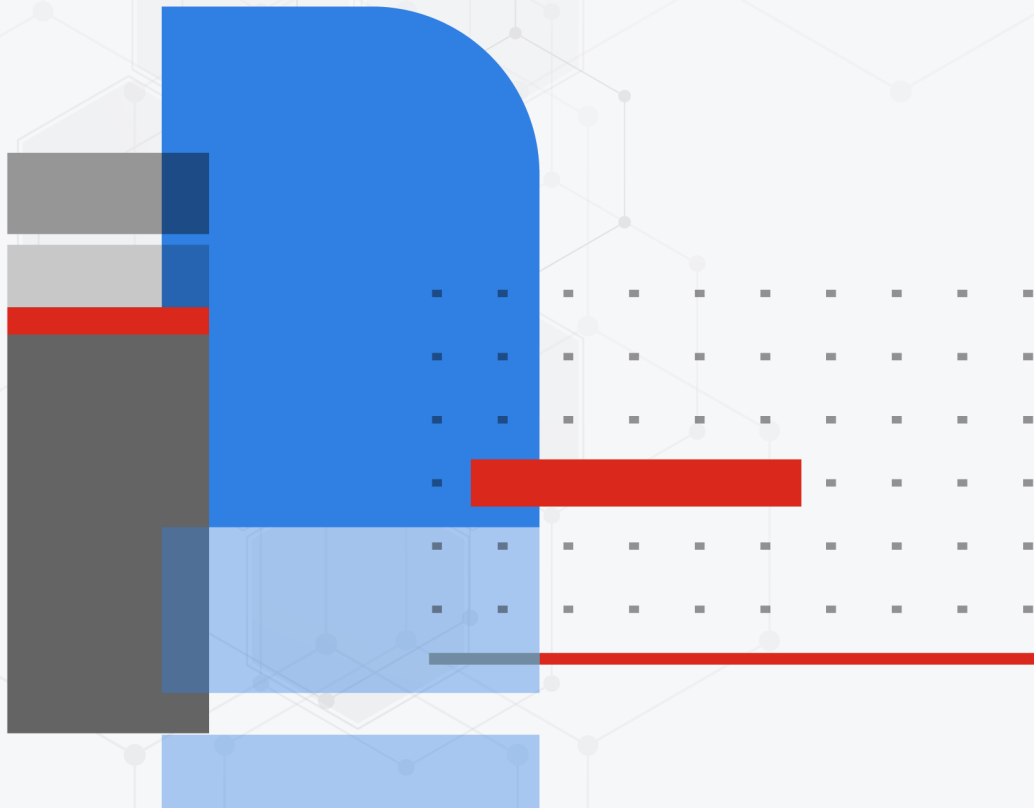


# Troubleshooting Cheat Sheet

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](mailto:techdoc@fortinet.com)



October 3, 2025

FortiNDR 7.6.3 Troubleshooting Cheat Sheet

55-760-1171529-20250618

# TABLE OF CONTENTS

<b>Troubleshooting Cheat Sheet</b> .....	<b>4</b>
<b>FortiNDR general troubleshooting tips</b> .....	<b>5</b>
File scanning related issues .....	6
Manual Upload/API Submission/FortiSandbox Integration .....	7
File Submitted but not processed .....	7
<b>FortiNDR health checks</b> .....	<b>8</b>
Sniffer diagnosis .....	9
<b>Managing FortiNDR disk usage</b> .....	<b>10</b>
Center mode: .....	10
Standalone and Sensor mode: .....	10
Exporting detected malware files .....	11
Formatting the database .....	13
<b>Rebuild RAID</b> .....	<b>14</b>
Rebuild RAID disk (3500F) .....	14
Rebuild Raid for FortiNDR1000F, 2500G and 3600G .....	18
Hot swap drives in FortiNDR 3600 (v7.6.2 or later) .....	21
<b>Export malware</b> .....	<b>22</b>
<b>False positives and false negatives</b> .....	<b>23</b>
<b>Troubleshoot ICAP and OFTP connection issues</b> .....	<b>24</b>
<b>Troubleshoot Log Settings</b> .....	<b>26</b>
<b>Troubleshoot Network Share</b> .....	<b>28</b>
Test the Network Share Connection .....	28
Diagnosing Network Share Errors .....	29
Debug version image .....	30
Check Crash Log .....	31
<b>Troubleshooting the VM License</b> .....	<b>32</b>
<b>Troubleshooting the updater</b> .....	<b>33</b>
FDS Authorization Failed .....	33
Clearing updater cache files .....	33
Diagnosing Other FDS Errors .....	34
<b>Sensor logs not displaying in Center GUI</b> .....	<b>35</b>
<b>Troubleshooting FortiNDR VM high CPU usage</b> .....	<b>36</b>
<b>Troubleshooting inactive Netflow status</b> .....	<b>37</b>
<b>Submit support tickets</b> .....	<b>38</b>

# Troubleshooting Cheat Sheet

This troubleshooting cheat sheet covers a wide range of FortiNDR troubleshooting topics, including file scanning issues, system health checks, disk management, network diagnostics, and integration problems. It also addresses RAID rebuild procedures, malware export, log analysis, licensing, and performance concerns across various deployment modes.

