FortiAuthenticator - Release Notes

Version 6.1.0

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

January 4, 2022
FortiAuthenticator 6.1.0 Release Notes
23-610-619983-20220401

TABLE OF CONTENTS

Change log

Date	Change Description
2020-03-28	Initial release.
2020-03-31	Added information about upgrading KVM and Xen virtual machines to Upgrade instructions on page 11
2020-04-01	Added an additional note about the upgrade procedure to Upgrade instructions on page 11
2020-04-13	Added information about the pre-authentication warning message to Special notices on page 6.
2020-05-13	Added known issue 627230.
2020-05-20	Updated support for FortiAuthenticator Agent for Microsoft Windows.
2020-06-01	Added known issue 632405.
2020-07-30	Note added about upgrading from FAC-3000E models on 6.0.x to Upgrade instructions on page 11.
2020-08-19	Added special notice about HA compatibility to Special notices on page 6.
2022-01-04	Updated Upgrade instructions on page 11.

FortiAuthenticator 6.1.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.1.0, build 0396.

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.

Disable the pre-authentication warning message

Enabling the pre-authentication warning message in 6.1.0 prevents access to the GUI, therefore, the pre-authentication warning message should not be enabled in 6.1.0.

Before upgrading to FortiAuthenticator 6.1.0 (i.e. in 6.0.4), **disable** the option to **Enable pre-authentication warning message** under **System** > **Administration** > **System Access**.

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

FortiAuthenticator 6.1.0 build 0396 officially supports upgrade from FortiAuthenticator 6.0.4.

All other versions of FortiAuthenticator must first be upgraded to 6.0.4 before upgrading to 6.1.0, 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.

HA compatibility

Secondary units that are freshly installed on 6.1.0 are not compatible with Primary units that have been upgraded from 6.0.4 and earlier to 6.1.0.

As a workaround, you can downgrade the Secondary unit to 6.0.4 and then upgrade it to 6.1.0, or perform a factory reset on the Primary in the HA configuration on 6.1.0.

This compatibility issue does not exist when the Primary and Secondary units are *both* fresh installations in 6.1.0.

What's new

FortiAuthenticator version 6.1.0 includes the following new features and enhancements:

REST API: Enforce permissions

Admin profiles are enforced when administrating the FortiAuthenticator via the REST API. The permissions required for each endpoint must match the permissions of the equivalent form(s) in the GUI.

See the REST API Solutions Guide for more information.

REST API: Statistics & logging

Add logs and/or statistics on FortiAuthenticator to allow profiling of the REST API usage.

See the REST API Solutions Guide for more information.

SAML IdP: Enhanced SP signature options

The following enhancements have been made to SAML Service Providers:

- During SAML SP configuration, when **SAML request must be signed by SP** is enabled, the certificate type can be configured as:
  - **SP certificate**: The SP request is signed by the specified certificate (default behavior prior to 6.1.0).
  - **Direct CA certificate**: The SP request must contain the certificate fingerprint that was used to sign the request, and the certificate must be issued by the CA specified in the configuration.
- The fingerprint algorithm **Use ACS URL from SP authentication request** can be enabled to indicate that the ACS URL must be included within the SP request, and that the FortiAuthenticator must use it instead of the preconfigured ACS URL.
- You can configure an alternative certificate fingerprint for SP and CA certificates. FortiAuthenticator will accept requests with valid signatures from either configured certificate.

SAML IdP: Single logout

FortiAuthenticator supports single logout for SAML IdP, causing logout from one SP to trigger logout from all other configured service providers.

Single logout for SAML IdP is configured in **Authentication > SAML IdP > Service Providers.** Alternative SLS URLs can be configured through the **Alternative ACS URLs** menu.

IdP-initiated SAML

Support has been added for IdP-initiated SAML authentication on FortiAuthenticator.

SAML IdP-initiated authentication works as follows:

1. A user attempts to access the IdP login portal, resulting in one of two possibilities:
   - The user's browser is already authenticated by the IdP. Proceed to **step 2**.
   - The user's browser is not yet authenticated by the IdP. The IdP requests and validates the user's credentials. If successful, go to **step 2**. Otherwise, access is denied.
2. The user is presented with an IdP portal landing page that includes a list of the SPs participating in IdP-initiated login. The user selects a service provider.
3. IdP generates the SAML assertions for the browser and sends it to the SP.
4. The SP receives the assertions and authenticates the user, resulting in one of two possibilities:
   - The user is authorized, and the SP provides the requested resource to the user.
   - The user is not authorized, and access to the SP is denied.

