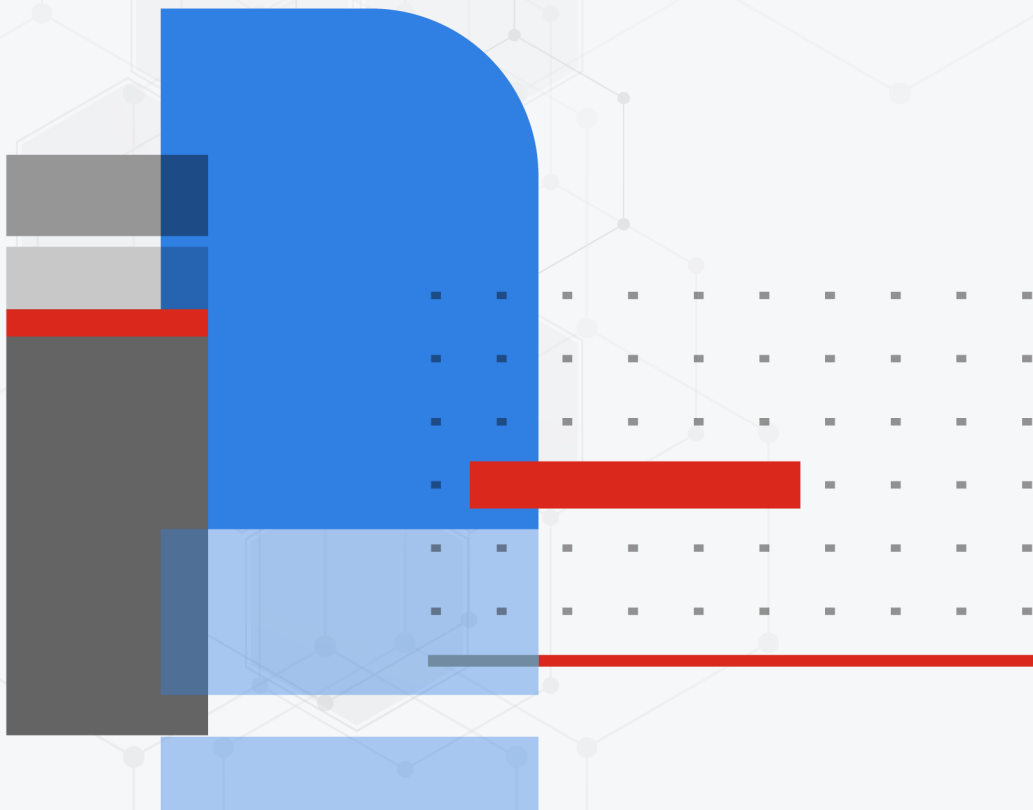




Administration Guide

FortiTrust Identity 24.1.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



January 31, 2024

FortiTrust Identity 24.1.b Administration Guide

65-241b-993542-20240131

TABLE OF CONTENTS

Change Log	4
Introduction	5
More information	5
Compatible Fortinet applications	6
Downloading FortiAuthenticator agents	6
Product documentation and support	7
Licensing	8
How to purchase a FortiTrust Identity license	8
SKUs	8
License expiry	9
Getting started	10
Registering FortiTrust Identity subscription	10
Logging in to FortiTrust Identity portal	10
Dashboard	12
Tab options	13
Log	14
License	15
Notification	16
Service status	16
FortiAuthenticator Cloud	17
Reboot an instance	19
Upgrade firmware	19
Backup and restore	20

Change Log

Date	Change Description
2024-01-31	Initial release.

Introduction

FortiTrust Identity is an Identity and Access Management as a Service (IDaaS) cloud service offered by Fortinet. FortiAuthenticator Cloud and FortiToken Cloud are available as a bundled service in FortiTrust Identity.

FortiTrust Identity delivers the following features using FortiAuthenticator Cloud:

- **Authentication:** FortiTrust Identity includes passwordless Fast Identity Online (FIDO), OAuth2 Authorization, OpenID Connect (OIDC), and Security Assertion Markup Language (SAML) authentication methods.
- **User Identification:** FortiTrust Identity 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:** FortiTrust Identity can create and sign digital certificates for use.
- **Integration:** FortiTrust Identity can integrate with third-party 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.

FortiTrust Identity delivers the following features using FortiToken Cloud:

- **Adaptive Authentication:** FortiTrust Identity 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. FortiTrust Identity 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:** FortiTrust Identity can act as a multi-factor authentication client using FortiToken Cloud.

