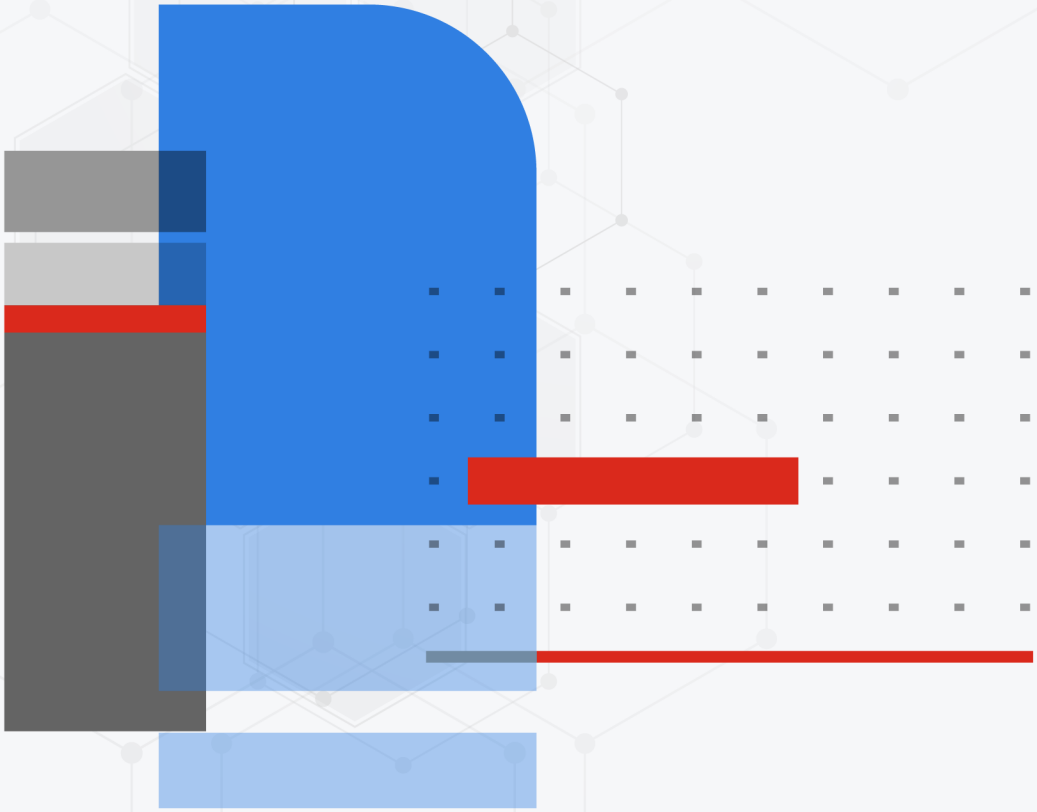
# Release Notes

FortiNDR 7.4.1



**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

April 12, 2024
FortiNDR 7.4.1 Release Notes
55-741-964110-20240412

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2023-12-01 | Initial release. |
| 2024-03-22 | Updated Introduction on page 5. |
| 2024-04-08 | Updated Resolved issues on page 19 |
| 2024-04-12 | Updated Resolved issues on page 19. |

# 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

FortiNDR requires the below SKU to enable FortiGuard downloads and lookups. The SKUs available are:

| Model | SKU | Description |
|---|---|---|
| FortiNDR-3500F | FNR-3500F | FortiNDR-3500F appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology.<br>2 x 10Gb GE Copper (supports 10/1000/10000 without transceivers), 4 x 10G SFP+ interfaces, 2x 1 Gigabit Ethernet connection (management). |
| | FNR-3500F-BDL-331-DD | Hardware plus 24x7 FortiCare, with NDR and ANN engine updates & baseline. |
| | FC3-10-AIVMS-461-02-DD | Subscriptions license for FortiNDR-VM (16 CPU) with 24x7 FortiCare with NDR and ANN engine updates & baseline |
| | FC4-10-AIVMS-461-02-DD | Subscriptions license for FortiNDR-VM (32 CPU) with 24x7 FortiCare with NDR and ANN engine updates & baseline |
| | FC-10-AI3K5-588-02-DD | Netflow Support for FortiNDR-3500F |
| FortiNDR-VM16 | FC3-10-AIVMS-588-02-DD | Netflow Support for FortiNDR-VM16 |
| FortiNDR-VM32 | FC4-10-AIVMS-588-02-DD | Netflow Support for FortiNDR-VM32 |

Netflow is purchased separately for hardware and VM platforms.

