Release Notes

FortiAuthenticator 8.0.0

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

February 2, 2026
FortiAuthenticator 8.0.0 Release Notes
23-800-1179257-20260202

TABLE OF CONTENTS

Change log

Date	Change Description
2025-10-02	Initial release.
2025-10-06	Updated Hardware and VM support on page 17 and Maximum values for hardware appliances on page 34.
2025-10-17	Updated Maximum values for hardware appliances on page 34.
2025-10-27	Updated What's new on page 9.
2025-11-04	Updated Maximum values for hardware appliances on page 34.
2025-12-12	Added Common Vulnerabilities and Exposures on page 30.
2026-02-02	Updated What's new on page 9.

FortiAuthenticator 8.0.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 8.0.0, build 0031.

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

What's new

FortiAuthenticator version 8.0.0 includes the following enhancements:

Allow multiple user certificate and key export

The **Certificate Expiry** tab in **Certificate Management > Policies** has been renamed to **General**.

A new **Delete user certificate's private key once downloaded** option is available in the **General** tab that controls if a user certificate private key is deleted after being downloaded from the admin UI.

SCEP with Microsoft InTune and EAP-TLS with Entra ID users/groups

FortiAuthenticator offers the following new settings to support integration with MS InTune client certificates distribution and EAP-TLS RADIUS authentication with Entra ID users/groups:

- A new **InTune** option in **Challenge Password > Password generation** when creating/editing a certificate enrollment request in **Certificate Management > SCEP > Enrollment Requests**.
- The **Azure AD tenant ID** field is no more dependent on the **Include for SSO** option when creating/editing a remote OAuth server in **Authentication > Remote Auth. Servers > OAuth**.
- A new **Certificate Bindings** pane available that allows you to configure certificate bindings when creating/editing a remote SAML user in **Authentication > User Management > Remote Users**.
- A new **RADIUS Attributes** pane available that allows you to configure RADIUS attributes when creating/editing a SAML user group in **Authentication > User Management > User Groups**.
- The **Realms** table can now include SAML realms and remote SAML group filters when configuring a RADIUS policy in **Authentication > RADIUS Service > Policies**.

FIDO authentication for IdP initiated SAML

The general SAML IdP settings page in **Authentication > SAML IdP > General** now offers the ability to specify the required authentication method for IdP initiated logins in the new **IdP Initiated Login** pane.

REST API enhancements for local users management

A new `users` field in the `/localusers/` endpoint that displays the list of users.

The following new allowed methods available for the `/localusers/` endpoint:

Method	Endpoint	Description
`POST`	`/api/v1/localusers/`	Create multiple new local users
`DELETE`	`/api/v1/localusers/`	Delete multiple local users

The following new allowed filtering available for the `/localusers/` endpoint:

- `custom1`
- `custom2`
- `custom3`

The following new allowed filtering available for the `/csv/localusers/` endpoint:

- `username`
- `abridged`
- `custom1`
- `custom2`
- `custom3`

See the latest *FortiAuthenticator REST API Guide*.

REST API enhancements: Track end-user operations

A new `X-Request-ID` header for request tracking and correlation across distributed systems to trace logs and debug issues.

HTTP Header	Type	Required	Other Restrictions
`X-Request-ID`	string	No	ASCII alphanumeric, dash (`-`), and underscore (_) only. Maximum length = 64 characters.

The `X-Request-ID` header is supported for all the read/write operations (`GET`, `POST`, `PUT`, `PATCH`, `DELETE`) for the following endpoints:

- `/localusers/`
- `/ldapusers/`

- `/iamaccounts/`
- `/iamusers/`
- `/fortitokens/`
- `/usergroups/`
- `/localgroup-memberships/`

Usage `Example`

cURL Example

```
curl -k -X GET \
 https://[FAC_IP]/api/v1/localusers/ \
 -H 'Content-Type: application/json' \
 -H 'X-Request-ID: request_12345' \
 -u "admin:[api_key]"
```

Sample Response

```
{
  "meta": {
  "request_id": "request_12345"
},
"objects": [
  {
    "username": "john.doe",
    "email": "john.doe@example.com"
  }
 ]
}
```

See the latest *FortiAuthenticator REST API Guide*.

