FORTINET

Administration Guide

FortiNDR 7.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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 CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 6, 2023
FortiNDR 7.2.0 Administration Guide
55-720-855930-20230828

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-03-09	Initial release.
2023-06-06	Updated Appendix C - FortiNDR ports on page 176.
2023-08-09	Updated FortiNDR health checks on page 141.
2023-08-14	Updated Operating mode, protocols, and file type support on page 14.
2023-08-21	Updated Operating mode, protocols, and file type support on page 14.
2023-08-28	Updated Introduction on page 8.

Introduction

FortiNDR (formerly FortiAI) is the first Fortinet Network Detection and Response product from Fortinet. Apart from the Virtual Security Analyst™ with rapid malware detection technology based on neural networks, FortiNDR is built on FortiAI's high throughput malware scanning technology with extended features to detect Network Anomalies with auto and manual mitigation techniques.

FortiNDR is the next generation of Fortinet breach detection technology, using both ML and Artificial Neural Networks (ANN) which can detect network anomalies and high velocity malware detection and verdict.

ANN is able to mimic human behavior using the Virtual Security Analyst (VSA)™, which is capable of the following:

- Detect encrypted attack (via JA3 hashs), look for presence of malicious web campaigns visited , weaker ciphers, vulnerable protocols, network intrusions and botnet-based attacks.
- Profile ML traffic and identify anomalies with user feedback mechanism.
- Quickly detect malicious files through neural network analysis including NFS file scan shares.
- Analyze malware scientifically by classifying malware based on its detected features, for example, ransomware, downloader, coinminer, and so on.
- Trace the origins of the attack, for example, worm infection.
- Outbreak search can use the similarity engine to search for malware outbreaks with hashes and similar variants in the network.
- Take advantage of Fortinet's Security Fabric with FortiGate(s) and other Fortinet Security Fabric solutions, along with 3rd party API calls, to quarantine infected hosts.

FortiNDR's neural networks run in a 2U form factor using accelerated hardware with a custom GPU such as FortiNDR-3500F, as well as using VMs with 16 or 32 vCPU support.

FortiNDR can operate in different modes: sniffer mode where it captures traffic on network from SPAN port (or mirrored if deployed as VM), integrated mode with FortiGate devices and input from other Fortinet devices (see release notes for supported devices), with inline blocking with FortiOS AV profiles (7.0.1 and higher). You can also configure FortiNDR as an ICAP server to serve ICAP clients such as FortiProxy and Squid. All modes can operate simultaneously.

Key advantages of FortiNDR include the following:

Detect network anomalies with different techniques where traditional security solutions might fail

- Provide more context to attacks such as malware campaign name, web campaign devices and users participate in, intrusions and botnet attacks
- Tracing and correlate source of malware events such as worm based detection
- Manual and automatic mitigation (AKA Response) with Fortinet Security Fabric devices (such as FortiGate, FortiSwitch, FortiNAC), as well as 3rd Party solutions (via API calls).

FortiNDR software and license are not limited by the number of devices/IPs supported. Without this limit, FortiNDR-1000F for example, can easily support more than 10K IPs which should be sufficient for most network deployments. For performance/sizing for other platforms, please consult with your local Fortinet system engineering team.

Getting started

Use the CLI for initial device configuration. You can enable SSH access on the port1 administration interface or any other administrative port set through the CLI command including RAID. You can also connect to the CLI using the console port. Some troubleshooting steps also use the CLI.

Use the GUI to configure and manage FortiNDR from a web browser on a management computer. We recommend using Google Chrome.

To connect to the FortiNDR GUI:

1. Connect to the port1 management interface using the following CLI commands:

```
config sys interface
    edit port1
    set ip x.x.x.x/24
end
```

2. In a web browser (Chrome recommended), browse to `https://192.168.1.88`.
   The GUI requires TCP port 443.
3. Use *admin* as the name and leave the password blank. Click *Login*.

Loading the ANN database to FortiNDR for malware detection

FortiNDR utilizes both FortiGuard updates to local DB as well as lookup for detecting network anomalies. For full list of updates please refer to Appendix D - FortiGuard updates on page 177 for details. The section below discusses one of the updates: ANN for malware detection.

The ANN (Artificial Neural Network) database enables scanning of malware using accelerated ANN. Unlike AV signatures, ANN DB does not require updates daily. ANN is only updated once or twice a week to enable detection of the latest malware.

There are two ways to update ANN. You can update using FDN (FortiGuard Distribution Network) if internet is available, or on Fortinet support website after the product is registered.

Currently FortiGuard updates are available via US, EMEA and Japan. Depending on your location, manual update might be faster. The average time of ANN update via Internet is about 1–2 hours. Using the local CLI takes about 10 minutes.

To update the ANN database using CLI:

```
execute restore kdb {disk <filename> | ftp <file name> <server_ipv4> | scp <file name>
     <server_ipv4> | tftp <file name> <server_ipv4>}
```

To update the ANN database by downloading from FDN to the FortiNDR device:

1. Format a USB drive in another Linux machine using the command `fdisk /dev/sdc`.
   Ensure the USB drive has enough capacity and create one partition using EXT4 or EXT3 format.

```
/# fdisk /dev/sdc

Welcome to fdisk (util-linux 2.25.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help):
```

2. Format `sdc1` using the `mkfs.ext4 /dev/sdc1` command.

```
/# mkfs.ext4 /dev/sdc1
mke2fs 1.43.7 (16-Oct-2017)
Creating filesystem with 7554430 4k blocks and 1888656 inodes
Filesystem UUID: faec541a-8f39-4a14-a643-93cf75ae748e
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

/#
```

FortiTester is a great companion for FortiNDR as FortiTester can send a malware strike pack over different protocols such as HTTP, SMB, SMTP, to simulate malware in the network. You can use FortiTester to generate malware and test FortiNDR for detection.

The following is an example of the result.

```
/# fdisk -l /dev/sdc

Disk /dev/sdc: 28.8 GiB, 30943995904 bytes, 60437492 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x2a7d7590

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdc1        2048 60437491 60435444 28.8G 83 Linux
```

3. Copy `moat_kdb_all.tar.gz` and `pae_kdb_all.tar.gz` to the root directory of USB drive, in this example, `/AI_DB`.

```
/# mkdir /AI_DB
/# mount /dev/sdc1 /AI_DB/
/#
```

The following is an example of the result.

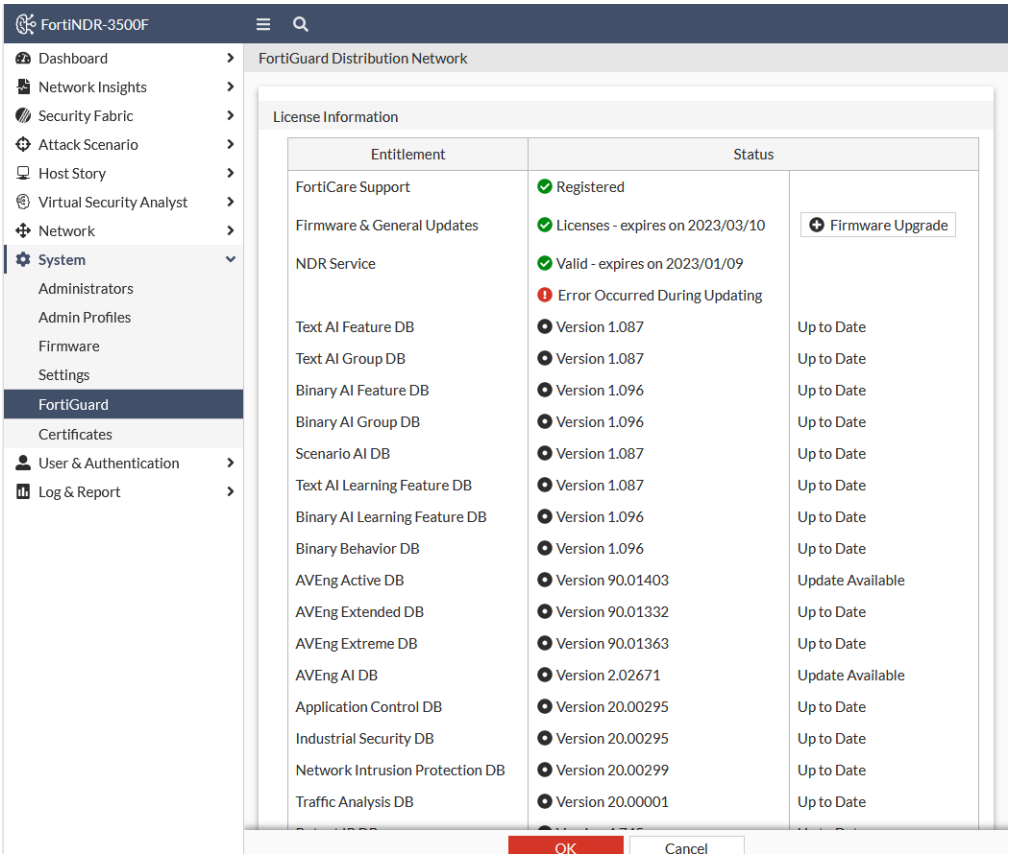
```
/AI_DB# ls
lost+found          moat_kdb_all.tar.gz  pae_kdb_all.tar.gz
/AI_DB#
```

4. Copy the files onto the FortiNDR by mounting the USB drive on the FortiNDR device and using the `execute restore kdb disk pae_kdb_all.tar.gz` and the `execute restore kdb disk moat_kdb_all.tar.gz` commands.

```
FAI35FT319000004 # execute restore kdb disk pae_kdb_all.tar.gz
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Mounting /dev/sda1
Mounting /dev/sdb1
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e51D0v
Copying file failed!
Mounting /dev/sdc1
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e51D0v
Get file OK.
MD5 verification succeed!
KDB files restoration completed
Scanner restart completed

FAI35FT319000004 #
```

```
FAI35FT319000004 # execute restore kdb disk moat_kdb_all.tar.gz
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Mounting /dev/sda1
Mounting /dev/sdb1
Try copying file from /kdb_disk/moat_kdb_all.tar.gz to /var/spool/tmp/up_uWobUb
Copying file failed!
Mounting /dev/sdc1
Try copying file from /kdb_disk/moat_kdb_all.tar.gz to /var/spool/tmp/up_uWobUb
Get file OK.
MD5 verification succeed!
KDB files restoration completed
Scanner restart completed

FAI35FT319000004 #
```

5. To verify the ANN database in the GUI, go to *System* > *FortiGuard*.



6. To verify the ANN database in the CLI, use the `diagnose kdb` command and check that there are four `KDB Test Passed` status lines.
   You can check the latest version of FortiNDR ANN at https://www.fortiguard.com/services/fortindr.

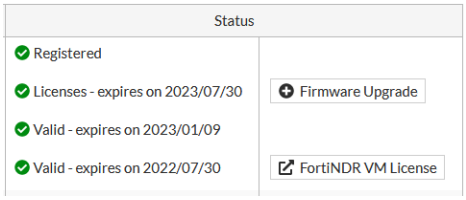
```
FAI35FT319000004 # diagnose kdb
System Time:  2020-02-11 14:50:34 PST (Uptime: 0d 22h 32m)
Start: /bin/pae2 -test

2020-2-11 14:50:34
[TEST] - Start KDB Test...
        [TEST] - Loading Group KDB...
        [TEST] - Group KDB Rec Num: 383887
        [TEST] - Loading Feature KDB...
        [TEST] - Feature KDB Rec Num: 45562000
[TEST] - KDB Test Passed

2020-2-11 14:50:48
Start: /bin/pae_learn -test

2020-2-11 14:50:48
[TEST] - Start KDB Test...
        [TEST] - Loading Mal KDB...
        [TEST] - Mal KDB Rec Num: 1770913
        [TEST] - Loading Clean KDB...
        [TEST] - Clean KDB Rec Num: 34625563
[TEST] - KDB Test Passed

2020-2-11 14:50:55
Start: /bin/moat_learn -test
2020-2-11 14:50:55
2020-2-11 14:50:55
[TEST] - Start KDB Test...
        [TEST] - Loading KDB-0...
        [TEST] - KDB-0 Rec Num: 127612293
        [TEST] - Loading KDB-1...
        [TEST] - KDB-1 Rec Num: 7058519
[TEST] - KDB Test Passed
2020-2-11 14:51:25
Start: /bin/moat_engine -test kdb
2020-2-11 14:51:25
[TEST] - Start KDB Test...
        [TEST] - Loading Group KDB...
        [TEST] - Group KDB Rec Num: 15235200
        [TEST] - Loading Feature KDB...
        [TEST] - Feature KDB Rec Num: 370576784
[TEST] - KDB Test Passed
2020-2-11 14:53:39
```

When you have finished using the USB or SSD drive, remove the drive from FortiNDR. Some disk-related CLI commands such as `execute factoryreset`, `execute partitiondisk`, or `diagnose hardware sysinfo` might treat the additional disk as the primary data partition.

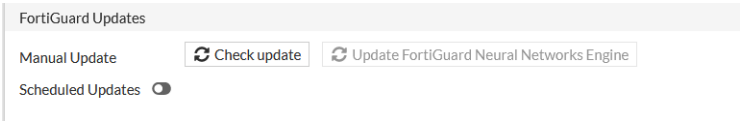
Updating the ANN database from FDS for malware detection

To update the ANN database from FDS:

1. Go to *System* > *FortiGuard*.
2. Check the *License Status* to ensure there is a valid license.
   If the license is not valid:
   - The unit cannot update from FDS.
   - Ensure the unit is not on internal FDS and the unit has a subscription for *FortiGuard Neural Networks engine updates & baseline*.



3. Click *Check Update*.
   If there are updates, an *Update Now* button appears and the *Status* column shows the components with updates.



4. Click *Update Now*.
   Due to the size of databases, the update might take several hours depending on your Internet speed. During the update, check the *Status* column.

License Status: Valid until 2021/01/03

Entitlement	Version	Last Update Date	Status
Binary AI 5			
Binary AI Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Binary AI Learning Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Binary AI Feature DB	Version 1.017	2020/03/02 04:57:45	Up to Date
Binary AI Group DB	Version 1.017	2020/03/02 04:57:45	Up to Date
Binary AI Learning Feature DB	Version 1.017	2020/03/02 04:57:45	Up to Date
Text AI 5			
Text AI Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Text AI Learning Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Text AI Feature DB	Version 1.000	2020/03/02 02:37:00	Downloading
Text AI Group DB	Version 1.000	2020/03/02 02:37:00	Downloading
Text AI Learning Feature DB	Version 1.000	2020/03/02 02:37:00	Downloading

Operating mode, protocols, and file type support

FortiNDR can operate in both detecting network anomalies as well as malware analysis using ANN. If FortiNDR functionalities are not needed, and you prefer pure file analysis, NDR functionalities can be switched off with the command "`execute ndrd {on|off}`"

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

Operating Mode	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
Sniffer	N/A	N/A	HTTP, SMBv2, IMAP, POP3, SMTP, FTP	TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP,SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors	Using SPAN port or network TAP
Integrated	FortiGate	OFTP (v5.6-v6.x), HTTP2 (v7.0 FOS)	HTTP, HTTPS (with SSL decryption), SMTP, POP3, IMAP,		FortiGate v7.0.1 supports INLINE blocking with AV profile
	FortiProxy	HTTP2	HTTP, HTTPS (with SSL decryption), SMTP, POP3, IMAP		
ICAP	FortiWeb	ICAP	HTTP, HTTPS		Supports using FortiNDR as ICAP server and multiple
	FortiProxy	ICAP	HTTP, HTTPS		FortiGates, FortiWeb and FortiProxy or third-party ICAP client such as Squid.
Other / API	FortiSOAR	HTTPS API upload	HTTPS		Using API

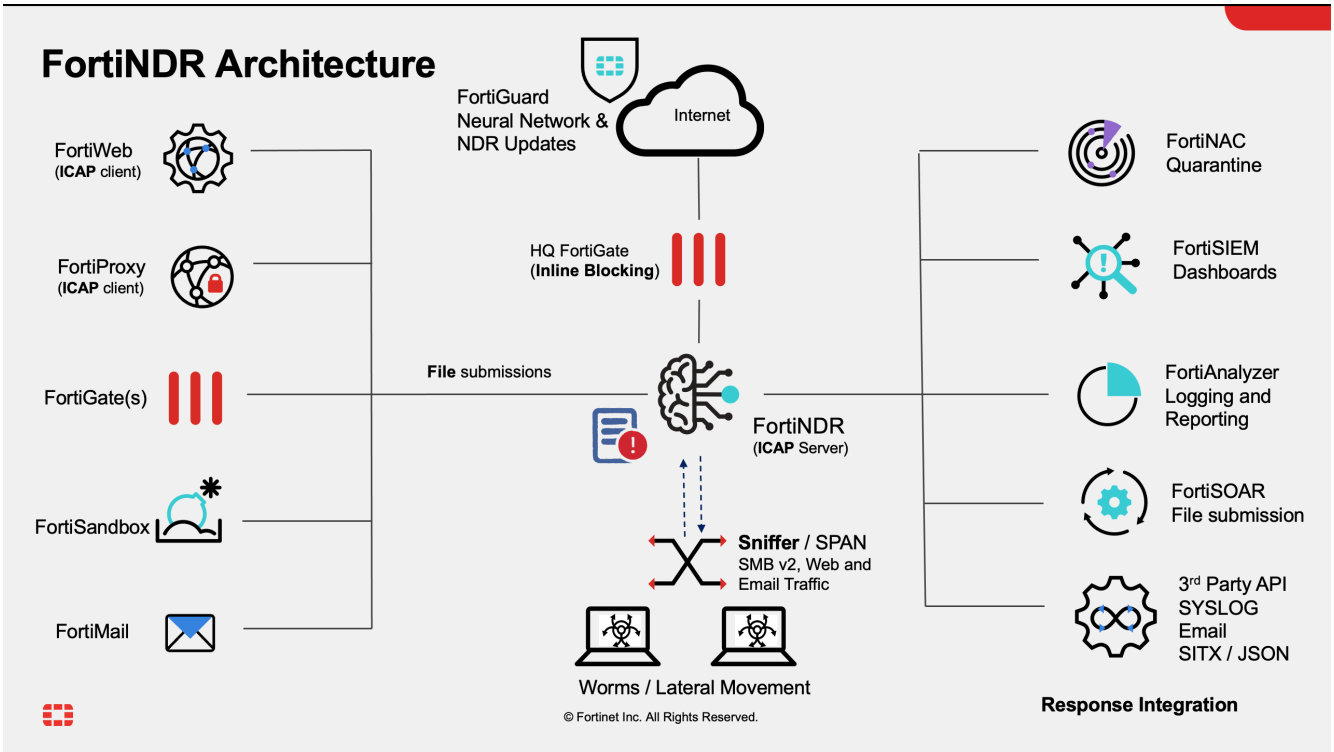
Operating Mode	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
					available from FortiNDR for file upload
	FortiMail	HTTPS API upload	HTTPS		Using API available from FortiNDR for file upload
	FortiSandbox	HTTPS API upload	HTTPS		Using API available from FortiNDR for file upload
	Scripts (refer to Appendix for sample scripts)	HTTPS API upload			
	NFS and SMB file shares	SMB/NFS			Direct map and scan

Supported file types for all operating modes:

32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, HWP Hangul_Office, TAR, XZ, GZIP, BZIP, BZIP2, RAR, LZH, LZW,ARJ, CAB, _7Z, PHP, XML, POWERSHELL, BAT, HTA, UPX, ACTIVEMIME, MIME, HLP, BASE64, BINHEX, UUE, FSG, ASPACK, GENSCRIPT, SHELLSCRIPT, PERLSCRIPT, MSC, PETITE, ACCESS, SIS, HOSTS, NSIS, SISX, INF, E32IMAGE, FATMACH, CPIO, AUTOIT, MSOFFICEX, OPENOFFICE, TNEF, SWF, UNICODE, PYARCH, EGG, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, LNK, KGB, Z, ACE, JAR, APK, MSI, MACH_O, DMG, DOTNET, XAR, CHM, ISO, CRX, INNO, THMX, FLAC, XXE, WORDML, WORDBASIC, OTF, WOFF, VSDX, EMF, DAA, GPG, PYTHON, CSS, AUTOITSCRIPT, RPM, EML, REGISTRY, PFILE, CEF, PRC, CLASS, JAD, COD, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN

- A sample that cannot be parsed as one of the types above is categorized as *Other*. Detection of these types is not supported by Artificial Neural Networks (ANN).
- The sniffer will not save unsupported file types or supported but corrupted files. For example, if the traffic contains a corrupted zip file that cannot be unzipped, the sniffer will not save it to the *Log & Report >Malware Log*.

FortiNDR supports quarantine with incoming webhook from FortiOS 6.4 and higher. For details, see the Release Notes. For FortiNDR to quarantine via FortiGate, you must provide VDOM information to FortiGate. For details, see Automation Framework on page 65.



Supported file types for ANN:

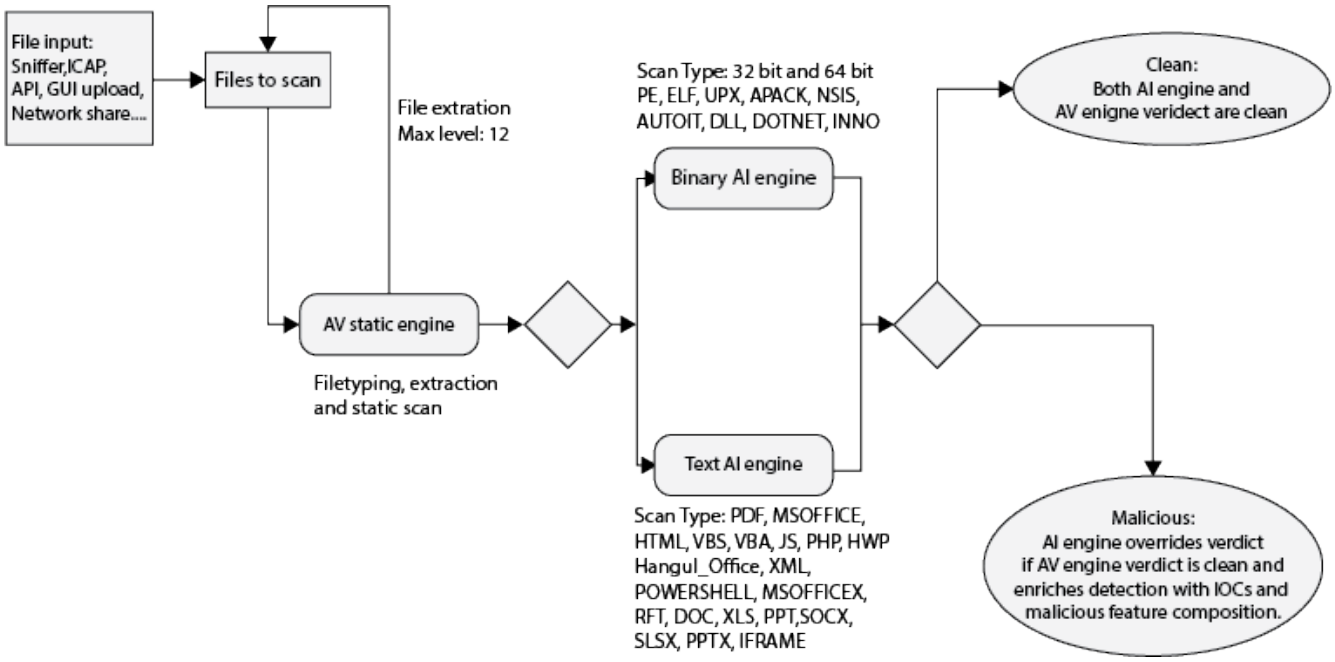
For ANN supported file types, ANN will process and provide a feature breakdown between different attack scenarios (like Ransomware, banking trojan etc) 32 bit and 64 bit PE, PDF, MSOFFICE, HTML, ELF, VBS, VBA, JS, PHP, HWP Hangul_Office, XML, POWERSHELL, UPX, ASPACK, NSIS, AUTOIT, MSOFFICEX, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, DOTNET, INNO, IFRAME

File types supported by ANN will be scanned by the ANN and AV engines. Other supported file types will be scanned by AV engine only.

File scan flow

Stage 1

All files to be scanned go through the same flow. First, the files are scanned by the Antivirus static engine. The AV engine identifies the file types and assigns a verdict at the same time. If the files are archive files such as ZIP or TAR, they are extracted at this stage (up to 12 layers). The extracted files are then sent back to be scanned by the Antivirus static engine.



Stage 2

If it is a supported file type by ANN (listed above), file type, files are sent to either the *Binary* or *Text AI* engine for the Stage 2 scan. Files will go through the Stage 2 Scan regardless of the verdict in Stage 1. The AI engine will only override the verdict if the file is *Clean* in Stage 1 and *Malicious* in Stage 2. The Stage 2 AI scan enriches the IOC information and malicious feature composition in the sample detail view.

Architecture considerations

FortiNDR comes in both appliance and VM form factor. The appliance is FortiNDR-3500F. The VM16 and VM32 is subscription-based.

FortiNDR can work in the following modes:

- Standalone sniffer mode.
- Integrated mode with FortiGates. This mode supports all files from FortiGates and other Fortinet Security Fabric devices such as FortiSandbox etc (please refer to release notes or the data sheet for list of products supported)
- ICAP mode. FortiNDR can act as ICAP server and serve ICAP clients such as FortiGate, FortiWeb, and Squid.
- All modes can operate simultaneously.

For proof of concept, consider the following in a deployment:

- FortiNDR is a non-inline, passive device that is capable of very high files-per-second scan rate and speedy detection and verdict of malware. This is achieved by hardware accelerated Neural Networks on the appliance. FortiNDR-3500F is rated at 100000 files per hour or 27.78 files per second. FortiNDR VM has approximately 40-80% of hardware performance without GPU.
- You can use FortiNDR with lots of email, HTTP, and SMBv2 traffic in sniffer mode, and other traffic or files from FortiGates.

- By observing web, email, HTTP, and SMBv2 traffic, the FortiNDR Virtual Analyst can determine the original IP address of the malware attack by examining the historical files/traffic/infection on the network. So the more traffic you send to FortiNDR, the more data FortiNDR can analyze and use.
- For response/mitigation after threats are detected, please refer to *Security Fabric* > *Enforcement Settings* and view the automation profile for details. FortiNDR is capable of calling APIs on different products such as FortiGate, FortiNAC, 3rd Party, and FortiSwitch (via FortiGate Fortlink) for quarantine.

For file type support, see the datasheet and Administration Guide for the most up-to-date information.

Planning deployment

This page contains information about estimating data storage for file analysis throughput.

Storage by model

- FAI-3500F (gen 1 & 2) uses 2 X 3.8TB SSD in RAID1 and comes with the option to purchase additional SSD HDDs.This model will support RAID 10 if 2 x (or more) additional SSD are purchased.
- FNR-3500F (gen3 with fiber card) uses 4 x 3.8TB SSD in RAID10 and comes with the option to purchase additional SSD HDDs.
- FNR-VM comes with 4 different size disk images.

The following table provide guidance for FortiNDR disk storage used for malware scanning only.

Model	Total disk size (RAID 10)	Storage retention
FNDR-3500F 4 SSD	6.6 TB	66 days
FNDR-3500F 2 SSD	3.3 TB	33 days
FNDR-3500 8 SSD	13.2 TB	132 days
FNDR-3500 16 SSD	26.4 TB	264 days
FNDR-VM	1024 GB	20 days
FNDR-VM	2048 GB	40 days
FNDR-VM	4096 GB	81 days
FNDR-VM	8192 GB	163 days

VM16 and VM32 published file processing rate at 40,000 and 80,000 files per hour respectively

* The max. process rate depends on the average size and composition of file types. NDR disk storage depends on a few factors such as:

- Size of data disk allocated in VM
- Number of disks inserted into hardware model

- Throughput of network e.g. with sniffer
- Whether unit is used for NDR and/or pure file analysis only

Please refer to disk management section under system for more information.

Additional SSD

FAI (gen1 & 2 hardware) supports RAID 1 configuration. 2 x 3.84 TB harddisk are shipped by default (max up to 16).

FNR (gen3 hardware) supports RAID 10 configuration. 4 x 3.84 TB harddisk are shipped by default (max up to 16).

Additional disks should be ordered in pairs to increase capacity. Increasing disk capacity will also improve the system input/output operations per second (IOPS) speed.

Total SSDs in FNR-3500F	4 (ship by default by FNR-3500F) 4 x 3.84TB	6	8	10	12	14	16
Total usable capacity (TB) (RAID 10 configuration)	7.7	11.52	15.36	19.2	23.04	26.88	30.72

To add additional SSD:

1. Shut down FNR-3500F
   - Press the power button on the front panel, or
   - Run the following commnd: `exec shut`
2. Insert the extra 4 x SSDs in slot 5-8 (total 16 slots).
3. Power on the unit.
4. Log in to the CLI or console and run the following CLI command:
   `exec raidlevel 10`

After the command is executed, the device will:

- Create the RAID including the new SSDs.
- Reboot and then format the new SSDs. The log can be viewed in the console.

To check the new SSD capacity with the GUI:

Go to *Dashboard* > *System Status*, and check the *System Information* widget.

To check the new SSD capacity with the CLI:

```
Get system raid-status
```

Sample output:

```
FortiNDR-3500F # get system raid-status
Controller Model Firware Driver
------------------------------------------------
a0 PERC H350 Ada 5.190.01-3614 07.714.04.00-
```

```
+---- Unit Status Level Part Of Size (GB)
| u0 OK LEVEL 10 a0 14304
+---- Port Status Part Of Size (GB)
| 64:0 OK u0 3575
| 64:1 OK u0 3575
| 64:2 OK u0 3575
| 64:3 OK u0 3575
| 64:4 OK u0 3575
| 64:5 OK u0 3575
| 64:6 OK u0 3575
| 64:7 OK u0 3575
```

Initial setup

For the meaning of LEDs, see the Quick Start Guide (QSG).

Internet Access

For FortiGuard updates please have a stable internet access from the FortiNDR unit. Go to *System* > *FortiGuard* for updates via Internet. For offline deployments please refer to Appendix D - FortiGuard updates on page 177.

Ports

Port1 and port2 are hard-coded to be management port and sniffer port.

The following is the initial port configuration.

Port	Type	Function
Port1	10GE copper (10G or 1G autodetect)	Management port, GUI, Fabric devices files receiving, REST API, ICAP. Default IP address is `192.168.1.88` using `admin` with no password.
Port2	10GE copper (10G or 1G autodetect)	Sniffer port.
Port3 Port4	1G Copper	High availability
Port5 Port6 Port7 Port8	10G SPF+ fiber (gen3 only)	Reserve for future use*
Console	Serial port	Console serial port. 9600 baud, 8 data bits, 1 stop bit, no parity, XON/XOFF.

While the FortiGate port2 sniffer comes in 10GE copper, it also auto detects 1/10G interfaces. If the switch supports SFP+, you can use the FN-TRAN-SFP+GC transceiver.

SKU: FN-TRAN-SFP+GC

Product Name: 10GE copper SFP+ RJ45 transceiver (30m range)

Description: 10GE copper SFP+ RJ45 Fortinet transceiver (30m range) for systems with SFP+ slots.

10GE copper supports up to 100m cable distance to switch or FortiGate. Ideally the shorter the cable the better the performance, avoiding retransmission and packet loss over physical medium.

Use CAT 8 copper cable to achieve the maximum performance of up to 40Gbps for sniffer. For differences in CAT cables, see https://www.cablesandkits.com/learning-center/what-are-cat8-ethernet-cables.

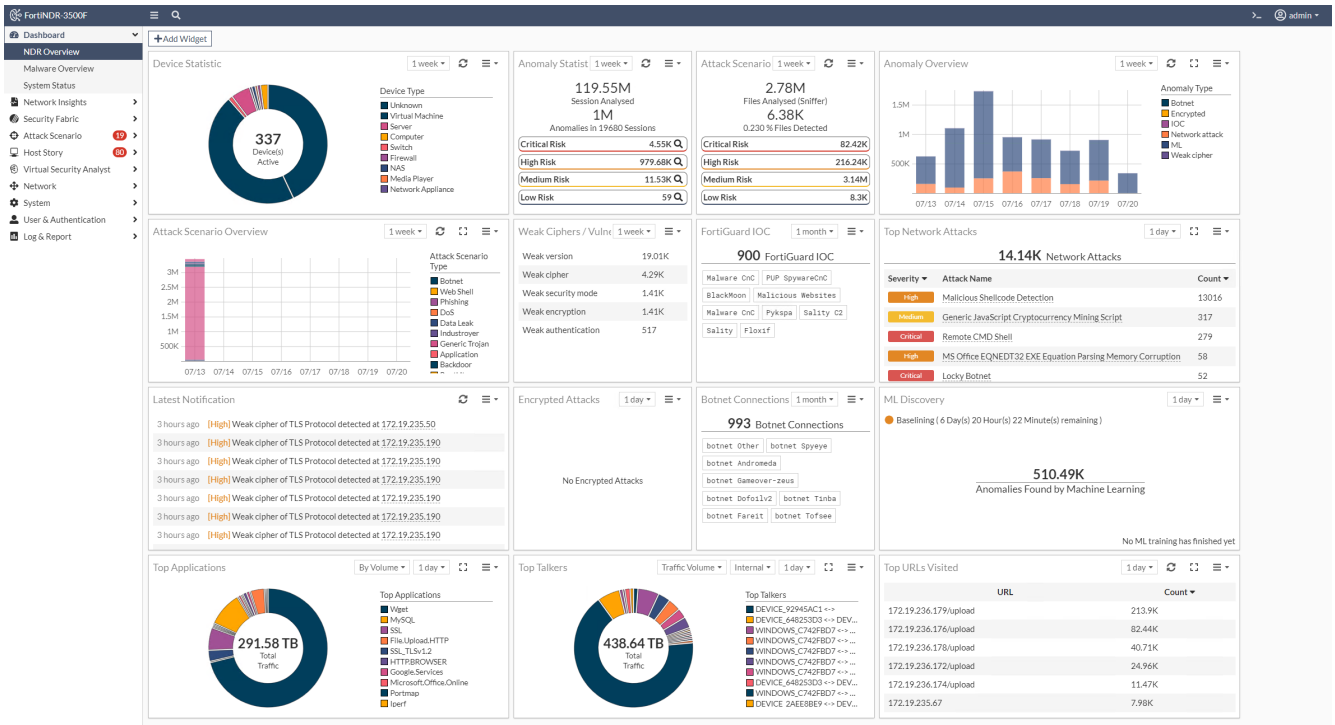
*For customers who are required to use SFP+ ports (available in gen3 hardware only) for management and capture (sniffer), pls contact local CSE for details.

Dashboard

The *Dashboard* displays the overall anomalies detected by FortiNDR as well as the system status. The Dashboard contains three views: *NDR Overview*, *Malware Overview*, and *System Status*.

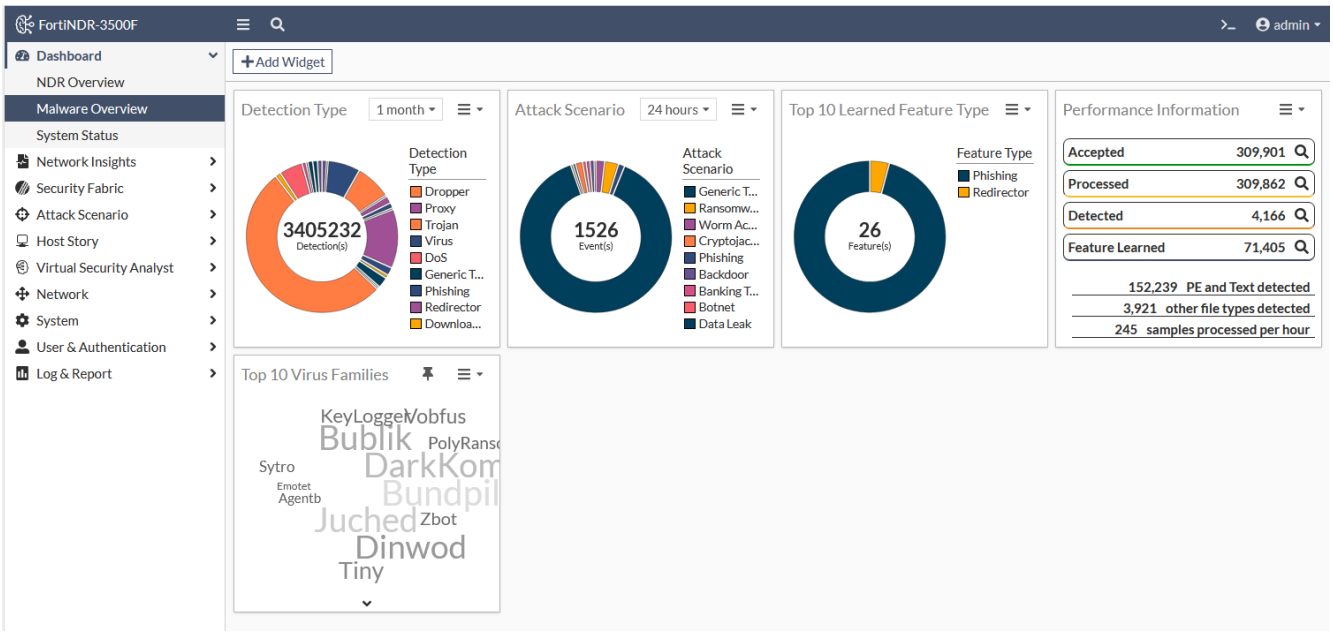
NDR Overview

The *NDR Overview* dashboard displays network detection and response statistics as charts and graphs. Each widget can be filtered with a time range of *1 day*, *1 week*, or *1 month*. When you click the *Network Insights* widgets, such as *ML Discovery* and *Botnet*, the widget expands to full screen.



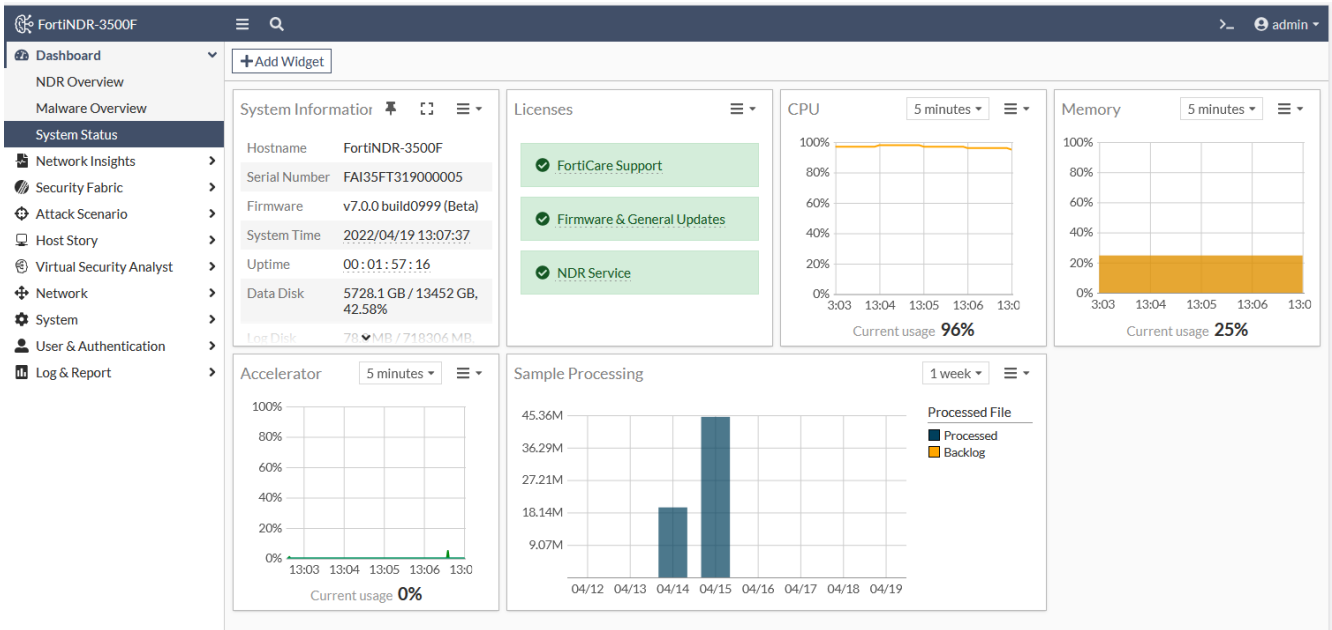
Malware Overview

The *Malware Overview* dashboard displays information about malware attacks and performance information as charts and graphs.



System Status

The *System Status* dashboard displays information about the FortiNDR device. Use this dashboard to view license information, resource usage, and the processing queue.



Custom dashboards

You can create a custom dashboard using *NDR Overview*, *Malware Overview* and *System Status* widgets.

To add a widget to a dashboard:

1. In the dashboard banner, click *Add Widget*. The *Add Dashboard Widget* window opens.
2. Click the plus sign (**+**) next to the widget name.
3. Click *OK*.

To create a custom dashboard:

1. Go to *Dashboard* and click the *Add* (+) button below the *System Status* dashboard. The *Create Custom Dashboard Widget* pane opens.
2. In the *Display Name* field, enter a name for the dashboard and click *Next*.
3. Select the widgets to add to the dashboard and click *Next*.
4. Review your selections and click *Next*. The dashboard is added to the navigation pane below *System Status*.

To delete a custom dashboard:

Click the *Actions* menu next to the dashboard name and click *Delete*.

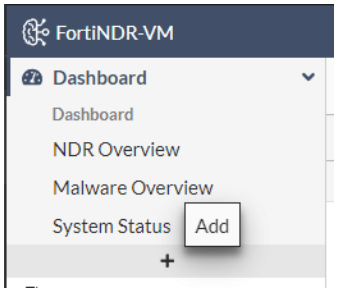
Create a custom dashboard

In a custom dashboard, users can insert their own choice of widgets.

You can create a custom dashboard using *NDR Overview*, *Malware Overview* and *System Status* widgets.

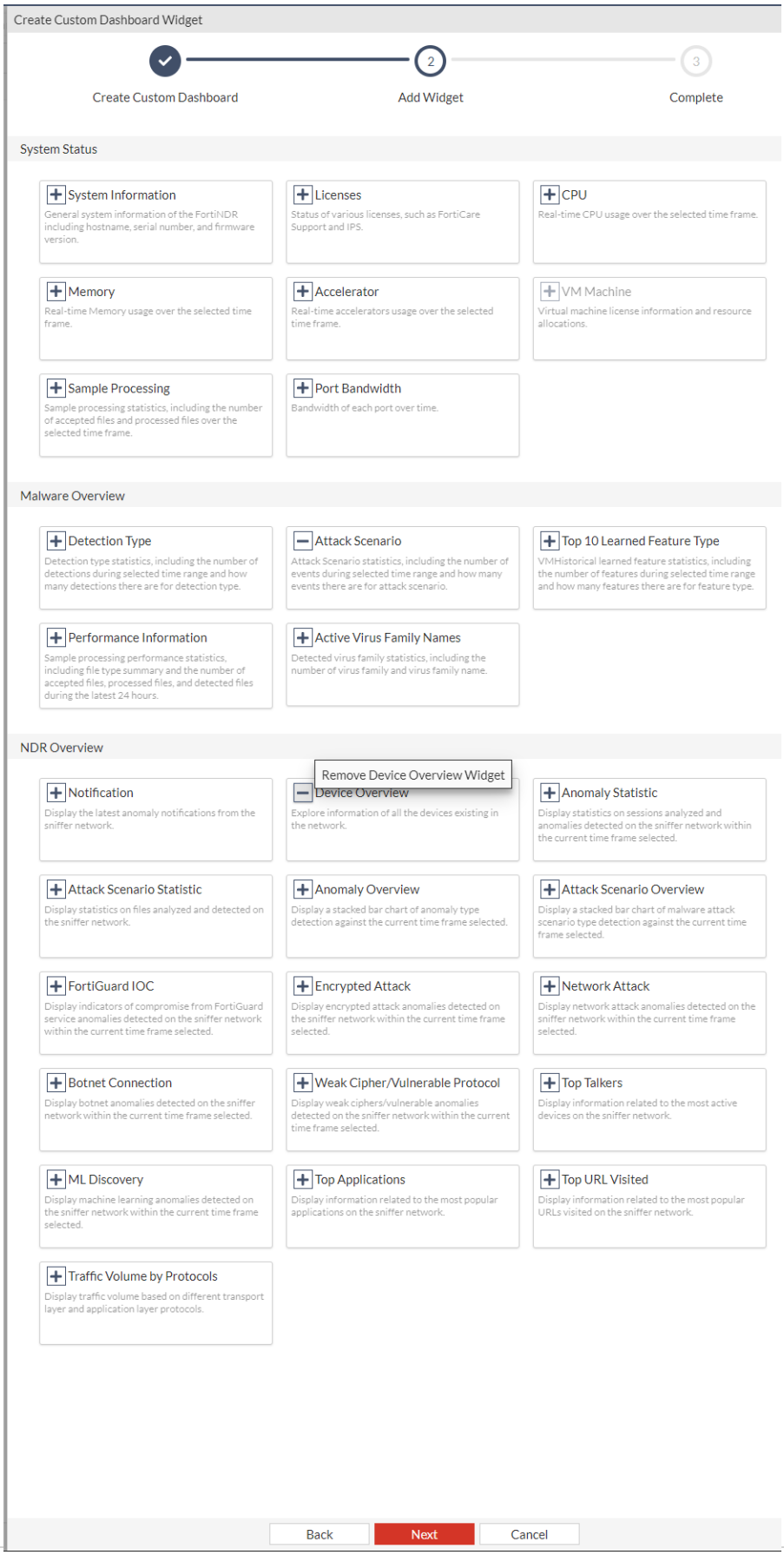
To insert a custom dashboard:

1. Go to Dashboard, and click the *Add* icon.



2. Select which widgets you want to appear on the dashboard by clicking the + icon next to the widget's name, and

click *Next*.


Create Custom Dashboard Widget
Create Custom Dashboard
2
Add Widget
3
Complete
System Status
System Information
General system information of the FortiNDR including hostname, serial number, and firmware version.
Licenses
Status of various licenses, such as FortiCare Support and IPS.
CPU
Real-time CPU usage over the selected time frame.
Memory
Real-time Memory usage over the selected time frame.
Accelerator
Real-time accelerators usage over the selected time frame.
VM Machine
Virtual machine license information and resource allocations.
Sample Processing
Sample processing statistics, including the number of accepted files and processed files over the selected time frame.
Port Bandwidth
Bandwidth of each port over time.
Malware Overview
Detection Type
Detection type statistics, including the number of detections during selected time range and how many detections there are for detection type.
Attack Scenario
Attack Scenario statistics, including the number of events during selected time range and how many events there are for attack scenario.
Top 10 Learned Feature Type
VMHistorical learned feature statistics, including the number of features during selected time range and how many features there are for feature type.
Performance Information
Sample processing performance statistics, including file type summary and the number of accepted files, processed files, and detected files during the latest 24 hours.
Active Virus Family Names
Detected virus family statistics, including the number of virus family and virus family name.
NDR Overview
Remove Device Overview Widget
Notification
Display the latest anomaly notifications from the sniffer network.
Device Overview
Explore information of all the devices existing in the network.
Anomaly Statistic
Display statistics on sessions analyzed and anomalies detected on the sniffer network within the current time frame selected.
Attack Scenario Statistic
Display statistics on files analyzed and detected on the sniffer network.
Anomaly Overview
Display a stacked bar chart of anomaly type detection against the current time frame selected.
Attack Scenario Overview
Display a stacked bar chart of malware attack scenario type detection against the current time frame selected.
FortiGuard IOC
Display indicators of compromise from FortiGuard service anomalies detected on the sniffer network within the current time frame selected.
Encrypted Attack
Display encrypted attack anomalies detected on the sniffer network within the current time frame selected.
Network Attack
Display network attack anomalies detected on the sniffer network within the current time frame selected.
Botnet Connection
Display botnet anomalies detected on the sniffer network within the current time frame selected.
Weak Cipher/Vulnerable Protocol
Display weak ciphers/vulnerable anomalies detected on the sniffer network within the current time frame selected.
Top Talkers
Display information related to the most active devices on the sniffer network.
ML Discovery
Display machine learning anomalies detected on the sniffer network within the current time frame selected.
Top Applications
Display information related to the most popular applications on the sniffer network.
Top URL Visited
Display information related to the most popular URLs visited on the sniffer network.
Traffic Volume by Protocols
Display traffic volume based on different transport layer and application layer protocols.
Back
Next
Cancel

Network Insights

Network Insights monitors display information about NDR detections. The charts in *Network Insights* can display a maximum of 30,000 insights. Detections are organized by category:

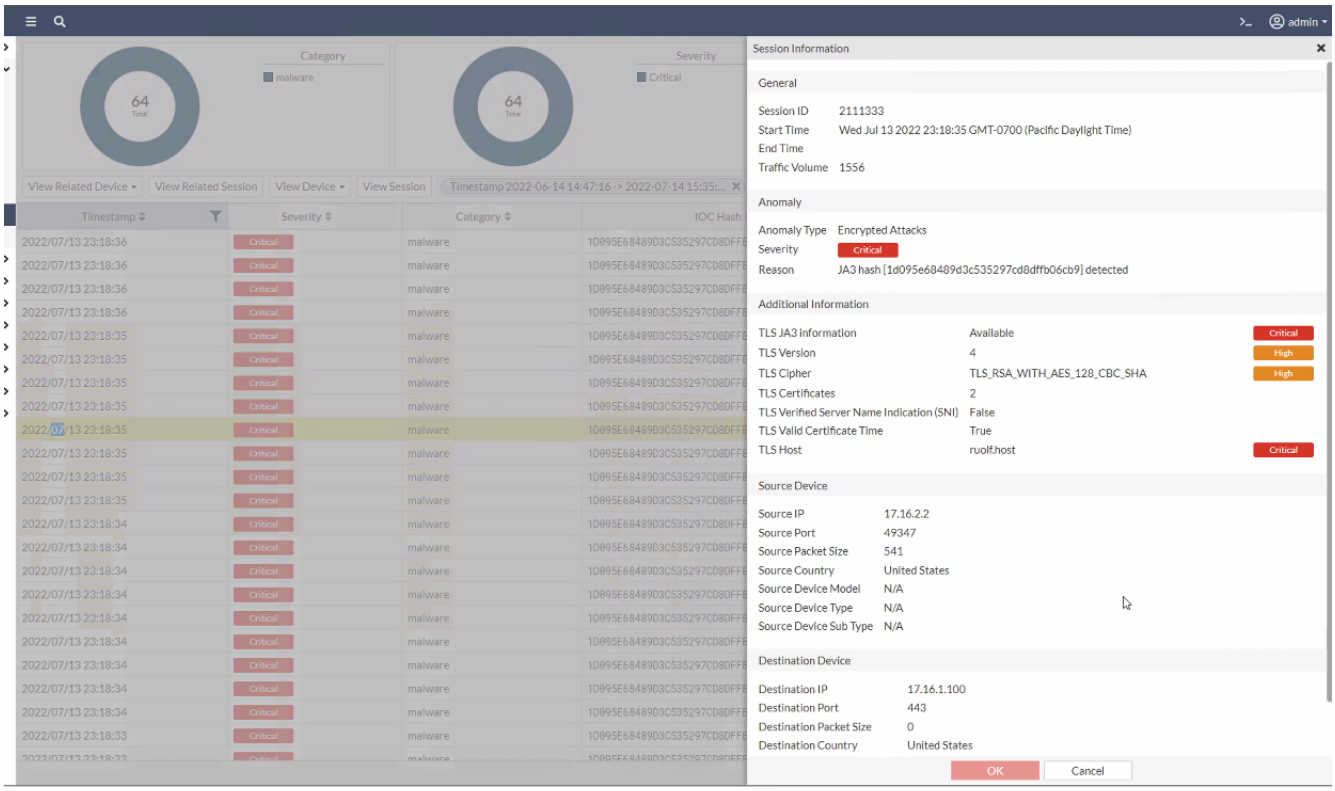
- Device Inventory
- Botnet
- FortiGuard IOC
- Network Attacks
- Weak/Vulnerable Communication
- Encrypted Attack
- ML Discovery

Double-click an entry in the monitor to view *Additional Information* in the *Session Information* pane. The *Additional Information* section contains useful information related to the attack. There could be multiple reasons for each session ID to be considered anomalies.

- For *Botnet* type anomalies, the *Additional Information* section shows *DNS Hostname*, *DNS OPCODE*, *DNS RETCODE*.
- For *Network Attack*, *Weak/Vulnerable Communication*, and *Encrypted Attack* types, the *Additional Information* section shows the reason why the session was flagged by Intrusion detection.

The reasons may vary depending on the severity levels. The Anomaly severity level is chosen by the highest level.

The image below shows the *Additional Information* in the *Encrypted Attack* anomaly. The reason for this anomaly is the JA3 hash. FortiNDR utilizes both JA3 client and server SSL fingerprints in detection, reducing the number of false positives.



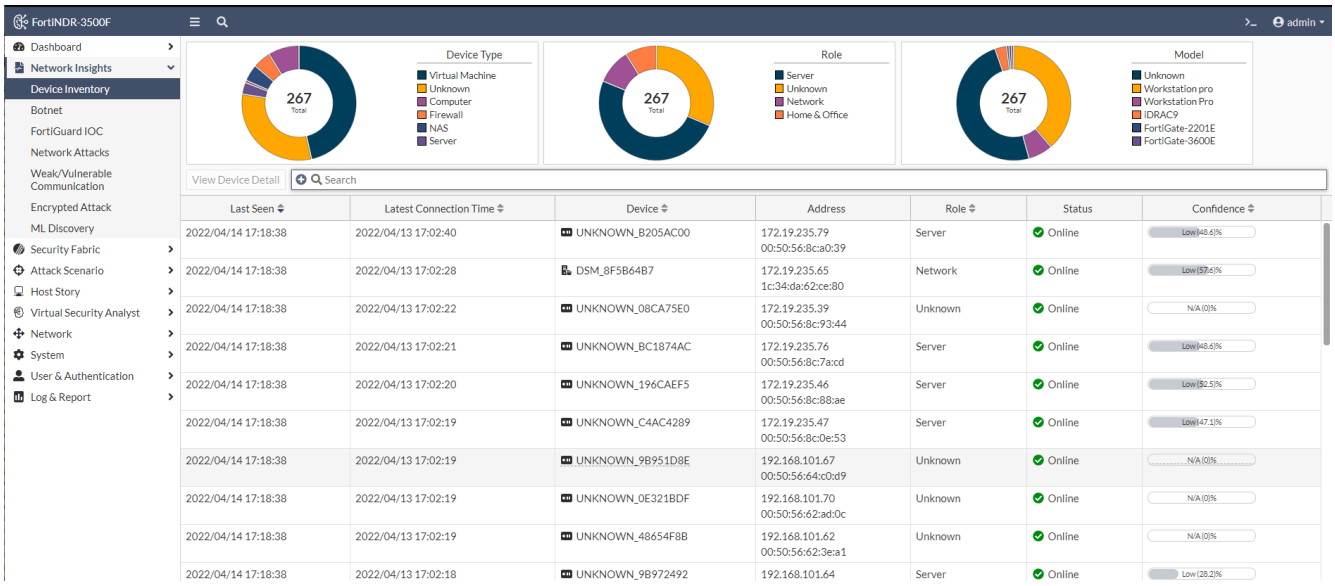
Device Inventory

The *Device Inventory* page displays the discovered devices. The *Device* and *Role* columns are dependent on IOT lookup service for information such as OS, device type etc.

The priority of devices inventory identifier is organised by the following priority from highest to lowest:

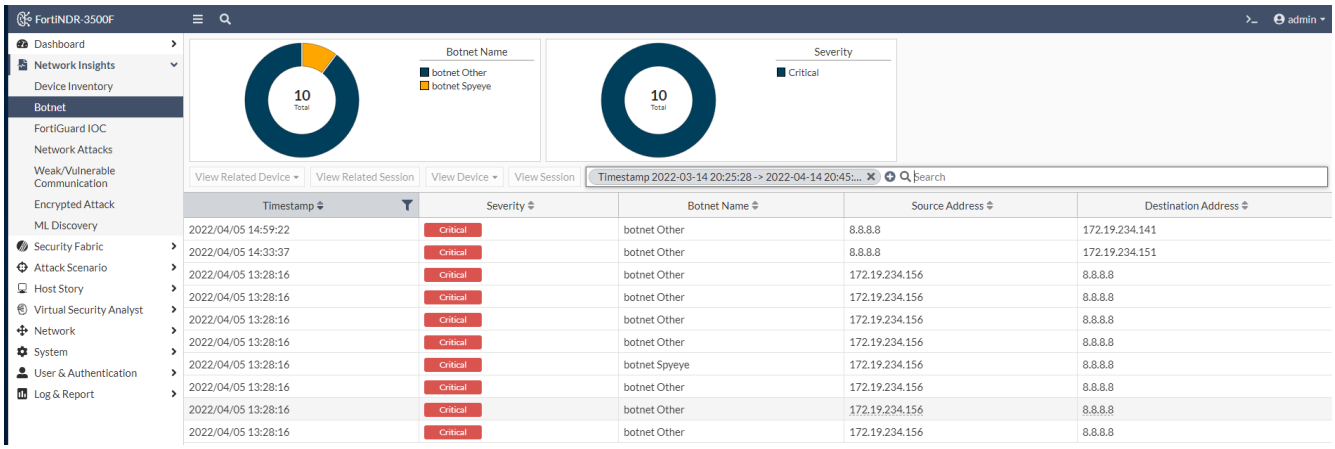
1. User defined (for example, finance server).
2. AD Device enrichment (hostname from AD, if configured).
3. System generated (OS_hash of the mac address).

The device name in the *Device* column is determined by *OS_hash* of the mac address *Status* (*online/offline*). If FortiNDR does not see a session from a device within 60 seconds, the status will be *offline*.



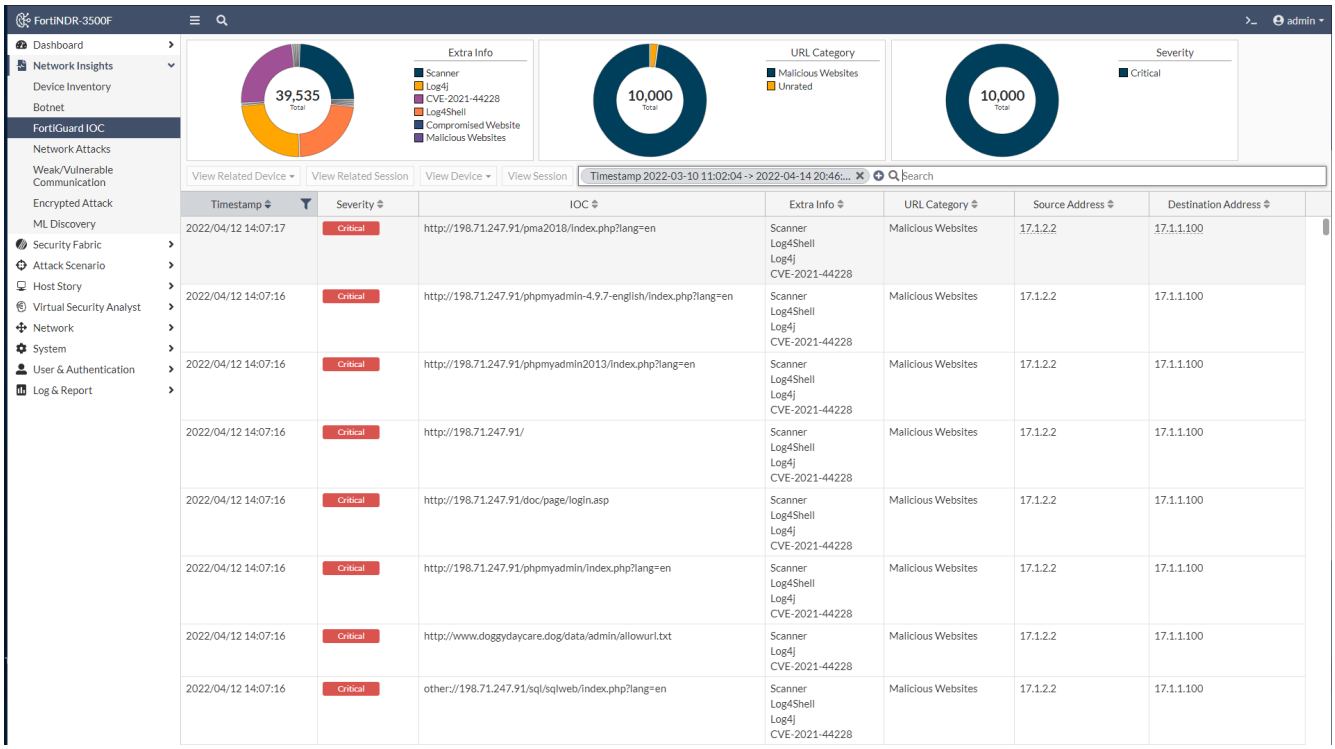
Botnet

Botnet displays the botnet traffic detections. If there is a known Botnet name, it will be displayed.



