FortiAuthenticator - Release Notes

Version 6.2.0

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

November 2, 2022
FortiAuthenticator 6.2.0 Release Notes
23-620-661166-20221102

TABLE OF CONTENTS

Change log

Date	Change Description
2020-09-16	Initial release.
2020-11-23	Updated Hardware and VM support.
2022-01-04	Updated Upgrade instructions on page 12.
2022-03-03	Updated Product integration and support on page 16.
2022-11-02	Updated Product integration and support on page 16.

FortiAuthenticator 6.2.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.2.0, build 0542.

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.

What's new

FortiAuthenticator version 6.2.0 includes the following new features and enhancements:

The following list contains new and expanded features added in FortiAuthenticator 6.2.0.

REST API enhancements

The following enhancements have been added for the FortiAuthenticator REST API:

- Filtering for user certificates.
- Configurable character delimiter for FSSO group membership.

TACACS+ support

FortiAuthenticator now includes TACACS+ authentication capabilities. TACACS+ settings can be configured in **Authentication > TACACS+ Service**. Before FortiAuthenticator can accept TACACS+ authentication requests from a client, the device must be registered on FortiAuthenticator, and it must be assigned to a policy. TACACS+ authorization can be specified by creating authorization rules that can be applied to users and user groups in FortiAuthenticator.

SAML IdP Proxy: 0365 Azure/ADFS hybrid support

SAML IdP proxy O365 Azure/ADFS hybrid support added.

Get Windows AD nested groups during SAML IdP configuration

A new configuration option to **Get nested groups for user** is available during IdP configuration. Enabling this feature allows the IdP to perform nested group lookup for Windows AD. See SAML IdP.

REST API key visibility for Admin users

After enabling **Web service access** on a local admin account and saving changes, the **User API Access Key** window is displayed where you can view, copy, and/or email the REST API key. Web service access can be enabled for admin users in **Authentication > User Management > Local Users**.

RADSEC support

RADSEC is now supported for RADIUS authentication by adding a RADSEC server certificate in **Authentication > RADIUS Service > Certificates**. All TLS communication on the specified RADSEC port will be treated as a regular RADIUS request. Access to RADSEC can be enabled or disabled on each network interface.

SCEP enrollment requests search

Certificate Management > SCEP > Enrollment Requests now includes a search field, allowing you to search for SCEP enrollment requests with subject fields matching the input search string.

LDAP group filter support for remote RADIUS realms

When using a RADIUS realm in a RADIUS policy, you can use a group filter to specify a previously configured LDAP group. Select **Allow remote LDAP groups** to see available LDAP groups.

When configured, the RADIUS authentication requires that a successfully authenticated user be a member of the specified LDAP group (through an LDAP lookup) in order to return an Access-Accept response.

Sync certificate bindings to load balancers

Certificate bindings settings for local and remote users are now synced to load balancers in HA load balancing configurations. This feature adds support for syncing the configuration objects required to effectively support EAP-TLS RADIUS authentication on load balancers.

Show Password toggle included in replacement messages

Each default replacement message for a login page containing an input password field now includes a "show password" toggle.

Legacy Self-service Portal disabled by default

In FortiAuthenticator 6.1.0, self-service portal configuration was added to **Authentication > Portals**.

In 6.2.0, the legacy **Self-service Portal** configuration is disabled by default in the GUI and can be manually re-enabled by going to **System > Administration > Features** and selecting **Enable legacy self-service portal**.

The **Replacement Messages** sub-menu is available in **System > Administration > Replacement Messages**.

Additional SCEP CRL/OCSP enrollment options

Two new optional settings are available for SCEP enrollment request configuration, located under the **Other Extensions** section in **Certificate Management > SCEP > Enrollment Requests**.

Settings include **Add CRL Distribution Points Extension** and **Add OCSP Responder URL**.

Revoked/expired user certificates hidden by default

By default, the user certificates page only displays valid (active and pending) user certificates. In **Certificate Management > End Entities > Users**, you can select **Revoked** or **Expired** in the filter menu to view revoked or expired certificates.