# FortiNDR general 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
System CPU and Memory Usage are really high and GUI became slow	Check NDR Overview and Malware Overview and make sure this unit is not oversubscribed according to specs from the <a href="#">FortiNDR Datasheet</a> .		
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 when it comes to a file sniffer or NDR logging issue.

## General Debug Logs Retrieval

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

## File scanning related issues

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

### To perform a general check:

1. Check and record network conditions from the FortiNDR server to file submitting clients using the following CLI commands:
  - `exec ping`
  - `exec traceroute`
2. Make sure all KDBs are updated. For example, no pending updates, no out of date db and no updating.
3. Try submitting a lower throughput, (no archive file type, smaller file size) to see if it is still reproducible.
4. Follow the PCAP dumping guidelines to dump files from port1 or port2 to make sure the traffic is there. Open *capture 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 in the FortiNDR Administration Guide](#).

### 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>`

# 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	187C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	NA (0%)	No Risk	
2022/04/14 11:55:06	5E88DE1C3B112734A7B9499385088B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2	NA (0%)	No Risk	
2022/04/14 11:55:06	187C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78	NA (0%)	No Risk	
2022/04/14 11:55:06	187C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	NA (0%)	No Risk	
2022/04/14 11:55:06	187C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.78	NA (0%)	No Risk	
2022/04/14 11:55:06	5E88DE1C3B112734A7B9499385088B6DF	HTML	Clean	Sniffer		10.10.1.251	172.19.235.2	NA (0%)	No Risk	
2022/04/14 11:55:06	187C22A214949975556626D7217E9A39	HTML	Clean	Sniffer		172.19.235.2	172.19.235.76	NA (0%)	No Risk	

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

	Open Time	Session ID	Source Address	Destination Address	Severity
Host Story	2022/04/14 13:51:01	5597328	172.19.235.76	172.19.235.2	Not Anomaly
Virtual Security Analyst	2022/04/14 13:51:01	5597320	10.244.57.73	10.244.43.192	Not Anomaly
Network	2022/04/14 13:51:01	5597312	172.19.235.76	172.19.235.2	Not Anomaly
System	2022/04/14 13:51:01	5597304	172.19.235.76	172.19.235.2	Not Anomaly
User & Authentication	2022/04/14 13:51:01	5597296	172.19.235.76	172.19.235.2	Not Anomaly
Malware Log	2022/04/14 13:51:01	5597288	172.19.235.76	172.19.235.2	Not Anomaly
NDR Log	2022/04/14 13:51:01	5597280	192.168.101.63	192.168.101.61	Not Anomaly
Event	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*.

# Managing FortiNDR disk usage

## 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.

## 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.

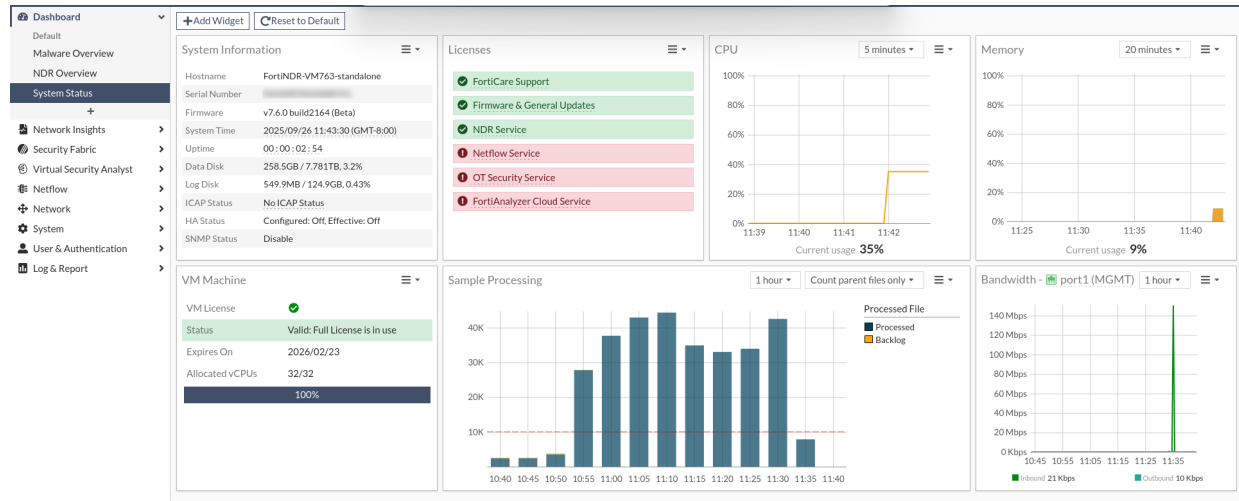
**Tip 2:** With FortiNDR 3500F, users can purchase more SSDs. Please see the data sheet and ordering guide for details.