In the FortiAuthenticator 8.0.0 GUI, a new *Request ID* column in *Logging > Log Access > Logs*.

It contains the value of the `X-Request-ID` header in the logs associated with the REST API operations for the supported endpoints.

Support for subscription VM license

FortiAuthenticator-VM now accepts subscription based licenses.

The following new CLI commands have been introduced:

- `get system license-info`: Displays the license information
- `diagnose system updated status`: Displays license information fetched from FDN
- `diagnose system updated info`: Displays the updated runtime information
- `diagnose debug application updated <level>`: Set debug level for updated

Once the license expires, all the authentication stops.

The administrator can still access the GUI for configuration and troubleshooting.

The subscription license requires FortiAuthenticator version 8.0.0 or above.

Override option in A/P HA

A new **Priority override** option when editing high availability settings in **System > Administration > High Availability**.

The **Priority override** option allows you to select from the following:

- **Favor healthy high priority node**: If the low priority node is active, failover to the high priority node whenever it becomes available.
- **Minimize HA failovers**: If the low priority node is active, do not failover to the high priority node until the low priority node becomes unavailable.

SmartConnect/EAP-TLS: Enforce client certificate install on unique endpoint

In FortiAuthenticator 8.0.0, when configuring a Smart Connect profile for EAP-TLS connections with the **Authentication** as **WPA2 Enterprise** in **Authentication > Portals > Smart Connect Profiles**, a new **Client certificate CN** dropdown indicates which user account attribute to use as the CN value in the client certificate (previously, hardcoded to `username`).

The **Client certificate CN** dropdown also offers a new **MAC Device** option.

Similarly, when configuring a Smart Connect profile with the **Connect type** as **Certificate**, the **Client certificate CN** dropdown is available.

When configuring an EAP-TLS RADIUS policy in **Authentication > RADIUS Service > Policies**, a new **Verify MAC address in CN of client certificate** (default = disabled) setting under **Device authorization** in the **Authentication factors** tab is available.

When enabled, the endpoint MAC address sent by the RADIUS client must match the `CN` in the subject field of the client certificate.

When configuring a portal in **Authentication > Portals > Portals**, **Device Tracking and Management** has been replaced with a new **Devices** option that includes the following:

- **Tracking and Management**
- **Tracking-only**

- **Management-only**

When device tracking is used, the end-user with successful log in to the captive portal with a new MAC device is asked to register the device (when under the maximum number of allowed MAC devices).

When device management is used and the end-user successfully logs in to the captive portal with a new MAC device in excess of the maximum number of devices per user, the end-user is asked if they will replace an existing device.

When device management is disabled and the end-user successfully logs in to the captive portal with a new MAC device, the access is denied since an existing device cannot be replaced.

In the post login portal:

- The **Devices** menu is only visible when device management is enabled.
- If `"Client certificate CN"=="MAC Device"`, the end-user is given a dropdown to select which device to use.
- If no MAC devices have been registered to the logged-in user account, e.g., device tracking is disabled, the Smart Connect menu shows an error message.

SAML IdP: Custom multi-value SAML attributes

FortiAuthenticator 8.0.0 now supports custom SAML assertion attributes in the SAML response sent to SPs.

A new **SAML Assertion Attributes** pane available when configuring a user group in **Authentication > User Management > User Groups**.

The following events are now logged:

- System logs: Add/edit/delete custom SAML assertion attributes in user groups.
- GUI debug logs: Information about the user groups used to build the list of custom SAML assertion attributes for the SAML response.

