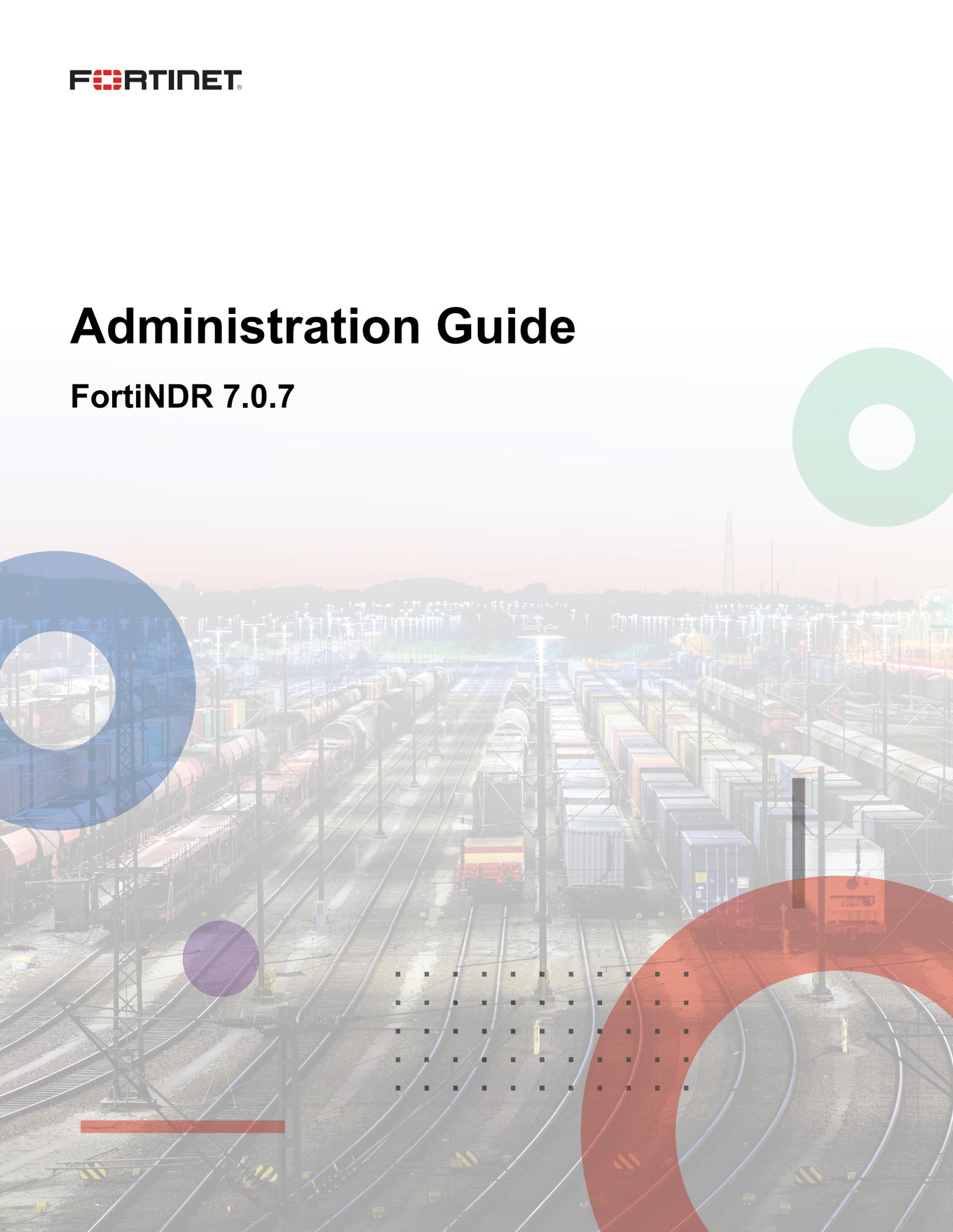


Administration Guide

FortiNDR 7.0.7



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>

NSE 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



April 22, 2025

FortiNDR 7.0.7 Administration Guide

55-707-848300-20250422

TABLE OF CONTENTS

Change Log	7
Introduction	8
Getting started	8
Demo mode	9
Loading the ANN database to FortiNDR for malware detection	10
Updating the ANN database from FDS for malware detection	14
Operating mode, protocols, and file type support	15
File scan flow	17
Stage 1	17
Stage 2	18
Architecture considerations	18
Planning deployment—estimating data storage for file analysis throughput	19
Initial setup	20
Internet Access	20
Ports	20
Dashboard	22
NDR Overview	22
Malware Overview	22
System Status	23
Security Fabric	25
FortiGate inline blocking (FOS 7.0.1 and higher)	25
Tips for using FortiNDR inline blocking	26
FortiNDR inline inspection with other AV inspection methods	27
Accepted file types	27
FortiGate integration (integrated mode with FOS 5.6 and higher)	28
Device input	30
FortiGate tab	30
Other Device tab	30
Network Share	30
Creating a Network Share	31
Testing connectivity	34
Scanning a network location	34
Scheduling a scan	34
Viewing scan results	35
Scanning Zip files	36
Network Share Quarantine	36
Quarantined files	36
Creating a quarantine profile	37
Combining network share and quarantine profiles	38
Fabric Connectors	40
ICAP Connectors	40
Security Fabric Connector	48
Enforcement	49

Enforcement Settings	49
Creating an Enforcement Profile	51
Automation Framework	53
FortiGate quarantine webhook setup example	55
FortiSwitch quarantine setup example	60
FortiNAC quarantine setup example	62
Generic Webhook setup example	63
Automation log	64
Automation Status and Post action	65
FortiSandbox integration (FortiSandbox 4.0.1 and higher)	65
Network Insights	67
Device Inventory	68
Botnet	68
FortiGuard IOC	69
Network Attacks	69
Weak/Vulnerable Communication	70
Weak/Vulnerable Communication types	70
Encrypted Attack	75
ML Discovery	76
Add feedback a session	78
View Session	79
View Source Device and View Destination Device	81
Attack Scenario	83
Scenario types	83
Attack scenario navigation and timeline	85
Understanding kill chain and scenario engine	86
Host Story	87
Virtual Security Analyst	88
Express Malware Analysis	88
Configuring the table	90
Upload files using API	91
Outbreak Search	91
Search lead type of hash or detection name	92
Search lead type of outbreak name	93
Recursive searches	93
Reports	94
Static Filter	94
ML Configuration	95
Malware Big Picture	98
Network	99
Interface	99
DNS and Static Routes	99
System	100
Administrator and Admin Profiles	100

Firmware	100
Settings	101
FortiGuard	102
Certificates	105
High Availability (HA)	105
HA setup requirements	105
Configuring an HA group	106
Check HA status	109
HA Failover	110
HA configuration settings synchronization	112
HA Logs	113
Using Virtual IP	113
User & Device	116
Log & Report	117
Malware Log	117
Advanced search	120
NDR Log	121
Anomaly tab	121
Session Tab	122
Device Tab	123
Events	125
Daily Feature Learned	126
Log Settings	127
NDR logs samples	128
Alert Email Setting	131
Email Alert Recipients	132
Troubleshooting	133
FortiNDR health checks	133
Sniffer diagnosis	134
Rebuild RAID disk	135
Managing FortiNDR disk usage	138
Exporting detected malware files	139
Formatting the database	141
Export malware	141
Working with false positives and false negatives	142
Troubleshoot ICAP and OFTP connection issues	142
Troubleshoot Log Settings	143
Troubleshoot Network Share	145
Test the Network Share Connection	145
Diagnosing Network Share Errors	147
Debug version image	148
Check Crash Log	148
Troubleshooting the VM License	149
Troubleshooting Updater	149
FDS Authorization Failed	149
Clearing updater cache files	149

Diagnosing Other FDS Errors	150
Appendix A - API guide	151
Appendix B - Sample script to submit files	158
Appendix C - FortiNDR ports	164
Appendix D - FortiGuard Updates	165
Appendix E - Event severity level by category	167

Change Log

Date	Change Description
2025-04-22	Initial release.

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 hashes), 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).

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.



Only admins with SuperAdminProfile privileges can SSH to use the CLI. For information, see [Administrator and Admin Profiles on page 100](#)

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*.
-



Only Super Admin users can access the CLI using SSH. For more information, see [Administrator and Admin Profiles on page 100](#).

Demo mode

The purpose of demo mode is to showcase FortiNDR GUI functionality without actual attacks, anomalies malware, nor with file scanning abilities. Demo mode will generate malware and anomalies log entries (but not the actual malware and attacks) to populate the GUI with different attack scenarios and allow you to try demo searching, logging and MITRE/JSON/IOC malware reporting functionalities.

Demo mode requires less computer resources and can run on newer laptops such as those with 2–4 vCPU and 8GB memory. For production, a minimum of 16 vCPUs and 32GB of memory is required.

If required, please contact the Fortinet sales team for an evaluation license. A licensed FortiNDR instance allows you to load ANN and have full scanning capabilities. Scanning capabilities including manual upload requires you to satisfy minimum production CPU and memory requirements (which is 16vCPU and 32GB of memory).



Demo Mode is only available on FortiNDR VM.

To turn on demo mode with the CLI:

```
execute demo on
```



Do not use functions which require scanning, such as Sniffer or Manual Upload, while in Demo Mode.

To exit demo mode with the CLI:

```
execute demo off
```

To erase the demo log with the CLI:

```
execute db restore
```

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 165](#) 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 `sdcl` using the `mkfs.ext4 /dev/sdcl` command.

```
/# mkfs.ext4 /dev/sdcl
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/sdcl           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/sdcl /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/sdal
Mounting /dev/sdbl
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e51D0v
Copying file failed!
Mounting /dev/sdcl
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/sdal
Mounting /dev/sdbl
Try copying file from /kdb_disk/moat_kdb_all.tar.gz to /var/spool/tmp/up_uWobUb
Copying file failed!
Mounting /dev/sdcl
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*.

FortiNDR-3500F

FortiGuard Distribution Network

License Information

Entitlement	Status	
FortiCare Support	Registered	
Firmware & General Updates	Licenses - expires on 2023/03/10	<input type="button" value="Firmware Upgrade"/>
NDR Service	Valid - expires on 2023/01/09	
Text AI Feature DB	Error Occurred During Updating	
Text AI Group DB	Version 1.087	Up to Date
Binary AI Feature DB	Version 1.087	Up to Date
Binary AI Group DB	Version 1.096	Up to Date
Scenario AI DB	Version 1.096	Up to Date
Text AI Learning Feature DB	Version 1.087	Up to Date
Binary AI Learning Feature DB	Version 1.096	Up to Date
Binary Behavior DB	Version 1.096	Up to Date
AVEng Active DB	Version 90.01403	Update Available
AVEng Extended DB	Version 90.01332	Up to Date
AVEng Extreme DB	Version 90.01363	Up to Date
AVEng AI DB	Version 2.02671	Update Available
Application Control DB	Version 20.00295	Up to Date
Industrial Security DB	Version 20.00295	Up to Date
Network Intrusion Protection DB	Version 20.00299	Up to Date
Traffic Analysis DB	Version 20.00001	Up to Date

OK Cancel

- 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.

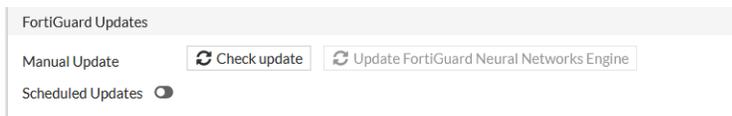
Updating the ANN database from FDS for malware detection

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*.

Status	
✓ Registered	
✓ Licenses - expires on 2023/07/30	Firmware Upgrade
✓ Valid - expires on 2023/01/09	
✓ Valid - expires on 2022/07/30	FortiNDR VM License

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](#).

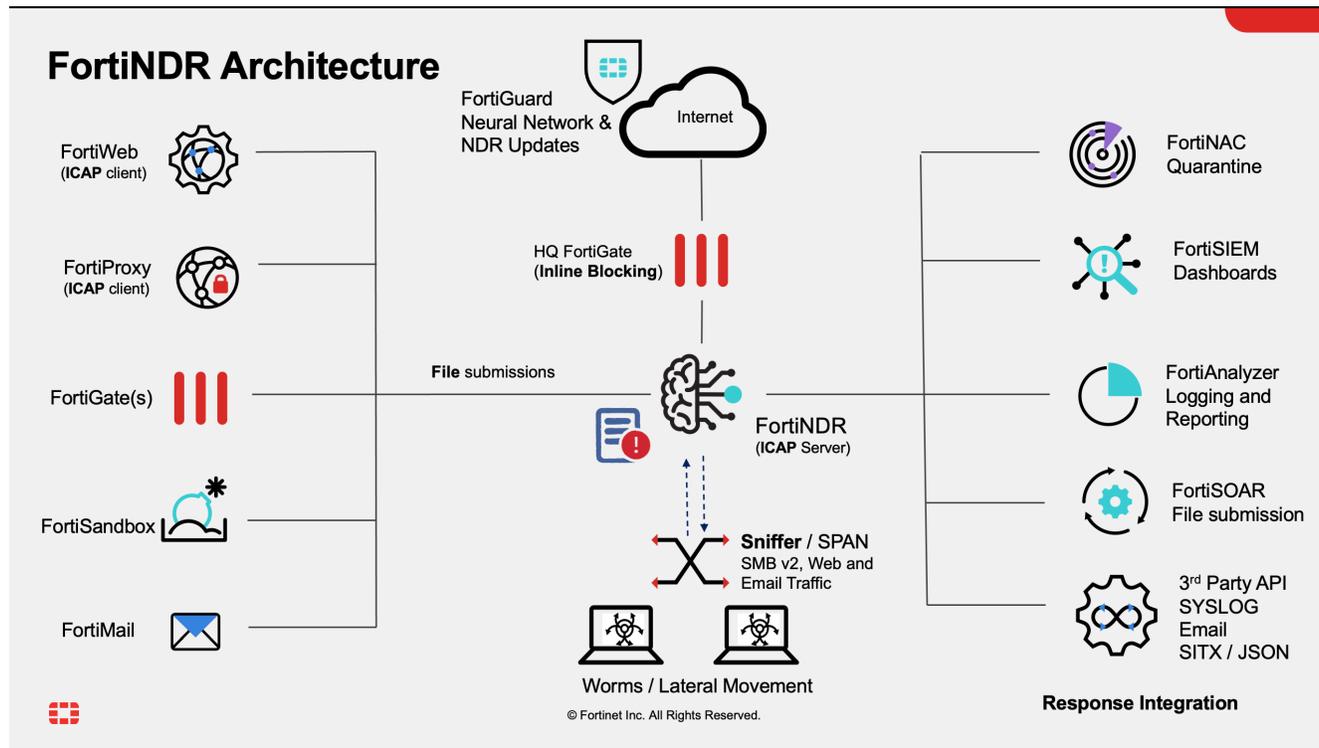
Operating Mode	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
Sniffer	N/A	N/A	HTTP, SMBv2, IMAP, POP3, SMTP, FTP	TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, 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,	N/A	FortiGate v7.0.1 supports INLINE blocking with AV profile
	FortiMail	HTTP2	SMTP		Configure under <i>AV profile</i> under FortiMail.
	FortiSandbox	HTTP2	MAPI, FTP, CIFS		
ICAP	FortiWeb	ICAP	HTTP, HTTPS	N/A	Supports using FortiNDR as ICAP server and multiple
	FortiProxy	ICAP	HTTP, HTTPS		FortiGates, FortiWeb and FortiProxy or third-party ICAP client such as Squid.

Operating Mode	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
Other / API	FortiSOAR	HTTPS API upload	HTTPS	N/A	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	N/A	N/A	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

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 53](#).



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

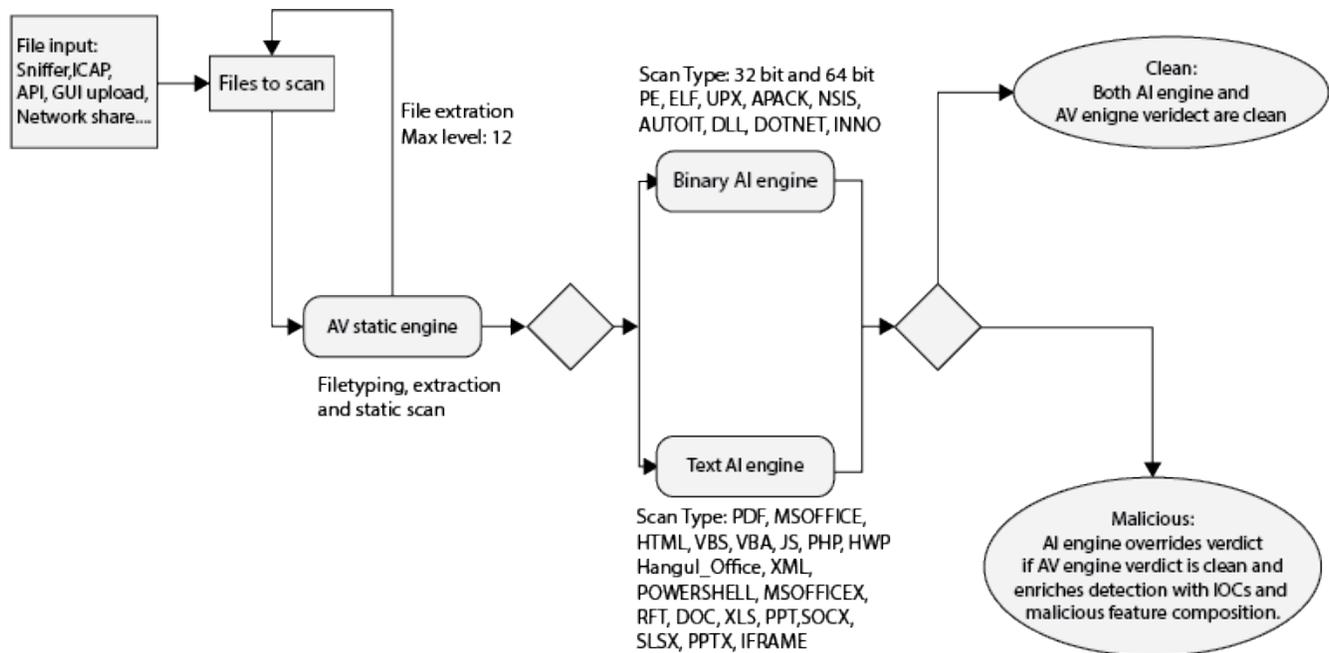


File types supported by ANN will be scanned by the ANN and AV engines. Other supported file types will be scanned by AV engine only.

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—estimating data storage for file analysis throughput

- FAI-3500F (gen 1 & 2) uses 2 X 3.8TB SSD in RAID1 and comes with the option to purchase additional SSD HDDs.
- 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	Default data storage (GB)	Max. Process rate* (files/hour)	Storage retention (approx. days / months / year)
FNDR-3500F	3517	100,000	270 days / 9 months / .75 years
FNDR-VM	1024	40,000 to 80,000	265 days / 8.5 months / .75 years
FNDR-VM	2048	40,000 to 80,000	625 days / 20.5 months / 1.7 years
FNDR-VM	4096	40,000 to 80,000	1345 days / 44.5 months / 3.7 years
FNDR-VM	8192	40,000 to 80,000	2700 days / 90 months / 7.4 years



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.

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 165](#).

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 SFP+ 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>.



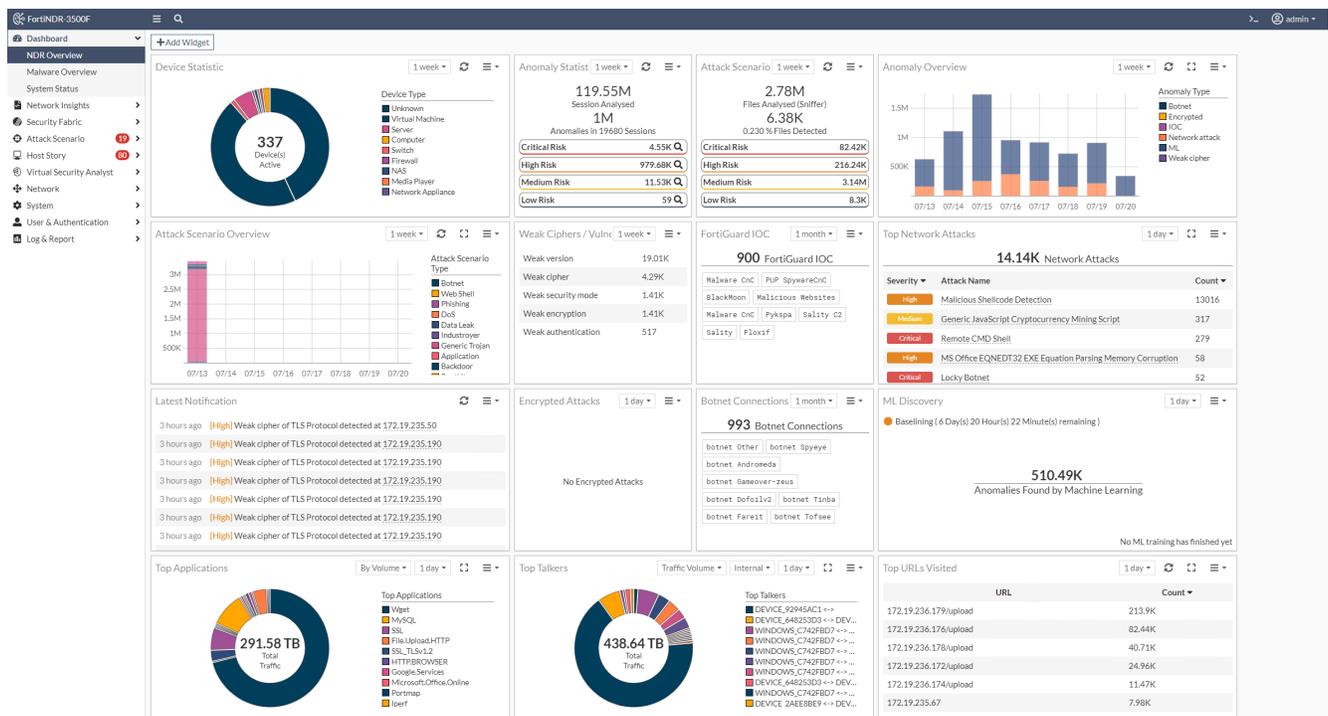
*For customers who are required to use SFP+ ports (available in gen3 hardware only) for management and capture (sniffer), pls contact local CSE for details.

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*.

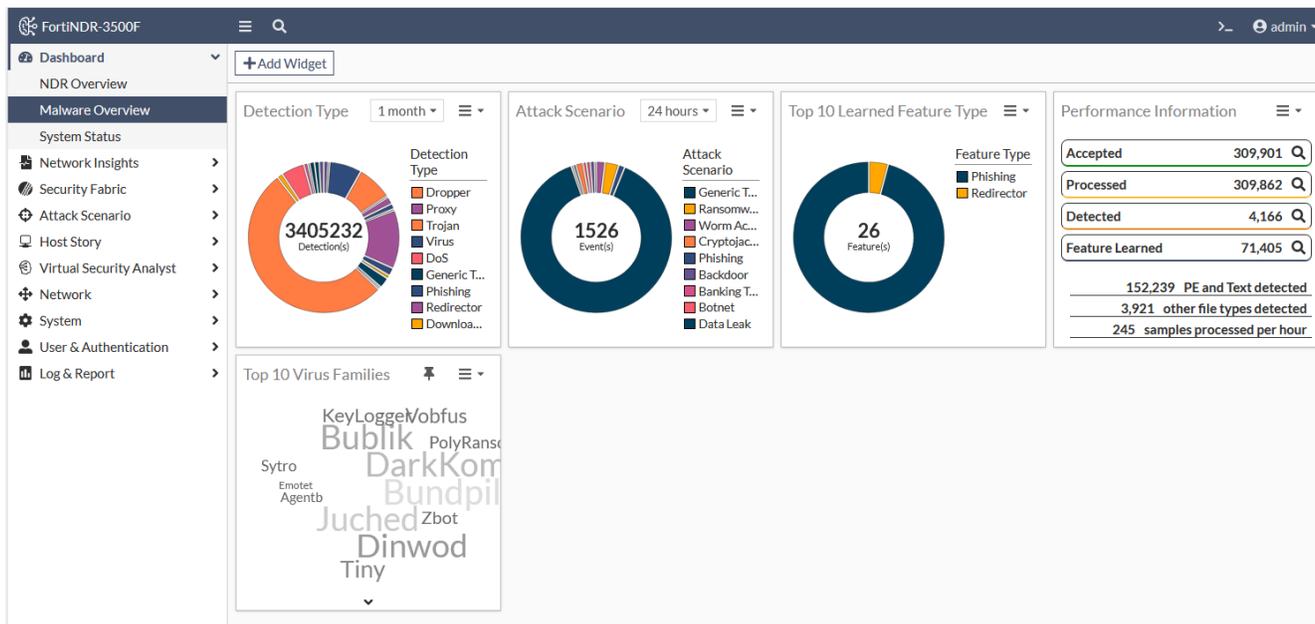
NDR Overview

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.



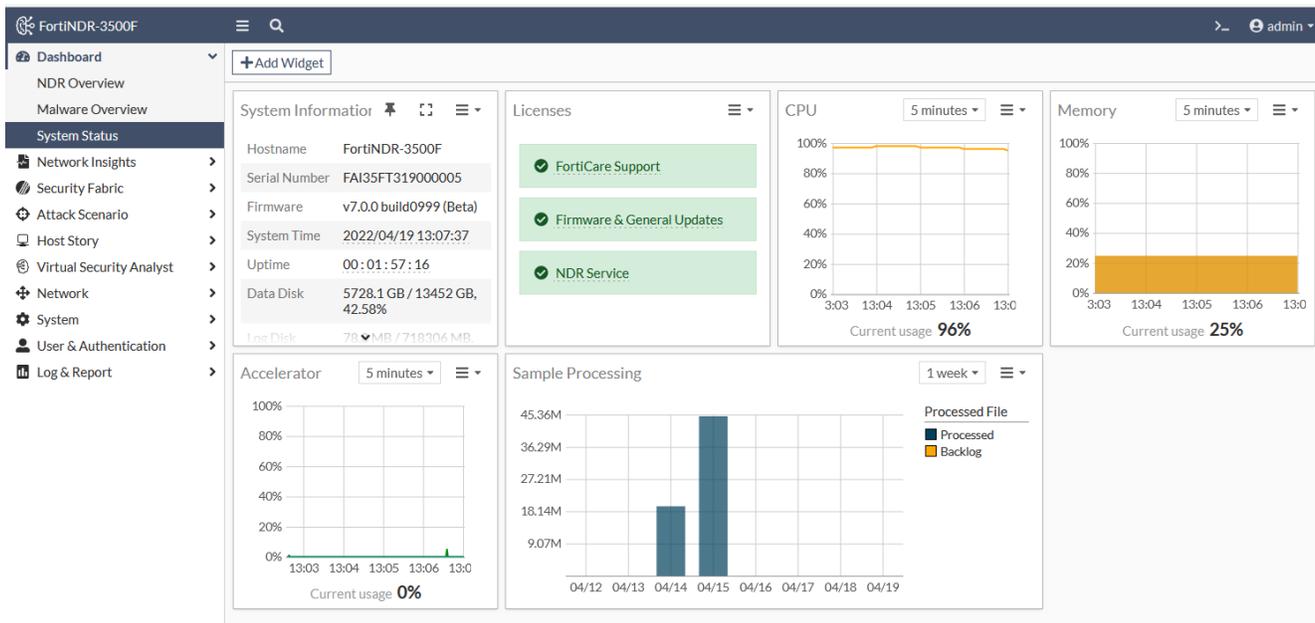
Malware Overview

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.



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*.

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.

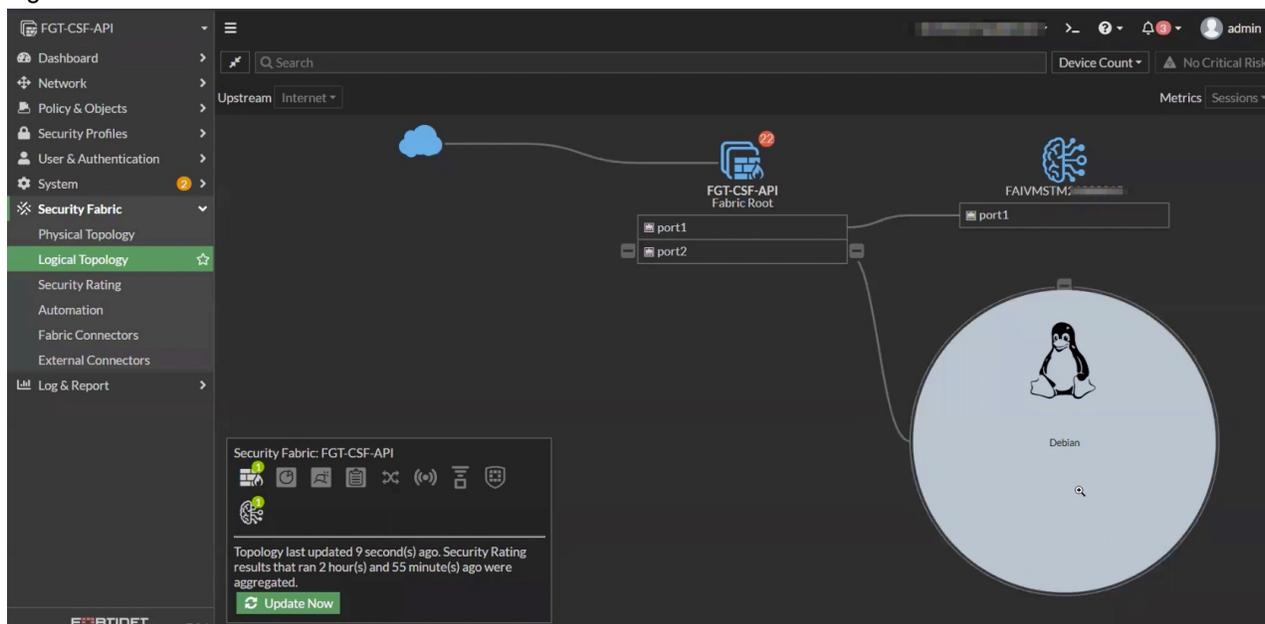
This provides more security than integrated mode because you can download the file first while the file is sent to FortiNDR (and FortiSandbox) for inspection.

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 40](#).

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.
```

```

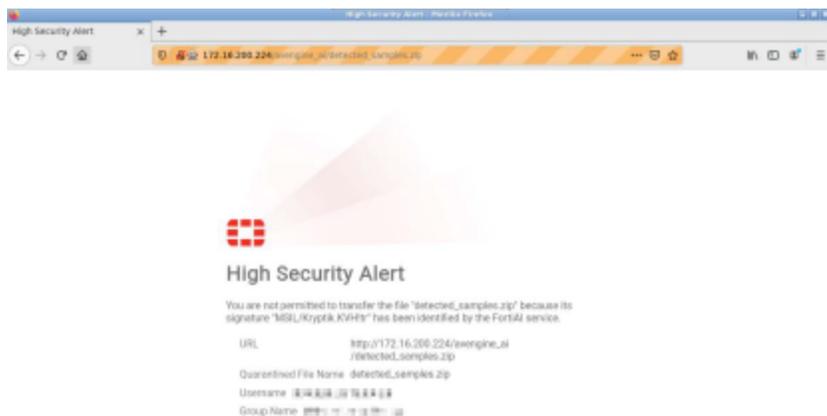
Set fortindr block << or monitor
End
Next
End