Customers need to have the correct SKU for NDR functionalities to work. If customers are running FortiAI VMs on v1.5.x versions, please follow upgrade information below.

For customers running FortiAI v1.5.x and would like to enjoy the new NDR features, a co-term upgrade is necessary. Please contact customer services at cs@fortinet.com. For current v1.5.x customers who do not require the new NDR features, they can upgrade to v7.0 and use their existing license to download ANN updates and continue to use ANN malware scanning features.

For customers wanting to use the 7.0 NDR features, v7.0 requires a new license to enable further download of packages and lookup to FortiGuard services. In order to enjoy v7.0 NDR features, customers should:

1. Prepare/purchase/coterm v7.0 license file for upgrade.
2. Upgrade the VM/hardware to v7.0.
3. Load the new license file into the unit with the GUI.

Customers can still upgrade to v7.0.x with the new GUI interface and better filtering using v1.5.x license, and continue to use v1.5.x FortiAI malware scanning features.

If a new v7.0 (or higher) license file is loaded on a 1.5.x VM, the VM will become non-functional. This does not apply to FAI-3500F hardware.

# 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

- 7.4.1 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 18.
- FNR-3500F gen3 only: Upgrade from v7.1.0 to v7.2.x GA is supported.
- When upgrading FNR-3500F from 7.4.0 to 7.4.1 in Center Mode, you will need to run the following command after upgrade:

```
execute db restore
```

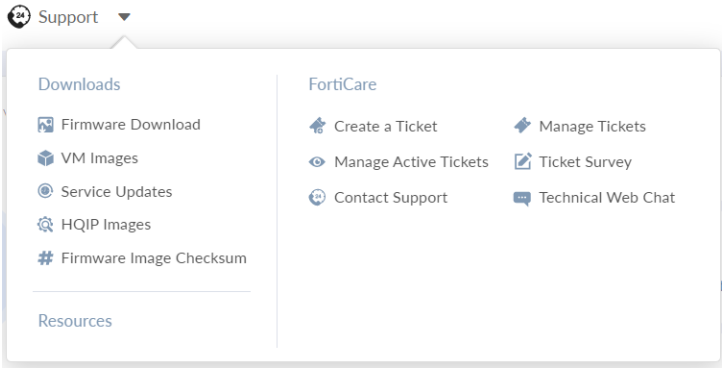
**VM Devices:**
Direct upgrade from v1.5.x, v7.0.x or v7.1.0 to v7.2.1 is not supported.

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

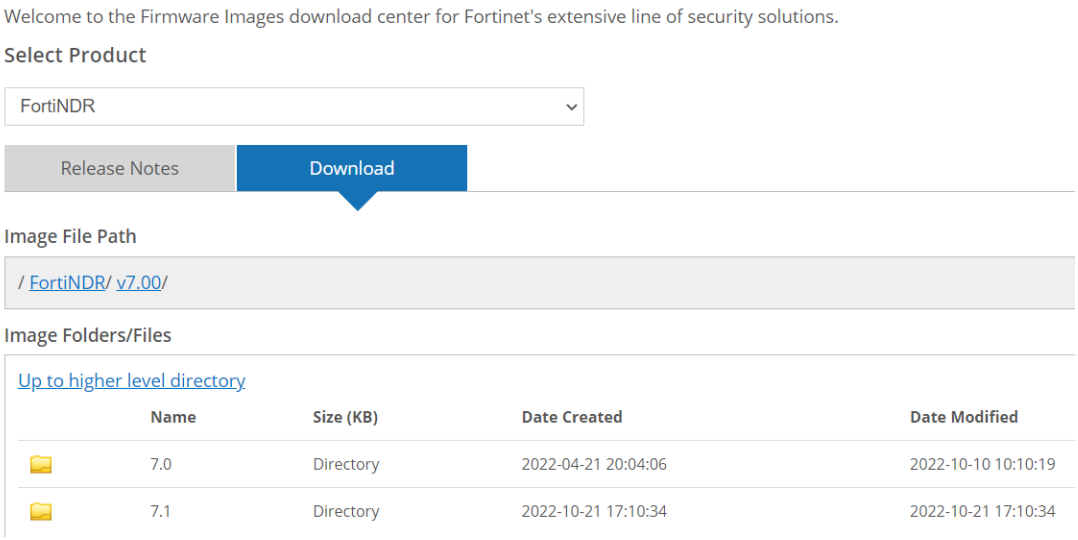
# Downloading the latest firmware version

**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.




# Upgrading the firmware version on hardware devices

**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. Due to a known issue, HA is not supported in v7.2.x. If HA was configured in the previous configuration file, use the following CLI to disable it.

