



# Administration Guide

FortiNDR 7.6.0



**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](mailto:techdoc@fortinet.com)



December 12, 2025

FortiNDR 7.6.0 Administration Guide

55-760-1054916-20251212

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>10</b>
<b>Introduction</b> .....	<b>11</b>
Getting Started .....	12
Standalone, Center and Sensor operating mode .....	13
FortiNDR Center and Licensing requirement .....	15
Dual Center mode support .....	16
FortiNDR traffic and files input types .....	17
Files and malware scan flow using AV and ANN .....	19
Stage 1 .....	19
Stage 2 .....	20
Planning deployment .....	20
Storage by model .....	20
Additional SSD .....	22
Preparing the virtual environment .....	23
Initial setup .....	23
Internet Access .....	24
Ports .....	24
Hardening .....	25
Physical security .....	26
Vulnerability - monitoring PSIRT .....	26
Firmware .....	26
Encrypted protocols .....	26
FortiGuard databases .....	27
Penetration testing .....	27
Password policies .....	27
Disable Unnecessary Services .....	27
Configuration backup .....	28
Logging .....	28
<b>Dashboard</b> .....	<b>29</b>
NDR Overview .....	29
Malware Overview .....	30
System Status .....	30
Custom dashboards .....	31
Dashboard widgets in Center mode .....	32
<b>Network Insights</b> .....	<b>33</b>
Anomaly, Connection and Session tabs .....	34
Common fields .....	34
Device Inventory .....	35
Device details .....	37
OT Devices .....	37
Botnet .....	43
FortiGuard IOC .....	43
Network Attacks .....	44

Weak/Vulnerable Communication .....	45
Anomaly information .....	47
General tab .....	47
Analytic tab .....	48
Encrypted Attack .....	53
Top talker .....	54
Top application .....	56
Top URL/Domain .....	58
MITRE ATT&CK .....	58
Mitre ATT&CK widget .....	59
Mitre ATT&CK Matrix .....	59
Filtering the matrix .....	61
Mitre ATT&CK detail .....	61
ML Discovery (Center Standalone) .....	63
Session information .....	64
Add feedback to a ML Discovery .....	65
ML Baseline information .....	66
Anomaly tab .....	66
Anomaly Information .....	67
Analytic tab .....	68
Connection tab .....	69
Session Information .....	70
Session tab .....	71
Session Information .....	72
View source and destination devices .....	73
View sessions .....	74
Malware Attack Scenario (formerly Attack Scenario) .....	77
Scenario types .....	77
Attack scenario navigation and timeline .....	79
Understanding kill chain and scenario engine .....	81
Malware Observed (formerly Host Story) .....	82
Malware Observed summary page .....	82
Event details .....	84
<b>Investigations (Center) .....</b>	<b>85</b>
Tag management system .....	85
Tag reference .....	85
Related tags .....	86
Global query .....	87
Sample queries .....	90
View all the anomaly descriptions with medium severity (value = 1) .....	90
List all countries communicated this week .....	90
List all external communication .....	91
List attributes of all malicious files transfered via SMB Session .....	91
Identify connection pairs based on an URI .....	91
Applications running on non standard port for HTTP .....	92
Internal host retrieves archive file pretending to be image .....	92
Find internal RDP servers exposed to outside .....	92

Detect EXE files transferred over SMB protocol from an external host .....	92
Detect FTP data exfiltration .....	93
Detect web traffic to an external IP check or geolocation service using non-browser mechanisms .....	93
Advanced Query Language .....	94
SQL statements .....	94
<b>Security Fabric .....</b>	<b>98</b>
Device Input .....	98
Supported models: .....	98
Network Share .....	98
Creating a Network Share profile .....	99
Testing connectivity .....	101
Scanning a network location .....	102
Scheduling a scan .....	102
Viewing scan results .....	102
Scanning Zip files .....	103
Network Share Quarantine .....	103
Quarantined files .....	104
Creating a quarantine profile .....	104
Combining network share and quarantine profiles .....	106
Cloud Storage .....	107
Creating a Cloud Storage profile .....	107
Testing connectivity .....	108
Scanning a cloud storage .....	108
Scheduling a scan .....	108
Viewing scan results .....	109
Scanning Zip files .....	109
Fabric Connectors .....	110
ICAP Connectors .....	110
Security Fabric Connector .....	112
Endace .....	113
Enforcement Settings .....	115
Creating enforcement profiles .....	116
Automation Framework .....	118
FortiGate quarantine webhook setup example .....	120
FortiSwitch quarantine setup example .....	124
FortiNAC quarantine setup example .....	126
Generic Webhook setup example .....	127
Automation log .....	127
Automation Status and Post action .....	128
FortiSandbox integration (FortiSandbox 4.0.1 and higher) .....	129
FortiGate inline blocking (FOS 7.0.1 and higher) .....	130
Tips for using FortiNDR inline blocking .....	131
FortiNDR inline inspection with other AV inspection methods .....	132
Accepted file types .....	133
FortiGate integration (integrated mode with FOS 6.2 and higher) .....	133

<b>Virtual Security Analyst</b> .....	<b>138</b>
Express Malware Analysis .....	138
Outbreak Search .....	142
Search lead type of hash or detection name .....	142
Search lead type of outbreak name .....	143
Recursive searches .....	144
Reports .....	144
Static Filter .....	144
NDR Muting .....	145
Muting rules in Network Insights .....	146
Managing muted rules .....	146
ML Configuration .....	147
Source IP tab .....	147
Default Tab .....	150
Sensor Group ID Tab (Center mode) .....	151
Retrain baseline .....	154
Malware Big Picture .....	155
Device Enrichment .....	156
Viewing the retrieved device identifier .....	157
Overwriting the device identifier .....	158
Creating a Device Enrichment Profile .....	159
<b>Netflow</b> .....	<b>161</b>
Netflow Dashboard .....	161
Customizing the Netflow Dashboard .....	163
Netflow Log .....	163
Viewing anomalies .....	164
Netflow ML discovery .....	165
Viewing flow information .....	166
Netflow ML Configuration .....	166
Default tab .....	167
Source IP tab .....	169
<b>Network</b> .....	<b>171</b>
Interface .....	171
DNS and Static Routes .....	171
<b>System</b> .....	<b>172</b>
Administrators .....	172
Password policy .....	173
Admin Profiles .....	174
Pre-defined profile types .....	174
Access Permissions .....	174
Sensor Settings (Center Standalone) .....	175
Sensor Details .....	176
Firmware .....	177
Settings .....	177
SNMP .....	178
Basic Configuration .....	178

SNMP MIB files .....	181
Artifact Storage (Standalone and Sensor) .....	182
Artifact Storage Config tab .....	182
PCAP tab .....	183
FortiGuard .....	184
FDS server override .....	187
Using FortiGuard Anycast servers .....	188
Using FortiManager for FDS updates .....	189
Using FortiManager IOC/WebFilter query .....	189
Certificates .....	190
High Availability (HA) .....	191
HA setup requirements .....	192
Configuring an HA group .....	192
Check HA status .....	195
HA Failover .....	196
HA configuration settings synchronization .....	198
HA Logs .....	199
Using Virtual IP .....	199
Conserve Mode .....	200
Backup or restore the system configuration .....	201
<b>User &amp; Authentication .....</b>	<b>203</b>
RADIUS Server .....	203
LDAP Servers .....	204
LDAP user query example .....	207
Alias member query example .....	207
Preparing your LDAP schema for FortiNDR LDAP profiles .....	208
Using common schema styles .....	208
<b>Log &amp; Report .....</b>	<b>210</b>
Malware Log .....	210
Download a sample .....	211
View items in a zip folder .....	212
Perform a batch download .....	212
Add detections to the Allow List .....	212
Advanced search .....	213
NDR Log .....	213
Anomaly tab .....	214
Session Tab .....	215
Device Tab .....	216
Forensic information .....	218
Events .....	219
Daily Feature Learned .....	220
Log Settings .....	221
Log Settings in Center mode .....	221
Alert Email Setting .....	221
Email Alert Recipients .....	222
NDR logs samples .....	223
Botnet .....	223

Encrypted .....	223
IOC .....	224
IPS attack .....	224
Weak cipher .....	224
ML .....	225
Common Fields .....	225
AV log samples .....	227
NetFlow logs samples .....	228
suspicious-activity .....	228
ML .....	228
<b>Troubleshooting .....</b>	<b>229</b>
FortiNDR troubleshooting tips .....	229
File scanning related issues .....	230
Manual Upload/API Submission/FortiSandbox Integration .....	230
File Submitted but not processed .....	231
Information for support tickets .....	231
FortiNDR health checks .....	232
Sniffer diagnosis .....	233
Rebuild RAID disk .....	234
Managing FortiNDR disk usage for Center mode .....	237
Managing FortiNDR disk usage for Standalone and Sensor mode .....	237
Exporting detected malware files .....	238
Formatting the database .....	240
Export malware .....	240
Working with false positives and false negatives .....	241
Troubleshoot ICAP and OFTP connection issues .....	241
Troubleshoot Log Settings .....	243
Troubleshoot Network Share .....	244
Test the Network Share Connection .....	244
Diagnosing Network Share Errors .....	246
Debug version image .....	247
Check Crash Log .....	247
Troubleshooting the VM License .....	248
Troubleshooting the updater .....	248
FDS Authorization Failed .....	248
Clearing updater cache files .....	249
Diagnosing Other FDS Errors .....	249
Troubleshooting tips for Network File Share .....	249
Sensor logs not displaying in Center GUI .....	253
Troubleshooting FortiNDR VM high CPU usage .....	253
Troubleshooting inactive Netflow status .....	253
<b>Appendix A: API guide .....</b>	<b>255</b>
Get an administrator API key .....	255
Upload files using API .....	255
Use an API key .....	256
Submit files .....	256

---

Upload file by JSON data .....	257
Retrieve file verdict results .....	258
Get file stix2 report .....	261
Start Network Share scan .....	262
Events API support .....	262
Start Cloud Storage scan .....	264
/api/v1/cloud/scan .....	264
Detected Samples .....	264
/api/v1/detected-samples/download .....	265
<b>Appendix B: Sample script to submit files .....</b>	<b>267</b>
<b>Appendix C: FortiNDR ports .....</b>	<b>273</b>
<b>Appendix D: FortiGuard updates .....</b>	<b>275</b>
Updating the ANN database from FDS for malware detection (GUI) .....	276
Updating ANN for malware detection (CLI) .....	277
<b>Appendix E: Event severity level by category .....</b>	<b>281</b>
<b>Appendix F: IPv6 support .....</b>	<b>282</b>
<b>Appendix G: Supported Application Protocol List .....</b>	<b>284</b>
<b>Appendix H: File types and protocols .....</b>	<b>285</b>
<b>Appendix I: Operational Technology / SCADA vendor and application list .....</b>	<b>286</b>
<b>Appendix J: Center Sensor Deployment .....</b>	<b>288</b>
Topology .....	288
Redundant Center Setup .....	289
On-premises and Private Cloud (FNDR3K5, VM and KVM) .....	289
Public Cloud IAAS (AWS IaaS) .....	289
Hybrid Cloud Deployment .....	289
NAT Support .....	289

# Change Log

Date	Change Description
2024-10-17	Initial release.
2024-10-23	Updated <a href="#">FortiNDR traffic and files input types</a> on page 17.
2024-12-20	Updated <a href="#">ML Configuration</a> on page 147 Added <a href="#">OT Devices</a> on page 37.
2025-01-20	Updated <a href="#">Conserve Mode</a> on page 200.
2025-03-06	Updated <a href="#">Appendix C: FortiNDR ports</a> on page 273.
2025-08-06	Updated <a href="#">Device Inventory</a> on page 35.
2025-11-21	Updated <a href="#">FortiGate quarantine webhook setup example</a> on page 120.
2025-12-12	Updated <a href="#">FortiGuard</a> on page 184.

# Introduction

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

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

FortiNDR is the next generation of Fortinet breach detection technology, using both ML and Artificial Neural Networks (ANN) which can detect network anomalies and high velocity malware detection and verdict using patented Artificial Neural Networks (abbreviated with ANN in document, [US patent US11574051B2](#)).

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

- Detect encrypted attack (via JA3 hashes), look for presence of malicious web campaigns visited, weaker ciphers, vulnerable protocols, network intrusions and botnet-based attacks.
- Profile ML traffic and identify anomalies with user feedback mechanism.
- Quickly detect malicious files through neural network analysis including NFS file scan shares.
- Analyze malware scientifically by classifying malware based on its detected features, for example, ransomware, downloader, coinminer, and so on.
- Trace the origins of the attack, for example, worm infection.
- Outbreak search can use the similarity engine to search for malware outbreaks with hashes and similar variants in the network.
- Analyze Netflow data including machine learning of Netflow data, to detect attacks and anomalies.
- 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 I](#) for list of OT applications support. Note: VM08 supports sensors mode only. Netflow is not supported)

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 anomalies with different techniques where traditional security solutions might fail. The NDR solution is a passive solution with analyzing network metadata and uses it to determine if an attack occurs.
- Provide more context to attacks such as malware campaign name, web campaign devices and users participate in, intrusions and botnet attacks
- Tracing and correlate source of malware events such as worm based detection
- Upon attacks or anomalies detected, FortiNDR can perform manual and automatic mitigation (AKA Response) with Fortinet Security Fabric devices (such as FortiGate, FortiSwitch, FortiNAC), as well as 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 174](#).

---

### 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 cCloud 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 7.6.0 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
<b>Dashboard</b>	✓	✓	✓	In Center mode, the widgets are used to monitor the sensors.
<b>Security Fabric</b>	✓		✓	Security Fabric is configured in the Sensor mode or via the Center mode settings.
<b>Virtual Security Analyst &gt; Express Malware Analysis</b>	✓		✓	

Feature	Standalone	Center	Sensor	Notes
<b>Virtual Security Analyst &gt; Static Filter</b>	✓	✓		Static Filters, including the <i>Allow List</i> and <i>Deny List</i> , are employed in Center mode and associated with specific sensors. These filters provide users with the capability to formulate and modify an <i>Allow</i> or <i>Deny</i> list for targeted sensors. Please note that these Static Filters cannot be set through the Sensor's GUI.
<b>Virtual Security Analyst &gt; NDR Muting</b>	✓	✓	✓	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.
<b>Virtual Security Analyst &gt; ML Discovery</b>	✓	✓		Both the <i>ML Discovery</i> dashboard widget and <i>ML Discovery</i> module are not available in Sensor mode.
<b>Virtual Security Analyst &gt; Device Enrichment</b>	✓			
<b>Virtual Security Analyst &gt; ML Configuration</b>		✓		
<b>Netflow</b>	✓	✓	✓	Sensor mode maintains the same design and functionality for the <i>Netflow Dashboard</i> and <i>Netflow Log</i> as seen in Standalone mode. Center mode's <i>Netflow Dashboard</i> and <i>Netflow Log</i> display the data collated from the Sensors.
<b>Global Investigation and Tagging</b>		✓		Query metadata and tagging of sessions. This feature is available in FNR-3600G only.

Feature	Standalone	Center	Sensor	Notes
				This feature is not supported in VM-CM and 3500F as of 7.6.0.
<b>System &gt; Admin Profiles</b>	✓	✓	✓	In Center mode, users can select which Sensor(s) are linked with the current profile. If a Sensor is selected to be included in this <i>Admin Profile</i> , the profile user will be able to view and manage the corresponding Sensor when they log into the FortiNDR Center.
<b>System &gt; Center Settings</b>		✓		
<b>System &gt; High Availability (HA)</b>	✓			
<b>Log &amp; Report &gt; Daily Feature Learned</b>	✓	✓		In Center mode, the Log Settings can be configured to send the center's system event log to the syslog servers. Detection logs, including malware logs and NDR logs that record events occurring in the sensors, are sent directly from the sensors themselves. These sensors' syslog configurations can be edited and uploaded via the <i>Center's System &gt; Sensor Settings</i> page using the <i>Restore Configuration</i> button.

## 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.

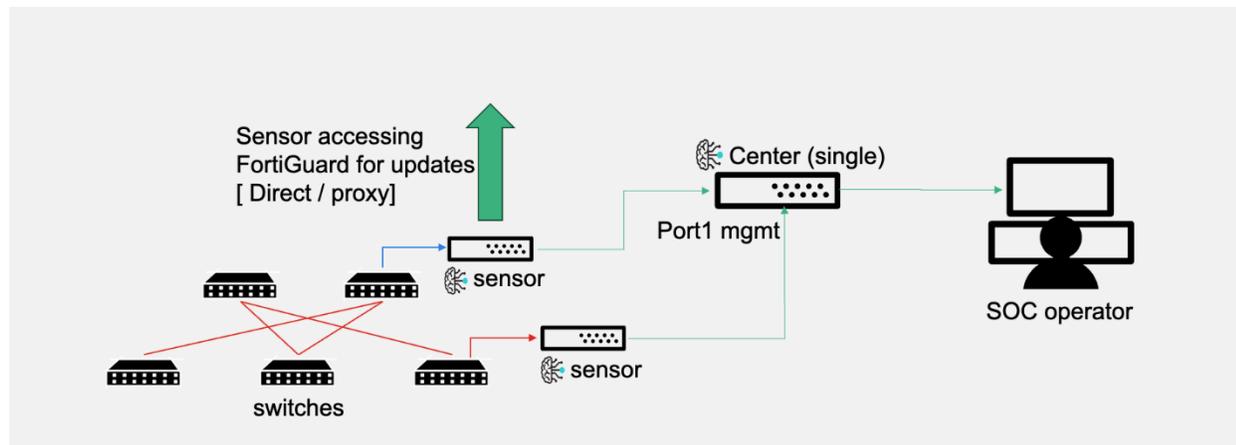
In Center Mode, the system does require a Neflow license to access the Netflow module.

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

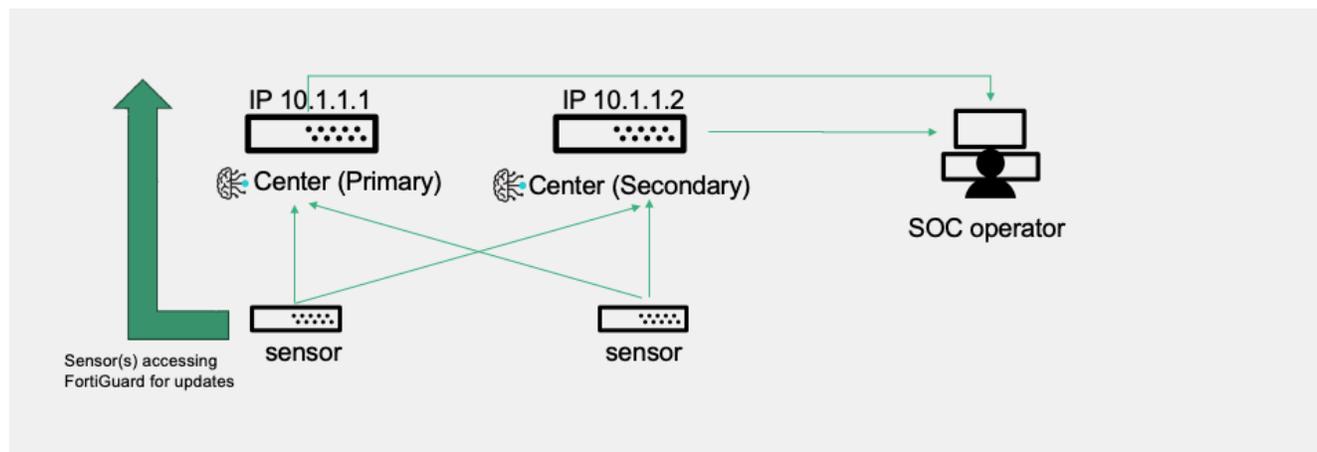
## Dual Center mode support

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:*

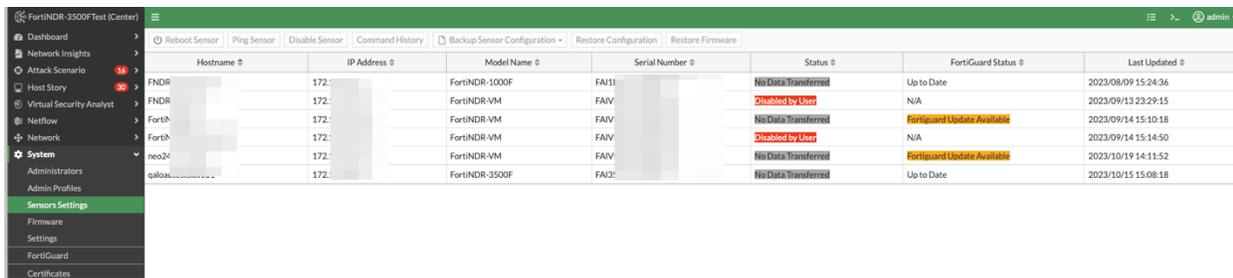


*Dual NDR center support:*

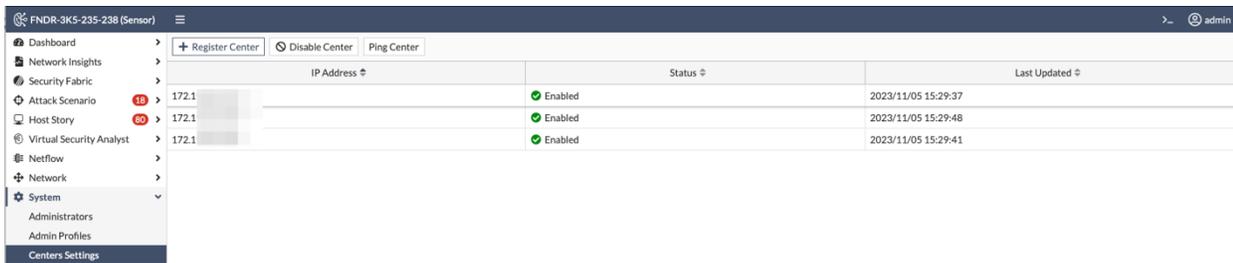


Sensors data are synchronized periodically between sensors and center using HTTPS port 443, connections are initiated by sensor to center. For a complete list of FortiNDR ports required, see [Appendix C: FortiNDR ports on page 273](#). If network issues occurs, sensors will resume synchronization again 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, see [Sensor Settings \(Center Standalone\)](#) on page 175 .

## FortiNDR traffic and files input types

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

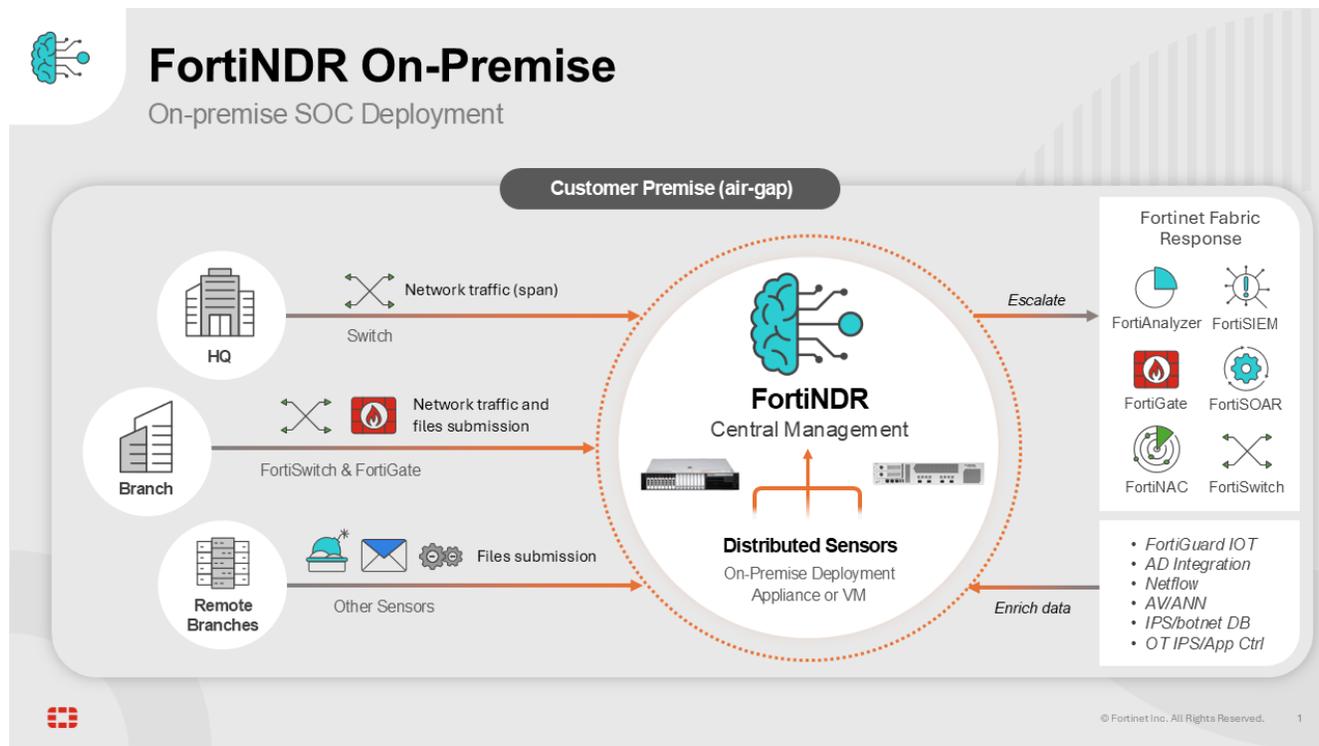
For more information, see the [FortiNDR CLI Reference Guide](#).

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
<b>Sniffer</b>			HTTP, SMBv2, IMAP, POP3, SMTP, FTP	TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP,SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors	Using SPAN port or network TAP. Using SPAN port, network tap or packet brokers to mirror traffic.

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	NDR Network Anomalies Protocols Supported	Notes
<b>Fabric devices</b>	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 <i>profile</i> under FortiMail.
	FortiSandbox	HTTP2	MAPI, FTP, CIFS		
	FortiProxy	HTTP2	HTTP, HTTPS		Supports FortiProxy 7.0.0 and higher
<b>ICAP</b>	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.
<b>Other / API</b>	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 285](#)

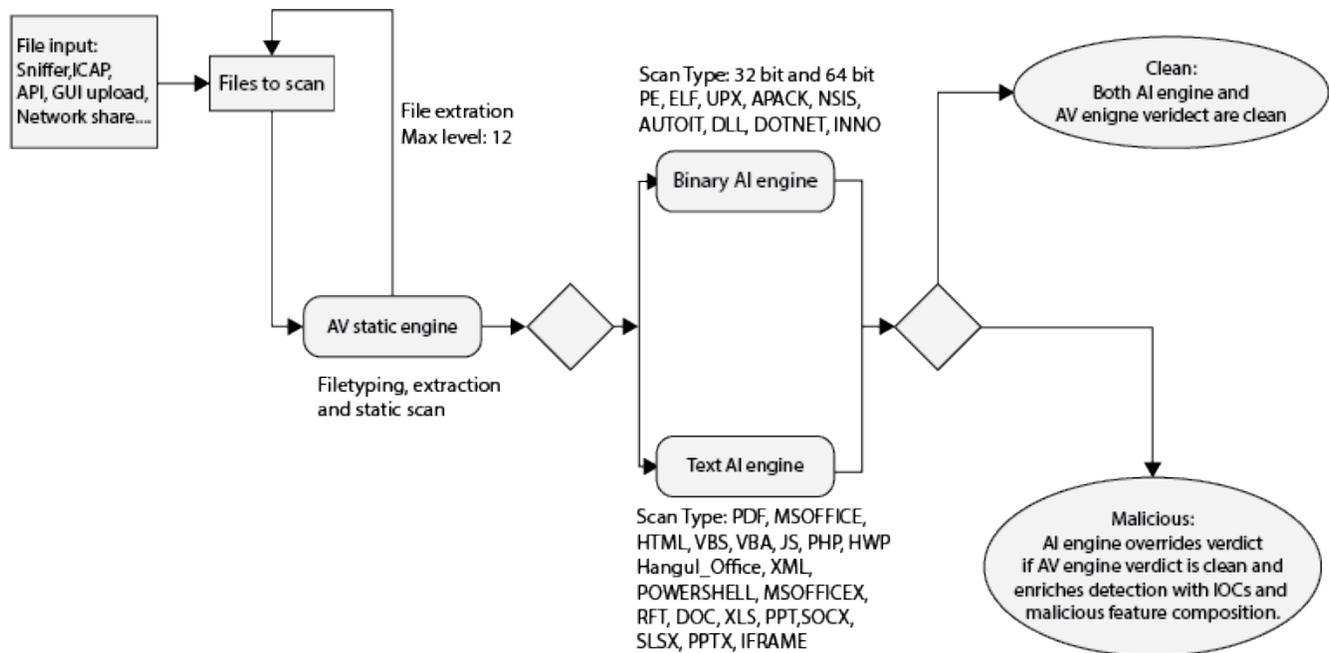
FortiNDR supports quarantine with incoming webhook from FortiOS 6.4 and higher. For details, see the [Release Notes](#). For FortiNDR to quarantine via FortiGate, you must provide VDOM information to FortiGate. For details, see [Automation Framework on page 118](#).



## Files and malware scan flow using AV and ANN

### Stage 1

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



## Stage 2

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

## Planning deployment

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



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

### Storage by model

- FNR-1000F supports 2 x 7.68TB SSD storage in RAID 1 configuration, this is not expandable.
- FNR-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
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).

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

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

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

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

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



For the latest performance related specs, please refer to the FortiNDR [datasheet](#).

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

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

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

## Additional SSD

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

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



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

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

### To add additional SSD to FortiNDR 3500F:

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

```
exec raidlevel 10
```

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

### To check the new SSD capacity with the GUI:

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

### To check the new SSD capacity with the CLI:

```
Get system raid-status
```

Sample output:

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

```

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

```

## Preparing the virtual environment

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

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

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



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

## Initial setup

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

## Internet Access

For FortiGuard updates please have a stable internet access from the FortiNDR unit. Go to *System > FortiGuard* for updates via Internet. For offline deployments please refer to [Appendix D: FortiGuard updates on page 275](#).



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.

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

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

The following is the initial port configuration for FNR-3500F.

Port	Type	Function
<b>Port1</b>	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.
<b>Port2</b>	10GE copper (10G or 1G autodetect)	Sniffer port.
<b>Port3</b>	1G Copper	High availability
<b>Port4</b>		
<b>Port5</b>	10G SPF+ fiber (gen3 only)	Sniffer port.
<b>Port6</b>		For VM, only Port5 is used as sniffer port among Port5, Port6, port7 and Port8.
<b>Port7</b>		
<b>Port8</b>		
<b>Console</b>	Serial port	Console serial port.

Port	Type	Function
		9600 baud, 8 data bits, 1 stop bit, no parity, XON/XOFF.

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

Port	Type	Function
Port1	10G fiber	Management port, GUI, Fabric devices files receiving, REST API, ICAP. Default IP address is 192.168.1.88 using admin with no password.
Port2	10G fiber	Reserved
Port3 Port4	10G fiber	Sniffer port.
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 26
- Vulnerability - monitoring PSIRT on page 26
- Firmware on page 26
- Encrypted protocols on page 26
- FortiGuard databases on page 27
- Penetration testing on page 27
- 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 172](#).

## 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 ndr <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 110](#).

## Configuration backup

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

## Logging

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

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

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

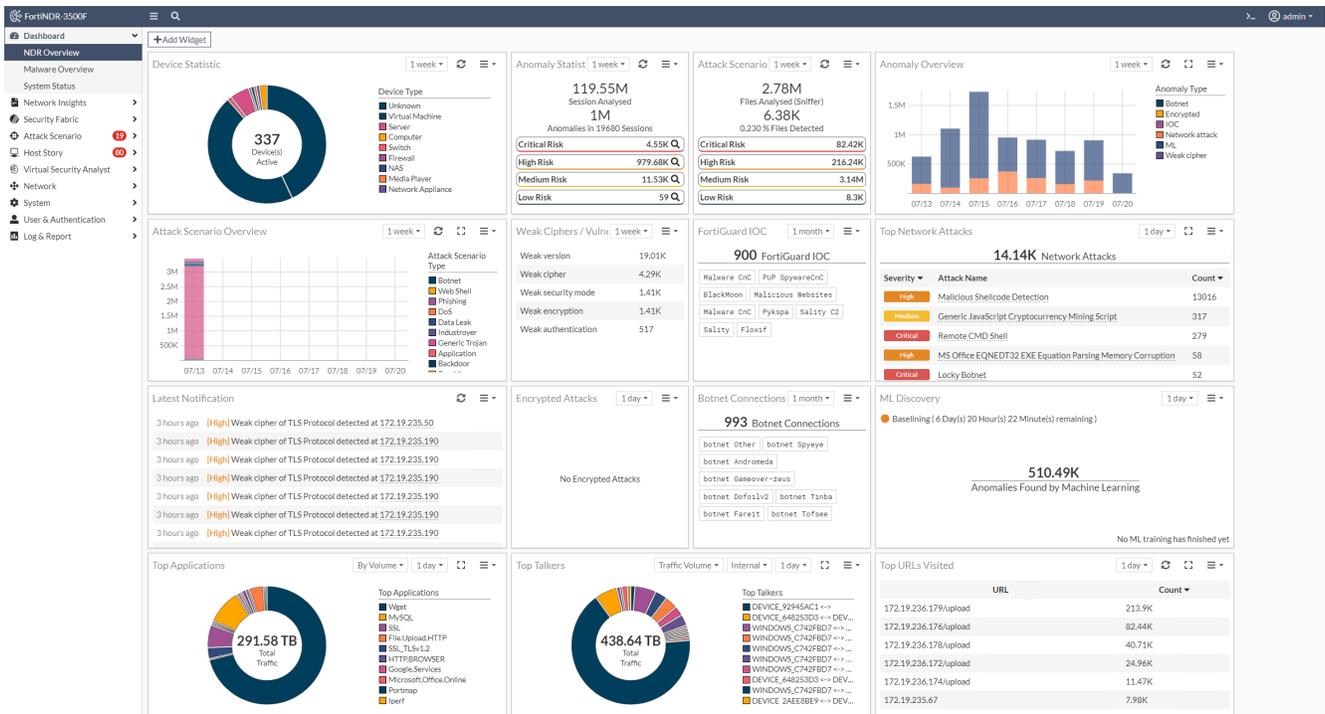
# Dashboard

The *Dashboard* displays the overall anomalies detected by FortiNDR as well as the system status. The Dashboard contains three views: *NDR Overview*, *Malware Overview*, and *System Status*. Users are welcome to add custom dashboards and appropriate widgets tailored for their operations. There are FortiNDR widgets such as *Botnet*, *Attack Scenarios*, and *Sessions Analyzed* to cater to different needs.

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

## NDR Overview

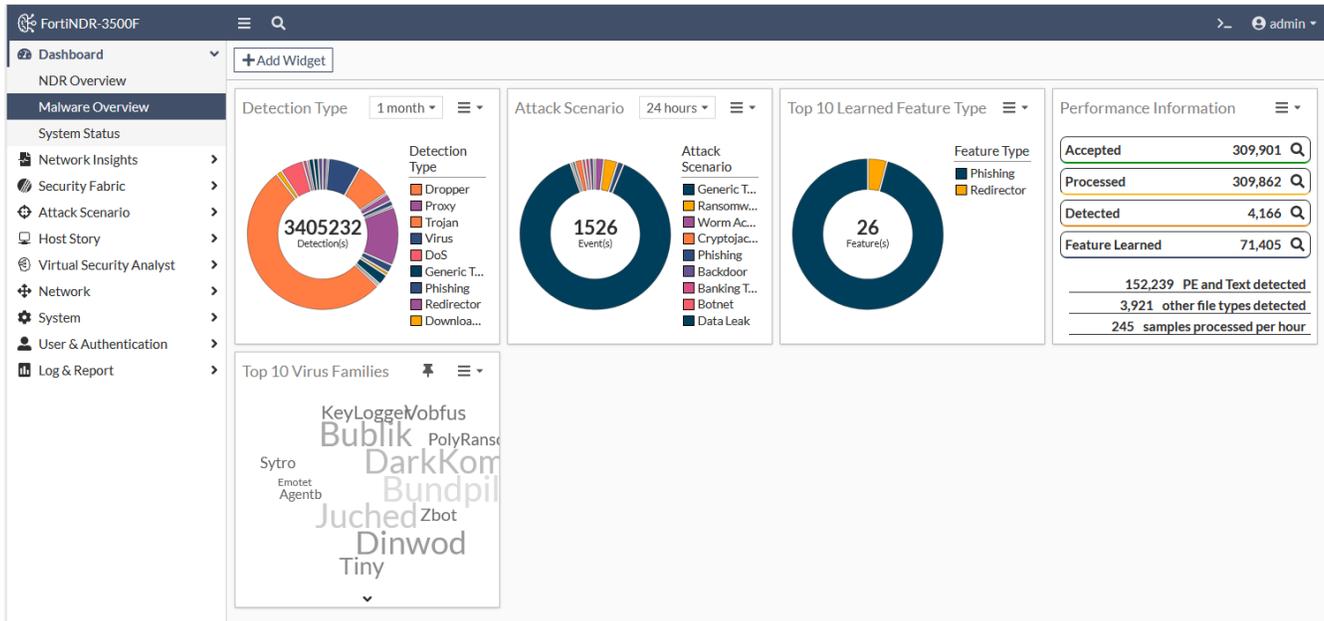
The *NDR Overview* dashboard displays the information in the *Network Insights* as charts and graphs. Each widget can be filtered with a time range of *1 day*, *1 week*, or *1 month*. When you click the *Network Insights* widgets, such as *ML Discovery* and *Botnet*, the widget expands to full screen.



*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.

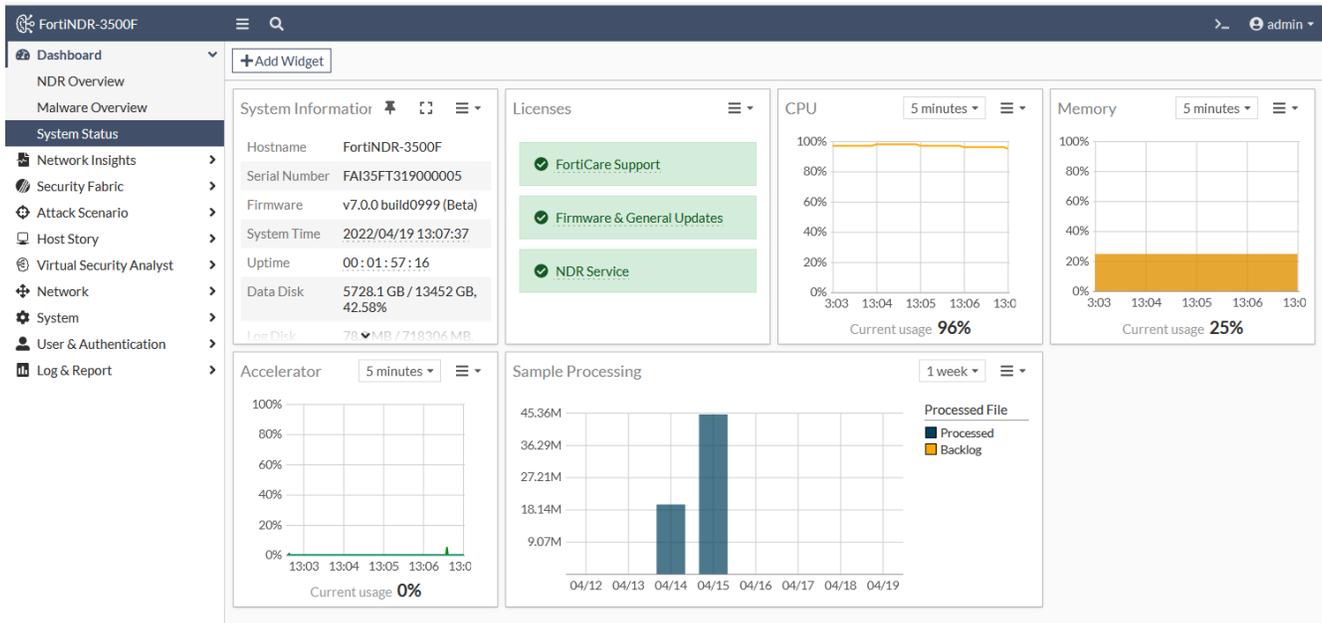
## Malware Overview

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



## System Status

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



## Custom dashboards

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

### To add a widget to a dashboard:

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



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.

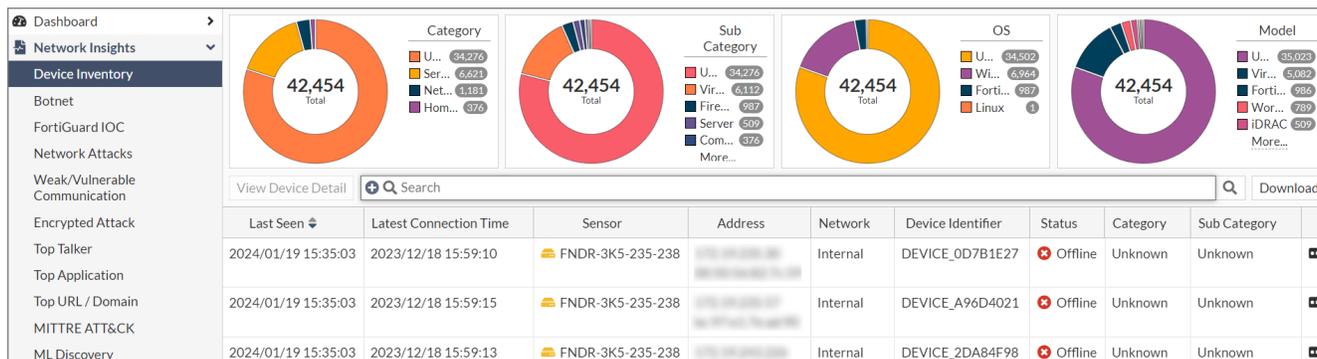
---

**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
<b>Device Inventory</b>	<p>Displays the discovered devices. The priority of devices is from highest to lowest:</p> <ol style="list-style-type: none"> <li>1. User defined (for example, finance server).</li> <li>2. AD Device enrichment (hostname from AD, if configured).</li> <li>3. System generated (OS_hash of the mac address).</li> </ol> <p>The device name in the <i>Device</i> column is determined by the <i>OS_hash</i> of the mac address Status (online/offline). If FortiNDR does not see a session from a device within 60 seconds, the status will be <i>Offline</i>.</p>
<b>Botnet</b>	<p>Displays the botnet traffic detections. If there is a known Botnet name, it will be displayed.</p>
<b>FortiGuard IOC</b>	<p>Displays suspicious URLs and IPs that are flagged by FortiGuard. This anomaly discovery depends on FortiNDR look up in the FortiGuard IOC service. Apart from URL category (e.g. malicious websites), you will also see an extra information column for any campaign name involved (e.g. Solarwind, Locky Ransomware).</p>
<b>Network Attacks</b>	<p>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.</p>
<b>Weak/Vulnerable Communication</b>	<p>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).</p>
<b>Encrypted Attack</b>	<p>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.</p>

Monitor	Description
<b>ML Discovery</b>	Displays a list of anomalies detected by Machine Learning configuration. Each row is based on a session. The configuration and baselining of ML Discovery is located under <i>Virtual Security Analyst &gt; ML configuration</i> . ML discovery is switched ON by default.

## Anomaly, Connection and Session tabs

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

<b>Anomaly</b>	<p>The records in the <i>Anomaly</i> tab are grouped by anomaly types and sensor. Each record may contain different IP pairs. If you display the <i>Destination IP</i> and <i>Source IP</i> columns, you will see the most recent Destination and Source IPs. Double-click a record to open the <i>Anomaly Information</i> pane which contains all the connection pairs. Connections are grouped by destination-source IP pairs.</p> <p><i>Example:</i> Network Attacks Insights</p> <ul style="list-style-type: none"> <li>• Sensor 1: TCP port scan (contain multiple src/dst IP pairs)</li> <li>• Sensor 1: DNS amplification attack</li> </ul> <p>For more information, see <a href="#">Anomaly tab on page 66</a>.</p>
<b>Connection</b>	<p>Shows attacks grouped by Source and Destination IP pairs, and sensor.</p> <p><i>Example:</i> Botnet Network Insights</p> <ul style="list-style-type: none"> <li>• Sensor 1: Src 1.1.1.1 dst 2.2.2.2 count</li> </ul> <p>For more information, see <a href="#">Connection tab on page 69</a>.</p>
<b>Session</b>	<p>Shows granular session information for each attack including the Source and Destination IPs.</p> <p>For more information, see <a href="#">Session tab on page 71</a>.</p>

## Common fields

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

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

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

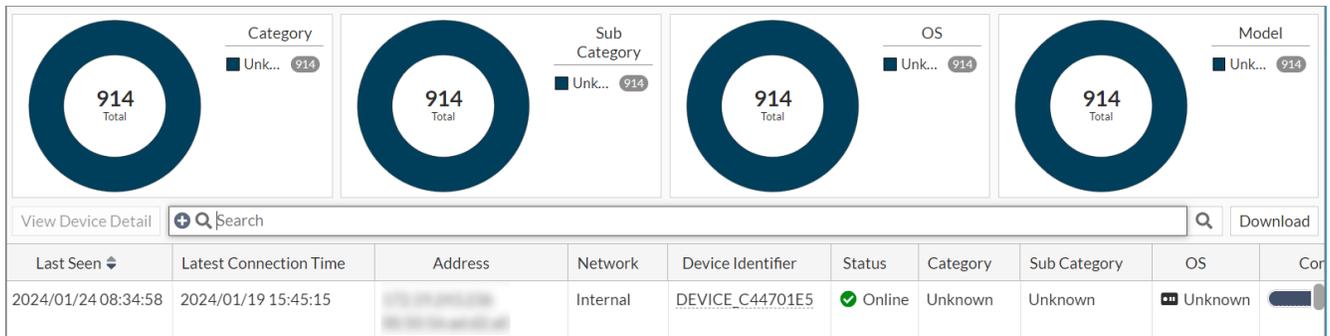
## Device Inventory

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

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

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

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



The *Device Inventory* monitor displays the following information:

Column	Description
<b>Last Seen</b>	The date and time the device was last seen.
<b>Latest Connection Time</b>	The date and time of latest connection.
<b>Address</b>	The device IP address
<b>Device Identifier</b>	The device identifier.
<b>Status</b>	The connection status ( <i>Online</i> or <i>Offline</i> ). If FortiNDR does not see a session from a device within 60 seconds, the status will be <i>Offline</i> .
<b>Category</b>	The device category ( <i>Unknown</i> , <i>Home &amp; Office</i> , <i>Mobile</i> and <i>Network</i> ).
<b>Sub Category</b>	The device sub category ( <i>Unknown</i> , <i>IP Phone</i> , <i>Computer</i> , <i>Phone</i> , or <i>Firewall</i> )
<b>OS</b>	The device operating system.
<b>Confidence</b>	The confidence level.
<b>Country</b>	The device country if known.
<b>Device ID</b>	The device ID.
<b>Latest Device Enrichment</b>	The timestamp for the latest device enrichment. See <a href="#">Device Enrichment on page 156</a>
<b>Model</b>	The device model.
<b>Vendor</b>	The device vendor.

**To download the Device Inventory:**

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

**To view Device Information:**

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

<b>General</b>	<ul style="list-style-type: none"> <li>• Device ID</li> <li>• Device Name</li> <li>• Status</li> <li>• Discovery Time</li> <li>• Last Seen</li> </ul>
<b>Hardware</b>	<ul style="list-style-type: none"> <li>• Model</li> <li>• Operating System</li> <li>• Category</li> <li>• Sub Category</li> <li>• Vendor</li> <li>• Confidence</li> </ul>
<b>Network</b>	<ul style="list-style-type: none"> <li>• Most Recent IP</li> <li>• Internal/External</li> <li>• Mac Address</li> <li>• Country</li> </ul>

## Device details

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

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

## OT Devices

Device Inventory has two tabs:

<b>Device Inventory</b>	All devices
<b>OT Device Inventory</b>	Devices recognized as an Operational Devices based on a device can be: <ul style="list-style-type: none"> <li>• Identified by OT APPDB</li> <li>• Queried from IoT DB and its category is <i>Industry</i></li> </ul>

### 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.

Last Seen	Latest Address	Risk	Device Identifier	Status	Purdue Level	Product	Model	Vendor	Serial Number	Version
2024/12/19 19:15:40	fe80::26fb:1974:d8b8:4bb4 00:50:56:8c:e8:4d	Low	DEVICE_9C70A07C	Online	3.5	Ubuntu	Virtual Machine	Canonical		22.04
2024/12/19 19:11:43	fe80::250:56ff:fe8c:8483 00:50:56:8c:84:83	Critical	DEVICE_8EFBD470	Online	3.5	Windows_2000	Virtual Machine	Microsoft		
2024/12/19 19:11:43	fe80::250:56ff:fe8c:109b 00:50:56:8c:10:9b	Critical	DEVICE_A8CE1F4E	Online	3.5	Windows_2000	Virtual Machine	Microsoft		SP2
2024/12/19 18:35:20	fe80::250:56ff:fe8c:133b 00:50:56:8c:13:3b	Critical	WINDOWS_DDD78370	Online	3.5	Windows_2000	Workstation pro	Microsoft		
2024/12/19 18:30:58	fe80::250:56ff:fe8c:f153 00:50:56:8c:f1:53	Critical	WINDOWS_613BBEF4	Online	3.5	Windows_2000	Virtual Machine	Microsoft		SP2
2024/12/17 15:53:23	172.19.11.158 d2:14:ac:13:0b:9e	Low	DEVICE_DBBB34FC	Offline	3.5	Black Pear	Unknown	Toshiba		
2024/12/17 15:48:56	172.19.11.58	Low	DEVICE_99107911	Offline	3.5	Unknown Model Digital Signal Processor	MDL-S2E-2	TI		

## 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.

The screenshot displays the 'Device Inventory' section of the FortiNDR Network Insights interface. It features a hierarchical tree on the left for navigation, a central table of device details, and a 'Device Information' pane on the right.

