



NDR Pro (v1.8.4): Product Guide

Published on:
September 24, 2026

Created by:
Vehere

BATTLE-TESTED AI CYBER DEFENSE™

Table of Contents

1. Patch Release 1.8.4..... 3

1. Patch Release 1.8.4

NDR Pro 1.8.4 Release Notes

[New Features & Enhancements](#) [Bug Fixes](#) [Known Issues](#) [Partition Sizing Details](#)

The **Release Note for NDR Pro 1.8.4** outlines key **new features and enhancements**, including **Vision AI, Capture Input Identification, Real-Time Alerting, JFlow, Whitelist**, and other **functionalities**. It also includes a detailed list of **bug fixes** across various system components, ensuring improved performance and user experience.

Discover the full feature list! [Explore](#)

Hardware Specifications

To view the mandatory hardware requirements for the **NDR Pro 1.8.4**, [click here](#):

BIOS Setup

The following BIOS configuration is suggested for all **HP servers** with **AMD** processors for best performance:

- System Utilities -> System Configuration -> BIOS -> Workload Profile -> HPC -> Save & Exit.
- Once the server reboots, check the number of NUMA nodes with the command "**numactl -H**".
- If there are multiple NUMA nodes, further BIOS configuration is required:
 - Workload Profile -> Custom
 - Memory -> NUMA memory domains per socket -> Two memory domain per socket

Note: The above configuration is only for **5GBPS** and **10GBPS** traffic on a Single-Server setup.

Flow Sizing

- Current flow sizing: 3Gbps = 18K flows/sec ~9K session/sec
- 2 flows = 1 session
- Max flow sizing: 5Gbps= 30k flows/sec

Installing on a VM

For the Virtual Machine, the recommended network setup is to use a "Bridged Adapter" and to permit "Promiscuous Mode" in the interface to enable the Virtual Machine to receive raw traffic stream.

To install on a VM, one should set up a bootable pen drive and mount it as a CD-ROM on some Hypervisors as an ISO image. Upon rebooting the Virtual Machine, the VNFS boot menu will be visible. Pressing the **Enter** key will commence the installation using the graphical interface.

Note: The server/system will restart once after the first bootup. The resource recommendation is only for Citrix Hypervisors.

Note: The Virtual Machine supports a maximum network speed of 1 Gbps.

Installing on a Dedicated Hardware:

To install on the 1G/ 5G/ 10G Platform, one needs to burn the ISO image on a DVD or a USB pen drive.

- Rebooting the system using DVD will bring up the VNFS boot menu.
- Pressing the **Enter** key will commence the installation using the graphical interface.

Note: The server/system will restart after the first bootup.

New Features & Enhancements

The **NDR Pro 1.8.4** release includes the following new features & enhancements:

VehereVision AI

NDR now introduces **Vehere Vision AI**, an AI-powered conversational assistant available as part of the **Vehere Vision AI** program. It enables users to quickly access product

knowledge, configuration guidance, operational procedures, troubleshooting information, and other documentation through natural language queries.

Key Highlights

- AI-powered conversational assistant
- Natural language access to product documentation
- Configuration and operational guidance
- Context-aware troubleshooting assistance
- Faster information discovery and improved productivity

[Learn more about Vehere Vision AI →](#)

Real Time Alerting

NDR now introduces **Real-Time Alerting**, enabling users to receive alerts as soon as relevant security events are detected. This provides timely visibility into potential threats, allowing teams to investigate and respond to critical events with minimal delay.

Key Highlights

- Real-time notification of security alerts
- Faster visibility into detected threats
- Timely investigation and response
- Improved security monitoring and situational awareness

[Learn more about Real Time Alerting→](#)



On Demand TLS Decryption

NDR now introduces **On-Demand TLS Decryption**, enabling authorized users to decrypt captured **TLS, HTTPS, and QUIC sessions** using the corresponding private server key or SSLKEYLOGFILE. Decryption is performed after packet capture, allowing analysts to inspect encrypted communications without impacting the packet collection process.

