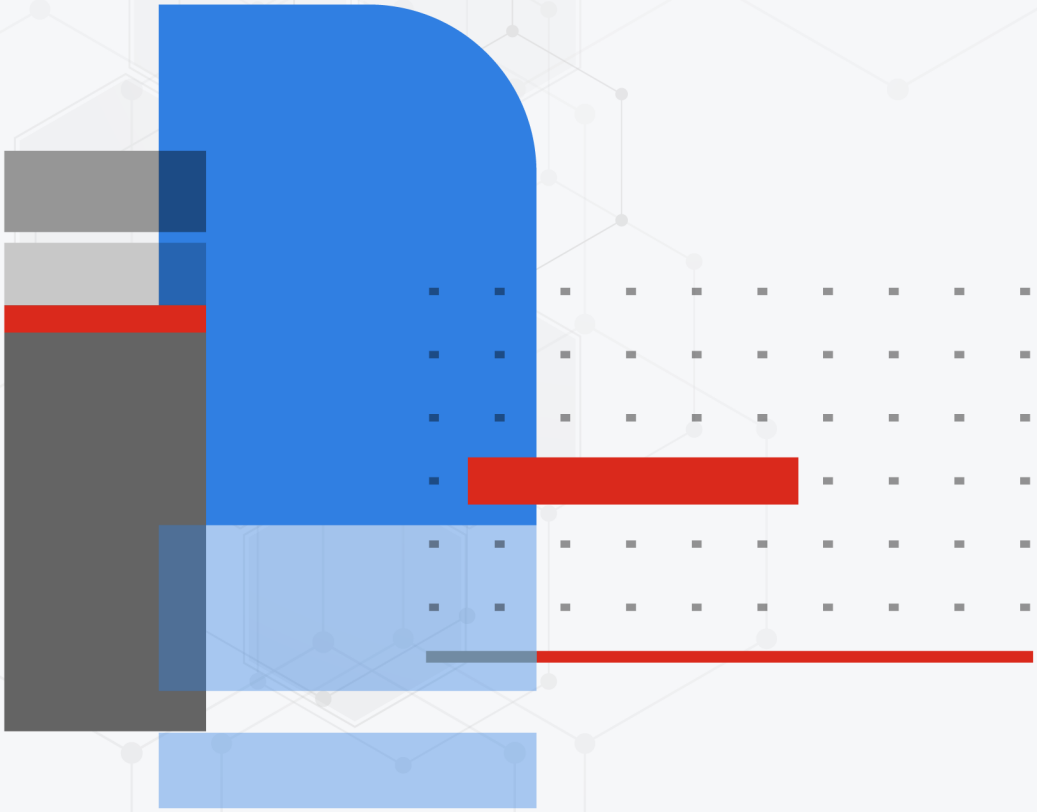
Troubleshooting Cheat Sheet

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

October 3, 2025
FortiNDR 7.6.3 Troubleshooting Cheat Sheet
55-760-1171529-20250618

TABLE OF CONTENTS

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

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

Recommended Debug Setup:

- A syslog server for FortiNDR events log as the GUI only has *1 days* events.
- A TFTP server for PCAP capture transfer 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	`diagnose debug crashlog <crash_log_date>`
Record kernel related logs from the bootup and save it to a file	`diagnose debug kernel display`

File scanning related issues

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

To perform a general check:

1. Check and record network conditions from the FortiNDR server to file submitting clients using the following CLI commands:
   - `exec ping`
   - `exec traceroute`
2. Make sure all KDBs are updated. For example, no pending updates, no out of date db and no updating.
3. Try submitting a lower throughput, (no archive file type, smaller file size) to see if it is still reproducible.
4. Follow the PCAP dumping 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	`diagnose system csf global`
Record output and make sure status is *authorized*	`diagnose system csf upstream`
Collect logs	`diag debug enable` and `diag debug application csfd 7`

Manual Upload/API Submission/FortiSandbox Integration

For all issues:

Start with a single file upload and fetch results from the same subnet as directed from where the client resides. See Appendix A - API guide 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`

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

To turn network traffic detection on and off:

Run the following command:

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

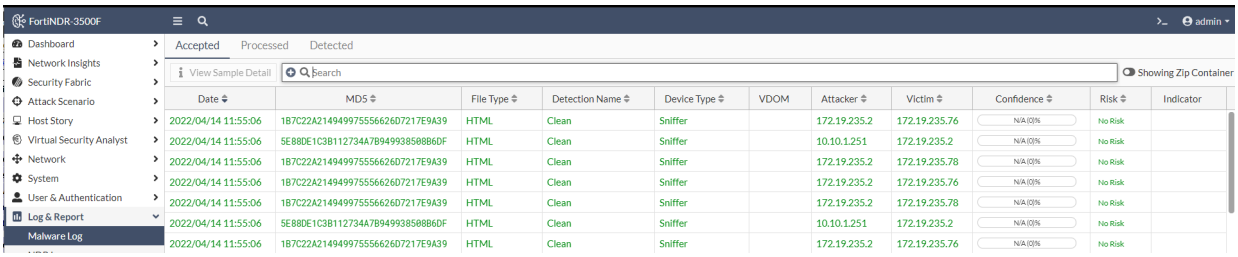
To turn sniffer malware detection on and off for troubleshooting:

Run the following command:

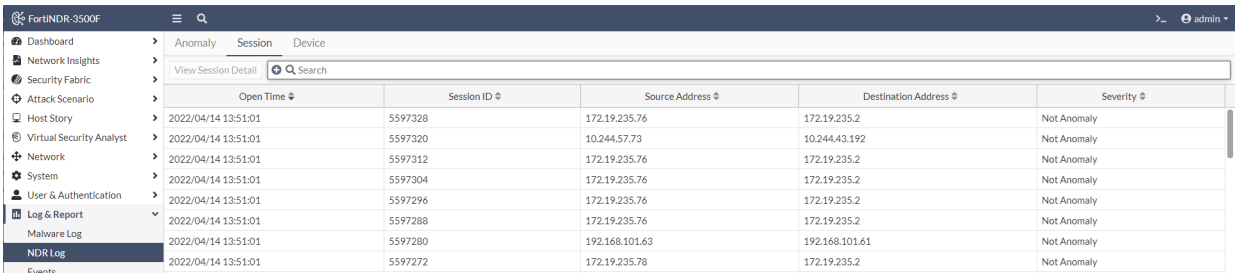
```
exec snifferd <on/off>
```

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

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



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



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.

