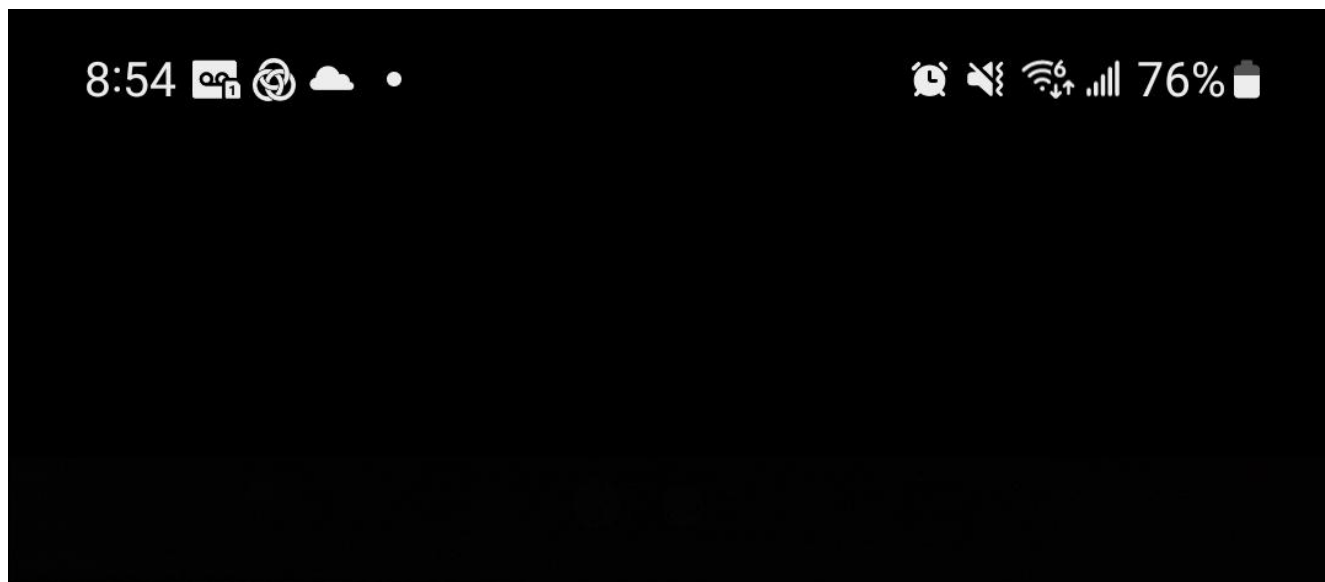


#### 5. Ensure Bluetooth is enabled in both your computer and the phone and scan the QR code . In this case , user Todd's phone will be used to scan the QR code.

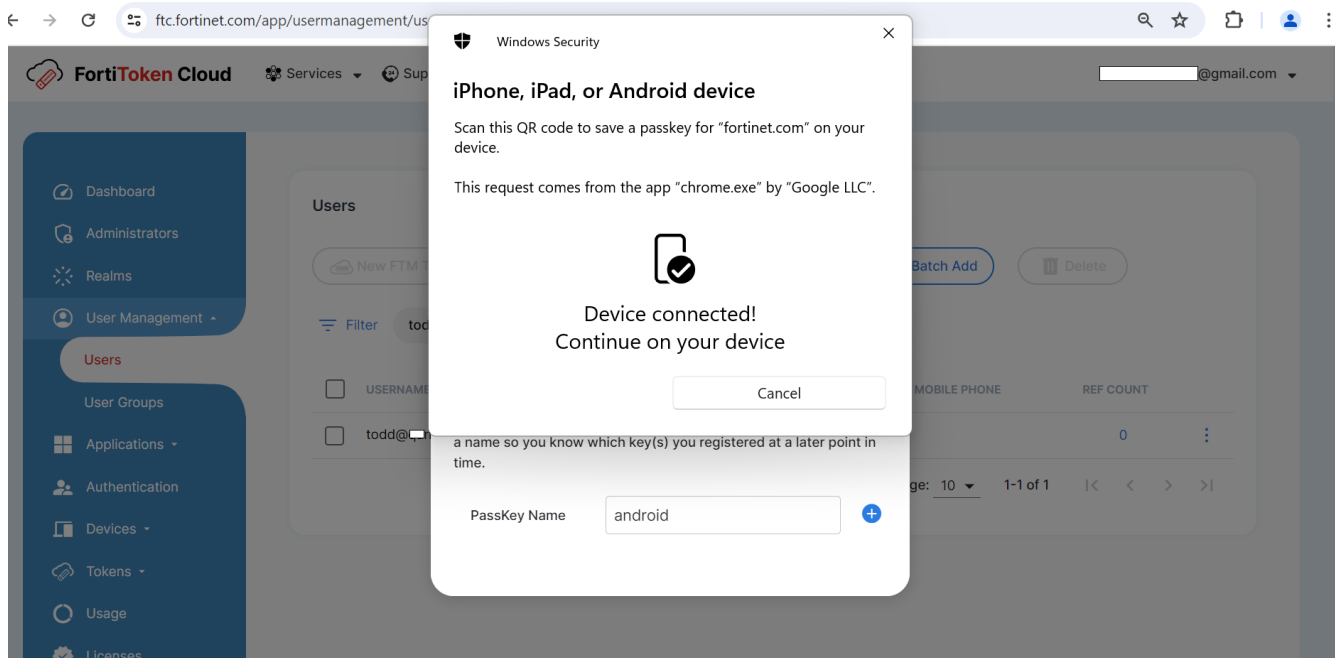




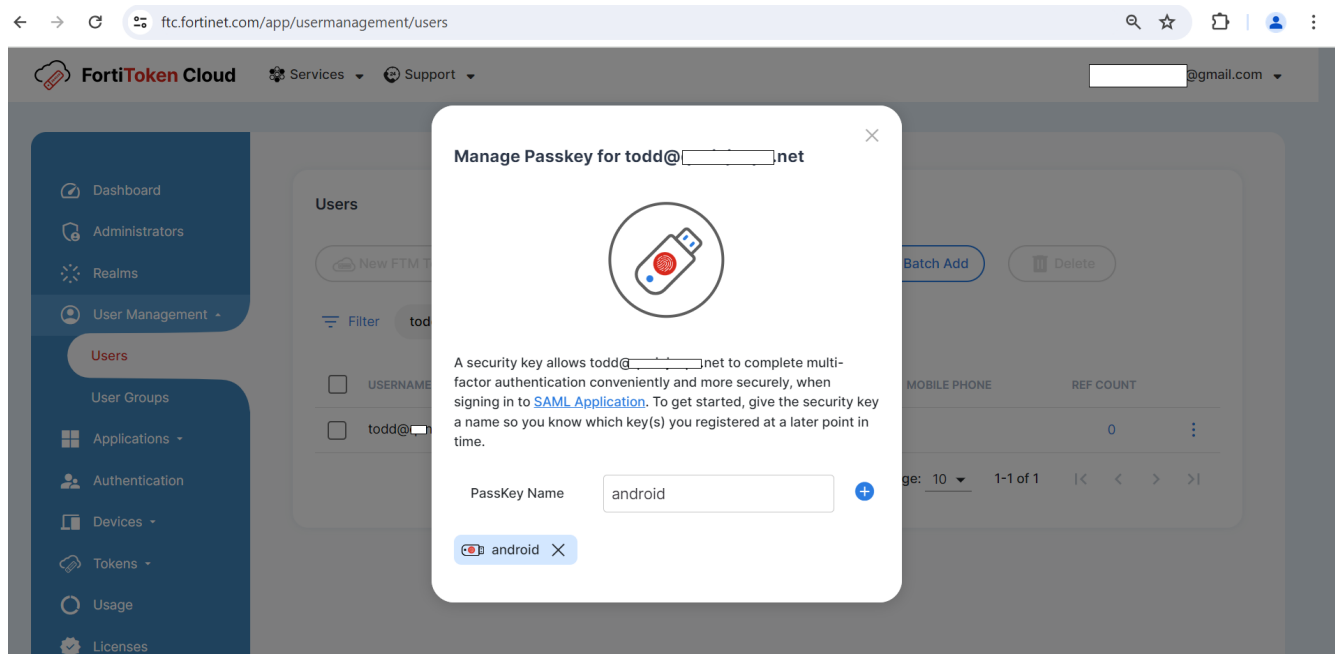
6. The phone will automatically prompt to provide your screenlock or other protection mechanism configured in your phone. Follow the instructions in your phone to add the passkey.



8. Once the phone is successfully added, the following confirmation will appear on the FTC portal screen to admin Bob.



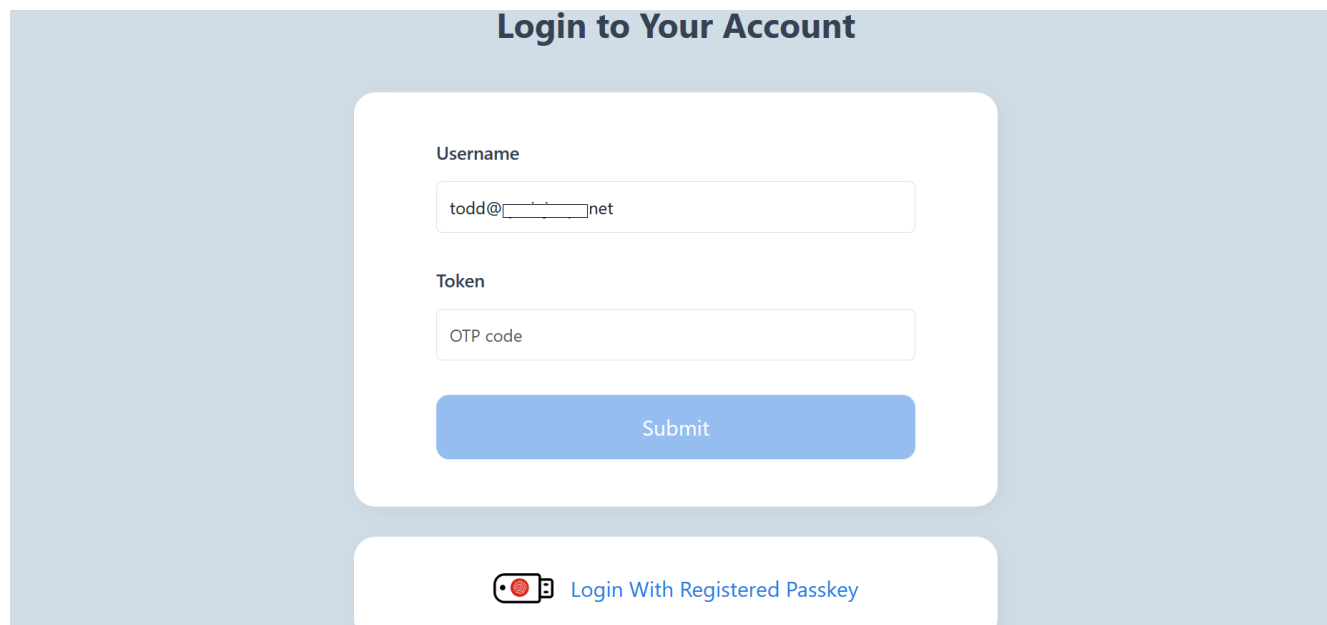
9. Once the phone is successfully added, the following confirmation will appear on the FTC portal screen to admin Bob.