OCSP and CRL distribution URLs for intermediate CA certificates

OCSP and/or CRL distribution URLs can be enabled for intermediate CA certificates.

Prompt administrator password change on first login

During initial setup of the FortiAuthenticator, administrators are required to create a non-blank password.

Dual two-factor authentication for remote user sync rules

The **Dual (Email and SMS)** option is now available in the list of token-based authentication sync priorities when creating or editing a remote user sync rule.

Additional configurations synchronized in HA load-balancing

The following additional configurations are synchronized between the standalone primary and load-balancers in an HA load-balancing configuration.

- Certificates included in:
  - **Certificate Management > End Entities > Local Services**, excluding firmware (Fortinet) certificates.
  - **Certificate Management > Certificate Authorities > Local CAs**, including firmware (Fortinet) certificates.

- SAML configurations:
  - IdP settings configured in **Authentication > SAML IdP > General**.
    Realm tables are not synchronized, but the default realm selection (radio button) is.
  - SP settings configured in **Authentication > SAML IdP > Service Providers**.
- Administrators with **Sync in HA Load Balancing mode** enabled.

The current synchronization status of the standalone primary to load-balancers can be viewed at **Dashboard > HA Status**.

NetHSM Support

Support has been added for using the Safenet Luna HSM with FortiAuthenticator for the following purposes:

- Storing the private keys of local CAs.
- Issuing (i.e. signing) user and local service certificates with local CAs that have their private key stored on the NetHSM.

HSM servers can be configured at **System > Administration > NetHSMs**.

Wizard-based authentication policies

The GUI has been streamlined for configuring RADIUS services and Portals, and a new setup wizard has been introduced for authentication policies. This update only impacts the GUI and does not remove or introduce new RADIUS or Portal configuration options. When upgrading from a version prior to 6.1.0, **RADIUS Services** and **Guest Portals** settings are configured to the corresponding 6.1.0 menus.

Guest Portals:

- **Authentication > Guest Portals** has been renamed to **Portals**.
- **Authentication > Guest Portals > General** has been renamed to **FortiWLC Pinholes.**
- **Authentication > Guest Portals > Rules** has been renamed to **Policies**.
- Portal authentication logic now resides in **Authentication > Portals > Policies**.

RADIUS Service:

- **Authentication > RADIUS Services > Policies** has been added as a new configuration menu.
- RADIUS authentication logic now resides in **Authentication > RADIUS Service > Policies**.

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 6.1.0 supports:

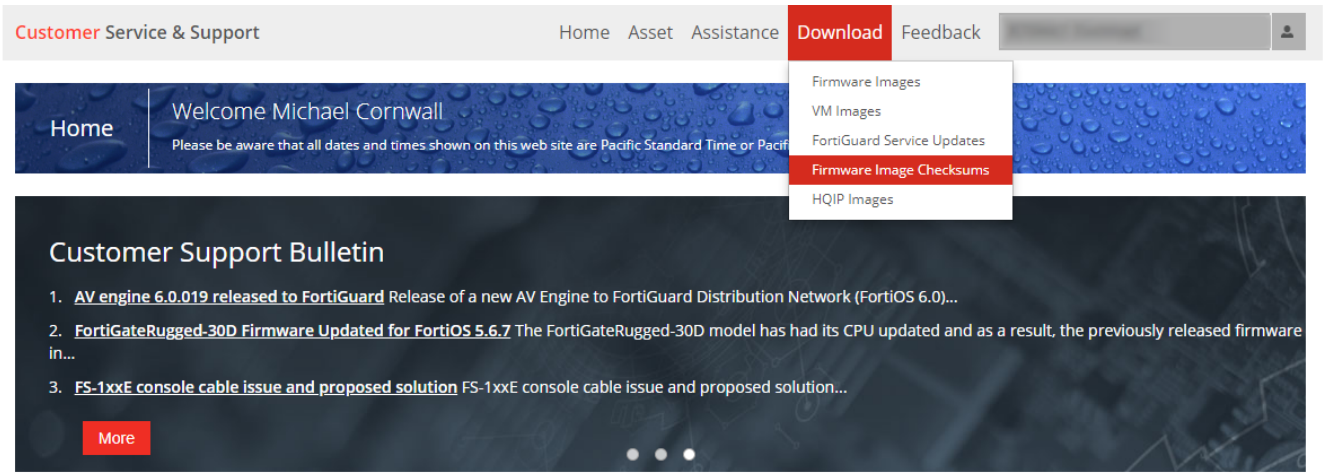
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, and Oracle OCI)

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 6.1.0 build 0396 officially supports upgrades 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 6.1.0, 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 6.1.0 directly.

