FortiAuthenticator - Release Notes

Version 6.1.1

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

January 4, 2022
FortiAuthenticator 6.1.1 Release Notes
23-611-631882-20220104

TABLE OF CONTENTS

Change log

Date	Change Description
2020-05-15	Initial release.
2020-05-19	631715 moved to Resolved issues on page 16.
2020-05-20	Updated Windows Agent for Microsoft Windows support.
2020-07-30	Note added about upgrading from FAC-3000E models on 6.0.x to Upgrade instructions on page 8.
2022-01-04	Updated Upgrade instructions on page 8.

FortiAuthenticator 6.1.1 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.1.1, build 0413.

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 6.1.1 build 0413 officially supports upgrade from FortiAuthenticator 6.1.0 and 6.0.4.

All other versions of FortiAuthenticator must first be upgraded to 6.0.4 before upgrading to 6.1.1, 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 6.1.1 includes the following new features and enhancements:

SAML IdP: 0365 Azure/ADFS hybrid support

To better support O365 Azure/ADFS hybrid environments, a new **LDAP/ms-DS-ConsistencyGuid** option is available in the **Subject NameID** dropdown in **Authentication > SAML IdP > Service Providers** when adding or editing a service provider.

HA: Failover sensitivity settings

This feature offers the ability to adjust the default HA failover parameters when a FortiAuthenticator is configured as an HA active cluster member:

- **Heartbeat interval**: Number of milliseconds between each HA heartbeats sent to the other cluster member. The default value is 1000 milliseconds.
- **Heartbeat loss threshold**: Number of consecutive heartbeats from the other active cluster member that must be missed before declaring it out-of-service. The standby member uses this measure to trigger a failover. The default value is 6.

You can modify these settings at **System > Administration > High Availability** or in the CLI.

FTM: Hosted Push Proxy server for FortiToken Mobile push

FortiAuthenticator now sends the FortiToken Mobile push request to a FortiGuard/FortiCloud push proxy.

In order to support the FTM push feature, FortiAuthenticator must be able to reach **push.fortinet.com** over **TCP/443**.

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 6.1.1 supports:

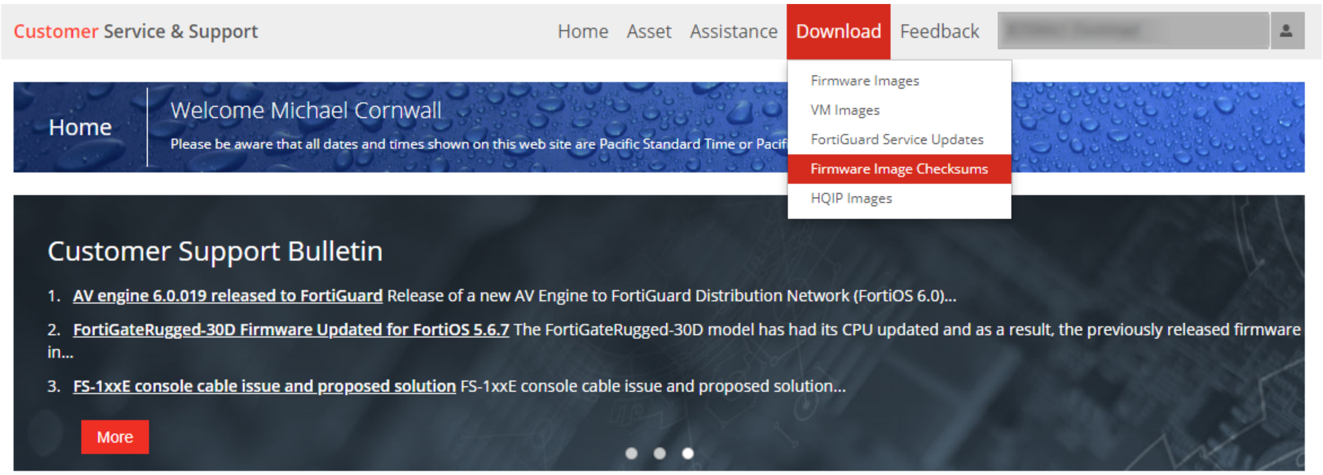
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, and Oracle OCI)

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



Welcome Michael Cornwall

Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacif

Customer Support Bulletin

1. AV engine 6.0.019 released to FortiGuard Release of a new AV Engine to FortiGuard Distribution Network (FortiOS 6.0)...
2. FortiGateRugged-30D Firmware Updated for FortiOS 5.6.7 The FortiGateRugged-30D model has had its CPU updated and as a result, the previously released firmware in...
3. FS-1xxE console cable issue and proposed solution FS-1xxE console cable issue and proposed solution...

