



Release Notes

FortiAuthenticator 6.6.10



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



July 9, 2026

FortiAuthenticator 6.6.10 Release Notes

23-6610-1278453-20260709

TABLE OF CONTENTS

Change log	4
FortiAuthenticator 6.6.10 release	5
Special notices	6
TFTP boot firmware upgrade process	6
Monitor settings for GUI access	6
Before any firmware upgrade	6
After any firmware upgrade	6
FortiAuthenticator does not support PEAP-MAB	6
SHA-1 cryptographic operations are no longer supported	7
Reconfigure LinkedIn social login	7
Using remote syslog servers with Secure connection enabled	7
Remote user synchronization rule behavior change for FortiToken Mobile activation	7
What's new	8
Upgrade instructions	9
Hardware and VM support	9
Image checksums	10
Upgrading from 4.x/5.x/6.x	10
Product integration and support	14
Web browser support	14
FortiOS support	14
Fortinet agent support	14
Virtualization software support	15
Third-party RADIUS authentication	15
FortiAuthenticator-VM	17
Resolved issues	18
Known issues	22
Maximum values for hardware appliances	26
Maximum values for VM	32
Data-at-rest protection	36

Change log

Date	Change Description
2026-05-15	Initial release.
2026-05-19	Updated Resolved issues on page 18 .
2026-07-09	Updated Special notices on page 6 .

FortiAuthenticator 6.6.10 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.6.10, build 1929.

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

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.

What's new

FortiAuthenticator version 6.6.10 is a patch release. There are no new features. See [Resolved issues on page 18](#) and [Known issues on page 22](#) for more information.

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 6.6.10 requires at least 4 GB of RAM.



When FortiAuthenticator 6.6.10 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 6.6.10 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 9](#)
- [Image checksums on page 10](#)
- [Upgrading from 4.x/5.x/6.x on page 10](#)

Hardware and VM support

FortiAuthenticator 6.6.10 supports:

- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400E
- FortiAuthenticator 800F
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000E
- FortiAuthenticator 3000F

- FortiAuthenticator VM
See [Virtualization software support on page 15](#).

Image checksums

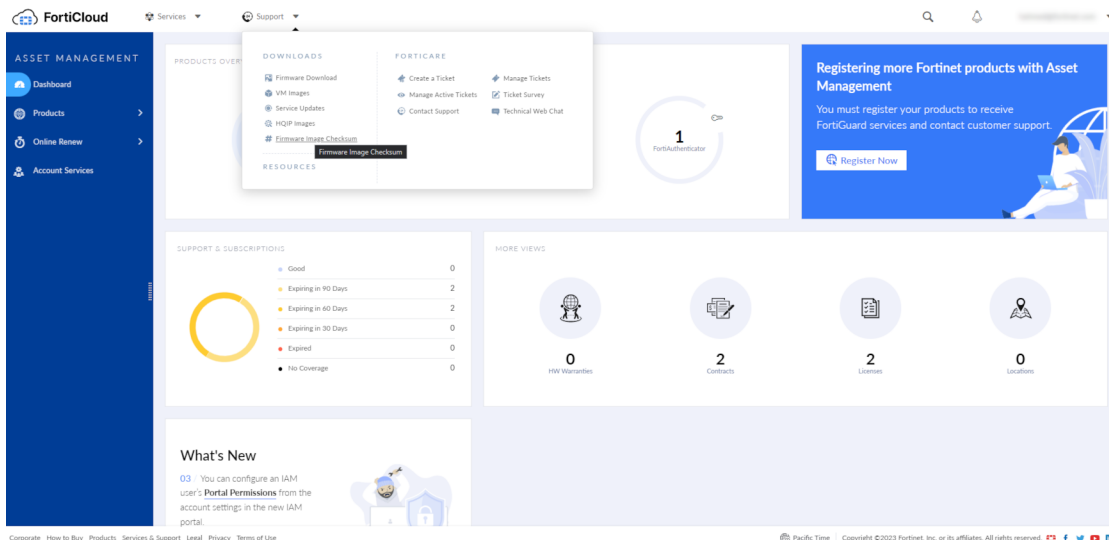
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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 6.6.10 build 1929 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 6.6.10, 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 6.6.10 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.6.10.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 6.6.10 directly.



