



Release Notes

FortiAuthenticator 8.0.4



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



October 22, 2026

FortiAuthenticator 8.0.4 Release Notes

TABLE OF CONTENTS

Change log	5
FortiAuthenticator 8.0.4 release	6
Special notices	7
TFTP boot firmware upgrade process	7
Monitor settings for GUI access	7
Before any firmware upgrade	7
After any firmware upgrade	7
FortiAuthenticator does not support PEAP-MAB	7
SHA-1 cryptographic operations are no longer supported	8
Reconfigure LinkedIn social login	8
Using remote syslog servers with Secure connection enabled	8
SAML IdP entity ID changes from HTTP to HTTPS after upgrade	8
Remote user synchronization rule behavior change for FortiToken Mobile activation	9
Mutual authentication required for RADSec connections	9
What's new	11
FSSO: Automated discovery of Domain Controllers for event log polling	11
Advanced/Carrier license: Unlimited RADIUS/TACACS+ clients	11
SAML IdP: IdP proxy FIDO exemption	12
Updated FortiAuthenticator version on the AWS Marketplace	12
OIDC: Same LDAP attribute options as SAML IdP for JWT	12
Remote SQL servers	12
MAU enforcement	13
Self-service portal: Password validation	14
GUI modernization	14
User Portals: Offline FortiToken Mobile reprovisioning	15
RADIUS: MAC device tracking	16
REST API: Custom tree location for LDAP Service directory auto-provisioning	16
REST API documentation (Redoc)	16
GUI based CLI console access	17
FortiAuthenticator available on GCP Marketplace	17
LDAP server: Authentication proxy	17
Support full PKI capability	17
SCIM Client Offline Mode CLI command	17
New FortiAuthenticator 300G and 800G hardware models	18
Upgrade instructions	19
Hardware and VM support	19
Image checksums	20
Upgrading from 4.x/5.x/6.x	20
Product integration and support	24
Web browser support	24
FortiOS support	24
Fortinet agent support	25
Virtualization software support	25

Third-party RADIUS authentication	26
FortiAuthenticator-VM	27
Resolved issues	28
Known issues	36
Maximum values for hardware appliances	38
System > Network	38
System > Messages	38
System > Administration	39
Realms	39
Authentication > General	39
Remote authentication servers	40
FSSO & Dynamic Policies	41
Accounting Proxy	41
Certificates > User Certificates	41
Certificates > Certificate Authorities	42
Certificates > SCEP	42
Certificates > CMP	42
Services	42
Maximum values for VM	43
System > Network	43
System > Messages	43
System > Administration	44
Authentication > General	44
Remote authentication servers	44
User Management	45
FSSO & Dynamic Policies > FSSO	46
FSSO & Dynamic Policies > Accounting Proxy	46
Certificates > User Certificates	47
Certificates > Certificate Authorities	47
Certificates > SCEP	47
Certificates > CMP	48
Services	48
Data-at-rest protection	49

Change log

Date	Change Description
2026-10-22	Initial release. Updated What's new on page 11 . Updated Hardware and VM support on page 19 . Added bug 1287775 to the Resolved issues on page 28 . Updated Maximum values for hardware appliances on page 38 .

FortiAuthenticator 8.0.4 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 8.0.4, build 0191.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit: <https://docs.fortinet.com/product/fortiauthenticator/>

Special notices

TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. From the administrator dropdown menu in the toolbar, go to **Restore/Backup**, and click **Download Backup File** to backup the configuration.

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

FortiAuthenticator does not support PEAP-MAB

FortiAuthenticator only supports MAB in clear-text and not the encapsulated MAB.

SHA-1 cryptographic operations are no longer supported

FortiAuthenticator does not support SHA-1 as the SHA-1 cryptographic algorithm is no longer considered secure.

Update SHA-1 certificate signing to use SHA-2 or above for enhanced security. If this is not possible, downgrade to FortiAuthenticator version 6.5.3 for SHA-1 support.

Reconfigure LinkedIn social login

LinkedIn has changed their OAuth app API.

If you are using LinkedIn social login, you will need to reconfigure your application on LinkedIn and update your remote OAuth server for LinkedIn with the new Key and Secret after upgrading to the FortiAuthenticator 6.6.1 GA firmware.

Using remote syslog servers with Secure connection enabled

In earlier firmware versions, FortiAuthenticator did not verify if the syslog server certificate contained a valid hostname while establishing a TLS connection.

In 8.0.4, if the remote syslog server is not configured to use a server certificate with a valid hostname, FortiAuthenticator fails to negotiate the TLS connection.

SAML IdP entity ID changes from HTTP to HTTPS after upgrade

When upgrading FortiAuthenticator from 6.x to 8.0.2 or 8.0.3, the SAML **IdP entity ID** changes from HTTP to HTTPS. The IdP single sign-on URL and IdP single logout URL are unaffected by this change.



If your SPs were registered using the HTTP version of the IdP entity ID prior to the upgrade, single sign-on will fail after the upgrade because the SP's metadata no longer matches the IdP entity ID.

To restore SAML SSO after upgrading:

1. Go to **Authentication > SAML IdP > Service Providers**.
2. For each SP, select **IdP metadata** to download the updated metadata file.
3. Import the updated metadata into each SP, or manually update the registered IdP entity ID to use HTTPS.



If you use alternate IdP prefixes, the entity ID generated for each prefix is also updated to HTTPS. Update each registered SP accordingly.

Remote user synchronization rule behavior change for FortiToken Mobile activation

Effective in FortiAuthenticator 6.6.10, remote user synchronization rules that assign a FortiToken Mobile to user accounts handle incomplete activations differently than in previous releases.

In FortiAuthenticator 6.6.9 and earlier, if an end user did not complete FortiToken Mobile activation within the specified activation period, FortiAuthenticator locked the corresponding user account. An administrator had to manually unlock the user account before the user could retry activation.

In FortiAuthenticator 6.6.10, if an end user does not complete FortiToken Mobile activation within the specified activation period, the remote user synchronization rule unlocks the user account and triggers a new FortiToken Mobile activation for that user. Administrator intervention is no longer required to restore access after a failed activation attempt.

Mutual authentication required for RADSec connections

Starting in FortiAuthenticator 8.0.3, RADSec clients must authenticate the RADSec TLS connection using a trusted client certificate. Review the following configuration requirements before upgrading to or configuring RADSec on FortiAuthenticator 8.0.3.

FortiGate must authenticate to the RADSec server with a client certificate:

1. Configure FortiGate to authenticate to the RADSec server using a client certificate.
2. Import the certificate authority (CA) certificate that issued the client certificate into the FortiAuthenticator Trusted CA's store.

