FortiAuthenticator - Release Notes

VERSION 5.4.1

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

September 7, 2018

FortiAuthenticator - Release Notes

23-541-512008-20180907

TABLE OF CONTENTS

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator™ 5.4.1, build 0297.

FortiAuthenticator is a User and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit:

http://docs.fortinet.com/fortiauthenticator/

Special notices

TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the web-based manager to be viewed properly without need for scrolling.

Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. Go to **System > Dashboard > Status** and select **Backup/Restore > Download backup file** to backup the configuration.

After any upgrade

If you are using the web-based manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the web-based manager screens are displayed properly.

What's new in FortiAuthenticator 5.4.1

Note that this is a patch release. See Resolved Issues and Known Issues for more information.

For more detailed information, see the FortiAuthenticator 5.4 Administration Guide.

There are no new features in this release.

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™ 5.4.1 supports:

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

Deprecated hardware models

The following hardware models are EOS and expected to no longer be supported in the upcoming FortiAuthenticator 5.5.0 release:

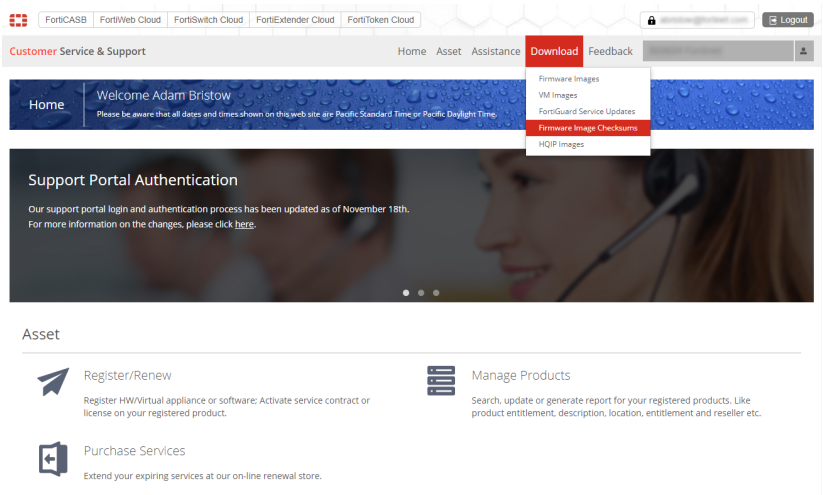
- FortiAuthenticator 3000B

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

FortiAuthenticator™ 5.4.1 build 0297 officially supports upgrade from all versions of FortiAuthenticator™ 4.x.x and 5.x.x.

Upgrading the FortiAuthenticator 3000D from 4.0.x to 4.1.x is not supported. The workaround for this model is to upgrade from any 4.0.x version directly to 4.2.0 or higher (skipping all 4.1.x versions).

If you install 4.1.x firmware on a FortiAuthenticator 3000D it stops responding. You can get the system running again by restoring valid firmware using the TFTP boot process.

Firmware upgrade process

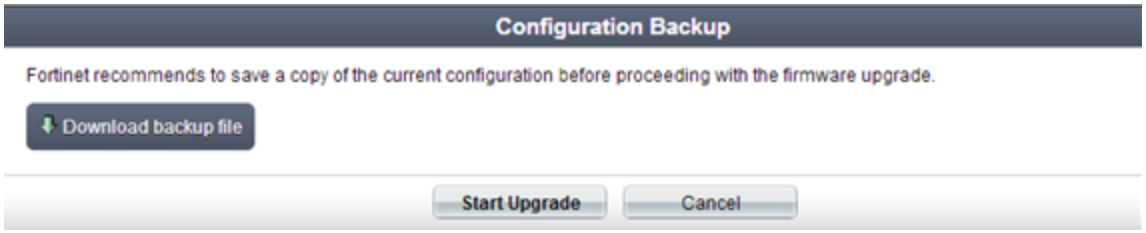
First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator™ firmware, you must download the firmware package 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™ 5.4.1:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 42
- Mozilla Firefox versions 61
- Google Chrome versions 68

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

FortiOS support

FortiAuthenticator™ 5.4.1 supports the following FortiOS versions:

- FortiOS v6.0.2
- FortiOS v5.6.5
- FortiOS v5.4.9

The above versions have been verified by QA. Other FortiOS versions may function correctly, but may not be supported by Fortinet. Refer to the What's new section and Known Issues for version compatibility information.

Fortinet agent support

FortiAuthenticator™ 5.4.1 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.2
- FortiAuthenticator Agent for Outlook Web Access 1.5
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but may not be 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™ 5.4.1 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
- 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 and AWS)

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 Appendix A: FortiAuthenticator VM 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). For more information, see the FortiAuthenticator Two-Factor Authentication Interoperability Guide.