When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.6.10 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 12](#).



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](#). In the **Support > Download** section of the page, select the **Firmware Download** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksum** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. 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.
5. 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 FAC-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 6.6.10, 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. Please 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 6.6.10

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 14](#)
- [FortiOS support on page 14](#)
- [Fortinet agent support on page 14](#)
- [Virtualization software support on page 15](#)
- [Third-party RADIUS authentication on page 15](#)

Web browser support

The following web browsers are supported by FortiAuthenticator 6.6.10:

- Microsoft Edge version 148
- Mozilla Firefox version 150
- Google Chrome version 148

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

FortiOS support

FortiAuthenticator 6.6.10 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 6.6.10 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 6.6.10 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 17](#) 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
973414	Downloading large summary debug report from GUI leads to Gateway Timeout Error.
1157337	Gateway timeout when downloading summary debug report (when the unprocessed raw log files are large).
1179387	Unable to use a certificate with multiple SAN as RADSEC server certificate.
1189147	Error Authorized certificate must be installed in Trusted Endpoint SSO after upgrade to 6.6.4.
1198648	Remote radius user password change failed from self-service-portal/admin-portal.
1211393	Certificates with 'noon' in expiring time cannot be revoked.
1212936	Group filtering not properly enforced by OAuth when accessing second RP.
1216973	FSSO randomly stops performing group lookups for SSOMA on native Entra ID-joined workstations.
1217419	3 rd party component upgrade required for security reasons: OpenSSH to 10.2/10.2p1.
1219592	Usage Profile allowing users to go over threshold for 30-90 seconds after reaching data quota.
1220308	SAML Sync Rule with No OTP method generates excessive logs.
1220448	HA Tables showing Out of Sync intermittently when tables are actually in sync.
1223330	If FortiGate filter includes group name starting with 'OU= ', FortiAuthenticator strips the leading 'OU= ' from the group name in FSSO sessions.
1223352	Too many static routes (5+) on unlicensed VM breaks route setup upon reboot.
1223664	Cross-Origin-Opener-Policy: same-origin breaks OIDC compatibility with vault.
1223922	Admin UI crash after CLI allows creating more static routes than the license limit.
1225477	FTM activation may fail with Activation Code is invalid when sync rules run concurrently.
1231468	Admin users cannot enable the 'allow LDAP browsing' feature.
1231845	RADIUS policies always become out-of-sync to LB HA node.

Bug ID	Description
1233747	RADIUS service may take a long time to restart after config changes under degraded LDAP server conditions.
1234449	Admin GUI login fails with third-party RADIUS push MFA; longer timeout setting not applied.
1235704	Update admin GUI for renaming of 'FortiToken Cloud' service to 'Fortidentity Cloud'.
1235720	Upgrade to OpenVPN 2.6.17.
1237759	Fiber network interface (port5) gets into a flapping state after an indeterminate period of normal function.
1238552	Locked-out IP addresses are getting unlocked before configured lockout period.
1239265	Upgrades to urllib3, filelock.
1239293	LACP: Creating or deleting a bonded interface throws firewall-related Python errors on CLI.
1239988	HA Primary node may report out-of-sync LB node status when LB node is actually in-sync.
1240543	Upgrade net-snmp component.
1240906	Error 0A000086:SSL routines::certificate verify failed appears in the CLI console during bootup.
1242025	Upgrade to glib for misc. vulnerabilities.
1243592	Unnecessary polling to FTM service when no registered FTMs; continuous error log events.
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 password reset page.
1244740	FortiAuthenticator allows a maximum of 255 TACACS+ service attributes.
1245178	Incorrect FSSO filtering when domain, e.g. dc=domain,dc=com, is root DN for the second distinct domain, e.g., dc=test,dc=domain,dc=com.
1245322	Local users cannot change passwords when legacy self-service portal (/login) network interface access is disabled.
1246232	Remote LDAP sync rule fails if imported user was promoted to Administrator role through the admin UI.
1246579	OAuth does not work when authorizing with LDAP groups filter.
1247625	End-users able to reconnect for 30-90 secs after exceeding their usage profile data usage limit.

