FortiAuthenticator - Release Notes

VERSION 5.2.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

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

FORTINET PRIVACY POLICY

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

FEEDBACK

Email: techdocs@fortinet.com

03/13/2018

FortiAuthenticator 5.2.1 - Release Notes

Revision 1

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™ 5.2.1, build 00161.

FortiAuthenticator is a User and Identity Management solution that provides Strong Authentication, Wireless 802.1X Authentication, Certificate Management, and Fortinet Single Sign-On.

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

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

For more detailed information, see the FortiAuthenticator 5.2.1 Administration Guide.

- Usernames are now included in SMS/Email token codes.
- Certificate Revocation List (CRL) enhancements.
- Active group cache enhancement.
- Increased the maximum group field size for Syslog FSSO.

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 & VM support

FortiAuthenticator™ 5.2.1 supports:

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

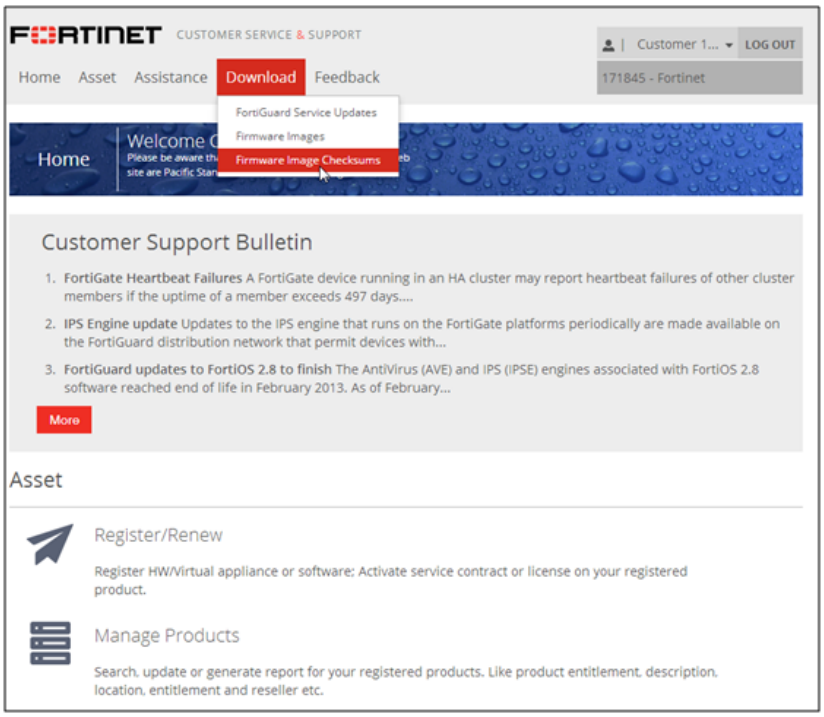
Image checksums

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 Fortinet Customer Service & Support:

https://support.fortinet.com

Customer Service & 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*.

Alternatively, near the bottom of the page, click the *Firmware Image Checksums* button. (The button appears only if one or more of your devices has a current support contract.) In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.

Upgrading from FortiAuthenticator 4.x/5.0/5.1

FortiAuthenticator™ 5.2.1 build 00161 officially supports upgrade from all versions of FortiAuthenticator™ 4.x.x., 5.0.x, and 5.1.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.

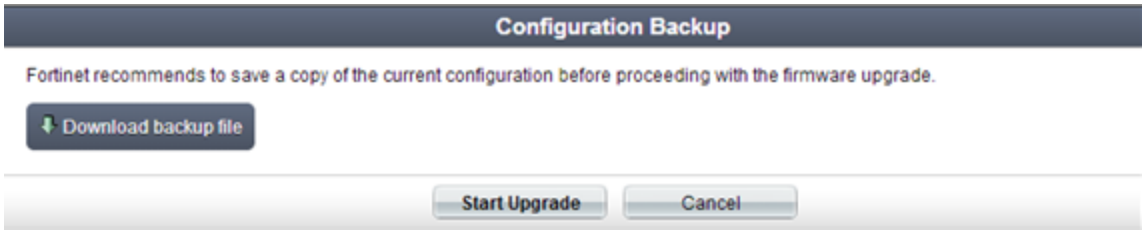
Firmware upgrade process

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 Customer Service & Support web site, then upload it from your computer to the FortiAuthenticator™ unit.

1. Log in to the Customer Service & Support web site at https://support.fortinet.com. 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, then 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™ 5.2.1:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 38
- Mozilla Firefox versions 18 to 54
- Google Chrome versions 28 to 59 (see note below)

Special Note for Google Chrome users

There is a known bug which exists in Google Chrome versions 44 and 45 where initially the GUI loads correctly, however after some time, pages will stop loading with the error on the chrome debug console *"Failed to load resource: net::ERR_INSECURE_RESPONSE"*.

