



# Release Notes

FortiNDR 7.6.2



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<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>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<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)



May 29, 2025

FortiNDR 7.6.2 Release Notes

55-762-1154830-20250529

# TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>Change Log</b>                                   | <b>4</b>  |
| <b>Introduction</b>                                 | <b>5</b>  |
| <b>FortiNDR version 7.6.2</b>                       | <b>6</b>  |
| <b>Licensing</b>                                    | <b>7</b>  |
| Netflow and OT Security Services licenses           | 7         |
| <b>New features and enhancements</b>                | <b>8</b>  |
| NDR muting profiles                                 | 8         |
| Security Fabric                                     | 8         |
| NDR logs  | 9         |
| FortiAuthenticator                                  | 10        |
| Supported models                                    | 10        |
| Demo mode   | 10        |
| Encrypted FortiAnalyzer connection                  | 10        |
| CLI   | 10        |
| New CLI commands:                                   | 10        |
| CLI updates:  | 11        |
| <b>System integration and support</b>               | <b>12</b> |
| <b>Upgrade information</b>                          | <b>13</b> |
| Firmware  | 13        |
| FNR-1000F, FNR-3500F (gen3 and above) and FNR-3600G | 13        |
| VM Devices  | 13        |
| Downloading the latest firmware version             | 14        |
| Upgrading the firmware version                      | 14        |
| <b>Supported models</b>                             | <b>16</b> |
| *Notice about hardware generations                  | 16        |
| <b>Resolved issues</b>                              | <b>18</b> |
| <b>Known issues</b>                                 | <b>19</b> |

# Change Log

| Date       | Change Description   |
|------------|--|
| 2025-05-23 | Initial release.   |
| 2025-05-26 | Updated <a href="#">Introduction</a> on page 5, <a href="#">New features and enhancements</a> on page 8, and <a href="#">Upgrade information</a> on page 13. |
| 2025-05-29 | Updated <a href="#">Upgrade information</a> on page 13 and <a href="#">Supported models</a> on page 16.  |

# Introduction

FortiNDR (On-premises) is Fortinet's Network Detection and Response product, targeted for on-premises installation where no network metadata leaves the network, supporting OT and air-gapped infrastructure. FortiNDR form factors include appliances, VM/KVM and public cloud (BYOL), with distributed sensor and center support. FortiNDR can classify both network-based and file-based (malware) threats, provide network visibility, including East-West traffic in Datacenter/Cloud environments. The solution is equipped with Artificial Neural Networks (ANN) to classify malware into attack scenarios, surface outbreak alerts, and trace the source of malware infections. Network-based attacks such as intrusions, botnets, compromised IOCs, weak ciphers and vulnerable protocols can also be detected. Supervised and unsupervised machine learning (ML) continuously analyze metadata across networks to identify threats; remediation can be leveraged via Fortinet Security Fabric.

# FortiNDR version 7.6.2

This document provides information about FortiNDR version 7.6.2 build 0645.

These Release Notes include the following topics:

- [New features and enhancements on page 8](#)
- [System integration and support on page 12](#)
- [Supported models on page 16](#)
- [Resolved issues on page 18](#)
- [Known issues on page 19](#)

# Licensing

Please refer to the FortiNDR ordering guide for licensing details:

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortindr.pdf>.

Customers must have the correct SKU for FortiNDR functionalities to work.

## Netflow and OT Security Services licenses

Netflow and OT Security Services licenses are ordered separately for sensors and standalone deployment.

# New features and enhancements

This document provides information about FortiNDR version 7.6.2 build 0645.

The following is a summary of new features and enhancements in version 7.6.2. For details, see the [FortiNDR 7.6.2 Administration Guide](#) in the [Document Library](#).