SAML IdP: Per SAML SP authorization

The remote LDAP group filters now offer a new **Subtype** setting (previously labeled **User retrieval**) in **Authentication > User Management > User Groups**.

The **Subtype** setting offers the following three options:

- **LDAP directory group**: Maps to a group object at the specified Distinguished Name in the remote LDAP directory.
- **List of users**
- **LDAP filter (advanced)** (default): Queries the remote LDAP server with a custom filter that returns the list of member users.

Selecting **Set Group Filter** imports the **Distinguished name** of the selected LDAP group only.

A new tooltip is available when the **User attribute** is **Group** while adding an **Assertion attribute**.

A new SAML IdP replacement message for SP authorization failure (**SAML IdP Unauthorized SP Page**).

The **Filter By Group** column has been renamed to **Global Authorization** in **Authentication > SAML IdP > User Sources**.

The IdP initiated portal now hides any SP for which the logged in user is unauthorized based on the SP group filters.

The following events are now logged:

- Add/edit/delete SP group filter.
- SP access is denied due to failed SP group filter authorization.

FortiAuthenticator- FortiGuest integration

Starting FortiAuthenticator 8.0.0, FortiGuest features are available from within FortiAuthenticator.

A new **Guest Portals (beta)** menu available in **Authentication** that offers FortiGuest configuration in FortiAuthenticator.

The following three tabs are available in **Guest Portals (beta)**:

- **Portals**: Allow administrators to create their portal pages and host them on FortiAuthenticator.
- **Portals Rules**: Create a set of rules to allow user access to different portals that have been created.
- **Guest Themes**: Create guest portal themes as per your business requirement.

Note: This is a beta feature.

Limitations:

- Only supports login for local users
- Configuration backup/restore does not preserve all the customizations
- HA A-P and HA A-A are not supported
- Only administrators with full permissions can access the configuration

Legacy self-service portal retired

Starting FortiAuthenticator 8.0.0, the **Legacy Self-service Portal** available in **Authentication** has been removed.

⚠ The administrator must now log in with their username only, i.e., `username + realm` is no longer accepted.

Also, the previously available **Legacy Self-Service Portal Settings** pane in **System > Administration > System Access** has been removed.

New CLI command for EAP

Starting FortiAuthenticator 8.0.0, a new `diagnose authentication radius-eap-ecdh-curve` CLI command has been added.

Use the CLI command to override the default `ECDH_CURVE` for EAP.

default = `secp521r1:secp384r1:prime256v1`

New CRL check mode for remote LDAP servers

Starting FortiAuthenticator 8.0.0, a new **CRL Check Mode** setting is available in the **Secure Connection** pane when configuring a remote LDAP server in **Authentication > Remote Auth. Servers > LDAP**.

New Exclude Windows AD computer accounts from SSO option in FSSO

Starting FortiAuthenticator 8.0.0, a new **Exclude Windows AD computer accounts from SSO** option is available in **Fortinet SSO > Settings > Methods**.

When **Exclude Windows AD computer accounts from SSO** is enabled, FortiAuthenticator does an AD lookup to determine whether an account ending with `$` is a computer or a user, and excludes it from FSSO if it is a computer.

New debug log categories for Web Server

In FortiAuthenticator 8.0.0, the following new debug categories are now available for **Web Server**:

- **SAML**
- **Generic API**

New OTP-Only Push notification setting in User Account Policies

Starting FortiAuthenticator 8.0.0, a new **OTP-Only Push notification mode** setting is available when configuring user account policies in **Authentication > User Account Policies > General**.

RADSec support enhancements

FortiAuthenticator RADIUS server can now process RADIUS accounting requests being sent over RADSec from RADIUS clients.

Furthermore, the RADIUS server now verifies that RADSec clients provide a certificate issued by one of the configured **Local CAs** or **Trusted CAs** under **Certificate Management > Certificate Authorities** during their TLS connection handshake.

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 8.0.0 requires at least 4 GB of RAM.