Before upgrading to FortiAuthenticator 6.1.0 (i.e. in 6.0.7), disable **Enable pre-authentication warning message** under **System** >**Administration** >**System Access**.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.1.0, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See Upgrading KVM / Xen virtual machines on page 13.

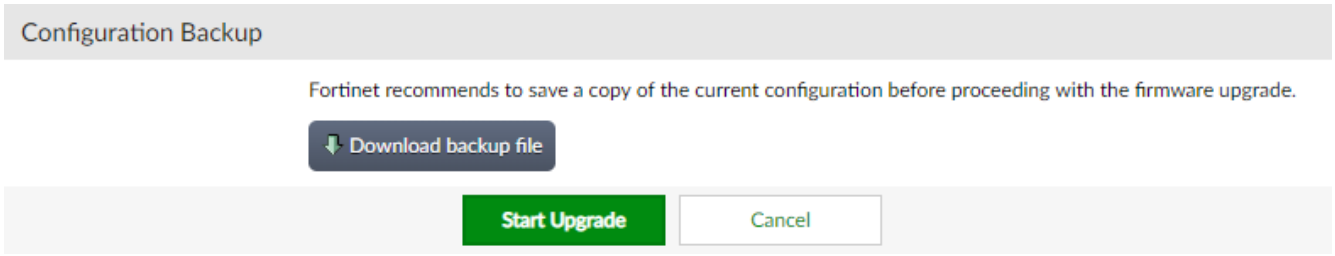
Firmware upgrade process

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. Go to **System > Dashboard > Status**.
5. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
6. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
7. 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

Prior to upgrading existing KVM and Xen virtual machines to FortiAuthenticator 6.1.0, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image.

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 6.4.1

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 6.1.0:

- 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 6.1.0 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 6.1.0 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 2.5 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 6.1.0 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 17 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
415685	Token-only user can log in to SP configured for "Enforce TFA" option if this user already has active session.
473605	Provide convenient method for admin to purge all offline token data for user.
481250	FortiAuthenticator- Private keys in file system. Not been protected by HSM.
482900	User registration via Guest Portal requires the approver to enable RADIUS authentication first.
495618	Windows Agent does not try to use secondary FortiAuthenticator upon DNS lookup failure for primary.
495872	EAP Server Certificate must be FQDN-specific, no wildcard permitted (for Windows 10 clients).
505497	FG-IR-18-182 PostgreSQL multiple releases.
510931	Clarification for Monitor, Authentication, and Windows AD statuses.
512913	One of the cluster units does not send traps while set as the active member.
519319	FortiAuthenticator is crashing every time when the LDAP Remote user sync rules are supposed to run.
519539	Cannot export local user if number of user is large.
526202	FortiAuthenticator does not check if signature of CSR is valid.
530922	Google+ is being shutdown.
532652	Users Audit Report not working on load-balancer.
536211	Should limit FSSO password to 15 characters since that is the limit on the Fortigate.
537531	Support dual 2FA for remote users sync rules.
538059	Importing an ECDSA-signed certificate/key causes an error dump.
538244	Add option for FortiAuthenticator SAML IdP to send Subject NameID in `example.com\username` format.
540587	GUI exception/crash occurs when clicking on a guest user in a load-balancer FortiAuthenticator.
540932	FSSOMA nested group search failing if nested via primary group.
542755	Password field in API call for remote users.
544023	Picking MD5-hashed certificate for system access causes Apache to crash repeatedly. FortiAuthenticator GUI becomes inaccessible.
544652	Django upgrading to v1.11.20 (python 2.7) or v2.2 (python 3).
544851	HA re-enable and interface in use.

