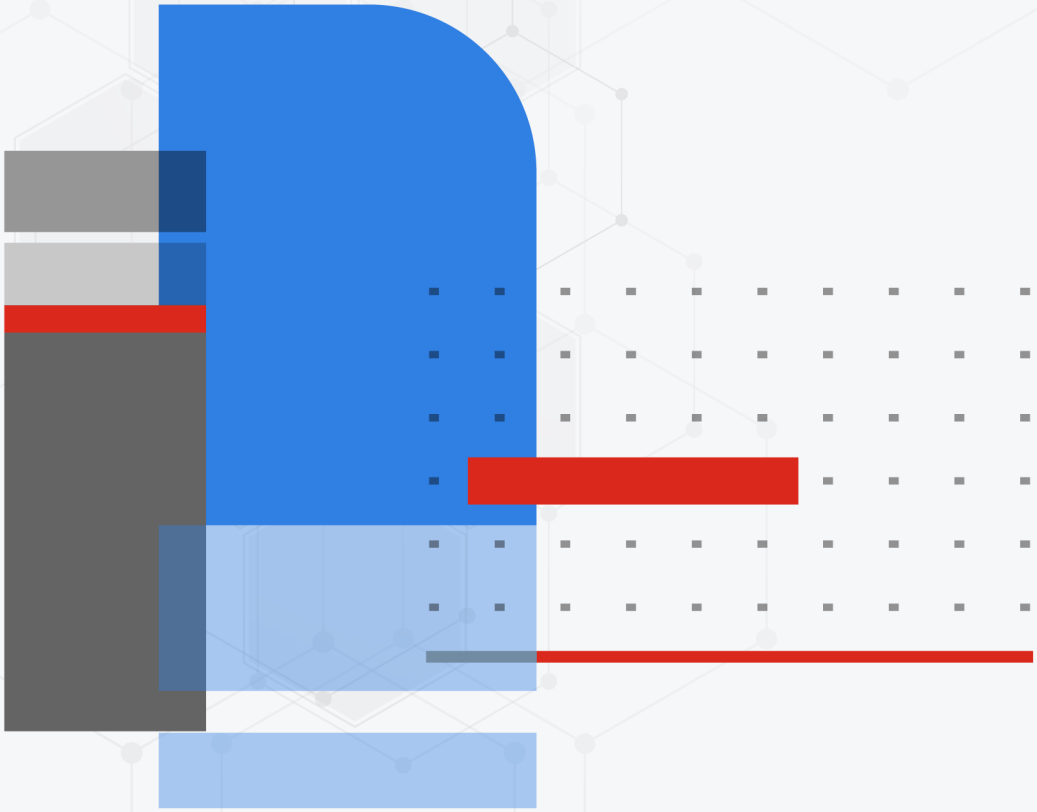
Getting Started

FortiNDR 7.6.3



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

October 16, 2025
FortiNDR 7.6.3 Getting Started
55-763-1184872-20251016

TABLE OF CONTENTS

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.

To connect to the FortiNDR GUI:

1. Connect to the port1 management interface (default 192.168.1.88) using the following CLI commands:

```
config sys interface
    edit port1
    set ip x.x.x.x/24
end
```

2. In a web browser (Chrome recommended), browse to `https://192.168.1.88`.
   The GUI requires TCP port 443.
3. Use *admin* as the name and leave the password blank. Click *Login*.

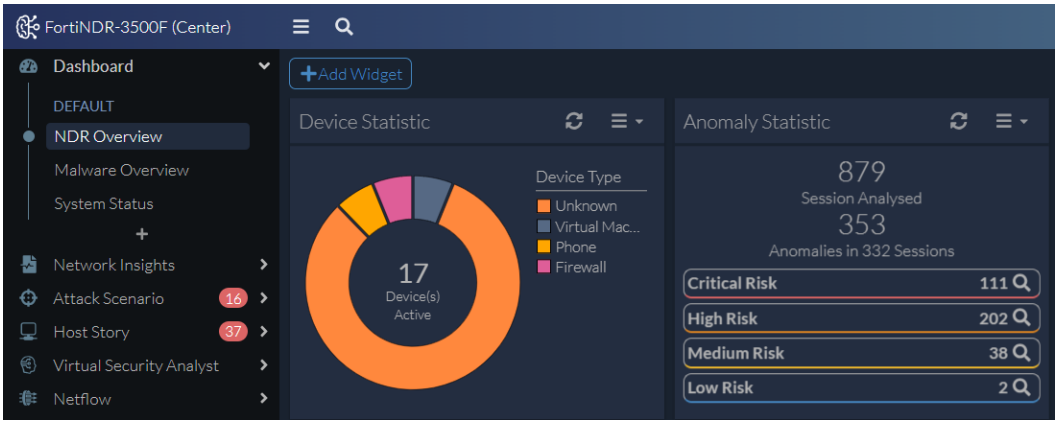
Standalone, Center and Sensor operating mode

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

- **Standalone**: Supports all the features and functionality of FortiNDR. FNR-1000F, VM16/32, FNR-3500F can all operate as standalone mode.
- **Center**: Supports centralized management of configurations and data collected by sensors. Most, but not all features and functionality are available.
  - FortiNDR 7.6 supports Center Mode in for FNR-3500F and FNR-3600G. For Public Cloud and mode support, please refer to Release Notes as well as Public Cloud documentation.
  - Center Mode is supported in VMs. See, Licensing.
- **Sensor**: Supports Sensor configuration upon first login. A minimal amount of features and functionality are available.
  - FortiNDR 7.6.3 supports sensor mode in FNR-1000F and VM models. For more information, see the Release Notes.

There is a separate image to be loaded for each mode in the customer support website.

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



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

Feature	Standalone	Center	Sensor	Notes
Dashboard	✓	✓	✓	In Center mode, the widgets are used to monitor the sensors.
Security Fabric	✓		✓	Security Fabric is configured in the Sensor mode or via the Center mode settings.