Last Seen	Latest Address	Risk	Device Identifier	Status	Purdue Level	Product
2024/12/19 19:15:40	fe80:26f8:1974:d8b8:4bb4 00:50:56:8c:e8:4d	Low	DEVICE_9C70A07C	Online	3.5	Ubuntu
2024/12/19 19:11:43	fe80:250:56ff:fe9c:8483 00:50:56:8c:84:83	Critical	DEVICE_8FBD470	Online	3.5	Windows_2000
2024/12/19 19:11:43	fe80:250:56ff:fe8c:109b 00:50:56:8c:10:9b	Critical	DEVICE_A8CE1F4E	Online	3.5	Windows_2000
2024/12/19 18:35:20	fe80:250:56ff:fe9c:133b 00:50:56:8c:13:3b	Critical	WINDOWS_DDD78370	Online	3.5	Windows_2000
2024/12/19 18:30:58	fe80:250:56ff:fe8c:f153 00:50:56:8c:f1:53	Critical	WINDOWS_613BFEF4	Online	3.5	Windows_2000
2024/12/17 15:53:23	172.19.11.158 d2:14ac:130b:9e	Low	DEVICE_DBBB34FC	Offline	3.5	Black Pear
2024/12/17 15:48:56	172.19.11.158	Low	DEVICE_99107911	Offline	3.5	Unknown Model Digital Signal Proc

The 'Device Information' pane on the right provides details for the selected device (DEVICE\_A8CE1F4E):

- General:** Device ID: 187, Device Name: DEVICE\_A8CE1F4E, Status: Online, Discovery Time: 2024/11/25 12:01:11, Last Seen: 2024/12/19 19:11:43.
- Hardware:** Category: Server, Sub Category: Virtual Machine, Operating System: N/A, Confidence: Low 16/255, Vendor: Microsoft, Model: Virtual Machine, Product: Windows\_2000, Firmware: N/A, Version: SP2, Serial Number: N/A.
- Purdue Model:** Purdue Level: 3.5, Purdue Source: Default.
- Network:** Most Recent IP: fe80:250:56ff:fe8c:109b.

## Export OT devices

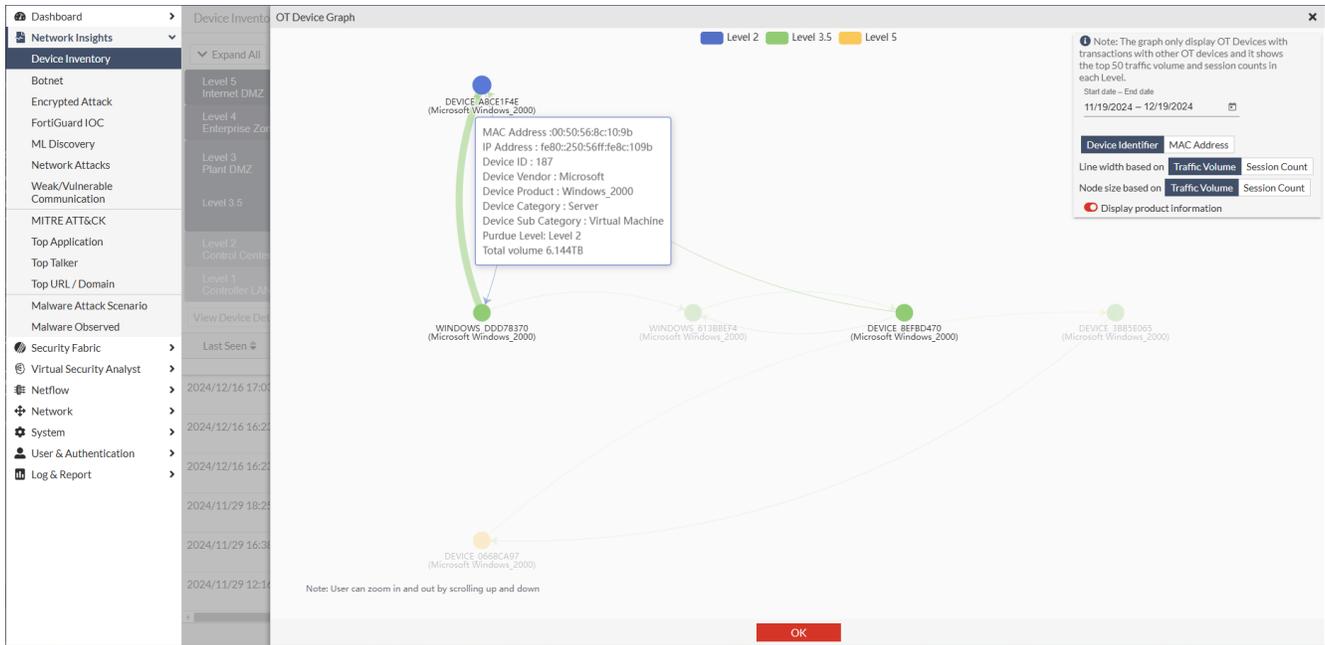
Click the *Download* button. The OT device table data is downloaded as a CSV file.

## 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.

<b>Start Date - End Date</b>	Sets the time range of the device with traffic to be included.
<b>The Device identifier vs MAC address</b>	Controls the legend display under each node that identifies it.
<b>Line Width based on Traffic Volume/Session Count</b>	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
<b>Node size Based on Traffic Volume/ Session</b>	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.



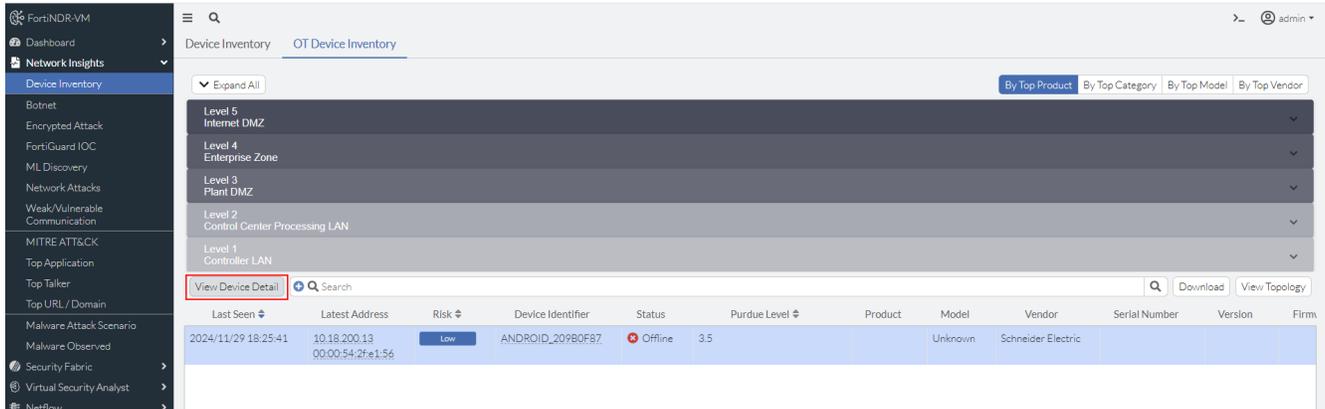
## Modifying the Purdue Level

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.

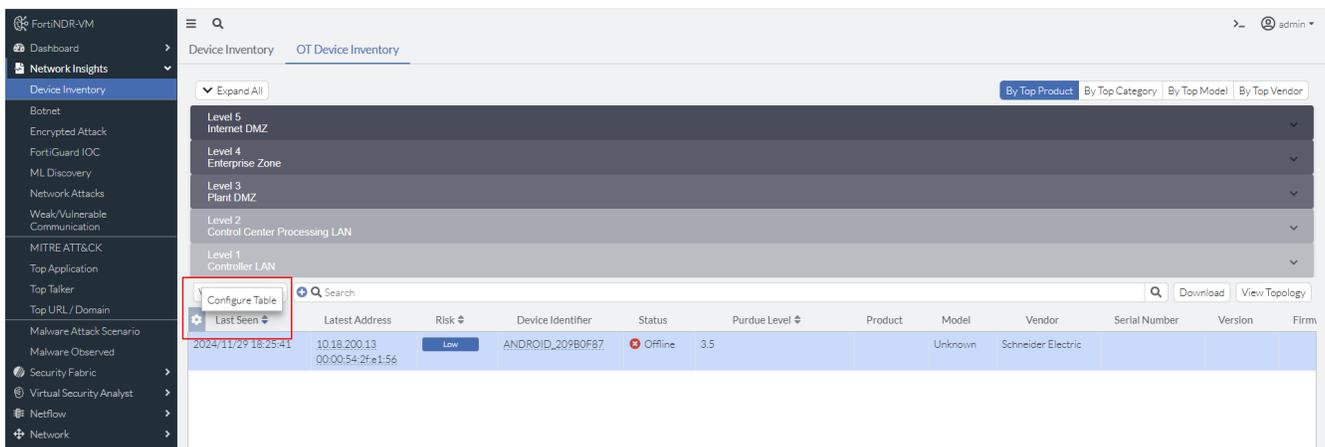
Last Seen	Latest Address	Risk	Device Identifier	Status	Purdue Level	Product	Model	Vendor	Serial Number	Version	Firm
2024/11/29 18:25:41	10.18.200.13 00:00:54:2f:e1:56	Low	ANDROID_209B0F87	Offline	3.5			Schneider Electric			

## 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.

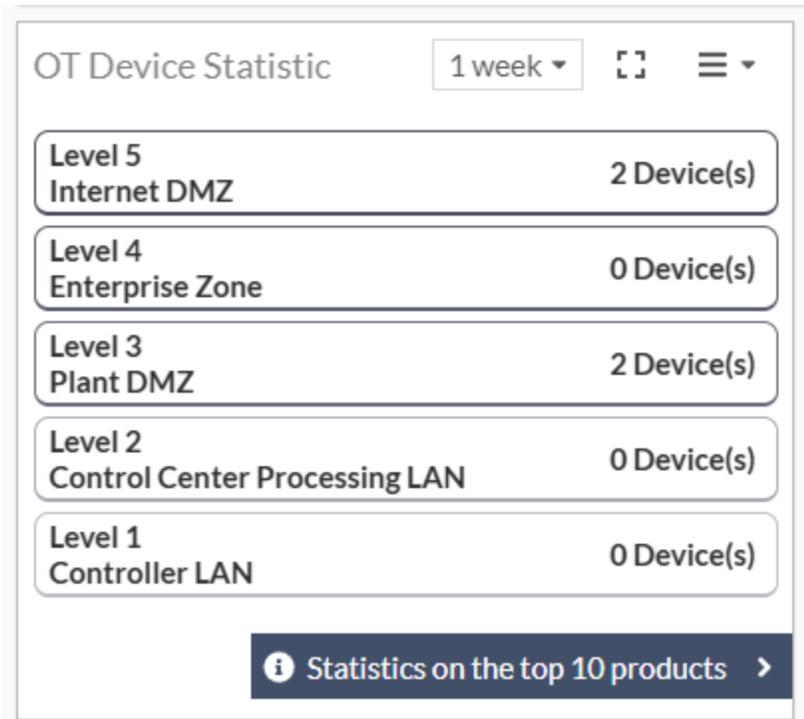


To show more hidden columns in the table, hover over the gear icon and click Configure Table to display the available columns.



## OT Device Widget

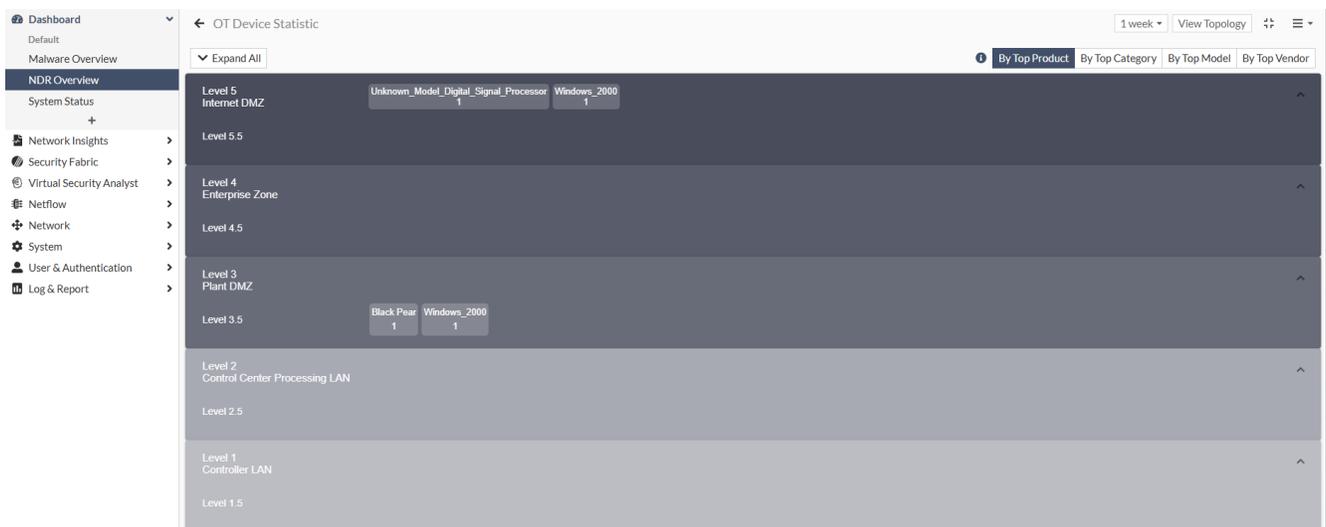
You can track the number of OT devices from different Purdue Levels with the OT device Widget.



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

- Product (Name)
- Category
- Model
- Vendor

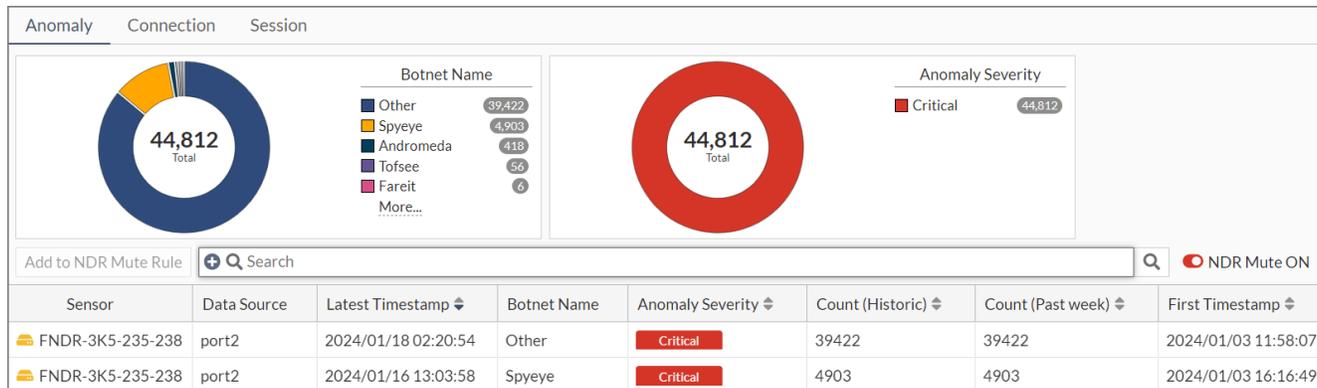
The number in each block below the text indicates the number of devices.



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:

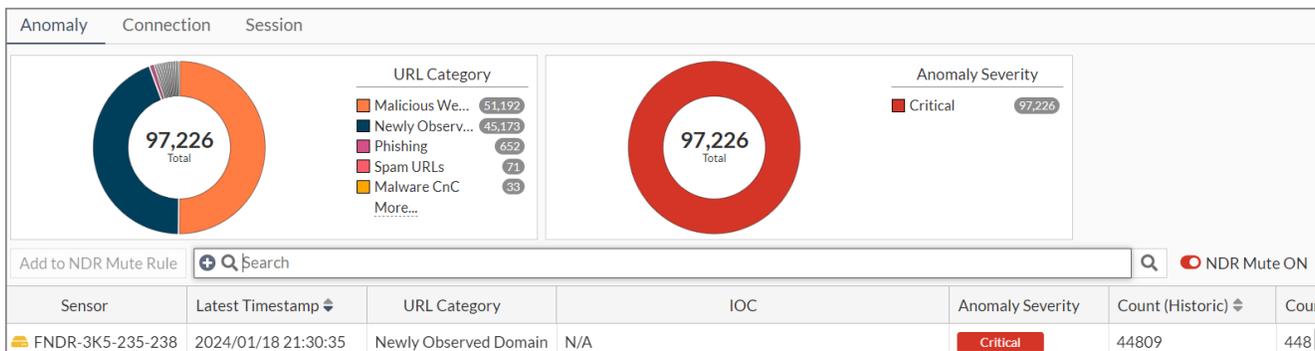
Column	Description
<b>Latest Timestamp</b>	The date the record was updated.
<b>Botnet Name</b>	The botnet name.
<b>Anomaly Severity</b>	The anomaly severity ( <i>Not Anomaly, Info, Low, Medium, High or Critical</i> ).
<b>Count (Historic)</b>	The total number of times the anomaly was observed.
<b>Count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



For information about muting rules, see [NDR Muting on page 145](#).

## FortiGuard IOC

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



The FortiGuard IOC monitor displays the following information:

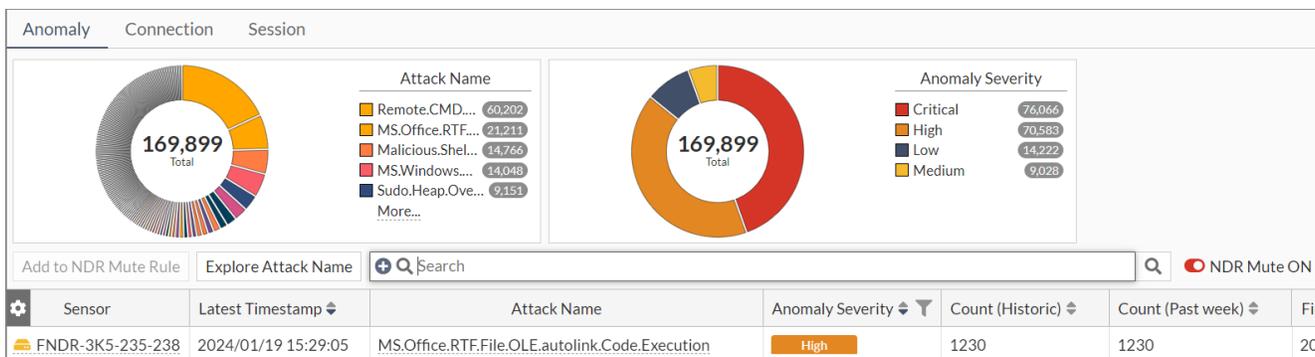
Column	Description
URL Category	The UR Category.
IOC	The Indications of Compromise service.
Anomaly Severity	The anomaly severity ( <i>Not Anomaly, Info, Low, Medium, High or Critical</i> ).
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times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



For information about muting rules, see [NDR Muting on page 145](#).

## 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.



The Network Attacks monitor displays the following information:

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

#### To view the attack information:

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

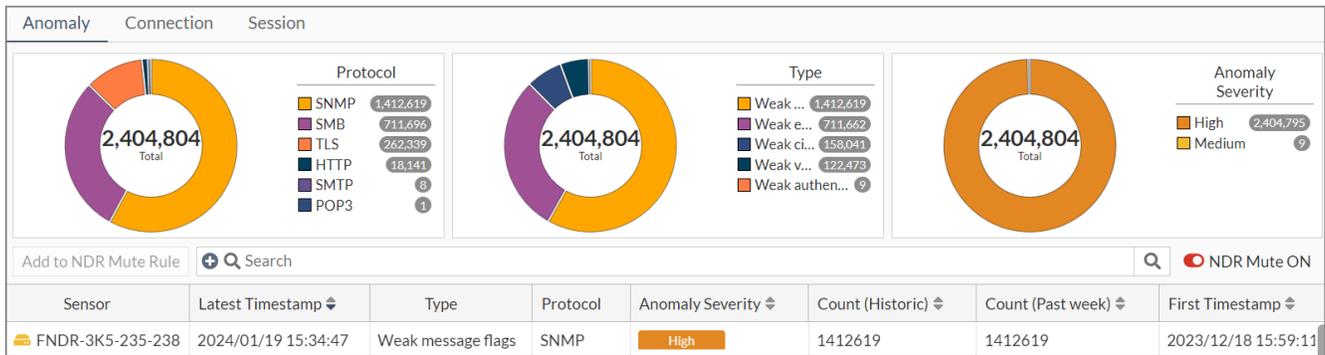
<b>Attack Name</b>	The attack name.
<b>Description</b>	A description of the attack.
<b>Impact</b>	The impact of the attack on your network.
<b>Product List</b>	The affected products.
<b>CVE List</b>	The Common Vulnerabilities and Exposures list.
<b>Mitre Attack Technique</b>	The Mitre Attack Technique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



For information about muting rules, see [NDR Muting on page 145](#).

## 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.



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

<b>Sensor (Center mode)</b>	The network sensor. Hover over the sensors ID to view the <i>IP Address</i> , Serial number ( <i>S/N</i> ), <i>Last Sync Time</i> and <i>Status</i> .																										
<b>Latest Timestamp</b>	The date record was updated.																										
<b>Type</b>	<table border="1"> <thead> <tr> <th>Communication type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>Weak record version</b></td> <td>Weak TLS record layer version.</td> </tr> <tr> <td><b>Weak version</b></td> <td>Weak TLS handshake version.</td> </tr> <tr> <td><b>Weak support version</b></td> <td>Weak TLS handshake extension supported version.</td> </tr> <tr> <td><b>Weak cipher</b></td> <td>Weak TLS handshake cipher suite.</td> </tr> <tr> <td><b>Weak security mode</b></td> <td>SMB protocol uses level security mode.</td> </tr> <tr> <td><b>Weak extended security</b></td> <td>SMB protocol uses outdated extended security negotiation option.</td> </tr> <tr> <td><b>Weak dialect</b></td> <td>SMB uses outdated dialect version.</td> </tr> <tr> <td><b>Weak encryption</b></td> <td>SMB or SSH uses risky encryption algorithm. For example, SMB protocol with encryption disabled.</td> </tr> <tr> <td><b>Weak authentication</b></td> <td>Email protocols are using risky authentication methods. For example, POP3 uses authentication cram-md5, Postgres uses MD5 password as authentication type.</td> </tr> <tr> <td><b>Weak server</b></td> <td>HTTP or RTSP server version is outdated.</td> </tr> <tr> <td><b>Weak method</b></td> <td>HTTP, SIP or RTSP protocol uses weak request method. For example, HTTP protocol uses DELETE as request method.</td> </tr> <tr> <td><b>Weak banner</b></td> <td>Weak or outdated email server version. For example, Outdated Cyrus IMAP server</td> </tr> </tbody> </table>	Communication type	Description	<b>Weak record version</b>	Weak TLS record layer version.	<b>Weak version</b>	Weak TLS handshake version.	<b>Weak support version</b>	Weak TLS handshake extension supported version.	<b>Weak cipher</b>	Weak TLS handshake cipher suite.	<b>Weak security mode</b>	SMB protocol uses level security mode.	<b>Weak extended security</b>	SMB protocol uses outdated extended security negotiation option.	<b>Weak dialect</b>	SMB uses outdated dialect version.	<b>Weak encryption</b>	SMB or SSH uses risky encryption algorithm. For example, SMB protocol with encryption disabled.	<b>Weak authentication</b>	Email protocols are using risky authentication methods. For example, POP3 uses authentication cram-md5, Postgres uses MD5 password as authentication type.	<b>Weak server</b>	HTTP or RTSP server version is outdated.	<b>Weak method</b>	HTTP, SIP or RTSP protocol uses weak request method. For example, HTTP protocol uses DELETE as request method.	<b>Weak banner</b>	Weak or outdated email server version. For example, Outdated Cyrus IMAP server
Communication type	Description																										
<b>Weak record version</b>	Weak TLS record layer version.																										
<b>Weak version</b>	Weak TLS handshake version.																										
<b>Weak support version</b>	Weak TLS handshake extension supported version.																										
<b>Weak cipher</b>	Weak TLS handshake cipher suite.																										
<b>Weak security mode</b>	SMB protocol uses level security mode.																										
<b>Weak extended security</b>	SMB protocol uses outdated extended security negotiation option.																										
<b>Weak dialect</b>	SMB uses outdated dialect version.																										
<b>Weak encryption</b>	SMB or SSH uses risky encryption algorithm. For example, SMB protocol with encryption disabled.																										
<b>Weak authentication</b>	Email protocols are using risky authentication methods. For example, POP3 uses authentication cram-md5, Postgres uses MD5 password as authentication type.																										
<b>Weak server</b>	HTTP or RTSP server version is outdated.																										
<b>Weak method</b>	HTTP, SIP or RTSP protocol uses weak request method. For example, HTTP protocol uses DELETE as request method.																										
<b>Weak banner</b>	Weak or outdated email server version. For example, Outdated Cyrus IMAP server																										

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

## Anomaly information

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

### General tab

The *General* tab displays the following information:

- General**
  - Anomaly Type

	<ul style="list-style-type: none"> <li>• Severity</li> <li>• Reason</li> </ul>
<b>Additional Information</b>	<ul style="list-style-type: none"> <li>• HTTP Version</li> <li>• HTTP Response Code</li> <li>• HTTP Server Name</li> <li>• HTTP URL</li> <li>• Malicious Behavior</li> </ul>
<b>Last Anomaly Occurrence</b>	<ul style="list-style-type: none"> <li>• Latest Occurrence</li> <li>• Count( Past Week)</li> <li>• Count( Historic)</li> <li>• Latest Source IP</li> <li>• Latest Source Port</li> <li>• Latest Source MAC</li> <li>• Latest Source Packet Size</li> <li>• Latest Source Country</li> <li>• Latest Source Device Model</li> <li>• Latest Source OS</li> <li>• Latest Source Device Category</li> <li>• Latest Source Device Sub Category</li> <li>• Latest Destination IP</li> <li>• Latest Destination Port</li> <li>• Latest Destination MAC</li> <li>• Latest Destination Packet Size</li> <li>• Latest Destination Country</li> <li>• Latest Destination Device Model</li> <li>• Latest Destination OS</li> <li>• Latest Destination Device Category</li> <li>• Latest Destination Device Sub Category</li> </ul>

## Analytic tab

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

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



## Weak security mode

The screenshot shows a Wireshark capture of an SMB session. The packet list pane shows several packets, with packet 7 selected. The packet details pane for packet 7 shows the SMB (Server Message Block Protocol) structure. Under the SMB Header, the Negotiate Protocol Response (0x72) is expanded, showing the Security Mode as NT LM 0.12, which is highlighted with a red box. Other details include Word Count (WCT): 17, Selected Index: 3, and various capabilities and session parameters.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.3	10.10.0.2	TCP	66	2204 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	0.000188	10.10.0.3	10.10.0.2	TCP	66	[TCP Out-Of-Order] [TCP Port numbers reused] 2204 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	0.000287	10.10.0.2	10.10.0.3	TCP	66	445 → 2204 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
4	0.000354	10.10.0.2	10.10.0.3	TCP	66	[TCP Out-Of-Order] 445 → 2204 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
5	0.000476	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.653863	10.10.0.3	10.10.0.2	SMB	146	Negotiate Protocol Request
7	0.654248	10.10.0.2	10.10.0.3	SMB	241	Negotiate Protocol Response
8	0.855430	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=89 Ack=210 Win=64031 Len=0
9	1.320851	10.10.0.3	10.10.0.2	SMB	241	Session Setup AndX Request, NTLMSSP_NEGOTIATE
10	1.321035	10.10.0.2	10.10.0.3	SMB	412	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED

```

> Frame 7: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface 0
> Ethernet II, Src: VMware_a8:45:c0 (00:50:56:a8:45:c0), Dst: VMware_a8:1f:7c (00:50:56:a8:1f:7c)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1113
> Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.3
> Transmission Control Protocol, Src Port: 445, Dst Port: 2204, Seq: 1, Ack: 89, Len: 209
> NetBIOS Session Service
> SMB (Server Message Block Protocol)
  > SMB Header
    > Negotiate Protocol Response (0x72)
      Word Count (WCT): 17
      Selected Index: 3: NT LM 0.12
      > Security Mode: NTLM
      Max Mpx Count: 50
      Max VCs: 1
      Max Buffer Size: 16644
      Max Raw Buffer: 65536
      Session Key: 0x00000000
      > Capabilities: 0x8001f3fc, Unicode, Large Files, NT SMBs, RPC Remote APIs, NT Status Codes, Level 2 Oplocks, Lock and Read, NT Find, Dfs, Infollevel Passth...
      System Time: Apr 23, 2015 03:11:08.611869400 Pacific Daylight Time
      Server Time Zone: 0 min from UTC
      Challenge Length: 0
      Byte Count (BCC): 136
      Server GUID: 96afd22e-c9d0-4b45-87ef-481fd5653e5
      > Security Blob: 607606062b0601050502a06c306aa03c303a060a2b06010401823702021e06092a864882..
    
```

## Weak extended security

The screenshot shows a Wireshark capture of an SMB negotiation session. The packet list pane highlights frame 7, which is a '267 Negotiate Protocol Response' from 10.10.0.2 to 10.10.0.3. The packet details pane for this frame shows the SMB command 'Negotiate Protocol (0x72)' with a success status. The 'Flags2' field is expanded to show various negotiation options, with 'Extended Security Negotiation: Extended security negotiation is supported' highlighted in red. The hex dump at the bottom shows the raw data of the response, including the 'P V E' signature and the 'ease\_ign' flag.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000354	10.10.0.2	10.10.0.3	TCP	66	[TCP Out-Of-Order] 445 → 2204 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460...
5	0.000476	10.10.0.3	10.10.0.2	TCP	64	2204 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.653863	10.10.0.3	10.10.0.2	SMB	140	Negotiate Protocol Request
7	0.654248	10.10.0.2	10.10.0.3	SMB	267	Negotiate Protocol Response

```

> Frame 7: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits)
> Ethernet II, Src: VMware_a8:45:c0 (00:50:56:a8:45:c0), Dst: VMware_a8:1f:7c (00:50:56:a8:1f:7c)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1113
> Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.3
> Transmission Control Protocol, Src Port: 445, Dst Port: 2204, Seq: 1, Ack: 89, Len: 209
> NetBIOS Session Service
  > SMB (Server Message Block Protocol)
    > SMB Header
      > Server Component: SMB
        > [Response to: 6]
          [Time from request: 0.000385000 seconds]
          SMB Command: Negotiate Protocol (0x72)
          Error Class: Success (0x00)
          Reserved: 00
          Error Code: No Error
        > Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
        > Flags2: 0x2801, Execute-only Reads, Extended Security Negotiation, Long Names Allowed
          > 0... .. = Unicode Strings: Strings are ASCII
          > .0.. .. = Error Code Type: Error codes are DOS error codes
          > .1. ... = Execute-only Reads: Permit reads if execute-only
          > 0 ... = Dfs: Don't resolve pathnames with Dfs
          > ....1... .. = Extended Security Negotiation: Extended security negotiation is supported
          > ....0... .. = reparse path: The request does not use a @! reparse path
          > ....0... .. = Long Names Used: Path names in request are not long file names
          > ....0... .. = Security Signatures Required: Security signatures are not required
          > ....0... .. = Compressed: Compression is not requested
          > ....0... .. = Security Signatures: Security signatures are not supported
          > ....0... .. = Extended Attributes: Extended attributes are not supported
    > 0000 00 50 56 a8 1f 7c 00 50 56 a8 45 c0 81 00 04 59  -PV-|P V E...Y
    > 0010 08 00 45 00 00 f9 6a 5f 40 00 00 06 74 f7 0a 0a  -E...j_@...t...
    > 0020 00 02 0a 0a 00 03 01 bd 08 9c 7a 75 3c 34 a0 ae  -...zuc4...
    > 0030 3c d7 50 18 fa f0 1b 94 00 00 00 00 00 cd ff 53  -<P...S...
    > 0040 4d 42 72 00 00 00 00 98 01 28 00 00 00 00 00  -MBr...
    > 0050 00 00 00 00 00 00 00 00 72 7c 00 00 a5 44 11 03  -...r|...D...
    > 0060 00 0f 32 00 01 00 04 41 00 00 00 00 01 00 00 00  -..2...A...
    > 0070 00 00 fc f3 01 80 26 a3 2f d1 ad 7d d0 01 00 00  -...&/...}...
    > 0080 00 88 00 96 af d2 2e c9 d0 4b 45 87 ef 48 1f df  -...KE...H...
    > 0090 56 53 e5 60 76 06 06 2b 06 01 05 05 02 a0 6c 30  -VS^v...+...10
    > 00a0 6a a0 3c 30 3a 06 0a 2b 06 01 04 01 82 37 02 02  -j-<0:..+...7...
    > 00b0 1e 06 09 2a 86 48 82 f7 12 01 02 02 06 09 2a 86  -...*H...*...
    > 00c0 48 86 f7 12 01 02 02 06 0a 2a 86 48 86 f7 12 01  -H...*...H...
    > 00d0 02 02 03 06 0a 2b 06 01 04 01 82 37 02 02 0a a3  -...+...7...
    > 00e0 2a 30 28 a0 26 1b 2a 6e 6f 74 5f 64 65 66 69 6e  -*0(&$n ot defin
    > 00f0 65 64 5f 69 6e 5f 52 46 43 34 31 37 38 40 70 6c  -ed_in_RF C4170@pl
    > 0100 65 61 73 65 5f 69 67 6e 6f 72 65
    
```

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

## Weak dialect

The screenshot shows a Wireshark capture of an SMB2 negotiation. The packet list pane highlights packet 5, which is a '294 Negotiate Protocol Response' from 10.0.0.12 to 10.0.0.11. The packet details pane shows the following structure:

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

The packet bytes pane shows the raw data of the response, with a red box highlighting the '02 02' bytes at offset 0070, which correspond to the 'Dialect' field in the details pane.

## Weak authentication

The image shows a Wireshark network capture of a PostgreSQL authentication request. The packet list pane shows a PostgreSQL authentication request (Frame 6) with a length of 12 bytes. The authentication type is MD5 password (5), and the salt value is 065e739f. The packet details pane shows the authentication request structure, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

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

Frame 6: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
 > Ethernet II, Src: VMware\_55:9c:c0 (00:0c:29:55:9c:c0), Dst: Fortinet\_cc:a2:09 (00:09:0f:cc:a2:09)  
 > Internet Protocol Version 4, Src: 10.218.0.100, Dst: 10.218.0.1  
 > Transmission Control Protocol, Src Port: 5432, Dst Port: 63238, Seq: 1, Ack: 43, Len: 13  
 > PostgreSQL  
 Type: Authentication request  
 Length: 12  
 Authentication type: MD5 password (5)  
 Salt value: 065e739f

