



FortiPortal - Release Notes

Version 5.3.3

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



August 6, 2020

FortiPortal 5.3.3 Release Notes

37-533-612126-20200806

TABLE OF CONTENTS

Change Log	4
Introduction	5
What's new	5
Product Integration and Support	6
FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions	6
Additional compatibility resources	7
Hypervisor support	7
Database Support	7
Web browser support	8
FortiPortal 5.3.3 software	8
Special Notices	10
Special Characters	10
Collector High Availability	10
Reconfiguring MySQL password on FortiPortal	10
Initial Log Aggregation Delay	11
SSID Naming	11
Supported FortiManager API Endpoints	11
Upgrade Information	12
Performing a backup	14
Upgrading the portal	14
Upgrading the collector	15
Upgrading to FortiPortal 5.3.3 and later if you are using a custom CSS file	15
Resolved Issues	17
Common vulnerabilities and exposures	18
Known Issues	19

Change Log

Date	Change Description
2020-03-20	Initial release.
2020-05-05	Updated to add support for FortiManager, FortiAnalyzer, and FortiOS 6.2.3.
2020-05-27	Updated to add support for FortiManager- FortiAnalyzer 6.2.5 and FortiOS 6.2.4.
2020-06-29	Added FortiManager- FortiAnalyzer 6.0.9 and FortiOS 6.0.10 to FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions on page 6.
2020-08-06	Added FortiOS 5.4.x support to FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions on page 6.

Introduction

FortiPortal is a self-service portal for FortiManager and a hosted security analytics management system for the FortiGate, FortiWifi, and FortiAP product lines. FortiPortal is available as a virtual machine (VM) software solution that can be deployed on a hosted services infrastructure. This allows enterprises and managed security service providers (MSSP) to build highly customized private cloud services for their customers.

This document provides information about FortiPortal version 5.3.3, build 0300. It includes the following sections:

- [What's new on page 5](#)
- [Product Integration and Support on page 6](#)
- [Special Notices on page 10](#)
- [Upgrade Information on page 12](#)
- [Resolved Issues on page 17](#)
- [Known Issues on page 19](#)

What's new

This release contains the following new features and enhancements:

- You now have more choices for filtering data on the service provider dashboard. You can now specify last 5 minutes, last 30 minutes, last 60 minutes, last 4 hours, last 12 hours, last 1 day, last 7 days, or custom time period.
- There is a new DB Version field on the System Info page (Admin > System Info) that displays the FortiPortal database version.
- You can now use the domain name when adding a FortiManager device or FortiAnalyzer device to your FortiPortal.
- When you update the Virtual IP object in FortiPortal, the changes are now automatically made in FortiManager.
- The client IP address is now displayed in the audit log instead of the proxy server address.

Product Integration and Support

FortiPortal 5.3.3 supports some FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox versions.

The section contains the following topics:

- [FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions on page 6](#)
- [Database Support on page 7](#)
- [FortiPortal 5.3.3 software on page 8](#)

FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions

The FortiPortal self-service interface for MSSP customers uses the FortiManager API for FortiGate firewall policy and IPsec VPN configuration.

FortiPortal optionally connects FortiGate wireless controllers for wireless analytics.

FortiPortal allows users to view FortiAnalyzer reports assigned to the MSSP customer.

FortiPortal 5.3.3 supports the following product versions:

Product	Supported Versions	Recommended Version
FortiAnalyzer (for reports and analytics)	<ul style="list-style-type: none">• 6.2.5• 6.2.1 to 6.2.3• 6.0.0 to 6.0.9	6.2.5
FortiAnalyzer (for reports)	<ul style="list-style-type: none">• 6.2.5• 6.2.1 to 6.2.3• 6.0.0 to 6.0.9• 5.6.7 to 5.6.11• 5.6.0 to 5.6.5	6.2.5
FortiManager	<ul style="list-style-type: none">• 6.2.5• 6.2.1 to 6.2.3• 6.0.0 to 6.0.9• 5.6.7 to 5.6.11• 5.6.0 to 5.6.5• 5.4.0 to 5.4.6• 5.2.10	6.2.5
FortiOS	<ul style="list-style-type: none">• 6.2.1 to 6.2.4• 6.0.10• 6.0.0 to 6.0.8• 5.6.0 to 5.6.11	6.2.4

Product	Supported Versions	Recommended Version
	<ul style="list-style-type: none"> • 5.4.x • 5.2.x 	
FortiSandbox	<ul style="list-style-type: none"> • 3.0.2 	3.0.2



Use FortiGate 4.0.0 or later to get support for local APs.



