



Administration Guide

FortiNDR 7.4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



September 22, 2023

FortiNDR 7.4.0 Administration Guide

55-740-933820-20230922

TABLE OF CONTENTS

Change Log	7
Introduction	8
Getting started	9
Standalone, Center and Sensor operating mode	9
FortiNDR traffic and files input types	12
Files and malware scan flow using AV and ANN	14
Stage 1	14
Stage 2	15
Planning deployment	15
Storage by model	15
Additional SSD	16
Initial setup	17
Internet Access	17
Ports	18
Dashboard	20
NDR Overview	20
Malware Overview	21
System Status	21
Custom dashboards	22
Dashboard widgets in Center mode	23
Network Insights	24
Device Inventory	25
Botnet	26
FortiGuard IOC	26
Network Attacks	27
Weak/Vulnerable Communication	27
Encrypted Attack	33
ML Discovery	34
Add feedback to a ML Discovery	36
View Session	37
View Source Device and View Destination Device	39
Security Fabric	41
Device Input	41
Network Share	41
Creating a Network Share profile	42
Testing connectivity	44
Scanning a network location	45
Scheduling a scan	45
Viewing scan results	45
Scanning Zip files	46
Network Share Quarantine	46
Quarantined files	47
Creating a quarantine profile	47

Combining network share and quarantine profiles	49
Fabric Connectors	50
ICAP Connectors	50
Security Fabric Connector	51
Enforcement Settings	52
Creating enforcement profiles	53
Automation Framework	55
FortiGate quarantine webhook setup example	57
FortiSwitch quarantine setup example	61
FortiNAC quarantine setup example	64
Generic Webhook setup example	65
Automation log	65
Automation Status and Post action	66
FortiSandbox integration (FortiSandbox 4.0.1 and higher)	67
FortiGate inline blocking (FOS 7.0.1 and higher)	68
Tips for using FortiNDR inline blocking	69
FortiNDR inline inspection with other AV inspection methods	70
Accepted file types	71
FortiGate integration (integrated mode with FOS 5.6 and higher)	71
Attack Scenario	74
Scenario types	74
Attack scenario navigation and timeline	76
Understanding kill chain and scenario engine	78
Host Story	80
Virtual Security Analyst	82
Express Malware Analysis	82
Configuring the table	84
Outbreak Search	86
Search lead type of hash or detection name	86
Search lead type of outbreak name	87
Recursive searches	88
Reports	88
Static Filter	88
NDR Muting	89
Muting rules in Network Insights	90
Managing muted rules	90
ML Configuration	90
Source IP tab	91
Default Tab	93
Sensor Group ID Tab (Center mode)	94
Malware Big Picture	97
Device Enrichment	98
Viewing the retrieved device identifier	99
Overwriting the device identifier	100
Creating a Device Enrichment Profile	101

Netflow	103
Netflow Dashboard	103
Netflow Log	105
Viewing anomalies	106
Network	108
Interface	108
DNS and Static Routes	108
System	109
Administrators	109
Admin Profiles	110
Pre-defined profile types	110
Access Permissions	110
Sensor Settings	111
Sensor Details	112
Firmware	113
Settings	113
FortiGuard	114
Certificates	117
High Availability (HA)	119
HA setup requirements	119
Configuring an HA group	120
Check HA status	122
HA Failover	123
HA configuration settings synchronization	125
HA Logs	126
Using Virtual IP	126
Conserve Mode	128
Backup or restore the system configuration	128
User & Authentication	130
RADIUS Server	130
LDAP Servers	131
LDAP user query example	134
Alias member query example	134
Preparing your LDAP schema for FortiNDR LDAP profiles	135
Using common schema styles	135
Log & Report	137
Malware Log	137
Viewing the sample details	138
Advanced search	140
NDR Log	140
Anomaly tab	140
Session Tab	141
Device Tab	142
Events	144
Daily Feature Learned	145
Log Settings	146

Log Settings in Center mode	146
Alert Email Setting	146
Email Alert Recipients	147
NDR logs samples	148
AV log samples	151
Troubleshooting	153
FortiNDR troubleshooting tips	153
File scanning related issues	154
Manual Upload/API Submission/FortiSandbox Integration	154
File Submitted but not processed	155
Information for support tickets	155
FortiNDR health checks	155
Sniffer diagnosis	156
Rebuild RAID disk	157
Managing FortiNDR disk usage	160
Exporting detected malware files	161
Formatting the database	163
Export malware	163
Working with false positives and false negatives	164
Troubleshoot ICAP and OFTP connection issues	164
Troubleshoot Log Settings	165
Troubleshoot Network Share	167
Test the Network Share Connection	167
Diagnosing Network Share Errors	169
Debug version image	170
Check Crash Log	170
Troubleshooting the VM License	171
Troubleshooting Updater	171
FDS Authorization Failed	171
Clearing updater cache files	171
Diagnosing Other FDS Errors	172
Troubleshooting tips for Network File Share	172
Appendix A: API guide	177
Appendix B: Sample script to submit files	184
Appendix C: FortiNDR ports	190
Appendix D: FortiGuard updates	191
Updating the ANN database from FDS for malware detection (GUI)	192
Updating ANN for malware detection (CLI)	193
Appendix E: Event severity level by category	197
Appendix F: IPv6 support	198
Appendix G : Supported Application Protocol List	200
Appendix H: File types and protocols	201
Appendix I: Operational Technology / SCADA vendor and application list	202

Change Log

Date	Change Description
2023-09-12	Initial release.
2023-09-21	Updated Sensor Settings on page 111.

Introduction

FortiNDR is a product family with both *on-premises* option and FortiNDR Cloud, a SaaS based offering. This administration guide is targeted for FortiNDR on-premises deployment.

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 using patented Artificial Neural Networks (abbreviated with ANN in document, [US patent US11574051B2](#)).

FortiNDR combined Network Detection Anomalies features along with ANN that scans and classify malware in file based attacks. These functions are usually provided by your security operations analyst, hence in FortiNDR there's a concept of Virtual Security Analyst TM, 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 on premise solution can run in both appliance and Virtual Machine format. Please refer to the [datasheet](#) for hardware models and specifications. VM comes in VM16 or VM32 subscription license. Both form factors will have Netflow and Operational Technology (OT)/SCADA licensed separately. The Netflow license will allow intake of Netflow data and inspection for security detections, while the OT/SCADA license will enable FortiNDR to detect and update industrial IPS and OT (Industroyer) malware classification, as well as identify OT applications for machine learning purpose. (See [appendix I](#) for list of OT applications support)

FortiNDR can receive both network traffic and inspect files using neural networks for scanning from different ways: 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. The NDR solution is a passive solution with analyzing network metadata and uses it to determine if an attack occurs. FortiNDR can:
- 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
- Upon attacks or anomalies detected, FortiNDR can perform manual and automatic mitigation (AKA Response) with Fortinet Security Fabric devices (such as FortiGate, FortiSwitch, FortiNAC), as well as 3rd Party solutions (via API calls).

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

Getting started

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

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

To connect to the FortiNDR GUI:

1. Connect to the port1 management interface (default 192.168.1.88) 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*.

Standalone, Center and Sensor operating mode

Starting in FortiNDR v7.4.0, FortiNDR supports three operating modes:

- **Standalone:** Supports all the features and functionality of FortiNDR. FNR-1000F, VM16/32, FNR-3500F can all operate as standalone mode.
- **Center:** Supports centralized management of configurations and data collected by sensors. Most, but not all features and functionality are available. At this time, FortiNDR 7.4 supports center mode in the FNR-3500F only.
- **Sensor:** Supports Sensor configuration upon first login. A minimal amount of features and functionality are available. For FNR-1000F and VM models (VM, KVM, AWS, Azure, GCP).

There is a separate image to be loaded for each mode in the [customer support website](#).

The mode you use is determined by the firmware image. A new firmware update package contains three types of firmware image (Standalone image, Center image, and Sensor image). After the Center and Sensor images are installed, the mode is displayed in brackets next to the image name at the top-left side of the GUI. A unit in standalone mode unit will not display *Center* or *Sensor* next to the image name.



The following table identifies the features available in Standalone, Center, and Sensor modes and how they behave:

Feature	Standalone	Center	Sensor	Notes
Dashboard	✓	✓	✓	In Center mode, the widgets are used to monitor the sensors.
Security Fabric	✓		✓	Security Fabric is configured in the Sensor mode or via the Center mode settings.
Attack Scenario	✓	✓	✓	This feature is incidental in Sensor and Standalone modes. Center mode collects and presents all Attack Scenarios reported from every Sensor connected to this Center.
Host Story	✓	✓	✓	This feature is incidental in Sensor and Standalone modes. Center mode consolidates and displays all Host Stories from all Sensors associated with the Center.
Virtual Security Analyst > Express Malware Analysis	✓		✓	
Virtual Security Analyst > Static Filter	✓	✓		Static Filters, including the <i>Allow List</i> and <i>Deny List</i> , are employed in Center mode and associated with specific sensors. These filters provide users with the capability to formulate and modify an <i>Allow</i> or <i>Deny</i> list for targeted sensors. Please note that these Static Filters cannot be set through the Sensor's GUI.

Feature	Standalone	Center	Sensor	Notes
Virtual Security Analyst > NDR Muting	✓	✓	✓	NDR Muting rules can be established in Center and Sensor mode. However, these rules only mask or hide specific NDR attack detections for that specific Center or Sensor. For instance, if you hide an attack on a Center, it does not automatically hide the same attack on the Sensor's user interface.
Virtual Security Analyst > ML Discovery	✓	✓		Both the <i>ML Discovery</i> dashboard widget and <i>ML Discovery</i> module are not available in Sensor mode.
Virtual Security Analyst > Device Enrichment	✓			
Virtual Security Analyst > ML Configuration		✓		
Netflow	✓	✓	✓	Sensor mode maintains the same design and functionality for the <i>Netflow Dashboard</i> and <i>Netflow Log</i> as seen in Standalone mode. Center mode's <i>Netflow Dashboard</i> and <i>Netflow Log</i> display the data collated from the Sensors.
System > Admin Profiles	✓	✓	✓	In Center mode, users can select which Sensor(s) are linked with the current profile. If a Sensor is selected to be included in this <i>Admin Profile</i> , the profile user will be able to view and manage the corresponding Sensor when they log into the FortiNDR Center.
System > Center Settings		✓		
System > High Availability (HA)	✓			

Feature	Standalone	Center	Sensor	Notes
Log & Report > Daily Feature Learned	✓	✓		In Center mode, the Log Settings can be configured to send the center's system event log to the syslog servers. Detection logs, including malware logs and NDR logs that record events occurring in the sensors, are sent directly from the sensors themselves. These sensors' syslog configurations can be edited and uploaded via the <i>Center's System > Sensor Settings</i> page using the <i>Restore Configuration</i> button.

FortiNDR traffic and files input types

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

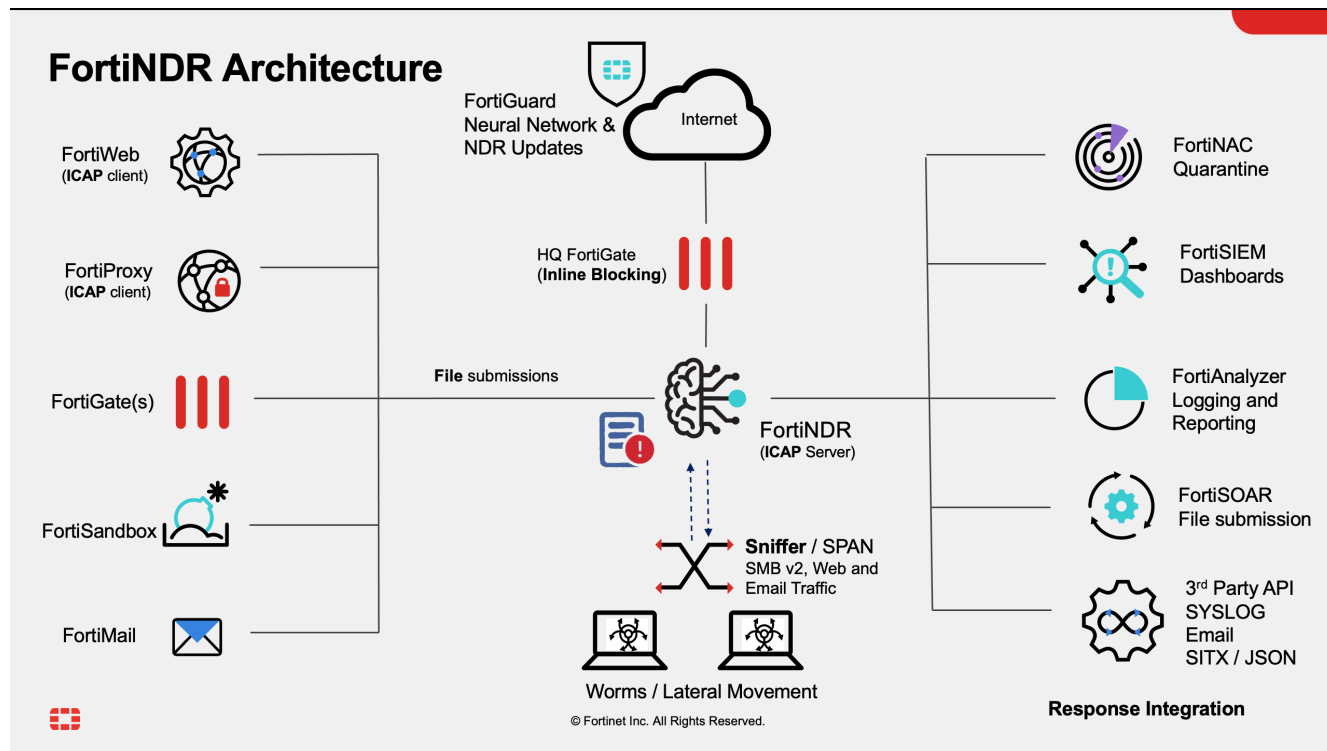
For more information, see the [FortiNDR CLI Reference Guide](#).

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
Sniffer			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. Using SPAN port, network tap or packet brokers to mirror traffic.
Fabric devices	FortiGate	HTTP2 (v7.0 FOS)	HTTP, HTTPS (with SSL decryption), SMTP,		FortiGate v7.0.1 supports INLINE blocking with AV

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
ICAP		OFTP (v5.6-6.0 FOS, legacy support)	POP3, IMAP,		profile
	FortiMail	HTTP2	SMTP		Configure under <i>AV profile</i> under FortiMail.
	FortiSandbox	HTTP2	MAPI, FTP, CIFS		
	FortiProxy	HTTP2	HTTP, HTTPS		
	FortiWeb	ICAP	HTTP, HTTPS		Supports using FortiNDR as ICAP server.
	FortiProxy	ICAP	HTTP, HTTPS		FortiGates, FortiWeb and FortiProxy or third-party ICAP client such as Squid.
Other / API	FortiSOAR	HTTPS API upload	HTTPS		Using API available from FortiNDR for file upload
	Scripts (refer to Appendix for sample scripts)	HTTPS API upload			
	NFS and SMB file shares	SMB/NFS			Direct map and scan

For a complete list of supported file types, see [Appendix H: File types and protocols on page 201](#)

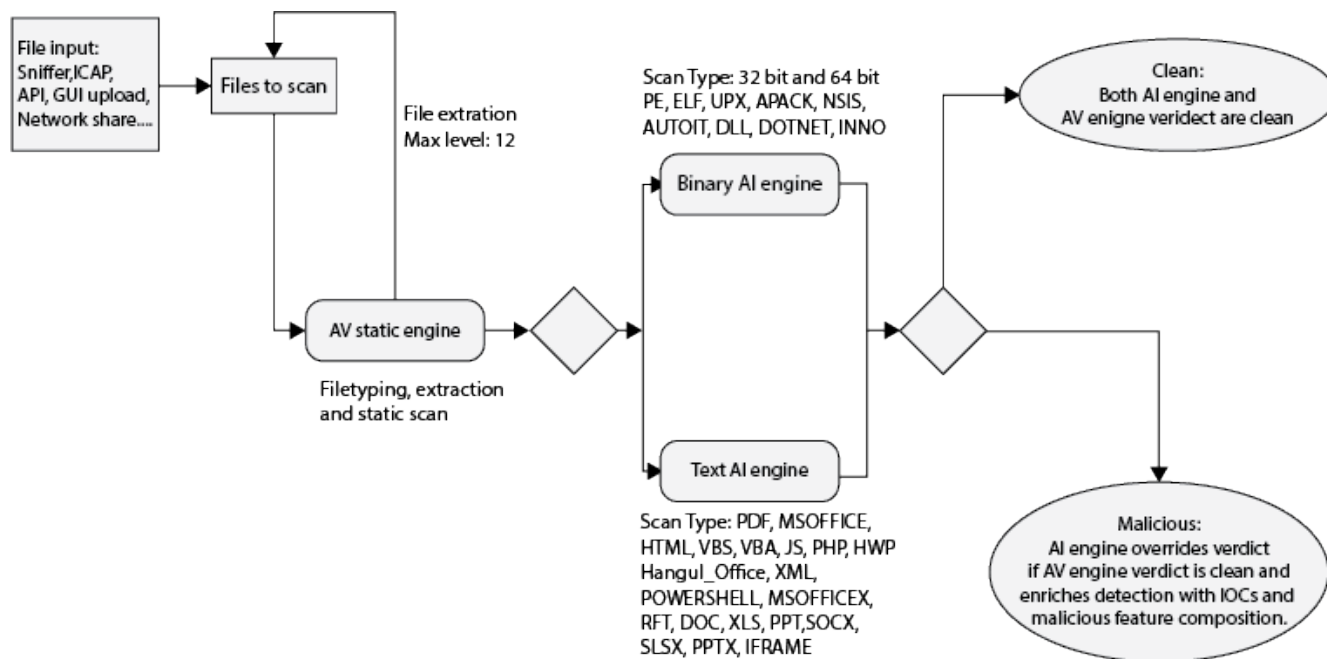
FortiNDR supports quarantine with incoming webhook from FortiOS 6.4 and higher. For details, see the Release Notes. For FortiNDR to quarantine via FortiGate, you must provide VDOM information to FortiGate. For details, see [Automation Framework on page 55](#).



Files and malware scan flow using AV and ANN

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.

Planning deployment

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

Storage by model

- FNR-1000F supports 2 x 7.68TB SSD storage in RAID 1 configuration, this is not expandable.
- FNR-3500F (gen3 with fiber card) uses 4 x 3.8TB SSD in RAID10 and comes with the option to purchase additional SSD HDDs.
- FAI-3500F (gen 1 & 2) uses 2 X 3.8TB SSD in RAID1 and comes with the option to purchase additional SSD HDDs. This model will support RAID 10 if 2 x (or more) additional SSD are purchased.
- FortiNDR-VM comes with 4 different size disk images.

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

Model	Total disk size	Storage retention
FortiNDR-1000F 2 SSD (not expandable)	2 x 7.68 TB (RAID 1)	66 days
FNDR-3500F 4 SSD	6.6 TB	66 days
FNDR-3500F 2 SSD	3.3 TB	33 days
FNDR-3500 8 SSD	13.2 TB	132 days
FNDR-3500 16 SSD	26.4 TB	264 days
FNDR-VM	1024 GB	20 days
FNDR-VM	2048 GB	40 days
FNDR-VM	4096 GB	81 days
FNDR-VM	8192 GB	163 days



VM16 and VM32 published file processing rate 130,000 and 170,000 files per hour respectively

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

- Size of data disk allocated in VM
- Number of disks inserted into hardware model
- Throughput of network e.g. with sniffer
- Whether unit is used for NDR and/or pure file analysis only

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

Additional SSD

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

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



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

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

To add additional SSD:

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

After the command is executed, the device will:

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

To check the new SSD capacity with the GUI:

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

To check the new SSD capacity with the CLI:

Get system raid-status

Sample output:

```
FortiNDR-3500F # get system raid-status
Controller Model Firmware Driver
-----
a0 PERC H350 Ada 5.190.01-3614 07.714.04.00-
+---- Unit Status Level Part Of Size (GB)
| u0 OK LEVEL 10 a0 14304
+---- Port Status Part Of Size (GB)
| 64:0 OK u0 3575
| 64:1 OK u0 3575
| 64:2 OK u0 3575
| 64:3 OK u0 3575
| 64:4 OK u0 3575
| 64:5 OK u0 3575
| 64:6 OK u0 3575
| 64:7 OK u0 3575
```

Initial setup

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

Internet Access

For FortiGuard updates please have a stable internet access from the FortiNDR unit. Go to *System > FortiGuard* for updates via Internet. For offline deployments please refer to [Appendix D: FortiGuard updates on page 191](#).



Proxy FortiGuard support is supported via CLI only, please refer to the [CLI guide](#).

Ports

For all FortiNDR appliances and hardware, Port1 and port2 are hard-coded to be management port and sniffer port. The following is the initial port configuration for FNR-3500F.

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



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

SKU: FN-TRAN-SFP+GC

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

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

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



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



*For customers who are required to use SFP+ ports (available in FNR-3500F gen3 hardware only) for management and capture (sniffer), pls contact local CSE for details.

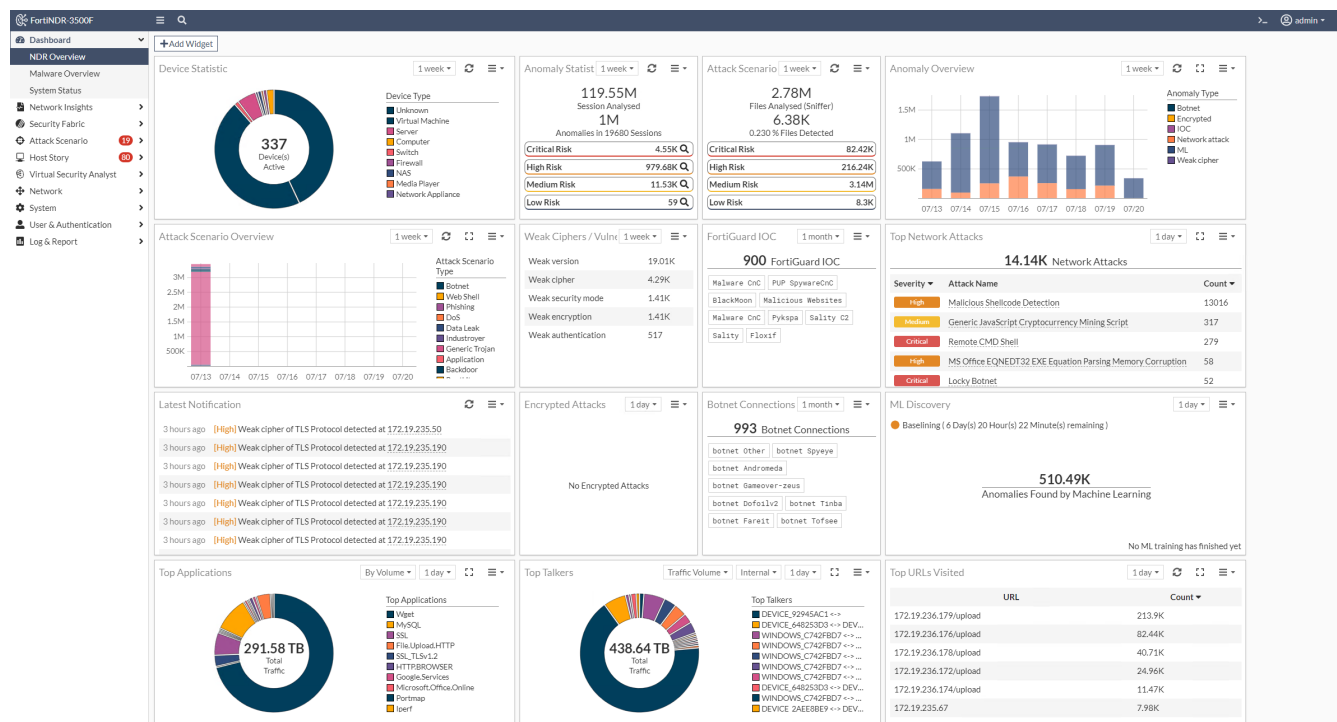
Dashboard

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*. Users are welcome to add custom dashboards and appropriate widgets tailored for their operations. There are FortiNDR widgets such as *Botnet*, *Attack Scenarios*, and *Sessions Analyzed* to cater to different needs.

The following sections describes the manual and usage in FortiNDR GUI:

NDR Overview

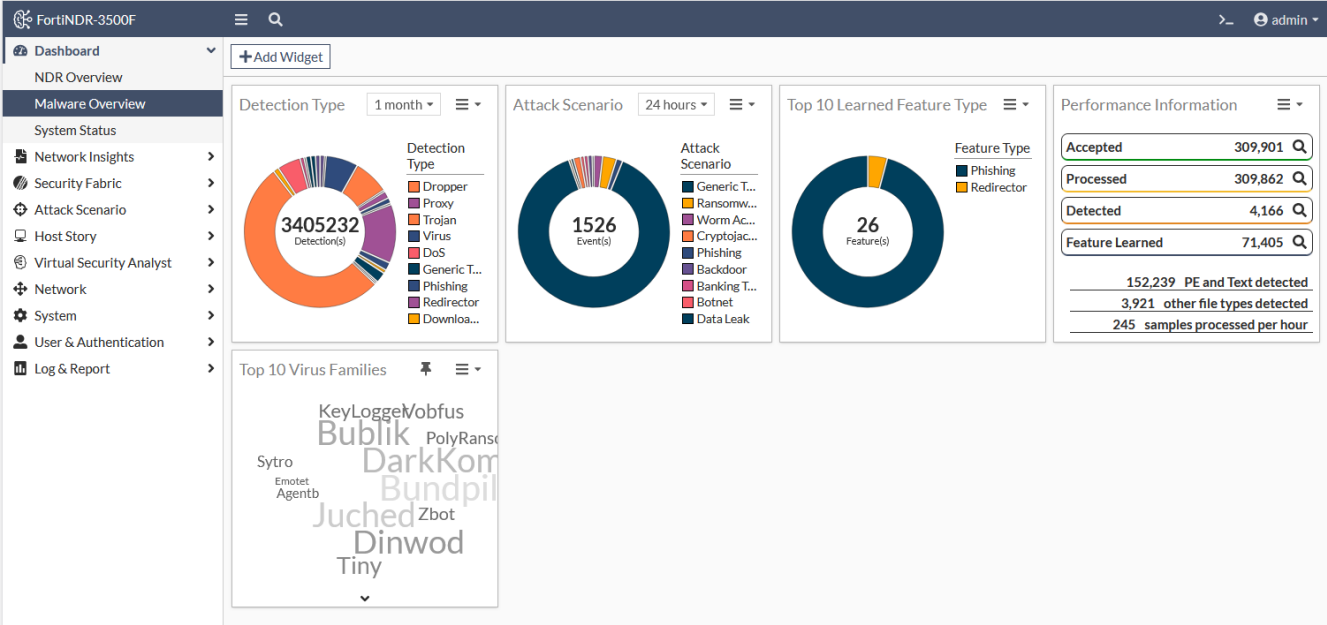
The *NDR Overview* dashboard displays network detection and response statistics as charts and graphs. Each widget can be filtered with a time range of *1 day*, *1 week*, or *1 month*. When you click the *Network Insights* widgets, such as *ML Discovery* and *Botnet*, the widget expands to full screen.



ML Discovery is not available in Sensor mode.

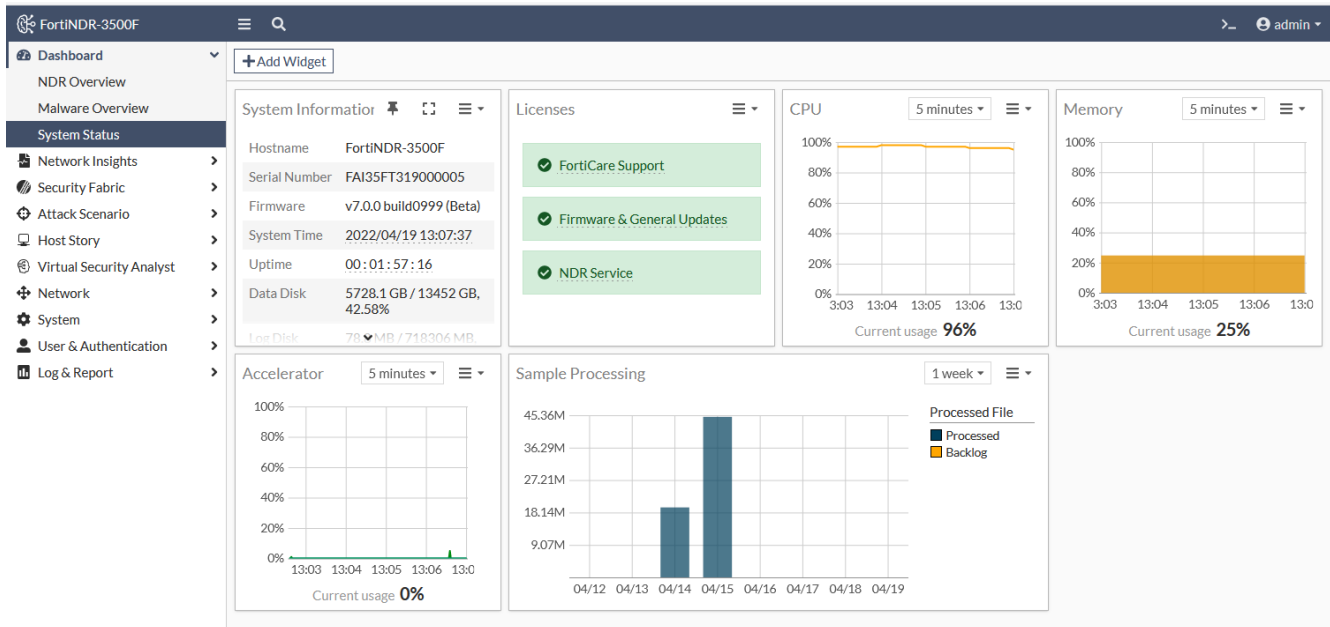
Malware Overview

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



System Status

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



Custom dashboards

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

To add a widget to a dashboard:

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

To create a custom dashboard:

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

To delete a custom dashboard:

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

Dashboard widgets in Center mode

In Center mode, dashboard widgets are used to monitor the sensors. You can add the same widget for each sensor in your network, allowing you to easily compare the sensor's statistics.

To add a widget in Center mode:

1. In the dashboard, click *Add Widget*.
2. In *Source Sensor*, click the plus (+) sign, then select a sensor from the list and click *Close*.
3. From the *Timeframe* dropdown, select *1 Hour*, *24 hours*, *1 Week* or *1 Month*.
4. Click *OK*.
5. (Optional) To add the same widget for a different sensor, click *Add Widget* and repeat steps 2-4.

