Administration Guide

FortiAuthenticator Cloud 26.1.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

January 9, 2026
FortiAuthenticator Cloud 26.1.a Administration Guide
65-261a-1238376-20260109

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-01-06	Initial release.
2026-02-09	Updated Limitations of FortiAuthenticator Cloud on page 23.

Introduction

FortiAuthenticator Cloud is an Identity and Access Management as a Service (IDaaS) cloud service offered by Fortinet.

FortiAuthenticator Cloud is a service hosted by Fortinet with FortiAuthenticator-VM, with token features offered by FortiIdentity Cloud.

For limitations of FortiAuthenticator Cloud vs standalone/BYOD FortiAuthenticator please refer to Limitations of FortiAuthenticator Cloud on page 23.

FortiAuthenticator Cloud delivers the following features:

- *Authentication*: FortiAuthenticator Cloud includes passwordless Fast IDentity Online (FIDO), OAuth2 Authorization, OpenID Connect (OIDC), and Security Assertion Markup Language (SAML) authentication methods.
- *User Identification*: FortiAuthenticator Cloud can identify users through multiple data sources, including Active Directory (AD), desktop client, guest portal logon, RADIUS accounting, Kerberos, and a Representational State Transfer (REST) API.

  It can then communicate this information to FortiGate or FortiMail units for use in identity based policies.
- *Certificate Management*: FortiAuthenticator Cloud can create and sign digital certificates for use.
- *Integration*: FortiAuthenticator Cloud can integrate with 3rd RADIUS, LDAP, and SAML authentication systems, allowing you to reuse existing information sources.

  The REST API can also be used to integrate with external provisioning systems.

FortiAuthenticator Cloud delivers the following features using FortiIdentity Cloud:

- *Adaptive Authentication*: FortiAuthenticator Cloud provides adaptive authentication where more information regarding a login attempt, including time of the day, geo-location, and so- on, is used to evaluate the risk of a login attempt.

  FortiAuthenticator Cloud allows end-users to bypass OTP verification of MFA under certain “safer” conditions and denies such attempts under certain otherwise “riskier” conditions.
- *Multi-Factor Authentication*: FortiAuthenticator Cloud can act as a multi-factor authentication client using FortiIdentity Cloud.

More information

End-customers use FortiAuthenticator Cloud the same way as the standalone FortiAuthenticator. As a result, end-customers can use the *FortiAuthenticator Admin Guide* and *FortiAuthenticator REST API Solution Guide* for information about using either the standalone FortiAuthenticator or FortiAuthenticator Cloud.

For more information, see the *FortiAuthenticator Admin Guide* and *FortiAuthenticator REST API Solution Guide* on the Fortinet Docs Library.

Compatible Fortinet applications

See the *FortiAuthenticator Cloud Release Notes* on the Fortinet Docs Library.

FortiAuthenticator Cloud supports FortiAuthenticator Agents for Microsoft Windows and OWA. However, offline tokens are not supported for FortiAuthenticator Agent for Microsoft Windows. Offline tokens support will be added in a future version.

FortiAuthenticator agents cannot be downloaded from FortiAuthenticator Cloud. See Downloading FortiAuthenticator agents on page 6.

Downloading FortiAuthenticator agents

To download FortiAuthenticator agents:

1. Log in to FortiCloud.
2. In the *Support* dropdown, select *Firmware Download*.
3. In the *Select Product* dropdown, select *FortiAuthenticator_and_FortiTrustID_Agents*.
4. Select *Download*.
5. In *FortiAuthenticator_and_FortiTrustID_Agents* folder, download the `FAC_Agent_Setup_vX.X.exe` file for FortiAuthenticator Agents for Microsoft Windows, and save the file to your computer.
   Download the `FAC_IIS_Agent_Setup_vX.X.exe` file for FortiAuthenticator Agent for Microsoft OWA, and save the file to your computer.
6. Open the file to install.
   For information on installing the agents, see the *FortiAuthenticator Agent for Microsoft Windows Install Guide* and the *FortiAuthenticator Agent for Microsoft OWA Install Guide* on the Fortinet Docs Library.

Product documentation and support

Following lists the FortiAuthenticator Cloud related documentation and support information:

- For information about the current release, see the *FortiAuthenticator Cloud Release Notes* on the Fortinet Docs Library.
- For detailed information about product features, click the help icon (▨) in the GUI.
- For frequently asked questions, see the *FAQs* on the Fortinet Docs Library.
- For terms of service, see the *Service Description* on FortiCloud.
- For licensing, see Licensing on page 8.
- For product support issues, select an option in *Support > FortiCare*.

Licensing

FortiAuthenticator Cloud is a subscription-based Identity and Access Management as a Service (IDaaS) cloud service. To use the service, you must subscribe by purchasing a license (i.e., SKU) based on the number of FortiAuthenticator Cloud end-users in your account for the year. See SKUs on page 8.

A FortiAuthenticator Cloud 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.

FortiAuthenticator Cloud does not include a free trial.

Also, see License expiry on page 9.

FortiAuthenticator Cloud decoupled from FortiIdentity Cloud

Starting FortiIdentity Cloud 4.1.0, FortiIdentity Cloud is decoupled from FortiAuthenticator Cloud.

