

# Release Notes

**FortiADC 7.2.0**



**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/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



February 3, 2023

FortiADC 7.2.0 Release Notes

01-544-677187-20230203

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>What's new</b>	<b>6</b>
<b>Hardware, VM, cloud platform, and browser support</b>	<b>9</b>
<b>Resolved issues</b>	<b>11</b>
<b>Known issues</b>	<b>13</b>
<b>Image checksums</b>	<b>14</b>
<b>Upgrade notes</b>	<b>15</b>
Supported upgrade paths	15
Upgrading a stand-alone appliance	16
Upgrading an HA cluster	17
Special notes and suggestions	18

## Change Log

Date	Change Description
February 3, 2023	FortiADC 7.2.0 Release Notes initial release.

# Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.2.0, Build 0210.

To upgrade to FortiADC 7.2.0, see [Upgrade notes](#).

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: <https://docs.fortinet.com/product/fortiadc>.

# What's new

FortiADC 7.2.0 offers the following new features:

## Global Load Balance

### DNS over HTTP, HTTPS and TLS support

FortiADC now supports DoH (DNS over HTTP/HTTPS) and DoT (DNS over TLS) to increase user privacy and security by using the HTTP/HTTPS or TLS protocol to encrypt the DNS queries. You can now enable DNS over HTTP, HTTPS or TLS through the GLB Zone Tools general settings.

## Server Load Balance

### New AUTH class Lua scripting function

The BEFORE\_AUTH function has been added to trigger the event before authentication is performed to enable the user-group specified by the function to override the authentication result of the original authentication policy. This allows users to apply different levels of authentication based on the client information via script.

### HTTP persistence Lua scripting function enhancements

Enhancements have been made to the HTTP persistence Lua scripting functions:

- HTTP:persist() function extended to support HTTP\_REQUEST event to enable access to other HTTP elements in PERSISTENCE.
- New LB:get\_value\_routing() function added to enable users to obtain an alternative backend.
- New LB:get\_current\_routing() function added to show the currently allocated backend.
- New LB:method\_assign\_server() function added to obtain the server through the current load balance method.

### New addrbook check added to avoid port conflict with named default port 53

Port 53 has been added to the addrbook when GLB is enabled to place a port limitation on port 53 when it is used in GLB as the named port and in GLB licd.

### Layer 4 server load balance debug flow enhancements

The Layer 4 server load balance diagnose debug flow has been enhanced to support the following:

- Filtering by virtual server name and/or the traffic pattern.
- Layer 4 flow debug messages for error cases.
- Enhanced help string filtering to match the protocol number with the protocol.

## Improvements to Layer 4 FTP profile

To minimize the impact of Layer 4 FTP virtual servers on Layer 7 virtual servers, L4 NAT/FullNAT will now only listen on port 21, and L4 Direct Routing/Tunneling will listen to ports 21/1024-65535.

In scenarios where the L4 load balance module cannot find an existing session or a service for an FTP data packet with port 20 or 1024-64435, the L4 load balance module would search for an FTP virtual server with the same IP. As the L4 load balance module is listening to port 20/1024-64435, as well as port 21 for L4 FTP virtual servers, it interferes with L7 virtual servers if the L7 VS has port 1024-65535, and the IP happens to be the same as the L4 FTP VS.

## Security

### New Bot Mitigation sub-modules for the Web Application Firewall

Two new Bot Mitigation sub-modules have been added to the FortiADC Web Application Firewall:

- Threshold Based Detection detects the occurrence of suspicious behaviors within a specified time frame to determine whether the request is coming from a human or a bot.
- Biometrics Based Detection detects client events, such as mouse movement, keyboard, screen touch, and scroll within a specified period to determine whether the request is coming from a human or a bot.

### ZTNA enhancements in FortiView

New columns have been added to the FortiView > ZTNA page to enhance the real-time status monitoring of the endpoints registered to FortiClient EMS. The new columns include: Public IP, Tags, MAC, OS Type, and OS Version.

## System

### FortiADC AWS Auto Scaling support

FortiADC now supports Auto Scaling on AWS. Multiple FortiADC-VM instances can form an Auto Scaling Group (ASG) to provide highly efficient clustering at times of high workloads. You can now deploy FortiADC-VMs to support Auto Scaling on AWS using the AWS Cloud Formation Template (CFT) as part of a manual deployment process.