Network Insights

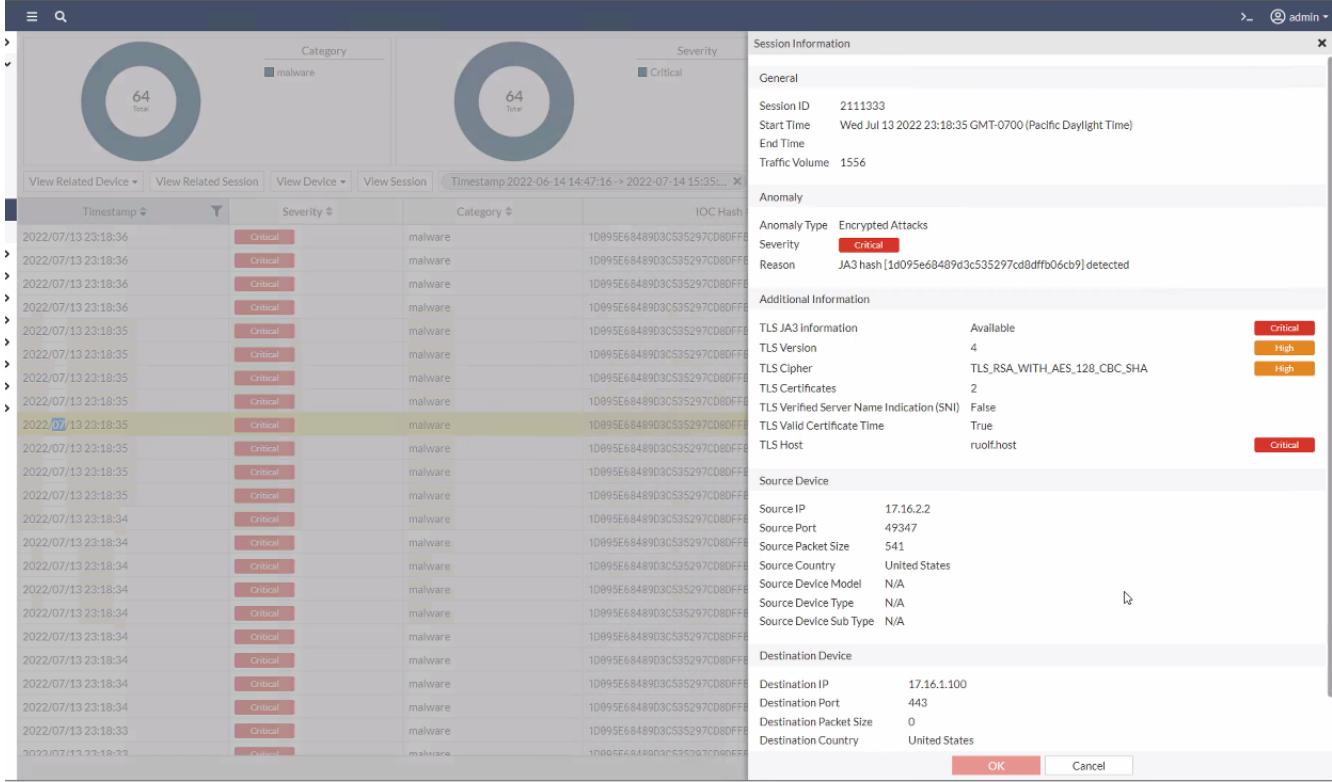
Network Insights monitors display information about NDR detections. The charts in *Network Insights* can display a maximum of 30,000 insights. Detections are organized by category:

- [Device Inventory](#)
- [Botnet](#)
- [FortiGuard IOC](#)
- [Network Attacks](#)
- [Weak/Vulnerable Communication](#)
- [Encrypted Attack](#)
- [ML Discovery](#)

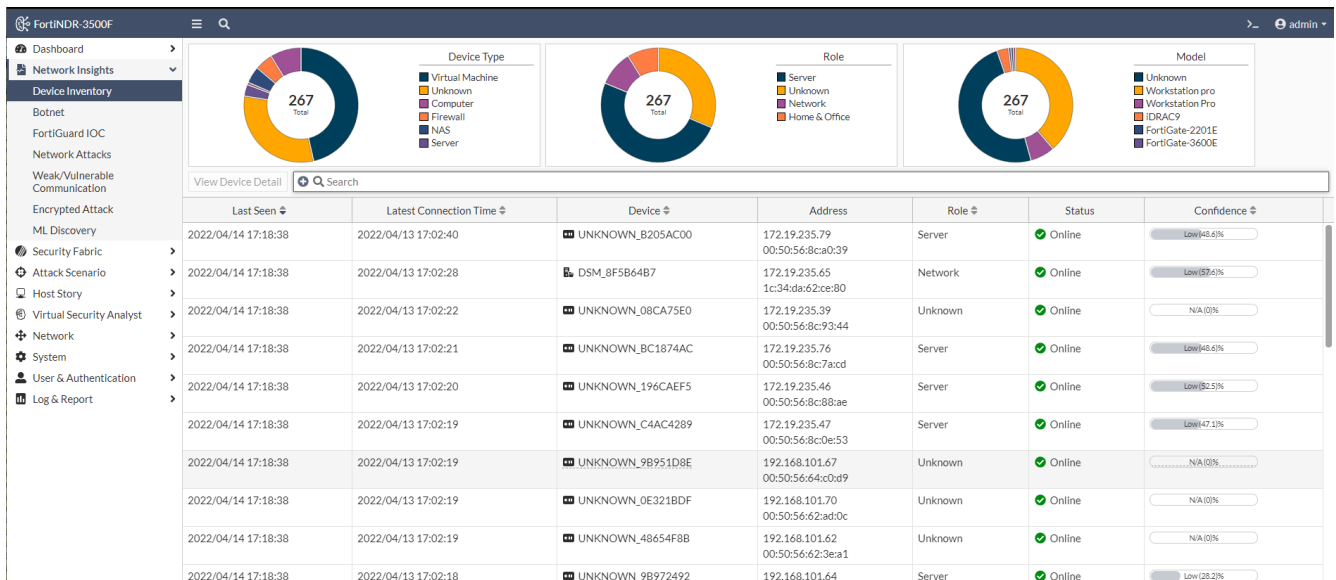
Double-click an entry in the monitor to view *Additional Information* in the *Session Information* pane. The *Additional Information* section contains useful information related to the attack. There could be multiple reasons for each session ID to be considered anomalies.

- For *Botnet* type anomalies, the *Additional Information* section shows *DNS Hostname*, *DNS OPCODE*, *DNS RETCODE*.
- For *Network Attack*, *Weak/Vulnerable Communication*, and *Encrypted Attack* types, the *Additional Information* section shows the reason why the session was flagged by Intrusion detection. The reasons may vary depending on the severity levels. The Anomaly severity level is chosen by the highest level.
- JA3 hashes are provided by FortiGuard research which tracks botnet which uses encrypted communications to C2 servers. FortiNDR will match both client and server JA3 hashes and if available, display the malware/botnet name associated.

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.

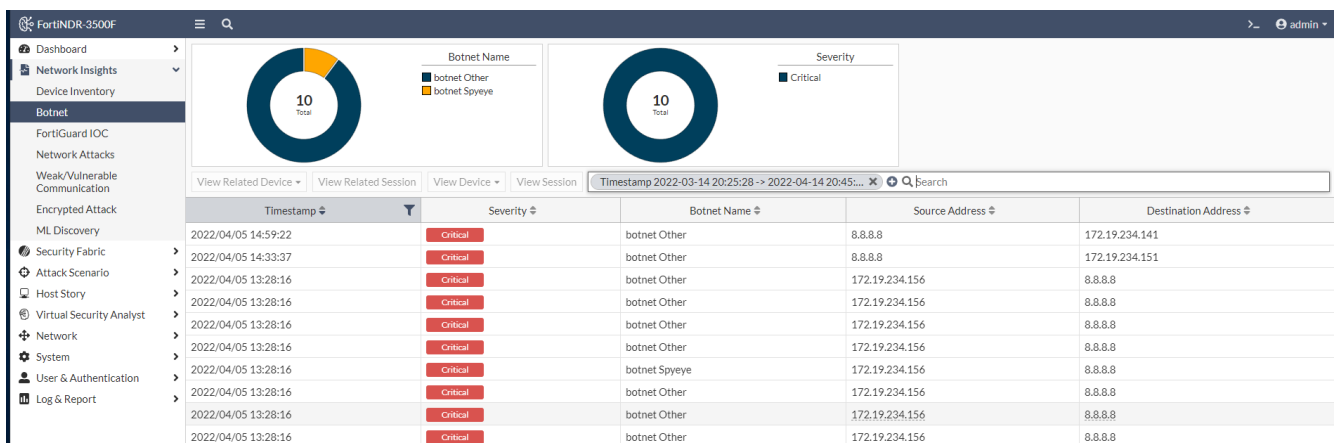


1. User defined (for example, finance server).
2. AD Device enrichment (hostname from AD, if configured).
3. System generated (OS hash of the mac address).



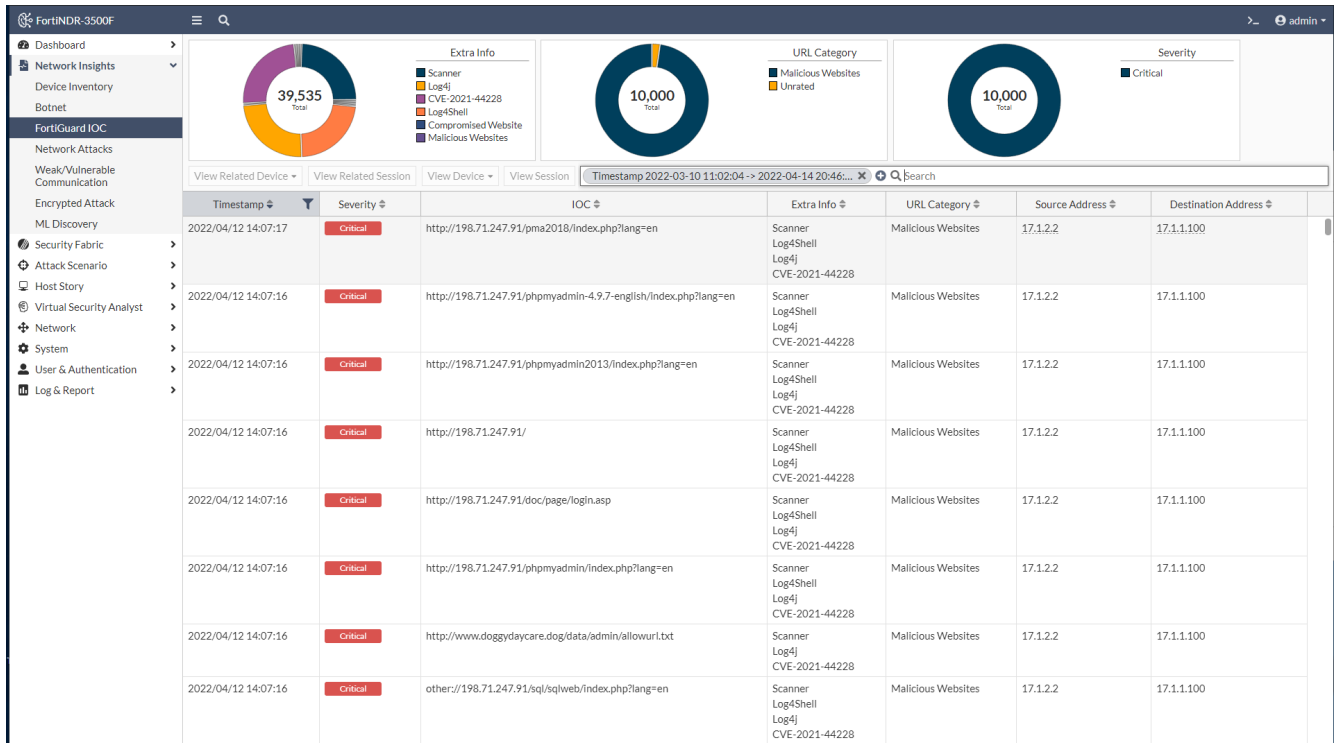
Botnet

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



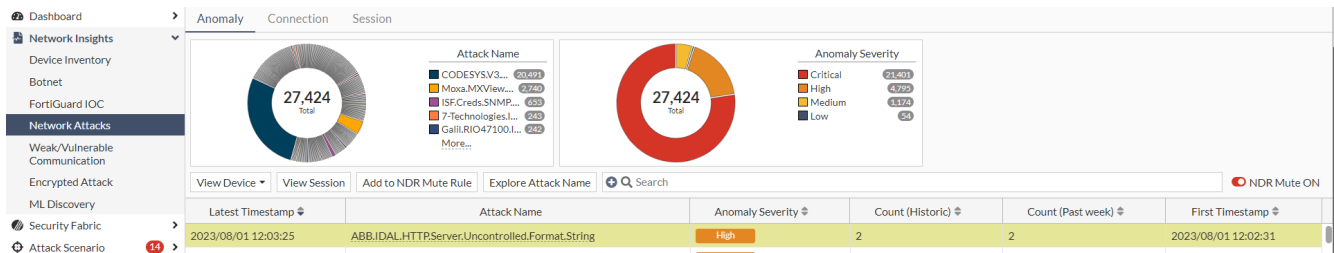
FortiGuard IOC

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



Network Attacks

Network Attacks are known attacks detected by the Network Intrusion Protection Database. FortiNDR can detect North-South, East-West IPS attacks depending on where NDR sniffer port(s) are placed.

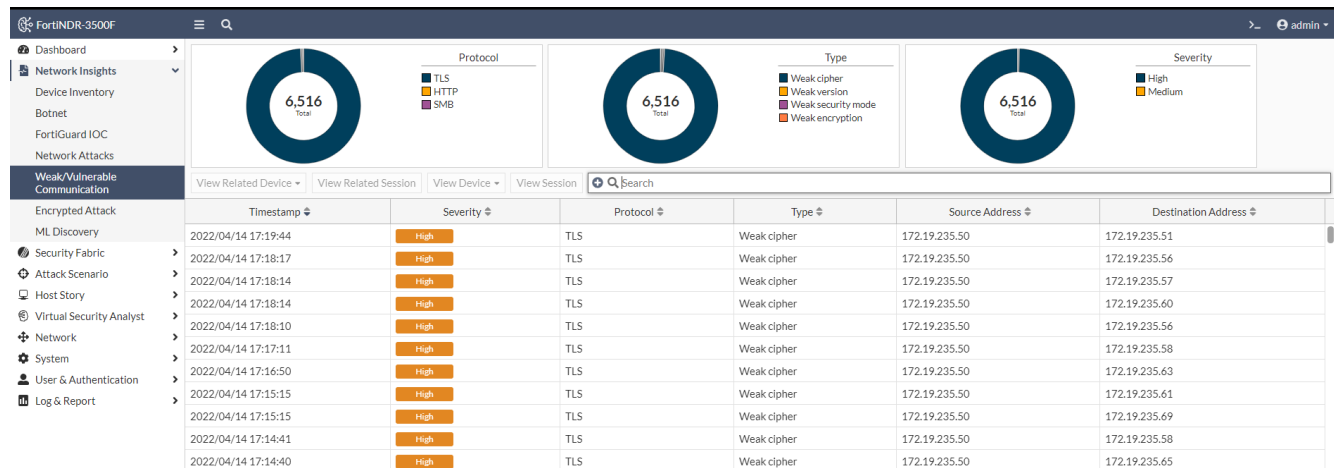


To view the *Mitre Attack Technique*, click *Explore Attack Name*.

Weak/Vulnerable Communication

The **Weak/Vulnerable Communication** page displays the list of weak or vulnerable communication detected on sniffer port(s) on NDR interfaces. Detection of weak and vulnerable communications in the network can be signs of week or

compromised network security, administrators should pay attention to. For example, a weak cipher used by an older version of SSL.



Weak/Vulnerable Communication types

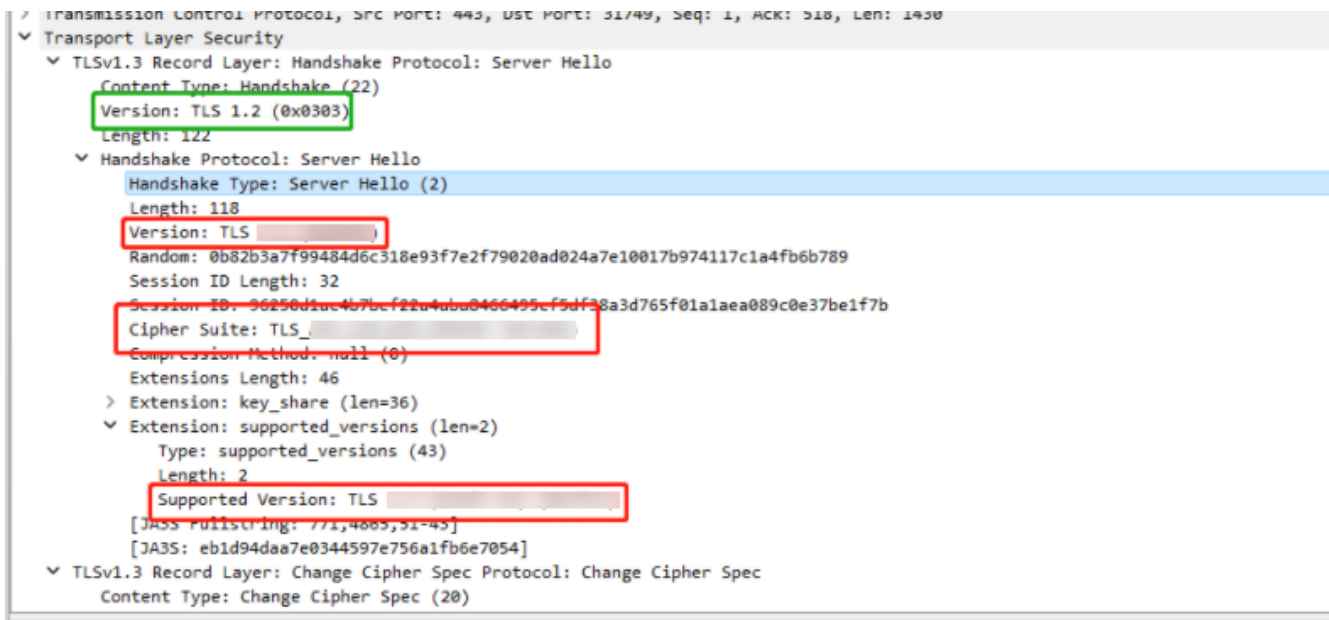
The following table provides a definition for each of the weak/vulnerable communication types:

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

Communication type	Description
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



Weak security mode

The image shows a Wireshark packet capture of SMB traffic. The packet list at the top shows several packets, including a Negotiate Protocol Request (SMB) and a Negotiate Protocol Response (SMB). The packet details pane for the Negotiate Protocol Response (SMB) is expanded, showing various fields. The 'Security Mode' field is highlighted with a red box, indicating a weak security mode.

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
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	0.000354	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	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...

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: 0x00000000
 - 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, Infolevel 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: 607606062b0601050502a06c306aa03c303a060a2b06010401823702021e06092a864882...

Weak extended security

smb-smb1-ascii.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

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...|P V E...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 aezu<4...

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 00 72 7c 00 00 a5 44 11 03r|...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 dfKE...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 ease_ign ore

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 packet capture of an SMB2 negotiation. The packet list pane at the top shows several packets, with packet 5 (SMB2 Negotiate Protocol Response) selected and highlighted in yellow. The packet details pane for packet 5 shows the SMB2 Header and the Negotiate Protocol Response (0x00). The Security mode is 0x01, indicating signing is enabled. The Dialect is highlighted in blue, and the NegotiateContextCount is 0. The Capabilities field shows 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..., and NegotiateContextOffset: 0x204d4c20.

The packet bytes pane at the bottom shows the raw data of the packet, with the dialect field (0x00000001) highlighted in blue. The status bar at the bottom indicates the dialect is smb2.dialect, 2 bytes, and the profile is Default.

Weak authentication

The image shows a Wireshark packet capture of a network traffic file named `linuxpostgrespostgres_payload_yliu_20121219.pcap`. The packet list shows several TCP and PostgreSQL packets. Packet 6 is selected, showing details for a PostgreSQL Authentication request. The authentication type is MD5 password (5), and the salt value is 065e739f. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.218.0.1	10.218.0.100	TCP	74	63238 → 5432 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=13184308...
2	0.000231	10.218.0.100	10.218.0.1	TCP	74	5432 → 63238 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSv...
3	0.000543	10.218.0.1	10.218.0.100	TCP	66	63238 → 5432 [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=1318430849 TSecr=971127
4	0.003033	10.218.0.1	10.218.0.100	PGSQL	108	>
5	0.003235	10.218.0.100	10.218.0.1	TCP	66	5432 → 63238 [ACK] Seq=1 Ack=43 Win=14480 Len=0 TSval=971128 TSecr=1318430849
6	0.006309	10.218.0.100	10.218.0.1	PGSQL	79	<R
7	0.006545	10.218.0.1	10.218.0.100	TCP	66	63238 → 5432 [ACK] Seq=43 Ack=14 Win=14656 Len=0 TSval=1318430850 TSecr=9711...
8	0.008786	10.218.0.1	10.218.0.100	PGSQL	107	>p
9	0.020284	10.218.0.100	10.218.0.1	PGSQL	390	<R/S/S/S/S/S/S/S/S/S/S/S/K/Z
10	0.025559	10.218.0.1	10.218.0.100	PGSQL	88	>Q

Frame 6: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)

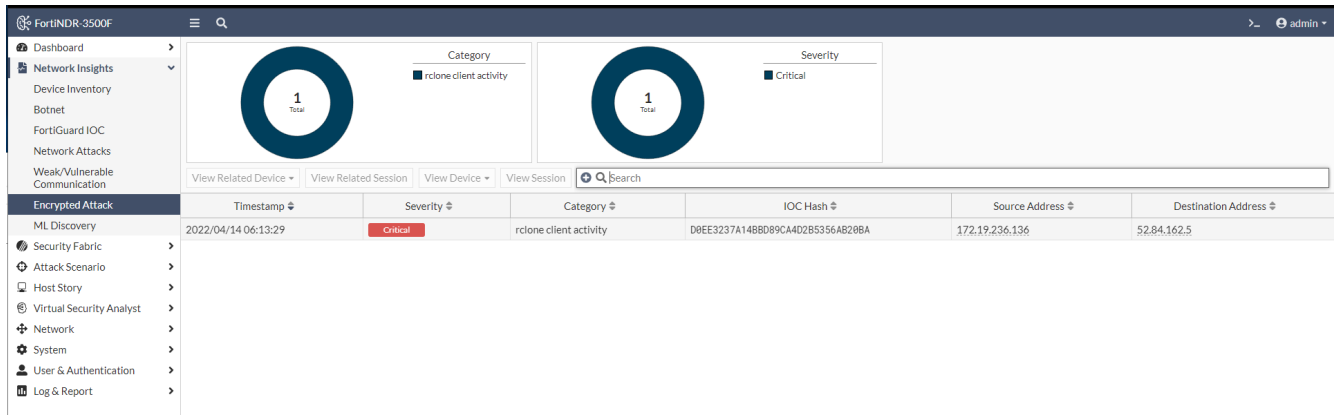
- Ethernet II, Src: VMware_55:9c:c0 (00:0c:29:55:9c:c0), Dst: Fortinet_cc:a2:09 (00:09:0f:cc:a2:09)
- Internet Protocol Version 4, Src: 10.218.0.100, Dst: 10.218.0.1
- Transmission Control Protocol, Src Port: 5432, Dst Port: 63238, Seq: 1, Ack: 43, Len: 13
- PostgreSQL
 - Type: Authentication request
 - Length: 12
 - Authentication type: MD5 password (5)
 - Salt value: 065e739f

The type of authentication requested by the backend. (pgsql.authtype), 4 bytes

Packets: 33 · Displayed: 33 (100.0%) Profile: Default

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



ML Discovery is not available in Sensor mode.

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.

Timestamp	Severity	Anomaly Feature(s)	Additional Information	User Feedback	Source Address	Source Model	Destination Address
2022/04/13 21:19:16	Low	TL Protocol Source Port	TL Protocol: UDP Source Port: 111	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:19:42	Low	TL Protocol AL Protocol Protocol/Application Behaviors/Action	TL Protocol: UDP AL Protocol: RPC Protocol/Application Behaviors/Action: Portmap	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:19:50	Low	Source Port Protocol/Application Behaviors/Action	Source Port: 137 Protocol/Application Behaviors/Action: NetBIOS.Name.Service	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:30:56	Low	Source Port	Source Port: 22	No Feedback	172.17.1.101	Workstation pro	172.17.2.3
2022/04/13 21:30:53	Low	Source Port	Source Port: 22	No Feedback	172.17.1.101	Workstation pro	172.17.2.4
2022/04/13 21:30:34	Low	Source Port	Source Port: 22	No Feedback	172.16.1.101	Workstation pro	172.16.2.10
2022/04/13 21:20:52	Low	Source Port	Source Port: 22	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:20:52	Low	Source Port	Source Port: 22	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:20:52	Low	Source Port	Source Port: 22	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:20:52	Low	Source Port	Source Port: 22	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:20:52	Low	Source Port	Source Port: 22	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:19:53	Low	Source Port	Source Port: 138	No Feedback	172.16.2.2	Workstation pro	172.16.1.100
2022/04/13 21:19:43	Low	Source Port	Source Port: 161	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:19:19	Low	Source Port	Source Port: 631	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:19:18	Low	Source Port	Source Port: 22	No Feedback	172.16.1.100	Workstation pro	172.16.2.2
2022/04/13 21:41:05	Low	Protocol/Application Behaviors/Action	Protocol/Application Behaviors/Action: SMTP	No Feedback	172.16.2.7		172.16.1.91
2022/04/13 21:30:55	Low	Protocol/Application Behaviors/Action	Protocol/Application Behaviors/Action: 16060	No Feedback	172.17.2.3		172.17.1.101

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:

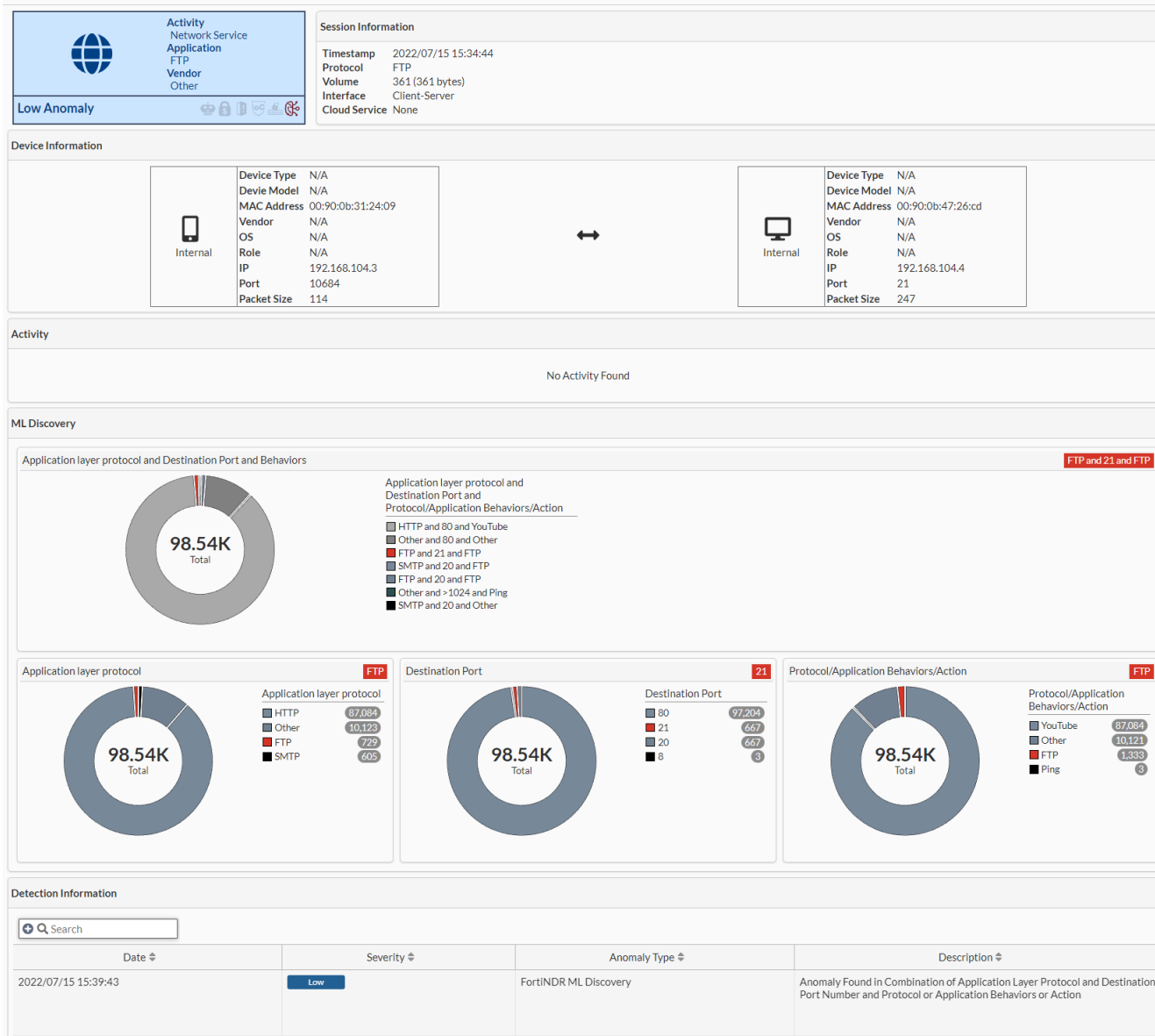
- *Application layer protocol*: FTP
- *Destination Port*: 21
- *Protocol/Application Behaviors/Action*: FTP

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



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

Add feedback to a ML Discovery

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

To add feedback to ML Discovery:

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

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

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



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

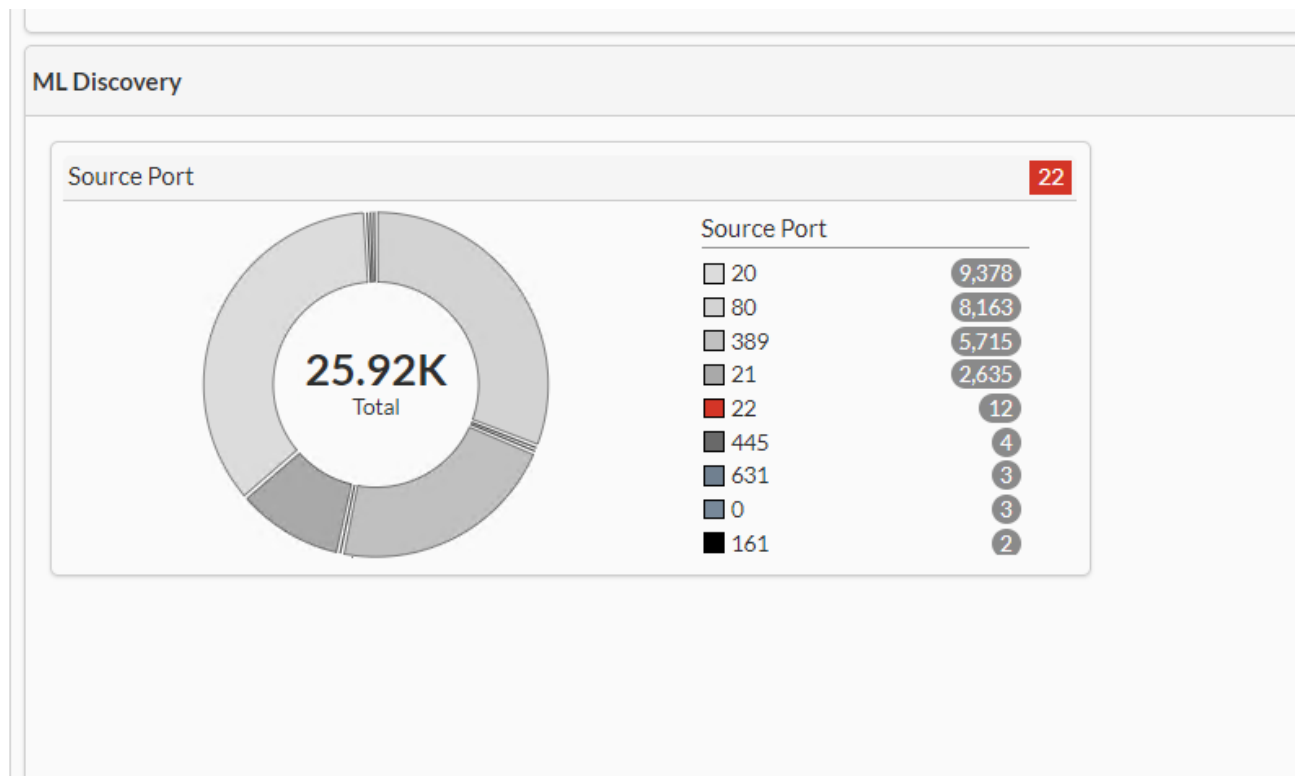
4. Click *Apply*.
The following image is an example of multiple ML discoveries with the same value in the *Anomaly Feature(s)* column. In this scenario, if you add feedback to the first session as Not Anomaly, the other sessions remain as Anomaly.

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

View Session

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

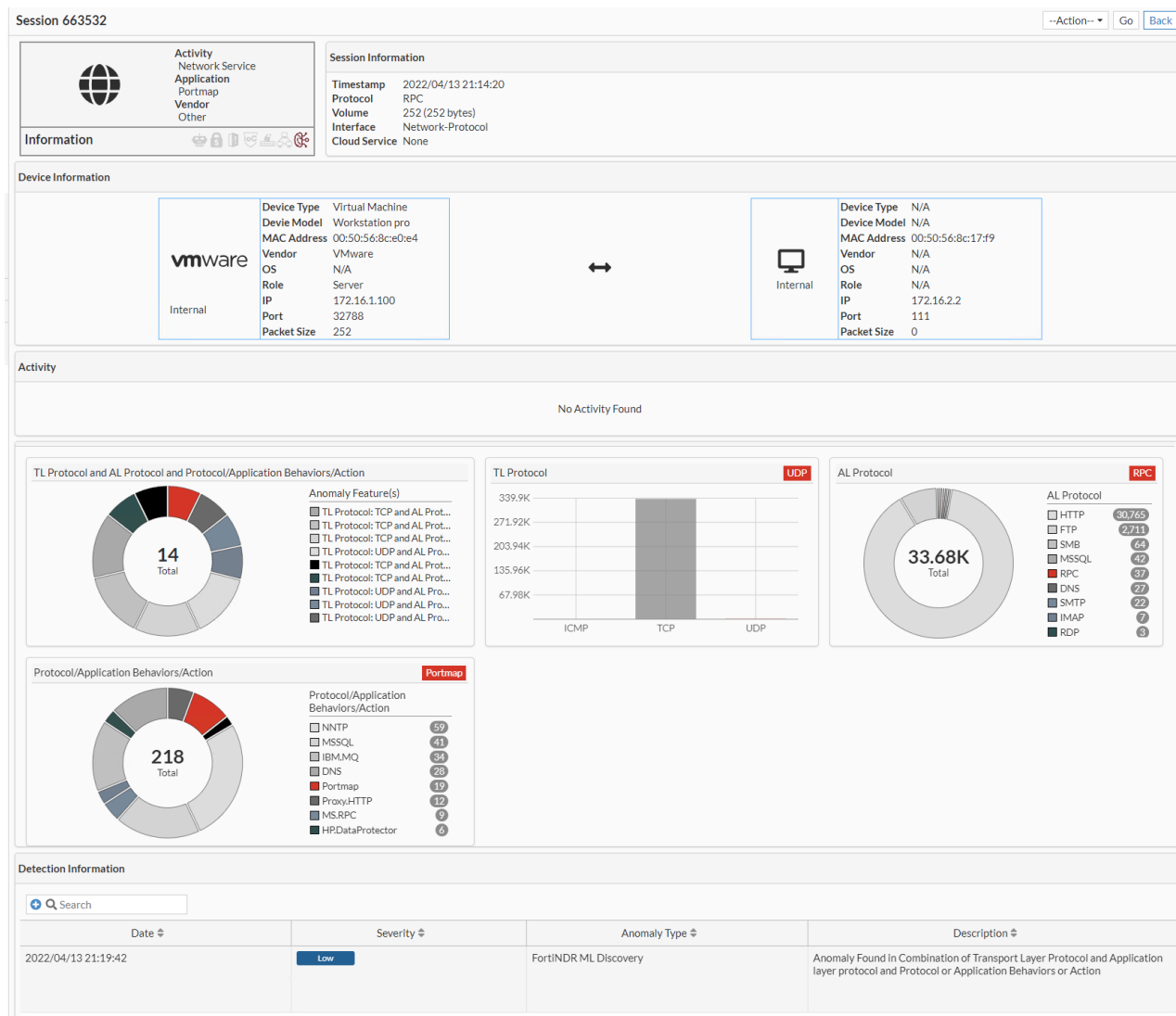
In *ML Discovery* the session shows the distribution of the feature that caused the anomaly. In the image below, the session was flagged because it was trying to use port 22, which is the SSH connection.