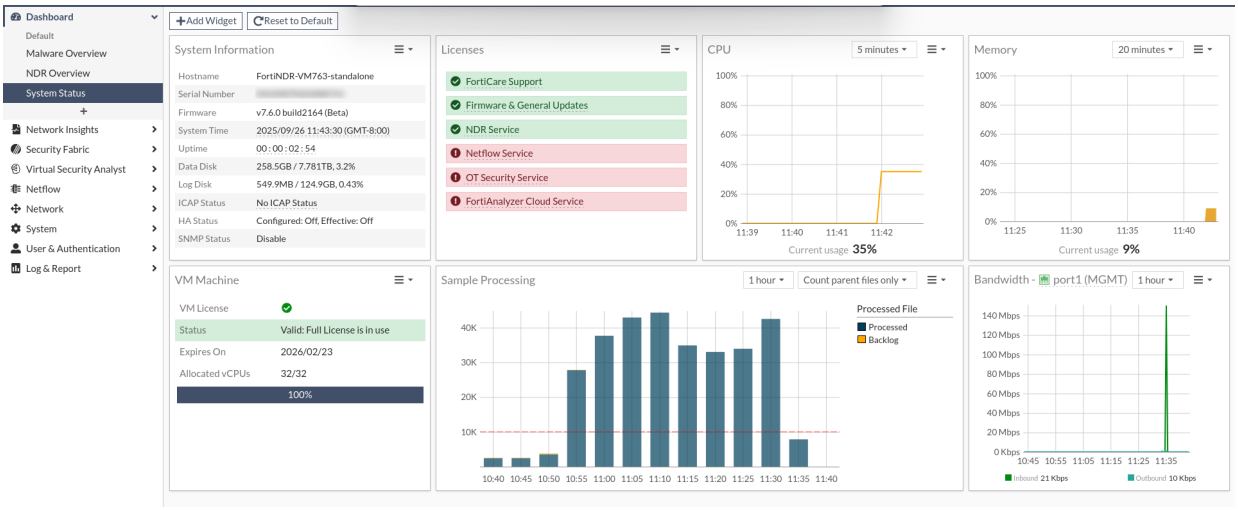
Tip 2: With FortiNDR 3500F, users can purchase more SSDs. Please see the data sheet and ordering guide for details.

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

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

To view the disk usage:

Go to *Dashboard* > *System Status*.



To expand FortiNDR VM storage with the CLI:

```
execute expandspooldisk.
```

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

Exporting detected malware files

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

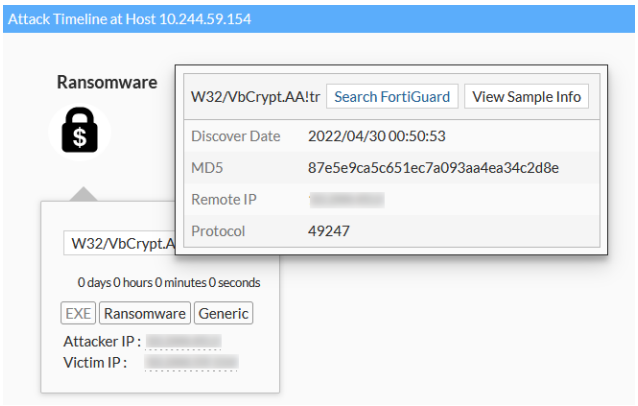
To export detected malware files with the CLI:

```
execute export file-report
```

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

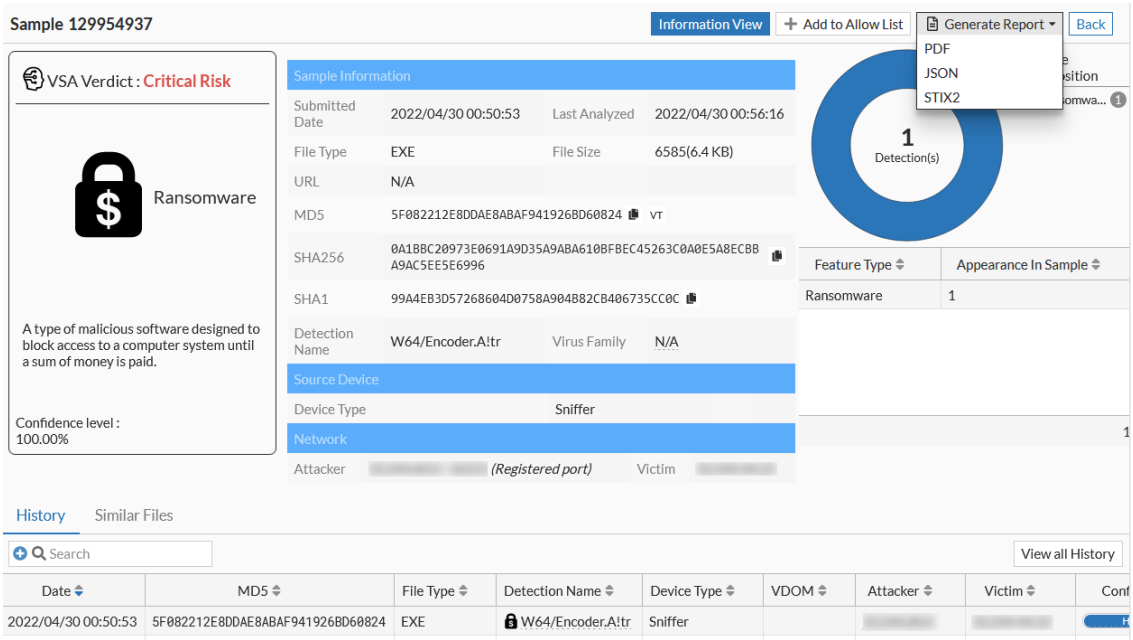
To export detected malware files with the GUI:

1. To export detected files under *Attack Scenario*:
   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.

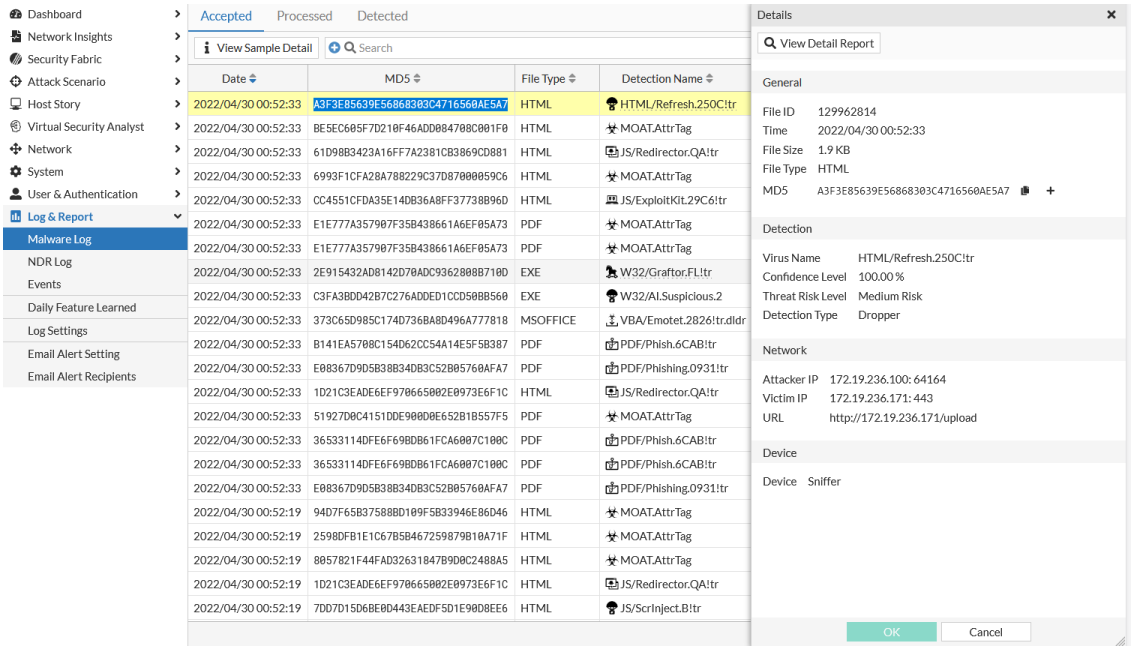


c. Click *View Sample Info*. The sample information is displayed.

d. Click *Generate Report* and select *PDF*, *JSON*, or *STIX2* format.



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.



   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)

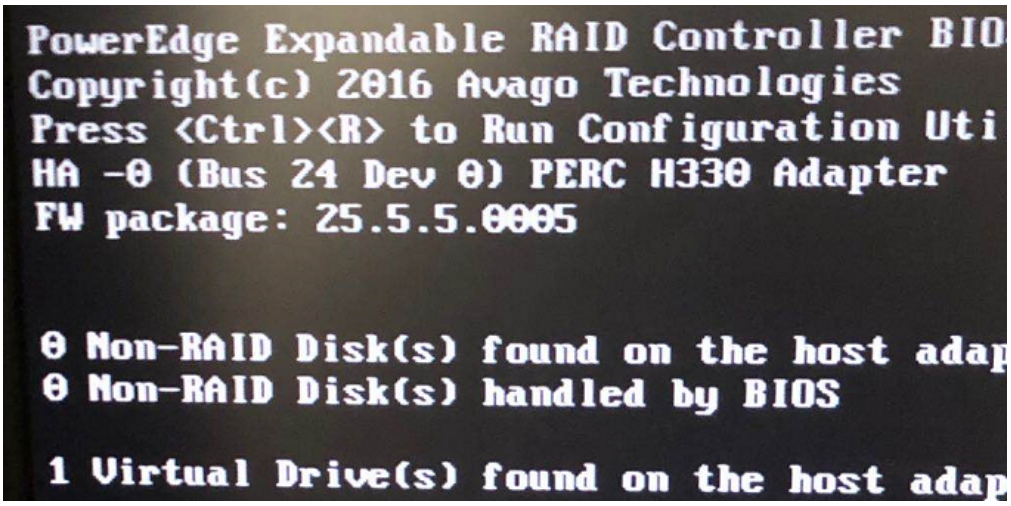
To rebuild the data disk and perform a fresh configuration of the FortiNDR-3500F, follow the steps outlined in this procedure.