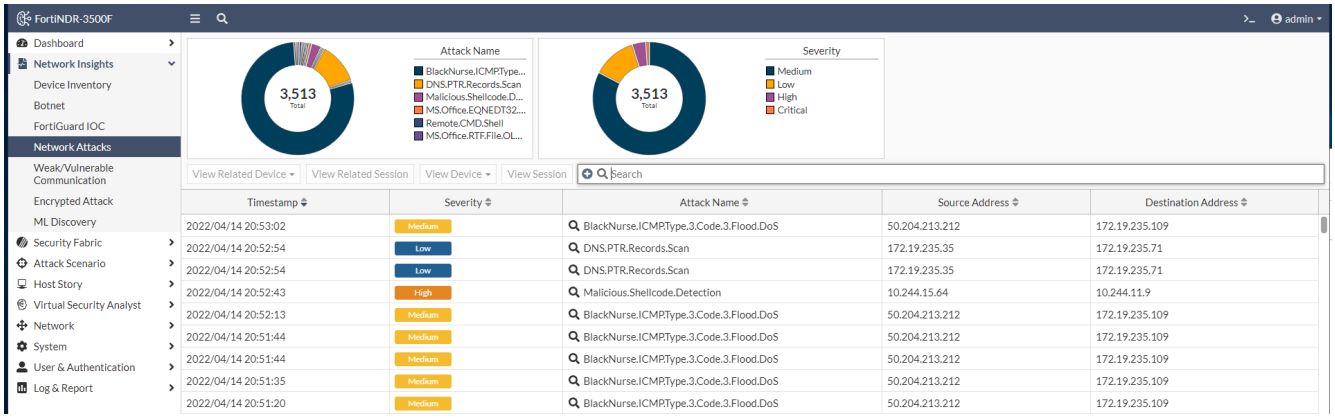
FortiGuard IOC

FortiGuard IOC detections are suspicious URLs and IPs that are flagged by FortiGuard. This anomaly discovery depends on FortiNDR look up in the FortiGuard IOC service. Apart from URL category (e.g. malicious websites), you will also see an *extra info* column for any campaign name involved (e.g. Solarwind, Locky Ransomware).



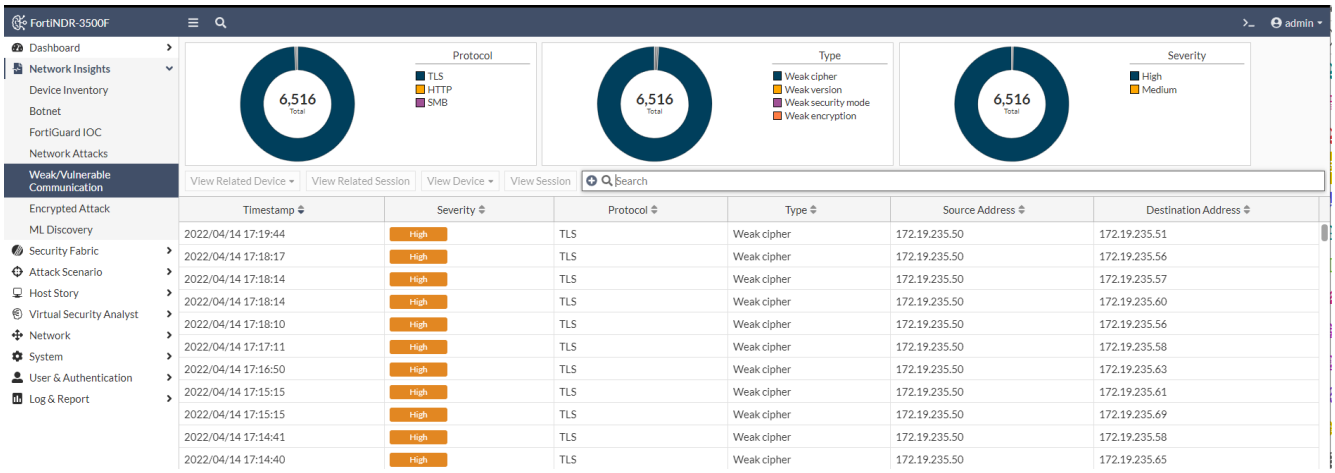
Network Attacks

Network Attacks are known attacks detected by the Network Intrusion Protection Database.



Weak/Vulnerable Communication

The *Weak/Vulnerable Communication* page displays the list of weak or vulnerable communication detected on port2. For example, a weak cipher used by an older version of SSL.



Weak/Vulnerable Communication types

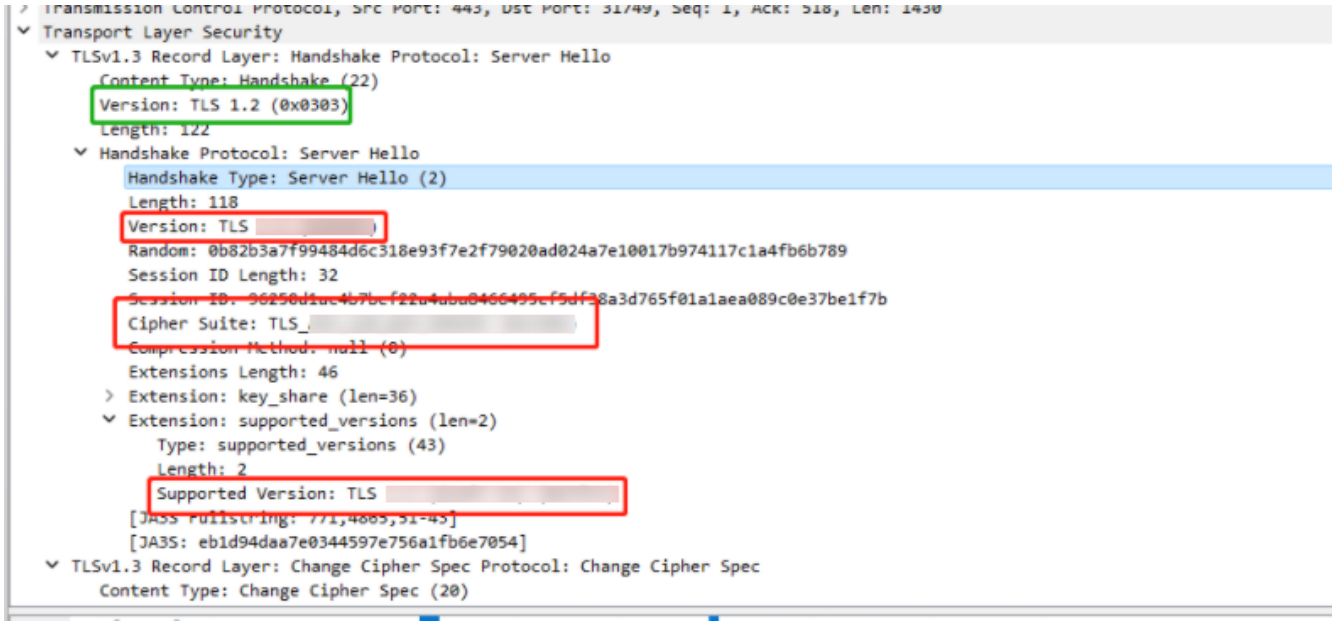
The following table provides a definition for each of the weak/vulnerable communication types:

Communication type	Description
Weak record version	Weak TLS record layer version.
Weak version	Weak TLS handshake version.
Weak support version	Weak TLS handshake extension supported version.
Weak cipher	Weak TLS handshake cipher suite.
Weak security mode	SMB protocol uses level security mode.
Weak extended security	SMB protocol uses outdated extended security negotiation option.
Weak dialect	SMB uses outdated dialect version.
Weak encryption	SMB or SSH uses risky encryption algorithm. For example, SMB protocol with encryption disabled.
Weak authentication	Email protocols are using risky authentication methods. For example, POP3 uses authentication cram-md5, Postgres uses MD5 password as authentication type.
Weak server	HTTP or RTSP server version is outdated.
Weak method	HTTP, SIP or RTSP protocol uses weak request method. For example, HTTP protocol uses DELETE as request method.
Weak banner	Weak or outdated email server version. For example, Outdated Cyrus IMAP server
Weak encrypt algo server client	Weak encryption option is used in SSH, such as rc4, rc3, rc2.
Weak capability	IMAP or POP3 capability command uses option AUTH=PLAIN.

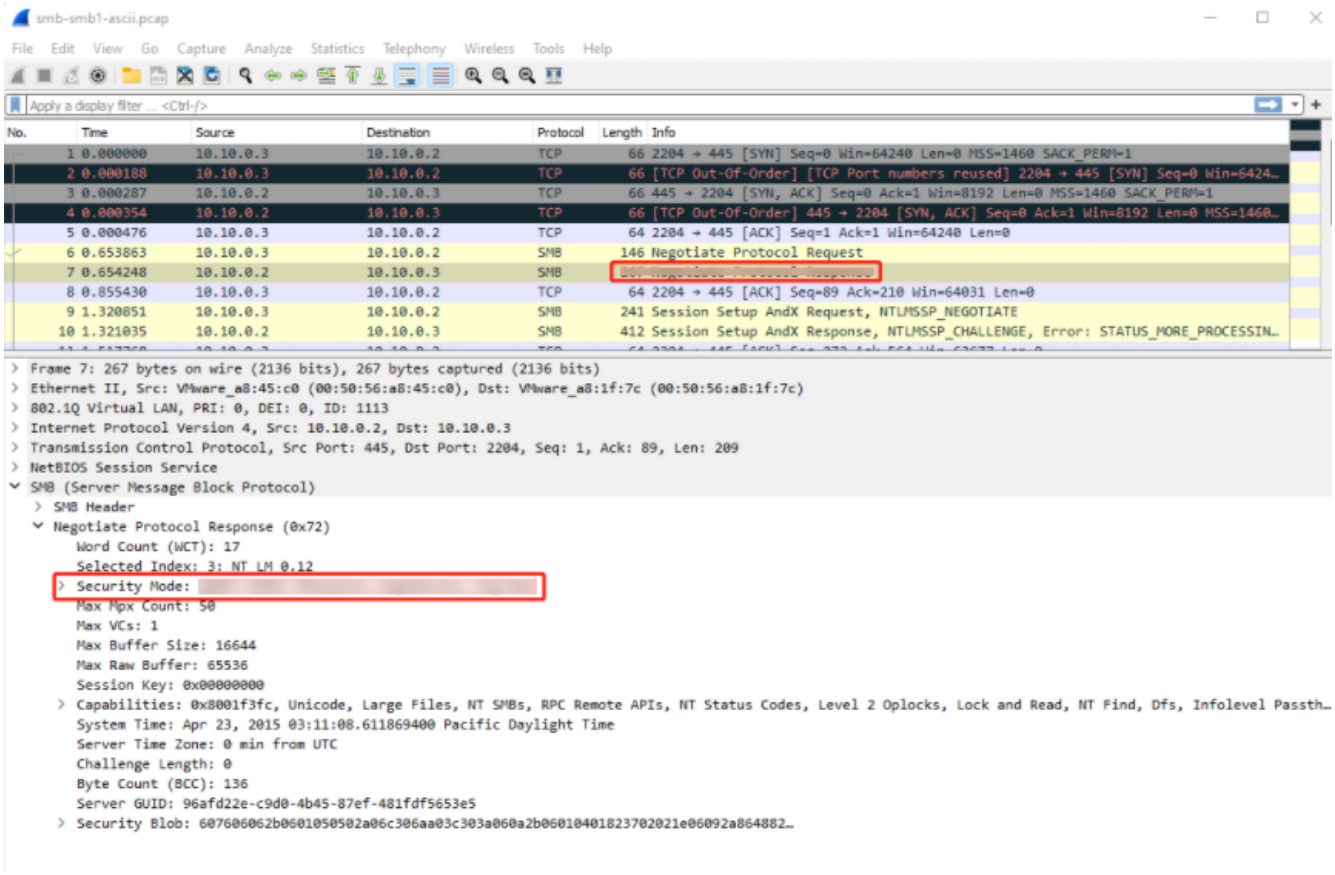
Communication type	Description
Weak security	SMB protocol uses low level security mode.
Weak encrypt method	RDP protocol uses low level encryption methods such as ENCRYPTION_METHOD_40BIT.
Weak encrypt level	RDP protocol uses low encryption level such as ENCRYPTION_LEVEL_NONE
Weak msg flags	SNMP protocol uses risky flags such as 0x00-02, 0x04-06 and 0x08-ff.
Weak server version	MYSQL, TDS, Posgres or SIP server version is outdated.
Weak auth algo	POP3, SMTP or IMAP authentication method option is too risky. For example, POP3 uses PLAIN authentication option.
Weak protocol version	MYSQL protocol version outdated.
Weak encrypt	TDS encryption option is disabled.
Weak fedauth	TDS protocol disables `FedAuthRequired` option.

Examples

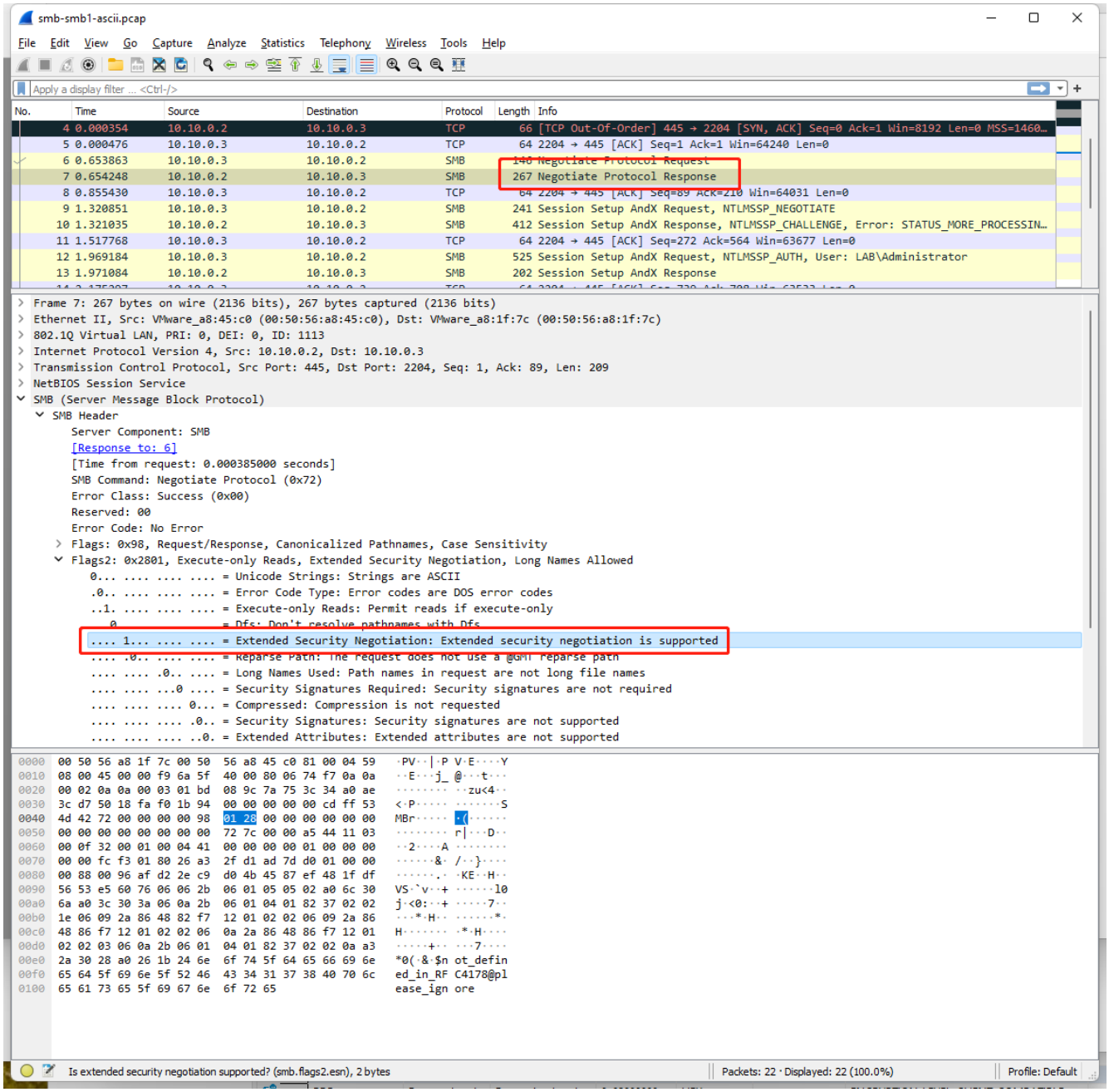
Wireshark pcap



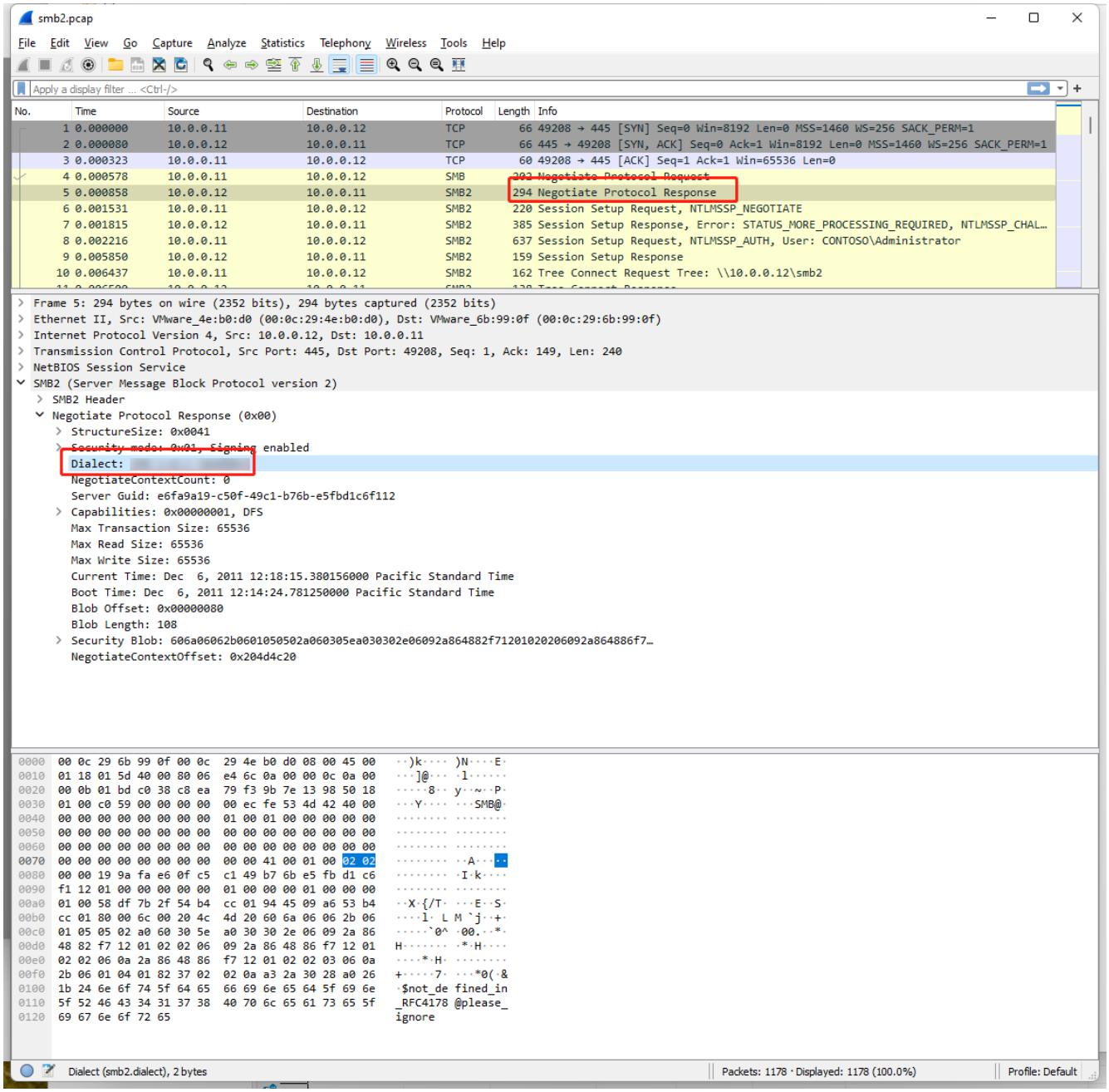
Weak security mode



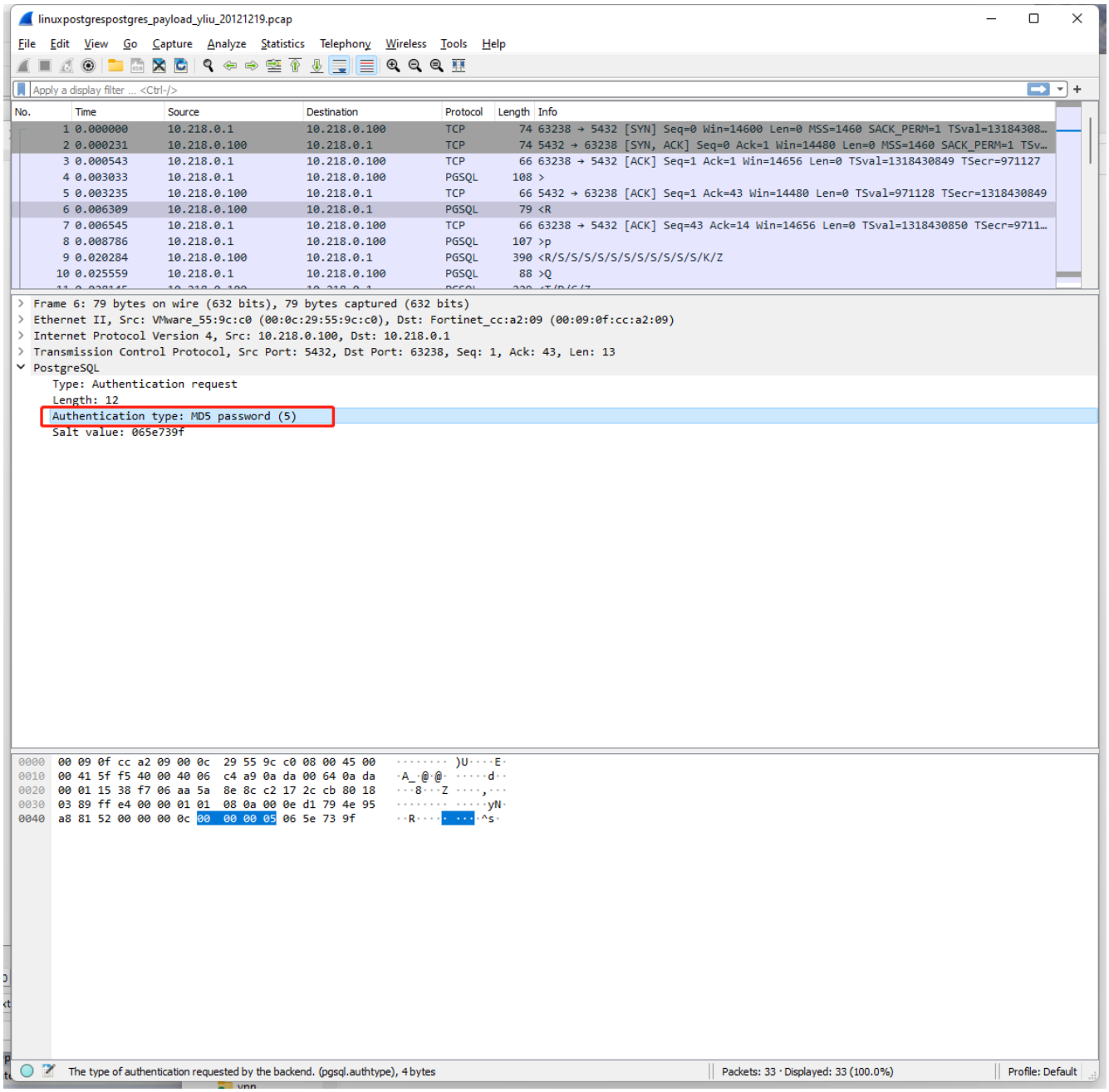
Weak extended security



Weak dialect

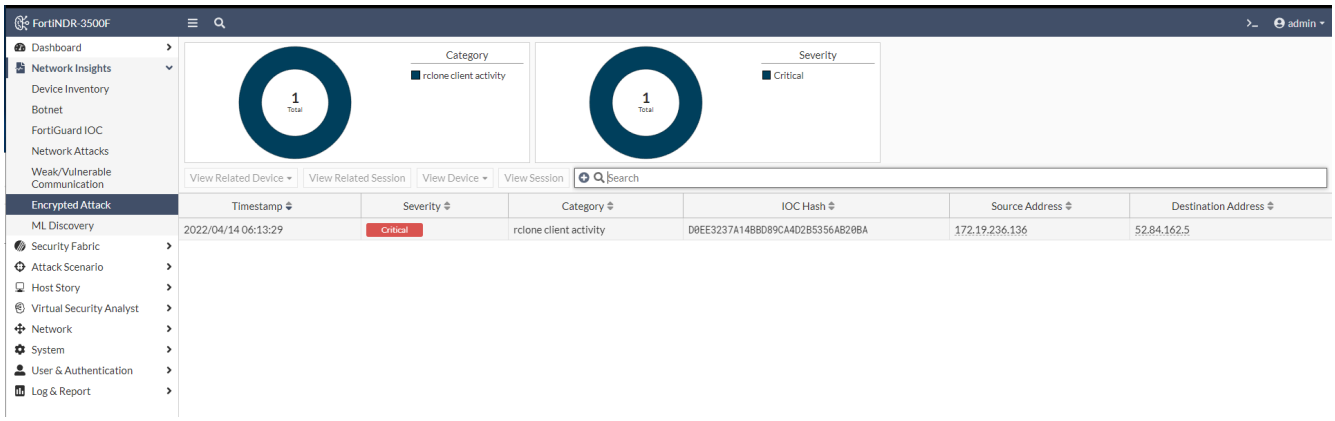


Weak authentication



Encrypted Attack

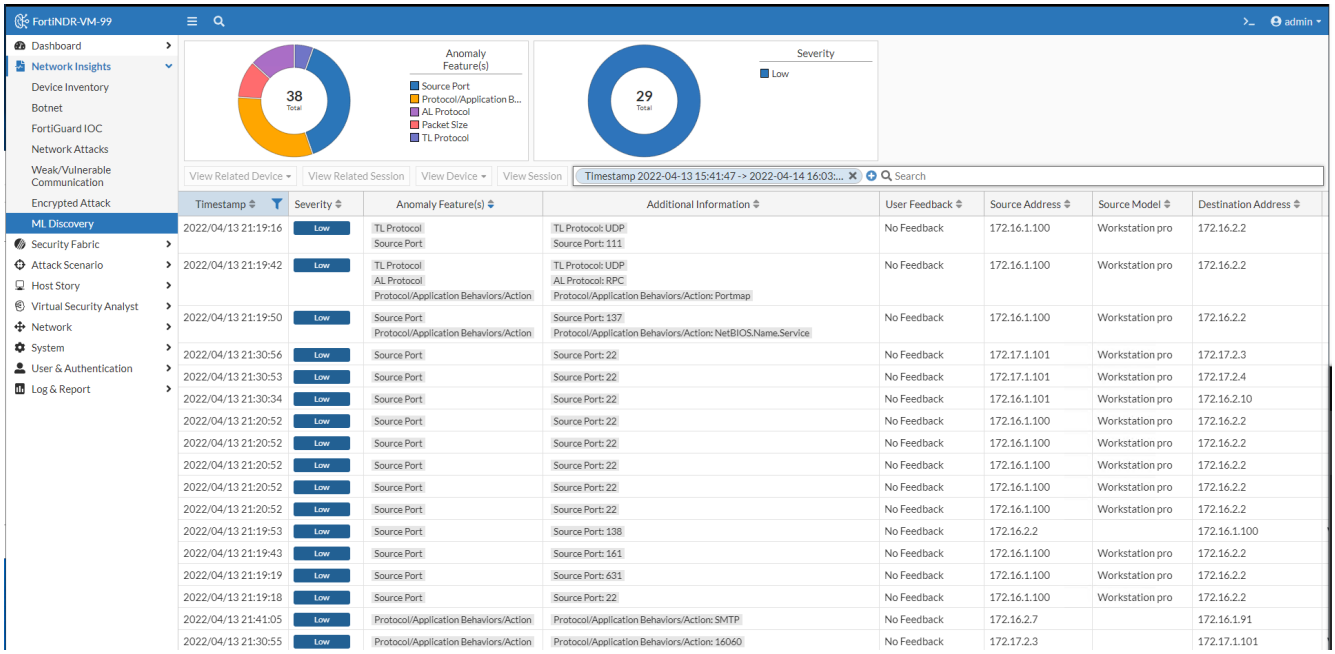
Encrypted attacks are detected by analyzing JA3 hashes in TLS transactions. FortiNDR will utilize both JA3 client and server SSL fingerprints in detection, resulting in fewer false positive detections.



ML Discovery

The *ML Discovery* page displays a list of anomalies detected by Machine Learning configuration. Each row is based on a session. The configuration and baselining of ML Discovery is located under *Virtual Security Analyst > ML configuration*. ML discovery is switched ON by default.

- The *Anomaly Features* column displays the feature or feature combinations that caused the anomaly.
- The *Additional Information* column provides a glance of the abnormal feature value(s).
- The *Use Feedback* column is where you can enter positive or negative feedback to the detection.



Double-click an entry to view the *Session Information* pane. Right-click an entry to:

- *View Related Device*: The related source and destination devices.
- *View Related Session*: All the sessions for the source device.

- *View Device*: The source and the destination device.
- *View Session*: The reason why the session is considered to be an anomaly by ML.

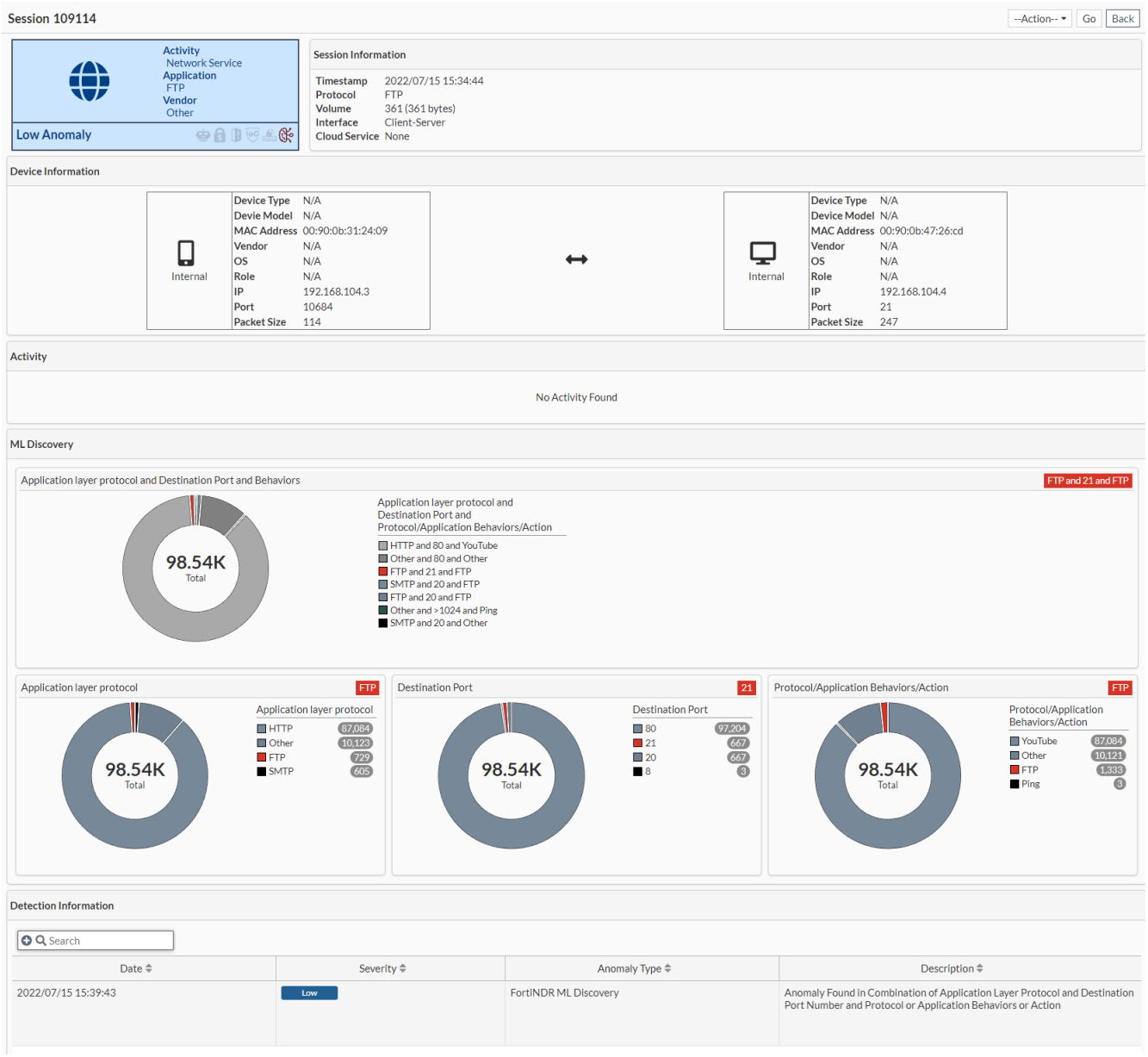
Example:

The image below shows a ML anomaly detection triggered by 3 features:

- *Application layer protocol*: FTP
- *Destination Port*: 21
- *Protocol/Application Behaviors/Action*: FTP

The *Application layer protocol and Destination Port and Behaviors* pie chart shows the distribution of the three features. The anomaly in the example is triggered because *FTP-21-FTP* has deviated from the baseline. In other words, the FTP connection from *192.168.104.3* to *192.168.104.4* has never been seen in the baseline before.

The *Application layer protocol*, *Destination Port* and *Protocol/Application Behaviors/Action* charts show the distribution for each feature. The distribution information is a snapshot based on the source device at the moment of the detection. It is normal for a feature highlighted in red not to have the lowest count in the chart. This is because the highlighted feature may occur multiple times suddenly within a very short period when being detected.



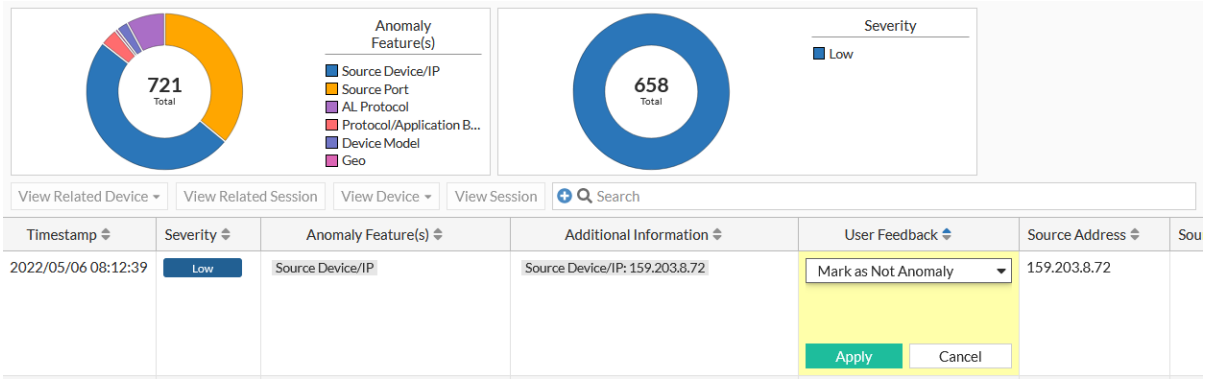
The *Application layer protocol and Destination Port and Behaviors* chart is not displayed when the ML anomaly detects a new Source IP or Destination IP that has never been seen in the baseline.

Add feedback to a ML Discovery

The *User Feedback* column allows you to provide feedback for Machine Learning discoveries to correct false positives.

To add feedback to ML Discovery:

1. Go to *Network Insights* > *ML Discovery* and select a session in the table.
2. Hover over the *User Feedback* column until the *Edit* icon appears and click it.



3. From the *Feedback* dropdown, select one of the following options.

Option	Description
Mark as unset	This is the default status for any ML anomalies detected. Select this option to unset your feedback. Note that this has the same effect as "Mark as Anomaly".
Mark as Not Anomaly	Select this option to exclude the same detection(s) in the future. This typically takes 5 - 10 minutes depending on the network traffic. Note that this option does not retrain the ML Database; there are other CLIs to retrain the database.
Mark as Anomaly	Select this option to mark an entry as an anomaly. This option can be used to undo the "Mark as Not Anomaly" option. Note that this option does not affect the baseline training.

When multiple sessions of the same Source Address share the same value in the Anomaly Feature(s) column, you will only need to add feedback once to apply the feedback to all of the sessions.

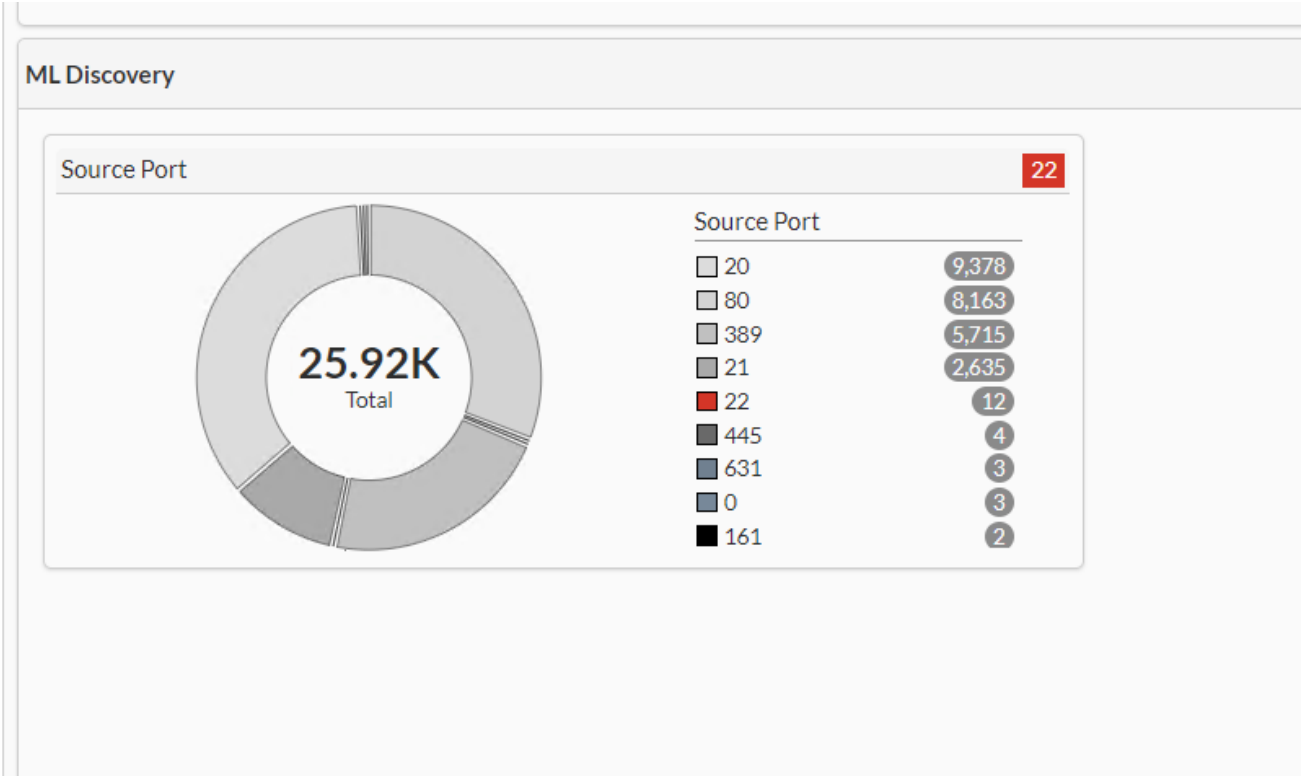
4. Click *Apply*.
The following image is an example of multiple ML discoveries with the same value in the *Anomaly Feature(s)* column. In this scenario, if you add feedback to the first session as Not Anomaly, the other sessions remain as Anomaly.

Timestamp	Severity	Anomaly Feature(s)	Source Address	Source Model	Destination Address	Destination Model	Session ID	Current Feedback Status	Additional Information
2023/02/28 11:15:13	Low	Source IP	192.168.2.10	Virtual Machine	192.168.2.255	N/A	20510	Marked as Not Anomaly	Source IP: 192.168.2.10
2023/02/28 11:03:13	Low	Source IP	192.168.2.10	Virtual Machine	192.168.2.255	N/A	20466	Marked as Not Anomaly	Source IP: 192.168.2.10
2023/02/28 10:51:12	Low	Source IP	192.168.2.10	Virtual Machine	192.168.2.255	N/A	20422	Marked as Not Anomaly	Source IP: 192.168.2.10
2023/02/28 10:39:12	Low	Source IP	192.168.2.10	Virtual Machine	192.168.2.255	N/A	20378	Marked as Not Anomaly	Source IP: 192.168.2.10

View Session

To drill-down to the session details, right-click an entry to open *View Session*.

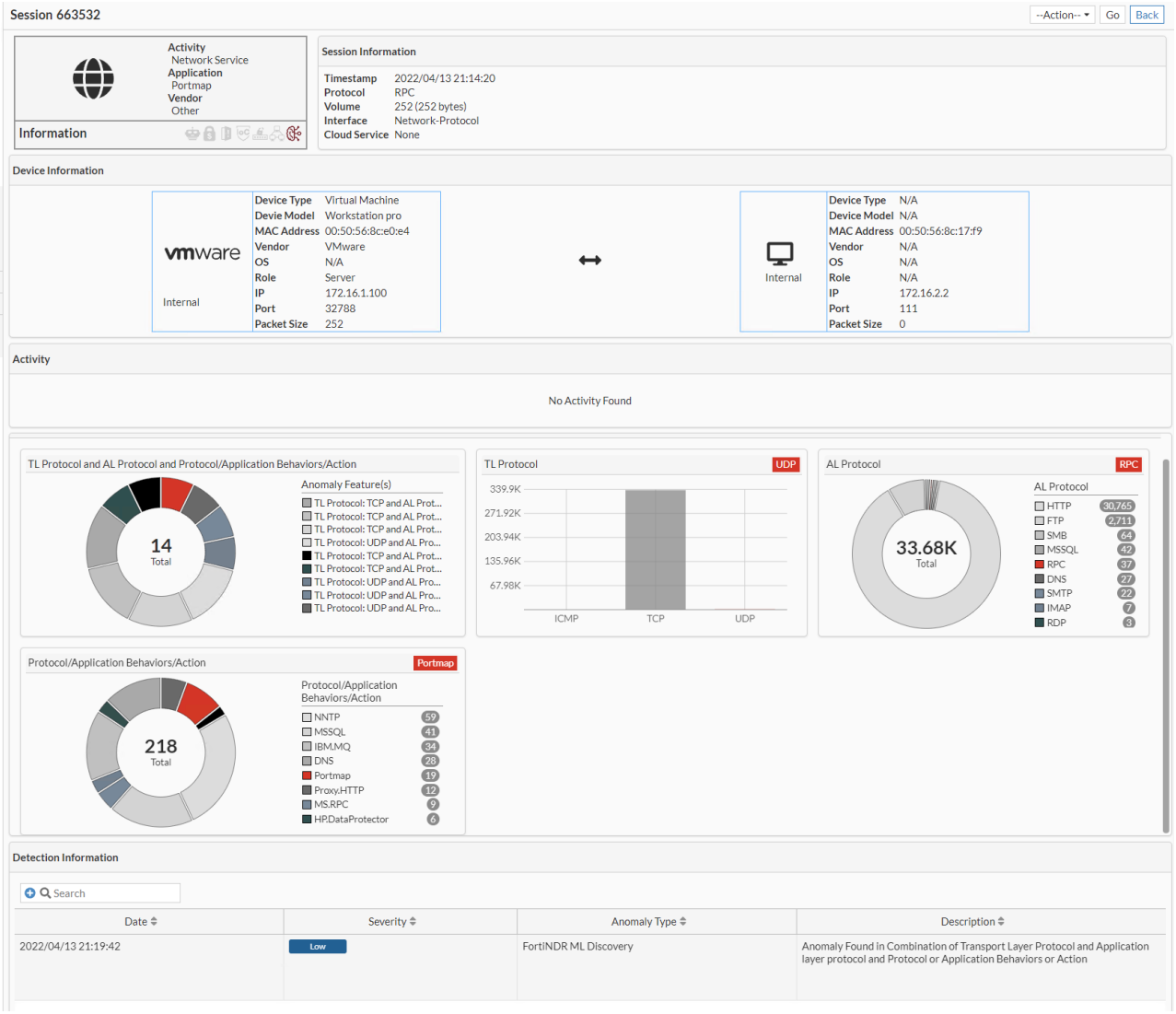
In *ML Discovery* the session shows the distribution of the feature that caused the anomaly. In the image below, the session was flagged because it was trying to use port 22, which is the SSH connection.



If the anomaly is caused by:

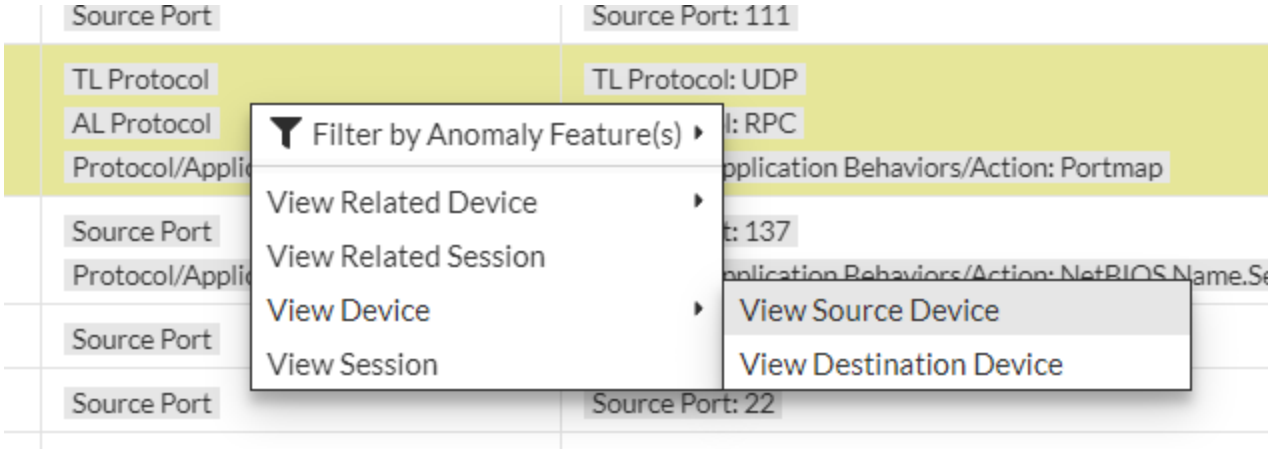
- A new IP joining the network, the distribution graph is not displayed. The new IP address is displayed instead.
- A combination of features the session displays the distribution of the combination as well as the individual distributions. For example, the following anomaly is caused by the combination of *Transport Layer Protocol*,

Application Protocol and *Protocol/Application Behaviors/Action*.

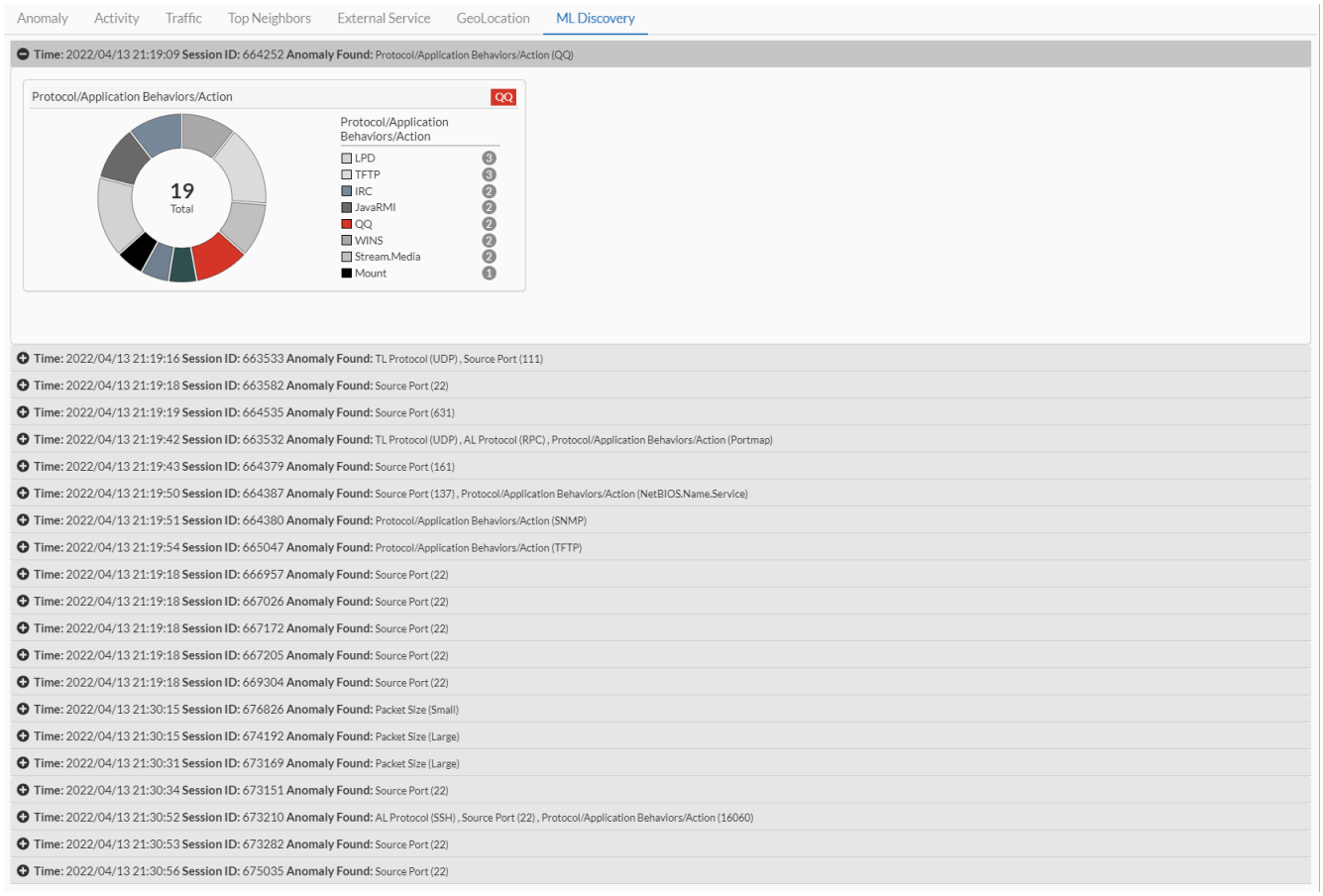


View Source Device and View Destination Device

You can view Source and Destination Device by right-clicking an entry and clicking in *View Device* > *View Source Device* or *View Destination Device*.



To view this device's ML anomalies, click the *ML Discovery* tab. The following image shows a series of ML anomalies found on the same device.



Security Fabric

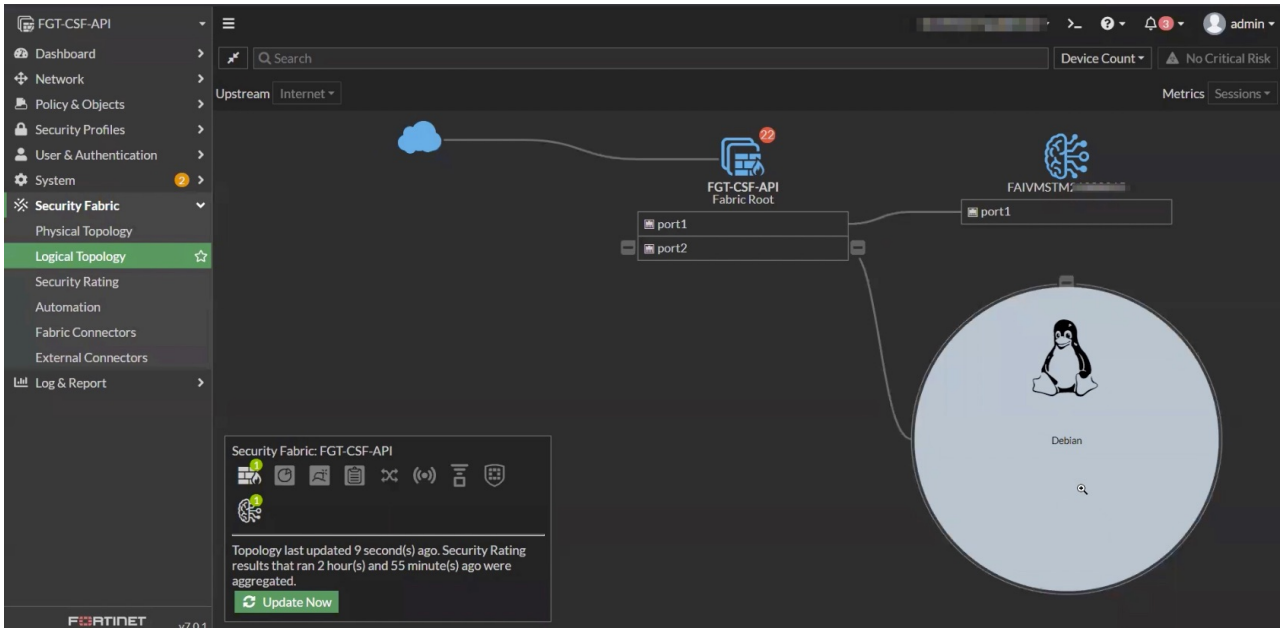
FortiGate inline blocking (FOS 7.0.1 and higher)

You can configure FortiGate to integrate with FortiNDR using inline blocking. Changes in FortiOS allow the AV profile to configure inline blocking by sending files to FortiNDR for rapid inspection and verdict. FortiGate temporarily holds the user session for FortiNDR to return a clean or malicious verdict, and then it decides if the user can download the file.

This provides more security than integrated moded because you can download the file first while the file is sent to FortiNDR (and FortiSandbox) for inspection.

To configure FortiGate AV profile inline blocking:

1. Configure FortiGate and FortiNDR Security Fabric pairing using the Security Fabric Connector. For details, see Fabric Connectors on page 59.
   This is needed for authentication between the two devices before file submission begins.
2. When pairing is complete, verify that FortiNDR appears in the FortiGate topology with the FortiNDR icon in the legend.



3. Configure the FortiGate AV profile using the following CLI commands.

```
Config system fortindr
    Set status enable
End

Config antivirus profile
    edit fai                << profile name
        Set feature-set proxy
        Config http         << or another protocol such as FTP, SMTP, IMCP, CIFS, etc.
```

```
        Set fortindr block  << or monitor
    End
Next
End
```

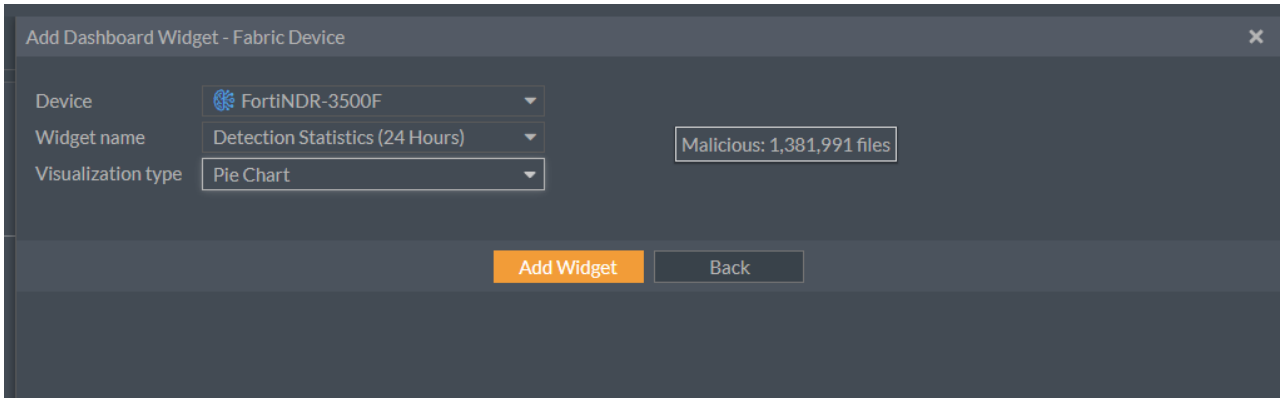
4. Apply this AV profile in the ForitOS NGFW policy.
   Both FortiGate Antivirus logs and FortiNDR logs and reports show corresponding log entries.

Tips for using FortiNDR inline blocking

- Similar to the FortiGate AV profile, a browser replacement message if as displayed if a virus is found.
  In FortiOS, the message is called FortiNDR block page, and is a customizable HTML page.

- For encrypted traffic such as HTTPS, the SSL profile must be configured on FortiGate to extract files in encrypted protocols.
- The maximum file size is determined by both FortiGate and FortiNDR. FortiNDR supports a default maximum file size of 200MB. In FortiNDR the maximum file size can be adjusted with the following CLI command:
  ```
  execute file-size-threshold
  ```
- If there are network connectivity issues that causes a timeout between the connections, FortiGate and user download operations resume after connectivity is restored.
- When FortiNDR is connected to the Security Fabric, you can configure a malware widget in the FortiOS Dashboard.

  Go to *Dashboard* > *Status* > *Add Widget* > *Fabric Device* to display the detected attack scenarios.



FortiNDR inline inspection with other AV inspection methods

The following inspection logic applies when FortiNDRinline inspection is enabled simultaneously with other AV inspection methods. The AV engine inspection and its verdict always takes precedence because of performance. The actual behavior depends on which inspected protocol is used.

HTTP, FTP, SSH, and CIFS protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
   - FortiNDR inline inspection occurs simultaneously.
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
   - FortiNDR inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
   - FortiNDR inline inspection occurs simultaneously.

If any AV inspection method returns an infected verdict, the FortiNDR inspection is aborted.

POP3, IMAP, SMTP, NNTP, and MAPI protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
   - FortiNDR inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
   - FortiNDR inline inspection occurs simultaneously.

In an AV profile, use `set fortindr-error-action {log-only | block | ignore}` to configure the action to take if FortiNDR encounters an error.

Accepted file types

The following file types are sent to FortiNDR for inline inspection:

7Z	HTML	RTF
ARJ	JS	TAR
BZIP	LZH	VBA
BZIP2	LZW	VBS
CAB	MS Office documents (XML and non-XML)	WinPE (EXE)
ELF	PDF	XZ
GZIP	RAR	ZIP

FortiGate integration (integrated mode with FOS 5.6 and higher)

You can send files to FortiNDR using FortiGate 5.6 and higher.

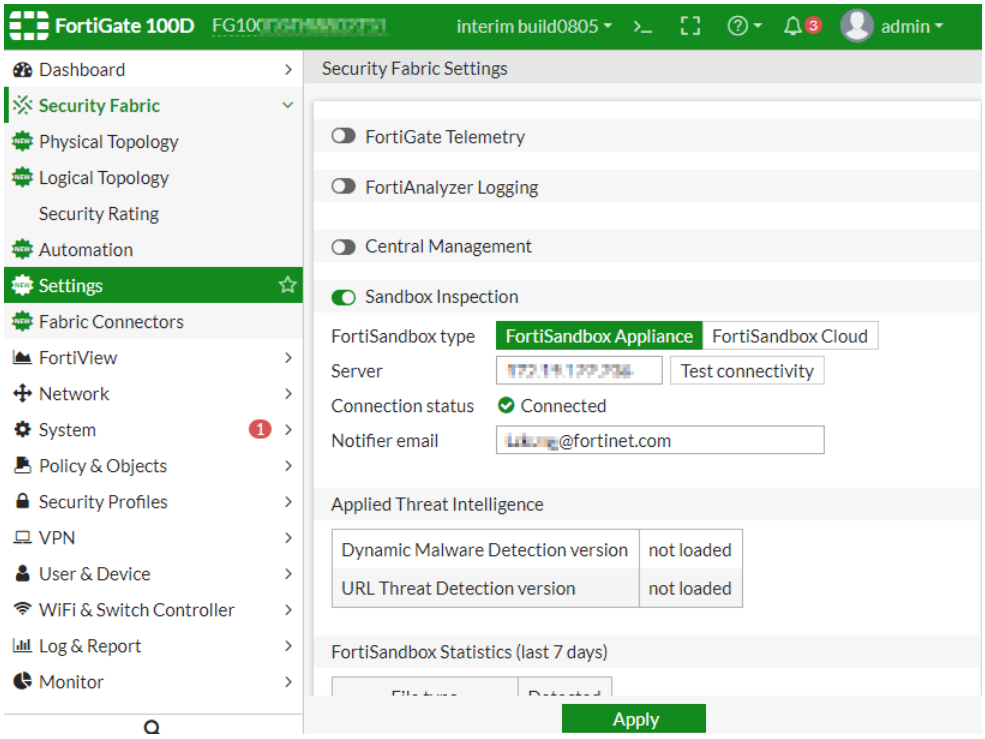
FortiGate cannot receive files from both FortiSandbox and FortiNDR simultaneously.If your FortiGate has FortiSandbox configured, consider using another mode.