Bug ID	Description
1248228	OTP bypassed in password change when Cisco ASA is the RADIUS client.
1251956	Upgrade to python-multipart 0.0.22.
1252308	Upgrade to openldap 2.6.12.
1253004	Upgrade to curl 8.19.0.
1253231	PATCH to REST API /api/v1/radiususers/[ID]/ endpoint to update mobile_number fails.
1256685	Upgrade to PostgreSQL 15.16.
1256955	Revoked client certificate (included in CRL) with serial number length less than 16 is not blocked by EAP-TLS.
1257765	TACACS+ service may fail to restart after config changes.
1258815	Upgrade with multiple templates should not break admin login page.
1261920	SAML IdP is leaking sessions for dead URLs causing infinite /tmp growth.
1262280	Error during captive portal user registration under high load.
1271207	Shell injection vector found inside admin interface.
1273279	Vulnerability fix in pyOpenSSL.
1273564	Smart Connect EAP-TLS Profile fails to install on macOS.
1276949	FortiAuthenticator exposes challenge password in SCEP debug logs.
1280494	Updating the Network Interface page logs out the admin and immediate relogin returns a 503 error.
1280943	Upgrade to OpenSSL 3.0.20 / 3.5.6.
1281723	Upgrade to python cryptography-46.0.7.
1282471	Getting error when trying to lock, disable, or re-enable a guest user.
1284014	3 rd party component upgrade required for security reasons: OpenSSH to 10.3/10.3p1.
1286261	IP lockout exemption not work properly for 0.0.0.0/32.
1286581	Upgrade libexpat to 2.8.0.
1286582	Upgrade libpng to 1.6.58.
1286694	Upgrade to Django 4.2.30.
1288887	Upgrade to kernel 5.10.254.
1290802	Upgrade to python-pillow 12.2.0.
1290812	Upgrade to Apache httpd 2.4.67.

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
801933	LDAP service logs 'LDAP_FAC' as source IP instead of the LDAP client IP address.
874293	FortiAuthenticator picks the incorrect IP address from proxied requests from the header when multiple headers are used in a request.
971708	Avoid using the default 'admin' account in AWS since restoring configuration resets its password to <code>instance-id</code> .
997200	SAML IdP Proxy not able to retrieve group memberships from remote OpenLDAP server.
1010053	Gateway Timeout Error on GUI when doing a Manual Sync for a Remote User Sync Rule with a large number of users (users are synced).
1010853	Invalid URL link in password reset email when username contains special UTF8 characters.
1026106	Failed to add new FIDO key in the Google Chrome with Bitwarden extension.
1037946	SMS does not replace replacement message tag <code>{{ :random_id_64 }}</code> with random 64-char value.
1048961	Unable to change a user portal policy priority order (403 Forbidden) if captive portal disabled for all network interfaces.
1068878	Unable to access FortiAuthenticator portals with IPv6 address if the interface does not also have IPv4 address.
1072845	Accounting requests sent by FortiGate over RADSec are ignored causing time out on FortiGate.
1084583	Exporting raw logs does not reflect filter selection on GUI.
1091168	Push notifications do not work if using UPN format username in the FortiAuthenticator Windows Agent.
1108618	RADIUS MFA bypass not working for users with FTC/Email or FTC/SMS.
1128643	FortiAuthenticator does not include rootCA cert in CMP Initialisation Response as required by 3GPP TS.33.310.
1130853	RADIUS client import via CSV does not support '.' (dot) character in RADIUS client name.
1133973	Delay in updating user counts after CSV import.