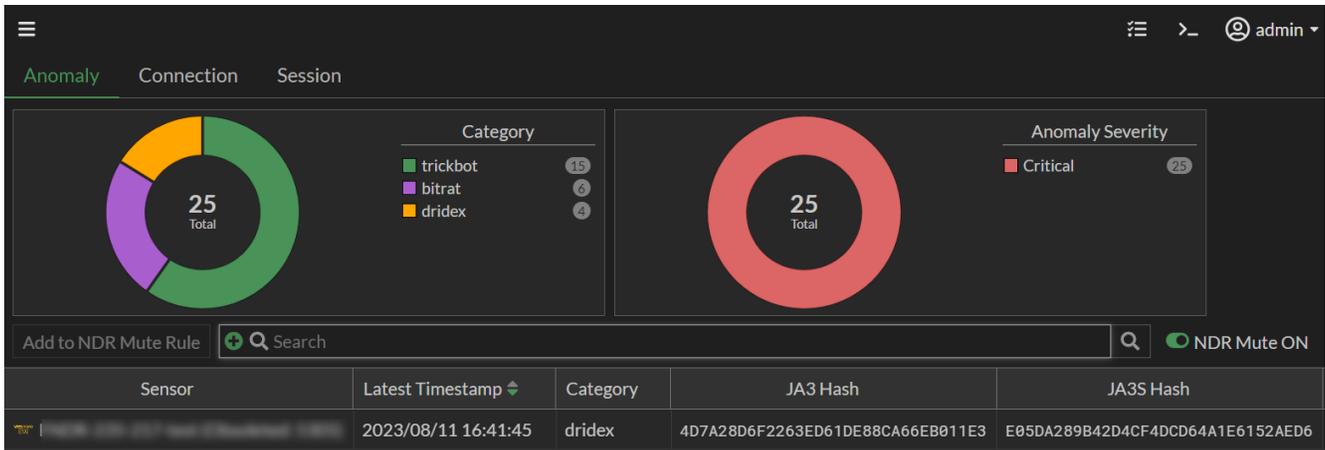
```

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

The type of authentication requested by the backend. (pgsql.authtype), 4 bytes | Packets: 33 · Displayed: 33 (100.0%) | Profile: Default

## Encrypted Attack

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



The *Encrypted Attack* monitor displays the following information:

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



For information about muting rules, see [NDR Muting on page 145](#).

## 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.

Sensor	Connection X <-> Y	X -> Y Volume	Y -> X Volume	X -> Y Traffic Rate	Y -> X Traffic Rate	Session Co
FNDR-3K5-235-238	DEVICE_69665F72 10.200.50.192 ↔ DEVICE_1C46F690 10.200.11.150	553.43 TB	546.43 TB	1.39 Mbps	1.16 Mbps	30,979.4
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_9E4547C8 172.19.243.223	31.15 TB	31.12 TB	130.12 kbps	125.47 kbps	13,186.3
FNDR-3K5-235-238	DEVICE_479E1696 172.19.235.117 ↔ DEVICE_27753EAC 172.16.77.46	26.98 TB	34.29 TB	681.27 kbps	1.34 Mbps	1,958.00
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_604220BF 172.19.243.224	30.45 TB	30.53 TB	127.56 kbps	124.04 kbps	13,127.8
FNDR-3K5-235-238	DEVICE_27753EAC 172.19.235.229 ↔ DEVICE_7FBC4008 172.19.236.120	40.43 GB	38.3 TB	174.32 bps	173.52 kbps	11,350.5

The *Top Talker* page displays the following information:

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

**To set the time range:**

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

**To view the sensor statistics:**

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

Sensor	Connection X <-> Y	X -> Y Volume	Y
FNDR-3K5-235-238	DEVICE_69665F72 10.200.50.192 ↔ DEVICE_1C46F690 10.200.11.150	553.43 TB	5
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_9E4547C8 172.19.243.223	31.15 TB	3
FNDR-3K5-235-238	DEVICE_479E1696 172.19.235.117 ↔ DEVICE_27753EAC 172.16.77.46	26.98 TB	3
FNDR-3K5-235-238	DEVICE_C44701E5 172.19.243.236 ↔ DEVICE_604220BF 172.19.243.224	30.45 TB	3
FNDR-3K5-235-238	DEVICE_27753EAC 172.19.235.229 ↔ DEVICE_7FBC4008 172.19.236.120	40.43 GB	3
FNDR-3K5-235-238	WINDOWS_DBF06816 172.19.236.123 ↔ DEVICE_27753EAC 172.19.235.229	38.17 TB	2
FNDR-3K5-235-238	DEVICE_C742FBD7 172.19.235.190 ↔ DEVICE_27753EAC 10.10.2.13	19.27 TB	1
FNDR-3K5-235-238	DEVICE_7D933B98 10.1.0.1 ↔ DEVICE_42E45E2B 10.1.0.10	14.59 TB	1
FNDR-3K5-235-238	DEVICE_7D933B98 172.19.243.235 ↔ DEVICE_1A5F448C 10.1.0.9	14.46 TB	1
FNDR-3K5-235-238	DEVICE_479E1696 172.19.235.117 ↔ DEVICE_27753EAC 172.19.243.115	24.58 TB	5
FNDR-3K5-235-238	DEVICE_881236A4 ↔ DEVICE_C2EBDA16	10.19 TB	1

1 month

Data from

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

Time Period: 1 month

Category: Traffic Volume

Network Type: Internal

## 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:

<b>Application Name</b>	The protocols and applications identified in the sniffer traffic. For more information, see <a href="#">Appendix G: Supported Application Protocol List on page 284</a> .
<b>Category</b>	The application or protocol category.
<b>Technologies</b>	The application or protocol technology.
<b>Vendor</b>	The application vendor.

<b>Total Count</b>	The number of times the application or protocol was detected during the time frame.
<b>Total Volume</b>	The application volume in MB.
<b>Risk</b>	The risk level ( <i>Critical, High, Medium, or Low</i> )

**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.

View D	Devices	Device	Total Count	Total Volume	Address	Entry Time	Last Seen	Is Internal?
SSL	<div style="border: 1px solid gray; padding: 5px;"> <div style="display: flex; align-items: center; margin-bottom: 5px;">  fe80::250:56ff:fead:f367             </div> <div style="margin-bottom: 5px;">Device DEVICE_7D933B98</div> <div style="margin-bottom: 5px;">MAC Address 00:50:56:ad:f3:67</div> <div style="margin-bottom: 5px;">IP Address fe80::250:56ff:fead:f367</div> <div style="margin-bottom: 5px;">Hardware VMware</div> <div style="margin-bottom: 5px;">OS Unknown</div> <div style="margin-bottom: 5px;">View Device Detail</div> </div>	DEVICE_7D933B98	68	5.98 kB	fe80::250:56ff:fead:f367 00:50:56:ad:f3:67	2024/01/19 15:45:15	2024/01/19 15:46:15	No
QUIC		DEVICE_4E3D2E	43	5.86 kB	fe80::250:56ff:fead:3f66 00:50:56:ad:3f:66	2024/01/19 15:45:16	2024/01/19 15:46:15	No
IPv6.ICM		DEVICE_8B1EF2	41	3.47 kB	fe80::250:56ff:fe9e:7104 00:50:56:9e:71:04	2024/01/19 15:45:18	2024/01/19 15:46:16	No
File.Uplo		DEVICE_E79185	40	5.1 kB	fe80::250:56ff:fead:592a 00:50:56:ad:59:2a	2024/01/19 15:45:17	2024/01/19 15:46:11	No
Fortigua		DEVICE_2D1084	36	2.45 kB	fe80::250:56ff:fe82:72c3 00:50:56:82:72:c3	2024/01/19 15:45:14	2024/01/19 15:46:16	No
DNS		DEVICE_3C5E53ED	36	2.45 kB	fe80::bace:f6ff:fe09:7d63 b8:ce:f6:09:7d:63	2024/01/19 15:45:17	2024/01/19 15:46:19	No
NTP		DEVICE_50671346	36	2.45 kB	fe80::250:56ff:fead:a1a 00:50:56:ad:0a:1a	2024/01/19 15:45:19	2024/01/19 15:46:11	No
ICMP		DEVICE_6587A542	36	2.45 kB	fe80::bace:f6ff:fe62:fc29 b8:ce:f6:62:fc:29	2024/01/19 15:45:17	2024/01/19 15:46:17	No
HTTPBF		DEVICE_37CE8C00	36	2.45 kB	fe80::250:56ff:fead:e86f 00:50:56:ad:e8:6f	2024/01/19 15:45:14	2024/01/19 15:46:15	No
Proxy,H		DEVICE_26FD510F	36	2.45 kB	fe80::250:56ff:fe9e:7a3d 00:50:56:9e:7a:3d	2024/01/19 15:45:16	2024/01/19 15:46:19	No
NFS								
Window								
sFlow								
IPFix								
Microso								
Multicas								
Microso								

0% 84 | Updated: 15:03:55

**To view connection pairs:**

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

Connection Pairs							
Total Count	Total Volume	Source Device	Source Address	Source Entry Time	Destination Device	Destination Address	Destina
6	552 B	DEVICE_7272204C	172.19.243.221 00:50:56:ad:de:59	2024/01/19 15:45:15	DEVICE_27753EAC	208.91.112.55 04:d5:90:fd:0b:d3	2024
6	552 B	DEVICE_485D3D65	172.19.235.228 00:50:56:ad:71:b9	2024/01/19 15:45:17	DEVICE_27753EAC	192.168.100.206 04:d5:90:fd:0b:d3	2024
5	643 B	DEVICE_555C4993	172.19.243.232 00:50:56:82:91:c8	2024/01/19 15:45:14	DEVICE_27753EAC	83.231.212.81 04:d5:90:fd:0b:d3	2024
4	368 B	DEVICE_1A5F448C	10.10.9 00:50:56:bf:37:9f	2024/01/19 15:45:15	DEVICE_7D933B98	208.91.112.55 00:50:56:ad:f3:67	2024

## Top URL/Domain

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

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

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

URL	Count
192.168.1.1	1
192.168.1.1	1
192.168.1.1	1
192.168.1.1	1
192.168.1.1	1
192.168.1.1	1
192.168.1.1	1
192.168.1.1	2

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

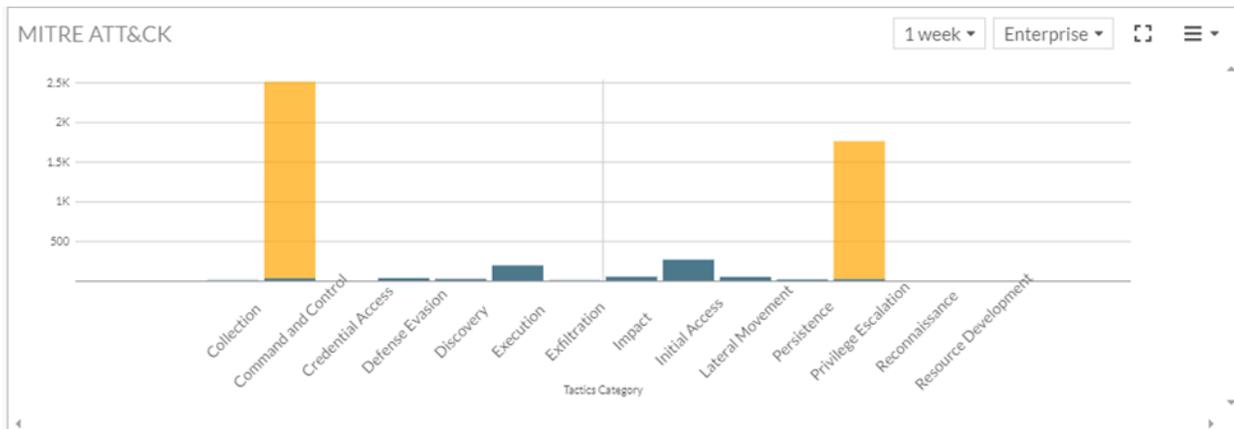
Domain	Count
192.168.1.1	1,350
192.168.1.1	99
192.168.1.1	22
192.168.1.1	11
192.168.1.1	9
192.168.1.1	8
192.168.1.1	6

## 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.

Enterprise Download Mitre Coverage 1 day

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discover
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Service Execution	Winlogon Helper DLL	Path Interception	Direct Volume Access	OS Credential Dumping	System Service Discovery
Gather Victim Network Information	Compromise Infrastructure	Replication Through Removable Media	Windows Management Instrumentation	Modify Existing Service	Boot or Logon Initialization Scripts	Rootkit	Network Sniffing	Application WMI Discovery
Gather Victim Org Information	Establish Accounts	External Remote Services	Scheduled Task/Job	Path Interception	New Service	Obfuscated Files or Information	Input Capture	Query Registry
Gather Victim Host Information	Compromise Accounts	Drive-by Compromise	Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Scheduled Task/Job	Masquerading	Brute Force	System Network Configuration Discovery
Search Open Websites/Domains	Develop Capabilities	Exploit Public-Facing Application	Graphical User Interface	Change Default File Association	Process Injection	Process Injection	Multi-Factor Authentication Interception	Remote System Discovery
Search Victim-Owned Websites	Obtain Capabilities	Supply Chain Compromise	Scripting	New Service	Exploitation for Privilege Escalation	Scripting	Hooking	System Owner, Discovery
<b>Legend</b> Select a type to view in highlight <input checked="" type="checkbox"/> Covered by Network Attack Detection <input checked="" type="checkbox"/> Covered by Botnet Detection <input checked="" type="checkbox"/> Covered by ANN Engine <input type="checkbox"/> Hide Revoked <input checked="" type="checkbox"/> Detections on primary or secondary ATT&CK ID <input type="checkbox"/> No Coverage								

## 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

ICS Download Mitre Coverage 1 day

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Re Funct
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Connection Enumeration	Default Credentials	Monitor Process State	Standard Application Layer Protocol	Activate Fir Update Mo
Exploit Public-Facing Application	Modify Controller Tasking	System Firmware	Exploitation for Privilege Escalation	Masquerading	Network Sniffing	Program Download	Automated Collection	Connection Proxy	Block Compr Message
External Remote Services	Graphical User Interface	Valid Accounts		Rootkit	Remote System Discovery	Valid Accounts	Data from Information Repositories	Commonly Used Port	Block Repo Message
Replication Through Removable Media	Native API	Project File Infection		Spoof Reporting Message	Wireless Sniffing	Exploitation of Remote Services	Adversary-in-the-Middle		Block Serial
Rogue Master	Scripting	Modify Program		Change Operating Mode	Remote System Information Discovery	Lateral Tool Transfer	Program Upload		Data Dest
Wireless Compromise	Change Operating Mode	Hardcoded Credentials		Indicator Removal on Host		Remote Services	Screen Capture		Denial of S
Supply Chain Compromise	User Execution					Hardcoded Credentials	Point & Tag Identification		Device Restart/Sf
Transient Cyber	Execution through API						Detect Operating Mode		Manipulat Image
<b>Legend</b> Select a type to view in highlight <input checked="" type="checkbox"/> Covered by ICS <input checked="" type="checkbox"/> Detections on primary or secondary ATT&CK ID <input type="checkbox"/> No Coverage									

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

Enterprise 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.

The screenshot displays the Network Insights matrix interface. At the top, there are controls for 'Enterprise' and 'Download Mitre Coverage'. A '1 day' filter is also visible. The matrix is organized into columns representing MITRE ATT&CK phases: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, and Discovery. Each column contains a list of techniques. A legend is open in the bottom-left corner, showing options to filter techniques by coverage: 'Covered by Network Attack Detection' (dark blue), 'Covered by Botnet Detection' (light blue), 'Covered by ANN Engine' (yellow), 'Hide Revoked' (grey), and 'No Coverage' (white). The legend also includes a checkbox for 'Detections on primary or secondary ATT&CK ID'. The matrix cells show techniques with colored backgrounds corresponding to the legend, indicating their detection status.

## Mitre ATT&CK detail

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

**Mitre ATT&CK Detail: T1586**

Information | NDR Anomaly | Malware Sample

Technique ID: T1586  
 Technique Name: Compromise Accounts  
 Tactics: resource-development  
 Platforms: PRE  
 Mitre Version: 1.2  
 Is Revoked?: False  
 URL: <https://attack.mitre.org/techniques/T1586>  
 Description: Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. [Establish Accounts] (<https://attack.mitre.org/techniques/T1585>)), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. A variety of methods exist for compromising accounts, such as gathering credentials via [Phishing for Information] (<https://attack.mitre.org/techniques/T1598>), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.(Citation: AnonHGBArv)

**Legend**  
 Select a type to view in highlight  
 Covered by Network Attack Detection  
 Covered by Botnet Detection  
 Covered by ANN Engine  
 Hide Revoked  
 Detections on primary or secondary ATT&CK ID  
 No Coverage

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

**Mitre ATT&CK Detail: T1190**

Information | NDR Anomaly | Malware Sample

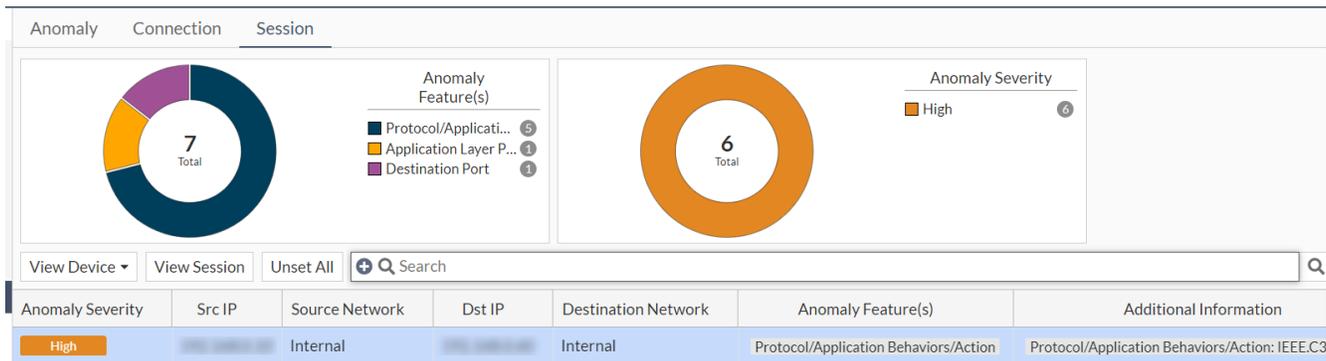
Timestamp	MITRE Technique	Session ID	Anomaly Type	Source Address	Source Network
2024/07/03 14:28:39	T1190 T1210	10960414	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 14:28:39	T1190 T1210	10960403	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 14:20:28	T1190 T1210	10948896	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 14:20:28	T1190 T1210	10948895	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 14:20:28	T1190 T1210	10948854	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 04:00:10	T1190 T1210	10593209	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 04:00:10	T1190 T1210	10593328	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 04:00:10	T1190 T1210	10593300	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 04:00:10	T1190 T1210	10593276	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 01:52:39	T1190 T1210	10479515	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 01:52:39	T1190 T1210	10479514	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 01:52:39	T1190 T1210	10479509	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/03 01:52:39	T1190 T1210	10479506	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/02 22:38:34	T1190 T1210	10025484	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/02 22:38:34	T1190 T1210	10025478	Network Attack/Intrusion	172.19.243.113	Internal
2024/07/02 16:05:23	T1190 T1203	10127528	Network Attack/Intrusion	172.19.233.111	Internal
2024/07/02 16:05:23	T1190 T1203	10127525	Network Attack/Intrusion	172.19.233.111	Internal
2024/07/02 16:05:23	T1190 T1203	10127525	Network Attack/Intrusion	172.19.233.111	Internal
2024/07/02 16:05:23	T1190 T1203	10127524	Network Attack/Intrusion	172.19.233.111	Internal

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

Date	MITRE Technique	MD5	File Type	Detection Name	Device
2024/07/09 15:45:04	T1055	517EC330222CD69C8338880DF84A...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:58:26	T1055	49BFEE117E5190F0440B50EA55913...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:41:02	T1055	C5D39A1F82B001697889AA713A48F...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:30:47	T1055	D4689496D8C5889134D63D81CF44E...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:25:42	T1055	C5D39A1F82B001697889AA713A48F...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:19:35	T1055	01A392B3E92226B00C83DC0F249BA3...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:18:24	T1055	C68880D56903FE652B88ED47279...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:06:57	T1055	8337523E003CCE190ED90810EB39...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:06:06	T1055	83C2A7689FDA52A88CD4F895E96C2...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:05:53	T1055	62745F61BD46AA7047EF17088802...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:05:15	T1055	870583C1558275C40499C9846FCA6...	PE	W32/Agent.CP!tr	Snif
2024/07/09 14:03:05	T1055	C5D39A1F82B001697889AA713A48F...	PE	W32/Agent.CP!tr	Snif
2024/07/09 13:55:16	T1055	442C0D0F97A5D0EEB5C6808E4F48E...	PE	W32/Agent.CP!tr	Snif
2024/07/09 13:54:15	T1055	48E8846C252ECDDCA9738C570780E...	PE	W32/Agent.CP!tr	Snif
2024/07/09 13:54:03	T1055	23B0941AB4E4C1CF2B0727548E1E...	PE	W32/Agent.CP!tr	Snif
2024/07/09 13:52:55	T1055	EE6C91E37C02B81DAEF78979AD748...	PE	W32/Agent.CP!tr	Snif
2024/07/09 13:51:35	T1055	7EC1A888C719441B3EAB4E2C1BD0F...	PE	W32/Agent.CP!tr	Snif
2024/07/09 13:51:06	T1055	568AB76F22C12F03E754667F3D8E...	PE	W32/Agent.CP!tr	Snif
2024/07/09 13:42:30	T1055	23E8457F784C28E8428DC28C7755B...	PE	W32/Agent.CP!tr	Snif

## ML Discovery (- Center - Standalone)

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



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

Column	Description
<b>Latest Timestamp</b>	The date the record was updated.
<b>Anomaly Features</b>	The feature or feature combinations that caused the anomaly.
<b>Additional Information</b>	The abnormal feature value(s).
<b>Anomaly Severity</b>	The anomaly severity ( <i>Not Anomaly, Info, Low, Medium, High or Critical</i> ).

Column	Description
<b>Count (Historic)</b>	The total number of times the anomaly was observed.
<b>Count (Past week)</b>	The total number of times the anomaly was observed during the past week .
<b>First Timestamp</b>	The timestamp for the first time the anomaly was detected.
<b>Current Feedback Status</b>	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 145](#).

## 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:

<b>General</b>	<ul style="list-style-type: none"> <li>• Session ID</li> <li>• Start Time</li> <li>• End Time</li> <li>• Traffic Volume</li> <li>• VLAN ID</li> <li>• Port ID</li> </ul>
<b>Anomaly</b>	<ul style="list-style-type: none"> <li>• Anomaly Type</li> <li>• Severity</li> </ul>
<b>Source Device</b>	<ul style="list-style-type: none"> <li>• Source IP</li> <li>• Source Port</li> <li>• Source MAC</li> <li>• Source Packet Size</li> <li>• Source Country</li> <li>• Source Device Model</li> <li>• Source OS</li> <li>• Source Device Category</li> <li>• Source Device Sub Category</li> </ul>
<b>Destination Device</b>	<ul style="list-style-type: none"> <li>• Destination IP</li> <li>• Destination Port</li> <li>• Destination MAC</li> <li>• Destination Packet Size</li> <li>• Destination Country</li> <li>• Destination Device Model</li> <li>• Destination OS</li> </ul>

- 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:

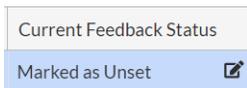
1. Go to *Network Insights > ML Discovery > Session* tab.
2. Hover over the column headings and then click the *Configure Table* icon.



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
<b>Mark as Anomaly</b>	Select this option to mark an entry as an anomaly. This option can be used to undo the <i>Mark as Not Anomaly</i> option. Note that this option does not affect the baseline training.
<b>Mark as Not Anomaly</b>	Select this option to exclude the same detection(s) in the future. This typically takes 5 - 10 minutes depending on the network traffic. Note that this option does not retrain the ML Database. For more information about retraining the database, see <a href="#">ML Configuration &gt; Retrain database</a> .
<b>Mark as unset</b>	This is the default status for any ML anomalies detected. Select this option to unset your feedback. Note that this has the same effect as "Mark as Anomaly".



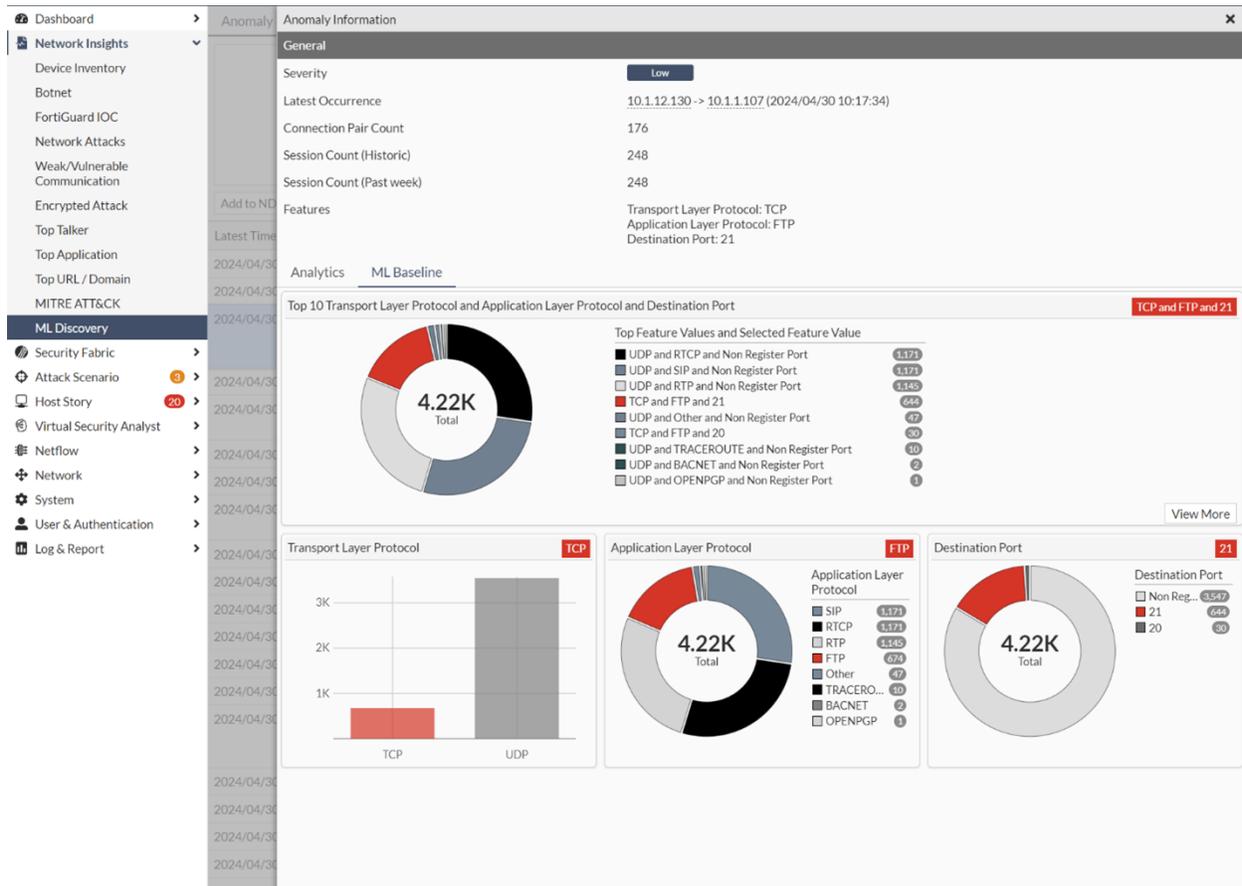
When multiple sessions of the same Source Address share the same value in the Anomaly Feature(s) column, you will only need to add feedback once to apply the feedback to all of the sessions.

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

## ML Baseline information

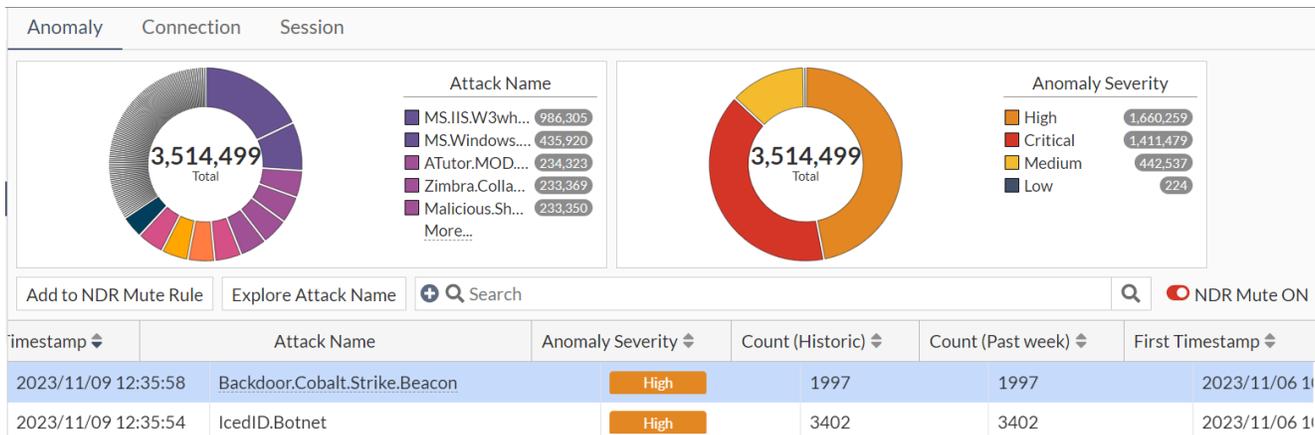
To view the ML Baseline information:

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



## Anomaly tab

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



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

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

**To view the sessions for a selected condition:**

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

From the *Session Log* pane, you have the option of viewing the source and destination device and viewing the sessions. For more information, see [Session tab on page 71](#).

## Anomaly Information

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

**General tab**

The *General* tab displays the following information:

<b>General</b>	<ul style="list-style-type: none"> <li>• Anomaly Type</li> <li>• Severity</li> </ul>
----------------	--

	<ul style="list-style-type: none"> <li>Reason</li> </ul>
<b>Additional Information</b>	<ul style="list-style-type: none"> <li>HTTP Version</li> <li>HTTP Response Code</li> <li>HTTP Server Name</li> <li>HTTP URL</li> <li>Malicious Behavior</li> </ul>
<b>Last Anomaly Occurrence</b>	<ul style="list-style-type: none"> <li>Latest Occurrence</li> <li>Count( Past Week)</li> <li>Count( Historic)</li> <li>Latest Source IP</li> <li>Latest Source Port</li> <li>Latest Source MAC</li> <li>Latest Source Packet Size</li> <li>Latest Source Country</li> <li>Latest Source Device Model</li> <li>Latest Source OS</li> <li>Latest Source Device Category</li> <li>Latest Source Device Sub Category</li> <li>Latest Destination IP</li> <li>Latest Destination Port</li> <li>Latest Destination MAC</li> <li>Latest Destination Packet Size</li> <li>Latest Destination Country</li> <li>Latest Destination Device Model</li> <li>Latest Destination OS</li> <li>Latest Destination Device Category</li> <li>Latest Destination Device Sub Category</li> </ul>

## Analytic tab

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

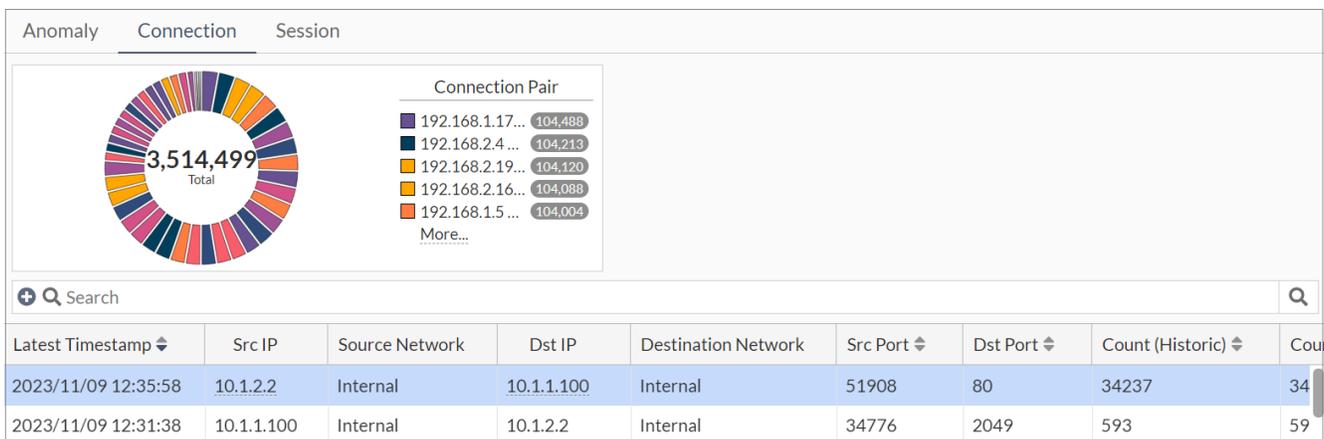
<b>Src IP</b>	The source IP. Hover over the record to view the view the <i>IP Address</i> , <i>Country</i> and <i>Related Service</i> .
<b>Source Network</b>	The source network. You can use this column to filter IP addresses based on the category of the IP, such as <i>Internal</i> , <i>External</i> (public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

<b>Count (Historic)</b>	The total number of times the anomaly was observed.
<b>Count (Past week)</b>	The total number of times the anomaly was observed during the past week .

## Connection tab

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



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

Column	Definition
<b>Latest Timestamp</b>	The date the record was updated.
<b>Src IP</b>	The source IP.
<b>Source Network</b>	The source network. You can use this column to filter IP addresses based on the category of the IP, such as <i>Internal</i> , <i>External</i> (public addresses), <i>Broadcast</i> , <i>Multicast address</i> , <i>Loopback</i> , <i>Reserved Address</i> and <i>Link-local Address</i> . You can filter for both IPv4 and IPv6 Addresses.
<b>Dst IP</b>	The destination IP.
<b>Destination Network</b>	The destination network. You can use this column to filter IP addresses based on the category of the IP, such as <i>Internal</i> , <i>External</i> (public addresses), <i>Broadcast</i> , <i>Multicast address</i> , <i>Loopback</i> , <i>Reserved Address</i> and <i>Link-local Address</i> . You can filter for both IPv4 and IPv6 Addresses.

Column	Definition
Src Port	The source port.
Dst Port	The destination port.
Count (Historic)	The total number of times the anomaly was observed.
Count (Past week)	The total number of times the anomaly was observed during the past week .
First Event Timestamp	The timestamp for the first time the anomaly event was detected.

#### To view the sessions for a selected condition:

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

From the *Session Log* pane, you have the option of viewing the source and destination device and viewing the sessions. For more information, see [Session tab on page 71](#).

## Session Information

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

### General tab

The *General* tab displays the following information:

<b>General</b>	<ul style="list-style-type: none"> <li>• Session ID</li> <li>• Start Time</li> <li>• End Time</li> <li>• Traffic Volume</li> <li>• VLAN ID</li> <li>• Port ID</li> </ul>
<b>Anomaly</b>	<ul style="list-style-type: none"> <li>• Anomaly Type</li> <li>• Severity</li> <li>• Reason</li> </ul>
<b>Additional Information</b>	<ul style="list-style-type: none"> <li>• HTTP Version</li> <li>• HTTP Response Code</li> <li>• HTTP Server Name</li> <li>• HTTP URL</li> <li>• Malicious Behavior</li> </ul>
<b>Source Device</b>	<ul style="list-style-type: none"> <li>• Source IP</li> <li>• Source Port</li> </ul>

- 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

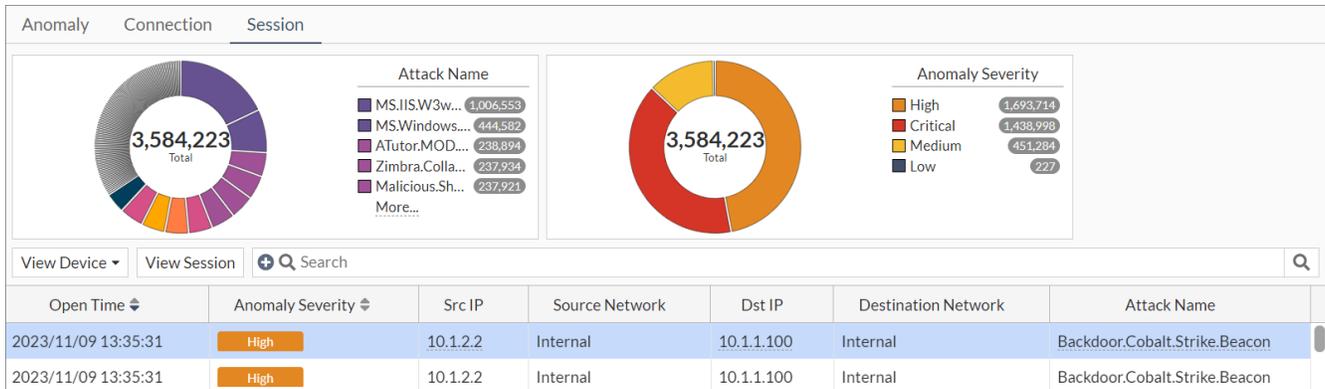
## Analytic tab

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

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

## Session tab

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



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

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

## Session Information

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

<b>General</b>	<ul style="list-style-type: none"> <li>• Session ID</li> <li>• Start Time</li> <li>• End Time</li> <li>• Traffic Volume</li> <li>• VLAN ID</li> <li>• Port ID</li> </ul>
<b>Anomaly</b>	<ul style="list-style-type: none"> <li>• Anomaly Type</li> <li>• Severity</li> </ul>

	<ul style="list-style-type: none"><li>• Reason</li></ul>
<b>Additional Information</b>	<ul style="list-style-type: none"><li>• HTTP Version</li><li>• HTTP Response Code</li><li>• HTTP Server Name</li><li>• HTTP URL</li><li>• Malicious Behavior</li></ul>
<b>Source Device</b>	<ul style="list-style-type: none"><li>• Source IP</li><li>• Source Port</li><li>• Source MAC</li><li>• Source Packet Size</li><li>• Source Country</li><li>• Source Device Model</li><li>• Source OS</li><li>• Source Device Category</li><li>• Source Device Sub Category</li></ul>
<b>Destination Device</b>	<ul style="list-style-type: none"><li>• Destination IP</li><li>• Destination Port</li><li>• Destination MAC</li><li>• Destination Packet Size</li><li>• Destination Country</li><li>• Destination Device Model</li><li>• Destination OS</li><li>• Destination Device Category</li><li>• Destination Device Sub Category</li></ul>

## View source and destination devices

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

### To view the source and destination devices:

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

← Back **Device 113**
Last 24 Hours --Action-- Go

Information Malware Host Story

**DEVICE\_DDD78370**

Update Device Identifier

Host IP	Mac Address	Discovery Date	Category
		2023/11/06 08:45:12	N/A
Sub Category	Operating System	Vendor	Model
N/A	N/A	VMware	N/A
Confidence Level <span style="background-color: #0070c0; color: white; padding: 2px;">High: 254/255</span>			

Critical Risk Anomaly	<b>518086</b>	Medium Risk Anomaly	<b>164.61K</b>
High Risk Anomaly	<b>1.04M</b>	Low Risk Anomaly	<b>71</b>

Top Application Top Service Top Protocol Top Neighbor Top Geolocation

Lateral Connection  External Service  Multiple IP(s)

Anomaly Activity Traffic Top Neighbors External Service GeoLocation ML Discovery

No ML training has finished yet

Date	Severity	Anomaly Type	Description	Source Address	Source Network	Destination Address
------	----------	--------------	-------------	----------------	----------------	---------------------

## View sessions

To view the session page:

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



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

The *Session* page contains the following information:

## Anomaly

**Activity**  
Web Client

**Application**  
HTTP.BROWSER

**Vendor**  
Other

**High Anomaly**

## Session Information

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

## Device Information

Device Information			
 Internal	Device Type	N/A	 Internal
	Devie Model	N/A	
	MAC Address	5a:01:0a:03:0a:39	
	Vendor	N/A	
	OS	N/A	
	Category	N/A	
	Sub Category	N/A	
	IP	10.3.10.57	
	Port	51255	
Packet Size	117		
↔			
	Device Type	N/A	
	Device Model	N/A	
	MAC Address	5a:01:0a:03:00:02	
	Vendor	N/A	
	OS	N/A	
	Category	N/A	
	Sub Category	N/A	
	IP	10.3.0.2	
	Port	80	
	Packet Size	415448	

## Activity

Activity	
2 minutes ago	Connected to 10.3.0.2/9b30e4de385251284139f576c2e3635f via HTTP

## ML Discovery

ML Discovery
No ML Feature Found

## Detection Information

Detection Information			
<input type="text" value="Search"/>			
Date ↕	Severity ↕	Anomaly Type ↕	Description ↕
2023/11/10 13:16:04	High	Weak Cipher/Vulnerable Protocol	Weak version of HTTP Protocol detected

## Mitre Attack

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

Mitre Attack							
Show All ▾							
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	
Gather Victim Network Information	Compromise Infrastructure	Replication Through Removable Media	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	
Gather Victim Org Information	Establish Accounts	External Remote Services	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job		Binary Padding
Gather Victim Host Information	Compromise Accounts	Drive-by Compromise	Graphical User Interface	Hypervisor	Process Injection		Software Packing
Search Open Websites/Domains	Develop Capabilities	Exploit Public-Facing Application	Scripting	Valid Accounts	Exploitation for Privilege Escalation	Obfuscated Files or Information	Steganography
Search Victim-Owned Websites	Obtain Capabilities	Supply Chain Compromise	Software Deployment Tools	Account Manipulation	Valid Accounts		Compile After Delivery
Active Scanning	Stage Capabilities	Trusted Relationship	Native API	Redundant Access	Access Token Manipulation		Indicator Removal from Tools
Search Open Technical Databases	Acquire Access	Hardware Additions	Shared Modules	External Remote Services	Domain Policy Modification		HTML Smuggling
Search Closed Sources		Phishing	Source	Create Account	Create or Modify System Process	Masquerading	Dynamic API Resolution
Phishing for Information			Component Object Model and Distributed COM	Office Application Startup	Event Triggered	Process Injection	Stripped Payloads
			Exploitation for Client Execution	Browser Extensions		Scripting	Embedded Payloads
				BITS Jobs		Indicator Removal	Command Obfuscation
						Valid Accounts	Fileless Storage

## Malware Attack Scenario (formerly 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.

Severity	Scenario Types	Scenario Types: Total Event Counts
Low	5	19421
Low	Cryptojacking	1057
Low	Application	1092
Low	Web Shell	16744
Low	SEP	0
Low	Phishing	528
Medium	4	132048
Medium	Sophisticated	0
Medium	Scenario Heuristic	0
Medium	DoS	0
Medium	Generic Trojan	132048
High	6	111359
High	Data Leak	525
High	Exploit	30487
High	Banking Trojan	80347
High	Backdoor	0

## Scenario types

FortiNDR can detect the following attack scenarios:

Scenario	Severity	Description
<b>Cryptojacking</b>	Low	Cryptojacking is a type of cybercrime where a malicious actor uses a victim's computing power to generate cryptocurrency.
<b>Application</b>	Low	A broad category of software that might download and install

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

Scenario	Severity	Description
		possible inside the victim's networks.
<b>Industroyer</b>	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.
<b>Worm Activity</b>	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.

The screenshot displays the FortiNDR-VM interface. At the top, a table lists various detections with columns for Discovery Date, Victim (Infected Host) IP, Malware family, Device Type, and Event Count. Below the table, the 'Attack Timeline at Host: 10.10.10.56' is shown, featuring three stages: Downloader, Infostealer, and Worm. Each stage includes a detection name, a timer, and buttons for 'HTML', 'Download', and 'Virus'. A popup window for 'W32/Bundpil.AA!tr' is open, showing details such as Discover Date, MD5, Remote IP, and Protocol.

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



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 Observed (formerly Host Story)

*Malware Observed* organizes malware attacks by host IP address while *Attack Scenario* organizes malware attacks by attack type. The *Malware Observed* 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.

Malware Last Observed	IP Address	Critical Risk Incidents	High Risk Incidents	Medium Risk Incidents	Low Risk Incidents	Total Incidents
2024/07/12 20:51:05		14	749	10770	3877	15410



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

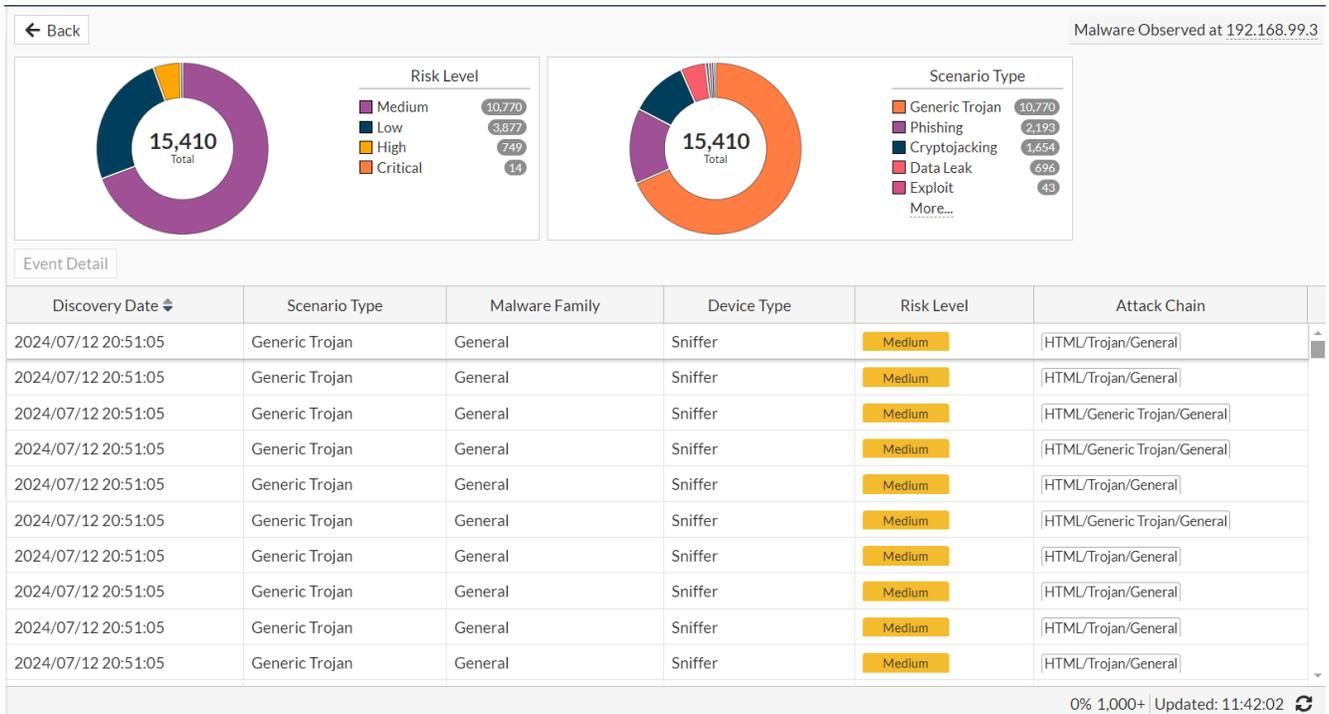
The *Malware Observed* summary page shows the following information:

<b>Malware Last Observed</b>	The date and time the malware was last observed.
<b>IP Address</b>	The IP address of the infected device. Hover over the address to view the <i>Device</i> , <i>MAC Address</i> , <i>Hardware</i> , <i>OS</i> and the <i>View Device Detail</i> button
<b>Critical Risk Incidents</b>	The number of critical risk Incidents
<b>High Risk Incidents</b>	The number of high risk Incidents
<b>Medium Risk Incidents</b>	The number of medium risk Incidents
<b>Low Risk Incidents</b>	The number of low risk Incidents
<b>Total Incidents</b>	The total number of incidents.

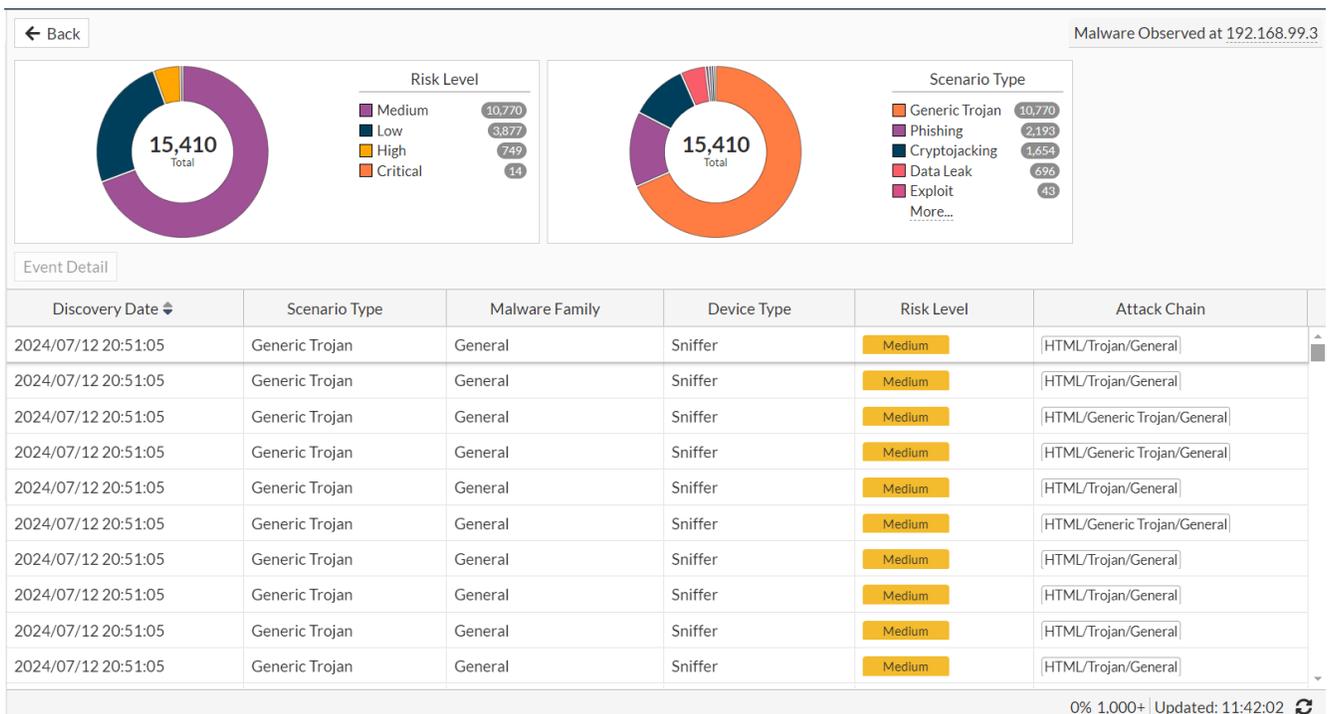
### Malware Observed summary page

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:

<b>Discovery Date</b>	The date the malware was discovered.
-----------------------	--------------------------------------

<b>Scenario Type</b>	The scenario type.
<b>Malware Family</b>	The malware family.
<b>Device Type</b>	The device type.
<b>Risk Level</b>	The risk level.
<b>Attack Chain</b>	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.

← Back

15,410  
Total

Risk Level

- Medium 10,770
- Low 3,577
- High 749
- Critical 14

15,410  
Total

Event Detail

Discovery Date	Scenario Type	Malware Family	Device Type
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer
2024/07/12 20:33:04	Exploit	General	Sniffer
2024/07/12 20:33:04	Generic Trojan	General	Sniffer

Details ✕

Date 2024/07/12 20:33:04

Event Type Generic Trojan

Attack Chain

**HTML/Dropper/General** [🔗](#)

MD5 4f9411aeeb2298c8ae4cb505a46511b4

Entry Date 2024/07/12 20:20:26

OK

# 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, Malware and Netflow 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.

## Tag management system

FortiNDR tags significant attributes with information from any incoming files and sessions. At this time, there are approximately 450 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*.

The screenshot shows the FortiNDR-3600G-Tag management interface. The left sidebar contains navigation options: Dashboard, Network Insights, Investigation (selected), Global Query, Virtual Security Analyst, Netflow, Network, System, User & Authentication, and Log & Report. The main area displays a SQL query:

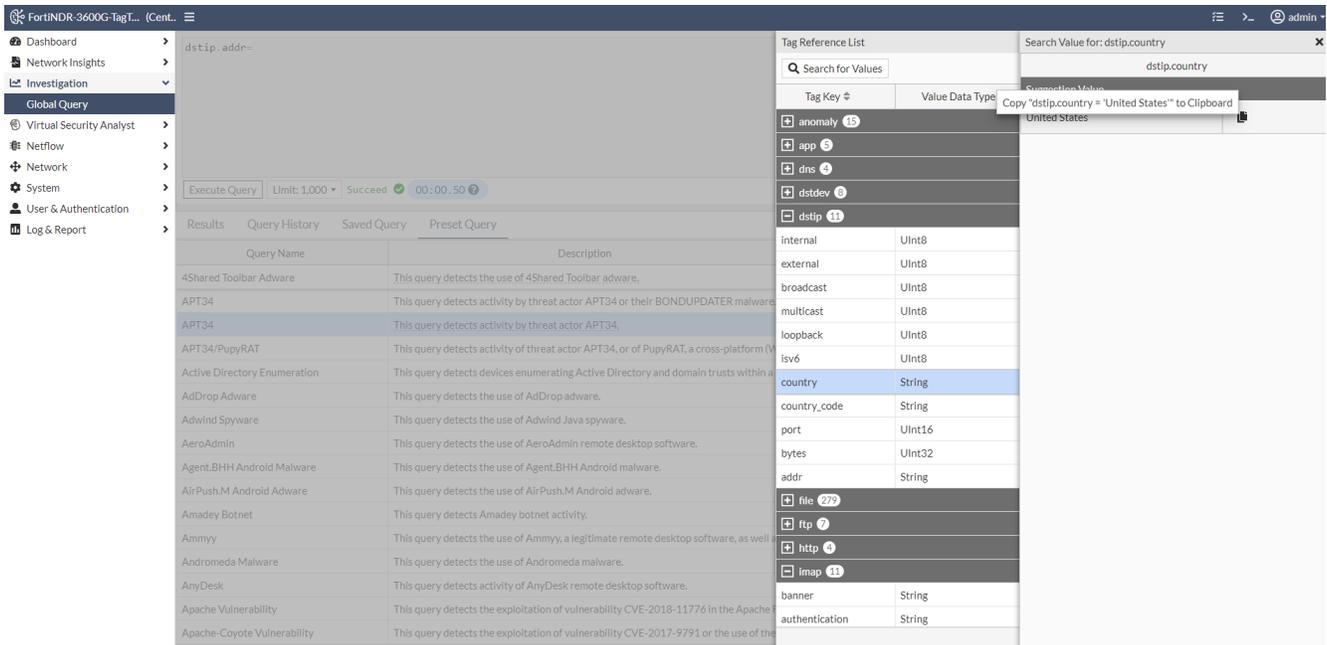
```
SELECT
  srcip.addr AS source_ip,
  dstip.addr AS destination_ip
FROM
  tag_mgmt.idx_tag_wide
GROUP BY
  srcip.addr,
  dstip.addr
```

Below the query, there are buttons for "Execute Query", "Limit: 1,000", "Succeed" (with a green checkmark), and "00:00.50". There are also buttons for "Save Query", "Clear Input", and "Tag Reference". The results are displayed in a table with columns "source\_ip" and "destination\_ip".

source_ip	destination_ip
10.10.10.105	10.10.10.102
192.168.1.111	192.168.1.255
192.168.1.101	192.168.1.102
172.22.5.116	172.22.5.22
10.1.1.1	10.2.2.2
17.1.2.2	17.1.1.100
192.168.1.100	192.168.2.101
10.0.0.9	10.0.0.3
10.6.6.6	10.1.1.1
192.168.1.110	172.16.100.100
10.1.1.1	10.4.4.4

## 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 or file is displayed. To use the key and value as a search clause, click the *Copy* button next to the value.

← Back Sample 4 (Sensor: FortiNDR-VM (6a9d))

VSA Verdict: **No Risk**

✓ CLEAN

Related Tags

file.size file.type file.dstip file.srcip
file.srcport file.dstport file.md5 file.sha1
file.sha256 file.url

Sample Information		
Submitted Date	2024/03/06 11:10:24	Last An
File Type	HTML	File
URL	http://newbucketname.s3.amazonaws.com/amazons3_50000bytes.docx	

Name	file.sha1	
Data Type	String	
Description	The computed file SHA1 hash.	
Value	f21740fe3c546ab51c7d08b92e5816d1e200b0b0	7FAFB445BBDD65

Detection Name	N/A	Vir Far
----------------	-----	---------

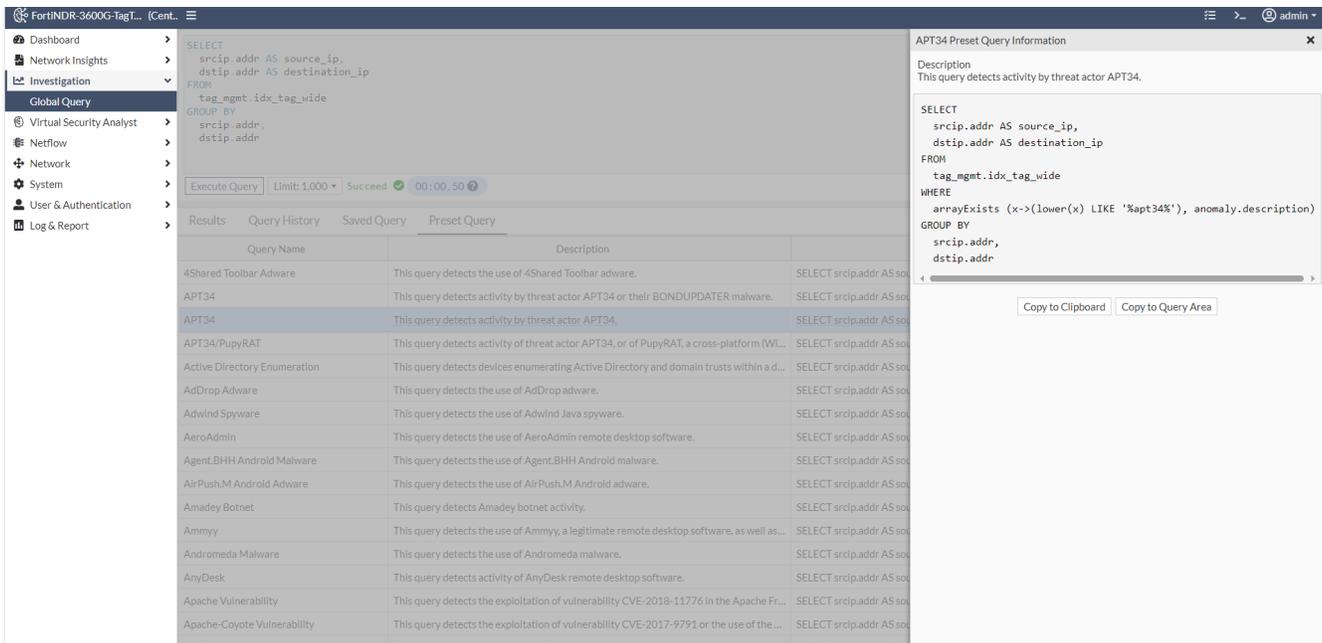
Source Device	
Device Type	Sniffer

Network	
Attacker	172.3.1.101: 80 (HTTP)
	Victim

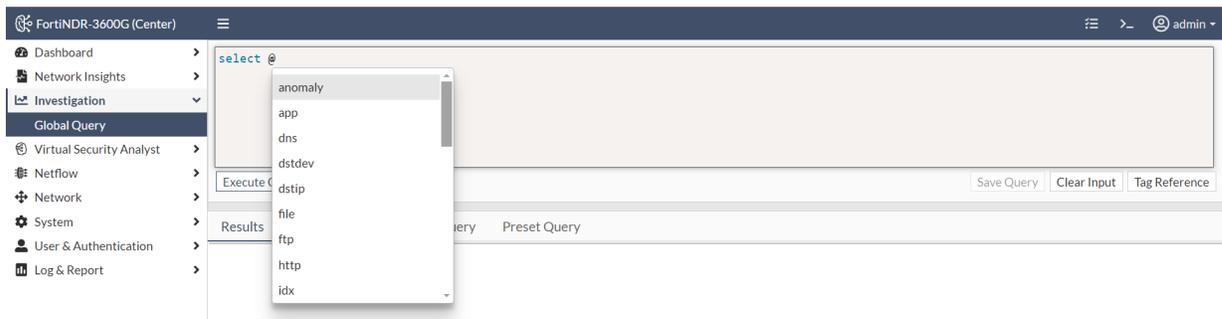
## Global query

The *Global Query* page is an easy-to-use SQL query interface to investigate suspicious activity on your network. Use the *Tag* selection dropdown or the *Tag Reference* tool to start a query. To refine your search, add clauses with specific values or a range of values. You can save queries as templates to use later, or re-execute a previous query. Additionally, the *Preset Query* tab contains 300 query templates to quickly launch an investigation.

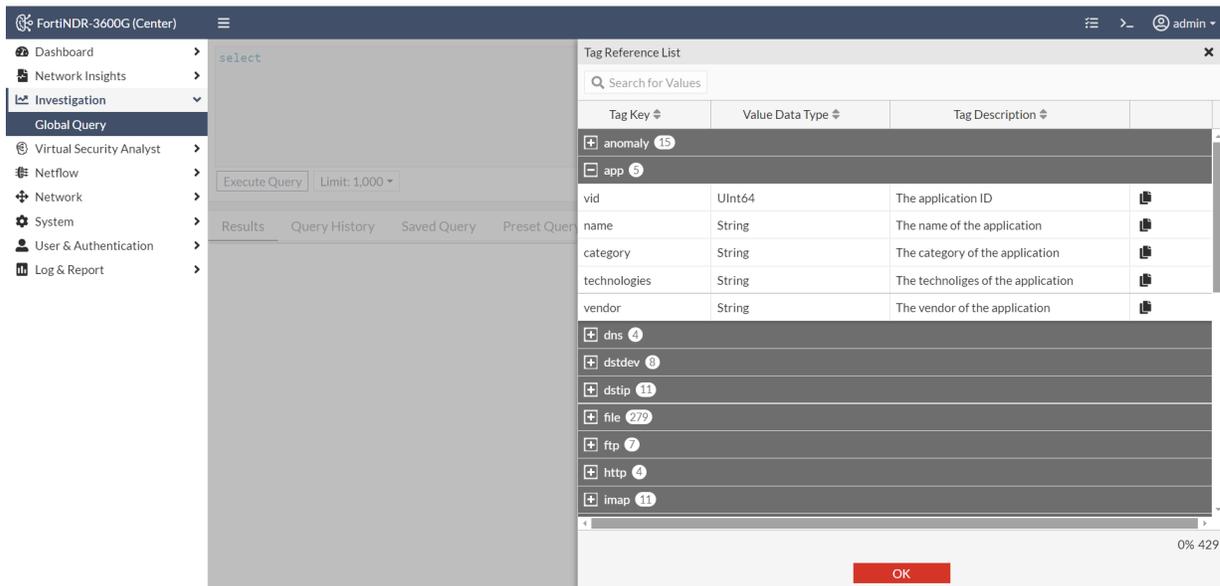


**To start an investigation:**

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 94](#)
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*.

## Sample queries

- [View all the anomaly descriptions with medium severity \(value = 1\) on page 90](#)
- [List all countries communicated this week on page 90](#)
- [List all external communication on page 91](#)
- [List attributes of all malicious files transferred via SMB Session on page 91](#)
- [Identify connection pairs based on an URI on page 91](#)
- [Applications running on non standard port for HTTP on page 92](#)
- [Internal host retrieves archive file pretending to be image on page 92](#)
- [Find internal RDP servers exposed to outside on page 92](#)
- [Detect EXE files transferred over SMB protocol from an external host on page 92](#)
- [Detect FTP data exfiltration on page 93](#)
- [Detect web traffic to an external IP check or geolocation service using non-browser mechanisms on page 93](#)

### View all the anomaly descriptions with medium severity (value = 1)

```
SELECT
    anomaly.description
FROM
    tag_mgmt.idx_tag_wide
WHERE
    arrayExists (x->x=2, anomaly.severity)=1
```

### List all countries communicated this week

```
SELECT
    dstip.country
FROM
    tag_mgmt.idx_tag_wide
WHERE
    dstip.country!=''
    AND dstip.country!='Reserved'
    AND tag_time>now()-INTERVAL '1 week'
GROUP BY
    dstip.country
```

## List all external communication

```
SELECT
  srcip.addr,
  srcip.external,
  dstip.addr,
  dstip.external
FROM
  tag_mgmt.idx_tag_wide
WHERE
  srcip.external=1
  OR dstip.external=1
```

## List attributes of all malicious files transfered via SMB Session



When \* is used in the query, all the attributes under the category are not shown in the result by default. You will need to select them individually in the column setting.

The screenshot shows the FortiNDR-3600G (Center) interface. On the left, there is a navigation menu with options like Dashboard, Network Insights, Investigation, Global Query, Virtual Security Analyst, Netflow, Network, System, User & Authentication, and Log & Report. The main area displays a 'Best Fit Columns' dialog box with a 'Select Columns' list. The list includes various file-related attributes such as file.create\_abnormal\_filename, file.create\_directory, file.create\_file, file.create\_file\_in\_recycle\_directory, file.create\_file\_in\_win\_directory, file.create\_file\_in\_win\_folder, file.create\_known\_dll, file.create\_memory\_object, file.create\_process, file.create\_registry\_key, file.create\_registry\_service, file.create\_remote\_thread, file.create\_user\_mode\_process, file.dean\_pack\_content, file.delete\_after\_execution, file.delete\_directory, file.delete\_file, file.delete\_registry\_key, file.delete\_registry\_keyvalue, file.delete\_system\_file, file.detection, file.detection\_type, file.device\_loctl, file.disable\_antivirus, file.download\_executable\_file, file.download\_file\_to\_exe, file.drop\_autorun\_file, file.drop\_hidden\_file, and file.dstip. The main window shows a table with columns for Sensor and ID, displaying a list of results with IDs ranging from 10492 to 10506.