```

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

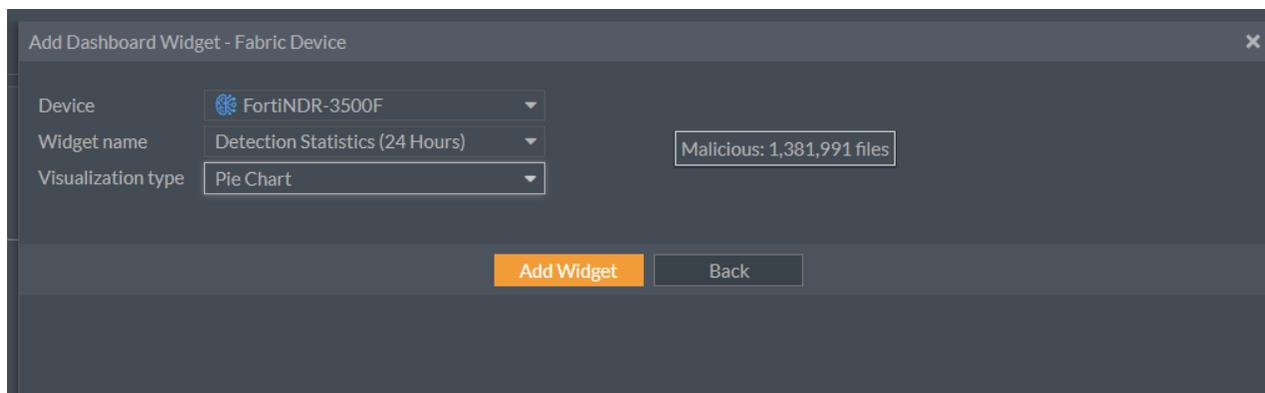
Tips for using FortiNDR inline blocking

- Similar to the FortiGate AV profile, a browser replacement message is 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 FortiNDR inline 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-	WinPE (EXE)
ELF	XML)	XZ
GZIP	PDF	ZIP
	RAR	

FortiGate integration (integrated mode with FOS 5.6 and higher)

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

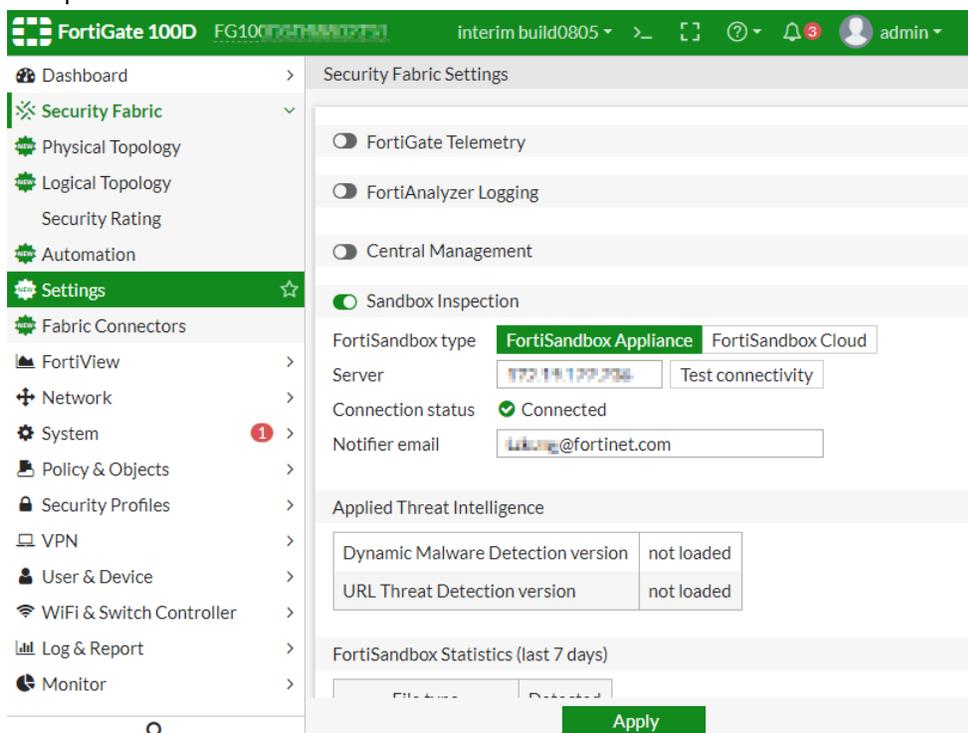
FortiGate cannot receive files from both FortiSandbox and FortiNDR simultaneously. If your FortiGate has FortiSandbox configured, consider using another mode.

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.

The screenshot shows the 'Edit AntiVirus Profile' configuration page. The profile name is 'default' and the comments are 'Scan files and block viruses.' The scan mode is set to 'Full' and the detect viruses option is set to 'Block'. Under 'Inspected Protocols', several protocols are enabled with toggle switches: HTTP, SMTP, POP3, IMAP, MAPI, FTP, and SMB. In the 'APT Protection Options' section, 'Content Disarm and Reconstruction' is enabled, and the 'Original File Destination' is set to 'FortiSandbox'. The 'Send Files to FortiSandbox Appliance for Inspection' option is set to 'All Supported Files'. There are also options for 'Do not submit files matching types' and 'Do not submit files matching file name patterns'. The 'Virus Outbreak Prevention' section includes options for 'Use FortiGuard Outbreak Prevention Database' and 'Use External Malware Block List'. An 'Apply' button is at the bottom.

3. Apply AV profile in the firewall policy.

The screenshot shows the 'IPv4 Policy' configuration page. A table of policies is displayed with the following data:

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Protocol Options	Security Profiles	Log	Bytes
1	fortiAI	lan	wan1	all	all	always	ALL	ACCEPT	Enabled	default	default	UTM	22.43TB

4. Authorize the FortiGate on FortiNDR for sending files.

The screenshot shows the 'Security Fabric' configuration page. A table of authorized FortiGates is displayed with the following data:

ID	Host Name	VDOM	IP Address	Malware Version	URL Version	Authorized
8	FG100D5C130002751		172.19.0.201	0	0	Enabled
10	FG100D5C130002751:root	root	172.19.0.201	0	0	Enabled
11	FGT80F8477020995		172.19.0.208	0	0	Enabled

5. Check the FortiNDR processed traffic. See [FortiGate integration \(integrated mode with FOS 5.6 and higher\)](#) on page 28.

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 25](#).

Device Name	VDOM	IP Address	Connection Type	Authorized	Status
FGVM_251	global	172.19.235.251	OFTP	Enabled	Connected
FGVM_251:root	root	172.19.235.251	OFTP	Enabled	Connected

Other Device tab

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

Device Name	VDOM	IP Address	Connection Type	Product Type	Authorized	Status
FSAVM01000016205	global	172.19.235.214	Internal API for FSA	FortiSandbox	Via Security Fabric	Connected

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.

Name	Scan Scheduled	Type	Share Path	Quarantine	Enabled	Status
172.19.235.244	Yes	SMBv3.0	//172.19.235.244/c	No	Enabled	Connected
shared2	Yes	SMBv3.0	//172.19.235.204/shared2	No	Enabled	Connected
Shared3	No	SMBv3.0	//172.19.235.204/shared3	No	Enabled	Connected

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	<i>Enable or Disable. Enable is the default.</i>
Mount Type	Select a Network Share protocol from the list. The following protocols are supported: <ul style="list-style-type: none"> • 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.
	 <p>FortiNDR does not process password protected files.</p>
Enable Quarantine Critical Risk Files	Moves detected files with critical risk to a designated quarantine location. This includes: <ul style="list-style-type: none"> • Fileless • Industroyer • Ransomware • Wiper • Worm

Enable Quarantine - High Risk Files	Moves detected files with high risk to a designated quarantine location. This includes: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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 <i>Network Share Quarantine</i> profile. See, Network Share Quarantine on page 36 . The <i>Moving</i> operation is only allowed for the quarantine location when <i>Keep Original File at Source Location</i> disabled. The <i>Copying</i> operation is only allowed for the quarantine location when <i>Keep Original File at Source Location</i> enabled. For information about combing Network Share and Quarantine profiles, see Network Share Quarantine on page 36 > <i>Combining network share and quarantine profiles</i> .

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.

Status Enable Disable

Mount Type SMBv1.0

Network Share Name

Server IP 0.0.0.0

Share Path

Username

Password

Confirm Password

Quarantine Confidence level equal and above 80 % Medium High

- Enable Quarantine Password Protected Files
- Enable Quarantine of Critical Risk files
- Enable Quarantine of Suspicious - High Risk files
- Enable Quarantine of Suspicious - Medium Risk files
- Enable Quarantine of Suspicious - Low Risk files
- Enable Quarantine of Others
- Enable copying or moving clean files to a sanitized location
- Enable Force Rescan
- Enable Scheduled Scan

Schedule Type Minutely

Every (minute) 15 Minutes

Description

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.

Name	Scan Scheduled	Type	Share Path
test	true	SMBv3.0	//test/share

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

Name	Scan Scheduled	Type	Share Path	Quarantine	Enabled	Status
98NFS4	No	NFSv4	/172.19.232.99/home/hec01nfs4	No	Enabled	Down
testshare	Yes	SMBv2.0	/172.19.235.204/share2	Yes	Enabled	Up



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*)

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.



A new scan task will not be added if the network location has a scan task in process.

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 corresponding 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.

Total	Start Time	End Time	Scan Finished	Critical Risk	High Risk	Medium Risk	Low Risk	Clean	Others	Scan Status
	2021/09/09 15:38:30		N/A	0 0	0 0	0 0	Detected Quarantined	0	0 0	Waiting
57837	2021/09/07 11:51:27	2021/09/07 13:42:51	100.00%	748 0	6526 0	48344 0	286 0	1933	0 0	Done

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

Detection Time	File Name	Source	Rating
2021/09/07 11:57:45	66d5222a705c3045fecbb5049dc95e060061459909a6c79c73115e5b0c70cb3.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	bc38f4a05e98469f7ad9b38574e259f36140b73150a7fd1d52ea786f8b9.gz	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	d2c729be39a3136d6e1a0e312f2cf6bfbcf4159f3b724b980e5ac2419a398.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	92495754dd61c60ad7542d49515051cd6637d2d076c9ffa848bb0d3f9baaa6c.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	b01fa74e309cfd0ee5f54a39a908df88a9577d5e21fe251361fa1a89addba06.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	55fda8fe5169419bcdfaf8e712b378085ddd86638e0f84e50e6b643cf19334.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	efc305faa37eeacd7abbc246b71630133b0e8adf2dc9f4189...	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	ce300fe22dd40237e443695aa13c19735e359100883aef58305c077127cf604.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	d3309f84719ce931f1741263eaf2ae1b7826f3a0e486b81b393389767916a9fb.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	af3fc65791861af1dfef759654edaddf7a4690d6c27987805933baf695226977.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	84f3302ec9aee2cc6d7e290e2f395131a22eb277323e91d4060b1c1637d950.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	c34205b4e8f316a75c6819a8c642461fd9b05b4f9862eb6e4f3e52fd11ef52bf.rar	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	1b17c7e9540c11b55defa15f6d050a6c5f87744e32cc7ee8eef9ca7f26cc97a.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	4894673038c422547aac401e1cfb76f8f9848aa903b3e7992e386686fea0acd8.gz	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	a34ef3b5de0fc73918c01a81518a658ee58fde47386e91de5e483c0822b7fe2.gz	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	23fb5bf57b70184335261dec8c9bd0976ef8c1d843486fddc5692aa9618e58e.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	f427ee2e2b27288bfd45d0aa985b3fc19e4b81fac28b8e6112529632040b2ab9.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High
2021/09/07 11:57:45	450f426b4ce996fa470014e739db5382c6ee5b68ee53020c8ad8cac6eda7cd4b.exe	//172.19.235.98/home/neo/ifs4/dataset-100K-suspicious/abuse-ch-prepared	High

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.

Name	Type	Share Path	Enabled	Status
Quarantine1	SMBv1.0	//172.19.235.204/shared	Enabled	✓

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	<i>Enable or Disable.</i>
Quarantine Name	Enter a name for the quarantine profile
Mount Type	Select a Network Share protocol from the list. The following protocols are supported: <ul style="list-style-type: none">• 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.

Status	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable	
Mount Type	SMBv1.0	
Quarantine Name	Quarantine1	?
Server IP	172.19.235.20	?
Share Path	/quarantine1	?
Username	tester1	
Password	••••••••	<input type="button" value="Change"/>
Confirm Password	••••••••	<input type="button" value="Change"/>
<input type="checkbox"/> Keep Original File At Source Location		
Description	<input type="text"/>	

- (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 38](#).

- (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
<i>Enabled</i>	Keeps the quarantine file in the source location.	<i>Enabled</i>	<ul style="list-style-type: none"> Creates a copy of the quarantine file in the quarantine location and renames it <i><Network Share File ID></i>. Creates a metafile with the naming pattern <i><Network Share File ID>.meta</i> for each quarantine file.
<i>Disabled</i>	FortiNDR creates a placeholder file with <i><Filename>.quarantined</i> in the original folder	<i>Enabled</i>	<ul style="list-style-type: none"> Copies the quarantine file to the quarantine location and renames it <i><Network Share File ID></i>. Creates a metafile with the naming pattern <i><Network Share File ID>.meta</i> 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.

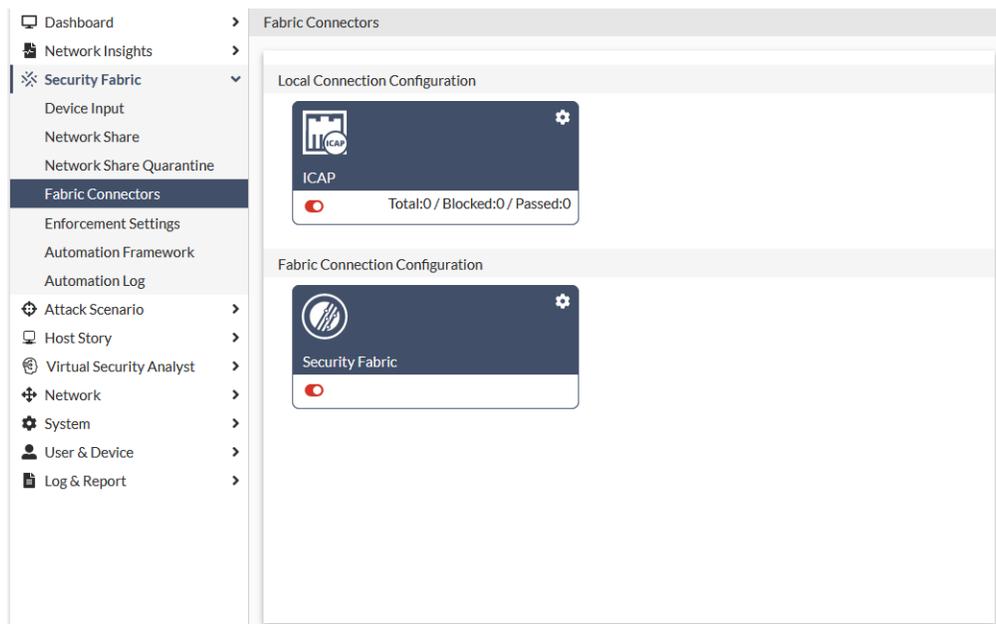
Keep original file at source location	Move/Copy clean files to sanitized location	Effect
<i>Enabled</i>	<i>Enabled</i>	<ul style="list-style-type: none"> Cleans files in the source location. Copy the clean files to the Network Share Quarantine.
<i>Enabled/Disabled</i>	<i>Disabled</i>	<ul style="list-style-type: none"> FortiNDR scans NFS but does not move or copy the files.
<i>Disabled</i>	<i>Enabled</i>	<ul style="list-style-type: none"> Move the clean files to the Network Share Quarantine. 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 submissions 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.

For an example of setting up an ICAP Connector, see [FortiNDR and FortiGate ICAP configuration example on page 41](#).

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*.

The screenshot shows the configuration page for the ICAP Connector in FortiNDR. It is divided into four sections: Status, Connection, Configuration, and Confidence Level.

- Status:** A toggle switch for "Enable ICAP Connector" is currently turned off (indicated by a red dot).
- Connection:** Includes fields for "Interface" (set to port1 (MGMT)), "Port" (1344), "SSL Support" (turned off), and "SSL Port" (11344).
- Configuration:** Includes a toggle for "Realtime FortiNDR Scan" (turned off) and a "Realtime FortiNDR Scan Timeout at" field set to 10 seconds (with a note: "second(s) (Between 1 to 20 second(s), Default: 10 seconds)").
- Confidence Level:** Includes a "Quarantine Confidence level equal and above" field set to 70% and radio buttons for "Medium" (selected) and "High".

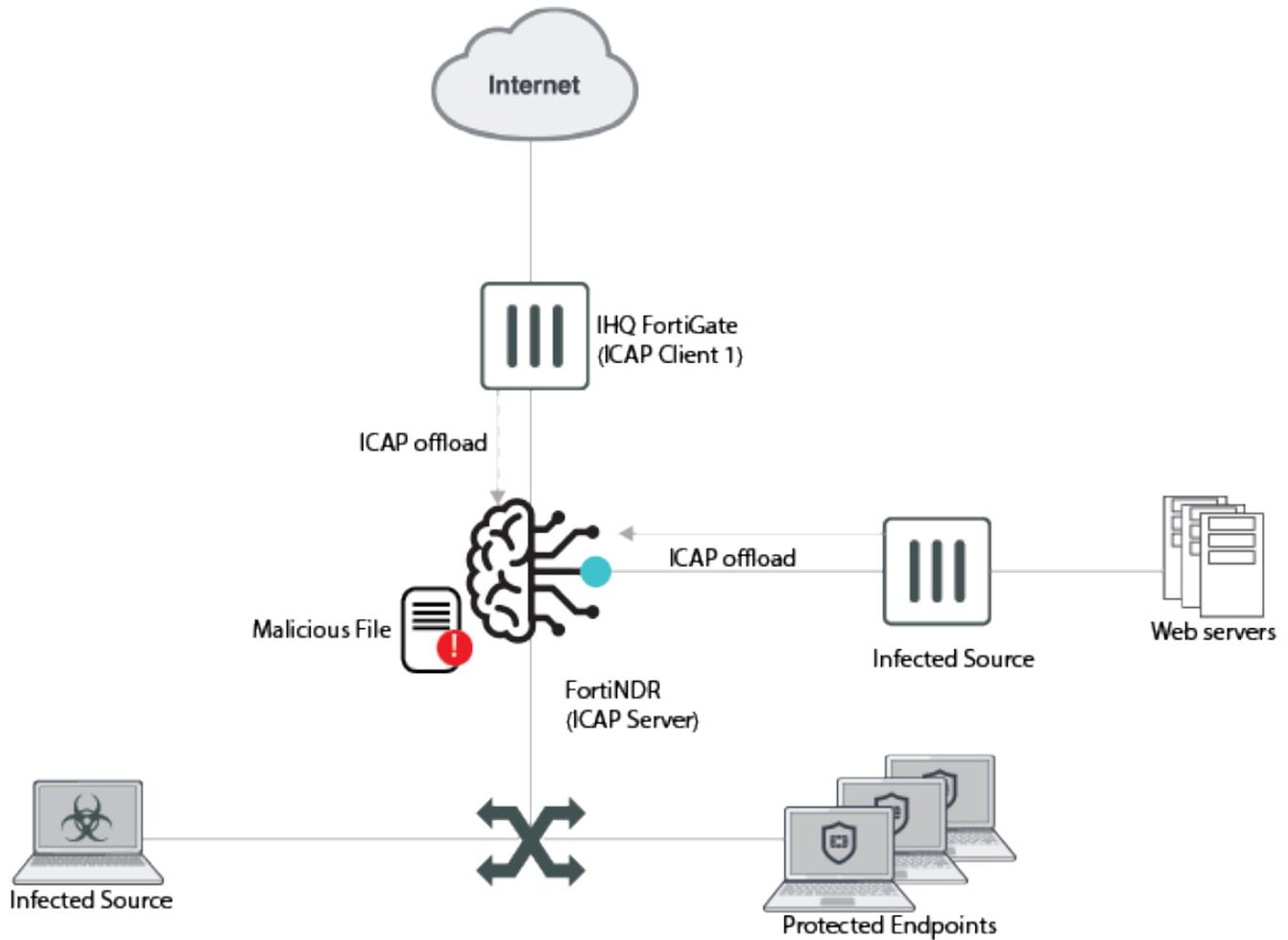
FortiNDR and FortiGate ICAP configuration example

The following is an example of setting up FortiNDR and FortiGate ICAP integration including client experience. This example requires FortiNDR(formerly FortiAI) 1.4 or higher and FortiOS 6.2 or higher.

Topology

In this example, the ICAP server performs malware scanning on HTTP and HTTPS requests. If the ICAP server is unable to process a request, then the request is blocked. Streaming media is not considered by the filter so it is allowed through and is not processed.

FortiNDR and FortiGate ICAP integration works with SSL deep inspection.



To add the ICAP server to the FortiGate in the GUI:

1. Go to *Security Profiles > ICAP Servers* and click *Create New*. If you do not see *ICAP* in the navigation menu, enable the feature with the GUI. See [Feature visibility](#).

FortiGate 90E FGT90E

Dashboard > Edit ICAP Server

Security Fabric >

Network >

System 1 >

Policy & Objects >

Security Profiles ▾

- AntiVirus
- Web Filter
- DNS Filter
- Application Control
- File Filter
- ICAP
- SSL/SSH Inspection

- Application Signatures
- Web Rating Overrides
- Web Profile Overrides

ICAP Servers ☆

Name

IP address

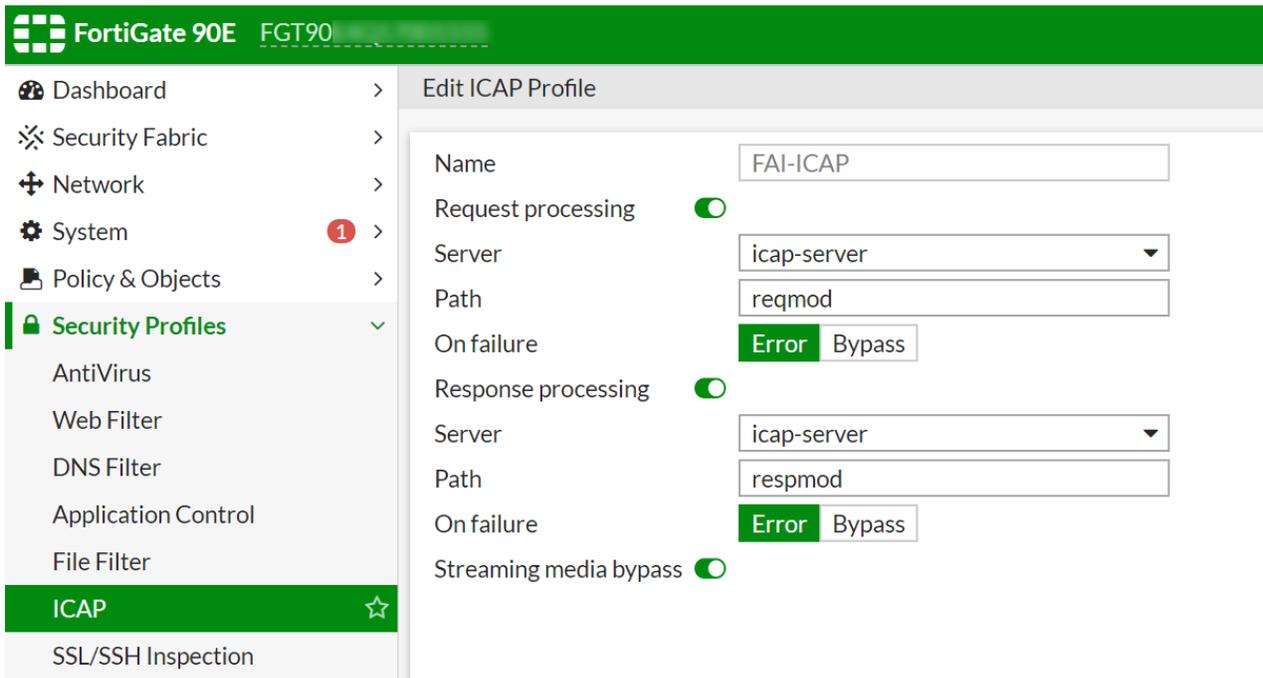
Port

2. For *Name*, enter a name for the ICAP server, such as *icap-server*.
3. Enter the *IP address* of the ICAP server.
4. If required, enter a new *Port* number. The default is 1344.
5. Click *OK*.

The default maximum number of concurrent connections to ICAP server is 512 connections. You can change this default using the CLI.

To create an ICAP profile in the FortiGate GUI:

1. Go to *Security Profiles > ICAP* and click *Create New*.



The screenshot shows the FortiGate GUI for editing an ICAP profile. The left sidebar is expanded to 'Security Profiles' and 'ICAP' is selected. The main panel is titled 'Edit ICAP Profile' and contains the following configuration fields:

- Name: FAI-ICAP
- Request processing:
- Server: icap-server
- Path: reqmod
- On failure: Error
- Response processing:
- Server: icap-server
- Path: respmod
- On failure: Error
- Streaming media bypass:

2. For *Name*, enter a name for the ICAP profile, such as *FAI-ICAP*.
3. Enable *Request processing* and set the following.

Server	Select the ICAP server. In this example, select <i>icap-server</i> .
Path	Enter the path to the processing component on the server. For FortiNDR, enter <i>reqmod</i> .
On failure	Select <i>Error</i> to block the request. If the message cannot be processed, it is blocked.

4. Enable *Response processing* and set the following.

Server	Select the ICAP server. In this example, select <i>icap-server</i> .
Path	Enter the path to the processing component on the server. For FortiNDR, enter <i>respmo</i> .
On failure	Select <i>Error</i> to block the request. If the message cannot be processed, it is blocked.

5. We recommend you enable *Streaming media bypass* to not offload streaming media to the ICAP server.



For optimal performance, disable this option only when traffic is low and all files must be inspected.

6. Click *OK*.

To add the ICAP profile to a policy in the FortiGate GUI:

1. Go to *Policy & Objects* > *FireWall Policy* and click *Create New*.

The screenshot displays the FortiGate GUI configuration for a new Firewall Policy. The left sidebar shows the navigation menu with 'Traffic Shapers' expanded. The main configuration area shows:

- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (unchecked), Proxy-based (checked)
- Firewall / Network Options:**
 - NAT:** Enabled (checked)
 - IP Pool Configuration:** Use Outgoing Interface Address (checked), Use Dynamic IP Pool (unchecked)
 - Preserve Source Port:** Disabled (unchecked)
 - Protocol Options:** default (selected)
- Security Profiles:**
 - AntiVirus:** Disabled (unchecked)
 - Web Filter:** Disabled (unchecked)
 - DNS Filter:** Disabled (unchecked)
 - Application Control:** Disabled (unchecked)
 - File Filter:** Disabled (unchecked)
 - ICAP:** Enabled (checked), FAI-ICAP (selected)
 - SSL Inspection:** certificate-inspection (selected)

2. Configure the policy to apply to the required traffic.
3. Set *Inspection Mode* to *Proxy-based*.
4. In the *Security Profiles* section, enable *ICAP* and select the ICAP server. In this example, select *FAI-ICAP*.
5. Click *OK*.

To add the ICAP server via the CLI:

```
config icap server
  edit "icap-server"
    set ip-address 172.19.235.238
    set port 1344
    set max-connections 512
  next
end
```

To create an ICAP profile via the CLI:

```

config icap profile
  edit "FAI-ICAP"
    set request enable
    set response enable
    set streaming-content-bypass enable
    set request-server "icap-server"
    set response-server "icap-server"
    set request-failure error
    set response-failure error
    set request-path "reqmod"
    set response-path "respmod"
    set methods delete get head options post put trace other
  next
end

```

To add the ICAP profile to a policy via the CLI:

```

config firewall policy
  edit 5
    set name "fai"
    set srcintf "virtual-wan-link"
    set dstintf "virtual-wan-link"
    set srcaddr "FABRIC_DEVICE"
    set dstaddr "FABRIC_DEVICE"
    set dstaddr-negate enable
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode proxy
    set ssl-ssh-profile "certificate-inspection"
    set icap-profile "FAI-ICAP"
    set logtraffic disable
    set fsso disable
    set nat enable
  next
end

```

FortiNDR ICAP configuration

Use the GUI to configure the ICAP server. Configuration via CLI is not currently supported.

To configure the ICAP server:

1. Go to *Security Fabric > Fabric Connectors*.
2. In the *ICAP* connector tile, click the settings icon at the top right.



3. Turn on *Enable ICAP Connector*.

The screenshot shows the configuration page for the ICAP Connector. It is divided into four sections: Status, Connection, Configuration, and Confidence Level.

- Status:** The 'Enable ICAP Connector' toggle is turned on, indicated by a red dot.
- Connection:**
 - Interface: A dropdown menu showing 'port1 (MGMT)'.
 - Port: A text input field containing '1344'.
 - SSL Support: A toggle switch that is turned on.
 - SSL Port: A text input field containing '11344'.
- Configuration:**
 - Realtime FortiNDR Scan: A toggle switch that is turned on.
 - Realtime FortiNDR Scan Timeout at: A text input field containing '10', followed by the text 'second(s) (Between 1 to 20 second(s), Default: 10 seconds)'.
- Confidence Level:**
 - Quarantine Confidence level equal and above: A text input field containing '70', followed by a percentage sign and two radio buttons labeled 'Medium' and 'High'.

4. In the *Connection* section, configure the following.

Interface	Select the interface from the dropdown menu. Default is <i>port1</i> .
Port	Enter the port number. Default is <i>1344</i> .
SSL Support	Enable.
SSL Port	Enter the SSL Port number. Default is <i>11344</i> .

5. In the *Configuration* section, configure the following.

Realtime FAI Scan	Enable. This setting allows FortiNDR to complete new file scanning and obtain the verdict result before sending back the ICAP response.
Realtime FAI Scan Timeout	Enter the value for the ICAP server to wait for the verdict result. Default is 30 seconds.

- 6. In the *Confidence Level* section, select or enter the *Quarantine Confidence level*. Default is 80%. Files verdict results with confidence level equal to or higher than this setting are treated as bad and block code is returned.
- 7. Click *OK*.

Client experience

On client PCs' web traffic, if the FortiNDR ICAP server returns a malicious verdict, the client PC gets a message in its browser. See the following example.

FORTINET

REAL TIME NETWORK PROTECTION

MD5: 980d345c8845b679459dee23f17cd323

File Name: index.php

Category: Downloader - A downloader is a type of malware that has the capability to download other malicious files or an updated version of itself.