Bug ID	Description
546764	Non-ASCII characters in replacement messages cause line-break in the middle of a URL in emails
548556	Enabling secure passwords options prevents LDAP clients from accessing FortiAuthenticator LDAP sever.
551478	FortiAuthenticator VM upgrade from 4.0 b6237 to 6.0 b010 not successful.
554282	Should have similar log messages for remote sync rules when either an admin or non-admin role is assigned to imported user.
555180	Push notification certificates not restored to disk following model conversion.
557070	One new jQuery CVE disclosed on 2019-04-19.
557773	Provide skeleton language pack for self-service portal.
558681	Load-balancer doesn't response to the accounting-request after the failover.
561190	Improve IdP metadata.
561563	Guest portal authentication fails with HTTP 500 if user name contains non-ASCII characters.
561588	Adding SMS license shows "connection timeout"in the GUI.
561794	Cannot edit guest user whose sponsor's account has been deleted.
563330	Error While accessing *Authentication* > *Remote* users.
566145	Usage Profile "TIME USAGE=Time used" is not triggering COA or disconnect request to FortiGate.
566767	FAC Agent - Include timestamps from FortiAuthenticator in the agent log when importing offline tokens.
567157	Trusted CA import shows pending when certificate is using SHA512 as hash.
567493	EAP-TLS authentication does not check *AuthorityKeyIdentifier* when matching allowed/trusted CAs.
568479	EAP-TLS - deletion of local CA#1 breaks authentication for local CA#2 with identical subjects.
569420	Certificate upload to FortiAuthenticator in PKCS#12 format fails.
570138	Local users screen crashes intermittently.
571226	FortiAuthenticator API - Call to *api/v1/usercerts.*
571537	Smart Connect profile is not working on MAC computer.
572513	FortiMobile push stopped working after upgrade from 5.5.0 to 6.0.2 while trying to log in to FortiAuthenticator admin access with remote users.
574824	No more than 20 Realms can be present in RADIUS client settings.
575996	FortiAuthenticator as RSSO > FSSO processing fails if fails RADIUS Accounting Sources is configured with FQDN instead of IP.
577590	FortiGuard server failed sending SMS because message is too long.
581951	Fortitoken Cloud status service error when no entitlement purchased.
581967	FTM trial license activation: Disable "Cannot find req_trial_ftm task. It might have been removed".

Bug ID	Description
582845	Revoked local service certificates not in CRL.
582850	RADIUS attributes are not added in Access-Accept packet.
583729	Unable to import users into LDAP directory tree.
585864	Random issue while accessing FortiAuthenticator Dashboard.
586033	FortiAuthenticator sends faulty class attribute in Access-Accept.
586645	'ftm_id' error returns to FTM Android when approve login request from push notification.
587355	The FortiAuthenticator not processing DC agent information.
591250	KVM Uptime is wrong after VM reboot.
591280	"Cluster not formed" message on HA Status page, but HA seems to work OK.
591814	Admin login from Guest Portal registration link that was emailed by FortiAuthenticator keeps failing.
592077	FCT: Reached maximum client number, cannot accept new connection
592533	FortiAuthenticator Agent should programmatically disable all installed credential providers instead of just the Windows defaults.
592858	Routing table breaks when updating IP.
593571	Disk monitor widget error on dashboard.
594410	Not able to select FortiToken Hardware under self-service portal.
595030	Performance improvement for Windows Authenticator for users with offline tokens.
595762	FortiAuthenticator-VM Azure maintainer account doesn't work.
596071	FortiAuthenticator AWS having issue connection to AWS NTP server address `169.254.169.123`.
596290	Accent character handling for remote LDAP user.
596406	Inconsistency on fiber ports, HA implementation.
596611	DCAgents marked as offline randomly in SSO Monitor, fail to process user events in that state.
596723	Delay in loading Guest Portal.
596740	SNMP trap for user lockout still getting sent even when it has been disabled.
596840	LDAP realm with token-only authentication works only with PAP
596905	Standalone primary unit in a load-balancing configuration restarts itself when a new connection replaces an existing one.
597116	FortiAuthenticator not accessible via port2 despite setting *allowaccess https*. 403 Forbidden error is presented.
598447	2FA field is named identically to password field.
598781	Add HA "debug mode" outputs additional data to the HA debug log.

