FortiAuthenticator - Release Notes

VERSION 4.2

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

11/10/2016

FortiAuthenticator 4.2 - Release Notes

Revision 1

TABLE OF CONTENTS

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions and caveats, resolved and known issues for FortiAuthenticator™ 4.2, build 0145.

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.

Support multiple domains for non-AD remote LDAP users

When configuring a remote LDAP server, the new *Add supported domain names* option allows you to enter multiple domain names for remote LDAP server configurations. The FortiAuthenticator can then identify the domain that users on the LDAP server belong to.

FTMv4 push notifications

FortiAuthenticator supports FortiToken one time password push notifications (also called FTMv4 push notifications). Using FTMv4, when required to authenticate with a one time password, users do not have to lookup a code in FortiToken and enter the code into their browser. Instead their FortiToken mobile application is queried and the user just responds to accept the connection and the session is authenticated and access is allowed.

Offline Token Validation - Windows Agent

In previous releases, when using the Windows Agent and being off the network, there were only two options available, both of which were either insecure or not user friendly:

1. **Fail Open:** User is allowed access without a token.
2. **Fail Closed:** User is not allowed access.

You can now configure FortiAuthenticator to allow the Windows Agent to cache future tokens for offline users. This is made possible by using the pre-shared secret to encrypt the OTPs that are sent to the Windows Agent. The file that stores the offline data on the local system is also encrypted.

This feature supports both TOTP and HOTP tokens:

- TOTP Cache can be set between 1 - 14 days (7 by default).
- HOTP Cache can be set between 1 - 100 counts (10 by default).

The new setting, *Enable Offline Support*, is available under *Authentication* > *User Account Policies* > *General*.

Settings for offline tokens (and more options) can be found in the Windows Agent under the *Offline* tab.

Windows AD Multi-Forest Authentication

You can now configure and manage multiple Windows Active Directory forests, up to a maximum of 20 Remote LDAP Servers with Windows AD enabled. This is available under *Authentication* > *Remote Auth. Servers* > *LDAP*.

Monitoring has been refined, including a new field to show the last update time and a reset connection button for each server.

SAML 2.0 IdP

Security Assertion Markup Language (SAML) is used for exchanging authentication and authorization data between an Identity Provider (IdP) and a Service Provider (SP). The FortiAuthenticator, as the IdP, provides trust relationship authentication for unauthenticated users trying to access an SP, such as Google Apps, Office 365, and Salesforce.

SAML Authentication works as follows:

1. A user tries to access a Service Provider, for example Google, using a browser.
2. The Service Provider's web server requests the SAML assertions for its service from the browser.
3. Two possibilities:
   a. The user's browser already has valid SAML assertions, so it sends them to the Service Provider's web server. The web server uses them to grant or deny access to the service. SAML authentication stops here.
   or
   b. The user's browser doesn't have valid SAML assertions, so the Service Provider's web server redirects the browser to the SAML IdP.
4. Two possibilities:
   a. The user's browser is already authenticated with the IdP, go to step 5.
   b. The user's browser is not yet authenticated with the IdP, IdP requests and validates the user's credentials. If successful, go to step 5. Otherwise, access denied.
5. IdP provides SAML assertions for the Service Provider's and redirects the user's browser back to the Service Provider's web server. Go back to step 2.

This feature is available under *Authentication* > *SAML IdP*. Different realms can be selectively enabled while configuring the FortiAuthenticator as the IdP. These realms are available under *Authentication* > *Self-service Portal* > *Access Control*, where they can be enabled, disabled, or group filtered.

GUI changes

Several items have been moved and reorganized in the GUI, including the following:

- *GUI Access* has been renamed to *System Access*, as it now contains GUI, CLI, REST API, and Pre-Authentication options. This is found under *System* > *Administration* > *System Access*.
- A new menu is available for all token settings under *Authentication* > *User Account Policies* > *Tokens*. In addition, *minutes* has been changed to *time steps*.
- Menu options have been refined under *Authentication* > *User Account Policies* > *General*.

Pre-Authentication Disclaimer

You can now add a disclaimer for HTTP, HTTPS, and CLI/SSH access prior to authentication.

These replacement message options, *Pre-Authentication Warning Page* and *Pre-Authentication Warning Message*, is available under *Authentication* > *Self-service Portal* > *Replacement Messages*.

RADIUS Access-Challenge token request

You can now add a RADIUS Access-Challenge replacement message that requires users to provide their token code. The replacement message is a text string for the Reply-Message attribute of the RADIUS Access-Challenge requesting the token code.

This is also available under *Authentication* > *Self-service Portal* > *Replacement Messages*.

Configurable CLI timeout

You can now control the timeout of the CLI separately from the GUI (between 0 - 480 minutes).

The option, *CLI Access*, is available under *System* > *Administration* > *System Access*.

SNMP trap - Disk Utilization

A new SNMP trap that controls the disk utilization threshold is available (default value is 80%).