FortiGate must be able to verify the FortiAuthenticator RADSec server certificate:

1. Import the CA certificate that issued the RADSec server certificate into the FortiGate Trusted CA's store.
2. Configure the FortiGate RADSec settings with the imported CA certificate.

```
config user radius
edit "FAC-RadSec"
set transport radsec
set client-cert "FGT-RadSec-Cert" #required for FortiAuthenticator 8.0.x
set ca-cert "FAC-Root-CA" #required for FortiAuthenticator 6.6.x and 8.0.x
next
end
```

What's new

FortiAuthenticator version 8.0.4 includes the following enhancements:

The following list contains new and expanded features added in FortiAuthenticator 8.0.4.

FSSO: Automated discovery of Domain Controllers for event log polling

When configuring a **Windows Event Log** in **Fortinet SSO > Source Management > Windows Event Log**, a new **Discovery mode** setting is available:



The **Discovery mode** setting defaults to **Auto** if there are auto-discovered sources.

- When **Auto** is selected, you can select **Windows Log sources** from a list of automatically discovered Domain Controllers.

Alternatively, you can configure the **Windows Event Log** settings manually by selecting **Manual**.



Multiple Windows event logs can now be edited in bulk by first selecting the Windows event logs and then selecting **Edit**.



Only the administrator credentials for all the selected Windows event log sources can be bulk edited.

Each time the auto-discovery process finds a new DC, it sends alerts to notify the FortiAuthenticator administrator that a new Domain Controller is available for FSSO event polling.

Advanced/Carrier license: Unlimited RADIUS/TACACS+ clients

FortiAuthenticator now checks for the Advanced/Carrier license entitlement enforcement by contacting FortiGuard.

When FortiAuthenticator has an Advanced/Carrier license, the **License Information** widget offers a new **Advanced Feature** row displaying **Carrier**:

- When FortiAuthenticator license is upgraded to Advanced/Carrier, FortiAuthenticator unlocks unlimited RADIUS and TACACS+ clients for FortiAuthenticator-VM and FortiAuthenticator 3000F/G hardware models.



All other configuration objects preserve the same limits as for a standard FortiAuthenticator license.

- When FortiAuthenticator Advanced/Carrier license expires (or invalidated in HA A-P scenario with a standard licensed peer), RADIUS and TACACS+ client limit reverts to those of the unlicensed/standard license.



In HA A-P, both primary and secondary FortiAuthenticator nodes must have an Advanced/Carrier license. If either of the FortiAuthenticator nodes do not have the Advanced/Carrier license, both the FortiAuthenticator nodes revert to their standard license limits.



In HA A-A, if primary/secondary FortiAuthenticator nodes have Advanced/Carrier license, but the LB FortiAuthenticator only has a standard license, the LB FortiAuthenticator enforces its standard license limits.

SAML IdP: IdP proxy FIDO exemption

A new **Authentication method enforced for IdP proxy logins** setting available when configuring an SP in **Authentication > SAML IdP > Service Providers**.

Enable **Authentication method enforced for IdP proxy logins** to control whether the authentication method is enforced for IdP proxy logins i.e., remote SAML user logins.

When disabled, FortiAuthenticator grants an IdP session to the remote SAML user after the user successfully logs in with an external IdP.

Updated FortiAuthenticator version on the AWS Marketplace

On the AWS Marketplace, the FortiAuthenticator version has been updated to 8.0.4.

OIDC: Same LDAP attribute options as SAML IdP for JWT

Starting FortiAuthenticator 8.0.4, **Claims** for the Relying Party settings in **Authentication > OAuth Service > Relying Party** offers new options under **User attribute** for **Remote LDAP server**, **Remote RADIUS server**, and **Other**. Previously available options are available under **FortiAuthenticator**. Also, a new **Realm** option is available under **FortiAuthenticator**.

Remote SQL servers

Starting FortiAuthenticator 8.0.4, you can now add/edit/delete SQL remote servers in **Authentication > Remote Auth. Servers > SQL**.

You can now add/edit/delete remote SQL user groups in **Authentication > User Management > User Groups**.

The following new options are available when configuring a user group:

- A new **Remote SQLType**.
- A new **Remote SQL** dropdown when the **Type** is **Remote SQL**.

- A new **SQL query to determine group membership** setting when the **Type** is **Remote SQL**.

You can also add realms for remote SQL servers in **Authentication > User Management > Realms**.

RADIUS authentication profiles in **Authentication > RADIUS Service > Auth Profiles** can now be configured with SQL realms.

Also, group filtering is available for SQL realms.

A new **SQL sync rule** can be configured in **Authentication > User Management > Remote User Sync Rules** to import MAC devices from a remote SQL server.

A new `/api/v2/realms` API endpoint is available that adds support for remote SQL servers.

The following are now logged in **Logging > Log Access > Logs**:

- Add/edit/delete events for new configuration objects (remote SQL servers, SQL realms, and SQL sync rules)
- Authentication outcome for remote SQL users (success/failure)
- MAC device sync rule events (similar to user sync rules)

MAU enforcement

The following widgets have been updated:

- **Monthly Active Users** has been renamed to **Monthly Active Usage**.
 - The **Monthly Active Usage** widget tracks client certificates, devices, and users related successful login activity.



Click the individual labels for users, devices, and certificates to display/hide each category.



FSSO users are not included in the **Users** count.

- **Monthly Active Usage** row has been removed from the **License Information** widget.
- The **User Inventory** widget now includes the following three new rows:
 - **Monthly Active Users**
 - **Monthly Active Certificates**
 - **Monthly Active Devices**

See [MAU Enforcement](#) on the [Fortinet Docs Library](#).

The **Licensing** tab in **Administration** now displays MAU related information.

Active Users in **Monitor > Authentication** has been renamed to **Active Usage**.

The following four new tabs are available in **Active Usage**:

- **Overview**
- **Users**
- **Devices**
- **Certificates**

The following are now logged in **Logging > Log Access > Logs**:

- **Information** level log if MAU counts are within license limits, e.g.:

Active usage: 80 users, 10 devices, 50 certificates

- **Warning** level log if monthly active devices and/or monthly active certificates exceed 100% of the license limit, e.g.:

Active usage above license limit: 80 users, 10 devices, 500 certificates

- **Critical** level log if monthly active users count exceeds 100% of the license limit, e.g.:

Active usage above license limit: 105 users, 10 devices, 50 certificates. System at risk of degraded performance enforcement

- **Alert** level log if monthly active users count exceeds 110% of the license limit, e.g.:

Active usage exceeding license limit: 125 users, 10 devices, 50 certificates. Degraded performance enforcement is in effect



Alert messages are sent when:

- Monthly active users count exceeds **100%** of the license limit.
- Monthly active users count exceeds **110%** of the license limit.



If user active usage exceeds **110%** of the license limit, authentications (user, device, and certificate) may randomly fail.