When FortiAuthenticator 8.0.0 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 8.0.0 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

FortiAuthenticator 8.0.0 supports:

- FortiAuthenticator 300F
- FortiAuthenticator 800F
- FortiAuthenticator 3000F
- FortiAuthenticator VM
  See Virtualization software support on page 22.

Image checksums

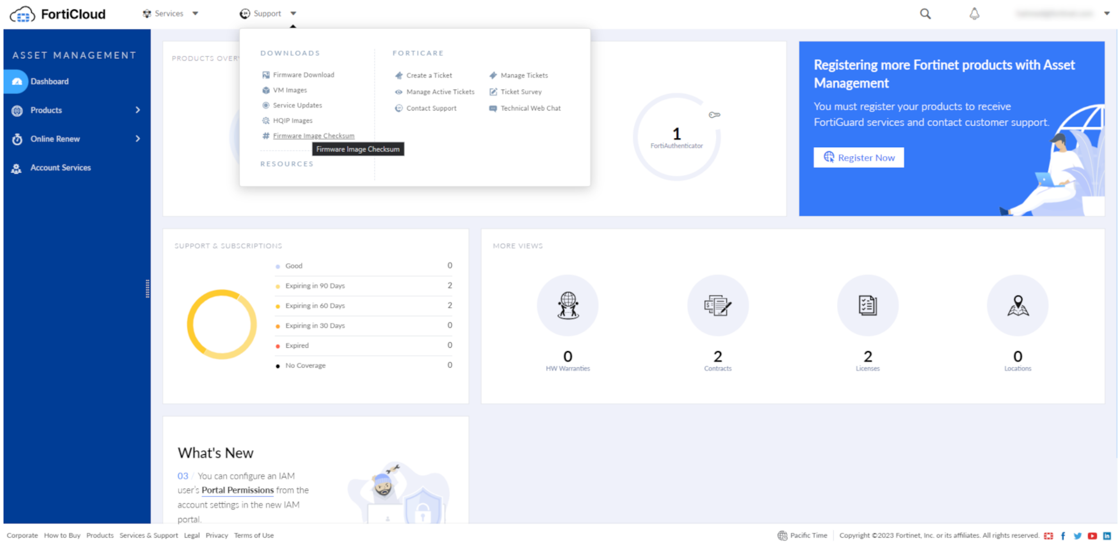
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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.



Registering more Fortinet products with Asset Management

You must register your products to receive FortiGuard services and contact customer support.

Good	0
Expiring in 90 Days	2
Expiring in 60 Days	2
Expiring in 30 Days	0
Expired	0
No Coverage	0

What's New

03 / You can configure an IAM user's Portal Permissions from the account settings in the new IAM portal.

Copyright ©2023 Fortinet, Inc. or its affiliates. All rights reserved.

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

FortiAuthenticator 8.0.0 build 0031 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 8.0.0, 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 8.0.0 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 8.0.0.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 8.0.0 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 8.0.0 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 20.

⚠ Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

⚠ Ensure the hypervisor provides at least 4 GB of memory to the FortiAuthenticator-VM.

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 8.0.0, 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 8.0.0

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 **initd** 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 21
- FortiOS support on page 21
- Fortinet agent support on page 21
- Virtualization software support on page 22
- Third-party RADIUS authentication on page 22

Web browser support

The following web browsers are supported by FortiAuthenticator 8.0.0:

- Microsoft Edge version 140
- Mozilla Firefox version 143
- Google Chrome version 141

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

FortiOS support

FortiAuthenticator 8.0.0 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 8.0.0 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 *Agents Compatibility Matrix* on the Fortinet Docs Library.

  Note that the FortiAuthenticator Agents for Microsoft Windows and OWA download files are now available in the `FortiTrustID_Agents` folder in *Support > Firmware Download* 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.

