FortiAuthenticator - Release Notes

Version 6.1.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 8, 2023
FortiAuthenticator 6.1.3 Release Notes
23-613-890551-20230308

TABLE OF CONTENTS

Change log

Date	Change Description
2023-03-08	Initial release.

FortiAuthenticator 6.1.3 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.1.3, build 0422.

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.

Upgrading from FortiAuthenticator 4.x/5.x/6.0.x

FortiAuthenticator 6.1.3 build 0422 officially supports upgrade from FortiAuthenticator 6.0.4 and higher.

All earlier versions of FortiAuthenticator must first be upgraded to 6.0.4 before upgrading to 6.1.3, otherwise the following message will be displayed: `Image validation failed: The firmware image model number is different from the appliance's.`

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

What's new

FortiAuthenticator version 6.1.3 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.

Hardware and VM support

FortiAuthenticator 6.1.3 supports:

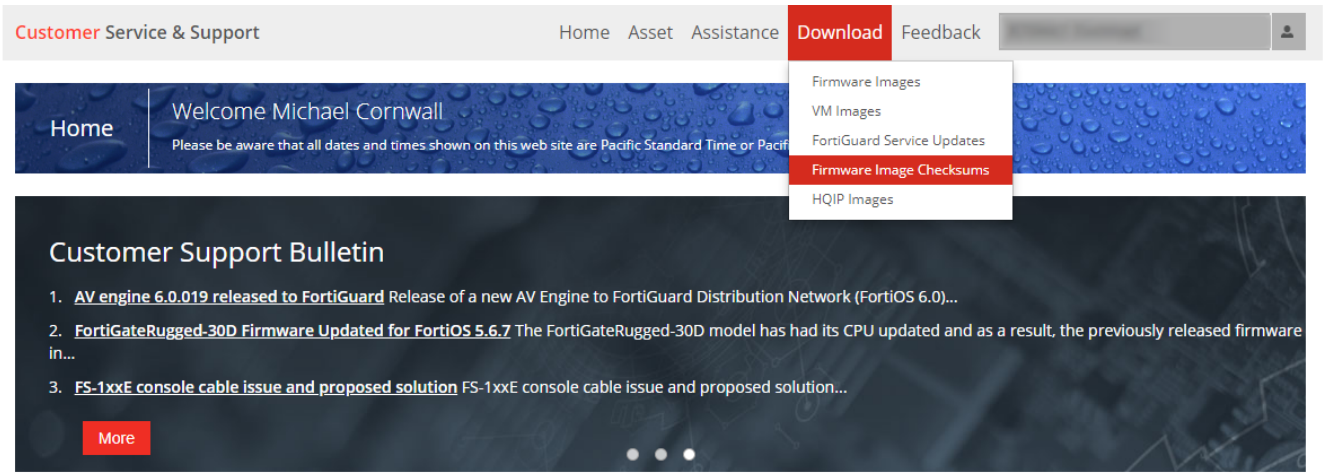
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, and Oracle OCI)

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 from the Fortinet Support website.

Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

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

Upgrading from FortiAuthenticator 4.x/5.x/6.0.x

FortiAuthenticator 6.1.3 build 0422 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 6.1.3, 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 or newer, then upgrade to 6.1.3 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.1.3 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.

Firmware upgrade process

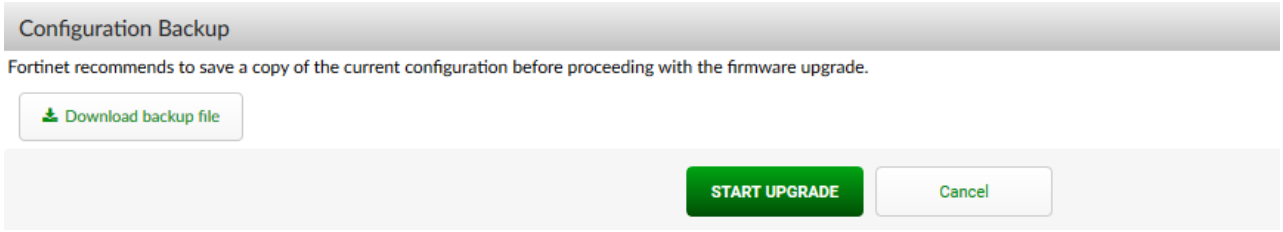
First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** 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 Checksums** 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:



   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 6.1.3, 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 6.1.3

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

Web browser support

The following web browsers are supported by FortiAuthenticator 6.1.3:

- Microsoft Edge 110
- Mozilla Firefox version 109
- Google Chrome version 110

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

FortiOS support

FortiAuthenticator 6.1.3 supports the following FortiOS versions:

- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x
- FortiOS v5.6.x
- FortiOS v5.4.x

Fortinet agent support

FortiAuthenticator 6.1.3 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (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.
- 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.

Virtualization software support

FortiAuthenticator 6.1.3 supports:

- VMware ESXi / ESX 4/5/6
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM)
- Amazon AWS
- Microsoft Azure
- Oracle OCI

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 the Fortinet Support website

Bug ID	Description
803891	SAML peer certificate expiration issue and XML security issue.
791452	OpenSSL 1.1.1n - Infinite loop in `BN_mod_sqrt()` reachable when parsing certificates (CVE-2022-0778).
800714	[3rd party component upgrade required for security reasons] FortiAuthenticator- OpenLDAP to 2.6.2.
837219	FortiAuthenticator-VM on same Hyper-V host cannot form HA A/A cluster after July 2022 Windows Updates.
814167	[3rd party component upgrade required for security reasons] FortiAuthenticator - libxml2 to 2.9.14.
861776	Upgrade OpenSSL from 1.1.1n to 1.1.1s, then again to 1.1.1t.

Common Vulnerabilities and Exposures

FortiAuthenticator is no longer vulnerable to the following CVE-Reference(s):

Bug ID	CVE references
791452	CVE-2022-0778

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

Known issues

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

Bug ID	Description
694664	FortiAuthenticator Agent with group exclusion is throwing a COMException error when accessing AD to check group membership.
876897	FortiAuthenticator memory usage showing in the widget is not matching with memory usage from SNMP (`facSysMemUsage`).
869867	FortiAuthenticator SSO database is not updating on time when domain users switch from wireless to wired or vice versa.
877432	Selecting Cloud option for group membership on SAML SP and will display 500 error if we do not select an OAuth server.
566145	Usage Profile `TIME USAGE=Time used` is not triggering COA or disconnect request to FortiGate.
775006	Occasionally, multiple SMS are received after LDAP user import instead of just one.
780558	When creating CA certficiate debug logs sometimes show error.
814255	Custom RADIUS attributes disappear on HA secondary after failover and we get 500 crash when clicking the RADIUS policy.
816070	DB issue if power down during a short window when booting from the factory reset.
787852	TACACS+ attribute value pair for authorization services shows undefined entries.
843334	KVM model does not obey hypervisor soft restart/shutdown commands.
863635	FIDO users status bug on SAML.
866392	FortiAuthenticator GUI/captive portal access freezes and becomes unresponsive during peak hours.
868836	TACACS+ failed authentications not counting towards IP lockouts.
870678	Recovery password and recovery token fail to send alternative email address.
854050	It takes a long time for FortiAuthenticator to reflect active certificates in the GUI after successful SCEP enrollment request.
876703	Not able to view supported methods and available fields using `/schema` at the end of the endpoint.
878673	Certificate GUI filter by status times out when there are thousands of revoked certificates.
879570	*Select All* checkbox for Remote User Sync rule does not select all rules for Firefox without private window.

