



Release Notes

FortiToken Cloud 23.4.b



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



December 21, 2023

FortiToken Cloud 23.4.b Release Notes

TABLE OF CONTENTS

Introduction	4
What's New	5
Important notes	6
Transfer auth clients	6
Use of non-officially supported FOS	7
The same token for the same user on multiple auth clients	7
FOS 6.2.3 and 6.4.0 CLI differences	7
Admin accounts and realms	7
Supported hard tokens	8
No SMS MFA with FAC as LDAP server	8
A single FTC user in multiple auth clients	8
FAC users' name issues on FTC GUI	9
How to use FortiClient	9
Use auto push	9
Use OTP	12
Compatible Fortinet applications	13
Supported browsers	14
Resolved Issues	15
Known Issues	16
Change Log	17

Introduction

Thank you for choosing FortiToken Cloud (FTC)!


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

What's New

FortiToken Cloud 23.4.b has implemented the following feature enhancement:

- Comprehensive GUI revamping.



- For more information about the new features, see the [Admin Guide](#) or click  (**Help**) in the upper-right corner of the FTC GUI.
 - For information about technical product, see [Technical Support](#).
-

Important notes

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

- [Credit-based licenses no longer available for purchase](#)
- [Use of non-officially supported FOS on page 7](#)
- [The same token for the same user on multiple auth clients on page 7](#)
- [A single FTC user in multiple auth clients on page 8](#)
- [Admin accounts and realms on page 7](#)
- [Supported hard tokens on page 8](#)
- [No SMS MFA with FAC as LDAP server on page 8](#)
- [FAC users' name issues on FTC GUI on page 9](#)
- [How to use FortiClient on page 9](#)
- [Enabling/Disabling users on FortiGate](#)

Transfer auth clients

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

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

Use of non-officially supported FOS

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

DO NOT use FTC with FOS 6.2.1!

The same token for the same user on multiple auth clients

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

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



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

For more detailed information, see [One Token shared by different auth clients](#) and [A single FTC user in multiple auth clients on page 8](#).

FOS 6.2.3 and 6.4.0 CLI differences

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

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

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

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

Admin accounts and realms

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

Upon upgrading to 20.1.a or later, the FTC account of your organization that has logged in to the FTC portal first and/or your master account in FortiCloud will be automatically assigned the FTC global admin role; all accounts under your FortiCloud master account will be assigned the sub-admin role by default, with no realm assigned (including the default

Realm) to them, and therefore will not be able to see any FTC data. The global admin must create admin groups and map the sub-admins with realms in order for them to view and manage realm resources.

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

Supported hard tokens

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

No SMS MFA with FAC as LDAP server

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

A single FTC user in multiple auth clients

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

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

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

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

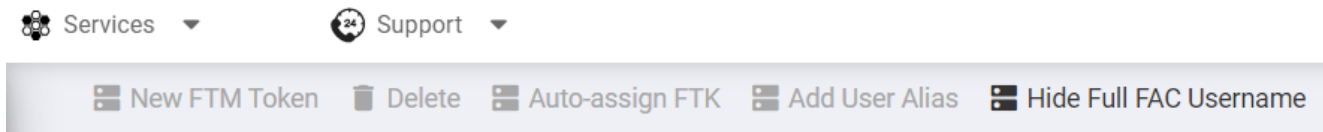
Now suppose, instead of enabling User-1 again in FGT-1, you assign SMS from FGT-1 (an FGT internal feature that is not available in FTC) as the MFA method for User-1. This is what is going to happen: If User-1 attempts to log into FGT-1, the user will get an SMS from FGT-1; but if User-1 attempts to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



