Release Notes

FortiAuthenticator 8.0.2

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

March 20, 2026
FortiAuthenticator 8.0.2 Release Notes
23-802-1258020-20260320

TABLE OF CONTENTS

Change log

Date	Change Description
2026-03-20	Initial release.

FortiAuthenticator 8.0.2 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 8.0.2, build 0097.

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 8.0.2, 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 8.0.2 includes the following enhancements:

TACACS+/RADIUS client groups

When configuring a TACACS+ policy, the FortiAuthenticator administrator selects the subset of TACACS+ client that uses the policy.

In large environments with hundreds of TACACS+ clients, selecting the TACACS+ clients one-by-one in the UI is cumbersome.

Therefore, it is useful for administrators to be able to group TACACS+ clients together and use them as a single unit when configuring the policies.

A new **Groups** tab available in **Authentication > TACACS+ Service > Clients**.

The TACACS+ policies allow selecting a combination of TACACS+ clients and TACACS+ client groups in **Authentication > TACACS+ Service > Policies**.

The FortiAuthenticator REST API now includes the following three new TACACS+ endpoints:

TACACS+ Client Groups (`/tacplusclientgroups/`)
TACACS+ Clients Group/Client Associations (`/tacplusgroupclient/`)
TACACS+ Policy/Group Associations (`/tacpluspolicygroup/`)

Redundant HA: Separate management interface and heartbeat interface

Starting FortiAuthenticator 8.0.2, in **System > Administration > High Availability**, the following have been renamed:

- **Interface** setting to **Management interface**.
- **Cluster member IP address** field to **Management IP address**.
- **HA admin access** to **Management access**.

Also, a new **Heartbeat Interface** setting is available that decouples the HA management interface and the heartbeat interface.

Mixed licensing support for HA and load balancing

Starting 8.0.2, FortiAuthenticator now supports mixed licensing models in High Availability (HA) and Load Balancing (LB) deployments, providing greater flexibility for hybrid environments.

Key capabilities:

- **Subscription and perpetual VM licensing**
  - Both licensing models are supported for FortiAuthenticator VMs.
  - Primary and secondary nodes in an active-passive HA pair must share the same licensing mode (either both perpetual or both subscription).
- **Load balancer flexibility**
  - Load balancing nodes can use a different licensing model than the primary HA pair.
  - Subscription VMs can act as LB nodes even when the primary HA pair uses perpetual licenses.
- **Hardware and VM mixing**
  - HA clusters can include hardware appliances and VMs, provided model and licensing rules are met.

Benefits

- Simplifies scaling by allowing subscription VMs for LB without changing the HA core.
- Reduces cost for distributed deployments by mixing licensing models strategically.

Supported configurations EXAMPLE

- Two FortiAuthenticator-300F units in active-passive HA with VM nodes for load balancing.
- FortiAuthenticator-VM (perpetual) as primary and secondary, with FortiAuthenticator-VM (subscription) as LB node.

LDAP Service: Offer authentication method options

In FortiAuthenticator, you can now specify which authentication factor is verified by the LDAP service during an LDAP bind.

Starting FortiAuthenticator 8.0.2, a new **Authentication Methods** option is available when editing the LDAP service settings in **Authentication > LDAP Service > General**.

Tracking Monthly Active Users (MAU)

Starting FortiAuthenticator 8.0.2, you can now track the number of monthly active users in the new **Monthly Active Users** widget in **System > Dashboard > Status**.

An active user is one with at least one successful login in the last 30 days.

Note: If **Monthly Active Users (MAU)** exceeds the user license entitlement, the **Monthly Active Users** widget displays the following warning in red:

```
User license violation
```

A new **Active Users** tab in **Monitor > Authentication** where you can view the list of the recorded active users.

FortiAuthenticator RADIUS: Support for EAP-TEAP

TEAP chains a machine authentication and a user authentication into a single authentication session.