### Automations workflow redesign and enhancements

The FortiADC Automations workflow has now been redesigned with the following enhancements:

- Triggers and Actions are now configured separately and referenced in the Automation configuration.
- System predefined configurations that were previously uneditable can now be modified and applied as user-defined configurations.
- System predefined configuration templates are now available to be cloned and used as templates for user-defined configurations.

### **TACACS+ remote authentication support**

FortiADC now supports Terminal Access Controller Access-Control System (TACACS+) as a remote authentication option. TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers.

### **Declarative REST API enhancements**

Declarative API capabilities have been enhanced to allow verifications of uploaded declarations and an easy means of getting a snapshot of the current system.



# Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.2.0. All supported platforms are 64-bit version of the system.

## Supported Hardware:

- FortiADC 300D
- FortiADC 400D
- FortiADC 100F
- FortiADC 120F
- FortiADC 200F
- FortiADC 220F
- FortiADC 300F
- FortiADC 400F
- FortiADC 1000F
- FortiADC 1200F
- FortiADC 2000F
- FortiADC 2200F
- FortiADC 4000F
- FortiADC 4200F
- FortiADC 5000F

For more information on the supported hardware models, see FortiADC's [Hardware Documents](#).

## Supported hypervisor versions:

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
Microsoft Hyper-V	Windows Server 2012 R2, 2016 and 2019
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5
OpenStack	Pike
Nutanix	AHV

## Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)

- OCI (Oracle Cloud Infrastructure)
- Alibaba Cloud

For more information on the supported cloud platforms, see the FortiADC [Private Cloud](#) and [Public Cloud](#) documents.

**Supported web browsers:**

- Mozilla Firefox version 59
- Google Chrome version 65

We strongly recommend you set either of the Web browsers as your default Web browser when working with FortiADC. You may also use other (versions of the) browsers, but you may encounter certain issues with FortiADC's Web GUI.

## Resolved issues

The following issues have been resolved in FortiADC 7.2.0 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0879270	Httpoxy crashes when deleting a hidden field name using the wrong object.
0878635	GCP spinlock issue.
0874221	NFR request to change the position of GUI drop-down menu items for "log out" and "reset configuration" to align with the GUI of other Fortinet products.
0874118	After upgrading to FortiADC 7.0.4, Automation alert email subjects default to "FADC_Alert".
0873838	In the GUI, HA remote IP monitor allowed to create children table before the parent table is saved.
0873773	Memory leak issue caused by configuration synchronization after upgrading to FortiADC 6.2.5.
0871641	Loss of connectivity between FortiADC and FortiAnalyzer due to hardware platforms attempting to use a certificate that is not available to them.
0868982	WCCP did not work with VDOM.
0867226	The Cookie Security policy Max Age unit is based in minutes in the GUI, but the value that is inserted to the cookie is based on seconds, which means the given range would be incorrect.
0865060	SNMP does not respond for power supply trap.
0862865	Layer 7 virtual server frontend SNI incorrectly contains real server local certificate.
0862575	File upload fails with Antivirus engine error when scanning JSON attachments due to access violation in the last byte of the body.
0858336	CORS Protection deny access even for legitimate traffic specified in Allowed Origin.
0857019	FortiADC console displays kernel related messages when <code>execute reload</code> command is executed.
0855871	Upgrade failed due to unsupported "firewall nat-snat" IPv6 configuration.
0852948	Unable to switch between polling/epoll mode in FortiADC 7.x.x due to shell user restrictions.
0850561	SLB stops responding to SSL requests due to WAF function handling special filename in multi-part, which contains invisible characters and longer than 255.

