Release Notes

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

January 14, 2026
FortiNDR 7.6.3 Release Notes
55-763-1180361-20250114

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-03	Initial release.
2025-10-15	Updated System integration and support on page 19.
2025-01-14	Updated Supported models on page 24.

Introduction

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

FortiNDR version 7.6.3

This document provides information about FortiNDR version 7.6.3 build 0656.

These Release Notes include the following topics:

Licensing

Please refer to the FortiNDR ordering guide for licensing details:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortindr.pdf.

Customers must have the correct SKU for FortiNDR functionalities to work.

Netflow and OT Security Services licenses

Netflow and OT Security Services licenses are ordered separately for sensors and standalone deployments.

Expired licenses

License expiration affects VMs and hardware appliances differently:

License	Service impact
VM	• The sniffer and IPS/ANN engine continue to process traffic with existing signatures, however users will lose access to the GUI, which redirects to the license upload page. • Users will lose access to any FortiGuard updates (ANN, IPS, IOT updates, etc). • Users lose access to any FortiGuard service lookups (webfilter, IOC lookups). • If the VM is in Sensor mode, it will stop syncing data to Centers.

Hardware	• The sniffer and IPS/ANN engine continues to process traffic with existing signatures. GUI access remains available in this case.
	• Users will lose access to any FortiGuard:
	  • Updates (ANN, IPS, IOT updates, etc)
	  • Service lookups (webfilter, IOC lookups)
	• If a physical appliance is in Sensor mode, data sync with any configured Center will continue and is not affected by the expired FortiNDR license.

OT	• Users lose access to any FortiGuard OT updates. • Traffic is processed with any existing OT signatures on the system.
Netflow	• Access to existing processed Netflow results in GUI is turned off. • The Netflow collector daemon and Netflow traffic processing are turned off.

There is no grace period for expired licenses.

New features and enhancements

This document provides information about FortiNDR version 7.6.3 build 0656.

The following is a summary of new features and enhancements in version 7.6.3.

For details, see the *FortiNDR7.6.3 Administration Guide* in the Document Library.

View user account information in the Sessions tab

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

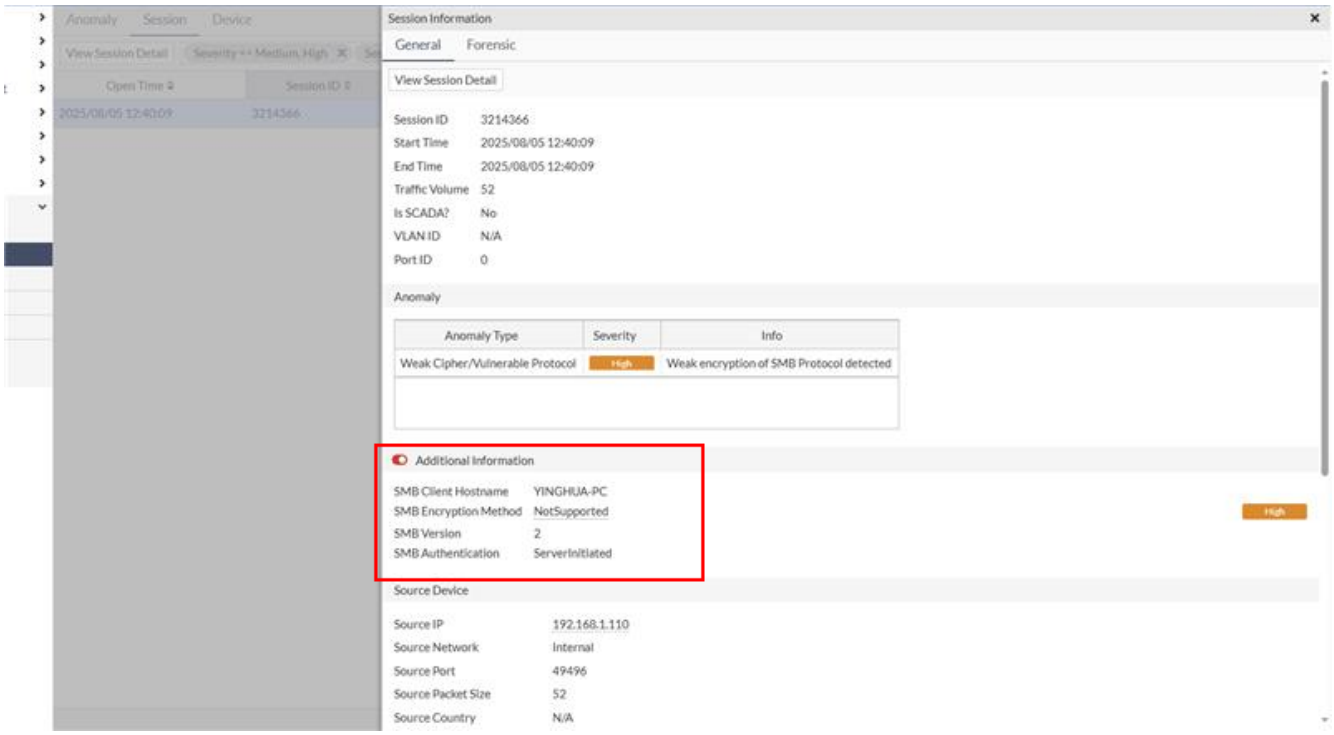
- SMB (Server Message Block) y version 1
- POP3 (Post Office Protocol version 3)
- IMAP (Internet Message Access Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Kerberos

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

To view the account Information:

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

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

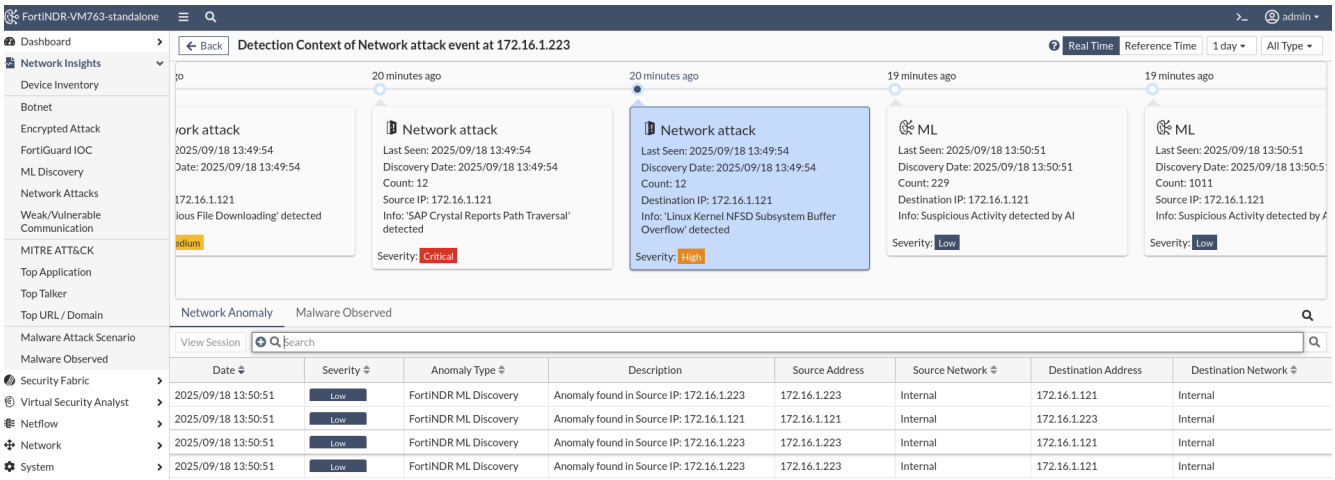


Detection context

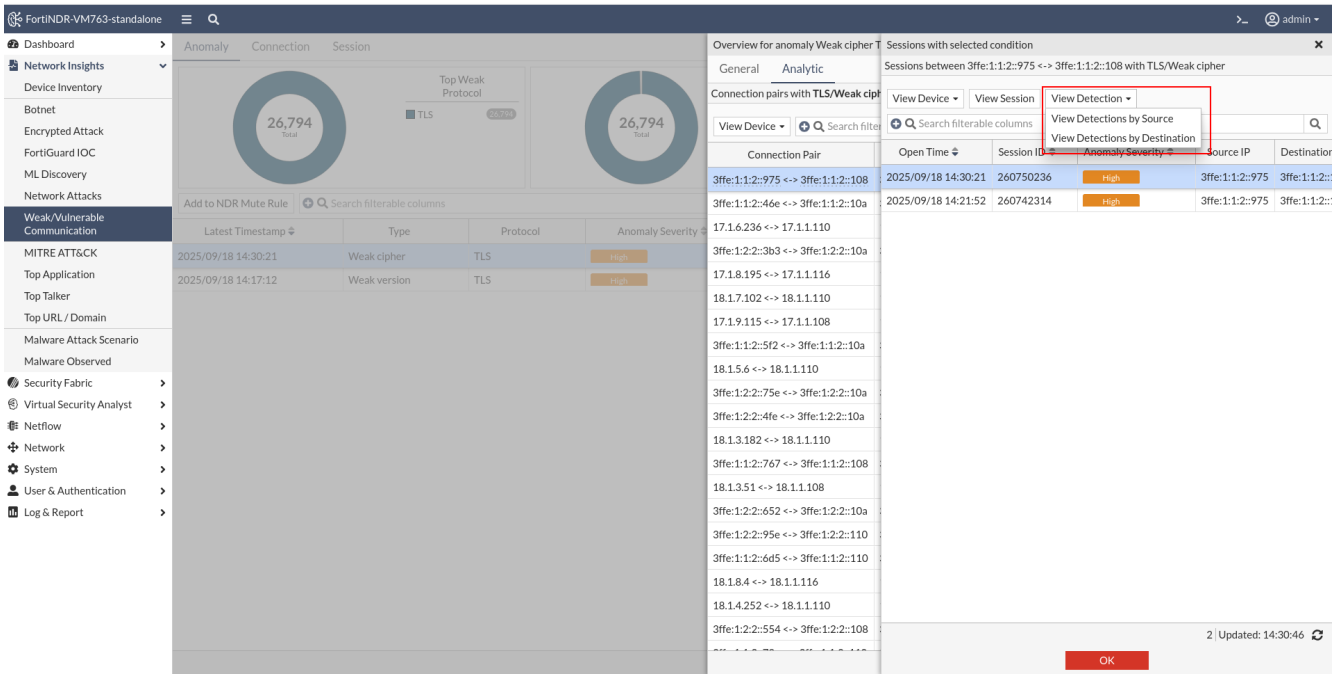
The *Detection Context* page allows you to view both malware and NDR detections in a single timeline. The page focuses on a specific IP address and a selected anomaly event, displaying all anomaly events surrounding the targeted event within a chosen time frame (1 day, 1 week, or 1 month). The timeline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