FortiNDR uses the same OFTP (Optimized Fabric Transfer Protocol) over SSL (encrypted) from FortiGate to FortiSandbox. If you are not using FortiSandbox, you can use FortiGate's *Sandbox Inspection* to send files to FortiNDR.

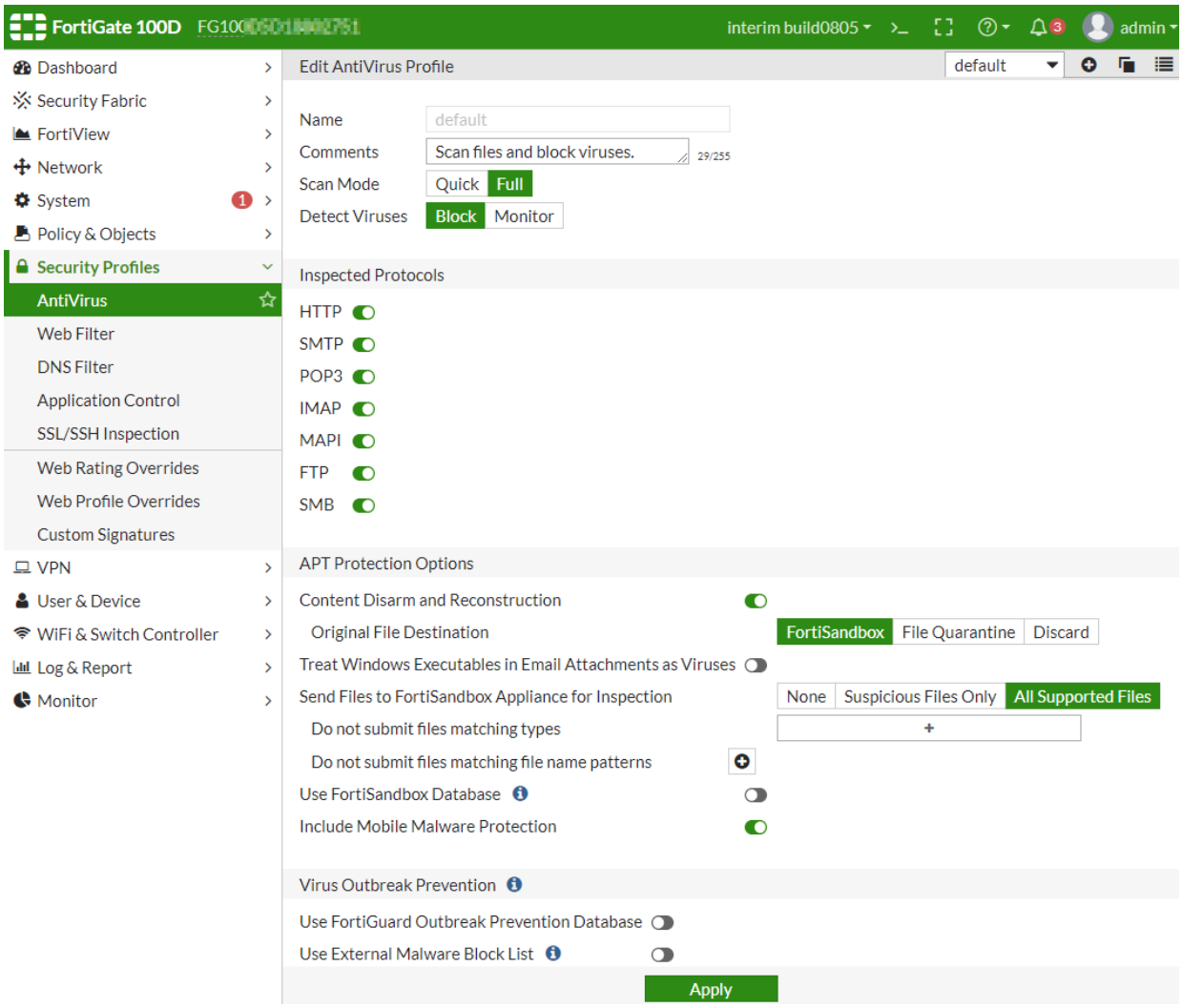
For information on configuring FortiGate, see the FortiGate documentation in the Fortinet Document Library.

To send files from FortiGate to FortiNDR:

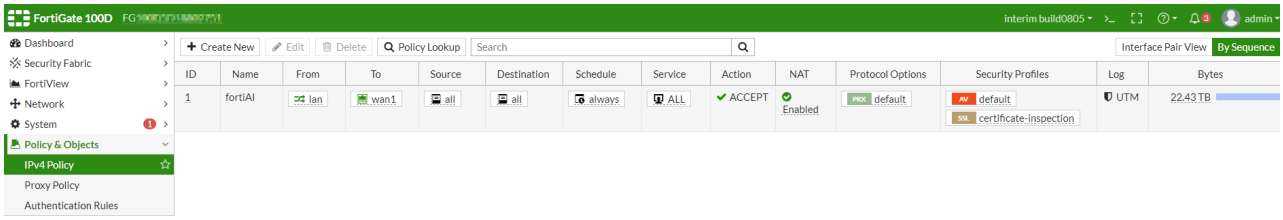
1. Set up the IP address on FortiGate.



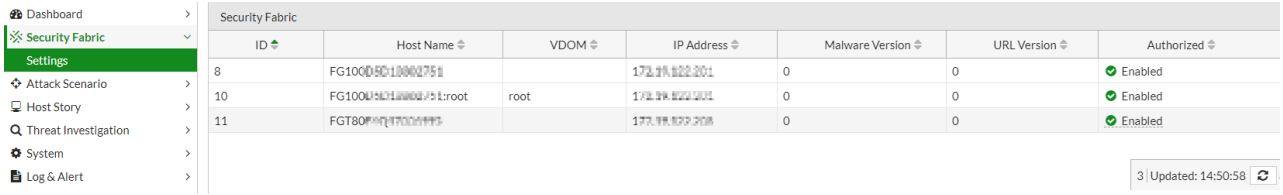
2. Configure an AV profile to send files to FortiNDR.



3. Apply AV profile in the firewall policy.



4. Authorize the FortiGate on FortiNDR for sending files.



5. Check the FortiNDR processed traffic. See FortiGate integration (integrated mode with FOS 5.6 and higher) on page 47.

Device input

The *Device Input* page displays the FortiGate (5.6 and higher) and FortiSandbox (4.0.1 and higher) devices that are sending files to FortiNDR. To view the Device Input page, go to *Security Fabric* > *Device Input*.

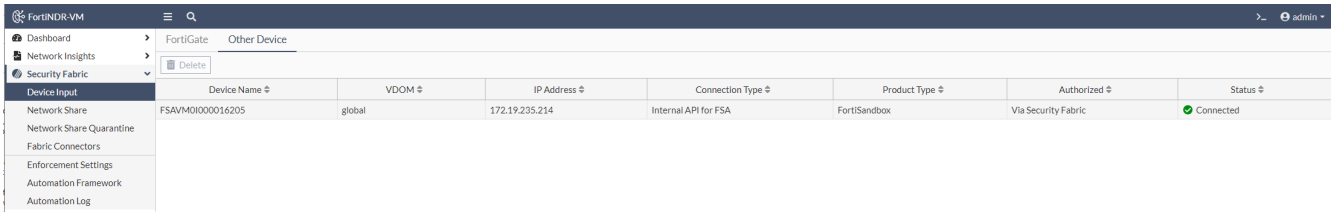
FortiGate tab

The *FortiGate* tab displays the FortiGates sending files via OFTP (FortiSandbox field with TCP port 514) and via HTTPs (FOS 7.0.1 and higher).

FortiNDR must authorize connections from FortiGate for OFTP and for inline blocking. Connect FortiNDR to the FortiGate Security Fabric to authorize the device via the Security Fabric protocol. For more information, see Security Fabric on page 44.

Other Device tab

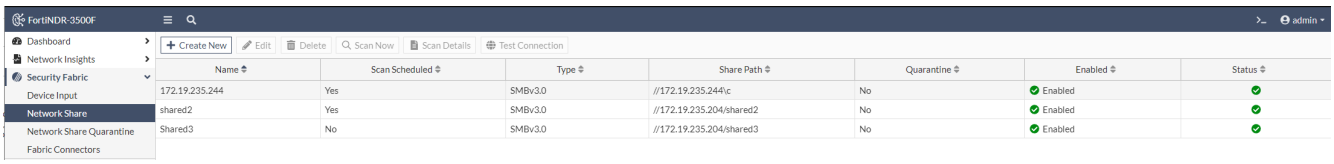
The *Other Device* tab displays FortiSandbox submissions via the FortiNDR API.



Network Share

Network File Share (or Network Share) allows FortiNDR to scan remote file locations via SMB and NFS protocol. Central quarantine with either *Move* or *Copy* of files is supported.

Create a *Network Share* profile to configure a Network Share location for inspection by FortiNDR. After the profile is configured, FortiNDR will scan the registered network's share directories.



Creating a Network Share

To create a Network Share profile, go to *Security Fabric* > *Network Share*. Register a new Network Share by providing the mounting information. Configure the profile to quarantine files separately based on their detected risk level. You can also use the profile to schedule a scan cycle of the network share location.

To create a Network Share profile:

1. Go to *Security Fabric* > *Network Share*.
2. In the toolbar, click *Create New*. The *New Network Share* page opens.
3. Enter the Network Share mounting information.

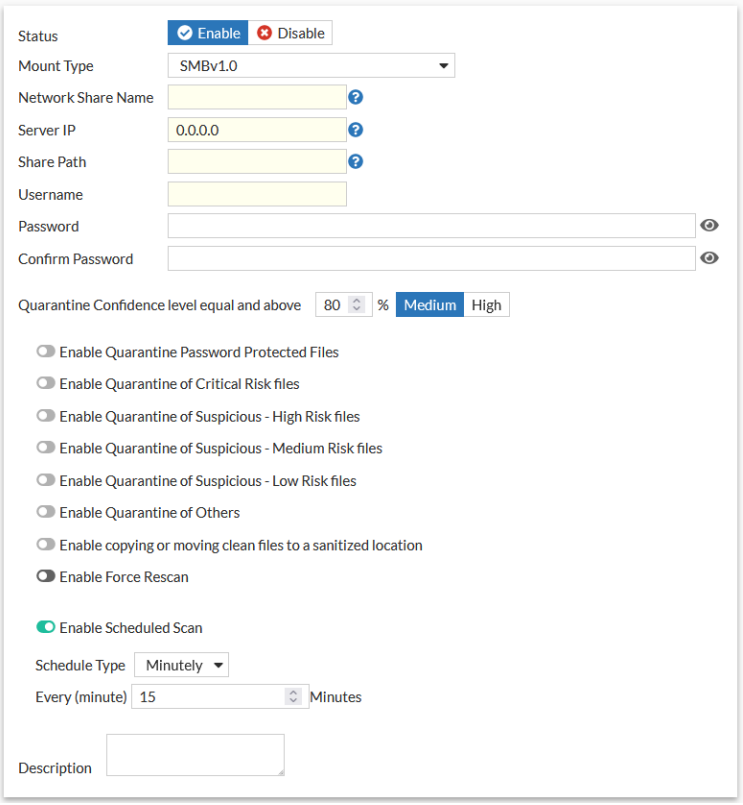
Status	*Enable* or *Disable*. *Enable* is the default.
Mount Type	Select a Network Share protocol from the list. The following protocols are supported: • SMBv1.0 • SMBv2.0 • SMBv2.1 • SMBv3.0 • NFSv2.0 • NFSv3.0 • NFS v4.0
Network Share Name	Enter a name for the Network Share.
Server IP	Enter the IP address for the Network Share.
Share Path	Enter the path for the Network Share.
Username	Enter the username for the Network Share.
Password	Enter the password for the Network Share and then confirm the password.

4. Configure the *Quarantine Confidence level equal and above*.
5. (Optional) Customize the quarantine and sanitize behaviors.

Enable Quarantine Password Protected Files	Moves password protected files to a designated quarantine location.  FortiNDR does not process password protected files.
Enable Quarantine Critical Risk Files	Moves detected files with critical risk to a designated quarantine location. This includes: • Fileless • Industroyer • Ransomware • Wiper • Worm

Enable Quarantine - High Risk Files	Moves detected files with high risk to a designated quarantine location. This includes: • Backdoor • Banking Trojan • Exploit • Infostealer • Proxy • PWS • Rootkit • Trojan
Enable Quarantine - Medium Risk Files	Moves detected files with medium risk to a designated quarantine location. This includes: • Clicker • DDoS • Downloader • Dropper • Phishing • Redirector • Virus
Enable Quarantine - Low Risk Files	Moves detected files with low risk to a designated quarantine location. This includes: • Application • CoinMiner • Generic Attack • Generic Trojan • SEP • WebShell
Enable Quarantine of Others	Moves other unprocessed files to a designated quarantine location. File types that falls under this category includes: • Files with unsupported file type • Files with Over size Limit • Empty/Irregular files
Enable Copying or Moving clean files to sanitized location	Moves or copies clean files to a location specified in the *Network Share Quarantine* profile. See, Network Share Quarantine on page 55. The *Moving* operation is only allowed for the quarantine location when *Keep Original File at Source Location* disabled. The *Copying* operation is only allowed for the quarantine location when *Keep Original File at Source Location* enabled. For information about combing Network Share and Quarantine profiles, see *Network Share Quarantine on page 55* > *Combining network share and quarantine profiles*.

Create a copy of clean files for every scheduled scan at the sanitized location	When enabled, FortiNDR will create a new folder <*Network Share Profile Name*>_<*Scan Task ID*> in the sanitized location for each scheduled scan. When disabled, FortiNDR will overwrite the sanitized location with the clean files from the latest scan. Enabling this option will increase the size of the Network Share location.
Create placeholder files for malicious/Suspicious/Other files at sanitized location	Adds a placeholder file in the sanitized location. The filename pattern of the placeholder file will be <*filename*>.<*severity*>.*txt*. This helps maintain the file structure of the original network in the share folder.
Enable Force Rescan	When enabled, FortiNDR will not use cache detection even if the files are previously scanned.

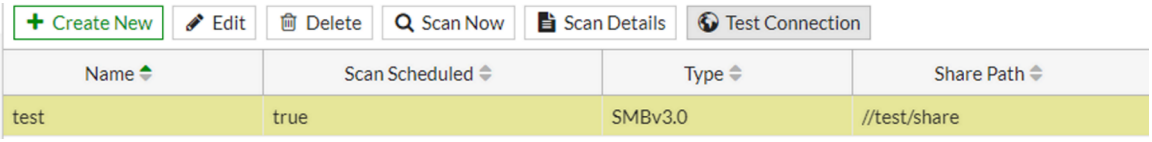


6. Click *OK*.

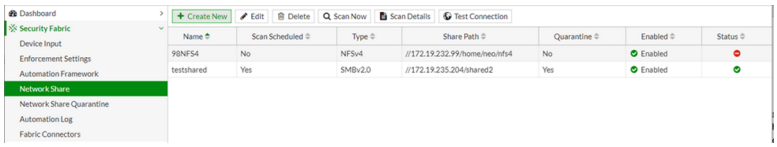
Testing connectivity

To validate the Network Share configuration:

1. Go to *Security Fabric* > *Network Share* and select a profile.
2. In the toolbar, click *Test Connection* to validate the Network Share configuration.



A green checkmark appears in the *Status* next to a valid connection.



Testing the connection will work when Network File Share is enabled. The test will fail if NFS is disabled.

Scanning a network location

To trigger a scan:

1. Go to *Security Fabric* > *Network Share* and select a profile.
2. In the toolbar, click *Scan Now*.

The *Scan Now* button will not create a new task when the Network Drive is:

- Currently mounting
- Scanning another task
- Disabled
- Not connected (*Status* is *Down*)

You can use a REST API call to start a scan. See, Start Network Share scan.

Scheduling a scan

You can schedule routine scanning for a Network Share location on an hourly, daily, or monthly basis. The minimum time interval for each scan is 15 minutes.

If an NFS scan takes longer than the next scheduled time, the next scheduled time is skipped and an event log is created to reflect this.

To schedule a scan:

1. Go to *Security Fabric* > *Network Share* and select a profile.
2. In the toolbar, click *Edit*. The *New Network Share* window opens.
3. Select *Enable Scheduled Scan*.
4. Configure the *Schedule Type* and the correspodning time interval.
5. Click *OK*.

Viewing scan results

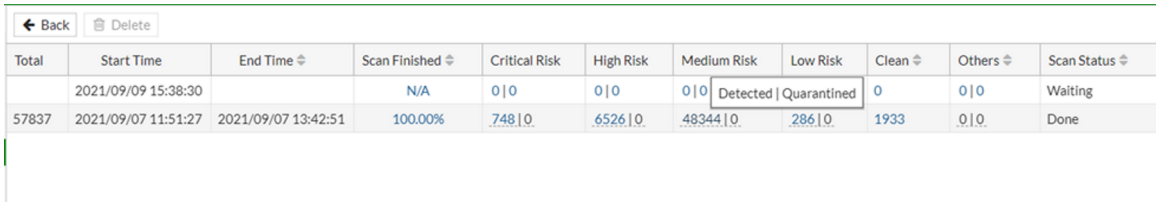
View the scan history of the Network Share directories.

To view the scan results:

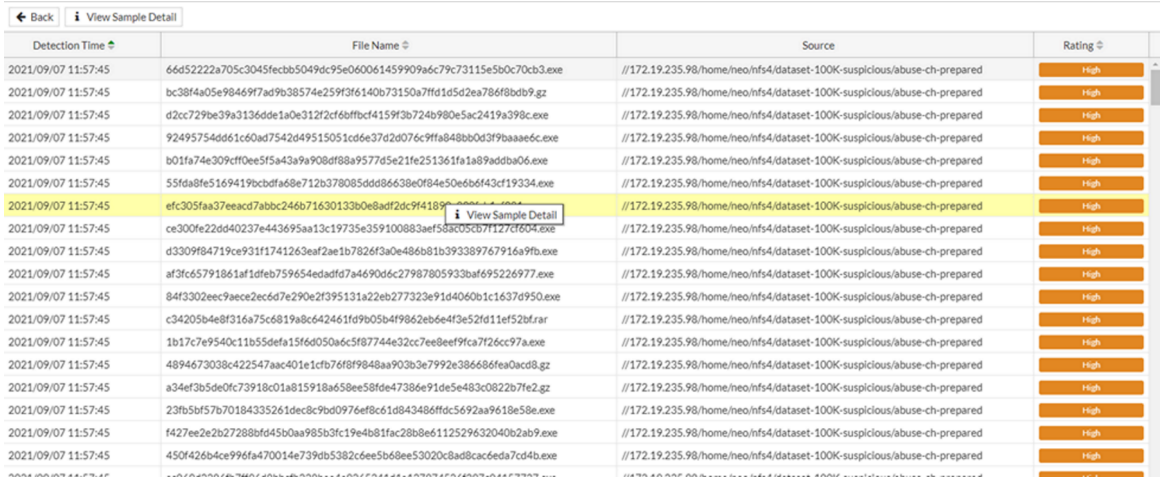
1. Go to *Security Fabric* > *Network Share* and select a profile.
2. In the toolbar, click *Scan Details*. The scan history is displayed.

   For columns with numbers:

   - The first number represents the total number of files that belong to that category.
   - The second number indicates the successful quarantine counts of that category.



3. Click the numbers to view the detection information for the samples that belong to the category.



4. Click *Back* to return to the *Network Share* pane.

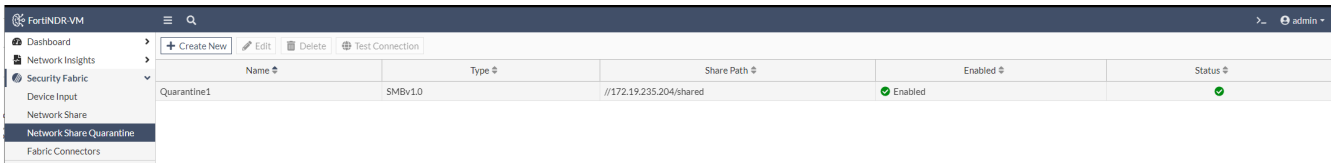
Scanning Zip files

FortiNDR can extract and process Zip files up to 10 levels. When any of the files inside the Zip file is detected, the whole zip file will be marked as malicious.

FortiNDR does not process password-protected zip files.

Network Share Quarantine

You can configure multiple quarantine profiles for different Network Share locations. Use different configurations to specify detection files with different levels to separate quarantine locations.



Quarantined files

When a file is quarantined, it creates two files in the quarantine folder:

- A copy of the original file, and
- A metadata file.

The metadata file provides information about FortiNDR's verdict of the malicious file, such as the virus name, path (URL), MD5 etc. You can refer to the meta file to understand why the file was moved or copied to the quarantine folder.

The metadata file uses the naming pattern *<Network Share File ID>.meta*. The file contains the following information:

- Network Share File ID
- Network Share ID
- Network Share Profile Name
- Scan Task ID
- File ID
- Filename
- URL
- MD5
- Detection Name

Example:

```
Network Share FileID: 351640
SID: 3 (Share ID)
JID: 44 (Job ID)
FileID: 1198941 (File ID)
```

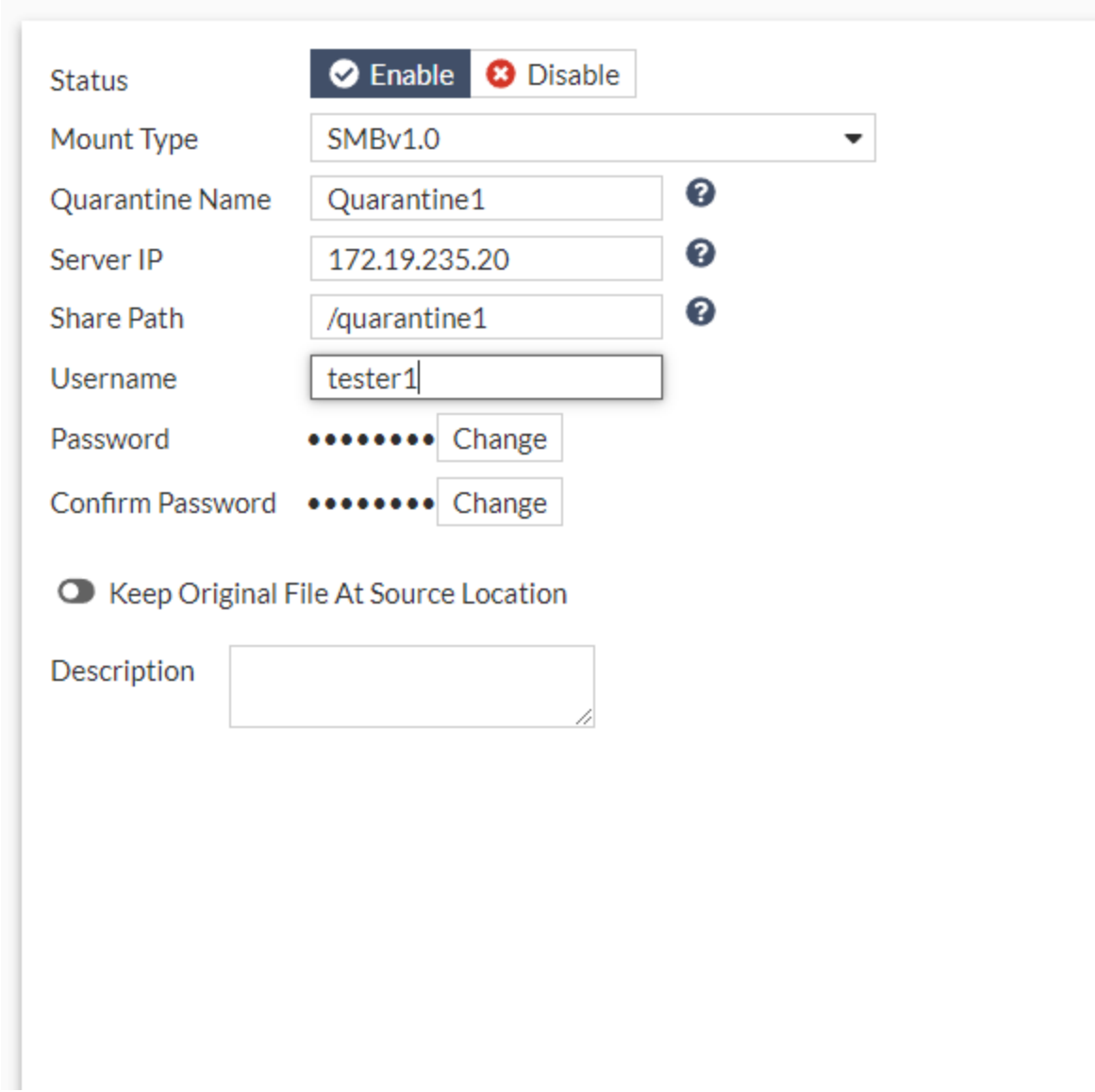
```
File Name: sample.vsc
Device: testshared
URL: //172.16.2.100/shared2/2/sample.vsc
MD5: 31e06f25de8b5623c3fdaba93ed2edde
Virus Name: W32/Wanna.A!tr.ransom
DelOriginalFile: Success
```

Creating a quarantine profile

To create a quarantine profile:

1. Go to *Security Fabric* > *Network Share Quarantine*.
2. In the toolbar, click *Create New*. The *New Quarantine Location* window opens.
3. Configure the quarantine profile mounting information.

Status	*Enable* or *Disable*.
Quarantine Name	Enter a name for the quarantine profile
Mount Type	Select a Network Share protocol from the list. The following protocols are supported: • SMBv1.0 • SMBv2.0 • SMBv2.1 • SMBv3.0 • NFSv2.0 • NFSv3.0 • NFS v4.0
Server IP	Enter the IP address for the Network Share.
Share Path	Enter the path for the Network Share.
Username	Enter the username for the Network Share.
Password	Enter the password for the Network Share and then confirm the password.



4. (Optional) Select *Keep Original File At Source Location*.

Enabling *Keep Original File At Source Location* may affect the behavior of your Network Share profile. For information, see Combining network share and quarantine profiles on page 57.

5. (Optional) In the *Description* field, enter a description of the profile.

Combining network share and quarantine profiles

The following table summarizes how enabling *Keep Original File At Source Location* affects the behavior of the quarantine and sanitize settings in a Network Share profile:

Keep Original File At Source Location	Effect	Enable Quarantine for (Critical/High/Med/Low/Password Protected/Other risk)	Effect
Enabled	Keeps the quarantine file in the source location.	*Enabled*	• Creates a copy of the quarantine file in the quarantine location and renames it *<Network Share File ID>*. • Creates a metafile with the naming pattern *<Network Share File ID>.meta* for each quarantine file.
Disabled	FortiNDR creates a placeholder file with *<Filename>.quarantined* in the original folder	*Enabled*	• Copies the quarantine file to the quarantine location and renames it *<Network Share File ID>*. • Creates a metafile with the naming pattern *<Network Share File ID>.meta* for each quarantine file. • If FortiNDR has enough permissions, it will delete the file in the source location.

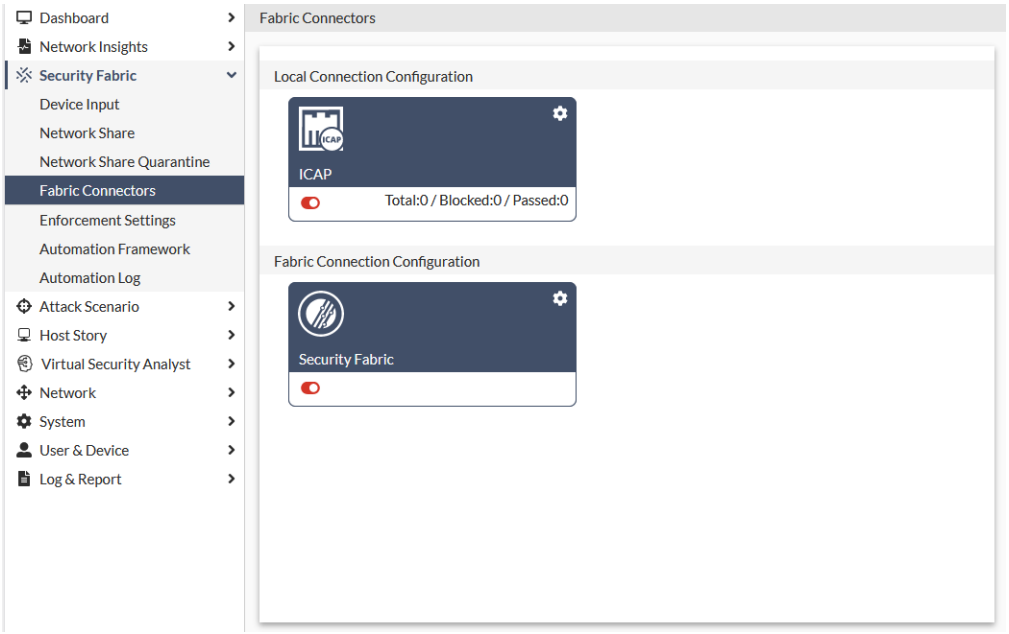
You can use the Network Share Quarantine location for both the quarantine of malicious files as well the Move/Copy of clean files. However, we recommend creating different folders for clean and malicious files.

Keep original file at source location	Move/Copy clean files to sanitized location	Effect
Enabled	*Enabled*	• Cleans files in the source location. • Copy the clean files to the Network Share Quarantine.
Enabled/*Disabled*	*Disabled*	• FortiNDR scans NFS but does not move or copy the files.
Disabled	*Enabled*	• Move the clean files to the Network Share Qaurantine. • FortiNDR attempts to delete the original files.

The *Move* operation involves copying and deleting files. FortiNDR can only delete files if it has sufficient permissions to do so.

Fabric Connectors

Fabric Connectors allow FortiNDR to connect to the Fortinet Security Fabric. ICAP allows connections to FortiGate and FortiWeb, and third-party devices such as Squid clients.



ICAP Connectors

FortiNDR can act as an ICAP server to allow ICAP clients such as FortiGate, Squid, and others to offload web traffic for scanning.

Use the ICAP connector to:

- Stop patient zero in the web browsing client.
- Stop malware coming from web browsing.
- Scan for malware in web traffic without using FortiGate AV profiles.
- Offload to FortiNDR for existing FortiSandbox customers who cannot use OFTP .

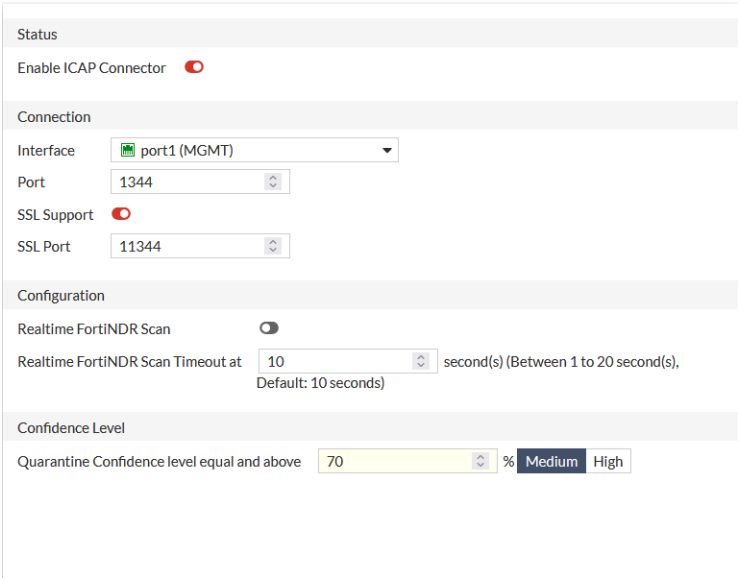
ICAP connectors are not suitable for high traffic volumes. If the sample submit rate is higher than six sumbmissions per second, we recommend using the *Inline Blocking* feature in FortiGate to do the sample submitting instead.

To integrate FortiNDR with FortiGate ICAP:

1. In FortiGate:
   a. Add the ICAP server.
   b. Create an ICAP profile.
   c. Add the ICAP profile to a policy.
2. In FortiNDR, configure the ICAP server.

To enable ICAP in FortiNDR:

1. Go to *Security Fabric* > *Fabric Connectors* and click the *ICAP* card.
2. Click *Enable ICAP Connector*.
3. Configure the ICAP settings and click *OK*.



Security Fabric Connector

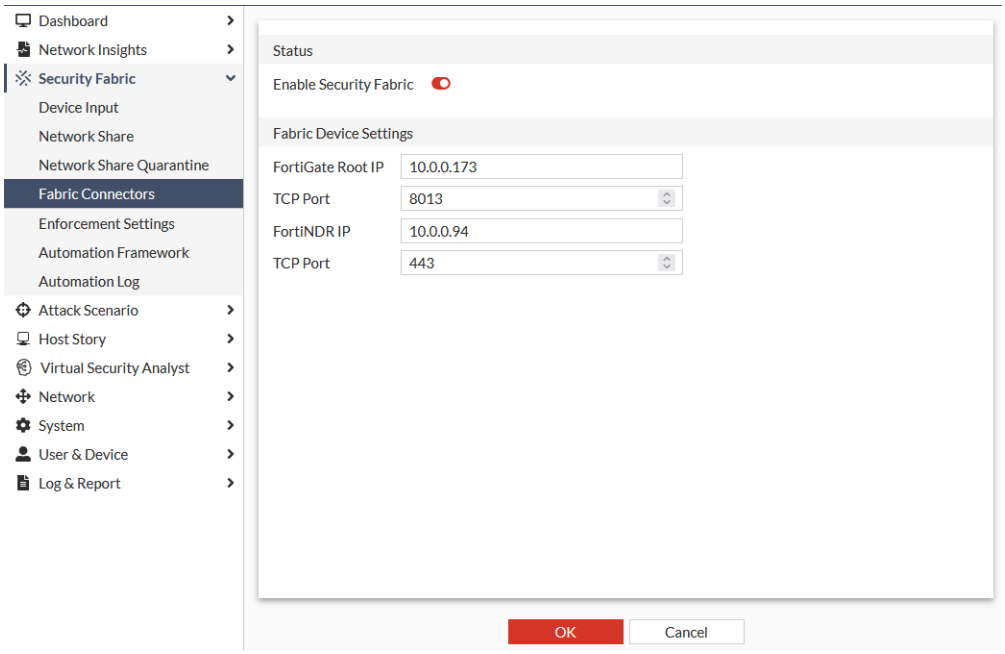
FortiNDR (formerly FortiAI) 1.5.0 and FortiOS 7.0.0, FortiNDR can join FortiGate Security Fabric. After connecting to the Security Fabric, FortiNDR can share information such as FortiNDR system information and malware types detected.

When FortiNDR has joined the FortiGate Security Fabric, FOS can see FortiNDR as a device in its physical and logical topology. FOS can add widgets such as malware distribution to identify the types of malware on the network, which is a function of the FortiNDR Virtual Security Analyst.

To configure the Security Fabric connector:

1. Go to *Security Fabric* > *Fabric Connectors* and click the *Security Fabric* card.
2. Click *Enable Security Fabric* to enable the connector.
3. Configure the connector settings and click *OK*.

   FortiNDR uses the port1 IP address as the management port. The FortiGate Security Fabric IP address uses the FortiGate root IP address. Changing default ports is not recommended.



Enforcement

Enforcement provides an extra layer of logic to deal with the detection discovered by FortiNDR and delivers follow-up actions to Security Fabric devices. FortiNDR periodically evaluates the latest batch of detection based on enforcement settings. If any detection satisfies the criteria for the next cause of action, the system then looks at which automation profile the detection falls under and performs the response action accordingly.

The system uses the webhook registered to the automation profiles or predefined APIs to carry out different enforcement strategies. FortiNDR supports the following action types:

- FortiGate Quarantine (Previously known as Ban IP action)
- FortiNAC Quarantine (FortiNAC version v9.2.0+ support)
- FortiSwitch Quarantine via FortiLink
- Generic Webhook

FortiNDR combines the information from the Automation Framework and the Enforcement Settings to generate enforcement actions.

Enforcement Settings

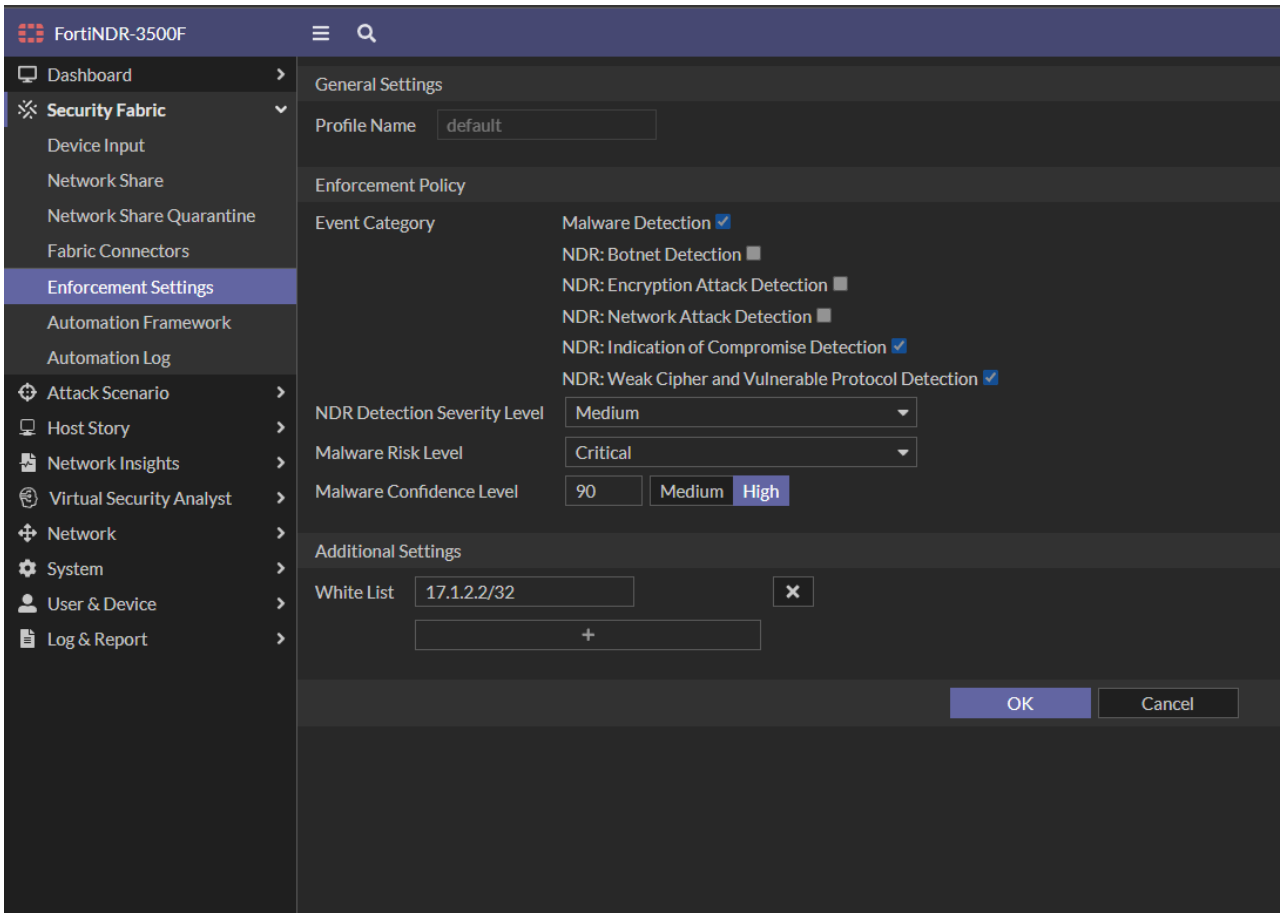
Enforcement Settings are policies for FortiNDR to filter out malicious detections and NDR anomaly detections when executing enforcement. These policies include Event Category, NDR Detection Severity Level, Malware Risk Level, Malware Confidence Level, and Allow List.

Register the automation stitches webhook you created in FortiGate so that FortiNDR can execute the enforcement. FortiNDR combines the information from the Automation Framework and the Enforcement Settings to generate enforcement actions.

To create and enforcement profile:

1. Go to *Security Fabric* > *Enforcement Settings*.
2. In the toolbar, click *Create New*. The *General Settings* page opens.
3. Configure the profile settings.

Profile Name	Enter a name for the profile.
Event Category	Select one of the following options: • *Malware Detection* • *NDR: Botnet Detection* • *NDR: Encryption Attack Detection* • *NDR: Network Attack Detection* • *NDR: Indication of Compromise Detection* • *NDR: Weak Cipher and Vulnerable Protocol Detection*
NDR Detection Severity Level	Select *Critical*, *High*, *Medium* or *Low* severity from the dropdown.
Malware Risk Level	Select *Critical*, *High*, *Medium* or *Low* severity from the dropdown.
Malware Confidence Level	Enter a numeric value for the confidence level and click either *Medium* or *High*.
White List	Enter the IP address you want to exclude as a trigger. If the source IP matches the entry, the profile will not be triggered even if the event and severity level match.



4. Click *OK*.

Creating an Enforcement Profile

Use Enforcement Profiles to triggers an NDR response based on event category and its risk level.

Response actions are based on API calls, either to Fortinet Fabric Products or third-party products. Please ensure API is enabled on the receiving side. FortiNDR supports execution and undo actions. Technically these are two different API calls, which are called to trigger an action and undo an action. For example, quarantine and release of IP.

Duplicate anomalies

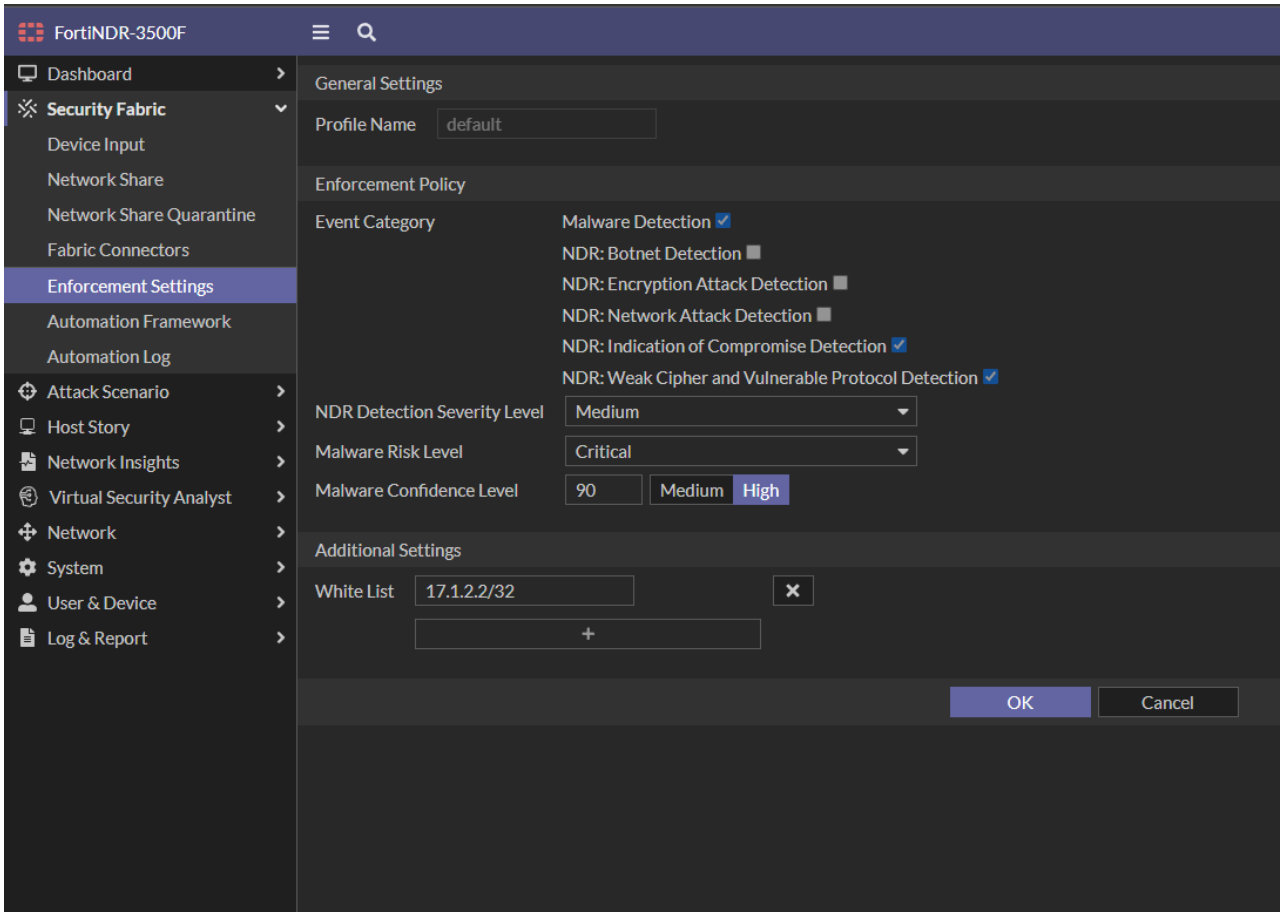
- A response is only triggered once when multiple events in NDR anomalies in the same category (e.g. IOC campaign) occurs within one minute.
- IA response is recorded as a duplicate when multiple events in NDR anomalies in the same category occur every minute after that.

To create and enforcement profile:

1. Go to *Security Fabric* > *Enforcement Settings*.
2. In the toolbar, click *Create New*. The *General Settings* page opens.

3. Configure the profile settings.

Profile Name	Enter a name for the profile.
Event Category	Select one of the following options: • *Malware Detection* • *NDR: Botnet Detection* • *NDR: Encryption Attack Detection* • *NDR: Network Attack Detection* • *NDR: Indication of Compromise Detection* • *NDR: Weak Cipher and Vulnerable Protocol Detection*
NDR Detection Severity Level	Select *Critical*, *High*, *Medium* or *Low* severity from the dropdown.
Malware Risk Level	Select *Critical*, *High*, *Medium* or *Low* severity from the dropdown.
Malware Confidence Level	Enter a numeric value for the confidence level and click either *Medium* or *High*.
White List	Enter the IP address you want to exclude as a trigger. If the source IP matches the entry, the profile will not be triggered even if the event and severity level match.

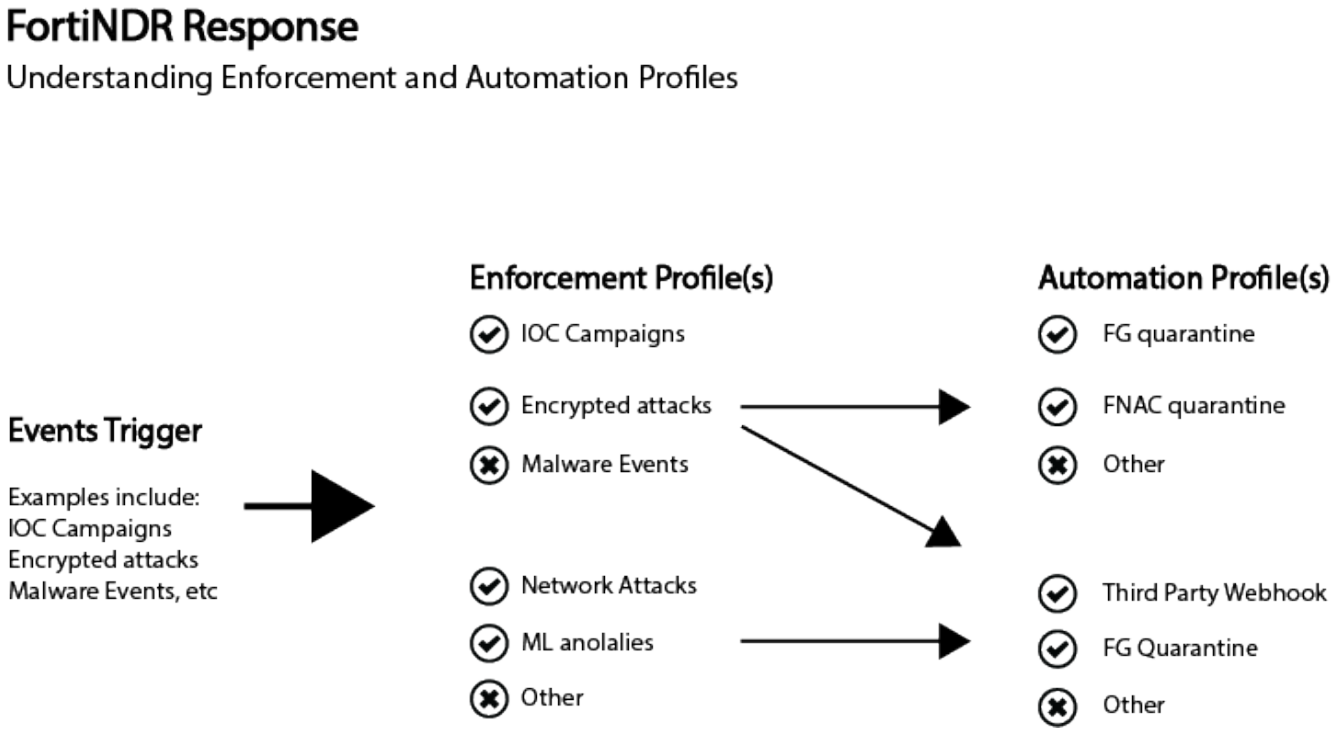


4. Click *OK*.

For NDR detection *Severity Level* and *Malware risk level*, severity is inclusive of higher severity levels. For example, if *High* is selected, the enforcement profile will match both HIGH and CRITICAL events.

Automation Framework

A single enforcement profile can be selected with different automation profiles. This provides you with more flexibility in the response action. The following diagram illustrates the relationship between Enforcement and Automation profiles.

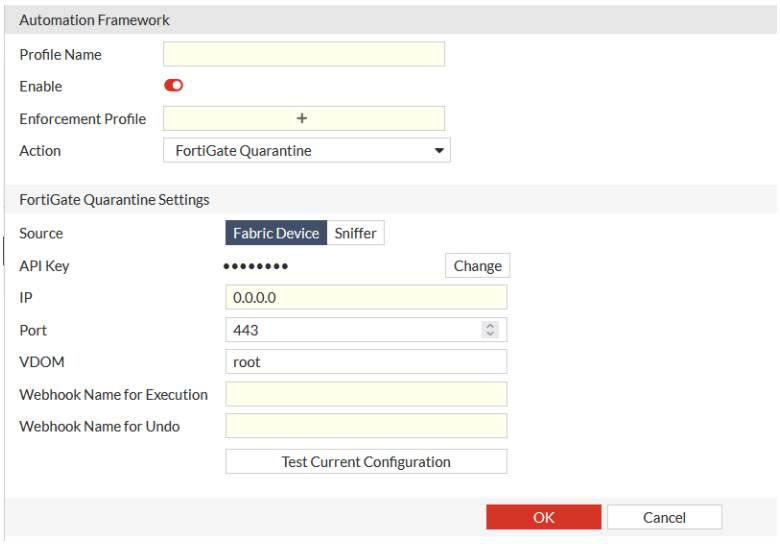


To create an automation profile:

1. Go to *Security Fabric* > *Automation Framework*.
2. In the toolbar, click *Create New*.

3. Configure the profile settings:

Profile Name	Enter a name for the profile.
Enable	Enable or disable the framework.
Enforcement Profile	Click to select and profile from the *Enforcement Settings*. See Creating an Enforcement Profile on page 63.
Action	Select one of the following actions: • *FortiGate Quarantine* • *FortiNAC Quaranitne* • *Generic Webhook*
Source	**Fabric Device**: If the source of detection came from OFTP, the enforcement is only executed to a matching automation profile with a matching IP address and VDOM.
	Sniffer: If the source of detection came from a sniffer, the enforcement is adapted by all profiles where *Trigger Source* is *Sniffer*. Since detection sourced from sniffer does not contain information about which fabric device monitors the infected IP address, it is your responsibility to specify the correct device IP address and VDOM.
API Key	Enter the device API key
IP	Enter the device IP address.
Port	Enter the device port number.
VDOM	Enter the VDOM info. Only applicable to FortiGate Quarantine and FortiSwitch Quarantine via FortiLink.
WebHook Name for Execution	Select the FortiGate webhook for execution action, such as `ip_blocker`. Only applicable to *FortiGate Quarantine* and *FortiSwitch Quarantine via FortiLink*.
WebHook Name for Undo	Select the FortiGate webhook for undo action, such as `ip_unblocker`. Only applicable to *FortiGate Quarantine* and *FortiSwitch Quarantine via FortiLink*.
Webhook Execution Settings	Enter the URL, Method, Header and HTTP body Template for Execution webhook settings. Only applicable to *Generic Webhook*.
Webhook Undo Settings	Enter the URL, Method, Header and HTTP body Template for Undo webhook settings. Only applicable to *Generic Webhook*.



4. Test the configureaiton
5. Click *OK*.

FortiGate quarantine webhook setup example

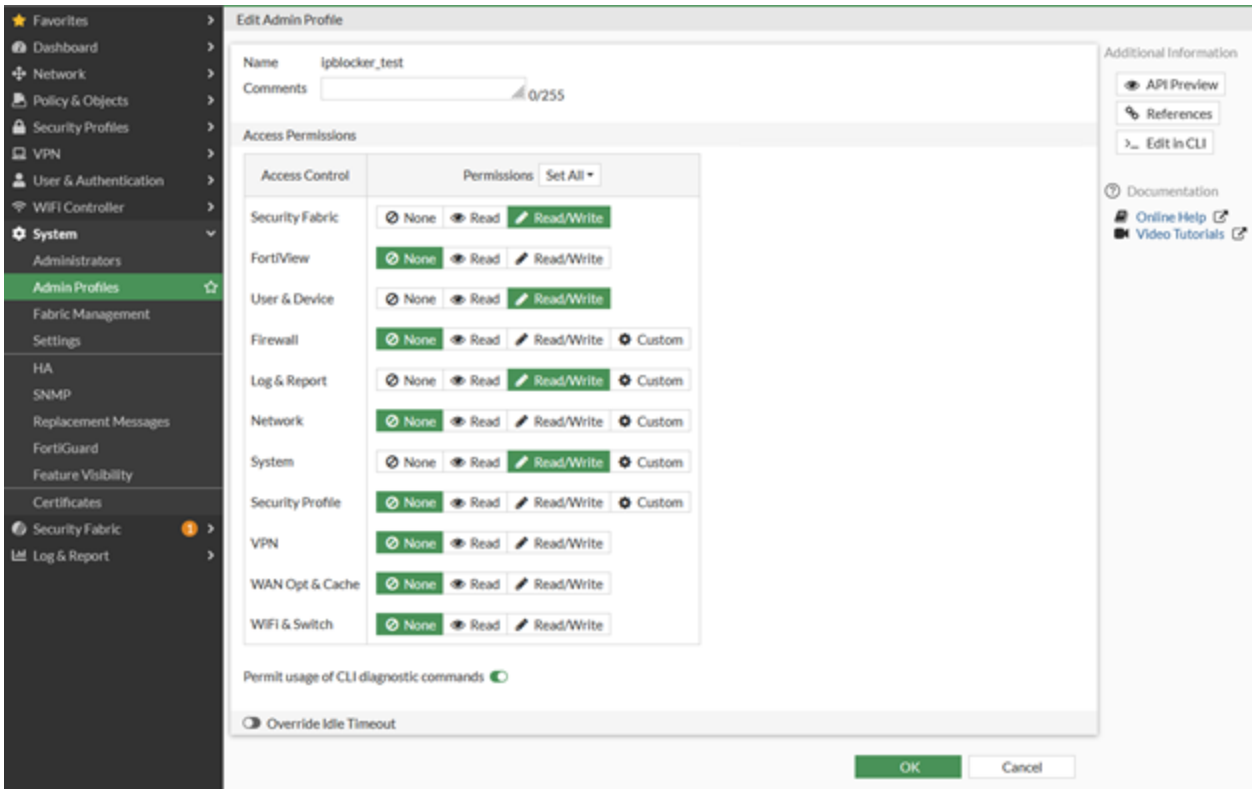
To create an automation profile for *FortiGate Quarantine* (Formerly Ban IP action) or *FortiSwitch Quarantine via FortiLink*, the incoming webhook needs to be setup on FortiGate to accept requests from FortiNDR. You can register them in *Security Fabric > Automation Framework*.

The following example shows you how to set up webhooks for FortiGate Quarantine to quarantine infected hosts through FortiGate.

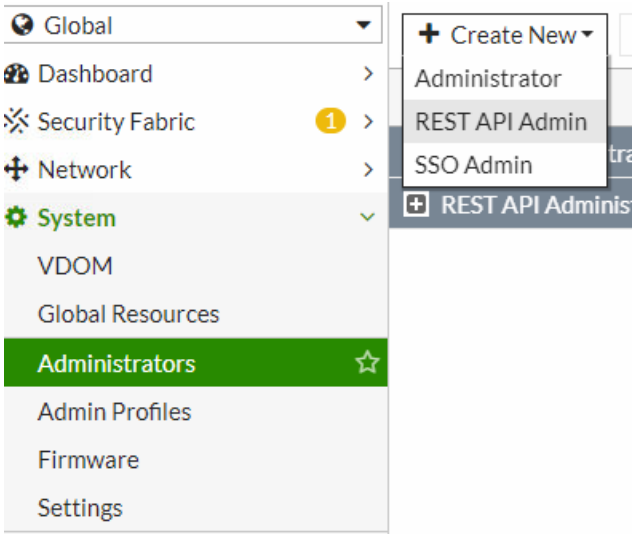
To set up a webhook for Ban IP:

1. In FortiGate, go to *System > Admin Profiles* and create a profile, for example, *ipblocker_test* and set the following *Access Permissions*.

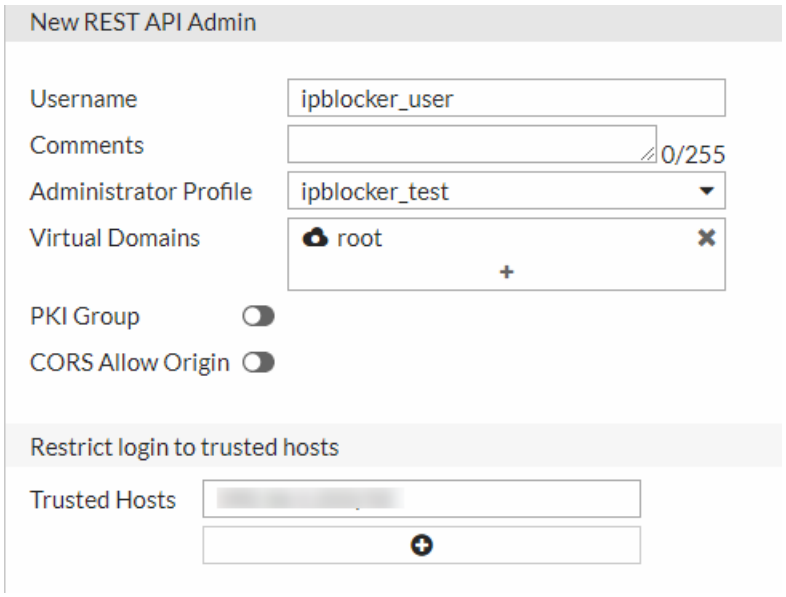
Ensure the selected Administrator profile has sufficient privileges to execute CLI scripts.