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

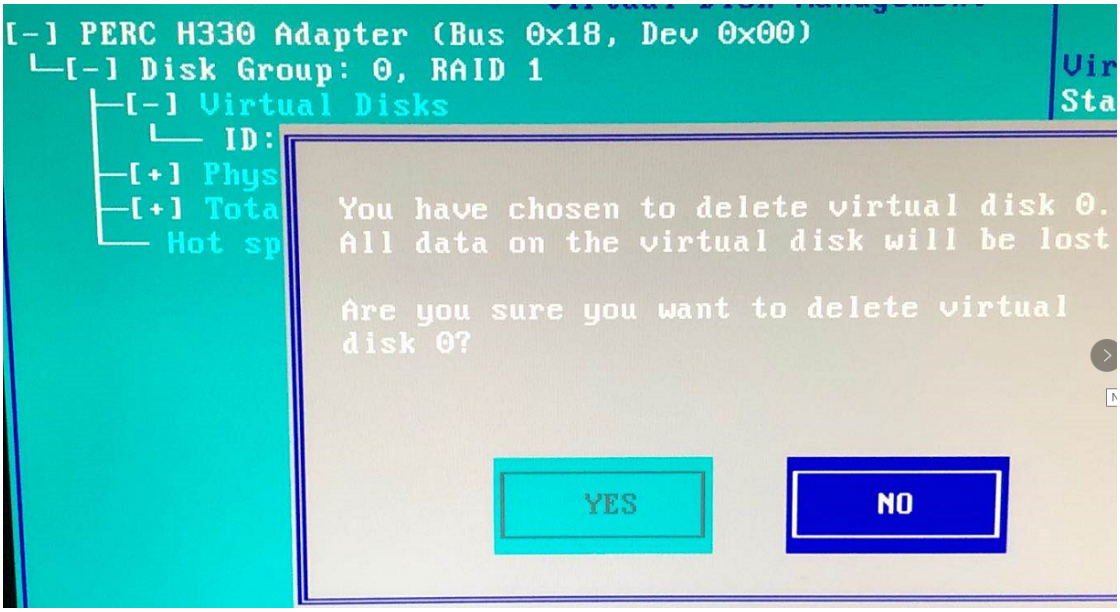
To rebuild the RAID disk for FAI3500F and FNDR3500F:

1. Plug the monitor and keyboard directly into FortiNDR.

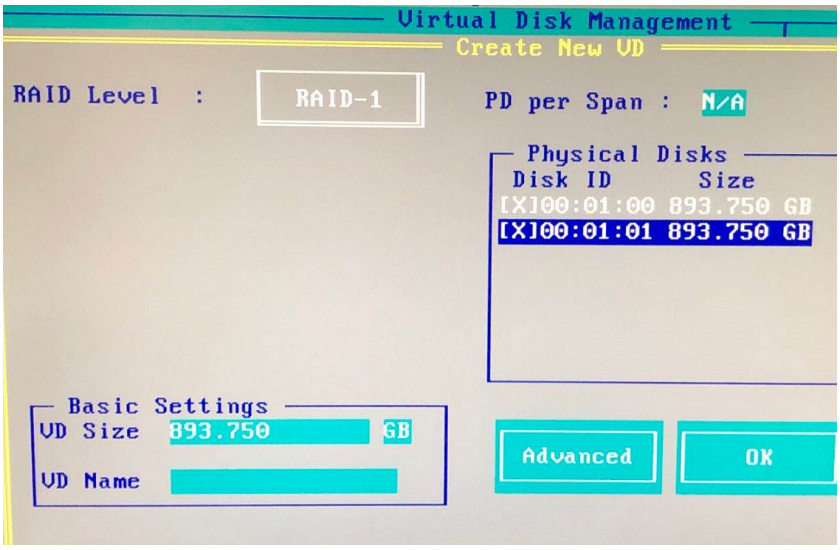
2. Boot FortiNDR and keep pressing `Ctrl R` when FortiNDR is booting.



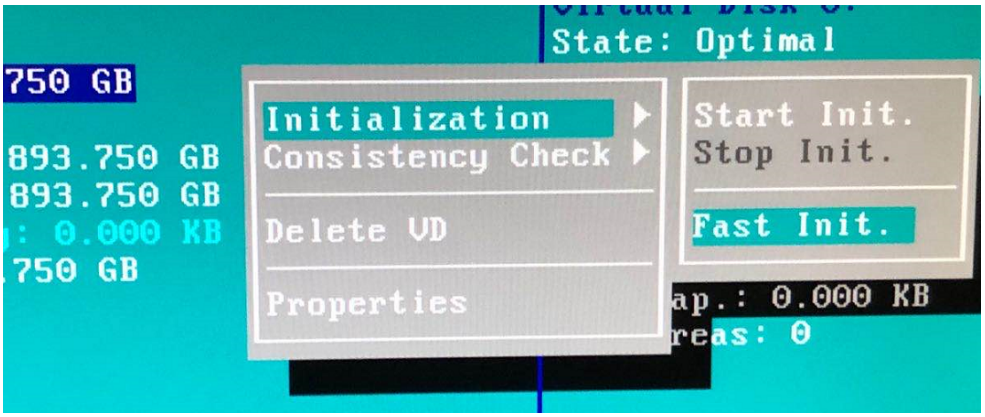
3. Delete virtual disk 0.