```
SELECT
  file.*
FROM
  tag_mgmt.idx_tag_wide
WHERE
  smb.version>0
```

## Identify connection pairs based on an URI

```
SELECT srcip.addr, dstip.addr FROM tag_mgmt.idx_tag_wide WHERE has (uri.host, '{URI}')
GROUP BY srcip.addr, dstip.addr
```

## Applications running on non standard port for HTTP

```
SELECT
    srcip.addr AS source_ip,
    dstip.addr AS destination_ip
FROM tag_mgmt.idx_tag_wide
WHERE (srcip.port NOT IN (80,8080,8443, 443) OR dstip.port NOT IN (80, 8080, 8443, 443))
    AND ((http.version > 0) OR (protocol.L7 = 'HTTP'))
GROUP BY
    srcip.addr,
    dstip.addr
```

## Internal host retrieves archive file pretending to be image

```
SELECT
    srcip.addr AS source_ip,
    dstip.addr AS destination_ip
FROM tag_mgmt.idx_tag_wide
WHERE
    (file.url LIKE '%.jpeg' OR file.url LIKE '%.jpg' OR
    file.url LIKE '%.gif' OR file.url LIKE '%.tiff' OR
    file.url LIKE '%.png' OR file.url LIKE '%.bmp') AND
    (file.type IN ('ZIP', 'TAR', 'XZ', 'GZIP', 'BZIP2', 'BZIP', 'RAR', '7Z', 'LZH',
'LZW', 'CAB', 'ARJ'))
GROUP BY
    srcip.addr,
    dstip.addr;
```

## Find internal RDP servers exposed to outside

```
SELECT
    srcip.addr AS source_ip,
    dstip.addr AS destination_ip
FROM tag_mgmt.idx_tag_wide
WHERE srcip.external = 1 AND
    dstip.internal = 1 AND
    protocol.L7 = 'RDP'
GROUP BY
    srcip.addr,
    dstip.addr;
```

## Detect EXE files transferred over SMB protocol from an external host

```
SELECT
    srcip.addr AS source_ip,
    dstip.addr AS destination_ip
FROM tag_mgmt.idx_tag_wide
WHERE
    (protocol.L7 = 'SMB') AND
```

```
(srcip.external = 1) AND
(file.type= 'PE' OR file.type='DLL')
GROUP BY
  srcip.addr,
  dstip.addr;
```

## Detect FTP data exfiltration

```
SELECT
  srcip.addr AS source_ip,
  dstip.addr AS destination_ip,
  SUM(srcip.bytes) AS sum_srcip_bytes
FROM tag_mgmt.idx_tag_wide
WHERE
  protocol.L7 = 'FTP' AND
  srcip.internal = 1 AND
  dstip.external = 1 AND
  arrayExists(x -> lower(x) LIKE '%retr%', ftp.args)
GROUP BY
  srcip.addr,
  dstip.addr
HAVING
  sum_srcip_bytes > {threshold};
```

## Detect web traffic to an external IP check or geolocation service using non-browser mechanisms

This is typically for network surveying after initial access.

```
SELECT
  srcip.addr AS source_ip,
  dstip.addr AS destination_ip
FROM tag_mgmt.idx_tag_wide
WHERE arrayExists(x -> (x IN ('ip-api.com', 'ipinfo.io', 'geoiptool.com',
  'whatismyipaddress.com', 'ipecho.net',
  'whatismyip.com', 'icanhazip.com',
  'checkip.amazonaws.com', 'ifconfig.co',
  'ipify.org', 'myexternalip.com',
  'wtfismyip.com', 'ip.seeip.org')), uri.host) AND
  lower(app.name) NOT IN ('http.browser', 'http.browser_chrome',
  'http.browser_ie', 'http.browser_firefox',
  'http.browser_edge', 'http.browser_safari',
  'http.browser_opera')
GROUP BY
  srcip.addr,
  dstip.addr;
```

## 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
  srcip.addr AS source_ip,
  dstip.addr AS destination_ip
FROM
  tag_mgmt.idx_tag_wide
GROUP BY
  srcip.addr,
  dstip.addr
HAVING
  destination_ip != ''

```

Execute Query

Limit: 1,000 ▾

Succeed 00:00.4 

Save Query

Clear Input

Tag Reference

Results

Query History

Saved Query

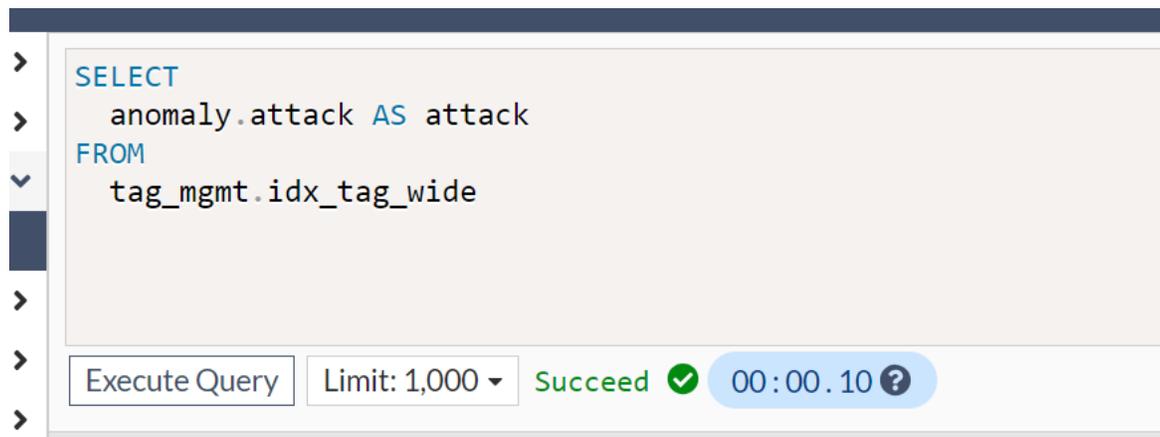
Preset Query

 Export ▾

source_ip	destination_ip
17.1.1.100	17.1.2.2
10.1.1.1	10.5.5.5
10.10.10.105	10.10.10.102
192.168.1.111	192.168.1.255
192.168.1.101	192.168.1.102
172.22.5.116	172.22.5.22
10.1.1.1	10.2.2.2
17.1.2.2	17.1.1.100
192.168.1.100	192.168.2.101
10.0.0.9	10.0.0.3
10.6.6.6	10.1.1.1
192.168.1.110	172.16.100.100
10.1.1.1	10.4.4.4
::1	::1

## SELECT clause

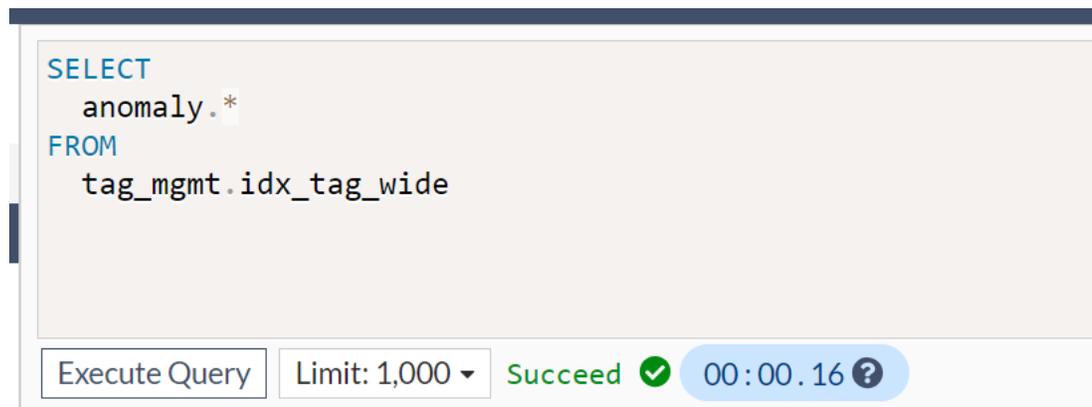
AS is supported for single column selection.



```
SELECT
  anomaly.attack AS attack
FROM
  tag_mgmt.idx_tag_wide
```

Execute Query    Limit: 1,000 ▾    Succeed ✓    00:00.10 ?

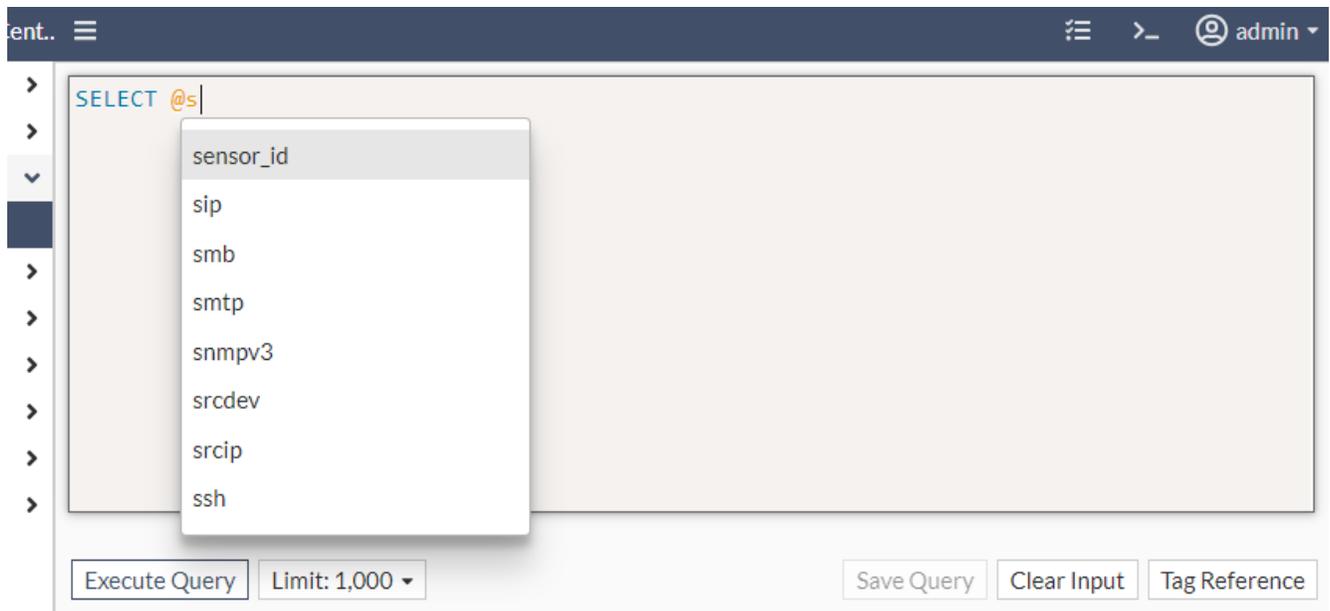
Use \* to select a range of columns under one tag category, (for example, srcip.\*).



```
SELECT
  anomaly.*
FROM
  tag_mgmt.idx_tag_wide
```

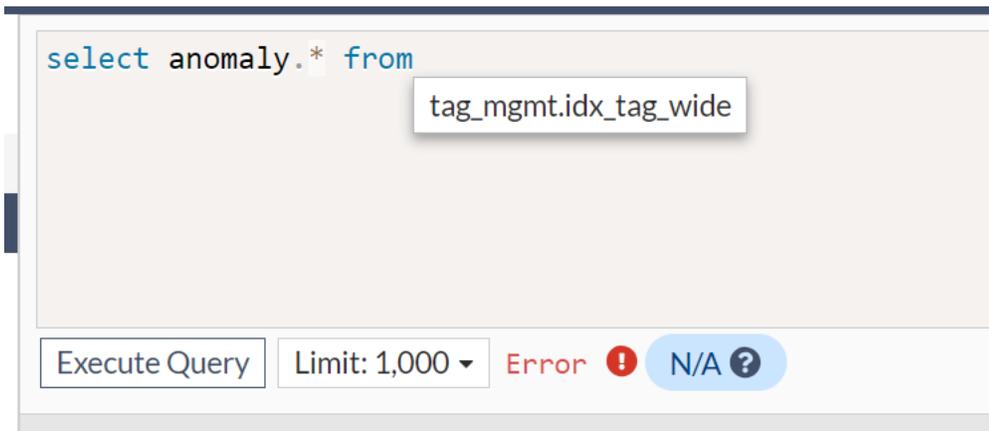
Execute Query    Limit: 1,000 ▾    Succeed ✓    00:00.16 ?

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_mgmt.idx_tag_wide` is supported.



## WHERE/HAVING clauses

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

## GROUP BY clause

`GROUP BY` is used to specify filters for the `ID` and `Sensor` columns:

- To group by `ID` column, use the `idx` and `tag_type` tags.
- To group by `Sensor` column, use the `sensor_id'` column.

# 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
<b>FortiGate tab</b>	The <i>FortiGate</i> tab displays the FortiGates sending files via OFTP (FortiSandbox field with TCP port 514) and via HTTPs (FOS 7.0.1 and higher). FortiNDR must authorize connections from FortiGate for OFTP and for inline blocking. Connect FortiNDR to the FortiGate Security Fabric to authorize the device via the Security Fabric protocol.
<b>Other Device tab</b>	The <i>Other Device</i> tab displays FortiSandbox submissions via the FortiNDR API such as FortiSandbox and FortiMail.

The *Device Input* page displays the following information:

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

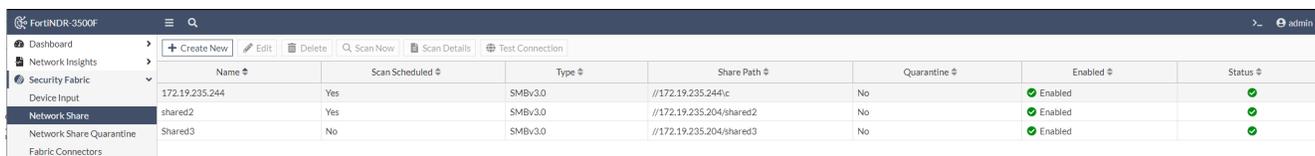
## Network Share

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:

<b>Name</b>	The Network Share profile name.
<b>Scan Scheduled</b>	Indicates scheduled scan is enabled/disabled.
<b>Type</b>	The Network Share protocol.
<b>Share Path</b>	The Network Share path.
<b>Quarantine</b>	Indicates if quarantine is enabled/disabled.
<b>Enabled</b>	Indicates the Network Share profile is enabled/disabled.
<b>Status</b>	The Network Share configuration status. See <a href="#">Testing connectivity</a> .



## 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.

<b>Status</b>	<i>Enable</i> or <i>Disable</i> . <i>Enable</i> is the default.
<b>Mount Type</b>	Select a Network Share protocol from the list. The following protocols are supported: <ul style="list-style-type: none"> <li>• SMBv1.0</li> <li>• SMBv2.0</li> <li>• SMBv2.1</li> <li>• SMBv3.0</li> <li>• NFSv2.0</li> <li>• NFSv3.0</li> <li>• NFS v4.0</li> </ul>
<b>Network Share Name</b>	Enter a name for the Network Share.
<b>Server IP</b>	Enter the IP address for the Network Share.

<b>Share Path</b>	Enter the path for the Network Share.
<b>Username</b>	Enter the username for the Network Share.
<b>Password</b>	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.

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

	<ul style="list-style-type: none"> <li>• Generic Attack</li> <li>• Generic Trojan</li> <li>• SEP</li> <li>• WebShell</li> </ul>
<b>Enable Quarantine of Others</b>	<p>Moves other unprocessed files to a designated quarantine location. File types that falls under this category includes:</p> <ul style="list-style-type: none"> <li>• Files with unsupported file type</li> <li>• Files with Over size Limit</li> <li>• Empty/Irregular files</li> </ul>
<b>Enable Copying or Moving clean files to sanitized location</b>	<p>Moves or copies clean files to a location specified in the <i>Network Share Quarantine</i> profile. See, <a href="#">Network Share Quarantine on page 103</a>.</p> <p>The <i>Moving</i> operation is only allowed for the quarantine location when <i>Keep Original File at Source Location</i> disabled.</p> <p>The <i>Copying</i> operation is only allowed for the quarantine location when <i>Keep Original File at Source Location</i> enabled.</p> <p>For information about combing Network Share and Quarantine profiles, see <a href="#">Network Share Quarantine on page 103 &gt; Combining network share and quarantine profiles</a>.</p>
<b>Create a copy of clean files for every scheduled scan at the sanitized location</b>	<p>When enabled, FortiNDR will create a new folder <i>&lt;Network Share Profile Name&gt;_&lt;Scan Task ID&gt;</i> in the sanitized location for each scheduled scan.</p> <p>When disabled, FortiNDR will overwrite the sanitized location with the clean files from the latest scan.</p>
<hr/>  <p>Enabling this option will increase the size of the Network Share location.</p> <hr/>	
<b>Create placeholder files for malicious/Suspicious/Other files at sanitized location</b>	<p>Adds a placeholder file in the sanitized location. The filename pattern of the placeholder file will be <i>&lt;filename&gt;.&lt;severity&gt;.txt</i>. This helps maintain the file structure of the original network in the share folder.</p>
<b>Enable Force Rescan</b>	<p>When enabled, FortiNDR will not use cache detection even if the files are previously scanned.</p>

6. Click *OK*.

## Testing connectivity

### To validate the Network Share configuration:

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.

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

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

## Scanning Zip files

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



FortiNDR does not process password-protected zip files.

## Network Share Quarantine

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

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

## Quarantined files

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

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

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

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

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

### Example:

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

## Creating a quarantine profile

To create a quarantine profile:

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

**Status**

Click to *Enable* or *Disable*.

<b>Quarantine Name</b>	Enter a name for the quarantine profile.
<b>Server IP</b>	Enter the IP address for the Network Share.
<b>Share Path</b>	Enter the path for the Network Share.
<b>Username</b>	Enter the username for the Network Share.
<b>Password</b>	Enter the password for the Network Share and then confirm the password.
<b>Confirm Password</b>	Re-enter the password.

Status  Enable  Disable

Mount Type

Quarantine Name  ?

Server IP  ?

Share Path  ?

Username

Password

Confirm Password

Keep Original File At Source Location

Description

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



Enabling *Keep Original File At Source Location* may affect the behavior of your Network Share profile. For information, see [Combining network share and quarantine profiles on page 106](#).

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
<i>Enabled</i>	Keeps the quarantine file in the source location.	<i>Enabled</i>	<ul style="list-style-type: none"> <li>Creates a copy of the quarantine file in the quarantine location and renames it <i>&lt;Network Share File ID&gt;</i>.</li> <li>Creates a metafile with the naming pattern <i>&lt;Network Share File ID&gt;.meta</i> for each quarantine file.</li> </ul>
<i>Disabled</i>	FortiNDR creates a placeholder file with <i>&lt;Filename&gt;.quarantined</i> in the original folder	<i>Enabled</i>	<ul style="list-style-type: none"> <li>Copies the quarantine file to the quarantine location and renames it <i>&lt;Network Share File ID&gt;</i>.</li> <li>Creates a metafile with the naming pattern <i>&lt;Network Share File ID&gt;.meta</i> for each quarantine file.</li> <li>If FortiNDR has enough permissions, it will delete the file in the source location.</li> </ul>



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

Keep original file at source location	Move/Copy clean files to sanitized location	Effect
<i>Enabled</i>	<i>Enabled</i>	<ul style="list-style-type: none"> <li>Cleans files in the source location.</li> <li>Copy the clean files to the Network</li> </ul>

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



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.

<b>Name</b>	The cloud storage profile name.
<b>Scan Scheduled</b>	Indicates scheduled scan is enabled/disabled.
<b>Type</b>	The cloud storage platform.
<b>Storage Path</b>	The URL of the cloud storage.
<b>Enabled</b>	Indicates the cloud storage profile is enabled/disabled.
<b>Status</b>	The cloud storage configuration status. See <a href="#">Testing connectivity on page 108</a> .

### 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.

<b>Status</b>	<i>Enable</i> or <i>Disable</i> . Enable is the default.
<b>Cloud Type</b>	Select a cloud storage platform from the list. The following platforms are supported: <ul style="list-style-type: none"> <li>• Amazon Web Service S3 Bucket</li> </ul>
<b>Cloud Storage Name</b>	Enter a name for the Cloud Storage.
<b>Bucket Name</b>	(AWS S3 Only) Enter the name of the Cloud Storage container.
<b>S3 Prefix</b>	(AWS S3 Only) Enter the common prefix of the keys to scan. Leave empty to scan the entire bucket.
<b>Access Key</b>	Enter the access key for the cloud storage.
<b>Secret Key</b>	Enter the secret key for the cloud storage.
<b>Enable Force Rescan</b>	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.

<b>Total</b>	The total number of files scanned.
<b>Start Time</b>	The date and time the scan started.
<b>End Time</b>	The date and time the scan completed.
<b>Scan Finished</b>	The scan progress as a percentage.
<b>Critical Risk</b>	The number of detected critical risk files.
<b>High Risk</b>	The number of detected critical high files.
<b>Medium Risk</b>	The number of detected medium risk files.
<b>Low Risk</b>	The number of detected critical low files.
<b>Clean</b>	The number of clean files.
<b>Others</b>	The number of detected other files.
<b>Scan Status</b>	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.

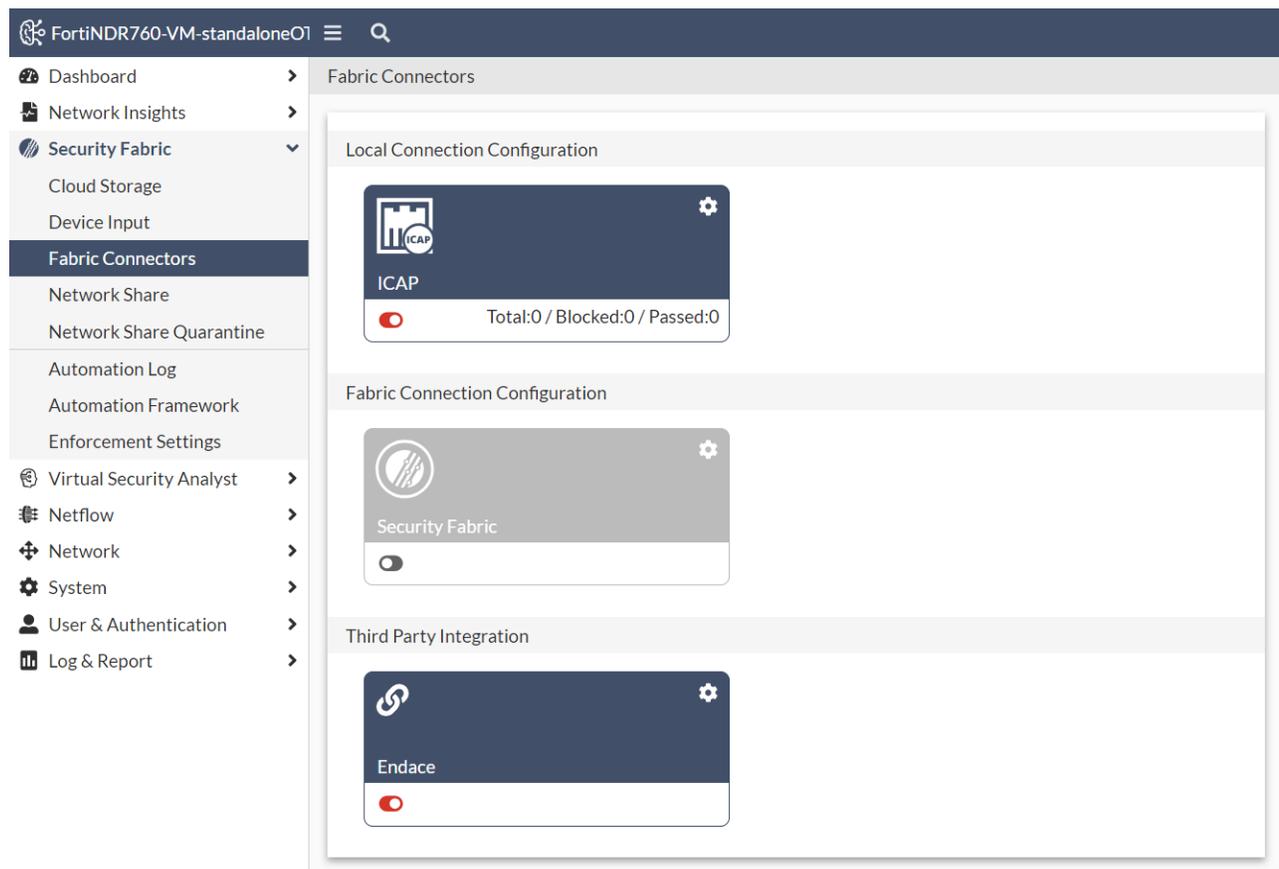
## Scanning Zip files

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 Anomaly > 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	
<b>Enable ICAP Connector</b>	Click to enable the ICAP connector.
<b>Monitor Only Mode</b>	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	
<b>Interface</b>	Select an interface from the dropdown.
<b>Port</b>	Enter port the connector will use to connect to FortiNDR. Default is 1344. <b>Note:</b> Avoid choosing the Sniffer port as the ICAP interface.
<b>SSL Support</b>	Click to enable Secure Sockets Layer.
<b>SSL Port</b>	Enter the SSL port. Default is 11344.
Configuration	
<b>Realtime FortiNDR Scan</b>	When enabled, FortiNDR will delay the response to the ICAP client until the scan result has been achieved or the timeout has been reached.
<b>Realtime FortiNDR Scan Timeout at</b>	Enter the number of seconds is realtime scan will timeout. Default is 10 seconds.
Confidence Level	
<b>Quarantine Confidence level equal and above</b>	Set the confidence level as a percentage and select <i>Medium</i> or <i>High</i> .

Status

Enable ICAP Connector

Monitor Only Mode

Connection

Interface

Port

SSL Support

SSL Port

Configuration

Realtime FortiNDR Scan

Realtime FortiNDR Scan Timeout at  second(s) (Between 1 to 20 second(s), Default: 10 seconds)

Confidence Level

Quarantine Confidence level equal and above  %

## Security Fabric Connector

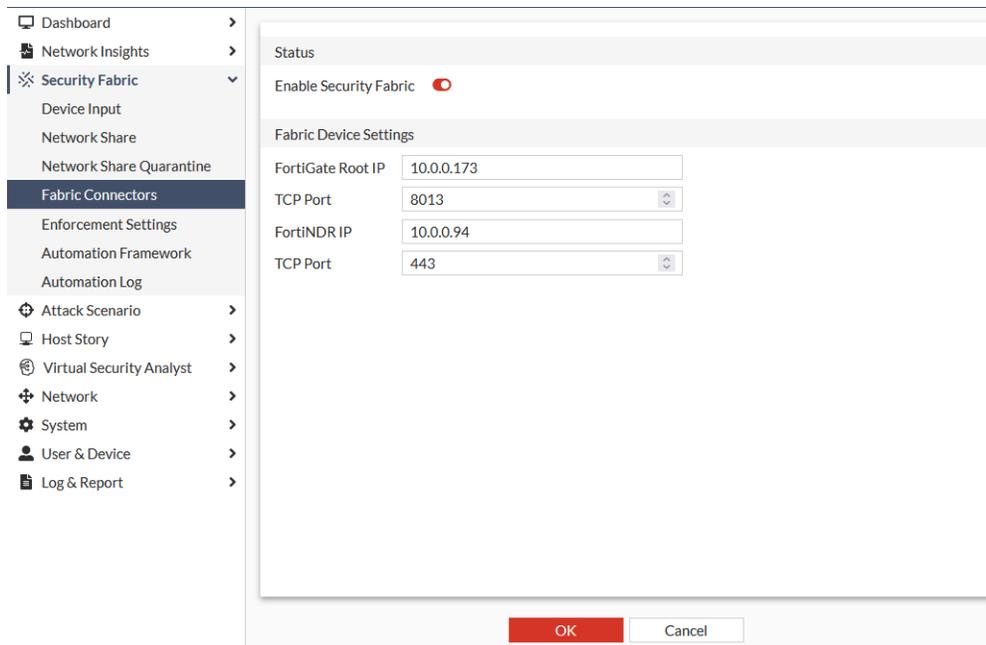
FortiNDR 1.5.0 and FortiOS 7.0.0, FortiNDR can join FortiGate Security Fabric. After connecting to the Security Fabric, FortiNDR can share information such as FortiNDR system information and malware types detected.

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.

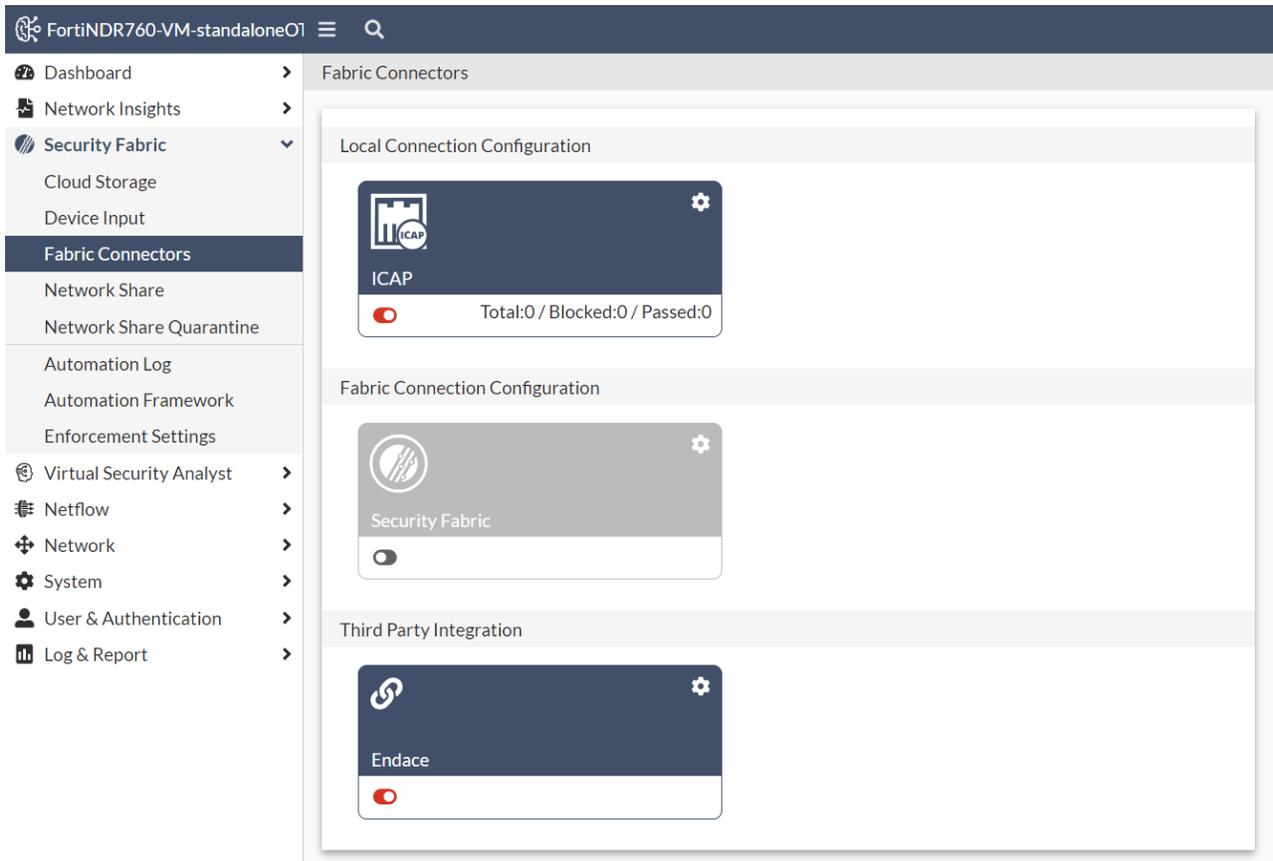


## Endace

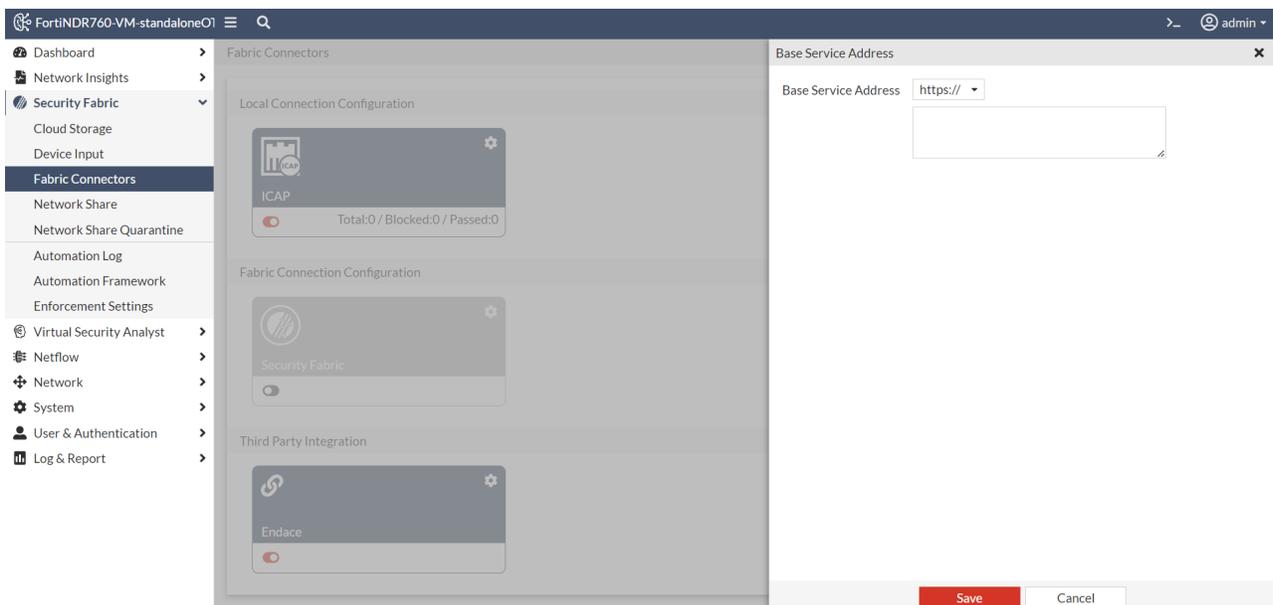
The Endace fabric connector allows you to investigate the PCAP related to the IP addresses. This integration is available in Standalone and Sensor modes.

## 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.

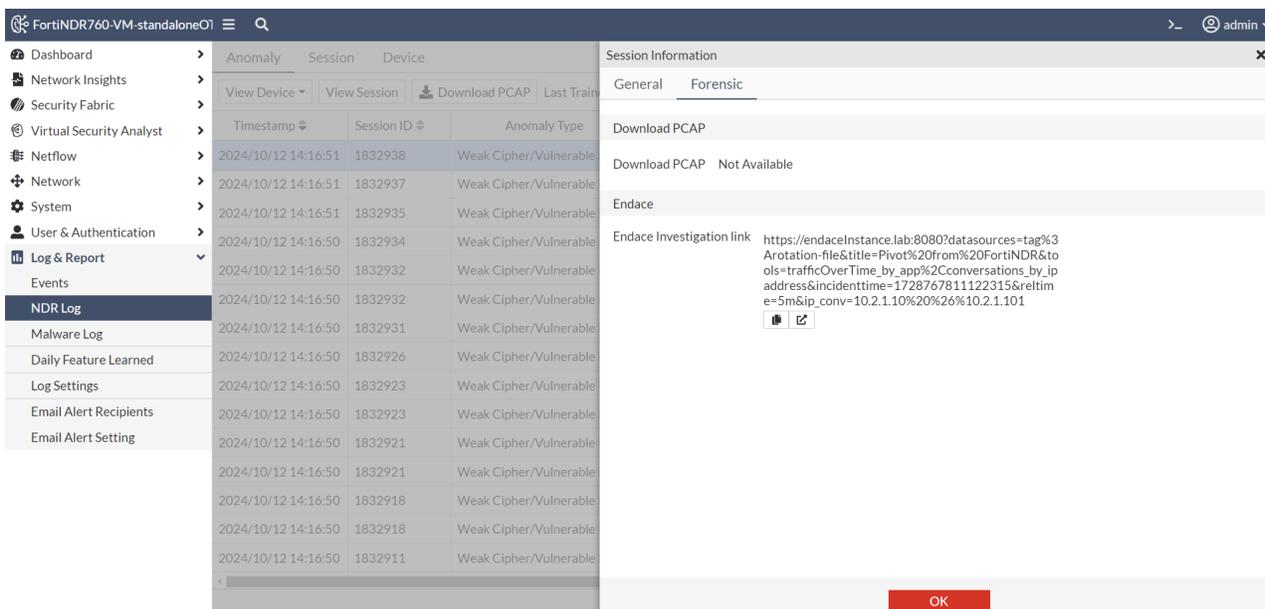
To enable the connector, you will need to re-enter the base URL

### 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 *Anomaly* 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.

## Enforcement Settings

*Enforcement Settings* provide an extra layer of logic to deal with the detection discovered by FortiNDR and delivers follow-up actions to Security Fabric devices. FortiNDR periodically evaluates the latest batch of detections based on

enforcement settings. If any detection satisfies the criteria for the next cause of action, the system then looks at which automation profile the detection falls under and performs the response action accordingly.

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

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

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

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

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

## Creating enforcement profiles

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

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

### Duplicate anomalies

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

#### To create 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*.

<b>Profile Name</b>	Enter a name for the profile.
<b>Enforcement Policy</b>	
<b>Event Category</b>	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Malware Detection</i></li> <li>• <i>NDR: Botnet Detection</i></li> <li>• <i>NDR: Encryption Attack Detection</i></li> <li>• <i>NDR: Network Attack Detection</i></li> <li>• <i>NDR: Indication of Compromise Detection</i></li> <li>• <i>NDR: Weak Cipher and Vulnerable Protocol Detection</i></li> <li>• <i>NDR: Machine Learning Detection</i></li> </ul>
<b>Malware Risk Level</b>	Select <i>Critical</i> , <i>High</i> , <i>Medium</i> or <i>Low</i> severity from the dropdown.
<b>Malware Confidence Level</b>	Enter a numeric value for the confidence level and click either <i>Medium</i> or <i>High</i> .
<b>Additional Settings</b>	
<b>Allow List</b>	Click the plus sign (+) to the IP address you want to exclude as a trigger. If the source IP matches the entry, the profile will not be triggered even if the event and severity level match.

General Settings

Profile Name

---

Enforcement Policy

Event Category

- Malware Detection
- NDR: Botnet Detection
- NDR: Encryption Attack Detection
- NDR: Network Attack Detection
- NDR: Indication of Compromise Detection
- NDR: Weak Cipher and Vulnerable Protocol Detection
- NDR: Machine Learning Detection

Malware Risk Level Critical

Malware Confidence Level 80 Medium High

---

Additional Settings

Allow List  +

OK
Cancel



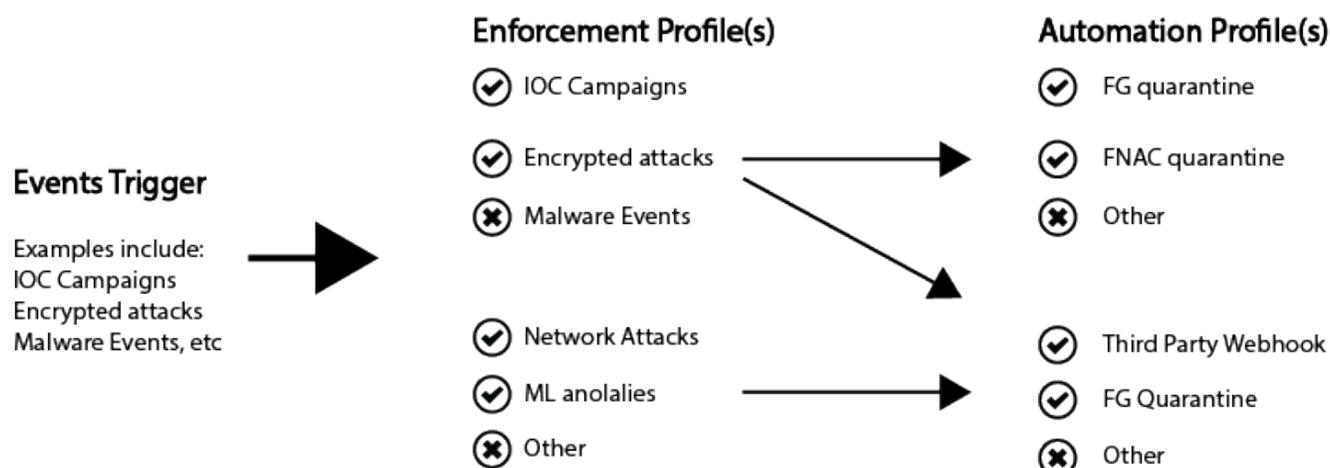
For NDR detection *Severity Level* and *Malware risk level*, severity is inclusive of higher severity levels. For example, if *High* is selected, the enforcement profile will match both *HIGH* and *CRITICAL* events.

## Automation Framework

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

### FortiNDR Response

#### Understanding Enforcement and Automation Profiles



#### To create an automation profile:

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

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

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

*Manage FortiGate Settings and FortiSwitch Quarantine via FortiLink.*

**Manage FortiGate Settings and FortiSwitch Quarantine Settings**

**Source**

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

**API Key**

Enter the device API key

**IP**

Enter the device IP address.

**Port**

Enter the device port number.

**VDOM**

Enter the VDOM name.

**WebHook Name for Execution**

Select the FortiGate webhook for execution action, such as *ip\_blocker*.

**WebHook Name for Undo**

Select the FortiGate webhook for undo action, such as *ip\_unblocker*.

*FortiNAC Quarantine*

**FortiNAC Quarantine Settings**

**API Key**

Click *Change* to update the API key.

**IP**

Enter the FortiNAC IP address.

**Port**

Enter the FortiNAC port number.

*Generic Webhook*

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

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

## FortiGate quarantine webhook setup example

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

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

### To set up a webhook for Ban IP:

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

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

New Admin Profile

Name

Comments  0/255

Access Permissions

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

Permit usage of CLI diagnostic commands

Override Idle Timeout

OK Cancel



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

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

Trusted Hosts	IPv6 Trusted Host	Profile	Type	Two-factor Authentication
		super_admin	Local	Disabled
		super_admin	Local	Disabled
		super_admin	Local	Disabled
		super_admin	API Key	

3. Configure the administrator settings:

**Username**

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

<b>Administrator Profile</b>	Where permissions for the REST API administrator are defined. A REST API administrator should have the minimum permissions required to complete the request.
<b>PKI Group</b>	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.
<b>CORS Allow Origin</b>	Cross Origin Resource Sharing (CORS) allows third-party web apps to make API requests to the FortiGate using the token.
<b>Trusted Hosts</b>	The following can be used to restrict access to FortiGate API: Multiple trusted hosts/subnets can be configured IPv6 hosts are supported Allow all (0.0.0.0/0) is not allowed You need your Source Address to create the trusted host.