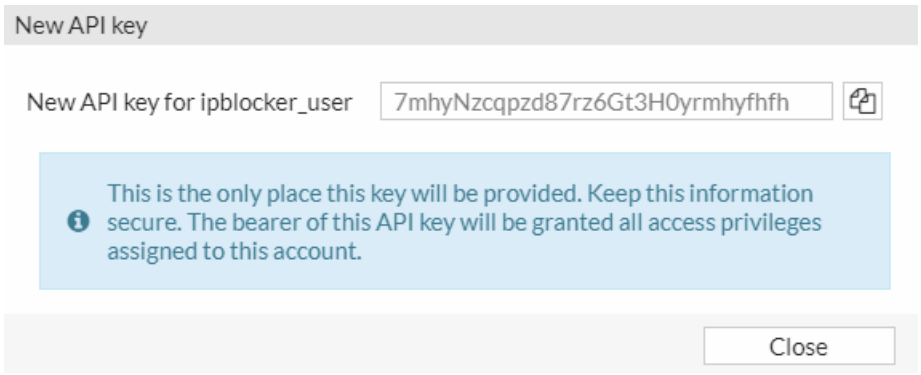
2. In FortiGate, go to *System* > *Administrators* and create a *REST API Admin* using the *ipblocker_test* admin profile.



3. Select the *Virtual Domains* to be associated with the generated API key.
   You can also restrict access to FortiNDR by setting up *Trusted Hosts* for the API profile.

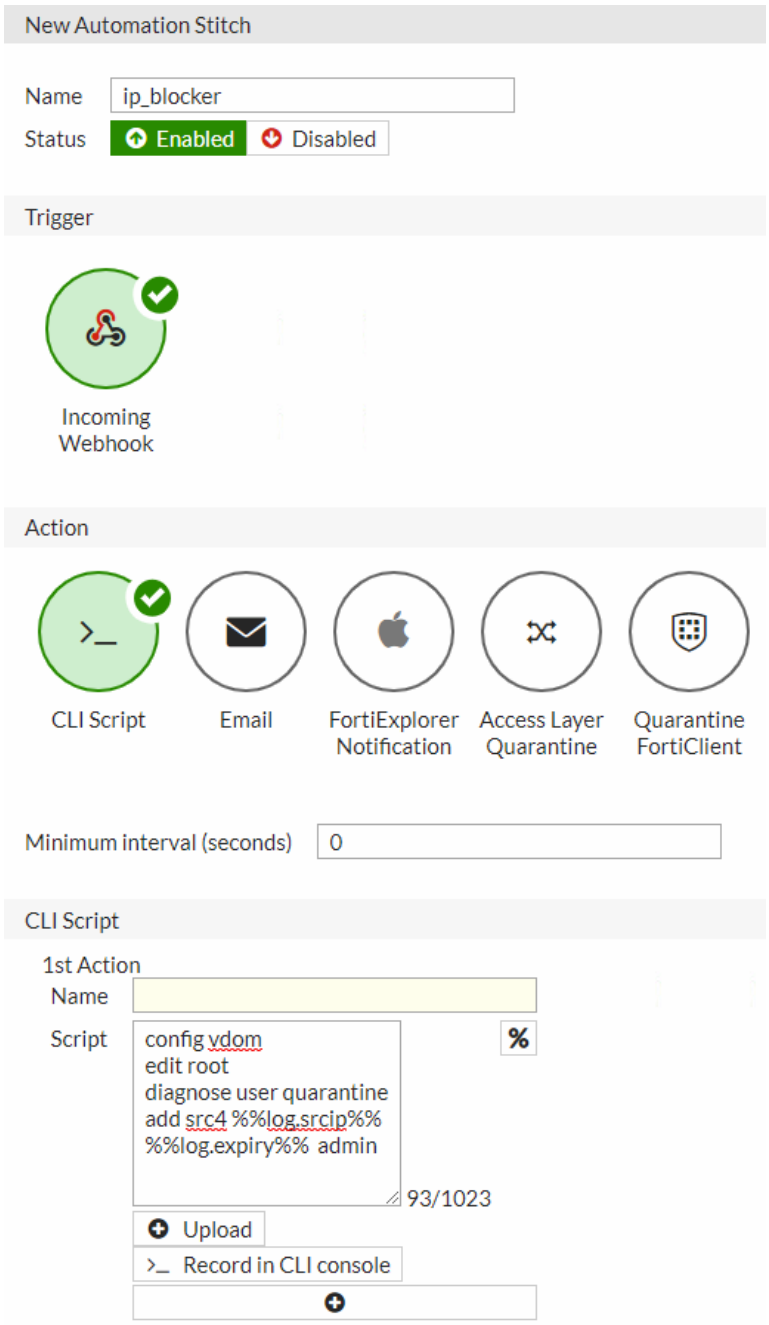


4. Save the generated *New API key* as you need that to register the automation profile in FortiNDR.



5. In FortiGate, go to *Security Fabric* > *Automation* and create an *Automation Stitch* for Ban IP actions. Select *Incoming Webhook* and enter a *Name* to be used to register the automation profile.
6. In the *New Automation StitchCLI Script* section, enter the following script. Substitute `root` with a VDOM.

```
config vdom
edit root
diagnose user quarantine add src4 %%log.srcip%% %%log.expiry%% admin
```



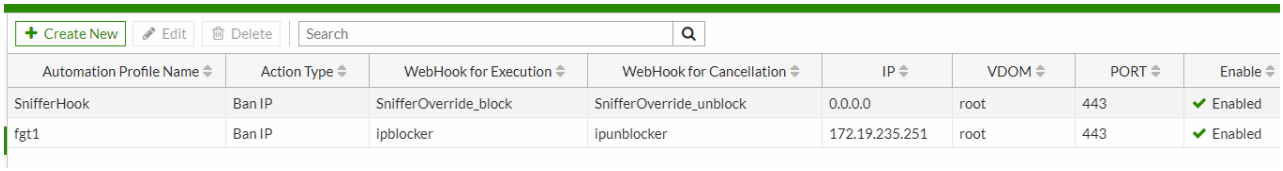
This example requires two webhooks, one that executes the Ban IP action (this *ip_blocker* example). Another webhook executes the unban IP action.

We recommend maintaining a consistent naming pattern for the Stitch and Trigger names. For example, *ip_blocker* and *ip_unblocker*.

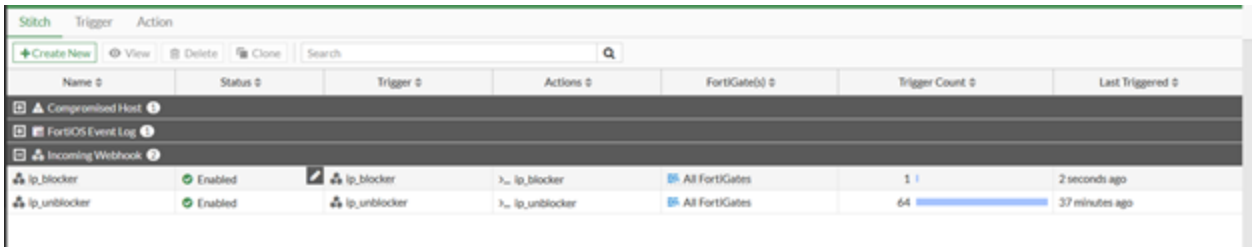
7. Repeat the above step to create a webhook to execute the unban IP action, for example, *ip_unblocker*.
In the *New Automation StitchCLI Script* section, enter the following script for the unban IP action. Substitute `root` with a VDOM.

```
config vdom
edit root
diagnose user quarantine delete src4 %%log.srcip%%
```

FortiOS v6.4:

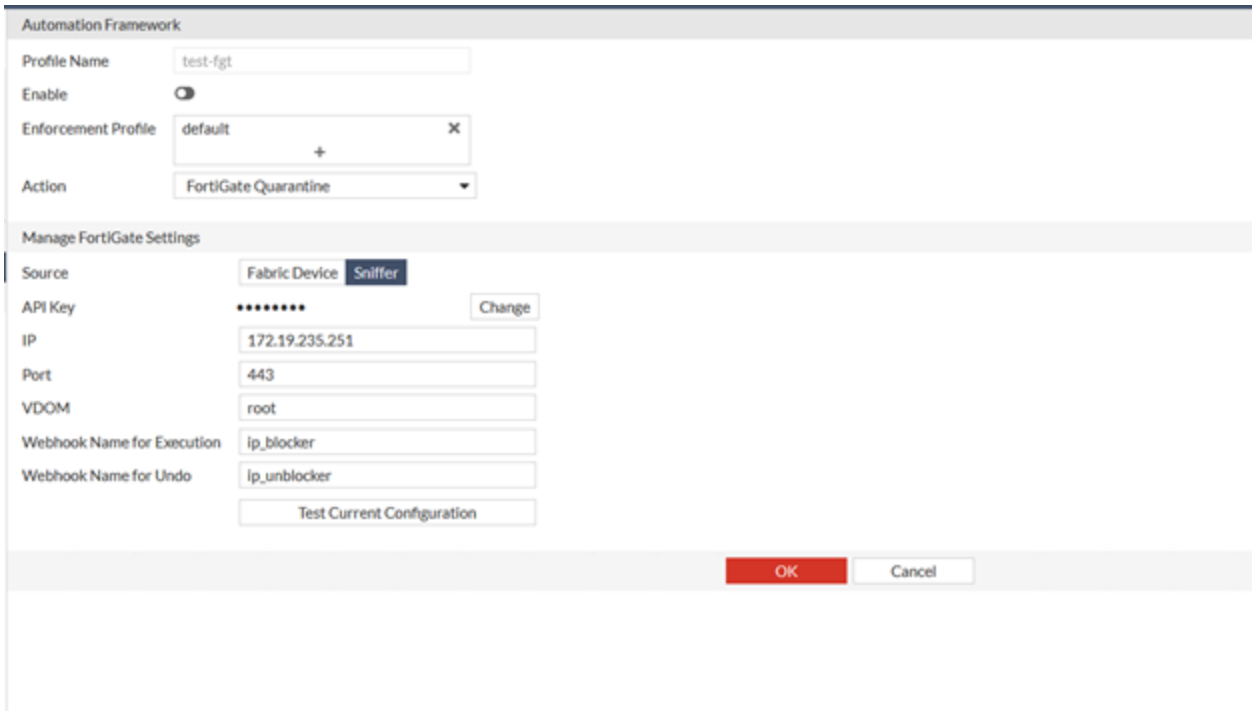


FortiOS v7.0.1



For the CLI script example, `config vdom edit root` is not needed when FortiGate disabled VDOM mode.

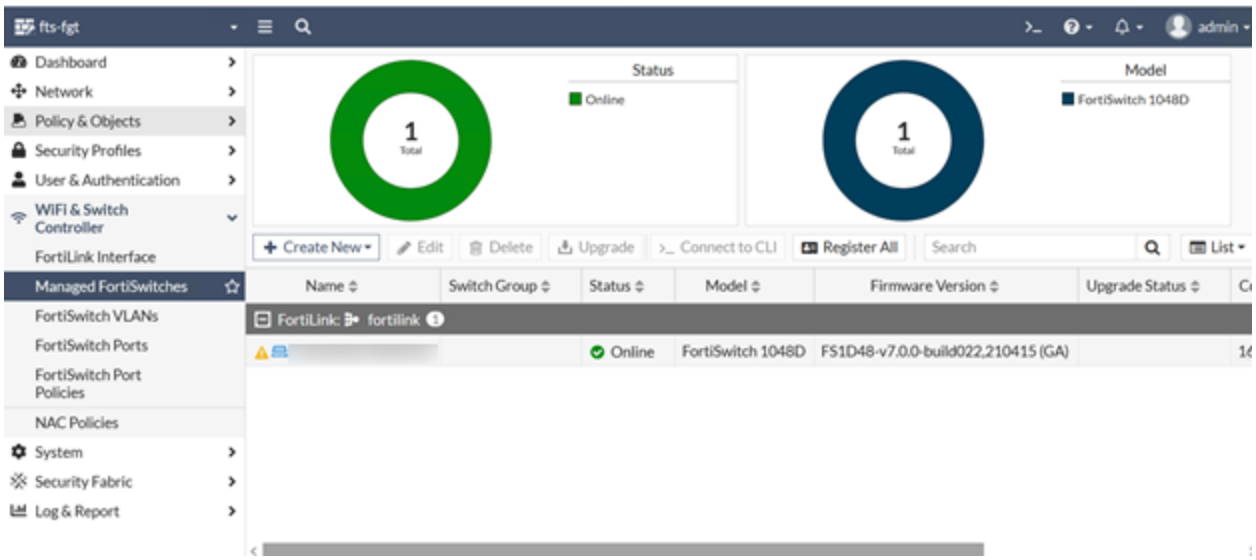
8. Register the Webhook name in the Automation Profile.



FortiSwitch quarantine setup example

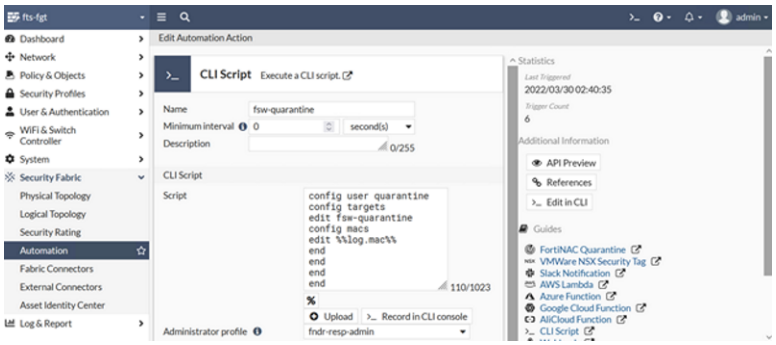
FortiNDR supports quarantining devices that are connected to a FortiSwitch which is managed by FortiGate. FortiSwitch is connected to a FortiGate and is configured in FortiLink mode. FortiNDR will utilize FortiGate's incoming webhook to provide the device's MAC address for quarantine/undo quarantine.

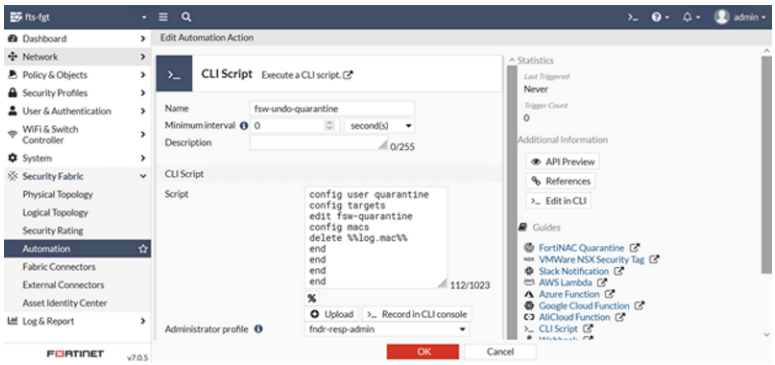
For information about configuring FortiLink, see Configuring FortiLink.



To setup FortiSwitch quarantine on FortiNDR:

1. Following the steps for creating a webhook on FortiGate in FortiGate quarantine webhook setup example on page 67. Note that the CLI script for quarantine and undo quarantine should be updated.

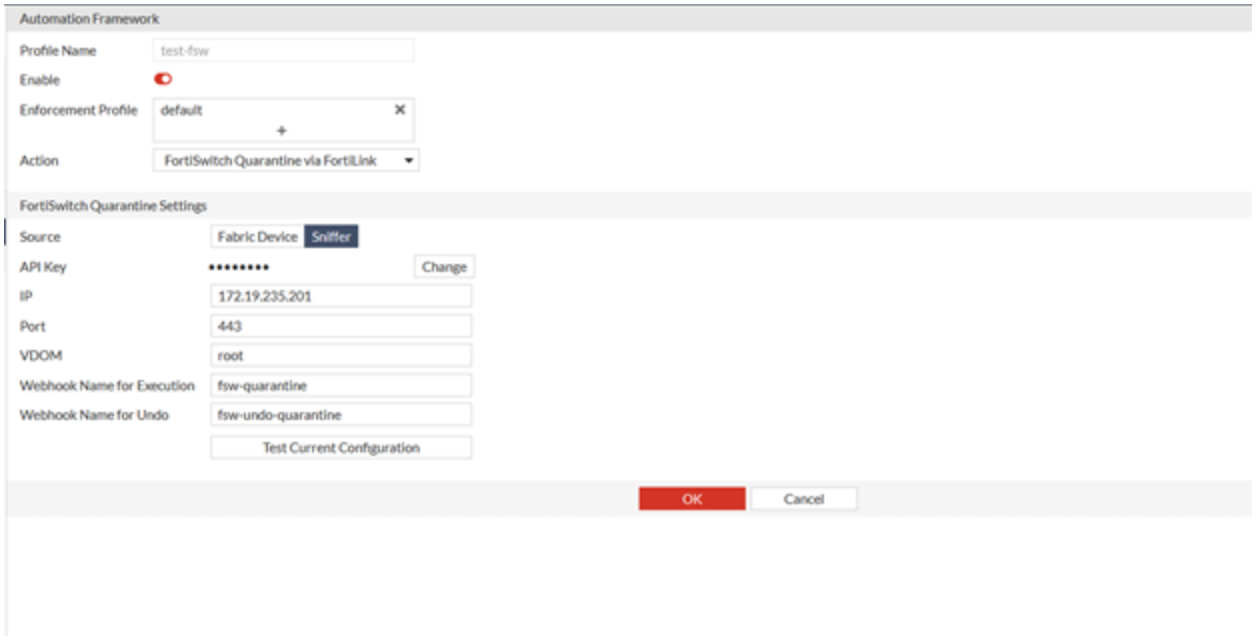




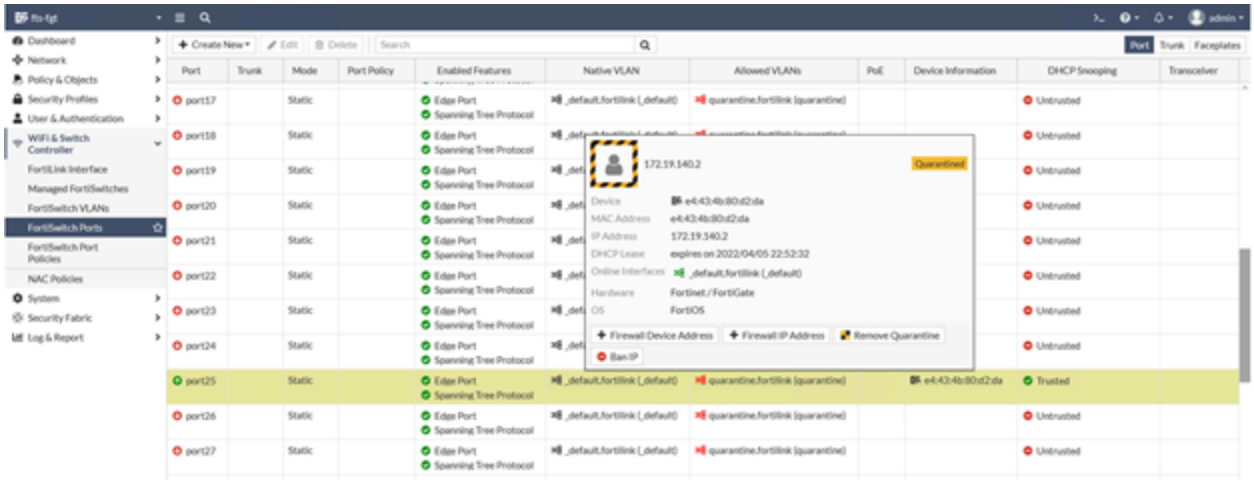
The CLI script for quarantine and undo quarantine should be updated.

2. Register webhooks on FortiNDR .

The device settings such as *IP* and *Port* are the IP and port of the managing FortiGate device.



3. Click the *Test* button to test the current configuration.



4. Click *OK*.

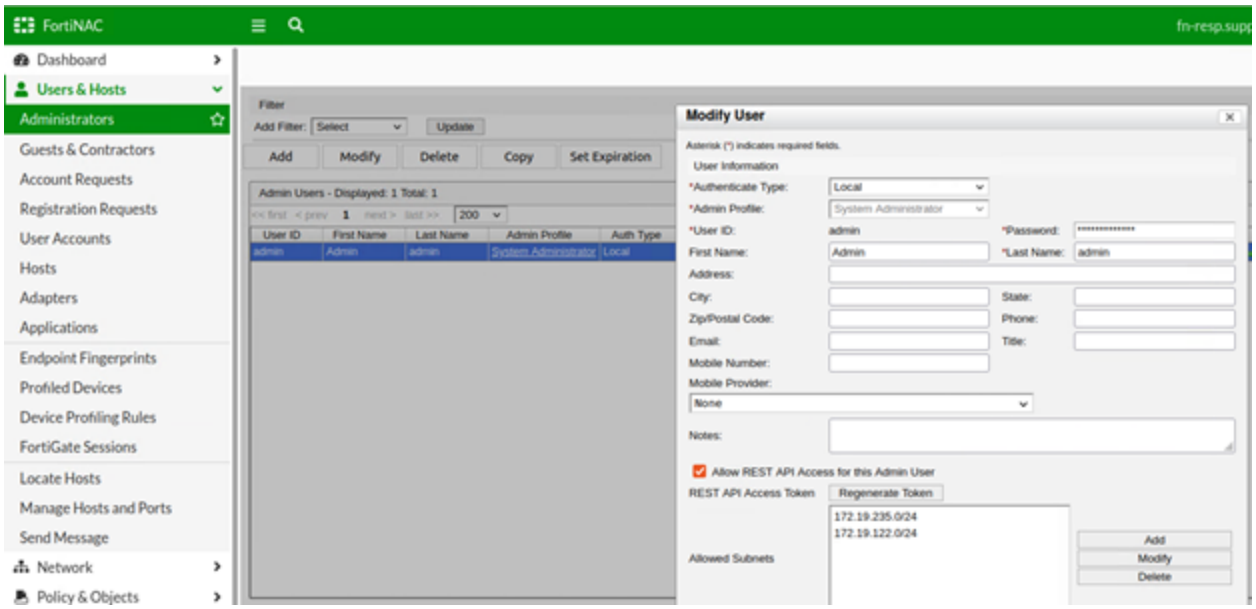
FortiNAC quarantine setup example

FortiNDR supports FortiNAC quarantine by calling FortiNAC rest API to enable and disable the Host record that matches the supplied IP address.

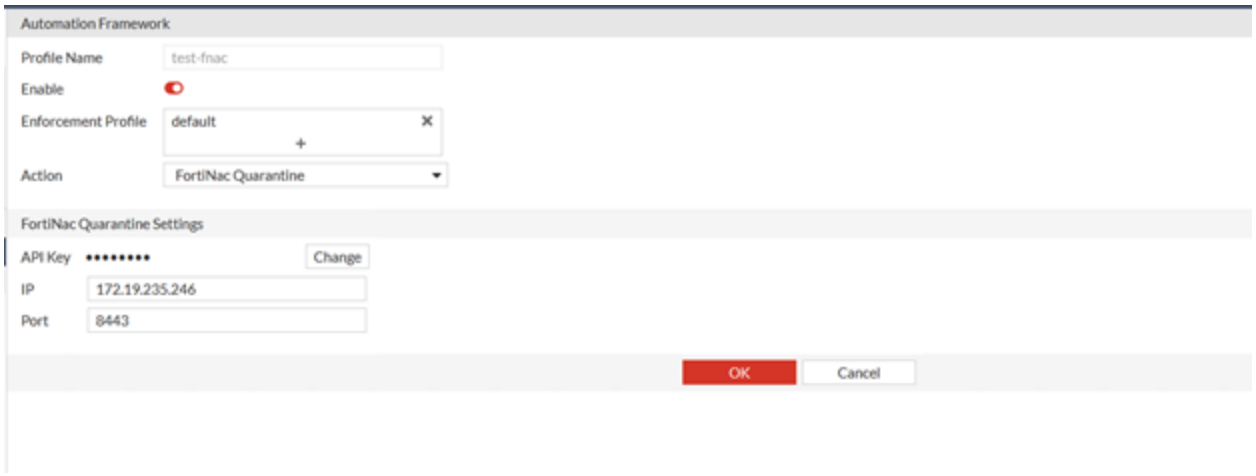
For information about configure FortiNAC, see the *FortiNAC Administration Guide* in the Document Library.

To setup FortiNAC quarantine on FortiNDR:

1. In FortiNAC:
   a. Go to *Users & Hosts* > *Administrators* > *Modify User*.
   b. Enable *REST API access to FortiNAC* and generate HTTP API access token.
   c. Click *OK*.



2. Create new automation profile with action type: *FortiNAC Quarantine*.

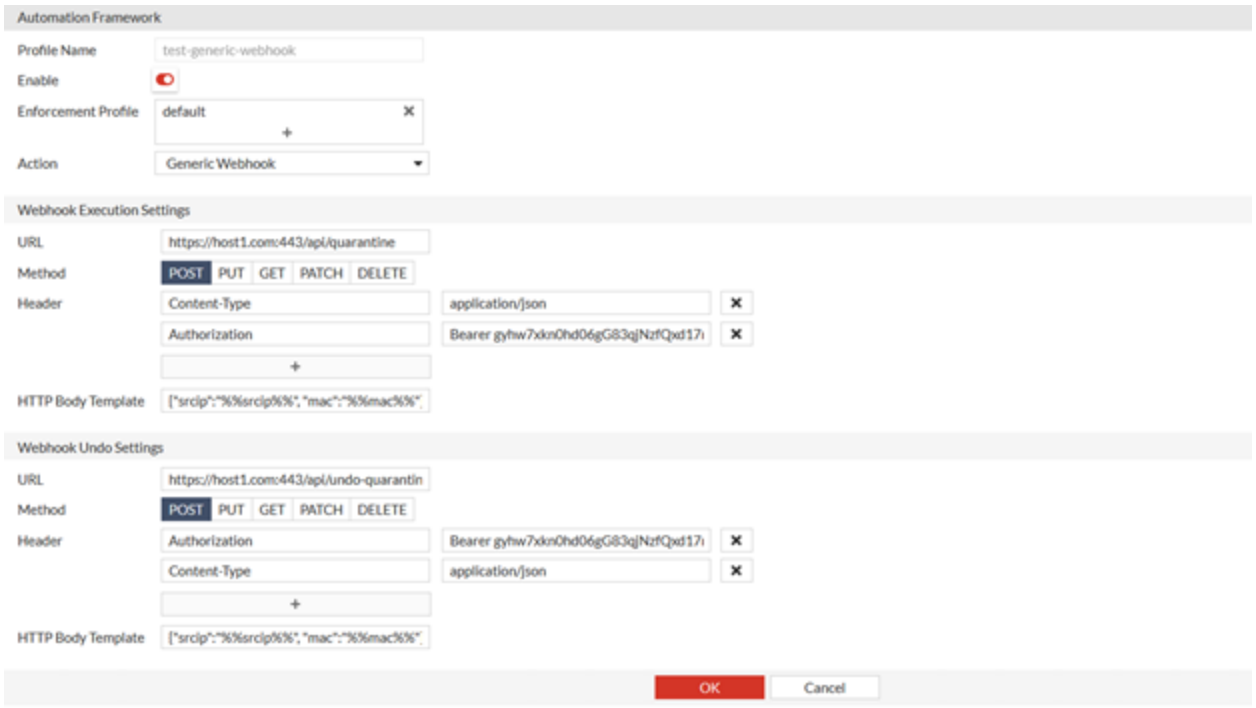


3. When response action has been triggered, the detected IP that needs to be quarantined will be sent to FortiNAC via FortiNAC's REST API call.

Generic Webhook setup example

Generic Webhook action makes HTTP requests to a specific server with custom headers, bodies, methods and URL. Please ensure API or webhook is enabled on the server side.

The HTTP body can use parameters from FortiNDR detection results. Wrapping the parameter with `%%` will replace the expression with the value for the parameter. The supported parameters are: `%%srcip%% and %%mac%%`

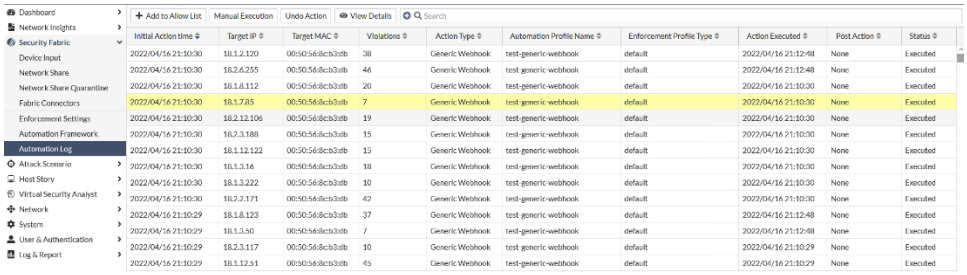


Automation log

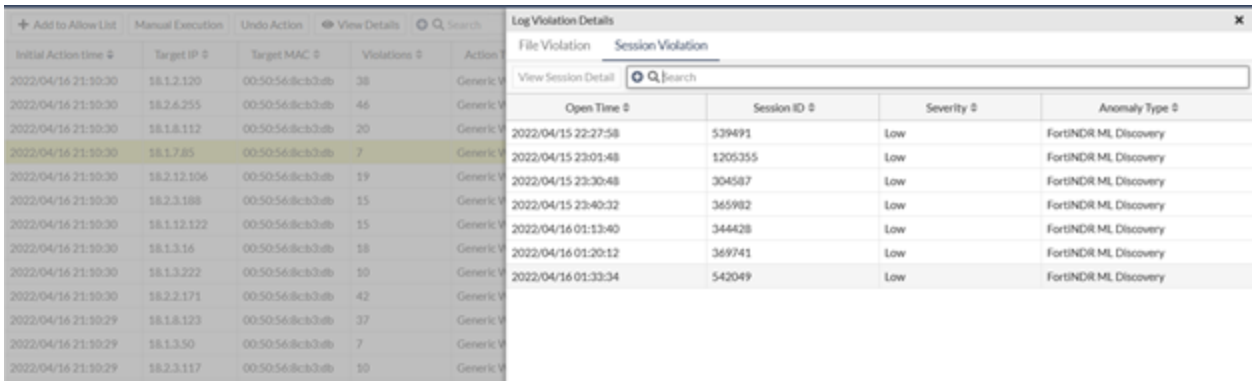
Automation Log records each enforcement action generated by FortiNDR.

The *Violations* column shows the total number of malware detections and NDR anomalies found on that target device. Double-click a log entry to see more details about the violation, such as malicious files that caused the violation. The number of violations is calculated within the digest cycle of 1 minute.

The *Enforcement Profile* column indicates which profile the enforcement settings set at the time the event is triggered.



Violation details



Automation Status and Post action

The following table is a summary of the *Status* and its relationship with *Post Action*. You can execute a post action by selecting an entry and clicking an action button above the table.

Status	Description	Possible Post Action
Active	When enforcement action fails, the system retries for five times. If the action succeeds, the *Status* changes to *Executed*. If the action fails, the *Status* changes back to *Active*.	None
Executed	Enforcement action succeeded.	Undo Action
Failed	Exceed the retry limit of five times.	Manual Execution
Duplicated	Another executed entry has been detected with same automation profile, target IP and target mac address.	None
Undo Success	Undo an enforcement action that succeeded.	None
Omitted	Action was prohibited from execution by restriction, for example, allow-listed.	Manual Execution

FortiSandbox integration (FortiSandbox 4.0.1 and higher)

The FortiSandbox deployment with an integrated FortiNDR can increase detection coverage and overall throughput. Submitted files goes through the following logic:

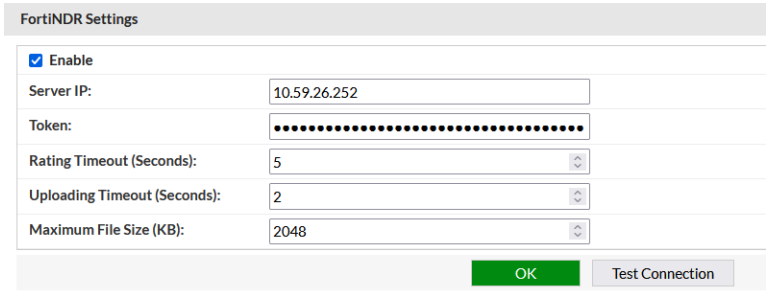
1. FortiSandbox performs its pre-filtering and Static Scan analysis. If any known malware is found, the result is returned.
2. When *FortiAI Entrust* is enabled under FortiSandbox *Scan Profile*, FortiSandbox sends the files to FortiNDR via API for FortiNDR's verdict of *malware* or *absolute clean*, and the result is returned. If a file is not *absolute clean*, then the next step is performed.
3. FortiSandbox performs its Dynamic Scan analysis to capture any IOC.

With this integration, FortiNDR reduces the load on FortiSandbox's Dynamic Scan and assists FortiSandbox with determining malware type, such as banking trojan, coinminer, and so on, based on the features observed.

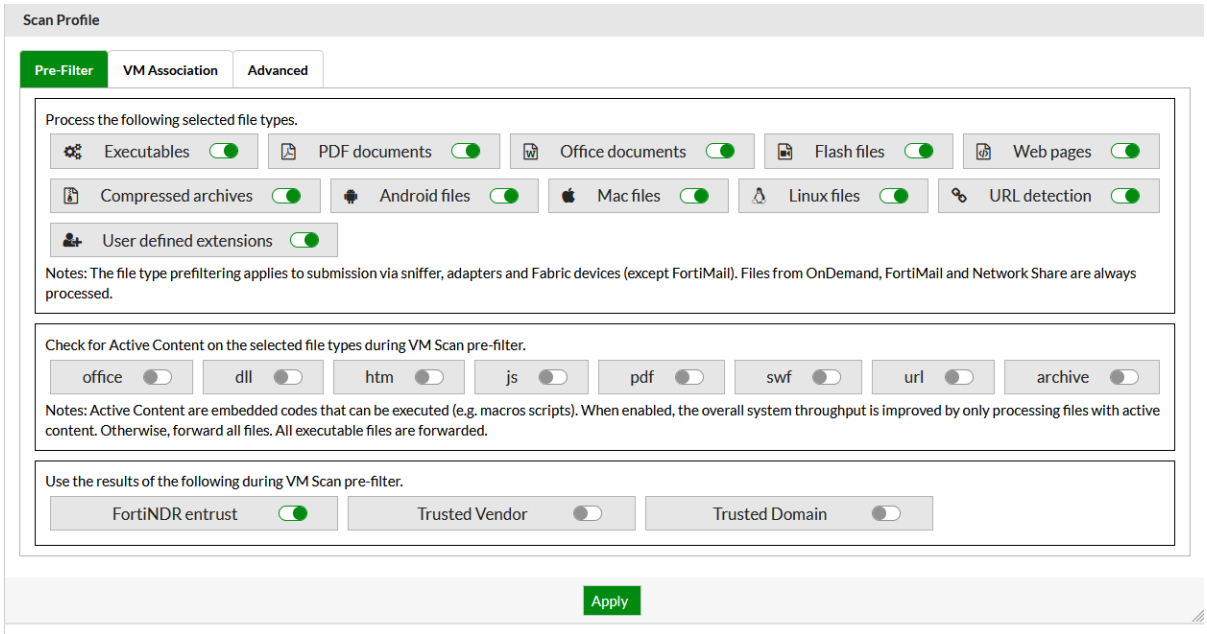
High level configuration steps are as follows:

1. Generate a FortiNDR API token associated with a user. You can use the GUI in *System* > *Administrator* or use the CLI command `execute api-key <user-name>` .
   For details, see Appendix A - API guide on page 163.
2. In FortiSandbox, configure FortiSandbox FortiAI settings using the FortiNDR IP address, token generated, and other parameters.
3. Click *Test Connection* and check that you get a message that *FortiNDR is accessible*.
4. Configure FortiSandbox scan profile to enable *FortiNDR Entrust*.
5. When file submission begins, FortiSandbox appears in FortiNDR in *Security Fabric* > *Device Input* in the *Other Devices* tab.
   You can review FortiNDR logs for submission details.

This is an example of the FortiSandbox FortiNDR setting.



This is an example of FortiSandbox Scan profile configuration with *FortiNDR Entrust*. When FortiSandbox is configured, it appears in FortiNDR under *Device Input*.

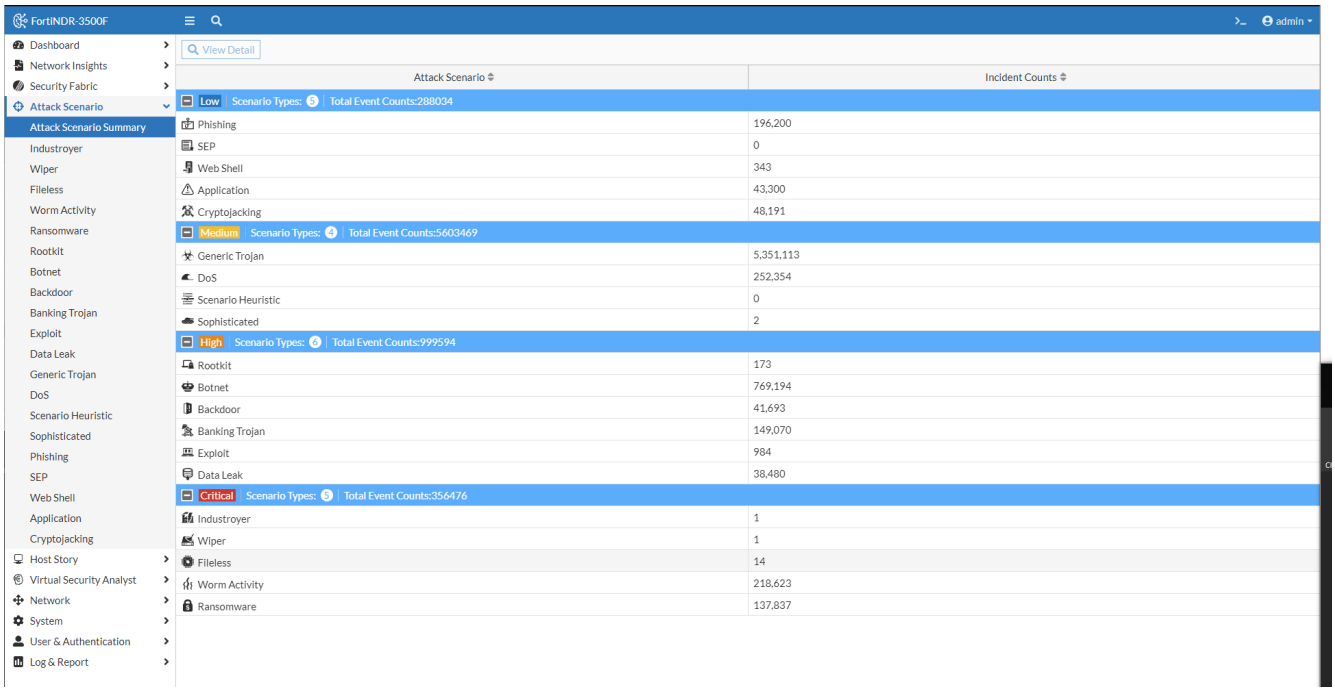


Attack Scenario

FortiNDR uses attack scenarios to identify malware attacks. FortiNDR scientifically classifies the malware attack times into attack scenarios, making FortiNDR your personal malware analyst on the network.

Most security technologies can only tell you that your network is infected with virus names without much context. FortiNDR moves beyond that to tell you exactly what the malware is trying to achieve providing SOC analysts more insightful information for their investigation.

The *Attack Scenario Summary* counts the number of incidents of all the attack scenario types. They are organized into *Critical*, *High*, *Medium*, or *Low* severity.



Scenario types

FortiNDR can detect the following attack scenarios:

Severity	Scenario	Description
Low	Cryptojacking	Cryptojacking is a type of cybercrime where a malicious actor uses a victim's computing power to generate cryptocurrency.
Low	Application	A broad category of software that might download and install additional, unwanted software that could perform activities not approved or expected by the user.

Severity	Scenario	Description
Low	Web Shell	A script that can be uploaded to a web server to allow remote administration of the machine. Infected web servers can be Internet-facing or internal to the network where the web shell is used to pivot further to internal hosts.
Low	SEP	Attackers use Search Engine Poisoning to take advantage of your rankings on search engine result pages.
Low	Phishing	A fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising itself as a trustworthy entity in an electronic communication.
Medium	Sophisticated	Malware that contains more than one attack scenario.
Medium	Scenario Heuristic	Scenario heuristic identifies applications or software that demonstrates an array of suspicious traits.
Medium	DoS	This can access connection handling remotely, perform denial of service, or distributed DoS.
Medium	Generic Trojan	Any malicious computer program which misleads users of its true intent.
High	Banking Trojan	Malicious software that can access confidential information stored or processed through online banking systems.
High	Backdoor	This can give a hacker unauthorized access and control of your computer.
High	Data Leak	A data leak is when sensitive data is exposed physically on the Internet where malicious actors can access it.
High	Rootkit	Software tools that enable an unauthorized user to get control of a computer system without being detected.
High	Exploit	A piece of software, a chunk of data, or a sequence of commands that uses a bug or vulnerability to cause unintended or unanticipated behavior on computer software, hardware, or something electronic, usually computerized.
High	Botnet	A botnet is a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker.
Critical	Ransomware	Malicious software that can block access to a computer system until money is paid.
Critical	Fileless	A variant of computer-related malicious software that is exclusively a computer memory-based artifact.
Critical	Wiper	Malware that erases contents in the hard disk of an infected computer. It's usually designed to destroy as many computers as possible inside the victim's networks.
Critical	Industroyer	A malware framework originally designed to deliver specific

Severity	Scenario	Description
		cyberattacks on power grids. The recent generation of this malware has also started to target industrial control systems.
Critical	Worm Activity	A worm is capable of spreading itself to other systems on a network.

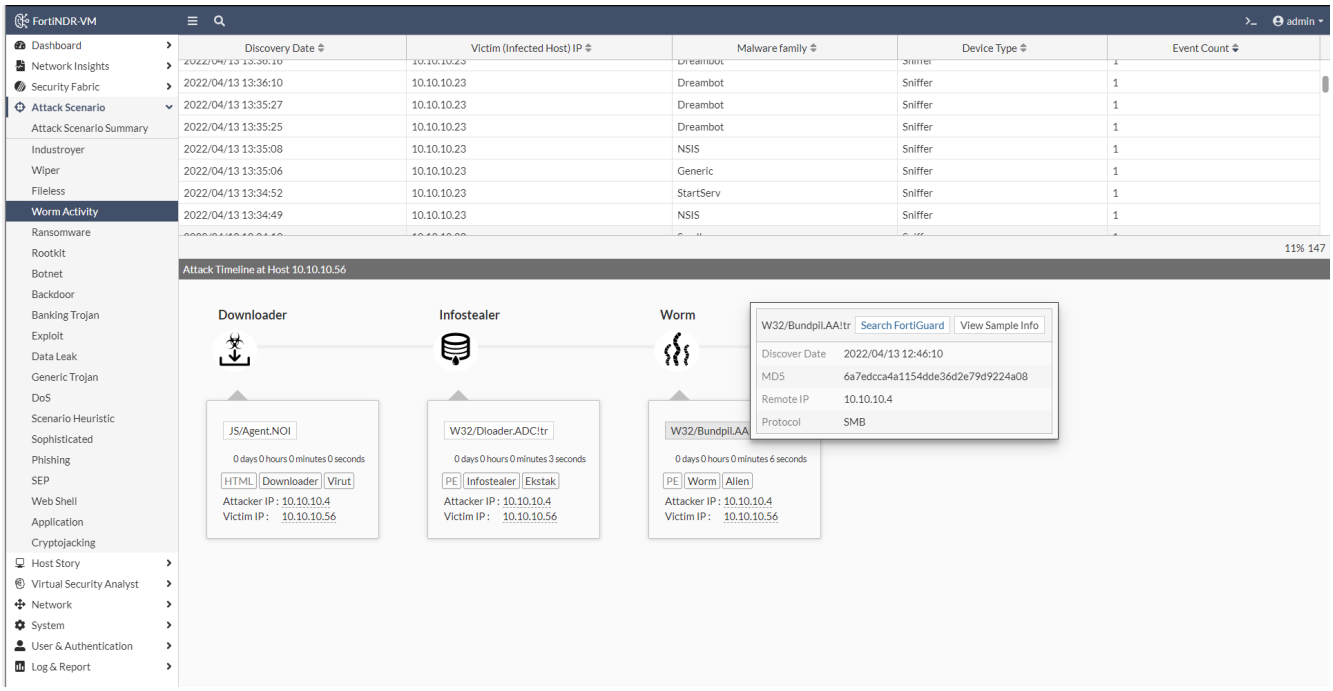
Attack scenario navigation and timeline

When there is an attack, infections often spread quickly and tracing the source (patient zero) can be very difficult for SOC analysts. FortiNDR Virtual Analyst is a scenario-based AI engine that can quickly locate the origin of the attack. This saves time during breach investigation, typically shortening it from days to seconds. FortiNDR helps analysts deal with the source of the problem in a timely manner.

Attack Scenario displays the victim IP addresses with the time of detection. Click the IP address to display the timeline of events as well as a graphical interpretation of an attack.

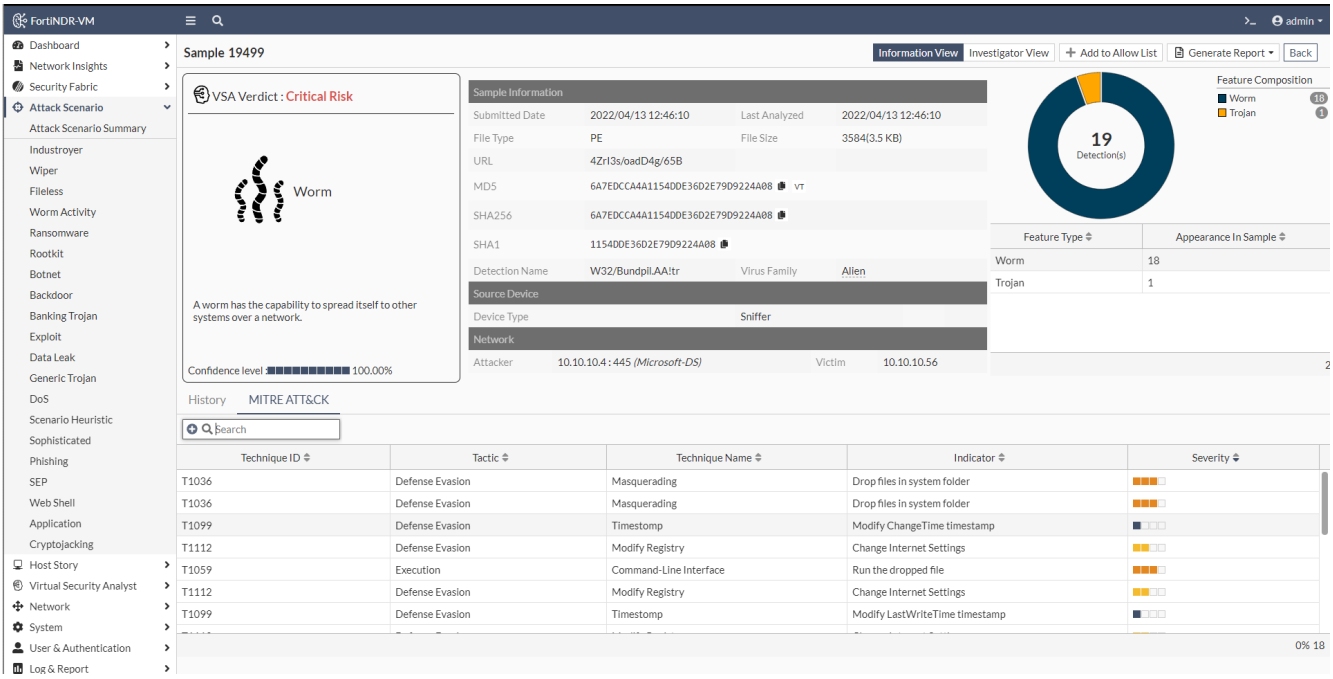
The following is an example of a worm infection. The virtual analyst shows the remote IP address where the attack originated, the timeline, and other malicious files discovered on the infected host, and the worm activity shows it is trying to spread.

In the *Attack Timeline* frame, hover over a detection name to view more information about the infection. Use the *Search FortiGuard* shortcut to look up the detection at FortiGuard's threat encyclopedia. Use the *View Sample Info* shortcut to view details of the detected file.

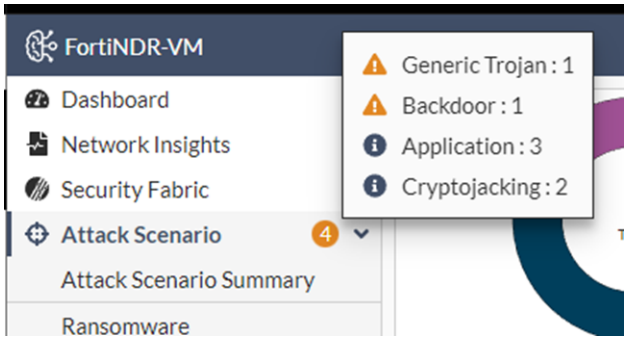


You might see the same IP address multiple times. This indicates that that IP address has been detected for the attack type multiple times, for example, ransomware.

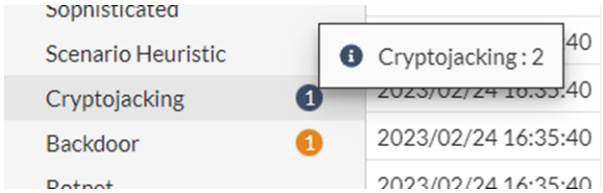
The following example shows a Sample Information page of the W32/Bundpil.AA!tr captures in the attack timeline.



The number displayed within the Attack Scenario bubble indicates the total number of attack types. Hovering over the bubble will reveal a detailed distribution of the attacks.



In the following example, the number displayed within the *Cryptojacking* bubble indicates the total types of severity of this type of attacks. Hovering over the bubble will reveal a detailed distribution of the attack in groups of severity.



Understanding kill chain and scenario engine

One of the strengths of FortiNDR is the ability to trace the source of a malware attack. In all attack scenarios, especially with worm, ransomware, and sophisticated attacks, there are often timeline and multi-stage kill chain type graphics. When there is a detection, the scenario engine tries to form a multi-stage scenario based on time and similarity of attacks. The maximum trace-back period is five days.

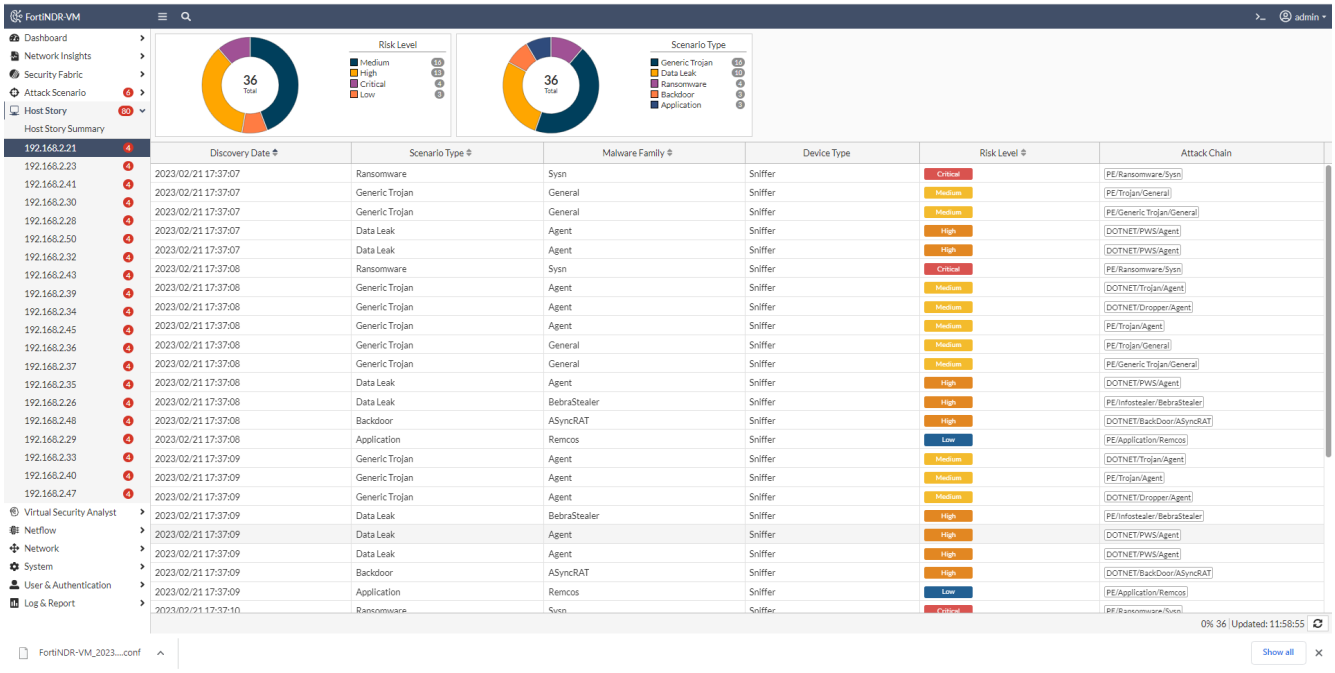
When ransomware is detected, the scenario engine goes back to see if there are other events such as dropper or downloader that happened before to the same victim. If the scenario engine cannot form a multi-stage attack, then it displays a single scenario.

Most attack scenario names are self explanatory as the sophisticated scenario engine searches for multiple payloads of the same attack. For attacks that do not fall under obvious scenarios, they are grouped under the attack scenario called *Scenario Heuristics*.

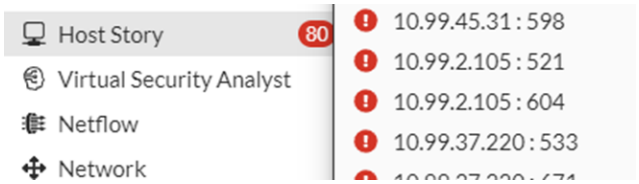
Host Story

Host Story organizes malware attacks by host IP address while *Attack Scenario* organizes malware attacks by attack type. The *Host Story* view helps you examine the host to see when the infections first took place. For example, a host might be obviously infected with ransomware because a ransomware note is displayed on the end user machine. However, many people might not know that the ransomware came from a dropper/downloader which can download malicious files to the same host. Providing a timetable based on host information allows SOC analysts to understand the attack by timeline, for example, a dropper might be sleeping in the PC for days until C&C kicks in to download other malicious code. Double-click each detection row to understand what was happening during this attack.

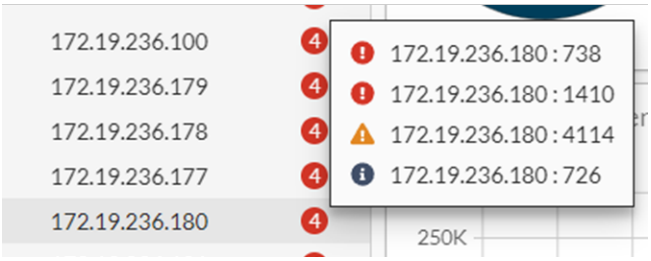
The *Host Story* summary page shows incident counts grouping by severities for each infected host.



The *Host Story* bubble displays the total number of hosts that have been attacked. Hovering over the bubble reveals a detailed distribution of the attack count for each individual host.



The bubble next to host *172.19.236.180* in the following example indicates the number of attack severity types found on that specific host. Hovering over the bubble reveals a detailed distribution of each severity type.


172.19.236.100
172.19.236.179
172.19.236.178
172.19.236.177
172.19.236.180
172.19.236.180 : 738
172.19.236.180 : 1410
172.19.236.180 : 4114
172.19.236.180 : 726
250K

Virtual Security Analyst

This section includes the following topics.

Express Malware Analysis

Use *Express Malware Analysis* to quickly upload a file to get the verdict. *Express Malware Analysis* is supported in both the GUI and the API. The default file size limit is 200MB. The file size limit can be changed using the CLI.

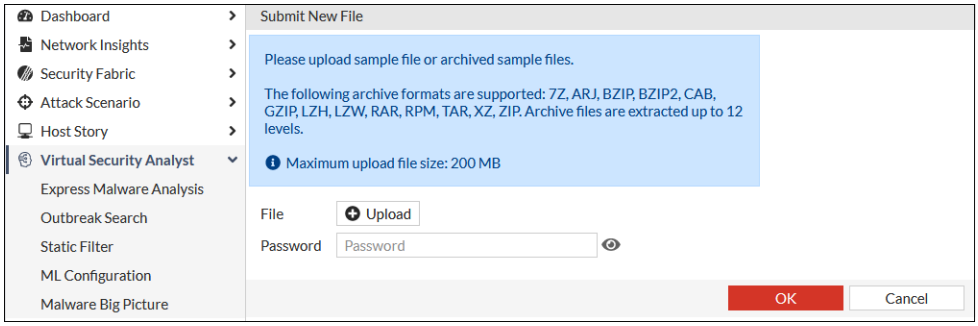
For information about using the API to submit files, see Appendix A - API guide on page 163 > Submit files.

To change the file size limit with the CLI:

```
execute file-size-threshold
```

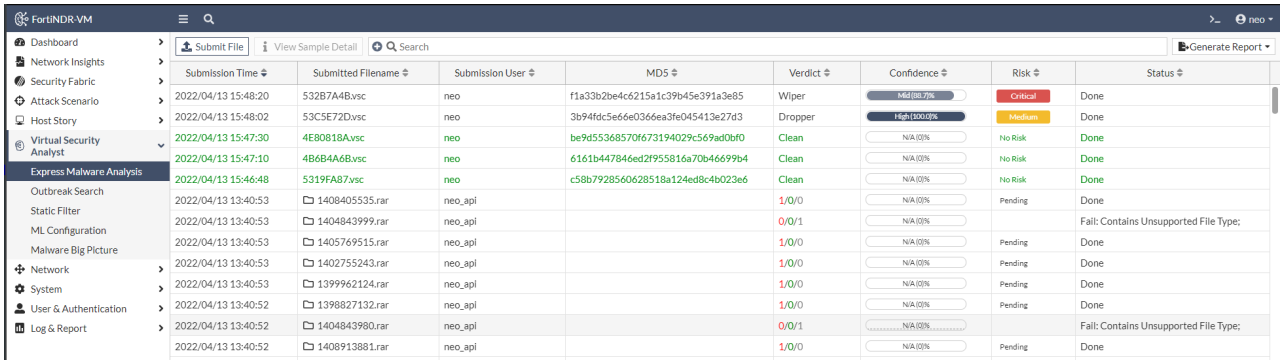
To submit a file for Express Malware Analysis:

1. Go to *Virtual Security Analyst* > *Express Malware Analysis*. The *Submit New File* window opens.



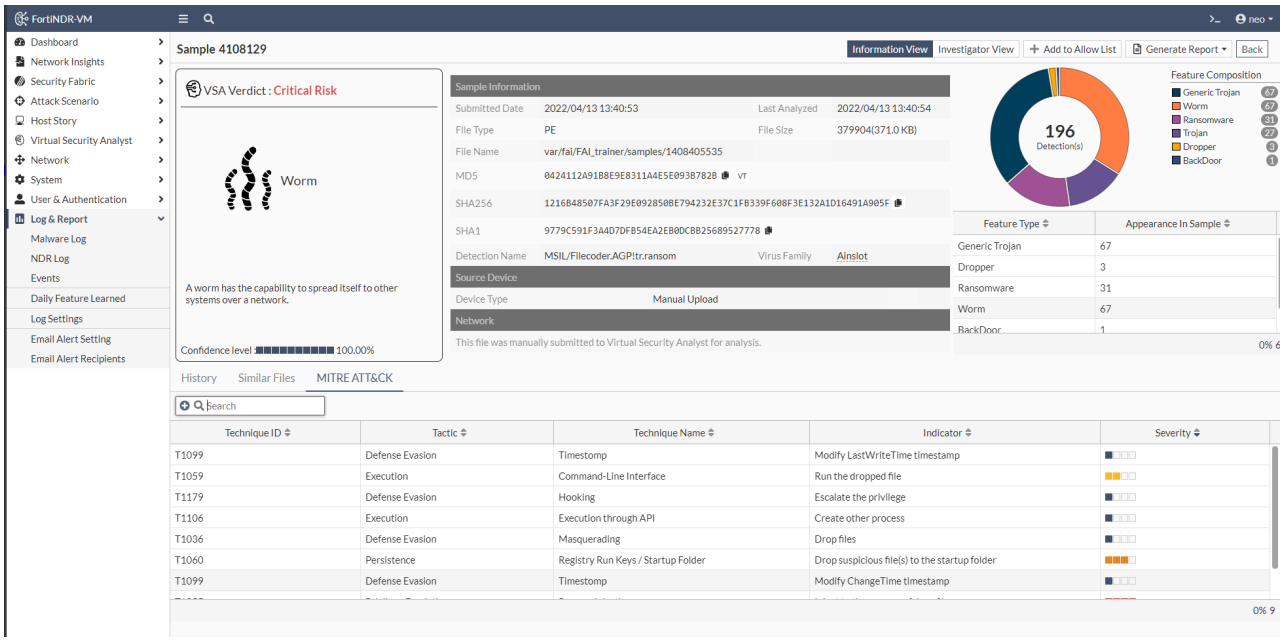
2. In the *Password* field, enter the password for the file. If the file does not require a password, FortiNDR will use *Infected* by default. The Password field is displayed whether the file requires a password or not.

