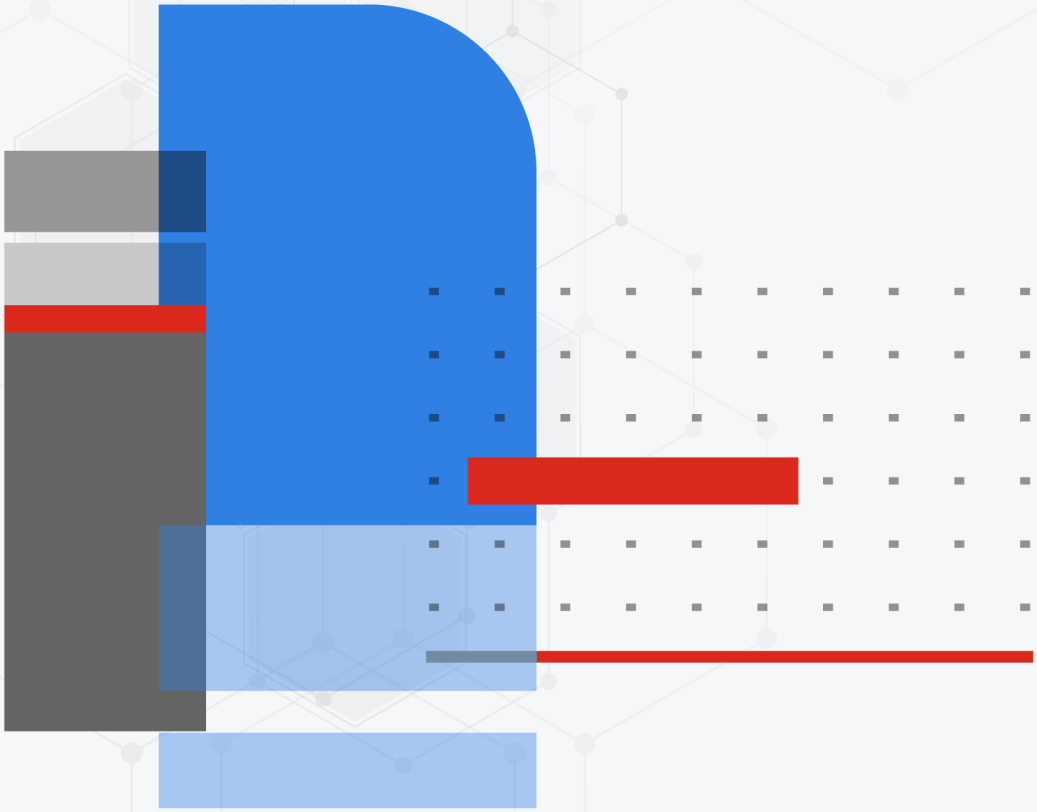
Release Notes

FortiNDR 7.4.3



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

may 14, 2025
FortiNDR 7.4.3 Release Notes
55-743-1004291-20250514

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-03-18	Initial release.
2024-03-19	Updated Introduction on page 5.
2024-03-20	Updated Upgrade information on page 7
2024-03-21	Updated Resolved issues on page 15.
2024-06-04	Updated Supported models on page 14
2024-06-27	Updated Supported models on page 14.
2025-05-14	Updated Resolved issues on page 15.

Introduction

FortiNDR (On-premise) 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 factor 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 EastWest traffic in Datacenter/Cloud environment. Artificial Neural Networks (ANN) is equipped with the solution to classify malware into attack scenarios, surface outbreak alerts and trace source of malware infections. Network Based attacks such as intrusions, botnet, 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.

Licensing

Please refer to the FortiNDR ordering guide for licensing details:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortindr.pdf..

Netflow and Scada licenses are ordered separately for sensors and standalone deployment.

v1.5.x firmware is no longer supported. Please refer to customer support bulletin for details:
https://support.fortinet.com/Information/Bulletin.aspx

Customers need to have the correct SKU for NDR functionalities to work.

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

Version 7.4.3 primarily fixes known issue 1006195 where upgrading to v7.2.2 will result in lost configuration.

Version 7.4.3 offers a few new functionalities such as SNMP polling, MITRE ATT&CK coverage plus some bug fixes. For details, please refer to Resolved issues on page 15.

FortiNDR 7.4.3 supports the following upgrade path: <mantis 1019961>

Upgrade from	Upgrade to	Notes
7.4.0-7.4.2	7.4.3	Direct upgrade is supported.
7.2.0-7.2.3	7.4.3	Direct upgrade is supported.
7.1.1	7.2.3	Gen2 FAI3500F can only support firmware version up to 7.1.x
1.5	7.0.6	Directed upgrade is supported

FNR-1000F, FNR-3500F (gen3 and above)

- 7.4.3 firmware is designed to run on FNR-1000F and FNR-3500F (gen3 and above) and is not compatible with older FAI-3500F hardware (gen1/2). For more information, see Supported models on page 14.
- When upgrading FNR-3500F from 7.4.0 to 7.4.3 in Center Mode, you will need to run the following command after upgrade:

```
execute db restore
```

This CLI will reset the database to an empty state. If upgrade is from 7.4.2 to 7.4.3 this step is not necessary.