Self-service portal: Password validation

Starting FortiAuthenticator 8.0.4, an admin can import a list of invalid passwords.

Every new import overwrites the previously imported invalid passwords list.

A new password is allowed only when the entered password does not show up in the invalid passwords list.



The self-service portal password reset and password change pages indicate the strength of the new password input.

GUI modernization

Starting FortiAuthenticator 8.0.4, the following menu items have been updated to a modernized layout for improved usability:

- **System > Network > Interfaces**
- **System > Network > Packet Capture**
- **FortiNACs**, previously available under **System > Administration**, has been moved to **Fortinet SSO > Source Management > FortiNACs**.
- **System > Administration > Licensing**

- **System > Administration > Firmware Upgrade**

The **Fortinet SSO** GUI menu has been reorganized as:

- **Network Topology**
 - FortiGate Connectors
 - Tiered Architecture
 - Advanced Settings
- **Source Management**
 - SSO Sources
 - Windows Event Log
 - RADIUS Accounting
 - FortiNACs
 - Syslog
 - Web Services
 - SAML Servers
- **Policies & Filtering**
 - AD Group Lookup
 - SSO Users
 - SSO Groups
 - Domain Sets
 - User/Group Policies
 - IP Rules
 - FortiGate Policies

New **Alert Logs** tab available in **Logging > Log Access**.

User Portals: Offline FortiToken Mobile reprovisioning

When the offline FortiToken mode is enabled, i.e., the **Provisioning Mode** is set to **Offline** while editing token policy settings in **Authentication > User Account Policies > Tokens**, user portal **Allow users to reconfigure their FortiToken Mobile** in **Authentication > Portals > Portals > Pre-Login Services** can be enabled/disabled.

When **Allow users to reconfigure their FortiToken Mobile** is enabled, FortiAuthenticator displays offline FortiToken Mobile options including **Display QR code**.



In offline FortiToken mode, you must restrict access to the user portal as the setting allows FortiToken Mobile change when the username and password is known.

When attempting to access the user portal, after the user clicks **Lost my token**, FortiAuthenticator displays the reprovision FortiToken Mobile page.

The offline FortiToken reprovisioning sequence is similar to the offline self-provisioning sequence.

RADIUS: MAC device tracking

Starting FortiAuthenticator 8.0.4, RADIUS MAB policies in **Authentication > RADIUS Service > Policies** display a new **Return User Group Attributes** column under the **RADIUS response** tab.

The new **Return User Group Attributes** column indicates which user group RADIUS attributes are returned:

- **All 'list of users' groups** (legacy and default)
- **Specified user groups**: When selected, additional **Specified User Groups** pane is displayed where you can select from any configured local, LDAP, or RADIUS user groups.



SAML/SQL user groups are not supported.

When configuring a RADIUS authentication profile in **Authentication > RADIUS Service > Auth Profiles** new device tracking settings are available:

Device tracking: Tracks devices that authenticate through this authentication profile by recording their MAC addresses.

- **Place registered devices into this group**: When enabled, FortiAuthenticator automatically adds each tracked device to the selected MAC user group.
- **Remove MAC devices after**: When enabled, FortiAuthenticator automatically removes a tracked device's MAC address record after the specified number of days (1 - 365).

When configuring a remote LDAP sync rule in **Authentication > User Management > Remote User Sync Rules**, a new **Active** (same as for SCIM sync rule) LDAP attribute mapping is available. The new **Active** LDAP attribute mapping syncs the user account status (enabled/disabled) from the remote LDAP server.

In **Authentication > User Management > MAC Devices**, a new **Description** column is available.

REST API: Custom tree location for LDAP Service directory auto-provisioning

Starting FortiAuthenticator 8.0.4, FortiAuthenticator allows the REST API client to optionally specify where to auto-provision the new local users to the LDAP service directory tree.

New `ldap_dn` field added to the following FortiAuthenticator endpoints:

- `/api/v1/localusers/`
- `/api/v1/csv/localusers/`

See the latest [FortiAuthenticator REST API Guide](#).

REST API documentation (Redoc)

FortiAuthenticator 8.0.4 adds Redoc documentation for the REST API v2, available at `https://<FortiAuthenticator-IP>/api/v2/redoc`.

Redoc provides a readable, searchable reference for REST API endpoints, but does not support running API commands.

GUI based CLI console access

FortiAuthenticator 8.0.4 provides CLI console access directly from the GUI. Select the >_ icon in the top banner to open the CLI console in a new browser tab.

The CLI console provides direct command-line access without requiring a separate SSH session or physical console connection.

FortiAuthenticator available on GCP Marketplace

FortiAuthenticator 8.0.4 is available as a Bring Your Own License (BYOL) listing on the Google Cloud Platform (GCP) Marketplace.

Administrators can locate the FortiAuthenticator listing in the [GCP Marketplace](#) and deploy it directly to a Compute Engine instance.

After deployment, apply an existing FortiAuthenticator license to activate the instance.

LDAP server: Authentication proxy

Starting FortiAuthenticator 8.0.4, the network interface settings offers the following two new settings in an interface in **System > Network > Interfaces** to control access to LDAP/LDAPS authentication proxy service:

- **LDAP Auth Proxy (8389)**
- **LDAPS Auth Proxy (8636)**

You can select the remote LDAP server for LDAP authentication proxy under the new **LDAP auth proxy remote LDAP server** setting in **Authentication > LDAP Service > General**.

Support full PKI capability

Starting FortiAuthenticator 8.0.4, the LB FortiAuthenticator can issue/renew/revoke certificates locally.

The certificate changes are propagated up to the primary and back to all the LB FortiAuthenticator nodes.

SCIM Client Offline Mode CLI command

FortiAuthenticator now includes the following CLI command that enables/disables offline mode for the SCIM client role:

```
execute scim-client-offline-mode {enable | disable}
```

Use this command when FortiAuthenticator acts as the identity provider (IdP), pushing user and user group updates to a remote SCIM server acting as the service provider (SP).

New FortiAuthenticator 300G and 800G hardware models

FortiAuthenticator 8.0.4 introduces support for two new hardware models: FortiAuthenticator 300G and FortiAuthenticator 800G.

Upgrade instructions



Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the [FortiAuthenticator Administration Guide](#).



FortiAuthenticator 8.0.4 requires at least 16 GB of RAM and 8 vCPUs.



When FortiAuthenticator 8.0.4 is the RADIUS server and *Require client to send Message-Authenticator attribute* is enabled in *Authentication > RADIUS Service > Clients*, the RADIUS client must include the message authenticator attribute in the RADIUS authentication requests. Otherwise, FortiAuthenticator discards the RADIUS authentication requests.



When FortiAuthenticator 8.0.4 is the RADIUS client, FortiAuthenticator always includes the message authenticator attribute when sending the RADIUS authentication requests.



