FortiAuthenticator - Release Notes

VERSION 4.3

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

FEEDBACK

Email: techdocs@fortinet.com

03/10/2017

FortiAuthenticator 4.3 - Release Notes

Revision 1

TABLE OF CONTENTS

Introduction 5
Special Notices 6
TFTP boot process 6
Monitor settings for web-based manager access 6
Before any upgrade 6
After any upgrade 6
What's New 7
Remote user sync rule and MAC-based authentication enhancements 7
Remote user sync rule enhancements 7
Manual import for remote LDAP users 7
MAC device groups 7
SAML SSO Service Provider enhancements 8
SAML IdP General Config: Add link to configure realms 8
Improve SAML IdP successful login page 8
Chained Authentication 8
Auth Client specified by network range 9
Configurable debug log file size 9
Ability to toggle on/off FTM Push for RADIUS users on global basis 9
KVM image for running on KVM server and FortiHypervisor 9
Increase RADIUS client and profile limit 9
LDAP query monitor 9
Update FTM Push credentials via FortiGuard 10
Increase max offline HOTP cache size 10
Upgrade Instructions 11
Hardware & VM support 11
Image checksums 11
Upgrading from FortiAuthenticator v4.0 12
Upgrading from FortiAuthenticator earlier releases 12
Product Integration and Support 14
Web browser support 14
FortiOS support 14
Fortinet agent support 14
Virtualization software support 15
Third party RADIUS authentication 15

Resolved Issues 16
API 16
Captive Portal 16
CLI 16
Certificates 17
FSSO 17
GUI 17
LDAP 18
Logging 18
RADIUS 18
SAML 18
SMS 18
System 19
Vulnerabilities 19
Known Issues 20
GUI 20
FSSO 20
RADIUS 20
SAML 21
SCEP 21
SSH 21
Appendix A: FortiAuthenticator VM 22
FortiAuthenticator VM system requirements 22
FortiAuthenticator VM firmware 22
Appendix B: Maximum values 23
Hardware appliances 23
VM appliances 26

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions and caveats, resolved and known issues for FortiAuthenticator™ 4.3.0, build 0216.

FortiAuthenticator is a User and Identity Management solution enabling including 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 *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

Before upgrading, review the following changes for impact to your unique deployment. Note that this list is not exhaustive but highlights the major feature enhancements in this release.

Remote user sync rule and MAC-based authentication enhancements

A combination of related features have been introduced that add the ability:

- to populate the certificate binding settings for users who use remote user sync rules,
- to use remote user sync rules to allow the importation of users with different username LDAP attributes within a single remote LDAP server,
- and assign MAC devices to different VLANs using RADIUS response attributes after a successful MAC-based authentication.

Remote user sync rule enhancements

Administrators can specify which LDAP attribute to use to populate a user's username and certificate binding CN. When the certificate binding CN field is populated, the *Certificate Binding CA* must also be specified (see under *Authentication* > *User Management* > *Remote User Sync Rules*). The certificate binding CA dropdown must contain the related local CA and trusted CA lists.

To remain consistent, the local and remote users edit page for creating new user certificate bindings have also been updated.

Manual import for remote LDAP users

Manual importations of remote LDAP users now incorporate the username and certificate binding LDAP attributes, as shown when configuring user attributes in the *Import Remote LDAP Users* edit page.

MAC device groups

A new user group type has been introduced for MAC devices (see under *Authentication* > *User Management* > *User Groups*). MAC devices will be available to add in a MAC user group once devices have been created or imported, under *Authentication* > *User Management* > *MAC Auth Bypass*.

Once created, MAC user groups can then be used under the MAC-based authentication section of RADIUS clients, under *Authentication* > *RADIUS Service* > *Clients*. When you enable *Allow MAC-based authentication*, you have the option to enable the *Group filter* which, when enabled, only MAC devices belonging to at least one of the listed groups are allowed to be authenticated. If however the filter is disabled, any of the MAC devices configured under *Authentication* > *User Management* > *MAC Auth Bypass* are accepted.

SAML SSO Service Provider enhancements

A couple enhancements to SAML SP FSSO have been made. The first improvement provides flexibility in determining the username. Most SAML IdP services will return the username in the Subject NameID assertion, however not all IdP services are consistent. In light of this, the administrator can select which assertion to extract the username from.