3. Click *Upload* and then click *OK*. The verdict is displayed.

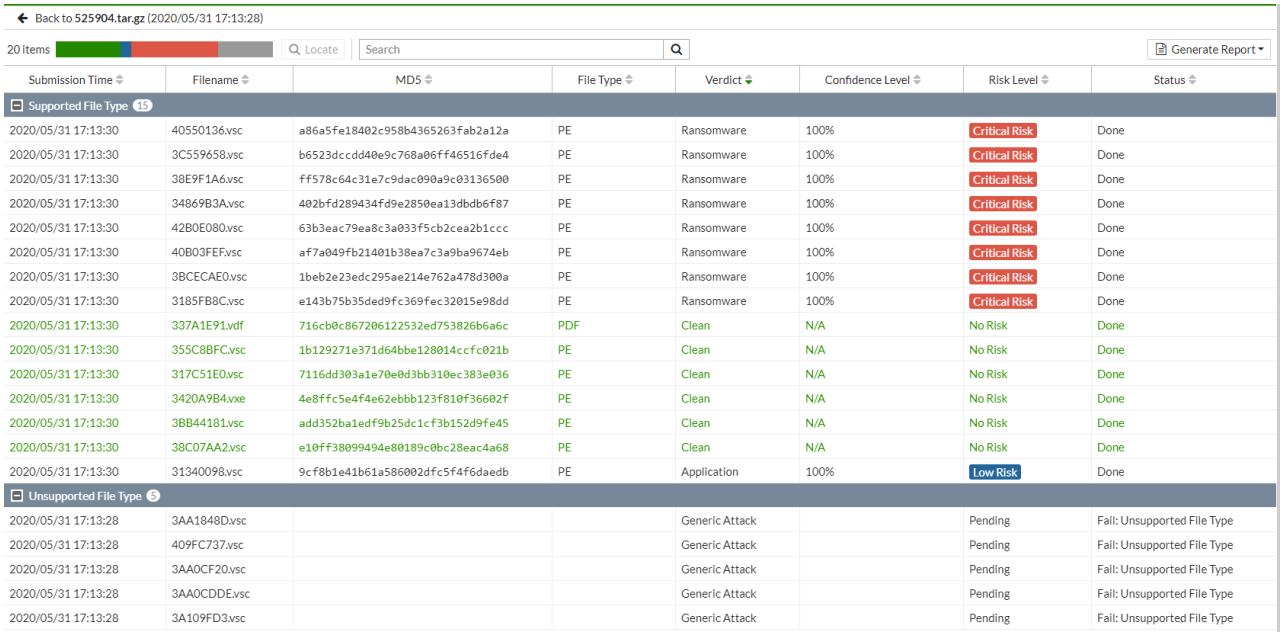


4. Click *View Sample Detail* to view the sample information. This page explains the verdict by showing the feature composition of the file.
   There are four tabs at the bottom of the page:

Tab	Description
History	Displays the history of the same malware (by hash) on the network. FortiNDR does not go back and rescan files based on the previous verdict. If you want to rescan a file based on the latest ANN, use manual or API upload instead.
Similar files	FortiNDR has a similar engine analysis based on the features detected. This is useful for detecting similar variants of the original malware.
MITRE information (and Investigator view)	For Portable Executable (PE) files, FortiNDR can display a drill down of the MITRE ATT&CK matrix that shows the TTPs used for a particular malware.
IOC (Indicators of Compromise)	For text-based malware, FortiNDR can display more contextual information of malware, such as *file contain abnormal javascipt*, and so on. This helps you understand why FortiNDR determines it is malware.



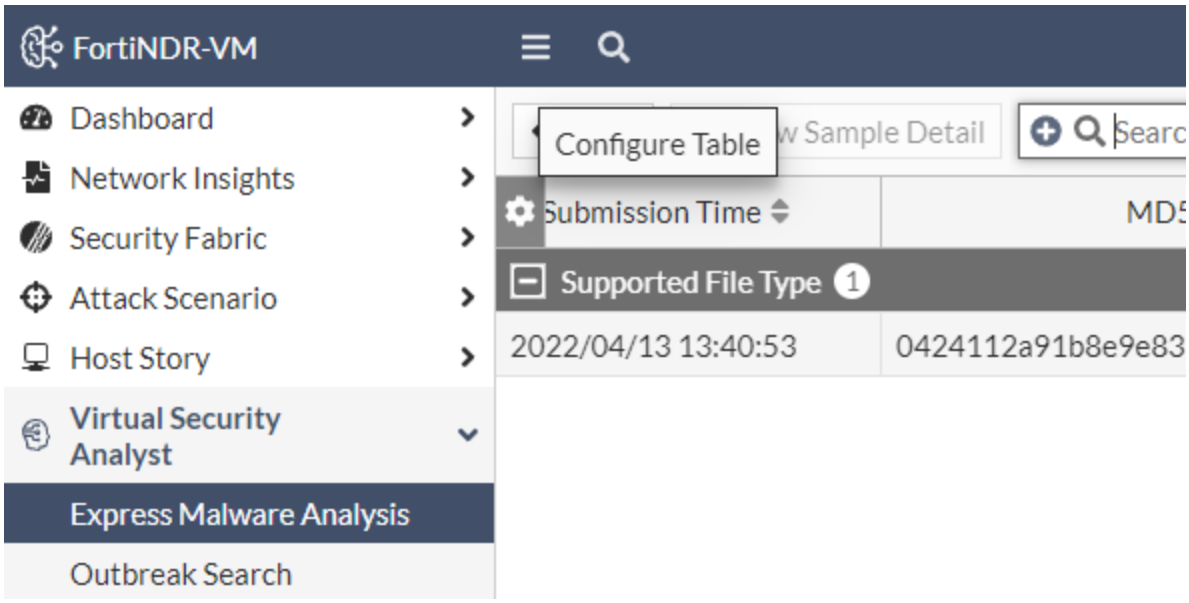
When a zip file is uploaded, double-click the entry to view the contents and verdict of the files.



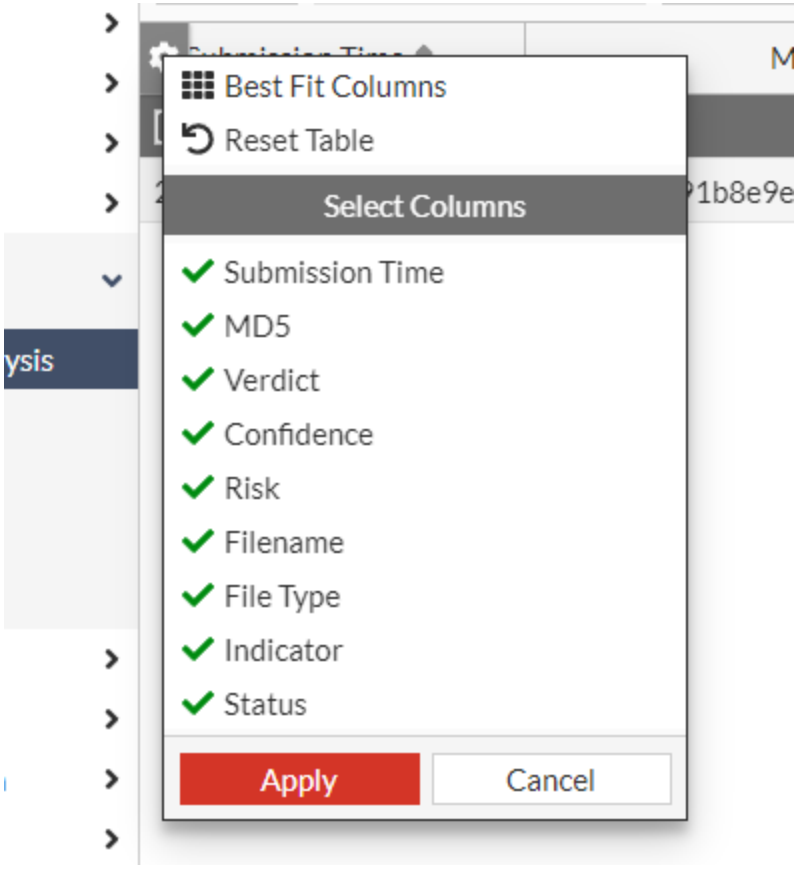
5. (Optional) Click *Generate Report*to view the report summary in PDF and JSON format.

Configuring the table

You can show or hide columns by clicking the gear icon in the header.



Click *Configure Table* to select the columns you want to show or hide.

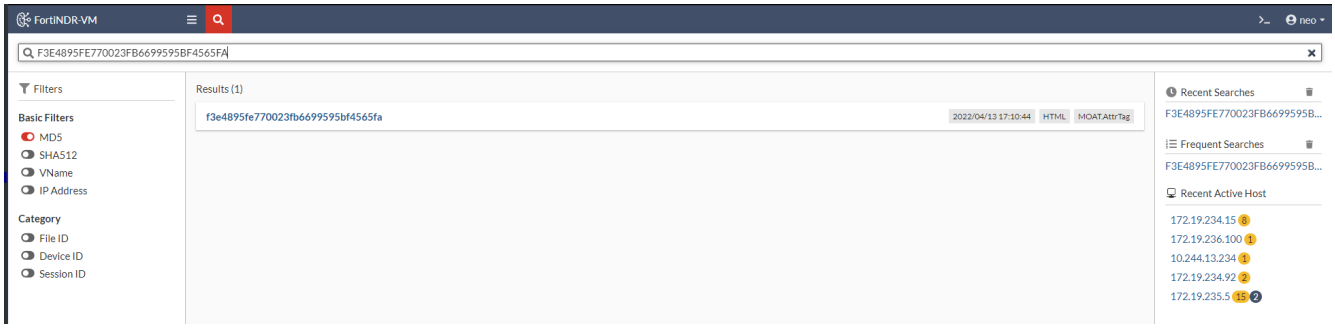


Outbreak Search

Virtual Security Analyst > *Outbreak Search* contains tools to determine if there is an outbreak in the network. FortiNDR lets you deal with an outbreak from two directions.

1. Using a known hash in the FortiNDR database or a physical copy of a file that belongs to the outbreak, you can search for other captured files that share similarities. See Search lead type of hash or detection name on page 90.
2. Using a known outbreak name or known virus family identifier, you can search for captured files that were grouped under the same categories by FortiNDR. See Search lead type of outbreak name on page 91.

You can also use quick search in the button bar at the top to search for and access sample profile pages. You can search by hash (MD5 or SHA512) or by exact detection name. If the search returns more than 10 results, there is a *View More* button and you are redirected to *Advance Threat report* with the search criteria inserted.



Search lead type of hash or detection name

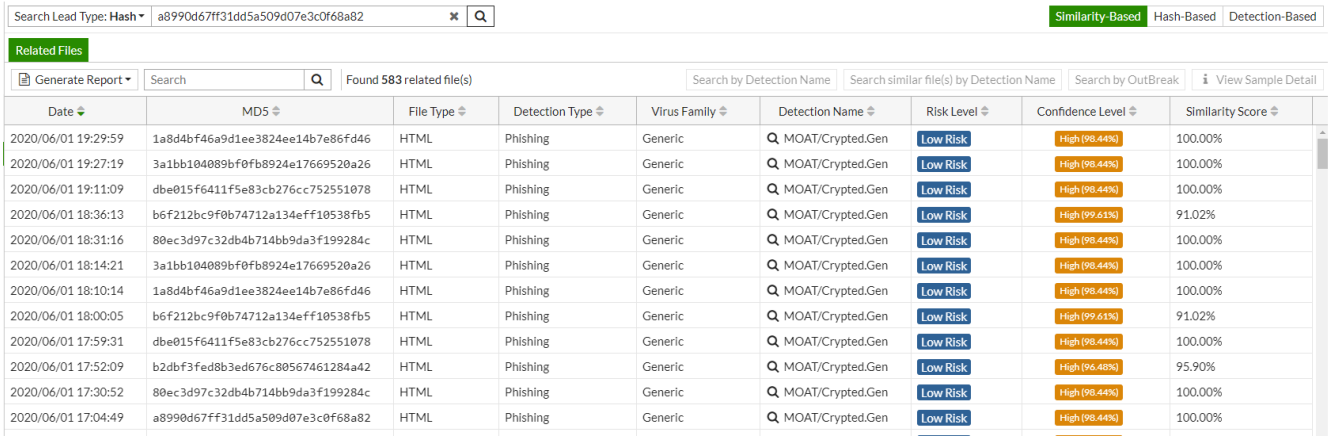
This search lead type accepts MD5 or SHA512 as a search value. You can submit the sample to FortiNDR in *Express Malware Analysis*. When the search lead type is detection name, the search value can be an exact detection name, such as W32/Phishing.DDS!tr, or a detection name with wildcards, such as W32/Phishing.%.

For these searches, you must choose one of these search methods: *Similarity-Based*, *Hash-Based*, or *Detection-Based*.

Similarity-Based search uses FortiNDR's similarity engine to search for files that have similar features to the input file. Outbreak search only returns samples with a similarity rate of over 77%.

Hash-Based search returns results based on hash matches. If search lead type is detection name and you select hash-detection, the search returns files that match the hashes of all the files with the input detection name. The result might include files from different detection names because the detection name can change over time.

Detection-Based search matches the input sample by detection name with or without wildcards. If search lead type is hash and you select *Detection-Based* search, the result returns files that share the same hash as the input detection name. Because detection names can change over time, this search lets you explore other detection names that are used to detect the same outbreak.



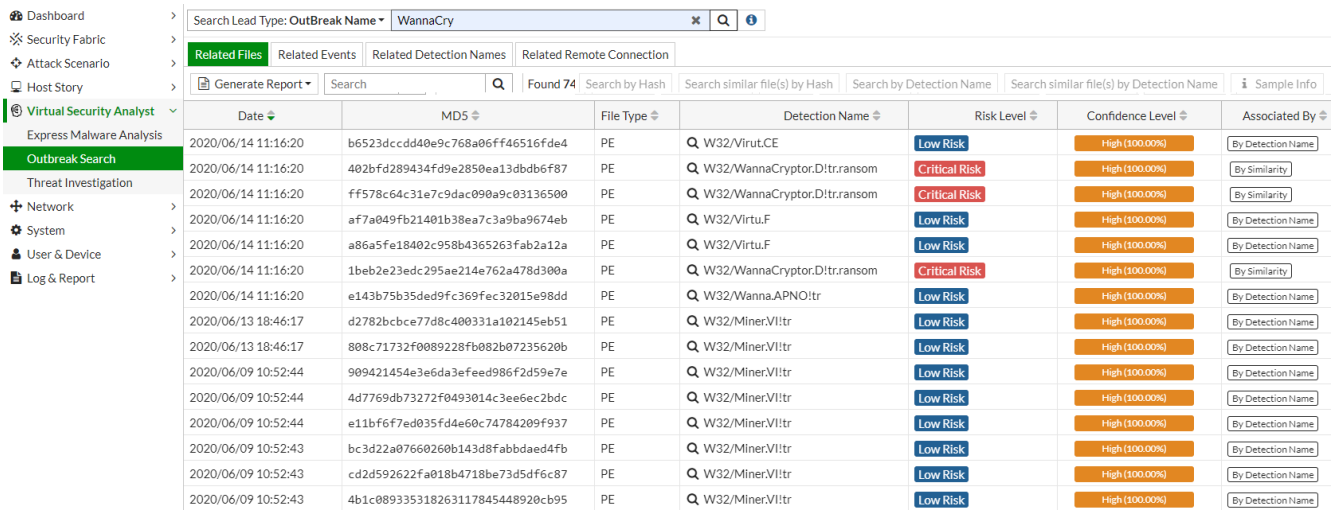
Date	MD5	File Type	Detection Type	Virus Family	Detection Name	Risk Level	Confidence Level	Similarity Score
2020/06/01 19:29:59	1a8d4bf46a9d1ee3824ee14b7e86fd46	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 19:27:19	3a1bb104089bf0fb8924e17669520a26	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 19:11:09	dbe015f6411f5e83cb276cc752551078	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:36:13	b6f212bc9f0b74712a134eff10538fb5	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (99.61%)	91.02%
2020/06/01 18:31:16	80ec3d97c32db4b714bb9da3f199284c	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:14:21	3a1bb104089bf0fb8924e17669520a26	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:10:14	1a8d4bf46a9d1ee3824ee14b7e86fd46	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:00:05	b6f212bc9f0b74712a134eff10538fb5	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (99.61%)	91.02%
2020/06/01 17:59:31	dbe015f6411f5e83cb276cc752551078	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 17:52:09	b2dbf3fed8b3ed676c80567461284a42	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (96.48%)	95.90%
2020/06/01 17:30:52	80ec3d97c32db4b714bb9da3f199284c	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 17:04:49	a8990d67ff31dd5a509d07e3c0f68a82	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%

Search lead type of outbreak name

When you use outbreak name as a search lead time, FortiNDR returns the following:

1. Any sample that matches FortiNDR's virus family classification (detection subtype).
2. Any sample that matches part of the detection name.
3. Any sample that shares any similarity with any of the files above.

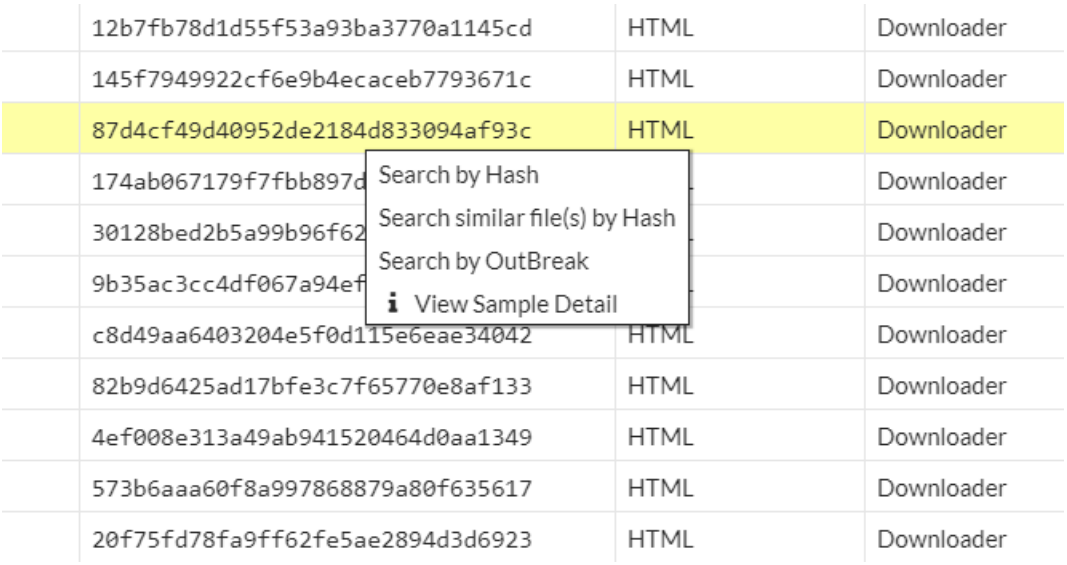
These files are listed in the *Related Files* tab. Other tabs that have a summary of the detection name, remote connections, and attack scenarios events.



Date	MD5	File Type	Detection Name	Risk Level	Confidence Level	Associated By
2020/06/14 11:16:20	b6523dccdd40e9c768a06ff46516fde4	PE	W32/Virut.CE	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	402bfd289434fd9e2850ea13dbdb6f87	PE	W32/WannaCryptor.D!tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	ff578c64c31e7c9dac090a9c03136500	PE	W32/WannaCryptor.D!tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	af7a049fb21401b38ea7c3a9ba9674eb	PE	W32/Virtu.F	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	a86a5fe18402c958b4365263fab2a12a	PE	W32/Virtu.F	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	1beb2e23edc295ae214e762a478d300a	PE	W32/WannaCryptor.D!tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	e143b75b35ded9fc369fec32015e98dd	PE	W32/Wanna.APNO!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	d2782bcbce77d8c400331a102145eb51	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	808c71732f0089228fb082b07235620b	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	909421454e3e6da3efeed986f2d59e7e	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	4d7769db73272f0493014c3ee6ec2bdc	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	e11bf6f7ed035fd4e60c74784209f937	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	bc3d22a07660260b143d8fabbdaed4fb	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	cd2d592622fa018b4718be73d5df6c87	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	4b1c089335318263117845448920cb95	PE	W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name

Recursive searches

You can right-click any file in the result and perform other types of searches. This feature lets you find more information that goes beyond the first degree of relationship in an outbreak.



Reports

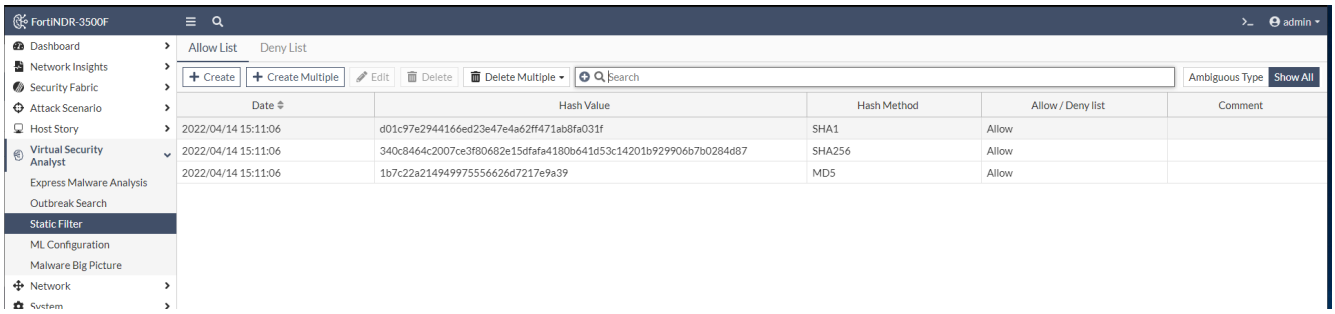
You can generate a PDF report of the verdict that includes the file's comprehensive information and analysis together with a list of similar files found on the system. Reports can be in PDF, CSV, JSON, or STIXv2 format.

Static Filter

Use the *Static Filter* to manage an allow hash list and a block hash list. This is useful when dealing with outbreaks, for example, inserting an outbreak malware hash for FortiNDR to identify as malicious. An example of the opposite use case is if there are certain files administrators determine are clean, hashes in the allowlist are not processed by ANN and AV, and FortiNDR marks them as clean.

The *Static Filter* contains two lists of file hashes, allowing input of MD5, SHA1, and SHA256 hashes that can alter the verdict of incoming samples.

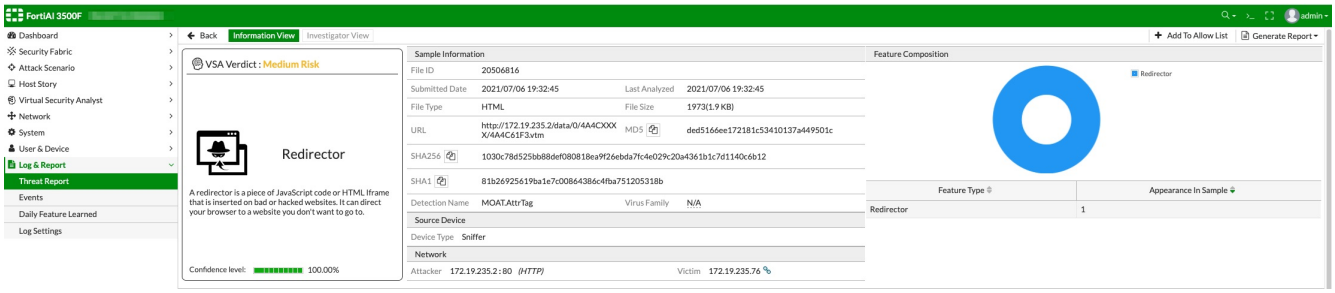
- Files with hashes in the *Allow List* are marked as *Clean*.
- Files with hashes in the *Deny List* are marked as *Malicious* and tagged with a *Detection Name* of `StaticFilter.AI.D`.



The effect of the static filter is prospective. It will only apply to samples received after the filter is added. Adding a duplicate hash entry updates the filter's timestamp to the current date.

For clashes, such as the same entry in both the *Allow List* and *Deny List*, FortiNDR flags the entry with *Ambigious type* filter so that you remove the conflicting entry.

Log & Report > *Threat Report* has a button for you to easily add or remove an entry to the *Allow List* or *Deny List*.



ML Configuration

Use the *ML Configuration* page to view and edit the machine learning baseline features for the traffic anomaly detection, as well as the status of the baseline training.

Key concepts

- **Baseline Status**: *Baselining* means the current training is still in progress.
- **Baseline ready**: Means the baseline training is done and is ready for anomaly detection.

The following features are enabled by default: *Source Device IP*, *Destination Device IP*, *Destination Device Geolocation*, *Transport Layer Protocol*, *Application Layer Protocol*, *Protocol/Application Behaviors/Action*, *Destination Port*.

We do not recommend editing these features, unless you have strong understanding of what they do.

ML Configuration contains the following settings:

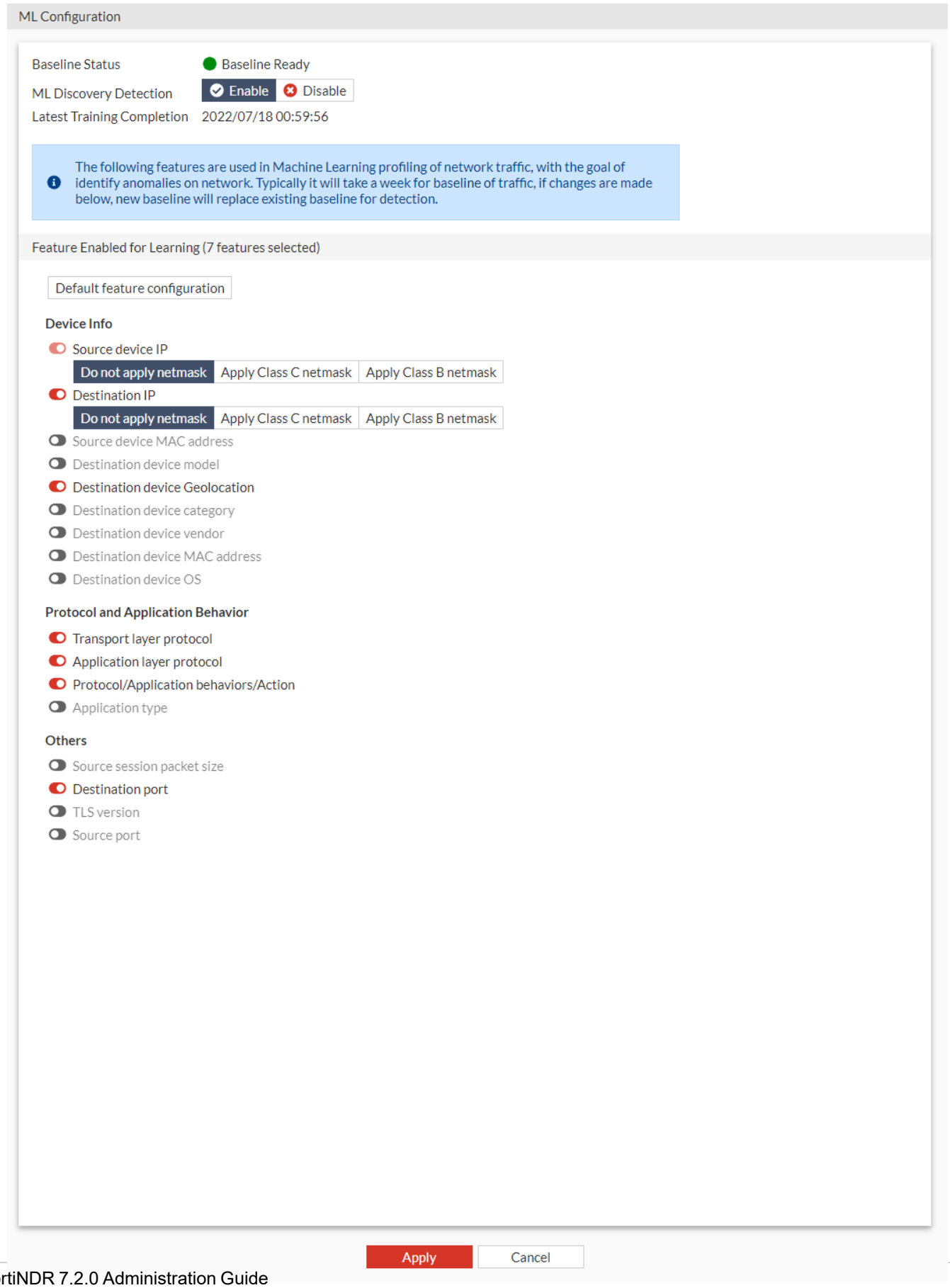
Device Info	
Source Device IP	The Source Device IP. Apply a netmask if you do not want to treat certain range changes in the IP as an anomaly.
Destination Device IP	The Destination Device IP. Apply netmask if you don't want to treat certain range change in the IP as anomaly
Destination MAC Address	Destination device MAC address.
Destination Device Model	Device model such as: *FortiGate*, *Workstation*, *IDRAC*, etc.
Destination Device Geolocation	Device geographical country such as *United States*.
Destination Device Category	Device category such as: *NAS*, *Virtual Machine, Firewall*, etc.
Destination Device Vendor	Device vendor such as *VMware*, *Dell*, *Synology*, etc.
Destination Device OS	Device Operating system such as *Windows*, *Linux*, etc.

Protocol and Application behavior	
Transport Layer Protocol	UPD, ICMP, TCP, etc
Application Layer Protocol	TLS, HTTP, SMB, etc
Protocol/Application Behaviors/Action	Specific application actions such as. *Adobe Reader form creation*, *WebDAV reload*, *Wasabi file upload*, etc

Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, *22*, *445*, *none reserved port*, etc.
TLS Version	The TLS version if TLS is being used.

Typically, it will take 7 days for baseline of traffic. Choosing different features to train new baseline will cause the ML system start another 7 day training period. The old baseline is discarded during the re-training. You will not be able to get ML detection during that time.

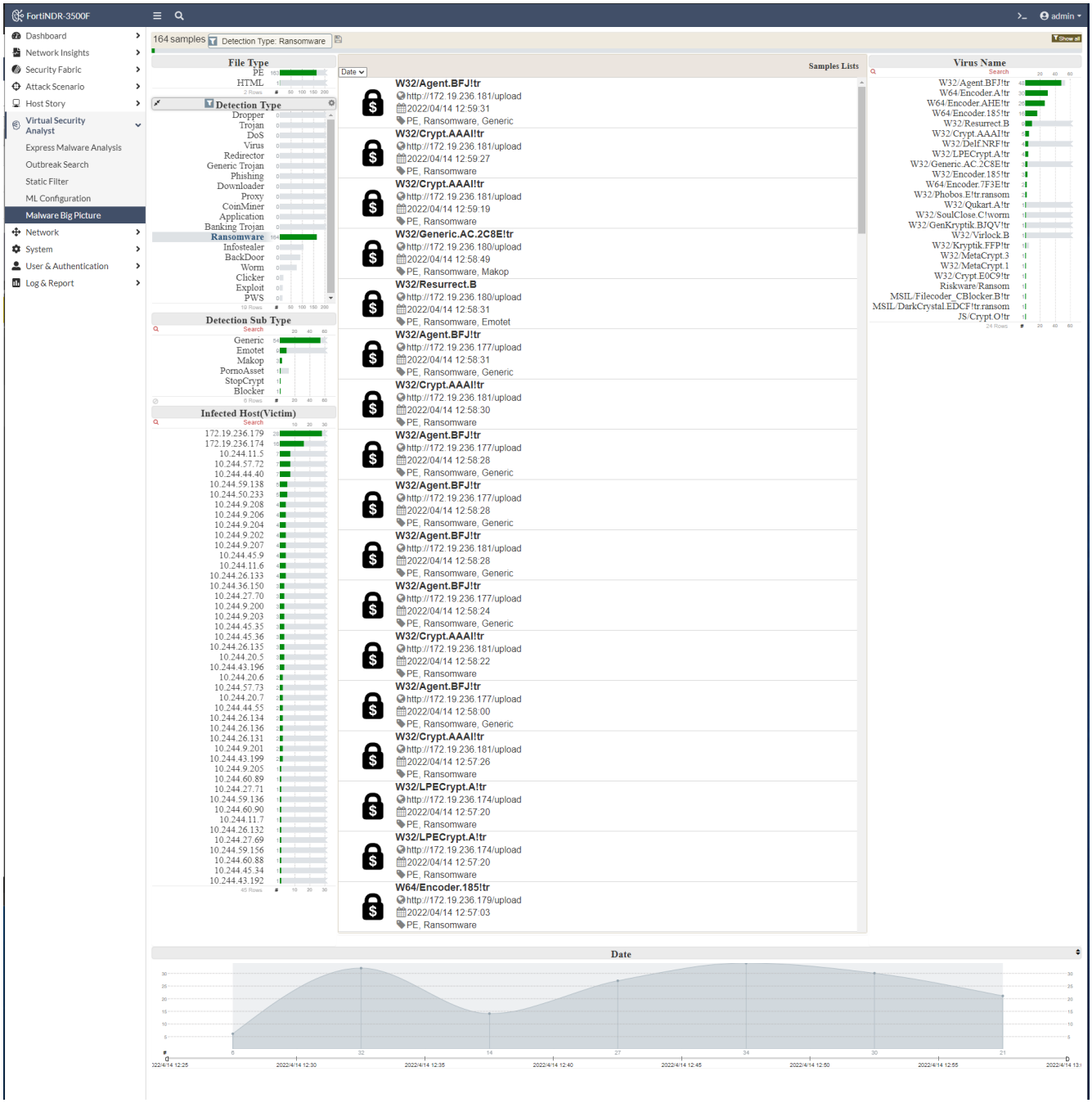
The CLI command `execute reset-ml-baseline-time` can be used to shorten the baselining time and commit training. For details , see the *FortiNDR CLI reference guide*.


ML Configuration
Baseline Status
Baseline Ready
ML Discovery Detection
Enable
Disable
Latest Training Completion
2022/07/18 00:59:56
The following features are used in Machine Learning profiling of network traffic, with the goal of identify anomalies on network. Typically it will take a week for baseline of traffic, if changes are made below, new baseline will replace existing baseline for detection.
Feature Enabled for Learning (7 features selected)
Default feature configuration
Device Info
Source device IP
Do not apply netmask
Apply Class C netmask
Apply Class B netmask
Destination IP
Do not apply netmask
Apply Class C netmask
Apply Class B netmask
Source device MAC address
Destination device model
Destination device Geolocation
Destination device category
Destination device vendor
Destination device MAC address
Destination device OS
Protocol and Application Behavior
Transport layer protocol
Application layer protocol
Protocol/Application behaviors/Action
Application type
Others
Source session packet size
Destination port
TLS version
Source port
Apply
Cancel

Malware Big Picture

Malware Big Picture proves useful for forensic analysis to assess damage to the network. This big picture view includes information such as detection time, =detection type and sub type. You can click a type to filter it.

The image below is an example a Ransomware filter. Infected IP addresses with Ransomware are highlighted. SOC analysts can view the infected hosts.

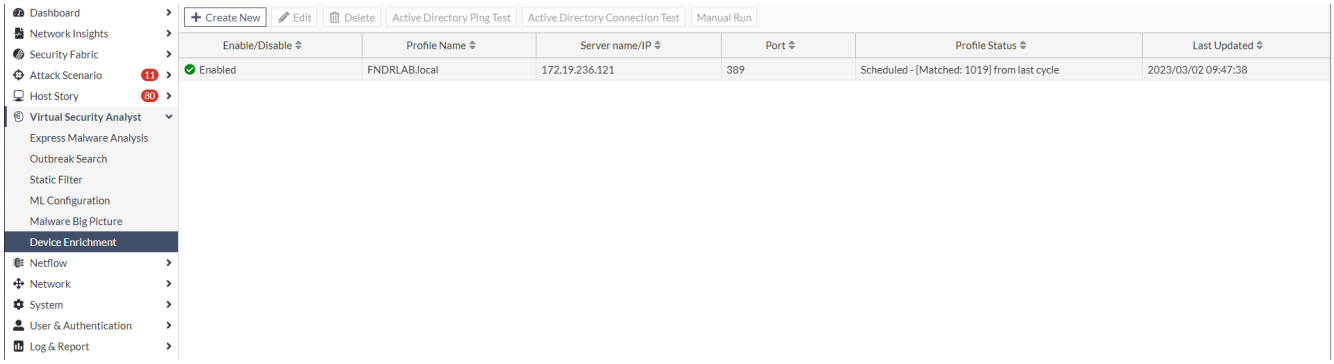


Device Enrichment

You can improve the Device Identifier by creating a *Device Information Enrichment Profile* that will retrieve Hostname information from the Windows Active Directory (AD) and DNS server of the target network. When the profile is enabled, the device enrichment process will run according to the scheduled cycle in the profile. You can also execute the profile manually.

After a cycle is completed, the Device Enrichment process will schedule a new cycle according to the profile. If the current cycle is not completed before the next scheduled cycle is to start, the enrichment process will skip the next cycle. For example, if you scheduled a cycle to run every hour, and the current cycle takes 120 minutes to run, the process will schedule the next cycle one hour after the current 120 minute cycle is finished running.

During the enrichment process, DNS Queries are fetched in batches via UDP. If there are failed queries in the batch, the system will retry three times before moving on to the next batch.

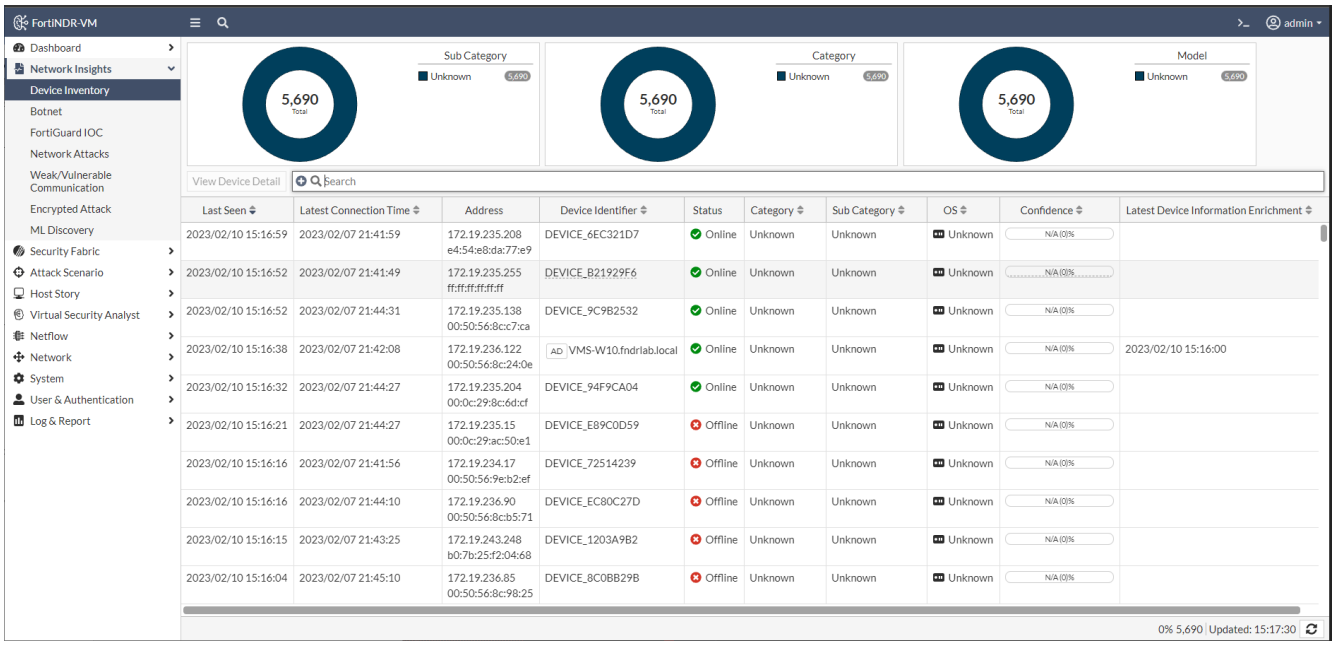


The *Device Enrichment* page displays the following information:

Enable/Disable	Indicates if the profile is enabled or disabled.
Profile Name	The name assigned to the profile.
Server name/IP	The IP address of the windows AD server or domain name.
Port	The port used by the profile. If SSL is enabled the port is 636 otherwise the default is 389.
Profile Status	After the first run is performed, the status changes to *Completed* with the previous running result. *Matched Count* is the number of IPs returned from the DNS server that matched the IPs in the Device inventory.
Last Updated	The date and time the device enrichment was updated.

Viewing the retrieved device identifier

If a new hostname is found, the device identifiers on the *Device Inventory* page and *Device Log Page* are replaced with the latest hostname found from AD and an icon (AD) appears next to the new identifier. The *Device Enrichment* time can be found at the *Latest Device Enrichment Column*. This column is disabled by default.

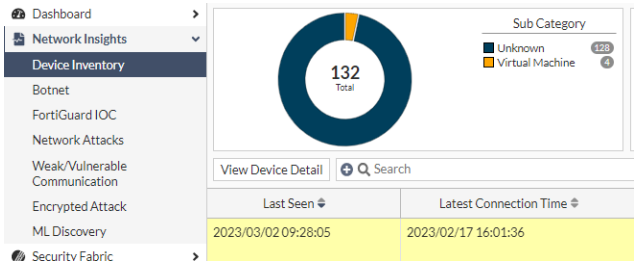


Overwriting the device identifier

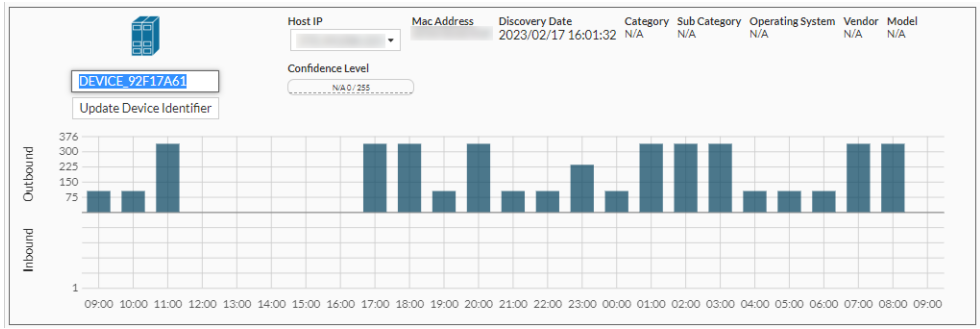
You can manually overwrite the device identifier in the device information page.

To overwrite the device identifier:

1. In the *Network Insights* module, select a device and click *View Device Detail* or *View Device*. The *Information* page opens.



2. Edit the device name and click *Update Device Identifier*.



Creating a Device Enrichment Profile

To create a Device Enrichment profile:

1. Go to *Virtual Security Analyst* > *Device Enrichment*.
2. In the toolbar, click *Create New*. The *Add New Device Enrichment Configuration* page opens.
3. Configure the profile settings.

Enable Device Configuration	Disable and enable the profile
Profile Name	Unique identifier for the Microsoft Active Directory Connection Profile
Microsoft Active Directory Connection Settings	
Sever name/ IP	Enter either the IP address of the windows AD server or domain name.
Enable SSL	SSL port and protocol to be use when selected
Base DN	The starting point of the LDAP Server for user authentication within the directory. For example, `DC=example-domain, DC=com`
Bind DN	The LDAP user and its LDAP directory tree location for binding. For example, `CN=fndr_svc,CN=testUser, DC= example-domain,DC= com`.
Bind Password	The password for the LDAP user account for binding. For example, `DC= example-domain,DC= com`.
Search Scope	The method of retrieving the information from the tree: • *Base*: only retrieve information from the base level of the directory tree specified in search base • *One Level*: only retrieve information from the search base and one level down • *Subtree*: retrieve everything underneath the specified search base
Search Base	The starting point of the directory tree for retrieving information
DNS Server Settings	
DNS Server	DNS Server is required as part of the enrichment process involved querying DNS server with hostnames to retrieve current IP address.
Automation	
Scheduling	• *Every*: the enrichment cycle will be preformed once right after the profile is saved. The next cycle will be run after the amount of hours user input • *Daily*: the enrichment cycle will start every day at the input time • *Weekly*: the enrichment cycle will start weekly at the input time.

4. Click *OK*.

Active Directory Profile Actions

Use the Active Directory Profile Actions in the toolbar to test the connect or run the Device Enrichment Profile.

Active Directory Server Ping Test	Ping the Active Directory (AD) server and port in the Device Enrichment Profile.
Active Directory Server Connection Test	Verify the *Microsoft Active Directory Connection Settings* by attempting to connect the AD server.
Active Directory Server Manual Run	Execute the selected Device Enrichment Profile . The result will be shown as a notification on the bottom left.

Netflow

NetFlow is a generic network protocol for collecting information about network traffic. It provides data about the source, destination, and volume of network traffic and is used for network monitoring, analysis and security purposes. The information collected by NetFlow can be used to monitor network usage, detect anomalies, and identify security threats.

FortiNDR supports receiving direct NetFlow flows from the following protocols and versions:

- NetFlow v5, v9 or IPFIX flow records, SFlow.

The FortiNDR needs to access to FDS server to verify the NetFlow license once before the initial use of this feature.

To turn NetFlow on/off with the CLI:

```
execute netflow <on>/<off>.
```

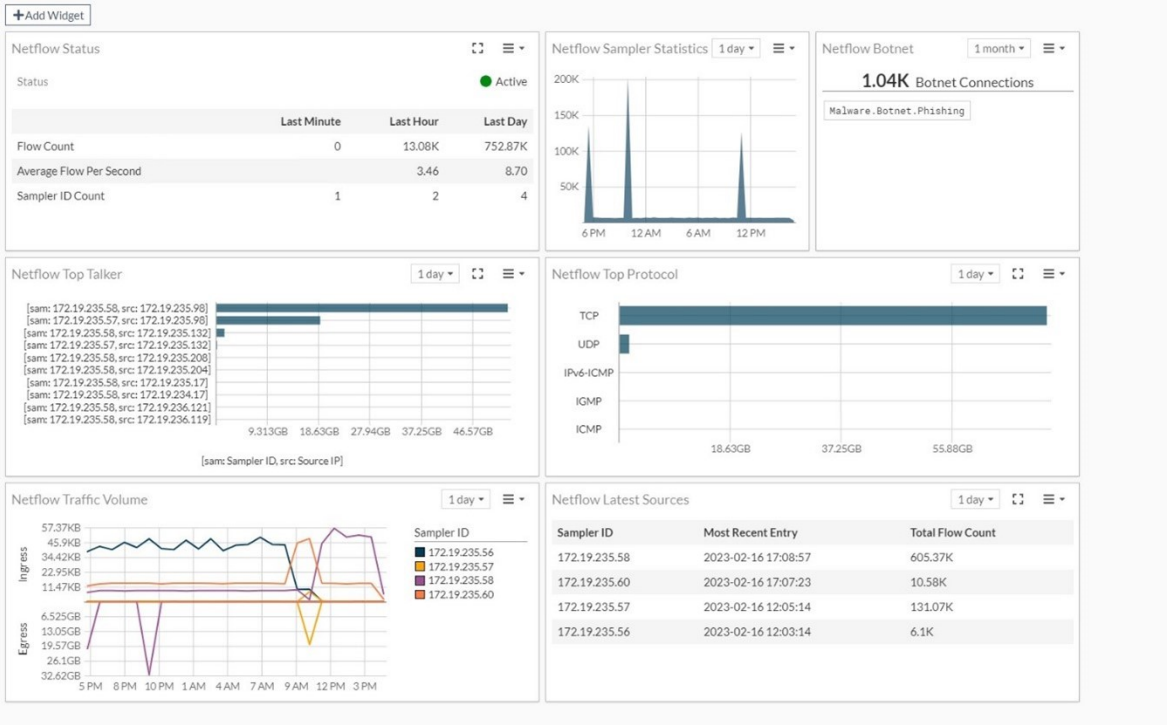
NetFlow ports

To use this feature, point your flow collector to FortiNDR's IP and port. The ports used by FortiNDR to listen on NDR flows are:

- UDP/2055: IPFIX, NetFlow
- UDP/6343: SFlow
- UDP/9995: NetFlow v5

Netflow Dashboard

The *Netflow Dashboard* provides an overview of NetFlow traffic statistics.



The *Netflow Dashboard* contains the following widgets:

Netflow Status	Displays the *Status* of this feature , *Flow Count*, *Average Flow Per Second* and *Sampler ID Count*. The statistics are broken down into last minute, hour, and day for users to view the volume and flow count coming into FortiNDR.
Netflow Botnet	Displays the Netflow botnet traffic detections. Netflow botnet detections are matched against the FortiGuard botnet database. Discovery of botnet detections are matched against destination IPs and ports within a flow. Click the widget to expand it to view a more detailed page about the detections.
Netflow Sampler Statistics	Displays the flow count over time.
Netflow Top Talker	Displays the IP addresses that are responsible for the most network traffic in a given time period. The *Top Talker* feature provides a method to identify the devices or IP addresses that are consuming the most bandwidth, allowing network administrators to troubleshoot performance issues and optimize network usage.
Netflow Top Protocol	Displays the most used transportation layer protocols in terms of bandwidth consumption. Protocols can include TCP, UDP, ICMP, among others. The *Top Protocols* feature provides a method for understanding which protocols are using the most bandwidth, helping network administrators optimize network usage and potentially identify security concerns.
Netflow Latest Sources	Displays the Flow activity statistics from active samplers within a selected time frame. The widget allows users to select one day, one week, or one month.
Netflow Traffic Volume	Displays aggregated Ingress and Egress traffic volume of each Sampler within a selected time frame.

For example, if sampler ID *1.1.1.1* has flows from different source(s) and destination(s), the widget will summarize the total ingress and egress traffic.

Customizing the Netflow Dashboard

You can add or remove widgets from the dashboard, or re-size a widget to fit the dashboard.

To remove a widget from the dashboard:

Click the widget menu and select *Remove*.

Alternatively, you can click *Add Widget* in the banner and then click the *Remove* button next to the widget name in the *Add NDR Dashboard Widget* pane.

To add a widget to the dashboard:

1. In the banner, click *Add Widget*. The *Add NDR Dashboard Widget* pane opens.
2. Click *Add* next to the widget name and the click *OK*.

To re-size a widget in the dashboard:

In the widget menu, click *Resize* and then select the widget length.

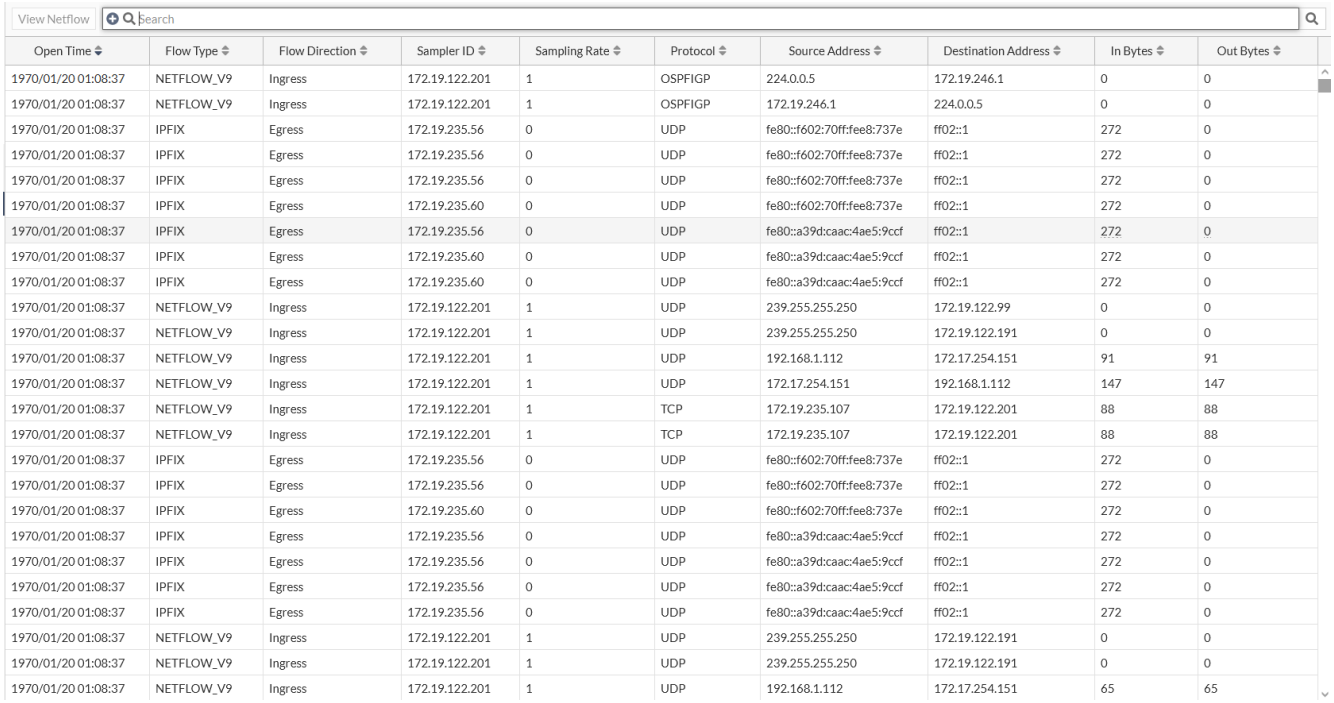
Netflow Log

Netflow Log shows the logs FortiNDR collected. You can view the Netflow for each entry or double-click an entry to view more information for each log. The *Flow Types* filters can be: NETFLOW_V5, NETFLOW_V9, IPFIX, SFLOW_5. The Flow Types filters are case sensitive.

The flow type may not appear under *Suggestions* because the suggestions are picked from the first 1000 records in the beginn of the page. The list will be enlarged as you scroll down the page.

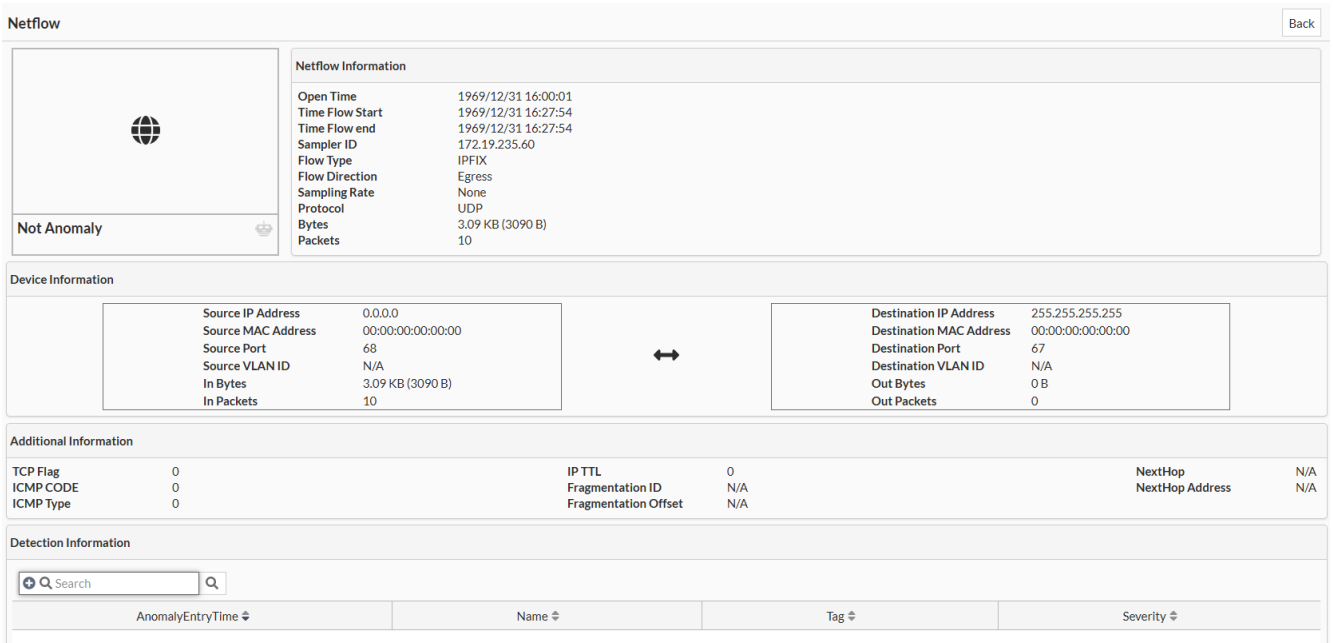
Netflow Log shows the logs FortiNDR collected. You can view the Netflow for each entry or double-click an entry to view more information for each log.

You may notice some columns are have *0*s in them. This means this column is not applicable to that type of flow or the sampler/exporter is not configured to send this field to FortiNDR. For example, NetFlow_v5 does not include *Destination MAC*, so you will see `00:00:00:00:00:00` in the *NetFlow_v5* column.



Viewing anomalies

To view the Netflow anomalies, select an entry in the table and click *View Netflow*.



The anomalies page displays the following information:

Not Anomaly/Anomaly	Indicates if FortiNDR determined the session to be an anomaly.

Netflow Information	Displays information about the sessions duration, Sampler ID, the flow type, direction and rate, as well as the protocol and the number of bytes and packages.
Device information	Displays information about the flow source and destination including the IP and MAC addresses, ports, VLAN ID and the number of bytes and packages.
Additional Information	Displays information about TCP, ICMP Fragmentation and NextHop.
Detection Information	Displays the *Anomaly Entry Time*, *Name* , *Tag* and *Severity*.

Network

Use the *Network* options to configure system settings such as configuring interfaces, DNS, and static routes.

Interface

FortiNDR has the following preset ports which cannot be changed.

Port (interface)	Type	Default open ports
Port1	10GE copper 10G	Management port. TCP 443 (HTTPS and GUI), TCP 22 SSH (CLI).
Port2	10GE copper 10G	Sniffer port (default).
Serial / Com1	Serial port	9600 baud, 8 data bits, 1 stop bit, no parity, XON/XOFF.
Port3 and Port4	1GE IPMI (Intelligent Platform Management Interface)	Disabled (default).
Port 5-8 (FortiNDR-3500F gen3)	Fiber 10G SFP+	Sniffer port (default)

DNS and Static Routes

Use the *DNS* and *Static Routes* pages to configure DNS and routing entries.

System

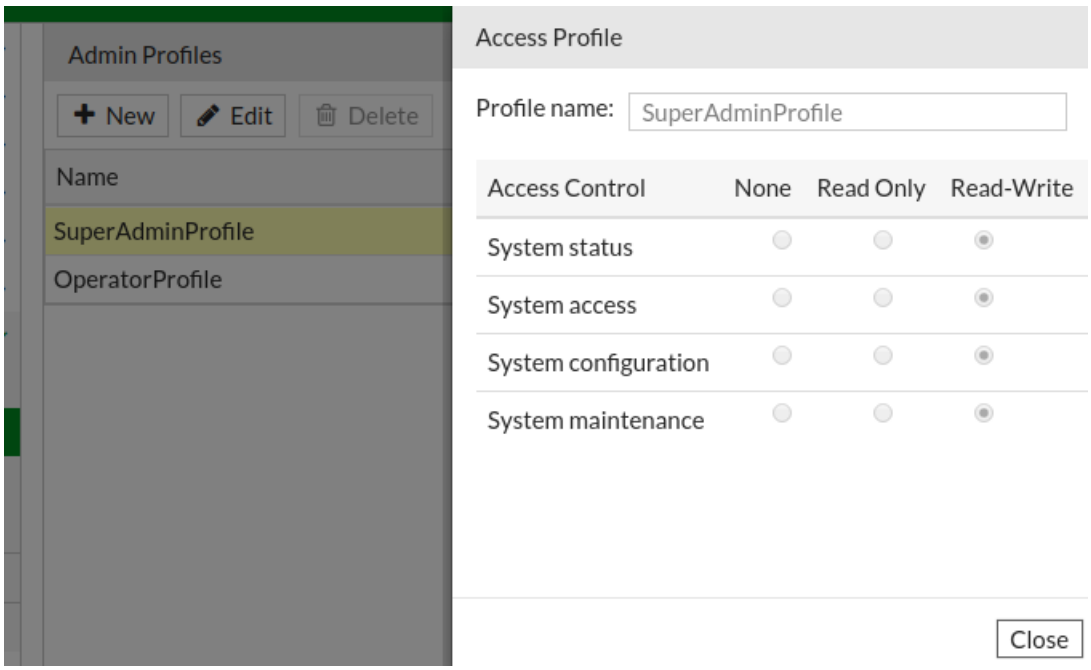
Use the *System* options to configure system settings.