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

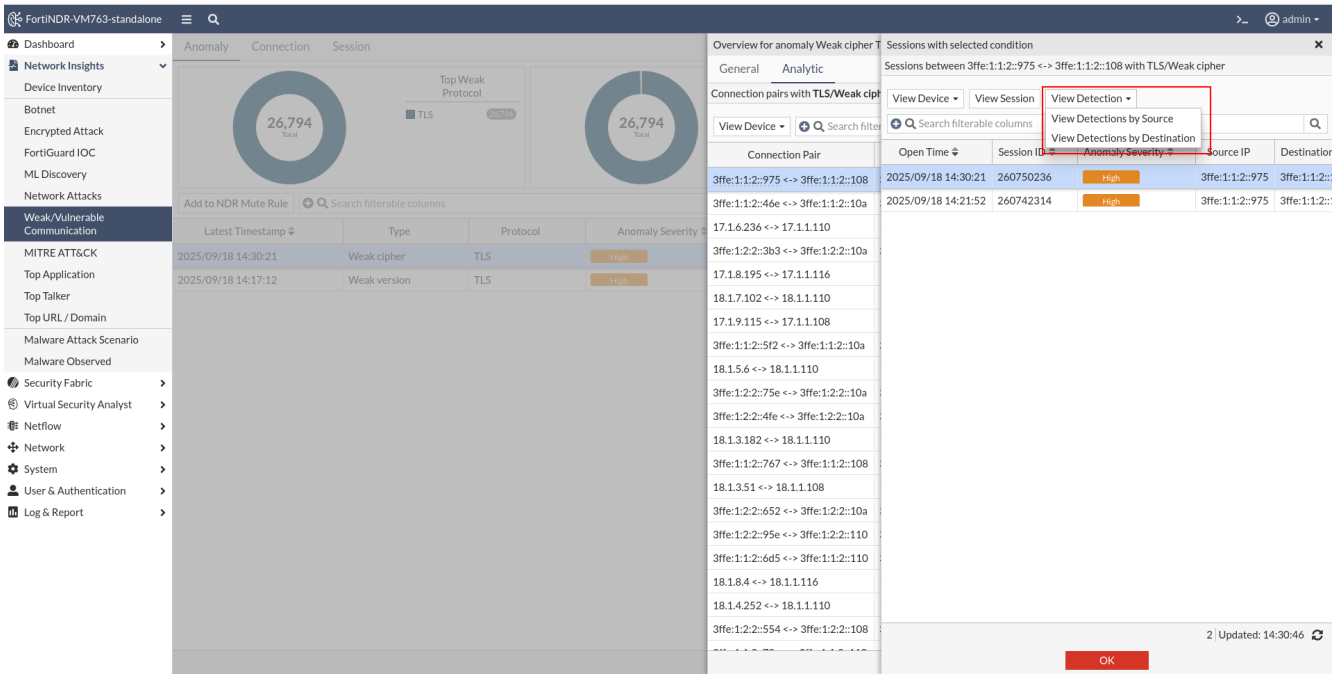
The *Network Anomaly* and *Malware Observed* tables below the timeline display ungrouped anomaly events or malware detection events individually, as shown in the timeline graph. The table can support up to 5,000 entries.



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



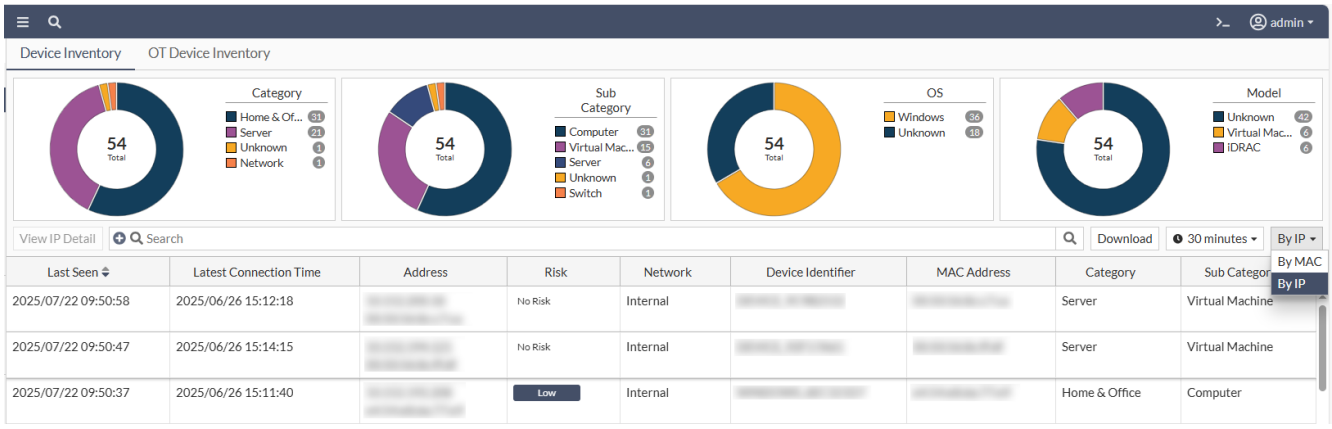
You can also access the *Detection Context* from the *Anomaly* tab or NDR logs by clicking a detection pair in the *Analytic* tab.



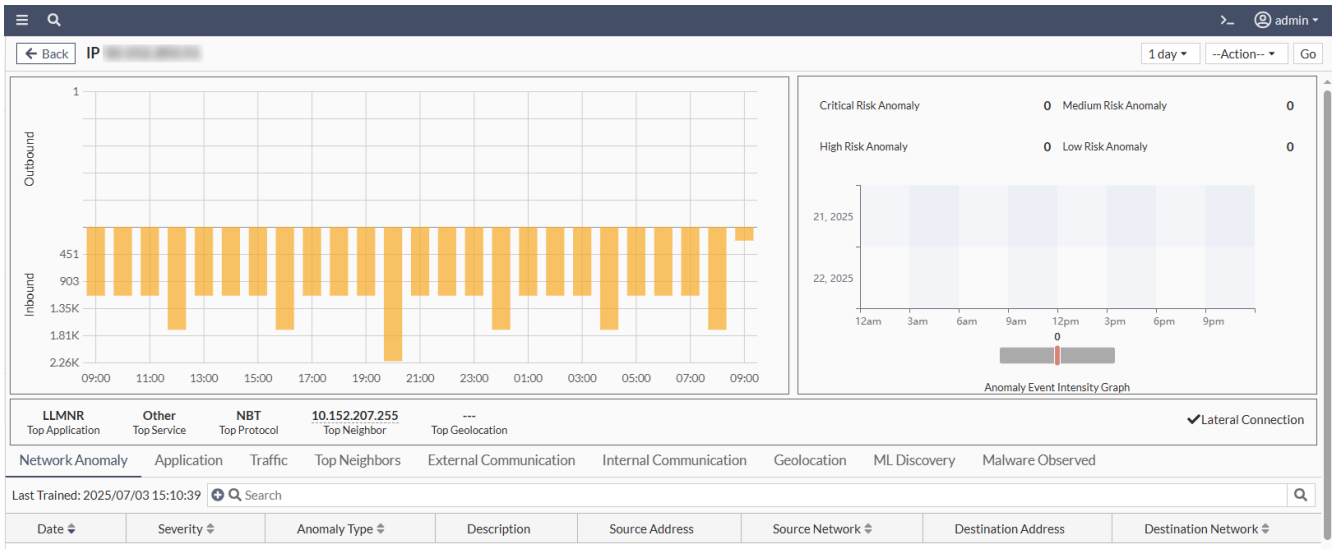
View device inventory by Mac or IP address

You can now use the view selector on the right corner of the *Device Inventory* table to view devices *By Mac* or *By IP*.