New REST API Admin

Username:

Comments:  0/255

Administrator profile:

PKI Group:

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

CORS Allow Origin:

Restrict login to trusted hosts

Trusted Hosts:

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

New API key

New API key for ipblocker\_user:

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

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

```
config vdom
edit root
diagnose user 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*.

- 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**

Stitch	Trigger	Action				
Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
Compromised Host						
FortiOS Event Log						
Incoming Webhook						
ip_blocker	Enabled	ip_blocker	ip_blocker	All FortiGates	1	2 seconds ago
ip_unblocker	Enabled	ip_unblocker	ip_unblocker	All FortiGates	64	37 minutes ago



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

- Register the Webhook name in the Automation Profile.

**Automation Framework**

Profile Name:

Enable:

Enforcement Profile:

Action:

---

**Manage FortiGate Settings**

Source:

API Key:

IP:

Port:

VDOM:

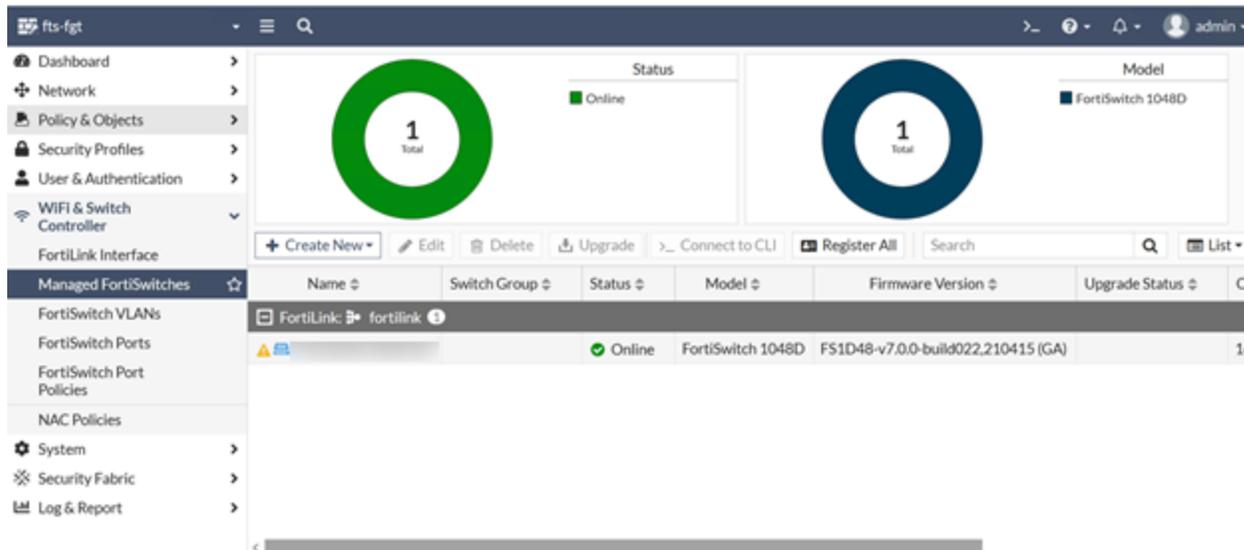
Webhook Name for Execution:

Webhook Name for Undo:

## FortiSwitch quarantine setup example

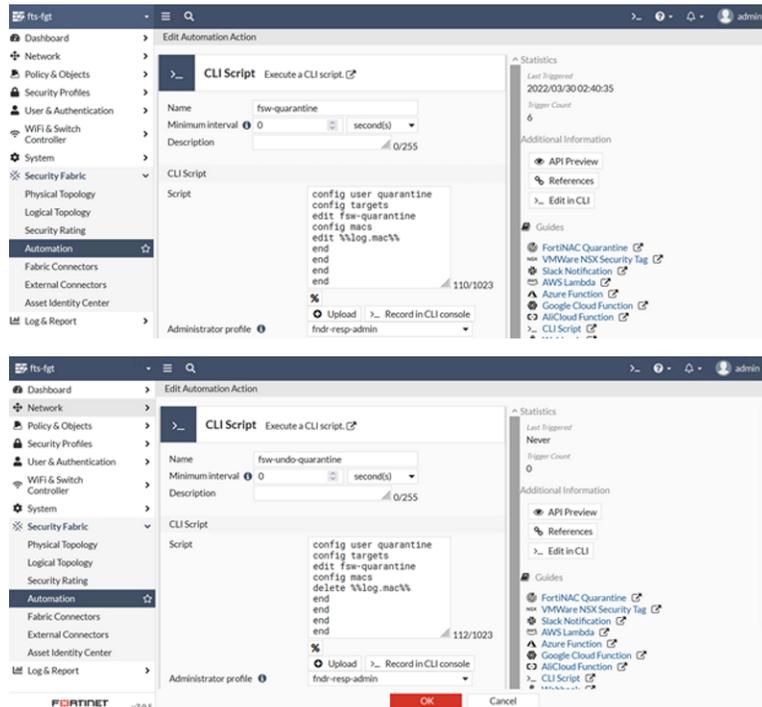
FortiNDR supports quarantining devices that are connected to a FortiSwitch which is managed by FortiGate. FortiSwitch is connected to a FortiGate and is configured in FortiLink mode. FortiNDR will utilize FortiGate's incoming webhook to provide the device's MAC address for quarantine/undo quarantine.

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



### To setup FortiSwitch quarantine on FortiNDR:

1. Following the steps for creating a webhook on FortiGate in [FortiGate quarantine webhook setup example](#) on page 120. Note that the CLI script for quarantine and undo quarantine should be updated.





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

2. Register webhooks on FortiNDR .



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

Automation Framework

Profile Name: test-fsw

Enable:

Enforcement Profile: default

Action: FortiSwitch Quarantine via FortiLink

---

FortiSwitch Quarantine Settings

Source: Fabric Device **Snitter**

API Key: \*\*\*\*\*

IP: 172.19.235.201

Port: 443

VDOM: root

Webhook Name for Execution: fsw-quarantine

Webhook Name for Undo: fsw-undo-quarantine

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

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping	Transceiver
port17		Static		Edge Port Spanning Tree Protocol	_,default,fortilink_(default)	quarantine,fortilink_(quarantine)				Untrusted
port18		Static		Edge Port Spanning Tree Protocol	_,default,fortilink_(default)	quarantine,fortilink_(quarantine)				Untrusted
port19		Static		Edge Port Spanning Tree Protocol	_,def	quarantine,fortilink_(quarantine)				Untrusted
port20		Static		Edge Port Spanning Tree Protocol	_,def	quarantine,fortilink_(quarantine)				Untrusted
port21		Static		Edge Port Spanning Tree Protocol	_,def	quarantine,fortilink_(quarantine)				Untrusted
port22		Static		Edge Port Spanning Tree Protocol	_,def	quarantine,fortilink_(quarantine)				Untrusted
port23		Static		Edge Port Spanning Tree Protocol	_,def	quarantine,fortilink_(quarantine)				Untrusted
port24		Static		Edge Port Spanning Tree Protocol	_,def	quarantine,fortilink_(quarantine)				Untrusted
port25		Static		Edge Port Spanning Tree Protocol	_,default,fortilink_(default)	quarantine,fortilink_(quarantine)		e-43-4b-80c2-da		Trusted
port26		Static		Edge Port Spanning Tree Protocol	_,default,fortilink_(default)	quarantine,fortilink_(quarantine)				Untrusted
port27		Static		Edge Port Spanning Tree Protocol	_,default,fortilink_(default)	quarantine,fortilink_(quarantine)				Untrusted

**Quarantined**

172.19.140.2

Device: e-43-4b-80c2-da

MAC Address: e-43-4b-80c2-da

IP Address: 172.19.140.2

DHCP Lease: expires on 2022/04/05 22:52:32

Online Interfaces: ,default,fortilink\_(default)

Hardware: Fortinet./FortiGate

OS: FortiOS

+ Firewall Device Address + Firewall IP Address

4. Click *OK*.

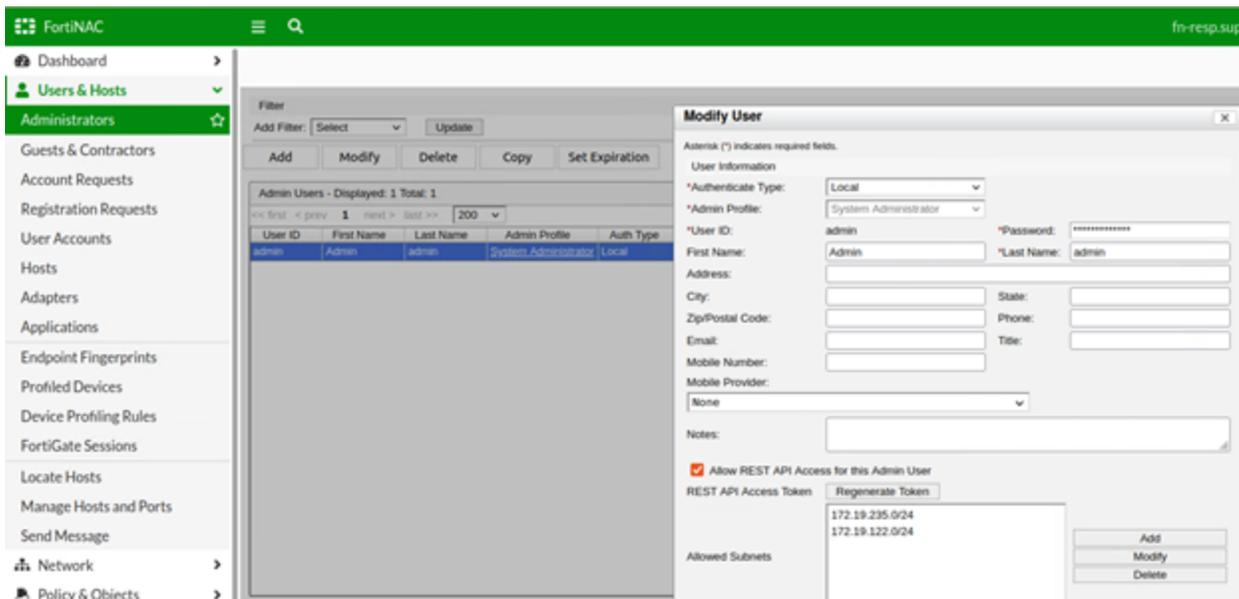
## FortiNAC quarantine setup example

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

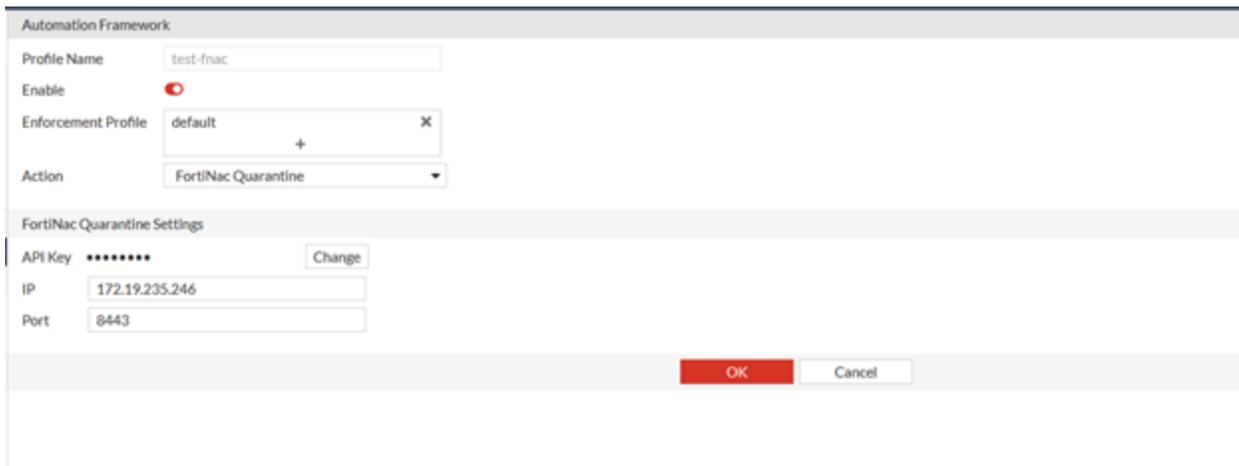
For information about configure FortiNAC, see the [FortiNAC Administration Guide](#) in the Document Library.

### To setup FortiNAC quarantine on FortiNDR:

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



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



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

## Generic Webhook setup example

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



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

Automation Framework

Profile Name:

Enable:

Enforcement Profile:  + ✕

Action:

---

Webhook Execution Settings

URL:

Method:

Header:

Content-Type	<input type="text" value="application/json"/>	✕
Authorization	<input type="text" value="Bearer gyhw7xkn0hd06gG83qjNzfQxd17i"/>	✕

+

HTTP Body Template:

---

Webhook Undo Settings

URL:

Method:

Header:

Authorization	<input type="text" value="Bearer gyhw7xkn0hd06gG83qjNzfQxd17i"/>	✕
Content-Type	<input type="text" value="application/json"/>	✕

+

HTTP Body Template:

## Automation log

*Automation Log* records each enforcement action generated by FortiNDR.

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

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

	Initial Action Time #	Target IP #	Target MAC #	Violations #	Action Type #	Automation Profile Name #	Enforcement Profile Type #	Action Executed #	Post Action #	Status #
Dashboard										
Network Insights										
Security Fabric										
Device Input	2022/04/16 21:30:30	18.1.2.120	00:50:56:8c:b3:db	38	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
Network Share	2022/04/16 21:30:30	18.2.6.255	00:50:56:8c:b3:db	46	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
Network Share Quarantine	2022/04/16 21:30:30	18.1.8.112	00:50:56:8c:b3:db	20	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Fabric Connectors	2022/04/16 21:30:30	18.1.7.85	00:50:56:8c:b3:db	7	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Enforcement Settings	2022/04/16 21:30:30	18.2.12.106	00:50:56:8c:b3:db	19	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Automation Framework	2022/04/16 21:30:30	18.2.3.188	00:50:56:8c:b3:db	15	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Automation Log	2022/04/16 21:30:30	18.1.12.122	00:50:56:8c:b3:db	15	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Attack Scenarios	2022/04/16 21:30:30	18.1.3.16	00:50:56:8c:b3:db	18	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Host Story	2022/04/16 21:30:30	18.1.3.222	00:50:56:8c:b3:db	10	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Virtual Security Analyst	2022/04/16 21:30:30	18.2.2.171	00:50:56:8c:b3:db	42	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:30	None	Executed
Network	2022/04/16 21:10:29	18.1.8.123	00:50:56:8c:b3:db	37	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
System	2022/04/16 21:10:29	18.1.3.50	00:50:56:8c:b3:db	7	Generic Webhook	test-generic-webhook	default	2022/04/16 21:12:48	None	Executed
User & Authentication	2022/04/16 21:10:29	18.2.3.117	00:50:56:8c:b3:db	10	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:29	None	Executed
Log & Report	2022/04/16 21:10:29	18.1.12.51	00:50:56:8c:b3:db	45	Generic Webhook	test-generic-webhook	default	2022/04/16 21:10:29	None	Executed

### Violation details

Initial Action Time #	Target IP #	Target MAC #	Violations #	Action #
2022/04/16 21:30:30	18.1.2.120	00:50:56:8c:b3:db	38	Generic V
2022/04/16 21:30:30	18.2.6.255	00:50:56:8c:b3:db	46	Generic V
2022/04/16 21:30:30	18.1.8.112	00:50:56:8c:b3:db	20	Generic V
2022/04/16 21:30:30	18.1.7.85	00:50:56:8c:b3:db	7	Generic V
2022/04/16 21:30:30	18.2.12.106	00:50:56:8c:b3:db	19	Generic V
2022/04/16 21:30:30	18.2.3.188	00:50:56:8c:b3:db	15	Generic V
2022/04/16 21:30:30	18.1.12.122	00:50:56:8c:b3:db	15	Generic V
2022/04/16 21:30:30	18.1.3.16	00:50:56:8c:b3:db	18	Generic V
2022/04/16 21:30:30	18.1.3.222	00:50:56:8c:b3:db	10	Generic V
2022/04/16 21:30:30	18.2.2.171	00:50:56:8c:b3:db	42	Generic V
2022/04/16 21:10:29	18.1.8.123	00:50:56:8c:b3:db	37	Generic V
2022/04/16 21:10:29	18.1.3.50	00:50:56:8c:b3:db	7	Generic V
2022/04/16 21:10:29	18.2.3.117	00:50:56:8c:b3:db	10	Generic V

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

## Automation Status and Post action

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

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

## FortiSandbox integration (FortiSandbox 4.0.1 and higher)

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

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

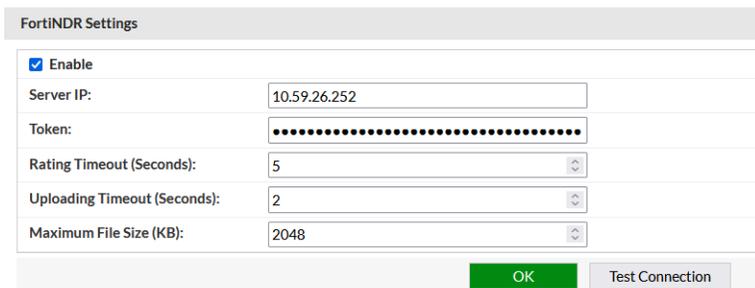
With this integration, FortiNDR reduces the load on FortiSandbox's Dynamic Scan and assists FortiSandbox with determining malware type, such as banking Trojan, coinminer, and so on, based on the features observed.

High level configuration steps are as follows:

1. Generate a FortiNDR API token associated with a user. You can use the GUI in *System > Administrator* or use the CLI command `execute api-key <user-name> .`  
For details, see [Appendix A: API guide on page 255](#).
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.



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

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

Buttons: OK, Test Connection

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

**Scan Profile**

Pre-Filter | VM Association | Advanced

---

Process the following selected file types.

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

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

---

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

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

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

---

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

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

**Apply**

## FortiGate inline blocking (FOS 7.0.1 and higher)

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

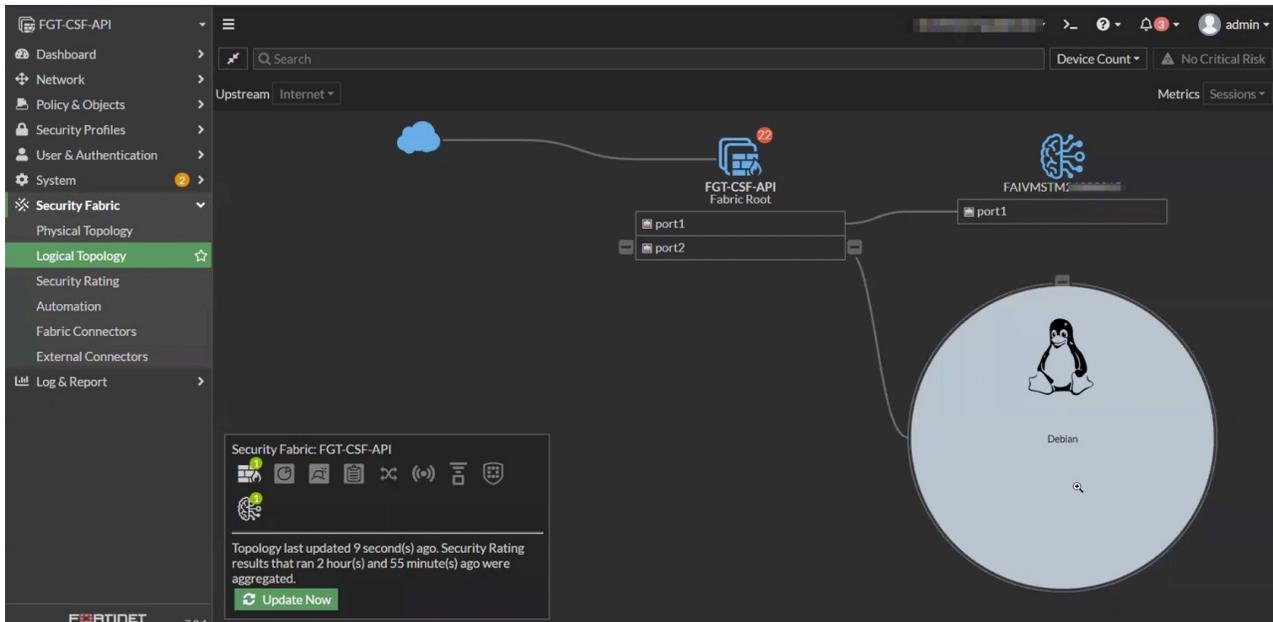


### When using multiple FortiGates:

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 110](#).  
This is needed for authentication between the two devices before file submission begins.
2. When pairing is complete, verify that FortiNDR appears in the FortiGate topology with the FortiNDR icon in the legend.



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

```

Config system fortindr
    Set status enable
End

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

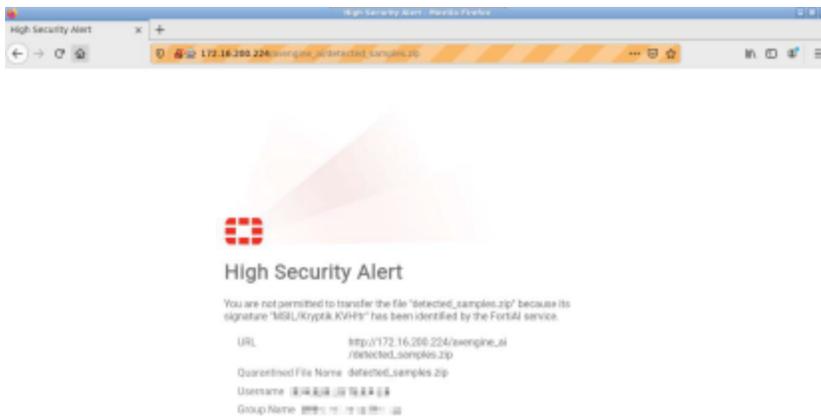
```

**4. Apply this AV profile in the FortiOS NGFW policy.**

Both FortiGate Antivirus logs and FortiNDR logs and reports show corresponding log entries.

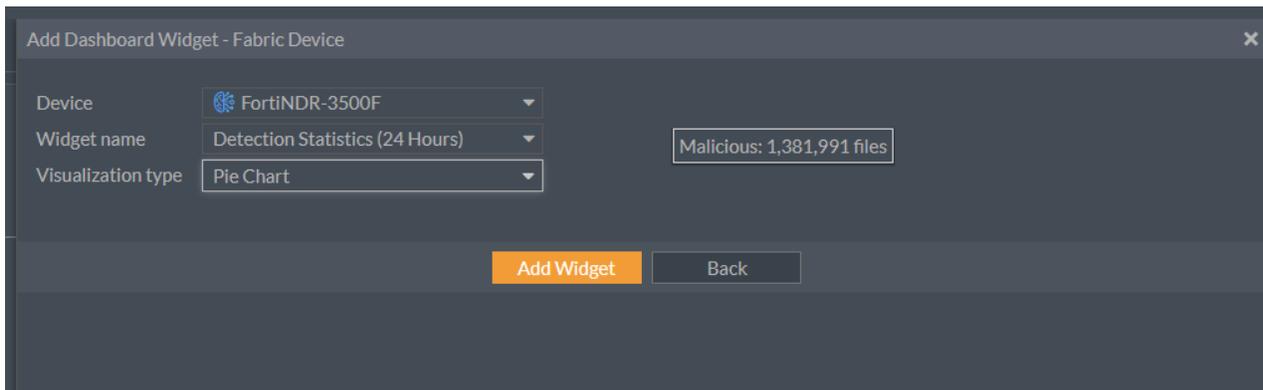
## Tips for using FortiNDR inline blocking

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



- For encrypted traffic such as HTTPS, the SSL profile must be configured on FortiGate to extract files in encrypted protocols.
- The maximum file size is determined by both FortiGate and FortiNDR. FortiNDR supports a default maximum file size of 200MB. In FortiNDR the maximum file size can be adjusted with the following CLI command:  

```
execute file-size-threshold
```
- If there are network connectivity issues that causes a timeout between the connections, FortiGate 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-	WinPE (EXE)
ELF	XML)	XZ
GZIP	PDF	ZIP
	RAR	

## 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.**

**Sandbox Settings**

Status:  Enabled  Disabled

Type:  FortiSandbox  FortiSandbox Cloud

Server:

Connection status: ✔ Reachable

Notifier email:

Inline scan:

Connection Status: ✔ Connected

Dynamic Malware Detection: **Version** not loaded

URL Threat Detection: **Version** 0.0

Entries: 0

Sandbox Statistics (last 7 days)

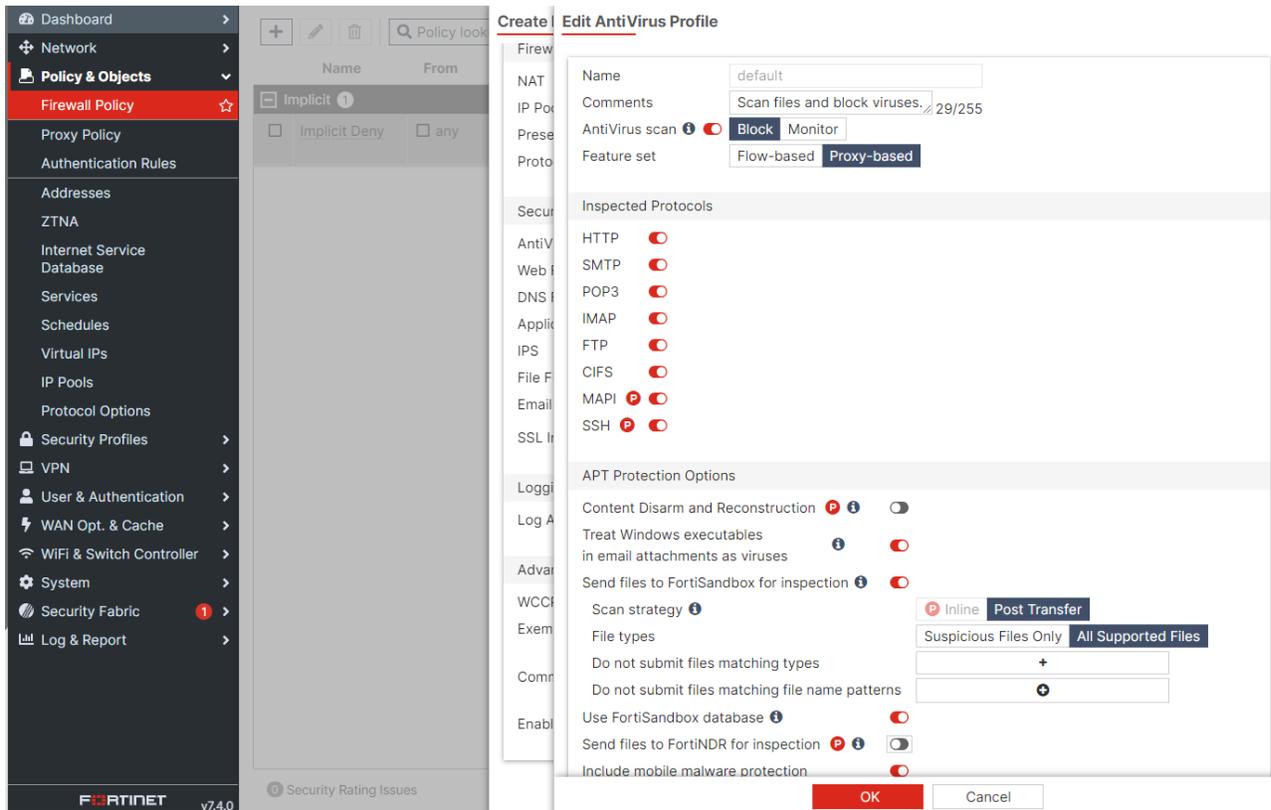
File type	Detected
Total submitted	0
Critical (Malicious)	0
High Risk	0
Medium Risk	0
Low Risk	0
Clean	0

Additional Information:

FortiSandbox Cloud Solutions [Amazon Web Services Marketplace](#)

OK Cancel

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



3. Apply an AV profile to the firewall policy.

The screenshot shows the FortiGate configuration interface. On the left is a navigation menu with 'Policy & Objects' selected, and 'Firewall Policy' highlighted. The main area displays a 'Create New Policy' dialog box. The 'Firewall/Network Options' section includes NAT (checked), IP Pool Configuration (Use Outgoing Interface Address), Preserve Source Port (unchecked), and Protocol Options (default). The 'Security Profiles' section is expanded, showing AntiVirus (checked, AV default), Web Filter (unchecked), DNS Filter (unchecked), Application Control (unchecked), IPS (unchecked), File Filter (unchecked), Email Filter (unchecked), and SSL Inspection (checked, SSL certificate-inspection). The 'Logging Options' section shows Log Allowed Traffic (checked) with Security Events and All Sessions selected. The 'Advanced' section shows WCCP (unchecked) and Exempt from Captive Portal (unchecked). The 'Comments' field is empty, and the 'Enable this policy' checkbox is checked. At the bottom are 'OK' and 'Cancel' buttons.

4. Authorize the FortiGate on FortiNDR for sending files.

The screenshot shows the FortiNDR-1000F (Sensor) configuration interface. The 'Security Fabric' section is expanded, showing a table of device inputs. The table has columns for Device Name, VDOM, IP Address, Connection Type, Authorized, and Status. The 'fts-igt' device is highlighted, and a dropdown menu is open over the 'Authorized' column, showing 'Enable' selected. The 'Status' column for 'fts-igt' shows 'Disconnected'. At the bottom of the dropdown are 'Apply' and 'Cancel' buttons.

Device Input	Device Name	VDOM	IP Address	Connection Type	Authorized	Status
Network Share	FGVM_251	global		OFTP	Enabled	Connected
Network Share Quarantine	FGVM_251:root	root		OFTP	Enabled	Connected
Fabric Connectors	fts-igt	global		OFTP	Enable	Disconnected

### 5. Check the FortiNDR processed traffic.

Category	Date #	MDS	File ID #	File Type	File Size #	Detection Name	Device Type	VDOM	Attacker	Attacker Network	Victim	Victim Network
Detected	2024/01/04 16:00:15	D8282C779FB0588C7D10E92789A...	8743458	PE	430.08 KB	W32/PossibleThreat	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Processed	2024/01/04 15:59:37	C1163EE3AE5DE384407262A8868...	8738635	ASPACK	418.3 KB	PossibleThreat	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Processing	2024/01/04 15:56:09	5E82538E775A67D1619595F40C75913...	8708717	PE	188.62 KB	W32/PWS.Gittr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Virtual Security Analyst	2024/01/04 15:53:03	38C71731E5232D78C98836A1680B...	8680220	PE	1.97 MB	Riskware/Application	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Netflow	2024/01/04 15:48:13	91A291A8B8A58FA8996F78A8473A5...	8652384	PE	73.99 KB	W32/Kryptik.CTYEtr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
System	2024/01/04 15:39:01	7876742BEE38E55948930478C96...	8565223	UPX	207.36 KB	Riskware/Portscan	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
User S. Authentication	2024/01/04 15:12:46	769830902F13F8D63C4C4835955B...	8396434	UPX	31.23 KB	W32/Generic.AC_2CBEtr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Log & Report	2024/01/04 15:08:51	4548B3F878249E98A4F5A38030C0B...	8366585	PE	94.21 KB	W32/VB.NBELtr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Malware Log	2024/01/04 15:00:41	9782348D58C7F01518E985F4A4720C...	8302032	PE	431.1 KB	W32/LEGION.D0tr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
NDR Log	2024/01/04 14:54:33	6A89C3F42D9A98031383588A888A...	8277142	ZIP	4.85 MB	W32/ChinGamerstr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Events	2024/01/04 14:54:06	3C2297715C261978E93464595E2C...	8258557	UPX	169.63 KB	Adware/WiFiAd	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Daily Feature Learned	2024/01/04 14:23:11	18632048894E11C36E23E3842C0476...	8044387	ZIP	1.91 MB	W32/DefN0F3tr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Log Settings	2024/01/04 14:20:34	C28FAC9CFF598787847C2A2861...	8022086	PE	2.91 MB	Riskware/SOPMedic	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Email Alert Settings	2024/01/04 14:16:29	F352819E9842485925C55D138C851...	7996404	ZIP	2.51 MB	MOGATAttv	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
Email Alert Recipients	2024/01/04 14:16:02	75E18411E43A129488662683F208D...	7994667	PE	197.63 KB	W32/BIOPKA1tr.bdr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
	2024/01/04 14:15:38	7702713297C1C8B4F4081C178C28A...	7869330	PE	50.69 KB	Adware/Newsdotnet	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
	2024/01/04 14:05:03	C38E6A8274A6A378E1101D81823A7...	7916854	PE	3.58 KB	W32/PossibleThreat	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
	2024/01/04 13:59:00	1489AD170F78AA9189E45218F10D7...	7868995	PE	167.94 KB	W32/PioneerC2tr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
	2024/01/04 13:56:55	4195A5D878F7458A41881C78C2412...	7852523	UPX	26.62 KB	Riskware/StartupRun	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
	2024/01/04 13:50:52	60A8D9231C17C5F0987E78AC3198...	7801765	CAB	120.83 KB	W32/DefDFAstr	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal
	2024/01/04 13:41:40	A98A1A56A054648A8046F021F8593...	7733721	PE	629.76 KB	PossibleThreat	HTTPI2(Fortigate)	root	172.16.77.46	Internal	192.168.100.2	Internal

# Virtual Security Analyst

This section includes the following topics.

- [Express Malware Analysis](#) on page 138
- [Outbreak Search](#) on page 142
- [Static Filter](#) on page 144
- [NDR Muting](#) on page 145
- [ML Configuration](#) on page 147
- [Malware Big Picture](#) on page 155
- [Device Enrichment](#) on page 156

## 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 255 > 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.

<b>Submission Time</b>	The date and time the file was uploaded.
<b>Submitted Filename</b>	The name of the file that was uploaded.
<b>Submission User</b>	The user that submitted the file.
<b>MD5</b>	The verdict result from MD5 checksum of the file.
<b>Verdict</b>	The attack scenario used to identify the malware attack.
<b>Confidence</b>	The confidence level as a percentage.
<b>Risk</b>	The risk verdict (High, Medium, Low or No Risk).
<b>Status</b>	The submission status.
<b>File Type</b>	The file type such as <i>Zip</i> or <i>PE</i> . <i>Other</i> indicates the detected file type is not supported by Artificial Neural Networks (ANN).
<b>Indicator</b>	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
<b>History</b>	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.
<b>Similar files</b>	FortiNDR has a similar engine analysis based on the features detected. This is useful for detecting similar variants of the original malware.
<b>MITRE information (and Investigator view)</b>	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.
<b>IOC (Indicators of Compromise)</b>	For text-based malware, FortiNDR can display more contextual information of malware, such as <i>file contain abnormal javascript</i> , and so on. This helps you understand why FortiNDR determines it is malware.

← Back Sample 178715 Information View + Add to Allow List Generate Report Download File

**VSA Verdict: Critical Risk**



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

Confidence level: M6187.7%

**Sample Information**

Submitted Date	2023/08/10 16:57:36	Last Analyzed	2023/08/10 16:57:37
File Type	PE	File Size	99328(97.0 KB)
File Name	Index.html.1		
MDS	5004DACB7AEASFF182EA807EB8EE835D VT		
SHA256	4587CCFECC9A1FF5C538A375409CA1687D3048CDE252077A119C436296857B		
SHA1	82D96268C6679F30B400BEA8DE50EFC4E15A63A4		
Detection Name	W32/Speccom.AN/tr.dldr	Virus Family	Industroyer
Detected By	AV Engine		
Source Device			
Device Type	Manual Upload		
Network			

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

**Feature Composition**

64  
Detection(s)

Feature Type	Appearance In Sample
Industroyer	64

History

🔍 Search View all History

Date	MDS	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk
2023/08/18 15:37:19	S004DACB7AEASFF182EA807EB8EE835D	PE	W32/Speccom.AN/tr.dldr	Manual Upload				M6187.7%	Critical
2023/08/10 16:57:36	S004DACB7AEASFF182EA807EB8EE835D	PE	W32/Speccom.AN/tr.dldr	Manual Upload				M6187.7%	Critical
2023/08/01 12:12:10	S004DACB7AEASFF182EA807EB8EE835D	PE	W32/Speccom.AN/tr.dldr	Network Share		172.19.235.15	172.19.235.15	M6187.7%	Critical
2023/08/01 12:09:53	S004DACB7AEASFF182EA807EB8EE835D	PE	W32/Speccom.AN/tr.dldr	Network Share		172.19.235.15	172.19.235.15	M6187.7%	Critical

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

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

20 Items 🔍 Search Generate Report

Submission Time	Filename	MDS	File Type	Verdict	Confidence Level	Risk Level	Status
<b>Supported File Type 13</b>							
2020/05/31 17:13:30	40550136.vsc	a86a5fe18402c958b4365263fab2a12a	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3C559658.vsc	b6523dcd40e9c768a06ff46516fdde4	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	38E9F1A6.vsc	ff578c64c31e7c9dac090a9c03136500	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3486983A.vsc	402bfd289434fd9e2850ea13dbdb6f87	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	42B0E080.vsc	63b3eac79ea8c3a033f5cb2cea2b1ccc	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	40B03FEF.vsc	af7a049fb21401b38ea7c3a9ba9674eb	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3BCECAE0.vsc	1beb2e23edc295ae214e762a478d300a	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	3185F88C.vsc	e143b75b35ded9fc369fec32015e98dd	PE	Ransomware	100%	Critical Risk	Done
2020/05/31 17:13:30	337A1E91.vdf	716cb0c867206122532ed753826b6a6c	PDF	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	355C8BFC.vsc	1b129271e371d64bbe128014ccfc021b	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	317C51E0.vsc	7116dd303a1e70e0d3bb310ec383e036	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	3420A9B4.vxe	4e8ffc5e4f4e62ebbb123f810f36602f	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	3BB44181.vsc	add352ba1edf9b25dc1cf3b152d9fe45	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	38C07AA2.vsc	e10ff38099494e80189c0bc28eac4a68	PE	Clean	N/A	No Risk	Done
2020/05/31 17:13:30	31340098.vsc	9cf8b1e41b61a586002dfc5f4f6daedb	PE	Application	100%	Low Risk	Done
<b>Unsupported File Type 5</b>							
2020/05/31 17:13:28	3AA1848D.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	409FC737.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3AA0CF20.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3AA0CDE.vsc			Generic Attack		Pending	Fail: Unsupported File Type
2020/05/31 17:13:28	3A109FD3.vsc			Generic Attack		Pending	Fail: Unsupported File Type

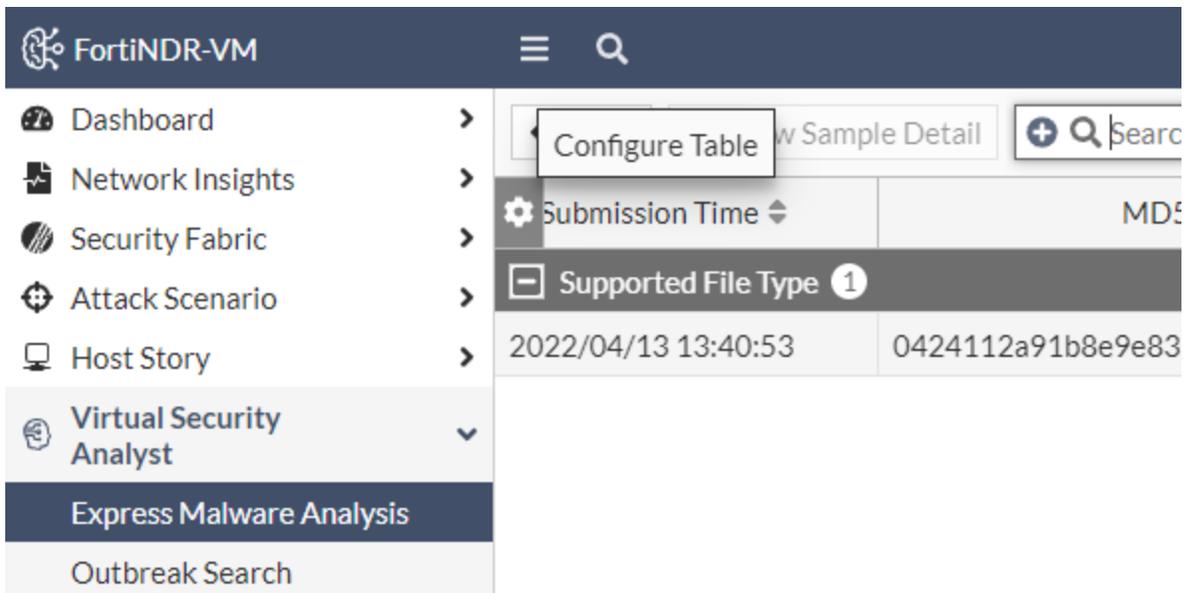
4. (Optional) Click *Generate Report* to view the report summary in PDF and JSON format.

### To change the file size limit with the CLI:

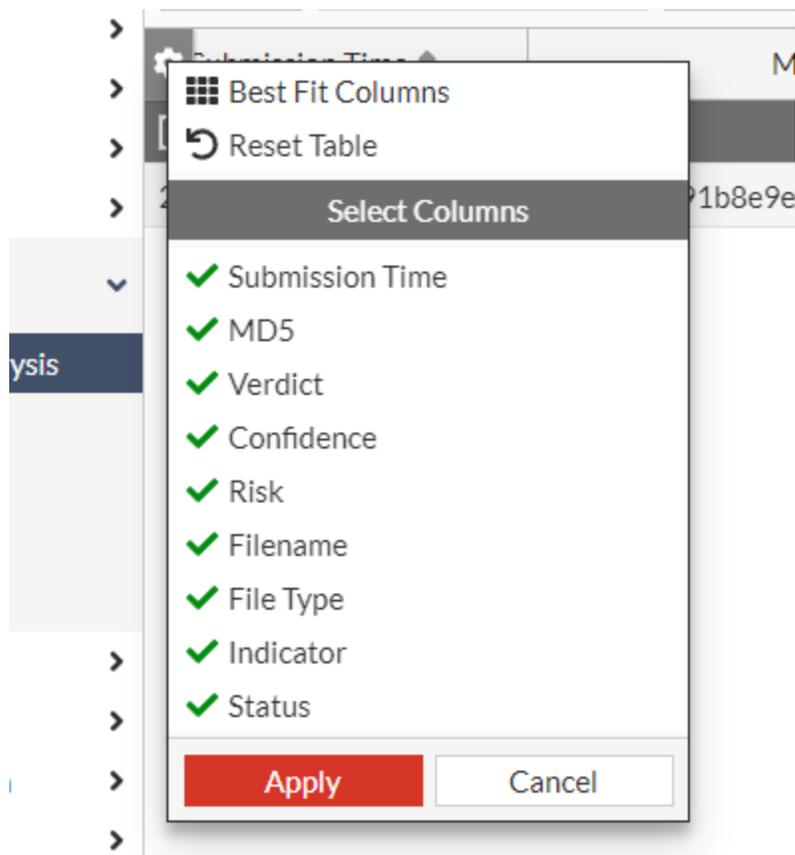
```
execute file-size-threshold
```

### 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.

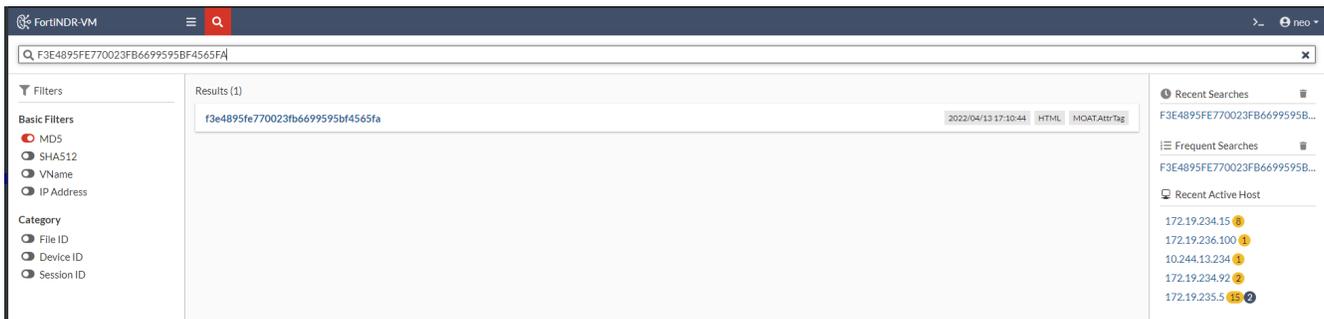


## Outbreak Search

*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 142](#).
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 143](#).

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



### Search lead type of hash or detection name

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

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

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

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

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

Search Lead Type: Hash a8990d67f31dd5a509d07e3c0f68a82 ✕ 🔍 Similarity-Based Hash-Based Detection-Based

**Related Files**

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

Date	MDS	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	dbe015f6411f5e83cb276c752551078	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	dbe015f6411f5e83cb276c752551078	HTML	Phishing	Generic	MOAT/Crypted.Gen	Low Risk	High (98.44%)	100.00%
2020/06/01 17:52:09	b2dbf3fed8b3ed67c80567461284a42	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	a8990d67f31dd5a509d07e3c0f68a82	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.

Dashboard Security Fabric Attack Scenario Host Story Virtual Security Analyst Express Malware Analysis **Outbreak Search** Threat Investigation Network System User & Device Log & Report

Search Lead Type: Outbreak Name WannaCry ✕ 🔍 📘

**Related Files** Related Events Related Detection Names Related Remote Connection

Generate Report Search Found 74 Search by Hash Search similar file(s) by Hash Search by Detection Name Search similar file(s) by Detection Name Sample Info

Date	MDS	File Type	Detection Name	Risk Level	Confidence Level	Associated By
2020/06/14 11:16:20	b6523dcd40e9c768a06ff46516fde4	PE	Q W32/Virut.CE	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	402bfd289434fd9e2850ea13dbdb6f87	PE	Q W32/WannaCryptor.D:tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	ff578c64c31e7c9dac090a9c03136500	PE	Q W32/WannaCryptor.D:tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	af7a049fb21401b38ea7c3a9ba9674eb	PE	Q W32/Virtu.F	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	a86a5fe18402c958b4365263fab2a12a	PE	Q W32/Virtu.F	Low Risk	High (100.00%)	By Detection Name
2020/06/14 11:16:20	1beb2e23edc295ae214e762a478d300a	PE	Q W32/WannaCryptor.D:tr.ransom	Critical Risk	High (100.00%)	By Similarity
2020/06/14 11:16:20	e143b75b35ded9fc369fec32015e98dd	PE	Q W32/Wanna.APNO:tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	d2782bcbe77d8c400331a102145eb51	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/13 18:46:17	808c71732f0089228fb082b07235620b	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	909421454e3e6da3efed986f2d59e7e	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	4d7769db73272f0493014c3ee6ec2bdc	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:44	e11bf6f7ed035fd4e60c74784209f937	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	bc3d22a07660260b143d8fabbdaed4fb	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	cd2d592622fa018b4718be73d5df6c87	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name
2020/06/09 10:52:43	4b1c08933518263117845448920cb95	PE	Q W32/Miner.VI!tr	Low Risk	High (100.00%)	By Detection Name

## Recursive searches

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

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

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

## Reports

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

## Static Filter

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

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

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

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

Date	Hash Value	Hash Method	Allow / Deny list	Comment
2022/04/14 15:11:06	d01c97e2944166ed23e47e4a62ff471ab8fa031f	SHA1	Allow	
2022/04/14 15:11:06	340c8464c2007ce3f80682e15dfafa4180b641d53c14201b929906b7b0284d87	SHA256	Allow	
2022/04/14 15:11:06	1b7c22a214949975556626d7217e9a39	MD5	Allow	

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

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



You can add a detection to the *Allow List* from the *Malware Log*. For information, see [Malware Log on page 210](#).

## NDR Muting

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

### Hide

- The anomaly in any insight page's *Anomaly* tab.
- The session related to the muted anomaly in any insight page's *Session* tab.
- The connection pair related to the muted anomaly in any insight page's *Connection* tab.

### Stop

- Triggering email alerts from the muted anomaly.
- Triggering enforcement from the muted anomaly.
- Generating syslog messages related to the muted anomaly (Standalone and Sensor mode only).

You can mute certain detections in the *Botnet*, *FortiGuard IOC*, *Network Attacks*, *Weak/Vulnerable Communication*, *Encrypted Attack*, and *ML Discovery* insight pages. Once the attack is muted, any information related to this anomaly will be hidden from the insight pages, although the information is not deleted.



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

The *NDR Muting* displays the following information:

### Last Modified

The date and time the rule was last modified.

<b>Rule ID</b>	The rule's unique ID.
<b>Rule Type</b>	The rule type.
<b>Rule</b>	The rule name and tag.
<b>Created By</b>	The name of the admin who created the rule.
<b>Comment</b>	Comments by the admin.
<b>Status</b>	The current status of the rule ( <i>enabled / disabled</i> ).
<b>Rule</b>	The rule content. For example, if the <i>Rule Type</i> is <i>Anomaly</i> , the rule will be a JSON of anomaly type and content.

## Muting rules in Network Insights

### To mute an NDR Rule:

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

### To view muted detections in Network Insights pages:

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

## Managing muted rules

### To enable/disable NDR muted rules:

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

### To delete multiple rules:

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

### To delete an NDR rule:

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

## ML Configuration

Go to the *Virtual Security Analyst > ML Configuration* page to view and edit the machine learning baseline features for the traffic anomaly detection, as well as the status of the baseline training. You can also use the page to create IP range groups. *ML Configuration* is not available in Sensor mode.

The *ML Configuration* page has two tabs:

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

The *ML Configuration* displays the following information:

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

**To customize the ML Configuration page:**

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

### Source IP tab

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

#### Example

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

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

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

### To create an IP range group:

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

## 3. Configure the source IP settings.

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

4. Click *Apply*.

## Default Tab

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



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



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

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

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

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

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



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

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

## Sensor Group ID Tab (Center mode)

### To create a Sensor Group:

In Center mode, go to

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

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

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

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

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

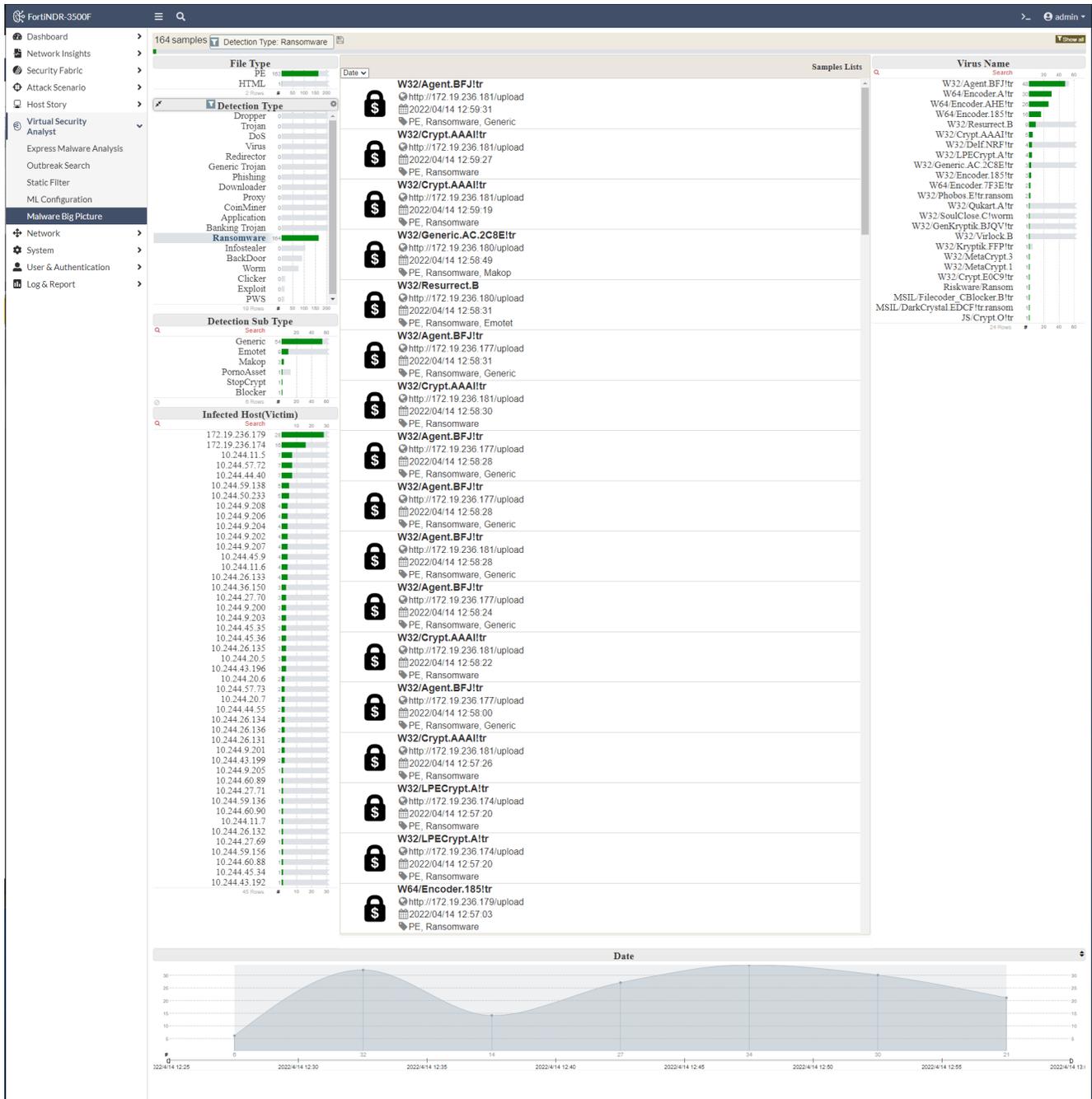
#### To retrain the Sensor Group from the earliest date of the sensors without changing any selected features and retrain detection logs:

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.

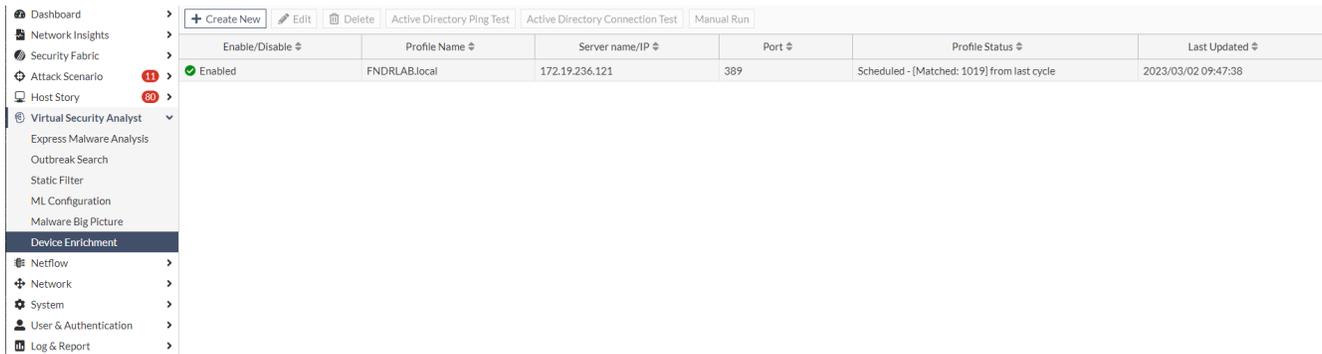


## Device Enrichment

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

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

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



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

The *Device Enrichment* page displays the following information:

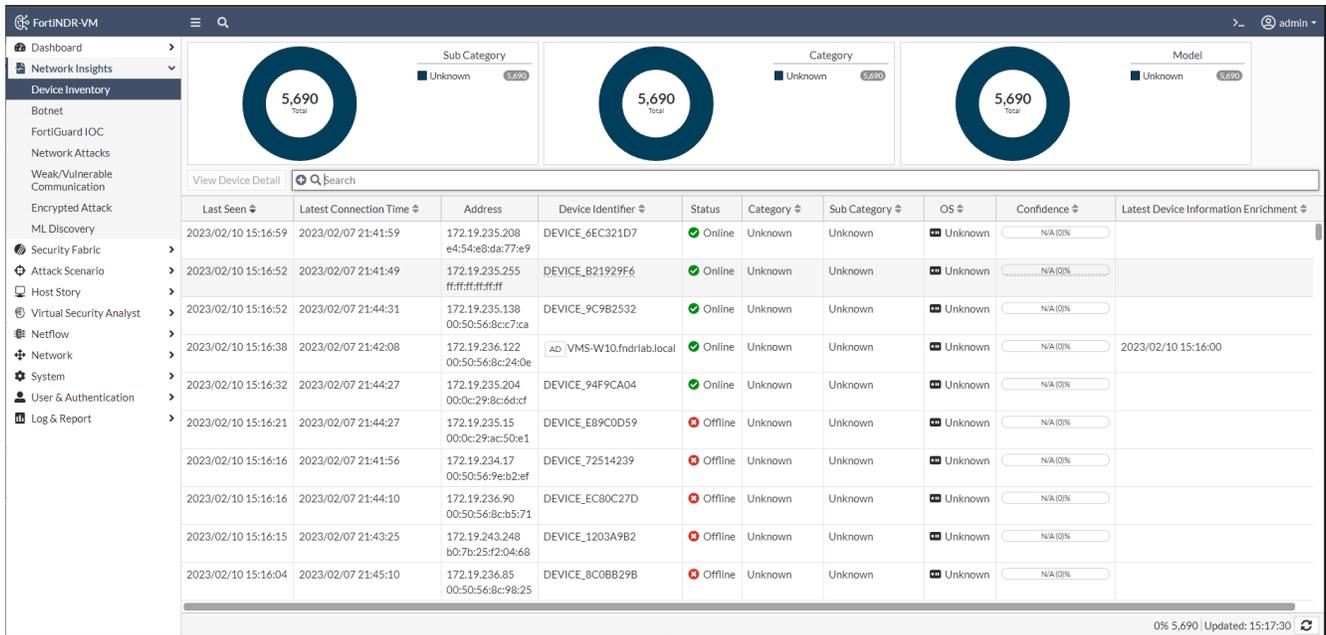
<b>Enable/Disable</b>	Indicates if the profile is enabled or disabled.
<b>Profile Name</b>	The name assigned to the profile.
<b>Server name/IP</b>	The IP address of the windows AD server or domain name.
<b>Port</b>	The port used by the profile. If SSL is enabled the port is 636 otherwise the default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

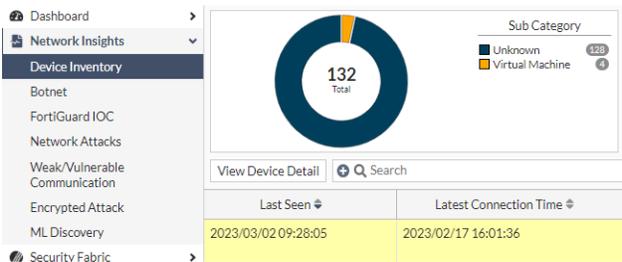


## Overwriting the device identifier

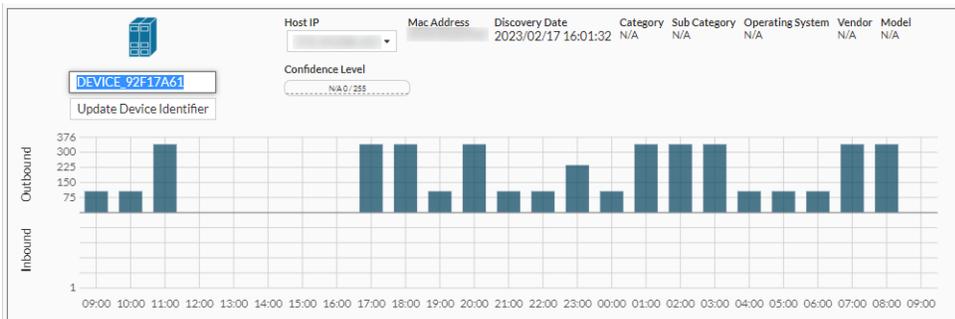
You can manually overwrite the device identifier in the device information page.

### 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.

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

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.

<b>Active Directory Server Ping Test</b>	Ping the Active Directory (AD) server and port in the Device Enrichment Profile.
<b>Active Directory Server Connection Test</b>	Verify the <i>Microsoft Active Directory Connection Settings</i> by attempting to connect the AD server.
<b>Active Directory Server Manual Run</b>	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>.
```