## Authentication with a Phone Passkey in IDP proxy

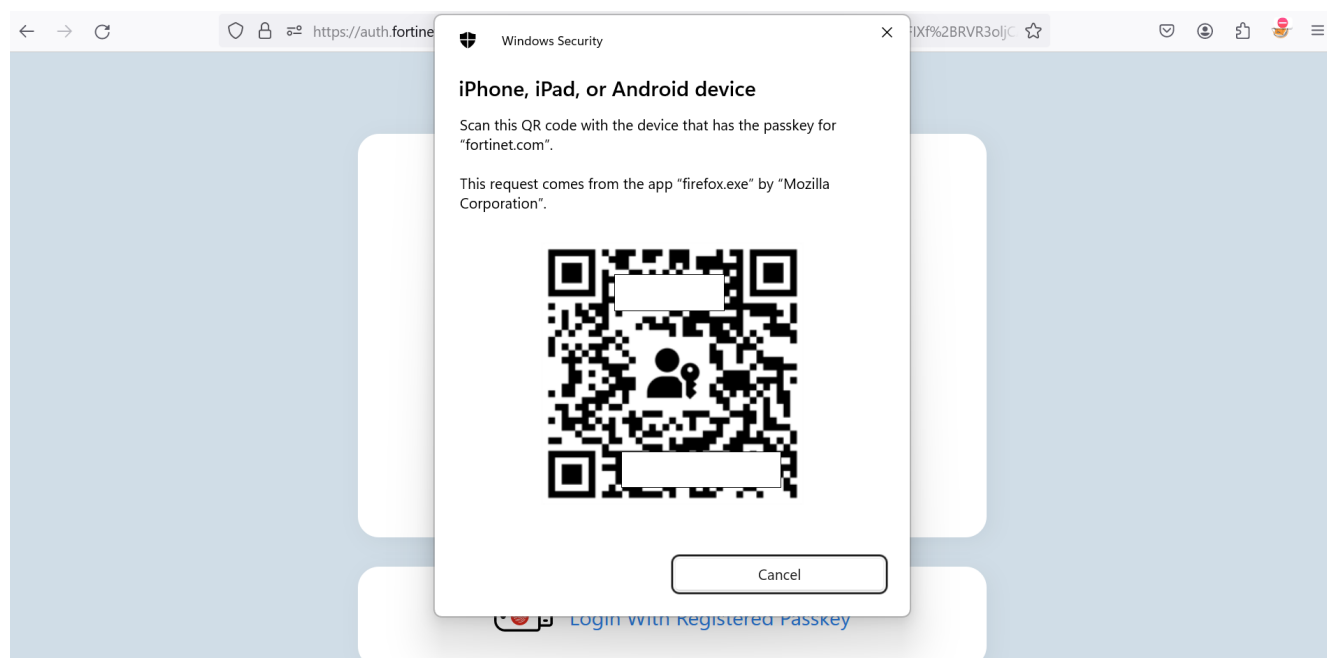
1. After successfully authentication with the external identity provider in his computer for a configured service provider, user (Todd in this case) will be presented with the auth.fortinet.com page from FTC for MFA. Choose 'Login with

Registered Passkey'.

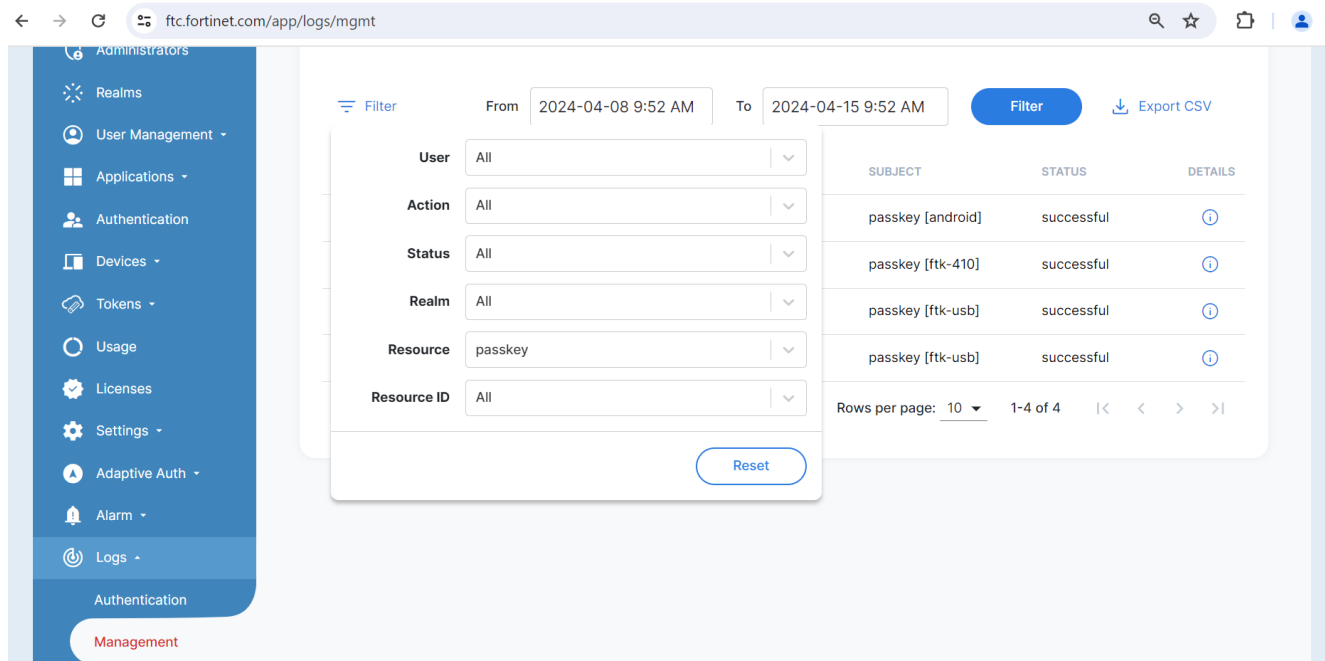


The image shows a login form titled "Login to Your Account". It has two input fields: "Username" with the text "todd@[ ]net" and "Token" with the text "OTP code". Below these fields is a blue "Submit" button. At the bottom of the form, there is a link with a passkey icon and the text "Login With Registered Passkey".

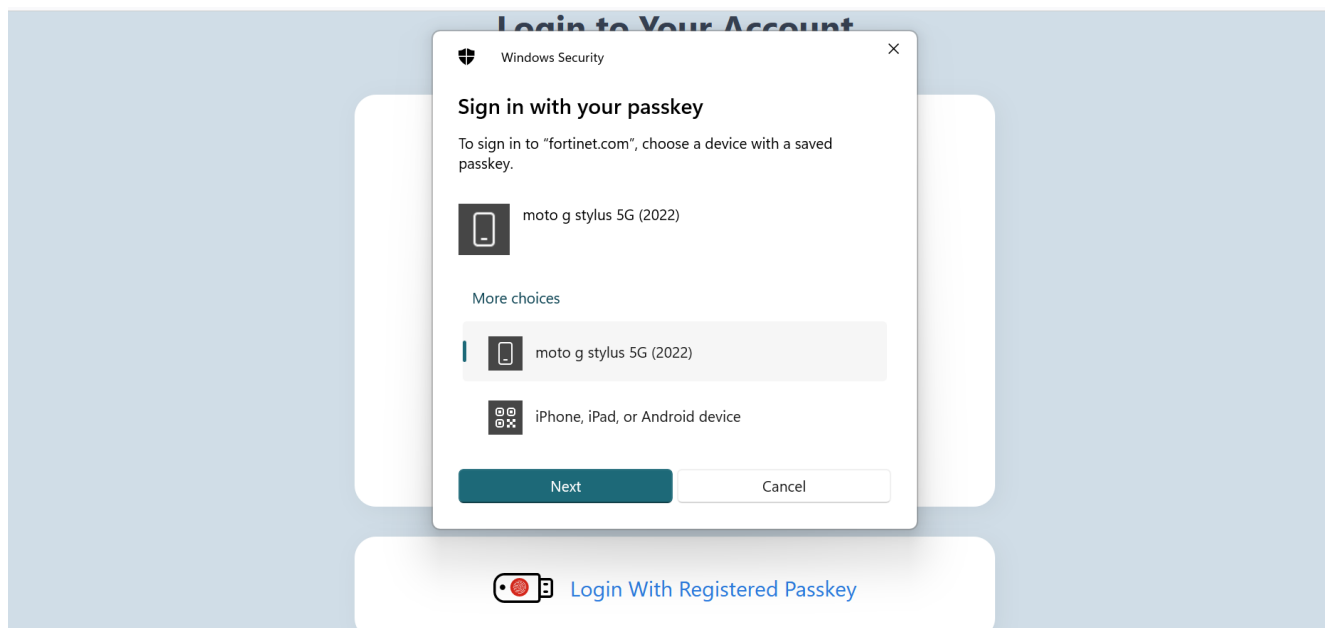
2. As the phone is used for the first time after provisioning, a QR code will popup. Todd will scan the QR code.