## NDR muting profiles

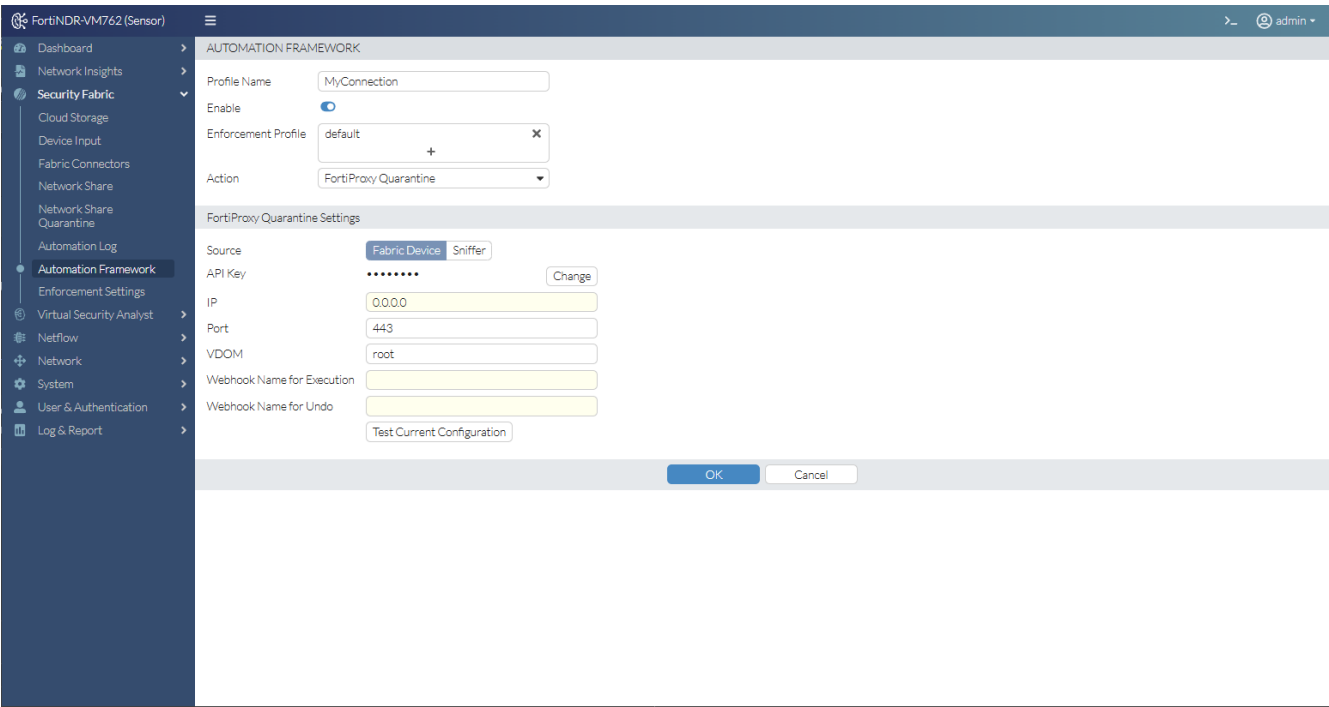
NDR muting has been enhanced with *Muting Profiles* that allow users to combine anomaly types, IP ranges, ports and sensors to create *Muting Rules*. Muting profiles allow you to configure an NDR muting rule from an anomaly type with any value. For example, when you mute the *FortiNDR ML Discovery* rule, you can configure the profile to only hide destination device vendor anomalies. You can also schedule the time the profile will be active. Muting rules are applied to future anomalies for the time period specified by the muting profile.

For more information, see [NDR Muting](#) in the *FortiNDR Administration Guide*.