When *Require Message-Authenticator Attribute in Response* is enabled in *Authentication > Remote Auth. Servers > RADIUS*, FortiAuthenticator only accepts the responses that include the message authenticator attribute that was sent.

- Hardware and VM support on page 19
- Image checksums on page 20
- Upgrading from 4.x/5.x/6.x on page 20

Hardware and VM support

FortiAuthenticator 8.0.4 supports:

- FortiAuthenticator 300F
 - FortiAuthenticator 300G
 - FortiAuthenticator 800F
 - FortiAuthenticator 800G
 - FortiAuthenticator 3000F
 - FortiAuthenticator VM
- See [Virtualization software support](#) on page 25.

Image checksums

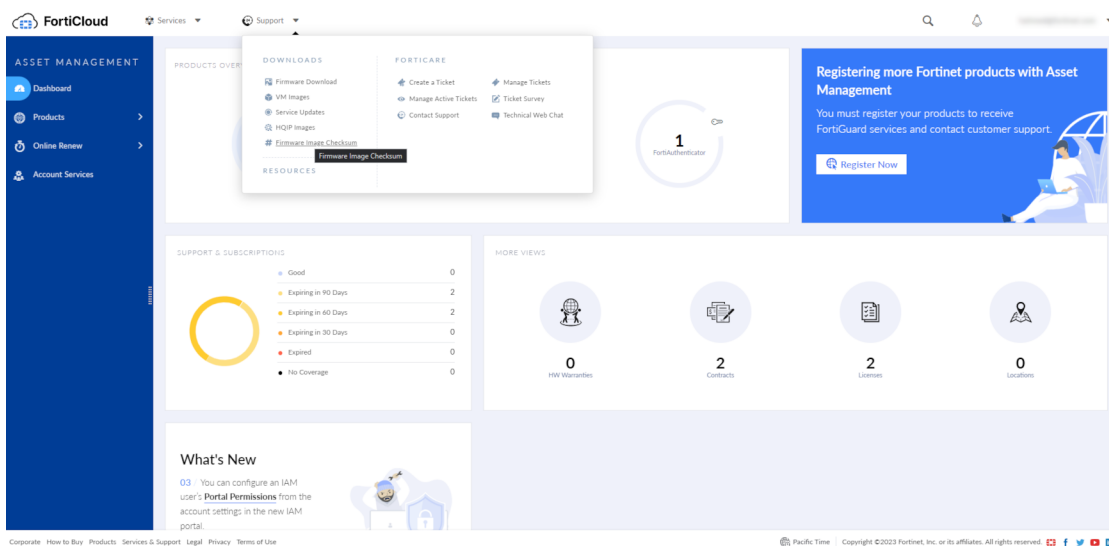
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available on [FortiCloud](#).

FortiCloud image checksum tool

After logging in to FortiCloud, in the menus at the top of the page, click **Support**, then click **Firmware Image Checksum**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code** to get the checksum code.



Upgrading from 4.x/5.x/6.x

FortiAuthenticator 8.0.4 build 0191 officially supports upgrades from previous versions by following these supported FortiAuthenticator upgrade paths:

- If currently running FortiAuthenticator 6.0.5 or older, first upgrade to 6.0.7, then upgrade to 8.0.4, else the following message will be displayed: Image validation failed: The firmware image model number is different from the appliance's.
- If currently running FortiAuthenticator 6.0.7, then upgrade to 8.0.4 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 8.0.4.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 8.0.4 directly.



When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 8.0.4 from FortiAuthenticator 6.0.7, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See [Upgrading KVM / Xen virtual machines](#) on page 22.



Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.



Ensure the hypervisor provides at least 16 GB of memory to the FortiAuthenticator-VM. Also, FortiAuthenticator-VM requires a minimum of 8 vCPUs.

Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the [FortiCloud](#), then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the [FortiCloud](#).
2. In the **Support > Download** section of the page, select the **Firmware Download** link to download the firmware.
3. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksum** link.
4. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
5. Upload the firmware and begin the upgrade.
When upgrading from FortiAuthenticator 6.0.4 and earlier:
 - a. Go to **System > Dashboard > Status**.
 - b. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
 - c. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
When upgrading from FortiAuthenticator 6.1.0 or later:
 - a. Click on the administrator name in the upper-right corner of the GUI to display the dropdown menu, and click **Upgrade**.
 - b. In the **Firmware Upgrade or Downgrade** section, select **Upload a file**, and locate the upgrade package that you downloaded.
6. Select **OK** to upload the file to the FortiAuthenticator.
Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:
Fortinet recommends to save a copy of the current configuration before proceeding with firmware upgrade.
It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.
Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.



Due to a known issue in 6.0.x and earlier releases, the port5 and port6 fiber ports are inverted in the GUI for FortiAuthenticator-3000E models (i.e. port5 in the GUI corresponds to the physical port6 and vice-versa).

This is resolved in 6.1.0 and later, however, the upgrade process does not swap these configurations automatically. If these ports are used in your configuration during the upgrade from 6.0.x to 6.1.0 and later, you will need to physically swap the port5 and port6 fibers to avoid inverting your connections following the upgrade.

Upgrading KVM / Xen virtual machines

When upgrading existing KVM and Xen virtual machines from FortiAuthenticator 6.0.7 to 8.0.4, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image before starting the upgrade. This requires file system write-access to the virtual machine disk drives, and must be performed while the virtual machines are in an offline state, fully powered down.



If your virtual machine has snapshots, the resize commands detailed below will exit with an error. You must delete the snapshots in order to perform this resize operation.

Make a separate copy of the virtual disk drives before deleting snapshots to ensure you have the ability to rollback.

Use the following command to run the resize on KVM:

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

Use the following command to run the resize on Xen:

```
qemu-img resize /path/to/facxen.qcow2 1G
```

After this command has been completed, you may proceed with the upgrade from 6.0.7 to 8.0.4

Recovering improperly upgraded KVM / Xen virtual machines

If the upgrade was performed without completing the resize operation above, the virtual machine will fail to properly boot, instead displaying many **initrd** error messages. If no snapshots are available, manual recovery is necessary.

To recover your virtual machine, you will need to replace the operating system disk with a good copy, which also requires write-access to the virtual hard disks in the file system while the virtual machines are in an offline state, fully powered down.

To recover an improperly upgraded KVM virtual machine:

1. Download the 6.0.7 GA ZIP archive for KVM, **FAC_VM_KVM-v6-build0059-FORTINET.out.kvm.zip**.
2. Extract the archive, then replace your virtual machine's **fackvm.qcow2** with the one from the archive.