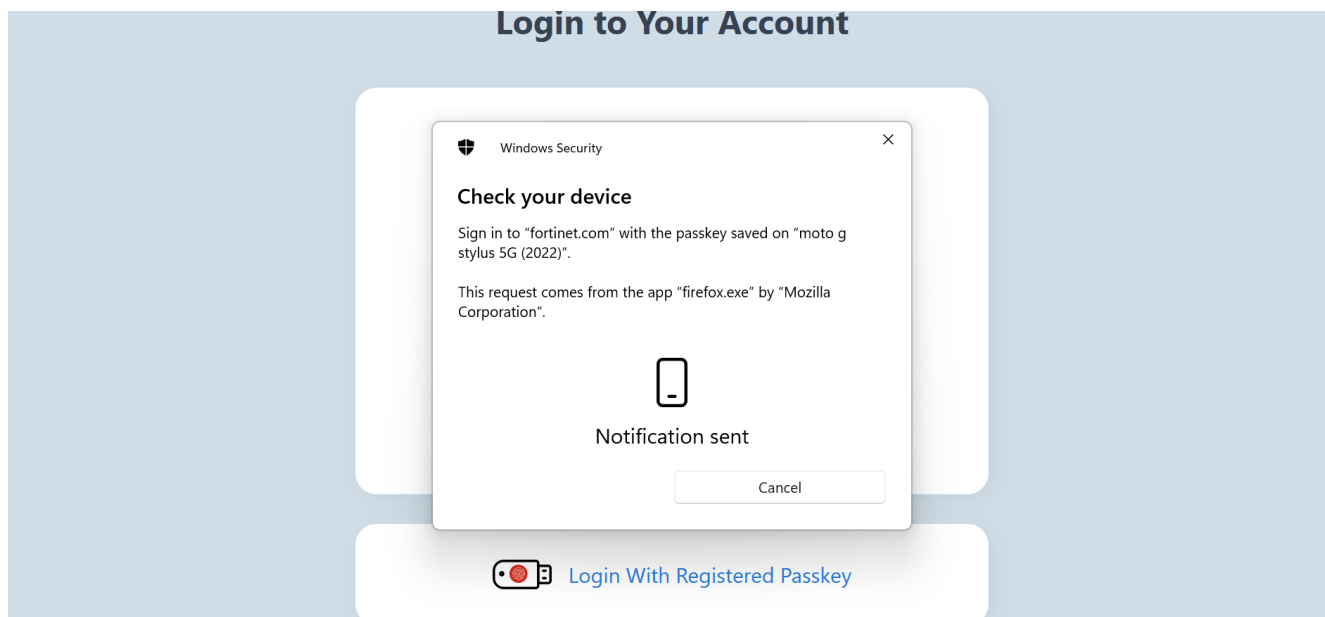
3. Follow the instruction on the phone to provide screenlock or other authentication mechanisms in the phone and it will register the phone successfully



4. After the steps in the phone are completed successfully, Todd will be able to login to the service provider successfully.
5. Now that the android phone is registered with Todd's computer, when Todd tried to login the next time, his phone will be listed as one of the choices. (moto g stylus 5G (2022) in the following screenshot).



6. Clicking on the phone as the choice will send a notification to the phone and the user will then have to provide the screenlock or other authentication mechanisms configured in the phone to authenticate..



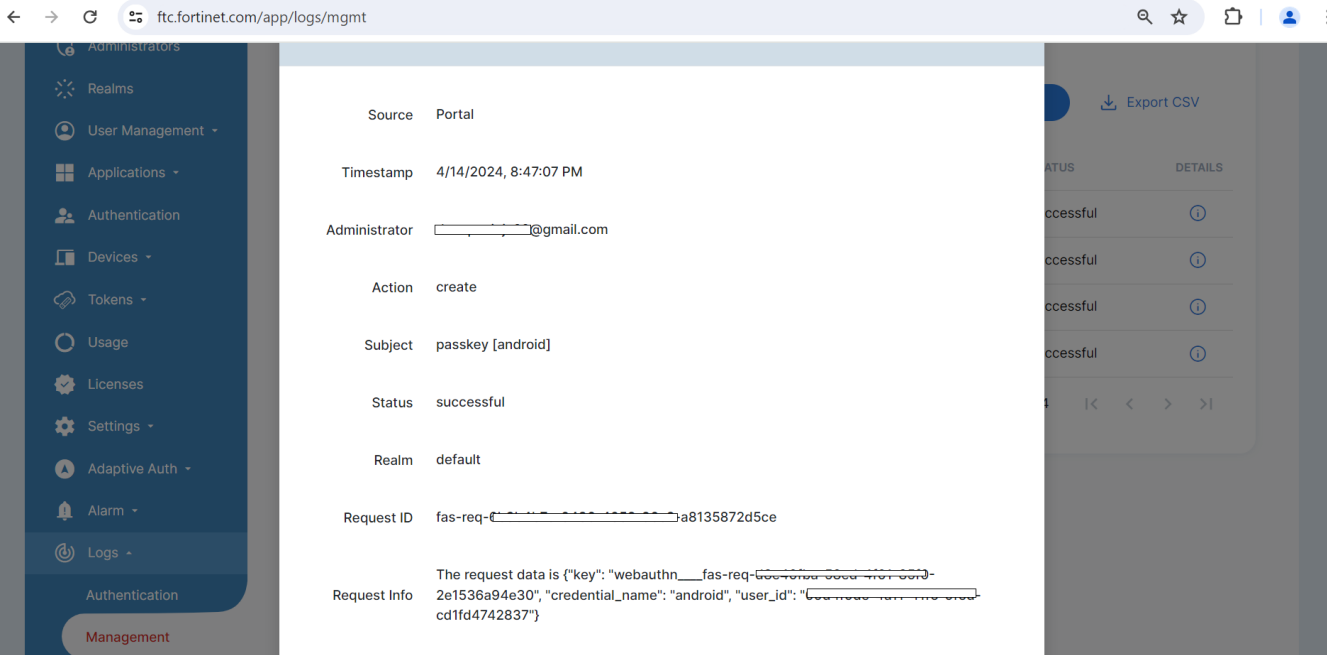
## Logs for Passkeys

### Management Logs:

The FTC admin can view all the management logs by navigating to Logs > Management. In the Filter option, Passkey logs can be filtered by choosing the resource as 'Passkey'.

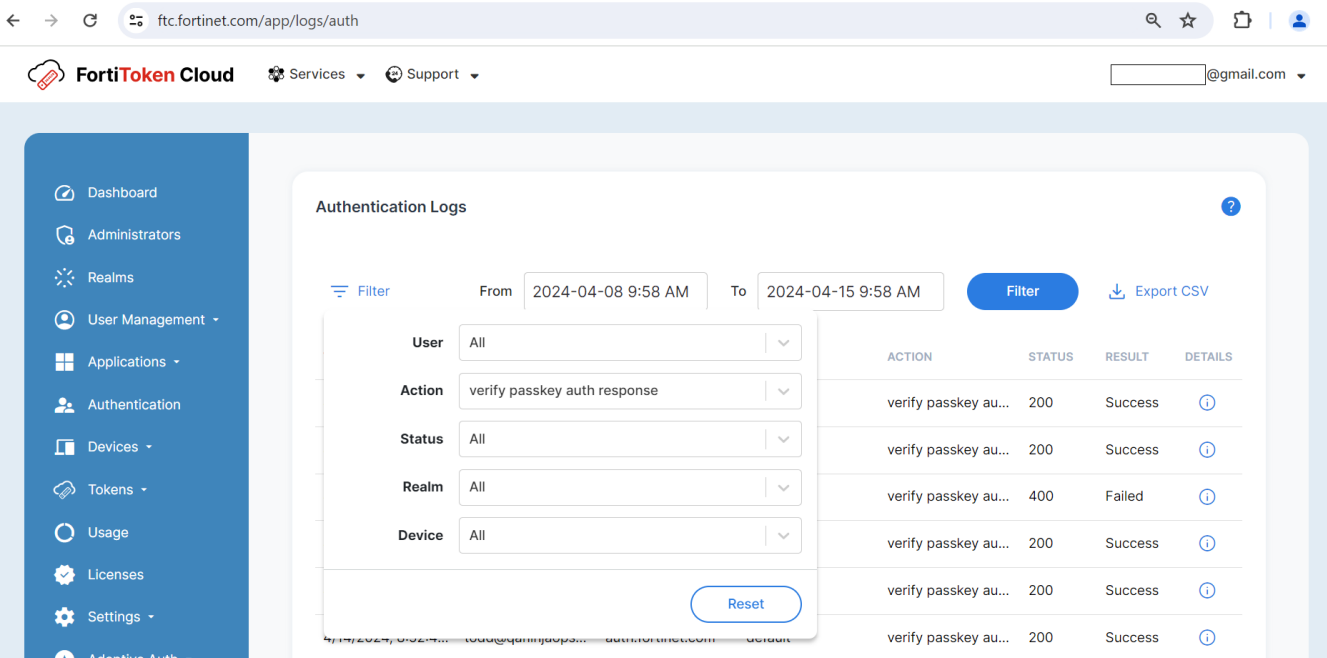
SUBJECT	STATUS	DETAILS
passkey [android]	successful	<a href="#">Details</a>
passkey [ftk-410]	successful	<a href="#">Details</a>
passkey [ftk-usb]	successful	<a href="#">Details</a>
passkey [ftk-usb]	successful	<a href="#">Details</a>

