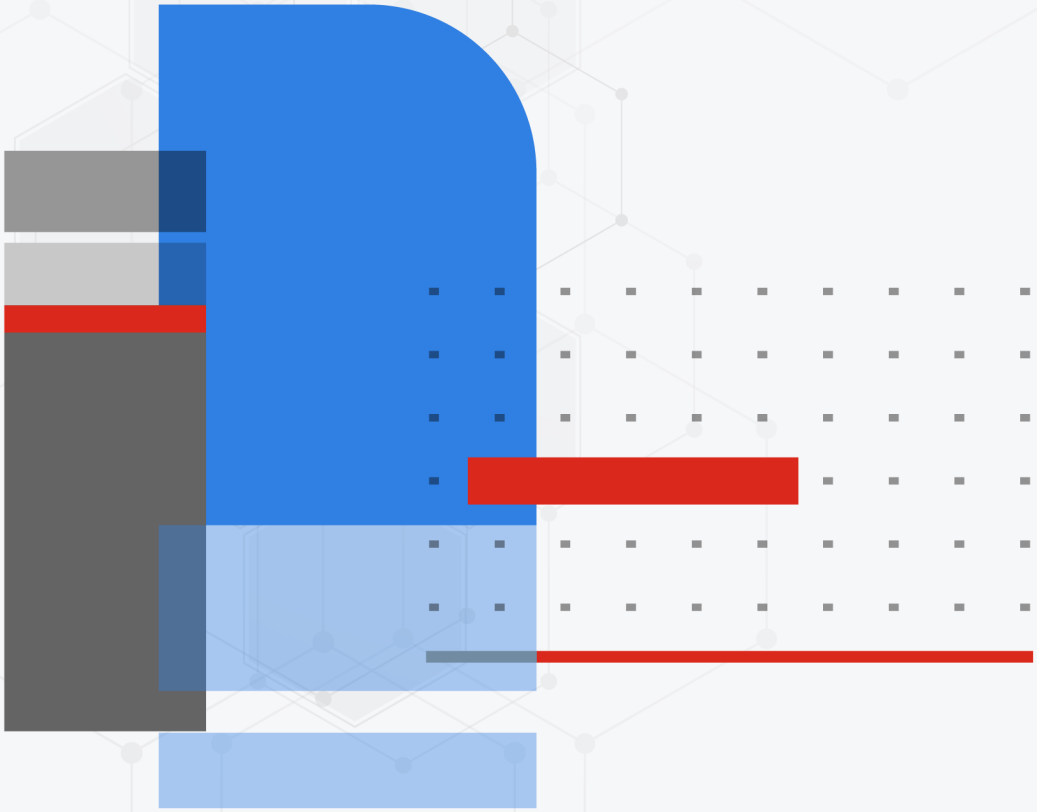
Release Notes

FortiNDR 7.6.0



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

October 22, 2024
FortiNDR 7.6.0 Release Notes
55-760-1054917-20241022

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-10-22	Initial release.

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.

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.

End of Support

FortiNDR 1.5.x firmware and FortiNDR 7.1.x is no longer supported. Please refer to customer support bulletin for details:
https://support.fortinet.com/Information/Bulletin.aspx

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 7.6.0 supports the following upgrade path:

Upgrade from	Upgrade to	Notes
7.4.0 - 7.4.6	7.6.0	Direct upgrade is supported for sensor, standalone and center.

- Direct upgrade from v7.0.x, v7.1.x or v7.2.x to v7.6.0 is not supported in any platform.
- 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.

Downgrade from v7.6.0 to v7.4.6 or any version before v7.4.6 is not supported as it could cause severe issues such as device lockout and database errors.

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 15.