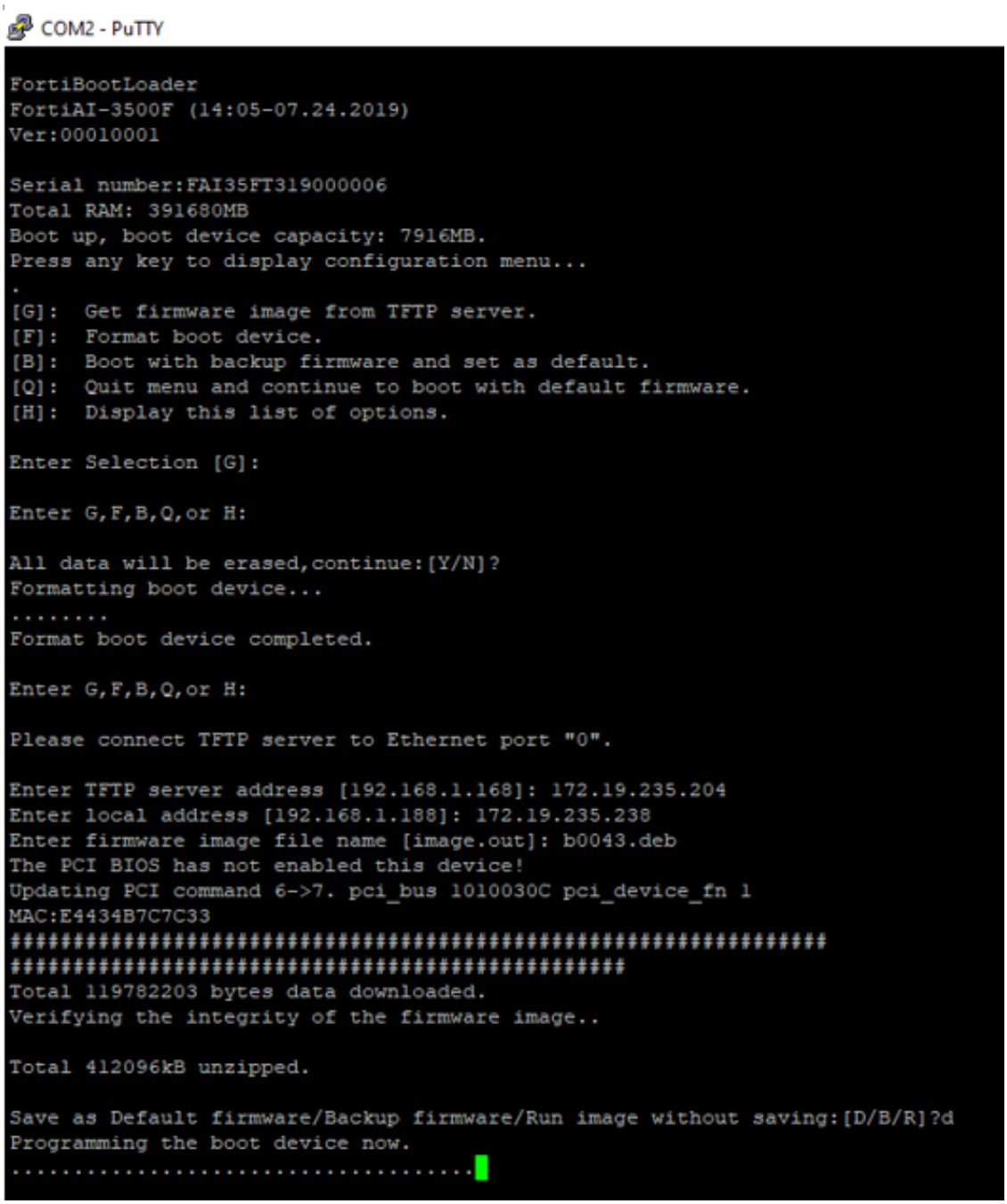
4. Create a virtual disk at *RAID Level 1*.



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.



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: `get system raid-status-detail`)
SSD1	69:0
SSD2	69:1

FortiNDR 2500G:

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

FortiNDR-3600G:

HDD label	EID:Slot (Displayed in output of CLI: `get system raid-status-detail`)
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} <filenmame-to-be-saved> <server>[:ftp port] <user-
     name> <password>
```

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

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

The zip file default password is `infected`.

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

For NDR/IPS signature related FN/FP:

Recommendation	Description
Submit feedback to FortiGuard IPS team	When you encounter a FP/FN for NDR/IPS signature, submit the related PCAP directly to vulnwatch@fortinet.com.

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
```

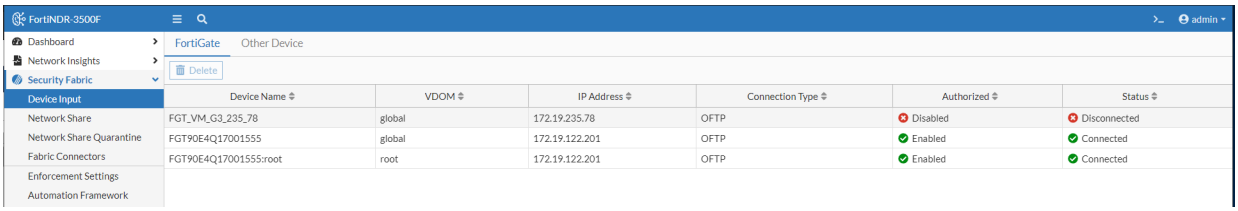
To check OFTP traffic in port1:

Use the CLI command:

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

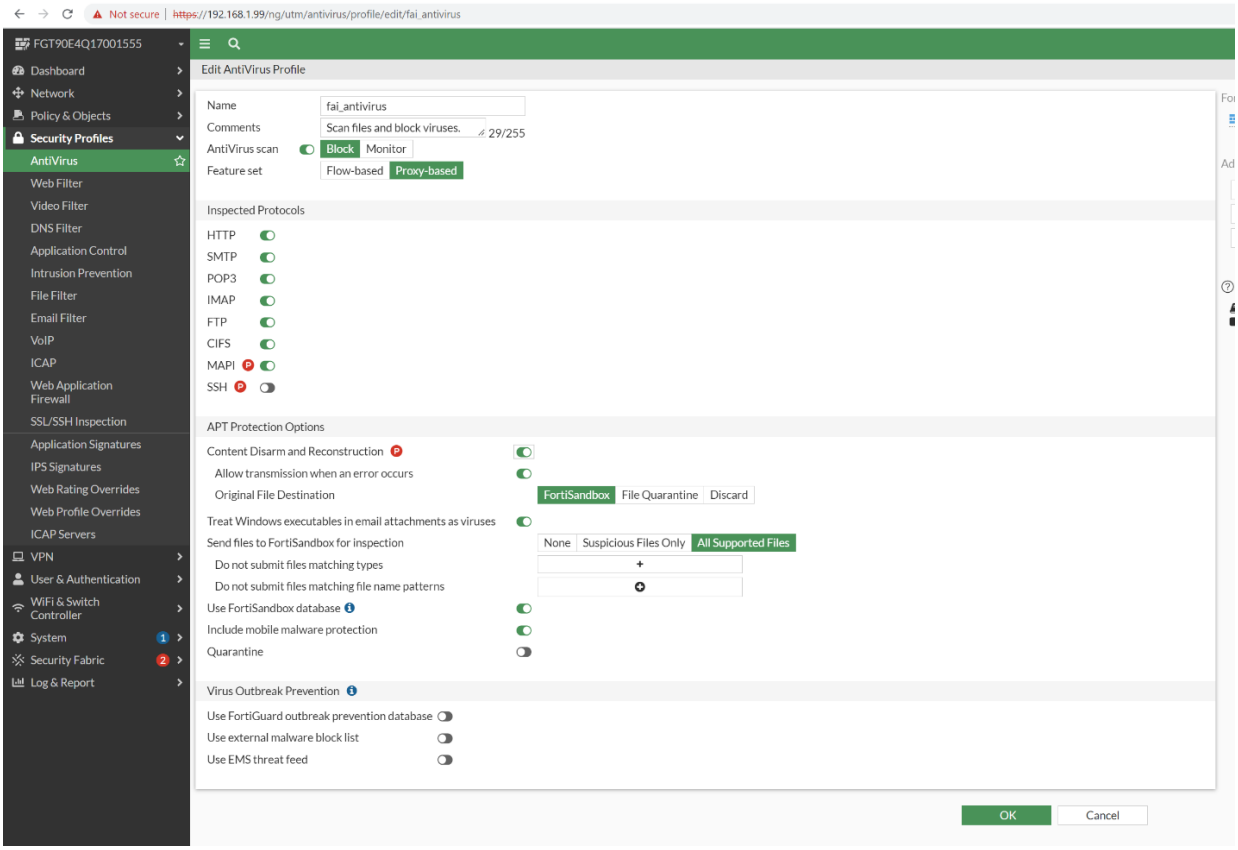
To verify a device is authorized:

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



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

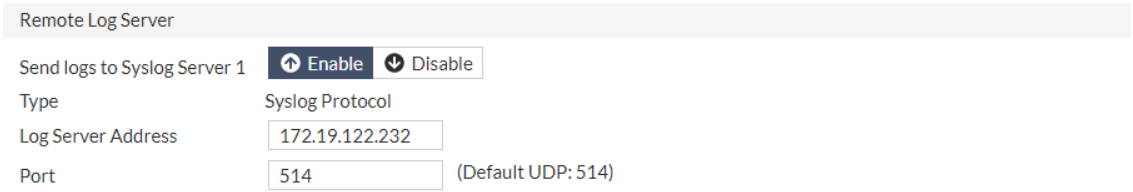
To troubleshoot the Client:

- 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


```
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
```

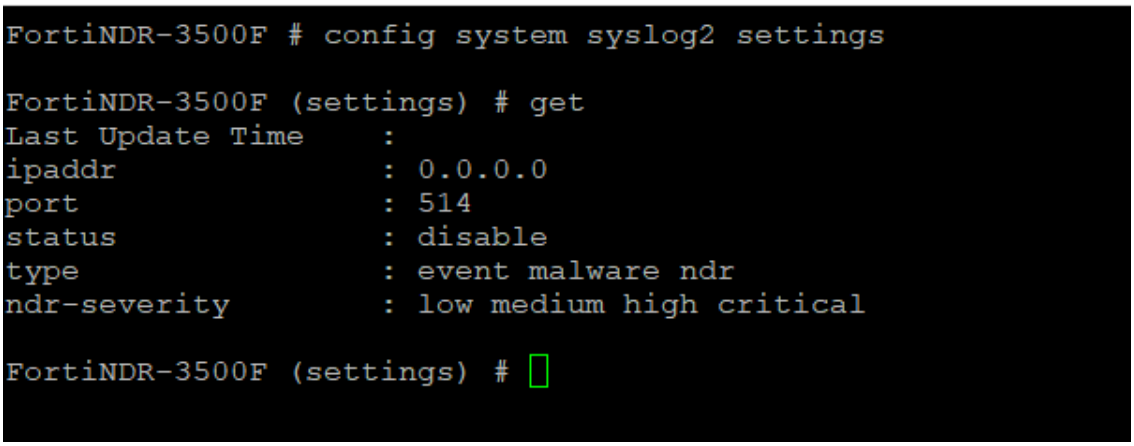
  - Send logs to Syslog Server 1




```
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



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"
  ```