Key Highlights

- On-demand decryption of captured encrypted sessions
- Support for TLS, HTTPS, and QUIC traffic
- Centralized private key and SSLKEYLOGFILE management
- Automatic key-to-session matching for eligible sessions
- Access to decrypted metadata and extracted files within the UI
- Role-Based Access Control (RBAC) for decryption operations
- Audit logging for key management and decryption activities
- Decrypted content remains accessible only through the product UI and cannot be exported

[Learn more about On Demand TLS Decryption →](#)



Key Management

NDR now introduces **Key Management**, providing a centralized interface for authorized users to securely import and manage the private keys and **SSLKEYLOGFILES** required for On-Demand TLS Decryption. Multiple keys can be maintained with associated system information and validity periods, enabling automatic matching of keys with captured encrypted sessions.

Key Highlights

- Centralized management of private keys and SSLKEYLOGFILES
- Support for PEM, DER, PKCS#8, PKCS#12/PFX, and SSLKEYLOGFILE formats
- Configurable key validity periods for controlled decryption
- Automatic matching of imported keys with eligible sessions
- Secure key management through Role-Based Access Control (RBAC)
- View and delete imported key records as required
- Automatic removal of expired or retained keys based on configured policies

[Learn more about Key Management →](#)



NDR now introduces **JFlow support**, extending the existing **Flow Collector** to process JFlow records from supported Juniper devices alongside NetFlow and sFlow. JFlow records are processed as flow-based session metadata and made available in the Data Lake and Vehere UI for monitoring, investigation, and analysis.

Key Highlights

- Support for JFlow records from Juniper devices
- Integration with the existing Flow Collector
- Flow-based visibility without full packet capture
- Traffic analysis by application, protocol, IP address, and port
- Visibility into top hosts, conversations, and autonomous systems
- Geographical traffic distribution and network behavior analysis
- Metadata availability for security analytics and threat detection

[Learn more about JFlow →](#)



NDR now introduces **Capture Input Identification**, enabling users to filter captured network data based on configured **VLAN IDs or MAC addresses**. Users can create, manage, edit, and delete identification filters directly from the configuration interface, providing more targeted visibility into captured traffic.

Key Highlights

- Filter captured data using VLAN ID or MAC address
- Create and manage multiple identification filters
- Edit or delete existing filters as required
- View filter details, creation information, and modification history

- Simplifies targeted traffic analysis and investigation

[Learn more about Capture Input Identification →](#)



NDR now enhances the **Setup & Licensing Management Console (SLMC)** with improved server management, command execution monitoring, log collection, and license management capabilities. These enhancements provide users with better visibility and control over server configuration and command execution activities.

Key Highlights

- **Dark Theme:** SLMC now supports a **dark theme** for the user interface.
- **Server Management:** The **Action** menu provides server management options, including **Edit, Delete, Restart, Fetch Server Details,** and **Download Log.**
- **Command Execution Log:** Users can view command execution progress and output logs and download the corresponding server-related logs as a **password-protected ZIP file.** The logs include command execution status and details that help users review and debug failed scenarios. The **system password** is required to open the ZIP file.
- **License Management:** SLMC now allows users to **install, update, and view licenses** for the selected application server using the **Email, Product Code,** and **License Key.**
- **Run Command Monitoring:** The functionality now displays the execution progress and status for each command. Users can also view the corresponding command output logs, providing visibility into command execution and its result.

[Learn more about SLMC →](#)



Audit Trail

Enhanced Audit Trail with Session Duration (Enhancement)

The audit trail has been enhanced to capture the **total authenticated session duration**. The logout event now records the login timestamp, logout timestamp, and session duration in **HH:MM:SS** format, providing complete visibility into the user session lifecycle for audit, compliance, and forensic analysis.

Enhanced Session Details Interaction (UI Enhancement)

Session details viewing has been enhanced for a more intuitive investigation workflow. After **Details** is selected once, the details panel now updates automatically when switching between sessions, while the selected session remains **highlighted and locked** for clear identification.

The details view also maintains the selected session context instead of collapsing the page, allowing users to easily track which session they are currently investigating.