3. Execute the following command:

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

To recover an improperly upgraded Xen virtual machine:

1. Download the 6.0.7 GA ZIP archive for Xen, **FAC_VM_XEN-v6-build0059-FORTINET.out.xen.zip**.
2. Extract the archive, then replace your virtual machine's **facxen.qcow2** with the one from the archive.
3. Execute the following command:

```
qemu-img resize /path/to/facxen.qcow2 1G
```

Product integration and support

FortiAuthenticator supports the following:

- [Web browser support on page 24](#)
- [FortiOS support on page 24](#)
- [Fortinet agent support on page 25](#)
- [Virtualization software support on page 25](#)
- [Third-party RADIUS authentication on page 26](#)

Web browser support

The following web browsers are supported by FortiAuthenticator 8.0.4:

Google Chrome version 154
Mozilla Firefox version 157
Microsoft Edge version 154



Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 8.0.4 supports the following FortiOS versions:

FortiOS v7.6.x
FortiOS v7.4.x
FortiOS v7.2.x
FortiOS v7.0.x
FortiOS v6.4.x
FortiOS v6.2.x
FortiOS v6.0.x

Fortinet agent support

FortiAuthenticator 8.0.4 supports the following Fortinet Agents:

FortiClient v.6.x , v.7.x for Microsoft Windows and macOS (Single Sign-On Mobility Agent)
For FortiAuthenticator Agents for Microsoft Windows and Outlook Web Access compatibility with FortiAuthenticator, see the <i>Agents Compatibility Matrix</i> on the Fortinet Docs Library .
 The FortiAuthenticator Agents for Microsoft Windows and OWA download files are now available in the <code>FortiTrustID_Agents</code> folder in <i>Support > Firmware Download</i> on FortiCloud.
FSSO DC Agent v.5.x
FSSO TS Agent v.5.x



Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.



FortiAuthenticator Agent for Microsoft Windows 4.0 and above required to support emergency offline access.

Also, FortiAuthenticator Agent for Microsoft Windows below 4.0 compatible for all other features.

Virtualization software support

FortiAuthenticator 8.0.4 supports:

Microsoft Hyper-V 2010, Hyper-V 2016, Hyper-V 2019, and Hyper-V 2022
Alibaba Cloud
AWS (Amazon Web Services)
GCP (Google Cloud Platform)
Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
Microsoft Azure
Nutanix
Oracle OCI
Proxmox

Saudi Cloud Computing Company (SCCC) and alibabacloud.sa domain (a standalone cloud backed by AliCloud)
VMware ESXi / ESX 6/7/8
Xen Virtual Machine (for Xen HVM)



Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See [FortiAuthenticator-VM on page 27](#) for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

RADIUS Challenge Response	Requires support by third party vendor
Token Passcode Appended	Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client/network access server (NAS).

FortiAuthenticator-VM

For information about FortiAuthenticator-VM deployments and system requirements, see the VM installation guide on the [Fortinet Docs Library](#).

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release.

For inquiries about a particular bug, please contact Technical Support within the [FortiCare portal](#).

Bug ID	Description
953185	Unable to configure (-) in the certificate ID field.
973414	Downloading large Summary Debug Report from GUI leads to Gateway Timeout Error.
1107132	Support Alcatel-ESAM RADIUS dictionary.
1135456	FTM self-provisioning portal page is shown as blank for some users.
1186398	Lost AES support in SCEP (due to MS incompatibility).
1198353	SCEP with aes-256-cbc fails with decryption.
1198648	Remote RADIUS user password change fails from self-service-portal/admin-portal.
1199749	LDAP user password change through RADIUS/User Portals does not work on Windows Server 2025 Domain Controller.
1212035	Automatic CRL download does not verify validity period.
1223664	Cross-Origin-Opener-Policy: same-origin breaks OIDC compatibility with vault.
1224319	Filter for 'All' certificates button does not display revoked certificates.
1229686	Changing default static route causes HA LB to stop synchronizing.
1232308	Unable to change admin password through CLI on Azure VM Marketplace instance with SSH Key.
1232741	If CRL is expired, EAP-TLS still uses it to check client certificate instead of reject the client certificate.
1232772	SubjectAltName has all values in one line separated by comma.
1234168	Changes to remote LDAP sync rule settings while the rule is running may be overwritten.
1235550	Change OIDC discovery endpoint to standard path.
1236866	Incorrect/misleading error message when trying to import remote SAML users with misconfigured SAML server settings.
1237340	FortiAuthenticator should reject connecting to secure syslog server missing id-kp-serverAuth (1.3.6.1.5.5.7.3.1) in its certificate.

Bug ID	Description
1238176	Certificate issuer is blank on remote SAML server and SAML Service Providers page.
1238274	SCIM getting 400 errors when trying to add user on Palo Alto Prisma (SCIM SP).
1244205	FortiAuthenticator not returning the Access-Control-Allow-Origin header in HTTP responses.
1244672	500 Internal Server Error if injecting very long parameter value into the password reset page.
1245914	Custom Vendors RADIUS Dictionaries not syncing to LB node.
1247171	SAML IdP User source setting 'search local users first' has no effect for SAML realms (IdP proxy).
1252254	SCEP fails to sign FortiGate CSR when subject includes a serial number.
1257765	TACACS+ service may fail to restart after configuration changes.
1257974	Logging to FortiAnalyzer Cloud fails due to missing SNI.
1259508	Stale legacy self-service portal settings left behind after upgrade from 6.x.
1259634	Synchronization with Entra ID SAML takes too long.
1260534	500 error when trying to reset the admin password via email.
1261769	Relax redirect URI scheme validation constraints for Relying Parties.
1262280	Error during captive portal user registration under high load.
1264703	FSSO randomly stops performing group lookups for SSOMA on native Entra ID-joined workstations.
1265223	Self-service password reset does not work if using hardware FortiTokens.
1265879	IdP Proxy: Local authorization groups not included in assertion.
1266052	Local Users GUI page should show the count of local user accounts only.
1266463	Importing users from LDAP server by group membership shows stale user accounts info.
1267154	500 error when trying to revoke user certificate.
1270122	api/v2/samlidpusersources- Improve descriptions and validation.
1271131	REST API v2 should accept URLs with or without a trailing slash.
1271803	Unable to sync more than 500 users using a Google SAML server.
1272491	Certificate policies are not displayed correctly when viewing certificate details.
1272893	FortiAuthenticator 500 internal server error when uploading CSR.
1273564	Smart Connect EAP-TLS Profile fails to install on macOS.