If you are using FortiManager version 5.2.3 or later, you must ensure that the FortiManager user account (that you created for FortiPortal) has *Remote Procedure Call (RPC)* set to *read-write*. In previous FortiManager releases, RPC was enabled by default. FortiManager version 5.2.3 introduced a new setting that you might need to configure as follows:

```
config system admin user
  get - lists all of the users (along with userids)
      - note the userid for the FPC user.
  edit <FPC userid>
    set rpc-permit read-write
```

Also see:

- [Additional compatibility resources on page 7](#)
- [Hypervisor support on page 7](#)

Additional compatibility resources

Refer to the FortiOS, FortiManager, and FortiAnalyzer release notes on the [Fortinet Docs Library](#) for detailed compatibility information.

Hypervisor support

The following hypervisor platforms are supported:

- VMware ESX Server versions 5.5, 6.0, 6.5, and 6.7
- KVM Version 2.6.x

Database Support

The following MySQL versions are supported:

- MySQL 5.5.x
- MySQL 5.7.x



If you are using MySQL 5.7.x, the following changes must be added to the `my.cnf` file:

```
sql_mode =
    STRICT_TRANS_TABLES,
    NO_ZERO_IN_DATE,
    NO_ZERO_DATE,
    ERROR_FOR_DIVISION_BY_ZERO,
    NO_AUTO_CREATE_USER,
    NO_ENGINE_SUBSTITUTION
```

In addition, the following MariaDB server versions are supported:

- 10.2.X-MariaDB-10.2.X+maria~xenial-log mariadb.org binary distribution
-



The MariaDB server versions do not require additional configuration, except for *Bind-Address* and *Grant Privileges*. See *FortiPortal Administration Guide > Upgrading FortiPortal software* on the [Fortinet Docs Library](#).

Web browser support

The following web browsers are supported:

- Microsoft Internet Explorer (IE) Version 11
 - Mozilla Firefox (up to) Version 49
 - Google Chrome Version 52
-



Other (versions of the) browsers might also function but are not fully supported in this release.

FortiPortal 5.3.3 software

FortiPortal is delivered as virtual machine OVF/QCOW2 files for the VMware/KVM hypervisors.

To download the OVF files:

1. Navigate to the Fortinet Customer Service and Support website (<https://support.fortinet.com/>).
2. Select *Download > Firmware Images*.
3. In the Firmware Images page, select *FortiPortal*.
4. To use OpenStack KVM, download the latest QCOW2 files (one portal file and one collector file):
fpcvm64image-kvm-portal.qcow2.zip
fpcvm64image-kvm-collector.qcow2.zip

OR

To use VMWare, download the latest OVF files (one portal file and one collector file):

fpcvm64imagePortal.out.ovf.zip
fpcvm64imageCollector.out.ovf.zip



If you are using VMWare, you can download one virtual application (vApp) file (instead of the above .ovf files) that contains the portal and collector VM information. The vApp file name is:

fpcvm64imagevApp.out.ovf.zip

When you install this .ovf file, the vSphere client will create the portal and collector VMs as a single cluster as well as an example MySQL VM.

Detailed installation instructions are included in the *FortiPortal Administration Guide* on the [Fortinet Docs Library](#).

Special Notices

This section contains the following:

- [Special Characters on page 10](#)
- [Collector High Availability on page 10](#)
- [Reconfiguring MySQL password on FortiPortal on page 10](#)
- [Initial Log Aggregation Delay on page 11](#)
- [SSID Naming on page 11](#)
- [Supported FortiManager API Endpoints on page 11](#)

Special Characters

In earlier releases, you could include some special characters in controller names. For example, the following name would be valid:

```
Name '1/3
```

However, in release 2.4.0 and later, you cannot use special characters. Before upgrading to release 2.4.0, you must remove these special characters from existing names.

Collector High Availability

When using collectors in an HA configuration, you must reboot the slave collectors and collector databases before adding them to FortiPortal.

Reconfiguring MySQL password on FortiPortal

If you change the password for the FortiPortal user in the MySQL portal database, you need to update the configuration in the portal and collector(s):

```
config system sql
  set status remote
  set database-type mysql
  set password <mysql_password>
end
```

Initial Log Aggregation Delay

After FortiPortal starts to receive logs, there may be a delay of up to 15 minutes before the aggregated data appears on the dashboard.