More information

End-customers use FortiAuthenticator Cloud the same way as the stand-alone FortiAuthenticator. As a result, end-customers can use the *FortiAuthenticator Admin Guide* for information about using either the stand-alone FortiAuthenticator or FortiAuthenticator Cloud. For more information, see the *FortiAuthenticator Admin Guide* on the [Fortinet Docs Library](#).

For information on the limitations of FortiAuthenticator Cloud, see the *FortiTrust Identity Release Notes* on the [Fortinet Docs Library](#).

Compatible Fortinet applications

See the *FortiTrust Identity Release Notes* on the [Fortinet Docs Library](#).



FortiTrust Identity 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 *FortiTrustID_Agents*.
4. Select *Download*.
5. In *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 FortiTrust Identity related documentation and support information:

- For information about the current release, see the *FortiTrust Identity 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

FortiTrust Identity 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 FortiTrust Identity end-users in your account for the year. See [SKUs on page 8](#).



A FortiTrust Identity 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.



FortiTrust Identity does not include a free trial.

Also, see [License expiry on page 9](#).

How to purchase a FortiTrust Identity license

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

To register FortiTrust Identity subscription, see [Registering FortiTrust Identity subscription on page 10](#).

SKUs

The following table lists licensing options by SKU.

SKU	Number of FortiTrust Identity 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 FortiTrust Identity users to an existing FortiTrust Identity license.

For more information, see *Stackable co-termed licenses* in the [FortiToken Cloud Admin Guide](#).

License expiry

When FortiTrust Identity 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.

FortiTrust Identity 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 FortiTrust Identity 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 FortiTrust Identity:

1. [Registering FortiTrust Identity subscription on page 10](#)
2. [Logging in to FortiTrust Identity portal on page 10](#)

Registering FortiTrust Identity subscription

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

To register a FortiTrust Identity subscription on [FortiCloud](#), see [Registering assets](#) in the latest [Asset Management Administration Guide](#).

Logging in to FortiTrust Identity portal



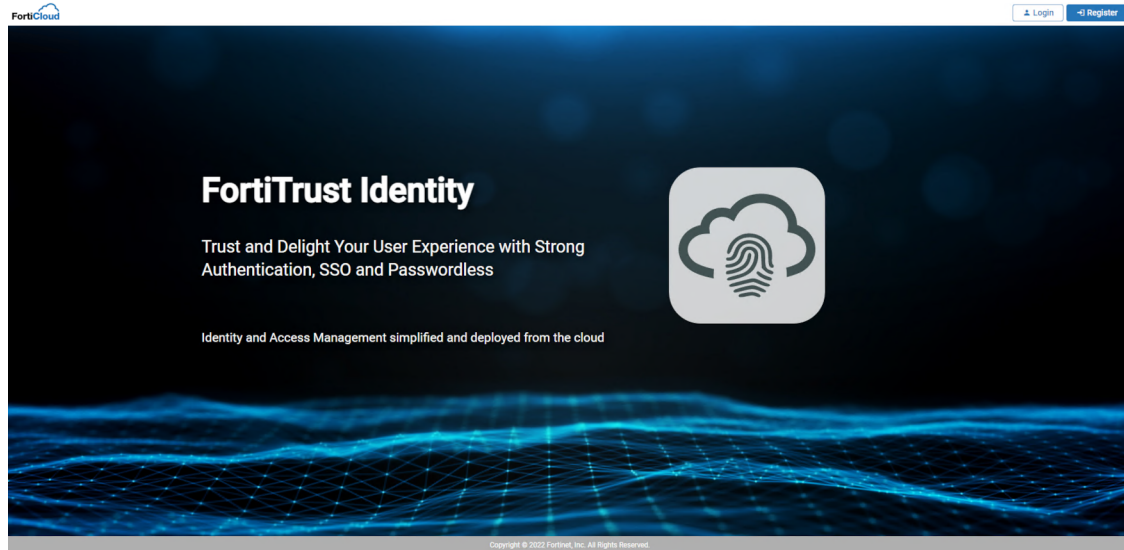
All FortiCloud registered users can access the FortiTrust Identity portal. If your organization has multiple FortiTrust Identity accounts, you see a list of FortiTrust Identity accounts after you sign in on FortiCloud. You can then select an account to open it on the FortiTrust Identity portal.

Access to FortiTrust Identity 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 FortiTrust Identity portal.