For the authentication session to succeed, both machine and the user authentication must be successful.

Further, the machine and user authentications can use EAP-MSCHAPv2 or EAP-TLS.

A new **Auth Profiles** tab is available in **Authentication > RADIUS Service**.

Previously available **Authentication type**, **Identity sources**, and **Authentication factors** tabs when configuring an authentication policy have been moved to authentication profiles.

You can now group RADIUS clients together and use them as a single unit when configuring the policies.

A new **Groups** tab available in **Authentication > RADIUS Service > Clients**.

A new **Authentication Profiles** tab is available when configuring a RADIUS policy in **Authentication > RADIUS Service**.

In the **Authentication Profiles** tab:

- Specify which authentication type and profile to use.

Certificates: Support Elliptic Curve Cryptography (ECC)

When creating a local CA certificate, a new **ECC** option is available for **Key type** in **Certificate Management > Certificate Authorities > Local CAs**.

When the **Key type** is **ECC**, a new **Ecc key size** option is available.

Similarly, **Key type** and **Ecc key size** options are available when creating a new user/local services certificate in **Certificate Management > End Entities**.

Smart Connect: Support for the latest application in the Microsoft Store

The Smart Connect menu in the self-service portal offers a new platform option for Windows.

Previously available **Windows Executable (.exe)** and **Windows Compressed (.zip)** have been removed.

The Smart Connect application for Windows does not support EAP-TTLS.

The following error message is displayed when you configure a self-service portal with an EAP-TTLS Smart Connect profile and attempt to download the Smart Connect application for Windows:

```
Smart Connect for Windows does not support the required network connection profile. Please contact your administrator.
```

The following warning appears when you configure a self-service portal with EAP-TTLS in **Authentication > Portals > Portals** with **Post-login Services** set as a Smart Connect profile:

```
Warning: You selected an EAP-TTLS Smart Connect profile, which is not supported for Windows users.
```

OCSP verification modes

FortiAuthenticator 8.0.2 introduces per-policy OCSP-based certificate verification.

A new **Reject usernames containing uppercase letters using OCSP to validate EAP-TLS client certificate** option available when configuring an authentication profile in **Authentication> RADIUS Service > Auth Profiles**.

Note: The **Client Credential** is **Certificates**.

Administrators can configure one of the following three modes:

Disable	OCSP verification is not performed (default).
Enable	Certificates must pass OCSP verification.
Enable-softfail	If the OCSP server does not respond or times out, the certificate is accepted unless an explicit `reject` is received.

The OCSP timeout is currently fixed at 3 seconds.

Future releases may allow this to be configurable either globally or per policy.

New `diag debug` CLI commands

FortiAuthenticator 8.0.2 introduces new diagnostic debugging commands in the CLI.

This enhancement provides administrators with a consistent and flexible way to troubleshoot and monitor system daemons.

Command	Description
diagnose debug app <app_name> <category> <level>	Enable debugging for a specific application with defined category and verbosity level.
diagnose debug app <app_name> {debugall | traceall | clear | show}	Apply global debug actions such as enabling all traces, clearing logs, or showing current debug status.
diagnose debug info	Display current debug configuration and active sessions.
diagnose debug clear-all	Clear all active debug settings across applications.
diagnose debug reset	Reset the debug framework to default state.

The framework currently supports debugging for the following daemons:

updated	Diagnose update process.
db_mond	Diagnose database monitoring daemon.

cfg_mond	Diagnose configuration monitoring daemon.
event_mond	Diagnose event monitoring daemon.
ha_proxyd	Diagnose HA proxy daemon.
winad_mon	Diagnose Windows AD monitoring daemon.
lb_sync	Diagnose load balancer synchronization daemon.
ftm_scimd	Diagnose FortiToken Mobile SCIM daemon.
scepd	Diagnose SCEP daemon.
radiusd	Diagnose RADIUS daemon.