SSID Naming

The SSID name and interface name (which is configured on the FortiGate or FortiWireless Controller) needs to be the same for the FortiPortal to receive the data for this controller.

Supported FortiManager API Endpoints

The following FortiManager API configuration endpoints are supported by FortiPortal.

Policy & Object endpoints

dynamic/interface
 spamfilter/profile
 webfilter/profile
 dlp/sensor
 antivirus/profile
 ips/sensor
 webfilter/ftgd-local-cat
 webfilter/ftgd-local-rating
 application/list
 firewall/address
 firewall/addrgrp
 firewall/schedule/onetime
 firewall/schedule/recurring
 firewall/service/custom
 firewall/service/group
 firewall/vip
 firewall/vipgrp
 firewall/ippool
 user/local
 user/group
 firewall/policy
 reinstall/package
 revision

Device Manager endpoints

vpn/ipsec/phase1-interface
 vpn/ipsec/phase2-interface
 router/static

Upgrade Information

This section provides instructions to upgrade FortiPortal from an earlier version to a more recent version.



Before upgrading FortiPortal, back up the portal database. If the upgrade fails, you can restore the portal database from the backup.

For FortiPortal 5.0 and later, you must download a new license file from <https://support.fortinet.com/>.

To upgrade from version 4.2.0 or later, you can upgrade directly to version 5.0.0.

To upgrade from version 3.2.2 or earlier, you must:

1. Perform a sequential set of upgrades to version 4.0.0.
2. Upgrade from version 4.0.0 to version 4.1.2.

If you are upgrading from a version prior to version 4.0.0, refer to the following table to determine your upgrade path. Find your existing version in the *Existing Version* column of the table and determine the more recent versions to which you can upgrade in the *Compatible Upgrade Version* column. When you upgrade to a more recent version, repeat this process until you're running the most recent version.

Existing Version	Compatible Upgrade Version
2.1.0	2.1.1
2.1.1	2.2.0
2.2.0	2.2.1, 2.2.2, 2.3.0
2.2.1	2.2.2, 2.3.0
2.2.2	2.3.0
2.3.0	2.3.1
2.3.1	2.4.0, 2.4.1
2.4.0	2.4.1, 2.5.0, 3.0.0
2.4.1	2.5.0, 2.5.1, 3.0.0, 3.1.0
2.5.0	2.5.1, 3.0.0, 3.1.0
2.5.1	3.0.0, 3.1.0, 3.1.1, 3.1.2
3.0.0	3.1.0, 3.1.1, 3.1.2
3.1.0	3.1.1, 3.1.2, 3.2.0
3.1.1	3.1.2, 3.2.0
3.1.2	3.2.0, 3.2.1, 3.2.2
3.2.0	3.2.1, 3.2.2, 4.0.0

Existing Version	Compatible Upgrade Version
3.2.1	3.2.2, 4.0.0, 4.0.1
3.2.2	4.0.0, 4.0.1, 4.0.2, 4.0.3
4.0.0	4.1.2
4.0.1	4.1.2
4.0.2	4.1.2
4.0.3	4.1.2
4.0.4	4.1.2
4.1.0	4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4
4.1.1	4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4
4.1.2	4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4
4.2.0	5.0.3
4.2.1	5.0.3
4.2.2	5.0.3
4.2.3	5.0.3
4.2.4	5.0.0, 5.0.1, 5.0.2, 5.0.3
5.0.0	5.2.0
5.0.1	5.2.0
5.0.2	5.2.0
5.0.3	5.2.0
5.1.0	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3
5.1.1	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3
5.1.2	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3
5.2.0	5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3
5.2.1	5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3
5.2.2	5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3
5.2.3	5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3
5.2.4	5.2.5
5.3.0	5.3.1, 5.3.2, 5.3.3
5.3.1	5.3.2, 5.3.3
5.3.2	5.3.3

Also see:

- [Performing a backup on page 14](#)
- [Upgrading the portal on page 14](#)
- [Upgrading the collector on page 15](#)
- [Upgrading to FortiPortal 5.3.3 and later if you are using a custom CSS file on page 15](#)

Performing a backup

To perform a backup:

1. You can export (or create a snapshot of) a VM for a backup. For example, for VMware, from the vSphere client, shut down the database VMs from the VM console. If you are using the sample MySQL database, log in as user `fpc`, get root privileges, type `sudo su`, and type `shutdown now`.
2. For VMware users, go to *File > Export > Export OVF Template* to export the VM.
3. For *Name*, set a name for the backup.
4. For *Directory*, select a directory from which you can restore the backup to vSphere.
5. Optionally, enter a *Description* for the backup.
6. Select *OK*.
7. After the backup is complete, right-click the virtual machine you backed up and go to *Power > Power On*.