   ```
   config system ha
   ```

   For information, see the *FortiNDR CLI Reference*.
4. Use the configuration settings you recorded earlier to manually restore the settings. For *Device Input*, you just need to re-authorize the device again.

# Upgrading the firmware version on VM devices

Direct upgrade from v7.2.x to v7.4.0 is supported.
Direct upgrade from v1.5.x, v7.0.x or v7.1.0 to v7.4.0 is not supported.

**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 deploy standalone VM:**

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. Deploy the VM from scratch. See Deploying FortiNDR VM.
3. Update the firmware version in the backup file you downloaded in Step 1.
   a. Open the backup file with a text editor such as Notepad ++.
   b. Update the firmware version in the first line of the file. For example:

      ```
      #config-version=FAIVMW-7.01-FW-build249-230302
      ```

      Will be updated to:

      ```
      #config-version=FAIVM-7.4.0-FW-build509-230302
      ```

4. Restore the backup configuration file.
   a. Click the Account menu at the top-right of the page.
   b. Go to *Configuration* > *Restore*.
   c. Click *Upload* and navigate to the location of the configuration file you downloaded.
5. 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 7.4.1

This document provides information about FortiNDR version 7.4.1 build 0520.

These Release Notes include the following topics:

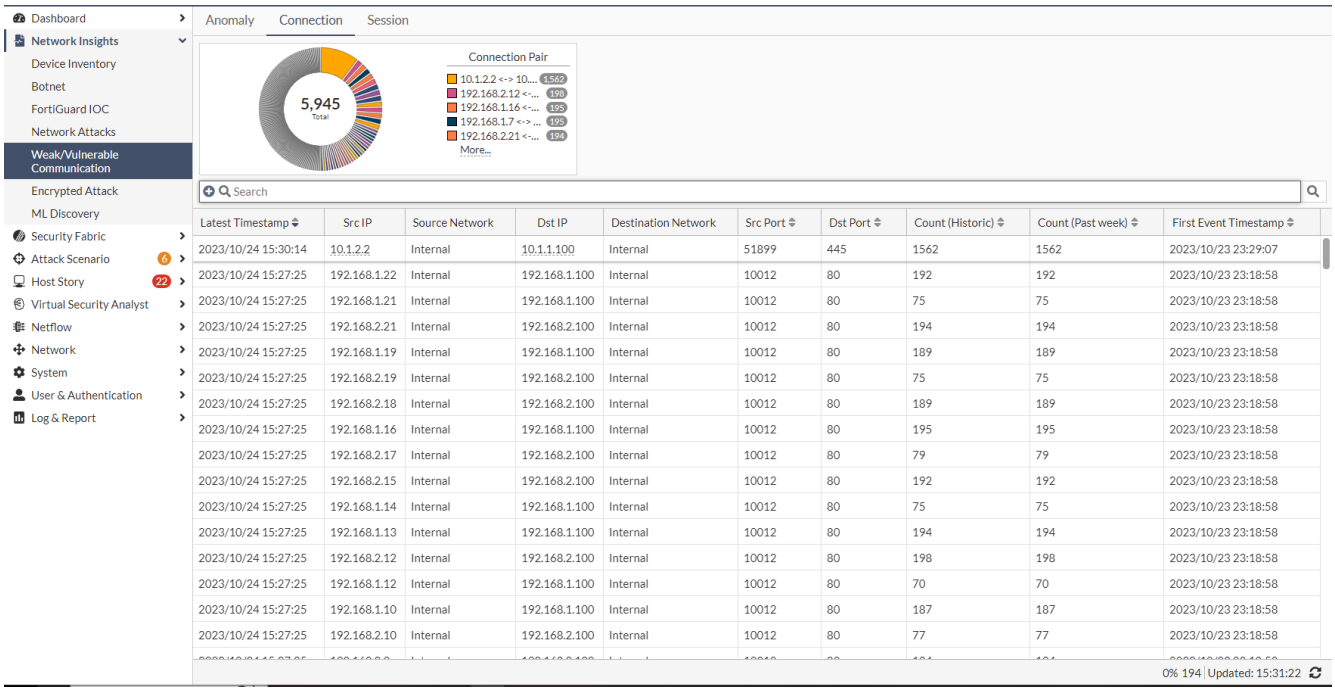


## New features and enhancements

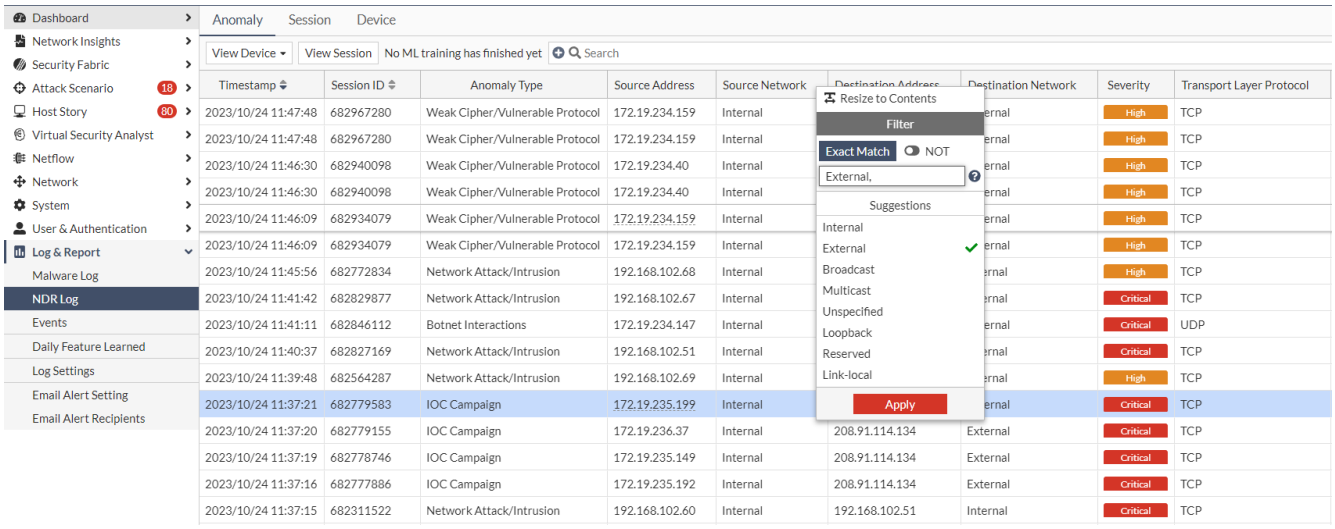
The following is a summary of new features and enhancements in version 7.4.1. For details, see the *FortiNDR 7.4.1 Administration Guide* in the Document Library.