Bug ID	Description
1134745	Changes to adaptive MFA rules in admin UI are not logged.
1134748	Generate a log entry when creating/editing/deleting a Zero Trust Tunnel.
1134751	Generate a log entry when there are changes made to NetHSM.
1135277	Changes to mobile number or email address of guest users are not logged.
1138014	'Username' is allowed as a password for IAM User.
1139476	Gateway Timeout when loading local users page with a large number of users.
1139721	Secure connection to remote syslog server does not verify server cert against CRL.
1140601	CLI logins attempts that fail without a successful follow-up are not being logged.
1141778	FortiAuthenticator GUI shows multiple Organization RDNs in subject but actual certificate only contains one.
1142209	PCI DSS SAML portal immediately fails on incorrect passwords if the IP falls under a trusted subnet.
1143190	Self-service portal shows empty page when all the post-login options are disabled.
1143578	MFA bypass does not work if the previous user portal authentication used password + token concatenation.
1144145	RADIUS bypasses MAC filtering and authorization checks for EAP-MSCHAPV2 2FA when FortiToken push is used.
1144845	FortiAuthenticator should not present SAML captcha when doing proxy authentication.
1145628	SAML IdP FIDO authentication fails on first try after FCT disconnect/reconnect.
1148829	SCEP enrollment fails when certmonger client sends a large GET request URI that exceeds maximum length of 8190 bytes.
1155278	Importing local users using FortiGate configuration file fails.
1156684	Non-fatal load_license error message on console after restoring config.
1157157	RADIUS sessions incorrectly labeled with 'external' user type due to username case-sensitivity mismatch.
1157369	When saving a user, even if no changes are made, a PUT request is sent to the FTC server.
1157522	OWA Agent MFA bypass option for users without token configured not working against FortiAuthenticator 6.6.
1159384	Log backups to FTP server failing repeatedly prevents log auto-deletion.
1169005	Need to do CRL check for full certificate chain when doing LDAPS connection to remote LDAP server.

Bug ID	Description
1170731	FortiAuthenticator HA cluster forming / routing issues in OpenStack environment.
1171320	Admin UI should not allow selecting an OU in the LDAP tree browser for 'Set Group'.
1178589	Typo in tooltip of Event 4768 in Event ID selection showing 6768 instead of 4768.
1180386	Permanent IP based lockout cannot be unlocked in the GUI.
1181816	IP lockout time reset by unknown user.
1183726	Failed tiered FSSO TLS connection due to invalid disk copy of the firmware certificate signed by Fortinet CA2 on FortiAuthenticator-3000F.
1189168	Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboot.
1192375	500 internal server error when provisioning a user with an FTM token in the self-service portal.
1192926	Cluster not forming with error PGRES_FATAL_ERROR ERROR: payload string too long.
1195161	HSTS: Increase default max-age and include includeSubDomains directive when HSTS enabled.
1196760	Failed to restore configuration after factory reset due to Database restore failed:.
1196880	Mismatched Cert/key in LB secondary side.
1204521	Zero-Trust Tunnel continues working even after server certificate is revoked.
1212035	Automatic CRL download does not verify validity period.
1212698	Unable to create a user certificate with OCSP URL when root domain contains a digit.
1218888	Local users REST API with LDAP auto-provisioning does not work.
1229075	SSO Webservices: 'Self-Service portal policies' search function shows that 'the results could not be loaded.'
1230521	FortiAuthenticator sends syslog messages with timestamp in obsolete RFC 3164 format.
1231262	LDAP service user search returns wrong responses to ~1 of 10K requests under heavy load and 200K users.
1231472	500 error when logging in with an IAM user to the OAuth portal.
1232741	EAP-TLS accepting client certificate even though CRL is expired.
1232965	SCIM client crash on restart.
1236010	500 server error when importing certificate with invalid format into remote SAML server.

Bug ID	Description
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.
1239281	Occasional slower (1 sec) SAML IdP response generation when a large number (1000+) of SPs configured.
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).
1247697	500 error in admin UI when editing user group if it contains an unknown RADIUS attribute.
1257974	Logging to FortiAnalyzer Cloud fails due to missing SNI.
1259634	Synchronization with Entra ID SAML takes too long.
1265223	Self-Service Password Reset does not work if using Hardware FortiTokens.
1266463	Importing users from LDAP server by group membership shows stale user accounts info.
1271803	Unable to sync more than 500 users using a Google SAML server.
1275900	FortiAuthenticator address Lockout Exemption for 0.0.0.0/32 not working causing global WiFi authentication lockouts.
1284484	SAML user sync does not clean up the lock file on exception.

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.



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.



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 $1500 \div 5 = 300$ user groups.

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

Refer to the [Maximum values for VM on page 32](#) section for all parameters, features, and their corresponding metrics.