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
508489	AD Server Monitoring for FSSO.
509458	Syslog SSO isn't working.
509447	Transfer token gets an error code 2 on FortiAuthenticator 5.4.0.
507719	Guest portal HTML errors for both SmartConnect and MAC address Bypass when Remote Users are used.
508762	Slony slave does not automatically recover from incorrect number of subscribed sets.
508767	Push notifications break HA setup processes on both master and slave.
509018	[500k+ users] HA - Both Slony and LB timeouts are not long enough for very large tables.
509907	LB slave will not reconnect to cluster master when there is no or minimal traffic from cluster slave.
508765	RADIUS: Excessive client collection logs occur when many RADIUS clients are configured.
507172	Change password fails in FortiGate SSL-VPN case if LDAP user has two-factor authentication enabled.
510530	SAML IdP fixes - Return to SP when no sp_data, cookie parsing fixes, avoid self-redirection.

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
454052	Push notifications aren't being sent out to guest users.
483582	Single Sign-On Mobility Agent fails if remote LDAP server is configured with Hostname instead of IP address.
488794	FortiAuthenticator fails to connect to LDAP server.
409763	SAML SP : SLS logout URL does not work, and returns an error page instead.
410566	SAML SP: Group list doesn't include selected implicit group when LDAP lookup option is selected.
509340	IP address changes on existing SSO sessions take too long to be re-verified.
460960	Support for remote RADIUS challenges in guest portals.
453822	Guest Portal: If HOTP token is out of sync, the guest portal login fails.
485621	After resetting a password when logging in via guest portal, the success page links the user to the self-service portal instead of the guest portal.
488991	Sponsor selection dropdown doesn't get added to the guest portal self-registration replacement messages after upgrading to 5.3.0.
488992	After upgrading the firmware, restoring the default replacement messages for a modified guest portal self-registration page doesn't add the Sponsor field.
491725	Microsoft Edge removes the referer field, causing a CSRF error.
485559	With PCI mode enabled, FortiToken self-revocation actions should not be allow to proceed if password is invalid.
467587	FQDN / CN comparison for admin GUI SSL certificate is case-sensitive.
468827	When a basic user is promoted to Admin role, their account's expiration date should be removed.
454016	Cannot unassign FortiTokens that are assigned to guest users.
481203	On the Edit RADIUS Client page, clicking the OK button too quickly after clicking Save can result in changes not being saved or an error.

Bug ID	Description
462772	Demoting a remote admin account who has an FortiToken assigned to a user account causes a system error.
476697	When importing local users from a FortiGate configuration file, email addresses and telephone numbers are not imported.
488149	PCI - Do not allow AD users with expired passwords to change them without token entry.
451990	Warning if FortiClient SSOMA secret key is larger than 15 characters.
476087	Can't grant administrator privileges to remote user with a space in their user name.
486544	FortiAuthenticator fails to connect to AD after cluster failover.
489005	Load-balancing doesn't work until after a reboot on FortiAuthenticator KVM.
511093	Radiusd on LB slave FortiAuthenticator in HA setup keeps crashing if large custom radius dictionary is uploaded to the master.
399417	FortiAuthenticator 4.0 - Failover to seconday LDAP server does not occur immediately, and then is not effective.
482913	Information from authorityKeyIdentifier is not used to check the correct CRL for revocation status of user cert.
436030	SAML IdP: Signature verification error on logout.
486198	Token self-provisioning doesn't work for remote users who belong to a group that uses an LDAP filter.
464556	Time-based user expiry configured in usage profile isn't applied to users when they already have an expiry date configured.
470667	FortiAuthenticator Windows Agent ignores certificate revocation.
449443	FortiAuthenticator Windows Agent does not display the user credentials when access the server through RDP.
486923	Unknown Publisher warning when uninstalling FortiAuthenticator Windows Agent.

Appendix A: 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 / 8
Virtual NICs supported (minimum / maximum)	1 / 4
Storage support (minimum / maximum)	60GB / 2TB
Memory support (minimum / maximum)	512 MB / 64GB
High Availability (HA) support	Yes

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**
  Use this image for new VM installations. It contains a deployable OVF virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, https://www.fortinet.com/products/identity-access-management.html#models-specifications.

Appendix B: Maximum values

This section lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware and VM configurations.

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

Hardware appliances

The following table describes the maximum values set for the various hardware models.

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	38	113	513	1013	2013
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333

Feature		Model				
		200E	400E	1000D	2000E	3000E
	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
	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

Feature		Model				
		200E	400E	1000D	2000E	3000E
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] Note that **Users** is the only metric used for the number of allowed users. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[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, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

VM appliances

The FortiAuthenticator-VM Appliance 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.

The following table describes the maximum values set for the various VM models.

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	5	Users / 20	18	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
	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

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
	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					
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

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
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] Note that there is one metric used for the number of allowed users which is **Users**. **Local Users** and **Remote Users** share the same limit value. This enables **Local Users** *or* **Remote Users** to be equal to **Users** or for there to be a mixture of user types, however, the total number of local and remote users cannot exceed the **Users** metric.

[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.