TABLE OF CONTENTS

Change Log

Date	Change Description
2025-03-18	Initial release.
2025-05-07	Updated Administrators on page 150 Added Creating remote wildcard administrators on page 183
2025-08-06	Updated Device Inventory on page 39

Introduction

FortiNDR (On-premise) is Fortinet’s Network Detection and Response product, targeted for on-premises installation where no network metadata leaves the network, supporting OT and air-gapped infrastructure. FortiNDR form factor include appliances, VM/KVM and public cloud (BYOL), with distributed sensor and center support. FortiNDR can classify both network based and file based (malware) threats, provide network visibility including East West traffic in Datacenter/Cloud environment. Artificial neural networks (ANN) is equipped with the solution to classify malware into attack scenarios, surface outbreak alerts and trace source of malware infections. Network Based attacks such as intrusions, botnet, compromised IOCs, weak ciphers and vulnerable protocols can also be detected. Supervised and unsupervised machine learning (ML) continuously analyze metadata across networks to identify threats, remediation can be leveraged via Fortinet Security Fabric.

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

FortiNDR 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 seperately. 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.

Only admins with SuperAdminProfile privileges can SSH to use the CLI.For information, see Admin Profiles on page 152.

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*.

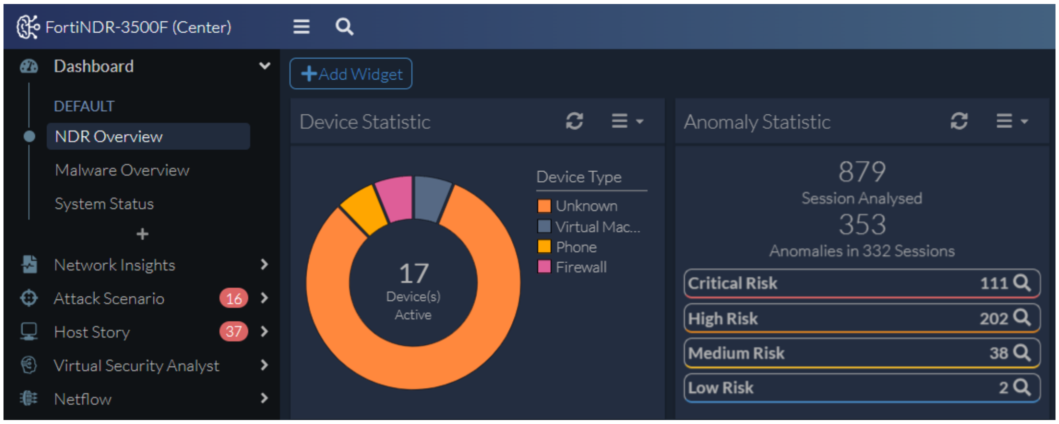
Standalone, Center and Sensor operating mode

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.
  - FortiNDR 7.4 supports Center Mode in for FNDR-3500F, VMCM (VM, KVM) and AWS.
  - Center Mode is supported in VMs. See, Licensing.
- **Sensor**: Supports Sensor configuration upon first login. A minimal amount of features and functionality are available.
  - FortiNDR 7.4.0 supports sensor mode in FNR-1000F and VM models (VM, KVM).
  - FortiNDR 7.4.1 supports sensor mode in FNR-1000F and VM models (VM, KVM, AWS).

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.

Feature	Standalone	Center	Sensor	Notes
				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 *Allow List* and *Deny List*, are employed in Center mode and associated with specific sensors. These filters provide users with the capability to formulate and modify an *Allow* or *Deny* list for targeted sensors. Please note that these Static Filters cannot be set through the Sensor's GUI.
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 *ML Discovery* dashboard widget and *ML Discovery* 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 *Netflow Dashboard* and *Netflow Log* as seen in Standalone mode. Center mode's *Netflow Dashboard* and *Netflow Log* display the data collated from the Sensors.

Feature	Standalone	Center	Sensor	Notes
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 *Admin Profile*, 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)	✓			
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 *Center's System > Sensor Settings* page using the *Restore Configuration* button.

FortiNDR Center and Licensing requirement

FortiNDR v7.4.0 and above supports running FNR-3500F as Center Mode managing up to 20 sensors. FNR-3500F has 8 hard disks by default (15TB) which can be expanded to 16 hard disks with 30TB (RAID 10). The more sensors and bandwidth you have for the deployment, the larger disk size you should prepare for center deployment.

FortiNDR center VM will be available in Q4 2023 as subscription service, with two license tiers (up to 10 sensors, or unlimited [up to 20]), please refer to FortiNDR ordering guide for reference.

Licensing

As of v7.4.0 sensors NDR, ANN, Netflow (optional) and OT/SCADA (optional) security services are all licensed separately and required for all sensors to operate and detect attacks. Users of FNR-3500F can operate in Standalone, Center mode (not Sensor). If FNR-3500F is to be run as standalone then netflow and OT security service licences maybe required.

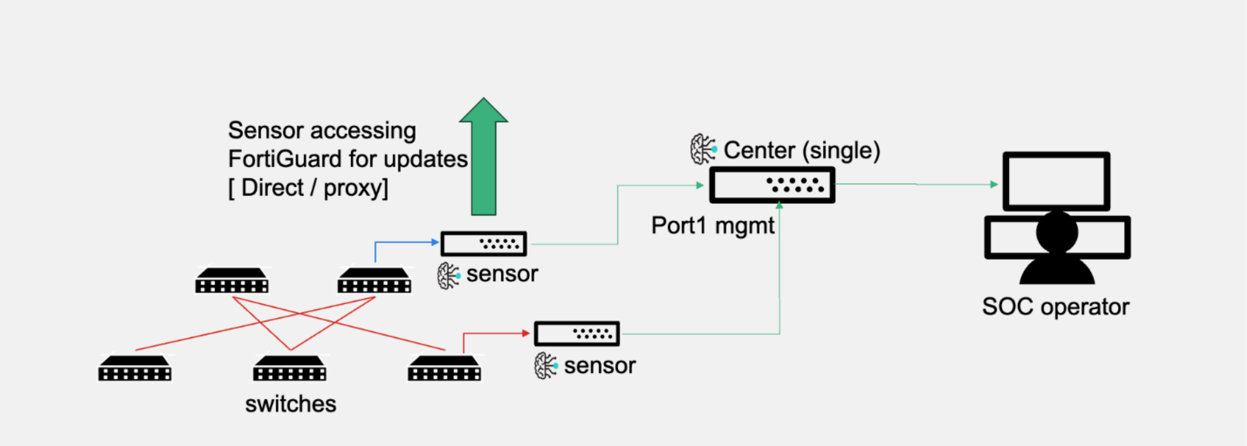
In Center Mode, the system does require a Neflow license to access the Netflow module.

You cannot load a VM Center license directly to an existing FortiNDR VM (Sensor or Standalone mode), because they have a different SKU.

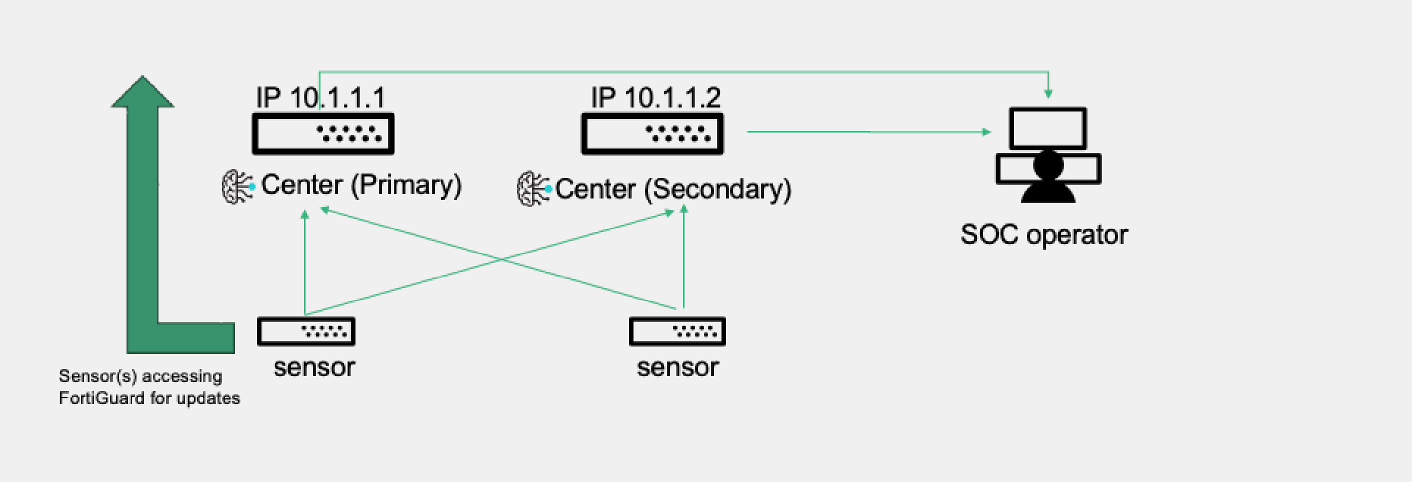
Dual Center mode support

Center mode can support both single and dual Center mode. Data redundancy can be achieved with dual center. There is no synchronization between dual centers hence there are no geographical limitations. Users can operate on either centers IP to view/filter sensors data by logging in with standard browsers.

Single NDR center support:

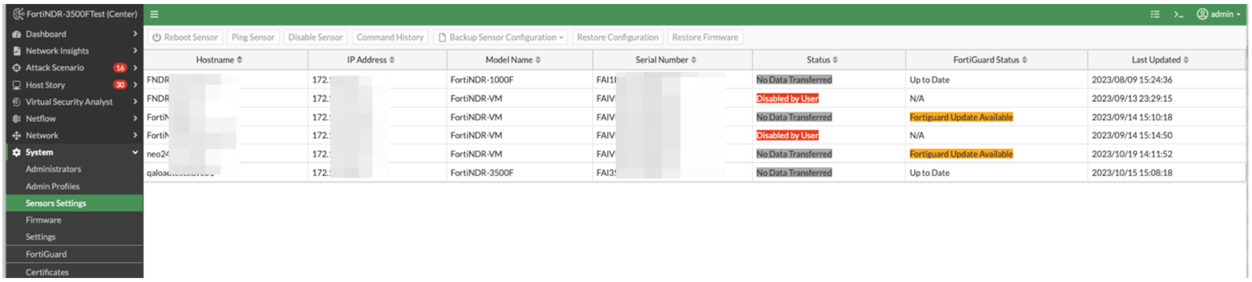


Dual NDR center support:



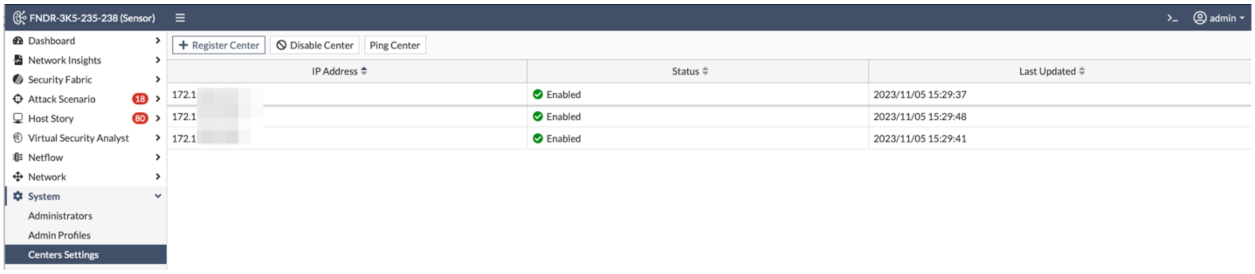
Sensors data are synchronized periodically between sensors and center using HTTPS port 443, connections are initiated by sensor to center. For a complete list of FortiNDR ports required, seeAppendix C: FortiNDR ports on page 265. If network issues occurs, sensors will resume synchronization again after network restores. Last updates can be viewed from both sensors and center, as follows:

Center's view of status and last update to center:



Hostname	IP Address	Model Name	Serial Number	Status	FortiGuard Status	Last Updated
FNDR[redacted]	172.[redacted]	FortiNDR-1000F	FAI1[redacted]	No Data Transferred	Up to Date	2023/08/09 15:24:36
FNDR[redacted]	172.[redacted]	FortiNDR-VM	FAIV[redacted]	Disabled by User	N/A	2023/09/13 23:29:15
Forti[redacted]	172.[redacted]	FortiNDR-VM	FAIV[redacted]	No Data Transferred	Fortiguard Update Available	2023/09/14 15:10:18
Forti[redacted]	172.[redacted]	FortiNDR-VM	FAIV[redacted]	Disabled by User	N/A	2023/09/14 15:14:50
neo24[redacted]	172.[redacted]	FortiNDR-VM	FAIV[redacted]	No Data Transferred	Fortiguard Update Available	2023/10/19 14:11:52
qaloa[redacted]	172.[redacted]	FortiNDR-3500F	FAI3[redacted]	No Data Transferred	Up to Date	2023/10/15 15:08:18

Sensor's view of status and last update to center:



IP Address	Status	Last Updated
172.1[redacted]	Enabled	2023/11/05 15:29:37
172.1[redacted]	Enabled	2023/11/05 15:29:48
172.1[redacted]	Enabled	2023/11/05 15:29:41

For information about sensors operations, seeSensor Settings (Center Standalone) on page 153 .

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}`"

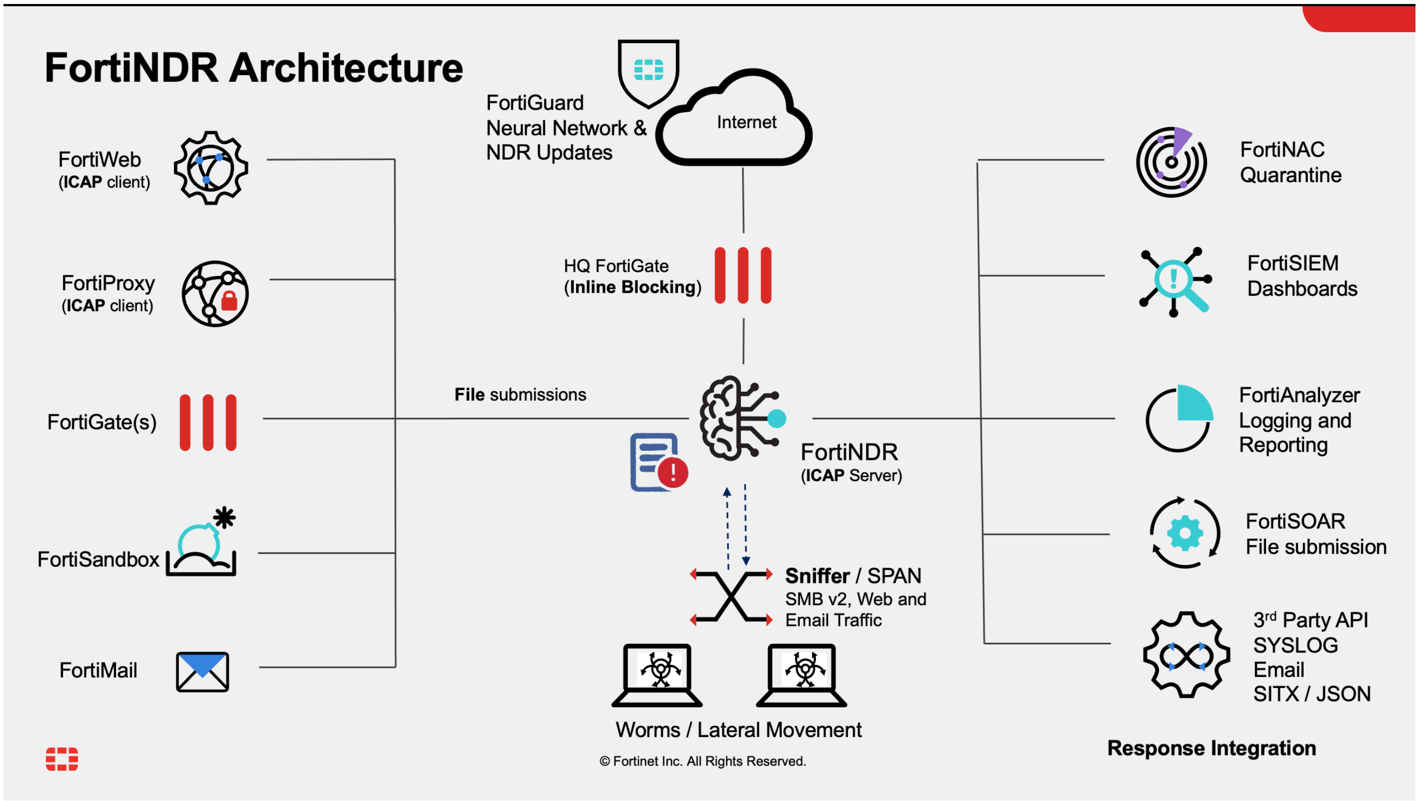
For more information, see the *FortiNDR CLI Reference Guide*.

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	FortiGate	HTTP2 (v7.0 FOS)	HTTP, HTTPS		FortiGate v7.0.1 supports

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
devices		OFTP (v5.6-6.0 FOS, legacy support)	(with SSL decryption), SMTP, POP3, IMAP,		INLINE blocking with AV profile
	FortiMail	HTTP2	SMTP		Configure under *AV profile* under FortiMail.
	FortiSandbox	HTTP2	MAPI, FTP, CIFS		
	FortiProxy	HTTP2	HTTP, HTTPS		Supports FortiProxy 7.0.0 and higher
ICAP	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 280

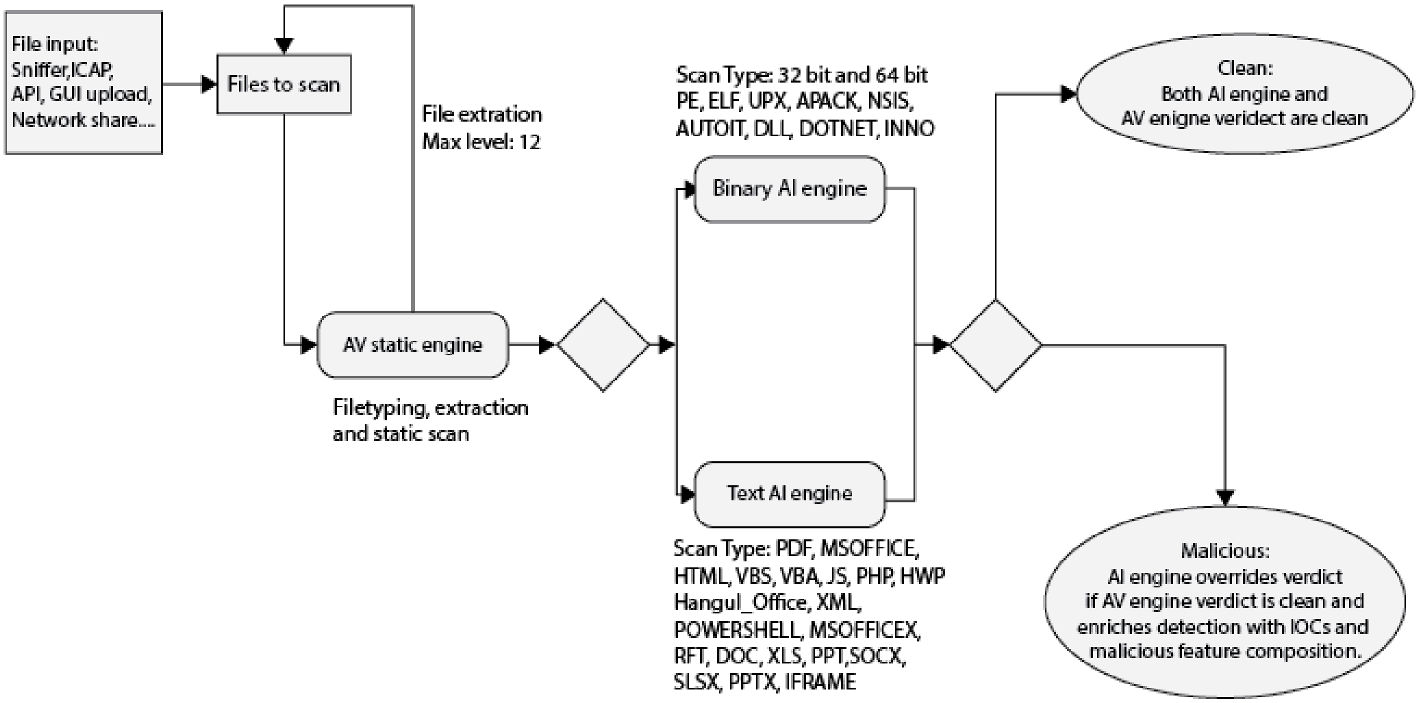
FortiNDR supports quarantine with incoming webhook from FortiOS 6.4 and higher. For details, see the Release Notes. For FortiNDR to quarantine via FortiGate, you must provide VDOM information to FortiGate. For details, see Automation Framework on page 91.



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 for estimating data storage for file analysis throughput (File scanning) and NDR deployment based on an average network.

Retention can vary depending on throughput. The following information is provided as a guide for estimation only.

Storage by model

- FNR-1000F supports 2 x 7.68TB SSD storage in RAID 1 configuration, this is not expandable.
- FNR-3500F uses 8 X 3 8TB SSD in RAID1 and comes with the option to purchase additional SSD HDDs (up to 16 SSDs max)

- 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 Standalone and Sensor comes with four different sizes of disk images.
- FortiNDR-VMCM (VM Center Management) comes with two additional different sized disk images

The following table provides guidance on disk storage requirements for FortiNDR, used for malware scanning and NDR events, based on an average 10Gbps network.

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 Standalone, Sensor, CM	1024 GB	10 days
FNDR-VM Standalone, Sensor, CM	2048 GB	20 days
FNDR-VM Standalone, Sensor, CM	4096 GB	40 days
FNDR-VM Standalone, Sensor, CM	8192 GB	73 days
FNDR-VMCM	15TB	115 days
FNDR-VMCM	30TB	264 days

While the above table documents the estimated retention days for different models (for file analysis + NDR events based on 10Gbps network tested), the following CLI controls the software retention for different tables (NDR events and file analysis table).

```
execute center-retention-setting
```

For more information, see the FortiNDR CLI Reference Guide.

The default Time To Live (TTL) for all the log tables are 264 days, meaning logs are retained for this duration. If FortiNDR reaches physical hard disk limits before software limits are hit, the NDR will

1. Stop processing files events (i.e. malware scanning will stop).
2. Stop inserting entries for NDR events.

Therefore it is practical to understand the deployment and set software limits to avoid physical hard disk being full.

For the latest performance related specs, please refer to the FortiNDR datasheet.

* 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 to FortiNDR 3500F:

1. Backup all configurations. Adding additional SSD will wipe all data.
2. Insert the extra SSDs in the available slots when the system is ON.
3. Log in to the CLI or console and run the following CLI command:
   ```
   exec raidlevel 10
   ```

After the command is executed and rebooted, the device will create the RAID including the new SSDs.

To check the new SSD capacity with the GUI:

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

To check the new SSD capacity with the CLI:

```
Get system raid-status
```

Sample output:

```
FortiNDR-3500F # get system raid-status
Controller Model Firware Driver
---------------------------------------------------
a0 PERC H350 Ada 5.190.01-3614 07.714.04.00-
+---- Unit Status Level Part Of Size (GB)
| u0 OK LEVEL 10 a0 14304
+---- Port Status Part Of Size (GB)
```

```
| 64:0 OK u0 3575
| 64:1 OK u0 3575
| 64:2 OK u0 3575
| 64:3 OK u0 3575
| 64:4 OK u0 3575
| 64:5 OK u0 3575
| 64:6 OK u0 3575
| 64:7 OK u0 3575
```

Preparing the virtual environment

Install VMware ESXi version 6.7 U2 or above on a physical server with enough resources to support FortiNDR and all other VMs deployed on that platform.

Memory is particularly important to guarantee no packet loss when it comes to sniffer operation, and also to load the ANN and operate correctly. While demo mode (and lab instances) can run with less resources. This is also a TAC support requirement. For lab instances running with less than required resources, there is a possibility that scanning operations such as sniffer will not operate correctly.

	vCPU	Reserved CPU GHz	Reserved Memory	Minimum Host‘s Disk Sequential (Read/Write)	Minimum Host's Disk 4KB Random (Read/Write)	Recommend Host‘s Disk Sequential (Read/Write)	Recommend Host's Disk 4KB Random (Read/Write)
VM16	16	32GHz	128GB	4000 MBps / 1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS
VM32	32	64GHz	256GB	4000 MBps / 1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS
VM Center mode	48	90GHz	384GB	4000 MBps /1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS

The minimum hardware footprint does not guarantee the maximum performance of the VM.

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 267.

Proxy FortiGuard support is supported via CLI only, please refer to the CLI guide.

Ports

For all FortiNDR 3500F appliances and VM, 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)	Sniffer port. For VM, only Port5 is used as sniffer port among Port5, Port6, port7 and Port8.
Console	Serial port	Console serial port. 9600 baud, 8 data bits, 1 stop bit, no parity, XON/XOFF.

The following is the initial port configuration for FNDR 1000F:

Port	Type	Function
Port1	10G fiber	Management port, GUI, Fabric devices files receiving, REST API, ICAP. Default IP address is `192.168.1.88` using `admin` with no password.
Port2	10G fiber	Reserved
Port3 Port4	10G fiber	Sniffer port.

Port	Type	Function
Port5 Port6	1G Copper	High availability. These are labeled as *HA1* and *HA2* on the device

While the FortiNDR 1000F's sniffer port3 and port4 are equipped with fiber ports, you can use the FN-TRAN-SFP+GC transceiver to convert them into copper ports.

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.

RAID encryption support (1000F and 3600G models)

To set up disk encryption on 1000F and 3600G models:

Run the following CLI command:

```
execute raidlevel <raid-level-option> [encryption <security_key>]
```

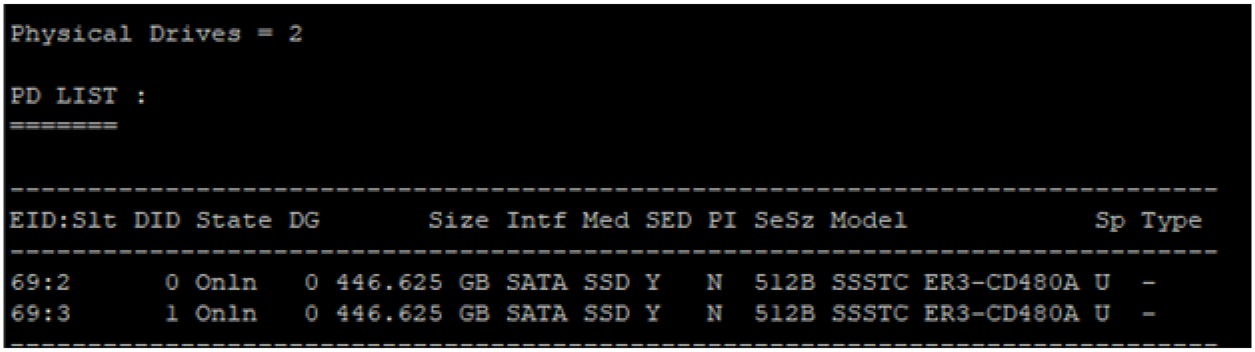
For 1000F models:

You must use the following CLI command to verify that the system supports Self-Encrypting Drives (SED):

```
diagnose system raid-status-detail
```

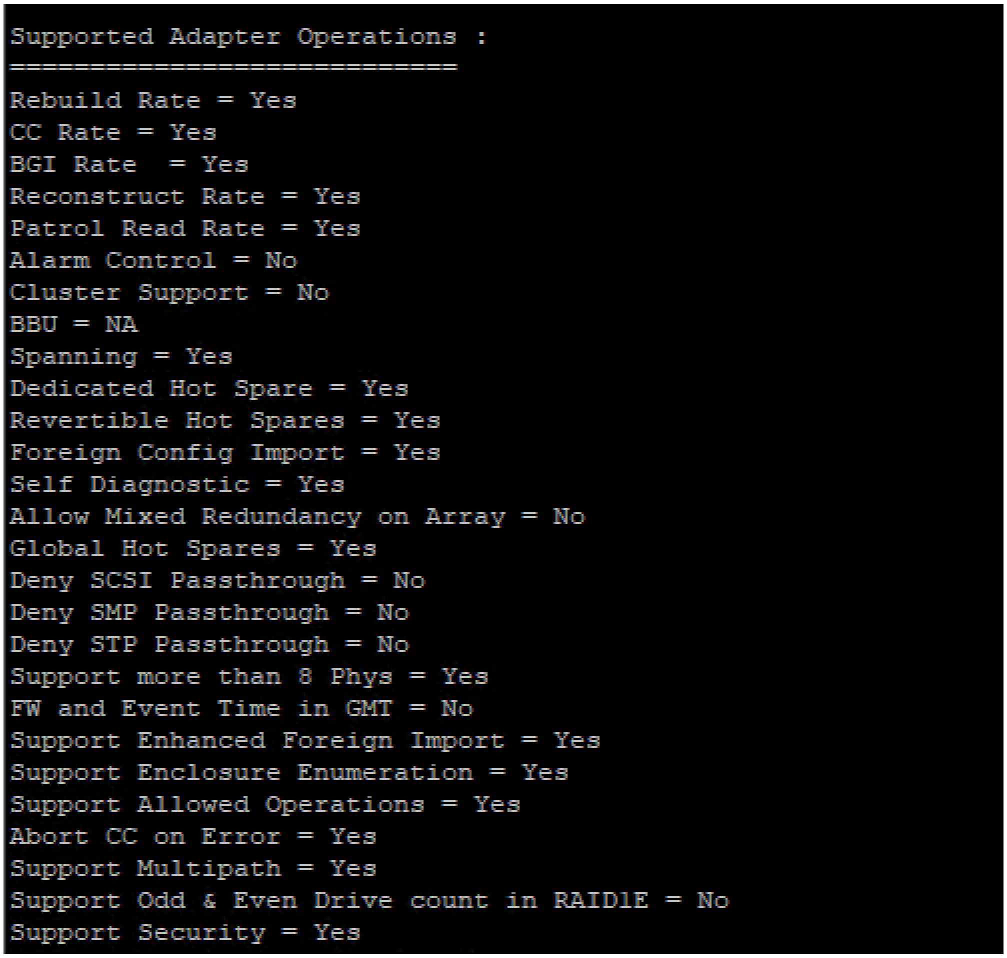
To verify both SSDs meet the requirements:

1. In the `PD LIST` table, verify the `SED` column displays `Y`.



```
Physical Drives = 2

PD LIST :
=======

-------------------------------------------------------------------------------
EID:Slt DID State DG       Size Intf Med SED PI SeSz Model            Sp Type
-------------------------------------------------------------------------------
69:2      0 Onln   0 446.625 GB SATA SSD Y   N  512B SSSTC ER3-CD480A U  -
69:3      1 Onln   0 446.625 GB SATA SSD Y   N  512B SSSTC ER3-CD480A U  -
-------------------------------------------------------------------------------
```

2. In the `Supported Adapter Operations` section, verify `Support Security = Yes` is displayed.



```
Supported Adapter Operations :
============================
Rebuild Rate = Yes
CC Rate = Yes
BGI Rate  = Yes
Reconstruct Rate = Yes
Patrol Read Rate = Yes
Alarm Control = No
Cluster Support = No
BBU = NA
Spanning = Yes
Dedicated Hot Spare = Yes
Revertible Hot Spares = Yes
Foreign Config Import = Yes
Self Diagnostic = Yes
Allow Mixed Redundancy on Array = No
Global Hot Spares = Yes
Deny SCSI Passthrough = No
Deny SMP Passthrough = No
Deny STP Passthrough = No
Support more than 8 Phys = Yes
FW and Event Time in GMT = No
Support Enhanced Foreign Import = Yes
Support Enclosure Enumeration = Yes
Support Allowed Operations = Yes
Abort CC on Error = Yes
Support Multipath = Yes
Support Odd & Even Drive count in RAID1E = No
Support Security = Yes
```

Hardening

System hardening reduces security risk by eliminating potential attack vectors and shrinking the system's attack surface.

- Register your product with Fortinet Support
- Physical security on page 30
- Vulnerability - monitoring PSIRT on page 30
- Firmware on page 30
- Encrypted protocols on page 30
- FortiGuard databases on page 31
- Penetration testing on page 31
- Password policies
- Disable Unnecessary Services
- Configuration backup
- Logging

Physical security

Install the FortiNDR in a physically secure location. Physical access to the FortiNDR can allow it to be bypassed, or other firmware could be loaded after a manual reboot.

Vulnerability - monitoring PSIRT

Product Security Incident Response Team (PSIRT) continually tests and gathers information about Fortinet hardware and software products, looking for vulnerabilities and weaknesses. The findings are sent to the Fortinet development teams, and serious issues are described, along with protective solutions, in advisories listed at https://www.fortiguard.com/psirt.

Firmware

Keep the FortiNDR firmware up to date. The latest patch release has the most fixed bugs and vulnerabilities, and should be the most stable. Firmware is periodically updated to add new features and resolve important issues.

- Read the release notes. The known issues may include issues that affect your business.
- Do not use out of support firmware. Review the Product Life Cycle > Software page and plan to upgrade before the FortiNDR End of Support (EOS) date, which is when Fortinet Support services for the firmware version expire.
- Enable *Restrict login to trusted hosts* in the *Administrator* settings to restrict admins to log in using a trusted host. For information, see Administrators on page 150.

Encrypted protocols

Use encrypted protocols whenever possible, for example:

- LDAPS instead of LDAP
- SNMPv3 instead of early SNMP versions
- SSH instead of telnet
- SCP instead of FTP or TFTP

⚠ When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials.

- To secure this connection, use LDAPS on both the Active Directory server and FortiGate. See Configuring an LDAP server and Configuring client certificate authentication on the LDAP server.
- Apply the principle of least privilege. For the LDAP regular bind operation, do not use credentials that provide full administrative access to the Windows server when using credentials. See Configuring least privileges for LDAP admin account authentication in Active Directory.

To secure RADIUS connections, consider using RADSEC over TLS instead. See Configuring a RADSEC client.

FortiGuard databases

Ensure that FortiGuard databases, such as IPS, AV, ANN and other NDR related DBs are updated punctually.

Penetration testing

Test your FortiNDR to try to gain unauthorized access, or use internal tools or third-party tools and companies to verify FortiNDR access and configuration.

Password policies

Create a secure password policy to ensure user passwords meeting the minimum number of characters, numbers, symbols and letters. For information, see config system password-policy.

Disable Unnecessary Services

To protect FortiNDR from unnecessary exposure, consider disabling the following features when not in use:

- Interface connectivity (ping/snmp/telnet etc)
- Netflow
  Run CLI: `execute netflow <on/off>`
- For pure malware scanning deployment, NDR daemon can be disabled:

  Run CLI: `execute ndrd <on|off>`
- If the deployment does not require malware scanning by AV/ANN, you can disable sniffer malware detection. Manual submission, HTTP2 and OFTP will still work as file input sources.
  Run CLI: `execute snifferd <on|off>`

- Disable ICAP server configuration if not required. This feature is disabled by default.
  See ICAP Connectors on page 85.

Configuration backup

The FortiNDR configuration file has important information that should always be kept secured, including details about your network, users, credentials, etc. There are many reasons to back up your configuration, such as disaster recovery, preparing for migrating to another device, and troubleshooting. Evaluate the risk involved if your configurations were exposed, and manage your risk accordingly. Store the configuration file in a secure location. Delete old configuration files that are no longer needed.

Logging

Logging generates system event, traffic, user login, and many other types of records that can be used for alerts, analysis, and troubleshooting. The records can be stored locally (data at rest) or remotely (data in motion). Due to the sensitivity of the log data, it is important to encrypt data in motion through the logging transmission channel. When logging to third party devices, make sure that the channel is secure. If it is not secure, it is recommended that you form a VPN to the remote logging device before transmitting logs to it.

Logging options include FortiAnalyzer, Syslog, and a local disk. Logging with Syslog only stores the log messages. Logging to FortiAnalyzer stores the logs and provides log analysis. If a Security Fabric is established, you can create rules to trigger actions based on the logs. For example, sending an email if the FortiNDR configuration is changed, or running a CLI script if a host is compromised.

FortiSIEM (Security Information and Event Management) and FortiSOAR (Security Orchestration, Automation, and Response) both aggregate security data from various sources into alerts and supports logging from FortiNDR.

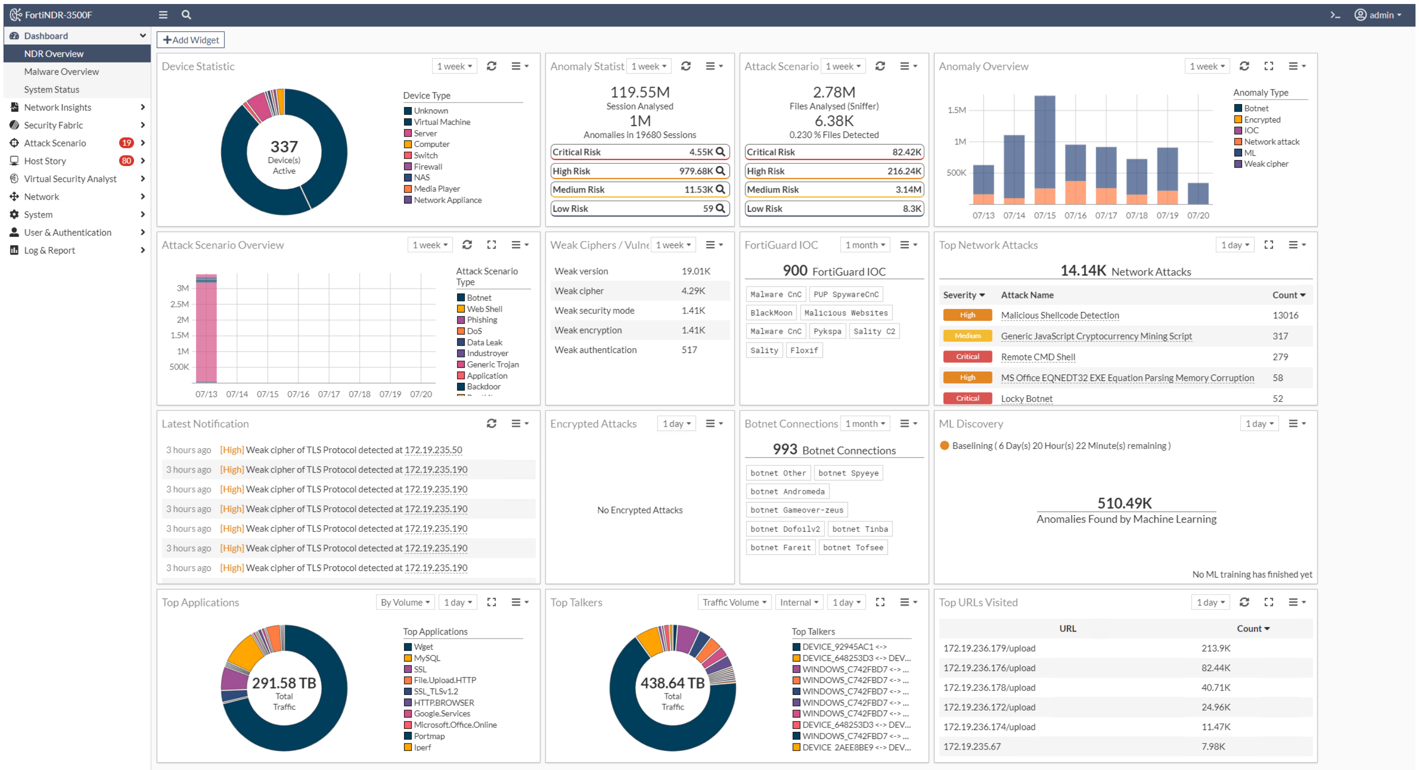
Dashboard

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.



Anomaly Statistics: 119.55M Session Analysed; 1M Anomalies in 19680 Sessions

Critical Risk	4.55K
High Risk	979.68K
Medium Risk	11.53K
Low Risk	59

Attack Scenario: 2.78M Files Analysed (Sniffer); 6.38K 0.230 % Files Detected

Critical Risk	82.42K
High Risk	216.24K
Medium Risk	3.14M
Low Risk	8.3K

Weak Ciphers / Vulne

Weak version	19.01K
Weak cipher	4.29K
Weak security mode	1.41K
Weak encryption	1.41K
Weak authentication	517

900 FortiGuard IOC

Malware CnC, PUP SpywareCnC, BlackMoon, Malicious Websites, Malware CnC, Pykspa, Sality C2, Sality, Floxif

14.14K Network Attacks

Severity	Attack Name	Count
High	Malicious Shellcode Detection	13016
Medium	Generic JavaScript Cryptocurrency Mining Script	317
Critical	Remote CMD Shell	279
High	MS Office EQNEDT32 EXE Equation Parsing Memory Corruption	58
Critical	Locky Botnet	52

Latest Notification

3 hours ago [High] Weak cipher of TLS Protocol detected at 172.19.235.50
3 hours ago [High] Weak cipher of TLS Protocol detected at 172.19.235.190
3 hours ago [High] Weak cipher of TLS Protocol detected at 172.19.235.190
3 hours ago [High] Weak cipher of TLS Protocol detected at 172.19.235.190
3 hours ago [High] Weak cipher of TLS Protocol detected at 172.19.235.190
3 hours ago [High] Weak cipher of TLS Protocol detected at 172.19.235.190
3 hours ago [High] Weak cipher of TLS Protocol detected at 172.19.235.190

No Encrypted Attacks

993 Botnet Connections

botnet Other, botnet Spyeye, botnet Andromeda, botnet Gameover-zeus, botnet Dofoilv2, botnet Tinba, botnet Fareit, botnet Tofsee

ML Discovery: Baselining (6 Day(s) 20 Hour(s) 22 Minute(s) remaining)

510.49K Anomalies Found by Machine Learning

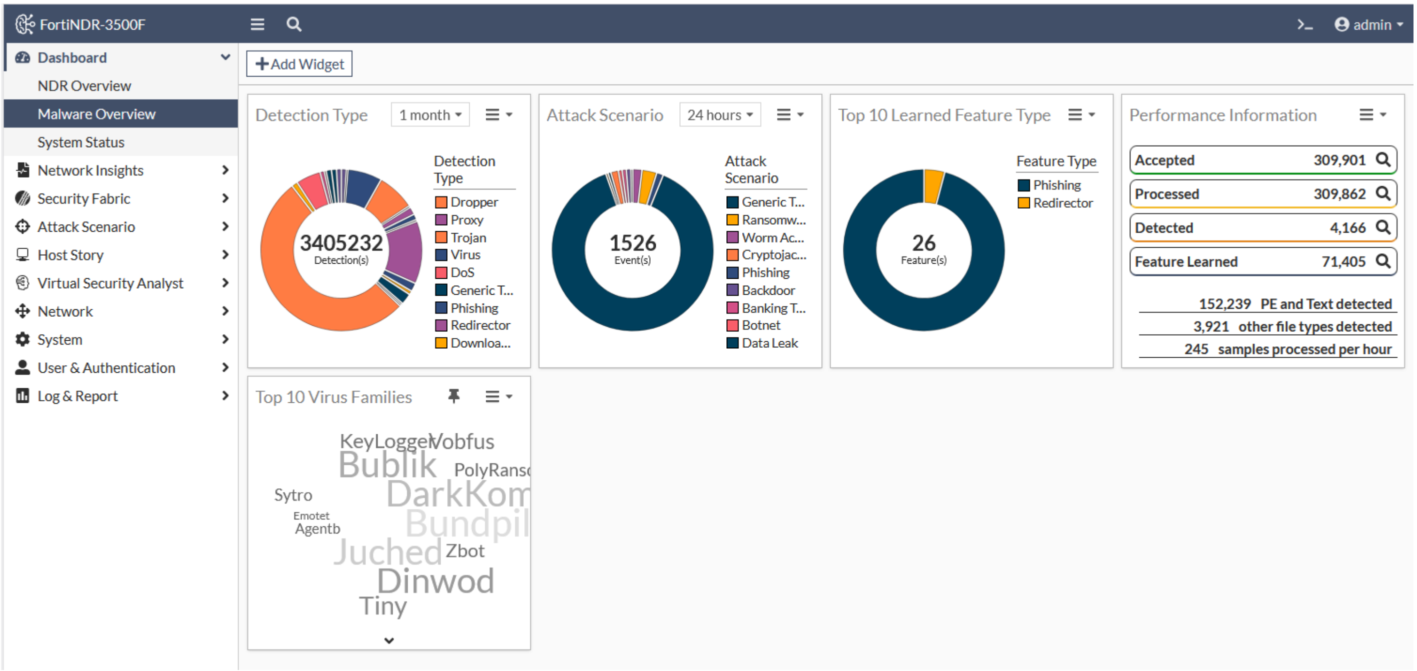
No ML training has finished yet

URL	Count
172.19.236.179/upload	213.9K
172.19.236.176/upload	82.44K
172.19.236.178/upload	40.71K
172.19.236.172/upload	24.96K
172.19.236.174/upload	11.47K
172.19.235.67	7.98K

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.



Accepted 309,901

Processed 309,862

Detected 4,166

Feature Learned 71,405

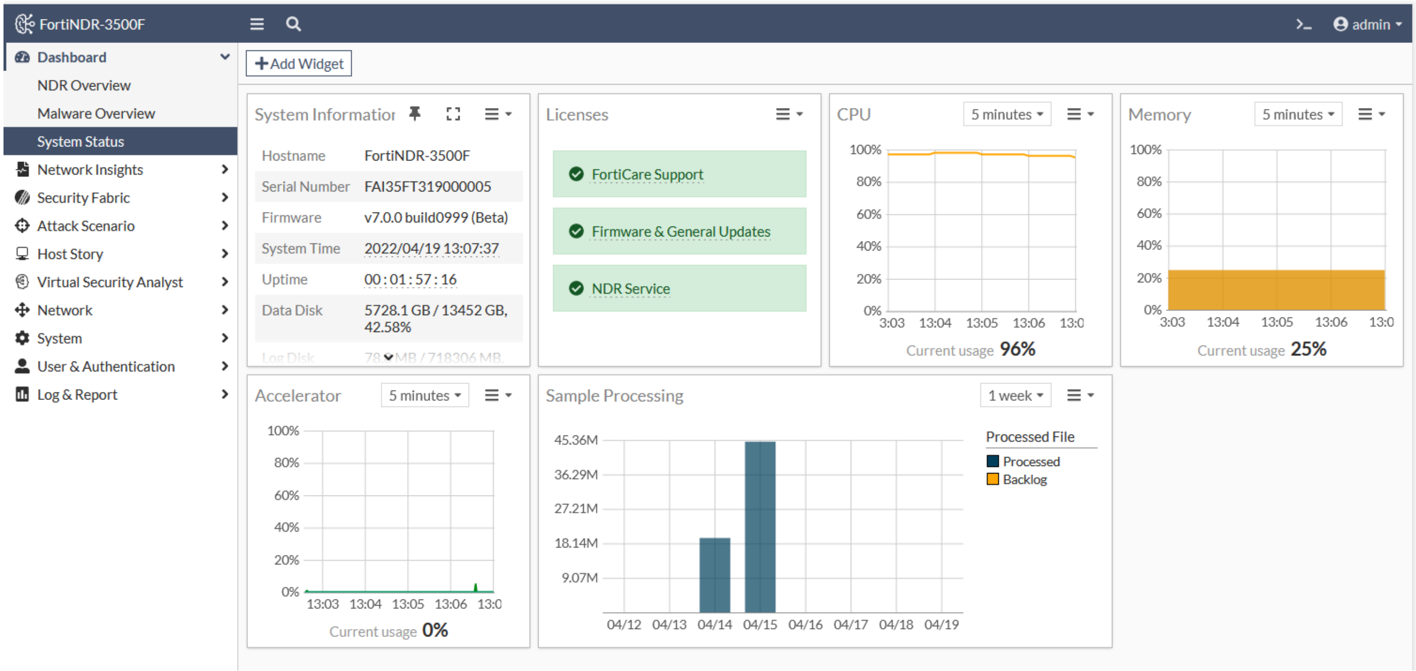
152,239 PE and Text detected

3,921 other file types detected

245 samples processed per hour

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.



Hostname FortiNDR-3500F
Serial Number FAI35FT319000005
Firmware v7.0.0 build0999 (Beta)
System Time 2022/04/19 13:07:37
Uptime 00:01:57:16
Data Disk 5728.1 GB / 13452 GB, 42.58%
Log Disk 78 MB / 718306 MB

CPU: Current usage 96%

Memory: Current usage 25%

Accelerator: Current usage 0%

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*.

The maximum number of widgets for each type of dashboard is as follows:

NDR dashboard: 60 widgets

- Malware: 20 widgets
- System: 30 widgets
- Netflow: 30 widgets
- Custom: 30 widgets

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*.

You can create up to four custom dashboards.

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.

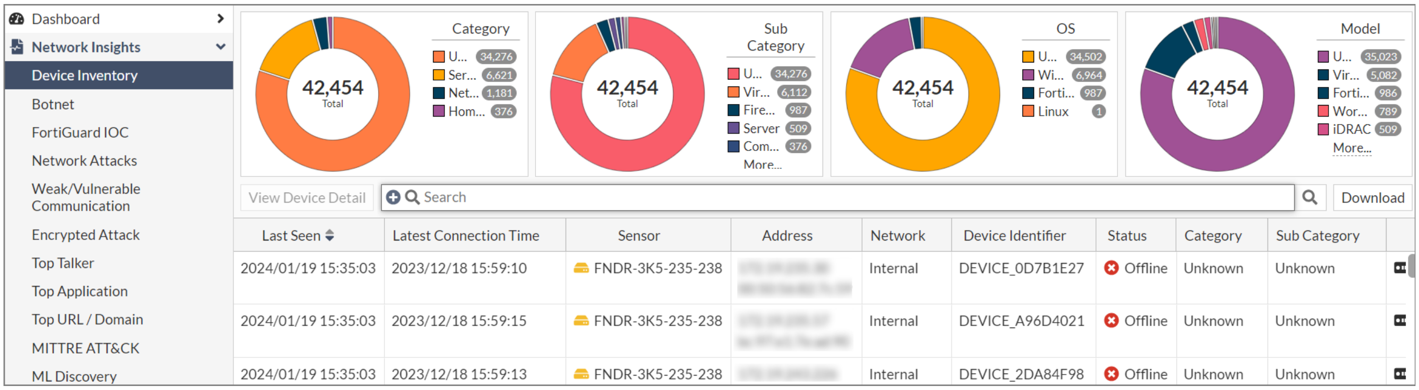
Remember to use the widget settings to include sensors, so their data is displayed in the widgets.

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.



Last Seen	Latest Connection Time	Sensor	Address	Network	Device Identifier	Status	Category	Sub Category
2024/01/19 15:35:03	2023/12/18 15:59:10	FNDR-3K5-235-238	[redacted]	Internal	DEVICE_0D7B1E27	Offline	Unknown	Unknown
2024/01/19 15:35:03	2023/12/18 15:59:15	FNDR-3K5-235-238	[redacted]	Internal	DEVICE_A96D4021	Offline	Unknown	Unknown
2024/01/19 15:35:03	2023/12/18 15:59:13	FNDR-3K5-235-238	[redacted]	Internal	DEVICE_2DA84F98	Offline	Unknown	Unknown

The *Network Insights* monitors display the following information:

Monitor	Description
Device Inventory	Displays the discovered devices. The priority of devices is from highest to lowest: 1. User defined (for example, finance server). 2. AD Device enrichment (hostname from AD, if configured). 3. System generated (OS_hash of the mac address). The device name in the *Device* column is determined by the *OS_hash* of the mac address Status (online/offline). If FortiNDR does not see a session from a device within 60 seconds, the status will be *Offline*.
Botnet	Displays the botnet traffic detections. If there is a known Botnet name, it will be displayed.
FortiGuard IOC	Displays 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 information column for any campaign name involved (e.g. Solarwind, Locky Ransomware).
Network Attacks	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.
Weak/Vulnerable Communication	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 weak or compromised network security (for example, a weak cipher used by an older version of SSL).
Encrypted Attack	Displays encrypted attacks that 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.

Monitor	Description
ML Discovery	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.

Anomaly, Connection and Session tabs

The *Botnet*, *FortiGuard IOC*, *Network Attacks*, *Weak/Vulnerable Communication*, *Encrypted Attack* and *ML Discovery* monitors contain the *Anomaly*, *Connection* and *Session* tabs. These tabs display the following information:

Anomaly	The records in the *Anomaly* tab are grouped by anomaly types and sensor. Each record may contain different IP pairs. If you display the *Destination IP* and *Source IP* columns, you will see the most recent Destination and Source IPs. Double-click a record to open the *Anomaly Information* pane which contains all the connection pairs. Connections are grouped by destination-source IP pairs. *Example*: Network Attacks Insights • Sensor 1: TCP port scan (contain multiple src/dst IP pairs) • Sensor 1: DNS amplification attack For more information, see Anomaly tab on page 65 .
Connection	Shows attacks grouped by Source and Destination IP pairs, and sensor. *Example*: Botnet Network Insights • Sensor 1: Src 1.1.1.1 dst 2.2.2.2 count For more information, see Connection tab on page 67.
Session	Shows granular session information for each attack including the Source and Destination IPs. For more information, see Session tab on page 70.

Common fields

The following fields are shared by all of the *Network Insights* dashboards:

Column	Description
Latest Timestamp	The date the record was updated.
URL Category	The URL category such as *Newly Observed Domain* or *Malicious Website*.
IOC	The Indications of Compromise.
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Category	The device category (*Unknown*, *Home & Office*, *Mobile* and *Network*).

Column	Description
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week.
First Timestamp	The timestamp for the first time the anomaly was detected.
Destination IP	The destination IP.
Source IP	The source IP.
Data Source	The *Interface*, *Link* and *Role* (if available).
Destination Category	The destination category *Unknown*, *Home & Office*, *Mobile* and *Network*).
Destination Model	The model number of the destination device (if available).
Destination Network	The destination network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Destination OS	The operating system of the destination device.
Destination Port	The destination port.
Destination Sub Category	The destination sub category (*Unknown*, *IP Phone*, *Computer*, *Phone*, or *Firewall*)
Destination Vendor	The destination vendor, such as *VMware*, *Dell Inc* or *Hewlett Packard*.
Session ID	The session ID.
Source Category	The source category (*Unknown*, *Home & Office*, *Mobile* and *Network*).
Source Model	The source model.
Source Network	The source network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Source OS	The source operating system.
Source Port	The source port.
Source Sub Category	The source sub category (*Unknown*, *IP Phone*, *Computer*, *Phone*, or *Firewall*)
Source Vendor	The source vendor, such as *VMware*, *Dell Inc* or *Hewlett Packard*.

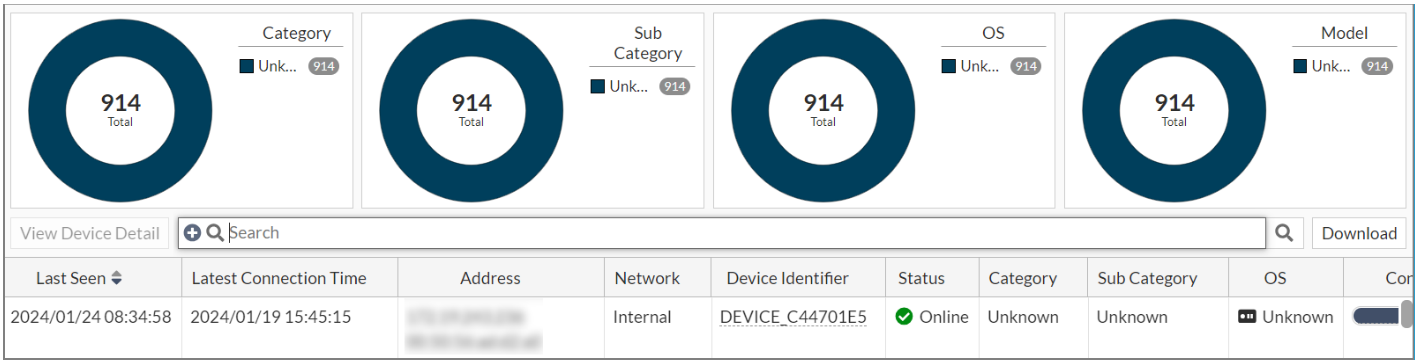
Device Inventory

The *Network Insights* > *Device Inventory* page displays the discovered devices.

The priority of device inventory identifier is organized by the following priority from highest to lowest:

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

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



Last Seen	Latest Connection Time	Address	Network	Device Identifier	Status	Category	Sub Category	OS	Cor
2024/01/24 08:34:58	2024/01/19 15:45:15	[redacted]	Internal	DEVICE_C44701E5	✓ Online	Unknown	Unknown	Unknown	

The *Device Inventory* monitor displays the following information:

Column	Description
Last Seen	The date and time the device was last seen.
Latest Connection Time	The date and time of latest connection.
Address	The device IP address
Device Identifier	The device identifier.
Status	The connection status (*Online* of *Offline*). If FortiNDR does not see a session from a device within 60 seconds, the status will be *Offline*.
Category	The device category (*Unknown*, *Home & Office*, *Mobile* and *Network*).
Sub Category	The device sub category (*Unknown*, *IP Phone*, *Computer*, *Phone*, or *Firewall*)
OS	The device operating system.
Confidence	The confidence level.
Country	The device country if known.
Device ID	The device ID.
Latest Device Enrichment	The timestamp for the latest device enrichment. SeeDevice Enrichment on page 139
Model	The device model.
Vendor	The device vendor.

To download the Device Inventory:

- Click the *Download* button next to the *Search* field. A pop-up window with download status opens.

To view Device Information:

- Double-click a record in the table to open the *Device Information* pane. The following information is displayed:

General	• Device ID • Device Name • Status • Discovery Time • Last Seen
Hardware	• Model • Operating System • Category • Sub Category • Vendor • Confidence
Network	• Most Recent IP • Internal/External • Mac Address • Country

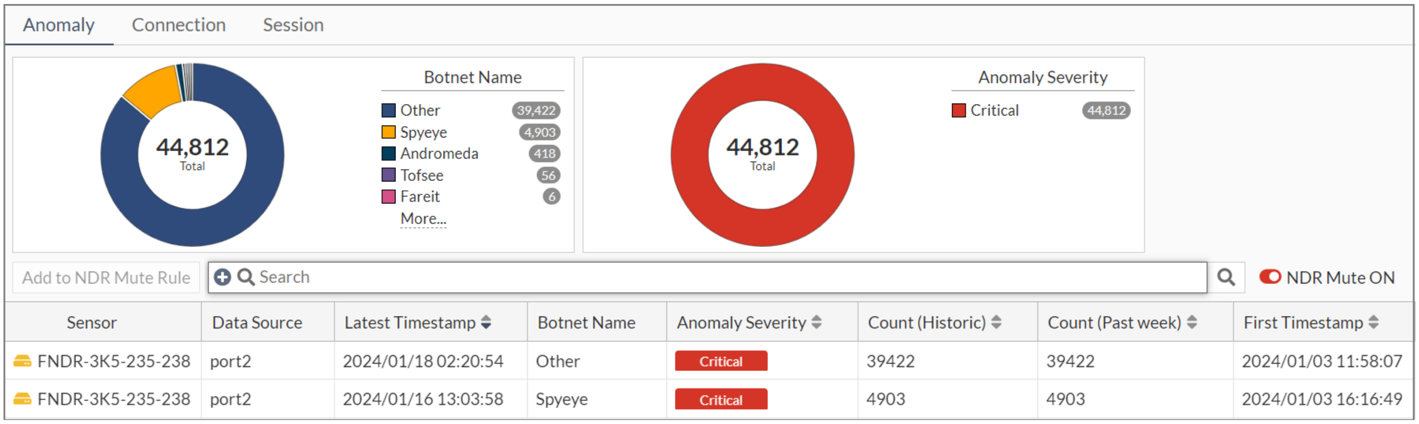
Device details

Select a record in the table and click *View Device Detail* next to the *Search* field. The *Device Details* pate is organized into two tabs:

Information	Displays information about the device and anomalies. You can use this tab to update the device identifier, set the time range, and view related sessions and anomalies.
Malware Host Story	Displays information about the malware such as the *Risk Level*, *Scenario Type* and *Malware Family*.

Botnet

The *Network Insights* > *Botnet* monitor displays the botnet traffic detections. If there is a known Botnet name, it will be displayed.



Botnet Name	
🟦 Other	39,422
🟨 Spyeye	4,903
🟦 Andromeda	418
🟪 Tofsee	56
🟪 Fareit	6
More...	

Anomaly Severity	
🟥 Critical	44,812

Sensor	Data Source	Latest Timestamp	Botnet Name	Anomaly Severity	Count (Historic)	Count (Past week)	First Timestamp
FNDR-3K5-235-238	port2	2024/01/18 02:20:54	Other	Critical	39422	39422	2024/01/03 11:58:07
FNDR-3K5-235-238	port2	2024/01/16 13:03:58	Spyeye	Critical	4903	4903	2024/01/03 16:16:49

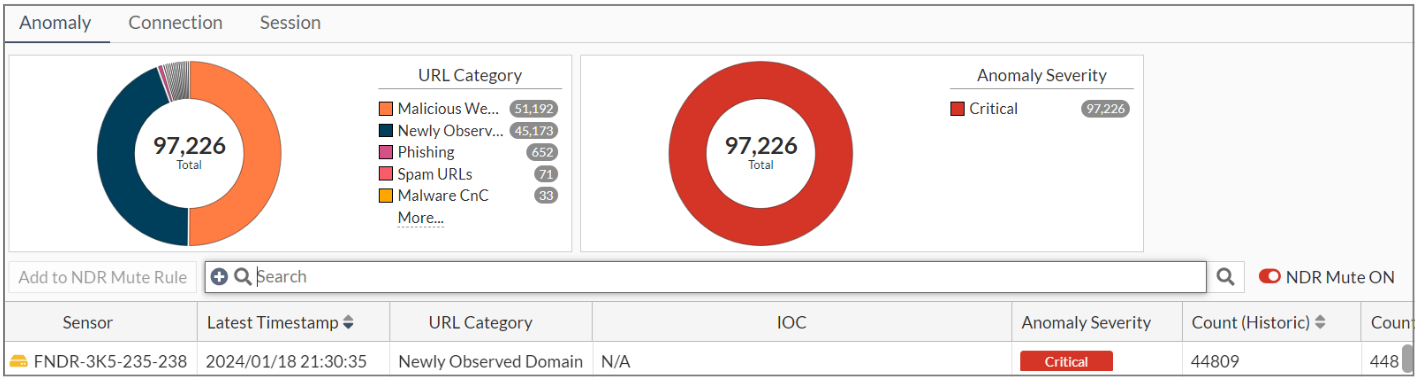
The *Botnet* monitor displays the following information:

Column	Description
Latest Timestamp	The date the record was updated.
Botnet Name	The botnet name.
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Timestamp	The date record was created.

For information about muting rules, see NDR Muting on page 127.

FortiGuard IOC

Network Insights > *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).



Sensor	Latest Timestamp	URL Category	IOC	Anomaly Severity	Count (Historic)	Coun
FNDR-3K5-235-238	2024/01/18 21:30:35	Newly Observed Domain	N/A	Critical	44809	448

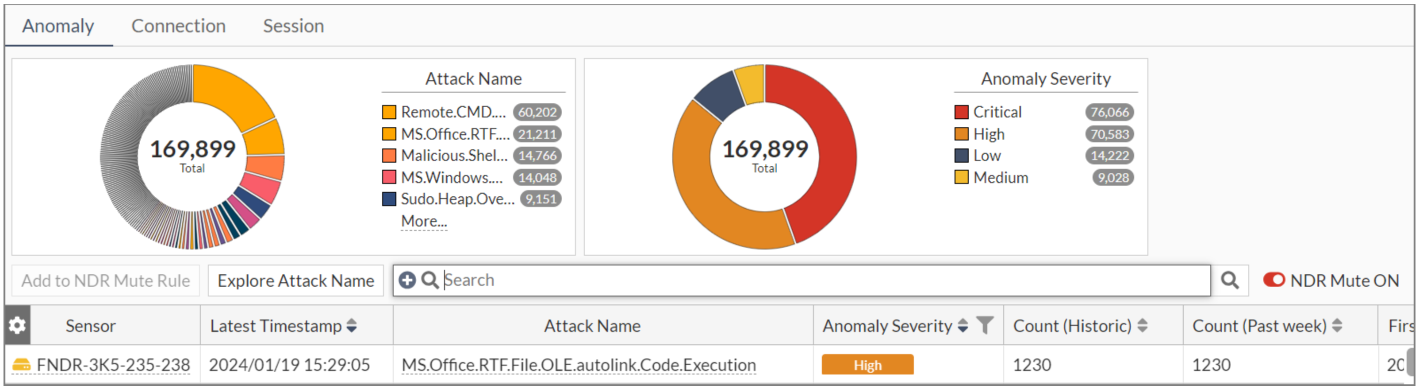
The *FortiGuard IOC* monitor displays the following information:

Column	Description
URL Category	The UR Category.
IOC	The Indications of Compromise service.
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Timestamp	The timestamp for the first time the anomaly was detected.

For information about muting rules, see NDR Muting on page 127.

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.



Sensor	Latest Timestamp	Attack Name	Anomaly Severity	Count (Historic)	Count (Past week)	Firs
FNDR-3K5-235-238	2024/01/19 15:29:05	MS.Office.RTF.File.OLE.autolink.Code.Execution	High	1230	1230	20

The *Network Attacks* monitor displays the following information:

Column	Description
Sensor (Center mode)	The network sensor. Hover over the sensors ID to view the *IP Address*, Serial number (*S/N*), *Last Sync Time* and *Status*.
URL Category	The URL Category
Attack Name	The attack name provided by FortiGuard. Hover over the name to view the *Impact*, *Product List* and *Recommended Action*. You can also use this column to explore the attack name and search FortiGuard.
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Timestamp	The timestamp for the first time the anomaly was detected.
Source Vendor	The source vendor, such as *VMware*, *Dell Inc* or *Hewlett Packard*.

To view the attack information:

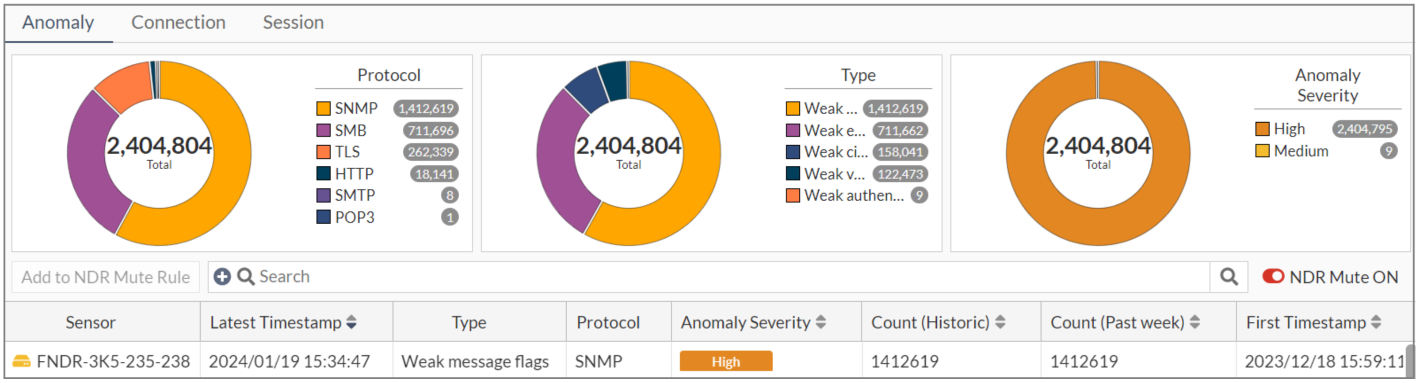
- Click *Explore Attack Name*. The *Attack Name Information* pane displays the following information:

Attack Name	The attack name.
Description	A description of the attack.
Impact	The impact of the attack on your network.
Product List	The affected products.
CVE List	The Common Vulnerabilities and Exposures list.
Mitre Attack Technique	The Mitre Attack Technique . Click the question mark (*?*) to view the details about the technique.
Recommended Action	The recommended actions to mitigate the attack.

For information about muting rules, see NDR Muting on page 127.

Weak/Vulnerable Communication

The *Weak/Vulnerable Communication* monitor displays the list of weak or vulnerable communications detected on sniffer port(s) on NDR interfaces. Detection of weak and vulnerable communications in the network can be signs of weak or compromised network security that administrators should pay attention to.



Sensor	Latest Timestamp	Type	Protocol	Anomaly Severity	Count (Historic)	Count (Past week)	First Timestamp
FNDR-3K5-235-238	2024/01/19 15:34:47	Weak message flags	SNMP	High	1412619	1412619	2023/12/18 15:59:11

The *Weak/Vulnerable Communication* displays the following information:

<table>
<tr><td><b>Sensor (Center mode)</b></td><td>The network sensor. Hover over the sensors ID to view the <i>IP Address</i>, Serial number (<i>S/N</i>), <i>Last Sync Time</i> and <i>Status</i>.</td></tr>
<tr><td><b>Latest Timestamp</b></td><td>The date record was updated.</td></tr>
<tr><td><b>Type</b></td><td>
<table>
<tr><th>Communication type</th><th>Description</th></tr>
<tr><td><b>Weak record version</b></td><td>Weak TLS record layer version.</td></tr>
<tr><td><b>Weak version</b></td><td>Weak TLS handshake version.</td></tr>
<tr><td><b>Weak support version</b></td><td>Weak TLS handshake extension supported version.</td></tr>
<tr><td><b>Weak cipher</b></td><td>Weak TLS handshake cipher suite.</td></tr>
<tr><td><b>Weak security mode</b></td><td>SMB protocol uses level security mode.</td></tr>
<tr><td><b>Weak extended security</b></td><td>SMB protocol uses outdated extended security negotiation option.</td></tr>
<tr><td><b>Weak dialect</b></td><td>SMB uses outdated dialect version.</td></tr>
<tr><td><b>Weak encryption</b></td><td>SMB or SSH uses risky encryption algorithm. For example, SMB protocol with encryption disabled.</td></tr>
<tr><td><b>Weak authentication</b></td><td>Email protocols are using risky authentication methods. For example, POP3 uses authentication cram-md5, Postgres uses MD5 password as authentication type.</td></tr>
<tr><td><b>Weak server</b></td><td>HTTP or RTSP server version is outdated.</td></tr>
<tr><td><b>Weak method</b></td><td>HTTP, SIP or RTSP protocol uses weak request method. For example, HTTP protocol uses DELETE as request method.</td></tr>
<tr><td><b>Weak banner</b></td><td>Weak or outdated email server version. For example, Outdated Cyrus IMAP server</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th>Communication type</th><th>Description</th></tr>
<tr><td><b>Weak encrypt algo server client</b></td><td>Weak encryption option is used in SSH, such as rc4, rc3, rc2.</td></tr>
<tr><td><b>Weak capability</b></td><td>IMAP or POP3 capability command uses option AUTH=PLAIN.</td></tr>
<tr><td><b>Weak security</b></td><td>SMB protocol uses low level security mode.</td></tr>
<tr><td><b>Weak encrypt method</b></td><td>RDP protocol uses low level encryption methods such as ENCRYPTION_METHOD_40BIT.</td></tr>
<tr><td><b>Weak encrypt level</b></td><td>RDP protocol uses low encryption level such as ENCRYPTION_LEVEL_NONE</td></tr>
<tr><td><b>Weak msg flags</b></td><td>SNMP protocol uses risky flags such as 0x00-02, 0x04-06 and 0x08-ff.</td></tr>
<tr><td><b>Weak server version</b></td><td>MYSQL, TDS, Posgres or SIP server version is outdated.</td></tr>
<tr><td><b>Weak auth algo</b></td><td>POP3, SMTP or IMAP authentication method option is too risky. For example, POP3 uses PLAIN authentication option.</td></tr>
<tr><td><b>Weak protocol version</b></td><td>MYSQL protocol version outdated.</td></tr>
<tr><td><b>Weak encrypt</b></td><td>TDS encryption option is disabled.</td></tr>
<tr><td><b>Weak fedauth</b></td><td>TDS protocol disables <code>FedAuthRequired</code> option.</td></tr>
</table>
</td></tr>
<tr><td><b>Protocol</b></td><td>The communication protocol.</td></tr>
<tr><td><b>Anomaly Severity</b></td><td>The anomaly severity (<i>Not Anomaly</i>, <i>Info</i>, <i>Low</i>, <i>Medium</i>, <i>High</i> or <i>Critical</i>).</td></tr>
<tr><td><b>Count (Historic)</b></td><td>The total number of times the anomaly was observed.</td></tr>
<tr><td><b>Count (Past week)</b></td><td>The total number of times the anomaly was observed during the past week .</td></tr>
<tr><td><b>First Timestamp</b></td><td>The date the record was created.</td></tr>
</table>

Anomaly information

Double-click an anomaly in the table to open the *Anomaly Information* pane. The *Anomaly Information* pane contains two tabs: *General* and *Analytic*.

General tab

The *General* tab displays the following information:

General	• Anomaly Type • Severity • Reason
Additional Information	• HTTP Version • HTTP Response Code • HTTP Server Name • HTTP URL • Malicious Behavior
Last Anomaly Occurrence	• Latest Occurrence • Count(Past Week) • Count(Historic) • Latest Source IP • Latest Source Port • Latest Source MAC • Latest Source Packet Size • Latest Source Country • Latest Source Device Model • Latest Source OS • Latest Source Device Category • Latest Source Device Sub Category • Latest Destination IP • Latest Destination Port • Latest Destination MAC • Latest Destination Packet Size • Latest Destination Country • Latest Destination Device Model • Latest Destination OS • Latest Destination Device Category • Latest Destination Device Sub Category

Analytic tab

The *Analytic* tab displays the following information about he the connection pair:

Src IP	The source IP. Hover over the record to view the view the *IP Address*, *Country* and *Related Service*.
Source Network	The source network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Dst Ip	The destination IP. Hover over the record to view the view the *IP Address*, *Country* and *Related Service*.

Destination Network	The destination network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .

To view the source and destination devices:

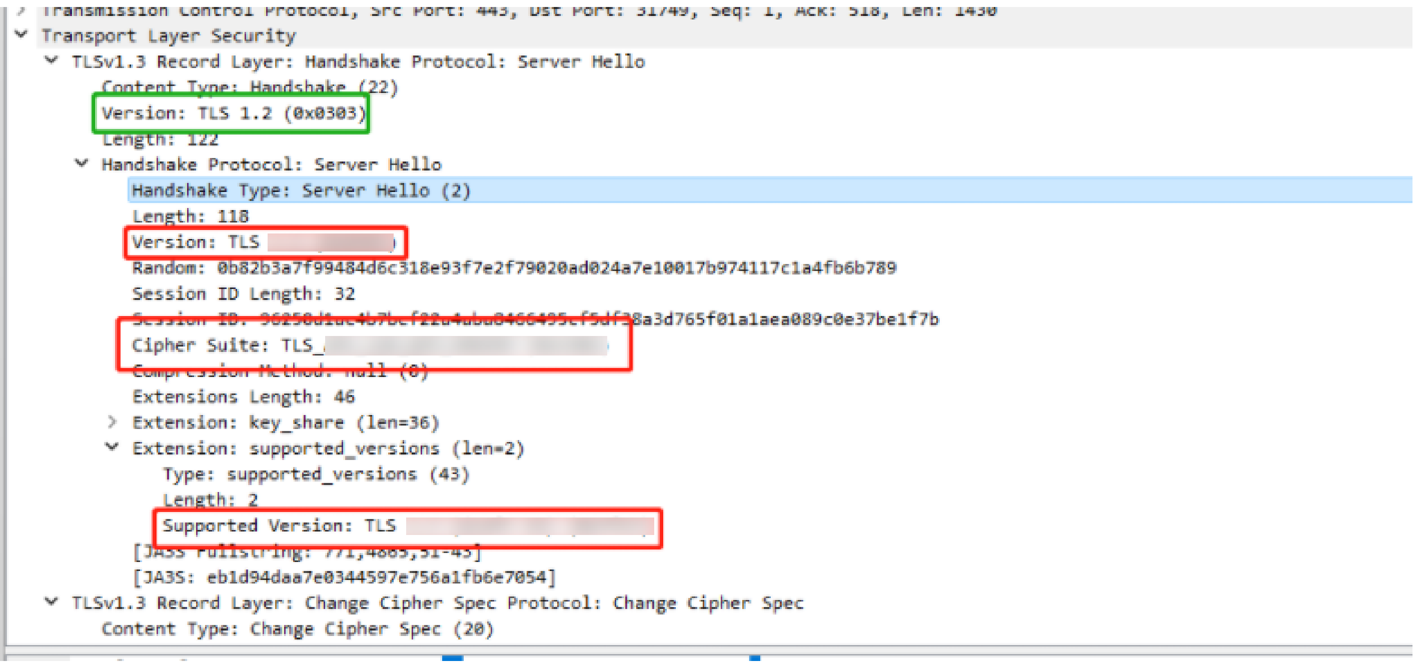
- Select a record in the table and click *View Device* > *View Source Device*, or *View Destination Device*.

To view the session logs for a condition:

- Double-click a record in the *Anomaly Information* pane. The *Sessions Log for selected condition* pane opens.