## Security Fabric

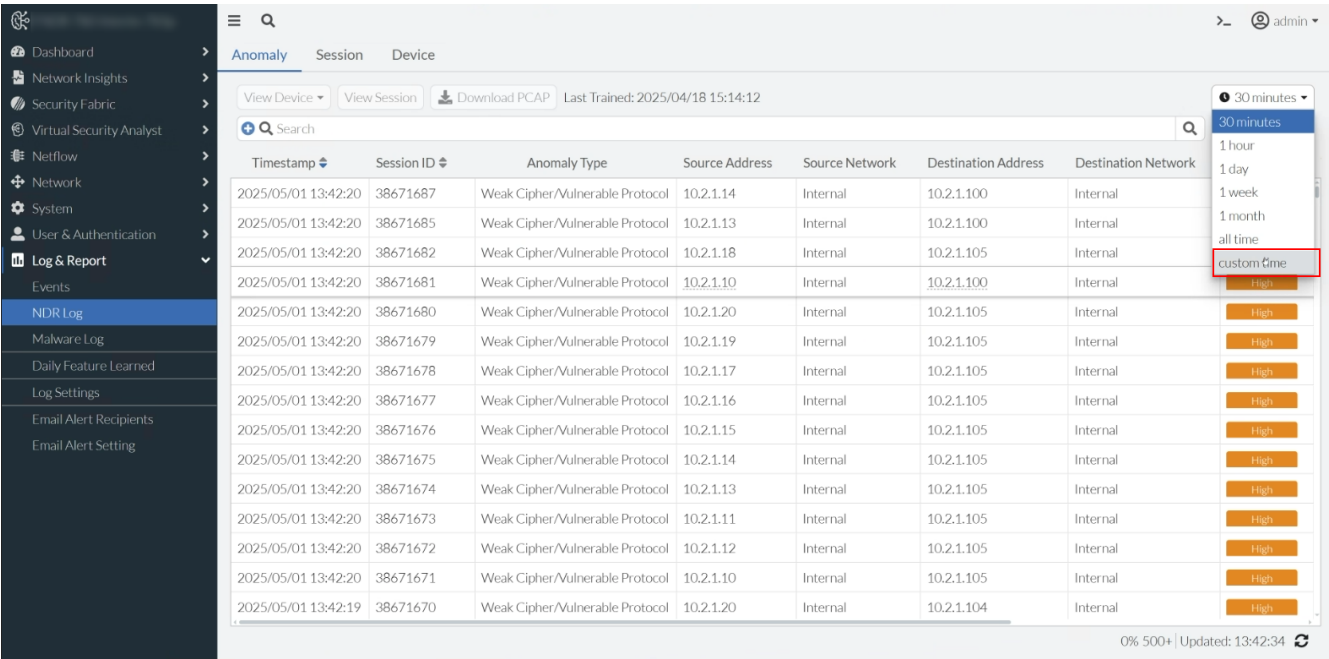
FortiNDR automation framework profiles now support FortiProxy.





## NDR logs

You can now create a custom time range in the *NDR Logs > Anomaly* tab. Custom time ranges are useful when you know the specific time of traffic activity, helping to reduce page load time.



## FortiAuthenticator

FortiNDR now supports FortiAuthenticator push notifications.

## Supported models

FortiNDR now supports FNDR-2500G hardware models and FortiNDR for OCI cloud deployments.

## Demo mode

FNDR demo mode has been enhanced with additional OT-related devices, enabling a wider range of NDR detections with diverse anomaly types and introducing new NetFlow-based detections.

## Encrypted FortiAnalyzer connection

You can now use the `config system syslog fortianalyzer settings` CLI command to create an OFTP-encrypted connection to FortiAnalyzer.

```
config system syslog fortianalyzer settings
    set protocol {syslog, oftps}
end
```

## CLI

### New CLI commands:

- `diagnose system top-fd`: Use this command to display the top processes with the highest number of open file descriptors.

New execute commands:

- `execute raidrebuild start`: Use this command to enable RAID rebuilding.
- `execute raidrebuild status`: Use this command to track RAID progress.
- `execute reboot force`: Use this command to immediately reboot the system without syncing or unmounting your disks.