Bug ID	Description
600065	FortiAuthenticator cannot use NTLMv2 in WINBIND process to join AD Domain.
600068	Mobile number verification for Guest portal Self-registration (pre-login service) does not use the configured SMS gateway.
600073	Cannot finish Guest Portal self-registration if *Device Tracking post-login* feature is enabled.
600357	SCEP Response with certificate, has three extra bytes.
600701	Social logins are denied when normal user license is exhausted.
600848	SNMP *sysUpTime* value reset to zero every four hours.
601812	Link in password reset email is split in two lines.
602138	Slony HA still needs an indicator for "in_sync" in the HA Status GUI.
602352	GUI error for SSO Group Fine-grained Controls
602443	Use mobile number as username pass in incorrect value causes GUI webpage crash.
602675	Update default FortiToken Mobile provisioning message.
602927	Merge OCI support into trunk.
602962	RADIUS MSCHAPv2 authentication fails even FortiAuthenticator is joined to the domain.
604394	*winbind* child process spikes CPU to 75%+.
604431	Vulnerability of HTTP host header value reflection.
605689	Custom dictionaries are not syncing with HA load balancing device.
606263	SSO users flushed after making LDAP server changes on FortiAuthenticator - 10 minute restart delay.
606707	It is possible to view/edit user data field from guest portal, even if profile view/edit options are not enabled.
606722	User information is missing the FortiAuthenticator logs.
607308	SAML user attribute "Remote LDAP Groups" - Limit of 200 insufficient.
607529	Change token default GUI display to six stars.
608937	Forbid firmware upgrades from 6.0.3 or earlier to 6.1.0 or later
610998	Unable to revoke user certificate - duplicate key value.
612114	Upgrade from 5.4.1 to 6.0.3 HTTPS swaps with RADIUS Account Monitor.
612233	jQuery not referenced causing FTM push failing on FortiClient SAML for SSLVPN.
612695	FortiAuthenticator sends DNS requests for the Client subnets configured in RADIUS accounting clients.
614490	Lengthy recovery time when connection to DC is interrupted.

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
548689	Don't delete a revoked local service certificate until expiration.
575261	RADIUS authentication is successful when using an invalid realm.
576691	Default Realm allowing RADIUS users to authenticate using non-existing Realms.
586851	The HTTP of FortiAuthenticator cannot be closed.
587113	RADIUS daemon needs to be restarted after adding a custom dictionary.
587537	RADIUS SSO proxy multiplies accounting packets five times.
596515	Load-balancer failed to sync the "Remote Users" from the standalone primary.
601591	FortiAuthenticator generating DNS query for RADIUS clients even if is set to a subnet or a range.
601603	CLI only supports configuring interfaces from port1 to port4.
601990	Guest users expiring due to a usage profile change to "unspecified" and cannot be purged.
603510	High memory usage when FortiAuthenticator is used as RADIUS server to authenticate VPN users.
604156	Packet captures on OCI often seem to be corrupt.
604270	HTTP access logs doesn't include the source IP address.
604839	Admin configuration logs not showing information for user field.
604935	Remote User *Re-enable* button says "You do not have a permission to perform such operation" when the user has correct permissions.
606471	SYSlog FSSO user disappears after the remote user was enabled.
608873	Downloading User Audit Reports displays "An error has occurred".
610259	Creating or editing MAC Device in GUI is slow in Google Chrome.
610360	FortiAuthenticator agent doesn't send the domain information once checking the token code.
610926	Unexpected HA failover.
611722	When FortiAuthenticator is an LDAP server, reassigning the UID of local user and selecting *More...* crashes GUI.
611837	Accessing the local user's menu in the GUI is causing crashes.
613578	SAML IdP Proxy to ADFS is unable to return group memberships.
614673	Remote user sync rule preview mapping for a mobile number shows attribute even if the field is wrongly formatted.

Bug ID	Description
615442	No Kerberos ticket requests (negotiate) on encrypted HTTPS traffic from FortiAuthenticator.
615444	Cannot disable Kerberos login in the web GUI.
617890	REST API - Cannot retrieve complete schema of everything.
618877	FortiGate filters are not syncing with FortiGate FSSO Fabric agent connectors.
627230	FTM push notifications fail when using the local realm for remote users.
632405	Unable to authenticate to GUI after upgrade from 6.0.2 to 6.1.0 GA but SSH works.

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
Certificate Authorities	Server Certificates	2	Users / 10	10	500
	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.