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 6.1.1 build 0413 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 6.1.1, 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 6.1.1 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.1.1 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.

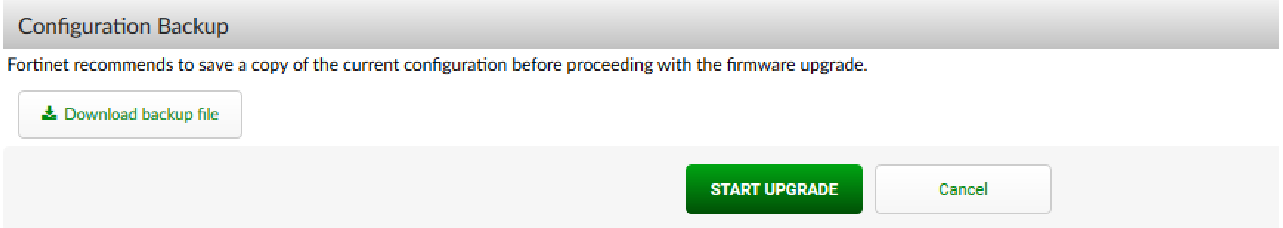
Firmware upgrade process

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.
   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:



Configuration Backup

Fortinet recommends to save a copy of the current configuration before proceeding with the 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 6.1.1, 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 6.1.1

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 6.1.1:

- Microsoft Edge 44
- Mozilla Firefox version 74
- Google Chrome version 80

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

FortiOS support

FortiAuthenticator 6.1.1 supports the following FortiOS versions:

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

Fortinet agent support

FortiAuthenticator 6.1.1 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.5 and 3.0.
- FortiAuthenticator Agent for Outlook Web Access 1.6
- 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 6.1.1 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

FortiAuthenticator-VM system requirements

The following table provides a detailed summary on FortiAuthenticator virtual machine (VM) system requirements. Installing FortiAuthenticator-VM requires that you have already installed a supported VM environment. For details, see the FortiAuthenticator VM Install Guide.

VM requirements

Virtual machine	Requirement
VM form factor	Open Virtualization Format (OVF)
Virtual CPUs supported (minimum / maximum)	1 / 64
Virtual NICs supported (minimum / maximum)	1 / 4
Storage support (minimum / maximum)	60 GB / 16 TB
Memory support (minimum / maximum)	2 GB / 1 TB
High Availability (HA) support	Yes

FortiAuthenticator-VM sizing guidelines

The following table provides FortiAuthenticator-VM sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

VM sizing guidelines

Users	Virtual CPUs	Memory	Storage*
1 - 500	1	2 GB	1 TB
500 to 2,500	2	4 GB	1 TB
2,500 to 7,500	2	8 GB	2 TB
7,500 to 25,000	4	16 GB	2 TB
25,000 to 75,000	8	32 GB	4 TB
75,000 to 250,000	16	64 GB	4 TB

Users	Virtual CPUs	Memory	Storage*
250,000 to 750,000	32	128 GB	8 TB
750,000 to 2,500,000	64	256 GB	16 TB
2,500,000 to 7,500,000	64	512 GB	16 TB

*1TB is sufficient for any number of users if there is no need for long-term storage of logs onboard FortiAuthenticator.

FortiAuthenticator-VM firmware

Fortinet provides FortiAuthenticator-VM firmware images in two formats:

- **.out**
  Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip / kvm.zip / hyperv.zip / xen.zip**
  Used for new VM installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site.