- *By MAC*: Each row represents a unique device identified by its MAC address. The IP address shown is the most recent one used by that device.
- *By IP*: Each row represents a unique IP address. The MAC address shown is the most recent device that used that IP.

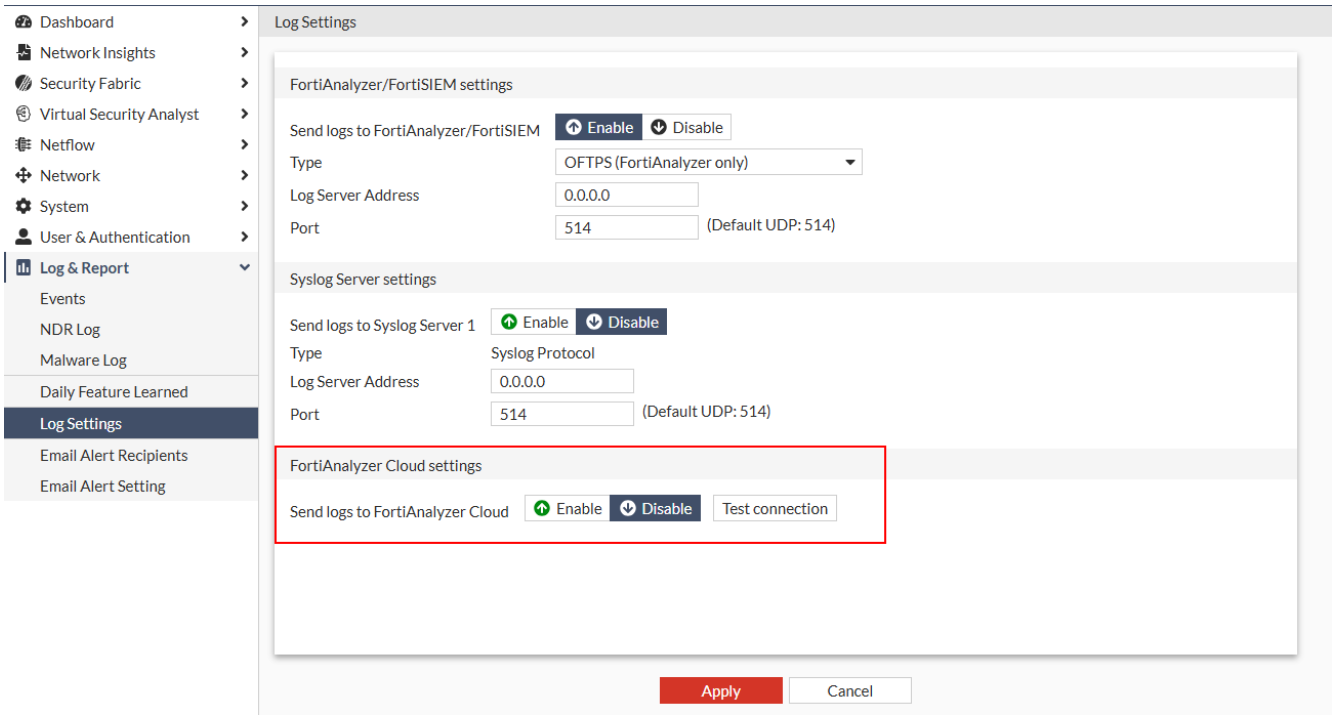


In *By IP* mode, selecting a row and clicking *View IP Detail* opens a page similar to the *Device Detail* view in *By MAC* mode. However, all information is based on the selected IP rather than the MAC address.



Log settings

The *Log Settings* can now be configured to send logs to FortiAnalyzer Cloud.



ML configuration and discovery

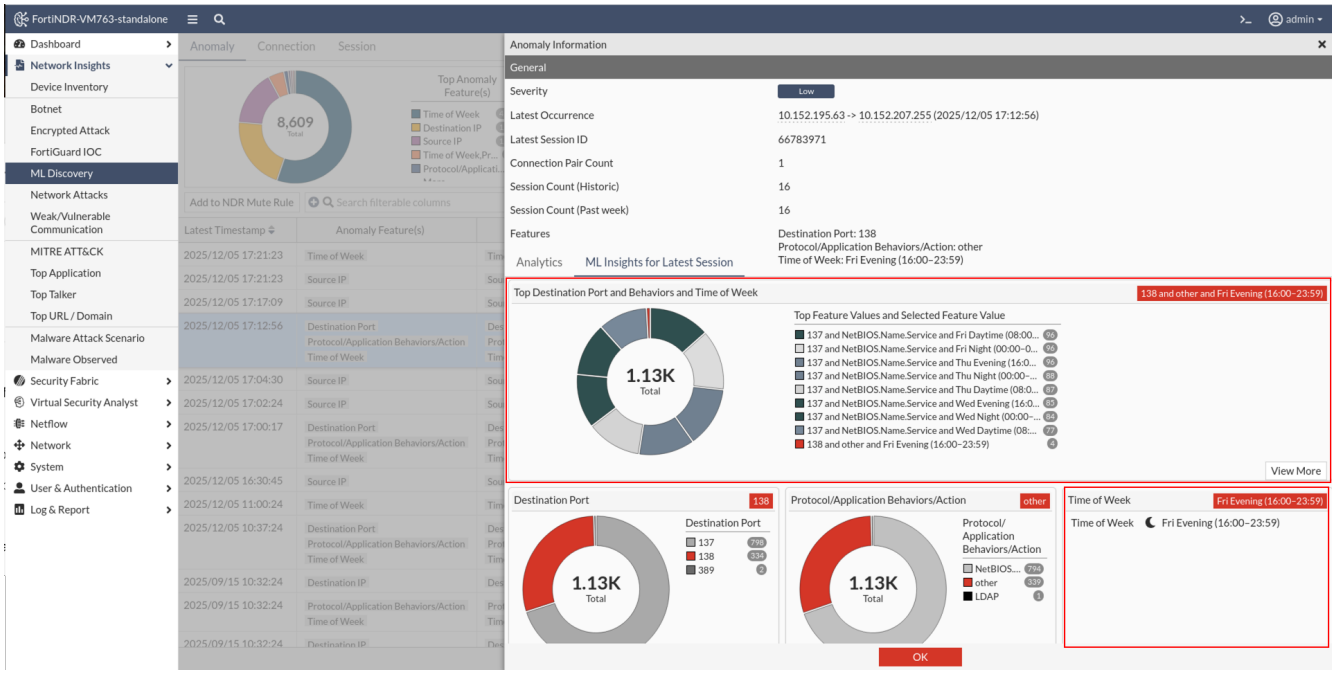
A new *Time of Week* option was added to the *ML Configuration* page to view anomalies based on the time of the week. During Machine Learning training, the system establishes a baseline of activity for each source IP. If traffic is observed during a time period where the baseline is zero (meaning no activity is expected) it is flagged as an anomaly. These anomalies are displayed in the *Time of Week* widget on the *Anomaly Information* page.

