

FortiAuthenticator - Release Notes

VERSION 4.3.3

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



08/04/2017

FortiAuthenticator 4.3.3 - Release Notes

Revision 1

TABLE OF CONTENTS

Introduction	4
Special Notices	5
TFTP boot process	5
Monitor settings for web-based manager access	5
Before any upgrade	5
After any upgrade	5
What's New	6
Upgrade Instructions	7
Hardware & VM support	7
Image checksums	7
Upgrading from FortiAuthenticator v4.0	8
Upgrading from FortiAuthenticator earlier releases	8
Product Integration and Support	10
Web browser support	10
FortiOS support	10
Fortinet agent support	10
Virtualization software support	11
Third party RADIUS authentication	11
Resolved Issues	12
Known Issues	13
Appendix A: FortiAuthenticator VM	14
FortiAuthenticator VM system requirements	14
FortiAuthenticator VM firmware	14
Appendix B: Maximum values	15
Hardware appliances	15
VM appliances	18

Introduction

This document provides a summary of enhancements, support information, installation instructions and caveats, resolved and known issues for FortiAuthenticator™ 4.3.3, build 0226.

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.

Note that this is a patch release which fixes a few issues found in the release of 4.3.2. See [Resolved Issues](#) for the issues addressed in this patch release.

To see the major feature enhancements of 4.3, see the [FortiAuthenticator 4.3.0 Release Notes](#).

There are no new features introduced 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 & VM support

FortiAuthenticator 4.3.3 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

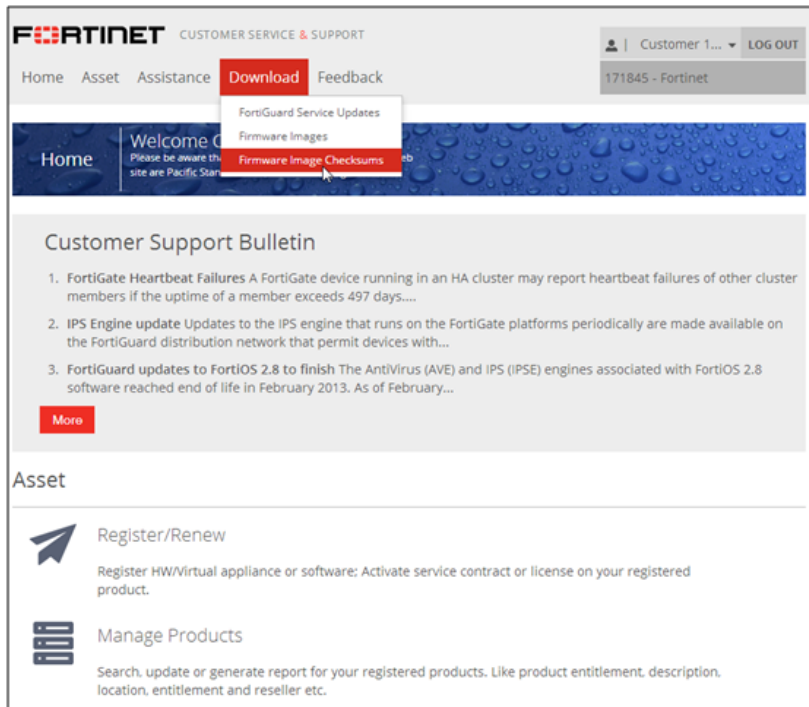
Image checksums

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™ 4.3.3 build 0226 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 4.3.3 build 0226 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.