REST API enhancements: New `display_name` field in the `Local users (/localusers/)` endpoint

Starting FortiAuthenticator 8.0.2, a new `display_name` field is available in the `Local users (/localusers/)` endpoint.

REST API enhancements: Support self-service to add an external IdP

Starting FortiAuthenticator 8.0.2, the following new endpoints are available:

- `/remotesamlservers/`
- `/samlidpusersources/`

Accessing the REST API Swagger documentation

Beginning with FortiAuthenticator 8.0.2, you can view the full REST API documentation through a built-in Swagger UI at:

```
https://<FAC_IP>/api/v2/docs
```

This interface allows you to explore, understand, and test API endpoints directly from your browser.

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 8.0.2 requires at least 4 GB of RAM.

When FortiAuthenticator 8.0.2 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 8.0.2 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 8.0.2 supports:

- FortiAuthenticator 300F
- FortiAuthenticator 800F
- FortiAuthenticator 3000F
- FortiAuthenticator VM
  See Virtualization software support on page 19.

Image checksums

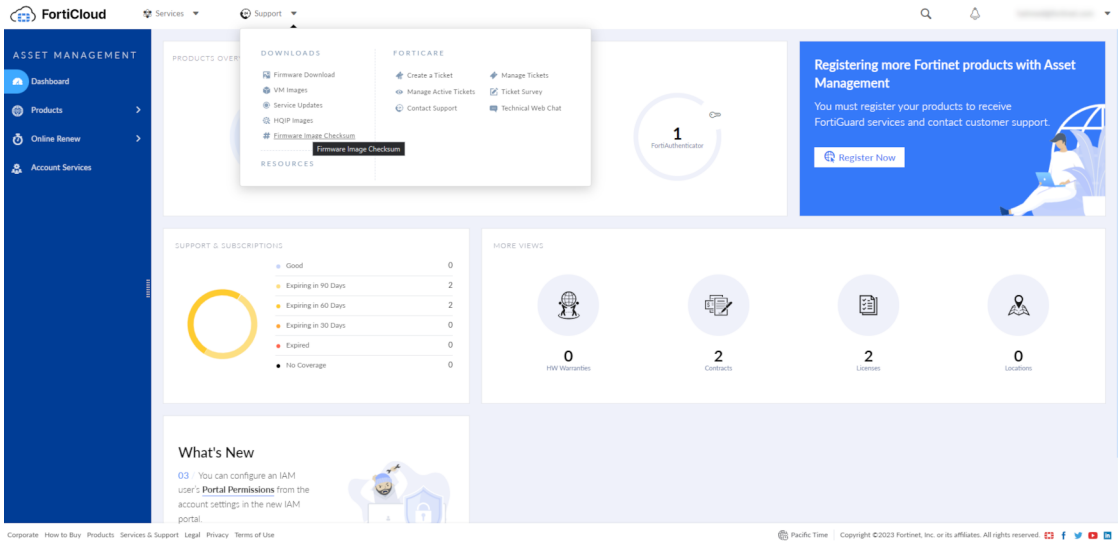
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available on FortiCloud.

FortiCloud image checksum tool

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

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



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

FortiAuthenticator 8.0.2 build 0097 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 8.0.2, 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 8.0.2 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 8.0.2.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 8.0.2 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 8.0.2 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 17.

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 8.0.2, 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 8.0.2

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

The following web browsers are supported by FortiAuthenticator 8.0.2:

Google Chrome version 146
Microsoft Edge version 145
Mozilla Firefox version 148

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

FortiOS support

FortiAuthenticator 8.0.2 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 8.0.2 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.
 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.