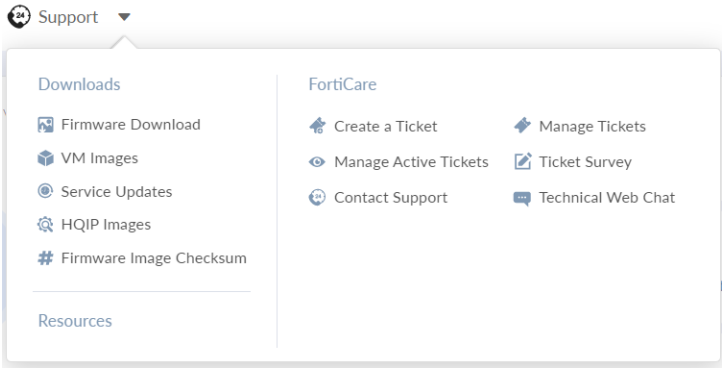
VM Devices

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

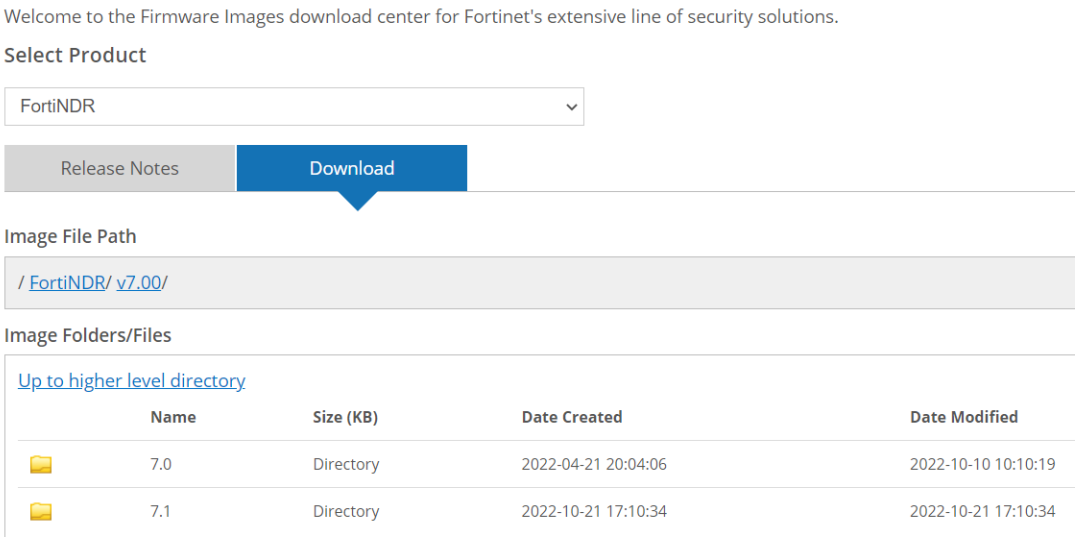
Downloading the latest firmware version

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.



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.

FortiNDR version 7.6.0

This document provides information about FortiNDR version 7.6.0 build 0637.

These Release Notes include the following topics:

New features and enhancements

The following is a summary of new features and enhancements in version 7.6.0. For details, see the *FortiNDR 7.6.0 Administration Guide* in the Document Library.

Security Enhancements

Netflow and ML Detections

- Introduced *Netflow ML Discovery* and *Netflow ML Configuration* to the *Netflow* module.
  - *Netflow ML Discovery*: The *Netflow ML Discovery* monitor displays a list of anomalies detected by *Netflow ML Configuration*.
  - *Netflow ML Configuration*: Configure the Machine Learning (ML) profile of network traffic to identify anomalies.
- The *Netflow ML Discovery* widget was added to the *Netflow* dashboard. This widget provides a brief summary of the current Netflow ML baselining status and number of anomalies detected in the selected time period.
- Suspicious Netflow traffic (matching botnet/proxy/spam/TOR IP DBs/Phishing) will be treated as detections, where FortiNDR will send SYSLOG and CEF. However, the enforcement profile and automation is not supported at this stage.

Global Internal Query Language and tagging for Investigation

- Users can copy and paste system defined queries, as well as customized queries to query the database of network metadata collected. This feature is supported on FortiNDR-3600G only (available Oct 2024).

Malware Observed and Attack Scenario

- *Host Story* has been renamed *Malware Observed* and relocated to the *Network Insights* module. *Attack Scenario* has been moved under *Network Insights*, and renamed *Malware Attack* scenario.

MITRE ATT&CK

- Expanded the *Mitre ATT&CK* matrix to include ICS techniques. These techniques are also displayed as a widget in the in the *NDR Overview* dashboard.

File type pre-filter

- FortiNDR now can apply pre-scan profile to include/exclude certain file types (for example, MS Office, PDFs, text documents). CLI feature, refer to "execute filtype-prefilter' for details

S3 bucket scan

- FortiNDR can now map to S3 bucket for malware scanning

OT Enhancements

IOT device identification

- IOT device identification queries to FortiGuard servers are now local inside FortiNDR (once you have updated FortiNDR's databases from FortiGuard Servers). The DB in use can found under *System* > *FortiGuard*: *IOT Single* and *IOT Range*.

IOT new column fields under OT devices tab

- FortiNDR now supports detecting OT devices, firmware, versions and product information by inspecting OT traffic using OTAPPDB.