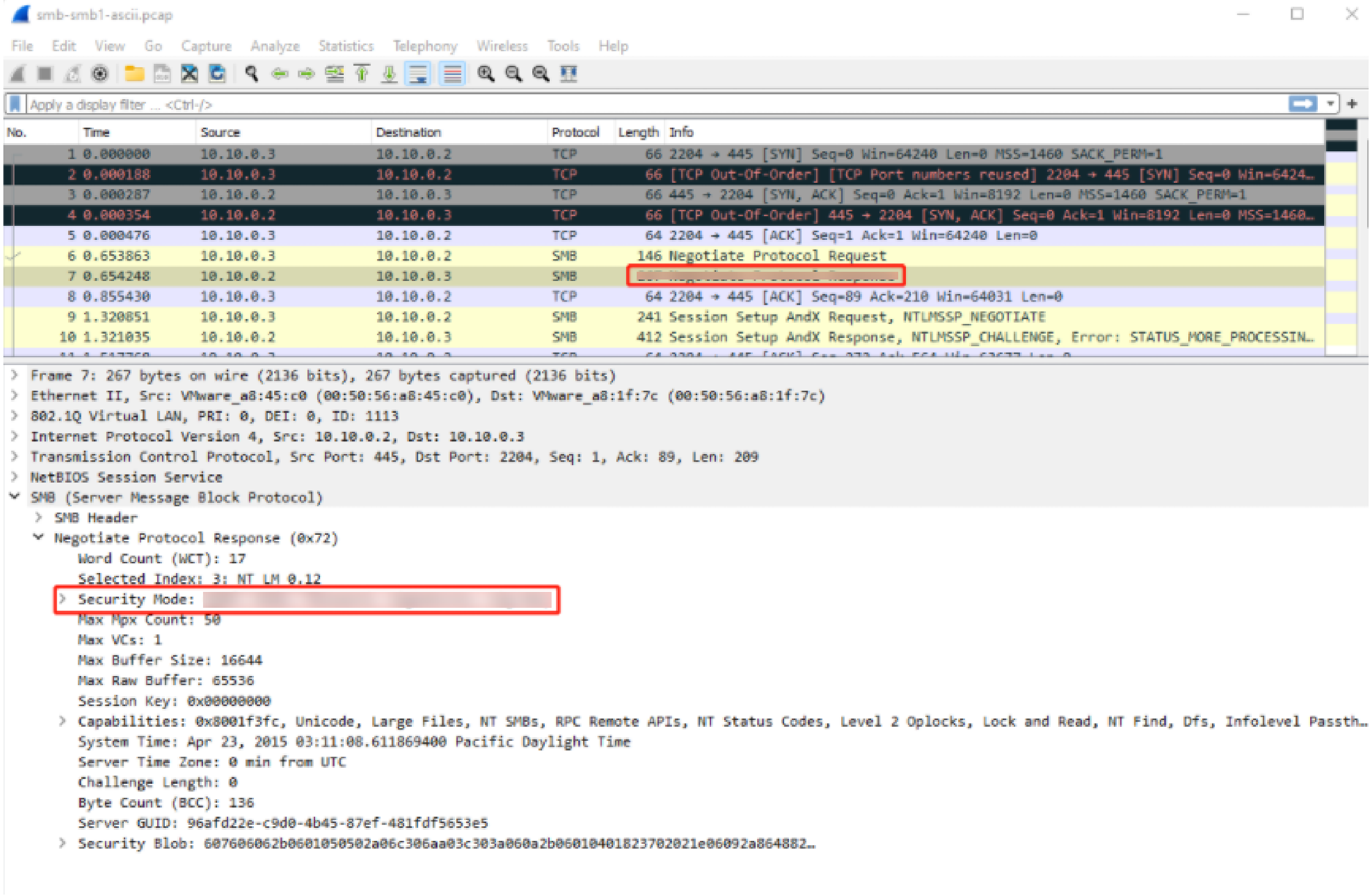
Examples

Wireshark pcap



```
> Transmission Control Protocol, Src Port: 443, Dst Port: 31749, Seq: 1, Ack: 518, Len: 1430
v Transport Layer Security
    v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 122
      v Handshake Protocol: Server Hello
          Handshake Type: Server Hello (2)
          Length: 118
          Version: TLS [redacted])
          Random: 0b82b3a7f99484d6c318e93f7e2f79020ad024a7e10017b974117c1a4fb6b789
          Session ID Length: 32
          Session ID: 96250d1ac4b7bcf22a4aba0466495cf5df38a3d765f01a1aea089c0e37be1f7b
          Cipher Suite: TLS_[redacted]
          Compression Method: null (0)
          Extensions Length: 46
        > Extension: key_share (len=36)
        v Extension: supported_versions (len=2)
              Type: supported_versions (43)
              Length: 2
              Supported Version: TLS [redacted]
          [JA3S Fullstring: 771,4865,51-43]
          [JA3S: eb1d94daa7e0344597e756a1fb6e7054]
    v TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
```

Weak security mode

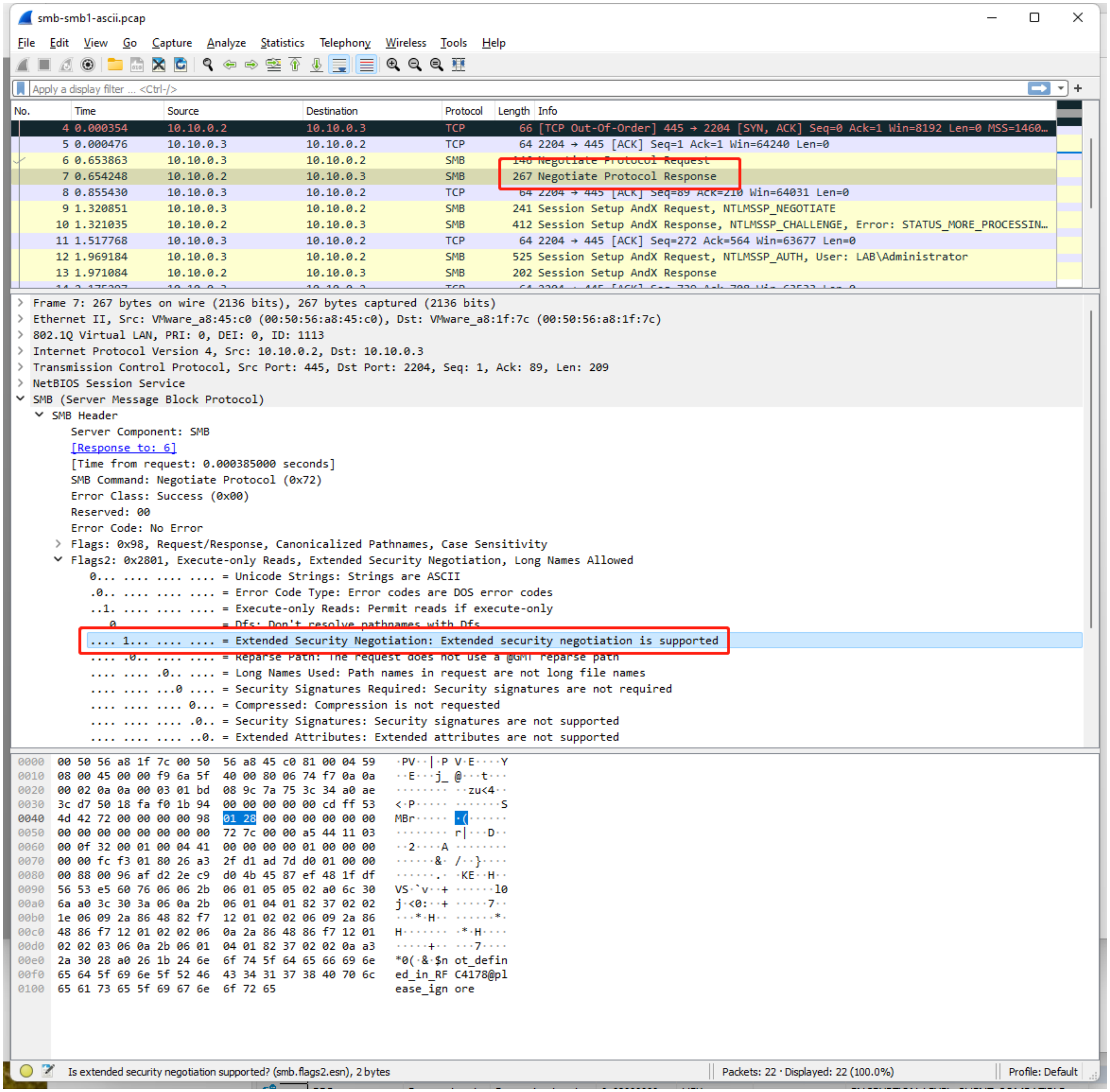


smb-smb1-ascii.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source     Destination Protocol Length Info
   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=6424…
   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      [redacted]
   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…
```

```
> 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
v SMB (Server Message Block Protocol)
  > SMB Header
  v Negotiate Protocol Response (0x72)
      Word Count (WCT): 17
      Selected Index: 3: NT LM 0.12
    > Security Mode: [redacted]
      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-481fdf5653e5
    > 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-/>

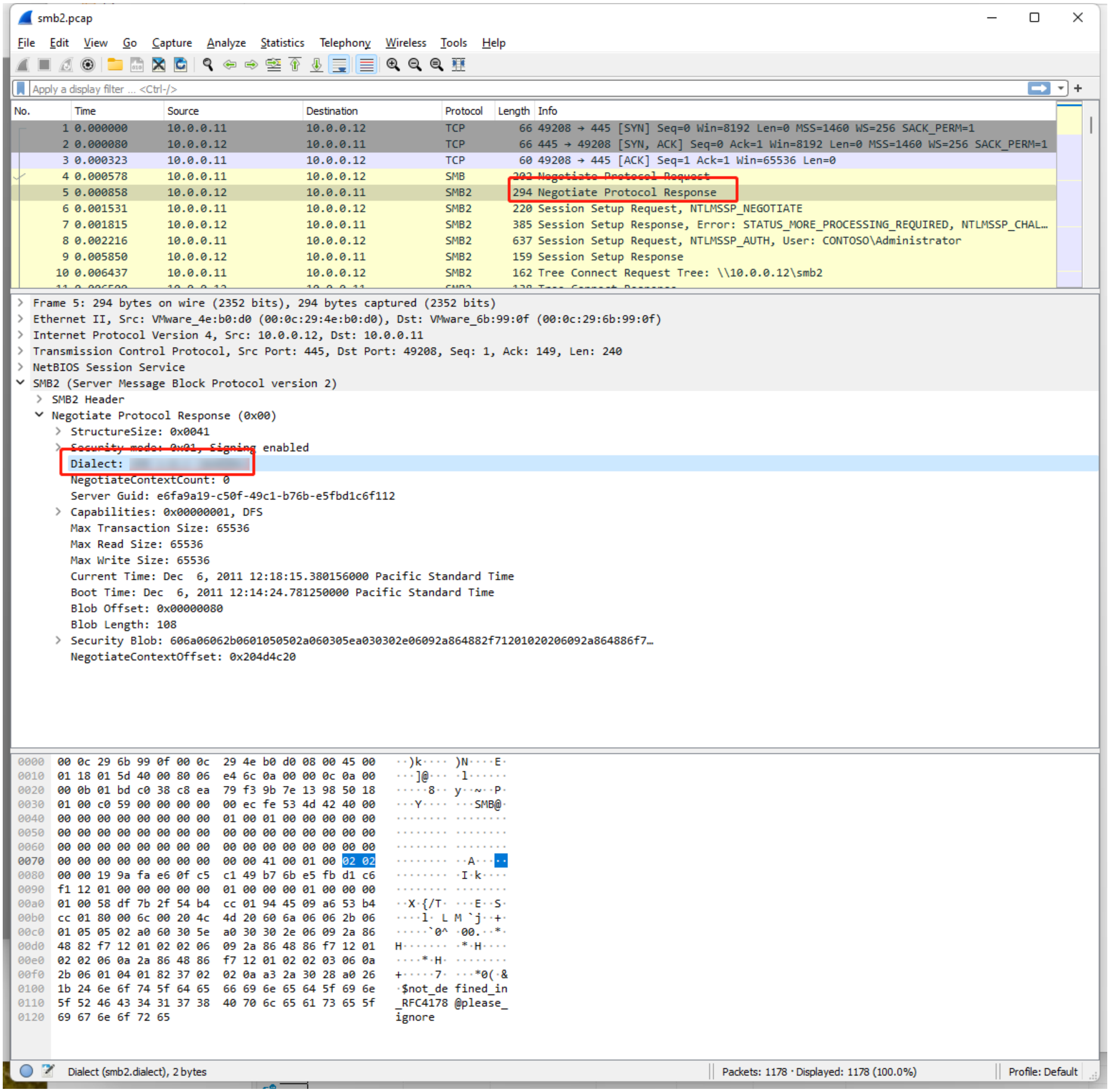
```
No.  Time      Source     Destination Protocol Length Info
   4 0.000354  10.10.0.2  10.10.0.3   TCP        66 [TCP Out-Of-Order] 445 → 2204 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460…
   5 0.000476  10.10.0.3  10.10.0.2   TCP        64 2204 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   6 0.653863  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
v SMB (Server Message Block Protocol)
  v 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
    v 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 ae   ········ ··zu<4··
0030  3c d7 50 18 fa f0 1b 94  00 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 00   MBr····· ·(······
0050  00 00 00 00 00 00 00 00  72 7c 00 00 a5 44 11 03   ········ r|···D··
0060  00 0f 32 00 01 00 04 41  00 00 00 00 01 00 00 00   ··2····A ········
0070  00 00 fc f3 01 80 26 a3  2f d1 ad 7d d0 01 00 00   ······&· /··}····
0080  00 88 00 96 af d2 2e c9  d0 4b 45 87 ef 48 1f df   ·······. ·KE··H··
0090  56 53 e5 60 76 06 06 2b  06 01 05 05 02 a0 6c 30   VS·`v··+ ······l0
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 5f 69 67 6e  6f 72 65                  ease_ign ore
```

Is extended security negotiation supported? (smb.flags2.esn), 2 bytes

Weak dialect



smb2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

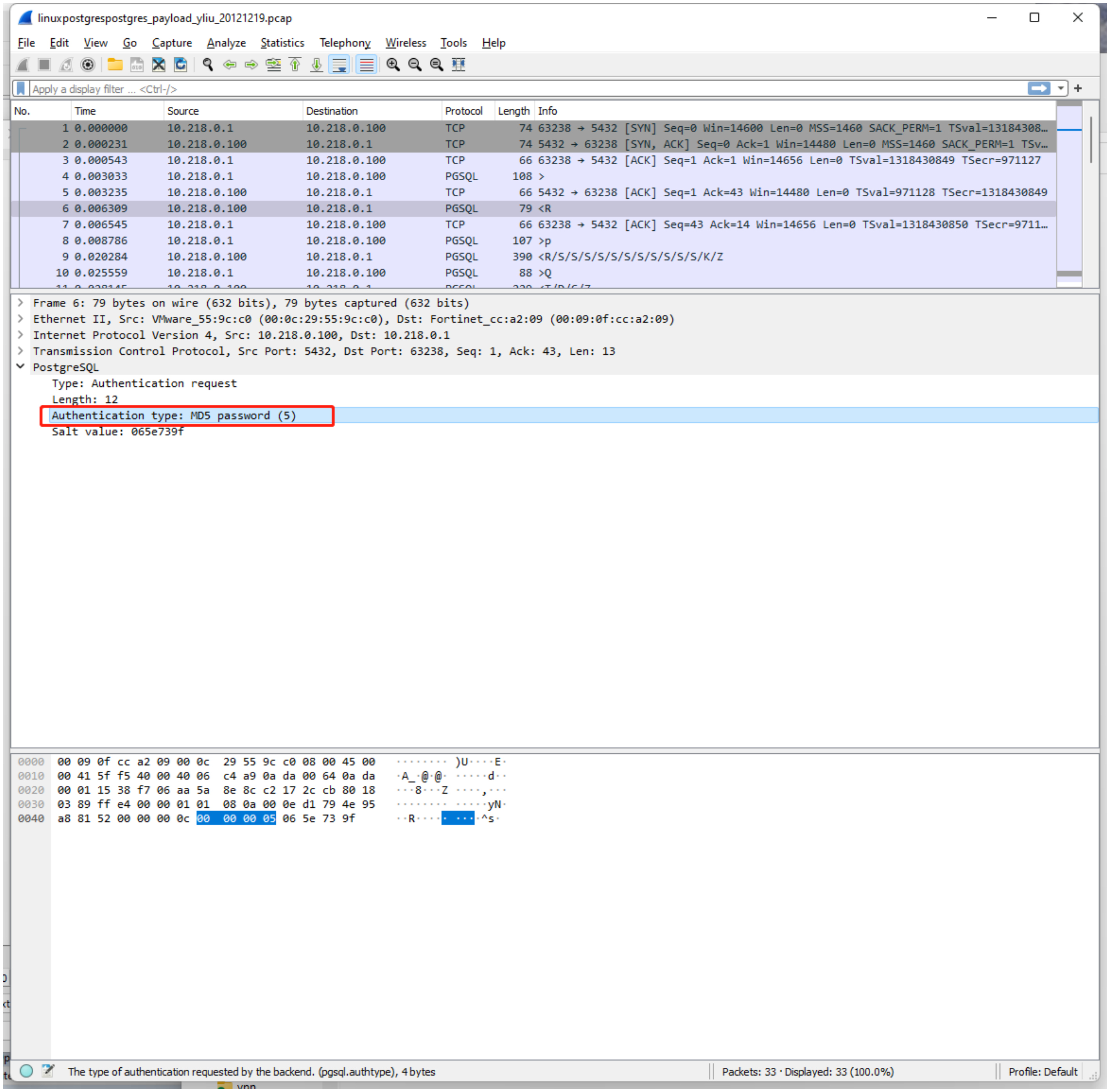
```
No.  Time      Source     Destination Protocol Length Info
   1 0.000000  10.0.0.11  10.0.0.12   TCP       66 49208 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   2 0.000080  10.0.0.12  10.0.0.11   TCP       66 445 → 49208 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   3 0.000323  10.0.0.11  10.0.0.12   TCP       60 49208 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   4 0.000578  10.0.0.11  10.0.0.12   SMB      292 Negotiate Protocol Request
   5 0.000858  10.0.0.12  10.0.0.11   SMB2     294 Negotiate Protocol Response
   6 0.001531  10.0.0.11  10.0.0.12   SMB2     220 Session Setup Request, NTLMSSP_NEGOTIATE
   7 0.001815  10.0.0.12  10.0.0.11   SMB2     385 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHAL…
   8 0.002216  10.0.0.11  10.0.0.12   SMB2     637 Session Setup Request, NTLMSSP_AUTH, User: CONTOSO\Administrator
   9 0.005850  10.0.0.12  10.0.0.11   SMB2     159 Session Setup Response
  10 0.006437  10.0.0.11  10.0.0.12   SMB2     162 Tree Connect Request Tree: \\10.0.0.12\smb2
```

```
> Frame 5: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits)
> Ethernet II, Src: VMware_4e:b0:d0 (00:0c:29:4e:b0:d0), Dst: VMware_6b:99:0f (00:0c:29:6b:99:0f)
> Internet Protocol Version 4, Src: 10.0.0.12, Dst: 10.0.0.11
> Transmission Control Protocol, Src Port: 445, Dst Port: 49208, Seq: 1, Ack: 149, Len: 240
> NetBIOS Session Service
v SMB2 (Server Message Block Protocol version 2)
  > SMB2 Header
  v Negotiate Protocol Response (0x00)
    > StructureSize: 0x0041
    > Security mode: 0x01, Signing enabled
      Dialect: [redacted]
      NegotiateContextCount: 0
      Server Guid: e6fa9a19-c50f-49c1-b76b-e5fbd1c6f112
    > Capabilities: 0x00000001, DFS
      Max Transaction Size: 65536
      Max Read Size: 65536
      Max Write Size: 65536
      Current Time: Dec  6, 2011 12:18:15.380156000 Pacific Standard Time
      Boot Time: Dec  6, 2011 12:14:24.781250000 Pacific Standard Time
      Blob Offset: 0x00000080
      Blob Length: 108
    > Security Blob: 606a06062b0601050502a060305ea030302e06092a864882f71201020206092a864886f7…
      NegotiateContextOffset: 0x204d4c20
```

```
0000  00 0c 29 6b 99 0f 00 0c  29 4e b0 d0 08 00 45 00   ··)k····)N····E·
0010  01 18 01 5d 40 00 80 06  e4 6c 0a 00 00 0c 0a 00   ···]@····l······
0020  00 0b 01 bd c0 38 c8 ea  79 f3 9b 7e 13 98 50 18   ·····8··y··~··P·
0030  01 00 c0 59 00 00 00 00  00 ec fe 53 4d 42 40 00   ···Y······SMB@·
0040  00 00 00 00 00 00 00 00  01 00 01 00 00 00 00 00   ················
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0070  00 00 00 00 00 00 00 00  00 00 41 00 01 00 02 02   ··········A·····
0080  00 00 19 9a fa e6 0f c5  c1 49 b7 6b e5 fb d1 c6   ·········I·k····
0090  f1 12 01 00 00 00 00 00  01 00 00 00 01 00 00 00   ················
00a0  01 00 58 df 7b 2f 54 b4  cc 01 94 45 09 a6 53 b4   ··X·{/T····E··S·
00b0  cc 01 80 00 6c 00 20 4c  4d 20 60 6a 06 06 2b 06   ····l· LM `j··+·
00c0  01 05 05 02 a0 60 30 5e  a0 30 30 2e 06 09 2a 86   ·····`0^·00.··*·
00d0  48 82 f7 12 01 02 02 06  09 2a 86 48 86 f7 12 01   H········*·H····
00e0  02 02 06 0a 2a 86 48 86  f7 12 01 02 02 03 06 0a   ····*·H·········
00f0  2b 06 01 04 01 82 37 02  02 0a a3 2a 30 28 a0 26   +·····7····*0(·&
0100  1b 24 6e 6f 74 5f 64 65  66 69 6e 65 64 5f 69 6e   ·$not_defined_in
0110  5f 52 46 43 34 31 37 38  40 70 6c 65 61 73 65 5f   _RFC4178@please_
0120  69 67 6e 6f 72 65                                  ignore
```

Dialect (smb2.dialect), 2 bytes
Packets: 1178 · Displayed: 1178 (100.0%)
Profile: Default

Weak authentication



linuxpostgrespostgres_payload_yliu_20121219.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
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
```

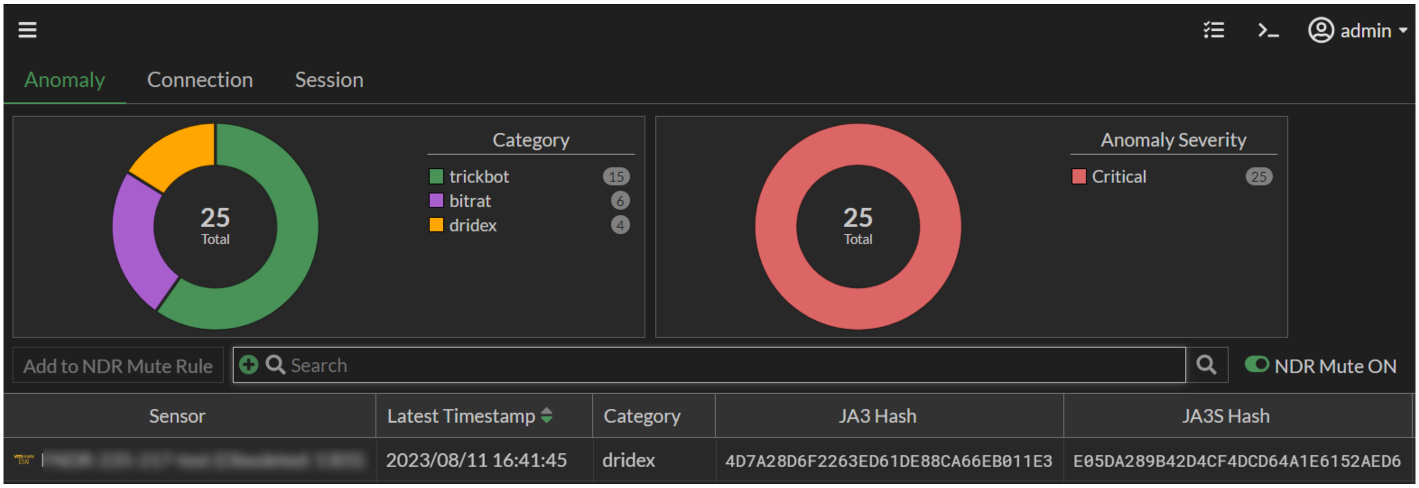
```
> Frame 6: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Ethernet II, Src: VMware_55:9c:c0 (00:0c:29:55:9c:c0), Dst: Fortinet_cc:a2:09 (00:09:0f:cc:a2:09)
> Internet Protocol Version 4, Src: 10.218.0.100, Dst: 10.218.0.1
> Transmission Control Protocol, Src Port: 5432, Dst Port: 63238, Seq: 1, Ack: 43, Len: 13
v PostgreSQL
    Type: Authentication request
    Length: 12
    Authentication type: MD5 password (5)
    Salt value: 065e739f
```