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 8.0.2 supports:

Alibaba Cloud
AWS (Amazon Web Services)
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
Microsoft Azure
Nutanix
Oracle OCI
Proxmox

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

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

See FortiAuthenticator-VM on page 21 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
993261	Provide a convenient way for admin to find if user belongs to a group when group contains hundreds of users.
1067454	Expired SAML IdP sessions not getting cleaned up.
1084913	3rd party component upgrade required for security reasons: sendmail to 8.18.1.
1108618	RADIUS MFA bypass not working for users with FortiToken Cloud/Email or FTC/SMS.
1138244	FortiAuthenticator does not send full certificate chain to the Syslog server.
1140550	User Lookup Account Status on LB FortiAuthenticator does not Update/Sync from the primary FortiAuthenticator.
1141373	Alert when Syslog server certificate is expired.
1144265	All HTTPS requests getting 500 Internal Server Error after days/weeks of normal operation until reboot.
1157157	RADIUS sessions incorrectly labeled `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 FortiToken Cloud server.
1158142	Cache-Control header not present for many SAML IdP pages.
1159384	Log backups to an FTP server failing repeatedly prevents log auto-deletion.
1167348	OIDC JWT token cannot include more than one groups.
1174109	User can https access the FortiAuthenticator webpage and disable the FortiAuthenticator interface related web access.
1181149	High CPU observed due to `fsae`.
1183019	3rd party component upgrade required for security reasons: `lxml` to 6.0.2.
1187703	Portal templates are not removed from the database when portal is deleted.
1189147	FortiAuthenticator gives error `Authorized certificate must be installed` in Trusted Endpoint SSO after upgrade to 6.6.4.
1192375	500 internal server error when provisioning a user with an FTM token in the self-service portal.

Bug ID	Description
1193229	LB node can become convinced that it is subscribed to NO sets of tables.
1194782	FortiAuthenticator IdP entity id metadata URL returns Default IdP certificate everytime; SP-specific certificate override not working.
1194901	Default to 'https' format for 'IdP entity id' field in SAML Service Provider config.
1196790	Deletion of CA certificate in FortiAuthenticator VM Trust Anchor store requires a reboot to take effect.
1198196	Radius Client configuration cannot be retrieved via REST API with an admin with read access to RADIUS services in admin profile.
1198648	Remote RADIUS user password change failed from self-service-portal/admin-portal.
1200754	REST API PATCH `api/v1/localapiadmin/` error when creating a new local admin.
1201055	Guest Portal: Full config backup/restore and HA replication.
1201163	Changing *Exclude from SSO* option does not take affect until other event triggers FSSO service restart.
1203989	HA connectivity/sync issues when bringing primary back up after failover.
1208720	Importing local user CSV wipes user bound RADIUS attributes.
1208814	Viewing first replacement message displays as blank; viewing next one works.
1209416	500 internal server error during user self-registration with SMS in a self-service portal.
1211104	Upgrade to `libexpat` 2.7.3.
1211124	SAML IdP session not initialized properly when end-user does logins with two different external IdPs.
1211202	`curl` upgrade to 8.16.0.
1211229	`Django` upgrade to 4.2.25.
1211393	Certificates with 'noon' in expiring time cannot be revoked.
1212070	CLI TFTP command ignoring response from the server.
1212698	Unable to create a user certificate with OCSP URL when root domain contains a digit.
1212936	Group filtering not properly enforced by OAuth when accessing second RP.
1214264	Upgrade to `open-vm-tools`13.0.5+.
1214431	Incorrect username in RADIUS response when username input contains substrings: `\r`, `\n` or `\t`.