**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.

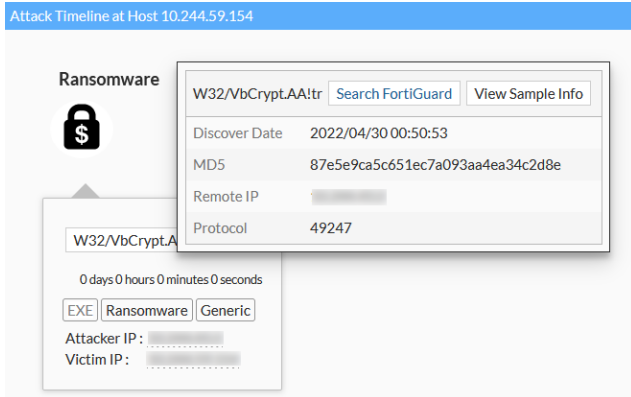
**To export detected malware files with the CLI:**

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**

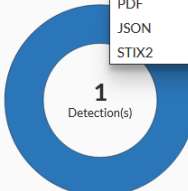


Ransomware

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	0A1BBC20973E0691A9D35A9ABA6108FBEC45263C0A0E5A8ECBB A9AC5EE5E6996		
SHA1	99A4EB3D57268604D0758A904B82CB406735CC0C		
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

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' is highlighted. The main area displays a table of logs with columns for Date, MD5, File Type, and Detection Name. The first row is selected, and its details are shown in a 'Details' pane on the right. The details pane includes a search bar, a 'View Detail Report' button, and sections for General information (File ID, Time, File Size, File Type, MD5), Detection information (Virus Name, Confidence Level, Threat Risk Level, Detection Type), Network information (Attacker IP, Victim IP, URL), and Device information (Device: Sniffer).

Date	MD5	File Type	Detection Name
2022/04/30 00:52:33	A3F3E85639E56868303C4716560AE5A7	HTML	HTML/Refresh.250C!tr
2022/04/30 00:52:33	BE5EC685F7D210F46ADD0884708C001F0	HTML	MOAT.AttrTag
2022/04/30 00:52:33	61D98B3423A16FF7A2381CB3869CD881	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:33	6993F1CF428A788229C37D87000059C6	HTML	MOAT.AttrTag
2022/04/30 00:52:33	CC4551CFDA35E140B36A8FF37738B96D	HTML	JS/ExploitKit.29C6!tr
2022/04/30 00:52:33	E1E777A357907F35B438661A6EF85A73	PDF	MOAT.AttrTag
2022/04/30 00:52:33	E1E777A357907F35B438661A6EF85A73	PDF	MOAT.AttrTag
2022/04/30 00:52:33	2E915432AD8142D70ADC936280887100	EXE	W32/Graftor.FL!tr
2022/04/30 00:52:33	C3FA38DD42B7C276ADDED1CCD508B569	EXE	W32/Al.Suspicious.2
2022/04/30 00:52:33	373C65D985C174D7368A8D496A777818	MSOFFICE	VBA/Emotet.2826!tr.dllr
2022/04/30 00:52:33	B141EA5708C154D62CC54A14E5F5B387	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	E08367D9D5B38B34DB3C52B05760AFA7	PDF	PDF/Phishing.0931!tr
2022/04/30 00:52:33	1D21C3EAD6E6EF978665002E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:33	51927D0C4151DDE90000E652B18557F5	PDF	MOAT.AttrTag
2022/04/30 00:52:33	36533114DFE6F69B0861FCA6007C100C	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	36533114DFE6F69B0861FCA6007C100C	PDF	PDF/Phish.6CAB!tr
2022/04/30 00:52:33	E08367D9D5B38B34DB3C52B05760AFA7	PDF	PDF/Phishing.0931!tr
2022/04/30 00:52:19	94D7F65B37588BD109F5B33946E86D46	HTML	MOAT.AttrTag
2022/04/30 00:52:19	2598DFB1E1C67B5B467259879B10A71F	HTML	MOAT.AttrTag
2022/04/30 00:52:19	8057821F44FAD32631847B9D0C2488A5	HTML	MOAT.AttrTag
2022/04/30 00:52:19	1D21C3EAD6E6EF978665002E0973E6F1C	HTML	JS/Redirector.QA!tr
2022/04/30 00:52:19	7DD7D15D6BE0D443EADF5D1E98D8EE6	HTML	JS/ScrInject.B!tr

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

## Formatting the database

To format the database with the CLI:

```
execute db restore
```



Using `execute db restore` will format and delete the entire database. Use caution when executing this command and backup detection beforehand if required.

## Rebuild RAID

- Rebuild RAID disk (3500F) on page 14
- Rebuild Raid for FortiNDR1000F, 2500G and 3600G on page 18

### Rebuild RAID disk (3500F)

To rebuild the data disk and perform a fresh configuration of the FortiNDR-3500F, follow the steps outlined in this procedure.



RAID rebuild will only work if the affected disk is under tolerance of the corresponding RAID configuration.

