Release Notes

FortiNDR 7.6.4

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

March 17, 2026
FortiNDR 7.6.4 Release Notes
55-764-1249832-20260317

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-03-17	Initial release.

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 7.6.4

This document provides information about FortiNDR version 7.6.4 build 0673.

These Release Notes include the following topics:

- New features and enhancements on page 9
- System integration and support on page 13
- Supported models on page 19
- Resolved issues on page 21
- Known issues on page 22

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 deployments.

Expired licenses

License expiration affects VMs and hardware appliances differently:

License	Service impact
VM	• The sniffer and IPS/ANN engine continue to process traffic with existing signatures, however users will lose access to the GUI, which redirects to the license upload page. • Users will lose access to any FortiGuard updates (ANN, IPS, IOT updates, etc). • Users lose access to any FortiGuard service lookups (webfilter, IOC lookups). • If the VM is in Sensor mode, it will stop syncing data to Centers.
Hardware	• The sniffer and IPS/ANN engine continues to process traffic with existing signatures. GUI access remains available in this case. • Users will lose access to any FortiGuard: • Updates (ANN, IPS, IOT updates, etc) • Service lookups (webfilter, IOC lookups) • If a physical appliance is in Sensor mode, data sync with any configured Center will continue and is not affected by the expired FortiNDR license.
OT	• Users lose access to any FortiGuard OT updates. • Traffic is processed with any existing OT signatures on the system.
Netflow	• Access to existing processed Netflow results in GUI is turned off. • The Netflow collector daemon and Netflow traffic processing are turned off.

There is no grace period for expired licenses.

New features and enhancements

This document provides information about FortiNDR version 7.6.4 build 0673.

The following is a summary of new features and enhancements in version 7.6.4.

For details, see the *FortiNDR7.6.4 Administration Guide* in the Document Library.

System & Data Handling Updates

- Database performance has been enhanced.

> ⚠ Before upgrade, please see Upgrade information on page 15

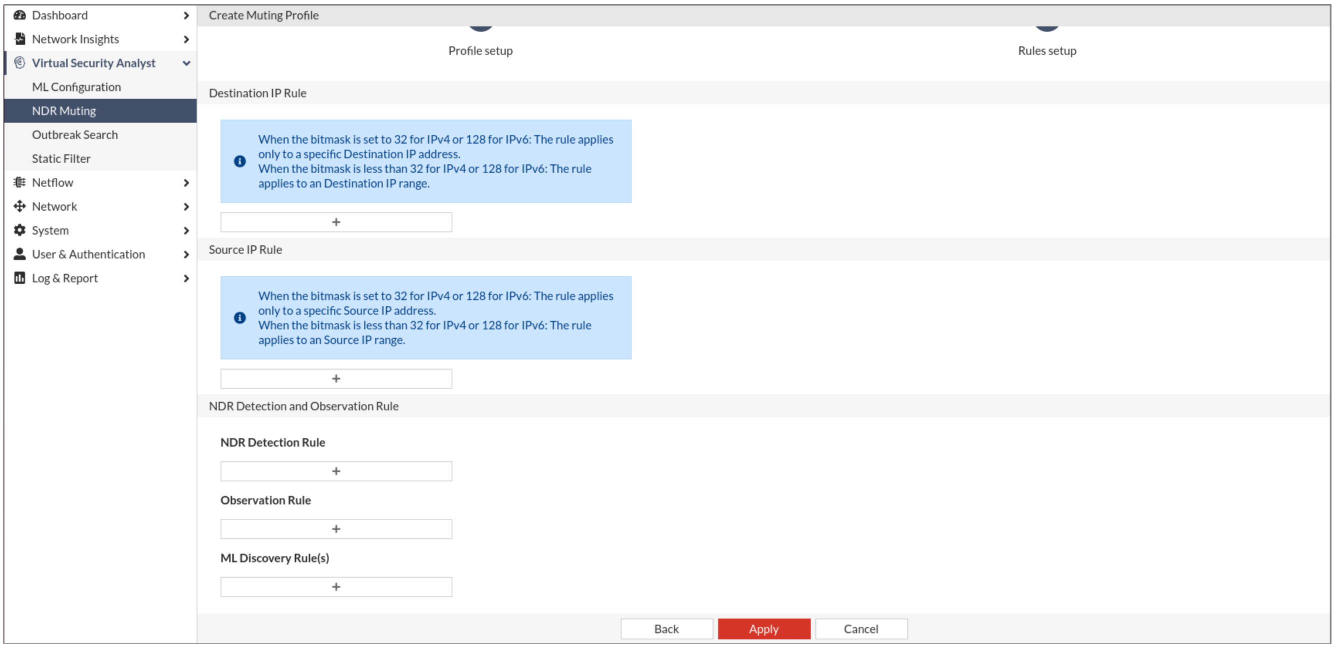
- The anti-virus database (AVDB) now supports patch updates.
- Enhanced PCAP handling to improve both performance and overall usability.
- Management port now supports LACP.
- File tagging (e.g., marking malicious files) is now supported in Center Investigations.