The second improvement addresses how group membership is acquired. FSSO requires group membership of each user with an active SSO session while different SAML IdP services require different methods of retrieving the group information. Before now, group information could only be obtained from very specific (hardcoded) SAML assertions. Now administrators can choose to convert Azure's group membership UUIDs into names, retrieve group membership from an LDAP service, or configure other assertions which can be used in group membership retrieval.

These new options can be found under *Fortinet SSO Method* > *SSO* > *SAML Authentication*.

If *Convert Azure UUIDs into names* is enabled, you must have already created an SSO group with the Azure UUID added already. To save time, administrators may instead choose to import them directly from Azure.

SAML IdP General Config: Add link to configure realms

A *Configure realms* link has been added in the *Authentication* > *SAML IdP* > *General* to link to the *Authentication* > *Self-service Portal* > *Access Control* page, where the realms are sourced from.

This is similar to the already implemented link between the *Fortinet SSO Methods* > *SSO* > *Portal Services* and *Authentication* > *Self-service Portal* > *Access Control* pages.

Improve SAML IdP successful login page

Successful SAML IdP login results in a hardcoded, non-customizable page appearing (which can be useful for troubleshooting) before the authenticated user is redirected to the SP website. Administrators can now customize the page. In addition, the page's default appearance has been changed to make it look more appealing.

To customize the successful SAML authentication page, go to *Authentication* > *Self-service Portal* > *Replacement Messages*, under a new section called *SAML IdP*.

To make it easier for troubleshooting, tags are included that can be used to display some of the previously available information, such as username, SP, and date/time.

Chained Authentication

FortiAuthenticator now supports chained authentication, providing the ability to chain two different authentication methods together so that, for example, a two-factor authentication RSA solution can validate passcodes via RADIUS.

To configure these settings, go to *Authentication* > *User Management* > *Realms*. When creating a new realm, enable *Chained token authentication with remote RADIUS server*. Note that this option should only be available when selecting a remote LDAP server as the *User source*.

Auth Client specified by network range

Subnets and IP ranges may now be defined in Auth Client settings, under *Authentication* > *RADIUS Service* > *Clients*. All Auth Clients within a defined subnet/IP range will share the same configuration and secret. For example, 192.168.0.0/24 would allow all 255 IP addresses to authenticate. This feature saves time, as the entry only takes up a single client entry in the license table.

Configurable debug log file size

To have access to a longer history of debug log files, a dropdown menu has been added at the top of the `https://<FAC_IP>/debug/` page for changing the maximum log file size, up to a maximum of 50 MB. This is available for only certain debug log types.

Ability to toggle on/off FTM Push for RADIUS users on global basis

Administrators may now toggle on/off FTM Push notifications for RADIUS users. This setting is controlled on a per RADIUS client basis, under *Authentication* > *Radius Service* > *Clients*. This setting is disabled by default.

KVM image for running on KVM server and FortiHypervisor

FortiAuthenticator 4.3.0 includes a KVM image for loading onto KVM servers, such as Linux running Virtual Machine Manager, and on FortiHypervisor.

Increase RADIUS client and profile limit

In some instances, more RADIUS clients are required relative to the number of users. Therefore the ratio for RADIUS clients has been increased from "number of max users / 10" to "number of max users / 3".

The number of RADIUS profiles has also been increased from "number of max users / 10" to "number of max users x 2", since each RADIUS client might need more than one profile.

LDAP query monitor

In some instances, FSSO's performance may have been impeded by Domain Controllers that were slow to answer LDAP queries for group lookup. Because of this, new enhancements for LDAP queries have been introduced, under *Monitor* > *SSO* > *Domains*.

Before now, mousing-over Domain Controllers and their most recent LDAP query showed the status of the query, and how long ago it was. Now it also shows the LDAP query's response time in milliseconds (ms). This response time will show a warning icon if the highest recent response time is above 500 ms.

In addition, you can click on the Domain Controller entry to view statistics for the 100-most recent LDAP queries. The listed response times will be colour coordinated as follows: green for less than 500 ms, orange for time between 500 and 1000 ms, and red for more than/equal to 1000 ms.

Update FTM Push credentials via FortiGuard

Push server credentials for Apple and Google can now be updated via FortiGuard.

Increase max offline HOTP cache size

The offline HOTP cache size limit has been increased from 100 to 1000, under *Authentication* > *User Account Policies* > *Tokens* > *FAC Agent Offline FortiToken Support* > *Enable offline support*.