New FortiAuthenticator Cloud licenses purchased after FortiIdentity Cloud is upgraded to version 4.1.0 will not include quotas in FortiIdentity Cloud.

You must purchase separate license for FortiIdentity Cloud if you want to use FortiIdentity Cloud.

All FortiAuthenticator Cloud licenses purchased prior to FortiIdentity Cloud version 4.1 will continue to function as expected until they expire.

How to purchase a FortiAuthenticator Cloud license

Contact your reseller to purchase FortiAuthenticator Cloud license. Upon purchasing services from your reseller, you will receive the registration code by email.

To register FortiAuthenticator Cloud subscription, see Registering FortiAuthenticator Cloud subscription on page 10.

SKUs

The following table lists licensing options by SKU.

SKU	Number of FortiAuthenticator Cloud end-users
FC2-10-ACCLD-511-02-DD	Cloud-managed identity user subscription including FortiCare premium support for 100 - 499 users.
FC3-10-ACCLD-511-02-DD	Cloud-managed identity user subscription including FortiCare premium support for 500 - 1,999 users.
FC4-10-ACCLD-511-02-DD	Cloud-managed identity user subscription including FortiCare premium support for 2,000 - 9,999 users.
FC5-10-ACCLD-511-02-DD	Cloud-managed identity user subscription including FortiCare premium support for 10,000+ users.

Use a co-termed license to add FortiAuthenticator Cloud users to an existing FortiAuthenticator Cloud license.

For more information, see *Stackable co-termed licenses* in the FortiIdentity Cloud Admin Guide.

License expiry

When FortiAuthenticator Cloud license expires, the customer has a 30 day grace period.

30 days after the grace period ends and if no license has been added, FortiAuthenticator Cloud instance is turned off.

To stop the grace period clock or in order to restart the instance, when a new license is added, the license must cover the existing user base.

If the FortiAuthenticator Cloud user limit in the license is less than the actual number of users in FortiAuthenticator Cloud (e.g., the user limit is zero after the license expires), you cannot add users anymore. The existing users will continue to be authenticated by FortiAuthenticator Cloud.

FortiAuthenticator Cloud sends an email notification to the customer administrator when a license is expiring. The notification specifies the license expiry date, SN, and information about the grace period and when the instance is powered down if no valid license is applied. The email is sent 7, 3, and 0 days before the license expires.

The notification is also displayed as a dismissable alert on the FortiAuthenticator Cloud login page with the option not to show the notification again starting 30 days before the license expiration date.

30 days after the FortiAuthenticator Cloud instance has been turned off, the instance is deleted.

Getting started

To get started with FortiAuthenticator Cloud:

1. Registering FortiAuthenticator Cloud subscription on page 10
2. Logging in to FortiAuthenticator Cloud portal on page 10

Registering FortiAuthenticator Cloud subscription

Upon purchasing the FortiAuthenticator Cloud service subscription, you receive a license certificate file (.pdf) with a registration code in your email.

To register a FortiAuthenticator Cloud subscription on FortiCloud, see Registering assets in the latest Asset Management Administration Guide.

Logging in to FortiAuthenticator Cloud portal

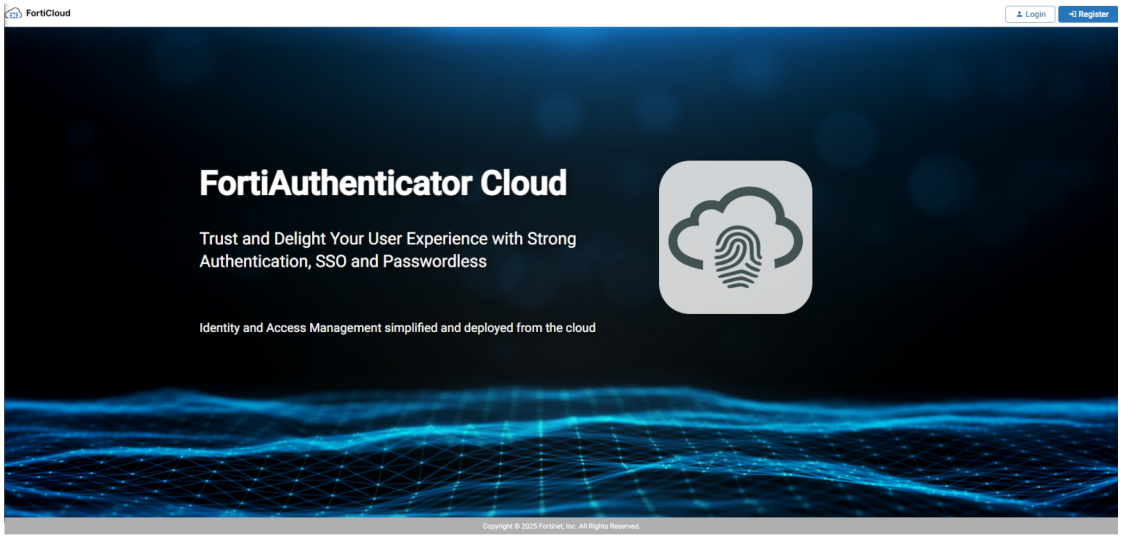
All FortiCloud registered users can access the FortiAuthenticator Cloud portal. If your organization has multiple FortiAuthenticator Cloud accounts, you see a list of FortiAuthenticator Cloud accounts after you sign in on FortiCloud. You can then select an account to open it on the FortiAuthenticator Cloud portal.