System > Network

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Static Routes	50	50	50	50	50	50	50	50

System > Messages

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
SMTP Servers	20	20	20	20	20	20	20	20
SMS Gateways	20	20	20	20	20	20	20	20
SNMP Hosts	20	20	20	20	20	20	20	20

System > Administration

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Syslog Servers	20	20	20	20	20	20	20	20
User Uploaded Images	40	90	115	415	515	1015	2015	2015
Language Files	50	50	50	50	50	50	50	50

Realms

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Realms	20	60	80	320	400	800	1600	1600

Authentication > General

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Auth Clients (NAS)	166	500	666	2666	3333	6666	13333	13333
Users (Local+ Remote) ¹	500	1500/ 3500*	2000	8000/ 18000*	10000	20000	40000/ 140000*	40000/ 140000*
User RADIUS Attributes	1500	4500	6000	24000	30000	60000	120000	120000
User Groups	100	300	400	1600	2000	4000	8000	8000
Group RADIUS Attributes	150	450	150	2400	600	6000	12000	12000
User Certificate Bindings	1000	3000	4000	16000	20000	40000	80000	80000
FortiTokens	1000	3000	4000	16000	20000	40000	80000	80000
FortiToken Mobile Licenses ²	200	200	200	200	200	200	200	200
LDAP Entries	1000	3000	4000	16000	20000	40000	80000	80000
Device (MAC based Auth.)	2500	7500	10000	40000	50000	100000	200000	200000
RADIUS Client Profiles	500	1500	2000	8000	10000	20000	40000	40000
Remote LDAP Users Sync Rule	50	150	200	800	1000	2000	4000	4000
Remote LDAP User Radius Attributes	1500	4500	6000	24000	30000	60000	120000	120000

Remote authentication servers

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Remote LDAP Servers	20	60	80	320	400	800	1600	1600
Remote RADIUS Servers	20	60	80	320	400	800	1600	1600
Remote SAML Servers	20	60	80	320	400	800	1600	1600
Remote OAuth Servers	20	60	80	320	400	800	1600	1600
Remote TACACS+ Servers	20	60	80	320	400	800	1600	1600

FSSO & Dynamic Policies

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
FSSO Users	500	1500	2000	8000	10000	20000	200000 ³	200000
FSSO Groups	250	750	10000	4000	5000	10000	20000	20000
Domain Controllers	10	15	20	80	100	200	400	400
RADIUS Accounting SSO Clients	166	500	666	2666	3333	6666	13333	13333
FortiGate Group Filtering	250	750	1000	4000	5000	10000	20000	20000
FSSO Tier Nodes	5	15	20	80	100	200	400	400
IP Filtering Rules	250	750	1000	4000	5000	10000	20000	20000

Accounting Proxy

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Sources	500	1500	2000	8000	10000	20000	40000	40000
Destinations	25	75	100	400	500	1000	2000	2000
Rulesets	25	75	100	400	500	1000	2000	2000

Certificates > User Certificates

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
User Certificates	2500	7500	10000	40000	50000	100000	200000	200000
Server Certificates	50	150	200	800	1000	2000	4000	4000

Certificates > Certificate Authorities

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
CA Certificates	10	10	10	50	50	50	50	50
Trusted CA Certificates	200	200	200	200	200	200	200	200
Certificate Revocation Lists	200	200	200	200	200	200	200	200

Certificates > SCEP

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Enrollment Requests	2500	7500	10000	40000	50000	100000	200000	200000

Certificates > CMP

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Enrollment Requests	2500	7500	10000	40000	50000	100000	200000	200000

Services

Feature	200E	300F	400E	800F	1000D	2000E	3000E	3000F
FortiGate Services	50	150	200	800	1000	2000	4000	4000
TACACS+ Services	50	150	200	800	1000	2000	4000	4000

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.

³ For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

* Upper limit

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.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19 (minimum)	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (RADIUS and TACACS+)	3	Users / 3	33	1666

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Remote authentication servers	Authentication Policy (RADIUS and TACACS+)	6	Users	100	5000
	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	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
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
	Realms	2	Users / 25	4	200

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO & Dynamic Policies					
FSSO	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
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	500	25000
CMP	Enrollment Requests	5	Users x 5	500	25000
Services					
	FortiGate Services	2	Users / 10	10	500

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