Richer logs for self-registered users

When a local user account is created through self-registration, log messages generated by FortiAuthenticator now contain the value of all non-blank fields from the registration form in addition to the username in the log's **Message** field. To view log messages, go to **Logging > Log Access > Logs**.

Usernames included in FTM activation messages

Usernames are now displayed in FortiToken Mobile activation messages. The following replacement messages will now display usernames.

- **System > Administration > Replacement Messages > Account > FortiToken Mobile Activation Email Message**
- **System > Administration > Replacement Messages > Account > FortiToken Mobile Activation SMS Message**
- **Authentication > Portals > Replacement Messages > Post-Login > FortiToken Mobile Activation Email Message**
- **Authentication > Portals > Replacement Messages > Post-Login > FortiToken Mobile Activation SMS Message**

FTC: Sync email and mobile number

FortiAuthenticator will now sync emails and mobile numbers to FTC.

SNMP trap for RAID status changes

A new SNMP trap for notification of RAID status changes is available. When configuring SNMP v1/v2c and v3 in **System > Administration > SNMP** select **RAID status changed**.

Administrator password required before changes can be made to administrator accounts

When adding, editing, or deleting an admin account in FortiAuthenticator, a dialog is displayed requesting the password for the currently logged in administrator before settings can be saved.

FortiAuthenticator Windows Agent: SMS/email 2FA support

SMS and email two-factor authentication support added for Microsoft Windows Agent.

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 6.2.0 supports:

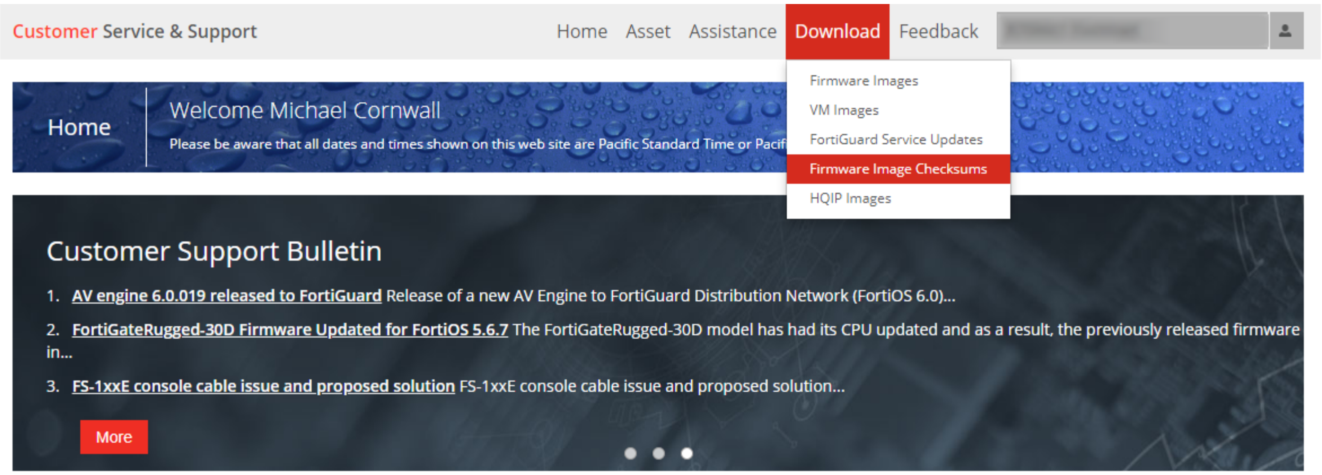
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 800F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, 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.x

FortiAuthenticator 6.2.0 build 0542 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 6.2.0, 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 6.2.0 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.2.0 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 14.