Bug ID	Description
0848745	Health check does not fail even when the real server is not configured with the services due to some daemon being unable to register the cmdb event.
0847611	High spike in CPU usage and random reboots.
0845338	FortiADC reporting wrong interface speed with SNMP.
0826635	FortiADC crashed after changing the virtual server type from Layer 4 to Layer 2.
0826540	<p>In the GUI, failed to append child list when configuring Automation. This results when an alert type has reached the maximum entry capacity. The current maximum is 256 entries for each alert type, as categorized in the backend CLI:</p> <ul style="list-style-type: none"> <li>• <code>config system alert-policy</code></li> <li>• <code>config system alert-action</code></li> <li>• <code>config system alert</code></li> <li>• <code>config system alert-email</code></li> <li>• <code>config system alert-snmp-trap</code></li> <li>• <code>config system alert-script</code></li> <li>• <code>config system alert-webhook</code></li> <li>• <code>config system alert-fortigate-ip-ban</code></li> <li>• <code>config system alert-syslog</code></li> </ul> <p><code>config system alert-policy</code> configurations are often composed of multiple <code>config system alert</code> entries, making the <code>config system alert</code> most likely to exceed the entry capacity. Please use <code>show full-configuration system alert</code> for details in the CLI.</p>
0823165	<p>HA synchronization issues caused by comments.</p> <p>In an HA environment, if you are using a predefined automation configuration, resetting the configuration through the GUI (using the reset button) or unsetting comments through CLI will cause the HA synchronization to fail whenever a device reboots and rejoins the cluster. Using the GUI reset button resets the predefined configuration values to the predefined default values, all except the comments value which is set to the default value on the backend. For example, if using the HA predefined configuration, the reset will result in <code>set comments HA</code> → <code>set comments comments</code>. When a new device (or a rebooted device) joins the HA cluster, the synchronization will fail due to the mismatched <code>set comments</code> value between the device that has the predefined default value (<code>set comments HA</code>) and the reset device that has the default value (<code>set comments comments</code>).</p> <p>In the CLI, if <code>set comments</code> in the predefined configuration has been unset and is the default value <code>set comments comments</code>, then the same HA synchronization issue will occur.</p>
0805652	Cannot revert predefined automation configurations to default values without affecting HA environment.

## Known issues

This section lists known issues in version FortiADC 7.2.0, but may not be a complete list. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0879016	GUI: The warning message for admin password conformation rules should not show for REST API admin.
0878735	GUI: Unable to save the parent Automation Trigger configuration and create the Alert Metric Expire Member child configuration on the same page.
0877061	GUI: An empty message box appears after saving FortiGSLB connector configuration.
0875825	GUI: Does not exit configuration dialog automatically by clicking "Save" when configuring Member for MD5 Key List.
0875812	When using FSA/FSA cloud, uploading a file larger than 1.3 MB (oversized) causes the AV logs to report "AV engine meet error: archive corrupted".
0875797	For the server-load-balance L7 virtual-server type explicit_http, the resolve host responds with incorrect IP address at certain condition.
0874263	GUI: When editing an existing Interface configuration, the Virtual Domain option should be greyed out.
0859571	PPPoE not functioning on physical interface.
0859565	After executing factory reset, the console shows the message indicating that the "bind failed" due to the address already being in use.
0838441	The same IP address can be configured on two different interfaces, with one being the static IP and the other from PPPoE.
0835874	Should be able to control minimal-responses to enhance named performance.

# Image checksums

To verify the integrity of the firmware file, use a checksum tool and 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 Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, 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.

## Customer Service & Support image checksum tool

The screenshot displays the Fortinet Customer Service & Support portal. At the top, a blue banner reads "Welcome Samuel Liu" and "Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time." Below this is a "Customer Support Bulletin" section with three items: "AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...", "IPS engine 3.532 released to FortiGuard for FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...", and "IPS engine 3.532 released to FortiGuard for FDS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...". A "More" button is visible. The "Asset" section includes "Register/Renew" and "Manage Products". The "Assistance" section contains "Create a Ticket", "Manage Tickets", "View Active Tickets", "Technical Web Chat", and "Contact Support". The "Quick Links" section on the left has a red box around "Firmware Images" and "VM Images Download". The "Resources" section on the right lists "Customer Support Bulletin", "Knowledge Base", "Fortinet Video Library", "Fortinet Document Library", "Discussion Forums", and "Training & Certification".

Home | Welcome Samuel Liu  
Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time.

**Customer Support Bulletin**

1. AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...
2. IPS engine 3.532 released to FortiGuard for FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FDS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...