Access to FortiAuthenticator Cloud is managed by FortiCloud SSO authentication via FortiAuthenticator. Upon receiving your login request, the system redirects you to FortiCloud which is the FortiCloud SSO page. From there, you must use your FortiCloud account username and password to log in.

After authenticating your identity using multi-factor authentication (MFA), the system grants you access to the FortiAuthenticator Cloud portal.

To log in to the FortiAuthenticator Cloud portal:

1. On the browser, go to https://fortitrustid.forticloud.com/.
   The FortiAuthenticator Cloud portal opens.



2. In the upper-right corner, click *Login*.
   The FortiCloud Login page opens.
3. Enter your FortiAuthenticator Cloud licensed FortiCloud account email and password, and click *LOG IN*.
   Alternatively, for IAM users, select *IAM Login*, enter the *ACCOUNT ID (or ALIAS)*, *USERNAME* and *PASSWORD*, and click *LOG IN*.
   Once you have logged in, the FortiAuthenticator Cloud landing page opens with your FortiAuthenticator Cloud account or a list of accounts if your organization has multiple FortiAuthenticator Cloud accounts.

   When you log in to FortiAuthenticator Cloud portal for the first time, FortiAuthenticator Cloud instance can take up to 5 minutes to be provisioned.

4. Click your account or one of your accounts to open it.
   For IAM users, once logged in, a new *Make a Selection to Proceed* page appears where you can click *Select* next to an account from the hierarchy to use.
   FortiAuthenticator Cloud dashboard opens by default. See Dashboard on page 13.

To switch accounts during a session:

1. Go to the *Account* dropdown in the upper-right, and then select *Switch Accounts*.
2. In the table that opens, select an account.

Adding IAM users

FortiAuthenticator Cloud Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiAuthenticator Cloud Cloud.

To add an IAM user:

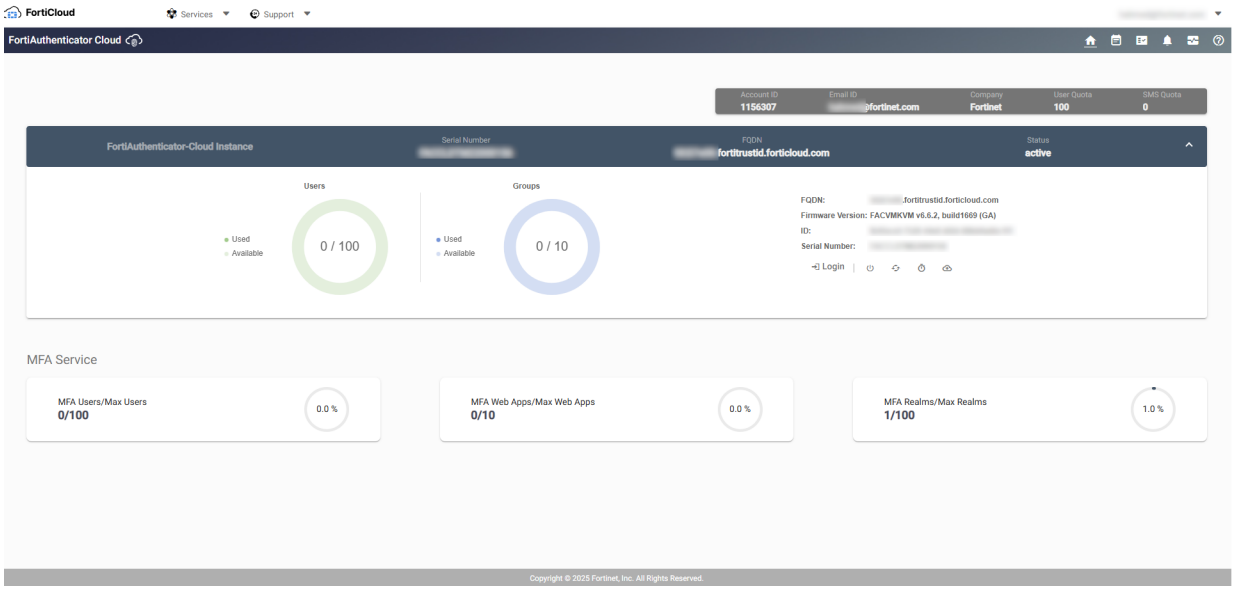
1. Go to FortiCloud (https://support.fortinet.com/), and log in.
2. From the *Services* menu, select *IAM* .
   The *IAM portal* is displayed.
3. Create a new IAM user.
   For more information, see Adding IAM Users.
4. Create a Permission Profile that includes FortiAuthenticator Cloud.
   For more information, see Permission profiles. When creating a permission profile that includes FortiTrust ID, you can define the access level for the following resource-based permissions:

Permission	Description
Upgrade	Upgrade the firmware version of the FortiAuthenticator Cloud instance.
Resize	Resize the resources available (CPU and memory) for FortiAuthenticator Cloud.
Reboot	Reboot FortiAuthenticator Cloud.
Restore	Restore FortiAuthenticator Cloud to a previous backup state.
FAC Login	Access to enter the FortiAuthenticator Cloud instance.