Feature	Standalone	Center	Sensor	Notes
Virtual Security Analyst > Express Malware Analysis	✓		✓	
Virtual Security Analyst > Static Filter	✓	✓		Static Filters, including the *Allow List* and *Deny List*, are employed in Center mode and associated with specific sensors. These filters provide users with the capability to formulate and modify an *Allow* or *Deny* list for targeted sensors. Please note that these Static Filters cannot be set through the Sensor's GUI.
Virtual Security Analyst > NDR Muting	✓	✓	✓	NDR Muting rules can be established in Center and Sensor mode. However, these rules only mask or hide specific NDR attack detections for that specific Center or Sensor. For instance, if you hide an attack on a Center, it does not automatically hide the same attack on the Sensor's user interface.
Virtual Security Analyst > ML Discovery	✓	✓		Both the *ML Discovery* dashboard widget and *ML Discovery* module are not available in Sensor mode.
Virtual Security Analyst > Device Enrichment	✓	✓	✓	Center and Sensor device enrichment is available starting in version 7.6.3.
Virtual Security Analyst > ML Configuration		✓		
Netflow	✓	✓	✓	Sensor mode maintains the same design and functionality for the *Netflow Dashboard* and *Netflow Log* as seen in Standalone mode.

Feature	Standalone	Center	Sensor	Notes
				Center mode's *Netflow Dashboard* and *Netflow Log* display the data collated from the Sensors.
Global Investigation and Tagging		✓		Query metadata and tagging of sessions. This feature is available in FNR-3600G and Central Management VM.
System > Admin Profiles	✓	✓	✓	In Center mode, users can select which Sensor(s) are linked with the current profile. If a Sensor is selected to be included in this *Admin Profile*, the profile user will be able to view and manage the corresponding Sensor when they log into the FortiNDR Center.
System > Center Settings		✓		
System > High Availability (HA)	✓			
Log & Report	✓	✓	✓	Log Settings are supported in all modes. See, Log Settings on page 1.

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.

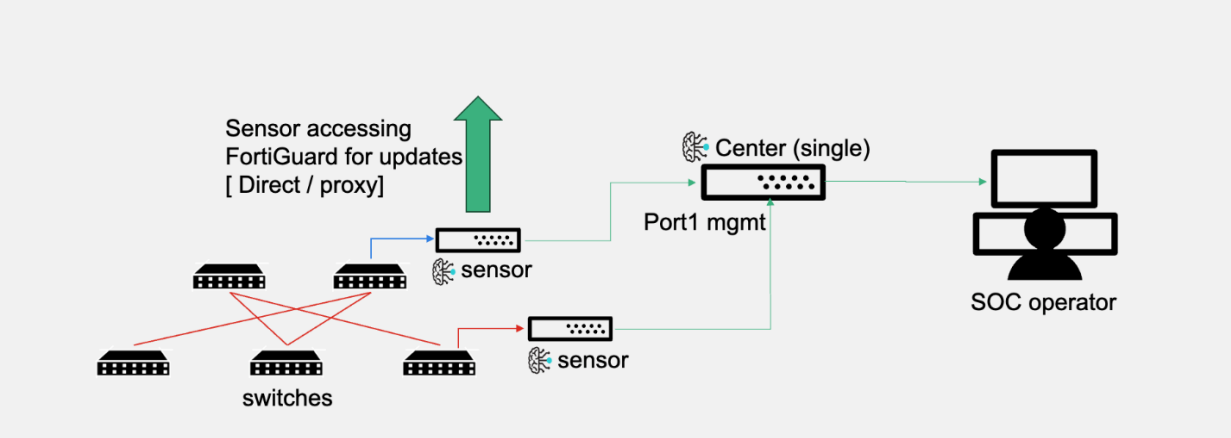
In Center Mode, the system does require a Neflow license to access the Netflow module.

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

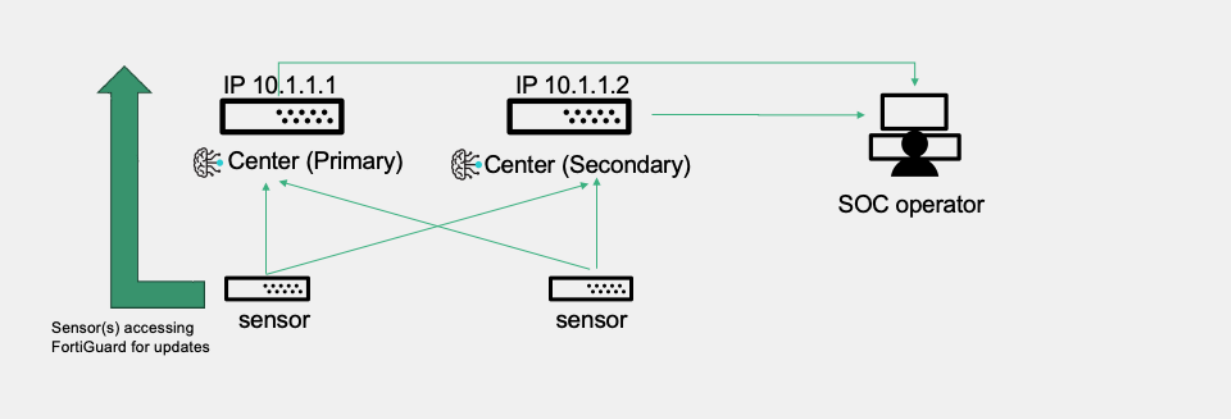
Dual Center mode support

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:

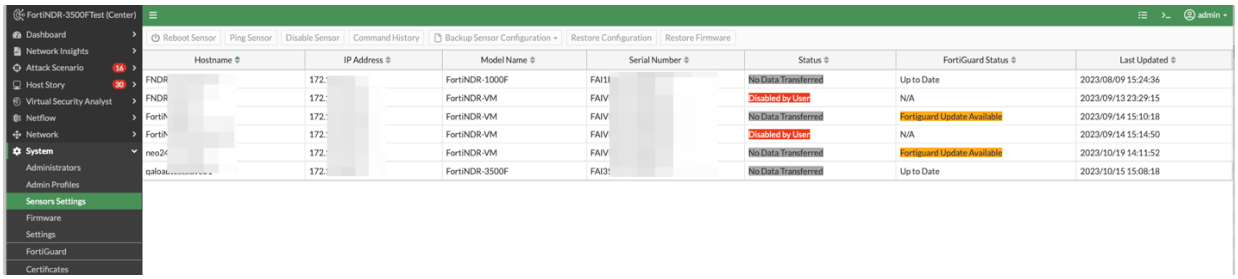


Dual NDR center support:

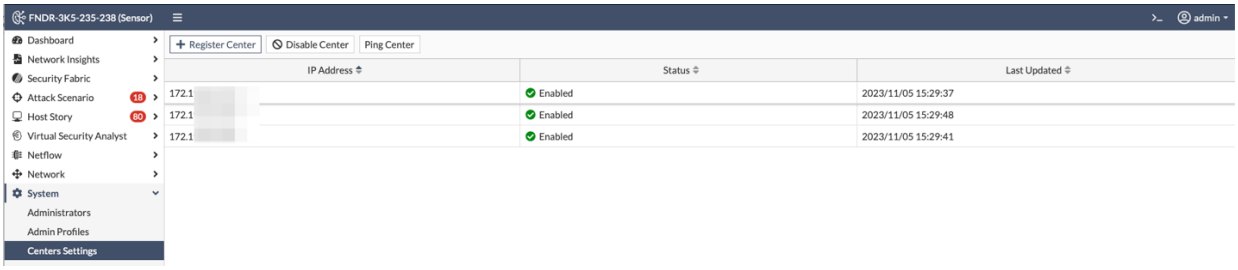


Sensors data are synchronized periodically between sensors and center using HTTPS port 443, connections are initiated by sensor to center. For a complete list of FortiNDR ports required, see FortiNDR ports on page 26. If network issues occurs, sensors will resume synchronization again after network restores. Last updates can be viewed from both sensors and center, as follows:

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



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



For information about sensors operations, seeSensor/Center settings on page 21 .

FortiNDR traffic and files input types

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

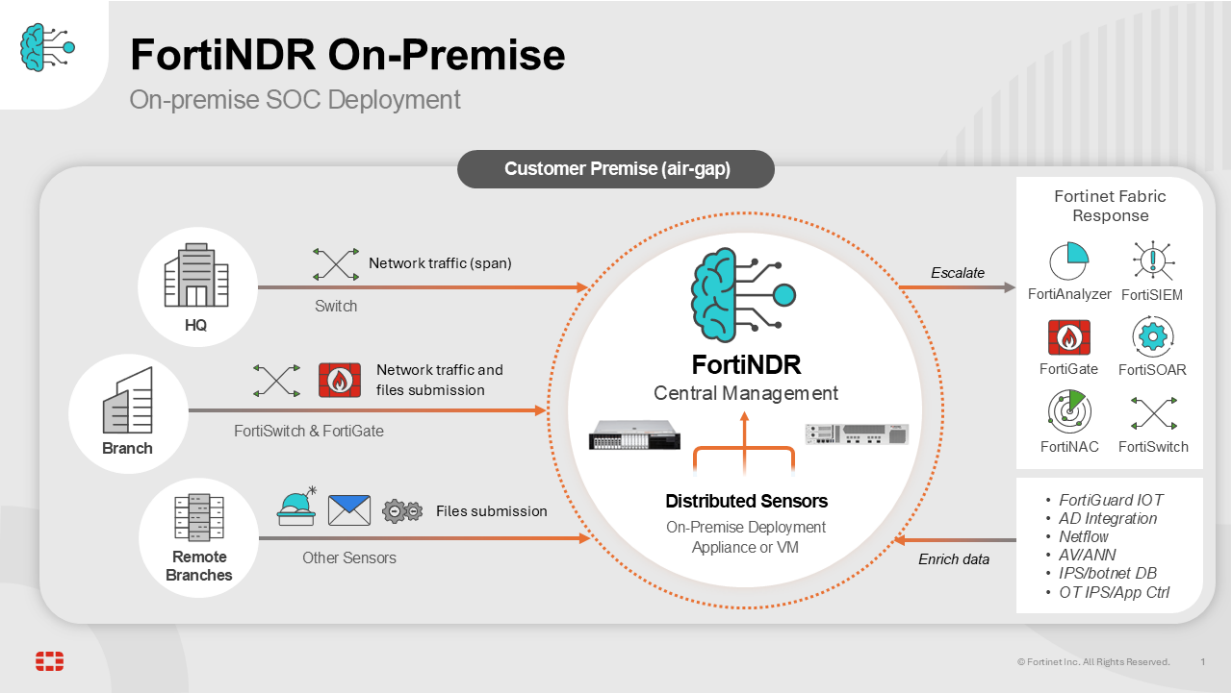
For more information, see the *FortiNDR CLI Reference Guide*.

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	Notes
Sniffer			Please refer to, Supported IPS (including OT), Application Control, and protocols on page 34.	Using SPAN port or network TAP. Using SPAN port, network tap or packet brokers to mirror traffic.
Fabric devices	FortiGate	HTTP2 (v7.0 FOS) OFTP (v5.6-6.0 FOS, legacy support)	HTTP, HTTPS (with SSL decryption), SMTP, POP3, IMAP,	FortiGate v7.0.1 supports INLINE blocking with AV profile
	FortiMail	HTTP2	SMTP	Configure under *AV profile* under FortiMail.
	FortiSandbox	HTTP2	MAPI, FTP, CIFS	
	FortiProxy	HTTP2	HTTP, HTTPS	Supports FortiProxy 7.0.0 and higher
ICAP	FortiWeb	ICAP	HTTP, HTTPS	Supports using FortiNDR as ICAP server.
	FortiProxy	ICAP	HTTP, HTTPS	FortiGates, FortiWeb and FortiProxy or third-party ICAP client such as Squid.
Other / API	FortiSOAR	HTTPS API upload	HTTPS	Using API available from FortiNDR for file upload
	Scripts (refer to Appendix for sample scripts)	HTTPS API upload		

Traffic input type	Supported Devices *	Communication Protocol	File/Malware Analysis Protocols supported	Notes
	NFS. SMB file shares, and S3 bucket	SMB/NFS		Direct map and scan

For a complete list of supported file types, see File types and protocols on page 35