Bug ID	Description
1274773	Re-importing a certificate using <code>/api/v2/servicecerts/import</code> fails silently.
1275165	RADIUS sessions sort option does not sort.
1275356	Adding local user with LDAP auto-provisioning fails when LDAP service directory tree contains large number of users.
1275478	Unnecessary geoip update attempts generate noise in the logs.
1275900	FortiAuthenticator IP lockout exemption for <code>0.0.0.0/32</code> not working leading to global WiFi authentication lockouts.
1276336	Customer wants to use UPN on their FSSO setup, but FortiAuthenticator fails to search LDAP, thus no FSSO logons are shown.
1276949	FortiAuthenticator exposes challenge password in SCEP debug logs.
1277309	<code>/api/v2/servicecerts-</code> Unable to delete a certificate with ID of 2 or 3.
1277386	Inoffensive but worrisome runtime warnings in radsecproxy debug logs.
1277504	Internal Server Error: <code>/api/v1/oauth/logout/</code> .
1278857	403 Forbidden error when trying to change password from self-service portal if the admin UI access is disabled.
1279225	REST API authentication uses case-sensitive check of username.
1280318	Rare deadlock between HA replication and web server processes.
1280983	The GUI error message shows a float instead of an integer (days) of validity period when allowing SCEP renewal before expiry is enabled.
1281867	PSU shows Voltage Input Fault at 241V. Acceptable range is too strict
1282471	Getting error when trying to lock, disable, or re-enable a guest user.
1282907	Typo in REST API response to create new user: 'status' is misspelled 'statue.'
1283157	FortiAuthenticator-300G - Support displaying single power supply in web GUI HW monitor.
1284484	SAML user sync does not clean up the lock file on exception.
1284756	Delivery options on the captive portal are not working.
1286236	FTM assigned via self-service portal in 'Assigned' state even if provisioning is never completed.
1287775	New hardware models supported: FortiAuthenticator 300G and 800G.
1288770	Intermittent GUI and SAML authentication failures due to <code>/tmp/sessions</code> file leakage.
1288905	Error when importing learned RADIUS users.

Bug ID	Description
1290269	Default VM templates do not require enough memory (2GB instead of 16GB).
1290959	Self-service portal resets when user tries to reset password using 2FA.
1290967	SAML authentication fails when SAML request does not include X509Certificate.
1292583	REST API responses with config object relative URI references are missing trailing slash.
1293385	[NFR] REST API: Admin password changes.
1293743	Reduce OAuth Authorization Code Maximum Lifetime.
1294042	OIDC JWT token omitting filter-based LDAP group when user object is nested in a deep OU.
1294138	Read only admins should not be able to do ftp/tftp transfers.
1294191	CLI is displaying incorrect bonded interface information.
1294353	FTM in pending state even if failed to send activation message.
1294802	'Response Timeout' setting for FortiAuthenticator as LDAP client applies to TCP connect, but not to LDAP search query.
1296087	REST API PATCH method on localapiadmin clears some attributes.
1296871	User license usage exceeds actual user count on FortiAuthenticator after upgrade from 6.6.2 to 8.0.3.
1298023	Sending system logs to remote syslog server through TLS may cause FortiAuthenticator to hang/stall if the server is unavailable.
1298249	RADIUS authentication not responding after HA cluster failover.
1298280	Response from creating single local user via REST API is not backward-compatible with earlier releases.
1298845	FortiAuthenticator OWA agent allows web mail login without 2FA for some users having same username as another user.
1300742	Generate system log event when an localapiadmin password is changed.
1301661	500 error when assigning FTM if email template includes reference to a missing image.
1304595	IPv6 addresses mishandled by adaptive MFA rules.
1304822	api/v2- Admin with certificate management write permission cannot update.
1305246	FortiToken prompt displays the domain name(realm) twice when Azure Entra ID is configured as proxy.
1305684	FortiToken Mobile transfer does not work.
1306166	Smart Connect not working with Android devices if EAP server certificate CA is different from the end-user certificates' CA.

Bug ID	Description
1306356	"LDAP directory group" and "LDAP filter (advanced)" fails with error "fac_auth_facgroup" violates not-null constraint"
1306972	Some ports are missing in Hardware models.
1307157	ACME certificate renewal fails due to EC curve error.
1307168	Slow SAML IdP login with large number of local users.
1307172	Unable to add certificate for 'SAML request must be signed by SP' when subject and/or issuer contains trailing whitespace.
1307780	'Understanding the captive portal workflow' button is broken.
1308242	LB HA: YubiKey/HOTP token counters not updated and synced back to primary after login on LB node.
1308947	Remote auth server SAML logout failing with Microsoft Entra ID.
1309022	Usage Information section of individual user edit pages only shows first active session found, not the sum of all.
1310756	Error 500 when trying to use Smart Connect Windows/Android app that does not support ECC certificates.
1311493	500 error in FortiAuthenticator IdP proxy after successful authentication if FortiAuthenticator detects errors in assertions of external IdP response.
1311601	Unsigned SAML logout requests sent to remote SAML servers.
1312107	Local user CSV export API cannot filter on username.
1313551	SCIM created groups with hyphens cannot be edited.
1314264	Unable to restore admin access when interface is bonded.
1314270	403 error in admin GUI after breaking bond interface.
1315238	Restore the automatic 'Get trial FTM tokens' logic for both FortiAuthenticator Cloud and unlicensed VMs.
1315401	50 entry hard code limit on SAML assertion attributes proxied from remote SAML server to SP.
1315717	FortiAuthenticator-VM in Azure may lose configuration upon reboot on instance sizes that include 'temporary storage disks' unless 16GB.
1315738	Disallow subject DN of issuer == subject DN of a cert when creating server cert/user cert in FortiAuthenticator.
1316311	HTTP 500 Error occurs when SAML request signing uses ECC certificate in the IdP proxy.
1316499	No FortiAuthenticator AMI exists in AWS ca-west-1 marketplace.
1316887	Performance improvement for AD authentication.

Bug ID	Description
1316899	Deadlock detected when inserting OU under LDAP directory tree.
1316901	SAML IdP response signing fails when an ECC certificate is selected as the server certificate.
1319427	Importing unsupported custom RADIUS dictionary leads to admin UI lockout.
1319598	FDN/FortiGuard SSL communication failure on FortiAuthenticator 300G and FortiAuthenticator 800G models; unable to register trial tokens.
1319844	500 Internal Server Error after upgrading to 6.6.10.
1319969	Internal Server error while creating RootCA with the 'Use nethSM server' option enabled.
1320189	/api/v2/remotesamlservers permissions cannot be controlled by Admin Profiles.
1320567	openid scope must be rejected for password-based OAuth token requests.
1322562	High SAML requests cause the database to run out of connections and become non-responsive.
1322845	Intermediate root CA fails when exporting PKCS12 with error Cannot export PKCS#12 certificate.
1326019	api/v2- name__in query parameter does not work.
1326485	SAML excludes LDAP custom attributes when 'Secure Connection' is enabled.
1327926	Realm attribute is not returned from user info endpoint.
1330473	Possible SCIM client race condition when moving user between groups.
1331223	Improve OIDC discovery metadata.
1332243	Request ID (X-Request-ID) present in FortiAuthenticator logs is not propagated to FortiAnalyzer logs.
1338048	Secure connections to Azure SMTP server are denied.
1340846	SCIM user update from Entra ID do not work when username contains uppercase letters.
1344950	Cisco ASA (AnyConnect SSL VPN) client radius authentication is failing against FortiAuthenticator (missing authenticator attribute).
1352143	SCIM maximum groups sync limit per RP from 128 to 256.