Virusname: HTML/Agent.G!tr

Powered by FortiAI

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.

Status	
Enable Security Fabric	<input checked="" type="checkbox"/>
Fabric Device Settings	
FortiGate Root IP	10.0.0.173
TCP Port	8013
FortiNDR IP	10.0.0.94
TCP Port	443

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

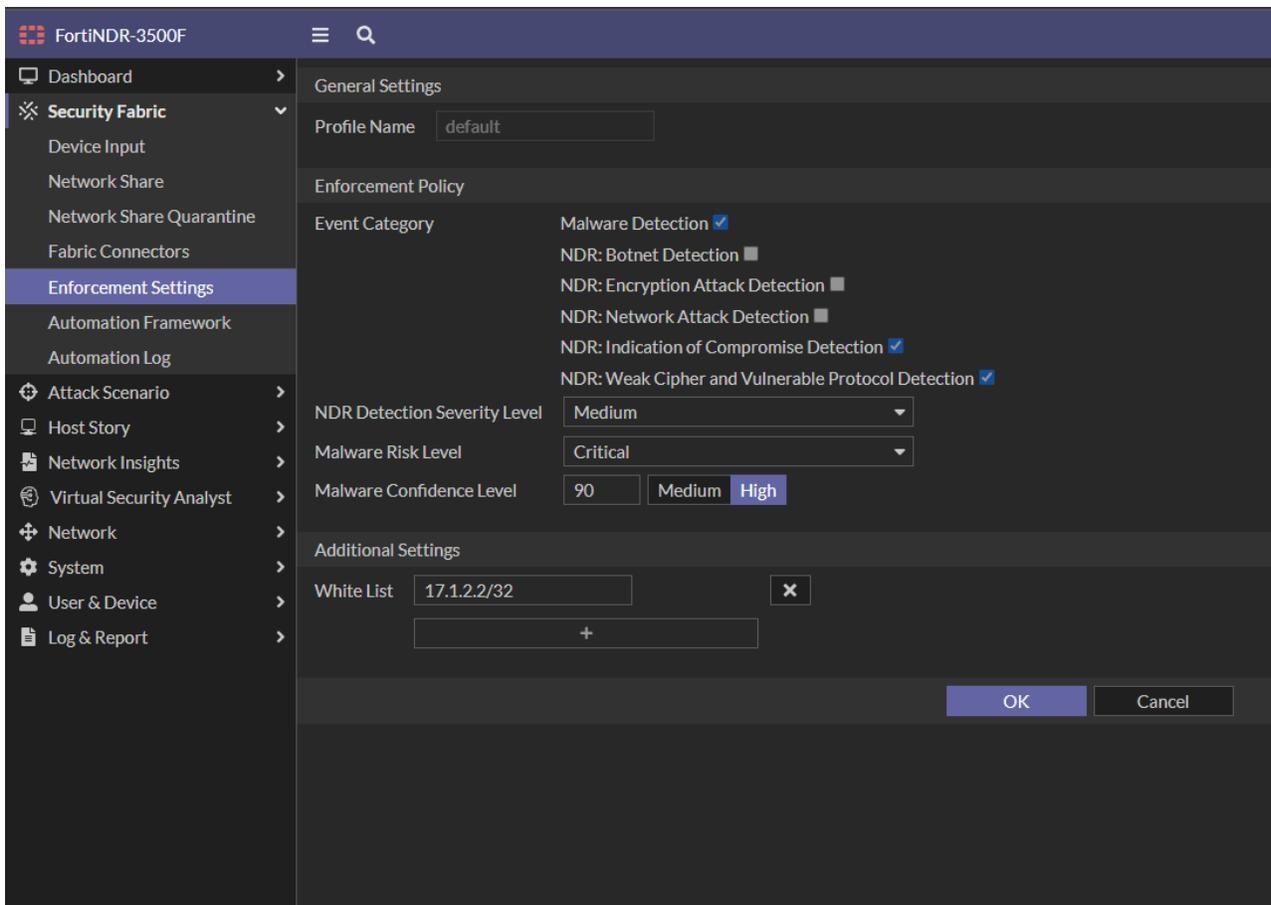
Enforcement Settings are policies for FortiNDR to filter out malicious detections and NDR anomaly detections when executing enforcement. These policies include Event Category, NDR Detection Severity Level, Malware Risk Level, Malware Confidence Level, and Allow List.

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: <ul style="list-style-type: none">• <i>Malware Detection</i>• <i>NDR: Botnet Detection</i>• <i>NDR: Encryption Attack Detection</i>• <i>NDR: Network Attack Detection</i>• <i>NDR: Indication of Compromise Detection</i>• <i>NDR: Weak Cipher and Vulnerable Protocol Detection</i>
NDR Detection Severity Level	Select <i>Critical, High, Medium</i> or <i>Low</i> severity from the dropdown.
Malware Risk Level	Select <i>Critical, High, Medium</i> or <i>Low</i> severity from the dropdown.
Malware Confidence Level	Enter a numeric value for the confidence level and click either <i>Medium</i> or <i>High</i> .
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: <ul style="list-style-type: none"> • <i>Malware Detection</i> • <i>NDR: Botnet Detection</i> • <i>NDR: Encryption Attack Detection</i> • <i>NDR: Network Attack Detection</i> • <i>NDR: Indication of Compromise Detection</i> • <i>NDR: Weak Cipher and Vulnerable Protocol Detection</i>
NDR Detection Severity Level	Select <i>Critical</i> , <i>High</i> , <i>Medium</i> or <i>Low</i> severity from the dropdown.
Malware Risk Level	Select <i>Critical</i> , <i>High</i> , <i>Medium</i> or <i>Low</i> severity from the dropdown.
Malware Confidence Level	Enter a numeric value for the confidence level and click either <i>Medium</i> or <i>High</i> .
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.

FortiNDR-3500F

Dashboard > Security Fabric > Enforcement Settings

General Settings

Profile Name: default

Enforcement Policy

Event Category: 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: Medium

Malware Risk Level: Critical

Malware Confidence Level: 90 Medium High

Additional Settings

White List: 17.1.2.2/32

OK Cancel

4. Click OK.



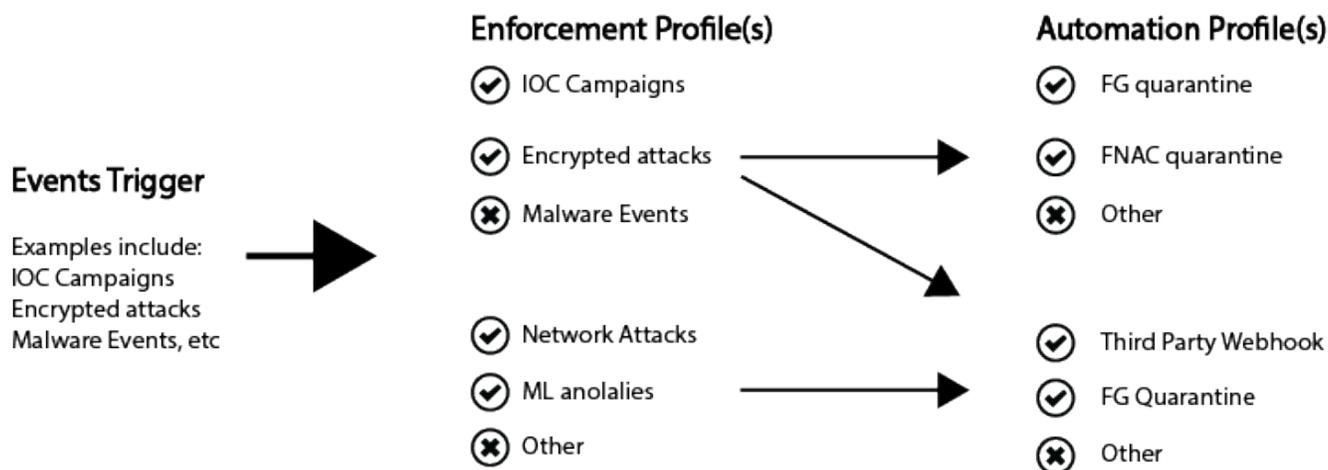
For NDR detection *Severity Level* and *Malware risk level*, severity is inclusive of higher severity levels. For example, if *High* is selected, the enforcement profile will match both HIGH and CRITICAL events.

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.

FortiNDR Response

Understanding 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 <i>Enforcement Settings</i> . See Creating an Enforcement Profile on page 51 .
Action	Select one of the following actions: <ul style="list-style-type: none"> • <i>FortiGate Quarantine</i> • <i>FortiNAC Quarantine</i> • <i>Generic Webhook</i>
Source	<p>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.</p> <p>Sniffer: If the source of detection came from a sniffer, the enforcement is adapted by all profiles where <i>Trigger Source</i> is <i>Sniffer</i>. 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.</p>
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 <code>ip_blocker</code> . Only applicable to <i>FortiGate Quarantine</i> and <i>FortiSwitch Quarantine</i> via <i>FortiLink</i> .
WebHook Name for Undo	Select the FortiGate webhook for undo action, such as <code>ip_unblocker</code> . Only applicable to <i>FortiGate Quarantine</i> and <i>FortiSwitch Quarantine</i> via <i>FortiLink</i> .
Webhook Execution Settings	Enter the URL, Method, Header and HTTP body Template for Execution webhook settings. Only applicable to <i>Generic Webhook</i> .
Webhook Undo Settings	Enter the URL, Method, Header and HTTP body Template for Undo webhook settings. Only applicable to <i>Generic Webhook</i> .

Automation Framework

Profile Name

Enable

Enforcement Profile

Action FortiGate Quarantine

FortiGate Quarantine Settings

Source Fabric Device Sniffer

API Key ●●●●●● Change

IP

Port 443

VDOM

Webhook Name for Execution

Webhook Name for Undo

Test Current Configuration

OK
Cancel

4. Test the configuration

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*.

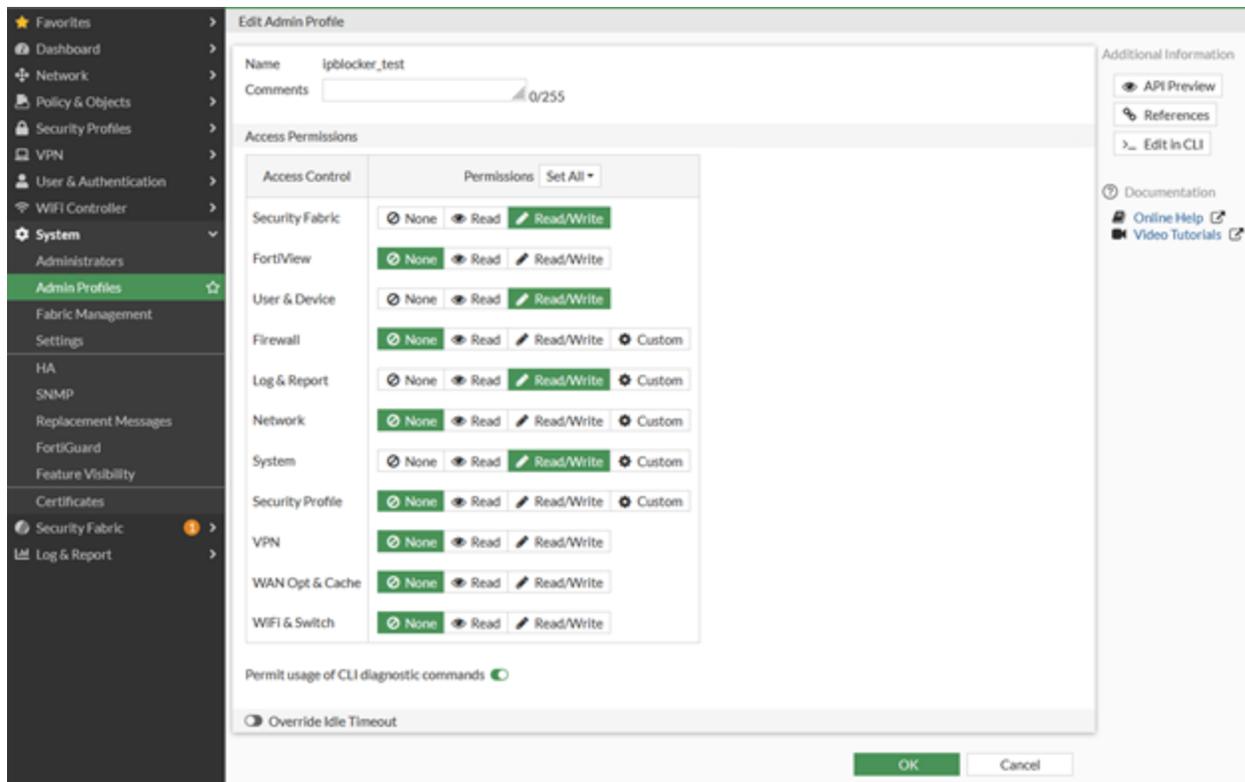
The following example shows you how to set up webhooks for FortiGate Quarantine to quarantine infected hosts through FortiGate.

To set up a webhook for Ban IP:

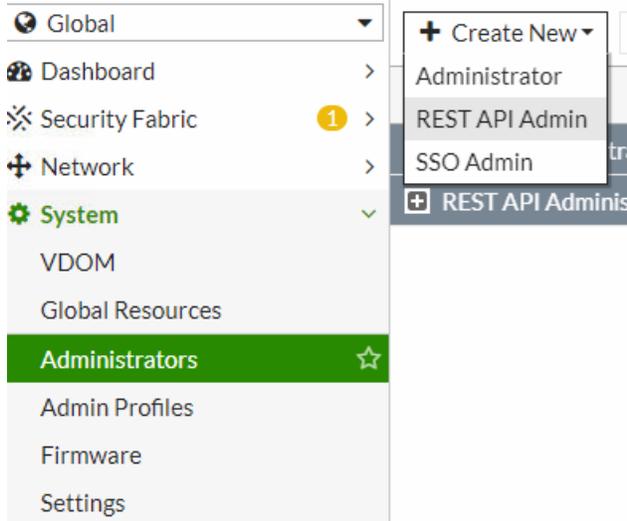
1. In FortiGate, go to *System > Admin Profiles* and create a profile, for example, *ipblocker_test* and set the following *Access Permissions*.



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.

New REST API Admin

Username

Comments 0/255

Administrator Profile

Virtual Domains

PKI Group

CORS Allow Origin

Restrict login to trusted hosts

Trusted Hosts

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

New API key

New API key for ipblocker_user

i This is the only place this key will be provided. Keep this information secure. The bearer of this API key will be granted all access privileges assigned to this account.

- 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.
- In the *New Automation Stitch CLI 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
```

New Automation Stitch

Name

Status Enabled Disabled

Trigger



Incoming Webhook

Action



CLI Script



Email



FortiExplorer Notification



Access Layer Quarantine



Quarantine FortiClient

Minimum interval (seconds)

CLI Script

1st Action

Name

Script

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

+ Upload

>_ Record in CLI console

+

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 Stitch* CLI 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:

Automation Profile Name	Action Type	WebHook for Execution	WebHook for Cancellation	IP	VDOM	PORT	Enable
SnifferHook	Ban IP	SnifferOverride_block	SnifferOverride_unblock	0.0.0.0	root	443	✔ Enabled
fgt1	Ban IP	ipblocker	ipunblocker	172.19.235.251	root	443	✔ Enabled

FortiOS v7.0.1

Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
ip_blocker	Enabled	ip_blocker	ip_blocker	All FortiGates	1	2 seconds ago
ip_unblocker	Enabled	ip_unblocker	ip_unblocker	All FortiGates	64	37 minutes ago



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.

Automation Framework

Profile Name:

Enable:

Enforcement Profile:

Action:

Manage FortiGate Settings

Source:

API Key:

IP:

Port:

VDOM:

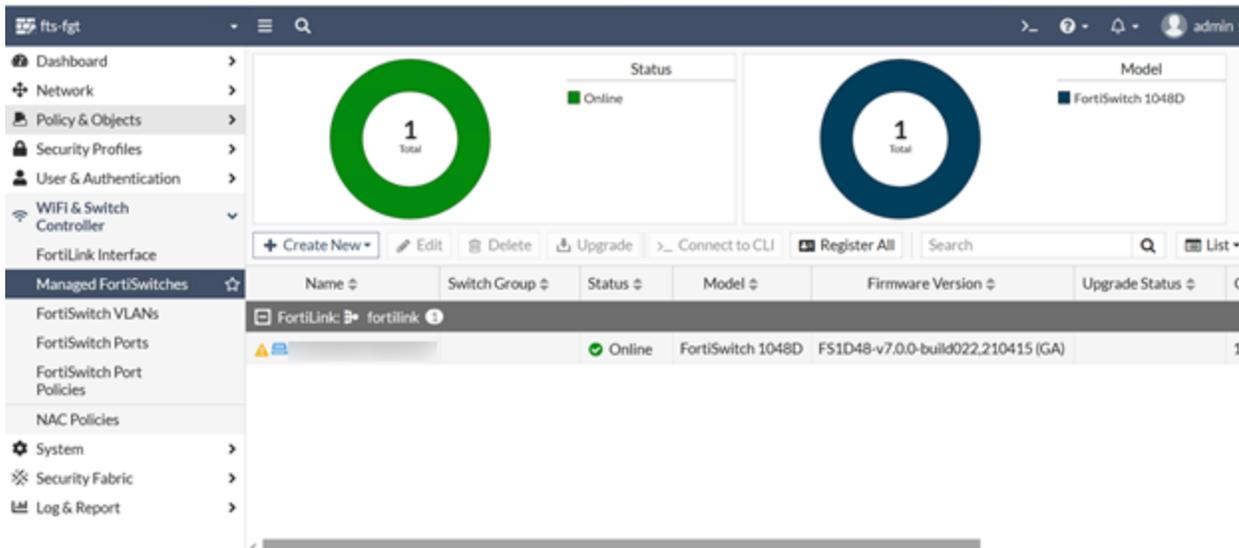
Webhook Name for Execution:

Webhook Name for Undo:

FortiSwitch quarantine setup example

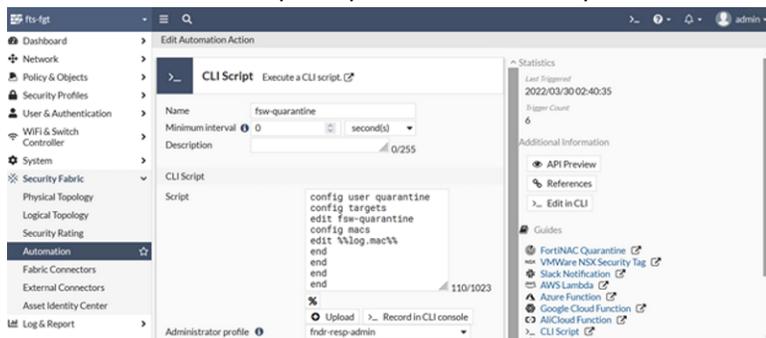
FortiNDR supports quarantining devices that are connected to a FortiSwitch which is managed by FortiGate. FortiSwitch is connected to a FortiGate and is configured in FortiLink mode. FortiNDR will utilize FortiGate’s incoming webhook to provide the device's MAC address for quarantine/undo quarantine.

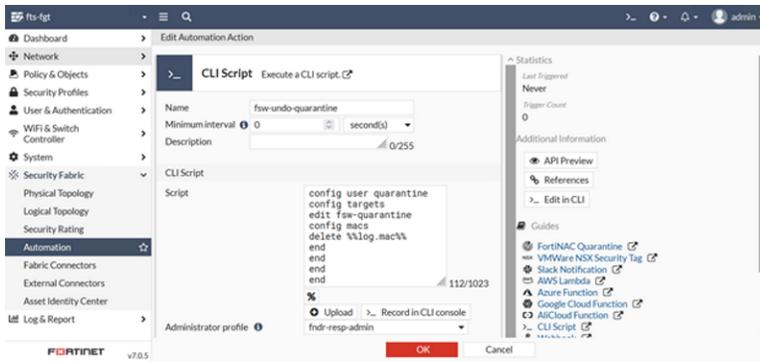
For information about configuring FortiLink, see [Configuring FortiLink](#).



To setup FortiSwitch quarantine on FortiNDR:

1. Following the steps for creating a webhook on FortiGate in [FortiGate quarantine webhook setup example](#) on page 55. Note that the CLI script for quarantine and undo quarantine should be updated.



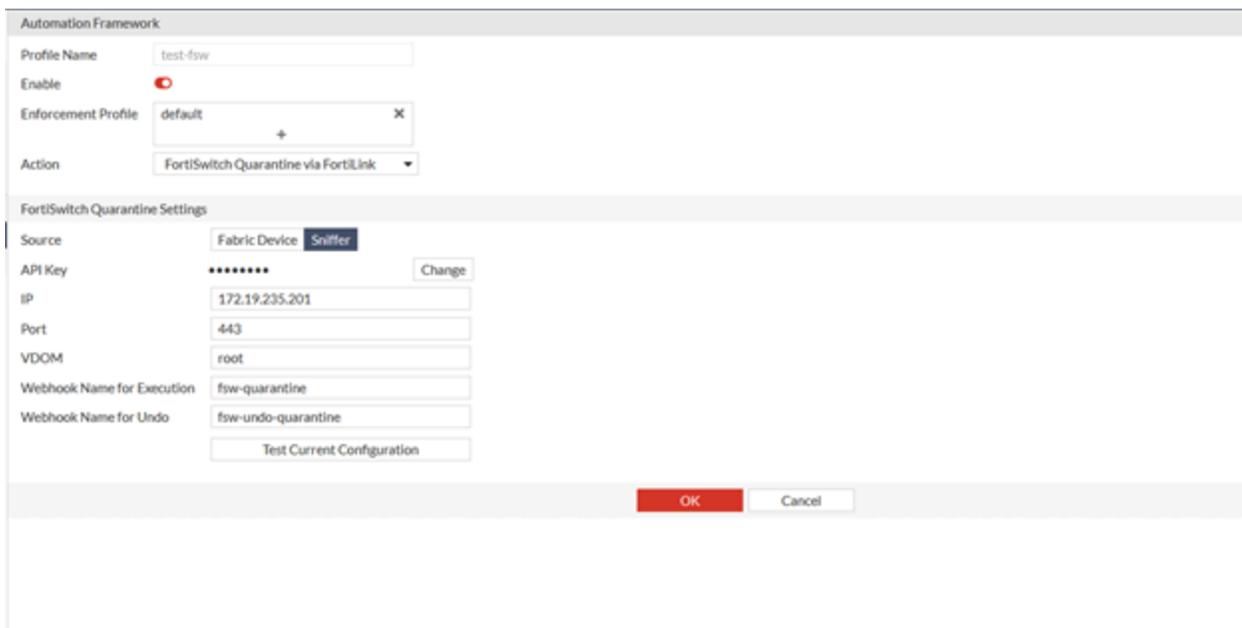


The CLI script for quarantine and undo quarantine should be updated.

2. Register webhooks on FortiNDR .



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



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

The screenshot shows the FortiNAC interface with a table of ports and a modal window for port 172.19.140.2. The table has columns for Port, Trunk, Mode, Port Policy, Enabled Features, Native VLAN, Allowed VLANs, PoE, Device Information, DHCP Snooping, and Transceiver. The modal window displays details for the device with IP 172.19.140.2, including MAC Address, DHCP Lease, Online Interfaces, Hardware, and OS. A 'Quarantine' button is visible in the modal window.

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping	Transceiver
port17		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port18		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port19		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port20		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port21		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port22		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port23		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port24		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port25		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)		e4-43-4b-80c2da	Trusted	
port26		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	
port27		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)	quarantine.fortilink (quarantine)			Untrusted	

- Click *OK*.

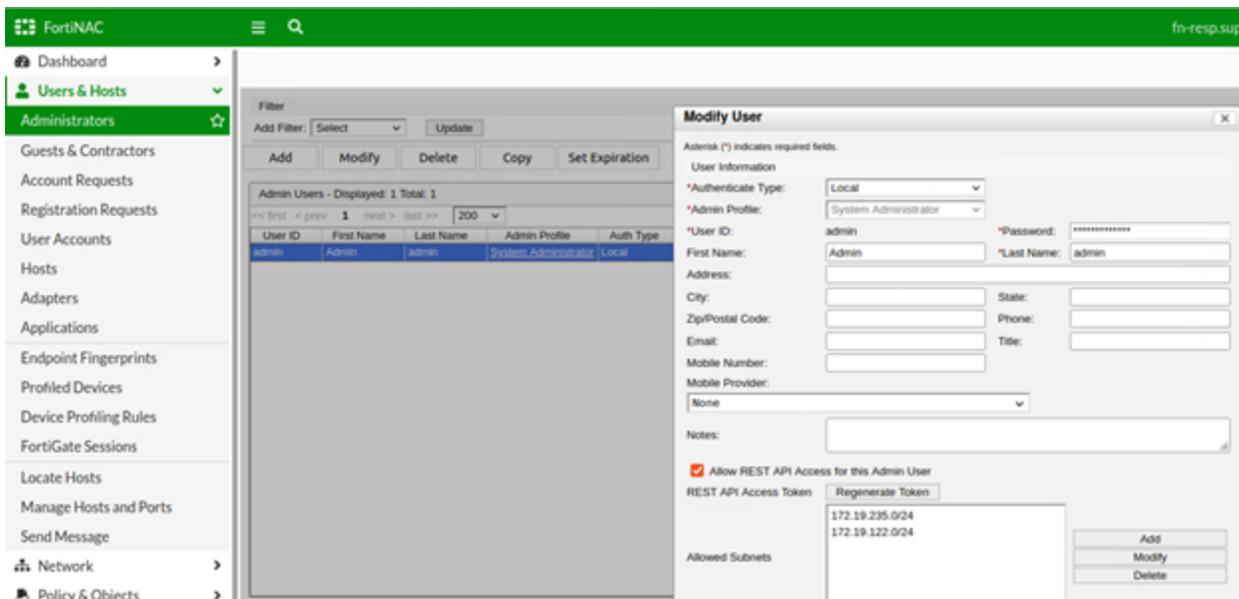
FortiNAC quarantine setup example

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

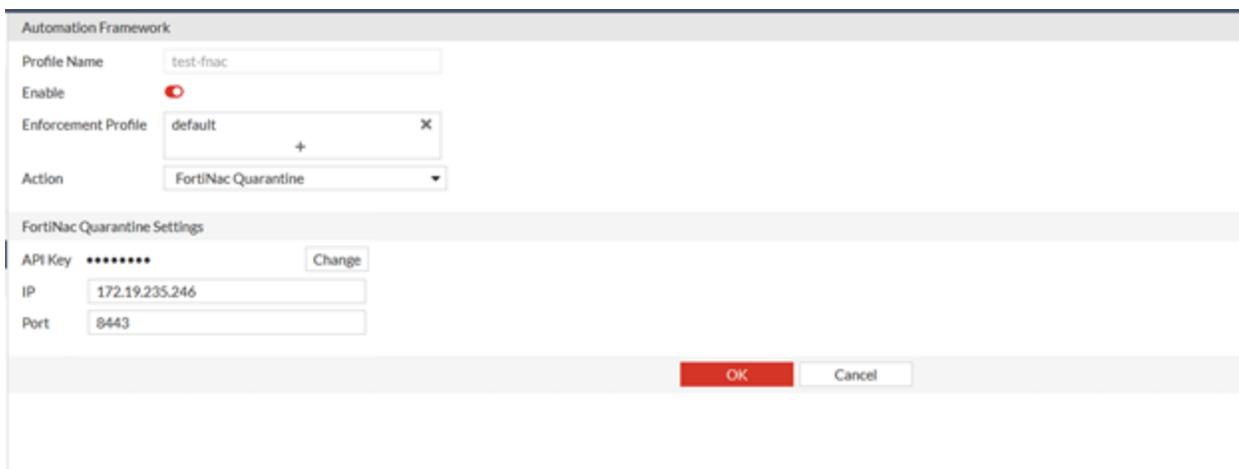
For information about configure FortiNAC, see the [FortiNAC Administration Guide](#) in the Document Library.

To setup FortiNAC quarantine on FortiNDR:

- In FortiNAC:
 - Go to *Users & Hosts > Administrators > Modify User*.
 - Enable *REST API access to FortiNAC* and generate HTTP API access token.
 - 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 Framework

Profile Name:

Enable:

Enforcement Profile: ✕

+

Action:

Webhook Execution Settings

URL:

Method:

Header:

Content-Type: ✕

Authorization: ✕

+

HTTP Body Template:

Webhook Undo Settings

URL:

Method:

Header:

Authorization: ✕

Content-Type: ✕

+

HTTP Body Template:

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.

	Initial Action time #	Target IP #	Target MAC #	Violations #	Action Type #	Automation Profile Name #	Enforcement Profile Type #	Action Executed #	Post Action #	Status #
Security Fabric	2022/04/16 21:30:30	18.1.2.120	00:50:56:8c:b3:db	38	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
Device Isolation	2022/04/16 21:30:30	18.2.6.255	00:50:56:8c:b3:db	46	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
Network Share Quarantine	2022/04/16 21:30:30	18.1.8.112	00:50:56:8c:b3:db	20	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Fabric Connectors	2022/04/16 21:30:30	18.1.7.85	00:50:56:8c:b3:db	7	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Enforcement Settings	2022/04/16 21:30:30	18.2.12.106	00:50:56:8c:b3:db	19	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Automation Framework	2022/04/16 21:30:30	18.2.1.188	00:50:56:8c:b3:db	15	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Automation Log	2022/04/16 21:30:30	18.1.12.122	00:50:56:8c:b3:db	15	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Attack Scenarios	2022/04/16 21:30:30	18.1.1.16	00:50:56:8c:b3:db	18	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Host Story	2022/04/16 21:30:30	18.1.3.222	00:50:56:8c:b3:db	10	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Virtual Security Analyst	2022/04/16 21:30:30	18.2.2.171	00:50:56:8c:b3:db	42	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Network	2022/04/16 21:30:29	18.1.8.123	00:50:56:8c:b3:db	37	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
System	2022/04/16 21:30:29	18.1.3.50	00:50:56:8c:b3:db	7	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
User & Authentication	2022/04/16 21:30:29	18.2.1.117	00:50:56:8c:b3:db	10	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:29	None	Executed
Log & Report	2022/04/16 21:30:29	18.1.12.1	00:50:56:8c:b3:db	45	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:29	None	Executed

Violation details

The screenshot shows a 'Log Violation Details' window. The main table lists violations with columns: Initial Action time, Target IP, Target MAC, Violations, and Action. A specific violation is highlighted. The 'View Session Detail' window is open, showing a table with columns: Open Time, Session ID, Severity, and Anomaly Type. The data in the session detail table is as follows:

Open Time	Session ID	Severity	Anomaly Type
2022/04/15 22:27:58	529491	Low	FortiNDR ML Discovery
2022/04/15 23:01:48	1205355	Low	FortiNDR ML Discovery
2022/04/15 23:30:48	304587	Low	FortiNDR ML Discovery
2022/04/15 23:40:32	365982	Low	FortiNDR ML Discovery
2022/04/16 01:13:40	344428	Low	FortiNDR ML Discovery
2022/04/16 01:20:12	369741	Low	FortiNDR ML Discovery
2022/04/16 01:33:34	542049	Low	FortiNDR ML Discovery

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 <i>Status</i> changes to <i>Executed</i> . If the action fails, the <i>Status</i> changes back to <i>Active</i> .	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 151](#).
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.

The screenshot shows the 'FortiNDR Settings' configuration window. It includes a table of settings and two buttons at the bottom.

Setting	Value
Enable	<input checked="" type="checkbox"/>
Server IP:	10.59.26.252
Token:
Rating Timeout (Seconds):	5
Uploading Timeout (Seconds):	2
Maximum File Size (KB):	2048

Buttons: **OK** (green), **Test Connection** (grey)

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

The screenshot shows the 'Scan Profile' configuration window with the 'Pre-Filter' tab selected. It contains several sections of file type and content filtering options.

Process the following selected file types.

- Executables:
- PDF documents:
- Office documents:
- Flash files:
- Web pages:
- Compressed archives:
- Android files:
- Mac files:
- Linux files:
- URL detection:
- User defined extensions:

Notes: The file type prefiltering applies to submission via sniffer, adapters and Fabric devices (except FortiMail). Files from OnDemand, FortiMail and Network Share are always processed.

Check for Active Content on the selected file types during VM Scan pre-filter.

- office:
- dll:
- htm:
- js:
- pdf:
- swf:
- url:
- archive:

Notes: Active Content are embedded codes that can be executed (e.g. macros scripts). When enabled, the overall system throughput is improved by only processing files with active content. Otherwise, forward all files. All executable files are forwarded.

Use the results of the following during VM Scan pre-filter.

- FortiNDR entrust:
- Trusted Vendor:
- Trusted Domain:

Button: **Apply** (green)

Network Insights

Network Insights monitors display information about NDR detections. Detections are organized by category *Botnet*, *FortiGuard IOC*, *Network Attacks*, *Weak/Vulnerable Communication*, *Encrypted Attack* and *ML Discovery*. The charts in *Network Insights* can display a maximum of 30,000 insights.

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.

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.

The screenshot displays the FortiNDR Network Insights interface. On the left, there are two donut charts: one for 'malware' with a count of 64 and another for 'Critical' with a count of 64. Below these are filters for 'View Related Device', 'View Related Session', 'View Device', and 'View Session', along with a timestamp range from 2022-06-14 14:47:16 to 2022-07-14 15:35:11. The main table lists anomalies with columns for Timestamp, Severity, Category, and IOC Hash. One entry is highlighted in green, corresponding to the 'Session Information' pane on the right.

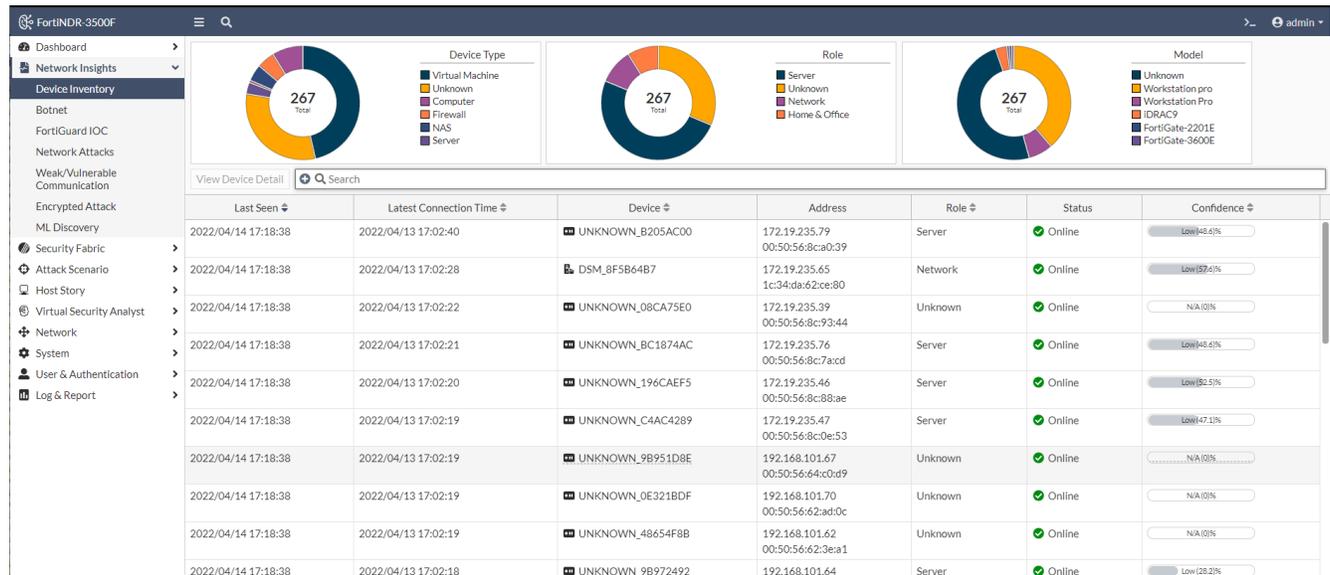
The 'Session Information' pane shows the following details:

- General:** Session ID: 2111333, Start Time: Wed Jul 13 2022 23:18:35 GMT-0700 (Pacific Daylight Time), End Time: (blank), Traffic Volume: 1556.
- Anomaly:** Anomaly Type: Encrypted Attacks, Severity: Critical, Reason: JA3 hash [1d095e68489d3c535297cd8dfb06cb9] detected.
- Additional Information:**
 - TLS JA3 Information: Available (Critical)
 - TLS Version: 4 (High)
 - TLS Cipher: TLS_RSA_WITH_AES_128_CBC_SHA (High)
 - TLS Certificates: 2
 - TLS Verified Server Name Indication (SNI): False
 - TLS Valid Certificate Time: True
 - TLS Host: ruoft.host (Critical)
- Source Device:**
 - Source IP: 17.16.2.2
 - Source Port: 49347
 - Source Packet Size: 541
 - Source Country: United States
 - Source Device Model: N/A
 - Source Device Type: N/A
 - Source Device Sub Type: N/A
- Destination Device:**
 - Destination IP: 17.16.1.100
 - Destination Port: 443
 - Destination Packet Size: 0
 - Destination Country: United States

Device Inventory

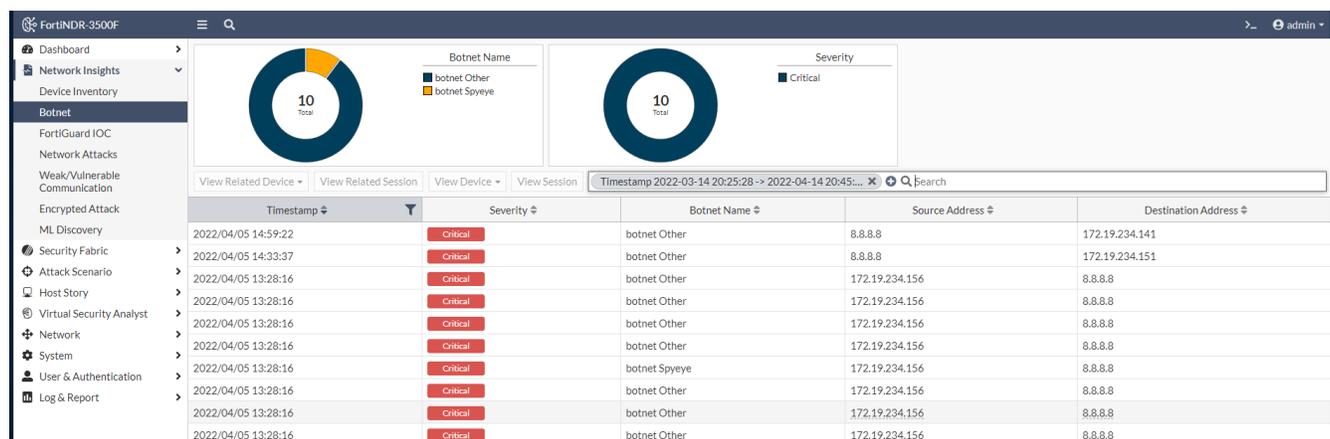
The Device Inventory page displays the discovered devices. The *Device* and *Role* columns are dependent on IOT lookup service.

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*.



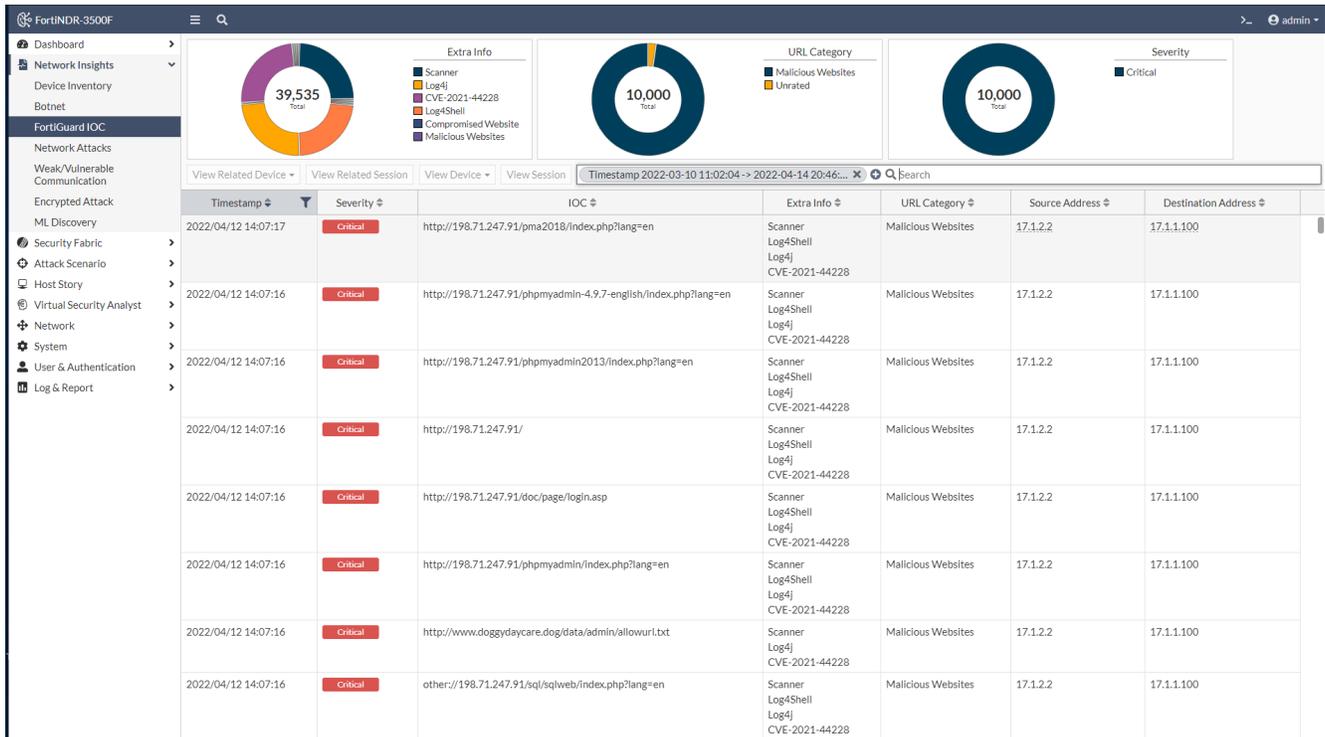
Botnet

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



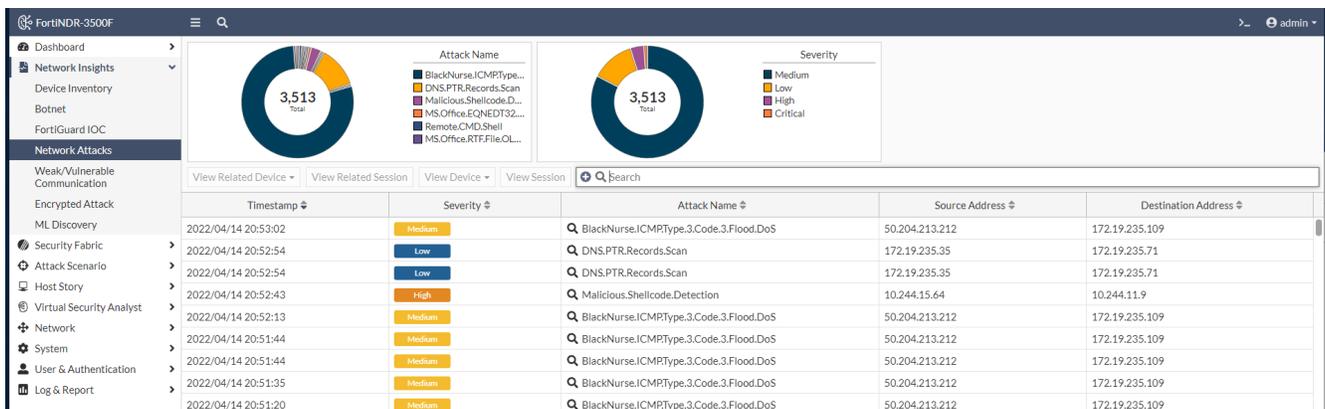
FortiGuard IOC

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



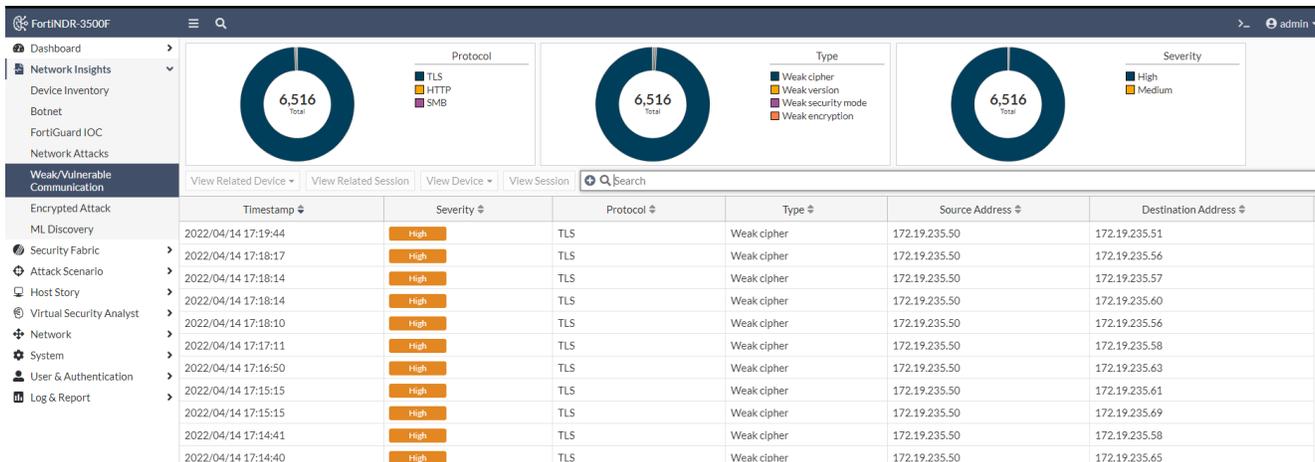
Network Attacks

Network Attacks are known attacks detected by 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 <i>cram-md5</i> , 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

Communication type	Description
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.
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