Detection enhancements

- Machine learning and NetFlow baselining are no longer started by default. You can now choose when to begin baselining, reducing unnecessary noise and alarms.
- FortiNDR can now submit files to FortiSandbox for additional analysis. This extends the current integration, where FortiSandbox is able to use FortiNDR as a pre-scan stage.

Muting enhancements

- You can now combine ML-based discovery, traditional detections, and observation types within a single rule.
- Multiple ML features can now be added as a single combined rule.
- FortiNDR muting now applies to both historical traffic and new detections entering the network.



Create Muting Profile

Profile setup

Rules setup

Destination IP Rule

When the bitmask is set to 32 for IPv4 or 128 for IPv6: The rule applies only to a specific Destination IP address.
When the bitmask is less than 32 for IPv4 or 128 for IPv6: The rule applies to an Destination IP range.

Source IP Rule

When the bitmask is set to 32 for IPv4 or 128 for IPv6: The rule applies only to a specific Source IP address.
When the bitmask is less than 32 for IPv4 or 128 for IPv6: The rule applies to an Source IP range.

NDR Detection and Observation Rule

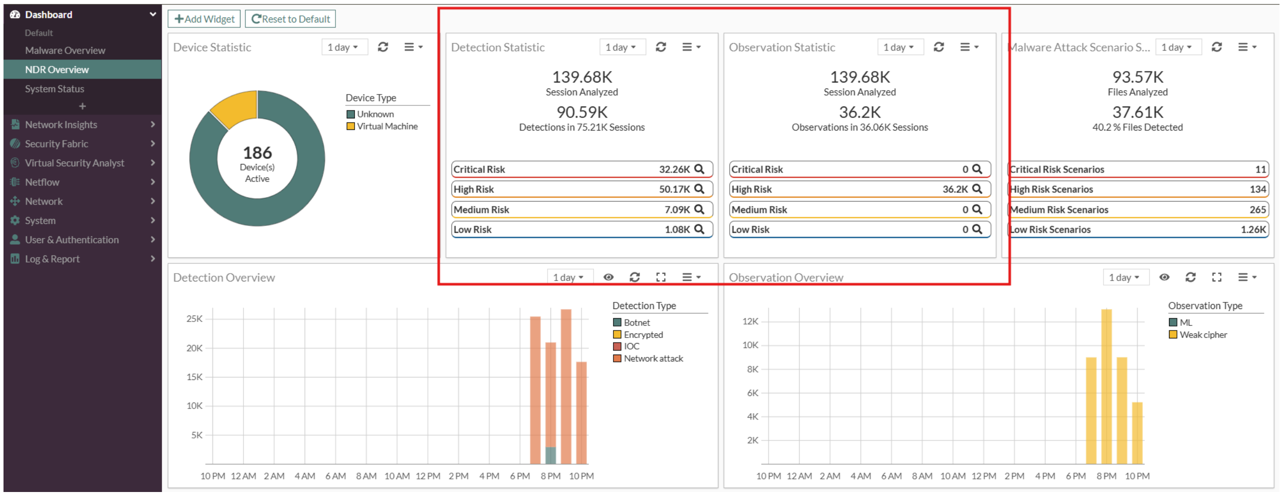
NDR Detection Rule

Observation Rule

ML Discovery Rule(s)