Note: 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 8.0.0 supports:

- VMware ESXi / ESX 6/7/8
- Microsoft Hyper-V 2010, Hyper-V 2016, Hyper-V 2019, and Hyper-V 2022
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM)
- Nutanix
- AWS (Amazon Web Services)
- Microsoft Azure
- Oracle OCI
- Alibaba Cloud
- Saudi Cloud Computing Company (SCCC) and alibabacloud.sa domain (a standalone cloud backed by AliCloud)
- Proxmox

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 24 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
1156684	Non-fatal `load_license` error message on the console after restoring the configuration.
1010853	Invalid URL link in password reset email when the username contains special UTF8 characters.
1183511	Unable to bypass: `Please correct the error below`.
1195784	Sending Guest user credentials via SMS to mobile phone fails; Test SMS function fails.
1192102	FortiAuthenticator- FortiGuest integration.
1148893	Support 'push' for otp-only authentication policies.
1023816	FSSO sessions are created for local users that are excluded from SSO in Fine-grained Controls.
1183726	Failed tiered FSSO TLS connection due to invalid disk copy of firmware certificate signed by Fortinet CA2 on FortiAuthenticator-3000F.
1147149	FSSO computer accounts override sessions of user accounts ending with `$`.
1193566	If multiple realm point to the same server, push authentication without realm is not working.
1006481	Shorten default FortiToken Mobile activation SMS message.
1195161	HSTS: Increase default max-age and include `includeSubDomains` directive when HSTS enabled.
1178589	Typo in tooltip for Event 4768 in the Event ID selection, showing 6768 instead of 4768.
1171320	Admin UI should not allow selecting an OU in the LDAP tree browser for 'Set Group.'
1200936	500 error occurs when attempting to save the default regex used to validate the email of the authorized endorsers.
1161149	Read-only admin able to read SMS gateway basic authentication password on the GUI.
1098310	Gateway timeout occurs when downloading the configuration backup with a very large number of users.

Bug ID	Description
1157337	Gateway timeout when downloading debug report (summary).
1161147	Read-only admin able to read the Smart Connect pre-shared key.
1048961	Unable to change the user portal policy priority order (403 Forbidden) if the captive portal disabled for all the network interfaces.
1155278	Importing local users using FortiGate configuration file fails.
1149569	Rename 'Trusted subnets' LB HA category to 'Trusted subnets and adaptive MFA rules.'
1179387	Unable to use a certificate with multiple SAN as RADSEC server certificate.
1130853	RADIUS client import via CSV does not support the '.' (dot) character in the RADIUS client name.
932783	FAC-2000E: PSU Monitor Widget doesn't accurately reflect the actual PSU statuses.
1202808	Unable to backup the configuration file for FortiAuthenticator with very large number of users.
1202615	Move test connection button for the SMS gateways list page.
1177229	Unable to change “MAC address parameter' to “client_mac” fallsback to“usermac.”
1159581	User-lookup widget does not show up-to-date 'Active RADIUS Sessions.'
1148138	Easyselect widget on the user pages for selecting FortiToken Mobile tokens loads all the rows in the DB (not partial).
973414	Downloading a large Summary Debug Report from the GUI leads to Gateway Timeout Error.
1189638	Under the LDAP tree adding same local userID is not possible within multiple OUs.
1040493	Unable to modify user and OAuth portal on secondary HA cluster member after failover
1152927	OAuth General setting (User Login session lifetime) does not sync over the LB node when OAuth service is enabled for HA LB sync.
1084364	Optimize heartbeat packets sent in the load-balancing HA mode.
1192926	Cluster not forming with error `PGRES_FATAL_ERROR ERROR: payload string too long`.
1170731	FortiAuthenticator HA cluster forming/routing issues in the OpenStack environment.
1189935	HTTP requests with header length > 4 KB rejected despite configuration allowing larger sizes.