This is a known issue and affects all sites using self-signed certificates and is fixed in Google Chrome version 46. Chrome bug reference: https://code.google.com/p/chromium/issues/detail?id=516808

To work around this issue in the meantime, use a different browser or Upgrade to the Chrome Beta Channel.

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

FortiOS support

FortiAuthenticator™ 5.2.1 supports the following FortiOS versions:

- FortiOS v5.2.11
- FortiOS v5.4.5
- FortiOS v5.6.0

Other FortiOS versions may function correctly, but may not be supported by Fortinet.

Fortinet agent support

FortiAuthenticator™ 5.2.1 supports the following Fortinet Agents:

- FortiClient v.5.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.0.2

- FortiAuthenticator Agent for Outlook Web Access 1.4.0
- 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™ 5.2.1 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0
- Microsoft Hyper-V 2010 and Microsoft Hyper-V 2012 R2
- 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 Fortinet Customer Service & Support:

https://support.fortinet.com.

Bug ID	Description
472878	Offline tokens: Random machine-specific salts containing null bytes not handled properly when generating tokens.
473430	802.1x MAB+Machine Auth+User Authentication do not add correct RADIUS Attributes in response to RADIUS request from FortiSwitch.
461885	Invalid custom dictionary breaks the FortiAuthenticator.
453613	FortiAuthenticator is not able to handle 200+ user 802.1x authentication request.
476754	Firmware upgrade failure.
462184	SAML IDP does not support saml2p prefix.
473233	SSOMA doesn't work with NTLM.
470170	SSO stops working.
472792	DC/TS Agents Logged-on Users shows N/A.
470559	FSSO doesn't capture the change when user is excluded from SSO.
475263	Updating group information manually via the Monitor page fails.
452322	FortiAuthenticator Halts/Impedes the Authentication process.
468042	Dynamic debug log sizes don't actually take effect.
447286	Enter Valid IP address error message for secondary LDAP GUI configuration. FQDN cannot be used.
467682	Sponsor portal: Express guest user creation with random pwd expiry causes GUI crash.
448560	Cannot create user groups.
472447	Remote Sync Rule does not work when some users are missing the search attribute.

Known Issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
451841	FortiAuthenticator Agent service fails to start and/or disconnects after windows update.
404902	FortiAuthenticator Agent for MSWindows: Domain Name contains Hyphen doesn't work correctly.
472625	Self-service portal: GUI crash when changing remote LDAP password
473716	FortiAuthenticator event logs ending with space character causing log search issues on FortiAnalyzer.
449324	Can't delete root CA.
457470	FortiAuthenticator doesn't create the SAN DNS request.
463194	FortiAuthenticator doesn't generate CSR with SAN.
464094	Router entry index increase with every CLI edit.
461156	The FortiClient/SSOMA and DC agent overwrite each other FSSO IP information.
456296	Unable to add another attribute to Radius Custom Dictionaries.
463904	GUI error while re-enabling a user.
476697	Import local users from FortiGate config file - password incorrect, email, telephone number not imported.
475821	SMS directives ignored for system generated password delivery.
462856	Fortigate communication with FAC acting as LDAPs server.

Appendix A: FortiAuthenticator VM

FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator VM system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported virtual machine (VM) environment. For details, see the *Install Guide for FortiAuthenticator VM* available at http://docs.fortinet.com.

VM Requirements

Virtual Machine	Requirement
Virtual Machine 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 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 Open Virtualization Format (OVF) virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortiauthenticator/index.html.

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		FortiAuthenticator 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	30	100	500	1000	2000
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333

Feature		FortiAuthenticator 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	120000
	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.)	50	200	1000	2000	4000
	RADIUS Client Profiles	500	2000	10000	20000	40000
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Sync Rule	25	100	500	1000	2000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120000
FSSO & Dynamic Policies						
FSSO	FSSO Users	500	2000	10000	20000	200000[3]
	FSSO Groups	1000	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		FortiAuthenticator 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 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.

[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.

Maximum Values - Virtual Machines

Feature		Model			
		Unlicensed VM	Calculating Metric	Base 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	5	100
	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	Users x 3	300	15000
	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.)	1	Users / 10	10	500

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
	RADIUS Client Profiles	3	Users	100	10000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Sync Rule	1	Users / 20	5	250
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	30	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	1000
	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	Base VM (100 Users)	Example 5000 licensed User VM
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	200	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.