The time ranges are defined as follows:

- Daytime: 08:00-15:59
- Evening: 16:00 – 23:59
- Night : 00:00 – 07:59

The *ML Insights* charts displays the cumulative number of sessions observed since the start of training. You can hover over any time period to view the exact session count.

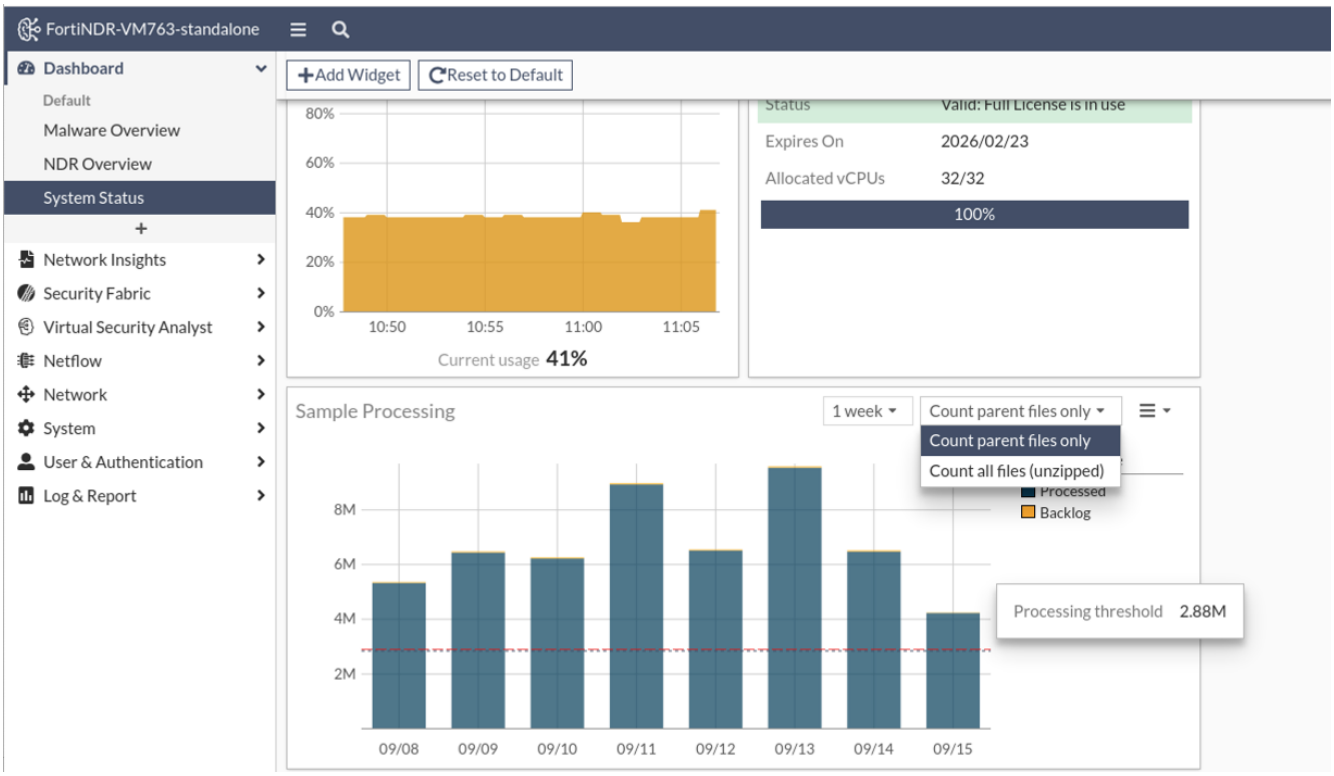
- A red tile indicates anomalous time periods. These had zero sessions during training but now show activity.
- An empty tile represent time periods with no sessions recorded since training began.



Sample processing widget

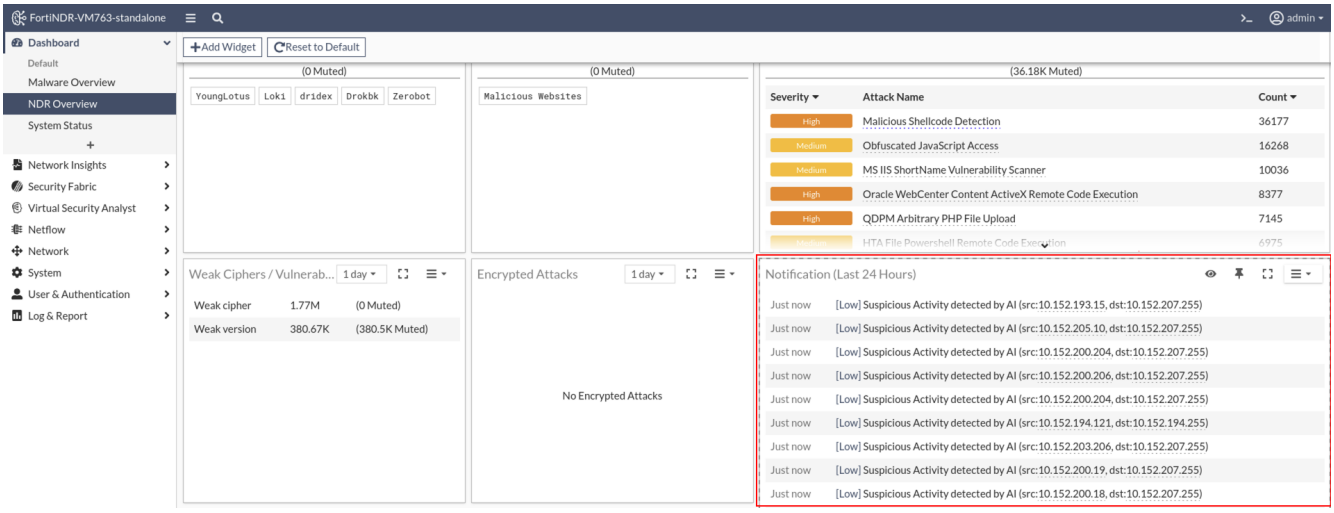
The *Sample Processing* widget has been enhanced with a new *Processing threshold* indicator. This red dotted line represents the maximum recommended processing rate for the specific appliance or VM model in use, based on the system's expected capacity as defined in the product datasheet. The performance threshold indicator will only appear when the number of accepted files approaches the threshold. The line remains hidden when file volume is significantly lower.