Bug ID	Description
1181816	IP address lockout time reset by unknown user.
1160794	Time-cap full database repair operation initiated by load-balancing sync daemon on startup/admin request from the GUI.
1169005	Need to do CRL check for full certificate chain when doing LDAPS connection to the remote LDAP server.
1157400	ftcd error log improvement.
1134749	Generate a log entry when starting or downloading a packet capture.
1140901	Missing log for 'Failed login attempt not followed by successful login' on RADIUS authentications.
1066439	FortiAuthenticator does not send a `user_ip` field to FortiToken Cloud when user authenticates with a FortiToken Mobile OTP.
1192975	Network interface IP address change does not get applied to the web server until restart.
1183920	500 error in OAuth portal if user tries to do password reset by email when not enabled in the user account.
1194230	OAuth /userinfo endpoint fails if configured to return group memberships in claims.
1177111	OAuth for authorization code grant type fails to complete authentication for some HTTP Content-Type variations.
1203714	OAuth sending double CORS headers.
1179610	Obtaining an OAuth token for a 2FA user with push fails.
1170384	OAuth login not working for some Relying Parties.
1182463	PSU data is missing in 6.6.x branch for FortiAuthenticator 2000E + FortiAuthenticator 3000E.
1198622	OTP challenge is not sent out to the RADIUS client when using chained authentication with EAP-MSCHAPv2.
1144145	RADIUS bypasses MAC filtering and authorization checks for EAP-MSCHAPV2 2FA when FortiToken push is used.
1072845	Accounting requests sent by FortiGate over RADSec are ignored, causing time out on the FortiGate.
1024455	EAP-TLS authentication looks for CN in the client certificate subject even in trusted CAs authentication mode; EAP-TTLS might match incorrect realm.
1150235	SMS OTP not sent for 2FA with the FortiAuthenticator OWA agent.
1091168	Push notifications do not work if using UPN format username in the FortiAuthenticator Window Agent.
1157522	FortiAuthenticator OWA Agent MFA bypass option for users without token not

Bug ID	Description
	working against FortiAuthenticator 6.6.x.
1201150	Signed-out SAML sessions should be cleaned up and no longer appear on the IdP Session Monitor page.
1150763	Remove legacy SAML SP URL.
1142209	PCI DSS SAML portal immediately fails on incorrect passwords if the IP address falls under a trusted subnet.
1192379	Unable to handle SAML assertion request containing validity period that does not match format `%Y-%m-%dT%H:%M:%SZ`.
1195262	SAML IdP fails to verify logout response external signature.
1163222	SAML IdP Proxy is not forwarding back assertions to the SP.
1192781	SCEP requests failing.
1174102	Error when connecting to SCIM server due to missing SNI in the FortiAuthenticator TLS handshake.
1195850	Integration with Zscaler cloud with POST data error code 0.
1037795	FortiToken Mobile provisioning with SMS as activation delivery method results in a 500 error.
1037946	SMS does not replace the replacement message tag `{{:random_id_64}}` with a random 64-character value.
1108535	SNMP becomes unresponsive if the thresholds setting configured with an empty value.
1185280	FortiAuthenticator logs error `User object has no attribute 'remote_radius_id` when syncing LDAP users as the remote RADIUS admin.
1192002	FortiToken Mobile provisioning error by remote LDAP sync rule when importing as a local user.
1189462	SAML sync rules do not support setting certificate bindings from Google.
1139721	Secure connection to remote syslog server does not verify server certificate against CRL.
1190167	Console errors and 500 error in the captive portal after upgrade.
1191973	GUI access gives `500 internal server error` after upgrading from 6.4.10 to 6.5.6/6.6.4/6.6.6.
1187703	Portal templates are not removed from the database when portal is deleted.
1200091	Upgrade may occasionally fail due to non-atomic user password reset option migration in 6.6.3.
1172660	RADIUS session 'Last Update Date' shows incorrect time after an upgrade.