## CLI updates:

- `diagnose hardware sensorinfo`: Now supports FortiNDR 2500G.
- `execute tac report`: Introduced new debug commands.
- `config system syslog fortianalyzer settings`: Added `set protocol {syslog, oftps}` variable to connect to the remote server.
- `config profile authentication radius`:
  - Added `set access-override {enable | disable}` variable to override the admin profile with Fortinet-Access-Profile attribute
  - Added `message-authenticator-attribute` to require the server to return the Message-Authenticator attribute.
- `diagnose debug`: Added `<days>` variable to display the crash log of the past number of days.
- `diagnose debug application`: Added the `lines` variable to display that number of lines from the end (tail) of the selected daemon log. Added new CLIs `diagnose debug application {pcapcleanerd|tgm}` in the same syntax.
- `diagnose system top`: Added variable support `<lines>` and `<iterations>` based on the existing CLI.

For more information, see the [FortiNDR CLI Reference Guide](#).

# System integration and support

The following integration is tested and supported in FortiNDR 7.6.2.

|                           |   |
|---------------------------|---|
| <b>FOS/FortiGate</b>      | <ul style="list-style-type: none"> <li>FortiNDR Fabric Device widgets including <i>Detection Statistics</i> and <i>System Information</i> supported in FOS 7.0.5 and 7.2.4</li> <li>File submission: FOS 6.4.0 and higher<br/>(FOS 6.2 and 5.6 file submission with OFTP, via the FortiSandbox field, is tested and compatible)</li> <li>FortiGate inline blocking (with AV profile) is supported in FOS 7.0.1 and higher (via HTTP2).</li> <li>FortiGate quarantine via webhook 6.4.0 and higher.</li> </ul> |
| <b>FortiProxy</b>         | <ul style="list-style-type: none"> <li>HTTP2 file submission from FortiProxy 7.0.0 and higher</li> <li>FortiProxy inline blocking (with AV profile) is supported in FPX 7.0.0 and higher.</li> </ul>  |
| <b>FortiAnalyzer</b>      | <ul style="list-style-type: none"> <li>FortiAnalyzer integration is supported in FortiAnalyzer 7.0.1 and higher.</li> </ul>   |
| <b>FortiSIEM</b>          | <ul style="list-style-type: none"> <li>Integration is supported in version 6.3.0 and higher.</li> </ul>   |
| <b>FortiSandbox</b>       | <ul style="list-style-type: none"> <li>FortiSandbox integration (API submission from FortiSandbox to FortiNDR) is supported from FortiSandbox version 4.0.1 and higher.</li> </ul>  |
| <b>FortiMail</b>          | <ul style="list-style-type: none"> <li>Version 7.2.0</li> </ul>   |
| <b>FortiAuthenticator</b> | <ul style="list-style-type: none"> <li>FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are supported.</li> </ul>  |
| <b>ICAP</b>               | <ul style="list-style-type: none"> <li>FortiGate 6.4.0 and higher.</li> <li>FortiWeb 6.3.11 and higher.</li> <li>Squid and other compatible ICAP clients.</li> <li>FortiProxy 7.0.0.</li> <li>FortiNAC quarantine support (v9.2.2+)</li> <li>FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are not supported at this time.</li> <li>FortiSwitch quarantine via FortiLink (FortiSwitch v7.0.0+ and FortiGate v7.0.5+)</li> </ul>                             |



FortiNDR 7.0.1 and later supports sending both malware and NDR logs to FortiAnalyzer and FortiSIEM or other syslog devices.

FortiAnalyzer 7.2.0 supports receiving logs from FortiNDR (log view only).



FortiAnalyzer 7.2.1 supports reporting based on logs.

# Upgrade information

The latest FortiNDR firmware versions are available for download from [FortiCloud](#). You should always backup your system configuration before upgrading the firmware on your device. Be aware that some configuration settings are not saved to the backup configuration file and will need to be manually restored after upgrade.