If the anomaly is caused by:

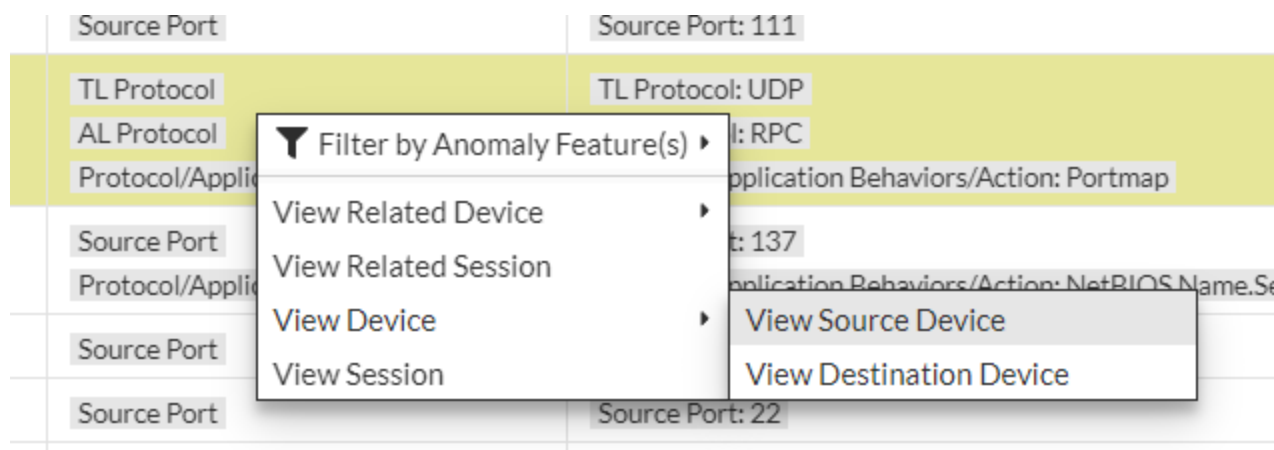
- A new IP joining the network, the distribution graph is not displayed. The new IP address is displayed instead.
- A combination of features the session displays the distribution of the combination as well as the individual distributions. For example, the following anomaly is caused by the combination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

Application Protocol and Protocol/Application Behaviors/Action.

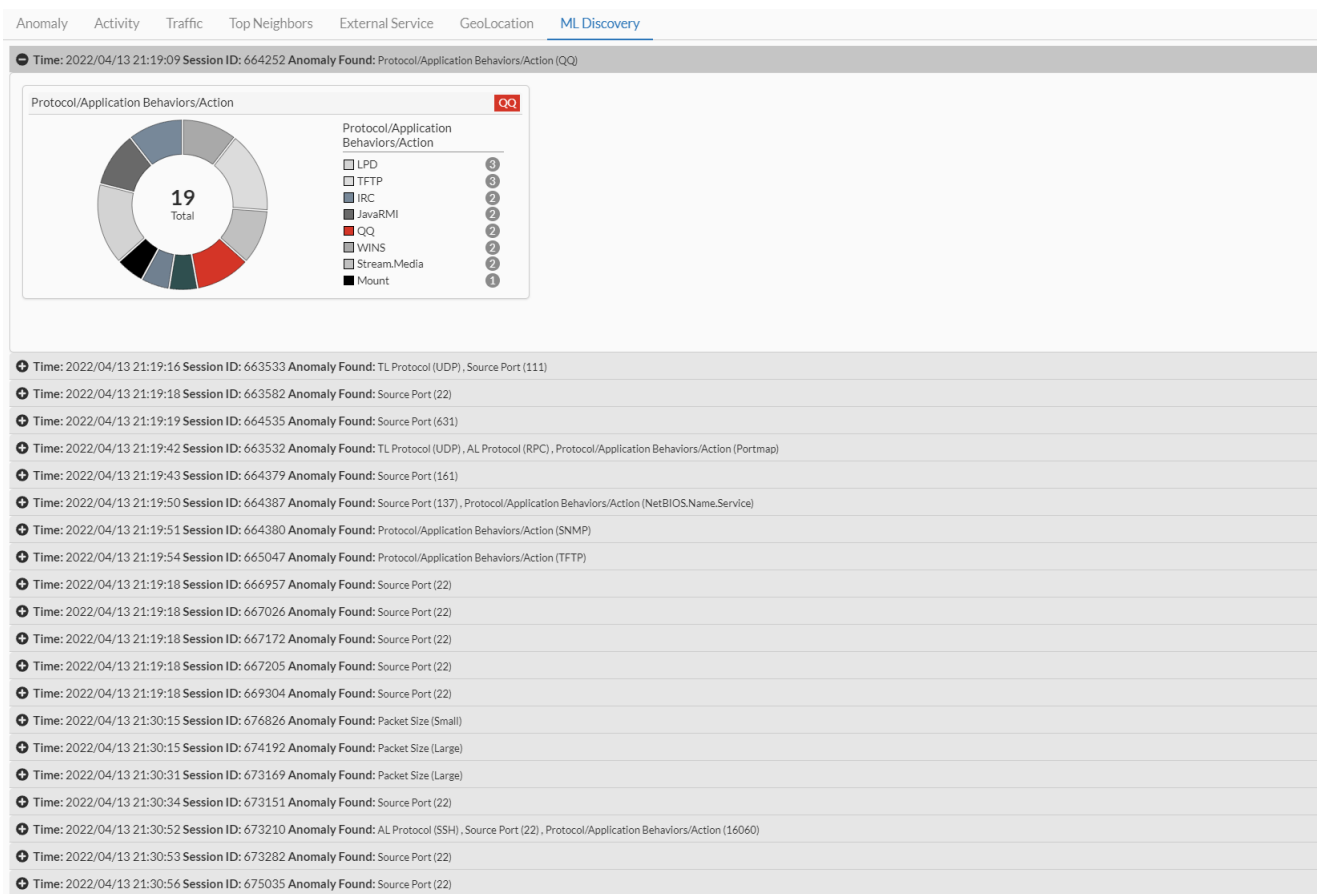


View Source Device and View Destination Device

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



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



Security Fabric

Device Input

The *Security Fabric > Device Input* page displays the FortiGate and FortiSandbox devices that are sending files to FortiNDR.

Supported models:

- FortiGate 5.6 and higher
- FortiSandbox 4.0.1 and higher

The *Device Input* page contains two tabs:

Tab	Description
FortiGate tab	The <i>FortiGate</i> 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.
Other Device tab	The <i>Other Device</i> tab displays FortiSandbox submissions via the FortiNDR API such as FortiSandbox and FortiMail.

The *Device Input* page displays the following information:

Device Name	The device name.
VDOM	The VDOM associated with the device.
IP Address	The device IP.
Connection Type	The connection type.
Authorized	The authorization method.
Status	The connection status.

Network Share

Go to *Security Fabric > Network Share* (also known as *Network File Share*) 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. After the profile is configured, FortiNDR will scan the registered network's share directories.

The *Network Share* page displays the following information:

Name	The Network Share profile name.
Scan Scheduled	Indicates scheduled scan is enabled/disabled.
Type	The Network Share protocol.
Share Path	The Network Share path.
Quarantine	Indicates if quarantine is enabled/disabled.
Enabled	Indicates the Network Share profile is enabled/disabled.
Status	The Network Share configuration status. See Testing connectivity .

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


Creating a Network Share profile


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	<p>Moves password protected files to a designated quarantine location.</p> <hr/> <div>  <p>FortiNDR does not process password protected files.</p> </div> <hr/>
Enable Quarantine Critical Risk Files	<p>Moves detected files with critical risk to a designated quarantine location. This includes:</p> <ul style="list-style-type: none"> • Fileless • Industroyer • Ransomware • Wiper • Worm
Enable Quarantine - High Risk Files	<p>Moves detected files with high risk to a designated quarantine location. This includes:</p> <ul style="list-style-type: none"> • Backdoor • Banking Trojan • Exploit • Infostealer • Proxy • PWS • Rootkit • Trojan
Enable Quarantine - Medium Risk Files	<p>Moves detected files with medium risk to a designated quarantine location. This includes:</p> <ul style="list-style-type: none"> • Clicker • DDoS • Downloader • Dropper • Phishing • Redirector • Virus
Enable Quarantine - Low Risk Files	<p>Moves detected files with low risk to a designated quarantine location. This includes:</p> <ul style="list-style-type: none"> • Application • CoinMiner • Generic Attack • Generic Trojan • SEP • WebShell

Enable Quarantine of Others	<p>Moves other unprocessed files to a designated quarantine location. File types that falls under this category includes:</p> <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	<p>Moves or copies clean files to a location specified in the <i>Network Share Quarantine</i> profile. See, Network Share Quarantine on page 46.</p> <p>The <i>Moving</i> operation is only allowed for the quarantine location when <i>Keep Original File at Source Location</i> disabled.</p> <p>The <i>Copying</i> operation is only allowed for the quarantine location when <i>Keep Original File at Source Location</i> enabled.</p> <p>For information about combining Network Share and Quarantine profiles, see Network Share Quarantine on page 46 > Combining network share and quarantine profiles.</p>
Create a copy of clean files for every scheduled scan at the sanitized location	<p>When enabled, FortiNDR will create a new folder <i><Network Share Profile Name>_<Scan Task ID></i> in the sanitized location for each scheduled scan.</p> <p>When disabled, FortiNDR will overwrite the sanitized location with the clean files from the latest scan.</p>
<div>  <p>Enabling this option will increase the size of the Network Share location.</p> </div>	
Create placeholder files for malicious/Suspicious/Other files at sanitized location	<p>Adds a placeholder file in the sanitized location. The filename pattern of the placeholder file will be <i><filename>.<severity>.txt</i>. This helps maintain the file structure of the original network in the share folder.</p>
Enable Force Rescan	<p>When enabled, FortiNDR will not use cache detection even if the files are previously scanned.</p>

6. Click OK.

Testing connectivity

To validate the Network Share configuration:

- Go to *Security Fabric > Network Share* and select a profile.
- In the toolbar, click *Test Connection* to validate the Network Share configuration. A green checkmark appears in the *Status* next to a valid connection.



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

Scanning a network location

To trigger a scan:

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



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

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



You can use a REST API call to start a scan. See, [Start Network Share scan](#).

Scheduling a scan

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



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

To schedule a scan:

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

Total

The total number of files scanned.

Start Time	The date and time the scan started.
End Time	The date and time the scan completed.
Scan Finished	The scan progress as a percentage.
Critical Risk	The number of <i>Detected/Quarantined</i> critical risk files.
High Risk	The number of <i>Detected/Quarantined</i> critical high files.
Medium Risk	The number of <i>Detected/Quarantined</i> medium risk files.
Low Risk	The number of <i>Detected/Quarantined</i> critical low files.
Clean	The number of clean files.
Others	The number of <i>Detected/Quarantined</i> other files.
Scan Status	The scan status as a string.

3. Click the numbers to view the detection information for the samples that belong to the category.
4. Click the link in the column to view the detected and quarantined files.
 - Select a sample in the list then click *View Sample Detail*.
 - Click *Back* to return to the *Scan Details*.
5. Click *Back* to return to the *Network Share* pane.

Scanning Zip files

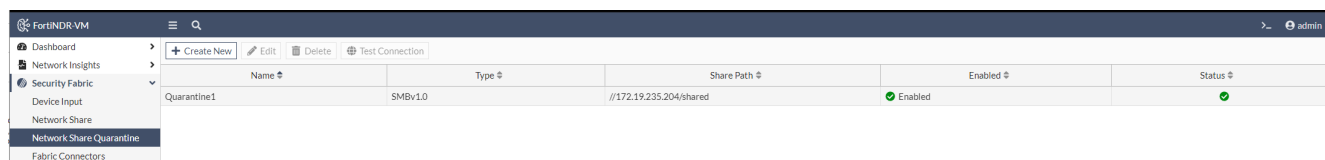
FortiNDR can extract and process Zip files up to 10 levels. When any of the files inside the Zip file is detected, the whole zip file will be marked as malicious.



FortiNDR does not process password-protected zip files.

Network Share Quarantine

Go to *Security Fabric > Network Share Quarantine* to configure multiple quarantine profiles for different Network Share locations. You can use different configurations to specify detection files with different levels to separate quarantine locations.



Quarantined files

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

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

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

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

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

Example:

```
Network Share FileID: 351640
SID: 3 (Share ID)
JID: 44 (Job ID)
FileID: 1198941 (File ID)
File Name: sample.vsc
Device: testshared
URL: //172.16.2.100/shared2/2/sample.vsc
MD5: 31e06f25de8b5623c3fdaba93ed2edde
Virus Name: W32/Wanna.A!tr.ransom
DelOriginalFile: Success
```

Creating a quarantine profile

To create a quarantine profile:

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

Status	Click to <i>Enable</i> or <i>Disable</i> .
Quarantine Name	Enter a name for the quarantine profile.
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.
Confirm Password	Re-enter the password.

Status

☒ Enable ☐ Disable

Mount Type

SMBv1.0

Quarantine Name

Quarantine1

?

Server IP

172.19.235.20

?

Share Path

/quarantine1

?

Username

tester1

Password

.....

Change

Confirm Password

.....

Change

☐ Keep Original File At Source Location

Description

- (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 49](#).

- (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

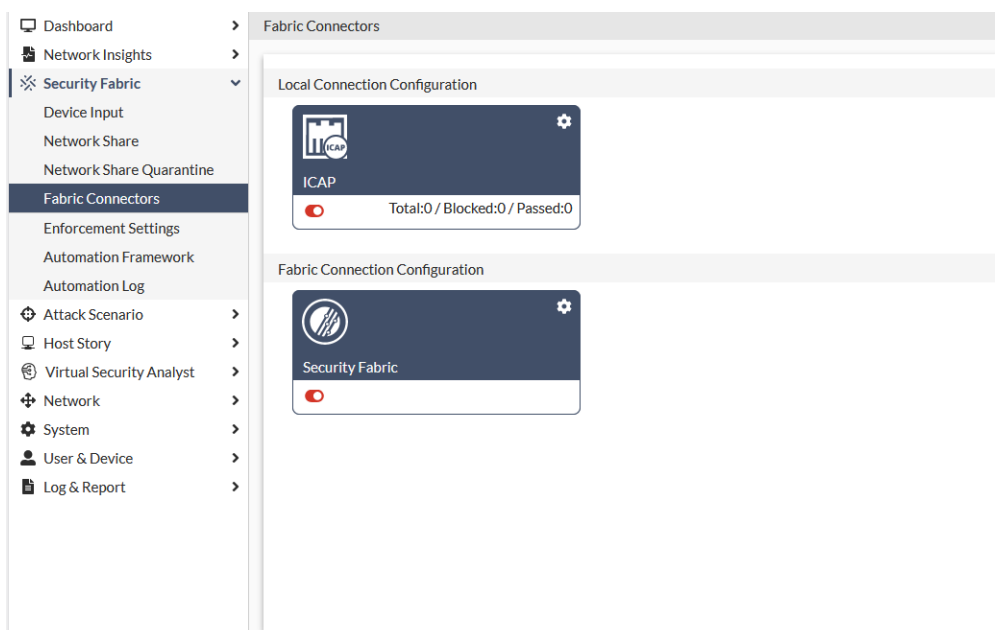
Keep original file at source location	Move/Copy clean files to sanitized location	Effect
<i>Disabled</i>	<i>Enabled</i>	<p>or copy the files.</p> <ul style="list-style-type: none"> Move the clean files to the Network Share Qaurantine. FortiNDR attempts to delete the original files.



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

Fabric Connectors

Security Fabric > Fabric Connectors to connect FortiNDR 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 attacks 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.
 For more information, see [ICAP](#) in the *FortiOS Administration Guide*.
2. In FortiNDR, configure the ICAP server.

To enable ICAP in FortiNDR:

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

Status	
Enable ICAP Connector	<input checked="" type="checkbox"/>
Connection	
Interface	port1 (MGMT)
Port	1344
SSL Support	<input checked="" type="checkbox"/>
SSL Port	11344
Configuration	
Realtime FortiNDR Scan	<input checked="" type="checkbox"/>
Realtime FortiNDR Scan Timeout at	10 second(s) (Between 1 to 20 second(s), Default: 10 seconds)
Confidence Level	
Quarantine Confidence level equal and above	70 % Medium High

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.

The screenshot displays the FortiNDR configuration interface. On the left, a sidebar menu includes options like Dashboard, Network Insights, Security Fabric, and various system settings. The 'Security Fabric' section is expanded, and 'Fabric Connectors' is the active selection. The main content area shows the 'Status' of the Security Fabric connector, which is currently 'Enabled'. Below this, the 'Fabric Device Settings' are configured with the following values: FortiGate Root IP is 10.0.0.173, TCP Port is 8013, FortiNDR IP is 10.0.0.94, and TCP Port is 443. At the bottom of the configuration window, there are 'OK' and 'Cancel' buttons.

Enforcement Settings

Enforcement Settings provide 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 detections 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 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.

Creating enforcement profiles

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 and then click **OK**.

Profile Name	Enter a name for the profile.
Enforcement Policy	
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> • <i>NDR: Machine Learning Detection</i>
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> .
Additional Settings	
Allow List	Click the plus sign (+) to 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.

General Settings

Profile Name

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: Machine Learning Detection ☐

Malware Risk Level Critical

Malware Confidence Level 80 Medium High

Additional Settings

Allow List +

OK Cancel



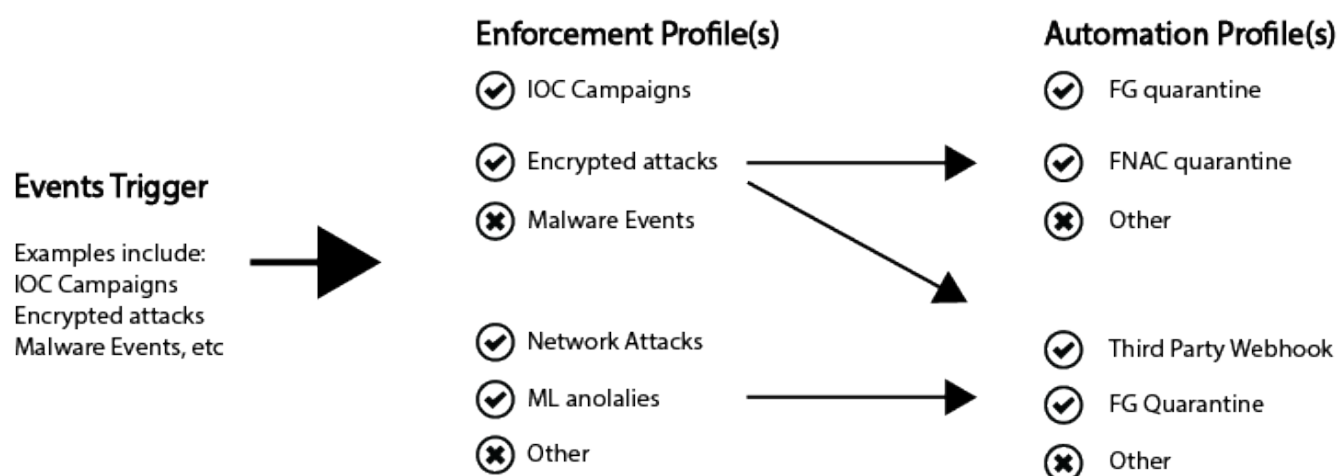
For NDR detection *Severity Level* and *Malware risk level*, severity is inclusive of higher severity levels. For example, if *High* is selected, the enforcement profile will match both *HIGH* and *CRITICAL* events.

Automation Framework

Go to *Security Fabric > Automation Framework* to create single enforcement profile that 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 *Automation Framework* settings:

Automation Framework	
Profile Name	Enter a name for the profile.
Enable	Click to enable or disable the framework.
Enforcement Profile	Click to select an Enforcement Settings profiles.
Action	Select one of the following actions: <ul style="list-style-type: none"> • <i>FortiGate Quarantine</i> • <i>FortiNAC Quarantine</i> • <i>FortiSwitch Quarantine via FortiLink</i> • <i>Generic Webhook</i>

The screenshot shows the 'Automation Framework' configuration window. Under 'Automation Framework', there are fields for 'Profile Name', 'Enable' (a toggle switch), 'Enforcement Profile' (with a '+' icon), and 'Action' (a dropdown menu set to 'FortiGate Quarantine'). Below this is the 'FortiGate Quarantine Settings' section. It includes a 'Source' dropdown with 'Fabric Device' and 'Sniffer' options. The 'API Key' field is masked with dots and has a 'Change' button. Other fields include 'IP' (0.0.0.0), 'Port' (443), 'VDOM' (root), 'Webhook Name for Execution', and 'Webhook Name for Undo'. A 'Test Current Configuration' button is at the bottom. At the very bottom of the window are 'OK' and 'Cancel' buttons.

4. Configure the quarantine settings. These settings will vary depending on the *Action* setting.

Manage FortiGate Settings and FortiSwitch Quarantine via FortiLink.

Manage FortiGate Settings and FortiSwitch Quarantine Settings

Source

- **Fabric Device:** If the source of detection came from OFTP, the enforcement is only executed to a matching automation profile with a matching IP address and VDOM.
- **Sniffer:** If the source of detection came from a sniffer, the enforcement is adapted by all profiles where *Trigger Source* is *Sniffer*. Since detection sourced from sniffer does not contain information about which fabric device monitors the infected IP address, it is your responsibility to specify the correct device IP address and VDOM.

API Key

Enter the device API key

IP

Enter the device IP address.

Port

Enter the device port number.

VDOM

Enter the VDOM name.

WebHook Name for Execution

Select the FortiGate webhook for execution action, such as `ip_blocker`.

WebHook Name for Undo

Select the FortiGate webhook for undo action, such as `ip_unblocker`.

FortiNac Quarantine

FortiNac Quarantine Settings

API Key

Click *Change* to update the API key.

IP

Enter the FortiNac IP address.

Port

Enter the FortiNac port number.

Generic Webhook

Webhook Execution Settings	
URL	Enter the webhook URL.
Method	Select <i>POST</i> , <i>PUT</i> , <i>GET</i> , <i>PATCH</i> or <i>DELETE</i> .
Header	Click the plus sign (+) and enter a value of the authorization key.
HTTP Body Template	Enter the HTTP Body Template.
Webhook Undo Settings	
URL	Enter the webhook URL.
Method	Select <i>POST</i> , <i>PUT</i> , <i>GET</i> , <i>PATCH</i> or <i>DELETE</i> .
Header	Click the plus sign (+) and enter a value of the authorization key.
HTTP Body Template	Enter the HTTP Body Template.

- Click *Test Current Configuration* to validate the settings. This option is displayed when *FortiGate Quarantine* and *FortiSwitch Quarantine via FortiLink* are selected.
- Click *OK*.

FortiGate quarantine webhook setup example

To create an automation profile for *FortiGate Quarantine* 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:

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

Security Fabric	Read/Write
User & Device	Read/Write
Log & Report	Read/Write
System	Read/Write
Permit usage of CLI diagnostic commands	Enable

New Admin Profile

Name:

Comments: 0/255

Access Permissions

Access Control	Permissions	Set All
Security Fabric	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
FortiView	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
User & Device	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Firewall	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="button" value="Custom"/>	
Log & Report	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="button" value="Custom"/>	
Network	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="button" value="Custom"/>	
System	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="button" value="Custom"/>	
Security Profile	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="button" value="Custom"/>	
VPN	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
WAN Opt & Cache	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
WiFi & Switch	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	

Permit usage of CLI diagnostic commands: ☒

☐ Override Idle Timeout



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.

	Trusted Hosts	IPv6 Trusted Host	Profile	Type	Two-factor Authentication
Administrator					
REST API Admin					
SSO Admin					
admin			super_admin	Local	Disabled
faz			super_admin	Local	Disabled
			super_admin	Local	Disabled
REST API Administrator					
fnfn			super_admin	API Key	

3. Configure the administrator settings:

Username

The username of the administrator.

Do not use the characters `<` `>` `()` `#` `"` `'` in the administrator username. Using these characters in an administrator username might have a cross site scripting (XSS) vulnerability.

Administrator Profile	Where permissions for the REST API administrator are defined. A REST API administrator should have the minimum permissions required to complete the request.
PKI Group	Certificate matching is supported as an extra layer of security. Both the client certificate and token must match to be granted access to the API.
CORS Allow Origin	Cross Origin Resource Sharing (CORS) allows third-party web apps to make API requests to the FortiGate using the token.
Trusted Hosts	The following can be used to restrict access to FortiGate API: Multiple trusted hosts/subnets can be configuredIPv6 hosts are supportedAllow all (0.0.0.0/0) is not allowed You need your Source Address to create the trusted host.

New REST API Admin

Username

Comments 0/255

Administrator profile

PKI Group ☒

i REST API clients must use client certificate authentication. Only certificates from this PKI group will be authorized.

CORS Allow Origin ☐

Restrict login to trusted hosts

Trusted Hosts ☒

- Save the generated *New API key*. You will need this 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 StitchCLI Script* section, enter the following script. Substitute `root` with a VDOM.


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

New Automation Stitch

Name


Status Enabled Disabled

Trigger




Incoming Webhook


Action



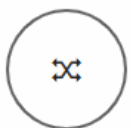
CLI Script




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*.

- 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 v7.0.1

Stitch Trigger Action						
+ Create New View Delete Clone <input type="text"/>						
Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
Compromised Host						
FortiOS Event Log						
Incoming Webhook						
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

default

+

×

Action

FortiGate Quarantine

Manage FortiGate Settings

Source

Fabric Device Sniffer

API Key

Change

IP

Port

VDOM

Webhook Name for Execution

Webhook Name for Undo

Test Current Configuration

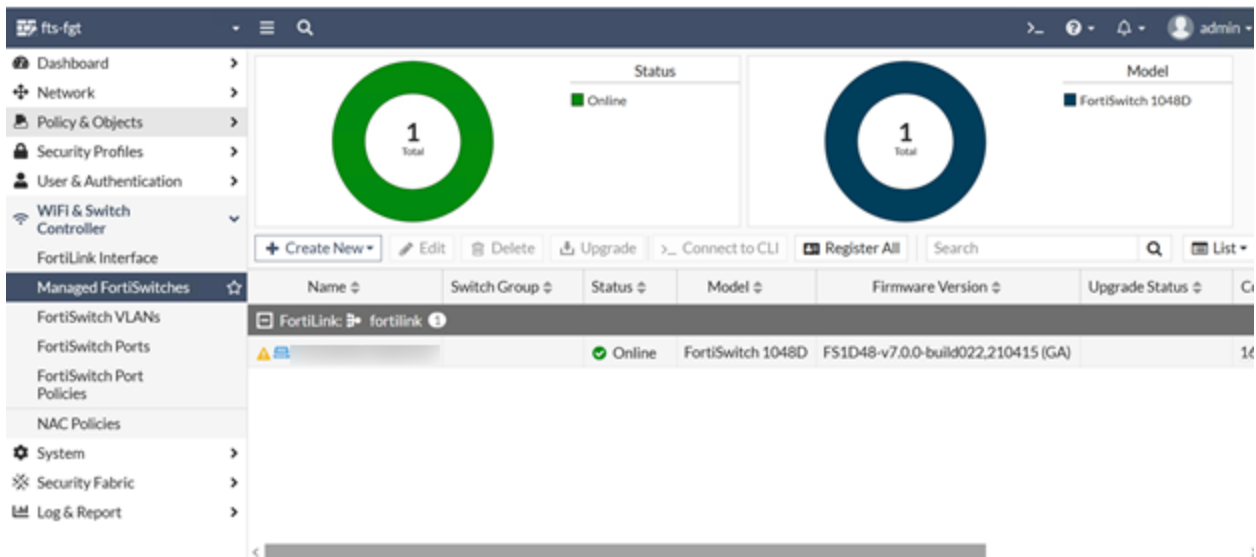
OK

Cancel

FortiSwitch quarantine setup example

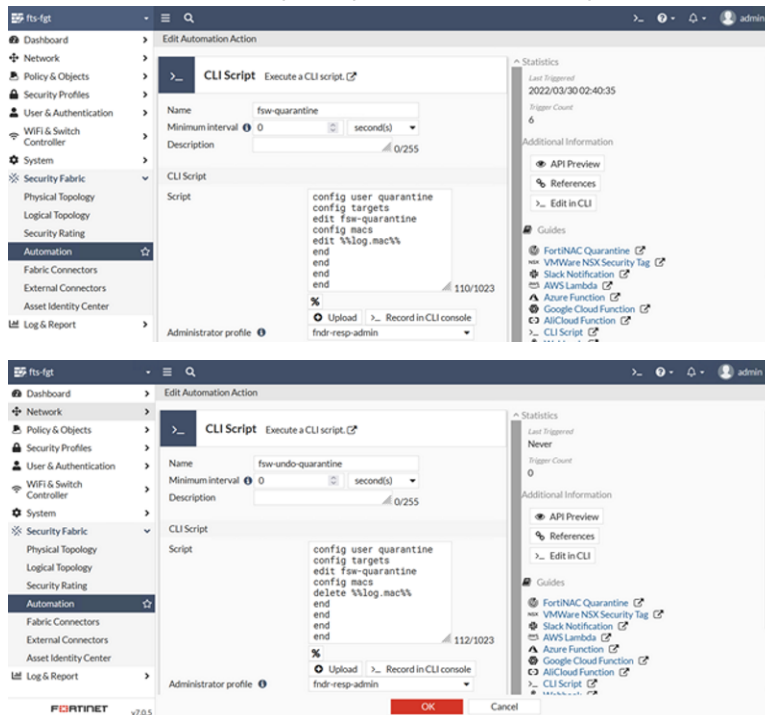
FortiNDR supports quarantining devices that are connected to a FortiSwitch which is managed by FortiGate. FortiSwitch is connected to a FortiGate and is configured in FortiLink mode. FortiNDR will utilize FortiGate's incoming webhook to provide the device's MAC address for quarantine/undo quarantine.

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 57](#). 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.

Automation Framework

Profile Name: test-fsw

Enable: ☒

Enforcement Profile: default

Action: FortiSwitch Quarantine via FortiLink

FortiSwitch Quarantine Settings

Source: Fabric Device **Sniffer**

API Key: ***** [Change](#)

IP: 172.19.235.201

Port: 443

VDOM: root

Webhook Name for Execution: fsw-quarantine

Webhook Name for Undo: fsw-undo-quarantine

[Test Current Configuration](#)

[OK](#) [Cancel](#)

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

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)		Device: e4-43-4b-80-42-da MAC Address: e4-43-4b-80-42-da IP Address: 172.19.140.2 DHCP Lease expires on 2022/04/05 22:52:32 Online Interfaces: default.fortilink (default) Hardware: Fortinet / FortiGate OS: FortiOS + Firewall Device Address + Firewall IP Address + Remove Quarantine Ban IP	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	

4. Click OK.

FortiNAC quarantine setup example

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

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

To setup FortiNAC quarantine on FortiNDR:

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

The screenshot shows the FortiNAC web interface. The left sidebar contains a navigation menu with items like Dashboard, Users & Hosts, Administrators, Guests & Contractors, Account Requests, Registration Requests, User Accounts, Hosts, Adapters, Applications, Endpoint Fingerprints, Profiled Devices, Device Profiling Rules, FortiGate Sessions, Locate Hosts, Manage Hosts and Ports, Send Message, Network, and Policy & Objects. The main content area displays a table of 'Admin Users' with columns for User ID, First Name, Last Name, Admin Profile, and Auth Type. The 'admin' user is selected. To the right, the 'Modify User' form is open, showing fields for User Information, Authentication Type, Admin Profile, and contact details. The 'Allow REST API Access for this Admin User' checkbox is checked, and the 'REST API Access Token' is displayed as '172.19.235.0/24'.

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

The screenshot shows the 'Automation Framework' configuration page in FortiNDR. The 'Profile Name' is 'test-fnac', 'Enable' is checked, 'Enforcement Profile' is 'default', and 'Action' is 'FortiNac Quarantine'. The 'FortiNac Quarantine Settings' section shows 'API Key' as '*****', 'IP' as '172.19.235.246', and 'Port' as '8443'. The 'OK' button is highlighted in red.

- 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

default

+

✕

Action

Generic Webhook

▼

Webhook Execution Settings

URL

Method

POST

PUT

GET

PATCH

DELETE

Header

Content-Type

✕

Authorization

✕

+

HTTP Body Template

Webhook Undo Settings

URL

Method

POST

PUT

GET

PATCH

DELETE

Header

Authorization

✕

Content-Type

✕

+

HTTP Body Template

OK

Cancel

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.