[Learn more about the Optimal HA →](#)

Whitelist

The **Whitelist** feature has been enhanced with support for **ML EBA** alerts. A new **ML EBA** option is now available alongside the existing MLDNN, MLDNS, and Rule whitelist types.

The ML EBA whitelist supports common matching parameters from MLDNN and MLDNS, along with additional parameters such as **ssl_server_name** and **dst_host**, providing more granular control over ML EBA alert suppression.

This enhancement ensures better overall system performance and scalability.

[Learn more about the Whitelist →](#)

Probe Traffic Reversal Fix

NDR introduces the **Probe Traversal Fix** to improve session direction handling for long-running communications split across multiple sessions due to active timeouts. The enhancement maintains session

context and a common session ID across split sessions, ensuring more consistent session tracking and accurate metadata generation.

It also introduces configurable port definitions to improve endpoint direction handling for environments using non-standard ports, enhancing the reliability of ML-based detections.

[Learn more about the Probe Traffic Reversal Fix →](#)

Rules Configuration

The following rule types are no longer supported and have been removed from the rule creation workflow in the Rules Configuration module:

- **Any**
- **Correlation**

[Learn more about the Rules Configuration →](#)

VAPT Fixes

Addressed several security vulnerabilities identified during VAPT assessments, including improvements to authentication controls, session management, input sanitization, and secure configuration settings to enhance overall platform security and compliance.

Bug Fixes

- **ES-964** Fixed an issue where **manual and scheduled configuration backups** failed in internet-isolated deployments during archive generation. The backup workflow no longer depends on internet connectivity or unnecessary OS package update operations, allowing configuration backup ZIP files to be generated successfully in offline environments.
- **ES-924** Completed the permanent removal of sensitive metadata fields `payload.password` and `payload.password_tried` from all user-accessible views. These fields have been permanently removed from searchable metadata and user-facing interfaces, including Data Grid, reports, exports, and APIs, preventing exposure of captured or attempted credential information.
- **ES-905** Fixed an issue where modifying TAXII threat feed configurations through **Settings → Integrations → Threat Feeds** resulted in an "invalid key passed" error. The configuration can now be updated and saved successfully through the GUI without validation errors.
- **ES-880** Fixed an issue where the syslog forwarding pipeline could stop processing alerts under high alert volumes, causing JSON alert files to accumulate locally instead of being forwarded to the configured SIEM. The forwarding workflow has been enhanced to improve pipeline stability and recovery, ensuring more reliable alert delivery during sustained or burst alert generation.
- **ES-878** Fixed an issue where filtering by multiple alert types in the Reporting Section failed to apply correctly, causing reports to display incomplete or inaccurate results when users selected more than one alert type. The

report filtering logic has been corrected to properly handle multi-selection queries, allowing users to successfully filter and view reports based on multiple selected alert types simultaneously.

- **ES-855** Fixed an issue where GUI-based configuration restoration failed due to oversized backup archives caused by inclusion of large runtime logs. The backup process now excludes non-critical logs and enforces size limits, allowing successful restoration.
- **ES-841** Fixed an issue where ML DNS alerts were triggered by volumetric aggregation of legitimate DNS sessions without supporting malicious indicators, resulting in false positive alerts. The detection logic has been refined to require identifiable suspicious traits (e.g., DGA, tunneling, abnormal payload) alongside volumetric anomalies, ensuring alerts are backed by concrete evidence and reducing alert fatigue.
- **ES-837** Fixed an issue where logs in /tmp and scheduled alert artifacts in /var/lib/backup_restore/ accumulated indefinitely without rotation or cleanup, leading to progressive disk space exhaustion. Retention policies and size-based cleanup have been implemented for both directories, ensuring controlled disk utilization and preventing drive-full conditions.
- **ES-835** Fixed an issue where blacklist IP alerts triggered via X-Forwarded-For displayed only internal private IPs without indicating the specific matching public IP. Alert metadata now explicitly highlights the matching field and IP value, enabling faster investigation and automated blocking actions.
- **ES-923** Improved blacklist alert context by adding threat feed source attribution for IOC matches. The originating threat feed name is now captured as a searchable metadata field, enabling analysts to assess IOC credibility and source reliability directly from alerts.
- **ES-906** Fixed an issue where the Advanced Configuration section was non-functional after upgrade due to missing Alert Throttling parameters in the globalconfig index. The upgrade workflow now automatically updates the required configuration parameters, ensuring full functionality of the Advanced Configuration section.
- **ES-879** Fixed an intermittent issue where PCAP data was missing in the Reconstruction Tab for certain sessions, displaying only JSON files with a "RAW not found" error. The reconstruction workflow has been enhanced to ensure consistent PCAP availability across all traffic sessions.
- **ES-858** Fixed an issue where millions of alerts were being generated across ML, Rule, and IDS engines post-deployment, with throttling mechanisms failing to reduce the volume. The alert generation logic has been optimized to apply effective suppression and baseline alignment, ensuring alert volumes stabilize within expected operational thresholds.
- **ES-920** Enhanced the Export Scheduler with automated retention-based cleanup to prevent root partition inode exhaustion. The scheduler now periodically removes older exported files based on configurable retention policies, ensuring root inode usage remains within operational limits and preventing downstream impact on Elasticsearch services.