It is recommended that you create a system backup file as part of your maintenance plan. Always perform a backup before upgrading firmware or making major system configuration changes. Save these configuration backups to your local computer in the event that you need to restore the system after a network event. For information, see Backup or restore the system configuration on page 113.

Administrator and Admin Profiles

FortiNDR supports local and remote authentication for administrators via LDAP and RADIUS. You can create *Administrator* accounts with an *Admin Profile* that allows access to selected areas.

An *Admin Profile* has the following *Access Control* options.



Firmware

Use the Firmware page to update or restore the system firmware. Downgrading to previous firmware versions is not supported.

Due to some database changes, after upgrade from 7.0.0 to 7.0.2, users will need to execute a CLI to clean up historical NDR log entries. Note this will clear all NDR logs, but malware logs will remain.

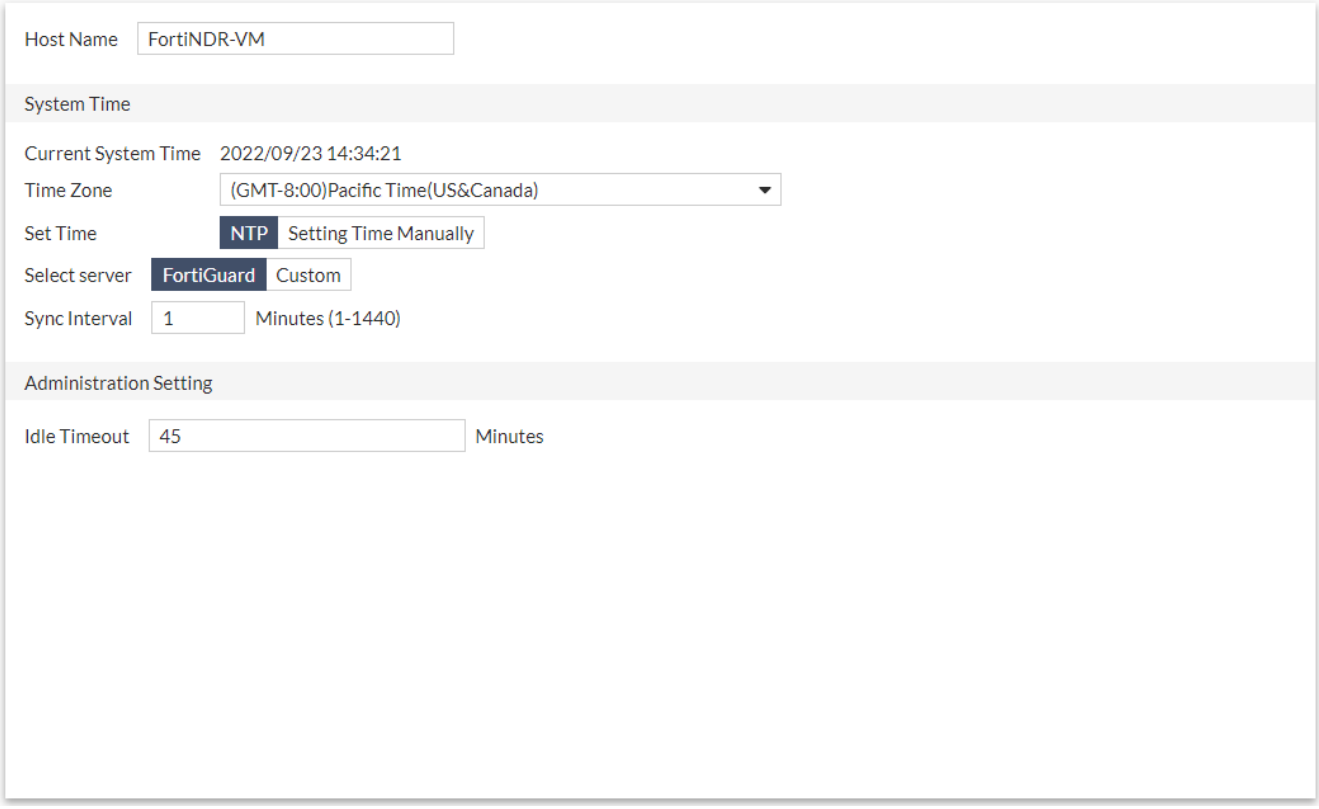
```
execute cleanup ndr
```

To update or restore the system firmware:

1. Locate and download the firmware file in the Fortinet support website.
2. Go to *System* > *Firmware*.
3. Click *Upload* and navigate to the firmware file on your computer and click *Open*.
4. Click *OK*.

Settings

Use *System* > *Settings* to configure the Host Name, set the system time and the idle timeout.



Host Name	The Host Name for the device.

System Time	
Current System Time	The current system time.
Time Zone	Select the time zone from the drop down list.
Set Time	Select *NTP* or select *Setting Time Manually* and then enter the *Date* and *Time*.
Select Server	Select *FortiGuard* or select *Custom* to add or remover the *Server*.
Sync Interval	Select a value between 1-1440 minutes.
Administration Setting	
Idle Timeout	Enter the idle timeout value in minutes.

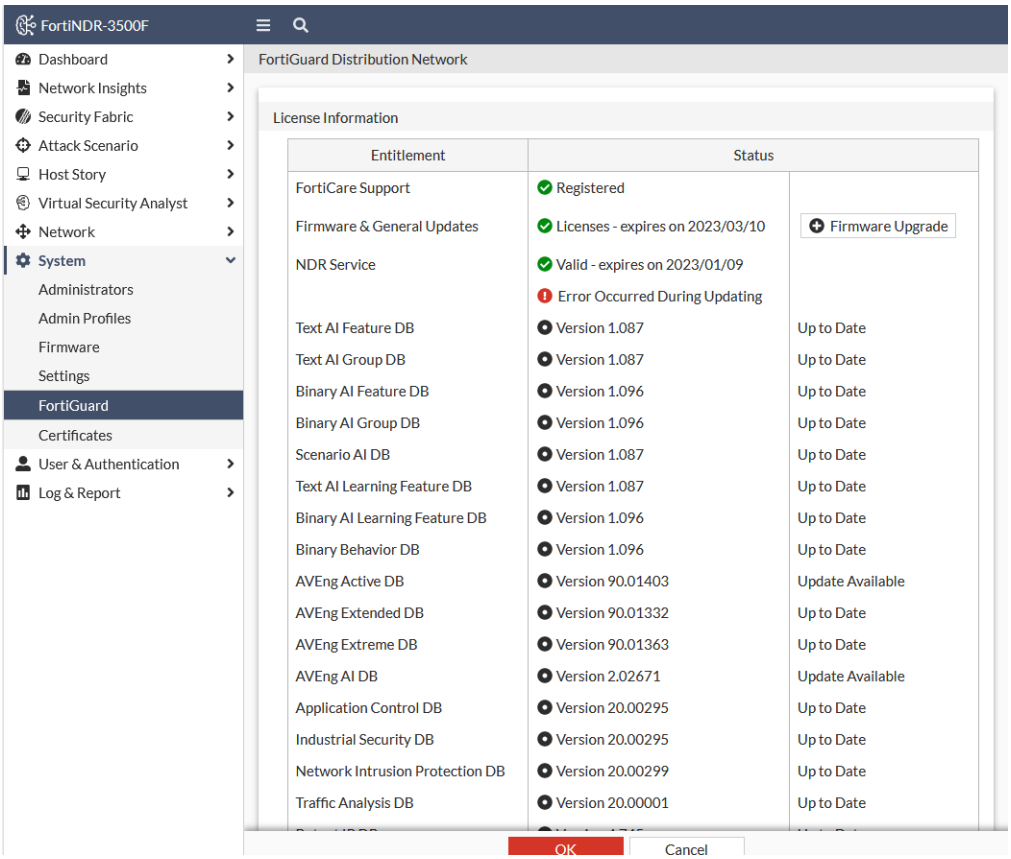
FortiGuard

FortiNDR relies on many local DB updates and some cloud lookups for detections to work. By default, the factory configuration of FortiNDR has local DB such as IPS and botnets loaded. Upon initial install it's important to get the most recent updates for accurate detection. The best way to get and install these updates is with an Internet connection. For offline deployments Please refer to Appendix D - FortiGuard updates on page 177. To view a list of updates, go to *System* > *FortiGuard*.

The latest version of NDR packages can be offline updated using the following CLI commnad:

```
execute restore ipsdb / avdb/ kdb [disk/tftp/ftp] filename
```

Please refer to Appendix D - FortiGuard updates on page 177 and CLI guide for more detail.



Use *System* > *FortiGuard* to view or update the version of *Entitlements* of your machine. You can update the version of entitlement using the GUI or CLI. For Malware detection using ANN (artificial neural network) is several GB in size, using the CLI to update the ANN database locally might be faster.

The latest version and updates of ANN are at FortiGuard service update at https://www.fortiguard.com/services/fortindr.

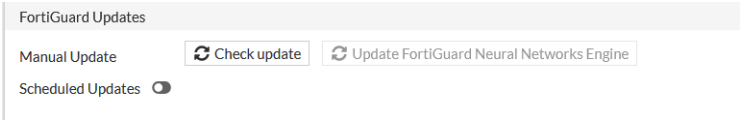
Currently, FortiNDR retrieves ANN updates from US and EMEA FortiGuard servers.

FortiNDR selects the update server based on proximity and location.

Besides ANN updates, FortiNDR also uses an AV engine for additional file scanning and accuracy, NDR and IPS engines for detecting network anomalies. Thus, regular updates to the AV/IPS/NDR databases are recommended. Note that AV signatures are used only when the ANN cannot determine if a file is malicious. If a file is determined to be malicious by ANN, then AV engine is not triggered.

To update the ANN database for malware detection using the GUI:

1. Go to *System* > *FortiGuard* and click *Check update*.



2. Click *Update FortiGuard Neural Networks Engine*.
   This triggers an install of the new ANN.

Because the ANN update is several GB in size, this procedure might take several hours. You can log out of the GUI after the update has started.

To update the ANN database using the CLI:

1. Go to the Fortinet support website and download the ANN network database files.
   There are two ANN network databases: `pae_kdb` and `moat_kdb`. `pae_kdb` has about six to eight individual files that you have to download.
   There is only one `moat_kdb.tar.gz` because it is small and doesn't have to be split. After downloading them for the `pae_kdb`, unzip them into `pae_kdb.tar.gz`.
2. Unzip the downloaded files to `pae_kdb.tar.gz` and `moat_kdb.tar.gz`.
   In Windows:
   a. `copy /B pae_kdb.zip.* pae_kdb.zip`
   b. Right-click the `pae_kdb.zip` package and click *Extract All*.
   In Linux:
   a. `cat pae_kdb.zip.* > pae_kdb.zip`
   b. `unzip pae_kdb.zip`
3. Put `pae_kdb.tar.gz` and `moat_kdb.tar.gz` on a disk that FortiNDR can access, such as a TFTP or FTP server, or a USB drive.
   If you use a USB drive, ensure its format is ext3 compatible, has only one partition, and the file is in the root directory.
4. Use the CLI command `execute restore kdb` to update the kdbs. Run this command once for `pae_kdb.tar.gz` and once for `pae_kdb.tar.gz`.
   For example, if `pae_kdb.tar.gz` and `moat_kdb.tar.gz` are in the FTP (IP:2.2.2.2) home folder of `/home/user/pae_kdb.tar.gz` and `/home/user/moat_kdb.tar.gz`, then use these commands:

```
execute restore kdb ftp pae_kdb.tar.gz 2.2.2.2 user password
execute restore kdb ftp moat_kdb.tar.gz 2.2.2.2 user password
```

   This is an example of the output:

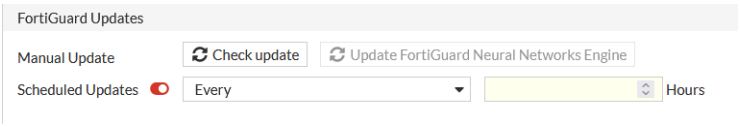
```
# execute restore kdb ftp pae_kdb.tar.gz 2.2.2.2 user password
This operation will first replace the current scanner db files and then restart the
scanner!
Do you want to continue? (y/n)y
Connect to ftp server 2.2.2.2 ...
Please wait...
Get file from ftp server OK.
Get file OK.
MD5 verification succeed!
KDB files restoration completed
Scanner restart completed
```

5. Go to *System* > *FortiGuard* to verify the updated versions.

Entitlement	Version
Binary AI 5	
Binary AI Engine	Version 1.009
Binary AI Learning Engine	Version 1.000
Binary AI Feature DB	Version 1.030
Binary AI Group DB	Version 1.030
Binary AI Learning Feature DB	Version 1.030
Scenario AI 2	
Scenario AI Engine	Version 1.000
Scenario AI DB	Version 1.001
Text AI 5	
Text AI Engine	Version 1.000
Text AI Learning Engine	Version 1.000
Text AI Feature DB	Version 1.001
Text AI Group DB	Version 1.001
Text AI Learning Feature DB	Version 1.001

To schedule FortiGuard updates:

1. Go to *System* > *FortiGuard*.
2. In the *FortiGuard Updates* area, enable *Scheduled Updates*.



3. From the frequency dropdown, select *Daily* or *Weekly*.
4. In the *Hours* field a numeric fall for the frequency.
5. Click *OK*.

Certificates

Use *System* > *Certificates* to import, view, and delete certificates. Certificates are used for secure connection to an LDAP server, system HTTPS, or SSH services. FortiNDR installs one default certificate.

Conserve Mode

FortiNDR has high throughput malware scanning which is published at 100K for FortiNDR-3500F in ideal lab conditions. Conserve mode is triggered if the submission backlog queue becomes too high. The system will enter conserve mode and continue scanning files already in the queue, however, it will stop taking in new files while operating in conserve mode.

The event log will display a warning when the unit enters or exists conserve mode.

Backup or restore the system configuration

It is recommended that you create a system backup file as part of your maintenance plan. Always perform a backup before upgrading firmware or making major system configuration changes. Save these configuration backups to your local computer in the event that you need to restore the system after a network event.

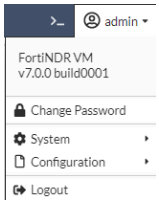
The following data is not backed up at this time:

- Network Share
- Network Share Quarantine
- File size limit (`execute file-size-threshold`)
- Email Alert Recipients

Please record these configuration settings before upgrading so the full configuration can be restored.

To backup the FortiNDR configuration to your local computer:

1. Go to the *Dashboard* and click the account menu at the top-right of the page.



2. Click *Configuration* > *Backup*. The configuration file is saved to your computer.

To restore the system configuration from your local computer:

1. Go to the *Dashboard* and click the account menu at the top-right of the page.
2. Click *Configuration* > *Restore*. *The Restore System Configuration* page opens.
3. Click *Upload* and navigate to the location of the configuration file on your computer.
4. Click *OK*. The system reboots.

User & Authentication

FortiNDR supports remote authentication for administrators using RADIUS or LDAP servers. To use remote authentication, configure the server entries in FortiNDR for each authentication server in your network.

If you have configured RADIUS or LDAP support, FortiNDR contacts the RADIUS or LDAP server for authentication. When you enter a username and password in FortiNDR, FortiNDR sends this username and password to the authentication server. If the server can authenticate the user, FortiNDR authenticates the user. If the server cannot authenticate the user, FortiNDR refuses the connection.

Two-factor authentication is supported in with FortiAuthenticator v6.4.5 and higher. Users will be prompted by the GUI to enter a 2FA token code. Push tokens are not supported at this time.

RADIUS Server

The FortiNDR system supports remote authentication of administrators using RADIUS servers. To use this feature, you must configure the appropriate server entries in the FortiNDR unit for each authentication server in your network.

If you have configured RADIUS support and require a user to authenticate using a RADIUS server, the FortiNDR unit contacts the RADIUS server for authentication. To authenticate with the FortiNDR unit, the user enters a user name and password. The FortiNDR unit sends this user name and password to the RADIUS server. If the RADIUS server can authenticate the user, the FortiNDR unit successfully authenticates the user. If the RADIUS server cannot authenticate the user, the FortiNDR unit refuses the connection.

The following options are available:

Create New	Select to add a RADIUS server.
Edit	Select a RADIUS server in the list and click *Edit* in the toolbar to edit the entry.
Clone	Select a RADIUS server in the list and click *Clone* in the toolbar to clone the entry.
Delete	Select a RADIUS server in the list and click *Delete* in the toolbar to delete the entry.

The following information is displayed:

Profile Name	The RADIUS server profile name.
SERVER Name/IP	The server name and IP address of the RADIUS server.
Ref	The RADIUS server's reference ID.

To create a new RADIUS server:

1. Go to User & Authentication > RADIUS Server.
2. Click *Create New*. The *Add New RADIUS Server* page opens.

3. Configure servers settings.

Profile name	Enter a name for the profile.
Server name/IP	Enter the server name and IP address.
Protocol	Select one of the following from the dropdown: • Default Authentication Scheme • Password Authentication • Challenge Handshake Authentication • MS Challenge Handshake Auth • Ms Challenge Handshake Auth V2
NAS IP/Called station ID	Enter the NAS IP address and called station ID.
Server Secret	Click *Change* to change the secret.

4. Click *OK*.

LDAP Servers

The FortiNDR system supports remote authentication of administrators using LDAP servers. To use this feature, configure the server entries in the FortiNDR unit for each authentication server in your network.

If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiNDR unit contacts the LDAP server for authentication. To authenticate with the FortiNDR unit, the user enters a username and password. The FortiNDR unit sends this username and password to the LDAP server. If the LDAP server can authenticate the user, the FortiNDR unit accepts the connection. If the LDAP server cannot authenticate the user, the FortiNDR unit refuses the connection.

The following options are available:

Create New	Select to add a LDAP server.
Edit	Select a LDAP server in the list and click *Edit* in the toolbar to edit the entry.
Clone	Select a LDAP server in the list and click *Clone* in the toolbar to clone the entry.
Delete	Select a LDAP server in the list and click *Delete* in the toolbar to delete the entry.

The following information is displayed:

Profile Name	The LDAP server profile name.
SERVER Name/IP	The server name and IP address of the LDAP server.
Port	The port number for the server.
Ref	The LDAP server's reference ID.

To add an LDAP server:

1. Go to *User & Authentication* > *LDAP Server*.
2. Click *Create New*. The *Add New LDAP Server* page opens.

3. Configure server settings.

Profile name	Enter a name for the profile.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server. Port: Enter the port number where the LDAP server listens. The default port number varies by your selection in *Use secure connection*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
Fall Back Server name/IP	Optional. Enter the fully qualified domain name (FQDN) or IP address of an alternate LDAP server that the FortiNDR unit can query if the primary LDAP server is unreachable. Port: Enter the port number where the fallback LDAP server listens. The default port number varies by your selection in *Use secure connection*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
Use secure connection	Select whether or not to connect to the LDAP servers using an encrypted connection. • *None*: Use a non-secure connection. • *SSL*: Use an SSL-secured (LDAPS) connection. Click *Test LDAP Query* to test the connection. A pop-up window appears.
Default Bind Options	
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiNDR will search for user objects, such as `ou=People`, `dc=example`, `dc=com`. User objects should be child nodes of this location.
Bind DN	Enter the bind DN, such as `cn=fortiNDR`, `dc=example`, `dc=com`, of an LDAP user account with permissions to query the Base DN.
Bind password	Enter the password of the Bind DN. Click *Browse* to locate the LDAP directory from the location that you specified in *Base DN*, or, if you have not yet entered a Base DN, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your Base DN, or need to look up attribute names. For example, if the Base DN is unknown, browsing can help you to locate it. Before using, first configure *Server name/IP*, *Use secure connection*, *Bind DN*, *Bind password*, and *Protocol version*, then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection.
User Query Options	
LDAP user query	Click *Schema* to select a schema style. You can edit the schema as desired or select *User Defined* and write your own schema.
Scope	Select the level of depth to query, starting from *Base DN*. • *One level*: Query only the one level directly below the Base DN in the

	LDAP directory tree. • *Subtree*: Query recursively all levels below the Base DN in the LDAP directory tree.
Derefer	Select the method to use, if any, when dereferencing attributes whose values are references. • *Never*: Do not dereference. • *Always*: Always dereference. • *Search*: Dereference only when searching. • *Find*: Dereference only when finding the base search object.
User Authentication Options	Enable to configure the authentication options. Select one of the followng from the dropdown. • *Try UPN or mail address as bind DN* • *Try common name with base DN as bind DN* • *Search user and try bind DN*.
Advanced Options	
Timeout (seconds)	Enter the maximum amount of time in seconds that the FortiNDR unit will wait for query responses from the LDAP server.
Protocol version	Select the LDAP protocol version used by the LDAP server: *LDAP Version 2* or *LDAP Version 3*.
Allow Unauthenticated Bind	Disable bind authentication.
Enable Cache	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiNDR unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.
Clear Cache	Select to empty the FortiNDR unit's LDAP query cache. This can be useful if you have updated the LDAP directory, and want the FortiNDR unit to refresh its LDAP query cache with the new information.
TTL (minutes)	Enter the amount of time, in minutes, that the FortiNDR unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiNDR unit to query the LDAP server, refreshing the cache. The default TTL value is 1440 minutes (one day). The maximum value is 10080 minutes (one week). Entering a value of 0 effectively disables caching. This option is applicable only if Enable cache is enabled.

4. Click *OK*.

To edit an LDAP server:

1. Go to *User & Authentication* > *LDAPServer*.
2. Select a profile and vlick *Edit*.
3. Configure the LDAP server setting and click *Apply current settings*. Optionally, you can click *Reset settings* to return to the default settings.
4. Click *OK*.

LDAP user query example

If user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be:

```
(& (objectClass=inetOrgPerson) (mail=$m))
```

where `$m` is the FortiNDR variable for a user's email address.

If the email address (`$m`) as it appears in the message header is different from the user's email address as it appears in the LDAP directory, such as when you have enabled recipient tagging, a query for the user by the email address ($m) may fail. In this case, you can modify the query filter to subtract prepended or appended text from the user name portion of the email address before performing the LDAP query. For example, to subtract `-spam` from the **end** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=inetOrgPerson) (mail=$m$
   {-spam}))
```

where `${-spam}` is the FortiNDR variable for the tag to remove before performing the query. Similarly, to subtract `spam-` from the **beginning** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=inetOrgPerson) (mail=$m$
   {^spam-}))
```

where `${^spam-}` is the FortiNDR variable for the tag to remove before performing the query.

For some schemas, such as Microsoft ActiveDirectory-style schemas, this query will retrieve both the user's primary email address and the user's alias email addresses. If your schema style is different, you may want to also configure User Alias Options to resolve aliases. For details, see Configuring user alias options.

Alias member query example

If user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail`attributes, the query filter might be:

```
(& (objectClass=alias) (mail=$m))
```

where `$m` is the FortiNDR variable for a user's email address.

If the email address (`$m`) as it appears in the message header is different from the alias email address as it appears in the LDAP directory, such as when you have enabled recipient tagging, a query for the alias by the email address (`$m`) may fail. In this case, you can modify the query filter to subtract prepended or appended text from the user name portion of the email address before performing the LDAP query. For example, to subtract `-spam` from the **end** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=alias) (mail=$m${-spam}))
```

where `${-spam}` is the FortiNDR variable for the tag to remove before performing the query. Similarly, to subtract `spam-` from the **beginning** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=alias) (mail=$m${^spam-}))
```

where `${^spam-}` is the FortiNDR variable for the tag to remove before performing the query.

Whether you should configure this query filter to retrieve user or alias objects depends on whether your schema resolves email addresses directly or indirectly (using references).

If alias objects in your schema provide **direct** resolution, configure this query string to retrieve alias objects. Depending on your schema style, you can do this either using the user name portion of the alias email address (`$u`), or the entire email address (`$m`). For example, for the email aliases `finance@example.com` and `admin@example.com`, if your LDAP directory contains alias objects distinguished by `cn: finance` and `cn: admin`, respectively, this query string could be `cn=$u`.

If alias objects in your schema provide **indirect** resolution, configure this query string to retrieve user objects by their distinguished name, such as `distinguishedName=$b or dn=$b`. Also enable User group expansion In advance, then configure Group member query to retrieve email address alias objects, and configure Group Member Attribute to be the name of the alias object attribute, such as member, whose value is the distinguished name of a user object.

Preparing your LDAP schema for FortiNDR LDAP profiles

FortiNDR units can be configured to consult an LDAP server for many things that you might otherwise normally have to configure on the FortiNDR unit itself, such as user authentication, group membership, mail routing, and other features. Especially if you have a large amount of users and groups already defined on an LDAP directory, you may find it more convenient to query those existing definitions than to recreate the definition of those same users locally on the FortiNDR unit. To accomplish this, you would configure an LDAP profile, then select that LDAP profile in other areas of the configuration that should use its LDAP queries.

LDAP profiles require compatible LDAP server directory schema and contents. Your LDAP server configuration may already be compatible. However, if your LDAP server configuration does **not** contain required information in a schema acceptable to LDAP profile queries, you may be required to modify either or both your LDAP profile and LDAP directory schema.

Verify your LDAP server's configuration for each query type that you enable and configure. For example, if you enable mail routing queries, verify connectivity and that each user object in the LDAP directory includes the attributes and values required by mail routing. Failure to verify enabled queries can result in unexpected mail processing behavior.

Using common schema styles

Your LDAP server schema may require no modification if your LDAP server:

- Already contains all information required by the LDAP profile queries you want to enable
- Uses a common schema style, and a matching predefined LDAP query configuration exists for that schema style

If both of those conditions are true, your LDAP profile configuration may also be very minimal. Some queries in LDAP profiles contain schema options that automatically configure the query to match common schema styles such as IBM Lotus Domino, Microsoft ActiveDirectory (AD), and OpenLDAP. If you will only enable those queries that have schema options, it may be sufficient to select your schema style for each query.

For example, your LDAP server might use an OpenLDAP-style schema, where two types of user object classes exist, but both already have mail and `userPassword` attributes. Your FortiNDR unit is in gateway mode, and you want to use LDAP queries to use users' email addresses to query for authentication.

In this scenario, it may be sufficient to:

1. In the LDAP profile, enter the domain name or IP address of the LDAP server.
2. Configure the LDAP profile queries:
   - In *User Query Options*, from *Schema* which OpenLDAP schema your user objects follow: either InetOrgPerson or InetLocalMailRecipient. Also enter the *Base DN*, *Bind DN*, and *Bind* password to authenticate queries by the FortiNDR unit and to specify which part of the directory tree to search.
   - In *User Authentication Options*, enable *Search user and try bind DN*.
   - Configure mail domains and policies to use the LDAP profile to authenticate users and perform recipient verification.

Log & Report

On rare occasions, after upgrading to a new version or running the CLI command, `execute cleanup (ndr)`, the pages in this section may still show older history browser cache. Please refresh the pages (F5) to trigger the reload.

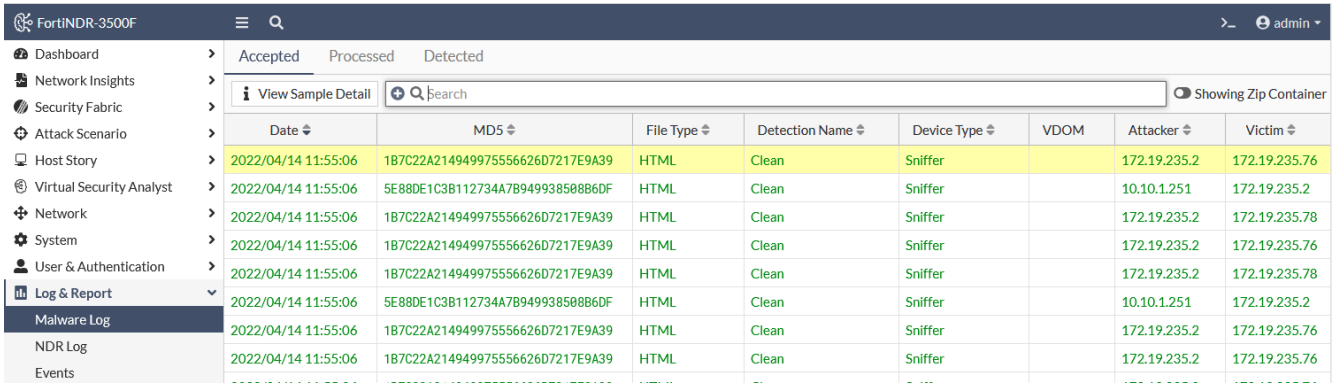
Malware Log

Malware Log reports provide administrators with a detailed view of malicious malware detected.

Details include *Date*, *MD5 checksum*, *File Type* such as portable executable, HTML, and so on. *Detection Name* is the unique name of the malware. *Device Type* is the source device from which the sample file is, eg. Sniffer, ICAP, etc.

The *Malware Log* also shows the *Confidence Level* as a percentage and as well as a Risk verdict of *High*, *Medium*, *Low* or *No Risk*.

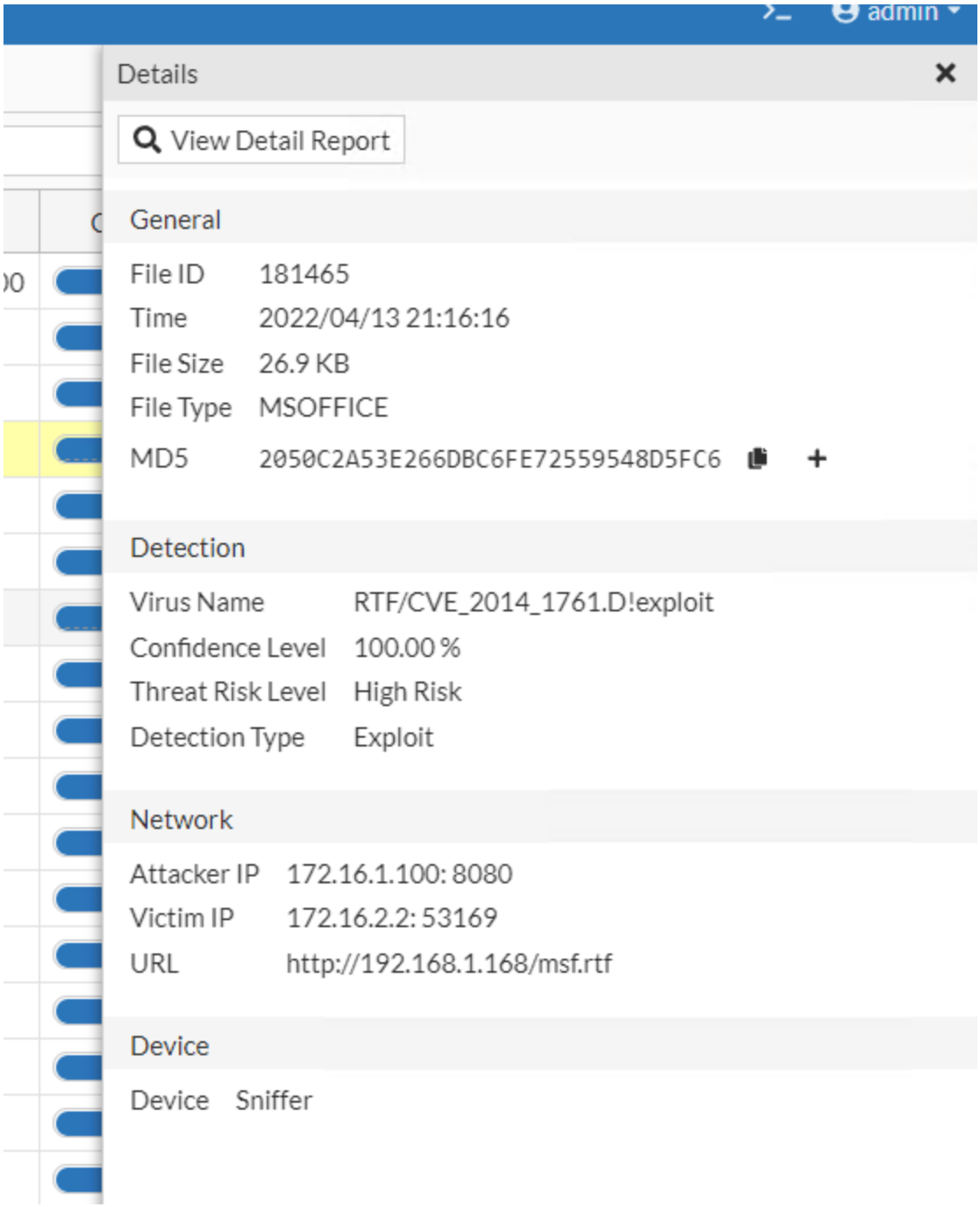
The *Indicator* displays icons if the detection has IOC detail. *Feature Detection* shows the detection feature type of the malware.



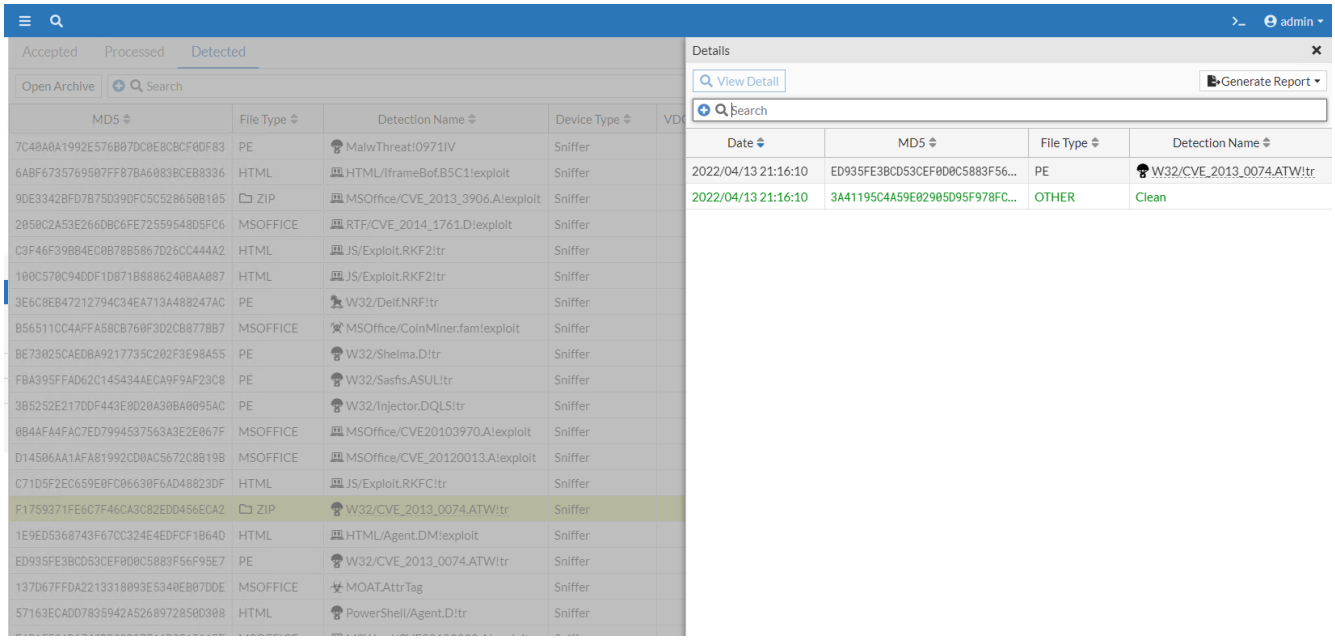
Threat Report has the following pages.

Accepted	Files accepted by FortiNDR parsers.
Processed	Both clean and malicious files processed by FortiNDR engines.
Detected	Malicious files processed by FortiNDR engines.

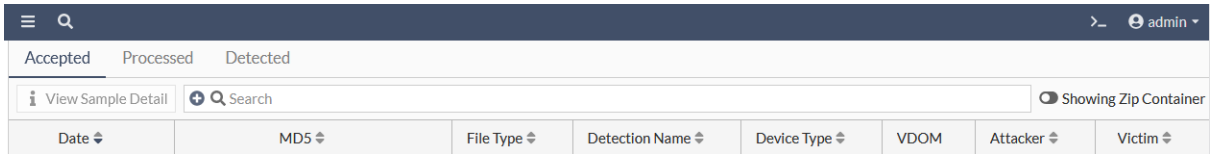
Double-click an entry to view a summary of the log entry


admin
Details
View Detail Report
General
File ID 181465
Time 2022/04/13 21:16:16
File Size 26.9 KB
File Type MSOFFICE
MD5 2050C2A53E266DBC6FE72559548D5FC6
Detection
Virus Name RTF/CVE_2014_1761.D!exploit
Confidence Level 100.00 %
Threat Risk Level High Risk
Detection Type Exploit
Network
Attacker IP 172.16.1.100: 8080
Victim IP 172.16.2.2: 53169
URL http://192.168.1.168/msf.rtf
Device
Device Sniffer

Double-click a zip folder to view what is inside the folder.

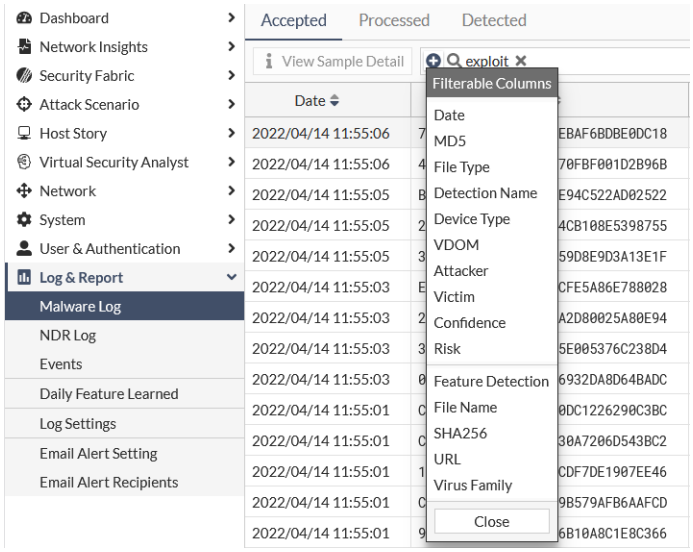


Enable *Showing Zip Container* to view the extracted files in the page.

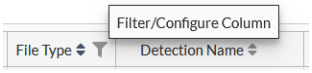


Advanced search

When you type a key words into the search field it will display partial results. Click the plus sign (+) to include filterable columns in your search. The *Search* function only supports exact matches. Wildcards are not supported.

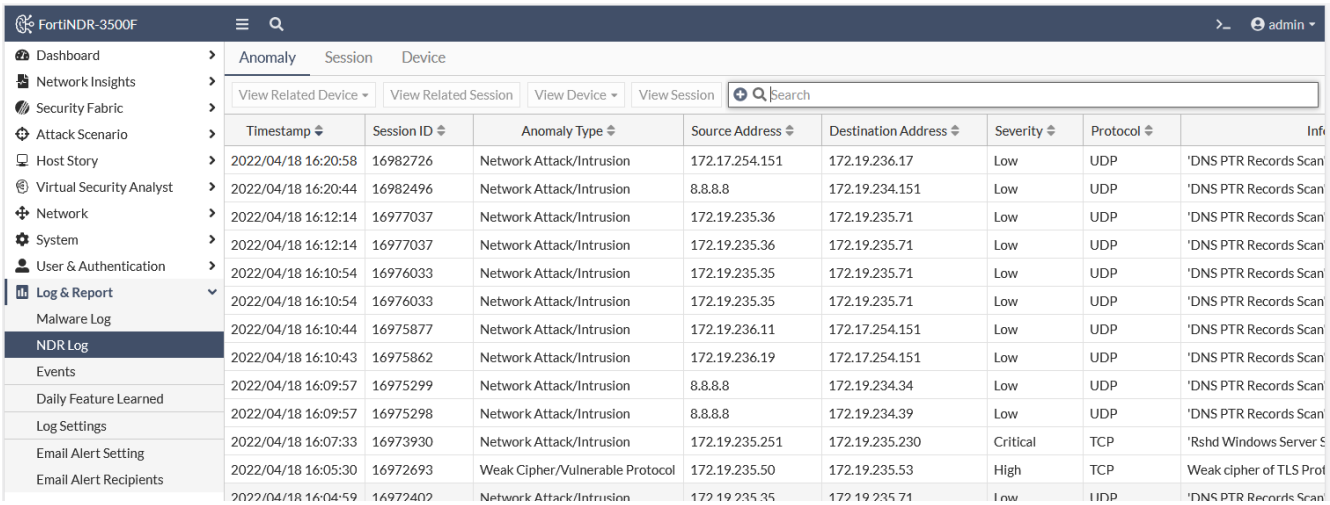


You can also filter the logs by clicking the filter icon in the column heading.



NDR Log

The NDR Log view displays information anomalies detected on the network, traffic sources and destinations, as well as devices discovered and detected by FortiNDR. Users are welcomed to use NDR Anomaly Type column to narrow and investigate the anomalies, by session or by device view.

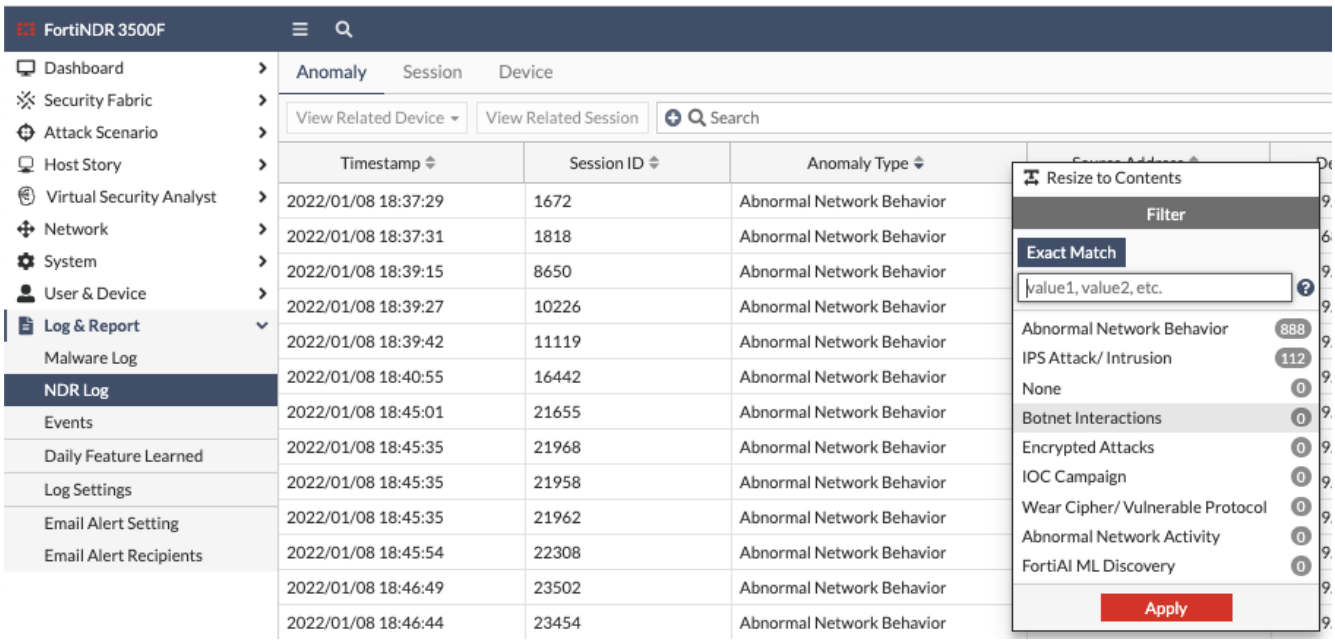


Anomaly tab

This *Anomaly* tab displays anomalies detected on the network. In a normal network, only a small percentage of network traffic are anomalies. The FortiNDR engine records both normal and anomaly traffic.

You can filter the logs by Anomaly Type but clicking the Filter icon in the column heading.

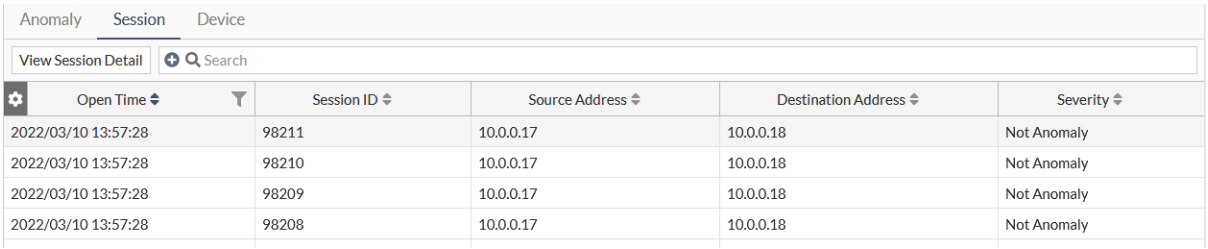
When filtering the Anomaly Type column, you can use `!=<type>` to filter out the types you don't want to see.



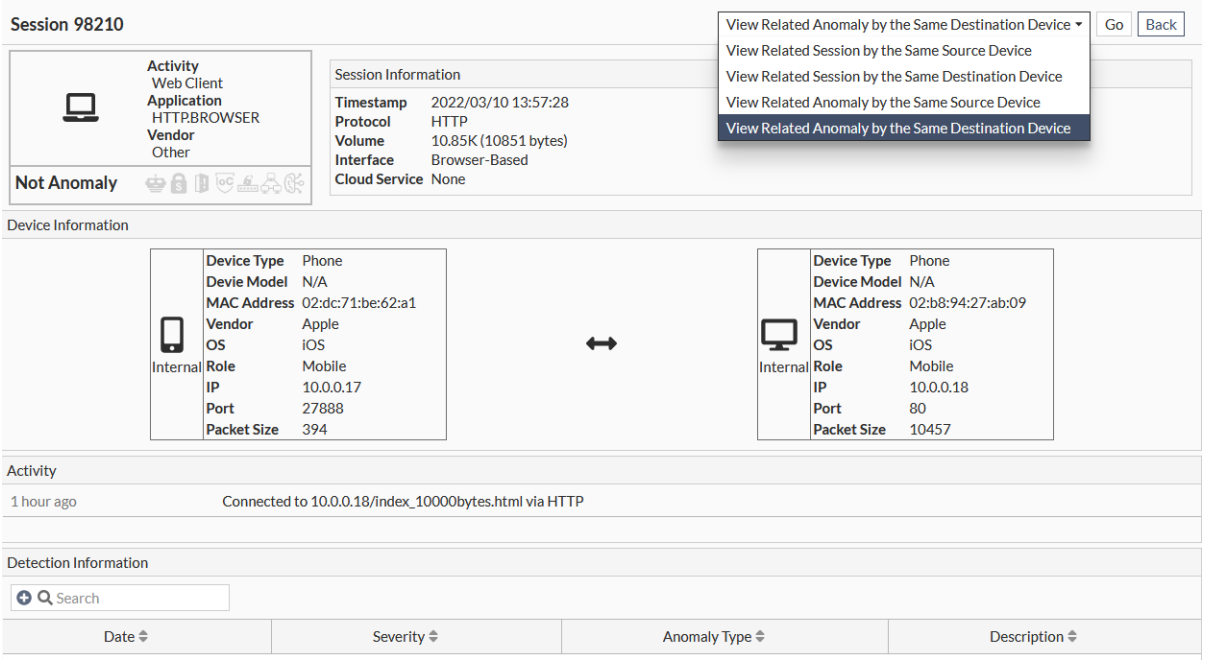
Session Tab

Use the *Sessions* tab to understand the relationship between sessions and anomalies. There could be multiple behaviors within a session and some connections within a session could be an anomaly. For example, a user accessing the Internet browses both Facebook normally and hits an IOC campaign Emotet within same session. You can also view the traffic *Source* and *Destination*, to determine whether the connection is internal or external.

To filter the sessions in the view, hover a column heading and click the filter icon.

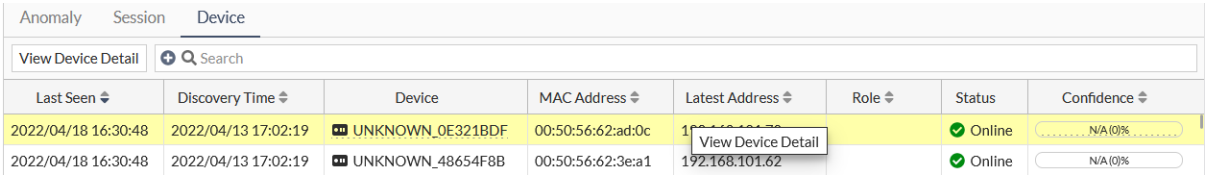


To drill down on the session information, click *View Session Detail*. Click the *Action* menu to view related information.



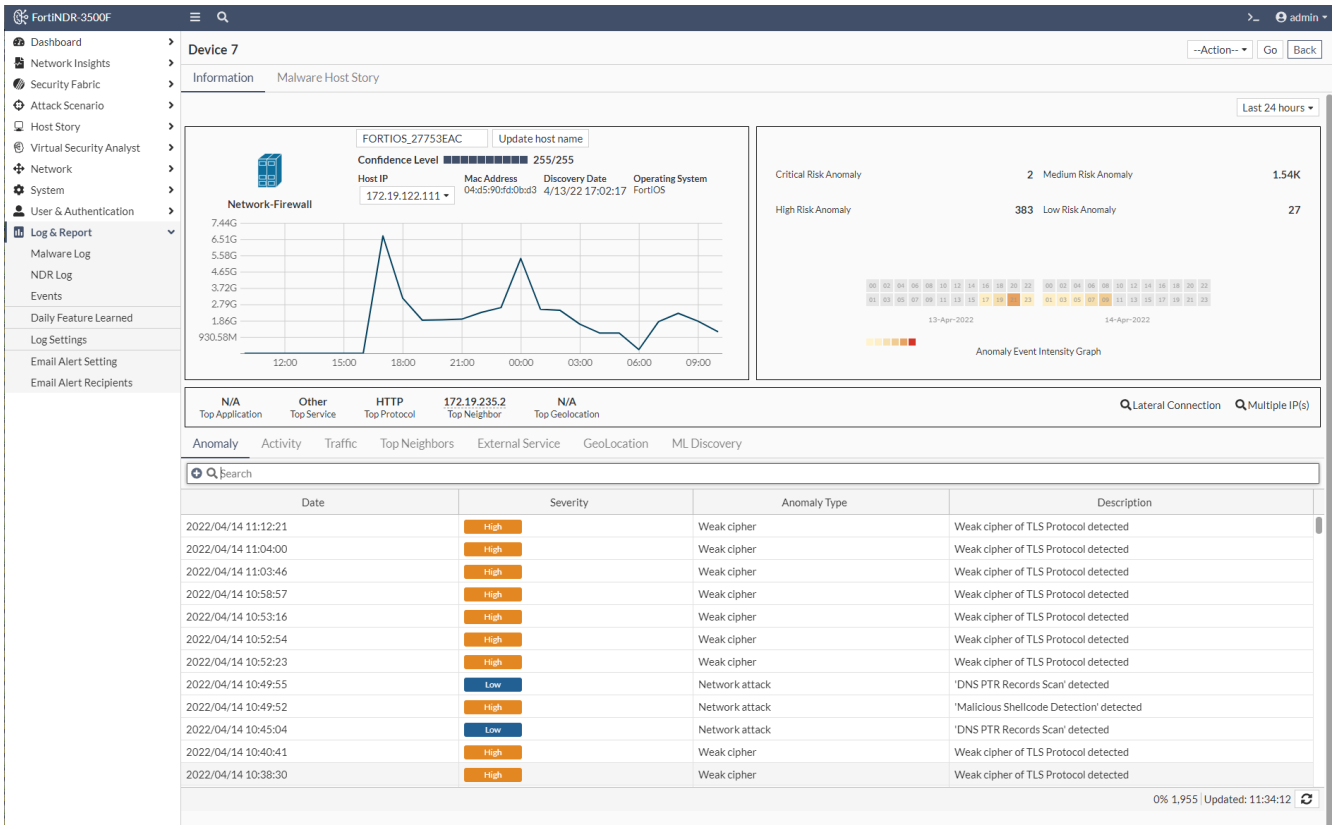
Device Tab

The Device tab the devices detected by FortiNDR. The FortiGuard IOT service is used to identify device information based on the MAC address. You can drill down to the devices page by clicking *View Device Detail* details.

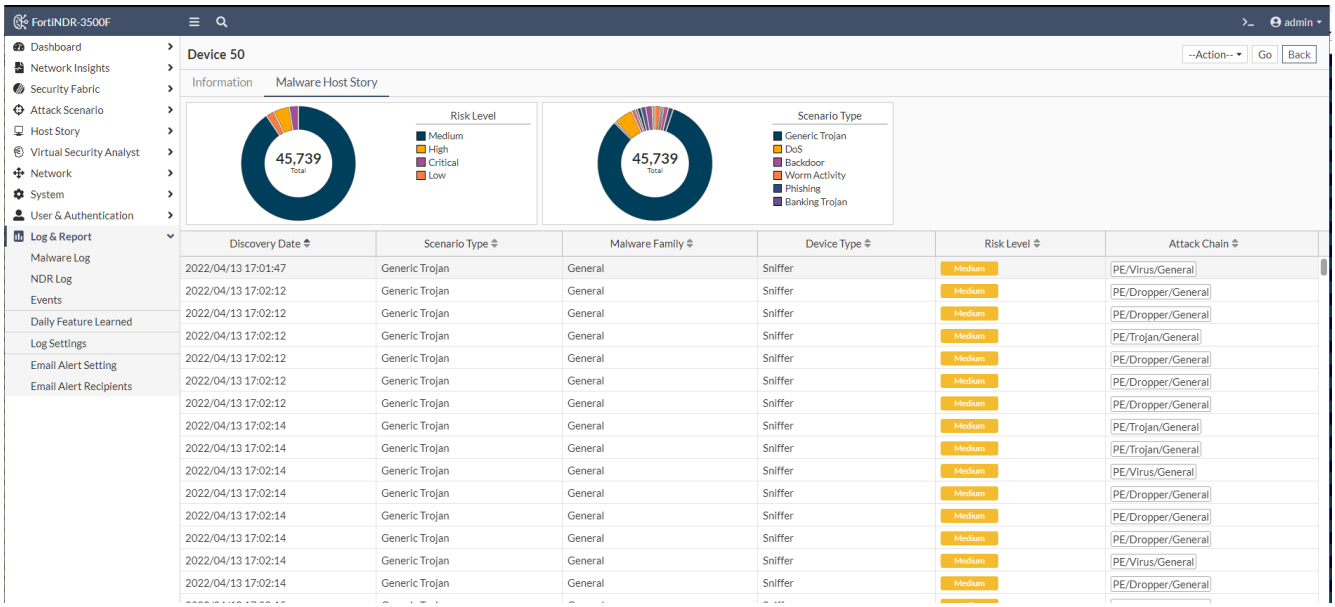


The *Device* page shows information about the device activity (both anomaly and normal events), as well as a heatmap for anomalies over the selected time period. A line graph shows the device traffic (inbound and outbound bandwidth combined). The *Confidence Level* indicates our confidence in identifying the device category.

In this following image, the device is identified as *Network Firewall*. The window at the bottom of the page shows the top anomalies, activities, traffic, neighbors, external services, a geolocation map of the device traffic and machine learning discovery.

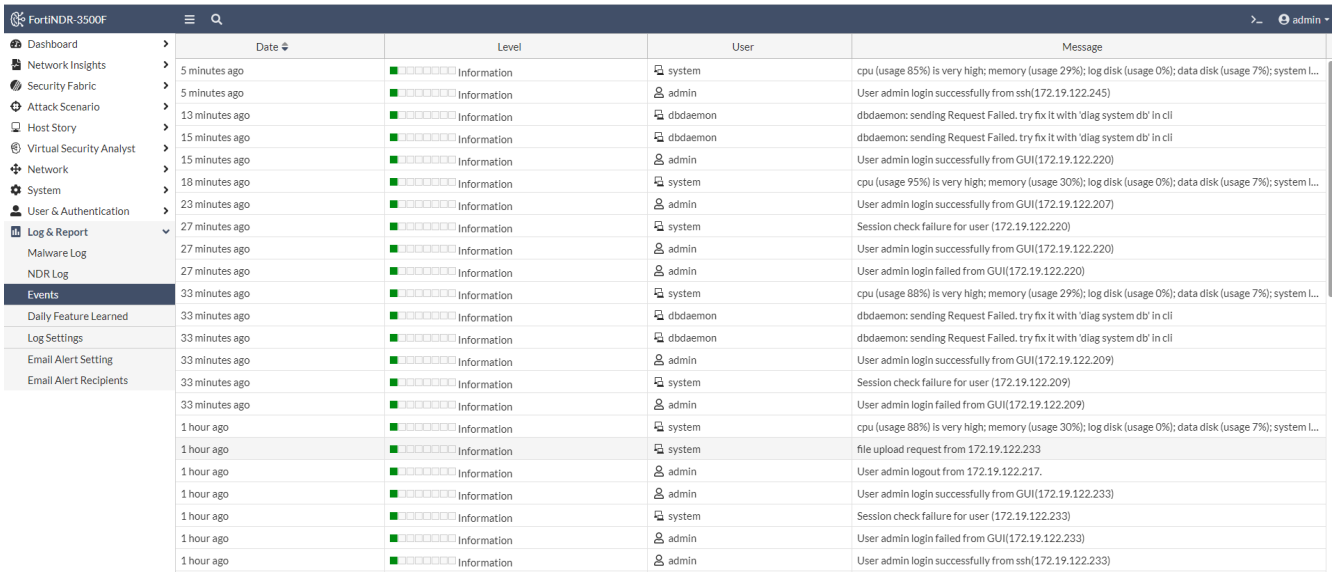


The Malware Host Story shows information about the malware *Risk Level* and *Scenario Type*.



Events

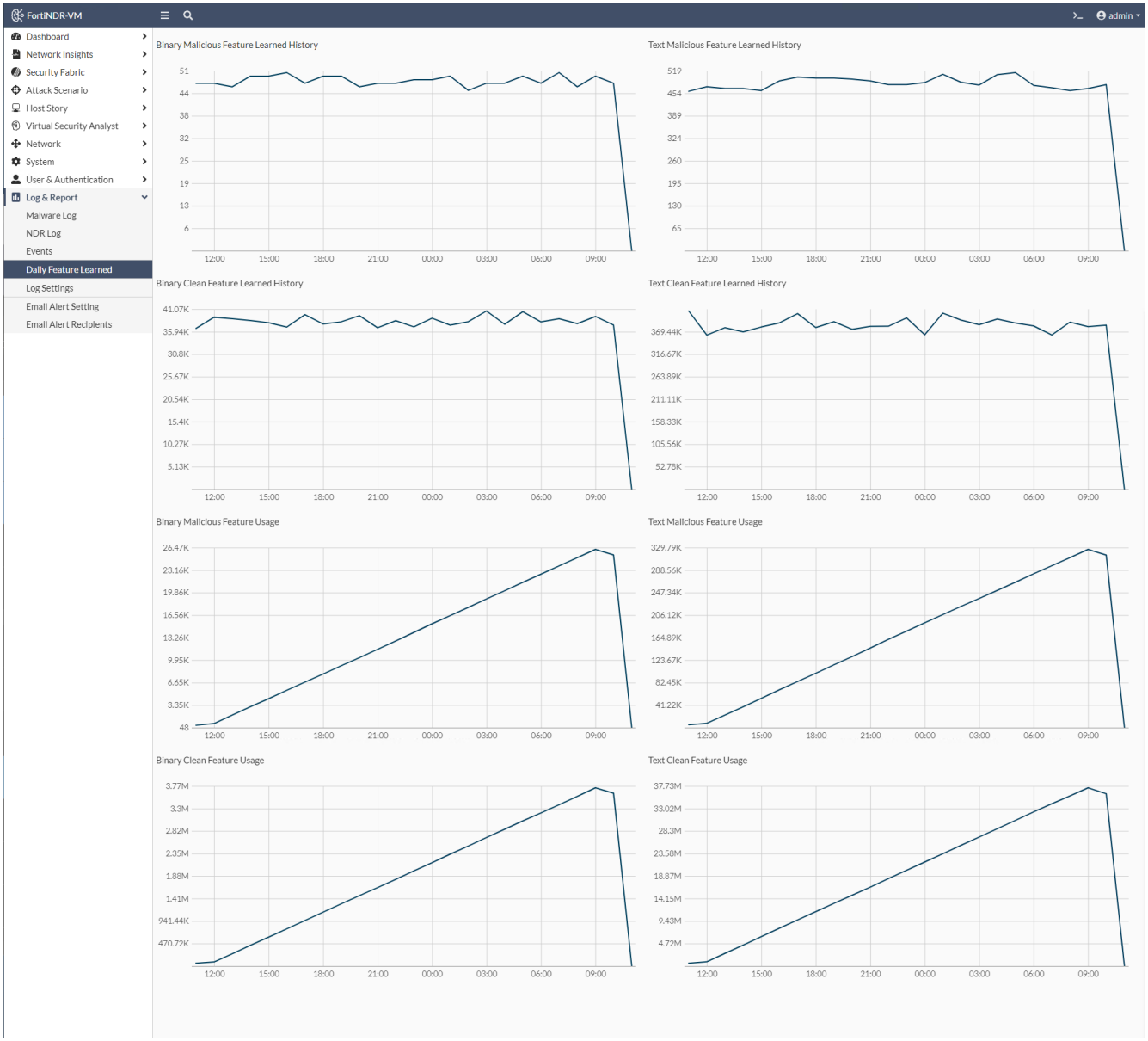
FortiNDR logs and displays system events such as CPU and memory usage, and attack kill chain.



