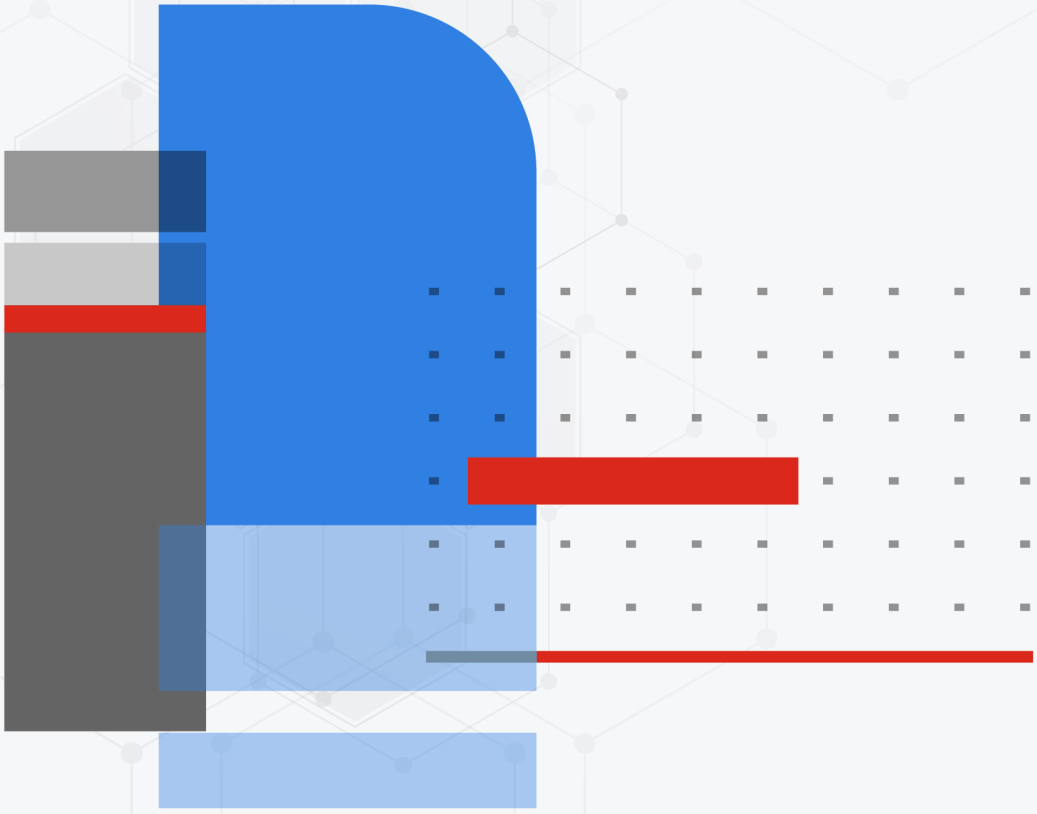
Administration Guide

FortiNDR 7.6.4



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

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 1, 2026
FortiNDR 7.6.4 Administration Guide
55-764-1249830-20260401

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-03-13	Initial release.
2026-04-01	Updated FortiSandbox on page 132 and FortiSandbox integration (FortiSandbox 4.0.1 and higher) on page 153.

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 events and high velocity malware detection and verdict using patented Artificial Neural Networks (abbreviated with ANN in document, US patent US11574051B2).

FortiNDR combined Network Detection features along with ANN that scans and classify malware in file based attacks. These functions are usually provided by your security operations analyst, hence in FortiNDR there's a concept of Virtual Security Analyst ^{TM}, which is capable of the following:

- Detect encrypted attack (via JA3 hashes), look for presence of malicious web campaigns visited, weaker ciphers, vulnerable protocols, network intrusions and botnet-based attacks.
- Profile ML traffic and identify events 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.
- Analyze Netflow data including machine learning of Netflow data, to detect attacks and events.
- 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. For more information, see Integration and Support in the Release Notes.

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 VM08, VM16 or VM32 subscription license. Both form factors will have Netflow and Operational Technology (OT)/SCADA licensed separately. The Netflow license will allow intake of Netflow data and inspection for security detections, while the OT/SCADA license will enable FortiNDR to detect and update industrial IPS and OT (Industroyer) malware classification, as well as identify OT applications for machine learning purposes.

See Appendix G: Supported IPS (including OT), Application Control, and protocols on page 303 for information about OT applications support.

VM08 supports sensor mode only and requires FortiNDR center to manage operations, VM08 does not support Netflow.

FortiNDR can receive both network traffic and inspect files using neural networks for scanning from different approaches: 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.

FortiNDR can also be deployed as standalone malware scanning technology, with integration with FortiGate(s) NGFW and FortiMail, FortiProxy for inline blocking, scanning network drives and S3 buckets, and integration with FortiSandbox as pre-scan.

Key advantages of FortiNDR include the following:

- Detect network events 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.
- 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 events detected, FortiNDR can perform manual and automatic mitigation (AKA Response) with Fortinet Security Fabric devices (such as FortiGate, FortiSwitch, FortiNAC), as well as third-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 206.

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*.

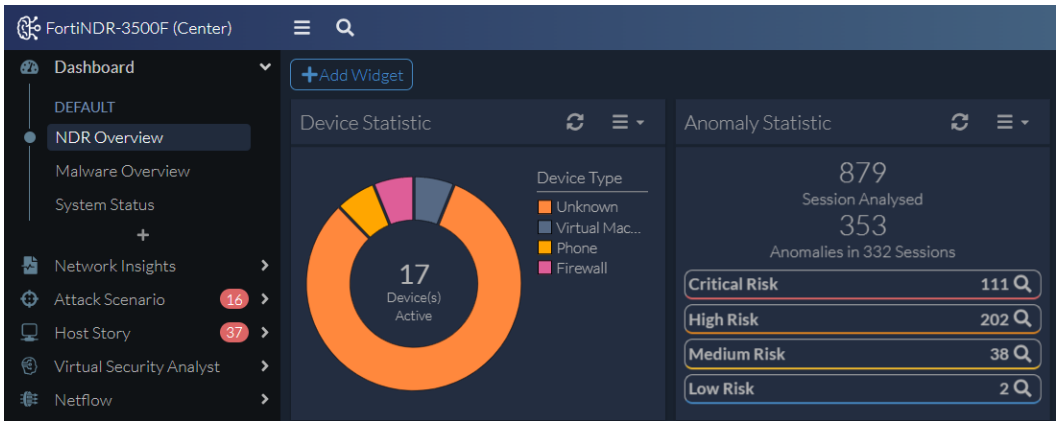
Standalone, Center and Sensor operating mode

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 7.6 supports Center Mode in for FNR-3500F and FNR-3600G. For Public Cloud and mode support, please refer to Release Notes as well as Public Cloud documentation.
  - 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 7.6.4 supports sensor mode in FNR-1000F and VM models. For more information, see the Release Notes.

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.
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	✔	✔	✔	Center and Sensor device enrichment is available starting in version 7.6.3.
Virtual Security Analyst > ML Configuration		✔		

Feature	Standalone	Center	Sensor	Notes
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.
Global Investigation and Tagging		✔		Query metadata and tagging of sessions. This feature is available in FNR-3600G and Central Management VM.
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	✔	✔	✔	Log Settings are supported in all modes. See, Log Settings on page 263.

FortiNDR Center and Licensing requirement

While FNR-3600G (a newer model) supports fully populated HDD when shipped,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 is available as a 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 v7.6.0 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 licenses maybe required.

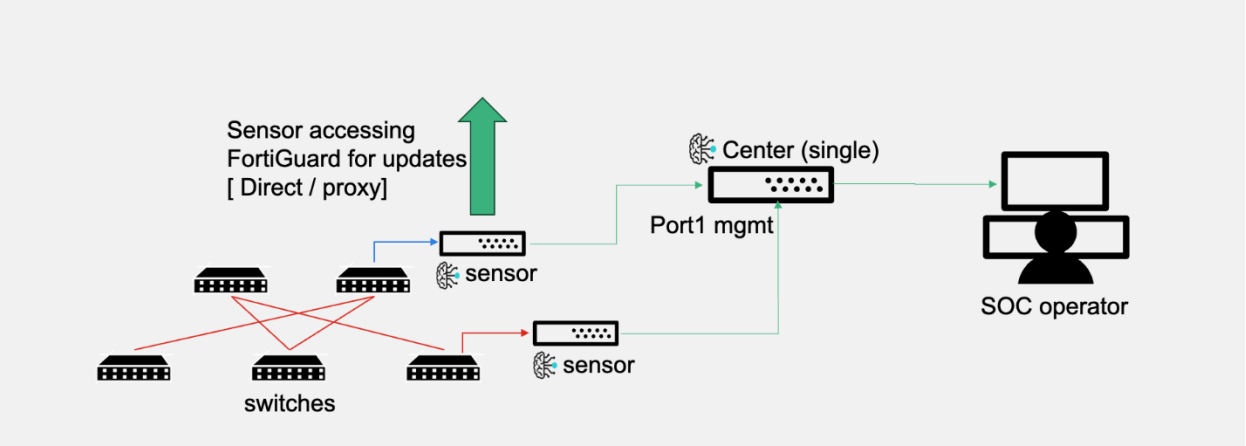
In Center Mode, the system does require a Neflow license to access the Netflow module.

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

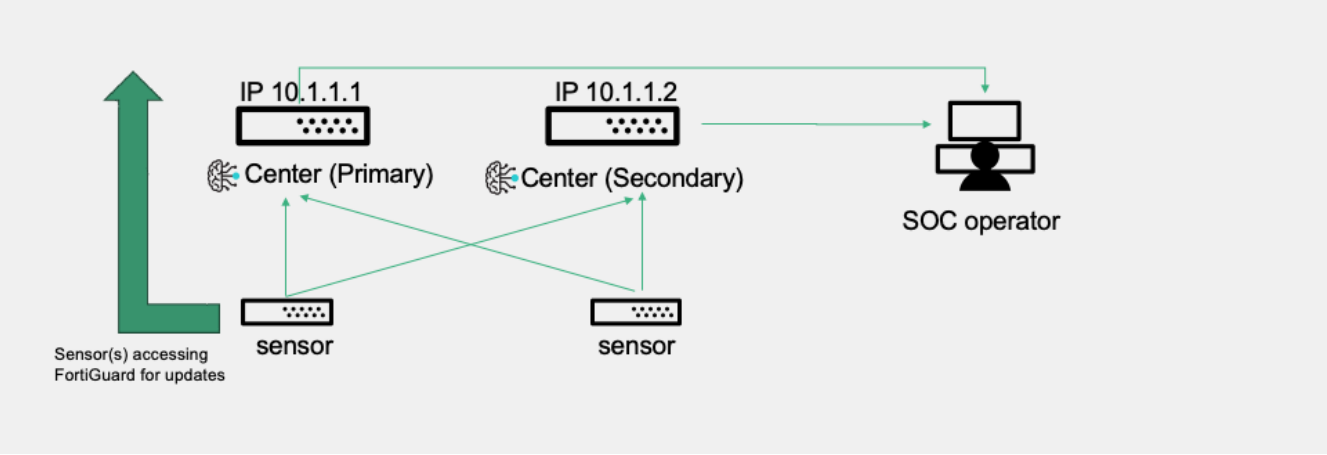
Dual Center mode support

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:



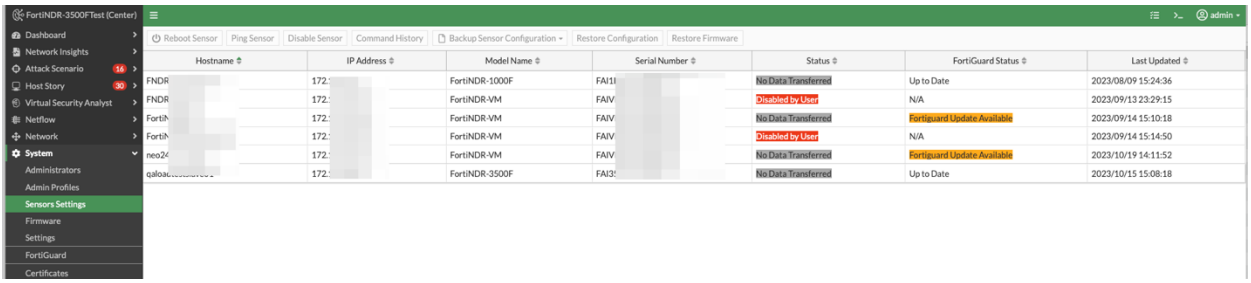
Dual NDR center support:



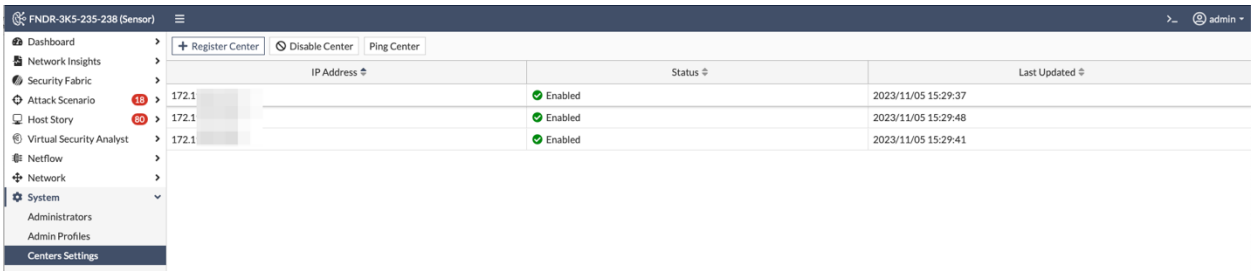
Sensors data are synchronized periodically between sensors and center using HTTPS port 443, connections are initiated by sensor to center. For a complete list of FortiNDR ports required, seeAppendix C: FortiNDR ports on

page 292. 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:



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



For information about sensors operations, seeSensor/Center settings on page 208 .

FortiNDR traffic and files input types

FortiNDR can operate in both detecting network events as well as malware analysis using ANN. If Network Detection 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}`"

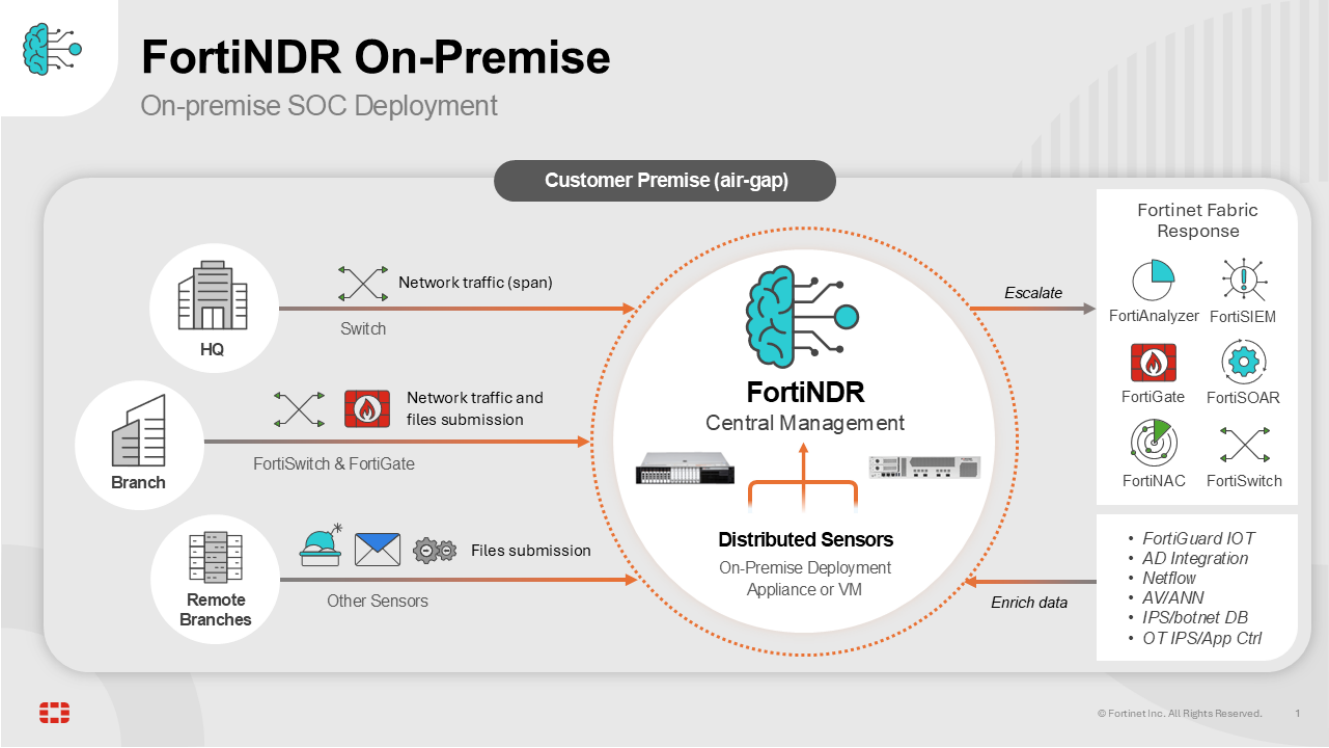
For more information, see the *FortiNDR CLI Reference Guide*.

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	Notes
Sniffer			Please refer to, Appendix G: Supported IPS (including OT), Application Control, and protocols on page 303.	Using SPAN port or network TAP. Using SPAN port, network tap or packet brokers to mirror traffic.

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	Notes
Fabric devices	FortiGate	HTTP2 (v7.0 FOS) OFTP (v5.6-6.0 FOS, legacy support)	HTTP, HTTPS (with SSL decryption), SMTP, POP3, IMAP,	FortiGate v7.0.1 supports 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. SMB file shares, and S3 bucket	SMB/NFS		Direct map and scan

For a complete list of supported file types, see Appendix H: File types and protocols on page 304

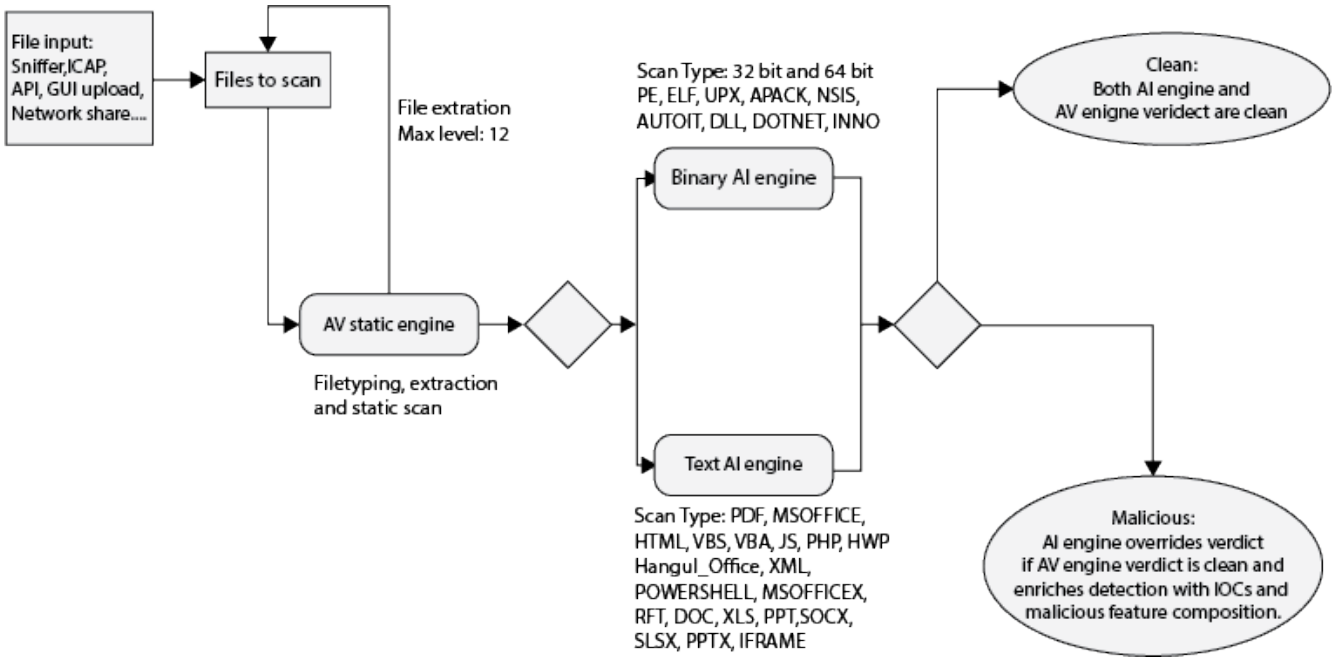
FortiNDR supports quarantine with incoming webhook from FortiOS 6.4 and higher. For details, see the Release Notes. For FortiNDR to quarantine via FortiGate, you must provide VDOM information to FortiGate. For details, see Automation Framework on page 138.



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.

File verdict caching is triggered automatically. When a cache hit occurs (based on the file hash) and no AVeng or AI database updates have taken place since the verdict was cached, FortiNDR uses the cached result. In this case, the file is not rescanned by the Binary or Text AI engines. For more details, see FortiGuard on page 218.

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.
- FNDR-2500G supports 4x 7.68TB RAID 10 15.36TB usable storage.
- FNR-3600G (center) supports 12 x 3.84 hot swapable SSD total of 176TB of disk in RAID 5)
- 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-2500G	15.36 TB	132 days
FortiNDR-3600G	12x16TB RAID5 176TB usable	365 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

*3600G retention can be adjusted with the CLI: `execute center-retention-setting`

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).

- Center mode: `execute center-retention-setting`
- Sensor/Standalone mode: `execute 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)
VM08	8	16GHz	64GB	4000 MBps / 1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS
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

	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)
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.

VM Center Mode with Investigation Feature ON (additional configuration)

These specifications apply only when the *Investigation* feature is enabled. Due to high compute and disk I/O requirements, this configuration may not be suitable for non-public cloud platforms.

vCPU	Reserved Memory	Reserved CPU GHz	Storage Type	Minimum Disk Performance	Recommended Disk Performance
128 cores	512 GB	307.2 GHz (128 × 2.4 GHz)	Local NVMe array on host (centralized storage not recommended) VMWare VSAN and Nutanix AOS are not supported.	Sequential: 12,000 MBps Read / 6,000 MBps Write4KB Random: 1,200,000 IOPS Read / 1,000,000 IOPS Write	Sequential: 18,000 MBps Read / 10,000 MBps Write4KB Random: 1,800,000 IOPS Read / 1,200,000 IOPS Write

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 294.

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

Ports

For FortiNDR VM and hardware, port1 and port2 are hard-coded to be management port and sniffer port. FortiNDR sniffer ports support both RSPAN and ERSPAN, allowing remote and encapsulated traffic mirroring for analysis.

The following is the initial port configuration for FNDR 3600G:

Port	Type	Function
Port1	10G SPF+ fiber	Management port, GUI, connection to sensors, REST API. Default IP address is 192.168.1.88 using admin with no password.
Port2	10G SPF+ fiber	Reserved for future use
Port3	10G SPF+ fiber	Reserved for future use
Port4	10G SPF+ fiber	Reserved for future use
Port5	RJ45 1G Copper	Only used by bootloader to transfer image

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.

Port	Type	Function
Console	Serial port	Console serial port. 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control.

The following is the initial port configuration for FNR-2500G.

Port	Type	Function
Port1	10G SFP+ 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 SFP+ Fiber	High Availability in Standalone mode, unused in Sensor mode
Port3 **Port4** **Port5** **Port6**	25G SFP28 Fiber	Sniffer port.
Port7	RJ45 1G Copper	Only used by bootloader to transfer image.
Console	Serial port	Console serial port. 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control.

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.
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.

FortiNDR-3600G can also use the following transceivers

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), please contact your local Fortinet representative for assistance.

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 27
- Vulnerability - monitoring PSIRT on page 28
- Firmware on page 28
- Encrypted protocols on page 28
- FortiGuard databases on page 28
- Penetration testing on page 29
- 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 204.

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 126.

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.

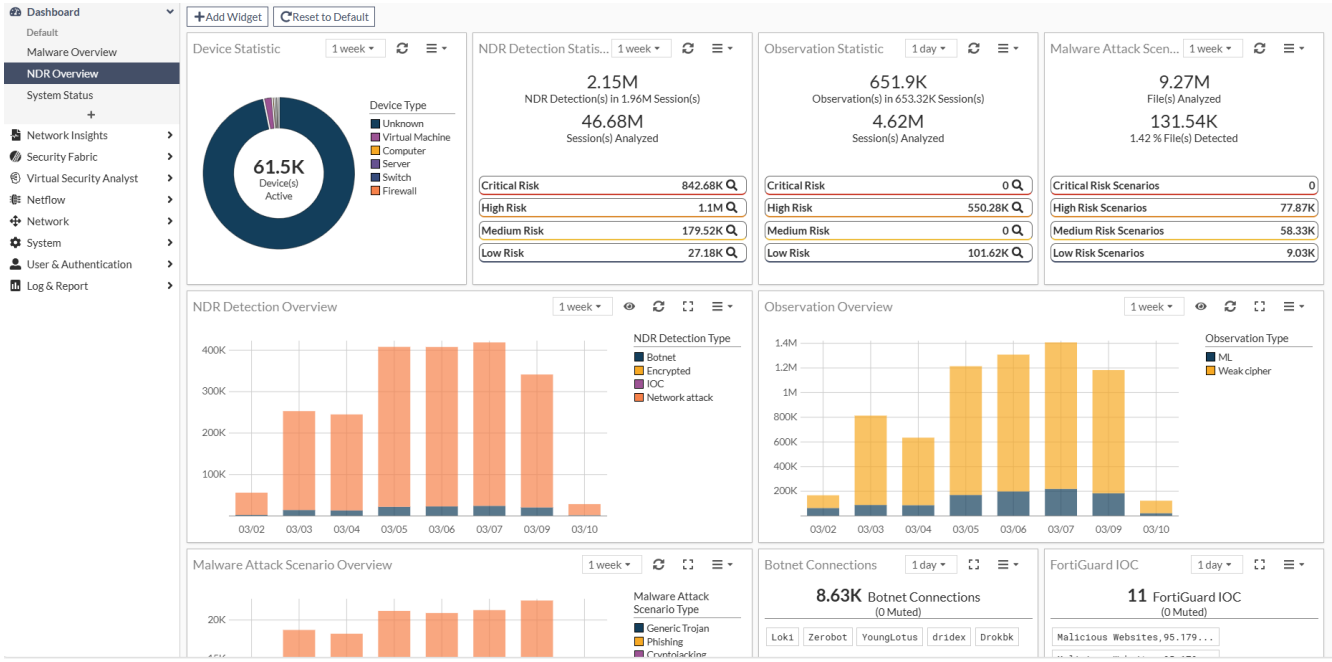
Dashboard

The *Dashboard* displays the overall events 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 the information in the *Network Insights* 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.



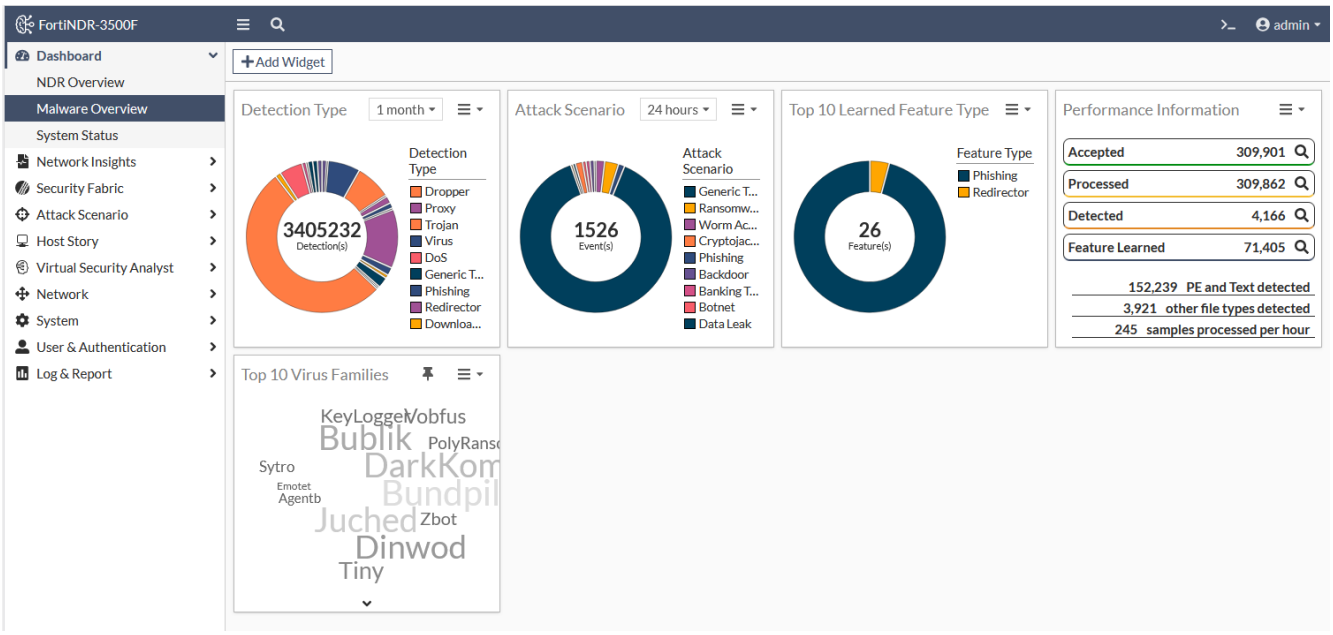
Available sensor(s) can be selected on top right of any widget(s) , it's important to include the sensors you want to view after adding new sensors.

Widget	Description
Device Statistic	Summarizes information from the *Device Inventory* dashboard. It displays device statistics for the past day, week, or month, showing the total number of active devices categorized by type. Click the widget to open the Device Inventory dashboard.
Detection/Observation Statistic	Summarizes security analysis for the past day, week, or month. It shows the number of sessions analyzed and the number of detections and observations detected across those sessions. Detections and observations are categorized by risk level. Click the magnifying glass icon next to the risk level to open the *NDR Log* page.
Malware Attack Scenarios	Shows the number of files analyzed over the past day, week, or month, along with the percentage detected as malicious. It categorizes scenarios by risk level. Click the widget to view a breakdown of scenario types for each risk level. You can drill down further to view the *Malware Attack Scenario Detail* page.
OT Device Statistic	Displays the number of operational technology (OT) devices detected across various layers of the Purdue Model over the past day, week, or month. Users can view statistics on the top 10 products for deeper insights into device types and activity trends. OT devices not yet assigned a Purdue level are still detected and shown in the inventory, where users can manually set their appropriate Purdue level.
NDR Detection Overview	Displays a stacked bar chart of detections against the current timeframe selected.
Observation Overview	Displays a stacked bar chart of observations against the current timeframe selected.
Malware Attack Scenario Overview	Summarizes the frequency of malware attacks over the past day, week, or month. Each bar in the chart represents a different malware type. It highlights peak attack periods to provide a clear visual of when and what types of malware activity are most prevalent. Click a bar to open the *Malware Attack Scenario Details* page.
Botnet Connections	Provides a snapshot of botnet activity over the past day, week, or month. It highlights the total number of botnet connections detected and identifies specific botnet families involved.
FortiGuard IOC	Displays threats detected over the past day, week, or month. It shows the number of IOCs, threat categories, and muted alerts.
Top Network Attacks	Displays the most frequent and severe network threats detected over the past day, week, or month. It reports the total number of attacks, including muted detections and their severity levels. Hover over an attack name to view recommended actions. You can also explore the attack name or view attack information in FortiGuard.
Weak Ciphers / Vulnerabilities	Shows the number of weak and vulnerable instances detected on sniffer port(s) on NDR interfaces over the past day, week, or month.

Widget	Description
Notifications	Displays real-time alerts for new detections. Events appear as they are received, and push notifications are supported. Hover over an alert to view the IP address or drill down to the IP details page.
Top Talkers (Internal) - By Traffic Volume	Shows internal network traffic over the past day, week, or month. The legend identifies each device pair.
ML Discovery	Displays machine learning-based event detection results from the past day, week, or month. It shows the number of events, including muted detections, and indicates baseline status. A timestamp at the bottom shows when the ML model was last trained. *ML Discovery* is visible in Standalone and Center mode. ML Discovery settings are configured and viewed from Center for all sensors. ML Discovery is not available in Sensor mode.
Top Applications	Displays the amount of network traffic distributed across various applications over the past day, week, or month. Hover over an application to view the traffic source.
Top URLs Visited	Displays the most frequently accessed URLs over the past day, week, or month. It lists high-traffic destinations and endpoints with visit counts.
Top Domains Visited	Displays the most accessed domains over the past day, week, or month. It shows visit counts for each domain, followed by internal IPs and external domains.
Traffic by Protocol	Provides a visual breakdown of network traffic by protocol over the past day. It features charts for internal and external traffic, segmented by protocol.
MITRE ATT&CK	Shows the frequency of various cyberattack tactics observed over the past day within an Enterprise or ICS environment. Click on a tactic to view the NDR Detection page where you can access the device and session details.

Malware Overview

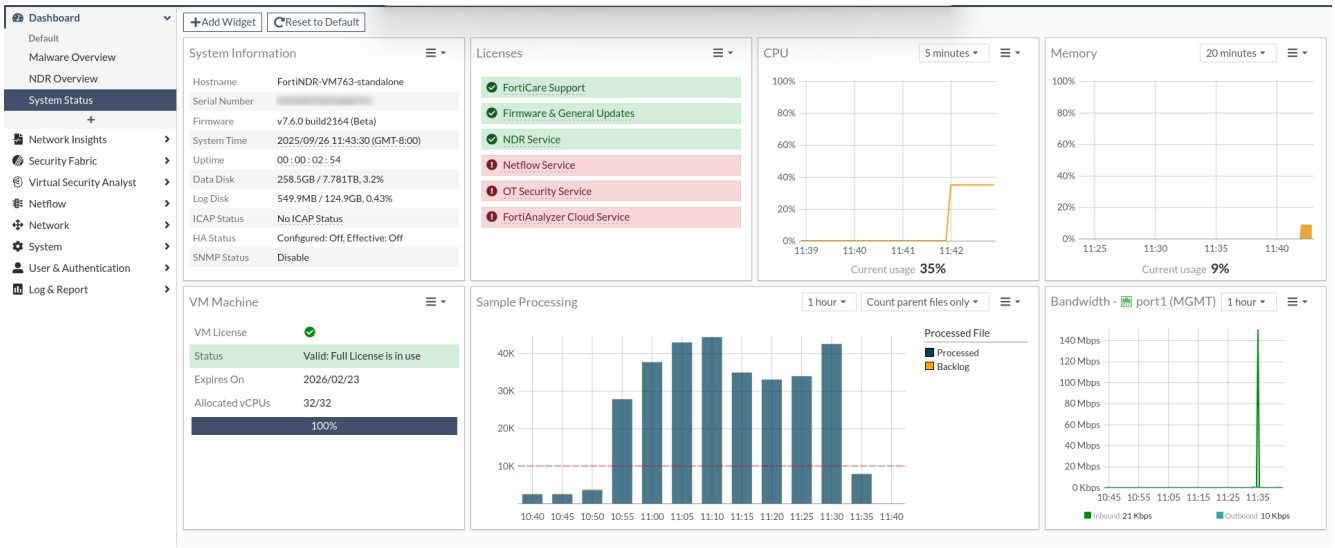
The *Malware Overview* dashboard displays information about malware attacks and performance information as charts and graphs.



Widget	Description
Malware Detection Type	Shows the distribution of threat detections by type over the past hour, day, or week.
Malware Attack Scenario	Summarizes malware attack types detected over the past day, week, or month. The chart segments represent attack categories and the total number of events. Click a segment in the chart to open the Malware Attack Scenario details page.
Top 10 Learned Feature Type	Displays the distribution of the top 10 learned feature types, based on the number of features. Each segment corresponds to a specific threat category, with color-coded labels in the legend for easy identification.
Performance Information	Displays key performance metrics over the past hour, day, or week, including the number of samples detected, processed, and accepted. It also shows the total number of features in use. Additional breakdowns include PE and text files detected, as well as other file types.
Weekly Top 10 Virus Families	Highlights the most prevalent virus families detected over the past day, week, or month. The names are displayed in varying font sizes to visually represent their relative frequency or impact.

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.



Widget	Description
System information	The *System Information* widget provides an overview of the FortiNDR device's operational state and configuration. It displays key details about the device, including its hostname, serial number, firmware version, system time, uptime, disk usage, and the status of features like ICAP, HA, and SNMP.
Licenses	The *Licenses* widget displays the status of Fortinet services, indicating which are active and which require attention. Active services are marked with a green checkmark, while inactive services or those with issues are marked with a red exclamation mark.
CPU	The *CPU* widget displays real-time CPU usage over 5, 10, and 20-minute intervals.
Memory	The *Memory* widget displays real-time memory usage over 5, 10, and 20-minute intervals.
VM Machine	The *VM Machine* widget displays licensing and resource allocation details, including license status, expiry date, and the number of vCPUs allocated.
Sample Processing	The *Sample Processing* widget monitors the system's file processing performance. A red dotted line indicates the performance threshold, which is the maximum recommended processing rate for the specific appliance or VM model in use. This threshold is based on the system's expected capacity as defined in the product datasheet. The performance threshold indicator appears only when the number of accepted files approaches the threshold; it remains hidden when file volume is significantly lower.
Bandwidth	The *Bandwidth* widget displays inbound and outbound traffic for port1 (MGMT) over 1-hour, 1-day, and 1-month periods. It shows how much data is being sent and received over time, with traffic levels measured in kilobites per second and plotted against a time-based graph.

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.

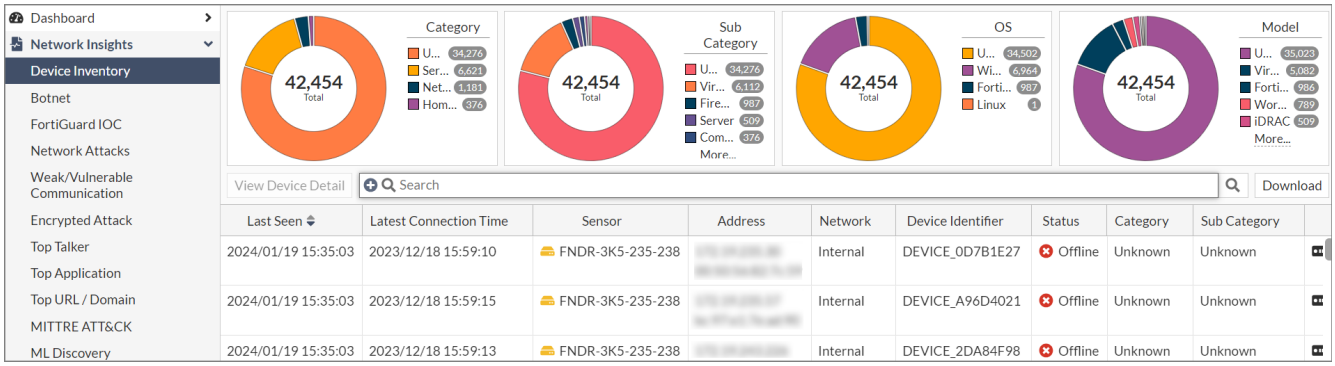
Remember to use the widget settings to include sensors, so their data is displayed in the widgets.

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.



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 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).

Monitor	Description
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.
ML Discovery	Displays a list of events 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.

NDR Detections, Observation, Connection and Session tabs

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

Tab	Description
NDR Detections	Provides a summarized view of all detected threat activity, displaying key monitors and detailed event records to help you quickly identify, assess, and investigate network-based detections.
Observation	Provides a summarized view of weak or vulnerable communication and ML observations, for quick assessment of protocol weaknesses, severity levels, and patterns of insecure network behavior.
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 86.
Session	Shows granular session information for each attack including the Source and Destination IPs. For more information, see Session tab on page 89.

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.
Severity	The event severity (*Not Observation*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Category	The device category (*Unknown*, *Home & Office*, *Mobile* and *Network*).
Count (Historic)	The total number of times the event was observed.
Count (Past week)	The total number of times the event was observed during the past week.
First Timestamp	The timestamp for the first time the event 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.

Column	Description
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*.

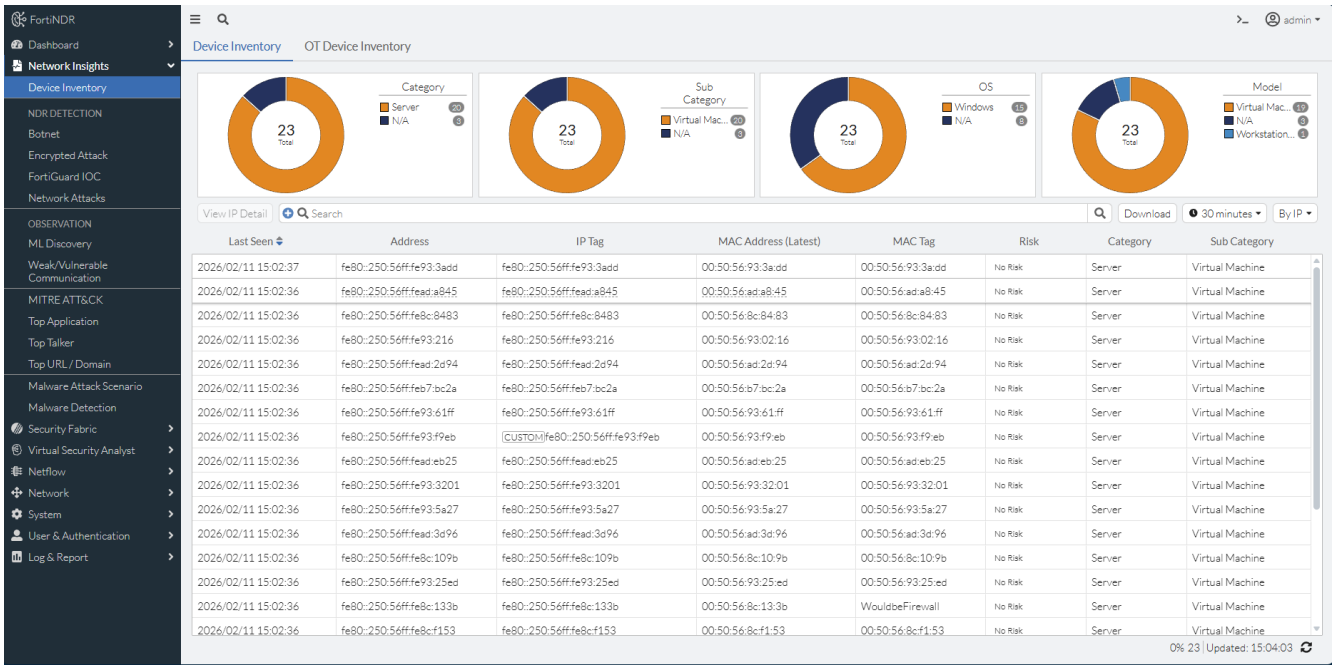
Device Inventory

The *Network Insights* > *Device Inventory* page monitors device activity and helps identify potential security risks across the network. It displays detailed information for all discovered devices, including IP address, MAC address, IP tag, MAC tag, risk level, category, subcategory, model, operating system, vendor, and last connection time. You can view enriched device names, download inventory data, and access deeper insights such as detections and malware history through the IP or Device Profiles pages.

IP Tag and MAC Tag

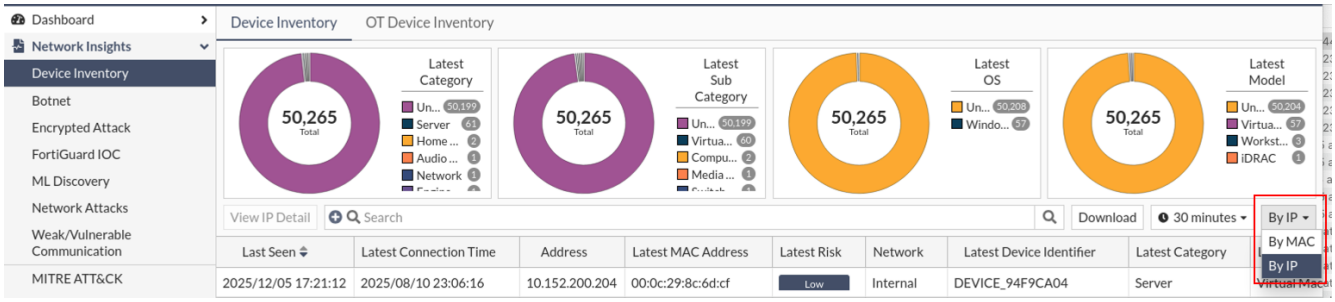
FortiNDR uses *IP Tag* and *MAC Tag* inventory identifiers to ensure consistent device naming across the system.

Tag	Description
IP Tag	The IP tag represents the name associated with a device's IP address. Priority (highest → lowest): **1.** User-defined IP tag (for example, *office*). **2.** AD device enrichment (hostname retrieved from Active Directory, when configured). **3.** Raw IP address.
MAC Tag	The MAC tag represents the name associated with a device's MAC address. Its priority (highest → lowest) is: **1.** User defined MAC tag (for example, *office*) **2.** Raw MAC address



Column	Description
Last Seen	The date and time the device was last seen.
Address	The device IP address ,
IP Tag	A user-assigned or system-generated tag that helps classify or identify the device based on its IP address.
MAC Address	The unique MAC address identifying the device's network interface.
MAC Tag	A user-assigned or system-generated tag applied to the device based on its MAC address.
Risk	The assessed risk level of the device based on observed behavior, vulnerabilities, or security posture.
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.
Device ID	The device ID.
Model	The device model.
Vendor	The device vendor.

View modes



You can use the view selector on the right corner of the table to view the page *By Mac* or *By IP* address.

- *By IP* (default): Each row represents a unique IP address. The MAC address shown is the most recent device that used that IP. The page may display multiple rows with the same MAC address because the device list is sorted by IP address. Duplicate MAC addresses will appear on separate rows, each associated with a different IP.
- *By MAC*: Each row represents a unique device identified by its MAC address. The IP address shown is the most recent one used by that device. This option displays the latest IPs. To view he IP address under the same MAC address, do one of the following:
  - Search by mac address in the *By MAC* mode
  - Double-click the device and select the *IP History* tab in the pane.

In *By IP* mode, the *Device Inventory* monitor displays the following information:

Column	Description
Last Seen	The date and time of the latest session of the device IP Address.
Address	The device IP address.
Latest Mac Address	The latest MAC address that has been assigned to the device IP Address.
Latest Risk	The risk level of the latest device assigned to the device IP Address.
Latest Category	The device category of the latest device assigned to the device IP Address.
Latest Sub Category	The device subcategory of the latest device assigned to the device IP Address.
Latest Model	The device model of the latest device assigned to the device IP Address.
Latest OS	The OS of the latest device assigned to the device IP Address.
Latest Vendor	The vendor of the latest device assigned to the device IP Address.
IP Tag	The name associated with a device's IP address.
MAC Tag	The name associated with a device's MAC address.

In *By MAC* mode, the *Device Inventory* monitor displays the following information:

Column	Description
Last Seen	The date and time the device was last seen.
Latest Address	The device IP address.
MAC Address	The device MAC Address.
Risk	The risk level of the device.
Category	The device category (Unknown, Home & Office, Mobile and Network).
Sub Category	The device sub category (Unknown, IP Phone, Computer, Phone, or Firewall).
Model	The device Model.
OS	The device Model.
Vendor	The device Vendor.
IP Tag	The name associated with a device's IP address.
MAC Tag	The name associated with a device's MAC address.

Differences between Device Inventory *By IP*, *By MAC* and the NDR Log's *Device Page*?

View	Description
Device Inventory *By IP*	Displays each discovered IP address with its most recent occurrence and the corresponding latest MAC address. Each IP appears only once in the table, while MAC addresses may be repeated if associated with multiple IPs.
Device Inventory *By MAC*	Displays each device's MAC address with its latest occurrence and the most recent IP address it used. Each MAC address appears only once in the table. IP addresses may be repeated if assigned to multiple devices over time.
Device Log	Shows the latest occurrences of each unique IP and MAC address pair, with related information. Each distinct IP–MAC pair appears only once.

Downloading device inventory

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

Viewing device information

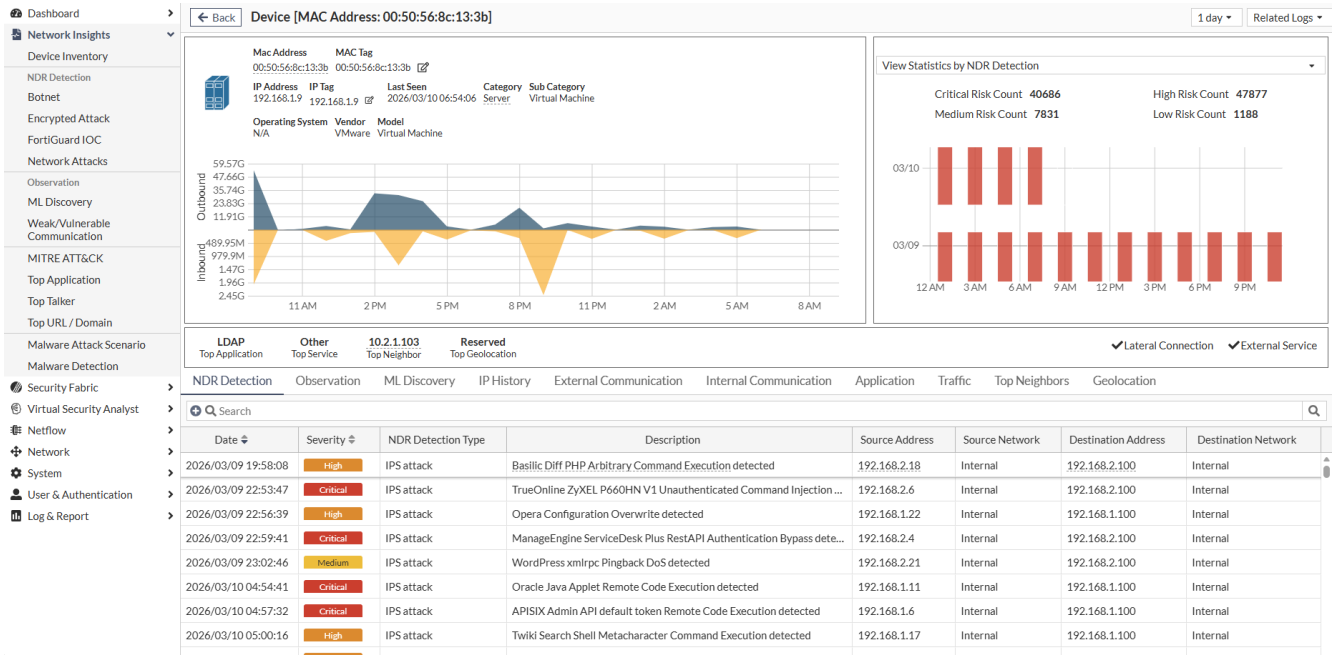
Double-click a record in the table to open the *Device Information* pane. The *General* tab includes:

- *General*: IP Tag/MAC Tag, Last Seen
- *Hardware*: MAC Address, Category, Sub Category, OS, Vendor, Model, Product, Firmware, Version, Serial Number
- *Network*: IP

If accessed from the *By IP* view in *Device Inventory*, a *Device History* tab is displayed, showing all MAC address occurrences associated with the selected IP. If accessed from the *By MAC* view or from *Device Log*, an *IP History* tab is displayed, showing all IP address occurrences associated with the selected MAC.

Device Profile page

The *Device Profile* page provides information about specific devices identified by MAC address including (but not limited to) statistics, traffic, IP used by the device, and neighboring devices.



To open the Device Profile page:

From	Description
Network Insights	1. Go to *Device Inventory*. 2. Select the *By MAC* view mode from the dropdown. 3. Double-click an entry in the table. 4. Click the *View Device Details* icon in the red handle.
Log & Report	1. Go to *NDR Log*. 2. Click the *Device* tab. 3. Double-click an entry in the table. 4. Click the *View Device Details* icon in the red handle.

The top right corner of the page contains a time range dropdown and a search option for the selected device. Click *Go* to apply your search criteria.

The monitor at the left side of the page displays the *MAC Tag* of the device and *IP Tag* of the latest IP associated with the device. You can change the MAC Tag/IP Tag by clicking the *Edit* icon.

Tag changes are local only. Updates made on sensors will not sync with Centers, and changes on Centers will not affect sensors.

The monitor also shows the latest IP used by the device, MAC address, and general information such as device category, OS, Vendor, and Model. The *Inbound* and *Outbound* graph shows the traffic volume for the selected time range.

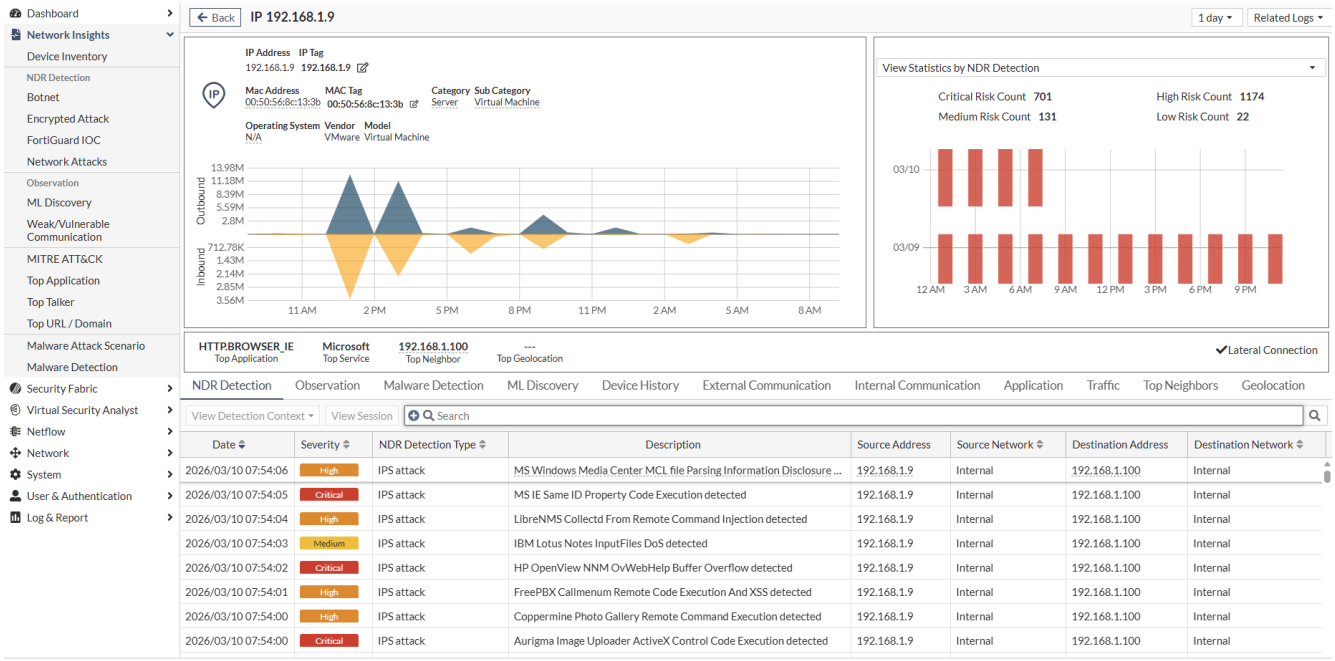
The *NDR Detection/Observation* heat map on the right side of the page shows the number of detection/observation occurrences by severity as well as the number of events in each period. Use the dropdown to choose between *NDR Detection* and *Observation*.

The following table provides an overview of the tables and tabs in the device profile page:

Column	Description
NDR Detection	Shows all NDR Detections (*IOC*, *Network Attack*, *Encrypted Attack*, *Botnet*) on this device in the selected time range. Double-click a row to show more information about the session.
Observation	Shows all Observations (*Weak cipher*, *ML*) on this device in the selected time range. Double-click a row to show more information about the session.
ML Discovery	Shows all suspicious sessions detected by ML on this device in the selected time range. Double-click a row to show insights regarding selected detection.
IP History	Shows all IP used by the device in the selected time range.
External Communication	Shows all sessions involving application services where the selected device communicates with an external IP address. Double-click a row to open the session information pane. Click a row and then click the *View Session Detail* button to be redirected to the session detail page.
Internal Communication	Shows all sessions with application services involved where the selected device communicates to an internal IP. Double-click a row to open the session information pane. Click a row and then click the *View Session Detail* button to be redirected to the session detail page.
Application	Shows all sessions that include the selected device with the corresponding application information.
Traffic	Shows all sessions that include the selected device with the corresponding network traffic.
Top Neighbors	Shows devices the selected device communicated with during the selected time range, ordered by total traffic size. Click a row and then click *View Device Detail*to redirect to the device detail page.
Geolocation	Shows the origin of all the external IPs that the selected device communicated with ordered by total session count.

IP Profile Page

The *IP Profile* page shows information about a specific IP including (but not limited to) statistics, traffic, devices that use the IP, and neighboring IPs.



To open the IP Profile page:

Option	Description
Network Insights	1. Go to *Device Inventory*. 2. Select the *By IP* view mode from the dropdown. 3. Select a device in the table and click *View IP Detail*.
Log & Report	1. Go to *NDR Log*. 2. Click the *Device* tab. 3. Select a device in the table and click *View Device Detail*.

The top right corner of the page contains a time range dropdown and a search option to search for the selected IP in the *Session Logs*, *NDR Detection Logs*, or *Observation Log*.

The monitor at the left side of the page displays the IP Tag of the device and *MAC Tag* of the latest MAC associated with the IP. You can change the MAC Tag/IP Tag by clicking the *Edit* icon.

Tag changes are local only. Updates made on sensors will not sync with Centers, and changes on Centers will not affect sensors.

The monitor also shows the information of the latest hardware that uses this IP such as MAC address, device category, OS, Vendor, and Model. The *Inbound* and *Outbound* graph shows the traffic volume for the selected time range.

The *NDR Detection/Observation* heat map on the right side of the page shows the number of detection/observation occurrences by severity as well as the number of events in each period. Use the dropdown to switch between *NDR Detection* and *Observation*.

The following table provides an overview of the tables and tabs in the IP profile page:

Column	Description
Malware Detected	Shows all malware detected on this IP in the selected time range. Double-click a row (or click each a row and then click *View Event Information*) to view the attack chain.
ML Discovery	Shows all suspicious sessions on this IP detected by ML in the selected time range. Double-click a row to show insights regarding selected detection.
Device History	Shows all devices that have used the selected IP in the selected time range.
External Communication	Shows all sessions involving an application service where the selected IP communicates with an external IP. Double-click a row to open the session information pane. Click a row and then click *View Session Detail* to be redirected to the session detail page.
Internal Communication	Shows all sessions with application service involved where the selected IP communicates with an internal IP. Double-click a row to view the session information. Click a row and then click *View Session Detail* button to view the session detail page.
Application	Shows all sessions for the selected IP along with its associated application information.
Traffic	Shows all sessions for the selected IP with network traffic.
Top Neighbors	Shows devices that the selected IP connected to within the selected time range, sorted by total traffic volume. Click a row and then click *View Device Detail* will redirect to the device detail page.
Geolocation	Shows the origin of all external IPs the selected IP connected to, ordered by total session count.
NDR Detection	Shows all NDR Detections (*IOC*, *Network Attack*, *Encrypted Attack*, *Botnet*) on this IP in the selected time range. Double-click a row to show more information about the session.
Observation	Shows all Observations (*Weak cipher*, *ML*) on this IP in the selected time range. Double-click a row to show more information about the session.

OT Devices

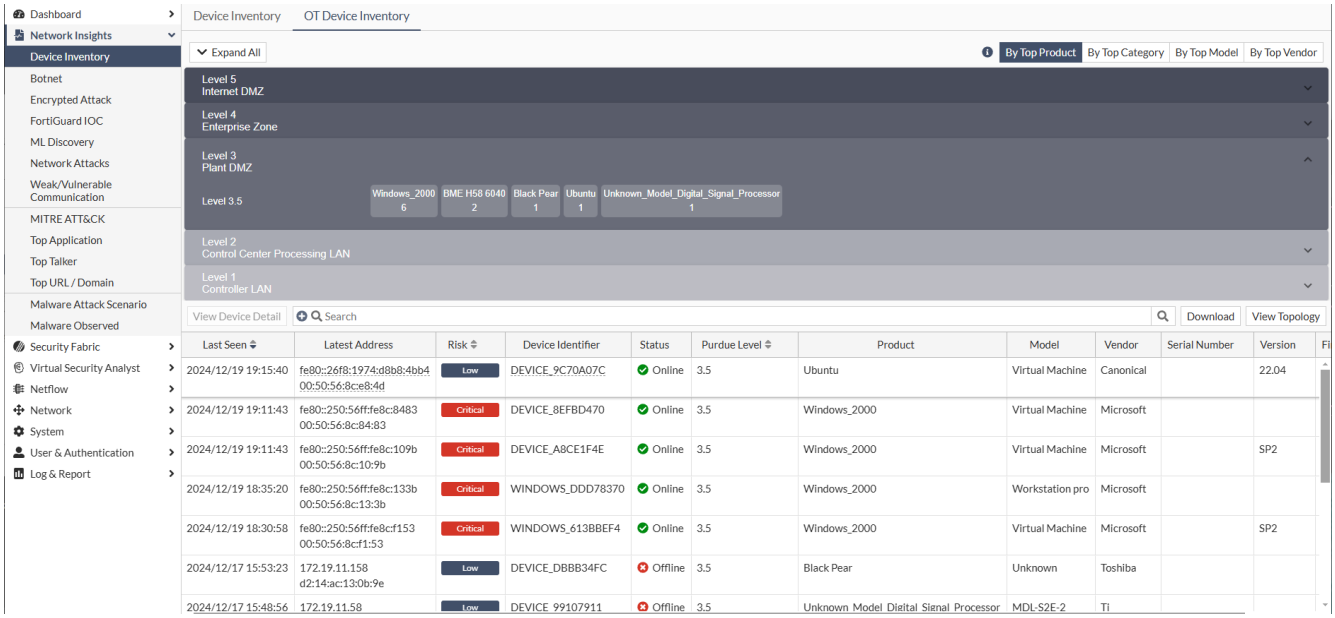
The *OT Devices* tab displays only devices recognized as Operational Technology (OT).

OT Device Inventory

The *Purdue Level chart* appears at the top of the page. The *Purdue Graph* shows the Top 10 devices of each Category. You can collapse and expand the chart by clicking the button at the top-left corner of the graph.

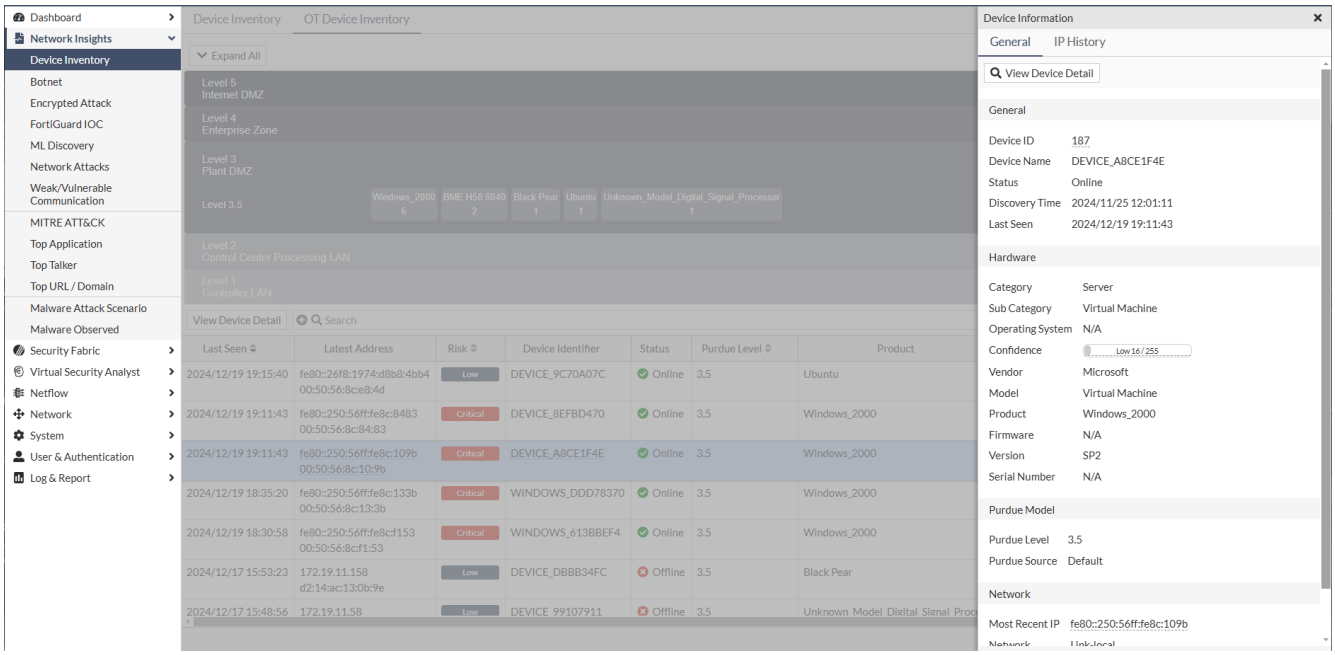
By Top Product	The Top 10 Product Type with the most devices will be shown in the Purdue level Chart.
By Top Category	The Top 10 Device Category with the most devices will be shown in the Purdue level Chart.
By Top Model	The Top 10 Device Model with the most devices will be shown in the Purdue level Chart.
By Top Vendor	The Top 10 Vendor with the most devices will be shown in the Purdue level Chart.

The table at the bottom of the page lists all the identified OT devices, featuring OT attributes identified by databases by default. You can view additional column attributes by enabling additional columns in the column settings.



Device Information

Double-click a device to open the *Device Information* pane. Click the *IP History* tab to track the selected device's IP history.



Export OT devices

Click the *Download* button. The OT device table data is downloaded as a CSV file.

Topology Graph

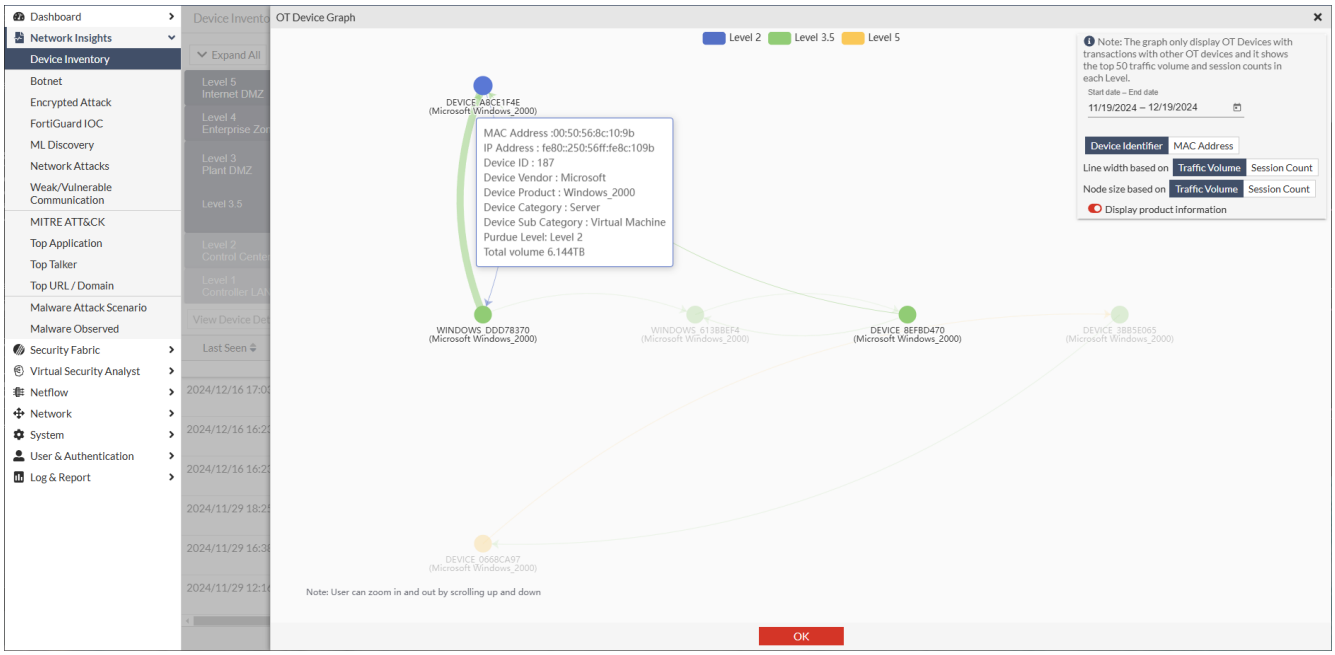
Click the *View Topology* button to view the *Topology Graph*.

The Topology graph displays active OT devices as nodes on the graph. All OT devices are split into levels based on their Purdue level. Each level shows the top 50 OT devices by traffic volume from each Purdue level (maximum 50 x (5 level + 5 sub-level) = 500 devices/nodes). You can set the line width and node size to represent traffic volume or session count with the toggles at the top-right corner of the graph. You can also zoom in and out the graph by scrolling up and down. Hover over each node to get more information about the node. Clicking a node will open the *Device Information* pane. All the nodes can be repositioned by dragging and dropping. You can hide or show the different Purdue level of devices by clicking the legend on the top of the graph.

You can set the time range of the device with traffic to be included.

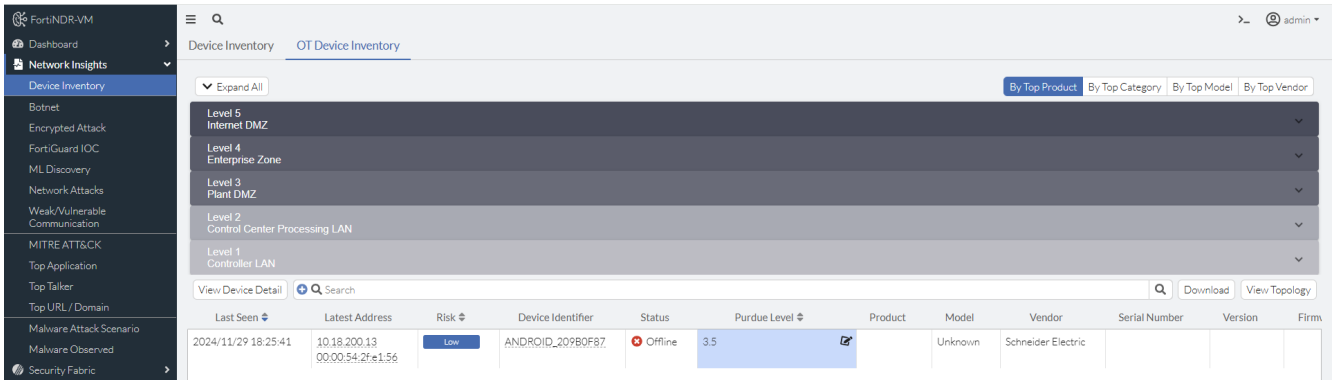
Start Date - End Date	Sets the time range of the device with traffic to be included.
The Device identifier vs MAC address	Controls the legend display under each node that identifies it.
Line Width based on Traffic Volume/Session Count	Modify the width of the connection in the graph by correlating to either Traffic Volume or Session counts. This helps to identify high frequency connections

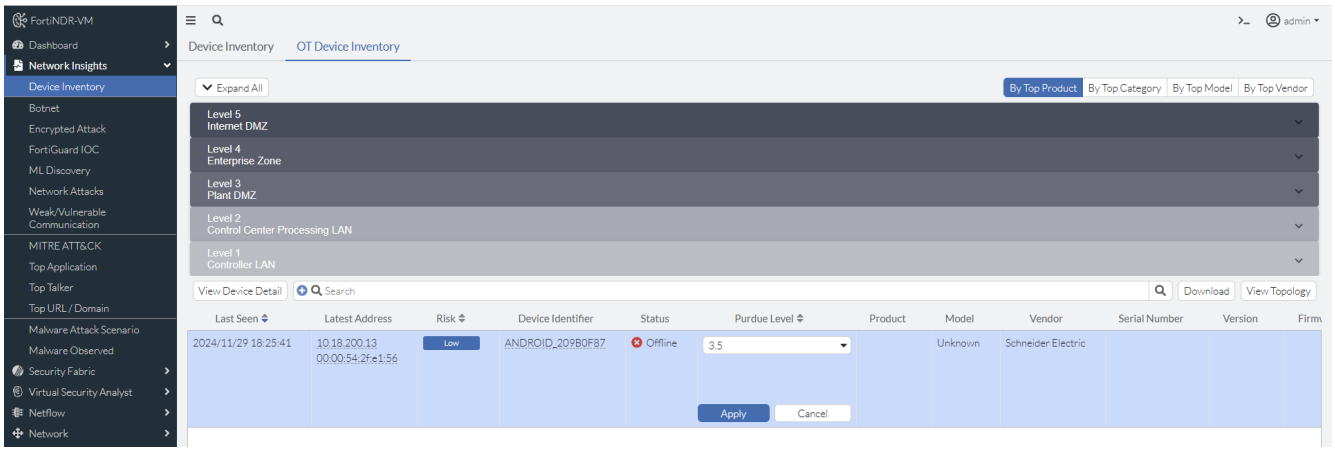
Node size Based on Traffic Volume/ Session	Modify the size of the node in the graph by correlating to it either Traffic Volume or Session counts. This helps to identify devices with high connectivity.



Modifying the Purdue Level

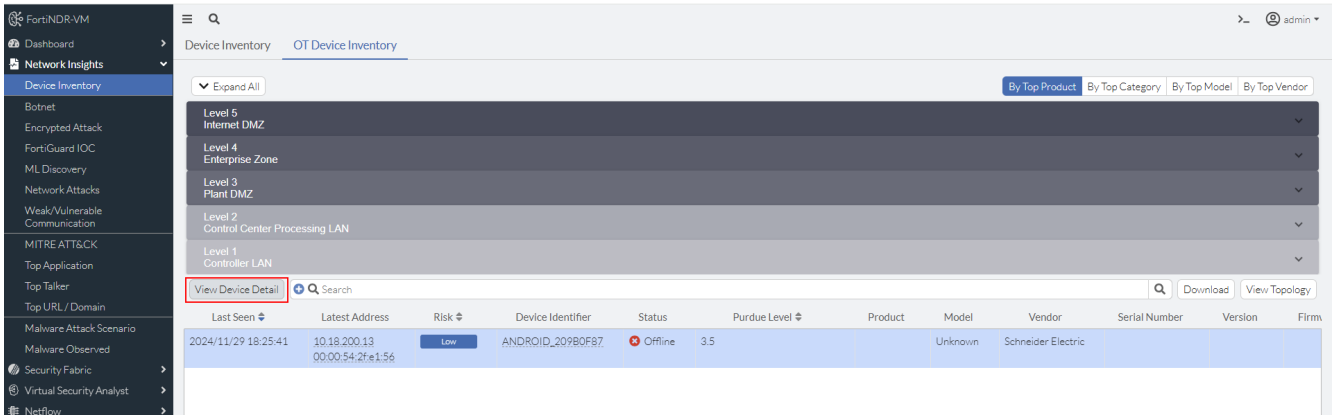
The Purdue level of any OT device recognized by the system defaults to 3.5. You can assign different Levels and sub levels in the table as shown below.