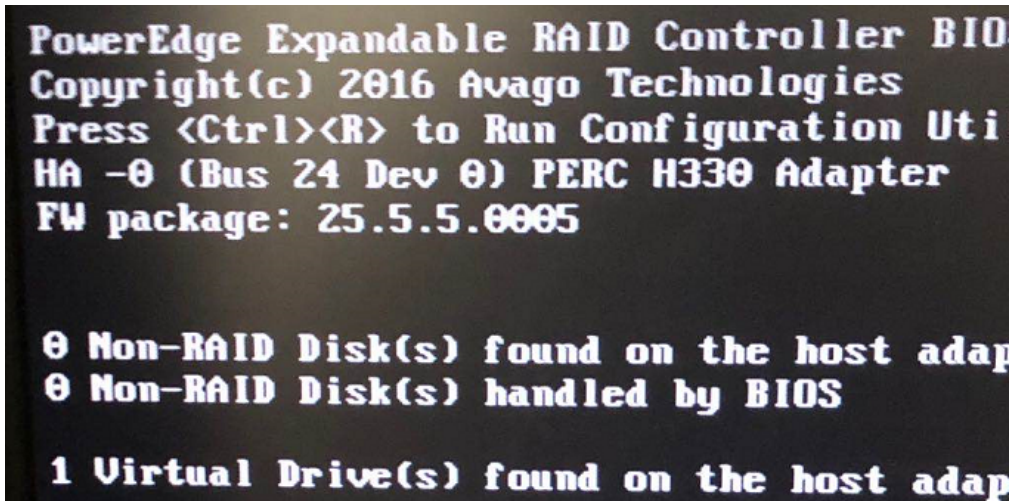
---

**To rebuild the RAID disk for FAI3500F and FNDR3500F:**

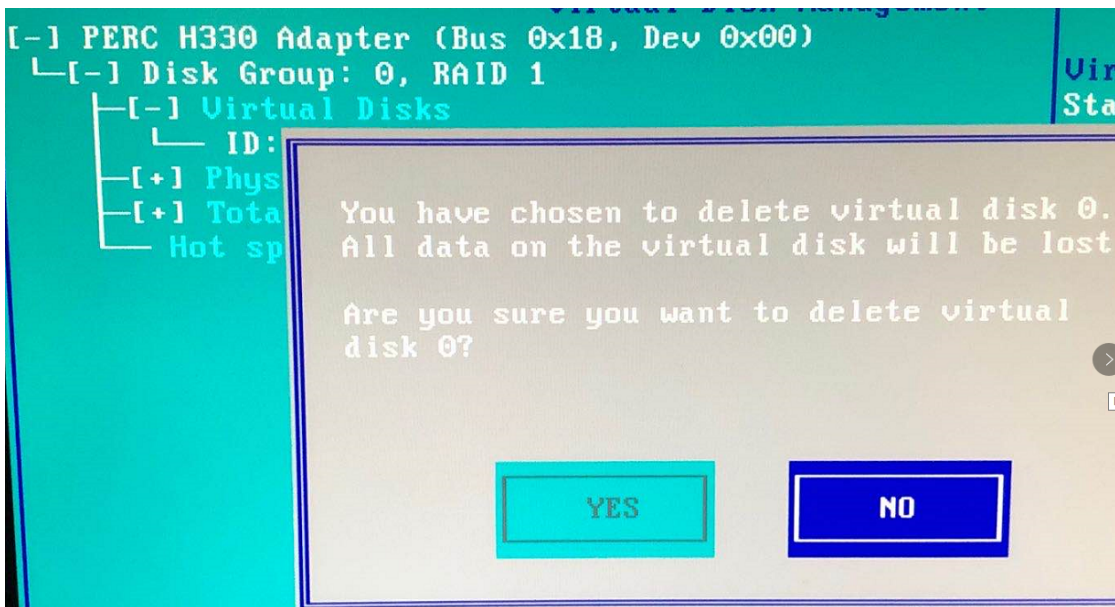
1. Plug the monitor and keyboard directly into FortiNDR.



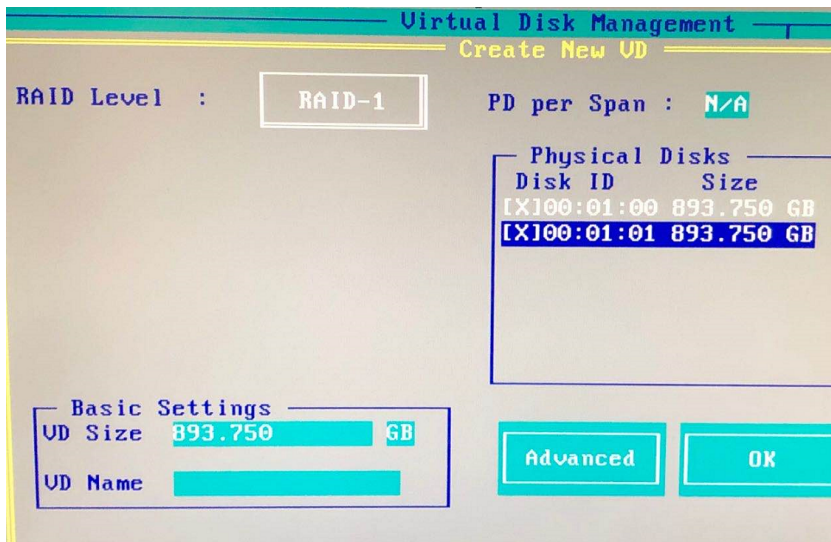
2. Boot FortiNDR and keep pressing `Ctrl R` when FortiNDR is booting.