5. Add an IAM user group, and add the user to it.
   For more information, see Adding IAM User Groups.
6. Generate an IAM user login password.
   For more information, see Generating the password reset link.
7. The IAM user can use the credentials to log in to FortiCloud.
   After logging in to FortiCloud, the IAM user has access to *FortiAuthenticator Cloud Cloud & Service* portal.

Dashboard

The FortiAuthenticator Cloud dashboard looks like the following:



The *Dashboard* displays the following widgets and information:

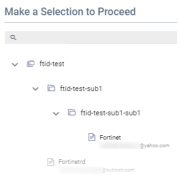
Information/widget	Description
Account ID	The account ID.
Email ID	The email associated with the account.
Company	The organization name.
User Quota	Maximum number of users.
SMS Quota	Maximum number of SMS.
FortiAuthenticator-Cloud Instance	
Serial Number	The serial number of FortiAuthenticator Cloud. The serial number is unique to FortiAuthenticator Cloud and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
FQDN	The FQDN domain name.
Status	The status of the FortiAuthenticator Cloud instance.
License expiry	Click the icon to see when the license expires.
Users	The current user count.

Information/widget	Description
Groups	The current group count.
Firmware Version	The version and build number of the firmware installed. To update the firmware, select the *Upgrade Firmware* ( ) icon. See Upgrade firmware on page 20.
ID	The ID of the FortiAuthenticator Cloud instance.
MFA Service	
MFA Users/Max Users	Users ready, in percentage.
MFA Web Apps/Max Web Apps	Web applications ready, in percentage.
MFA Realms/Max Realms	Realms ready, in percentage.

Users and *Groups* widgets refresh when the user logs in. Once logged in, the widgets refresh on-demand.

If there are notifications, the *Attention* dialog pops up when you log in to the FortiAuthenticator Cloud portal.

You can use the dropdown on the top-right to select a different OU IAM user.



Some options in the *Dashboard* may be grayed out as you may not have the necessary permissions.

To set up permission profiles on FortiCloud, see Permission profiles.

See Tab options on page 14.

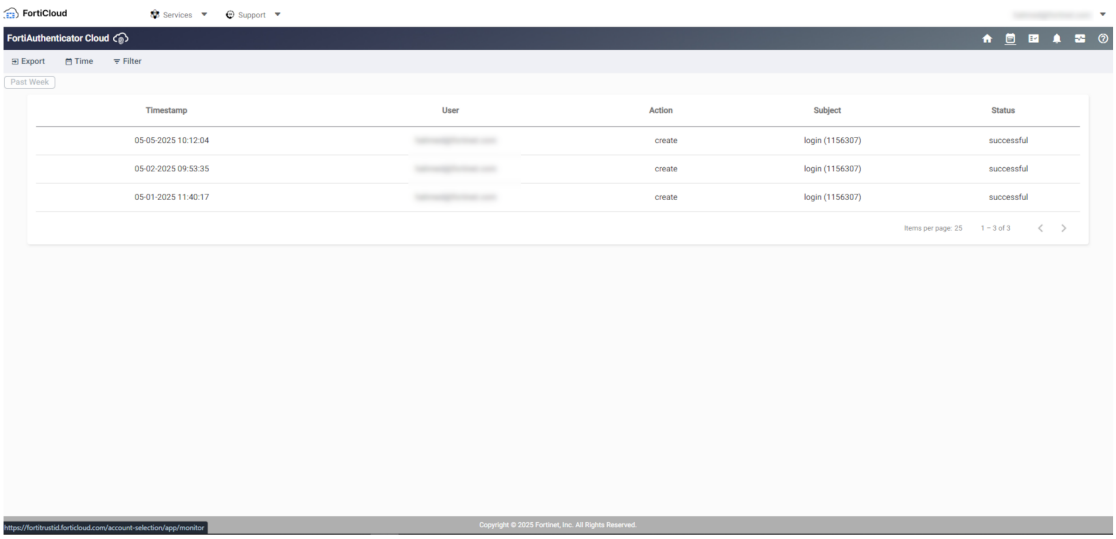
Tab options

The following options are available in the *Dashboard* tab:

Options	Description
Services	Access other FortiCloud services. See Services.
Support	Support options including *Downloads* and *FortiCare*. See Support.
OU IAM user	From the dropdown, select a different OU IAM user.
User	From the dropdown, select user related options. See User Settings.
Home	Click icon to open the *Dashboard* tab.
Log	Click icon to open the *Log* tab. See Log on page 15.
License	Click icon to open the *License* tab. See License on page 16.
Notification	Click icon to open notifications. See Notification on page 17.
Status	Click icon to open the FortiAuthenticator Cloud service status page. See Service status on page 18.
Help	Click icon to go to the *FortiAuthenticator Cloud Admin Guide* on the Fortinet Docs Library.
Login	Click icon to enter the FortiAuthenticator Cloud instance. See FortiAuthenticator Cloud on page 19.
Reboot instance	Click icon to reboot the instance. See Reboot an instance on page 20.
Refresh information	Click icon to refresh the information and widgets on the *Dashboard*. **Note:** Once clicked, *Refresh Information* grays out for 10 seconds before you can click again.
Restore config	Click icon to restore the backup configuration.
Backup config	Click icon to backup the current configuration. See Backup and restore on page 21.
Upgrade firmware	Click icon to upgrade the instance. See Upgrade firmware on page 20.
Resize	Click icon to enlarge the size of the resource used (CPU and memory). **Note**: The option only appears when you have an additional user quota.

Log

Logging menu provides a record of the events that have taken place on FortiAuthenticator Cloud.



The following actions are available in the *Log* tab:

- *Export*: click to export the logs as a CSV file.
- *Time*: filter the logs by *Past Day*, *Past Week*, *Past Month*, or select the *Calendar* icon, select a date and time, and then click *Set*.
- *Filter*: filter the logs by options in *Action*, *Resource*, *Status*, or *User* dropdowns, and then click *Apply Filters*.

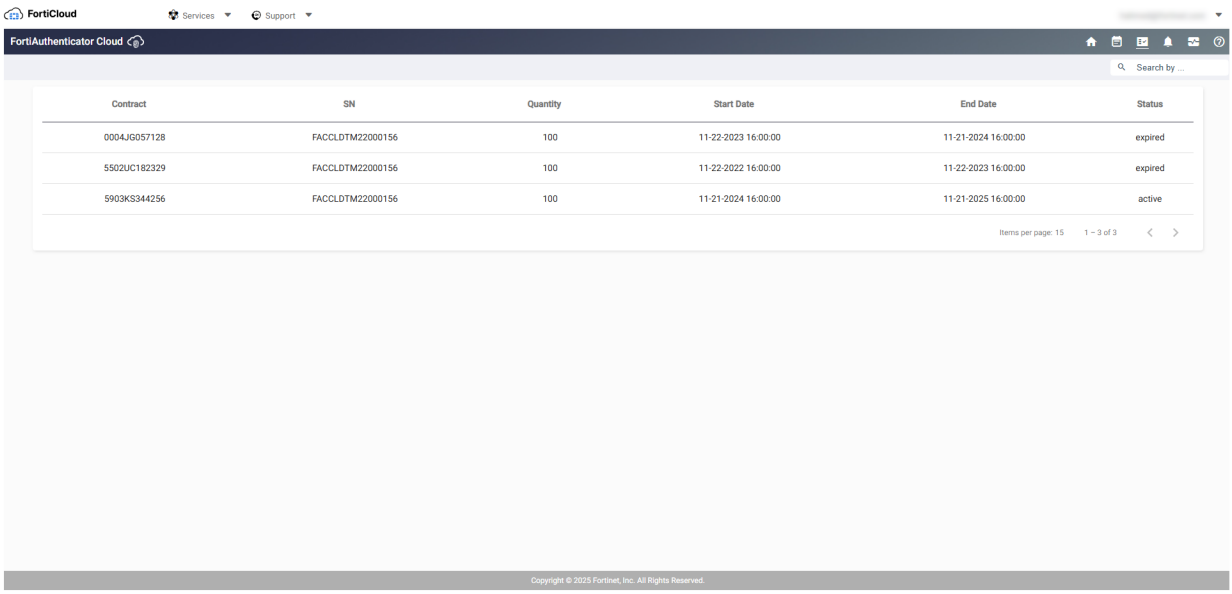
Use *Clear* to remove all filters.

Click a log entry to see the log request ID and information.

You can use < and > buttons on the bottom-right for page navigation.

License

To check the license status, click *License* ().



Use the search bar to look for a license related information.

You can use < and > buttons on the bottom-right for page navigation.

The *License* tab contains the following information:

Field	Description
Contract	The contract number.
SN	The serial number of FortiAuthenticator Cloud. See Dashboard on page 13.
Quantity	The maximum number of users.
Start Date	Start date of the license.
End Date	End date of the license.
Status	The status of the instance.