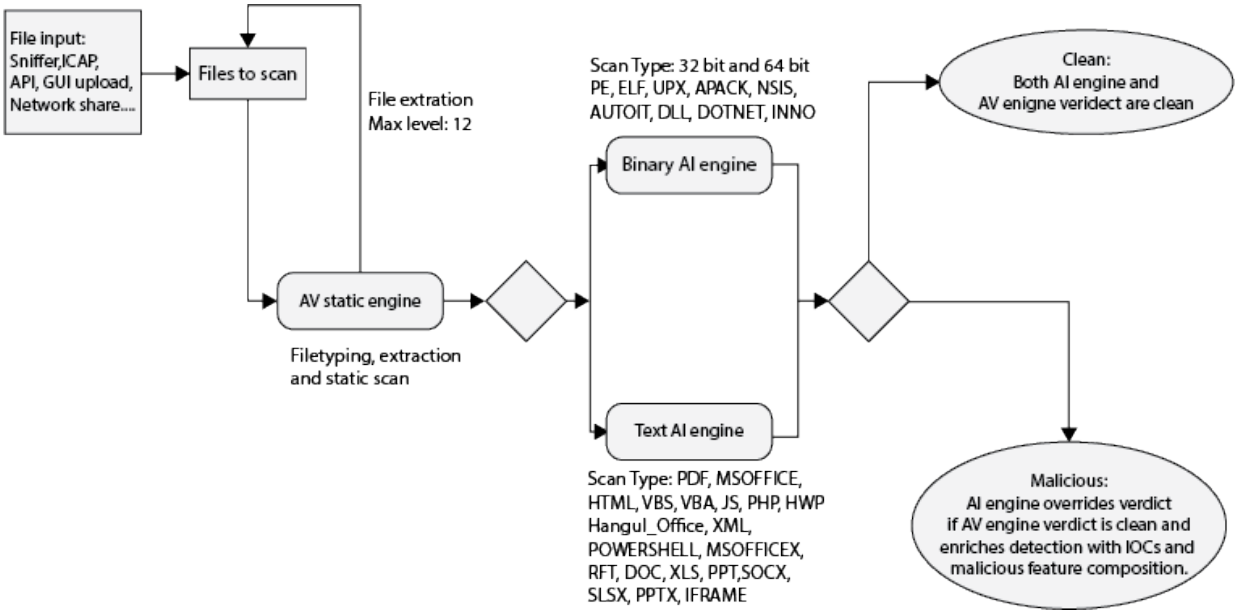
FortiNDR supports quarantine with incoming webhook from FortiOS 6.4 and higher. For details, see the Release Notes. For FortiNDR to quarantine via FortiGate, you must provide VDOM information to FortiGate. For details, see Automation Framework on page 23.



Files and malware scan flow using AV and ANN

Stage 1

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



Stage 2

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

File verdict caching is triggered automatically. When a cache hit occurs (based on the file hash) and no AVeng or AI database updates have taken place since the verdict was cached, FortiNDR uses the cached result. In this case, the file is not rescanned by the Binary or Text AI engines. For more details, see FortiGuard on page 1.

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
FNDR-2500G	13.2 TB	132 days
FortiNDR-3600G	12x16TB RAID5 176TB usable	365 days*
FNDR-VM Standalone, Sensor, CM	1024 GB	10 days
FNDR-VM Standalone, Sensor, CM	2048 GB	20 days
FNDR-VM Standalone, Sensor,	4096 GB	40 days

Model	Total disk size	Storage retention
CM		
FNDR-VM Standalone, Sensor, CM	8192 GB	73 days
FNDR-VMCM	15TB	115 days
FNDR-VMCM	30TB	264 days

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

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

- Center mode: `execute center-retention-setting`
- Sensor/Standalone mode: `execute retention-setting`

For more information, see the FortiNDR CLI Reference Guide.

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

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

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

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

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

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

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

Additional SSD

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

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

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

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

To add additional SSD to FortiNDR 3500F:

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

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

To check the new SSD capacity with the GUI:

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

To check the new SSD capacity with the CLI:

```
Get system raid-status
```

Sample output:

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

Preparing the virtual environment

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

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

	vCPU	Reserved CPU GHz	Reserved Memory	Minimum Host's Disk Sequential (Read/Write)	Minimum Host's Disk 4KB Random (Read/Write)	Recommend Host's Disk Sequential (Read/Write)	Recommend Host's Disk 4KB Random (Read/Write)
VM08	8	16GHz	64GB	4000 MBps / 1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS
VM16	16	32GHz	128GB	4000 MBps / 1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS
VM32	32	64GHz	256GB	4000 MBps / 1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS
VM Center mode	48	90GHz	384GB	4000 MBps /1500 MBps	92000/31000 IOPS	6200 MBps / 2350 MBps	1,000,000 / 60,000 IOPS

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

VM Center Mode with Investigation Feature ON (additional configuration)

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

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

Initial setup

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

Internet Access

For FortiGuard updates please have a stable internet access from the FortiNDR unit. Go to *System* > *FortiGuard* for updates via Internet. For offline deployments please refer to FortiGuard updates on page 28.

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

Ports

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

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

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

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

Port	Type	Function
Port1	10GE copper (10G or 1G autodetect)	Management port, GUI, Fabric devices files receiving, REST API, ICAP.

Port	Type	Function
		Default IP address is `192.168.1.88` using `admin` with no password.
Port2	10GE copper (10G or 1G autodetect)	Sniffer port.
Port3 **Port4**	1G Copper	High availability
Port5 **Port6** **Port7** **Port8**	10G SPF+ fiber (gen3 only)	Sniffer port. For VM, only Port5 is used as sniffer port among Port5, Port6, port7 and Port8.
Console	Serial port	Console serial port. 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control.

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

Port	Type	Function
Port1	10G SFP+ Fiber	Management port, GUI, Fabric devices files receiving, REST API, ICAP. Default IP address is 192.168.1.88 using admin with no password.
Port2	10G SFP+ Fiber	High Availability in Standalone mode, unused in Sensor mode
Port3 **Port4** **Port5** **Port6**	25G SFP28 Fiber	Sniffer port.
Port7	RJ45 1G Copper	Only used by bootloader to transfer image.
Console	Serial port	Console serial port. 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control.

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

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

Port	Type	Function
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.

Sensor/Center settings

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

The *Center Settings* page displays the following information:

Hostname	The sensor hostname.
IP Address	The sensor IP address.
Model Name	The sensor model name.
Serial Number	The sensor serial number.
Status	The connection status.

Registered	Indicates that the Sensor has completed the registration process but has yet to undergo a license check.
Connected	Indicates the Sensor is prepared for synchronization and is actively transmitting data to the Center.
No Data Transferred	Indicates the Sensor has not sent any data to the Center for a span of 3 minutes while still maintaining a connection.
Firmware Mismatched	Indicates the Sensor's firmware is incompatible with the Center, and the Sensor is currently disabled. This does not mean the Sensor is inoperative. However, the Center will not accept any data from it.
Sensor License Invalid	Indicates that the Sensor does not possess a valid license, and has been disabled.
Disabled By User	Indicates the Sensor has been manually disabled by a user in the Center. This does not mean the Sensor is inoperative. However, the Center will not receive any data from it.

