Service Description

FortiToken Cloud 23.3.b

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 23, 2023
FortiToken Cloud 23.3.b Service Description

TABLE OF CONTENTS

Introduction

FortiToken Cloud (FTC hereafter) is an Identity and Access Management as a Service (IDaaS) cloud service offered by Fortinet. It enables multi-factor authentication (MFA) on clients such as FortiGate™ (FGT), FortiAuthenticator™ (FAC), and FortiSandbox™ products as described in the then-current product data sheets and release notes (the “Supported Products” and the “Service”). For a full list of supported platforms, please refer to the Admin Guide. FTC provides centralized token authentication in the cloud, simplifying FortiToken management and the provisioning of users with no additional hardware or software required.

Many large-scale, costly, and most damaging data breaches in recent memory have been attributed to weak, insecure, and/or compromised user passwords. In response, businesses of all sizes are moving beyond the traditional password only authentication in favor of MFA. Adding a second factor to the authentication process, whether with traditional hardware, or more recently through mobile device applications, has become the new norm. Unfortunately, implementing and managing MFA deployments has proven to be no easy task. It requires dedicated IT personnel with the technical know-how, and the process is complex, on-going, and time-consuming.

Seamlessly integrated with Fortinet's industry-leading, award-winning, hardened, and trusted network security management products and technologies, FTC offers a secure, effective way to manage MFA for your Fortinet appliances through an intuitive, easy-to-use web interface that can be accessed from anywhere over the Internet. The FTC service includes a FortiToken Mobile App with PUSH technology to provide smooth multi-factor end-user experience.

FTC is hosted on the FortiCloud™ service portal whose features, deliverables and terms of use are described in the then-current FortiCloud service description made available at https://support.fortinet.com/Information/DocumentList.aspx (the “FortiCloud Service Description”). The terms of the FortiCloud Service Description are incorporated herein by reference and, in the event of a conflict, this service description shall prevail over the FortiCloud Service Description.

Service features and deliverables

FortiToken Cloud is managed 24 hours a day and 7 days a week. The service is monitored for device availability and management and authentication activities in customer accounts. The service is available in various regional Fortinet data centers, that may share data and which are compliant with pertinent security industry standards.

FortiToken Cloud offers its customers the following features and benefits:

- A cloud-based multi-factor authentication (MFA) solution for all your supported Fortinet appliances, with a target portal availability of 99.99%.
- A flexible time-based licensing model that allows any combination of any users and days of use.
- Automatically locking out end-users when they have breached their specified MFA failure threshold to ensure security and integrity of customer accounts.
- Enabling FTC admin users to allow end-uses to bypass MFA and request new tokens on behalf of their end-users easily from the GUI.
- Secure transfer of FTC and third-party tokens between iOS and Android devices using the FortiToken Mobile (FTM) app.
- Synchronizing end-users from supported end clients like FortiGate or FortiAuthenticator to FTC. The user base of record is always the Auth Client (e.g., FGT or FAC), and trumps the user base that exists in FTC (if different) prior to running the sync command.
- Automatically logging out when the GUI has been idle for more than 10 minutes to safeguard the security and integrity of customer account information
- Easy access to data about the authentication clients, end-users, and usage, as well as management and authentication events in their account.
- Comprehensive authentication and management logs to enable customers to keep track of all authentication and management events that have happened in their account.
- Support for FortiGate and FortiAuthenticator HA cluster configuration. Customers can view their FGT and/or FAC devices in any cluster from the FTC GUI.
- Support for customer logo to replace the default Fortinet banner at the bottom of the FTM app on end-users' mobile devices.
- Option for sending token activation/transfer codes to end-user mobile devices by SMS.
- Super-admin users are able to access all FTC accounts of their organization — they can choose any of their accounts to display upon logging in and switch to any of their accounts during a session.
- Retention of customer usage data and logs (authentication and management) for up to one (1) year.

Customer required contribution and responsibilities

In addition to the customer required contributions and responsibilities included in the FortiCloud Service

Description, the customer agrees for the duration of the Service the following:

- Register their FortiToken Cloud licenses to the same FortiCloud account where their clients are registered on the Fortinet Customer Service and Support website.
- Configure their devices correctly to enable their end-users to use FortiToken Cloud for MFA service.
- Provide network connectivity to enable devices to communicate with the FortiToken Cloud service portal.
- Be able to access the Fortinet Customer Service and Support website and the Fortinet corporate website using a supported web browser.
- Replenish their account quota balance by purchasing new licenses with adequate quotas when their current quota balance is running low or negative.
- Ensure the products and versions to be covered by the service correspond to Supported Products and are supported by the Service.
- Renew their existing service subscription before their current license expires to ensure their uninterrupted use of FTC.
- Ensure the client’s firmware is compatible with FTC supported firmware.
- Manage the device configuration to make sure any transmitted data meets customer data privacy requirements.
- Ensure that their local platform is properly configured and has adequate bandwidth to communicate with the FTC service.
- Complete the service renewal before the expiration of the Service term. Thirty (30) days prior to the Service expiration, the customer will receive a renewal notification from the cloud portal on a weekly basis. The service expiration date and daily notifications for service renewal will be displayed within the FortiToken Cloud instance.
- Upon service expiration, insufficient user quota or termination, the FortiToken Cloud instance will be disabled and an email notification will be sent to the customer. A retention period of thirty (30) days after service expiration or termination within which to renew the service, after which the FortiToken Cloud instance will be deleted and an email notification sent to the customer.
- For clarity, the customer is explicitly advised that the data will be no longer recoverable upon the deletion of the FortiToken Cloud instance.