Known Issues

Not Applicable

Partition Sizing Details

10 Gbps NDR Pro Solution:

For the **10 Gbps NDR Pro solution**, the minimum storage requirements for different partitions are listed below:

Partitions	Requirement	Storage
EFI Partition	50 GB	For Boot Partition
Root ("/")	500 GB	-
Log ("/var/log")	600 GB	System Files and Log Files Storage
Vehere ("/var/log/vehere")	2.69 TB	Probe and Alert Metadata Storage [~If Raw Storage is enabled, else Allocate 1.4 TB]
Elasticsearch ("/var/lib/elasticsearch")	75 TB	Search Engine Data Storage [~ For 89 days data retention with metadata size @ 800 GB/day] [~ For 1 day data retention with full metadata size @ 2 TB/day]
Raw ("/var/lib/raw")	750 TB	Raw Storage [~ For the minimum of 7 Days raw retention with data rate of 1.25 GB/sec] [~ If Raw Storage is enabled, else Allocate 1.4 TB]

5 Gbps NDR Pro solution:

For the **5Gbps NDR Pro solution**, the minimum storage requirements for different partitions are listed below:

Partitions	Requirement	Storage
EFI Partition	50 GB	For Boot Partition
Root ("/")	500 GB	-
Log ("/var/log")	600 GB	System Files and Log Files Storage
Vehere ("/var/log/vehere")	2.69 TB	Probe and Alert Metadata Storage [~If Raw Storage is enabled, else Allocate 1.4 TB]
Elasticsearch ("/var/lib/elasticsearch")	37 TB	Search Engine Data Storage [~ For 89 days data retention with metadata size @ 396.5 GB/day]

Partitions	Requirement	Storage
		[~ For 1 day data retention with full metadata size @ 1 TB/day]
Raw ("var/lib/raw")	371 TB	Raw Storage [~ For the minimum of 7 Days raw retention with data rate of 640 MB/sec [~If Raw Storage is enabled, else Allocate 1.4 TB}

1Gbps NDR Pro solution:

For the **1Gbps NDR Pro solution**, the minimum storage requirements for different partitions are listed below:

Partitions	Requirement	Storage
EFI Partition	50 GB	For Boot Partition
Root ("/")	500 GB	-
Log ("/var/log")	400 GB	System Files and Log Files Storage
Vehere ("/var/log/vehere")	1 TB	Probe and Alert Metadata Storage [~If Raw Storage is enabled, else Allocate 500 GB]
Elasticsearch ("/var/lib/elasticsearch")	7.5 TB	Search Engine Data Storage [~ For 89 days data retention with metadata size @ 81.2 GB/day [~ For 1 day data retention with full metadata size @ 204 GB/day]
Raw ("var/lib/raw")	74 TB	Raw Storage [~ For the minimum of 7 days raw retention with a data rate of 128 MB/sec [~If Raw Storage is enabled, else Allocate 500 GB}

New Rules:

Not Applicable