For example, in a VM32 deployment, the system is rated to process approximately 120,000 files per hour. Multiplied over 24 hours, this equates to a daily capacity of 2.88 million files, which is reflected by the *Processing threshold* line on the graph.



Notifications widget

Push notification functionality has been added to the *Notifications* widget.



IOC detection improvements

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

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

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

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

Global investigations

Global investigations are now supported in Central Management VM in addition to FNR-3600G. Before upgrading, please be aware of the following:

- After upgrade, queries used in 7.6.2 or earlier will not work with the new enhanced table. Users are recommended to run the existing queries and save results before upgrading to 7.6.3. All preconfigured queries have been updated to be compatible with the new enhanced tables.
- Queries in 7.6.3 do not support file-based operations (e.g. `virus_name`, hashes etc).
- Tags from 7.6.2 in previous NDR sessions and Malware file logs will be removed after upgrade.

Device enrichment

Version 7.6.3 introduces Active Directory (AD) integration for both Sensor and Center modes. This update also adds Import and Export Configuration options to the settings, making it easier to replicate, back up, or restore configurations.

Custom IP Signature

The new `config ips custom` CLI command allows you to create or modify custom Intrusion Prevention System (IPS) signatures on a FortiGate device. You can use the command to define detection patterns, assign severity

levels, add comments, and enable or disable the signature as needed.

CLI

For detailed information about CLI commands, please refer to the FortiNDR CLI Reference.

New CLI:

- `config system fortiguard ioc`: Use this command to configure FortiNDR to query IOC (Indicator of Compromise) data from a custom FortiGuard server instead of the default.
- `config system fortiguard webfilter`: Configure how FortiNDR connects to the FortiGuard Web Filter service, which classifies URLs and domains during traffic analysis and threat detection.
- `config system syslog cloud settings`: Use this command to configure FortiAnalyzer Cloud as the syslog destination. FortiNDR will send logs with the specified type and severity (applicable only to NDR-type logs) to the configured destination.
- `diagnose system db-fix-metadata`: This command diagnoses and resolves database loading issues caused by incompatible metadata.
- `diagnose system kafka-reset`: Use this command to reset the NetFlow Kafka flow by dropping and recreating the related NetFlow Kafka tables.
- `execute backup entire-db`: Use this command to create a full backup of the entire ClickHouse database and store it at the specified location `<filename-to-be-saved>`. The backup includes all databases, tables, and metadata except for System tables, temporary information and cache tables.
- `execute export logs`: Use this command to export the FortiNDR debug logs into a single compressed archive file. It helps gather diagnostic logs in an organized manner, thereby facilitating issue analysis, troubleshooting, and system verification.
- `execute factoryreset-shutdown`: Use this command to reset FortiNDR to its factory default settings for the currently installed firmware version. The system will shut down after execution and all current configurations will be lost.
- `execute restore entire-db`: Use this command to perform a full restoration of the ClickHouse database from a previously saved backup file `<saved-filename>`. The restore operation retrieves the backup from the specified source and restores it to the local device.

Updated CLI:

- `diagnose debug application`: Updated to include `filearch` logs for Standalone and Sensor modes.
- `execute tac report`: Added `diagnose debug application filearch lines 10000` (for Standalone and Sensor Modes) and `diagnose debug application ldaprich display lines 10000` (for Standalone and Sensor Modes).
- `execute db restore`: Updated to remove all locally stored files, including detected samples and anomaly PCAP files.

Other improvements

- Improved risk level accuracy on the *Device Profile* page by resolving ambiguity caused by multiple IPs mapping to a single MAC address. Risk is now evaluated based on the selected timeframe and method (*By IP* or *By MAC*). This applies to new detections post-firmware upgrade; existing data remains unchanged.
- Streamlined device filtering by disabling the *Latest Device Enrichment Filter* in both the *Device Log* and *Device Inventory*.
- Resolved an issue preventing addition of the *Bandwidth* widget to dashboards.
- Fixed a query error that occurred during outbreak searches, improving reliability.
- Restored functionality of the *Download* button in the *OT Device* tab of *Device Inventory*.
- Fixed an issue that prevented users from changing to the *Neutrino* theme.
- Corrected the display when *NDR Muting* failed to delete a profile; it now accurately reflects deletion status.
- Improved the filtering in the *Traffic Volume* columns to ensure consistent behavior.
- Fixed a filtering issue for the *Data Source* column in the *Connection* tab on the *Weak Cipher* page.
- Enhanced login experience by ensuring users land on the *NDR Overview Dashboard* after logging in.
- Removed invalid cloud storage types from the *Cloud Storage* page for better clarity and usability.
- Fixed ML discovery detection time column filters to support accurate data sorting and analysis.
- Expanded configuration backup permissions. Now any user with *Configuration* read access can export GUI configuration, and users with read/write access can import it. This no longer limited to *Superadmins*.

System integration and support

The following integration is tested and supported in FortiNDR 7.6.3.