The following issues were introduced during 8.0.4 development and were not present in 8.0.3 GA; they affected only systems that had upgraded to 8.0.4 build 0187 and are resolved in this release.

Bug ID	Description
1313622	Admin Profiles require at least one permission in custom permission sets.
1331705	Checkbox/toggle labels not toggling the control on clicking the Neutrino pages.

Bug ID	Description
1346481	AWS FortiAuthenticator upgrade resets the 'admin' account password to the instance ID.
1353513	RADIUS client IP range migration fix.
1353607	Fix UI components missing in system access.
1353964	User cannot login using username@fortinet.com for FIDO enabled SAML entries.
1353977	SAML SP with password and FIDO does not work, but works with FIDO-only.
1354789	500 error when searching for locked out user.
1356716	Unable to download IDP metadata from metadata URL.

Known issues

This section lists the known issues of this release, but is not a complete list.

For inquiries about a particular bug, please contact Technical Support within the [FortiCare portal](#).

Bug ID	Description
971708	Avoid using the default 'admin' account in AWS since restoring config resets its password to instance-id.
997200	SAML IdP proxy not able to retrieve group memberships from remote OpenLDAP server.
1026106	Failed to add new FIDO key in Chrome with Bitwarden extension.
1139476	Gateway Timeout when loading local users page with a large number of users.
1140601	CLI logins attempts that fail without a successful follow-up are not being logged.
1143190	Self-service portal shows empty page when all the post-login options are disabled.
1144845	FortiAuthenticator should not present SAML captcha when performing proxy authentication.
1145628	SAML IdP FIDO authentication fails on first try after FortiClient disconnect/reconnect.
1180386	Permanent IP based lockout cannot be unlocked in the GUI.
1187237	Add support to modify debugging level for LB sync daemon from admin UI.
1189168	Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboot.
1196760	Failed to restore configuration just after factory reset due to Database restore failed:.
1196880	Mismatched cert/key in the LB secondary.
1201488	GUI cannot show the imported image as previous release.
1203907	Guest portal not showing correct message when user or source IP address is locked out.
1203911	FortiAuthenticator should record a log when a guest portal is created/edited/deleted.
1203923	Guest portal creation should not be allowed without a default language.
1204521	Zero-Trust Tunnel continues working even after server certificate is revoked.
1236990	In FortiAuthenticator Cloud, pre-configured 'FortiTrust Identity' SMS gateway settings are read-write.

Bug ID	Description
1237187	SCEP requests fail to complete; getCA request fails when using ECC CA certificate.
1237759	Fiber network interface (port5) gets into a flapping state after an indeterminate period of normal function.
1250768	Getting an encoding failed error when the FortiGate sends a CSR over SCEP using an ECC key type.
1253985	Server groups on user source page should match the selected server.
1256620	Confusing success message after saving the guest portal label in the admin UI.
1257979	No log when deleting local user through the REST API.
1260519	Unable to view HTML tags in Replacement Messages using the Google Chrome browser.
1263898	FSSO cannot poll event logs from Windows Server 2025.
1287827	Certificate Management page is missing the setting to delete the user certificate private key once downloaded.
1292993	Factory reset causes software RAID to fail on FortiAuthenticator-300F.
1321131	Smart Connect certificate installation error on Windows 11 without wireless adapter.
1338283	Token delivery option always shows 'Default' for Fortiidentity Cloud selection, even when other options are selected.
1346442	Read-only admin gets 403 forbidden error when loading <i>Authentication > Guest Portals (beta) > Portal Rules</i> page.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, for FortiAuthenticator-300F, the maximum number of auth clients (RADIUS and TACACS+) that can authenticate to the system is:

$$1500 / 3 = 500$$

Where this relative system is not used, e.g., for static routes, the **Calculating metric** is denoted by **N/A**.



Similar to the FortiAuthenticator-VM, when user license upgrades are applied, the corresponding metrics increase proportionally.

For example, a FortiAuthenticator-300F with a base license supports 1500 users, which allows $1500 / 5 = 300$ user groups.

If the customer upgrades the FortiAuthenticator-300F to the maximum of 3500 users, the number of user groups becomes $3500 / 5 = 700$.



Similar to the FortiAuthenticator-VM, the FortiAuthenticator hardware appliances permit stacking licenses.



The maximum values in this document are the maximum configurable values and are not a commitment of performance.

System > Network

Feature	Calculating metric	300F	300G	800F	800G	3000F
Static Routes	N/A	50	50	50	50	50

System > Messages

Feature	Calculating metric	300F	300G	800F	800G	3000F
SMTP Servers	N/A	20	20	20	20	20

Feature	Calculating metric	300F	300G	800F	800G	3000F
SMS Gateways	N/A	20	20	20	20	20
SNMP Hosts	N/A	20	20	20	20	20

System > Administration

Feature	Calculating metric	300F	300G	800F	800G	3000F
Syslog Servers	N/A	20	20	20	20	20
User Uploaded Images	N/A	79	79	404	404	2004
Language Files	N/A	50	50	50	50	50

Realms

Feature	Calculating metric	300F	300G	800F	800G	3000F
Realms	Users / 25	60	60	320	320	1600

Authentication > General

Feature	Calculating metric	300F	300G	800F	800G	3000F
Auth Clients (RADIUS and TACACS+)	Users / 3	500	500	2666	2666	13333
Users (Local+ Remote)	N/A	1500 (minimum)/ 3500 (maximum)	1500 (minimum)/ 3500 (maximum)	8000 (minimum)/ 18000 (maximum)	8000 (minimum)/ 18000 (maximum)	40000 (minimum)/ 140000 (maximum)
User RADIUS Attributes	Users x 3	4500	4500	24000	24000	120000
User Groups	Users / 5	300	300	1600	1600	8000

Feature	Calculating metric	300F	300G	800F	800G	3000F
Group RADIUS Attributes	Users groups x 3	900	900	4800	4800	24000
User Certificate Bindings	Users x 2	3000	3000	16000	16000	80000
FortiTokens	Users x 2	3000	3000	16000	16000	80000
LDAP Entries	Users x 2	3000	3000	16000	16000	80000
Device (MAC based Auth.)	Users x 5	7500	7500	40000	4000	200000
RADIUS Client Profiles	N/A	1500	1500	8000	8000	40000
Remote LDAP Users Sync Rule	Users / 10	150	150	800	800	4000
Remote LDAP User Radius Attributes	Users x 3	4500	4500	24000	24000	120000



The FortiAuthenticator Advance/Carrier license (FC-10-ACTCR-1343-02-DD) removes the *Auth Clients (RADIUS and TACACS+)* limit shown above, providing unlimited RADIUS and TACACS+ clients for FortiAuthenticator-VM and FortiAuthenticator 3000F/G hardware models.