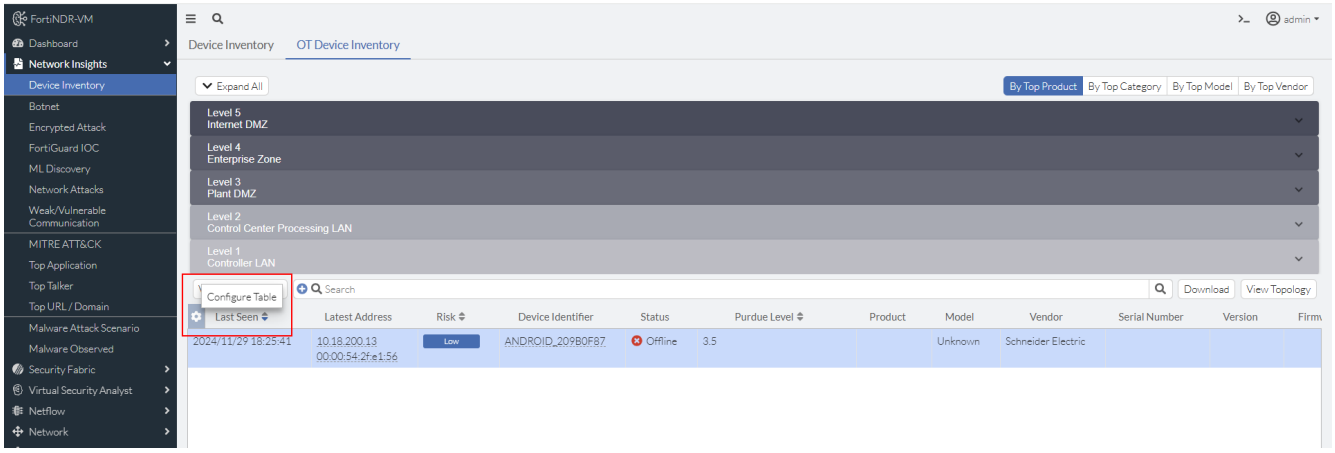


OT Device Inventory Table

You can link to the detailed device profile page by selecting a specific entry and clicking *View Device Detail* at the top-left corner of the table.

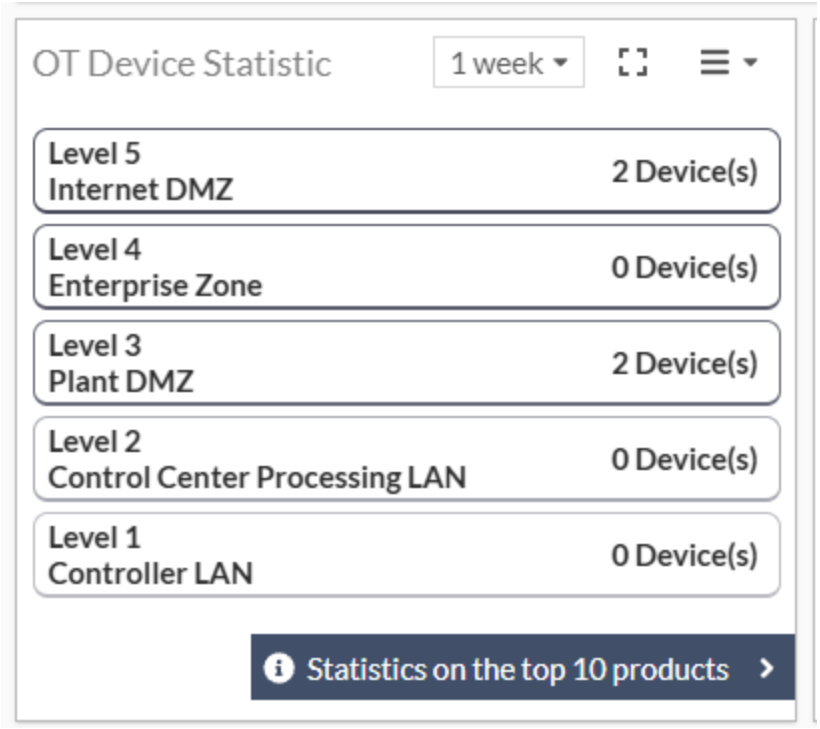


To show more hidden columns in the table, hover over the gear icon and click Configure Table to display the available columns.



OT Device Widget

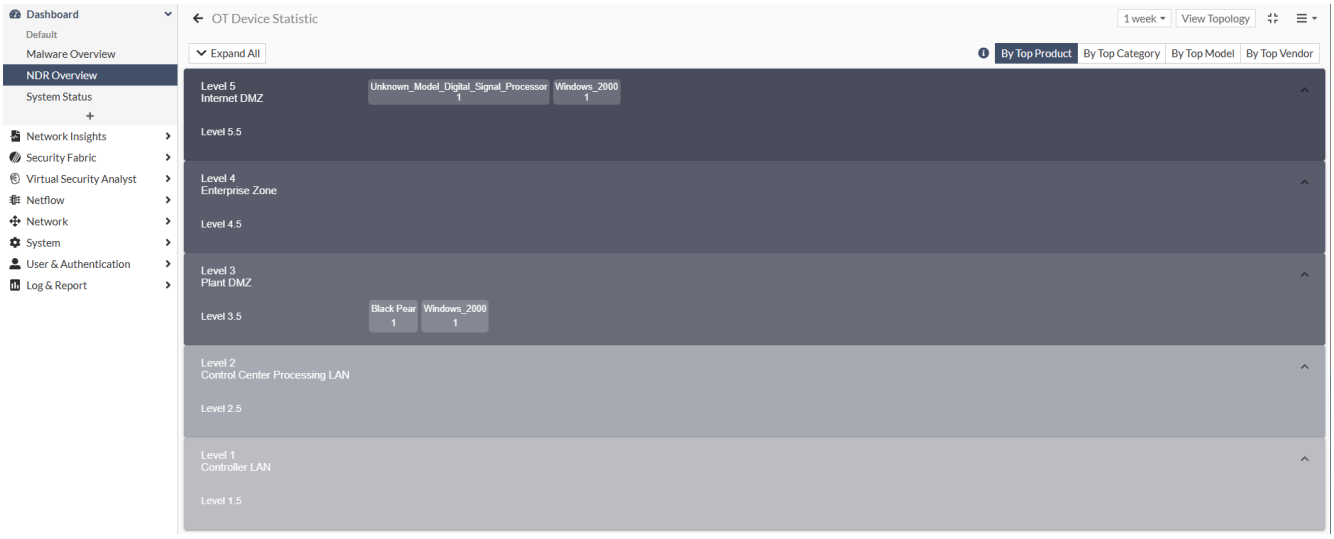
You can track the number of OT devices from different Purdue Levels with the OT device Widget.



The expanded view of the *OT device Statistic* widget shows the Top 10 device by:

- Product (Name)
- Category
- Model
- Vendor

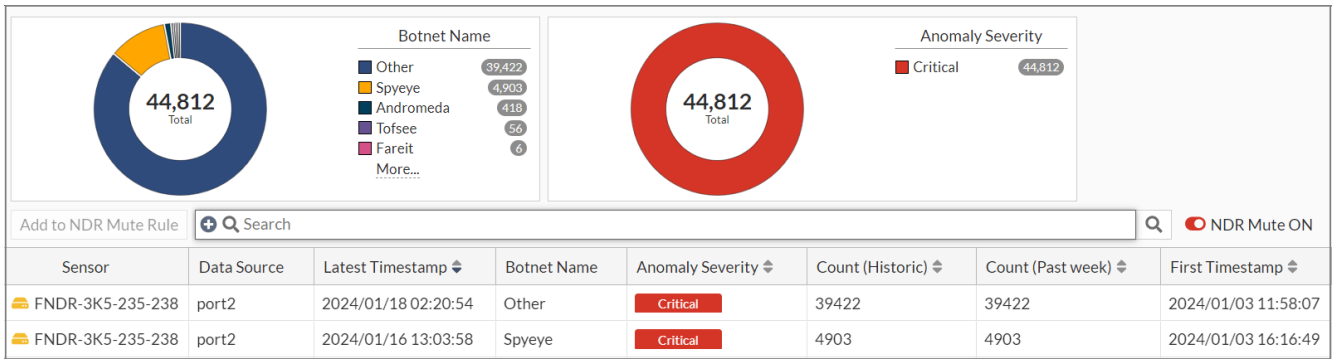
The number in each block below the text indicates the number of devices.



For example, on level 3, there is 1 Black Pear Device that belongs to the Level 3.5 Purdue level(Plant DMZ) .

Botnet

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



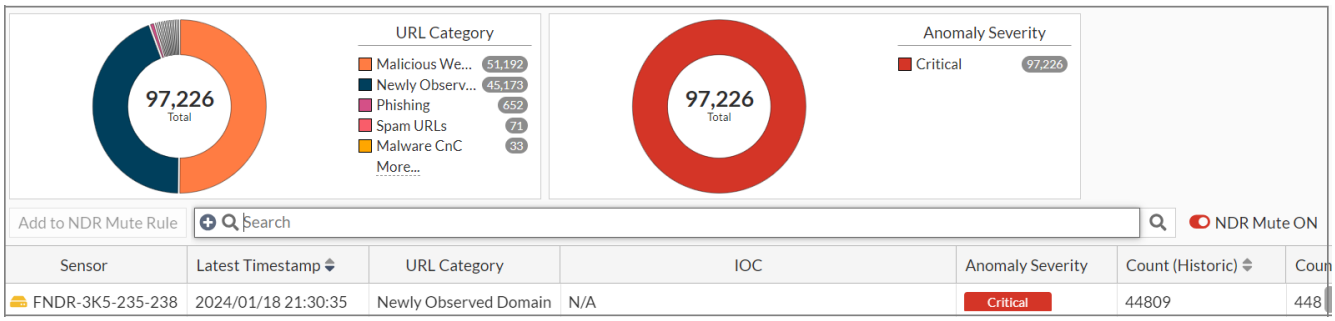
The *Botnet* monitor displays the following information:

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

For information about muting rules, see NDR Muting on page 169.

FortiGuard IOC

Network Insights > *FortiGuard IOC* detections are suspicious URLs and IPs that are flagged by FortiGuard. This event 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).

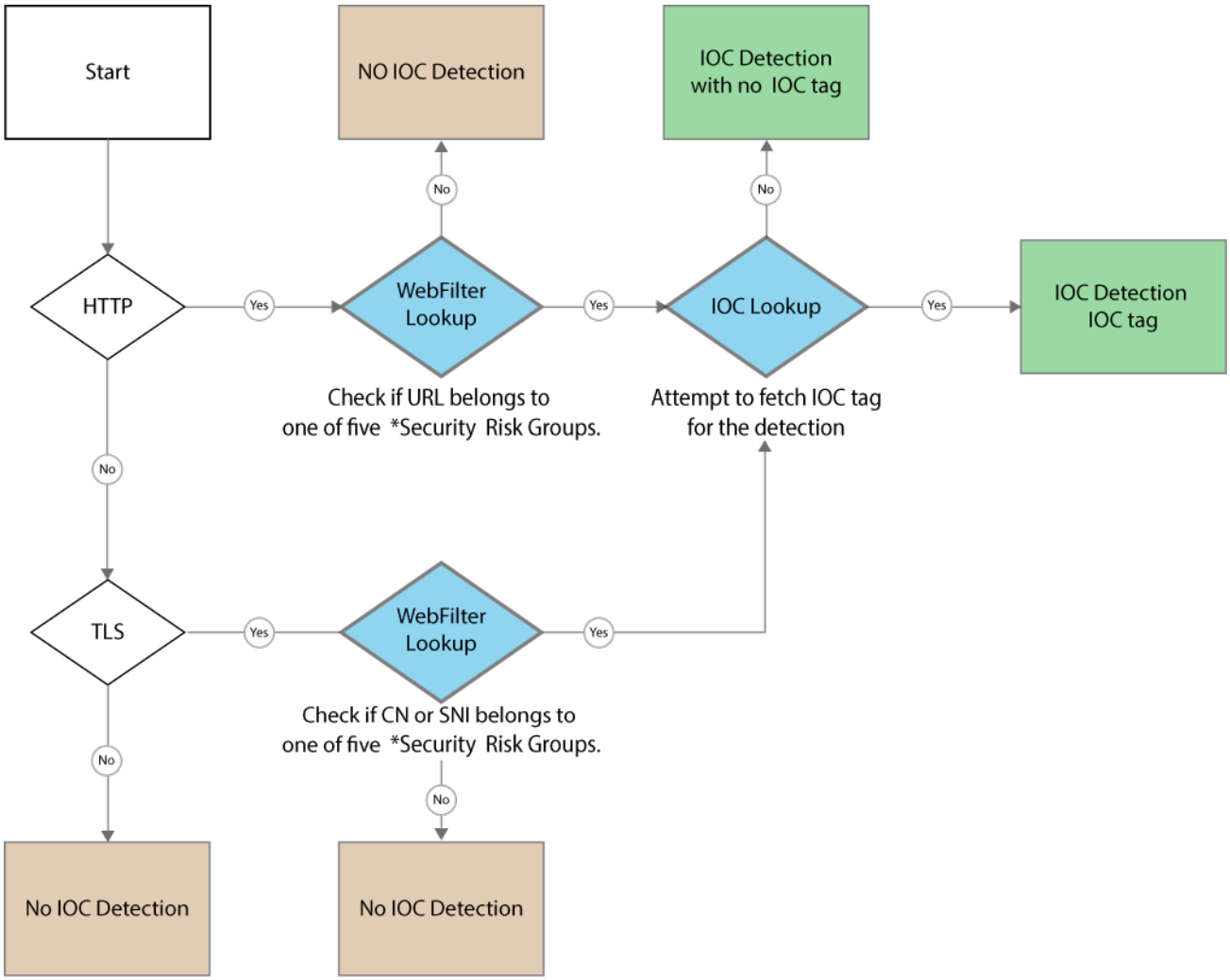


The *FortiGuard IOC* monitor displays the following information:

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

For information about muting rules, see NDR Muting on page 169.

The following topology illustrates how HTTP and TLS traffic is analyzed using WebFilter and IOC lookups to detect potential security threats.

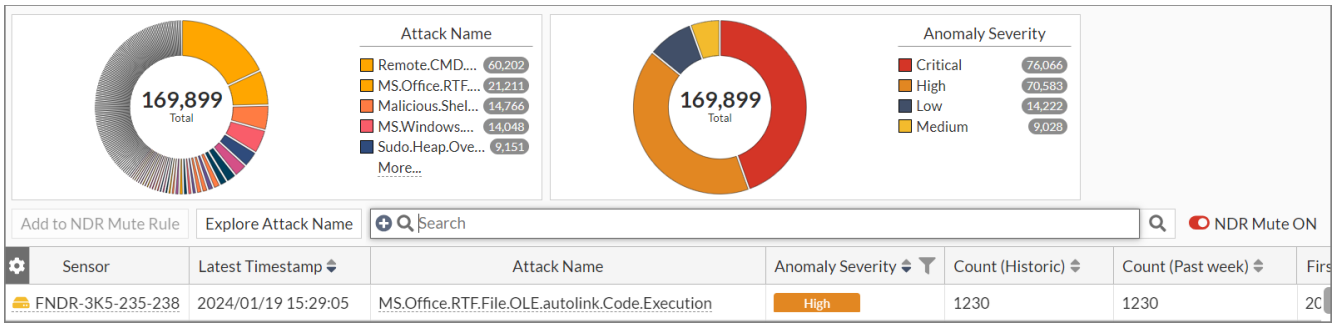


***Security Risk Groups**: Newly Observed Domain, Newly Registered Domain, Dynamic DNS, Spam URLs and Phishing

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.

In addition to the built-in IPS database, FortiNDR also supports custom IPS signatures, allowing users to define and detect specific network-based threats. For information, see Appendix J: Custom IPS signatures on page 308



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.
Severity	The event severity (*Not Observation*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the event was observed.
Count (Past week)	The total number of times the event was observed during the past week .
First Timestamp	The timestamp for the first time the event 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.

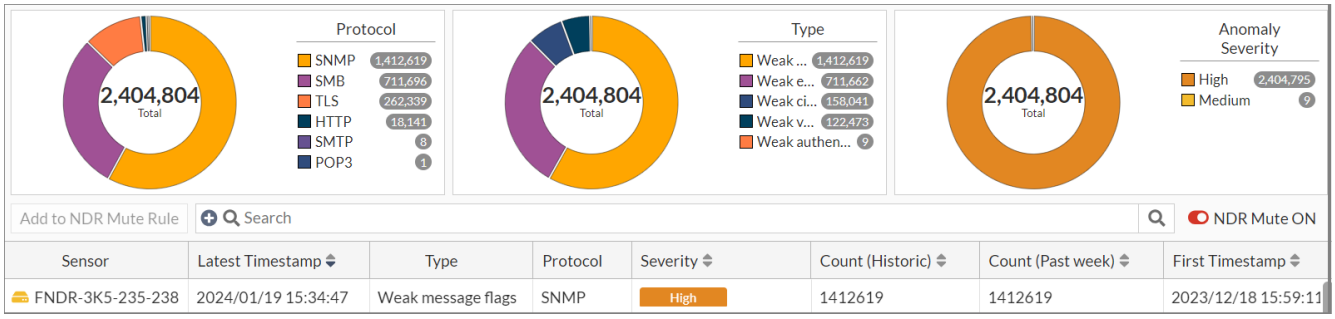
For information about muting rules, see NDR Muting on page 169.

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.

FortiNDR supports detection of weak cipher with the following protocols:

- TLS
- FTP
- HTTP
- IRC
- POP3
- RTSP
- SMB
- SMTP
- IMAP
- SSH
- RDP
- DNS
- SNMP
- MySQL
- MSSQL
- PostgreSQL
- SIP



The *Weak/Vulnerable Communication* 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*.
Latest Timestamp	The date record was updated.
Type	

Communication type	Description
Weak record version	Weak TLS record layer version.
Weak version	Weak TLS handshake version.
Weak support version	Weak TLS handshake extension supported version.
Weak cipher	Weak TLS handshake cipher suite.
Weak security mode	SMB protocol uses level security mode.
Weak extended security	SMB protocol uses outdated extended security negotiation option.

Communication type	Description
Weak dialect	SMB uses outdated dialect version.
Weak encryption	SMB or SSH uses risky encryption algorithm. For example, SMB protocol with encryption disabled.
Weak authentication	Email protocols are using risky authentication methods. For example, POP3 uses authentication cram-md5, Postgres uses MD5 password as authentication type.
Weak server	HTTP or RTSP server version is outdated.
Weak method	HTTP, SIP or RTSP protocol uses weak request method. For example, HTTP protocol uses DELETE as request method.
Weak banner	Weak or outdated email server version. For example, Outdated Cyrus IMAP server
Weak encrypt algo server client	Weak encryption option is used in SSH, such as rc4, rc3, rc2.
Weak capability	IMAP or POP3 capability command uses option AUTH=PLAIN.
Weak security	SMB protocol uses low level security mode.
Weak encrypt method	RDP protocol uses low level encryption methods such as ENCRYPTION_METHOD_40BIT.
Weak encrypt level	RDP protocol uses low encryption level such as ENCRYPTION_LEVEL_NONE
Weak msg flags	SNMP protocol uses risky flags such as 0x00-02, 0x04-06 and 0x08-ff.
Weak server version	MYSQL, TDS, Posgres or SIP server version is outdated.
Weak auth algo	POP3, SMTP or IMAP authentication method option is too risky. For example, POP3 uses PLAIN authentication option.
Weak protocol version	MYSQL protocol version outdated.
Weak encrypt	TDS encryption option is disabled.
Weak fedauth	TDS protocol disables `FedAuthRequired` option.
Protocol	The communication protocol.
Severity	The event severity (*Low*, *Medium*, *High* or *Critical*).

Count (Historic)	The total number of times the event was observed.
Count (Past week)	The total number of times the event was observed during the past week .
First Timestamp	The date the record was created.

General tab

The *General* tab displays the following information:

General	• Event Type • Severity • Reason
Additional Information	• HTTP Version • HTTP Response Code • HTTP Server Name • HTTP URL • Malicious Behavior
Last 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 event was observed.
Count (Past week)	The total number of times the event was observed during the past week .

To view the source and destination devices:

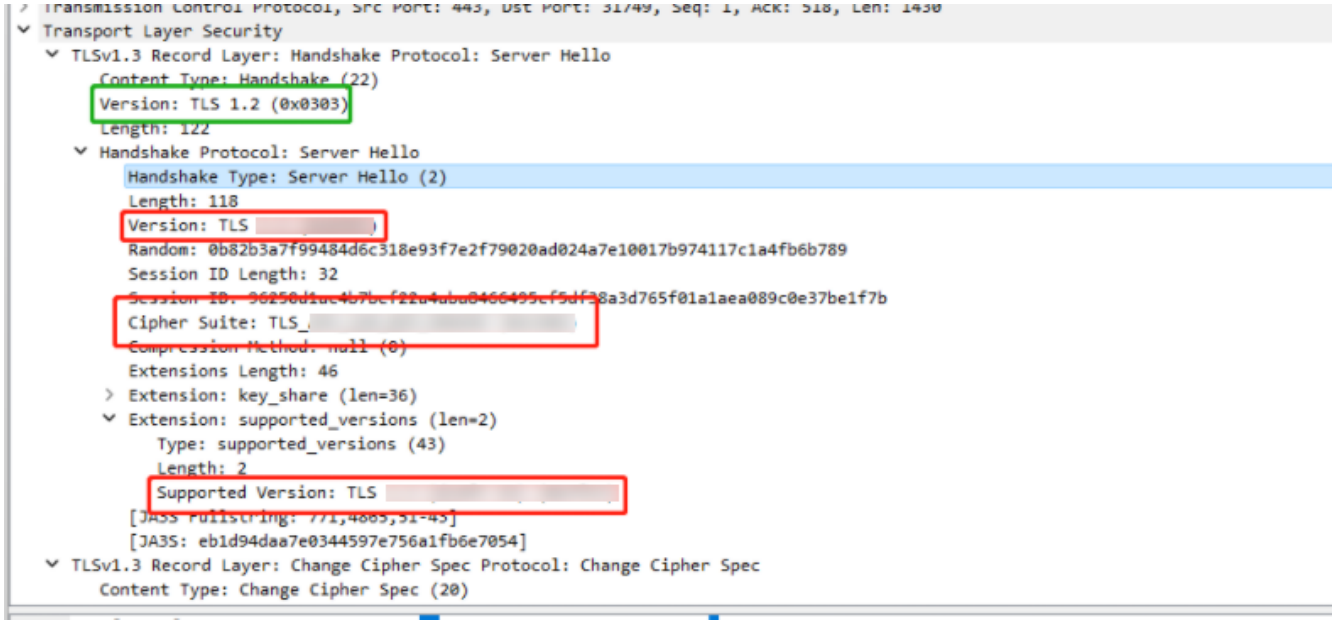
- Select a record in the table and click *View Device* > *View Source Device*, or *View Destination Device*.

To view the session logs for a condition:

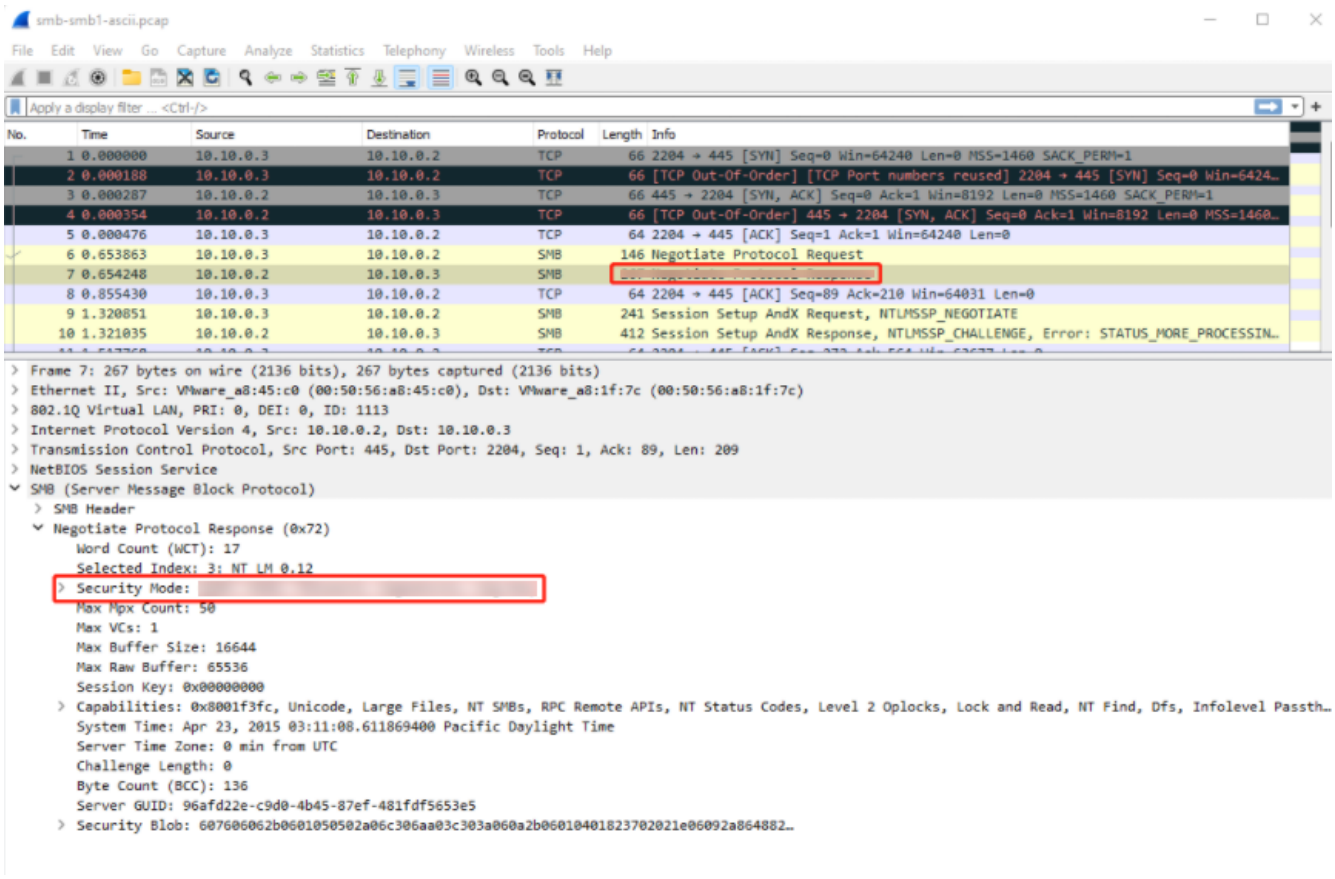
- Double-click a record in the *Information* pane. The *Sessions Log for selected condition* pane opens.

Examples

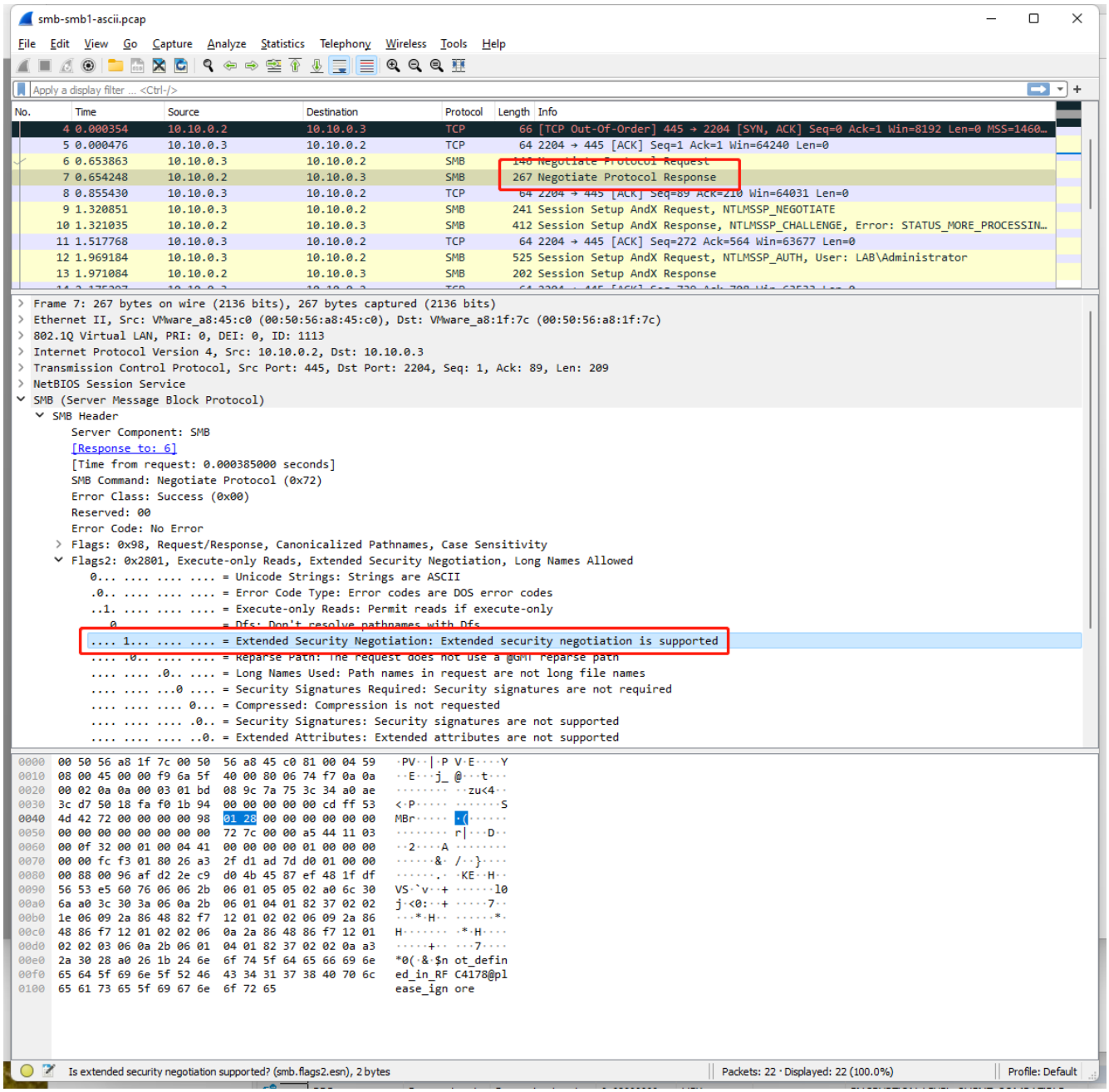
Wireshark pcap



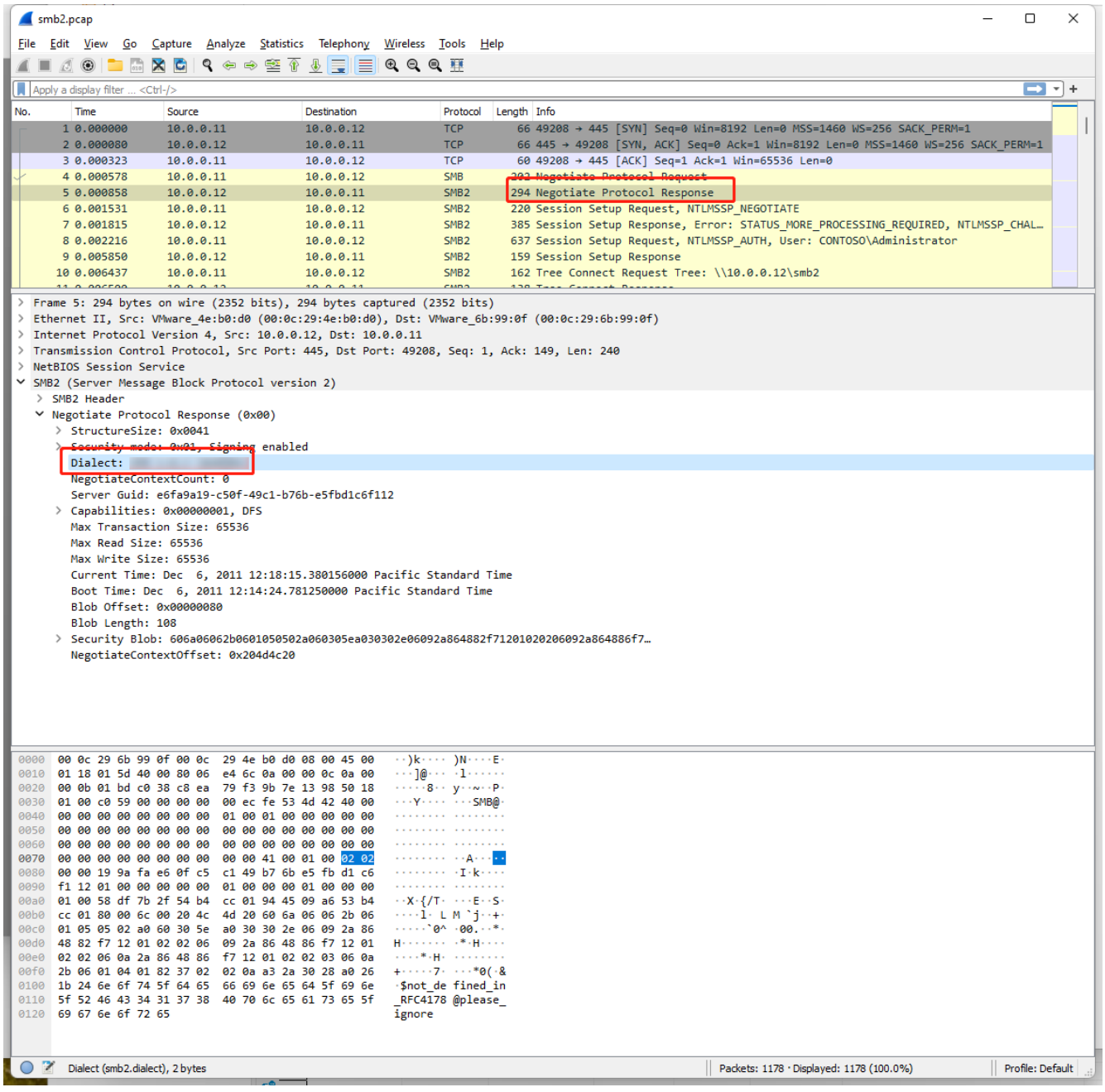
Weak security mode



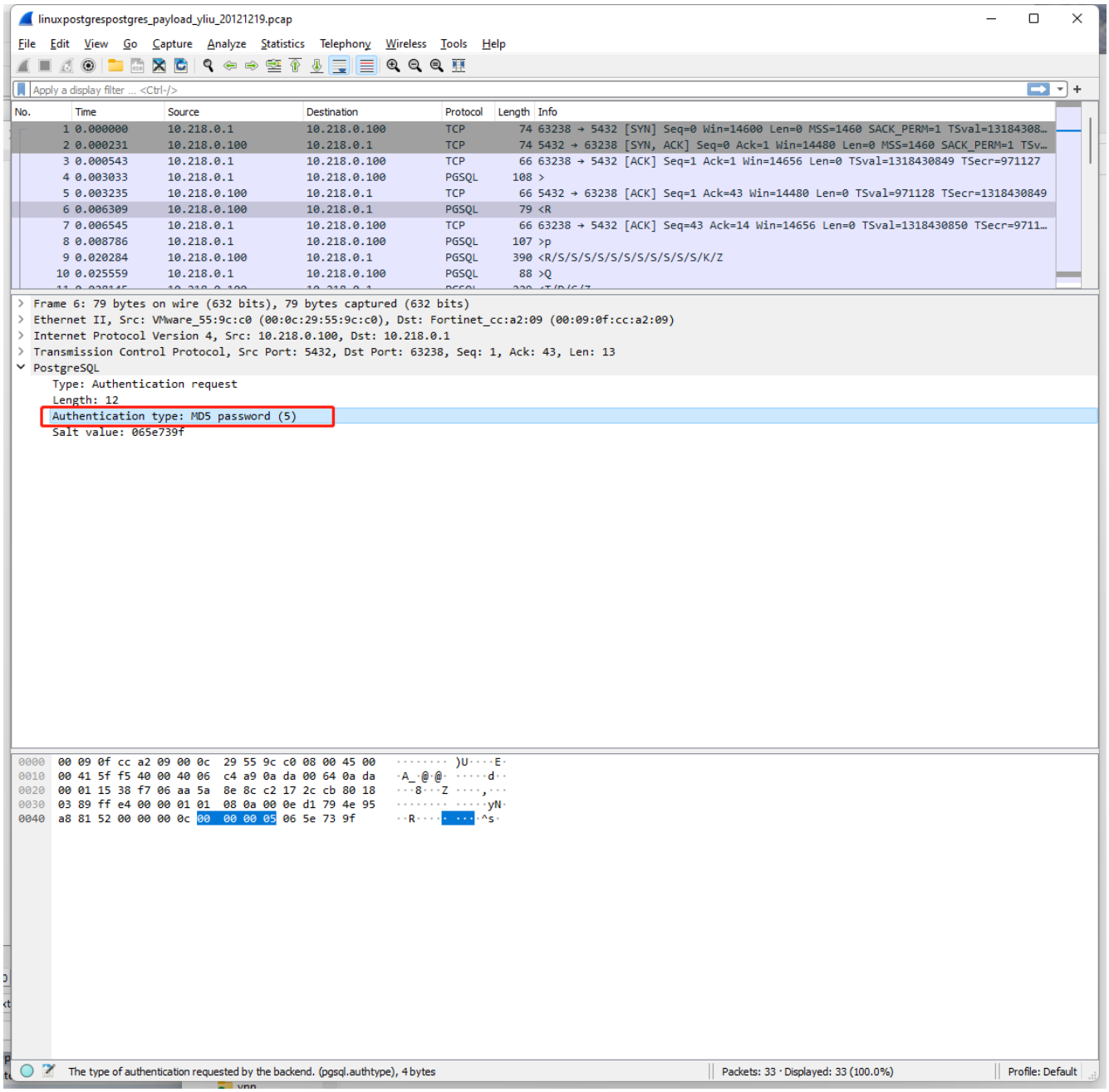
Weak extended security



Weak dialect

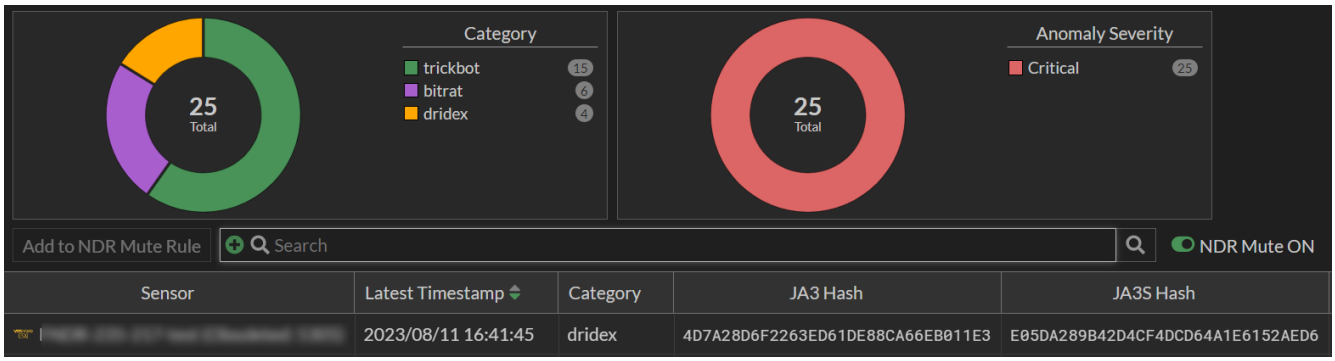


Weak authentication



Encrypted Attack

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



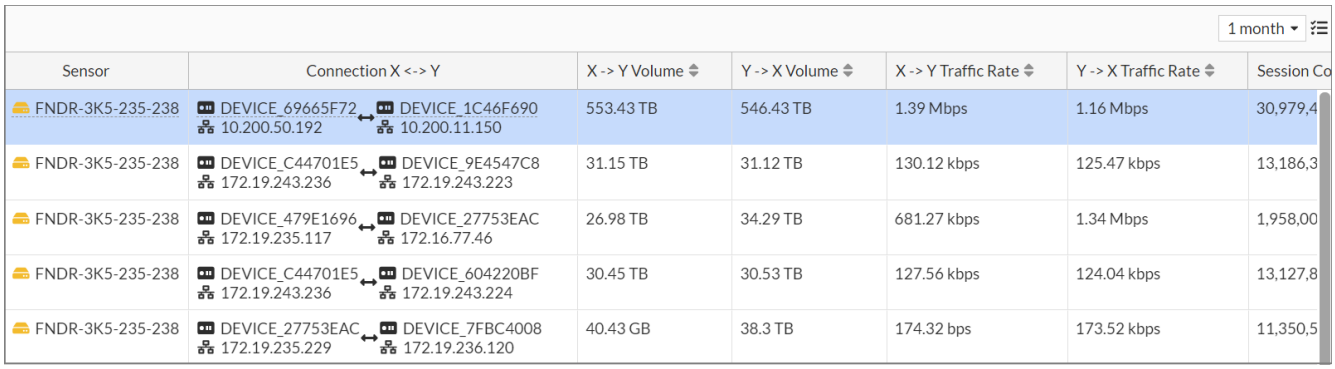
The *Encrypted Attack* monitor displays the following information:

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 *Server*.
Severity	The event severity (*Not Observation*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the event was observed.
Count (Past week)	The total number of times the event was observed during the past week .
First Timestamp	The timestamp for the first time the event was detected.

For information about muting rules, see NDR Muting on page 169.

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.



The *Top Talker* page displays the following information:

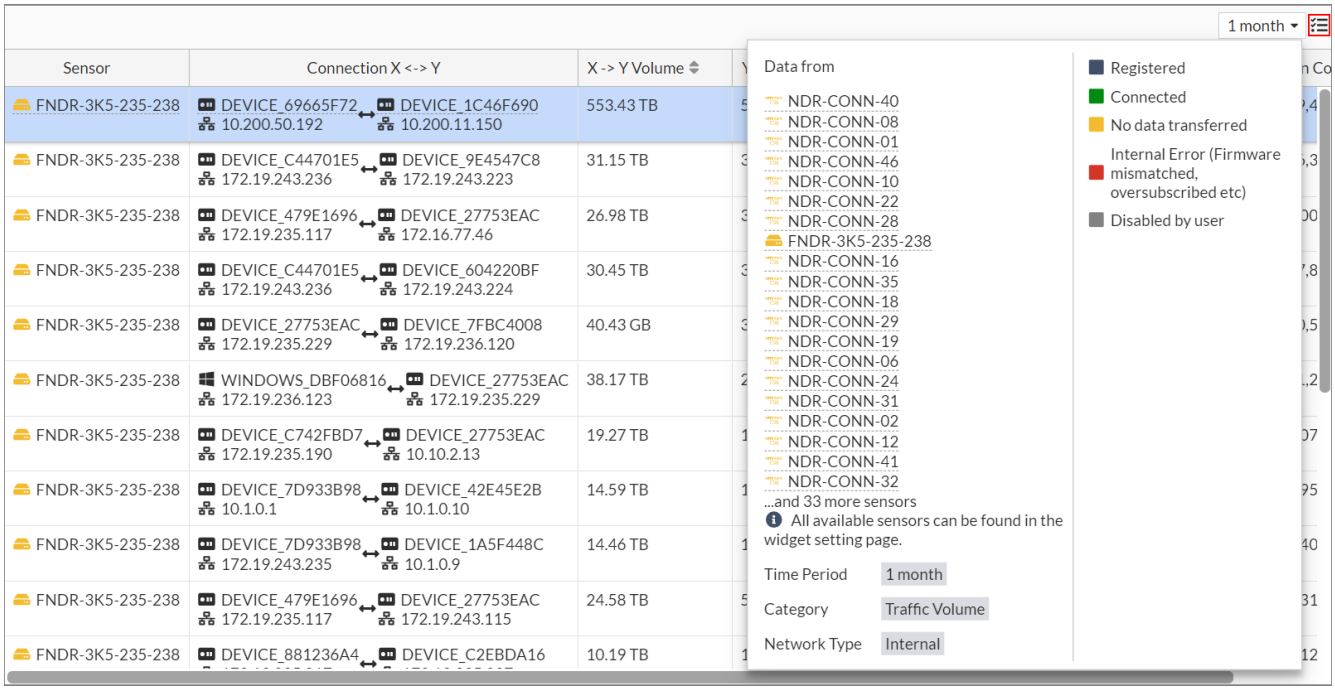
Sensor (Center mode)	The network sensor. Hover over the sensors ID to view the *IP Address*, Serial number (*S/N*), *Last Sync Time* and *Status*.
Connection X <-> Y	The source and destination device IPs. Hover over the IP address to view the *Device* ID, *MAC Address*, *IP Address*, *Hardware*, and *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*.

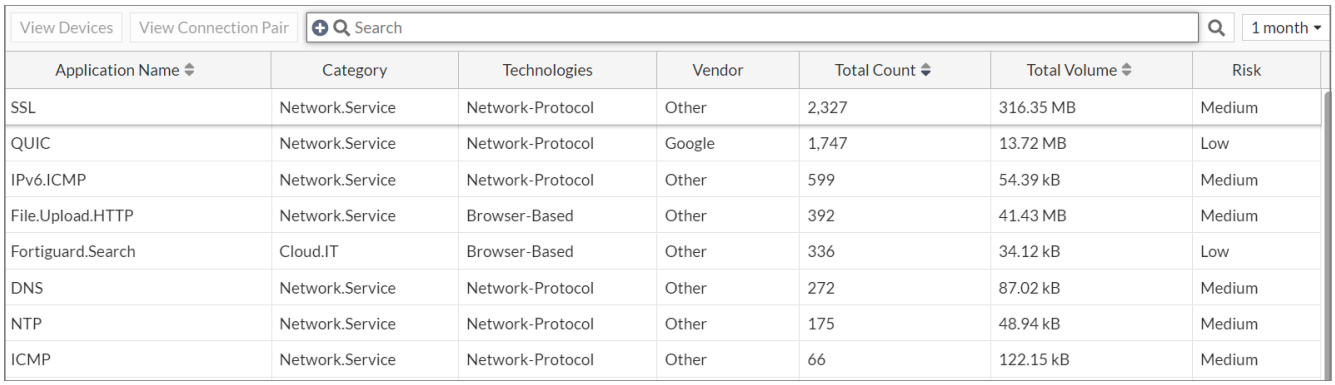
To view the sensor statistics:

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



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*).



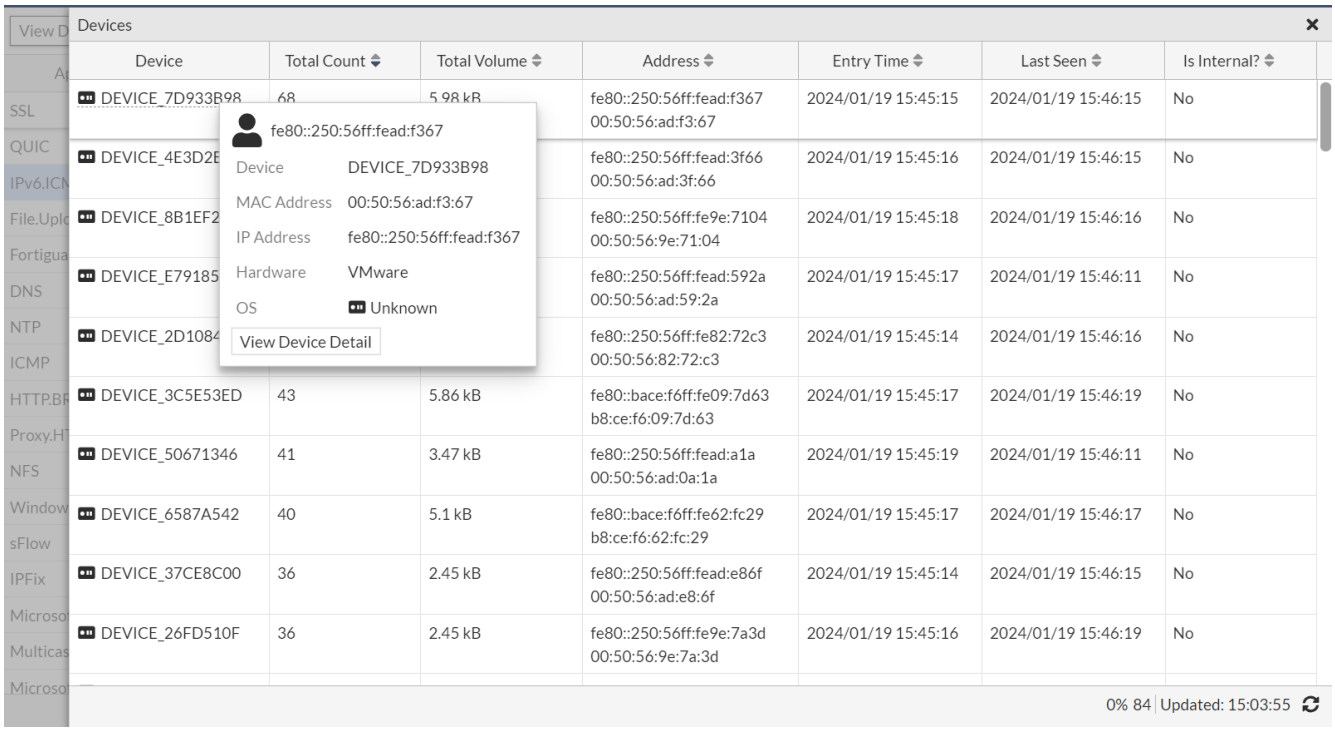
Application Name	Category	Technologies	Vendor	Total Count	Total Volume	Risk
SSL	Network.Service	Network-Protocol	Other	2,327	316.35 MB	Medium
QUIC	Network.Service	Network-Protocol	Google	1,747	13.72 MB	Low
IPv6.ICMP	Network.Service	Network-Protocol	Other	599	54.39 kB	Medium
File.Upload.HTTP	Network.Service	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 IPS (including OT), Application Control, and protocols on page 303.
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*)

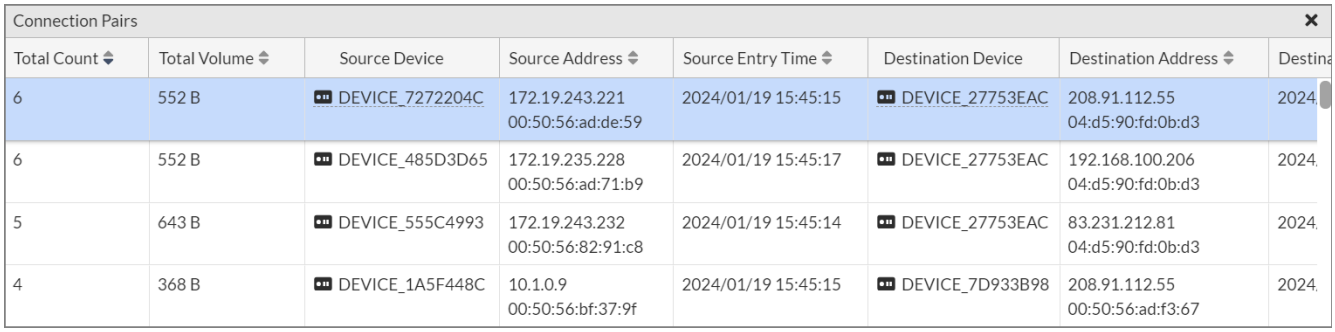
To view devices:

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.



To view connection pairs:

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



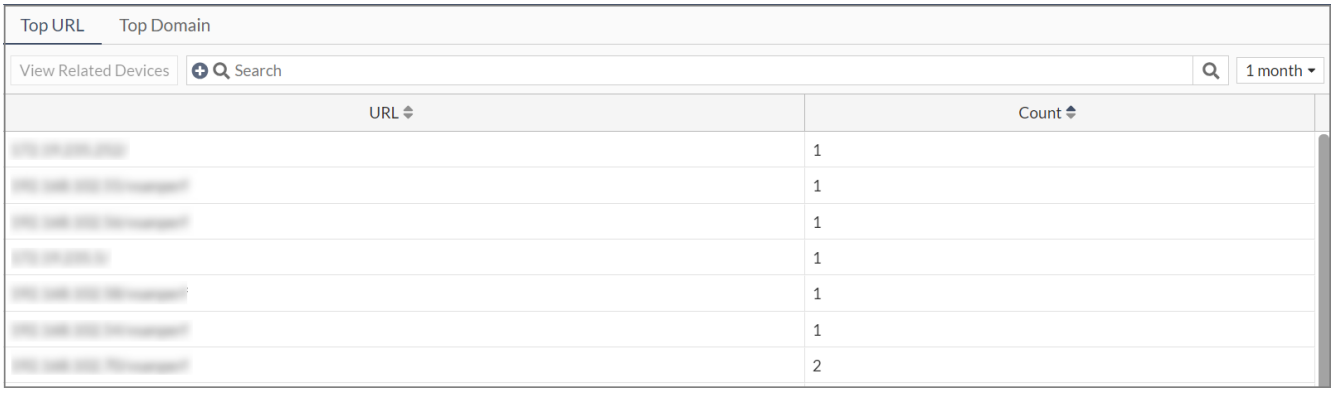
Top URL/Domain

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*).

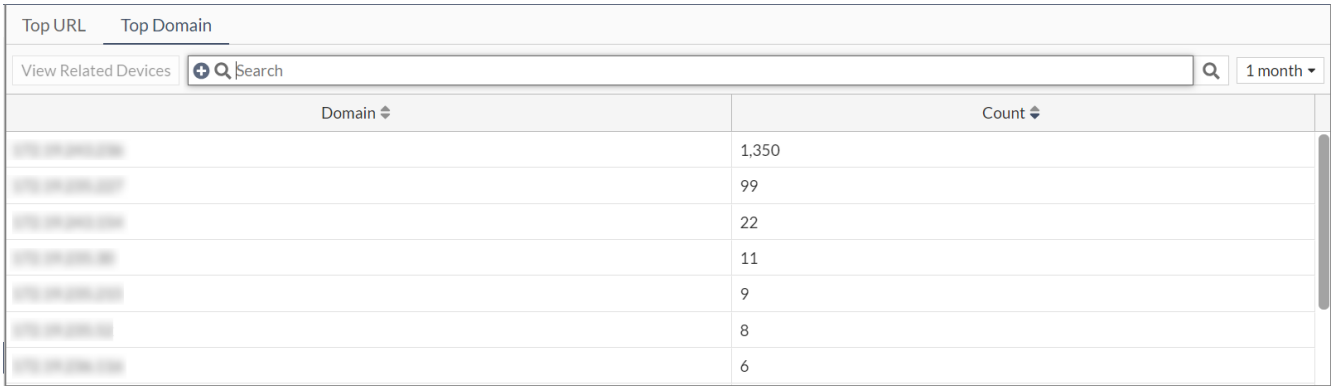
The *Top URL / Domain* page displays following information:

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.



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

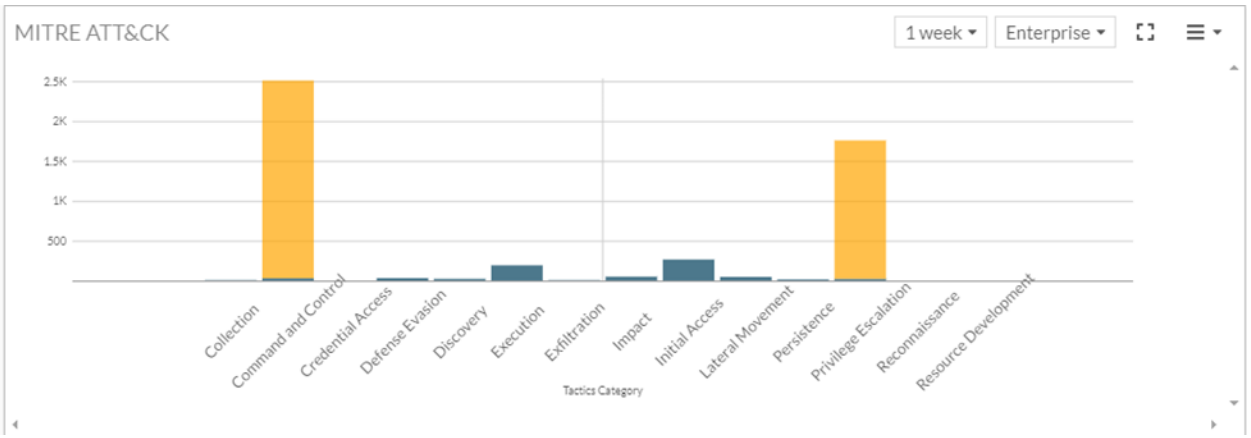


MITRE ATT&CK

MITRE ATT&CK is a knowledge base of threat behaviors relied upon by security professionals worldwide. FortiNDR provides a matrix view to display detection for enterprise domain and ICS domain with extensive mapping to TTPs and recommended remediation actions.

Mitre ATT&CK widget

The *Mitre ATT&CK* widget is located in the *NDR Overview* dashboard (go to *Dashboard* > *NDR Overview*). This widget displays the detection statistics, including the number of sessions and malware detected based on different tactics over the selected period within the enterprise domain or ICS domain. When *Enterprise* is selected, detection covered by botnet or IPS appears as a dark blue bar. A yellow bar indicates the detection is covered by ANN engine.



Mitre ATT&CK Matrix

The *Network Insights* > *MITRE ATT&CK* page tracks the detection events that occurred for each MITRE attack tactics category with different domain.

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

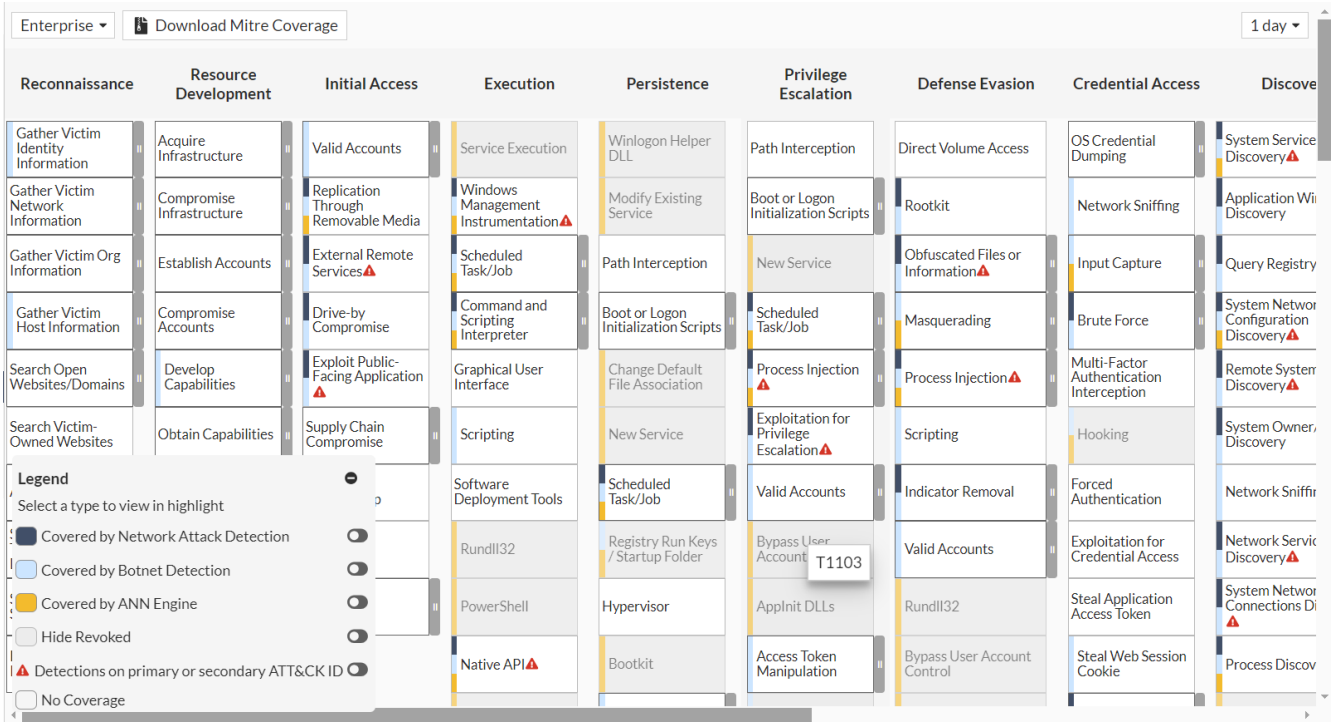
- The Primary technique is what is used to detect the behavior.
- The Secondary technique is not always related to what is seen on the network, but is related to the threat in general. The secondary technique will not be displayed in some instances.

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 is indicated with a colored bar at the left side of the tile.

Enterprise domains

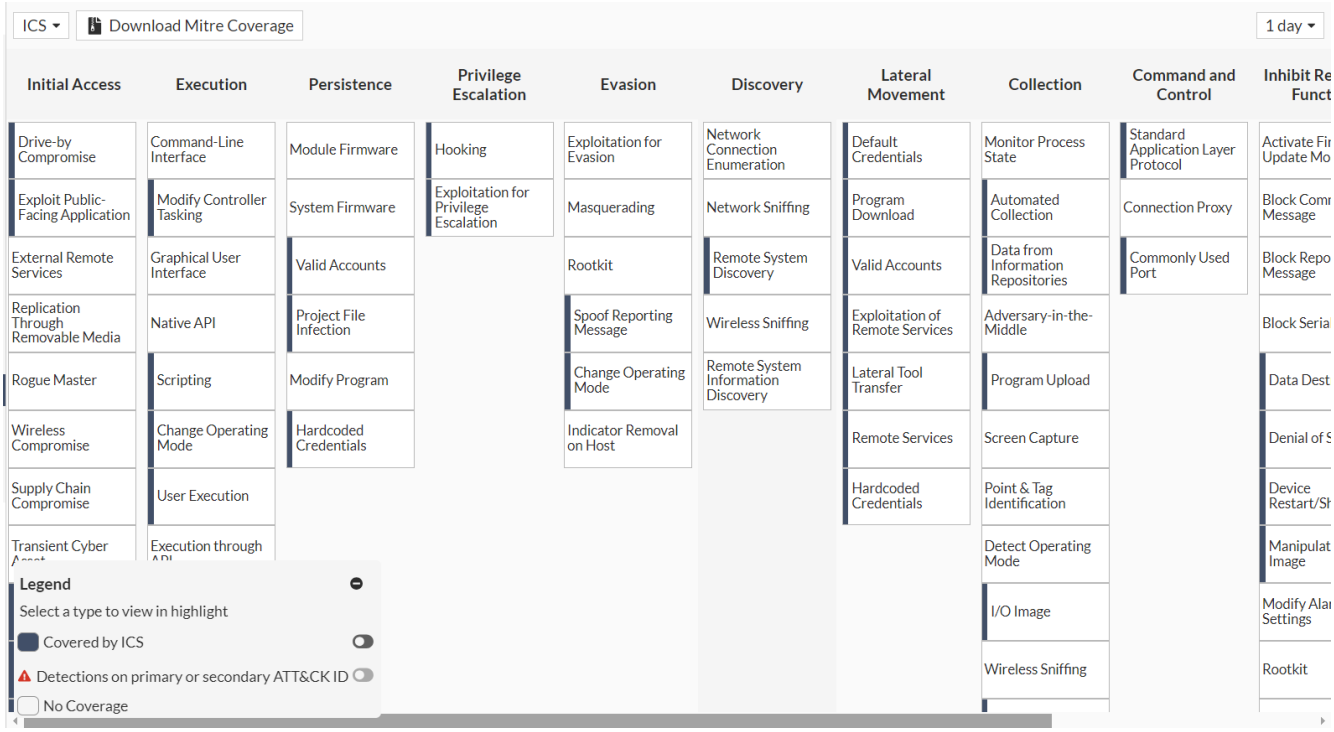
The matrix displays detections in the enterprise domain by default. When *Enterprise* is selected, a dark blue bar indicates the technique is covered by network attack detection, a light blue bar indicates it is covered by botnet detection and a yellow bar indicates it is covered by ANN engine. A gray bar is used to identify an obsolete technique. 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.

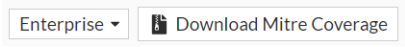


ICS domains

To view detections in ICS domains, click the dropdown at the left side of the banner and select *ICS*. The MITRE ATT&CK techniques with FortiNDR ICS coverage appears with a dark blue bar at the left side of the border

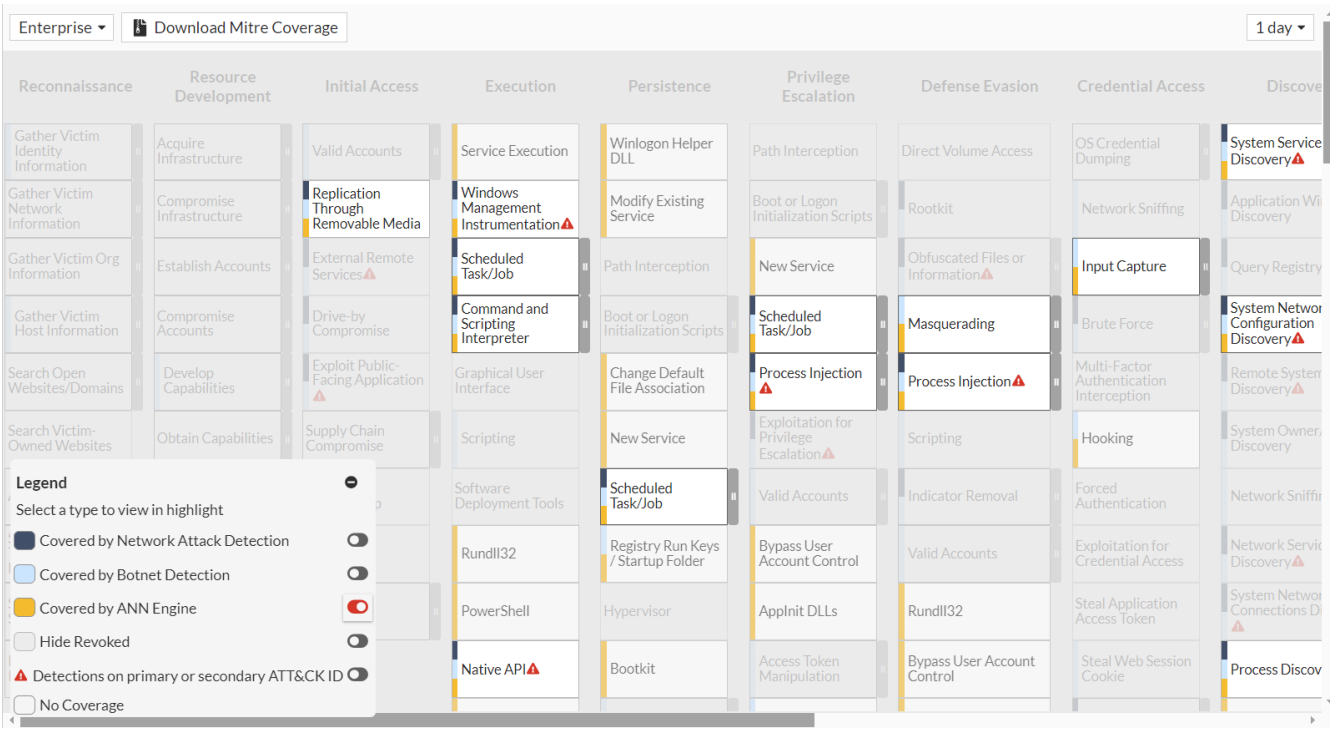


To download the matrix as a CSV file, in *Enterprise* or *IS* views, click *Download Mitre Coverage*.



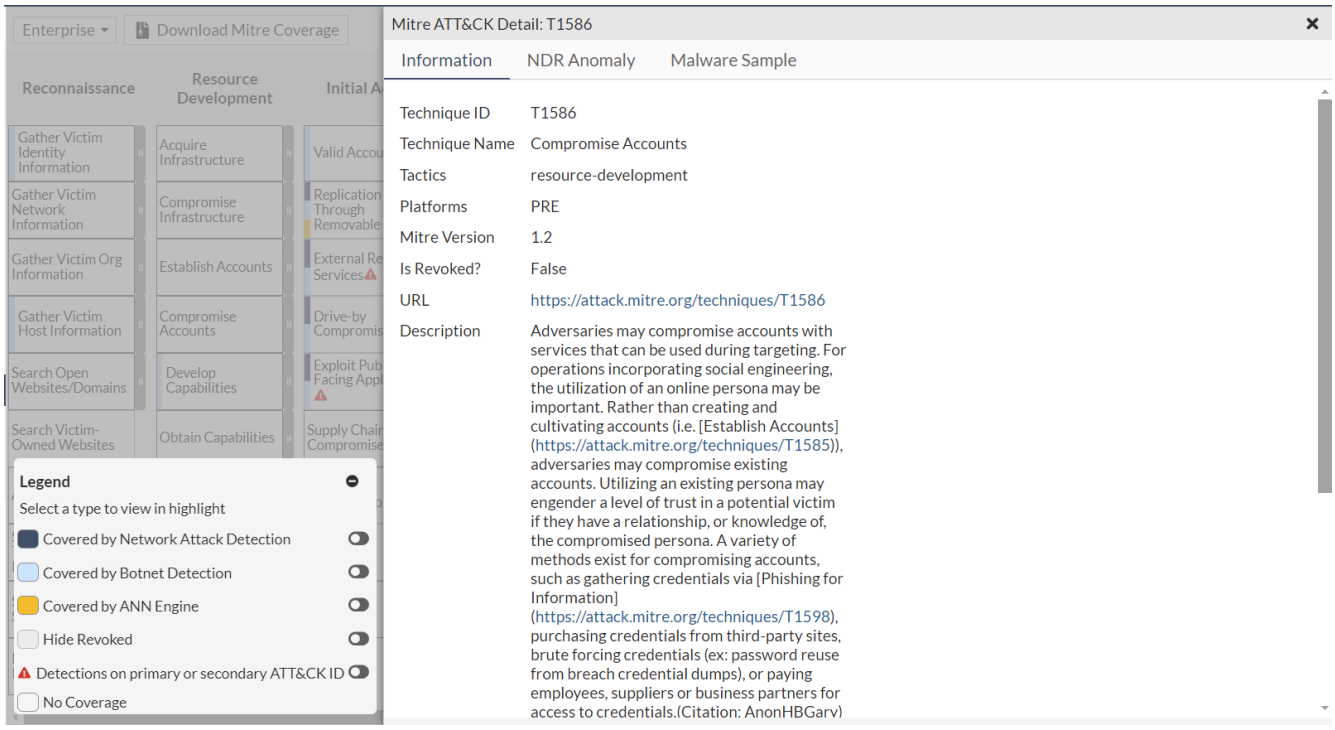
Filtering the matrix

Use the toggles in the legend to filter the matrix by coverage. Techniques that match the coverage will be highlighted in the matrix. Click the minimize icon at the top right of the legend to hide the legend.

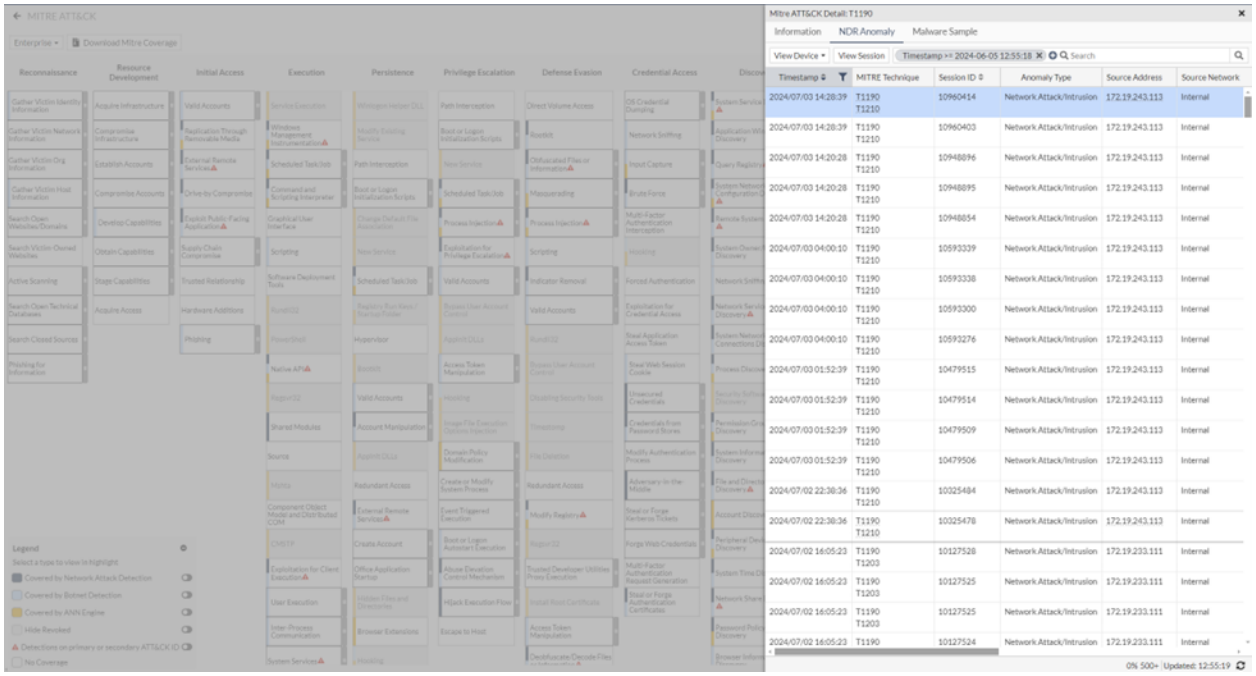


Mitre ATT&CK detail

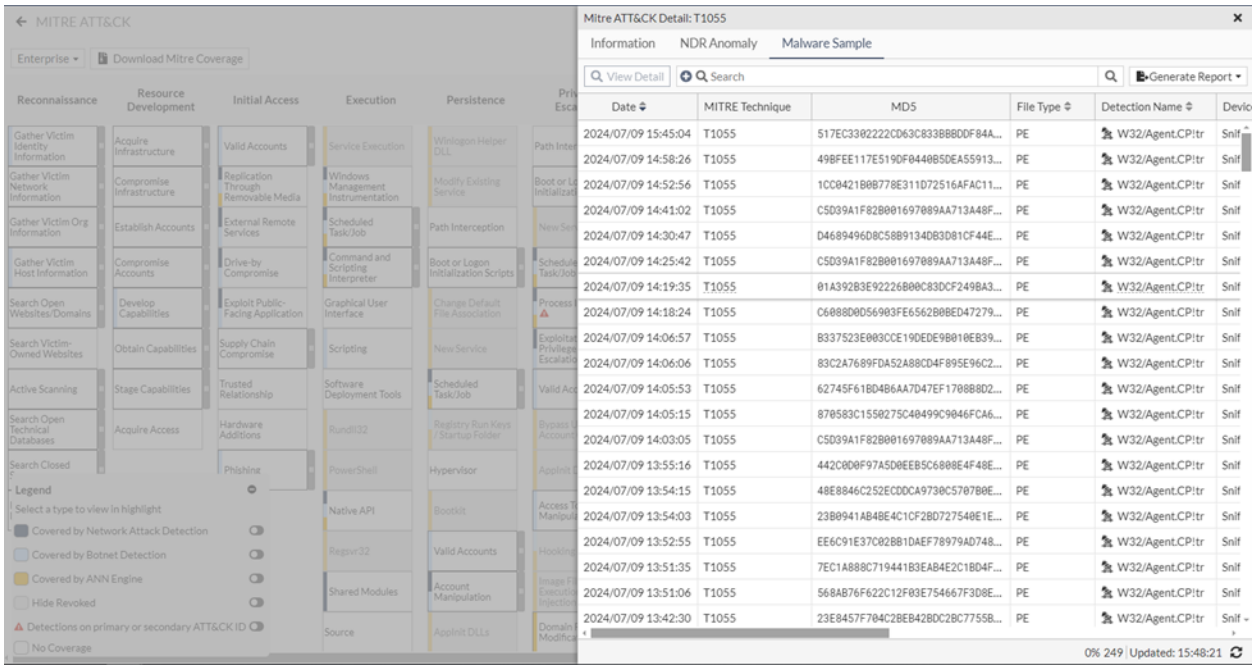
Click a tile in the column to view Information about the technique:



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

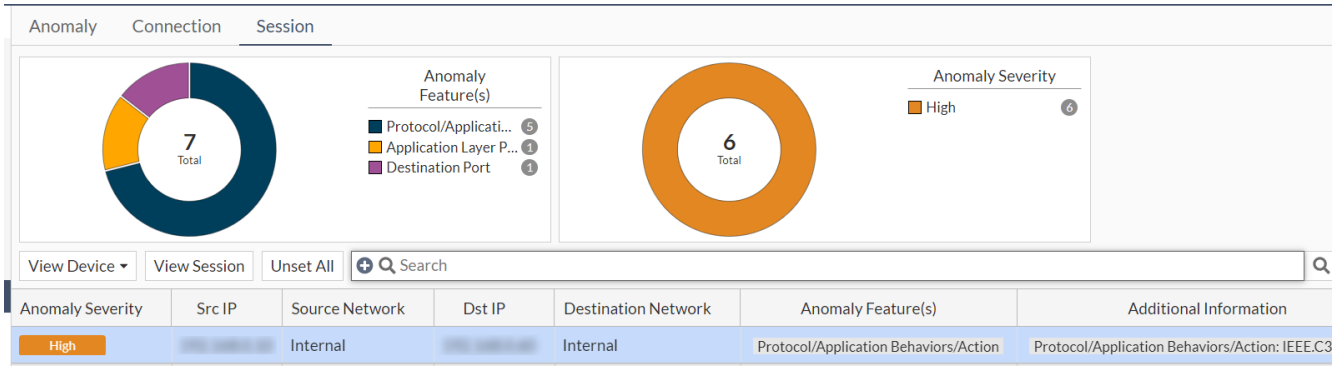


Click the *Malware Sample* tab to view all the sample files associated with the selected technique.