GUI and navigation improvements

- Replaced the term *Anomaly* with *Detection* and *Observation*, in *Network Insights*, *Log & Report* and throughout FortiNDR.



Device Statistic

Detection Statistic

139.68K
Session Analyzed
90.59K
Detections in 75.21K Sessions

Critical Risk	32.26K
High Risk	50.17K
Medium Risk	7.09K
Low Risk	1.08K

Observation Statistic

139.68K
Session Analyzed
36.2K
Observations in 36.06K Sessions

Critical Risk	0
High Risk	36.2K
Medium Risk	0
Low Risk	0

Malware Attack Scenario S...

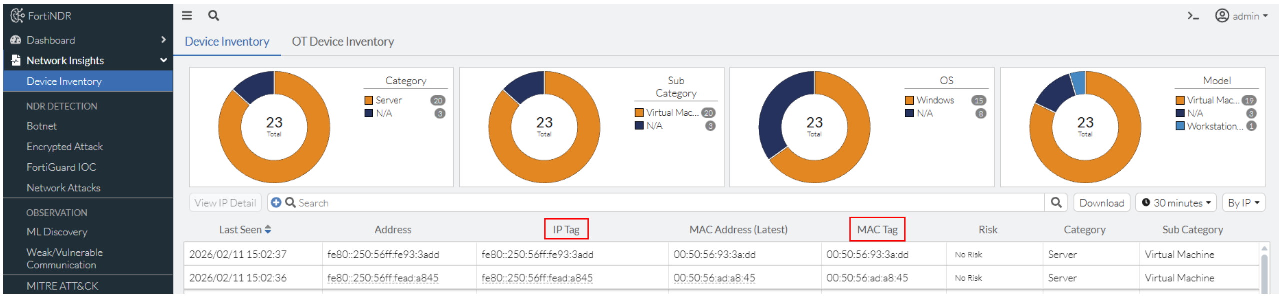
93.57K
Files Analyzed
37.61K
40.2 % Files Detected

Critical Risk Scenarios	11
High Risk Scenarios	134
Medium Risk Scenarios	265
Low Risk Scenarios	1.26K