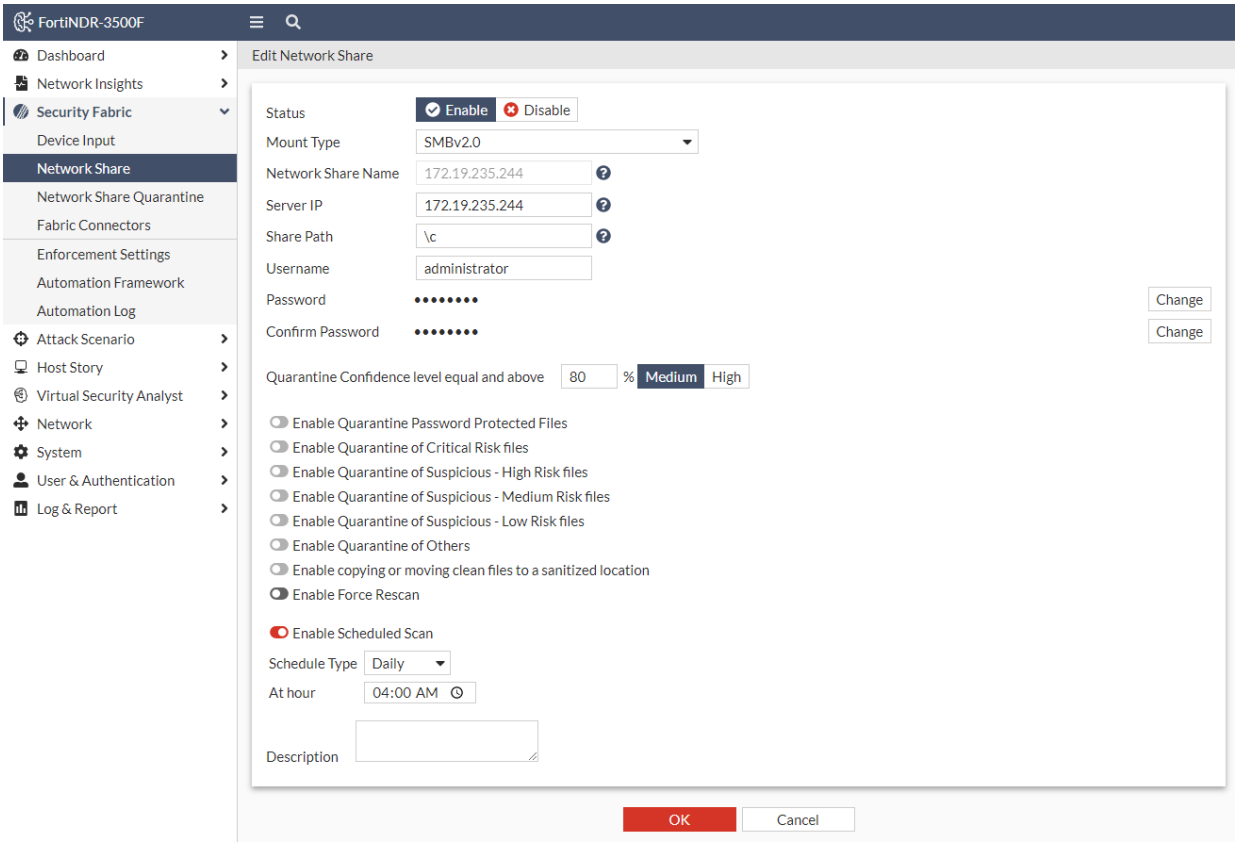
Troubleshoot Network Share

Test the Network Share Connection

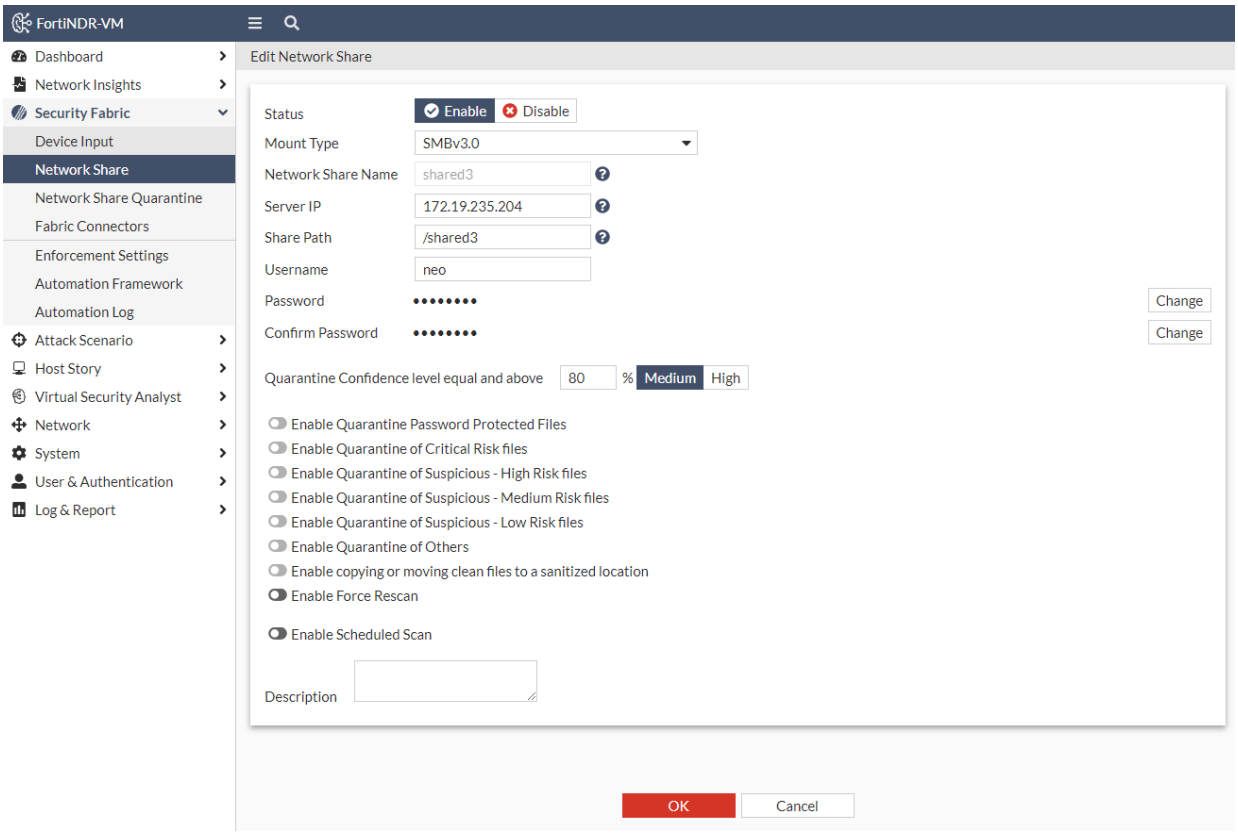
To test the Network Share Connection:

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

To troubleshoot mounting problems:

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

```
diagnose debug kernel display
```

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

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

You will see the error code if the mounting failed.