ML Discovery (Center and Standalone)

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



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

Column	Description
Latest Timestamp	The date the record was updated.
Observation Features	The feature or feature combinations that caused the observation.
Additional Information	The abnormal feature value(s).

Column	Description
Observation Severity	The event severity (*Not Observation*, *Info*, *Low*, *Medium*, *High* or *Critical*).
Count (Historic)	The total number of times the event was observed.
Count (Past week)	The total number of times the event was observed during the past week .
First Timestamp	The timestamp for the first time the event 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 169.

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
Type	• Observation or Detection 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.

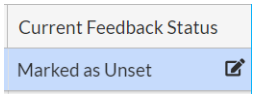
To view the Current Feedback Status column:

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.



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

Option	Description
Mark as Observation	Select this option to mark an entry as an NDR Detection or Observation. This option can be used to undo the *Mark as Not Observation* option. This option updates the baseline without triggering baseline re-training.
Mark as No Observation	Select this option to exclude the same detection(s) in the future. This typically takes 5 - 10 minutes depending on the network traffic. This option updates the baseline without triggering baseline re-training. For information about retraining the database, see ML Configuration > Retrain database.
Mark as unset	This is the default status for any ML events detected. Select this option to unset your feedback. This has the same effect as *Mark as Observation*.

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

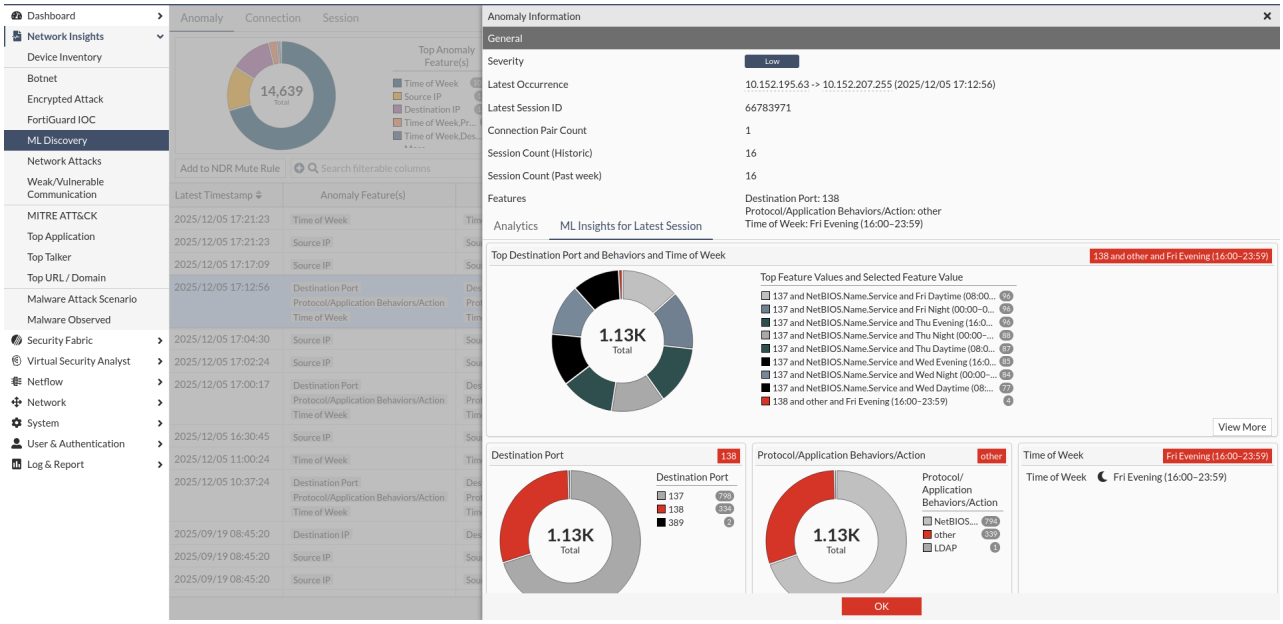
4. Click *Apply*.

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

Viewing ML insights for latest session

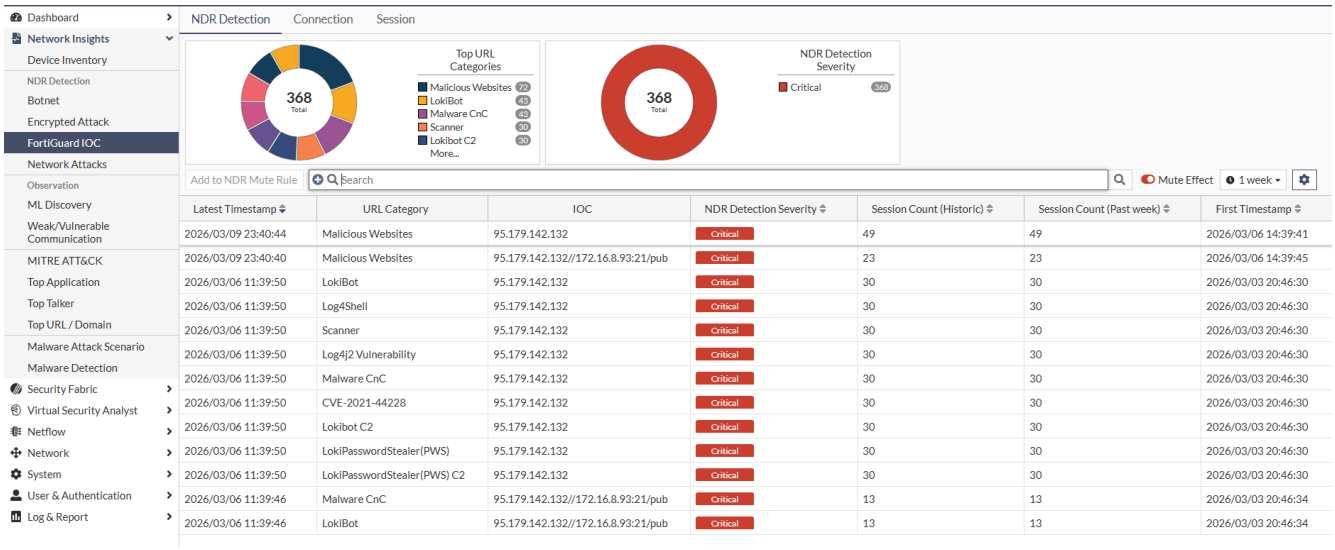
To view the ML insights:

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



NDR Detection tab

The *NDR Detection* tab provides an overview of all detected network threats, combining visual summaries with detailed event listings to show the scale and nature of suspicious activity. This view highlights which malicious categories are most active, how frequently sessions associated with each threat have occurred, and when activity was first and most recently detected. The Detections tab is available in the *Botnet*, *Encrypted Attack*, *FortiGuard IOC*, and *Network Attacks* pages.



Detection monitors

The detection monitors provide a high-level summary of threat activity using visual indicators. These monitors help you understand detection patterns, severity distribution, and key attributes associated with the selected category.

The first monitor (or set of monitors) depends on the type of detection you are viewing. For example, you may see monitors for URL categories, botnet names, attack categories, or other IOC-specific attributes. These monitors highlight the most common detection attributes and help you identify which threat patterns occur most frequently.

The *NDR Detection Severity* monitor is persistent across all detection types. It shows the overall severity distribution for all detections and indicates the total number of detection events. This monitor also highlights whether any lower-severity events are present, providing an overview of risk impact regardless of the category.

Detections table

The detections table shows how each detection has behaved over time, helping you understand its impact, recognize patterns, prioritize issues, and see whether activity is increasing or decreasing.

The table lists all detection events associated with the selected category. It provides a structured view of each event, allowing you to review detection details, compare entries, and drill down into specific activity as needed.

Additional columns appear in the detections table depending on the detection type. For example, you may see fields such as *URL Category* for web-based detections, *Botnet Name* for botnet-related detections, or *Attack Name* for network attacks, along with any other IOC-specific attributes generated by the detection .

Detections toolbar

Add to NDR Mute Rule	Hide events that are not relevant to your network. These detections will no longer be visible in insight pages and prevents related alerts and enforcement actions. See, NDR Muting on page 169.
Explore Attack Name	Displays the attack name and description. Click the *Search FortiGuard* button for more information in FortiGuard Labs. This option only appears in *Network Attacks*.
Search	Enter search terms or click the plus symbol (**+**)to filter the columns.
Mute Effect	Displays events when NDR muting is enabled. See, NDR Muting on page 169.
Time range	Set the time range from 30 minutes to 1 month.
Persist Table Settings	Click the gear icon at the right-side of the toolbar to retain their selections after navigating away from the page. **Persist Table Column Selection** — Retain selected column selected for display. **Persist Table Column Filter Selection** — Retain column filter applied. **Persist Table Time Window Selection** — Retain timeframe selection.

General tab

The *General* tab provides a detailed snapshot of the detection, including the type of vulnerability, severity, associated MITRE techniques, and the specific source and destination device attributes observed during the latest occurrence.

Field	Desription
NDR Detection or Observation Type	This indicates the type of security issue detected.
Type	Specifies the subtype of the issue detected.
Severity	The risk rating assigned to the detection.
Latest Occurrence	The most recent date and time when this issue was observed on the network.
Mitre Detected	Lists the MITRE ATT&CK techniques associated with the detection.
Last NDR Detection or Observation Occurrence Source Device	
Source IP	The IP address of the device that initiated the network traffic related to the detection.

Field	Desription
Source Network	Indicates the network classification of the source device.
Source Port	The network port number used by the source device when sending the traffic.
Source Packet Size	The size, in bytes, of the packet sent by the source device.
Source Country	The geographical country associated with the source IP.
Source MAC	The hardware MAC address of the source device.
Source Device Model	Identifies the type of hardware or environment of the source device.
Source OS	The operating system running on the source device.
Source Device Category	The general category of the device.
Source Device Sub Category	A detailed classification of the device.
Last NDR Detection or Observation Occurrence Destination Device	
Destination IP	The IP address of the device receiving the traffic related to the detection.
Destination Network	Indicates the network classification of the destination device.
Destination Port	The network port number on the destination device that received the traffic.
Destination Packet Size	The size, in bytes, of the packet received by the destination device.

Analytic tab

The *Analytics* tab summarizes all connection pairs that share the same observation, helping to show where the vulnerable protocol is being used across the environment.

Column	Description
Connection Pair	Shows the two endpoints involved in a network communication flow.
Source IP	Identifies the address of the device that initiated the connection.
Source Network	Indicates whether the originating device is on an internal or external network.
Destination IP	Identifies the address of the device receiving the connection.
Destination Network	Indicates whether the destination device resides on an internal or external network.

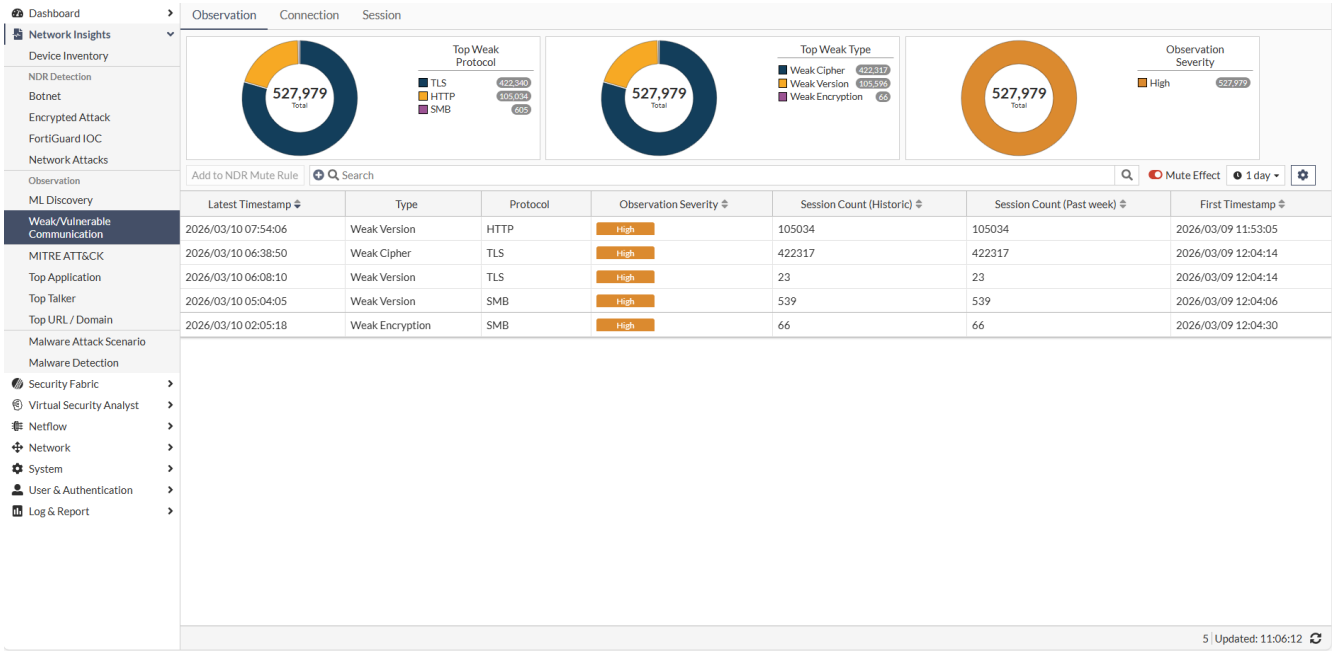
Observation tab

The *Observation* tab provides a summarized view of weakness-related activity detected in network traffic. It highlights insecure protocol usage, weak configurations, and other communication patterns that may require attention. This tab is available in both the *ML Discovery* and *Weak/Vulnerable Communication* pages.

The tab displays:

- The total number of observations for the selected time range
- The most frequently detected weak protocols
- The primary weakness types, such as weak versions, weak ciphers, or weak encryption
- The severity level distribution
- A detailed table showing the latest observation timestamp, weakness type, protocol, severity, and session counts

Use this tab to quickly identify where weak or vulnerable communication is occurring and to monitor trends that may help prioritize remediation.



Observation monitors

The observation monitors provide a high-level summary of weakness-related activity detected in network traffic. These monitors help you understand patterns of weak protocol usage, vulnerability types, and severity across the selected time range.

The first monitor or set of monitors varies depending on the observation data. These monitors highlight the most frequently detected weak protocols and weakness categories, such as weak versions, weak ciphers, or weak encryption. They help you identify common patterns of weak or vulnerable communication within the network.

The Observation Severity monitor is persistent across all observation types. It shows the overall severity distribution for all observations and the number of events that fall under each severity level. This monitor provides an overview of the overall weakness impact, regardless of the protocol or weakness category.

Observation table

The Observations table lists all weakness-related events within the selected time range. The table columns allow you to review the observation type, associated protocol, occurrence timestamps, severity, and activity counts. It serves as the primary workspace for examining observed weak or vulnerable communication.

Additional columns appear depending on the page and observation type:

- *Weak/Vulnerable Communication* examples include fields such as Protocol, Type (weakness category), Latest Timestamp, Severity, and Session Count (historic and past week). The table adjusts automatically to display the fields most relevant to the selected weakness or protocol.
- *ML Discovery* includes feature combinations, Severity, Count (Historic), Count (Past Week), First/Latest Timestamp, and the optional Current Feedback Status for user feedback.

Double-clicking an ML Discovery entry opens the Session Information page with detailed source and destination device attributes and timestamps. Use this to validate why a session was flagged and where it occurred.

Observation toolbar

Add to NDR Mute Rule	Hide observations that are not relevant to your network. These detections will no longer be visible in insight pages and prevents related alerts and enforcement actions. See, NDR Muting on page 169.
Explore Attack Name	Displays the attack name and description. Click the *Search FortiGuard* button for more information in FortiGuard Labs. This option only appears in *Network Attacks*.
Search	Enter search terms or click the plus symbol (**+**)to filter the columns.
Mute Effect	Displays observations when NDR muting is enabled. See, NDR Muting on page 169.
Time range	Set the time range from 30 minutes to 1 month.
Persist Table Settings	Click the gear icon at the right-side of the toolbar to retain their selections after navigating away from the page.

Persist Table Column Selection	Retain selected column selected for display.
Persist Table Column Filter Selection	Retain column filter applied.
Persist Table Time Window Selection	Retain timeframe selection.

Observation information

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

General tab

The *General* tab provides a detailed snapshot of the detection, including the type of vulnerability, severity, associated MITRE techniques, and the specific source and destination device attributes observed during the latest occurrence.

Field	Desription
NDR Detection or Observation Type	This indicates the type of security issue detected.
Protocol	The communication protocol involved in the detection.
Type	Specifies the subtype of the issue detected.
Severity	The risk rating assigned to the detection.
Latest Occurrence	The most recent date and time when this issue was observed on the network.
Mitre Detected	Lists the MITRE ATT&CK techniques associated with the detection.
Last NDR Detection or Observation Occurrence Source Device	
Source IP	The IP address of the device that initiated the network traffic related to the detection.
Source Network	Indicates the network classification of the source device.
Source Port	The network port number used by the source device when sending the traffic.
Source Packet Size	The size, in bytes, of the packet sent by the source device.
Source Country	The geographical country associated with the source IP.
Source MAC	The hardware MAC address of the source device.
Source Device Model	Identifies the type of hardware or environment of the source device.
Source OS	The operating system running on the source device.
Source Device Category	The general category of the device.
Source Device Sub Category	A detailed classification of the device.
Last NDR Detection or Observation Occurrence Destination Device	
Destination IP	The IP address of the device receiving the traffic related to the detection.
Destination Network	Indicates the network classification of the destination device.
Destination Port	The network port number on the destination device that received the traffic.
Destination Packet Size	The size, in bytes, of the packet received by the destination device.

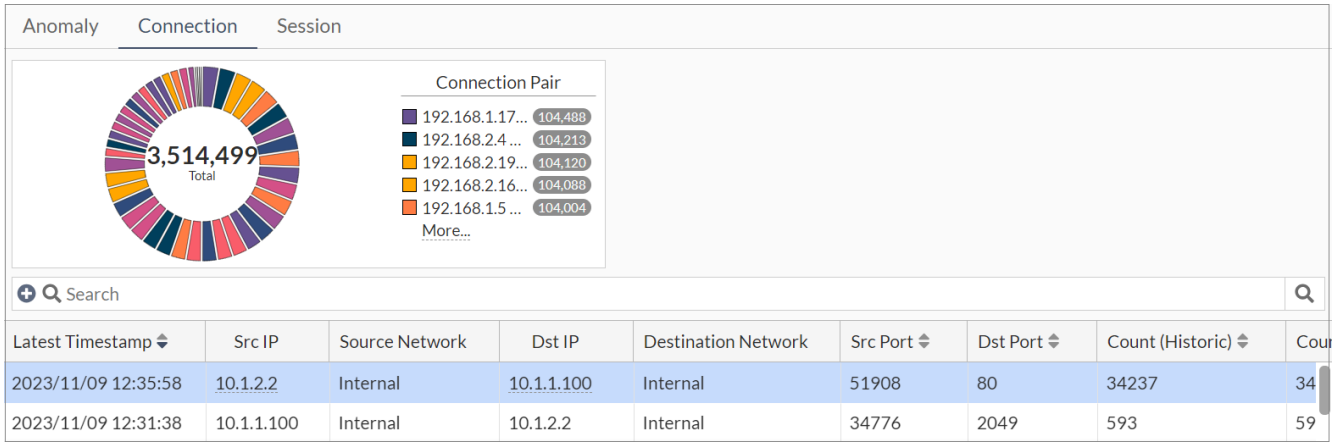
Analytic tab

The *Analytics* tab summarizes all connection pairs that share the same observation, helping to show where the vulnerable protocol is being used across the environment.

Column	Description
Connection Pair	Shows the two endpoints involved in a network communication flow.
Source IP	Identifies the address of the device that initiated the connection.
Source Network	Indicates whether the originating device is on an internal or external network.
Destination IP	Identifies the address of the device receiving the connection.
Destination Network	Indicates whether the destination device resides on an internal or external network.

Connection tab

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



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 event was observed.
Count (Past week)	The total number of times the event was observed during the past week .
First Event Timestamp	The timestamp for the first time the event was detected.

To view the sessions for a selected condition:

1. In the *NDR Detection* or *Observation* tab, double-click a record in the list. The *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 89.

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

Type	• Event 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

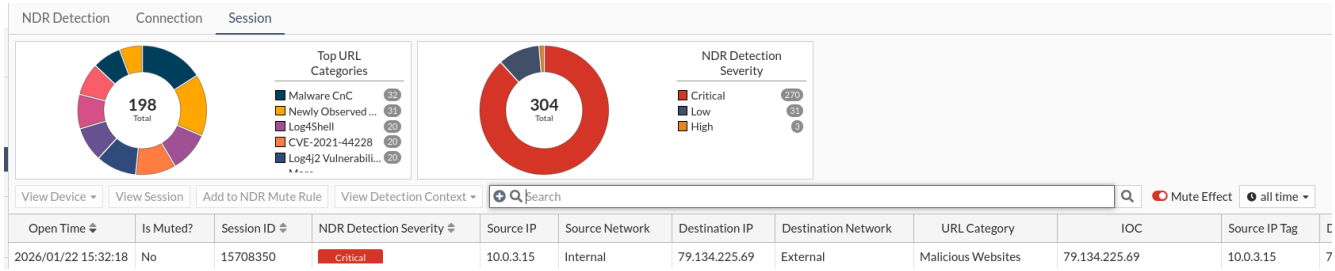
Analytic tab

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

Column	Definition
Severity	The event severity (*Not Observation*, *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 event was observed.
Count (Past week)	The total number of times the event was observed during the past week .

Session tab

The *Session* tab lists all sessions associated with the same event type (such as *Network Attacks* or *Encrypted Attacks*). Each row represents a single event. If a session contains multiple events of the same type, it will appear in multiple rows sharing the same session ID.



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

Column	Description
Open Time	The date and time the session started.
NDR Detection/Observation Severity	The detection severity (*Not Observation*, *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 session in the list to open the *Session Information* page. The following information is displayed:

- *General*: Session ID, Start Time, End Time
- *Traffic Volume*: VLAN ID, Port ID

- *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

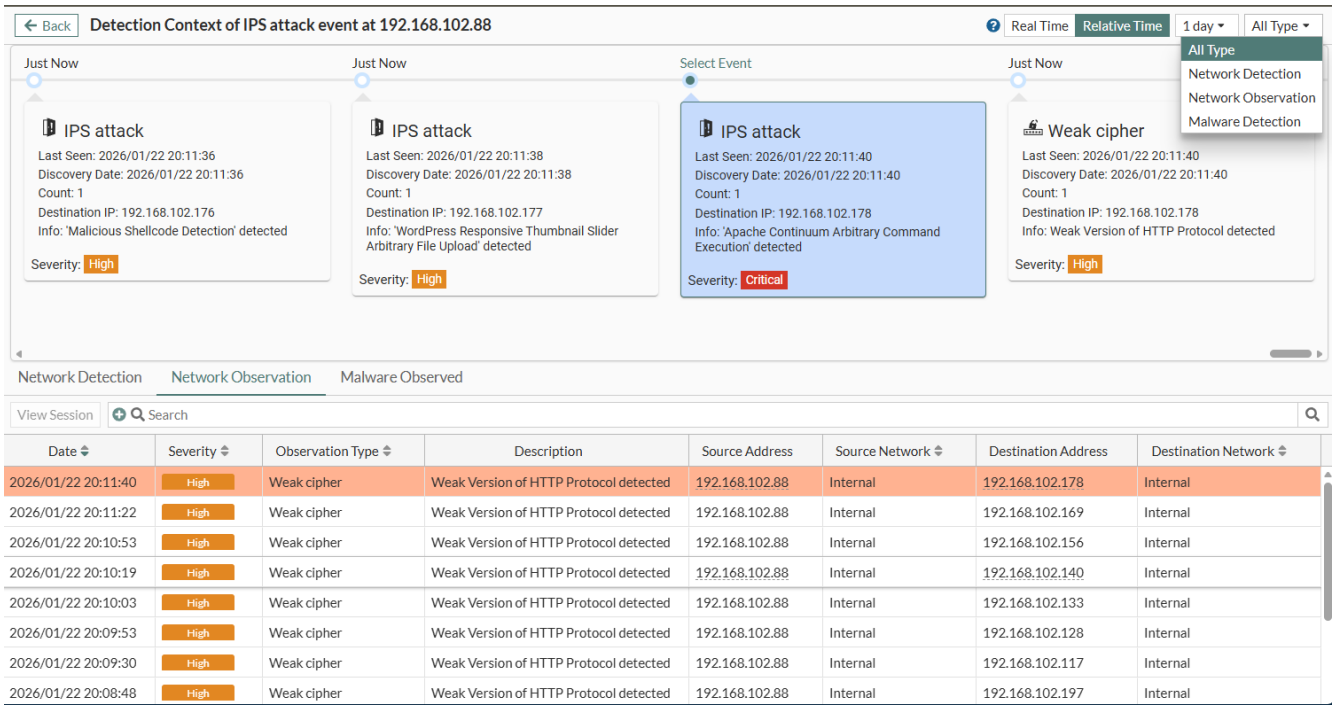
Detection context

The *Detection Context* page allows you to view Network Detections, Network Observations, and Malware Detections in a single timeline. The page focuses on a specific IP address and a selected events, displaying all detection and observation events surrounding the targeted event within a chosen time frame (1 day, 1 week, or 1 month). The timeline graph supports a maximum of 5,000 events: 2,500 before and 2,500 after the selected network attack.

Identical events (defined by the same source IP, destination IP, type, and content) are grouped into a single event block. Each block includes a count indicating the number of actual occurrences. When these identical events are separated by other types of detections in the timeline, the block is anchored to the timestamp of the first occurrence, which is labeled as the *Discovery Date*.

The timeline graph can be viewed in *Real Time* or *Relative Time*. In *Real Time* mode, the timeline shows events in relation to the current date. For example, *2 weeks ago* means two weeks before today. In *Relative Time* mode, the timeline shows events in relation to a selected event. For example, *1 day ago* means one day before that event was detected. You can filter the timeline by detection type: *Show All* displays everything, *Network Detection* shows network events, *ML Discovery* shows machine-learning discoveries, and *Malware Observed* shows malware-related events.

The *Network Detection* and *Malware Detection* tables below the timeline display ungrouped events or malware detection events individually, as shown in the timeline graph. The table can support up to 60,000 entries.

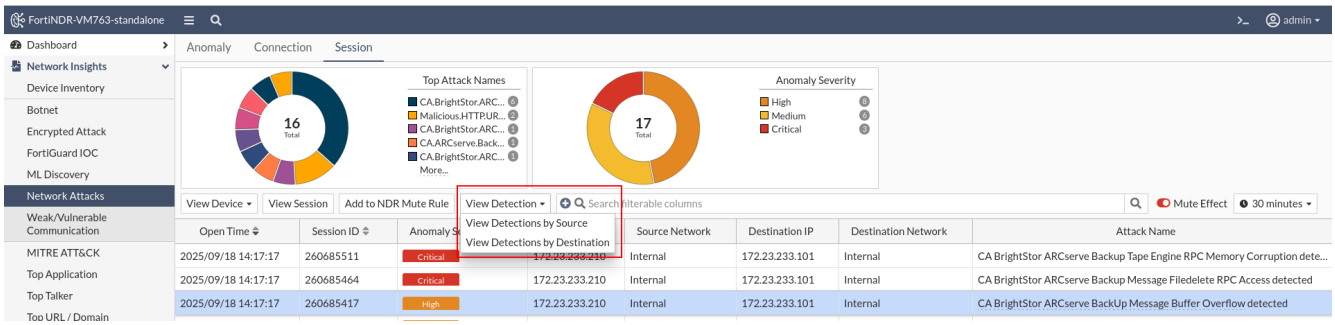


The *Detection Context* timeline displays the following information:

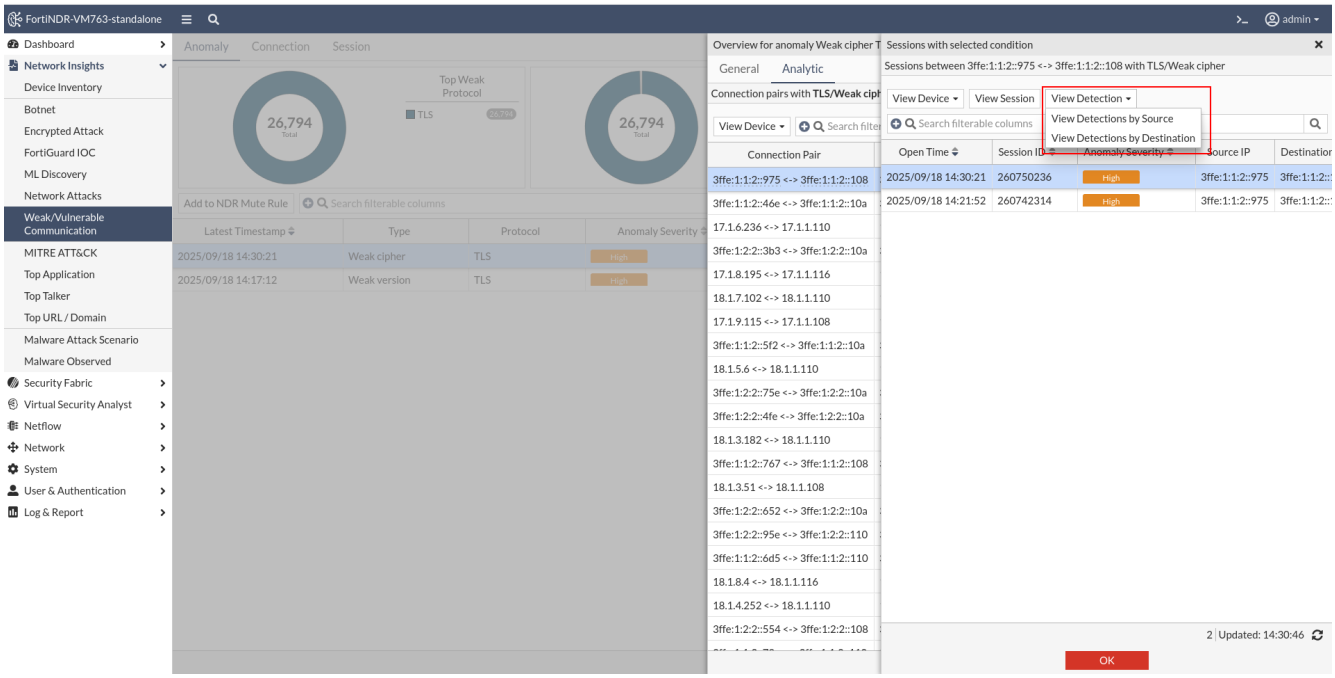
Field	Description
Last Seen	The latest appearance of a specific type of event (with identical Source IP, Destination IP, Type, and Content).
Discovery Date	The first occurrence of the \event (with identical Source IP, Destination IP, Type, and Content).
Count	The number of events with identical Source IP, Destination IP, Type, and Content.
Destination IP	The destination IP address of the event.
Info	The detection context of the event.
Severity	The severity level of the detection or observation.

Accessing the Detection Context page

You can access the *Detection Context* by selecting a session in the *Session* tab, clicking *View Detection*, and then selecting either *View Detections by Source* or *View Detections by Destination*.



You can also access the *Detection Context* from the *NDR Detection* tab or NDR logs by clicking a detection pair in the *Analytic* tab.



View source and destination devices

Use the *View Device* dropdown in the *Session* tab to view source and destination device details. This 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.

Viewing the session page

The *Session* page provides a detailed view of a selected session related to a network event.

To view the session page, select a record in the *Session* tab and click *View Session*You can use the right-side navigation panel to scroll through the content.

The *Session* page contains the following information:

Section	Description
NDR Detection or Observation	Displays the type and severity of the network event.
Session Information	Includes session metadata such as Session ID, Start Time, End Time, VLAN ID, and Port ID.
Device Information	Details about source and destination devices, including IP, port, MAC address, packet size, country, device model, OS, and category.
Activity	Shows session-related activity data.
ML Discovery	Displays insights from machine learning analysis.
NDR Detection	Shows the detection date, severity, type and description.
Observation	Shows the observation date, severity, type and description.
MITRE ATT&CK	Visual widget mapping detected events to MITRE ATT&CK tactics categories.

View user account information

FortiNDR supports extracting and displaying user account information from legacy and unencrypted protocols. This includes:

- SMB (Server Message Block) y version 1
- POP3 (Post Office Protocol version 3)
- IMAP (Internet Message Access Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Kerberos

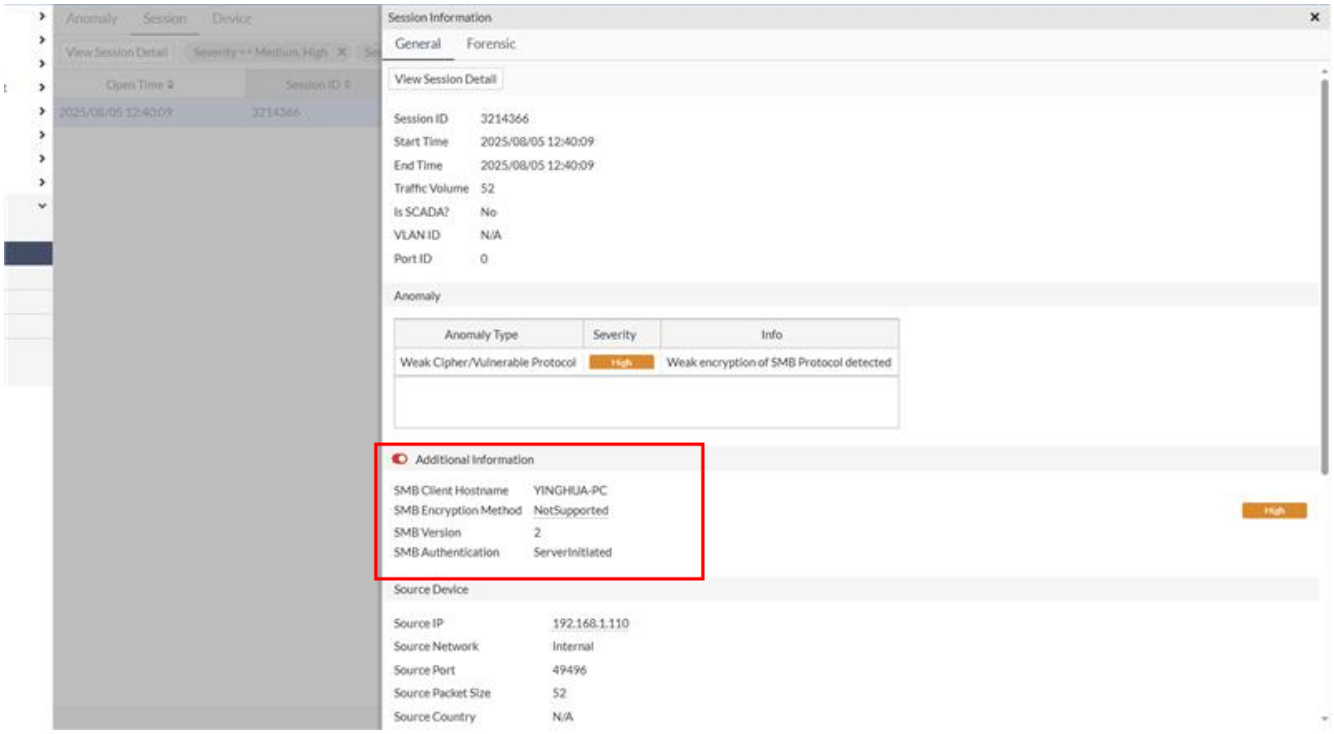
When these protocols are used in network communications, the system can extract and display the account information such as the username or email address.

To view account Information:

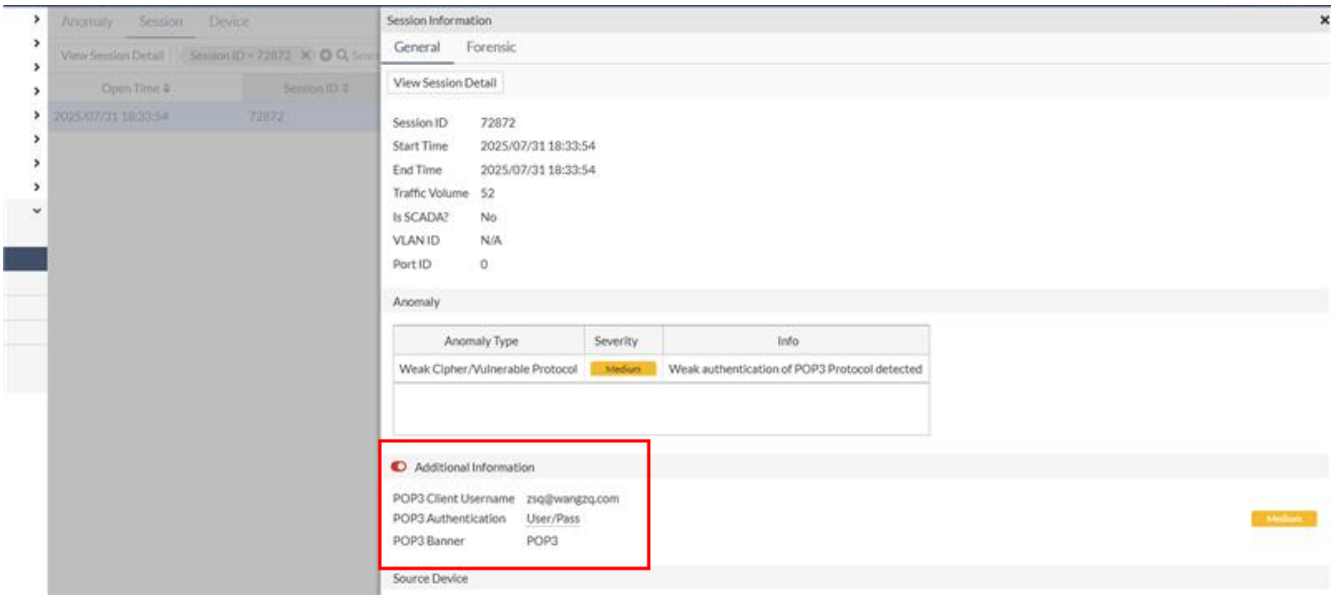
1. Open the *Sessions* tab.
2. Double-click on an individual session.

Within the session details, you will find extracted account information under *Additional Information* .

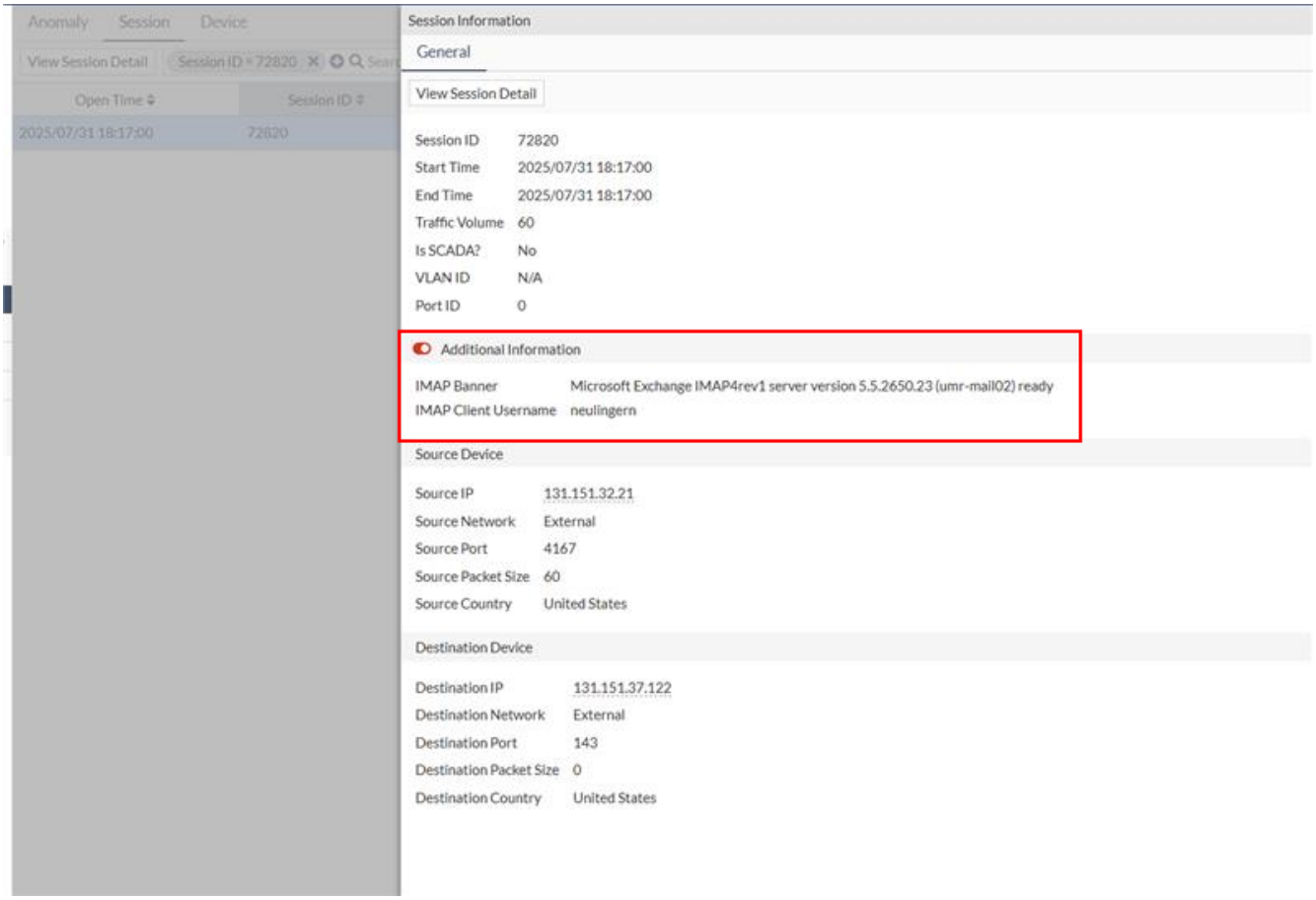
SMB



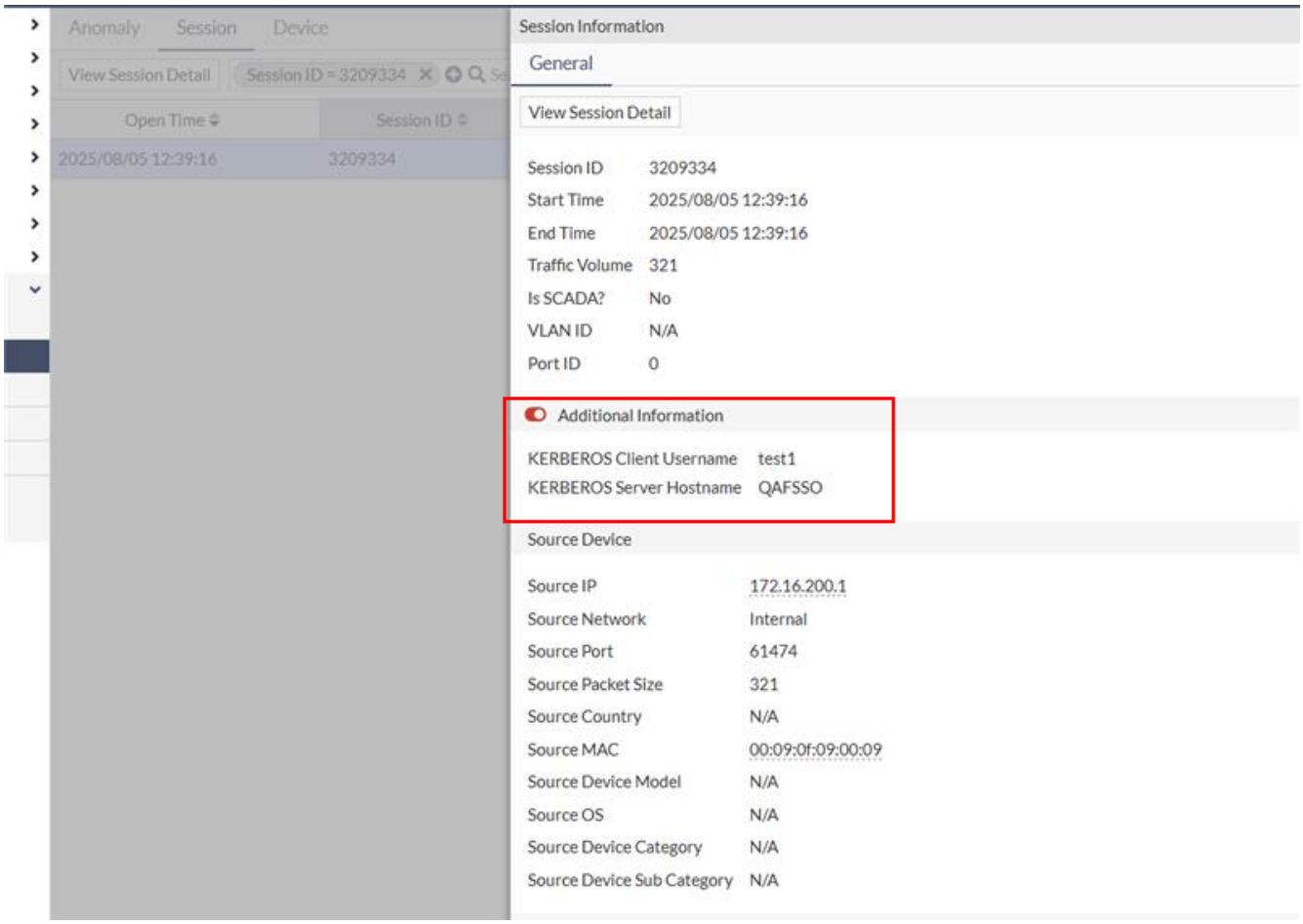
POP3


Anomaly
Session
Device
Session Information
General
Forensic
View Session Detail
Session ID 72872
Start Time 2025/07/31 18:33:54
End Time 2025/07/31 18:33:54
Traffic Volume 52
Is SCADA? No
VLAN ID N/A
Port ID 0
Anomaly
Anomaly Type
Severity
Info
Weak Cipher/Vulnerable Protocol
Medium
Weak authentication of POP3 Protocol detected
Additional Information
POP3 Client Username zsq@wangzq.com
POP3 Authentication User/Pass
POP3 Banner POP3
Source Device

IMAP


Anomaly
Session
Device
Session Information
General
View Session Detail
Session ID 72820
Start Time 2025/07/31 18:17:00
End Time 2025/07/31 18:17:00
Traffic Volume 60
Is SCADA? No
VLAN ID N/A
Port ID 0
Additional Information
IMAP Banner Microsoft Exchange IMAP4rev1 server version 5.5.2650.23 (umr-mail02) ready
IMAP Client Username neulingern
Source Device
Source IP 131.151.32.21
Source Network External
Source Port 4167
Source Packet Size 60
Source Country United States
Destination Device
Destination IP 131.151.37.122
Destination Network External
Destination Port 143
Destination Packet Size 0
Destination Country United States

KERBEROS


Anomaly
Session
Device
View Session Detail
Session ID = 3209334
Open Time
Session ID
2025/08/05 12:39:16
3209334
Session Information
General
View Session Detail
Session ID 3209334
Start Time 2025/08/05 12:39:16
End Time 2025/08/05 12:39:16
Traffic Volume 321
Is SCADA? No
VLAN ID N/A
Port ID 0
Additional Information
KERBEROS Client Username test1
KERBEROS Server Hostname QAFSSO
Source Device
Source IP 172.16.200.1
Source Network Internal
Source Port 61474
Source Packet Size 321
Source Country N/A
Source MAC 00:09:0f:09:00:09
Source Device Model N/A
Source OS N/A
Source Device Category N/A
Source Device Sub Category N/A

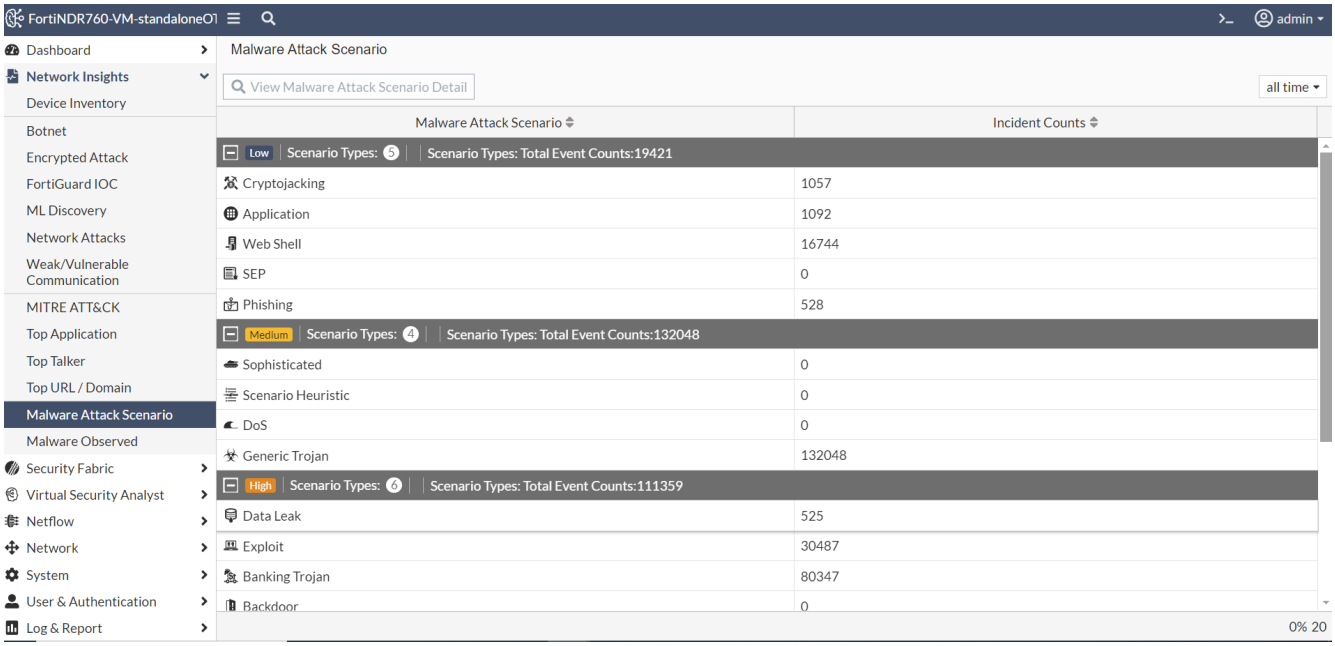
Malware Attack Scenario

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.



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.

Scenario	Severity	Description
Application	Low	A broad category of software that might download and install additional, unwanted software that could perform activities not approved or expected by the user.
Web Shell	Low	A script that can be uploaded to a web server to allow remote administration of the machine. Infected web servers can be Internet-facing or internal to the network where the web shell is used to pivot further to internal hosts.
SEP	Low	Attackers use Search Engine Poisoning to take advantage of your rankings on search engine result pages.
Phishing	Low	A fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising itself as a trustworthy entity in an electronic communication.
Sophisticated	Medium	Malware that contains more than one attack scenario.
Scenario Heuristic	Medium	Scenario heuristic identifies applications or software that demonstrates an array of suspicious traits.
DoS	Medium	This can access connection handling remotely, perform denial of service, or distributed DoS.
Generic Trojan	Medium	Any malicious computer program which misleads users of its true intent.
Banking Trojan	High	Malicious software that can access confidential information stored or processed through online banking systems.
Backdoor	High	This can give a hacker unauthorized access and control of your computer.
Data Leak	High	A data leak is when sensitive data is exposed physically on the Internet where malicious actors can access it.
Rootkit	High	Software tools that enable an unauthorized user to get control of a computer system without being detected.
Exploit	High	A piece of software, a chunk of data, or a sequence of commands that uses a bug or vulnerability to cause unintended or unanticipated behavior on computer software, hardware, or something electronic, usually computerized.
Botnet	High	A botnet is a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker.
Ransomware	Critical	Malicious software that can block access to a computer system until money is paid.
Fileless	Critical	A variant of computer-related malicious software that is exclusively a computer memory-based artifact.

Scenario	Severity	Description
Wiper	Critical	Malware that erases contents in the hard disk of an infected computer. It's usually designed to destroy as many computers as possible inside the victim's networks.
Industroyer	Critical	A malware framework originally designed to deliver specific cyber attacks 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.

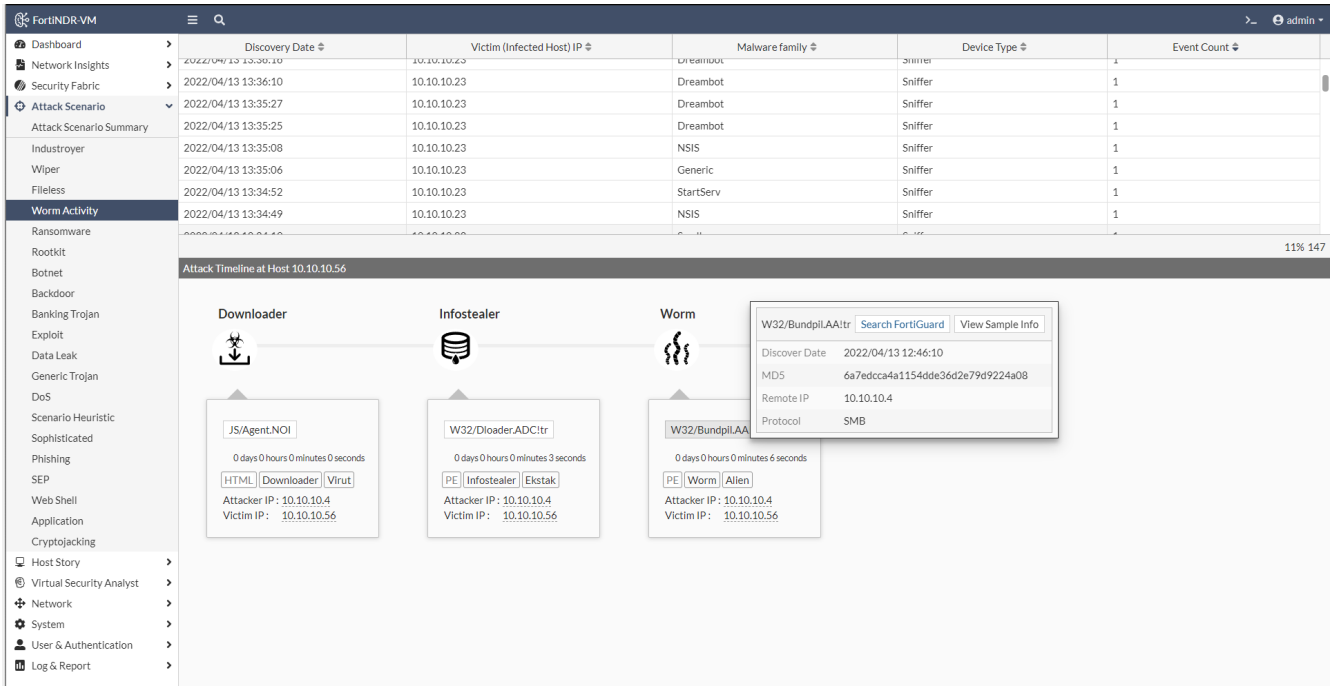
Attack scenario navigation and timeline

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.

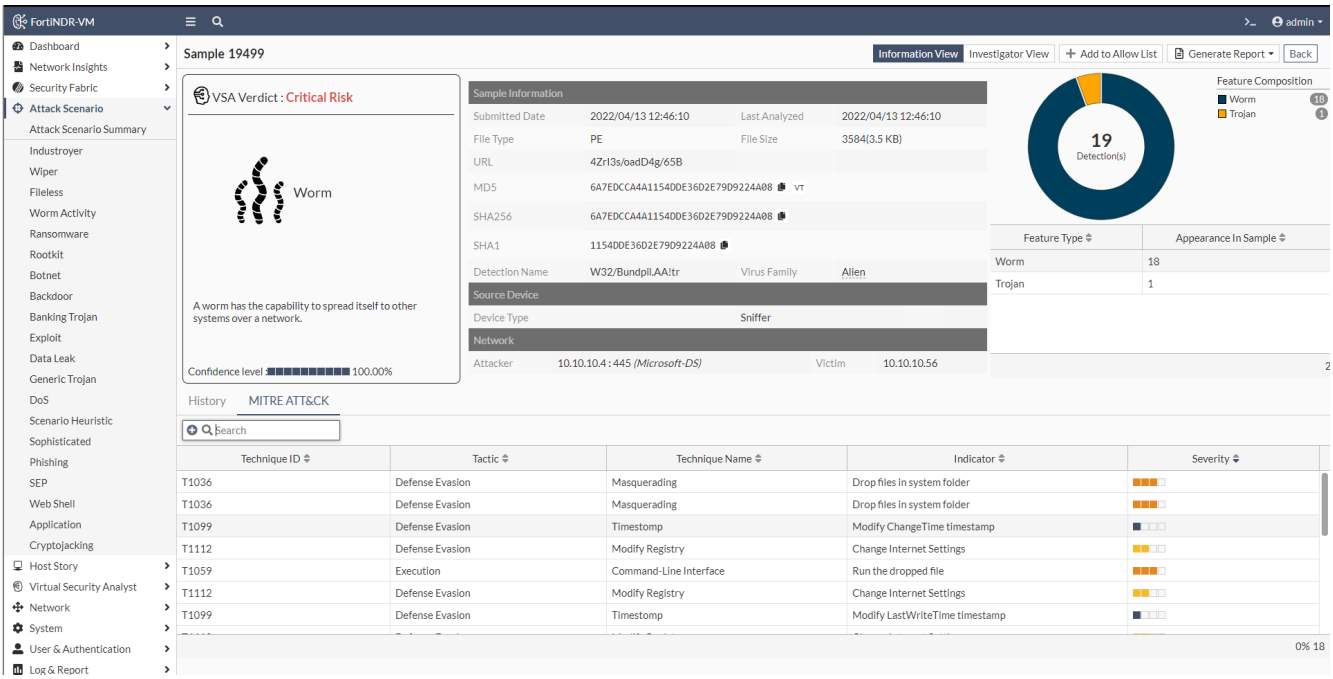
The following is an example of a worm infection. The virtual analyst shows the remote IP address where the attack originated, the timeline, and other malicious files discovered on the infected host, and the worm activity shows it is trying to spread.

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.

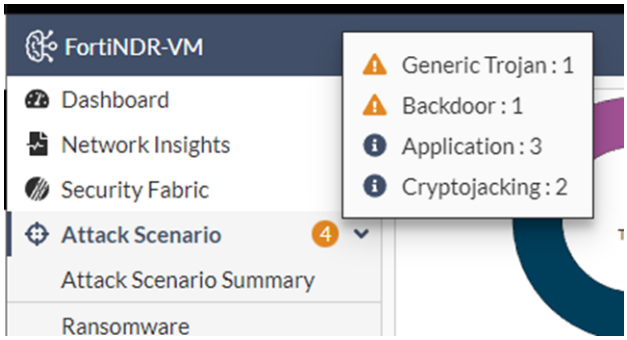


> You might see the same IP address multiple times. This indicates that IP address has been detected for the attack type multiple times, for example, ransomware.

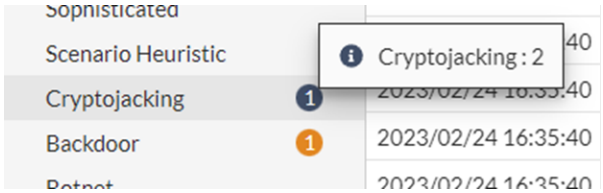
The following example shows a Sample Information page of the W32/Bundpil.AA!tr captures in the attack timeline.



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



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



Understanding kill chain and scenario engine

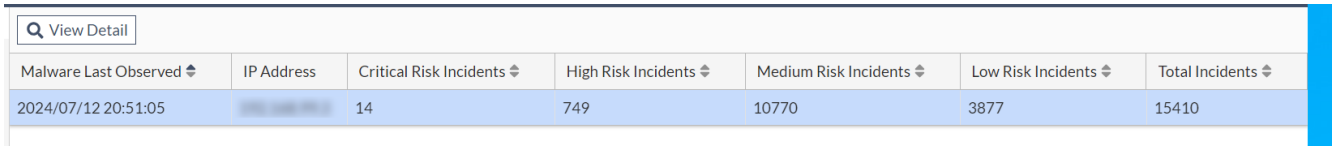
One of the strengths of FortiNDR is the ability to trace the source of a malware attack. In all attack scenarios, especially with worm, ransomware, and sophisticated attacks, there are often timeline and multi-stage kill chain type graphics. When there is a detection, the scenario engine tries to form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

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

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

Malware Detection

Malware Detection organizes malware attacks by host IP address while *Attack Scenario* organizes malware attacks by attack type. The *Malware Detection* view helps you examine the host to see when the infections first took place. For example, a host might obviously be 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, *Malware Observed* consolidates and displays all stories from all Sensors associated with the Center.

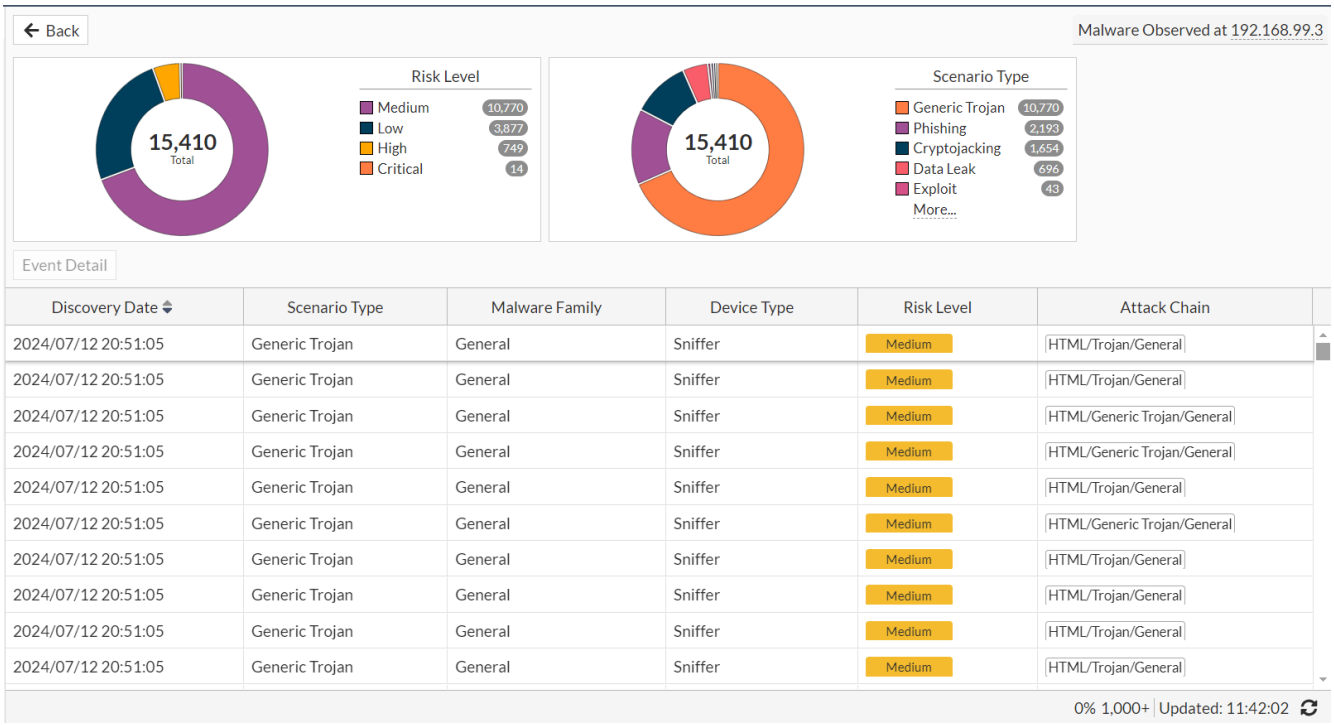
The *Malware Observed* summary page shows the following information:

Sensor	The sensor that detected the malware.
Malware Last Detection	The date and time the malware was last observed.
IP Address	The IP address of the infected device. Hover over the address to view the *Device*, *MAC Address*, *Hardware*, *OS* and the *View Device Detail* button
Critical Risk Incidents	The number of critical risk Incidents
High Risk Incidents	The number of high risk Incidents
Medium Risk Incidents	The number of medium risk Incidents
Low Risk Incidents	The number of low risk Incidents
Total Incidents	The total number of incidents.

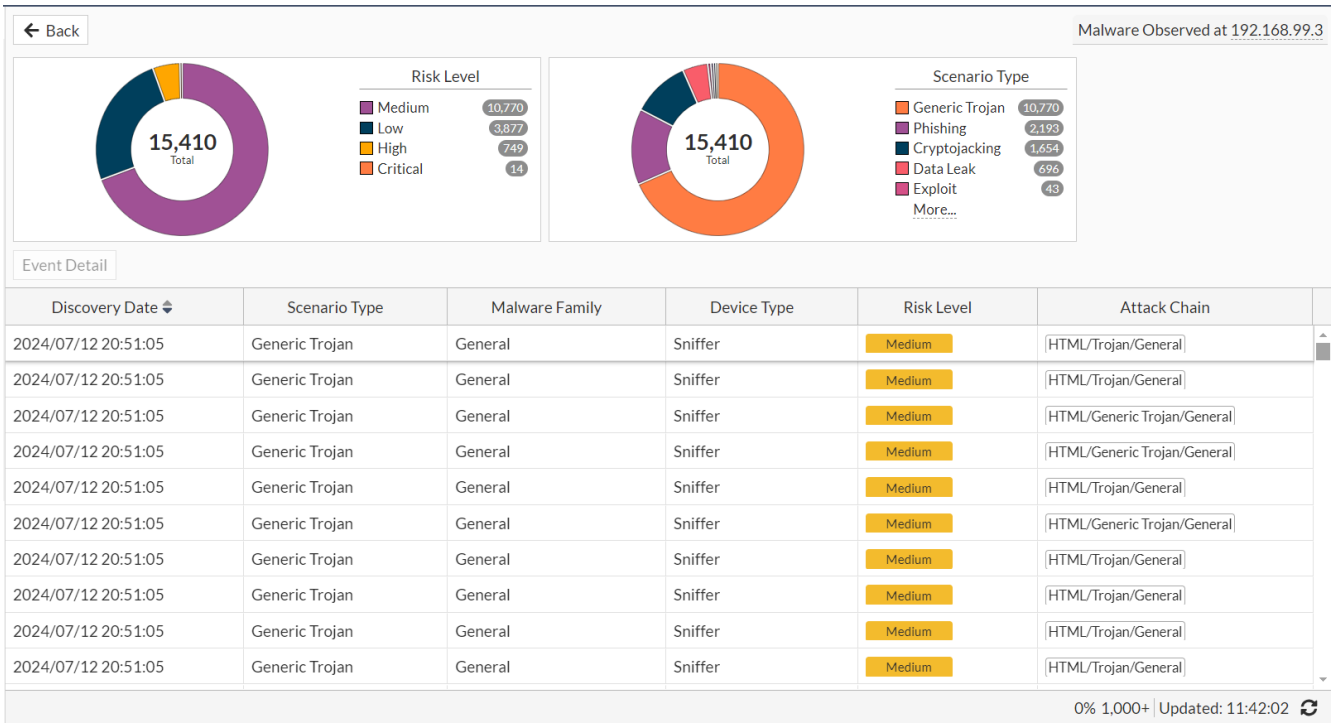
Malware Observed summary page

The *Malware Observed* summary page shows incident counts grouping by severities for each infected host.

To view *Malware Observed* summary page, select an incident and click *View Detail* at the top of the page.



The charts at the top of the page show the malware observed as pie charts by *Risk Level* and *Scenario Type*. To filter the charts, click a piece of the chart or an item in the legend.



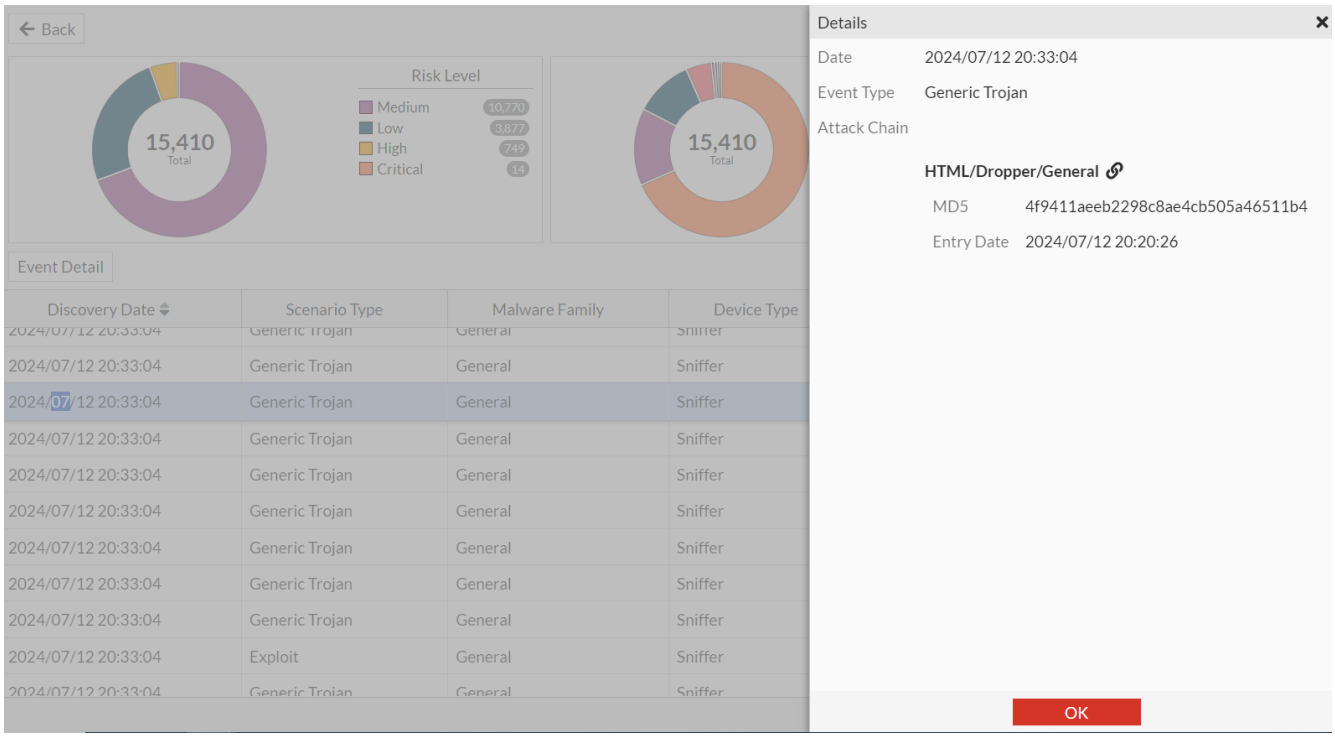
The *Malware Observed* table displays the following information:

Discovery Date	The date the malware was discovered.

Scenario Type	The scenario type.
Malware Family	The malware family.
Device Type	The device type.
Risk Level	The risk level.
Attack Chain	The attack chain.

Event details

To view the event details, select an event in the table and click *Event Detail* or double-click the event.



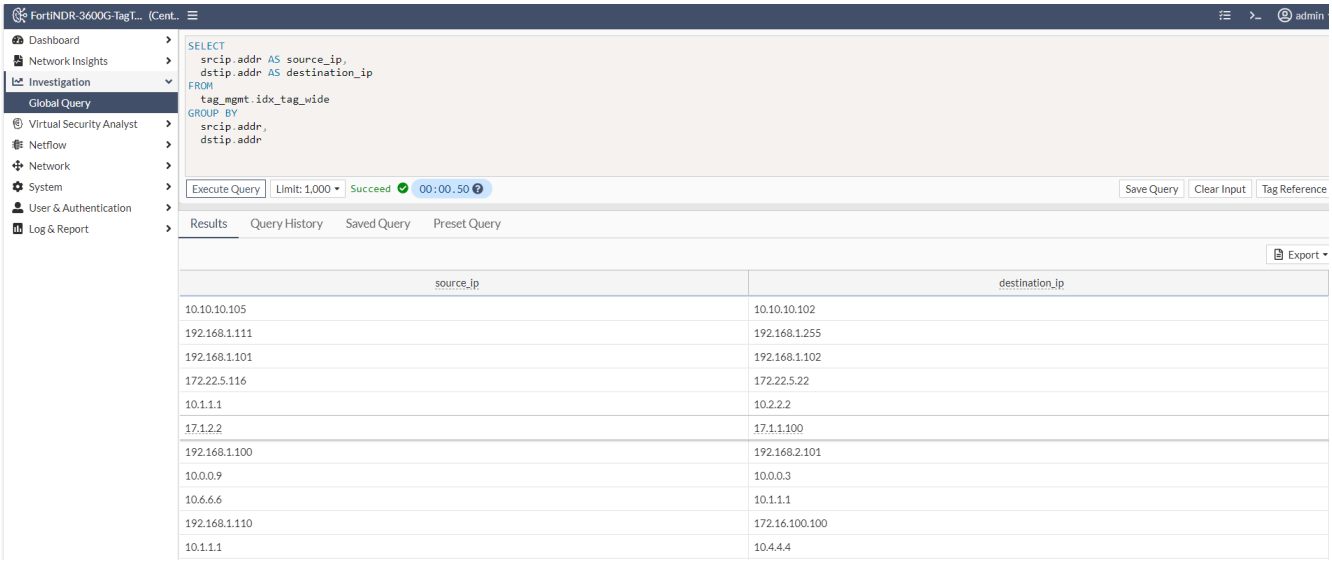
Investigations (Center)

The *Investigations* module allows you to search network metadata to easily identify breaches for incident investigation. FortiNDR's tagging mechanism extracts the significant attributes of all processed Session logs and exposes the data in a flexible interface to utilize the data gathered.

This feature is only available in FNR 3600G in Center mode or VM in Center Mode

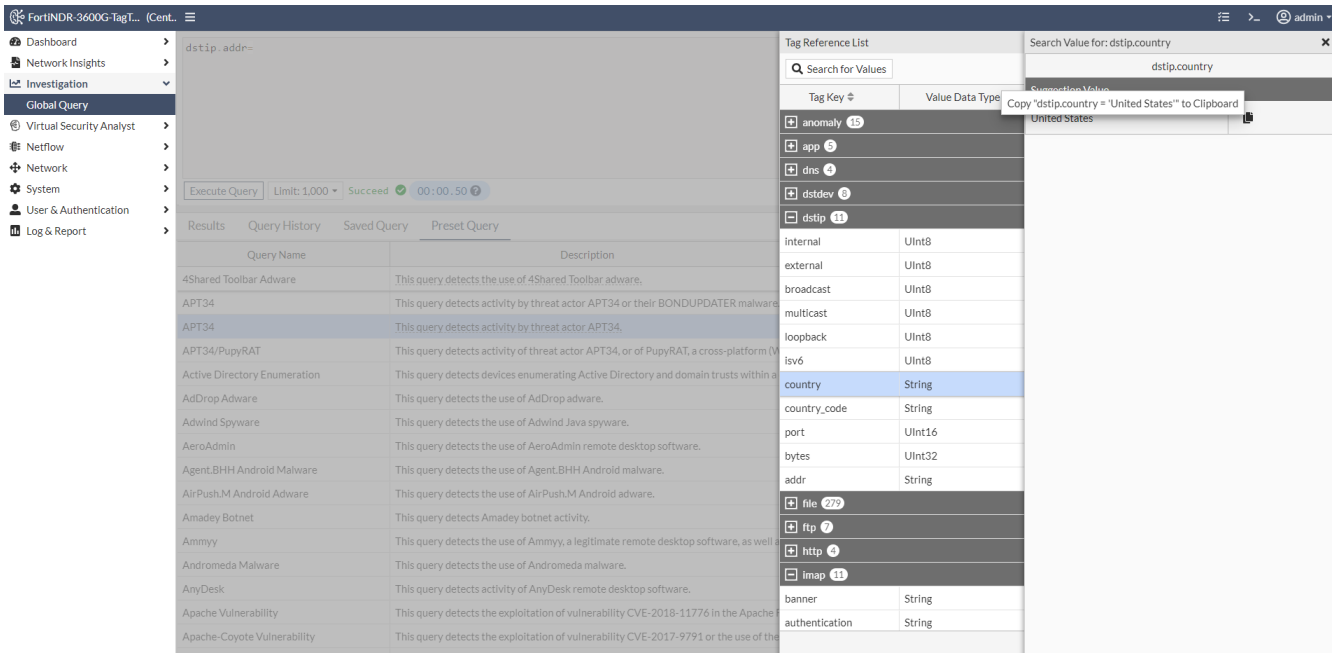
Tag management system

FortiNDR tags significant attributes with information from any incoming files and sessions. At this time, there are approximately 180 searchable tags. Information about these tags can be found by clicking the *Tag Reference* button in the *Global Query* page or the *Global Investigations Syntax Guide*.