Detection Overview

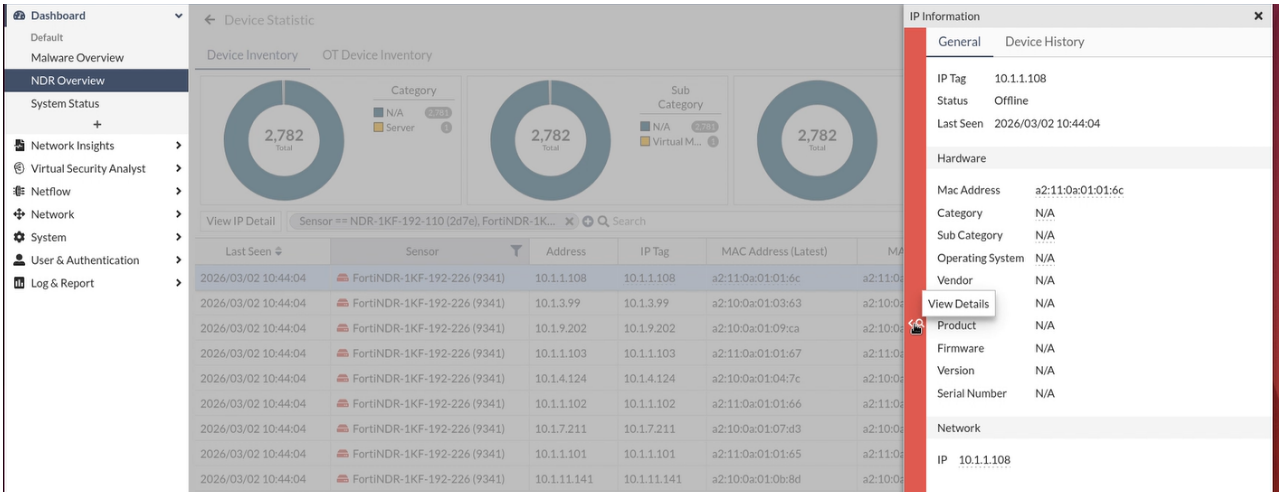
Observation Overview

- *Device Name* has been replaced with *IP Tag* and *MAC Tag*. These tags are configurable and can be used in scenarios where a firewall with many IP addresses sits behind a single MAC address.



Last Seen	Address	IP Tag	MAC Address (Latest)	MAC Tag	Risk	Category	Sub Category
2026/02/11 15:02:37	fe80::250:56ff:fe93:3add	fe80::250:56ff:fe93:3add	00:50:56:93:3a:dd	00:50:56:93:3a:dd	No Risk	Server	Virtual Machine
2026/02/11 15:02:36	fe80::250:56ff:fead:a845	fe80::250:56ff:fead:a845	00:50:56:ad:a8:45	00:50:56:ad:a8:45	No Risk	Server	Virtual Machine

- Introduced a new sliding-pane navigation method for accessing *Profile Pages*, making it easier for users to reach a device’s profile page.



Last Seen	Sensor	Address	IP Tag	MAC Address (Latest)	MA
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.1.108	10.1.1.108	a2:11:0a:01:01:6c	a2:11:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.3.99	10.1.3.99	a2:10:0a:01:03:63	a2:10:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.9.202	10.1.9.202	a2:10:0a:01:09:ca	a2:10:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.1.103	10.1.1.103	a2:11:0a:01:01:67	a2:11:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.4.124	10.1.4.124	a2:10:0a:01:04:7c	a2:10:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.1.102	10.1.1.102	a2:11:0a:01:01:66	a2:11:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.7.211	10.1.7.211	a2:10:0a:01:07:d3	a2:10:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.1.101	10.1.1.101	a2:11:0a:01:01:65	a2:11:0
2026/03/02 10:44:04	FortiNDR-1KF-192-226 (9341)	10.1.11.141	10.1.11.141	a2:10:0a:01:0b:8d	a2:10:0

IP Information

General | Device History

IP Tag 10.1.1.108
Status Offline
Last Seen 2026/03/02 10:44:04

Hardware

Mac Address a2:11:0a:01:01:6c
Category N/A
Sub Category N/A
Operating System N/A
Vendor N/A
N/A
Product N/A
Firmware N/A
Version N/A
Serial Number N/A

Network

IP 10.1.1.108

- A demo indicator has been added to the top-right banner to show when demo mode is active.
- Users are required to enter their current password when changing to a new one.

CLI

For detailed information about CLI commands, please refer to the FortiNDR CLI Reference.

New CLI:

- `config system fortisandbox`: Use this command to configure FortiSandbox settings. FortiNDR can send suspicious malware files to FortiSandbox and receive verdicts to validate whether they are false positives.
- `execute db sample_process_summary`: Use this command to get the processing status of FortiNDR within a specific time period.
- `execute factoryreset-shutdown`: Use this command to reset FortiNDR to its factory default settings for the current installed firmware version and shut down.
- `execute factoryreset-shutdown config`: Use this command to reset FortiNDR to its factory default configurations for the current installed firmware version.
- `execute expandspooldisk`: Use this command to expand /var/spool and `/var/log` disks on VM without losing pre-existing data.