FOS/FortiGate	• FortiNDR Fabric Device widgets including *Detection Statistics* and *System Information* supported in FOS 7.0.5 and 7.2.4 • File submission: FOS 6.4.0 and higher (FOS 6.2 and 5.6 file submission with OFTP, via the FortiSandbox field, is tested and compatible) • FortiGate inline blocking (with AV profile) is supported in FOS 7.0.1 and higher (via HTTP2). • FortiGate quarantine via webhook 6.4.0 and higher.
FortiProxy	• HTTP2 file submission from FortiProxy 7.0.0 and higher • FortiProxy inline blocking (with AV profile) is supported in FPX 7.0.0 and higher. • Quarantining with FortiProxy 7.6.3 and higher.
FortiAnalyzer	• FortiAnalyzer integration is supported in FortiAnalyzer 7.0.1 and higher.
FortiAnalyzer Cloud	• Integration is supported in version 7.6.3 and higher.
FortiSIEM	• Integration is supported in version 6.3.0 and higher.
FortiSandbox	• FortiSandbox integration (API submission from FortiSandbox to FortiNDR) is supported from FortiSandbox version 4.0.1 and higher.
FortiMail	• Version 7.2.0
FortiAuthenticator	• FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are supported.
ICAP	• FortiGate 6.4.0 and higher. • FortiWeb 6.3.11 and higher. • Squid and other compatible ICAP clients. • FortiProxy 7.0.0. • FortiNAC quarantine support (v9.2.2+) • FortiAuthenticator v6.4.5 and higher is supported for 2FA token login with the GUI. Push tokens are not supported at this time. • FortiSwitch quarantine via FortiLink (FortiSwitch v7.0.0+ and FortiGate v7.0.5+)  FortiNDR 7.0.1 and later supports sending both malware and NDR logs to FortiAnalyzer and FortiSIEM or other syslog devices. FortiAnalyzer 7.2.0 supports receiving logs from FortiNDR (log view only). FortiAnalyzer 7.2.1 supports reporting based on logs.

Upgrade information

The latest FortiNDR firmware versions are available for download from FortiCloud. You should always backup your system configuration before upgrading the firmware on your device. Be aware that some configuration settings are not saved to the backup configuration file and will need to be manually restored after upgrade.

Firmware

FortiNDR 7.6.3 supports the following upgrade path:

Upgrade from	Upgrade to
7.4.9, 7.6.2	7.6.3
7.4.8, 7.6.0 (and later)	7.6.2

IMPORTANT: Metadata issue post-upgrade

Some standalone FNDR systems that follow specific upgrade paths may experience database metadata corruption. This issue can cause the GUI to become unresponsive or trigger *Cannot attach table* errors in the diagnose debug database error-log.

Affected configurations:

- **Models**: Any FNDR standalone model
- **Initial firmware**: 7.4.x
- **Upgrade path**: 7.4.x to 7.6.3

Issues observed after upgrade:

- GUI becomes unresponsive
- *diagnose debug database error-log* shows returns the following errors:
  - `Dictionary definition contains unsupported elements`
  - `Cannot attach table`
  - `Waited job failed`

To remediate this issue:

1. Run the following CLI command: `diagnose system db-fix-metadata`
2. If the issue persists, run : `execute db restore`

- Direct upgrade from v7.0.x, v7.1.x or v7.2.x to v7.6.0 is not supported in any platform.
- When upgrading from v7.2.0 - v7.2.3 or v7.4.0 - v7.4.6 to v7.6.0, you will be prompted to update the password upon successful login.

Downgrade from v7.6.x to v7.4.x is not supported as it could cause severe issues such as device lockout and database errors.

FNR-1000F, FNR-3500F (gen3 and above) and FNR-3600G

- 7.6.0 firmware is designed to run on VM and hardware appliances such as FNR-1000F, FNR-3600G, FNDR-3500F (center gen3 and above) and is not compatible with older FAI-3500F hardware (gen1/2). For more information, see Supported models on page 24.

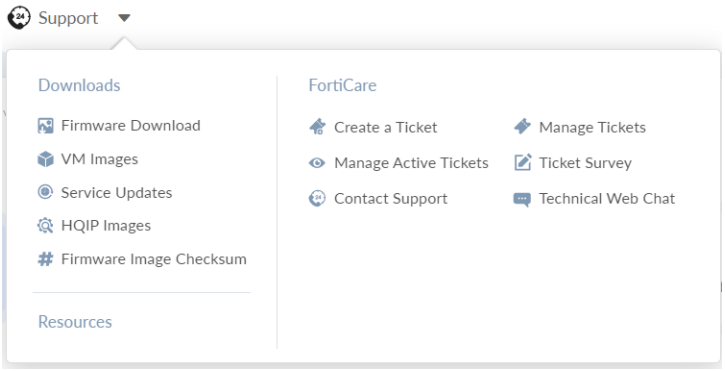
VM Devices

If your current version FortiNDR does not have a password, you will be prompted to create a password after upgrading, otherwise you cannot login.

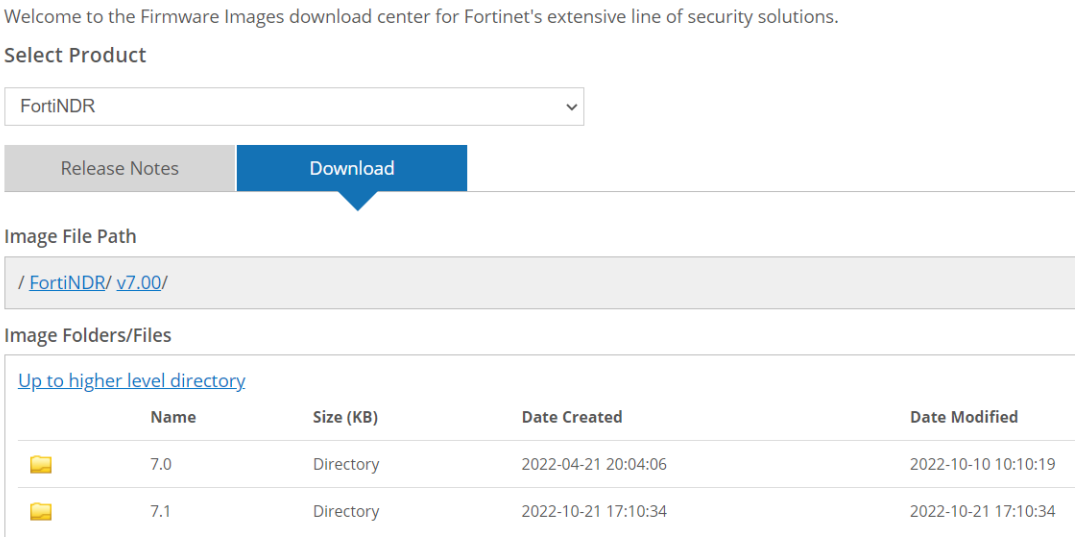
Downloading the latest firmware version

To download the latest version of FortiNDR:

1. Log into FortiCloud.
2. In the banner, click *Support* > *Firmware Download*.



3. From the *Select Product* dropdown, select *FortiNDR*.
4. Click the *Download* tab.
5. Use the folders in the directory to locate and download the latest firmware version.