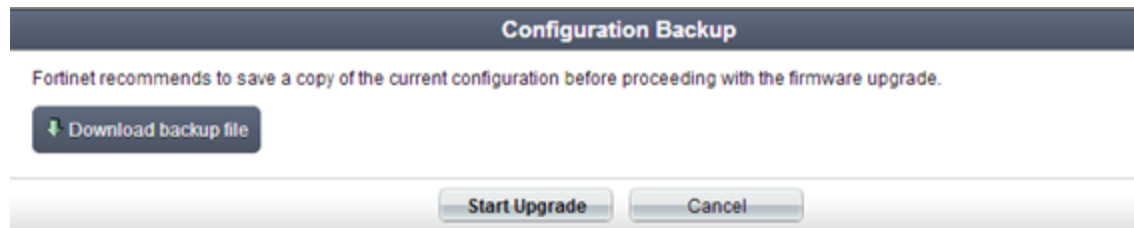
Firmware upgrade process

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™ 4.3.3:

- 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™ 4.3.3 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™ 4.3.3 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™ 4.3.3 supports VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0.

FortiAuthenticator™ 4.3.3 supports Microsoft Hyper-V 2010 and Microsoft Hyper-V 2012 R2.

FortiAuthenticator™ 4.3.3 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>.

This patch release fixes the following issues found in the release of 4.3.2.

Bug ID	Category	Description
439392	Power Supplies Monitor (FAC-2KE/3KE only)	FAC-2000E: PSU Voltage Fault.
422886	Power Supplies Monitor (FAC-2KE/3KE only)	FAC-3000E: recurring false positive logs about missing power supply unit.
442253	2FA	FTM push notification delivery failure on iOS devices.
407405	SCEP	B0008: Unable to renew the Certificate automatically when the auto-regenerate-days expired.
434968	SCEP	Make SCEP enrollment table size limit same as User Certificates.
440338	SCEP	B0012: SCEP enrollment does not work - cannot generate certificate from FortiManager.
424106	FAC-KVM	Missing the graphical components required for the menu layout after licensing the FortiAuthenticator.
412039	Remote LDAP user sync	Remote LDAP user sync failed with group filter.

Known Issues

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

<https://support.fortinet.com>

Bug ID	Category	Description
415911	GUI	B0155: FortiAuthenticator becomes unresponsive after disabling HA feature.
440255	GUI	GUI Packet Capture not working.
385150	GUI	B0081: User Inventory widget shows negative numbers.
416413	Self-service Portal	When "Allow users to re-provision their FortiToken Mobile" is enabled remote LDAP users cannot log in to self-registration portal.
415023	Remote LDAP users sync rule	Remote LADP sync can't add all returned users.
436525	Remote LDAP user sync rule	User DN Field limit to 255 characters.
412856	Remote LDAP user sync rule	Can't get correct result while filtering on FortiAuthenticator.
420935	2FA	B0218: FTM Push Authentication not working when public IP/FQDN configured with alternate port.
440645	Certificates	UTF8 support in Certificates.
435094	RADIUS	FortiAuthenticator Version 4.3.2 build 0222 MAC Authentication Bypass does not work with DELL Switch N-Series.
392437	RADIUS	B0081: SSH FortiAuthenticator login fails using CHAP/MS.CHAP/MS.CHAPv2 authentication to Cisco ACS remote radius users.
442176	FSSO	SSO failed to connect to LDAP server.
437004	FSSO	FortiGate Explicit proxy - NTLM issues seen between FortiGate and FortiAuthenticator.
442900	HA	Remote Radius Administrator causing HA Sync anomalies with LB Slave.
408883	SMS	SMS with third-party vendors generates errors for HTTP status codes other than 200.

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
	Sources	50	200	1000	2000	4000
Accounting Proxy	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
	CA Certificates	10	10	50	50	50
Certificate Authorities	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					

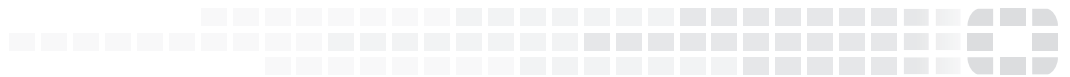
Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	30	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	3	Users / 3	33	1666
	RADIUS Client Profiles	3	Users 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.

FORTINET®

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.