```

> Transmission Control Protocol, Src Port: 443, Dst Port: 31749, Seq: 1, ACK: 518, Len: 1430
  Transport Layer Security
    TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 118
      Version: TLS ( )
      Random: 0b82b3a7f99484d6c318e93f7e2f79020ad024a7e10017b974117c1a4fb6b789
      Session ID Length: 32
      Session ID: 96250d1c4b7bf2244ba0466495cf5df38a3d765f01a1aea089c0e37be1f7b
      Cipher Suite: TLS_ ( )
      Compression Method: null (0)
      Extensions Length: 46
      > Extension: key_share (len=36)
      > Extension: supported_versions (len=2)
        Type: supported_versions (43)
        Length: 2
        Supported Version: TLS ( )
        [JA3S Fullstring: 771,4005,31-45]
        [JA3S: eb1d94daa7e0344597e756a1fb6e7054]
    TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
  
```

Weak security mode

The screenshot displays a network capture of SMB traffic. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.3	10.10.0.2	TCP	66	2204 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	0.000188	10.10.0.3	10.10.0.2	TCP	66	[TCP Out-Of-Order] [TCP Port numbers reused] 2204 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	0.000287	10.10.0.2	10.10.0.3	TCP	66	445 → 2204 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
4	0.000754	10.10.0.2	10.10.0.3	TCP	66	[TCP Out-Of-Order] 445 → 2204 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
5	0.000476	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.653863	10.10.0.3	10.10.0.2	SMB	146	Negotiate Protocol Request
7	0.654248	10.10.0.2	10.10.0.3	SMB	267	Negotiate Protocol Response
8	0.855430	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=89 Ack=210 Win=64031 Len=0
9	1.320851	10.10.0.3	10.10.0.2	SMB	241	Session Setup AndX Request, NTLMSSP_NEGOTIATE
10	1.321035	10.10.0.2	10.10.0.3	SMB	412	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED

The packet details pane for the selected SMB Negotiate Protocol Response (Frame 7) shows the following information:

- Frame 7: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits)
- Ethernet II, Src: VMware_a8:45:c0 (00:50:56:a8:45:c0), Dst: VMware_a8:1f:7c (00:50:56:a8:1f:7c)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1113
- Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.3
- Transmission Control Protocol, Src Port: 445, Dst Port: 2204, Seq: 1, Ack: 89, Len: 209
- NetBIOS Session Service
- SMB (Server Message Block Protocol)
 - SMB Header
 - Negotiate Protocol Response (0x72)
 - Word Count (WCT): 17
 - Selected Index: 3: NT LM 0.12
 - Security Mode: NT LM 0.12**
 - Max Mpx Count: 50
 - Max VCs: 1
 - Max Buffer Size: 16644
 - Max Raw Buffer: 65536
 - Session Key: 0x00000000
 - Capabilities: 0x8001f3fc, Unicode, Large Files, NT SMBs, RPC Remote APIs, NT Status Codes, Level 2 Oplocks, Lock and Read, NT Find, Dfs, Infollevel Passth...
 - System Time: Apr 23, 2015 03:11:08.611869400 Pacific Daylight Time
 - Server Time Zone: 0 min from UTC
 - Challenge Length: 0
 - Byte Count (BCC): 136
 - Server GUID: 96afd22e-c9d0-4b45-87ef-481dfd5653e5
 - Security Blob: 607606062b0601050502a06c306aa03c303a060a2b06010401823702021e06092a064882...

Weak extended security

The screenshot shows a Wireshark capture of SMB traffic. The packet list pane shows a sequence of packets, with packet 7 (SMB) selected. The packet details pane shows the SMB structure, including the SMB Header and Flags2 field. The Flags2 field contains several bits, with the 'Extended Security Negotiation' bit (0x2801) set, which is highlighted by a red box. The status bar at the bottom indicates 'Is extended security negotiation supported? (smb.flags2.esn), 2 bytes'.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000354	10.10.0.2	10.10.0.3	TCP	66	[TCP Out-Of-Order] 445 → 2204 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460...
5	0.000476	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.653863	10.10.0.3	10.10.0.2	SMB	140	Negotiate Protocol Request
7	0.654248	10.10.0.2	10.10.0.3	SMB	267	Negotiate Protocol Response
8	0.855430	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=89 Ack=210 Win=64031 Len=0
9	1.320851	10.10.0.3	10.10.0.2	SMB	241	Session Setup AndX Request, NTLMSSP_NEGOTIATE
10	1.321035	10.10.0.2	10.10.0.3	SMB	412	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSIN...
11	1.517768	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=272 Ack=564 Win=63677 Len=0
12	1.969184	10.10.0.3	10.10.0.2	SMB	525	Session Setup AndX Request, NTLMSSP_AUTH, User: LAB\Administrator
13	1.971084	10.10.0.2	10.10.0.3	SMB	202	Session Setup AndX Response

```

> Frame 7: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits)
> Ethernet II, Src: VMware_a8:45:c0 (00:50:56:a8:45:c0), Dst: VMware_a8:1f:7c (00:50:56:a8:1f:7c)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1113
> Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.3
> Transmission Control Protocol, Src Port: 445, Dst Port: 2204, Seq: 1, Ack: 89, Len: 209
> NetBIOS Session Service
  SMB (Server Message Block Protocol)
    SMB Header
      Server Component: SMB
      [Response to: 6]
      [Time from request: 0.000385000 seconds]
      SMB Command: Negotiate Protocol (0x72)
      Error Class: Success (0x00)
      Reserved: 00
      Error Code: No Error
    > Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
    > Flags2: 0x2801, Execute-only Reads, Extended Security Negotiation, Long Names Allowed
      0... .. = Unicode Strings: Strings are ASCII
      .0.. .. = Error Code Type: Error codes are DOS error codes
      .1. .... = Execute-only Reads: Permit reads if execute-only
      0... .. = Dfs: Don't resolve pathnames with Dfs
      .... 1... .. = Extended Security Negotiation: Extended security negotiation is supported
      .... .0.. .. = Reparse Path: The request does not use a @gmt reparse path
      .... ..0. .... = Long Names Used: Path names in request are not long file names
      .... ..0. .... = Security Signatures Required: Security signatures are not required
      .... ..0... .. = Compressed: Compression is not requested
      .... ..0.. = Security Signatures: Security signatures are not supported
      .... ..0. = Extended Attributes: Extended attributes are not supported
  
```

```

0000 00 50 56 a8 1f 7c 00 50 56 a8 45 c0 81 00 04 59  PV...|PVE...Y
0010 08 00 45 00 00 f9 6a 5f 40 00 80 06 74 f7 0a 0a  ..E...j_@...t...
0020 00 02 0a 0a 00 03 01 bd 08 9c 7a 75 3c 34 a0 ae  ....zuku4...
0030 3c d7 50 18 fa f0 1b 94 00 00 00 00 cd ff 53  <P.....S
0040 4d 42 72 00 00 00 00 98 01 28 00 00 00 00 00  MBr...(.
0050 00 00 00 00 00 00 00 72 7c 00 00 a5 44 11 03  ....r|...D...
0060 00 0f 32 00 01 00 04 41 00 00 00 00 01 00 00 00  ..2...A.....
0070 00 00 fc f3 01 80 26 a3 2f d1 ad 7d d0 01 00 00  ....&/.}....
0080 00 88 00 96 af d2 2e c9 d0 4b 45 87 ef 48 1f df  ....,KE..H...
0090 56 53 e5 60 76 06 06 2b 06 01 05 05 02 a0 6c 30  VS.v...+.....10
00a0 6a a0 3c 30 3a 06 0a 2b 06 01 04 01 82 37 02 02  j-<0:++.....7...
00b0 1e 06 09 2a 86 48 82 f7 12 01 02 02 06 09 2a 86  ...*..H.....*
00c0 48 86 f7 12 01 02 02 06 0a 2a 86 48 86 f7 12 01  H.....*..H....
00d0 02 02 03 06 0a 2b 06 01 04 01 82 37 02 02 0a a3  ...+.....7....
00e0 2a 30 28 a0 26 1b 24 6e 6f 74 5f 64 65 66 69 6e  *0(&.$n ot defin
00f0 65 64 5f 69 6e 5f 52 46 43 34 31 37 38 40 70 6c  ed_in_RF_C4178@pl
0100 65 61 73 65 6f 69 67 6e 6f 72 65  ..e...ign one
  
```

Is extended security negotiation supported? (smb.flags2.esn), 2 bytes | Packets: 22 · Displayed: 22 (100.0%) | Profile: Default

Weak dialect

The image shows a Wireshark capture of SMB traffic. The packet list pane displays several packets, with packet 4 (SMB) and packet 5 (SMB) highlighted. Packet 4 is a Negotiate Protocol Request (293) and packet 5 is a Negotiate Protocol Response (294). The packet details pane for packet 5 shows the following structure:

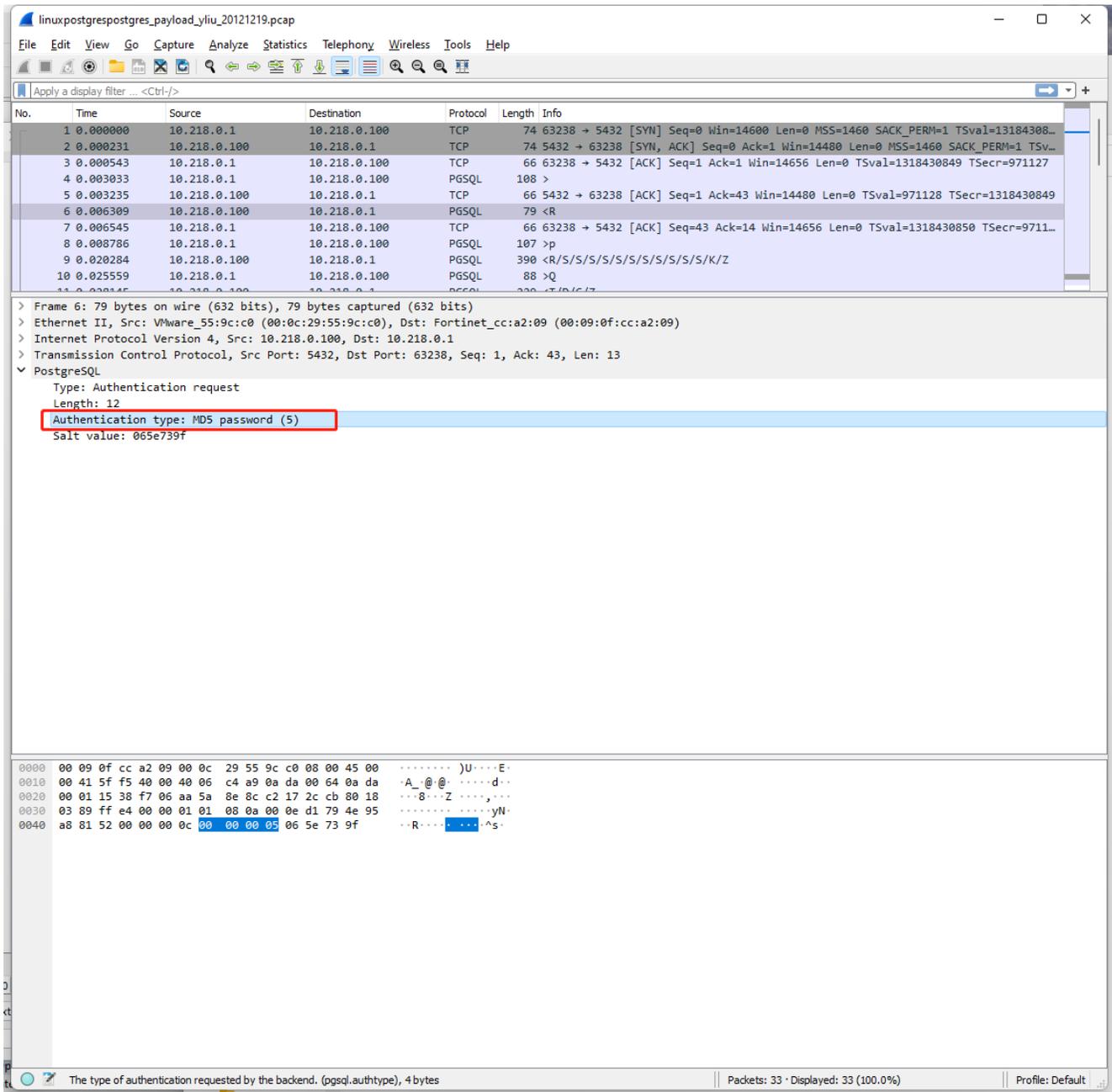
- SMB2 (Server Message Block Protocol version 2)
 - SMB2 Header
 - Negotiate Protocol Response (0x00)
 - StructureSize: 0x0041
 - Security mode: 0x01, Signing enabled
 - Dialect:
 - NegotiateContextCount: 0
 - Server Guid: e6fa9a19-c50f-49c1-b76b-e5fbd1c6f112
 - Capabilities: 0x00000001, DFS
 - Max Transaction Size: 65536
 - Max Read Size: 65536
 - Max Write Size: 65536
 - Current Time: Dec 6, 2011 12:18:15.380156000 Pacific Standard Time
 - Boot Time: Dec 6, 2011 12:14:24.781250000 Pacific Standard Time
 - Blob Offset: 0x00000080
 - Blob Length: 108
 - Security Blob: 606a06062b0601050502a060305ea030302e06092a864882f71201020206092a864886f7...
 - NegotiateContextOffset: 0x204d4c20

The hex dump at the bottom shows the raw bytes of the response, with the dialect field (0x00) highlighted in blue.