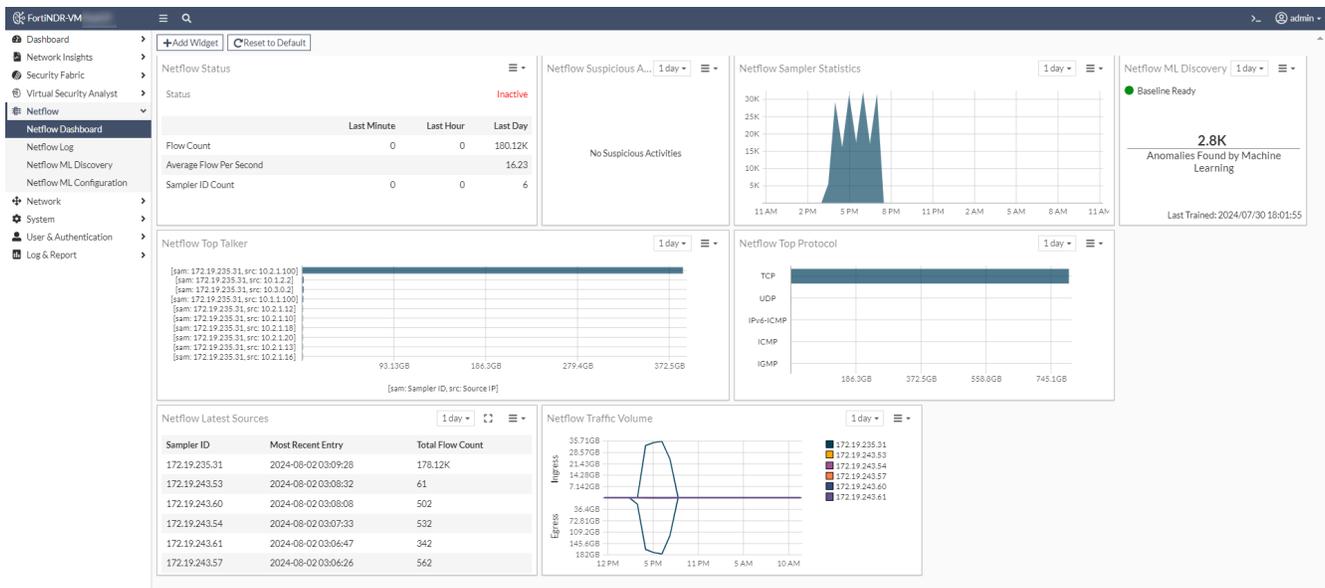
## NetFlow ports

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** 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.
- 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* 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 anomalies detected during the selected time period.

- To view the current Netflow ML baseline configuration, go to *Netflow > Netflow ML configuration*.
- To view the anomalies detected, 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 then 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 *0s* in them. This means this column is not applicable to that type of flow or the sampler/exporter is not configured to send this field to FortiNDR. For example, NetFlow\_v5 does not include *Destination MAC*, so you will see *00:00:00:00:00:00* in the *NetFlow\_v5* column.

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	OSPF/IGP	224.0.0.5	172.19.246.1	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	OSPF/IGP	172.19.246.1	224.0.0.5	0	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.99	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.191	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	192.168.1.112	172.17.254.151	91	91
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	172.17.254.151	192.168.1.112	147	147
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	TCP	172.19.235.107	172.19.122.201	88	88
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	TCP	172.19.235.107	172.19.122.201	88	88
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.60	0	UDP	fe80::f602:70ff:fee8:737e	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	IPFIX	Egress	172.19.235.56	0	UDP	fe80::a39d:caac:4ae5:9ccf	ff02::1	272	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.191	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	239.255.255.250	172.19.122.191	0	0
1970/01/20 01:08:37	NETFLOW_V9	Ingress	172.19.122.201	1	UDP	192.168.1.112	172.17.254.151	65	65

## Viewing anomalies

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

Netflow
Back

**Not Anomaly**

**Netflow Information**

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

**Device Information**

<table style="width: 100%; border-collapse: collapse;"> <tr><td>Source IP Address</td><td>0.0.0.0</td></tr> <tr><td>Source MAC Address</td><td>00:00:00:00:00:00</td></tr> <tr><td>Source Port</td><td>68</td></tr> <tr><td>Source VLAN ID</td><td>N/A</td></tr> <tr><td>In Bytes</td><td>3.09 KB (3090 B)</td></tr> <tr><td>In Packets</td><td>10</td></tr> </table>	Source IP Address	0.0.0.0	Source MAC Address	00:00:00:00:00:00	Source Port	68	Source VLAN ID	N/A	In Bytes	3.09 KB (3090 B)	In Packets	10	↔	<table style="width: 100%; border-collapse: collapse;"> <tr><td>Destination IP Address</td><td>255.255.255.255</td></tr> <tr><td>Destination MAC Address</td><td>00:00:00:00:00:00</td></tr> <tr><td>Destination Port</td><td>67</td></tr> <tr><td>Destination VLAN ID</td><td>N/A</td></tr> <tr><td>Out Bytes</td><td>0 B</td></tr> <tr><td>Out Packets</td><td>0</td></tr> </table>	Destination IP Address	255.255.255.255	Destination MAC Address	00:00:00:00:00:00	Destination Port	67	Destination VLAN ID	N/A	Out Bytes	0 B	Out Packets	0
Source IP Address	0.0.0.0																									
Source MAC Address	00:00:00:00:00:00																									
Source Port	68																									
Source VLAN ID	N/A																									
In Bytes	3.09 KB (3090 B)																									
In Packets	10																									
Destination IP Address	255.255.255.255																									
Destination MAC Address	00:00:00:00:00:00																									
Destination Port	67																									
Destination VLAN ID	N/A																									
Out Bytes	0 B																									
Out Packets	0																									

**Additional Information**

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

**Detection Information**

AnomalyEntryTime	Name	Tag	Severity

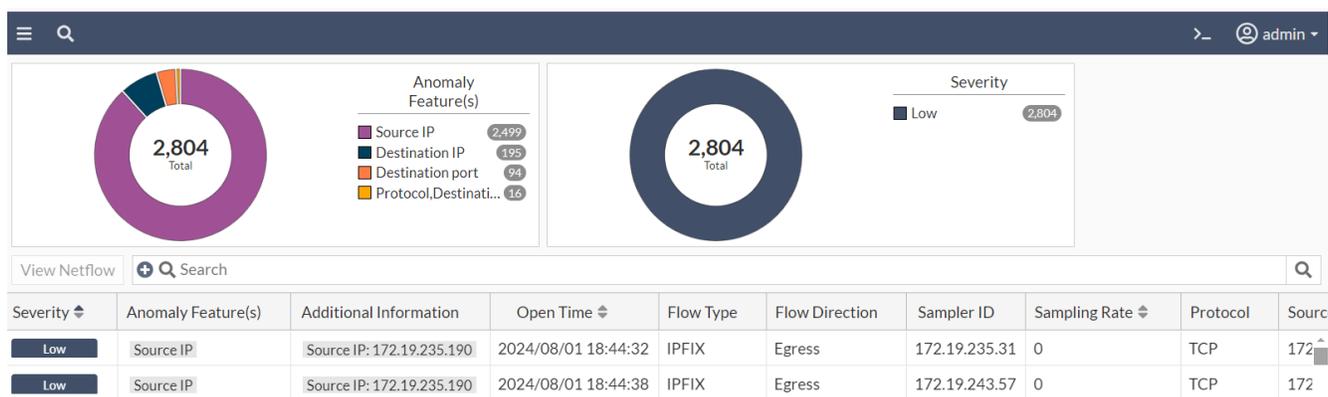
The anomalies page displays the following information:

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

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

## Netflow ML discovery

The *Netflow ML Discovery* monitor displays a list of anomalies 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.

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

<b>Destination Address</b>	The destination IP.
<b>Destination Network</b>	The destination network.
<b>In Bytes</b>	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:

The screenshot displays a Netflow interface with a table of records and a detailed 'Flow Information' pane. The table has columns for Severity, Anomaly Feature(s), Additional Information, Open Time, and Flow ID. The 'Flow Information' pane is divided into sections: General, Flow Details, and Source Device Information.

Severity	Anomaly Feature(s)	Additional Information	Open Time	Flow ID
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:32	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:38	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:38	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:53	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:53	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:58	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:58	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:58	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:58	IPFI...
Low	Source IP	Source IP: 172.19.235.190	2024/08/01 18:44:58	IPFI...

Flow Information	
<b>General</b>	
Open Time	2024/08/01 18:44:32
Time Flow Start	2024/08/01 18:44:16
Time Flow end	2024/08/01 18:44:16
<b>Flow Details</b>	
Sampler ID	172.19.235.31
Flow Type	IPFIX
Flow Direction	1
Sampling Rate	0
In Bytes	729.27 KB (729266 B)
Out Bytes	0 B
Bytes	729.27 KB (729266 B)
Packets	4097
In Packets	4097
Out Packets	0
Protocol	TCP
<b>Source Device Information</b>	
Source IP Address	172.19.235.190
Source MAC Address	00:00:00:00:00:00

## 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 anomaly 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 anomaly detection.

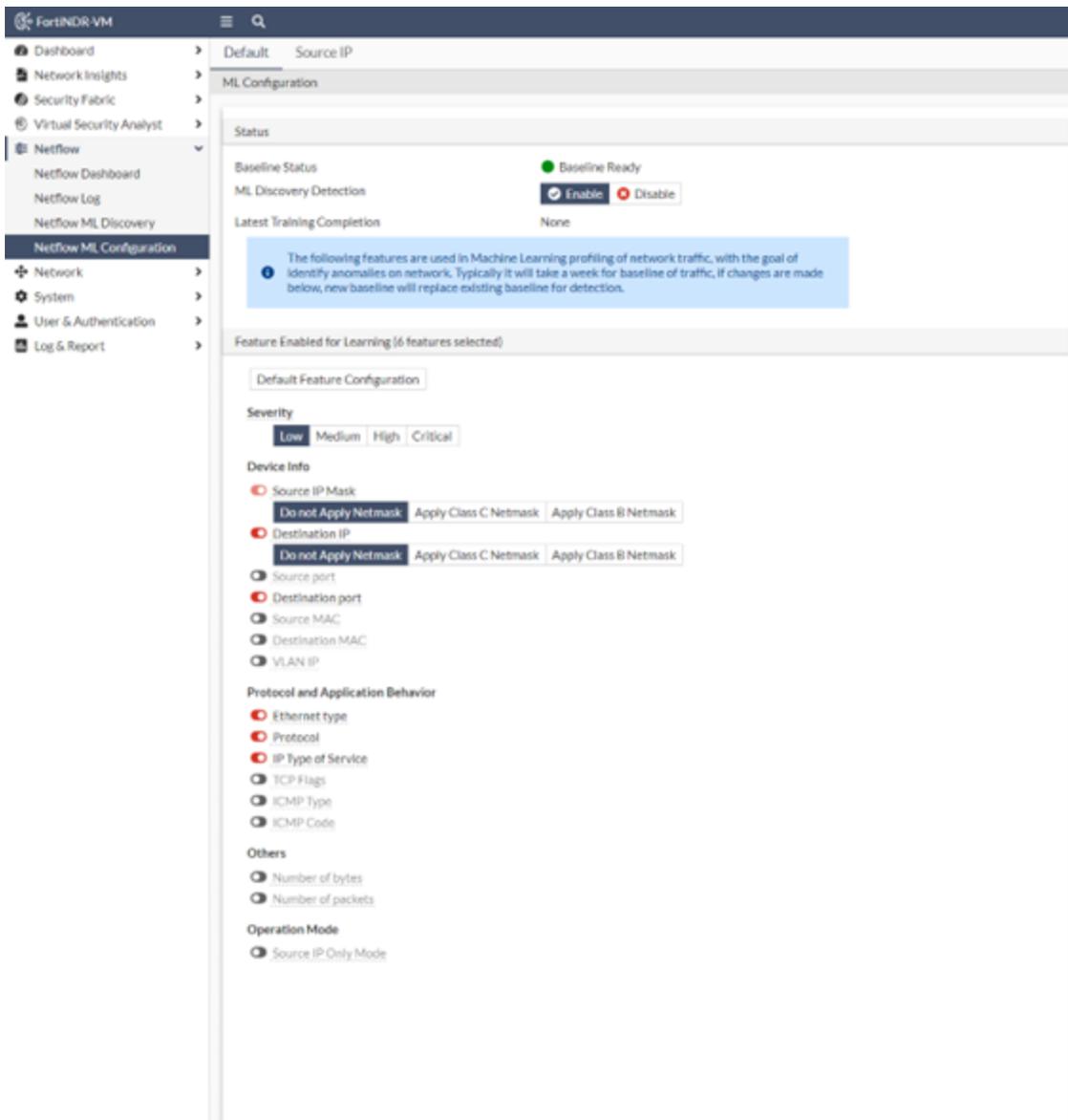
## Default tab

### To configure the ML Configuration profile:

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

<b>Status</b>	
<b>Baseline Status</b>	The current baseline training status: <ul style="list-style-type: none"> <li>• <i>Baselining</i>: The current training is still in progress.</li> <li>• <i>Baseline ready</i>: The baseline training is done and is ready for anomaly detection.</li> </ul>
<b>ML Discovery Detection</b>	Click to <i>Enable</i> or <i>Disable</i> baseline training.
<b>Latest Training Completion</b>	The date and time of the last baseline training.
<b>Feature Enabled for Learning</b>	
<b>Default Feature Configuration</b>	Click to enable the default ML configuration settings.
<b>Severity</b>	Select <i>Low</i> , <i>Medium</i> , <i>High</i> or <i>Critical</i> .
<b>Device Info</b>	
<b>Source IP Mask</b>	The Source Device IP. Apply a netmask if you do not want to treat certain range changes in the IP as an anomaly. Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Do Not Apply Netmask</i>: This is the default.</li> <li>• <i>Apply Class C Netmask: /24</i></li> <li>• <i>Apply Class B Netmask: /16</i></li> </ul>
<b>Destination IP</b>	The Destination Device IP. Apply netmask if you do not want to treat certain range changes in the IP as an anomaly Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Do Not Apply Netmask</i>: This is the default.</li> <li>• <i>Apply Class C Netmask: /24</i></li> <li>• <i>Apply Class B Netmask: /16</i></li> </ul>
<b>Source Port</b>	Port number such as, 22, 445, <i>none reserved port</i> , etc.
<b>Destination Port</b>	Port number such as, 22, 445, <i>none reserved port</i> , etc.
<b>Source MAC</b>	Source device MAC address.
<b>VLAN IP</b>	The VLAN IP.
<b>Protocol and Application Behavior</b>	
<b>Ethernet type</b>	Enable to monitor the Ethernet type.
<b>Protocol</b>	Enable to enter the protocol.
<b>IP Type of Service</b>	Enable to monitor the IP service type.

<b>TCP Flags</b>	Enable to monitor the TCP Flags.
<b>ICMP Type</b>	Enable to monitor the ICMP type.
<b>ICMP Code</b>	Enable to monitor the ICMP code.
<b>Others</b>	
<b>Number of Bytes</b>	FortiNDR categorizes Bytes into 3 groups: <ul style="list-style-type: none"><li>• Small: Less than 100 bytes</li><li>• Medium: 100-9999999</li><li>• Larger: Equal to and greater than 10000000 bytes</li></ul>
<b>Number of packets</b>	FortiNDR categorizes Packets into 3 groups: <ul style="list-style-type: none"><li>• Small: Less than 2</li><li>• Medium: 2-6249</li><li>• Larger: Equal to and greater than 6250</li></ul>
<b>Operation Mode</b>	
<b>Source IP Only Mode</b>	When enabled, ML will only monitor the traffic for IPs in the <i>Source IP</i> 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*.

<b>Device Info</b>	
<b>Source IP Mask</b>	The Source Device IP. Apply a netmask if you do not want to treat certain range changes in the IP as an anomaly. Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Do Not Apply Netmask</i>: This is the default.</li> <li>• <i>Apply Class C Netmask: /24</i></li> <li>• <i>Apply Class B Netmask: /16</i></li> </ul>
<b>Destination IP</b>	The Destination Device IP. Apply netmask if you don't want to treat certain range change in the IP as anomaly Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Do Not Apply Netmask</i>: This is the default.</li> <li>• <i>Apply Class C Netmask: /24</i></li> <li>• <i>Apply Class B Netmask: /16</i></li> </ul>
<b>Source Port</b>	Port number such as, 22, 445, none reserved port, etc.
<b>Destination Port</b>	Port number such as, 22, 445, none reserved port, etc.
<b>Source MAC</b>	Source device MAC address.
<b>VLAN IP</b>	The VLAN IP.
<b>Protocol and Application Behavior</b>	
<b>Ethernet type</b>	Enable to monitor the Ethernet type.
<b>Protocol</b>	Enable to enter the protocol.
<b>IP Type of Service</b>	Enable to monitor the IP service type.
<b>TCP Flags</b>	Enable to monitor the TCP Flags.
<b>ICMP Type</b>	Enable to monitor the ICMP type.
<b>ICMP Code</b>	Enable to monitor the ICMP code.
<b>Others</b>	
<b>Number of Bytes</b>	FortiNDR categorizes Bytes into 3 groups: <ul style="list-style-type: none"> <li>• Small: Less than 100 bytes</li> <li>• Medium: 100-9999999</li> <li>• Larger: Equal to and greater than 10000000 bytes</li> </ul>
<b>Number of packets</b>	FortiNDR categorizes Packets into 3 groups: <ul style="list-style-type: none"> <li>• Small: Less than 2</li> <li>• Medium: 2-6249</li> <li>• Larger: Equal to and greater than 6250</li> </ul>

# 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 174](#).

## DNS and Static Routes

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

# System

Use the *System* options to configure system settings.



It is recommended that you create a system backup file as part of your maintenance plan. Always perform a backup before upgrading firmware or making major system configuration changes. Save these configuration backups to your local computer in the event that you need to restore the system after a network event. For information, see [Backup or restore the system configuration on page 201](#).

## 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*.

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

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

## Password policy

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

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

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

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

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

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

### To create a system password policy the CLI:

```
config sys password-policy
config system password-policy
  set status enable
```

```

set apply-to admin-user
set minimum-length 8
set must-contain upper-case-letter lower-case-letter number non-alphanumeric
end

```

## Admin Profiles

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

## Pre-defined profile types

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

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

## Access Permissions

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

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

To create an Admin Profile:

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

Access Permissions	Description
System status	Grant permissions to settings critical to FortiNDR network accessibility, including GUI console, <i>Network</i> , <i>Administrators</i> , <i>Admin Profiles</i> , <i>Certificates</i> , and RADIUS/LDAP authentication.
System Access	Grant permission to modify other system settings such as system time

Access Permissions	Description
	settings, system FortiGuard update, and <i>Security Fabric</i> settings.
<b>System Configuration</b>	Grant permissions to access system maintenance settings such as back up system configuration, restore configuration, and restore firmware.
<b>System Maintenance</b>	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.
<b>Virtual Security Analyst</b>	Grant permissions to access settings in <i>Virtual Security Analyst</i> such as <i>Express Malware Analysis</i> , <i>Outbreak Search</i> , <i>Static Filter</i> , <i>NDR Muting</i> , <i>ML Configuration</i> , <i>Malware Big Picture</i> and <i>Device Enrichment</i> .

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

## Sensor Settings (- Center - Standalone)

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

The *Center Settings* page displays the following information:

<b>Hostname</b>	The sensor hostname.								
<b>IP Address</b>	The sensor IP address.								
<b>Model Name</b>	The sensor model name.								
<b>Serial Number</b>	The sensor serial number.								
<b>Status</b>	The connection status. <table border="1" data-bbox="560 1344 1459 1755"> <tbody> <tr> <td><b>Registered</b></td> <td>Indicates that the Sensor has completed the registration process but has yet to undergo a license check.</td> </tr> <tr> <td><b>Connected</b></td> <td>Indicates the Sensor is prepared for synchronization and is actively transmitting data to the Center.</td> </tr> <tr> <td><b>No Data Transferred</b></td> <td>Indicates the Sensor has not sent any data to the Center for a span of 3 minutes while still maintaining a connection.</td> </tr> <tr> <td><b>Firmware Mismatched</b></td> <td>Indicates the Sensor's firmware is incompatible with the Center, and the Sensor is currently disabled. This does not mean the Sensor is inoperative. However, the Center will not accept any data from it.</td> </tr> </tbody> </table>	<b>Registered</b>	Indicates that the Sensor has completed the registration process but has yet to undergo a license check.	<b>Connected</b>	Indicates the Sensor is prepared for synchronization and is actively transmitting data to the Center.	<b>No Data Transferred</b>	Indicates the Sensor has not sent any data to the Center for a span of 3 minutes while still maintaining a connection.	<b>Firmware Mismatched</b>	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.
<b>Registered</b>	Indicates that the Sensor has completed the registration process but has yet to undergo a license check.								
<b>Connected</b>	Indicates the Sensor is prepared for synchronization and is actively transmitting data to the Center.								
<b>No Data Transferred</b>	Indicates the Sensor has not sent any data to the Center for a span of 3 minutes while still maintaining a connection.								
<b>Firmware Mismatched</b>	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.								

	<b>Sensor License Invalid</b>	Indicates that the Sensor does not possess a valid license, and has been disabled.
	<b>Disabled By User</b>	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.
<b>FortiGuard Status</b>	Compares the Sensor's FortiGuard updates against the Center's FortiGuard updates. <i>FortiGuard Update Available</i> will appear if an update is required.	
<b>Last Updated</b>	The date the sensor was last updated.	
<b>CPU Usage</b>	The CPU usage as a percentage.	
<b>Disk Usage</b>	The disk usage as a percentage.	
<b>Memory Usage</b>	The memory usage as a percentage.	

The following options are available:

<b>Reboot Sensor</b>	Initiates a reboot command for the selected Sensor.
<b>Ping Sensor</b>	Sends a ping command to the chosen Sensor, to test its connectivity.
<b>Disable Sensor</b>	Changes the status of the selected Sensor to <i>disabled</i> , preventing the Center from receiving further data. However, the historical data from the Sensor is retained.
<b>Activate Sensor</b>	Activates the sensor.
<b>Command History</b>	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.
<b>Backup Sensor Configuration</b>	Creates of a backup for the selected Sensor's Configuration.
<b>Restore Firmware</b>	Restores and updates the selected Sensor's Firmware.
<b>Upload VM License</b>	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:

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

## Firmware

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



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

```
execute cleanup ndr
```



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

### To update or restore the system firmware:

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

## Settings

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

### To configure the system settings:

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

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

The screenshot displays the configuration interface for a FortiNDR system. It is divided into two main sections: System Time and Administration Setting.

**System Time Section:**

- Host Name: FortiNDR-VM
- Current System Time: 2022/09/23 14:34:21
- Time Zone: (GMT-8:00)Pacific Time(US&Canada)
- Set Time: NTP (selected) and Setting Time Manually
- Select server: FortiGuard (selected) and Custom
- Sync Interval: 1 Minutes (1-1440)

**Administration Setting Section:**

- Idle Timeout: 45 Minutes

## SNMP

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

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

## Basic Configuration

### To configure SNMP in the GUI:

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

2. Configure the SNMP agent:
  - a. Enable *SNMP Agent* and configure the following settings:

<b>Description</b>	Description of the SNMP agent.
<b>Location</b>	The location of the FortiNDR.
<b>Contact</b>	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:

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

<b>User Name</b>	Enter the user name.
<b>Security Level</b>	Configure the security level: <ul style="list-style-type: none"> <li>• <i>No Authentication</i>: No authentication or encryption.</li> <li>• <i>Authentication</i>: Select the authentication algorithm and password.</li> <li>• <i>Authentication and Private</i>: Select both the authentication and encryption algorithms and password.</li> </ul>
<b>Hosts</b>	<i>IP Address</i> : Click the plus sign (+) to enter the IP address for each SNMP manager.
<b>Queries</b>	Enable or disable queries, then enter the port number that the SNMP managers will use.
<b>Traps</b>	Enable or disable traps, then enter the local and remote port numbers that the SNMP managers will use.
<b>SNMP Trap Events</b>	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. 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.

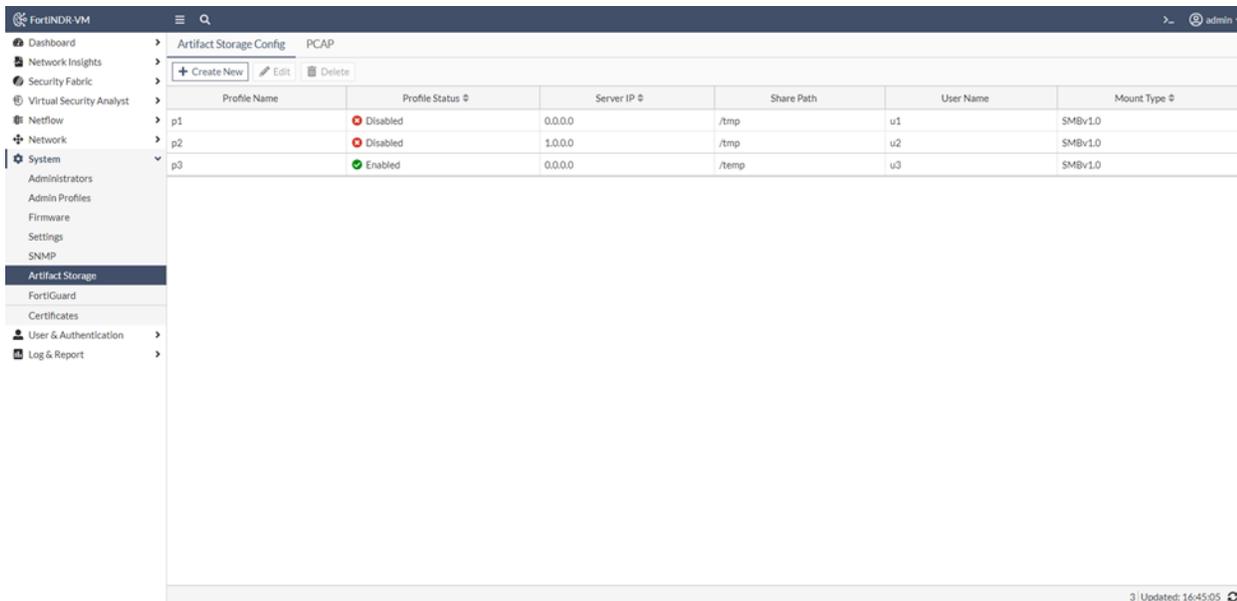
### Example:

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.

<b>Server IP</b>	Enter the server IP. This IP should be unique among all existing storage profile entries.
<b>Share Path</b>	Enter the share page for the profile. This path should be unique among all existed storage profile entries.
<b>Container Name</b>	Enter the container name.
<b>User name</b>	Enter the username for the profile.
<b>Password</b>	Enter the password for the profile and then confirm the password.
<b>Description</b>	Enter a description of the profile.

## PCAP tab

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

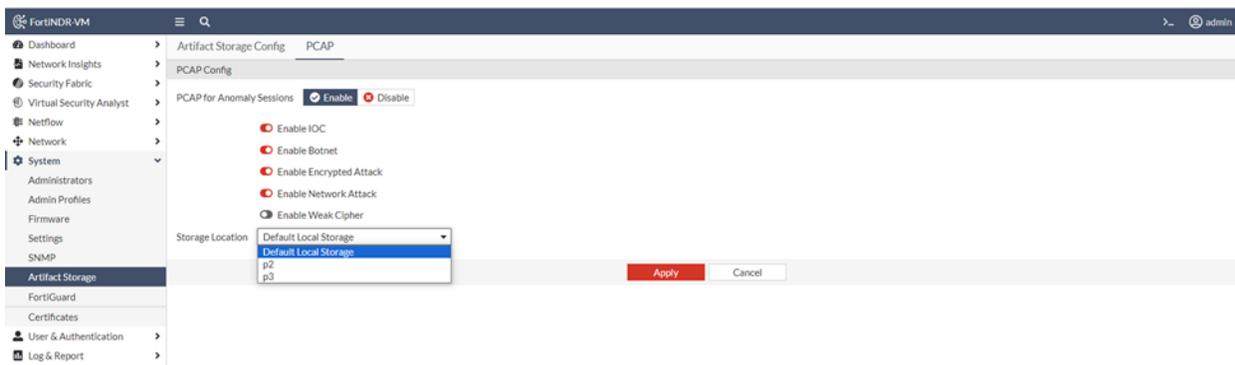


- The number of anomaly session captures and packets that can be collected will depend on the device model.
- This feature is not supported on VM models.
- The maximum size of each capture file is 1 MB.
- PCAP availability is commonly subject to latency.
- The tested FortiNDR-1000F max throughput when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

<b>PCAP for Anomaly Sessions</b>	Enable to configure the type of network anomaly event you want to capture as a PCAP file. Enabled by default.
<b>Enable IOC</b>	Enable to capture IOC events as a PCAP file. Enabled by default.
<b>Enable Botnet</b>	Enable to capture Botnet events as a PCAP file. Enabled by default.
<b>Enable Encrypted Attack</b>	Enable to capture Encrypted Attack events as a PCAP file. Enabled by default.
<b>Enable Network Attack</b>	Enable to capture Network Attack events as a PCAP file. Enabled by default.
<b>Enable Weak Cipher</b>	Enable to capture Weak Cipher events as a PCAP file.
<b>Default Local Storage</b>	Set the storage location for the PCAP files. The storage location options are pulled from the <i>Artifact Storage Config</i> tab. Only artifact storage profiles with the <i>Profile Status</i> set to <i>On</i> are listed.



An error message will appear when you click *Apply* when you enable PCAP for *Anomaly Sessions* without selecting a network anomaly event type.

## 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 275](#). 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 275](#) and [CLI guide](#) for more detail.

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

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

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



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

FortiNDR selects the update server based on proximity and location.

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

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

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

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

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

### To update the ANN database using the CLI:

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

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

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

In Windows:

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

In Linux:

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

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

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

4. Use the CLI command `execute restore kdb` to update the kdb. Run this command once for `pae_kdb.tar.gz` and once for `moat_kdb.tar.gz`.

For example, if `pae_kdb.tar.gz` and `moat_kdb.tar.gz` are in the FTP (IP:2.2.2.2) home folder of `/home/user/pae_kdb.tar.gz` and `/home/user/moat_kdb.tar.gz`, then use these commands:

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

This is an example of the output:

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

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

Entitlement	Version
<b>Binary AI 5</b>	
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
<b>Scenario AI 2</b>	
Scenario AI Engine	Version 1.000
Scenario AI DB	Version 1.001
<b>Text AI 5</b>	
Text AI Engine	Version 1.000
Text AI Learning Engine	Version 1.000
Text AI Feature DB	Version 1.001
Text AI Group DB	Version 1.001
Text AI Learning Feature DB	Version 1.001

### To schedule FortiGuard updates:

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

FortiGuard Updates

Manual Update  Check update  Update FortiGuard Neural Networks Engine

Scheduled Updates  Every  Hours

- From the frequency dropdown, select *Daily* or *Weekly*.
- In the *Hours* field a numeric fall for the frequency.
- 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 want 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.netupdate* 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
```

## Using FortiManager IOC/WebFilter query

FortiNDR can direct WebFilter and IOC queries to FortiManager. WebFilter queries will use the FortiManager's web filter database and IOC queries are proxied to FortiGuard servers.

**Requirements:**

- FortiManager v7.6.0

**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:

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

The following options are available:

<b>Generate</b>	Generate a certificate signing request.
<b>Download</b>	Download the certificate file.
<b>Set Default</b>	Set the default certificate.
<b>Import</b>	Import a local, CA or remote certificate.
<b>Delete</b>	Delete a certificate.
<b>View Details</b>	View the certificate details.
<b>Generate Report</b>	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*.

<b>Certification Name</b>	Enter the certificate name.
<b>Subject Information</b>	
<b>Certification Type</b>	Select <i>Host IP, Domain Name, or E-Mail</i> .
<b>IP</b>	Enter the certificate IP address.
<b>Optional Information</b>	
<b>Organization</b>	Enter the name of the organization issuing the certificate.
<b>Locality(City)</b>	Enter the city the certificate is issued in.
<b>State/Province</b>	Enter the state or province the certificate is issued in.
<b>Country</b>	Enter the country the certificate is issued in.
<b>E-mail</b>	Enter the email address of the person issuing the certificate.
<b>Key type</b>	Select the key type from the dropdown list.
<b>Key size</b>	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.



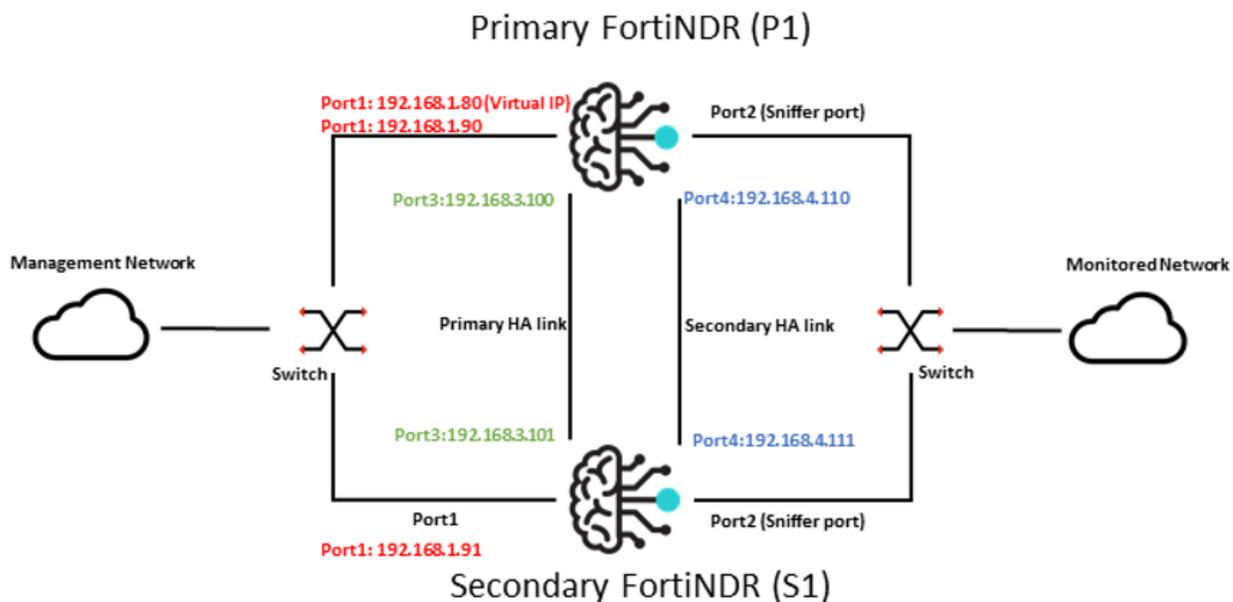
High Availability (HA) is only available in Standalone mode.

## 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 192](#).
- 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

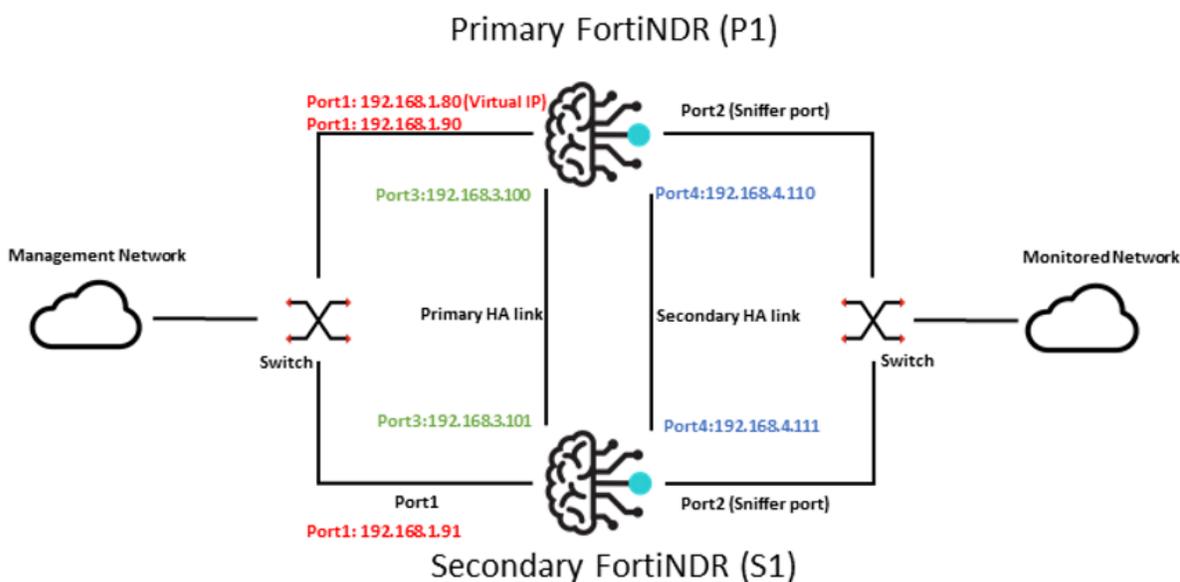
Before configuring an HA group, we recommend performing a factory reset or restoring the database on both FortiNDR primary and secondary units.



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 275](#)).



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

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

```
config system ha
  set mode primary
  set password xxx
  config interface
    edit port1
      set virtual-ip 192.168.1.80/24
      set action-on-primary use-vip
      set port-monitor enable
    end
```

```

    edit port3
      set heartbeat-status primary
      set peer-ip 192.168.3.101          << IP of secondary unit's port3
interface
  end
  edit port4
    set heartbeat-status secondary
    set peer-ip 192.168.4.111        << IP of secondary unit's port4 interface
  end
end
end

```

CLI option	Description
mode	<p>Enables or disables HA, selects the initial configured role:</p> <ul style="list-style-type: none"> <li>• <b>Off:</b> disable HA.</li> <li>• <b>Primary:</b> configured as primary Unit.</li> <li>• <b>Secondary:</b> configured as secondary Unit.</li> </ul>
password	<p>Enter an HA password for the HA group.</p> <p>You must configure the same password value on both the primary and secondary units.</p>
heartbeat-status	<p>Specify if this interface will be used for HA heartbeat and synchronization:</p> <ul style="list-style-type: none"> <li>• <b>Disable:</b> The interface is not used for HA heartbeat and synchronization.</li> <li>• <b>Primary:</b> We recommend to using port3 as the primary HA interface.</li> <li>• <b>Secondary:</b> We recommend having a secondary HA interface to improve availability. Use port4 as the secondary HA interface.</li> </ul>
peer-ip	<p>When configuring primary HA interfaces:</p> <ul style="list-style-type: none"> <li>• When configuring the primary unit, enter the IP address of the secondary unit's primary HA interface.</li> <li>• When configuring the secondary unit, enter the IP address of the primary unit's primary HA interface.</li> </ul> <p>The same rule should be applied when configuring the secondary HA interface.</p>
virtual-ip	<p>Enter the virtual IP address and netmask for this interface.</p> <p>If configured, this virtual IP can serve as the external IP of the HA group.</p> <p>When failover occurs, this setting will take effect on the new Primary unit. For details, see <a href="#">Using Virtual IP on page 199</a>.</p>
action-on-primary	<p><code>ignore-vip</code> [Default]: Ignore the Virtual IP interface configuration on the new Primary unit after failover.</p> <p><code>use-vip</code>: Add the specified Virtual IP address and netmask to the interface on the new Primary unit after failover.</p>
port-monitor	<p>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.</p> <p>This does not apply to heartbeat interfaces.</p>

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

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

5. Check the HA status of both units.
- Ensure the HA effective mode on both units has been updated successfully.
  - Check the HA status details. See, [Check HA status on page 195](#).
  - Ensure no errors appear on the HA event log. See, [HA Logs on page 199](#).

#### 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 198](#).
- 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
```

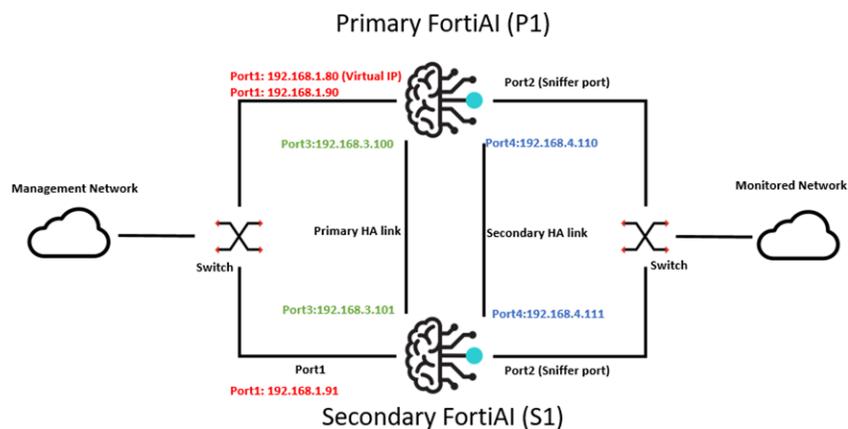
```
# get system status
Version: FortiAI-VM v1.5.2,buid120,211029 (Beta) (Debug)
Architecture: 64-bit
Serial-Number:
BIOS version: n/a
Log disk: Capacity 48 GB, Used 71 MB (0.15%), Free 48 GB
Data disk: Capacity 926 GB, Used 434 GB (46.88%), Free 492 GB
Remote disk: n/a
Memory: Capacity 31 GB, Used 27 GB (88.83%), Free 3590 MB
Swap Memory: Capacity 31 GB, Used 12 GB (37.95%), Free 19 GB
Hostname:
HA configured mode: Primary
HA effective mode: Primary
```

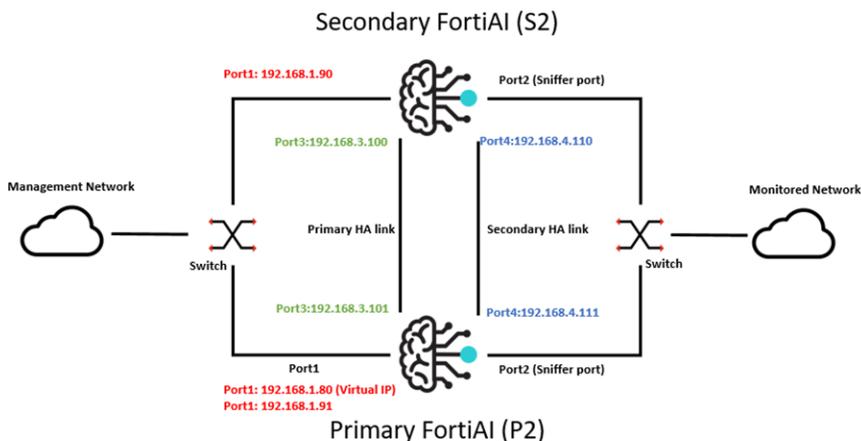
**To check the HA status with the GUI:**

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

## HA Failover

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

**Network topology before failover:**

**Network topology after failover:****Failover scenario 1: Temporary failure of the primary unit**

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

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

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

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



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

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

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

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



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

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

### Failover scenario 3: Heartbeat links fail

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

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

### Trigger HA failover using CLI

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

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

## HA configuration settings synchronization

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

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

## HA Logs

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



Once the HA group has been configured, the log data will be not synchronized from the Primary unit to the Secondary unit.