FortiGuard Status	Compares the Sensor's FortiGuard updates against the Center's FortiGuard updates. *FortiGuard Update Available* will appear if an update is required.
Last Updated	The date the sensor was last updated.
CPU Usage	The CPU usage as a percentage.
Disk Usage	The disk usage as a percentage.
Memory Usage	The memory usage as a percentage.

The following options are available:

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

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

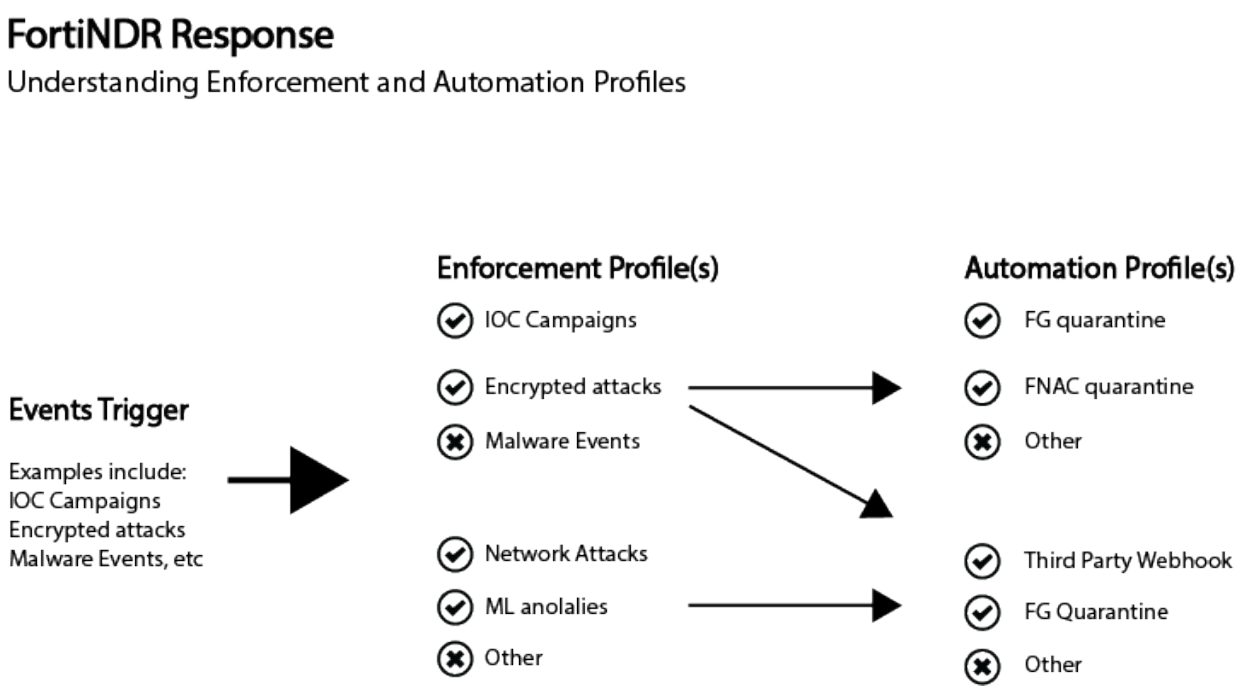
Sensor Details

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

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

Automation Framework

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



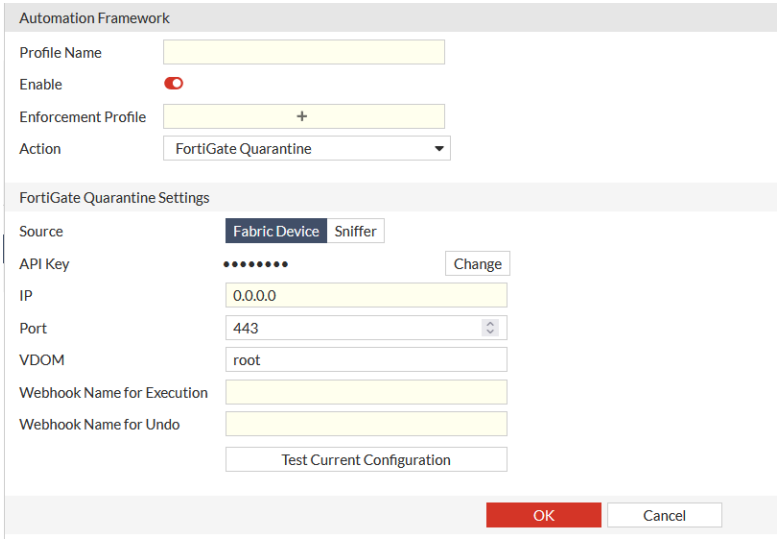
NDR Muted Resultswill not be included in the quarantine response.

To create an automation profile:

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

Profile Name	Enter a name for the profile.
Enable	Click to enable or disable the framework.
Enforcement Profile	Click to select an Enforcement Settings profiles.
Action	Select one of the following actions: • *FortiGate Quarantine* • *FortiNAC Quarantine* • *FortiSwitch Quarantine via FortiLink*

- *FortiProxy Quarantine*
- *Generic Webhook*



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

   Manage FortiGate Settings and *FortiSwitch Quarantine via FortiLink*.

Manage FortiGate Settings and **FortiSwitch Quarantine Settings**	
Source	• **Fabric Device**: If the source of detection came from OFTP, the enforcement is only executed to a matching automation profile with a matching IP address and VDOM. • **Sniffer**: If the source of detection came from a sniffer, the enforcement is adapted by all profiles where *Trigger Source* is *Sniffer*. Since detection sourced from sniffer does not contain information about which fabric device monitors the infected IP address, it is your responsibility to specify the correct device IP address and VDOM.
API Key	Enter the device API key
IP	Enter the device IP address.
Port	Enter the device port number.
VDOM	Enter the VDOM name.
WebHook Name for Execution	Select the FortiGate webhook for execution action, such as `ip_blocker`.
WebHook Name for Undo	Select the FortiGate webhook for undo action, such as `ip_unblocker`.

   FortiNAC Quarantine

FortiNAC Quarantine Settings

API Key	Click *Change* to update the API key.
IP	Enter the FortiNAC IP address.
Port	Enter the FortiNAC port number.