Detailed logs from each row can be viewed by clicking on the Details icon

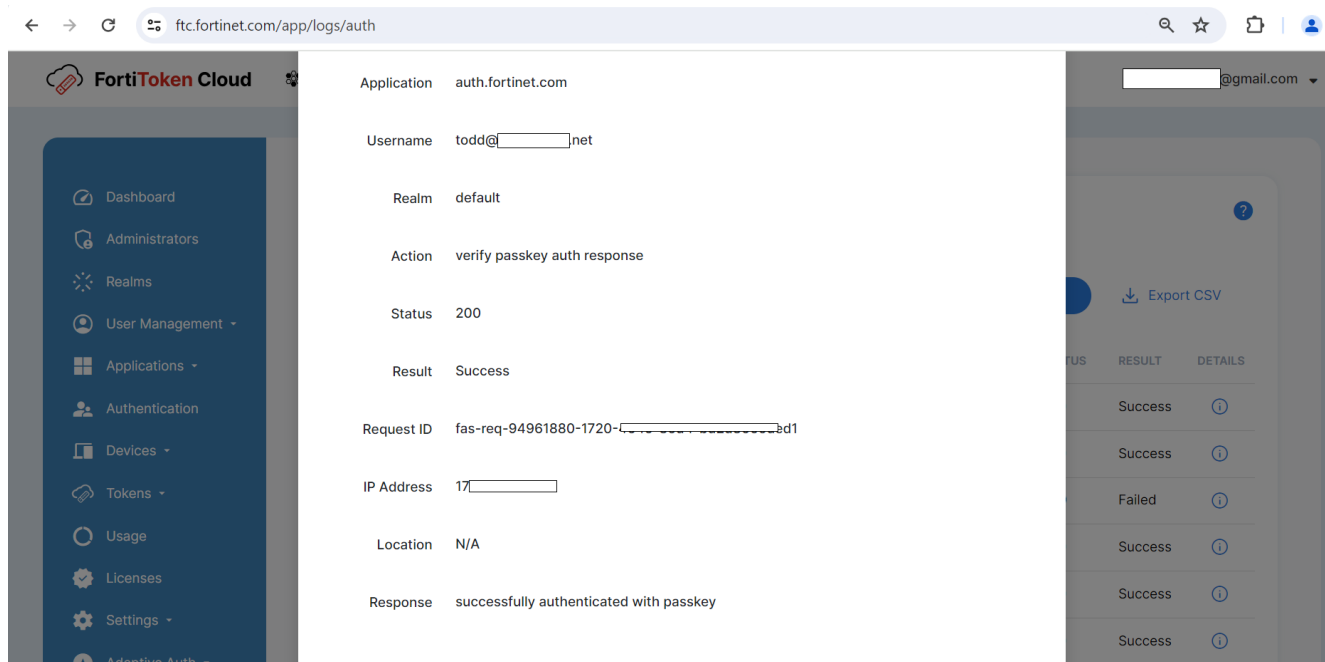


### Authentication Logs

The FTC admin can view all the management logs by navigating to Logs > Management. In the filter option choose 'verify passkey auth response' against Action to narrow the search to passkey auth responses.



Click on details icon on any row to view details log information.

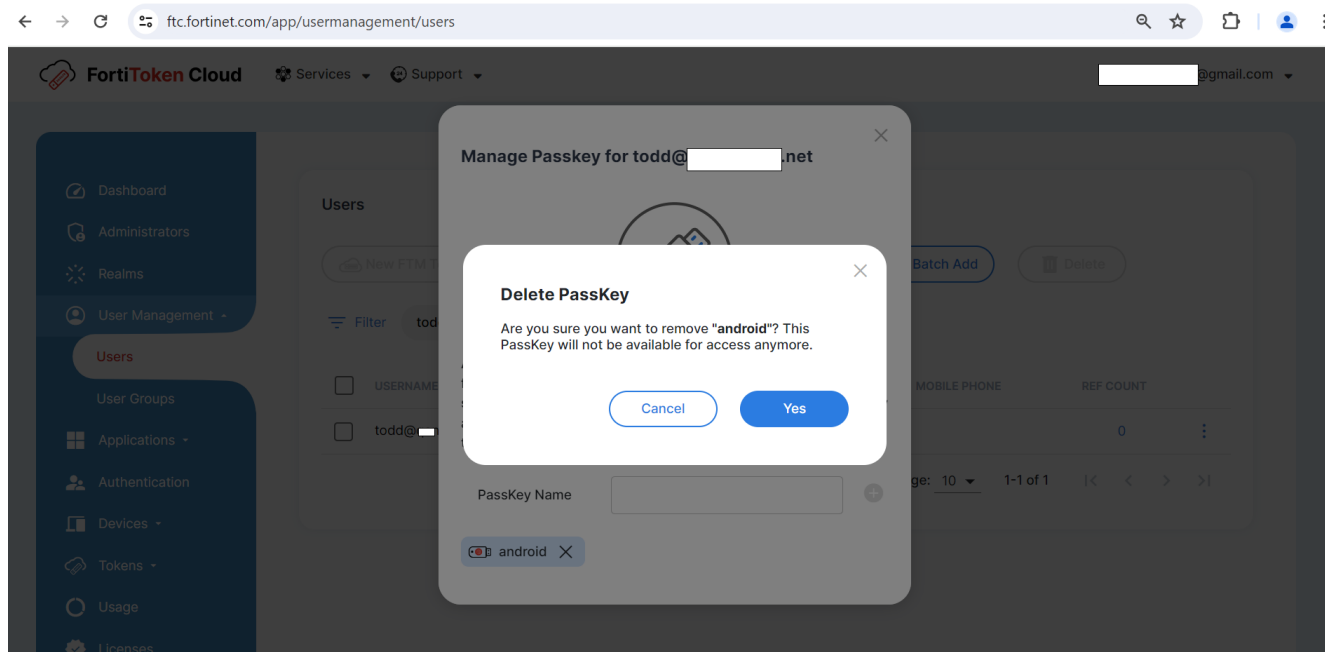


## Delete PassKey

There are two ways to delete passkeys. The following are the options

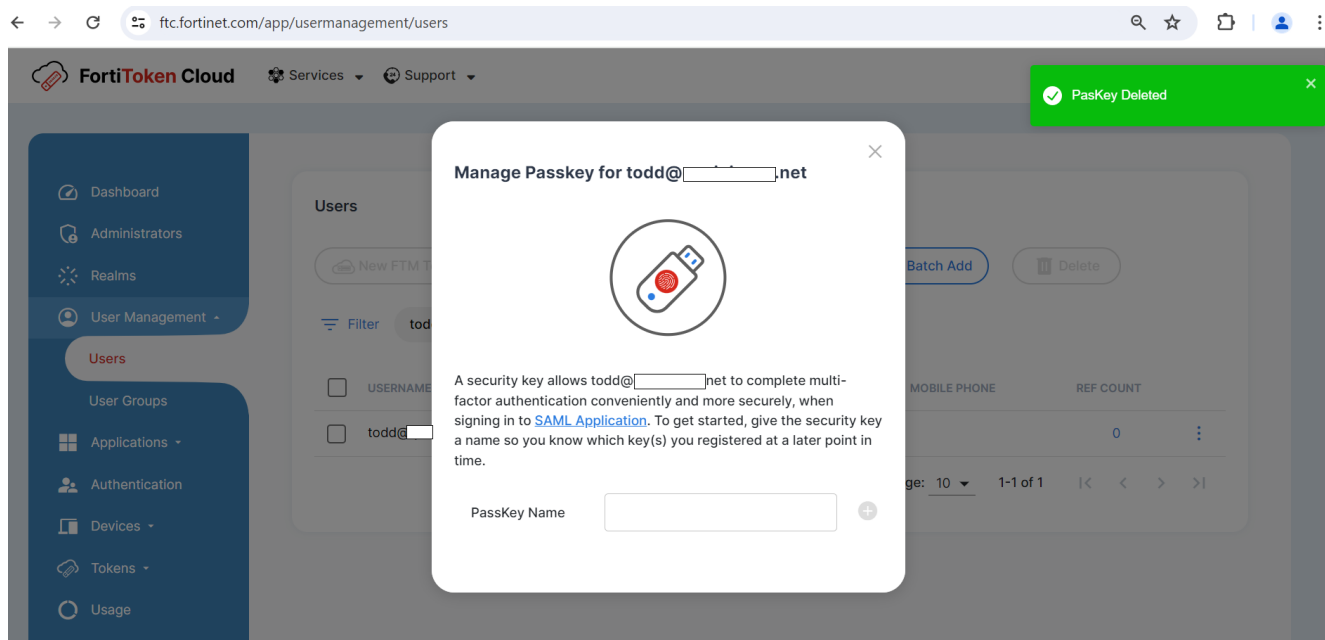
### Delete from User Management

1. Navigate to users , search for the user and click 'Manage Passkeys'. Click on the 'X' against the passkey and you will get a confirmation prompt.



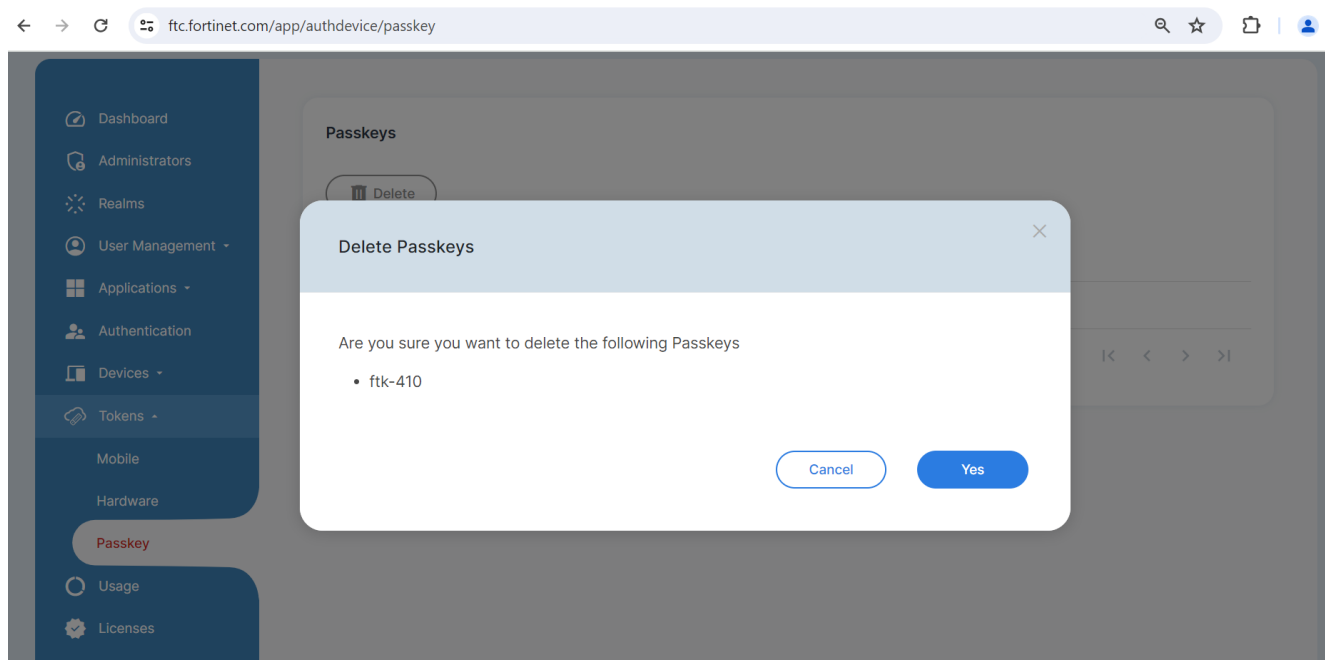


2. Click on 'Yes' and the Passkey will be deleted.



## Delete from Passkey Management

1. Navigate to 'Token > Passkey'. choose the Passkey to be deleted and click on 'Delete'. Click on 'Yes' in the confirmation prompt to have the passkey deleted.



