FortiAuthenticator - Release Notes

Version 6.0.8

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

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

March 8, 2023
FortiAuthenticator 6.0.8 Release Notes
23-608-891026-20230308

TABLE OF CONTENTS

Change log

Date	Change Description
2023-03-08	Initial release.

FortiAuthenticator 6.0.8 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.0.8, build 0073.

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. Go to **System > Dashboard > Status** and select **Backup/Restore > 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 6.0.8 is a patch release. There are no new features. See Resolved issues on page 15 and Known issues on page 17 for more information.

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Hardware and VM support

FortiAuthenticator 6.0.8 supports:

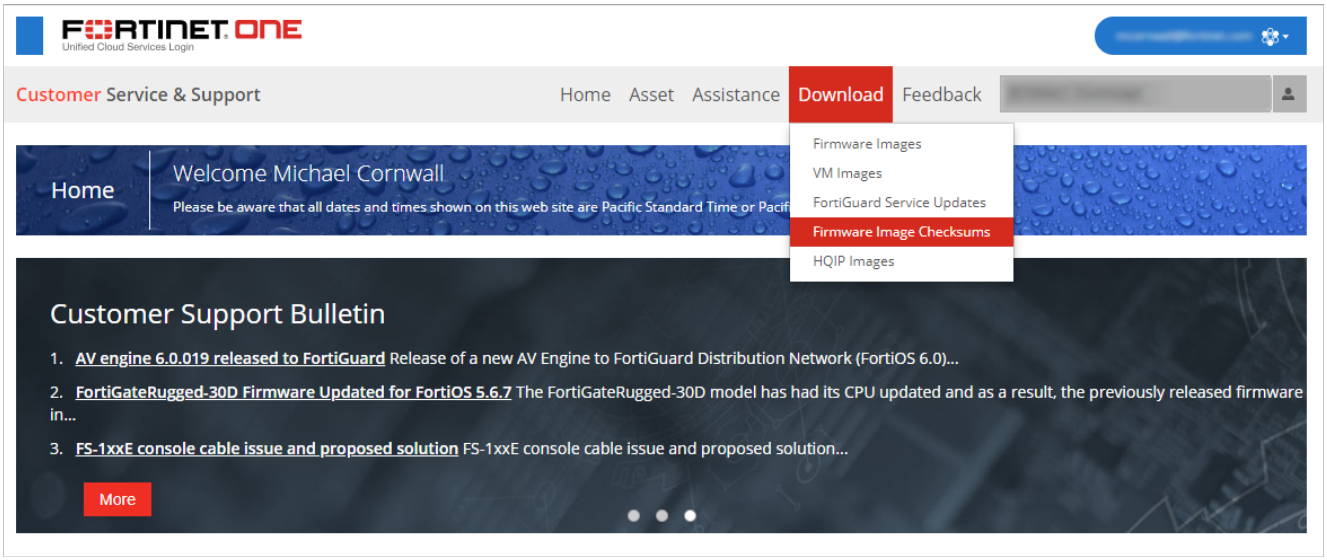
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, AWS, Azure, and OCI)

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 6.0.8 build 0073 officially supports upgrade from all versions of FortiAuthenticator 4.x, 5.x, and 6.0.x.

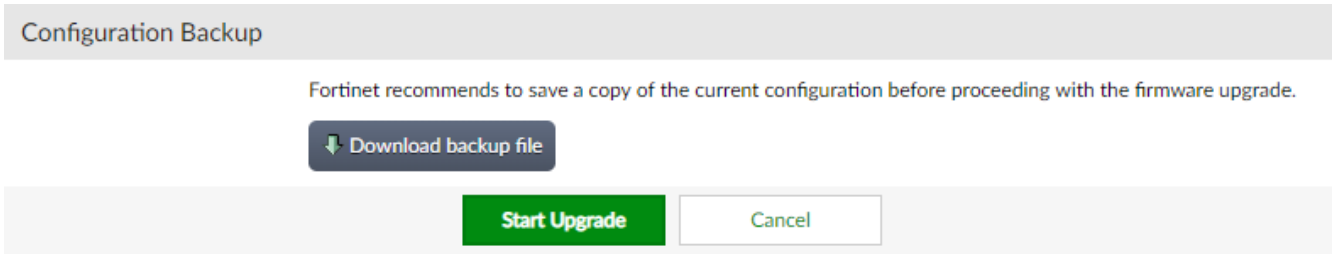
Firmware upgrade process

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.