To troubleshoot a Network Share scan that it is stuck:

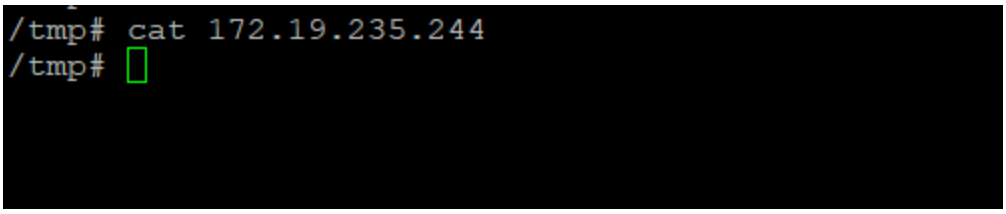
A scanning job may get stuck for the following issues:

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

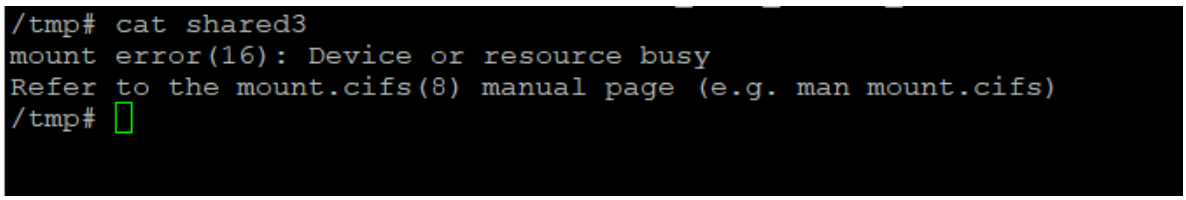
Debug version image

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



- Otherwise, refer to *mount.cifs*, *mount.nfs* documents



- 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. Enure FortiNDR's port UDP 2055, 6343, and 9995 are open. To monitor the packets, run the following CLI command:
   `diagnose sniffer packet`

   For example: `diagnose sniffer packet port1 'port 9995'`
2. Verify that HA mode is *off*. Netflow does not support HA: secondary mode.
   Run the following CLI command:
   `get system status`

   ```
   Hostname:                      FNDR-1KF-
   HA configured mode:            Off
   HA effective mode:             Off
   Strong-crypto:                 enabled
   ```
3. Check the logs to see if there are any crashes related to the flow daemon. The following CLI commands can retrieve logs:
   `diagnose debug crashlog <crash_log_date>`
   `diagnose sys top`
   `diagnose deb database error`
4. Try reloading the daemon with the CLI:
   `execute reload [<daemon_name>]`

If you use the command `execute netflow on`:

1. Be aware that it takes time for the daemon to activate after running `execute reload` and the daemon does not immediately indicate that it is on. We recommend waiting a few seconds before checking its status.

Submit support tickets

If user has tried troubleshooting FortiNDR, and the issue still persist, please submit an support ticket via Fortinet Support Site.

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

TAC Report	Generate and record the output from `execute-tac-report`. For more information, see `execute-tac-report` in the FortiNDR CLI Reference Guide.
For Sniffer and NDR related issue	Minimal reproducible PCAP obtained using the CLI command `diagnose sniffer dump`. For more information, see `diagnose sniffer dump` in the FortiNDR CLI Reference Guide.
Model Name	What model is your platform?
Firmware Version	Which firmware version is your platform on?
Always Reproducible	True/False
Reproducible Steps	If this issue is reproducible, please include the steps to reproduce this issue.
Actual Result vs Expected Results	What are the expected results and actual results?
Troubleshooting recommendations used	Please describe the troubleshooting recommendations you attempted and the outcome.
Crash Log output	Run the following CLI command `crash_log_date` and provide the output. For more information see, `diagnose debug` in the FortiNDR CLI Reference Guide.
Kernel Log output	Record the output from `diag debug kernel` display. For more information see, `diagnose debug` in the FortiNDR CLI Reference Guide.
Application Log Output	Specified log output from affected application. For more information see, `diagnose debug` in the FortiNDR CLI Reference Guide.
Database Error Log	Record the log output from `diag deb database error-log`.
FortiNDR Event Log	If configured with FortiAnalyzer/FortiSIEM, please provide logs from FortiAnalyzer/FortiSIEM. Otherwise, please include a screen shot from *Event* tab.
Client-Side Log	When FortiNDR acts as a server role (ICAP, OFTP and HTTP2 inline blocking etc.), please also include logs from the client side.

System Status	Provide the CPU and MEM usage when the issue occurs.
FortiNDR configuration	How many ports are configured/used? How many applications are used, and how are they configured? If you have a backup configuration file, please include it in your support ticket. For more information, see Backup or restore the system configuration in the FortiNDR Administration Guide.
FortiNDR Load	For configured applications, how much load are applied. For example: • For AV, how many files are being sent to FortiNDR, and what is the file size distributions and file type distributions? • For NDR, what is the bandwidth for traffic and what is the distribution of application type?
For non-hardware platform:	
Virtual machine provisioning	• How many CPU/Mems are provisioned? • How was the disk provisioned: Thin, Thick, etc.
Hosting hardware specifications	CPU Model Number, RAM Channels, DISK model number.
Physical hosting hardware load	A historical log of host hardware status to indicate CPU and MEM usage.

www.fortinet.com