Dashboard	+ Add to Allow List	Manual Execution	Undo Action	View Details	Search						
Network Insights	Initial Action time #	Target IP #	Target MAC #	Violations #	Action Type #	Automation Profile Name #	Enforcement Profile Type #	Action Executed #	Post Action #	Status #	
Security Fabric	Device Intel	2022/04/16 21:10:30	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
	Network Share	2022/04/16 21:10:30	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 21:10:30	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 Connections	2022/04/16 21:10:30	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 21:10:30	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 Frameworks	2022/04/16 21:10:30	18.2.3.188	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 21:10:30	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 Scenario		2022/04/16 21:10:30	18.1.3.16	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 21:10:30	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 21:10:30	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 21:10:29	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
Systems		2022/04/16 21:10:29	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 21:10:29	18.2.3.117	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 21:10:29	18.1.2.51	00:50:56:8c:b3:db	45	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:29	None	Executed

Violation details

+ Add to Allow List	Manual Execution	Undo Action	View Details	Search
Initial Action time #	Target IP #	Target MAC #	Violations #	Action #
2022/04/16 21:10:30	18.1.2.120	00:50:56:8c:b3:db	38	Generic V
2022/04/16 21:10:30	18.2.6.255	00:50:56:8c:b3:db	46	Generic V
2022/04/16 21:10:30	18.1.8.112	00:50:56:8c:b3:db	20	Generic V
2022/04/16 21:10:30	18.1.7.85	00:50:56:8c:b3:db	7	Generic V
2022/04/16 21:10:30	18.2.12.106	00:50:56:8c:b3:db	19	Generic V
2022/04/16 21:10:30	18.2.3.188	00:50:56:8c:b3:db	15	Generic V
2022/04/16 21:10:30	18.1.12.122	00:50:56:8c:b3:db	15	Generic V
2022/04/16 21:10:30	18.1.3.16	00:50:56:8c:b3:db	18	Generic V
2022/04/16 21:10:30	18.1.3.222	00:50:56:8c:b3:db	10	Generic V
2022/04/16 21:10:30	18.2.2.171	00:50:56:8c:b3:db	42	Generic V
2022/04/16 21:10:29	18.1.8.123	00:50:56:8c:b3:db	37	Generic V
2022/04/16 21:10:29	18.1.3.50	00:50:56:8c:b3:db	7	Generic V
2022/04/16 21:10:29	18.2.3.117	00:50:56:8c:b3:db	10	Generic V

Log Violation Details				
File Violation		Session Violation		
View Session Detail Search				
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 go 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 177](#).
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.

FortiNDR Settings	
<input checked="" type="checkbox"/> Enable	
Server IP:	<input type="text" value="10.59.26.252"/>
Token:	<input type="text" value="....."/>
Rating Timeout (Seconds):	<input type="text" value="5"/>
Uploading Timeout (Seconds):	<input type="text" value="2"/>
Maximum File Size (KB):	<input type="text" value="2048"/>
<input type="button" value="OK"/> <input type="button" value="Test Connection"/>	

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

Scan Profile

Pre-Filter | VM Association | Advanced

Process the following selected file types.

Executables <input checked="" type="checkbox"/>	PDF documents <input checked="" type="checkbox"/>	Office documents <input checked="" type="checkbox"/>	Flash files <input checked="" type="checkbox"/>	Web pages <input checked="" type="checkbox"/>
Compressed archives <input checked="" type="checkbox"/>	Android files <input checked="" type="checkbox"/>	Mac files <input checked="" type="checkbox"/>	Linux files <input checked="" type="checkbox"/>	URL detection <input checked="" type="checkbox"/>
User defined extensions <input checked="" type="checkbox"/>				

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 <input type="checkbox"/>	dll <input type="checkbox"/>	htm <input type="checkbox"/>	js <input type="checkbox"/>	pdf <input type="checkbox"/>	swf <input type="checkbox"/>	url <input type="checkbox"/>	archive <input type="checkbox"/>
---------------------------------	------------------------------	------------------------------	-----------------------------	------------------------------	------------------------------	------------------------------	----------------------------------

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 <input checked="" type="checkbox"/>	Trusted Vendor <input type="checkbox"/>	Trusted Domain <input type="checkbox"/>
------------------------------------------------------	-----------------------------------------	-----------------------------------------

Apply

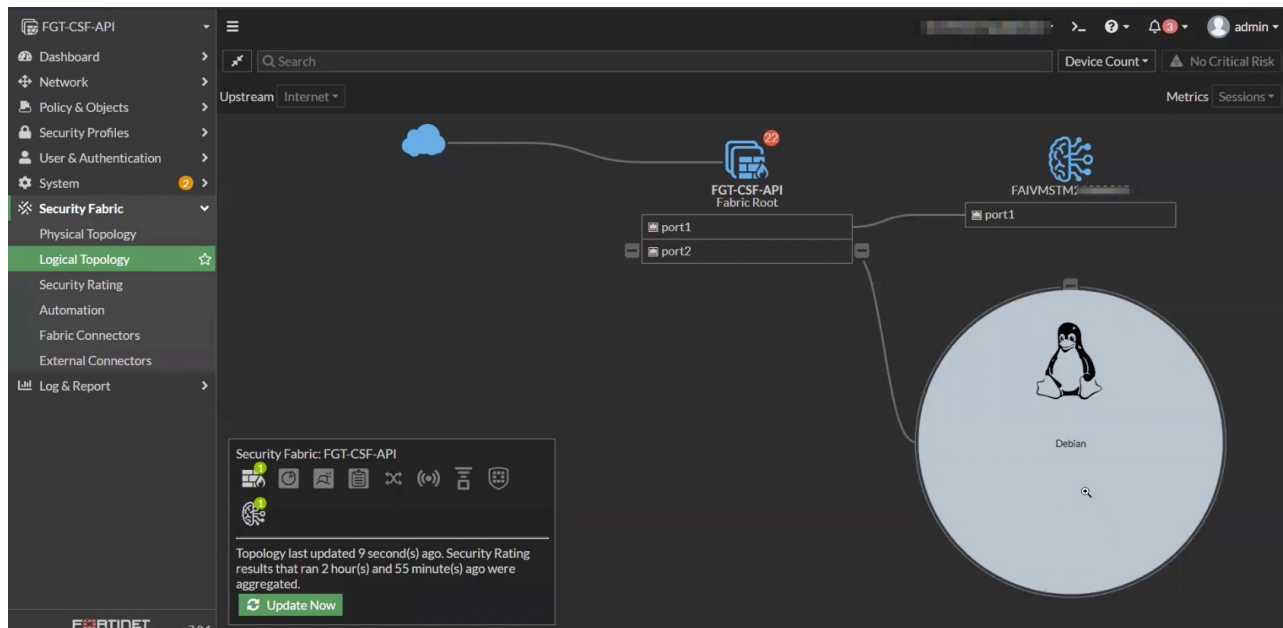
FortiGate inline blocking (FOS 7.0.1 and higher)

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 50](#).
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