Upgrading the firmware version

Before you begin:

You should always backup your system configuration before upgrading the firmware on your device.

Be aware the following settings are not backed up to the configuration file:

- *Network Share*
- *Network Share Quarantine*
- *File size limit*
- *Email Alert Recipients*

Record these settings so you can manually restore them after upgrade.

The *File size limit* can be found by pressing the Tab key in the following CLI:

```
execute file-size-threshold {ICAP|OFTP|inline-blocking|manual-upload|network-share|sniffer} <size_
limit_1-10240MB>
```

```
FortiNDR-VM # exec file-size-threshold ICAP
<Size Limit>            A integer between 1~10240 for size in MB

  --- current value ---
ICAP:  200 MB
```

Please make a note for each file input value.

These settings cannot be recovered after they are removed.

To upgrade the FortiNDR firmware version:

1. Back up the configuration file:
   a. Click the Account menu at the top-right of the page.
   b. Go to *Configuration* > *Backup*. The configuration file is saved to your computer.
2. Upgrade the firmware:
   a. Go to *System* > *Firmware*.
   b. Click *Upload* and navigate to the location of the file you downloaded from FortiCloud.
   c. Click *OK*. After the firmware is upgraded the system reboots.
   d. After the upgrade is complete, the new version of firmware should be ready. In the case where the firmware upgrade does not follow the upgrade path. or there is a VM hosting hardware failure, or a power outage during upgrade, please consider to use following CLI to restore the database.

      ```
      execute db restore
      ```

      This command will format the database and remove all the logs and the following settings: *Device input*, *Network Share*, *Network Share Quarantine*, *File size limit* and *Email Alert Recipients*.
3. Use the configuration settings you recorded earlier to manually restore the settings. For *Device Input*, you just need to re-authorize the device again.

Supported models

FortiNDR version 7.6.3 supports the following models:

Model	Mode	Details
FortiNDR-3600G	Center	
FortiNDR-1000F	Standalone and Sensor	
FNDR-2500G	Standalone and Sensor	
FortiNDR-3500F gen3*	Standalone and Center	Supports FortiNDR central management. For hardware details please visit hardware quick start guide or the following notice.
FortiNDR VM 08	Sensor	Requires Center to manage. Supported for ESXi, KVM, AWS, GCP, Azure and OCI only.
FortiNDR VM 16 & 32	Standalone and Sensor	
FortiNDR on Alibaba (BYOL)	Standalone	
FortiNDR on AWS (BYOL)	Standalone, Sensor and Center	
FortiNDR on Azure (BYOL)	Standalone, Sensor and Center	
FortiNDR on GCP (BYOL)	Standalone, Sensor and Center	
FortiNDR KVM	Standalone and Sensor	
FortiNDR on Nutanix	Standalone, Sensor and Center	Nutanix version AOS 7.3.1
FortiNDR on OCI (BYOL)	Sensor	
FortiNDR Centralized Management VM	Center	Supported on ESXi and KVM only

*Notice about hardware generations

The hardware model is printed on the label on the back of the unit.

- FortiNDR gen3 - P24935-03 supports v7.1.x, v7.2.x, 7.4.x and 7.6.x
- FortiAI gen1 - P24935-01 does not support 7.1.x 7.2.x 7.4.x
- FortiAI gen2 - P24935-02 does not support 7.1.x 7.2.x 7.4.x

To confirm the hardware generation with the CLI:

```
get system status
```

This allows you to check the BIOS version. Gen3 models use BIOS version *00010032* and above. Any version below *00010032*, such as *00010001*, indicates a Gen2 or Gen1 model.

Resolved issues

The following issues have been fixed in version 7.6.3. For inquires about a particular bug, contact Customer Service & Support.

Bug ID	Description
1079077	Resolved an issue in malware logs where FortiNDR incorrectly displayed integrated FortiProxy (HTTP2) traffic as FortiGate.
1137025	Confirmed Endace GUI pivot functionality is working in 7.6.1.
1164553	Resolved an issue where email alerts failed when the service password contained an ampersand (&).
1167932	Improved IOC detection transparency by including TLS Host information for both HTTP and TLS traffic.
1168485	Fixed the filters on the *Device Details* page.
1169283	Resolved an issue on 3600G devices, where the RAID status would change to Degraded if a physical HDD failed or was manually removed.
1169288	Added *Application Layer Protocol* column to the *NDR Anomaly Log*.
1170570	Fixed an issue where the *Sample Processing Rate* was inaccurately displayed in the *Performance Information Widget*.
1187874	Resolved an issue where the GUI was displaying dates in the future.
1196632	Resolved an issue where the Netflow dashboard incorrectly showed the feature as inactive, despite continuous sFlow telemetry being received.
1203113	NDR Sensor or Standalone memory usage occasionally remains high even when system is idle.
1205342	FortiNDR log messages sent to FAZ/FAZ Cloud now include the platform name in the *Version* field.
1208220	Resolved a metadata corruption issue affecting FNDR standalone systems after following a specific upgrade path. To remediate, see *Metadata Issue Post-Upgrade* in Upgrade information on page 20

Known issues

The following issues have been identified in version 7.6.3. For inquires about a particular bug or to report a bug, contact Customer Service & Support.

Bug ID	Description
1211337	IPv6 is not supported in NDR Center and Sensor deployments.
1210637	The time shown under *Zone Time* and *Setting Time Manually* on the *System Setting* page is inaccurate. To view the correct system time currently set for the FNDR, click your username in the top-right corner of the header bar and refer to the time displayed in the dropdown menu.

www.fortinet.com