```
0000  00 09 0f cc a2 09 00 0c  29 55 9c c0 08 00 45 00   ········ )U····E·
0010  00 41 5f f5 40 00 40 06  c4 a9 0a da 00 64 0a da   ·A_·@·@· ·····d··
0020  00 01 15 38 f7 06 aa 5a  8e 8c c2 17 2c cb 80 18   ···8···Z ····,···
0030  03 89 ff e4 00 00 01 01  08 0a 00 0e d1 79 4e 95   ········ ·····yN·
0040  a8 81 52 00 00 00 0c 00  00 00 05 06 5e 73 9f      ··R····· ···^s·
```

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 uses both JA3 client and server SSL fingerprints in detection, resulting in fewer false positive detections.



Sensor	Latest Timestamp	Category	JA3 Hash	JA3S Hash
[redacted]	2023/08/11 16:41:45	dridex	4D7A28D6F2263ED61DE88CA66EB011E3	E05DA289B42D4CF4DCD64A1E6152AED6

The *Encrypted Attack* monitor displays the following information:

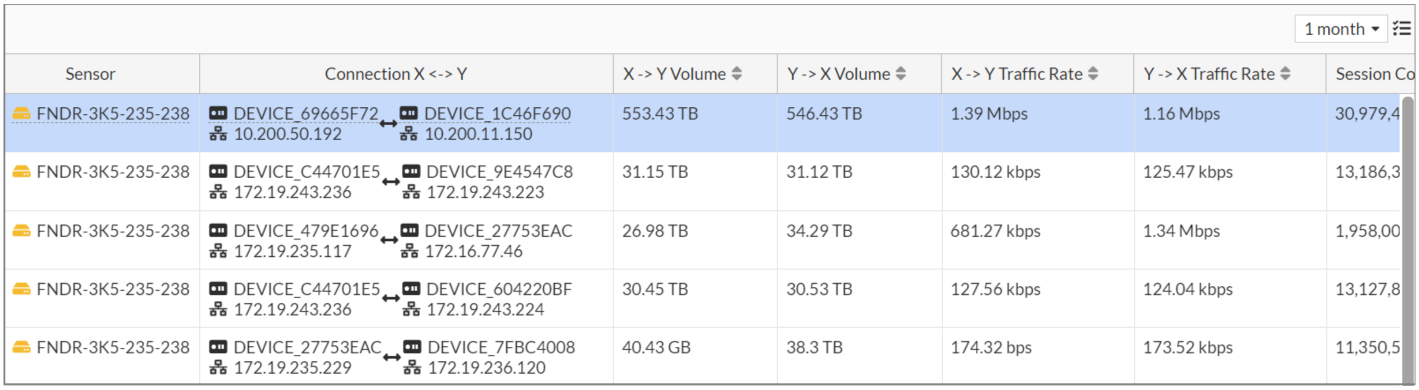
Column	Description
Latest Timestamp	The date the record was updated.
Category	The device category (*Unknown*, *Home & Office*, *Mobile* and *Network*).
JA3 Hash	The JA3 Client.
JA3S Hash	The JA3 Client. *S* indicates *Severe*.
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Timestamp	The timestamp for the first time the anomaly was detected.

For information about muting rules, see NDR Muting on page 127.

Top talker

The *Network Insights* > *Top Talker* page displays the IP addresses that are responsible for the most network traffic in a given time period. You can use this page to troubleshoot performance issues and optimize network usage by identifying the devices or

IP addresses that are consuming the most bandwidth.



1 month

Sensor	Connection X <-> Y	X -> Y Volume	Y -> X Volume	X -> Y Traffic Rate	Y -> X Traffic Rate	Session Co
FNDR-3K5-235-238	DEVICE_69665F72 10.200.50.192 ↔ DEVICE_1C46F690 10.200.11.150	553.43 TB	546.43 TB	1.39 Mbps	1.16 Mbps	30,979,4
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_9E4547C8 172.19.243.223	31.15 TB	31.12 TB	130.12 kbps	125.47 kbps	13,186,3
FNDR-3K5-235-238	DEVICE_479E1696 172.19.235.117 ↔ DEVICE_27753EAC 172.16.77.46	26.98 TB	34.29 TB	681.27 kbps	1.34 Mbps	1,958,00
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_604220BF 172.19.243.224	30.45 TB	30.53 TB	127.56 kbps	124.04 kbps	13,127,8
FNDR-3K5-235-238	DEVICE_27753EAC 172.19.235.229 ↔ DEVICE_7FBC4008 172.19.236.120	40.43 GB	38.3 TB	174.32 bps	173.52 kbps	11,350,5

The *Top Talker* page displays the following information:

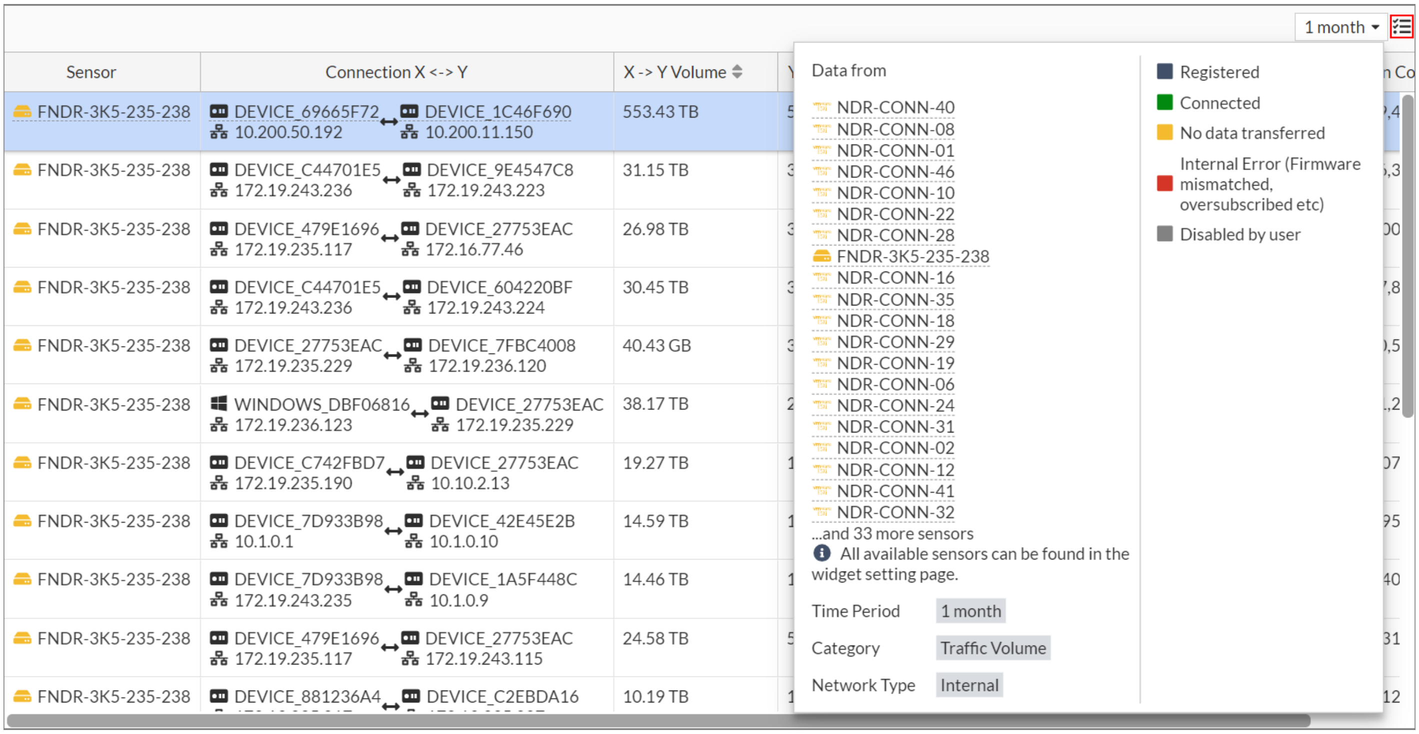
Sensor (Center mode)	The network sensor. Hover over the sensors ID to view the *IP Address*, Serial number (*S/N*), *Last Sync Time* and *Status*.
Connection X <-> Y	The source and destination device IPs. Hover over the IP address to view the *Device* ID, *MAC Address*, *IP Address*, *Hardware*, and *OS* (if known). Click *View Device Detail* to view the device information page.
X-> Y Volume	The amount of traffic traveling from the source device to the destination device in TB.
Y-> X Volume	The amount of traffic traveling from the destination device to the source device in TB.
X -> Y Traffic Rate	The traffic rate from the source device to the destination device in bps.
Y -> X Traffic Rate	The traffic rate from the destination device to the source device in bps.
Session Count	The number of sessions.

To set the time range:

At the top-right side of the page, click the dropdown and select *1 day*, *1 week* or *1 month*.

To view the sensor statistics:

In Center mode, click the statistics icon at the top-right corner of the page.



Sensor	Connection X <-> Y	X -> Y Volume
FNDR-3K5-235-238	DEVICE_69665F72 10.200.50.192 ↔ DEVICE_1C46F690 10.200.11.150	553.43 TB
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_9E4547C8 172.19.243.223	31.15 TB
FNDR-3K5-235-238	DEVICE_479E1696 172.19.235.117 ↔ DEVICE_27753EAC 172.16.77.46	26.98 TB
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_604220BF 172.19.243.224	30.45 TB
FNDR-3K5-235-238	DEVICE_27753EAC 172.19.235.229 ↔ DEVICE_7FBC4008 172.19.236.120	40.43 GB
FNDR-3K5-235-238	WINDOWS_DBF06816 172.19.236.123 ↔ DEVICE_27753EAC 172.19.235.229	38.17 TB
FNDR-3K5-235-238	DEVICE_C742FBD7 172.19.235.190 ↔ DEVICE_27753EAC 10.10.2.13	19.27 TB
FNDR-3K5-235-238	DEVICE_7D933B98 10.1.0.1 ↔ DEVICE_42E45E2B 10.1.0.10	14.59 TB
FNDR-3K5-235-238	DEVICE_7D933B98 172.19.243.235 ↔ DEVICE_1A5F448C 10.1.0.9	14.46 TB
FNDR-3K5-235-238	DEVICE_479E1696 172.19.235.117 ↔ DEVICE_27753EAC 172.19.243.115	24.58 TB
FNDR-3K5-235-238	DEVICE_881236A4 ↔ DEVICE_C2EBDA16	10.19 TB

Data from

NDR-CONN-40
NDR-CONN-08
NDR-CONN-01
NDR-CONN-46
NDR-CONN-10
NDR-CONN-22
NDR-CONN-28
FNDR-3K5-235-238
NDR-CONN-16
NDR-CONN-35
NDR-CONN-18
NDR-CONN-29
NDR-CONN-19
NDR-CONN-06
NDR-CONN-24
NDR-CONN-31
NDR-CONN-02
NDR-CONN-12
NDR-CONN-41
NDR-CONN-32
...and 33 more sensors

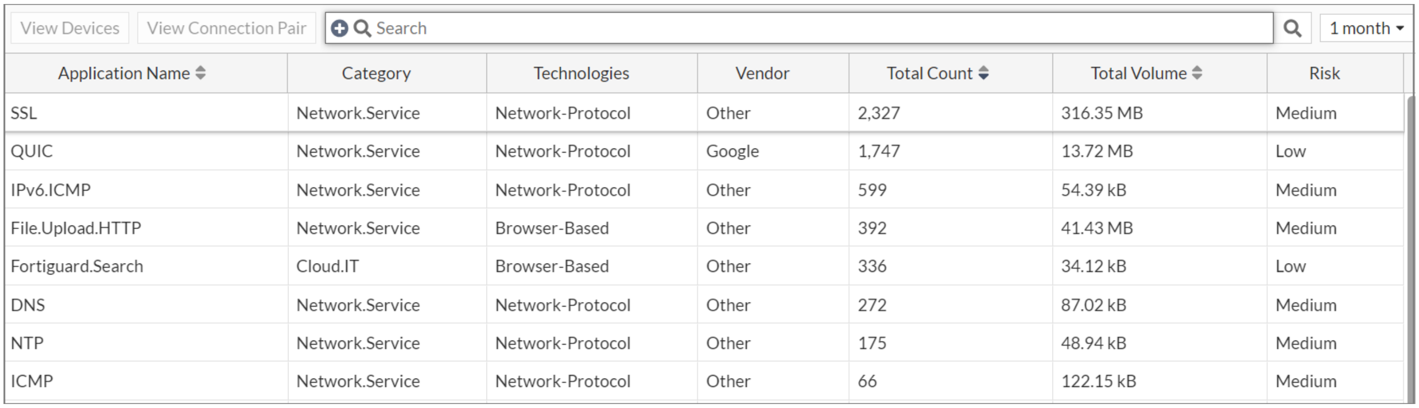
ℹ All available sensors can be found in the widget setting page.

Time Period: 1 month
Category: Traffic Volume
Network Type: Internal

- ■ Registered
- 🟩 Connected
- 🟨 No data transferred
- 🟥 Internal Error (Firmware mismatched, oversubscribed etc)
- ■ Disabled by user

Top application

The *Network Insights* > *Top Application* page displays the top applications and protocols that were discovered on the network (*1 day*, *1 week*, *1 month*).



Application Name	Category	Technologies	Vendor	Total Count	Total Volume	Risk
SSL	Network.Service	Network-Protocol	Other	2,327	316.35 MB	Medium
QUIC	Network.Service	Network-Protocol	Google	1,747	13.72 MB	Low
IPv6.ICMP	Network.Service	Network-Protocol	Other	599	54.39 kB	Medium
File.Upload.HTTP	Network.Service	Browser-Based	Other	392	41.43 MB	Medium
Fortiguard.Search	Cloud.IT	Browser-Based	Other	336	34.12 kB	Low
DNS	Network.Service	Network-Protocol	Other	272	87.02 kB	Medium
NTP	Network.Service	Network-Protocol	Other	175	48.94 kB	Medium
ICMP	Network.Service	Network-Protocol	Other	66	122.15 kB	Medium

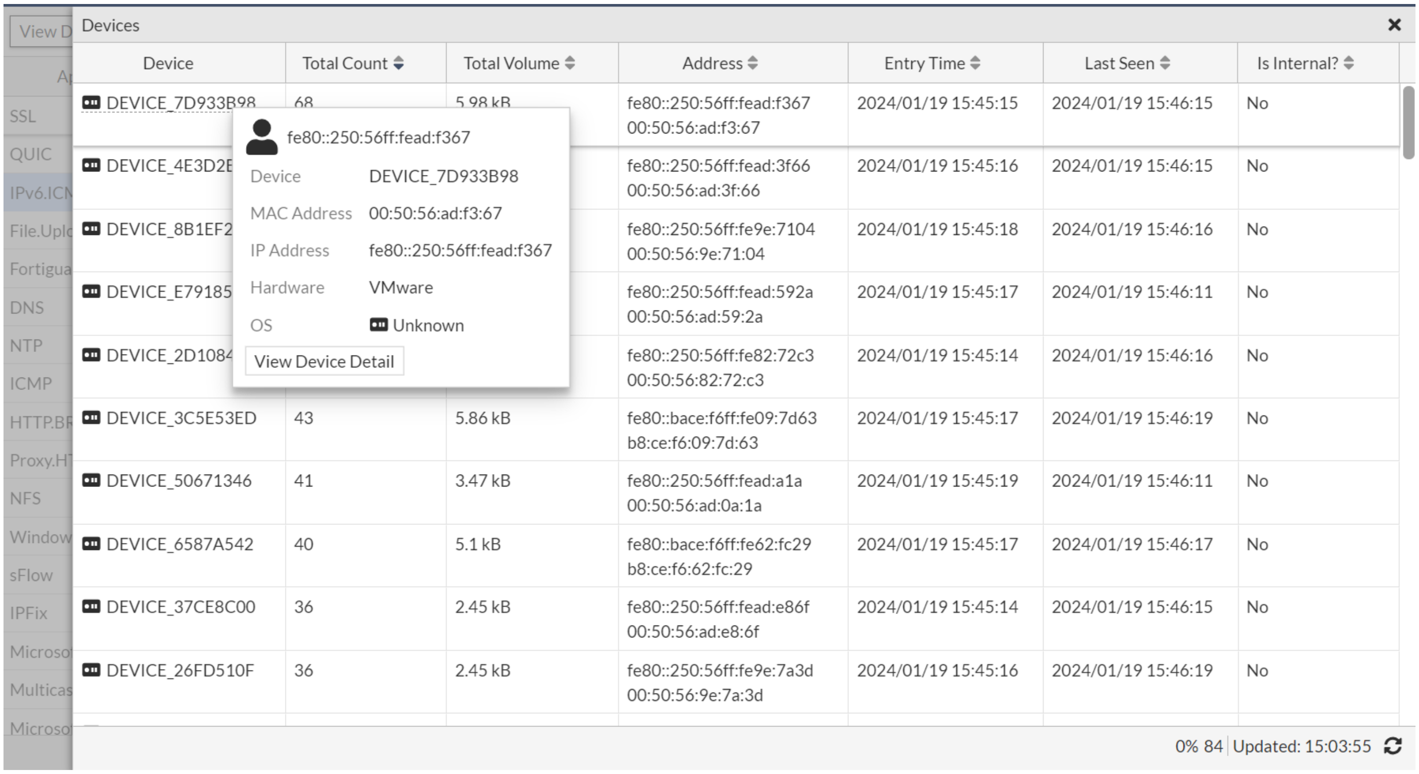
The *Top Application* page displays the following information:

Application Name	The protocols and applications identified in the sniffer traffic. For more information, see Appendix G: Supported Application Protocol List on page 279.
Category	The application or protocol category.

Technologies	The application or protocol technology.
Vendor	The application vendor.
Total Count	The number of times the application or protocol was detected during the time frame.
Total Volume	The application volume in MB.
Risk	The risk level (*Critical*, *High*, *Medium*, or *Low*)

To view devices:

Click an entry in the table and then click *View Devices*. The *Devices* pane opens. Hover over the device ID to view the *MAC Address*, *IP Address*, *Hardware*, and *OS*. Click *View Device Detail* to view the *Device Information* page.



Devices ✕

Device	Total Count	Total Volume	Address	Entry Time	Last Seen	Is Internal?
DEVICE_7D933B98	68	5.98 kB	fe80::250:56ff:fead:f367 00:50:56:ad:f3:67	2024/01/19 15:45:15	2024/01/19 15:46:15	No
DEVICE_4E3D2E			fe80::250:56ff:fead:3f66 00:50:56:ad:3f:66	2024/01/19 15:45:16	2024/01/19 15:46:15	No
DEVICE_8B1EF2			fe80::250:56ff:fe9e:7104 00:50:56:9e:71:04	2024/01/19 15:45:18	2024/01/19 15:46:16	No
DEVICE_E79185			fe80::250:56ff:fead:592a 00:50:56:ad:59:2a	2024/01/19 15:45:17	2024/01/19 15:46:11	No
DEVICE_2D1084			fe80::250:56ff:fe82:72c3 00:50:56:82:72:c3	2024/01/19 15:45:14	2024/01/19 15:46:16	No
DEVICE_3C5E53ED	43	5.86 kB	fe80::bace:f6ff:fe09:7d63 b8:ce:f6:09:7d:63	2024/01/19 15:45:17	2024/01/19 15:46:19	No
DEVICE_50671346	41	3.47 kB	fe80::250:56ff:fead:a1a 00:50:56:ad:0a:1a	2024/01/19 15:45:19	2024/01/19 15:46:11	No
DEVICE_6587A542	40	5.1 kB	fe80::bace:f6ff:fe62:fc29 b8:ce:f6:62:fc:29	2024/01/19 15:45:17	2024/01/19 15:46:17	No
DEVICE_37CE8C00	36	2.45 kB	fe80::250:56ff:fead:e86f 00:50:56:ad:e8:6f	2024/01/19 15:45:14	2024/01/19 15:46:15	No
DEVICE_26FD510F	36	2.45 kB	fe80::250:56ff:fe9e:7a3d 00:50:56:9e:7a:3d	2024/01/19 15:45:16	2024/01/19 15:46:19	No

fe80::250:56ff:fead:f367

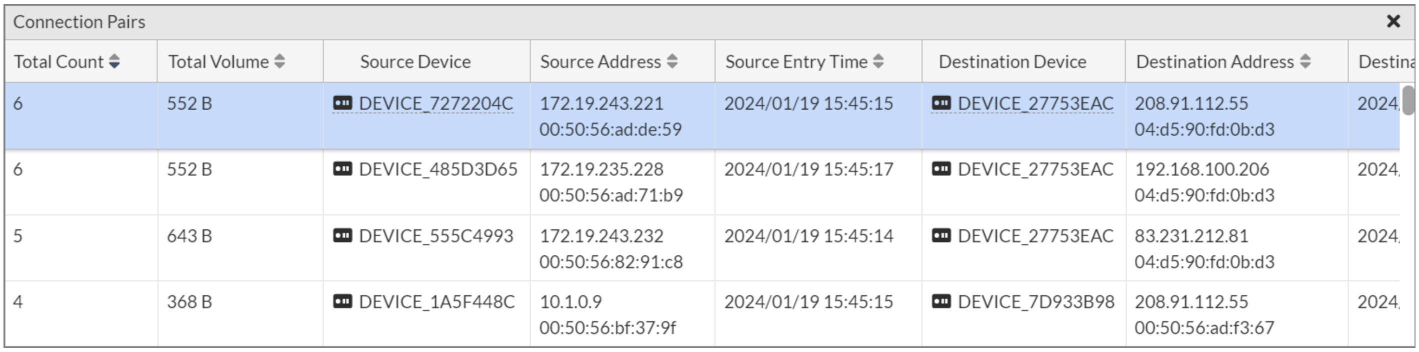
Device	DEVICE_7D933B98
MAC Address	00:50:56:ad:f3:67
IP Address	fe80::250:56ff:fead:f367
Hardware	VMware
OS	Unknown

View Device Detail

0% 84 | Updated: 15:03:55

To view connection pairs:

Click an entry in the table and then click *View Connection Pair*. The *Connection Pairs* pane opens.



Connection Pairs ✕

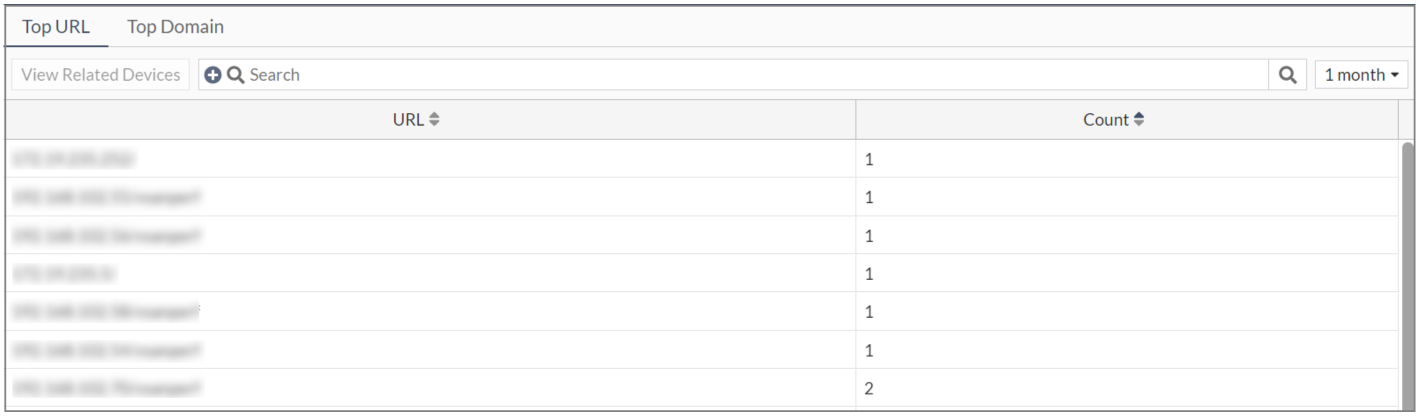
Total Count ⬍	Total Volume ⬍	Source Device	Source Address ⬍	Source Entry Time ⬍	Destination Device	Destination Address ⬍	Destina
6	552 B	DEVICE_7272204C	172.19.243.221 00:50:56:ad:de:59	2024/01/19 15:45:15	DEVICE_27753EAC	208.91.112.55 04:d5:90:fd:0b:d3	2024.
6	552 B	DEVICE_485D3D65	172.19.235.228 00:50:56:ad:71:b9	2024/01/19 15:45:17	DEVICE_27753EAC	192.168.100.206 04:d5:90:fd:0b:d3	2024.
5	643 B	DEVICE_555C4993	172.19.243.232 00:50:56:82:91:c8	2024/01/19 15:45:14	DEVICE_27753EAC	83.231.212.81 04:d5:90:fd:0b:d3	2024.
4	368 B	DEVICE_1A5F448C	10.1.0.9 00:50:56:bf:37:9f	2024/01/19 15:45:15	DEVICE_7D933B98	208.91.112.55 00:50:56:ad:f3:67	2024.

Top URL/Domain

The *Network Insights* > *Top URL / Domain* page displays the IP address for the top URLs and domains detected within the time range (*1 day*, *1 week* and *1 month*).

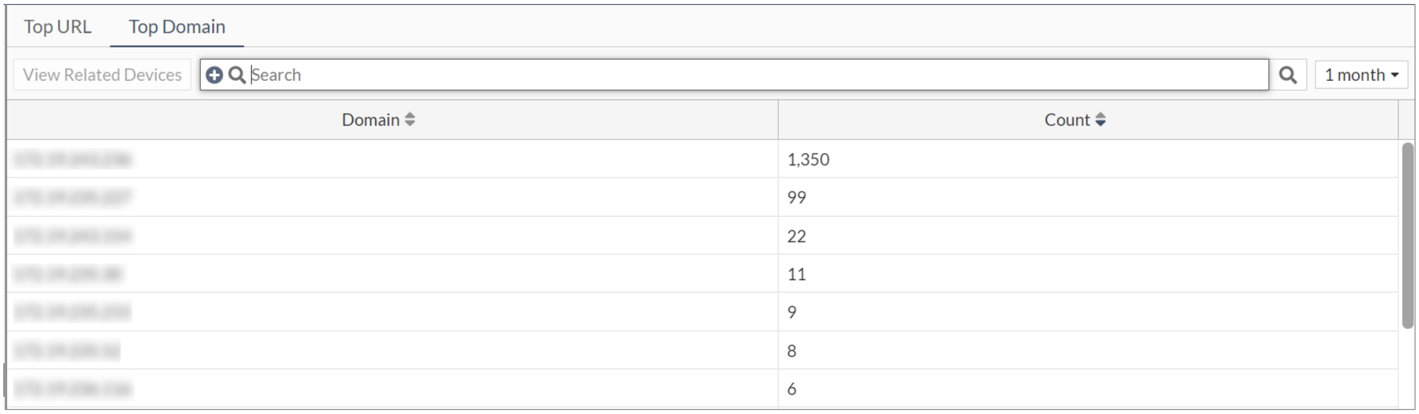
The *Top URL / Domain* page displays following information:

URL	The URL IP address.
Domain	The domain IP address.
Count	The number of times the URL or domain were detected with the time range.



URL ⬍	Count ⬍
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	2

Click the *Top Domain* tab to view the domain IP and count.



Domain	Count
[redacted]	1,350
[redacted]	99
[redacted]	22
[redacted]	11
[redacted]	9
[redacted]	8
[redacted]	6

MITRE ATT&CK

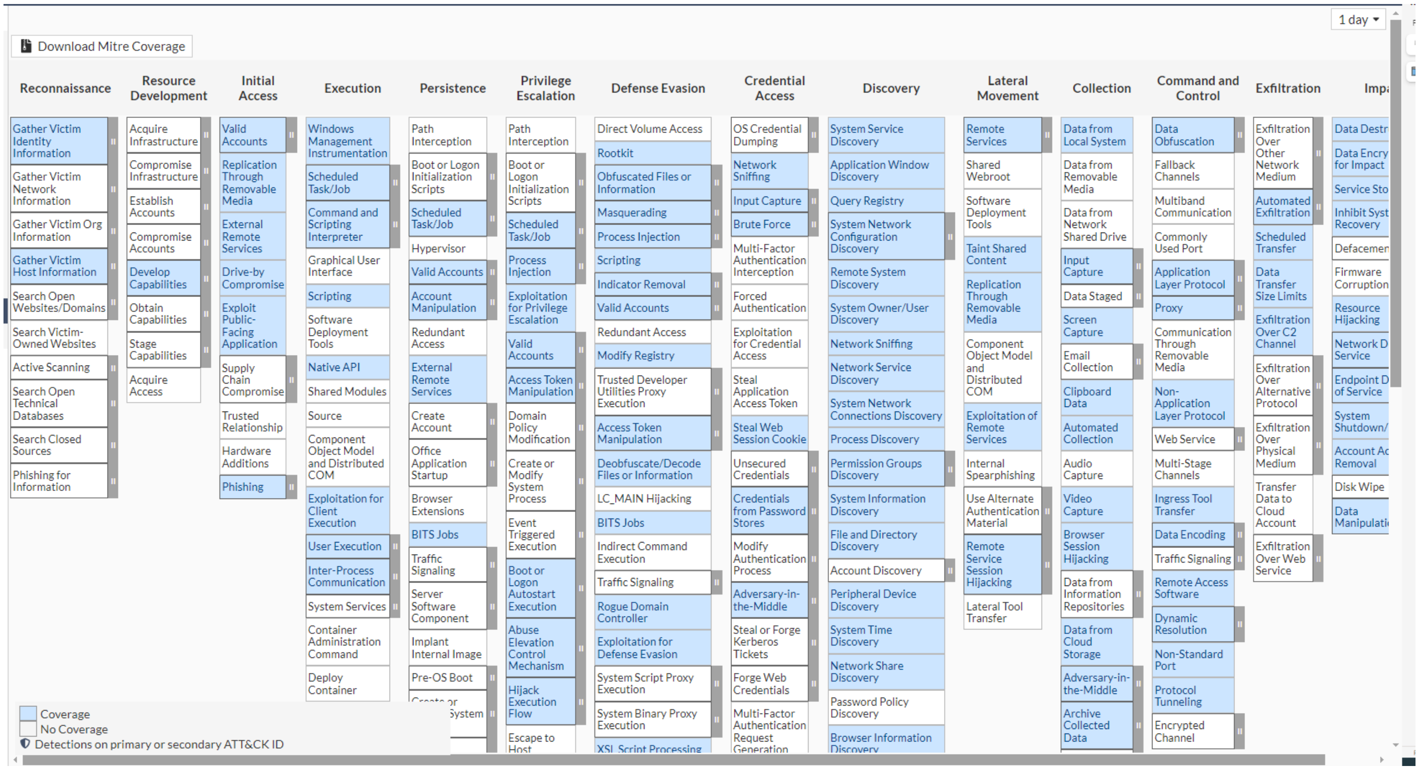
MITRE ATT&CK is a knowledge base of threat behaviors relied upon by security professionals worldwide. The *Network Insights > MITRE ATT&CK* page tracks the number of events that occurred for each MITRE attack tactics category.

The dashboard displays the detection by behavior (behavioral and non-behavioral) and by technique (primary and secondary).

- The Primary technique is what is used to detect the behavior.
- The Secondary technique is not always related to what is seen on the network, but is related to the threat in general. The secondary technique will not be displayed in some instances.

The column headers in the *MITRE ATT&CK* page are tactics, and the tiles within these columns are the relevant techniques. The MITRE ATT&CK technique with FortiNDR coverage appears as a blue block. When a MITRE ATT&CK technique detection has been triggered, the technique block will display a shield icon.

Click *Download Mitre Coverage* to export the data as CSV file.



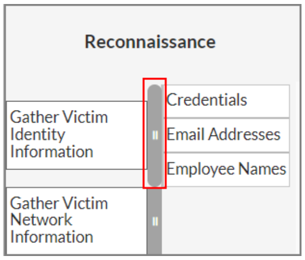
Download Mitre Coverage

1 day ▾

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impa
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destr
Gather Victim Network Information	Compromise Infrastructure	Replication Through Removable Media	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	Network Sniffing	Application Window Discovery	Shared Webroot	Data from Removable Media	Fallback Channels	Automated Exfiltration	Data Encry for Impact
Gather Victim Org Information	Establish Accounts	External Remote Services	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information	Input Capture	Query Registry	Software Deployment Tools	Data from Network Shared Drive	Multiband Communication	Scheduled Transfer	Service Sto
Gather Victim Host Information	Compromise Accounts	Drive-by Compromise	Graphical User Interface	Hypervisor	Process Injection	Masquerading	Brute Force	System Network Configuration Discovery	Taint Shared Content	Input Capture	Commonly Used Port	Data Transfer Size Limits	Inhibit Syst Recovery
Search Open Websites/Domains	Develop Capabilities	Exploit Public-Facing Application	Scripting	Valid Accounts	Exploitation for Privilege Escalation	Process Injection	Multi-Factor Authentication Interception	Remote System Discovery	Replication Through Removable Media	Data Staged	Application Layer Protocol	Exfiltration Over C2 Channel	Defacemen
Search Victim-Owned Websites	Obtain Capabilities	Supply Chain Compromise	Software Deployment Tools	Account Manipulation	Valid Accounts	Scripting	Forced Authentication	System Owner/User Discovery	Component Object Model and Distributed COM	Screen Capture	Proxy	Exfiltration Over Alternative Protocol	Firmware Corruption
Active Scanning	Stage Capabilities	Trusted Relationship	Native API	Redundant Access	Access Token Manipulation	Indicator Removal	Exploitation for Credential Access	Network Sniffing	Exploitation of Remote Services	Email Collection	Communication Through Removable Media	Exfiltration Over Physical Medium	Resource Hijacking
Search Open Technical Databases	Acquire Access	Hardware Additions	Shared Modules	External Remote Services	Domain Policy Modification	Valid Accounts	Steal Application Access Token	Network Service Discovery	Internal Spearphishing	Clipboard Data	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network D Service
Search Closed Sources		Phishing	Source	Create Account	Create or Modify System Process	Redundant Access	Steal Web Session Cookie	System Network Connections Discovery	Use Alternate Authentication Material	Automated Collection	Web Service	Exfiltration Over Web Service	Endpoint D of Service
Phishing for Information			Component Object Model and Distributed COM	Office Application Startup	Event Triggered Execution	Modify Registry	Unsecured Credentials	Process Discovery	Remote Service Session Hijacking	Audio Capture	Multi-Stage Channels		System Shutdown/
			Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution	Trusted Developer Utilities Proxy Execution	Credentials from Password Stores	Permission Groups Discovery	Lateral Tool Transfer	Video Capture	Ingress Tool Transfer		Account Ac Removal
			User Execution	BITS Jobs	Abuse Elevation Control Mechanism	Access Token Manipulation	Modify Authentication Process	System Information Discovery		Browser Session Hijacking	Data Encoding		Disk Wipe
			Inter-Process Communication	Traffic Signaling	Hijack Execution Flow	Deobfuscate/Decode Files or Information	Adversary-in-the-Middle	File and Directory Discovery		Data from Information Repositories	Traffic Signaling		Data Manipulati
			System Services	Server Software Component	Escape to Host	LC_MAIN Hijacking	Steal or Forge Kerberos Tickets	Account Discovery		Data from Cloud Storage	Remote Access Software		
			Container Administration Command	Implant Internal Image		BITS Jobs	Forge Web Credentials	Peripheral Device Discovery		Adversary-in-the-Middle	Dynamic Resolution		
			Deploy Container	Pre-OS Boot		Indirect Command Execution	Multi-Factor Authentication Request Generation	System Time Discovery		Archive Collected Data	Non-Standard Port		
				Create or System		Traffic Signaling		Network Share Discovery			Protocol Tunneling		
						Rogue Domain Controller		Password Policy Discovery			Encrypted Channel		
						Exploitation for Defense Evasion		Browser Information Discovery					
						System Script Proxy Execution							
						System Binary Proxy Execution							
						XSL Script Processing							

🟦 Coverage
□ No Coverage
Detections on primary or secondary ATT&CK ID

To view the secondary technique, click the vertical bars at right side of the tile.



Reconnaissance

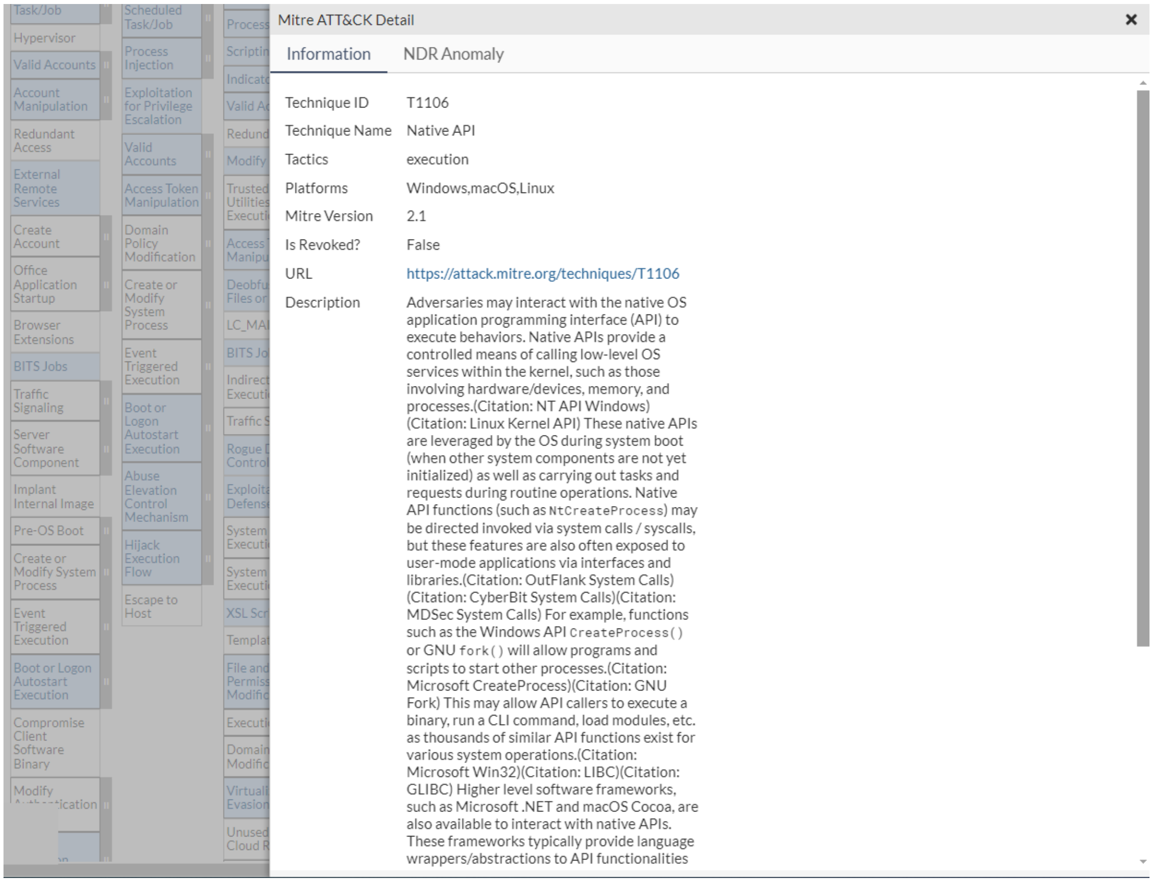
Gather Victim Identity Information	Credentials Email Addresses Employee Names
Gather Victim Network Information	

Mitre ATT&CK detail

Click a tile in the column to view Information about the technique:

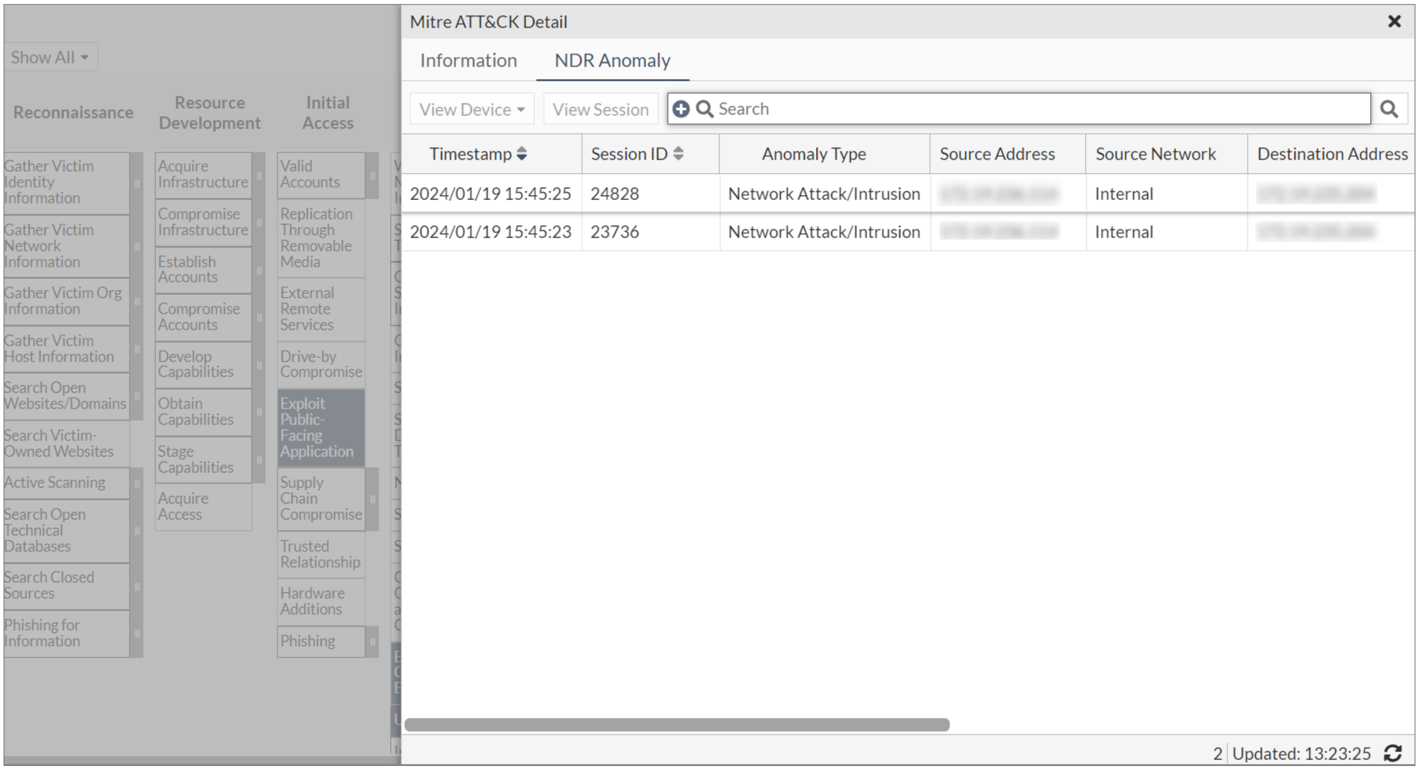
Technique ID	The technique ID.
Technique Name	The technique name.
Tactics	The tactic name.
Platforms	The technique platform.
Mitre Version	The MITRE version.
Is Revoked?	*True* or *False*.
URL	The link to the MITRE description on https://attack.mitre.org.

Description	The MITRE description.


Task/Job
Hypervisor
Valid Accounts
Account Manipulation
Redundant Access
External Remote Services
Create Account
Office Application Startup
Browser Extensions
BITS Jobs
Traffic Signaling
Server Software Component
Implant Internal Image
Pre-OS Boot
Create or Modify System Process
Event Triggered Execution
Boot or Logon Autostart Execution
Compromise Client Software Binary
Modify Authentication
Scheduled Task/Job
Process Injection
Exploitation for Privilege Escalation
Valid Accounts
Access Token Manipulation
Domain Policy Modification
Create or Modify System Process
Event Triggered Execution
Boot or Logon Autostart Execution
Abuse Elevation Control Mechanism
Hijack Execution Flow
Escape to Host
Mitre ATT&CK Detail
Information
NDR Anomaly

Technique ID	T1106
Technique Name	Native API
Tactics	execution
Platforms	Windows,macOS,Linux
Mitre Version	2.1
Is Revoked?	False
URL	https://attack.mitre.org/techniques/T1106
Description	Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities

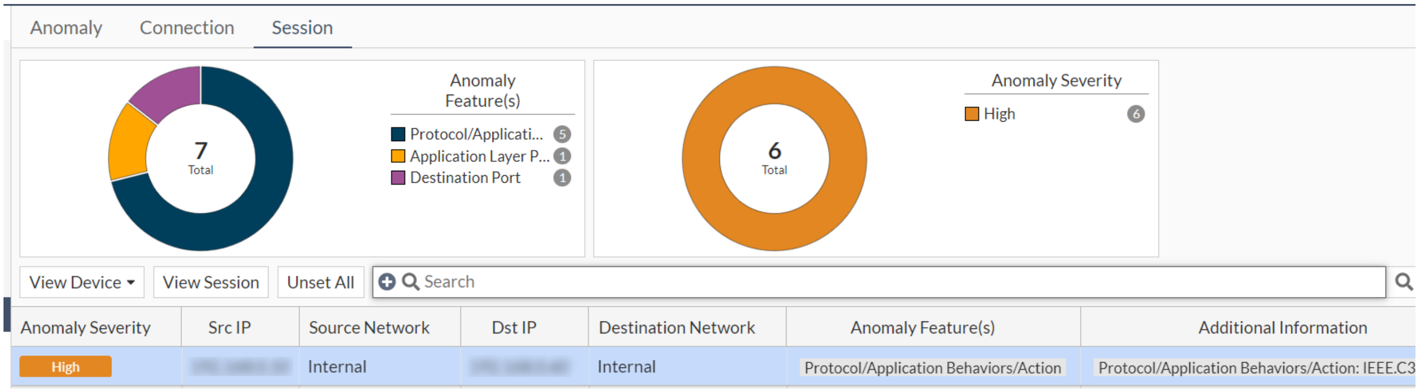
Click the *NDR Anomaly* tab to view all the NDR sessions associated with the selected technique.



Timestamp	Session ID	Anomaly Type	Source Address	Source Network	Destination Address
2024/01/19 15:45:25	24828	Network Attack/Intrusion	[redacted]	Internal	[redacted]
2024/01/19 15:45:23	23736	Network Attack/Intrusion	[redacted]	Internal	[redacted]

ML Discovery (- Center - Standalone)

The *ML Discovery* monitor 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.



Anomaly Severity	Src IP	Source Network	Dst IP	Destination Network	Anomaly Feature(s)	Additional Information
High	[redacted]	Internal	[redacted]	Internal	Protocol/Application Behaviors/Action	Protocol/Application Behaviors/Action: IEEE.C3

The *ML Discovery* monitor displays the following information by default:

Column	Description
Latest Timestamp	The date the record was updated.
Anomaly Features	The feature or feature combinations that caused the anomaly.
Additional Information	The abnormal feature value(s).
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Timestamp	The timestamp for the first time the anomaly was detected.
Current Feedback Status	The user feedback provided for Machine Learning discoveries to correct false positives. This column is not displayed by default.

For information about muting rules, see NDR Muting on page 127.

Session information

To view the session information for an ML Discovery:

1. Click the *Session* tab.
2. Double-click a record in the table. The *Session Information* pane displays the following information:

General	• Session ID • Start Time • End Time • Traffic Volume • VLAN ID • Port ID
Anomaly	• Anomaly Type • Severity
Source Device	• Source IP • Source Port • Source MAC • Source Packet Size • Source Country • Source Device Model • Source OS • Source Device Category • Source Device Sub Category

Destination Device	• Destination IP • Destination Port • Destination MAC • Destination Packet Size • Destination Country • Destination Device Model • Destination OS • Destination Device Category • Destination Device Sub Category

Add feedback to a ML Discovery

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

To view the Current Feedback Status column:

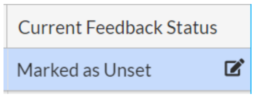
1. Go to *Network Insights* > *ML Discovery* > *Session* tab.
2. Hover over the column headings and then click the *Configure Table* icon.

   ⚙

3. From the *Select Columns* list, select *Current Feedback Status*.
4. Click *Apply*.

To add feedback to a ML Discovery:

1. Go to *Network Insights* > *ML Discovery* > *Session* tab and select a record in the table.
2. In the *Current Feedback Status* column, click the edit button.



Current Feedback Status

Marked as Unset

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

Option	Description
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.
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 Calais to retrain the database.
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".

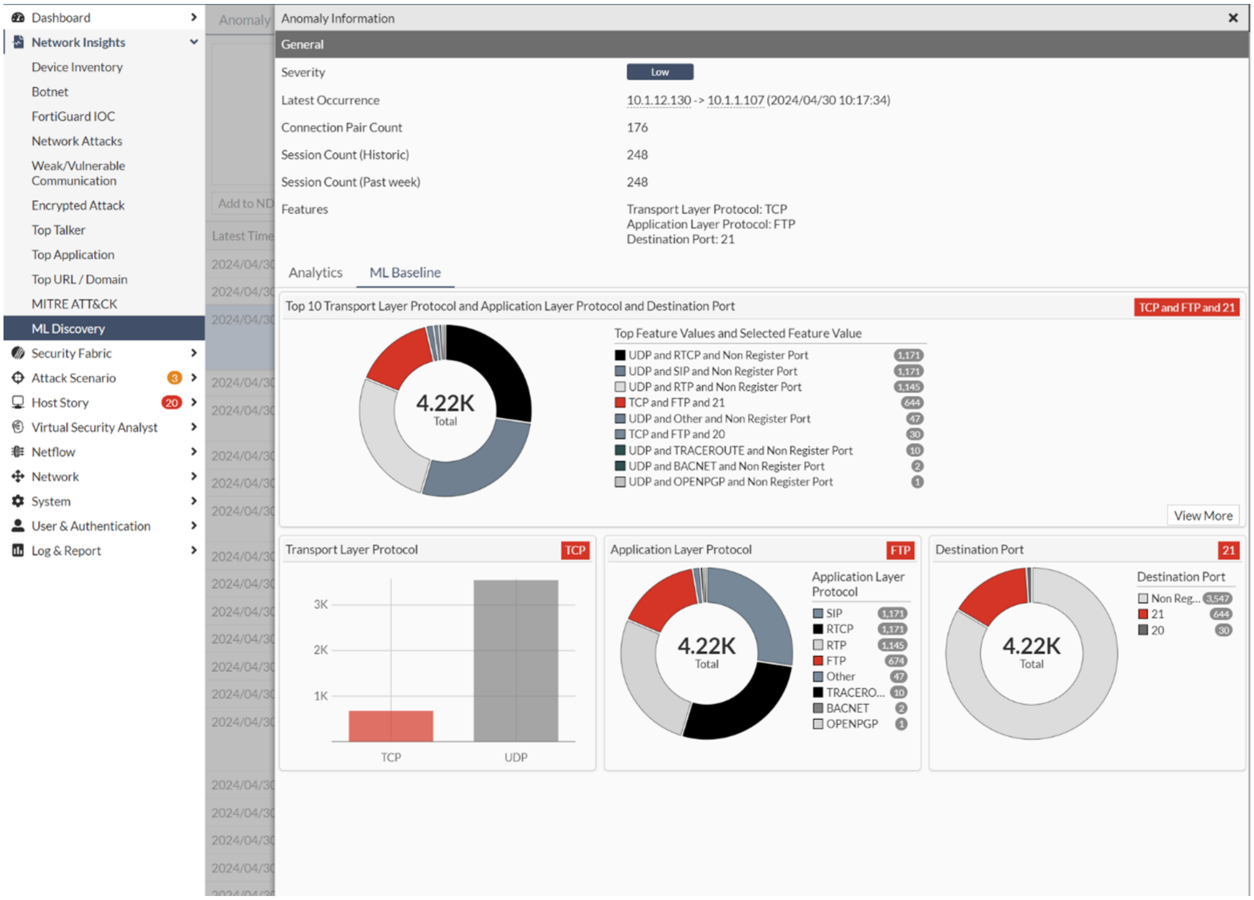
When multiple sessions of the same Source Address share the same value in the Anomaly Feature(s) column, you will only need to add feedback once to apply the feedback to all of the sessions.

4. Click *Apply*.
5. (Optional) To unset all feedback click *Unset All* next to the *Search* field.

ML Baseline information

To view the ML Baseline information:

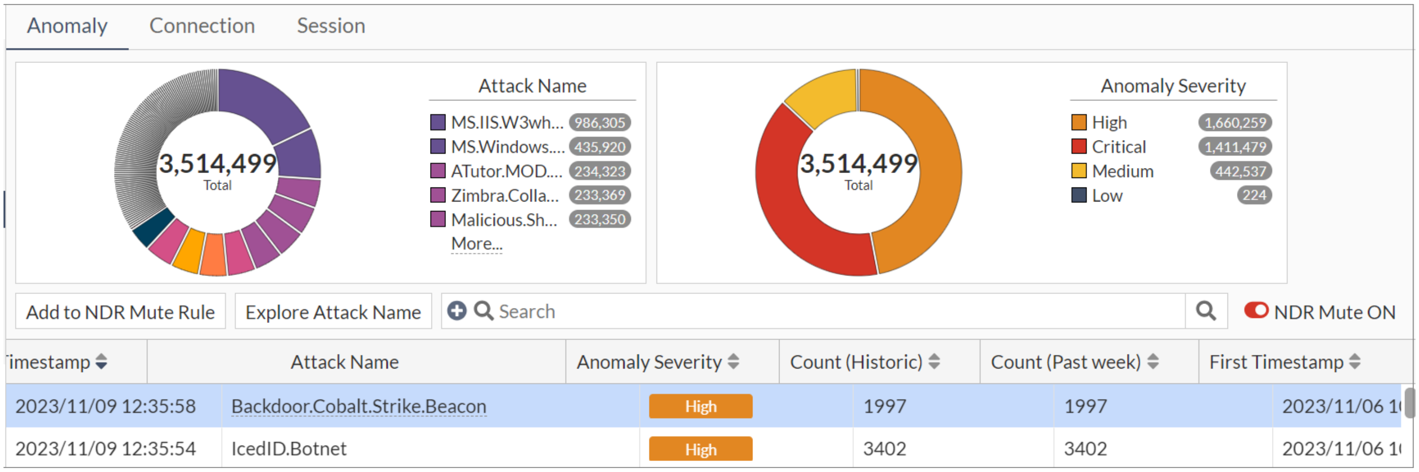
1. Go to *Network Insights* > *ML Discovery* > *Anomaly* tab.
2. Double-click an entry in the table. The *Anomaly Information* pane opens.
3. Click the *ML Baseline* tab.



Severity	Low
Latest Occurrence	10.1.12.130 -> 10.1.1.107 (2024/04/30 10:17:34)
Connection Pair Count	176
Session Count (Historic)	248
Session Count (Past week)	248
Features	Transport Layer Protocol: TCP Application Layer Protocol: FTP Destination Port: 21

Anomaly tab

The *Anomaly* tab provides insight into the anomaly content detected by FortiNDR and its occurrences in the network. To learn more about the connections related to a specific anomaly, double-click a record in the list to open the *Anomaly Information* pane. This pane contains all the connection pairs if there are multiple combinations of source and destination.



imestamp	Attack Name	Anomaly Severity	Count (Historic)	Count (Past week)	First Timestamp
2023/11/09 12:35:58	Backdoor.Cobalt.Strike.Beacon	High	1997	1997	2023/11/06 1
2023/11/09 12:35:54	IcedID.Botnet	High	3402	3402	2023/11/06 1

By default the *Anomaly* tab displays the following information:

Column	Description
Latest Timestamp	The date the record was updated.
Attack Name	The attack name provided by FortiGuard. Hover over the name to view the *Impact*, *Product List* and *Recommended Action*. You can also use this column to explore the attack name and search FortiGuard.
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Timestamp	The timestamp for the first time the anomaly was detected.

To view the sessions for a selected condition:

1. In the *Anomaly* tab, double-click a record in the list. The *Anomaly Information* pane opens.
2. Click the *Analytic* tab.
3. Double-click a log in the list. The *Sessions Log for selected condition* pane opens. The connection pair information is displayed.

From the *Session Log* pane, you have the option of viewing the source and destination device and viewing the sessions. For more information, see Session tab on page 70.

Anomaly Information

The *Anomaly Information* pane contains two tabs: *General* and *Analytic*.

General tab

The *General* tab displays the following information:

General	• Anomaly Type • Severity • Reason
Additional Information	• HTTP Version • HTTP Response Code • HTTP Server Name • HTTP URL • Malicious Behavior
Last Anomaly Occurrence	• Latest Occurrence • Count(Past Week) • Count(Historic) • Latest Source IP • Latest Source Port • Latest Source MAC • Latest Source Packet Size • Latest Source Country • Latest Source Device Model • Latest Source OS • Latest Source Device Category • Latest Source Device Sub Category • Latest Destination IP • Latest Destination Port • Latest Destination MAC • Latest Destination Packet Size • Latest Destination Country • Latest Destination Device Model • Latest Destination OS • Latest Destination Device Category • Latest Destination Device Sub Category

Analytic tab

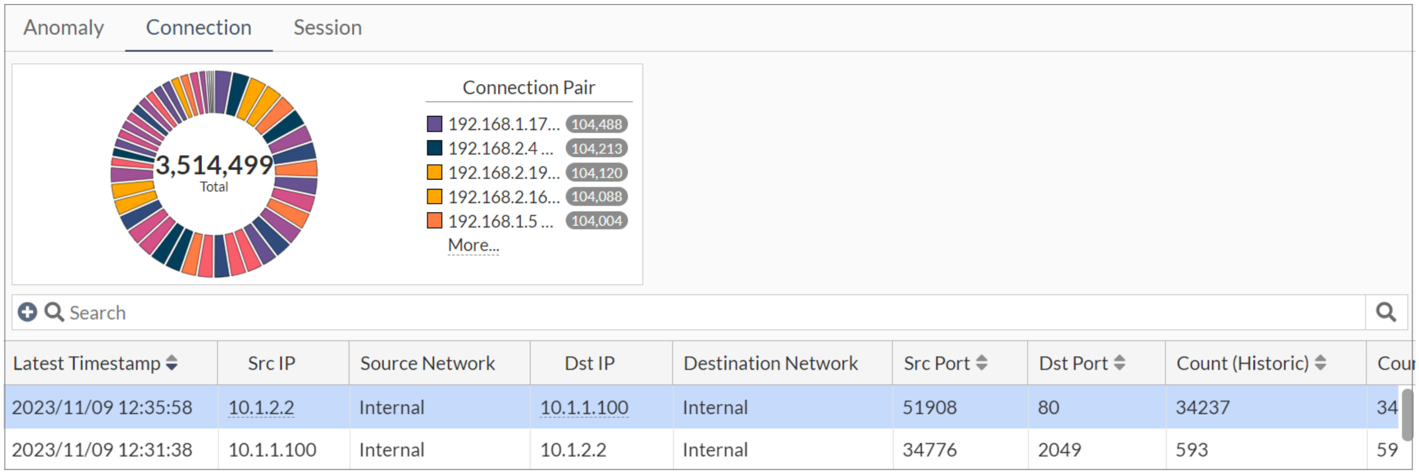
The *Analytic* tab displays the following information about he the connection pair:

Src IP	The source IP. Hover over the record to view the view the *IP Address*, *Country* and *Related Service*.

Source Network	The source network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Dst Ip	The destination IP. Hover over the record to view the view the *IP Address*, *Country* and *Related Service*.
Destination Network	The destination network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .

Connection tab

The *Connection* tab lists all the connection pairs for the anomaly type (such as *Network Attacks* and *Encrypted Attack*). Double-click an entry to explore the anomaly content for anomalies that have occurred within the same connection pair.



Latest Timestamp	Src IP	Source Network	Dst IP	Destination Network	Src Port	Dst Port	Count (Historic)	Cou
2023/11/09 12:35:58	10.1.2.2	Internal	10.1.1.100	Internal	51908	80	34237	34
2023/11/09 12:31:38	10.1.1.100	Internal	10.1.2.2	Internal	34776	2049	593	59

By default, the *Connection* tab displays the following information:

Column	Definition
Latest Timestamp	The date the record was updated.
Src IP	The source IP.
Source Network	The source network.

Column	Definition
	You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Dst IP	The destination IP.
Destination Network	The destination network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Src Port	The source port.
Dst Port	The destination port.
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Event Timestamp	The timestamp for the first time the anomaly event was detected.

To view the sessions for a selected condition:

1. In the *Anomaly* tab, double-click a record in the list. The *Anomaly Information* pane opens.
2. Click the *Analytic* tab.
3. Double-click a log in the list. The *Sessions Log for selected condition* pane opens. the connection pair information is displayed.

From the *Session Log* pane, you have the option of viewing the source and destination device and viewing the sessions. For more information, see Session tab on page 70.

Session Information

The *Session Information* pane contains two tabs: *General* and *Analytic*.

General tab

The *General* tab displays the following information:

General	• Session ID • Start Time • End Time • Traffic Volume • VLAN ID • Port ID

Anomaly	• Anomaly Type • Severity • Reason
Additional Information	• HTTP Version • HTTP Response Code • HTTP Server Name • HTTP URL • Malicious Behavior
Source Device	• Source IP • Source Port • Source MAC • Source Packet Size • Source Country • Source Device Model • Source OS • Source Device Category • Source Device Sub Category
Destination Device	• Destination IP • Destination Port • Destination MAC • Destination Packet Size • Destination Country • Destination Device Model • Destination OS • Destination Device Category • Destination Device Sub Category

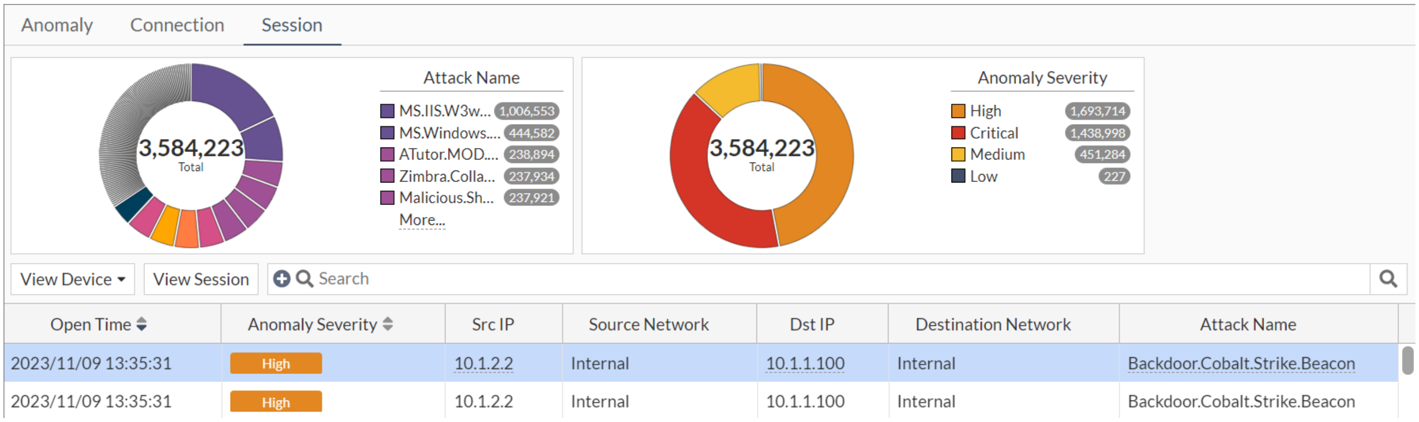
Analytic tab

By default, he *Analytic* tab displays the following information about he the connection pair:

Column	Definition
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Attack Name	The attack name provided by FortiGuard. Hover over the name to view the *Impact*, *Product List* and *Recommended Action*. You can also use this column to explore the attack name and search FortiGuard.
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .

Session tab

The *Session* tab lists all the sessions related to the same anomaly type (such as *Network Attacks* and *Encrypted Attack*). Each row is an anomaly event. Sessions with multiple anomaly events under the same anomaly type will have multiples rows with the same session ID.



Open Time	Anomaly Severity	Src IP	Source Network	Dst IP	Destination Network	Attack Name
2023/11/09 13:35:31	High	10.1.2.2	Internal	10.1.1.100	Internal	Backdoor.Cobalt.Strike.Beacon
2023/11/09 13:35:31	High	10.1.2.2	Internal	10.1.1.100	Internal	Backdoor.Cobalt.Strike.Beacon

By default, the *Session* tab displays the following information:

Column	Description
Open Time	The date and time the session started.
Anomaly Severity	The anomaly severity (*Not Anomaly*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Src IP	The source IP.
Source Network	The source network. You can use this column to filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Dst IP	The destination IP.
Destination Network	Filter IP addresses based on the category of the IP, such as *Internal*, *External* (public addresses), *Broadcast*, *Multicast address*, *Loopback*, *Reserved Address* and *Link-local Address*. You can filter for both IPv4 and IPv6 Addresses.
Attack Name	The attack name provided by FortiGuard. Hover over the name to view the *Impact*, *Product List* and *Recommended Action*. You can also use this column to explore the attack name and search FortiGuard.

Session Information

Double-click a sessions in the list to view the *Session Information* page. The following information is displayed:

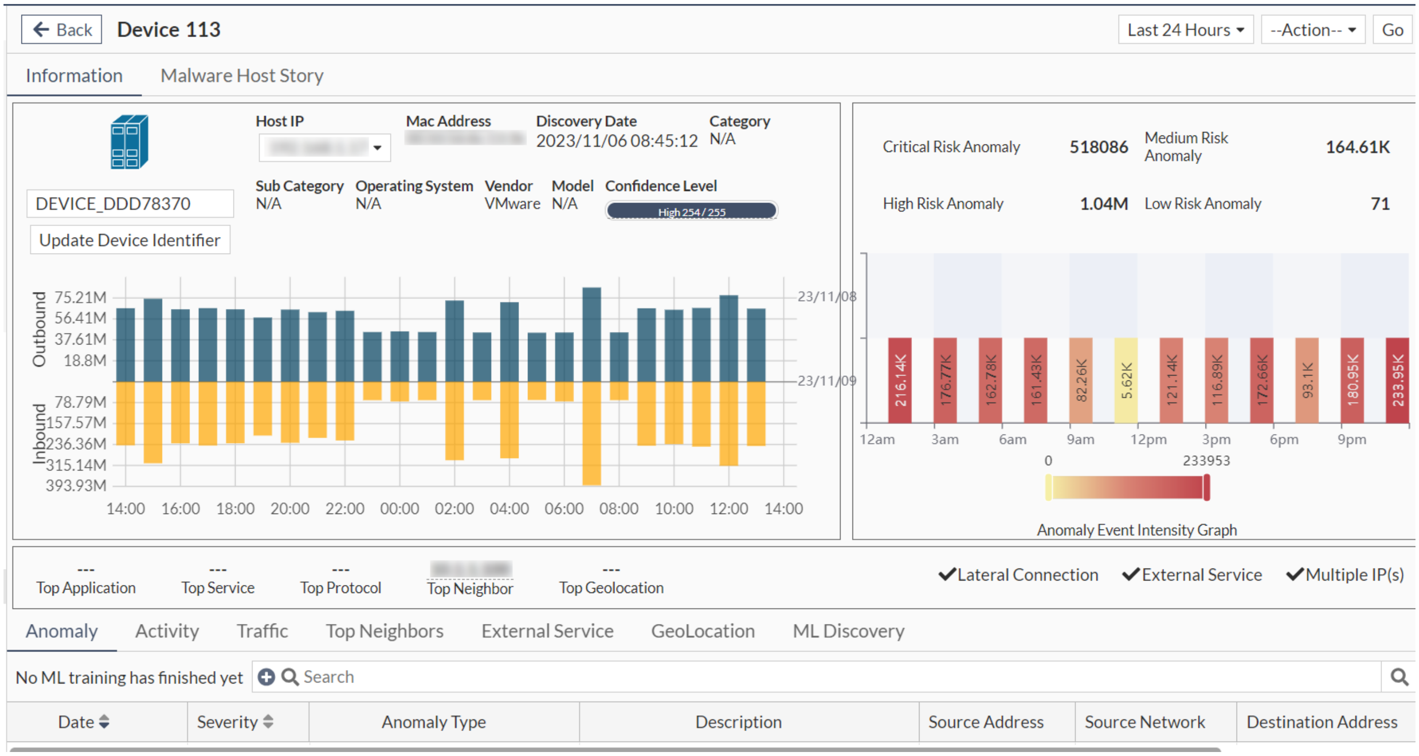
General	• Session ID • Start Time • End Time • Traffic Volume • VLAN ID • Port ID
Anomaly	• Anomaly Type • Severity • Reason
Additional Information	• HTTP Version • HTTP Response Code • HTTP Server Name • HTTP URL • Malicious Behavior
Source Device	• Source IP • Source Port • Source MAC • Source Packet Size • Source Country • Source Device Model • Source OS • Source Device Category • Source Device Sub Category
Destination Device	• Destination IP • Destination Port • Destination MAC • Destination Packet Size • Destination Country • Destination Device Model • Destination OS • Destination Device Category • Destination Device Sub Category

View source and destination devices

You can view the source and destination device from the *View Device* dropdown in the *Session* tab. The *Session* tab is available in all the *Network Insights* monitors except for *Device History.*

To view the source and destination devices:

1. In the Session tab, select a record in the table.
2. Click *View Device* > *View Source Device*, or *View Destination Device*. The *Information* and *Malware Host Story* tabs are displayed.



Device 113

Host IP: [redacted]
Mac Address: [redacted]
Discovery Date: 2023/11/06 08:45:12
Category: N/A
DEVICE_DDD78370
Sub Category: N/A
Operating System: N/A
Vendor: VMware
Model: N/A
Confidence Level: High 254 / 255

Critical Risk Anomaly	518086	Medium Risk Anomaly	164.61K
High Risk Anomaly	1.04M	Low Risk Anomaly	71

Top Application	Top Service	Top Protocol	Top Neighbor	Top Geolocation
---	---	---	[redacted]	---

✓Lateral Connection ✓External Service ✓Multiple IP(s)

No ML training has finished yet

Date	Severity	Anomaly Type	Description	Source Address	Source Network	Destination Address

View sessions

To view the session page:

- Select a record in the *Session* tab and click *View Session*. The Session page opens.

You can use the right-side navigation to move up and down the page.

The *Session* page contains the following information:

Anomaly

Activity
Web Client
Application
HTTP.BROWSER
Vendor
Other

High Anomaly

Session Information

Session Information

Timestamp	2023/11/10 13:16:04
Transport Layer Protocol	TCP
Application Layer Protocol	HTTP
Volume	415.57K (415565 bytes)
VLAN ID	N/A
Sniffer Source Port	port2 (SNIFFER)
Technology	Browser-Based
Cloud Service	None

Device Information

Device Information

Internal

Device Type	N/A
Devie Model	N/A
MAC Address	5a:01:0a:03:0a:39
Vendor	N/A
OS	N/A
Category	N/A
Sub Category	N/A
IP	10.3.10.57
Port	51255
Packet Size	117

↔

Internal

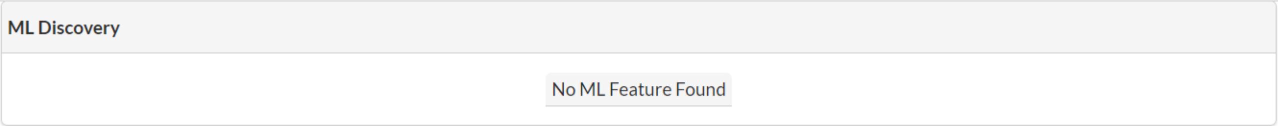
Device Type	N/A
Device Model	N/A
MAC Address	5a:01:0a:03:00:02
Vendor	N/A
OS	N/A
Category	N/A
Sub Category	N/A
IP	10.3.0.2
Port	80
Packet Size	415448

Activity

Activity

2 minutes ago	Connected to 10.3.0.2/9b30e4de385251284139f576c2e3635f via HTTP

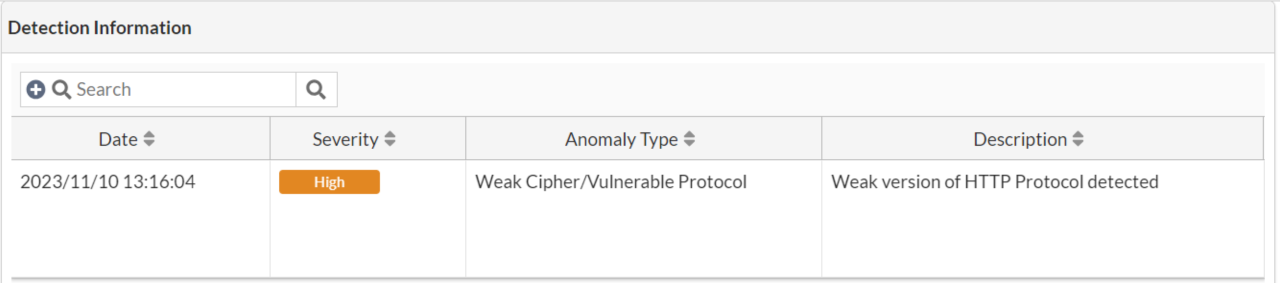
ML Discovery



ML Discovery

No ML Feature Found

Detection Information

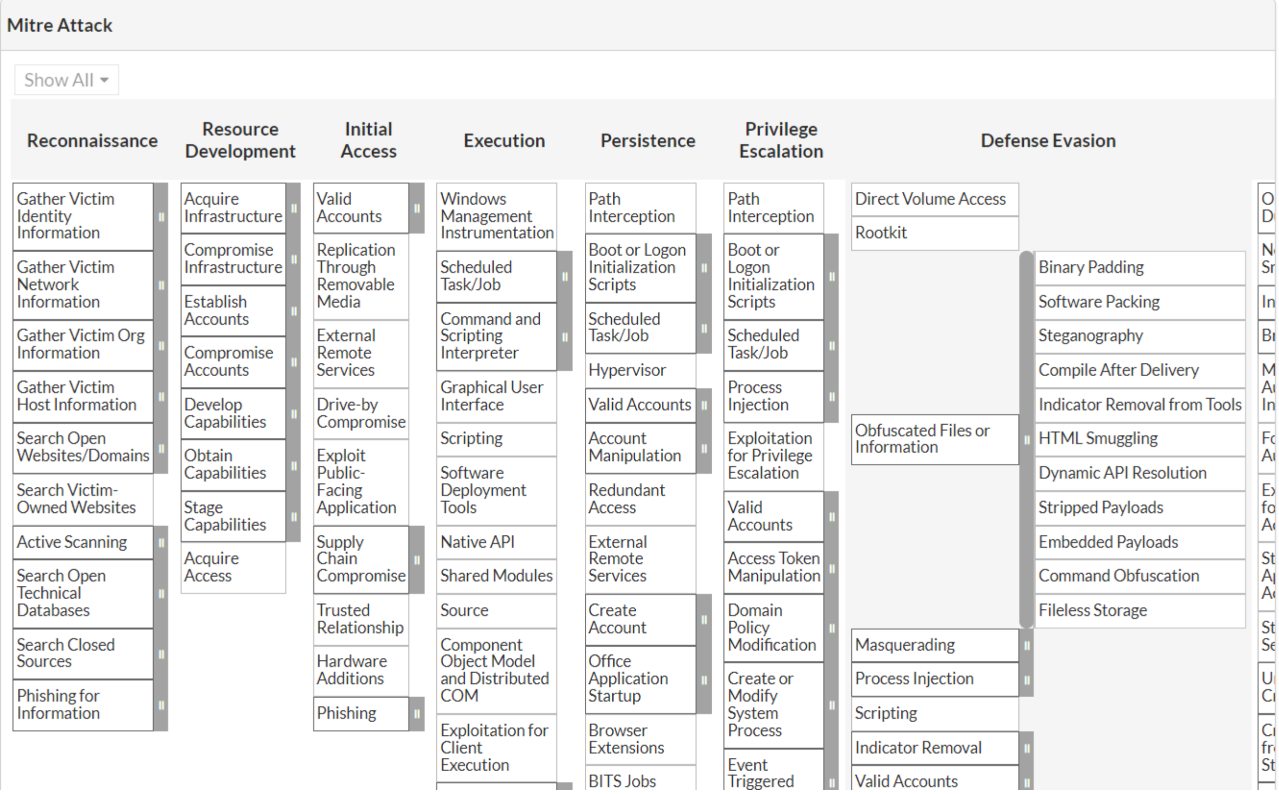


Detection Information

Date	Severity	Anomaly Type	Description
2023/11/10 13:16:04	High	Weak Cipher/Vulnerable Protocol	Weak version of HTTP Protocol detected

Mitre Attack

The *Mitre Attack* widget tracks the number of events that occurred for each MITRE attack tactics category. For more information, see MITRE ATT&CK on page 58.



Mitre Attack

Reconnaissance
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Gather Victim Host Information
- Search Open Websites/Domains
- Search Victim-Owned Websites
- Active Scanning
- Search Open Technical Databases
- Search Closed Sources
- Phishing for Information

Resource Development
- Acquire Infrastructure
- Compromise Infrastructure
- Establish Accounts
- Compromise Accounts
- Develop Capabilities
- Obtain Capabilities
- Stage Capabilities
- Acquire Access

Initial Access
- Valid Accounts
- Replication Through Removable Media
- External Remote Services
- Drive-by Compromise
- Exploit Public-Facing Application
- Supply Chain Compromise
- Trusted Relationship
- Hardware Additions
- Phishing

Execution
- Windows Management Instrumentation
- Scheduled Task/Job
- Command and Scripting Interpreter
- Graphical User Interface
- Scripting
- Software Deployment Tools
- Native API
- Shared Modules
- Source
- Component Object Model and Distributed COM
- Exploitation for Client Execution

Persistence
- Path Interception
- Boot or Logon Initialization Scripts
- Scheduled Task/Job
- Hypervisor
- Valid Accounts
- Account Manipulation
- Redundant Access
- External Remote Services
- Create Account
- Office Application Startup
- Browser Extensions
- BITS Jobs

Privilege Escalation
- Path Interception
- Boot or Logon Initialization Scripts
- Scheduled Task/Job
- Process Injection
- Exploitation for Privilege Escalation
- Valid Accounts
- Access Token Manipulation
- Domain Policy Modification
- Create or Modify System Process
- Event Triggered

Defense Evasion
- Direct Volume Access
- Rootkit
- Obfuscated Files or Information
  - Binary Padding
  - Software Packing
  - Steganography
  - Compile After Delivery
  - Indicator Removal from Tools
  - HTML Smuggling
  - Dynamic API Resolution
  - Stripped Payloads
  - Embedded Payloads
  - Command Obfuscation
  - Fileless Storage
- Masquerading
- Process Injection
- Scripting
- Indicator Removal
- Valid Accounts

- O D
- N Sr
- In
- Br
- M Ai In
- Fc Ai
- Ex fo Ai
- St Ai Ai
- St Se
- U Ci
- Ci fr St

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 *FortiGate* tab displays the FortiGates sending files via OFTP (FortiSandbox field with TCP port 514) and via HTTPs (FOS 7.0.1 and higher). FortiNDR must authorize connections from FortiGate for OFTP and for inline blocking. Connect FortiNDR to the FortiGate Security Fabric to authorize the device via the Security Fabric protocol.
Other Device tab	The *Other Device* 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.

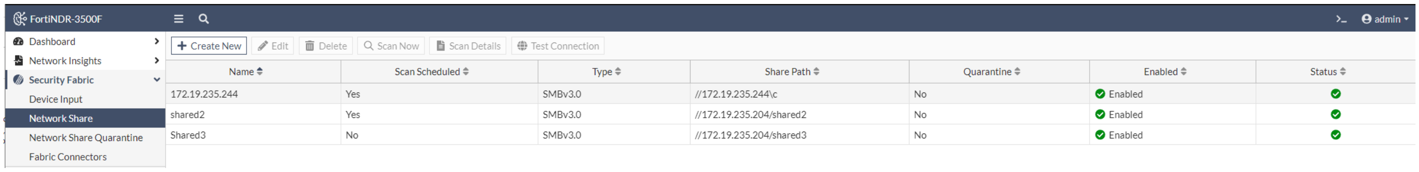
Network Share

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

To create a Network Share profile:

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

Status	*Enable* or *Disable*. *Enable* is the default.
Mount Type	Select a Network Share protocol from the list. The following protocols are supported: • SMBv1.0 • SMBv2.0 • SMBv2.1 • SMBv3.0 • NFSv2.0 • NFSv3.0 • NFS v4.0
Network Share Name	Enter a name for the Network Share.

Server IP	Enter the IP address for the Network Share.
Share Path	Enter the path for the Network Share.
Username	Enter the username for the Network Share.
Password	Enter the password for the Network Share and then confirm the password.

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

Enable Quarantine Password Protected Files	Moves password protected files to a designated quarantine location. FortiNDR does not process password protected files.
Enable Quarantine Critical Risk Files	Moves detected files with critical risk to a designated quarantine location. This includes: • Fileless • Industroyer • Ransomware • Wiper • Worm
Enable Quarantine - High Risk Files	Moves detected files with high risk to a designated quarantine location. This includes: • Backdoor • Banking Trojan • Exploit • Infostealer • Proxy • PWS • Rootkit • Trojan
Enable Quarantine - Medium Risk Files	Moves detected files with medium risk to a designated quarantine location. This includes: • Clicker • DDoS • Downloader • Dropper • Phishing • Redirector • Virus

Enable Quarantine - Low Risk Files	Moves detected files with low risk to a designated quarantine location. This includes: • Application • CoinMiner • Generic Attack • Generic Trojan • SEP • WebShell
Enable Quarantine of Others	Moves other unprocessed files to a designated quarantine location. File types that falls under this category includes: • Files with unsupported file type • Files with Over size Limit • Empty/Irregular files
Enable Copying or Moving clean files to sanitized location	Moves or copies clean files to a location specified in the *Network Share Quarantine* profile. See, Network Share Quarantine on page 81. The *Moving* operation is only allowed for the quarantine location when *Keep Original File at Source Location* disabled. The *Copying* operation is only allowed for the quarantine location when *Keep Original File at Source Location* enabled. For information about combing Network Share and Quarantine profiles, see *Network Share Quarantine on page 81 > Combining network share and quarantine profiles*.
Create a copy of clean files for every scheduled scan at the sanitized location	When enabled, FortiNDR will create a new folder <*Network Share Profile Name*>_<*Scan Task ID*> in the sanitized location for each scheduled scan. When disabled, FortiNDR will overwrite the sanitized location with the clean files from the latest scan. Enabling this option will increase the size of the Network Share location.
Create placeholder files for malicious/Suspicious/Other files at sanitized location	Adds a placeholder file in the sanitized location. The filename pattern of the placeholder file will be <*filename*>.<*severity*>*.txt*. This helps maintain the file structure of the original network in the share folder.
Enable Force Rescan	When enabled, FortiNDR will not use cache detection even if the files are previously scanned.

6. Click *OK*.

Testing connectivity

To validate the Network Share configuration:

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

Testing the connection will work when Network File Share is enabled. The test will fail if 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 correspodning time interval.
5. Click *OK*.

Viewing scan results

View the scan history of the Network Share directories.

To view the scan results:

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

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 *Detected/Quarantined* critical risk files.
High Risk	The number of *Detected/Quarantined* critical high files.
Medium Risk	The number of *Detected/Quarantined* medium risk files.
Low Risk	The number of *Detected/Quarantined* critical low files.
Clean	The number of clean files.
Others	The number of *Detected/Quarantined*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.

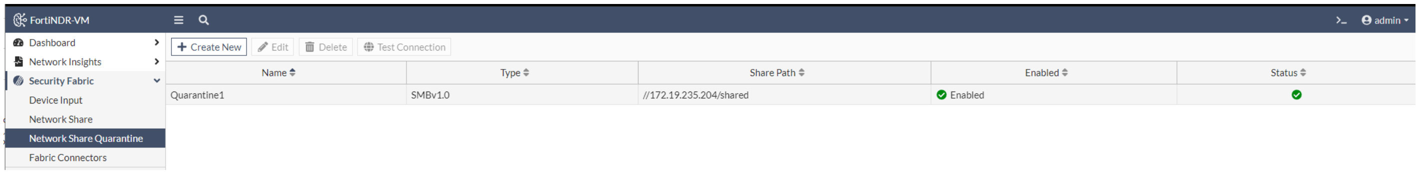
Scanning Zip files

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.



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

Quarantined files

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

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

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

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

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

Example:

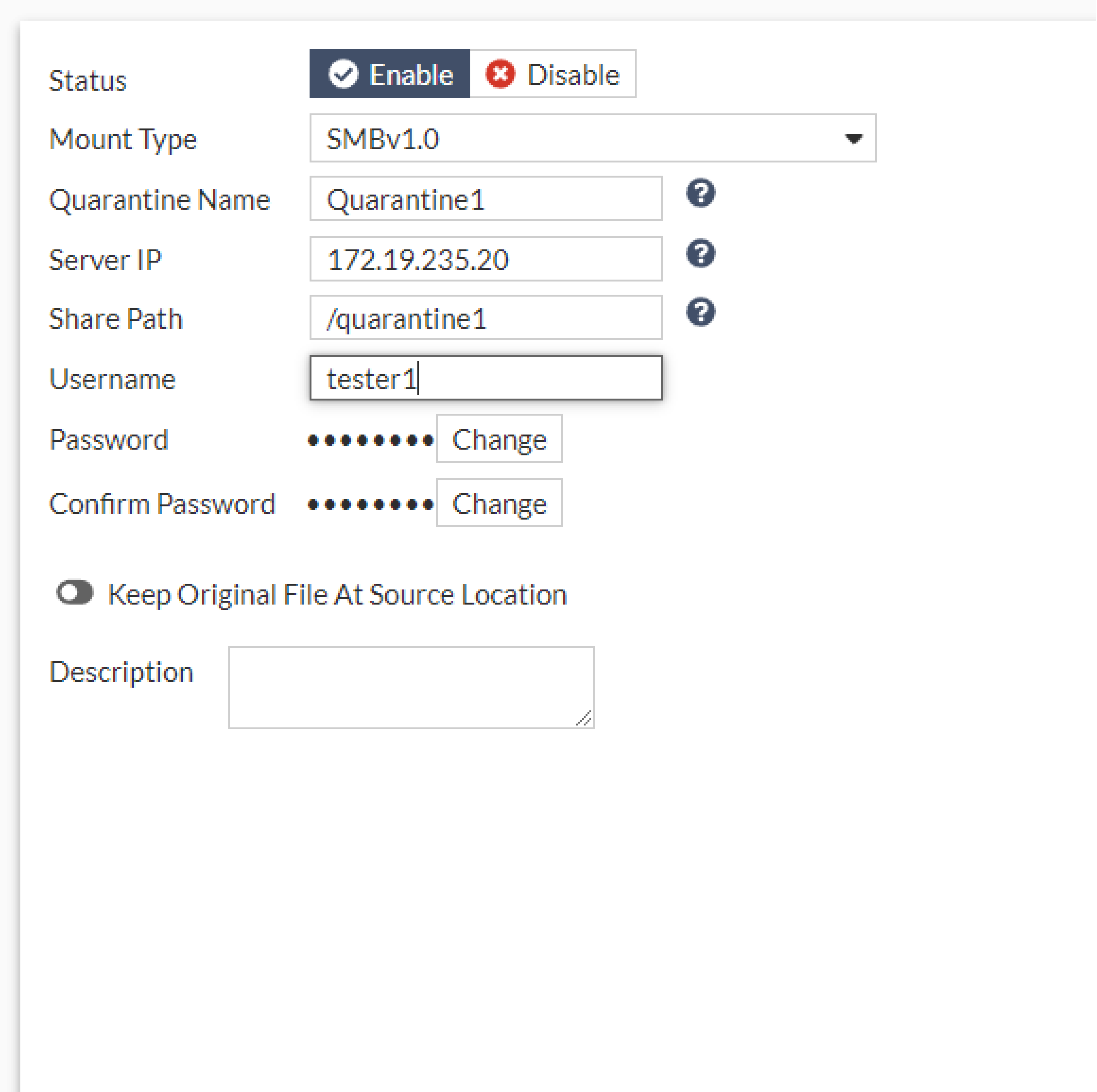
```
Network Share FileID: 351640
SID: 3 (Share ID)
JID: 44 (Job ID)
FileID: 1198941 (File ID)
File Name: sample.vsc
Device: testshared
URL: //172.16.2.100/shared2/2/sample.vsc
MD5: 31e06f25de8b5623c3fdaba93ed2edde
Virus Name: W32/Wanna.A!tr.ransom
DelOriginalFile: Success
```

Creating a quarantine profile

To create a quarantine profile:

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

Status	Click to *Enable* or *Disable*.
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

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

> Enabling *Keep Original File At Source Location* may affect the behavior of your Network Share profile. For information, see Combining network share and quarantine profiles on page 83.

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

Combining network share and quarantine profiles

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

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

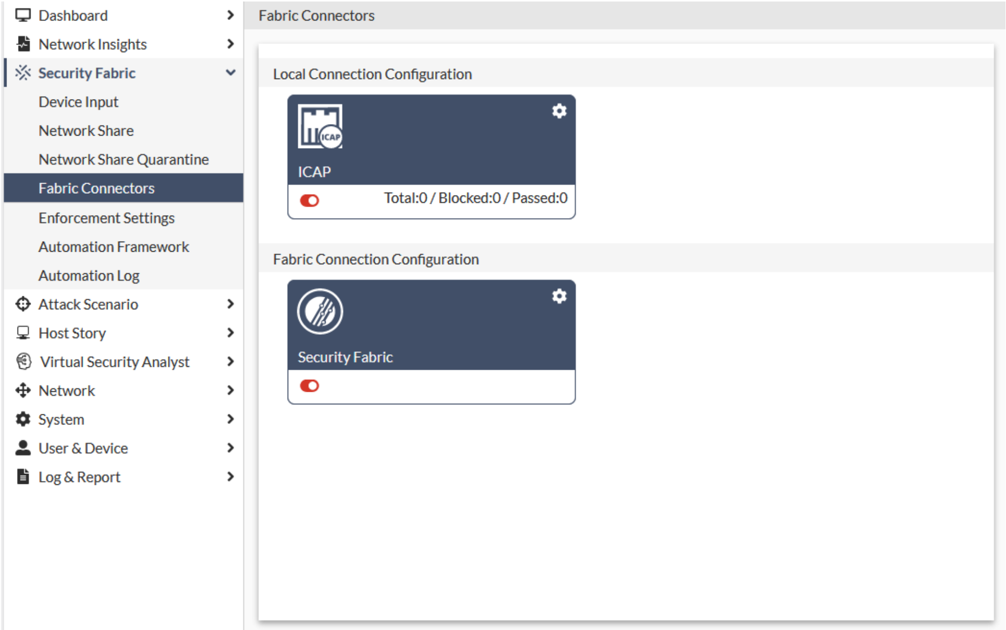
You can use the Network Share Quarantine location for both the quarantine of malicious files as well the Move/Copy of clean files. However, we recommend creating different folders for clean and malicious files.

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

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

Fabric Connectors

*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 sumbmissions per second, we recommend using the *Inline Blocking* feature in FortiGate to do the sample submitting instead.

To integrate FortiNDR with FortiGate ICAP:

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

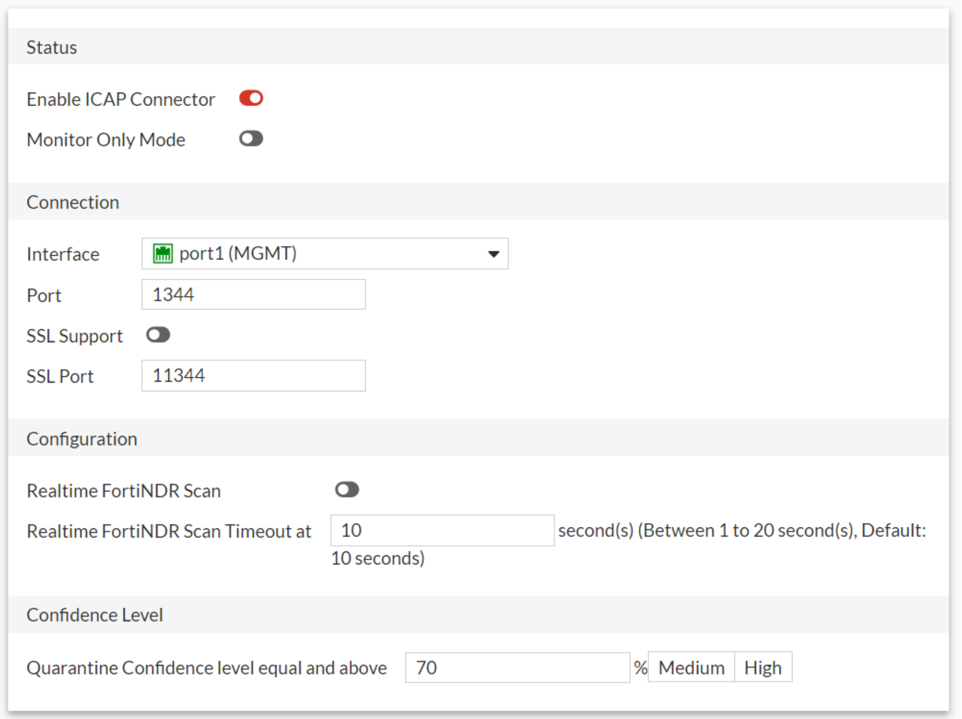
For more information, see ICAP in the *FortiOS Administration Guide*.

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. Configure the ICAP settings and click *OK*.

Status	
Enable ICAP Connector	Click to enable the ICAP connector.
Monitor Only Mode	When enabled, FortiNDR will only log the detection, no block action will be performed. Youcannot enable realtime FortiNDR scan configuration and change the confidence level.
Connection	
Interface	Select an interface from the dropdown.
Port	Enter the port the the connector will use to connec to FortiNDR. Default is 1344. **Note**: Avoid choosing the Sniffer port as the ICAP interface.
SSL Support	Click to enable Secure Sockets Layer.
SSL Port	Enter the SSL port. Default is 11344.
Configuration	
Realtime FortiNDR Scan	When enabled, FortiNDRwill delay the response to the ICAP client until the scan result has been achieved or the timeout has been reached.
Realtime FortiNDR Scan Timeout at	Enter the number of seconds is realtime scan will timeout. Default is 10 seconds.
Confidence Level	
Quarantine Confidence level equal and above	Set the confidence level as a percentage and select *Medium* or *High*.



Status

Enable ICAP Connector ●

Monitor Only Mode ○

Connection

Interface port1 (MGMT)

Port 1344

SSL Support ○

SSL Port 11344

Configuration

Realtime FortiNDR Scan ○

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

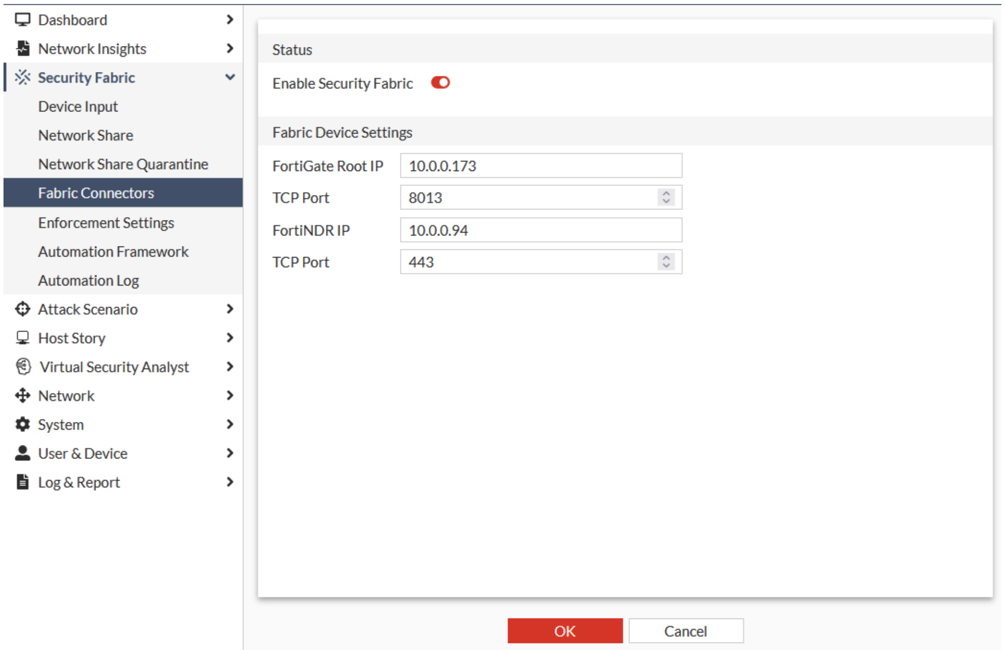
FortiNDR 1.5.0 and FortiOS 7.0.0, FortiNDR can join FortiGate Security Fabric. After connecting to the Security Fabric, FortiNDR can share information such as FortiNDR system information and malware types detected.

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

To configure the Security Fabric connector:

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

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



Status

Enable Security Fabric ●

Fabric Device Settings

FortiGate Root IP	10.0.0.173
TCP Port	8013
FortiNDR IP	10.0.0.94
TCP Port	443

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 isenabled 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

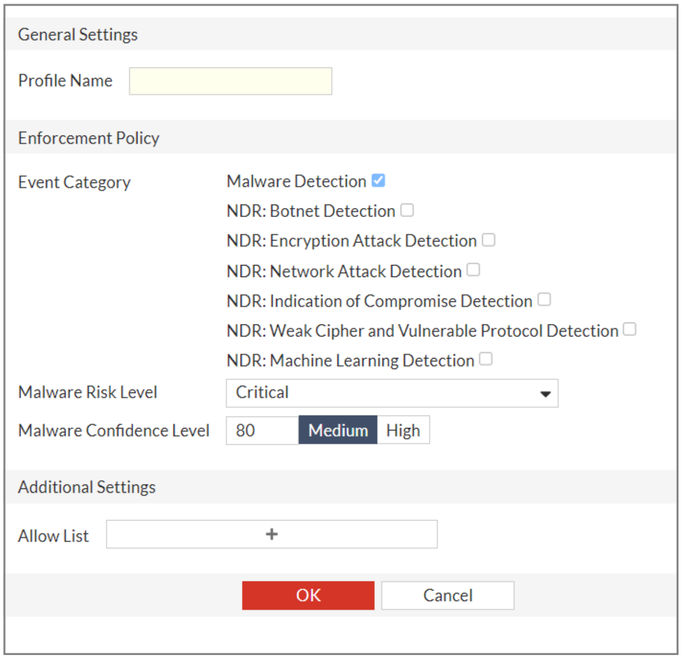
- A response is only triggered once when multiple events in NDR anomalies in the same category (e.g. IOC campaign) occurs within one minute.
- IA response is recorded as a duplicate when multiple events in NDR anomalies in the same category occur every minute after that.

To create an 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: • *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	Select *Critical*, *High*, *Medium* or *Low* severity from the dropdown.
Malware Confidence Level	Enter a numeric value for the confidence level and click either *Medium* or *High*.
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

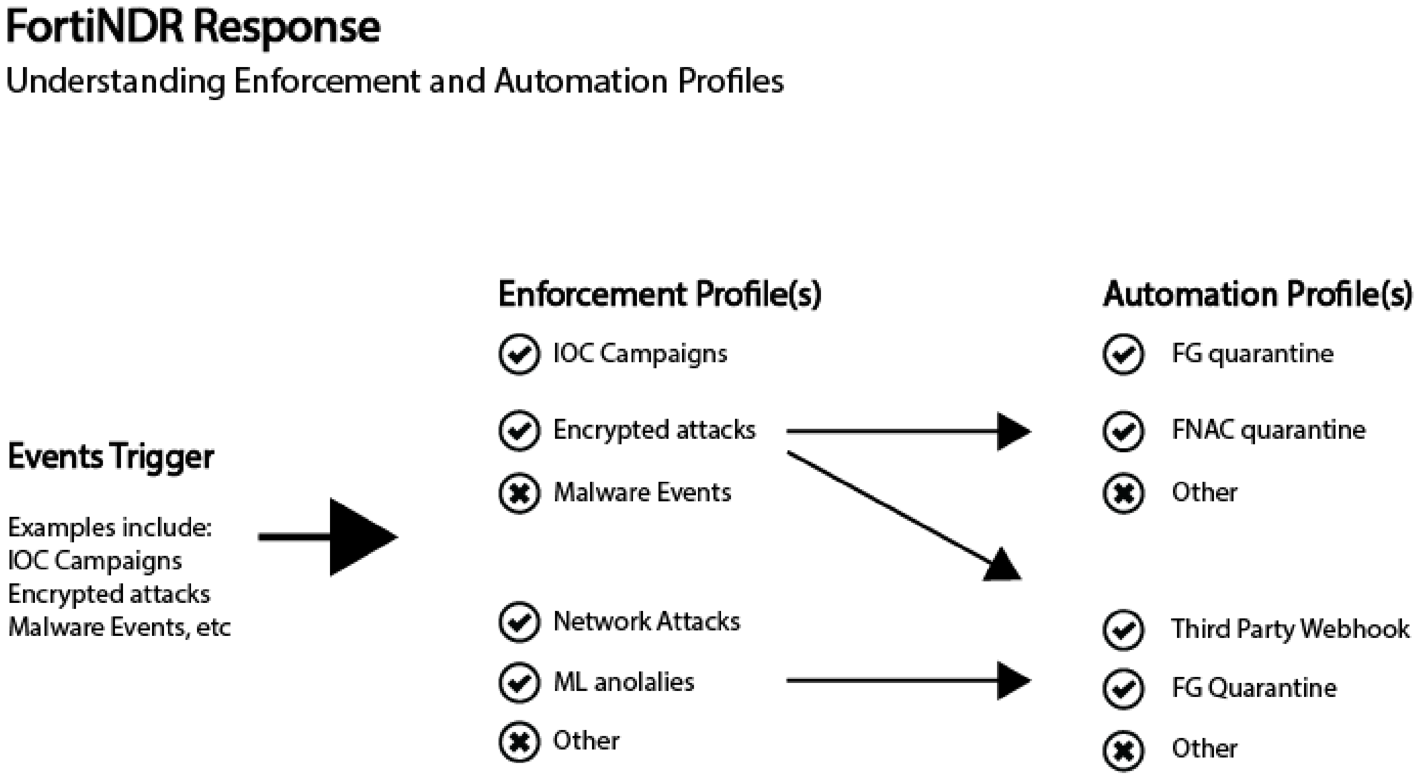
Additional Settings

Allow List +

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

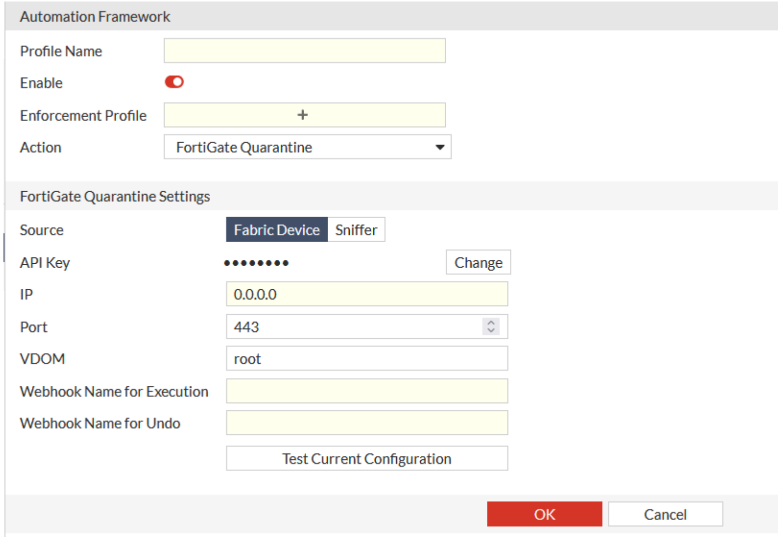
Go to *Security Fabric > Automation Framework* to create single enforcement profile that can be selected with different automation profiles. This provides you with more flexibility in the response action. The following diagram illustrates the relationship between Enforcement and Automation profiles.



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: • *FortiGate Quarantine* • *FortiNAC Quarantine* • *FortiSwitch Quarantine via FortiLink* • *Generic Webhook*



Automation Framework

Profile Name

Enable

Enforcement Profile +

Action: FortiGate Quarantine

FortiGate Quarantine Settings

Source: Fabric Device | Sniffer

API Key: •••••••• Change

IP: 0.0.0.0

Port: 443

VDOM: root

Webhook Name for Execution

Webhook Name for Undo

Test Current Configuration

OK Cancel

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 *POST*, *PUT*, *GET*, *PATCH* or *DELETE*.
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 *POST*, *PUT*, *GET*, *PATCH* or *DELETE*.
Header	Click the plus sign (+) and enter a value of the authorization key.
HTTP Body Template	Enter the HTTP Body Template.

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

FortiGate quarantine webhook setup example

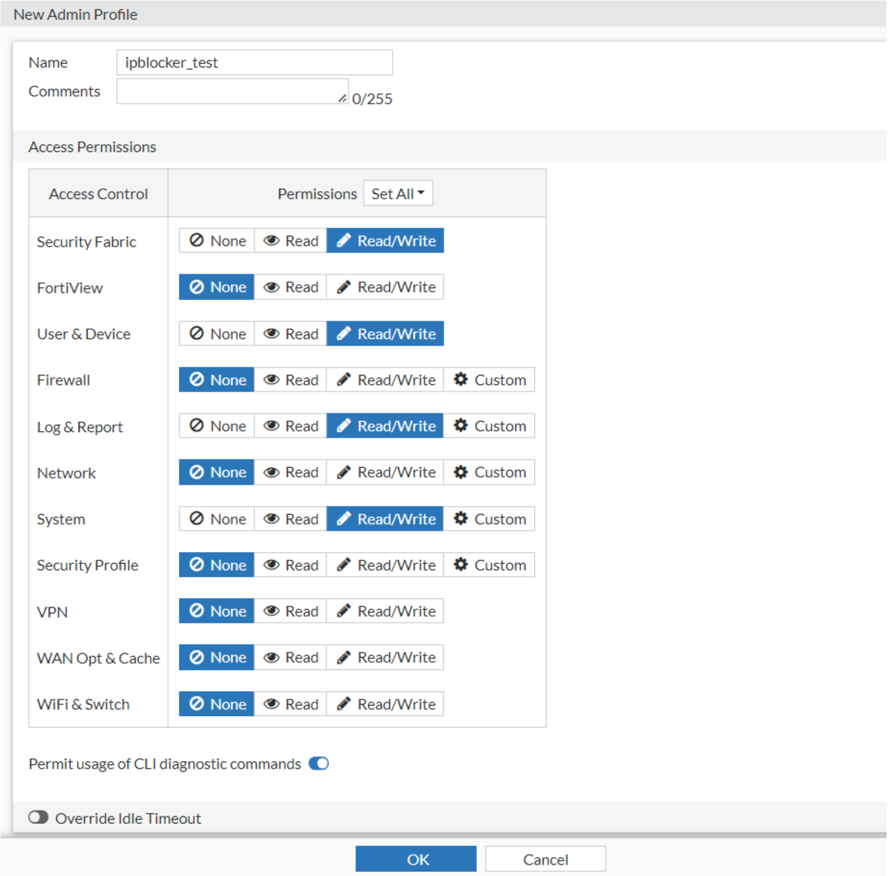
To create an automation profile for *FortiGate Quarantine* or *FortiSwitch Quarantine via FortiLink*, the incoming webhook needs to be setup on FortiGate to accept requests from FortiNDR. You can register them in *Security Fabric > Automation Framework*.

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:

1. 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: ipblocker_test

Comments: 0/255

Access Permissions

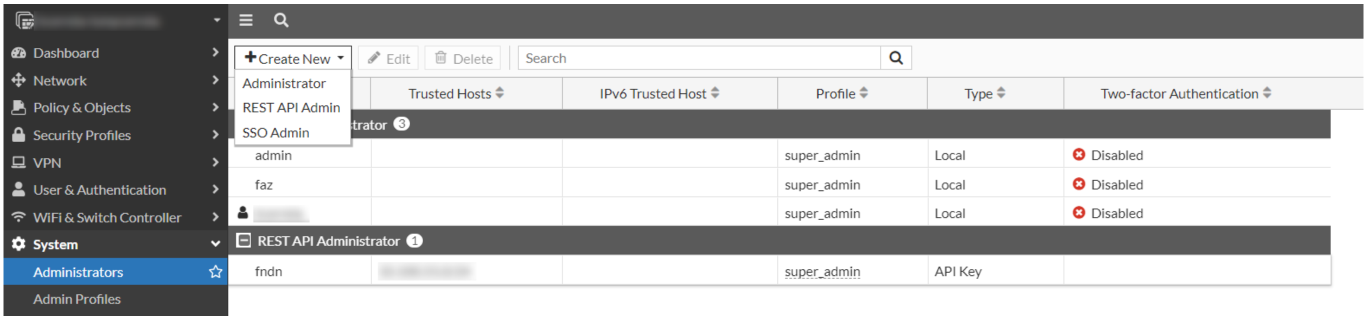
Access Control	None	Read	Read/Write	Custom
Security Fabric	○	○	●	
FortiView	●	○	○	
User & Device	○	○	●	
Firewall	●	○	○	○
Log & Report	○	○	●	○
Network	●	○	○	○
System	○	○	●	○
Security Profile	●	○	○	○
VPN	●	○	○	
WAN Opt & Cache	●	○	○	
WiFi & Switch	●	○	○	

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.

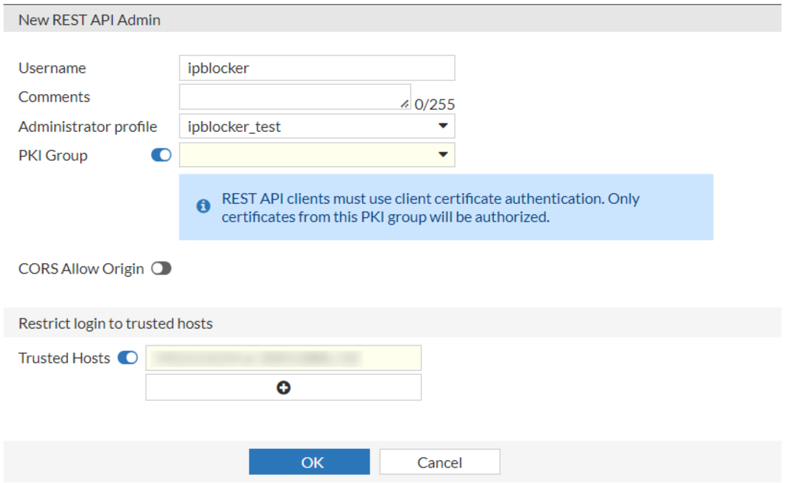


	Trusted Hosts	IPv6 Trusted Host	Profile	Type	Two-factor Authentication
trator 3					
admin			super_admin	Local	Disabled
faz			super_admin	Local	Disabled
[redacted]			super_admin	Local	Disabled
REST API Administrator 1					
fndn	[redacted]		super_admin	API Key	

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: ipblocker

Comments: 0/255

Administrator profile: ipblocker_test

PKI Group

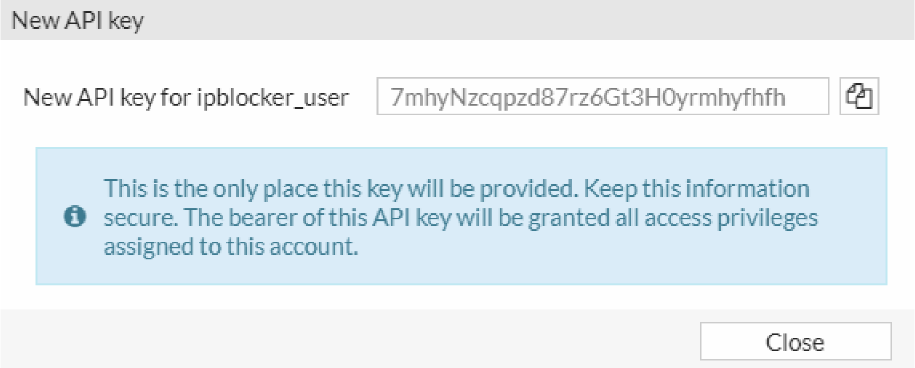
REST API clients must use client certificate authentication. Only certificates from this PKI group will be authorized.

CORS Allow Origin

Restrict login to trusted hosts

Trusted Hosts: [redacted]

4. Save the generated *New API key*. You will need this to register the automation profile in FortiNDR.



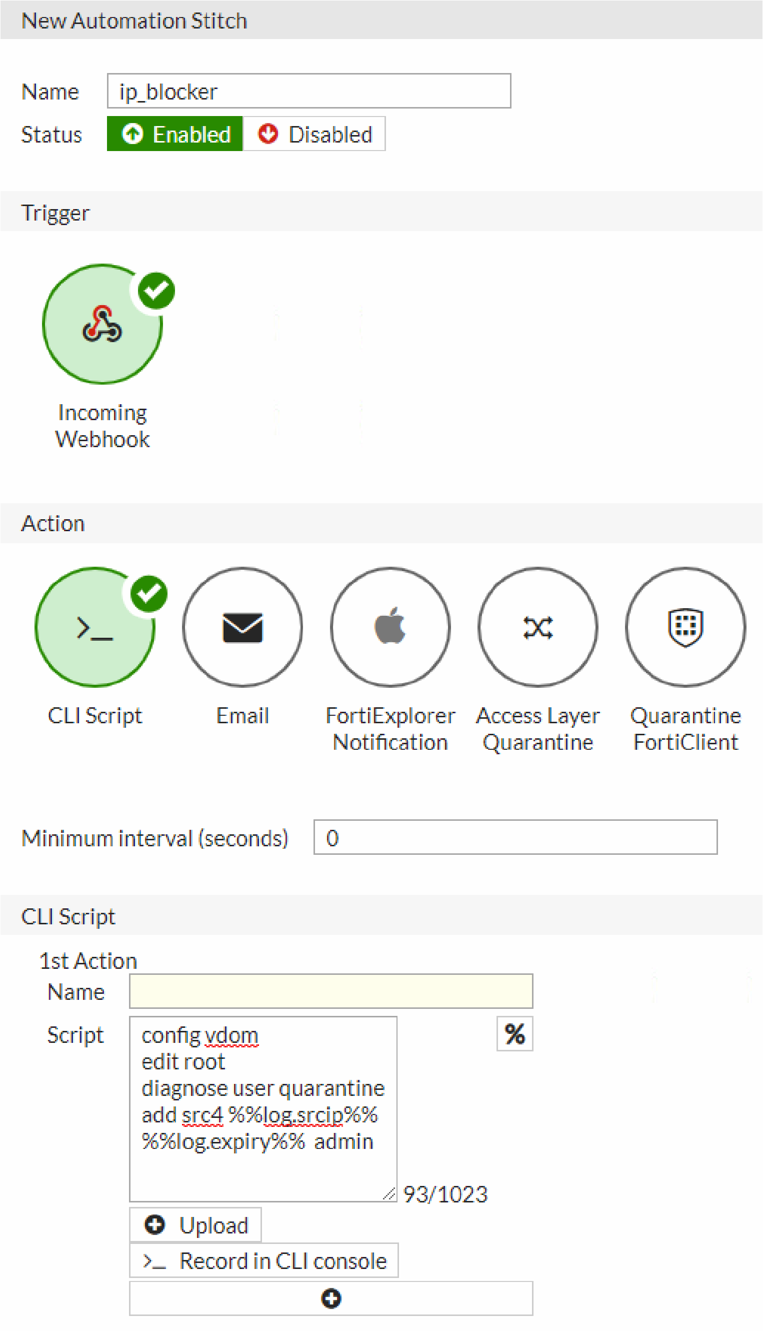
New API key

New API key for ipblocker_user: 7mhyNzcqpzd87rz6Gt3H0yrmhyfhfh

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.

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

```
config vdom
edit root
diagnose user banned-ip add src4 %%log.srcip%% %%log.expiry%% admin
```



New Automation Stitch

Name: ip_blocker

Status: Enabled

Trigger: Incoming Webhook

Action: CLI Script

Minimum interval (seconds): 0

CLI Script

1st Action

Name:

Script:

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

93/1023

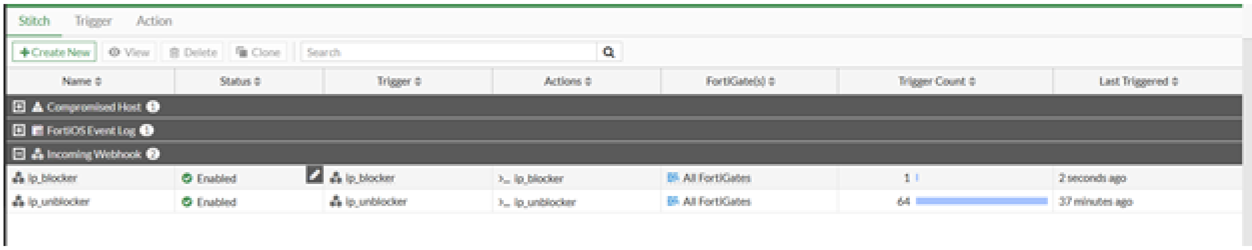
This example requires two webhooks, one that executes the Ban IP action (this *ip_blocker* example). Another webhook executes the unban IP action.

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

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

   ```
   config vdom
   edit root
   diagnose user banned-ip delete src4 %%log.srcip%%
   ```

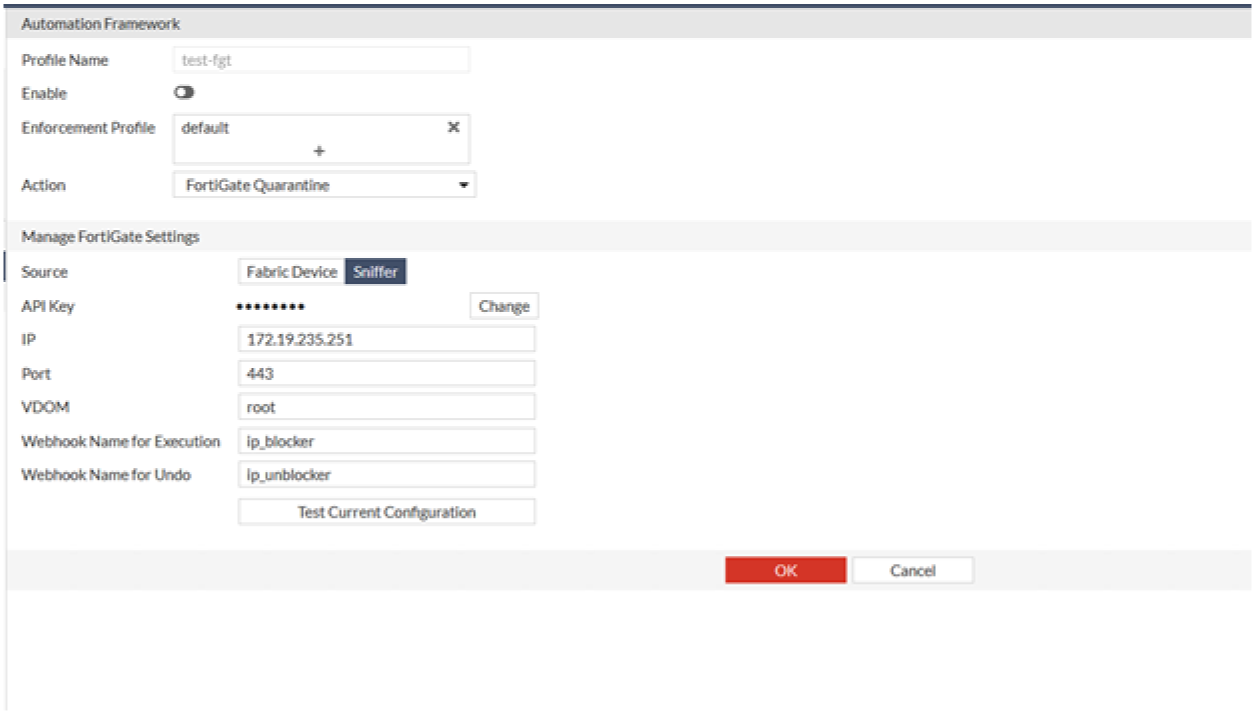
   FortiOS v7.0.1

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	test-fgt
Enable	
Enforcement Profile	default
Action	FortiGate Quarantine

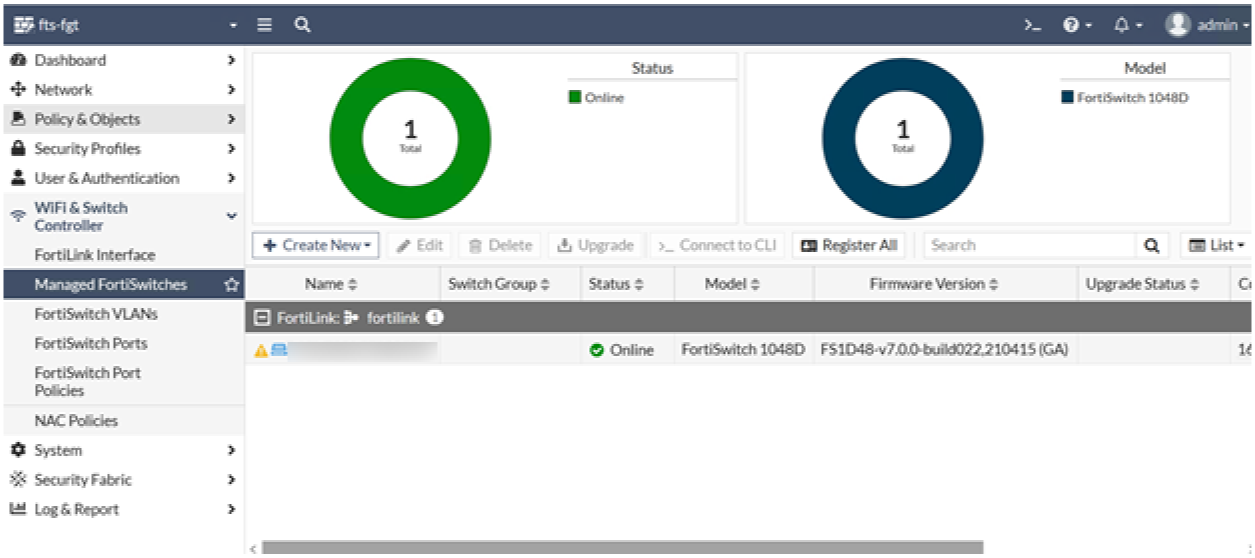
   Manage FortiGate Settings

Source	Fabric Device [✓ Sniffer]
API Key	••••••••
IP	172.19.235.251
Port	443
VDOM	root
Webhook Name for Execution	ip_blocker
Webhook Name for Undo	ip_unblocker

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.

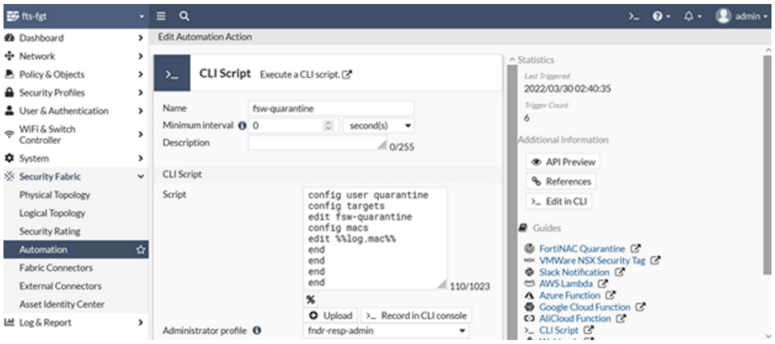
For information about configuring FortiLink, see Configuring FortiLink.



Name	Switch Group	Status	Model	Firmware Version	Upgrade Status
FortiLink: fortilink					
[redacted]		Online	FortiSwitch 1048D	FS1D48-v7.0.0-build022,210415 (GA)	

To setup FortiSwitch quarantine on FortiNDR:

1. Following the steps for creating a webhook on FortiGate in FortiGate quarantine webhook setup example on page 93. Note that the CLI script for quarantine and undo quarantine should be updated.



Edit Automation Action

CLI Script Execute a CLI script.

Name: fsw-quarantine
Minimum interval: 0 second(s)
Description: 0/255

CLI Script

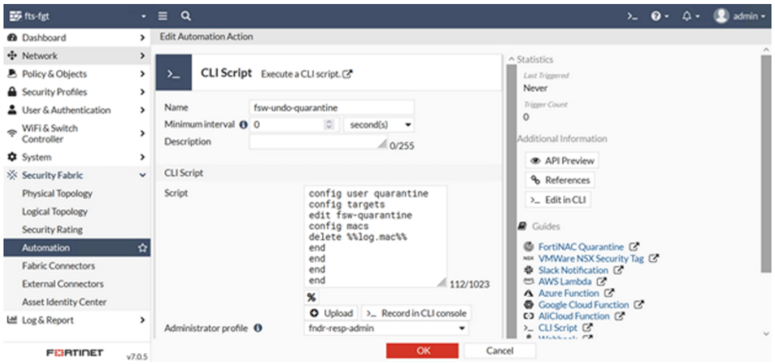
Script:

```
config user quarantine
config targets
edit fsw-quarantine
config macs
edit %%log.mac%%
end
end
end
end
```

110/1023

Administrator profile: fndr-resp-admin

Statistics: Last Triggered 2022/03/30 02:40:35; Trigger Count 6



Edit Automation Action

CLI Script Execute a CLI script.

Name: fsw-undo-quarantine
Minimum interval: 0 second(s)
Description: 0/255

CLI Script

Script:

```
config user quarantine
config targets
edit fsw-quarantine
config macs
delete %%log.mac%%
end
end
end
end
```

112/1023

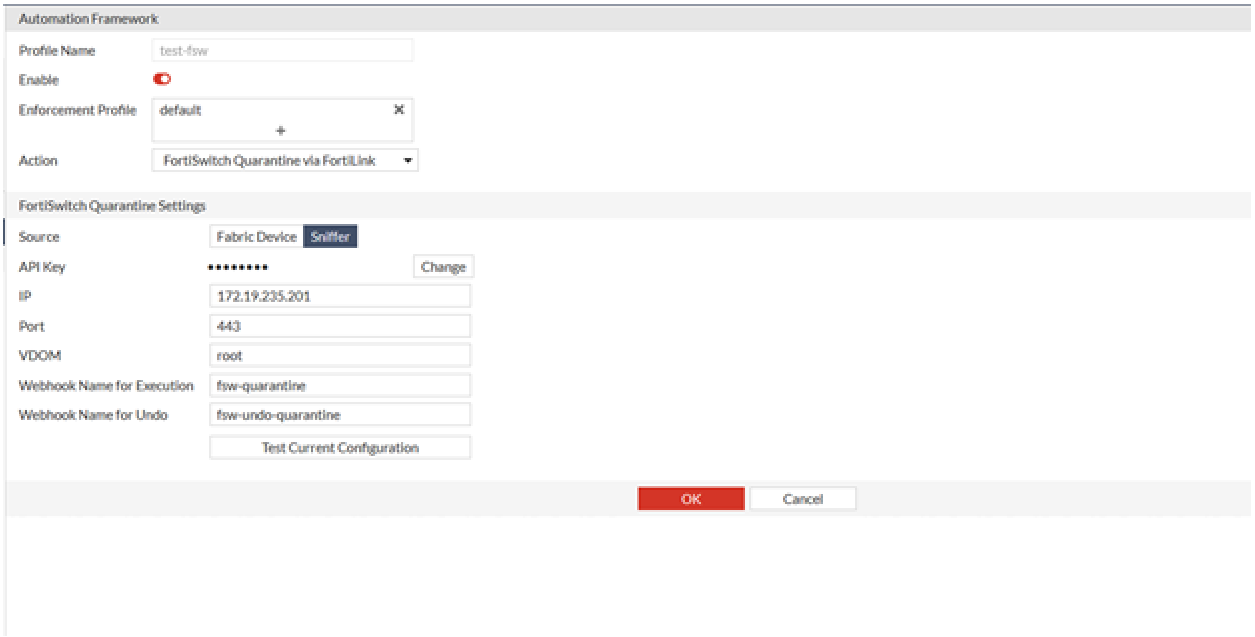
Administrator profile: fndr-resp-admin

Statistics: Last Triggered Never; Trigger Count 0

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.



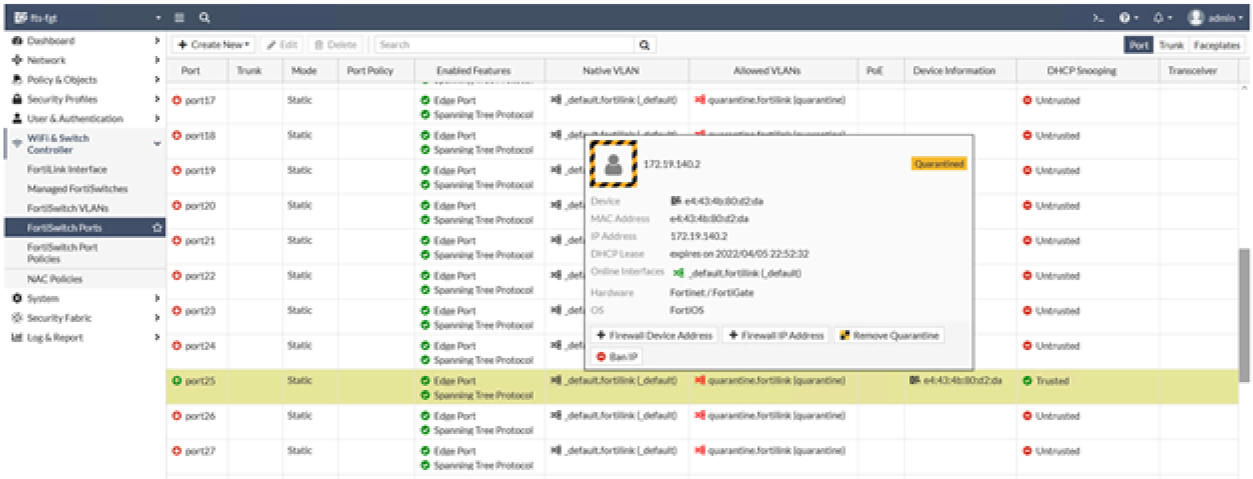
Automation Framework

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

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	_def				Untrusted	
port20		Static		Edge Port Spanning Tree Protocol	_def				Untrusted	
port21		Static		Edge Port Spanning Tree Protocol	_def				Untrusted	
port22		Static		Edge Port Spanning Tree Protocol	_def				Untrusted	
port23		Static		Edge Port Spanning Tree Protocol	_def				Untrusted	
port24		Static		Edge Port Spanning Tree Protocol	_def				Untrusted	
port25		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		e4:43:4b:80:d2:da	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	

172.19.140.2 Quarantined

Device	e4:43:4b:80:d2:da
MAC Address	e4:43:4b:80:d2: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

4. Click *OK*.

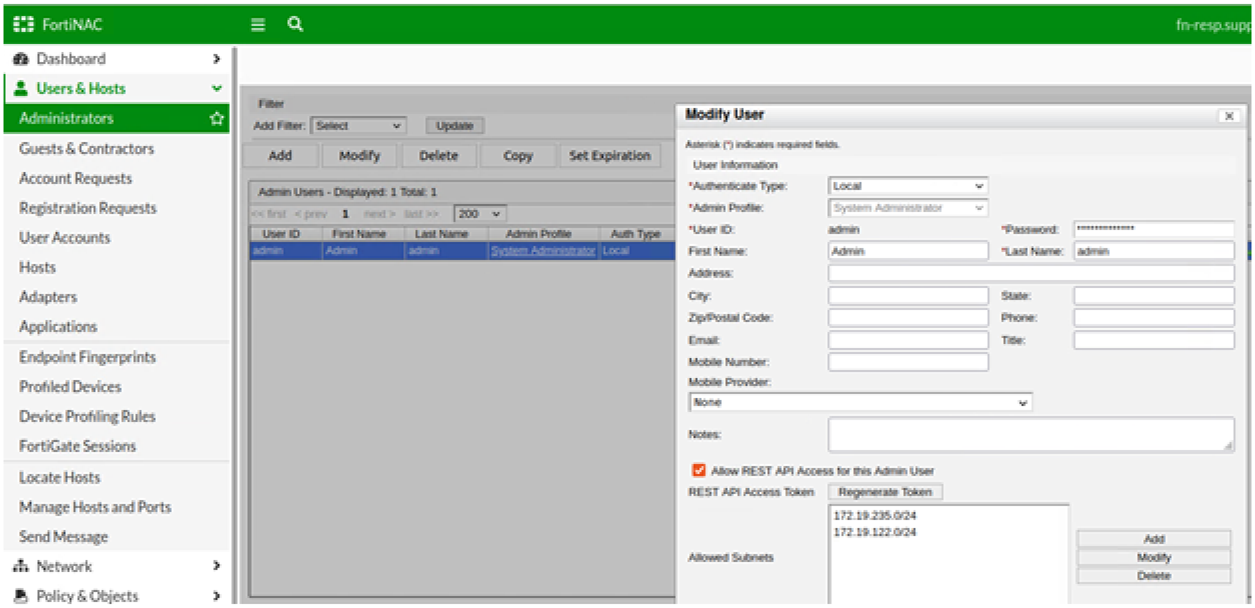
FortiNAC quarantine setup example

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*.



Add Filter: Select

Admin Users - Displayed: 1 Total: 1

<< first < prev 1 next > last >> 200

User ID	First Name	Last Name	Admin Profile	Auth Type
admin	Admin	admin	System Administrator	Local

Modify User

Asterisk (*) indicates required fields.

User Information

*Authenticate Type: Local

*Admin Profile: System Administrator

*User ID: admin

*Password: ***************

First Name: Admin

*Last Name: admin

Address:

City:

State:

Zip/Postal Code:

Phone:

Email:

Title:

Mobile Number:

Mobile Provider: None

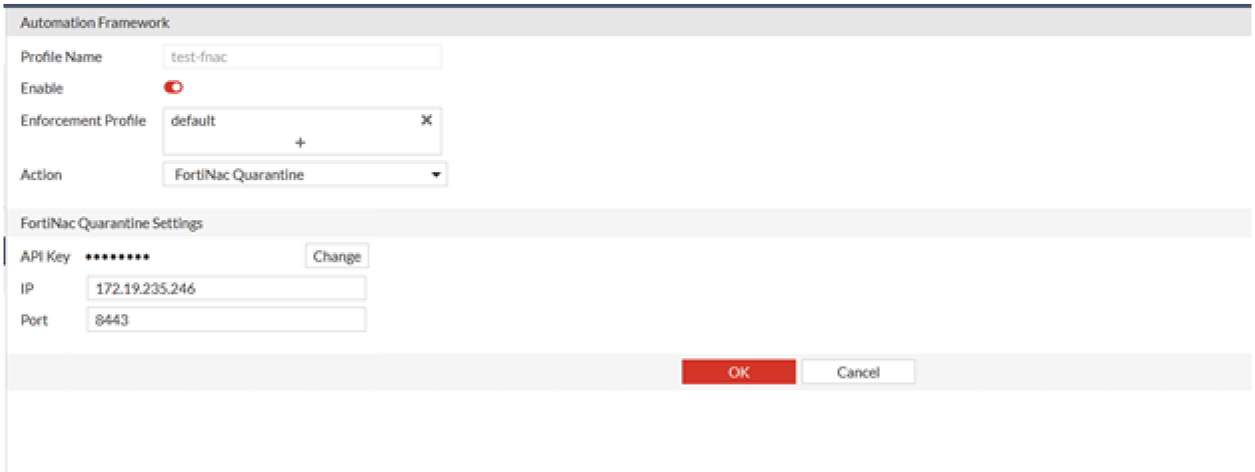
Notes:

☑ Allow REST API Access for this Admin User

REST API Access Token

Allowed Subnets: 172.19.235.0/24, 172.19.122.0/24

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



Profile Name: test-fnac

Enable: ●

Enforcement Profile: default

Action: FortiNac Quarantine

API Key: ••••••••

IP: 172.19.235.246

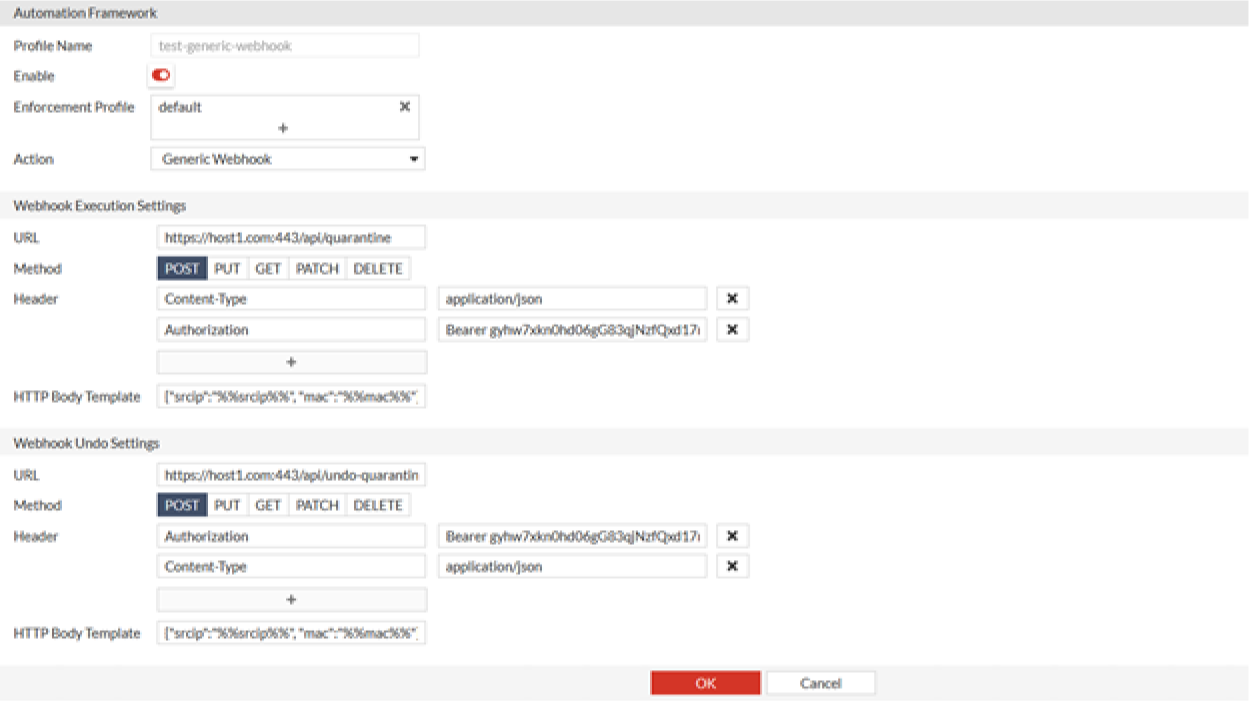
Port: 8443

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

Generic Webhook setup example

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

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



Automation Framework

Profile Name	test-generic-webhook	
Enable	●	
Enforcement Profile	default ✕ +	
Action	Generic Webhook ▾	

Webhook Execution Settings

URL	https://host1.com:443/api/quarantine		
Method	POST | PUT | GET | PATCH | DELETE		
Header	Content-Type	application/json	✕
	Authorization	Bearer gyhw7xkn0hd06gG83qjNzfQxd17i	✕
	+		
HTTP Body Template	{"srcip":"%%srcip%%", "mac":"%%mac%%"		

Webhook Undo Settings

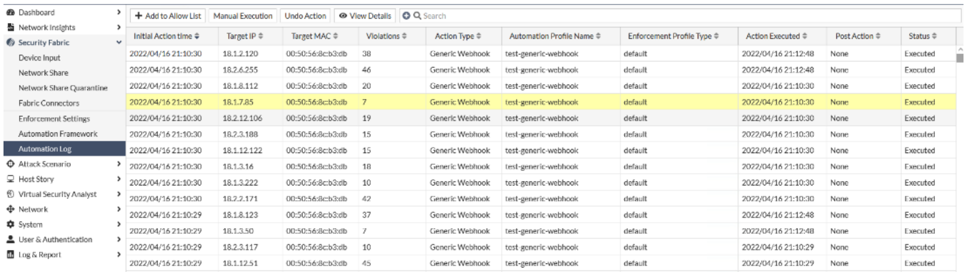
URL	https://host1.com:443/api/undo-quarantin		
Method	POST | PUT | GET | PATCH | DELETE		
Header	Authorization	Bearer gyhw7xkn0hd06gG83qjNzfQxd17i	✕
	Content-Type	application/json	✕
	+		
HTTP Body Template	{"srcip":"%%srcip%%", "mac":"%%mac%%"		

Automation log

Automation Log records each enforcement action generated by FortiNDR.

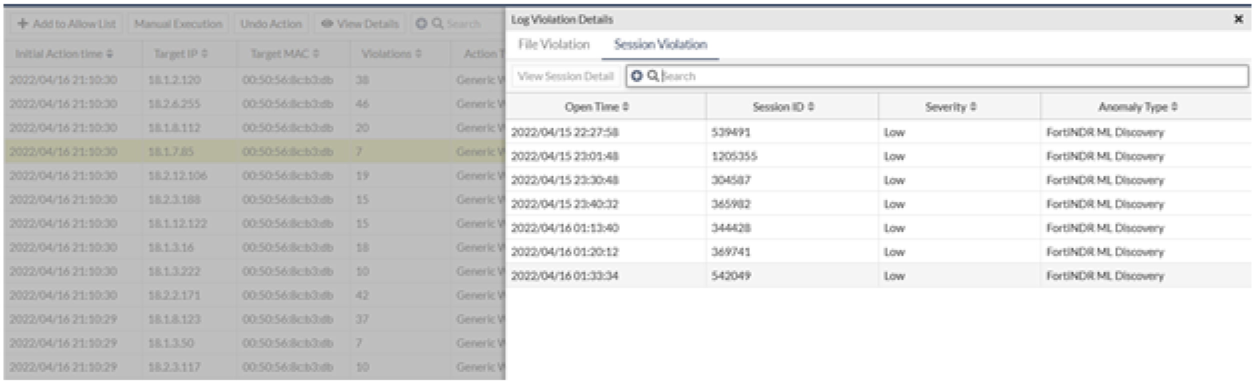
The *Violations* column shows the total number of malware detections and NDR anomalies found on that target device. Double-click a log entry to see more details about the violation, such as malicious files that caused the violation. The number of violations is calculated within the digest cycle of 1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

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



Initial Action time	Target IP	Target MAC	Violations	Action Type	Automation Profile Name	Enforcement Profile Type	Action Executed	Post Action	Status
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
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
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
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
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
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
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
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
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
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
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
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
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
2022/04/16 21:10:29	18.1.12.51	00:50:56:8c:b3:db	45	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:29	None	Executed

Violation details



Open Time	Session ID	Severity	Anomaly Type
2022/04/15 22:27:58	539491	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 *Status* changes to *Executed*. If the action fails, the *Status* changes back to *Active*.	None
Executed	Enforcement action succeeded.	Undo Action
Failed	Exceed the retry limit of five times.	Manual Execution
Duplicated	Another executed entry has been detected with same automation profile, target IP and target mac address.	None
Undo Success	Undo an enforcement action that succeeded.	None
Omitted	Action was prohibited from execution by restriction, for example, allow-listed.	Manual Execution

FortiSandbox integration (FortiSandbox 4.0.1 and higher)

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

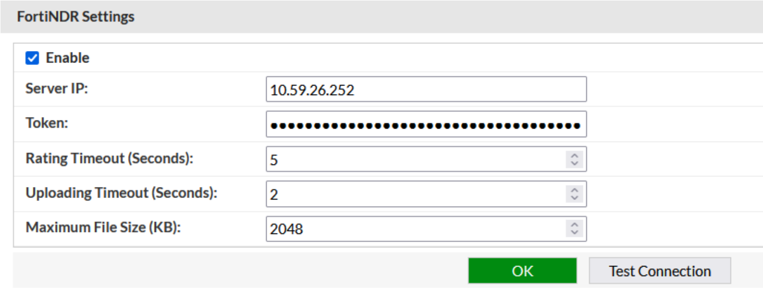
1. FortiSandbox performs its pre-filtering and Static Scan analysis. If any known malware is found, the result is returned.
2. When *FortiNDR Entrust* is enabled under FortiSandbox *Scan Profile*, FortiSandbox sends the files to FortiNDR via API for FortiNDR's verdict of *malware* or *absolute clean*, 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 248.
2. In FortiSandbox, configure FortiSandbox FortiNDR 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.

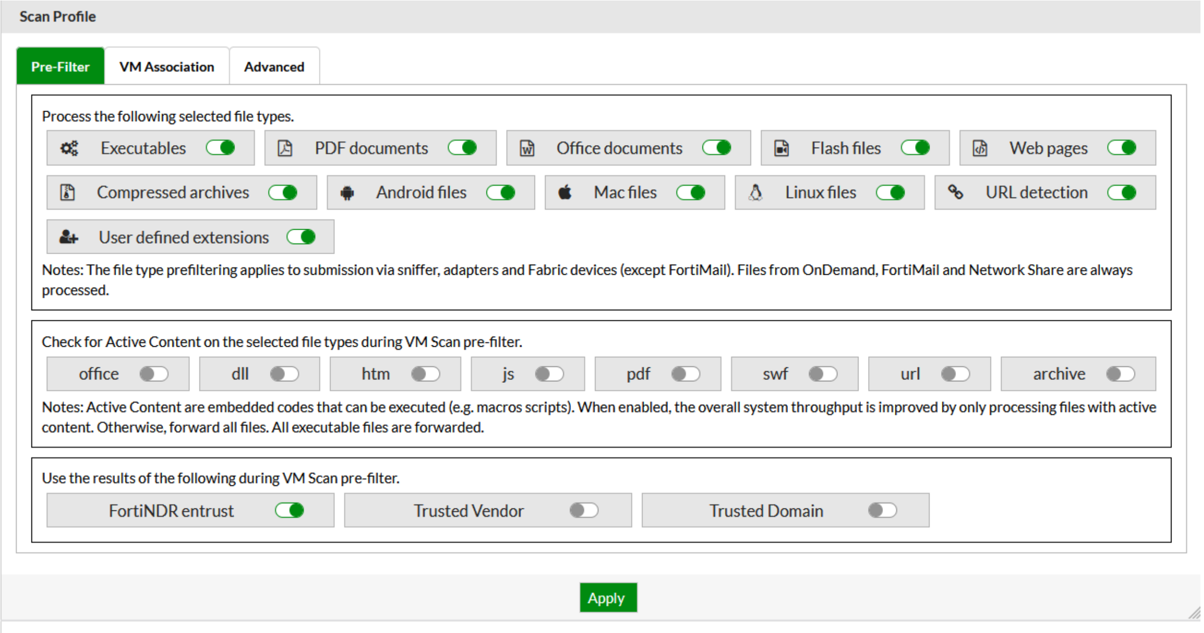


FortiNDR Settings

☑ Enable

Server IP:	10.59.26.252
Token:	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
Rating Timeout (Seconds):	5
Uploading Timeout (Seconds):	2
Maximum File Size (KB):	2048

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



Process the following selected file types.

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

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

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

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

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

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

- FortiNDR entrust ●
- Trusted Vendor ○
- Trusted Domain ○

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.

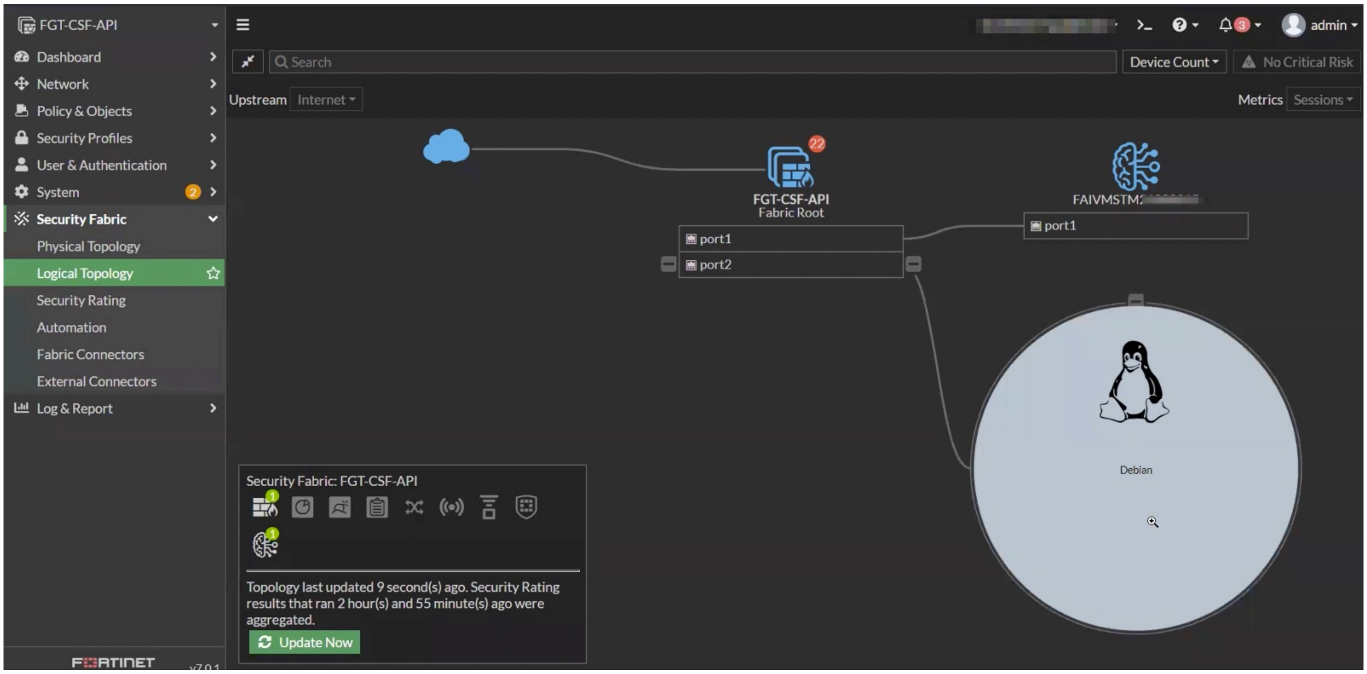
When using multiple FortiGates:

Submissions to single a FortiNDR or FortiGate(s) are required to be in the same Security Fabric, as authentication is performed by a Fabric Connector.

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 85.
   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.



Topology last updated 9 second(s) ago. Security Rating results that ran 2 hour(s) and 55 minute(s) ago were aggregated.

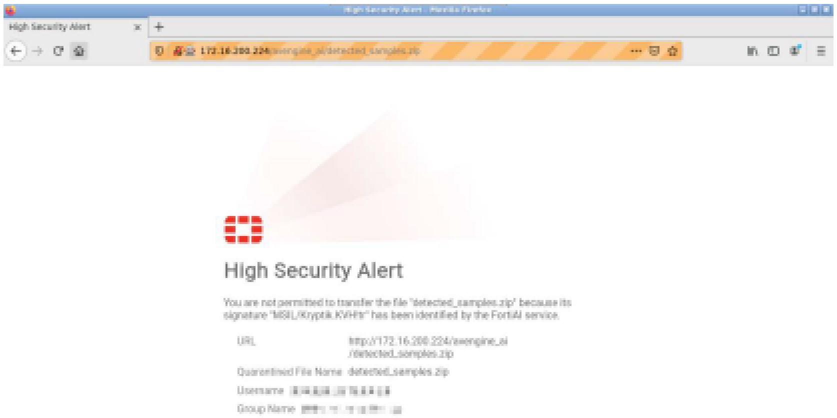
3. Configure the FortiGate AV profile using the following CLI commands.

```
Config system fortindr
    Set status enable
End

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

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

Tips for using FortiNDR inline blocking

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



High Security Alert

You are not permitted to transfer the file "detected_samples.zip" because its signature "MSIL/Kryptik.KVHR" has been identified by the FortiAI service.

URL http://172.16.200.224/avengine_ai/detected_samples.zip

Quarantined File Name detected_samples.zip

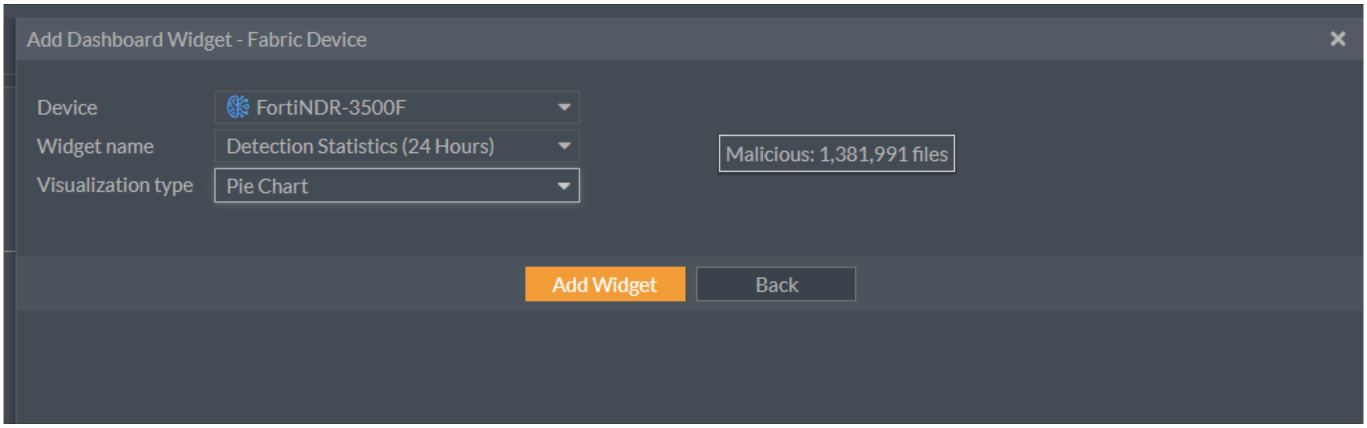
Username [redacted]

Group Name [redacted]

- 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 end 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.



Device: FortiNDR-3500F

Widget name: Detection Statistics (24 Hours)

Visualization type: Pie Chart

Malicious: 1,381,991 files

FortiNDR inline inspection with other AV inspection methods

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

HTTP, FTP, SSH, and CIFS protocols:

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

3. Outbreak prevention and external hash list resources.
    - FortiNDR inline inspection occurs simultaneously.

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

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

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

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

Accepted file types

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

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

FortiGate integration (integrated mode with FOS 6.2 and higher)

You can send files to FortiNDR using FortiGate 6.2 and higher.

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

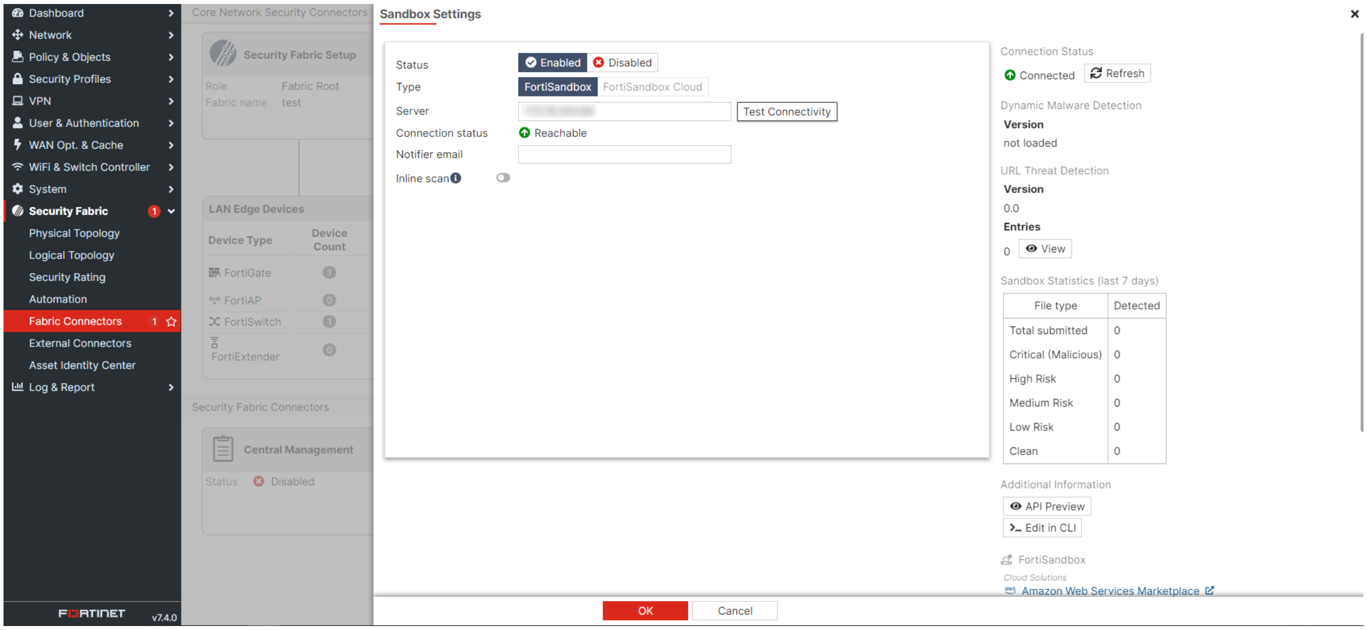
FortiNDR uses the same OFTP (Optimized Fabric Transfer Protocol) over SSL (encrypted) from FortiGate to FortiSandbox. If you are not using FortiSandbox, you can use FortiGate's *Sandbox Inspection* to send files to FortiNDR.

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

For FortiGate Integration we recommend tusing FortiGate inline blocking (FOS 7.0.1 and higher) unless the FortiGate/FortiOS version is lower than 7.0.1

To send files from FortiGate to FortiNDR:

1. Set up the IP address on FortiGate.



Sandbox Settings

Status	Enabled ~ Disabled
Type	FortiSandbox ~ FortiSandbox Cloud
Server	[redacted] Test Connectivity
Connection status	Reachable
Notifier email	
Inline scan	○

Connection Status

Connected Refresh

Dynamic Malware Detection

Version

not loaded

URL Threat Detection

Version

0.0

Entries

0 View

Sandbox Statistics (last 7 days)

File type	Detected
Total submitted	0
Critical (Malicious)	0
High Risk	0
Medium Risk	0
Low Risk	0
Clean	0

Additional Information

API Preview

Edit in CLI

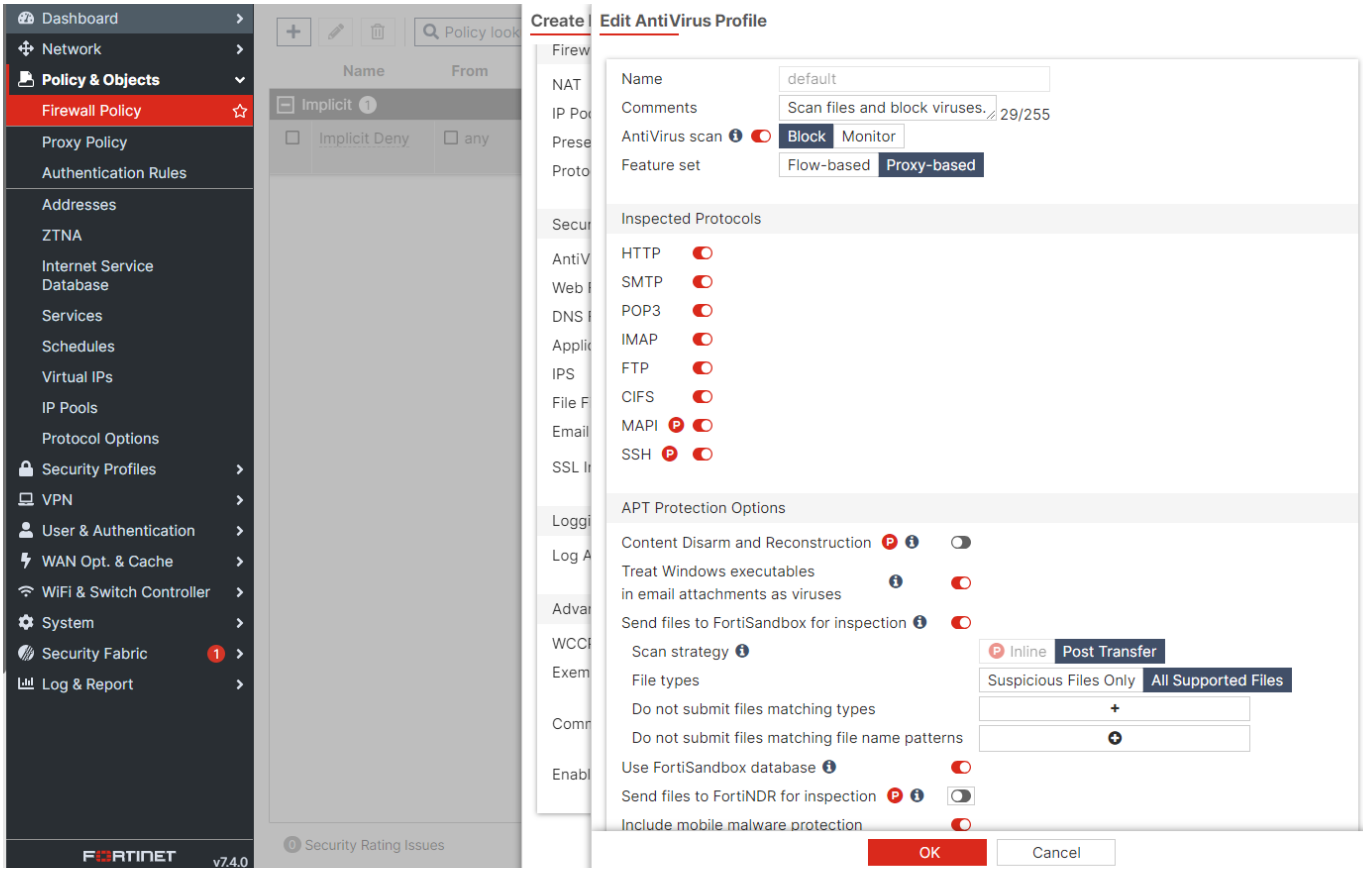
FortiSandbox

Cloud Solutions

Amazon Web Services Marketplace

OK Cancel

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



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: ● Block | Monitor

Feature set: Flow-based | Proxy-based

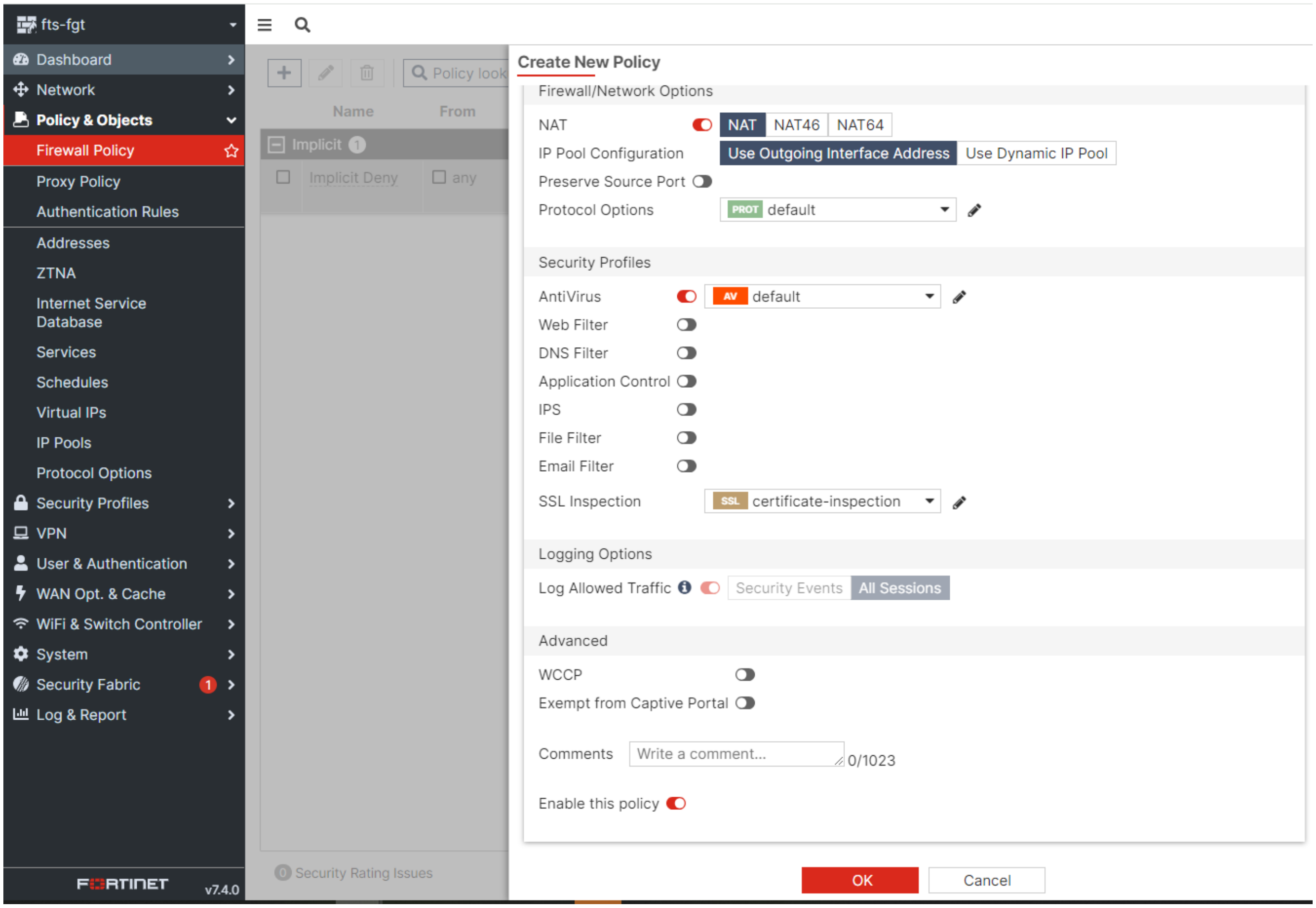
Inspected Protocols

- HTTP ●
- SMTP ●
- POP3 ●
- IMAP ●
- FTP ●
- CIFS ●
- MAPI ●
- SSH ●

APT Protection Options

- Content Disarm and Reconstruction ○
- Treat Windows executables in email attachments as viruses ●
- Send files to FortiSandbox for inspection ●
  - Scan strategy: Inline | Post Transfer
  - File types: Suspicious Files Only | All Supported Files
  - Do not submit files matching types
  - Do not submit files matching file name patterns
- Use FortiSandbox database ●
- Send files to FortiNDR for inspection ○
- Include mobile malware protection ●

3. Apply an AV profile to the firewall policy.



Create New Policy

Firewall/Network Options

NAT ● NAT | NAT46 | NAT64

IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool

Preserve Source Port ○

Protocol Options: PROT default

Security Profiles

AntiVirus ● AV default

Web Filter ○

DNS Filter ○

Application Control ○

IPS ○

File Filter ○

Email Filter ○

SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic ● Security Events | All Sessions

Advanced

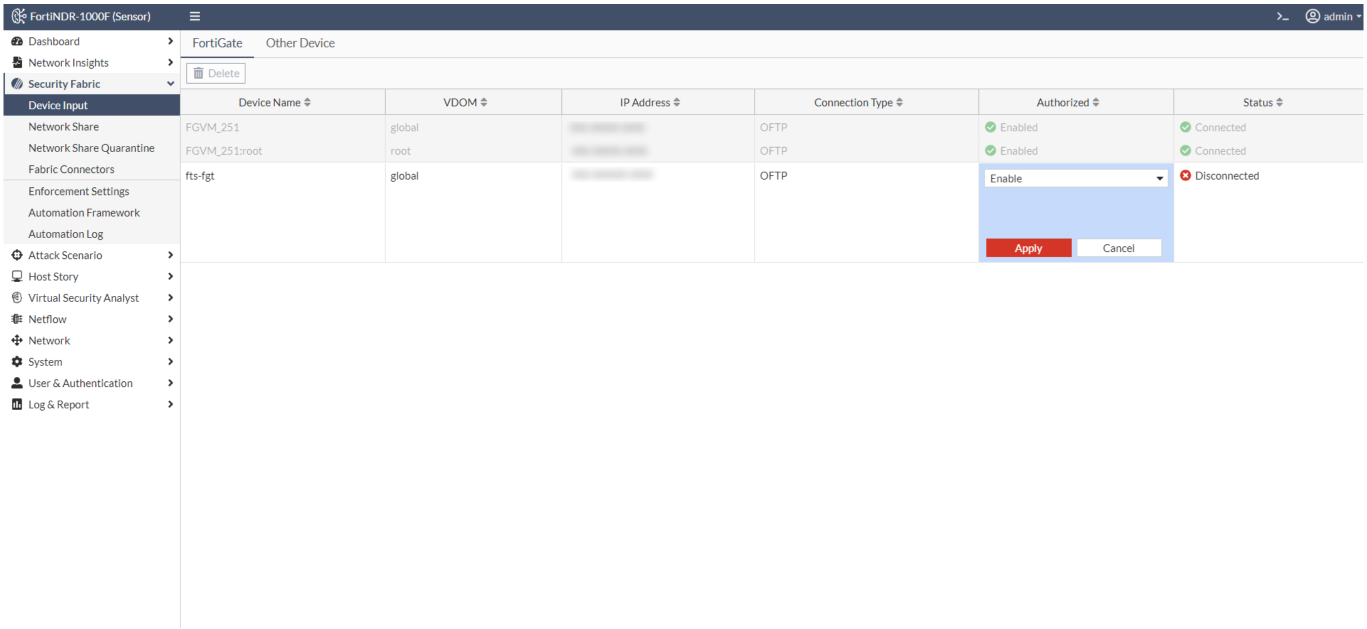
WCCP ○

Exempt from Captive Portal ○

Comments: Write a comment... 0/1023

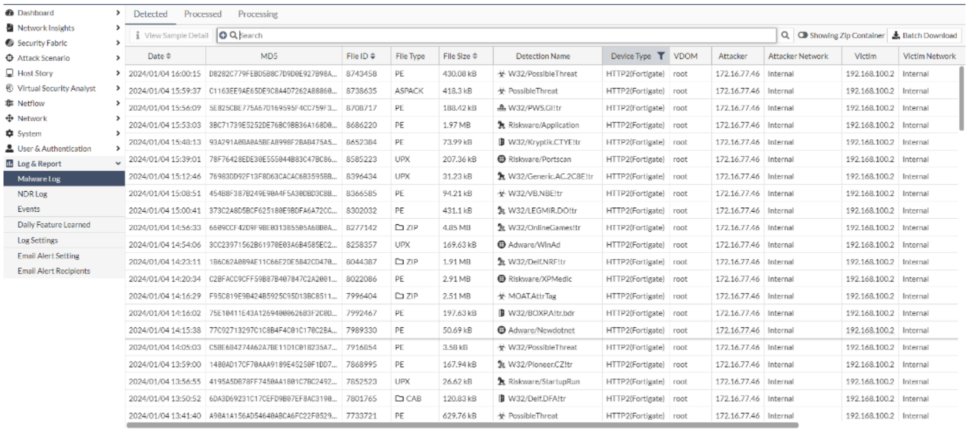
Enable this policy ●

4. Authorize the FortiGate on FortiNDR for sending files.



Device Name	VDOM	IP Address	Connection Type	Authorized	Status
FGVM_251	global	[redacted]	OFTP	Enabled	Connected
FGVM_251:root	root	[redacted]	OFTP	Enabled	Connected
fts-fgt	global	[redacted]	OFTP	Enable	Disconnected

5. Check the FortiNDR processed traffic.



Date	MD5	File ID	File Type	File Size	Detection Name	Device Type	VDOM	Attacker	Attacker Network	Victim	Victim Network
2024/01/04 16:00:15	D8282C779FEBD588C7D9D0E927B98A...	8743458	PE	430.08 kB	W32/PossibleThreat	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:59:37	C1163EE9AE65DE9C8A4D7262A88860...	8738635	ASPACK	418.3 kB	PossibleThreat	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:56:09	5E825CBE775A67D169595F4CC759F3...	8708717	PE	188.42 kB	W32/PWS.GI!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:53:03	3BC71739E5252DE76BC9BB36A168D0...	8686220	PE	1.97 MB	Riskware/Application	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:48:13	93A291A0BA0A5BEA899BF2BAB475A5...	8652384	PE	73.99 kB	W32/Kryptik.CTYE!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:39:01	78F76428EDE30E555044B83C47BC86...	8585223	UPX	207.36 kB	Riskware/Portscan	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:12:46	76983DD92F13F8D63CACAC6B3595BB...	8396434	UPX	31.23 kB	W32/Generic.AC.2C8E!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:08:51	454B8F387B249E90A4F5A30DBD3CBB...	8366585	PE	94.21 kB	W32/VB.NBE!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 15:00:41	373C2A8D5BCF625180E9BDFA6A72CC...	8302032	PE	431.1 kB	W32/LEGMIR.DO!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:56:33	6609CCF42D9F9BE0313B5505A68B8A...	8277142	ZIP	4.85 MB	W32/OnlineGames!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:54:06	3CC23971562B61970E03A6B4585EC2...	8258357	UPX	169.63 kB	Adware/WinAd	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:23:11	1B6C62A089AE11C66E2DE5B42CD470...	8044387	ZIP	1.91 MB	W32/Delf.NRF!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:20:34	C2BFACC9CFF59B87B407847C2A2001...	8022086	PE	2.91 MB	Riskware/XPMedic	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:16:29	F95C819E9B424B5925C95D13BC8511...	7996404	ZIP	2.51 MB	MOAT.AttrTag	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:16:02	75E10411E43A126940008626B3F2C0D...	7992467	PE	197.63 kB	W32/BOXP.A!tr.bdr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:15:38	77C92713297C1C8B4F4C01C170C2BA...	7989330	PE	50.69 kB	Adware/Newdotnet	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 14:05:03	C58E6B4274A62A7BE11D1C018235A7...	7916854	PE	3.58 kB	W32/PossibleThreat	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 13:59:00	1480AD17CF70AAA9189E45250F1DD7...	7868995	PE	167.94 kB	W32/Pioneer.CZ!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 13:56:55	4195A5DB78FF7450AA1801C7BC2492...	7852523	UPX	26.62 kB	Riskware/StartupRun	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 13:50:52	6DA3D69231C17CEFD9B07EF8AC3190...	7801765	CAB	120.83 kB	W32/Delf.DFA!tr	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
2024/01/04 13:41:40	A90A1A156AD54640ABCA6FC22F0529...	7733721	PE	629.76 kB	PossibleThreat	HTTP2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal

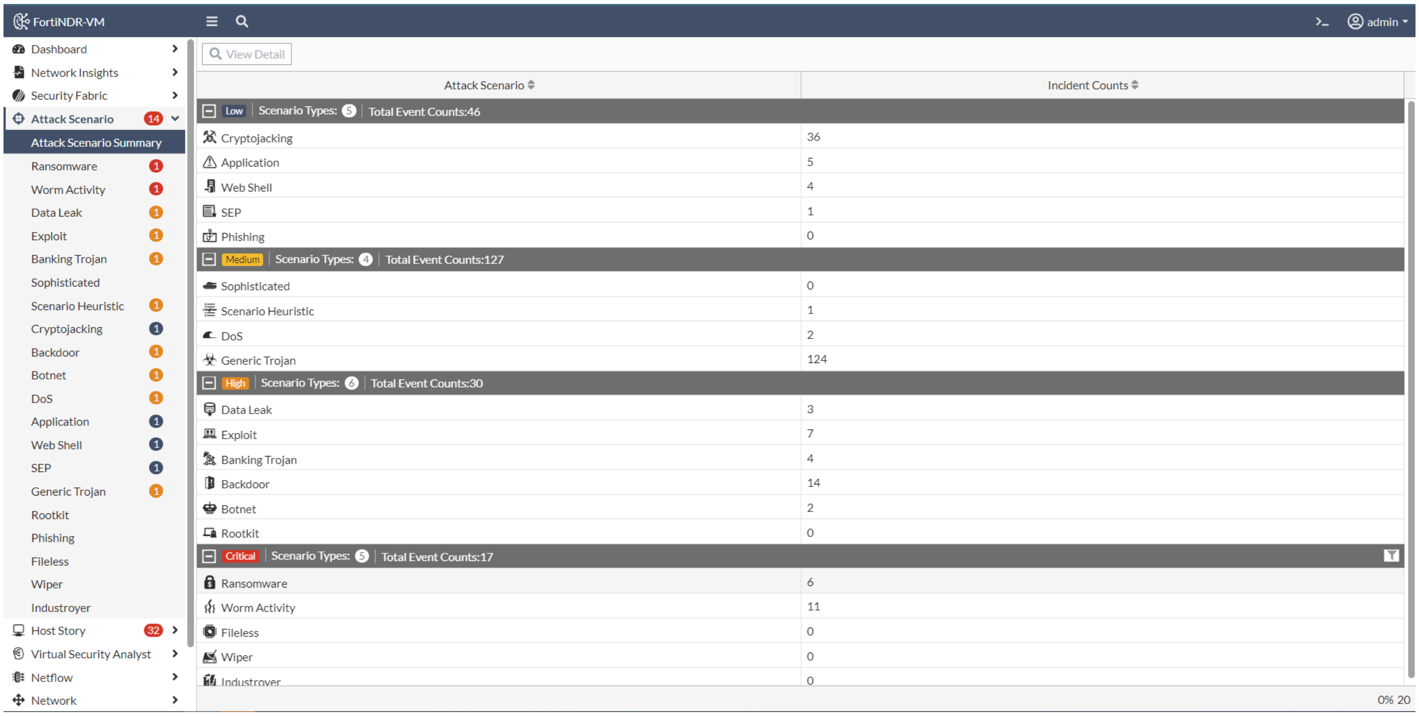
Attack Scenario

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.



Attack Scenario	Incident Counts
Low | Scenario Types: 5 | Total Event Counts:46	
Cryptojacking	36
Application	5
Web Shell	4
SEP	1
Phishing	0
Medium | Scenario Types: 4 | Total Event Counts:127	
Sophisticated	0
Scenario Heuristic	1
DoS	2
Generic Trojan	124
High | Scenario Types: 6 | Total Event Counts:30	
Data Leak	3
Exploit	7
Banking Trojan	4
Backdoor	14
Botnet	2
Rootkit	0
Critical | Scenario Types: 5 | Total Event Counts:17	
Ransomware	6
Worm Activity	11
Fileless	0
Wiper	0
Industroyer	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 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

Scenario	Severity	Description
		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.
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.

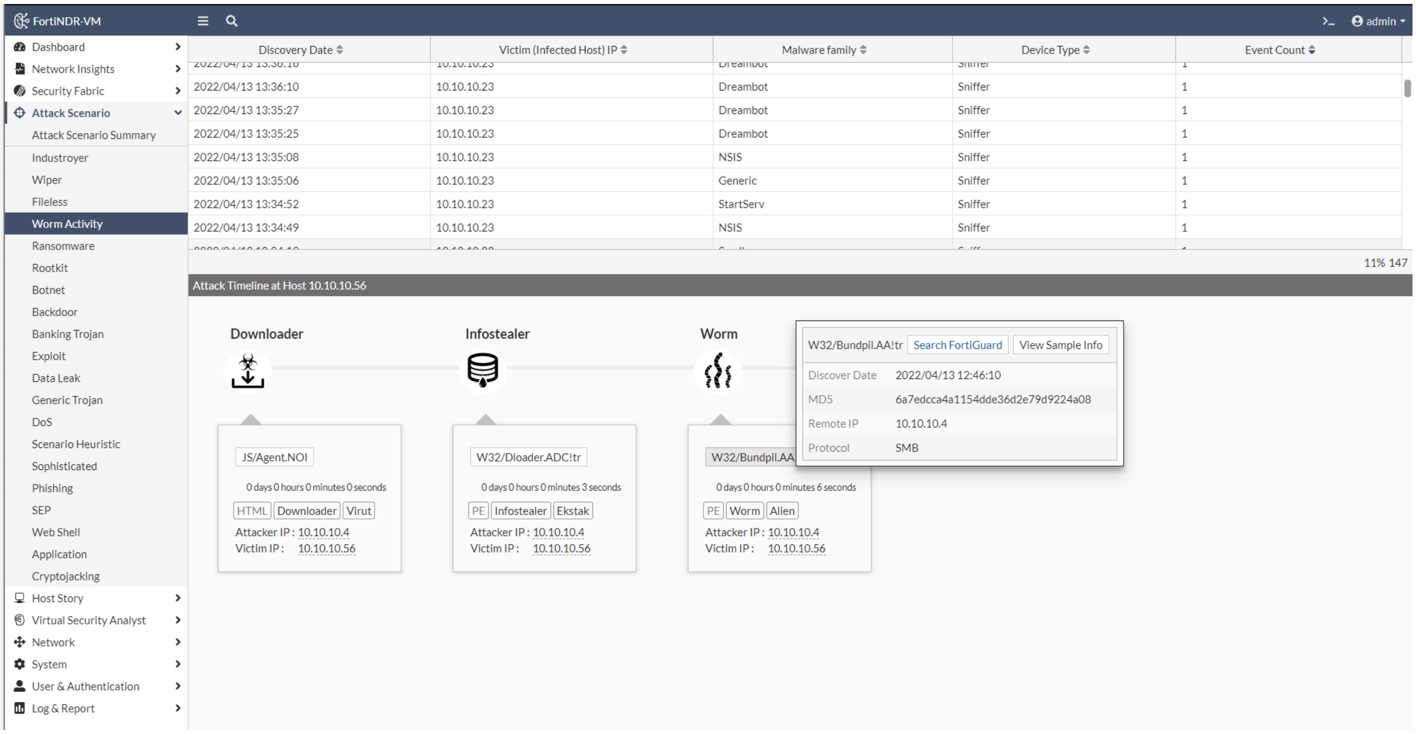
Attack scenario navigation and timeline

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.



Discovery Date	Victim (Infected Host) IP	Malware family	Device Type	Event Count
2022/04/13 13:36:16	10.10.10.23	Dreambot	Sniffer	1
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

11% 147

Attack Timeline at Host 10.10.10.56

Downloader

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

Infostealer

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

Worm

W32/Bundpil.AA

0 days 0 hours 0 minutes 6 seconds

PE Worm Alien

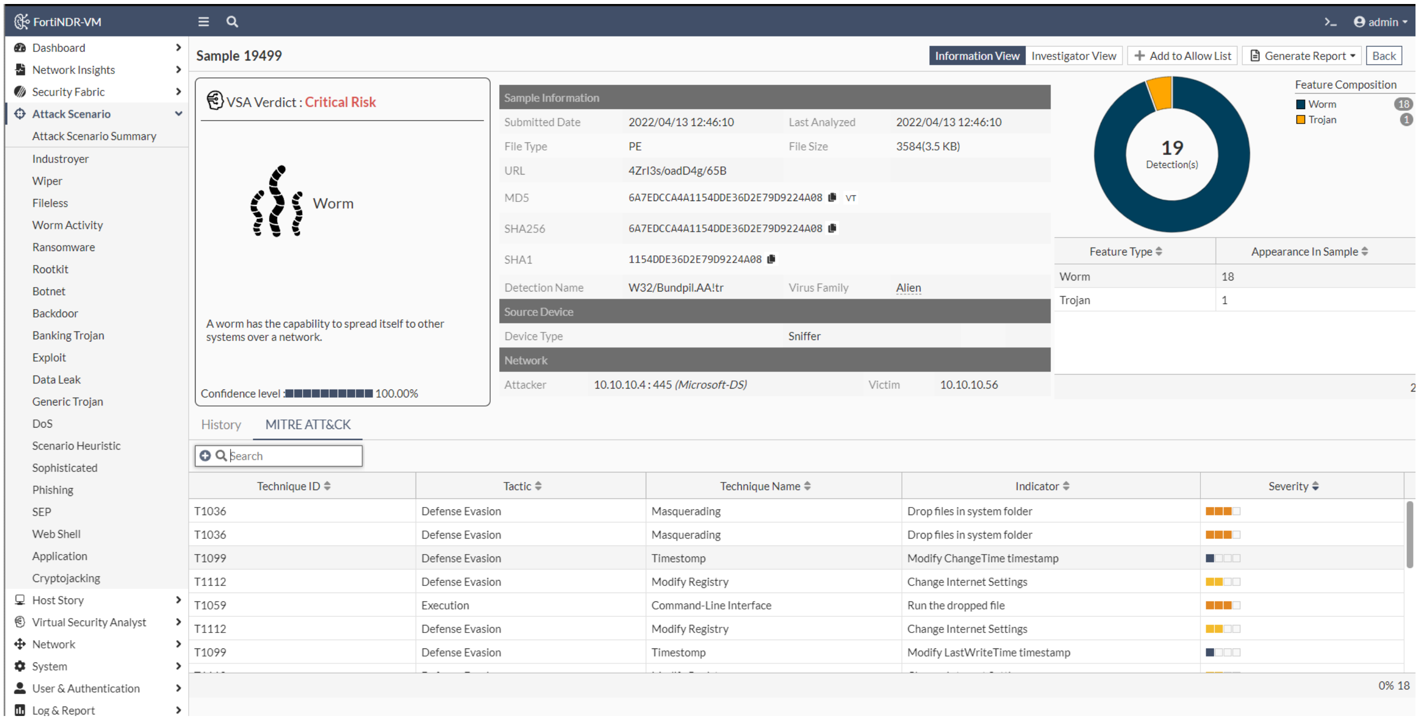
Attacker IP : 10.10.10.4
Victim IP : 10.10.10.56

W32/Bundpil.AA!tr Search FortiGuard View Sample Info

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.



Sample 19499

VSA Verdict : Critical Risk

Worm

A worm has the capability to spread itself to other systems over a network.

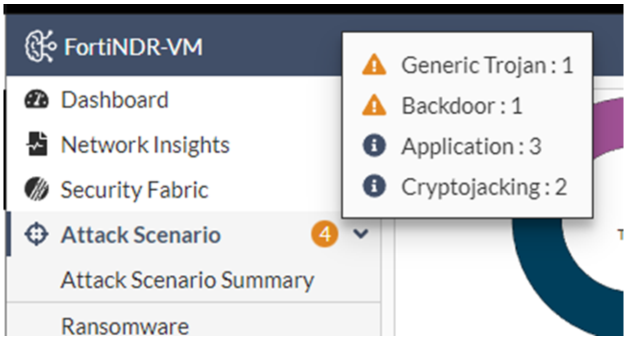
Confidence level : ■■■■■■■■■■ 100.00%

Sample Information			
Submitted Date	2022/04/13 12:46:10	Last Analyzed	2022/04/13 12:46:10
File Type	PE	File Size	3584(3.5 KB)
URL	4Zrl3s/oadD4g/65B		
MD5	6A7EDCCA4A1154DDE36D2E79D9224A08 VT		
SHA256	6A7EDCCA4A1154DDE36D2E79D9224A08		
SHA1	1154DDE36D2E79D9224A08		
Detection Name	W32/Bundpil.AA!tr	Virus Family	Alien
Source Device			
Device Type		Sniffer	
Network			
Attacker	10.10.10.4 : 445 *(Microsoft-DS)*	Victim	10.10.10.56

Feature Type	Appearance In Sample
Worm	18
Trojan	1

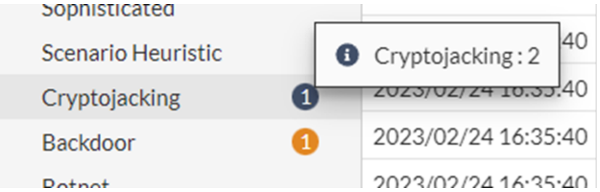
Technique ID	Tactic	Technique Name	Indicator	Severity
T1036	Defense Evasion	Masquerading	Drop files in system folder	■■■□
T1036	Defense Evasion	Masquerading	Drop files in system folder	■■■□
T1099	Defense Evasion	Timestomp	Modify ChangeTime timestamp	■□□□
T1112	Defense Evasion	Modify Registry	Change Internet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

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.



Generic Trojan : 1
Backdoor : 1
Application : 3
Cryptojacking : 2

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.



Cryptojacking : 2

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.

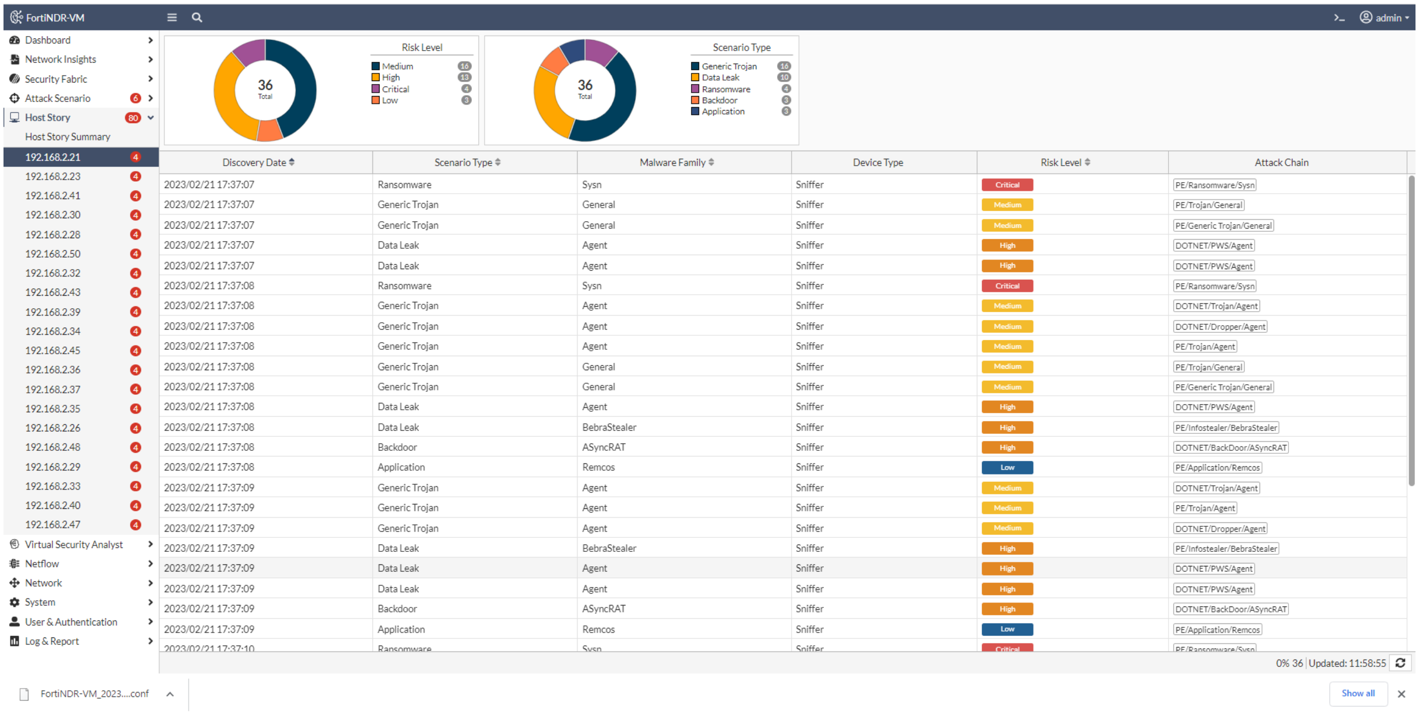
Most attack scenario names are self explanatory as the sophisticated scenario engine searches for multiple payloads of the same attack. For attacks that do not fall under obvious scenarios, they are grouped under the attack scenario called *Scenario Heuristics*.

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.

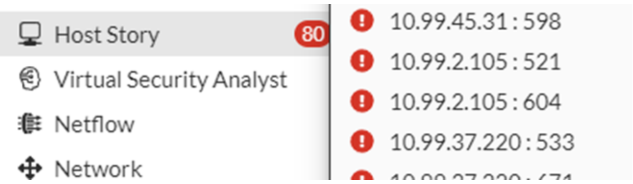
In Center mode, *Host Story* consolidates and displays all stories from all Sensors associated with the Center.

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



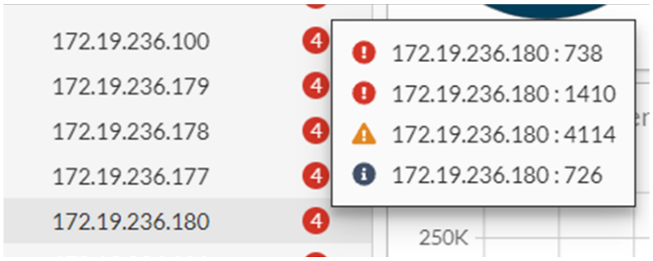
Discovery Date	Scenario Type	Malware Family	Device Type	Risk Level	Attack Chain
2023/02/21 17:37:07	Ransomware	Sysn	Sniffer	Critical	PE/Ransomware/Sysn
2023/02/21 17:37:07	Generic Trojan	General	Sniffer	Medium	PE/Trojan/General
2023/02/21 17:37:07	Generic Trojan	General	Sniffer	Medium	PE/Generic Trojan/General
2023/02/21 17:37:07	Data Leak	Agent	Sniffer	High	DOTNET/PWS/Agent
2023/02/21 17:37:07	Data Leak	Agent	Sniffer	High	DOTNET/PWS/Agent
2023/02/21 17:37:08	Ransomware	Sysn	Sniffer	Critical	PE/Ransomware/Sysn
2023/02/21 17:37:08	Generic Trojan	Agent	Sniffer	Medium	DOTNET/Trojan/Agent
2023/02/21 17:37:08	Generic Trojan	Agent	Sniffer	Medium	DOTNET/Dropper/Agent
2023/02/21 17:37:08	Generic Trojan	Agent	Sniffer	Medium	PE/Trojan/Agent
2023/02/21 17:37:08	Generic Trojan	General	Sniffer	Medium	PE/Trojan/General
2023/02/21 17:37:08	Generic Trojan	General	Sniffer	Medium	PE/Generic Trojan/General
2023/02/21 17:37:08	Data Leak	Agent	Sniffer	High	DOTNET/PWS/Agent
2023/02/21 17:37:08	Data Leak	BebraStealer	Sniffer	High	PE/Infostealer/BebraStealer
2023/02/21 17:37:08	Backdoor	ASyncRAT	Sniffer	High	DOTNET/BackDoor/ASyncRAT
2023/02/21 17:37:08	Application	Remcos	Sniffer	Low	PE/Application/Remcos
2023/02/21 17:37:09	Generic Trojan	Agent	Sniffer	Medium	DOTNET/Trojan/Agent
2023/02/21 17:37:09	Generic Trojan	Agent	Sniffer	Medium	PE/Trojan/Agent
2023/02/21 17:37:09	Generic Trojan	Agent	Sniffer	Medium	DOTNET/Dropper/Agent
2023/02/21 17:37:09	Data Leak	BebraStealer	Sniffer	High	PE/Infostealer/BebraStealer
2023/02/21 17:37:09	Data Leak	Agent	Sniffer	High	DOTNET/PWS/Agent
2023/02/21 17:37:09	Data Leak	Agent	Sniffer	High	DOTNET/PWS/Agent
2023/02/21 17:37:09	Backdoor	ASyncRAT	Sniffer	High	DOTNET/BackDoor/ASyncRAT
2023/02/21 17:37:09	Application	Remcos	Sniffer	Low	PE/Application/Remcos
2023/02/21 17:37:10	Ransomware	Sysn	Sniffer	Critical	PE/Ransomware/Sysn

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.



10.99.45.31 : 598
10.99.2.105 : 521
10.99.2.105 : 604
10.99.37.220 : 533
10.99.37.220 : 671

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



172.19.236.100 4
172.19.236.179 4
172.19.236.178 4
172.19.236.177 4
172.19.236.180 4

❗ 172.19.236.180 : 738
❗ 172.19.236.180 : 1410
⚠ 172.19.236.180 : 4114
ℹ 172.19.236.180 : 726

Virtual Security Analyst

This section includes the following topics.

- Express Malware Analysis on page 120
- Outbreak Search on page 124
- Static Filter on page 126
- NDR Muting on page 127
- ML Configuration on page 129
- Malware Big Picture on page 137
- Device Enrichment on page 139

Express Malware Analysis

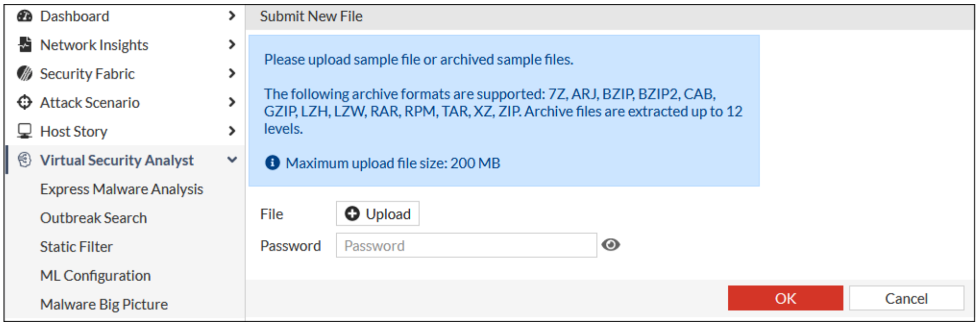
Go to *Virtual Security Analysis* > *Express Malware Analysis* to quickly upload a file and get the verdict. *Express Malware Analysis* is supported in both the GUI and the API. The default file size limit is 200MB. The file size limit can be changed using the CLI.

For information about using the API to submit files, see Appendix A: API guide on page 248 > 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.



Please upload sample file or archived sample files.

The following archive formats are supported: 7Z, ARJ, BZIP, BZIP2, CAB, GZIP, LZH, LZW, RAR, RPM, TAR, XZ, ZIP. Archive files are extracted up to 12 levels.

Maximum upload file size: 200 MB

File

Password: Password

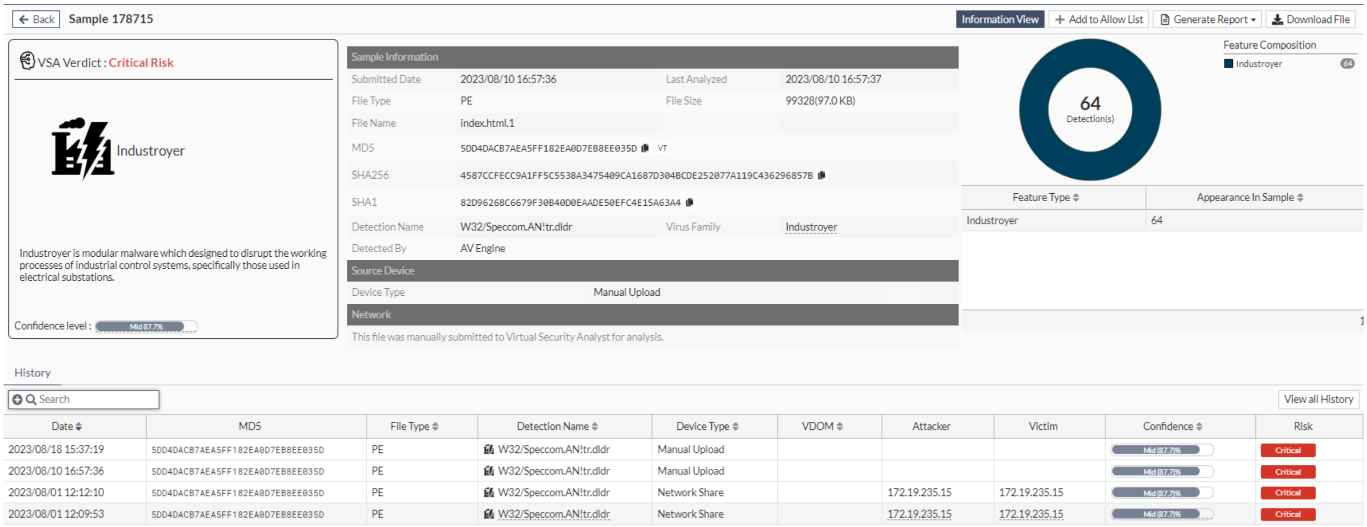
2. Submit a file for analysis. The default file size limit is 200MB. The file size limit can be changed using the CLI.
   a. Click *Upload* then navigate to the file location on your device and click *Open*.
   b. In the *Password* field, enter the password for the file. If the file does not require 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 *Zip* or *PE*. *Other* 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 *file contain abnormal javascipt*, and so on. This helps you understand why FortiNDR determines it is malware.



Sample 178715

VSA Verdict : Critical Risk

Industroyer

Industroyer is modular malware which designed to disrupt the working processes of industrial control systems, specifically those used in electrical substations.

Confidence level : Mid 87.7%

Sample Information			
Submitted Date	2023/08/10 16:57:36	Last Analyzed	2023/08/10 16:57:37
File Type	PE	File Size	99328(97.0 KB)
File Name	index.html.1		
MD5	5DD4DACB7AEA5FF182EA0D7EB8EE035D VT		
SHA256	4587CCFECC9A1FF5C5538A3475409CA1687D304BCDE252077A119C436296857B		
SHA1	82D96268C6679F30B40D0EAADE50EFC4E15A63A4		
Detection Name	W32/Speccom.AN!tr.dldr	Virus Family	Industroyer
Detected By	AV Engine		

Source Device

Device Type	Manual Upload

Network

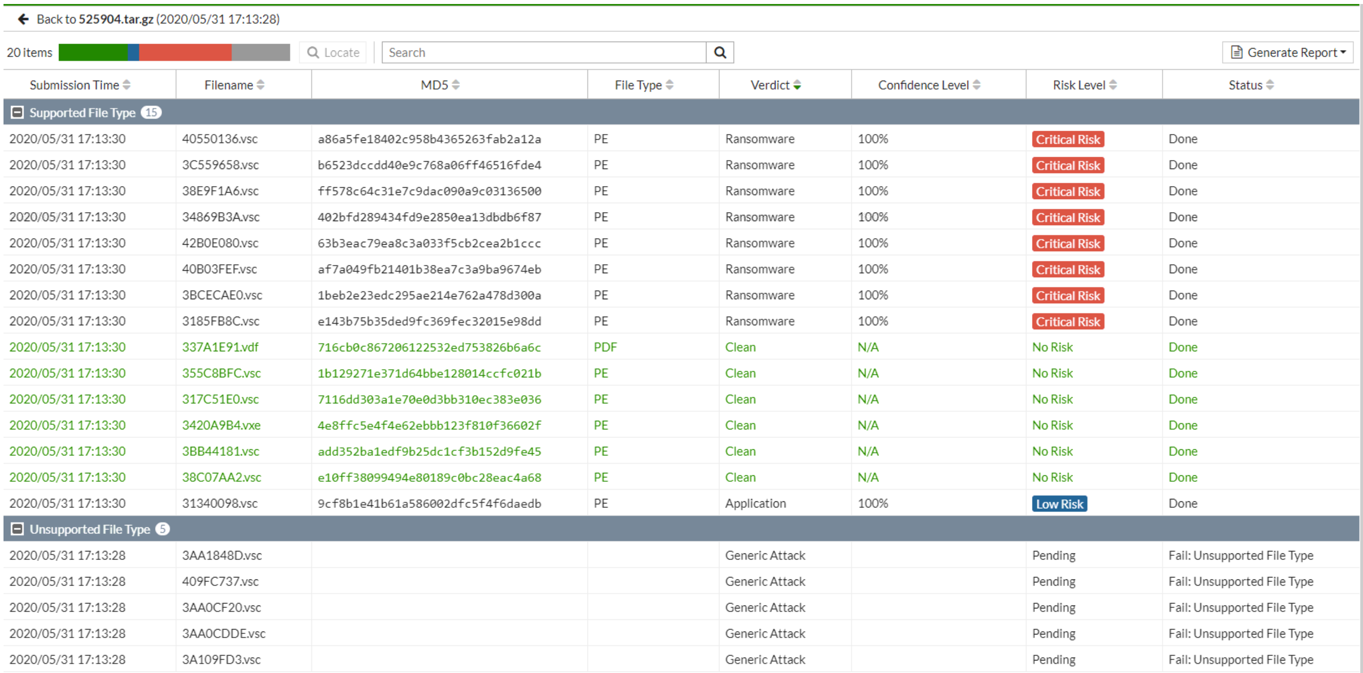
This file was manually submitted to Virtual Security Analyst for analysis.

Feature Type	Appearance In Sample
Industroyer	64

History

Date	MD5	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk
2023/08/18 15:37:19	5DD4DACB7AEA5FF182EA0D7EB8EE035D	PE	W32/Speccom.AN!tr.dldr	Manual Upload				Mid (87.7)%	Critical
2023/08/10 16:57:36	5DD4DACB7AEA5FF182EA0D7EB8EE035D	PE	W32/Speccom.AN!tr.dldr	Manual Upload				Mid (87.7)%	Critical
2023/08/01 12:12:10	5DD4DACB7AEA5FF182EA0D7EB8EE035D	PE	W32/Speccom.AN!tr.dldr	Network Share		172.19.235.15	172.19.235.15	Mid (87.7)%	Critical
2023/08/01 12:09:53	5DD4DACB7AEA5FF182EA0D7EB8EE035D	PE	W32/Speccom.AN!tr.dldr	Network Share		172.19.235.15	172.19.235.15	Mid (87.7)%	Critical

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

Submission Time	Filename	MD5	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	b6523dccdd40e9c768a06ff46516fde4	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	38E9F1A6.vsc	ff578c64c31e7c9dac090a9c03136500	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	34869B3A.vsc	402bfd289434fd9e2850ea13dbdb6f87	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	42B0E080.vsc	63b3eac79ea8c3a033f5cb2cea2b1ccc	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	40B03FEF.vsc	af7a049fb21401b38ea7c3a9ba9674eb	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3BCECAE0.vsc	1beb2e23edc295ae214e762a478d300a	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3185FB8C.vsc	e143b75b35ded9fc369fec32015e98dd	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	337A1E91.vdf	716cb0c867206122532ed753826b6a6c	PDF	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	355C8BFC.vsc	1b129271e371d64bbe128014ccfc021b	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	317C51E0.vsc	7116dd303a1e70e0d3bb310ec383e036	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	3420A9B4.vxe	4e8ffc5e4f4e62ebbb123f810f36602f	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	3BB44181.vsc	add352ba1edf9b25dc1cf3b152d9fe45	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	38C07AA2.vsc	e10ff38099494e80189c0bc28eac4a68	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	31340098.vsc	9cf8b1e41b61a586002dfc5f4f6daedb	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	3AA0CDDE.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3A109FD3.vsc			Generic Attack		Pending	Fail: Unsupported File Type

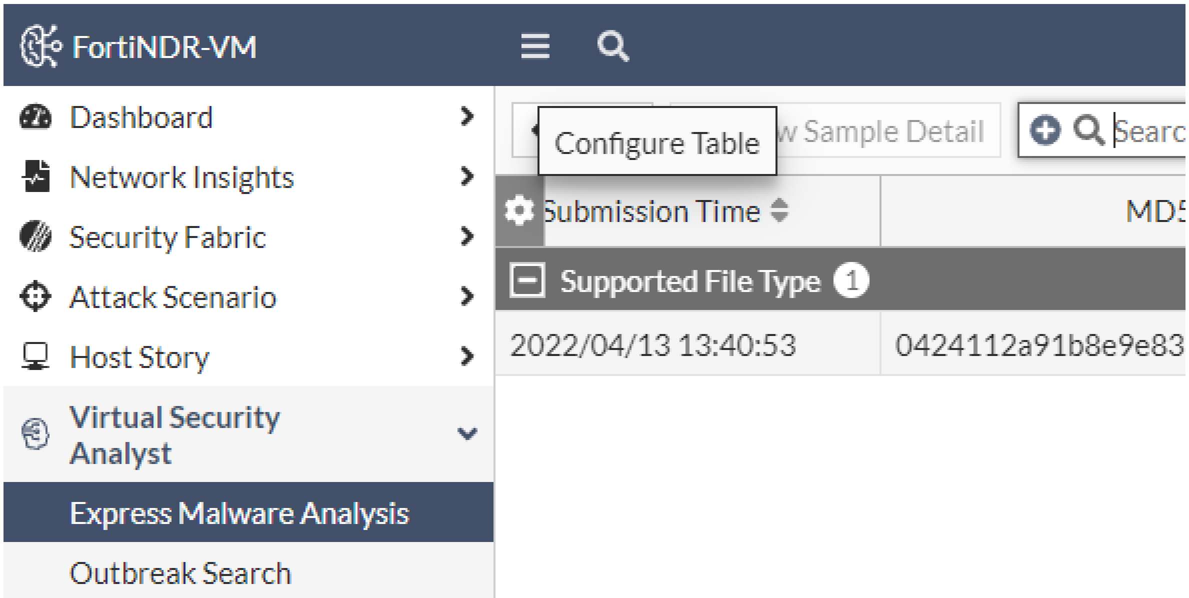
4. (Optional) Click *Generate Report*to view the report summary in PDF and JSON format.

To change the file size limit with the CLI:

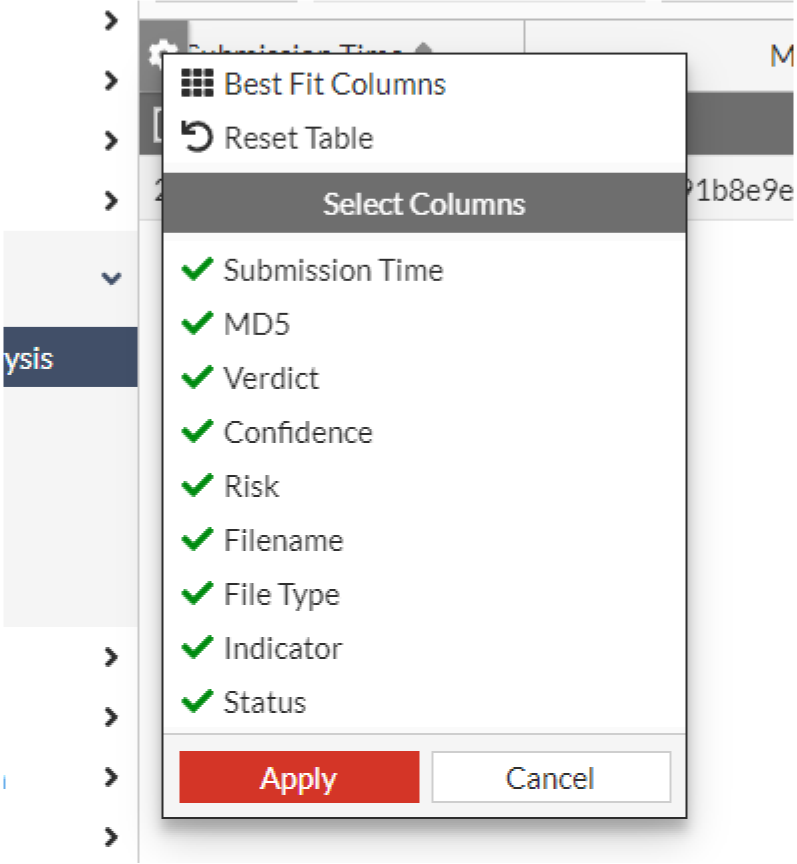
```
execute file-size-threshold
```

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.

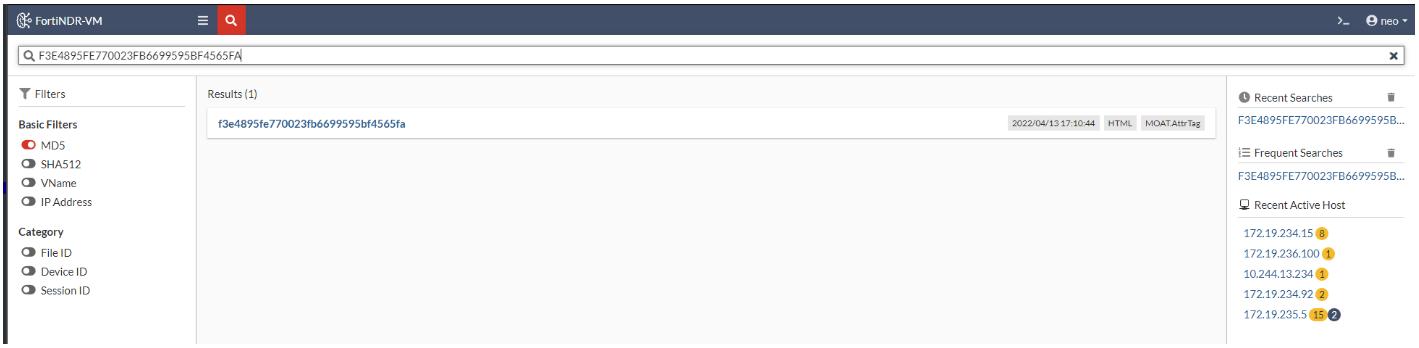


Outbreak Search

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.
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.

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.



FortiNDR-VM

neo

F3E4895FE770023FB6699595BF4565FA

Filters

Basic Filters

● MD5
○ SHA512
○ VName
○ IP Address

Category

○ File ID
○ Device ID
○ Session ID

Results (1)

f3e4895fe770023fb6699595bf4565fa 2022/04/13 17:10:44 HTML MOAT.AttrTag

Recent Searches

F3E4895FE770023FB6699595B...

Frequent Searches

F3E4895FE770023FB6699595B...