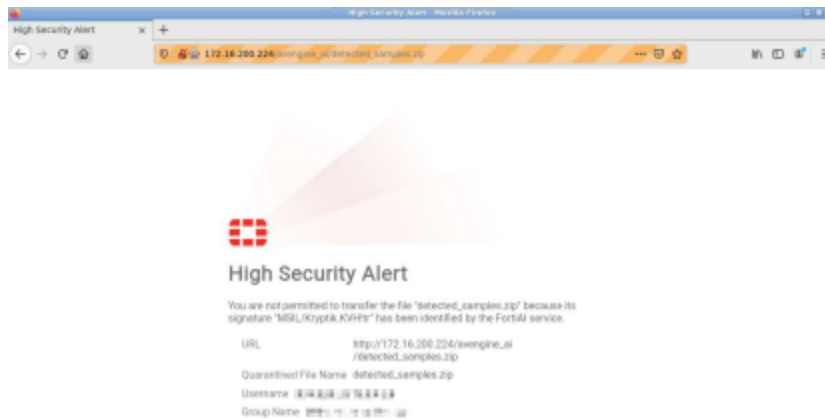
Config antivirus profile
    edit fai << profile name
        Set feature-set proxy
        Config http << or another protocol such as FTP, SMTP, IMCP, CIFS, etc.
        Set fortindr block << or monitor
    End
Next
End
```

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

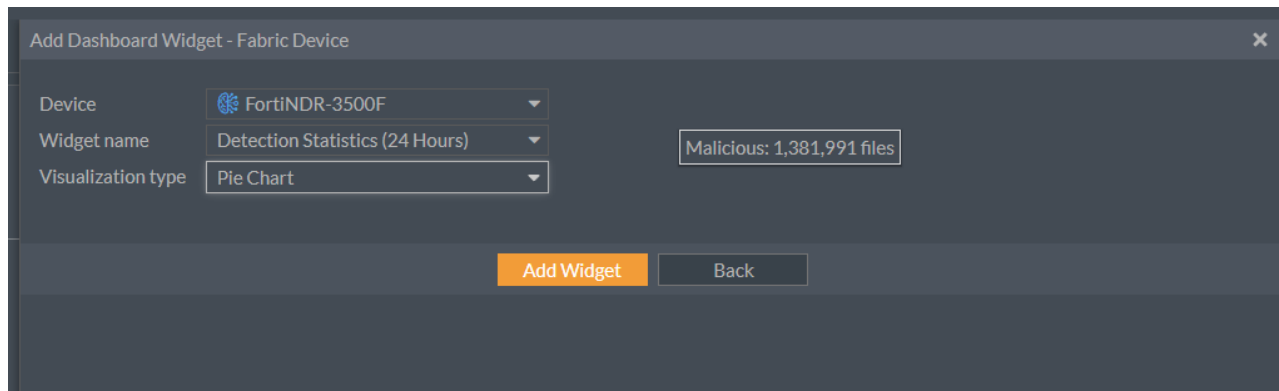
- Similar to the FortiGate AV profile, a browser replacement message is displayed if a virus is found. In FortiOS, the message is called FortiNDR block page, and is a customizable HTML page.



- 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.

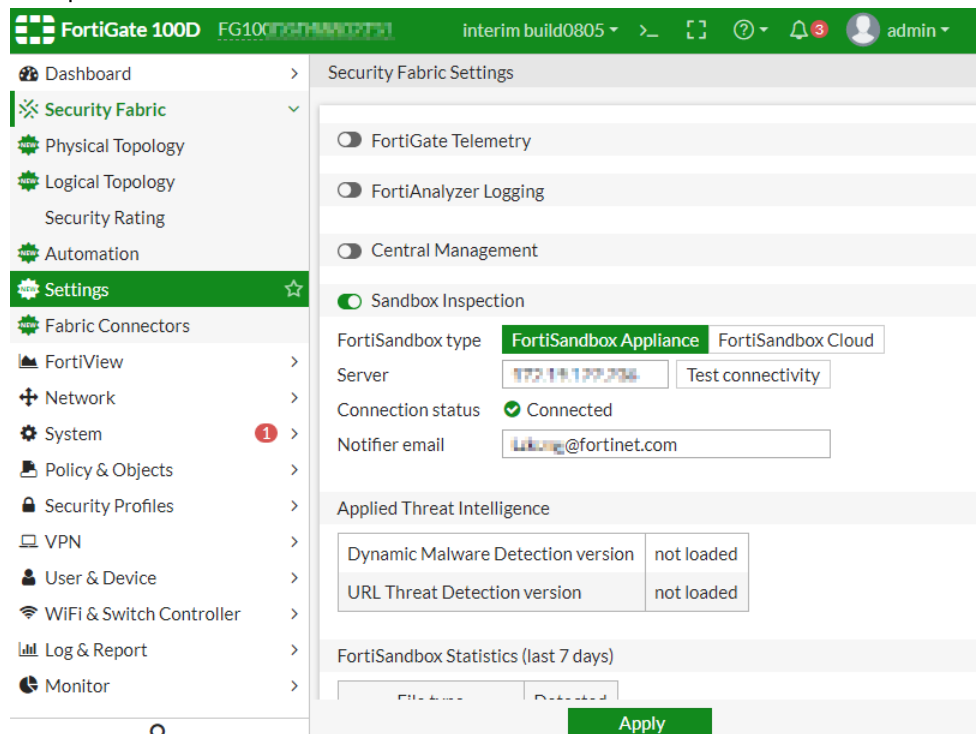
FortiGate cannot receive files from both FortiSandbox and FortiNDR simultaneously. If your FortiGate has FortiSandbox configured, consider using another mode.

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.

FortiGate 100D FG100D5C10002751 interim build0805 admin

Edit AntiVirus Profile default

Name: default

Comments: Scan files and block viruses. 29/255

Scan Mode: Quick Full

Detect Viruses: Block Monitor

Inspected Protocols

- HTTP ☒
- SMTP ☒
- POP3 ☒
- IMAP ☒
- MAPI ☒
- FTP ☒
- SMB ☒

APT Protection Options

Content Disarm and Reconstruction ☒

Original File Destination: FortiSandbox File Quarantine Discard

Treat Windows Executables in Email Attachments as Viruses ☐

Send Files to FortiSandbox Appliance for Inspection: None Suspicious Files Only All Supported Files

Do not submit files matching types: +

Do not submit files matching file name patterns: +

Use FortiSandbox Database ☐

Include Mobile Malware Protection ☒

Virus Outbreak Prevention

Use FortiGuard Outbreak Prevention Database ☐

Use External Malware Block List ☐

Apply

3. Apply AV profile in the firewall policy.

FortiGate 100D FG100D5C10002751 interim build0805 admin

Policy & Objects

IPv4 Policy

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.

FortiGate 100D FG100D5C10002751 interim build0805 admin

Security Fabric

ID	Host Name	VDOM	IP Address	Malware Version	URL Version	Authorized
8	FG100D5C10002751		172.19.222.201	0	0	Enabled
10	FG100D5C10002751:root	root	172.19.222.201	0	0	Enabled
11	FGT80F474700000000		172.19.222.208	0	0	Enabled

3 | Updated: 14:50:58

5. Check the FortiNDR processed traffic. See [FortiGate integration \(integrated mode with FOS 5.6 and higher\)](#) on page 71.

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.



In Center mode, FortiNDR collects and presents all Attack Scenarios reported from every Sensor connected to this Center.

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.

FortiNDR-VM

admin

Dashboard

Network Insights

Security Fabric

Attack Scenario14

Attack Scenario Summary

Ransomware1

Worm Activity1

Data Leak1

Exploit1

Banking Trojan1

Sophisticated

Scenario Heuristic1

Cryptojacking1

Backdoor1

Botnet1

DoS1

Application1

Web Shell1

SEP1

Generic Trojan1

Rootkit

Phishing

Fileless

Wiper

Industroyer

Host Story32

Virtual Security Analyst

Netflow

Network

View Detail

Attack Scenario

Incident Counts

LowScenario Types: 5Total Event Counts: 46

Cryptojacking36

Application5

Web Shell4

SEP1

Phishing0

MediumScenario Types: 4Total Event Counts: 127

Sophisticated0

Scenario Heuristic1

DoS2

Generic Trojan124

HighScenario Types: 6Total Event Counts: 30

Data Leak3

Exploit7

Banking Trojan4

Backdoor14

Botnet2

Rootkit0

CriticalScenario Types: 5Total Event Counts: 17

Ransomware6

Worm Activity11

Fileless0

Wiper0

Industroyer0

0%

Scenario types

FortiNDR can detect the following attack scenarios:

Scenario	Severity	Description
Cryptojacking	Low	Cryptojacking is a type of cybercrime where a malicious actor

Scenario	Severity	Description
		uses a victim's computing power to generate cryptocurrency.
Application	Low	A broad category of software that might download and install additional, unwanted software that could perform activities not approved or expected by the user.
Web Shell	Low	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.
SEP	Low	Attackers use Search Engine Poisoning to take advantage of your rankings on search engine result pages.
Phishing	Low	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.
Sophisticated	Medium	Malware that contains more than one attack scenario.
Scenario Heuristic	Medium	Scenario heuristic identifies applications or software that demonstrates an array of suspicious traits.
DoS	Medium	This can access connection handling remotely, perform denial of service, or distributed DoS.
Generic Trojan	Medium	Any malicious computer program which misleads users of its true intent.
Banking Trojan	High	Malicious software that can access confidential information stored or processed through online banking systems.
Backdoor	High	This can give a hacker unauthorized access and control of your computer.
Data Leak	High	A data leak is when sensitive data is exposed physically on the Internet where malicious actors can access it.
Rootkit	High	Software tools that enable an unauthorized user to get control of a computer system without being detected.
Exploit	High	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.
Botnet	High	A botnet is a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker.
Ransomware	Critical	Malicious software that can block access to a computer system until money is paid.
Fileless	Critical	A variant of computer-related malicious software that is exclusively a computer memory-based artifact.

Scenario	Severity	Description
Wiper	Critical	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.
Industroyer	Critical	A malware framework originally designed to deliver specific cyberattacks on power grids. The recent generation of this malware has also started to target industrial control systems.
Worm Activity	Critical	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.

FortiNDR-VM

admin

Dashboard

Network Insights

Security Fabric

Attack Scenario

Attack Scenario Summary

Industroyer

Wiper

Fileless

Worm Activity

Ransomware

Rootkit

Botnet

Backdoor

Banking Trojan

Exploit

Data Leak

Generic Trojan

DoS

Scenario Heuristic

Sophisticated

Phishing

SEP

Web Shell

Application

Cryptojacking

Host Story

Virtual Security Analyst

Network

System

User & Authentication

Log & Report

Discovery Date	Victim (Infected Host) IP	Malware family	Device Type	Event Count
2022/04/13 13:36:10	10.10.10.23	Dreambot	Sniffer	1
2022/04/13 13:35:27	10.10.10.23	Dreambot	Sniffer	1
2022/04/13 13:35:25	10.10.10.23	Dreambot	Sniffer	1
2022/04/13 13:35:08	10.10.10.23	NSIS	Sniffer	1
2022/04/13 13:35:06	10.10.10.23	Generic	Sniffer	1
2022/04/13 13:34:52	10.10.10.23	StartServ	Sniffer	1
2022/04/13 13:34:49	10.10.10.23	NSIS	Sniffer	1

Attack Timeline at Host 10.10.10.56

Downloader

Infostealer

Worm

JS/Agent.NOI

0 days 0 hours 0 minutes 0 seconds

HTML | Downloader | Virut

Attacker IP: 10.10.10.4

Victim IP: 10.10.10.56

W32/Dloader.ADC!tr

0 days 0 hours 0 minutes 3 seconds

PE | Infostealer | Ekstak

Attacker IP: 10.10.10.4

Victim IP: 10.10.10.56

W32/Bundpil.AA!tr

0 days 0 hours 0 minutes 6 seconds

PE | Worm | Alien

Attacker IP: 10.10.10.4

Victim IP: 10.10.10.56

W32/Bundpil.AA!tr

Discover Date 2022/04/13 12:46:10

MD5 6a7edcca4a1154dde36d2e79d9224a08

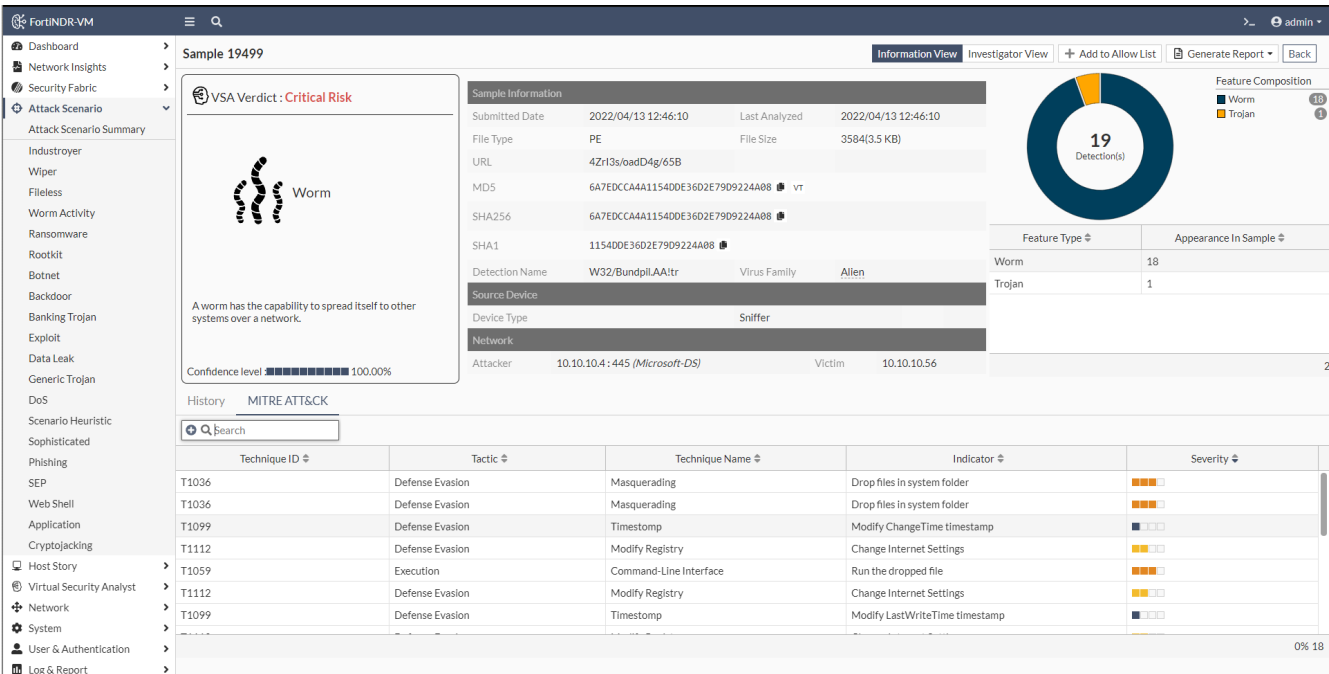
Remote IP 10.10.10.4

Protocol SMB

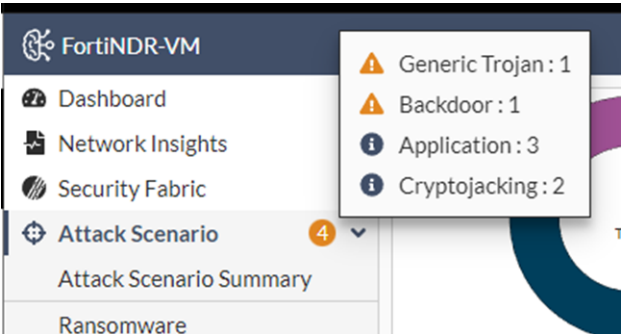


You might see the same IP address multiple times. This indicates that that IP address has been detected for the attack type multiple times, for example, ransomware.

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



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



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



Understanding kill chain and scenario engine

One of the strengths of FortiNDR is the ability to trace the source of a malware attack. In all attack scenarios, especially with worm, ransomware, and sophisticated attacks, there are often timeline and multi-stage kill chain type graphics.

When there is a detection, the scenario engine tries to form a multi-stage scenario based on time and similarity of attacks. The maximum trace-back period is five days.

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

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

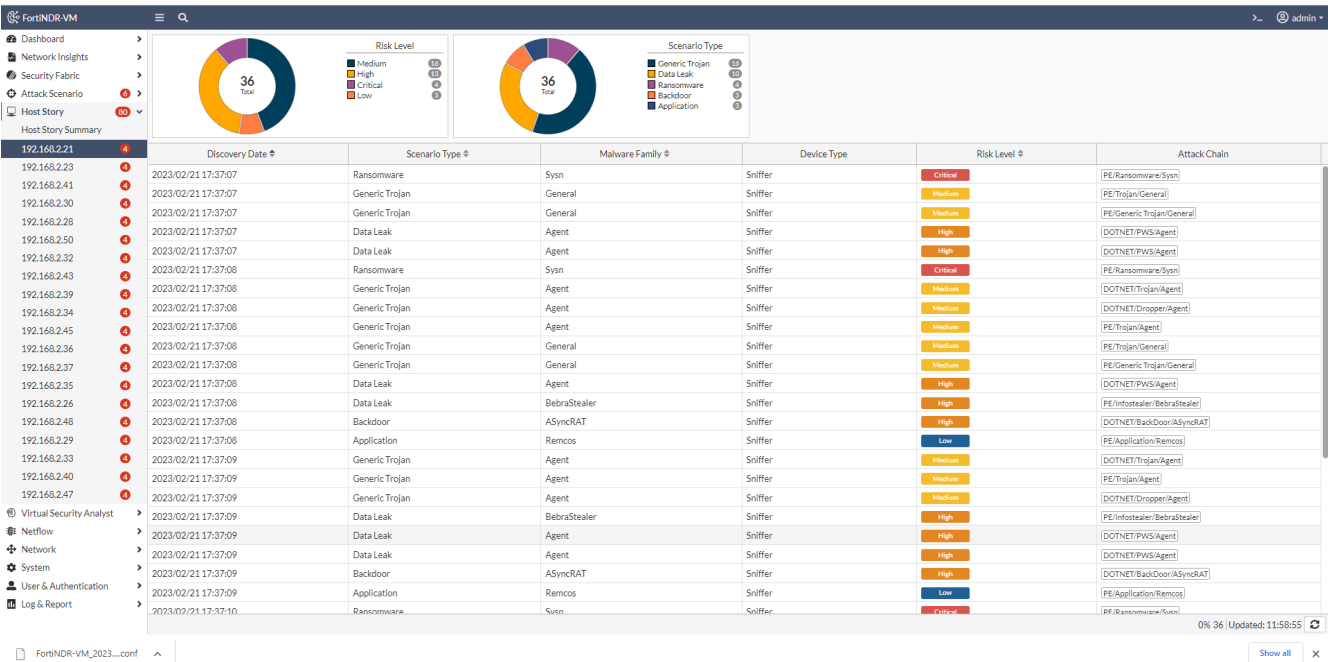
Host Story

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

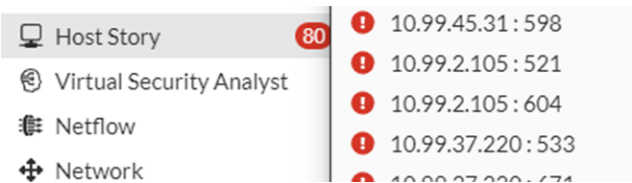


In Center mode, *Host Story* consolidates and displays all stories from all Sensors associated with the Center.

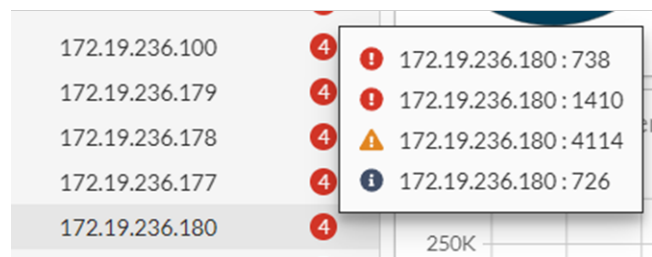
The *Host Story* summary page shows incident counts grouping by severities for each infected host.



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



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



Virtual Security Analyst

This section includes the following topics.

- [Express Malware Analysis on page 82](#)
- [Outbreak Search on page 86](#)
- [Static Filter on page 88](#)
- [NDR Muting on page 89](#)
- [ML Configuration on page 90](#)
- [Malware Big Picture on page 97](#)
- [Device Enrichment on page 98](#)

Express Malware Analysis

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

For information about using the API to submit files, see [Appendix A: API guide on page 177 > Submit files](#).



Express Malware Analysis is not available in Center mode.

To submit a file for Express Malware Analysis:

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

2. Submit a file for analysis. The default file size limit is 200MB. The file size limit can be changed using the CLI.
 - a. Click *Upload* then navigate to the file location on your device and click *Open*.
 - b. In the *Password* field, enter the password for the file. If the file does not require a password, FortiNDR will use

Infected by default. The *Password* field is displayed whether the file requires a password or not.

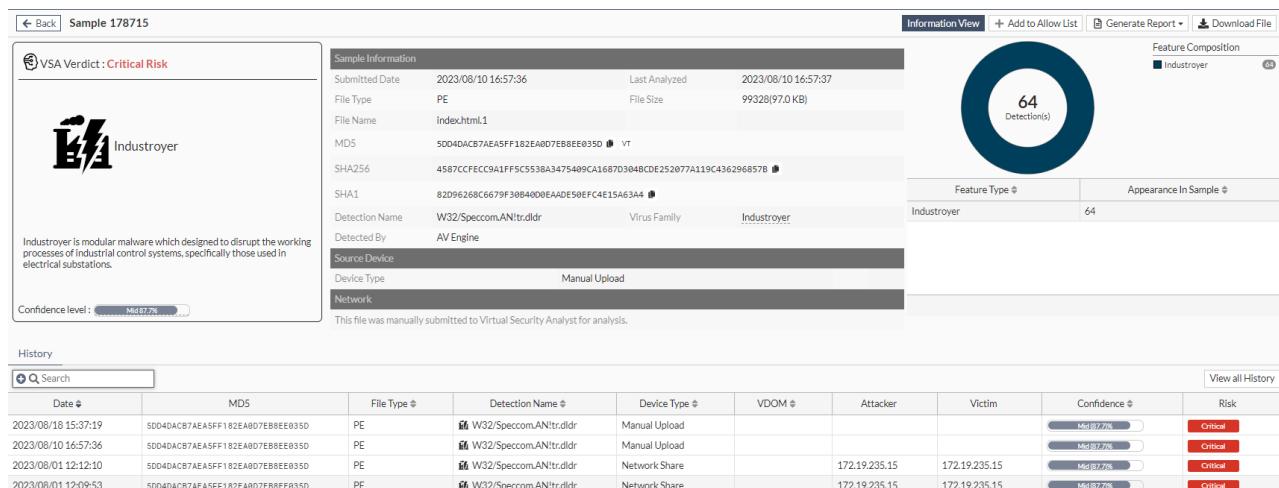
- c. Click OK. The verdict is displayed.

Submission Time	The date and time the file was uploaded.
Submitted Filename	The name of the file that was uploaded.
Submission User	The user that submitted the file.
MD5	The verdict result from MD5 checksum of the file.
Verdict	The attack scenario used to identify the malware attack.
Confidence	The confidence level as a percentage.
Risk	The risk verdict (High, Medium, Low or No Risk).
Status	The submission status.
File Type	The file type such as <i>Zip</i> or <i>PE</i> . <i>Other</i> indicates the detected file type is not supported by Artificial Neural Networks (ANN).
Indicator	Indicates the detection has IOC details.

3. Click *View Sample Detail* to view the sample information. This page explains the verdict by showing the feature composition of the file.

There are four tabs at the bottom of the page:

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



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

Back to 525904.tar.gz (2020/05/31 17:13:28)							
20 Items		<input type="text" value="Q"/> <input type="button" value="Locate"/> <input type="text" value="Search"/> <input type="button" value="Q"/>	<input type="button" value="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	b6523dcdd40e9c768a06ff46516fde4	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	402bfd289434fd9e2850ea130dbb6f87	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	38CECAE0.vsc	1beb2e23edc295ae214e762a478d300a	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3185FB8C.vsc	e143b7b35ded9f9c369fec32015e98dd	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	337A1E91.vdf	716cb0e867206122532ed753826b6a6c	PDF	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	355C8BFC.vsc	1b129271e371d64bbe128014cfc021b	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	4e8ffc5e4f4e62ebbb123f810f36602f	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	3BB44181.vsc	add352ba1edf9b25dc1cf3b152d9f4e5	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	38C07AA2.vsc	e10ff3809494e4a80189c0bc28ea4a68	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	31340098.vsc	9cf8b1e41b61a58600d2fc5f4f6daedb	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	3AA0CDEE.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3A109FD3.vsc			Generic Attack		Pending	Fail: Unsupported File Type

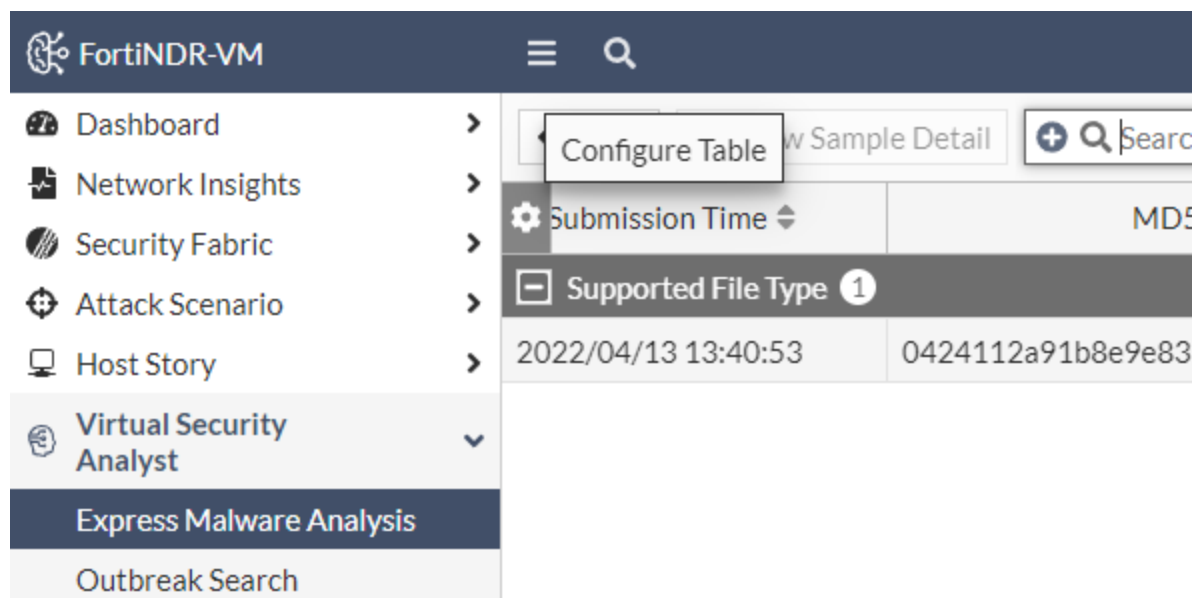
4. (Optional) Click *Generate Report* to view the report summary in PDF and JSON format.

To change the file size limit with the CLI:

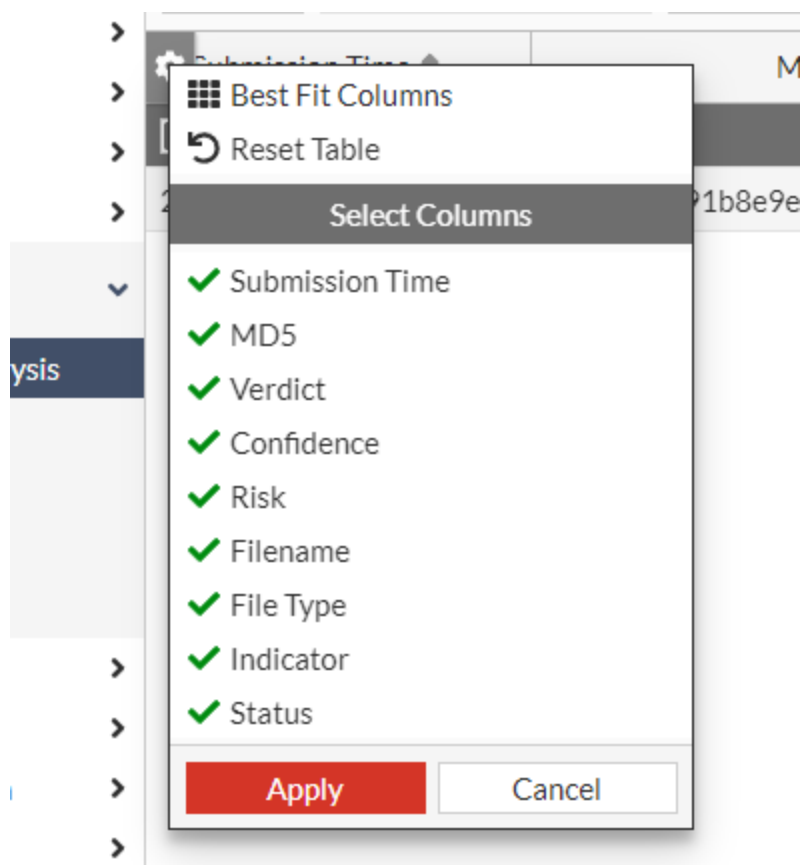
```
execute file-size-threshold
```

Configuring the table

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



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

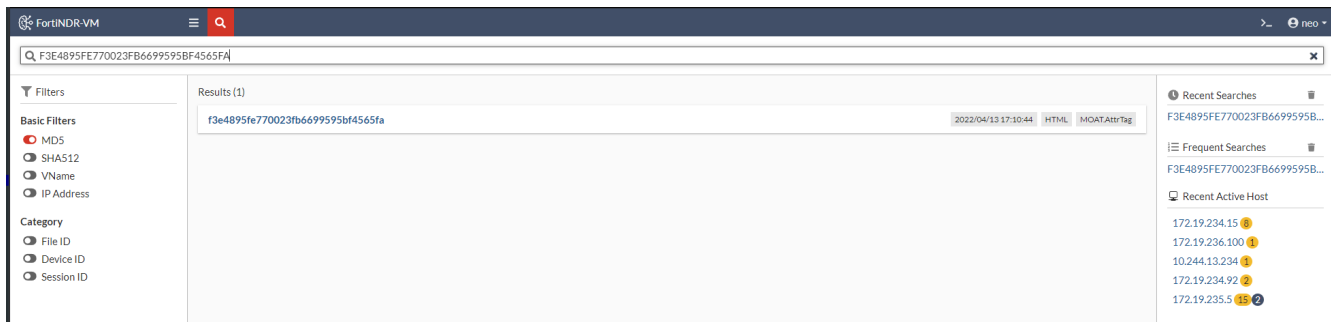


Outbreak Search

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

1. Using a known hash in the FortiNDR database or a physical copy of a file that belongs to the outbreak, you can search for other captured files that share similarities. See [Search lead type of hash or detection name on page 86](#).
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 87](#).

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

×

Q

Similarity-Based

Hash-Based

Detection-Based

Related Files

Generate Report

Search

Q

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	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 19:27:19	3a1bb104089bf0fb8924e17669520a26	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 19:11:09	db015f6411f5e83cb276cc752551078	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:36:13	b6f212bc9f0b74712a134eff10538fb5	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (99.61%)	91.02%
2020/06/01 18:31:16	80ec3d97c32db4b714bb9da3f199284c	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:14:21	3a1bb104089bf0fb8924e17669520a26	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:10:14	1a8d4bf46a9d1ee3824ee14b7e86fd46	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 18:00:05	b6f212bc9f0b74712a134eff10538fb5	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (99.61%)	91.02%
2020/06/01 17:59:31	db015f6411f5e83cb276cc752551078	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 17:52:09	b2dbf3fed8b3ed67c80567461284a42	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (96.48%)	95.90%
2020/06/01 17:30:52	80ec3d97c32db4b714bb9da3f199284c	HTML	Phishing	Generic	Q MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 17:04:49	a8990d67ff31dd5a509d07e3c0f68a82	HTML	Phishing	Generic	Q 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:

- Any sample that matches FortiNDR's virus family classification (detection subtype).
- Any sample that matches part of the detection name.
- 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.

Dashboard

Security Fabric

Attack Scenario

Host Story

Virtual Security Analyst

Express Malware Analysis

Outbreak Search

Threat Investigation

Network

System

User & Device

Log & Report

Search Lead Type: Outbreak Name

WannaCry

x

Q

i

Related Files

Related Events

Related Detection Names

Related Remote Connection

Generate Report

Search

Q

Found 74

Search by Hash

Search similar file(s) by Hash

Search by Detection Name

Search similar file(s) by Detection Name

Sample Info

Date	MD5	File Type	Detection Name	Risk Level	Confidence Level	Associated By
2020/06/14 11:16:20	b6523dcd40e9c768a06ff46516fde4	PE	Q W32/Virut.CE	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	402bfd289434fd9e2850ea13dbdb6f87	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	a77a049fb21401b38ea7c3a9ba9674eb	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	1beb2e23edc295ae214e762a478d300a	PE	Q W32/WannaCryptor.D:tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	e143b75b35ded9fc369fec32015e98dd	PE	Q W32/Wanna.APNO:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	d2782bcbce77d8c400331a102145eb51	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	808c71732f0089228fb082b07235620b	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	909421454e3e6da3efed986f2d59e7e	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	4d7769db73272f0493014c3ee6ec2bdc	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	e11bf6f7ed035fd4e60c74784209f937	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	bc3d22a07660260b143d8fabbdad4fb	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	cd2d592622fa018b4718be73d5df6c87	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	4b1c089335318263117845448920cb95	PE	Q W32/Miner.VI:tr	Low Risk	High (100.00%)	By Detection Name

Recursive searches

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

12b7fb78d1d55f53a93ba3770a1145cd	HTML	Downloader
145f7949922cf6e9b4ecaceb7793671c	HTML	Downloader
87d4cf49d40952de2184d833094af93c	HTML	Downloader
174ab067179f7fbb897d		Downloader
30128bed2b5a99b96f62		Downloader
9b35ac3cc4df067a94ef		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

Reports

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

Static Filter

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

In Center mode, *Static Filter* is associated with specific sensors. These filters allow you to create and modify an Allow or Deny list for targeted sensors.

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

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

Date	Hash Value	Hash Method	Allow / Deny list	Comment
2022/04/14 15:11:06	d01c97e2944166ed23e47e4a62ff471ab8fa031f	SHA1	Allow	
2022/04/14 15:11:06	340c8464c2007ce3f80682e15dfafa4180b641d53c14201b929906b7b0284d87	SHA256	Allow	
2022/04/14 15:11:06	1b7c22a21494997556626d7217e9a39	MD5	Allow	

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

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



You can add a detection to the *Allow List* from the *Malware Log*. For information, see [Malware Log on page 137](#).

NDR Muting

The *Virtual Security Analyst > NDR Muting* page displays a list of rules that no longer appear as detections in *Network Insights* pages.

You can mute certain detections in the *Botnet*, *FortiGuard IOC*, *Network Attacks*, *Weak/Vulnerable Communication*, *Encrypted Attack*, and *ML Discovery* insight pages. Once the attack is muted, it will no longer appear as a detection.



NDR Muting rules can be established in Center and Sensor mode. However, these rules only mask or hide specific NDR attack detections for that specific Center or Sensor. For instance, if you hide an attack on a Center, it does not automatically hide the same attack on the Sensor's user interface.

The *NDR Muting* displays the following information:

Last Modified	The date and time the rule was last modified.
Rule ID	The rule's unique ID.
Rule Type	The rule type.
Rule	The rule name and tag.
Created By	The name of the admin who created the rule.
Comment	Comments by the admin.
Status	The current status of the rule (<i>enabled / disabled</i>).

Muting rules in Network Insights

To mute an NDR Rule:

1. Go to *Network Insights* and open a page.
2. Right click a detection and select *Add to NDR Mute Rule*. The detection is muted and hidden in the page.

To view muted detections in Network Insights pages:

1. Go to *Network Insights* and open a page.
2. Disable *NDR Mute OFF*.

Managing muted rules

To enable/disable NDR muted rules:

1. Go to *Virtual Security Analyst > NDR Muting*, and select a rule in the list.
2. In the toolbar, click *Edit*.

To delete multiple rules:

1. In the toolbar, click the *Delete Multiple* dropdown.
2. Select one of the following:
 - Delete older than 30 days
 - Delete All

To delete an NDR rule:

1. Go to *Virtual Security Analyst > NDR Muting*, and select a rule in the list.
2. In the toolbar, click *Delete*.

ML Configuration

Go to the *Virtual Security Analyst > 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. You can also use the page to create IP range groups. *ML Configuration* is not available in Sensor mode.

The *ML Configuration* page has two tabs:

- **Source IP:** Use this tab to categorize IP ranges. Each group of IP ranges can be individually trained based on the ML configuration. This allows for varying levels of severity to be applied to distinct IP ranges for custom anomaly detection.
- **Default (Standalone mode) :** Use this tab to view and adjust the machine learning baseline features for traffic anomaly detection and to monitor the status of baseline training.
- **Sensor Group ID (Center mode):** Use this tab to set up IP ranges, each with its desired Severity and chosen features to be incorporated in the baseline. There is an additional option to specify the *Sensor Group* that this

specific Source IP corresponds to. After changes are applied to a Source IP range in this tab, the associated Sensor Group will automatically initiate baseline retraining

The *ML Configuration* displays the following information:

Source IP	The source IP address of the IP range.
Severity	The severity level assigned to the IP (<i>Low</i> , <i>Medium</i> , <i>High</i> or <i>Critical</i>).
Number of Features	The number of features enabled in the <i>Default</i> tab.
Last Modified Time	The date and time the ML configuration was modified.
Start Training Time	The date and time baseline training started.
End Training Time	The date and time baseline training was completed.

To customize the **ML Configuration** page:

- In the table header, click the gear icon and select *Best Fit Columns*, *Reset Table*, or show or hide columns.
- In column header click the ellipses and select *Resize to Contents* or *Group By This Column*.

Source IP tab

When creating an IP range group, careful attention needs to be paid to the groupings and the number of features in the *Source IP* tab. Proper organization ensures that each IP range group functions correctly for effective anomaly detection.

Example:

The organization and categorization of IP ranges can have a significant effect on the ML baseline's functionality. In the image below, the second *Source IP* group is comprised of the IP range 172.19.122.0 with a *Class C Netmask* applied. This will mask all IPs within the range 172.19.122.0/24.

However, the broad masking of the second group, interferes with the functioning of the third *Source IP* group which is set up for exclusively the IP 172.19.122.220. This is because the broader second group supersedes the more specific settings of the third group.

Source IP		Default					
+ Create		Edit	Delete	Delete All			
Source IP	Severity	Number of Feature(s)	Create Time	End Training Time	ID	Start Training Time	Sub-ID
172.19.235.0	Low	7	2023/07/28 17:27:00	2023/07/28 17:29:00	7	2023/07/28 17:27:00	2
172.19.122.0	Critical	8	2023/07/28 17:27:00	2023/07/28 17:29:00	7	2023/07/28 17:27:00	3
172.19.122.220	High	6	2023/07/28 17:27:00	2023/07/28 17:29:00	7	2023/07/28 17:27:00	1

To create an IP range group:

- Go to *Virtual Security Analyst > ML Configuration*.
- In the *Source IP* tab, click *Create*. The *ML Configuration for Source IP* pane opens.
You cannot create an IP group if the baseline is training.

3. Configure the source IP settings.

Source IP and Severity	
Source IP	Enter the source IP.
Severity	Select <i>Low</i> , <i>Medium</i> , <i>High</i> or <i>Critical</i> .
Device Info	
Source IP Mask	<p>The Source Device IP. Apply a netmask if you do not want to treat certain range changes in the IP as an anomaly.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default. • <i>Apply Class C Netmask: /24</i> • <i>Apply Class B Netmask: /16</i>
Destination IP Mask	<p>The Destination Device IP. Apply netmask if you don't want to treat certain range change in the IP as anomaly</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default. • <i>Apply Class C Netmask: /24</i> • <i>Apply Class B Netmask: /16</i>
Source Device MAC Address	Source device MAC address.
Destination Device Model	Device model such as: <i>FortiGate</i> , <i>Workstation</i> , <i>IDRAC</i> , etc.
Destination Device Geolocation	Device geographical country such as <i>United States</i> .
Destination Device Category	Device category such as: <i>NAS</i> , <i>Virtual Machine</i> , <i>Firewall</i> , etc.
Destination Device Vendor	Device vendor such as <i>VMware</i> , <i>Dell</i> , <i>Synology</i> , etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as <i>Windows</i> , <i>Linux</i> , etc.
Protocol and Application Behavior	
Transport Layer Protocol	UDP, ICMP, TCP, etc
Application Layer Protocol	TLS, HTTP, SMB, etc
Protocol/Application Behaviors/Action	Specific application actions such as. <i>Adobe Reader form creation</i> , <i>WebDAV reload</i> , <i>Wasabi file upload</i> , etc
Others	
Session Packet Size	<p>FortiNDR categorizes the packet size into 3 groups:</p> <ul style="list-style-type: none"> • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, <i>22</i> , <i>445</i> , <i>none reserved port</i> , etc.
Source Port	Port number such as, <i>22</i> , <i>445</i> , <i>none reserved port</i> , etc.

4. Click *Apply*.

Default Tab

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



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



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.

The *Default* tab displays the following information and features:

Status	
Baseline Status	The current baseline training status: <ul style="list-style-type: none"> • <i>Baselining</i>: The current training is still in progress. • <i>Baseline ready</i>: The baseline training is done and is ready for anomaly detection.
ML Discovery Detection	Click to <i>Enable</i> or <i>Disable</i> baseline training.
Latest Training Completion	The date and time of the last baseline training.
Feature Enabled for Learning	
Default Feature Configuration	Click to enable the default ML configuration settings.
Severity	Select <i>Low, Medium, High</i> or <i>Critical</i> .
Device Info	
Source IP Mask	The Source Device IP. Apply a netmask if you do not want to treat certain range changes in the IP as an anomaly. Select one of the following options: <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default. • <i>Apply Class C Netmask</i>: /24 • <i>Apply Class B Netmask</i>: /16
Destination IP Mask	The Destination Device IP. Apply netmask if you don't want to treat certain range change in the IP as anomaly Select one of the following options: <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default.

	<ul style="list-style-type: none"> • <i>Apply Class C Netmask: /24</i> • <i>Apply Class B Netmask: /16</i>
Source Device MAC Address	Source device MAC address.
Destination Device Model	Device model such as: <i>FortiGate, Workstation, IDRAC</i> , etc.
Destination Device Geolocation	Device geographical country such as <i>United States</i> .
Destination Device Category	Device category such as: <i>NAS, Virtual Machine, Firewall</i> , etc.
Destination Device Vendor	Device vendor such as <i>VMware, Dell, Synology</i> , etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as <i>Windows, Linux</i> , etc.
Protocol and Application Behavior	
Transport Layer Protocol	UDP, 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</i> , etc
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: <ul style="list-style-type: none"> • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, <i>22, 445, none reserved port</i> , etc.
Source Port	Port number such as, <i>22, 445, none reserved port</i> , etc.



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.

Sensor Group ID Tab (Center mode)

To create a Sensor Group:

In Center mode, go to

1. Go to *Virtual Security Analyst > ML Configuration*.
2. Click the *Sensor Group ID* tab.

3. Click *Create*. The *Sensor Group ID* pane opens.
4. Configure the group settings and click *OK*

Sensor Group	
Sensor Group	This value is populated by the system.
Sensor Selection	Click the plus (+) sign to select the sensor and then click <i>Close</i> .
Feature Enabled for Learning	
Default Feature Configuration	Click to enable the default ML configuration settings.
Severity	Select <i>Low</i> , <i>Medium</i> , <i>High</i> or <i>Critical</i> .
Device Info	
Source IP Mask	<p>The Source Device IP. Apply a netmask if you do not want to treat certain range changes in the IP as an anomaly.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default. • <i>Apply Class C Netmask</i>: /24 • <i>Apply Class B Netmask</i>: /16
Destination IP Mask	<p>The Destination Device IP. Apply netmask if you don't want to treat certain range change in the IP as anomaly</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default. • <i>Apply Class C Netmask</i>: /24 • <i>Apply Class B Netmask</i>: /16
Source Device MAC Address	Source device MAC address.
Destination Device Model	Device model such as: <i>FortiGate</i> , <i>Workstation</i> , <i>IDRAC</i> , etc.
Destination Device Geolocation	Device geographical country such as <i>United States</i> .
Destination Device Category	Device category such as: <i>NAS</i> , <i>Virtual Machine</i> , <i>Firewall</i> , etc.
Destination Device Vendor	Device vendor such as <i>VMware</i> , <i>Dell</i> , <i>Synology</i> , etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as <i>Windows</i> , <i>Linux</i> , etc.
Protocol and Application Behavior	
Transport Layer Protocol	UDP, ICMP, TCP, etc
Application Layer Protocol	TLS, HTTP, SMB, etc
Protocol/Application Behaviors/Action	Specific application actions such as. <i>Adobe Reader form creation</i> , <i>WebDAV reload</i> , <i>Wasabi file upload</i> , etc
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups:

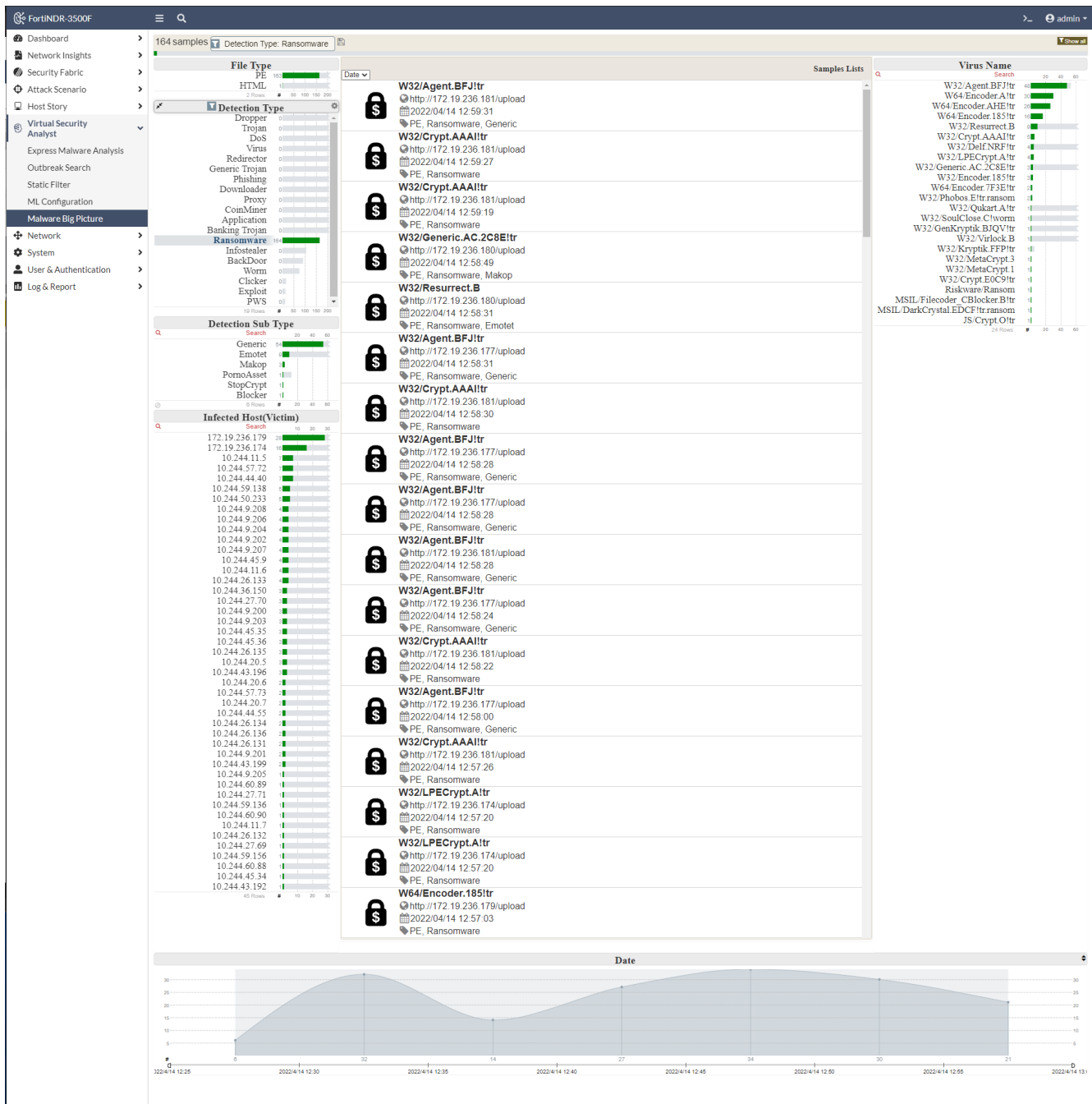
	<ul style="list-style-type: none"> • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, 22, 445, <i>none reserved port</i> , etc.
Source Port	Port number such as, 22, 445, <i>none reserved port</i> , etc.
Status	
Baseline Status	The current baseline training status: <ul style="list-style-type: none"> • <i>Baselining</i>: The current training is still in progress. • <i>Baseline ready</i>: The baseline training is done and is ready for anomaly detection.
ML Discovery Detection	Click to <i>Enable</i> or <i>Disable</i> baseline training.
Latest Training Completion	The date and time of the last baseline training.
Feature Enabled for Learning	
Default Feature Configuration	Click to enable the default ML configuration settings.
Severity	Select <i>Low</i> , <i>Medium</i> , <i>High</i> or <i>Critical</i> .
Device Info	
Source IP Mask	The Source Device IP. Apply a netmask if you do not want to treat certain range changes in the IP as an anomaly. Select one of the following options: <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default. • <i>Apply Class C Netmask</i>: /24 • <i>Apply Class B Netmask</i>: /16
Destination IP Mask	The Destination Device IP. Apply netmask if you don't want to treat certain range change in the IP as anomaly Select one of the following options: <ul style="list-style-type: none"> • <i>Do Not Apply Netmask</i>: This is the default. • <i>Apply Class C Netmask</i>: /24 • <i>Apply Class B Netmask</i>: /16
Source Device MAC Address	Source device MAC address.

Destination Device Model	Device model such as: <i>FortiGate, Workstation, IDRAC</i> , etc.
Destination Device Geolocation	Device geographical country such as <i>United States</i> .
Destination Device Category	Device category such as: <i>NAS, Virtual Machine, Firewall</i> , etc.
Destination Device Vendor	Device vendor such as <i>VMware, Dell, Synology</i> , etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as <i>Windows, Linux</i> , etc.
Protocol and Application Behavior	
Transport Layer Protocol	UDP, 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</i> , etc
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: <ul style="list-style-type: none"> • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, <i>22, 445, none reserved port</i> , etc.
Source Port	Port number such as, <i>22, 445, none reserved port</i> , etc.

Malware Big Picture

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

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



Device Enrichment

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

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

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

Dashboard	>	+ Create New	Edit	Delete	Active Directory Ping Test	Active Directory Connection Test	Manual Run
Network Insights	>	Enable/Disable	Profile Name	Server name/IP	Port	Profile Status	Last Updated
Security Fabric	>	Enabled	FNDRLAB.local	172.19.236.121	389	Scheduled - [Matched: 1019] from last cycle	2023/03/02 09:47:38
Attack Scenario	11 >						
Host Story	20 >						
Virtual Security Analyst	>						
Express Malware Analysis	>						
Outbreak Search	>						
Static Filter	>						
ML Configuration	>						
Malware Big Picture	>						
Device Enrichment	>						
Netflow	>						
Network	>						
System	>						
User & Authentication	>						
Log & Report	>						

The *Device Enrichment* page displays the following information:

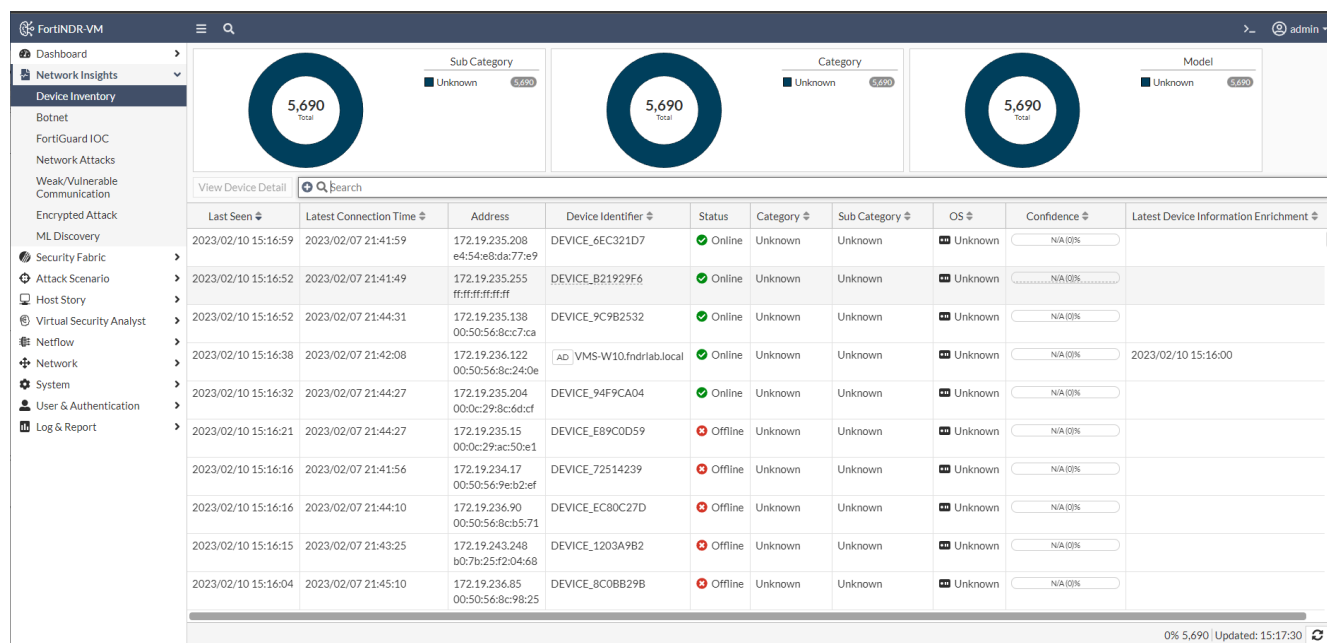
Enable/Disable	Indicates if the profile is enabled or disabled.
Profile Name	The name assigned to the profile.
Server name/IP	The IP address of the windows AD server or domain name.
Port	The port used by the profile. If SSL is enabled the port is 636 otherwise the default is 389.
Profile Status	After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



The *Device Enrichment* page is not available in Sensor and Center mode.

Viewing the retrieved device identifier

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

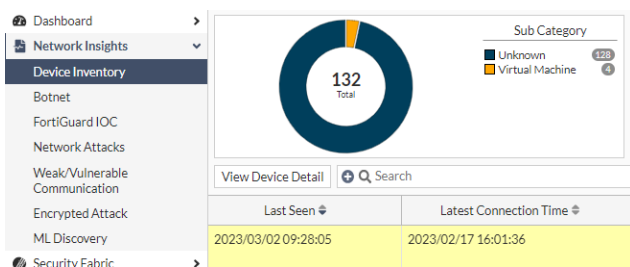


Overwriting the device identifier

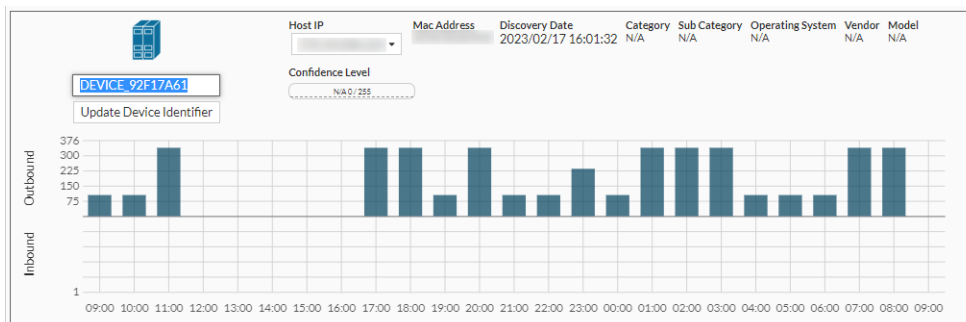
You can manually overwrite the device identifier in the device information page.

To overwrite the device identifier:

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



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



Creating a Device Enrichment Profile

To create a Device Enrichment profile:

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

Enable Device Configuration	Disable and enable the profile
Profile Name	Unique identifier for the Microsoft Active Directory Connection Profile
Microsoft Active Directory Connection Settings	
Sever name/ IP	Enter either the IP address of the windows AD server or domain name.
Enable SSL	SSL port and protocol to be use when selected
Base DN	The starting point of the LDAP Server for user authentication within the directory. For example, DC=example-domain, DC=com
Bind DN	The LDAP user and its LDAP directory tree location for binding. For example, CN=fndr_svc,CN=testUser, DC= example-domain,DC= com.
Bind Password	The password for the LDAP user account for binding. For example, DC= example-domain,DC= com.
Search Scope	<p>The method of retrieving the information from the tree:</p> <ul style="list-style-type: none"> • <i>Base</i>: only retrieve information from the base level of the directory tree specified in search base • <i>One Level</i>: only retrieve information from the search base and one level down • <i>Subtree</i>: retrieve everything underneath the specified search base
Search Base	The starting point of the directory tree for retrieving information
DNS Server Settings	
DNS Server	DNS Server is required as part of the enrichment process involved querying DNS server with hostnames to retrieve current IP address.
Automation	
Scheduling	<ul style="list-style-type: none"> • <i>Every</i>: the enrichment cycle will be preformed once right after the profile is saved. The next cycle will be run after the amount of hours user input • <i>Daily</i>: the enrichment cycle will start every day at the input time • <i>Weekly</i>: the enrichment cycle will start weekly at the input time.

4. Click *OK*.

Active Directory Profile Actions

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

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

Netflow

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

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

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



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

To turn NetFlow on/off with the CLI:

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

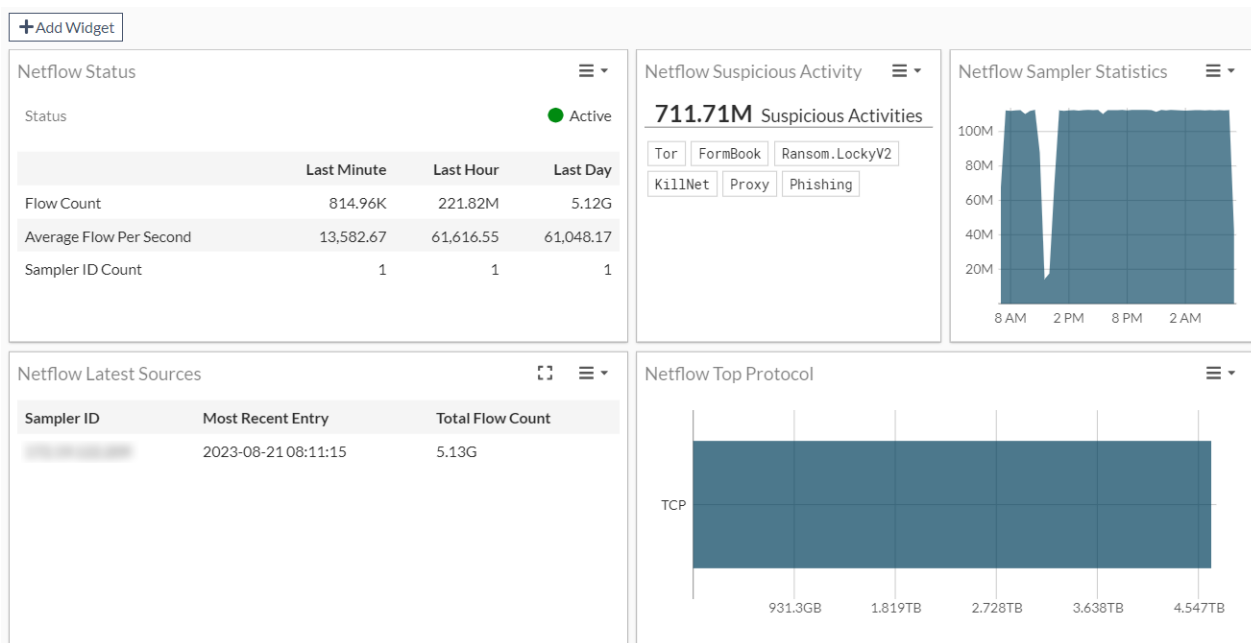
NetFlow ports

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

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

Netflow Dashboard

The *Netflow Dashboard* provides an overview of NetFlow traffic statistics. In Center mode, the *Netflow Dashboard* displays the data collated from the Sensors.



The *Netflow Dashboard* contains the following widgets:

Netflow Status	Displays the <i>Status</i> of this feature , <i>Flow Count</i> , <i>Average Flow Per Second</i> and <i>Sampler ID Count</i> . The statistics are broken down into last minute, hour, and day for users to view the volume and flow count coming into FortiNDR.
Netflow Suspicious Activity	Displays the Netflow botnet, Spam, Phising, Tor and Proxy traffic detections. Netflow botnet detections are matched against the FortiGuard botnet database. Discovery of botnet detections are matched against destination IPs and ports within a flow. Click the widget to expand it to view a more detailed page about the detections.
Netflow Sampler Statistics	Displays the flow count over time.
Netflow Top Talker	Displays the IP addresses that are responsible for the most network traffic in a given time period. The <i>Top Talker</i> feature provides a method to identify the devices or IP addresses that are consuming the most bandwidth, allowing network administrators to troubleshoot performance issues and optimize network usage.
Netflow Top Protocol	Displays the most used transportation layer protocols in terms of bandwidth consumption. Protocols can include TCP, UDP, ICMP, among others. The <i>Top Protocols</i> feature provides a method for understanding which protocols are using the most bandwidth, helping network administrators optimize network usage and potentially identify security concerns.
Netflow Latest Sources	Displays the Flow activity statistics from active samplers within a selected time frame. The widget allows users to select one day, one week, or one month.
Netflow Traffic Volume	Displays aggregated Ingress and Egress traffic volume of each Sampler within a selected time frame. For example, if sampler ID <i>1.1.1.1</i> has flows from different source(s) and destination(s), the widget will summarize the total ingress and egress traffic.

Customizing the Netflow Dashboard

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

To remove a widget from the dashboard:

Click the widget menu and select *Remove*.

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

To add a widget to the dashboard:

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

To re-size a widget in the dashboard:

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

Netflow Log

Netflow Log shows the logs FortiNDR collected. In Center mode, the *Netflow Log* displays the data collated from the Sensors.

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



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

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

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

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

Network

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

Interface

FortiNDR has the following preset ports which cannot be changed.

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

DNS and Static Routes

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

System

Use the *System* options to configure system settings.



It is recommended that you create a system backup file as part of your maintenance plan. Always perform a backup before upgrading firmware or making major system configuration changes. Save these configuration backups to your local computer in the event that you need to restore the system after a network event. For information, see [Backup or restore the system configuration on page 128](#).

Administrators

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

To create a new Administrator:

- 1. Go to *Settings > Administrators* and click *Create New*. The *New Administrator* page opens.
- 2. Configure the administrator settings and click *OK*.

Username	Enter a username for the administrator.
Admin Profile	<ul style="list-style-type: none">1. From the dropdown, select an Admin Profile.2. (Optional) Click New to create a new Admin Profile.3. (Optional) Click Edit to modify an existing Admin Profile.
Authentication	<p>From the dropdown select one of the following:</p> <ul style="list-style-type: none">• Local• RADIUS• Local Plus RADIUS• LDAP
Password	Enter a password for the administrator.
Confirm Password	Re-enter the administrator password.
Preference	
Theme	<p>Select a them for the administrator. The following options are available:</p> <ul style="list-style-type: none">• Neutrino• Jade• Mariner• Graphite• Melongene

	<ul style="list-style-type: none"> • Cloud App Light • Onyx • Dark Matter • Eclipse • Cloud App Dark
Restrict login to trusted hosts	Enable to add a trusted host.

Admin Profiles

Administrator profiles are used to control administrator access privileges to system features. Profiles are assigned to administrator accounts when an administrator is created.

Pre-defined profile types

The following pre-defined administrator profiles cannot be modified or deleted:

- *Operator Profile*: Can view certain pages. This profile cannot change any system settings.
- *Super Admin Profile*: All functionalities are accessible.

Access Permissions

The following table shows the default settings for the pre-defined profile types:

Access Permissions	Operator Profile	Super Admin Profile
System status	Read	Read/Write
System Access	None	Read/Write
System Configuration	None	Read/Write
System Maintenance	None	Read/Write
Virtual Security Analyst	Read	Read/Write

To create an Admin Profile:

1. Go to *System > Admin Profiles*.
2. Click *Create New*. The *Create Access Profile* page opens.
3. Configure the *Access Permissions*.

Access Permissions	Description
System status	Grant permissions to settings critical to FortiNDR network accessibility, including GUI console, <i>Network</i> , <i>Administrators</i> , <i>Admin Profiles</i> , <i>Certificates</i> ,

Access Permissions	Description
	and RADIUS/LDAP authentication.
System Access	Grant permission to modify other system settings such as system time settings, system FortiGuard update, and <i>Security Fabric</i> settings.
System Configuration	Grant permissions to access system maintenance settings such as back up system configuration, restore configuration, and restore firmware.
System Maintenance	Grant permissions to access to the system to check its status. Users with this permission set to none cannot log into the system. The default is none in the GUI.
Virtual Security Analyst	Grant permissions to access settings in <i>Virtual Security Analyst</i> such as <i>Express Malware Analysis</i> , <i>Outbreak Search</i> , <i>Static Filter</i> , <i>NDR Muting</i> , <i>ML Configuration</i> , <i>Malware Big Picture</i> and <i>Device Enrichment</i> .

System status Grant access to Dashboard > System Status System Access Grant access to the features in Security Fabric System Configuration Grant access to the features in Network System Maintenance Grant access to the features in System Virtual Security Analyst Grant access to the features in Virtual Security Analyst

4. If you are operating in Center mode, select a sensor.
 - a. Under *Sensor*, click *Selection*.
 - b. Select the sensor from the list and click *Close*.
5. Click *OK*.

Sensor Settings

In Center and Sensor modes, go to *Settings > Center Settings* to link an active sensor to a Center.

The *Center Settings* page displays the following information:

Hostname	The sensor hostname.	
IP Address	The sensor IP address.	
Model Name	The sensor model name.	
Serial Number	The sensor serial number.	
Status	The connection status.	
	Registered	Indicates that the Sensor has completed the registration process but has yet to undergo a license check.
	Connected	Indicates the Sensor is prepared for synchronization and is actively transmitting data to the Center.
	No Data Transferred	Indicates the Sensor has not sent any data to the Center for a span of 3 minutes while still maintaining a connection.

	Firmware Mismatched Indicates the Sensor's firmware is incompatible with the Center, and the Sensor is currently disabled. This does not mean the Sensor is inoperative. However, the Center will not accept any data from it.
	Sensor License Invalid Indicates that the Sensor does not possess a valid license, and has been disabled.
	Disabled By User Indicates the Sensor has been manually disabled by a user in the Center. This does not mean the Sensor is inoperative. However, the Center will not receive any data from it.
FortiGuard Status	Compares the Sensor's FortiGuard updates against the Center's FortiGuard updates. <i>FortiGuard Update Available</i> will appear if an update is required.
Last Updated	The date the sensor was last updated.
CPU Usage	The CPU usage as a percentage.
Disk Usage	The disk usage as a percentage.
Memory Usage	The memory usage as a percentage.

The following options are available:

Reboot Sensor	Initiates a reboot command for the selected Sensor.
Ping Sensor	Sends a ping command to the chosen Sensor, to test its connectivity.
Disable Sensor	Changes the status of the selected Sensor to <i>disabled</i> , preventing the Center from receiving further data. However, the historical data from the Sensor is retained.
Activate Sensor	Activates the sensor.
Command History	Displays the history of commands that have been sent to the selected Sensor, including reboot, ping, restore configuration, restore firmware, and upload VM license commands.
Backup Sensor Configuration	Creates of a backup for the selected Sensor's Configuration.
Restore Firmware	Restores and updates the selected Sensor's Firmware.
Upload VM License	Click to upload a FortiNDR VM license to the selected Sensor.



These commands may not function properly when the sensors are positioned behind a NAT. This limitation will be resolved in upcoming versions.

Sensor Details

Double-click a sensor to view the Sensor Details pane. This pane contains the following tabs:

Sensor	Displays detailed information about the sensor.
Command History	Displays a list of recent commands dispatched to the selected sensor.
FortiGuard	Compares the Sensor's FortiGuard updates against the Center's FortiGuard updates. <i>FortiGuard Update Available</i> will appear if an update is required.

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
```