# 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



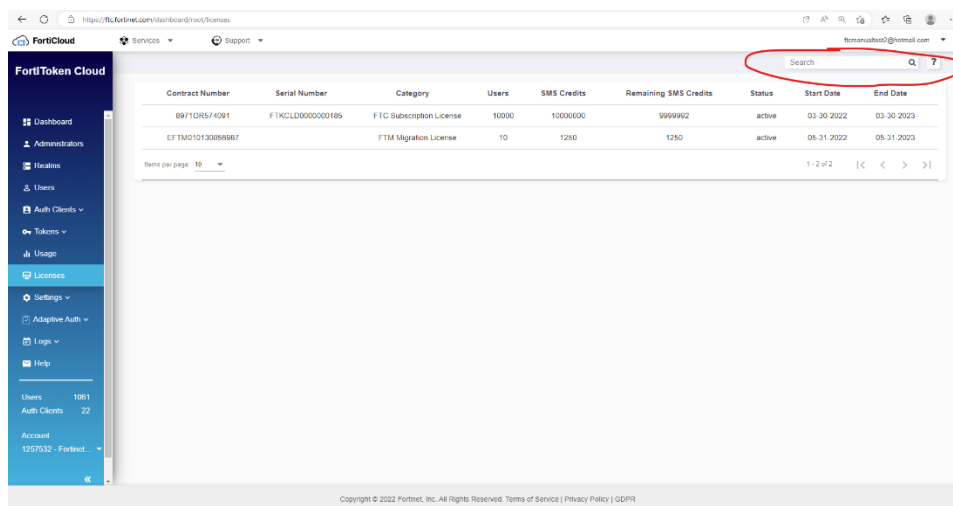
The *Licenses* page applies to customers of time-based subscriptions only. For more information about the time-based subscriptions, see [Subscription licensing on page 11](#).

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

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

## License search bar

There is a newly added search bar in the Licenses tab which should now allow you to search licenses by typing in keywords related to any of the fields of the license you are searching for. This should make it easier to find your licenses if you have many in your account.



# Manage global settings



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 224](#)
- [Auto-create an application on page 225](#)
- [Share-quota Mode on page 225](#)
- [Username Case & Accent Sensitive on page 225](#)
- [Account Disable/Delete Notification on page 226](#)

## 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 applications to better allocate and manage applications and end-users.

By design, *Multi-realm Mode* is enabled for new FTC customers. When *Multi-realm Mode* is disabled, new applications are assigned to the default realm; when multi-realm mode is enabled, new applications 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 applications to them. You must assign an application 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 applications support the "pre-generated applications" feature and *Multi-realm Mode* is enabled, you cannot add users to or sync users from pre-generated applications 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 [Manage realms on page 113](#).

## Auto-create an application



This feature applies to FortiGate/FortiOS VDOMs only.

---

Normally, the FortiGate administrator can add a VDOM to FTC as an application 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 application. This may inadvertently allow unintended applications to consume your FTC quotas or credits. To prevent this from happening, FTC has introduced the *Auto-create application* option to make the "add-auth-client-on-creation-of-first-user" feature optional in its global settings.

## Disable Auto-create application

By default, *Auto-create application* 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 application* button to turn it off.
3. In the *Auto-create application* dialog, read the messages and click *OK* to proceed.
4. Click *Apply Changes*.
5. Click *Confirm*.

## Enable Auto-create application

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

## Share-quota Mode

When *Share-quota Mode* is enabled (by default), the remaining user quotas will be shared by all realms. When it is disabled, the remaining user quotas will not be shared among realms.

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

By default, *Account Disable/Delete Notification* is enabled, but you can click the button turn it off.

## Manage realm settings

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

- [General settings on page 226](#)
- [FTM MFA settings on page 229](#)
- [Email MFA settings on page 231](#)
- [SMS MFA settings on page 231](#)


**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 settings

Parameter	Default value
<b>Default MFA Method</b>	<p>Select one of the following as the default MFA method that your FTC uses to authenticate end users:</p> <ul style="list-style-type: none"> <li>• <i>FTM</i> (default)—FTC sends a unique one-time passcode (OTP) to the FortiToken Mobile app on end-users' smart phones.</li> </ul> <p><b>Note:</b> This option requires that your end users must have the FortiToken Mobile app installed on their smart phones.</p>

Parameter	Default value
	<ul style="list-style-type: none"> <li><b>SMS</b>—FTC sends an OTP via text message to your end-users' smart phones. Upon receiving the OTP, the end-user must enter it on the log-in page to gain access to the application. <b>Note:</b> To use this option, FTC must have the end users' valid smart phone numbers in its database.</li> <li><b>Email</b>—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 application (i.e., FGT or FAC).</li> <li><b>FTK</b>—FTC requires end-users to provide the OTP generated by their FortiToken (hardware token) for MFA. <b>Note:</b> 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 <a href="#">Use hardware tokens on page 200</a>. 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 <a href="#">Manage users on page 115</a>.</li> </ul>
<b>Max Login Attempts Before Lockout</b>	<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><b>Note:</b> FTC does not allow locked users to authenticate. Instead, it displays the message "Locked, please try again in &lt;lockout interval&gt; minutes."</p>
<b>Lockout Period</b>	<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>
<b>Enable Bypass</b>	<p>Enable or disable bypass.</p> <ul style="list-style-type: none"> <li><b>Enable</b>—End-users can bypass MFA. If enabled, you must also set the <i>Bypass Expiration Time</i>, as described below.</li> <li><b>Disable</b> (default)—End-users cannot bypass MFA.</li> </ul> <p><b>Note:</b> 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 <a href="#">Manage users on page 115</a>.</p>
<b>Bypass Expiration Time</b>	<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>
<b>Auto-alias by Email</b>	<p>Enable or disable the <i>Auto-alias by Email</i> feature.</p> <p><b>Note:</b> The feature is disabled by default. For more information, see <a href="#">Enable Auto-alias by Email on page 228</a>.</p>
<b>Allow Rooted Device</b>	<p>This option is enabled by default. When it is disabled, FTC will remove all the tokens it has issued for rooted devices when end users are trying to activate new tokens using the devices. This will render the devices unusable with FTC.</p> <p>When you re-enable the option, rooted devices can be used to activate new tokens.</p>

Parameter	Default value
<b>Replay Protection</b>	<p><i>HIGH (forbid all replays)</i> – The authentication follows the current mechanism and does not allow any OTP replay.</p> <p><i>MEDIUM (ignore FTM push replay)</i> – The authentication counts OTP replays for manual input only. All the requests from push authentications are not counted and are not restricted by OTP replay protection.</p> <p><i>LOW (ignore FTM/FTK auth replay)</i> – OTP replay protection is disabled.</p> <p><b>Note:</b> For email and SMS, OTP replay are always rejected no matter what the setting is.</p>
<b>Adaptive Auth Profile</b>	Select an adaptive auth profile.
<b>Allowed MFA Methods</b>	<div>  <ul style="list-style-type: none"> <li>This feature enables end users of SSO applications to authenticate using MFA methods other than the default setting, based on the configuration made by the administrator.</li> <li>If the Default MFA Method is set to SMS, setting Email to be an allowed MFA method here will let FTC automatically switch to email authentication and send OTP codes by email if the end users are unable to use SMS.</li> </ul> </div> <p>The drop-down menu shows all the MFA methods that you may allow your end users to use. By default, all the options except Email are preselected. If you are satisfied with the default settings, do nothing; otherwise, you can use the tools here to customize your allowed MFA methods.</p> <ul style="list-style-type: none"> <li><i>All</i> – Select all allowed options at once.</li> <li><i>Passkey</i> (preselected) – Select Passkey.</li> <li><i>FTK</i> (preselected) – Select FTK.</li> <li><i>FTM</i> (preselected) – Select FTM.</li> <li><i>SMS</i> (preselected) – Select SMS.</li> <li><i>Email</i> – Select Email. Refer to the note above.</li> </ul>

## 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 applications. 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 MFA settings

Parameter	Default value
<b>1. Settings</b>	
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"> <li>• <i>Email</i>—Token activation/transfer codes are sent to users' email addresses.</li> <li>• <i>SMS</i>—Token activation/transfer codes are sent by SMS to users' mobile phone numbers.</li> </ul> <p><b>Note:</b> 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 <a href="#">Manage users on page 115</a>.</p> <p><b>Note:</b> 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"> <li>• <i>Disabled</i> (default)—No app PIN is required.</li> <li>• <i>Enable</i>—If enabled, you must select a PIN Length and PIN Required Mode, as described below.</li> </ul>
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"> <li>• 4</li> <li>• 6 (default)</li> <li>• 8</li> </ul> <p><b>Note:</b> 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"> <li>• <i>Anytime</i>—App PIN is required all the time.</li> <li>• <i>Unlock</i>—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.</li> </ul>
OTP Algorithm	<ul style="list-style-type: none"> <li>• <i>TOTP</i> (default). No action is needed.</li> </ul>

Parameter	Default value
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"> <li>• 30 (default)</li> <li>• 60</li> </ul> <p><b>Note:</b> <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"> <li>• 6 (default)</li> <li>• 8</li> </ul> <p><b>Note:</b> 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><b>Note:</b> 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"> <li>• <i>Upload Custom Logo</i>—Click this button to upload a custom logo image to replace the default Fortinet logo. For instructions on how to use this feature, see <a href="#">Use a custom logo on page 230</a>.</li> <li>• <i>Restore Default Logo</i>—Click this button to reverse to the default Fortinet logo on FTM.</li> </ul>
<b>2. Notification Templates</b>	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 settings

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. <b>Note:</b> 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. <b>Note:</b> You can view the content of the selected template by clicking the view button on the right.