[More](#)

**Asset**

[Register/Renew](#)  
Register HW/Virtual appliance or software; Activate service contract or license on your registered product.

[Manage Products](#)  
Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

**Assistance**

[Create a Ticket](#)  
The recommended way to contact Fortinet support team for your registered product. Please provide detailed information in the ticket to ensure efficient support.

[Manage Tickets](#)  
Check ticket status, add comment, update contact or view history etc.

[View Active Tickets](#)  
Check latest active tickets for current user, update ticket information or change ticket status.

[Technical Web Chat](#)  
Provide quick answers on-line for general technical questions.

[Contact Support](#)  
Contact information of Fortinet worldwide support centers.

**Quick Links**

- [Firmware Images](#)
- [VM Images Download](#)
- [Service Updates](#)
- [Product Life Cycle](#)
- [Fortinet Service Terms & Conditions](#)
- [Guidelines, Policies & Documents](#)
- [Help Documents](#)

**Resources**

- [Customer Support Bulletin](#)
- [Knowledge Base](#)
- [Fortinet Video Library](#)
- [Fortinet Document Library](#)
- [Discussion Forums](#)
- [Training & Certification](#)

# Upgrade notes

This section includes upgrade information about FortiADC 7.2.0.

## Supported upgrade paths

This section discusses the general paths to upgrade FortiADC from previous releases.

If you are upgrading to a version that is in a higher version level, you will need to upgrade to the nearest branch of the major level incrementally until you reach the desired version. For example, to upgrade from 5.3.5 to 6.1.5, you will follow the upgrade path below:

5.3.5 → 5.4.x → 6.0.x → 6.1.5

(wherein "x" refers to the latest version of the branch)

### 7.1.x to 7.2.x

Direct upgrade via the web GUI or the Console.

### 7.0.x to 7.1.x

Direct upgrade via the web GUI or the Console.

### 6.2.x to 7.0.x

Direct upgrade via the web GUI or the Console.

### 6.1.x to 6.2.x

Direct upgrade via the web GUI or the Console.

### 6.0.x to 6.1.x

Direct upgrade via the web GUI or the Console.

### 5.4.x to 6.0.x

Direct upgrade via the web GUI or the Console.

### 5.3.x to 5.4.x

Direct upgrade via the web GUI or the Console.

### 5.2.x to 5.3.x

Direct upgrade via the web GUI or the Console.



For more information on upgrading from versions earlier than 5.2.x, please see the Upgrade Instructions document for that version.

## Upgrading a stand-alone appliance

The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- Updates the firmware on the inactive partition and then makes it the active partition.
- Copies the firmware on the active partition, upgrades it, and installs it in place of the configuration on the inactive partition.

For example, if partition 1 is active, and you perform the upgrade procedure:

- Partition 2 is upgraded and becomes the active partition; partition 1 becomes the alternate partition.
- The configuration on partition 1 remains in place; it is copied, upgraded, and installed in place of the configuration on partition 2.

This is designed to preserve the working system state in the event the upgrade fails or is aborted.

Firmware			
<a href="#">Upgrade Firmware</a>			
Partition	Active	Last Upgrade	Firmware Version
1	Enable	Thu Jul 7 05:15:02 2022	FA-VMX-7.00.01-FW-build0022
2	Disable	Mon Jun 6 14:12:21 2022	FA-VMX-6.01.04-FW-build0140
<a href="#">Boot Alternate Firmware</a>			


### Before you begin:

- You must have super user permission (user admin) to upgrade firmware.
- Download the firmware file from the Fortinet Customer Service & Support website:  
<https://support.fortinet.com/>
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

### To update the firmware:

1. Go to **System > Settings**.
2. Click the **Maintenance** tab.
3. Scroll to the **Firmware** section.
4. Click **Upgrade Firmware** to locate and select the firmware file.



5. Click  to upload the firmware and reboot.  
The system replaces the firmware on the alternate partition and reboots. The alternate (upgraded) partition becomes the active, and the active becomes the alternate.
6. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

## Upgrading an HA cluster

The upgrade page includes an option to upgrade the firmware on all nodes in an HA cluster from the primary node.