```

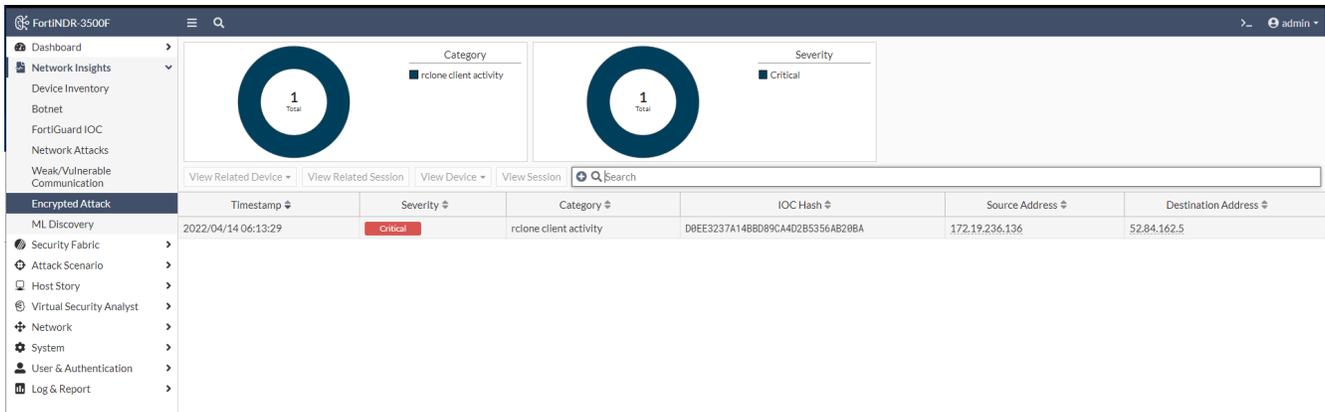
0000 00 0c 29 6b 99 0f 00 0c 29 4e b0 d0 08 00 45 00  ..)k....)N...E
0010 01 18 01 5d 40 00 80 06 e4 6c 0a 00 00 0c 0a 00  ...]@...l....
0020 00 0b 01 bd c0 38 c8 ea 79 f3 9b 7e 13 98 50 18  ....8...y...P
0030 01 00 c0 59 00 00 00 00 00 ec fe 53 4d 42 40 00  ...Y.....SMB@
0040 00 00 00 00 00 00 00 00 01 00 01 00 00 00 00 00  .....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0070 00 00 00 00 00 00 00 00 00 00 41 00 01 00 02 02  .....A...
0080 00 00 19 9a fa e6 0f c5 c1 49 b7 6b e5 fb d1 c6  .....I.k....
0090 f1 12 01 00 00 00 00 00 01 00 00 00 01 00 00 00  .....X{/T...E.S
00a0 01 00 58 df 7b 2f 54 b4 cc 01 94 45 09 a6 53 b4  ....l L M `j...+
00b0 cc 01 80 00 6c 00 20 4c 4d 20 60 6a 06 06 2b 06  ....^0^..0...*
00c0 01 05 05 02 a0 60 30 5e a0 30 30 2e 06 09 2a 86  .....H...*H...
00d0 48 82 f7 12 01 02 02 06 09 2a 86 48 86 f7 12 01  H.....*H...
00e0 02 02 06 0a 2a 86 48 86 f7 12 01 02 02 03 06 0a  +....7...*0(&
00f0 2b 06 01 04 01 82 37 02 02 0a a3 2a 30 28 a0 26  $not de fined_in
0100 1b 24 6e 6f 74 5f 64 65 66 69 6e 65 64 5f 69 6e  _RFC4178 @please_
0110 5f 52 46 43 34 31 37 38 40 70 6c 65 61 73 65 5f  ignore
0120 69 67 6e 6f 72 65
    
```

Weak authentication



Encrypted Attack

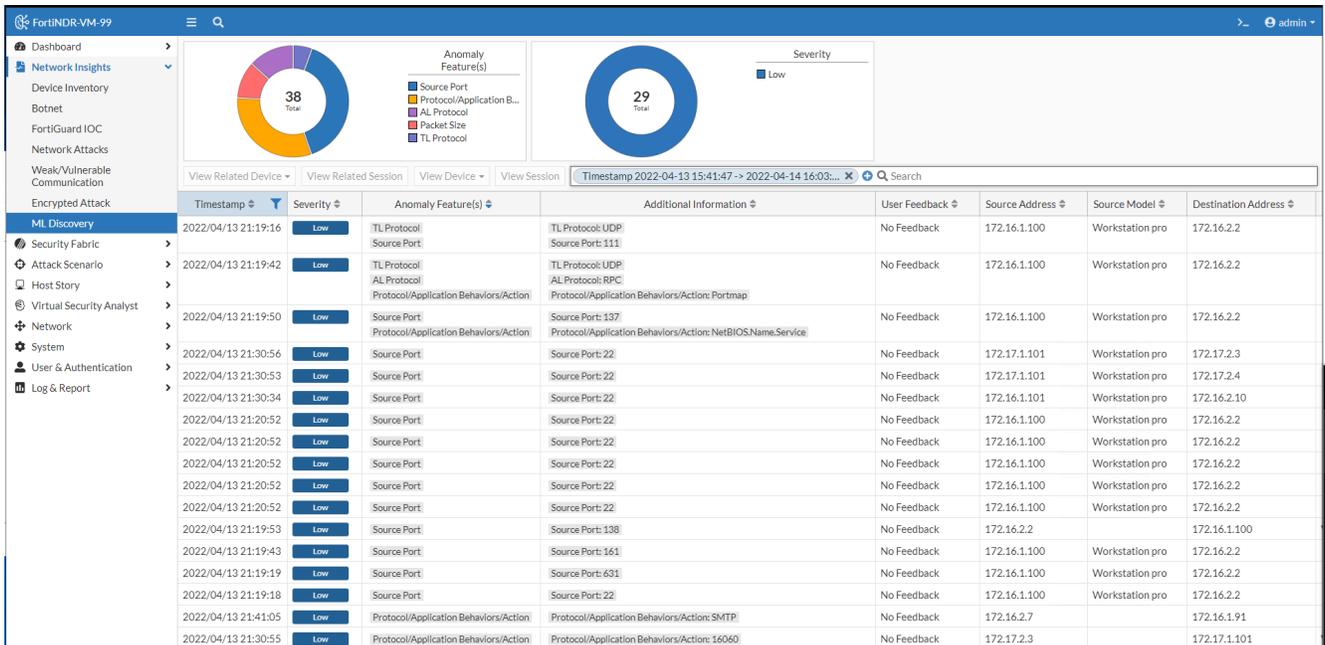
Encrypted attacks are detected by analyzing JA3 hashes in TLS transactions. FortiNDR will utilize both JA3 client and server SSL fingerprints in detection, resulting in fewer false positive detections.



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.

Session 109114
--Action-- Go Back



Activity
Network Service
Application
FTP
Vendor
Other

Low Anomaly

Session Information

Timestamp 2022/07/15 15:34:44
 Protocol FTP
 Volume 361 (361 bytes)
 Interface Client-Server
 Cloud Service None

Device Information

Internal

Device Type N/A
 Device Model N/A
 MAC Address 00:90:0b:31:24:09
 Vendor N/A
 OS N/A
 Role N/A
 IP 192.168.104.3
 Port 10684
 Packet Size 114

↔

Internal

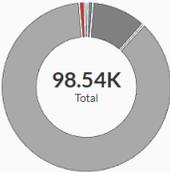
Device Type N/A
 Device Model N/A
 MAC Address 00:90:0b:47:26:cd
 Vendor N/A
 OS N/A
 Role N/A
 IP 192.168.104.4
 Port 21
 Packet Size 247

Activity

No Activity Found

ML Discovery

Application layer protocol and Destination Port and Behaviors



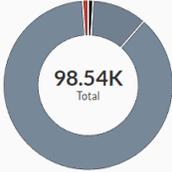
98.54K
Total

Application layer protocol and Destination Port and Behaviors/Action

- HTTP and 80 and YouTube
- Other and 80 and Other
- FTP and 21 and FTP
- SMTP and 20 and FTP
- FTP and 20 and FTP
- Other and -1024 and Ping
- SMTP and 20 and Other

FTP and 21 and FTP

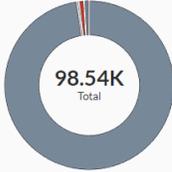
Application layer protocol



98.54K
Total

- HTTP 87,084
- Other 10,123
- FTP 729
- SMTP 606

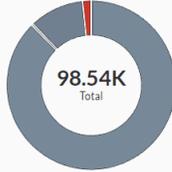
Destination Port



98.54K
Total

- 80 97,204
- 21 667
- 20 667
- 8 3

Protocol/Application Behaviors/Action



98.54K
Total

- YouTube 87,084
- Other 10,121
- FTP 1,333
- Ping 3

Detection Information

Date	Severity	Anomaly Type	Description
2022/07/15 15:39:43	Low	FortiNDR ML Discovery	Anomaly Found In Combination of Application Layer Protocol and Destination Port Number and Protocol or Application Behaviors or Action



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 a session

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

To add feedback to session anomaly:

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 Not Anomaly	Select this option to force the next baseline training with new traffic to EXCLUDE the same detection in future. This typically takes 5-10 minutes depending on the network traffic.
Mark as Anomaly	Select this option to add positive feedback to the detection. This does not affect the baseline training other than acting a place for you to comment on the detection.



When multiple sessions 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.

The screenshot shows the ML Discovery interface. At the top, there are two donut charts: one for 'Anomaly Feature(s)' with a total of 721, and another for 'Severity' with a total of 658. Below the charts is a table with columns: Timestamp, Severity, Anomaly Feature(s), Additional Information, User Feedback, Source Address, and Source Model. A session entry is highlighted with a yellow background, and a dropdown menu is open over the 'User Feedback' column, showing 'Mark as Not Anomaly' as the selected option. Below the dropdown are 'Apply' and 'Cancel' buttons.

4. Click *Apply*.

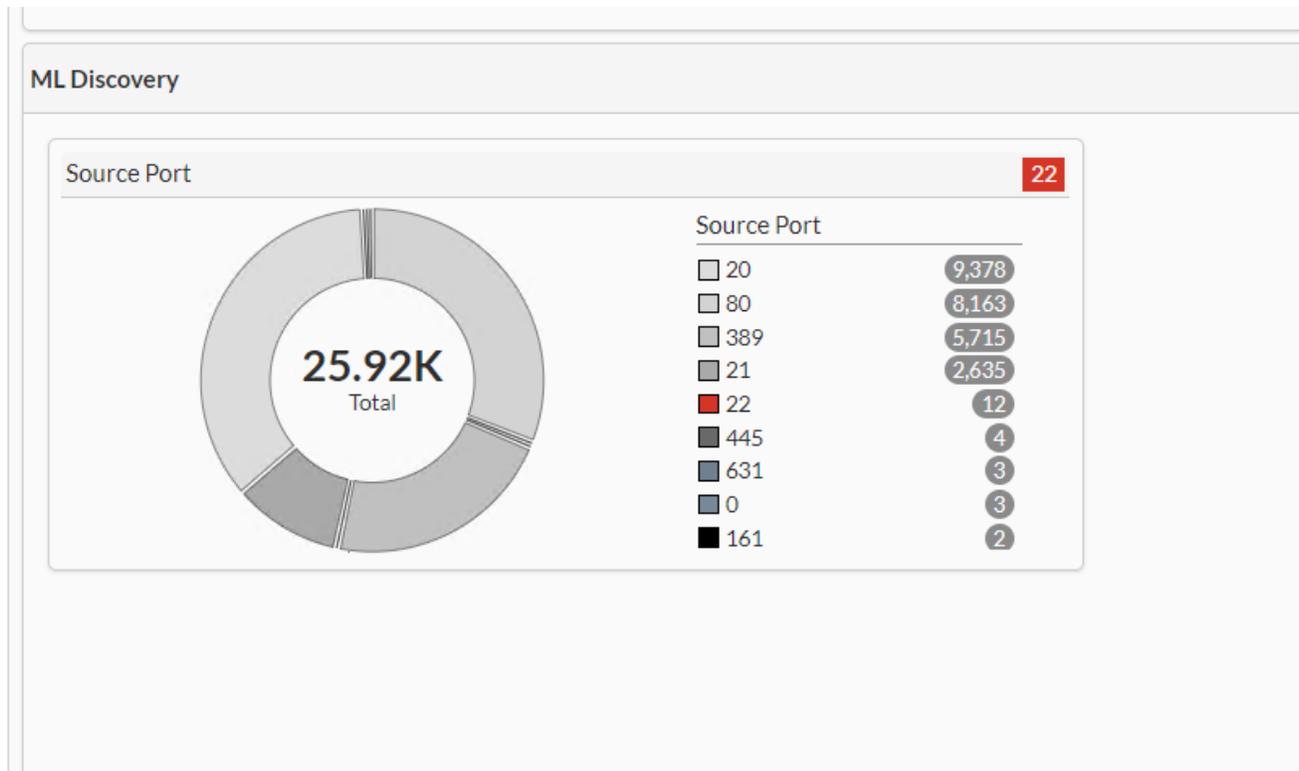
The following image is an example of multiple ML discoveries with the same value in the *Anomaly Feature(s)* column. In this scenario, you will only need to add feedback once to mark all the sessions as *Anomaly*.

Timestamp	Severity	Anomaly Feature(s)	Additional Information	User Feedback	Source Address	Source Model	Destination Address	Destination Model
2022/04/15 14:46:54	Low	AL Protocol Protocol/Application Behaviors/Action	AL Protocol: SSH Protocol/Application Behaviors/Action: SSH	Anomaly	172.16.2.8		172.16.1.101	Workstation pro
2022/04/15 14:46:54	Low	AL Protocol Protocol/Application Behaviors/Action	AL Protocol: SSH Protocol/Application Behaviors/Action: SSH	Anomaly	172.16.2.8		172.16.1.101	Workstation pro
2022/04/15 14:46:54	Low	AL Protocol Protocol/Application Behaviors/Action	AL Protocol: SSH Protocol/Application Behaviors/Action: SSH	Anomaly	172.16.2.8		172.16.1.101	Workstation pro
2022/04/15 14:47:39	Low	AL Protocol Protocol/Application Behaviors/Action	AL Protocol: SSH Protocol/Application Behaviors/Action: SSH	Anomaly	172.16.2.8		172.16.1.101	Workstation pro

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.

Session 663532 --Action-- Go Back

Activity
Network Service
Application
Portmap
Vendor
Other

Information

Session Information

Timestamp: 2022/04/13 21:14:20
 Protocol: RPC
 Volume: 252 (252 bytes)
 Interface: Network-Protocol
 Cloud Service: None

Device Information

vmware

Internal

Device Type: Virtual Machine
Device Model: Workstation pro
MAC Address: 00:50:56:8c:e0:e4
Vendor: VMware
OS: N/A
Role: Server
IP: 172.16.1.100
Port: 32788
Packet Size: 252

↔

Internal

Device Type: N/A
Device Model: N/A
MAC Address: 00:50:56:8c:17:f9
Vendor: N/A
OS: N/A
Role: N/A
IP: 172.16.2.2
Port: 111
Packet Size: 0

Activity

No Activity Found

TL Protocol and AL Protocol and Protocol/Application Behaviors/Action

14
Total

Anomaly Feature(s)

- TL Protocol: TCP and AL Prot...
- TL Protocol: TCP and AL Prot...
- TL Protocol: TCP and AL Prot...
- TL Protocol: UDP and AL Pro...
- TL Protocol: TCP and AL Prot...
- TL Protocol: TCP and AL Prot...
- TL Protocol: UDP and AL Pro...
- TL Protocol: UDP and AL Pro...
- TL Protocol: UDP and AL Pro...

TL Protocol UDP

AL Protocol RPC

33.68K
Total

AL Protocol

- HTTP: 30,765
- FTP: 2,711
- SMB: 64
- MSSQL: 42
- RPC: 37
- DNS: 27
- SMTP: 22
- IMAP: 7
- RDP: 6

Protocol/Application Behaviors/Action Portmap

218
Total

Protocol/Application Behaviors/Action

- NNTP: 59
- MSSQL: 41
- IBM.MQ: 34
- DNS: 28
- Portmap: 19
- Proxy-HTTP: 12
- MS.RPC: 9
- HPDataProtector: 6

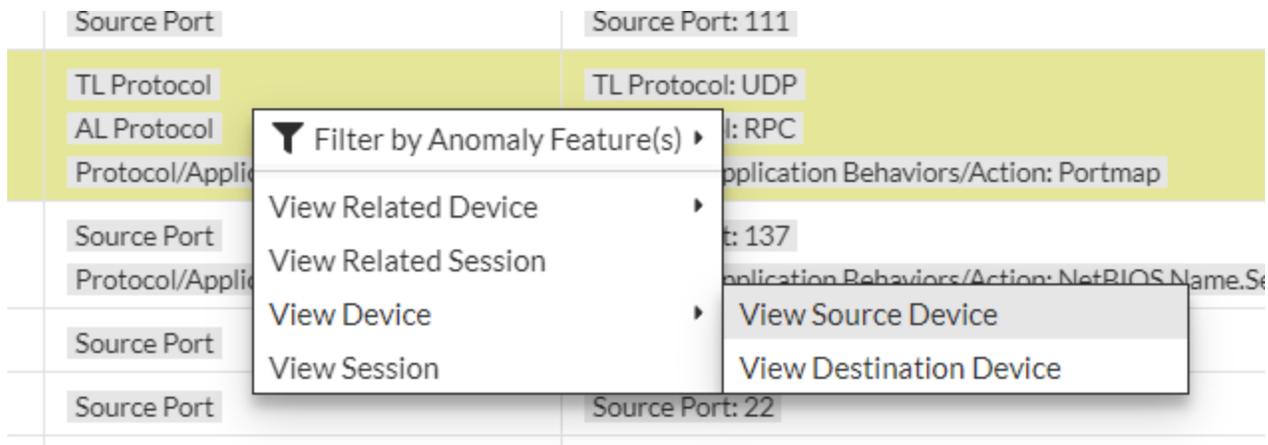
Detection Information

Search

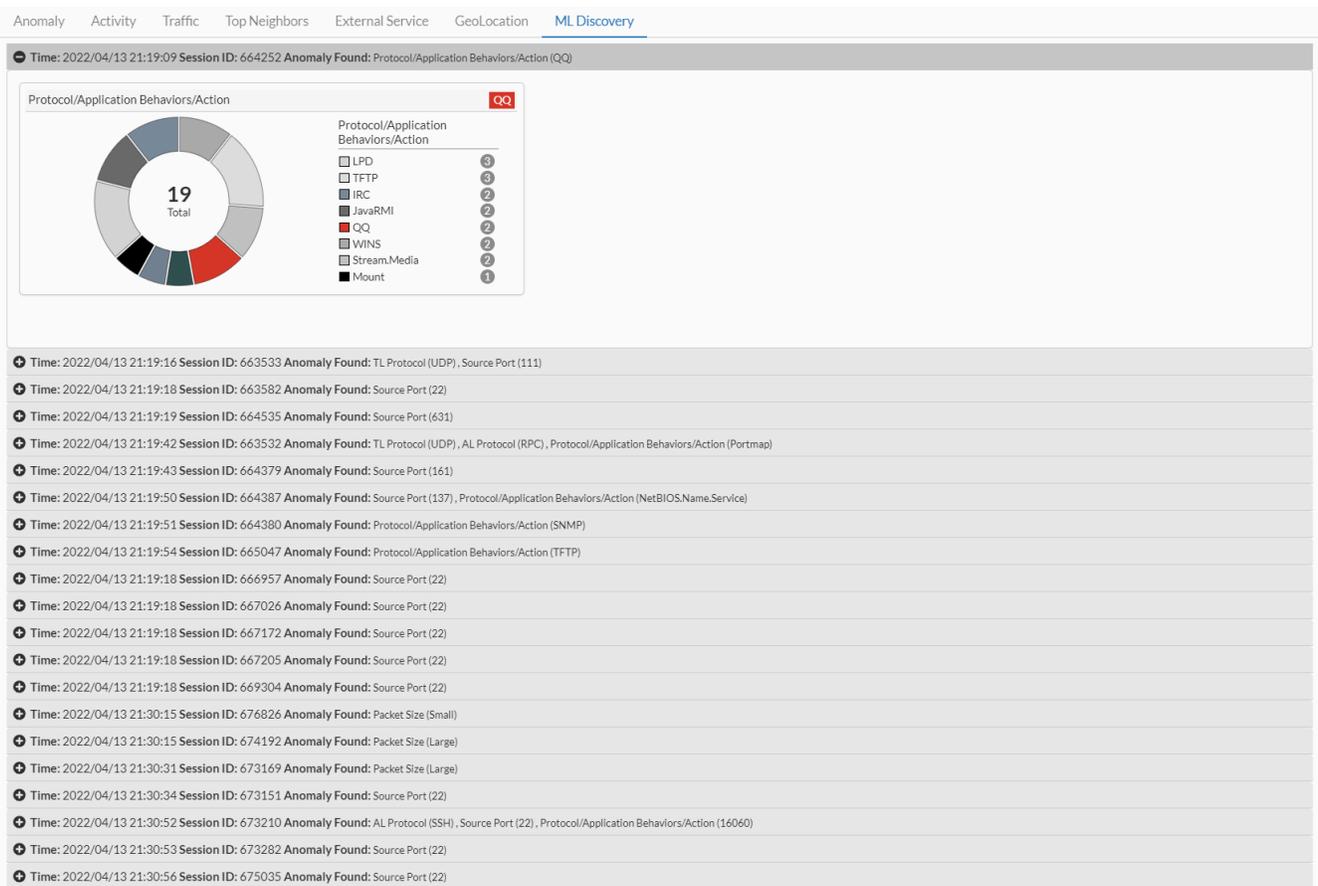
Date	Severity	Anomaly Type	Description
2022/04/13 21:19:42	Low	FortINDR ML Discovery	Anomaly Found In Combination of Transport Layer Protocol and Application layer protocol and Protocol or Application Behaviors or Action

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.



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.

Severity	Scenario	Incident Counts
Low	Phishing	196,200
	SEP	0
	Web Shell	343
	Application	43,300
	Cryptojacking	48,191
Medium	Generic Trojan	5,351,113
	DoS	252,354
	Scenario Heuristic	0
	Sophisticated	2
High	Rootkit	173
	Botnet	769,194
	Backdoor	41,693
	Banking Trojan	149,070
	Exploit	984
Critical	Data Leak	38,480
	Industroyer	1
	Wiper	1
	Fileless	14
	Worm Activity	218,623
	Ransomware	137,837

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.

The screenshot displays the FortiNDR-VM interface. At the top, a table lists various attack scenarios. The 'Worm Activity' scenario is selected, showing a detection on 2022/04/13 at 13:34:49 on host 10.10.10.23, identified as 'NSIS' malware family, detected by a 'Sniffer' device.

Below the table, the 'Attack Timeline at Host 10.10.10.56' is shown. It features three main stages:

- Downloader:** Shows the detection of 'JS/Agent.NOI' at 12:46:10. It lists associated files like 'HTML', 'Downloader', and 'Virus'. The attacker IP is 10.10.10.4 and the victim IP is 10.10.10.56.
- Infostealer:** Shows the detection of 'W32/Dloader.ADC!tr' at 12:46:10. It lists associated files like 'PE', 'Infostealer', and 'Ekstak'. The attacker IP is 10.10.10.4 and the victim IP is 10.10.10.56.
- Worm:** Shows the detection of 'W32/BundpILAA!tr' at 12:46:10. It lists associated files like 'PE', 'Worm', and 'Alien'. The attacker IP is 10.10.10.4 and the victim IP is 10.10.10.56.

 A tooltip for the 'W32/BundpILAA!tr' detection provides additional details: Discover Date (2022/04/13 12:46:10), MD5 (6a7edcca4a1154dde36d2e79d9224a08), Remote IP (10.10.10.4), and Protocol (SMB).



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.

Sample Information

Submitted Date	2022/04/13 12:46:10	Last Analyzed	2022/04/13 12:46:10
File Type	PE	File Size	3584(3.5 KB)
URL	42r13s/oadD4g/65B		
MD5	6A7EDCC4A411540DE36D2E7909224A08	vt	
SHA256	6A7EDCC4A411540DE36D2E7909224A08		
SHA1	11540DE36D2E7909224A08		
Detection Name	W32/Bundpil.AA!tr	Virus Family	Alien
Source Device			
Device Type	Sniffer		
Network			
Attacker	10.10.10.4:445 (Microsoft-DS)	Victim	10.10.10.56

Feature Composition

Feature Type	Appearance In Sample
Worm	18
Trojan	1

History MITRE ATT&CK

Technique ID	Tactic	Technique Name	Indicator	Severity
T1036	Defense Evasion	Masquerading	Drop files in system folder	High
T1036	Defense Evasion	Masquerading	Drop files in system folder	High
T1099	Defense Evasion	Timestomp	Modify ChangeTime timestamp	High
T1112	Defense Evasion	Modify Registry	Change Internet Settings	High
T1059	Execution	Command-Line Interface	Run the dropped file	High
T1112	Defense Evasion	Modify Registry	Change Internet Settings	High
T1099	Defense Evasion	Timestomp	Modify LastWriteTime timestamp	High

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.

IP Address	Critical Risk Incidents	High Risk Incidents	Medium Risk Incidents	Low Risk Incidents	Total Incidents
172.19.235.3	569	0	0	0	569
172.19.122.83	498	0	0	0	498
10.10.10.23	212	1,617	1,076	44	2,949
172.19.235.2	85	0	0	0	85
10.10.10.53	32	40	155	26	253
10.10.10.23	20	32	194	27	273
10.10.10.54	12	19	119	13	163
172.16.92.175	11	12	117	27	167
10.10.10.51	9	36	155	70	270
172.19.235.237	8	0	0	0	8
172.16.92.175	7	0	0	0	7
10.10.10.52	7	111	267	86	471
10.10.10.55	6	37	114	7	164
10.10.10.52	6	20	94	97	217
172.19.235.52	5	1	25	5	36
10.10.10.55	3	0	0	0	3
10.10.10.57	3	0	0	0	3
172.17.45.105	1	0	0	0	1
172.19.235.51	0	3	2	0	5
10.10.10.3	0	0	2	6	8
10.10.10.58	0	0	2	6	8

Virtual Security Analyst

This section includes the following topics.

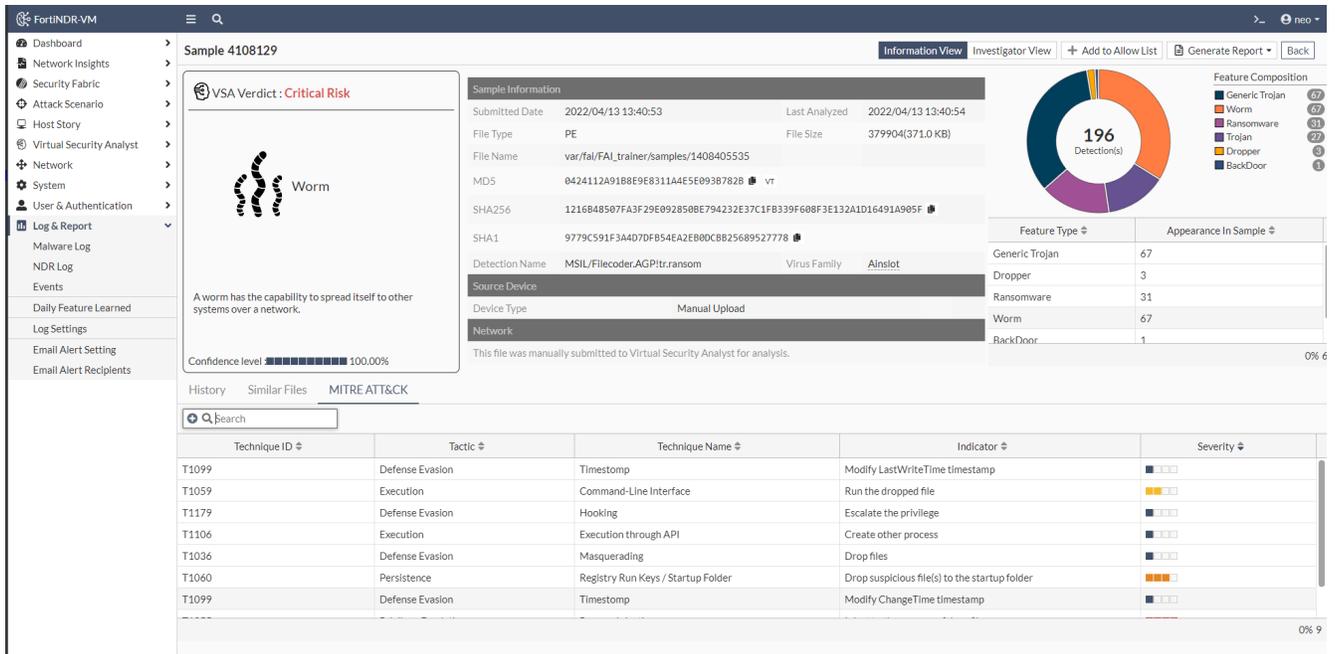
- [Express Malware Analysis on page 88](#)
- [Outbreak Search on page 91](#)
- [Static Filter on page 94](#)

Express Malware Analysis

Express Malware Analysis offers a fast solution to provide the verdict of the file. You can submit the files up to 200MB in default via GUI or via API (Use CLI: `execute file-size-threshold` to change file size limit). Submitted files enter a queue in the system for analysis. Use *Virtual Security Analyst > Express Malware Analysis* to check the status of your submitted files and the verdict.

Submission Time	Submitted Filename	Submission User	MD5	Verdict	Confidence	Risk	Status
2022/04/13 15:48:20	532B7A4B.vsc	neo	f1a33b2be4c6215a1c39b45e391a3e85	Wiper	Mid (80.0%)	Critical	Done
2022/04/13 15:48:02	53C5E72D.vsc	neo	3b94fdc5e66e0366ea3fe045413e27d3	Dropper	High (100.0%)	Medium	Done
2022/04/13 15:47:30	4E80818A.vsc	neo	be9d55368570f673194029c569ad0bf0	Clean	N/A (0%)	No Risk	Done
2022/04/13 15:47:10	4B6B4A6B.vsc	neo	6161b447846ed2f955816a70b46699b4	Clean	N/A (0%)	No Risk	Done
2022/04/13 15:46:48	5319FA87.vsc	neo	c58b7928560628518a124ed8c4b023e6	Clean	N/A (0%)	No Risk	Done
2022/04/13 13:40:53	1408405535.rar	neo_api		1/0/0	N/A (0%)	Pending	Done
2022/04/13 13:40:53	1404843999.rar	neo_api		0/0/1	N/A (0%)		Fail: Contains Unsupported File Type:
2022/04/13 13:40:53	1405769515.rar	neo_api		1/0/0	N/A (0%)	Pending	Done
2022/04/13 13:40:53	1402755243.rar	neo_api		1/0/0	N/A (0%)	Pending	Done
2022/04/13 13:40:53	1399962124.rar	neo_api		1/0/0	N/A (0%)	Pending	Done
2022/04/13 13:40:52	1398827132.rar	neo_api		1/0/0	N/A (0%)	Pending	Done
2022/04/13 13:40:52	1404843980.rar	neo_api		0/0/1	N/A (0%)		Fail: Contains Unsupported File Type:
2022/04/13 13:40:52	1408913881.rar	neo_api		1/0/0	N/A (0%)	Pending	Done

Click *View Sample Detail* to view its sample information. This page explains the verdict by showing the feature composition of the file. You can also find a list of related files with a similar score at the bottom of the page. To generate a report summary in PDF and JSON format, click *Generate Report* at the top right.



The VSA report has tabs at the bottom.

Tab	Description
History	Display 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 based analysis based on features detected. This is good for detecting similar variants of the original malware.
MITRE information (and Investigator view)	For PE (portable executable) files, FortiNDR can optionally display a drill down the MITRE ATT&CK matrix displaying the TTPs used for a particular malware.
IOC (Indicators of Compromise)	For text-based malware, FortiNDR can optionally display more contextual information of malware, such as <i>file contain abnormal javascript</i> , and so on. This helps users understand why FortiNDR determines it is malware.

When a zip file is uploaded, you can view the contents and verdict of the files in the zip file by double-clicking on the zip file entry.

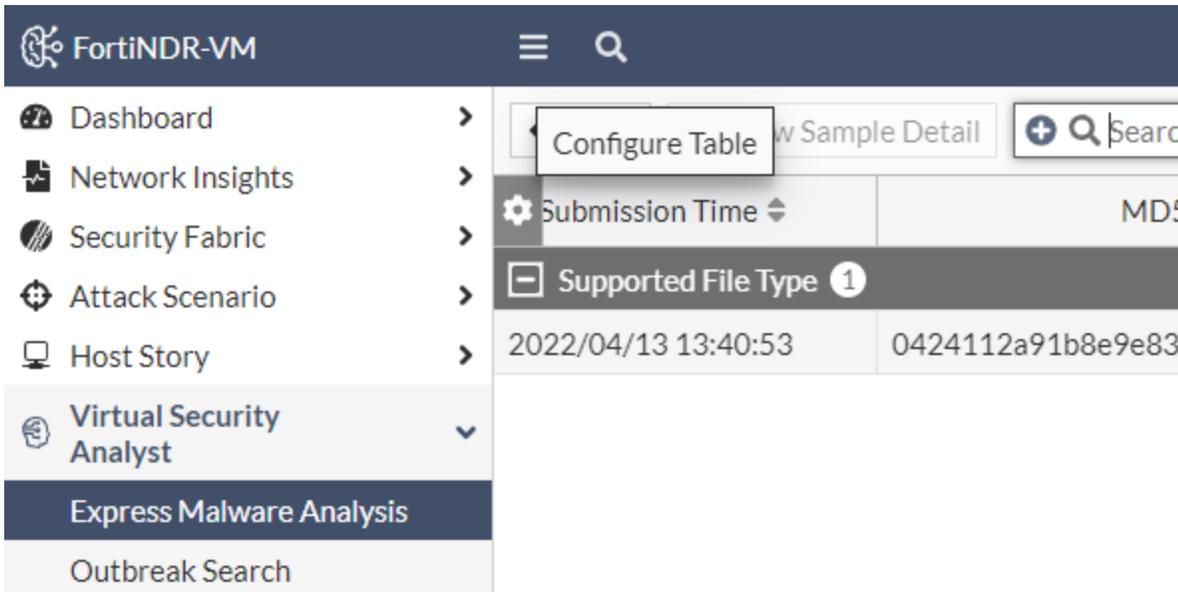
← Back to 525904.tar.gz (2020/05/31 17:13:28)

20 Items Generate Report ▾

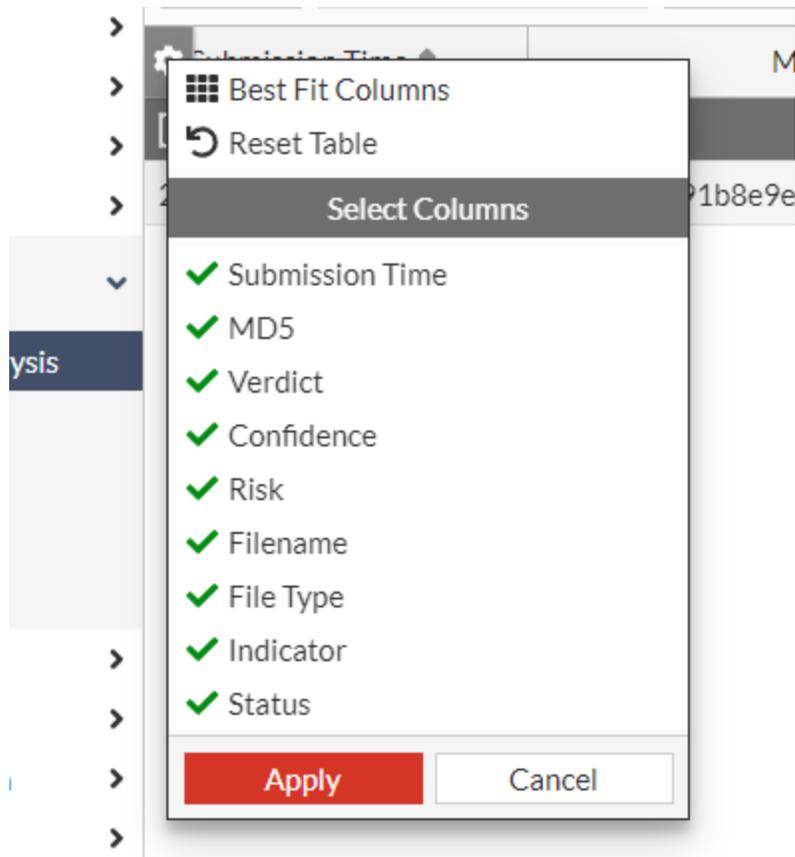
Submission Time	Filename	MDS	File Type	Verdict	Confidence Level	Risk Level	Status
Supported File Type (15)							
2020/05/31 17:13:30	40550136.vsc	a86a5fe18402c958b4365263fab2a12a	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3C559658.vsc	b6523dcd40e9c768a06ff46516fde4	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	38E9F1A6.vsc	ff578c64c31e7c9dac090a9c03136500	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	34869B3A.vsc	402bfd289434fd9e2850ea13dbdb6f87	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	42B0E080.vsc	63b3eac79ea8c3a033f5cb2cea2b1ccc	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	40B03FEF.vsc	af7a049fb21401b38ea7c3a9ba9674eb	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3BCECAE0.vsc	1beb2e23edc295ae214e762a478d300a	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3185FB8C.vsc	e143b75b35ded9fc369fec32015e98dd	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	337A1E91.vdf	716cb0c867206122532ed753826b6a6c	PDF	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	355C8BFC.vsc	1b129271e371d64bbe128014ccfc021b	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	317C51E0.vsc	7116dd303a1e70e0d3bb310ec383e036	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	3420A9B4.vxe	4e8ffc5e44e62ebbb123f810f36602f	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	3BB44181.vsc	add352ba1edf9b25dc1cf3b152d9fe45	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	38C07AA2.vsc	e10ff38099494e80189c0bc28eac4a68	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	31340098.vsc	9cf8b1e41b61a586002dfc5f46daedb	PE	Application	100%	Low Risk	Done
Unsupported File Type (5)							
2020/05/31 17:13:28	3AA1848D.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	409FC737.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3AA0CF20.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3AA0CDE.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3A109FD3.vsc			Generic Attack		Pending	Fail: Unsupported File Type

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.



Upload files using API

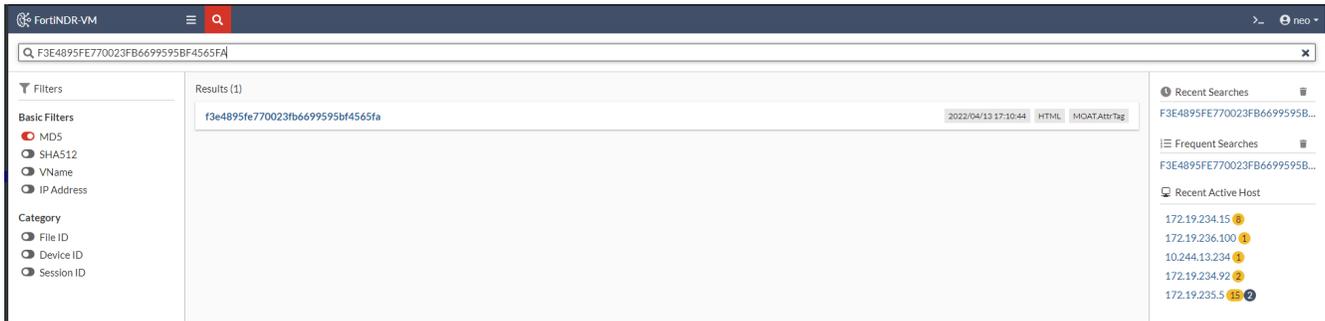
You can submit files for analysis using API with an API key. See [Submit files on page 152](#).

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 92](#).
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 93](#).

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.

Search Lead Type: Hash a8990d67ff31dd5a509d07e3c0f68a82 Similarity-Based Hash-Based Detection-Based

Related Files

Generate Report Search Found 583 related file(s) Search by Detection Name Search similar file(s) by Detection Name Search by OutBreak View Sample Detail

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	MDS	File Type	Detection Name	Risk Level	Confidence Level	Associated By
2020/06/14 11:16:20	b6523dcccdd40e9c768a06ff46516fde4	PE	Q W32/Virut.CE	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	402bFd289434f9e2850ea13dbdb6f87	PE	Q W32/WannaCryptor.D!tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	ff578c64c31e7c9dac090a9c03136500	PE	Q W32/WannaCryptor.D!tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	af7a049fb21401b38ea7c3a9ba9674eb	PE	Q W32/Virtu.F	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	a86a5fe18402c958b4365263fab2a12a	PE	Q W32/Virtu.F	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	1be2e23edc295ae214e762a478d300a	PE	Q W32/WannaCryptor.D!tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	e143b75b35ded9fc369fec32015e98dd	PE	Q W32/WannaAPNO!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	d2782bcce77d8c400331a102145eb51	PE	Q W32/Miner.V!l!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	808c71732f0089228fb082b07235620b	PE	Q W32/Miner.V!l!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	909421454e3e6da3efeed986f2d59e7e	PE	Q W32/Miner.V!l!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	4d7769db73272f0493014c3ee6ec2bdc	PE	Q W32/Miner.V!l!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	e11bf6f7ed035fd4e60c74784209f937	PE	Q W32/Miner.V!l!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	bc3d22a07660260b143d8fabbaed4fb	PE	Q W32/Miner.V!l!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	cd2d592622fa018b4718be73d5df6c87	PE	Q W32/Miner.V!l!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	4b1c089335318263117845448920cb95	PE	Q W32/Miner.V!l!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.

12b7fb78d1d55f53a93ba3770a1145cd	HTML	Downloader
145f7949922cf6e9b4ecaceb7793671c	HTML	Downloader
87d4cf49d40952de2184d833094af93c	HTML	Downloader
174ab067179f7fbb897d	HTML	Downloader
30128bed2b5a99b96f62	HTML	Downloader
9b35ac3cc4df067a94ef	HTML	Downloader
c8d49aa6403204e5f0d115e6eae34042	HTML	Downloader
82b9d6425ad17bfe3c7f65770e8af133	HTML	Downloader
4ef008e313a49ab941520464d0aa1349	HTML	Downloader
573b6aaa60f8a997868879a80f635617	HTML	Downloader
20f75fd78fa9ff62fe5ae2894d3d6923	HTML	Downloader

- Search by Hash
- Search similar file(s) by Hash
- Search by OutBreak
- View Sample Detail

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: <i>FortiGate, Workstation, IDRAC, etc.</i>
Destination Device Geolocation	Device geographical country such as <i>United States.</i>
Destination Device Category	Device category such as: <i>NAS, Virtual Machine, Firewall, etc.</i>
Destination Device Vendor	Device vendor such as <i>VMware, Dell, Synology, etc.</i>
Destination Device OS	Device Operating system such as <i>Windows, Linux, etc.</i>
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. <i>Adobe Reader form creation, WebDAV reload, Wasabi file upload, etc</i>
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: <ul style="list-style-type: none"> • Small: Less than 100 bytes

Others

- 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.

ML Configuration

Baseline Status ● Baseline Ready

ML Discovery Detection Enable Disable

Latest Training Completion 2022/07/18 00:59:56

i 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

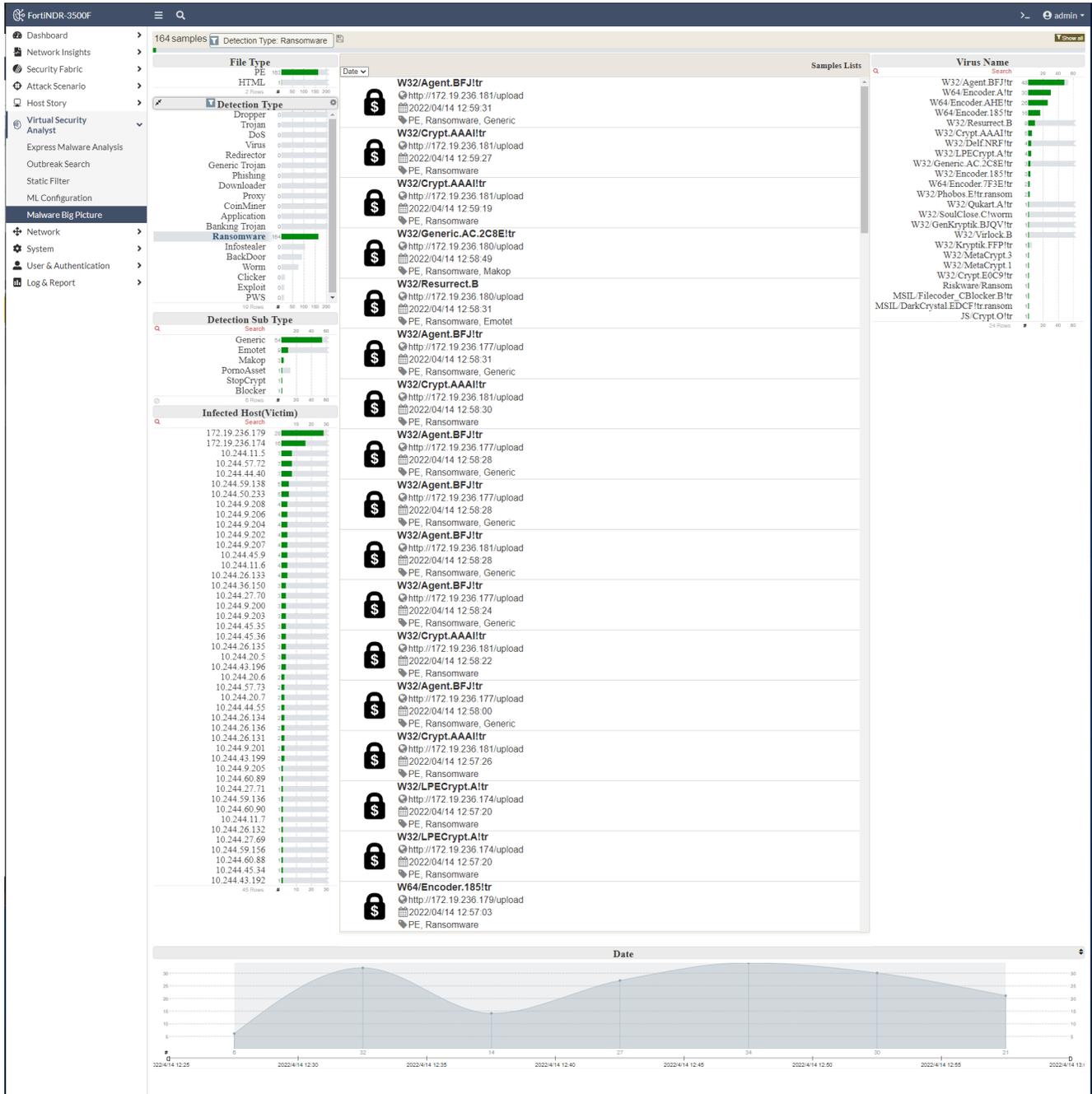
Others

- Source session packet size
- Destination port
- TLS version
- Source port

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.



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).



Only Super Admin users can access the CLI using SSH. For more information, see [Administrator and Admin Profiles on page 100](#).

DNS and Static Routes

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

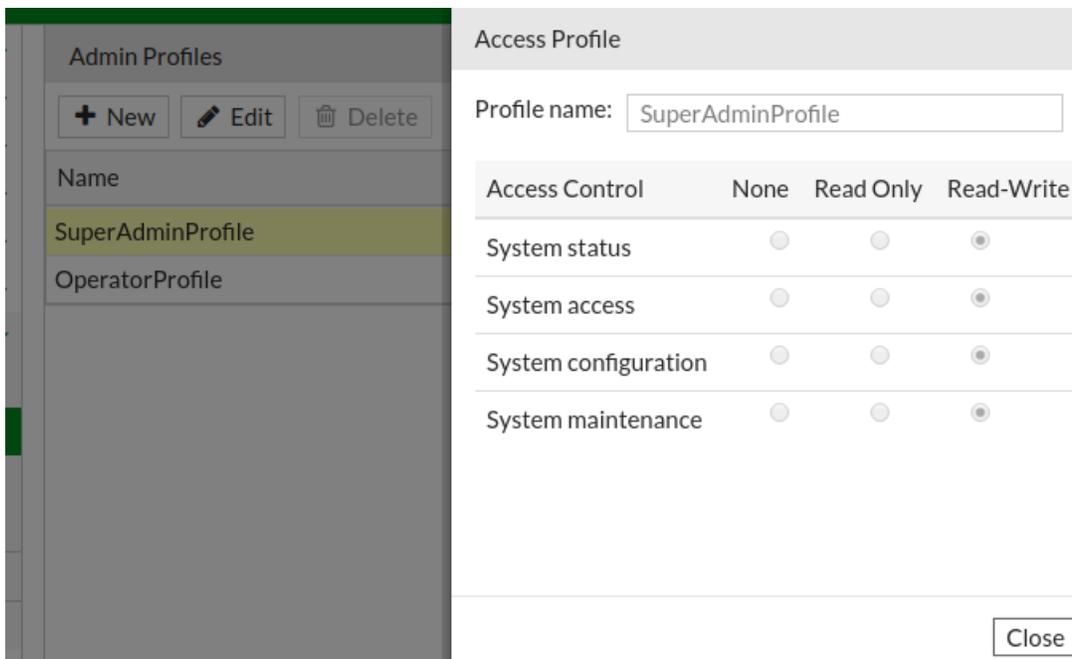
System

Use the *System* options to configure system settings.

Administrator and Admin Profiles

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

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



Access Profile

Profile name:

Access Control	None	Read Only	Read-Write
System status	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
System access	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
System configuration	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
System maintenance	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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

System Time

Current System Time 2022/09/23 14:34:21

Time Zone

Set Time NTP Setting Time Manually

Select server FortiGuard Custom

Sync Interval Minutes (1-1440)

Administration Setting

Idle Timeout Minutes

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 <i>NTP</i> or select <i>Setting Time Manually</i> and then enter the <i>Date</i> and <i>Time</i> .
Select Server	Select <i>FortiGuard</i> or select <i>Custom</i> to add or remover the <i>Server</i> .

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 165](#). To view a list of updates, go to *System > FortiGuard*.

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

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

Please refer to [Appendix D - FortiGuard Updates on page 165](#) and [CLI guide](#) for more detail.

Entitlement	Status
FortiCare Support	Registered
Firmware & General Updates	Licenses - expires on 2023/03/10 Firmware Upgrade
NDR Service	Valid - expires on 2023/01/09
	Error Occurred During Updating
Text AI Feature DB	Version 1.087 Up to Date
Text AI Group DB	Version 1.087 Up to Date
Binary AI Feature DB	Version 1.096 Up to Date
Binary AI Group DB	Version 1.096 Up to Date
Scenario AI DB	Version 1.087 Up to Date
Text AI Learning Feature DB	Version 1.087 Up to Date
Binary AI Learning Feature DB	Version 1.096 Up to Date
Binary Behavior DB	Version 1.096 Up to Date
AVEng Active DB	Version 90.01403 Update Available
AVEng Extended DB	Version 90.01332 Up to Date
AVEng Extreme DB	Version 90.01363 Up to Date
AVEng AI DB	Version 2.02671 Update Available
Application Control DB	Version 20.00295 Up to Date
Industrial Security DB	Version 20.00295 Up to Date
Network Intrusion Protection DB	Version 20.00299 Up to Date
Traffic Analysis DB	Version 20.00001 Up to Date

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>.

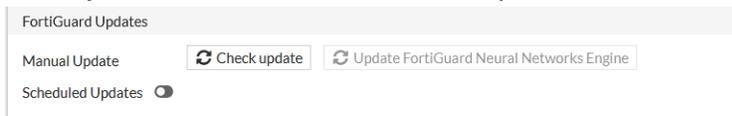


Currently, FortiNDR retrieves ANN updates from US and EMEA FortiGuard servers. FortiNDR selects the update server based on proximity and location.

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 kdb. Run this command once for `pae_kdb.tar.gz` and once for `moat_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*.

FortiGuard Updates

Manual Update

Scheduled Updates Hours

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.

High Availability (HA)

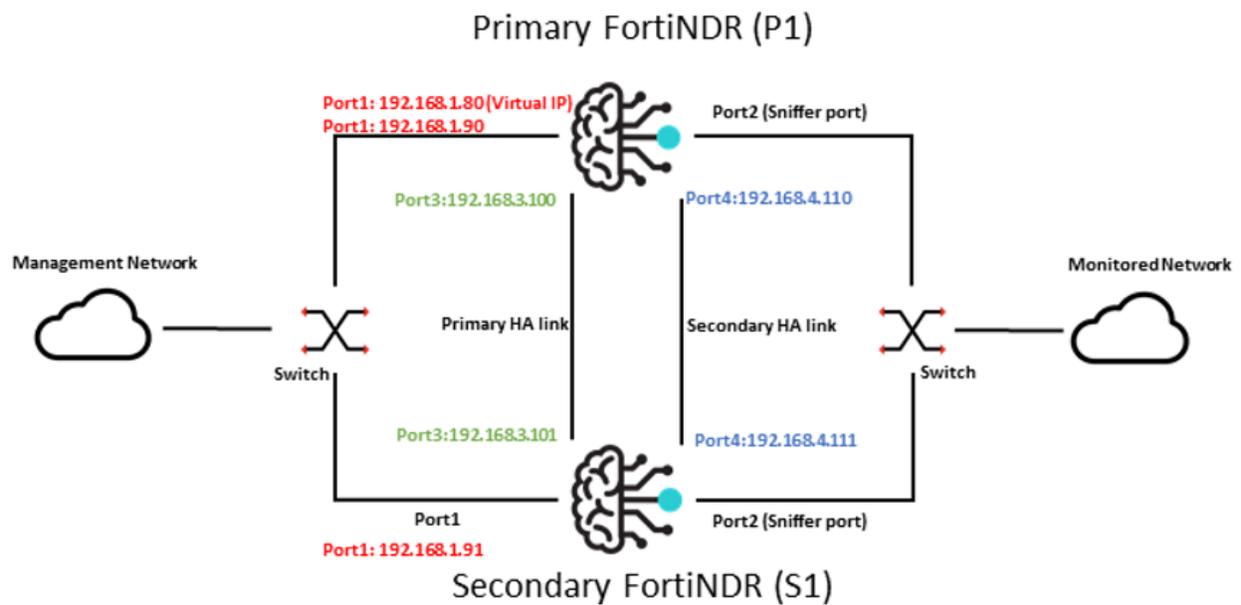
FortiNDR HA supports active-passive mode, in both hardware and virtual machines, which consists of two FortiNDR units in the HA group: the primary unit and the secondary unit. The primary unit will act as the active unit performing malware detection and verdict, as well as synchronize configurations and data to the secondary unit. The secondary unit will perform these functions if the primary unit fails.

HA setup requirements

Before configuring the HA group, the two FortiNDR units must meet the following requirements:

- Both units must have the same firmware version.
- Both FortiNDR units should have the default management interface port1 be accessible. Port1 will be used for HA configuration and checking HA status. Port1 management IPs for both units will be different, please see the example in [Configuring an HA group on page 106](#).
- We recommend using Port3 and Port4 for HA heartbeat and synchronization. The heartbeat interfaces between the two units should be connected directly or through a dedicated switch and have IP addresses in the same subnet. While two heartbeat interfaces are recommended for fail-safe, one heartbeat link can also be used.

The following image is an example of active-passive HA topology:



Configuring an HA group

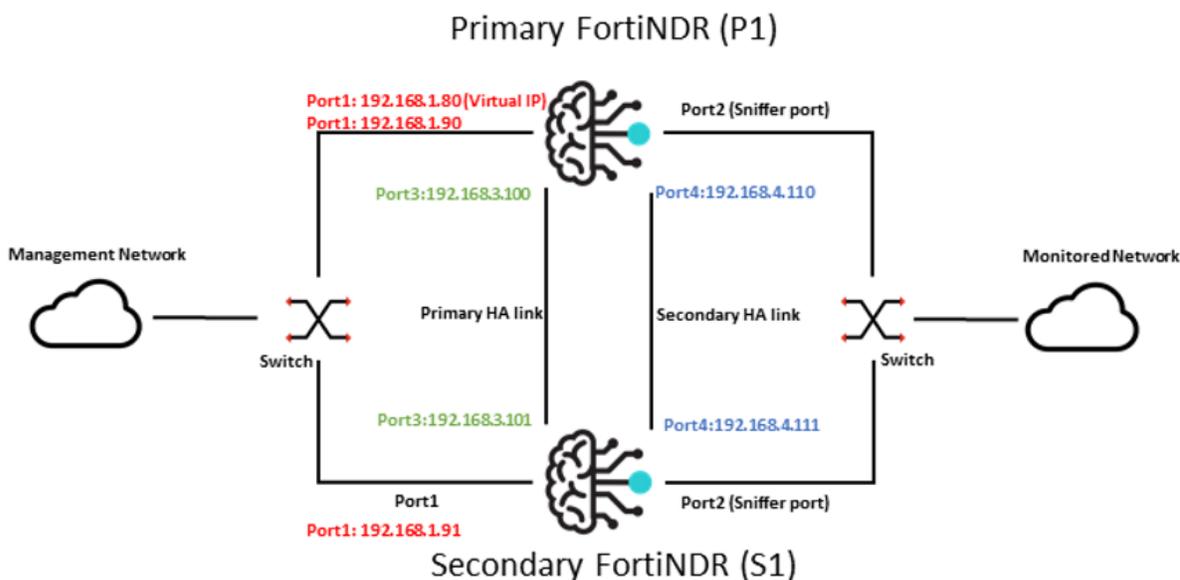
Before configuring an HA group, we recommend performing a factory reset or restoring the database on both FortiNDR primary and secondary units.



If your FortiNDR unit is running, you can join a secondary unit to form the HA. However, you should allow more time to synchronize larger databases.

To configure an HA group:

1. Make all the necessary connections and network settings configuration. Individual interface settings for both units can be configured from the *Network* page or with the CLI.
The following image shows an example network settings configuration:



- Load the latest ANN database on both FortiNDR units. The ANN database can be updated from FDS (see, [Updating the ANN database from FDS for malware detection on page 14](#)) or with the CLI (see, [Loading the ANN database to FortiNDR for malware detection on page 10](#)).



- The ANN database is not synchronized.
- The ANN scheduled update settings are not synchronized. You will need to configure both units to ensure the latest ANN is used after failover.

- On the primary unit, use the CLI to configure the HA for the network topology (see the example above):