Bug ID	Description
1216923	Manual import of CRL gives error `Unable to load CRL file. Ensure that it has a valid format and not empty`.
1216973	FSSO randomly stops performing group lookups for SSOMA on native Entra ID-joined workstations.
1217316	Local user CSV import is broken in REST API.
1217419	3rd party component upgrade required for security reasons: OpenSSH to `10.2/10.2p1`.
1217848	Certificate issuer/Certificate subject fields are blank on remote SAML server config page.
1218489	FSSO group lookups fail due to failed OAuth token validation with EntraID.
1218888	Local users REST API with LDAP auto-provisioning does not work.
1218907	Bulk delete local users can timeout for large number of users.
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.
1220520	Creating Remote LDAP Groups with 'LDAP directory group' fails DN validation when attribute value contains a space.
1223246	Unable to create FortiAuthenticator CA with expiry date beyond 2038 (end of Unix epoch).
1223330	If FortiGate filter includes group name starting with 'OU=', FAC stripping the leading 'OU=' from that group name in FSSO sessions.
1223352	Too many static routes (5+) on unlicensed VM breaks route setup upon reboot.
1223599	SAML authentication redirects to 403 error when `Web Interface (TCP/443)` access is revoked after upgrade to 6.6.7.
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.
1224327	Sending guest users credentials via Email or SMS in sponsor portal fails due to auto-added semicolon in recipients field.
1224409	Restricted admins cannot manage tokens after upgrade.
1224722	After upgrade, admin cannot export remote LDAP users.
1224992	FortiAuthenticator Cloud instance stuck in 'Evaluation' license type.
1225477	FTM activation may fail with 'Activation Code is invalid' when sync rules run concurrently.

Bug ID	Description
1225733	Sponsor cannot view/print guest user passwords while the admin can.
1226093	Upgrade to `OpenSSL` 3.5.4.
1226099	Upgrade to `PostgreSQL` 15.15.
1227635	Missing accessibility to Provisioning Activity Logs in the admin UI when users are synced by SCIM sync rule.
1227700	Unable to import usergroups with CSV file.
1227859	SCIM server does not reenable user account on update from EntraID.
1229968	Possible pending FTM deprovisioning after FTM app activation due to mishandling of connection termination by FGD server.
1230446	Invalid license expiry on dashboard after restoring config backup converted from VM to hardware model.
1230521	FortiAuthenticator sends syslog messages with timestamp in obsolete RFC 3164 format.
1231229	`libpng16` upgrade to 1.6.52.
1231262	LDAP service user search returns wrong responses to ~1 of 10K requests under heavy load and 200K users.
1231273	Guest Portals: Portal Setup Complete wizard step should show captive portal.
1231351	Add button RADIUS debug page to restart the RADIUS daemon.
1231468	Admin users cannot enable the 'allow LDAP browsing' feature.
1231472	500 error when logging in with an IAM user to the OAuth portal.
1231845	RADIUS policies always become out-of-sync to LB HA node.
1232521	Stranded foreign keys in `PortalTemplateMatching` tables cause 500 error.
1232741	EAP-TLS accepting client certificate even though CRL is expired.
1232772	`SubjectAltName` have all values in one line separated by comma.
1232965	SCIM client crash on restart.
1233366	Unable to remove corrupt local user accounts.
1233690	SAML sync rule adds user account even though FortiToken assignment failed.
1233747	RADIUS service may take a long time to restart after config changes under degraded LDAP server conditions.
1233939	Change password does not seem to work.
1234449	Admin GUI login fails with third-party RADIUS push MFA; longer timeout setting not applied.
1234473	FTK and FTM registration not yet supported by FortiGuard/FortiCloud.

Bug ID	Description
1235193	Unresponsive web server on race condition after WAD crash.
1235572	upgrade to `apache httpd`2.4.66.
1235704	Update admin GUI for renaming of 'FortiToken Cloud' service to 'FortiIdentity Cloud.'
1235720	Upgrade to OpenVPN 2.6.17.
1236010	500 server error when importing certificate with invalid format into remote SAML server.
1236384	Smart Connect for Windows installs CA in Personal Certificates.
1236512	LDAPS user syncing is broken if specific CA is selected.
1238010	Update Fortinet RADIUS VSA dictionary.
1238151	FTM/FTK self-provisioning not available in user portal.
1238418	Add support for FortiGuard SMS.
1238552	Locked-out IP addresses are getting unlocked before configured lockout period.
1238912	All OAuth and REST API URLs should be accessible with or without trailing slash.
1239265	Upgades to urllib3, filelock.
1239281	Occasional slower (1 sec) SAML IdP response generation when large number (1000+) of Service Providers configured.
1239289	LACP: Unable to create bonded interface if you ever visited the GUI packet capture page.
1239293	LACP: Creating or deleting a bonded interface throws firewall-related python errors on CLI.
1239312	Optimize SAML Service Provider Attribute Query.
1239341	Upgrade to `libpcre2`.
1239988	HA Primary node may report out-of-sync LB node status when LB node is actually in-sync.
1240168	Unable to view details of an imported CSR.
1240543	Upgrade net-snmp component.
1240773	Default `fortinet_logo` image cannot be edited.
1240906	Error `0A000086:SSL routines::certificate verify failed` appears in the CLI console during bootup.
1242025	Upgrade for glib.