Purdue model View

- FortiNDR now supports displaying OT devices in Purdue model under *Network Insights* > *Device Inventory* (configurable with the GUI for each device), device traffic and Purdue level will be plotted in the topology view.

System Enhancements

Log & Report

- Introduced a *Forensics* tab to *Log & Report* > *NDR Log* to allow users to view and download packet capture information. This tab is used when Conditional Attack PCAP is configured and enabled with the CLI.

API to retrieve malware files

- We have introduced new API to support download of infected files.

Email alert settings

Two new triggers were added to the email alert settings:

- Netflow: Netflow Suspicious Activity
- Netflow: Netflow Machine Learning Detection

Artifact storage

- Introduced *Artifact Storage* under the *System* module to manage storage profiles and PCAP configuration. This external storage is used for attack PCAP storage.

FortiGuard Anycast servers support

- By default, FortiNDR will now use Anycast FortiGuard servers *globalupdate.fortinet.net* instead of unicast servers *update.fortiguard.net*. This is to download latest IOT DB for device classification.

System integration and support

FortiManager support

- FortiGuard database updates can be downloaded directly from FortiManager (starting in FortiManager v7.6.2).

ML baseline

We have added the ability to backup and restore ML baseline. This is useful when the device is replaced or undergoes the RMA process. This is a CLI-based feature, see `execute backup system-db ml-baseline`.

New hardware model support

FortiNDR-3600G is released as a center-only appliance with global investigation query and tagging features (not supported on CM-VM).

Comment Event Format support

FortiNDR can now send out CEF formatted logs. This is CLI feature only. Please refer to: `config system syslog settings, set format {default|cef}`.

Endace support

New security fabric connector Endace is supported. Once configured, under NDR log, forensic tab users can pivot to Endace for PCAP analysis.This can be used instead of the FortiNDR conditional attack PCAP feature so users do not experience degradation in performance.

CLI

New CLI commands:

- `execute filetype-prefilter sniffer [file-type-groups]`:Set the file type to be processed in sniffer mode.
- `execute backup system-db ml-baseline`: Backup FortiNDR ML baseline information in Standalone or Center mode.
- `execute restore system-db ml-baseline`: Restore FortiNDR ML baseline informaiton in Standalone or Center mode.
- `execute export top-queries`: Export the FortiNDR top queries as a zip file with password.
- `configure system ndr settings`: New otapp option was added to ips-dbs setting. Introduced new settings to manage pcap capturing which support local and remote storage.
- `config system syslog fortianalyzer settings`: Add support to the new Netflow anomaly and ML detection log.
- `config system syslog1 settings`: Add support to the new Netflow anomaly and ML detection log. Add CEF log format support.
- `config system syslog2 settings`: Add support to the new Netflow anomaly and ML detection log. Add CEF log format support.
- `execute filetype-prefilter`: Enhanced to included *file type groups* to allows user to choose which file types to process.

Updated CLI commands:

- `exec reset-ml-baseline-time netflow`: Enhanced to include a *sensor group id*.
- `diagnose hardware sensorinfo`: Now supported in FortiNDR 3500F, 1000F and 3600G.
- The `set sniffer {off | ndrd | snifferd}` option was added to `config system interface`. Use this option to change the Sniffer mode of the network interface.
- `execute cleanup netflow_ml`: Added support to clean up all Netflow ML Discovery logs.
- `execute raidlevel`: Added support for disk encryption in FortiNDR 1000F and 3600G platforms.
- `diagnose debug` for ctrl/sync daemon in center and sensor mode.

System integration and support

The following integration is tested and supported in FortiNDR 7.6.0.

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 7.6.0 supports the following models:

Model	Mode	Details
FortiNDR-3600G	Center	
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 08	Sensor	Requires Center to manage. Supported for ESXi, KVM, AWS, GCP, Azure 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 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 7.6.0. For inquires about a particular bug, contact Customer Service & Support.

Bug ID	Description
1055570	Resolved an issue where LDAP integration did not work properly on FNDR KVM
1063045	Fixed filtering for user feedback in ML Network Insights.

Known issues

The following issues have been identified in version 7.6.0. For inquires about a particular bug or to report a bug, contact Customer Service & Support.

Bug ID	Description
1074419	FortiNDR encounters errors when attempting to download FortiGuard updates from FortiManager (FortiManager v7.6.0 and v7.6.1 are affected).
1076983	FortiNDR models 3600G and VM CM cannot download FortiGuard updates from FortiManager (FortiManager v7.6.0 and v7.6.1 are affected).

www.fortinet.com