Scope and conditions

In addition to the scope and conditions included in the FortiCloud Service Description, the following terms apply:

- The customer acknowledges and agrees that Fortinet may access the customer's FortiToken Cloud instance for the purpose of troubleshooting and applying fixes in relation to issues in relation to support tickets submitted or otherwise reported by the customer or identified through established monitoring and/or system notifications and will be entitled to perform maintenance and fixes on the customer's FTC instance without customer's consent or prior notice.
- In the event that continued provision of the service to the customer would compromise the integrity or security of the service, the customer agrees that Fortinet may temporarily limit or suspend the service to the customer.
- The customer agrees to use the service for legitimate and lawful business purposes only. Should Fortinet discover illegal activity, or activity likely to undermine the integrity of the service, regardless of intent, the service may be terminated without notice and relevant authorities notified where appropriate.
- After the retention period, all logs are deleted permanently.
- Any loss of connectivity by the customer that is not as a result of failure of the Fortinet-managed infrastructure is the responsibility of the customer with the service continuing to be considered as being utilized. Availability targets only apply to the FTC infrastructure.
- Where maintenance of the FTC infrastructure is required, the FTC team will aim to perform such maintenance without any service disruption. With any planned maintenance activity that may cause service disruption, Fortinet will provide the customer with a 48-hour advanced notice. Planned maintenance will not be performed between the hours of 8:00 AM and 6:00 PM in the time zone where the infrastructure is located. Notification will be made through the most appropriate method, such as email or portal messages, dependent on users impacted.
- On the rare occasion that the integrity of the FTC service is at risk, Fortinet may be required to take emergency maintenance actions. In this instance, Fortinet will target to inform all affected parties within one hour of the start of the maintenance activity.
- The service will be delivered in accordance with the Fortinet Privacy Policy. The customer is responsible for ensuring that their use of the service is in accordance with relevant laws or regulations. The service is subject to the terms of the then-current Fortinet’s Service Terms & Conditions located at https://www.fortinet.com/content/dam/fortinet/assets/legal/Fortinet-Service-Offering-Terms.pdf.
- The service is available in English only.

Availability and purchasing

The service is available for purchase by an end-customer (the “Customer”) through authorized Fortinet resellers and distributors globally (“Channel Partners”). Channel Partners are independent third parties that conduct business in their own name and account and, consequently, cannot bind Fortinet in any way. The service is delivered to the Customer as referenced in the purchase order placed with Fortinet by a Customer or a Channel Partner. This service is separate from any purchase of other Fortinet’s products or other services.

The date of the service registration determines the start date of the service which will run for the period determined by the Service SKU purchased by the Customer notwithstanding if the service entitlements are not fully consumed. The registration and delivery of the service covered by this service description must commence in accordance with service activation policies made available at https://www.fortinet.com/corporate/about-us/legal, failure of which, will result in, as the case may be, the service being partially or completely forfeited, without any right to obtain a refund. In no circumstances will the duration of the service be extended. All sales are final.

FortiToken Cloud has five annual subscription licensing options which include one year of FortiCare Premium support service. The following table highlights the user and SMS message quotas that each of the annual licenses offers.

SKU	User Quota	SMS Credit Quota
FC1-10-TKCLD-445-01-12	25	3,125
FC2-10-TKCLD-445-01-12	100	12,500
FC3-10-TKCLD-445-01-12	500	62,500
FC4-10-TKCLD-445-01-12	2,000	250,000
FC5-10-TKCLD-445-01-12	10,000	1,250,000

SMS service licenses

In addition to the annual licenses, FTC offers separate SMS licenses with SMS credits to enable customers to take full advantage of its SMS service.

The number of credits that FTC charges varies, depending on the country or region of the world where the end-users' phone numbers are registered. The following table highlights the number of SMS credits each SMS license SKU offers.

SKU	Number of SMS credits
FTC-SMS-2500	2,500
FTC-SMS-10K	10,000
FTC-SMS-25K	25,000

FortiToken Cloud is available for purchase through Fortinet-authorized resellers worldwide. You must contact an authorized reseller in your region to place your order. To find an authorized reseller in your region, click Resellers or go to https://www.fortinet.com/partners/partner-program/find-a-partner.html.

All SMS licenses must be activated within one year of purchase. Unused SMS credits expire three years after the date of activation.

FORTINET®

www.fortinet.com