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™ 4.3.0 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)
- FortiAuthenticator KVM

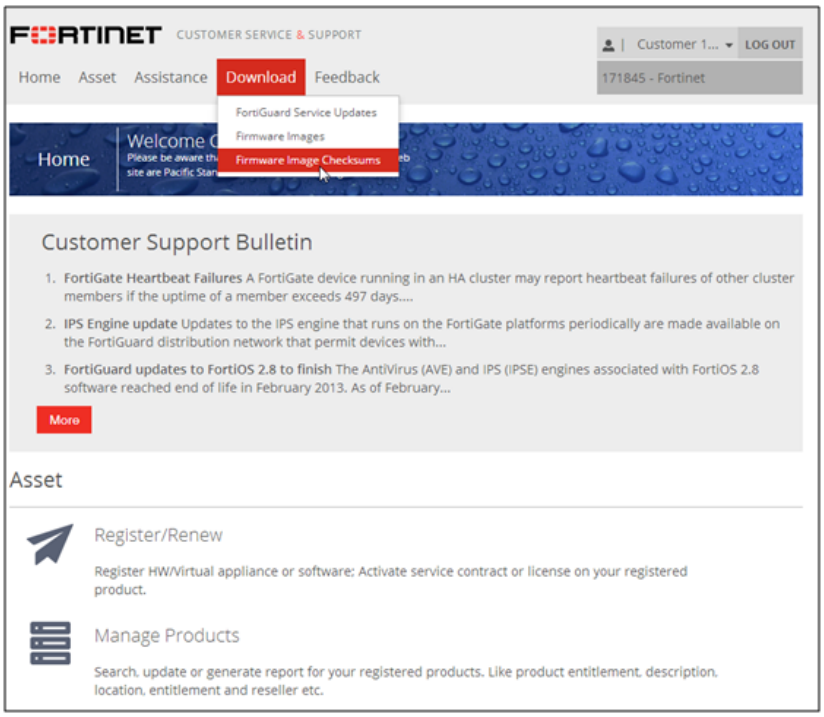
Image checksums

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 v4.0

FortiAuthenticator™ 4.3.0 build 0216 officially supports upgrade from all versions of FortiAuthenticator 4.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 (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.

Upgrading from FortiAuthenticator earlier releases

FortiAuthenticator™ 4.3.0 build 0216 supports upgrade from FortiAuthenticator 3.3.2 build 0182. To upgrade, please follow instructions shown in the relevant firmware release notes.

FortiAuthenticator 4.0.0 build 0008 does **not** support upgrade from FortiAuthenticator 3.3.2 build 0182.

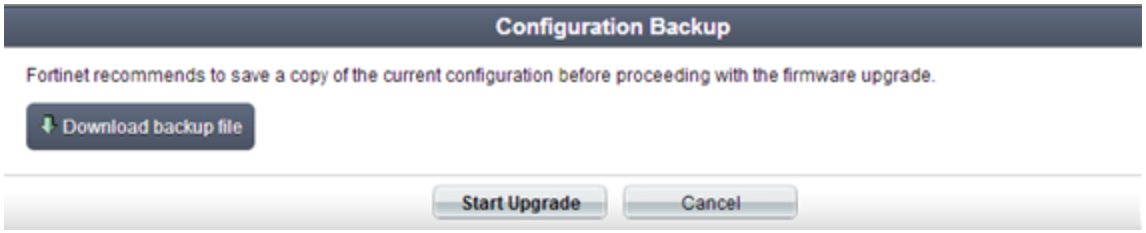
Firmware upgrade process

After backing up your configuration first, follow the following procedure 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™ 4.3.0:

- Microsoft Internet Explorer versions 9 to 11
- Mozilla Firefox versions 18 to 45
- Google Chrome versions 28 to 49 (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™ 4.3.0 supports the following FortiOS versions:

- FortiOS v5.2.9
- FortiOS v5.4.0

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

Fortinet agent support

FortiAuthenticator™ 4.3.0 supports the following Fortinet Agents.

- FortiClient v.5.2.3 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™ 4.3.0 supports VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0.

FortiAuthenticator™ 4.3.0 supports Microsoft Hyper-V 2010 and Microsoft Hyper-V 2012 R2.

FortiAuthenticator™ 4.3.0 supports Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0.

See Appendix A: VM on page 1 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.

API

Bug ID	Description
401260	Revise error message returned by PushAuth.
401370	Error message (pushauthresp) misspells "Alert" (spelled "Alter" instead).
401382	Missing Action and Status messages in the log after a REST API push notification auth attempt.
401579	Rest API push authentication doesn't find a match for LDAP users .

