Release Notes

FortiAuthenticator 8.0.3

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

April 29, 2026
FortiAuthenticator 8.0.3 Release Notes
23-803-1276583-20260429

TABLE OF CONTENTS

Change log

Date	Change Description
2026-04-21	Initial release.
2026-04-29	Updated Upgrade instructions on page 10 and Upgrading from 4.x/5.x/6.x on page 11.

FortiAuthenticator 8.0.3 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 8.0.3, build 0099.

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 8.0.3, 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 8.0.3 is a patch release.

There are no new features. See Resolved issues on page 19 and Known issues on page 20 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 8.0.3 requires at least 16 GB of RAM.

When FortiAuthenticator 8.0.3 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 8.0.3 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 8.0.3 supports:

- FortiAuthenticator 300F
- FortiAuthenticator 800F
- FortiAuthenticator 3000F
- FortiAuthenticator VM
  See Virtualization software support on page 16.

Image checksums

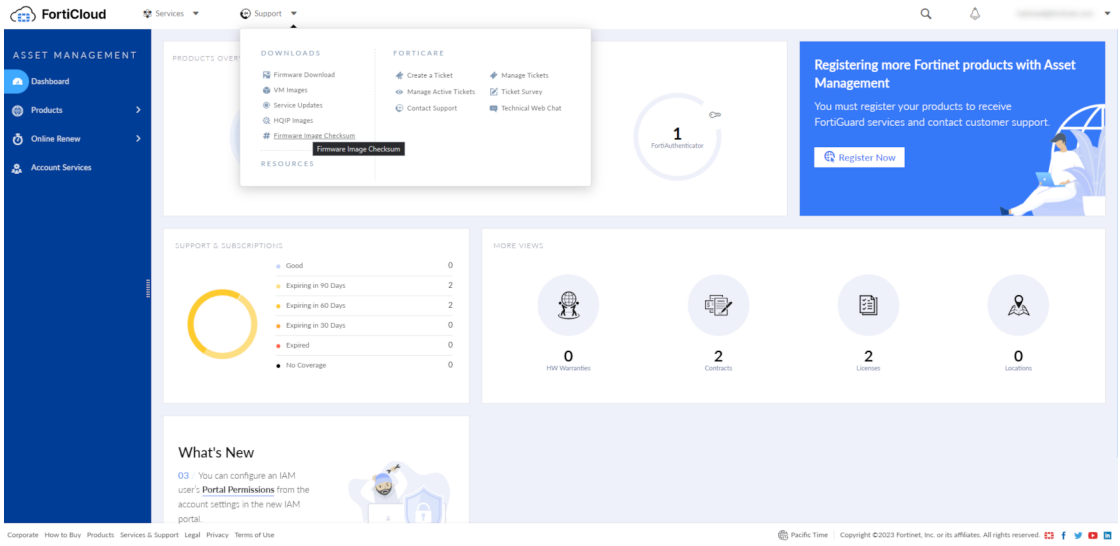
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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 8.0.3 build 0099 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 8.0.3, 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 8.0.3 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 8.0.3.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 8.0.3 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 8.0.3 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 13.

Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

Ensure the hypervisor provides at least 16 GB of memory to the FortiAuthenticator-VM.

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 8.0.3, 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 8.0.3

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 8.0.3:

Google Chrome version 147
Microsoft Edge version 147
Mozilla Firefox version 149

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

FortiOS support

FortiAuthenticator 8.0.3 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 8.0.3 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 8.0.3 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 18 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
1273259	IAM user API is broken.
1276841	Upgrade to `pyca/cryptography` 46.0.6.
1276851	Upgrade to `lodash` 4.18.1.
1279437	SSLVPN authentication with FortiClient does not trigger FortiToken push.
1280659	RADIUS service crashes during EAP-TLS authentication if client certificate has no `akid`.

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 address instead of the LDAP client IP address.
971708	Avoid using the default 'admin' account in AWS since restoring config resets its password to `instance-id`.
973414	Downloading large Summary Debug Report from the GUI leads to Gateway Timeout Error.
997200	SAML IdP Proxy not able to retrieve group memberships from the remote OpenLDAP server.
1010053	Gateway Timeout Error on GUI when performing a Manual Sync for a Remote User Sync Rule with a large number of users (users synced).
1026106	Failed to add new FIDO key in Google Chrome with Bitwarden extension.
1033509	Log message should be recorded when SAML user session expires.
1068878	Unable to access FortiAuthenticator portals with IPv6 address if interface does not have IPv4 address.
1084583	Exporting raw logs does not reflect filter selection on the GUI.
1128643	FortiAuthenticator does not include rootCA cert in CMP Initialisation Response as required by 3GPP TS.33.310.
1133973	Delay in updating user counts after CSV import.
1134745	Changes to adaptive MFA rules in the admin UI are not logged.
1134748	Generate a log entry when creating, editing, or 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 a large number of users.
1140601	CLI logins attempts that fail without a successful follow-up are not being logged.
1143190	Self-service portal shows empty page when all the post-login options are disabled.
1144845	FortiAuthenticator should not present SAML captcha when doing proxy authentication.
1145628	SAML IdP FIDO authentication fails on the first attempt after FortiClient

Bug ID	Description
	disconnects/reconnects.
1148829	SCEP enrollment fails when certmonger client sends a large GET request URI (exceeds maximum length of 8190 bytes).
1180386	Permanent IP address based lockout cannot be unlocked in the GUI.
1187237	Add support to modify debugging level for LB sync daemon from the admin UI.
1189168	Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboots.
1196760	Failed to restore configuration just after factory reset due to `Database restore failed`.
1196880	Mismatched Cert/key in the secondary LB side.
1201488	GUI unable to show the imported image as the previous release.
1203907	Guest portal not showing correct message when user or source IPaddress 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.
1232772	`SubjectAltName` have all values in one line separated by comma.
1237187	SCEP requests fail to complete; getCA request fails when using ECC CA certificate.
1238176	Certificate issuer is blank on the remote SAML server page.
1244672	500 Internal Server Error if injecting a long parameter value into the password reset 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 the user source page should match the selected server.
1256620	Confusing success message after saving guest portal label in admin UI.
1257765	TACACS+ service may fail to restart after config changes.
1257974	Logging to FortiAnalyzer Cloud fails due to missing SNI.
1257979	No log when deleting local user through REST API.
1277881	DB remote user column length is too short.
1282907	Typo in REST API response to create new user: 'status' is misspelled 'statue'.

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

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

Feature	Calculating metric	300F	800F	3000F
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

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