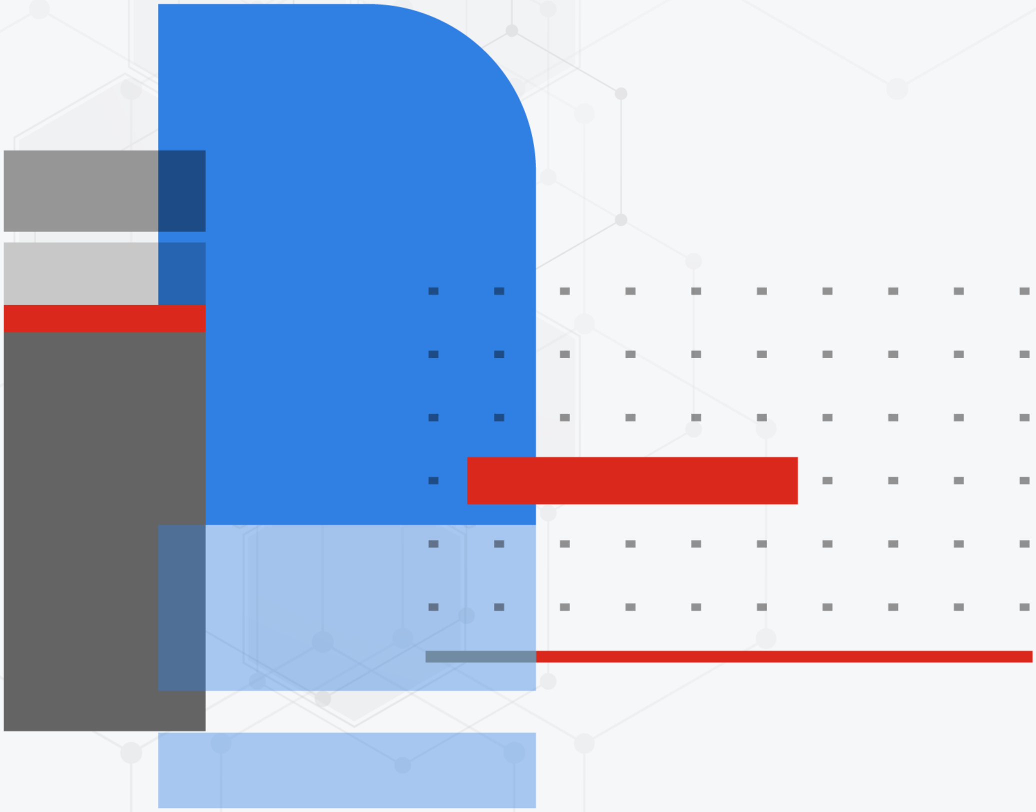
FORTINET

Release Notes

FortiNDR 7.0.7



April 17, 2025
FortiNDR 7.0.7 Release Notes
55-707-1098216-20250228

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Licensing **6**
Upgrade information **7**
Firmware 7
FNR-3500F (Gen1 and Gen2) 7
VM Devices 7
Downloading the latest firmware version 8
Upgrading the firmware version 8
FortiNDR version 7.0.7 .... **10**
New features and enhancements 10
System integration and support 10
Supported models **11**
Resolved issues **12**
Common Vulnerabilities and Exposures 12

Change Log

Date	Change Description
2025-04-17	Initial release of version 7.0.7.
2025-05-15	Updated Resolved issues on page 12.

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 East West 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.

If you are using a FortiNDR that does not have a password, you will be forced to change the password after upgrading, otherwise you cannot login.

Firmware

FNR-3500F (Gen1 and Gen2)

- 7.0.7 firmware is designed to run on FNR-3500F (gen3 and above) and is not compatible with older FAI-3500F hardware (gen1/2). For more information, see Supported models on page 11.

VM Devices

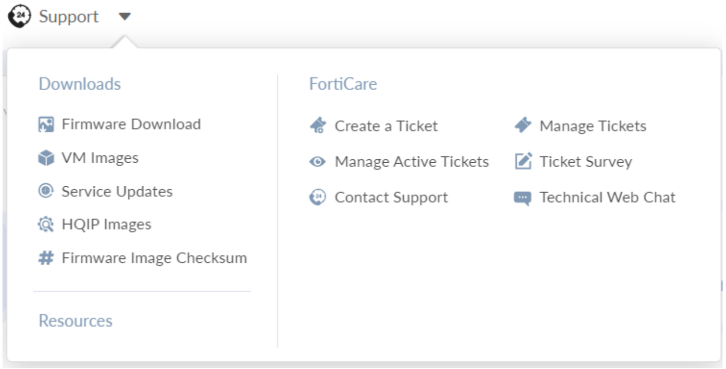
- Direct upgrade from 7.0.x is supported.