You can use <https://mysqlbackupftp.com> to back up the portal and collector database.

Upgrading the portal

To upgrade the portal:

1. Log in to the portal using a service provider (administrator) account.
2. Select the *Admin* tab.
3. Select *FPC Admin* to open the administrator portal. The administrator portal opens in a new browser tab.
4. Log in to the administrator portal. The default user name is `admin`, and there is no default password.
5. Select the *System Settings* tab.
6. In the *System Information* widget, select the *Update* button beside the *Firmware Version*.
7. In the pop-up dialog, select *Choose File* and select the portal `.out` file that you downloaded from the Fortinet Customer Service & Support website (<https://support.fortinet.com/>).
8. Select *OK*. The portal will upgrade. After the firmware is upgraded, the system will restart automatically.



Check that the version number in the *Admin > System Info > Version Information > Version* field in the FortiPortal administrative web interface matches the version number in the administrator portal (*System Settings > Dashboard > Firmware Version*). If these two numbers do not match, the portal has not finished upgrading. You must wait for the portal to finish upgrading before upgrading the collector.



If you have a RADIUS server configured in an existing version, you must re-enter the RADIUS attributes after the portal upgrade is complete. For details, see the *FortiPortal Administration and User Guide*.

Upgrading the collector

For a collector HA cluster, first upgrade the master and then the slaves. Repeat these steps for each collector:

1. Restart each collector, one at a time.
2. Log in to the portal using a service provider (administrator) account.
3. Select the *Devices* tab.
4. Select the *FPC Collectors* tab.
5. Click the IP address of the collector to open that collector's administrator portal. The administrator portal opens in a new browser tab.
6. Log in to the administrator portal. The default user name is `admin`, and there is no default password.
7. Go to *System Settings*.
8. In the *System Information* widget, select the *Update* button beside the *Firmware Version*.
9. In the pop-up dialog, select *Choose File* and select the collector `.out` file that you downloaded from the Fortinet Customer Service & Support website (<https://support.fortinet.com/>).
10. Select *OK*. The collector will upgrade. After the firmware is upgraded, the system will restart automatically.

Upgrading to FortiPortal 5.3.3 and later if you are using a custom CSS file



If you are using a CSS file for a custom theme, back up the CSS file before upgrading to FortiPortal5.3.3.

This section focuses on significant changes in FortiPortal5.3.3 that affect using a custom CSS file as the color scheme when upgrading to version 5.3.3 and later. The following changes were made to the FortiPortal CSS:

- FortiPortal5.3.3 uses Bootstrap 4 style naming, grid system, table, button, and other styles.
 - FortiPortal5.3.3 uses Font Awesome as the font for the entire web interface.
-



The Fontello font family is not supported.

- The button style has been changed and renamed. The previous `.flat_button` class will be deprecated in the future. Two new buttons, solid and hollow, have been added. Use `.fpc-btn` with `.btn.btn-primary` and `.btn.btn-outline-secondary`.
- Fortinet recommends using the `.btn.btn-primary.fpc-btn` class for general function buttons (such as *Submit*, *Save*, *OK*, *Yes*, and *Add*) and using the `.btn.btn-outline-secondary.fpc-btn` class for negative buttons (such as *Cancel* and *No*).
- The following CSS classes have been removed and will no longer be used:
 - `.device_box_progress`
 - `.login-footer-text`
 - `.login-info-header`
 - `.login-header`
 - `.header-user-info`
 - `.ui-widget textarea`
 - `.ui-widget button`
 - `.menu_button_on_c`
 - `.menu_button_off_c`
 - `.sbHolder`
 - `.sbOptions`
 - `.settingsHeaderDiv`
 - `.myNavigation`
- The header height has been reduced. The header logo ratio is the same, which prevents the image from overlapping the menu.