The setting, *Disk Utilization Trap Threshold (%)*, is available under *System* > *Administration* > *SNMP*.

Changes to SSH

Similarly to the change made to the CLI, SSH has been modified:

- **Limited SSH login attempts:** After three (3) attempts the interface/connection will reset.
- **SSH timeout:** SSH will timeout after 60 seconds for an incomplete login or broken session. Successful logins will still be subject to the CLI timeout setting.

In addition, OpenSSH has been patched.

Added FortiToken 220 support

FortiAuthenticator 4.2 officially supports the new FortiToken 220, a form factor OTP token card with an integrated NFC chip. The NFC chip can be used, with compatible devices, to read the token data and copy the token to your local clipboard for pasting into required applications.

These tokens will be used in the same way existing FortiToken 200 tokens are. Incidentally, all references to "FTK 200" have been replaced with "FortiToken Hardware" to accommodate for the new product.

NTP enhancements

A number of NTP enhancements have been added for this release:

- You can now configure a second additional NTP server, where the first NTP server can be configured to be the preferred server.
  - The second server is configurable under the *System Information* widget when changing the *System Time*.
- MD5/SHA1 symmetric authentication has been added.
- Logging of repeated error messages is now set to once an hour instead of every two (2) minutes.
- NTP server code has been updated.

Native FortiAnalyzer Logging support

Logging settings have been refined to support Syslog and Native FortiAnalyzer separately. Note that FortiAnalyzer logging only supports configuration for one FortiAnalyzer unit running version 5.4.2 B1117.

These settings are available under *Logging* > *Log Config* > *Log Settings* > *FortiManager/FortiAnalyzer*.

OpenSSL update

OpenSSL has been upgraded to 1.0.1u.

TCP Stack Hardening

You can now configure the number of TCP SYNACK retries for the Linux kernel between 1 - 255 (3 by default). This is available at:

`https://<FAC_IP>/debug/tcp_tuning`

For more information about these features, please refer to the What's New or Administration Guides.

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™ 4.2 supports:

- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000C
- FortiAuthenticator 1000D
- FortiAuthenticator 3000B
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare & Hyper-V)

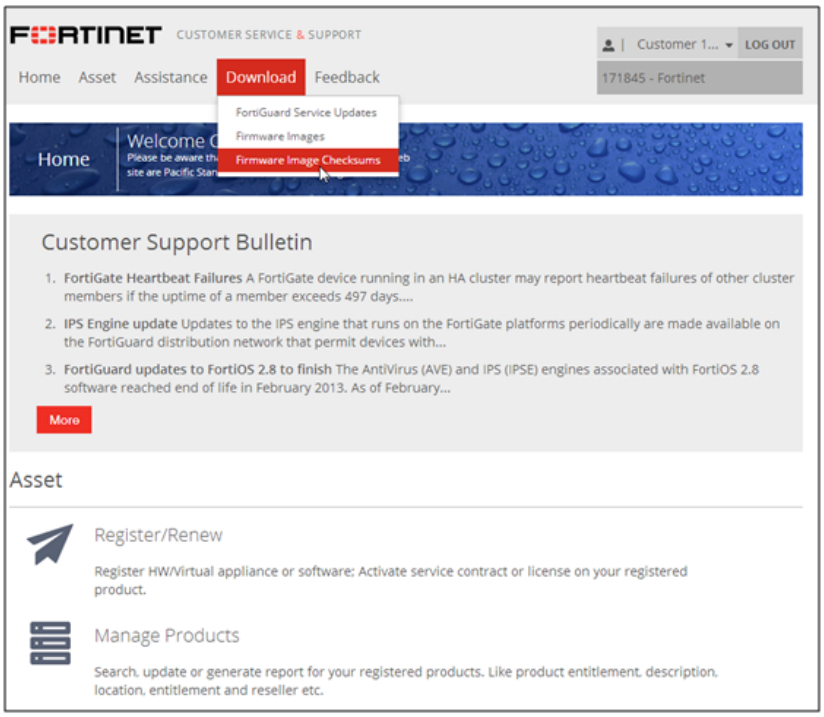
Image checksums

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™ 4.2 build 0144 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™ 4.2 build 0144 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.

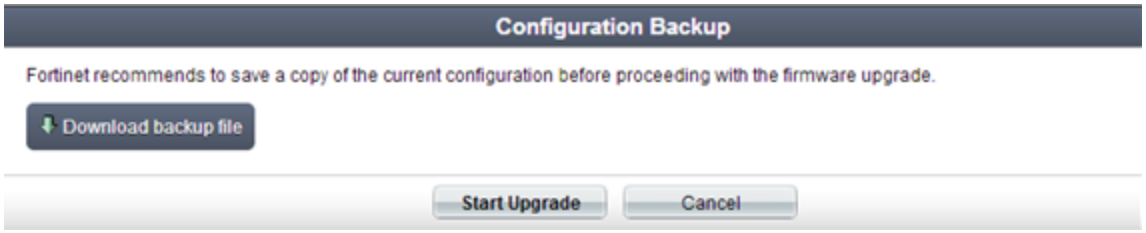
Firmware upgrade process

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™ 4.2:

- 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™ 4.2 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™ 4.2 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™ 4.2 supports VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0

FortiAuthenticator™ 4.2 supports Microsoft Hyper-V 2010 and Microsoft Hyper-V 2012 R2.