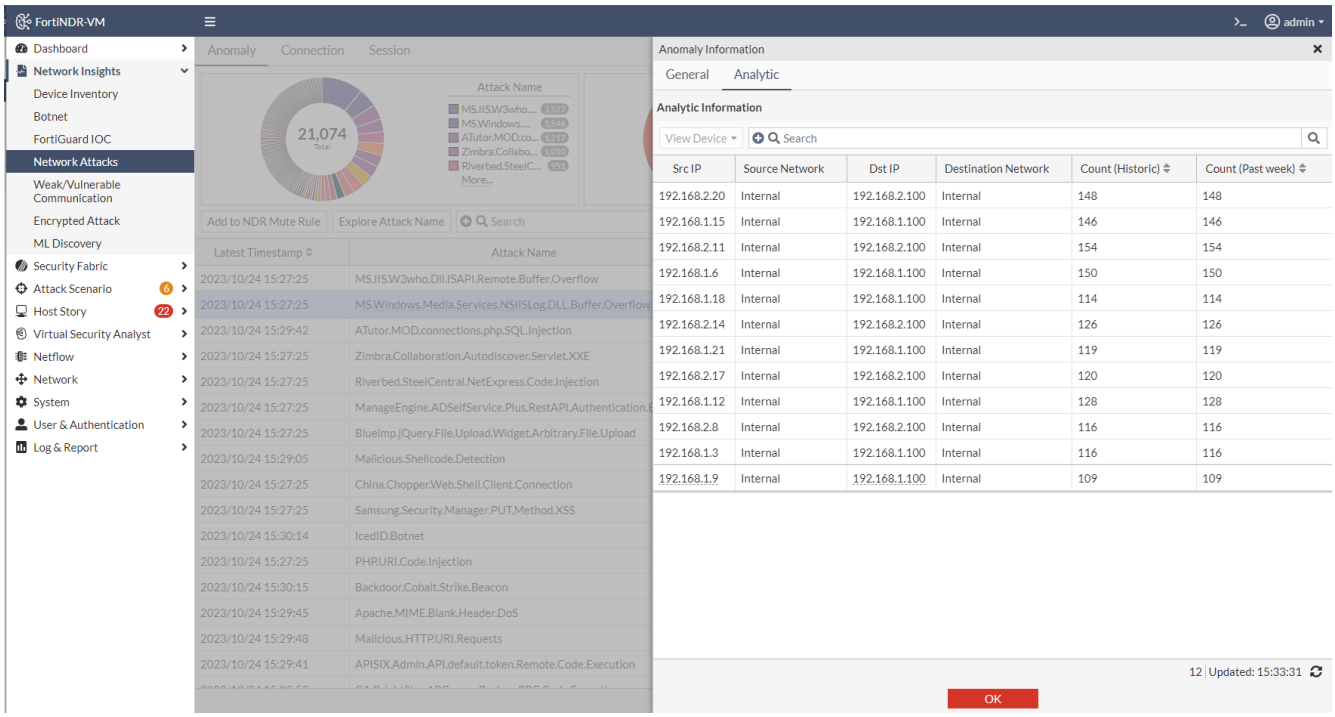
### Internal External network identifier support

We have added *Source Network* and *Destination Network* columns to all NDR related tables.