- `execute cleanup pcap`: Use this command to clean up PCAP related information in database and files in disk.
- `execute db migrate`: Use this command to migrate or cleanup legacy table data (max of 7 days data at a time) when you upgrade FortiNDR to 7.6.4GA.
-

Updated CLI:

- `config system interface`: Added `set type {aggregate}` and `set redundant-member <member-interface_name>`.
- `config system global`: Added `set remoteauthtimeout <seconds>` to set the global timeout (in seconds) for remote authentication transactions.
- `execute tac report`: Updated pre-defined CLI commands

System integration and support

The following integration is tested and supported in FortiNDR 7.6.4.

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. • Quarantining with FortiProxy 7.6.3 and higher.
FortiAnalyzer	• FortiAnalyzer integration is supported in FortiAnalyzer 7.0.1 and higher.
FortiAnalyzer Cloud	• Integration is supported in version 7.6.3 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 supported.
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.

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 7.6.4 supports the following upgrade path:

Upgrade from	Upgrade to
7.6.3	7.6.4
7.6.2	7.6.3
7.6.0 (and later)	7.6.2
7.4.x	7.4.10 > 7.6.3 > 7.6.4

Important: Retrain ML baseline after upgrading to 7.6.4

After upgrading to version 7.6.4, the ML baseline, including the NetFlow ML baseline, must be retrained in both Standalone mode and Center mode to ensure proper ML anomaly-detection functionality.

Although ML features may appear to operate normally immediately after the upgrade, detection accuracy will degrade or stop entirely until retraining is completed. To clean up existing data and trigger the retraining process, run the following CLI command:

```
execute cleanup ml/netflow_ml
```

⚠ For details on post-upgrade metadata issues in version 7.6.3, refer to Important: Metadata issue post-upgrade.

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, FNDR-3500F (center gen3 and above) and is not compatible with older FAI-3500F hardware (gen1/2). For more information, see Supported models on page 19.