## Firmware

FortiNDR 7.6.2 supports the following upgrade path:

| Upgrade from  | Upgrade to  | Notes |
|---|---|-------|
| 7.4.8, 7.6.0 (and later)  | 7.6.2   |       |
| <hr/>   |   |       |
|   | <ul style="list-style-type: none"><li>• Direct upgrade from v7.0.x, v7.1.x or v7.2.x to v7.6.0 is not supported in any platform.</li><li>• When upgrading from v7.2.0 - v7.2.3 or v7.4.0 - v7.4.6 to v7.6.0, you will be prompted to update the password upon successful login.</li></ul> |       |
| <hr/>   |   |       |
|  | Downgrade from v7.6.x to v7.4.x is not supported as it could cause severe issues such as device lockout and database errors.  |       |
| <hr/>   |   |       |

## FNR-1000F, FNR-3500F (gen3 and above) and FNR-3600G

- 7.6.0 firmware is designed to run on VM and hardware appliances such as FNR-1000F, FNR-3600G, FNR-3500F (center gen3 and above) and is not compatible with older FNR-3500F hardware (gen1/2). For more information, see [Supported models on page 16](#).

## VM Devices

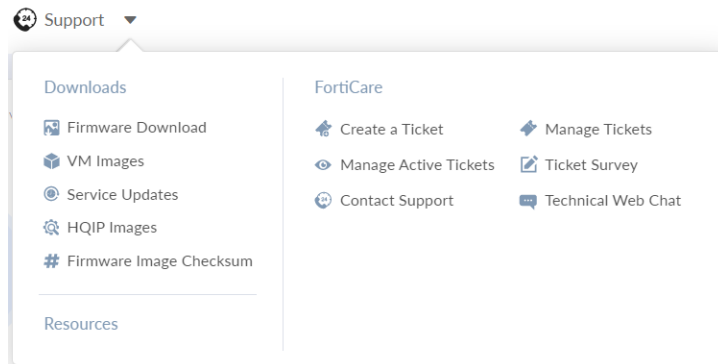


If your current version FortiNDR does not have a password, you will be prompted to create a password after upgrading, otherwise you cannot login.

# Downloading the latest firmware version

To download the latest version of FortiNDR:

1. Log into [FortiCloud](#).
2. In the banner, click *Support > Firmware Download*.



3. From the *Select Product* dropdown, select *FortiNDR*.
4. Click the *Download* tab.
5. Use the folders in the directory to locate and download the latest firmware version.

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiNDR

Release Notes

Download

Image File Path

/ [FortiNDR/ v7.00/](#)

Image Folders/Files

[Up to higher level directory](#)

|  | Name | Size (KB) | Date Created        | Date Modified       |
|--|------|-----------|---------------------|---------------------|
|  | 7.0  | Directory | 2022-04-21 20:04:06 | 2022-10-10 10:10:19 |
|  | 7.1  | Directory | 2022-10-21 17:10:34 | 2022-10-21 17:10:34 |

## Upgrading the firmware version

**Before you begin:**

You should always backup your system configuration before upgrading the firmware on your device.

Be aware the following settings are not backed up to the configuration file:

- *Network Share*
- *Network Share Quarantine*
- *File size limit*
- *Email Alert Recipients*

Record these settings so you can manually restore them after upgrade.

The *File size limit* can be found by pressing the Tab key in the following CLI:

```
execute file-size-threshold {ICAP|OFTP|inline-blocking|manual-upload|network-share|sniffer} <size_limit_1-10240MB>
```

```
FortiNDR-VM # exec file-size-threshold ICAP
<Size Limit>          A integer between 1~10240 for size in MB

--- current value ---
ICAP: 200 MB
```

Please make a note for each file input value.



These settings cannot be recovered after they are removed.