Captive Portal

Bug ID	Description
383599	FAC 4.x external captive portal doesn't function as expected with System Director wireless controller.

CLI

Bug ID	Description
374027	Wrong tz in both CLI and GUI.
388269	CLI is not synchronized with GUI in terms of changing IP address in HA.
406196	FAC-400E: CLI status reporting the wrong number of hard disks.

Certificates

Bug ID	Description
408785	Second local root CA certificate has incorrect expiry time.

FSSO

Bug ID	Description
405638	Delays in processing syslog messages within rsyslog.
405887	FSSO LDAP group lookup performance improvements & monitoring.

GUI

Bug ID	Description
303031	Hide Register link from login page if self-registration disabled.
368775	Admin login does not display source IP.
392769	SAML IDP Settings page shows groups checkbox by default; should only be shown if the parent option is enabled.
400807	FAC FGT Group Filter - Not Importing Groups based on OU.
401473	Push authentication doesn't log in remote RADIUS or LDAP users through GUI.
402463	Missing field causes GUI crash and unit test failure.
405827	Imported RADIUS client's default profile cannot be moved UP/DOWN.
406335	Value too long for type character varying (30) for more than ten Thai characters.
406502	Create RADIUS Client page: TypeError: parent.editorLoaded is not a function.

LDAP

Bug ID	Description
303105	Unable to import LDAP users from Group membership if not expanded.
400193	Remote LDAP users import fails if username contains special character.

Logging

Bug ID	Description
395271	Incorrect Event logged when TOTP token code is reused.
401259	Debug report does not include the logs from "PushAuth" services.
401384	Push notification auth logs in the GUI should be more user-friendly.

RADIUS

Bug ID	Description
403760	RADIUS Authentication allowance can be bypassed by setting NAS-identifier to "FAC_GUI".

SAML

Bug ID	Description
402701	Need a new SAML user attribute: Remote LDAP DisplayName.
406024	Alert on logout.
406704	Log which SP made an authentication request.

SMS

Bug ID	Description
378581	HTTP Parameters' value can not be set to null.

System

Bug ID	Description
400808	NTP Timezone - 'Istanbul, Moscow, St Petersburg, Volgograd' is incorrect.

Vulnerabilities

Bug ID	Description
404706	Samba library vulnerabilities.

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

GUI

Bug ID	Description
401938	FAC2000E - Power supply widget displays PSU's horizontally instead of vertically.
407717	Error when order the Local users by Groups or Authentication Methods at User Management.
408485	Authentication Activity widget causes high CPU/memory usage.
409345	When the "Self-service Portal" is enabled, a user (remote user) with admin access can not log into FAC with two-factor authentication.
409388	Authentication Activity widget displays double the number of actual logins to the FAC.

FSSO

Bug ID	Description
391724	FortiAuthenticator SSO on login portal with LDAP slow for guest wireless users.
409763	SLS (logout) URL doesn't work. Returns error page instead.

RADIUS

Bug ID	Description
375401	Password authentication fails for admins in EAP.
409925	FTM push notification is not sent for admins.
410093	Chained Authentication: Apply to select LDAP group only.

SAML

Bug ID	Description
400466	Support signed auth request with embedded signature.

SCEP

Bug ID	Description
407405	Unable to renew the Certificate automatically when the auto-regenerate-days expired.

SSH

Bug ID	Description
392437	SSH FAC login fails using CHAP/MS.CHAP/MS.CHAPv2 authentication to Cisco ACS remote RADIUS users.

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
	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						

Feature		FortiAuthenticator Model				
		200E	400E	1000D	2000E	3000E
FSSO	FSSO Users	500	2000	10000	20000	200000[3]
	FSSO Groups	1000	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	4000
	RADIUS Accounting SSO Clients	166	666	3333	6666	13333
	RADIUS Client Profiles	500	2000	10000	20000	40000
	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
	TS Agents	512	512	512	512	512
Accounting Proxy	Sources	50	200	1000	2000	4000
	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	500	2000	10000	20000	40000

[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

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
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
	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					

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
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	3	Users / 3	33	1666
	RADIUS Client Profiles	3	Users x 2	200	10000
	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
	TS Agents	512	512	512	512
Accounting Proxy	Sources	3	Users / 10	10	500
	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	200	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users	100	5000

[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.