FORTINET

Release Notes

FortiAuthenticator 6.5.3

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

November 6, 2023
FortiAuthenticator 6.5.3 Release Notes
23-653-933486-20231106

TABLE OF CONTENTS

Change log

Date	Change Description
2023-07-20	Initial release.
2023-08-29	Updated Upgrading from 4.x/5.x/6.x on page 9.
2023-09-28	Updated Maximum values for hardware appliances on page 19.
2023-11-06	Added bug 937201 to Known issues on page 17.

FortiAuthenticator 6.5.3 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.5.3, build 1355.

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.

What's new

FortiAuthenticator version 6.5.3 is a patch release. There are no new features. See Resolved issues on page 15 and Known issues on page 17 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 6.5.3 requires at least 4GB of RAM.

Hardware and VM support

FortiAuthenticator 6.5.3 supports:

- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400E
- FortiAuthenticator 800F
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000E
- FortiAuthenticator 3000F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, Oracle OCI, and Alibaba Cloud)

Image checksums

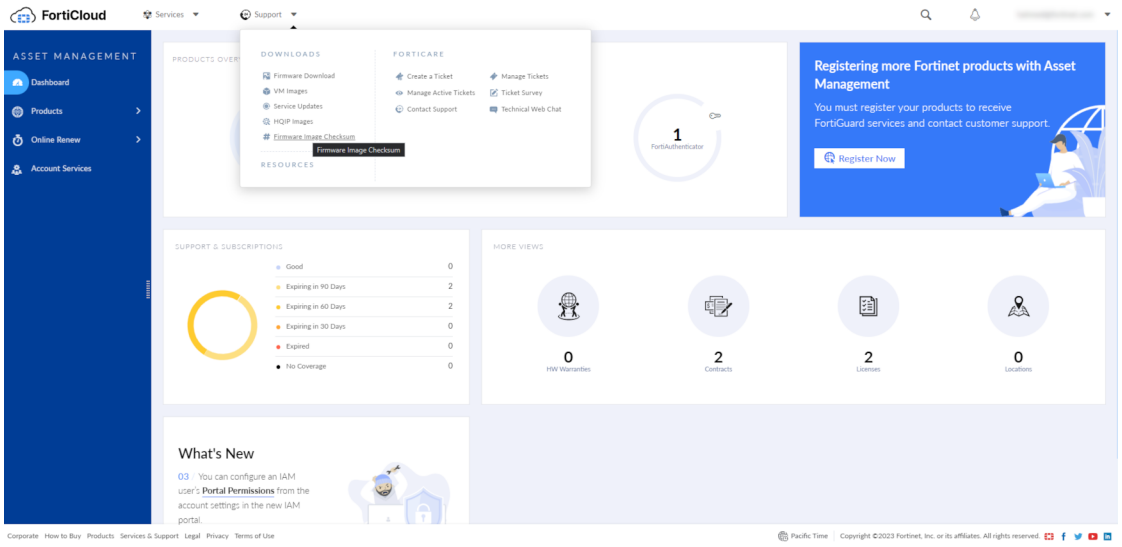
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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 6.5.3 build 1355 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 6.5.3, 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 6.5.3 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.5.3.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 6.5.3 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.5.3 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 10.

Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

Ensure the hypervisor provides at least 4GB 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 6.5.3, 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. 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 6.5.3

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 6.5.3:

- Microsoft Edge version 114
- Mozilla Firefox version 115
- Google Chrome version 114

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

FortiOS support

FortiAuthenticator 6.5.3 supports the following FortiOS versions:

- 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 6.5.3 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.

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 6.5.3 supports:

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

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 14 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 visit FortiCloud.