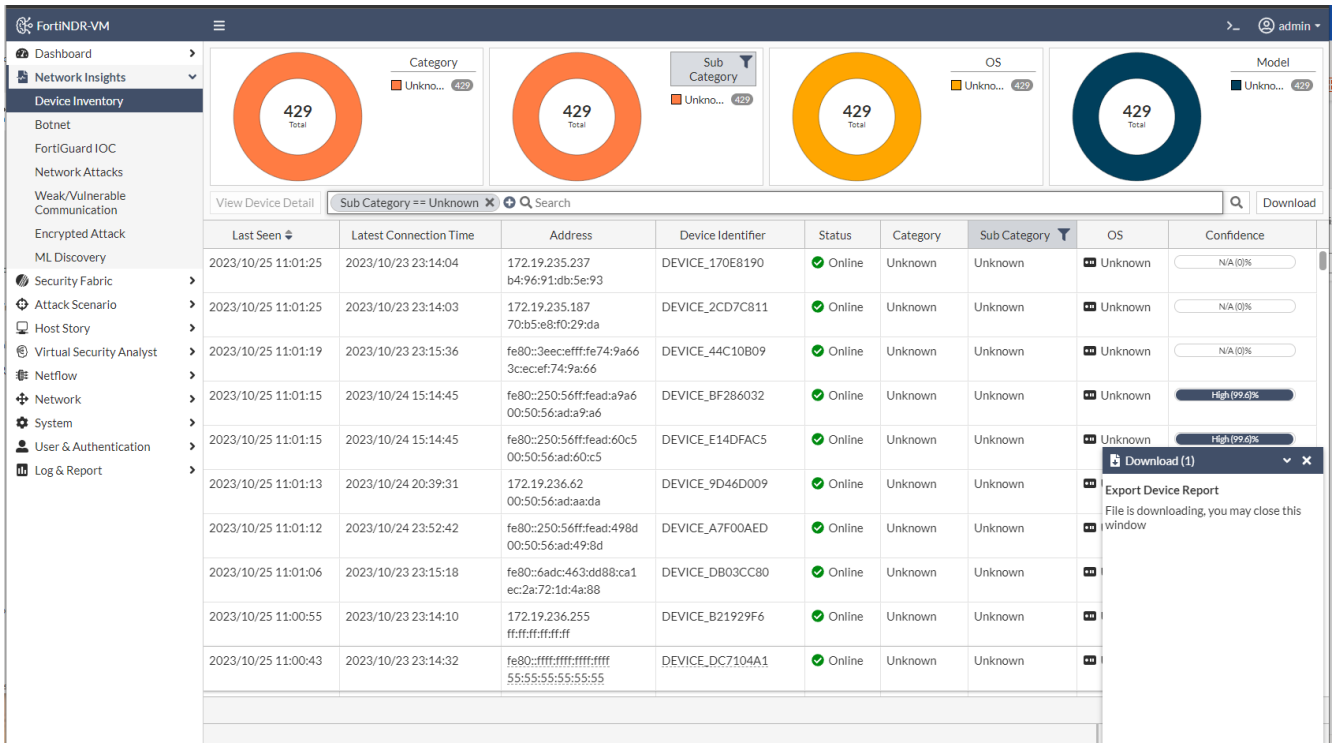

The new *Network* columns allow you to filter the address based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. The filtering mechanism works for both IPv4 and IPv6 Addresses.



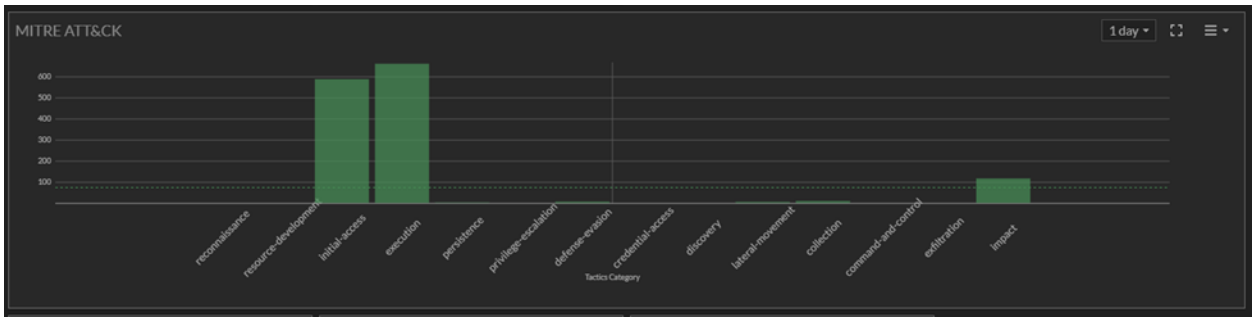

## Download device inventory

A new *Download* button was added to the *Device Inventory* page. This allows you to download the most recent 5 million entries as a zipped file in a CSV format. Once you click the *Download* button, a window will pop up at the lower-right corner with the download status of the zip file. You can navigate away from the page while the download is still in progress. Once the download is complete, you will be prompted to close it.