A changing the mode during firmware upgrade (for example, changing standalone mode to sensor mode) will result in the previous data being wiped out.

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

Go to *System > Settings* to configure the Host Name, System Time and the Idle Timeout.

To configure the system settings:

1. Go to *System > Settings*.
2. Configure the system settings and click *OK*.

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.

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

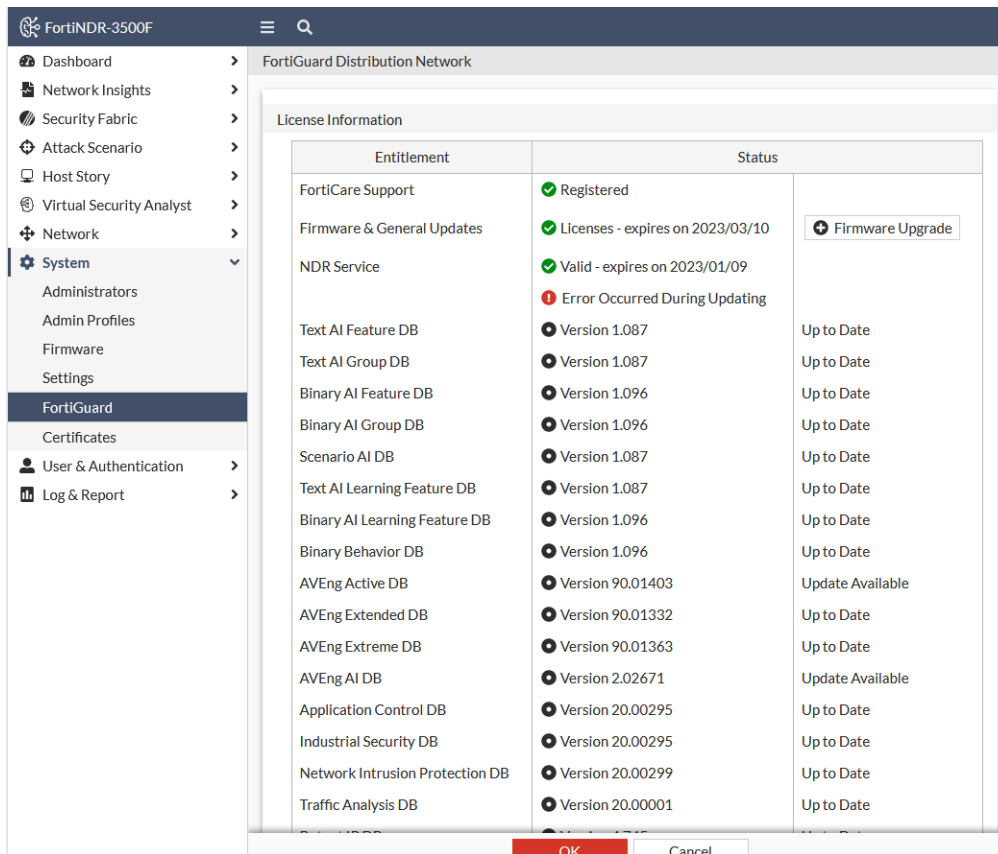
FortiGuard

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

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

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

Please refer to [Appendix D: FortiGuard updates on page 191](#) and [CLI guide](#) for more detail.



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

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



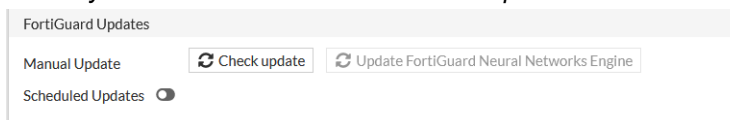
Currently, FortiNDR retrieves ANN updates from US and EMEA FortiGuard servers.

FortiNDR selects the update server based on proximity and location.

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

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

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



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

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

To update the ANN database using the CLI:

1. Go to the [Fortinet support website](#) and download the ANN network database files.
There are two ANN network databases: `pae_kdb` and `moat_kdb`. `pae_kdb` has about six to eight individual files that you have to download.

There is only one `moat_kdb.tar.gz` because it is small and doesn't have to be split. After downloading them for the `pae_kdb`, unzip them into `pae_kdb.tar.gz`.

2. Unzip the downloaded files to `pae_kdb.tar.gz` and `moat_kdb.tar.gz`.

In Windows:

- a. `copy /B pae_kdb.zip.* pae_kdb.zip`
- b. Right-click the `pae_kdb.zip` package and click *Extract All*.

In Linux:

- a. `cat pae_kdb.zip.* > pae_kdb.zip`
- b. `unzip pae_kdb.zip`

3. Put `pae_kdb.tar.gz` and `moat_kdb.tar.gz` on a disk that FortiNDR can access, such as a TFTP or FTP server, or a USB drive.

If you use a USB drive, ensure its format is ext3 compatible, has only one partition, and the file is in the root directory.

4. Use the CLI command `execute restore kdb` to update the 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
```


- 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:

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

FortiGuard Updates

Manual Update

Scheduled Updates ☒

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

Certificates

Go to *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.

The *Certificates* page displays the following information:

Name	The name assigned to the certificate at the time it was created.
Subject	The Common Name (CN), Organization (O), Organization Unit (OU), Locality (L), State (ST), Country/Region (C) and Email Address (emailAddress).
Issuer	The organization that issued the certificate.
Expires	The certificate expiry date.
Status	The current status of the certificate.

The following options are available:

Generate	Generate a certificate signing request.
Download	Download the certificate file.
Set Default	Set the default certificate.
Import	Import a local, CA or remote certificate.
Delete	Delete a certificate.
View Details	View the certificate details.
Generate Report	Generate a CSV, JSON or PDF report.

To generate a certificate:

1. Go to *System > Certificates*.
2. Click *Generate*. The *Generate Certificate Signing Request* page opens.
3. Enter the certificate information and click *OK*.

Certification Name	Enter the certificate name.
---------------------------	-----------------------------

Subject Information

Certification Type	Select <i>Host IP</i> , <i>Domain Name</i> , or <i>E-Mail</i> .
---------------------------	-----------------------------------------------------------------

IP	Enter the certificate IP address.
-----------	-----------------------------------

Optional Information

Organization	Enter the name of the organization issuing the certificate.
---------------------	-------------------------------------------------------------

Locality(City)	Enter the city the certificate is issued in.
-----------------------	----------------------------------------------

State/Province	Enter the state or province the certificate is issued in.
-----------------------	-----------------------------------------------------------

Country	Enter the country the certificate is issued in.
----------------	-------------------------------------------------

E-mail	Enter the email address of the person issuing the certificate.
---------------	----------------------------------------------------------------

Key type	Select the key type from the dropdown list.
-----------------	---------------------------------------------

Key size	Select 512, 1024, 153 or 2018 Bit.
-----------------	------------------------------------

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.



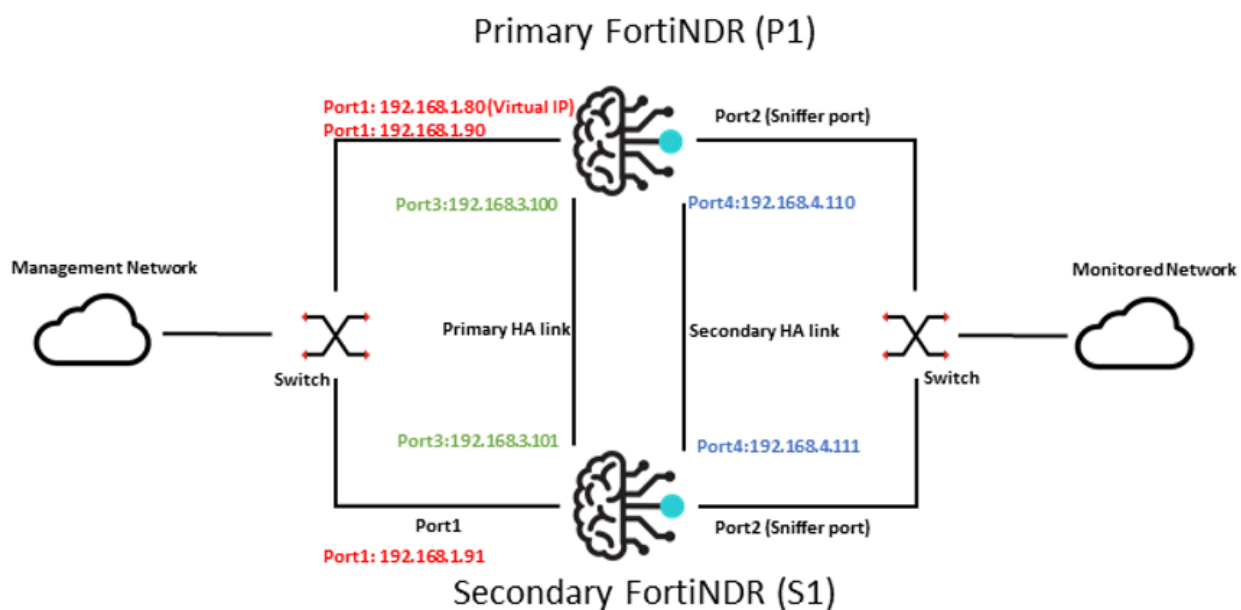
High Availability (HA) is only available in Standalone mode.

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 120](#).
- 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.

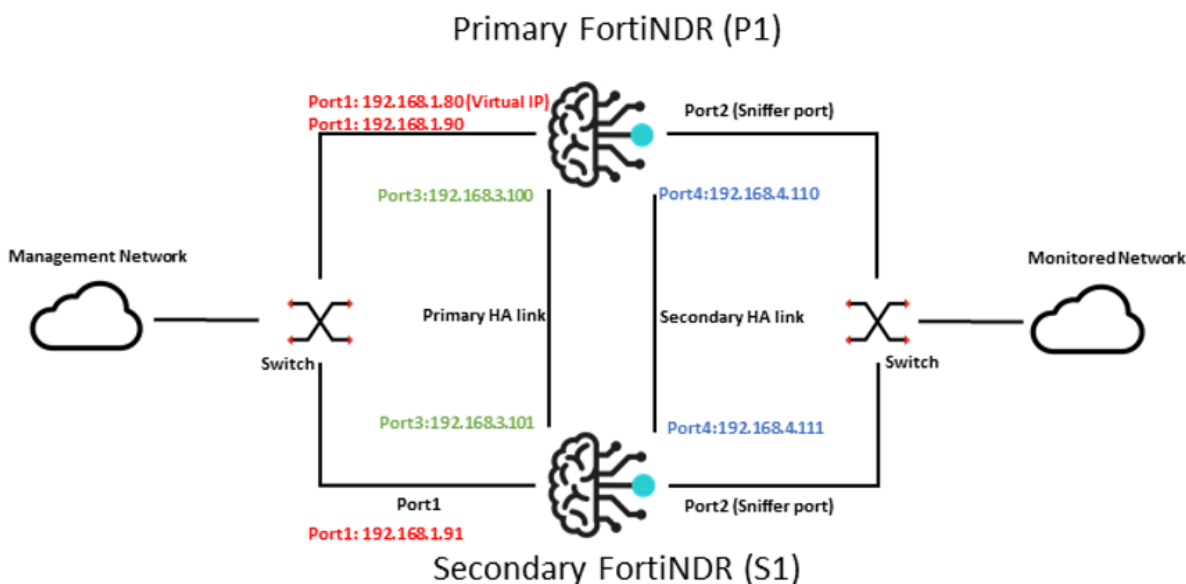


If your FortiNDR unit is running, you can join a secondary unit to form the HA. However, you should allow more time to synchronize larger databases.

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:



2. Load the latest ANN database on both FortiNDR units. The ANN database can be updated from FDS or with the CLI (see, [Appendix D: FortiGuard updates on page 191](#)).



- 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.

3. 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
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	<p>Enables or disables HA, selects the initial configured role:</p> <ul style="list-style-type: none"> • Off: disable HA. • Primary: configured as primary Unit. • Secondary: configured as secondary Unit.
password	<p>Enter an HA password for the HA group.</p> <p>You must configure the same password value on both the primary and secondary units.</p>
heartbeat-status	<p>Specify if this interface will be used for HA heartbeat and synchronization:</p> <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	<p>When configuring primary HA interfaces:</p> <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. <p>The same rule should be applied when configuring the secondary HA interface.</p>
virtual-ip	<p>Enter the virtual IP address and netmask for this interface.</p> <p>If configured, this virtual IP can serve as the external IP of the HA group.</p> <p>When failover occurs, this setting will take effect on the new Primary unit. For details, see Using Virtual IP on page 126.</p>
action-on-primary	<p>ignore-vip [Default]: Ignore the Virtual IP interface configuration on the new Primary unit after failover.</p> <p>use-vip: Add the specified Virtual IP address and netmask to the interface on the new Primary unit after failover.</p>

CLI option	Description
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 122](#).
- Ensure no errors appear on the HA event log. See, [HA Logs on page 126](#).

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 125](#).
- 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
```

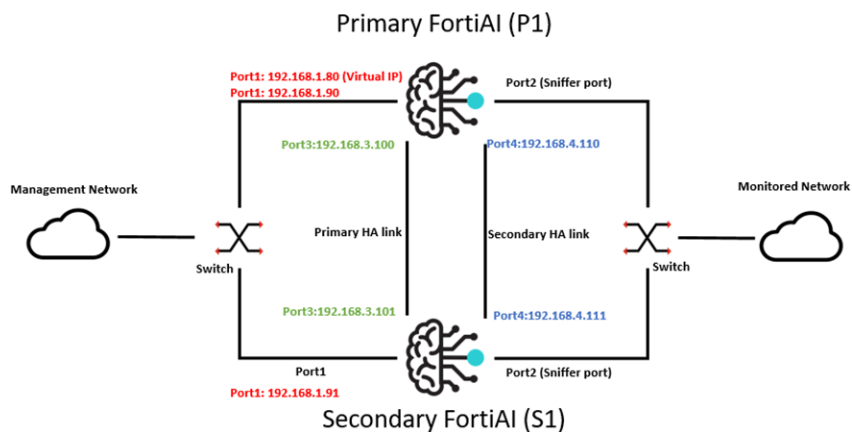
To check the HA status with the GUI:

1. Go to *Dashboard > System Status > Network*.
2. In the *System Information* widget, go to *HA Status*.
3. Go to *Log & Report > Events*. In the event log, verify that the HA DB mode has been changed successfully and matches the HA effective mode.

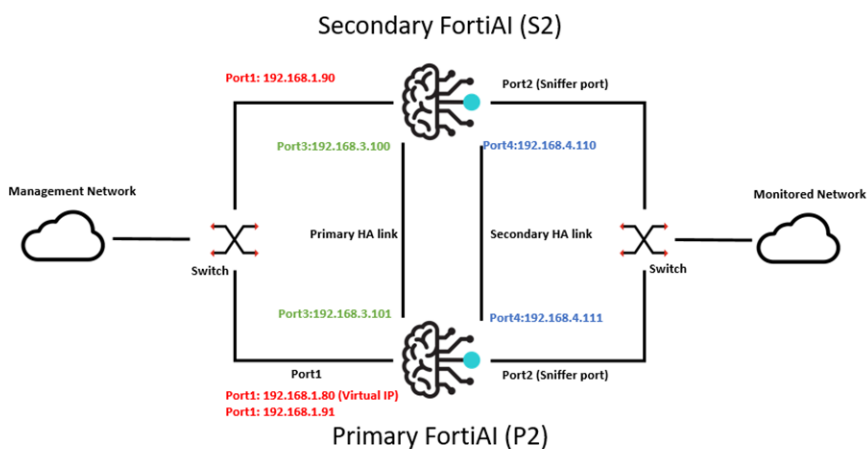
HA Failover

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 not synchronized from the Primary unit to the Secondary unit.

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

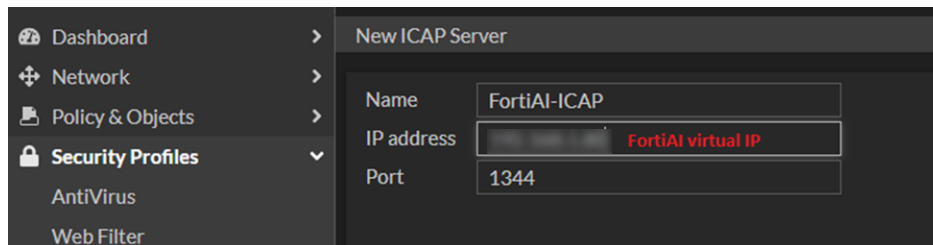
Using Virtual IP

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 120](#).

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.

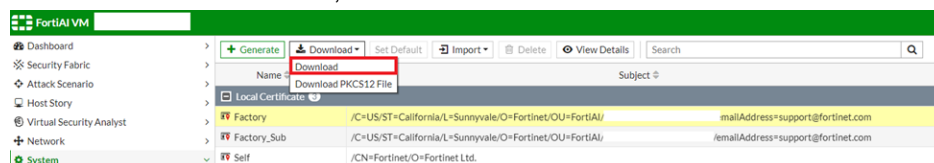


Example: Configure FortiGate Security fabric settings for inline blocking

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.

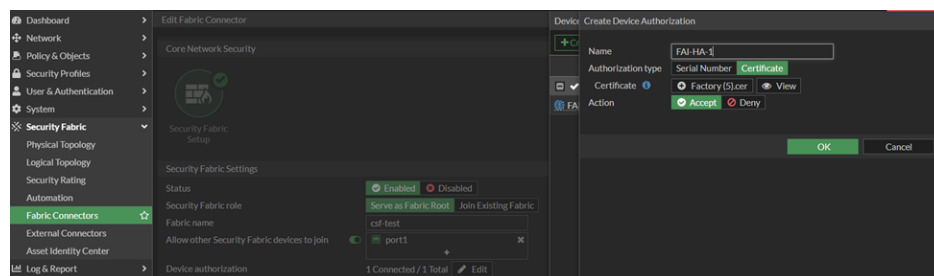
To configure FortiGate for inline blocking:

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



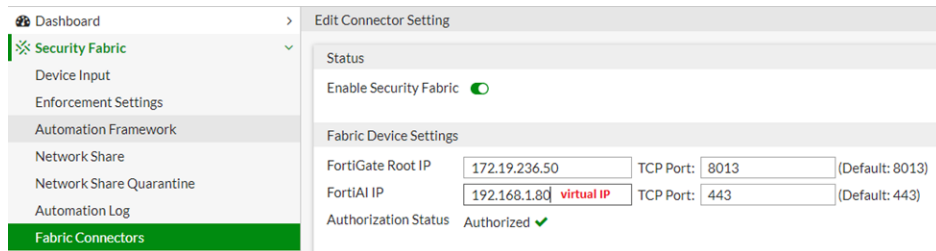
To add the certificate to FortiGate

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.




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 68.

Conserve Mode

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

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

Backup or restore the system configuration

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



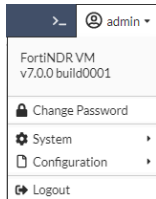
The following data is not backed up at this time:

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

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

To backup the FortiNDR configuration to your local computer:

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



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

To restore the system configuration from your local computer:

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

User & Authentication

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

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



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

RADIUS Server

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

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

The following options are available:

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

The following information is displayed:

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

To create a new RADIUS server:

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

3. Configure servers settings.

Profile name	Enter a name for the profile.
Server name/IP	Enter the server name and IP address.
Protocol	Select one of the following from the dropdown: <ul style="list-style-type: none"> • Default Authentication Scheme • Password Authentication • Challenge Handshake Authentication • MS Challenge Handshake Auth • Ms Challenge Handshake Auth V2
NAS IP/Called station ID	Enter the NAS IP address and called station ID.
Server Secret	Click <i>Change</i> to change the secret.

4. Click OK.

LDAP Servers

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

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

The following options are available:

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

The following information is displayed:

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

To add an LDAP server:

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

3. Configure server settings.

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

	<p>LDAP directory tree.</p> <ul style="list-style-type: none"> • <i>Subtree</i>: Query recursively all levels below the Base DN in the LDAP directory tree.
Derefer	<p>Select the method to use, if any, when dereferencing attributes whose values are references.</p> <ul style="list-style-type: none"> • <i>Never</i>: Do not dereference. • <i>Always</i>: Always dereference. • <i>Search</i>: Dereference only when searching. • <i>Find</i>: Dereference only when finding the base search object.
User Authentication Options	<p>Enable to configure the authentication options.</p> <p>Select one of the following from the dropdown.</p> <ul style="list-style-type: none"> • <i>Try UPN or mail address as bind DN</i> • <i>Try common name with base DN as bind DN</i> • <i>Search user and try bind DN</i>.
Advanced Options	
Timeout (seconds)	Enter the maximum amount of time in seconds that the FortiNDR unit will wait for query responses from the LDAP server.
Protocol version	Select the LDAP protocol version used by the LDAP server: <i>LDAP Version 2</i> or <i>LDAP Version 3</i> .
Allow Unauthenticated Bind	Disable bind authentication.
Enable Cache	<p>Enable to cache LDAP query results.</p> <p>Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiNDR unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently.</p> <p>If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.</p>
Clear Cache	<p>Select to empty the FortiNDR unit's LDAP query cache.</p> <p>This can be useful if you have updated the LDAP directory, and want the FortiNDR unit to refresh its LDAP query cache with the new information.</p>
TTL (minutes)	<p>Enter the amount of time, in minutes, that the FortiNDR unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiNDR unit to query the LDAP server, refreshing the cache.</p> <p>The default TTL value is 1440 minutes (one day). The maximum value is 10080 minutes (one week). Entering a value of 0 effectively disables caching.</p> <p>This option is applicable only if Enable cache is enabled.</p>

4. Click **OK**.

To edit an LDAP server:

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

LDAP user query example

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

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

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

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

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

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

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

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

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

Alias member query example

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

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

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

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

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

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

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

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

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

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

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

Preparing your LDAP schema for FortiNDR LDAP profiles

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

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



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

Using common schema styles

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

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

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

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

In this scenario, it may be sufficient to:

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

Log & Report



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

Malware Log

The *Log & Report > Malware Log* page displays the malicious malware detected by FortiNDR. Double-click an entry to view a summary of the log.

FortiNDR-VM											
Detected Processed Processing											
View Sample Detail Search Showing Zip Container											
Date	MD5	File ID	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk	Indicator
2023/08/01 13:50:19	ED63C3DA4A4EAF54E85885CF66A74CADA	169664	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	
2023/08/01 13:50:19	8A548168990BC78AFAFC63FE77A53ED8	169662	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	
2023/08/01 13:50:19	7DF8258FD825538313596694E28F8584	169659	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	IOC
2023/08/01 13:50:19	7B7F4398283F886DAD83263A3D17FE2	169655	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	

The *Malware Log* contains the following tabs:

Detected	Malicious files processed by FortiNDR engines.
Processed	Both clean and malicious files processed by FortiNDR engines.
Processing	Files that still being processed by FortiNDR parsers. The <i>Processing</i> tab is not available in Center mode.

Each tab displays the following information:

Date	The detection date.
MD5	The MD5 has value.
Sensor	The sensor type. Hover over the sensor to view the sensor the <i>IP Address</i> , <i>Last Synch Time</i> , and <i>Status</i>
File ID	The file ID.
File type	The file type. <i>Other</i> indicates the detected file type is not supported by Artificial Neural Networks (ANN).
Detection Name	The unique name of the malware. Click the name view a description in FortiGuard.
Device Type	The device type.
VDOM	The VDOM name.

Attacker	The attacker IP address.
Victim	The victim IP address.
Confidence	The confidence level as a percentage.
Risk	The risk verdict (High, Medium, Low or No Risk).
Indicator	Indicates the detection has IOC details.
Feature Detection	The detection feature type of the malware.

Viewing the sample details

The *Sample* details page contains the sample meta data and detection information if detected by FortiNDR. You can download the sample from the details page if the sample has been detected as malware. The downloaded sample is compressed as ZIP file with default password *Infected*.

To download a sample:

1. Go to *Log & Report > Malware Log*.
2. (Optional) Enable *Showing Zip Container* to download samples detected as malware.
3. Select a sample and click the *View Sample Detail* button at the left side of the *Search* field. The *Sample* details page opens.
4. Click the *Download File* button at the top right-side of the page.