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
452967	Error when setting allowed-hosts: bad option in substitution expression.
583516	Gateway timeout error when downloading user audit report.
601990	Guest users expiring due to a usage profile change to *unspecified* and cannot be purged.
604935	Remote User Re-enable button says *You do not have a permission to perform such operation* when user has the correct permission.
606405	Regular User should not be able to edit/view user profile page if they do not have permissions.
606471	Syslog FSSO user disappear after the remote user was enabled.
608873	*An error has occurred* when downloading User Audit Reports.
610259	In the GUI, creating or editing *MAC Device* is very slow in Google Chrome.
610812	RADIUS Policy unable to select default local realm through specific steps.
612695	FortiAuthenticator sends DNS requests for the Client subnets configured in RADIUS accounting clients.
613224	Gateway timeout when clicking *User Lookup* page in FortiAuthenticator which has 55k user loaded.
613523	HA flapping when adding a load-balancer in original standalone primary.
614381	Load-balancer warning *Version mismatch* when the versions are the same.
615444	Cannot disable Kerberos login in the web GUI.
616370	Newly created CRL can not be downloaded by the provided HTTP link before clicking *Export* on FortiAuthenticator GUI.
618092	User passwords in plaintext with RADIUS debug mode enabled.
618308	User Portal doesn't redirect to Login page after successful password reset.
618877	FortiGate Filters are not syncing with FortiGate FSSO Fabric agent Connectors.
622534	FortiToken Cloud status shouldn't be reported as "Service Error" when no FTC license purchased.
622839	Seeing strange log messages on console port upgrading from 6.0.4 to 6.1.0.
622846	Upgrade FAC-VM-KVM / FAC-VM-XEN to v6.1.0 GA failed.
622887	EAP cannot use an imported server certificate which already has serverAuth extended key usage.
622931	Login page doesn't load if *Enable pre-authentication warning message* is enabled.
623135	Error trying to access SSO - General.
623205	Failed to run migration when upgrading from 6.1 GA to any further build.

Bug ID	Description
623599	Fabric Connector widgets for FortiAuthenticator stop working post upgrade to FAC 6.1.0.
623789	FortiAuthenticator HA Cluster Member does not start after upgrade to 6.1.0.
624490	Large number of Password reset issues: Internal Server Error: /user/reset password/new/confirm.
624659	Email field sizes are inconsistent depending on new install / upgrade.
625031	Unexposed permission set errors in upgraded image (debug image admin warning).
625177	HA active cluster member becomes the standby member adding or deleting a load-balancer configured on the active member.
625214	Upgrading to 6.1.0 causes CA certificate selection in *System Access* page to switch to default selection.
625705	DST not updated for Santiago Chile.
625767	Sync token on login is broken.
625947	Manual CSR against CA that uses NetHSM fails.
626467	Fresh install produces lots of errors in the terminal during bootup.
627112	Errors on CLI fresh FortiAuthenticator installation.
627878	Exporting Key and Cert should not be allowed for intermediate NetHSM certificate.
627933	*FIELD NOT FOUND* logs on FortiAnalyzer and Syslog.
627935	Certificate Bindings got lost during upgrade from 6.0.3 to 6.1.0 (via 6.0.4).
628652	Errors on CLI after upgrading to build 0404.
629126	CRL file shows 0 revoked certificates.
629274	High Availability configuration is not available.
630376	Cisco vendor specific attributes sent in wrong order in RADIUS access-accept.
630992	CRL is not regenerated 1 day after revocation happens.
631143	CRL is not updated.
631310	Upgrade issue with Kerberos keytab.
631380	FortiToken drift URL no longer accessible on FortiAuthenticator.
631383	Smart Connect Profiles cannot be downloaded for Windows Clients.
631696	Oauth social login failure after upgrading FortiAuthenticator from 6.0.4 to 6.1.0.
631715	Error occurred when adding more than 1500 users in a User group.
631805	GUI National language partially implemented.
631850	Failed to complete token transfer: Unknown reasons.
631852	SAML IdP: Import SP metadata incorrectly sets certificate fields.
631986	Smart Connect user certificate not compatible with Windows.