Bug ID	Description
1192375	500 internal server error when provisioning a user with an FortiToken Mobile token in the self-service portal.
1161321	Unable to register a FIDO key after enabling a FortiToken Mobile.
1157304	Upgrade to OpenSSL 3.5.0 for longer long term support.
1138014	'Username' is allowed as a password for an IAM user.
1172238	Slowloris HTTP DoS attack.
1198422	Privilege escalation in debug kit uploads.
1195245	Upgrade to the latest PostgreSQL postgres 15.14.
1195141	No HTTP content-type is set for woff2 font files.
1152796	3rd party component upgrade required for security reasons: sudo up to 1.9.16p2.
1199952	upgrade to `libexpat`-2.7.1.
1197074	Patches for `libxslt` vulnerabilities.
1163762	3rd party component upgrade required for security reasons: Python to 3.10.17/3.11.12/3.12.10/3.13.3.
1171174	Upgrade Neutrino to 17.1.4
1199500	MIT Kerberos/krb5 1.22.1.
1199455	Vulnerability fixes in Bootstrap.js 3.4.1.
1199414	Blackduck wants vulnerability fixes in gnutls 3.8.9
1193711	Upgrade kernel from 5.10 to 6.12.
1188713	`radiusd` upgrade.
1200473	Patch for CVE-2025-57052 in latest version of cJSON.
1199910	Upgrade to `Django` 4.2.24.
1199928	Upgrade to `Starlette` 0.47.3.
1199929	Upgrade to `urllib3` 2.5.0.
1199917	Upgrade to python requests 2.32.5.
1199913	Upgrade to `Pillow` 11.3.0.
1199939	Additional patch for a vulnerability in SQLite.
1199921	Upgrade to `python-protobuf` 5.29.5.
874293	FortiAuthenticator picks the incorrect IP address from the proxied requests (from the header) when multiple headers are used in a request.

Common Vulnerabilities and Exposures

Bug ID	CVE references
1192494	FortiAuthenticator 8.0.0 is no longer vulnerable to the following CVE-Reference (s): • CVE-2025-57823
1154180	FortiAuthenticator8.0.0 is no longer vulnerable to the following CVE-Reference (s): • CVE-2025-59923
1192498	FortiAuthenticator8.0.0 is no longer vulnerable to the following CVE-Reference (s): • CVE-2026-21743

Visit https://fortiguard.com/psirt for more information.

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
1203911	FortiAuthenticator should record a log when a guest portal is created/edited/deleted.
1201488	GUI cannot show the imported image as previous release.
1208814	Viewing first replacement message displays as blank; viewing next one works.
1201055	Guest portal backup/restore is incomplete.
1203907	Guest portal not showing correct message when user or source IP address is locked out.
1196790	Deletion of CA certificate in FortiAuthenticator VM Trust Anchor store requires a reboot to take effect.
1203923	Guest portal creation should not be allowed without a default language.
1187237	Add support to modify debugging level for LB sync daemon from the admin UI.
1198196	Radius Client configuration cannot be retrieved via REST API with admin with read access for the RADIUS services in admin profile.
1181149	High CPU observed due to fsae.
1201163	When changing the 'Exclude from SSO' option (logoff current user when excluded user logs in) to other option (do not affect current user when excluded user logs in), the logoff log remains generated.
1204521	Zero Trust Tunnel continues working even after the server certificate is revoked.
1194782	FortiAuthenticator IdP entity id metadata URL returns the default IdP certificate everytime; SP-specific certificate override is not working.
1192975	Network interface IP address change does not get applied to the web server until restart.
1200754	REST API PATCH `api/v1/localapiadmin/` error when creating a new local admin.
1189168	Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboot.
1196880	Mismatched cert/key in LB secondary side.
1180386	Permanent IP based lockout cannot be unlocked in the GUI.