The following table describes major changes in CSS class names in the `place_holder_custom.css` file:

CSS class (before FortiPortal5.3.3)	CSS class in FortiPortal5.3.3 and later
<code>.login-header</code>	<code>.pub-temp-body .headerTopClass</code>
<code>.footerText</code>	<code>.footerText</code> <code>.footerText a</code>
<code>.login-footer-text</code>	<code>.pub-temp-body .footerText</code> , <code>.pub-temp-body .footerText a</code>
<code>#fpcfooterDiv a</code>	<code>.footerText a</code>
<code>.flat_button</code>	<code>.btn-primary.fpc-btn</code>
<code>.widget-header</code>	<code>.ui-dialog .ui-widget-header</code> <code>.modal-header</code>
<code>.ui-button</code>	<code>.btn-primary.fpc-btn</code>
<code>.ui-widget-content</code>	<code>.ui-state-default .ui-widget-content .ui-state-default:not(('.fpc-btn'))</code>

Resolved Issues

The following issues have been fixed in 5.3.3. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
571078	After four failed login attempts, FortiPortal does not block the user.
574497	Remote user authentication using FortiAuthenticator does not work.
591891	When a policy package is shared with multiple devices, you cannot install it on a single device.
595644	Changing the authentication from local to RADIUS and then configuring it causes a 403 Forbidden error.
598897	After upgrading FortiPortal and changing from Collector mode to FortiAnalyzer mode, FortiPortal does not display customer dashboard information.
599343	Some emailed FortiPortal reports cannot be opened.
599854	Users cannot edit policies when the Internet Service option is not used.
601313	Adding or editing application overrides in an application sensor profile causes a "data is invalid for selected url" error.
605703	Resetting the password in FortiPortal causes an "old password is not correct" error.
606218	A custom service group cannot be created if the customer role does not include the VipObject-Read-Only permission.
606847	Tomcat's property file is not updated when restoring the backup on a FortiPortal unit.
607048	The "secure" attribute needs to be added to the Set-Cookie HTTP response header, and the SSLCertificateChainFile and the ca_chain.crt file need to be removed.
608728	When an admin selects a log file to download, the latest ftnt_fpc.log is always downloaded.
608738	When failover happens to a FortiManager HA cluster, FortiPortal loses connectivity with the FortiManager cluster.
608941	The user cannot change the report time period from "Last 1 Day" on the Reports > FortiPortal page.
611839	After disabling the "Send Files to Sandbox for inspection" option and saving the configuration, the "Send Files to Sandbox for inspection" option is not displayed in the Edit Antivirus Filter Profile form.
612542	Updating FortiPortal should update the web.xml file as well.

Common vulnerabilities and exposures

FortiPortal 5.3.3 is no longer vulnerable to the following CVEs:

- CVE-2004-1653

Visit <https://fortiguard.com/psirt> for more information.

Known Issues

The following issues have been identified in FortiPortal 5.3.3. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
408255	With SSO enabled after upgrading from version 3.2.0 to 3.2.1, the default login page loads rather than the SSO login page.
424414	The Wildcard FQDN option for address objects need to be disabled for ADOM versions 5.4.X and earlier.
458423	When policies and objects have been imported from the FortiManager unit, the status is displayed as "Policy Package Uninstalled" in the <i>Policy & Objects > Policy</i> navigation pane. Workaround: Re-install the policy package to make the status show as "installed."
530216	Nested virtual IP groups are not displayed when editing the firewall policy.
590535	FortiPortal cannot connect to the MySQL (8.0) server.
592068	The FortiPortal collector database grows bigger than the configured size and ignores the global retention policy.
595541	The table element <code>role="presentation"</code> should be added to all tables.
599001	After upgrading to FortiPortal 5.2.4, some web profiles are not working correctly.
603635	The FortiPortal administrator should be able to decrease the customer database quota when needed.
604392	After upgrading to FortiPortal 5.3.1, the number in the Devices Allowed [Used] field changed on the <i>Admin > System Info</i> page.
604702	Session logs are not displayed on the View page in FortiPortal, even though the collector VM is collecting logs.
610340	The FortiAnalyzer 6.0.0 API does not generate FortiAnalyzer reports in HTML format.
611411	Upgrading from FortiPortal 5.2.3 to 5.3.2 failed.
611913	The <i>View > Sandbox</i> page does not provide information about source and destination IP addresses.
620175	Under Policy & Object Edit Permissions, the DLP Sensor check box is mislabeled as "properties."



FORTINET®



Copyright© 2020 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.