← Back
Sample 169636
Information View
+ Add to Allow List
Generate Report
Download File

Generic Trojan

Confidence level: High 100.0%

Sample Information

Submitted Date	2023/08/01 13:50:19	Last Analyzed	2023/08/01 13:50:23
File Type	PE	File Size	15911(15.5 KB)
URL	//172.19.243.167/mal/c31d022f9c3dc06655d0d4951b8dcb2e		
File Name	c31d022f9c3dc06655d0d4951b8dcb2e		
MDS	C31D022F9C3DC06655D0D4951B8DCB2E VT		
SHA256	E699BA2868DEC7D2314FA576A695EB0765C3D6593AE33F1454138D3F9F7FEED2		
SHA1	448D7FF0E773134E2A6C8721D6586481587AF8F		
Detection Name	W32/CorruptRop/Sidam	Virus Family	N/A
Detected By	AV Engine		

Source Device

Device Type	Network Share
-------------	---------------

Network

Attacker	172.19.243.167: N/A	Victim	172.19.243.167: N/A
----------	---------------------	--------	---------------------

Feature Composition

- Generic Trojan

1 Detection(s)

Feature Type	Appearance In Sample
Generic Trojan	1

History

Search

View all History

Date	MDS	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk
2023/08/01 13:50:19	C31D022F9C3DC06655D0D4951B8DCB2E	PE	W32/CorruptRop/Sidam	Network Share		172.19.243.167	172.19.243.167	High 100.0%	Low

To view items in a zip folder:

1. In the *File Type* column, click the *Filter/Configure Column* icon and select *Zip*.

FortiNDR-VM				Filter																	
Detected Processed Processing																					
View Sample Detail				File Type == ZIP X Search																	
Date	MDS	File ID	File Type																		
2023/08/01 12:42:24	58EF5AD5826AA7F51C73755860F832D3	25175	ZIP																		
2023/08/01 12:40:47	D8825A2B7F199F4D068885488154C46F	23527	ZIP																		
2023/08/01 12:40:37	585388D63D885C6314C7C48A8A8E788B	22494	ZIP																		
2023/08/01 12:39:38	7A8787446EBFF1B986588F9B7DC898C7	19597	ZIP																		
2023/08/01 12:37:51	93880DEBC90DFD9C8D23FC6F317AF	18016	ZIP																		
2023/08/01 12:35:52	83134E3819341C1965895826F8238E7A	14921	ZIP																		
2023/08/01 12:35:46	CC43A5625B9C88E82A78FA78D885FA43	14236	ZIP																		
2023/08/01 12:35:31	287193885948FE2E8FB879F92F91DEC6	12842	ZIP																		
2023/08/01 12:35:30	13A4C749DA89886411C7C21854F91AB	12768	ZIP																		
2023/08/01 12:35:22	92AD7143E8AC8258BAC8648BCD9588	12522	ZIP																		
2023/08/01 12:35:07	8A86986C7F81B31A238EFA95DE72E64	11673	ZIP																		
2023/08/01 12:34:56	67DC9A84FE4D014ED5F14F7D3D2C8ABC	11073	ZIP																		
2023/08/01 12:14:02	8A818478A3246FA683F19E56E8CEFC6	9657	ZIP																		
2023/08/01 12:13:59	8F44D288633962E89F3CD21F065F538D	9597	ZIP																		
2023/08/01 12:13:56	A3C3E427D78143596C53437878855198	9547	ZIP																		

2. Double-click a log to view the contents of the folder.

Detected Processed Processing							Details			
Open Archive File Type == ZIP X Search							View Detail Search Generate Report			
Date	MDS	File ID	File Type	Detection Name	Device Type	VDOM	Date	MDS	File Type	Detection Name
2023/08/01 12:42:24	58EF5AD5826AA7F51C73755860F832D3	25175	ZIP	W32/CorruptRop.Sldam	Network Share		2023/08/01 12:13:59	01A8F78098D078EAC9738CAE3DC8...	PE	W32/WannaCry.1E881tr
2023/08/01 12:40:47	D8825A2B7F199F4D068885488154C46F	23527	ZIP	W32/CorruptRop.Sldam	Network Share		2023/08/01 12:13:59	88ADE53A3983859899AAEAE6268...	ZIP	Clean
2023/08/01 12:40:37	585388D63D885C6314C7C48A8A8E788B	22494	ZIP	W32/CorruptRop.Sldam	Network Share		2023/08/01 12:13:59	C8FA78C87EEBC8680E841FF83A68...	7Z	Clean
2023/08/01 12:39:38	7A8787446EBFF1B986588F9B7DC898C7	19597	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:37:51	93880DEBC90DFD9C8D23FC6F317AF	18016	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:35:52	83134E3819341C1965895826F8238E7A	14921	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:35:46	CC43A5625B9C88E82A78FA78D885FA43	14236	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:35:31	287193885948FE2E8FB879F92F91DEC6	12842	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:35:30	13A4C749DA89886411C7C21854F91AB	12768	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:35:22	92AD7143E8AC8258BAC8648BCD9588	12522	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:35:07	8A86986C7F81B31A238EFA95DE72E64	11673	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:34:56	67DC9A84FE4D014ED5F14F7D3D2C8ABC	11073	ZIP	W32/CorruptRop.Sldam	Network Share					
2023/08/01 12:14:02	8A818478A3246FA683F19E56E8CEFC6	9657	ZIP	W32/Svls.A/tr	Network Share					
2023/08/01 12:13:59	8F44D288633962E89F3CD21F065F538D	9597	ZIP	W32/WannaCry.1E881tr	Network Share					
2023/08/01 12:13:56	A3C3E427D78143596C53437878855198	9547	ZIP	W32/Agent.4FE0/tr	Network Share					

To perform a batch download:

1. Select the files to download.
2. Click Batch Download. The files are zipped with a password and downloaded to your device.

To add detections to the Allow List:

1. Go to *Log & Report > Malware Log*.
2. Right-click a sample and select, *Add to Allow List*. The *Add to Allow List* pane opens.

Optionally, you can click *View Sample Detail* and click *Add to Allow List*.

3. (Optional) In the *Comments* field, enter a comment about the detection.
4. (Optional) Enable *Submit feedback to FortiGuard* and then enter your *Contact Email* and your feedback in the *Comment* field.
5. Click *OK*.

Optionally, you can click *View Sample Detail* and click *Add to Allow List*.

Advanced search

You can search for detections with *Search* function or by right-clicking a detection and selecting an option from the menu.

To use the Search feature:

1. Type key words into the *Search* field. Partial results are displayed.
2. Click the plus sign (+) to include filterable columns in your search.
3. To refine the search results, click the filter icon in the column header.

To search a detection:

Right-click a detection and select one of the following options:

- *Filter by MD5*
- *Search by Hash*
- *Search similar file(s) with Hash*
- *Search by Detection Name*
- *Search similar file(s) by Detection name*

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

admin

Dashboard

Network Insights

Security Fabric

Attack Scenario

Host Story

Virtual Security Analyst

Network

System

User & Authentication

Log & Report

Malware Log

NDR Log

Events

Daily Feature Learned

Log Settings

Email Alert Setting

Email Alert Recipients

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.

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

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.

Open Time	Session ID	Source Address	Destination Address	Severity	Application Layer Protocol
2023/08/01 12:02:41	9215			Not Anomaly	MODBUS
2023/08/01 12:02:41	9211			Not Anomaly	MODBUS
2023/08/01 12:02:41	9168			Not Anomaly	MODBUS
2023/08/01 12:02:41	9130			Not Anomaly	MODBUS
2023/08/01 12:02:41	9116			Not Anomaly	MODBUS

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

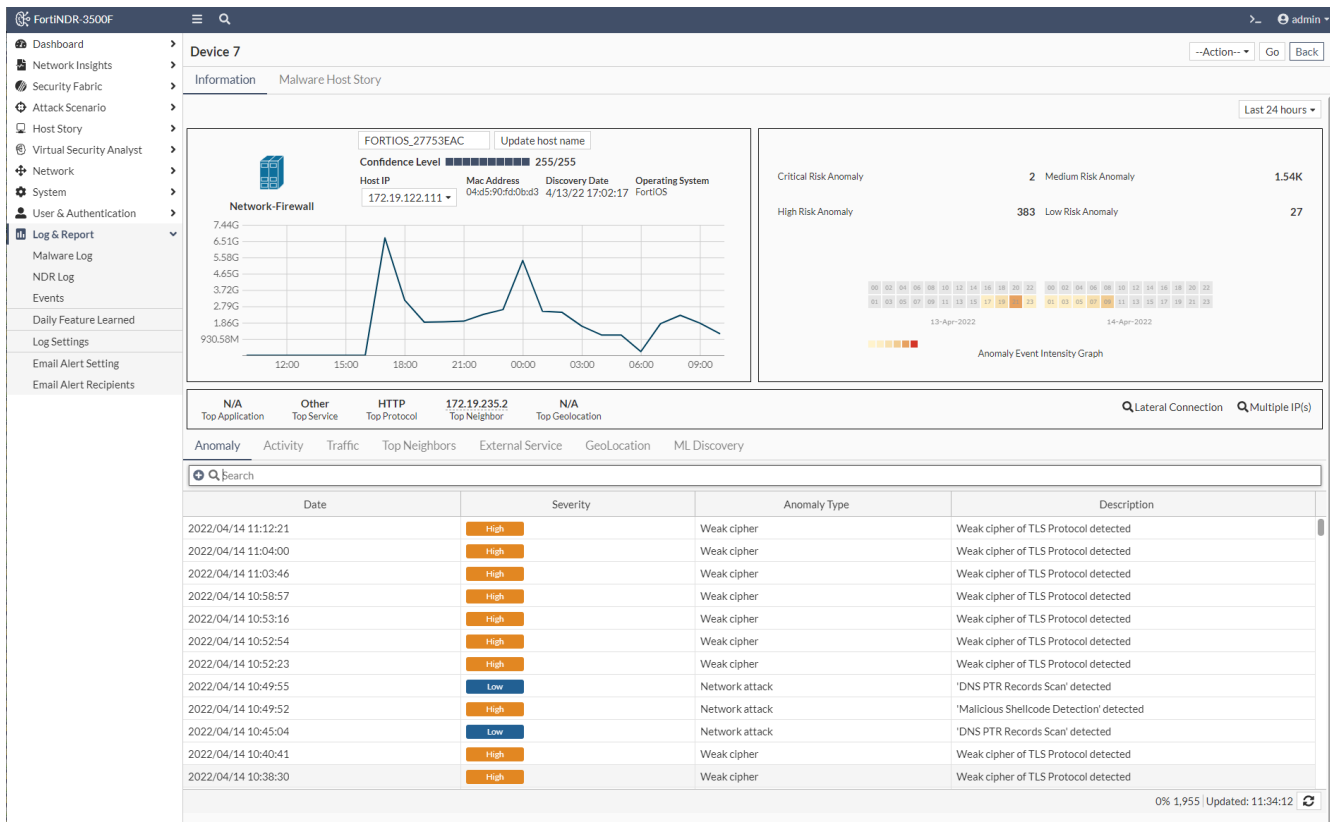
Device Tab

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.

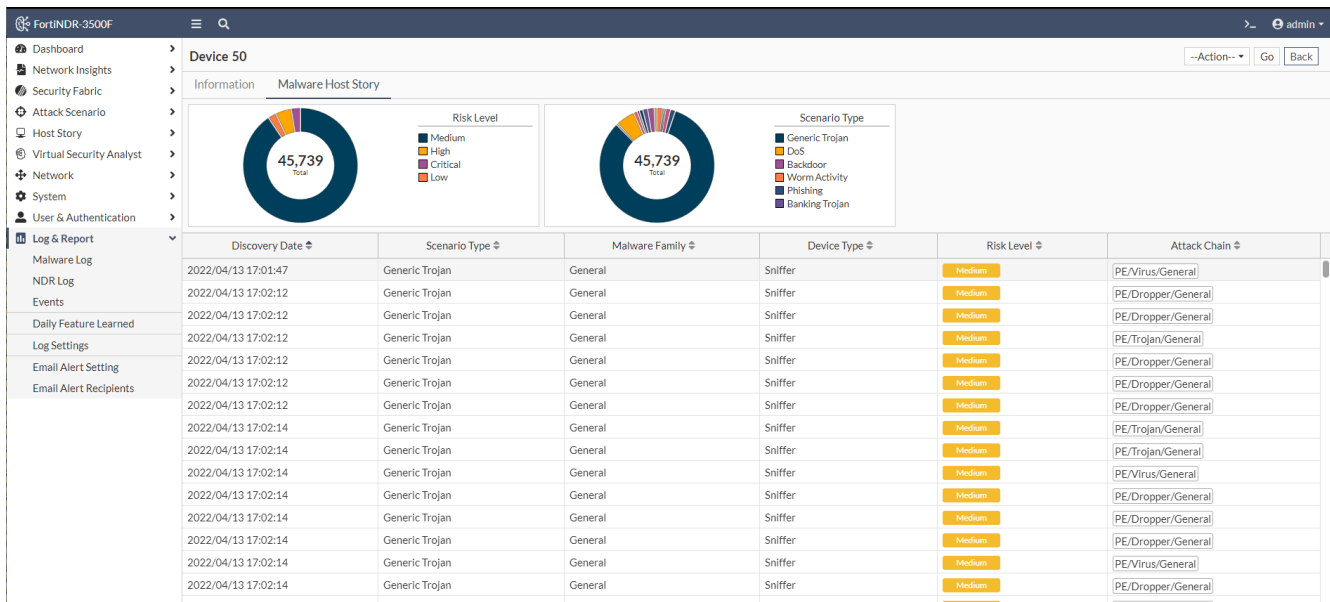
Anomaly Session Device							
View Device Detail + Q Search							
Last Seen	Discovery Time	Device	MAC Address	Latest Address	Role	Status	Confidence
2022/04/18 16:30:48	2022/04/13 17:02:19	UNKNOWN_0E321BDF	00:50:56:62:ad:0c	192.168.101.62		Online	N/A (0)%
2022/04/18 16:30:48	2022/04/13 17:02:19	UNKNOWN_48654F8B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



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



Events

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

The *Events* page displays the following information:

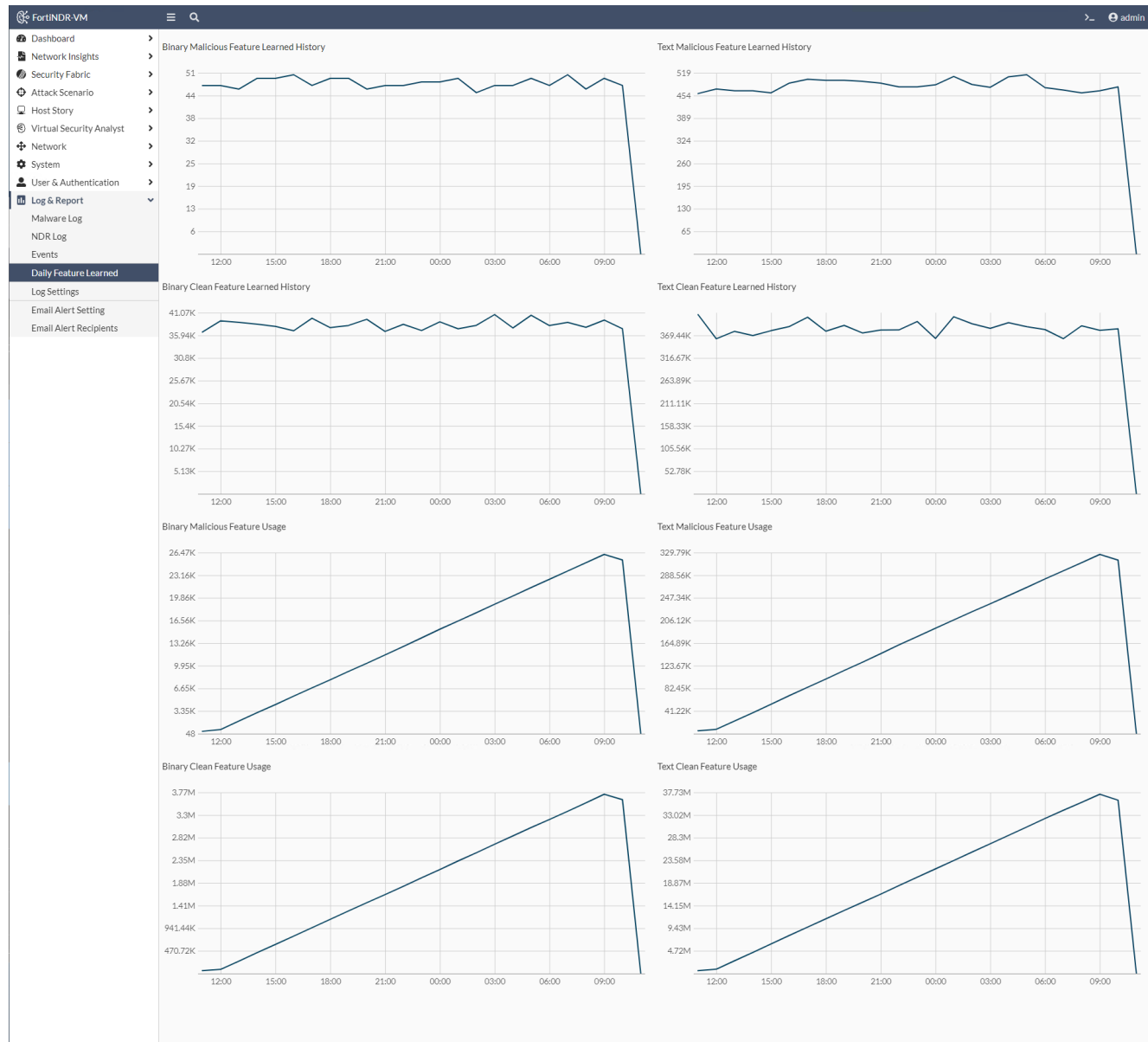
Date	The date the event occurred.
Level	The security level.
User	The user that triggered the event.
Message	The log message.

Double-click an entry in the table to view the event details:

General	The entry date.
Source	The event source.
Action	The <i>Action</i> and <i>Status</i> .
Security	The security level.
Event	The event message describing the event.
Other	The <i>Log ID</i> , <i>Category</i> and <i>Sub Category</i> if available.

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. This page is not available in Sensor mode.



Log Settings

Go to *Log & Report > Log Settings* 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 cannot trigger *Attack Scenario*. This is because the sample flows from attacker to victim and they do not have flows of virus.
- Inline, ICAP, Sniffer and OFTP detections will trigger Syslog being sent to FortiAnalyzer or FortiSIEM, since they have this information.

Log Settings in Center mode

In Center mode, the Log Settings can be configured to send the Center's system event log to the syslog servers. Detection logs, including malware logs and NDR logs that record events occurring in the sensors, are sent directly from the sensors themselves. To upload and edit the sensor syslog configurations, go to *System > Sensor Settings* and click *Restore Configuration*. For more information, see [Sensor Settings on page 111](#).

To configure the Log Settings:

1. Go to *Log & Report > Log Settings*.
2. Configure the following settings:

Send logs to FortiAnalyzer/FortiSIEM	Click to <i>Enable</i> or <i>Disable</i> .
Type	<i>Syslog Protocol</i> .
Log Server Address	Enter the FortiAnalyzer/FortiSIEM log server address.
Port	Enter the FortiAnalyzer/FortiSIEM port number. Default is <i>UDP: 514</i> .
Send logs to Syslog Server 1	Click to <i>Enable</i> or <i>Disable</i> .
Type	<i>Syslog Protocol</i> .
Log Server Address	Enter the Syslog Server 1 log server address.
Port	Enter the Syslog Server 1 log server port number. Default is <i>UDP: 514</i> .

3. Click *OK*.

Alert Email Setting

Go to *System > Alert Email Setting* to create email alerts when 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: [Change](#)

Using Openssl: ☒ Enable ☐ Disable

Trigger Setting

☐ HA Related Events
☐ Generic System Information including high cpu / low memory, notifications about file upload etc
☐ (VM Only) License Expired
☐ Scenario Detection Events
☐ NDR: Botnet Anomaly
☐ NDR: Encrypted Attack
☐ NDR: Indication of Compromise Detection
☐ NDR: Network Attack Detection
☐ NDR: Weak Cipher and Vulnerable Protocol Detection
☐ NDR: Machine Learning Detection

[OK](#) [Cancel](#)

3. Click **OK**.
4. Add email addresses to the email recipient list. See, [Email Alert Recipients on page 147](#).

Email Alert Recipients

Go to *Log & Report > Email Alert Recipients* to create a distribution list for email alerts.

To add recipients to an email 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.

NDR logs samples

Botnet

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

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

Fields

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

Encrypted

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

Fields

behavior	User activity, e.g. CONN, RESP, VISIT, GET etc.
vers	The version of alproto, str
cipher	The encryption algorithm.
md5	md5/hash of ja3 fingerprint

IOC

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

Fields

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

IPS attack

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

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

Fields

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

Weak cipher

```
date="2022-02-07" time="14:18:57" tz="PST" logid="0606000001" devid="FAIVMSTM21000033"
type="ndr" subtype="Weak cipher" severity="medium" sessionid=569705 alproto="IMAP"
tlproto="TCP" srcip="17.1.6.20" srcport=63310 dstip="18.2.1.114" dstport=443 behavior="CONN"
vers="2" cipher="TLS_NULL_WITH_NULL_NULL" ciphername="weak cipher"
```

```
date="2022-02-07" time="14:18:57" tz="PST" logid="0606000001" devid="FAIVMSTM21000033"
type="ndr" subtype="Weak cipher" severity="medium" sessionid=570387 alproto="SMB"
```

```
tlproto="TCP" srcip="17.2.12.171" srcport=10001 dstip="17.1.1.119" dstport=443
behavior="CONN" vers="1" cipher="TLS_RSA_WITH_AES_256_GCM_SHA384"
md5="9a157673907688965992b40304f50a1e" ciphername="weak version"
```

Fields

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

ML

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

Fields

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

Common Fields

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

dstip	Destination IP
dstport	Destination port

AV log samples

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

Log Type	Subtype	Log Sample
Attack	Attack chain	date="2021-05-21" time="10:23:05" tz="PDT" logid="0500000001" devhost="FAI35FT321000001" devid="FAI35FT321000001" type="attack" subtype="Attack Chain" level="alert" user="admin" ui="daemon" action="none" status="success" eventid=7255021 discoverydate="2021-05-21 10:13:27" risklevel="High", malwarefamily="N/A" scenariotype="Botnet" filecnt=1 filelist="435387294"
	Malware	date="2021-05-21" time="10:23:05" tz="PDT" logid="0521000001" devid="FAI35FT321000001" type="attack" subtype="Malware" level="alert" action="none" devicetype="sniffer" fossn="" fosvd="" fileid=435387294 filetype="PE" md5="ddc770fa317b4a49b4194e4dcf8d308e" virusname="W32/Rbot.15B3!tr" url="http://172.19.235.2/data/0/4B72XXXX/4B72B9D2.vRG" detype="N/A" subdetype="N/A" attackerip="172.19.235.2" attackerport=80 victimip="172.19.235.76" victimport=10578 detype1stcnt=3 detype1st="worm,trojan,downloader" detypecounts="64,64,2"

Troubleshooting

FortiNDR troubleshooting tips

For more information about the CLI commands below, please see the [FortiNDR CLI Reference Guide](#).

Best practices:

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

Recommended Debug Setup:

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

General Debug Logs Retrieval

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

File scanning related issues

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

To perform a general check:

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

Troubleshooting ICAP issues:

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

Troubleshooting OFTP issues:

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

Troubleshooting HTTP2 issues from FortiGate v7.0 onwards:

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

Manual Upload/API Submission/FortiSandbox Integration

For all issues:

Start with a single file upload and fetch results from the same subnet as directed from where the client resides. See [Appendix A: API guide on page 177](#).

To verify the process is successful:

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

- `diag debug enable`

and

- `diagnose debug application 7`

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

File Submitted but not processed

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

- `diag debug enable`

and

- `diagnose debug process <process_name>`

Information for support tickets

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

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

FortiNDR health checks

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

<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.

moat_engine	Script AI engine.
moat_learn	Script AI learner.

To turn network traffic detection on and off:

Run the following command:

```
exec ndrdr <on/off>
```

To turn sniffer malware detection on and off for troubleshooting:

Run the following command:

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



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

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

FortiNDR-3500F											
Accepted Processed Detected											
View Sample Detail Search Showing Zip Container											
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	5E88DE1C3B112734A7B94993850886DF	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	5E88DE1C3B112734A7B94993850886DF	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.

FortiNDR-3500F					
Anomaly Session Device					
View Session Detail Search					
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.



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

Rebuild RAID disk

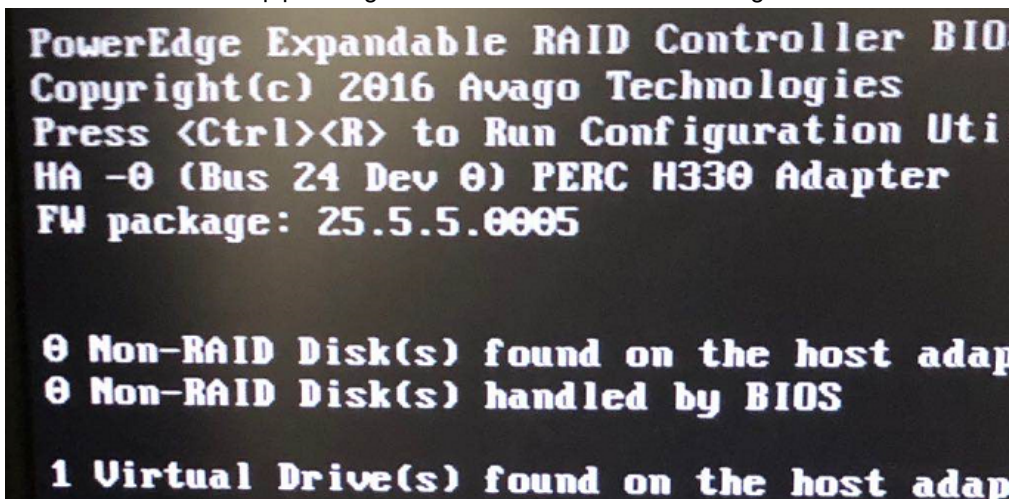
If you need to rebuild the data disk and configure FortiNDR-3500F from scratch, follow this procedure.

To rebuild the RAID disk:

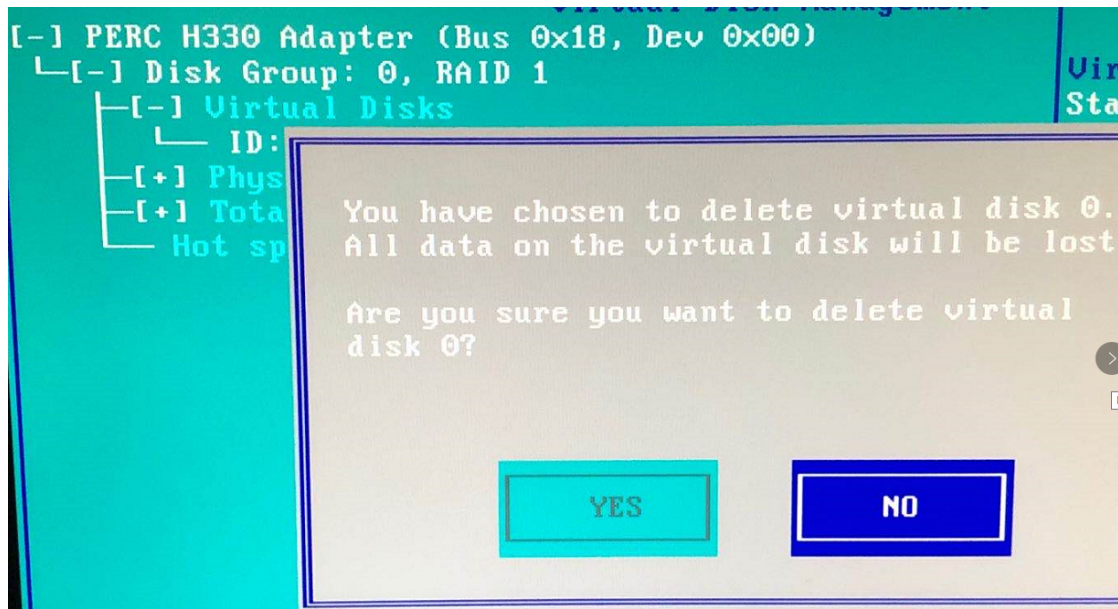
1. Plug the monitor and keyboard directly into FortiNDR.



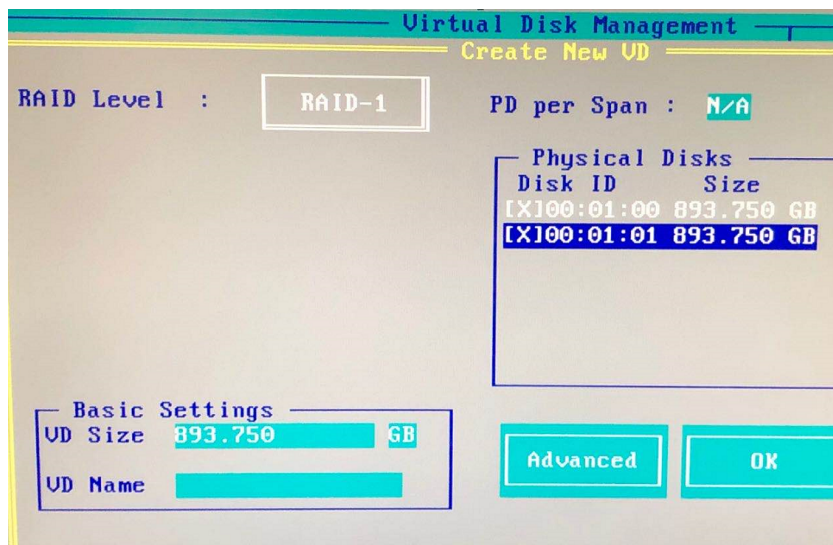
2. Boot FortiNDR and keep pressing **Ctrl R** when FortiNDR is booting.



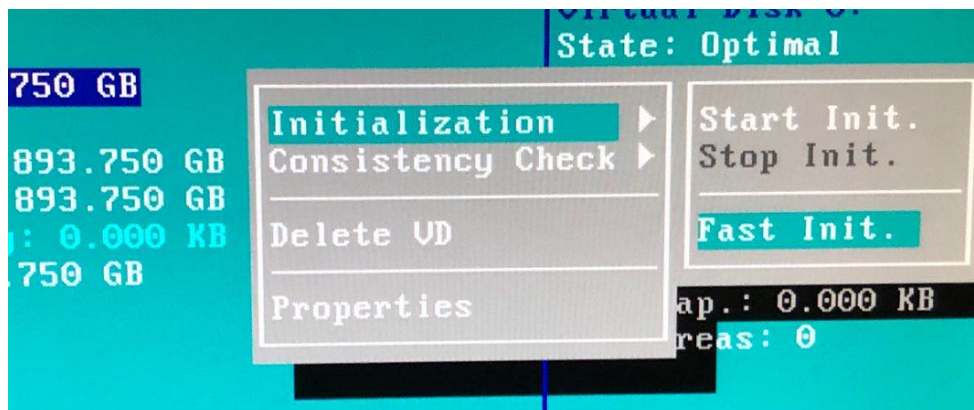
3. Delete virtual disk 0.



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



5. Fast init the new virtual disk.



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

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 four SSD drives by default and can add up to 16 SSD in total.

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

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

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

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

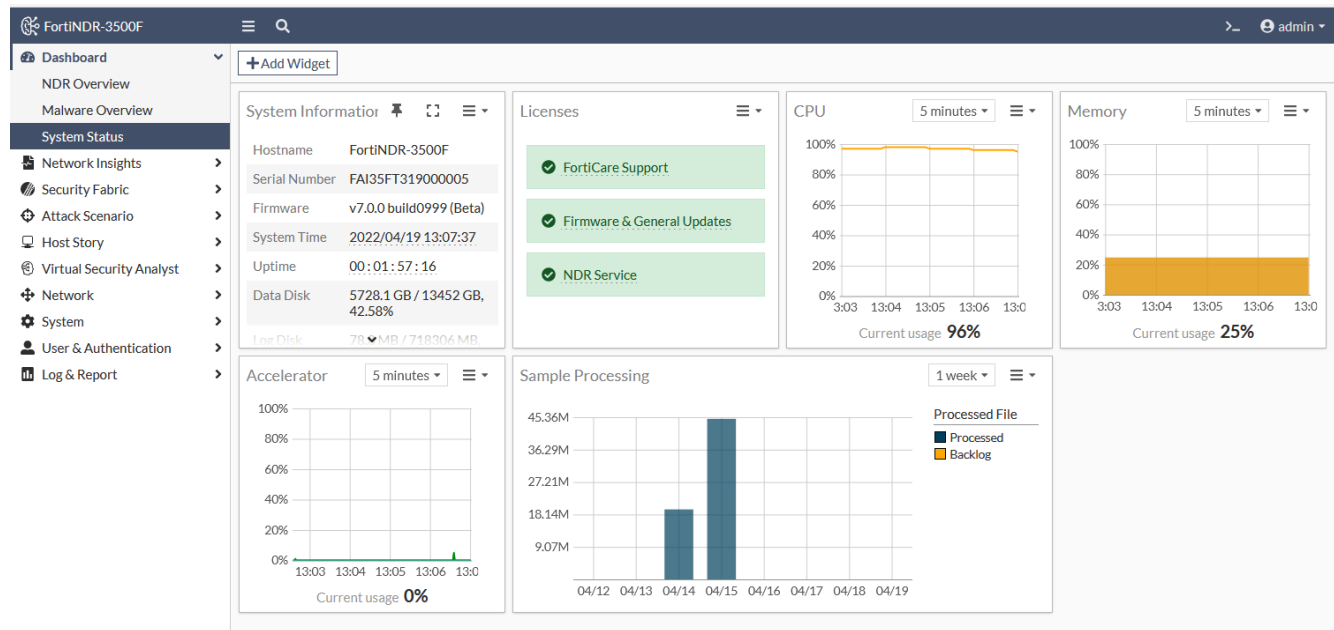
Tip 3: You should consider using CLIs to clean up the DB:

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

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

To view the disk usage:

Go to *Dashboard > System Status*.



To expand FortiNDR VM storage with the CLI:

```
execute expandspooldisk.
```

For more information, see the [FortiNDR CLI Reference Guide](#).

Exporting detected malware files

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

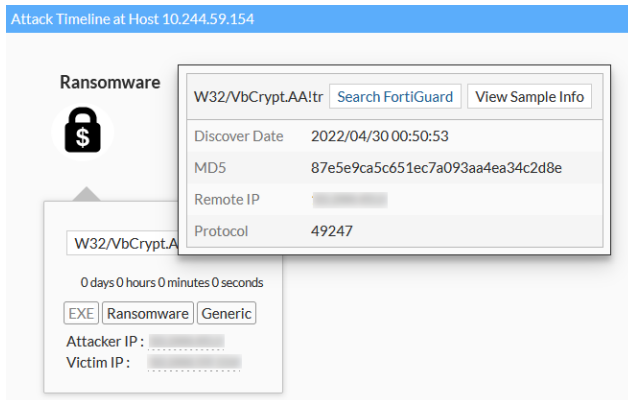
To export detected malware files with the CLI:

```
execute export file-report
```

For more information, see the [FortiNDR CLI Reference Guide](#).