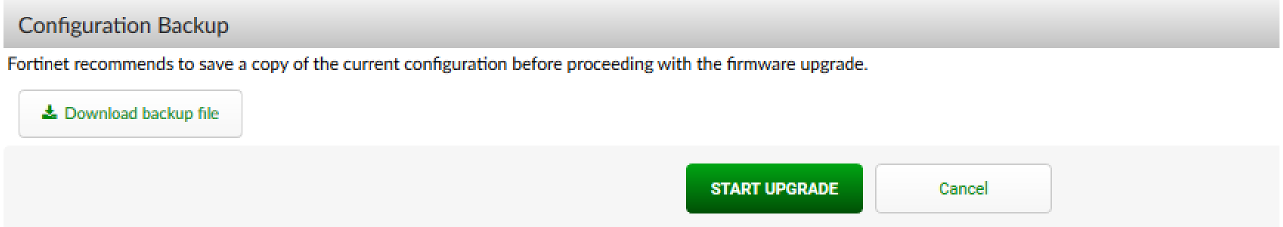
Firmware upgrade process

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:



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 6.2.0, 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 6.2.0

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 6.2.0:

- Microsoft Edge version 85
- Mozilla Firefox version 80
- Google Chrome version 85

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

FortiOS support

FortiAuthenticator 6.2.0 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 6.2.0 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 2.6, 3.2, 3.5, 3.7, 3.8, 4.0, and 4.1.
- 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 6.2.0 supports:

- VMware ESXi / ESX 4/5/6
- Microsoft Hyper-V 2010 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 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

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
449443	FortiAuthenticator Agent For Microsoft Windows does not display the user credentials when access the server through RDP.
481255	Gpart root shell implant against VM appliances.
530392	Cannot log in with social users on guest portal if their account has expired.
548527	Cannot unlock a user account that has been locked due to repeated invalid password entry from User Lookup page.
548689	Don't delete a revoked local service cert until expiry.
567598	FortiAuthenticator doesn't check that converted-format organization image meets file size requirements.
571782	Misc-Reverse-Tabnabbing.
573346	FortiAuthenticator delays forwarding authentication request to remote RADIUS.
575128	Allow deletion of imported Local Service certificates.
575261	RADIUS authentication is successful when using an invalid realm.
578190	Cancel button does not work throughout creation of a Guest Portal Smart Connect Profile.
580360	OK button doesn't do anything under when importing an SSO User.
583516	Gateway timeout error when downloading user audit report.
587113	RADIUS daemon needs to be restarted after adding a custom dictionary.
587370	Make it easier to use strings with RADIUS attributes of OCTETS type.
596985	Anonymous PEAP/TTLS issues.
598856	Cannot revoke localservices cert with Remote CA issuer.
600388	CVE-2019-9193 postgresql allow run system commands through COPY SQL command.
604222	Use bcrypt hash for initial blank admin password after factory reset.
604270	HTTP access logs doesn't include the source IP address.
604496	CLI "exec restore" and "exec backup" commands appear not to check permissions.
607920	Unable to add some RADIUS attribute types to Custom Dictionaries.
609383	Update VMware OVF - Provide HW13 or HW14 profile.
610318	Using X-forwaded-for header to verify source IP allows spoofing and inaccurate logging.
610360	FortiAuthenticator agent doesn't send the domain information once checking the token code.

Bug ID	Description
610790	Admin user without permissions trying to enter local page/guest users page will crash.
610792	Admin Profile with read and write access to widget cannot access Locked Out Users.
610827	Social Login users should show how many more available users can be created.
611424	Group membership is currently "+" delimited. Move or provide option to use "," as the delimeter.
611722	FortiAuthenticator as LDAP server changing eisting LDAP local user UID and select more GUI crashes.
612955	HA status page no response if anomalies are very large.
613996	Nested group search fix for SAML IdP.
614105	Reboot required prompt when loading or changing FortiClient license.
614673	Remote User Sync Rule preview mapping for mobile number shows attribute even if field is incorrectly formatted.
617282	FTM Token activated in mobile app has inaccurate issuer info.
617890	REST API - Cannot retrieve complete schema of everything.
619070	Exposed HA maintenance mode on CLI.
620314	Last login time for remote users not updated on standalone primary after logins on load balancers.
620496	Typo in HTML doc on infosite.
621089	RADIUS accounting response not being sent from FortiAuthenticator to a second client if another RADIUS client is added first.
622299	HA coordinated upgrade should not show up for load balancing.
623421	FortiAuthenticator 6.1.0 RUSR GUI - add user group.
624293	FortiAuthenticator displays UTC instead of configured time.
625179	Admin profiles permission sets Users and Devices unable to add remote LDAP users.
626438	CRL link displayed on the cert creation page for cert signed by intermediate certificate is improperly formatted.
626926	Remote User Sync Rule downgrades the role of a local admin with identical username.
627230	FTM Push for SSLVPN Fails, not possible see push notification in mobile.
627608	GUI log search in /debug section always returns "No results found".
628027	While downloading the debug logs from Web GUI getting "Gateway timeout" error message.
628649	Upgrades with a lot of social users is very slow.
629370	HA communication doesn't work over networks with effective MTU smaller than 1500 bytes.
630044	Request for a single-page config overview for RADIUS and Portal policies.
631603	Refreshing Access Token for fabric API causes Django crash.
632033	Unable to change local user password after upgrade - "You do not have permission to perform such