Bug ID	Description
1242365	403 error when clicking the `Understanding the captive portal workflow` book icon in portal policies list views.
1242444	FortiAuthenticator Cloud firmware upgrade exception due to HTTP 201 response.
1242678	Add Windows SmartConnect application installation instructions in the self-service portal.
1243592	Unnecessary polling to FTM service when no registered FTMs (continuous error log events).
1244740	FortiAuthenticator allows a maximum of 255 TACACS+ service attributes.
1244779	Sponsor user able to read Guest Portals resource.
1245178	Incorrect FSSO filtering when domain, e.g. `dc=domain,dc=com`, is root DN of 2nd distinct domain (e.g. `dc=test,dc=domain,dc=com`).
1246202	Error `CRL file size is too large` when importing relatively small CRL file.
1246207	500 Internal server error when browsing the IdP entity ID URL copied from the admin UI.
1246232	Remote LDAP sync rule fails if imported user was promoted to Administrator role through admin UI.
1246579	OAuth does not work when authorizating with LDAP groups filter.
1247496	`radsecproxy` timeout value is too small.
1247625	End users able to reconnect for 30-90 secs after exceeding their usage profile data usage limit.
1247697	500 error in admin UI when editing user group if it contains unknown RADIUS attribute.
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.
1252729	Activation code for offline token activation cannot be used.
1252988	Upgrade to `Django` 4.2.28.
1253004	Upgrade to `curl` 8.19.0.
1253026	Upgrade to `pyasn1` 0.6.2.
1253028	Upgrade to `filelock` 3.20.3.
1253031	Upgrade to `protobuf` 5.29.6.
1253102	Upgrade to `libpng` 1.6.55.
1253114	Upgrade to `libgnutls` 3.8.9-3+deb13u1.

Bug ID	Description
1253231	PATCH to REST API `/api/v1/radiususers/[ID]/` endpoint to update `mobile_number` fails.
1254806	Upgrade to `libexpat` 2.7.4.
1256685	Upgrade to `PostgreSQL`15.16.
1256885	Upgrade to `python-pillow` 12.1.1.
1256955	Revoked client certificate (included in CRL) with serial number length less than 16 is not blocked by EAP-TLS.
1257302	Inconsistent result when filtering on `/api/v1/localusers` API endpoint with offset parameter.
1258090	Guest portal rules not working.
1258275	Upgrade to `pyca/cryptography` 46.0.5.
1258276	Upgrade to `sqlparse` 0.5.5.
1258815	Upgrade with multiple templates should not break the admin login page.
1261920	SAML IdP is leaking sessions for dead URLs causing infinite `/tmp` growth.
1264801	SAML Trusted Endpoint SSL fails when LDAP group membership list includes non-ascii characters.
1265328	Optimize private key loading calls in SAML IdP.
1266776	Logs to FortiAnalyzer does not contain enough details in the Message field.
1266816	DB is not rolled back in case of error in SAML.
1266831	relation `saml_respondedspsessiondata` does not exist.
1266898	Unable to import local users via CSV.
1268077	Unable to import the local users CSV file via GUI when the user has OTP enabled.