Bug ID	Description
1196760	Failed to restore configuration after factory reset due to: `Database restore failed`.
1134745	Changes to the adaptive MFA rules in the admin UI are not logged.
1167348	OIDC JWT token cannot include more than one group.
1157369	When saving a user, even if no changes are made, a `PUT` request is sent to the FortiToken Cloud server.
1144845	FortiAuthenticator should not present SAML captcha when performing proxy authentication.
1147278	SCEP with FortiGate client in FIPS-CC mode does not work because FortiAuthenticator cannot import CA certificates signed with RSA-PSS.
1134751	Generate a log entry when there are changes made to NetHSM.
1108618	RADIUS MFA bypass not working for users with FortiToken Cloud/Email or FortiToken Cloud/SMS.
1133973	Delay in updating user counts after CSV import.
1134748	Generate a log entry when creating/editing/deleting a Zero Trust Tunnel.
1135277	Changes to mobile number or email address of guest users are not logged.
1164075	SmartConnection/EAP-TLS client certificate failed on Android.
1157157	Radius sessions user-type incorrectly labled 'external' with case sensitivity.
1140601	CLI logins attempts that fail without a successful follow-up are not logged.
1158142	Cache-Control header not present on SAML pages served by FastAPI/Gunicorn.
1145628	SAML IdP FIDO authentication fails on first try after FortiClient disconnect/reconnect.
1128643	FortiAuthenticator does not include rootCA cert in CMP Initialisation Response as required by 3GPP TS.33.310.
1068878	Unable to access FortiAuthenticator portals with IPv6 address if the interface does not also have an IPv4 address.
1084900	Device Self-Enrollment in the legacy self-service portal not working with placeholder variables `{{:cn}}` for certificate SAN fields.
1139476	Gateway timeout when loading local users page with a large number of users.
1148829	SCEP enrollment fails when certmonger client sends large GET request URI (exceeds the maximum length of 8190 bytes).
1033509	Log message should be recorded when SAML user session expires.
1026106	Failed to add new Fido key in Chrome with the Bitwarden extension.
997200	SAML IdP Proxy not able to retrieve the group memberships from the remote OpenLDAP server.

Bug ID	Description
1143190	Self-service portal shows empty page when all the post-login options are disabled.
1010053	Gateway timeout error in the GUI when performing a manual sync for a remote user sync rule with a large number of users (users are synced).
1084583	Exporting raw logs does not reflect the filter selection on the GUI.
971708	Avoid using the default 'admin' account in AWS since restoring configuration resets its password to `instance-id`.
1174109	User still can `https` access the FortiAuthenticator web page and disable the FortiAuthenticator interface related web access.
801933	LDAP service logs `LDAP_FAC` as the source IP address instead of the LDAP client IP address.

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	800F	3000F
Static Routes	N/A	50	50	50

System > Messages

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

System > Administration

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

Realms

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

Authentication > General

Feature	Calculating metric	300F	800F	3000F
Auth Clients (RADIUS and TACACS+)	Users / 3	500	2666	13333
Users (Local+ Remote)	N/A	1500 (minimum)/ 3500 (maximum)	8000 (minimum)/ 18000 (maximum)	40000 (minimum)/ 140000 (maximum)
User RADIUS Attributes	Users x 3	4500	24000	120000
User Groups	Users / 5	300	1600	8000
Group RADIUS Attributes	Users groups x 3	900	4800	24000
FortiTokens	Users x 2	3000	16000	80000
LDAP Entries	Users x 2	3000	16000	80000
Device (MAC based Auth.)	Users x 5	7500	40000	200000
RADIUS Client Profiles	N/A	1500	8000	40000
Remote LDAP Users Sync Rule	Users / 10	150	800	4000
Remote LDAP User Radius Attributes	Users x 3	4500	24000	120000

Remote authentication servers

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

FSSO & Dynamic Policies

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

Accounting Proxy

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

Certificates > User Certificates

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

Certificates > Certificate Authorities

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

Certificates > SCEP

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

Certificates > CMP

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

Services

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

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
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
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
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

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
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

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
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.