The following chain of events occur when you use this option:

1. The primary node pushes the firmware image to the member nodes.
2. The primary node notifies the member nodes of the upgrade, and takes on their user traffic during the upgrade.
3. The upgrade command is run on the member nodes, the systems are rebooted, and the member nodes send the primary node an acknowledgment that the upgrade has been completed.
4. The upgrade command is run on the primary node, and it reboots. While the primary node is rebooting, a member node assumes the primary node status, and traffic fails over from the former primary node to the new primary node.

After the upgrade process is completed, the system determines whether the original node becomes the primary node, according to the HA Override settings:

- If Override is enabled, the cluster considers the Device Priority setting. Both nodes usually make a second failover in order to resume their original roles.
- If Override is disabled, the cluster considers the uptime first. The original primary node will have a smaller uptime due to the order of reboots during the firmware upgrade. Therefore, it will not resume its active role. Instead, the node with the greatest uptime will remain the new primary node. A second failover will not occur.

### Before you begin, do the following:

1. Make sure that you have super user permission (user admin) on the appliance whose firmware you want to upgrade.
2. Download the firmware file from the Fortinet Customer Service & Support website:  
<https://support.fortinet.com/>
3. Back up your configuration before beginning this procedure. Reverting to an earlier version of the firmware could reset the settings that are not compatible with the new firmware.
4. Verify that the cluster node members are powered on and available on all of the network interfaces that you have configured. (Note: If required ports are not available, HA port monitoring could inadvertently trigger an additional failover, resulting in traffic interruption during the firmware update.)
5. You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

**To update the firmware for an HA cluster:**

1. Log into the web UI of the *primary* node as the `admin` administrator.
2. Go to **System > Settings**.
3. Click the **Maintenance** tab.
4. Scroll to the **Upgrade Firmware** button.
5. Click **Choose File** to locate and select the file.
6. Enable the **HA Cluster Upgrade**.
7. Click ⓘ to upload the firmware and start the upgrade process.

After the new firmware has been installed, the system reboots.



When you update software, you are also updating the web UI. To ensure the web UI displays the updated pages correctly:

- Clear your browser cache.
- Refresh the page.

In most environments, press Ctrl+F5 to force the browser to get a new copy of the content from the web application. See the Wikipedia article on browser caching issues for a summary of tips for many environments:

[https://en.wikipedia.org/wiki/Wikipedia:Bypass\\_your\\_cache](https://en.wikipedia.org/wiki/Wikipedia:Bypass_your_cache).

---

## Special notes and suggestions

### 7.2.0

- HSM does not support TLS v1.3. If the HSM certificate is used in VS, the TLS v1.3 handshake will fail.  
**Workaround:** Uncheck the TLSv1.3 in the SSL profile if you are using the HSM certificate to avoid potential handshake failure.
- Keep the old SSL version predefined configuration to ensure a smooth upgrade.

### 7.0.2/7.1.x

- After upgrading to 7.0.2/7.1.x, in Virtual Machine HA environments where both nodes have been installed with certificate embedded licenses you must reinstall those licenses. As some backend certificate files would have been synchronized and overwritten by the HA Peer (due to an existing bug), the certificate file would not be recoverable. Reinstalling the certificate embedded licenses is required to ensure they would work properly where they are needed, such as in ZTNA or FortiSandbox Cloud.

### 7.0.0

- When deploying the new GSLB based on FortiADC 7.0.0, the verify-CA function will be enabled by default.

### 6.2.2

- To use the SRIOV feature, users must deploy a new VM.

## **6.2.0**

- In version 6.2.0, the default mode of QAT SSL has been changed to polling.

## **6.1.4**

- Before downgrading from 6.1.4, ensure the new L7 TCP or L7 UDP application profiles are deleted or changed to a profile type that is supported in the downgrade version. Otherwise, this will cause the cmdb to crash.

## **5.2.0-5.2.4/5.3.0-5.3.1**

- The backup configuration file in versions 5.2.0-5.2.4/5.3.0-5.3.1 containing the certificate configuration might not be restored properly (causing the configuration to be lost). After upgrading, please discard the old 5.2.x/5.3.x configuration file and back up the configuration file in the upgraded version again.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.