## SMS MFA settings

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 application.

Parameter	Description
1. Settings	

Parameter	Description
OTP Expiration Time	Click the down arrow to select an OTP expiration time. <b>Note:</b> 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. <b>Note:</b> You can view the content of the selected template by clicking the view button on the right.

## Use templates

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

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



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

## Add a template

To add a template:

1. On the main menu, click *Settings>Templates* to open the *Templates* page.
2. In the upper-left corner of the *Templates* page, click *Add Template*.  
The *Add New Template* dialog opens.
3. For *Method*, click the down arrow to select a notification method.  
**Note:** Method refers to the means that FTC uses to send OTP and token activation or transfer notifications to its end-users. To use email, you must provide a valid email address; to use SMS, you must provide a valid phone

number with the correct country code for each and every end-user.

4. For *Type*, click the down arrow to select a desired message template.  
**Note:** FTC offers three types of template, and each template is for a specific purpose. Be sure to create all the three types of template to take full advantage of this feature.
5. Click *Confirm*.  
The dialog refreshes, showing more fields.
6. Specify a unique name for the template.
7. Make the desired changes to the subject of the message, if you like.
8. Make the desired changes to the message content, if you like.
9. Click *Preview* to review the message.
10. Click *Save*.

## Edit a template



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

---

### To edit a template:

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

## Delete a template



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

---

### To delete a template:

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

4. Click **Yes**.
5. The template is deleted from the *Templates* page after the page refreshes.

## Apply templates



All templates are applied at the realm level.

---

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

1. On the main menu, click *Realms* to open the *Realms* page.
2. On the *Realms* page, locate the realm of interest and mouse over it.  
The tool bar slides in from the right end of the row.
3. Click the *Settings* tool to open the *Realm* page.
4. Across the top of the *Realm* page, click the *FTM Setting* tab.
5. Scroll down the page and click *Notification Templates*.
6. In each of the field, click the down arrow and select the template of interest.
7. Click *Apply Changes*.  
The selected templates are now applied to the realm and will be used when FTC sends token activation and/or transfer notifications to your end-users.

### To apply an email OTP template:

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

### To apply an SMS OTP template:

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

## Manage custom branding

The branding feature enables you to customize the look and feel of your SSO applications or end-user portals with your own branding theme. This includes background color, text color, and button color, etc. You can also use your own logos or tag lines.

- [Create an SSO application branding theme on page 235](#)
- [Create an end-user portal branding theme on page 235](#)
- [Delete a branding scheme configuration on page 236](#)
- [Apply custom branding theme to SSO application on page 236](#)
- [Apply custom branding theme to end-user portals on page 237](#)

### Create an SSO application branding theme

1. From the main menu, select *Settings > Branding > Add Branding*.
2. In the *Add New Branding* dialog, make the entries and selections as described in the following table.
3. Click *Save* when done.

Parameter	Description
Name	Enter a unique name for the SSO application branding theme configuration.
Site	Single Sign-On
Primary Color	Select the primary color of the SSO application branding theme.
Accent Color	Select the accent color of the SSO application branding theme.
Logo	Copy and paste the link to your logo image file here.

### Create an end-user portal branding theme

1. From the main menu, select *Settings > Branding > Add Branding*.
2. In the *Add New Branding* dialog, make the entries and selections as described in the following table.
3. Click *Save* when done.

Parameter	Description
Name	Enter a unique name for the end-user portal branding theme configuration.
Site	Click the down arrow and select End-user Portal from the drop-down menu.
Button Background Color	Select the button background color.
Button Color	Select the button color.
Menu Background Color	Select the sidebar menu background color.
Sidebar Menu Active	Select the menu active background color.

Parameter	Description
Background Color	
Sidebar Menu Font Color	Select the sidebar menu font color.
Landing Logo	Copy and paste the link to your landing logo image file here.
Logo	Copy and paste the link to your logo image file here.
Tagline	Enter your tagline.
Subtagline	Enter your subtagline.

## Delete a branding scheme configuration

1. From the Settings>Branding page, locate the branding scheme configuration.
2. Click the tool button at the end of the row, and select *Delete* from the drop-down menu.
3. Click *Yes*.

To delete multiple branding scheme configurations at once:

1. Select all the branding scheme configurations.
2. From the top of page, click *Delete*.
3. Click *Yes*.

## Apply custom branding theme to SSO application

1. Click *Applications > SSO Applications > Add SSO Application*.

2. For Custom Branding, click the down arrow and select the branding theme from the drop-down list.



## Apply custom branding theme to end-user portals

1. Click *Applications > End-user Portals > Add New Portal*.
2. In the *General* section of the *Add New User Portal*, locate the Custom Branding field, click the down arrow, and select the desired branding theme.

## Manage certificates

The Certificates page enables you to configure Identity Provider (IdP) Signing Certificates. This certificate is used by the IdP Proxy to sign SAML assertions, ensuring that data exchanged between the IdP and Service Provider (SP) is secure and authentic.

## 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 238](#)
- [Create an adaptive authentication policy on page 238](#)
- [Edit an adaptive auth policy on page 239](#)
- [Delete an adaptive auth policy on page 240](#)
- [View adaptive auth profiles on page 240](#)
- [Create an adaptive authentication profile on page 240](#)
- [Edit an adaptive auth profile on page 241](#)
- [Delete an adaptive authentication profile on page 241](#)
- [Apply adaptive authentication profiles on page 241](#)

## 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
<b>Name</b>	The name of the policy.
<b>Action</b>	<p>The action specified in the policy, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Multi-factor Authentication</i> (default)</li> <li>• <i>Block</i></li> <li>• <i>Bypass</i></li> </ul> <p><b>Note:</b> The FTC server takes the specified action when an authentication request matches the policy.</p>
<b>Profile References</b>	The adaptive authentication profile that uses the policy.
<b>Last Update</b>	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
<b>Name</b>	Specify a unique name for the policy.
<b>Action</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Enforce MFA</i> – By default, the FTC server will require login attempts from the specified source to use MFA.</li> <li>• <i>Block</i> – The FTC server will block login attempts from the specified source.</li> <li>• <i>Bypass MFA</i> – The FTC server will let the login attempts from the specified</li> </ul>

Parameter	Description
	<p>source bypass the MFA requirement.</p> <p><b>Note:</b> The FTC server takes the specified action when an authentication request matches the policy settings.</p>
<b>Filters</b>	<p>Select the filter</p> <ul style="list-style-type: none"> <li>• <i>Subnet Filter</i> – See <i>Subnet Filter</i> below.</li> <li>• <i>Location Filter</i> – See <i>Location Filter</i> below.</li> <li>• <i>No Source Filter</i> – Select this option if you do not want to use any filter.</li> <li>• <i>Schedule</i> – Check the checkbox to enable scheduling. See <i>Schedule</i> below for details.</li> </ul>
<b>Subnet Filter</b>	<p><b>Note:</b> 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"> <li>• IP address, e.g., 10.10.1.1</li> <li>• IP range, e.g., 10.10.0.0 - 10.10.10.2</li> <li>• CIDR notation, e.g., 10.10.1.0/24</li> </ul> <p><b>Note:</b> 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>
<b>Location Filter</b>	<p><b>Note:</b> 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"> <li>• Use the list menu to select the countries or regions of interest.</li> <li>• Select Unknown Country or Region if the location is unknown.</li> </ul>
<b>Schedule</b>	<p><b>Note:</b> 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"> <li>• <i>Weekdays</i> – Select the days of the week.</li> <li>• <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.</li> <li>• <i>Time Range</i> – Select either <i>All day</i> (default) or a specific time frame of the day. <b>Note:</b> 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.</li> </ul>

## 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
<b>Name</b>	The name of the adaptive auth profile.
<b>Action</b>	<p>The action specified in the policy, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Multi-factor Authentication</i> (default)</li> <li>• <i>Block</i></li> <li>• <i>Bypass</i></li> </ul> <p><b>Note:</b> The FTC server takes the specified action when an authentication request matches the profile.</p>
<b>Realm References</b>	The number of realms that are using the profile.
<b>Client References</b>	The number of applications 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
<b>Name</b>	Specify a unique profile name.
<b>Default action</b>	<p>Select a default action, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Multi-factor Authentication</i> (default)</li> <li>• <i>Block</i></li> <li>• <i>Bypass</i> (<b>Note:</b> If an authentication did not fall into any policies, FTC will take this action on the authentication request.)</li> </ul>
<b>Policy Sequence</b>	Select the priority of the policies to be selected below.

Parameter	Description
	<b>Note:</b> The two policy fields below could be empty (no selection). If no policy is selected, the FTC server takes the default action specified above. When two policies are selected, Policy 1 takes priority over Policy 2.
Policy 1	Select a policy as Policy 1. (Optional)
Policy 2	Select a policy as Policy 2. (Optional)

## Apply adaptive authentication profiles

Adaptive authentication profiles can be applied to applications and/or realms. A profile applied to applications has higher priority than a profile applied to realms. For example, an authentication from application 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 application:

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

### To apply an adaptive auth profile to a realm:

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

## Edit an adaptive auth profile

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

## Delete an adaptive authentication profile

### To delete an adaptive authentication profile:

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

## Create a last-login policy

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

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

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

## Create an impossible-to-travel policy

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

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

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

# Alarms

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

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

- [Configure receivers on page 243](#)
- [Configure receiver groups on page 243](#)
- [Create a user quota alarm event on page 244](#)
- [Create an SMS credit balance alarm event on page 243](#)

## Configure receivers

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

## Configure receiver groups

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

## Create an SMS credit balance alarm event

1. From the main menu, select *Alarm>Event*.
2. On top of the page, click *Add Alarm Event*.
3. For *Resources*, select *SMS*.
4. For *Level*, select *Realm* or *Global*. (Note: If *Global* is selected, the alarm will be applied to your entire account; if *Realm* is selected, you must select the specific realm or realms from list of realms.)