Common Vulnerabilities and Exposures

Bug ID	CVE references
1200473	FortiAuthenticator 8.0.2 is no longer vulnerable to the following CVE-Reference (s): • CVE-2025-57052
1211039	FortiAuthenticator8.0.2 is no longer vulnerable to the following CVE-Reference (s): • CVE-2025-9230

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 the source IP instead of the LDAP client IP address.
971708	Avoid using the default 'admin' account in AWS since restoring config resets the password to `instance-id`.
997200	SAML IdP proxy not able to retrieve group memberships from the 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).
1026106	Failed to add new FIDO key in Chrome with Bitwarden extension.
1033509	Log message should be recorded when the SAML user session expires.
1068878	Unable to access FortiAuthenticator portals with IPv6 address if interface does not also have IPv4 address.
1084583	Exporting raw logs does not reflect filter selection on GUI.
1128643	FortiAuthenticator does not include rootCA cert in CMP Initialization Response as required by `3GPP TS.33.310`.
1133973	Delay in updating user counts after CSV import.
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.
1139476	Gateway Timeout when loading local users page with large number of users.
1140601	CLI logins attempts that fail without a successful follow-up are not being logged.
1143190	Self-service portal shows empty page when all post-login options are disabled.
1144845	FortiAuthenticator should not present SAML captcha when performing proxy authentication.
1145628	SAML IdP FIDO authentication fails on first try after FortiClient disconnect/reconnect.

Bug ID	Description
1148829	SCEP enrollment fails when certmonger client sends large GET request URI (exceeds maximum length of 8190 bytes).
1189168	Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboot.
1196760	Failed to restore configuration just after factory reset due to `Database restore failed:`.
1196880	Mismatched cert/key in LB secondary.
1201488	GUI unable to display the imported image as previous releases.
1203907	Guest portal not displaying correct message when the user or source IP is locked out.
1203911	FortiAuthenticator should record a log when guest portal is created/edited/deleted.
1203923	Guest portal creation should not be allowed without a default language.
1204521	Zero Trust Tunnel continues working even after server certificate is revoked.
1237187	SCEP requests fail to complete; getCA request fails when using ECC CA certificate.
1238176	Certificate issuer is blank on the emote SAML server page.
1247171	FortiAuthenticator SAML IdP user source setting 'search local users first' has no effect. It is called after authentication.
1250768	Getting an `encoding failed` error when FortiGate sends a CSR over SCEP using an ECC key type.
1253985	Server groups on user source page should match the selected server.
1256620	Confusing success message after saving guest portal label in admin UI.
1256659	Timezone in the guest portal rule should be required by the admin UI.
1257979	No log when deleting a local user through REST API.

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)

Feature	Calculating metric	300F	800F	3000F
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
User Certificate Bindings	Users x 2	3000	16000	80000
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

Feature	Calculating metric	300F	800F	3000F
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

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

User Management

Feature	Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
Users (Local + Remote)[1]	5	**********	100	5000
User RADIUS Attributes	15	Users x 3	300	15000
User Groups	3	Users / 5	20	1000
Group RADIUS Attributes	9	User groups x 3	30	1500
User Certificate Bindings	10	Users x 2	200	10000
FortiTokens	10	Users x 2	200	10000
FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
LDAP Entries	20	Users x 2	200	10000
Device (MAC-based Auth.)	5	Users x 5	500	25000
Remote LDAP Users Sync Rule	1	Users / 10	10	500
Remote LDAP User Radius Attributes	15	Users x 3	300	15000
Realms	2	Users / 25	4	200

FSSO & Dynamic Policies > FSSO

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

FSSO & Dynamic Policies > Accounting Proxy

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

Certificates > User Certificates

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

Certificates > Certificate Authorities

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

Certificates > SCEP

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

Certificates > CMP

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

Services

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

[1] Users includes both local and remote users.

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

Data-at-rest protection

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

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

www.fortinet.com