To log in to the FortiTrust Identity portal:

1. On the browser, go to <https://fortitrustid.forticloud.com/>.
The FortiTrust Identity portal opens.



2. In the upper-right corner, click *Login*.
The FortiCloud Login page opens.
3. Enter your FortiTrust Identity 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 FortiTrust Identity landing page opens with your FortiTrust Identity account or a list of accounts if your organization has multiple FortiTrust Identity accounts.



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

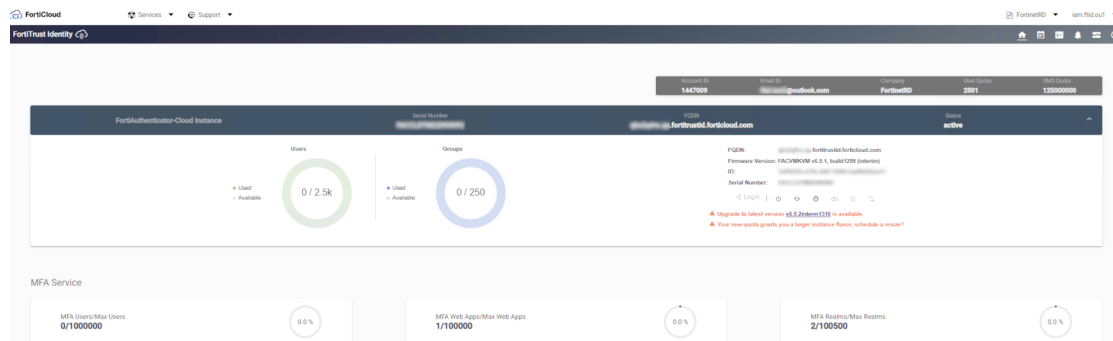
4. Click your account or one of your accounts to open it.
For IAM users, once logged in, a new *Make a Selection to Proceed* page appears where you can click *Select* next to an account from the hierarchy to use.
FortiTrust Identity dashboard opens by default. See [Dashboard on page 12](#).

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.

Dashboard

The FortiTrust Identity 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.
Groups	The current group count.
Firmware Version	The version and build number of the firmware installed. To update the firmware, select the <i>Upgrade Firmware</i> (⚙️) icon. See Upgrade firmware on page 19 .
ID	The ID of the FortiAuthenticator Cloud instance.

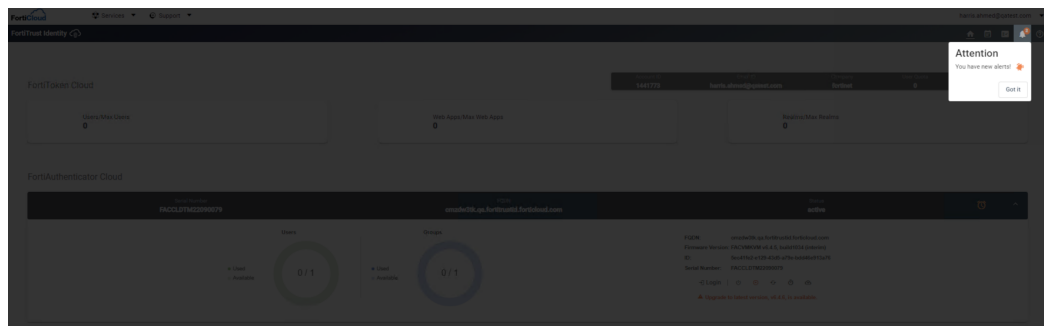
Information/widget	Description
MFA Service	
MFA Users/Max Users	Users ready, in percentage.
MFA Web Apps/Max Web Apps	Web applications ready, in percentage.
MFA Realms/Max Realms	Realms ready, in percentage.



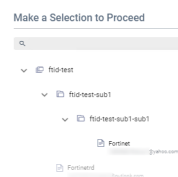
Users and Groups widgets refresh when the user logs in. Once logged in, the widgets refresh on-demand.



If there are notifications, the *Attention* dialog pops up when you log in to the FortiTrust Identity 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 13.