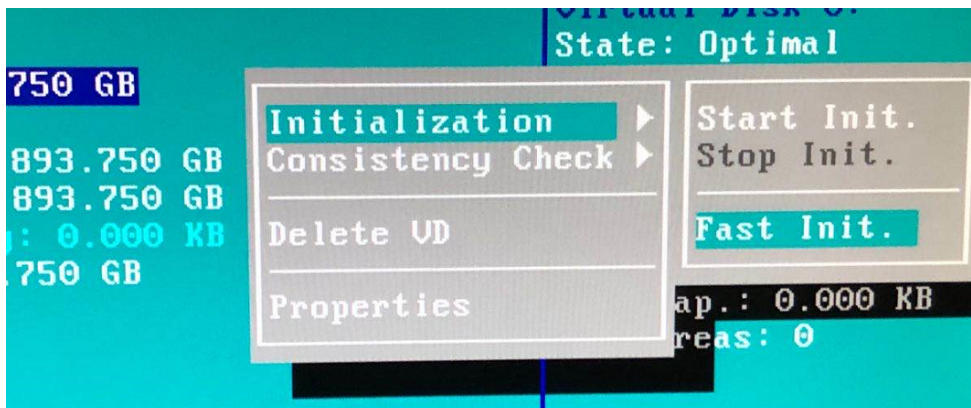
3. Delete virtual disk 0.



4. Create a virtual disk at RAID Level 1.



5. Fast init the new virtual disk.



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

```
COM2 - PuTTY
FortiBootLoader
FortiAI-3500F (14:05-07.24.2019)
Ver:00010001

Serial number:FAI35FT319000006
Total RAM: 391680MB
Boot up, boot device capacity: 7916MB.
Press any key to display configuration menu...
.
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter Selection [G]:

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

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

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

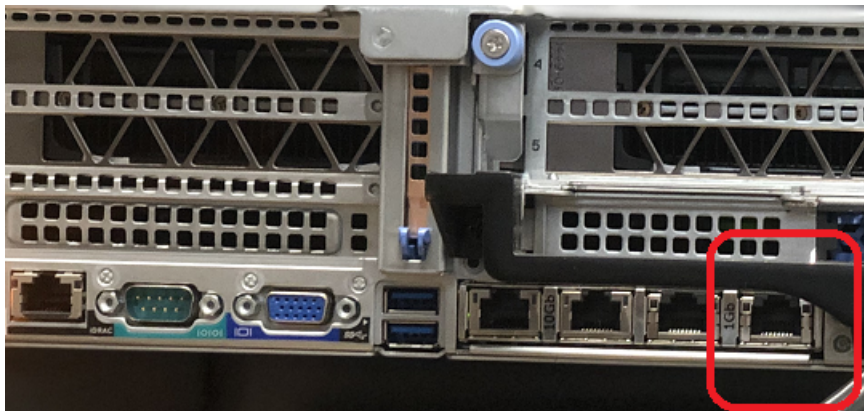
Please connect TFTP server to Ethernet port "0".

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

Total 412096kB unzipped.

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

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



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

## Rebuild Raid for FortiNDR1000F, 2500G and 3600G

This document explains how to rebuild a hardware RAID array on FortiNDR appliances after a single HDD failure, and preserves the data. It covers three models (FortiNDR-3000F, FortiNDR-3500F, and FortiNDR-3600G) and their default RAID configurations.

Model	Drive Count	RAID Level	Fault tolerance
FortiNDR-1000F	2	RAID 1 (mirror)	1 drive
FortiNDR-2500G	4	RAID 10	1 drive per mirror (2 total)
FortiNDR-3600G	12	RAID 5	1 drive

### Requirements:

- FortiNDR version 7.6.2 or higher.

### To rebuild a hardware RAID array on FortiNDR appliances:

1. Confirm which HDD is offline (`Offln`) or failed state by running the following CLI command: `get system raid-status-detail`

The slot map is based on a front view, and the order increases from bottom-left to top-right.

#### FortiNDR 1000F:

SSD label	EID:Slot (Displayed in output of CLI: <code>get system raid-status-detail</code> )
SSD1	69:0
SSD2	69:1



**FortiNDR 2500G:**

SSD label	EID:Slot (Displayed in output of CLI: <code>get system raid-status-detail</code> )
1	252:4
2	252:5
3	252:6
4	252:7



**FortiNDR-3600G:**

HDD label	EID:Slot (Displayed in output of CLI: <code>get system raid-status-detail</code> )
HDD1	252:0
HDD2	252:1
HDD3	252:2
HDD4	252:3
HDD5	252:4
HDD6	252:5
HDD7	252:6
HDD8	252:7
HDD9	252:8
HDD10	252:9
HDD11	252:10
HDD12	252:11





FortiNDR 1000F and 2500G use consecutive slots 252:0 – 252:1 and 252:0 – 252:3 respectively.

2. Remove the failed HDD and insert a new one of equal or larger capacity.
3. Check the status of the new HDD by running the CLI command: `get system raid-status`
4. Check the New HDD Status:
  - If the status is `UBad`, proceed to step 5
  - If the status is `UGOOD`, proceed to step 6
  - If the status is `REBUILDING`, proceed to step 7
5. Start the rebuild (FortiNDR 7.6.2+) with the CLI command: `exec raidrebuild start`  
If the rebuild operation is triggered, the output will display `start rebuild operation succ.`
  - To verify the HDD is rebuilding (`REBUILDING`), run: `get system raid-status`
  - To track the rebuild progress, run: `exec raidrebuild status`
6. If the rebuild process does not start, reboot the FortiNDR appliance. This will trigger the rebuild process. If the rebuild process has started, then do nothing.
7. Allow 12 to 24 hours to rebuild depending on the RAID size. Keep the appliance powered on.

## Hot swap drives in FortiNDR 3600 (v7.6.2 or later)

The FortiNDR 3600G supports hot-swappable drives, allowing you to replace a failed drive without shutting down the system. If issues arise during or after a drive replacement, perform the following steps to resolve the problem.

### To hot swap drives in FortiNDR 3600:

1. After inserting the replacement drive, verify RAID status with the following CLI command:  
`diagnose system raid-status`
2. If the array is not rebuilding automatically on 7.6.2 or later, run the following CLI command:  
`execute raidrebuild start`

## 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.

## 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.

For malware related FN/FP:

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 FortiNDR Sample Team</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 in the FortiNDR Administration Guide</a> .

For NDR/IPS signature related FN/FP:

Recommendation	Description
<b>Submit feedback to FortiGuard IPS team</b>	When you encounter a FP/FN for NDR/IPS signature, submit the related PCAP directly to <a href="mailto:vulnwatch@fortinet.com">vulnwatch@fortinet.com</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
```