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

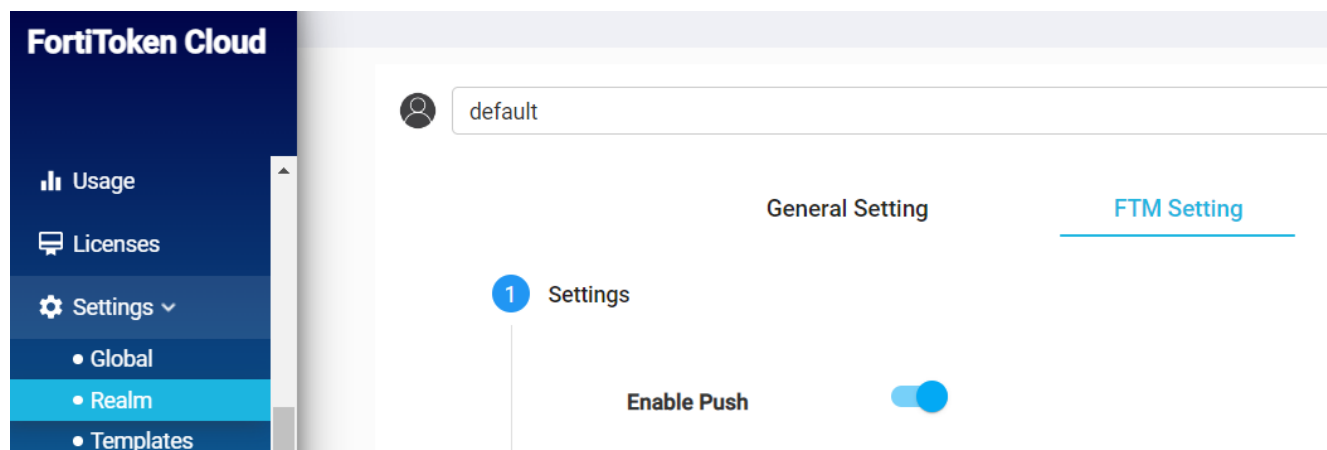
FAC users' name issues on FTC GUI

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



How to use FortiClient

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



Use auto push

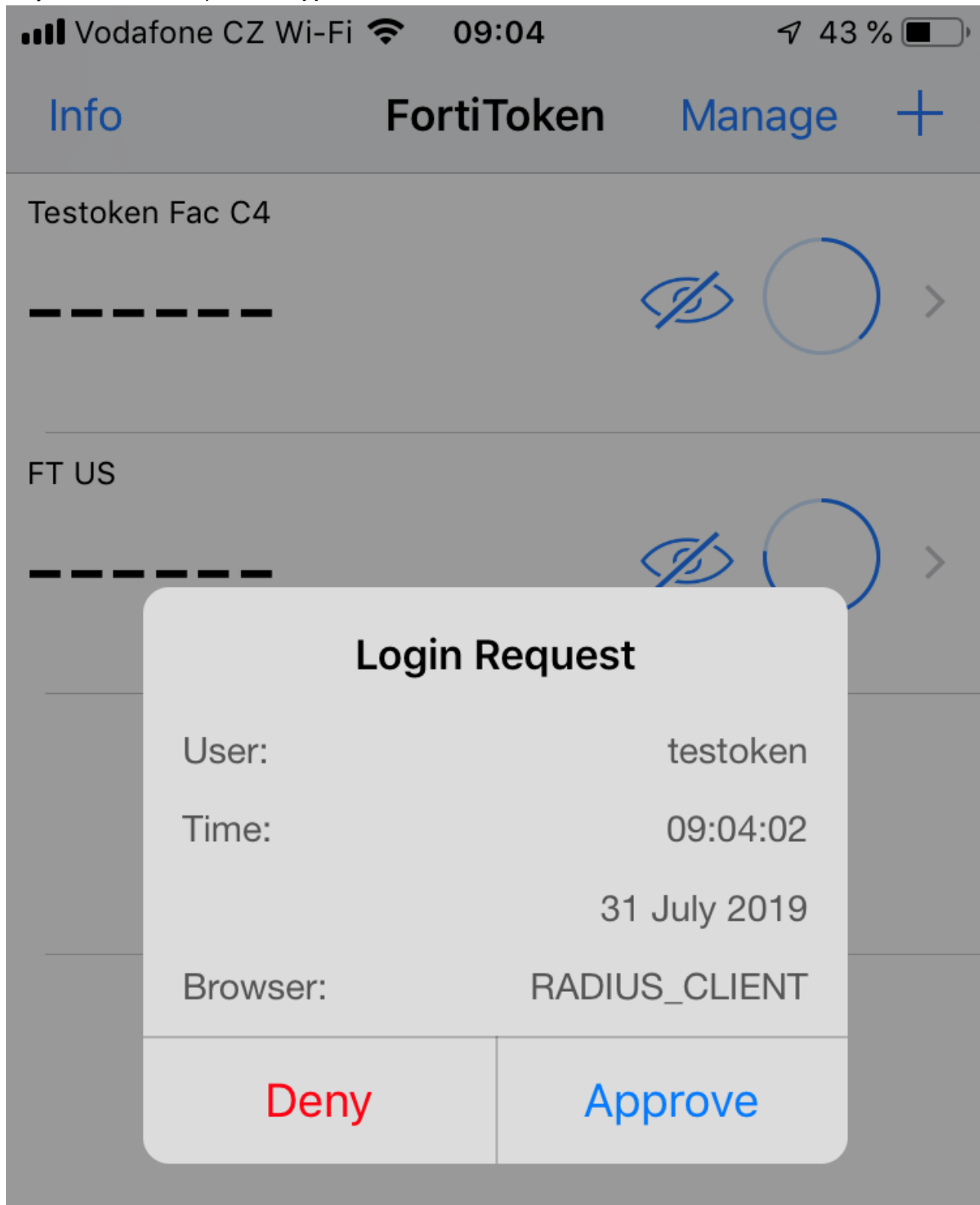
Upon entering your username and password, do the following:

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



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 the **Approve** button.



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

Use OTP

Upon entering your username and password, do the following:

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

The screenshot shows the FortiClient interface. On the left is a blue sidebar with a user profile icon labeled 'dussaufl', a 'REMOTE ACCESS' button, and links for 'Notifications', 'Settings', and 'About'. The main area displays a login window with a globe and laptop icon. It contains fields for 'VPN Name' (set to 'TFL'), 'Username', 'Password', and 'Token'. The 'Token' field is highlighted with a red border. Below the fields are 'OK' and 'Cancel' buttons. At the bottom, a 'FortiToken 8012' display shows the number '270827' in a large font, which is also highlighted with a red border. To the right of the display are an eye icon, a circular progress indicator, and a right arrow.

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

Compatible Fortinet applications

FortiToken Cloud 23.4.b works in tandem with the following Fortinet applications:

- FortiOS 6.2.3 or later, FortiOS 6.4.0 or later, FortiOS 7.0.0 or later, FortiOS 7.2.0 or later, and FortiOS 7.4.0 or later
- FortiClient for Windows 6.4.0 or later and FortiClient for Windows 7.0.0 or later
- FortiClient for MacOS 6.2.2 or later and FortiClient for MacOS 7.0.0 or later
- FortiClient for Linux 6.4.0 or later and FortiClient for Linux 7.0.0 or later
- FortiAuthenticator 6.2.0 or later, FortiAuthenticator 6.3.0 or later, FortiAuthenticator 6.4.0 or later, and FortiAuthenticator 6.5.0 or later
- FortiSandbox 3.2.0 or later
- FortiADC 7.1.3 or later, FortiADC 7.2.1 or later, and FortiADC 7.4.0 or later
- FortiManager 7.2.2 or later and FortiManager 7.4.0 or later
- FortiAnalyzer 7.2.2 or later and FortiAnalyzer 7.4.0 or later
- FortiPortal 7.0.0 or later
- FortiToken Mobile for iOS 5.4.2 or later
- FortiToken Mobile for Android 5.3.2 or later
- FortiToken Mobile for Windows 4.2.0



- FortiToken Cloud works best with FortiOS 6.2.3 or later. If you have to use FortiOS 6.2.0, we strongly recommend that you turn off the multi-realm mode and move your auth clients to the default realm.
 - FortiToken Cloud does not work well with FortiOS 7.0.2. We recommend upgrading to FortiOS 7.0.5 or later for best performance.
 - For end-users with FortiAuthenticator 6.3.0 or later as an auth client, FortiToken Cloud supports OTP via email or SMS.
-

Supported browsers

FortiToken Cloud 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.

Resolved Issues

The following are the major issues that have been resolved in FortiToken Cloud 23.4.b release.

Bug ID	Description
0722384	The user might not be able to drag the bubble knob to adjust the quota of a realm.
0712629	It may take longer for the Users page to be populated with all users as the number of end-users increases.
0907218	The GUI does not show the progress of migrations.
0983028	Realms cannot be sorted properly by user quota if there are NA's present.

Known Issues

The following are the major known issues that are found in FortiToken Cloud 23.4.b release.

Bug ID	Description
0970367	Cookie set in API put is not properly called.
0870957	The temporary token log is unable to record any expiration action.
0926225	In Chrome, pressing the Back button to go to FTC after the FC menus is opened could cause the GUI to freeze if you try to change the zoom ratio of the page.
0945180	FTC allows users to delete alarm receivers that are part of a group, or groups that are part of an event
0984563	The pop-up window shows "There are no records to display" while waiting for API's returns under Auth Clients.
0984540	Some support links do not work as expected.

Change Log

Date	Description
December 21, 2023	Initial release.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.