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
387846	REST API SSO authentication is case sensitive for local users.
376107	Manual importing users from an LDAP server creates new users instead of updating existing users if their OU or CN has changed.
390222	802.1x EAP-TLS: client certificates not working with 3rd Party CA.

CLI

Bug ID	Description
386653	Administrator name case checking now works correctly when logging into the CLI.
392821	Fixed OpenSSH memory exhaustion vulnerability (CVE-2016-8858).

FSSO

Bug ID	Description
380880	User filtering doesn't work in FSSO FortiGate filtering.
380458	SSO Portal: no logoff button after user logs on to portal.
385345	FortiAuthenticator Agent log gives incorrect date for last known token.
390212	Fixed the issue caused by NT_STATUS_BUFFER_TOO_SMALL error.
393368	IPfiltering rule cannot be deleted.

GUI

Bug ID	Description
373796	LDAP Browser performance issues, added checkboxes to nodes.
381523	Slow dashboard widgets.
391232	End of Daylight Savings (DST) timezone Turkey/Istanbul GMT +3.
381997	Set HTTPS cookies to be secure-only.
390032	Password reset form does not normalise local user username.
389044	FAC-VM: Enter Valid IP address error message for LDAP GUI configuration. FQDN cannot be used.
387744	Choosing a different realm from the Access Control Settings page causes 'duplicate key value' server error.
371026	FTM trial license activation enable/disable in wrong section of GUI page.
374105	Multiple non-functioning 'Add a realm' links appear in the Self-service Portal Access Control page.
380447	Improper sanitization of NTP IP address.
381305	Tooltip for 'Email/SMS token timeout' field has been rephrased to make it clearer.
391758	Added a confirmation dialog for the Logoff All button in the SSO Sessions page.
393200	Fixed GUI user authentication with FortiToken.

HA

Bug ID	Description
370834	HA A-P: Slave clock drifting.
366197	Demo FTM tokens are not supported and cannot be used in a FortiAuthenticator HA-LB configuration.
388522	HA A-P cluster reports incorrect HA status on the GUI.
391670	LB cluster becomes out of sync after removing several local user accounts.
392194	Users get disabled in LB backup unit next day after enabling lockout inactive user.

RADIUS

Bug ID	Description
390525	RADIUS process stops responding after failure to send sms via http/https leading to fac login failure.

System

Bug ID	Description
389212, 389197	OpenSSL Security Advisory.
374507	Linux Kernel Vulnerabilities.
380910	Add TCP Stack Hardening Configuration.
370012	FAC stops responding after upgrading from 4.0.1 B0019 to 4.1.0 B0073.
392981	Fixed CVE-2016-5195 - Linux Kernel Dirty Cow Vulnerability.
373699	NTP enhancements to fix a number of NTP-related vunlerabilities including CVE-2016-1551, CVE-2016-1549, CVE-2016-2516, CVE-2016-2518, CVE-2016-2519, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2015-7704, and CVE-2015-8138.

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

Authentication

Bug ID	Description
379529	Error when trying to clone a RADIUS client die to duplicate key value.

FortiAuthenticator Agents

Bug ID	Description
393234	FortiAuthenticator Agent reported as malicious by some virus scanners.
394402	FortiAuthenticator OWA agent version 1.4 does not run on Exchange 2016 OWA servers.

System

Bug ID	Description
389676	MAC address configured as a local user is not matching if there is no '-' (hyphen) in the name.
289457	FAC Windows Agent not pre-filling RDP domain in some circumstances.
393692	User's password expiration and notification email's timing.
390602	The FortiAuthenticator fsae processes crashes with signal 11 (Segmentation fault).
390218	Insufficient NTLM debug log message: invalid domain/user from NTLM type3: (unknown).
384540	Some FortiAuthenticator log messages are not compatable with FortiAnalyzer.

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				
		200D	400C	1000C/D	3000B	3000D
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	25	100	500	1000	2000
	Language Files	50	50	50	50	50
Authentication						
General	Auth Clients (NAS)	50	200	1000	2000	4000

Feature		FortiAuthenticator Model				
		200D	400C	1000C/D	3000B	3000D
	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	120K
FSSO & Dynamic Policies						

Feature		FortiAuthenticator Model				
		200D	400C	1000C/D	3000B	3000D
FSSO	FSSO Users	500	2000	10000	20000	200K[3]
	FSSO Groups	1000	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	4000
	RADIUS Accounting SSO Clients	50	200	1000	2000	4000
	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	100K	200K
	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 3000D, 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 / 10	10	500

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 / 10 (min=10)	10	50
	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.