Recent Active Host

172.19.234.15 8
172.19.236.100 1
10.244.13.234 1
172.19.234.92 2
172.19.235.5 15 2

Search lead type of hash or detection name

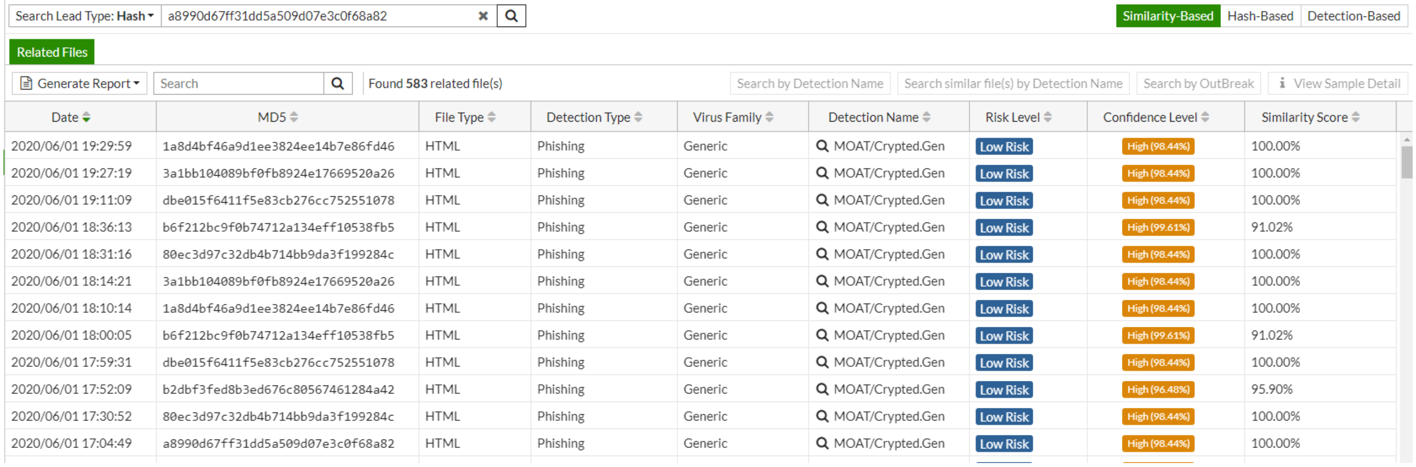
This search lead type accepts MD5 or SHA512 as a search value. You can submit the sample to FortiNDR in *Express Malware Analysis*. When the search lead type is detection name, the search value can be an exact detection name, such as W32/Phishing.DDS!tr, or a detection name with wildcards, such as W32/Phishing.%.

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

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

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

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



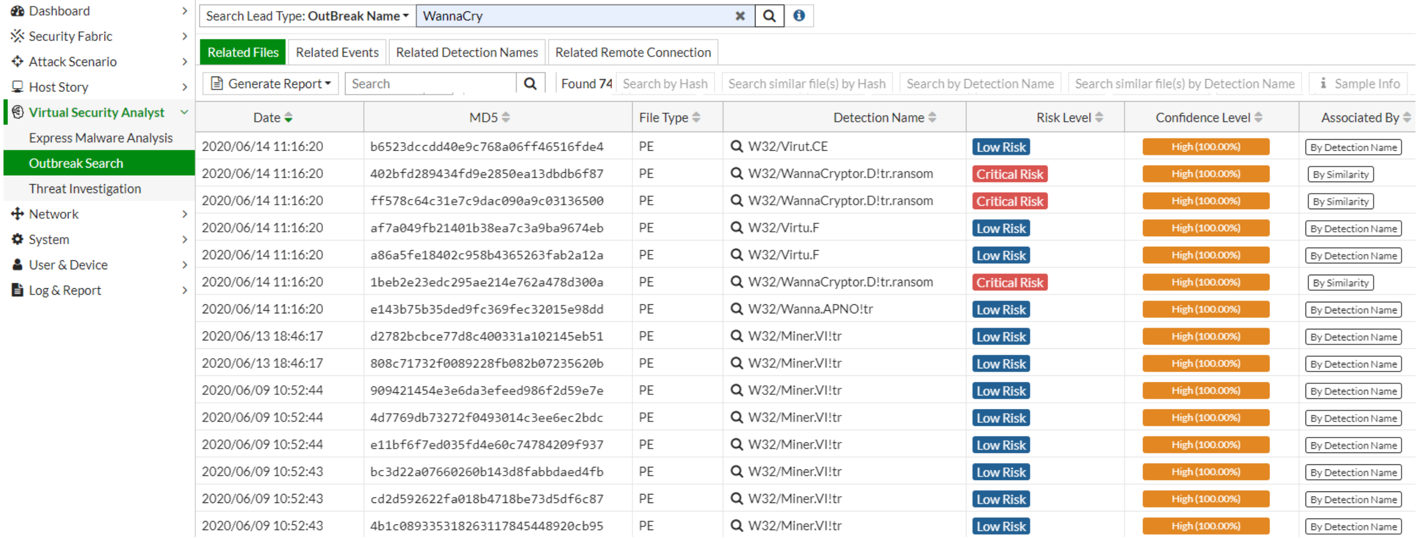
Date	MD5	File Type	Detection Type	Virus Family	Detection Name	Risk Level	Confidence Level	Similarity Score
2020/06/01 19:29:59	1a8d4bf46a9d1ee3824ee14b7e86fd46	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 19:27:19	3a1bb104089bf0fb8924e17669520a26	HTML	Phishing	Generic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

Search lead type of outbreak name

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

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

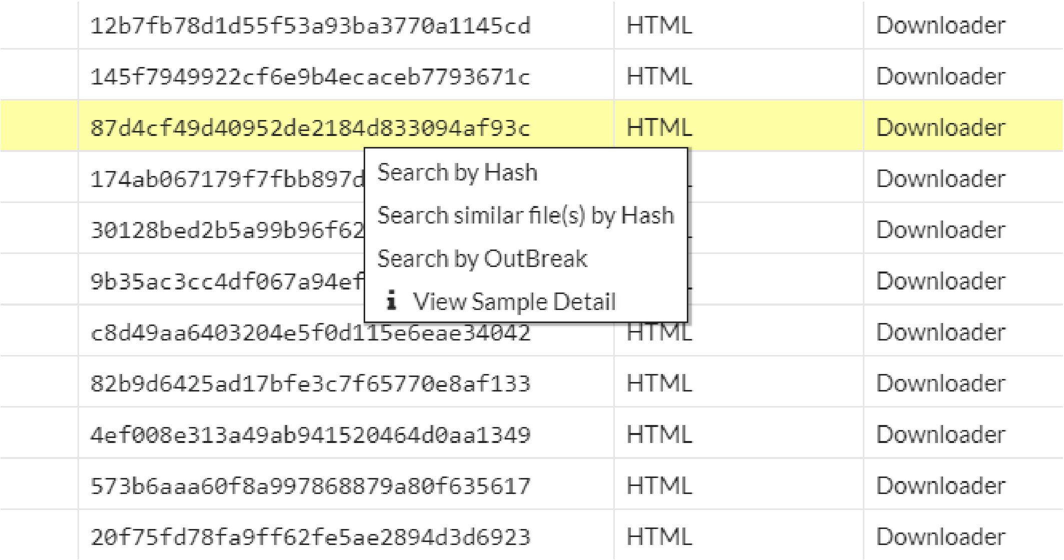
These files are listed in the *Related Files* tab. Other tabs that have a summary of the detection name, remote connections, and attack scenarios events.



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

Recursive searches

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



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

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.

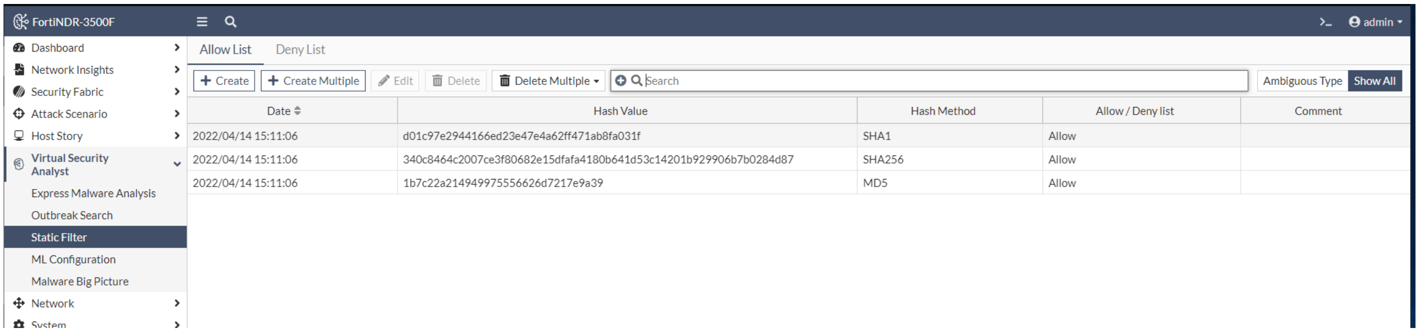
Static Filter

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	1b7c22a214949975556626d7217e9a39	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.

NDR Muting

The *Virtual Security Analyst > NDR Muting* page displays all the rules added to hide detections that you are not interested in. Once an anomaly is muted, FortiNDR will:

Hide	• The anomaly in any insight page's *Anomaly* tab. • The session related to the muted anomaly in any insight page's *Session* tab. • The connection pair related to the muted anomaly in any insight page's *Connection* tab.
Stop	• Triggering email alerts from the muted anomaly. • Triggering enforcement from the muted anomaly. • Generating syslog messages related to the muted anomaly (Standalone and Sensor mode only).

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, any information related to this anomaly will be hidden from the insight pages, although the information is not deleted.

NDR Muting rules can be applied in Center and Sensor mode. However, these muting rules are only applied locally. For example, if you hide an attack on a Center device, the same attack is not automatically hidden in the GUI of a Sensor device and vice versa.

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 (*enabled* / *disabled*).
Rule	The rule content. For example, if the *Rule Type* is *Anomaly*, the rule will be a JSON of anomaly type and content.

Muting rules in Network Insights

To mute an NDR Rule:

1. Go to *Network Insights* and open a page with the *Anomaly* Tab (*Botnet*, *FortiGuard IOC*, *Network Attacks*, *Weak/Vulnerable Communication*, *Encrypted Attack*, or *ML Discovery*).
2. Right-click a detection and select *Add to NDR Mute Rule*.

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*.
3. Next to *Status*, select *Enable* or *Disable*.

To delete multiple rules:

1. In the toolbar, click the *Delete Multiple* dropdown.
2. Select one of the following options:
   - *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 (*Low*, *Medium*, *High* or *Critical*).
Number of Features	The number of features enabled in the *Default* 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*.

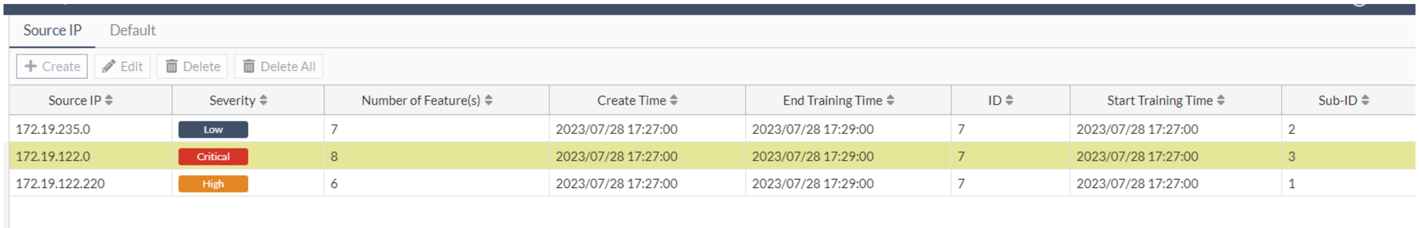
Source IP tab

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	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:

1. Go to *Virtual Security Analyst > ML Configuration*.
2. 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 *Low*, *Medium*, *High* or *Critical*.
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: • *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /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: • *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /16
Source Device MAC Address	Source device MAC address.
Destination Device Model	Device model such as: *FortiGate*, *Workstation*, *IDRAC*, etc.
Destination Device Geolocation	Device geographical country such as *United States*.
Destination Device Category	Device category such as: *NAS*, *Virtual Machine, Firewall*, etc.
Destination Device Vendor	Device vendor such as *VMware*, *Dell*, *Synology*, etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as *Windows*, *Linux*, etc.
Protocol and Application Behavior	
Transport Layer Protocol	UPD, ICMP, TCP, etc
Application Layer Protocol	TLS, HTTP, SMB, etc
Protocol/Application Behaviors/Action	Specific application actions such as. *Adobe Reader form creation*, *WebDAV reload*, *Wasabi file upload*, etc
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Source Port	Port number such as, *22*, *445*, *none reserved port*, 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: • *Baselining*:The current training is still in progress. • *Baseline ready*: The baseline training is done and is ready for anomaly detection.
ML Discovery Detection	Click to *Enable* or *Disable* 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 *Low*, *Medium*, *High* or *Critical*.
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: • *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /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:

	• *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /16
Source Device MAC Address	Source device MAC address.
Destination Device Model	Device model such as: *FortiGate*, *Workstation*, *IDRAC*, etc.
Destination Device Geolocation	Device geographical country such as *United States*.
Destination Device Category	Device category such as: *NAS*, *Virtual Machine, Firewall*, etc.
Destination Device Vendor	Device vendor such as *VMware*, *Dell*, *Synology*, etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as *Windows*, *Linux*, etc.
Protocol and Application Behavior	
Transport Layer Protocol	UPD, ICMP, TCP, etc
Application Layer Protocol	TLS, HTTP, SMB, etc
Protocol/Application Behaviors/Action	Specific application actions such as. *Adobe Reader form creation*, *WebDAV reload*, *Wasabi file upload*, etc
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Source Port	Port number such as, *22*, *445*, *none reserved port*, 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 *Close*.
Feature Enabled for Learning	
Default Feature Configuration	Click to enable the default ML configuration settings.
Severity	Select *Low*, *Medium*, *High* or *Critical*.
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: • *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /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: • *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /16
Source Device MAC Address	Source device MAC address.
Destination Device Model	Device model such as: *FortiGate*, *Workstation*, *IDRAC*, etc.
Destination Device Geolocation	Device geographical country such as *United States*.
Destination Device Category	Device category such as: *NAS*, *Virtual Machine, Firewall*, etc.
Destination Device Vendor	Device vendor such as *VMware*, *Dell*, *Synology*, etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as *Windows*, *Linux*, etc.
Protocol and Application Behavior	
Transport Layer Protocol	UPD, ICMP, TCP, etc
Application Layer Protocol	TLS, HTTP, SMB, etc
Protocol/Application Behaviors/Action	Specific application actions such as. *Adobe Reader form creation*, *WebDAV reload*, *Wasabi file upload*, etc
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: • Small: Less than 100 bytes

	• Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Source Port	Port number such as, *22*, *445*, *none reserved port*, etc.

Status	
Baseline Status	The current baseline training status: • *Baselining*:The current training is still in progress. • *Baseline ready*: The baseline training is done and is ready for anomaly detection.
ML Discovery Detection	Click to *Enable* or *Disable* 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 *Low*, *Medium*, *High* or *Critical*.
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: • *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /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: • *Do Not Apply Netmask*: This is the default. • *Apply Class C Netmask*: /24 • *Apply Class B Netmask:* /16
Source Device MAC Address	Source device MAC address.

Destination Device Model	Device model such as: *FortiGate*, *Workstation*, *IDRAC*, etc.
Destination Device Geolocation	Device geographical country such as *United States*.
Destination Device Category	Device category such as: *NAS*, *Virtual Machine, Firewall*, etc.
Destination Device Vendor	Device vendor such as *VMware*, *Dell*, *Synology*, etc.
Destination MAC Address	Destination device MAC address.
Destination Device OS	Device Operating system such as *Windows*, *Linux*, etc.
Protocol and Application Behavior	
Transport Layer Protocol	UPD, ICMP, TCP, etc
Application Layer Protocol	TLS, HTTP, SMB, etc
Protocol/Application Behaviors/Action	Specific application actions such as. *Adobe Reader form creation*, *WebDAV reload*, *Wasabi file upload*, etc
Others	
Session Packet Size	FortiNDR categorizes the packet size into 3 groups: • Small: Less than 100 bytes • Medium: 101- 99999 bytes • Larger: Equal to and greater than 100000 bytes
Destination Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Source Port	Port number such as, *22*, *445*, *none reserved port*, etc.

.

Retrain baseline

When the baseline becomes outdated, you can initiate retraining with the following the CLI command:

```
execute cleanup ml
```

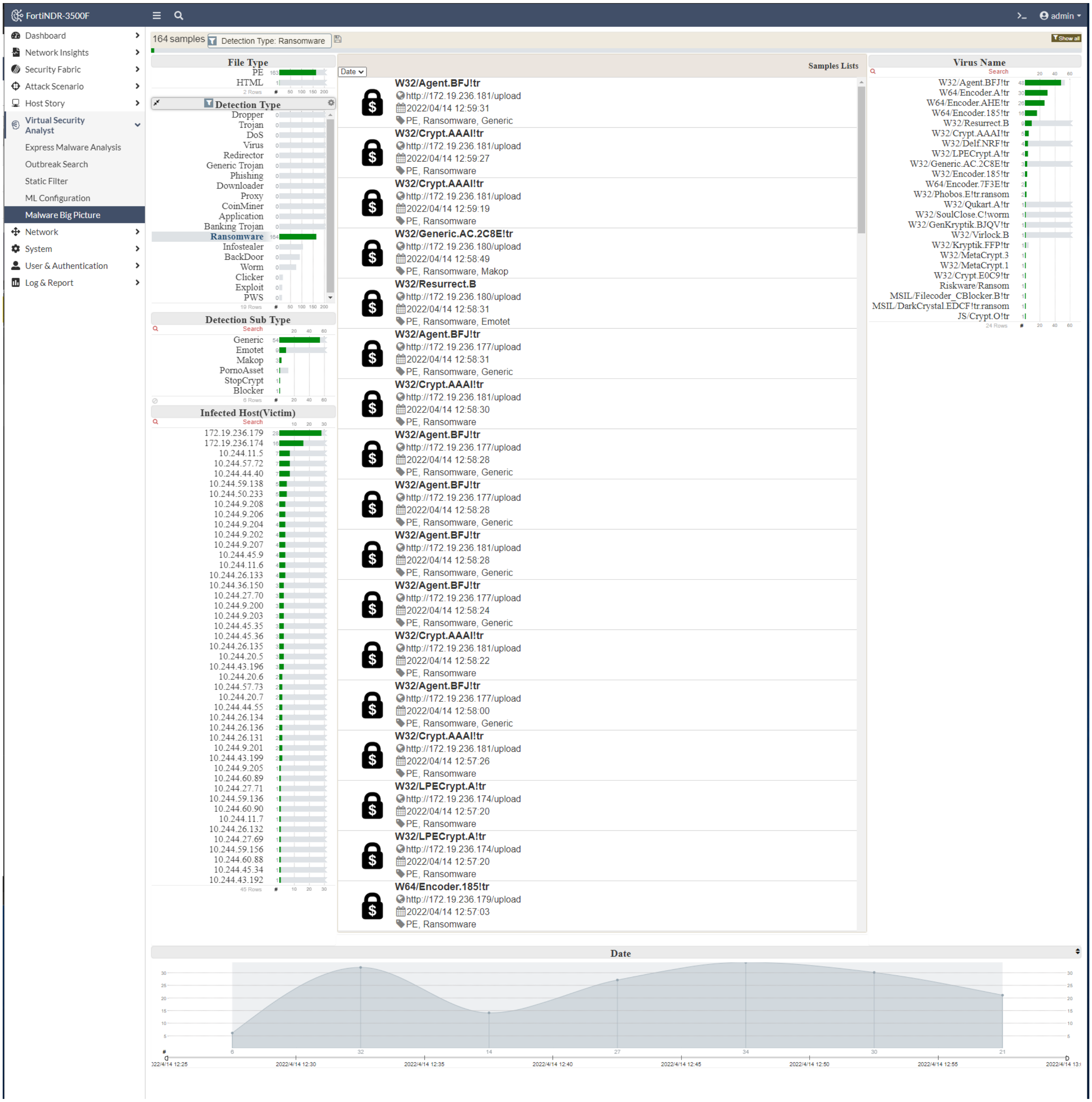
For information, see execute cleanup ml.

During the retraining process, ML detection will be temporarily disabled.

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.



164 samples Detection Type: Ransomware

File Type

PE	163
HTML	1

2 Rows

Detection Type

Dropper	0
Trojan	0
DoS	0
Virus	0
Redirector	0
Generic Trojan	0
Phishing	0
Downloader	0
Proxy	0
CoinMiner	0
Application	0
Banking Trojan	0
Ransomware	164
Infostealer	0
BackDoor	0
Worm	0
Clicker	0
Exploit	0
PWS	0

19 Rows

Detection Sub Type

Generic	54
Emotet	9
Makop	3
PornoAsset	1
StopCrypt	1
Blocker	1

6 Rows

Infected Host(Victim)

172.19.236.179	28
172.19.236.174	16
10.244.11.5	7
10.244.57.72	7
10.244.44.40	7
10.244.59.138	5
10.244.50.233	5
10.244.9.208	4
10.244.9.206	4
10.244.9.204	4
10.244.9.202	4
10.244.9.207	4
10.244.45.9	4
10.244.11.6	4
10.244.26.133	4
10.244.36.150	3
10.244.27.70	3
10.244.9.200	3
10.244.9.203	3
10.244.45.35	3
10.244.45.36	3
10.244.26.135	3
10.244.20.5	3
10.244.43.196	3
10.244.20.6	2
10.244.57.73	2
10.244.20.7	2
10.244.44.55	2
10.244.26.134	2
10.244.26.136	2
10.244.26.131	2
10.244.9.201	2
10.244.43.199	2
10.244.9.205	1
10.244.60.89	1
10.244.27.71	1
10.244.59.136	1
10.244.60.90	1
10.244.11.7	1
10.244.26.132	1
10.244.27.69	1
10.244.59.156	1
10.244.60.88	1
10.244.45.34	1
10.244.43.192	1

45 Rows

Samples Lists

Date

W32/Agent.BFJ!tr
http://172.19.236.181/upload
2022/04/14 12:59:31
PE, Ransomware, Generic

W32/Crypt.AAAI!tr
http://172.19.236.181/upload
2022/04/14 12:59:27
PE, Ransomware

W32/Crypt.AAAI!tr
http://172.19.236.181/upload
2022/04/14 12:59:19
PE, Ransomware

W32/Generic.AC.2C8E!tr
http://172.19.236.180/upload
2022/04/14 12:58:49
PE, Ransomware, Makop

W32/Resurrect.B
http://172.19.236.180/upload
2022/04/14 12:58:31
PE, Ransomware, Emotet

W32/Agent.BFJ!tr
http://172.19.236.177/upload
2022/04/14 12:58:31
PE, Ransomware, Generic

W32/Crypt.AAAI!tr
http://172.19.236.181/upload
2022/04/14 12:58:30
PE, Ransomware

W32/Agent.BFJ!tr
http://172.19.236.177/upload
2022/04/14 12:58:28
PE, Ransomware, Generic

W32/Agent.BFJ!tr
http://172.19.236.177/upload
2022/04/14 12:58:28
PE, Ransomware, Generic

W32/Agent.BFJ!tr
http://172.19.236.181/upload
2022/04/14 12:58:28
PE, Ransomware, Generic

W32/Agent.BFJ!tr
http://172.19.236.177/upload
2022/04/14 12:58:24
PE, Ransomware, Generic

W32/Crypt.AAAI!tr
http://172.19.236.181/upload
2022/04/14 12:58:22
PE, Ransomware

W32/Agent.BFJ!tr
http://172.19.236.177/upload
2022/04/14 12:58:00
PE, Ransomware, Generic

W32/Crypt.AAAI!tr
http://172.19.236.181/upload
2022/04/14 12:57:26
PE, Ransomware

W32/LPECrypt.A!tr
http://172.19.236.174/upload
2022/04/14 12:57:20
PE, Ransomware

W32/LPECrypt.A!tr
http://172.19.236.174/upload
2022/04/14 12:57:20
PE, Ransomware

W64/Encoder.185!tr
http://172.19.236.179/upload
2022/04/14 12:57:03
PE, Ransomware

Virus Name

W32/Agent.BFJ!tr	48
W64/Encoder.A!tr	30
W64/Encoder.AHE!tr	26
W64/Encoder.185!tr	16
W32/Resurrect.B	9
W32/Crypt.AAAI!tr	5
W32/Delf.NRF!tr	4
W32/LPECrypt.A!tr	4
W32/Generic.AC.2C8E!tr	3
W32/Encoder.185!tr	3
W64/Encoder.7F3E!tr	2
W32/Phobos.E!tr.ransom	2
W32/Qukart.A!tr	1
W32/SoulClose.C!worm	1
W32/GenKryptik.BJQV!tr	1
W32/Virlock.B	1
W32/Kryptik.FFP!tr	1
W32/MetaCrypt.3	1
W32/MetaCrypt.1	1
W32/Crypt.E0C9!tr	1
Riskware/Ransom	1
MSIL/Filecoder_CBlocker.B!tr	1
MSIL/DarkCrystal.EDCF!tr.ransom	1
JS/Crypt.O!tr	1

24 Rows

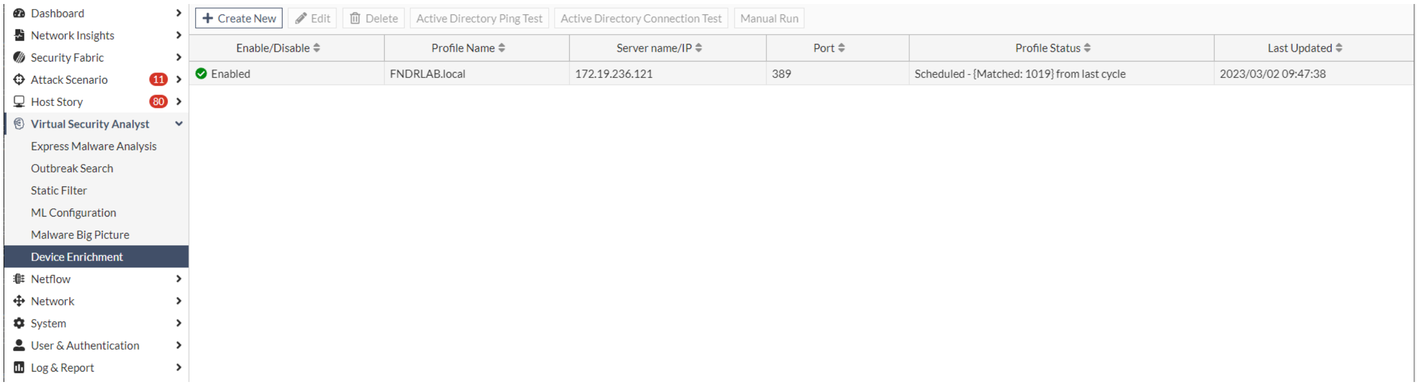
Date

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.



Enable/Disable	Profile Name	Server name/IP	Port	Profile Status	Last Updated
✓ Enabled	FNDRLAB.local	172.19.236.121	389	Scheduled - {Matched: 1019} from last cycle	2023/03/02 09:47:38

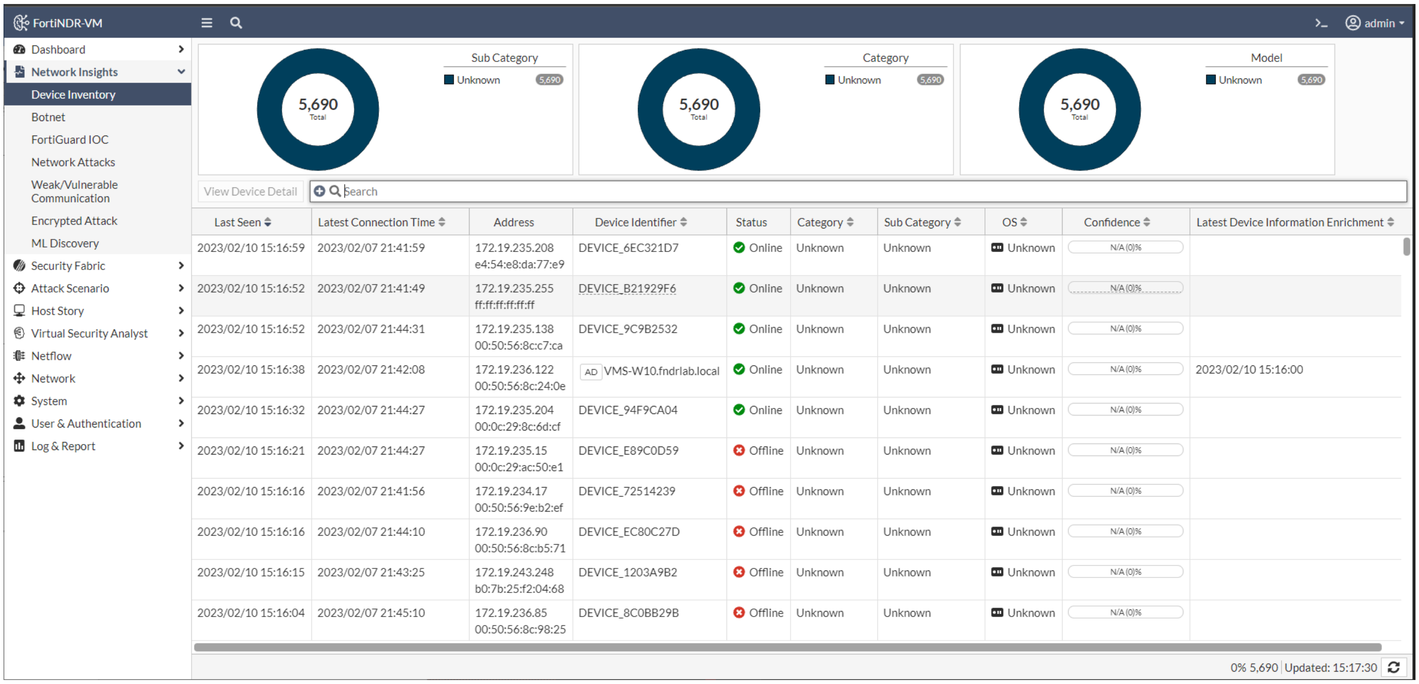
The *Device Enrichment* page displays the following information:

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

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.



Last Seen	Latest Connection Time	Address	Device Identifier	Status	Category	Sub Category	OS	Confidence	Latest Device Information Enrichment
2023/02/10 15:16:59	2023/02/07 21:41:59	172.19.235.208 e4:54:e8:da:77:e9	DEVICE_6EC321D7	✓ Online	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:52	2023/02/07 21:41:49	172.19.235.255 ff:ff:ff:ff:ff:ff	DEVICE_B21929F6	✓ Online	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:52	2023/02/07 21:44:31	172.19.235.138 00:50:56:8c:c7:ca	DEVICE_9C9B2532	✓ Online	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:38	2023/02/07 21:42:08	172.19.236.122 00:50:56:8c:24:0e	AD VMS-W10.fndrlab.local	✓ Online	Unknown	Unknown	Unknown	N/A (0)%	2023/02/10 15:16:00
2023/02/10 15:16:32	2023/02/07 21:44:27	172.19.235.204 00:0c:29:8c:6d:cf	DEVICE_94F9CA04	✓ Online	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:21	2023/02/07 21:44:27	172.19.235.15 00:0c:29:ac:50:e1	DEVICE_E89C0D59	✕ Offline	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:16	2023/02/07 21:41:56	172.19.234.17 00:50:56:9e:b2:ef	DEVICE_72514239	✕ Offline	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:16	2023/02/07 21:44:10	172.19.236.90 00:50:56:8c:b5:71	DEVICE_EC80C27D	✕ Offline	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:15	2023/02/07 21:43:25	172.19.243.248 b0:7b:25:f2:04:68	DEVICE_1203A9B2	✕ Offline	Unknown	Unknown	Unknown	N/A (0)%	
2023/02/10 15:16:04	2023/02/07 21:45:10	172.19.236.85 00:50:56:8c:98:25	DEVICE_8C0BB29B	✕ Offline	Unknown	Unknown	Unknown	N/A (0)%	

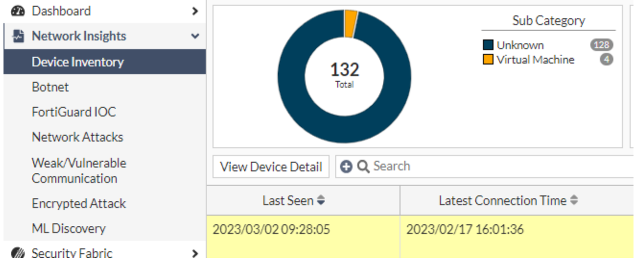
0% 5,690 | Updated: 15:17:30

Overwriting the device identifier

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

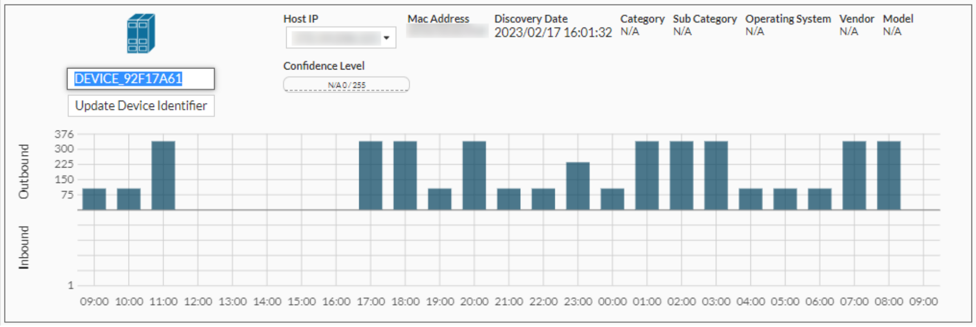
To overwrite the device identifier:

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



Last Seen	Latest Connection Time
2023/03/02 09:28:05	2023/02/17 16:01:36

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



Host IP	Mac Address	Discovery Date	Category	Sub Category	Operating System	Vendor	Model
[redacted]	[redacted]	2023/02/17 16:01:32	N/A	N/A	N/A	N/A	N/A

DEVICE_92F17A61

Update Device Identifier

Confidence Level: N/A 0 / 255

Creating a Device Enrichment Profile

To create a Device Enrichment profile:

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

3. Configure the profile settings.

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

4. Click *OK*.

Active Directory Profile Actions

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

Active Directory Server Ping Test	Ping the Active Directory (AD) server and port in the Device Enrichment Profile.
Active Directory Server Connection Test	Verify the *Microsoft Active Directory Connection Settings* by attempting to connect the AD server.

Active Directory Server Manual Run	Execute the selected Device Enrichment Profile . The result will be shown as a notification on the bottom left.

Netflow

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

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

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

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

To turn NetFlow on/off with the CLI:

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

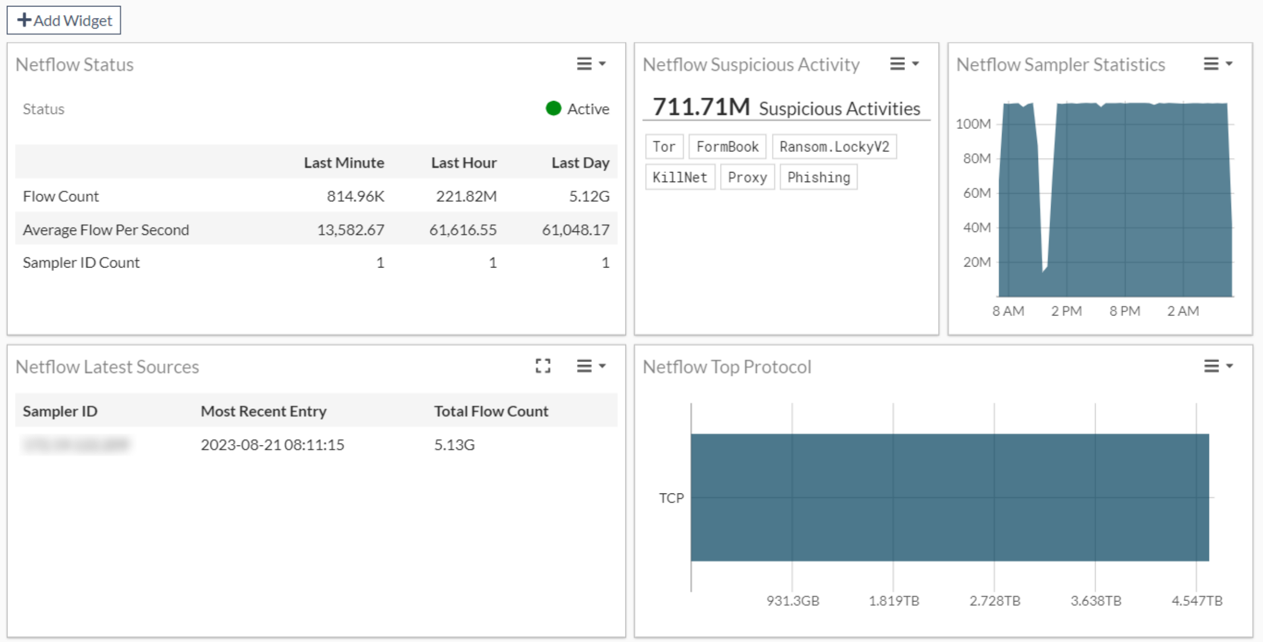
NetFlow ports

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

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

Netflow Dashboard

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



Netflow Status

Status ● Active

	Last Minute	Last Hour	Last Day
Flow Count	814.96K	221.82M	5.12G
Average Flow Per Second	13,582.67	61,616.55	61,048.17
Sampler ID Count	1	1	1

Netflow Suspicious Activity

711.71M Suspicious Activities

Tor FormBook Ransom.LockyV2 KillNet Proxy Phishing

Netflow Sampler Statistics

Netflow Latest Sources

Sampler ID	Most Recent Entry	Total Flow Count
[redacted]	2023-08-21 08:11:15	5.13G

Netflow Top Protocol

The *Netflow Dashboard* contains the following widgets:

Netflow Status	Displays the *Status* of this feature , *Flow Count*, *Average Flow Per Second* and *Sampler ID Count*. The statistics are broken down into last minute, hour, and day for users to view the volume and flow count coming into FortiNDR.
Netflow 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 *Top Talker* feature provides a method to identify the devices or IP addresses that are consuming the most bandwidth, allowing network administrators to troubleshoot performance issues and optimize network usage.
Netflow Top Protocol	Displays the most used transportation layer protocols in terms of bandwidth consumption. Protocols can include TCP, UDP, ICMP, among others. The *Top Protocols* feature provides a method for understanding which protocols are using the most bandwidth, helping network administrators optimize network usage and potentially identify security concerns.
Netflow Latest Sources	Displays the Flow activity statistics from active samplers within a selected time frame. The widget allows users to select one day, one week, or one month.
Netflow Traffic Volume	Displays aggregated Ingress and Egress traffic volume of each Sampler within a selected time frame. For example, if sampler ID *1.1.1.1* has flows from different source(s) and destination (s), the widget will summarize the total ingress and egress traffic.

Customizing the Netflow Dashboard

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

To remove a widget from the dashboard:

Click the widget menu and select *Remove*.

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

To add a widget to the dashboard:

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

To re-size a widget in the dashboard:

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

Netflow Log

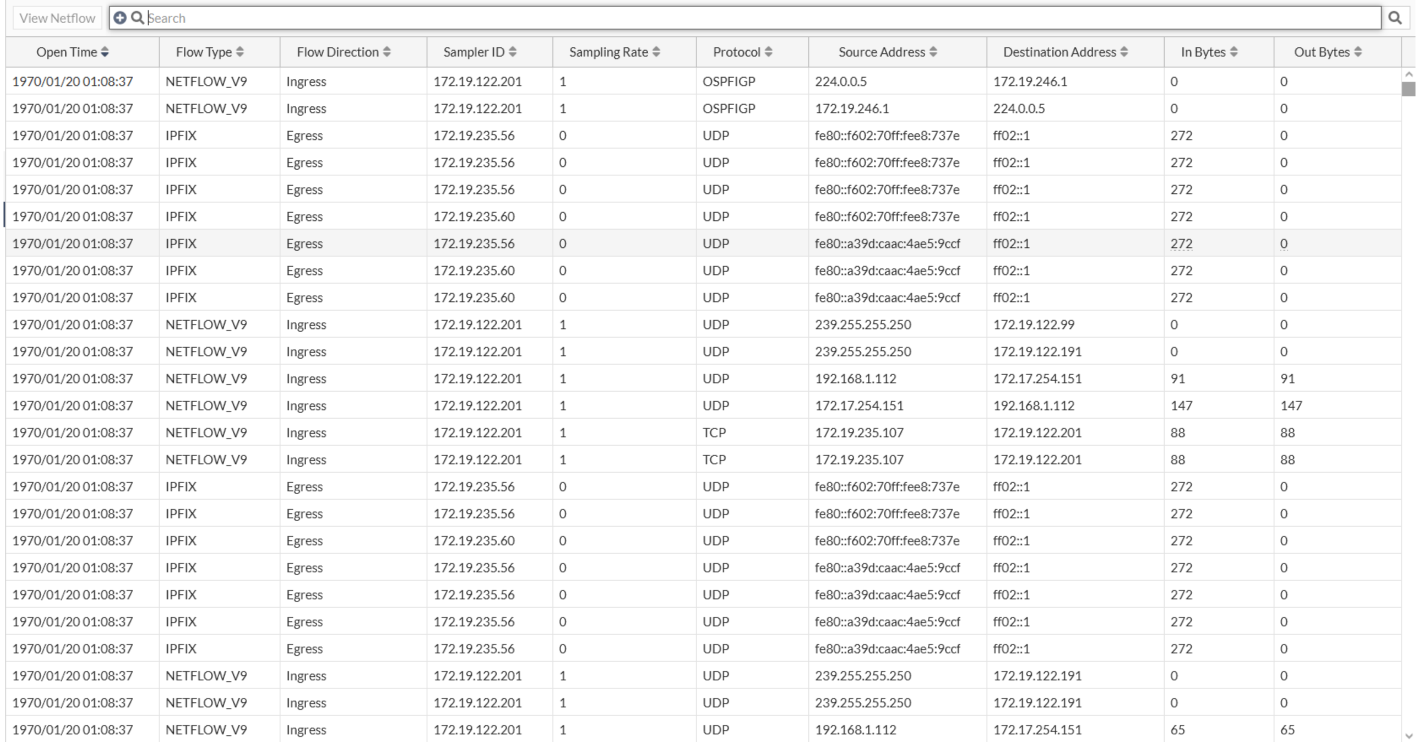
Netflow Log shows the logs FortiNDR collected. In Center mode, the *Netflow Log* displays the data collated from the Sensors.

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.

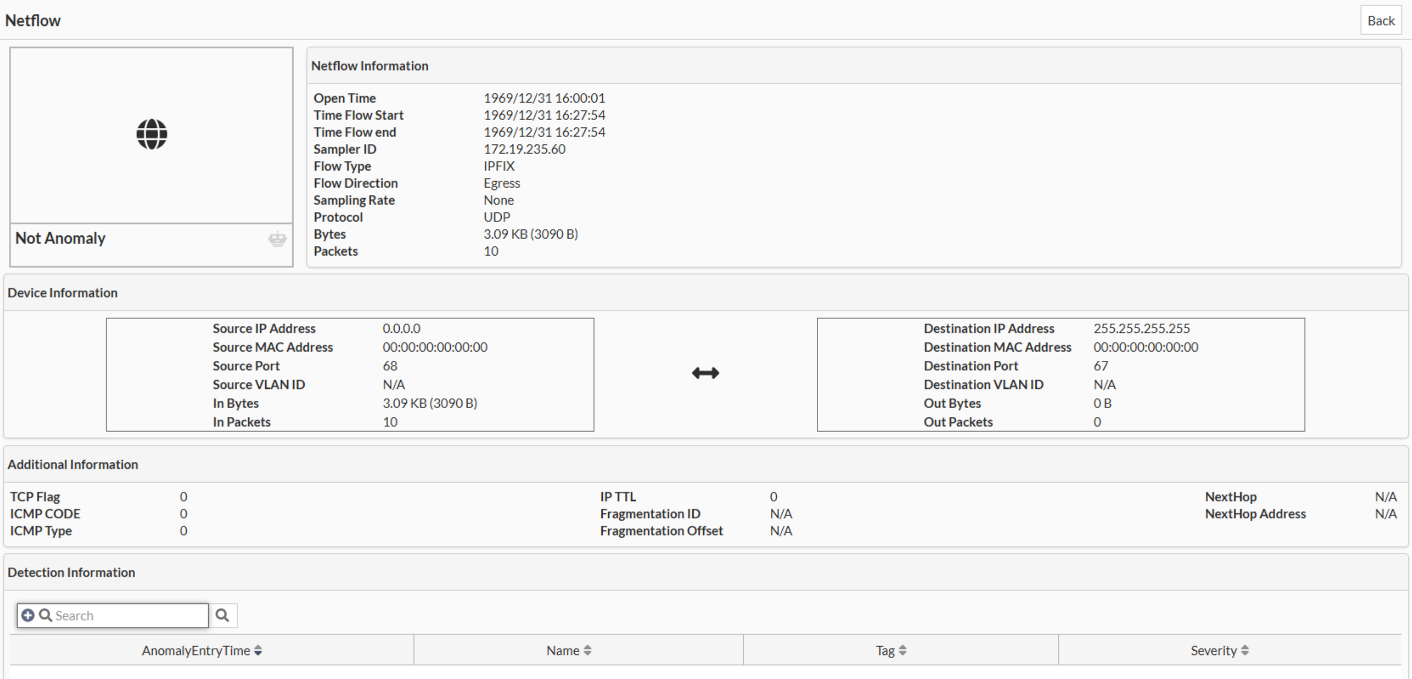
You may notice some columns are have *0*s in them. This means this column is not applicable to that type of flow or the sampler/exporter is not configured to send this field to FortiNDR. For example, NetFlow_v5 does not include *Destination MAC*, so you will see `00:00:00:00:00:00` in the *NetFlow_v5*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



Open Time	Flow Type	Flow Direction	Sampler ID	Sampling Rate	Protocol	Source Address	Destination Address	In Bytes	Out Bytes
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	OSPFIGP	224.0.0.5	172.19.246.1	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	OSPFIGP	172.19.246.1	224.0.0.5	0	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.99	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.191	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	192.168.1.112	172.17.254.151	91	91
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	172.17.254.151	192.168.1.112	147	147
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	TCP	172.19.235.107	172.19.122.201	88	88
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	TCP	172.19.235.107	172.19.122.201	88	88
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.191	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.191	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	192.168.1.112	172.17.254.151	65	65

Viewing anomalies

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



Netflow Information

Open Time	1969/12/31 16:00:01
Time Flow Start	1969/12/31 16:27:54
Time Flow end	1969/12/31 16:27:54
Sampler ID	172.19.235.60
Flow Type	IPFIX
Flow Direction	Egress
Sampling Rate	None
Protocol	UDP
Bytes	3.09 KB (3090 B)
Packets	10

Device Information

Source IP Address	0.0.0.0
Source MAC Address	00:00:00:00:00:00
Source Port	68
Source VLAN ID	N/A
In Bytes	3.09 KB (3090 B)
In Packets	10

Destination IP Address	255.255.255.255
Destination MAC Address	00:00:00:00:00:00
Destination Port	67
Destination VLAN ID	N/A
Out Bytes	0 B
Out Packets	0

Additional Information

TCP Flag	0	**IP TTL**	0	**NextHop**	N/A
ICMP CODE	0	**Fragmentation ID**	N/A	**NextHop Address**	N/A
ICMP Type	0	**Fragmentation Offset**	N/A		

Detection Information

AnomalyEntryTime	Name	Tag	Severity

The anomalies page displays the following information:

Not Anomaly/Anomaly	Indicates if FortiNDR determined the session to be an anomaly.
Netflow Information	Displays information about the sessions duration, Sampler ID, the flow type, direction and rate, as well as the protocol and the number of bytes and packages.
Device information	Displays information about the flow source and destination including the IP and MAC addresses, ports, VLAN ID and the number of bytes and packages.
Additional Information	Displays information about TCP, ICMP Fragmentation and NextHop.
Detection Information	Displays the *Anomaly Entry Time*, *Name* , *Tag* and *Severity*.

Network

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

Interface

FortiNDR has the following preset ports which cannot be changed. For more information about port configuration, see *Initial setup > Ports*.

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)

Only Super Admin users can access the CLI using SSH. For more information, see Admin Profiles.

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.

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.

In 7.4.6 and earlier, some administrators without *SuperAdminProfile* permissions, will not see the correct sensor data, nor will they be able to arrange the widgets in the *Dashboard*. To ensure an administrator account is seeing the correct sensor data, the admin profile linked to the administrator account is required to have *System Access* set to *Read/Write* permissions. For more information, see Creating remote wildcard administrators.

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	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	From the dropdown select one of the following: • Local • RADIUS • Local Plus RADIUS • LDAP
Password	Enter a password for the administrator.
Confirm Password	Re-enter the administrator password.
Preference	

Theme	Select a them for the administrator. The following options are available: • Neutrino • Jade • Mariner • Graphite • Melongene • Cloud App Light • Onyx • Dark Matter • Eclipse • Cloud App Dark
Restrict login to trusted hosts	Enable to add a trusted host.

Password policy

Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. For example, if `p4ssw0rd` is used as a password, it can be cracked.

Using secure passwords is vital for preventing unauthorized access to your FortiNDR. When changing the password, consider the following to ensure better security:

- Do not use passwords that are obvious, such as the company name, administrator names, or other obvious words or phrases.
- Use numbers in place of letters, for example: `passw0rd`.
- Administrator passwords can be up to 64 characters.
- Include a mixture of numbers, symbols, and upper and lower case letters.
- Use multiple words together, or possibly even a sentence, for example: `correcthorsebatterystaple`.
- Use a password generator.
- Change the password regularly and always make the new password unique and not a variation of the existing password. for example, do not change from `password` to `password1`.
- Make note of the password and store it in a safe place away from the management computer, in case you forget it; or ensure at least two people know the password in the event one person becomes unavailable. Alternatively, have two different admin logins.

FortiNDR allows you to create a password policy for administrators and IPsec pre-shared keys. With this policy, you can enforce regular changes and specific criteria for a password policy, including:

- The minimum length, between 8 and 64 characters.
- If the password must contain:
  - Uppercase (A, B, C) and/or lowercase (a, b, c) characters
  - Numbers (1, 2, 3)
  - Special or non-alphanumeric characters: !, @, #, $, %, ^, &, *,
- Where the password applies (admin or IPsec or both).
- The duration of the password before a new one must be specified.
- The minimum number of unique characters that a new password must include.

If you add a password policy or change the requirements on an existing policy, the next time that administrator logs into the FortiNDR, the administrator is prompted to update the password to meet the new requirements before proceeding to log in.

To create a system password policy the CLI:

```
config sys password-policy
config system password-policy
   set status enable
   set apply-to admin-user
   set minimum-length 8
   set must-contain upper-case-letter lower-case-letter number non-alphanumeric
end
```

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:

- *OperatorProfile*: Can view certain pages. This profile cannot change any system settings.
- *SuperAdminProfile*: All functionalities are accessible.

LDAP and RADIUS admin profiles:
You can use *Admin Profiles* to specify the sensors for LDAP and RADIUS administrators. However, without *SuperAdminProfile* permissions, some administrators will not see the correct sensor data, nor will they be able to arrange the widgets in the *Dashboard*. For more information, see Creating remote wildcard administrators.

Access Permissions

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

Access Permissions	Operator Profile	SuperAdminProfile
System status	Read	Read/Write
System Access	None	Read/Write
System Configuration	None	Read/Write

Access Permissions	Operator Profile	SuperAdminProfile
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, *Network*, *Administrators*, *Admin Profiles*, *Certificates*, and RADIUS/LDAP authentication.
System Access	Grant permission to modify other system settings such as system time settings, system FortiGuard update, and *Security Fabric* 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 *Virtual Security Analyst* such as *Express Malware Analysis*, *Outbreak Search*, *Static Filter*, *NDR Muting*, *ML Configuration*, *Malware Big Picture* and *Device Enrichment*.

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 (- Center - Standalone)

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.

<table>
<tr><td></td><td><b>Registered</b></td><td>Indicates that the Sensor has completed the registration process but has yet to undergo a license check.</td></tr>
<tr><td></td><td><b>Connected</b></td><td>Indicates the Sensor is prepared for synchronization and is actively transmitting data to the Center.</td></tr>
<tr><td></td><td><b>No Data Transferred</b></td><td>Indicates the Sensor has not sent any data to the Center for a span of 3 minutes while still maintaining a connection.</td></tr>
<tr><td></td><td><b>Firmware Mismatched</b></td><td>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.</td></tr>
<tr><td></td><td><b>Sensor License Invalid</b></td><td>Indicates that the Sensor does not possess a valid license, and has been disabled.</td></tr>
<tr><td></td><td><b>Disabled By User</b></td><td>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.</td></tr>
<tr><td><b>FortiGuard Status</b></td><td colspan="2">Compares the Sensor’s FortiGuard updates against the Center’s FortiGuard updates. <i>FortiGuard Update Available</i> will appear if an update is required.</td></tr>
<tr><td><b>Last Updated</b></td><td colspan="2">The date the sensor was last updated.</td></tr>
<tr><td><b>CPU Usage</b></td><td colspan="2">The CPU usage as a percentage.</td></tr>
<tr><td><b>Disk Usage</b></td><td colspan="2">The disk usage as a percentage.</td></tr>
<tr><td><b>Memory Usage</b></td><td colspan="2">The memory usage as a percentage.</td></tr>
</table>

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 *disabled*, preventing the Center from receiving further data. However, the historical data from the Sensor is retained.
Activate Senor	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. *FortiGuard Update Available* 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*.

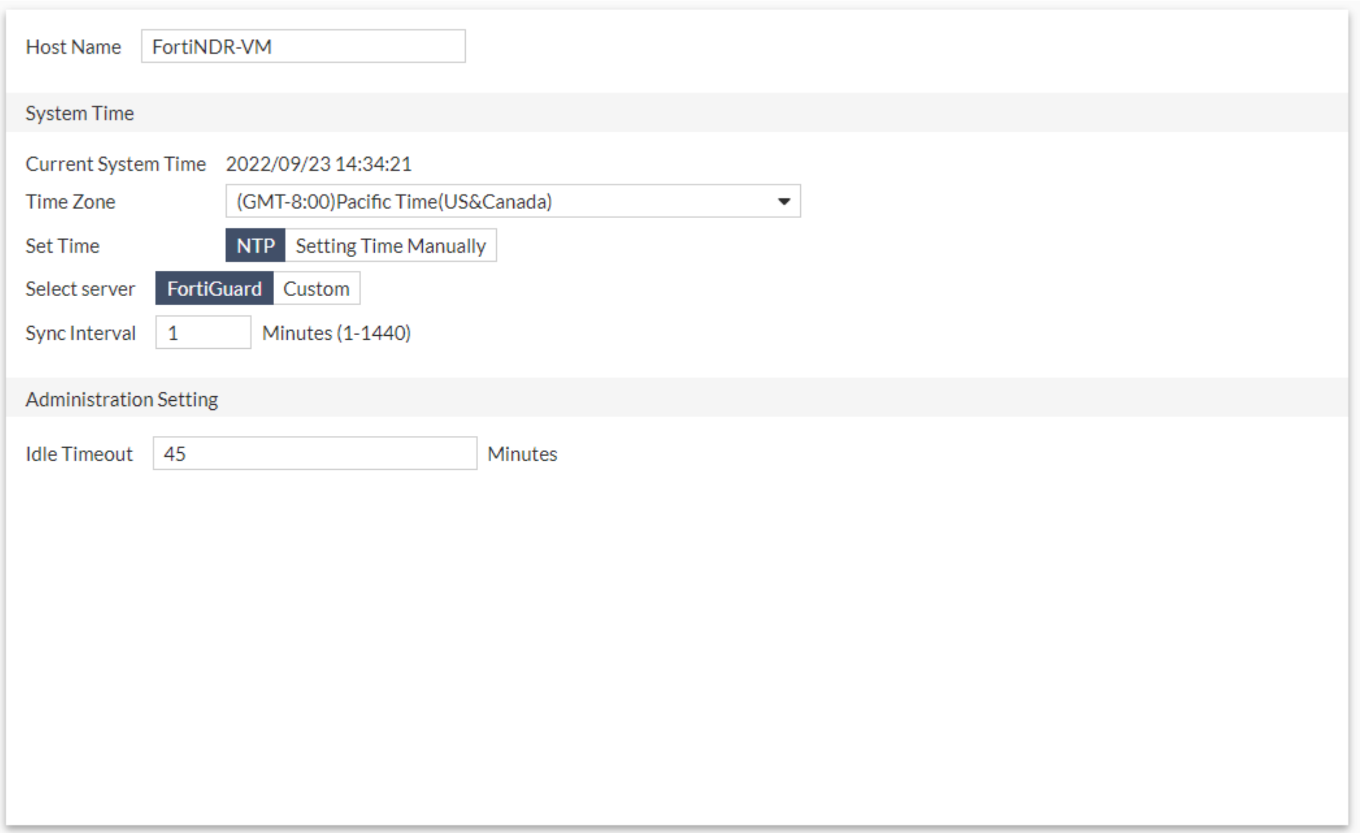
Settings

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 *NTP* or select *Setting Time Manually* and then enter the *Date* and *Time*.
Select Server	Select *FortiGuard* or select *Custom* to add or remover the *Server*.
Sync Interval	Select a value between 1-1440 minutes.
Administration Setting	
Idle Timeout	Enter the idle timeout value in minutes.



Host Name FortiNDR-VM

System Time

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

Time Zone (GMT-8:00)Pacific Time(US&Canada)

Set Time NTP Setting Time Manually

Select server FortiGuard Custom

Sync Interval 1 Minutes (1-1440)

Administration Setting

Idle Timeout 45 Minutes

SNMP

FortiNDR system information and system status can be monitored by utilizing SNMP. When configuring SNMP manager to connect to FortiNDR's SNMP agent, you must add the Fortinet proprietary MIBs to have access to Fortinet specific information.

The FortiNDR SNMP implementation is read-only. SNMP v1, v2c and v3 compliant SNMP managers have read-only access to FortiNDR system information and can receive FortiNDR traps.

Basic Configuration

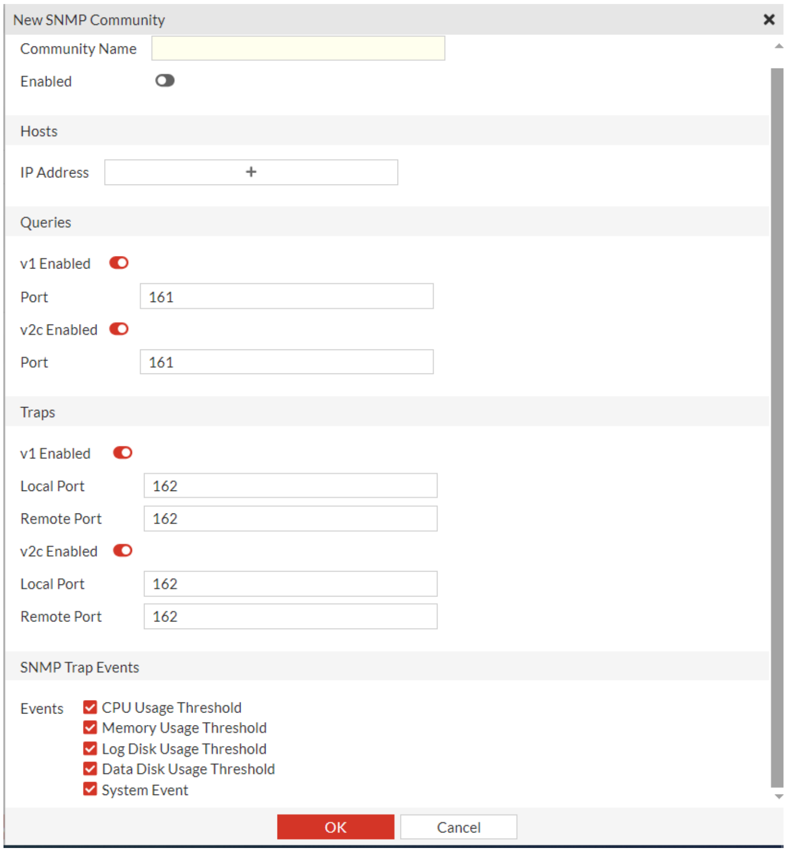
To configure SNMP in the GUI:

1. Configure interface access:
   - **a.** Go to *Network > Interface* and double-click the *port1* interface to edit it.
   - **b.** Under *Administrative Access*, enable *SNMP*.
   - **c.** Click *OK*.
2. Configure the SNMP agent:
   - **a.** Enable *SNMP Agent* and configure the following settings:

Description	Description of the SNMP agent.
Location	The location of the FortiNDR.
Contact	Contact for the SNMP agent or FortiNDR.

   - **b.** Click *Apply*.
3. Configure an SNMP V1/V2C community:
   - **a.** In the *SNMP V1/V2C* table, click *Create New*. The *New SNMP Community* pane opens.
   - **b.** Configure the community:

Community Name	Enter the name of the community.
Hosts	*IP Address*: Click the plus sign (**+**) to enter the IP address for each SNMP manager.
Queries	Enable or disable v1 and v2c queries, then enter the port numbers that the SNMP managers in this community will use.
Traps	Enable or disable v1 and v2c traps, then enter the local and remote port numbers that the SNMP managers in this community will use.
SNMP Trap Events	Enable or disable the events that activate traps in this community.



New SNMP Community

Community Name:

Enabled: ○

Hosts

IP Address: +

Queries

v1 Enabled: ●

Port: 161

v2c Enabled: ●

Port: 161

Traps

v1 Enabled: ●

Local Port: 162

Remote Port: 162

v2c Enabled: ●

Local Port: 162

Remote Port: 162

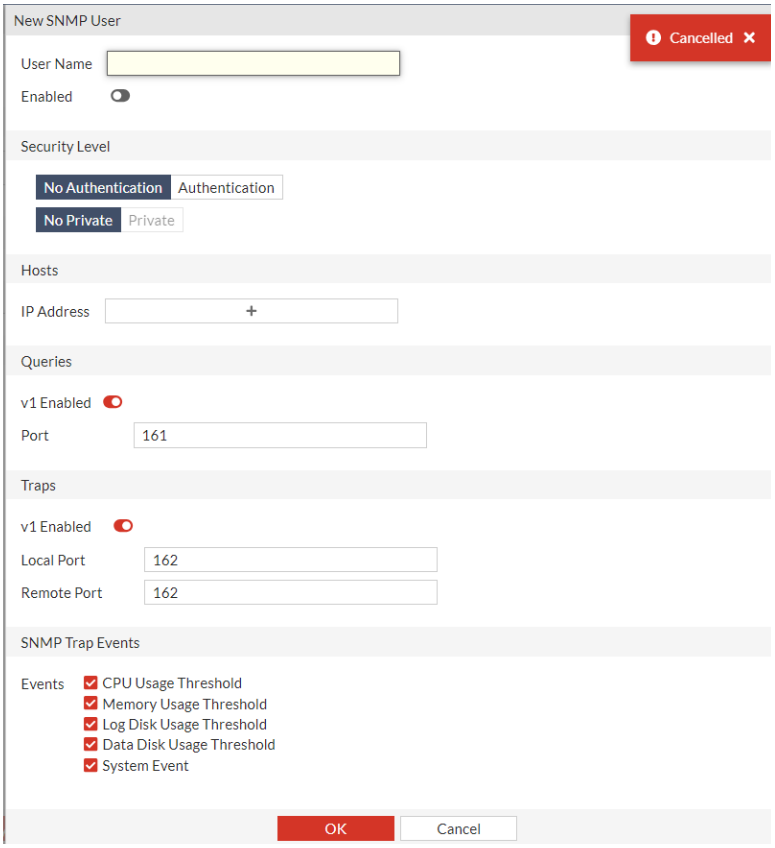
SNMP Trap Events

Events:
- ☑ CPU Usage Threshold
- ☑ Memory Usage Threshold
- ☑ Log Disk Usage Threshold
- ☑ Data Disk Usage Threshold
- ☑ System Event

 c. Click *OK*.

4. Configure an *SNMP v3* user:
   a. In the *SNMP v3* table, click *Create New*. The *New SNMP User* pane opens.
   b. Configure the user settings:

User Name	Enter the user name.
Security Level	Configure the security level: • *No Authentication*: No authentication or encryption. • *Authentication*: Select the authentication algorithm and password. • *Authentication* and *Private*: Select both the authentication and encryption algorithms and password.
Hosts	*IP Address*: Click the plus sign (**+**) to enter the IP address for each SNMP manager.
Queries	Enable or disable queries, then enter the port number that the SNMP managers will use.
Traps	Enable or disable traps, then enter the local and remote port numbers that the SNMP managers will use.
SNMP Trap Events	Enable or disable the events that activate traps.



New SNMP User

Cancelled ✕

User Name

Enabled ○

Security Level

[✓ No Authentication] Authentication

[✓ No Private] Private

Hosts

IP Address +

Queries

v1 Enabled ●

Port 161

Traps

v1 Enabled ●

Local Port 162

Remote Port 162

SNMP Trap Events

Events
- ☑ CPU Usage Threshold
- ☑ Memory Usage Threshold
- ☑ Log Disk Usage Threshold
- ☑ Data Disk Usage Threshold
- ☑ System Event

c. Click *OK*.

SNMP MIB files

The FortiNDR SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiNDR unit configuration.

The FortiNDR MIBs are listed in the following table. You can obtain these MIB files from Fortinet Technical Support. To communicate with the SNMP agent, you must load these MIBs into your SNMP manager.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you do not have to compile them again.

MIB file name	Description
FORTINET-CORE-MIB.mib	The Fortinet core MIB includes all system configuration and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet device settings and receive traps from the FortiNDR SNMP agent.

MIB file name	Description
FORTINET-FORTINDR-MIB.mib	The FortiNDR MIB includes all system configuration and trap information that is specific to FortiNDR product. Your SNMP manager requires this information to receive traps from the FortiNDR SNMP agent.

SNMP Traps

FortiNDR supports the following SNMP traps that will be sent to SNMP managers. To receive traps, you must pre-load the FortiNDR trap MIB into the SNMP manager.

Trap	Description
fndrTrapCpuHighThreshold	Trap sent if CPU usage became too high.
fndrTrapMemLowThreshold	Trap sent if memory usage became too high.
fndrTrapLogDiskHighThreshold	Trap sent if log disk usage became too high.
fndrTrapDataDiskHighThreshold	Trap sent if data disk usage became too high.

Example:

The following is an example of how to configure the trap threshold with the CLI. For more information, see config system snmp threshold in the *FortiNDR CLI Reference*.

```
config system snmp threshold
   set cpu 80 3 600 30
   set mem 80 3 600 30
   set logdisk 90 1 7200 3600
   set datadisk 90 1 7200 3600
end
```

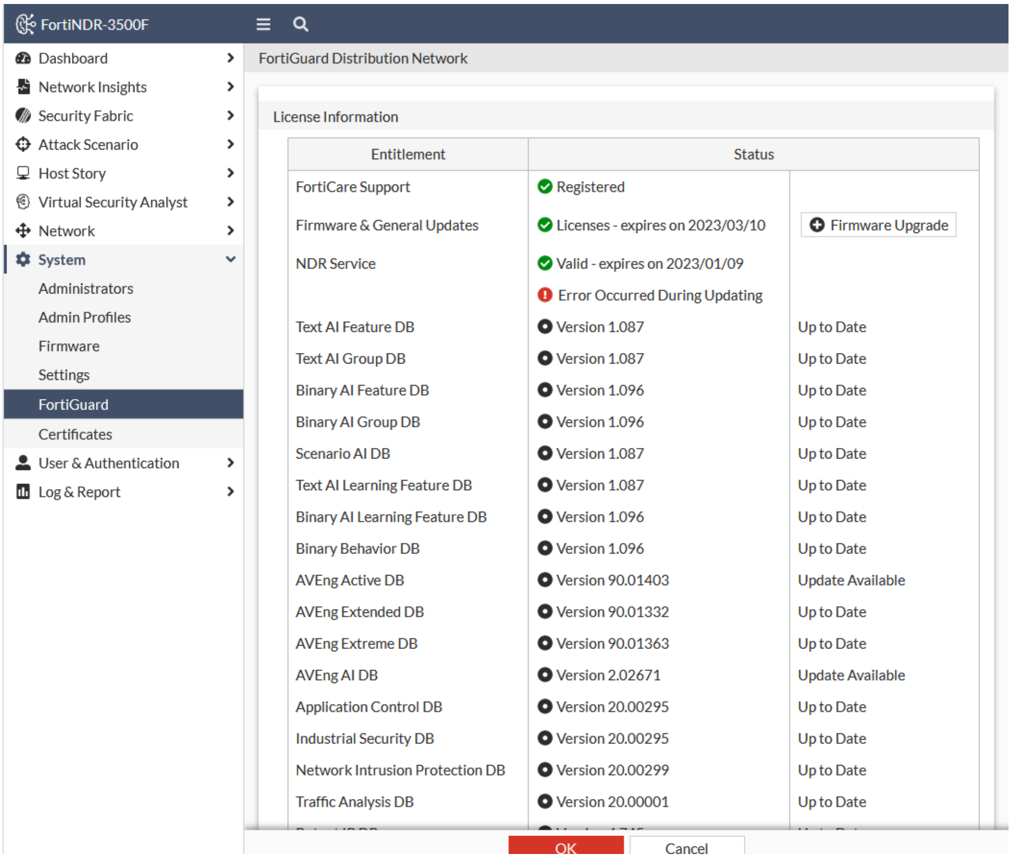
FortiGuard

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 267. 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 267 and CLI guide for more detail.



License Information

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

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

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

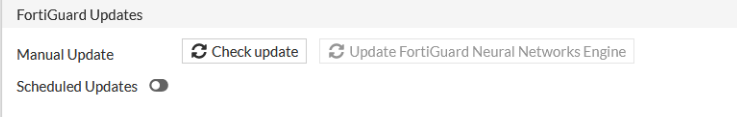
Currently, FortiNDR retrieves ANN updates from US and EMEA FortiGuard servers.

FortiNDR selects the update server based on proximity and location.

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

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

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



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

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

To update the ANN database using the CLI:

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

   There is only one `moat_kdb.tar.gz` because it is small and doesn't have to be split. After downloading them for the `pae_kdb`, unzip them into `pae_kdb.tar.gz`.
2. Unzip the downloaded files to `pae_kdb.tar.gz` and `moat_kdb.tar.gz`.
   In Windows:
   - **a.** `copy /B pae_kdb.zip.* pae_kdb.zip`
   - **b.** Right-click the `pae_kdb.zip` package and click *Extract All*.

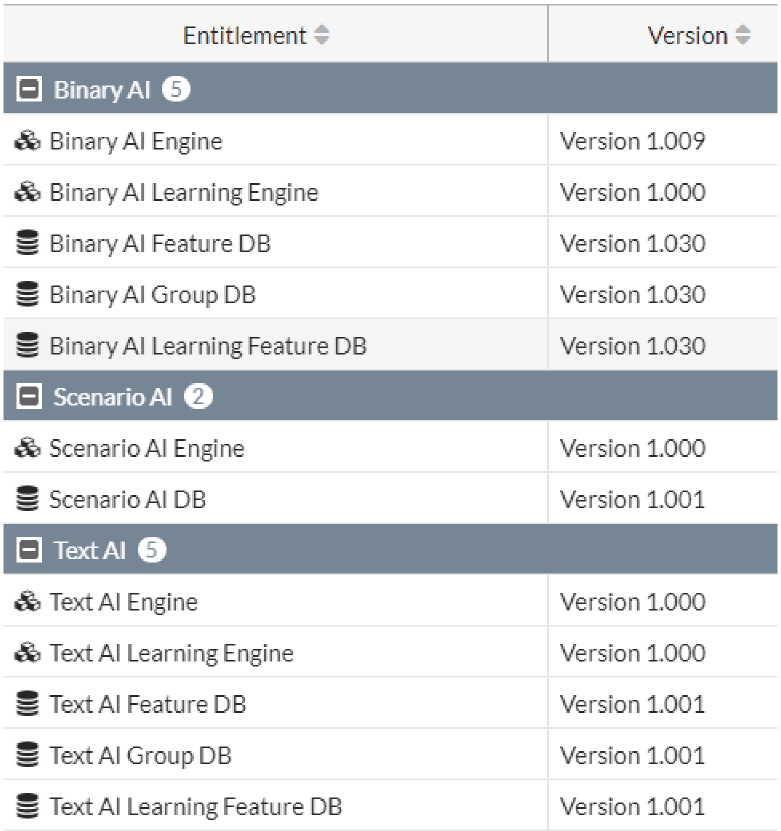
   In Linux:
   - **a.** `cat pae_kdb.zip.* > pae_kdb.zip`
   - **b.** `unzip pae_kdb.zip`
3. Put `pae_kdb.tar.gz` and `moat_kdb.tar.gz` on a disk that FortiNDR can access, such as a TFTP or FTP server, or a USB drive.
   If you use a USB drive, ensure its format is ext3 compatible, has only one partition, and the file is in the root directory.
4. Use the CLI command `execute restore kdb` to update the kdbs. Run this command once for `pae_kdb.tar.gz` and once for `pae_kdb.tar.gz`.
   For example, if `pae_kdb.tar.gz` and `moat_kdb.tar.gz` are in the FTP (IP:2.2.2.2) home folder of `/home/user/pae_kdb.tar.gz` and `/home/user/moat_kdb.tar.gz`, then use these commands:

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

   This is an example of the output:

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

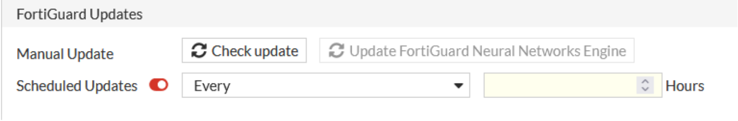
5. Go to *System > FortiGuard* to verify the updated versions.



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

To schedule FortiGuard updates:

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



FortiGuard Updates

Manual Update: Check update | Update FortiGuard Neural Networks Engine

Scheduled Updates: ● Every ▾ | Hours

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

FDS server override

In special cases such as network connection problems, there may be a need to force FDS updates to go to a specific server or a set of specific servers instead of the default ones. By default, the FDS updates will talk to *fai.fortinet.net* and *update.fortiguard.net* to get a list of the close-by FDS servers. The updater will use the closest ones. The current list of FDS servers that are retreived this way can be found by using the CLI `diagnose fds list`. if you wants to use a specific server, you can specify the override servers to connect to. Please note that both *override-server-address-main* and *override-server-address-alt* have to be set to get all the updates.

Example 1: Use specific IPs for the FDS servers and do not fall back to default servers if none of the specified override servers can be reached.

```
config system fortiguard update
   set override-server-status enable
   set override-include-default-servers disable
   set override-server-port 443
   set override-server-address-main 208.184.237.78 140.174.22.36
   set override-server-address-alt 208.184.237.66
end
```

This configuration will use the servers `208.18.237.78` and `140.174.22.36` to replace *fai.fortinet.net* and *208.184.237.66* to replace *update.fortiguard.net* when downloading from FDS servers.

Example 2: The FortiNDR device cannot perform DNS lookups and a proxy is in use.

By default, a FortiNDR device will use the list of IPs returned from the FDS servers after initially talking to *fai.fortinet.net* and *update.fortiguard.net*. However, if a proxy server is used to connect to the FDS servers and you would like the DNS resolution to be done by the proxy server, the following configuration can be used:

```
config system fortiguard update
   set override-server-status enable
   set override-include-default-servers disable
   set override-server-port 443
   set override-server-address-main fai.fortinet.net
   set override-server-address-alt update.fortiguard.net
   set tunneling-status enable
   set tunneling-address 192.168.1.50
   set tunneling-port 8080
end
```

This setting will defer the DNS resolution to the proxy server `192.168.1.50` and a proxy and/or firewall policy can be used with FQDNs instead of individual FDS server IPs.

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 *Host IP*, *Domain Name*, or *E-Mail*.
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.

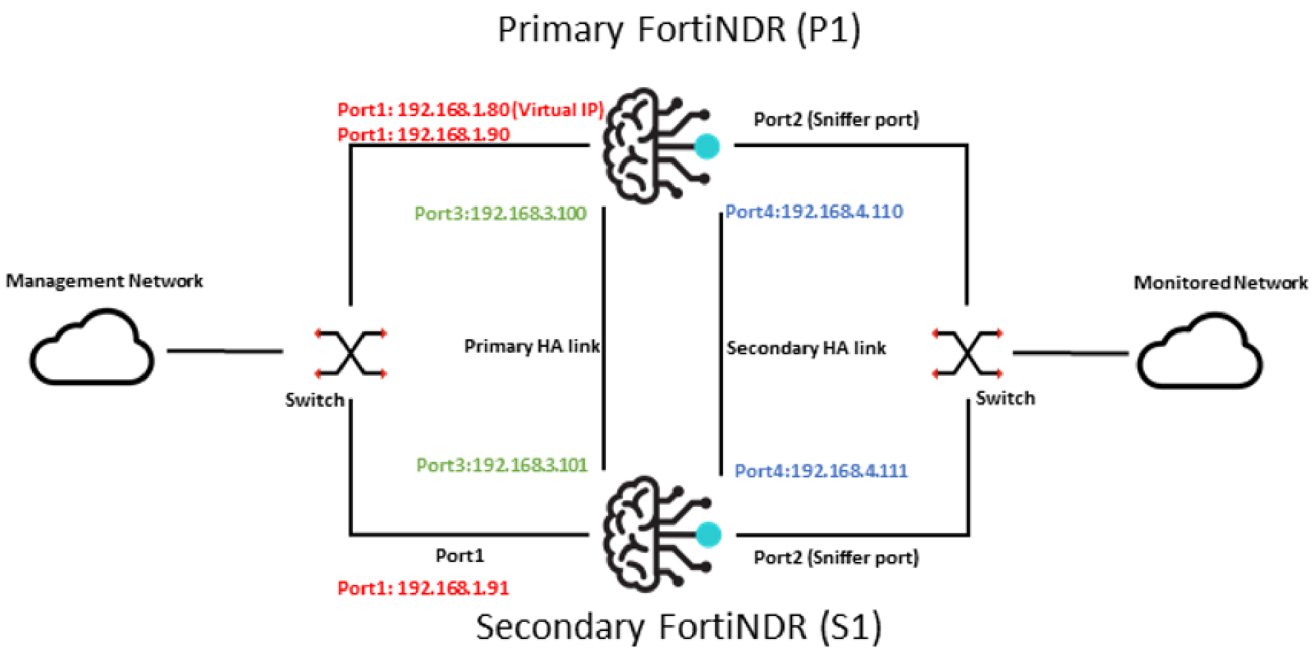
High Availability (HA) is only available in Standalone mode.