Bug ID	Description
	operation".
632109	Unable to "set and email random password" when creating new user.
634017	PSKC Output shows HOTP when in fact token is TOTP.
634215	FortiAuthenticator adds escape character (backslash) to SMS gateway when HTTP is used.
634637	Unable to list Social Login Users: "An error has occurred".
634783	SAML unable to download metadata until the form is saved.
637162	Removed Certificate is still included in a Smart Connect Profile.
637625	Change default user retrieval selection to "Set a list of imported remote LDAP users" in new user group menu.
637998	REST API for localusers stopped working.
638359	Social login captive portal login page showing default HTML instead of customized one.
638885	AD authentication failed if cleartext password with character " received by FortiAuthenticator.
638970	Heartbeat interval and lost threshold doesn't get edited on first HA connection.
639366	Load balancer goes out of sync for FTM continuously.
639601	802.1x authentication failing with "request queueing too long and discarded".
639724	Close button on sync attributes help dialog doesn't work.
639937	PoV issue with Certificate Binding CA in Remote LDAP user sync rule not showing up.
642052	Organization validation.
642056	Show FTM info to help with troubleshooting push.
642961	DCAgents marked as offline randomly in SSO Monitor.
644618	Second OTP screen should be bypassed if the user or the usergroup is exempted.
644657	GET, POST, DELETE methods are not working for RADIUS attributes.
645705	Spelling error on SMTP Test Connection Dialog.
645983	Syslog SSO service does not start unless FortiAuthenticator is rebooted.
646901	User with admin role cannot import users from remote LDAP.
647160	Not able to bind trusted CA to remote user if no local CA is created.
647329	FortiAuthenticator Windows Agent not honoring 2FA group exemption.
647500	User look up fails to show information of a locked user.
648441	Routing configuration changes when rebooting Azure VM.
649141	Unable to update certificate.
652079	SAML IdP - Signature verification of SP request fails.

Bug ID	Description
652254	CLI login always times out after FortiAuthenticator boots up during authentication.
652279	API: Make realm input case-insensitive.
655804	FortiAuthenticator is sending FSSO logoffs to FGT when receiving the same user info again from TS-agent.
657660	Upgrading standalone primary unit from 6.0.4 to 6.1.2 gets stuck in "Loading /rootfs.gz...ok".
658148	Remote User with the same username different DN override.
658152	Importing Fortioken FTK211 seed file gets error "unable to decrypt seed for FortiToken".
659131	Oauth Api TFA Broken, various issues after Django upgrade.
663132	User is locked out after one failed OTP login where it's configured to three.

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.