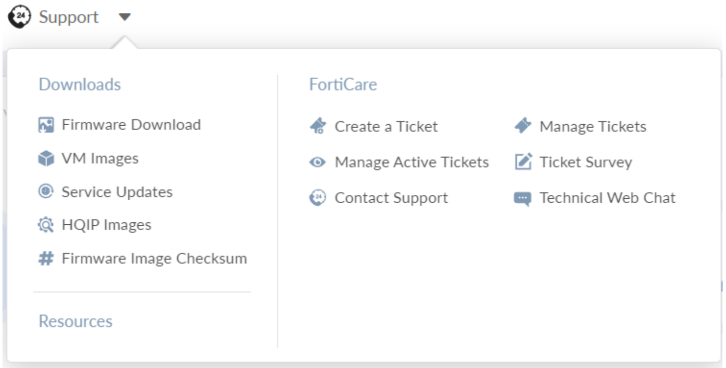
VM Devices

> 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

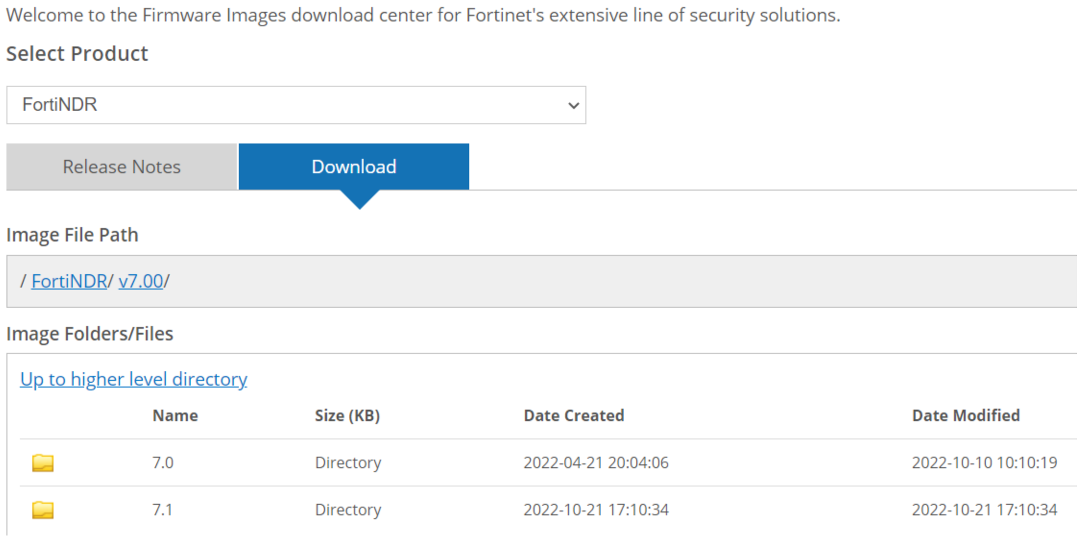
To download the latest version of FortiNDR:

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

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.

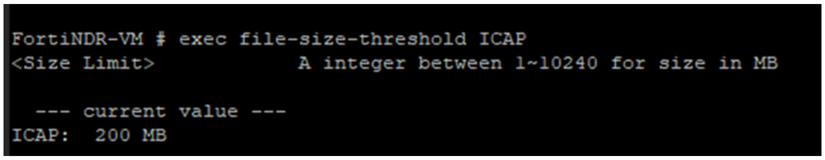
Be aware the following settings are not backed up to the configuration file:

- *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 7.6.4 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 notice.
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 on Alibaba (BYOL)	Standalone	
FortiNDR on AWS (BYOL)	Standalone, Sensor and Center	
FortiNDR on Azure (BYOL)	Standalone, Sensor and Center	
FortiNDR on GCP (BYOL)	Standalone, Sensor and Center	
FortiNDR KVM	Standalone and Sensor	
FortiNDR on Nutanix	Standalone, Sensor and Center	Nutanix version AOS 7.3.1
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 7.6.4. For inquires about a particular bug, contact Customer Service & Support.

Bug ID	Description
1074921	Fixed an issue where FortiNDR binary files could leak during upload and vulnerability-scan operations.
1138944	Improved the PCAP download mechanism to address reliability and performance problems.
1174207	Fixed an issue where LDAP enrichment processes were not functioning correctly.
1193872	FortiNDR no longer enforces username and password requirements when using the NFS protocol.
1194382	Resolved an issue where the event log consistently showed the message `hasyncd: timeout logging to x.x.x.x.`
1205810	Resolved an issue where data from Sensors was not being ingested or received by Center.
1209739	Resolved an issue where customers encountered a reboot loop when upgrading from v7.6.0 to v7.6.2 on the FNR-1000F.
1218484	Fixed high storage utilization after upgrading to firmware version 7.6.3.
1223327	Resolved an issue where a high input discard rate occurred on the FortiNDR interface.
1232685	Resolved an issue where FortiNDR was unable to send alert emails to multiple recipients.
1234941	Fixed an issue where FortiNDR suddenly stopped processing traffic.
1235771	Resolved an issue where the Center was not ingesting or receiving data from sensors.
1237264	Fixed an issue where the Center device was not ingesting or receiving data from sensors.
1252360	Resolved an issue where FortiNDR was unable to send email alerts.

Known issues

The following issues have been identified in version 7.6.4. For inquires about a particular bug or to report a bug, contact Customer Service & Support.

Bug ID	Description
1247687	There is a significant delay when viewing malware log sample details.
1259246	The Bandwidth widget does not display the interface monitor option.
1262238	File submission through the API fails, and all subsequent attempts also fail.
1263056	FortiNDR may generate duplicate IDs when both demo and sniffer are enabled.

www.fortinet.com

Copyright© 2026 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.