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

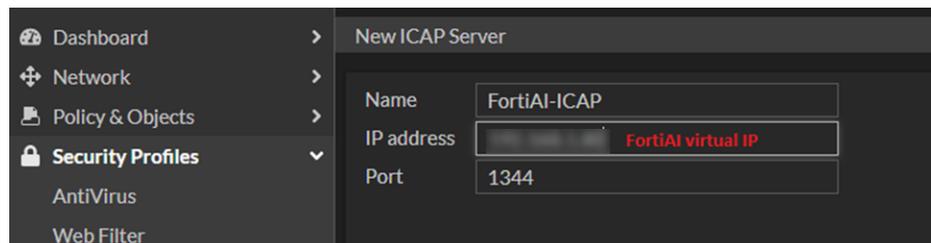
## Using Virtual IP

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

To use Virtual IP, you will need to configure and enable both the primary and secondary units with the same Virtual IP and netmask. To see an example of configuring a Virtual IP on interface port1, see [Configuring an HA group on page 192](#).

### 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.

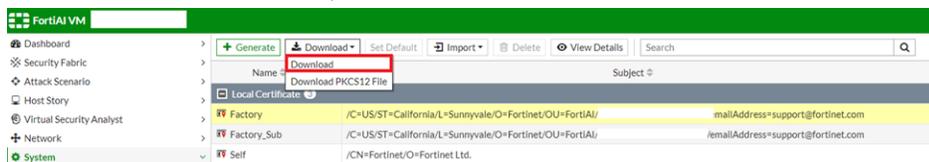


### Example: Configure FortiGate Security fabric settings for inline blocking

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.

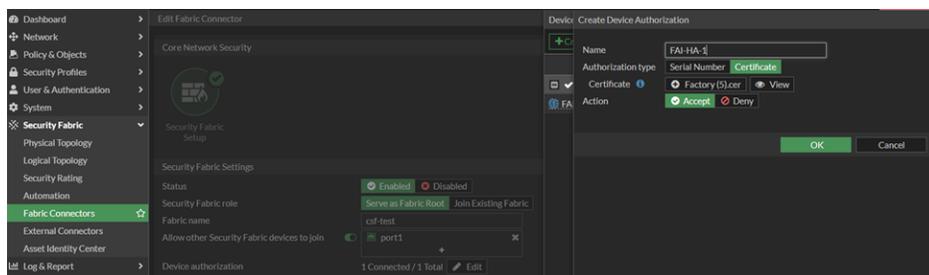
**To configure FortiGate for inline blocking:**

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



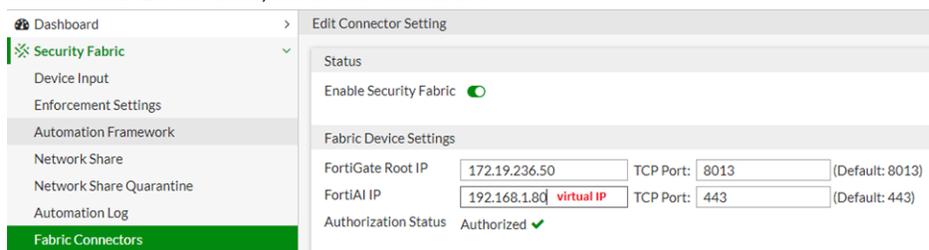
**To add the certificate to FortiGate**

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 130.

## 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 anomaly 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



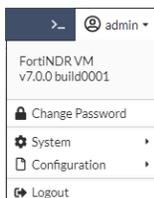
Please record these configuration settings before upgrading so the full configuration can be restored.

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

---

## RADIUS Server

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

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

The following options are available:

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

The following information is displayed:

<b>Profile Name</b>	The RADIUS server profile name.
<b>SERVER Name/IP</b>	The server name and IP address of the RADIUS server.
<b>Ref</b>	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.

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

## 4. Click OK.

## LDAP Servers

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

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

The following options are available:

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

The following information is displayed:

<b>Profile Name</b>	The LDAP server profile name.
<b>SERVER Name/IP</b>	The server name and IP address of the LDAP server.
<b>Port</b>	The port number for the server.
<b>Ref</b>	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.

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

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

4. Click *OK*.

**To edit an LDAP server:**

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

## LDAP user query example

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

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

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

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

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

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

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

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

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

## Alias member query example

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

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

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

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

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

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

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

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

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

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

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

## Preparing your LDAP schema for FortiNDR LDAP profiles

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

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



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

## Using common schema styles

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

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

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

# Log & Report



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

## Malware Log

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

Date	MD5	File ID	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk	Indicator
2023/08/01 13:50:19	ED63C3DA44EAF54E85B885CF66A74CADA	169664	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	
2023/08/01 13:50:19	8A5481689906C78AAFC63FE77A53ED8	169662	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	
2023/08/01 13:50:19	7DF8258FD025538313596694E28F0584	169659	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	IOC
2023/08/01 13:50:19	787F4398283F886DAD03263A3D17FE2	169655	HTML	HTML/RedirBA.INF:tr	Network Share		172.19.243.167	172.19.243.167	High (100%)	Medium	

The *Malware Log* contains the following tabs:

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

Each tab displays the following information:

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

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

## Download a sample

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

### To download a sample:

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

Sample 169636

VSA Verdict: Low Risk

Generic Trojan

Confidence level: 100%

Sample Information

Submitted Date	2023/08/01 13:50:19	Last Analyzed	2023/08/01 13:50:23
File Type	PE	File Size	15911(15.5 KB)
URL	//172.19.243.167/mal/c31d022f9c3dc06655d0d4951b8dcb2e		
File Name	c31d022f9c3dc06655d0d4951b8dcb2e		
MDS	C31D022F9C3DC06655D0D4951B8DCB2E VT		
SHA256	E699BA2868DEC FD2314FA576A695EB0765C3D6593AE33F1454138D3F9F7FEED2		
SHA1	448D7FF80E773134E2A6C0721D6586481587AF8F		
Detection Name	W32/CorruptRoopS/dam	Virus Family	N/A
Detected By	AV Engine		

Source Device

Device Type	Network Share
Network	
Attacker	172.19.243.167: N/A
Victim	172.19.243.167: N/A

1 Detection(s)

Feature Type	Appearance In Sample
Generic Trojan	1

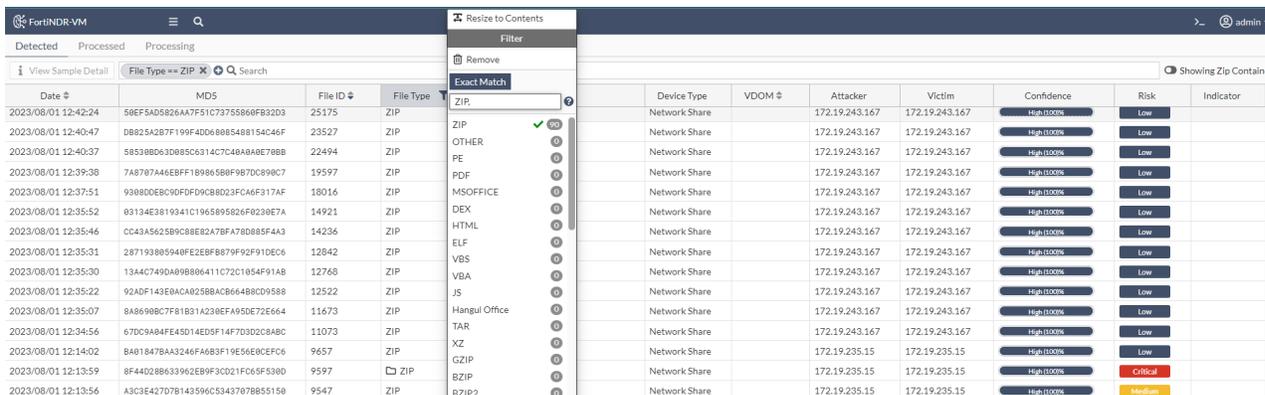
History

Date	MDS	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk
2023/08/01 13:50:19	C31D022F9C3DC06655D0D4951B8DCB2E	PE	W32/CorruptRoopS/dam	Network Share		172.19.243.167	172.19.243.167	100%	Low

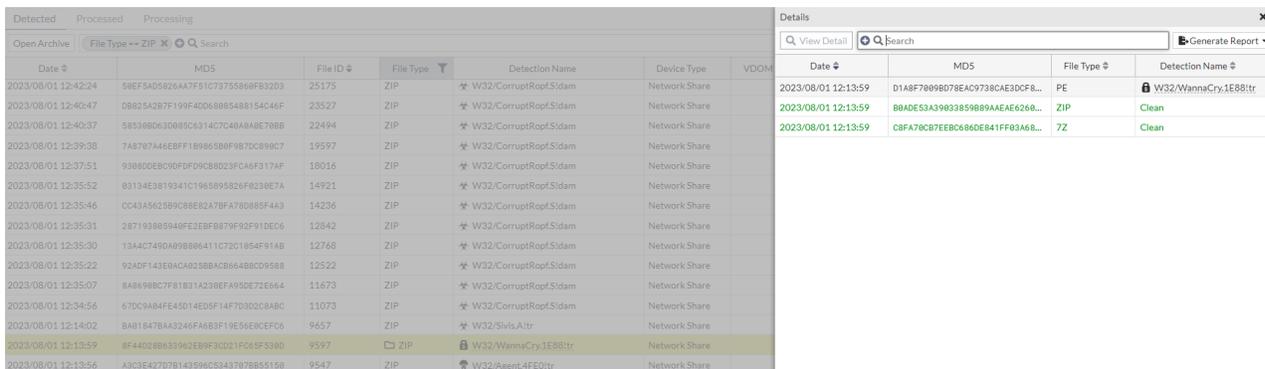
## View items in a zip folder

To view items in a zip folder:

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



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



## Perform a batch download

To perform a batch download:

- Select the files to download.
- 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:

- Go to *Log & Report > Malware Log*.
- Right-click a sample and select, *Add to Allow List*. The *Add to Allow List* pane opens. Optionally, you can click *View Sample Detail* and click *Add to Allow List*.

3. (Optional) In the *Comments* field, enter a comment about the detection.

Date	MD5	File ID	File Type	File Size	Detection Name	File Name	Device Type	VDOM	Attacker	Attac
2024/03/19 16:38:42	299607439888530488F4E5C7184FE197	39375	PE	4.1 kB	W32/Al.Suspicious.2	file_275.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	89843476858AFE89E40880D898E402D	39374	PE	4.1 kB	W32/Al.Suspicious.2	file_237.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	9E32882D93CB9A4A6EAF876F12E9F9F81	39373	PE	4.1 kB	W32/Al.Suspicious.2	file_85.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	750F2A2D801AD9F8E3F612C0296887D	39372	PE	4.1 kB	W32/Al.Suspicious.2	file_53.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	1CEFD20258783387F598D92EA7871C4E7	39371	PE	4.1 kB	W32/Al.Suspicious.2	file_214.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	181D6C4EA8BE12D8248551EE083E8C7	39370	PE	4.1 kB	W32/Al.Suspicious.2	file_49.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	A48AD696E4FF7D6D58A293FC7D1C3669	39369	PE	4.1 kB	W32/Al.Suspicious.2	file_151.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	8891166448F9878F8EAE96668048613	39368	PE	4.1 kB	W32/Al.Suspicious.2	file_128.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	8568EFC2E987973A938D338E6A562D9E	39367	PE	4.1 kB	W32/Al.Suspicious.2	file_113.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	BE9A1A71D4C8DC84BC0D8A8A2558347A	39366	PE	4.1 kB	W32/Al.Suspicious.2	file_108.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	28FA87B813A9FD4FE93E251FB362AF7	39365	PE	4.1 kB	W32/Al.Suspicious.2	file_33.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	8FE9FC3555C3350D54A81B671A50988F	39364	PE	4.1 kB	W32/Al.Suspicious.2	file_99.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	2EE6EE12502539DF9558963D9A05D132	39363	PE	4.1 kB	W32/Al.Suspicious.2	file_120.abc	Network Share		172.19.235.204	Intern
2024/03/19 16:38:42	DF7359FE36A8DEC510FC38599F4882	39362	PE	4.1 kB	W32/Al.Suspicious.2	file_232.abc	Network Share		172.19.235.204	Intern

Add to Allow List x

Mark as Clean

▲ Add Sample to Allow List

Comments

Submit feedback to FortiGuard

▲ Submit feedback to FortiGuard (includes new verdict and original file)

Contact Email

Comments

4. (Optional) Enable *Submit feedback to FortiGuard* and then enter your *Contact Email* and your feedback in the *Comment* field.

5. Click *OK*.

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

## Advanced search

You can search for detections with *Search* function or by right-clicking a detection and selecting an option from the menu. The *Search* function only supports exact matches. Wildcards are not supported.

### To use the search feature:

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

### To search a detection:

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

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

## NDR Log

The NDR Log view displays information anomalies detected on the network, traffic sources and destinations, as well as devices discovered and detected by FortiNDR.

Timestamp	Session ID	Anomaly Type	Source Address	Source Network	Destination Address	Destination Network	Severity	Transport Layer Protocol	Info
2024/12/02 13:53:24	7587253	Botnet Interactions	[REDACTED]	External	[REDACTED]	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:24	7587251	Network Attack/In...	[REDACTED]	Internal	[REDACTED]	Internal	Medium	TCP	Malicious File Downloading detected
2024/12/02 13:53:24	7587250	IOC Campaign	[REDACTED]	External	[REDACTED]	External	Critical	TCP	IOC: 'Malicious Websites' detected
2024/12/02 13:53:23	7587247	Network Attack/In...	[REDACTED]	Internal	[REDACTED]	Internal	High	TCP	CA BrightStor ARCserve Discovery Servic
2024/12/02 13:53:23	7587240	Network Attack/In...	[REDACTED]	External	[REDACTED]	External	Critical	TCP	CA BrightStor ARCserve Backup RPC Cod
2024/12/02 13:53:23	7587240	Network Attack/In...	[REDACTED]	External	[REDACTED]	External	Critical	TCP	CA BrightStor ARCserve Backup RPC Cod
2024/12/02 13:53:22	7587233	Network Attack/In...	[REDACTED]	Internal	[REDACTED]	Internal	Critical	TCP	CA BrightStor ARCserve Tape Engine RPC
2024/12/02 13:53:21	7587228	Network Attack/In...	[REDACTED]	External	[REDACTED]	External	High	TCP	ClamAV Mail Filter Crafted Recipient Cor
2024/12/02 13:53:21	7587226	Botnet Interactions	[REDACTED]	External	[REDACTED]	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:20	7587215	Network Attack/In...	[REDACTED]	Internal	[REDACTED]	Internal	High	TCP	Citrix IMA Invalid Event Data Length DoS
2024/12/02 13:53:20	7587211	Network Attack/In...	[REDACTED]	Internal	[REDACTED]	Internal	High	TCP	Citrix Access Gateway nsepacom ActiveX C
2024/12/02 13:53:20	7587206	Botnet Interactions	[REDACTED]	External	[REDACTED]	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:19	7587204	Network Attack/In...	[REDACTED]	External	[REDACTED]	External	High	UDP	Cisco Secure ACS EAP-TLS Authentication
2024/12/02 13:53:19	7587198	Network Attack/In...	[REDACTED]	External	[REDACTED]	External	Medium	TCP	Cisco AnyConnect VPN Client Software Sr
2024/12/02 13:53:19	7587198	Botnet Interactions	[REDACTED]	External	[REDACTED]	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:19	7587198	Botnet Interactions	[REDACTED]	External	[REDACTED]	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:19	7587197	Network Attack/In...	[REDACTED]	Internal	[REDACTED]	Internal	Medium	TCP	Cisco AnyConnect VPN Client Software Sr
2024/12/02 13:53:19	7587194	IOC Campaign	[REDACTED]	External	[REDACTED]	External	Critical	TCP	IOC: 'Malicious Websites' detected
2024/12/02 13:53:19	7587190	Network Attack/In...	[REDACTED]	External	[REDACTED]	External	High	TCP	CA eTrust Intrusion Detection Encryption
2024/12/02 13:53:18	7587187	Network Attack/In...	[REDACTED]	Internal	[REDACTED]	Internal	Critical	TCP	CA eTrust Intrusion Detection caller DLL /
2024/12/02 13:53:18	7587184	Network Attack/In...	[REDACTED]	External	[REDACTED]	External	Critical	TCP	CA Alert Notification Server Buffer Overfl
2024/12/02 13:53:18	7587184	Weak Cipher Algor...	[REDACTED]	External	95.178.142.122	External	High	TCP	Weak version of SMB Protocol detected

## Anomaly tab

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

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

Click *Download PCAP* to view Packet Capture information for the anomaly event. If the PCAP information is no longer available, an error message will appear.



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

Timestamp	Session ID	Anomaly Type	Source Address	Source Network	Destination Address	Destination Network	Severity	Transport Layer Protocol	Info
2024/12/02 13:53:19	7587204	Network Attack/Intrusion	...	Internal	...	External	High	UDP	Cisco Secure ACS EAP-TLS Authentication
2024/12/02 13:53:19	7587198	Network Attack/Intrusion	...	Internal	...	External	Medium	TCP	Cisco AnyConnect VPN Client Software S...
2024/12/02 13:53:19	7587198	Botnet Interactions	...	Internal	...	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:19	7587198	Botnet Interactions	...	Internal	...	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:19	7587197	Network Attack/Intrusion	...	Internal	...	Internal	Medium	TCP	Cisco AnyConnect VPN Client Software S...
2024/12/02 13:53:19	7587194	IOC Campaign	...	Internal	...	External	Critical	TCP	IOC: 'Malicious Websites' detected
2024/12/02 13:53:19	7587190	Network Attack/Intrusion	...	Internal	...	External	High	TCP	CA eTrust Intrusion Detection Encryption
2024/12/02 13:53:18	7587187	Network Attack/Intrusion	...	Internal	...	Internal	Critical	TCP	CA eTrust Intrusion Detection caller DLL f...
2024/12/02 13:53:18	7587184	Network Attack/Intrusion	...	Internal	...	External	Critical	TCP	CA Alert Notification Server Buffer Overfl...
2024/12/02 13:53:18	7587184	Weak Cipher/Vulnerable Protocol	...	Internal	...	External	High	TCP	Weak version of SMB Protocol detected
2024/12/02 13:53:18	7587183	Network Attack/Intrusion	...	Internal	...	Internal	Critical	TCP	CA Alert Notification Server Buffer Overfl...
2024/12/02 13:53:18	7587181	Network Attack/Intrusion	...	Internal	...	Internal	Critical	TCP	CA BrightStor ARCserve AddColum Activ...
2024/12/02 13:53:17	7587180	Botnet Interactions	...	Internal	...	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:17	7587179	Network Attack/Intrusion	...	Internal	...	Internal	Low	TCP	CA AV Engine CAB Header Parsing Buffer
2024/12/02 13:53:17	7587178	Botnet Interactions	...	Internal	...	External	Critical	TCP	'Botnet LokiBot' detected
2024/12/02 13:53:17	7587173	Network Attack/Intrusion	...	Internal	...	Internal	Critical	TCP	CA BrightStor ARCserve Backup XDR Par...
2024/12/02 13:53:17	7587172	Network Attack/Intrusion	...	Internal	...	External	Critical	TCP	CA BrightStor ARCserve Backup Tape Eng...
2024/12/02 13:53:16	7587164	Network Attack/Intrusion	...	Internal	...	External	High	TCP	CA BrightStor ARCserve Media Service Bl...
2024/12/02 13:53:16	7587163	Network Attack/Intrusion	...	Internal	...	Internal	High	TCP	CA BrightStor ARCserve Media Service Bl...
2024/12/02 13:53:16	7587158	Network Attack/Intrusion	...	Internal	...	Internal	High	TCP	CA BrightStor ARCserve Media Service Bl...
2024/12/02 13:53:15	7587150	Network Attack/Intrusion	...	Internal	...	Internal	Medium	TCP	CA ARCserve Backup DB Engine DoS dete...

## Session Tab

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

Open Time	Session ID	Source Address	Source Network	Destination Address	Destination Network	Severity	Application Layer Protocol
2024/12/02 17:00:32	7606023	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:59:26	7605905	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:58:56	7605716	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:58:56	7605714	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:57:05	7605554	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:55:18	7605355	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:55:15	7605354	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:54:26	7605280	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:54:08	7605239	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:53:56	7605209	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:53:56	7605205	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:53:56	7605206	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:53:44	7605196	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:53:37	7605186	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:53:26	7605169	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:53:26	7605167	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:51:50	7604992	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:51:26	7604951	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:49:13	7604601	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:48:56	7604580	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:48:56	7604578	...	Internal	...	Internal	Not Anomaly	NBT
2024/12/02 16:48:34	7604565	...	Internal	...	Internal	Not Anomaly	NBT

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

**Session 7603679**

**Activity**  
Network Service  
Application IPv6, ICMP  
Vendor Other

**Session Information**

Timestamp	2024/12/02 16:42:12
Transport Layer Protocol	ICMPV6
Application Layer Protocol	Other
Volume	64 (64 bytes)
VLAN ID	N/A
Sniffer Source Port	port2 (SNIFFER)
Technology	Network-Protocol
Is SCADA?	No
Cloud Service	None

**Device Information**

vmware	IP	fe80::250:56ff:fe8c:8483	↔	IP	fe80::1a5a:58ff:fec4:99e0
Link-local	Port	16384		Link-local	Port 136
Link-local	Packet Size	64		Link-local	Packet Size 0

**Certificate Information**  
No Certificate Found

**Activity**  
No Activity Found

**ML Discovery**  
No ML Feature Found

**--Action--**  
View Related Session by the Same Source Device  
View Related Session by the Same Destination Device  
View Related Anomaly by the Same Source Device  
View Related Anomaly by the Same Destination Device

Device  
Activity  
ML Discovery  
Detection  
Mitre ATT&CK

## 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*.

Anomaly	Session	Device	Last Seen	Latest Connection Time	Latest Address	Risk	Network	Device Identifier	MAC Address	Category	Status	Confidence
			2024/12/02 17:08:28	2024/11/29 14:48:53		No Risk	Link-local			Server	Online	Low (6.3%)
			2024/12/02 17:08:18	2024/11/29 14:43:40	10.152.192.208		Local			Unknown	Online	High (99.6%)
			2024/12/02 17:08:10	2024/11/29 14:53:12			Internal			Server	Online	Low (6.3%)
			2024/12/02 17:08:05	2024/11/29 14:43:53			Local			Server	Online	N/A (0%)
			2024/12/02 17:07:56	2024/11/29 14:43:40			Internal			Server	Online	N/A (0%)
			2024/12/02 17:07:53	2024/11/29 14:42:44		No Risk	Internal			Home & Office	Online	N/A (0%)
			2024/12/02 17:07:45	2024/11/29 14:42:39		Critical	Link-local			Server	Online	N/A (0%)
			2024/12/02 17:07:43	2024/11/29 14:44:41		No Risk	Internal			Server	Online	Low (6.3%)
			2024/12/02 17:07:41	2024/11/29 14:44:37		No Risk	Link-local			Home & Office	Online	Low (6.3%)
			2024/12/02 17:07:26	2024/11/29 14:43:08		No Risk	Internal			Unknown	Online	High (99.6%)
			2024/12/02 17:07:26	2024/11/29 14:43:08		No Risk	Internal			Network	Online	N/A (0%)
			2024/12/02 17:07:25	2024/11/29 14:44:34		No Risk	Link-local			Home & Office	Online	N/A (0%)
			2024/12/02 17:07:23	2024/11/29 14:43:07		No Risk	Link-local			Home & Office	Online	N/A (0%)

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

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

← Back
Device 1
Last 24 Hours
--Action--
Go

Host IP	Mac Address	Discovery Date	Category	Sub Category	Operating System	Vendor
10.2.1.16		2024/11/29 14:42:39	Server	Virtual Machine	N/A	Microsoft

Model	Confidence Level	Purdue Level	Purdue Source	Serial Number	Version	Product	Firmware
Virtual Machine	N/A/255	3.5	default	N/A	N/A	Windows_2000	N/A

DEVICE\_DDD78370

Update Device Identifier

Critical Risk Anomaly: 30930    Medium Risk Anomaly: 8.76K

High Risk Anomaly: 525.12K    Low Risk Anomaly: 868

HTTP.BROWSER	Other	HTTP	10.2.1.105	United States
Top Application	Top Service	Top Protocol	Top Neighbor	Top Geolocation

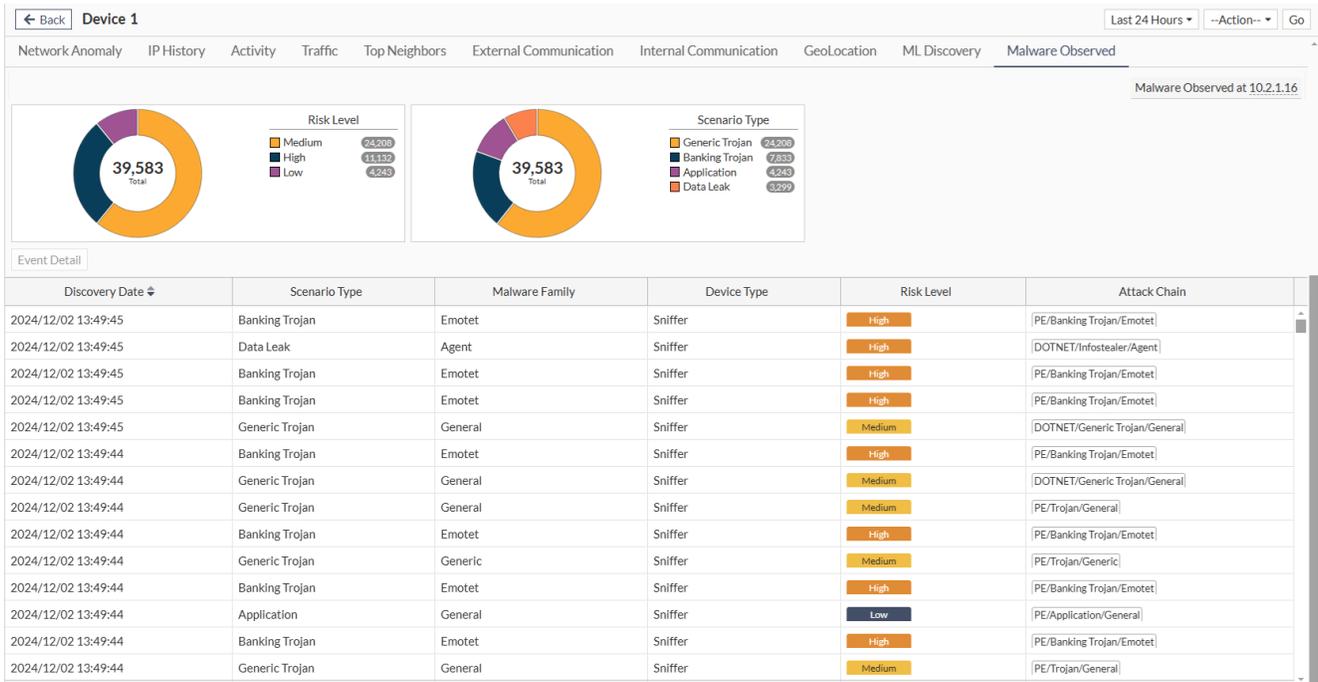
Lateral Connection   
  External Service   
  Multiple IP(s)

Network Anomaly
IP History
Activity
Traffic
Top Neighbors
External Communication
Internal Communication
GeoLocation
ML Discovery
Malware Observed

No ML training has finished yet

Date	Severity	Anomaly Type	Description	Source Address	Source Network	Destination Address	Destination Network
2024/12/02 13:53:24	Critical	Botnet Interactions	Botnet LokiBot detected		External		External
2024/12/02 13:53:24	Critical	IOC Campaign	IOC: 'Malicious Websites' detected		External		External
2024/12/02 13:53:23	Critical	Network Attack/Intrusion	'CA BrightStor ARCserve Backup RPC Code Execution' detected		External		External
2024/12/02 13:53:23	Critical	Network Attack/Intrusion	'CA BrightStor ARCserve Backup RPC Code Execution' detected		External		External
2024/12/02 13:53:21	High	Network Attack/Intrusion	'ClamAV Mail Filter Crafted Recipient Command Execution' detected		External		External
2024/12/02 13:53:21	Critical	Botnet Interactions	Botnet LokiBot detected		External		External
2024/12/02 13:53:20	Critical	Botnet Interactions	Botnet LokiBot detected		External		External
2024/12/02 13:53:19	Critical	Botnet Interactions	Botnet LokiBot detected		External		External

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.

Anomaly Session Device						Session Information
View Device	View Session	Download PCAP		No ML training has finished yet		Search
Timestamp	Session ID	Anomaly Type	Source Address	Source Network	Destination	
2024/12/02 13:53:24	7587253	Botnet Interactions	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:24	7587251	Network Attack/Intrusion	172.16.1.121	Internal	172.16.1.121	
2024/12/02 13:53:24	7587250	IOC Campaign	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:23	7587247	Network Attack/Intrusion	172.16.1.121	Internal	172.16.1.121	
2024/12/02 13:53:23	7587240	Network Attack/Intrusion	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:23	7587240	Network Attack/Intrusion	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:22	7587233	Network Attack/Intrusion	172.16.1.121	Internal	172.16.1.121	
2024/12/02 13:53:21	7587228	Network Attack/Intrusion	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:21	7587226	Botnet Interactions	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:20	7587215	Network Attack/Intrusion	172.16.1.121	Internal	172.16.1.121	
2024/12/02 13:53:20	7587211	Network Attack/Intrusion	172.16.1.121	Internal	172.16.1.121	
2024/12/02 13:53:20	7587206	Botnet Interactions	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:19	7587204	Network Attack/Intrusion	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:19	7587198	Network Attack/Intrusion	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:19	7587198	Botnet Interactions	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:19	7587198	Botnet Interactions	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:19	7587197	Network Attack/Intrusion	172.16.1.121	Internal	172.16.1.121	
2024/12/02 13:53:19	7587194	IOC Campaign	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:19	7587190	Network Attack/Intrusion	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:18	7587187	Network Attack/Intrusion	172.16.1.121	Internal	172.16.1.121	
2024/12/02 13:53:18	7587184	Network Attack/Intrusion	95.179.142.130	External	95.179.142.130	
2024/12/02 13:53:18	7587184	Weak Cipher/Vulnerable Protocol	95.179.142.130	External	95.179.142.130	

**Session Information** ✕

General Forensic

Download PCAP

Download PCAP Not Available

Endace

Endace Investigation link [https://www.example.com?datasources=tag%3Arotation-file&title=Pivot%20from%20FortiNDR&tools=trafficOverTime\\_by\\_app%20conversations\\_by\\_ipaddress&incidenttime=1733176403458547&rettime=5m&ip\\_conv=95.179.142.130%20%26%95.179.142.132](https://www.example.com?datasources=tag%3Arotation-file&title=Pivot%20from%20FortiNDR&tools=trafficOverTime_by_app%20conversations_by_ipaddress&incidenttime=1733176403458547&rettime=5m&ip_conv=95.179.142.130%20%26%95.179.142.132)

OK

## Events

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

The *Events* page displays the following information:

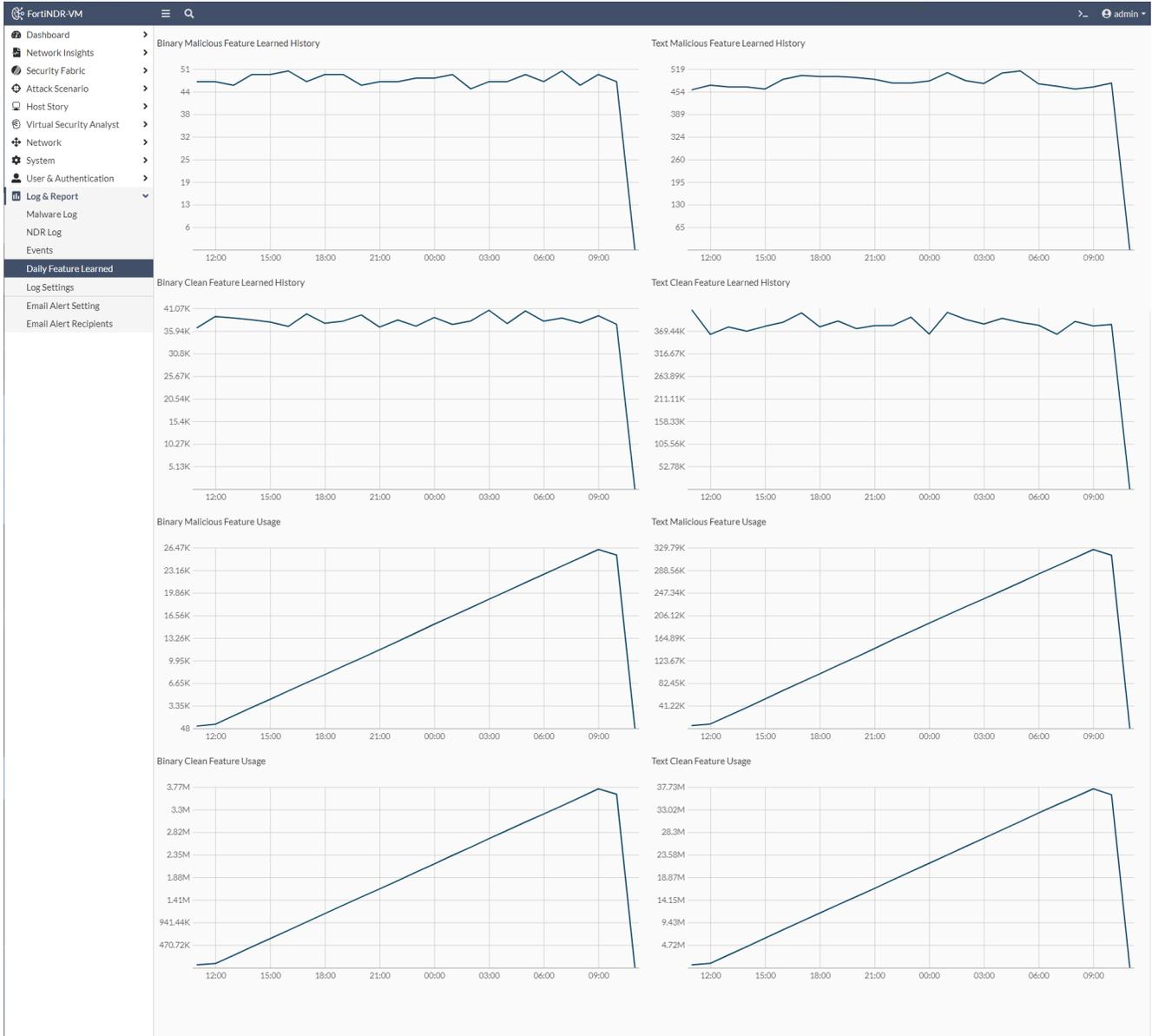
<b>Date</b>	The date the event occurred.
<b>Level</b>	The security level.
<b>User</b>	The user that triggered the event.
<b>Message</b>	The log message.

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

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

# Daily Feature Learned

This page in FortiNDR shows a graphical count of the features learned and used. The display includes the text and binary engines. This page is not available in Sensor mode.



## Log Settings

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

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



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

### Log Settings in Center mode

In Center mode, the Log Settings can be configured to send the Center's system event log to the syslog servers. Detection logs, including malware logs and NDR logs that record events occurring in the sensors, are sent directly from the sensors themselves. To upload and edit the sensor syslog configurations, go to *System > Sensor Settings* and click *Restore Configuration*. For more information, see [Sensor Settings \(Center Standalone\) on page 175](#).

#### To configure the Log Settings:

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

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

3. Click *OK*.

## Alert Email Setting

Go to *System > Alert Email Setting* to create email alert triggers when malware and system event threats are detected.

**To configure email alerts:**

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

<b>SMTP Server Address</b>	Enter the SMTP server address.
<b>Port</b>	Enter the port number.
<b>Sender's Email Account</b>	Enter the sender's email account
<b>Service Login Account</b>	Enter the service login account.
<b>Service Login Password</b>	Enter the service login password.
<b>Using Openssl</b>	Enable or disable open SSL
<b>Trigger Setting</b>	<p>Select an option(s) from the list and enter the email message text. If now text is provided, the default trigger message will be sent.</p> <p>Select the <i>Trigger Sensitivity</i> where required.</p> <ul style="list-style-type: none"> <li>• <i>HA Related Events</i></li> <li>• <i>Generic System Information including high cpu / low memory, notifications about file upload etc</i></li> <li>• <i>(VM Only) License Expired</i></li> <li>• <i>Scenario Detection Events</i> Set the <i>Trigger Sensitivity equal and above to Low Risk, Medium Risk, High Risk, or Critical Risk (default)</i>.</li> <li>• <i>NDR: Botnet Anomaly</i></li> <li>• <i>NDR: Encrypted Attack</i></li> <li>• <i>NDR: Indication of Compromise Detection</i></li> <li>• <i>NDR: Network Attack Detection</i> Set the <i>Trigger Sensitivity equal and above to Low Risk, Medium Risk, High Risk, or Critical Risk (default)</i>.</li> <li>• <i>NDR: Weak Cipher and Vulnerable Protocol Detection</i> Set the <i>Trigger Sensitivity equal and above to Low Risk, Medium Risk, High Risk, or Critical Risk (default)</i>.</li> <li>• <i>NDR: Machine Learning Detection</i></li> <li>• <i>Netflow: Netflow Suspicious Activity</i></li> <li>• <i>Netflow: Netflow Machine Learning Detection</i></li> </ul>

3. Add email addresses to the email recipient list. See, [Email Alert Recipients on page 222](#).

## Email Alert Recipients

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

**To add recipients to an email list:**

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

## NDR logs samples

### Botnet

```
date="2022-02-09" time="16:43:13" tz="PST" logid="0602000001" devid="FAIVMSTM21000033"
type="ndr" subtype="Botnet" severity="high" sessionid=63313 alproto="DNS" tlproto="UDP"
srcip="18.1.2.2" srcport=10000 dstip="18.1.1.100" dstport=53 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	<p>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"</p> <p>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"</p>

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

## NetFlow logs samples

### suspicious-activity

```
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="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" vlandid=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"
```

# Troubleshooting

## FortiNDR troubleshooting tips

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

### Best practices:

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

### Recommended Debug Setup:

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

### General Debug Logs Retrieval

Scenario	CLI
Collect all crash logs from the	<code>diagnose debug crashlog &lt;crash_log_date&gt;</code>

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

## File scanning related issues

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

### To perform a general check:

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

### Troubleshooting HTTP2 issues from FortiGate v7.0 onwards:

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

## Manual Upload/API Submission/FortiSandbox Integration

### For all issues:

Start with a single file upload and fetch results from the same subnet as directed from where the client resides. See [Appendix A: API guide on page 255](#).

### To verify the process is successful:

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

- `diag debug enable`

and

- `diagnose debug application 7`

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

## File Submitted but not processed

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

- `diag debug enable`

and

- `diagnose debug process <process_name>`

## Information for support tickets

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

<b>Model Name</b>	What Model is your platform?
<b>Firmware Version</b>	Which Firmware is your platform?
<b>Always Reproducible</b>	True/False
<b>Reproducible Steps</b>	If this issue is reproducible, please include the steps to reproduce this issue.
<b>Actual Result vs Expected Results</b>	What are the expected results and actual results?
<b>Troubleshooting recommendations used</b>	Please describe the troubleshooting recommendations you attempted and the outcome.
<b>Crash Log output</b>	Run the following CLI command <code>crash_log_date</code> and provide the output. For more information see, <a href="#">diagnose debug</a> .
<b>Kernel Log output</b>	Record the output from <code>diag debug kernel display</code> . For more information see, <a href="#">diagnose debug</a> .
<b>Application Log Output</b>	Specified log output from affected application. For more information see, <a href="#">diagnose debug</a> .
<b>Database Error Log</b>	Record the log output from <code>diag deb database error-log</code>
<b>FortiNDR Event Log</b>	If configured with FAZ/FortiSIEM, please provide logs from FAZ/FortiSIEM. Otherwise, please include a screen shot from <i>Event</i> tab.
<b>Client-Side Log</b>	When FortiNDR acts as a server role (ICAP, OFTP and HTTP2 inline blocking etc.), please also include logs from the client side.
<b>System Status</b>	Provide the CPU and MEM usage when the issue occurs.
<b>FortiNDR configuration</b>	How many ports are configured/used? How many applications are used, and how are they configured?

If you have a backup configuration file, please include it in your support ticket. For more information, see [Backup or restore the system configuration on page 201](#).

<b>FortiNDR Load</b>	For configured applications, how much load are applied. For example: <ul style="list-style-type: none"> <li>• For AV, how many files are being sent to FortiNDR, and what is the file size distributions and file type distributions?</li> <li>• For NDR, what is the bandwidth for traffic and what is the distribution of application type?</li> </ul>
<b>For non-hardware platform:</b>	
<b>Virtual machine provisioning</b>	<ul style="list-style-type: none"> <li>• How many CPU/Mems are provisioned?</li> <li>• How was the disk provisioned: Thin, Thick etc.</li> </ul>
<b>Hosting hardware specifications</b>	CPU Model Number, RAM Channels, DISK model number.
<b>Physical hosting hardware load</b>	A historical log of host hardware status to indicate CPU and MEM usage

## FortiNDR health checks

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

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

### To turn network traffic detection on and off:

Run the following command:

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

**To turn sniffer malware detection on and off for troubleshooting:**

Run the following command:

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



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

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

Date	MDS	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk	Indicator
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	N/A (0%)	No Risk	
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78	N/A (0%)	No Risk	
2022/04/14 11:55:06	5E88DE1C3B112734A7B949938508B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2	N/A (0%)	No Risk	
2022/04/14 11:55:06	1B7C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	N/A (0%)	No Risk	

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

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

## Sniffer diagnosis

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



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

## Rebuild RAID disk

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

### To rebuild the RAID disk:

1. Plug the monitor and keyboard directly into FortiNDR.



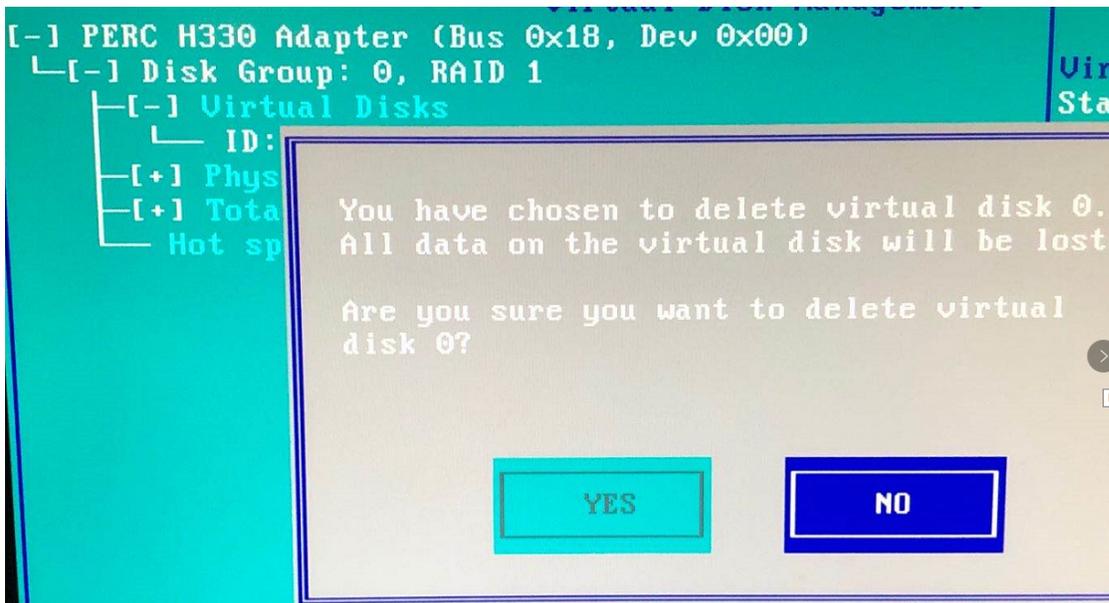
2. Boot FortiNDR and keep pressing `Ctrl R` when FortiNDR is booting.

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

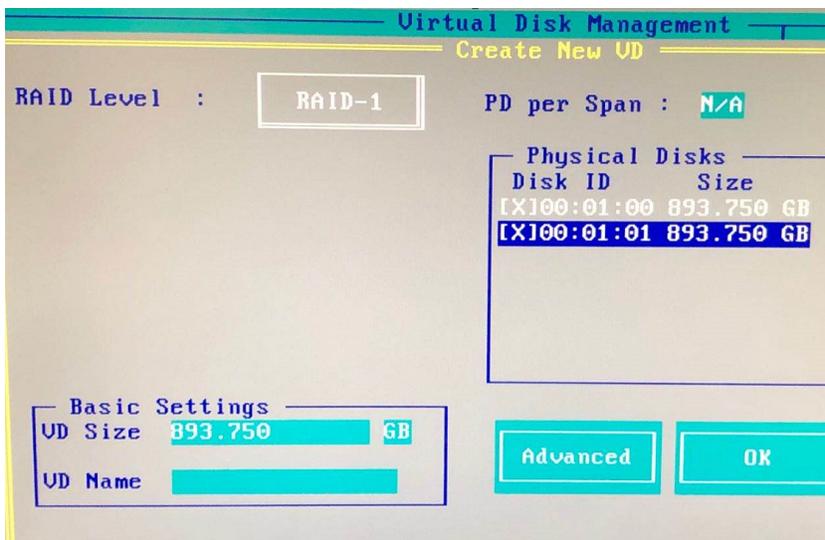
0 Non-RAID Disk(s) found on the host adapter
0 Non-RAID Disk(s) handled by BIOS

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

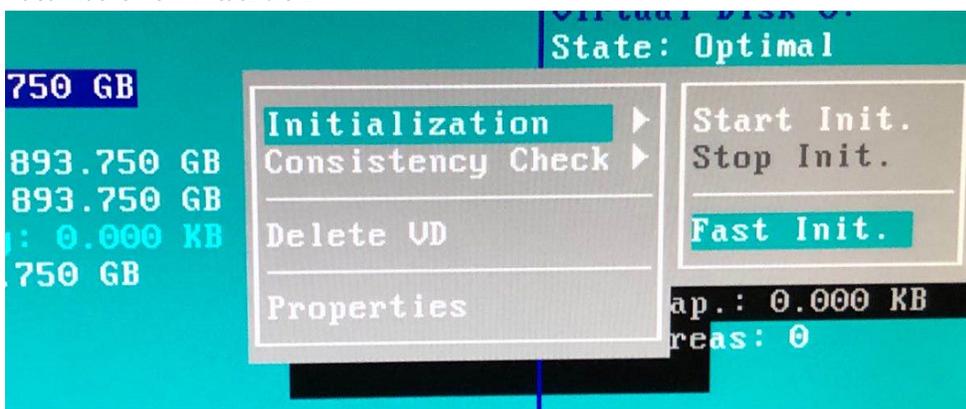
3. Delete virtual disk 0.



4. Create a virtual disk at RAID Level 1.



5. Fast init the new virtual disk.



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

COM2 - PuTTY

```

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

Serial number:FAI35FT319000006
Total RAM: 391680MB
Boot up, boot device capacity: 7916MB.
Press any key to display configuration menu...