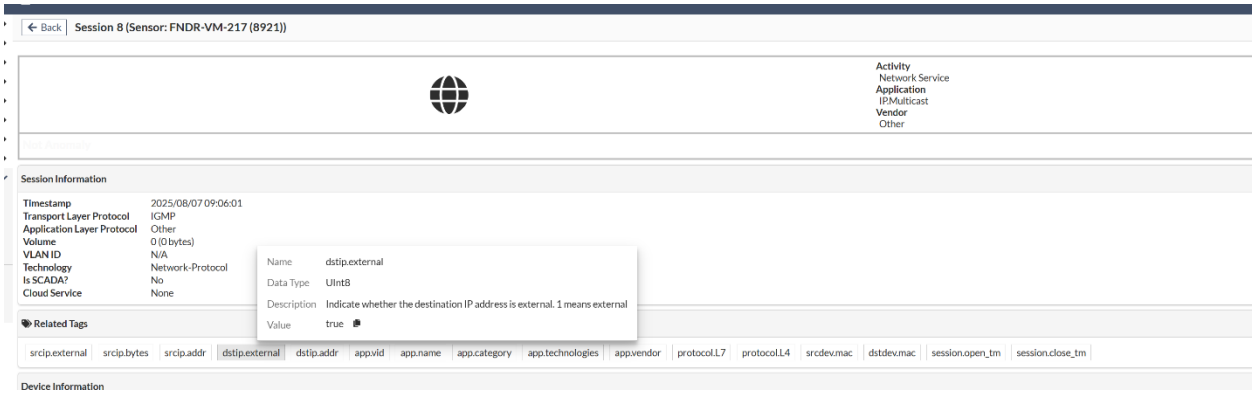
Tag reference

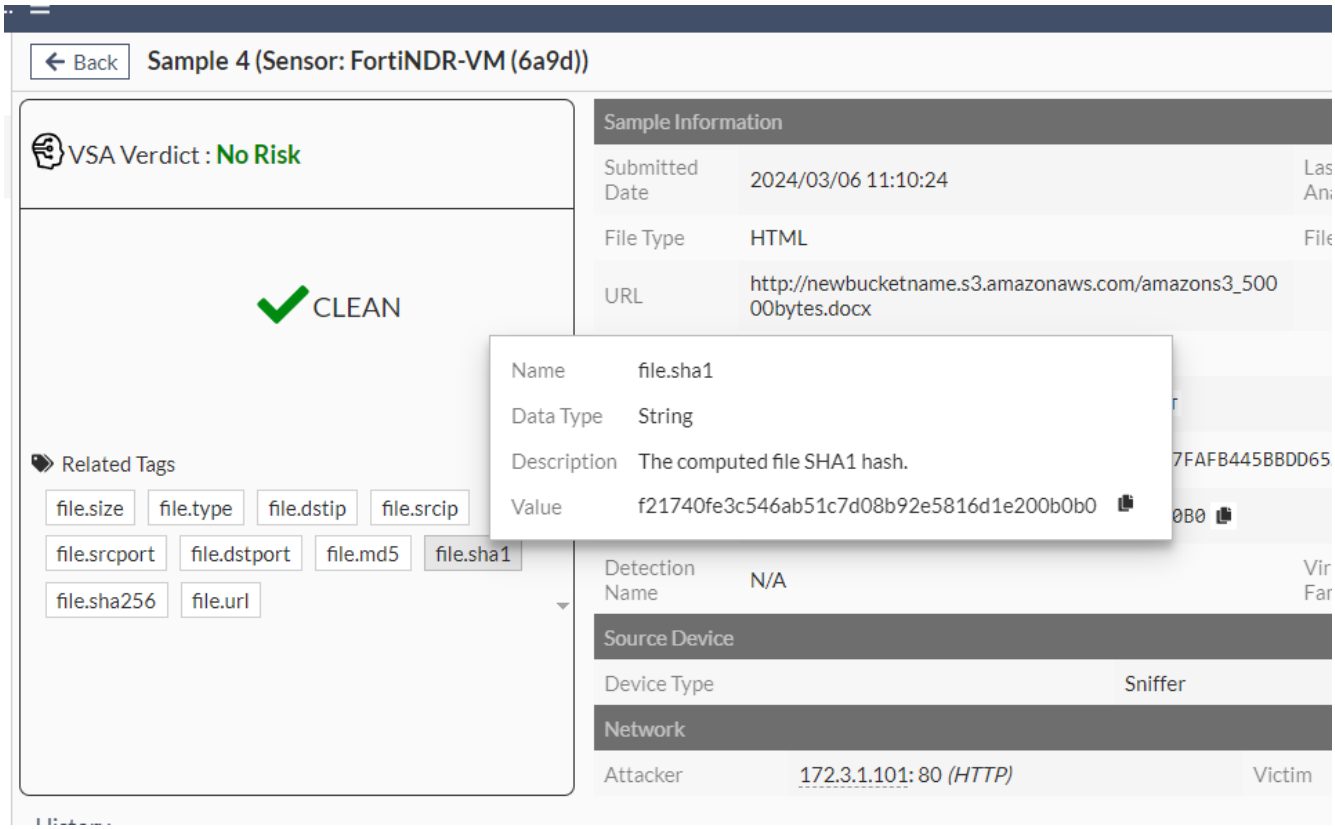
The *Tag Reference* button allows you to search for keywords and values when you create a query. To view a suggested value, double-click a keyword in the list. Once you have identified a keyword and value pair to use, click the *Copy* button to copy it to the clipboard, then paste the new condition in the desired location of the query field.



Related tags

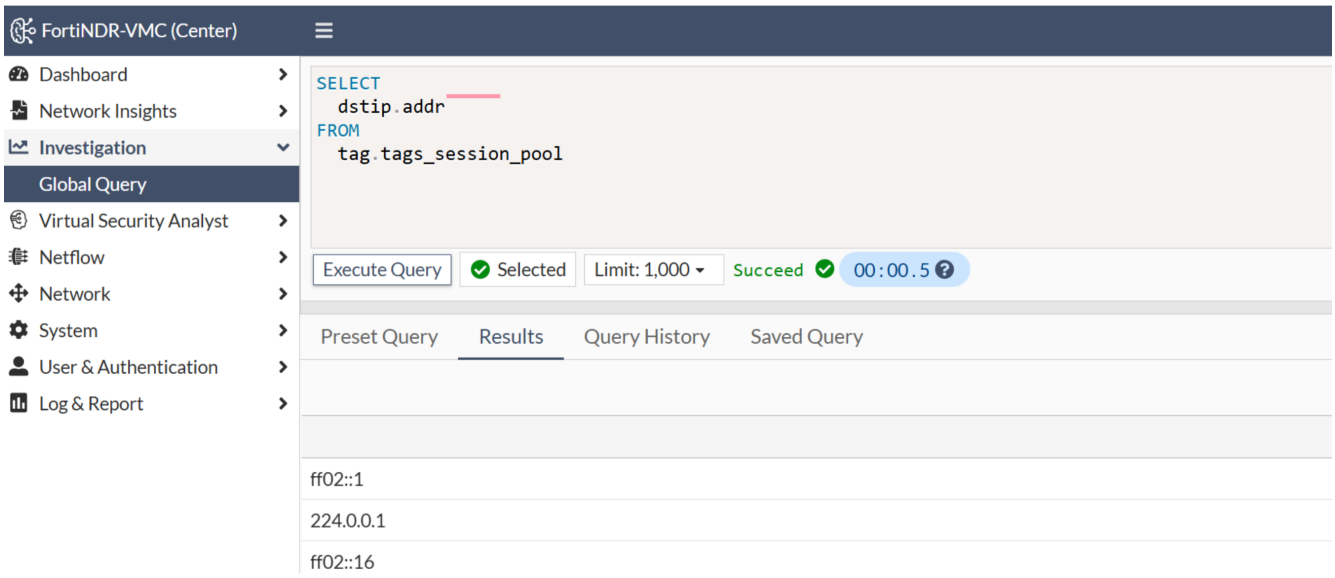
All of the session details pages contain a *Related Tags* section. When you hover over a tag, the tag's value for that session is displayed. To use the key and value as a search clause, click the *Copy* button next to the value.





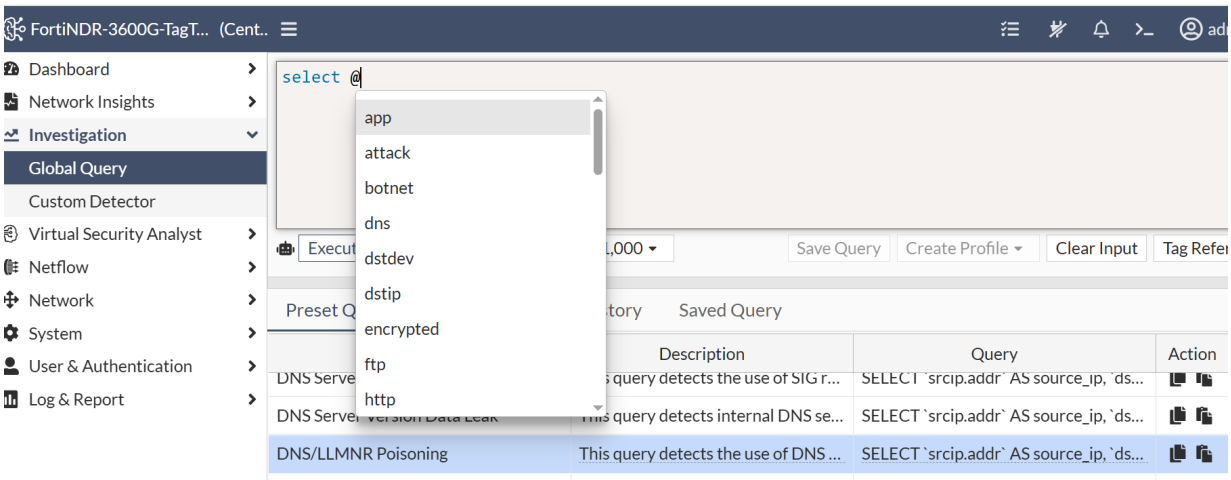
Global query

The *Global Query* page provides an intuitive SQL-based interface for investigating suspicious activity across your network. Start a query using the *Tag* selection dropdown or the *Tag Reference* tool. To narrow your results, add clauses with specific values or value ranges. You can save queries as templates for future use or re-run previous queries. Additionally, the Preset Query tab includes over 80 pre-built templates to help you quickly launch investigations.

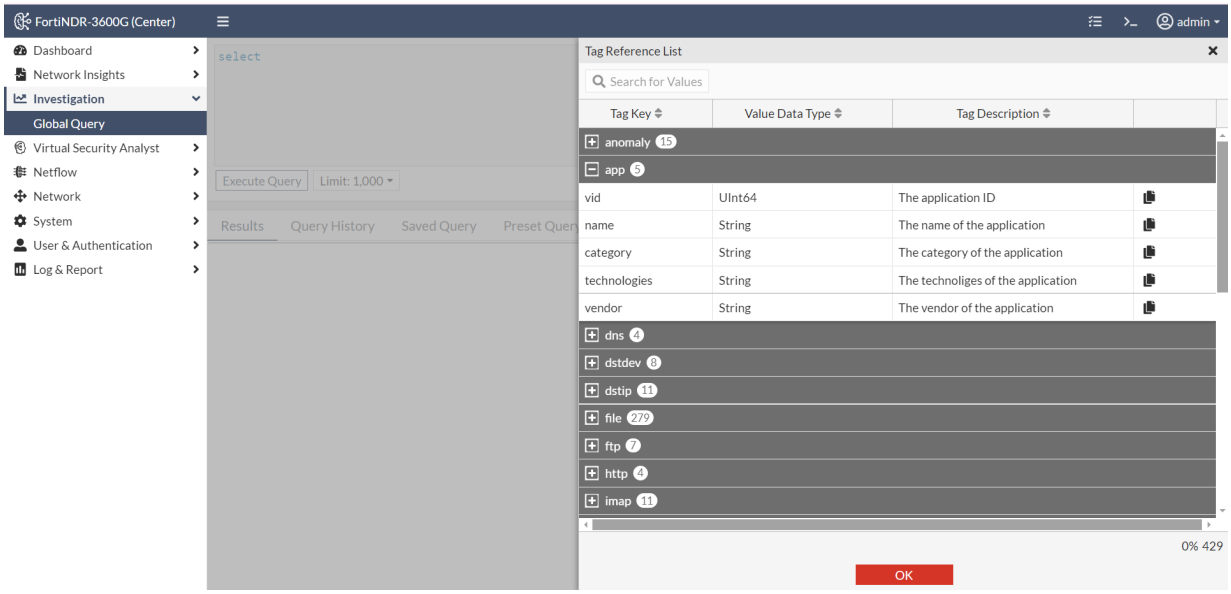


To start an investigation:

1. Go to *Investigations* > *Global Query*.
2. In the query field, type `SELECT`.
3. Add a tag/value pair to the query using one of the following methods:
   - Type the @ sign to activate the tag dropdown.



   - Click *Tag Reference*. Select a tag/value pair and click *Copy to clipboard* icon to paste it into the query field.



4. Use clauses to group and refine the query. For more information, see Advanced Query Language on page 110
5. Click the *Limit* dropdown to limit the number of results.
6. (Optional) Click *Clear Input* to clear the field.
7. Click *Execute Query*. The results are displayed.
8. (Optional) Click *Save Query* to save the query as a template.

To run a query from the Query History tab:

1. Click the *Query History* tab.
2. Double-click a query from the list. The *Query Detail* pane opens.
3. To copy the query:
   - Click *Copy to Query Area*. The query is pasted into the query field.
   - Click *Copy to Clipboard* to paste the query in the desired location.
4. Click *OK*.
5. Click *Execute Query*.

To run a saved query:

1. Click the *Saved Query* tab.
2. Double-click a query from the list. The *Query Detail* pane opens.
3. To copy the query:
   - Click *Copy to Query Area*. The query is pasted into the query field.
   - Click *Copy to Clipboard* to paste the query in the desired location.
4. Click *OK*.
5. Click *Execute Query*.

To run a query from a template:

1. Click the *Preset Query* tab.
2. Double-click a query from the list. The *Query Information* pane opens.
3. To copy the query:
   - Click *Copy to Query Area*. The query is pasted into the query field.
   - Click *Copy to Clipboard* to paste the query in the desired location.
4. Click *OK*.
5. Click *Execute Query*.

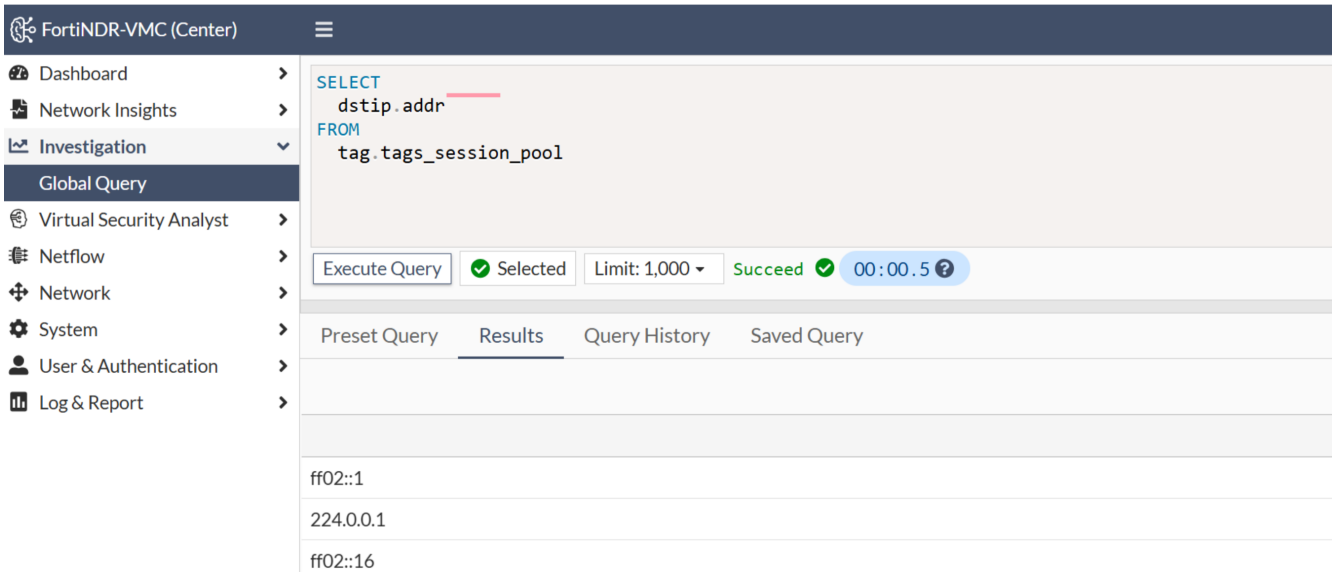
Advanced Query Language

SQL statements

The following SQL statements are supported:

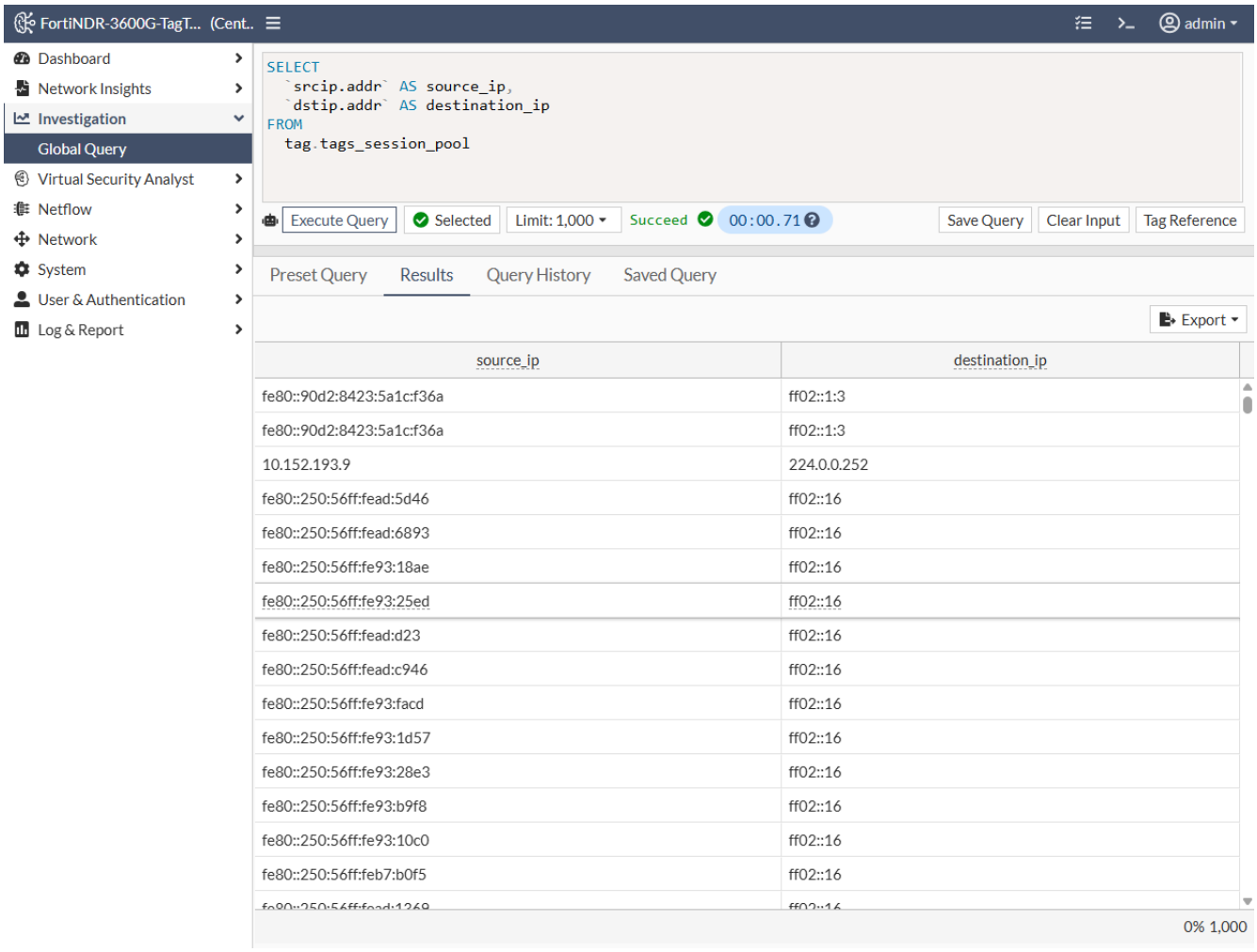
`SELECT | FROM | WHERE | GROUP BY | HAVING | AS`

Use the `Limit` clause dropdown to specify the number of records to return.

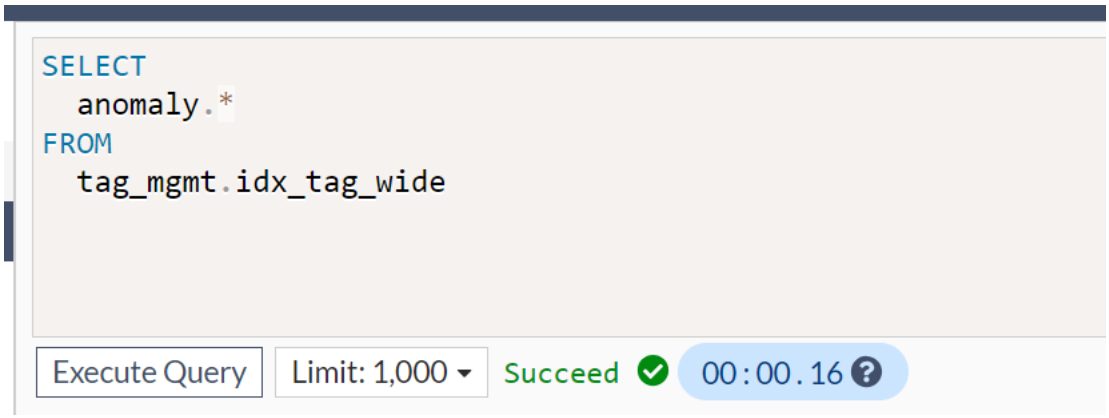


SELECT clause

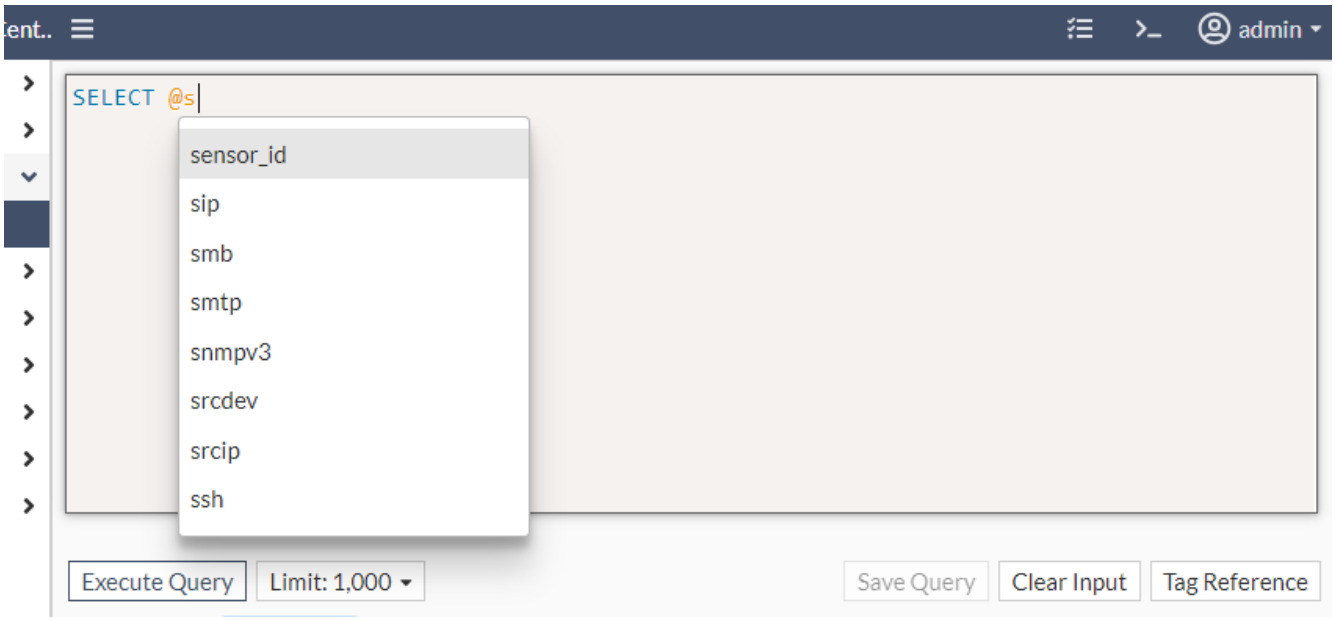
AS is supported for single column selection.



Use * to select a range of columns under one tag category, (for example, `srcip.*`).

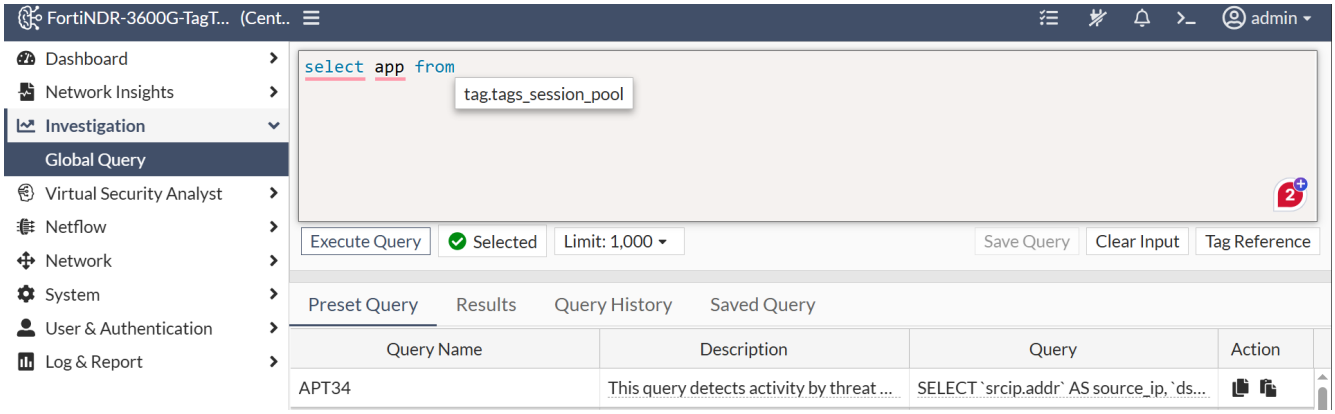


Click the *Tag Reference* button to view which tags are supported. Alternatively, you can type @ in the query field to activate the tag list.



FROM clause

Only `tag.tags_session_pool` is supported.



WHERE/HAVING clauses

Use the `WHERE` and `HAVING` clause to narrow the search criteria.

GROUP BY clause

`GROUP BY` is used to group rows that have the same values in specified columns.

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.

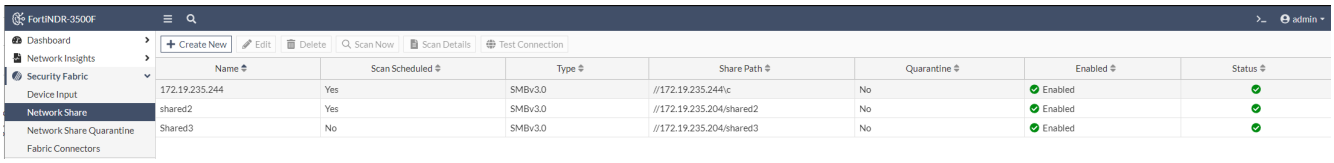
Network Share

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.



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 119. 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 119 > 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 check mark appears in the *Status* next to a valid connection.

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

Scanning a network location

To trigger a scan:

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

> The *Scan Now* button will not create a new task when the Network Drive is:
> - Currently mounting
> - Scanning another task
> - Disabled
> - Not connected (*Status* is *Down*)

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

Scheduling a scan

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

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

To schedule a scan:

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

5. Click *OK*.

Viewing scan results

View the scan history of the Network Share directories.

To view the scan results:

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

Total	The total number of files scanned.
Start Time	The date and time the scan started.
End Time	The date and time the scan completed.
Scan Finished	The scan progress as a percentage.
Critical Risk	The number of *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.

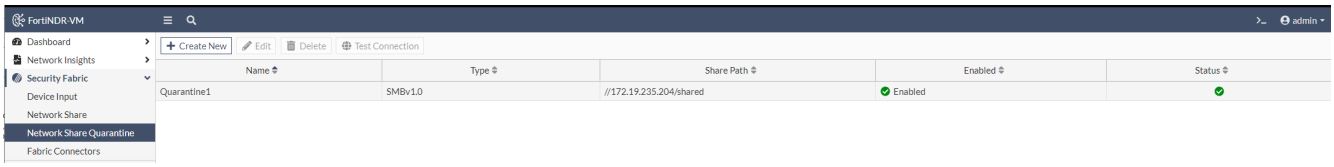
Scanning Zip files

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.



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:

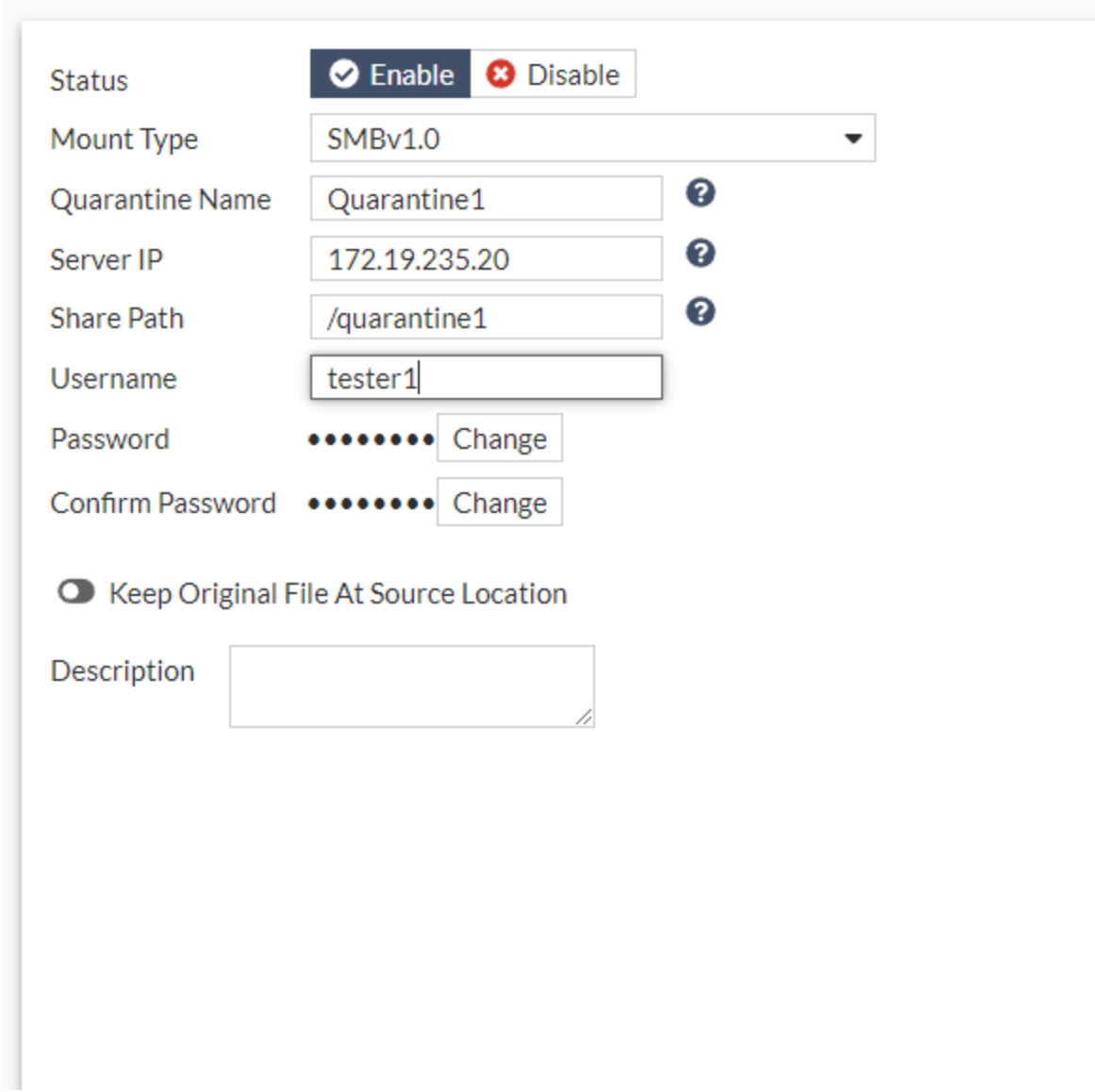
```
Network Share FileID: 351640
SID: 3 (Share ID)
JID: 44 (Job ID)
FileID: 1198941 (File ID)
File Name: sample.vsc
Device: testshared
URL: //172.16.2.100/shared2/2/sample.vsc
MD5: 31e06f25de8b5623c3fdaba93ed2edde
Virus Name: W32/Wanna.A!tr.ransom
DelOriginalFile: Success
```

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.



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 121.

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.

Keep original file at source location	Move/Copy clean files to sanitized location	Effect
		• 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.

Cloud Storage

Go to *Security Fabric > Cloud Storage* to scan remote cloud storage platforms.

Create a Cloud Storage profile to configure a Cloud Storage location for inspection. After the profile is configured, FortiNDR will scan the registered cloud storage's contents.

Name	The cloud storage profile name.
Scan Scheduled	Indicates scheduled scan is enabled/disabled.
Type	The cloud storage platform.
Storage Path	The URL of the cloud storage.
Enabled	Indicates the cloud storage profile is enabled/disabled.
Status	The cloud storage configuration status. See Testing connectivity on page 124.

Creating a Cloud Storage profile

To create a Cloud Storage profile, go to *Security Fabric > Cloud Storage*. Register a new Cloud Storage by providing access information. You can also use the profile to schedule a scan cycle of the cloud storage.

To create a Cloud Storage profile:

1. Go to *Security Fabric > Cloud Storage*.
2. In the toolbar, click *Create New*. The *New Cloud Storage* page opens.

3. Enter the Cloud Storage access information.

Status	*Enable* or *Disable*. Enable is the default.
Cloud Type	Select a cloud storage platform from the list. The following platforms are supported: • Amazon Web Service S3 Bucket
Cloud Storage Name	Enter a name for the Cloud Storage.
Bucket Name	(AWS S3 Only) Enter the name of the Cloud Storage container.
S3 Prefix	(AWS S3 Only) Enter the common prefix of the keys to scan. Leave empty to scan the entire bucket.
Access Key	Enter the access key for the cloud storage.
Secret Key	Enter the secret key for the cloud storage.
Enable Force Rescan	When enabled, FortiNDR will not use cache detection even if the files are previously scanned.

4. Click *OK*.

Testing connectivity

To validate the Cloud Storage configuration

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

A green check mark appears in the *Status* column next to a valid connection.

Scanning a cloud storage

To trigger a scan:

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

The *Scan Now* button will not create a new task when the Cloud Storage is:

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

You can use a REST API call to start a scan.

Scheduling a scan

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

To schedule a scan:

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

Viewing scan results

View the scan history of the Cloud Storage directories.

To view the scan results:

1. Go to *Security Fabric > Cloud Storage* 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 critical risk files.
High Risk	The number of detected critical high files.
Medium Risk	The number of detected medium risk files.
Low Risk	The number of detected critical low files.
Clean	The number of clean files.
Others	The number of detected other files.
Scan Status	The scan status as a string.

- Click the numbers to view the detection information for the samples that belong to the category.
- 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.
- Click *Back* to return to the Cloud Storage pane.

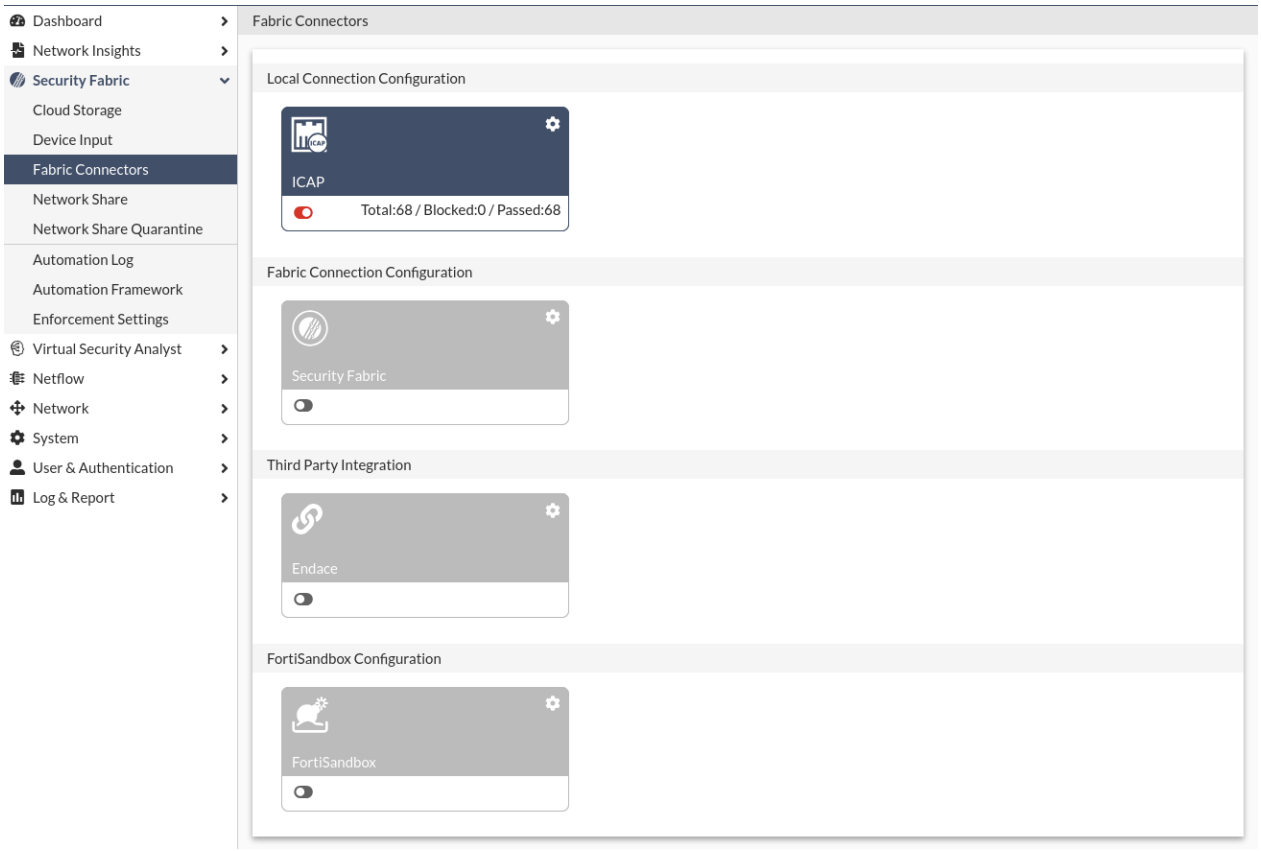
Scanning Zip files

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.

Fabric Connectors

Use the *Security Fabric > Fabric Connectors* page to connect FortiNDR to the Fortinet Security Fabric. ICAP allows connections to FortiGate and FortiWeb, and third-party devices such as Squid clients. The Endace connector supports pivoting results from NDR findings under *Log & Report > NDR Log > Forensic* tab to the Endace GUI. This integration allows you to investigate the PCAP related to the IP addresses.



ICAP Connectors

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

Use the ICAP connector to:

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

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

To integrate FortiNDR with FortiGate ICAP:

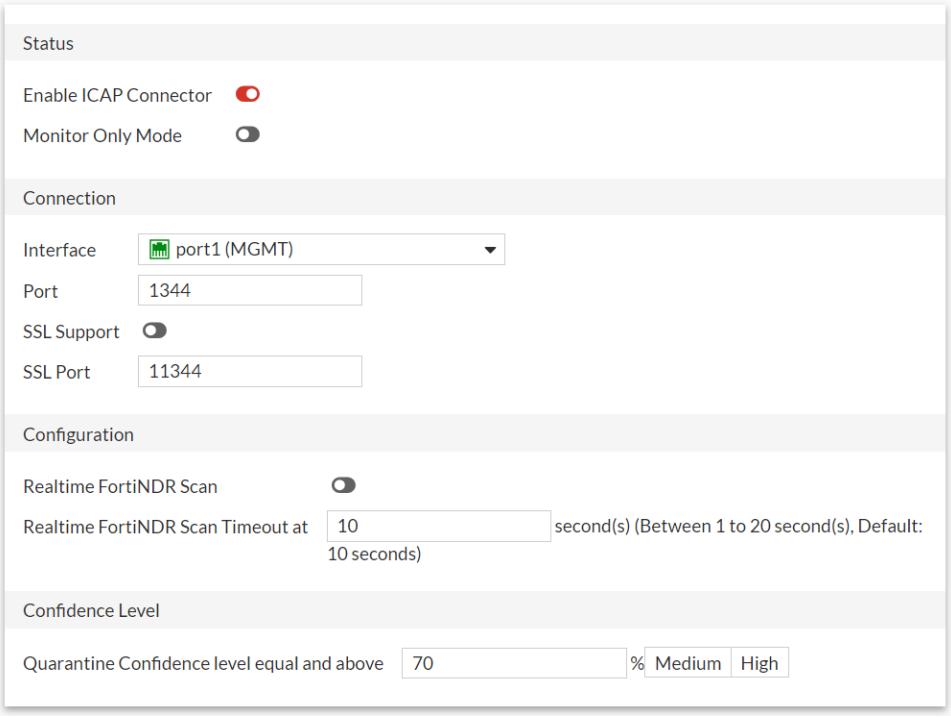
1. In FortiGate:
   a. Add the ICAP server.
   b. Create an ICAP profile.
   c. Add the ICAP profile to a policy.
   For more information, see ICAP in the *FortiOS Administration Guide*.
2. In FortiNDR, configure the ICAP server.

To enable ICAP in FortiNDR:

1. Go to *Security Fabric > Fabric Connectors* and click the *ICAP* card.
2. 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. You cannot enable realtime FortiNDR scan configuration and change the confidence level.
Connection	
Interface	Select an interface from the dropdown.
Port	Enter port the connector will use to connect 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, FortiNDR will 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*.



Security Fabric Connector

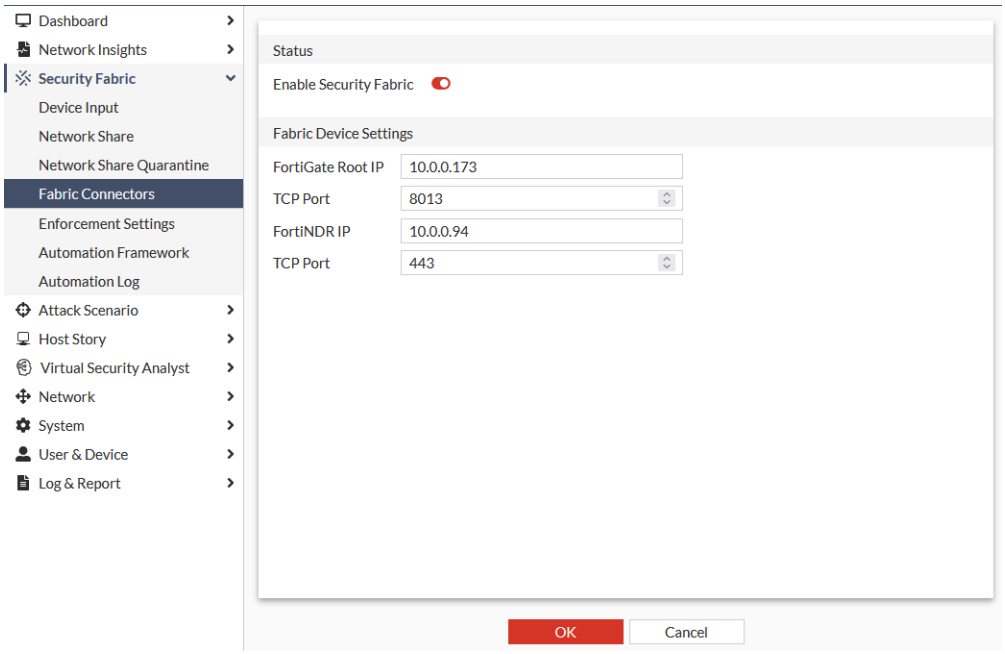
FortiNDR 1.5.0 and FortiOS 7.0.0, FortiNDR can join FortiGate Security Fabric. After connecting to the Security Fabric, FortiNDR can share information such as FortiNDR system information and malware types detected.

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.

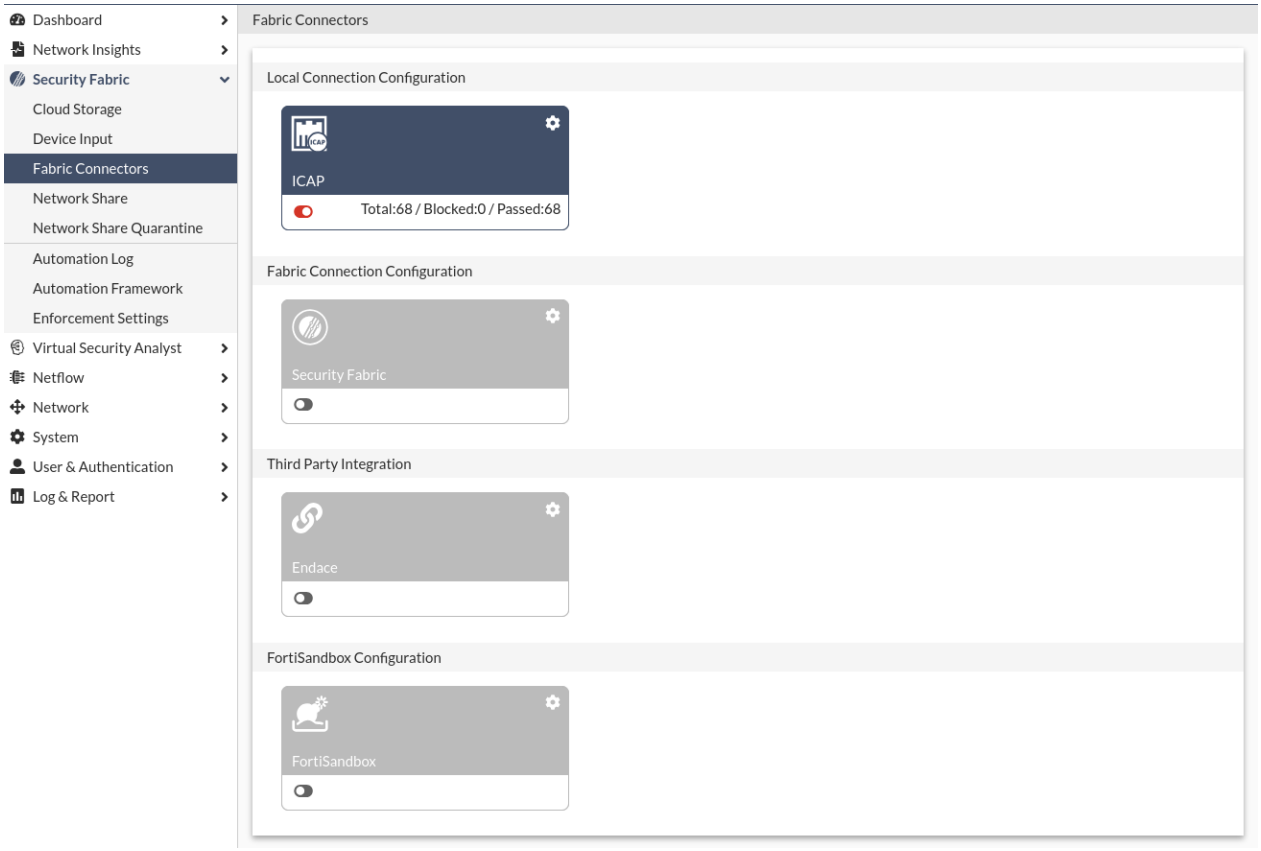


Endace

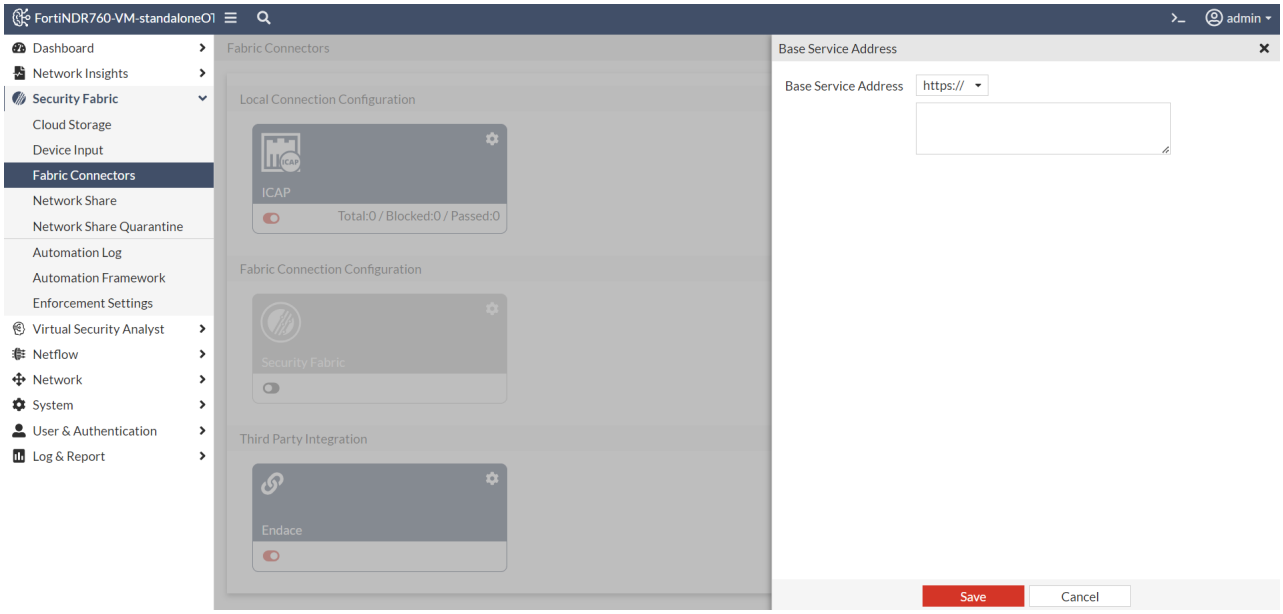
The Endace fabric connector allows you to investigate the PCAP related to the IP addresses. This integration is available in Standalone and Sensor modes.

To integrate FortiNDR with Endace:

1. Go to *Security Fabric > Fabric Connectors*.
2. Under *Third Party Integration*, click the gear icon in the *Endace* tile. The *Base Service Address* pane opens.



3. Enter the Endace URL address and click *Save*.



To disable the Endace connector

1. Go to *Security Fabric* > *Fabric Connectors*.
2. In the *Endace* tile, click the toggle to disable the connector. The existing base URL is erased.

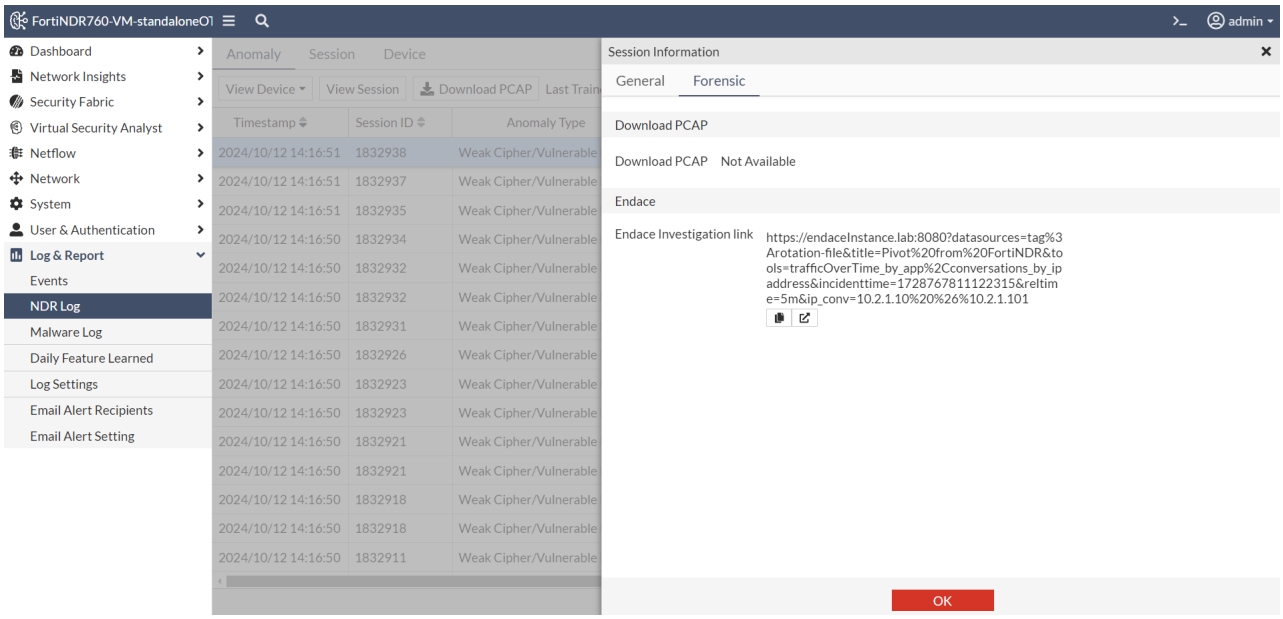
To enable the connector, you will need to re-enter the base URL

Viewing Forensic data

The *Endace* connector supports pivoting results from NDR findings to the Endace GUI.

To view the forensic data:

1. Go to *Log & Report* > *NDR Log*.
2. In the *NDR Detection*or *Observation* tab, click a session in the table. The *Session Information* page opens.
3. Click the *Forensic* tab.



4. To view the information related to the session on the Endace Deployment, do one of the following:
   - Click the *Copy* icon to copy the link.

     
   - Click the *Open* icon to open the link in a new tab.

FortiSandbox

> This topic describes the Fabric Connector workflow where FortiNDR sends files to FortiSandbox for verification. For the Entrust API workflow, see FortiSandbox integration (FortiSandbox 4.0.1 and higher) on page 153.

FortiNDR supports integration with FortiSandbox to verify whether suspicious malware files detected by FortiNDR are false positives. Once a successful connection is established, FortiNDR submits the detected files to FortiSandbox for analysis within a secure and isolated environment. The final verdict returned by FortiSandbox is used to confirm or override the initial detection result.

- If the FortiSandbox verdict aligns with the original FortiNDR detection, the FortiNDR result is retained.
- If the verdict differs, the detection is treated as a false positive and the result is updated to *Clean*.

For all successfully validated files, the FortiSandbox column in the log displays *Evaluated*.

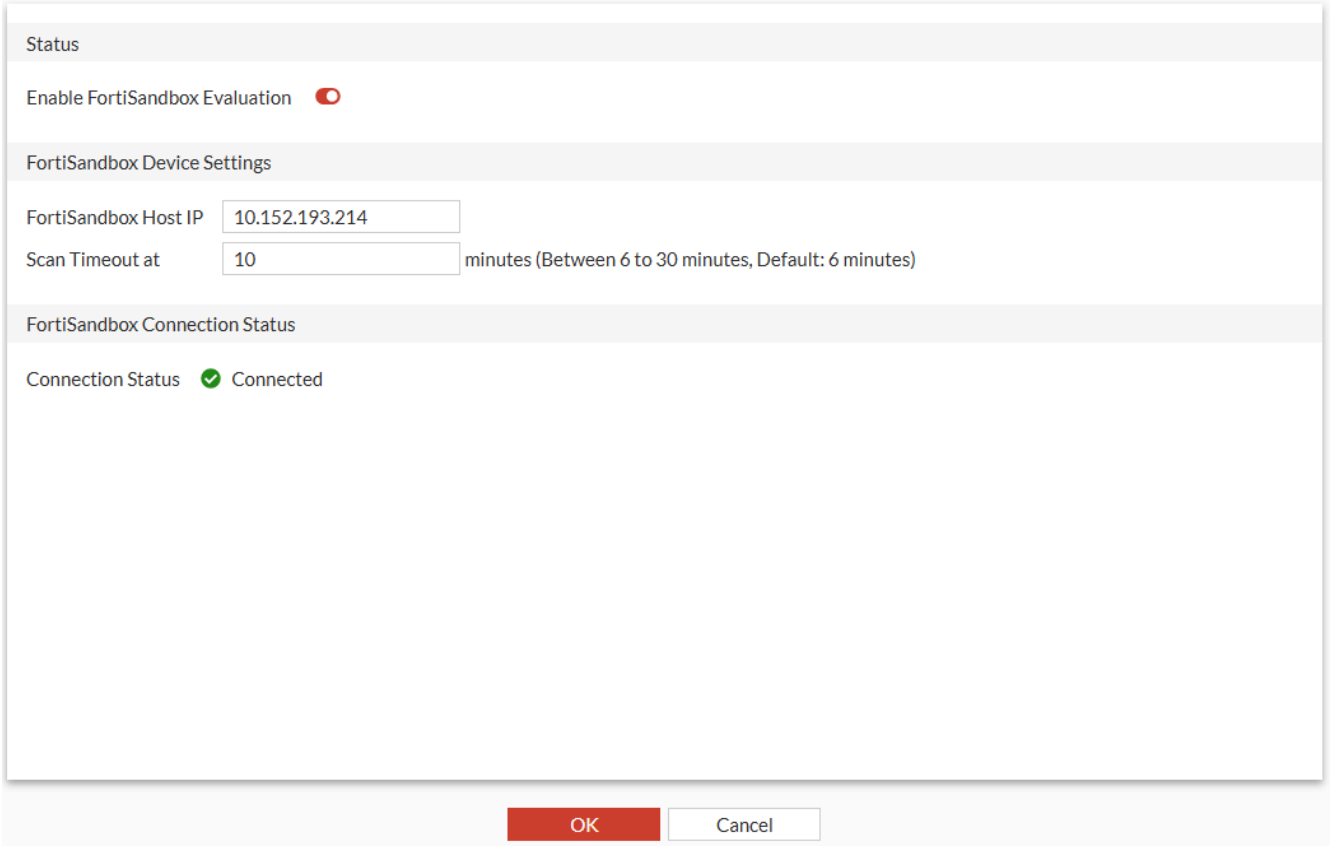
If validation fails due to a timeout or other issues, the status is displayed as *Evaluation Failed*.

Before configuring the connector, ensure that the FortiNDR device has direct network reachability to the FortiSandbox host, and that FortiNDR is authorized on the FortiSandbox host under *Security Fabric > Device*.

To configure the FortiSandbox connector:

1. Go to *Security Fabric > Fabric Connectors*, and click the *FortiSandbox* card.
2. Click *Enable FortiSandbox Verification* to activate the connector.
3. Enter the *FortiSandbox Host IP*.
4. (Optional) Adjust the *Scan Timeout at* interval. The configurable range is 6–30 minutes (default is 6 minutes).
5. Click *OK*.

Once configured, wait for the *Connection Status* to display *Connected* to confirm communication. After the connection is established, FortiNDR automatically submits detected malware files to FortiSandbox and updates results when false positives are identified, improving overall detection accuracy.



Viewing FortiSandbox scan results

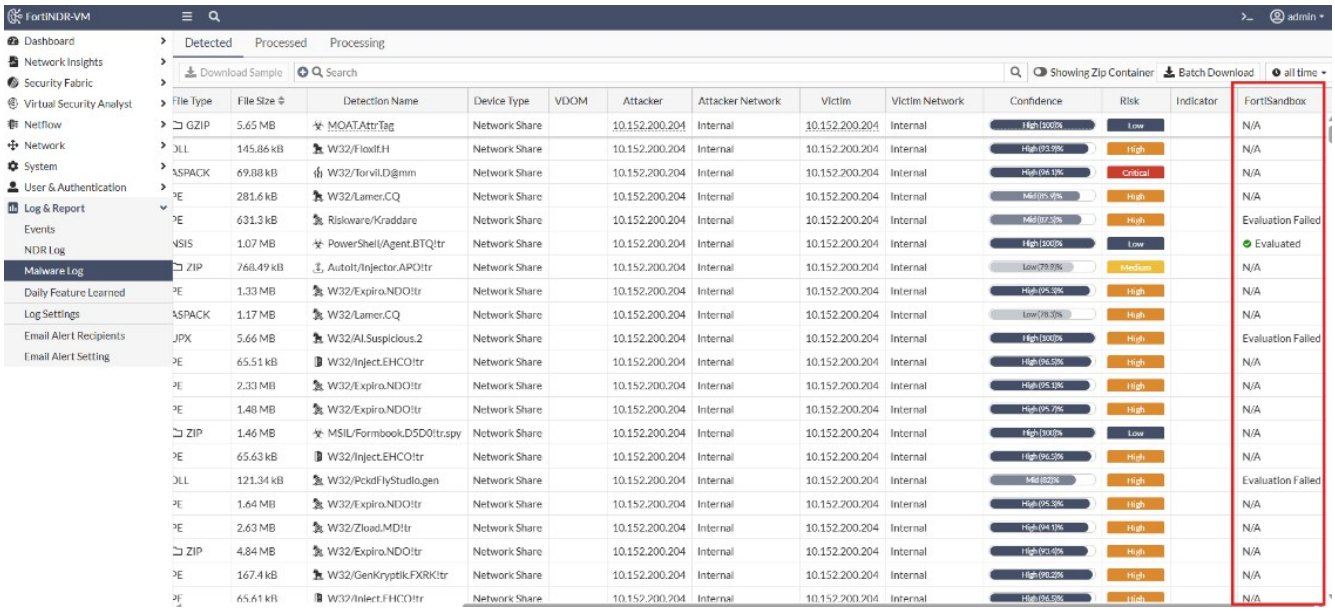
When the FortiSandbox connector is enabled and functioning properly, the evaluated results will appear in the page in the *FortiSandbox* column. There are three possible verification results: *N/A*, *Evaluated*, and *Evaluation Failed*.

- *N/A* indicates that the file has no risk and does not require further verification.
- *Evaluated* or *Evaluation Failed* indicates the file was submitted to FortiSandbox for additional analysis.

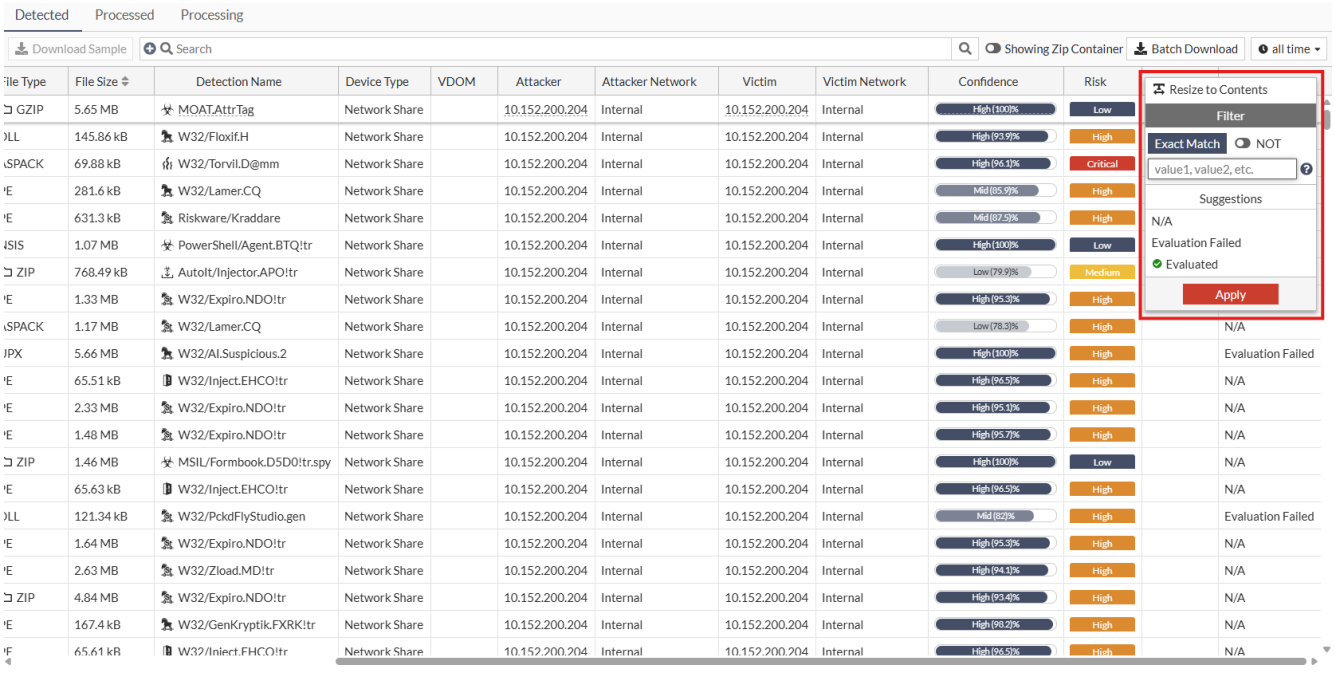
For files with an *Evaluated* status:

- If FortiSandbox confirms the presence of malware, FortiNDR will retain its original detection result.
- If FortiSandbox determines that no malware is present, the file should be classified as a *false positive*, and the result will be updated to *Clean*.

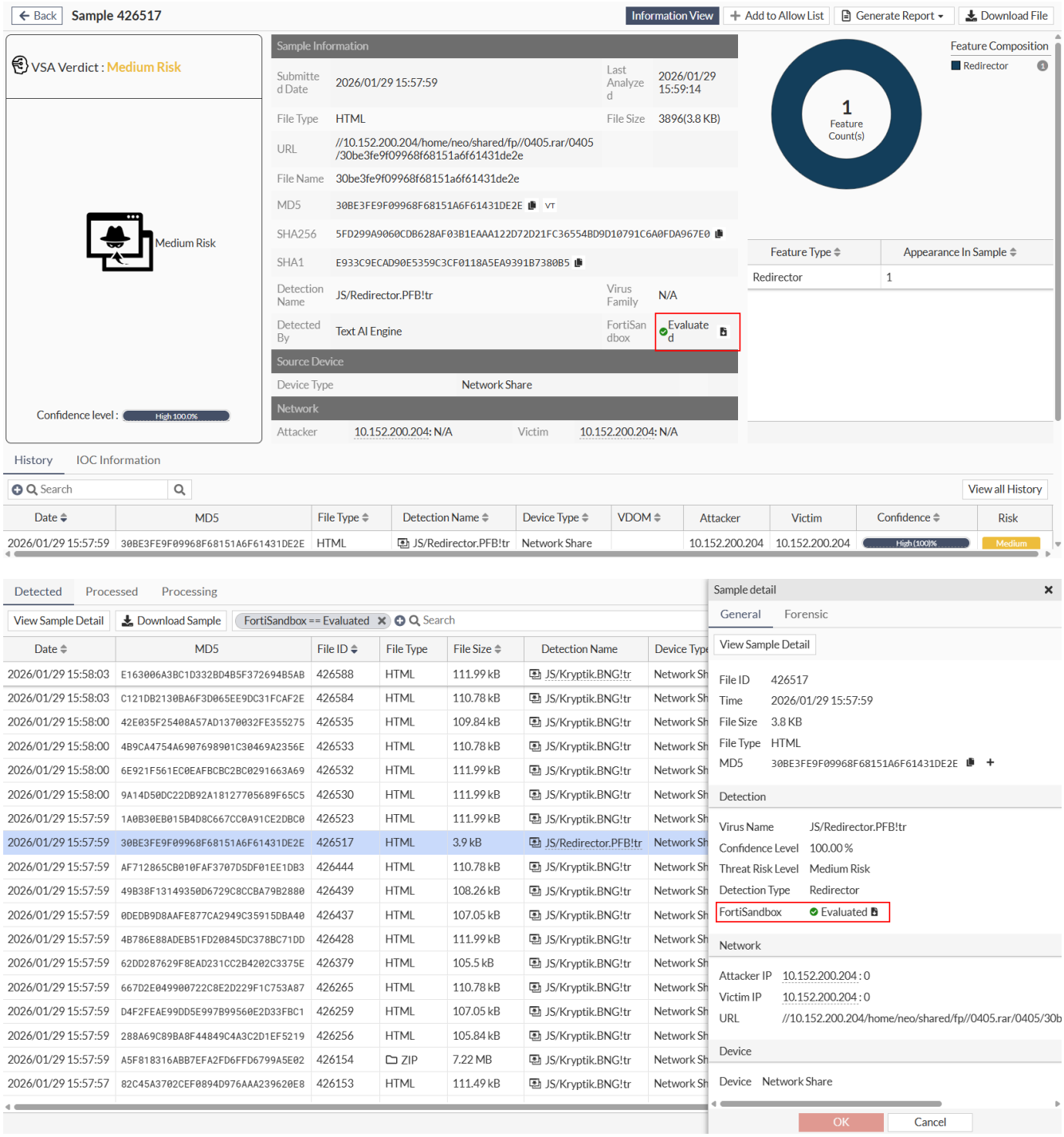
A result of *Evaluation Failed*, may indicate that the file type is not supported by FortiSandbox, the scan timed out, or an issue occurred during the verification process. In these cases, FortiNDR will retain its original detection result.



To filter the *FortiSandbox* column, click it then choose which result types to show. You can select one or multiple types.



A FortiSandbox PDF report can be downloaded for evaluated malware file once the report is available. To download it, click the *download* icon located beside the verification result on the *Sample Detail* page.


Back
Sample 426517
Information View
Add to Allow List
Generate Report
Download File
VSA Verdict : Medium Risk
Medium Risk
Confidence level : High 100.0%
Sample Information
Submitted Date 2026/01/29 15:57:59
Last Analyzed 2026/01/29 15:59:14
File Type HTML
File Size 3896(3.8 KB)
URL //10.152.200.204/home/neo/shared/fp//0405.rar/0405/30be3fe9f09968f68151a6f61431de2e
File Name 30be3fe9f09968f68151a6f61431de2e
MD5 30BE3FE9F09968F68151A6F61431DE2E
SHA256 5FD299A9060CDB628AF03B1EAAA122D72D21FC36554BD9D10791C6A0FDA967E0
SHA1 E933C9ECAD90E5359C3CF0118A5EA9391B7380B5
Detection Name JS/Redirector.PFB!tr
Virus Family N/A
Detected By Text AI Engine
FortiSandbox Evaluated
Source Device
Device Type Network Share
Network
Attacker 10.152.200.204: N/A
Victim 10.152.200.204: N/A
Feature Composition
Redirector
1
Feature Count(s)
Feature Type
Appearance In Sample
Redirector 1
History
IOC Information
Search
View all History
Date
MD5
File Type
Detection Name
Device Type
VDOM
Attacker
Victim
Confidence
Risk
2026/01/29 15:57:59 30BE3FE9F09968F68151A6F61431DE2E HTML JS/Redirector.PFB!tr Network Share 10.152.200.204 10.152.200.204 High (100)% Medium
Detected
Processed
Processing
View Sample Detail
Download Sample
FortiSandbox == Evaluated
Search
Date
MD5
File ID
File Type
File Size
Detection Name
Device Type
2026/01/29 15:58:03 E163006A3BC1D332BD4B5F372694B5AB 426588 HTML 111.99 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:58:03 C121DB2130BA6F3D065EE9DC31FCAF2E 426584 HTML 110.78 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:58:00 42E035F25408A57AD1370032FE355275 426535 HTML 109.84 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:58:00 4B9CA4754A6907698901C30469A2356E 426533 HTML 110.78 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:58:00 6E921F561EC0EAFBCBC2BC0291663A69 426532 HTML 111.99 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:58:00 9A14D50DC22DB92A18127705689F65C5 426530 HTML 111.99 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 1A0B30EB015B4D8C667CC0A91CE2DBC0 426523 HTML 111.99 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 30BE3FE9F09968F68151A6F61431DE2E 426517 HTML 3.9 kB JS/Redirector.PFB!tr Network Sh
2026/01/29 15:57:59 AF712865CB010FAF3707D5DF01EE1DB3 426444 HTML 110.78 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 49B38F13149350D6729C8CCBA79B2880 426439 HTML 108.26 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 0DEDB9D8AAFE877CA2949C35915DBA40 426437 HTML 107.05 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 4B786E88ADEB51FD20845DC378BC71DD 426428 HTML 111.99 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 62DD287629F8EAD231CC2B4202C3375E 426379 HTML 105.5 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 667D2E049900722C8E2D229F1C753A87 426265 HTML 110.78 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 D4F2FEAE99DD5E997B99560E2D33FBC1 426259 HTML 107.05 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 288A69C89BA8F44849C4A3C2D1EF5219 426256 HTML 105.84 kB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:59 A5F818316ABB7EFA2FD6FFD6799A5E02 426154 ZIP 7.22 MB JS/Kryptik.BNG!tr Network Sh
2026/01/29 15:57:57 82C45A3702CEF0894D976AAA239620E8 426153 HTML 111.49 kB JS/Kryptik.BNG!tr Network Sh
Sample detail
General
Forensic
View Sample Detail
File ID 426517
Time 2026/01/29 15:57:59
File Size 3.8 KB
File Type HTML
MD5 30BE3FE9F09968F68151A6F61431DE2E
Detection
Virus Name JS/Redirector.PFB!tr
Confidence Level 100.00 %
Threat Risk Level Medium Risk
Detection Type Redirector
FortiSandbox Evaluated
Network
Attacker IP 10.152.200.204 : 0
Victim IP 10.152.200.204 : 0
URL //10.152.200.204/home/neo/shared/fp//0405.rar/0405/30b
Device
Device Network Share
OK
Cancel

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 observations when executing enforcement. These policies include *Event Category*, *NDR Detection Severity Level*, *Malware Risk Level*, *Malware Confidence Level*, and *Allow List*.

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

Creating enforcement profiles

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

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

Duplicate detections

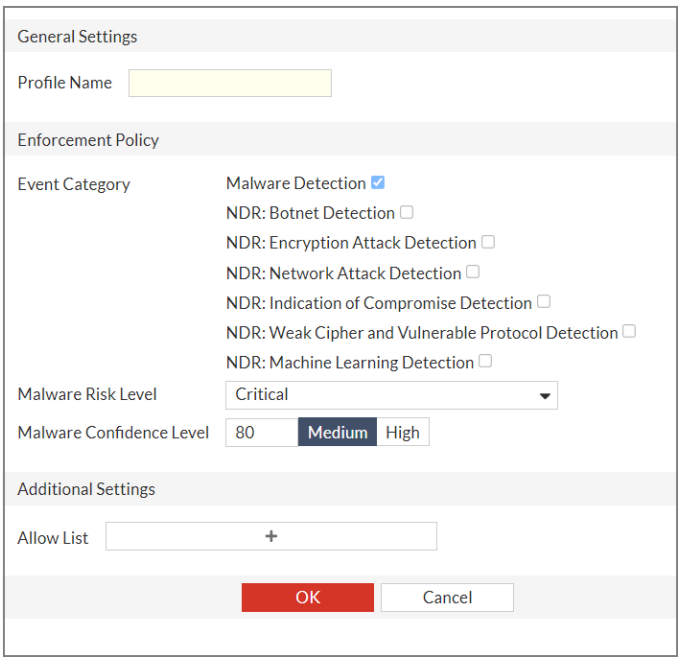
- A response is only triggered once when multiple events in NDR detections in the same category (e.g. IOC campaign) occurs within one minute.
- IA response is recorded as a duplicate when multiple events in NDR detections in the same category occur every minute after that.