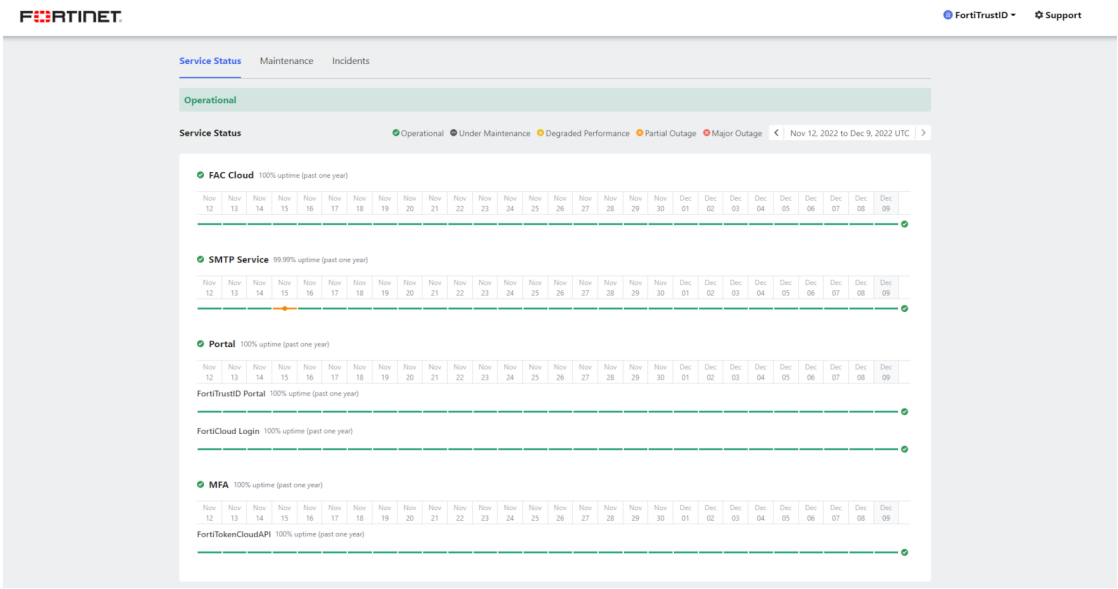
Notification

To check notifications, click *Notification ( )*.

License expiry related notifications appear here.

Service status

To check the FortiAuthenticator Cloud service status, click *Service Status* ( ).



Alternatively, the FortiAuthenticator Cloud service status is available when you go to: https://status.fortistatus.com/guest-portal/fortitrustid/incident/overview.

The page displays status of the following services over the past one year:

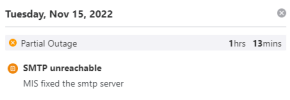
- *FAC Cloud*
- *SMTP Service*
- *Portal* (*FortiAuthenticator Cloud Portal* and *FortiCloud Login*)
- *MFA*

Use < and > to change the date range.

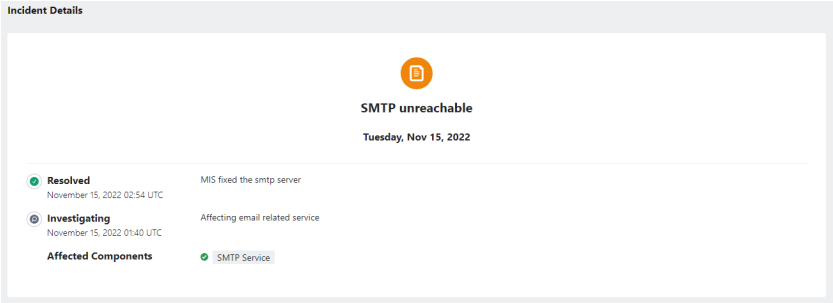
Go to *Maintenance* and *Incidents* to see a list of maintenance events and incidents.

To see more information about a incident:

1. Hover over a date to see more information about the service status.



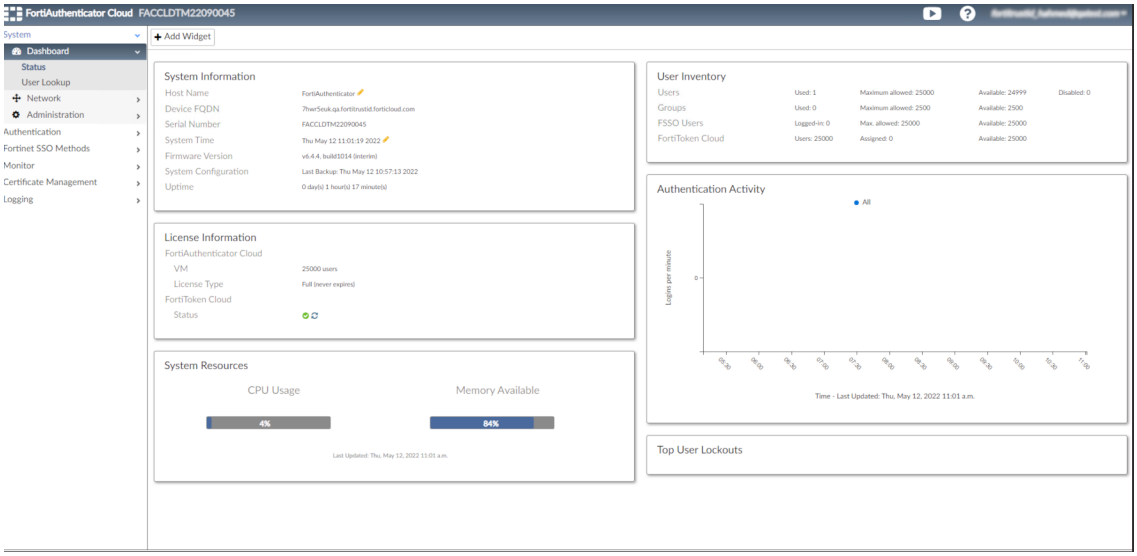
2. Click on the status message to see more information in a new tab.