Mantis ID	Description
526202	FortiAuthenticator does not check if signature of CSR is valid.
543729	RADIUS client service not working after upgrade.
586570	FortiToken self-reprovision fails when token does not belong to product, allows user/admin to login without 2FA.
588346	An expired certificate is delivered toward Wifi authenticated users.
589219	Multiple DC's Kerberos traffic after FortiAuthenticator joining the domain with local DC.
600509	FTM Push "Accept" shouldn't fail because it's already been accepted.
601883	Test SMS doesn't work in adding a gateway.
602707	Can not add multiple alternate DNS names into certificate for user certificates.
604156	Packet captures on OCI often seem to be corrupt.
604924	SAML SSO/Proxy metadata download fails with "invalid_xml".
606562	FortiAuthenticator rejects certificate signing request from FortiGate client with invalid password error.
616181	SAML IdP - Post-login debug page does not show relevant SAML attributes.
620127	Changing from maint-mode-no-sync to maint-mode-sync doesn't appear to restore syncing.
628815	Remote SAML user import from Azure AD fails Authorization issue.
630041	FAC FSSO - TS Agent sessions stuck at zero after server reboot until FSSOTA service is restarted.
631600	SCEP request by certmonger can't be recognized by automatic enrollment request.
632411	Crash when setting non-blank password that doesn't comply to password policy rule.
632629	Smart Connect WPA2-Personal profile fails when WPA2-Enterprise settings are left in place.
634084	Cannot export third party signed certificate with private key when CSR is generated locally on FortiAuthenticator
635893	Change password not working with Checkpoint VPN when 2FA is enabled.
637040	HA Status showing "out of sync" when load balancer has synced user changed to role Admin.
640048	FortiAuthenticator failed to load the license.
643334	If MAC filter is enabled, but the configured RADIUS attribute is missing from the packet, we deny the authentication.
646299	Nutanix AHV KVM based Hypervisor FortiAuthenticator upgrades from 6.0.4 to 6.1.x and hangs on

Mantis ID	Description
	"Waiting for Database".
646764	CLI "get disk * " commands fail on KVM.
652072	LDAP user password expired, user not prompted for RSA Token code (chained Token Authentication).
655350	The lockout policy does not appear to apply to username/token submissions to the /auth API endpoint.
657522	0396: SAML Authentication Fails When AD Display Name Contains a Coma (,) and User has Admin Role
660357	FSSO FGT IP Filter ignored when Global Group Prefilter is enabled
660851	Force password change on next logon produces 403 forbidden with local user after login to selfservice or captive portal

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	800F	1000D	2000E	3000E
System							
Network	Static Routes	50	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20	20
	SMS Gateways	20	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20	20
	User Uploaded Images	39	114	414	514	1014	2014
	Language Files	50	50	50	50	50	50
Realms		20	80	320	400	800	1600
Authentication							
General	Auth Clients (NAS)	166	666	2666	3333	6666	13333
	Users (Local + Remote)[1]	500	2000	8000	10000	20000	40000
	User RADIUS Attributes	1500	6000	24000	30000	60000	120000
	User Groups	50	200	800	1000	2000	4000
	Group RADIUS Attributes	150	150	2400	600	6000	12000
	FortiTokens	1000	4000	16000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200	200
	LDAP Entries	1000	4000	16000	20000	40000	80000
	Device (MAC-based	2500	10000	40000	50000	100000	200000

Feature		Model					
		200E	400E	800F	1000D	2000E	3000E
	Auth.)						
	RADIUS Client Profiles	500	2000	8000	10000	20000	40000
	Remote LDAP Servers	20	80	320	400	800	1600
	Remote LDAP Users Sync Rule	50	200	800	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	6000	24000	30000	60000	120000
FSSO & Dynamic Policies							
FSSO	FSSO Users	500	2000	8000	10000	20000	200000[3]
	FSSO Groups	250	1000	4000	5000	10000	20000
	Domain Controllers	10	20	80	100	200	400
	RADIUS Accounting SSO Clients	166	666	2666	3333	6666	13333
	FortiGate Services	50	200	800	1000	2000	4000
	FortiGate Group Filtering	250	1000	4000	5000	10000	20000
	FSSO Tier Nodes	5	20	80	100	200	400
	IP Filtering Rules	250	1000	4000	5000	10000	20000
Accounting Proxy	Sources	500	2000	8000	10000	20000	40000
	Destinations	25	100	400	500	1000	2000
	Rulesets	25	100	400	500	1000	2000
Certificates							
User Certificates	User Certificates	2500	10000	40000	50000	100000	200000
	Server Certificates	50	200	800	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50	50
	Trusted CA Certificates	200	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	40000	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.