Generic Webhook

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

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

FortiNDR ports

FortiNDR requires the following ports.

Item	Protocol and port number	Direction
API submission, such as FortiSandbox	TCP 443	Inbound
Auto sample submit,	TCP 25	Outbound to fndr.fortinet.com
CLI	TCP 22	Inbound SSH
Data synchronization	TCP 20003	Inbound and outbound between FortiNDR units in an HA group.
DB synchronization	TCP 9561	Inbound and outbound between FortiNDR units in an HA group.
File synchronization	TCP 20002	Inbound and outbound between FortiNDR units in an HA group.
FortiGate quarantine	TCP 443	Outbound to FortiGate
FortiGuard update	TCP 443 TCP 8890 (When using FortiManager)	Initial outbound to: • fai.fortinet.net • globalupdate.fortinet.net (Default when Anycast is enabled) • fds1.fortinet.com (When Anycast disabled) • update.fortiguard.net (When Anycast disabled) For a complete list of the current FortiGuard update servers, use the CLI `diagnose fds list`. To enable/disable Anycast, please use the CLI `config system fortiguard update` and then set `anycast` to `disabled`. Please be aware this list of IPs can and will change over time without notice.
GUI	TCP 443	Inbound web browser
ICAP	TCP 1344, 11344	Inbound
IOC lookup	TCP 443 TCP 8888 (When using FortiManager)	Outbound to productapi.fortinet.com

Item	Protocol and port number	Direction
IOT lookup	TCP 443	Outbound to globalguardservice.fortinet.net
Microsoft Active Directory	TCP 636,389	Inbound and outbound
NetFlow listen ports	UDP 2055,6343,9995	Inbound
Network File Share/PCAP Artifact Storage	TCP 139, 445, 2049 (NFS)	Outbound to file server
OFTP server	TCP 514	Inbound
Security Fabric with FortiGate	TCP 443	Outbound to root FortiGate for Security Fabric communication
Security Fabric with FortiGate	TCP 8013	Outbound to root FortiGate in Security Fabric
Sensor Center command communication	UDP 5566	Sensor to Center (SSL encrypted)
Sensor Center data synchronization	TCP 9094 9096	Sensor to Center (SSL encrypted)
SYSLOG	UDP 514	SYSLOG outbound
Web Filter query	UDP 53 TCP 8888 (When using FortiManager)	Outbound to service.fortiguard.net

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).

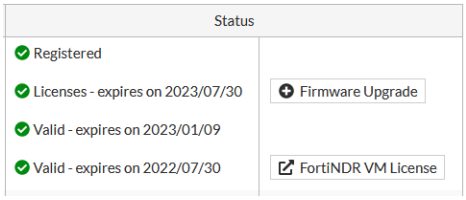
Detection Techniques	Supports offline manual update	Comments
Malware via ANN	Yes	Can be updated manually via GUI or with an offline package via CLI.
AV engine	Yes	Shipped by default. Can be updated with internet via GUI or with an offline package via CLI.
Botnet detection	Yes	Has DB by default. Can be 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
Device inventory	Yes	Has minimal DB on firmware image by default. The IOT query service is now local (previous lookup was through FortiGuard servers). Can be updated with internet via GUI or with an offline package via CLI.
FortiGuard IOC	No	Requires Internet to lookup URLs and IP for web campaigns associated.
ML Discovery	NA	Local ML algorithm updates via firmware.
Geo DB	No	Comes with firmware, does not update often, supports FortiGuard Update via internet.
OT Threat and OT device inventory	Yes	Has minimal DB by default. Can be updated with internet via GUI or with an offline package via CLI. Requires SCADA/OT license to download the packages.

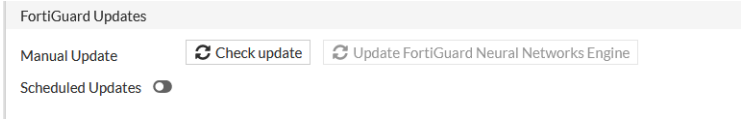
Updating the ANN database from FDS for malware detection (GUI)

To update the ANN database from FDS:

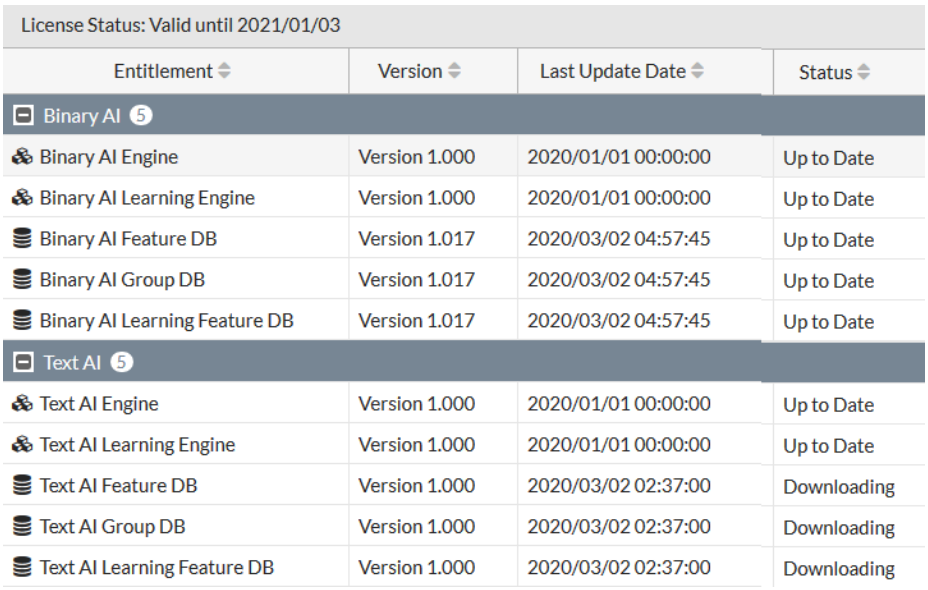
1. Go to *System* > *FortiGuard*.
2. Check the *License Status* to ensure there is a valid license.
   If the license is not valid:
   - The unit cannot update from FDS.
   - Ensure the unit is not on internal FDS and the unit has a subscription for *FortiGuard Neural Networks engine updates & baseline*.