FortiAuthenticator Cloud

Once you click *Login ( )*, you enter a FortiAuthenticator Cloud instance.

FortiAuthenticator Cloud looks like the following:



Admin profiles

The FortiCloud account owner has full permission for FortiAuthenticator Cloud.

By default, members of an account other than the account owner are assigned the *No-access Administrator* profile in FortiAuthenticator Cloud, i.e., they have no-read/no-write permission to everything in FortiAuthenticator Cloud.

As the name implies, no-access administrators in FortiAuthenticator Cloud initially have no access to any GUI menu item, and no GUI menu items are displayed when a no-access administrator attempts to access FortiAuthenticator Cloud.

The FortiCloud account owner will have full admin permissions in FortiAuthenticator Cloud and must explicitly give access to individual no-access administrators. Full FortiAuthenticator Cloud administrators can promote a no-access administrator and define their level of access by assigning them an admin profile in *Authentication > User Management > Local Users*.

Zero trust tunnels

See Zero trust tunnels in the *FortiAuthenticator Admin Guide*.

`154.52.4.227` and `69.167.109.243` are WAN IP addresses to build zero trust tunnels into an on-prem environment.

On-prem firewall allows the source to build a ZTNA tunnel.

Returning to FortiAuthenticator Cloud

To return to the FortiAuthenticator Cloud portal, select the FortiCloud account from the upper-right and then click *Return to FortiTrust ID portal*.

For more information on FortiAuthenticator Cloud, see More information on page 5.

Reboot an instance

To perform a restart of the FortiAuthenticator Cloud instance, click *Reboot instance (* *)*.

The following reboot settings are available:

- *Hard (* *)*: select, then click *OK* to forcefully reboot the FortiAuthenticator Cloud instance, i.e. the FortiAuthenticator Cloud instance is shut down immediately, then reboot.
- *Soft (* *)*: select, then click *OK* to gracefully reboot the FortiAuthenticator Cloud instance, i.e. the FortiAuthenticator Cloud instance is shut down normally, then reboot.

Upgrade firmware

Before proceeding to upgrade your system, Fortinet recommends you back up your configuration. See Backup and restore on page 21.

When a new firmware is available, *Upgrade Firmware (* *)* is displayed.

A warning is displayed if a new version is available for upgrade.

To upgrade the firmware now:

1. Click *Upgrade Firmware (* *)*, and then select *Now*.
2. Click *OK* to confirm.

To schedule a firmware upgrade:

1. Click *Upgrade Firmware (* *)*.
2. Click *Pick a time* or the calendar icon, then select a date and time.
3. Click *Set*.

4. Click *Schedule*.
5. In the confirmation dialog that appears, click *OK*.

Once the FortiAuthenticator Cloud instance is successfully upgraded, *Upgrade Firmware ( )* is hidden.

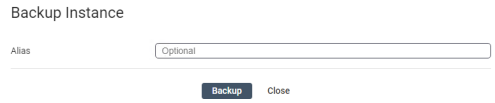
Upgrading a FortiAuthenticator Cloud instance may take up to 5 minutes.

Backup and restore

Fortinet recommends that you back up your FortiAuthenticator Cloud configuration on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal effect to the network. You should also perform a back up after making any changes to FortiAuthenticator Cloud.

To create a backup configuration:

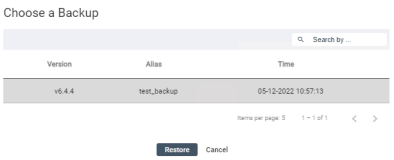
1. Click *Backup config ( )* to back up the configuration.



2. Optionally, enter an alias for the backup configuration, and select *Backup*.

To restore a backup:

1. Click *Restore config ( )* .
   The *Choose a Backup* window opens.



Use the search bar to look for a backup file.

You can use < and > buttons on the bottom-right for page navigation.

2. Select a backup, and click *Restore*.

FortiAuthenticator Cloud configurations are backed up every 24 hours.

When the permission profile is set to *Read Only* for restoring a backup, you can see the restore candidates in *Choose a Backup* window, but you cannot restore a backup file as the *Restore* option is grayed out.

Limitations of FortiAuthenticator Cloud

The table lists the features currently unavailable in FortiAuthenticator Cloud, GA v6.6.7, special build 5555.

Feature or GUI options	Feature available?	Details of feature
Upgrade, Restore/Backup, Reboot, Shutdown	No	Upgrade, restore, backup, reboot, and shutdown are available via FortiAuthenticator Cloud portal.
System > Dashboard		
HA Status	N/A	
System > Dashboard > Status		
Device FQDN	Yes	*Device FQDN* is read-only.
User Inventory	Yes	• *FortiToken Hardware* and *FortiToken Mobile* are available. • The *FortiToken Cloud* related option displays number of allowed, assigned, and available users in FortiIdentity Cloud.
License Information	Yes	Total FortiAuthenticator Cloud SMS quota shown on the FortiAuthenticator Cloud portal.
System > Network		
Interface	No	
DNS	No	
Static Routing	No	
Packet Capture	No	
System > Administration		
System Access	Yes	• *HTTPS Certificate* and *CA certificate that issued the server certificate* dropdowns are locked with *Default-Server-Certificate* and *Fortinet_CA1_Root* respectively.
High Availability	No	
Firmware Upgrade	No	Managed via FortiAuthenticator Cloud portal.
Config Auto-backup	No	
SNMP	No	
Licensing	No	Managed via FortiAuthenticator Cloud portal.
FortiNACs	No	