```

config system ha
  set mode primary
  set password xxx
  config interface
    edit port1
      set virtual-ip 192.168.1.80/24
      set action-on-primary use-vip
      set port-monitor enable
    end
    edit port3
      set heartbeat-status primary
      set peer-ip 192.168.3.101          << IP of secondary unit's port3
  end
interface
  end
  edit port4
    set heartbeat-status secondary
    set peer-ip 192.168.4.111        << IP of secondary unit's port4 interface
  end
end
end

```

CLI option	Description
mode	Enables or disables HA, selects the initial configured role: <ul style="list-style-type: none"> • Off: disable HA. • Primary: configured as primary Unit. • Secondary: configured as secondary Unit.
password	Enter an HA password for the HA group. You must configure the same password value on both the primary and secondary units.
heartbeat-status	Specify if this interface will be used for HA heartbeat and synchronization: <ul style="list-style-type: none"> • Disable: The interface is not used for HA heartbeat and synchronization. • Primary: We recommend to using port3 as the primary HA interface. • Secondary: We recommend having a secondary HA interface to improve availability. Use port4 as the secondary HA interface.
peer-ip	When configuring primary HA interfaces: <ul style="list-style-type: none"> • When configuring the primary unit, enter the IP address of the secondary unit's primary HA interface. • When configuring the secondary unit, enter the IP address of the primary unit's primary HA interface. The same rule should be applied when configuring the secondary HA interface.
virtual-ip	Enter the virtual IP address and netmask for this interface. If configured, this virtual IP can serve as the external IP of the HA group. When failover occurs, this setting will take effect on the new Primary unit. For details, see Using Virtual IP on page 113 .
action-on-primary	ignore-vip [Default]: Ignore the Virtual IP interface configuration on the new Primary unit after failover. use-vip: Add the specified Virtual IP address and netmask to the interface on the new Primary unit after failover.
port-monitor	Enable to monitor a network interface for failure on the Primary unit. If the interface failure is detected, the Primary unit will trigger a failover. This does not apply to heartbeat interfaces.

4. On the Secondary unit, configure the HA using the same CLI configuration except for the `ha mode` and `peer-ip` settings for the HA interface.