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*.

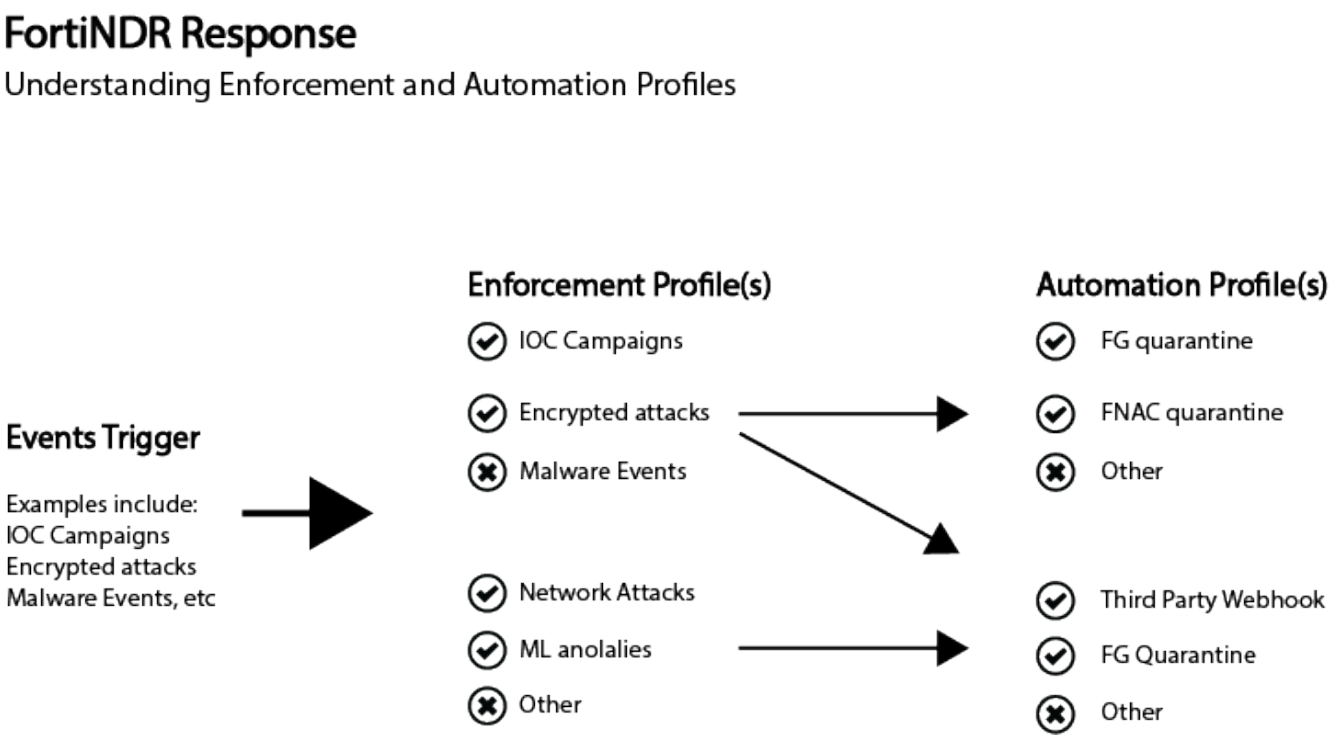
Profile Name	Enter a name for the profile.
Enforcement Policy	
Event Category	Select one of the following options: • *Malware Detection* • *NDR: Botnet Detection* • *NDR: Encryption Attack Detection* • *NDR: Network Attack Detection* • *NDR: Indication of Compromise Detection* • *NDR: Weak Cipher and 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.



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.

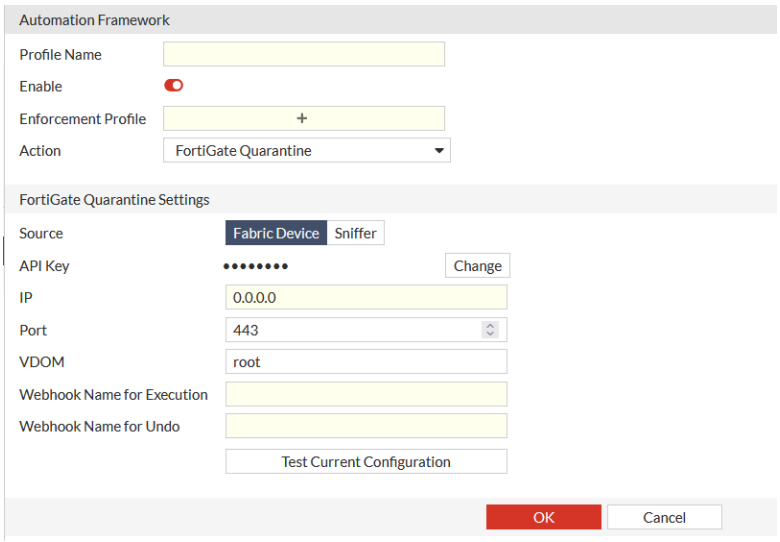


NDR Muted Resultswill not be included in the quarantine response.

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:

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* • *FortiProxy Quarantine* • *Generic Webhook*



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

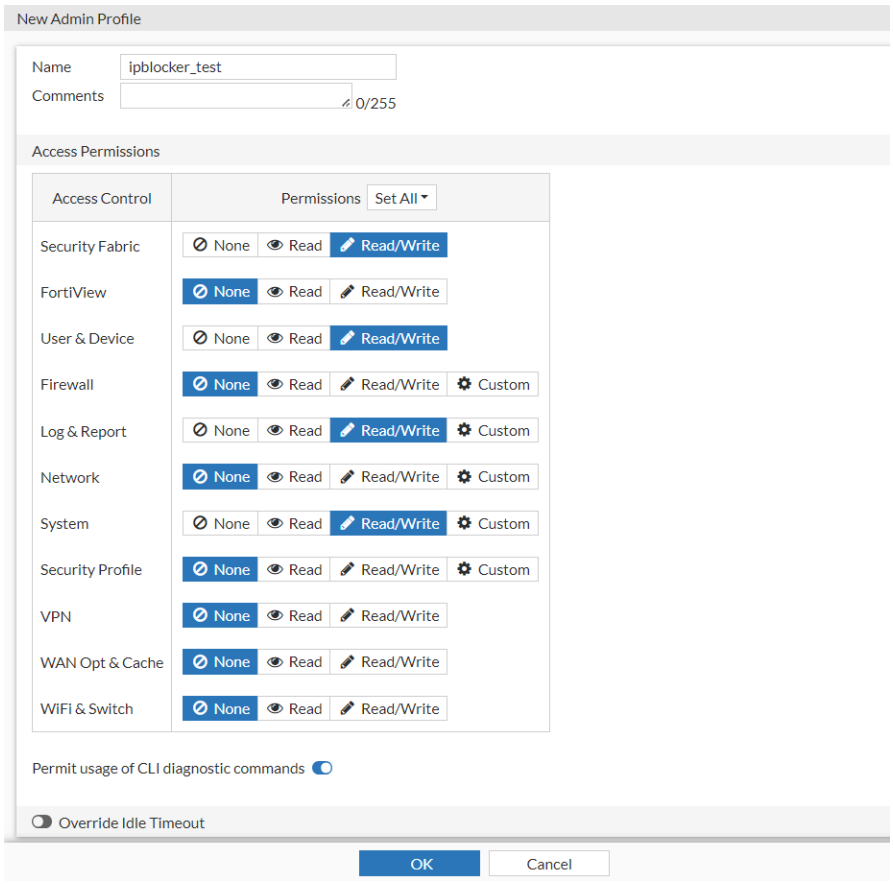
To create an automation profile for *FortiGate Quarantine* or *FortiSwitch Quarantine via FortiLink*, the incoming webhook needs to be setup on FortiGate to accept requests from FortiNDR. You can register them in *Security Fabric > Automation Framework*.

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:

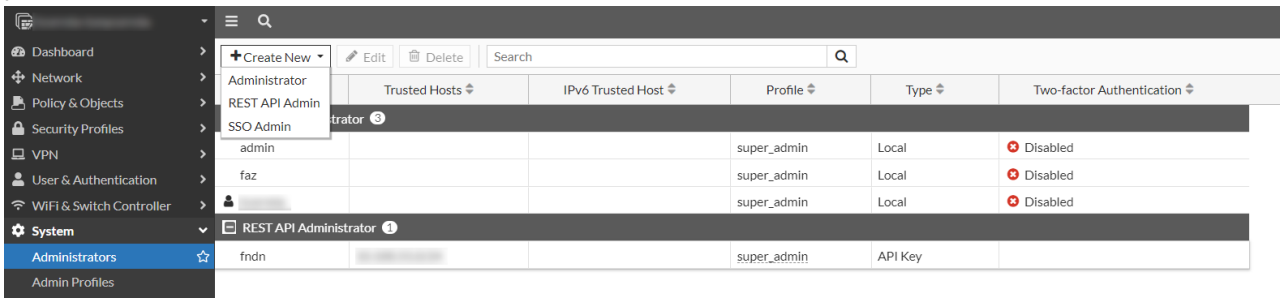
1. In FortiGate, go to *System > Admin Profiles* and create a profile, for example, *ipblocker_test* and set the following *Access Permissions*.

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



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

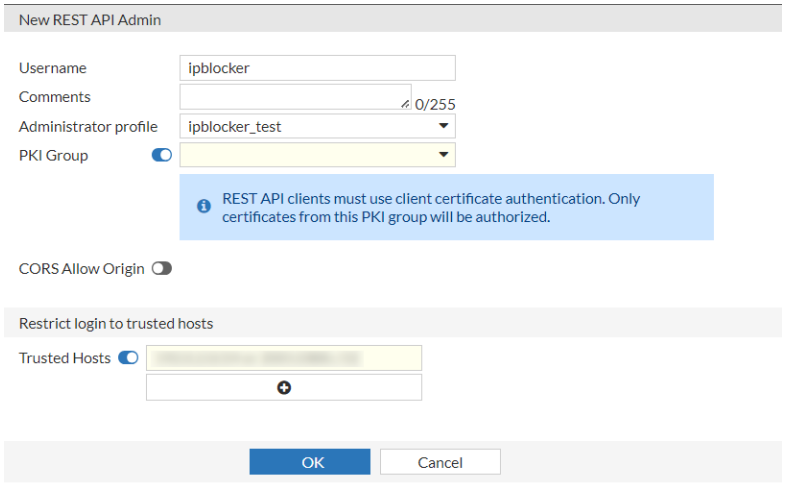
2. In FortiGate, go to *System* > *Administrators* and create a *REST API Admin* using the *ipblocker_test* admin profile.



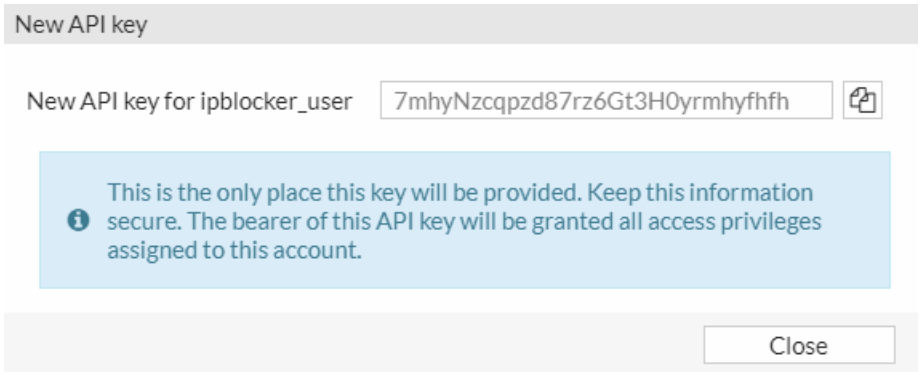
3. Configure the administrator settings:

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.



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



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

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

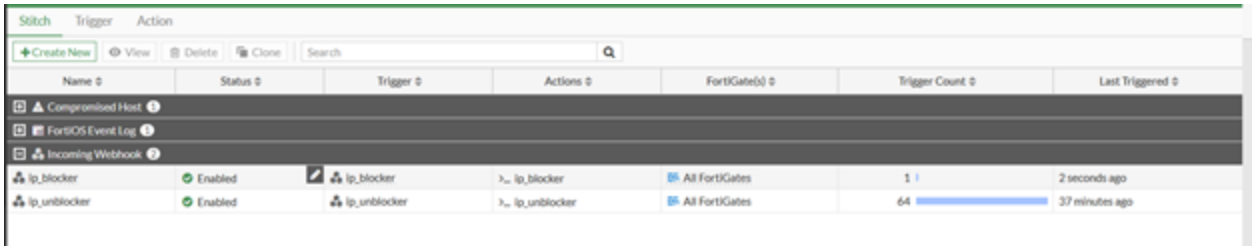
This example requires two webhooks, one that executes the Ban IP action (this *ip_blocker* example). Another webhook executes the unban IP action.

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

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

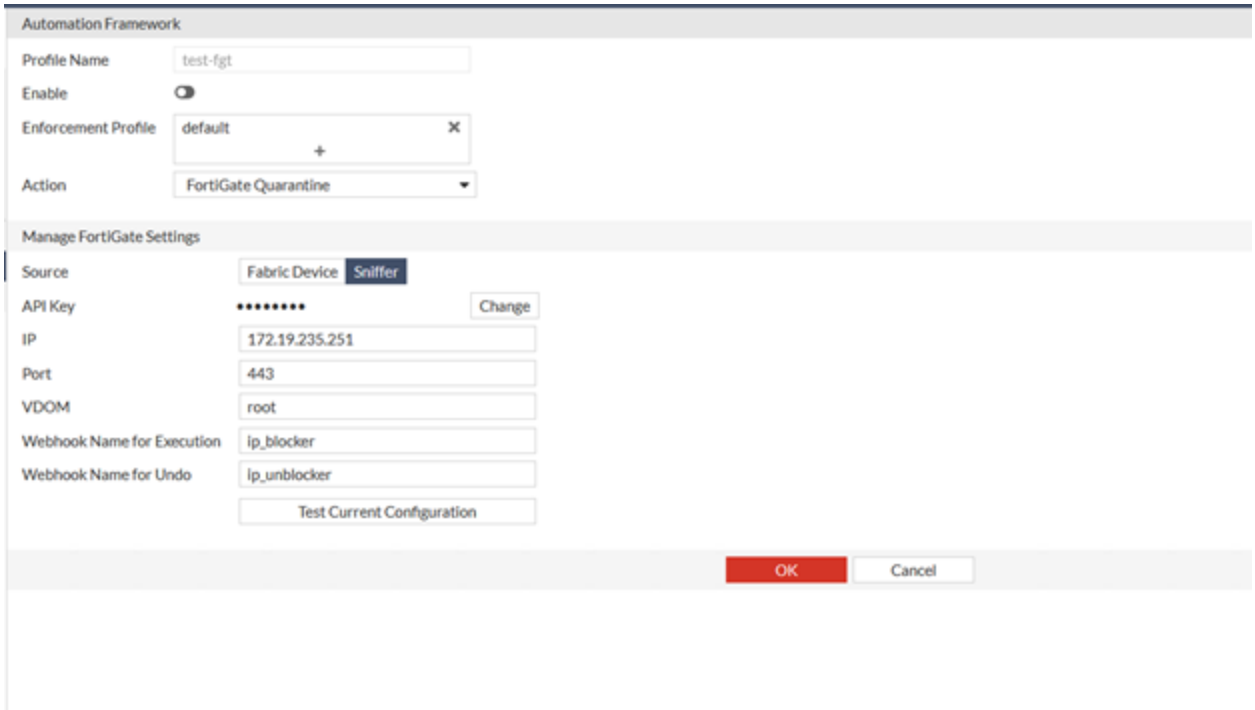
```
config vdom
edit root
diagnose user banned-ip delete src4 %%log.srcip%%
```

FortiOS v7.0.1



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

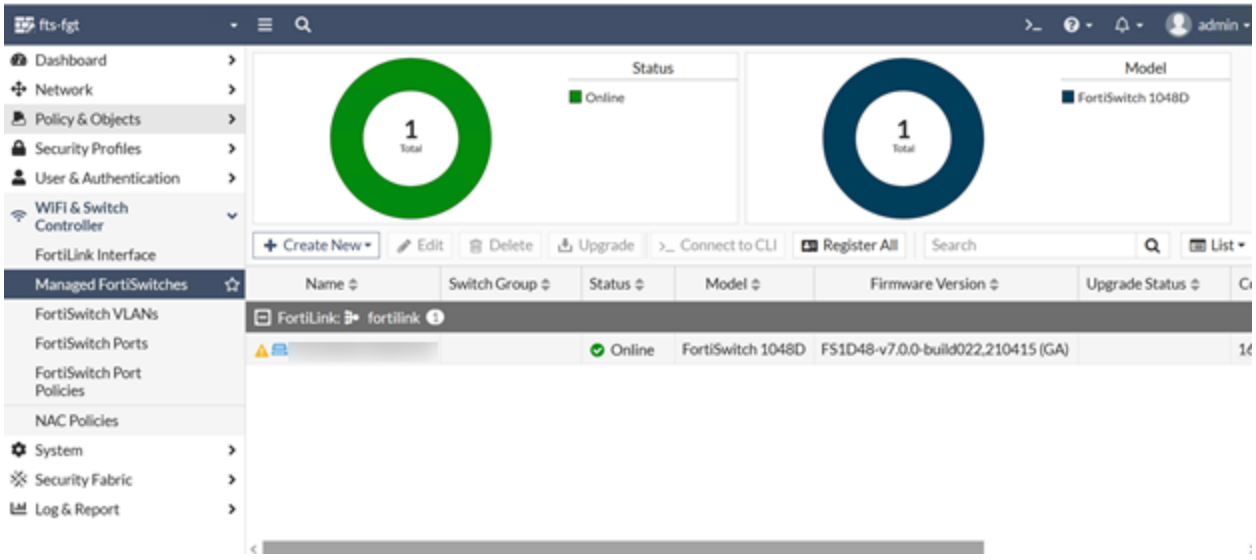
8. Register the Webhook name in the Automation Profile.



FortiSwitch quarantine setup example

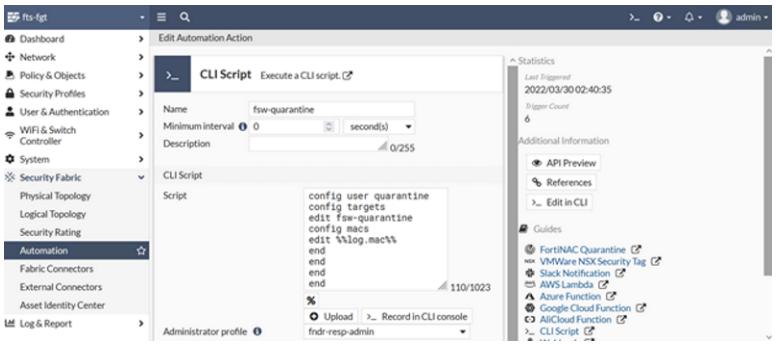
FortiNDR supports quarantining devices that are connected to a FortiSwitch which is managed by FortiGate. FortiSwitch is connected to a FortiGate and is configured in FortiLink mode. FortiNDR will utilize FortiGate's incoming webhook to provide the device's MAC address for quarantine/undo quarantine.

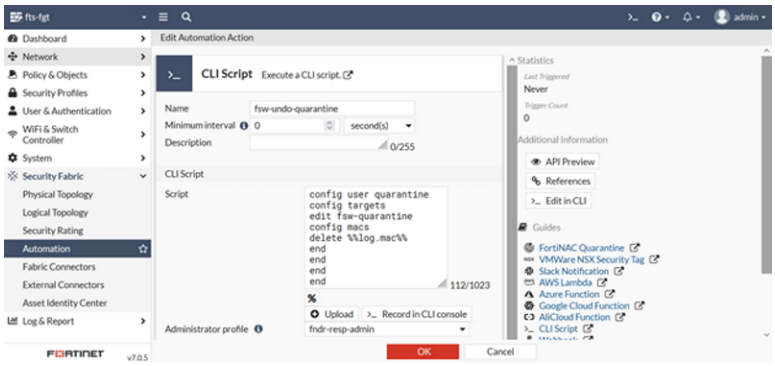
For information about configuring FortiLink, see Configuring FortiLink.



To setup FortiSwitch quarantine on FortiNDR:

1. Following the steps for creating a webhook on FortiGate in FortiGate quarantine webhook setup example on page 140. Note that the CLI script for quarantine and undo quarantine should be updated.

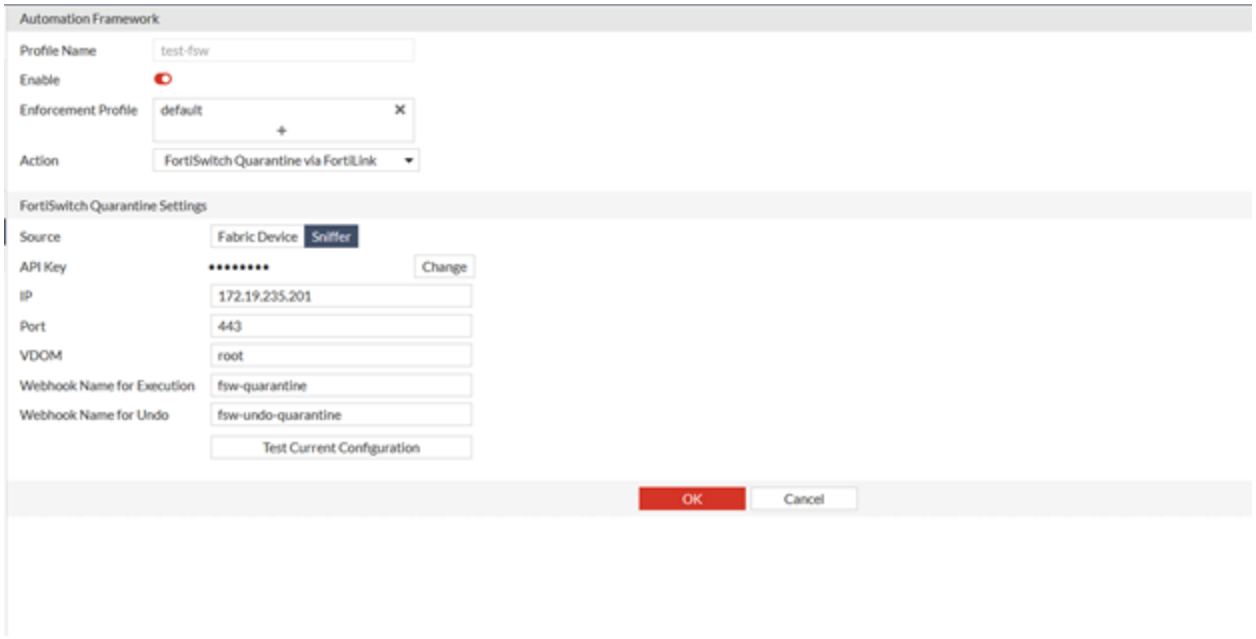




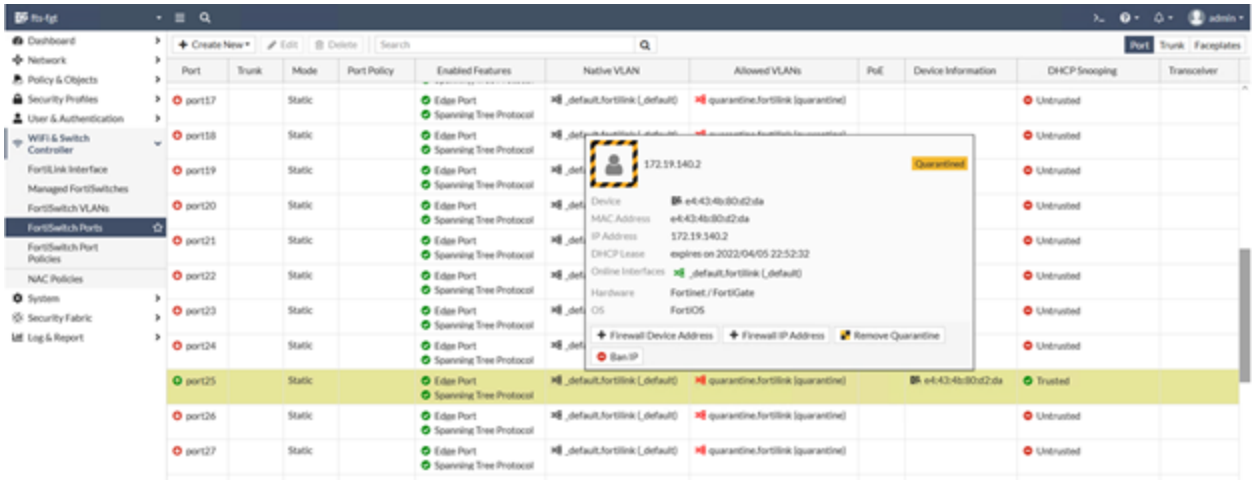
The CLI script for quarantine and undo quarantine should be updated.

2. Register webhooks on FortiNDR .

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



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



4. Click *OK*.

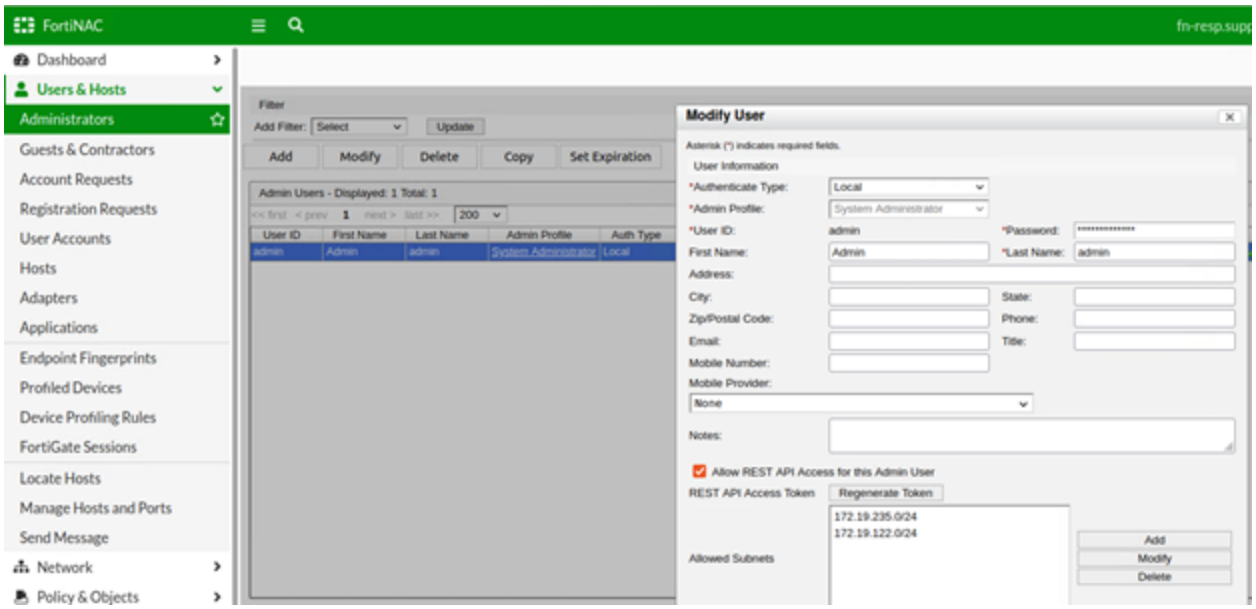
FortiNAC quarantine setup example

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

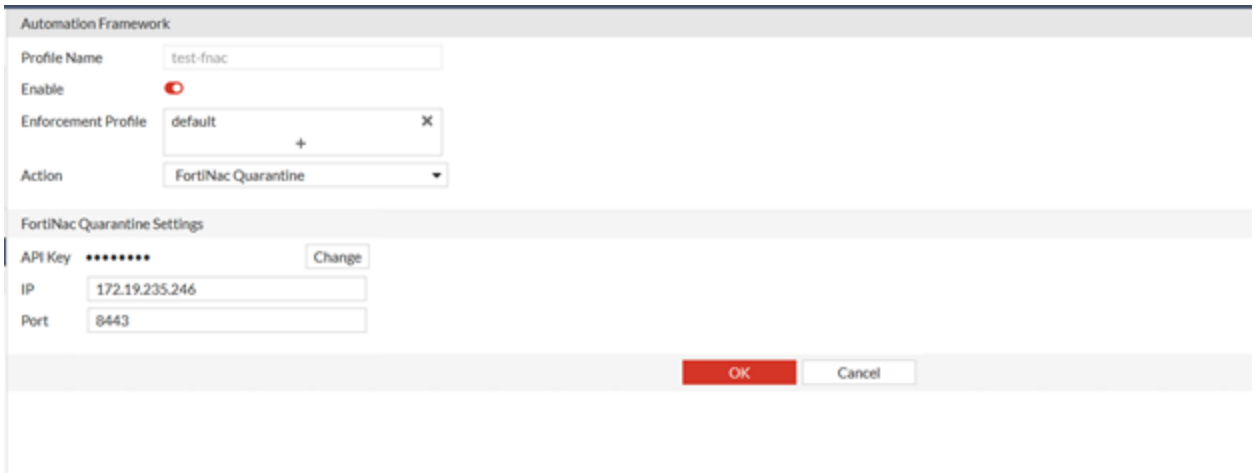
For information about configure FortiNAC, see the *FortiNAC Administration Guide* in the Document Library.

To setup FortiNAC quarantine on FortiNDR:

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



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



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

FortiProxy quarantine webhook setup example

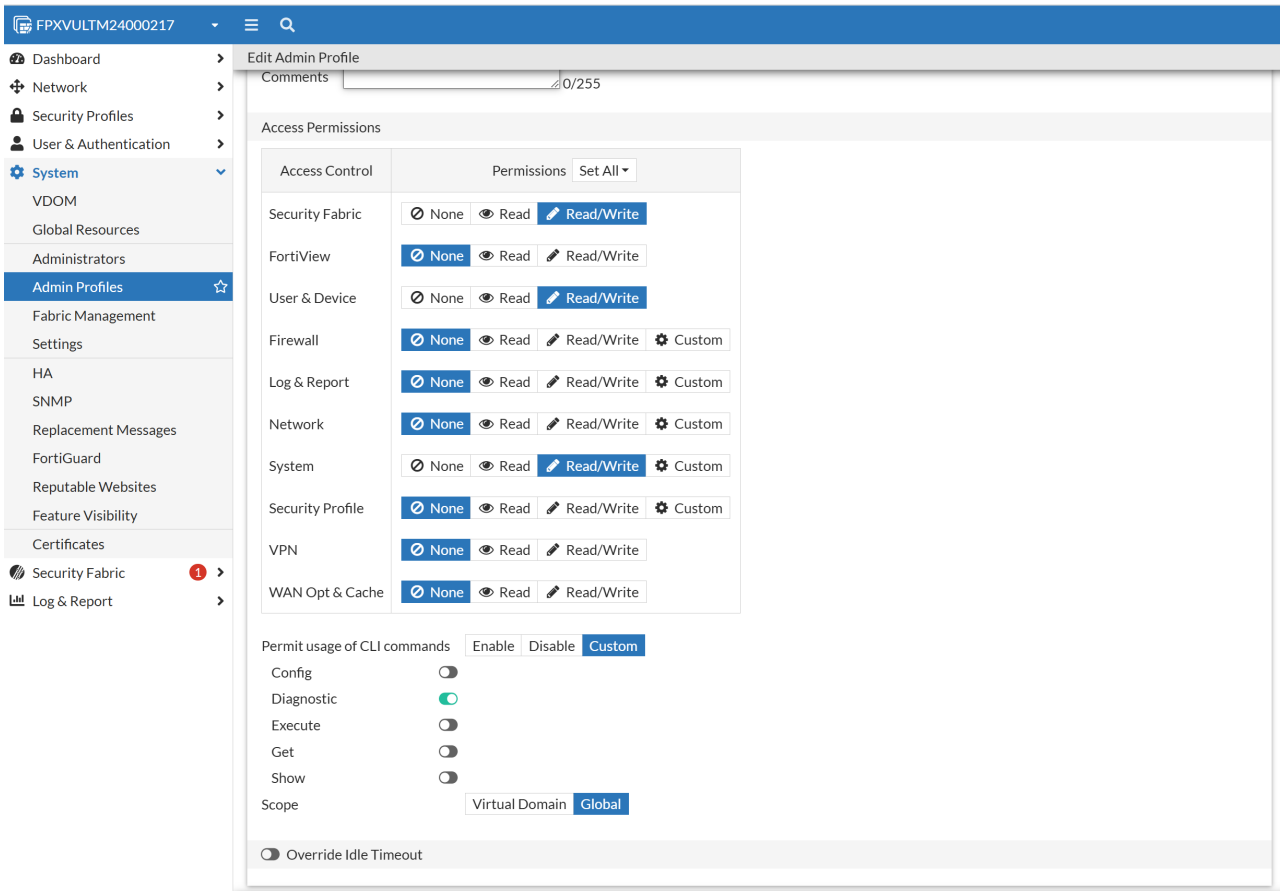
To create an automation profile for *FortiProxy Quarantine* the incoming webhook needs to be setup on FortiProxy to accept requests from FortiNDR. You can register them in *Security Fabric > Automation Framework*.

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

To set up a webhook for Ban IP:

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

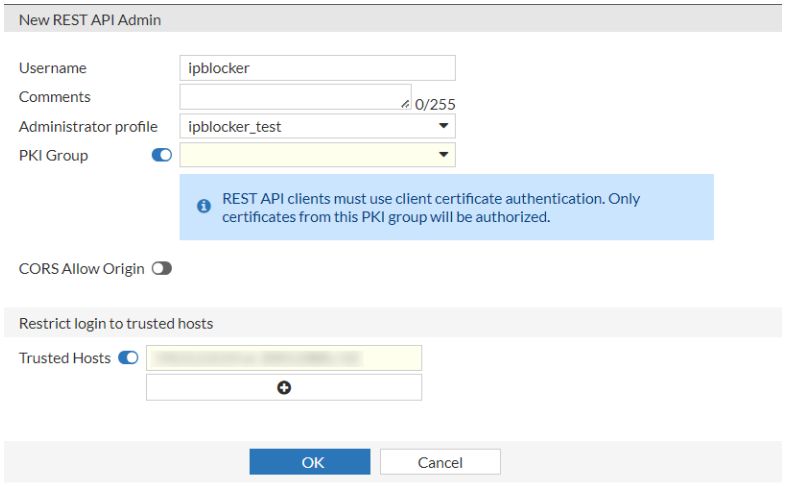
Security Fabric	Read/Write
User & Device	Read/Write
Log & Report	Read/Write
System	Read/Write
Permit usage of CLI diagnostic commands	Custom
Diagnostic	Enable
Scope	Global



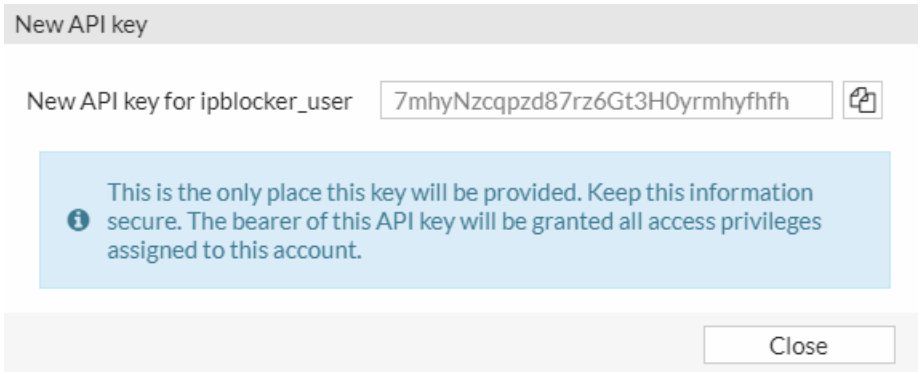
2. In FortiProxy, go to *System* > *Administrators* and create a *REST API Admin* using the admin profile you created in the previous step.
3. Configure the administrator settings:

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	Select the admin profile you created in the previous step. A REST API administrator should have the minimum permissions required to complete the request.
PKI Group	Enable this option for REST API clients and then select which PKI group to accept.
CORS Allow Origin	Enable this option for cross-origin resource sharing (CORS) and then specify the URL that can access the REST API.
Trusted Hosts	Enter the trusted hosts allowed to log in to the REST API.



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



5. In FortiProxy, 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
```

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

If VDOMs are disabled use:

```
diagnose user banned-ip add src4 %%log.srcip%% %%log.expiry%% admin
```

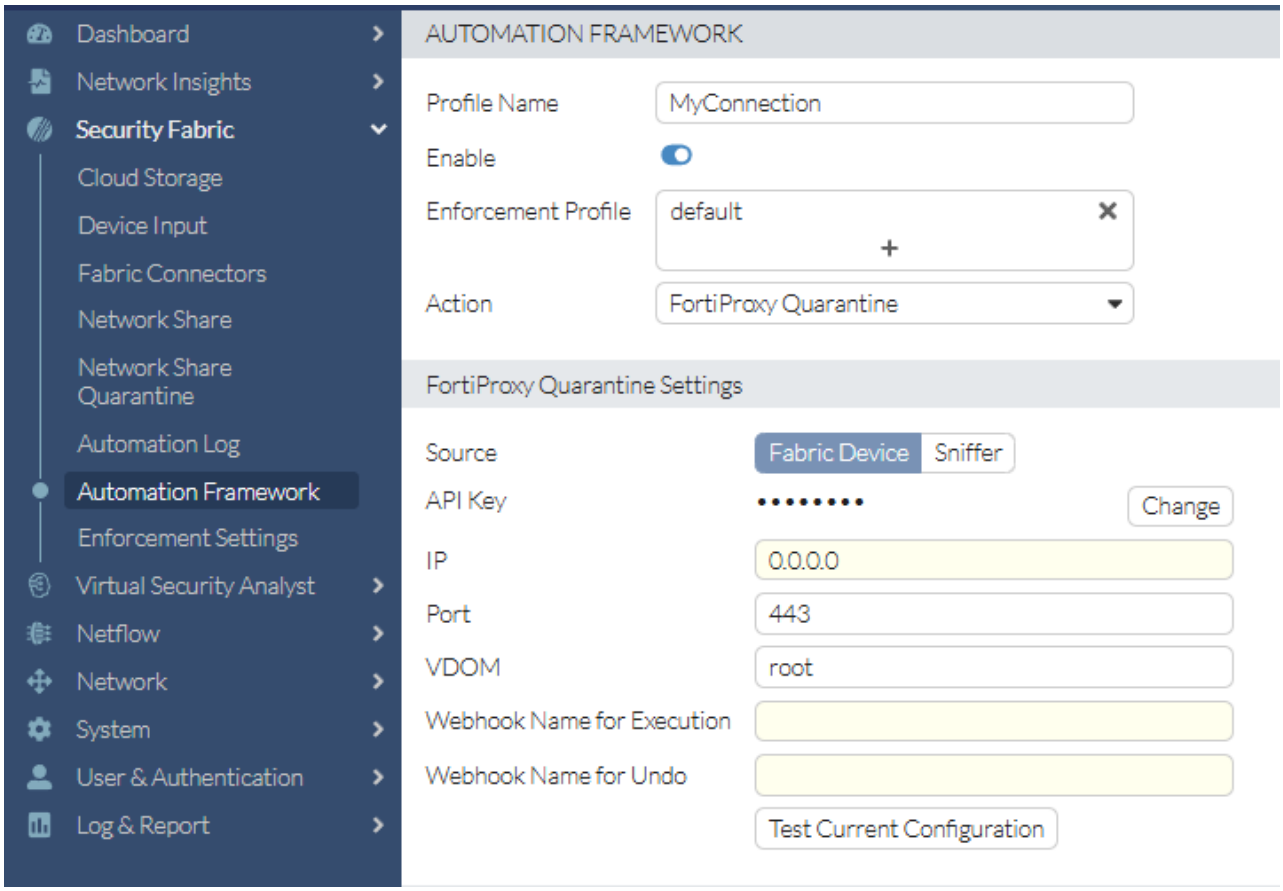
> We recommend maintaining a consistent naming pattern for the Stitch and Trigger names. For example, *ip_blocker* and *ip_unblocker*.

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%%
```

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

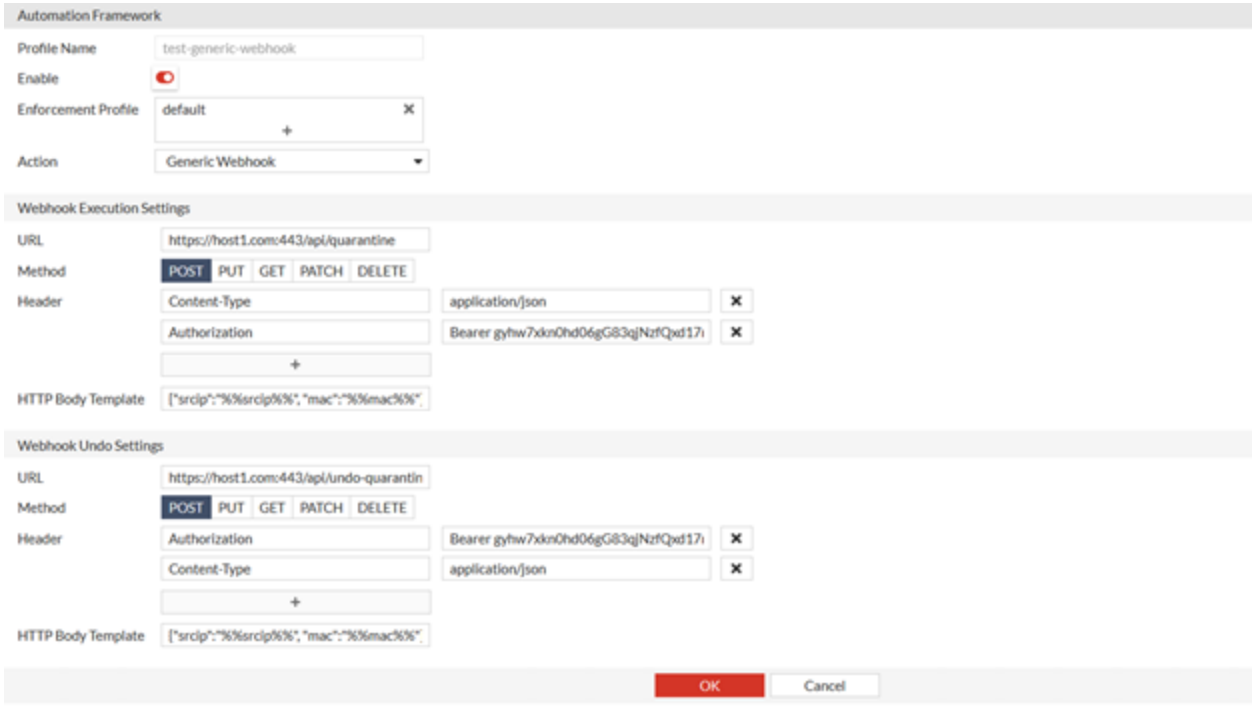
8. In FortiNDR, register the ebhook name in the *Automation Profile*.



Generic Webhook setup example

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

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

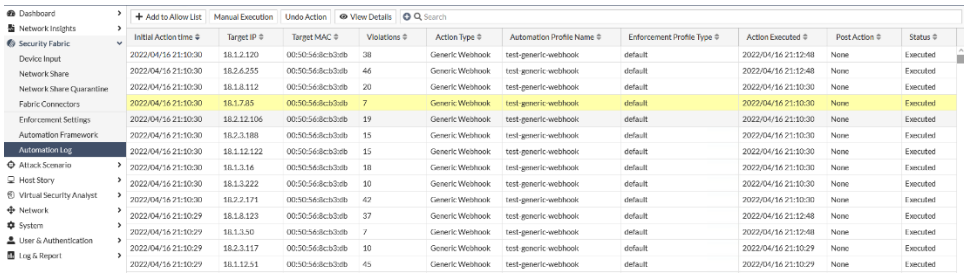


Automation log

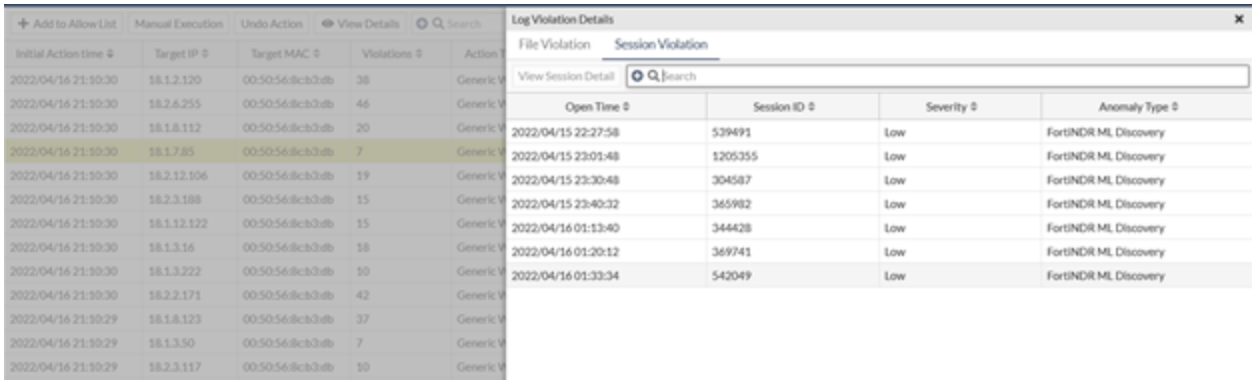
Automation Log records each enforcement action generated by FortiNDR.

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

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



Violation details



Automation Status and Post action

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

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

FortiSandbox integration (FortiSandbox 4.0.1 and higher)

> This topic describes the Entrust API workflow where FortiSandbox sends files to FortiNDR for an additional verdict. For the connector-based workflow, see FortiSandbox on page 132.

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

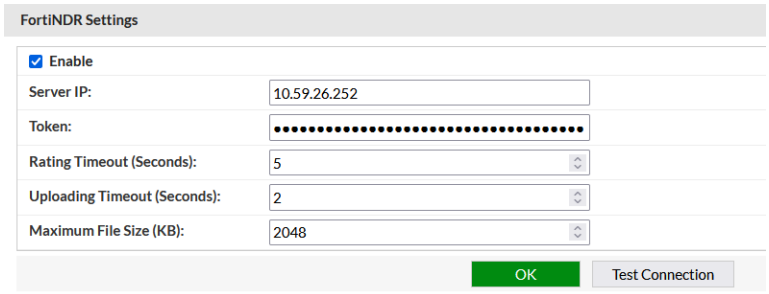
1. FortiSandbox performs its pre-filtering and Static Scan analysis. If any known malware is found, the result is returned.
2. When *FortiNDR Entrust* is enabled under FortiSandbox *Scan Profile*, FortiSandbox sends the files to FortiNDR via API for FortiNDR's verdict of *malware* or *absolute clean*,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

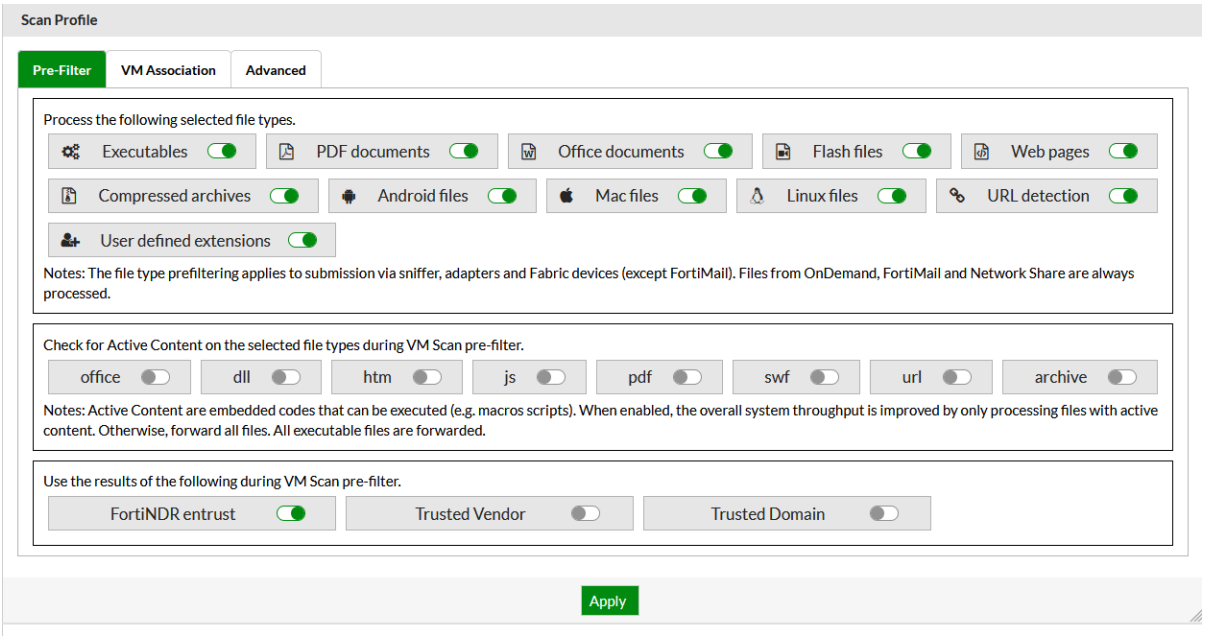
High level configuration steps are as follows:

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 273.
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.



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



FortiGate inline blocking (FOS 7.0.1 and higher)

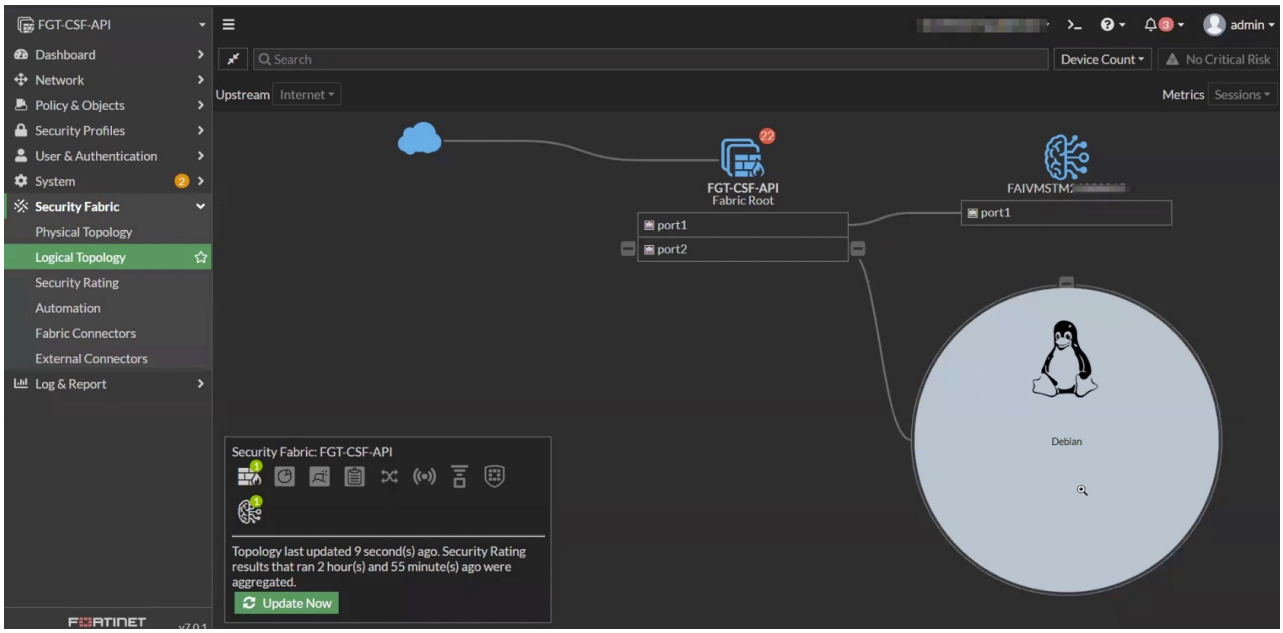
You can configure FortiGate to integrate with FortiNDR using inline blocking. Changes in FortiOS allow the AV profile to configure inline blocking by sending files to FortiNDR for rapid inspection and verdict. FortiGate temporarily holds the user session for FortiNDR to return a clean or malicious verdict, 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 126.
   This is needed for authentication between the two devices before file submission begins.
2. When pairing is complete, verify that FortiNDR appears in the FortiGate topology with the FortiNDR icon in the legend.



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

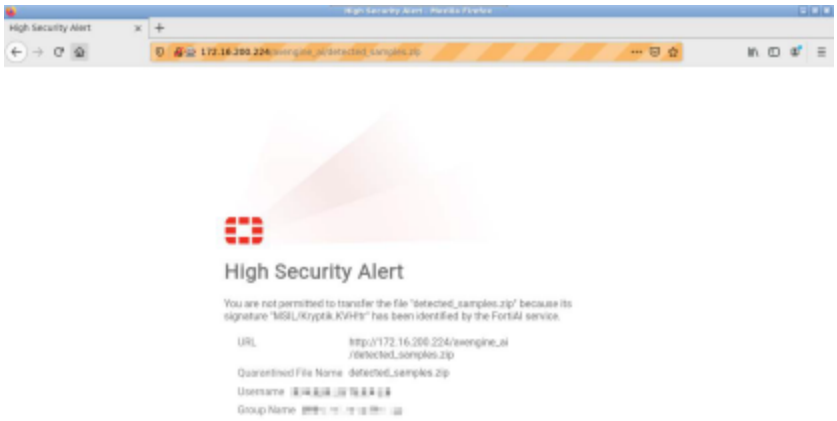
```
Config system fortindr
    Set status enable
End
```

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

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

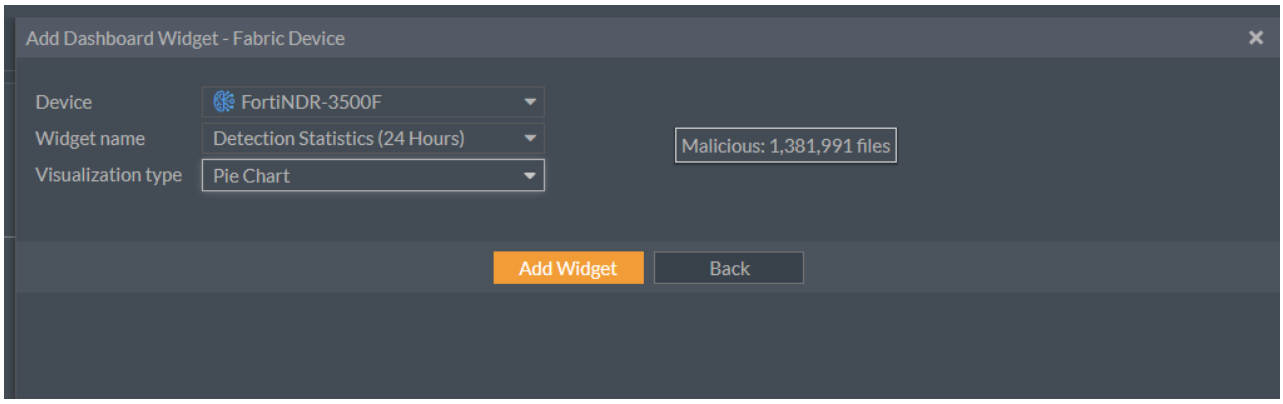
Tips for using FortiNDR inline blocking

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



- For encrypted traffic such as HTTPS, the SSL profile must be configured on FortiGate to extract files in encrypted protocols.
- The maximum file size is determined by both FortiGate and FortiNDR. FortiNDR supports a default maximum file size of 200MB. In FortiNDR the maximum file size can be adjusted with the following CLI command:
  ```
  execute file-size-threshold
  ```
- If there are network connectivity issues that causes a timeout between the connections, FortiGate 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.



FortiNDR inline inspection with other AV inspection methods

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

HTTP, FTP, SSH, and CIFS protocols:

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

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

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

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

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

Accepted file types

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

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

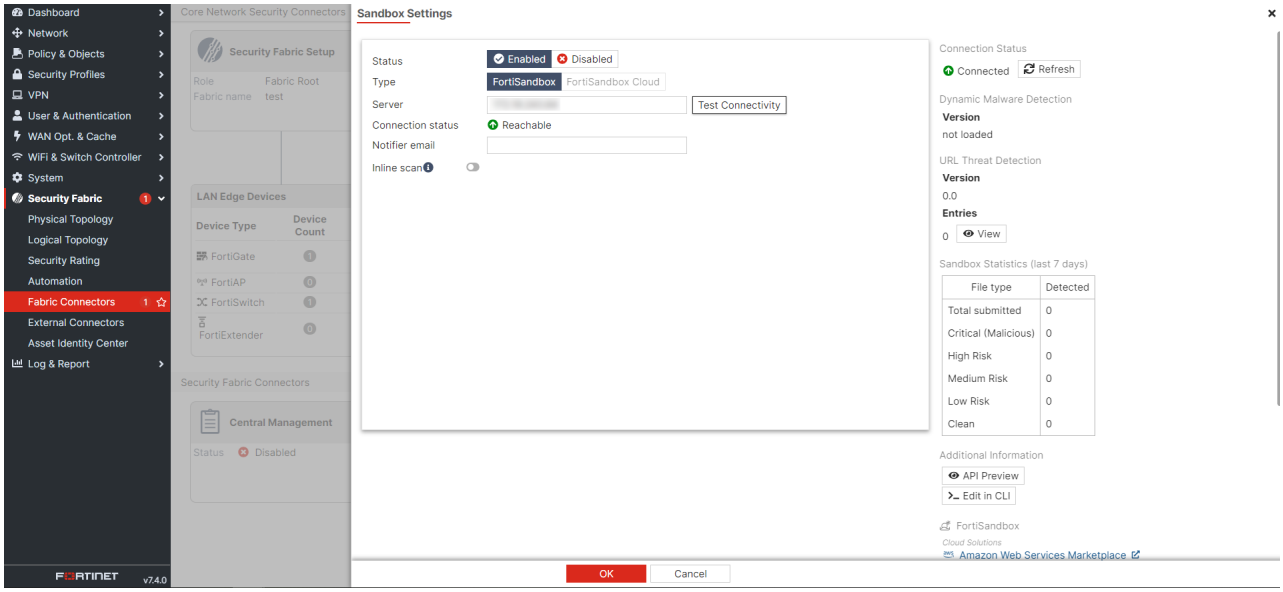
FortiNDR uses the same OFTP (Optimized Fabric Transfer Protocol) over SSL (encrypted) from FortiGate to FortiSandbox. If you are not using FortiSandbox, you can use FortiGate's *Sandbox Inspection* to send files to FortiNDR.

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

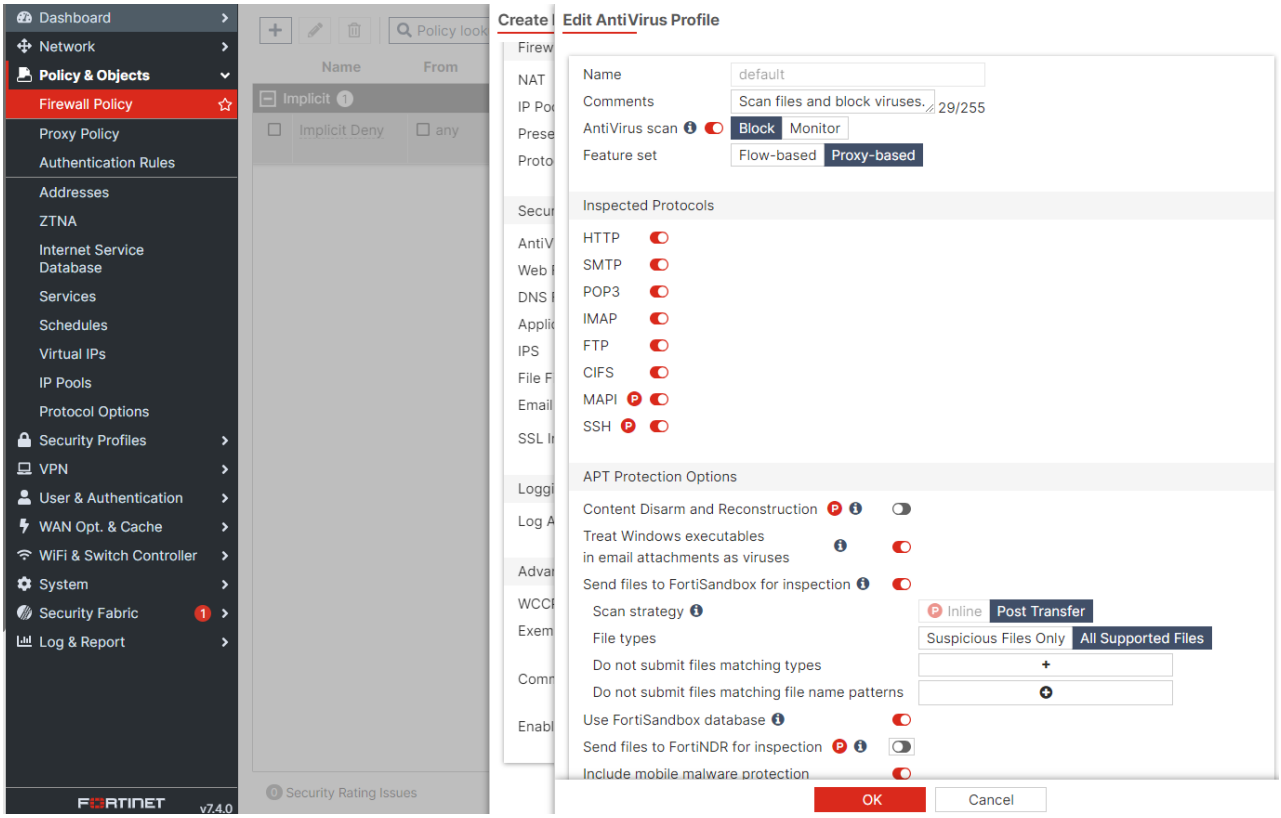
For FortiGate Integration we recommend using FortiGate inline blocking (FOS 7.0.1 and higher) unless the FortiGate/FortiOS version is lower than 7.0.1

To send files from FortiGate to FortiNDR:

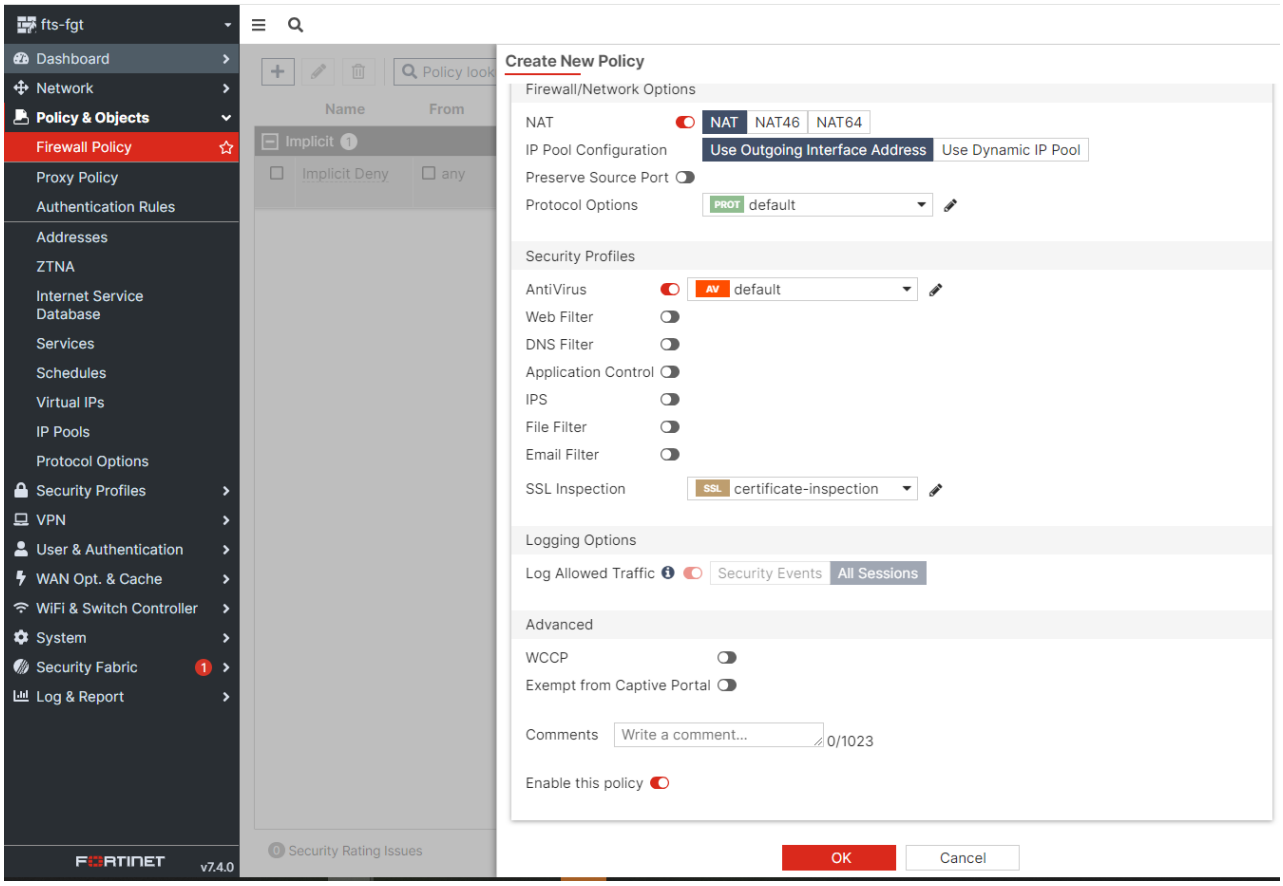
1. Set up the IP address on FortiGate.



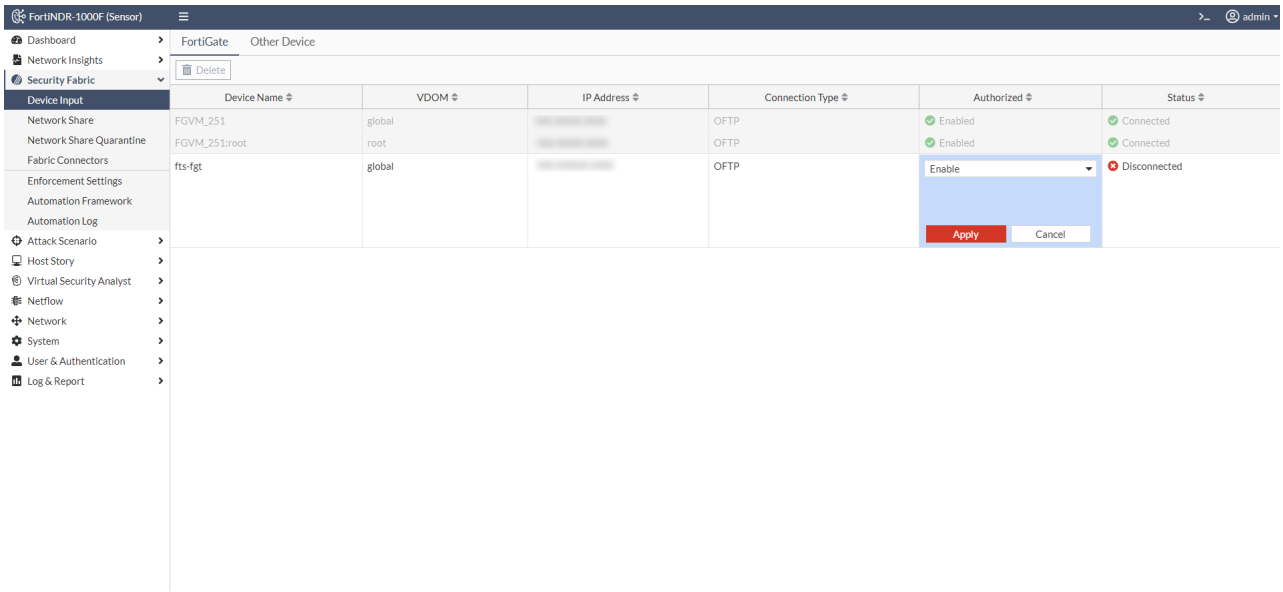
2. Configure an AV profile to send files to FortiNDR.



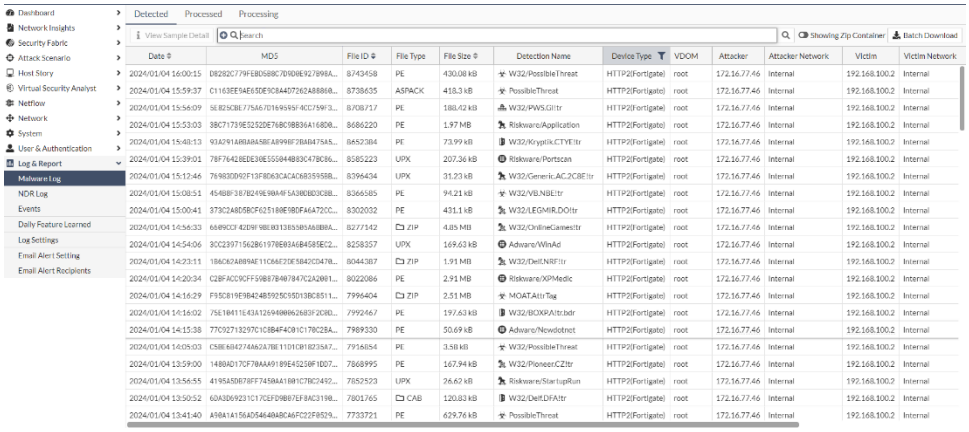
3. Apply an AV profile to the firewall policy.



4. Authorize the FortiGate on FortiNDR for sending files.



5. Check the FortiNDR processed traffic.



Virtual Security Analyst

This section includes the following topics.

Express Malware Analysis

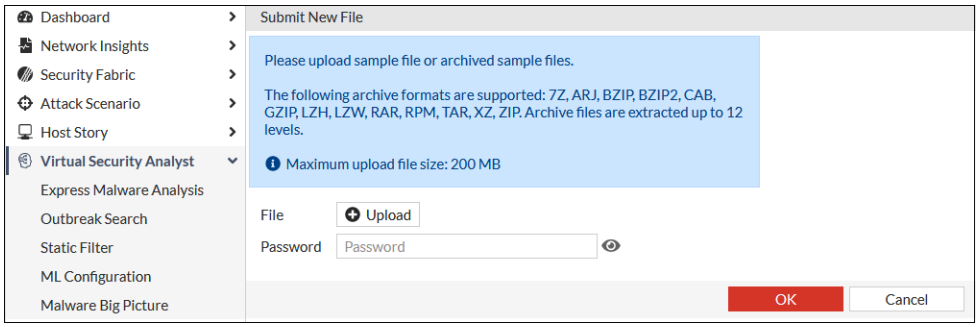
Go to *Virtual Security Analysis* > *Express Malware Analysis* to quickly upload a file and get the verdict. *Express Malware Analysis* is supported in both the GUI and the API. The default file size limit is 200MB. The file size limit can be changed using the CLI.

For information about using the API to submit files, see Appendix A: API guide on page 273 > Submit files.

Express Malware Analysis is not available in Center mode.

To submit a file for Express Malware Analysis:

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



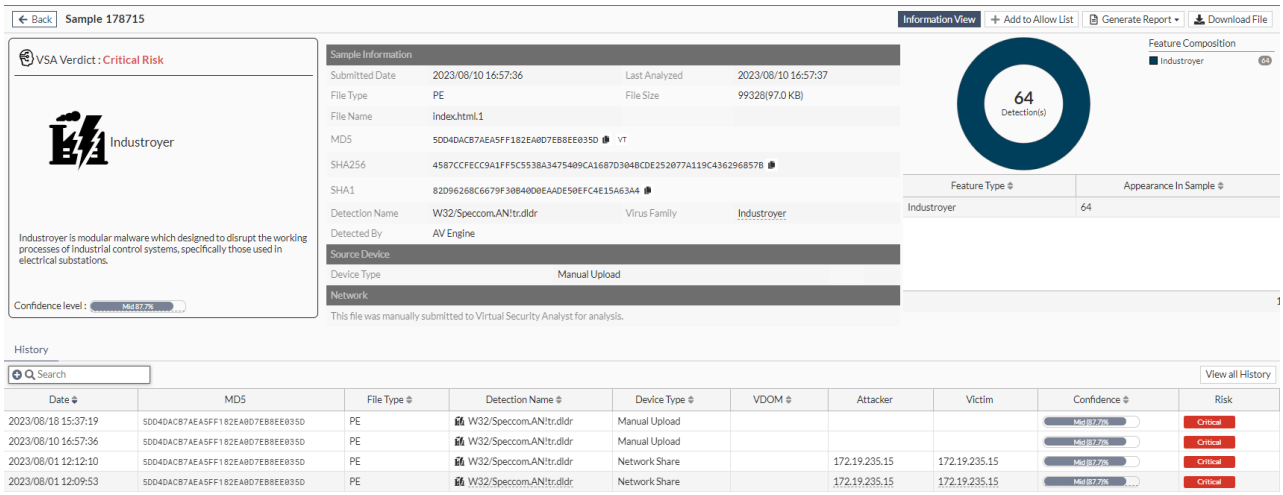
2. Submit a file for analysis. The default file size limit is 200MB. The file size limit can be changed using the CLI.
   a. Click *Upload* then navigate to the file location on your device and click *Open*.
   b. In the *Password* field, enter the password for the file. If the file does not require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

c. Click *OK*. The verdict is displayed.

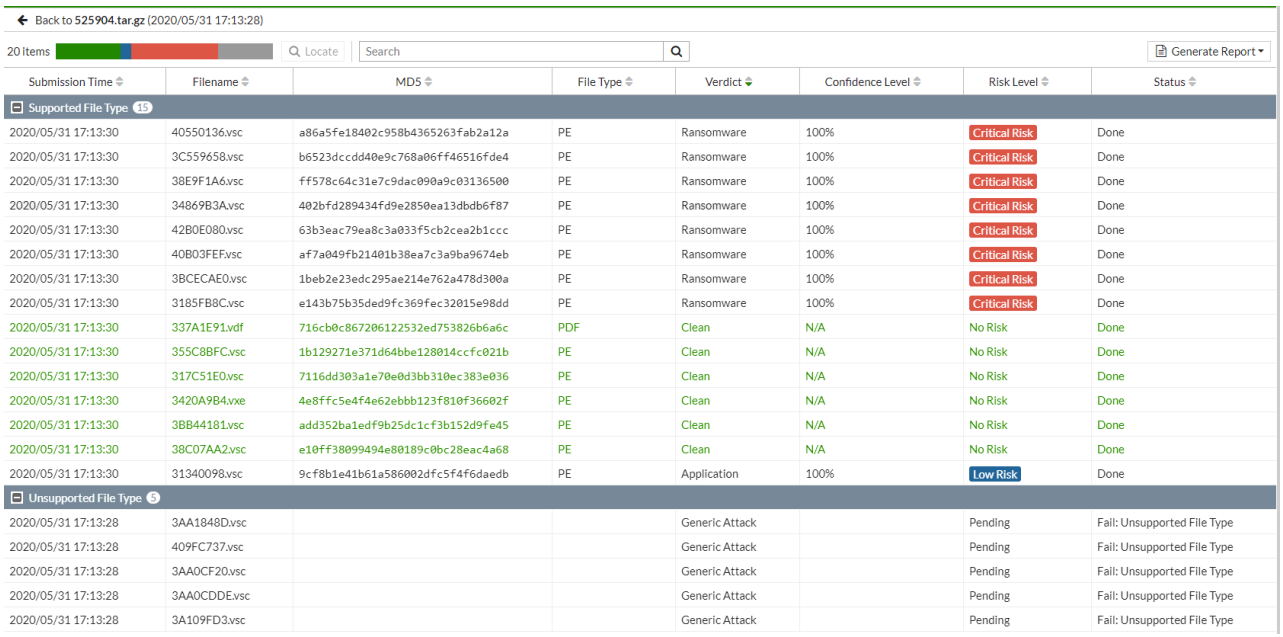
Submission Time	The date and time the file was uploaded.
Submitted Filename	The name of the file that was uploaded.
Submission User	The user that submitted the file.
MD5	The verdict result from MD5 checksum of the file.
Verdict	The attack scenario used to identify the malware attack.
Confidence	The confidence level as a percentage.
Risk	The risk verdict (High, Medium, Low or No Risk).
Status	The submission status.
File Type	The file type such as *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.