Feature or GUI options	Feature available?	Details of feature
FTP Servers	No	
NetHSMS	N/A	
Replacement Messages	Yes	The following replacement messages are not available: • FortiToken Request Email Subject • FortiToken Request Email Message • FortiToken Mobile Activation Email Subject • FortiToken Mobile Activation Email Message • FortiToken Mobile Activation SMS Message • FortiToken Mobile Transfer Email Subject • FortiToken Mobile Transfer Email Message
System > Messaging	Yes	You cannot edit/delete the pre-configured FortiIdentity Cloud SMTP server (`smtp2.fortinet.com`). You cannot edit/delete the pre-configured FortiIdentity Cloud SMS gateway.
Authentication		
RADIUS Service	No	
RADSec	Yes	SNI is needed on the RADSec client.
TACACS+ Service	No	
LDAP Service	No	
FAC Agent	Yes	FortiAuthenticator Cloud supports FortiAuthenticator Agents for Microsoft Windows and OWA. However, offline tokens are not supported for the FortiAuthenticator Agent for Microsoft Windows. Offline tokens support will be added in a future version. **Note**: FortiAuthenticator agents cannot be downloaded from FortiAuthenticator Cloud. **To download FortiAuthenticator agents:** 1. Log in to FortiCloud. 2. In the *Support* dropdown, select *Firmware Download*. 3. In the *Select Product* dropdown, select *FortiAuthenticator_and_FortiTrustID_Agents*. 4. Select *Download*. 5. In the *FortiAuthenticator_and_FortiTrustID_Agents* folder, download the `FAC_Agent_Setup_vX.X.exe` file for FortiAuthenticator Agents for Microsoft Windows, and save the file to your computer. Download the `FAC_IIS_Agent_Setup_vX.X.exe` file for FortiAuthenticator Agent for Microsoft OWA, and save the file to your computer. 6. Open the file to install. For information on installing the agents, see the *FortiAuthenticator*

Feature or GUI options	Feature available?	Details of feature
		Agent for Microsoft Windows Install Guide and the *FortiAuthenticator Agent for Microsoft OWA Install Guide* on the Fortinet Docs Library.
Authentication > User Management		

Local Users	Yes	• All the OTP options available.
		Note: You can now disable both *Password authentication* and *One-Time Password (OTP)* authentication.
		• When editing a local user, the following options are not available:
		  • *Sync in HA Load Balancing mode*
		  • *Role*
		  • *Allow LDAP browsing*
		  • *TACACS+*

Remote Users	Yes	• All the OTP options available remote LDAP/RADIUS/SAML users.
		Note: You can now disable both *Password authentication* and *One-Time Password (OTP)* authentication.
		• When editing a remote user, the following options are not available:
		  • *Sync in HA Load Balancing mode*
		  • *Role*
		  • *TACACS+*

User Groups	Yes	*TACACS+ authorization rule* and *RADIUS Attributes* not available.
Usage Profile	Yes	The following menu options are not available when creating or editing a usage profile: • *Time Usage* • *Data Usage* • *Time Schedule*
Authentication > Portals > Portals		
Pre-Login Services	Yes	All the token options available in pre/post-login services.
Post-Login Services	Yes	All the token options available in pre/post-login services.
Authentication > User Management > Remote User Sync Rules All the OTP methods available for LDAP/SAML/SCIM sync rules.		
Authentication > SAML IdP > Service Providers		
Application name for FTM push notification	No	
Fortinet SSO > Methods		
Windows Event Log Sources	No	

Feature or GUI options	Feature available?	Details of feature
RADIUS Accounting Sources	No	
Tiered Architecture	No	
SSO MA	Yes	
Fortinet SSO > Settings > Methods > DC/TS Agent Clients	Yes	Ensure that you are using a recent DC/TS agent version that supports SNI. In *System > Administration > Access Rights*, ensure that *DC/TS Agent FSSO (TCP/8002)* is enabled under *HTTPS (TCP/443)*.
CLI	No	

The table lists the endpoints not available to customers in FortiAuthenticator Cloud.

`/radiusclients/`
`/radiuspolicies/`
`/radiuspolicyclient/`
`/tacplusclients/`
`/tacpluspolicies/`
`/tacpluspolicyclient/`
`/fortitokens/`
`/localusers/`
`/ldapusers/`
`/radiususers/`
`/localusers/[id]/radiusattributes/`
`/localapiadmin/`
`/pushauth/`
`/pushauthresp/`
`/system/external_ip_fqdn/`
`/fortiguardmessages/`
`/fortitokenmobilelicenses/`
`/smtpservers/`
`/upgrade/`
`/recovery/`

/scheduledbackupsettings/
/ftpservers/
/logsettings/
/licensing/
/fortitokenmobileprovisioning/

Customers can access the REST API endpoints using the port 443.

www.fortinet.com