```

config system ha
  set mode secondary
  set password xxx    << password should be same as primary unit
  config interface
    edit port1
      << HA configuration for port1 should be same
as primary unit
      set virtual-ip 192.168.1.80/24
      set action-on-primary use-vip
      set port-monitor enable

```

```

end
edit port3
    set heartbeat-status primary
    set peer-ip 192.168.3.100    << IP of primary unit's port3 interface
end
edit port4
    set heartbeat-status secondary
    set peer-ip 192.168.4.110    << IP of primary unit's port4 interface
end
end
end

```

5. Check the HA status of both units.

- Ensure the HA effective mode on both units has been updated successfully.
- Check the HA status details. See, [Check HA status on page 109](#).
- Ensure no errors appear on the HA event log. See, [HA Logs on page 113](#).

After the HA group is configured:

- The heartbeat check between the primary and secondary units will be done through the HA port. The default heartbeat check is 30 seconds. This is configurable via the CLI.
- Configuration changes will be synced from the primary unit to the secondary unit. See [HA configuration settings synchronization on page 112](#).
- Data (Database and sample files) will be synced from the primary unit to the secondary unit.



The database on the primary unit is large. Database synchronization may take a while.

Check HA status

After HA is enabled, the HA status needs to be checked on both the Primary and Secondary units. Once HA has been configured, the effective operating mode is typically the same as the configured mode. However, the effective operating mode may diverge from the configured mode after HA failover is triggered.

HA Configured Mode	Displays the HA mode that you configured <ul style="list-style-type: none"> • <i>Primary</i>: Configured to be the primary unit. • <i>Secondary</i>: Configured to be the secondary unit.
HA Effective Mode	Displays the current operating mode <ul style="list-style-type: none"> • <i>Primary</i>: Acting as primary unit • <i>Secondary</i>: Acting as secondary unit • <i>Failed</i>: Occurs when network interface monitoring has detected a failure, failover is triggered afterward.

To check HA status with the CLI:

```
get system status
```

```
# get system status
Version: FortiAI-VM v1.5.2,build120,211029 (Beta) (Debug)
Architecture: 64-bit
Serial-Number:
BIOS version: n/a
Log disk: Capacity 48 GB, Used 71 MB (0.15%), Free 48 GB
Data disk: Capacity 926 GB, Used 434 GB (46.88%), Free 492 GB
Remote disk: n/a
Memory: Capacity 31 GB, Used 27 GB (88.83%), Free 3590 MB
Swap Memory: Capacity 31 GB, Used 12 GB (37.95%), Free 19 GB
Hostname:
HA configured mode: Primary
HA effective mode: Primary
```

To check the HA status with the GUI:

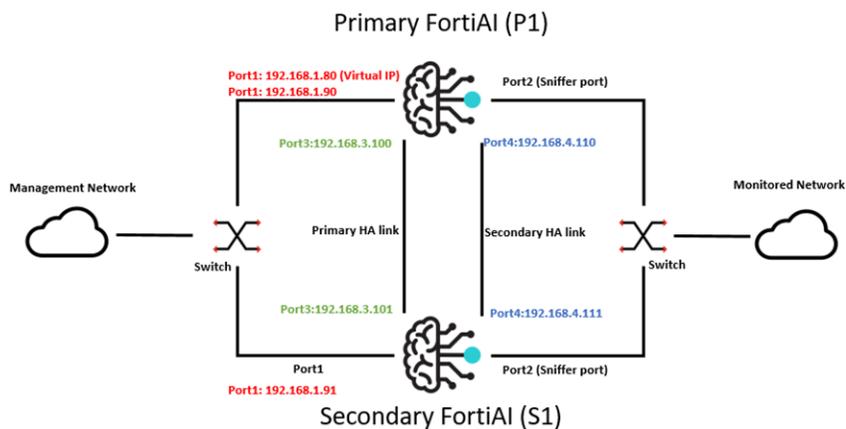
1. Go to *Dashboard* > *System Status* > *Network*.
2. In the *System Information* widget, go to *HA Status*.

The screenshot shows the FortiAI VM GUI. The left sidebar has a menu with 'Network' selected. The main content area displays the 'System Information' widget. At the bottom of this widget, the 'HA Status' is shown as 'Configured: Primary, Effective: Primary', which is highlighted with a red box.

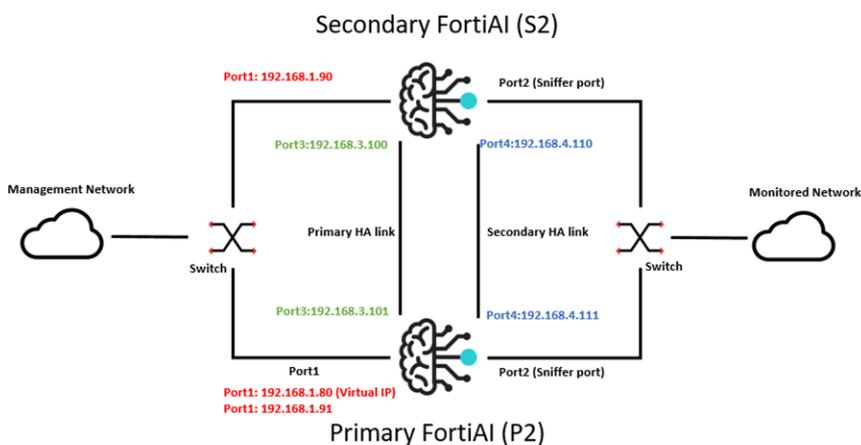
HA Failover

When an HA Failover occurs, the primary and secondary units switch roles.

Network topology before failover:



Network topology after failover:



Failover scenario 1: Temporary failure of the primary unit

Temporary failure of the Primary unit when the primary unit's:

- System is down due to a sudden loss of power.
- Monitored port link has failed.

When any of the two scenarios above occurs on the primary unit:

- The FortiNDR HA group is operating normally. *P1* is the primary unit and *S2* is the secondary unit.
- *P1* runs into failure which could be a sudden loss of power, or the monitored port link has been detected as failed.
- The effective HA operating mode of *S2* changes to *primary*.
- When the monitored port link fails, the effective HA operating mode of *P1* changes to *fail*.
- The effective HA operating mode of *P1* changes to *secondary* when the system is back or the monitored port link is up again.



The failover time in this scenario will depend on the heartbeat settings.

Failover scenario 2: System reboot or reload of the primary unit

System reboot or reload of the primary unit occurs when you trigger a system reboot or reload on the primary FortiNDR:

1. *P1* will send a `HOLDOFF` command to *S2* so that *S2* will not take over the primary role during *P1*'s reboot/reload.
 2. *S2* will hold off checking the heartbeat with *P1*.
-



S2 will only hold off for about 15 minutes. This is not configurable.

3. If *P1* reboot/reloads successfully within 15 minutes, *P1* will stay in primary mode and *S2* will go back to secondary from hold off.
4. Otherwise, *S2* will take over the primary role, and *P1* will change to secondary role when it is back.

Failover scenario 3: Heartbeat links fail

This occurs when the primary heartbeat link fails, and no secondary heartbeat link is configured or secondary heartbeat failed as well:

- The FortiNDR HA group is operating normally. Then the heartbeat link fails between the Primary unit and Secondary unit.
- The effective HA mode of *S2* changes to *primary*. At this time both units are acting as Primary units.
- When the heartbeat link is reconnected, one of the units will be picked to switch back to Secondary unit, while the other will stay as Primary unit.

Trigger HA failover using CLI

You can also trigger and HA failover by running the CLI on the primary unit:

- The FortiNDR HA group is operating normally. Then on the primary unit, run the failover testing CLI:
`execute ha test-failover.`
- The effective HA mode of the secondary unit changes to primary. The effective HA mode of the primary unit changes to secondary. The secondary unit will act as primary and take over operation.
- If you want to restore the effective mode to be same as the configured mode, run the failover testing CLI again on the new primary unit.

HA configuration settings synchronization

All configuration settings on the primary unit are synchronized to the secondary unit once the HA group has been configured successfully, with the excepting the following settings:

Configuration Settings	Description
HA Settings	HA related configurations
Network Settings	System network settings including: <ul style="list-style-type: none"> • System interface settings • System DNS settings • System Route settings
Host name	The host name distinguishes members of the HA group.
Default certificates	The default certificates.
FortiGuard update settings	The FortiGuard update settings are not synchronized. To keep up-to-date with the latest ANN database on the Secondary unit, you will need to manually trigger the update or enable scheduled updates on Secondary unit.
System Appearance	The appearance settings such as web GUI theme.

HA Logs

To view the HA event logs go to *Log & Report > Events*.



Once the HA group has been configured, the log data will be synchronized from the Primary unit to the Secondary unit.

System		Date/Time	Level	User	User Action	Message
Dashboard	>	a minute ago	Notification	ha	none	hahbd: heartbeat: change in status 'primary-heartbeat-port3=OK;secondary-heartbeat-port4=OK'
Security Fabric	>	a minute ago	Notification	ha	none	hahbd: peer heartbeat appeared, signalling our role
Attack Scenario	>	a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: heart beat status changed to OK
Host Story	>	a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: initialising, peer responded, changing to SECONDARY mode
Virtual Security Analyst	>	a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: peer heartbeat appeared, signalling our configured role
Network	>	a minute ago	Notification	ha	none	hahbd: heart beat status changed to OK
System	>	a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: starting
User & Device	>	a minute ago	Notification	ha	none	hahbd: heartbeat: change in status 'primary-heartbeat-port3=FAILED;secondary-heartbeat-port4=FAILED'
Log & Report	>	2 minutes ago	Notification	ha	none	hahbd: heart beat status changed to primary-heartbeat-port3=FAILED;secondary-heartbeat-port4=FAILED
Threat Report	>	2 minutes ago	Notification	ha	none	
Events	>	2 minutes ago	Notification	ha	none	
Daily Feature Learned	>	2 minutes ago	Notification	ha	none	

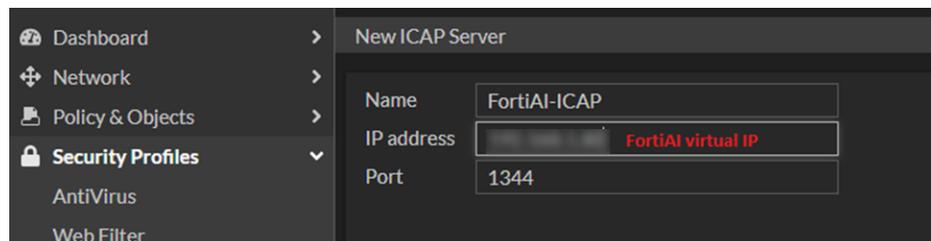
Using Virtual IP

Virtual IP serves as the external IP of the HA group used by other services in order to improve the handling of a single FortiNDR unit failure. When failover occurs, the new primary unit will replace that IP.

To use Virtual IP, you will need to configure and enable both the primary and secondary units with the same Virtual IP and netmask. To see an example of configuring a Virtual IP on interface port1, see [Configuring an HA group on page 106](#).

Example: Configure FortiGate ICAP server with FortiNDR virtual IP

Instead of using the actual IP, you will need to provide the Virtual IP of the HA group when creating an ICAP server profile on FortiGate. For detailed ICAP configuration information, see [FortiNDR and FortiGate ICAP configuration example on page 41](#).

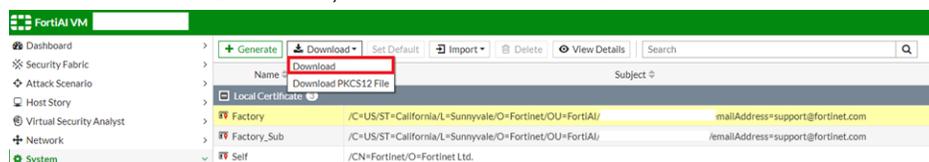


Example: Configure FortiGate Security fabric settings for inline blocking

FortiGate inline blocking requires FortiGate and FortiNDR Security Fabric pairing using the Security Fabric Connector. In order to allow a new primary unit pairing with FortiGate, both the certificate of the two FortiNDR units need to be added to the *Device authorization* list beforehand.

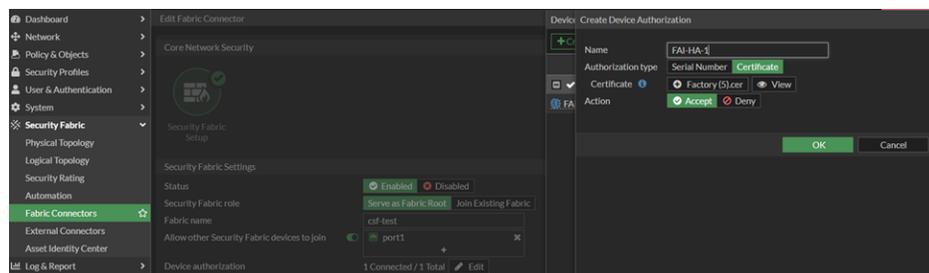
To configure FortiGate for inline blocking:

1. On the FortiNDR go to *System > Certificate*.
2. Under *Local Certificate*, select *Factory*.
3. In the toolbar click *Download*, to download the certificate.



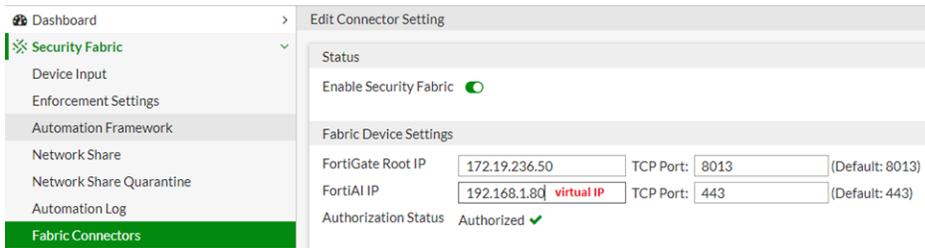
To add the certificate to FortiGate

1. On the FortiGate, go to *Security Fabric > Fabric Connectors*, and double-click *Security Fabric Setup*.
2. Double-click *Edit* in *Device authorization* and click *Create new*.



To enable FortiGate inline blocking:

1. On the Primary FortiNDR, go to *Security Fabric > Fabric Connectors*.
2. In the *FortiNDR IP* field, enter the Virtual IP.



The screenshot shows the 'Edit Connector Setting' page in the FortiNDR web interface. The left sidebar is expanded to 'Fabric Connectors'. The main content area shows the following settings:

Status	
Enable Security Fabric	<input checked="" type="checkbox"/>

Fabric Device Settings	
FortiGate Root IP	172.19.236.50 TCP Port: 8013 (Default: 8013)
FortiAI IP	192.168.1.80 virtual IP TCP Port: 443 (Default: 443)
Authorization Status	Authorized ✓



You are not required to configure inline blocking on the secondary unit since the configuration will be synchronized.

For detailed information about inline blocking configuration, see [FortiGate inline blocking \(FOS 7.0.1 and higher\)](#) on page 25.

User & Device

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.

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.

Date	MD5	File Type	Detection Name	Device Type	VDOM	Attacker	Victim
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76

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

The screenshot shows a 'Details' window for a security log entry. At the top right, the user 'admin' is logged in. Below the title bar is a search bar with the text 'View Detail Report'. The main content is organized into sections: 'General', 'Detection', 'Network', and 'Device'. The 'General' section lists File ID (181465), Time (2022/04/13 21:16:16), File Size (26.9 KB), File Type (MSOFFICE), and MD5 (2050C2A53E266DBC6FE72559548D5FC6). The 'Detection' section lists Virus Name (RTF/CVE_2014_1761.D!exploit), Confidence Level (100.00%), Threat Risk Level (High Risk), and Detection Type (Exploit). The 'Network' section lists Attacker IP (172.16.1.100: 8080), Victim IP (172.16.2.2: 53169), and URL (http://192.168.1.168/msf.rtf). The 'Device' section lists Device (Sniffer).

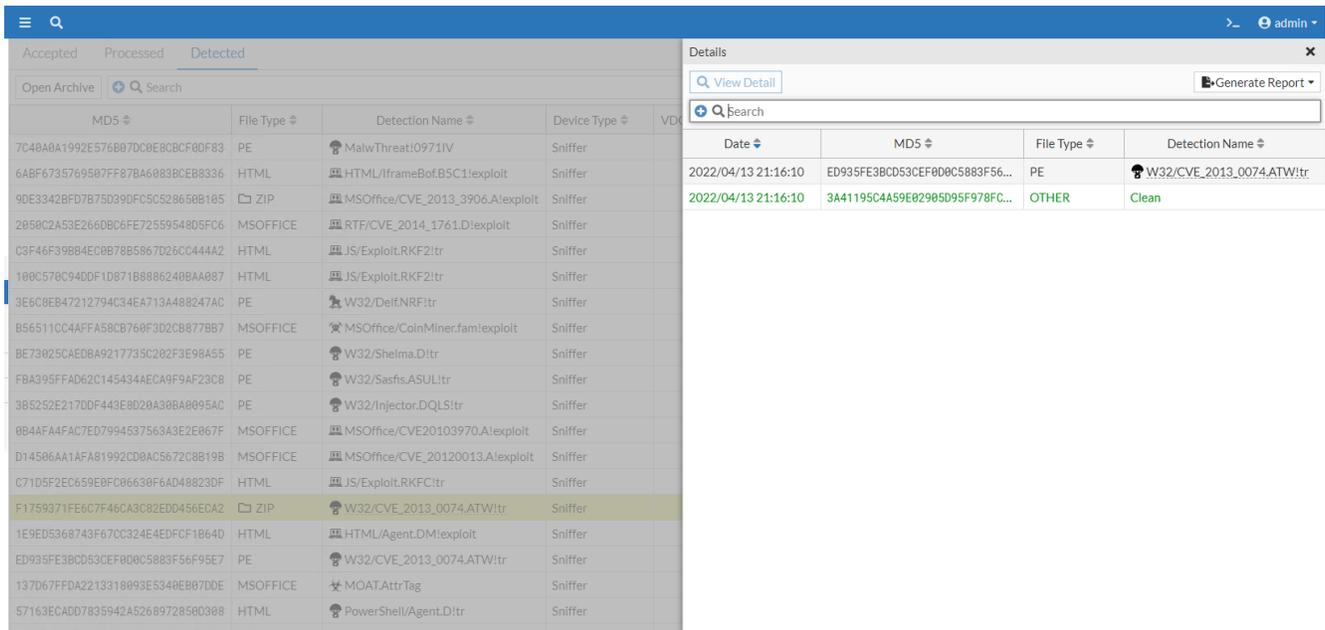
General	
File ID	181465
Time	2022/04/13 21:16:16
File Size	26.9 KB
File Type	MSOFFICE
MD5	2050C2A53E266DBC6FE72559548D5FC6

Detection	
Virus Name	RTF/CVE_2014_1761.D!exploit
Confidence Level	100.00 %
Threat Risk Level	High Risk
Detection Type	Exploit

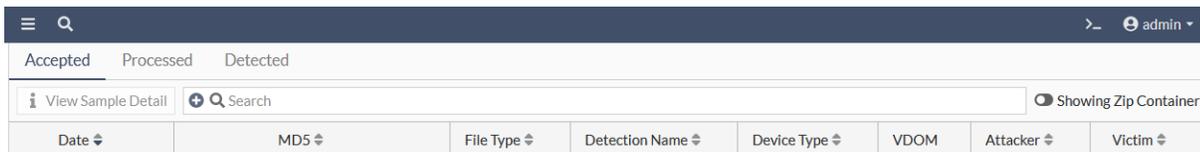
Network	
Attacker IP	172.16.1.100: 8080
Victim IP	172.16.2.2: 53169
URL	http://192.168.1.168/msf.rtf

Device	
Device	Sniffer

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

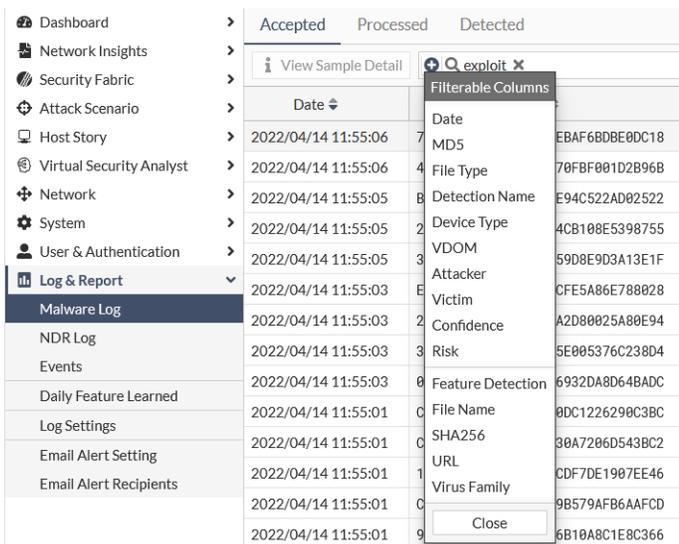


Enable *Showing Zip Container* to view the extracted files in the page.

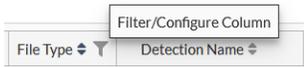


Advanced search

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.

FortiNDR-3500F									
Anomaly Session Device									
View Related Device View Related Session View Device View Session Search									
Timestamp	Session ID	Anomaly Type	Source Address	Destination Address	Severity	Protocol	Info		
2022/04/18 16:20:58	16982726	Network Attack/Intrusion	172.17.254.151	172.19.236.17	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:20:44	16982496	Network Attack/Intrusion	8.8.8.8	172.19.234.151	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:12:14	16977037	Network Attack/Intrusion	172.19.235.36	172.19.235.71	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:12:14	16977037	Network Attack/Intrusion	172.19.235.36	172.19.235.71	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:10:54	16976033	Network Attack/Intrusion	172.19.235.35	172.19.235.71	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:10:54	16976033	Network Attack/Intrusion	172.19.235.35	172.19.235.71	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:10:44	16975877	Network Attack/Intrusion	172.19.236.11	172.17.254.151	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:10:43	16975862	Network Attack/Intrusion	172.19.236.19	172.17.254.151	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:09:57	16975299	Network Attack/Intrusion	8.8.8.8	172.19.234.34	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:09:57	16975298	Network Attack/Intrusion	8.8.8.8	172.19.234.39	Low	UDP	'DNS PTR Records Scan		
2022/04/18 16:07:33	16973930	Network Attack/Intrusion	172.19.235.251	172.19.235.230	Critical	TCP	'Rshd Windows Server S		
2022/04/18 16:05:30	16972693	Weak Cipher/Vulnerable Protocol	172.19.235.50	172.19.235.53	High	TCP	Weak cipher of TLS Prot		
2022/04/18 16:04:59	16972402	Network Attack/Intrusion	172.19.235.35	172.19.235.71	Low	UDP	'DNS PTR Records Scan		

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.

The screenshot shows the FortiNDR 3500F interface. On the left is a navigation menu with 'Log & Report' selected. The main area shows the 'Anomaly' tab with a table of anomalies. A filter dropdown menu is open over the 'Anomaly Type' column, showing a search bar and a list of anomaly types with counts.

Timestamp	Session ID	Anomaly Type
2022/01/08 18:37:29	1672	Abnormal Network Behavior
2022/01/08 18:37:31	1818	Abnormal Network Behavior
2022/01/08 18:39:15	8650	Abnormal Network Behavior
2022/01/08 18:39:27	10226	Abnormal Network Behavior
2022/01/08 18:39:42	11119	Abnormal Network Behavior
2022/01/08 18:40:55	16442	Abnormal Network Behavior
2022/01/08 18:45:01	21655	Abnormal Network Behavior
2022/01/08 18:45:35	21968	Abnormal Network Behavior
2022/01/08 18:45:35	21958	Abnormal Network Behavior
2022/01/08 18:45:35	21962	Abnormal Network Behavior
2022/01/08 18:45:54	22308	Abnormal Network Behavior
2022/01/08 18:46:49	23502	Abnormal Network Behavior
2022/01/08 18:46:44	23454	Abnormal Network Behavior

The filter dropdown menu shows the following options:

- Exact Match
- value1, value2, etc.
- Abnormal Network Behavior (888)
- IPS Attack/ Intrusion (112)
- None (0)
- Botnet Interactions (0)
- Encrypted Attacks (0)
- IOC Campaign (0)
- Wear Cipher/ Vulnerable Protocol (0)
- Abnormal Network Activity (0)
- FortiAI ML Discovery (0)

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.

The screenshot shows the 'Session' tab in the FortiNDR interface. It features a table with columns for session details and a filter icon over the 'Open Time' column.

Open Time	Session ID	Source Address	Destination Address	Severity
2022/03/10 13:57:28	98211	10.0.0.17	10.0.0.18	Not Anomaly
2022/03/10 13:57:28	98210	10.0.0.17	10.0.0.18	Not Anomaly
2022/03/10 13:57:28	98209	10.0.0.17	10.0.0.18	Not Anomaly
2022/03/10 13:57:28	98208	10.0.0.17	10.0.0.18	Not Anomaly

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

Session 98210

Activity
Web Client

Application
HTTPBROWSER

Vendor
Other

Not Anomaly

Session Information

Timestamp 2022/03/10 13:57:28

Protocol HTTP

Volume 10.85K (10851 bytes)

Interface Browser-Based

Cloud Service None

View Related Anomaly by the Same Destination Device

View Related Session by the Same Source Device

View Related Session by the Same Destination Device

View Related Anomaly by the Same Source Device

View Related Anomaly by the Same Destination Device

Go Back

Device Information

Device Type Phone

Device Model N/A

MAC Address 02:dc:71:be:62:a1

Vendor Apple

OS iOS

Role Mobile

IP 10.0.0.17

Port 27888

Packet Size 394

↔

Device Type Phone

Device Model N/A

MAC Address 02:b8:94:27:ab:09

Vendor Apple

OS iOS

Role Mobile

IP 10.0.0.18

Port 80

Packet Size 10457

Activity

1 hour ago Connected to 10.0.0.18/index_10000bytes.html via HTTP

Detection Information

+ Q Search

Date	Severity	Anomaly Type	Description
------	----------	--------------	-------------

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.

Anomaly Session Device							
View Device Detail + Q Search							
Last Seen	Discovery Time	Device	MAC Address	Latest Address	Role	Status	Confidence
2022/04/18 16:30:48	2022/04/13 17:02:19	UNKNOWN_0E321BDF	00:50:56:62:ad:0c	192.168.101.62	Network Firewall	Online	N/A (0)%
2022/04/18 16:30:48	2022/04/13 17:02:19	UNKNOWN_48654F8B	00:50:56:62:3e:a1	192.168.101.62	Network Firewall	Online	N/A (0)%

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.

Device 7 Malware Host Story

Information

FORTIOS_27753EAC Update host name

Confidence Level ██████████ 255/255

Host IP: 172.19.122.111 Mac Address: 04:d5:90:fd:0b:d3 Discovery Date: 4/13/22 17:02:17 Operating System: FortiOS

Network-Firewall

7.44G
6.51G
5.98G
4.65G
3.72G
2.79G
1.86G
930.58M

12:00 15:00 18:00 21:00 00:00 03:00 06:00 09:00

Critical Risk Anomaly: 2 Medium Risk Anomaly: 1.54K
High Risk Anomaly: 383 Low Risk Anomaly: 27

13-Apr-2022 14-Apr-2022

Anomaly Event Intensity Graph

N/A Top Application Other Top Service HTTP Top Protocol 172.19.235.2 Top Neighbor N/A Top Geolocation

Search

Date	Severity	Anomaly Type	Description
2022/04/14 11:12:21	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 11:04:00	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 11:03:46	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 10:58:57	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 10:53:16	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 10:52:54	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 10:52:23	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 10:49:55	Low	Network attack	'DNS PTR Records Scan' detected
2022/04/14 10:49:52	High	Network attack	'Malicious Shellcode Detection' detected
2022/04/14 10:45:04	Low	Network attack	'DNS PTR Records Scan' detected
2022/04/14 10:40:41	High	Weak cipher	Weak cipher of TLS Protocol detected
2022/04/14 10:38:30	High	Weak cipher	Weak cipher of TLS Protocol detected

0% 1,955 Updated: 11:34:12

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

Device 50 Malware Host Story

Information

Risk Level

45,739 Total

Scenario Type

45,739 Total

Discovery Date	Scenario Type	Malware Family	Device Type	Risk Level	Attack Chain
2022/04/13 17:01:47	Generic Trojan	General	Sniffer	Medium	PE/Virus/General
2022/04/13 17:02:12	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:12	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:12	Generic Trojan	General	Sniffer	Medium	PE/Trojan/General
2022/04/13 17:02:12	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:12	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:12	Generic Trojan	General	Sniffer	Medium	PE/Trojan/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Trojan/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Virus/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Trojan/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Virus/General
2022/04/13 17:02:14	Generic Trojan	General	Sniffer	Medium	PE/Dropper/General

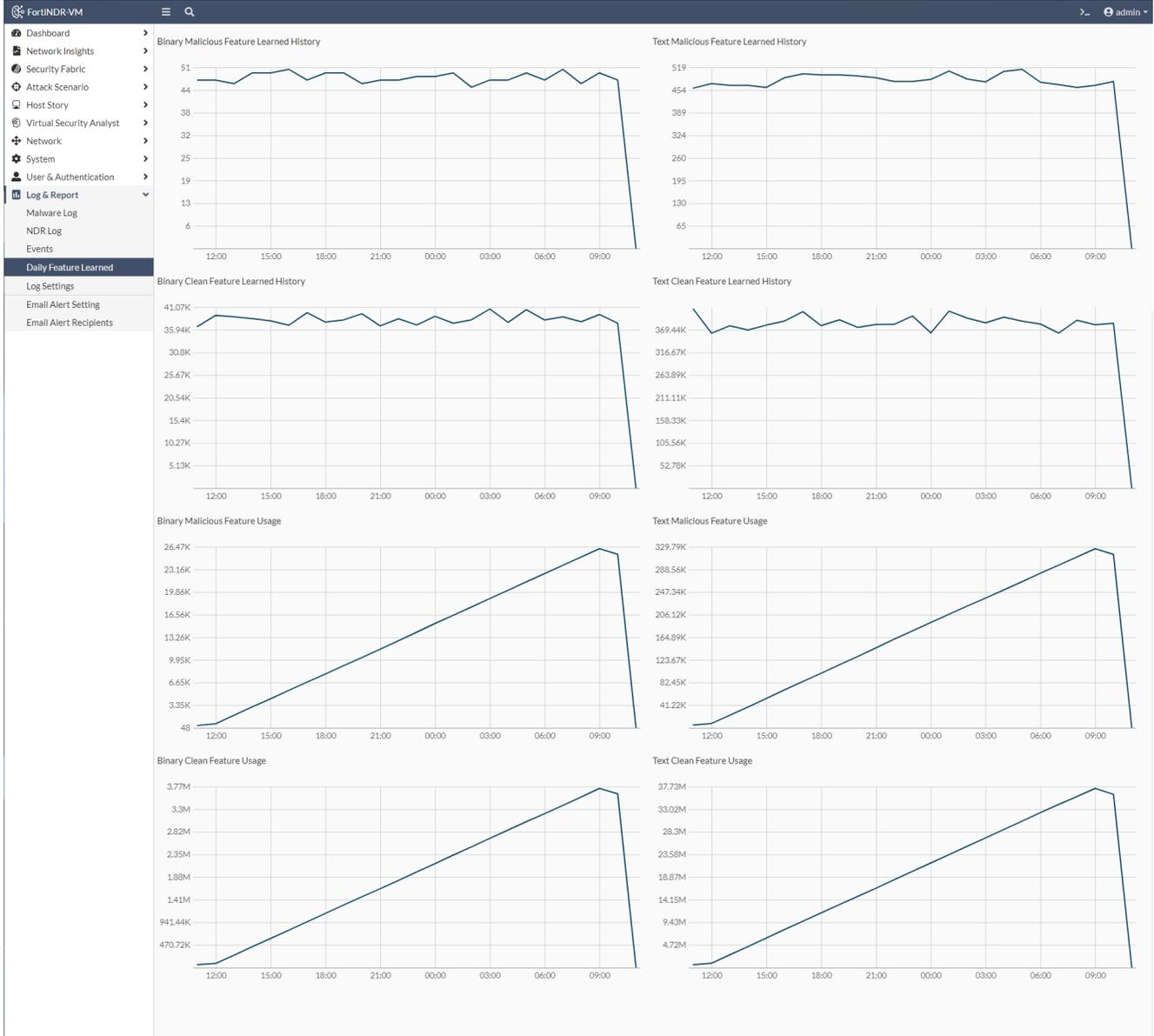
Events

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

FortiNDR-3500F					
	Date	Level	User	Message	
Dashboard	5 minutes ago	Information	system	cpu (usage 85%) is very high; memory (usage 29%); log disk (usage 0%); data disk (usage 7%); system l...	
Network Insights	5 minutes ago	Information	admin	User admin login successfully from ssh(172.19.122.245)	
Security Fabric	13 minutes ago	Information	dbdaemon	dbdaemon: sending Request Failed. try fix it with 'diag system db' in cli	
Attack Scenario	15 minutes ago	Information	dbdaemon	dbdaemon: sending Request Failed. try fix it with 'diag system db' in cli	
Host Story	15 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.220)	
Virtual Security Analyst	18 minutes ago	Information	system	cpu (usage 95%) is very high; memory (usage 30%); log disk (usage 0%); data disk (usage 7%); system l...	
Network	23 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.207)	
System	27 minutes ago	Information	system	Session check failure for user (172.19.122.220)	
User & Authentication	27 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.220)	
Log & Report	27 minutes ago	Information	admin	User admin login failed from GUI(172.19.122.220)	
Malware Log	33 minutes ago	Information	system	cpu (usage 88%) is very high; memory (usage 29%); log disk (usage 0%); data disk (usage 7%); system l...	
NDR Log	33 minutes ago	Information	dbdaemon	dbdaemon: sending Request Failed. try fix it with 'diag system db' in cli	
Events	33 minutes ago	Information	admin	User admin login successfully from GUI(172.19.122.209)	
Daily Feature Learned	33 minutes ago	Information	system	Session check failure for user (172.19.122.209)	
Log Settings	33 minutes ago	Information	admin	User admin login failed from GUI(172.19.122.209)	
Email Alert Setting	1 hour ago	Information	system	file upload request from 172.19.122.233	
Email Alert Recipients	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.

The screenshot displays the 'Log Settings' page for a FortiNDR-3500F device. The left sidebar contains a navigation menu with 'Log & Report' expanded, showing options like Malware Log, NDR Log, Events, Daily Feature Learned, Log Settings (selected), Email Alert Setting, and Email Alert Recipients. The main content area is titled 'Log Settings' and contains two 'Remote Log Server' configuration sections.

Remote Log Server (Top):

- Send logs to FortiAnalyzer/FortiSIEM: Enable Disable
- Type: Syslog Protocol
- Log Server Address:
- Port: (Default UDP: 514)

Remote Log Server (Bottom):

- Send logs to Syslog Server 1: Enable Disable
- Type: Syslog Protocol
- Log Server Address:
- Port: (Default UDP: 514)

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 <code>xxxx-xx-xx</code>
time	The time the log was sent in the format <code>hh:mm:ss</code>
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

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 SMTP 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 <i>Trigger Sensitivity</i> where required.

Alert Email Setting

Server Setting

SMTP Server Address

Port

Sender's Email Account

Service Login Account

Service Login Password

Using Openssl Enable Disable

Trigger Setting

- Generic system information including high cpu / low memory etc
- (VM Only) license expired
- HA related events
- Scenario Detection Events
- NDR: Botnet Anomaly
- NDR: Encrypted Attack
- NDR: IOC Events
- NDR: IPS attack
- NDR: Weak cipher
- NDR: Suspicious Activity
- NDR: Events based on Machine Learning

3. Click *OK*.
4. Add email addresses to the email recipient list. See, [Email Alert Recipients on page 132](#).

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 from the list.

Troubleshooting

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`

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

To turn network traffic detection on and off:

Run the following command:

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



802.1Q encapsulation for VLAN is not supported in network traffic detection.

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:

Date	MDS	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk	Indicator
2022/04/14 11:55:06	1B7C22A21494997555662607217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	N/A (0%)	No Risk	
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A21494997555662607217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A21494997555662607217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A21494997555662607217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78	N/A (0%)	No Risk	
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A21494997555662607217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	N/A (0%)	No Risk	

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

Open Time	Session ID	Source Address	Destination Address	Severity
2022/04/14 13:51:01	5597328	172.19.235.76	172.19.235.2	Not Anomaly
2022/04/14 13:51:01	5597320	10.244.57.73	10.244.43.192	Not Anomaly
2022/04/14 13:51:01	5597312	172.19.235.76	172.19.235.2	Not Anomaly
2022/04/14 13:51:01	5597304	172.19.235.76	172.19.235.2	Not Anomaly
2022/04/14 13:51:01	5597296	172.19.235.76	172.19.235.2	Not Anomaly
2022/04/14 13:51:01	5597288	172.19.235.76	172.19.235.2	Not Anomaly
2022/04/14 13:51:01	5597280	192.168.101.63	192.168.101.61	Not Anomaly
2022/04/14 13:51:01	5597272	172.19.235.78	172.19.235.2	Not Anomaly

Sniffer diagnosis

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

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.



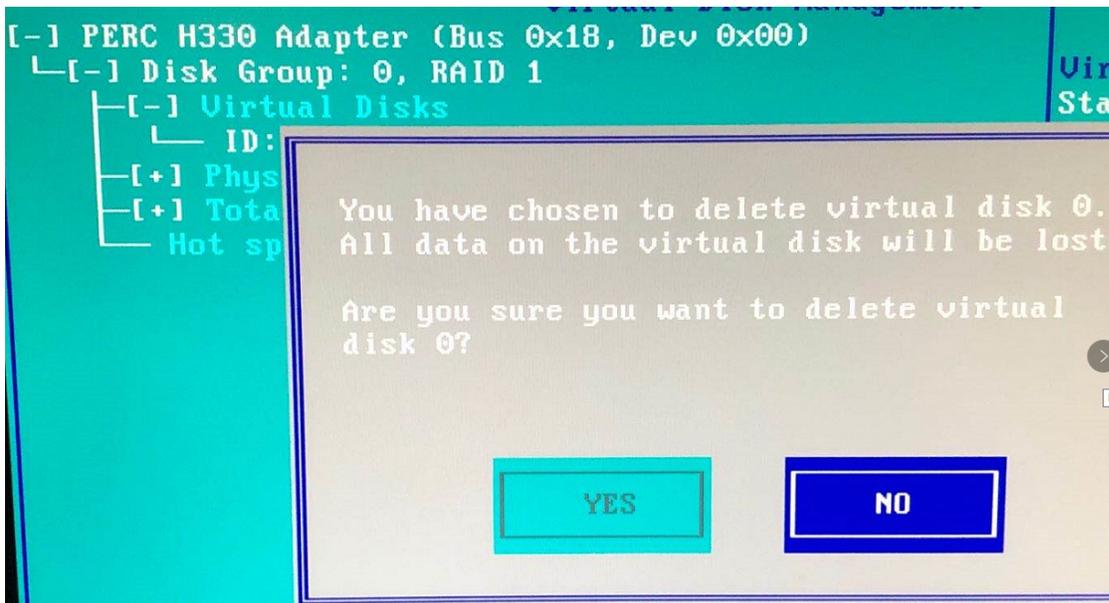
2. Boot FortiNDR and keep pressing `Ctrl R` when FortiNDR is booting.