Bug ID	Description
922632	FortiGate FortiCloud SSO IAM login.
915248	500 internal server error when importing remote LDAP groups as SSO groups.
919817	RADIUS Access-Accept does not return User-Name as UPN.
829365	Azure admin password reset is not working reliably.
927907	Occasional 500 error after an admin logs in.
915898	Root CA key and certificate can be exported after modifying the GUI.
931970	FortiAuthenticator 2000E power supply monitor should show PSUs as vertically aligned.
918513	Trusted endpoint SSO fails with FortiAuthenticator sending TCP RST to client.
930090	Collapse buttons in *Monitor* > *SSO* > *Domains* page does not work.
923977	Change the scope type to something more readable.
917607	Inability to assign identical claim names to different relying parties.
920749	Authentication API response is missing the message field.
914030	FortiAuthenticator does not reach 100% of the processed windows events and experiences delays.
928812	GUI error when creating a new OAuth relying party.
922839	OAuth response contains scopes even when they are not configured for the relying party.
919820	CA certificate Advanced Options: Key Usages section elements misformatted.
921791	The user registration on a captive portal is not working after successful token verification.
926151	Inline script cannot be executed in the *User Registration Confirmation* and *User Registration Receipt* pages.
876897	FortiAuthenticator memory usage showing in the widget does not match with memory usage from SNMP (`facSysMemUsage`).
908291	FortiAuthenticator does not properly revoke a user certificate.
926650	500 error when registering a portal device.
917321	500 error when creating a RADIUS policy with MAB and eduroam enabled.
921574	Having enabled HTTP-POST in the SP for SAML IAM login results in 403 error.
915152	Remote sync rule assigns a new mobile token again after the OTP is manually disabled for the user.
908142	Using Yubikey as OTP second factor increases drift/counter unexpectedly.

Bug ID	Description
924305	An `Uncaught TypeError: o.includes is not a function` error in *Authentication* > *User Management* > *Local Users*.
927254	Revoke button for the root CA should be grayed out.
925486	JavaScript error when trying to log off an FSSO session.
925741	JS error `o.includes is not a function` shows up on several GUI pages.
926693	REST API - Internal server error while trying to modify existing RADIUS attributes using PUT call.
906339	RADIUS attributes cannot be added to local users via REST API (Error: `local variable 'vendor' referenced before assignment`).
927110	Admin GUI message when using the trusted endpoint SSO feature.
926587	OAuth - Internal server error while trying to get an authentication code when no scopes are configured for the RP.
925860	REST API debug report not decrypting properly.
923596	Preserve the scopes when upgrade from 6.4.
861557	Remote user sync rules - Set group filter is not working if OU has special characters in name, e.g., `(` , `)` , `+`.
901379	HA cluster failover causes FortiAuthenticator to give up on logging.
923401	SAML FSSO returns error 403 when the FSSO session is removed.
921975	Same OAuth relying party scope created multiple times.
925303	*Authorize* or *Deny* page does not show up in the code base for OAuth relying party.
919706	FIDO login with remote admin users fail on the SAML IdP portal due to an attribute error.
917772	Trusted endpoint SSO produces 500 internal server error when an AzureAD workstation joins by using a custom domain name.
905593	Admin username is missing from the log details after an upgrade.
918507	Portals not saving the *Restrict token self-provisioning to members of specific groups* setting.
919755	500 error after successful SAML authentication with local admin user on a FIDO portal.
915713	Trusted SSO default port 8008 is in conflict with the FortiGate default open `http` port 8008 for FortiGuard.
921007	SAML token retry error on FIDO authentication when previous FIDO authentication has failed.
919326	Memory leak in the `fn_hash_table` if a collision occurs.
901776	SAML logout using POST will return `CSRF token missing or incorrect` (HTTP 403).
918778	Hide deprecated models from the `tablesizes.html` output.
899836	Passwords expires one day earlier than expected.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit FortiCloud.