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

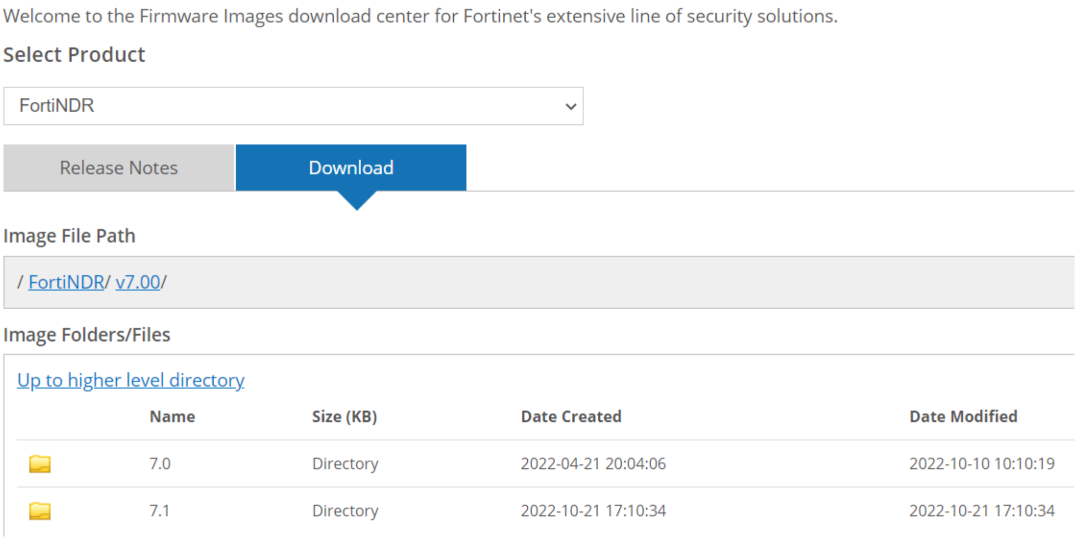
Downloading the latest firmware version

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.

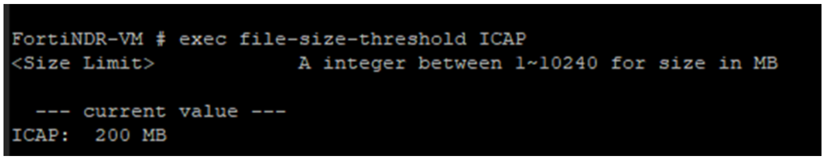
Be aware the following settings are not backed up to the configuration file:

- *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, 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 7.0.7

This document provides information about FortiNDR version 7.0.7 build 0054.

These Release Notes include the following topics:

- New features and enhancements on page 10
- System integration and support on page 10
- Supported models on page 11

New features and enhancements

FortiNDR 7.0.7includes performance improvements but does not introduce any new features or enhancements.

System integration and support

The following integration is tested and supported in FortiNDR 7.0.7.

- While FOS 6.2 and 5.6 file submission with OFTP, via the FortiSandbox field, is tested and compatible, official support for submitting files is in FOS 6.4.0 and higher.
- HTTP2 file submission from FortiGate 7.2.0
- FortiGate inline blocking (with AV profile) is supported in FOS 7.0.1 and higher.
- FortiAnalyzer integration is supported in FortiAnalyzer 7.0.1 and higher.
- FortiSIEM integration is supported in FortiSIEM 6.3.0 and higher.
- FortiSandbox integration (API submission from FortiSandbox to FortiNDR) is supported from FortiSandbox 4.0.1 and higher.
- FortiGate quarantine via webhook 6.4.0 and higher.
- FortiMail 7.2.0
- ICAP is supported for:
  - 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+)
  - FortiSwitch quarantine via FortiLink (FortiSwitch v7.0.0+ and FortiGate v7.0.5+)

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

Supported models

FortiNDR version 7.0.7 supports the following models:

- FortiNDR-3500F generation 1 & 2 hardware.
- FortiNDR VM 16 & 32 (supports upgrade from FortiNDR VM16 & 32)
- FortiNDR KVM (supports upgrade from FortiNDR KVM)
- FortiNDR on AWS (BYOL)

Resolved issues

The following issues have been fixed in version 7.0.7. For inquires about a particular bug, contact Customer Service & Support.

Common Vulnerabilities and Exposures

Bug ID	Description
1147099	FortiNDR 7.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2025-32756

www.fortinet.com