Tab options

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

Options	Description
Services	Access other FortiCloud services. See Services .
Support	Support options including <i>Downloads</i> and <i>FortiCare</i> . 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 <i>Dashboard</i> tab.
Log	Click  icon to open the <i>Log</i> tab. See Log on page 14 .
License	Click  icon to open the <i>License</i> tab. See License on page 15 .
Notification	Click  icon to open notifications. See Notification on page 16 .
Status	Click  icon to open the FortiTrust Identity service status page. See Service status on page 16 .
Help	Click  icon to go to the <i>FortiTrust Identity Admin Guide</i> on the Fortinet Docs Library .
Login	Click  icon to enter the FortiAuthenticator Cloud instance. See FortiAuthenticator Cloud on page 17 .
Reboot instance	Click  icon to reboot the instance. See Reboot an instance on page 19 .
Refresh information	Click  icon to refresh the information and widgets on the <i>Dashboard</i> . Note: Once clicked, <i>Refresh Information</i> grays out for 10 seconds before you can click again.
Restore instance	Click  icon to restore the backup instance.
Backup instance	Click  icon to backup the current instance. See Backup and restore on page 20 .
Upgrade firmware	Click  icon to upgrade the instance. See Upgrade firmware on page 19 .
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 FortiTrust Identity.

Timestamp	User	Action	Subject	Status
05-12-2022 11:01:17	fortitrustid_hahmed@qatest.com	get	fac login (FACCOLSTM22090945)	successful
05-12-2022 11:01:16	fortitrustid_hahmed@qatest.com	get	fac login (FACCOLSTM22090945)	successful
05-12-2022 10:57:13	fortitrustid_hahmed@qatest.com	create	fac config backup (a4f8885a425e-4ea0-a57b-611f60983776)	successful
05-12-2022 10:52:14	fortitrustid_hahmed@qatest.com	create	login (1325588)	successful
05-12-2022 10:22:49	fortitrustid_hahmed@qatest.com	get	fac login (FACCOLSTM22090945)	successful
05-12-2022 09:40:53	fortitrustid_hahmed@qatest.com	create	login (1325588)	successful

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.

05-12-2022 14:21:00	fortitrustid_hahmed@qatest.com	create	login (1325588)	successful
<div> <div>Request ID fortrustid58581-7645-413f-a4a2-7ee59a82274</div> <div>Request Info Called endpoint /login with parameter { "key": "source_app", "FortiTrustID": "account_id", "1325588", "user_id": "1", "user_fullaccess": true, "context_data": "", "visited_links": [] } return response with code 200</div> </div>				



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

License

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

Contract	SN	Quantity	Start Date	End Date	Status
482518329437	FACCOLSTM22090945	23000	04-17-2022 17:00:00	04-17-2023 17:00:00	active

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 12 .
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

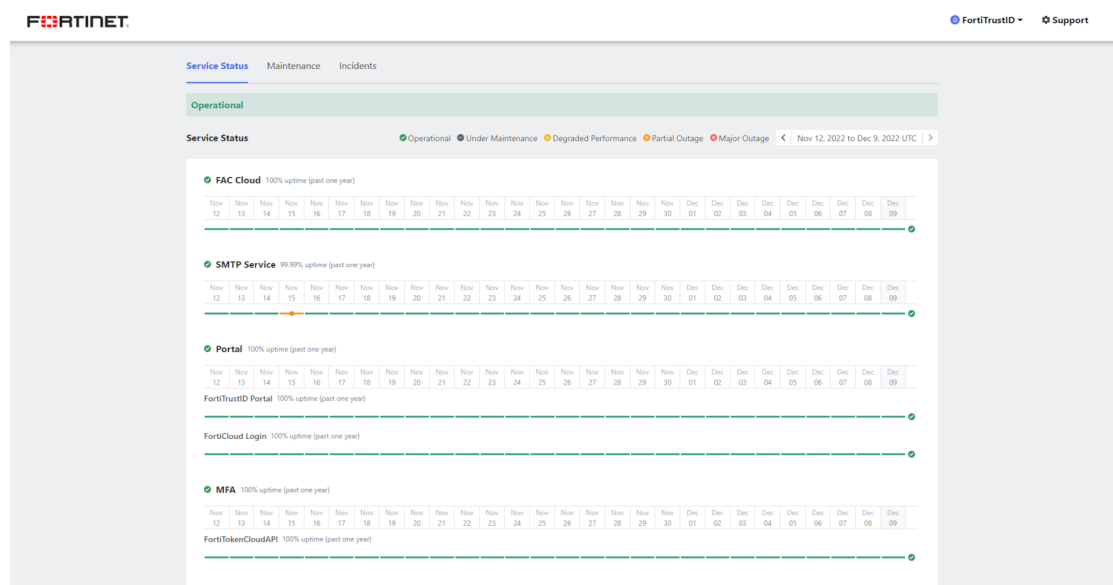
To check notifications, click *Notification* (🔔).

License expiry related notifications appear here.



Service status

To check the FortiTrust Identity service status, click *Service Status* (📊).