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



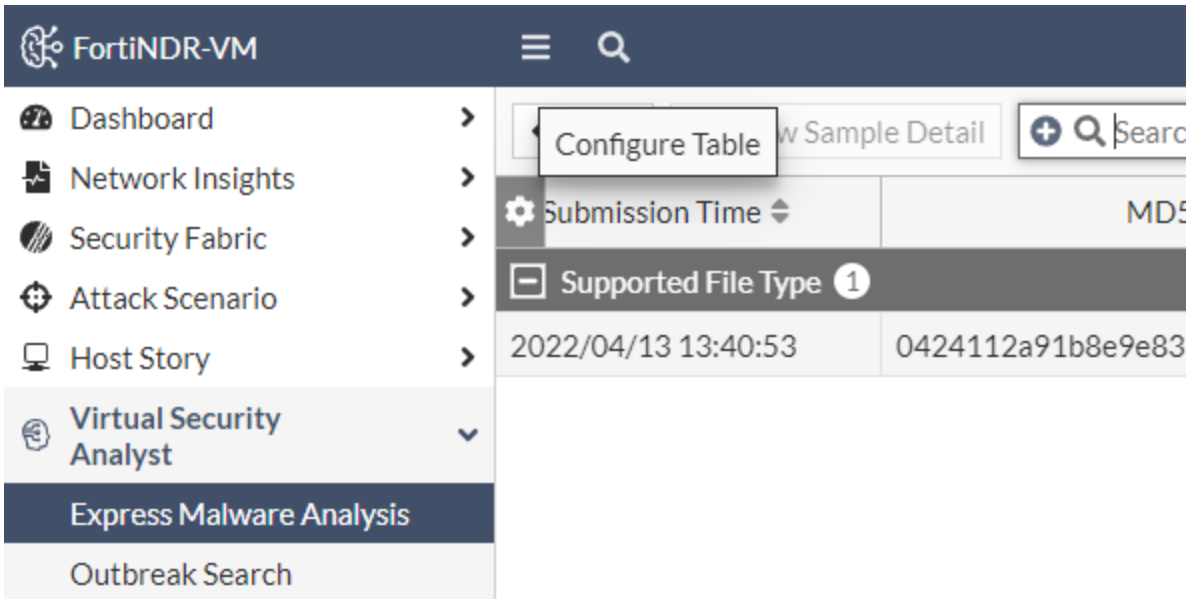
4. (Optional) Click *Generate Report* to view the report summary in PDF and JSON format.

To change the file size limit with the CLI:

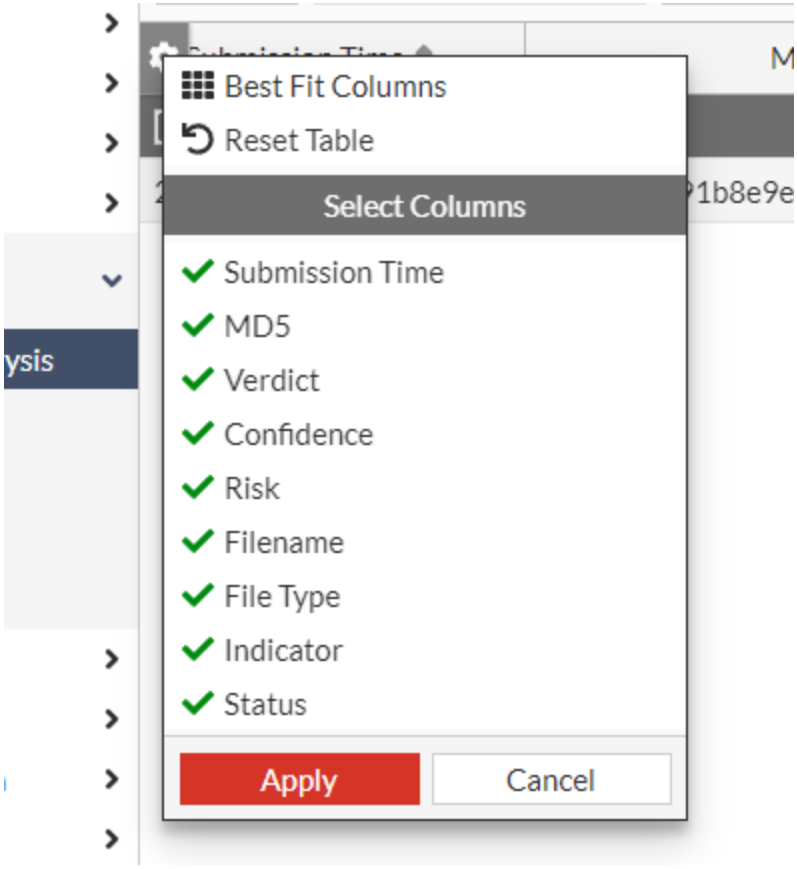
```
execute file-size-threshold
```

Configuring the table

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



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

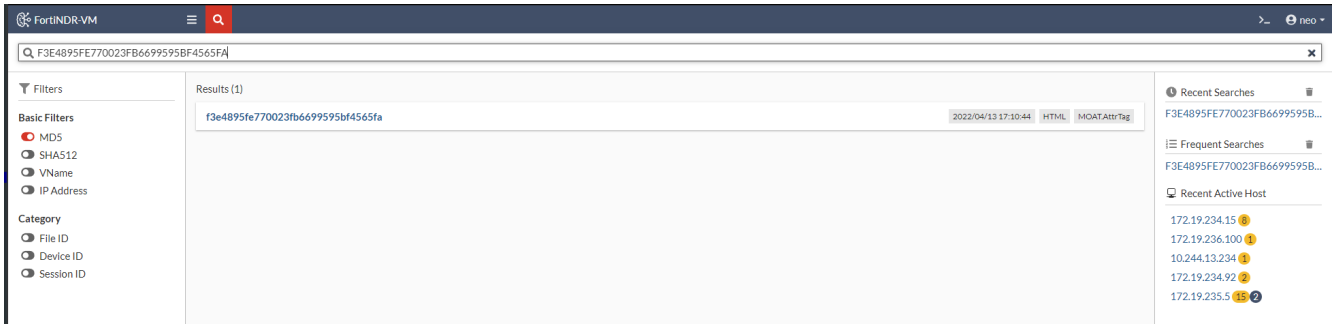


Outbreak Search

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

1. Using a known hash in the FortiNDR database or a physical copy of a file that belongs to the outbreak, you can search for other captured files that share similarities. See Search lead type of hash or detection name on page 166.
2. Using a known outbreak name or known virus family identifier, you can search for captured files that were grouped under the same categories by FortiNDR. See Search lead type of outbreak name on page 167.

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



Search lead type of hash or detection name

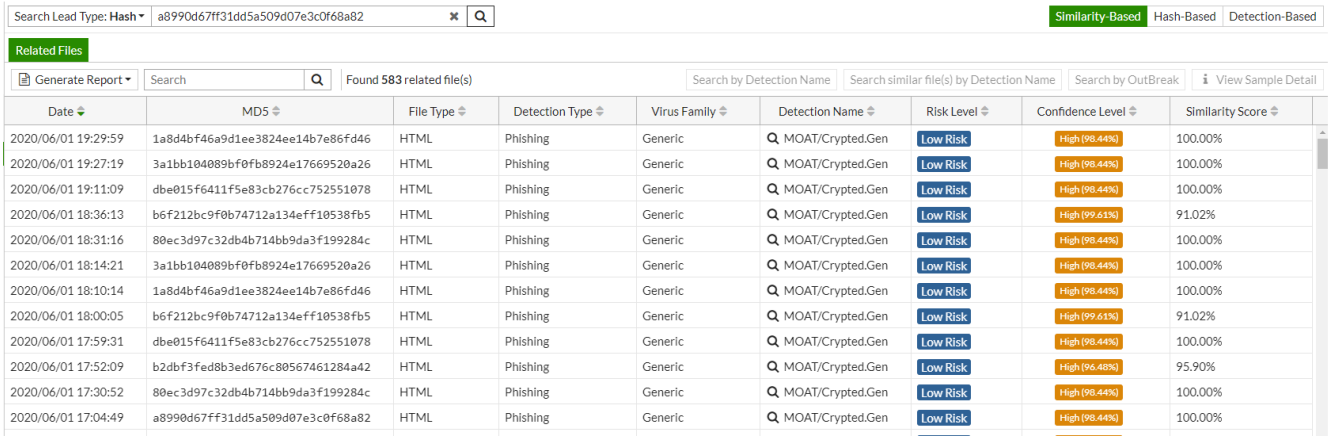
This search lead type accepts MD5 or SHA512 as a search value. You can submit the sample to FortiNDR in *Express Malware Analysis*. When the search lead type is detection name, the search value can be an exact detection name, such as W32/Phishing.DDS!tr, or a detection name with wildcards, such as W32/Phishing.%.

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

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

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

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



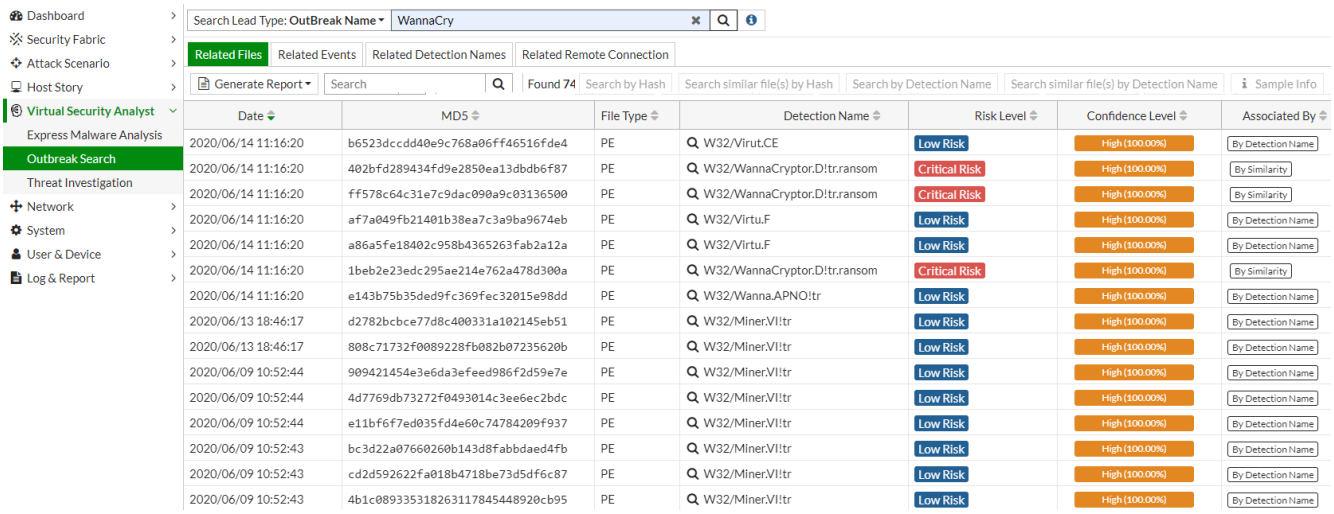
Date	MD5	File Type	Detection Type	Virus Family	Detection Name	Risk Level	Confidence Level	Similarity Score
2020/06/01 19:29:59	1a8d4bf46a9d1ee3824ee14b7e86fd46	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 19:27:19	3a1bb104089bf0fb8924e17669520a26	HTML	Phishing	Generic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

Search lead type of outbreak name

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

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

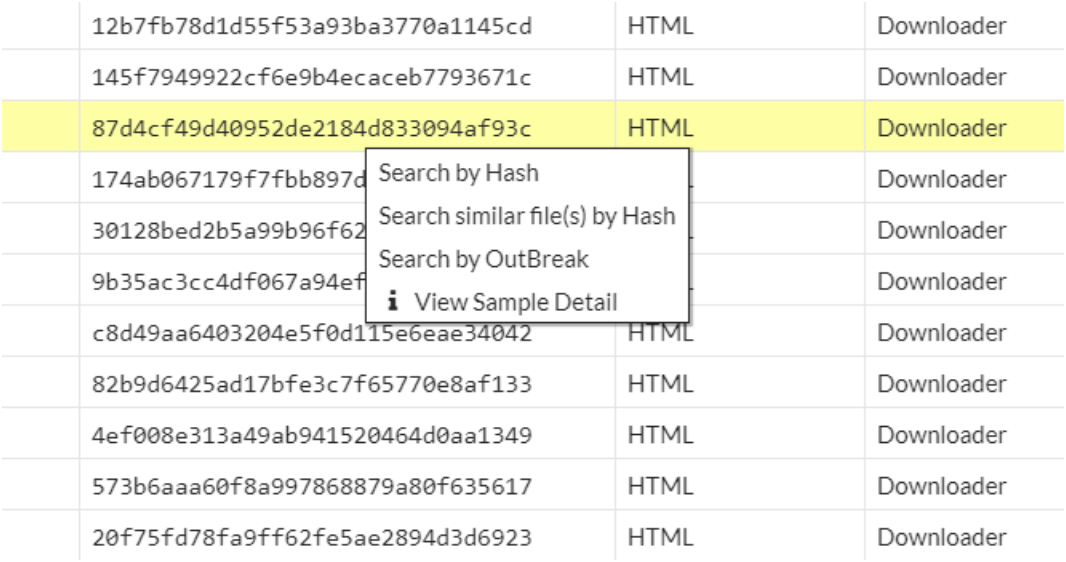
These files are listed in the *Related Files* tab. Other tabs that have a summary of the detection name, remote connections, and attack scenarios events.



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

Recursive searches

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



Reports

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

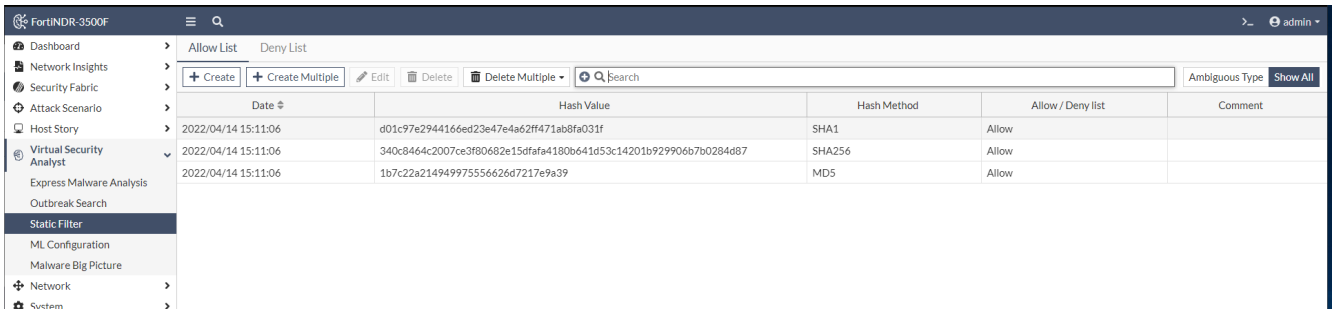
Static Filter

Use the *Static Filter* to manage an *Allow* hash list and a *Block* hash list. This is useful when dealing with outbreaks. For example, inserting an outbreak malware hash for FortiNDR to identify as malicious. An example of the opposite use case is if there are certain files administrators determine are clean, hashes in the 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`.



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

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

You can add a detection to the *Allow List* from the *Malware Log*. For information, see Malware Log on page 254.

NDR Muting

NDR Muting helps streamline security monitoring by hiding NDR detections and observations that are not relevant to your network, helping you focus on the most critical threats. Once an attack is muted, the detection, observation, and all related information are no longer visible on insight pages, and related alerts and enforcement actions are prevented. The information is not deleted, and muted entries are omitted from Syslog and are not quarantined by the Automation Framework.

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* page manages all the NDR muting profiles created for the system. The profile will be applied to the following widgets and pages:

Widgets	• NDR Detection Overview • Observation Overview • Notification • Botnet Connections • FortiGuard IOC • Top Network Attacks • Weak Cipher/ Vulnerable Protocol • Encrypted Attacks • ML Discovery
Network Insight Pages	• Botnet

	• Encrypted Attack • FortiGuard IOC • ML Discovery • Network Attacks • Weak/ Vulnerable Communication

The *NDR Muting* page displays the following information:

Profile Name	NDR Mute Profile name
Profile Name	The name assigned to the muting profile.
Total Number of Rules	Total number of rules that belong to this profile.
Status	Enable to apply all the rules in this profile.
Activation Status	Evaluated based on the *Status* and *Schedule*. • *In Effect* : The status is enabled, but no schedule is set or the current time is within the scheduled period. • *Scheduled* : The status is enabled but the schedule is set at a future time. • *Disabled*: The status is disabled.
Scheduled Start Time	The defined schedule start time.
Scheduled End Time	The defined schedule end time.
Last Modified	The date and time the profile was modified.
Sensor	The sensor assigned to the profile.

You are be able to Create, Edit , Delete, Export and import profiles in the *ML Muting* page.

Muting profiles

Muting profiles let you define a reusable set of rules that suppress specific NDR detections and observations across the GUI. When a muting profile is enabled, all rules within the profile are applied together, helping you hide noise, avoid false positives during known activities, or limit visibility to only the detections that matter.

Each profile includes its own status toggle, which enables or disables all rules in that profile. You can also configure an active schedule, allowing the profile to take effect only during a defined time window, this is useful during planned events such as audits, penetration testing, or maintenance periods.

A muting profile can contain rules from any combination of the following categories:

- **Source IP / Netmask**
  Mutes detections where the specified IP address or subnet appears as the source address.
- **Destination IP / Netmask**
  Mutes detections where the specified IP address or subnet appears as the destination address.

- **NDR Detection Rules**
  Includes Botnet Interactions, Encrypted Attacks, Network Attack/Intrusion, and IOC Campaign. You can mute individual detection types or entire classes, such as Mute All Botnet Interactions or Mute All Network Detections.
- **Observation Rules**
  Targets observations such as Weak Cipher or Vulnerable Protocol. Muting applies when all selected features appear together within the same observation.
- **ML Discovery Rules**
  Supports two modes:
  - *Single feature*: Any selected feature triggers muting (OR logic).
  - *Combined features*: All selected features must match simultaneously (AND logic).

How rules are evaluated

Rules are grouped into categories, and the system uses a combination of AND and OR logic to determine whether a detection or observation is muted.

Across categories:

- The relationship is AND. All selected categories must match for the detection to be muted.

Within a category:

- The relationship is typically OR, unless noted otherwise (e.g., observation rules may use AND logic when multiple features must match together).

Within each category, the matching behavior is as follows:

Category	Matching behavior
Source IP / Netmask	Matches when the specified IP or subnet appears as the source.
Destination IP / Netmask	Matches when the specified IP or subnet appears as the destination.
NDR Detection Rules	Covers Botnet Interactions, Encrypted Attacks, Network Attack/Intrusion, and IOC Campaign.
Observation Rules	Features such as VLAN ID, TLS version, or weak/vulnerable protocols must all match together (AND). Different combinations require separate profiles.
ML Discovery Rules	• Single feature mode: any selected feature may match (OR). • Combined mode: all selected features must match together (AND).

Examples

- **Profile with Source IP + Network Attack (All)**: Mutes only when traffic is from the specified Source IP and the detection is a network attack (category-level AND).
- **Observation with VLAN ID + TLS Version**: Mutes entries only if both features appear together within the same observation (observation-level AND).
- **ML Discovery (Combined) with three features:** Mutes entries that match all three features; entries matching only one or two features are not muted.

Creating muting profiles

To create a custom muting profile:

1. Go to *Virtual Security Analyst > NDR Muting* and click *Create Profile*. The *Create Muting Profile* wizard opens.
2. Configure the profile and click *Next*.

Status	Toggle to enable or disable the profile.
Profile name	Enter a name for the profile.
Schedule Active Time	Use the date picker to select the time range the profile will be active.
Source Sensor	Click the plus sign (+) to open the *Select Entries* pane and then select a sensor from the list. You can select more than one sensor.

3. Configure the *Destination IP Rule*.
   a. Click the plus sign (+) to expand the rule settings
   b. Enter the source IP and Bitmask.
   c. (Optional) Write a comment about the IP address.
   d. Click the plus sign (+) to add another IP to the rule.
4. Configure the *Source IP Rule*.
   a. Click the plus sign (+) to expand the rule settings
   b. Enter the source IP and Bitmask.
   c. Click the plus sign (+) to add another IP to the rule.
5. Configure the *NDR Detection Rule*.
   a. Click the plus sign (+) and select a rule from the drop down.

Rule	Description
Botnet Interactions	Mute a single or multiple botnet detection(s). You also have the option to *Mute All Botnet Interactions*.
Encrypted Attacks	Mute all encrypted attacks. You can also mute one or any *Encrypted Attack* from a list of JA3 and JA3s values.
Network Attack/Intrusion	Mute a single or multiple Network Detection(s). You also have the option to *Mute All Network Detections*.
IOC Campaign	Mute all IOC Campaign attack or Mute All Unclassified IOC Campaign (Detection with no URL). You can also mute one or any *Encrypted Attack* using JA3 and JA3s.

   b. Configure the rule's options. The options will vary depending on the rule.
   c. (Optional) In the *Comment* field, provide details about the rule.
   d. Click the plus sign (+) to add another rule.

6. Configure the *Observation Rule*.
   a. Click the plus sign (+) and select the rule from the drop down.

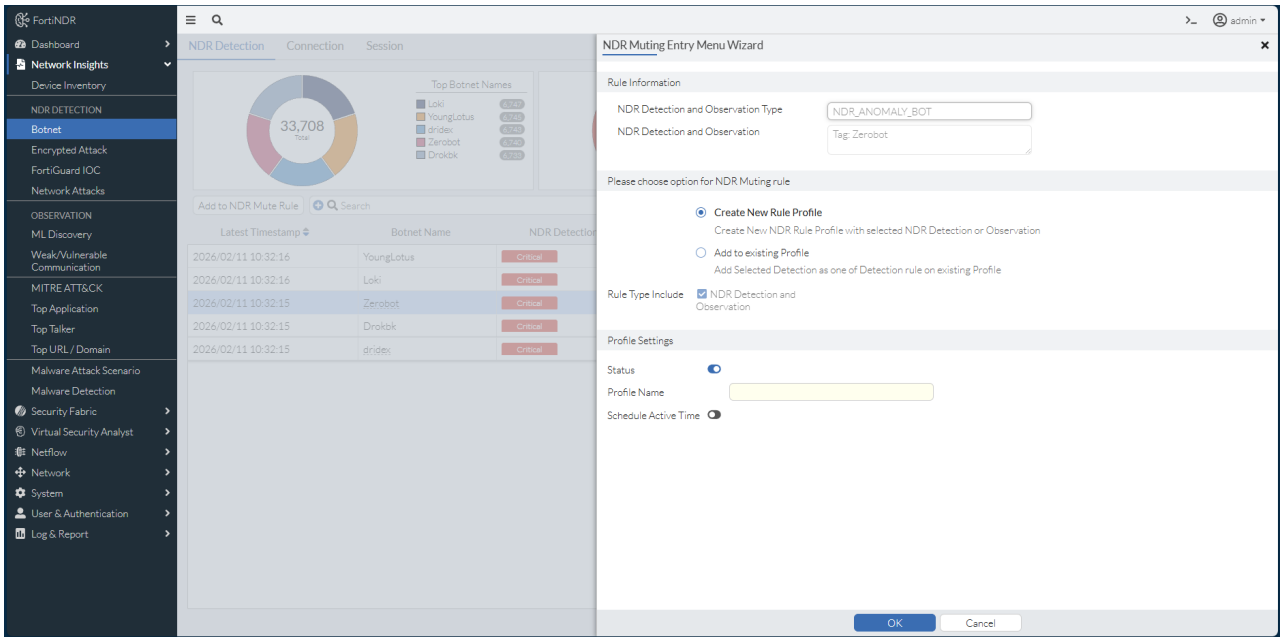
Rule	Description
Weak Cipher/Vulnerable Protocol	Mute a single or multiple protocols with weak cipher or vulnerable protocol. You also have the option to *Mute All Weak Cipher/ Vulnerable Protocols*.

   b. (Optional) In the *Comment* field, provide details about the rule.
   c. Click the plus sign (+) to select a cipher or protocol.
7. Configure the *ML Discovery Rule(s)*.
   a. Select either *Single feature* or *Combined Features*.
   b. Add the feature(s) to the rule.
   c. (Optional) In the *Comment* field, provide details about the rule.
   d. Click the plus sign (+) to select a cipher or protocol.
8. Click *Apply*. The rule is added to the NDR Muting page.

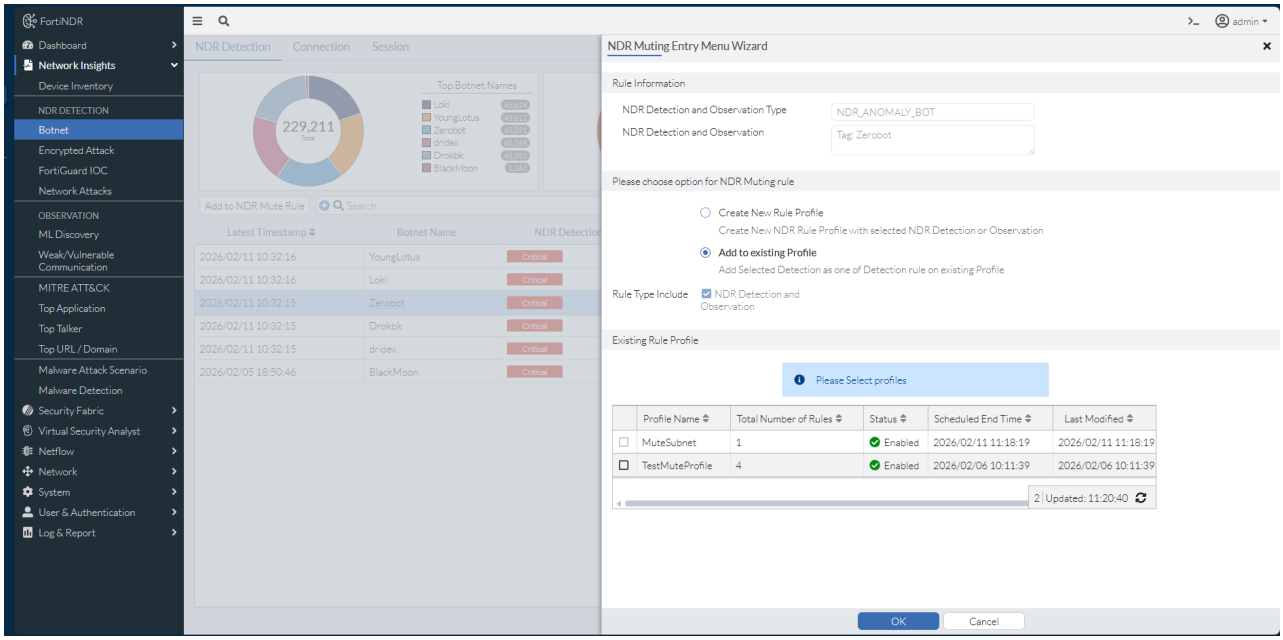
Muting rules in Network Insights

To create a muting profile from a detection:

1. Go to *Network Insights* and open a page with the *NDR Detection* 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*. Alternatively, you can select a detection and click the *Add to NDR Mute Rule* next to the *Search* field. The *NDR Muting Entry Menu Wizard* opens.
3. Create a new profile:



Or add the rule to an existing profile:



4. Click *OK*.

Managing muted rules

To enable/disable NDR Profile and change the sensor selection (Center Mode only):

1. Go to *Virtual Security Analyst* > *NDR Muting*, and select a rule in the list.
2. In the toolbar, click *Edit*.
3. Click *Profile Settings*. The *Profile Settings* pane appears.
4. Next to *Status*, select *Enable* or *Disable*.

To edit or delete profile rules:

1. Go to *Virtual Security Analyst* > *NDR Muting*, and select a profile in the list.
2. In the toolbar, click *Edit*.
3. Click *Edit Rules*. The *Edit Rules* pane appears.
4. Do one of the following
   a. Edit the existing rules.
   b. Remove rules by clicking the **X** button.
5. Click *OK*.

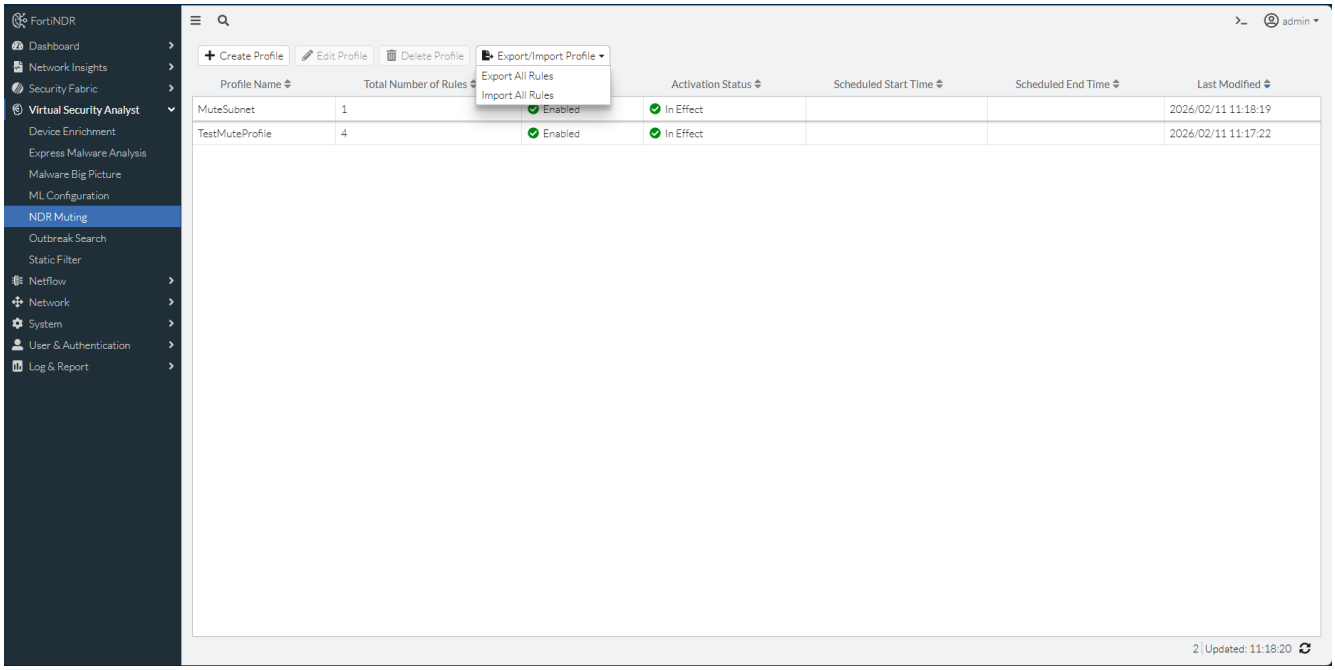
Importing and exporting a profile

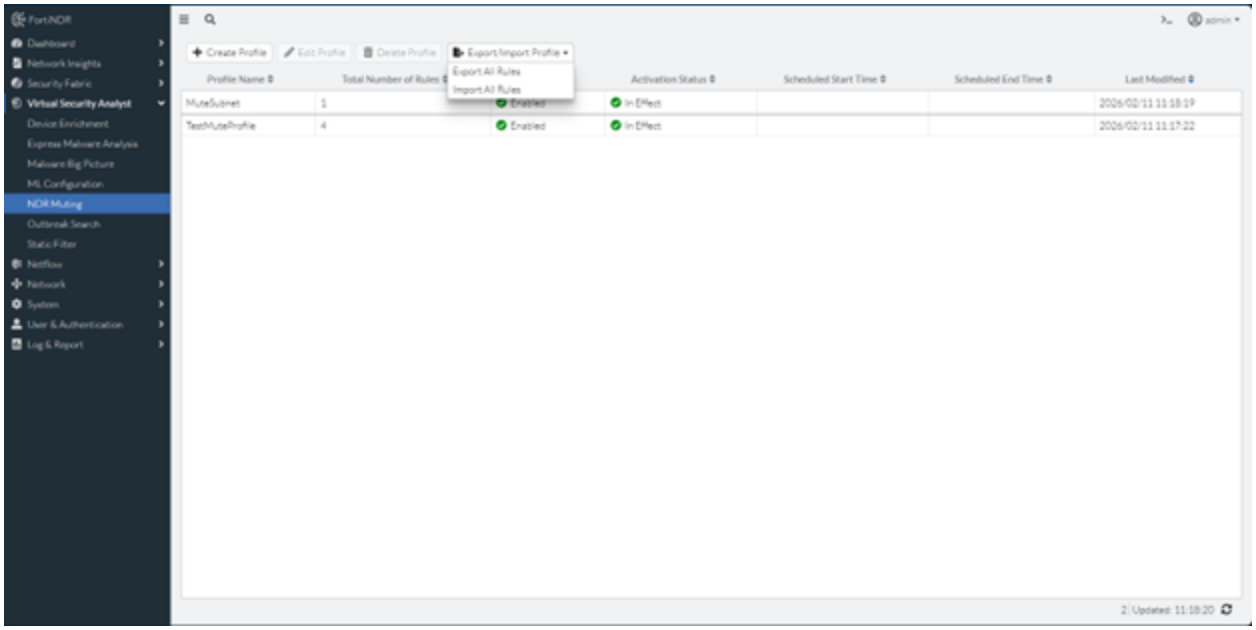
The NDR Muting page allows you to export and import NDR mute rules using a file. All imported NDR Mute profiles will be disabled by default.

When the source machine is in:

- Standalone and Sensor mode and the target machine is in Center mode, you will be prompted to add sensor information when enabling the NDR muting profiles after import.
- Center mode and the target machine is in Sensor or Standalone mode, the sensor selection will not be included in the import process because Sensor and Standalone mode does not support NDR Mute attributes.

> ⚠ The existing NDR Mute profiles on the target machine will be overwritten by the NDR Mute profiles from the file.





ML Configuration

Go to the *Virtual Security Analyst > ML Configuration* page to view and edit the machine learning baseline features for the traffic event 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 Baseline must be retrained after upgrading to version 7.6.4. While ML may appear to function normally immediately after the upgrade, it will either stop detecting or produce inaccurate ML discovery results until

retraining is completed.

The *ML Configuration* page has three 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 event detection.
- **Default** (Standalone mode) : Use this tab to view and adjust the machine learning baseline features for traffic event 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*.

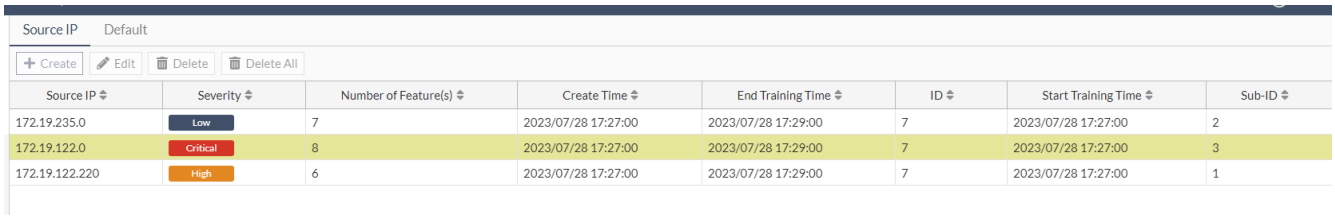
Source IP tab

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 event 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.



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 a NDR Detection or Observation. 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 not want to treat certain range change in the IP as a NDR Detection or Observation. 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.
Time of Week	Enable this option to view events based on the time of week. During machine learning training, the system establishes a baseline of activity for each source IP. If traffic is observed during a time period where the baseline is zero (meaning no activity is expected) it is flagged as a NDR Detection or Observation. These events are displayed in the *Time of Week* widget on the *Information* page. The time ranges are defined as follows: • Daytime: 08:00-15:59 • Evening: 16:00 – 23:59 • Night : 00:00 – 07:59
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, FTP, 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 event 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 event 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 a NDR Detection or Observation. 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 not want to treat certain range change in the IP as a NDR Detection or Observation 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, FTP, 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 a NDR Detection or Observation. 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 do not want to treat certain range change in the IP as NDR Detection or Observation 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, FTP, 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 event 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 a NDR Detection or Observation. 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 do not want to treat certain range changes in the IP as a NDR Detection or Observation 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, FTP, 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.

.

In Center mode, the baseline for newly added sensors will be trained starting from their earliest session log date up to the time specified by the CLI command: `execute reset-ml-baseline-time`. Training does not begin from the current date. If you wish to start training from the current date, please refer to the following Retrain baseline section for a workaround.

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.

Retaining ML Discover detection logs

Please be aware that the CLI command `execute cleanup ml` will clear all ML detection logs. If you wish retain the detection log please review the following guidelines and follow the recommended workarounds.

Standalone mode

In Standalone mode, changing the selected features for training will trigger retraining from the current time up to the time specified by the CLI command `execute reset-ml-baseline-time`, while preserving the previous detection logs.

Center mode

In Center mode, adding or removing sensors from a Sensor Group can trigger baseline retraining for all sensors in the group while preserving the previous detection logs. However, existing sensors will be trained starting from the current date (assuming there are no sensor sync delays), whereas newly added sensors will be trained from their earliest session log date up to the time specified by the CLI command: `execute reset-ml-baseline-time`.

Changing the selected features for a Sensor Group will also trigger retraining for the group, starting from the current date (assuming there is no delay on processing the session logs) up to the time specified by the CLI command: `execute reset-ml-baseline-time`.

To workaround retraining a newly added sensor from the current date:

1. Change the selected features to initiate retraining and wait for the process to complete.
2. Revert the selected features to their original configuration.

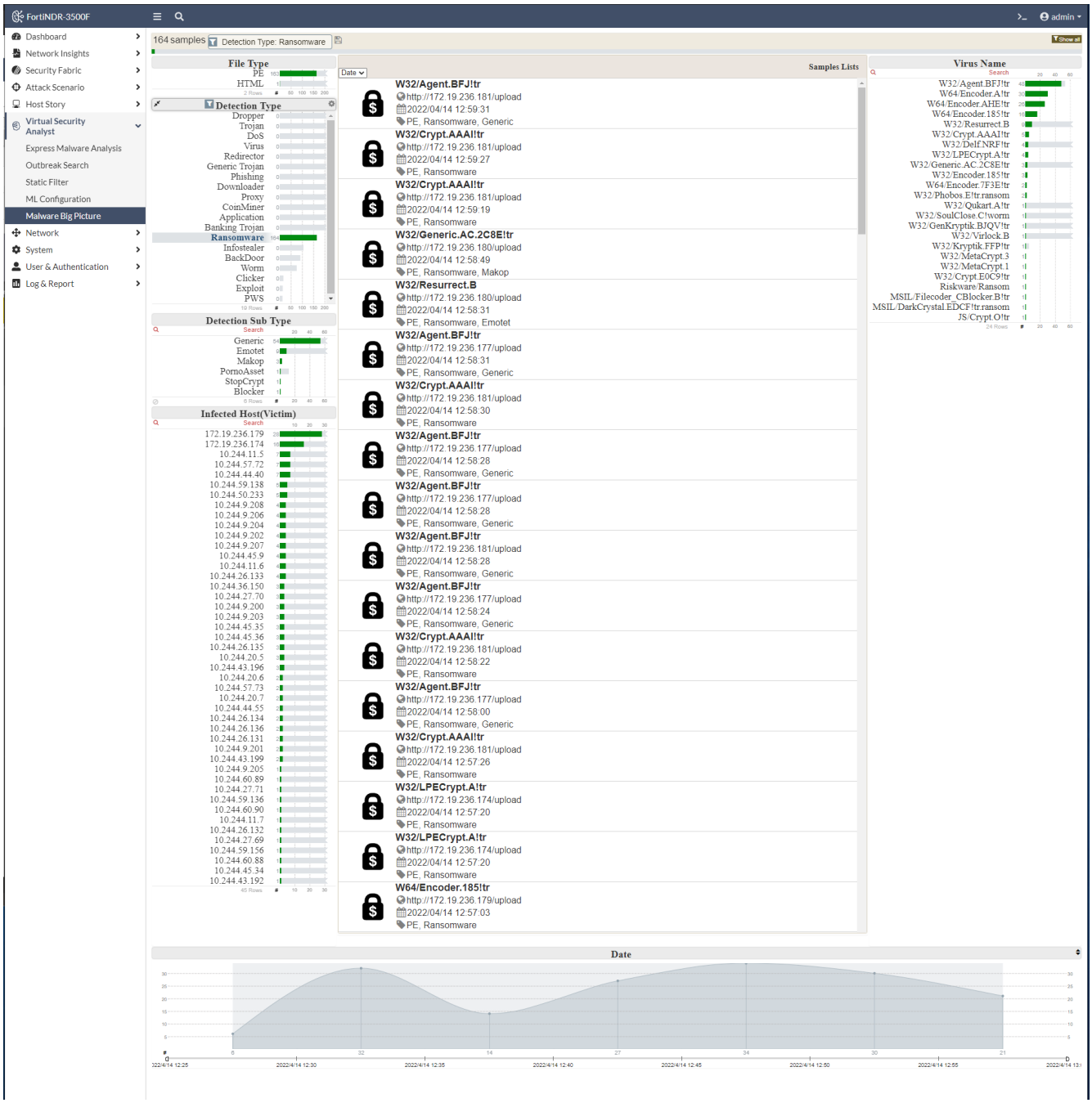
To retrain the Sensor Group from the earliest date of the sensors without changing any selected features and retrain detection logs:

1. Remove all sensors from the target Sensor Group.
2. Create a new Sensor Group containing all the sensors from the original group.

Malware Big Picture

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

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



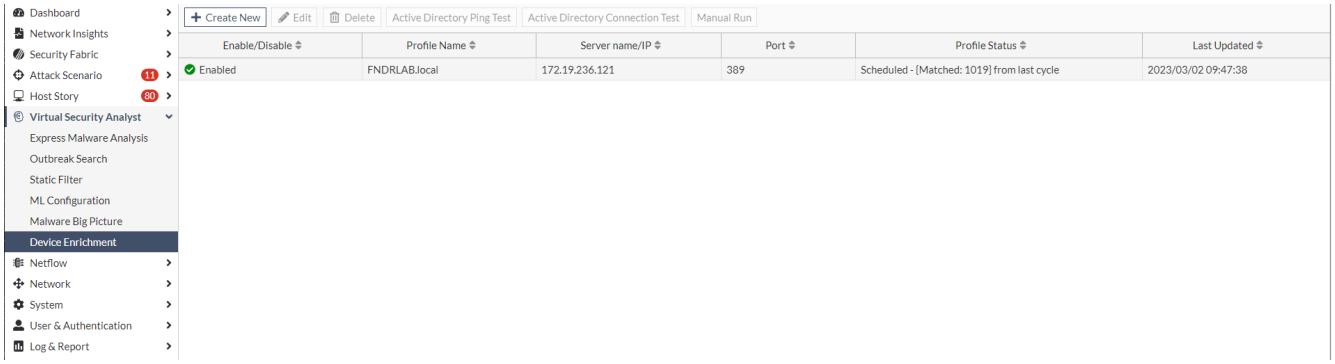
Device Enrichment (Standalone, Sensor and Center)

You can improve the Device Identifier by creating a *Device Information Enrichment Profile* that will retrieve Hostname information from the Windows Active Directory (AD) and DNS server of the target network. When the

profile is enabled, the device enrichment process will run according to the scheduled cycle in the profile. You can also execute the profile manually.

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

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



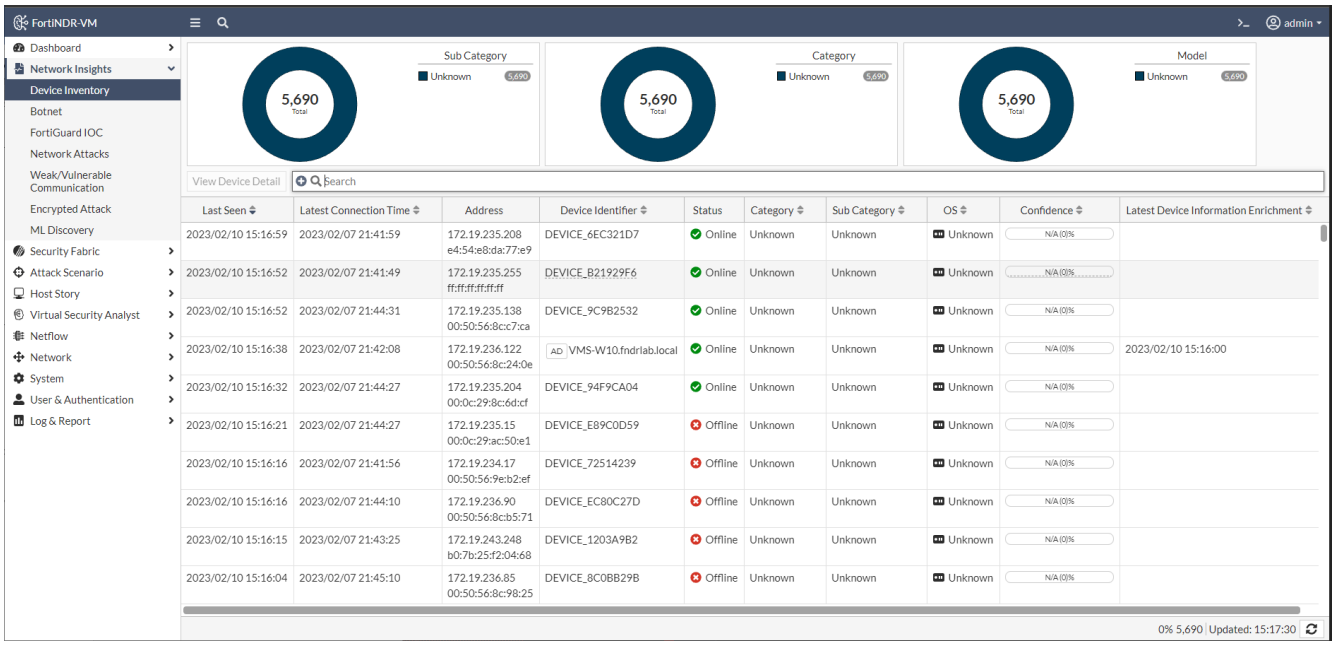
The *Device Enrichment* page displays the following information:

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

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

Viewing the retrieved device identifier

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

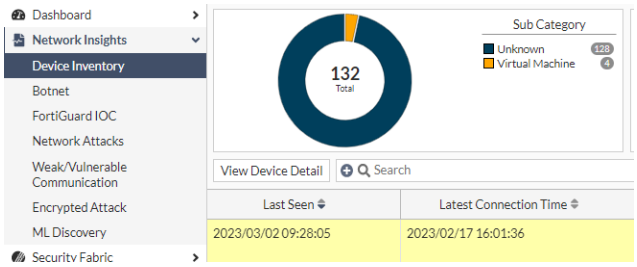


Overwriting the device identifier

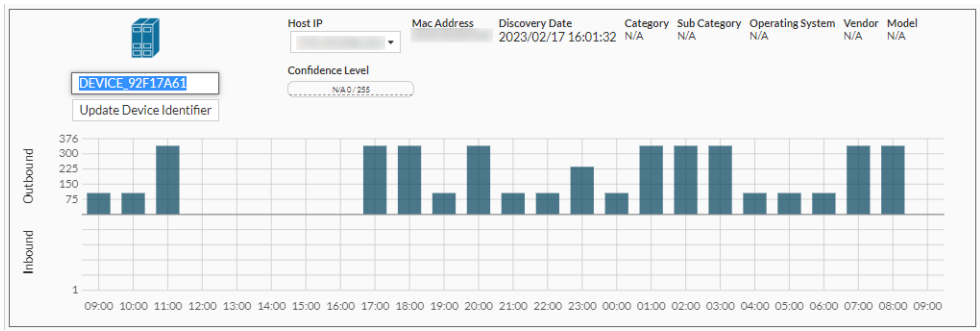
You can manually overwrite the device identifier in the device information page.

To overwrite the device identifier:

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



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



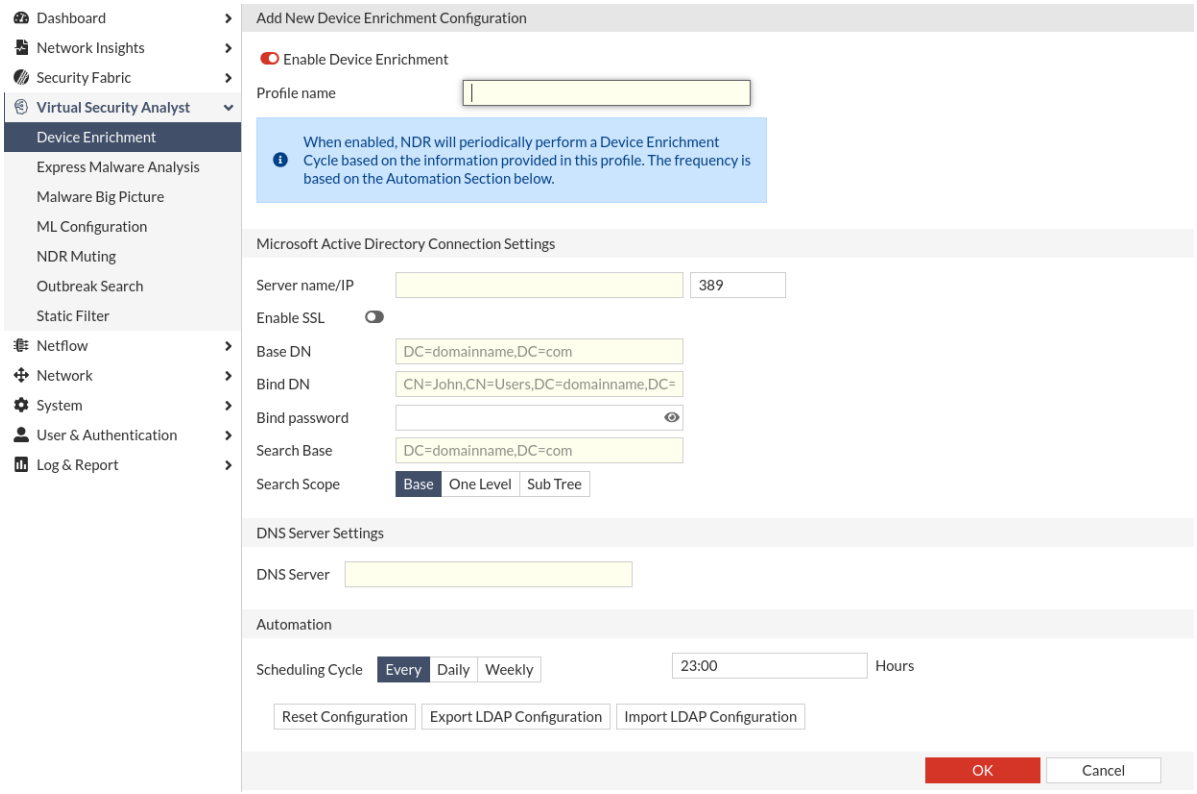
Creating a Device Enrichment Profile

To create a Device Enrichment profile:

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

Enable Device Configuration	Disable or enable the profile
Profile Name	Provide a 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	Enable this option to select the SSL port and protocol to be used.
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 Base	The starting point of the directory tree for retrieving information
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.
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 cycle	• *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.
Reset Configuration	Click to reset the configuration.

Export Configuration	Click to export the configuration as a config file. The password is not exported.
Import Configuration	Click to import a config file. Importing new profile will \replace all profile settings and clear the password.



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 the FDS server to verify the NetFlow license once before the initial use of this feature.

To turn NetFlow on/off with the CLI:

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

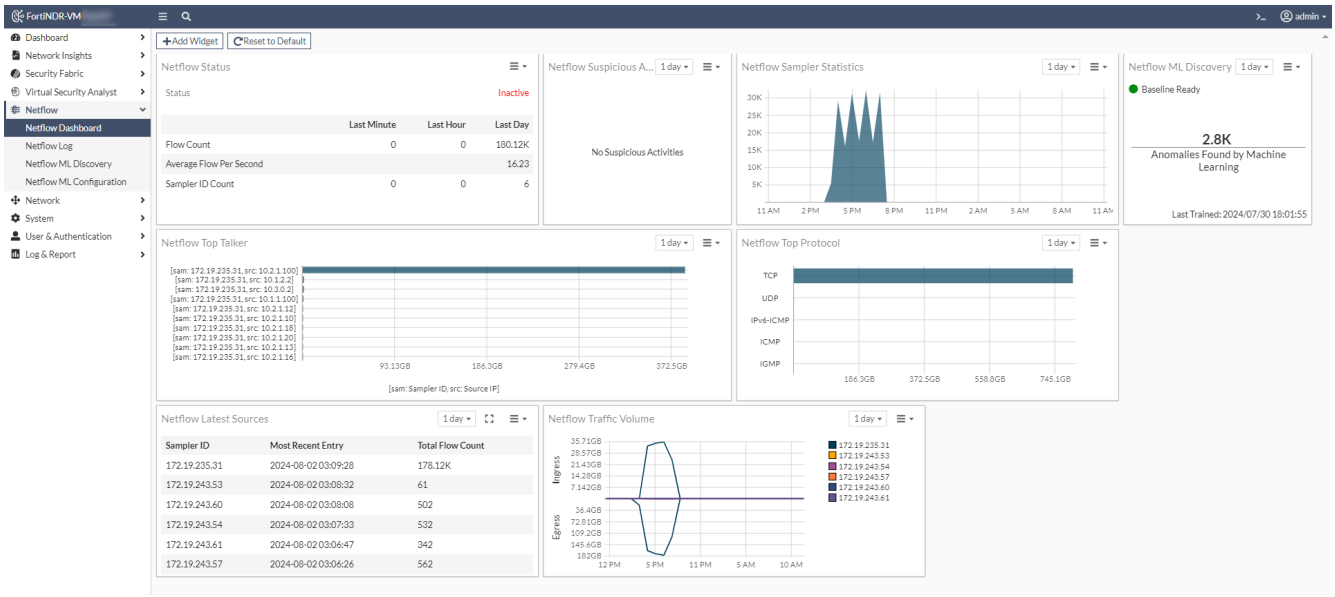
NetFlow ports

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

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

Netflow Dashboard

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



The *Netflow Dashboard* contains the following widgets:

Netflow Status	Displays the *Status* of this feature including, *Flow Count*, *Average Flow Per Second* and *Sampler ID Count*. The statistics show the volume and flow count coming into FortiNDR by minute, hour, and day.
Netflow Suspicious Activity	Netflow has two main types of detections: 1. Displays the Netflow *botnet*, *Spam*, *Phishing*, *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. 2. IOC lookup on Destination IP address will surface any malicious/suspicious IPs and tag them accordingly. Please see FortiGuard IOC on page 54 for more information.
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.
ML Discovery	The *Netflow ML Discovery* widget provides a brief summary of the current Netflow ML baselining status and the number of events detected during the selected time period. • To view the current Netflow ML baseline configuration, go to *Netflow > Netflow ML configuration*. • To view the observation, click on the widget to expand it, or go to *Netflow > Netflow ML Discovery*.

Customizing the Netflow Dashboard

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

To add a widget to the dashboard:

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

To remove a widget from the dashboard:

Click the widget menu and select *Remove*.

To re-size a widget in the dashboard:

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

Netflow Log

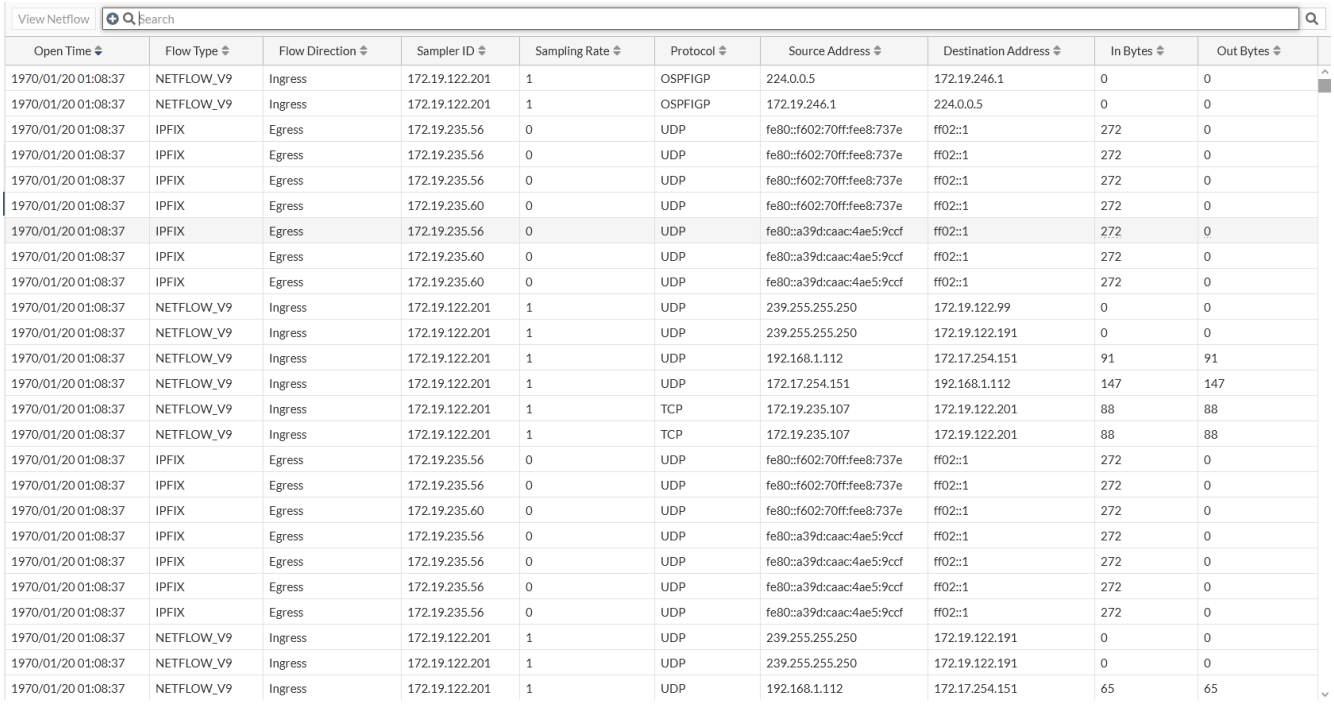
Netflow Log shows the logs FortiNDR collected. In Center mode, the *Netflow Log* displays the data collated from the Sensors.

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.

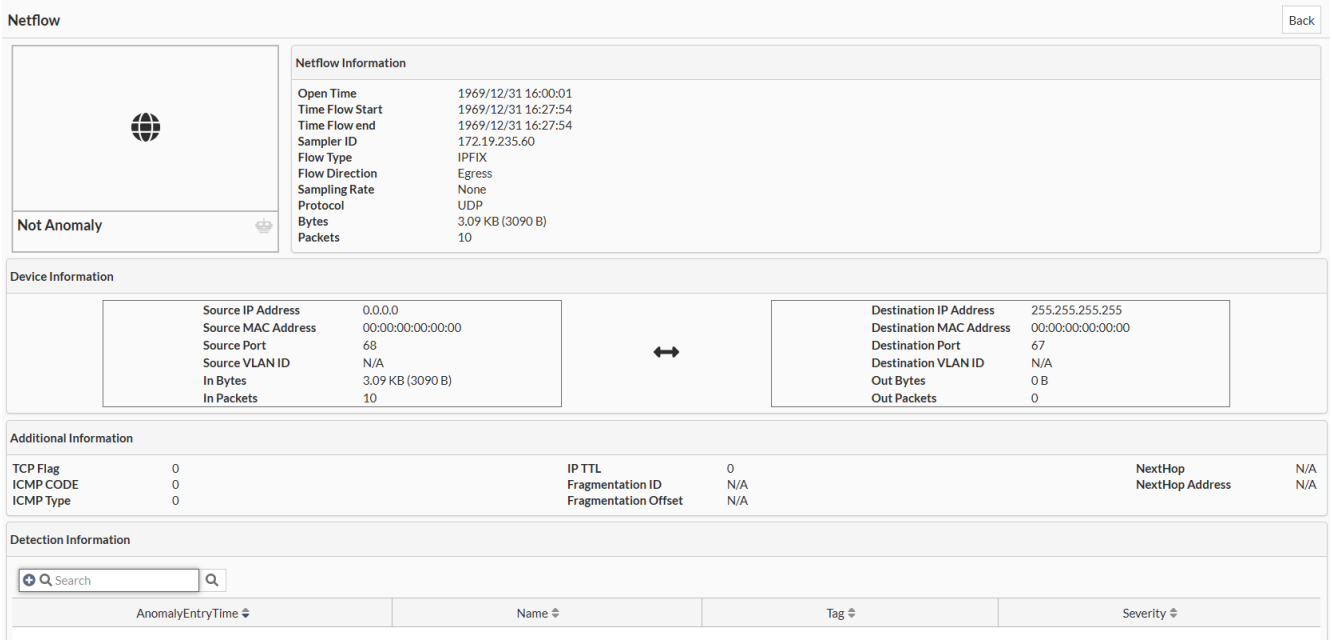

View Netflow

Search

Open Time	Flow Type	Flow Direction	Sampler ID	Sampling Rate	Protocol	Source Address	Destination Address	In Bytes	Out Bytes
1970/01/20 01:08:37	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 detections and observations

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

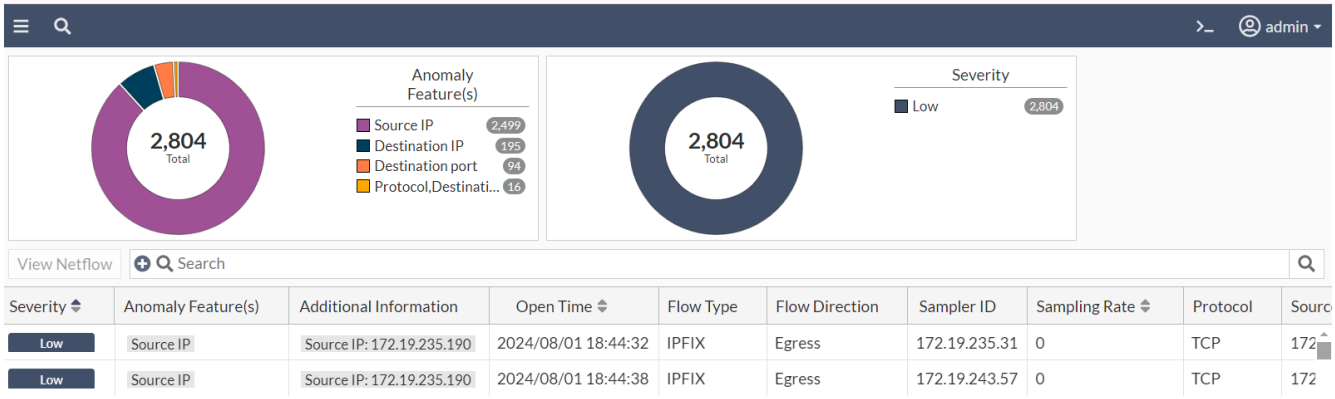


The anomalies page displays the following information:

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

Netflow ML discovery

The *Netflow ML Discovery* monitor displays a list of events detected by Netflow ML Configuration. Each row is based on a flow. The configuration and baselining of Netflow ML Discovery is located under *Netflow > Netflow ML configuration*. Netflow ML discovery is enabled by default.

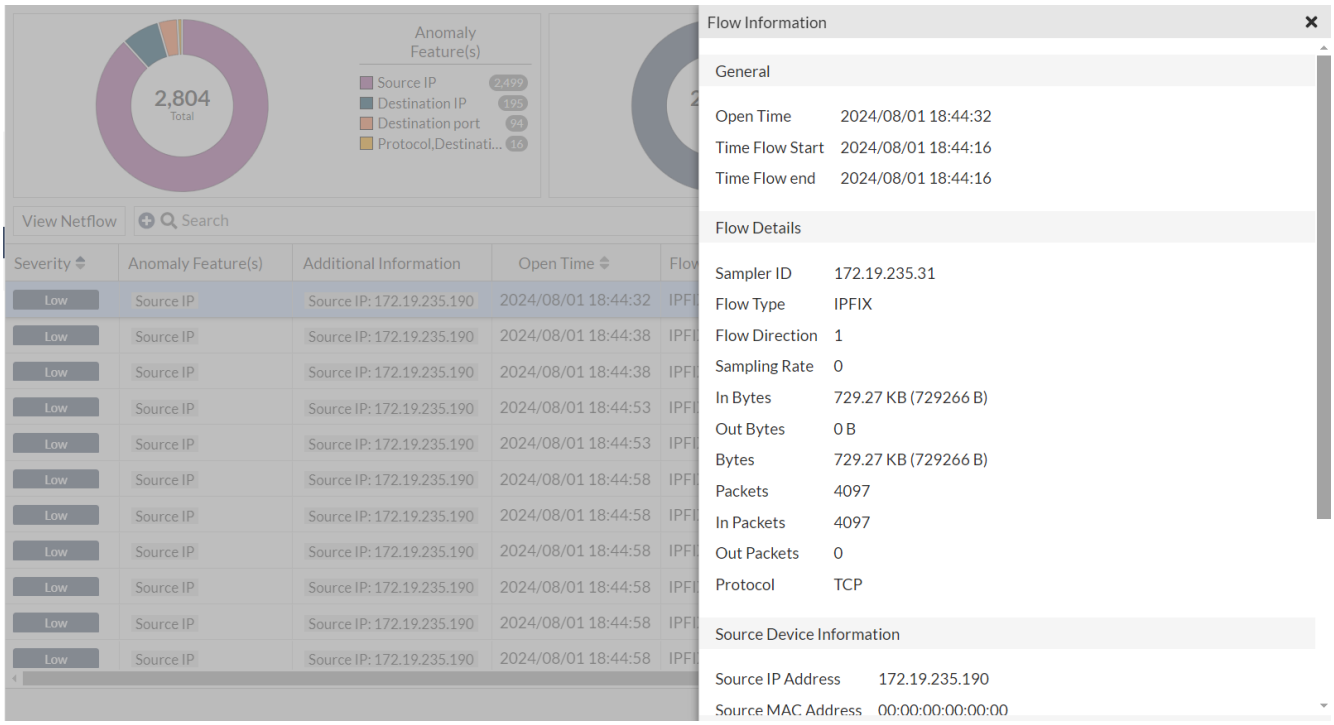


The *Netflow ML Discovery* page displays the following information.

Severity	The severity level assigned to the IP (*Low*, *Medium*, *High* or *Critical*). The severity levels can be customized in *Netflow ML Configuration*.
Observation Feature(s)	The feature or feature combinations that caused the observation.
Additional Information	The abnormal feature value(s).
Open Time	The date and time the session started.
Flow Type	The Flow Types can be: *NETFLOW_V5*, *NETFLOW_V9*, *IPFIX*, or *SFLOW_5*.
Flow Direction	The flow direction (*Ingress* or *Egress*).
Sampler ID	The sample IP address
Sampling Rate	The number of packets Netflow Collector drops for every 1 packet collected.
Protocol	The communication protocol.
Source Address	The source IP address.
Source Network	The source network.
Destination Address	The destination IP.
Destination Network	The destination network.
In Bytes	The sample in bytes.

Viewing flow information

To view the flow information for a Netflow ML Discovery, double-click a record in the table. The *Flow Information* pane displays the following information:



Netflow ML Configuration

Configure the Machine Learning (ML) profile of network traffic to identify anomalies.

The *ML Configuration* page has two tabs:

- **Default** (Standalone mode): Use this tab to view and adjust the machine learning baseline features for traffic event detection and to monitor the status of baseline training.
- **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 event detection.

Default tab

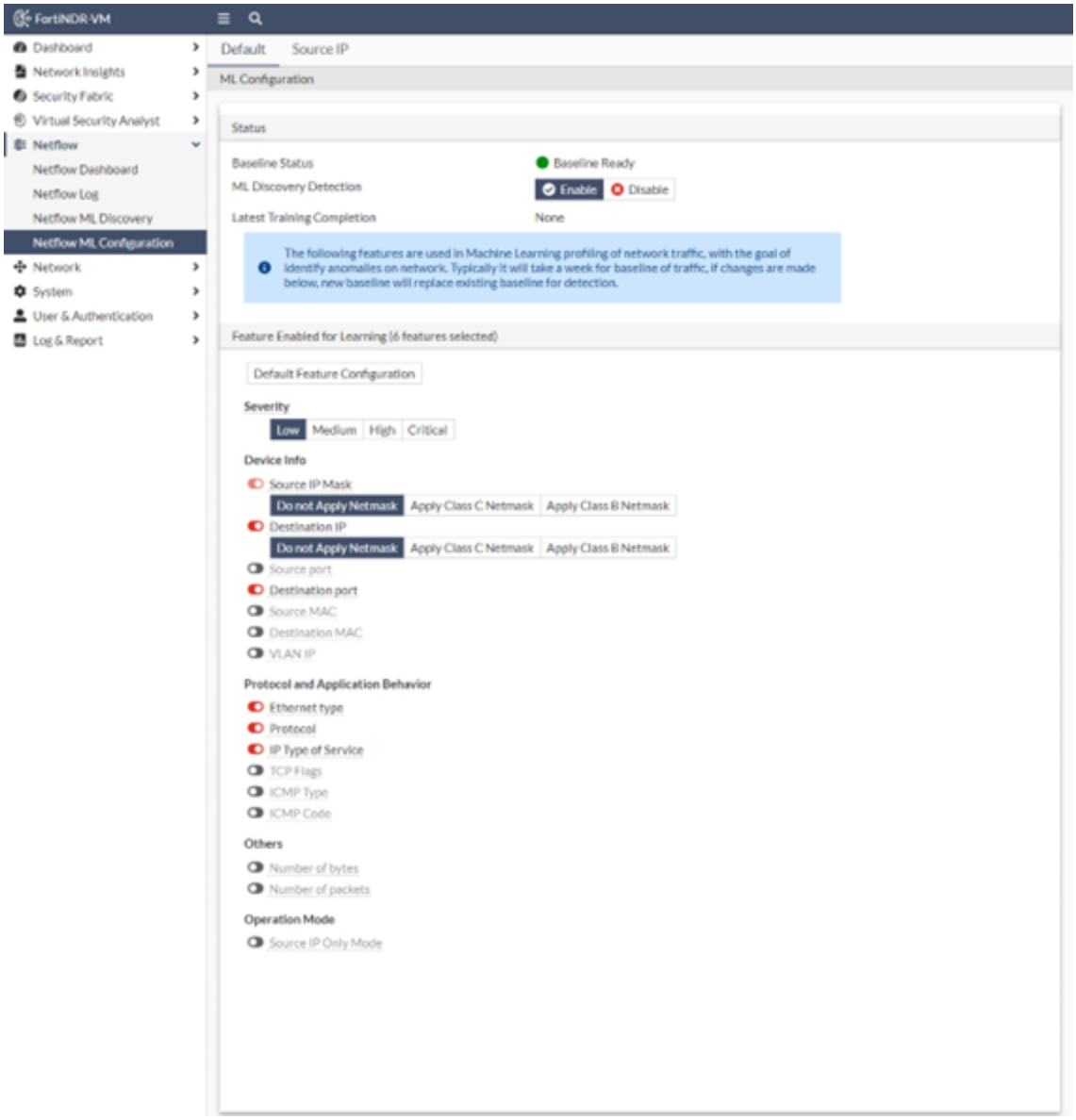
To configure the ML Configuration profile:

1. Go to *Netflow* > *Netflow ML Configuration*.
2. Configure the following settings:

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 event 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 NDR Detection or Observation. 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	The Destination Device IP. Apply netmask if you do not want to treat certain range changes in the IP as an NDR Detection or Observation. 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 Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Destination Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Source MAC	Source device MAC address.
VLAN IP	The VLAN IP.
Protocol and Application Behavior	
Ethernet type	Enable to monitor the Ethernet type.
Protocol	Enable to enter the protocol.
IP Type of Service	Enable to monitor the IP service type.
TCP Flags	Enable to monitor the TCP Flags.
ICMP Type	Enable to monitor the ICMP type.
ICMP Code	Enable to monitor the ICMP code.
Others	
Number of Bytes	FortiNDR categorizes Bytes into 3 groups: • Small: Less than 100 bytes • Medium: 100-9999999 • Larger: Equal to and greater than 10000000 bytes

Number of packets	FortiNDR categorizes Packets into 3 groups: • Small:Less than 2 • Medium: 2-6249 • Larger: Equal to and greater than 6250
Operation Mode	
Source IP Only Mode	When enabled, ML will only monitor the traffic for IPs in the *Source IP* tab. Other traffic will be skipped.



Source IP tab

To configure the Source IP:

1. Go to *Netflow* > *Netflow ML Configuration* and click the *Source IP* tab.
2. Click *Create*. The *ML Configuration for Source IP* pane opens.
3. Configure the following settings:

Source IP and Severity	
Source IP	Enter the source IP address.
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 NDR Detection or Observation. 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	The Destination Device IP. Apply netmask if you don nptt want to treat certain range change in the IP as an NDR Detection or Observation. 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 Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Destination Port	Port number such as, *22*, *445*, *none reserved port*, etc.
Source MAC	Source device MAC address.
VLAN IP	The VLAN IP.
Protocol and Application Behavior	
Ethernet type	Enable to monitor the Ethernet type.
Protocol	Enable to enter the protocol.
IP Type of Service	Enable to monitor the IP service type.
TCP Flags	Enable to monitor the TCP Flags.
ICMP Type	Enable to monitor the ICMP type.
ICMP Code	Enable to monitor the ICMP code.
Others	
Number of Bytes	FortiNDR categorizes Bytes into 3 groups: • Small: Less than 100 bytes

	• Medium: 100-9999999 • Larger: Equal to and greater than 10000000 bytes
Number of packets	FortiNDR categorizes Packets into 3 groups: • Small:Less than 2 • Medium: 2-6249 • Larger:Equal to and greater than 6250

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 on page 206.

DNS and static routes

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

Static routes control how traffic exits from the FortiNDR unit. They allow you to specify the network interface through which a packet should be sent, as well as the IP address of the next-hop router accessible via that interface.

A default route is a special type of static route that matches all packets. It specifies a gateway router to which packets are sent when no other specific route exists for the destination IP address. To ensure normal operation of the FortiNDR unit, a default route configuration is required.

To add a static route:

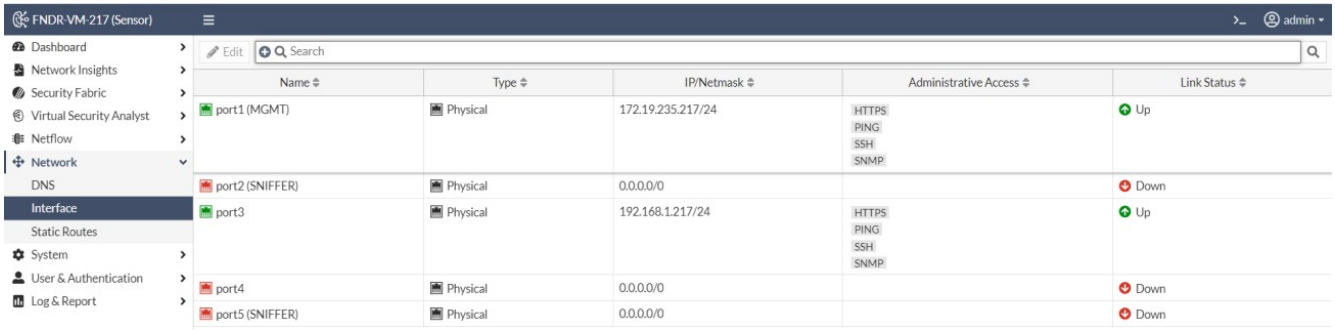
1. Go to *Network >Static Routes*.
2. Click *Create New* to create a new route or double-click a route to modify it.
3. In *Destination IP/Netmask*, enter the destination IP address and netmask of packets that will be subject to this static route.
   To create a default route that will match all packets, enter `0.0.0.0/0`.
4. Select the interface that this route applies to. Choose port1 (MGMT) when creating a default route.
5. Enter the *Gateway Address*.
6. Click *OK* to save the static route.