5. For *Threshold*, enter the numeric value to be used as the SMS credit threshold.
6. Enter a description of the alarm event. (Optional)
7. For *Groups*, select the receiver group(s).
8. Click *OK*.

## Create a user quota alarm event

1. From the main menu, select *Alarm>Event*.
2. On top of the page, click *Add Alarm Event*.
3. For *Resources*, select *users*.
4. For *Level*, select *Realm* or *Global*. (Note: If *Global* is selected, the alarm will be applied to your entire account; if *Realm* is selected, you must select the specific realm or realms from list of realms.)
5. For *Threshold*, enter a value between 0 and 99 as a percentage.
6. Enter a description of the alarm event. (Optional)
7. For *Groups*, select the receiver group(s).
8. Click *OK*.

## Logs

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

FTC has two types of logs:

- [Authentication on page 244](#)
- [Management on page 246](#)
- [SMS on page 248](#)

## 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. <b>Note:</b> 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.
application	Shows either of the following: <ul style="list-style-type: none"> <li>The serial number and VDOM name if the application is an FGT device.</li> <li>The source IP address if the application is a third-party device.</li> </ul>
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 <a href="#">List of HTTP Status Codes</a> .
Result	The outcome of an authentication request, which can be either of the following: <ul style="list-style-type: none"> <li><i>Success</i></li> <li><i>Failed</i></li> </ul>

## 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*
- *applications*
- *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"><li>• <i>application</i></li><li>• <i>FTC portal</i></li></ul>
Timestamp	The date and time of the request. <b>Note:</b> 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"><li>• The serial number of FGT if the request was made from FGT.</li><li>• The username of the FTC user if the request was made from the FTC portal.</li></ul>
Action	The action of the request, which can be one of the following: <ul style="list-style-type: none"><li>• <i>Create</i></li><li>• <i>Get</i></li><li>• <i>Modify</i></li></ul>
Subject	The target of an action. For example, who or what is changed? <b>Note:</b> If the subject is an FTC end-user, it should also include the account to which the user belongs.
Location	Location where the administrator logged in to the system.
IP Address	The IP address of the device from which the administrator logged in.
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.
application	The application that sent SMS message.
Realm	The realm to which the application is assigned.
Action	The action that FTC took.
User	The end-user upon whom the action was performed.
Country	The country or region where the end-user's phone number is registered.
Rate	The wireless phone rate.

## Filter SMS logs

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

## Filter logs by date

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

3. Click *Filter*.

## Export SMS logs

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

# FOS CLI commands for FortiToken Cloud

This section discusses the FOS (version 6.4.0 and later) CLI commands supported in this FTC release.

- [Global system configuration on page 250](#)
- [Access FTC management commands on page 250](#)
- [Configure admin users on page 251](#)
- [Configure local users on page 252](#)
- [Configure local LDAP users for FTC service on page 253](#)
- [Configure wildcard LDAP users for FTC service on page 253](#)
- [Configure local RADIUS users for FTC service on page 254](#)
- [Diagnose FortiToken Cloud on page 255](#)
- [Show user ldap on page 256](#)

## 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 applications (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 "FG101ETK000000000"
  set hostname "FG101ETK000000000"
  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.

```

FG101ETK00000000 # 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.

FG101ETK00000000 # execute fortitoken-cloud new ?
<user name>   User name for new token.

FG101ETK00000000 # execute fortitoken-cloud sync ?
<user type>   {Enter <return> | all | local | remote}

FG101ETK00000000 # execute fortitoken-cloud trial ?
<Enter>

FG101ETK00000000 # 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 `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+xpmpksgsJ9CfAMIjG8Z0Vu8yGDk=
  next
end

```

Command	Description
<code>config system admin</code>	Starts the configuration of a system admin user.
<code>edit &lt;username&gt;</code>	Specify the admin username.

Command	Description
<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> .
<code>set two-factor</code>	Select an MFA method: <ul style="list-style-type: none"> <li><code>disable</code>—No MFA.</li> <li><code>fortitoken</code>—FortiToken (FTK) or FortiToken Mobile (FTM).</li> <li><code>email</code>—Email.</li> <li><code>sms</code>—Simple message service. This option requires an SMS server and SMS phones.</li> <li><code>fortitoken-cloud</code>—FortiToken Cloud. <b>Note:</b> FortiToken Cloud is the default MFA method.</li> </ul>
<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 EKhm1TBu1hmHUokESNTkNjxV8mBQ+AgyRP1Inw==
  next
end
```

Command	Description
<code>config user local</code>	Starts the configuration of a local user.
<code>edit &lt;username&gt;</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"> <li><code>disable</code>—No MFA.</li> <li><code>fortitoken</code>—FortiToken (FTK) or FortiToken Mobile (FTM).</li> <li><code>email</code>—Email.</li> <li><code>sms</code>—Simple message service. <b>Note:</b> This option requires an SMS server and SMS phones.</li> <li><code>fortitoken-cloud</code>—FortiToken Cloud. <b>Note:</b> FTC is the default MFA</li> </ul>



Command	Description
	method.
set email-to <email address>	Specify the email address to which the authentication code is sent.
set sms-phone	Set the mobile phone number for receiving SMS messages.
set passwd-time	Set the time the password is created.
set passwd	Set the password .

## Configure local LDAP users for FTC service

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 EKhm1TBu1hmHUokESNTkNjxV8mBQ+AgyRP1Inw==
  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=srv,dc=world"
    set type regular
    set two-factor fortitoken-cloud
    set username "cn=Manager,dc=srv,dc=world"
    set password ENC LWdyb+/k6e4TtSk070t0DaCZAcbgEGKohA==
  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.



- 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. An FTC account administrator can migrate FTM token to FTC from any FTC-supported FortiProducts. The following sections show to;

- [Migrate FTM tokens from FortiGate on page 71](#)
- [Migrate FTM tokens from FortiAuthenticator on page 72](#)

## Diagnose FortiToken Cloud

Use the following commands to diagnose and troubleshoot FTC issues.

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

### Examples

```
FG100D3G000000000 (global) # diag fortitoken-cloud debug {enable | disable}
```

```
FG100D3G000000000 (global) # diag fortitoken-cloud server
```

```
FG100D3G000000000 (global) # diag fortitoken-cloud show {server | realm | users | user <username> <VDOM>}
```

```
FG100D3G000000000 (global) # diag fortitoken-cloud delete <username>
```

```
FG100D3G000000000 (global) # diag fortitoken-cloud set-http <number>
```

```
FG100D3G000000000 (global) # diag fortitoken-cloud clear <Enter>
```

```
FG100D3G000000000 (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}
```

```

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm
<string>      Enter command: show, start, abort, add-users, delete-users, ftm2ftc.
FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm show
<string>      FTM license number.

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm start
<string>      FTM license number.

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm abort
<string>      FTM license number.

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm add-users
<string>      FTM license number.

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm delete-users
<string>      FTM license number.

FGVM01TM00000000 (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.

## Show user ldap

Starting from FortiOS 7.2.1, the `group-filter` setting has been replaced with `two-factor-filter`, as shown in the following example command:

```

FGVMULTM24003711 (root) # show user ldap
config user ldap
  edit "ad-136"
    set server "10.160.13.6"
    set cnid "sAMAccountName"
    set dn "DC=cloudsolutionsqa,DC=com"
    set type regular
    set two-factor fortitoken-cloud
    set two-factor-filter "(&(objectClass=user)(memberOf=Cn=ftc-ops,ou=QA,dc=cloudsolutionsqa,dc=com))"
    set username "ldapadmin"
    set password ENC

```

```


next
end

```

In this configuration, only users from group `ftc-ops` will be synched to FortiToken Cloud when running the execute `fortitoken-cloud sync` command. If the sync command is not run, only users from the configured group will be synched to FTC after the first login.

# Product documentation and support

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

- For information about the current release, see the [Release Notes](#).
- For detailed information about product features, click the  (Help) on the GUI or see [Admin Guide](#).
- For product API, see [REST API](#).
- For frequently asked questions, see [FAQs](#).
- For SSL VPN configuration instructions, see [SSL VPN Configuration Guide](#).
- For terms of service, see [Service Descriptions](#).
- For licensing, see [Purchasing Guide](#).
- For SMS rates, see [SMS Rate Card](#).
- For product support issues, click [Technical Support](#) (<https://docs.fortinet.com/document/fortitoken-cloud/latest/technical-support/891133/technical-support>).

# 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 30](#).

## 25.2.a

Release date: June 9, 2025

- Revamp of FortiToken Cloud GUI
- Support for Local IdP (beta feature)
- New terms for the free trial license
- Allow Rooted Device in realm settings.
- Support for OIDC OpenID Provider (OP)

## 25.1.a

Release date: January 16, 2025

- End-user Portals
- Integration with Microsoft Entra ID
- Allow additional MFA methods
- Integration with FortiClient to provide MFA service for FortiSASE VPN users

## 24.3.a

Release date: July 30, 2024

- Simplification of FortiGate SP configuration
- Default user source for IdP Proxy
- Addition of location and IP address to Management logs
- Limited access to Web application APIs and IdP-related APIs for trial customers
- FTC Introduction page for potential customers

## 24.2.a

Release date: May 3, 2024

- IdP Proxy
- Passkeys
- SCIM
- Batch-add users
- User groups
- FTM token migrations from FAC to FTC

## 23.4.b

Release date: December 21, 2023

- GUI revamping

## 23.4.a

Release date: November 16, 2023

- SMS rate update
- Support for pagination
- SMS restriction alert

## 23.3.b

Release date: August 11, 2023

FortiToken Cloud 23.3.b is a patch release only; no new feature or enhancement has been implemented in this release.

## 23.3.a

Release date: July 28, 2023



- **Data migration enhancement**—The *Devices (HA)* page has been updated to provide better user experience in managing transfer of device ownership. See [Transfer devices on FTC on page 195](#).
- **Last Login**—The Last Login column of the *Users* page now shows the timestamp of the user's most recent successful MFA login. See [Manage users on page 115](#).
- **Welcome email**—FTC now sends welcome email messages to customers when they start their free trial license or activate their paid license. See [Purchasing Guide](#).
- **Replay protection**—FTC now offers three levels of replay protection in realm setting configuration. See [General settings on page 226](#).