3. Click *Check Update*.
   If there are updates, an *Update Now* button appears and the *Status* column shows the components with updates.



4. Click *Update Now*.
   Due to the size of databases, the update might take several hours depending on your Internet speed. During the update, check the *Status* column.



License Status: Valid until 2021/01/03

Entitlement	Version	Last Update Date	Status
Binary AI 5			
Binary AI Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Binary AI Learning Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Binary AI Feature DB	Version 1.017	2020/03/02 04:57:45	Up to Date
Binary AI Group DB	Version 1.017	2020/03/02 04:57:45	Up to Date
Binary AI Learning Feature DB	Version 1.017	2020/03/02 04:57:45	Up to Date
Text AI 5			
Text AI Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Text AI Learning Engine	Version 1.000	2020/01/01 00:00:00	Up to Date
Text AI Feature DB	Version 1.000	2020/03/02 02:37:00	Downloading
Text AI Group DB	Version 1.000	2020/03/02 02:37:00	Downloading
Text AI Learning Feature DB	Version 1.000	2020/03/02 02:37:00	Downloading

Updating ANN for malware detection (CLI)

FortiNDR utilizes both FortiGuard updates to local DB as well as lookup for detecting network 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 FortiGuard updates on page 28 for details. The section below discusses one of the updates: ANN for malware detection.

The ANN (Artificial Neural Network) database enables scanning of malware using accelerated ANN. Unlike AV signatures, ANN DB does not require updates daily. ANN is only updated once or twice a week to enable detection of the latest malware.

There are two ways to update ANN. You can update using FDN (FortiGuard Distribution Network) if internet is available, or on Fortinet support website after the product is registered.

Currently FortiGuard updates are available via US, EMEA and Japan. Depending on your location, manual update might be faster. The average time of ANN update via Internet is about 1–2 hours. Using the local CLI takes about 10 minutes.

To update the ANN database using CLI:

```
execute restore kdb {disk <filename> | ftp <file name> <server_ipv4> | scp <file
     name> <server_ipv4> | tftp <file name> <server_ipv4>}
```

To update the ANN database by downloading from FDN to the FortiNDR device:

1. Format a USB drive in another Linux machine using the command `fdisk /dev/sdc`.
   Ensure the USB drive has enough capacity and create one partition using EXT4 or EXT3 format.

```
/# fdisk /dev/sdc

Welcome to fdisk (util-linux 2.25.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help):
```

2. Format `sdc1` using the `mkfs.ext4 /dev/sdc1` command.

```
/# mkfs.ext4 /dev/sdc1
mke2fs 1.43.7 (16-Oct-2017)
Creating filesystem with 7554430 4k blocks and 1888656 inodes
Filesystem UUID: faec541a-8f39-4a14-a643-93cf75ae748e
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

/#
```

FortiTester is a great companion for FortiNDR as FortiTester can send a malware strike pack over different protocols such as HTTP, FTP, SMTP, to simulate malware in the network. You can use FortiTester to generate malware and test FortiNDR for detection.

The following is an example of the result.

```
/# fdisk -l /dev/sdc

Disk /dev/sdc: 28.8 GiB, 30943995904 bytes, 60437492 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x2a7d7590

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdc1        2048 60437491 60435444 28.8G 83 Linux
```

3. Copy `moat_kdb_all.tar.gz` and `pae_kdb_all.tar.gz` to the root directory of USB drive, in this example, `/AI_DB`.

```
/# mkdir /AI_DB
/# mount /dev/sdc1 /AI_DB/
/#
```

The following is an example of the result.

```
/AI_DB# ls
lost+found          moat_kdb_all.tar.gz  pae_kdb_all.tar.gz
/AI_DB#
```

4. Copy the files onto the FortiNDR by mounting the USB drive on the FortiNDR device and using the `execute restore kdb disk pae_kdb_all.tar.gz` and the `execute restore kdb disk moat_kdb_all.tar.gz` commands.

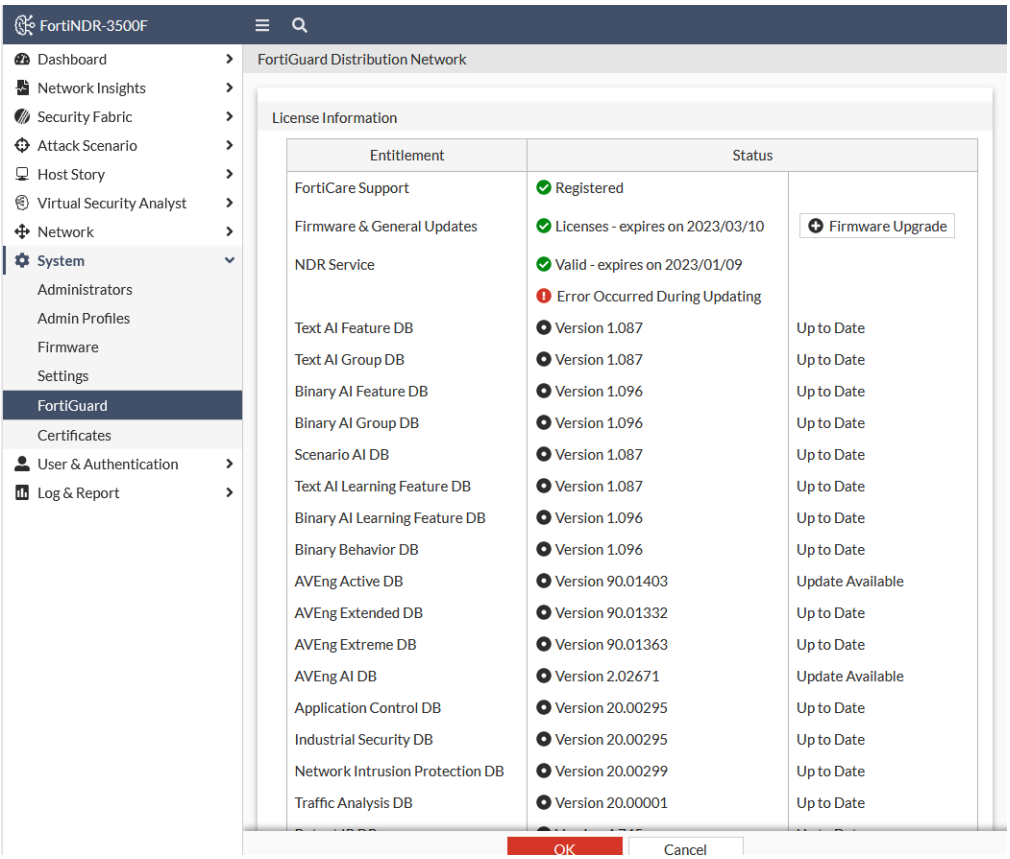
```
FAI35FT319000004 # execute restore kdb disk pae_kdb_all.tar.gz
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Mounting /dev/sda1
Mounting /dev/sdb1
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e51D0v
Copying file failed!
Mounting /dev/sdc1
Try copying file from /kdb_disk/pae_kdb_all.tar.gz to /var/spool/tmp/up_e51D0v
Get file OK.
MD5 verification succeed!
KDB files restoration completed
Scanner restart completed

FAI35FT319000004 #
```

```
FAI35FT319000004 # execute restore kdb disk moat_kdb_all.tar.gz
This operation will first replace the current scanner db files and then restart the scanner!
Do you want to continue? (y/n)y
Mounting /dev/sda1
Mounting /dev/sdb1
Try copying file from /kdb_disk/moat_kdb_all.tar.gz to /var/spool/tmp/up_uWobUb
Copying file failed!
Mounting /dev/sdc1
Try copying file from /kdb_disk/moat_kdb_all.tar.gz to /var/spool/tmp/up_uWobUb
Get file OK.
MD5 verification succeed!
KDB files restoration completed
Scanner restart completed

FAI35FT319000004 #
```