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 166.
- 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:



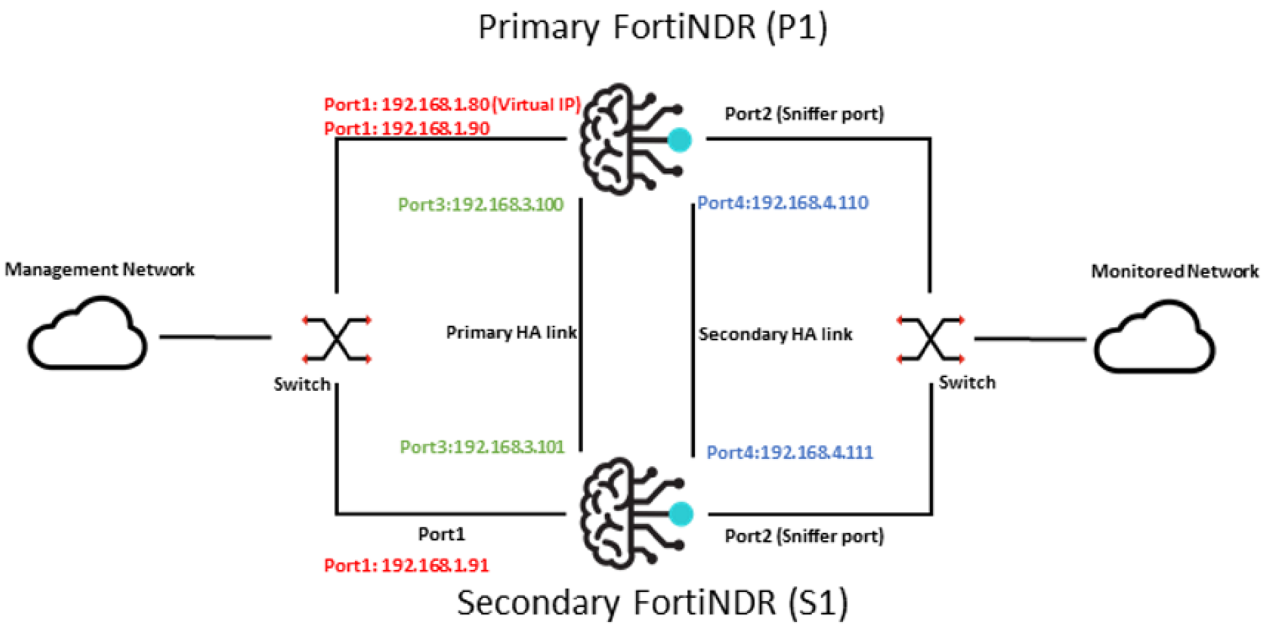
Configuring an HA group

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 267).

- The ANN database is not synchronized.
- The ANN scheduled update settings are not synchronized. You will need to configure both units to enusre 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
```

CLI option	Description
`mode`	Enables or disables HA, selects the initial configured role: • `Off`: disable HA. • `Primary`: configured as primary Unit. • `Secondary`: configured as secondary Unit.
`password`	Enter an HA password for the HA group. You must configure the same password value on both the primary and secondary units.
`heartbeat-status`	Specify if this interface will be used for HA heartbeat and synchronization: • `Disable`: The interface is not used for HA heartbeat and synchronization. • `Primary`: We recommend to using port3 as the primary HA interface. • `Secondary`: We recommend having a secondary HA interface to improve availability. Use port4 as the secondary HA interface.
`peer-ip`	When configuring primary HA interfaces: • When configuring the primary `unit`, enter the IP address of the secondary unit’s `primary` HA interface. • When configuring the secondary `unit`, enter the IP address of the primary unit’s `primary` HA interface. The same rule should be applied when configuring the secondary HA interface.
`virtual-ip`	Enter the virtual IP address and netmask for this interface. If configured, this virtual IP can serve as the external IP of the HA group. When failover occurs, this setting will take effect on the new Primary unit. For details, see Using Virtual IP on page 173.
`action-on-primary`	`ignore-vip [Default]`: Ignore the Virtual IP interface configuration on the new Primary unit after failover. `use-vip`: Add the specified Virtual IP address and netmask to the interface on the new Primary unit after failover.
`port-monitor`	Enable to monitor a network interface for failure on the Primary unit. If the interface failure is detected, the Primary unit will trigger a failover. This does not apply to heartbeat interfaces.

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

```
config system ha
    set mode secondary
    set password xxx    << password should be same as primary unit
    config interface
```

```
        edit port1                         << HA configuration for port1  should be same as
primary unit
            set virtual-ip 192.168.1.80/24
            set  action-on-primary use-vip
            set port-monitor enable
        end
        edit port3
            set heartbeat-status primary
            set peer-ip 192.168.3.100      << IP of primary unit’s port3 interface
        end
        edit port4
            set heartbeat-status secondary
            set peer-ip 192.168.4.110      << IP of primary unit’s port4 interface
    end
end
```

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 169.
    - Ensure no errors appear on the HA event log. See, HA Logs on page 172.

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 172.
- 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.

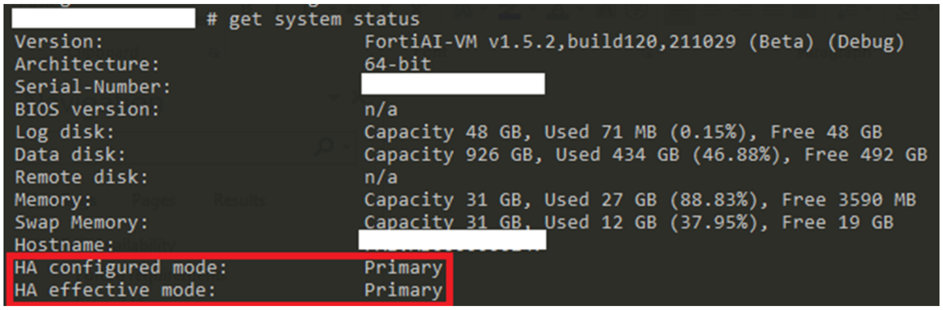
Check HA status

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 • *Primary*: Configured to be the primary unit. • *Secondary*: Configured to be the secondary unit.
HA Effective Mode	Displays the current operating mode • *Primary*: Acting as primary unit • *Secondary*: Acting as secondary unit • *Failed*: Occurs when network interface monitoring has detected a failure, failover is triggered afterward.

To check HA status with the CLI:

```
get system status
```



```
[redacted] # get system status
Version:                      FortiAI-VM v1.5.2,build120,211029 (Beta) (Debug)
Architecture:                 64-bit
Serial-Number:                [redacted]
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:                     [redacted]
HA configured mode:           Primary
HA effective mode:            Primary
```

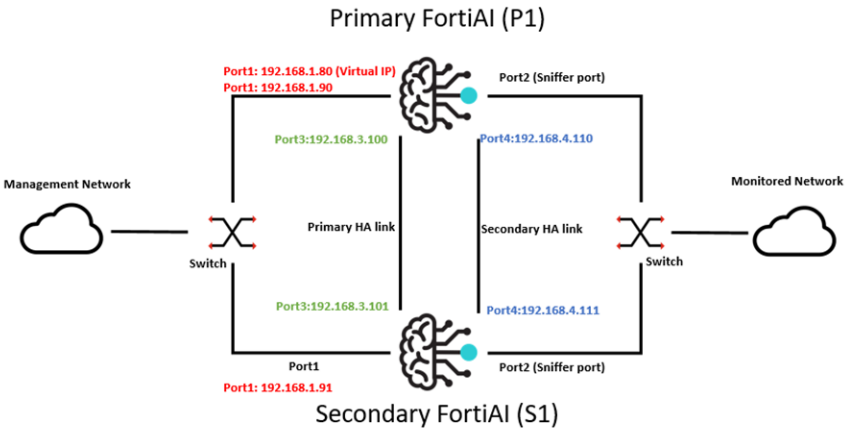
To check the HA status with the GUI:

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.

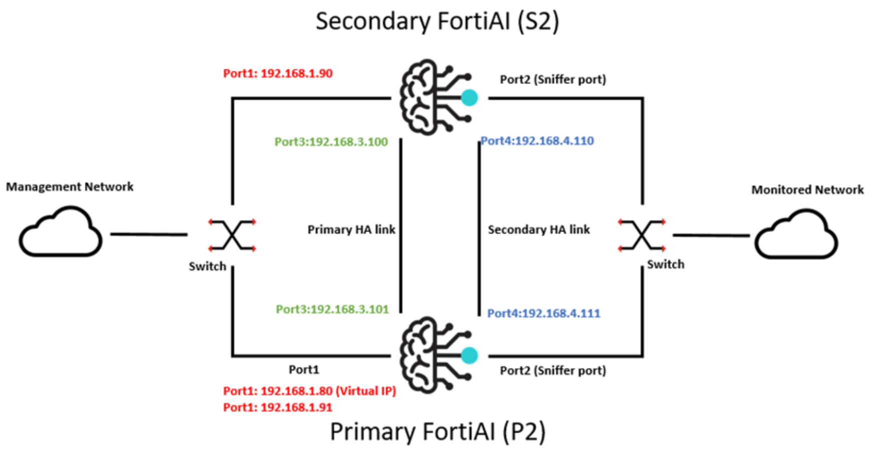
HA Failover

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

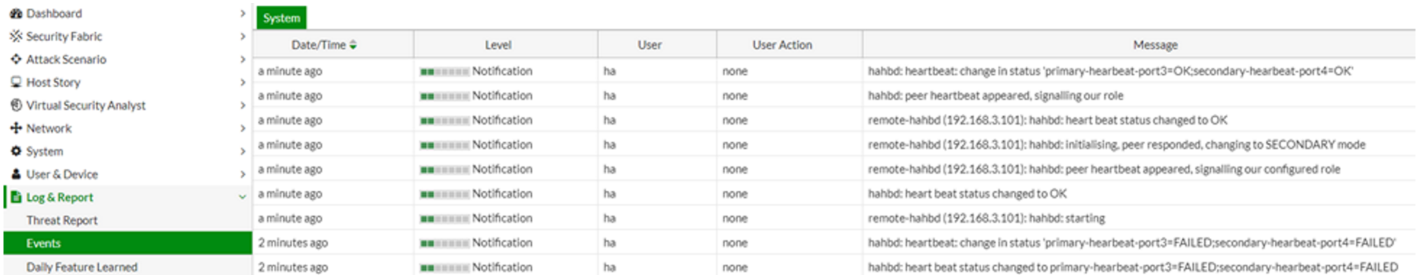
All configuration settings on the primary unit are synchronized to the secondary unit once the HA group has been configured successfully, with the exception of the following settings:

Configuration Settings	Description
HA Settings	HA related configurations
Network Settings	System network settings including: • 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.



Date/Time	Level	User	User Action	Message
a minute ago	Notification	ha	none	hahbd: heartbeat: change in status 'primary-hearbeat-port3=OK;secondary-hearbeat-port4=OK'
a minute ago	Notification	ha	none	hahbd: peer heartbeat appeared, signalling our role
a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: heart beat status changed to OK
a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: initialising, peer responded, changing to SECONDARY mode
a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: peer heartbeat appeared, signalling our configured role
a minute ago	Notification	ha	none	hahbd: heart beat status changed to OK
a minute ago	Notification	ha	none	remote-hahbd (192.168.3.101): hahbd: starting
2 minutes ago	Notification	ha	none	hahbd: heartbeat: change in status 'primary-hearbeat-port3=FAILED;secondary-hearbeat-port4=FAILED'
2 minutes ago	Notification	ha	none	hahbd: heart beat status changed to primary-hearbeat-port3=FAILED;secondary-hearbeat-port4=FAILED

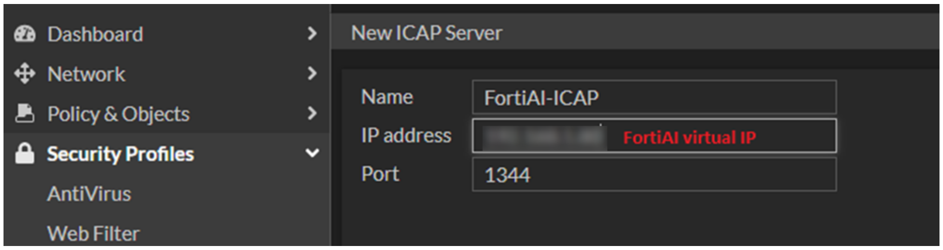
Using Virtual IP

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 166.

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.



Name: FortiAI-ICAP
IP address: [redacted] FortiAI virtual IP
Port: 1344

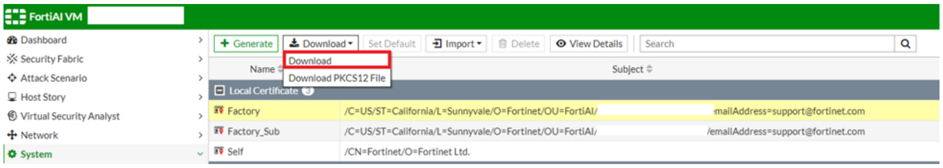
Example: Configure FortiGate Security fabric settings for inline blocking

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* .

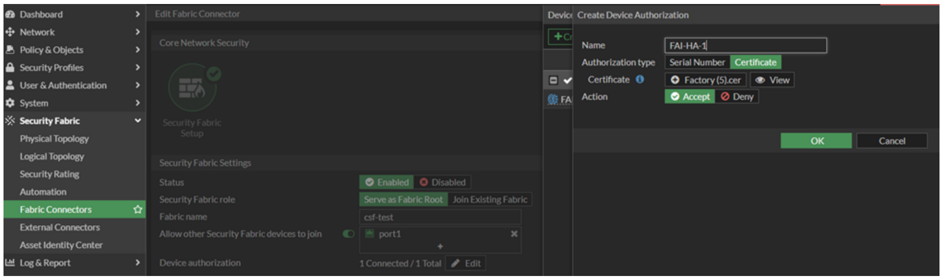
3. In the toolbar click *Download* , to download the certificate.



Name	Subject
Local Certificate 3	
Factory	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=FortiAI/[redacted]mailAddress=support@fortinet.com
Factory_Sub	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=FortiAI/[redacted]/emailAddress=support@fortinet.com
Self	/CN=Fortinet/O=Fortinet Ltd.

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*.



Security Fabric Settings

Status: Enabled | Disabled

Security Fabric role: Serve as Fabric Root | Join Existing Fabric

Fabric name: csf-test

Allow other Security Fabric devices to join: port1

Device authorization: 1 Connected / 1 Total Edit

Create Device Authorization

Name: FAI-HA-1

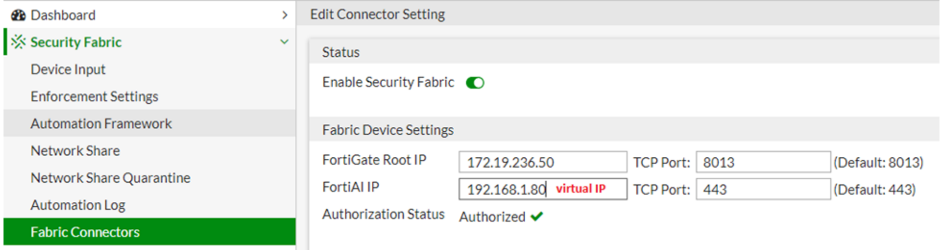
Authorization type: Serial Number | Certificate

Certificate: Factory (5).cer View

Action: Accept | Deny

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.



Edit Connector Setting

Status

Enable Security Fabric

Fabric Device Settings

FortiGate Root IP: 172.19.236.50 TCP Port: 8013 (Default: 8013)

FortiAI IP: 192.168.1.80 TCP Port: 443 (Default: 443)

Authorization Status: Authorized ✓

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

For detailed information about inline blocking configuration, see FortiGate inline blocking (FOS 7.0.1 and higher) on page 104.

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 exits 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.

Limitations of backup/restore workflow:

You cannot use the GUI to back up and restore the following system settings:

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

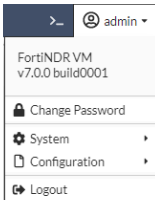
Please record these configuration settings before upgrading so the full configuration can be restored.

Network Share Configuration backup and restore is managed by its own CLI:

- To back up, see execute backup system-db network-share-config
- To restore, see execute restore system-db network-share-config

To backup the FortiNDR configuration to your local computer:

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



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

To restore the system configuration from your local computer:

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

User & Authentication

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

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

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

RADIUS Server

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

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

The following options are available:

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

The following information is displayed:

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

To create a new RADIUS server:

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

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

4. Click *OK*.

LDAP Servers

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

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

The following options are available:

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

The following information is displayed:

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

To add an LDAP server:

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

Profile name	Enter a name for the profile.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server. Port: Enter the port number where the LDAP server listens. The default port number varies by your selection in *Use secure connection*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
Fall Back Server name/IP	Optional. Enter the fully qualified domain name (FQDN) or IP address of an alternate LDAP server that the FortiNDR unit can query if the primary LDAP server is unreachable. Port: Enter the port number where the fallback LDAP server listens. The default port number varies by your selection in *Use secure connection*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
Use secure connection	Select whether or not to connect to the LDAP servers using an encrypted connection. • *None*: Use a non-secure connection. • *SSL*: Use an SSL-secured (LDAPS) connection. Click *Test LDAP Query* to test the connection. A pop-up window appears.
Default Bind Options	

Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiNDR will search for user objects, such as `ou=People`, `dc=example`, `dc=com`. User objects should be child nodes of this location.
Bind DN	Enter the bind DN, such as `cn=fortiNDR`, `dc=example`, `dc=com`, of an LDAP user account with permissions to query the Base DN.
Bind password	Enter the password of the Bind DN. Click *Browse* to locate the LDAP directory from the location that you specified in *Base DN*, or, if you have not yet entered a Base DN, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your Base DN, or need to look up attribute names. For example, if the Base DN is unknown, browsing can help you to locate it. Before using, first configure *Server name/IP*, *Use secure connection*, *Bind DN*, *Bind password*, and *Protocol version*, then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection.
User Query Options	
LDAP user query	Click *Schema* to select a schema style. You can edit the schema as desired or select *User Defined* and write your own schema.
Scope	Select the level of depth to query, starting from *Base DN*. • *One level*: Query only the one level directly below the Base DN in the LDAP directory tree. • *Subtree*: Query recursively all levels below the Base DN in the LDAP directory tree.
Derefer	Select the method to use, if any, when dereferencing attributes whose values are references. • *Never*: Do not dereference. • *Always*: Always dereference. • *Search*: Dereference only when searching. • *Find*: Dereference only when finding the base search object.

User Authentication Options	Enable to configure the authentication options. Select one of the followng from the dropdown. - *Try UPN or mail address as bind DN* - *Try common name with base DN as bind DN* - *Search user and try bind DN*.
Advanced Options	
Timeout (seconds)	Enter the maximum amount of time in seconds that the FortiNDR unit will wait for query responses from the LDAP server.
Protocol version	Select the LDAP protocol version used by the LDAP server: *LDAP Version 2* or *LDAP Version 3*.
Allow Unauthenticated Bind	Disable bind authentication.
Enable Cache	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiNDR unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.
Clear Cache	Select to empty the FortiNDR unit's LDAP query cache. This can be useful if you have updated the LDAP directory, and want the FortiNDR unit to refresh its LDAP query cache with the new information.
TTL (minutes)	Enter the amount of time, in minutes, that the FortiNDR unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiNDR unit to query the LDAP server, refreshing the cache. The default Time To Live (TTL) value is 1440 minutes (one day). The maximum value is 10080 minutes (one week). Entering a value of 0 effectively disables caching. This option is applicable only if Enable cache is enabled.

4. Click *OK*.

To edit an LDAP server:

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

LDAP user query example

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

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

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

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

(& (objectClass=inetOrgPerson) (mail=m

{-spam}))

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

(& (objectClass=inetOrgPerson) (mail=m

{^spam-}))

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

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

Alias member query example

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

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

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

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

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

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

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

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

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

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

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

Preparing your LDAP schema for FortiNDR LDAP profiles

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

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

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

Using common schema styles

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

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

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

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

In this scenario, it may be sufficient to:

1. In the LDAP profile, enter the domain name or IP address of the LDAP server.
2. Configure the LDAP profile queries:

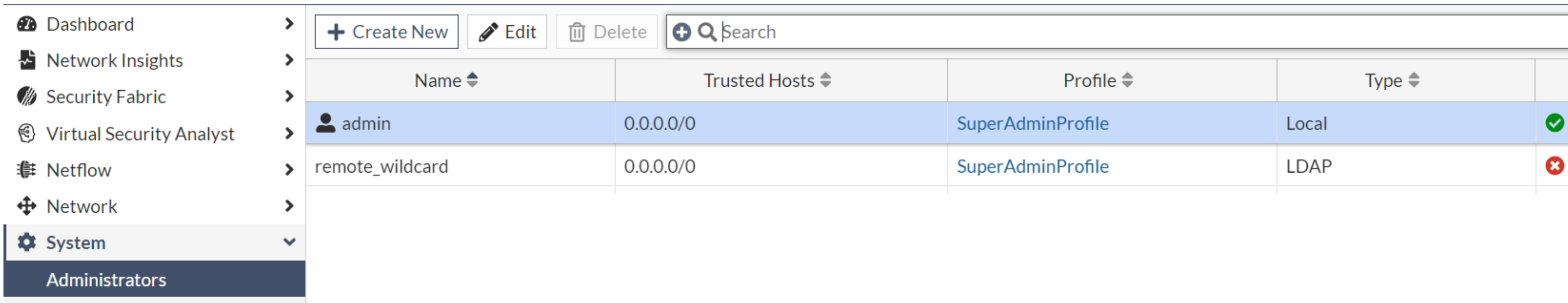
    - In *User Query Options*, from *Schema* which OpenLDAP schema your user objects follow: either InetOrgPerson or InetLocalMailRecipient. Also enter the *Base DN*, *Bind DN*, and *Bind* password to authenticate queries by the FortiNDR unit and to specify which part of the directory tree to search.
  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

Creating remote wildcard administrators

You can enable LDAP and RADIUS login by registering the login username as an Administrator profile name. However, if all the user accounts from an LDAP/RADIUS profile will be sharing the same admin profile permissions, the *remote_wildcard* profile can be used to bypass registering all user accounts individually on the system. You can still register LDAP credentials individually in addition to the wildcard profile if you wish to give those accounts different access privileges.

In 7.4.6 and earlier, some administrators without *SuperAdminProfile* permissions, will not see the correct sensor data, nor will they be able to arrange the widgets in the *Dashboard*. To ensure an administrator account is seeing the correct sensor data, the admin profile linked to the administrator account is required to have *System Access* set to *Read/Write* permissions.

Only the Administrator account *admin* can modify the admin profile field in any administrator's account.



Name	Trusted Hosts	Profile	Type	
admin	0.0.0.0/0	SuperAdminProfile	Local	✓
remote_wildcard	0.0.0.0/0	SuperAdminProfile	LDAP	✗

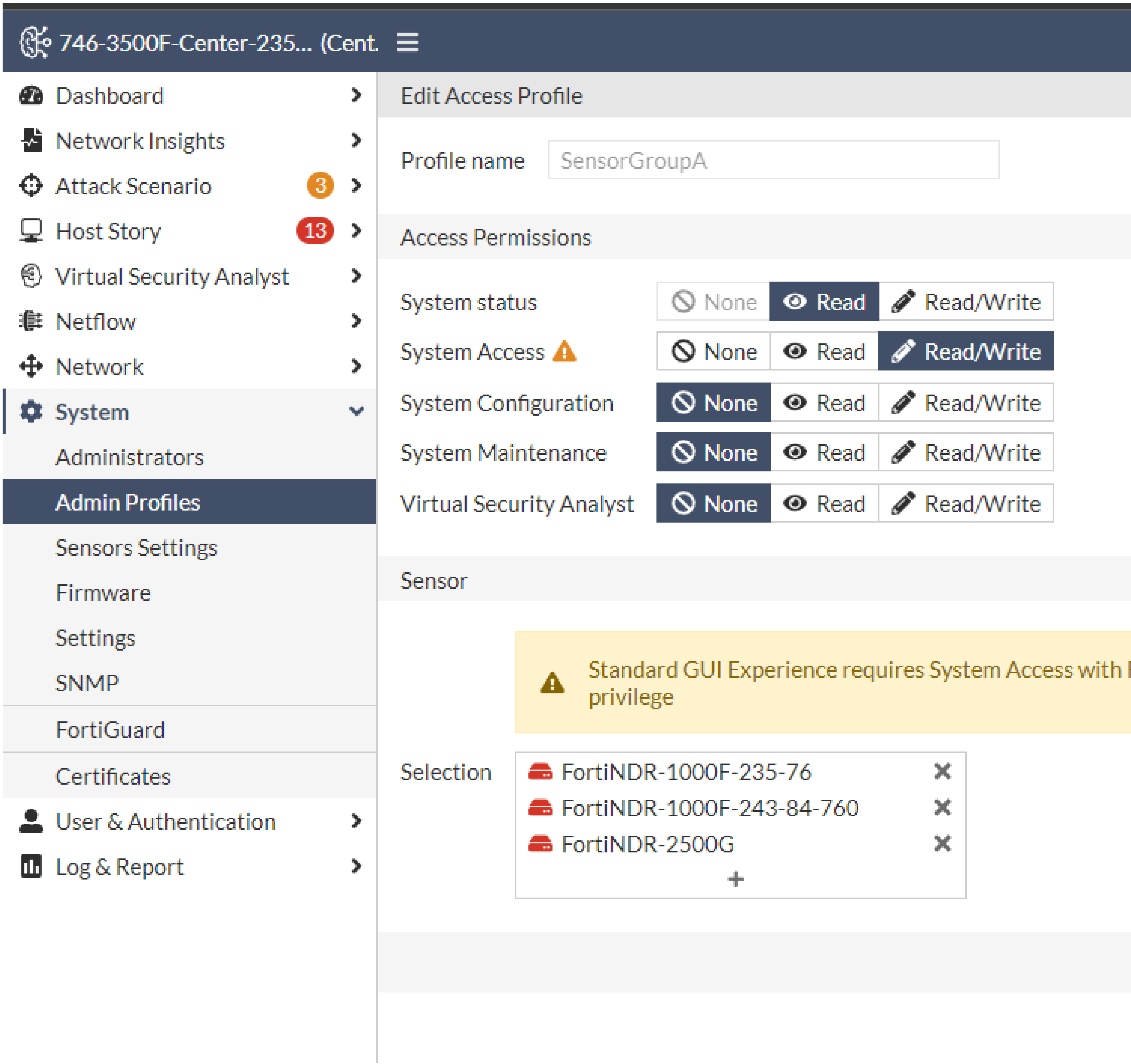
Assigning sensors to an admin profile

Admin profiles allow you to create different permission structures for specific sensors that are assigned to administrators. For more information about the *SuperAdminProfile* and pre-defined profile types, see "Admin Profiles" on page 152

To assign sensors to an Admin Profile:

1. Go to *System > Admin Profiles* and click *Create New*. The *Create Access Profile* page opens.
2. Give the profile a descriptive name.
3. (Required) Under *Access Permissions*, set *System Access* to *Read/Write*. You can configure the other permissions as necessary.

4. To add sensors to the profile, in the *Sensor* section, click the *Selection* button and select the sensors.



Edit Access Profile

Profile name: SensorGroupA

Access Permissions

System status: None [✓ Read] Read/Write

System Access ⚠: None Read [✓ Read/Write]

System Configuration: [✓ None] Read Read/Write

System Maintenance: [✓ None] Read Read/Write

Virtual Security Analyst: [✓ None] Read Read/Write

Sensor

⚠ Standard GUI Experience requires System Access with I privilege

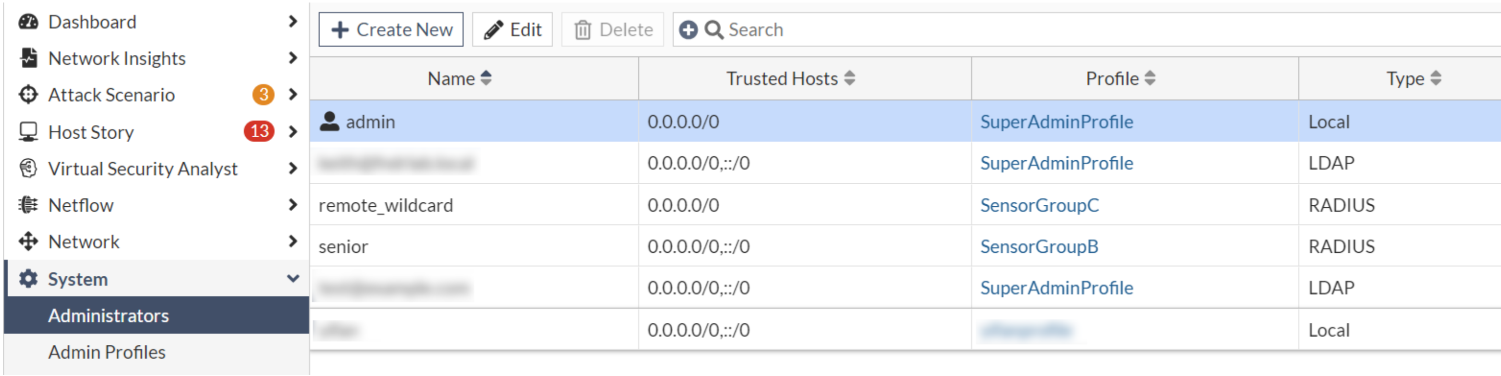
Selection:
- FortiNDR-1000F-235-76 ✕
- FortiNDR-1000F-243-84-760 ✕
- FortiNDR-2500G ✕
- +

5. Click *OK*.

Assigning admin and LDAP/RADIUS profiles to the *remote_wildcard* administrator

To assign the profiles to the *remote_wildcard* administrator:

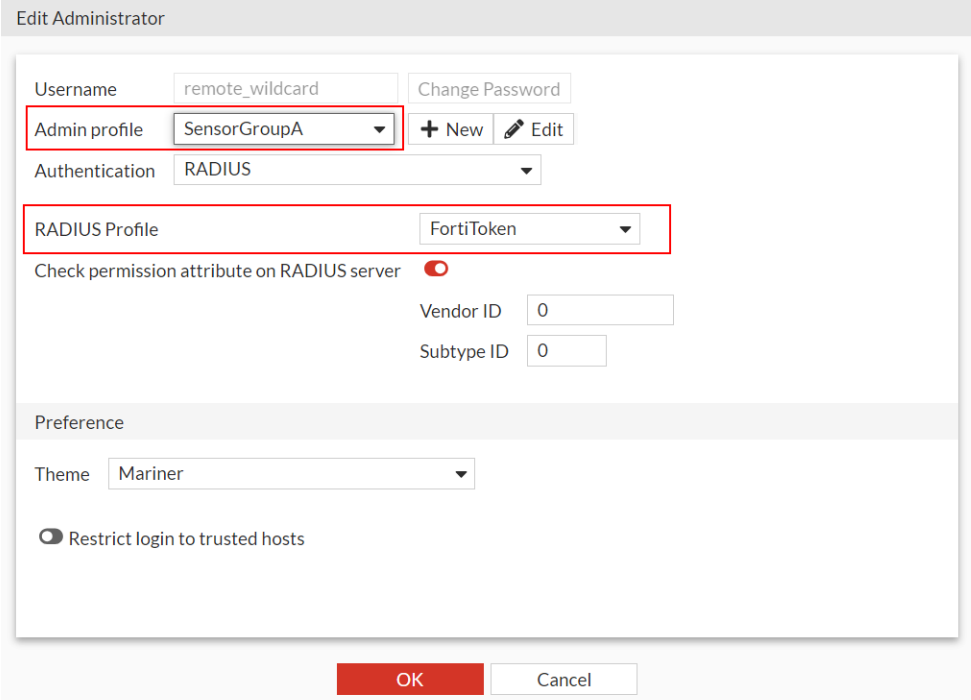
1. Go to *System* > *Administrator* and double-click *remote_wildcard*. The *Edit Administrator* page opens.



Name	Trusted Hosts	Profile	Type
admin	0.0.0.0/0	SuperAdminProfile	Local
[redacted]	0.0.0.0/0,::/0	SuperAdminProfile	LDAP
remote_wildcard	0.0.0.0/0	SensorGroupC	RADIUS
senior	0.0.0.0/0,::/0	SensorGroupB	RADIUS
[redacted]	0.0.0.0/0,::/0	SuperAdminProfile	LDAP
[redacted]	0.0.0.0/0,::/0	[redacted]	Local

2. From the *Admin Profile* dropdown, select the profile you created in the previous steps.
3. Select the *Authentication* method.

LDAP	Select *LDAP* and then select the *LDAP* profile.
RADIUS	Select *RADIUS* and then select the *RADIUS* profile.



Username: remote_wildcard

Admin profile: SensorGroupA

Authentication: RADIUS

RADIUS Profile: FortiToken

Check permission attribute on RADIUS server

Vendor ID: 0

Subtype ID: 0

Theme: Mariner

Restrict login to trusted hosts

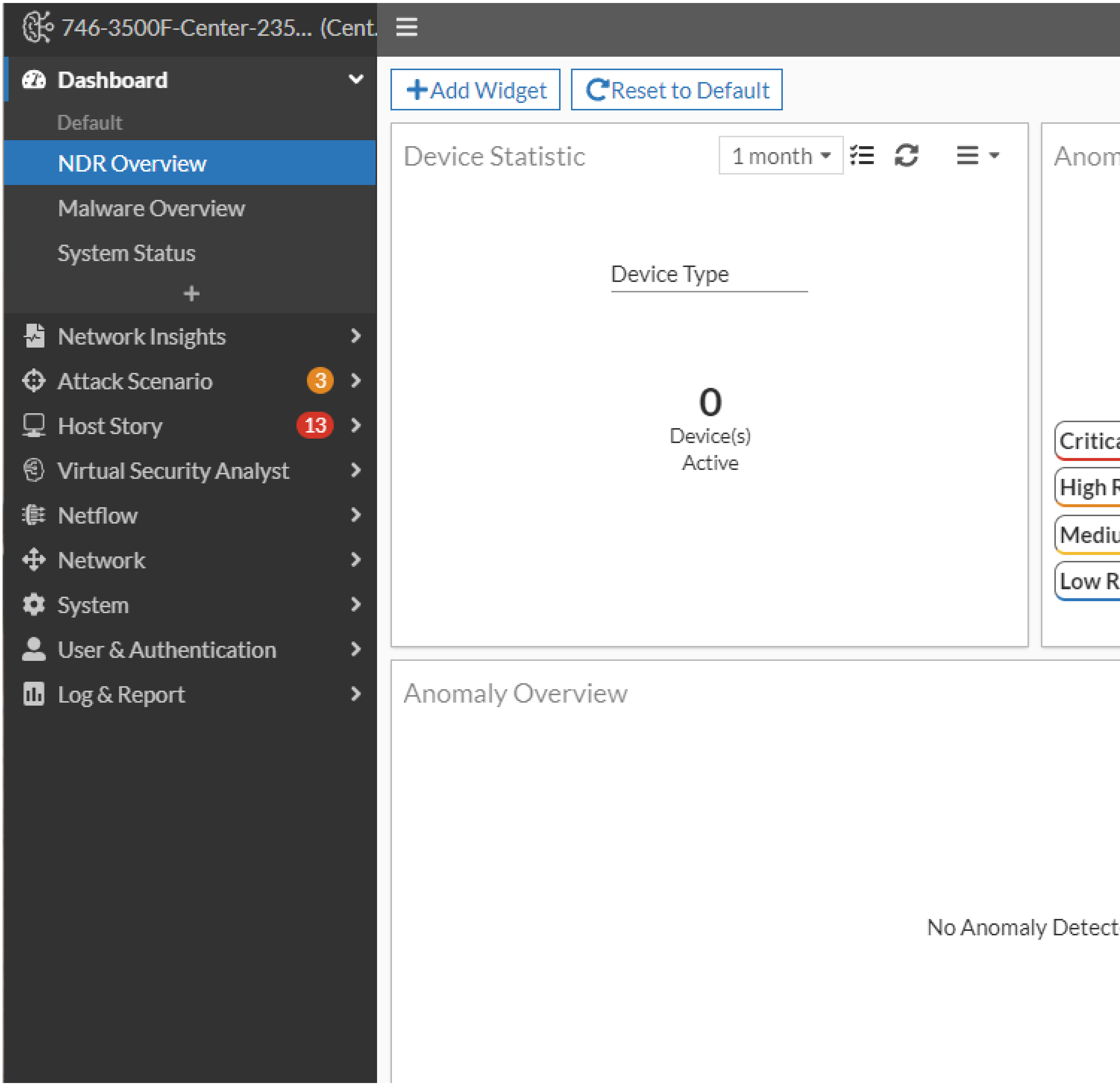
4. Click *OK*.

Resetting the available sensors resources in FortiNDR

When you add and disable sensors in an admin profile, the widgets in the *Dashboard* retain the current sensor settings even though they are no longer available to the current account. To update the widget sensor settings for all users simultaneously, use the *Reset to Default* button.

To reset the Available Sensors Resources:

1. Log into FortiNDR as the *remote_wildcard* administrator with the LDAP or RADIUS server.
2. Hover over the *Available Sensors Resources* icon and verify the sensors are assigned to the Admin Profile you created.



3. In the *Dashboard*, click *Reset to Default* button to automatically load all the widgets with all the available sensor data.

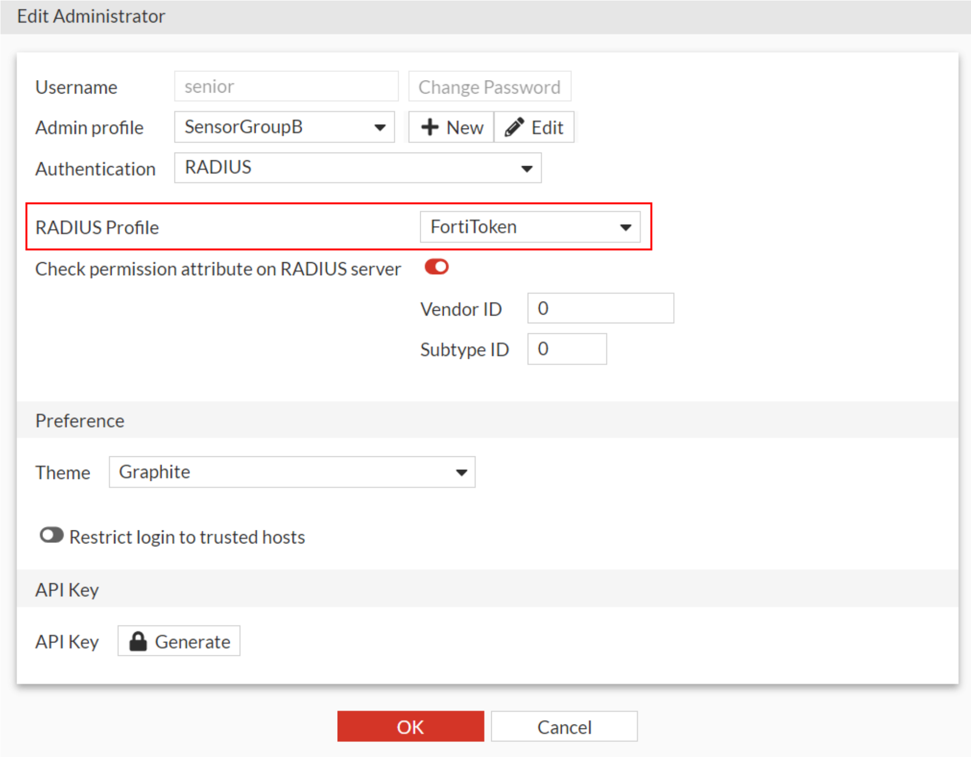
All users that access FortiNDR as a *remote_wildcard* administrator will see this dashboard view.

Creating LDAP/RADIUS administrators with different permissions

You can use Admin Profiles to assign sensors and permissions to specific administrators. When an LDAP/RADIUS administrator logs into FortiNDR, the system will use the LDAP/RADIUS profile assigned to the *remote_wildcard* administrator to authenticate the user.

To create multiple LDAP administrators:

1. Create a new Admin Profile. See, "Assigning sensors to an admin profile " on page 184.
2. Create a new administrator. See, "Administrators" on page 150
3. In from the *LDAP profile* or *RADIUS Profile* dropdown, select the profile used by the *remote_wildcard* administrator.



Edit Administrator

Username: senior

Admin profile: SensorGroupB

Authentication: RADIUS

RADIUS Profile: FortiToken

Check permission attribute on RADIUS server: ●

Vendor ID: 0

Subtype ID: 0

Preference

Theme: Graphite

○ Restrict login to trusted hosts

API Key

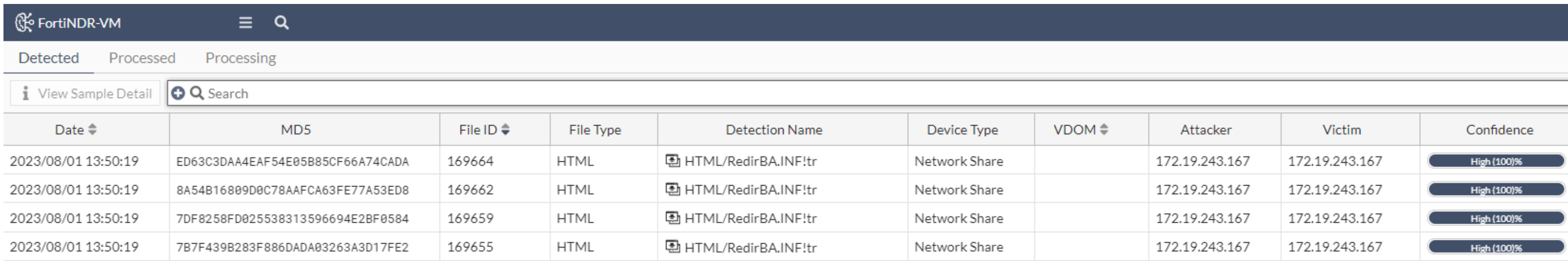
4. Click *OK*.

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.



Date	MD5	File ID	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence
2023/08/01 13:50:19	ED63C3DAA4EAF54E05B85CF66A74CADA	169664	HTML	HTML/RedirBA.INF!tr	Network Share		172.19.243.167	172.19.243.167	High (100)%
2023/08/01 13:50:19	8A54B16809D0C78AAFCA63FE77A53ED8	169662	HTML	HTML/RedirBA.INF!tr	Network Share		172.19.243.167	172.19.243.167	High (100)%
2023/08/01 13:50:19	7DF8258FD025538313596694E2BF0584	169659	HTML	HTML/RedirBA.INF!tr	Network Share		172.19.243.167	172.19.243.167	High (100)%
2023/08/01 13:50:19	7B7F439B283F886DADA03263A3D17FE2	169655	HTML	HTML/RedirBA.INF!tr	Network Share		172.19.243.167	172.19.243.167	High (100)%

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 *Processing* 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 *IP Address*, *Last Synch Time*, and *Status*
File ID	The file ID.
File type	The file type. *Other* 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.

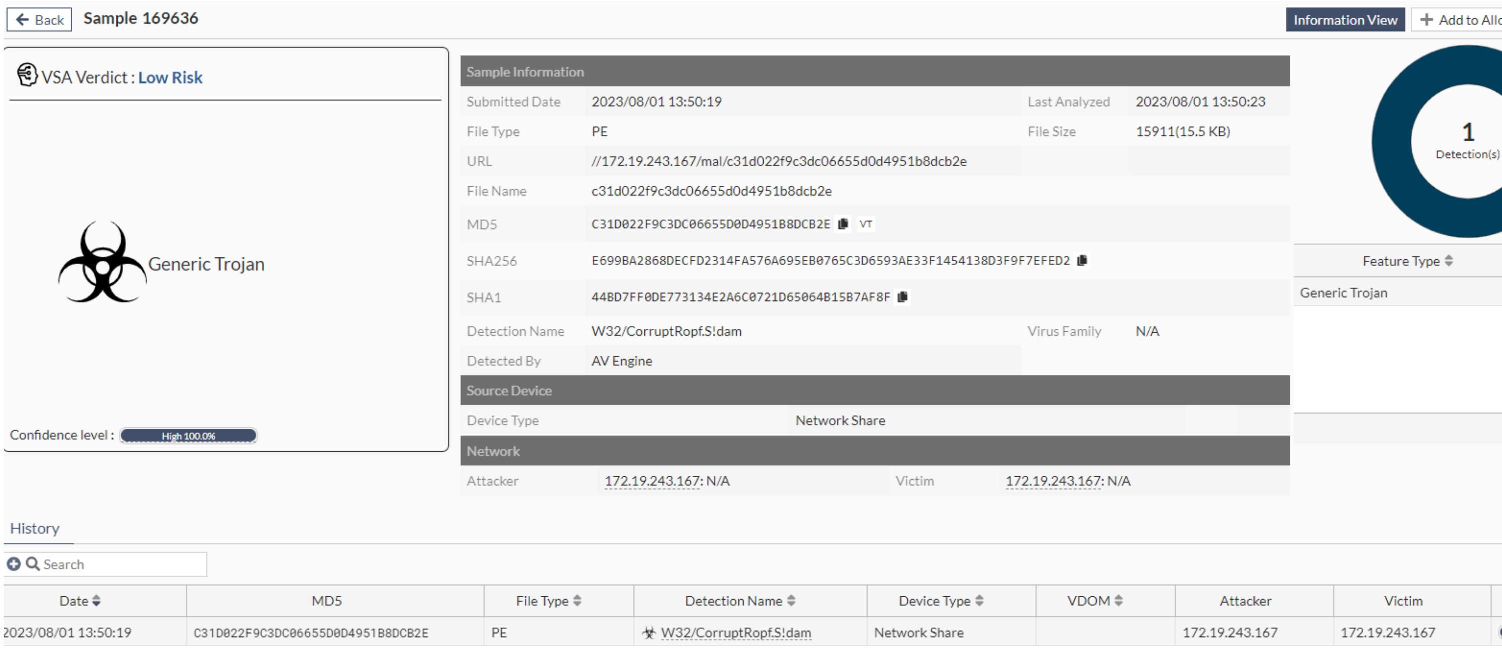
Download a sample

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.



Sample 169636

VSA Verdict : Low Risk

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		
MD5	C31D022F9C3DC06655D0D4951B8DCB2E VT		
SHA256	E699BA2868DECFD2314FA576A695EB0765C3D6593AE33F1454138D3F9F7EFED2		
SHA1	44BD7FF0DE773134E2A6C0721D65064B15B7AF8F		
Detection Name	W32/CorruptRopf.S!dam	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 Type
Generic Trojan

History

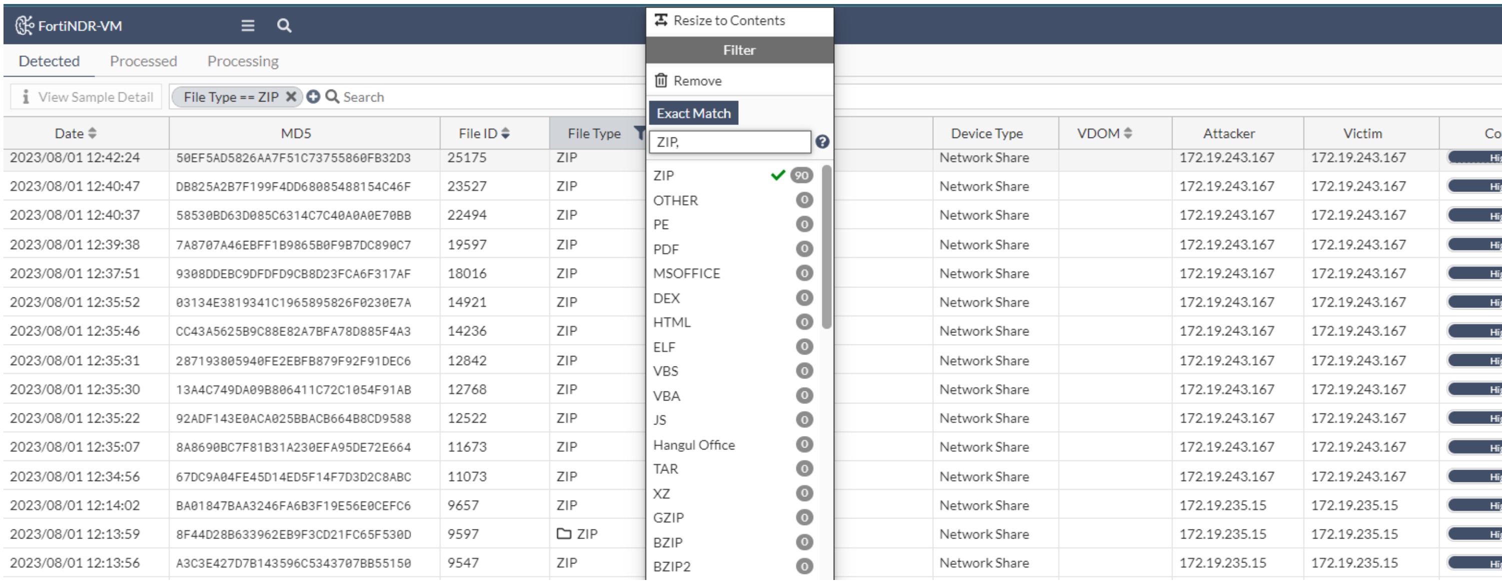
Search

Date	MD5	File Type	Detection Name	Device Type	VDOM	Attacker	Victim
2023/08/01 13:50:19	C31D022F9C3DC06655D0D4951B8DCB2E	PE	W32/CorruptRopf.S!dam	Network Share		172.19.243.167	172.19.243.167

View items in a zip folder

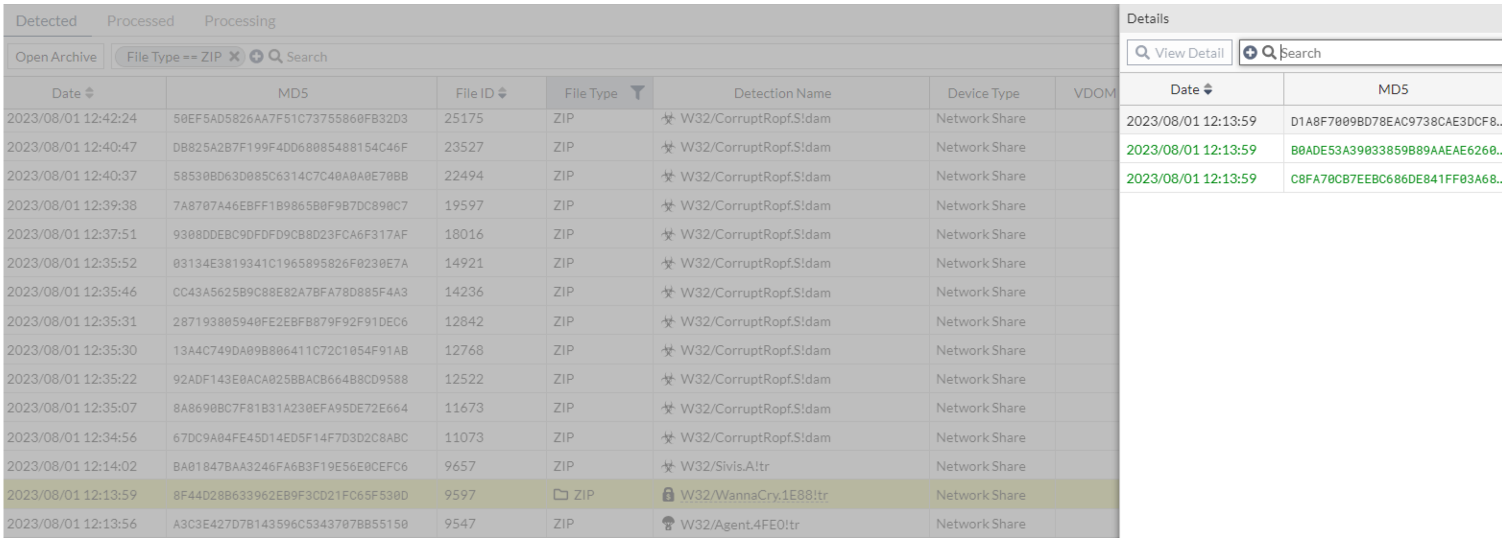
To view items in a zip folder:

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



Date	MD5	File ID	File Type	Device Type	VDOM	Attacker	Victim	Co
2023/08/01 12:42:24	50EF5AD5826AA7F51C73755860FB32D3	25175	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:40:47	DB825A2B7F199F4DD68085488154C46F	23527	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:40:37	58530BD63D085C6314C7C40A0A0E70BB	22494	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:39:38	7A8707A46EBFF1B9865B0F9B7DC890C7	19597	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:37:51	9308DDEBC9DFDFD9CB8D23FCA6F317AF	18016	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:35:52	03134E3819341C1965895826F0230E7A	14921	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:35:46	CC43A5625B9C88E82A7BFA78D885F4A3	14236	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:35:31	287193805940FE2EBFB879F92F91DEC6	12842	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:35:30	13A4C749DA09B806411C72C1054F91AB	12768	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:35:22	92ADF143E0ACA025BBACB664B8CD9588	12522	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:35:07	8A8690BC7F81B31A230EFA95DE72E664	11673	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:34:56	67DC9A04FE45D14ED5F14F7D3D2C8ABC	11073	ZIP	Network Share		172.19.243.167	172.19.243.167	Hi
2023/08/01 12:14:02	BA01847BAA3246FA6B3F19E56E0CEFC6	9657	ZIP	Network Share		172.19.235.15	172.19.235.15	Hi
2023/08/01 12:13:59	8F44D28B633962EB9F3CD21FC65F530D	9597	🗀 ZIP	Network Share		172.19.235.15	172.19.235.15	Hi
2023/08/01 12:13:56	A3C3E427D7B143596C5343707BB55150	9547	ZIP	Network Share		172.19.235.15	172.19.235.15	Hi

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



Date	MD5	File ID	File Type	Detection Name	Device Type	VDOM
2023/08/01 12:42:24	50EF5AD5826AA7F51C73755860FB32D3	25175	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:40:47	DB825A2B7F199F4DD68085488154C46F	23527	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:40:37	58530BD63D085C6314C7C40A0A0E70BB	22494	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:39:38	7A8707A46EBFF1B9865B0F9B7DC890C7	19597	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:37:51	9308DDEBC9DFDFD9CB8D23FCA6F317AF	18016	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:35:52	03134E3819341C1965895826F0230E7A	14921	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:35:46	CC43A5625B9C88E82A7BFA78D885F4A3	14236	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:35:31	287193805940FE2EBFB879F92F91DEC6	12842	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:35:30	13A4C749DA09B806411C72C1054F91AB	12768	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:35:22	92ADF143E0ACA025BBACB664B8CD9588	12522	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:35:07	8A8690BC7F81B31A230EFA95DE72E664	11673	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:34:56	67DC9A04FE45D14ED5F14F7D3D2C8ABC	11073	ZIP	W32/CorruptRopf.S!dam	Network Share	
2023/08/01 12:14:02	BA01847BAA3246FA6B3F19E56E0CEFC6	9657	ZIP	W32/Sivis.A!tr	Network Share	
2023/08/01 12:13:59	8F44D28B633962EB9F3CD21FC65F530D	9597	ZIP	W32/WannaCry.1E88!tr	Network Share	
2023/08/01 12:13:56	A3C3E427D7B143596C5343707BB55150	9547	ZIP	W32/Agent.4FE0!tr	Network Share	

Date	MD5
2023/08/01 12:13:59	D1A8F7009BD78EAC9738CAE3DCF8..
2023/08/01 12:13:59	B0ADE53A39033859B89AAEAE6260..
2023/08/01 12:13:59	C8FA70CB7EEBC686DE841FF03A68..

Perform a batch download

To perform a batch download:

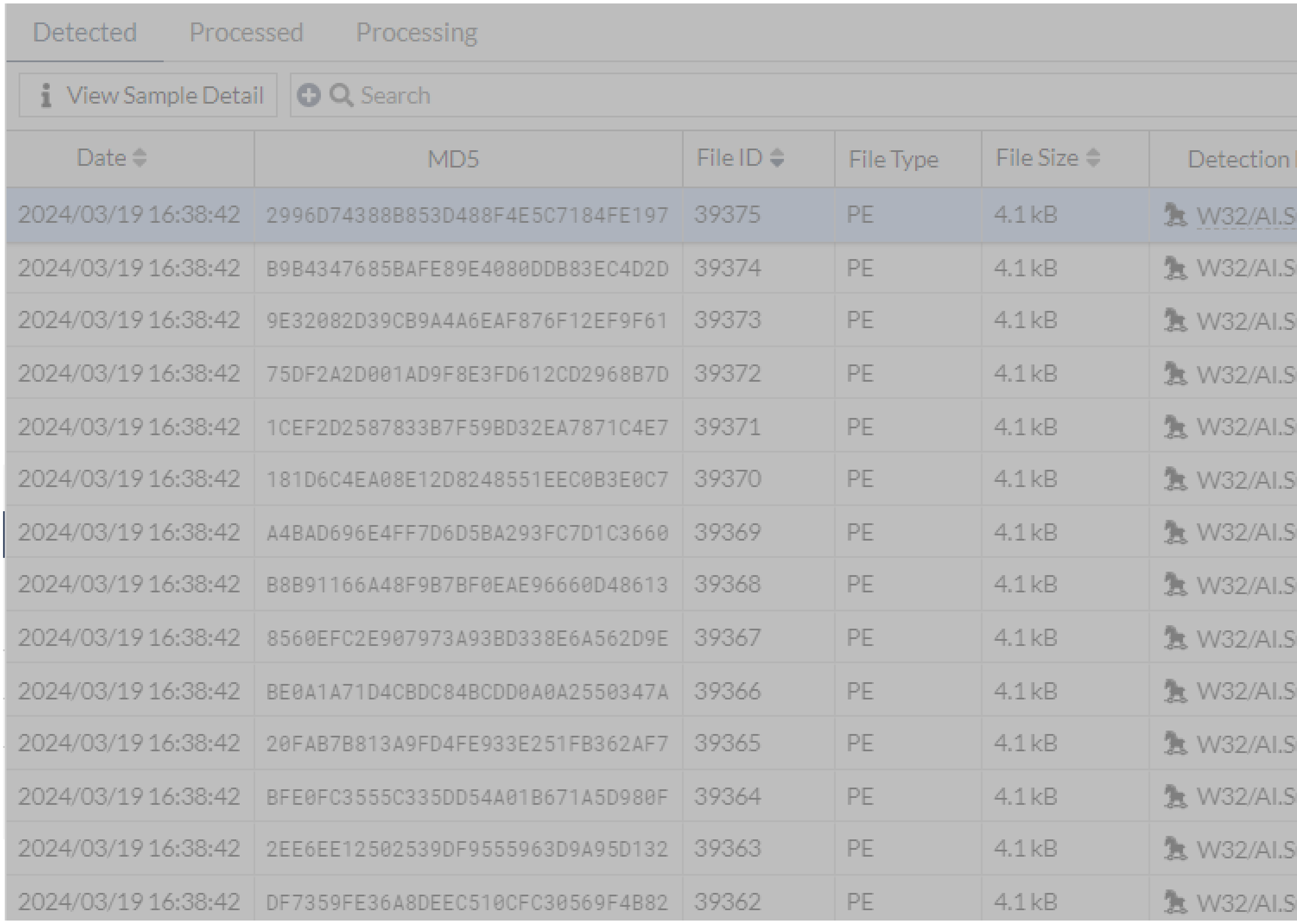
1. Select the files to download.
2. Click Batch Download. The files are zipped with a password and downloaded to your device.

Add detections to the Allow List

To add detections to the allow list and submit feedback:

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.



Date	MD5	File ID	File Type	File Size	Detection
2024/03/19 16:38:42	2996D74388B853D488F4E5C7184FE197	39375	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	B9B4347685BAFE89E4080DDB83EC4D2D	39374	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	9E32082D39CB9A4A6EAF876F12EF9F61	39373	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	75DF2A2D001AD9F8E3FD612CD2968B7D	39372	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	1CEF2D2587833B7F59BD32EA7871C4E7	39371	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	181D6C4EA08E12D8248551EEC0B3E0C7	39370	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	A4BAD696E4FF7D6D5BA293FC7D1C3660	39369	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	B8B91166A48F9B7BF0EAE96660D48613	39368	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	8560EFC2E907973A93BD338E6A562D9E	39367	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	BE0A1A71D4CBDC84BCDD0A0A2550347A	39366	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	20FAB7B813A9FD4FE933E251FB362AF7	39365	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	BFE0FC3555C335DD54A01B671A5D980F	39364	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	2EE6EE12502539DF9555963D9A95D132	39363	PE	4.1 kB	W32/AI.S
2024/03/19 16:38:42	DF7359FE36A8DEEC510CFC30569F4B82	39362	PE	4.1 kB	W32/AI.S

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. The *Search* function only supports exact matches. Wildcards are not supported.

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.

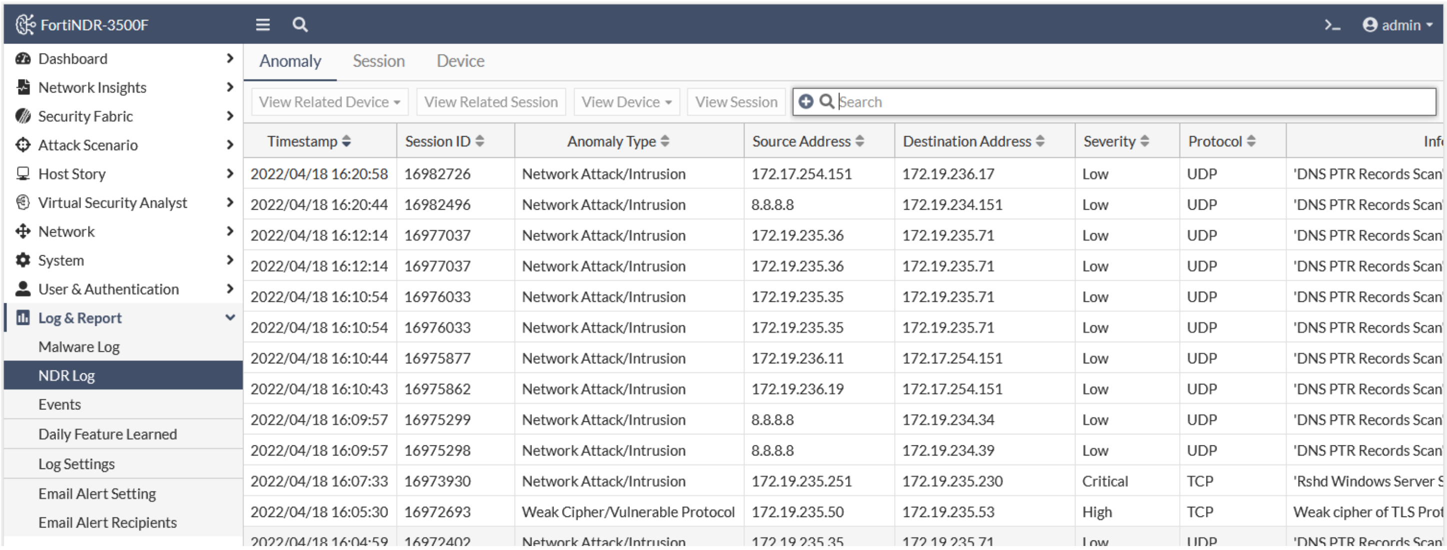
To search a detection:

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.



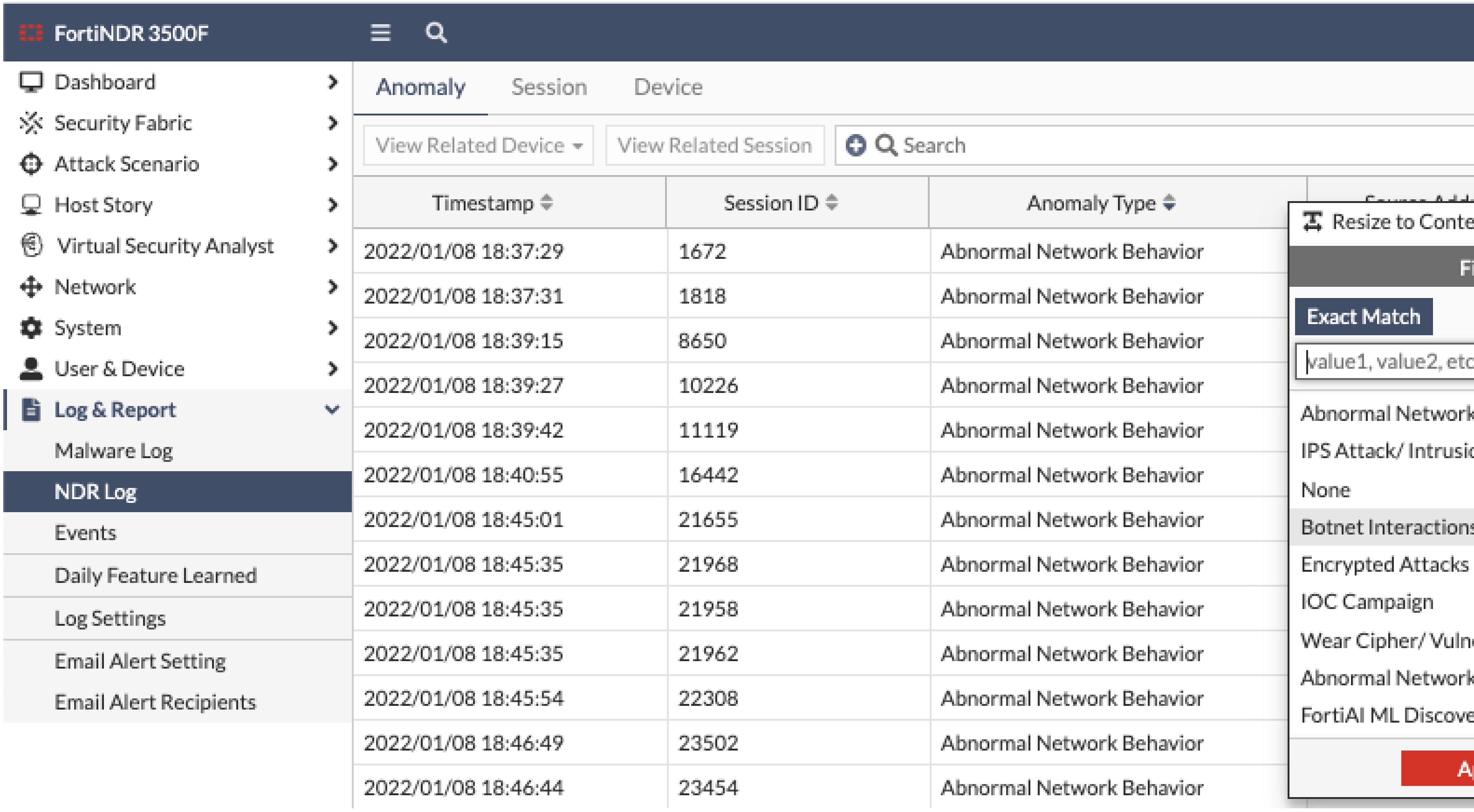
Timestamp	Session ID	Anomaly Type	Source Address	Destination Address	Severity	Protocol	Inf
2022/04/18 16:20:58	16982726	Network Attack/Intrusion	172.17.254.151	172.19.236.17	Low	UDP	'DNS PTR Records Scan'
2022/04/18 16:20:44	16982496	Network Attack/Intrusion	8.8.8.8	172.19.234.151	Low	UDP	'DNS PTR Records 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.

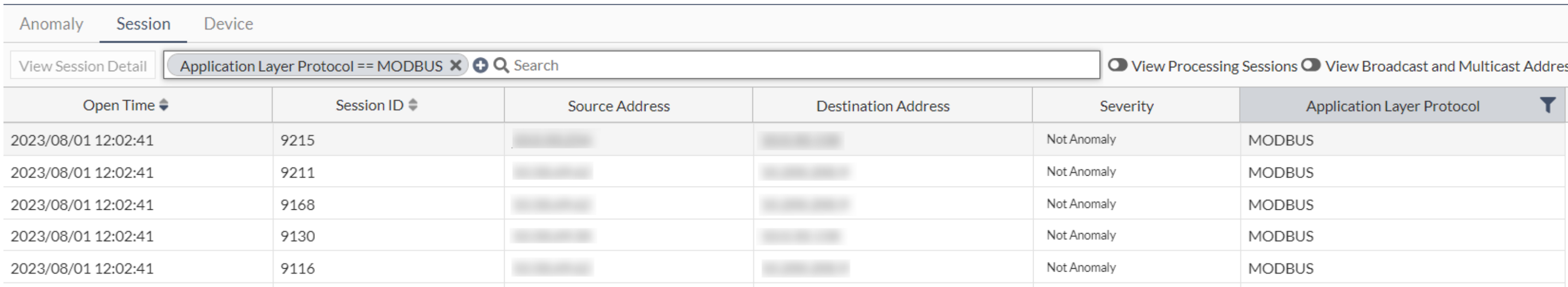


Timestamp	Session ID	Anomaly Type
2022/01/08 18:37:29	1672	Abnormal Network Behavior
2022/01/08 18:37:31	1818	Abnormal Network Behavior
2022/01/08 18:39:15	8650	Abnormal Network Behavior
2022/01/08 18:39:27	10226	Abnormal Network Behavior
2022/01/08 18:39:42	11119	Abnormal Network Behavior
2022/01/08 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

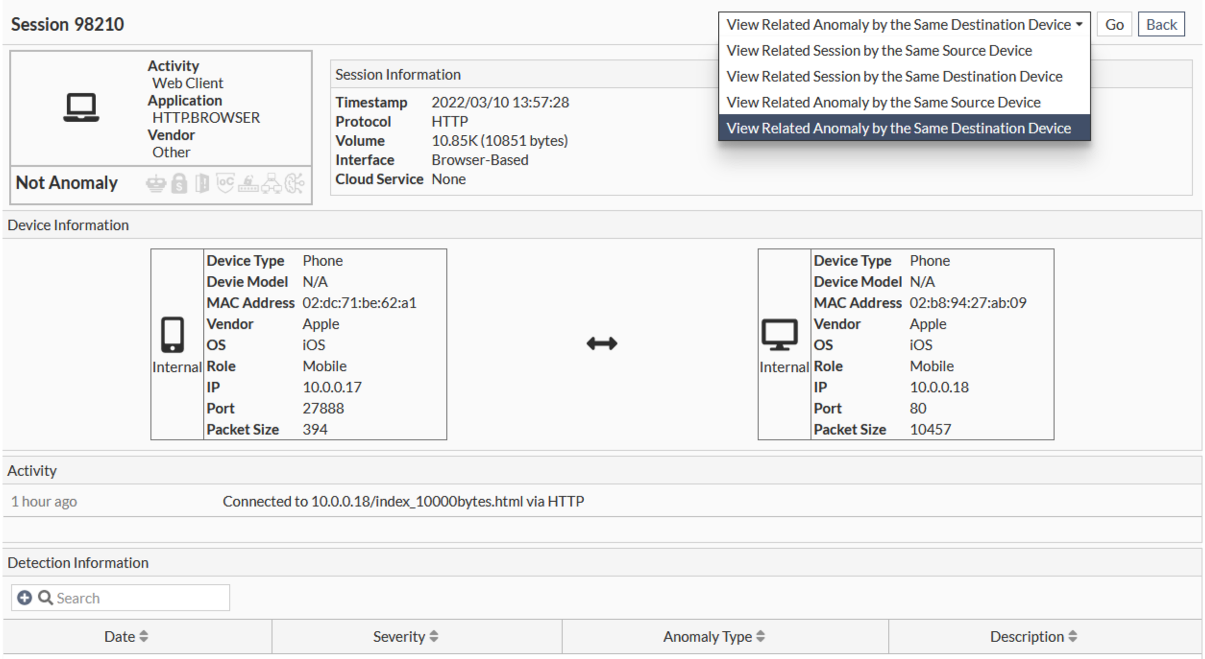
Use the *Sessions* tab to understand the relationship between sessions and anomalies. There could be multiple behaviors within a session and some connections within a session could be an anomaly. For example, a user accessing the Internet browses both Facebook normally and hits an IOC campaign Emotet 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.


Anomaly
Session
Device
View Session Detail
Application Layer Protocol == MODBUS
Search
View Processing Sessions
View Broadcast and Multicast Addre

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

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



Session 98210

View Related Anomaly by the Same Destination Device
Go
Back
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

Activity Web Client
Application HTTP.BROWSER
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

Device Information

Internal

Device Type	Phone
Devie 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

Internal

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

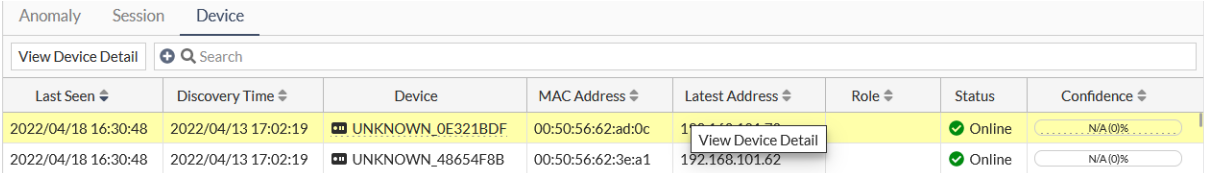
1 hour ago	Connected to 10.0.0.18/index_10000bytes.html via HTTP

Detection Information

Date	Severity	Anomaly Type	Description

Device Tab

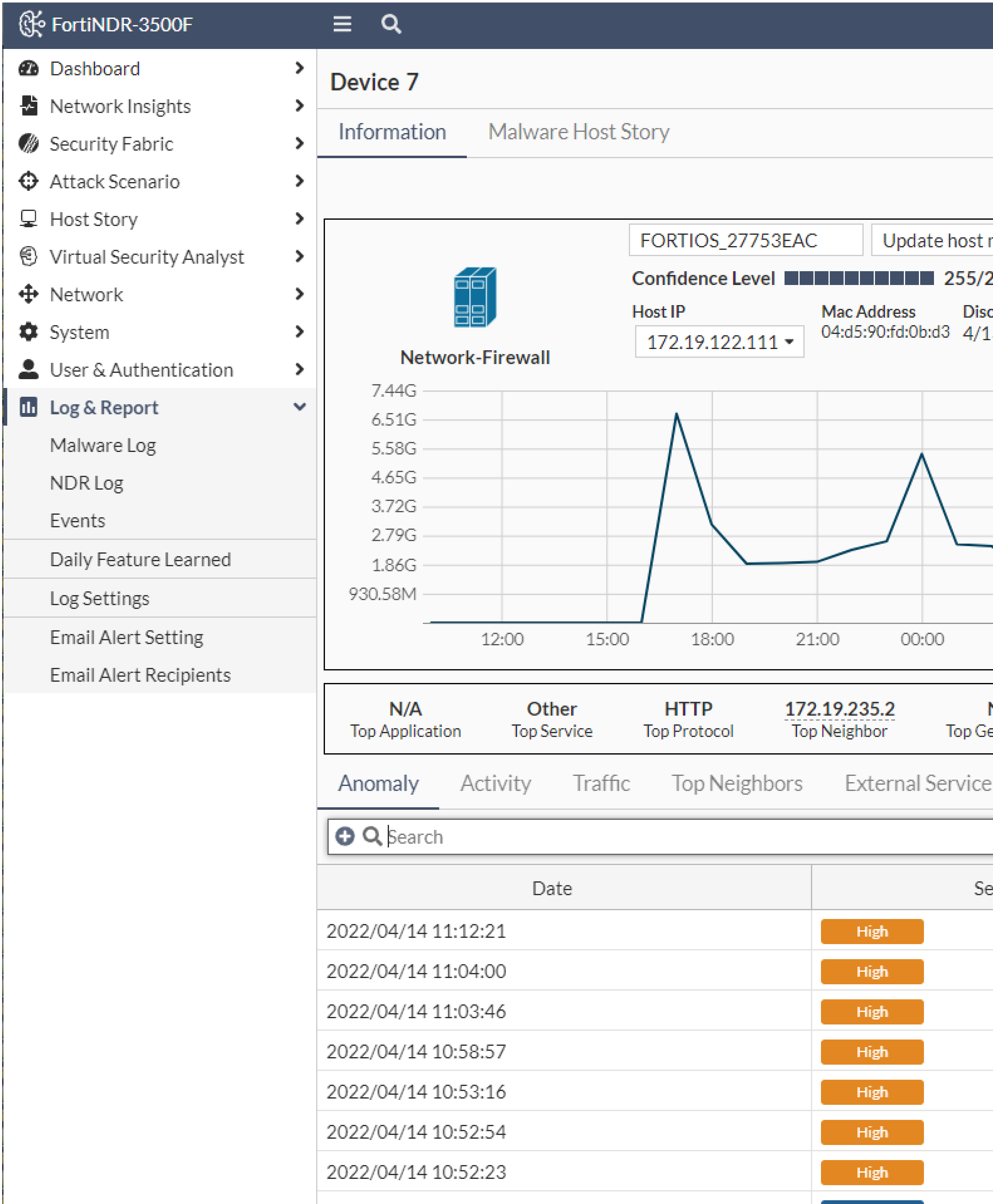
The Device tab the devices detected by FortiNDR. The FortiGuard IOT service is used to identify device information based on the MAC address. You can drill down to the devices page by clicking *View Device Detail* details.



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	1[illegible]		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 heat-map for anomalies over the selected time period. A line graph shows the device traffic (inbound and outbound bandwidth combined). The *Confidence Level* indicates our confidence in identifying the device category.

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



Device 7

FORTIOS_27753EAC

Confidence Level 255/2

Host IP: 172.19.122.111

Mac Address: 04:d5:90:fd:0b:d3

Disc: 4/1

N/A Top Application

Other Top Service

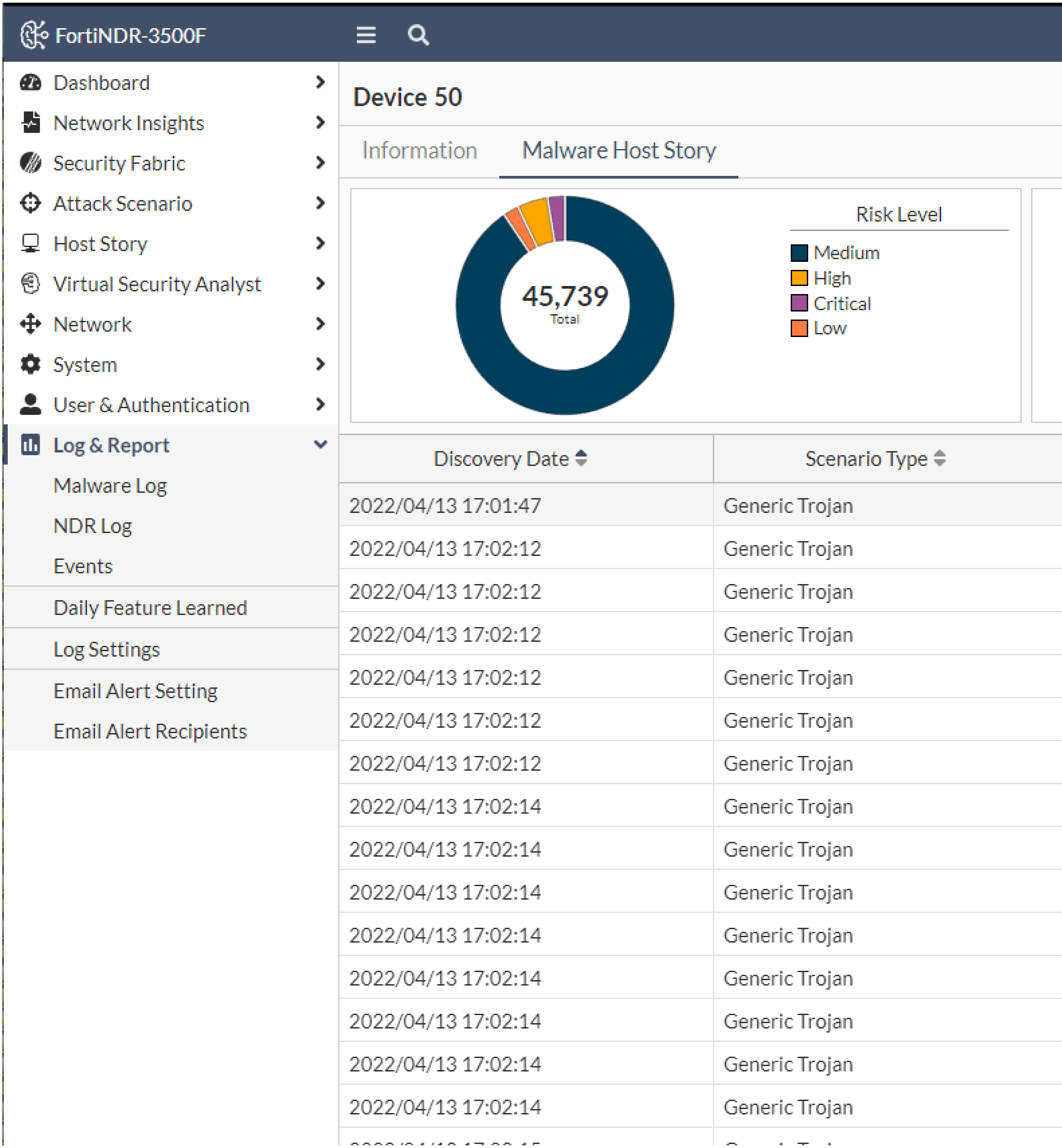
HTTP Top Protocol

172.19.235.2 Top Neighbor

N Top Ge

Date	Se
2022/04/14 11:12:21	High
2022/04/14 11:04:00	High
2022/04/14 11:03:46	High
2022/04/14 10:58:57	High
2022/04/14 10:53:16	High
2022/04/14 10:52:54	High
2022/04/14 10:52:23	High

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



Discovery Date	Scenario Type
2022/04/13 17:01:47	Generic Trojan
2022/04/13 17:02:12	Generic Trojan
2022/04/13 17:02:12	Generic Trojan
2022/04/13 17:02:12	Generic Trojan
2022/04/13 17:02:12	Generic Trojan
2022/04/13 17:02:12	Generic Trojan
2022/04/13 17:02:12	Generic Trojan
2022/04/13 17:02:14	Generic Trojan
2022/04/13 17:02:14	Generic Trojan
2022/04/13 17:02:14	Generic Trojan
2022/04/13 17:02:14	Generic Trojan
2022/04/13 17:02:14	Generic Trojan
2022/04/13 17:02:14	Generic Trojan
2022/04/13 17:02:14	Generic Trojan
2022/04/13 17:02:14	Generic Trojan

Events

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

The *Events* page displays the following information:

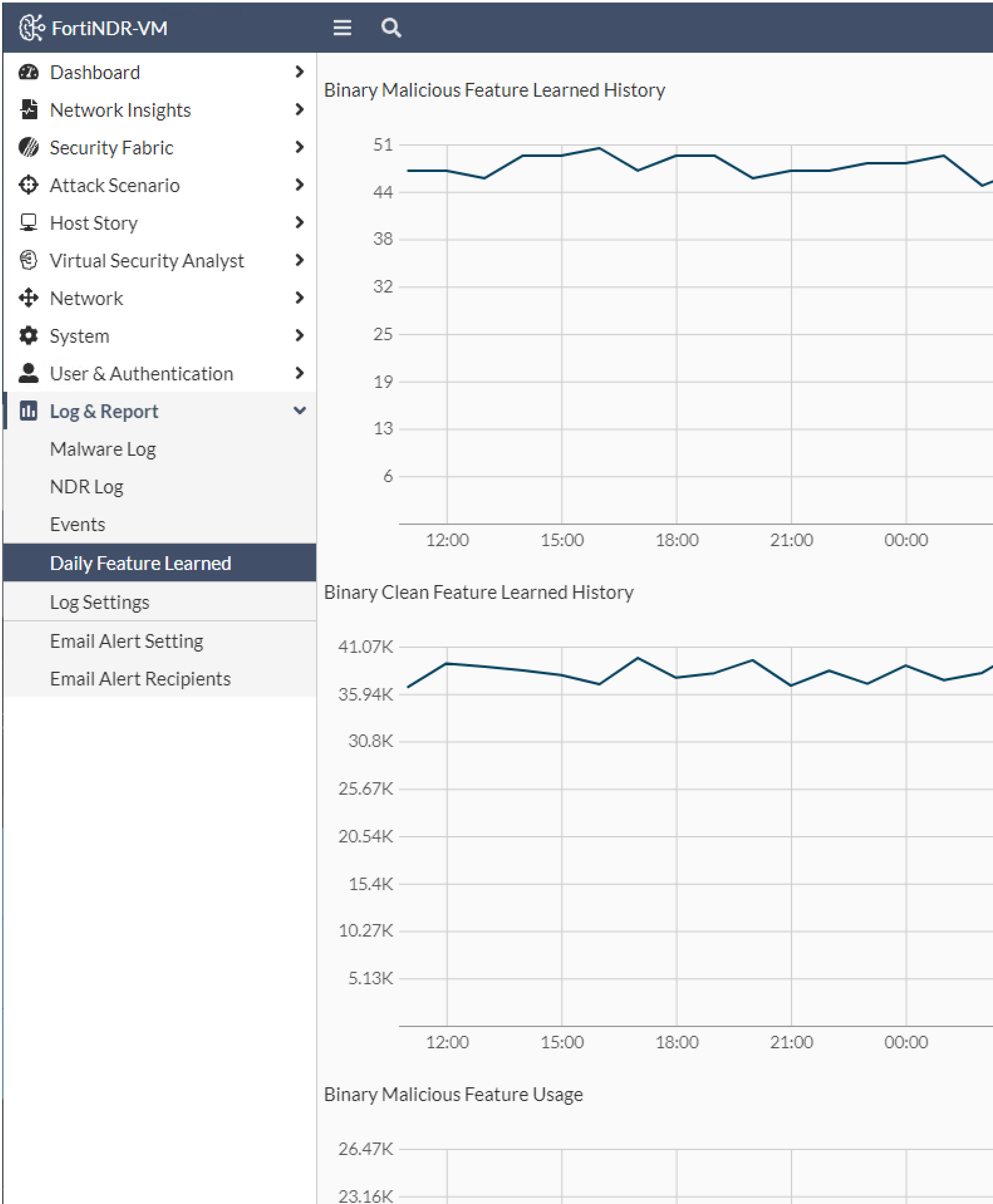
Date	The date the event occurred.
Level	The security level.
User	The user that triggered the event.
Message	The log message.

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

General	The entry date.
Source	The event source.
Action	The *Action* and *Status*.
Security	The security level.
Event	The event message describing the event.
Other	The *Log ID*, *Category* and *Sub Category* 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.



Binary Malicious Feature Learned History

Binary Clean Feature Learned History

Binary Malicious Feature Usage

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 (Center Standalone) " on page 153.

To configure the Log Settings:

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

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

3. Click *OK*.

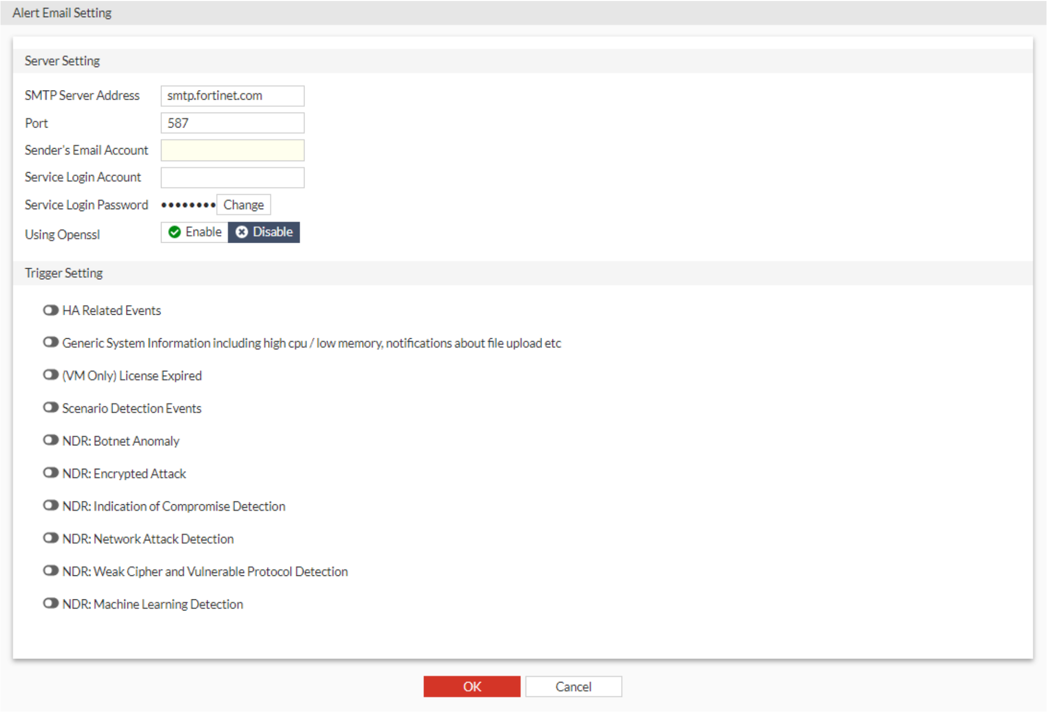
Alert Email Setting

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



Alert Email Setting

Server Setting

SMTP Server Address: smtp.fortinet.com

Port: 587

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

3. Click *OK*.
4. Add email addresses to the email recipient list. See, "Email Alert Recipients" below.

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 Recipien*t 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" devidd="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" devidd="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" vnamee="DNS.Amplification.Detection" vulntype="Anomaly"
```

```
date="2022-02-10" time="18:32:54" tz="PST" logid="0604000001" devid-
d="FAI35FT321000001" type="ndr" subtype="IPS attack" severity="medium" ses-
sionid=9092973 alproto="OTHER" tlproto="ICMP" srcip="172.19.235.62" srcport=0
dstip="172.19.236.50" dstport=771 behavior="CONN" vname-
e="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-
d="FAIVMSTM21000033" type="ndr" subtype="Weak cipher" severity="medium" ses-
sionid=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-
d="FAIVMSTM21000033" type="ndr" subtype="Weak cipher" severity="medium" ses-
sionid=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-
d="FAIVMSTM21000033" type="ndr" subtype="ML" severity="low" sessionid=1135774
```

```
alproto="DNS" tlproto="TCP" srcip="17.1.10.185" srcport=35546 dstip-
p="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-

Log Type	Subtype	Log Sample
		="0400000001" devid="FAI35FT319000026" type="event" subtype="user" level="information" user="admin" ui="init" actionn="none" status="none" msg="changed settings of 'ipaddr' for 'system syslog fortianalyzer settings'"
	System	date=”2021-03-31” time=”15:50:19” tz=”PDT” logidd=”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” logidd=”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” logidd=”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” logidd=”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” logidd=”0408000001” devid=”FAIVMSTM21000033” type=”event” subtype=”malware” level=”information” status=”success” featurelstcnt=19 featurelst= “Generic Trojan, Trojan, BackDoor, Application, Virus, Worm, Downloader, Redirector, Dropper, Phishing, Exploit, Proxy, Ransomware, Banking Trojan, PWS, Infostealer, Clicker, CoinMiner, WebShell” featurecounts=”35476, 81, 15, 9, 7, 3, 3, 3, 3, 1, 1,1,1,1,1,1,1,1,1”
		date=”2021-03-31” time=”16:18:28” tz=”PDT” logidd=”0408000001” devid=”FAIVMSTM21000033” type=”event” subtype=”malware” level=”information” status=”success”

Log Type	Subtype	Log Sample
Attack		featurelstcnt=10 featurelst= “Generic Trojan, Trojan, BackDoor, Application, Virus, Worm, Downloader, Redirector, Dropper, Phishing” featurecounts=”35476, 81, 15, 9, 7, 3, 3, 3, 3, 1”
	Attack chain	date="2021-05-21" time="10:23:05" tz="PDT" logid="0500000001" devhost="FAI35FT321000001" devid="FAI35FT321000001" typee="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" md55="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 detypelstcnt=3 detypelst=”worm,trojan,downloader” detypecounts=”64,64,2”

Troubleshooting

FortiNDR troubleshooting tips

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

Best practices:

Issue Type	Recommendations / Possible cause	CLI command	Comments
General hang issue and disconnect issues	Reload all services to see if the issue is still reproducible	`exec reload`	
CPU usage consistently above 85%	Turn off feature learning to save more resources	`exec learner off`	
GUI not responsive/DB related error (*and you can afford to lose all current data*)	If you installed an interim build (other than GA) and are willing to wipe all db records	`exec db restore`	Run exec reload to see if issue is still reproducible
GUI not responsive/DB related error (*and you to make a best effort to keep your data*)	If you installed an interim build (other than GA) and cannot wipe all db records	`diagnose system db`	Patches db at best efforts.
General Issues	Retrieve and record all information	`get sys status`	If you are seeing high CPU and MEM usage, please consider provisioning more resources.
General VM issues	Retrieve and record all information for VMs	`diag sys vm`	Observe for any FDS code other than 200, and if not 200, please check connections to FDN and license status.

Recommended Debug Setup:

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

General Debug Logs Retrieval

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

File scanning related issues

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

To perform a general check:

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

Troubleshooting HTTP2 issues from FortiGate v7.0 onwards:

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

Manual Upload/API Submission/FortiSandbox Integration

For all issues:

Start with a single file upload and fetch results from the same subnet as directed from where the client resides. See "Appendix A: API guide" on page 248.

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

For an optimal support experience, we recommend including the following information in your support ticket:

Model Name	What Model is your platform
Firmware Version	Which Firmware is your platform
Always Reproducible	True/False
Reproducible Steps	If this issue is reproducible, please include the steps to reproduce this issue.
Actual Result vs Expected Results	What are the expected results and actual results.
Troubleshooting recommendations used	Please describe the troubleshooting recommendations you attempted and the outcome.
Crash Log output	Run the following CLI command `crash_log_date` and provide the output. For more information see, diagnose debug.
Kernel Log output	Record the output from `diag debug kernel display`. For more information see, diagnose debug.

Application Log Output	Specified log output from affected application. For more information see, diagnose debug.
Database Error Log	Record the log output from `diag deb database error-log.`
FortiNDR Event Log	If configured with FAZ/FortiSIEM, please provide logs from FAZ/FortiSIEM. Otherwise, please include a screen shot from *Event* tab.
Client-Side Log	When FortiNDR acts as a server role (ICAP, OFTP and HTTP2 inline blocking etc.), please also include logs from the client side.
System Status	Provide the CPU and MEM usage when the issue occurs.
FortiNDR configuration	How many ports are configured/used? How many applications are used, and how are they configured? If you have a backup configuration file, please include it in your support ticket. For more information, see "Backup or restore the system configuration" on page 175.
FortiNDR Load	For configured applications, how much load are applied. For example: • For AV, how many files are being sent to FortiNDR, and what is the file size distributions and file type distributions? • For NDR, what is the bandwidth for traffic and what is the distribution of application type?
For non-hardware platform:	
Virtual machine provisioning	• How many CPU/Mems are provisioned? • How was the disk provisioned: Thin, Thick etc.
Hosting Hardware specifications	CPU Model Number, RAM Channels, DISK model number.
Physical hosting hardware load	A historical log of host hardware status to indicate CPU and MEM usage

FortiNDR health checks

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

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

To turn network traffic detection on and off:

Run the following command:

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

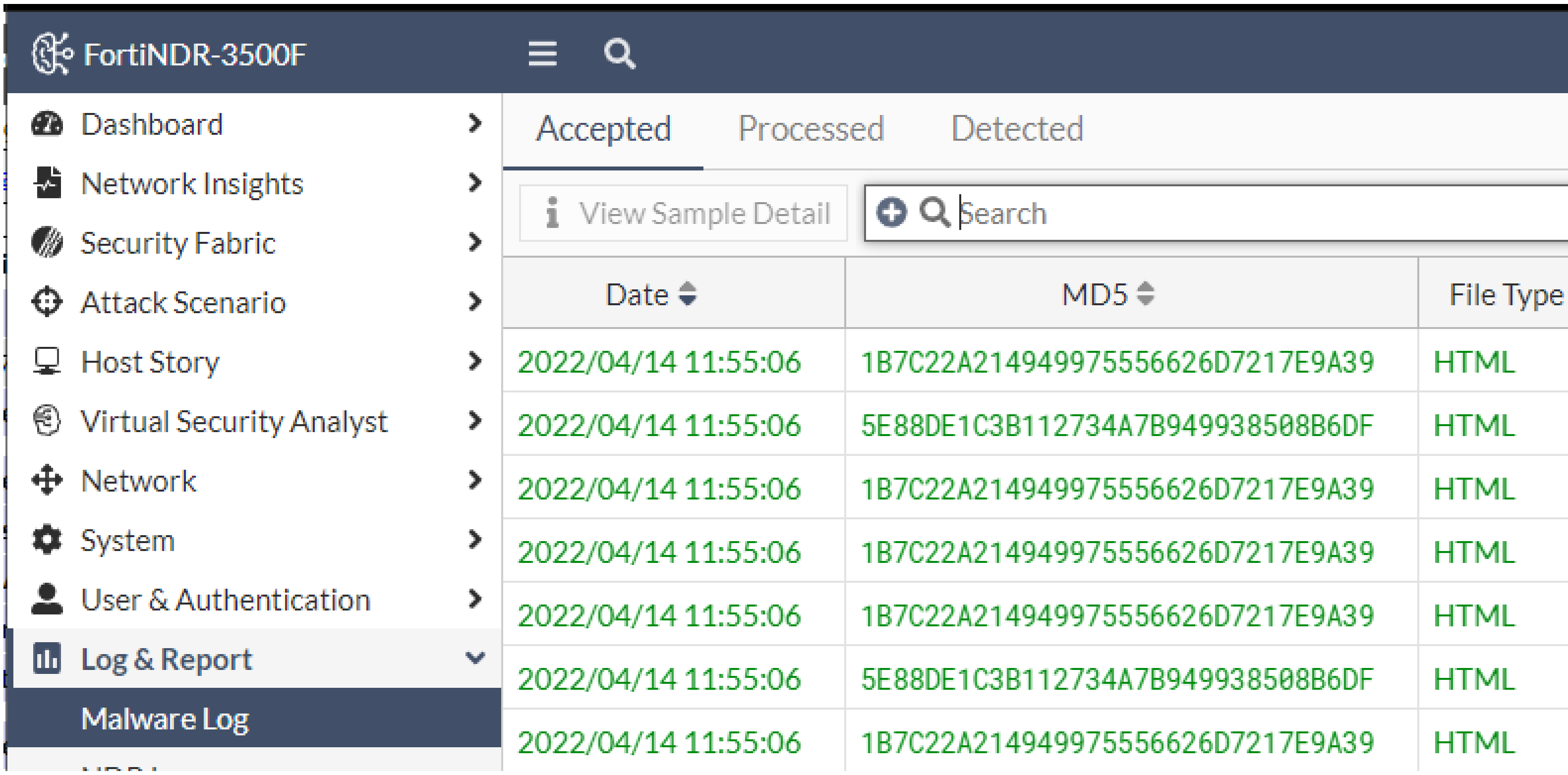
To turn sniffer malware detection on and off for troubleshooting:

Run the following command:

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

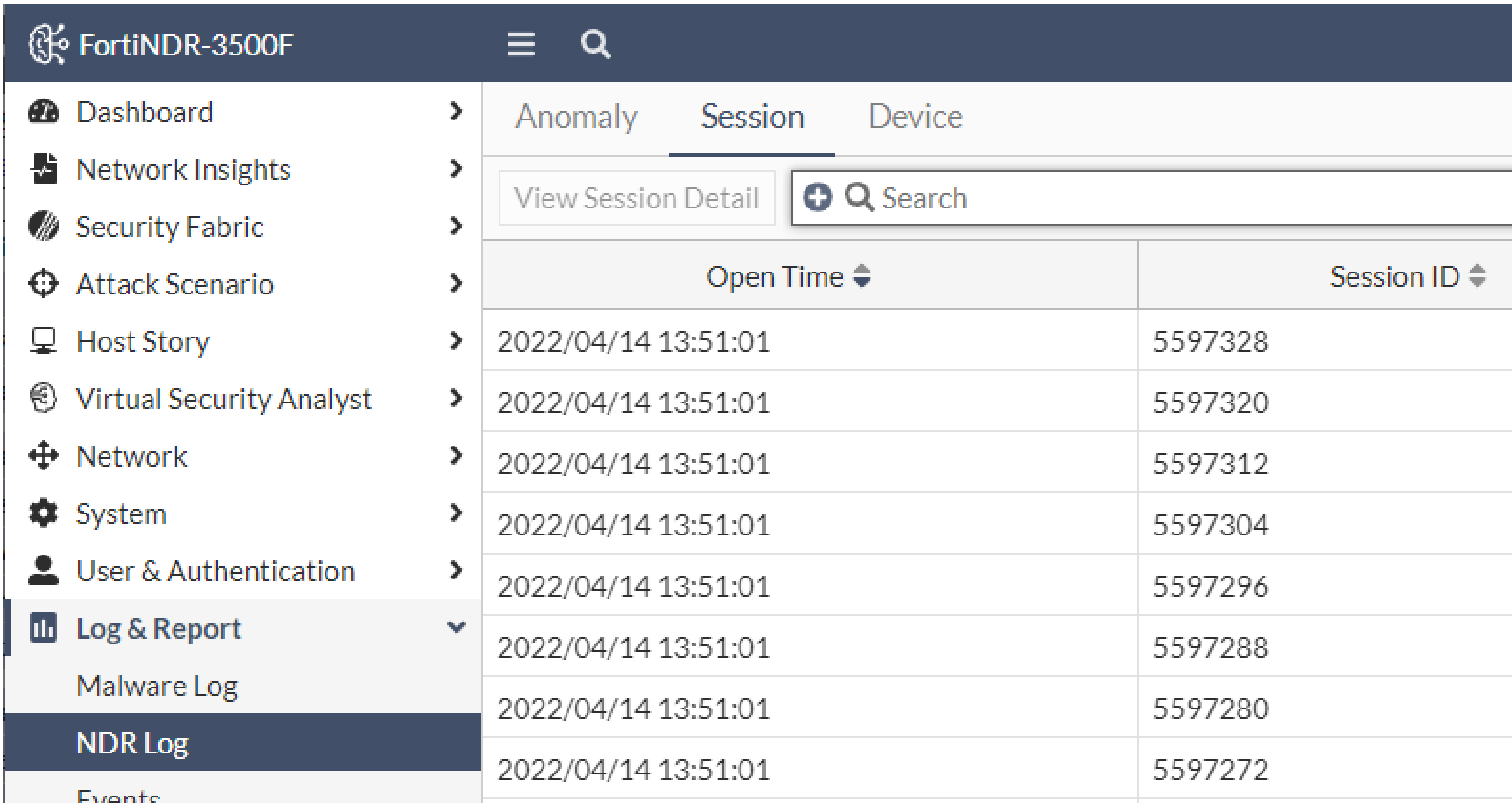
The current version of the Malware sniffer only sniffs traffic on Port2.

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



Date	MD5	File Type
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML

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



Open Time	Session ID
2022/04/14 13:51:01	5597328
2022/04/14 13:51:01	5597320
2022/04/14 13:51:01	5597312
2022/04/14 13:51:01	5597304
2022/04/14 13:51:01	5597296
2022/04/14 13:51:01	5597288
2022/04/14 13:51:01	5597280
2022/04/14 13:51:01	5597272

Sniffer diagnosis

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

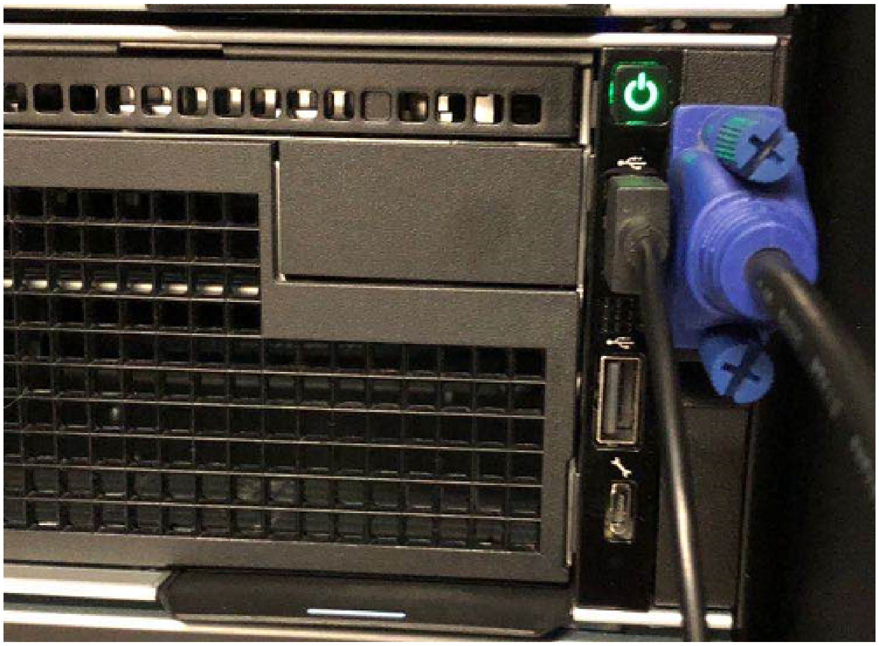
The sniffer will not save unsupported file types or supported but corrupted files. For example, if the traffic contains a corrupted zip file that cannot be unzipped, the sniffer will not save it to the *Log & Report >Malware Log*.

Rebuild RAID disk

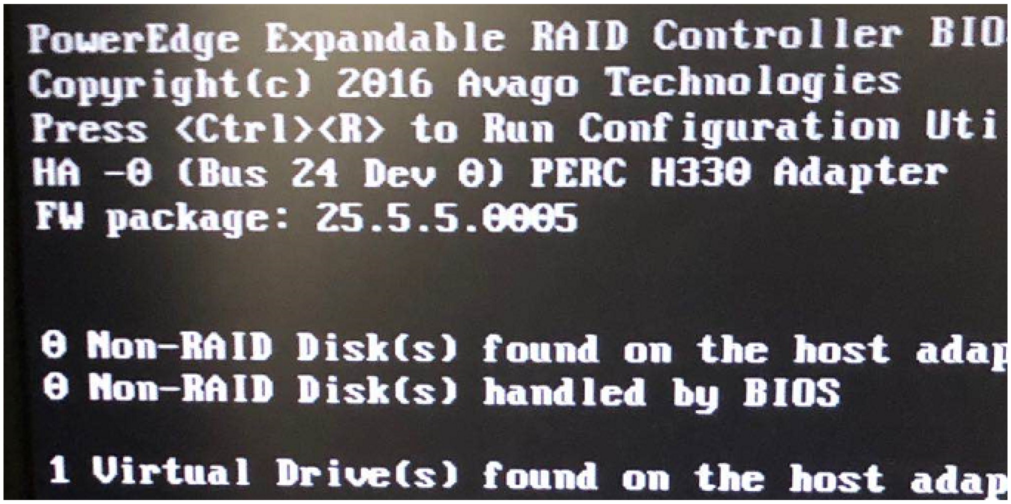
If you need to rebuild the data disk and configure FortiNDR-3500F from scratch, follow this procedure.

To rebuild the RAID disk:

1. Plug the monitor and keyboard directly into FortiNDR.

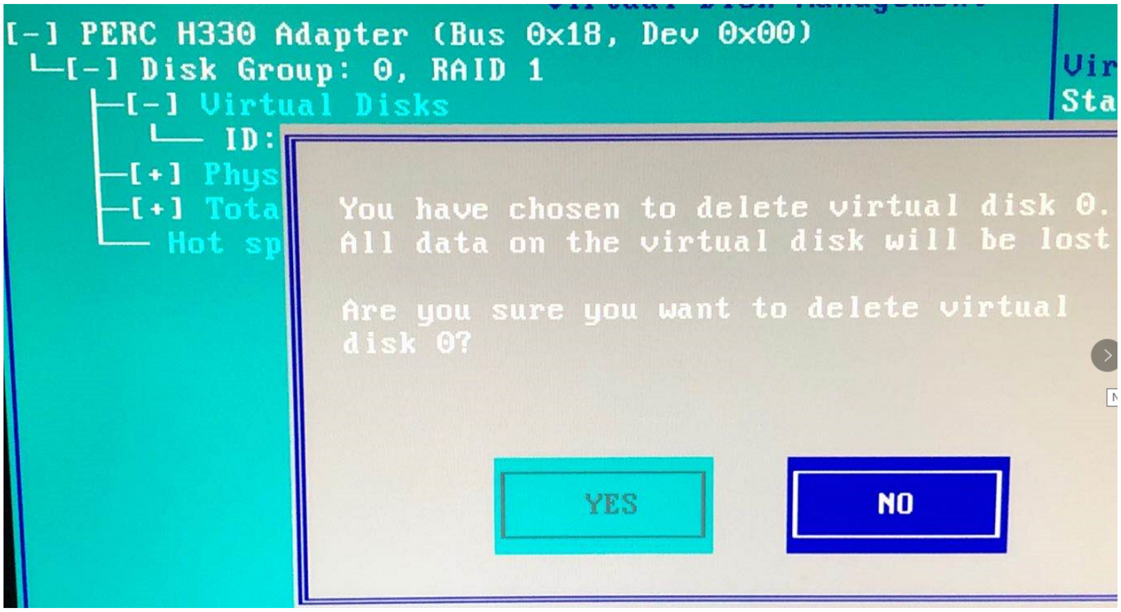


2. Boot FortiNDR and keep pressing `Ctrl R` when FortiNDR is booting.



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


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

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

3. Delete virtual disk 0.

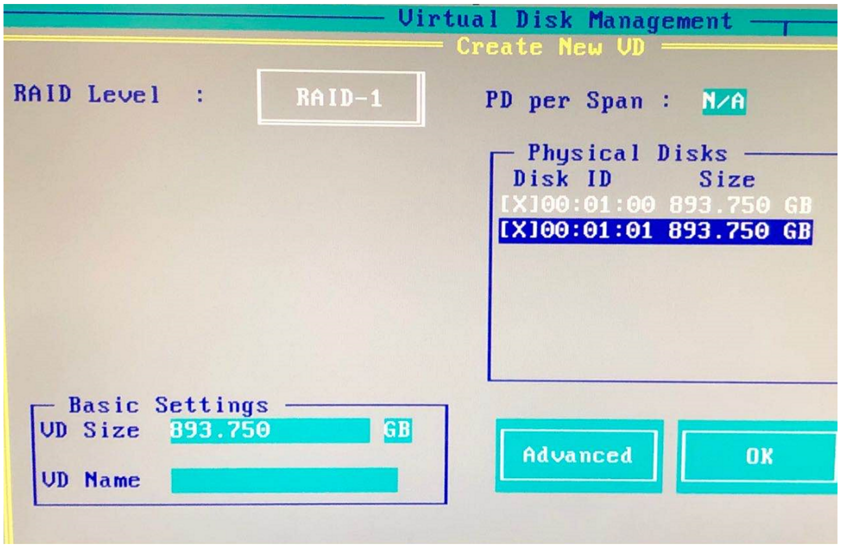