Configuration example

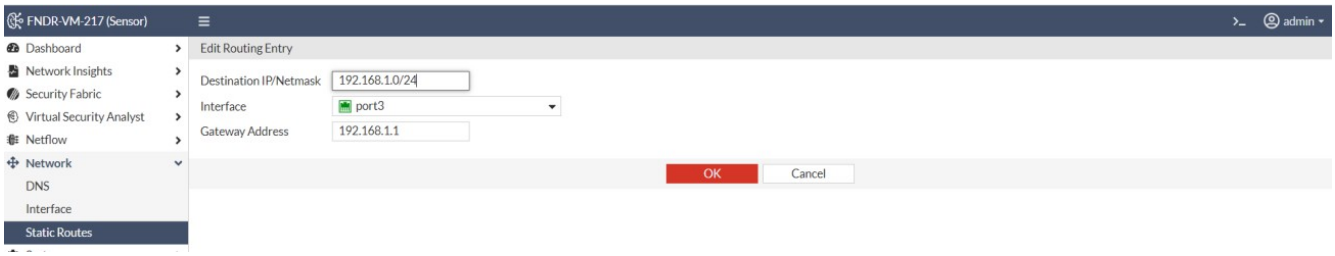
In the following example, a dedicated interface *port3* is used to handle file API submissions, separate from the default management interface *port1*.

While other ports such as port2 can be used, it is recommended to select a non-sniffer port or turn off the sniffer feature with the CLI to avoid additional overhead from sniffing traffic. See, `config system interface` in the FortiNDR CLI Reference Guide.

The management *port1* is connected to the 172.19.235.0/24 subnet (*Management network*). The data interface *port3* is connected to the 192.168.1.0/24 subnet (*data network*).



In addition to the static rule for management interface, a new rule for file submission traffic must be added as shown below. Any file submission client residing in the data network should be able to submit samples to the FortiNDR device via port3.



The management network and data network must not share the same subnet.

System

Use the *System* options to configure system settings.

It is recommended that you create a system backup file as part of your maintenance plan. Always perform a backup before upgrading firmware or making major system configuration changes. Save these configuration backups to your local computer in the event that you need to restore the system after a network event. For information, see Backup or restore the system configuration on page 237.

Administrators

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

To create a new Administrator:

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

Username	Enter a username for the administrator.
Admin Profile	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.

Predefined profile types

The following predefinedadministrator profiles cannot be modified or deleted:

- *SuperAdminProfile*: All functionalities are accessible.
- *OperatorProfile*: Can view certain pages. This profile is prohibited from making changes to system settings or accessing the CLI.

Access Permissions

The following table shows the default settings for the predefinedprofile types:

Access Permissions	Operator Profile	SuperAdminProfile
System status	Read	Read/Write
System Access	None	Read/Write
System Configuration	None	Read/Write
System Maintenance	None	Read/Write
Virtual Security Analyst	Read	Read/Write
Logs and Reports	None	None

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*.
Log and Reports	Grant permissions to access logs and reports. Click *Custom* to grant access to *Events* logs or *Other Logs and Reports (Except Events)*. To create a user group that can access all logs and reports except *Events*, configure the following: • **Events**: None • **Other Logs and Reports (Except Events)**: Read/Write To create a user group that can only access event logs, configure the following: • **Events**: Read/Write • **Other Logs and Reports (Except Events)**: None

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*.

   Available Sensors under administrator profile is an important setting as it affects the user's ability to view sensors data in Dashboard, Network Insights, logs etc.

5. Click *OK*.

Sensor/Center settings

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

The *Center Settings* page displays the following information:

Hostname	The sensor hostname.	
IP Address	The sensor IP address.	
Model Name	The sensor model name.	
Serial Number	The sensor serial number.	
Status	The connection status.	
	Registered	Indicates that the Sensor has completed the registration process but has yet to undergo a license check.
	Connected	Indicates the Sensor is prepared for synchronization and is actively transmitting data to the Center.
	No Data Transferred	Indicates the Sensor has not sent any data to the Center for a span of 3 minutes while still maintaining a connection.
	Firmware Mismatched	Indicates the Sensor's firmware is incompatible with the Center, and the Sensor is currently disabled. This does not mean the Sensor is inoperative. However, the Center will not accept any data from it.
	Sensor License Invalid	Indicates that the Sensor does not possess a valid license, and has been disabled.
	Disabled By User	Indicates the Sensor has been manually disabled by a user in the Center. This does not mean the Sensor is inoperative. However, the Center will not receive any data from it.
FortiGuard Status	Compares the Sensor's FortiGuard updates against the Center's FortiGuard updates. *FortiGuard Update Available* will appear if an update is required.	
Last Updated	The date the sensor was last updated.	
CPU Usage	The CPU usage as a percentage.	
Disk Usage	The disk usage as a percentage.	
Memory Usage	The memory usage as a percentage.	

The following options are available:

Reboot Sensor	Initiates a reboot command for the selected Sensor.
Ping Sensor	Sends a ping command to the chosen Sensor, to test its connectivity.
Disable Sensor	Changes the status of the selected Sensor to *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*.

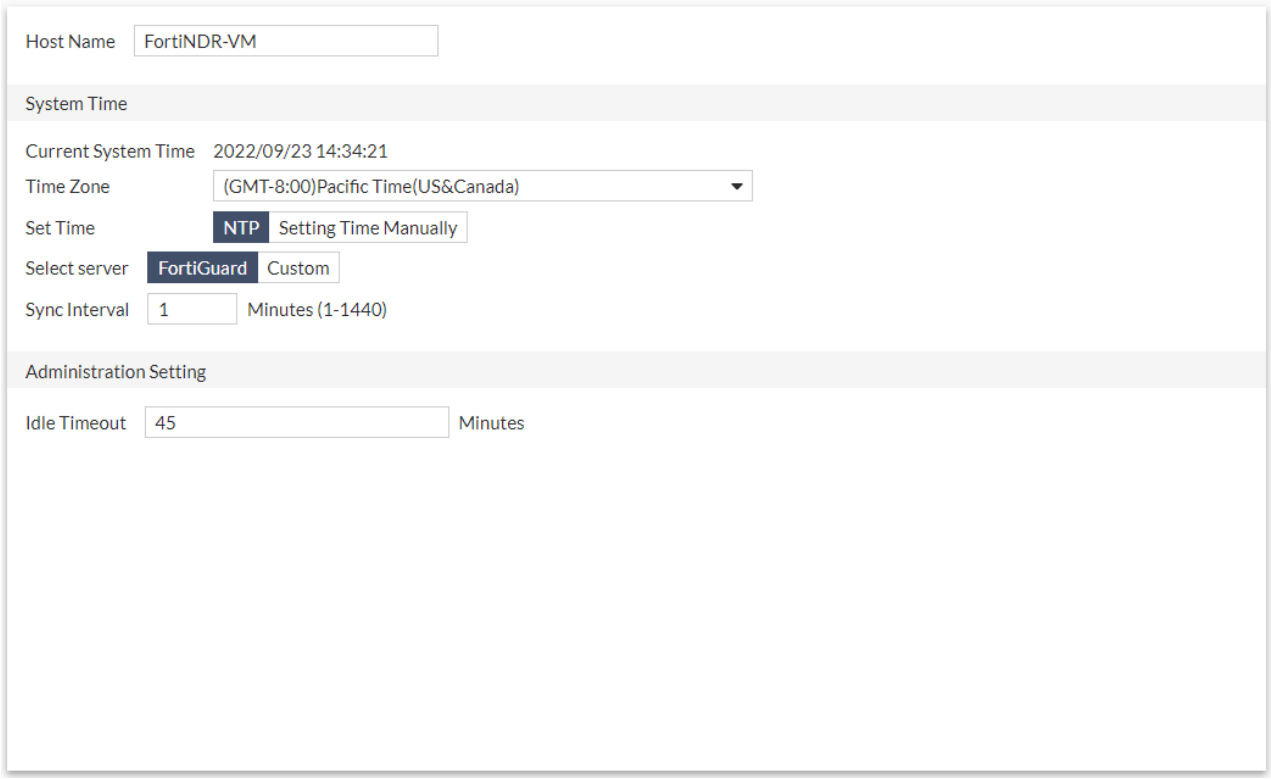
Settings

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.



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:

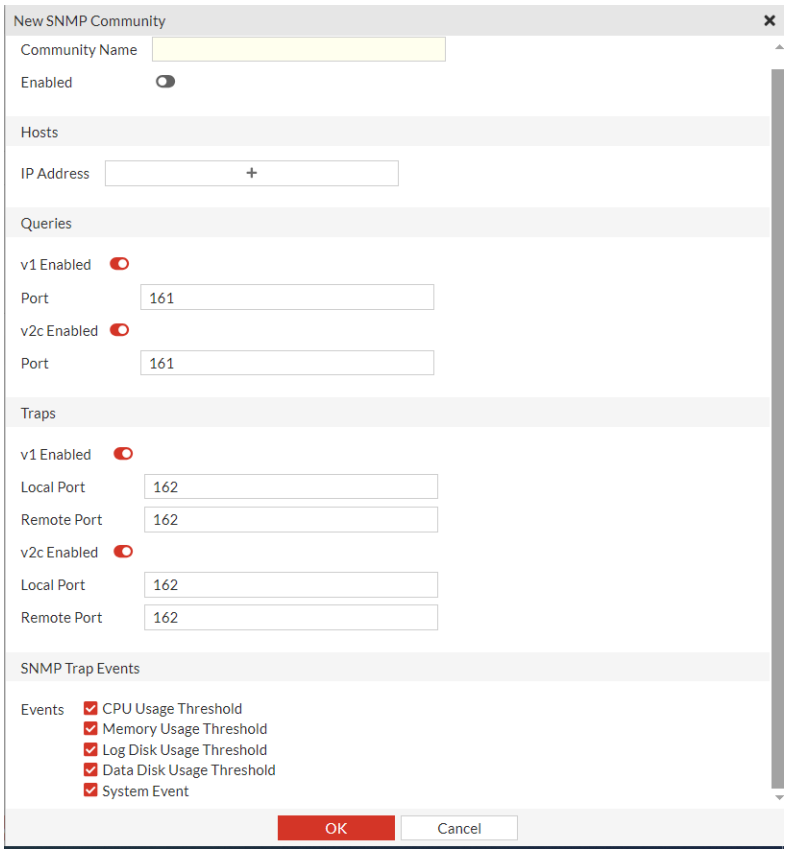
1. Configure interface access:
   a. Go to *Network* > *Interface* and double-click the *port1* interface to edit it.
   b. Under *Administrative Access*, enable *SNMP*.
   c. Click *OK*.

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:

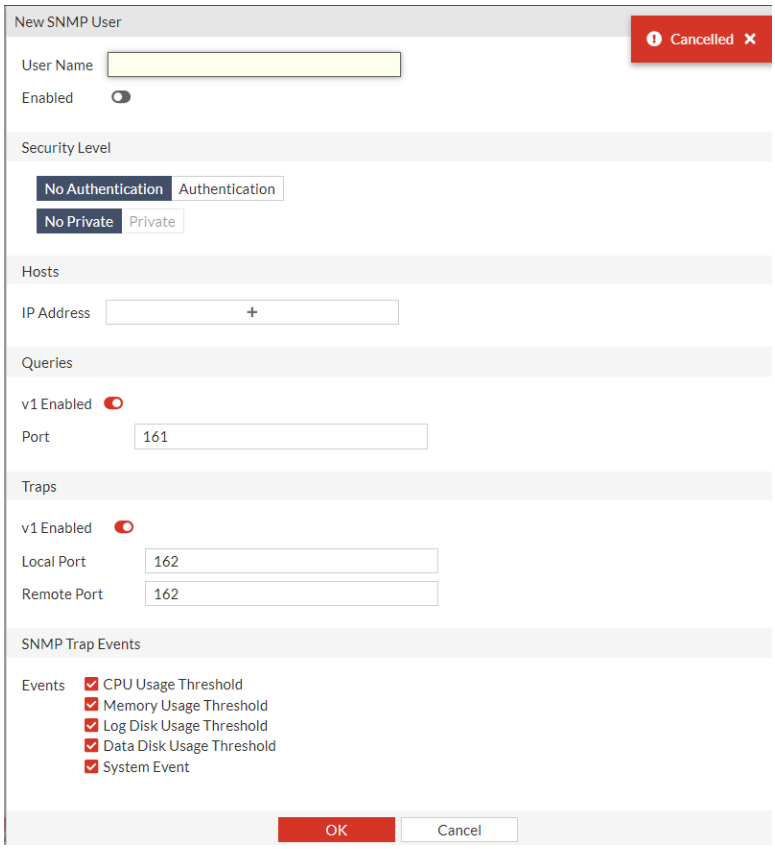
Community Name	Enter the name of the community.
Hosts	*IP Address*: Click the plus sign (**+**) to enter the IP address for each SNMP manager.
Queries	Enable or disable v1 and v2c queries, then enter the port numbers that the SNMP managers in this community will use.
Traps	Enable or disable v1 and v2c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



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.



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.
FORTINET-FORTINDR-MIB.mib	The FortiNDR MIB includes all system configuration and trap information that is specific to FortiNDR product.

MIB file name	Description
	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.

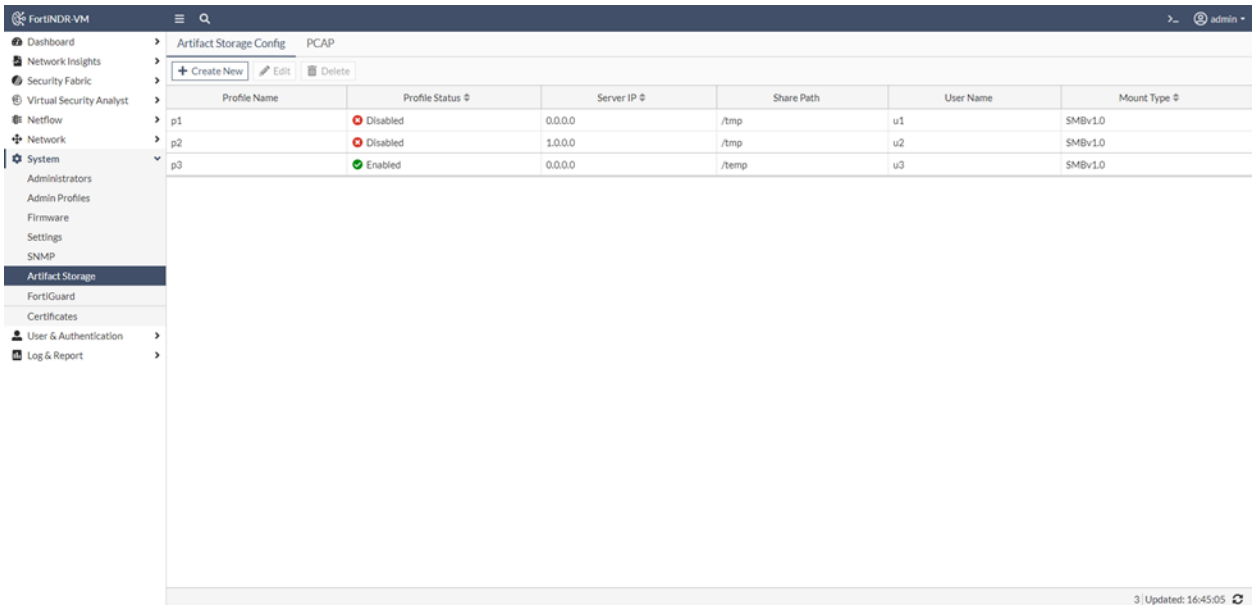
Example:

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
```

Artifact Storage (Standalone and Sensor)

Use the *Artifact Storage* page to manage storage profiles and PCAP configuration.



Artifact Storage Config tab

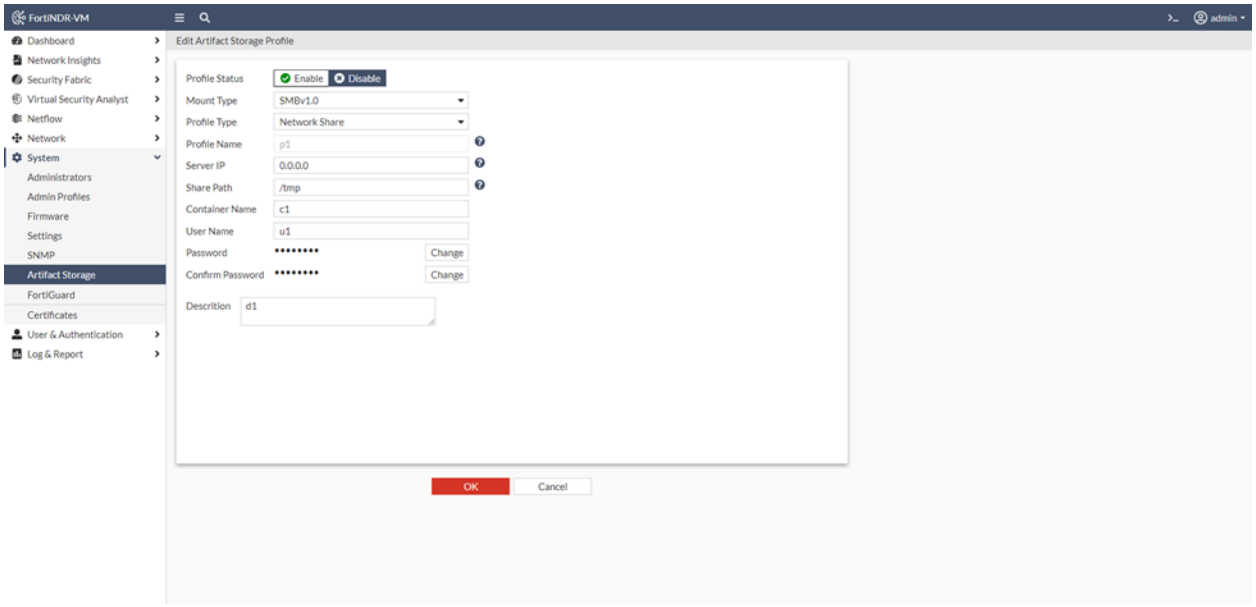
Use the *Artifact Storage Config* tab to create, edit, delete, and view a storage profiles. The *Edit* and *Delete* buttons will be enabled when you select a storage profile.

To create a storage profile:

1. Go to *System* > *Artifact Storage* and click *Create New*.
2. Configure the following settings and click *OK*.

Profile 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
Profile Type	Select the profile type from the dropdown list.
Profile Name	Enter a profile name.
Server IP	Enter the server IP. This IP should be unique among all existing storage profile entries.
Share Path	Enter the share page for the profile. This path should be unique among all

	existed storage profile entries.
Container Name	Enter the container name.
User name	Enter the username for the profile.
Password	Enter the password for the profile and then confirm the password.
Description	Enter a description of the profile.



PCAP tab

Use the *PCAP* tab to enable and configure PCAP recording rules.

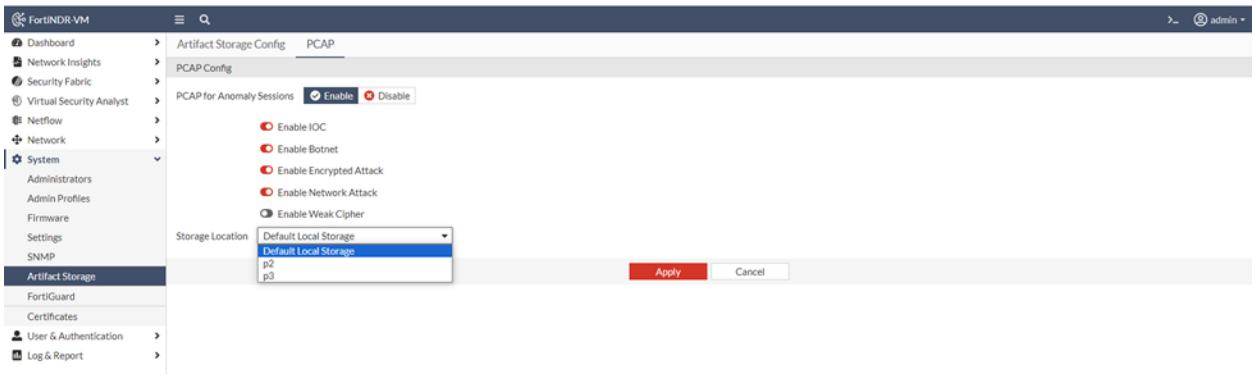
- The number of deflection and observation session captures and packets that can be collected will depend on the device model.
- This feature is not supported on VM models.
- The maximum size of each capture file is 1 MB.
- PCAP availability is commonly subject to latency.
- The tested FortiNDR-1000F max throughput when `pcap-dump` is enabled is 2Gbps for 1 hour.

To configure PCAP recording rules:

1. Go to *System* > *Artifact Storage* and click the *PCAP* tab. The *PCAP config* page opens.
2. Configure the following settings and click *Apply*.

CAP for NDR Detection or Observation Sessions	Enable to configure the type of network event you want to capture as a PCAP file. Enabled by default.

Enable IOC	Enable to capture IOC events as a PCAP file. Enabled by default.
Enable Botnet	Enable to capture Botnet events as a PCAP file. Enabled by default.
Enable Encrypted Attack	Enable to capture Encrypted Attack events as a PCAP file. Enabled by default.
Enable Network Attack	Enable to capture Network Attack events as a PCAP file. Enabled by default.
Enable Weak Cipher	Enable to capture Weak Cipher events as a PCAP file.
Default Local Storage	Set the storage location for the PCAP files. The storage location options are pulled from the *Artifact Storage Config* tab. Only artifact storage profiles with the *Profile Status* set to *On* are listed.



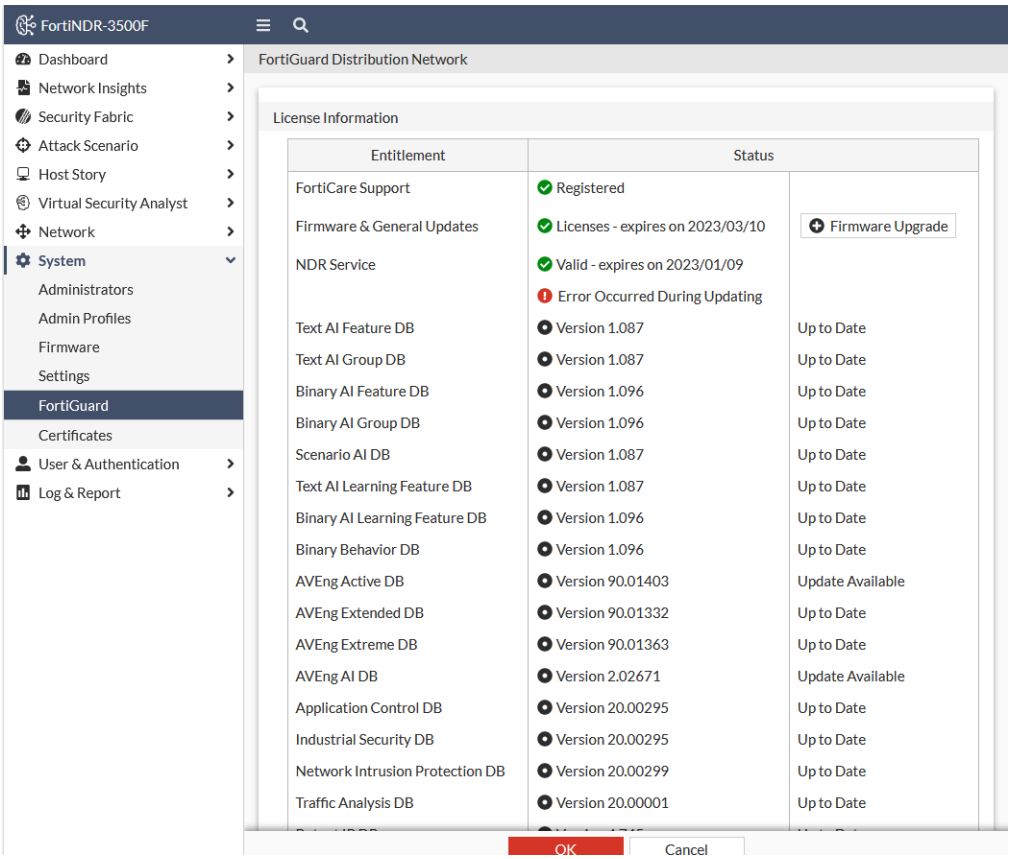
FortiGuard

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 294. To view a list of updates, go to *System* > *FortiGuard*.

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

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

Please refer to Appendix D: FortiGuard updates on page 294 and CLI guide for more detail.



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

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

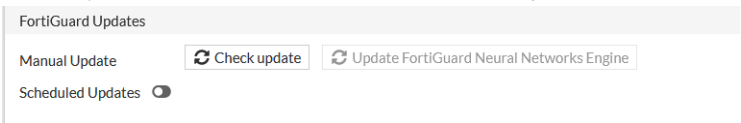
Currently, FortiNDR retrieves ANN updates from US and EMEA FortiGuard servers.

FortiNDR selects the update server based on proximity and location.

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

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

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



2. Click *Update FortiGuard Neural Networks Engine*.
   This triggers an install of the new ANN.
   Because the ANN update is several GB in size, this procedure might take several hours. You can log out of the GUI after the update has started.

To update the ANN database using the CLI:

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

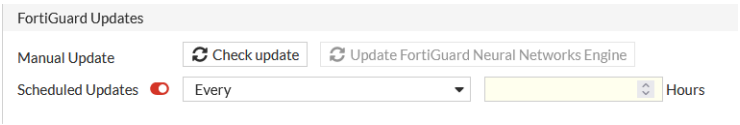
```
# execute restore kdb ftp pae_kdb.tar.gz 2.2.2.2 user password
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Connect to ftp server 2.2.2.2 ...
Please wait...
Get file from ftp server OK.
Get file OK.
MD5 verification succeed!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

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

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

To schedule FortiGuard updates:

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



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

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 retrieved 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.

Using FortiGuard Anycast servers

By default, FortiNDR will download some of the update packages from FortiGuard Anycast servers (*globalupdate.fortinet.net*). This Anycast server has one IP address to match its domain name. The FortiGate connects with a single server address, regardless of where the FortiGate is located.

For IOT device database updates, the Anycast setting must be enabled. If Anycast is disabled, the FQDNs *fds1.fortinet.net* and *fortiguard.net*update will be used.

To enable/disable Anycast with the CLI:

```
config system fortiguard update
   set anycast-status <enable/disable>
end
```

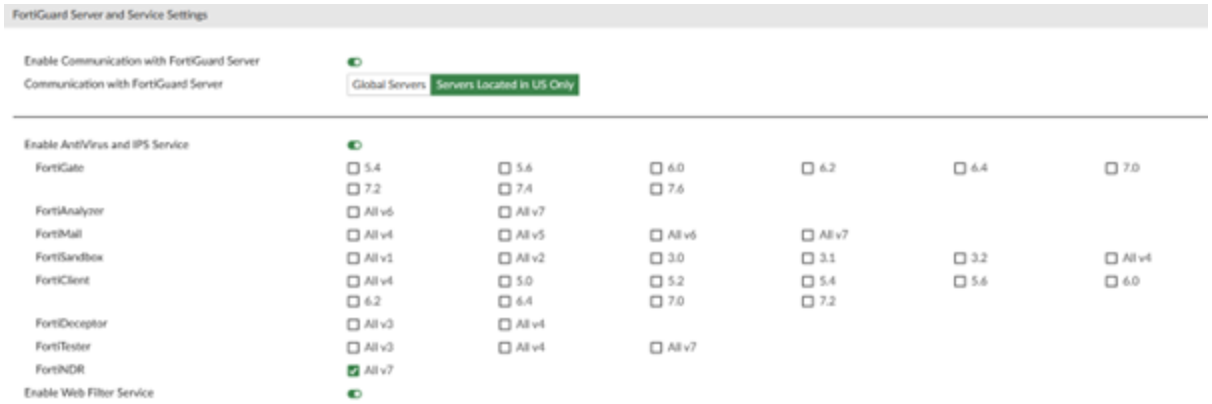
Using FortiManager for FDS updates

FortiNDR can download FortiGuard updates from FortiManager (starting with FortiManager v7.6.2).

Configuring FortiManager for FDS updates

To configure FortiManager support for FortiNDR updates:

1. Go to *FortiGuard > Settings*.
2. Under *Enable Antivirus and IPS Services*, enable the FortiNDR version.



To configure FortiManager with the CLI:

```
config fmupdate fds-setting
   set fortiguard-anycast enable
   set system-support-fai 7.x
end
```

Configuring FortiNDR for FDS updates

On the FortiNDR, set the update server override CLI settings:

```
config system fortiguard update
   set override-server-status enable
   set override-include-default-servers disable
   set override-server-main-port 8890 <--- for ANN and IPS updates
   set override-server-address-main {FortiManager_IP}
   set override-server-alt-port 8890 <--- for other DB updates
   set override-server-address-alt {FortiManager_IP}
   set anycast-status disable
end
```

FortiManager WebFilter and IOC queries

WebFilter and IOC queries can be directed to FortiManager. WebFilter queries will use FortiManager's web filter database, while IOC queries are proxied to FortiGuard servers.

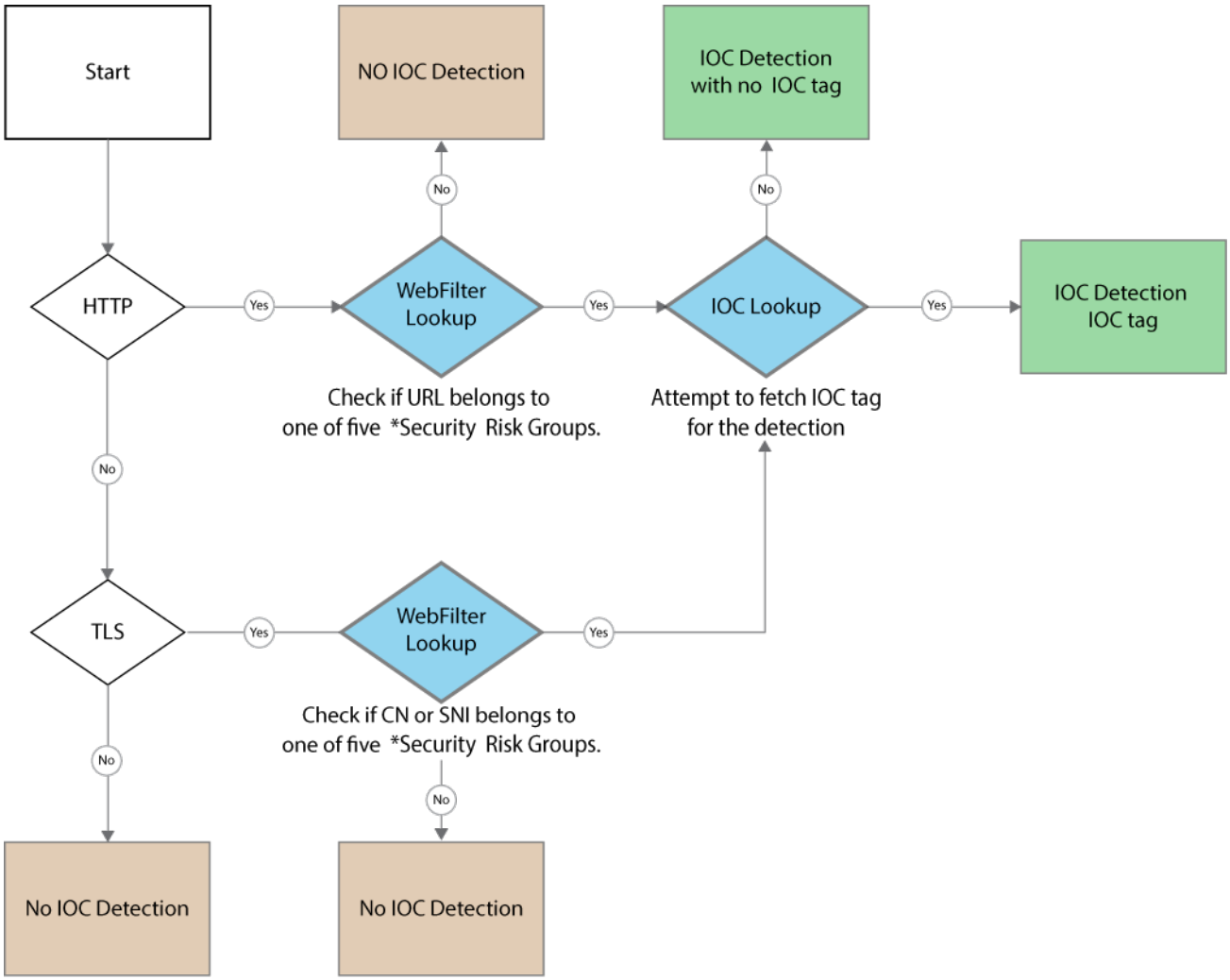
Security Risk Groups are used during web filtering to help identify potentially malicious traffic. When HTTP or TLS traffic is processed, the system checks if the URL (HTTP) or CN/SNI (TLS) belongs to one of the following groups:

- Newly Observed Domain
- Newly Registered Domain
- Dynamic DNS
- Spam URLs
- Phishing

If a match is found, an Indicator of Compromise (IOC) lookup is performed. Depending on the result, the system may trigger an IOC detection with or without an IOC tag. If no match is found, no IOC detection occurs.

Requirements:

- FortiManager v7.6.0



***Security Risk Groups**: Newly Observed Domain, Newly Registered Domain, Dynamic DNS, Spam URLs and Phishing

Configuring FortiManager for IOC/WebFilter query

On the FortiManager, enable the WebFilter and IOC query server:

```
config fmupdate service
   set query-ioc enable
   set query-webfilter enable
end
```

Configuring FortiNDR for IOC/WebFilter query

To use FortiManager as a query server, on the FortiNDR ,set the CLI:

To configure the WebFilter:

```
config system fortiguard webfilter
```

```
   set override-server-status enable
   set override-server-address {FortiManager IP}
   set override-server-port 8888
end
```

To configure the IOC query server:

```
config system fortiguard ioc
   set override-server-status enable
   set override-server-address {FortiManager IP}
   set override-server-port 8888
end
```

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.

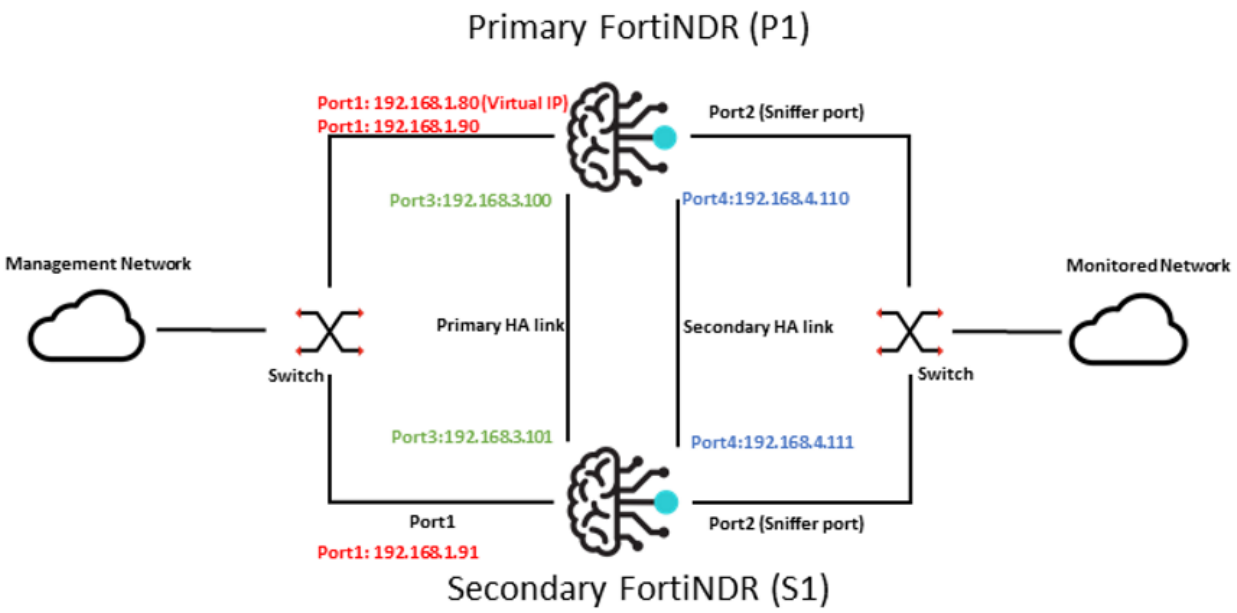
High Availability (HA) is only available in Standalone mode.

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 228.
- 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:



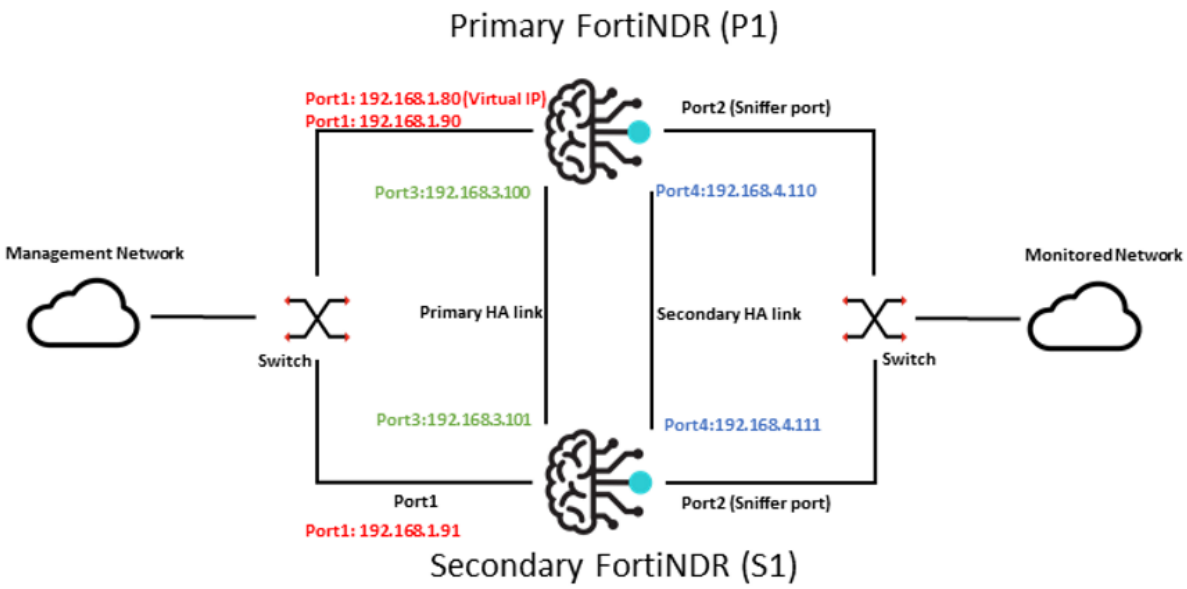
Configuring an HA group

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 294).

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

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

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

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 235.
`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 231.
   - Ensure no errors appear on the HA event log. See, HA Logs on page 235.

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 234.
- 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
```

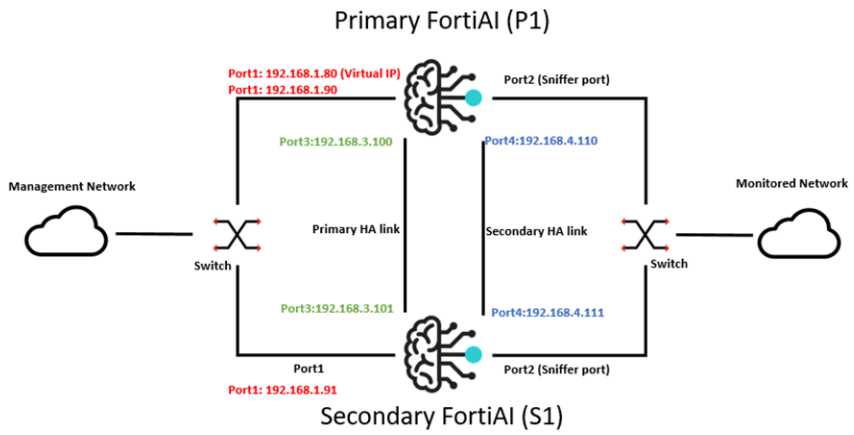
To check the HA status with the GUI:

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.

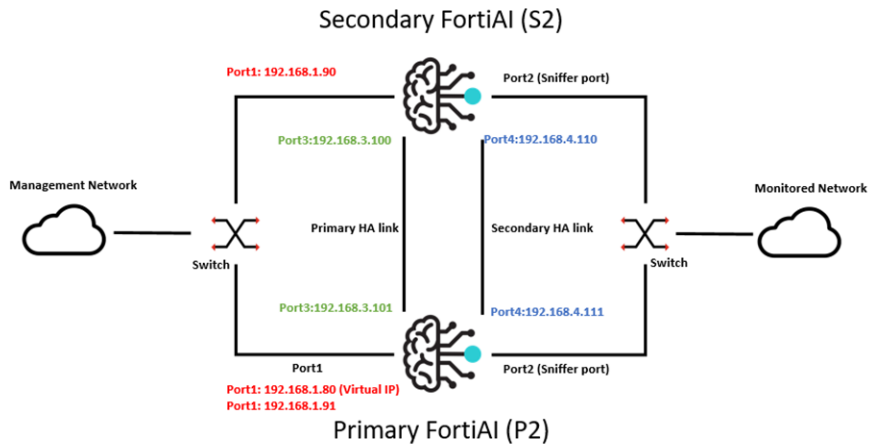
HA Failover

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:

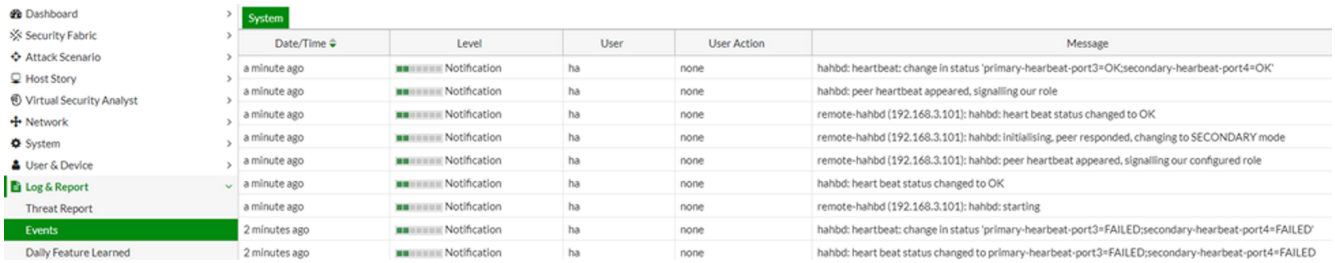
Configuration Settings	Description
HA Settings	HA related configurations
Network Settings	System network settings including: • System interface settings • System DNS settings • System Route settings
Host name	The host name distinguishes members of the HA group.
Default certificates	The default certificates.
FortiGuard update settings	The FortiGuard update settings are not synchronized.

Configuration Settings	Description
	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.



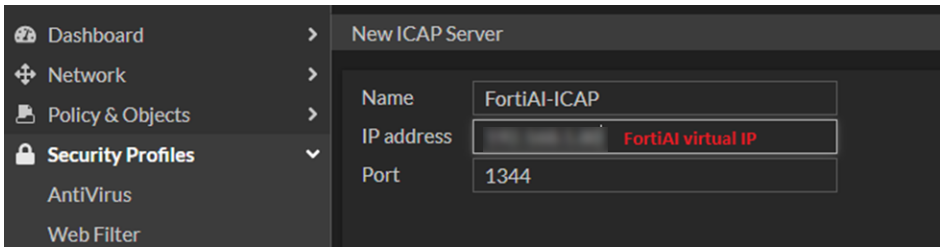
Using Virtual IP

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 228.

Example: Configure FortiGate ICAP server with FortiNDR virtual IP

Instead of using the actual IP, you will need to provide the Virtual IP of the HA group when creating an ICAP server profile on FortiGate.

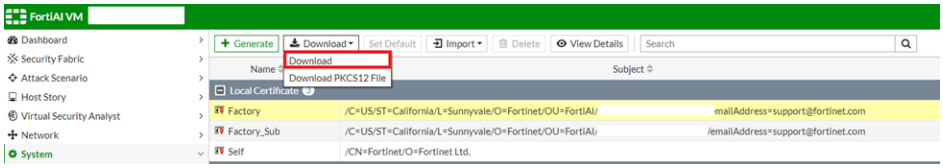


Example: Configure FortiGate Security fabric settings for inline blocking

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

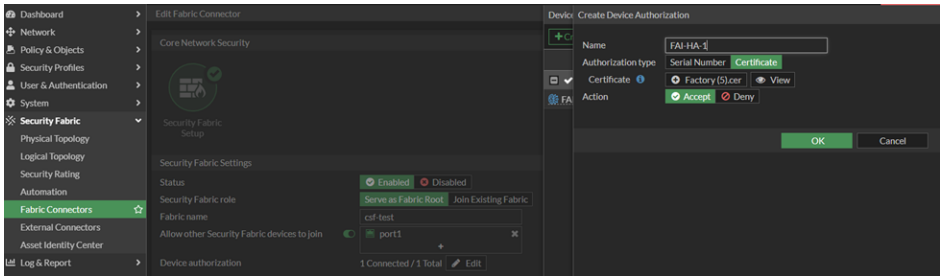
To configure FortiGate for inline blocking:

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



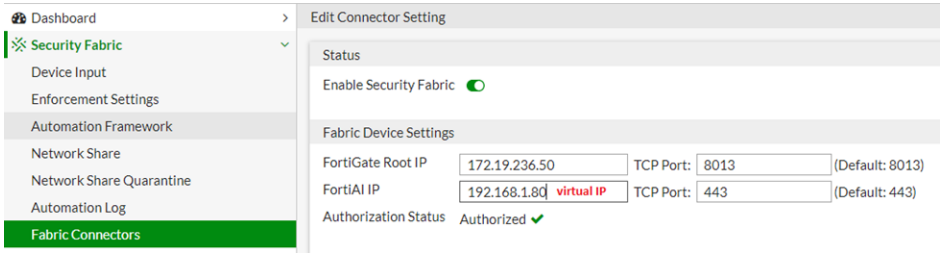
To add the certificate to FortiGate

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



To enable FortiGate inline blocking:

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



> You are not required to configure inline blocking on the secondary unit since the configuration will be synchronized.
>
> For detailed information about inline blocking configuration, see FortiGate inline blocking (FOS 7.0.1 and higher) on page 154.

Conserve Mode

FortiNDR provides high-throughput malware scanning, published at 100K for FortiNDR-3500F under ideal lab conditions. Conserve Mode is triggered when either of the following conditions is met:

- *Submission Backlog Queue*: The submission backlog queue becomes too high.
- *High Disk Usage*: Disk usage exceeds a critical threshold. Conserve Mode is triggered to prevent potential system instability.

In Conserve Mode, the system will:

- Continue scanning files already in the queue but stop accepting new files.
- Temporarily halt network traffic analysis and detection to conserve system resources and maintain stability.

These measures ensure the system remains stable and efficient, even during high resource usage or heavy load.

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

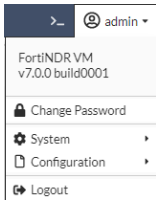
Please record these configuration settings before upgrading so the full configuration can be restored.

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 with FortiAuthenticator v7.6.2 and later. When enabled, users are prompted to enter their 2FA token code. Push-based 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.
Access Profile Override	Enable or disable the *Fortinet-Access-Profile* attribute to override the administrator profile. For more information, see *Administrator Access Group Mapping* in Creating remote wildcard administrators on page 245.

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 following 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 click *Edit*.
3. Configure the LDAP server setting and click *Apply current settings*. Optionally, you can click *Reset settings* to return to the default settings.
4. Click *OK*.

LDAP user query example

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

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

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

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

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

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

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

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

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

Alias member query example

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

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

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

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

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

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

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

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

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

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

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

Preparing your LDAP schema for FortiNDR LDAP profiles

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

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

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

Using common schema styles

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

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

If both of those conditions are true, your LDAP profile configuration may also be very minimal. Some queries in LDAP profiles contain schema options that automatically configure the query to match common schema styles such as IBM Lotus Domino, Microsoft Active Directory (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:

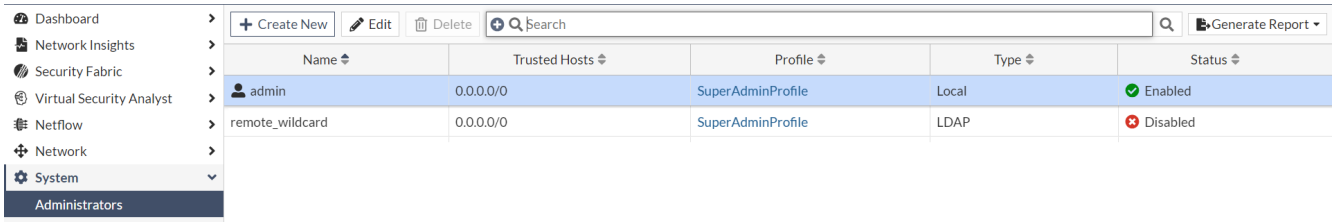
1. In the LDAP profile, enter the domain name or IP address of the LDAP server.
2. Configure the LDAP profile queries:
   - In *User Query Options*, from *Schema* which OpenLDAP schema your user objects follow: either InetOrgPerson or InetLocalMailRecipient. Also enter the *Base DN*, *Bind DN*, and *Bind* 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.



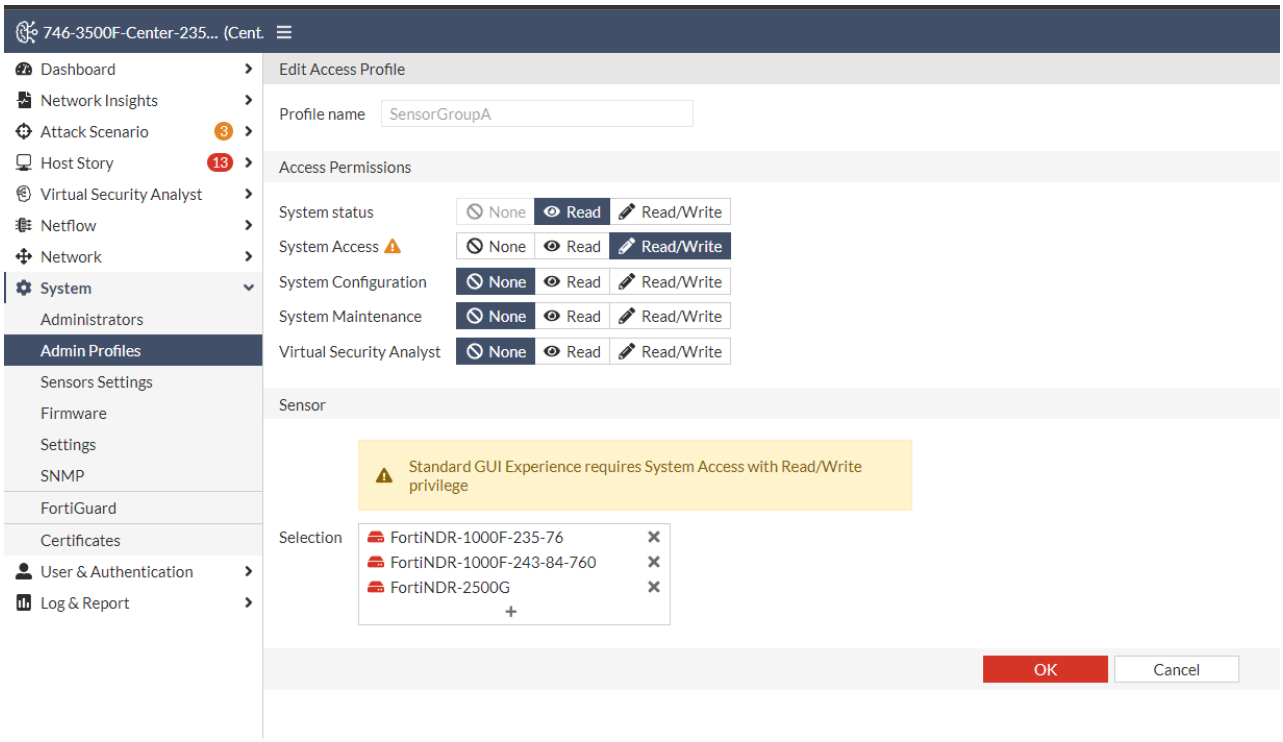
Assigning sensors to an admin profile

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 206

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.

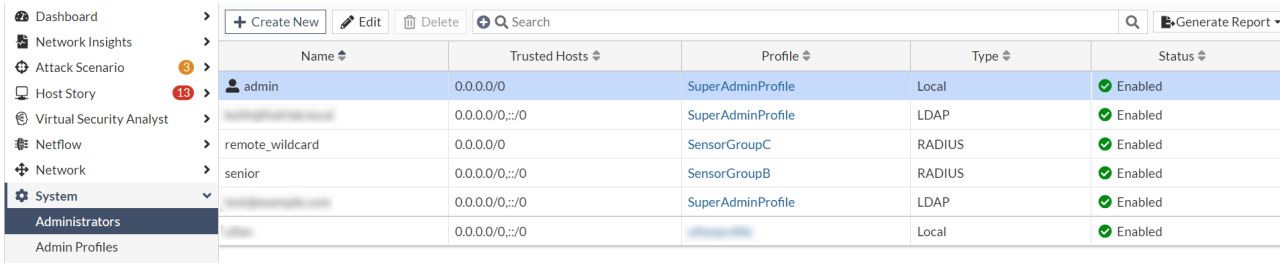


5. Click *OK*.

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

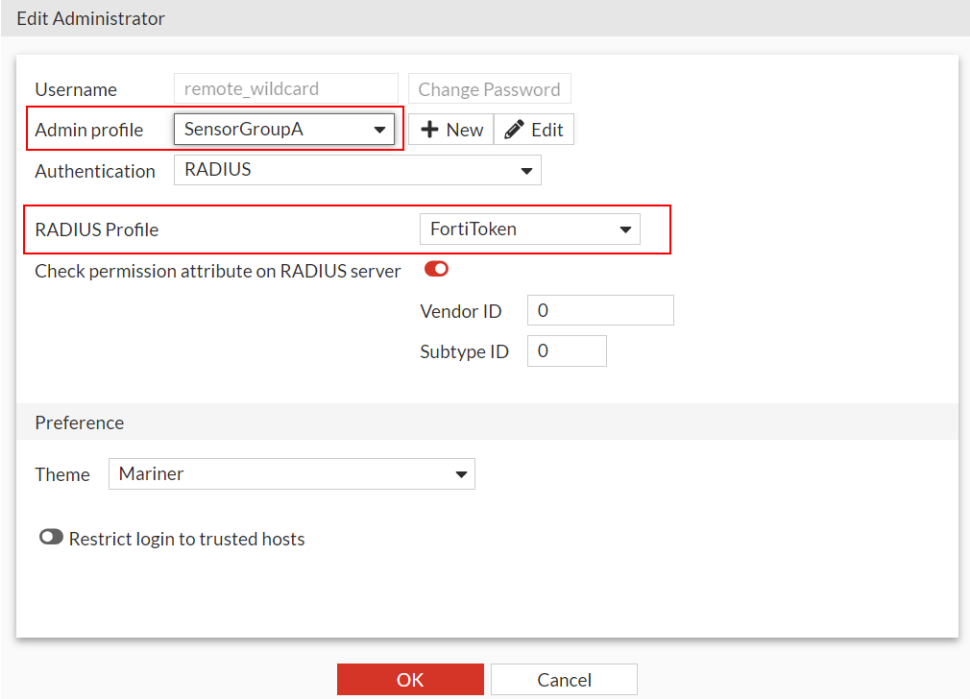
To assign the profiles to the *remote_wildcard* administrator:

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



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.



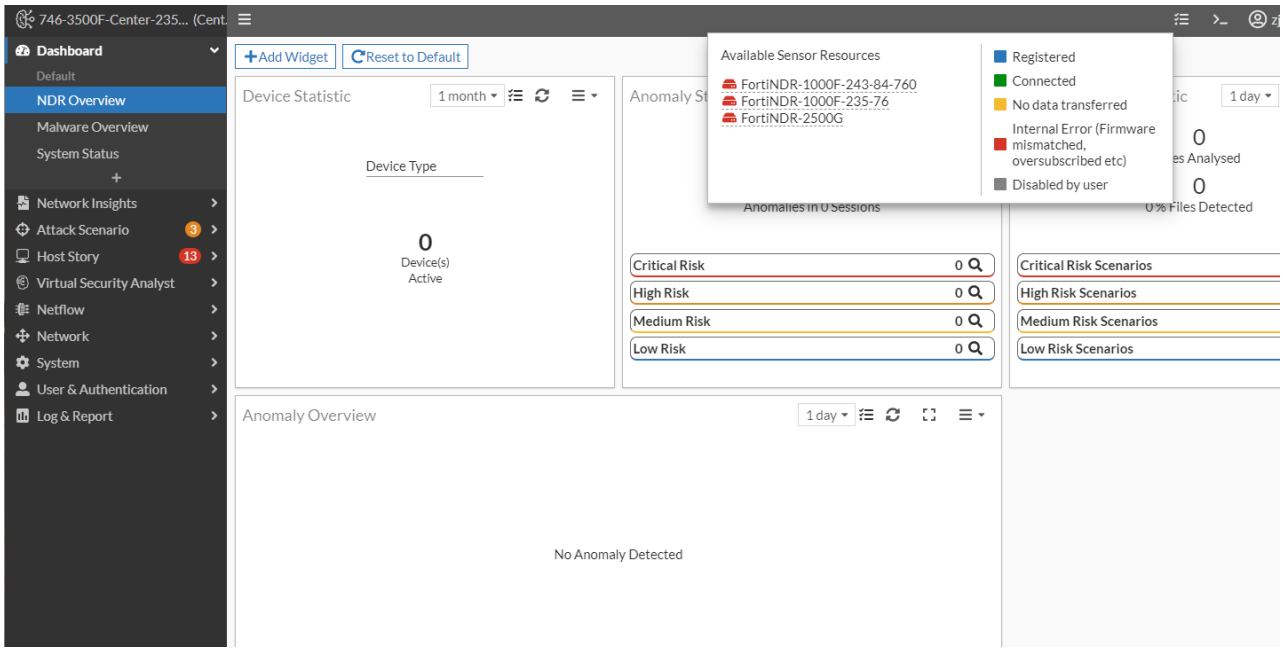
4. Click *OK*.

Resetting the available sensors resources in FortiNDR

When sensors are added or disabled in an admin profile, the Dashboard widgets retain the current sensor settings, even if those sensors are no longer available to the current account. To update the widget sensor settings for all users at once, including any newly registered sensors, click 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.

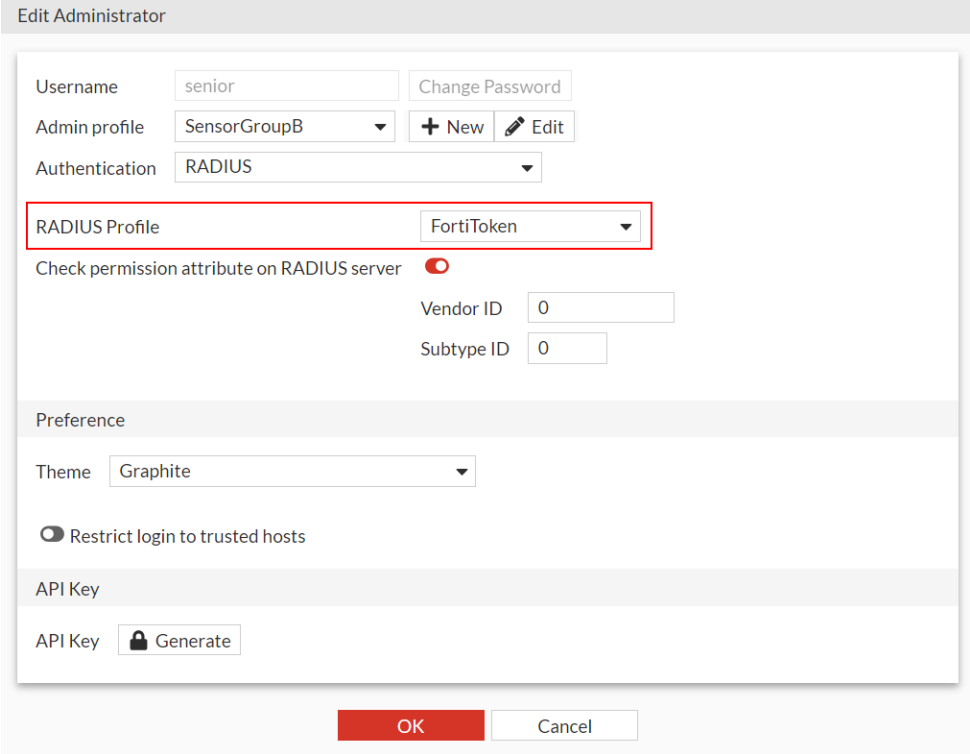
All users that access FortiNDR as a *remote_wildcard* administrator will see this dashboard view

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.
2. Create a new administrator. See, Administrators.
3. In from the *LDAP profile* or *RADIUS Profile* dropdown, select the profile used by the *remote_wildcard* administrator.



4. Click *OK*.

Administrator Access Group Mapping

Administrator Access Group Mapping allows administrators to override the access profile on the remote server. This saves time manually creating accounts with the proper access profile permissions for each machine. In addition to authentication, you can use Administrator Access Groups in the Active Directory to assign roles to users. For example, users in an *admin* group can have a *Read / Write* role whereas users in an *Operator* group may only have a *Read Only* role.

Enabling Administrator Access Group Mapping

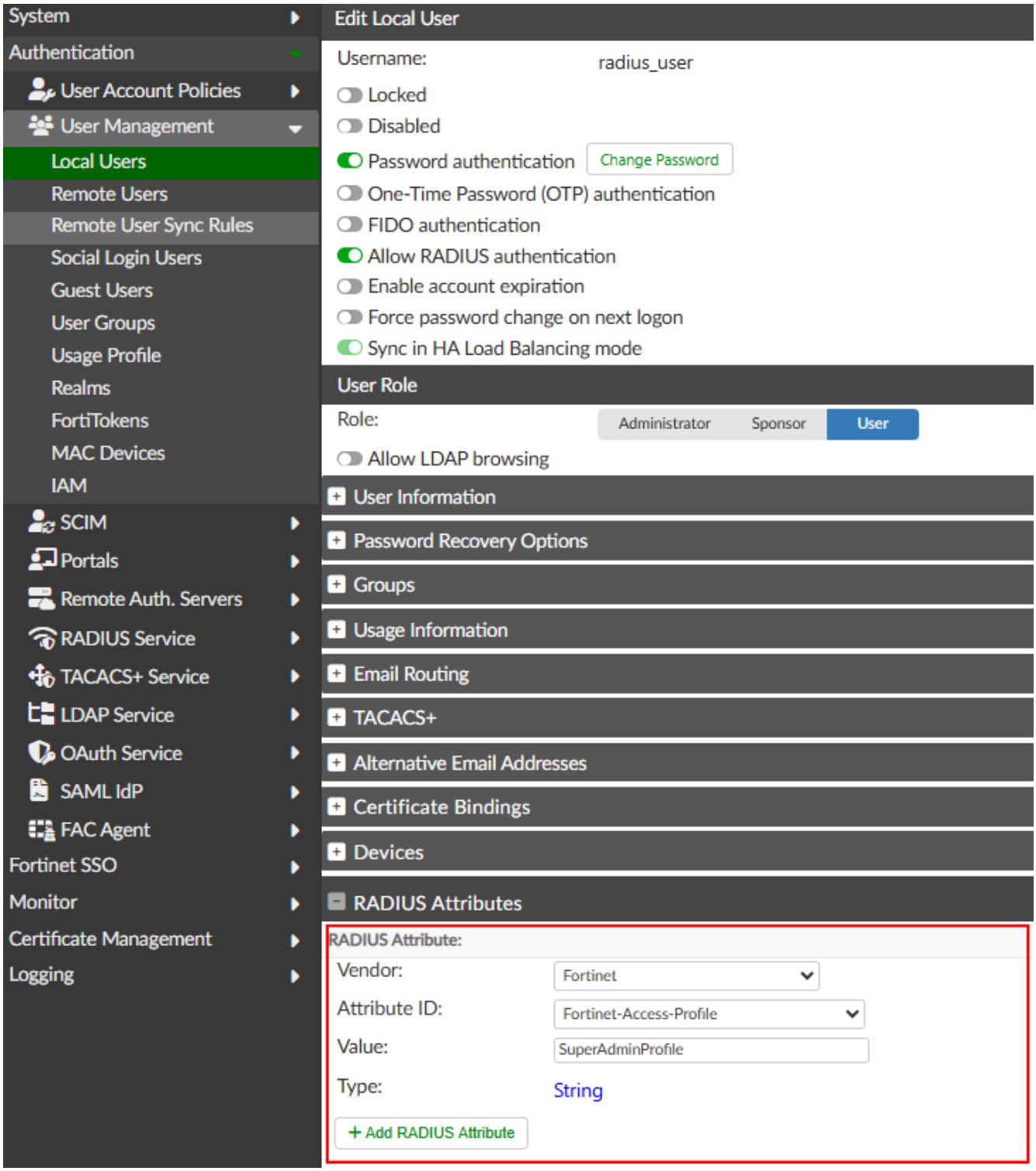
You can configure FortiNDR and the RADIUS server in any order as long as both are configured by the time authentication occurs.

To configure FortiNDR:

1. In FortiNDR, go to *User & Authentication* > *RADIUS Server*. Create or edit a new RADIUS profile. See, RADIUS Server on page 239
2. Ensure *Access Profile Override* is enabled.

To configure the RADIUS server:

- Configure the RADIUS server to include the attribute *Fortinet-Access-Profile* in the *Access-Accept message*. The following image shows an example configuration in FortiAuthenticator.



If the RADIUS server returns a *Fortinet-Access-Profile* attribute value that:

- Can be found in FortiNDR's admin profile list, the user's session Access Profile will be overridden to that profile.
- Cannot be found in FortiNDR's admin profile list, the user's session Access Profile will be mapped to the original profile set for that user.

Configuring Administrator Access Group Mapping with RADIUS

You can configure FortiNDR and the RADIUS server in any order as long as both are configured by the time authentication occurs.

To configure group mapping with RADIUS:

1. In FortiNDR , go to *User & Authentication* > *RADIUS Server*.
2. Create or edit a new RADIUS profile. See, RADIUS Server on page 239.
3. Enable *Access Profile Override*.

Configuring Administrator Access Group Mapping with LDAP

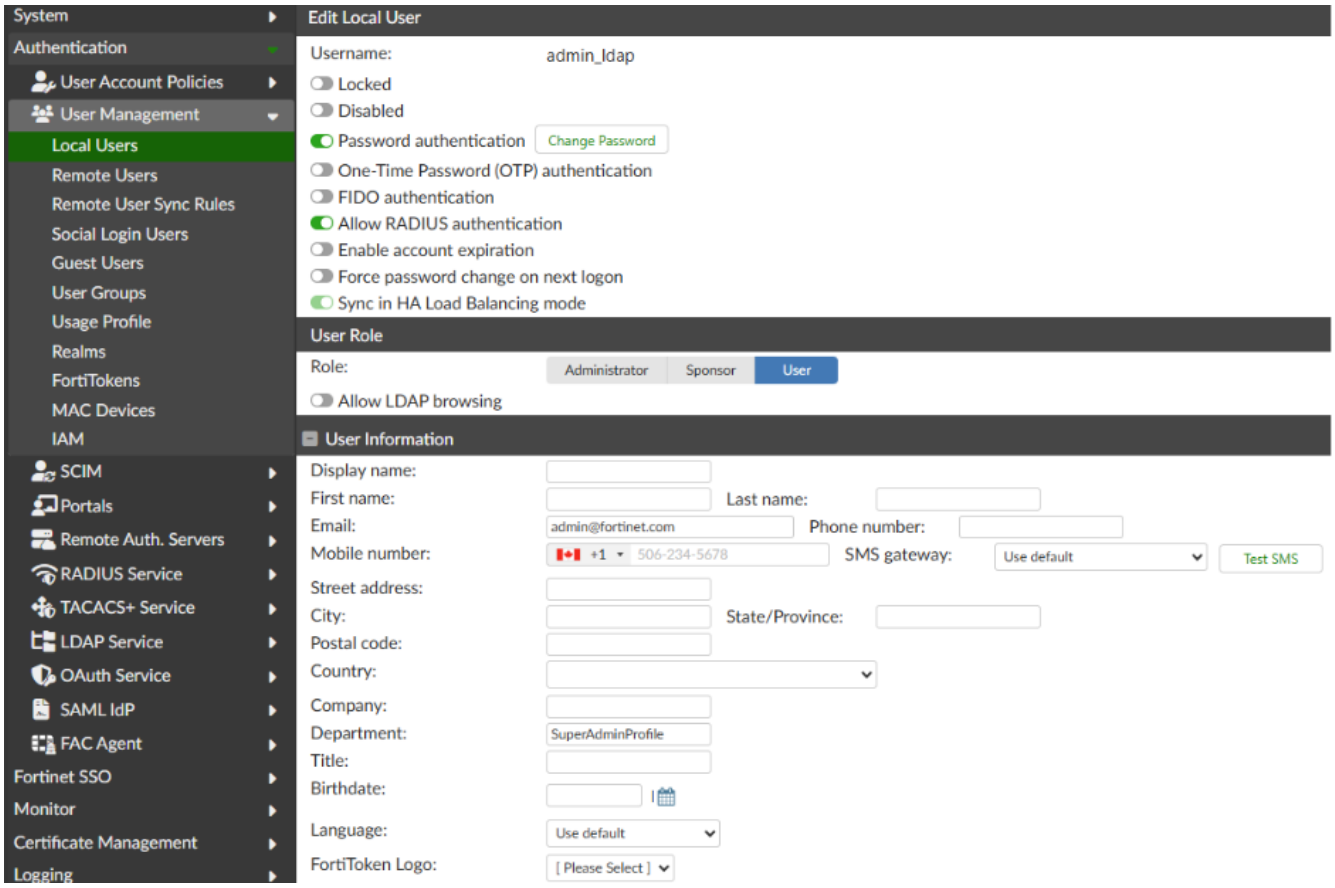
To configure group mapping with LDAP:

1. In FortiNDR, go to *User & Authentication* > *LDAP Server*.
2. Create or edit a new LDAP profile. See, LDAP Servers on page 240.
3. Open the CLI console and , enable `access-override` and `set access-override-attribute` to the attribute FortiNDR should use to override the user profile.