Alternatively, the FortiTrust Identity 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 (FortiTrust Identity Portal and FortiCloud Login)*
- *MFA*

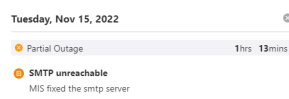


Use < and > to change the date range.

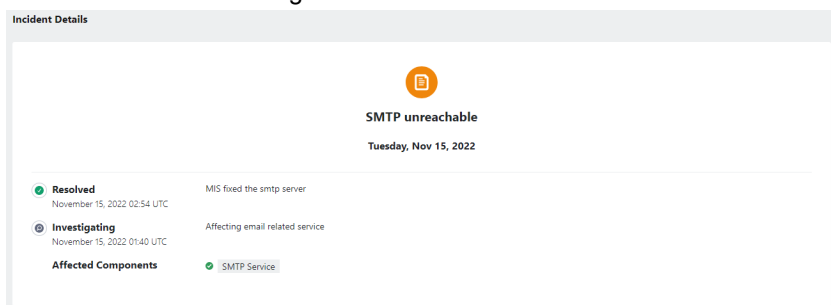
Go to *Maintenance* and *Incidents* to see a list of maintenance events and incidents.

To see more information about a incident:


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



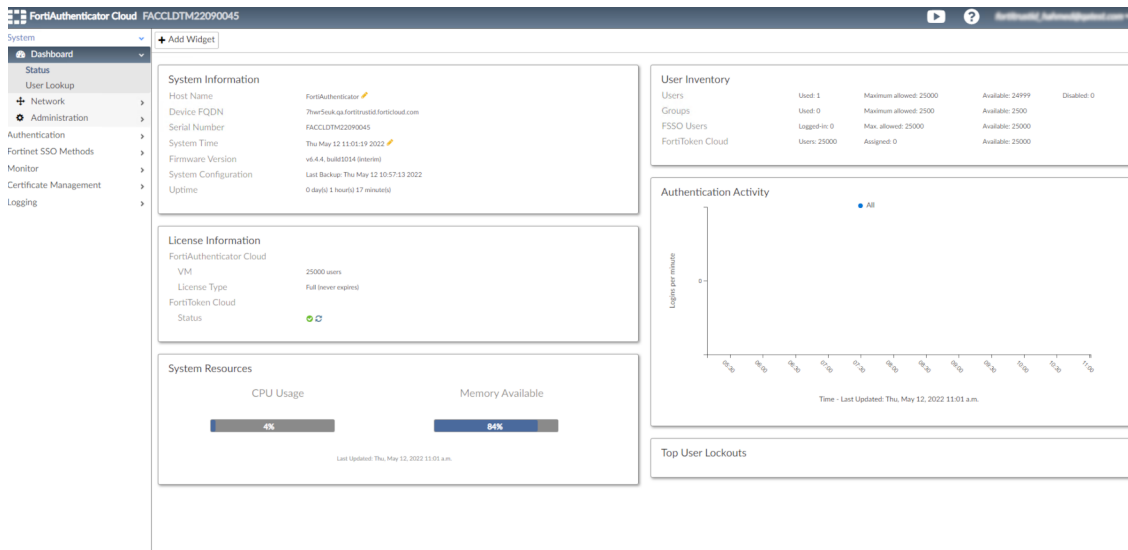
2. Click on the status message to see more information in a new tab.



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 is the fixed WAN IP address to build zero trust tunnels into an on-prem environment.

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

Returning to FortiTrust Identity

To return to the FortiTrust Identity 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 FortiTrust Identity instance, click *Reboot instance* (⚙️).

The following reboot settings are available:

- *Hard* (⚡): select, then click *OK* to forcefully reboot the FortiTrust Identity instance, i.e. the FortiTrust Identity instance is shut down immediately, then reboot.
- *Soft* (⌚): select, then click *OK* to gracefully reboot the FortiTrust Identity instance, i.e. the FortiTrust Identity 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 20](#).

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 FortiTrust Identity 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 FortiTrust Identity.

To create a backup instance:

1. Click *Backup instance* (🔒) to create an instance of data backup.

Backup Instance

Alias

Backup Close

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

To restore a backup:

1. Click *Restore instance* (🔒) .

The *Choose a Backup* window opens.

Choose a Backup

Version	Alias	Time
v6.4.4	test_backup	05-10-2022 10:57:13

Items per page: 5 1 - 1 of 1 < >

Restore Cancel



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 12 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.



www.fortinet.com

Copyright© 2024 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.