Bug ID	Description
632038	SAML IdP - Login sequence causing crash on mobile apps.
632141	API `api/v1/localusers/` password reset removes group memberships.
632351	REST API pushAuth for FortiToken mobile. Clicking deny does not send reply to client, resulting in 504 Gateway timeout.
632405	Unable to authenticate to GUI after upgrade from 6.0.2 to 6.1.0 GA but SSH works.
632417	SAML IdP issue in FortiCloud test environment.

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
449443	FortiAuthenticator Agent For Microsoft Windows does not display the user credentials when access the server through RDP.
467883	RDP Users prompted for credentials twice and failing the second time due to token reuse (if they don't wait).
478985	FortiAuthenticator Windows Agent sometimes doesn't see the domain name and user is not able to log in.
485396	Sponsor/Admin can place created Guest users into any group.
528231	Log showing *Can not add any more users because limit of 1100 has been reached*.
548689	Don't delete a revoked local service cert until expiry.
573346	FortiAuthenticator delays forwarding auth request to remote RADIUS.
575261	RADIUS authentication is successful when using an invalid realm.
576691	Default realm allowing RADIUS users to authenticate using non-existant realms.
586570	FortiToken self-reprovision fails when token does not belong to product, allows user/admin to login without 2FA.
586851	The HTTP of the FortiAuthenticator cannot be closed.
587113	RADIUS daemon needs to be restarted after adding a custom dictionary.
588346	An expired certificate is delivered toward WiFi authenticated users.
591227	API user with 2FA unable to authenticate on subsequent attempts after inputting incorrect code on the first try.
592837	Sponsor Accounts Can add Guest User Accounts to non guest Groups.
593089	Log filter limitation.
601554	Delay in first OTP verification, REST API.
601603	CLI only supports configuring interfaces port1 - port4.
604156	Packet captures on OCI often seem to be corrupt.
604270	HTTP access logs doesn't include the source IP address.
604924	SAML SSO/Proxy metadata download fails with *invalid_xml*.
606760	HA cluster, FortiAuthenticator GUI does not reflect correct HA status when the active cluster member fails and the standby member becomes the active member.

Bug ID	Description
608459	Secondary member of the cluster does not send *Access-Challenge* to RADIUS client.
610360	FortiAuthenticator agent doesn't send the domain information once checking the token code.
610833	Passwords containing two consecutive backslashes (\\ ) are not handled correctly by FortiAuthenticator's LDAP server.
611722	When FortiAuthenticator is an LDAP server, changing existing LDAP local user UID and selecting *More...* causes GUI crash.
613578	SAML IdP Proxy to ADFS is unable to return group memberships.
614673	Remote User Sync Rule Preview mapping for mobile number shows attribute even if field is wrongly formatted.
616181	SAML IdP - Post-login debug page does not show relevant SAML attributes.
617890	REST API - Cannot retrieve complete schema of everything.
618537	RADIUS SSO Sessions not generated when using UPN as login name for multiple domains/realms.
623421	FortiAuthenticator 6.1.0 Remote User Sync Rules GUI - add user group.
624293	FortiAuthenticator displays UTC instead of configured time.
626926	Remote User Sync Rule downgrades the role of a local admin with identical username.
627230	FTM push notifications fail when using the local realm for remote users.
627608	6.1.0 GUI - log search in /debug section always returns *No results found*.
627764	Certificate has been renewed but old certificate hasn't been revoked.
627917	Remote user authenticate in wrong user group.
628027	While downloading the debug logs from Web GUI, receiving Gateway timeout error message.
628815	Remote SAML user import from Azure AD fails authorization issue.
629289	Lost GUI access.
630041	FortiAuthenticator FSSO - TS Agent sessions stuck at zero after server reboot until FSSOTA service is restarted.

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 / 10 = 10

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
User Management	**Users** (Local + Remote)[1]	5	***********	100	5000

Feature		**Model**			
		Unlicensed VM	**Calculating metric**	**Licensed VM (100 users)**	**Example 5000 licensed user VM**
	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
	RADIUS Client Profiles	3	Users	100	5000
	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
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.