Date	Level	User	Message
5 minutes ago	Information	system	cpu (usage 85%) is very high; memory (usage 29%); log disk (usage 0%); data disk (usage 7%); system l...
5 minutes ago	Information	admin	User admin login successfully from ssh(172.19.122.245)
13 minutes ago	Information	dbdaemon	dbdaemon: sending Request Failed. try fix it with 'diag system db' in cli
15 minutes ago	Information	dbdaemon	dbdaemon: sending Request Failed. try fix it with 'diag system db' in cli
15 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.220)
18 minutes ago	Information	system	cpu (usage 95%) is very high; memory (usage 30%); log disk (usage 0%); data disk (usage 7%); system l...
23 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.207)
27 minutes ago	Information	system	Session check failure for user (172.19.122.220)
27 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.220)
27 minutes ago	Information	admin	User admin login failed from GUI(172.19.122.220)
33 minutes ago	Information	system	cpu (usage 88%) is very high; memory (usage 29%); log disk (usage 0%); data disk (usage 7%); system l...
33 minutes ago	Information	dbdaemon	dbdaemon: sending Request Failed. try fix it with 'diag system db' in cli
33 minutes ago	Information	dbdaemon	dbdaemon: sending Request Failed. try fix it with 'diag system db' in cli
33 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.209)
33 minutes ago	Information	system	Session check failure for user (172.19.122.209)
33 minutes ago	Information	admin	User admin login failed from GUI(172.19.122.209)
1 hour ago	Information	system	cpu (usage 88%) is very high; memory (usage 30%); log disk (usage 0%); data disk (usage 7%); system l...
1 hour ago	Information	system	file upload request from 172.19.122.233
1 hour ago	Information	admin	User admin logout from 172.19.122.217.
1 hour ago	Information	admin	User admin login successfully from GUI(172.19.122.233)
1 hour ago	Information	system	Session check failure for user (172.19.122.233)
1 hour ago	Information	admin	User admin login failed from GUI(172.19.122.233)
1 hour ago	Information	admin	User admin login successfully from ssh(172.19.122.233)

Daily Feature Learned

This page in FortiNDR shows a graphical count of the features learned and used. The display includes the text and binary engines.

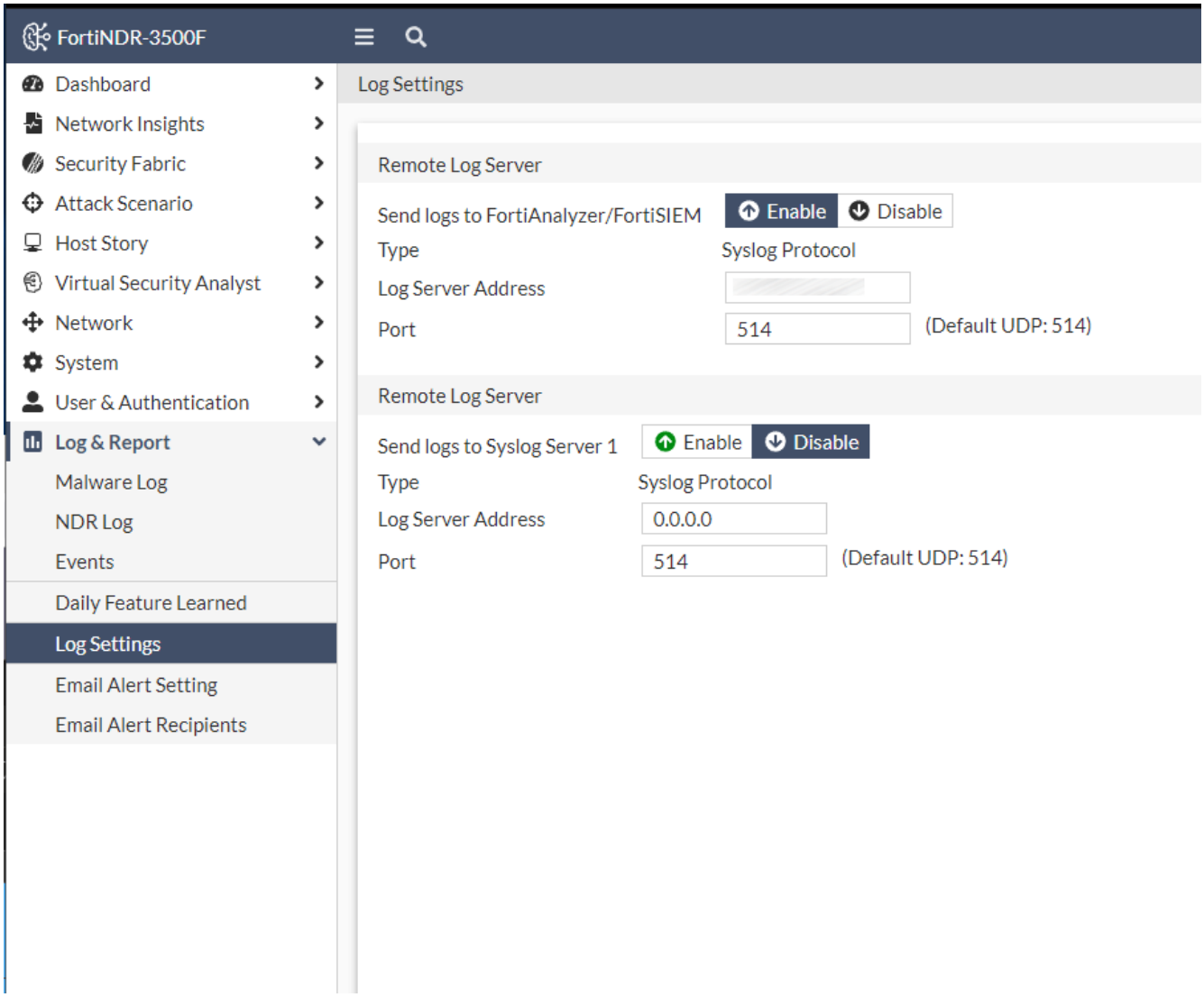


Log Settings

Use the *Log Settings* page to configure Syslog settings for FortiAnalyzer (7.0.1 and higher) and FortiSIEM (6.3.0 and higher). You can use the secondary Syslog field to send the same logs to different Syslog servers. You can configure both fields to send to both FortiAnalyzer and FortiSIEM.

Log Settings send Syslog messages about the *Attack Scenario* to other devices such as FortiAnalyzer or FortiSIEM.

- Upload file and Network share file detection will not send Syslog upon detection because they do not trigger Attack Scenario since they do not have flows of virus, meaning the sample flows from attacker to victim.
- Inline, ICAP, Sniffer and OFTP detections will trigger Syslog being sent to FortiAnalyzer or FortiSIEM, since they have this information.



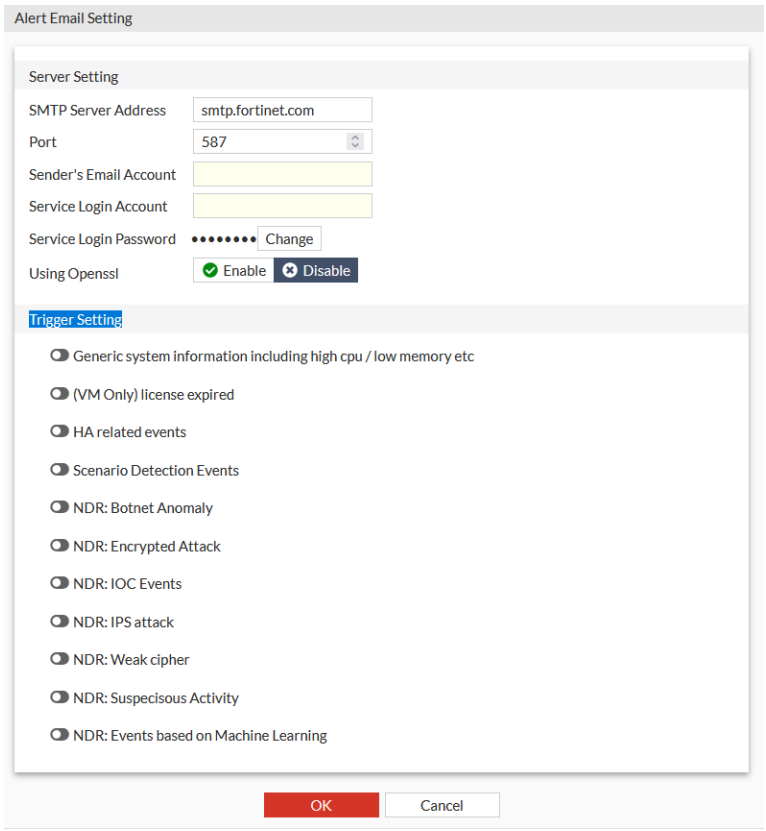
Alert Email Setting

Receive email alerts with malware and system event threats are detected.

To configure email alerts:

1. Go to *Log & Report* > *Email Alert Setting*.
2. Configure the server settings.

SMTP Server Address	Enter the STMP server address.
Port	Enter the port number.
Sender's Email Account	Enter the sender's email account
Service Login Account	Enter the service login account.
Service Login Password	Enter the service login password.
Using Openssl	Enable or disable open SSL
Trigger Setting	Select an option(s) from the list and enter the email message text. Select the *Trigger Sensitivty* where required.



3. Click *OK*.
4. Add email addresses to the email recipient list. See, Email Alert Recipients on page 133.

Email Alert Recipients

Create a distribution list for email alerts.

To add email recipients to recipient list:

1. Go to *Log & Report* > *Email Alert Recipients*.
2. Click *Add Recipient*. The *Add Recipient* pane opens.
3. In the *Email* field, enter the recipient's email address and click *OK*.
4. (Optional) Click *Send Verification Email* to send a test notification to the distribution list.
5. (Optional) Select an email(s) and click Remove Selected Recipient to delete an address ffromm the list.

NDR logs samples

Botnet

```
date="2022-02-09" time="16:43:13" tz="PST" logid="0602000001" devid="FAIVMSTM21000033"
type="ndr" subtype="Botnet" severity="high" sessionid=63313 alproto="DNS" tlproto="UDP"
srcip="18.1.2.2" srcport=10000 dstip="18.1.1.100" dstport=53 behavior="CONN" botname="botnet
Andromeda" hostname="orrisbirth.com"
```

```
date="2022-02-09" time="16:43:13" tz="PST" logid="0602000001" devid="FAIVMSTM21000033"
type="ndr" subtype="Botnet" severity="high" sessionid=63313 alproto="DNS" tlproto="UDP"
srcip="18.1.2.2" srcport=10000 dstip="18.1.1.100" dstport=53 behavior="RESP" botname="botnet
Other"  hostname="cdn12-web-security.com"
```

Fields

behavior	User activity. For example, CONN, RESP, VISIT, GET etc.
botname	The name for this botnet
hostname	Hostname

Encrypted

```
date="2022-02-11" time="10:19:03" tz="PST" logid="0603000001" devid="FAI35FT321000001"
type="ndr" subtype="Encrypted" severity="critical" sessionid=11554817 alproto="TLS"
tlproto="TCP" srcip="172.19.236.140" srcport=5326 dstip="173.245.59.98" dstport=443
behavior="CONN" vers="7" cipher="TLS_AES_256_GCM_SHA384"
md5="f436b9416f37d134cadd04886327d3e8"
```

Fields

behavior	User activity, e.g. CONN, RESP, VISIT, GET etc.
vers	The version of alproto, str

cipher	The encryption algorithm.
md5	md5/hash of ja3 fingerprint

IOC

```
date="2022-02-14" time="07:36:13" tz="PST" logid="0605000001" devid="FAI35FT321000001"
type="ndr" subtype="IOC" severity="critical" sessionid=19906026 alproto="HTTP" tlproto="TCP"
srcip="172.19.235.198" srcport=49304 dstip="178.63.120.205" dstport=443 behavior="CONN"
vers="7" cipher="TLS_AES_128_GCM_SHA256" md5="52bea59cf17d9fd5dedd2835fd8e1afe"
campaign="CoinMiner" hostname="s3.amazonaws.com" url="/"
```

Fields

behavior	User activity. For example, CONN, RESP, VISIT, GET etc
vers	The version of alproto
cipher	The encryption algorithm.
md5	md5/hash of ja3 fingerprint
campaign	IOC campaign
hostname	The hostname
url	The URL visited

IPS attack

```
date="2022-02-10" time="19:16:56" tz="PST" logid="0604000001" devid="FAI35FT321000001"
type="ndr" subtype="IPS attack" severity="low" sessionid=9237954 alproto="OTHER"
tlproto="UDP" srcip="172.19.236.145" srcport=57325 dstip="194.69.172.33" dstport=53
behavior="CONN" vname="DNS.Amplification.Detection" vulntype="Anomaly"

date="2022-02-10" time="18:32:54" tz="PST" logid="0604000001" devid="FAI35FT321000001"
type="ndr" subtype="IPS attack" severity="medium" sessionid=9092973 alproto="OTHER"
tlproto="ICMP" srcip="172.19.235.62" srcport=0 dstip="172.19.236.50" dstport=771
behavior="CONN" vname="BlackNurse.ICMP.Type.3.Code.3.Flood.DoS" vulntype="DoS"
```

Fields

behavior	User activity. For example, CONN, RESP, VISIT, GET etc.
vname	The virus name
vulntype	Vulnerability type

Weak cipher

```
date="2022-02-07" time="14:18:57" tz="PST" logid="0606000001" devid="FAIVMSTM21000033"
type="ndr" subtype="Weak cipher" severity="medium" sessionid=569705 alproto="IMAP"
```

```
tlproto="TCP" srcip="17.1.6.20" srcport=63310 dstip="18.2.1.114" dstport=443 behavior="CONN"
vers="2" cipher="TLS_NULL_WITH_NULL_NULL" ciphername="weak cipher"

date="2022-02-07" time="14:18:57" tz="PST" logid="0606000001" devid="FAIVMSTM21000033"
type="ndr" subtype="Weak cipher" severity="medium" sessionid=570387 alproto="SMB"
tlproto="TCP" srcip="17.2.12.171" srcport=10001 dstip="17.1.1.119" dstport=443
behavior="CONN" vers="1" cipher="TLS_RSA_WITH_AES_256_GCM_SHA384"
md5="9a157673907688965992b40304f50a1e"  ciphername="weak version"
```

Fields

behavior	User activity. For example, CONN, RESP, VISIT, GET etc. str
vers	The version of alproto
cipher	The encryption algorithm.
md5	md5/hash of ja3 fingerprint
ciphername	The type name of weak cipher or vulnerable protocols

ML

```
date="2022-02-18" time="15:54:39" tz="PST" logid="0608000001" devid="FAIVMSTM21000033"
type="ndr" subtype="ML" severity="low" sessionid=1135774 alproto="DNS" tlproto="TCP"
srcip="17.1.10.185" srcport=35546 dstip="17.1.1.119" dstport=389 reasons="Device IP,Device
MAC address,Session packet size,Transport layer protocol,Application layer protocol,Source
port number,TLS version,Id of nta_dev_ip,Protocol or application behaviors or action"
```

Fields

reasons	A list of reasons leading to a ML anomaly detection, separated by a comma.

Common Fields

date	The date the log was sent in the format xxxx-xx-xx
time	The time the log was sent in the format hh:mm:ss
tz	System timezone
logid	The ID generated by log type and log subtype
devid	Device serial number
type	ndr, str (fixed)
subtype	The anomaly type by category
severity	The severity of the traffic, defined by NDR
sessionid	The session ID referring to NDR LOG in FortiNDR
alproto	Application layer protocols

`tlproto`	Transport layer protocols
`srcip`	Source IP
`srcport`	Source port
`dstip`	Destination IP
`dstport`	Destination port

AV log samples

Log Type	Subtype	Log Sample
Event	**User**	date="2021-05-21" time="13:41:38" tz="MDT" logid="0400000001" devid="FAI35FT319000026" type="event" subtype="user" level="information" user="admin" ui="init" action="none" status="none" msg="changed settings of 'ipaddr' for 'system syslog fortianalyzer settings'"
	System	date=”2021-03-31” time=”15:50:19” tz=”PDT” logid=”0802001914” devid=”FAIVMSTM21000033” type=”event” subtype=”system” level=”information” user=”none” ui=”none” action=”none” status=”success” msg="ldapcached is being stopped; all connections to remote host(s) will be terminated."
	File-stats	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0403000001” devid=”FAIVMSTM21000033” type=”event” subtype=”file-stats” level=”information” status=”success” fileaccepted=100 fileprocessed=99 filedetected=99
	Automation	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0404000001” devid=”FAIVMSTM21000033” type=”event” subtype=”automation” level=”information” status=”success” profilename=”profile1” targetip=”10.10.3.4” policyconf=87 postaction=”block” modtime=”2021-05-13 15:16:23” attemptcnt=12
	Perf-stats	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0405000001” devid=”FAIVMSTM21000033” type=”event” subtype=”perf-stats” level=”information” status=”success” cpu=20 mem=70 logdisk=0 datadisk=21
	Malware	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0408000001” devid=”FAIVMSTM21000033” type=”event” subtype=”malware” level=”information” status=”success” featurelstcnt=19 featurelst= “Generic Trojan, Trojan, BackDoor, Application, Virus, Worm, Downloader, Redirector, Dropper, Phishing, Exploit, Proxy, Ransomware, Banking Trojan, PWS, Infostealer, Clicker, CoinMiner, WebShell” featurecounts=”35476, 81, 15, 9, 7, 3, 3, 3, 3, 1, 1,1,1,1,1,1,1,1,1” date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0408000001” devid=”FAIVMSTM21000033” type=”event” subtype=”malware” level=”information” status=”success” featurelstcnt=10 featurelst= “Generic Trojan, Trojan, BackDoor, Application, Virus, Worm, Downloader, Redirector, Dropper, Phishing” featurecounts=”35476, 81, 15, 9, 7, 3, 3, 3, 3, 1”

Log Type	Subtype	Log Sample
Attack	**Attack chain**	date="2021-05-21" time="10:23:05" tz="PDT" logid="0500000001" devhost="FAI35FT321000001" devid="FAI35FT321000001" type="attack" subtype="Attack Chain" level="alert" user="admin" ui="daemon" action="none" status="success" eventid=7255021 discoverydate="2021-05-21 10:13:27" risklevel="High", malwarefamily="N/A" scenariotype="Botnet" filecnt=1 filelist="435387294"
	Virus logs	date="2021-05-31" time="09:26:02" tz="PDT" logid="0500000001" devhost="FAI35FT319000005" devid="FAI35FT319000005" type="attack" subtype="Attack Chain" level="alert" user="admin" ui="daemon" action="none" status="success" eventid=13009509 discoverydate="2021-05-31 09:21:51" risklevel="critical", malwarefamily="N/A" scenariotype="Worm Activity" filecnt=1 filelist="1133760292" date="2021-05-21" time="10:23:05" tz="PDT" logid="0521000001" devid="FAI35FT321000001" type="attack" subtype="Proxy" level="alert" action="none" devicetype="sniffer" fossn="" fosvd="" fileid=435387294 filetype="PE" md5="ddc770fa317b4a49b4194e4dcf8d308e" virusname="W32/Rbot.15B3!tr" url="http://172.19.235.2/data/0/4B72XXXX/4B72B9D2.vRG" detype="N/A" attackerip="172.19.235.2" attackerport=80 victimip="172.19.235.76" victimport=10578 detypelstcnt=3 detypelst=”worm,trojan,downloader” detypecounts=”64,64,2”

Troubleshooting

FortiNDR troubleshooting tips

For more information about the CLI commands below, please see the *FortiNDR CLI Reference Guide*.

Best practices:

Recommendations	CLI command	Comments
Reload all services and see if the issue is still reproducible	`exec reload`	
Turn off feature learning	`exec learner off`	
If you loaded an interim build (other than GA) and are willing to wipe all db records	`exec db restore`	Run `exec reload` to see if issue is still reproducible
If you loaded an interim build (other than GA) and *cannot* wipe all db records	`diagnose system db`	Patches db at best efforts.
Retrieve and record all information	`get sys status`	If you are seeing high CPU and MEM usage, please consider provisioning more resources.
Retrieve and record all information for VMs	`diag sys vm`	Observe for any FDS code other than 200, and if not 200, please check connections to FDN and license status.

Recommended Debug Setup:

- A syslog server for FortiNDR events log as the GUI only has *1 days* events.
- A TFTP server for PCAP capture transfer.

General Debug Logs Retrieval

Scenario	CLI
Collect all crash logs from the first day FortiNDR started	`diagnose debug crashlog <crash_log_date>`
Record kernel related logs from the bootup and save it to a file	`diagnose debug kernel display`

File scanning related issues

The following troubleshooting tips are intended to diagnose the error message: *File Not Accepted (Client side shows files are submitted but NDR does not have details of file)*.

To perform a general check:

1. Check and record network conditions from the FortiNDR server to file submitting clients using the following CLI commands:
   - `exec ping`
   - `exec traceroute`
2. Make sure all KDBs are updated. For example, no pending updates, no out of date db and no updating.
3. Try submitting a lower throughput, (no archive file type, smaller file size) to see if it is still reproducible.
4. Follow the PCAP dumping guide to dump files from port1 or port2 to make sure the traffic is there. Open *dapture pcap* with Wireshark to see if there are any redline/blacklines from Wireshark default filter setting which indicates bad network traffic quality. From previous troubleshooting experience, this is the most frequent cause of *File Not Accepted*.

Troubleshooting ICAP issues:

1. After you reproduce the issue:
   a. Retrieve the latest ICAP server logs by running the CLI command: `diag debug icap`
   b. Save the server logs to a file.
2. Usually you can resolve any outstanding issues by running the following CLI command: `exec reload`

Troubleshooting OFTP issues:

1. From OFTP clients (usually FortiGate), record all traffic forward/AntiVirus Event logs from the Fortigate side.
2. Refer to PCAP capturing guide, and save corresponding PCAPs.

Troubleshooting HTTP2 issues from FortiGate v7.0 onwards:

Recommendation	Run the following CLI command:
Record output and check for errors	`diagnose system csf global`
Record output and make sure status is *authorized*	`diagnose system csf upstream`
Collect logs	`diag debug enable` and `diagnose debug csfd 7`

Manual Upload/API Submission/FortiSandbox Integration

For all issues:

Start with a single file upload and fetch results from the same subnet as directed from where the client resides. See Appendix A - API guide on page 163.

To verify the process is successful:

If a single file submit/fetch is working from the previous step. Run the following CLI commands:

- `diag debug enable`

and

- `diagnose debug application 7`

Record all output and look for any non `200 http` code or stack traces.

File Submitted but not processed

Collect all the information from the process and record it using the following CLI commands:

- `diag debug enable`

and

- `diagnose debug process <process_name>`

Information for support tickets

If none of these recommendations work and you need to create a support ticket, please include the following information:

1. PCAPs from Port1 or Port2 sniffer capturing. If the poc includes private traffic you do not want to share, provide a general analysis from NDR's port1 or port2 from Wireshark. Include stats about the default filter, redlines and black line (tcp error).
2. What actions were taken.
3. Logs collected from your troubleshooting steps.

FortiNDR health checks

When FortiNDR is set up, use the CLI command `diag sys top` to check that the following key FortiNDR processes are running. For NDR to function correctly the following processes are required to run: `ndrd`, `isniff4ndr`

`sniffer`	Sniffer daemon.
`ndrd`	NDR daemon.
`isniff4ndr`	Second Sniffer daemon.
`fdigestd`	Upload file daejmon
`oftpd`	OFTP daemon that receives files from FortiGate.
`pae2`	Portable executable AI engine.
`pae_learn`	Portable executable AI learner. If no features have been learned, this process does not appear.

`moat_engine`	Script AI engine.
`moat_learn`	Script AI learner.

To turn network traffic detection on and off:

Run the following command:

```
exec ndrd <on/off>
```

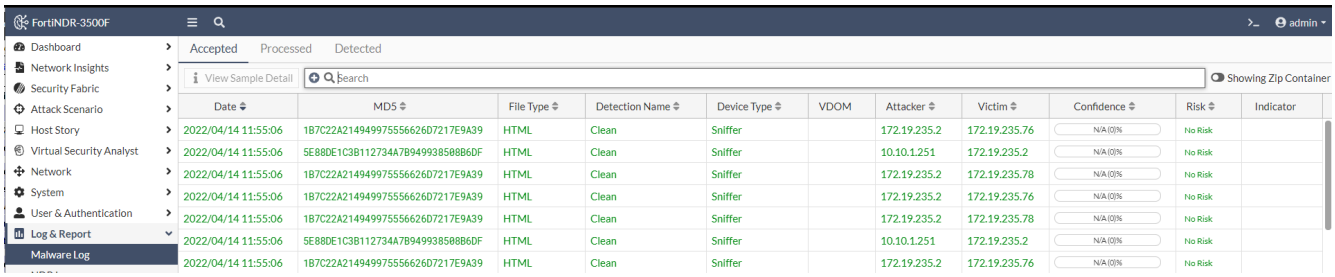
To turn sniffer malware detection on and off for troubleshooting:

Run the following command:

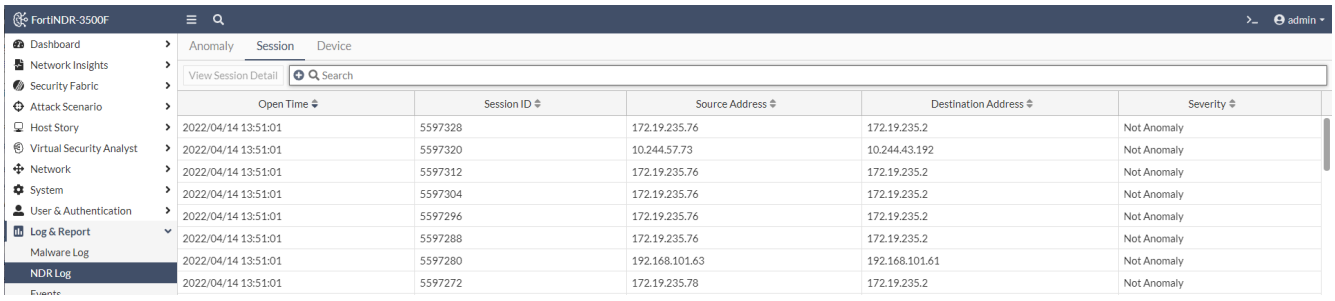
```
exec snifferd <on/off>
```

The current version of the Malware sniffer only sniffs traffic on Port2.

When FortiNDR sniffer malware detection feature is operating normally, *Log & Report* > *Malware Log* > *Accepted* shows the following accepted traffic:



Log & Report > *NDR Log* > *Session* shows the incoming sessions.



Sniffer diagnosis

Use the CLI command `diag sniffer file ?` to show sniffer output for port2. The TFTP server is required to store sniffer output.

The sniffer will not save unsupported file types or supported but corrupted files. For example, if the traffic contains a corrupted zip file that cannot be unzipped, the sniffer will not save it to the *Log & Report >Malware Log*.

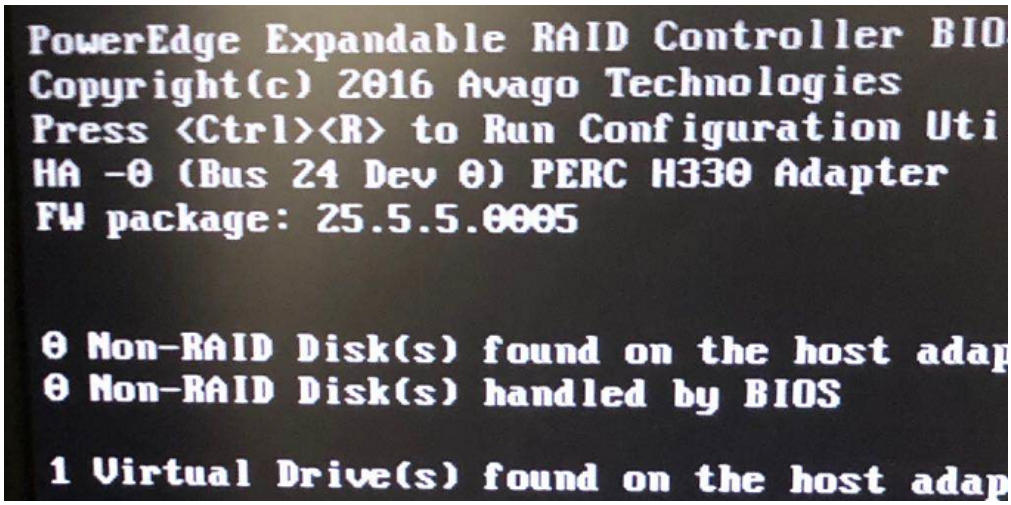
Rebuild RAID disk

If you need to rebuild the data disk and configure FortiNDR-3500F from scratch, follow this procedure.

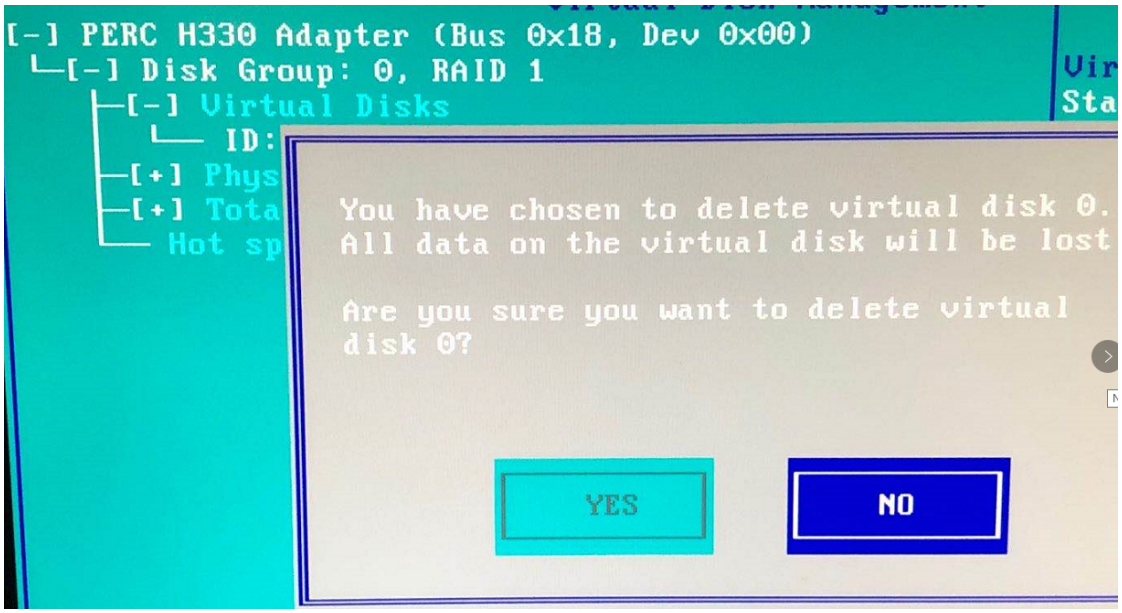
To rebuild the RAID disk:

1. Plug the monitor and keyboard directly into FortiNDR.

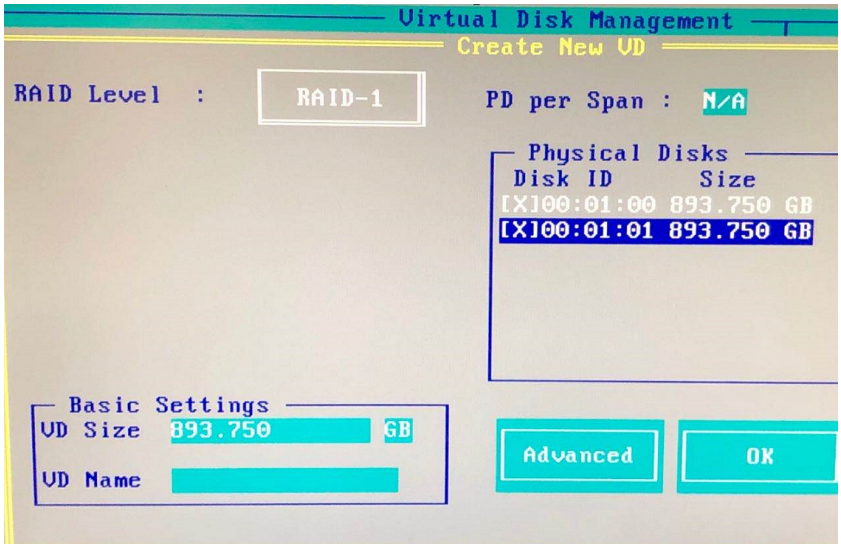
2. Boot FortiNDR and keep pressing `Ctrl R` when FortiNDR is booting.



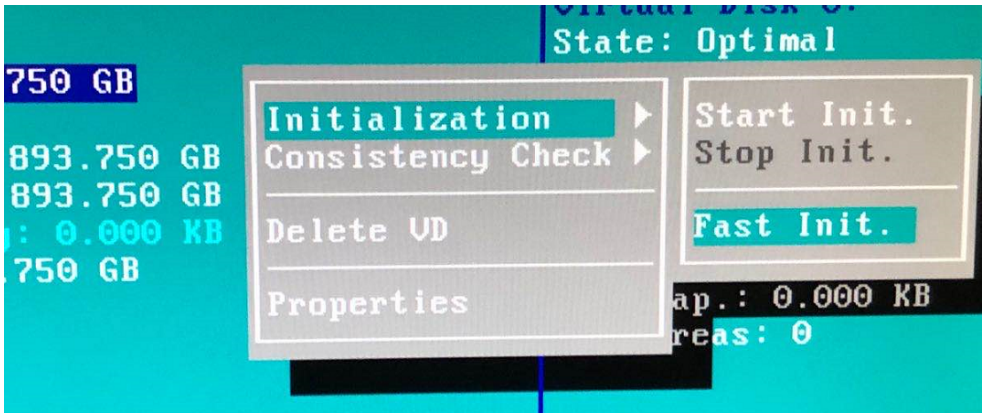
3. Delete virtual disk 0.



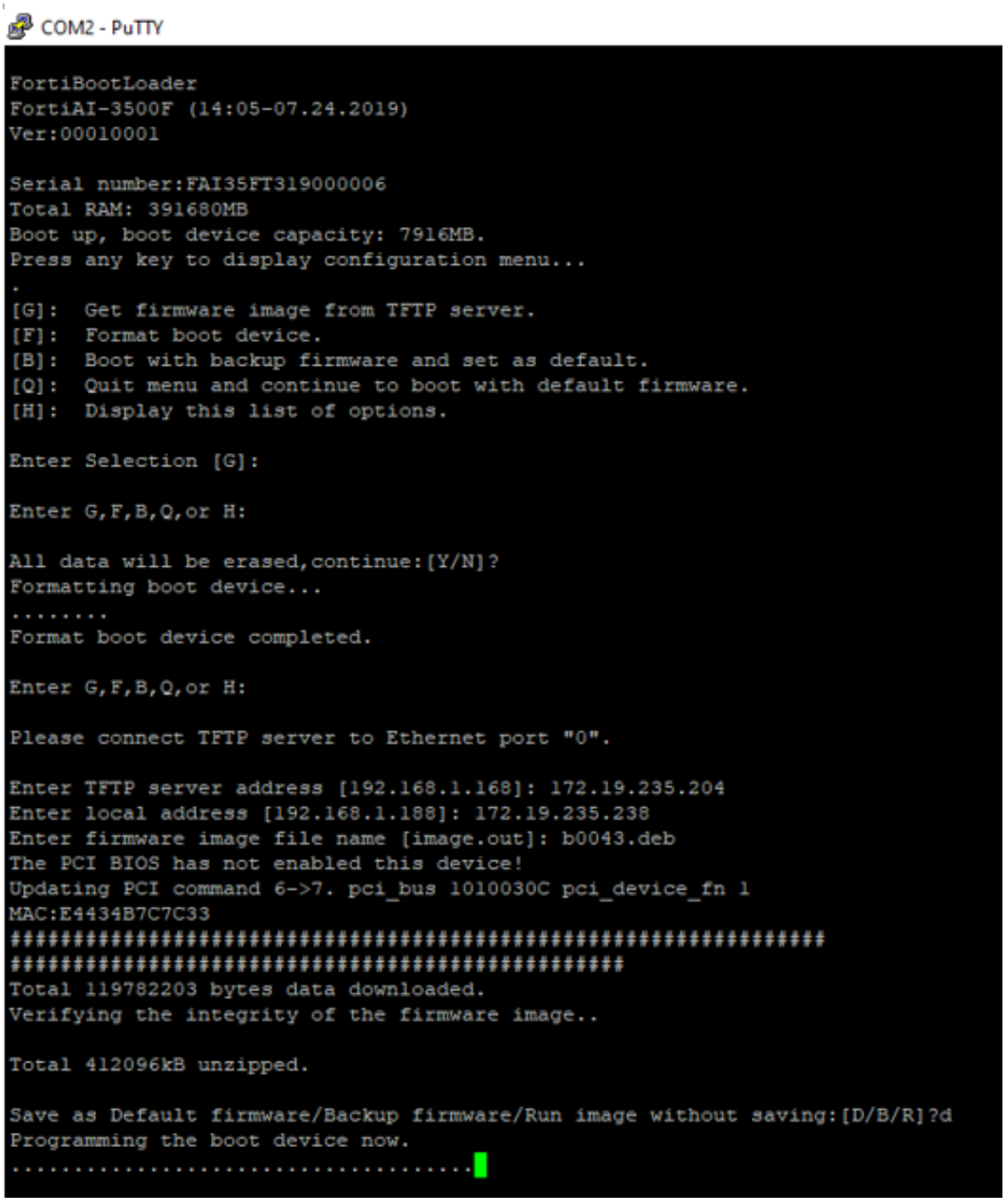
4. Create a virtual disk at *RAID Level 1*.



5. Fast init the new virtual disk.



6. When the initialization is finished, reboot FortiNDR.
7. During reboot, press any key to enter bootloader.
   Ensure the keyboard is not plugged directly into FortiNDR as that might prevent you from entering into the bootloader menu.



8. Plug the monitor and keyboard back into the machine with the COM1 connection.
9. Enter F to format the boot drive.
10. Enter G to get the firmware image from the TFTP server.
    Getting firmware from TFTP server requires connecting to the TFTP server using port4 (1G port).

11. When booting is complete, use the command `execute factoryreset` or `execute partitiondisk` to make partitions.
12. Copy the ANN database to FortiNDR since rebuilding RAID deletes the ANN database.

Managing FortiNDR disk usage

FortiNDR analyzes files and packets 'on the fly' and requires plenty of disk space to store attacks. FortiNDR -3500F comes with four SSD drives by default and can add up to 16 SSD in total.

By default, FortiNDR stores all detected events (network anomalies, sessions and malware detection). When the disk reaches:

Disc Usage	Description
90%	The FortiNDR system will terminate all of its services, including logging, detection, sniffer, network share scanning, file uploading, OFTP, ICAP, and NDR. However, the graphical user interface (GUI) and command-line interface (CLI) console will remain operational in this scenario. To restore the services, the user could execute the 'exec cleanup' command.

Tip 1: Database logs have time to live set to 264 days which is the max theoretical retention days for all models.

Tip 2: With FortiAI and FortiNDR 3500F, users can purchase more SSDs. Please see the data sheet and ordering guide for details.

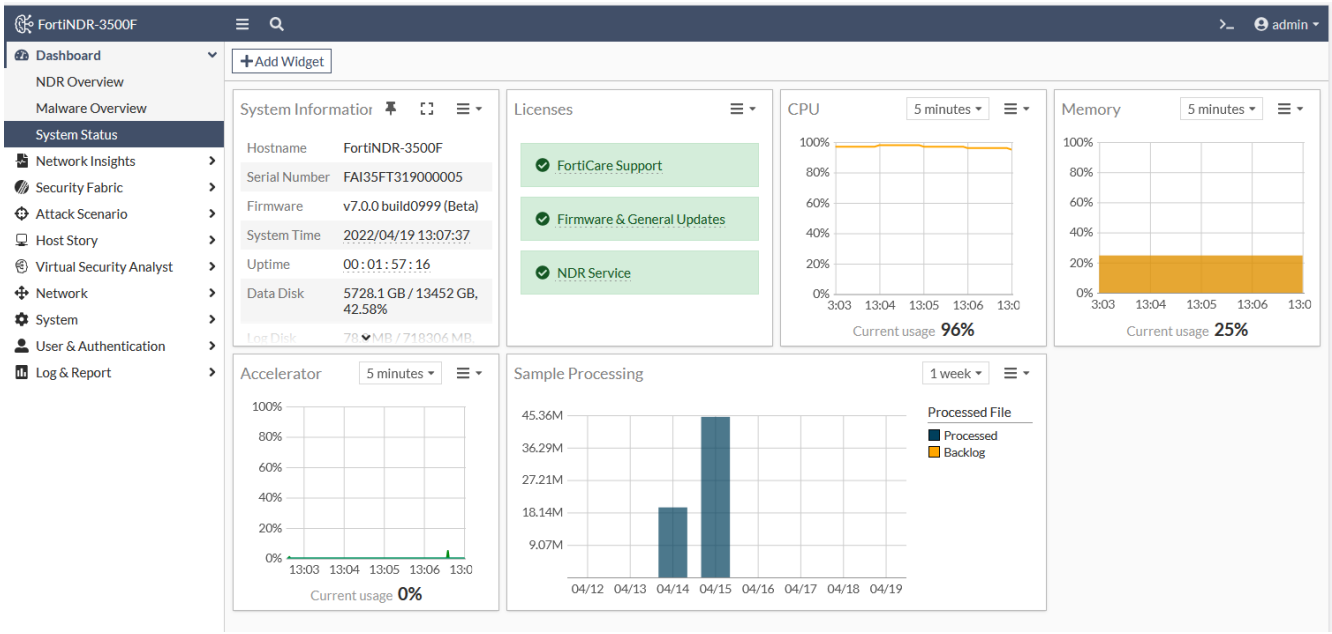
Tip 3: You should consider using CLIs to clean up the DB:

`execute cleanup`	This command removes all logs including all counts in Dashboard, Malware Log, NDR log, ML Discovery log, but will keep ML baseline and feedback.
`execute cleanup ml`	This command will clean up all ML Discovery logs. It also retrains baseline, but keeps user feedback.
`execute cleanup ndr`	This command removes logs including: NDR related widgets on the Dashboard, NDR log, ML Discovery log, but will keep ML baseline and feedback. This is a subset of `execute cleanup`.
`execute db restore`	This command cleans all the database data and log including what `execute`

`cleanup` does and also ML baseline/feedback, Scenario AI DB and Binary Behavior DB, which is updated from FortiGuard.

To view the disk usage:

Go to *Dashboard* > *System Status*.



To expand FortiNDR VM storage with the CLI:

`execute expandspooldisk`.

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

Exporting detected malware files

You can export detected malware files with the CLI or with the GUI under *Attack Scenario* or *Log & Report* as a PDF, JSON and STIX2 file.

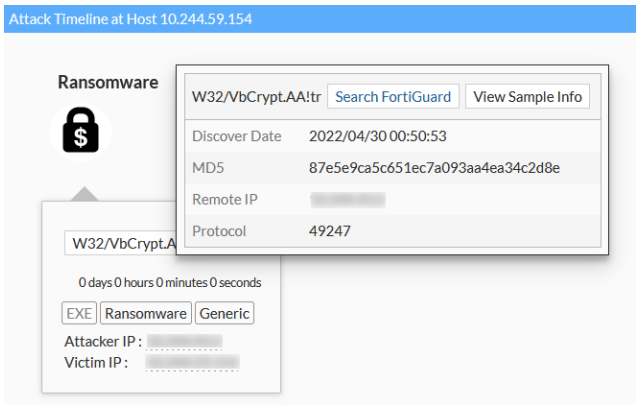
To export detected malware files with the CLI:

```
execute export file-report
```

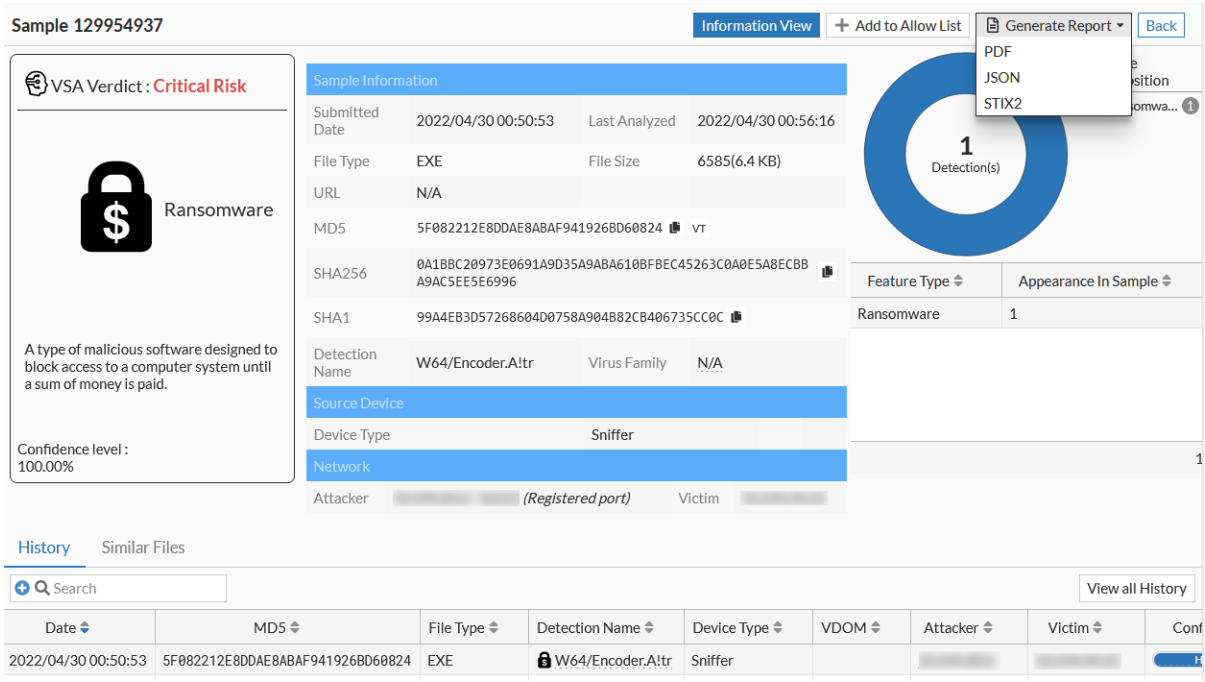
For more information, see the *FortiNDR CLI Reference Guide*.

To export detected malware files with the GUI:

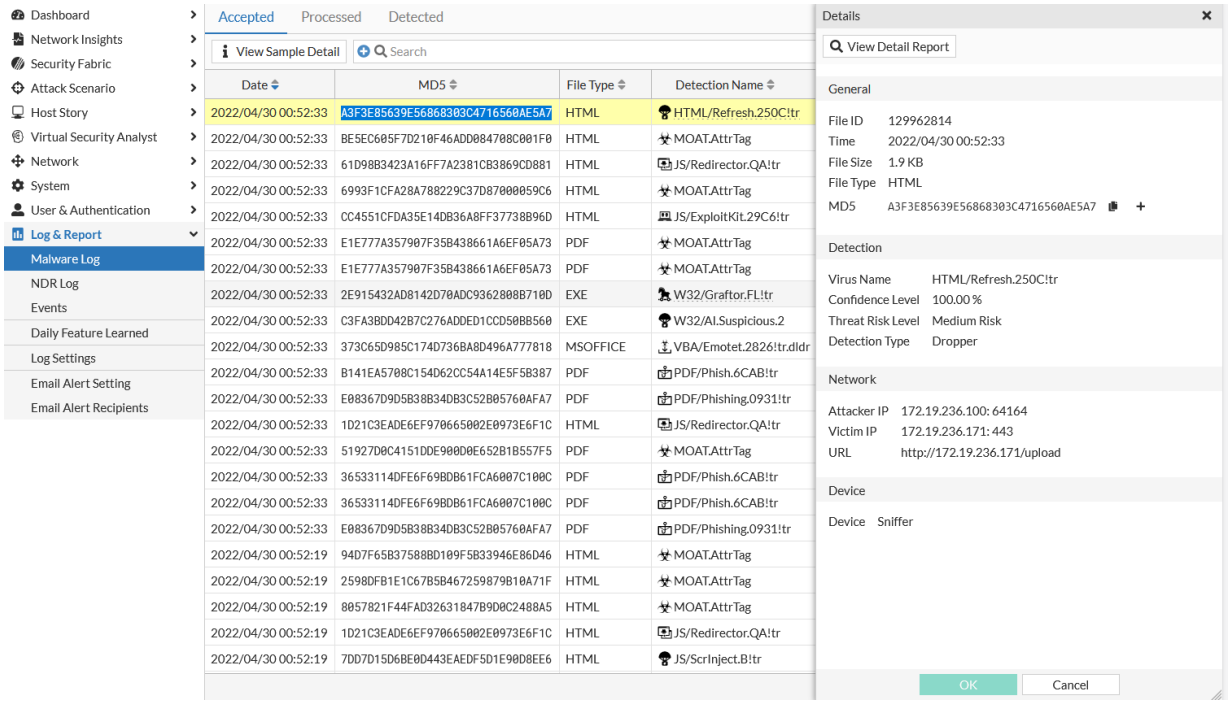
1. To export detected files under *Attack Scenario*:
   a. Go to *Attack Scenario* and click an attack type such as *Ransomware*.
   b. Select an infected host and then in the timeline, hover over the detection name until the dialog appears.



   c. Click *View Sample Info*. The sample information is displayed.
   d. Click *Generate Report* and select *PDF*, *JSON*, or *STIX2* format.



2. To export detected files under *Log & Report* :
   a. Go to *Log & Report* > *Malware Log*.
   b. Double-click a log in the list. The *Details* pane opens.



   c. Click *View Detail Report*. The sample information is displayed.
   d. Click *Generate Report* and select *PDF*, *JSON*, or *STIX2* format.

Formatting the database

To format the database with the CLI:

```
execute db restore
```

Using `execute db restore` will format and delete the entire database.
Use caution when executing this command and backup detection beforehand if required.

Export malware

In v1.3 and higher, you can export detected malware and history logs.

To export the FortiNDR detection history as a .csv file:

```
execute export {disk|scp|ftp|tftp} <filenmame-to-be-saved> <server>[:ftp port] <user-name>
     <password>
```

To export the detected files by FortiNDR as a zip file with password:

```
execute export detected-files {disk|scp|ftp|tftp} <filenmame-to-be-saved> <server>[:ftp
     port] <user-name> <password>
```

The zip file default password is `infected`.

Working with false positives and false negatives

Every technology encounters false positives and false negatives, and expectations need to be realistic.

For example, when there is a lot of HTTP traffic from sniffer, you might have some false positive files among thousands of files. If there are five false positive samples out of 2000 files, the false positive rate is: 0.25%.

False negative is when FortiNDR does not detect a malware.

Ensure you are using the latest ANN. Check the latest version of FortiNDR ANN at https://www.fortiguard.com/services/fortindr.

Troubleshoot ICAP and OFTP connection issues

To check ICAP traffic in port1:

Use the CLI command:

```
diagnose sniffer packet port1 'port 1344 or port 11344' 6 0
```

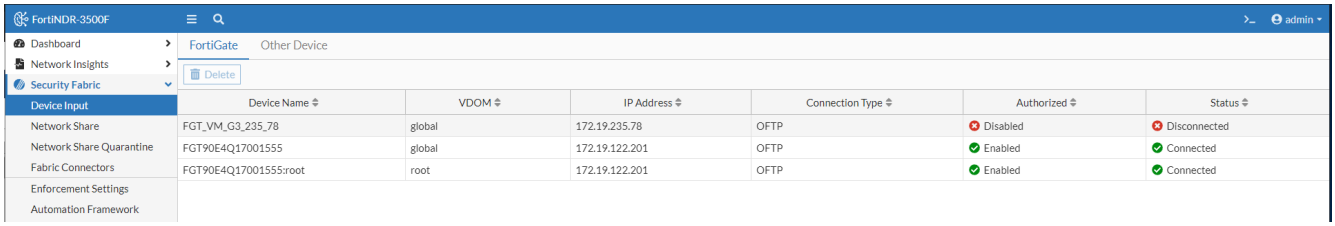
To check OFTP traffic in port1:

Use the CLI command:

```
diagnose sniffer packet port1 'port 514' 6 0
```

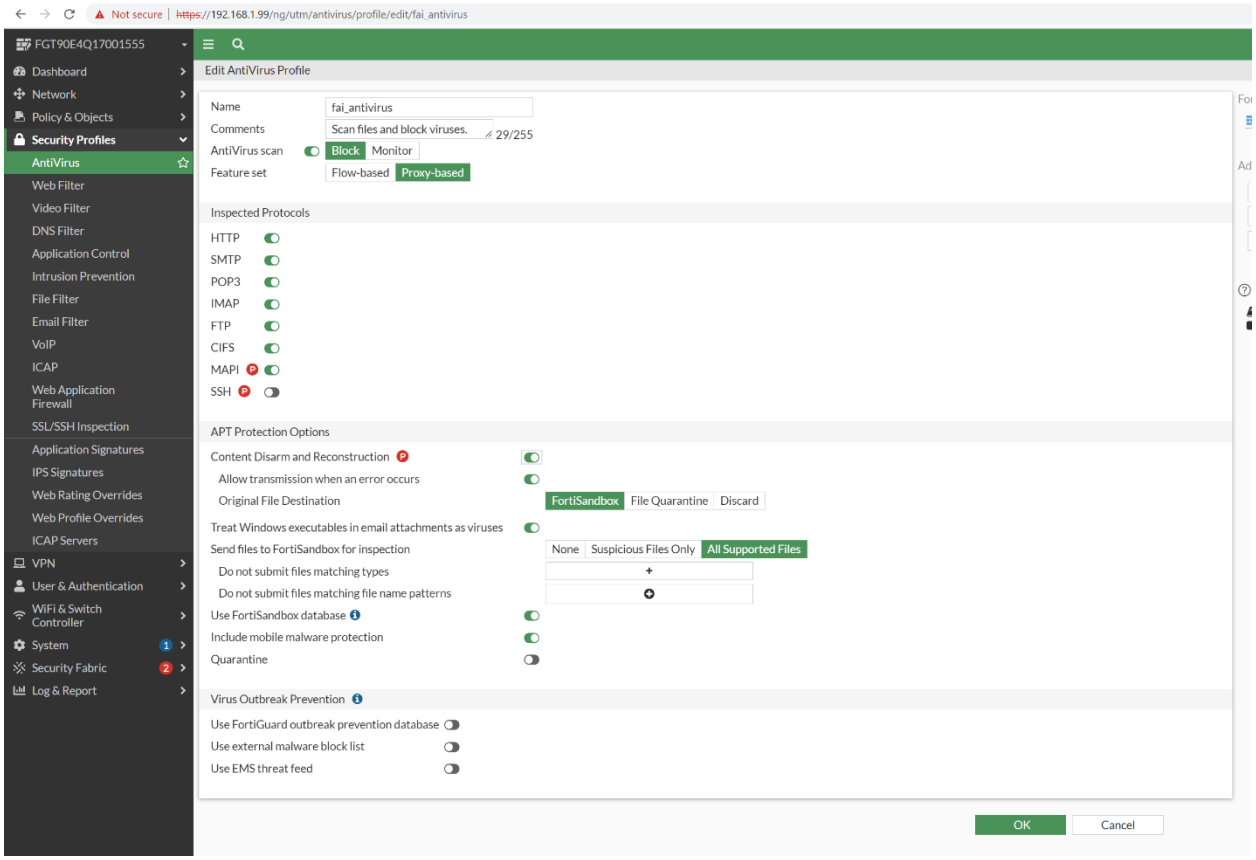
To verify a device is authorized:

Go to *Security Fabric* > *Device Input* and check the Authorized column.



To verify All Supported Files are enabled in FortiGate:

Go to *Security Profiles* > *AntiVirus* and verify *Send files to FortiSandbox for inspection* is set to *All Supported Files*.



To verify the firewall policy is not blocking the connection:

Check if firewall policy is blocking ICAP port 1344, 11344 and OFTP port 514.