```
[-] PERC H330 Adapter (Bus 0x18, Dev 0x00)                 Vir
 └[-] Disk Group: 0, RAID 1                                 Sta
    ├[-] Virtual Disks
    │  └── ID:
    ├[+] Phys
    ├[+] Tota
    └── Hot sp
```

You have chosen to delete virtual disk 0.
All data on the virtual disk will be lost

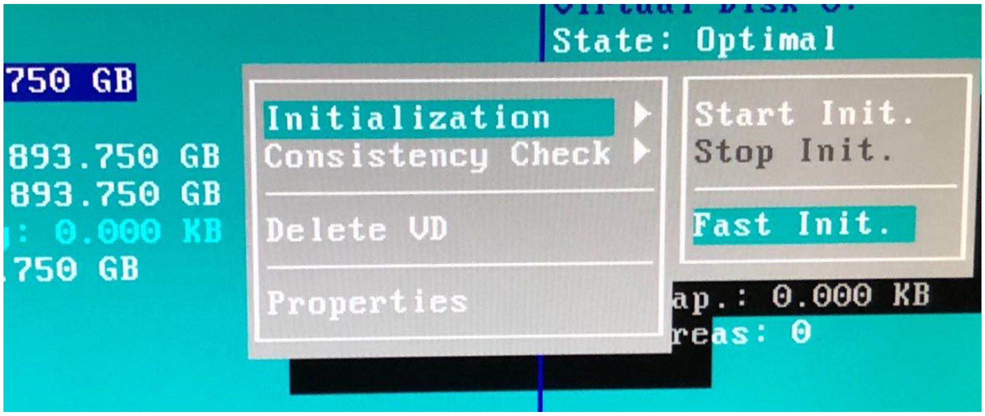
Are you sure you want to delete virtual
disk 0?

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



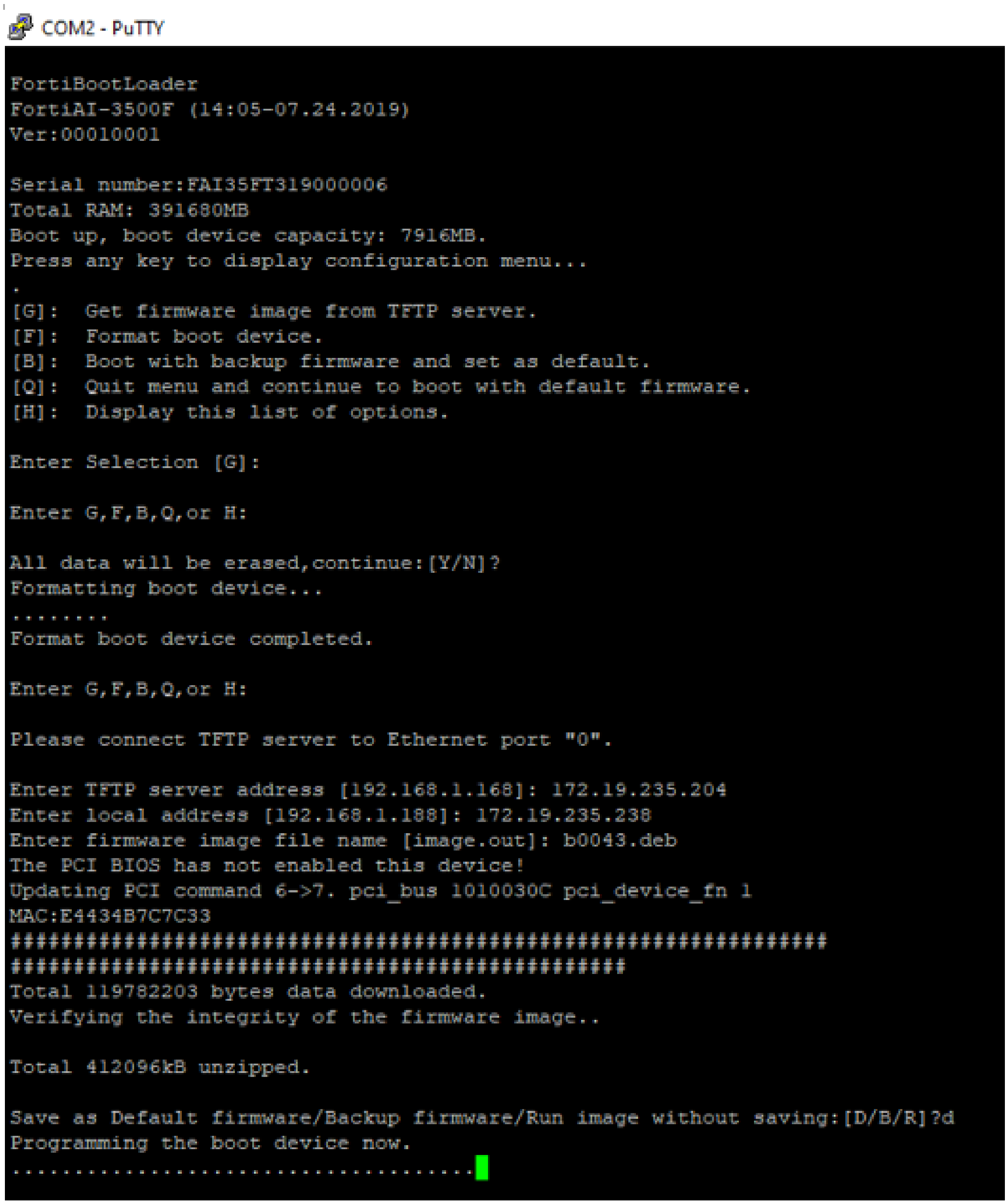
```
                     Virtual Disk Management
                          Create New VD
RAID Level  :    RAID-1          PD per Span :  N/A

                                  Physical Disks
                                  Disk ID       Size
                                 [X]00:01:00 893.750 GB
                                 [X]00:01:01 893.750 GB

  Basic Settings
 VD Size   893.750        GB
 VD Name
```

5. Fast init the new virtual disk.



6. When the initialization is finished, reboot FortiNDR.
7. During reboot, press any key to enter bootloader.

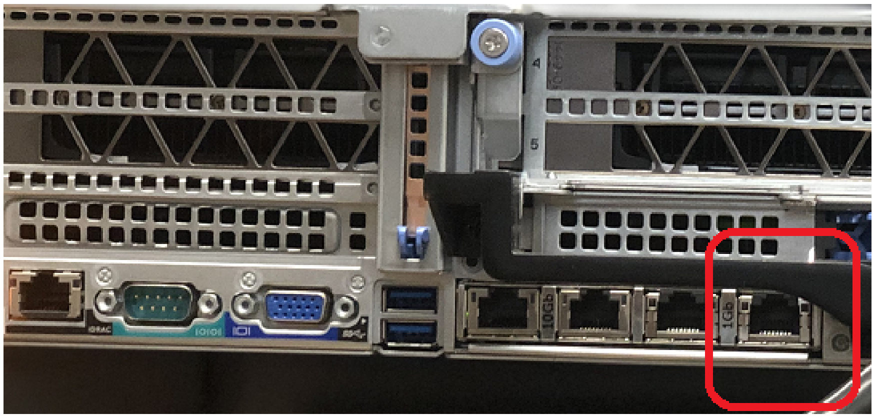
   Ensure the keyboard is not plugged directly into FortiNDR as that might prevent you from entering into the bootloader menu.



```
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 for Center mode

FortiNDR Center mode aggregates data from sensors periodically and performs machine learning on traffic on sensors based on the configured profiles. Disk retention on Center mode is controlled by CLI command `execute center-retention-setting`.

Disk retention will depend on the number of sensors and traffic analyzed.

Managing FortiNDR disk usage for Standalone and Sensor mode

FortiNDR analyzes files and packets "on the fly" and requires plenty of disk space to store attacks. FortiNDR-1000F comes with 2 disks with RAID and is not expandable. FortiNDR -3500F comes with eight SSD drives by default and can support up to 16 SSD in total. The more disks the better the unit performs. For better retention (for example, in center mode) managing multiple sensors fully populated with 16 disk is recommended.

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

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

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

To view the disk usage:

Go to *Dashboard > System Status*.

To expand FortiNDR VM storage with the CLI:

```
execute expandspooldisk.
```

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

Exporting detected malware files

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

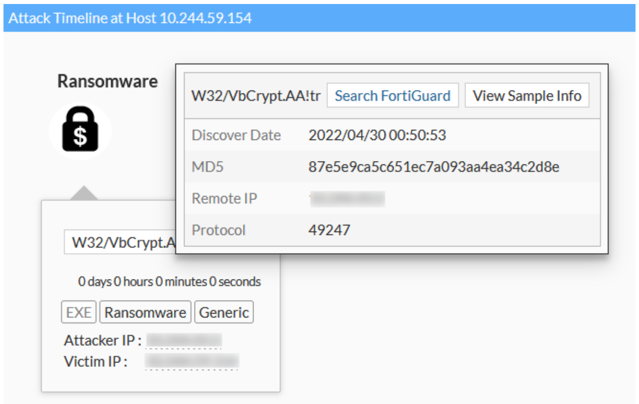
To export detected malware files with the CLI:

```
execute export file-report
```

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

To export detected malware files with the GUI:

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



Attack Timeline at Host 10.244.59.154

Discover Date	2022/04/30 00:50:53
MD5	87e5e9ca5c651ec7a093aa4ea34c2d8e
Remote IP	[redacted]
Protocol	49247

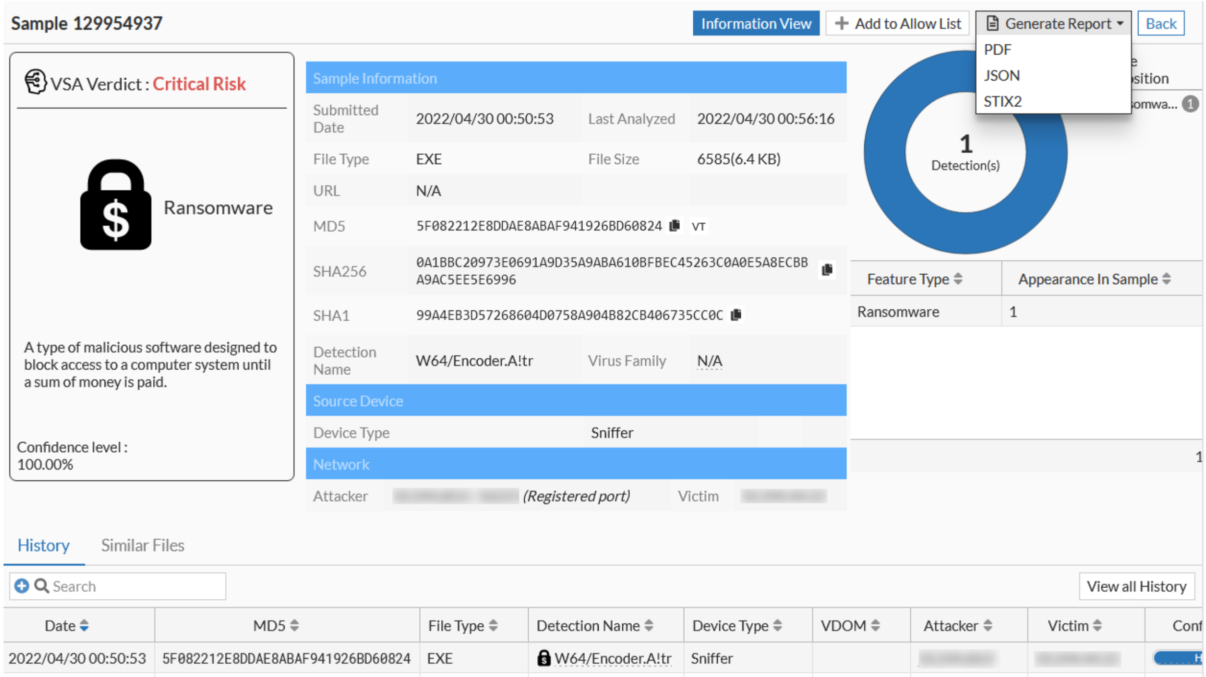
W32/VbCrypt.A

0 days 0 hours 0 minutes 0 seconds

Attacker IP : [redacted]

Victim IP : [redacted]

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



Sample 129954937

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	0A1BBC20973E0691A9D35A9ABA610BFBEC45263C0A0E5A8ECBB A9AC5EE5E6996		
SHA1	99A4EB3D57268604D0758A904B82CB406735CC0C		
Detection Name	W64/Encoder.A!tr	Virus Family	N/A

Source Device

Device Type	Sniffer

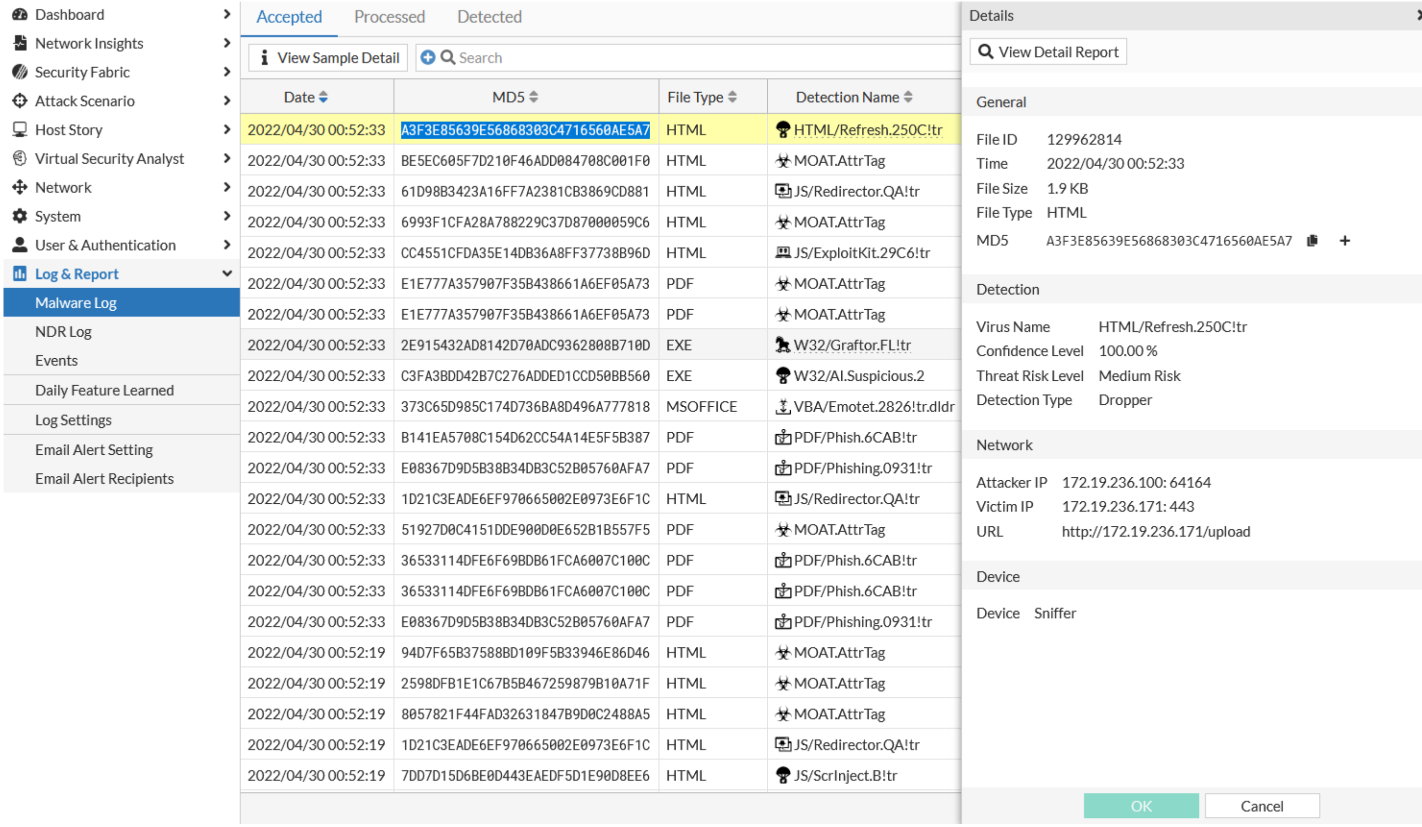
Network

Attacker [redacted] (Registered port) Victim [redacted]

Feature Type	Appearance In Sample
Ransomware	1

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]	H

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



Date	MD5	File Type	Detection Name
2022/04/30 00:52:33	A3F3E85639E56868303C4716560AE5A7	HTML	HTML/Refresh.250C!tr
2022/04/30 00:52:33	BE5EC605F7D210F46ADD084708C001F0	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	CC4551CFDA35E14DB36A8FF37738B96D	HTML	JS/ExploitKit.29C6!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/Graftor.FL!tr
2022/04/30 00:52:33	C3FA3BDD42B7C276ADDED1CCD50BB560	EXE	W32/AI.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	1D21C3EADE6EF970665002E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:33	51927D0C4151DDE900D0E652B1B557F5	PDF	MOAT.AttrTag
2022/04/30 00:52:33	36533114DFE6F69BDB61FCA6007C100C	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	36533114DFE6F69BDB61FCA6007C100C	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	1D21C3EADE6EF970665002E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:19	7DD7D15D6BE0D443EAEDF5D1E90D8EE6	HTML	JS/ScrInject.B!tr

General

File ID 129962814
Time 2022/04/30 00:52:33
File Size 1.9 KB
File Type HTML
MD5 A3F3E85639E56868303C4716560AE5A7

Detection

Virus Name HTML/Refresh.250C!tr
Confidence Level 100.00 %
Threat Risk Level Medium Risk
Detection Type Dropper

Network

Attacker IP 172.19.236.100: 64164
Victim IP 172.19.236.171: 443
URL http://172.19.236.171/upload

Device

Device Sniffer

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

Formatting the database

To format the database with the CLI:

```
execute db restore
```

Using `execute db restore` will format and delete the entire database.

Use caution when executing this command and backup detection beforehand if required.

Export malware

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

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

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

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

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

The zip file default password is `infected`.

Working with false positives and false negatives

False positives and false negatives are to be expected in every technology. For example, you may encounter a small percentage of false positives among thousands of files when there is a high volume of HTTP traffic processed by the sniffer. If there are five false positive samples out of 2000 files, the false positive rate is: 0.25%. A false negative occurs when FortiNDR does not detect any malware.

To minimize false positive and negatives:

Recommendation	Description
Ensure you are using the latest version of ANN	To check the latest version of FortiNDR ANN, see the *Network Detection and Response Service* page at https://www.fortiguard.com/services/fortindr.
Submit feedback to FortiGuard	When you encounter a false positive (FP), you have the option to add the sample to the *Allow list* with the GUI. Furthermore, you can enable *Submit feedback to FortiGuard* to submit the sample directly to Fortiguard. For information, see "Malware Log " on page 190.

Troubleshoot ICAP and OFTP connection issues

Troubleshooting ICAP issues:

1. Reproduce the issue:
   1. Retrieve the latest ICAP server logs by running the CLI command: `diag debug icap`
   2. 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.

To check ICAP traffic in port1:

Use the CLI command:

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

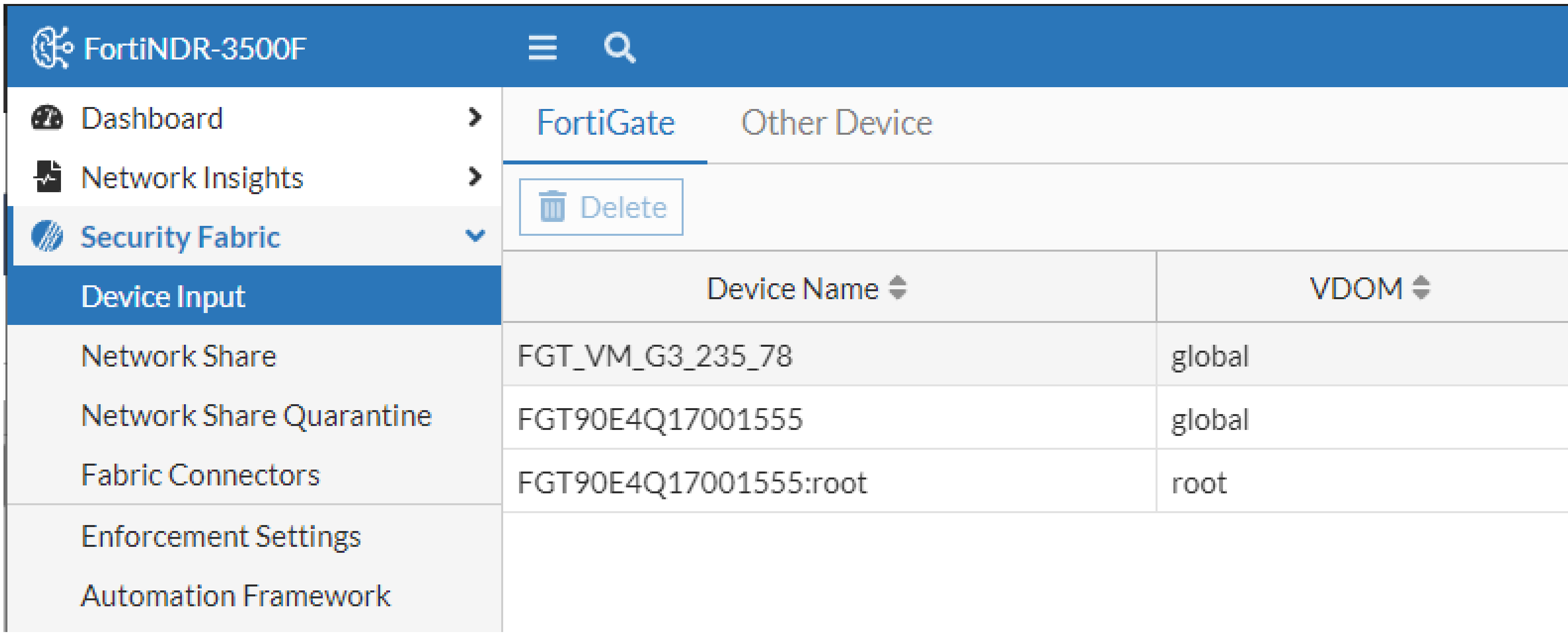
To check OFTP traffic in port1:

Use the CLI command:

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

To verify a device is authorized:

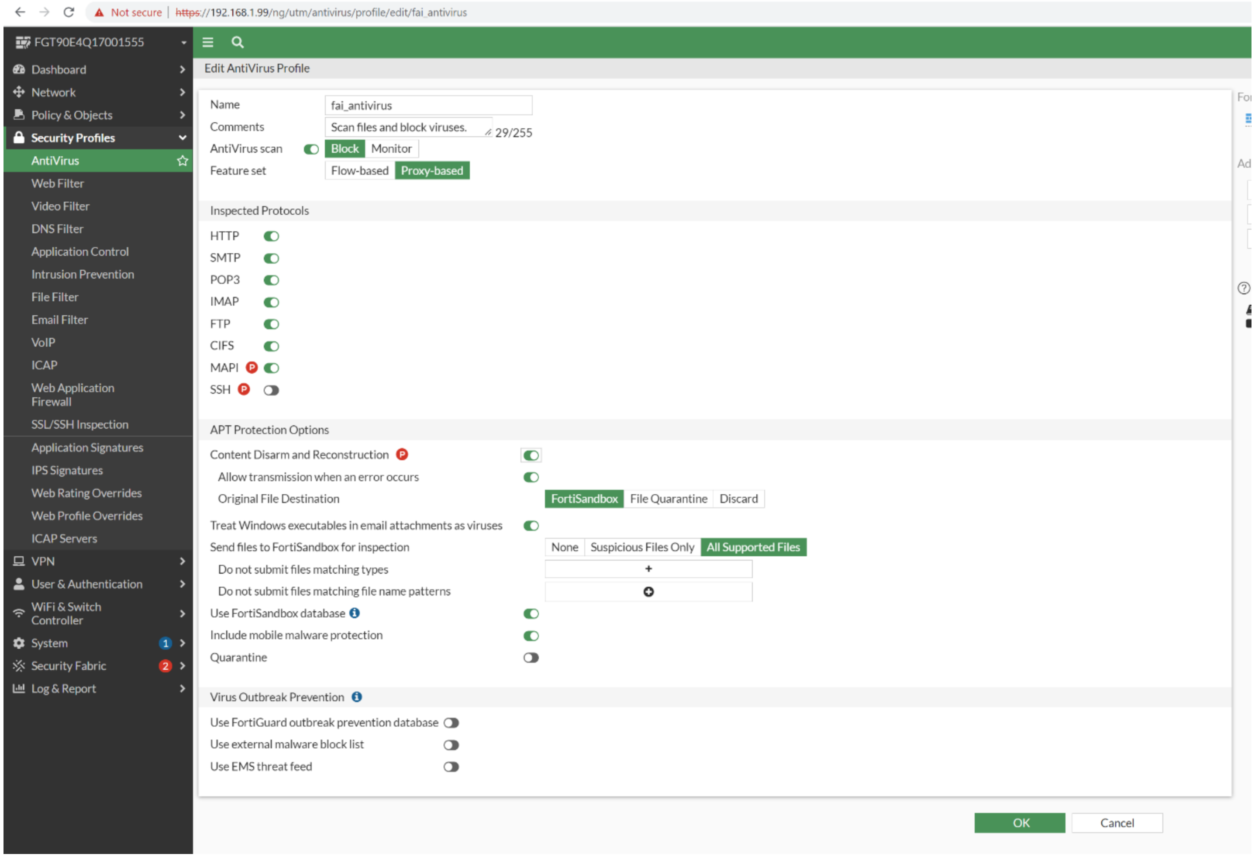
Go to *Security Fabric > Device Input* and check the Authorized column.



Device Name	VDOM
FGT_VM_G3_235_78	global
FGT90E4Q17001555	global
FGT90E4Q17001555:root	root

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*.



Edit AntiVirus Profile

Name: fai_antivirus
Comments: Scan files and block viruses. 29/255
AntiVirus scan: ● Block | Monitor
Feature set: Flow-based | Proxy-based (selected)

Inspected Protocols

- HTTP ●
- SMTP ●
- POP3 ●
- IMAP ●
- FTP ●
- CIFS ●
- MAPI ●
- SSH ○

APT Protection Options

- Content Disarm and Reconstruction ●
  - Allow transmission when an error occurs ●
  - Original File Destination: FortiSandbox (selected) | File Quarantine | Discard
- Treat Windows executables in email attachments as viruses ●
- Send files to FortiSandbox for inspection: None | Suspicious Files Only | All Supported Files (selected)
  - Do not submit files matching types +
  - Do not submit files matching file name patterns +
- Use FortiSandbox database ●
- Include mobile malware protection ●
- Quarantine ○

Virus Outbreak Prevention

- Use FortiGuard outbreak prevention database ○
- Use external malware block list ○
- Use EMS threat feed ○

To verify the firewall policy is not blocking the connection:

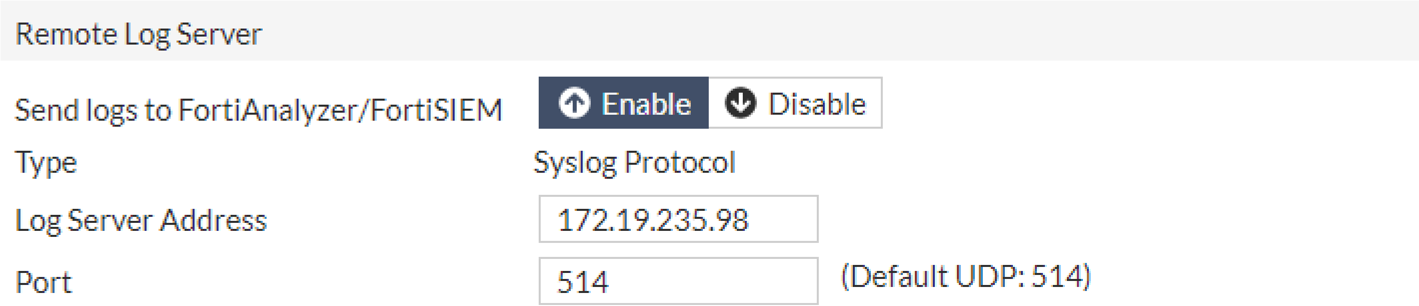
Check if firewall policy is blocking ICAP port 1344, 11344 and OFTP port 514.

Troubleshoot Log Settings

To troubleshoot the Client:

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

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



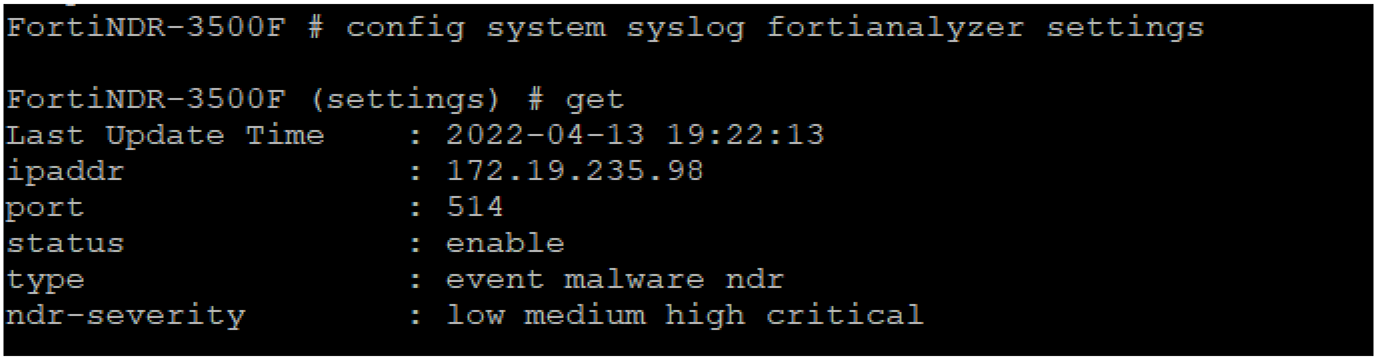
Remote Log Server

Send logs to FortiAnalyzer/FortiSIEM [✓ Enable] Disable

Type: Syslog Protocol

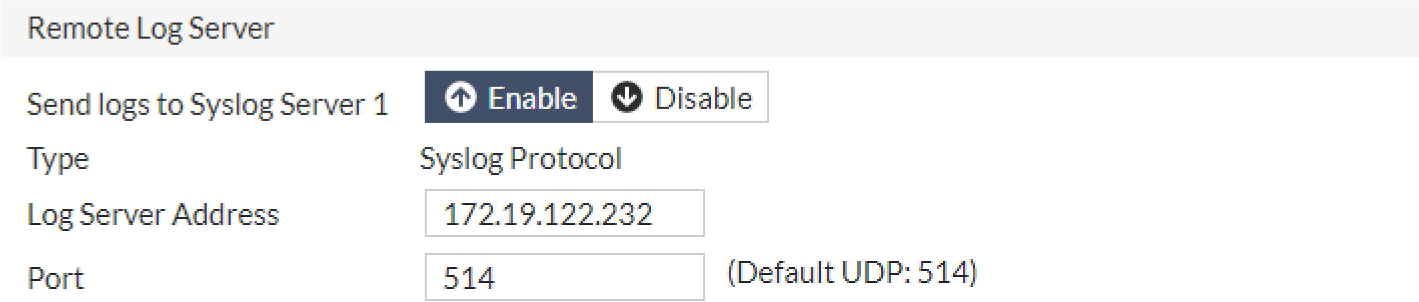
Log Server Address: 172.19.235.98

Port: 514 (Default UDP: 514)



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

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

  - Send logs to Syslog Server 1



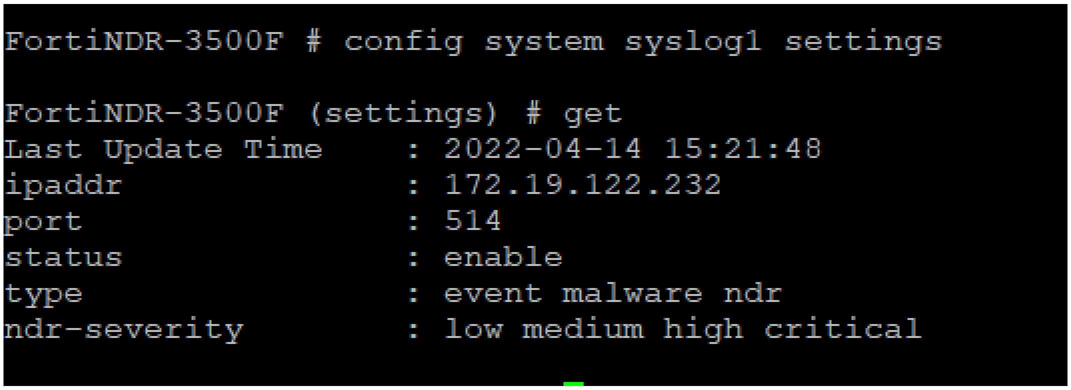
Remote Log Server

Send logs to Syslog Server 1 [✓ Enable] Disable

Type: Syslog Protocol

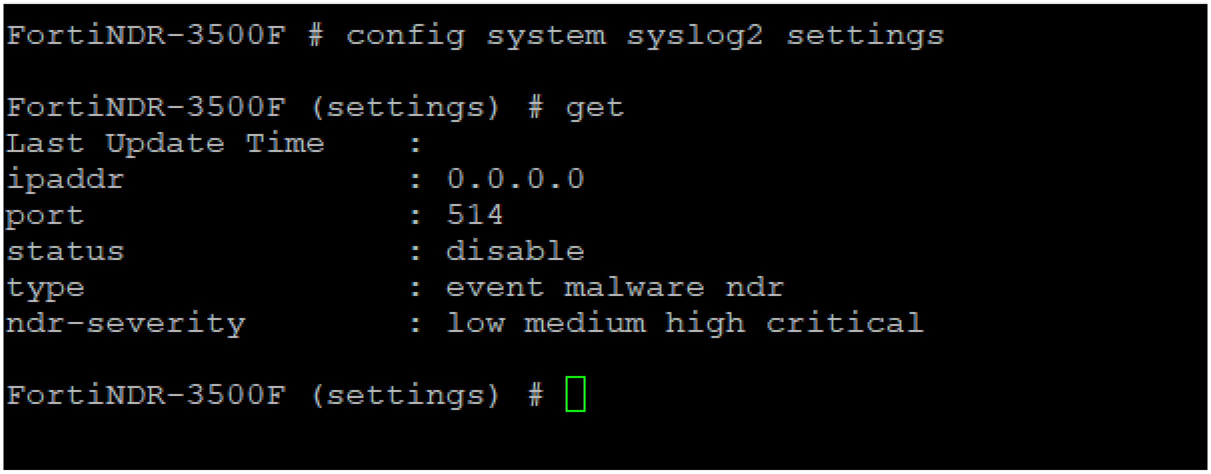
Log Server Address: 172.19.122.232

Port: 514 (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

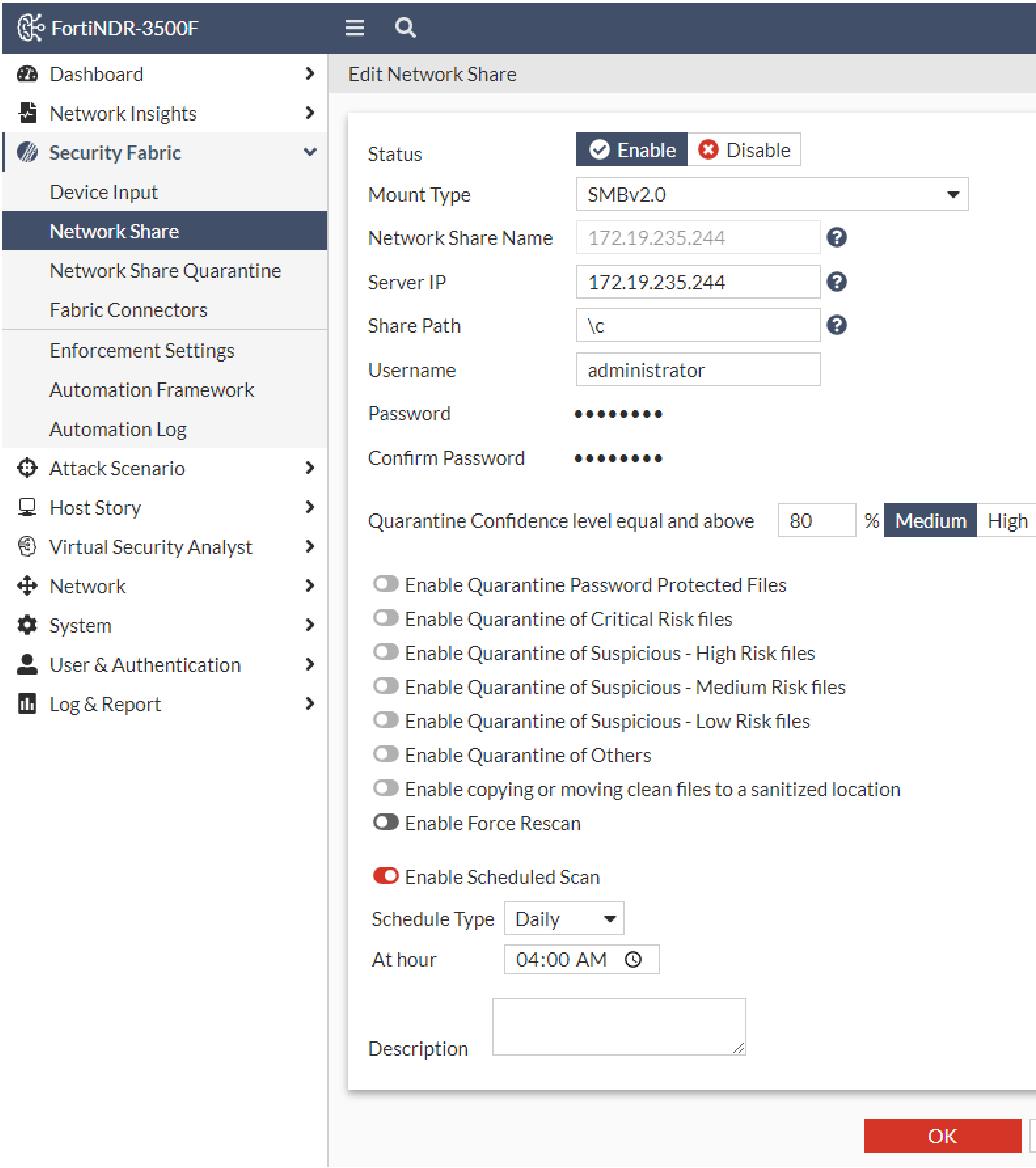
Test the Network Share Connection

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.



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: ●●●●●●●●

Confirm Password: ●●●●●●●●

Quarantine Confidence level equal and above: 80 % [✓ Medium] High

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

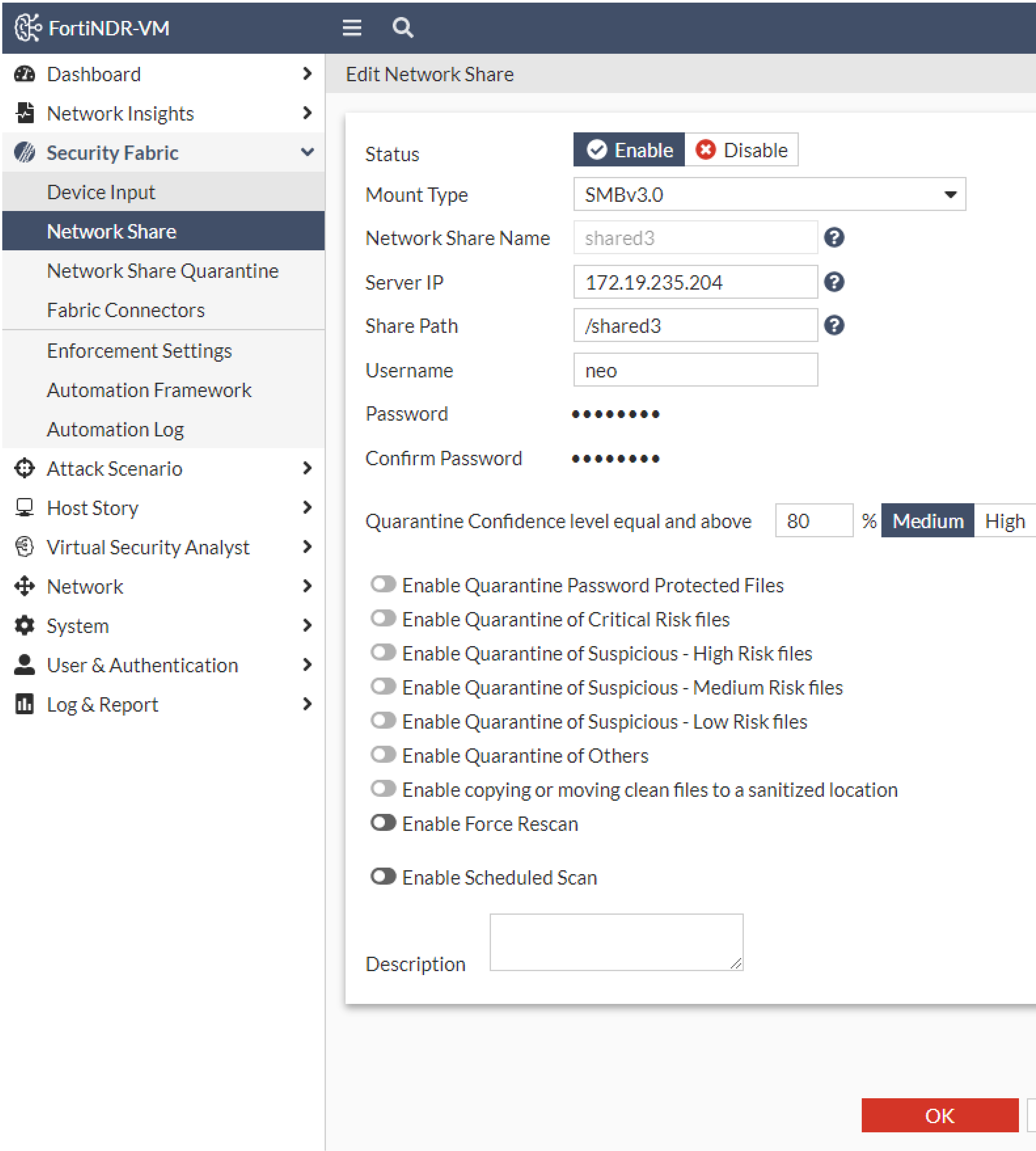
● Enable Scheduled Scan

Schedule Type: Daily

At hour: 04:00 AM

Description:

The following images shows the Network Share configuration for Linux.



Edit Network Share

Status: ● Enable ○ Disable

Mount Type: SMBv3.0

Network Share Name: shared3

Server IP: 172.19.235.204

Share Path: /shared3

Username: neo

Password: ••••••••

Confirm Password: ••••••••

Quarantine Confidence level equal and above: 80 % [✓ Medium] High

○ Enable Quarantine Password Protected Files

○ Enable Quarantine of Critical Risk files

○ Enable Quarantine of Suspicious - High Risk files

○ Enable Quarantine of Suspicious - Medium Risk files

○ Enable Quarantine of Suspicious - Low Risk files

○ Enable Quarantine of Others

○ Enable copying or moving clean files to a sanitized location

○ Enable Force Rescan

○ Enable Scheduled Scan

Description:

Diagnosing Network Share Errors

To diagnose Network Share scanning errors:

Run the following CLI commands:

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

diagnose debug enable

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

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

To troubleshoot mounting problems:

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

diagnose debug kernel display

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

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

You will see the error code if the mounting failed.

To troubleshoot a Network Share scan that it is stuck:

A scanning job may get stuck for the following issues:

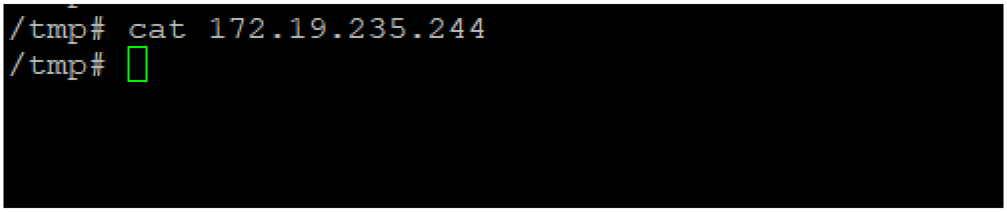
Issue	Recommendation
Mounting issue	See To troubleshoot mounting problems above.
Daemon crashed	Run the following CLI command to see if there are any `sdigestd` related crashes:

Issue	Recommendation
	`diagnose debug crashlog xxxx-xx-xx`
Data disk usage over 90%	Clean up the data disk. See, "Managing FortiNDR disk usage for Standalone and Sensor mode" on page 222.

Debug version image

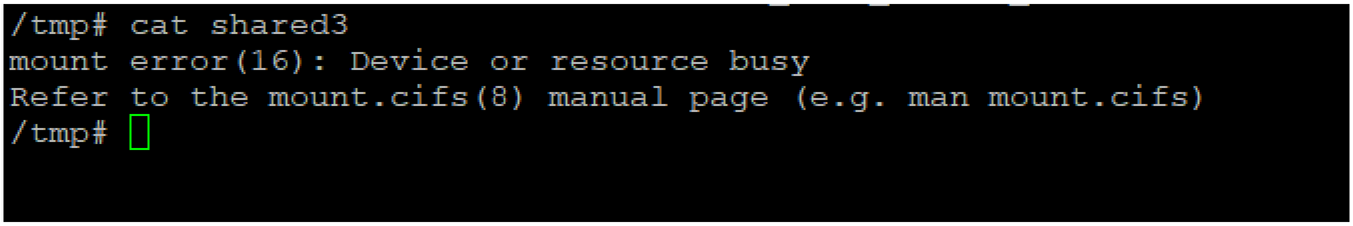
If you are using debug version image, check the `/tmp/NETWORK_SHARE_NAME` for mounting message

- 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.

To verify the FDS (FortiGuard Distribution Services) server:

1. Use the following CLI command to list the FDS servers:

   diagnose fds list

2. Perform a traceroute to the FDS server IP to ensure the network route is not blocked:

   execute traceroute <fds_ip>

3. Replace `<fds_ip>` with the actual IP address of the FDS server.

A successful routing path to the FDS server, with a policy allowing destination port 443, is crucial for the validation of the VM license.