```
FortiNDR-VM (fac_test) # show
config profile ldap
  edit fac_test
    set server ldap.example.com
    set fallback-server ldap.example.com
    set base-dn dc=fortinet,dc=com
    set bind-dn uid=ldap_admin,cn=ldap_admins,dc=fortinet,dc=com
    set dereferencing find
    set query (&(objectClass=facPerson)(uid=$u))
    set cache-state disable
    set access-override enable
    set access-override-attribute Department
  next
end
```

To configure the LDAP server:

Configure the LDAP server to set the value attribute defined in FortiNDR with the profile name to override. The following image shows an example configuration in FortiAuthenticator.



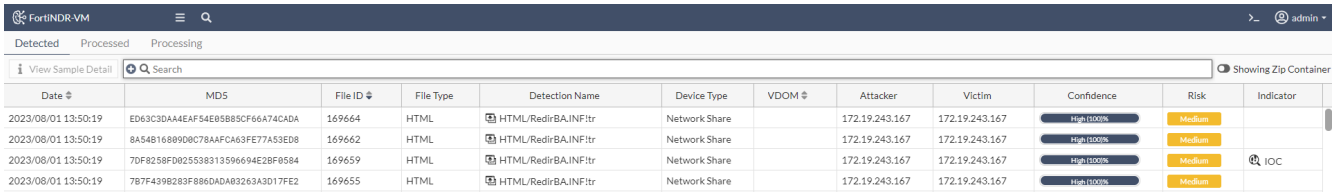
The value of the remote attribute returned by the LDAP server will override the locally configured user attribute if it matches an existing access profile. If no match is found, the default access profile configured in FortiNDR will be applied.

Log & Report

In Center mode, the ability for different administrators to see logs from different sensors is affected by the *Available Sensors* setting that is configured in admin profile settings under *System > Admin Profile*. Please ensure you have rights to see the sensor(s) logs.

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.



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* Please ensure you have the correction sensors selected under *Available Senors* under admin profile settings. See Admin Profiles on page 206.
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.

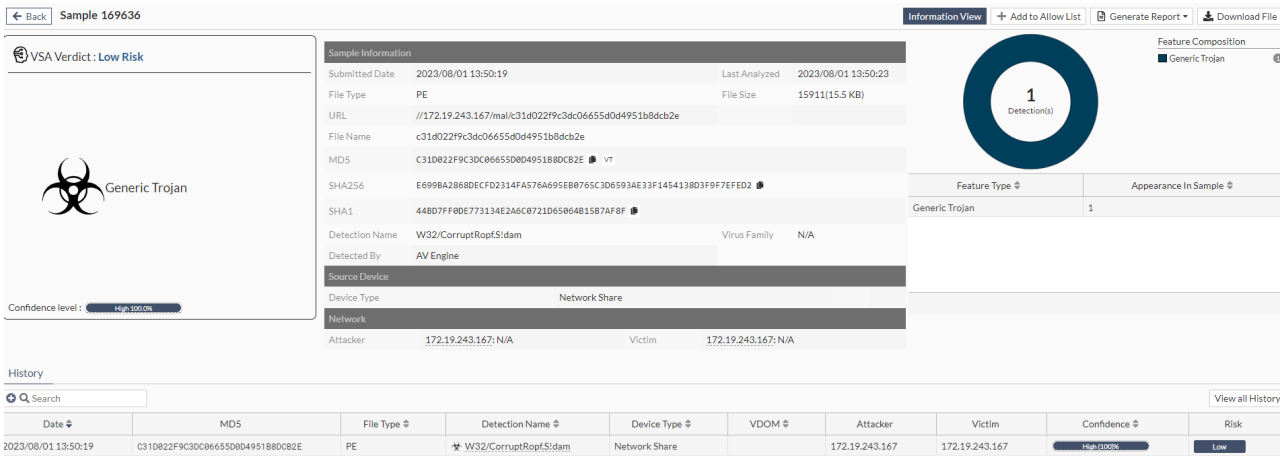
Device Type	The device type.
VDOM	The VDOM name.
Attacker	The attacker IP address.
Victim	The victim IP address.
Confidence	The confidence level as a percentage.
Risk	The risk verdict (High, Medium, Low or No Risk).
Indicator	Indicates the detection has IOC details.
Feature Detection	The detection feature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

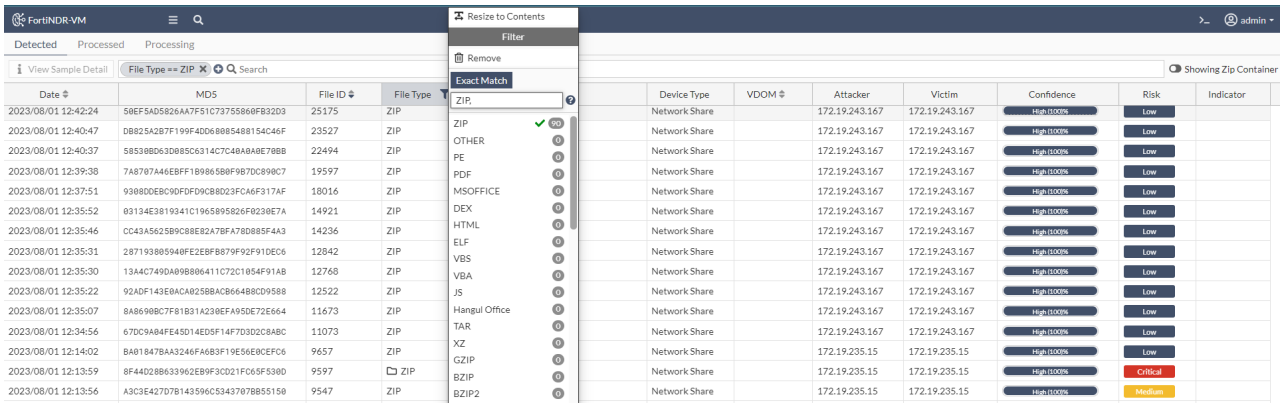
1. Go to *Log & Report* > *Malware Log*.
2. (Optional) Enable *Showing Zip Container* to download samples detected as malware.
3. Select a sample and click the *View Sample Detail* button at the left side of the *Search* field. The *Sample* details page opens.
4. Click the *Download File* button at the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



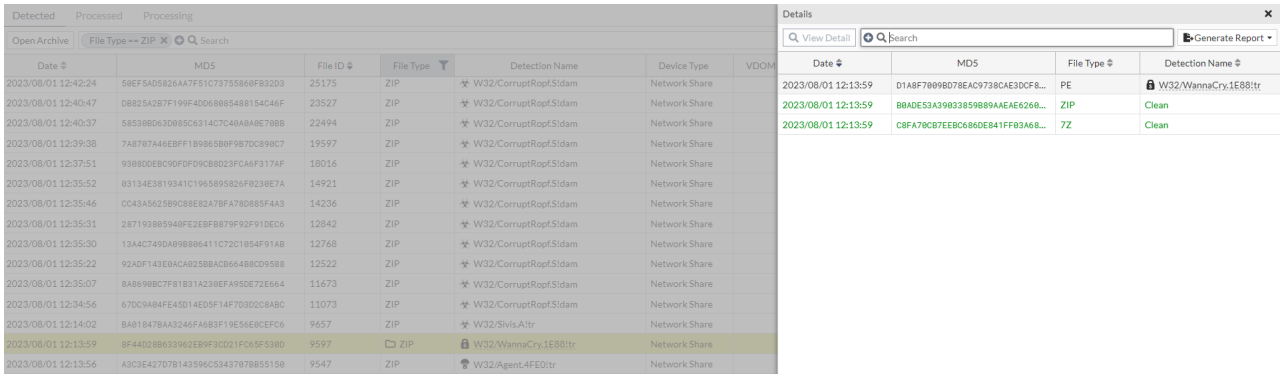
View items in a zip folder

To view items in a zip folder:

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



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



Perform a batch download

To perform a batch download:

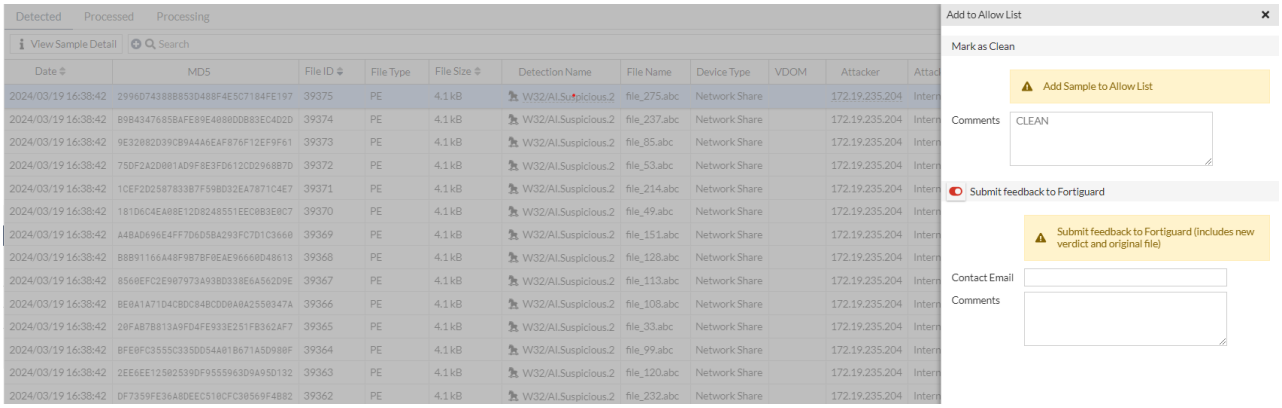
1. Select the files to download.
2. Click Batch Download. The files are zipped with a password and downloaded to your device.

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.



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:

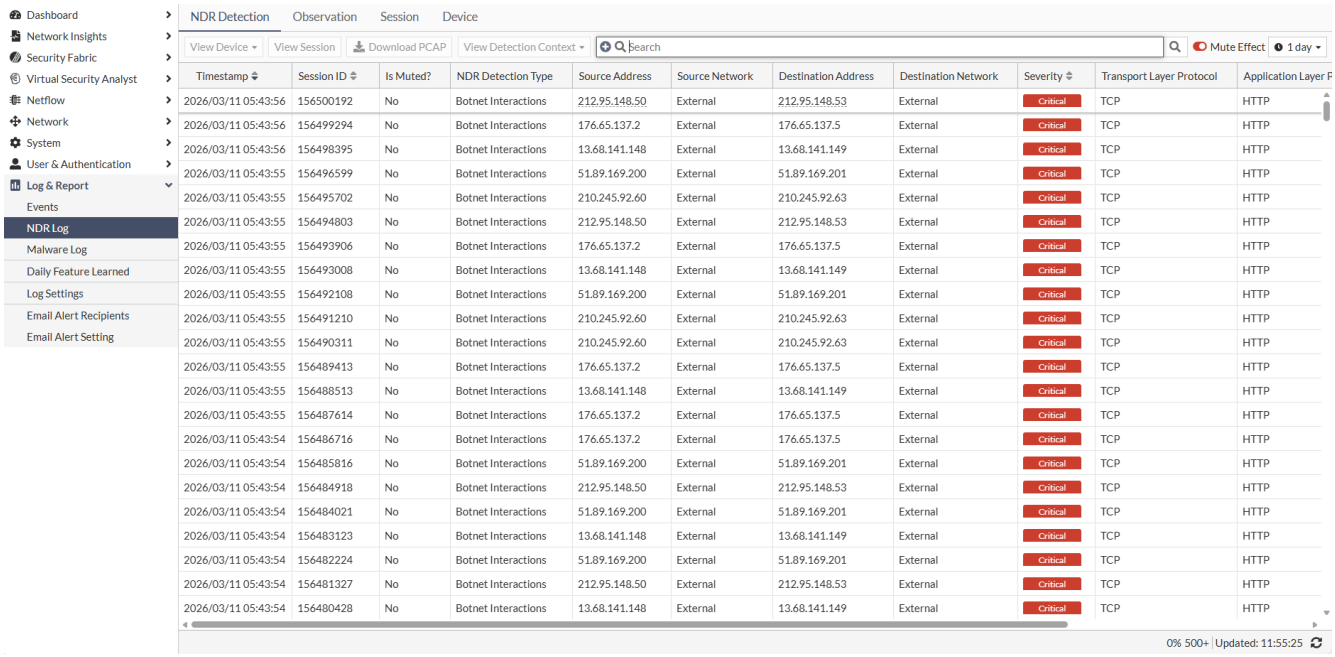
Right-click a detection and select one of the following options:

- *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

FortiNDR provides detailed NDR logs that capture and categorize network detections, observations, threats, and suspicious behaviors. These logs help you identify and respond to incidents such as botnet activity,

encrypted traffic, and intrusion attempts. Each log entry includes metadata such as timestamps, IP addresses, protocols, and severity levels, offering deep visibility into network events.



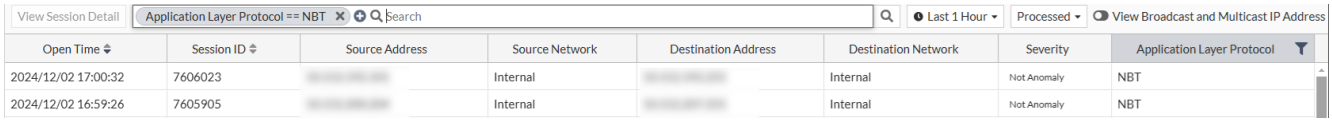
For information about the *NDR Detection* and *Observation* tabs see:

- NDR Detection tab on page 79
- Observation tab on page 83

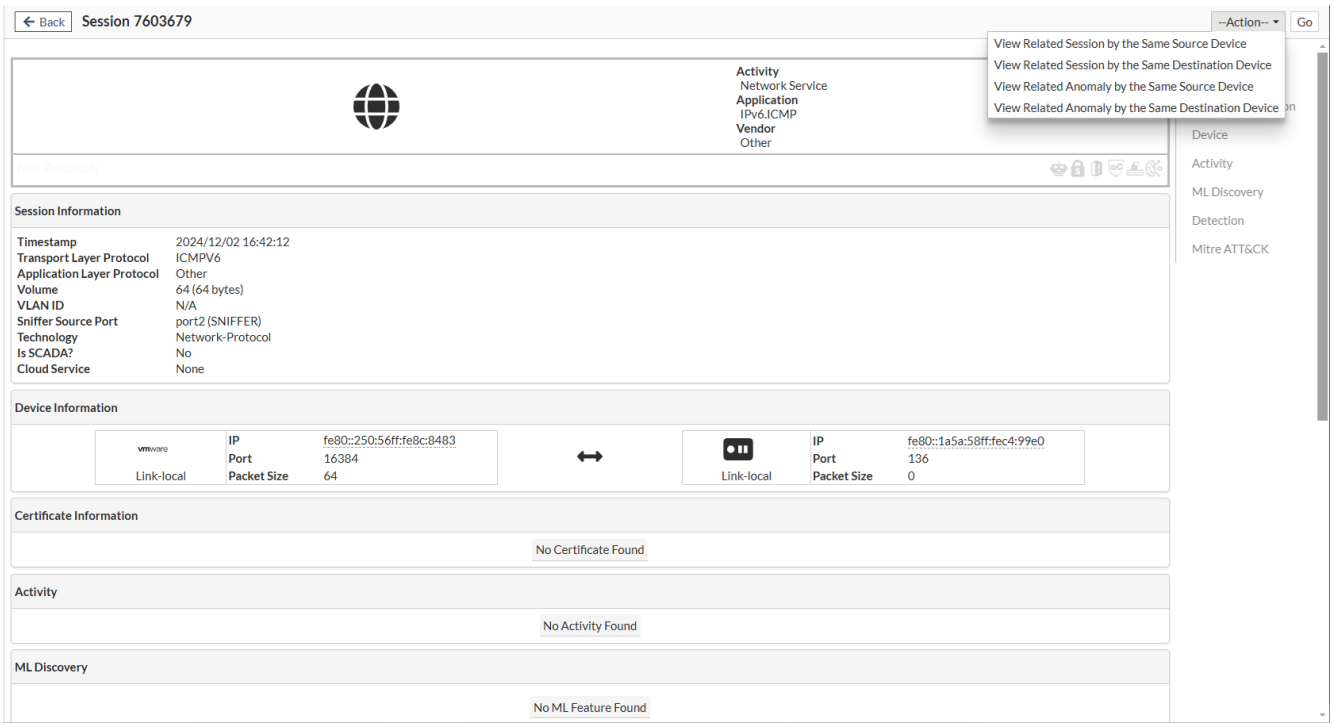
Session Tab

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

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

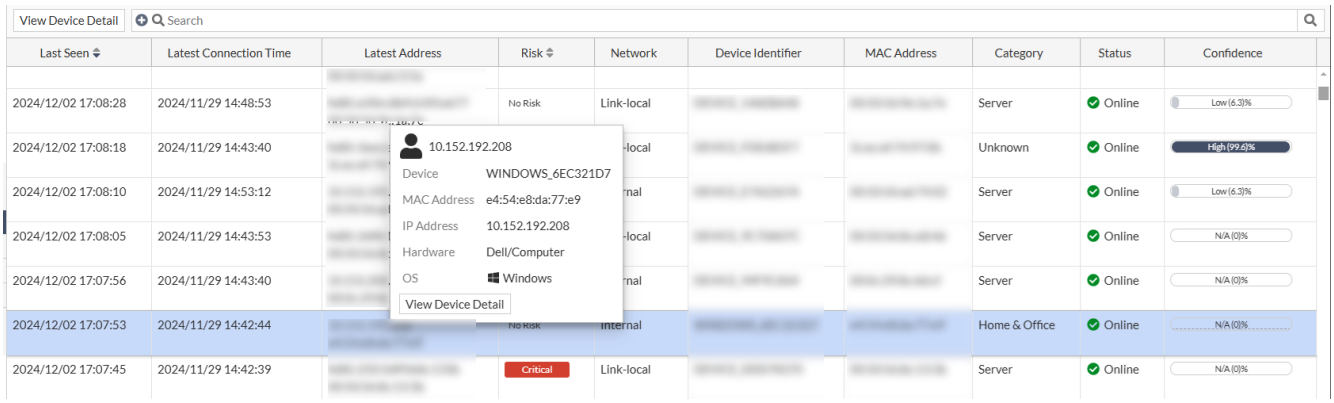


To drill down on the session information, click *View Session Detail*. Click the *Action* menu to view related information.



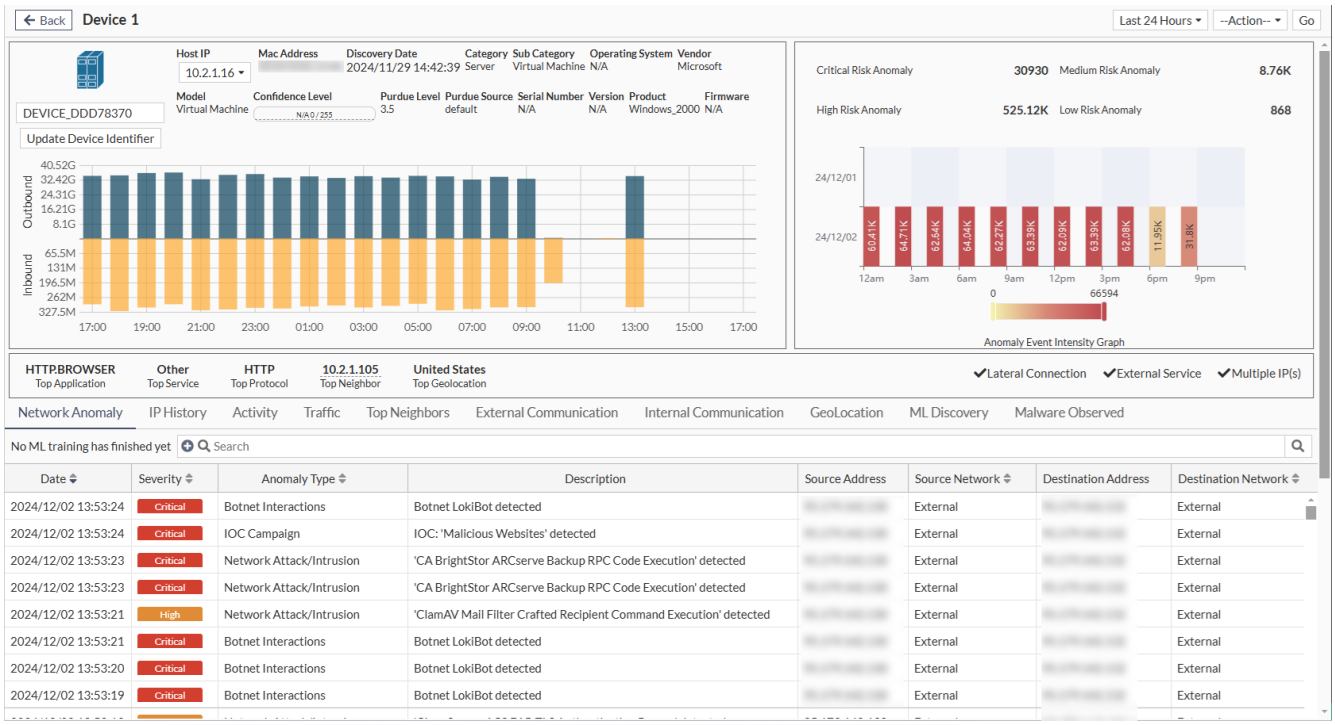
Device Tab

The *Device* tab shows 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 *Device* page by hovering over the *Latest Address* or *Device Identifier* and clicking *View Device Detail*.

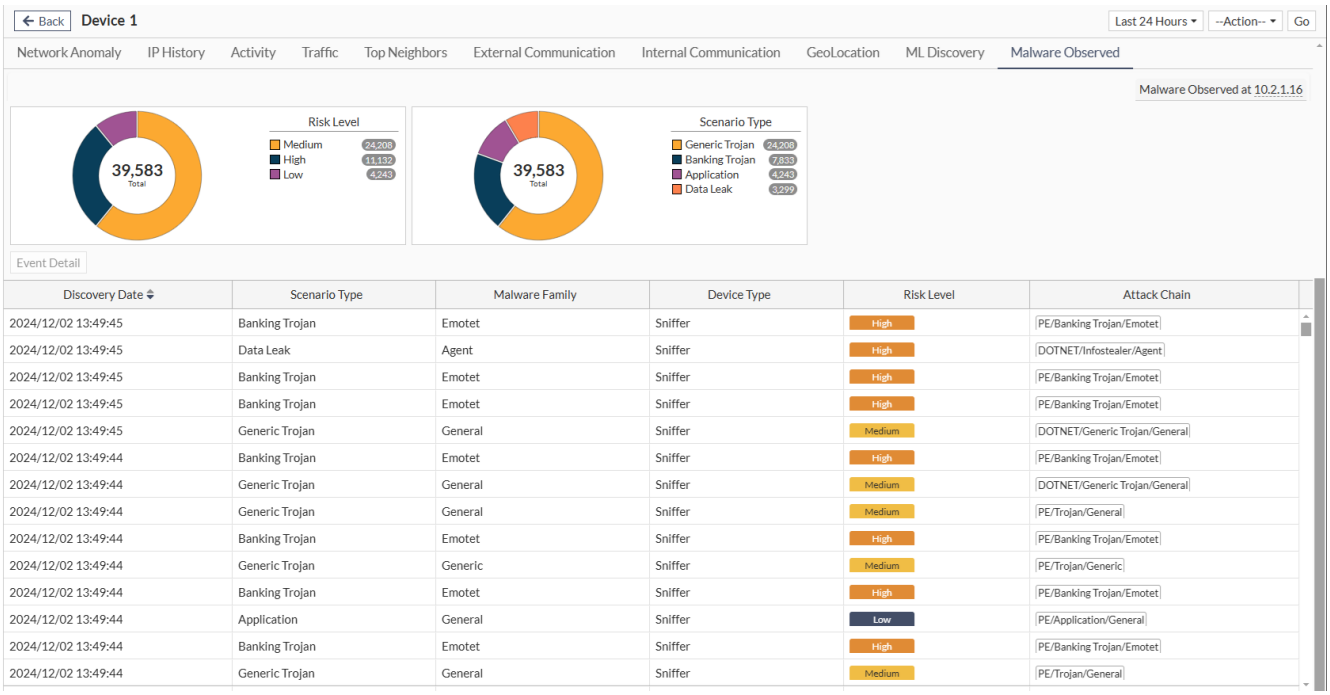


The *Device* page shows information about the device activity, as well as a heatmap for network events over the selected time period. A line graph shows the device traffic (inbound and outbound bandwidth combined). The *Confidence Level* indicates our confidence in identifying the device category.

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

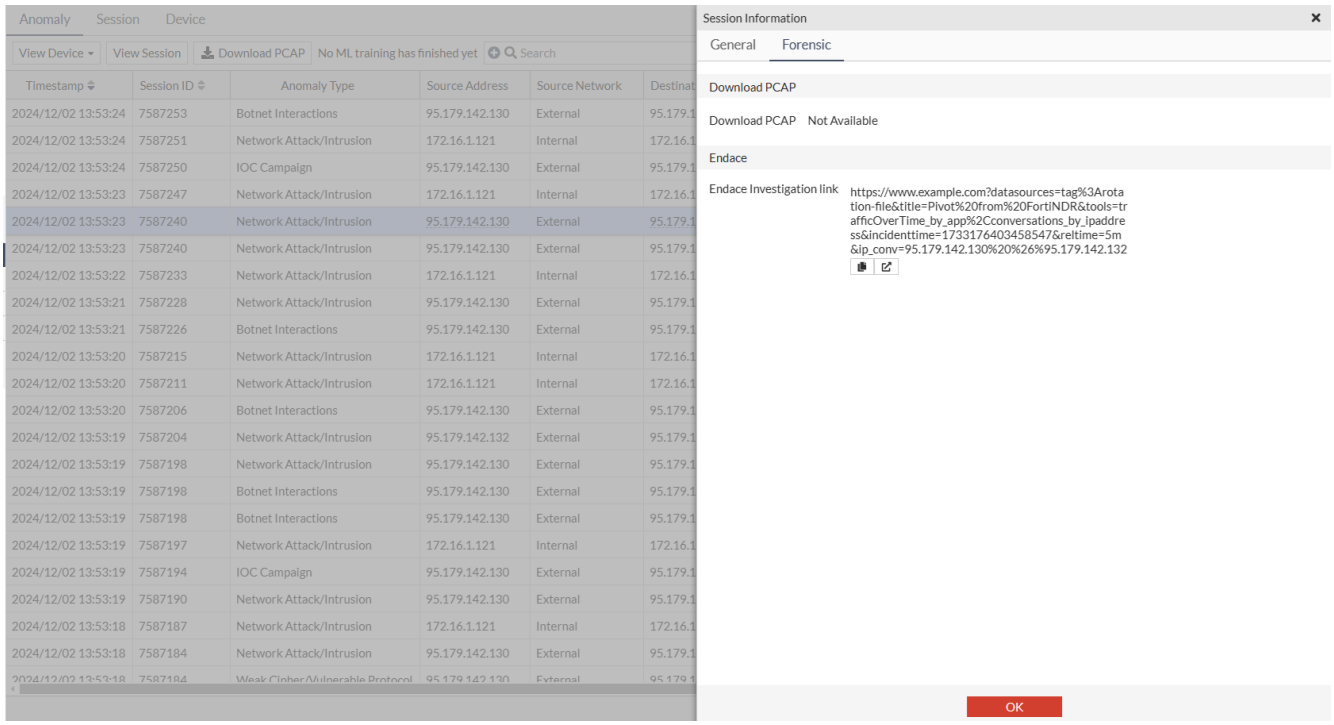


The *Malware Host Story* shows information about the malware *Risk Level* and *Scenario Type*.



Forensic information

You can view and download packet capture information from the *Session Information* page. Double-click a log in the table to open the *Session Information* pane and then click the *Forensics* tab. To view the investigation information click the *Copy URL* or *Go to Web* icons.



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.

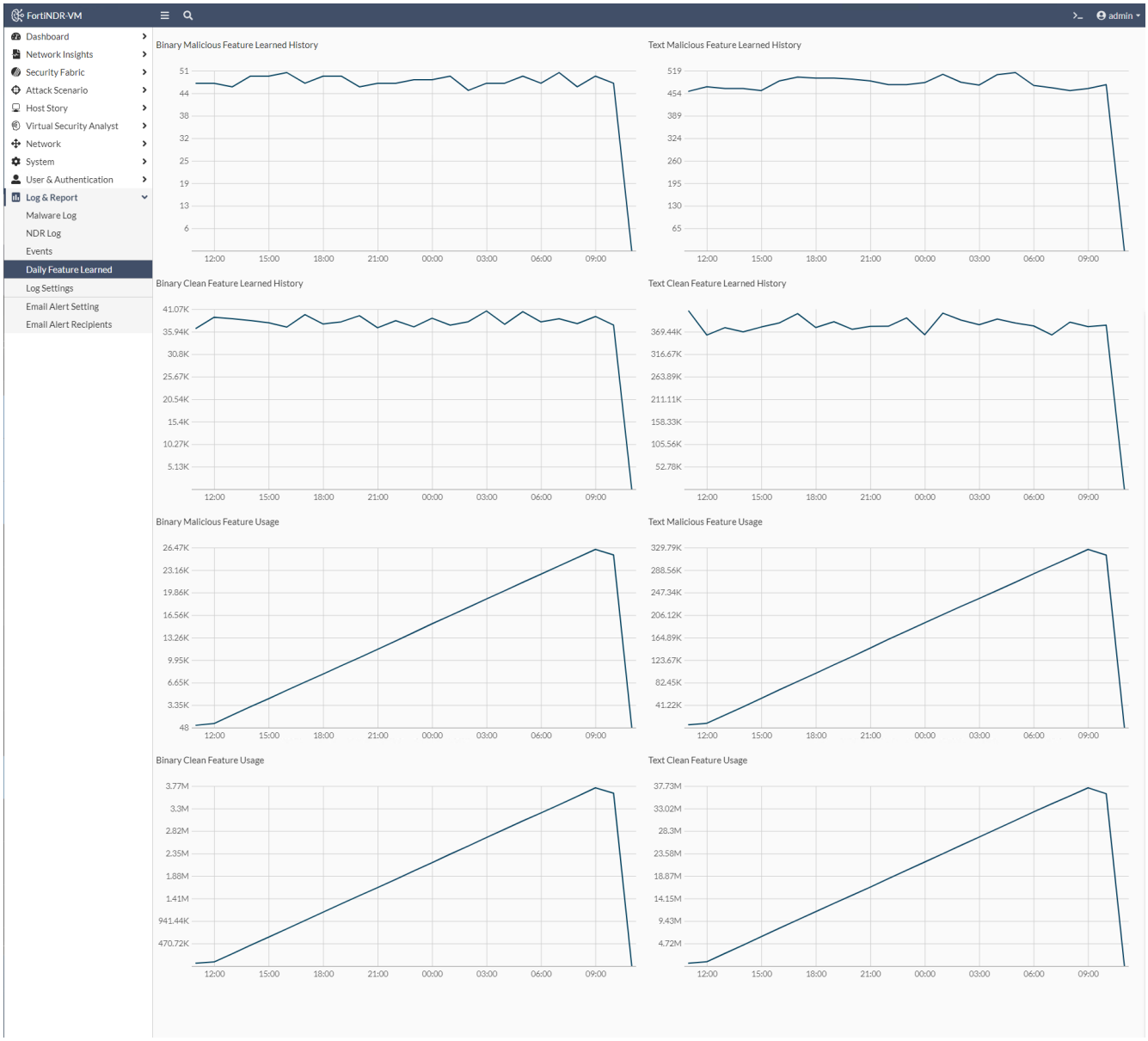
Double-click an entry in the table to view the event details:

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.



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 Syslog Server settings to send the same logs to different Syslog servers. Both settings can be configured to send the logs 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 due to the sample flowing from attacker to victim without a virus flow.
- Inline, ICAP, Sniffer and OFTP detections will trigger Syslog messages being sent to FortiAnalyzer or FortiSIEM, as they contain this information.
- NDR muted results will be omitted from the Syslog.

The Log Settings can be configured to send event logs to the Syslog servers in all modes. 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/Center settings on page 208.

To configure the log settings:

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

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

Send logs to FortiAnalyzer Cloud	Click to *Enable* or *Disable*.

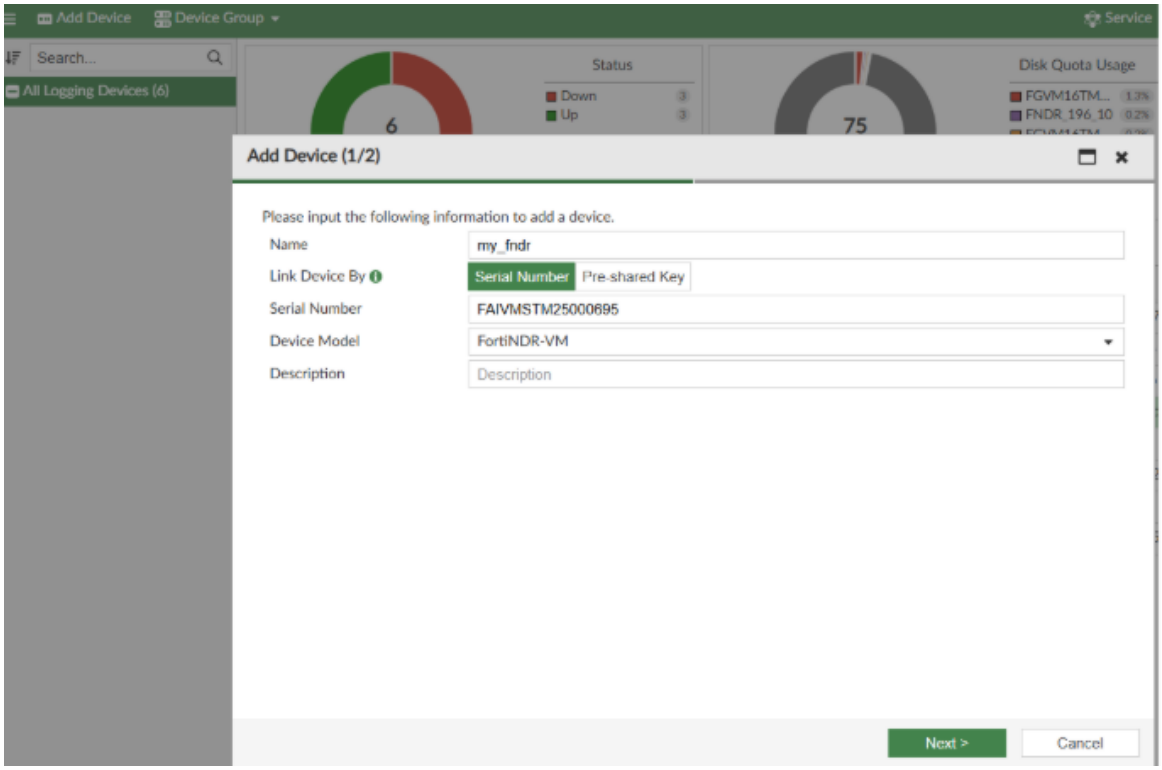
3. Click *OK*.

To configure the FortiAnalyzer Cloud Settings:

Requirements:

- A FortiAnalyzer Cloud Storage Subscription license to log into the cloud service.
- FortiAnalyzer Cloud must be manually configured to accept FortiNDR logs. For information, see the FortiAnalyzer Cloud Deployment Guide.

1. Go to *Log & Report* > *Log Settings*.
2. Under FortiAnalyzer Cloud settings, enable *Send logs to FortiAnalyzer* Cloud and click *Apply*.
   If FortiNDR does not have the correct license registered with FortiCare, this action will fail. For information about available storage licenses see the FortiAnalyzer Cloud Deployment Guide > Licensing.
3. Click *Test connection* to test and troubleshoot network connections. When FortiNDR has the correct license registered with FortiCare, the connection will be established with FortiAnalyzer Cloud. If the test connection fails,
   - Verify that the correct license registered with FortiCare.
   - Ensure that the FortiNDR model has been supported by FortiAnalyzer instance. For information, see the FortiAnalyzer release notes.
   - Ensure that the FortiNDR device information (serial number and model) is added manually to the device list in your FortiAnalyzer Cloud instance.



4. To configure log categories and severity level, use the CLI command: config system syslog fortianalyzer settings
5. Click *Apply*.

Alert Email Setting

Alert Email Settings allow you to configure email notifications for various system events and malware detections. By setting up triggers and specifying sensitivity levels, you can ensure timely alerts for potential threats and system issues.

You can trigger an email alert for the following threats:

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

To configure email alerts:

1. Go to *Log & Report > Email Alert Setting*.
2. Configure the *Server setting*.

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

3. Configure the *Trigger Setting*:
   a. Enable a trigger from the list.
   b. Enter the email message text. The default trigger message is delivered if the message text is not provided.

c. Set the *Trigger Sensitivity equal and above* to *Low*, *Medium*, *High* or *Critical Risk*. The trigger is applied to the risk severity and higher. For example, when *High Risk* is selected, the alert is triggered when a High and Critical risk is detected. This setting is not available in all triggers.

4. Click *Apply*. A privacy disclaimers appears.
5. Click *Accept* to save your settings.

Email Alert Recipients

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

To add recipients to an email list:

1. Go to *Log & Report* > *Email Alert Recipients*.
2. Click *Add Recipient*. The *Add Recipient* pane opens.
3. In the *Email* field, enter the recipient's email address and click *OK*.
4. (Optional) Click *Send Verification Email* to send a test notification to the distribution list.
5. (Optional) Select an email(s) and click *Remove Selected Recipient*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 srcmac="c0:25:a5:b3:a8:d7" dstmac="ff:ff:ff:ff:ff:ff"
vlanid=0 behavior="CONN" botname="botnet Andromeda" hostname="orrisbirth.com"
 Copy
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 srcmac="c0:25:a5:b3:a8:d7" dstmac="ff:ff:ff:ff:ff:ff"
vlanid=0 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 srcmac="c0:25:a5:b3:a8:d7"
dstmac="ff:ff:ff:ff:ff:ff" vlanid=0 behavior="CONN" vers="7" cipher="TLS_AES_256_GCM_SHA384"
md5="f436b9416f37d134cadd04886327d3e8"
```

Fields

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

IOC

```
date="2022-02-14" time="07:36:13" tz="PST" logid="0605000001" devid="FAI35FT321000001" type="ndr"
subtype="IOC" severity="critical" sessionid=19906026 alproto="HTTP" tlproto="TCP"
srcip="172.19.235.198" srcport=49304 dstip="178.63.120.205" dstport=443 srcmac="c0:25:a5:b3:a8:d7"
dstmac="ff:ff:ff:ff:ff:ff" vlanid=0 behavior="CONN" vers="7" cipher="TLS_AES_128_GCM_SHA256"
md5="52bea59cf17d9fd5dedd2835fd8e1afe" campaign="CoinMiner" hostname="s3.amazonaws.com" url="/"
```

Fields

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

IPS attack

```
date="2022-02-10" time="19:16:56" tz="PST" logid="0604000001" devid="FAI35FT321000001" type="ndr"
subtype="IPS attack" severity="low" sessionid=9237954 alproto="OTHER" tlproto="UDP"
srcip="172.19.236.145" srcport=57325 dstip="194.69.172.33" dstport=53 srcmac="c0:25:a5:b3:a8:d7"
```

```
dstmac="ff:ff:ff:ff:ff:ff" vlanid=0 behavior="CONN" vname="DNS.Amplification.Detection"
vulntype="Anomaly"

date="2022-02-10" time="18:32:54" tz="PST" logid="0604000001" devid="FAI35FT321000001" type="ndr"
subtype="IPS attack" severity="medium" sessionid=9092973 alproto="OTHER" tlproto="ICMP"
srcip="172.19.235.62" srcport=0 dstip="172.19.236.50" dstport=771 srcmac="c0:25:a5:b3:a8:d7"
dstmac="ff:ff:ff:ff:ff:ff" vlanid=0 srcmac="c0:25:a5:b3:a8:d7" dstmac="ff:ff:ff:ff:ff:ff" vlanid=0
behavior="CONN" vname="BlackNurse.ICMP.Type.3.Code.3.Flood.DoS" vulntype="DoS"
```

Fields

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

Weak cipher

```
date="2022-02-07" time="14:18:57" tz="PST" logid="0606000001" devid="FAIVMSTM21000033" type="ndr"
subtype="Weak cipher" severity="medium" sessionid=569705 alproto="IMAP" tlproto="TCP"
srcip="17.1.6.20" srcport=63310 dstip="18.2.1.114" dstport=443 srcmac="c0:25:a5:b3:a8:d7"
dstmac="ff:ff:ff:ff:ff:ff" vlanid=0 behavior="CONN" vers="2" cipher="TLS_NULL_WITH_NULL_NULL"
ciphername="weak cipher"

date="2022-02-07" time="14:18:57" tz="PST" logid="0606000001" devid="FAIVMSTM21000033" type="ndr"
subtype="Weak cipher" severity="medium" sessionid=570387 alproto="SMB" tlproto="TCP"
srcip="17.2.12.171" srcport=10001 dstip="17.1.1.119" dstport=443 srcmac="c0:25:a5:b3:a8:d7"
dstmac="ff:ff:ff:ff:ff:ff" vlanid=0 behavior="CONN" vers="1" cipher="TLS_RSA_WITH_AES_256_GCM_
SHA384" md5="9a157673907688965992b40304f50a1e"  ciphername="weak version" Copy
```

Fields

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

ML

```
date="2022-02-18" time="15:54:39" tz="PST" logid="0608000001" devid="FAIVMSTM21000033" type="ndr"
subtype="ML" severity="low" sessionid=1135774 alproto="DNS" tlproto="TCP" srcip="17.1.10.185"
srcport=35546 dstip="17.1.1.119" dstport=389 sensor_hostname="FNDR-VM-217" sensor_
```

```
ip="172.19.235.217" sensor_sn="FAIVMSTM21000015" srcmac="c0:25:a5:b3:a8:d7"
dstmac="ff:ff:ff:ff:ff:ff" vlanid=0 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
srcmac	Source mac address
Dstmac	Destination mac address
vlanid	VLAN ID
sensor_hostname	Sensor Hostname (Only apply to Center NDR ML syslog)
sensor_ip	Sensor IP (Only apply to Center NDR ML syslog)
sensor_sn	Sensor SN (Only apply to Center NDR ML syslog)

AV log samples

Log Type	Subtype	Log Sample
Event	**User**	date="2021-05-21" time="13:41:38" tz="MDT" logid="0400000001" devid="FAI35FT319000026" type="event" subtype="user" level="information" user="admin" ui="init" action="none" status="none" msg="changed settings of 'ipaddr' for 'system syslog fortianalyzer settings'"
	System	date=”2021-03-31” time=”15:50:19” tz=”PDT” logid=”0802001914” devid=”FAIVMSTM21000033” type=”event” subtype=”system” level=”information” user=”none” ui=”none” action=”none” status=”success” msg="ldapcached is being stopped; all connections to remote host(s) will be terminated."
	File-stats	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0403000001” devid=”FAIVMSTM21000033” type=”event” subtype=”file-stats” level=”information” status=”success” fileaccepted=100 fileprocessed=99 filedetected=99
	Automation	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0404000001” devid=”FAIVMSTM21000033” type=”event” subtype=”automation” level=”information” status=”success” profilename=”profile1” targetip=”10.10.3.4” policyconf=87 postaction=”block” modtime=”2021-05-13 15:16:23” attemptcnt=12
	Perf-stats	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0405000001” devid=”FAIVMSTM21000033” type=”event” subtype=”perf-stats” level=”information” status=”success” cpu=20 mem=70 logdisk=0 datadisk=21
	Malware	date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0408000001” devid=”FAIVMSTM21000033” type=”event” subtype=”malware” level=”information” status=”success” featurelstcnt=19 featurelst= “Generic Trojan, Trojan, BackDoor, Application, Virus, Worm, Downloader, Redirector, Dropper, Phishing, Exploit, Proxy, Ransomware, Banking Trojan, PWS, Infostealer, Clicker, CoinMiner, WebShell” featurecounts=”35476, 81, 15, 9, 7, 3, 3, 3, 3, 1, 1,1,1,1,1,1,1,1,1” date=”2021-03-31” time=”16:18:28” tz=”PDT” logid=”0408000001” devid=”FAIVMSTM21000033” type=”event” subtype=”malware” level=”information” status=”success” featurelstcnt=10 featurelst= “Generic Trojan, Trojan, BackDoor, Application, Virus, Worm, Downloader, Redirector, Dropper, Phishing” featurecounts=”35476, 81, 15, 9, 7, 3, 3, 3, 3, 1” 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 filesize=3132 filetype="PE" md5="ddc770fa317b4a49b4194e4dcf8d308e" sha1=”68e42b283515d124d2c8bf9ddc47db0f6fc54c9f” sha256=” a89aa817d6ffec1502190973ef32f60253a673579fedaae2762a9bca4dfcfecf” virusname="W32/Rbot.15B3!tr" confidence="low" risklevel="medium" url="http://172.19.235.2/data/0/4B72XXXX/4B72B9D2.vRG" attackerip="172.19.235.2" attackerport=80 victimip="172.19.235.76" victimport=10578 totalproctime=4 detype="N/A" subdetype="N/A" detypelstcnt=3 detypelst=”worm,trojan,downloader” detypecounts=”64,64,2” eventtime=1746660460019287

Log Type	Subtype	Log Sample
Attack	**Attack chain**	date="2021-05-21" time="10:23:05" tz="PDT" logid="0500000001" devhost="FAI35FT321000001" devid="FAI35FT321000001" type="attack" subtype="Attack Chain" level="alert" user="admin" ui="daemon" action="none" status="success" eventid=7255021 discoverydate="2021-05-21 10:13:27" risklevel="High", malwarefamily="N/A" scenariotype="Botnet" filecnt=1 filelist="435387294"
	Malware	date="2021-05-21" time="10:23:05" tz="PDT" logid="0521000001" devid="FAI35FT321000001" type="attack" subtype="Malware" level="alert" action="none" devicetype="sniffer" fossn="" fosvd="" fileid=435387294 filesize=3132 filetype="PE" md5="ddc770fa317b4a49b4194e4dcf8d308e" sha1="68e42b283515d124d2c8bf9ddc47db0f6fc54c9f" sha256="a89aa817d6ffec1502190973ef32f60253a673579fedaae2762a9bca4dfcfecf" virusname="W32/Rbot.15B3!tr" confidence="low" risklevel="medium" url="http://172.19.235.2/data/0/4B72XXXX/4B72B9D2.vRG" attackerip="172.19.235.2" attackerport=80 victimip="172.19.235.76" victimport=10578 totalproctime=4 detype="N/A" subdetype="N/A" detypelstcnt=3 detypelst="worm,trojan,downloader" detypecounts="64,64,2" eventtime=1746660460019287

NetFlow logs samples

Suspicious activity

```
date="2024-07-05" time="16:43:13" tz="PST" logid="0602000001" devid="FAIVMSTM21000033"
type="netflow" subtype="suspicious-activity" severity="high" tag="Phishing" eventtime=1710879771
flowtype="NETFLOW_V5" flowdirection="Ingress" sampleip="127.0.0.1" tlproto="TCP"
srcip="212.102.209.138" srcport=7033 dstip="123.31.20.78" dstport=63294 srcmac="00:00:00:00:00:00"
dstmac="00:00:00:00:00:00" vlanid=0
```

ML

```
date="2024-07-05" time="12:42:35" tz="PDT" logid="0702000001" devid="FAIVMSTM22001135"
type="netflow" subtype="ML" severity="low" eventtime="1720208468" flowtype="IPFIX"
flowdirection="Ingress" sampleip="127.0.01" tlproto="TCP" srcip="68.198.100.91" srcport=47010
distip="146.23.194.10" dstport=7716 srcmac="00:00:00:00:00:00" dstmac= "00:00:00:00:00:00"
vlanid=0 reasons= "Destination address (IP)"   sensor_hostname="FNDR-VM-217" sensor_
ip="172.19.235.217" sensor_sn="FAIVMSTM21000015"
```

The sensor fields are exclusive to Center mode.

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.

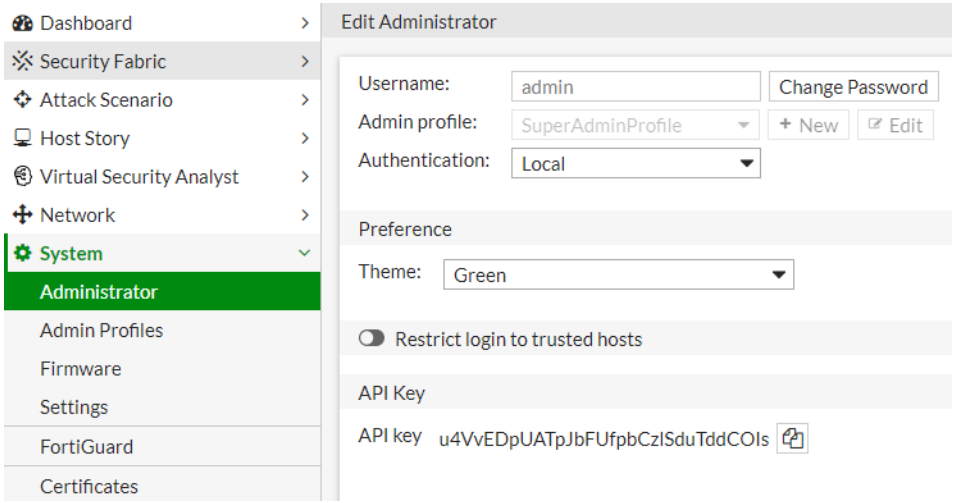
To use API to upload files, generate a token. The token is only displayed once. If you lose the token, generate a new one.

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*.



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 17.

Submit a file using one of the following methods.

Method	Description
JSON data	The JSON data must be encoded in base64 format. Encode the file directly into the HTTP body as JSON data using the `file_content` field.

Method	Description
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')})
```

File Upload API result

If the API key is correct and the file is successfully uploaded, the API will return with the submission id. This submission id can be used in the verdict API to get the scan results.

```
{"submit_id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"}
```

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":
"cce8e67772f19bcfe5861e4c1b8eec87016bb7cf298735db633490243bc0391a017c7d6b805f225775405598614be48c5
479cb7f1c54d957e6129effbf9cca37",
    "file_size": 1141544,
    "source": "http://172.16.77.46/api/sample_download/1106042791/",
    "severity": "High",
    "category": "Trojan",
    "family":"Emotet",
    "feature_composition": [
      {
        "feature_type": "Trojan",
        "appearance_in_sample": 986
      },
      {
        "feature_type": "Application",
        "appearance_in_sample": 95
      }
    ],
    "create_date": "2020-07-31",
    "confidence": "High",
    "file_type": "PE",
    "victim_ip": "172.19.235.225",
    "attacker_ip": "172.16.77.46",
    "victim_port": 35400,
    "attacker_port": 80,
    "engine_version": 1.013,
    "kdb_version": 1.037,
    "tmfc": 0,
    "pbit": 3
  }
}
```

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

Example of problems retrieving results

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

Field	Description
`http_code`	See HTTP status table on page 280.
`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= ***submission_id***` 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.
mac	Get anomaly events with device mac address. User needs specify one of [ip, hostname, mac] in the request.
ip_tag	Get anomaly events with a user-defined tag on an IP address. You will need to specify one of [ip, ip_tag, mac, mac_tag] in the request.
mac_tag	Get anomaly events with a user-defined tag on a mac address. You will need to specify one of [ip, ip_tag, mac, mac_tag] in the request.
type	Specify the anomaly type events, one of [botnet, encrypted-attack, network-attack, fortiguard-ioc, weak-communication, ml-discovery, malware, netflow-anomaly, netflow-ml].
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=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",
            "source_mac":"08:5b:0e:5c:a0:61",
            "destination_mac":"38:c0:ea:d9:cf:bf"
         },
         {
            "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",
            "source_mac":"08:5b:0e:5c:a0:61",
            "destination_mac":"38:c0:ea:d9:cf:bf"
         }
      ]
}
```


Start Cloud Storage scan

/api/v1/cloud/scan

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

Examples:

```
POST /api/v1/cloud/scan?sname= ***cloud storage profile name***
 {
 "http_code": 200,
 "message": "OK"
 }
```

Example of failed to start Cloud Storage Scan:

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

Detected Samples

Field	Description
`start_time`	The start time of event log, specified as a Unix timestamp in seconds.
`end_time`	The end time of event log, specified as a Unix timestamp in seconds.
`file_type_group`	A comma separated list of file type groups to search for; any of executables, *pdf_documents*, *office_documents*, *web_pages*, *compressed_archives*, *flash_files*, *android_files*, *mac_files*, *linux_files*, *others*
`submission_source`	A comma separated list of submission sources to search for; any of *http2*, *sniffer*, *fsa*, *fml*, *icap*, *manual_upload*, *oftp*, *network_share*, *cloud_storage*.
`risk`	A comma separated list of risk levels to search for; any of *low*, *medium*, *high*, *critical*.
`offset`	The starting index of the query results to return; for pagination support.
`size`	The maximum number of SHA256 hashes to return per query; hard limited to 10000.

Example:

```
GET /api/v1/detected-samples/hashes?submission_source=network_share,sniffer&end_
time=1719881150&file_type_group=web_pages,android_files&risk=low

{
    "results": {
        "size": 2,
        "hashes": [
            "9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08",
            "60303ae22b998861bce3b28f33eec1be758a213c86c93c076dbe9f558c11c752"
        ]
    }
}
```

Field	Description
`size`	Number of SHA256 hashes returned.
`hashes`	SHA256 hashes of samples matching the search query, ordered ascending by the entry date of its first appearance.

Example of problems retrieving hashes:

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

Field	Description
`http_code`	See HTTP status table.
`message`	Messages include: `INVALID_PARAM` when search query value is not valid.

/api/v1/detected-samples/download

Supported search query parameters	Description
`sha256_hashes`	A comma separated list of SHA256 hashes to download. Limited to 10 hashes per query.

Example:

```
GET /api/v1/detected-samples/download?sha256_
hashes=9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08,60303ae22b998861bce3b28f33
eec1be758a213c86c93c076dbe9f558c11c752
{
    "results": {
        "files": [
            {
                "filename": "9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08",
                "found": true,
                "data": "<base64 encoded data>"
            },
            {
                "filename": "60303ae22b998861bce3b28f33eec1be758a213c86c93c076dbe9f558c11c752",
                "found": true,
                "data": "<base64 encoded data>"
            }
        ]
    }
}
```

Field	Description
`files`	Array of files searched for.
`filename`	The filename of the downloaded file. Currently set to the SHA256 hash.
`found`	If the file was saved in the system and its contents could be retrieved.
`data`	The file data encoded in base64. When decoded the file will be an encrypted zip file with the password *infected*.

Example of problems downloading samples:

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

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.SSLEr
as e:
                                valid = False

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

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

                        else:
                                parse_url (links)


        return (url_list_depth)

def load_file_for_upload(path_to_file):

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

        return gzip.compress(data)

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

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

        try:
                results_output = subprocess.check_output(command, shell=True)
```

```
                data =  json.loads(results_output)

        except subprocess.CalledProcessError as e:

                print(e)
                sys.exit(0)

        return (data)

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

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

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

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

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


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

                                                                except KeyError as e:
                                                                   next

                                                        print (results_metadata)
```

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

                sys.exit(0)

def parse_url (tmp_url):

        client = FAIApiClient_file(host)

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

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

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

                                except Exception  as e:
                                        pass

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

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

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


def getpreferredencoding(do_setlocale = True):
```

```
        return "utf-8"

def main(argv):
        locale.getpreferredencoding = getpreferredencoding

        urllib3.disable_warnings()

        parser = argparse.ArgumentParser(description='Test upload files to 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 9561	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 TCP 8890 (When using FortiManager)	Initial outbound to: • fai.fortinet.net • globalupdate.fortinet.net (Default when Anycast is enabled) • fds1.fortinet.com (When Anycast disabled) • update.fortiguard.net (When Anycast disabled) For a complete list of the current FortiGuard update servers, use the CLI `diagnose fds list`. To enable/disable Anycast, please use the CLI `config system fortiguard update` and then set `anycast` to `disabled`. 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 TCP 8888 (When using FortiManager)	Outbound to productapi.fortinet.com

Item	Protocol and port number	Direction
IOT lookup	TCP 443	Outbound to globalguardservice.fortinet.net
Microsoft Active Directory	TCP 636,389	Inbound and outbound
NetFlow listen ports	UDP 2055,6343,9995	Inbound
Network File Share/PCAP Artifact Storage	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 (SSL encrypted)
Sensor Center data synchronization	TCP 9094 9096	Sensor to Center (SSL encrypted)
SYSLOG	UDP 514	SYSLOG outbound
Web Filter query	UDP 53 TCP 8888 (When using FortiManager)	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 summarizes whether detection will work on/off line (no internet access). All of the detection techniques below can be updated via FortiGuard Distribution Network (Internet).

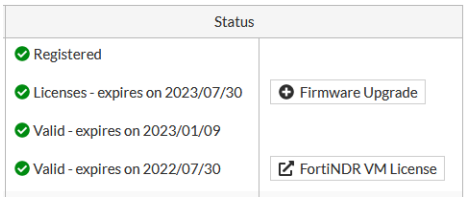
Detection Techniques	Supports offline manual update	Comments
Malware via ANN	Yes	Can be updated manually via GUI or with an offline package via CLI.
AV engine	Yes	Shipped by default. Can be updated with internet via GUI or with an offline package via CLI.
Botnet detection	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.
Network Attacks / Application control	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.
Encrypted attacks (via JA3)	Yes	Has DB by default. Can be updated with internet via GUI or with an offline package via CLI.
Weak cipher/vulnerable protocol detection	NA	Comes with firmware, no updates required.
Device inventory	Yes	Has minimal DB on firmware image by default. The IOT query service is now local (previous lookup was through FortiGuard servers). Can be updated with internet via GUI or with an offline package via CLI.

Detection Techniques	Supports offline manual update	Comments
FortiGuard IOC	No	Requires Internet to lookup URLs and IP for web campaigns associated.
ML Discovery	NA	Local ML algorithm updates via firmware.
Geo DB	No	Comes with firmware, does not update often, supports FortiGuard Update via internet.
OT Threat and OT device inventory	Yes	Has minimal DB by default. Can be updated with internet via GUI or with an offline package via CLI. Requires SCADA/OT license to download the packages.

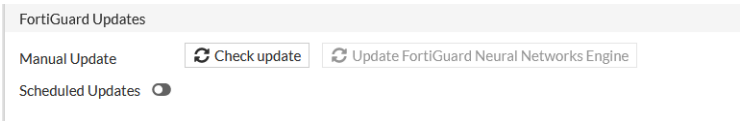
Updating the ANN database from FDS for malware detection (GUI)

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*.



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 events. 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 294 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, FTP, 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.

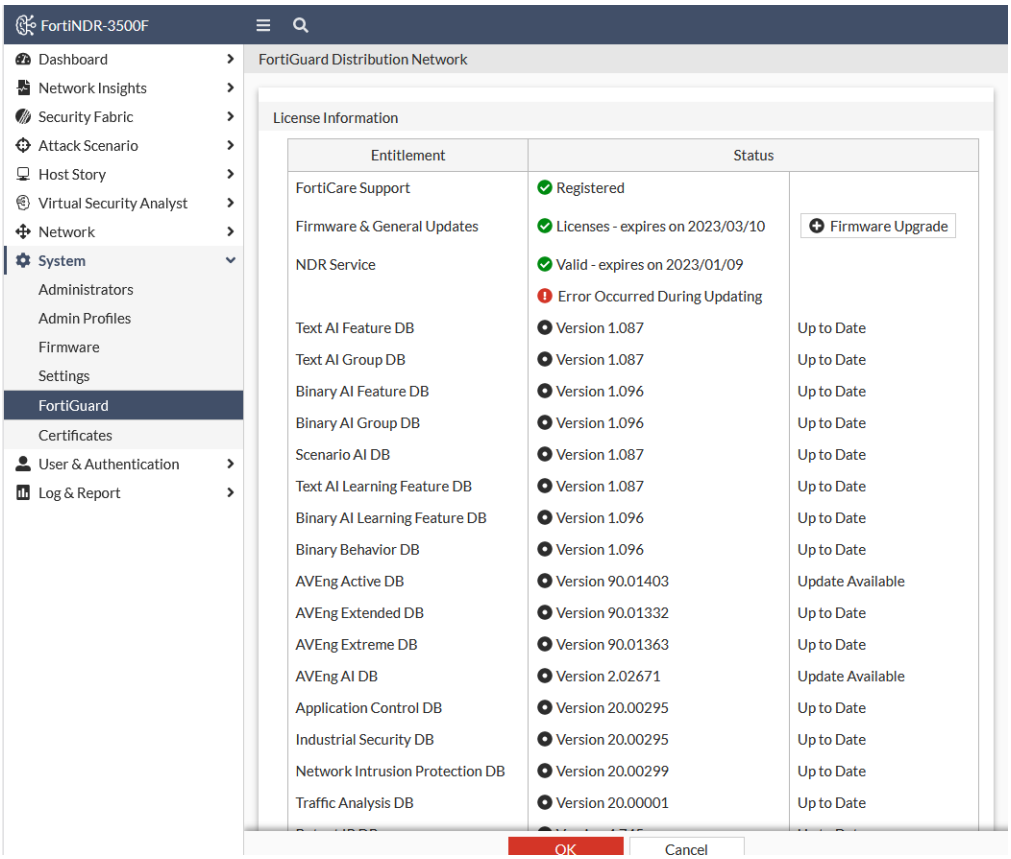
```
FAI35FT319000004 # execute restore kdb disk pae_kdb_all.tar.gz
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Mounting /dev/sda1
Mounting /dev/sdb1
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e51D0v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



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

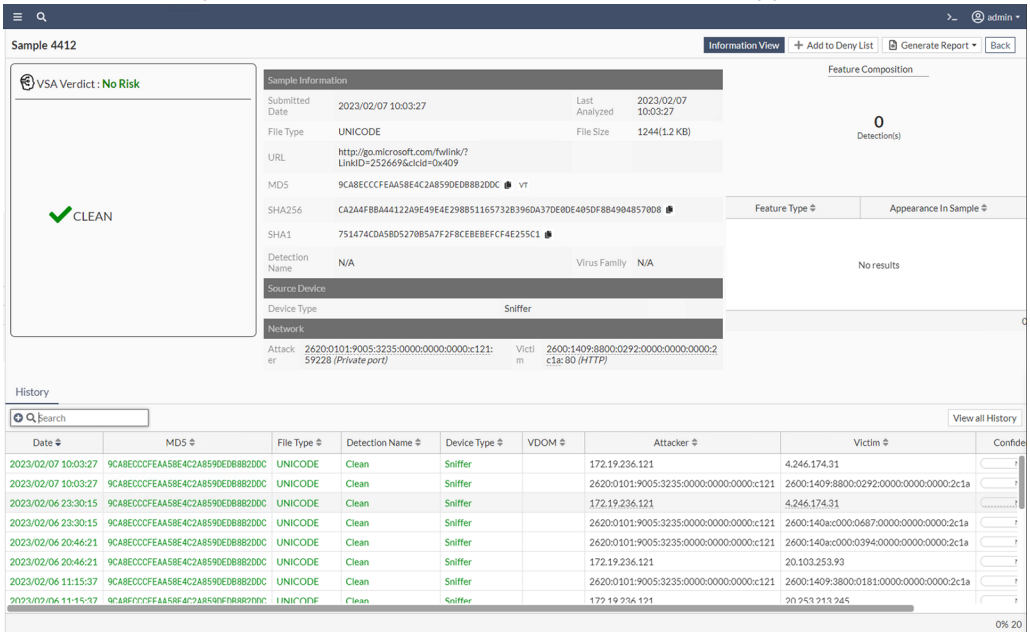
Event Category	NDR Detection Severity Level
Malware Detection	Low|Medium|High|Critical
Botnet Detection	Critical
Encryption Attack Detection	Critical
Network Attack Detection	Low|Medium|High|Critical
Indication of Compromise Detection	Critical
Weak Cipher and Vulnerable Protocol Detection	Low|Medium|High|Critical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

Appendix F: IPv6 support

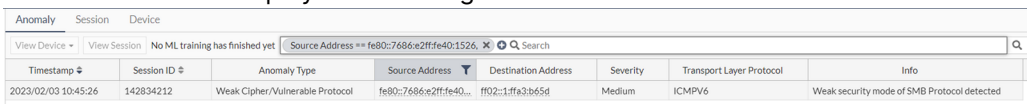
The following topic covers IPv6 support in FortiNDR.

IPV6 in detections:

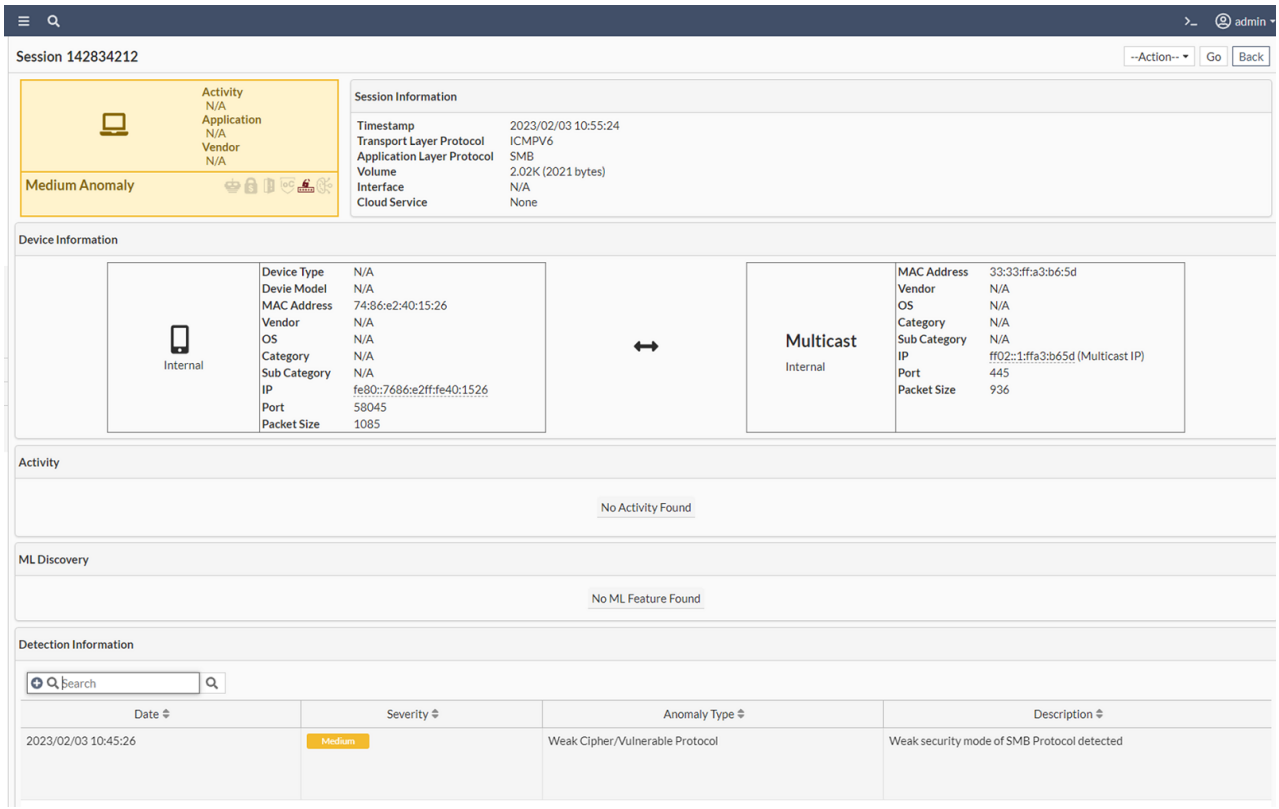
- Files from sniffer port with IPv6 source and/or destination are supported.



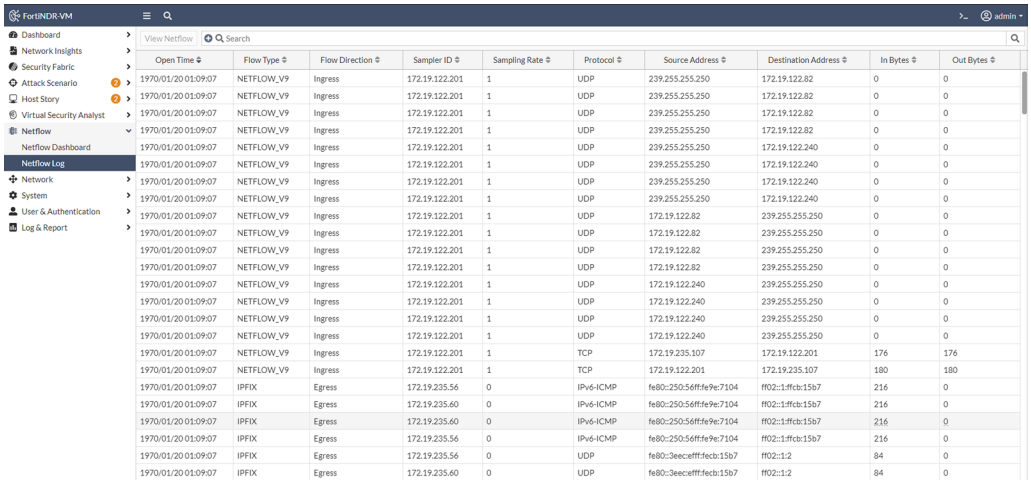
- IPv6 addresses are displayed in NDR logs.



- IPv6 is shown in the session detail page.



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



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

Appendix G: Supported IPS (including OT), Application Control, and protocols

FortiNDR has multiple techniques to identify protocols and applications from sniffer traffic.

1. **Intrusion(s) Detection**: This includes both IPS extended as well as OT, signatures are listed on FortiGuard website.
2. **Application Control**: Identification of application in sessions captured, as illustrated in Session tab on page 89. Applications that are supported are searchable from: https://www.fortiguard.com/services/appcontrol.

   > After FortiNDR detects the application, it can then detect events in applications based on ML baselining described here: ML Configuration on page 176
   >
   > FortiNDR will build a baseline of traffic (default 7 days, configurable via the CLI) and detect anything not within the baseline. This detection method can be used along with other features such as dst IP, geo, src port, dst port, etc.

3. **Network metadata extraction support**: This is a more in-depth level of support which includes the ability for the FortiNDR engine to parse the 'network metadata' and the user's ability to query them using the investigation feature. For example, User agent string in HTTP, DNS code in DNS protocol.

   This requires ability for the engine to extract this metadata from protocols and store the metadata in the database for users to search.
4. **Operational Technology vendor and application list**
   FortiNDR supports the following from an OT perspective:
   - OT IPS signatures can be found at *OT threat* on the FortiGuard Operational Technology Security Service page.
   - OT Device Identification under Device Inventory on page 41.
   - Identify OT applications with Application Control (refer to point 2 above), as well as the *OT App Detection* database which is found on the FortiGuard Operational Technology Security Service page.

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, SMBv1, 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).

SMBv2/3 file scanning involves multiple files extraction within same / reused session, which FortiNDR does not support.

Supported file types for ANN:

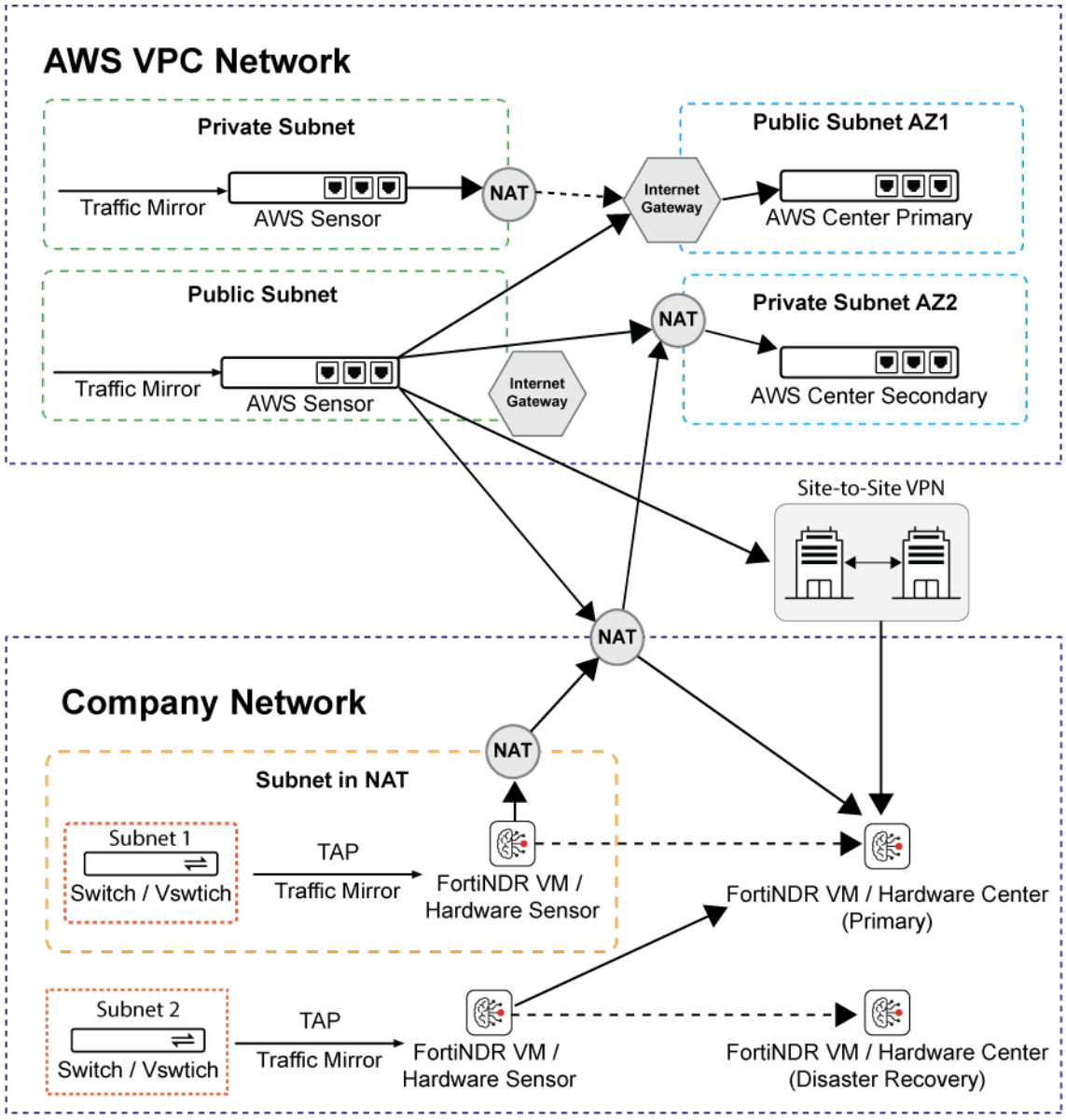
For ANN supported file types, ANN will process and provide a feature breakdown between different attack scenarios (like Ransomware, banking trojan etc) 32 bit and 64 bit PE, PDF, MSOFFICE, HTML, ELF, VBS, VBA, JS, PHP, HWP Hangul_Office, XML, POWERSHELL, UPX, ASPACK, NSIS, AUTOIT, MSOFFICEX, RTF, DLL, 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: Center Sensor Deployment

Topology

The following shows an example of a dual-center deployment. Each sensor is connected to a center NDR.



Redundant Center Setup

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 292 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 292.

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:

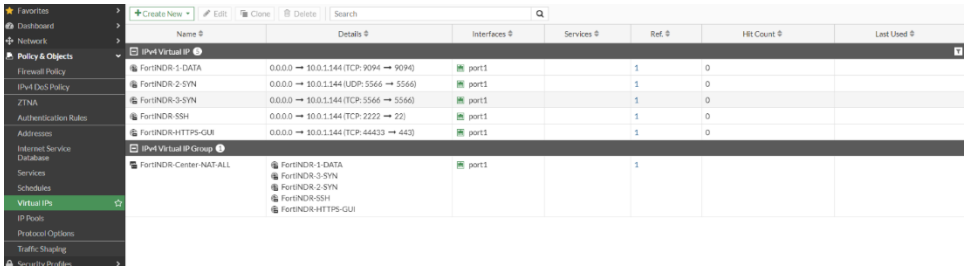
Please reserve 10Gbps for FortiNDR Center Port1 and ensure 1Gbps of network bandwidth are reserved from Sensor to Center. The network path should also maintain a low latency from Sensor to Center (P99 Round Trip time from ping should be <10ms).

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



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.

Appendix J: Custom IPS signatures

Custom Intrusion Prevention System (IPS) signatures are designed to detect specific network-based threats. These signatures are tailored to identify malicious behaviors associated with known attack techniques and tools, including Empire C2, Kerberos AS-REP roasting, SMB enumeration, and remote task creation via DCERPC.

You can use the CLI command `config ips custom` to create or modify custom Intrusion Prevention System (IPS) signatures. This command allows you to define detection patterns, assign severity levels, add comments, and enable or disable the signature as needed. For more information, see the FortiNDR CLI Reference Guide.

Detection Logic and tuning

hping3.SYN.Flood.Custom (ID 1001)

Purpose	Detect SYN flood attacks targeting TCP port 80.
How it matches	Counts bare SYN packets with zero payload from the same source IP to `dst_port 80`. Triggers when the rate exceeds 100 per second.
Tuning	Increase or decrease `--rate 100,1` based on baseline. Remove `--dst_port 80` to cover any port. Good to keep `--data_size 0` to avoid flagging normal handshakes carrying options-only payloads.

Example:

```
config ips custom
  edit hping3.SYN.Flood.Custom
    set signature "F-SBID( --attack_id 1001; --name hping3.SYN.Flood.Custom; --protocol tcp; --
flow from_client; --dst_port 80; --tcp_flags S; --data_size 0; --rate 100,1; --track SRC_IP;)"
  next
end
```

Empire.psexec_curl.2.Custom (attack_id 1003)

Purpose	Detect the Empire psexec HTTP fetch on the C2 server.
How it matches	Client HTTP on port 8183, URI contains `/parse.jsp?mn=`, headers contain `User-Agent` with `MSIE 8`.
Tuning	Adjust `--dst_port` or `'User-Agent'` string based on observed variations.

Example:

```
config ips custom
  edit Empire.psexec_curl.2.Custom
   set signature "F-SBID( --attack_id 1003; --name Empire.psexec_curl.custom; --protocol tcp; --
service http; --flow from_client; --dst_port 8183; --pattern \"/parse.jsp|3f|mn=\"; --context uri;
--no_case; --pattern \"User-Agent\"; --context header; --no_case; --pattern \"MSIE 8\"; --context
header; --no_case; --distance 0; --within 100; )"
  next
end
```

EmpireHTTPC2.Custom (attack_id 1004)

Purpose	Detect Empire HTTP C2 beacons.
How it matches	Client HTTP GET to port 8183 where the URI contains `jsp?mn=`.
Tuning	Add alternative ports if your lab shows them. You can make it stricter by requiring a known User-Agent string if needed.

Example:

```
config ips custom
  edit EmpireHTTPC2.Custom
       set signature "F-SBID( --attack_id 1004; --name EmpireHTTPC2.Custom; --protocol tcp; --dst_port
8183; --service http; --parsed_type http_get; --flow from_client; --pattern \"jsp|3f|mn=\"; --
context uri; --no_case;)"
  next
end
```

SMB.NetrShareEnumAll.Custom (attack_id 1011)

Purpose	Detect SMB share enumeration using SRVSVC NetrShareEnumAll.
How it matches	`NBSS` and `SMB` header bytes, followed by `DCERPC` call bytes and the `NetrShareEnumAll` opnum at expected offsets. Optional rate limiter provided.
Tuning	Use `--rate 5,1,limit --track src_ip` to alert only on bursts and lower FP. Adjust thresholds for your environment.

Example:

```
config ips custom
 edit SMB.NetrShareEnumAll.Custom
    set signature "F-SBID( --attack_id 1011; --name SMB.NetrShareEnumAll.Custom; --protocol tcp; -
```

```
-flow from_client; --service NBSS; --pattern \"|FE|SMB|40 00|\"; --distance 4,packet; --within
6,packet; --pattern \"|05 00 00|\"; --context packet; --distance 64; --pattern \"|0f 00|\"; --
context packet; --distance 19; --within 2; --rate 5,1,limit; --track src_ip; )"
  next
end
```

Example configuration

```
config ips custom
  edit hping3.SYN.Flood.Custom
    set signature "F-SBID( --attack_id 1001; --name hping3.SYN.Flood.Custom; --protocol tcp; --
flow from_client; --dst_port 80; --tcp_flags S; --data_size 0; --rate 100,1; --track SRC_IP;)"
  next
  edit Empire.psexec_curl.2.Custom
    set signature "F-SBID( --attack_id 1003; --name Empire.psexec_curl.custom; --protocol tcp; --
service http; --flow from_client; --dst_port 8183; --pattern \"/parse.jsp|3f|mn=\"; --context uri;
--no_case; --pattern \"User-Agent\"; --context header; --no_case; --pattern \"MSIE 8\"; --context
header; --no_case; --distance 0; --within 100; )"
  next
  edit EmpireHTTPC2.Custom
    set signature "F-SBID( --attack_id 1004; --name EmpireHTTPC2.Custom; --protocol tcp; --dst_
port 8183; --service http; --parsed_type http_get; --flow from_client; --pattern \"jsp|3f|mn=\"; -
-context uri; --no_case;)"
  next
  edit SMB.NetrShareEnumAll.Custom
    set signature "F-SBID( --attack_id 1011; --name SMB.NetrShareEnumAll.Custom; --protocol tcp; -
-flow from_client; --service NBSS; --pattern \"|FE|SMB|40 00|\"; --distance 4,packet; --within
6,packet; --pattern \"|05 00 00|\"; --context packet; --distance 64; --pattern \"|0f 00|\"; --
context packet; --distance 19; --within 2; --rate 5,1,limit; --track src_ip; )"
  next
end
```

www.fortinet.com