Troubleshoot Log Settings

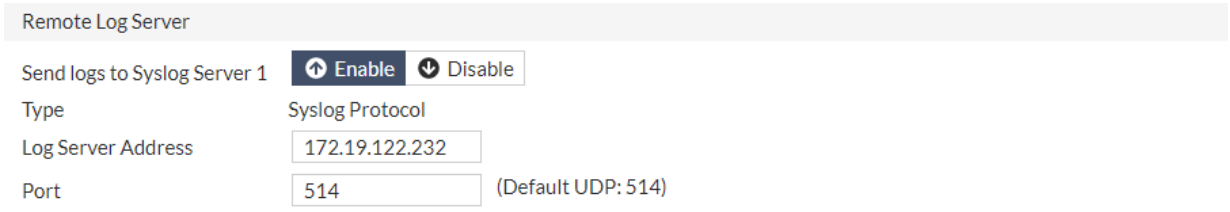
To troubleshoot the Client:

- Enable *Send logs* to your syslog server
- Verify you are using a valid remote server address

- Check if the GUI settings match CMDB settings:
  - Send logs to FortiAnalyzer/FortiSIEM


```
FortiNDR-3500F # config system syslog fortianalyzer settings

FortiNDR-3500F (settings) # get
Last Update Time     : 2022-04-13 19:22:13
ipaddr               : 172.19.235.98
port                 : 514
status               : enable
type                 : event malware ndr
ndr-severity         : low medium high critical
```

  - Send logs to Syslog Server 1




```
FortiNDR-3500F # config system syslog1 settings

FortiNDR-3500F (settings) # get
Last Update Time     : 2022-04-14 15:21:48
ipaddr               : 172.19.122.232
port                 : 514
status               : enable
type                 : event malware ndr
ndr-severity         : low medium high critical
```

- An extra remote server setting which only set via CLI command

```
FortiNDR-3500F # config system syslog2 settings

FortiNDR-3500F (settings) # get
Last Update Time     :
ipaddr               : 0.0.0.0
port                 : 514
status               : disable
type                 : event malware ndr
ndr-severity         : low medium high critical

FortiNDR-3500F (settings) #
```

To view the traffic with the CLI:

```
diag sniffer packet any "udp and port 514" 3 0 a
```

To troubleshoot the server:

- Verify the sever has rsyslog installed.
- Make sure udp port 514 is open

  ```
  sudo ss -tulnp | grep "rsyslog"
  ```

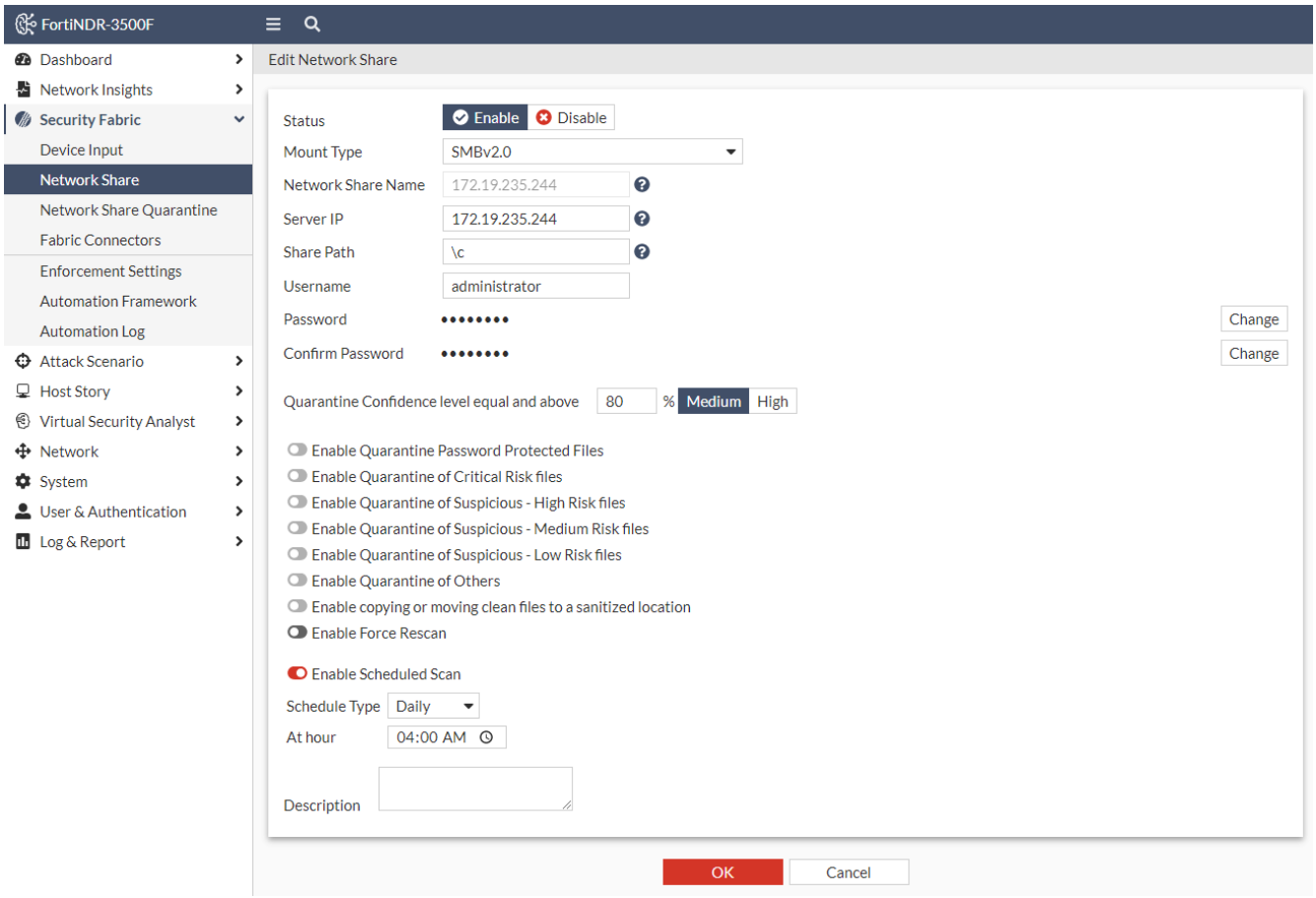
Troubleshoot Network Share

Test the Network Share Connection

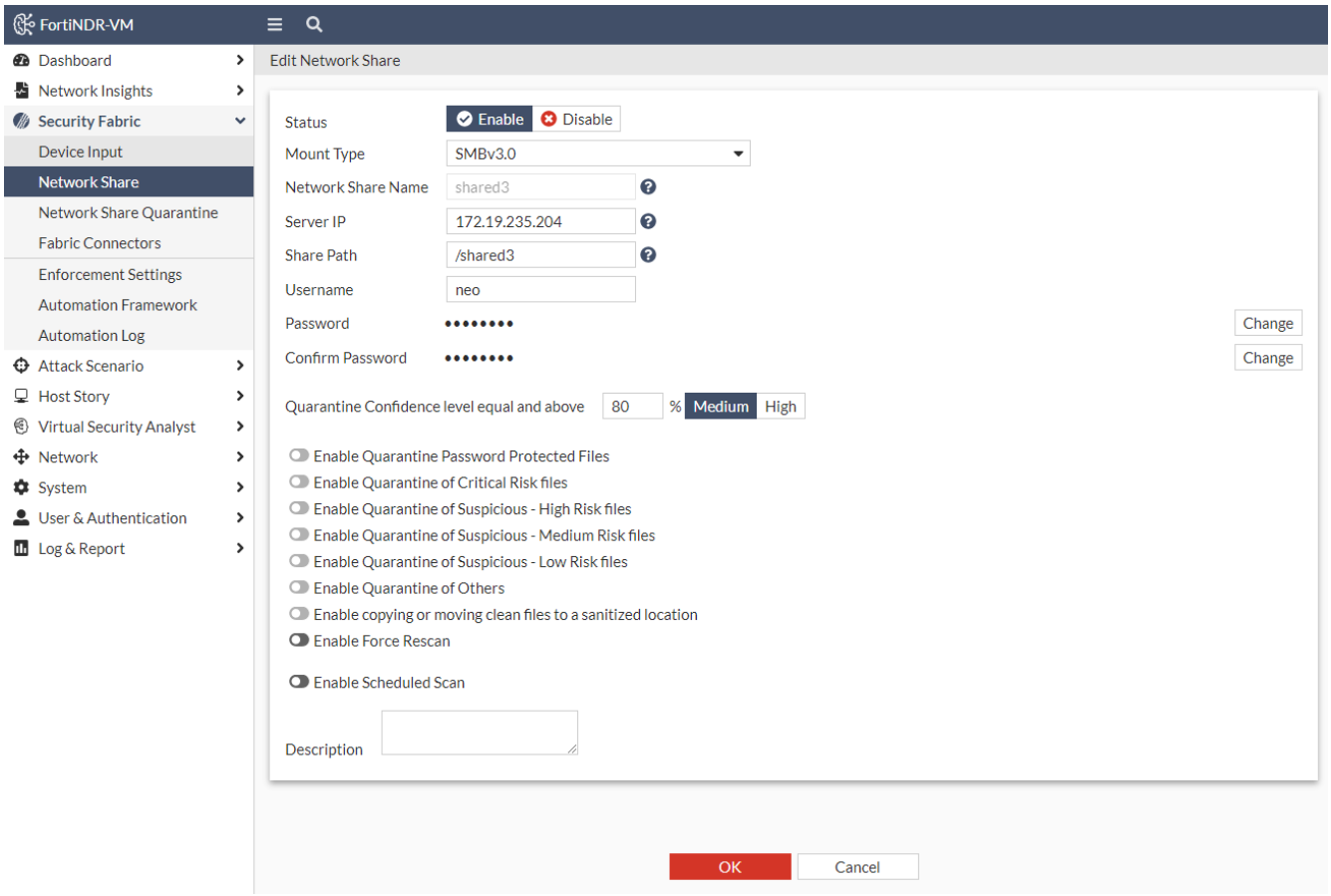
To test the Network Share Connection:

- Verify the Remote Sever is connectable
- Verify the folder to mount is shareable
- Verify the current user has read and write permissions to the shared folder.
- Verify you have chose the correct mount type, e.g. Windows 10 will not support SMB1.0 if SMB 1.0/CIFS File Sharing Support isn't turned on
- Verify the Share Path is using a backslash (\) for Windows Folders while forward (/) slash for Linux Folders

The following images shows the Network Share configuration for Windows.



The following images shows the Network Share configuration for Linux.



Diagnosing Network Share Errors

To diagnose Network Share scanning errors:

Run the following CLI commands:

```
diagnose debug application sdigestd DEBUG_LEVEL <1,2,4,7>
diagnose debug enable
```

A `DEBUG_LEVEL` is a bit mask consisting of four bits.

DEBUG_LEVEL	Will show:
1	Only the error. For example, `memory allocation error`.
2	The warning messages. For example, `connection warning`, `job scheduling warning` etc. A `DEBUG_LEVEL` of `2` is a good start to find an issue.
4	The information. For example, `job creation`, `file scanned` etc.
7	All events and errors.

To troubleshoot mounting problems:

If you still have mounting problems which are not indicated by the CLI above, try running the following CLI command:

```
diagnose debug kernel display
```

Keep an eye for any message about `CIFS`. For example:

```
[280041.880696] CIFS VFS: Free previous auth_key.response = ffff881c78591200
```

You will see the error code if the mounting failed.

To troubleshoot a Network Share scan that it is stuck:

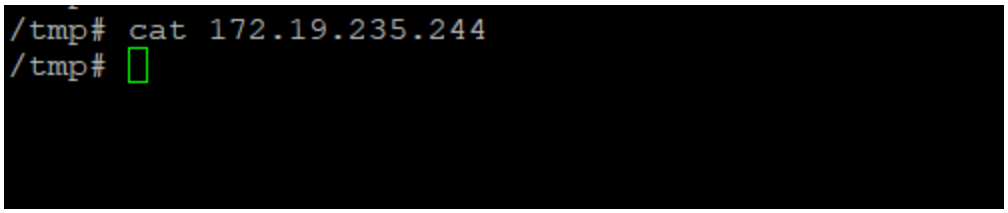
A scanning job may get stuck for the following issues:

Issue	Recommendation
Mounting issue	See To troubleshoot mounting problems above.
Daemon crashed	Run the following CLI command to see if there are any `sdigestd` related crashes: `diagnose debug crashlog xxxx-xx-xx`
Data disk usage over 90%	Clean up the data disk. See, Managing FortiNDR disk usage on page 146.

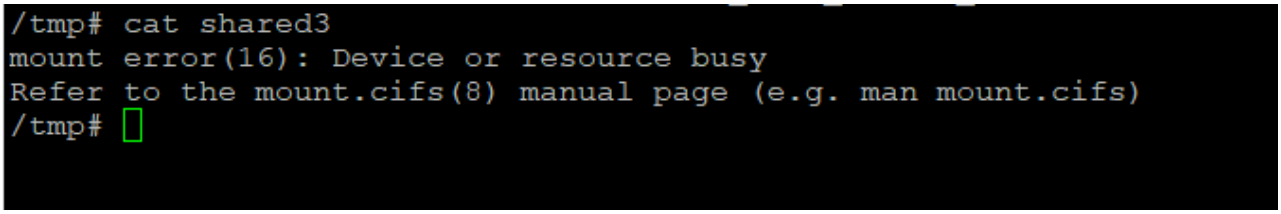
Debug version image

If you are using debug version image, check the `/tmp/NETWORK_SHARE_NAME` for mounting message

- If the message is empty, there is no mounting issue detected



- Otherwise, refer to *mount.cifs*, *mount.nfs* documents



- Double-check, the direct mounting path `/tmp/mnt/SHAREID` and see if the files exist.

Check Crash Log

Go to '`/var/spool/crashlog/DATE` and check for any crash logs about *sdigest*.

Troubleshooting the VM License

To view the status of the VM license:

```
diagnose system vm
```

When using a VM with a new UUID with an existing license (for example, if you have to respawn a new VM due to disk failure and reuse the existing VM license), it will take 90 mins before the FDS server will accept/validate the new license.

Troubleshooting Updater

FDS Authorization Failed

Go to the *System* > *FortiGuard*.

If the following databases show *FDS Authorization Failed*, that means the FortiNDR unit is using a Fortiguard License that does not include FortiNDR entitlements (for example, a machine that was upgraded from FortiAI v1.5.3 GA to FortiNDR v7.0 GA).

Although some functions will still work, important new features in v7.0 such as web filtering cannot be used and any NDR-related databases cannot be downloaded. Please contact sales for information about updating the existing FortiGuard support license.

Application Control DB	Version 18.00072	FDS Authorization Failed
Industrial Security DB	Version 18.00187	FDS Authorization Failed
Network Intrusion Protection DB	Version 18.00072	FDS Authorization Failed
Traffic Analysis DB	Version 20.00001	Up to Date
Botnet IP DB	Version 4.728	FDS Authorization Failed
GeoIP DB	Version 2.001	Update Available
Botnet Domain DB	Version 2.007	Update Available
JA3 DB	Version 1.000	FDS Authorization Failed
JA3S DB	Version 1.000	FDS Authorization Failed

For other FDS Authorization Failed errors, this is most likely due to an expired FortiGuard support license or a network configuration problem such as a DNS setting that is directing the updater to the wrong FDS servers.

Clearing updater cache files

Normally, after triggering an update through the CLI with `exec update now` or through the GUI with the *Update FortiGuard Neural Network Engine* button, the status will change to *Downloading* or *Installing*:

	Downloading..	
Text AI Feature DB	Version 1.087	Up to Date
Text AI Group DB	Version 1.087	Up to Date

Sometimes an update will not go through due to failed FDS connection during a download and the cache will need to be cleared.

Running the command and then try updating again:

```
exec update clean-up
```

Thius should solve that problem. Rebooting the machine will also trigger a FDS download cache-cleanup operation upon startup.

Diagnosing Other FDS Errors

To further diagnose updating errors, please run the CLI commands:

```
diagnose debug application updated DEBUG_LEVEL
diagnose debug enable
```

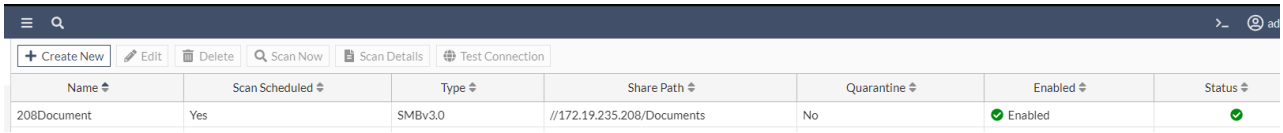
A DEBUG_LEVEL is a bit mask consisting of 3 bits.

- A `DEBUG_LEVEL` of 1 will show only the error. Usually a `DEBUG_LEVEL` of 1 is enough to pinpoint the problem.
- A `DEBUG_LEVEL` of 3 will show all major events and errors.
- A `DEBUG_LEVEL` of 7 will show all events and errors.

Troubleshooting tips for Network File Share

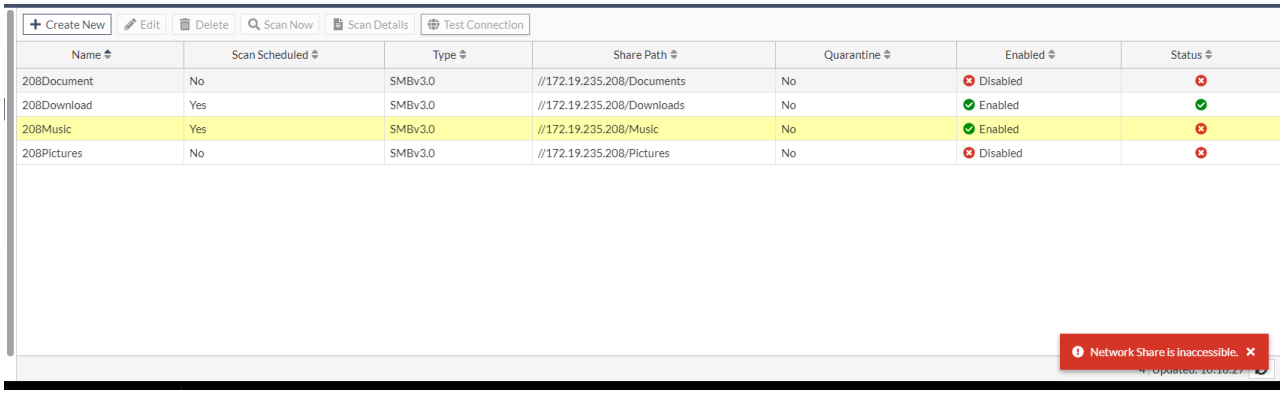
To troubleshoot Network File Share issues:

1. Disable or delete other mounts and limit the network share mount to only one so that the logs that are collected later on will not be too complex.

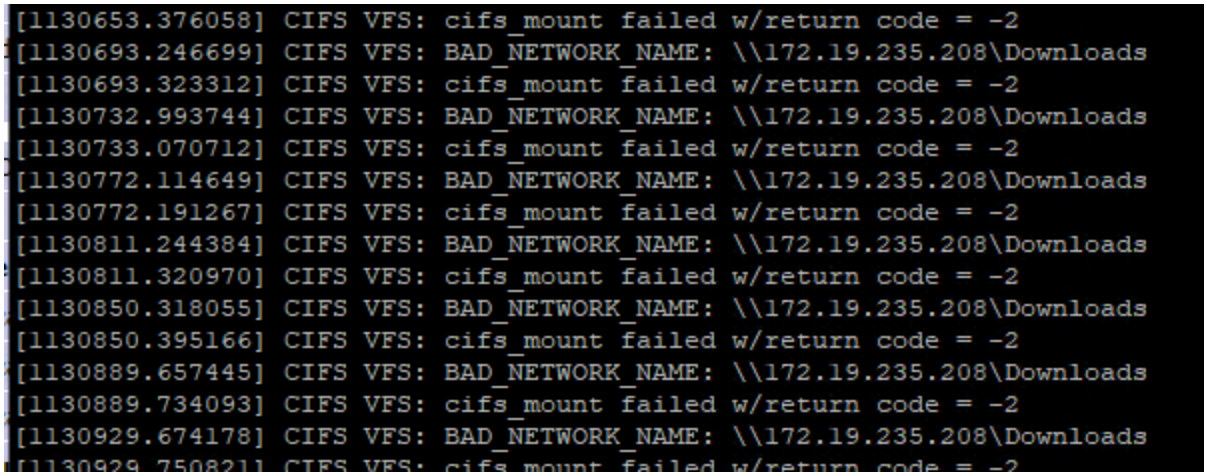


2. Turn off FortiGuard scheduled updates to rule out any update related issues.
3. Turn off the NDR daemon to isolate the environment using CLI command:
   ```
   exec ndrd off
   ```
   This command is not persistent. If a reboot is required, run the command again.
4. Turn off Sniffer daemon to isolate the environment using
   ```
   exec snifferd off
   ```
   This command is not persistent. If a reboot is required, run the command again.
5. 5. Set filesize limit to smaller size to rule file size issues using the CLI command:
   ```
   exec file-size-threshold network-share 20 (MB)
   ```

6. Click *Test Connection*.
   - If *Network Share is inaccessible* is returned, it means FortiNDR cannot mount the folder. Proceed to the next step to check the detail about the mount error. Sometimes it takes time for the network share's setting to sync in the server. If you change the network share setting in the server, you may not connect to it right away.
   - If *Mounting in progress*is returned, wait about 2-5 minutes and try again.



7. When the scan is stuck, please the following logs using the CLI:
   a. a. `exec deb kernel display`



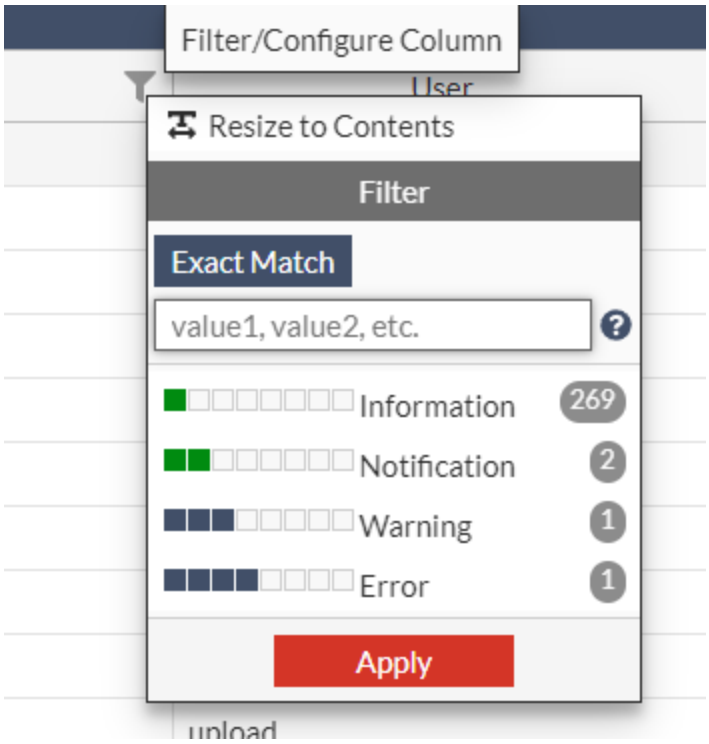
   `Return code = -2` is the most common error. Most times it means there were too many connections to the folder or the folder is not accessible for mounting yet.

   b. `exec deb crashlog <the date this issue occured>`

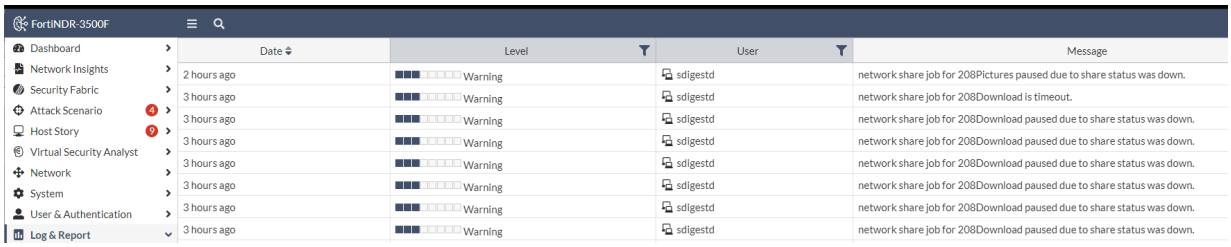
8. Get system status and save the output log to determine if the issue is related to storage.
   `get system status`

```
BIOS version:                   00010001
Log disk:                       Capacity 349 GB, Used 76 MB (0.03%), Free 349 GB
Data disk:                      Capacity 6710 GB, Used 910 GB (13.57%), Free 5799 GB
Remote disk:                    n/a
Memory:                         Capacity 375 GB, Used 76 GB (20.32%), Free 299 GB
Swap Memory:                    Capacity 31 GB, Used 0 MB (0.00%), Free 31 GB
Hostname:                       FortiNDR-3500F
HA configured mode:             Off
HA effective mode:              Off
Strong-crypto:                  enabled
Distribution:                   International
Branch point:                   27
Uptime:                         13 days  5 hours  33 minutes
Last reboot:                    Fri Nov 04 16:23:45 PDT 2022
System time:                    Thu Nov 17 20:57:12 PST 2022
Firmware & ANN update expiry:   Sun Mar 12 00:00:00 PST 2023
NDR services/update expiry:     Mon Feb 20 00:00:00 PST 2023
Binary AI Feature DB:           1.11000(2022-11-17 20:28)
```

9. For network share scan errors, go to *Log & Report > Events*.
   a. Select *Level: Warning, Error and User: sdigestd*
   b. Take a screen shot. The *Events* page contains 1 day history.
   c. To record more history, use the Log settings to set logs to another logging device.



This is example below, network share is experiencing mounting problems. Share status was down meaning at that time this FortiNDR could not access the remote mounting folder:



10. Open *sdigestd* log using the following command:<ERROR>

```
diagnose debug crashlog xxxx-xx-xx
```

`sdigestd`is the daemon responsible for network share mount and copying. 7 means all level logs, if there are too many logs, use 2 <WARN> or 1.

For more information, see Troubleshoot Network Share on page 153.

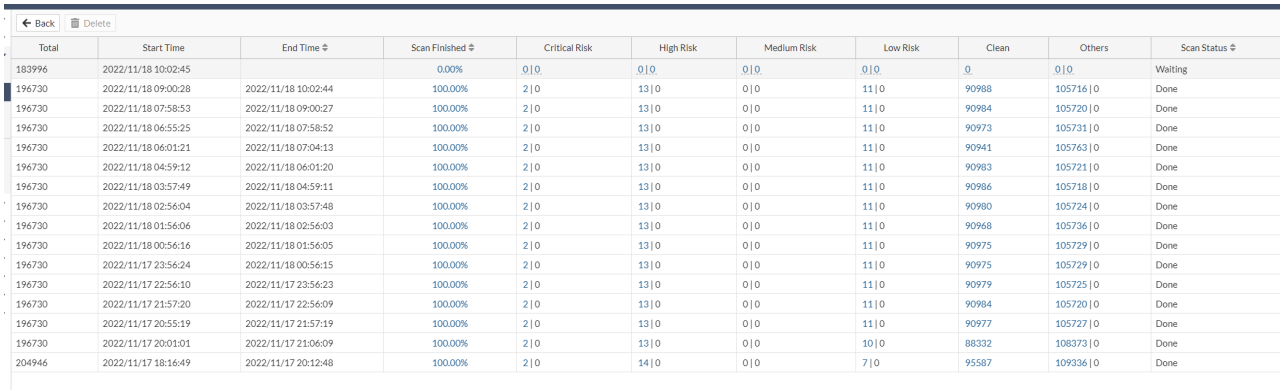
You can configure a scheduled scan,by clicking *Scan now* in the GUI, or you can trigger the output right away with the CLI:

- `diag deb app sdigestd 7`
- `diag deb enable`

Here is an example showing which mount failed during mounting:

```
FortiNDR-3500F # diag deb enable
System Time:  2022-11-17 20:55:40 PST (Uptime: 13d 5h 31m)

FortiNDR-3500F # 11.17-20:55:42 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Document

11.17-20:55:42 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Document)

11.17-20:55:42 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Pictures)

11.17-20:55:42 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Pictures)

11.17-20:55:42 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Music)

11.17-20:55:42 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Music)

11.17-20:55:48 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Document)

11.17-20:55:48 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Document)

11.17-20:55:48 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Pictures)

11.17-20:55:48 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Pictures)

11.17-20:55:48 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Music)

11.17-20:55:48 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Music)
```

11. The image below shows how the completed scan jobs for Network File Scan should look:



Back Delete

Total	Start Time	End Time	Scan Finished	Critical Risk	High Risk	Medium Risk	Low Risk	Clean	Others	Scan Status
183996	2022/11/18 10:02:45		0.00%	0 | 0	0 | 0	0 | 0	0 | 0	0	0 | 0	Waiting
196730	2022/11/18 09:00:28	2022/11/18 10:02:44	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90988	105716 | 0	Done
196730	2022/11/18 07:58:53	2022/11/18 09:00:27	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90984	105720 | 0	Done
196730	2022/11/18 06:55:25	2022/11/18 07:58:52	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90973	105731 | 0	Done
196730	2022/11/18 06:01:21	2022/11/18 07:04:13	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90941	105763 | 0	Done
196730	2022/11/18 04:59:12	2022/11/18 06:01:20	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90983	105721 | 0	Done
196730	2022/11/18 03:57:49	2022/11/18 04:59:11	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90986	105718 | 0	Done
196730	2022/11/18 02:56:04	2022/11/18 03:57:48	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90980	105724 | 0	Done
196730	2022/11/18 01:56:06	2022/11/18 02:56:03	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90968	105736 | 0	Done
196730	2022/11/18 00:56:16	2022/11/18 01:56:05	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90975	105729 | 0	Done
196730	2022/11/17 23:56:24	2022/11/18 00:56:15	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90975	105729 | 0	Done
196730	2022/11/17 22:56:10	2022/11/17 23:56:23	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90979	105725 | 0	Done
196730	2022/11/17 21:57:20	2022/11/17 22:56:09	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90984	105720 | 0	Done
196730	2022/11/17 20:55:19	2022/11/17 21:57:19	100.00%	2 | 0	13 | 0	0 | 0	11 | 0	90977	105727 | 0	Done
196730	2022/11/17 20:01:01	2022/11/17 21:06:09	100.00%	2 | 0	13 | 0	0 | 0	10 | 0	88332	108373 | 0	Done
204946	2022/11/17 18:16:49	2022/11/17 20:12:48	100.00%	2 | 0	14 | 0	0 | 0	7 | 0	95587	109336 | 0	Done

Appendix A - API guide

This section shows how to use the FortiNDR API.

Get an administrator API key

You can submit files for analysis using API with an API key. You can generate an API key using the GUI or CLI. The API key has all access privileges of the admin user.

The token is only displayed once. If you lose the token, you must generate a new one.

Upload files using API

You can use API to upload files for *Express Malware Analysis*. The maximum upload file size is 200MB.

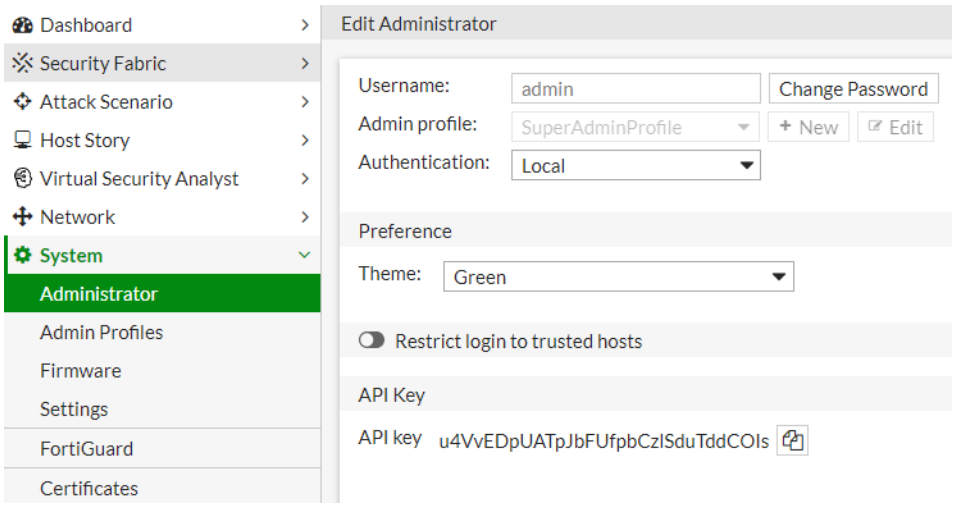
To use API to upload files, generate a token. The token is only displayed once. If you lose the token, generate a new one.

To generate a token using CLI:

```
execute api-key <user-name>
```

To generate a token using GUI:

1. Go to *System* > *Administrator* and edit an administrator.
2. In the *API Key* section, click *Generate*.



Use an API key

When making API calls, the API key is required in the request. You can include the API key in the API request header or URL parameter.

To pass the API token by request header, explicitly add the following field to the request header.

```
Authorization: Bearer <YOUR-API-TOKEN>
```

To pass the API token by URL parameter, explicitly include the following field in the request URL parameter.

```
access_token=<YOUR-API-TOKEN>
```

Submit files

/api/v1/files

You can submit files for analysis through the `/api/v1/files` endpoint with an administrator API key.

For a list of supported file types and formats, see Operating mode, protocols, and file type support on page 14.

Submit a file using one of the following methods.

Method	Description
JSON data	The JSON data must be encoded in base64 format. Encode the file directly into the HTTP body as JSON data using the `file_content` field.
Multi-part file	The multi-part file does not need to be encoded in base64 format. Include the file in the HTTP body as a multi-part file.

In both methods, you can use the API key as a URI parameter or the Authorization field in the header. Passwords for zip files are optional. You can view the verdict of submitted files in *Virtual Security Analyst > Express Malware Analysis*.

Example 1 of submitting a file or zip file via JSON data using the Python Requests module:

```
self.session.post(url='/api/v1/files?access_token=***API-KEY HERE***',
     data={" file_name": " b64encode(FILENAME)",
       "file_content": b64encode(open(PATH_TO_FILE, "rb").read())},
       "password":" ***ZIP FILE PASSWORD HERE(OPTIONAL)***")
```

Example 2 of submitting a file or zip file via JSON data using the Python Requests module:

```
self.session.post(url='/api/v1/files',
     headers={'Authorization': 'Bearer ***API-KEY HERE***'}
     data={" file_name": " b64encode(FILENAME)",
       "file_content": b64encode(open(PATH_TO_FILE, "rb").read())},
        "password":" ***ZIP FILE PASSWORD HERE(OPTIONAL)***")
```

Example 1 of submitting a file or zip file as a multi-part file using the Python Requests module:

```
self.session.post(url='/api/v1/files? access_token=***API-KEY HERE***'',
     data={"password":"***ZIP FILE PASSWORD HERE(OPTIONAL)***"},
     files={"file":( os.path.basename(PATH_TO_FILE),open(PATH_TO_FILE,"rb"))})
```

Example 2 of submitting a file or zip file as a multi-part file using the Python Requests module:

```
self.session.post(url='/api/v1/files',
     headers={'Authorization': 'Bearer ***API-KEY HERE***'},
```

```
    data={"password":"***ZIP FILE PASSWORD HERE(OPTIONAL)***"},
    files={"file":( os.path.basename(PATH_TO_FILE),open(PATH_TO_FILE,"rb"))})
```

Upload file by JSON data

Encode the file name into the HTTP body as JSON data using the `file_name` field.

Encode the file contents into the HTTP body as JSON data using the `file_content` field. The maximum file size is 200MB.

You have the option to include the password in the HTTP body as JSON data using the `password` field where a password is needed to extract an archived file.

The following is an example of Python request module by JSON data.

```
requests.post(url='/api/v1/files',
   params={'access_token': 'u4VvEDpUATpJbFUfpbCzlSduTddCOIs'},
   data={ 'file_name': b64encode('samples.zip'),
   ' file_content': b64encode(open('samples.zip', 'rb').read()),
   ' password': 'xxxxxxxx'})
```

Upload file by multi-part file

The following is an example of Python request module by multi-part file.

```
requests.post(url='/api/v1/files',
   params={'access_token': 'u4VvEDpUATpJbFUfpbCzlSduTddCOIs'},
   files={'samples.zip':open('samples.zip', 'rb')})
```

Retrieve file verdict results

/api/v1/verdict

Supported search query parameters	Description
`sid`	Get file IDs from a submission ID obtained after uploading a file.
`fileid`	Get verdict result from file ID.
`md5`	Get the latest verdict result from MD5 checksum of the file.
`sha1`	Get the latest verdict result from SHA1 checksum of the file.
`Sha256`	Get the latest verdict result from SHA256 checksum of the file.

The query string can only have one search query parameter.

Examples

```
GET /api/v1/verdict?sid= ***submission_id***
```

```
{
  "results": {
```

```
    "fileids": [
      7,8,9,10,11,12,13,14,15
    ],
    "total_fileids": 9
  }
}
```

Field	Description
fileids	File IDs in one file submission. If the file is an archived or compressed file, only files supported by FortiNDR after extraction are accepted and only file IDs of supported files appear.
total_fileids	Total number of file IDs.

```
GET /api/v1/verdict?fileid= ***file_id***
```

```
{
  "results": {
    "file_id": 5742600,
    "virus_name": "W32/Miner.VI!tr",
    "md5": "bbd72472f8d729f4c262d6fe2d9f2c8c",
    "sha512":
"cce8e67772f19bcfe5861e4c1b8eec87016bb7cf298735db633490243bc0391a017c7d6b805f225775405598614
be48c5479cb7f1c54d957e6129effbf9cca37",
    "file_size": 1141544,
    "source": "http://172.16.77.46/api/sample_download/1106042791/",
    "severity": "High",
    "category": "Trojan",
    "family":"Emotet",
    "feature_composition": [
      {
        "feature_type": "Trojan",
        "appearance_in_sample": 986
      },
      {
        "feature_type": "Application",
        "appearance_in_sample": 95
      }
    ],
    "create_date": "2020-07-31",
    "confidence": "High",
    "file_type": "PE",
    "victim_ip": "172.19.235.225",
    "attacker_ip": "172.16.77.46",
    "victim_port": 35400,
    "attacker_port": 80,
    "engine_version": 1.013,
    "kdb_version": 1.037,
    "tmfc": 0,
    "pbit": 3
  }
}
```

Field	Description
file_id	ID of the file.
virus_name	FortiNDR virus name.
source	For file uploaded by API or GUI, source is *manual upload*, otherwise it is an URL.
severity	*No Risk*, *Low*, *Medium*, *High*, or *Critical*.
category	For clean file: *Clean*. For malicious file, one of the following: *Generic Attack*, *Downloader*, *Redirector*, *Dropper*, *Ransomware*, *Worm*, *PWS*, *Rootkit*, *Banking Trojan*, *Infostealer*, *Exploit*, *Virus*, *Application*, *Multi*, *CoinMiner*, *DoS*, *BackDoor*, *WebShell*, *SEP*, *Proxy*, *Trojan*, *Phishing*, *Fileless*, *Wiper*, or *Industroyer*.
family	FortiNDR virus family name.
Feature_composition	JSON objects containing feature composition data for malicious file. feature_type is the category which the detected feature belongs to. appearance_in_sample is the number of appearances that the feature FortiNDR has detected.
confidence	For clean file: *N/A*. For other file: *Low*, *Medium*, or *High*.
file_type	*PE*, *PDF*, *MSOFFICE*, *HTML*, *ELF*, *VBS*, *VBA*, *JS*.
tmfc	Reserved.
pbit	Debug only.
parent_fname	The archive file name if the current file was extracted from an archive/zip file.

Example of problems retrieving results

```
{
  "http_code": 400,
  "message": "INVALID_PARAM"
}
```

Field	Description
http_code	See HTTP status table on page 169.
message	Messages include: DATA_NOT_EXIST when result data cannot be found given the search query parameter. DATA_IN_PROCESS when result data is still under process, such as after one submission, the accepted files have not been assigned file IDs. This might happen when uploading a big archive or compressed file. INVALID_PARAM_NUMBER when zero or more than one search query parameters exist. INVALID_PARAM when search query value is not valid.

Submitted file errors explanation:

When using `/ap1/v1/verdict?sid=xxx` to retrieve the file verdict in the following two cases:

- Oversized file
- Oversized archive contents

You will get reply: {`"http_code": 400, "message":"OVERSIZED_FILE"}`

In the other following cases:

- Unextractable archive
- File is still in queue
- File is still scanned

You will get successful reply with only supported file ids in the fileids list:

```
{

"results": {

    "fileids": [xx],

    "total_fileids": x

}

}
```

Once you get the `fileid` from submit id, using `/ap1/v1/verdict?fileid=xxx`

In the following two cases:

- File is still in queue
- File is still to be scanned

You will get reply: `{"http_code": 200, "message":"DATA_IN_PROCESS"}`

Get file stix2 report

/api/v1/report

Supported search query parameters	Description
`fileid`	Get report from file ID.
`md5`	Get report of the latest file with the MD5 checksum of the file.
`sha1`	Get report of the latest file with the SHA1 checksum of the file.
`sha256`	Get report of the latest file with the SHA256 checksum of the file.

The query string can only have one search query parameter.

Examples

```
GET /api/v1/report?fileid= ***file_id***
```

```
{
  "results": {
    *** STIX2 report content ***
  }
}
```

HTTP status table

HTTP code	Description
200	OK: API request successful.
400	Bad Request.
403	Forbidden: Request is missing authentication token, invalid authentication token, or administrator is missing access profile permissions.
404	Resource Not Found: Unable to find the specified resource.
405	Method Not Allowed: Specified HTTP method is not allowed for this resource.
413	Request Entity Too Large.
424	Failed Dependency.
500	Internal Server Error.

Start Network Share scan

/api/v1/nfs/scan

Required query parameters	Description
sname	The Network Share profile name under which the scan task will be created.

Examples

```
GET /api/v1/nfs/scan?sname= ***network share profile name***
{
       "http_code": 200,
       "message": "OK"
}
```

Example of failed to start Network Share scan

```
{
       "http_code": 400,
       "message": "Scanning in Progress"
}
```

Appendix B - Sample script to submit files

This is a sample script in python to submit files and retrieve results from FortiNDR.

```
#!/usr/bin/python3

# Version 1.0
# par Fortinet
# Jan 2021

import os
import requests
import getopt
import argparse
import simplejson as json
from base64 import b64encode, b64decode
import urllib3
import sys
import gzip
import subprocess
import urllib.request
import validators
from fake_useragent import UserAgent
import locale
from bs4 import BeautifulSoup
import requests


host = "IP"
AI_api_key = "API_KEY"

# Please be careful when regenerate api token. Once new token has been generated, old one will be
invalid.


class FAIApiClient_file():

       def __init__(self, url):
              self.url = 'https://' + url + '/api/v1/files?access_token=' + AI_api_key
              self.body = {"file_name": "",
                           "file_content": "",
                           "password": ""}

       def _handle_post(self, data):
              """
              POST JSON request..

              @type data: dict
              @param data: JSON request data.
              @rtype: HttpResponse
              @return: JSON response data.
              """
              response = requests.post(self.url, data=json.dumps(data), verify=False)

              return response
```

```
def _load_file_for_upload(self, path_to_file, test_input, filename=''):
        """
        Load file contents into input mapping.

        @type path_to_file: basestring
        @param path_to_file: files absolute path.
        @type test_input: dict
        @param test_input: JSON request data.
        @type filename: basestring
        @param filename: filename override optional param.
        @rtype: dict
        @return: updated JSON request dict.
        """
        with open(path_to_file, 'rb') as f:
                data = f.read()
        filename = os.path.basename(path_to_file) if not filename else filename
        test_input['file_name'] = b64encode(filename.encode('utf-8'))
        test_input['file_content'] = b64encode(data)
        test_input['password'] = "1"
        return test_input

def send_file(self, OVERRIDE_FILE = '../Resources/samples.zip'):
        # NOTE: 'OVERRIDE_FILE' should be the absolute path to the file.
        #       When submitting a file via API the noted file ('OVERRIDE_FILE')
        #       will be used as an OVERRIDE.
        test_input = self.body
        test_input = self._load_file_for_upload(OVERRIDE_FILE, test_input)
        response = self._handle_post(test_input)
        return response

def _load_memory_for_upload(self, text_data, test_input, filename=''):
        """
        Load file contents into input mapping.

        @type path_to_file: basestring
        @param path_to_file: files absolute path.
        @type test_input: dict
        @param test_input: JSON request data.
        @type filename: basestring
        @param filename: filename override optional param.
        @rtype: dict
        @return: updated JSON request dict.
        """

        tmp_str = ""

        data = b64encode(text_data)

        test_input['file_name'] = b64encode(filename.encode('utf-8'))
        test_input['file_content'] = data
        test_input['password'] = "1"
        return test_input

def send_url(self, url_page,filename):
        # NOTE: 'OVERRIDE_FILE' should be the absolute path to the file.
        #       When submitting a file via API the noted file ('OVERRIDE_FILE')
        #       will be used as an OVERRIDE.
        test_input = self.body
        test_input = self._load_memory_for_upload(url_page, test_input,filename)
        response = self._handle_post(test_input)
```

```
                return response

def crawl(url,depth):

        count = 3  # amount of urls in each level
        url_list_depth = [[] for i in range(0, depth + 1)]
        url_list_depth[0].append(url)
        for depth_i in range(0, depth):
                for links in url_list_depth[depth_i]:
                        valid = True
                        try:
                                response = requests.get(links,verify=False)

                        except
(requests.exceptions.InvalidSchema,requests.exceptions.MissingSchema,requests.exceptions.SSLError) as
e:
                                valid = False

                        if (valid):
                                soup = BeautifulSoup(response.text, 'html.parser')
                                tags = soup.find_all('a')
                                for link in tags:
                                        url_new = link.get('href')
                                        flag = False
                                        for item in url_list_depth:
                                                for l in item:
                                                        if url_new == l:
                                                                flag = True

                                        if url_new is not None and "http" in url_new and flag is False:
                                                url_list_depth[depth_i + 1].append(url_new)
                                                #print(links, "->", url_new)

                        else:
                                parse_url (links)


        return (url_list_depth)

def load_file_for_upload(path_to_file):

        with open(path_to_file, 'rb') as f:
                data = f.read()

        return gzip.compress(data)

def check_file_id(host, file_id):
        data = ""
        results_output  = ""

        tmp_url = "https://" + str(host) + "/api/v1/verdict?access_token=" + str(AI_api_key) + "&fileid=" +
str(file_id)
        command= "curl -k -X GET \""+ tmp_url  + "\"  -H \"Content-Type: application/json\" "

        try:
                results_output = subprocess.check_output(command, shell=True)
                data =  json.loads(results_output)

        except subprocess.CalledProcessError as e:
```

```
                print(e)
                sys.exit(0)

        return (data)

def check_submission_results (submit_id,filename):
        data = ""
        results_output  = ""

        tmp_url = "https://" + str(host) + "/api/v1/verdict?access_token=" + str(AI_api_key) + "&sid=" + str
(submit_id)
        command= "curl -k -X GET \""+ tmp_url  + "\"  -H \"Content-Type: application/json\" "

        try:
                results_output = subprocess.check_output(command, shell=True)
                data =  json.loads(results_output)

                if (len(data) > 0):
                        for key in data:
                                if (key == "results"):
                                   tmp_data = data[key]
                                   for key, value in tmp_data.items():
                                        if (key == "fileids"):
                                                if (len(value) > 0):
                                                   for i in range(0,len(value)):
                                                        file_id = value[i]
                                                        new_data  = "DATA_IN_PROCESS"
                                                        stop = True
                                                        i = 1
                                                        while stop:
                                                           new_data = check_file_id(host, file_id)
                                                           tmp_check = str(new_data)
                                                           i = i + 1

                                                           if (not ("DATA_IN_PROCESS" in tmp_check)):
                                                              stop = False
                                                           elif (i == 50 ):
                                                              stop = False
                                                              break


                                                        results_metadata = "filename:" + str(filename)
                                                        if (len(new_data) > 0):
                                                           for key in data:
                                                              if (key == "results"):
                                                                 try:
                                                                    tmp_data = new_data[key]
                                                                    for key, value in tmp_data.items():
                                                                       results_metadata = results_metadata + ","
+ str(key) + ":" + str(value)
                                                                 except KeyError as e:
                                                                    next

                                                        print (results_metadata)

                                                        else:
                                                                print ("filename:" + str(filename)  + ",NO RESULTS")
        except subprocess.CalledProcessError as e:

                sys.exit(0)
```

```
def parse_url (tmp_url):

        client = FAIApiClient_file(host)

        if (validators.url(tmp_url)):
                ua = UserAgent()
                the_page = ""

                try:
                        request = urllib.request.Request(tmp_url, data=None, headers={'User-Agent':  str(ua)})
                        response = urllib.request.urlopen(request)

                        with urllib.request.urlopen(request) as response:
                                try:
                                        the_page = response.read()

                                except Exception  as e:
                                        pass

                except (urllib.error.URLError,urllib.error.ContentTooShortError,urllib.error.HTTPError) as e:
                                print ("CANNOT GET  URL:"  + str(tmp_url))
                                sys.exit(0)

                if (len(the_page) > 1):
                        filename = tmp_url.replace(",","_")
                        tmp_data = json.loads(client.send_url(the_page,"url").text)
                        if ("submit_id" in tmp_data):
                                submit_id = tmp_data['submit_id']
                                if (submit_id > 0) :
                                        filename = tmp_url.replace(",","_")
                                        check_submission_results (submit_id,filename)
                                else:
                                        print ("url:" + str(tmp_url) , "NO RESULTS")
                else:
                        print ("url:" + str(tmp_url) , "NO RESULTS")

        else:
                the_page = str.encode(tmp_url)
                if (len(the_page) > 1):
                        filename = tmp_url.replace(",","_")
                        tmp_data = json.loads(client.send_url(the_page,"url").text)
                        if ("submit_id" in tmp_data):
                                submit_id = tmp_data['submit_id']
                                if (submit_id > 0) :
                                        filename = tmp_url.replace(",","_")
                                        check_submission_results (submit_id,"url")
                                else:
                                        print ("url:" + str(tmp_url) , "NO RESULTS")
                else:
                        print ("url:" + str(tmp_url) , "NO RESULTS")


def getpreferredencoding(do_setlocale = True):
        return "utf-8"

def main(argv):
        locale.getpreferredencoding = getpreferredencoding

        urllib3.disable_warnings()
```

```
        parser = argparse.ArgumentParser(description='Test upload files to FortiAi and fortisandbox tool')

        parser.add_argument("-f","--file",   type=str, help="Filename to submit")
        parser.add_argument("-u","--url",   type=str, help="Filename to submit")
        parser.add_argument("-d","--depth",  type=int, help="Depth for url analysis, default 0 (just the url
page), if depth not defined, maxdepth 3")

        args = parser.parse_args()

        if ( not (args.file or args.url)):
                parser.print_help()
                sys.exit(0)

        if (args.depth):
                depth = args.depth
        else:
                depth = 0

        if (depth > 3):
                depth = 3

        if (args.file):
                client = FAIApiClient_file(host)
                tmp_data = json.loads(client.send_file(args.file).text)
                if ("submit_id" in tmp_data):
                        submit_id = tmp_data['submit_id']
                        if (submit_id > 0) :
                                check_submission_results (submit_id,args.file)
                        else:
                                print ("filename:" + str(args.file) , "NO RESULTS")

        if (args.url):

                if (depth == 0):

                        parse_url (args.url)
                else:

                        list_of_url_to_parse = ""
                        list_url = crawl (args.url,depth)

                        for i in list_url:
                                tmp_list = i
                                for j in tmp_list:
                                        parse_url(j)


# Example command: python FAI_Client.py <fai_ip> <api key> <sample file path>
if __name__ == '__main__':
    main(sys.argv)
```

Appendix C - FortiNDR ports

FortiNDR requires the following ports.

Item	Protocol and port number	Direction
API submission, such as FortiSandbox	TCP 443	Inbound
CLI	TCP 22	Inbound SSH
FortiGate quarantine	TCP 443	Outbound to FortiGate
FortiGuard update	TCP 443	Outbound to: • fai.fortinet.net • fds1.fortinet.com • update.fortiguard.net
IOC lookup	TCP 443	Outbound to productapi.fortinet.com
IOT lookup	TCP 443	Outbound to globalguardservice.fortinet.net
GUI	TCP 443	Inbound web browser
ICAP	TCP 1344, 11344	Inbound
NetFlow listen ports	UDP 2055,6343,9995	Inbound
Network File Share	TCP 139, 445, 2049 (NFS)	Outbound to file server
OFTP server	TCP 514	Inbound
Security Fabric with FortiGate	TCP 443	Outbound to root FortiGate for Security Fabric communication
Security Fabric with FortiGate	TCP 8013	Outbound to root FortiGate in Security Fabric
Web Filter query	UDP 53	Outbound to service.fortiguard.net
Microsoft Active Directory	TCP 636,389	Inbound and outbound

Appendix D - FortiGuard updates

For deployments that have Internet connections, FortiNDR by default relies on the Internet to get updates via the FortiGuard Distribution Network. In the occasions where FortiNDR cannot reach the Internet, you have the following options:

Malware artificial neural network (ANN) updates: You can update the ANN manually. These updates (in several GB) can be obtained via support website (https://support.fortinet.com) with a registered support contract. The latest ANN version can be viewed at: https://www.fortiguard.com/services/fortindr

For v7.0.1 and later, the offline package files have more data compared to the v1.0 and v7.0 packages. The number of packages has increased as well.

The v7.0.1 packages have additional data and they will fail to load in previous firmware versions. However, the v1.0/v7.0 ANN packages can be loaded in v7.0.1 and later firmware versions. Please download the corresponding packages according to the firmware version on the support website.

For more information about loading offline packages , see the `exec restore kdb`, `exec restore avdb`, and `exec restore ipsdb` commands in the CLI Reference Guide. IPSDB offline packages includes 3 DB (network attacks, botnet and JA3 encrypted attacks).

Other detection techniques:

The following table summarises whether detection will work on/off line (no internet access). All of the detection techniques below can be updated via FortiGuard Distribution Network (Internet).

Detection Techniques	Supports offline manual update	Comments
Malware via ANN	Yes	Can be updated manually via GUI or with an offline package via CLI.
AV engine	Yes	Shipped by default. Can be updated with internet via GUI or with an offline package via CLI.
Botnet detection	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.
Network Attacks / Application control	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.
Encrypted attacks (via JA3)	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.
Weak cipher/vulnerable protocol detection	NA	Comes with firmware, no updates required.
Device inventory	No	Lookup IOT services to determine device role/type/OS

Detection Techniques	Supports offline manual update	Comments
FortiGuard IOC	No	Requires Internet to lookup URLs and IP for web campaigns associated.
ML Discovery	NA	Local ML algorithm updates via firmware.
Geo DB	No	Comes with firmware, does not update often, supports FortiGuard Update via internet.

Appendix E - Event severity level by category

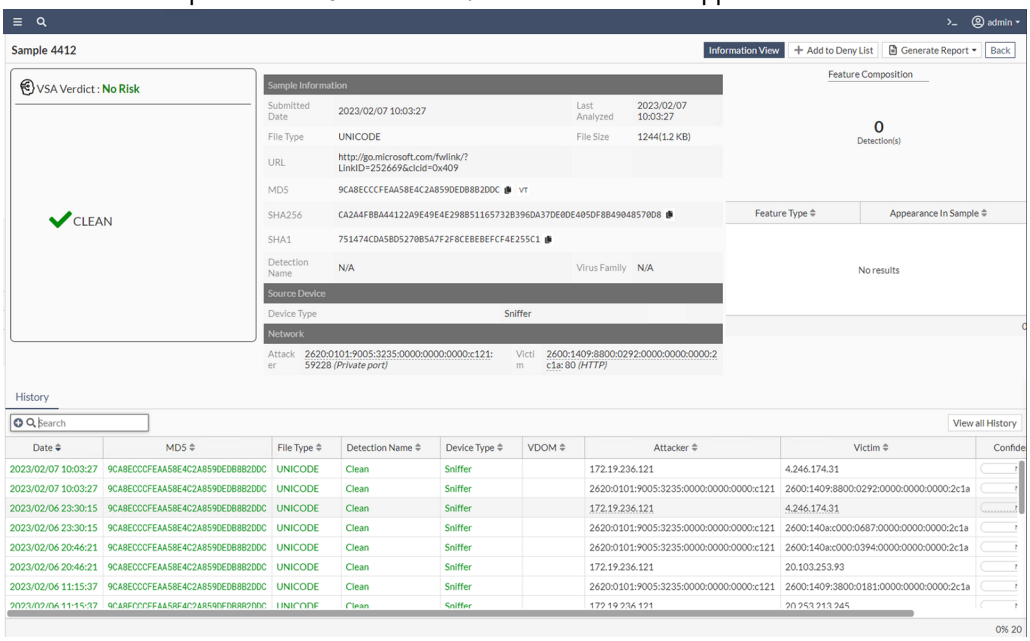
Event Category	NDR Detection Severity Level
Malware Detection	Low|Medium|High|Critical
Botnet Detection/Netflow Botnet Detection	Critical
Encryption Attack Detection	Critical
Network Attack Detection	Low|Medium|High|Critical
Indication of Compromise Detection	Critical
Weak Cipher and Vulnerable Protocol Detection	Low|Medium|High|Critical
Machine Learning Detection	Low

Appendix F - IPv6 support

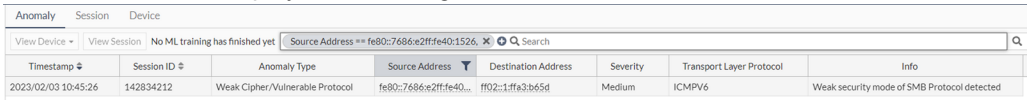
The following topic covers IPv6 support in FortiNDR.

IPV6 in detections:

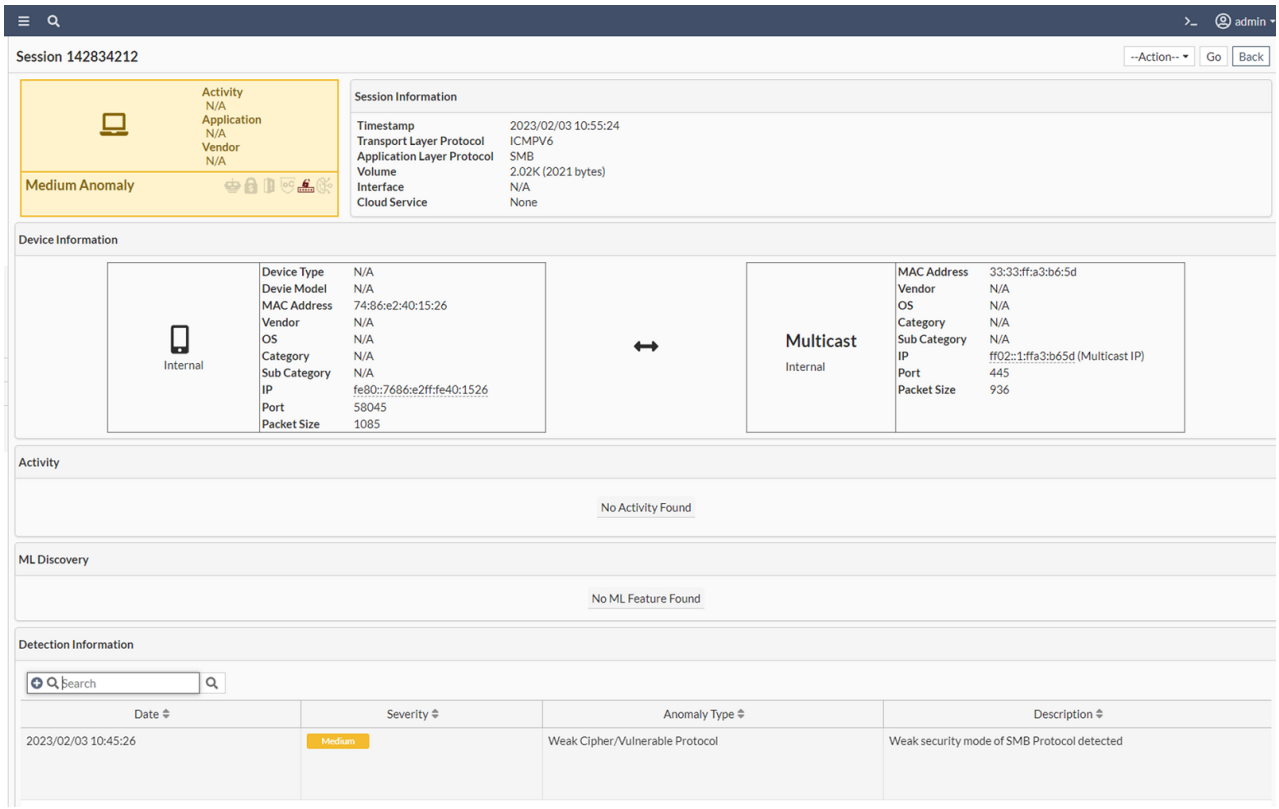
- Files from sniffer port with IPv6 source and/or destination are supported.



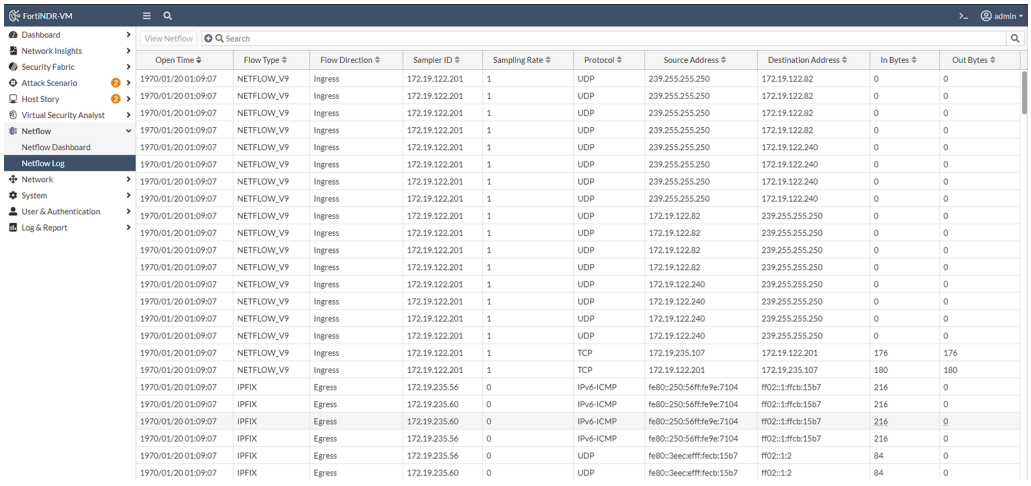
- IPv6 addresses are displayed in NDR logs.



- IPv6 is shown in the session detail page.



- ML Discovery works against IPv6 source and destination IPs.
- Ingest IPv6 Netflow including NetFlow, SFlow, and IPFIX. The IPv6 display shares existing source and destination address column.



- CLI only for interface and routing with IPv6 configurations WebGUI, and SSH support.

Appendix G - Supported Application Protocol List

The following application protocols are supported by FortiNDR:

- TLS
- HTTP
- HTTPS
- SMB
- SMTP
- SSH
- FTP
- POP3
- DNS
- IRC
- IMAP
- RTSP
- RPC
- SIP
- RDP
- SNMP
- MYSQL
- MSSQL
- POSTGRESQL

Appendix H - File types and protocols

FortiNDR file scanning supports the following file types:

NDR engine	Common protocols such as TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors
File-based analyses	32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, Hangul_Office, TAR, XZ, GZIP, BZIP, BZIP2, RAR, LZH, LZW,ARJ, CAB, _7Z, PHP, XML, POWERSHELL, BAT, HTA, UPX, ACTIVEMIME, MIME, HLP, BASE64, BINHEX, UUE, FSG, ASPACK, GENSCRIPT, SHELLSCRIPT, PERLSCRIPT, MSC, PETITE, ACCESS, SIS, HOSTS, NSIS, SISX, INF, E32IMAGE, FATMACH, CPIO, AUTOIT, MSOFFICEX, OPENOFFICE, TNEF, SWF, UNICODE, PYARCH, EGG, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, LNK, KGB, Z, ACE, JAR, APK, MSI, MACH_O, DMG, DOTNET, XAR, CHM, ISO, CRX, INNO, THMX, FLAC, XXE, WORDML, WORDBASIC, OTF, WOFF, VSDX, EMF, DAA, GPG, PYTHON, CSS, AUTOITSCRIPT, RPM, EML, REGISTRY, PFILE, CEF, PRC, CLASS, JAD, COD, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN

www.fortinet.com