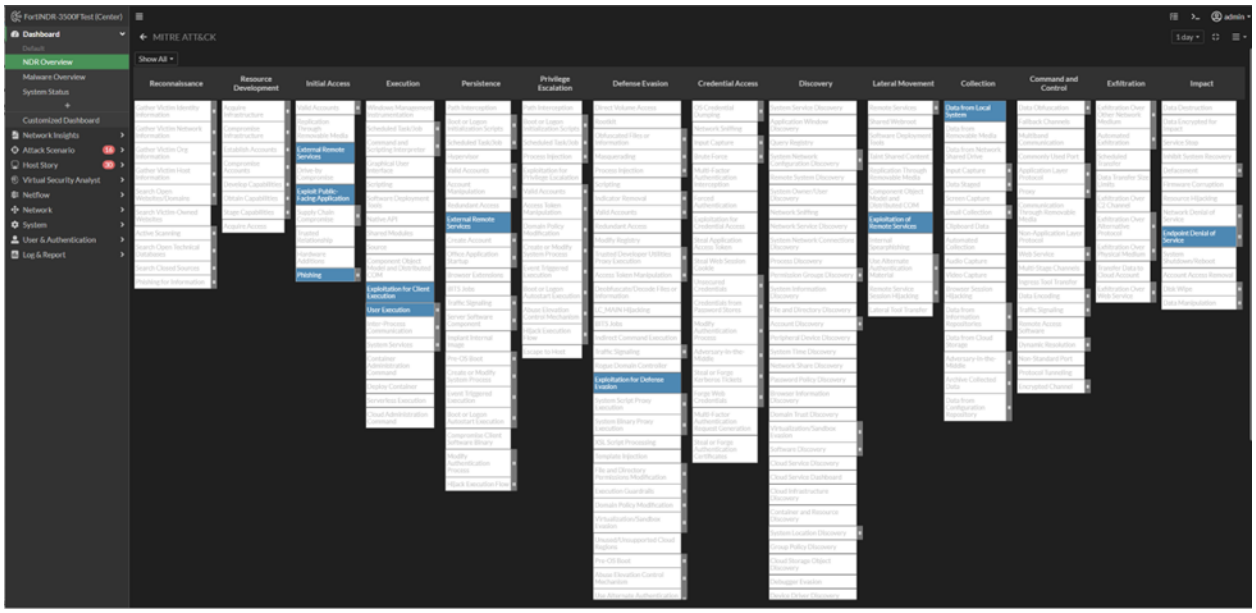



# MITRE Attack Widget

The MITRE attack widget maps network attacks and botnet under each MITRE attack tactics category. You can view data from different time frames (*1 day*, *1 week* and *1 month*) using the dropdown menu at the top-right corner of the page.




In the expanded view of this widget, a MITRE Attack matrix map will detail each specific MITRE attack tactic employed against the network.



## Events API

We have added an new *Events* API to retrieve anomaly events. For more information, see the API guide in the *FortiNDR Administration Guide*.

## System integration and support

The following integration is tested and supported in FortiNDR 7.4.1.

| | |
|---|---|
| **FOS/FortiGate** | • FortiNDR Fabric Device widgets including *Detection Statistics* and *System Information* supported in FOS 7.0.5 and 7.2.4<br>• 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)<br>• HTTP2 file submission from FortiGate 7.2.0<br>• FortiGate inline blocking (with AV profile) is supported in FOS 7.0.1 and higher.<br>• FortiGate quarantine via webhook 6.4.0 and higher. |
| **FortiProxy** | • HTTP2 file submission from FortiProxy 7.0.0 and higher<br>• 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.<br>• FortiWeb 6.3.11 and higher.<br>• Squid and other compatible ICAP clients.<br>• FortiProxy 7.0.0.<br>• FortiNAC quarantine support (v9.2.2+)<br>• FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are not supported at this time.<br>• FortiSwitch quarantine via FortiLink (FortiSwitch v7.0.0+ and FortiGate v7.0.5+)<br>  FortiNDR 7.0.1 and later supports sending both malware and NDR logs to FortiAnalyzer and FortiSIEM or other syslog devices.<br>FortiAnalyzer 7.2.0 supports receiving logs from FortiNDR (log view only).<br>FortiAnalyzer 7.2.1 supports reporting based on logs. |

# Supported models

FortiNDR version 7.4.1 supports the following models:

- FortiNDR-1000F
- FortiNDR-3500F gen3*
  For hardware details please visit hardware quick start guide or the notice below.
- FortiNDR VM 16 & 32
- FortiNDR KVM
- FortiNDR on AWS (BYOL)
- FortiNDR on GCP (BYOL)
- FortiNDR on Alibaba (BYOL)
- FortiNDR on Azure (BYOL)

## *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 and v7.2.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 7.4.1. For inquires about a particular bug, contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 919802 | An error pops up when clicking the *Download File* button. |
| 923363 | Fixed typo for baselining below one minute message. |
| 925108 | *Explore Host Story* link *in Malware Big Picture* details does not work. |
| 955625 | In Center mode, commands do not function properly when sensors are positioned behind a NAT. |
| 958755 | Malware log device type filter failed to filter corresponding malware. |
| 964048 | The *Time Period* dropdown is not displayed in widgets. |

## Common Vulnerabilities and Exposures

| Bug ID | Description |
|---|---|
| 961070 | FortiNDR 7.4.1 is no longer vulnerable to the following CVE Reference:<br>• CVE-2023-38545 |

# Known issues

The following issues have been identified in version 7.4.1. 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 click-house. |
| 928978 | Logs sent to FortiAnalyzer from FortiNDR are not displaying the same time stamps. |
| 933649 | ICAP is not showing response from submissions. |
| 950842 | Blinking Amber LED is appears at the front of the FAI 3500F |
| 951919 | In GUI, *Big picture*, *Hostname modification*, *Download sample* button and *FortiGuard FP* submission are disabled in Center mode |
| 972581 | The right-click filtering operation on an IP without a mask is not working at this time. The selection in either *Overlaps* or *Does not overlap*in the right-click menu options will not work. **Workaround**: Use the column header to filter the IP. |
| 978096 | Malware download button malfunction at sample details on standalone FortiNDR. |

www.fortinet.com