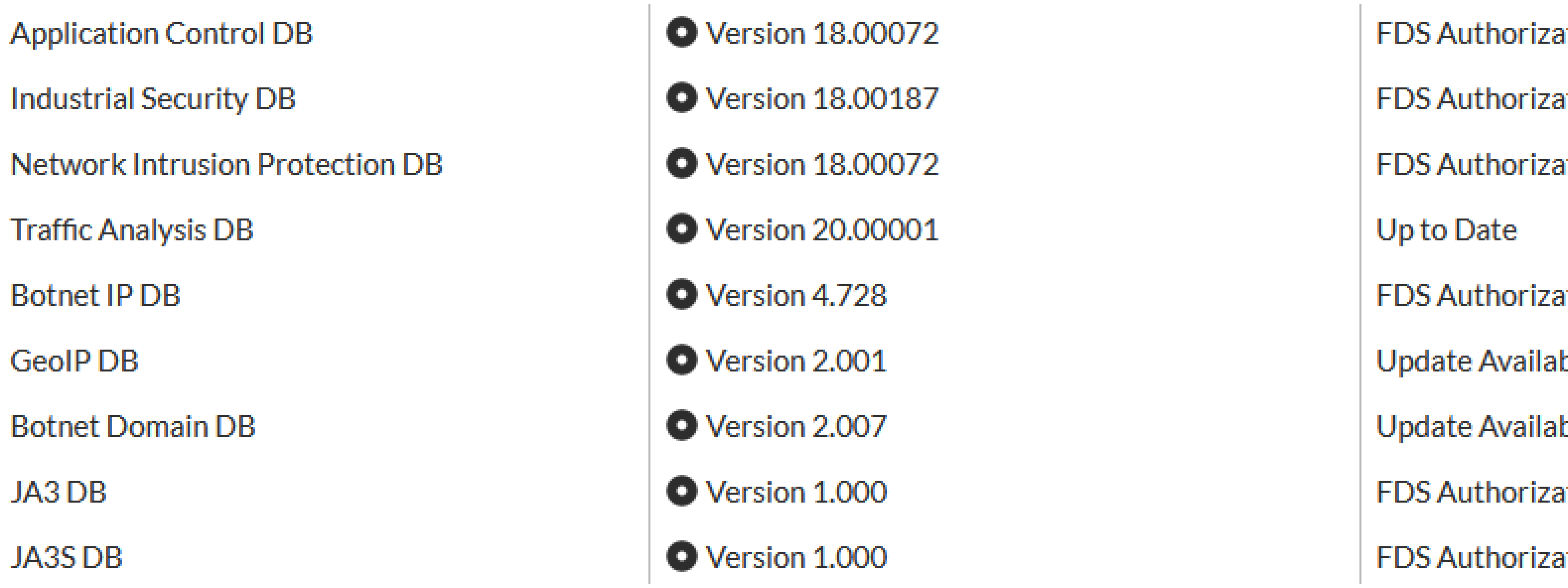
Troubleshooting the updater

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.

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.

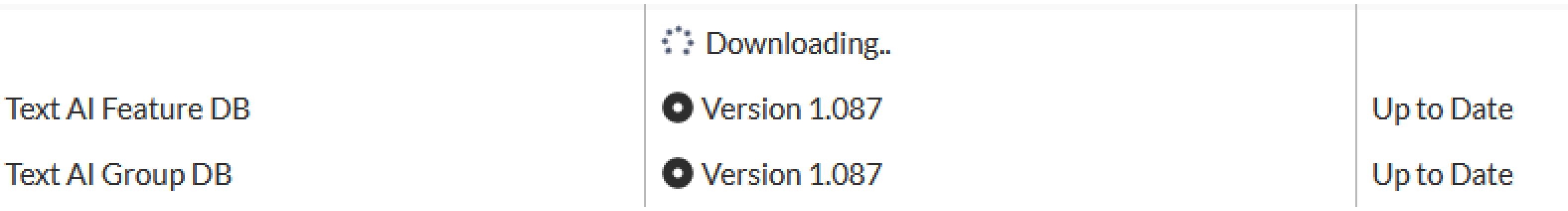


Application Control DB	Version 18.00072	FDS Authoriza
Industrial Security DB	Version 18.00187	FDS Authoriza
Network Intrusion Protection DB	Version 18.00072	FDS Authoriza
Traffic Analysis DB	Version 20.00001	Up to Date
Botnet IP DB	Version 4.728	FDS Authoriza
GeoIP DB	Version 2.001	Update Availab
Botnet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

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

Clearing updater cache files

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



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

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

Running the command and then try updating again:

```
exec update clean-up
```

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

Diagnosing Other FDS Errors

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

```
diagnose debug application updated DEBUG_LEVEL
```

```
diagnose debug enable
```

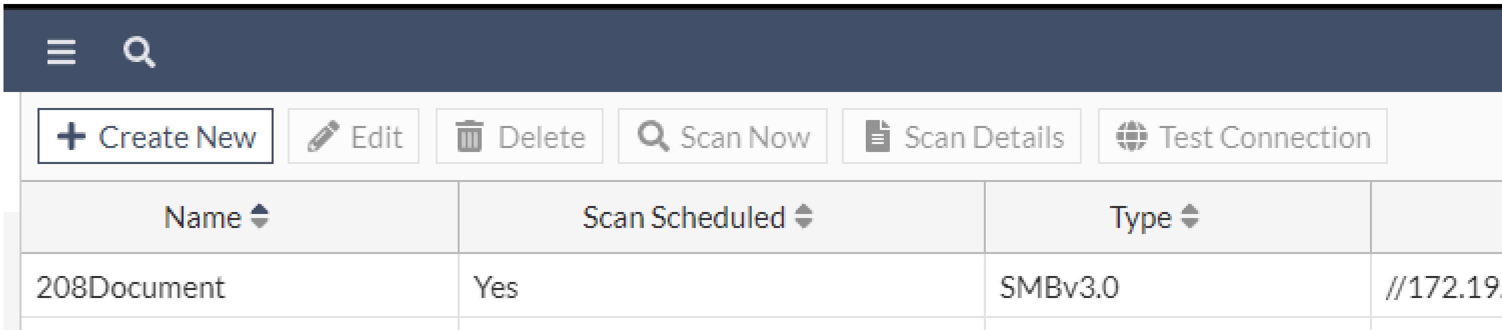
A DEBUG_LEVEL is a bit mask consisting of 3 bits.

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

Troubleshooting tips for Network File Share

To troubleshoot Network File Share issues:

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



Name	Scan Scheduled	Type	
208Document	Yes	SMBv3.0	//172.19

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

   ```
   exec ndrd off
   ```

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

4. Turn off Sniffer daemon to isolate the environment using

   ```
   exec snifferd off
   ```

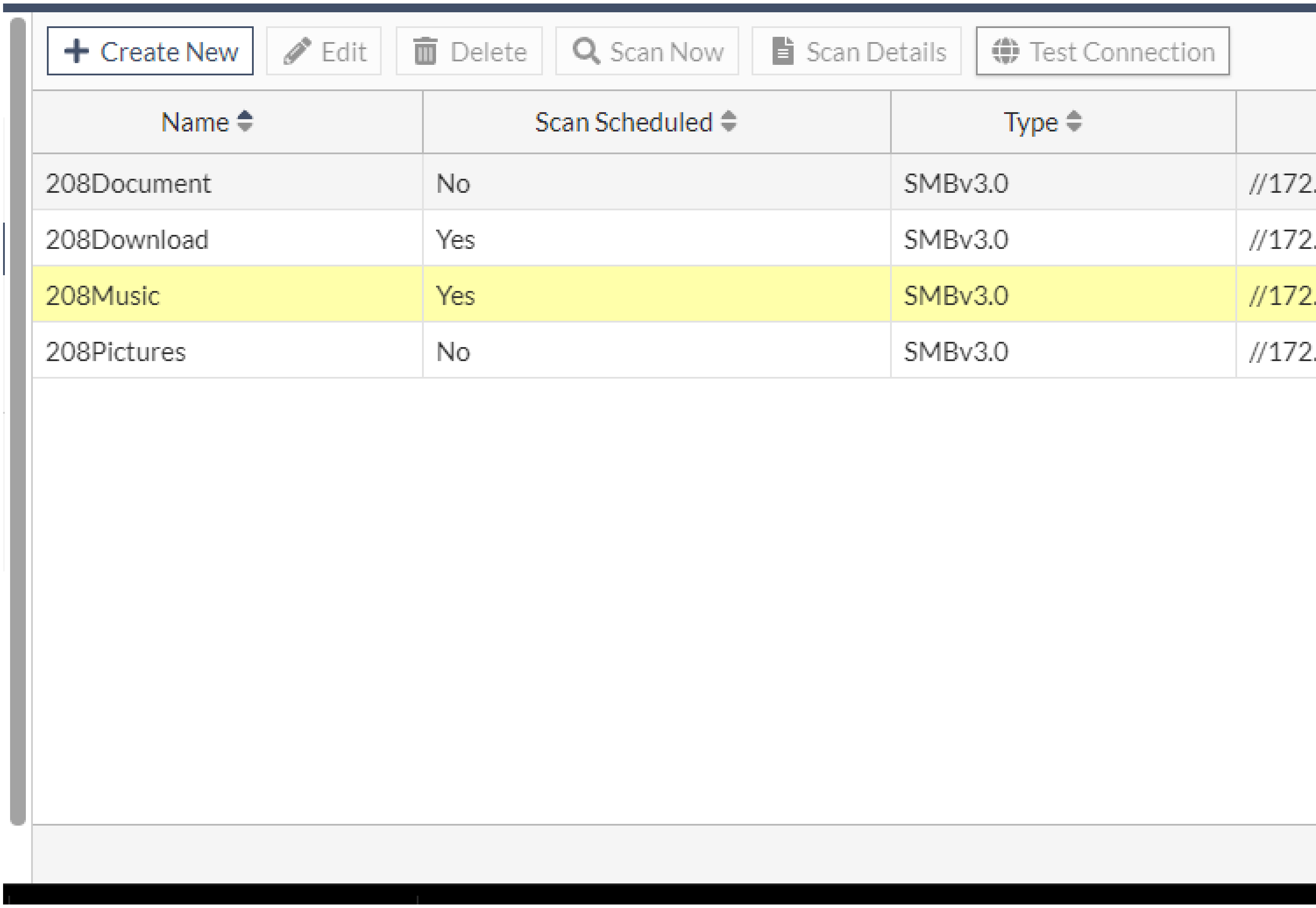
   This command is not persistent. If a reboot is required, run the command again.

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

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

6. Click *Test Connection*.

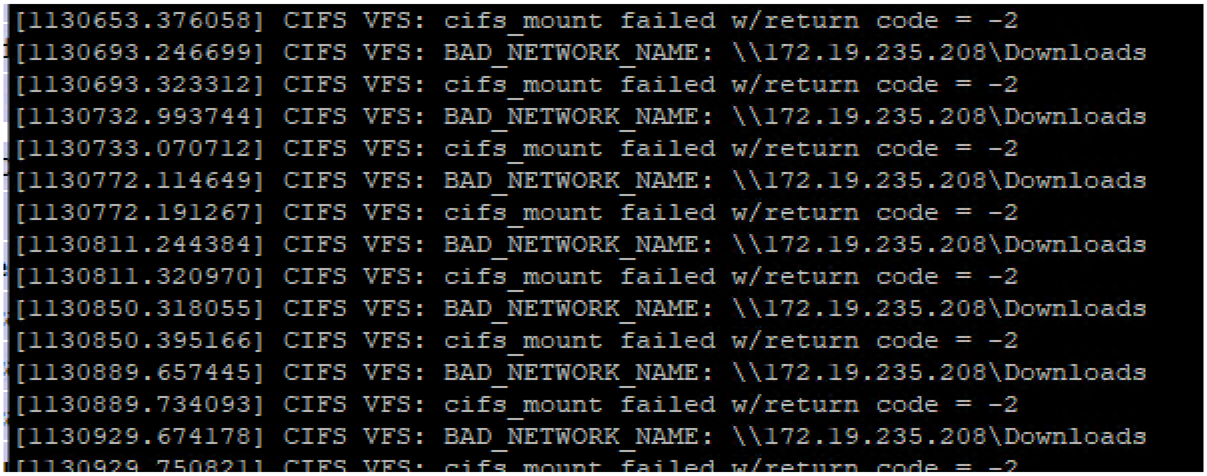
   - If *Network Share is inaccessible* is returned, it means FortiNDR cannot mount the folder. Proceed to the next step to check the detail about the mount error. Sometimes it takes time for the network share's setting to sync in the server. If you change the network share setting in the server, you may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



Name	Scan Scheduled	Type	
208Document	No	SMBv3.0	//172.
208Download	Yes	SMBv3.0	//172.
208Music	Yes	SMBv3.0	//172.
208Pictures	No	SMBv3.0	//172.

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

    1. a. `exec deb kernel display`

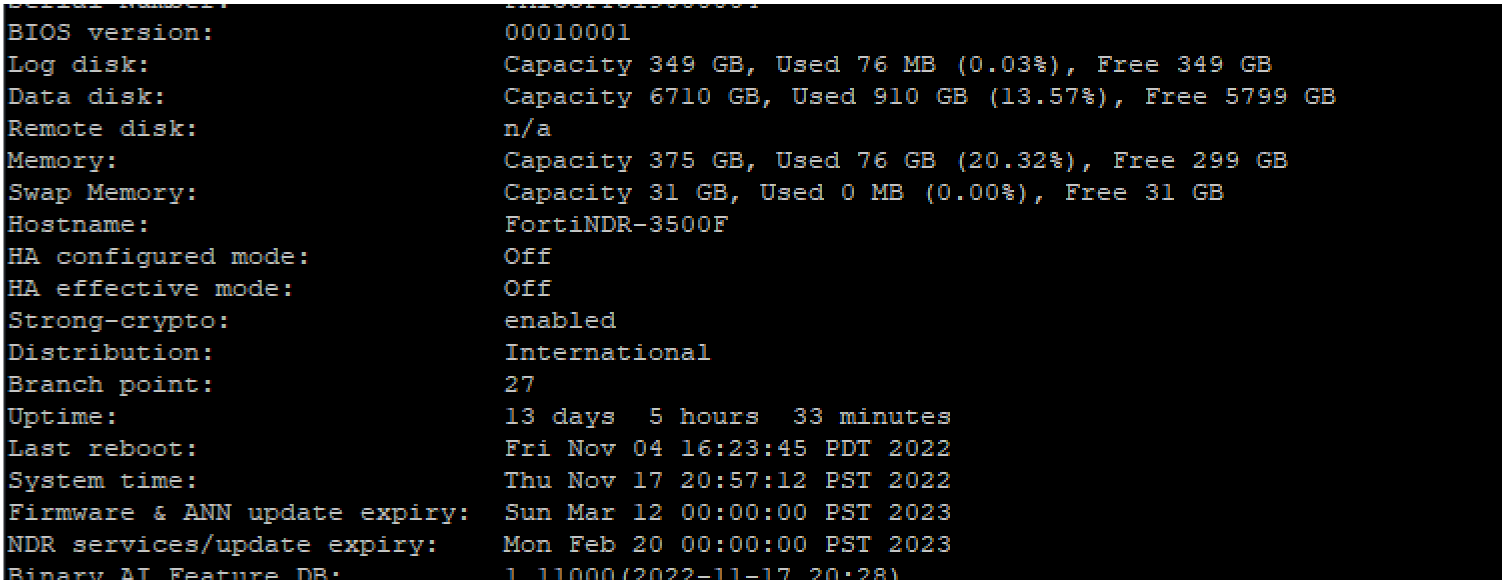
       ```
       [1130653.376058] CIFS VFS: cifs_mount failed w/return code = -2
       [1130693.246699] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
       [1130693.323312] CIFS VFS: cifs_mount failed w/return code = -2
       [1130732.993744] CIFS VFS: BAD_NETWORK_NAME: \\172.19.235.208\Downloads
       [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.

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

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

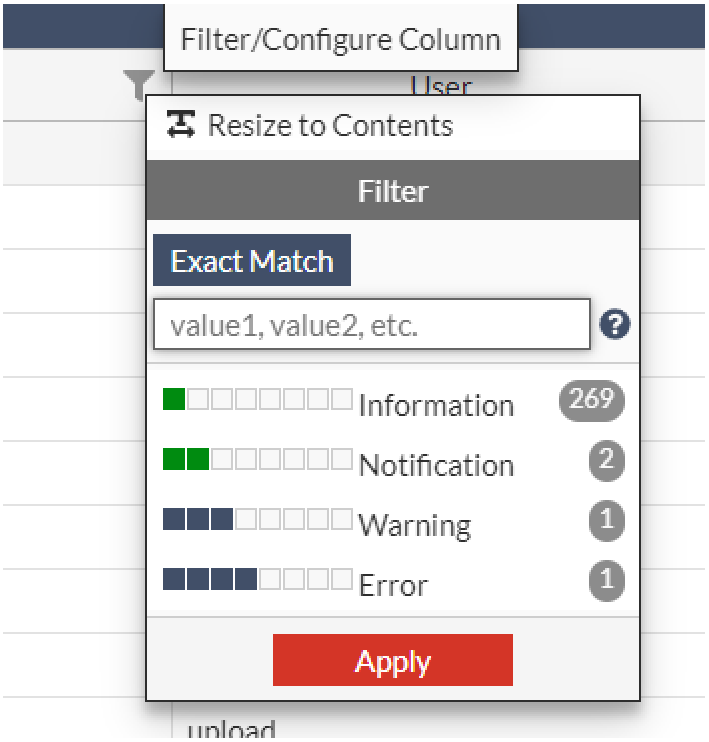
    get system status

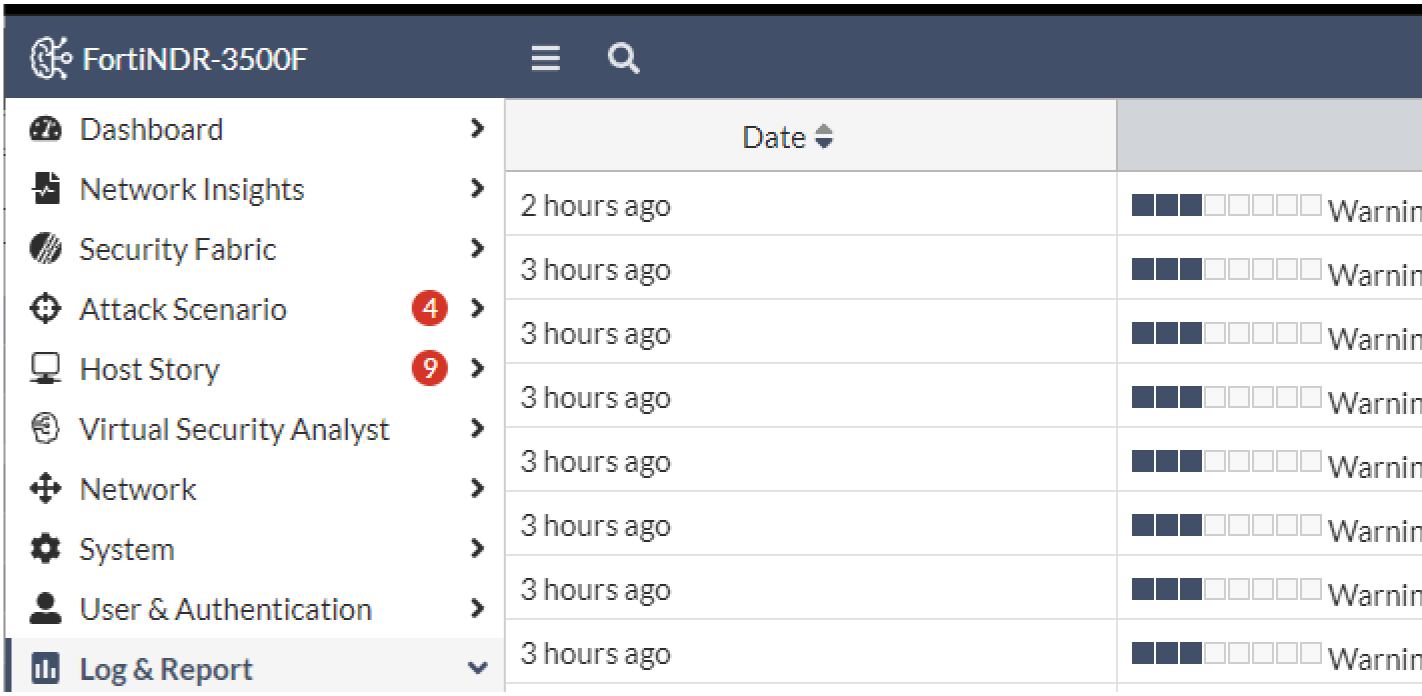
    ```
    BIOS version:                  00010001
    Log disk:                      Capacity 349 GB, Used 76 MB (0.03%), Free 349 GB
    Data disk:                     Capacity 6710 GB, Used 910 GB (13.57%), Free 5799 GB
    Remote disk:                   n/a
    Memory:                        Capacity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

9. For network share scan errors, go to *Log & Report > Events*.
    1. Select *Level: Warning, Error and User: sdigestd*
    2. Take a screen shot. The *Events* page contains 1 day history.

3. 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:



Date	
2 hours ago	Warnin
3 hours ago	Warnin
3 hours ago	Warnin
3 hours ago	Warnin
3 hours ago	Warnin
3 hours ago	Warnin
3 hours ago	Warnin
3 hours ago	Warnin

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

    diagnose debug crashlog xxxx-xx-xx

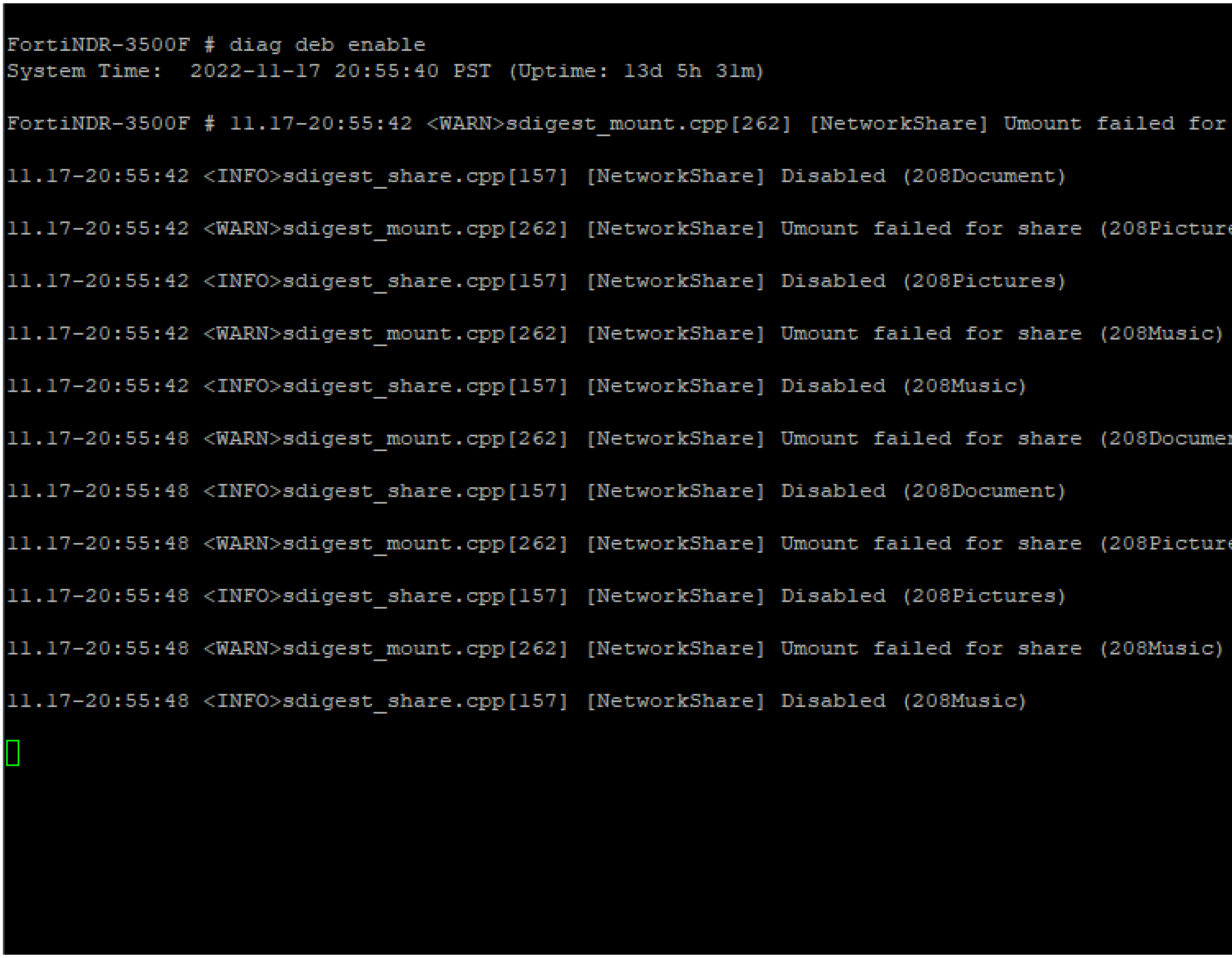
    `sdigestd`is the daemon responsible for network share mount and copying. 7 means all level logs, if there are too many logs, use 2 <WARN> or 1.

    For more information, see "Troubleshoot Network Share" on page 230.

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

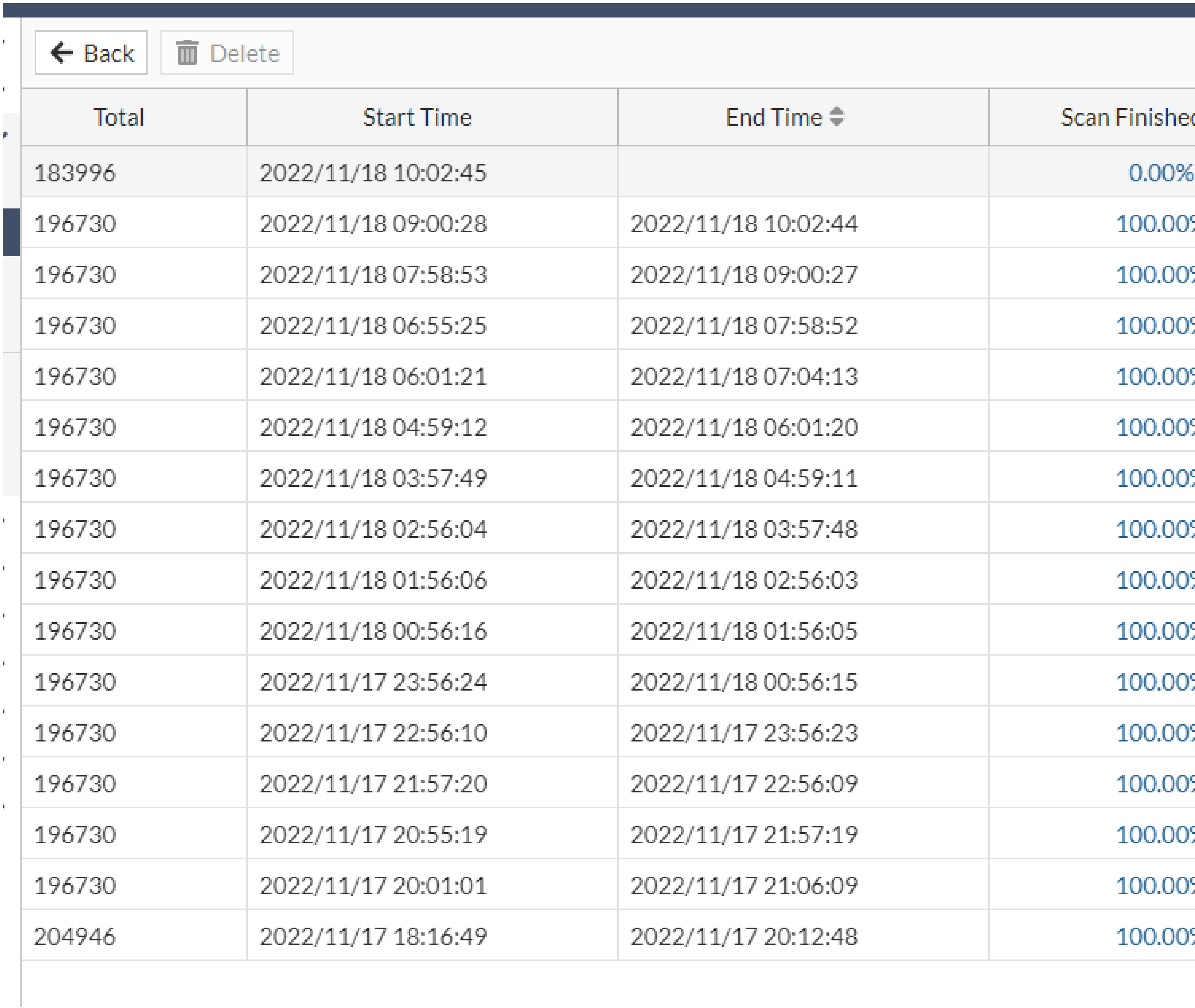
    - `diag deb app sdigestd 7`
    - `diag deb enable`

    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

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 (208Picture

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 (208Documen

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 (208Picture

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:



Total	Start Time	End Time	Scan Finished
183996	2022/11/18 10:02:45		0.00%
196730	2022/11/18 09:00:28	2022/11/18 10:02:44	100.00%
196730	2022/11/18 07:58:53	2022/11/18 09:00:27	100.00%
196730	2022/11/18 06:55:25	2022/11/18 07:58:52	100.00%
196730	2022/11/18 06:01:21	2022/11/18 07:04:13	100.00%
196730	2022/11/18 04:59:12	2022/11/18 06:01:20	100.00%
196730	2022/11/18 03:57:49	2022/11/18 04:59:11	100.00%
196730	2022/11/18 02:56:04	2022/11/18 03:57:48	100.00%
196730	2022/11/18 01:56:06	2022/11/18 02:56:03	100.00%
196730	2022/11/18 00:56:16	2022/11/18 01:56:05	100.00%
196730	2022/11/17 23:56:24	2022/11/18 00:56:15	100.00%
196730	2022/11/17 22:56:10	2022/11/17 23:56:23	100.00%
196730	2022/11/17 21:57:20	2022/11/17 22:56:09	100.00%
196730	2022/11/17 20:55:19	2022/11/17 21:57:19	100.00%
196730	2022/11/17 20:01:01	2022/11/17 21:06:09	100.00%
204946	2022/11/17 18:16:49	2022/11/17 20:12:48	100.00%

Sensor logs not displaying in Center GUI

To troubleshoot sensor logs not displaying in the GUI:

1. Check if the sensors are included in the widget settings.
2. In the FortiNDR *Overview* dashboard, click *Reset to Default*.
3. Log out and then log back into the GUI.

4. Clear the browser cache.
5. As a last resort, use the CLI command: `execute factoryreset disk`

Troubleshooting FortiNDR VM high CPU usage

Ensure you reserve a minimum of 60GHz CPU capacity for the VM if it is a cpu32 VM. For cpu16 VM, reserve at least 30GHz.

For Center mode VM, please reserve a minimum of 90GHz CPU capacity, 48vcpu and 384GB of memory.

Visit the host Summary page in the vSphere Client to check for Host CPU usage. If you see a warning, consider relocating other CPU-intensive virtual machines away from the same host of the FortiNDR VM. After doing so, reboot the FortiNDR VM.

Troubleshooting inactive Netflow status

The *Netflow Status* widget displays *Inactive* when no flows are seen in the last five minutes.

To diagnose an inactive Netflow status:

1. Enure FortiNDR's port UDP 2055, 6343, and 9995 are open. To monitor the packets, run the following CLI command:

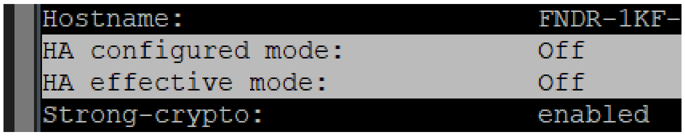
   diagnose sniffer packet

   For example: `diagnose sniffer packet port1 'port 9995'`

2. Verify that HA mode is *off*. Netflow does not support HA: secondary mode.

   Run the following CLI command:

   get system status

   ```
   Hostname:                    FNDR-1KF-
   HA configured mode:          Off
   HA effective mode:           Off
   Strong-crypto:               enabled
   ```

3. Check the logs to see if there are any crashes related to the flow daemon. The following CLI commands can retrieve logs:

   diagnose debug crashlog <crash_log_date>

   diagnose sys top

   diagnose deb database error

4. Try reloading the daemon with the CLI:

   execute reload [<daemon_name>]

If you use the command `execute netflow on`:

1. Be aware that it takes time for the daemon to activate after running `execute reload` and the daemon does not immediately indicate that it is on. We recommend waiting a few seconds before checking its status.

Appendix A: API guide

This section explains how to use the FortiNDR API.

FortiNDR REST API currently supports the following:

- Files submission for scanning
- Retrieve files verdict result
- Get file STIX2 report
- Starting network share scan
- Events API support (detections based on source IP/Mac/hostname and anomaly type)

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.

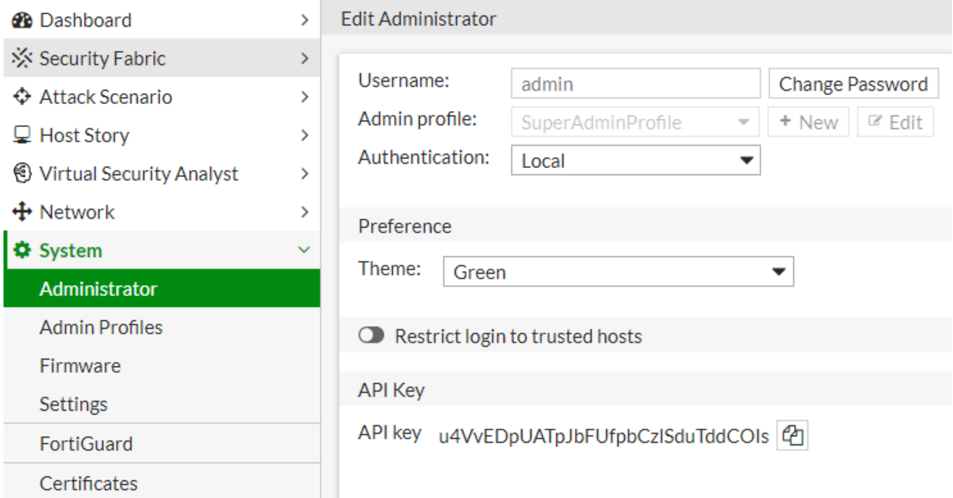
To use API to upload files, generate a token. The token is only displayed once. If you lose the token, generate a new one.

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*.



Username: admin

Admin profile: SuperAdminProfile

Authentication: Local

Theme: Green

Restrict login to trusted hosts

API key u4VvEDpUATpJbFUfpbCzlSduTddCOIs

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 20.

Submit a file using one of the following methods.

Method	Description
JSON data	The JSON data must be encoded in base64 format.

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

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

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

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

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

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

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

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

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

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

Upload file by JSON data

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

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

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

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

```
requests.post(url='/api/v1/files',

params={'access_token': 'u4VvEDpUATpJbFUfpbCzlSduTddCOIs'},

data={ 'file_name': b64encode('samples.zip'),

' file_content': b64encode(open('samples.zip', 'rb').read()),

' password': 'xxxxxxxx'})
```

Upload file by multi-part file

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

```
requests.post(url='/api/v1/files',

params={'access_token': 'u4VvEDpUATpJbFUfpbCzlSduTddCOIs'},

files={'samples.zip':open('samples.zip', 'rb')})
```

Retrieve file verdict results

/api/v1/verdict

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

The query string can only have one search query parameter.

Examples

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

```
{
  "results": {
    "fileids": [
      7,8,9,10,11,12,13,14,15

    ],
    "total_fileids": 9
  }
}
```

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

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

```
{
  "results": {
    "file_id": 5742600,
    "virus_name": "W32/Miner.VI!tr",
    "md5": "bbd72472f8d729f4c262d6fe2d9f2c8c",
    "sha512": "cce8e67772f19b-
cfe5861e4c1b8eec87016b-
b7cf298735d-
b633490243b-
c0391a017c7d6b805f225775405598614be48c5479cb7f1c54d957e6129effbf9cca37",
    "file_size": 1141544,
    "source": "http://172.16.77.46/api/sample_download/1106042791/",
    "severity": "High",
    "category": "Trojan",
    "family":"Emotet",
    "feature_composition": [
      {
        "feature_type": "Trojan",
        "appearance_in_sample": 986
      },
      {
        "feature_type": "Application",
        "appearance_in_sample": 95
      }
    ],
    "create_date": "2020-07-31",
    "confidence": "High",
    "file_type": "PE",
    "victim_ip": "172.19.235.225",
    "attacker_ip": "172.16.77.46",
    "victim_port": 35400,
    "attacker_port": 80,
    "engine_version": 1.013,
    "kdb_version": 1.037,
    "tmfc": 0,
    "pbit": 3
  }
}
```

Field	Description
`file_id`	ID of the file.
`virus_name`	FortiNDR virus name.
`source`	For file uploaded by API or GUI, `source` is *manual upload*, otherwise it is an URL.
`severity`	*No Risk*, *Low*, *Medium*, *High*, or *Critical*.
`category`	For clean file: *Clean*. For malicious file, one of the following: *Generic Attack*, *Downloader*, *Redirector*, *Dropper*, *Ransomware*, *Worm*, *PWS*, *Rootkit*, *Banking Trojan*, *Infostealer*, *Exploit*, *Virus*, *Application*, *Multi*, *CoinMiner*, *DoS*, *BackDoor*, *WebShell*, *SEP*, *Proxy*, *Trojan*, *Phishing*, *Fileless*, *Wiper*, or *Industroyer*.
`family`	FortiNDR virus family name.
`Feature_composition`	JSON objects containing feature composition data for malicious file. `feature_type` is the category which the detected feature belongs to. `appearance_in_sample` is the number of appearances that the feature FortiNDR has detected.
`confidence`	For clean file: *N/A*. For other file: *Low*, *Medium*, or *High*.

Field	Description
file_type	*PE*, *PDF*, *MSOFFICE*, *HTML*, *ELF*, *VBS*, *VBA*, *JS*.
tmfc	Reserved.
pbit	Debug only.
parent_fname	The archive file name if the current file was extracted from an archive/zip file.

Example of problems retrieving results

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

Field	Description
http_code	See "HTTP status table" on page 256.
message	Messages include: DATA_NOT_EXIST when result data cannot be found given the search query parameter. DATA_IN_PROCESS when result data is still under process, such as after one submission, the accepted files have not been assigned file IDs. This might happen when uploading a big archive or compressed file. INVALID_PARAM_NUMBER when zero or more than one search query parameters exist. INVALID_PARAM when search query value is not valid.

Submitted file errors explanation:

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

- Oversized file
- Oversized archive contents

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

In the other following cases:

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

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

```
{

"results": {

    "fileids": [xx],

    "total_fileids": x

}

}
```

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

In the following two cases:

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

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

Get file stix2 report

/api/v1/report

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

The query string can only have one search query parameter.

Examples

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

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

HTTP status table

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

Start Network Share scan

/api/v1/nfs/scan

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

Examples

```
POST /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"
}
```

Events API support

/api/v1/events

Query parameters	Description
ip	Get anomaly events with device IPv4 or IPv6 address. User needs specify one of [ip, hostname, mac] in the request.
hostname	Get anomaly events with device hostname. User needs specify one of [ip, hostname, mac] in the request.
mac	Get anomaly events with device mac address. User needs specify one of [ip, hostname, mac] in the request.
type	Specify the anomaly type events, one of [botnet, entrypted-attack, network-attack, fortiguard-ioc, week-communication, ml-discovery, malware].
start_time	The start time of events, specified as a Unix timestamp in seconds.
end_time	The end time of events, specified as a Unix timestamp in seconds.
start	The starting point or offset from which the paginated events are returned. Default 0.
size	The number of events to be returned per page. Default 500.

Examples

```
GET /api/v1/events?ip= 192.168.1.114 &type=network-attack&start_time-
e=1695020154&end_time=1698111999 &start=0&size=2
{
   "results":[
      {
         "event_time":"2023-10-23 16:15:53",
         "source_ip":"192.168.1.114",
         "source_port":38123,
         "destination_ip":"192.168.1.110",
         "destination_port":17185,
         "severity":"Low",
         "attack_name":"Nmap.Script.Scanner"
      },
      {
         "event_time":"2023-10-23 16:15:53",
         "source_ip":"192.168.1.114",
         "source_port":38124,
         "destination_ip":"192.168.1.110",
         "destination_port":17185,
         "severity":"Low",
         "attack_name":"Nmap.Script.Scanner"
      }
   ]
}
```

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.SSLE
                                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 FortiNDR 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 fndr.fortinet.com
CLI	TCP 22	Inbound SSH
Data synchronization	TCP 20003	Inbound and outbound between FortiNDR units in an HA group.
DB synchronization	TCP 9440	Inbound and outbound between FortiNDR units in an HA group.
File synchronization	TCP 20002	Inbound and outbound between FortiNDR units in an HA group.
FortiGate quarantine	TCP 443	Outbound to FortiGate
FortiGuard update	TCP 443	Initial outbound to: • fai.fortinet.net • fds1.fortinet.com • update.fortiguard.net For a complete list of the current Fortiguard update servers, please use the CLI `diagnose fds list`. Please be aware this list of IPs can and will change over time without notice.
GUI	TCP 443	Inbound web browser
ICAP	TCP 1344, 11344	Inbound
IOC lookup	TCP 443	Outbound to productapi.fortinet.com
IOT lookup	TCP 443	Outbound to globalguardservice.fortinet.net

Item	Protocol and port number	Direction
Microsoft Active Directory	TCP 636,389	Inbound and outbound
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
Sensor Center command communication	UDP 5566|	Sensor to Center
Sensor Center data synchronization	TCP 9094 9096	Sensor to Center
SYSLOG	UDP 514	SYSLOG outbound
Web Filter query	UDP 53	Outbound to service.fortiguard.net

Appendix D: FortiGuard updates

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

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

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

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

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

Other detection techniques:

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

Detection Techniques	Supports offline manual update	Comments
Malware via ANN	Yes	Can be updated manually via GUI or with an offline package via CLI.
AV engine	Yes	Shipped by default. Can be updated with internet via GUI or with an offline package via CLI.
Botnet detection	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.
Network Attacks / Application control	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.

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

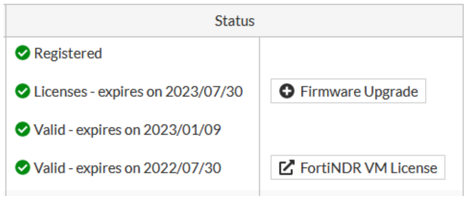
Updating the ANN database from FDS for malware detection (GUI)

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

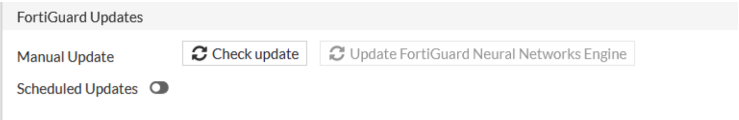
   ✓ Licenses - expires on 2023/07/30

   ✓ Valid - expires on 2023/01/09

   ✓ Valid - expires on 2022/07/30

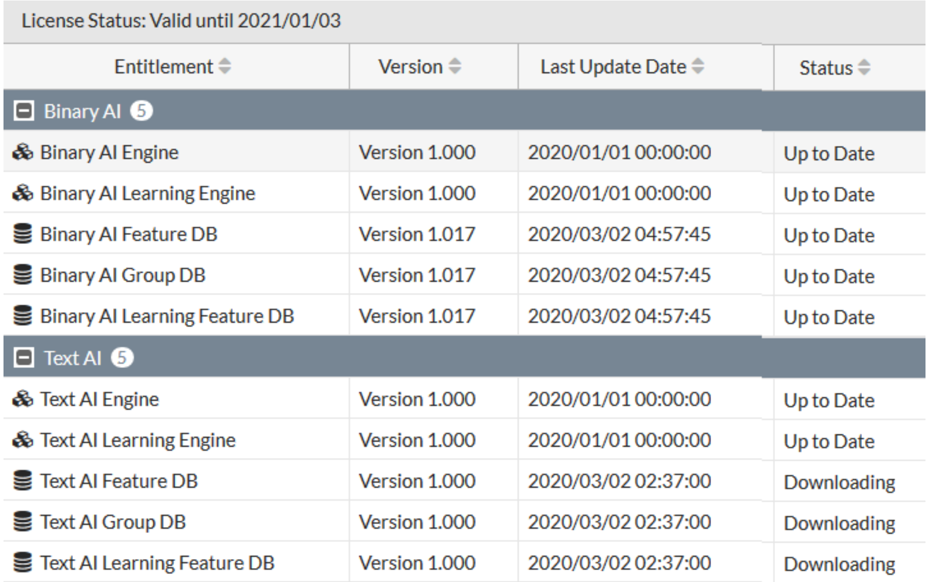
3. Click *Check Update*.

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

4. Click *Update Now*.

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



License Status: Valid until 2021/01/03

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

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 267 for details. The section below discusses one of the updates: ANN for malware detection.

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

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

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

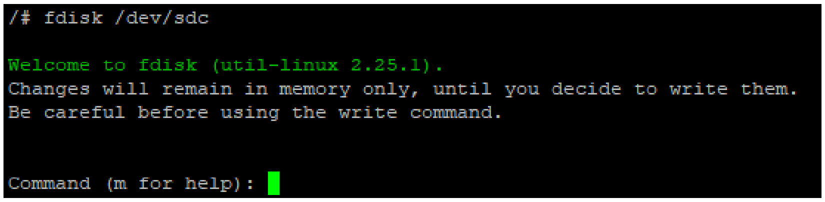
To update the ANN database using CLI:

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

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

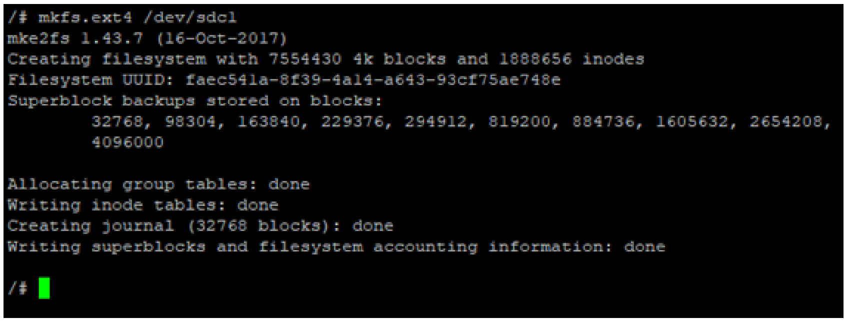
1. Format a USB drive in another Linux machine using the command `fdisk /dev/sdc`.

   Ensure the USB drive has enough capacity and create one partition using EXT4 or EXT3 format.

   ```
   /# fdisk /dev/sdc

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


   Command (m for help):
   ```

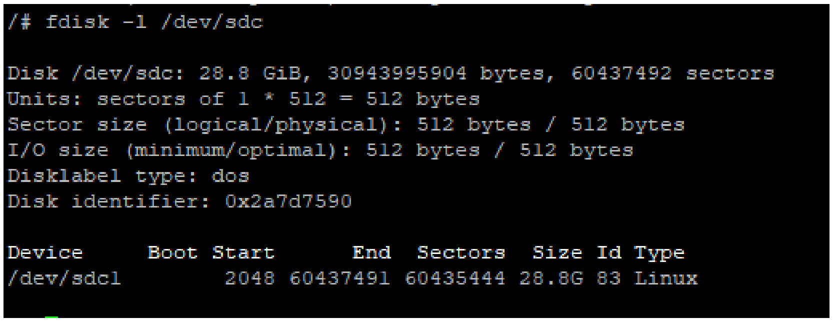
2. Format `sdc1` using the `mkfs.ext4 /dev/sdc1` command.

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

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

   /#
   ```

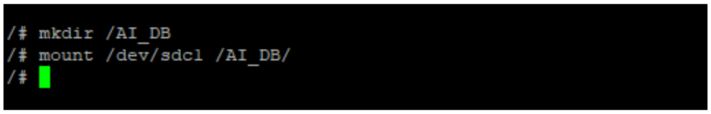
   FortiTester is a great companion for FortiNDR as FortiTester can send a malware strike pack over different protocols such as HTTP, SMB, SMTP, to simulate malware in the network. You can use FortiTester to generate malware and test FortiNDR for detection.

   The following is an example of the result.

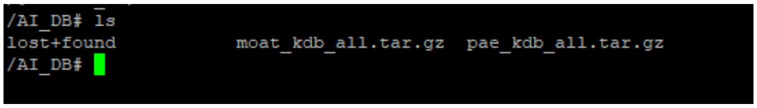
   ```
   /# fdisk -l /dev/sdc

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

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

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



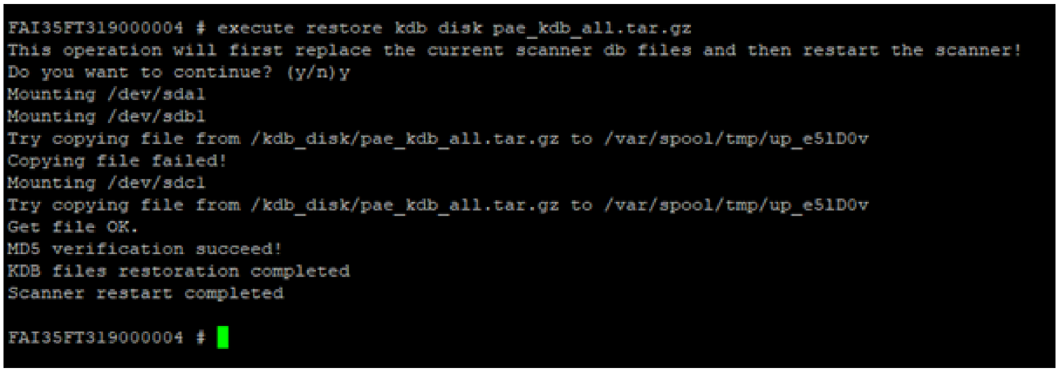
```
/# mkdir /AI_DB
/# mount /dev/sdc1 /AI_DB/
/#
```

The following is an example of the result.

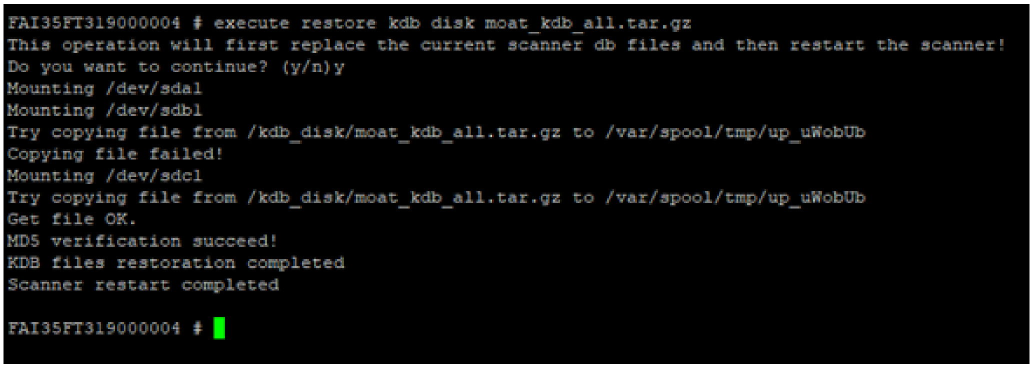


```
/AI_DB# ls
lost+found           moat_kdb_all.tar.gz  pae_kdb_all.tar.gz
/AI_DB#
```

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

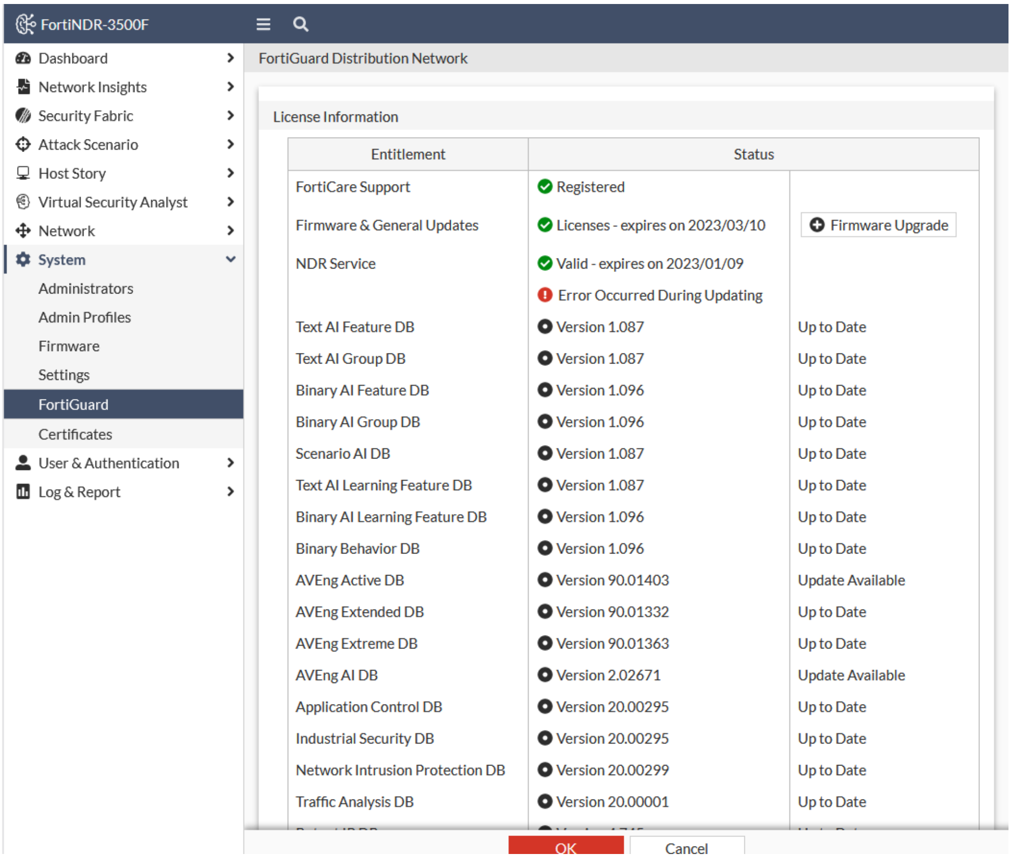


```
FAI35FT319000004 # execute restore kdb disk pae_kdb_all.tar.gz
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Mounting /dev/sda1
Mounting /dev/sdb1
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e51D0v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

FAI35FT319000004 #
```



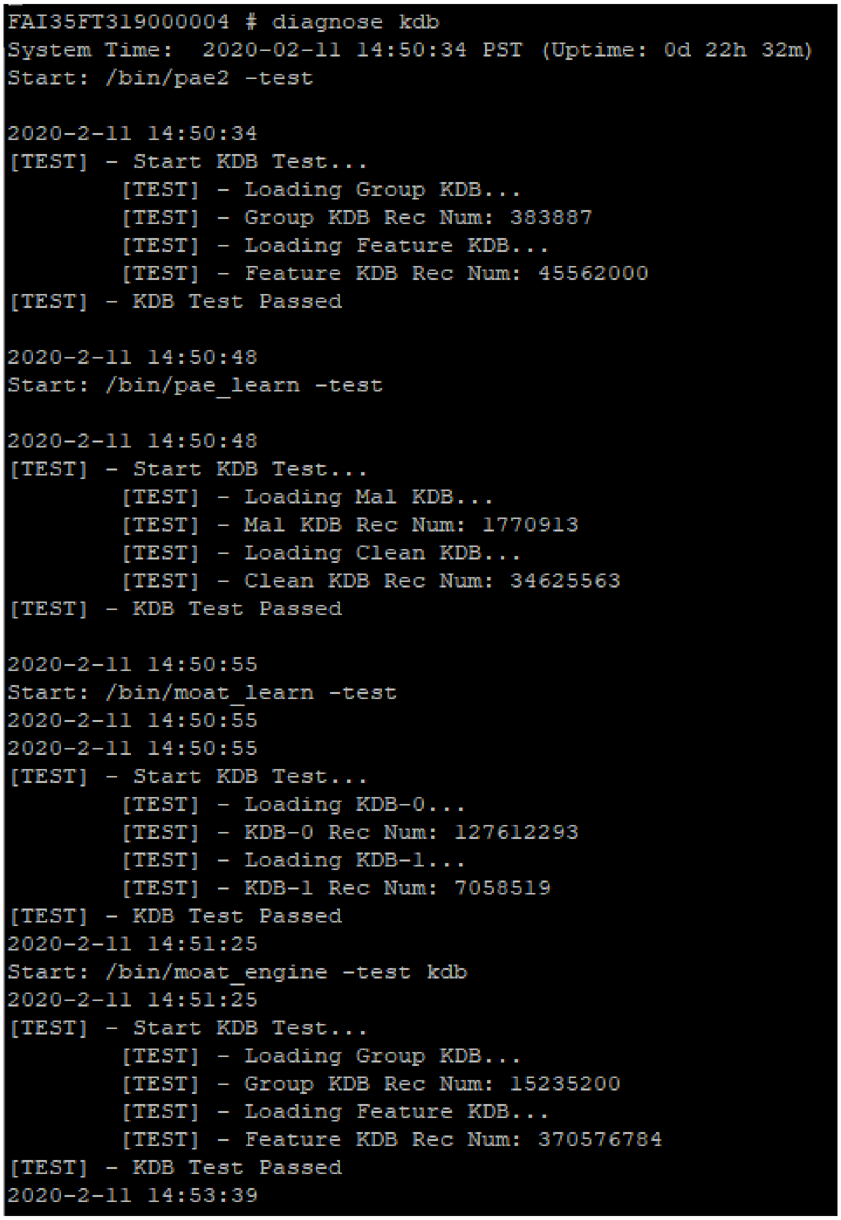
```
FAI35FT319000004 # execute restore kdb disk moat_kdb_all.tar.gz
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Mounting /dev/sda1
Mounting /dev/sdb1
Try copying file from /kdb_disk/moat_kdb_all.tar.gz to /var/spool/tmp/up_uWobUb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

FAI35FT319000004 #
```

5. To verify the ANN database in the GUI, go to *System* > *FortiGuard*. 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	Firmware Upgrade
NDR Service	✓ Valid - expires on 2023/01/09 ! Error Occurred During Updating	
Text AI Feature DB	● Version 1.087	Up to Date
Text AI Group DB	● Version 1.087	Up to Date
Binary AI Feature DB	● Version 1.096	Up to Date
Binary AI Group DB	● Version 1.096	Up to Date
Scenario AI DB	● Version 1.087	Up to Date
Text AI Learning Feature DB	● Version 1.087	Up to Date
Binary AI Learning Feature DB	● Version 1.096	Up to Date
Binary Behavior DB	● Version 1.096	Up to Date
AVEng Active DB	● Version 90.01403	Update Available
AVEng Extended DB	● Version 90.01332	Up to Date
AVEng Extreme DB	● Version 90.01363	Up to Date
AVEng AI DB	● Version 2.02671	Update Available
Application Control DB	● Version 20.00295	Up to Date
Industrial Security DB	● Version 20.00295	Up to Date
Network Intrusion Protection DB	● Version 20.00299	Up to Date
Traffic Analysis DB	● Version 20.00001	Up to Date

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

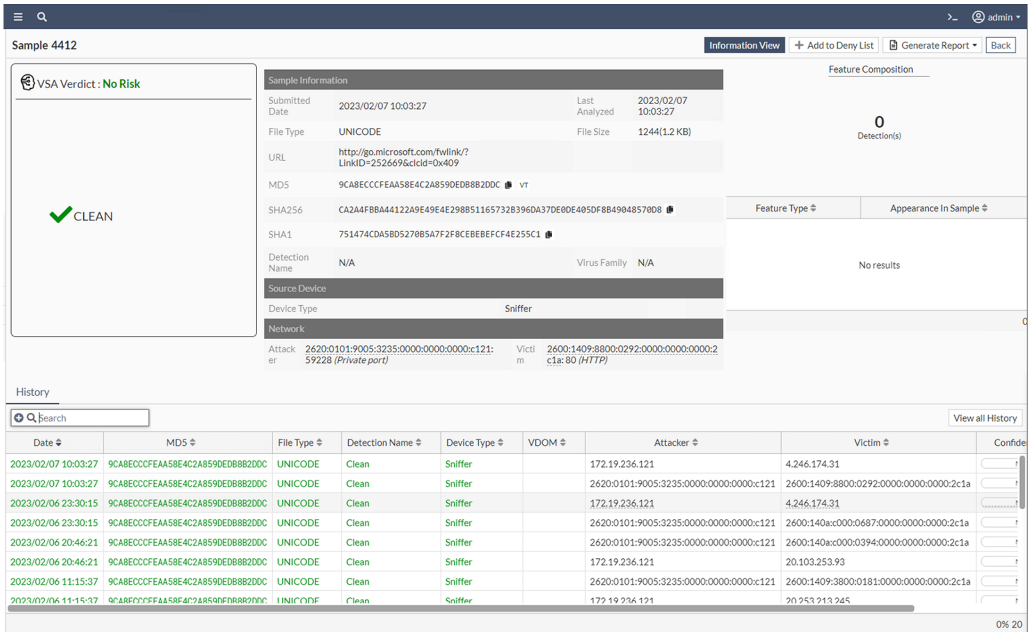
Event Category	NDR Detection Severity Level
Malware Detection	Low|Medium|High|Critical
Botnet Detection/Netflow Botnet Detection	Critical
Encryption Attack Detection	Critical
Network Attack Detection	Low|Medium|High|Critical
Indication of Compromise Detection	Critical
Weak Cipher and Vulnerable Protocol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



Sample 4412

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=252669&clcid=0x409		
MD5	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC VT		
SHA256	CA2A4FBBA44122A9E49E4E298B51165732B396DA37DE0DE405DF8B49048570D8		
SHA1	751474CDA5BD5270B5A7F2F8CEBEBEFCF4E255C1		
Detection Name	N/A	Virus Family	N/A

Source Device

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)*

0
Detection(s)

Feature Type	Appearance In Sample
No results	

History

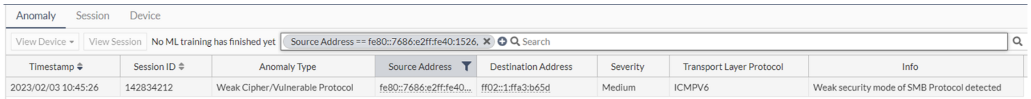
Search

View all History

Date	MD5	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confide
2023/02/07 10:03:27	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	UNICODE	Clean	Sniffer		172.19.236.121	4.246.174.31	
2023/02/07 10:03:27	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	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	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	UNICODE	Clean	Sniffer		172.19.236.121	4.246.174.31	
2023/02/06 23:30:15	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	UNICODE	Clean	Sniffer		2620:0101:9005:3235:0000:0000:0000:c121	2600:140a:c000:0687:0000:0000:0000:2c1a	
2023/02/06 20:46:21	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	UNICODE	Clean	Sniffer		2620:0101:9005:3235:0000:0000:0000:c121	2600:140a:c000:0394:0000:0000:0000:2c1a	
2023/02/06 20:46:21	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	UNICODE	Clean	Sniffer		172.19.236.121	20.103.253.93	
2023/02/06 11:15:37	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	UNICODE	Clean	Sniffer		2620:0101:9005:3235:0000:0000:0000:c121	2600:1409:3800:0181:0000:0000:0000:2c1a	
2023/02/06 11:15:37	9CA8ECCCFEAA58E4C2A859DEDB8B2DDC	UNICODE	Clean	Sniffer		172.19.236.121	20.253.213.245	

0% 20

- IPv6 addresses are displayed in NDR logs.

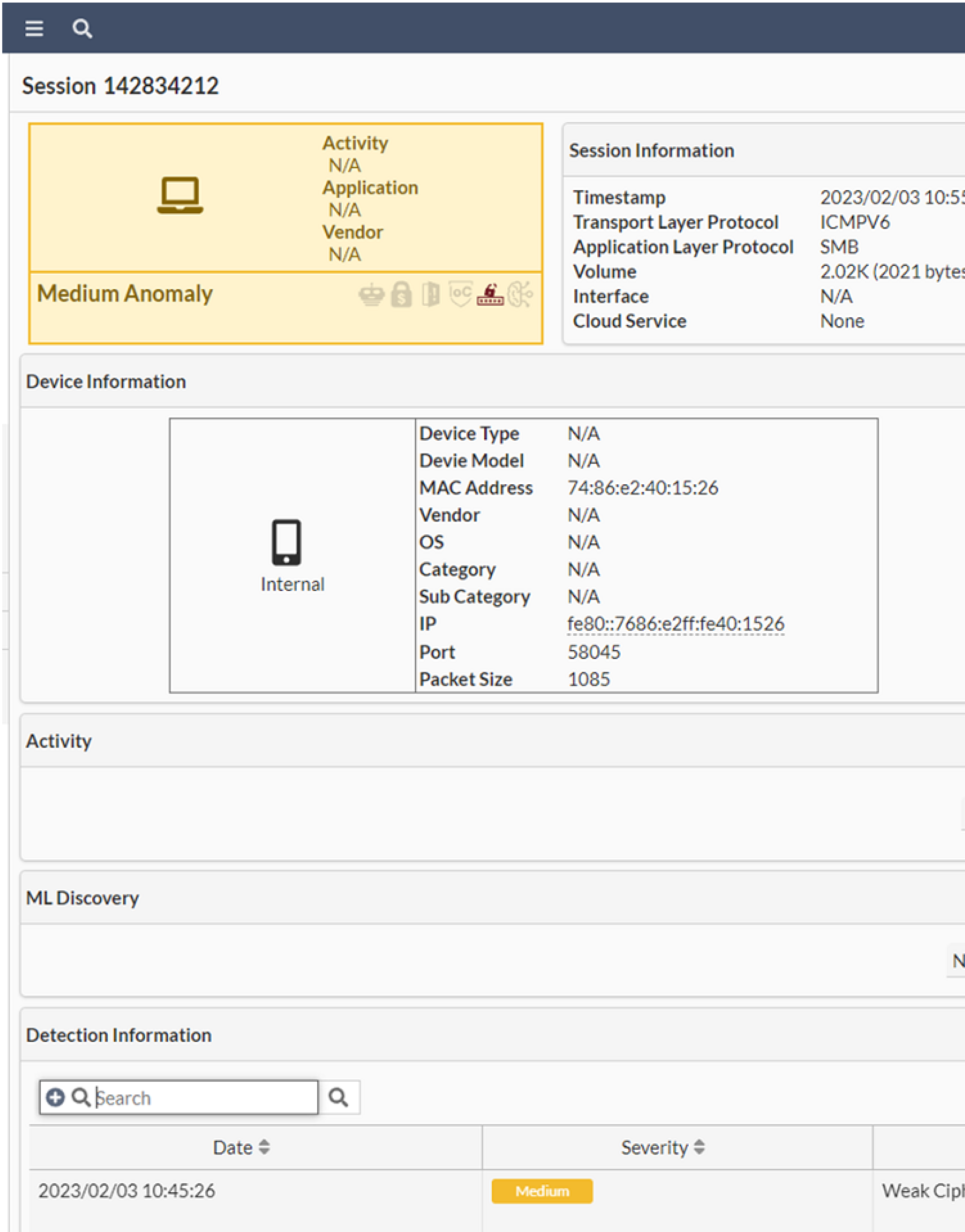


No ML training has finished yet

Source Address == fe80::7686:e2ff: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:e2ff:fe40...	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 10:5
Transport Layer Protocol	ICMPV6
Application Layer Protocol	SMB
Volume	2.02K (2021 byte
Interface	N/A
Cloud Service	None

Device Information

Internal

Device Type	N/A
Devie 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

Activity

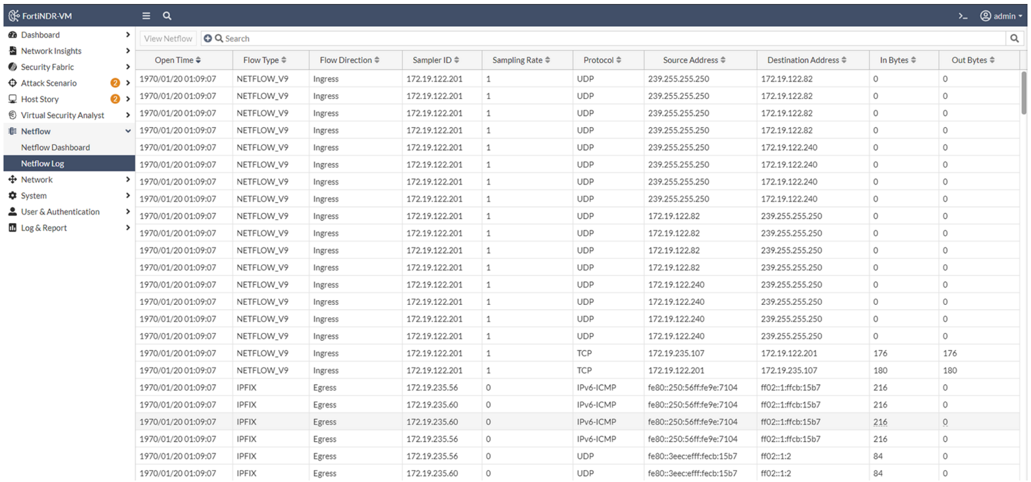
ML Discovery

N

Detection Information

Date	Severity	
2023/02/03 10:45:26	Medium	Weak Cip

- 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.



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	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	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::250:56ff:fe9e:7104	ff02::1:ffcb:15b7	216	0
1970/01/20 01:09:07	IPFIX	Egress	172.19.235.60	0	IPv6-ICMP	fe80::250:56ff:fe9e:7104	ff02::1:ffcb:15b7	216	0
1970/01/20 01:09:07	IPFIX	Egress	172.19.235.60	0	IPv6-ICMP	fe80::250:56ff:fe9e:7104	ff02::1:ffcb:15b7	216	0
1970/01/20 01:09:07	IPFIX	Egress	172.19.235.56	0	IPv6-ICMP	fe80::250:56ff:fe9e:7104	ff02::1:ffcb:15b7	216	0
1970/01/20 01:09:07	IPFIX	Egress	172.19.235.56	0	UDP	fe80::3eec:efff:fecb:15b7	ff02::1:2	84	0
1970/01/20 01:09:07	IPFIX	Egress	172.19.235.60	0	UDP	fe80::3eec:efff:fecb: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

FortiNDR has multiple ways to identify protocols and applications from sniffer traffic. The NDR engine supports in-depth analysis of the following protocols, plus thousands of applications available here. Application and protocols= identification is used to profile traffic for Machine Learning as well as identifying attacks against weak ciphers, botnets, intrusion etc.

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

Appendix H: File types and protocols

FortiNDR file scanning supports the following file types:

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

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

Appendix I: Operational Technology / SCADA vendor and application list

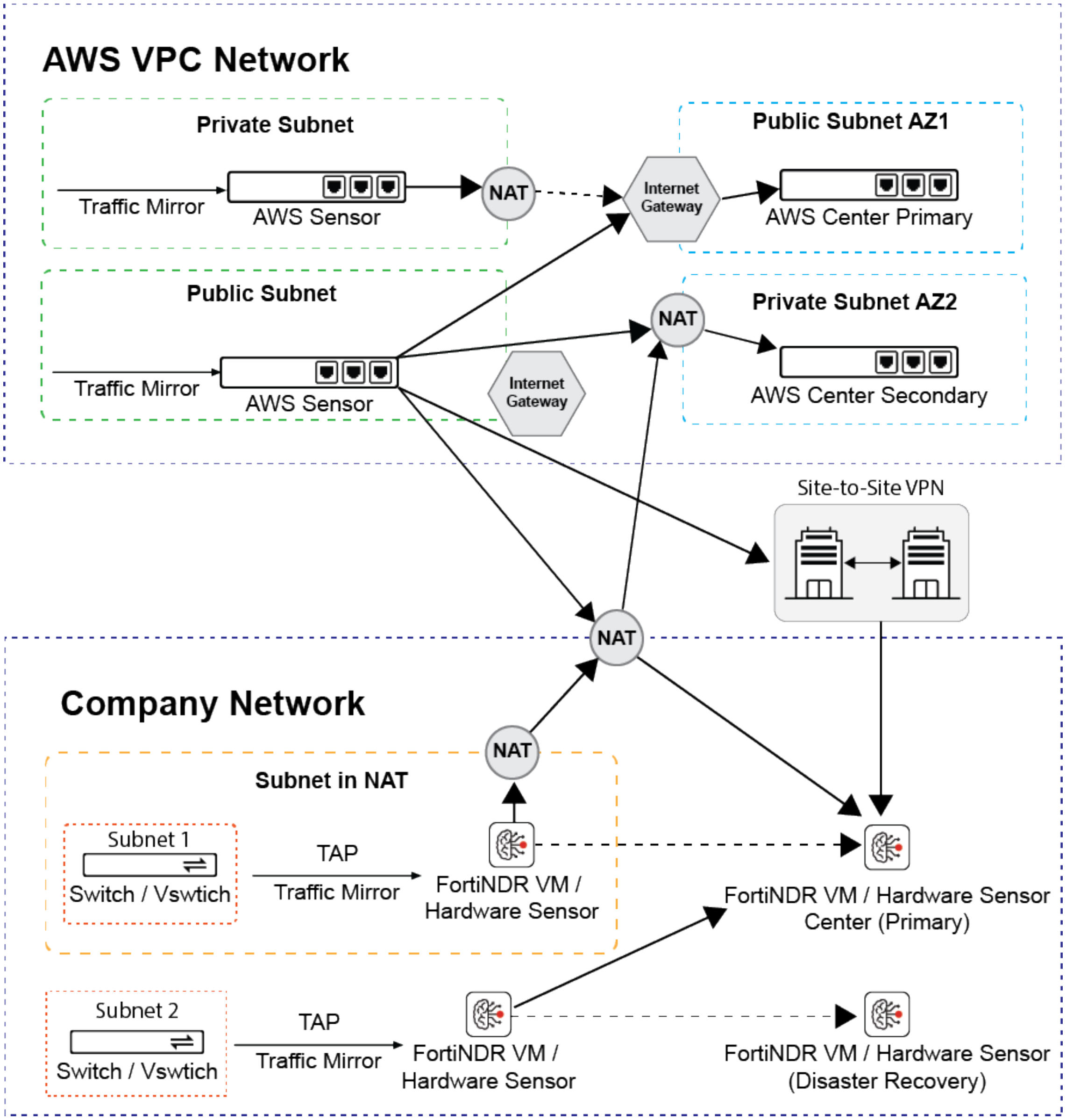
- 3S-Smart
- 7-Technologies
- ABB
- Advantech
- AzeoTech
- B&R
- Beckhoff
- Broadwin
- CODESYS
- CirCarLife
- CitectSCADA
- Cogent
- DATAC
- Delta
- Dut
- Eaton
- Fuji
- GE
- Gemalto
- Guardzilla
- IBM
- Iconics
- InduSoft
- Intellicom
- KeySight
- KingScada
- KingView
- Korenix
- LAquis
- Measuresoft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

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

Appendix J: Center Sensor Deployment

Topology

The following is an example topology showing NDR CM and Sensor deployment in AWS, or Hybrid with on-premise devices.



Redundant Center Setup

To achieve better availability, two center topologies are recommended to deploy in two different availability zones as illustrated in the topology above.

On-premises and Private Cloud (FNDR3K5, VM and KVM)

For deployment of on-premises and private cloud, please make sure the network access list listed in "Appendix C: FortiNDR ports" on page 265 are configured properly.

For VMCM/KVMCM deployment, please make sure the hosting platform satisfies the recommended disk specs of minimum 15TB (recommended 20TB), and that at least 48 cores (64 cores recommended) and minimum 384GB memory is assigned (recommended 512GB). For more information, refer to FortiNDR data sheet for details: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortindr.pdf

Public Cloud IAAS (AWS IaaS)

Enable access and configure security groups and ACLs for services and ports in the network access list found in "Appendix C: FortiNDR ports" on page 265.

Hybrid Cloud Deployment

When a scenario requires AWS hosted and on-premise Center topology, please ensure sure that network access is configured properly.

NAT Support

Network bandwidth and latency:

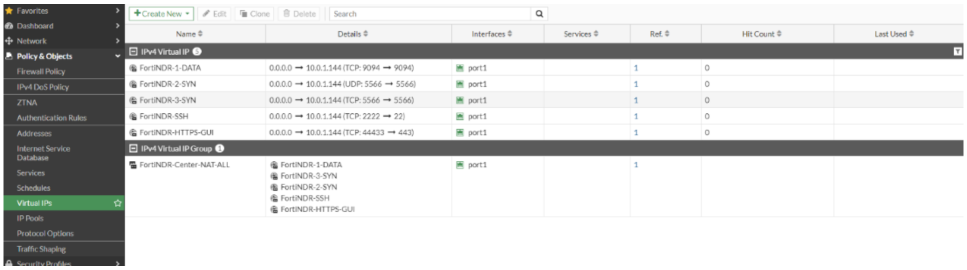
Please reserve 10Gbps for FortiNDR Center Port1 and ensure 1Gbps of network bandwidth are reserved from Sensor to Center. The network path should also maintain a low latency from Sensor to Center (P99 Round Trip time from ping should be <10ms).

For NAT deployment:

- Sensors deployed behind NAT do not require extra setup.
- For Centers behind NAT, please configure the following port forwarding in addition to HTTPS (Port 443) and SSH (Port 22). If multiple layers of NAT are involved, please make sure cascaded port forwarding is configured properly.
- For sensors and centers deployed behind NAT and using port-mapping from NAT gateways, please consider using the CLI for firmware upgrade. See, execute restore image.

NAT IP PORT	NDR Private Subnet Port	Protocol
5566	5566	UDP and TCP
9094(IPv4 deployment), 9096(IPv6 deployment)	9094(IPv4 deployment), 9096(IPv6 deployment)	TCP

Example: FortiGate Virtual IP configuration



Name	Details	Interfaces	Services	Ref.	Hit Count	Last Used
IPv4 Virtual IP 5						
FortINDR-1-DATA	0.0.0.0 → 10.0.1.144 (TCP: 9094 → 9094)	port1		1	0	
FortINDR-2-SYN	0.0.0.0 → 10.0.1.144 (UDP: 5566 → 5566)	port1		1	0	
FortINDR-3-SYN	0.0.0.0 → 10.0.1.144 (TCP: 5566 → 5566)	port1		1	0	
FortINDR-SSH	0.0.0.0 → 10.0.1.144 (TCP: 2222 → 22)	port1		1	0	
FortINDR-HTTPS-GUI	0.0.0.0 → 10.0.1.144 (TCP: 44433 → 443)	port1		1	0	
IPv4 Virtual IP Group 1						
FortINDR-Center-NAT-ALL	FortINDR-1-DATA FortINDR-3-SYN FortINDR-2-SYN FortINDR-SSH FortINDR-HTTPS-GUI	port1		1		

Limitations:

There is no limitation for sensor deployment behind NAT. For center deployment behind NAT, please ensure all sensors are using the same NAT address to connect.

Example:

For a NAT setup: 10.0.1.2 > 172.19.1.2 > FNDR Center Deployment, ensure all sensors are configured with center IP as 10.0.1.2 or 172.19.1.2. A mixed configuration of center address of 10.0.1.2 and 172.19.1.2 will lead to undefined behavior.