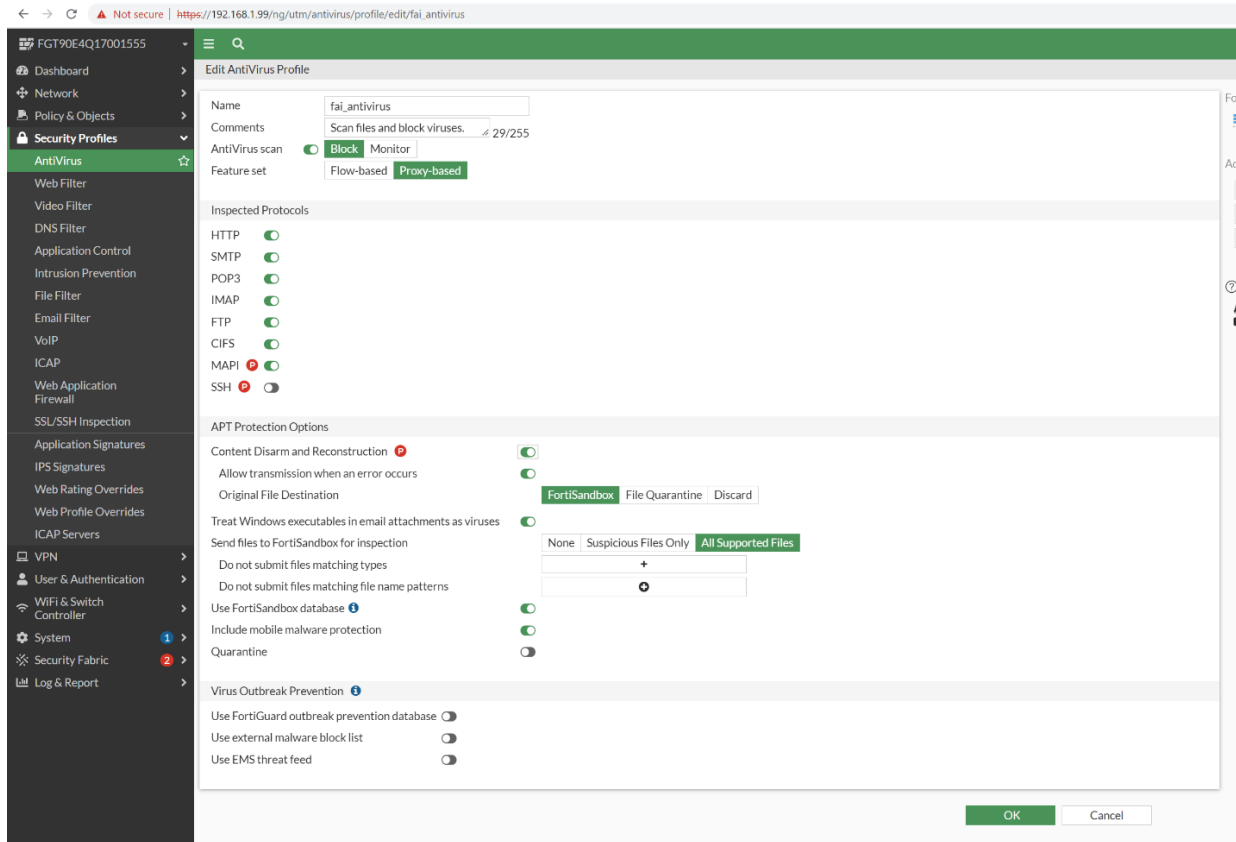
## To verify a device is authorized:

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

## To verify All Supported Files are enabled in FortiGate:

Go to *Security Profiles > AntiVirus* and verify *Send files to FortiSandbox for inspection* is set to *All Supported Files*.



### To verify the firewall policy is not blocking the connection:

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

# Troubleshoot Log Settings

## To troubleshoot the Client:

- Enable *Send logs* to your syslog server
- Verify you are using a valid remote server address
- Check if the GUI settings match Cmdb settings:
  - Send logs to FortiAnalyzer/FortiSIEM

Remote Log Server

Send logs to FortiAnalyzer/FortiSIEM  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"`

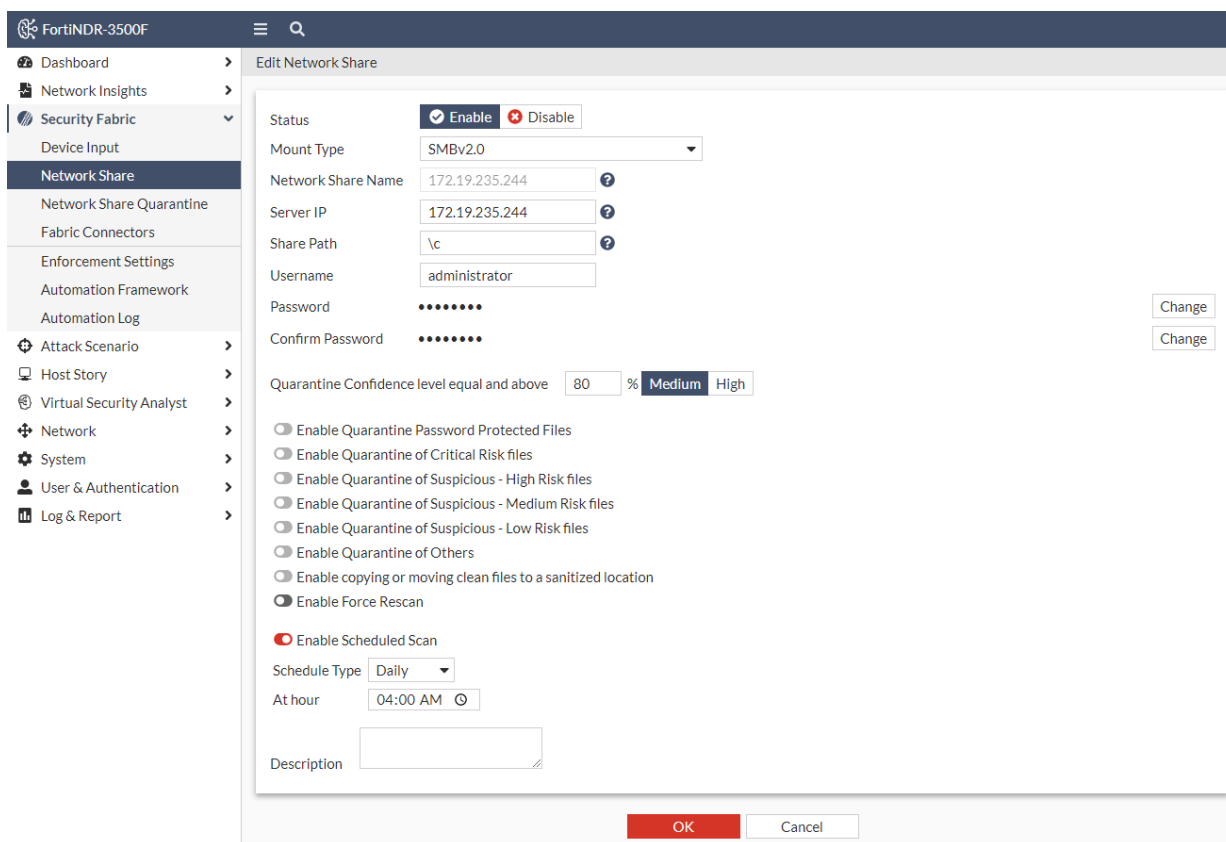
# Troubleshoot Network Share

## Test the Network Share Connection

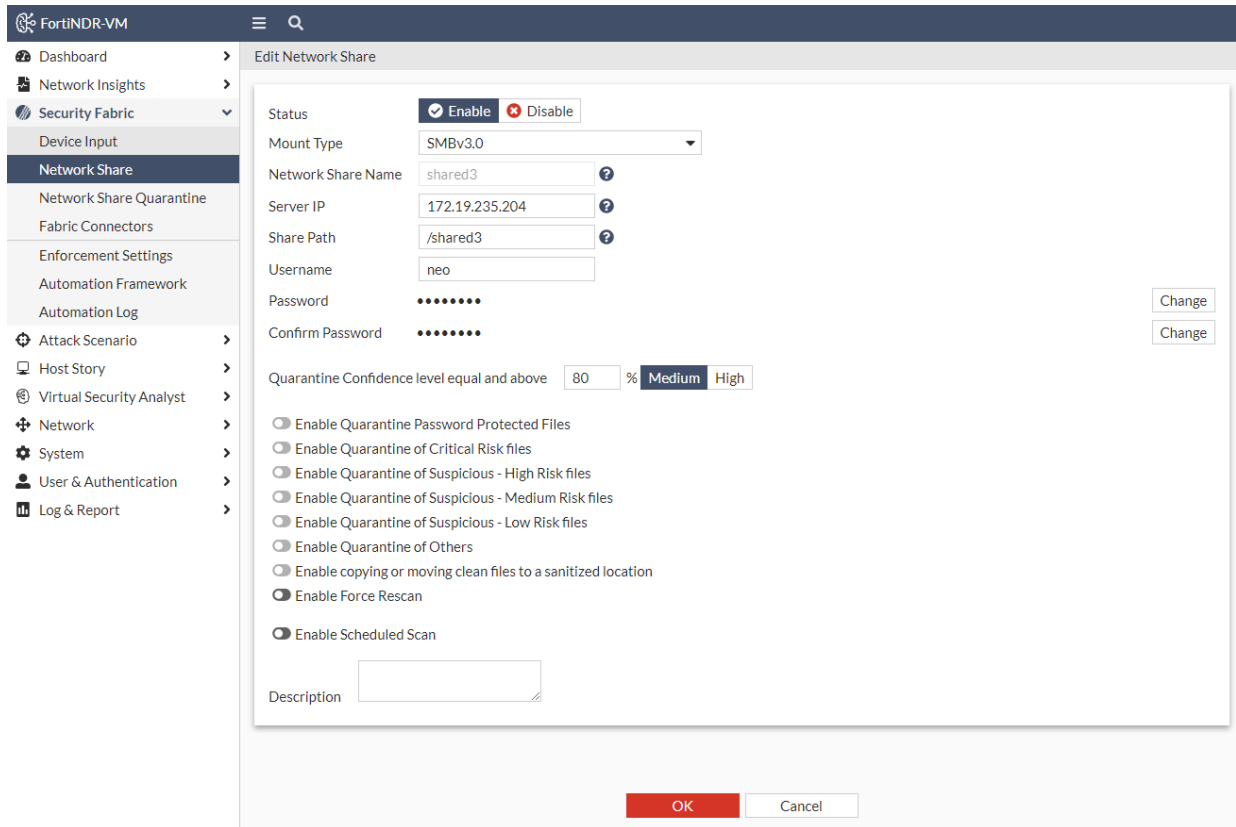
**To test the Network Share Connection:**

- Verify the Remote Server 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 chosen 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 show the Network Share configuration for Windows.



The following images show the Network Share configuration for Linux.



## Diagnosing Network Share Errors

### To diagnose Network Share scanning errors:

Run the following CLI commands:

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

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

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

**To troubleshoot mounting problems:**

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

```
diagnose debug kernel display
```

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

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

You will see the error code if the mounting failed.

**To troubleshoot a Network Share scan that it is stuck:**

A scanning job may get stuck for the following issues:

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

## 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.

## 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.

## Submit support tickets

If user has tried troubleshooting FortiNDR, and the issue still persist, please submit a support ticket via [Fortinet Support Site](#).

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

<b>TAC Report</b>	Generate and record the output from <code>execute-tac-report</code> . For more information, see <code>execute-tac-report</code> in the <a href="#">FortiNDR CLI Reference Guide</a> .
<b>For Sniffer and NDR related issue</b>	Minimal reproducible PCAP obtained using the CLI command <code>diagnose sniffer dump</code> . For more information, see <code>diagnose sniffer dump</code> in the <a href="#">FortiNDR CLI Reference Guide</a> .
<b>Model Name</b>	What model is your platform?
<b>Firmware Version</b>	Which firmware version is your platform on?
<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, <code>diagnose debug</code> in the <a href="#">FortiNDR CLI Reference Guide</a> .
<b>Kernel Log output</b>	Record the output from <code>diag debug kernel display</code> . For more information see, <code>diagnose debug</code> in the <a href="#">FortiNDR CLI Reference Guide</a> .
<b>Application Log Output</b>	Specified log output from affected application. For more information see, <code>diagnose debug</code> in the <a href="#">FortiNDR CLI Reference Guide</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 FortiAnalyzer/FortiSIEM, please provide logs from FortiAnalyzer/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 <a href="#">Backup or restore the system configuration in the FortiNDR Administration Guide</a> .
<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.



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

Copyright© 2025 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.