### To upgrade the FortiNDR firmware version:

1. Back up the configuration file:
  - a. Click the Account menu at the top-right of the page.
  - b. Go to *Configuration > Backup*. The configuration file is saved to your computer.
2. Upgrade the firmware:
  - a. Go to *System > Firmware*.
  - b. Click *Upload* and navigate to the location of the file you downloaded from FortiCloud.
  - c. Click *OK*. After the firmware is upgraded the system reboots.
  - d. After the upgrade is complete, the new version of firmware should be ready. In the case where the firmware upgrade does not follow the upgrade path, or there is a VM hosting hardware failure, or a power outage during upgrade, please consider to use following CLI to restore the database.

```
execute db restore
```



This command will format the database and remove all the logs and the following settings: *Device input*, *Network Share*, *Network Share Quarantine*, *File size limit* and *Email Alert Recipients*.

3. Use the configuration settings you recorded earlier to manually restore the settings. For *Device Input*, you just need to re-authorize the device again.

# Supported models

FortiNDR version 7.6.2 supports the following models:

| Model                              | Mode                          | Details  |
|------------------------------------|-------------------------------|--|
| FortiNDR-3600G                     | Center                        |  |
| FortiNDR-1000F                     | Standalone and Sensor         |  |
| FNDR-2500G                         | Standalone and Sensor         |  |
| FortiNDR-3500F gen3*               | Standalone and Center         | Supports FortiNDR central management. For hardware details please visit hardware quick start guide or the following <a href="#">notice</a> . |
| FortiNDR VM 08                     | Sensor                        | Requires Center to manage. Supported for ESXi, KVM, AWS, GCP, Azure and OCI only.  |
| FortiNDR VM 16 & 32                | Standalone and Sensor         |  |
| FortiNDR KVM                       | Standalone and Sensor         |  |
| FortiNDR on AWS (BYOL)             | Standalone, Sensor and Center |  |
| FortiNDR on GCP (BYOL)             | Standalone, Sensor and Center |  |
| FortiNDR on Alibaba (BYOL)         | Standalone                    |  |
| FortiNDR on Azure (BYOL)           | Standalone, Sensor and Center |  |
| FortiNDR on OCI (BYOL)             | Sensor                        |  |
| FortiNDR Centralized Management VM | Center                        | Supported on ESXi and KVM only   |

## \*Notice about hardware generations



The hardware model is printed on the label on the back of the unit.



- FortiNDR gen3 - P24935-03 supports v7.1.x, v7.2.x, 7.4.x and 7.6.x
- FortiAI gen1 - P24935-01 does not support 7.1.x 7.2.x 7.4.x
- FortiAI gen2 - P24935-02 does not support 7.1.x 7.2.x 7.4.x

### **To confirm the hardware generation with the CLI:**

```
get system status
```

This allows you to check the BIOS version. Gen3 models use BIOS version *00010032* and above. Any version below *00010032*, such as *00010001*, indicates a Gen2 or Gen1 model.

# Resolved issues

The following issues have been fixed in version 7.6.2. For inquiries about a particular bug, contact [Customer Service & Support](#).

| Bug ID  | Description   |
|---------|---|
| 1058214 | Resolved an issue where FortiNDR failed to apply RADIUS authorization attributes.                               |
| 1090326 | Manual execution actions between FortiNDR and FortiNAC no longer result in errors.                              |
| 1091134 | An issue that prevented the export of detected malware files reports from the CLI has been fixed.               |
| 1103918 | Resolved an issue where FortiNDR always returned a score of 1 for clean files.                                  |
| 1104382 | The secondary node in FortiNDR standalone HA mode now correctly sends logs to FortiAnalyzer and syslog servers. |
| 1130139 | Resolved an issue in which FortiNDR was not capturing traffic samples.  |
| 1131569 | FortiNDR no longer sends the OVERSIZED_FILE message with an HTTP_FORBIDDEN response code.                       |
| 1151818 | Resolved an issue where FortiNDR could stop logging events when a high volume of anomalies was detected.        |

# Known issues

The following issues have been identified in version 7.6.2. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

| Bug ID  | Description   |
|---------|---|
| 1138944 | FortiNDR log does not download the PCAP due to a <i>PCAP info not recorded</i> error. |



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

Copyright© 2025 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 Chief Legal Officer, 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.