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.0.8:

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

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

FortiOS support

FortiAuthenticator 6.0.8 supports the following FortiOS versions:

- FortiOS v7.0.x
- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x
- FortiOS v5.6.x
- FortiOS v5.4.x

Fortinet agent support

FortiAuthenticator 6.0.8 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- For FortiAuthenticator Agents for Microsoft Windows and Outlook Web Access compatibility with FortiAuthenticator, see the *Agents Compatibility Matrix* on the Fortinet Docs Library.
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Virtualization software support

FortiAuthenticator 6.0.8 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
- AWS
- Microsoft Azure
- Oracle Cloud Infrastructure

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

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
791452	CVE-2022-0778

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

Known issues

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

Bug ID	Description
529178	FortiAuthenticator 5.5.0 search for serial number in certificate subject.
526662	FortiAuthenticator SNMP TRAP on disk failure or / and SNMP OID for disk status.
576691	Default realm allowing RADIUS users to authenticate using non-existing realms.
582850	RADIUS attributes are not added in the Access-Accept packet.
540932	FSSOMA nested group search failing if nested via primary group.
478985	FortiAuthenticator Windows Agent sometimes does not see the domain name and the user is not able to log in.
551706	FortiAuthenticator LB HA Cluster cannot have two remote FortiAuthenticator Admins with same username when 2FA FortiToken is enabled.
570138	Local user screen crashes intermittently.
490281	GUI issue with FortiAuthenticator logging.
554282	Should have similar log messages for remote sync rule when either admin or non-admin role is assigned to an imported user.
583729	Unable to import users into LDAP directory tree.
551478	FortiAuthenticator-VM upgrade from 4.0 b6237 to 6.0 b010 is not successful.
577590	FortiGuard server fails to send SMS because the message is too long.
555320	Captive Portal time schedule for device only (MAC address) is not working.
581951	FortiToken Cloud status service error when no entitlement purchased.
569420	Certificate upload to FortiAuthenticator in PKCS#12 format fails.
581967	FTM trial license activation: Disable "Cannot find req_trial_ftm task. It might have been removed".
544851	HA re-enable and interface in use.
573278	GUI SSO Portal Services page hiding elements.
528231	Log showing cannot add any more users because limit of 1100 has been reached.
574824	No more than 20 realms can be present in RADIUS client settings.
567157	Trusted CA import shows pending when certificate is using SHA512 as hash.
526202	FortiAuthenticator does not check if the signature of CSR is valid.
566145	Usage Profile "TIME USAGE=Time used" is not triggering COA or Disconnect request to FortiGate.

Bug ID	Description
445313	Default behavior for FTM deprovision.
563330	Error while accessing *Authentication> Remote Users*.
565635	2FA: When FortiAuthenticator receives AVP with multiple VSA for MSCHAP-v2, it rejects the 2nd request (response to challenge).
512913	One of the cluster units does not send traps while acting as primary.
536211	Should limit FSSO password to 15 characters since that is the limit on the FortiGate.
519319	FortiAuthenticator is crashing every time when the LDAP Remote user sync rules are supposed to run.
561563	Guest portal authentication fails with HTTP 500 if the user's name contains non-ASCII characters.
568479	EAP-TLS - deletion of local CA#1 breaks authentication for local CA#2 with identical subject.
532652	Users Audit Report not working on secondary of LB cluster.
555180	Push notification certificates not restored to disk following model conversion.
544691	Remote LDAP admins have no certificate bindings.
561588	Adding SMS license shows "connection timeout" in the GUI.
541884	FortiAuthenticator constantly drops connection to FortiGate with error "sock_recv() failed, error: 104".
582845	Revoked local service certificates not in CRL.
567493	EAP-TLS authentication does not check AuthorityKeyIdentifier when matching allowed/trusted CAs.
538059	Importing an ECDSA-signed certificate/key causes an error dump.
546764	Non-ASCII characters in replacement messages cause line-break in the middle of a URL in emails.
510931	Monitor - Authentication - Windows AD statuses are unclear.
528352	FortiAuthenticator HA CLI errors.
566500	Activation Failed. FTM Server: provision code not exist (40).
543729	RADIUS client service not working after upgrade.
575996	FortiAuthenticator as RSSO > FSSO processing fails if fails RADIUS Accounting Sources is configured with FQDN instead of IP.
571537	Smart Connect profile is not working with MAC computer.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

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

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

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

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

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

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator]-VM Base License, the number of auth clients (NAS devices) that can authenticate to the system is:

100 / 3 = 33

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
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
	FSSO Filtering Object	30	Users x 2	200	10000
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	2500	10000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.