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



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

```
FAI35FT319000004 # diagnose kdb
System Time:  2020-02-11 14:50:34 PST (Uptime: 0d 22h 32m)
Start: /bin/pae2 -test

2020-2-11 14:50:34
[TEST] - Start KDB Test...
        [TEST] - Loading Group KDB...
        [TEST] - Group KDB Rec Num: 383887
        [TEST] - Loading Feature KDB...
        [TEST] - Feature KDB Rec Num: 45562000
[TEST] - KDB Test Passed

2020-2-11 14:50:48
Start: /bin/pae_learn -test

2020-2-11 14:50:48
[TEST] - Start KDB Test...
        [TEST] - Loading Mal KDB...
        [TEST] - Mal KDB Rec Num: 1770913
        [TEST] - Loading Clean KDB...
        [TEST] - Clean KDB Rec Num: 34625563
[TEST] - KDB Test Passed

2020-2-11 14:50:55
Start: /bin/moat_learn -test
2020-2-11 14:50:55
2020-2-11 14:50:55
[TEST] - Start KDB Test...
        [TEST] - Loading KDB-0...
        [TEST] - KDB-0 Rec Num: 127612293
        [TEST] - Loading KDB-1...
        [TEST] - KDB-1 Rec Num: 7058519
[TEST] - KDB Test Passed
2020-2-11 14:51:25
Start: /bin/moat_engine -test kdb
2020-2-11 14:51:25
[TEST] - Start KDB Test...
        [TEST] - Loading Group KDB...
        [TEST] - Group KDB Rec Num: 15235200
        [TEST] - Loading Feature KDB...
        [TEST] - Feature KDB Rec Num: 370576784
[TEST] - KDB Test Passed
2020-2-11 14:53:39
```

When you have finished using the USB or SSD drive, remove the drive from FortiNDR. Some disk-related CLI commands such as `execute factoryreset`, `execute partitiondisk`, or `diagnose hardware sysinfo` might treat the additional disk as the primary data partition.

Supported IPS (including OT), Application Control, and protocols

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

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

   After FortiNDR detects the application, it can then detect 'anomalies' in applications based on ML baselining described here: ML Configuration on page 1.

   FortiNDR will build a baseline of traffic (default 7 days, configurable via the CLI) and detect anything not within the baseline. This detection method can be used along with other features such as dst IP, geo, src port, dst port, etc.

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

   This requires ability for the engine to extract this metadata from protocols and store the metadata in the database for users to search.
4. **Operational Technology vendor and application list**
   FortiNDR supports the following from an OT perspective:
   - OT IPS signatures can be found at *OT threat* on the FortiGuard Operational Technology Security Service page.
   - OT Device Identification under Device Inventory on page 1.
   - Identify OT applications with Application Control (refer to point 2 above), as well as the *OT App Detection* database which is found on the FortiGuard Operational Technology Security Service page.

File types and protocols

FortiNDR file scanning supports the following file types:

NDR engine	Common protocols such as TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMBv1, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors
File-based analyses	32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, Hangul_Office, TAR, XZ, GZIP, BZIP, BZIP2, RAR, LZH, LZW,ARJ, CAB, _7Z, PHP, XML, POWERSHELL, BAT, HTA, UPX, ACTIVEMIME, MIME, HLP, BASE64, BINHEX, UUE, FSG, ASPACK, GENSCRIPT, SHELLSCRIPT, PERLSCRIPT, MSC, PETITE, ACCESS, SIS, HOSTS, NSIS, SISX, INF, E32IMAGE, FATMACH, CPIO, AUTOIT, MSOFFICEX, OPENOFFICE, TNEF, SWF, UNICODE, PYARCH, EGG, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, LNK, KGB, Z, ACE, JAR, APK, MSI, MACH_O, DMG, DOTNET, XAR, CHM, ISO, CRX, INNO, THMX, FLAC, XXE, WORDML, WORDBASIC, OTF, WOFF, VSDX, EMF, DAA, GPG, PYTHON, CSS, AUTOITSCRIPT, RPM, EML, REGISTRY, PFILE, CEF, PRC, CLASS, JAD, COD, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN
OT/SCADA protocols support	DNP3, MODBUS, IEC104, ETHERNET_IP,S7(TSAP), MMS(TSAP), LONTALK, PROFINET, Synchrophasor, NMXSVC, HART, OPC, KNXnet_IP, CIP, CoAP, ELCom, NFP, BACNet

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

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

Supported file types for ANN:

For ANN supported file types, ANN will process and provide a feature breakdown between different attack scenarios (like Ransomware, banking trojan etc) 32 bit and 64 bit PE, PDF, MSOFFICE, HTML, ELF, VBS, VBA, JS, PHP, HWP Hangul_Office, XML, POWERSHELL, UPX, ASPACK, NSIS, AUTOIT, MSOFFICEX, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, DOTNET, INNO, IFRAME

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

www.fortinet.com