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.

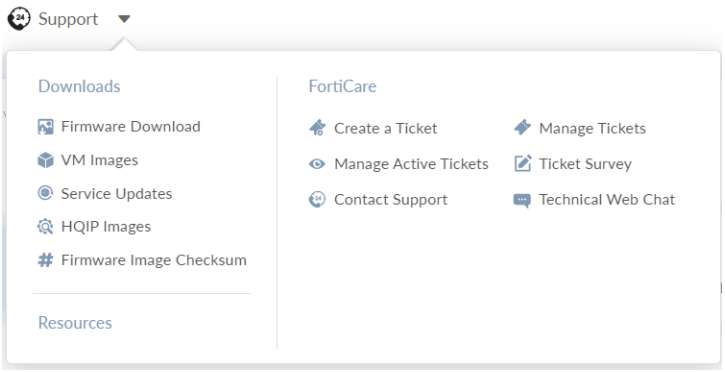
FortiNDR VM supports the following upgrade path: <mantis 1019961>

Upgrade from	Upgrade to	Notes
7.4.0-7.4.2	7.4.3	Direct upgrade is supported.
7.2.0-7.2.3	7.4.3	Direct upgrade is supported.
7.1.1	7.2.3	
1.5	7.0.6	Directed upgrade is supported

Downloading the latest firmware version

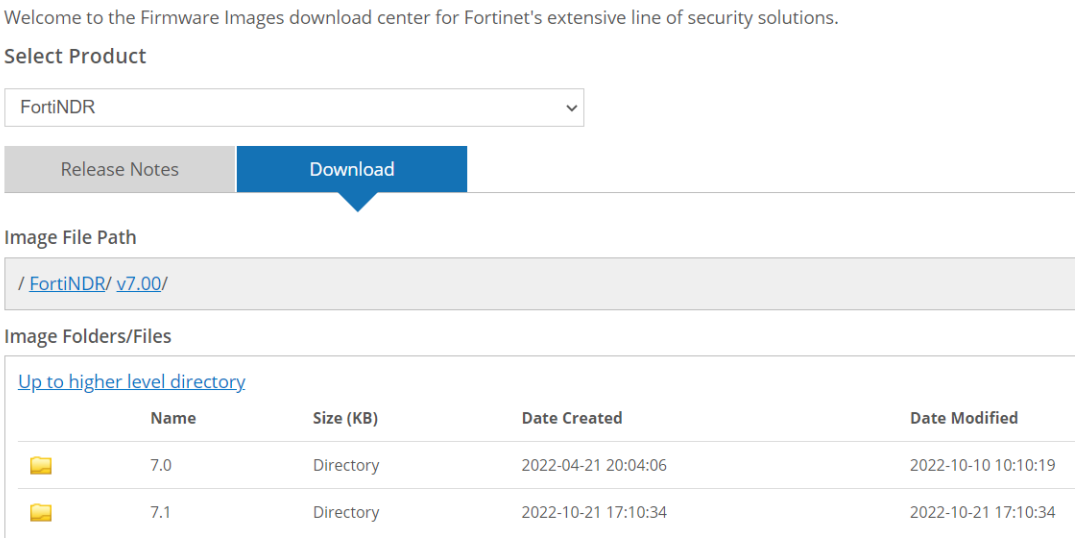
To download the latest version of FortiNDR:

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.



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, use the following the 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.

FortiNDR version 7.4.3

This document provides information about FortiNDR version 7.4.3 build 0529.

These Release Notes include the following topics:

New features and enhancements

The following is a summary of new features and enhancements in version 7.4.3. For details, see the *FortiNDR 7.4.3 Administration Guide* in the Document Library.

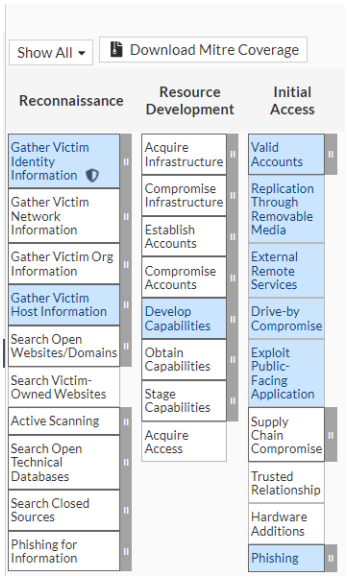
MITRE ATTACK

The *MITRE ATT&CK* page has been updated with new features.

When *View All* is selected, the MITRE ATT&CK with FNDR coverage blocks are colored light blue. When a MITRE ATT&CK technique detection has been triggered, the technique block will display a shield icon. You can click the blocks to drill down to view the source of the detection in the *NDR Anomaly* tab.

When *Show Coverage* is selected, all the technique blocks without FNDR coverage are hidden so that the matrix fits the page. In this view, the colored blocks indicate the MITRE Technique detection has been triggered.

For information, see MITRE ATT&CK.