## 23.1.a

Release date: March 16, 2023

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

## 22.4.a

Release date: November 28, 2022

FortiToken Cloud 22.4.a offers the following new feature:

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

## 22.3.a

Release date: July 19, 2022

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

## 22.2.d

Release date: June 30, 2022

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

- Account Disable/Delete Notification

## 22.2.c

Release date: June 1, 2022

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

## 22.2.b

Release date: May 9, 2022

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

## 22.2.a

Release date: May 4, 2022

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

- Location Filter by country/region on Adaptive Auth page
- application 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 "applications/Max applications"

## 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 applications and serve their end-users.
- **API for generic applications**—The applications page now shows application type, application name, user count, and realm name.
- **Revamped GUI**—The applications page now has three sub-pages, with the FortiProducts sub-page showing application alias, application type, application 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 applications 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 application**—The **Settings>Global** page now has added an "Auto-create application" option, which enables the global admin user to enable or disable (default) the auto-creation of applications. 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 applications from consuming credits.
- **Administrators page enhancements**—The Administrators page has gone through some enhancements. You are now able to select multiple realms to add to an admin group, and to view all accounts associated with a customer ID by clicking the Member Count in the Administrators page.
- **Export to CSV**—The Usage page now has an option to enable you to export usage data in .csv file format.
- **Contact Support**—The main menu now has an "Contact Support" menu, which enables you to contact Fortinet support team by email directly from the FTC portal.

## 20.2.c

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

## 20.1.b

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

## 20.1.a

- **Hard Tokens**—FTC now supports FortiToken (FTK) which is a hardware token. See [Use hardware tokens on page 200](#).
- **Global administrator and sub-admins**—FTC now enables the global administrator to create sub-admins and allocate resources to them. See [Manage admin groups on page 110](#).
- **Multi-realm support**—FTC now allows the global admin to create realms. See [Manage realms on page 113](#).

- **More MFA methods**—This release adds support for e-mail, SMS, and FTK (FortiToken, which is a hardware token) as options for MFA. See .

## 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 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 for more information.
- **Access to all accounts by admin users**—FTC admin users are able to access all FTC accounts belonging to their own organization. They can choose which of their accounts to open upon login, and switch to any of their other accounts during a session.

## 4.2.d

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

## 4.2.c

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

## 4.2.b

FortiToken Cloud 4.2.b is the FortiToken Cloud GA release, which offers many of the major features of the product. For more information, see [Features and benefits](#).



# Technical support

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

## Prepare for technical support

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

- Your FTC account ID, the serial number and version number of your FortiProducts (e.g., FortiAuthenticator, FortiGate), including FortiClient version if using FortiClient.
- A detailed description of your problem, including relevant background information. If the issue is about login authentication failure, be sure to provide your FTC username, token serial number, and the version number of the FortiToken mobile app.
- Debug log(s), error messages, 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 us expedite your service request. How you get your Fortinet product serial number depends on your license, as discussed in the following paragraphs.

### Licensed customers

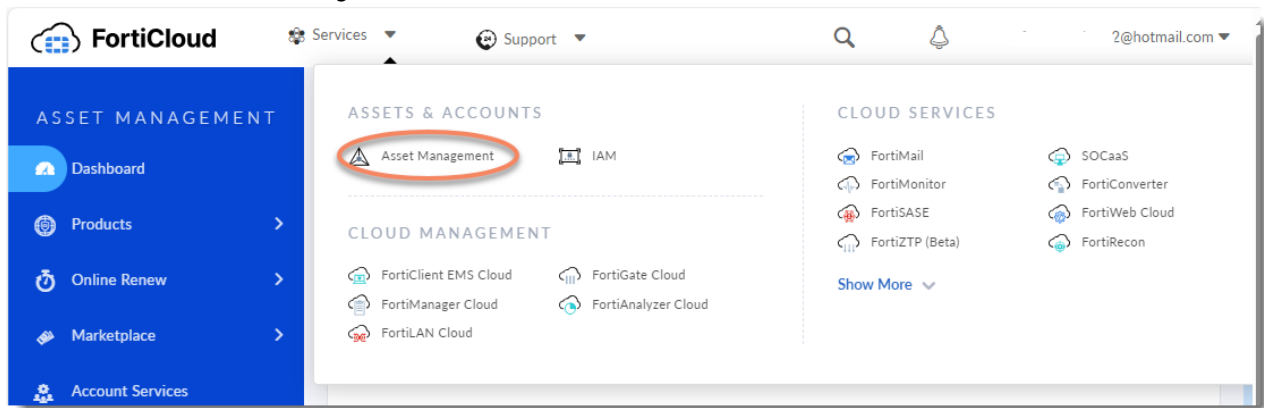
If you are using a time-based FTC license, follow the steps below to locate your Fortinet product serial number:

1. Log into the FortiToken Cloud portal.
2. On the left-side menu, select *Licenses* to open the Licenses page.
3. Take note of the serial number for the contract which you are having trouble with.

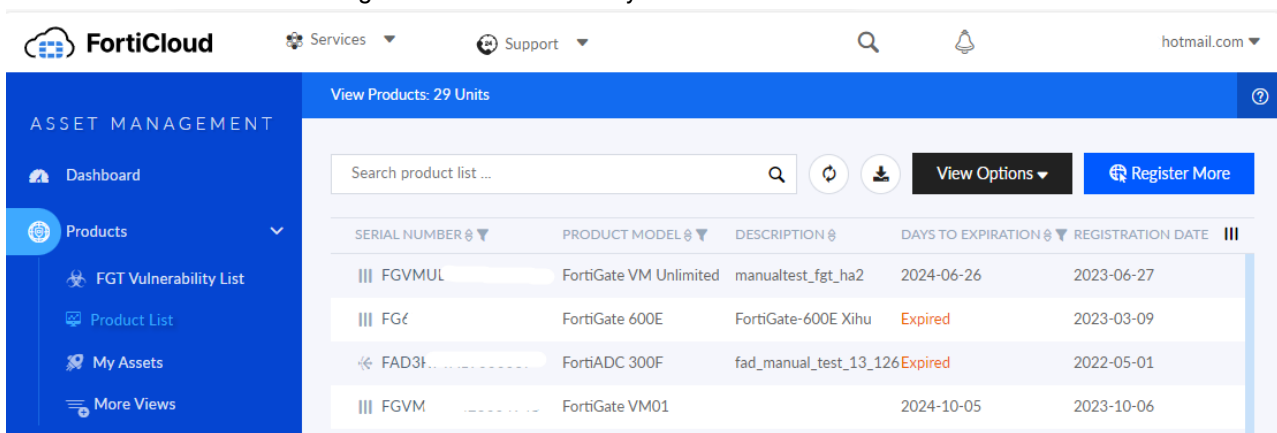
### Customers with FTM tokens migrated from FortiGate to FTC

If you have migrated your FTM tokens from FortiGate to FTC, take the following steps to get your serial number:

1. Got to *Services > Asset Management*.

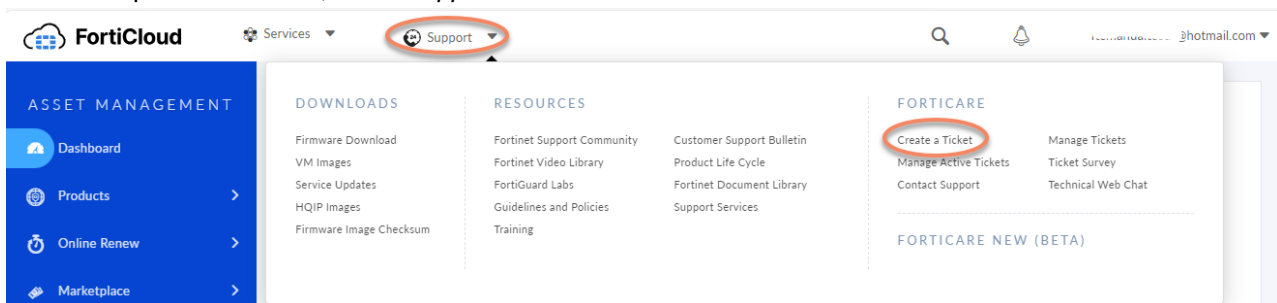


2. Click *Products > Product List* to get the serial number of your FortiGate.



## 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

Search our Knowledge Base

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
06/09/2025	FortiToken Cloud 25.2.a
01/16/2025	FortiToken Cloud 25.1.a
07/30/2024	FortiToken Cloud 24.3.a
05/03/2024	FortiToken Cloud 24.2.a
12/21/2023	FortiToken Cloud 23.4.b
11/16/2023	FortiToken Cloud 23.4.a
08/11/2023	FortiToken Cloud 23.3.b
07/28/2023	FortiToken Cloud 23.3.a
03/16/2023	FortiToken Cloud 23.1.a
11/28/2022	FortiToken Cloud 22.4.a
07/19/2022	FortiToken Cloud 22.3.a
06/30/2009	FortiToken Cloud 22.2.d
06/01/2022	FortiToken Cloud 22.2.c
05/09/2022	FortiToken Cloud 22.2.b
05/04/2022	FortiToken Cloud 22.2.a.
01/18/2022	FortiToken Cloud 21.4.d.
10/11/2021	FortiToken Cloud 21.4.a.
09/30/2021	FortiToken Cloud 21.3.d.
09/16/2021	FortiToken Cloud 21.3.c.
08/13/2021	FortiToken Cloud 21.3.b.
07/26/2021	FortiToken Cloud 21.3.a.
06/09/2021	FortiToken Cloud 21.2.d.
04/15/2021	FortiToken Cloud 21.2.c.
03/01/2021	FortiToken Cloud 21.1.a.
12/02/2020	FortiToken Cloud 20.4.d.
11/30/2020	FortiToken Cloud 20.4.c.
10/07/2020	FortiToken Cloud 20.4.a.

Release Date	Product Version
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](http://www.fortinet.com)

Copyright© 2025 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 Chief Legal Officer, 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.