To export detected malware files with the GUI:

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



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

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	5F082212E8DDAE8ABAF941926BD60824 vt		
SHA256	0A18BC20973E0691A9D35A9ABA610BF8EC45263C0A0E5A8ECBB A9AC5EE5E6996		
SHA1	99A4EB3D57268604D0758A904B82C8406735CC0C		
Detection Name	W64/Encoder.A!tr	Virus Family	N/A
Source Device			
Device Type	Sniffer		
Network			
Attacker	[redacted] (Registered port)	Victim	[redacted]

1 Detection(s)

Feature Type	Appearance In Sample
Ransomware	1

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	5F082212E8DDAE8ABAF941926BD60824	EXE	W64/Encoder.A!tr	Sniffer		[redacted]	[redacted]	100.00%

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 options like Dashboard, Network Insights, Security Fabric, Attack Scenario, Host Story, Virtual Security Analyst, Network, System, User & Authentication, Log & Report, Malware Log, NDR Log, Events, Daily Feature Learned, Log Settings, Email Alert Setting, and Email Alert Recipients. The 'Log & Report' section is expanded, and 'Malware Log' is selected. The main area displays a table of detected files. The first row is highlighted in yellow. To the right of the table is a 'Details' pane for the selected log entry, showing general information (File ID, Time, File Size, File Type, MD5), detection details (Virus Name, Confidence Level, Threat Risk Level, Detection Type), network information (Attacker IP, Victim IP, URL), and device information (Device, Sniffer).

Date	MD5	File Type	Detection Name
2022/04/30 00:52:33	A3F3E85639E56868383C4716560AE5A7	HTML	HTML/Refresh.250C!tr
2022/04/30 00:52:33	BE5EC605F7D210F46AD0804708C001F0	HTML	MOAT.AttrTag
2022/04/30 00:52:33	61D98B3423A16FF7A2381CB3869CD881	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:33	6993F1CFA28A788229C37D87000059C6	HTML	MOAT.AttrTag
2022/04/30 00:52:33	CC4551CFDA35E14D836A8FF37738B96D	HTML	JS/ExploitKIL29C6!tr
2022/04/30 00:52:33	E1E777A357907F35B438661A6EF05A73	PDF	MOAT.AttrTag
2022/04/30 00:52:33	E1E777A357907F35B438661A6EF05A73	PDF	MOAT.AttrTag
2022/04/30 00:52:33	2E915432AD8142D70ADC9362808B710D	EXE	W32/Graffor.FL!tr
2022/04/30 00:52:33	C3FA38DD42B7C276ADDED1CCD508B560	EXE	W32/AL.Suspicious.2
2022/04/30 00:52:33	373C65D985C174D736BA8D496A777818	MSOFFICE	VBA/Emotet.2826!tr.dldr
2022/04/30 00:52:33	B141EA5708C154D62CC54A14E5F5B387	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	E08367D9D5B38B34DB3C52B05760AFA7	PDF	PDF/Phishing.0931!tr
2022/04/30 00:52:33	1D21C3EAD6E6F97066500E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:33	51927D0C4151DDE98000E652B1B557F5	PDF	MOAT.AttrTag
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	MOAT.AttrTag
2022/04/30 00:52:19	2598DFB1E1C67B5B467259879B10A71F	HTML	MOAT.AttrTag
2022/04/30 00:52:19	8057821F44FAD32631847B9D0C2488A5	HTML	MOAT.AttrTag
2022/04/30 00:52:19	1D21C3EAD6E6F97066500E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:19	7DD7D15D6BE0D443EAEDF5D1E90D8EE6	HTML	JS/ScriptInject.B!tr

- 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
```

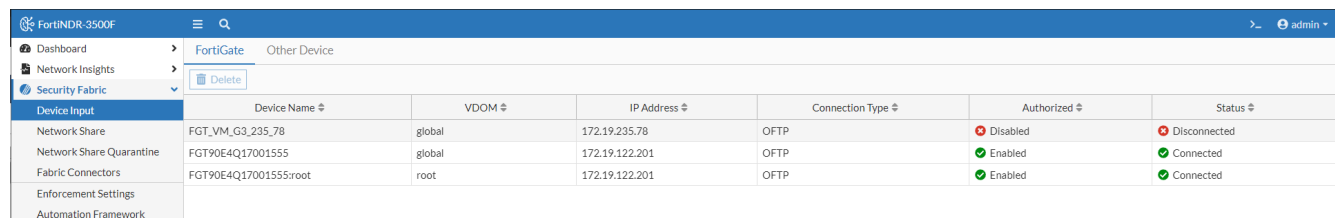
To check OFTP traffic in port1:

Use the CLI command:

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

To verify a device is authorized:

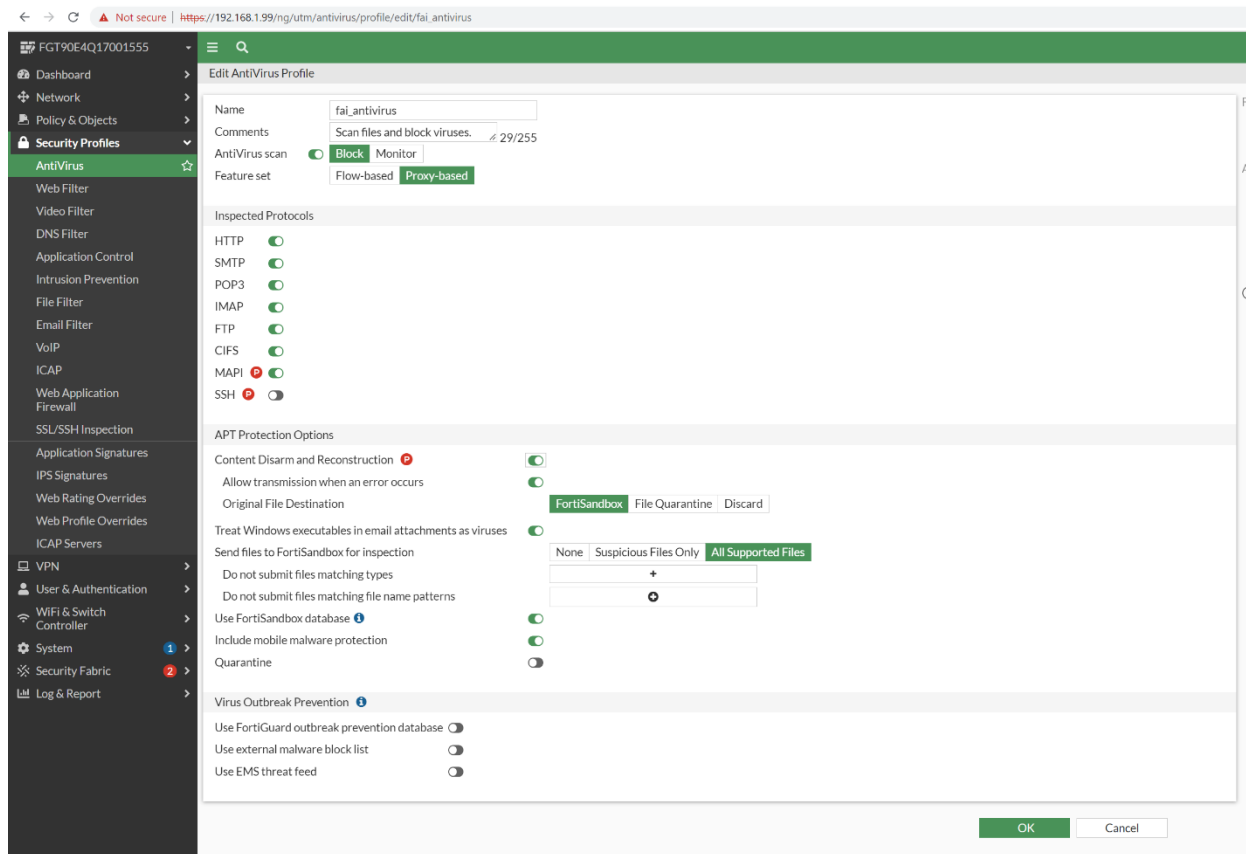
Go to *Security Fabric > Device Input* and check the Authorized column.



	Device 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
Enforcement Settings						
Automation Framework						

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

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

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.

FortiNDR-3500F

Dashboard > Network Insights > Security Fabric > Network Share > Network Share Quarantine > Fabric Connectors > Enforcement Settings > Automation Framework > Automation Log > Attack Scenario > Host Story > Virtual Security Analyst > Network > System > User & Authentication > Log & Report >

### Edit Network Share

Status: ☒ Enable ☐ Disable

Mount Type: SMBv2.0

Network Share Name: 172.19.235.244 ?

Server IP: 172.19.235.244 ?

Share Path: \\c ?

Username: administrator

Password: ..... [Change](#)

Confirm Password: ..... [Change](#)

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: Daily

At hour: 04:00 AM

Description:

[OK](#) [Cancel](#)

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 <a href="#">To troubleshoot mounting problems</a> above.                                                                                    |
| Daemon crashed           | Run the following CLI command to see if there are any <code>sdigestd</code> related crashes:<br><code>diagnose debug crashlog xxxx-xx-xx</code> |
| Data disk usage over 90% | Clean up the data disk. See, <a href="#">Managing FortiNDR disk usage on page 160</a> .                                                         |

## 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.. | 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
```

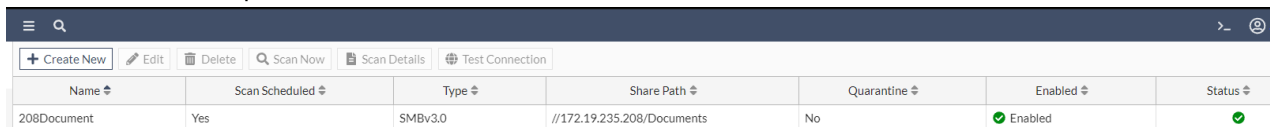
A `DEBUG_LEVEL` is a bit mask consisting of 3 bits.

- 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.

## Troubleshooting tips for Network File Share

**To troubleshoot Network File Share issues:**

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



| Name        | Scan Scheduled | Type    | Share Path                 | Quarantine | Enabled | Status |
|-------------|----------------|---------|----------------------------|------------|---------|--------|
| 208Document | Yes            | SMBv3.0 | //172.19.235.208/Documents | No         | Enabled | ✓      |

2. Turn off FortiGuard scheduled updates to rule out any update related issues.
3. Turn off the NDR daemon to isolate the environment using CLI command:

```
exec ndrd off
```

This command is not persistent. If a reboot is required, run the command again.

4. Turn off Sniffer daemon to isolate the environment using

```
exec snifferd off
```

This command is not persistent. If a reboot is required, run the command again.

5. Set filesize limit to smaller size to rule file size issues using the CLI command:

```
exec file-size-threshold network-share 20 (MB)
```



6. Click *Test Connection*.

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

| + Create New Edit Delete Scan Now Scan Details Test Connection |                |         |                            |            |          |        |
|----------------------------------------------------------------|----------------|---------|----------------------------|------------|----------|--------|
| Name                                                           | Scan Scheduled | Type    | Share Path                 | Quarantine | Enabled  | Status |
| 208Document                                                    | No             | SMBv3.0 | //172.19.235.208/Documents | No         | Disabled |        |
| 208Download                                                    | Yes            | SMBv3.0 | //172.19.235.208/Downloads | No         | Enabled  |        |
| 208Music                                                       | Yes            | SMBv3.0 | //172.19.235.208/Music     | No         | Enabled  |        |
| 208Pictures                                                    | No             | SMBv3.0 | //172.19.235.208/Pictures  | No         | Disabled |        |

Network Share is inaccessible. X

7. When the scan is stuck, please the following logs using the CLI:

- a. `exec deb kernel display`

```
[1130653.376058] CIFS VFS: cifs_mount failed w/return code = -2
[1130693.246699] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
[1130693.323312] CIFS VFS: cifs_mount failed w/return code = -2
[1130732.993744] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
[1130733.070712] CIFS VFS: cifs_mount failed w/return code = -2
[1130772.114649] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
[1130772.191267] CIFS VFS: cifs_mount failed w/return code = -2
[1130811.244384] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
[1130811.320970] CIFS VFS: cifs_mount failed w/return code = -2
[1130850.318055] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
[1130850.395166] CIFS VFS: cifs_mount failed w/return code = -2
[1130889.657445] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
[1130889.734093] CIFS VFS: cifs_mount failed w/return code = -2
[1130929.674178] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
[1130929.750821] CIFS VFS: cifs_mount failed w/return code = -2
```

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

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

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

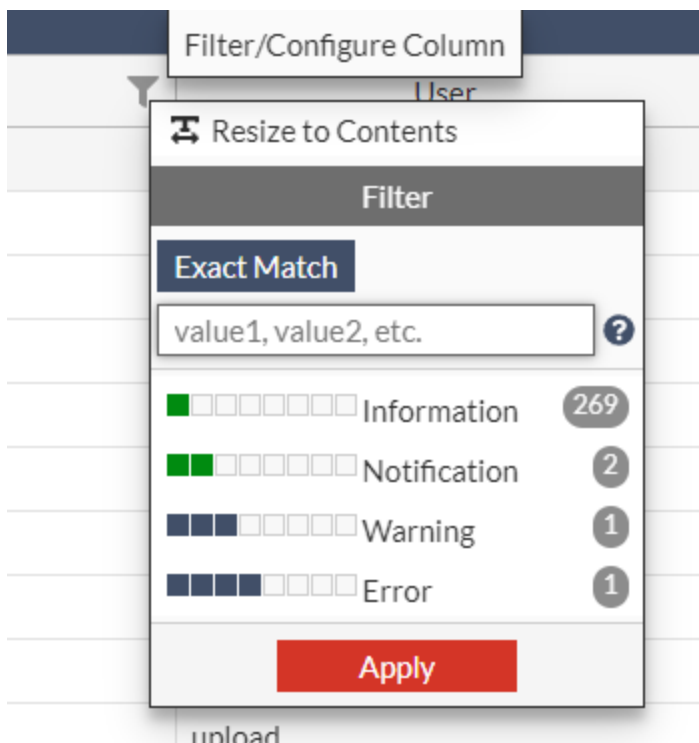
`get system status`

```

Serial Number: 1H2001102900001
BIOS version: 00010001
Log disk: Capacity 349 GB, Used 76 MB (0.03%), Free 349 GB
Data disk: Capacity 6710 GB, Used 910 GB (13.57%), Free 5799 GB
Remote disk: n/a
Memory: Capacity 375 GB, Used 76 GB (20.32%), Free 299 GB
Swap Memory: Capacity 31 GB, Used 0 MB (0.00%), Free 31 GB
Hostname: FortiNDR-3500F
HA configured mode: Off
HA effective mode: Off
Strong-crypto: enabled
Distribution: International
Branch point: 27
Uptime: 13 days 5 hours 33 minutes
Last reboot: Fri Nov 04 16:23:45 PDT 2022
System time: Thu Nov 17 20:57:12 PST 2022
Firmware & ANN update expiry: Sun Mar 12 00:00:00 PST 2023
NDR services/update expiry: Mon Feb 20 00:00:00 PST 2023
Binary AI Feature DB: 1_11000(2022-11-17 20:28)

```

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



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

| FortiNDR-3500F           |             |         |          |                                                                        |
|--------------------------|-------------|---------|----------|------------------------------------------------------------------------|
|                          | Date        | Level   | User     | Message                                                                |
| Dashboard                | 2 hours ago | Warning | sdigestd | network share job for 208Pictures paused due to share status was down. |
| Network Insights         | 3 hours ago | Warning | sdigestd | network share job for 208Download is timeout.                          |
| Security Fabric          | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |
| Attack Scenario          | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |
| Host Story               | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |
| Virtual Security Analyst | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |
| Network                  | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |
| System                   | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |
| User & Authentication    | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |
| Log & Report             | 3 hours ago | Warning | sdigestd | network share job for 208Download paused due to share status was down. |

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

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

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

For more information, see [Troubleshoot Network Share on page 167](#).

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

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

Here is an example showing which mount failed during mounting:

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

FortiNDR-3500F # 11.17-20:55:42 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Document)
11.17-20:55:42 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Document)
11.17-20:55:42 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Pictures)
11.17-20:55:42 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Pictures)
11.17-20:55:42 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Music)
11.17-20:55:42 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Music)
11.17-20:55:48 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Document)
11.17-20:55:48 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Document)
11.17-20:55:48 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Pictures)
11.17-20:55:48 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Pictures)
11.17-20:55:48 <WARN>sdigest_mount.cpp[262] [NetworkShare] Umount failed for share (208Music)
11.17-20:55:48 <INFO>sdigest_share.cpp[157] [NetworkShare] Disabled (208Music)
```

□

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

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

# Appendix A: API guide

This section shows how to use the FortiNDR API.

## Get an administrator API key

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

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

## Upload files using API

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

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

### To generate a token using CLI:

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

### To generate a token using GUI:

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

The screenshot shows the FortiNDR GUI. On the left is a sidebar with a navigation menu. The 'System' menu item is highlighted in green, and under it, 'Administrator' is also highlighted. The main content area is titled 'Edit Administrator'. It contains several sections: 'Username' with a text input field containing 'admin' and a 'Change Password' button; 'Admin profile' with a dropdown menu showing 'SuperAdminProfile' and '+ New' and 'Edit' buttons; 'Authentication' with a dropdown menu showing 'Local'; 'Preference' section with a 'Theme' dropdown menu showing 'Green'; a toggle switch for 'Restrict login to trusted hosts'; and an 'API Key' section at the bottom. The 'API Key' section displays the generated API key: 'u4VvEDpUATpJbFUfpbCzISduTddCOIs'.

## 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 [FortiNDR traffic and files input types on page 12](#).

Submit a file using one of the following methods.

| Method          | Description                                                                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| JSON data       | The JSON data must be encoded in base64 format.<br>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.<br>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': 'xxxxxxx'})
```

## 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 obtained after uploading a file. |
| fileid                            | Get verdict result from file ID.                                   |
| md5                               | Get the latest verdict result from MD5 checksum of the file.       |
| sha1                              | Get the latest verdict result from SHA1 checksum of the file.      |
| Sha256                            | Get the latest verdict result from SHA256 checksum of the file.    |

The query string can only have one search query parameter.

### Examples

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

{
 "results": {
```

```

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

```

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

GET /api/v1/verdict?fileid= \*\*\*file\_id\*\*\*

```

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

```



| Field               | Description                                                                                                                                                                                                                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| file_id             | ID of the file.                                                                                                                                                                                                                                                                                                                         |
| virus_name          | FortiNDR virus name.                                                                                                                                                                                                                                                                                                                    |
| source              | For file uploaded by API or GUI, <i>source</i> is <i>manual upload</i> , otherwise it is an URL.                                                                                                                                                                                                                                        |
| severity            | <i>No Risk, Low, Medium, High, or Critical.</i>                                                                                                                                                                                                                                                                                         |
| category            | For clean file: <i>Clean</i> .<br>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.<br><i>feature_type</i> is the category which the detected feature belongs to.<br><i>appearance_in_sample</i> is the number of appearances that the feature FortiNDR has detected.                                                                                  |
| confidence          | For clean file: <i>N/A</i> .<br>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.                                                                                                                                                                                                                                                                                                                             |
| parent_fname        | The archive file name if the current file was extracted from an archive/zip file.                                                                                                                                                                                                                                                       |

### Example of problems retrieving results

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

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| http_code | See <a href="#">HTTP status table on page 183</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| message   | Messages include:<br><i>DATA_NOT_EXIST</i> when result data cannot be found given the search query parameter.<br><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.<br><i>INVALID_PARAM_NUMBER</i> when zero or more than one search query parameters exist.<br><i>INVALID_PARAM</i> when search query value is not valid. |

**Submitted file errors explanation:**

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

- Oversized file
- Oversized archive contents

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

In the other following cases:

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

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

```
{
 "results": {
 "fileids": [xx],
 "total_fileids": x
 }
}
```

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

In the following two cases:

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

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

**Get file stix2 report****/api/v1/report**

| Supported search query parameters | Description                                                         |
|-----------------------------------|---------------------------------------------------------------------|
| <code>fileid</code>               | Get report from file ID.                                            |
| <code>md5</code>                  | Get report of the latest file with the MD5 checksum of the file.    |
| <code>sha1</code>                 | Get report of the latest file with the SHA1 checksum of the file.   |
| <code>sha256</code>               | Get report of the latest file with the SHA256 checksum of the file. |

The query string can only have one search query parameter.

**Examples**

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

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

### HTTP status table

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

## Start Network Share scan

### /api/v1/nfs/scan

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

### Examples

GET /api/v1/nfs/scan?sname= \*\*\*network share profile name\*\*\*

```
{
 "http_code": 200,
 "message": "OK"
}
```

### Example of failed to start Network Share scan

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

## Appendix B: Sample script to submit files

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

```
#!/usr/bin/python3

Version 1.0
par Fortinet
Jan 2021

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

host = "IP"
AI_api_key = "API_KEY"

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

class FAIApiClient_file():

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

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

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

 return response
```

```

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

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

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

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

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

 tmp_str = ""

 data = b64encode(text_data)

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

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

```

```

 return response

def crawl(url,depth):

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

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

 valid = False

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

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

 else:
 parse_url (links)

 return (url_list_depth)

def load_file_for_upload(path_to_file):

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

 return gzip.compress(data)

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

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

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

 except subprocess.CalledProcessError as e:

```

```

 print(e)
 sys.exit(0)

 return (data)

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

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

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

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

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

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

 except KeyError as e:
 next

 print (results_metadata)

 else:
 print ("filename:" + str(filename) + ",NO RESULTS")

 except subprocess.CalledProcessError as e:

 sys.exit(0)

```

```

def parse_url (tmp_url):

 client = FAIApiClient_file(host)

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

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

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

 except Exception as e:
 pass

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

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

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

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

def main(argv):
 locale.getpreferredencoding = getpreferredencoding

 urllib3.disable_warnings()

```



```

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

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

args = parser.parse_args()

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

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

if (depth > 3):
 depth = 3

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

if (args.url):

 if (depth == 0):

 parse_url (args.url)

 else:

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

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

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

```

## Appendix C: FortiNDR ports

FortiNDR requires the following ports.

| Item                                 | Protocol and port number | Direction                                                                                                                                                                                                                                                              |
|--------------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| API submission, such as FortiSandbox | TCP 443                  | Inbound                                                                                                                                                                                                                                                                |
| Auto sample submit,                  | TCP 25                   | Outbound to <a href="https://fndr.fortinet.com">fndr.fortinet.com</a>                                                                                                                                                                                                  |
| CLI                                  | TCP 22                   | Inbound SSH                                                                                                                                                                                                                                                            |
| FortiGate quarantine                 | TCP 443                  | Outbound to FortiGate                                                                                                                                                                                                                                                  |
| FortiGuard update                    | TCP 443                  | Outbound to: <ul style="list-style-type: none"><li>• <a href="https://fai.fortinet.net">fai.fortinet.net</a></li><li>• <a href="https://fds1.fortinet.com">fds1.fortinet.com</a></li><li>• <a href="https://update.fortiguard.net">update.fortiguard.net</a></li></ul> |
| IOC lookup                           | TCP 443                  | Outbound to <a href="https://productapi.fortinet.com">productapi.fortinet.com</a>                                                                                                                                                                                      |
| IOT lookup                           | TCP 443                  | Outbound to <a href="https://globalguardservice.fortinet.net">globalguardservice.fortinet.net</a>                                                                                                                                                                      |
| GUI                                  | TCP 443                  | Inbound web browser                                                                                                                                                                                                                                                    |
| ICAP                                 | TCP 1344, 11344          | Inbound                                                                                                                                                                                                                                                                |
| NetFlow listen ports                 | UDP 2055,6343,9995       | Inbound                                                                                                                                                                                                                                                                |
| Network File Share                   | TCP 139, 445, 2049 (NFS) | Outbound to file server                                                                                                                                                                                                                                                |
| OFTP server                          | TCP 514                  | Inbound                                                                                                                                                                                                                                                                |
| Security Fabric with FortiGate       | TCP 443                  | Outbound to root FortiGate for Security Fabric communication                                                                                                                                                                                                           |
| Security Fabric with FortiGate       | TCP 8013                 | Outbound to root FortiGate in Security Fabric                                                                                                                                                                                                                          |
| Web Filter query                     | UDP 53                   | Outbound to <a href="https://service.fortiguard.net">service.fortiguard.net</a>                                                                                                                                                                                        |
| Microsoft Active Directory           | TCP 636,389              | Inbound and outbound                                                                                                                                                                                                                                                   |

## Appendix D: FortiGuard updates

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

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



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

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

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

### Other detection techniques:

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

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

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

## Updating the ANN database from FDS for malware detection (GUI)

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.

| FortiGuard Updates |                                                          |
|--------------------|----------------------------------------------------------|
| Manual Update      | Check update    Update FortiGuard Neural Networks Engine |
| Scheduled 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 |

## Updating ANN for malware detection (CLI)

FortiNDR utilizes both FortiGuard updates to local DB as well as lookup for detecting network anomalies. FortiNDR comes with a trained ANN, but users can update it before placing solution live on network. The ANN version can be checked at FortiGuard webpage: <https://www.fortiguard.com/services/fortindr>. For full list of updates please refer to [Appendix D: FortiGuard updates on page 191](#) 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_e5lD0v
Copying file failed!
Mounting /dev/sdcl
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e5lD0v
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 #
```

- To verify the ANN database in the GUI, go to **System > FortiGuard**. The latest version of ANN can be found on FortiGuard website: <https://www.fortiguard.com/services/fortindr>

| Entitlement                     | Status                           |                                   |
|---------------------------------|----------------------------------|-----------------------------------|
| FortiCare Support               | Registered                       |                                   |
| Firmware & General Updates      | Licenses - expires on 2023/03/10 | <button>Firmware Upgrade</button> |
| 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                        |

6. To verify the ANN database in the CLI, use the `diagnose kdb` command and check that there are four KDB Test Passed status lines.

```
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.



## Appendix E: Event severity level by category

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

# Appendix F: IPv6 support

The following topic covers IPv6 support in FortiNDR.

## IPv6 in detections:

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

VSA Verdict: **No Risk**

CLEAN

Sample Information

Submitted Date

2023/02/07 10:03:27

Last Analyzed

2023/02/07 10:03:27

File Type

UNICODE

File Size

1244(1.2 KB)

URL

http://go.microsoft.com/fwlink/?LinkID=25269&clcid=0x409

MD5

9CABECCCFEAA58E4C2A8590ED882DDC

SHA256

CA24A4F8BA44122A9E49E4E298851165732B396DA37DE0DE485DF884984857808

SHA1

751474CDA58D5270B5A7F2F8CEBE8EFCF4E255C1

Detection Name

N/A

Virus Family

N/A

Source Device

Sniffer

Device Type

Sniffer

Network

Attacker 2620:0101:9005:3235:0000:0000:0000:c121:59228 (Private port)

Victim

2600:1409:8800:0292:0000:0000:0000:2c1a:80 (HTTP)

Feature Composition

0

Detection(s)

Feature Type

Appearance In Sample

No results

History

Search

View all History

| Date                | MD5                             | File Type | Detection Name | Device Type | VDOM | Attacker                                | Victim                                  | Confidence |
|---------------------|---------------------------------|-----------|----------------|-------------|------|-----------------------------------------|-----------------------------------------|------------|
| 2023/02/07 10:03:27 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 4.246.174.31                            | ?          |
| 2023/02/07 10:03:27 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:1409:8800:0292:0000:0000:0000:2c1a | ?          |
| 2023/02/06 23:30:15 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 4.246.174.31                            | ?          |
| 2023/02/06 23:30:15 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:1409:8800:0292:0000:0000:0000:2c1a | ?          |
| 2023/02/06 20:46:21 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:1409:8800:0292:0000:0000:0000:2c1a | ?          |
| 2023/02/06 20:46:21 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 20.103.253.93                           | ?          |
| 2023/02/06 11:15:37 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:1409:8800:0292:0000:0000:0000:2c1a | ?          |
| 2023/02/06 11:15:37 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 20.103.253.93                           | ?          |

- IPv6 addresses are displayed in NDR logs.

| Anomaly             |            | Session                                                | Device                          |                     |          |                          |                                             |
|---------------------|------------|--------------------------------------------------------|---------------------------------|---------------------|----------|--------------------------|---------------------------------------------|
| View Device         |            | View Session                                           | No ML training has finished yet |                     |          |                          |                                             |
|                     |            | Source Address == fe80::7686:a2ff:fe40:1526, 🔍🔍 Search |                                 |                     |          |                          |                                             |
| Timestamp           | Session ID | Anomaly Type                                           | Source Address                  | Destination Address | Severity | Transport Layer Protocol | Info                                        |
| 2023/02/03 10:45:26 | 142834212  | Weak Cipher/Vulnerable Protocol                        | fe80::7686:a2ff:fe40:1526       | ff02::1:ffa3:b65d   | Medium   | ICMPV6                   | Weak security mode of SMB Protocol detected |

- IPv6 is shown in the session detail page.

Session 142834212

Activity

N/A

Application

N/A

Vendor

N/A

Medium Anomaly

Session Information

Timestamp

2023/02/03 10:55:24

Transport Layer Protocol

ICMPV6

Application Layer Protocol

SMB

Volume

2.02K (2021 bytes)

Interface

N/A

Cloud Service

None

Device Information

Internal

Device Type

N/A

Device Model

N/A

MAC Address

74:86:e2:40:15:26

Vendor

N/A

OS

N/A

Category

N/A

Sub Category

N/A

IP

fe80::7686:e2ff:fe40:1526

Port

58045

Packet Size

1085

Multicast

Internal

MAC Address

33:33:ff:a3:b6:5d

Vendor

N/A

OS

N/A

Category

N/A

Sub Category

N/A

IP

ff02::1:ffa3:b6:5d (Multicast IP)

Port

445

Packet Size

936

Activity

No Activity Found

ML Discovery

No ML Feature Found

Detection Information

Search

| Date                | Severity | Anomaly Type                    | Description                                 |
|---------------------|----------|---------------------------------|---------------------------------------------|
| 2023/02/03 10:45:26 | Medium   | Weak Cipher/Vulnerable Protocol | Weak security mode of SMB Protocol detected |

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

FortiNDR-VM

View Netflow

Search

| Open Time           | Flow Type  | Flow Direction | Sampler ID     | Sampling Rate | Protocol  | Source Address            | Destination Address | In Bytes | Out Bytes |
|---------------------|------------|----------------|----------------|---------------|-----------|---------------------------|---------------------|----------|-----------|
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250           | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 172.19.122.82             | 239.255.255.250     | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 172.19.122.82             | 239.255.255.250     | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 172.19.122.82             | 239.255.255.250     | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 172.19.122.82             | 239.255.255.250     | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 172.19.122.240            | 239.255.255.250     | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 172.19.122.240            | 239.255.255.250     | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 172.19.122.240            | 239.255.255.250     | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | TCP       | 172.19.235.107            | 172.19.122.201      | 176      | 176       |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | TCP       | 172.19.122.201            | 172.19.235.107      | 180      | 180       |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.56  | 0             | IPv6-ICMP | fe80::250:56fff:fe9e:7104 | ff02::1:ffcb:15b7   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.60  | 0             | IPv6-ICMP | fe80::250:56fff:fe9e:7104 | ff02::1:ffcb:15b7   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.60  | 0             | IPv6-ICMP | fe80::250:56fff:fe9e:7104 | ff02::1:ffcb:15b7   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.56  | 0             | IPv6-ICMP | fe80::250:56fff:fe9e:7104 | ff02::1:ffcb:15b7   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.56  | 0             | UDP       | fe80::3eeca7fff:febd:15b7 | ff02::1:2           | 84       | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.60  | 0             | UDP       | fe80::3eeca7fff:febd:15b7 | ff02::1:2           | 84       | 0         |

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

## Appendix G : Supported Application Protocol List

The following application protocols are supported by FortiNDR:

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

## Appendix H: File types and protocols

FortiNDR file scanning supports the following file types:

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NDR engine</b>                 | Common protocols such as TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>File-based analyses</b>        | 32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, Hangu 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 |
| <b>OT/SCADA protocols support</b> | DNP3, MODBUS, IEC104, ETHERNET_IP, S7(TSAP), MMS(TSAP), LONTALK, PROFINET, Synchrophasor, NMXSVC, HART, OPC, KNXnet_IP, CIP, CoAP, ELCom, NFP, BACNet                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



*Other* indicates the detected file type is not supported by Artificial Neural Networks (ANN).

### 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, Hangu 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.

## Appendix I: Operational Technology / SCADA vendor and application list

- 3S-Smart
- 7-Technologies
- ABB
- Advantech
- AzeoTech
- B&R
- Beckhoff
- Broadwin
- CODESYS
- CirCarLife
- CitectSCADA
- Cogent
- DATAC
- Delta
- Dut
- Eaton
- Fuji
- GE
- Gemalto
- Guardzilla
- IBM
- Iconics
- InduSoft
- Intellicom
- KeySight
- KingScada
- KingView
- Korenix
- LAquis
- Measuresoft
- Microsys
- Mitsubishi
- Moxa
- Nordex
- OMRON
- PcVue
- QNX
- RSLogix
- RealFlex

- Rockwell
- Schneider
- SE
- Siemens
- Sunway
- TeeChart
- WECON
- WellinTech
- Yokogawa



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2023 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.