[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter Selection [G]:

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

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

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

Please connect TFTP server to Ethernet port "0".

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

Total 412096kB unzipped.

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

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



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

## Managing FortiNDR disk usage for Center mode

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

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

## Managing FortiNDR disk usage for Standalone and Sensor mode

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

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

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

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

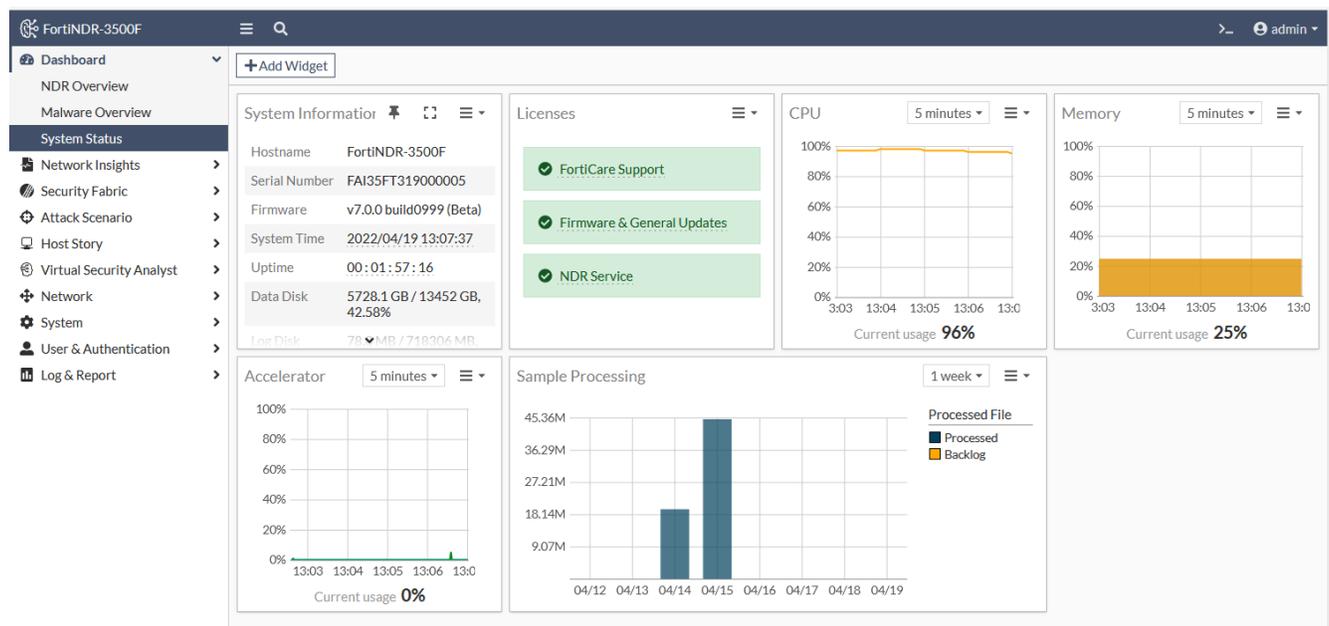
**Tip 2:** With FortiNDR 3500F, users can purchase more SSDs. Please see the data sheet and ordering guide for details.

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

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

**To view the disk usage:**

Go to *Dashboard > System Status*.



**To expand FortiNDR VM storage with the CLI:**

`execute expandspooldisk.`

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

**Exporting detected malware files**

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

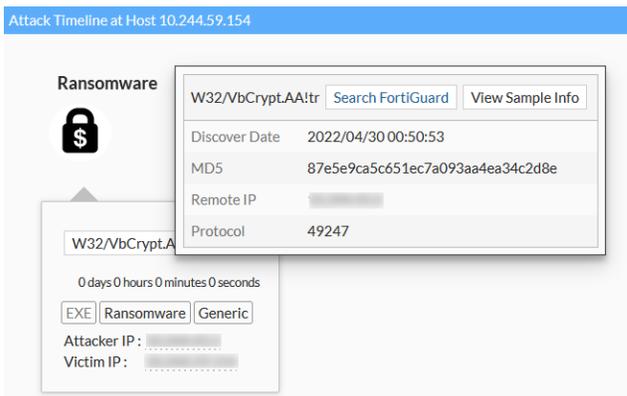
**To export detected malware files with the CLI:**

`execute export file-report`

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

**To export detected malware files with the GUI:**

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



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

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

VSA Verdict: **Critical Risk**

**Ransomware**

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

Confidence level: 100.00%

**Sample Information**

Submitted Date	2022/04/30 00:50:53	Last Analyzed	2022/04/30 00:56:16
File Type	EXE	File Size	6585(6.4 KB)
URL	N/A		
MD5	5F082212E8DDAE8ABAF941926BD60824 vt		
SHA256	0A1BBC20973E0691A9D35A9ABA610BFBECA45263C0A0E5A8ECBB A9AC5EE5E6996		
SHA1	99A4EB3D57268604D0758A904882CB406735CC8C		
Detection Name	W64/Encoder.A!tr	Virus Family	N/A

**Source Device**

Device Type	Sniffer
-------------	---------

**Network**

Attacker	(Registered port)	Victim
----------	-------------------	--------

1 Detection(s)

Feature Type	Appearance In Sample
Ransomware	1

**History** Similar Files View all History

Search View all History

Date	MD5	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Conf
2022/04/30 00:50:53	5F082212E8DDAE8ABAF941926BD60824	EXE	W64/Encoder.A!tr	Sniffer				

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

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

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

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

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

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

## Formatting the database

To format the database with the CLI:

```
execute db restore
```



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

## Export malware

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

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

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

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

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

The zip file default password is `infected`.

## Working with false positives and false negatives

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

To minimize false positive and negatives:

Recommendation	Description
<b>Ensure you are using the latest version of ANN</b>	To check the latest version of FortiNDR ANN, see the <i>Network Detection and Response Service</i> page at <a href="https://www.fortiguard.com/services/fortindr">https://www.fortiguard.com/services/fortindr</a> .
<b>Submit feedback to FortiGuard</b>	When you encounter a false positive (FP), you have the option to add the sample to the <i>Allow list</i> with the GUI. Furthermore, you can enable <i>Submit feedback to FortiGuard</i> to submit the sample directly to FortiGuard. For information, see <a href="#">Malware Log on page 210</a> .

## Troubleshoot ICAP and OFTP connection issues

**Troubleshooting ICAP issues:**

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

**Troubleshooting OFTP issues:**

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

**To check ICAP traffic in port1:**

Use the CLI command:

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

**To check OFTP traffic in port1:**

Use the CLI command:

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

**To verify a device is authorized:**

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

	Device Name	VDOM	IP Address	Connection Type	Authorized	Status
Network Share	FGT_VM_G3_235_78	global	172.19.235.78	OFTP	Disabled	Disconnected
Network Share Quarantine	FGT90E4Q17001555	global	172.19.122.201	OFTP	Enabled	Connected
Fabric Connectors	FGT90E4Q17001555:root	root	172.19.122.201	OFTP	Enabled	Connected
Enforcement Settings						
Automation Framework						

**To verify All Supported Files are enabled in FortiGate:**

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

The screenshot shows the 'Edit AntiVirus Profile' configuration page for 'fai\_antivirus'. Under the 'Inspected Protocols' section, various protocols are listed with toggle switches. In the 'APT Protection Options' section, the 'Send files to FortiSandbox for inspection' option is expanded, showing three choices: 'None', 'Suspicious Files Only', and 'All Supported Files'. The 'All Supported Files' option is selected and highlighted in green.

**To verify the firewall policy is not blocking the connection:**

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

## Troubleshoot Log Settings

**To troubleshoot the Client:**

- Enable *Send logs* to your syslog server
- Verify you are using a valid remote server address
- Check if the GUI settings match CMDB settings:
  - Send logs to FortiAnalyzer/FortiSIEM

Remote Log Server

Send logs to FortiAnalyzer/FortiSIEM  Enable  Disable

Type Syslog Protocol

Log Server Address

Port  (Default UDP: 514)

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

- Send logs to Syslog Server 1

Remote Log Server

Send logs to Syslog Server 1  Enable  Disable

Type Syslog Protocol

Log Server Address

Port  (Default UDP: 514)

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

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

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

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

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

FortiNDR-3500F (settings) #
```

**To view the traffic with the CLI:**

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

**To troubleshoot the server:**

- Verify the sever has rsyslog installed.
  - Make sure udp port 514 is open
- ```
sudo ss -tulnp | grep "rsyslog"
```

## Troubleshoot Network Share

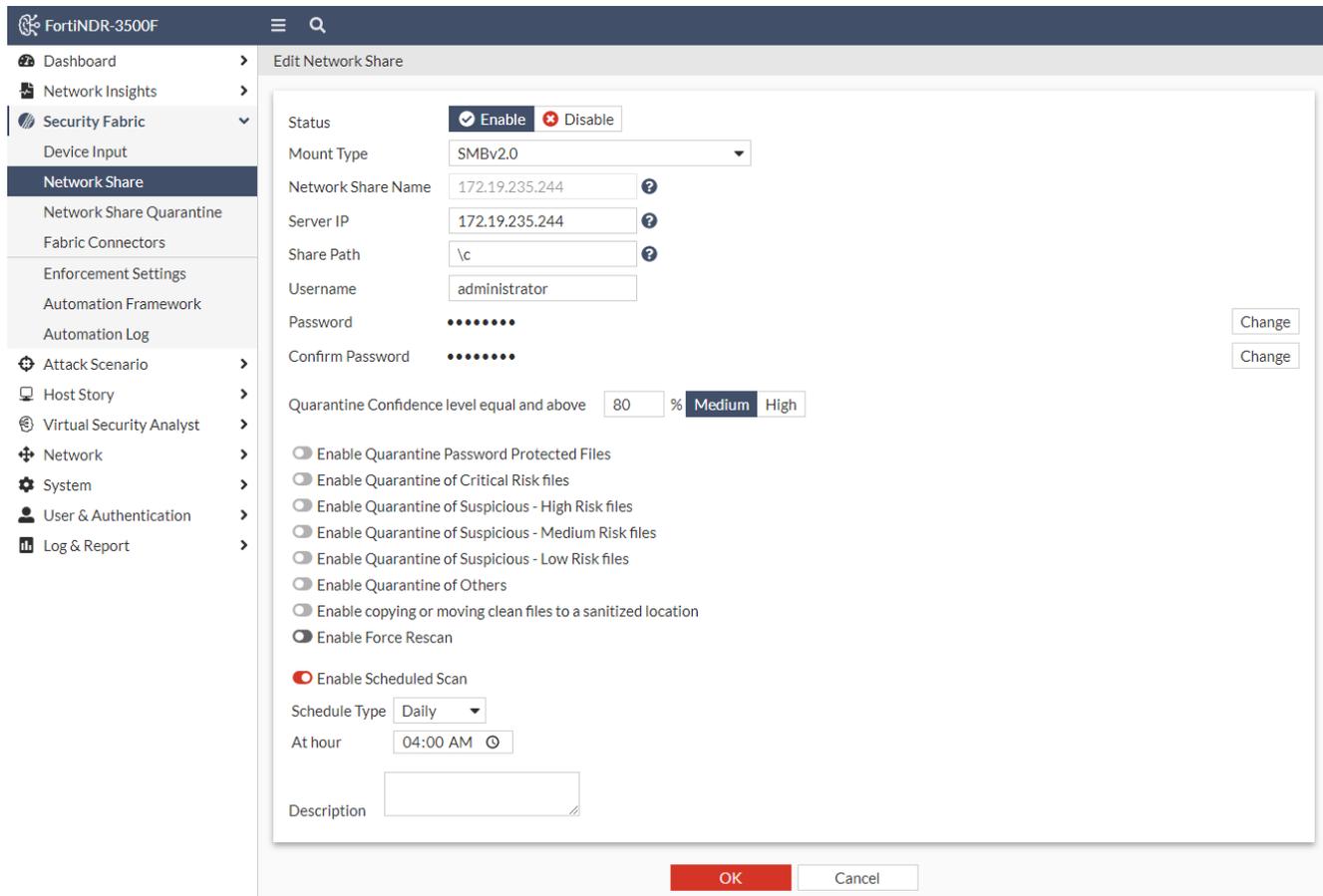
### Test the Network Share Connection

**To test the Network Share Connection:**

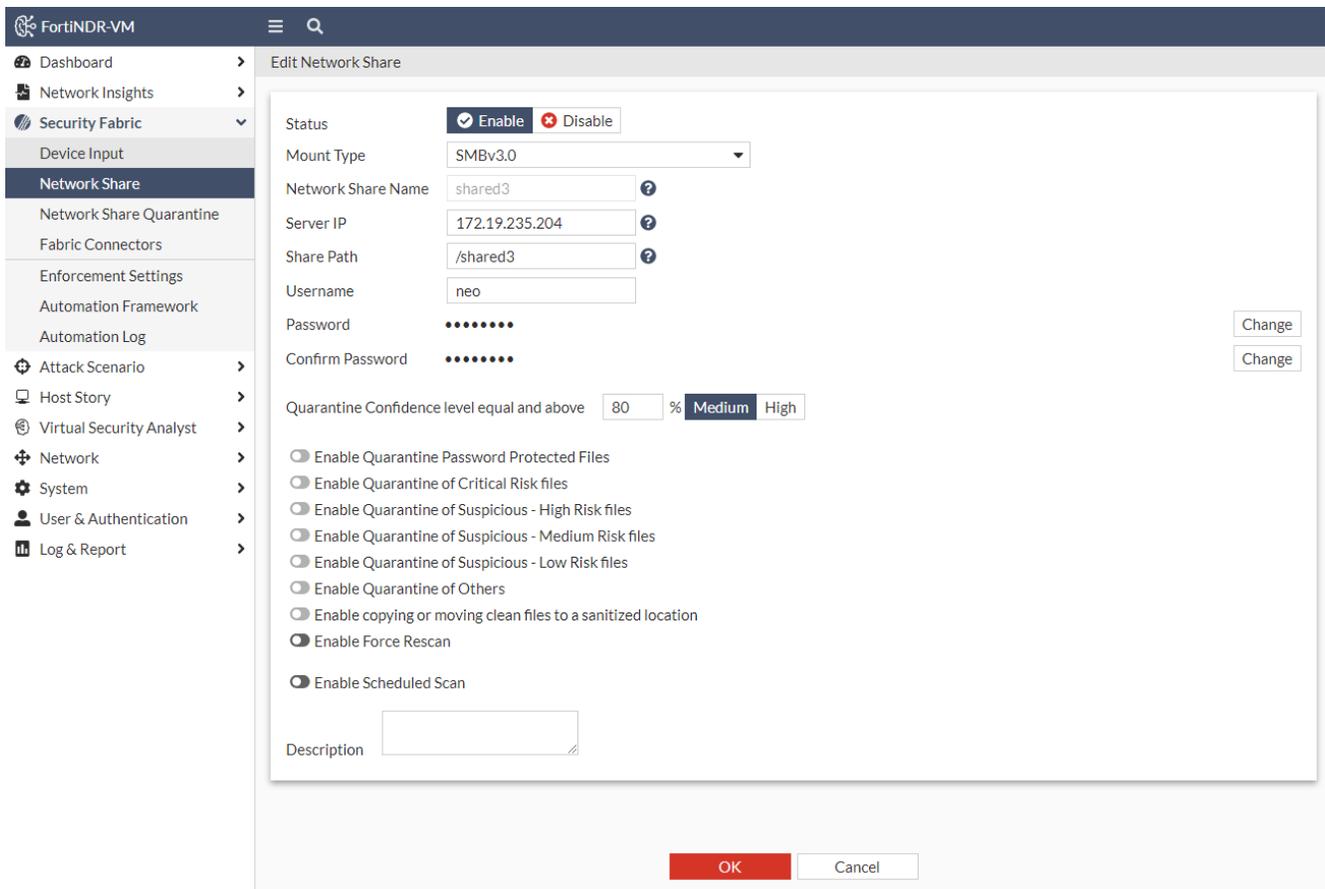
- Verify the Remote Sever is connectable
- Verify the folder to mount is shareable
- Verify the current user has read and write permissions to the shared folder.

- Verify you have chose the correct mount type, e.g. Windows 10 will not support SMB1.0 if SMB 1.0/CIFS File Sharing Support isn't turned on
- Verify the Share Path is using a backslash (\) for Windows Folders while forward (/) slash for Linux Folders

The following images shows the Network Share configuration for Windows.



The following images shows the Network Share configuration for Linux.



## Diagnosing Network Share Errors

### To diagnose Network Share scanning errors:

Run the following CLI commands:

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

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

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

### To troubleshoot mounting problems:

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

diagnose debug kernel display

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

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

You will see the error code if the mounting failed.

**To troubleshoot a Network Share scan that it is stuck:**

A scanning job may get stuck for the following issues:

| Issue                    | Recommendation                                                                                                                                  |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Mounting issue           | See <a href="#">To troubleshoot mounting problems</a> above.                                                                                    |
| Daemon crashed           | Run the following CLI command to see if there are any <code>sdigestd</code> related crashes:<br><code>diagnose debug crashlog xxxx-xx-xx</code> |
| Data disk usage over 90% | Clean up the data disk. See, <a href="#">Managing FortiNDR disk usage for Standalone and Sensor mode on page 237</a> .                          |

## Debug version image

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

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

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

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

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

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

## Check Crash Log

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

## Troubleshooting the VM License

### To view the status of the VM license:

```
diagnose system vm
```



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

### To verify the FDS (FortiGuard Distribution Services) server:

1. Use the following CLI command to list the FDS servers:  
`diagnose fds list`
2. Perform a traceroute to the FDS server IP to ensure the network route is not blocked:  
`execute traceroute <fds_ip>`
3. Replace <fds\_ip> with the actual IP address of the FDS server.

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

## Troubleshooting the updater

### FDS Authorization Failed

Go to the *System > FortiGuard*.

If the following databases show *FDS Authorization Failed*, that means the FortiNDR unit is using a FortiGuard License that does not include FortiNDR entitlements.

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

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

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

## Clearing updater cache files

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

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

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

Running the command and then try updating again:

```
exec update clean-up
```

This should solve that problem. Rebooting the machine will also trigger a FDS download cache-cleanup operation upon start up.

## Diagnosing Other FDS Errors

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

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

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

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

## Troubleshooting tips for Network File Share

To troubleshoot Network File Share issues:

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



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

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

```
exec ndr off
```

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

4. Turn off Sniffer daemon to isolate the environment using

```
exec snifferd off
```

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

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

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

6. Click *Test Connection*.

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

| Name        | Scan Scheduled | Type    | Share Path                 | Quarantine | Enabled  | Status |
|-------------|----------------|---------|----------------------------|------------|----------|--------|
| 208Document | No             | SMBv3.0 | //172.19.235.208/Documents | No         | Disabled | ✖      |
| 208Download | Yes            | SMBv3.0 | //172.19.235.208/Downloads | No         | Enabled  | ✔      |
| 208Music    | Yes            | SMBv3.0 | //172.19.235.208/Music     | No         | Enabled  | ✔      |
| 208Pictures | No             | SMBv3.0 | //172.19.235.208/Pictures  | No         | Disabled | ✖      |

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

- a. `exec deb kernel display`

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

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

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

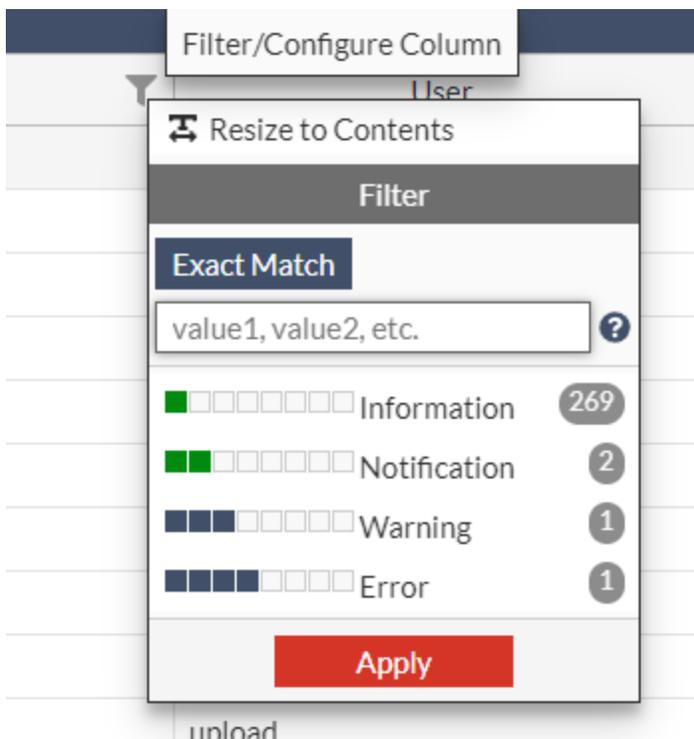
8. Get system status and save the output log to determine if the issue is related to storage.

```
get system status
```

```

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

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



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

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

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

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

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

For more information, see [Troubleshoot Network Share on page 244](#).

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

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

Here is an example showing which mount failed during mounting:

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

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

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

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

## Sensor logs not displaying in Center GUI

**To troubleshoot sensor logs not displaying in the GUI:**

1. Check if the sensors are included in the widget settings.
2. In the FortiNDR Overview dashboard, click *Reset to Default*.
3. Log out and then log back into the GUI.
4. Clear the browser cache.
5. As a last resort, use the CLI command: `execute factoryreset disk`

## Troubleshooting FortiNDR VM high CPU usage

Ensure you reserve a minimum of 60GHz CPU capacity for the VM if it is a cpu32 VM. For cpu16 VM, reserve at least 30GHz.

For Center mode VM, please reserve a minimum of 90GHz CPU capacity, 48vcpu and 384GB of memory.

Visit the host Summary page in the vSphere Client to check for Host CPU usage. If you see a warning, consider relocating other CPU-intensive virtual machines away from the same host of the FortiNDR VM. After doing so, reboot the FortiNDR VM.

## Troubleshooting inactive Netflow status

The *Netflow Status* widget displays *Inactive* when no flows are seen in the last five minutes.

**To diagnose an inactive Netflow status:**

1. Ensure FortiNDR's port UDP 2055, 6343, and 9995 are open. To monitor the packets, run the following CLI command:

```
diagnose sniffer packet
```

For example: `diagnose sniffer packet port1 'port 9995'`

2. Verify that HA mode is *off*. Netflow does not support HA: secondary mode.

Run the following CLI command:

```
get system status
```

```
Hostname: FNDR-1KF-
HA configured mode: Off
HA effective mode: Off
Strong-crypto: enabled
```

3. Check the logs to see if there are any crashes related to the flow daemon. The following CLI commands can retrieve logs:

```
diagnose debug crashlog <crash_log_date>
```

```
diagnose sys top
```

```
diagnose deb database error
```

4. Try reloading the daemon with the CLI:

```
execute reload [<daemon_name>]
```



If you use the command `execute netflow on`:

1. Be aware that it takes time for the daemon to activate after running `execute reload` and the daemon does not immediately indicate that it is on. We recommend waiting a few seconds before checking its status.
-

# Appendix A: API guide

This section explains how to use the FortiNDR API.

FortiNDR REST API currently supports the following:

- Files submission for scanning
- Retrieve files verdict result
- Get file STIX2 report
- Starting network share scan
- Events API support (detections based on source IP/Mac/hostname and anomaly type)

## Get an administrator API key

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

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

## Upload files using API

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

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

### To generate a token using CLI:

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

**To generate a token using GUI:**

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

The screenshot shows the 'Edit Administrator' page in the FortiNDR GUI. The left sidebar is expanded to 'System' and 'Administrator' is selected. The main content area has the following sections:

- Username:**
- Admin profile:**
- Authentication:**
- Preference**
  - Theme:**
  - Restrict login to trusted hosts
- API Key**
  - API key:

## 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.<br>Encode the file directly into the HTTP body as JSON data using the <code>file_content</code> field. |
| Multi-part file | The multi-part file does not need to be encoded in base64 format.                                                                                      |

| Method | Description                                             |
|--------|---------------------------------------------------------|
|        | Include the file in the HTTP body as a multi-part file. |

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

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

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

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

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

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

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

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

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

## Upload file by JSON data

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

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

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

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

```
requests.post(url='/api/v1/files',
              params={'access_token': 'u4VvEDpUATpJbFUfpbCz1SduTddCOIs'},
              data={'file_name': b64encode('samples.zip'),
                    'file_content': b64encode(open('samples.zip', 'rb').read()),
                    'password': 'xxxxxxxx'})
```

## Upload file by multi-part file

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

```
requests.post(url='/api/v1/files',
              params={'access_token': 'u4VvEDpUATpJbFUfpbCz1SduTddCOIs'},
              files={'samples.zip':open('samples.zip', 'rb')})
```

## Retrieve file verdict results

### /api/v1/verdict

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

The query string can only have one search query parameter.

### Examples

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

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

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

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

```
{
  "results": {
    "file_id": 5742600,
    "virus_name": "W32/Miner.VI!tr",
  }
}
```

```

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

```

| Field               | Description                                                                                                                                                                                                                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| file_id             | ID of the file.                                                                                                                                                                                                                                                                                                                         |
| virus_name          | FortiNDR virus name.                                                                                                                                                                                                                                                                                                                    |
| source              | For file uploaded by API or GUI, <i>source</i> is <i>manual upload</i> , otherwise it is an URL.                                                                                                                                                                                                                                        |
| severity            | <i>No Risk, Low, Medium, High, or Critical.</i>                                                                                                                                                                                                                                                                                         |
| category            | For clean file: <i>Clean</i> .<br>For malicious file, one of the following: <i>Generic Attack, Downloader, Redirector, Dropper, Ransomware, Worm, PWS, Rootkit, Banking Trojan, Infostealer, Exploit, Virus, Application, Multi, CoinMiner, DoS, BackDoor, WebShell, SEP, Proxy, Trojan, Phishing, Fileless, Wiper, or Industroyer.</i> |
| family              | FortiNDR virus family name.                                                                                                                                                                                                                                                                                                             |
| Feature_composition | JSON objects containing feature composition data for malicious file.<br><i>feature_type</i> is the category which the detected feature belongs to.<br><i>appearance_in_sample</i> is the number of appearances that the feature FortiNDR has detected.                                                                                  |

| Field        | Description                                                                       |
|--------------|-----------------------------------------------------------------------------------|
| confidence   | For clean file: <i>N/A</i> .<br>For other file: <i>Low, Medium, or High</i> .     |
| file_type    | <i>PE, PDF, MSOFFICE, HTML, ELF, VBS, VBA, JS</i> .                               |
| tmfc         | Reserved.                                                                         |
| pbit         | Debug only.                                                                       |
| parent_fname | The archive file name if the current file was extracted from an archive/zip file. |

### Example of problems retrieving results

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

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| http_code | See <a href="#">HTTP status table on page 261</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| message   | Messages include:<br><i>DATA_NOT_EXIST</i> when result data cannot be found given the search query parameter.<br><i>DATA_IN_PROCESS</i> when result data is still under process, such as after one submission, the accepted files have not been assigned file IDs. This might happen when uploading a big archive or compressed file.<br><i>INVALID_PARAM_NUMBER</i> when zero or more than one search query parameters exist.<br><i>INVALID_PARAM</i> when search query value is not valid. |

### Submitted file errors explanation:

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

- Oversized file
- Oversized archive contents

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

In the other following cases:

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

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

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

```

    "total_fileids": x
  }
}

```

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

In the following two cases:

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

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

## Get file stix2 report

### `/api/v1/report`

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

The query string can only have one search query parameter.

### Examples

```

GET /api/v1/report?fileid= ***file_id***
{
  "results": {
    *** STIX2 report content ***
  }
}

```

### HTTP status table

| HTTP code | Description                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 200       | OK: API request successful.                                                                                                               |
| 400       | Bad Request.                                                                                                                              |
| 403       | Forbidden: Request is missing authentication token, invalid authentication token, or administrator is missing access profile permissions. |

| HTTP code | Description                                                                 |
|-----------|-----------------------------------------------------------------------------|
| 404       | Resource Not Found: Unable to find the specified resource.                  |
| 405       | Method Not Allowed: Specified HTTP method is not allowed for this resource. |
| 413       | Request Entity Too Large.                                                   |
| 424       | Failed Dependency.                                                          |
| 500       | Internal Server Error.                                                      |

## Start Network Share scan

### /api/v1/nfs/scan

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

### Examples

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

### Example of failed to start Network Share scan

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

## Events API support

### /api/v1/events

| Query parameters | Description                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| ip               | Get anomaly events with device IPv4 or IPv6 address. User needs specify one of [ip, hostname, mac] in the request. |
| hostname         | Get anomaly events with device hostname. User needs specify one of [ip, hostname, mac] in the request.             |

| Query parameters | Description                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac              | Get anomaly events with device mac address. User needs specify one of [ip, hostname, mac] in the request.                                                                   |
| type             | Specify the anomaly type events, one of [botnet, 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 <i>executables, pdf_documents, office_documents, web_pages, compressed_archives, flash_files, android_files, mac_files, linux_files, others</i> |
| submission_source | A comma separated list of submission sources to search for; any of <i>http2, sniffer, fsa, fml, icap, manual_upload, oftp, network_share, cloud_storage</i> .                                                    |
| risk              | A comma separated list of risk levels to search for; any of <i>low, medium, high, critical</i> .                                                                                                                 |
| 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:<br>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=9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08,60303ae22b998861bce3b28f33eec1be758a213c86c93c076dbe9f558c11c752
```

```
{
  "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 <i>infected</i> . |

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.SSLError) as
e:

                valid = False

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

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

            else:
                parse_url (links)

    return (url_list_depth)

def load_file_for_upload(path_to_file):

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

    return gzip.compress(data)

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

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

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

    except subprocess.CalledProcessError as e:

```

```

        print(e)
        sys.exit(0)

    return (data)

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

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

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

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

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

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

                                except KeyError as e:
                                    next

                    print (results_metadata)

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

    except subprocess.CalledProcessError as e:

        sys.exit(0)

```

```
def parse_url (tmp_url):

    client = FAIApiClient_file(host)

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

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

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

                except Exception as e:
                    pass

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

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

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

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

def main(argv):
    locale.getpreferredencoding = getpreferredencoding

    urllib3.disable_warnings()
```

```
parser = argparse.ArgumentParser(description='Test upload files to 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 <a href="https://fndr.fortinet.com">fndr.fortinet.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 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<br>TCP 8890 (When using FortiManager) | Initial outbound to: <ul style="list-style-type: none"> <li>• <a href="https://fai.fortinet.net">fai.fortinet.net</a></li> <li>• <a href="https://globalupdate.fortinet.net">globalupdate.fortinet.net</a> (Default when Anycast is enabled)</li> <li>• <a href="https://fds1.fortinet.com">fds1.fortinet.com</a> (When Anycast disabled)</li> <li>• <a href="https://update.fortiguard.net">update.fortiguard.net</a> (When Anycast disabled)</li> </ul> For a complete list of the current FortiGuard update servers, use the CLI <code>diagnose fds list</code> .<br>To enable/disable Anycast, please use the CLI <code>config system fortiguard update</code> and then <code>set anycast to disabled</code> .<br>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<br>TCP 8888 (When using FortiManager) | Outbound to <a href="https://productapi.fortinet.com">productapi.fortinet.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Item                                     | Protocol and port number                     | Direction                                                                                         |
|------------------------------------------|----------------------------------------------|---------------------------------------------------------------------------------------------------|
| IOT lookup                               | TCP 443                                      | Outbound to <a href="https://globalguardservice.fortinet.net">globalguardservice.fortinet.net</a> |
| 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<br>TCP 8888 (When using FortiManager) | Outbound to <a href="https://service.fortiguard.net">service.fortiguard.net</a>                   |

## 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).

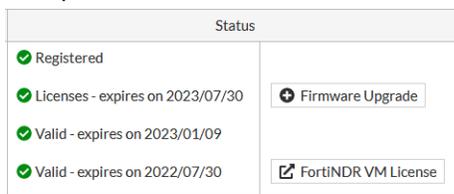
| Detection Techniques                      | Supports offline manual update | Comments                                                                                     |
|-------------------------------------------|--------------------------------|----------------------------------------------------------------------------------------------|
| 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.                                                    |

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

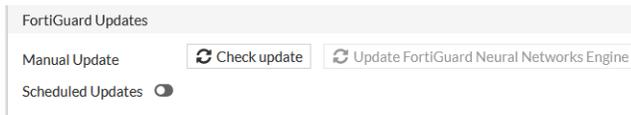
## Updating the ANN database from FDS for malware detection (GUI)

### To update the ANN database from FDS:

- Go to *System > FortiGuard*.
- 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*.



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



- 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      |
| <b>Binary AI 5</b>                     |               |                     |             |
| 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  |
| <b>Text AI 5</b>                       |               |                     |             |
| Text AI Engine                         | Version 1.000 | 2020/01/01 00:00:00 | Up to Date  |
| Text AI Learning Engine                | Version 1.000 | 2020/01/01 00:00:00 | Up to Date  |
| Text AI Feature DB                     | Version 1.000 | 2020/03/02 02:37:00 | Downloading |
| Text AI Group DB                       | Version 1.000 | 2020/03/02 02:37:00 | Downloading |
| Text AI Learning Feature DB            | Version 1.000 | 2020/03/02 02:37:00 | Downloading |

## Updating ANN for malware detection (CLI)

FortiNDR utilizes both FortiGuard updates to local DB as well as lookup for detecting network anomalies. FortiNDR comes with a trained ANN, but users can update it before placing solution live on network. The ANN version can be checked at FortiGuard webpage: <https://www.fortiguard.com/services/fortindr>. For full list of updates please refer to [Appendix D: FortiGuard updates on page 275](#) for details. The section below discusses one of the updates: ANN for malware detection.

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

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

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

### To update the ANN database using CLI:

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

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

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

```

/# fdisk /dev/sdc

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

Command (m for help): █

```

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

```

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

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

/# █

```



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

The following is an example of the result.

```

/# fdisk -l /dev/sdc

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

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

```

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

```

/# mkdir /AI_DB
/# mount /dev/sdcl /AI_DB/
/# █

```

The following is an example of the result.

```

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

```

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

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

FAI35FT319000004 # █
```

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

FAI35FT319000004 # █
```

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

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

- 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.

**Sample 4412** Information View + Add to Deny List Generate Report Back

**VSA Verdict: No Risk**  
CLEAN

**Sample Information**

|                |                                                                                                                                  |               |                     |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------|
| Submitted Date | 2023/02/07 10:03:27                                                                                                              | Last Analyzed | 2023/02/07 10:03:27 |
| File Type      | UNICODE                                                                                                                          | File Size     | 1244(1.2 KB)        |
| URL            | http://go.microsoft.com/fwlink/?LinkID=252669&clcid=0x409                                                                        |               |                     |
| MDS            | 9CABECCCFEAA58E4C2A8590ED882DDC vt                                                                                               |               |                     |
| SHA256         | CA2A4F8BA44122A9E49E4E298851165732B396DA37DE0DE485DF8849848578D8                                                                 |               |                     |
| SHA1           | 751474CDA58D5270B5A7F2F8CEBEFEFCF4E255C1                                                                                         |               |                     |
| Detection Name | N/A                                                                                                                              | Virus Family  | N/A                 |
| Source Device  | Sniffer                                                                                                                          |               |                     |
| Device Type    | Sniffer                                                                                                                          |               |                     |
| Network        | Attacker: 2620:0101:9005:3235:0000:0000:0000:c121:59228 (Private port) Victim: 2600:1409:8800:0292:0000:0000:0000:2c1a:80 (HTTP) |               |                     |

**Feature Composition**

0 Detection(s)

Feature Type Appearance In Sample

No results

**History**

| Date                | MDS                             | File Type | Detection Name | Device Type | VDOM | Attacker                                | Victim                                  | Confidence |
|---------------------|---------------------------------|-----------|----------------|-------------|------|-----------------------------------------|-----------------------------------------|------------|
| 2023/02/07 10:03:27 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 4.246.174.31                            | ?          |
| 2023/02/07 10:03:27 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:1409:8800:0292:0000:0000:0000:2c1a | ?          |
| 2023/02/06 23:30:15 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 4.246.174.31                            | ?          |
| 2023/02/06 23:30:15 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:140ac000:0687:0000:0000:0000:2c1a  | ?          |
| 2023/02/06 20:46:21 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:140ac000:0394:0000:0000:0000:2c1a  | ?          |
| 2023/02/06 20:46:21 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 20.103.253.93                           | ?          |
| 2023/02/06 11:15:37 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 2620:0101:9005:3235:0000:0000:0000:c121 | 2600:1409:3800:0181:0000:0000:0000:2c1a | ?          |
| 2023/02/06 11:15:37 | 9CABECCCFEAA58E4C2A8590ED882DDC | UNICODE   | Clean          | Sniffer     |      | 172.19.236.121                          | 20.953.213.245                          | ?          |

- IPv6 addresses are displayed in NDR logs.

Anomaly Session Device

View Device View Session No ML training has finished yet Source Address == fe80::7686:a2ff:fe40:1526, Search

| Timestamp           | Session ID | Anomaly Type                    | Source Address            | Destination Address | Severity | Transport Layer Protocol | Info                                        |
|---------------------|------------|---------------------------------|---------------------------|---------------------|----------|--------------------------|---------------------------------------------|
| 2023/02/03 10:45:26 | 142834212  | Weak Cipher/Vulnerable Protocol | fe80::7686:a2ff:fe40:1526 | ff02::1:fa3:b65d    | Medium   | ICMPV6                   | Weak security mode of SMB Protocol detected |

- IPv6 is shown in the session detail page.

**Session 142834212**

**Activity**  
N/A  
Application  
N/A  
Vendor  
N/A  
**Medium Anomaly**

**Session Information**  
Timestamp: 2023/02/03 10:55:24  
Transport Layer Protocol: ICMPV6  
Application Layer Protocol: SMB  
Volume: 2.02K (2021 bytes)  
Interface: N/A  
Cloud Service: None

**Device Information**

|          |              |                           |
|----------|--------------|---------------------------|
| Internal | Device Type  | N/A                       |
|          | Devie Model  | N/A                       |
|          | MAC Address  | 74:86:e2:40:15:26         |
|          | Vendor       | N/A                       |
|          | OS           | N/A                       |
|          | Category     | N/A                       |
|          | Sub Category | N/A                       |
|          | IP           | fe80::7686:e2ff:fe40:1526 |
|          | Port         | 58045                     |
|          | Packet Size  | 1085                      |

**Multicast**  
Internal

|              |                                   |
|--------------|-----------------------------------|
| MAC Address  | 33:33:ff:a3:b6:5d                 |
| Vendor       | N/A                               |
| OS           | N/A                               |
| Category     | N/A                               |
| Sub Category | N/A                               |
| IP           | ff02::1:ffa3:b6:5d (Multicast IP) |
| Port         | 445                               |
| Packet Size  | 936                               |

**Activity**  
No Activity Found

**ML Discovery**  
No ML Feature Found

**Detection Information**

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

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

| Open Time           | Flow Type  | Flow Direction | Sampler ID     | Sampling Rate | Protocol  | Source Address        | Destination Address | In Bytes | Out Bytes |
|---------------------|------------|----------------|----------------|---------------|-----------|-----------------------|---------------------|----------|-----------|
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.82       | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | UDP       | 239.255.255.250       | 172.19.122.240      | 0        | 0         |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | TCP       | 172.19.235.107        | 172.19.122.201      | 176      | 176       |
| 1970/01/20 01:09:07 | NETFLOW_V9 | Ingress        | 172.19.122.201 | 1             | TCP       | 172.19.122.201        | 172.19.235.107      | 180      | 180       |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.56  | 0             | IPv6-ICMP | fe80::250:56fff9e7104 | ff02::1:ffcb:1567   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.60  | 0             | IPv6-ICMP | fe80::250:56fff9e7104 | ff02::1:ffcb:1567   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.60  | 0             | IPv6-ICMP | fe80::250:56fff9e7104 | ff02::1:ffcb:1567   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.56  | 0             | IPv6-ICMP | fe80::250:56fff9e7104 | ff02::1:ffcb:1567   | 216      | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.56  | 0             | UDP       | fe80::3ecccfff9e71567 | ff02::1:2           | 84       | 0         |
| 1970/01/20 01:09:07 | IPFIX      | Egress         | 172.19.235.60  | 0             | UDP       | fe80::3ecccfff9e71567 | ff02::1:2           | 84       | 0         |

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

## Appendix G: Supported Application Protocol List

FortiNDR has multiple ways to identify protocols and applications from sniffer traffic. The NDR engine supports in-depth analysis of the following protocols, plus thousands of applications available [here](#). Application and protocols= identification is used to profile traffic for Machine Learning as well as identifying attacks against weak ciphers, botnets, intrusion etc.

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

## Appendix H: File types and protocols

FortiNDR file scanning supports the following file types:

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NDR engine</b>                 | Common protocols such as TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>File-based analyses</b>        | 32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, 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, PERLSRIPT, 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, JEPG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN |
| <b>OT/SCADA protocols support</b> | DNP3, MODBUS, IEC104, ETHERNET_IP, S7(TSAP), MMS(TSAP), LONTALK, PROFINET, Synchrophasor, NMXSVC, HART, OPC, KNXnet_IP, CIP, CoAP, ELCom, NFP, BACNet                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



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

### Supported file types for ANN:

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



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

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

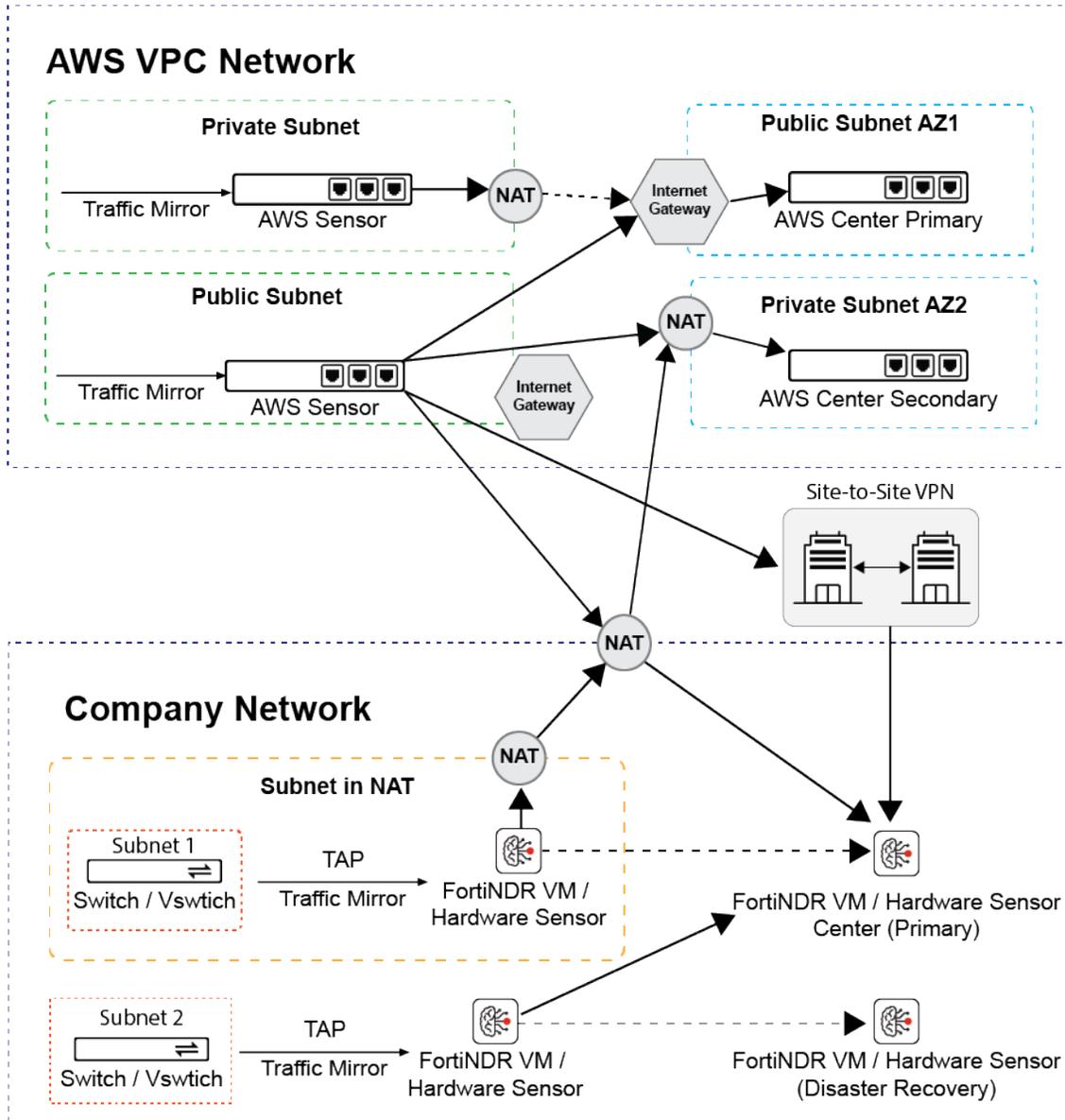
- 3S-Smart
- 7-Technologies
- ABB
- Advantech
- AzeoTech
- B&R
- Beckhoff
- Broadwin
- CODESYS
- CirCarLife
- CitectSCADA
- Cogent
- DATAC
- Delta
- Dut
- Eaton
- Fuji
- GE
- Gemalto
- Guardzilla
- IBM
- Iconics
- InduSoft
- Intellicom
- KeySight
- KingScada
- KingView
- Korenix
- LAquis
- Measuresoft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

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

# Appendix J: Center Sensor Deployment

## Topology

The following is an example topology showing NDR CM and Sensor deployment in AWS, or Hybrid with on-premise devices.



## Redundant Center Setup

To achieve better availability, two center topologies are recommended to deploy in two different availability zones as illustrated in the topology above.

## On-premises and Private Cloud (FNDR3K5, VM and KVM)

For deployment of on-premises and private cloud, please make sure the network access list listed in [Appendix C: FortiNDR ports on page 273](#) 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 273](#).

## 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).

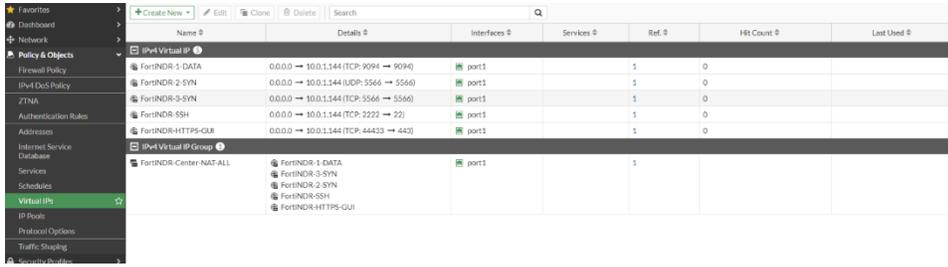
### For NAT deployment:

- 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.



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

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.