Bug ID	Description
920262	Some of the users logged in a MAC device are unable to get user sessions listed on FortiAuthenticator.
931960	radiusd appears to be stale with `unfinished request in component authenticate module facauth` that matches no Access-request ID.
929279	Self-service portal password change fails for remote LDAP users.
929943	Push authentication does not work on the FortiAuthenticator Windows agent when using FortiTrust Identity.
929004	Unable to add longer mobile phone numbers for certain country codes.
929090	FortiAuthenticator issues with User Principal Name (UPN) and tokens.
922921	Old and newly revoked certificates in FortiAuthenticator 6.5.2 GA shows active if the revocation reason is 'unspecified.'
932783	*FAC2KE PSU Monitor* widget does not accurately reflect the actual statuses of the PSUs on the device.
887081	SAML: Launching SP-initiated SAML session for a user with FIDO AUTH produces server errors,
924446	500 error for remote user on SAML portal with both FIDO and FortiToken Mobile/FortiToken Cloud tokens.
920970	Preview mapping does not work under remote user sync rule.
928034	Issue authenticating IPsecVPN IKEv2 EAP (MSCHAPv2) to FortiAuthenticator + remote RADIUS server.
924632	FortiAuthenticator not able to return more than 100 groups from Azure AD when using SSOMA.
869867	FortiAuthenticator SSO database is not updating on time when the domain users switch from wireless to wired or vice versa.
923405	Enrollment request made to the secondary unit not synchronized to the primary unit after it takes control again.
928643	radiusd cannot handle two parallel authentication sessions and removes partially authenticated user when the second attempt happens.
913981	Non-admin SAML FIDO authentication ends with error 500.
929462	Internal server error: `/guests/social/register/`.
900550	2FA codes via SMS is not working.
924321	Second factor setup against PEAP-MSCHAPv2 client fails with `EAP authentication failed due to missing token`.
894888	User lookup does not display token information with view-only admin profiles.

Bug ID	Description
907286	FortiAuthenticator LDAP server does not support PW+OTP concatenation for FortiToken Cloud-issued FortiToken Mobile tokens.
904353	Daylight saving time (DST) time zone change for Egypt starting end of April.
876009	FortiAuthenticator ignores the groups filtering rules and sends all the SSO groups to FortiGate if the FortiGate is configured with FQDN.
878854	Remote LDAP usernames greater than 255 character fails to authenticate through SSL VPN.
900664	Certificate only smart connect in iOS does not work.
801933	FortiAuthenticator as an LDAP server: log shows `LDAP_FAC` in the *Source IP* field.
756414	Incorrect Italian translation of *Next* button displayed on the reset password page.
909342	The status of the hardware tokens is "Missing seed" if imported through the serial number file.
908091	When timezone = GMT, London, user audit report download fails with internal server error 500.
928334	Incorrect message on the landing page for `No-Access-Admin` login.
816070	DB issue if the power is down during a short window when booting from factory reset.
925924	Unable to get SSO session on FortiAuthenticator when using UPN to login.
937201	Synchronization rule without an OTP method generates excessive logs.

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.

Feature		Model							
		200E	300F	400E	800F	1000D	2000E	3000E	3000F
System									
Network	Static Routes	50	50	50	50	50	50	50	50
Messages	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
Administration	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		20	60	80	320	400	800	1600	1600
Authentication									
General	Auth Clients (NAS)	166	500	666	2666	3333	6666	13333	13333

Feature	Model							
	200E	300F	400E	800F	1000D	2000E	3000E	3000F
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	50	150	200	800	1000	2000	4000	4000
Group RADIUS Attributes	150	450	150	2400	600	6000	12000	12000
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

Feature		Model							
		200E	300F	400E	800F	1000D	2000E	3000E	3000F
Remote authentication servers	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
FSSO & Dynamic Policies									
FSSO	FSSO Users	500	1500	2000	8000	10000	20000	200000[3]	200000
	FSSO Groups	250	750	1000	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 Services	50	150	200	800	1000	2000	4000	4000
	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

Feature		Model							
		200E	300F	400E	800F	1000D	2000E	3000E	3000F
Accounting Proxy	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	User Certificates	2500	7500	10000	40000	50000	100000	200000	200000
	Server Certificates	50	150	200	800	1000	2000	4000	40000
Certificate Authorities	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
SCEP	Enrollment Requests	2500	7500	10000	40000	50000	100000	200000	200000

[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
User Management	**Users** (Local + Remote)[1]	5	**********	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
	Realms	2	Users / 25	4	200
FSSO & Dynamic Policies					

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

[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.

www.fortinet.com