```
PowerEdge Expandable RAID Controller BIOS
Copyright(c) 2016 Avago Technologies
Press <Ctrl><R> to Run Configuration Utility
HA -0 (Bus 24 Dev 0) PERC H330 Adapter
FW package: 25.5.5.0005

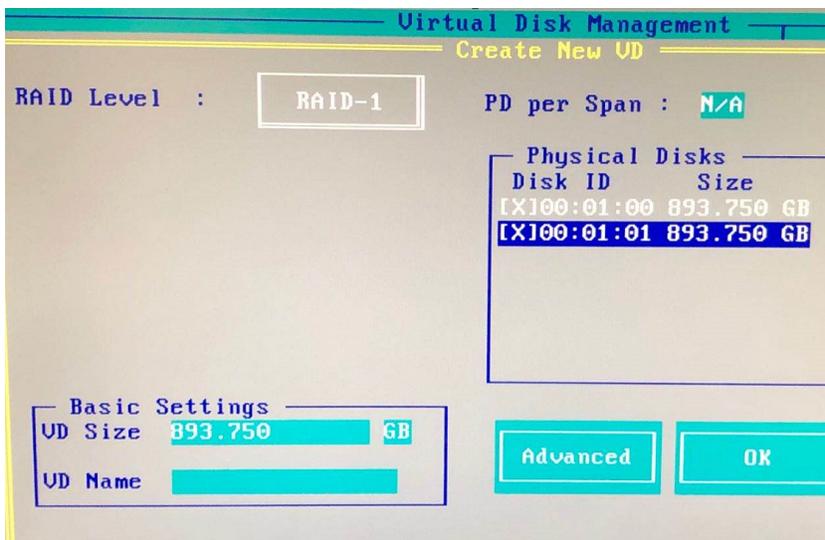
0 Non-RAID Disk(s) found on the host adapter
0 Non-RAID Disk(s) handled by BIOS

1 Virtual Drive(s) found on the host adapter
```

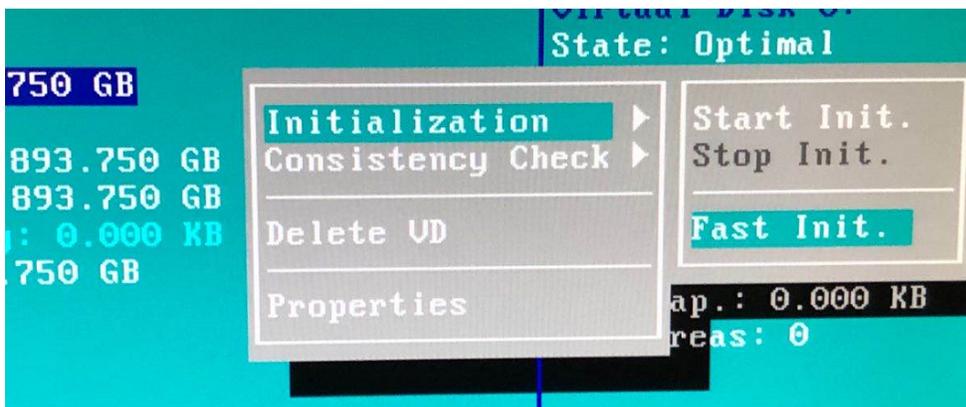
3. Delete virtual disk 0.



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.

COM2 - PuTTY

```

FortiBootLoader
FortiAI-3500F (14:05-07.24.2019)
Ver:00010001

Serial number:FAI35FT319000006
Total RAM: 391680MB
Boot up, boot device capacity: 7916MB.
Press any key to display configuration menu...
.
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter Selection [G]:

Enter G,F,B,Q,or H:

All data will be erased,continue:[Y/N]?
Formatting boot device...
.....
Format boot device completed.

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "0".

Enter TFTP server address [192.168.1.168]: 172.19.235.204
Enter local address [192.168.1.188]: 172.19.235.238
Enter firmware image file name [image.out]: b0043.deb
The PCI BIOS has not enabled this device!
Updating PCI command 6->7. pci_bus 1010030C pci_device_fn 1
MAC:E4434B7C7C33
#####
#####
Total 119782203 bytes data downloaded.
Verifying the integrity of the firmware image..

Total 412096kB unzipped.

Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?d
Programming the boot device now.
.....
    
```

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 two 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
50%	FortiNDR will start deleting older clean files and detections. Malicious and anomalies detection will remain. This process will stop if the free storage space goes below 50%.
90%	FortiNDR will stop the services (including logging, detection, sniffer, network share scanning, file uploading, oftp, icap and NDR) if it is operating at bandwidth capacity and inserting events faster than the deletion rate at the same time. The GUI and CLI console will still operate in this scenario.

Tip 1: Daemons will auto-restart when the disk falls below the above percentage thresholds.

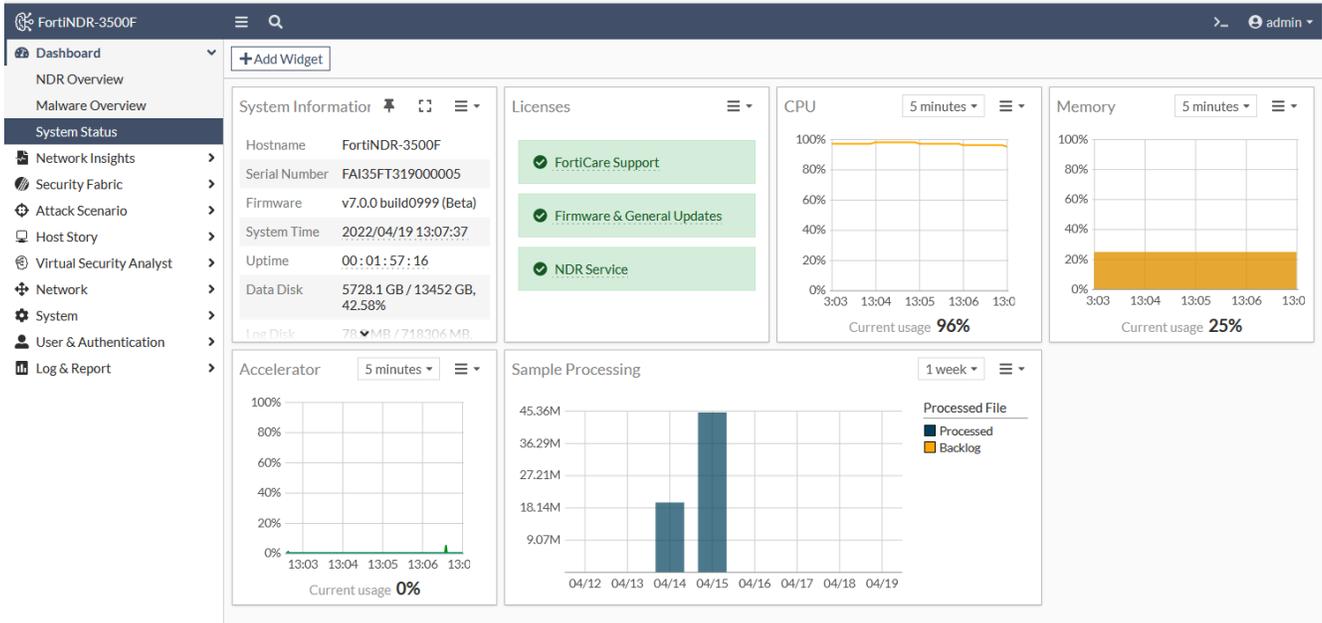
Tip 2: With FortiAI and FortiNDR 3500F, users can purchase more SSDs. Please see the data sheet and ordering guide for details.

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

- `exec cleanup` to clear the log history to free up space.
- `exec db restore` to clean all the data (including some of the AI db 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.

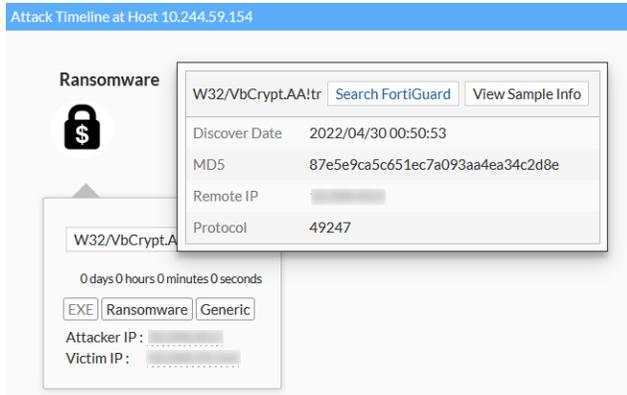
To export detected malware files with the CLI:

```
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.

Sample 129954937 Information View + Add to Allow List Generate Report Back

VSA Verdict: Critical Risk

Ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid.

Confidence level: 100.00%

Sample Information			
Submitted Date	2022/04/30 00:50:53	Last Analyzed	2022/04/30 00:56:16
File Type	EXE	File Size	6585(6.4 KB)
URL	N/A		
MD5	5F082212E8DDAE8ABAF9419268D60824 vt		
SHA256	0A18BC20973E0691A9D35A9ABA610BFBECA45263C0A0E5A8ECBB A9AC5EE5E6996		
SHA1	99A4EB3D57268604D0758A904882CB406735CC0C		
Detection Name	W64/Encoder.A:tr	Virus Family	N/A
Source Device			
Device Type	Sniffer		
Network			
Attacker	(Registered port)	Victim	

1 Detection(s)

History Similar Files

Search View all History

Date	MD5	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Conf
2022/04/30 00:50:53	5F082212E8DDAE8ABAF9419268D60824	EXE	W64/Encoder.A:tr	Sniffer				

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.

The screenshot shows the FortiNDR interface. On the left is a navigation menu with 'Log & Report' selected, and 'Malware Log' highlighted. The main area displays a table of detected files. The selected row is highlighted in yellow. To the right, the 'Details' pane is open, showing information for the selected file.

Date	MDS	File Type	Detection Name
2022/04/30 00:52:33	A3F3E85639E56868383C4716560AE5A7	HTML	HTML/Refresh.250C!tr
2022/04/30 00:52:33	BE5EC605F70210F46ADD0804708C001F0	HTML	MOATAttrTag
2022/04/30 00:52:33	61D98B3423A16FF7A2381C83869CD881	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:33	6993F1CFA28A788229C37D87000059C6	HTML	MOATAttrTag
2022/04/30 00:52:33	CC4551CFDA35E14D836A8FF37738B96D	HTML	JS/ExploitKIL29C6!tr
2022/04/30 00:52:33	E1E777A357907F35B438661A6EF05A73	PDF	MOATAttrTag
2022/04/30 00:52:33	E1E777A357907F35B438661A6EF05A73	PDF	MOATAttrTag
2022/04/30 00:52:33	2E915432AD8142D70ADC9362808B710D	EXE	W32/Graftor.FL!tr
2022/04/30 00:52:33	C3FA3BDD42B7C276ADDED1CCD508B560	EXE	W32/Al.Suspicious.2
2022/04/30 00:52:33	373C65D985C174D736BA8D496A777818	MSOFFICE	VBA/Emotet.2826!tr,ldr
2022/04/30 00:52:33	B141EA5708C154D62CC54A14E5F58387	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	E08367D9D5B38B34DB3C52B05760AFA7	PDF	PDF/Phishing.0931!tr
2022/04/30 00:52:33	1D21C3EADE6EF970665002E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:33	51927D0C4151DDE980D0E652B1B557F5	PDF	MOATAttrTag
2022/04/30 00:52:33	36533114DFE6F698DB61FCA6007C100C	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	36533114DFE6F698DB61FCA6007C100C	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	E08367D9D5B38B34DB3C52B05760AFA7	PDF	PDF/Phishing.0931!tr
2022/04/30 00:52:19	94D7F65B37588BD109F5B33946E86D46	HTML	MOATAttrTag
2022/04/30 00:52:19	2598DFB1E1C67B5B467259879B10A71F	HTML	MOATAttrTag
2022/04/30 00:52:19	8057821F44FAD32631847B9D0C2488A5	HTML	MOATAttrTag
2022/04/30 00:52:19	1D21C3EADE6EF970665002E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:19	7DD7D15D6BE9D443EAEDF5D1E90D8EE6	HTML	JS/ScrInject.B!tr

The Details pane shows the following information for the selected file:

- General: File ID 129962814, Time 2022/04/30 00:52:33, File Size 1.9 KB, File Type HTML, MDS A3F3E85639E56868383C4716560AE5A7
- Detection: Virus Name HTML/Refresh.250C!tr, Confidence Level 100.00 %, Threat Risk Level Medium Risk, Detection Type Dropper
- Network: Attacker IP 172.19.236.100: 64164, Victim IP 172.19.236.171: 443, URL http://172.19.236.171/upload
- Device: Device Sniffer

- 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} <filename-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} <filename-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
```

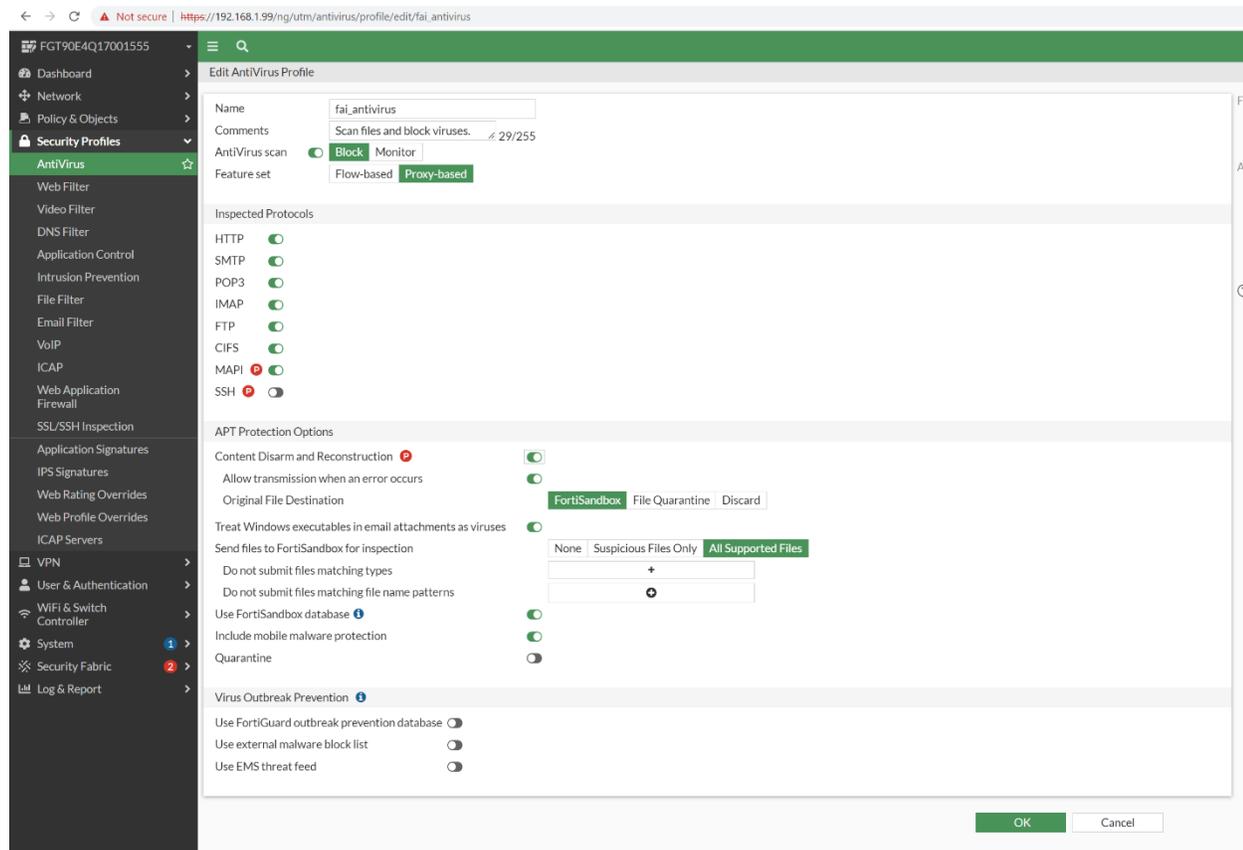
To verify a device is authorized:

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

Device Input	Device Name	VDOM	IP Address	Connection Type	Authorized	Status
Network Share	FGT_VM_G3_235.78	global	172.19.235.78	OFTP	Disabled	Disconnected
Network Share Quarantine	FGT90E4Q17001555	global	172.19.122.201	OFTP	Enabled	Connected
Fabric Connectors	FGT90E4Q17001555:root	root	172.19.122.201	OFTP	Enabled	Connected

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

Remote Log Server

Send logs to FortiAnalyzer/FortiSIEM Enable Disable

Type Syslog Protocol

Log Server Address

Port (Default UDP: 514)

```
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

Remote Log Server

Send logs to Syslog Server 1 Enable Disable

Type Syslog Protocol

Log Server Address

Port (Default UDP: 514)

```
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

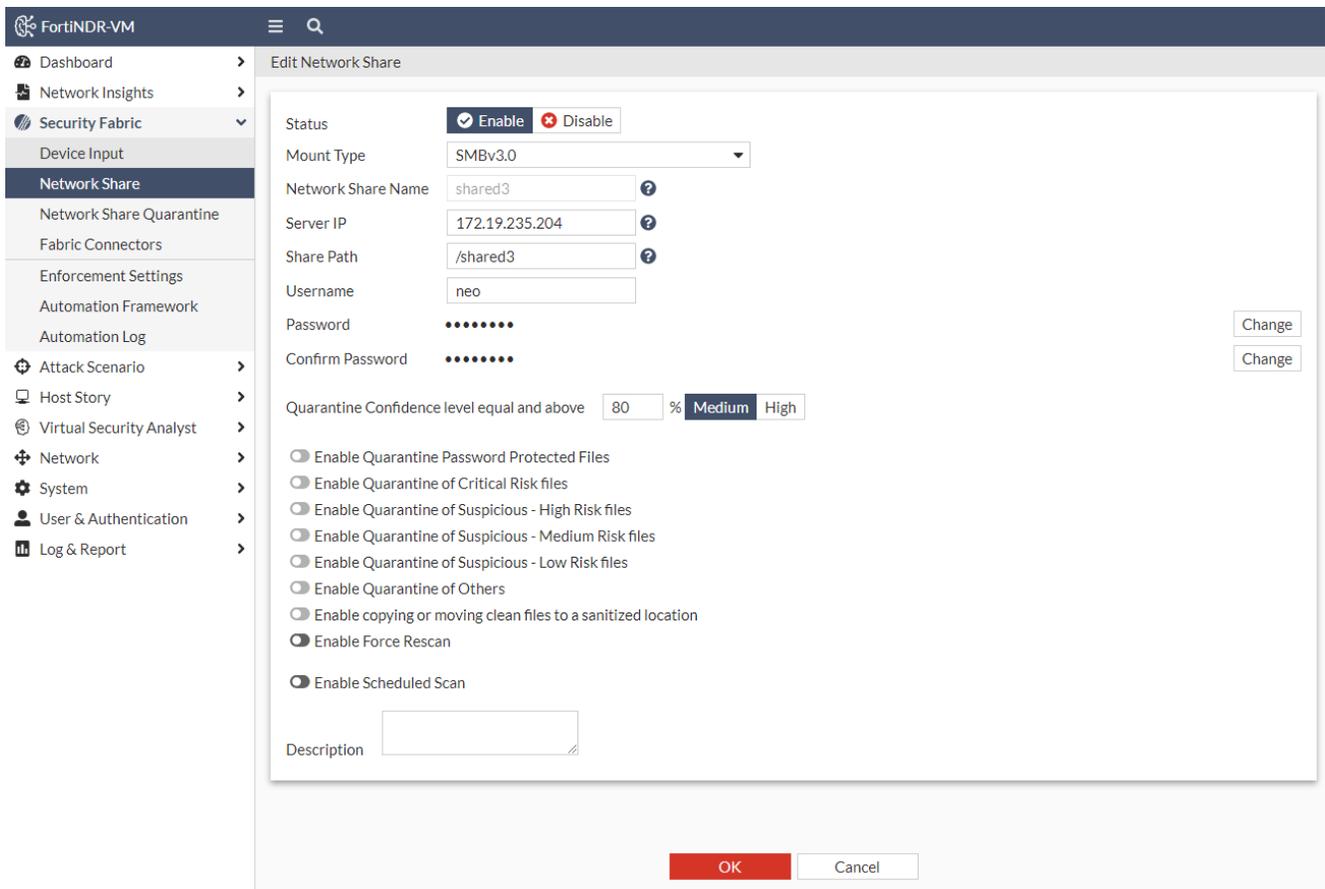
The following images shows the Network Share configuration for Windows.

The screenshot displays the 'Edit Network Share' configuration interface in the FortiNDR-3500F web console. The left sidebar shows the navigation menu with 'Network Share' selected. The main configuration area includes the following fields and options:

- Status:** A toggle switch set to 'Enable'.
- Mount Type:** A dropdown menu set to 'SMBv2.0'.
- Network Share Name:** A text input field containing '172.19.235.244'.
- Server IP:** A text input field containing '172.19.235.244'.
- Share Path:** A text input field containing '\\c'.
- Username:** A text input field containing 'administrator'.
- Password:** A masked text input field with 10 dots.
- Confirm Password:** A masked text input field with 10 dots.
- Quarantine Confidence level equal and above:** A percentage input set to '80' and radio buttons for 'Medium' (selected) and 'High'.
- Quarantine Options:** A list of radio buttons for enabling various quarantine features:
 - Enable Quarantine Password Protected Files
 - Enable Quarantine of Critical Risk files
 - Enable Quarantine of Suspicious - High Risk files
 - Enable Quarantine of Suspicious - Medium Risk files
 - Enable Quarantine of Suspicious - Low Risk files
 - Enable Quarantine of Others
 - Enable copying or moving clean files to a sanitized location
 - Enable Force Rescan
- Scheduled Scan:** A radio button labeled 'Enable Scheduled Scan' is selected.
- Schedule Type:** A dropdown menu set to 'Daily'.
- At hour:** A time input field set to '04:00 AM'.
- Description:** An empty text area.

At the bottom of the configuration window, there are 'OK' and 'Cancel' buttons.

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 <code>DEBUG_LEVEL</code> 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 <code>sdigestd</code> related crashes: <code>diagnose debug crashlog xxxx-xx-xx</code>
Data disk usage over 90%	Clean up the data disk. See, Managing FortiNDR disk usage on page 138 .

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

```
/tmp# cat 172.19.235.244
/tmp#
```

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

```
/tmp# cat shared3
mount error(16): Device or resource busy
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
/tmp#
```

- 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*:

Text AI Feature DB	 Downloading..  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
```

Thus 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.

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*.

The screenshot displays the 'Edit Administrator' configuration page in the FortiNDR GUI. The left sidebar shows the navigation menu with 'System' expanded and 'Administrator' selected. The main content area shows fields for Username (admin), Admin profile (SuperAdminProfile), and Authentication (Local). Below these are Preference settings, including Theme (Green) and a toggle for 'Restrict login to trusted hosts'. At the bottom, the 'API Key' section displays a generated key: 'u4VvEDpUATpJbFUfpbCzISduTddCOIs' with a copy icon.

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 15](#).

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 <code>file_content</code> 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': 'u4VvEDpUATpJbFUfpbCz1SduTddCOIs'},
              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': 'u4VvEDpUATpJbFUfpbCz1SduTddCOIs'},
              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 we got after uploading a file.
fileid	Get verdict result from file ID.
md5	Get the latest verdict result from MD5 checksum of the file.

The query string can only have one search query parameter.

Examples

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

```
{
  "results": {
    "fileids": [
      8068321
    ],
    "total_fileids": 1
  }
}
```

```
}
}
```

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, <i>source</i> is <i>manual upload</i> , otherwise it is an URL.

Field	Description
severity	<i>No Risk, Low, Medium, High, or Critical.</i>
category	For clean file: <i>Clean.</i> For malicious file, one of the following: <i>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.</i>
family	FortiNDR virus family name.
Feature_composition	JSON objects containing feature composition data for malicious file. <i>feature_type</i> is the category which the detected feature belongs to. <i>appearance_in_sample</i> is the number of appearances that the feature FortiNDR has detected.
confidence	For clean file: <i>N/A.</i> For other file: <i>Low, Medium, or High.</i>
file_type	<i>PE, PDF, MSOFFICE, HTML, ELF, VBS, VBA, JS.</i>
tmfc	Reserved.
pbit	Debug only.

Example of problems retrieving results

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

Field	Description
http_code	See HTTP status table on page 157 .
message	Messages include: <i>DATA_NOT_EXIST</i> when result data cannot be found given the search query parameter. <i>DATA_IN_PROCESS</i> 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. <i>INVALID_PARAM_NUMBER</i> when zero or more than one search query parameters exist. <i>INVALID_PARAM</i> 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:

- Unsupported file type
- 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 `/api/v1/verdict?fileid=xxx`

In the following two cases:

- File is still in queue
- File is still 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.

The query string can only have one search query parameter.

Examples

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

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

Example of problems retrieving report

```
{
  "http_code": 400,
```

```
"message": "INVALID_PARAM_NUMBER"  
}
```

Field	Description
http_code	See HTTP status table on page 157 .
message	Messages include: DATA_NOT_EXIST when result data cannot be found given the search query parameter. INVALID_PARAM_NUMBER when zero or more than one search query parameters exist. INVALID_PARAM when search query value is not valid.

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.

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
Checksum synchronization	TCP 20004	Inbound and outbound between FortiNDR units in an HA group.
CLI	TCP 22	Inbound SSH
Data synchronization	TCP 20003	Inbound and outbound between FortiNDR units in an HA group.
DB synchronization	TCP 5432	Inbound and outbound between FortiNDR units in an HA group.
File synchronization	TCP 20002	Inbound and outbound between FortiNDR units in an HA group.
FortiGate quarantine	TCP 443	Outbound to FortiGate
FortiGuard update	TCP 443	Outbound
IOC lookup	TCP 443	Outbound to productapi.fortinet.com
IOT lookup	TCP 443	Outbound to globalguardservice.fortinet.net
GUI	TCP 443	Inbound web browser
HA heartbeat signal	UDP 20000	Inbound and outbound between FortiNDR units in an HA group.
ICAP	TCP 1344, 11344	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
Synchronization control	UDP 20001	Inbound and outbound between FortiNDR units in an HA group.
Web Filter query	UDP 53	Outbound to service.fortiguard.net

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
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
Malware Detection	Low



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.