Remote authentication servers

Feature	Calculating metric	300F	300G	800F	800G	3000F
Remote LDAP Servers	Users / 25	60	60	320	320	1600
Remote RADIUS Servers	Users / 25	60	60	320	320	1600
Remote SAML Servers	Users / 25	60	60	320	320	1600
Remote OAuth Servers	Users / 25	60	60	320	320	1600
Remote TACACS+ Servers	Users / 25	60	60	320	320	1600

FSSO & Dynamic Policies

Feature	Calculating metric	300F	300G	800F	800G	3000F
FSSO Users	Users	1500	1500	8000	8000	40000
FSSO Groups	Users / 2	750	750	4000	4000	20000
Domain Controllers	Users / 100	15	15	80	80	400
RADIUS Accounting SSO Clients	Users / 3	500	500	2666	26666	13333
FortiGate Group Filtering	Users / 2	750	750	4000	4000	20000
FSSO Tier Nodes	Users / 100	15	15	80	80	400
IP Filtering Rules	Users / 2	750	750	4000	4000	20000

Accounting Proxy

Feature	Calculating metric	300F	300G	800F	800G	3000F
Sources	Users	1500	1500	8000	8000	40000
Destinations	Users / 20	75	75	400	400	2000
Rulesets	Users / 20	75	75	400	400	2000

Certificates > User Certificates

Feature	Calculating metric	300F	300G	800F	800G	3000F
User Certificates	Users x 5	7500	7500	40000	40000	200000
Server Certificates	Users / 10	150	150	800	800	4000

Certificates > Certificate Authorities

Feature	Calculating metric	300F	300G	800F	800G	3000F
CA Certificates	N/A	10	10	50	50	50
Trusted CA Certificates	N/A	200	200	200	200	200
Certificate Revocation Lists	N/A	200	200	200	200	200

Certificates > SCEP

Feature	Calculating metric	300F	300G	800F	800G	3000F
Enrollment Requests	Users x 5	7500	7500	40000	40000	200000

Certificates > CMP

Feature	Calculating metric	300F	300G	800F	800G	3000F
Enrollment Requests	Users x 5	7500	7500	40000	4000	200000

Services

Feature	Calculating metric	300F	300G	800F	800G	3000F
FortiGate Services	Users / 10	150	150	800	800	4000
TACACS+ Services	Users / 10	150	150	800	800	4000

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

 The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of auth clients (RADIUS and TACACS+) that can authenticate to the system is:

$$100 / 3 = 33$$

Where this relative system is not used, e.g., for static routes, the **Calculating metric** is denoted by a "-".

The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

System > Network

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Static Routes	2	50	50	50

System > Messages

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
SMTP Servers	2	20	20	20
SMS Gateways	2	20	20	20
SNMP Hosts	2	20	20	20

System > Administration

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Syslog Servers	2	20	20	20
User Uploaded Images	19	Users / 20	19 (minimum)	250
Language Files	5	50	50	50

Authentication > General

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Auth Clients (RADIUS and TACACS+)	3	Users / 3	33	1666
Authentication Policy (RADIUS and TACACS+)	6	Users	100	5000



The FortiAuthenticator Advance/Carrier license (FC-10-ACTCR-1343-02-DD) removes the *Auth Clients (RADIUS and TACACS+)* limit shown above, providing unlimited RADIUS and TACACS+ clients for FortiAuthenticator-VM and FortiAuthenticator 3000F/G hardware models.

Remote authentication servers

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Remote LDAP Servers	4	Users / 25	4	200

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Remote RADIUS Servers	1	Users / 25	4	200
Remote SAML Servers	1	Users / 25	4	200
Remote OAuth Servers	1	Users / 25	4	200
Remote TACACS+ Servers	1	Users / 25	4	200

User Management

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Users (Local + Remote) ¹	5	*****	100	5000
User RADIUS Attributes	15	Users x 3	300	15000
User Groups	3	Users / 5	20	1000
Group RADIUS Attributes	9	User groups x 3	30	1500
User Certificate Bindings	10	Users x 2	200	10000
FortiTokens	10	Users x 2	200	10000
FortiToken Mobile Licenses (Stacked) ²	3	200	200	200
LDAP Entries	20	Users x 2	200	10000
Device (MAC-based Auth.)	5	Users x 5	500	25000
Remote LDAP Users Sync Rule	1	Users / 10	10	500

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Remote LDAP User Radius Attributes	15	Users x 3	300	15000
Realms	2	Users / 25	4	200

FSSO & Dynamic Policies > FSSO

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO Users	5	Users	100	5000
FSSO Groups	3	Users / 2	50	2500
Domain Controllers	3	Users / 100 (min=10)	10	50
RADIUS Accounting SSO Clients	10	Users	100	5000
FortiGate Group Filtering	30	Users / 2	50	2500
FSSO Tier Nodes	3	Users / 100 (min=5)	5	50
IP Filtering Rules	30	Users / 2	50	2500
FSSO Filtering Object	30	Users x 2	200	10000

FSSO & Dynamic Policies > Accounting Proxy

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Sources	3	Users	100	5000
Destinations	3	Users / 20	5	250
Rulesets	3	Users / 20	5	250

Certificates > User Certificates

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
User Certificates	5	Users x 5	500	25000
Server Certificates	2	Users / 10	10	500

Certificates > Certificate Authorities

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
CA Certificates	3	Users / 20	5	250
Trusted CA Certificates	5	200	200	200
Certificate Revocation Lists	5	200	200	200

Certificates > SCEP

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Enrollment Requests	5	Users x 5	500	25000

Certificates > CMP

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Enrollment Requests	5	Users x 5	500	25000

Services

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FortiGate Services	2	Users / 10	10	500
TACACS+ Services	5	Users / 10	10	500

¹ Users includes both local and remote users.

² **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

Data-at-rest protection

FortiAuthenticator protects data-at-rest in the following ways:

- Data secrets for which FortiAuthenticator needs access to the plaintext for operations are encrypted with AES256-CBC with a random initialization vector (IV) and a key-encryption key (KEK).
- Data secrets for which access to the hashed is sufficient for operations are encrypted using SHA256 with a random salt.
- Symmetric encryption keys are used for debug logs and config files.
- The FortiAuthenticator file system is encrypted.



www.fortinet.com

Copyright© 2026 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.