SNMP

FortiNDR system information and system status can be monitored by utilizing SNMP. When configuring the SNMP manager to connect to FortiNDR's SNMP agent, you must add the Fortinet proprietary MIBs to have access to Fortinet specific information. For more information, see SNMP.

Additional Public Cloud Support

FortiNDR Center and Sensor are now supported in Azure and GCP. Please refer to Supported Model for details.

Support FortiGuard Override

Users can specify a server for updating FortiGuard updates for FortiNDR . Please see CLI `config system fortiguard update` for details.

CLI

The following commands were added:

- `diagnose hardware sensorinfo`: Use this CLI for monitoring and obtaining information about Power Supply, Temperature, and Fan sensors.
- `config system snmp threshold`: Use this command to configure the event types that trigger an SNMP trap.
- `config system snmp community`: Use this command to configure simple network management protocol (SNMP) v1/2 settings. These commands apply only if the SNMP agent is enabled.
- `config system snmp user`: Use this command to configure SNMP v3 user settings.
- `config system fortiguard update`: Five new commands were added.

For more information, see the *FortiNDR CLI Reference Guide*.

System integration and support

The following integration is tested and supported in FortiNDR 7.4.3.

FOS/FortiGate	• FortiNDR Fabric Device widgets including *Detection Statistics* and *System Information* supported in FOS 7.0.5 and 7.2.4 • File submission: FOS 6.4.0 and higher (FOS 6.2 and 5.6 file submission with OFTP, via the FortiSandbox field, is tested and compatible) • FortiGate inline blocking (with AV profile) is supported in FOS 7.0.1 and higher (via HTTP2). • FortiGate quarantine via webhook 6.4.0 and higher.
FortiProxy	• HTTP2 file submission from FortiProxy 7.0.0 and higher

	• FortiProxy inline blocking (with AV profile) is supported in FPX 7.0.0 and higher.
FortiAnalyzer	• FortiAnalyzer integration is supported in FortiAnalyzer 7.0.1 and higher.
FortiSIEM	• Integration is supported in version 6.3.0 and higher.
FortiSandbox	• FortiSandbox integration (API submission from FortiSandbox to FortiNDR) is supported from FortiSandbox version 4.0.1 and higher.
FortiMail	• Version 7.2.0
FortiAuthenticator	• FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are not supported at this time.
ICAP	• FortiGate 6.4.0 and higher. • FortiWeb 6.3.11 and higher. • Squid and other compatible ICAP clients. • FortiProxy 7.0.0. • FortiNAC quarantine support (v9.2.2+) • FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are not supported at this time. • FortiSwitch quarantine via FortiLink (FortiSwitch v7.0.0+ and FortiGate v7.0.5+)  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.

Supported models

FortiNDR version 7.4.3 supports the following models:

Model	Mode	Details
FortiNDR-1000F	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 notice.
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 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, and 7.4.x
- FortiAI gen1 - P24935-01 does not support 7.1.x and 7.2.x
- FortiAI gen2 - P24935-02 does not support 7.1.x and 7.2.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 *00010031* and above. Any version below *00010031*, such as *00010001*, indicates a Gen2 or Gen1 model.

Resolved issues

The following issues have been fixed in version 7.4.3. For inquires about a particular bug, contact Customer Service & Support.

Bug ID	Description
896473	Resolved an issue with the *Netflow Traffic Volume* widget time display.
950842	Fixed the blinking Amber LED showing at the front of the NDR 3500F.
977754	FNDR now supports scan of ICAP multipart messages/MIME.
0982104	It is now possible to configure generic webhook from the GUI menu.
0991666	Resolved an issue where the *Netflow Suspicious Activity* widget expanded view was empty.
993835	Activating *Demo Mode* no longer displays an error message.
0995781	Filters on device detail page work as expected.
995793	File analysis result no longer displays *Clean* for password protect files.
998235	Resolved an issue where there was no detection for a file on the first attempt via ICAP.
1000162	Fixed an issue where FortiNDR *Network Share* scan incorrectly processed non-ASCII filenames.
1002796	Fixed the *Sample* view to show the correct matched fields for attacker/victim IP.
1006124	FortiNDR factory reset no longer breaks the ICAP connector.
1013325	Fixed FortiNDR Network Share showing the improper file type and size handling.
9840489	Fixed the mismatch between *Attacker* and *Victim IP* addresses in the *Malware Sample* detail view.

Common Vulnerabilities and Exposures

Bug ID	Description
987495	FortiNDR7.4.3 is no longer vulnerable to the following CVE Reference: • CVE CVE-2023-48795

Known issues

The following issues have been identified in version 7.4.3. For inquires about a particular bug or to report a bug, contact Customer Service & Support.

Bug ID	Description
902308	CPU Utilization is *High* due to process clickhouse
933649	ICAP does not display response from submissions from MoveIT client.
951919	GUI: *Big picture*, *hostname modification*, *download sample* button, *fortiguard FP submission* is disabled in Center mode.
978096	Malware download button malfunctions when dowlnloading sample details on Standalone FortiNDR.
1000934	FortiNDR sends *Clean* result to FortiGate when a timeout occurs.
1012103	FortiNDR Network Share fails to detect malicious archive file.

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.