Bug ID	Description
808748	Self-service portal password change fails for remote LDAP users if UPN format is used.
781832	Token bypass not working for FIDO enabled self-service portal.
743775	SCEP Get CA requests intermittently fail under high SCEP load.
857399	FortiAuthenticator fails send out COA disconnect to FortiGate.
868829	IP lockout not being logged in on FortiAuthenticator logs.
871533	Incorrect FIDO token does not count towards user lockout.
874285	Unable to use FortiAuthenticator images in System replacement messages.
837791	TACACS+ authentication fails when the authentication process takes long.
881296	SNMP v3 with non-ENG letter pass gives authentication failed.
876009	FortiAuthenticator ignores the groups filtering rules and send all SSO groups to FortiGate if FortiGate is configured with FQDN.
751108	FortiAuthenticator does not support admin OIDs from `FORTINET-CORE-MIB` properly.
801933	FortiAuthenticator as LDAP server; logs show `LDAP_FAC` in the *Source IP* field.
620127	Changing from `maint-mode-no-sync` to `maint-mode-sync` does not restore syncing.
873050	It show 403 Forbidden while do SAML authentication after OAuth succeeds.
755752	Power supplies show voltage input fault on both CLI and GUI.
865372	FortiNAC can overwhelm FortiAuthenticator with 'many' TACACS+ logins on the same service account.
866709	Admin password recheck issues.
837728	Local services cannot use cert with >97 character subject length.
872920	Portal policy realms table values are in the wrong column.
861027	RADIUS attribute name should be only unique within the dictionary, not across all dictionaries.
861112	NTLM authentication does not work with child domain.
878665	500 error when launching a Smart Connect profile that contains a CSR for Android.
741765	REST API `/api/v1/tacpluspolicyclient/` endpoint does not recognize `policy_name` or `client_name` parameters.
861557	FortiAuthenticator Remote User Sync rules - Set Group Filter not working if OU have special characters in name, e.g., `( , ) , +`.
868810	FortiAuthenticator HA device with low priority is stays as primary.
842886	Upgrading FortiAuthenticator in HA-LB removes the MAC-address records form the LB node.
861611	Smart Connect for Android running on version 12 and 13 never installed the configuration profile.
871196	LDAP disconnects every few seconds.

Bug ID	Description
838976	Windows log events in FSSO are dropping after some time.
873972	Single group is passed by FortiAuthenticator as an IdP when FIDO only authentication is used in SP settings.
882098	FortiAuthenticator HA is out of sync and web server crashes when clicking on *Packet Capture* with 500 Internal server error.
680776	AP HA secondary cannot change `mgmt` interface access configuration, and the option does not sync from the primary either.
875536	User account extension gives `CSRF token missing or incorrect`.
850023	HA Cluster not forming due to difference in the SmartConnect primary key name (upgrade path mismatch, but should work).

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 maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model				
		200E	400E	1000D	2000E	3000E
System						
Network	Static Routes	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20
	SMS Gateways	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20
	User Uploaded Images	39	114	514	1014	2014
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333
	Users (Local + Remote)[1]	500	2000	10000	20000	40000
	User RADIUS Attributes	1500	6000	30000	60000	120000
	User Groups	50	200	1000	2000	4000
	Group RADIUS Attributes	150	150	600	6000	12000
	FortiTokens	1000	4000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200
	LDAP Entries	1000	4000	20000	40000	80000
	Device (MAC-based Auth.)	2500	10000	50000	100000	200000
	RADIUS Client Profiles	500	2000	10000	20000	40000

Feature		Model				
		200E	400E	1000D	2000E	3000E
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Users Sync Rule	50	200	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120000
FSSO & Dynamic Policies						
FSSO	FSSO Users	500	2000	10000	20000	200000[3]
	FSSO Groups	250	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	400
	RADIUS Accounting SSO Clients	166	666	3333	6666	13333
	FortiGate Services	50	200	1000	2000	4000
	FortiGate Group Filtering	250	1000	5000	10000	20000
	FSSO Tier Nodes	5	20	100	200	400
	IP Filtering Rules	250	1000	5000	10000	20000
Accounting Proxy	Sources	500	2000	10000	20000	40000
	Destinations	25	100	500	1000	2000
	Rulesets	25	100	500	1000	2000
Certificates						
User Certificates	User Certificates	2500	10000	50000	100000	200000
	Server Certificates	50	200	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50
	Trusted CA Certificates	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	50000	100000	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.

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 (NAS devices) 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	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
	Authentication Policy (NAS)	6	Users	100	5000

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
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 Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
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	2500	10000

[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.