NetWitness® Platform

Version 12.5

Release Notes

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

September, 2024

Contents

What's New in 12.5.0.0 Release

The NetWitness 12.5.0.0 Release Notes describe new features, enhancements, security updates, upgrade paths, fixed issues, known issues, end-of-life functionality, build numbers, and self-help resources.

Enhancements

The following sections are a complete list and description of enhancements to specific capabilities:

- Dashboard
- Investigate
- Respond
- Insight
- User and Entity Behavior Analytics
- SASE Capability
- Endpoint
- Policy-based Centralized Content Management (CCM)
- Concentrator, Decoder, Log Collector, and Archiver Services
- Log Integrations
- Context Hub
- Live Cloud Service

To locate the documents that are referred to in this section, see https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246.

The Product Documentation section has links to the documentation for this release.

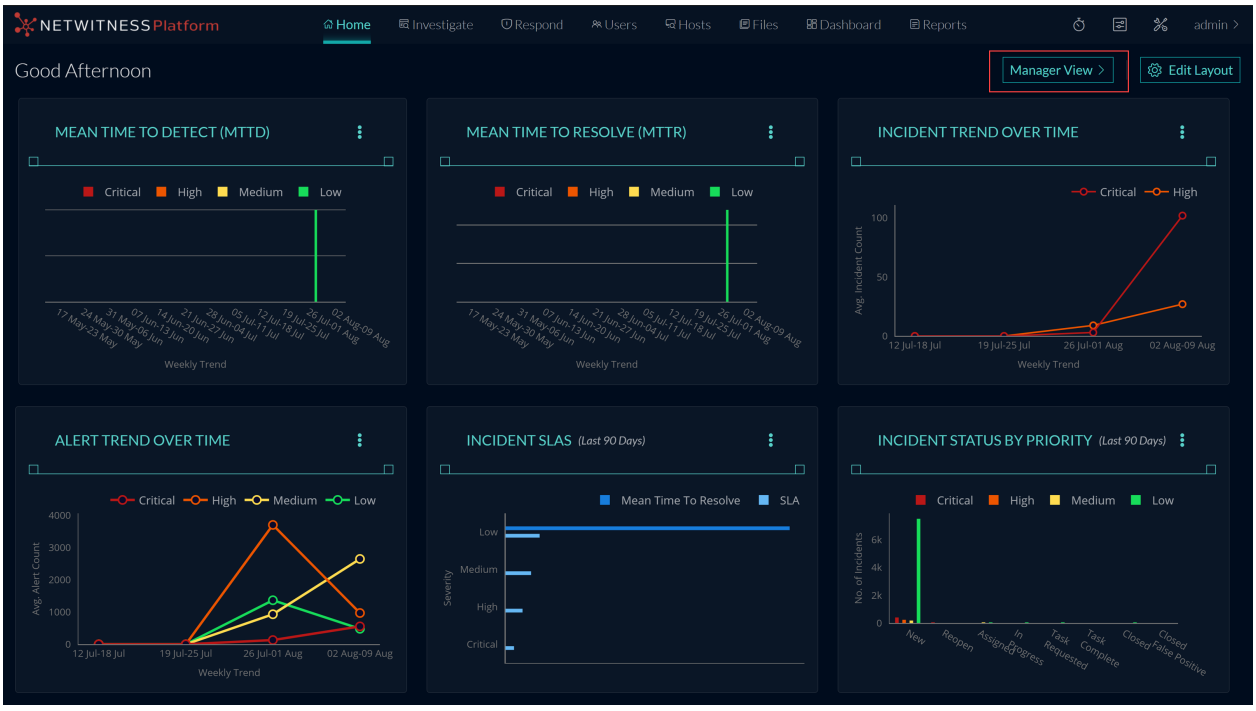
Dashboard

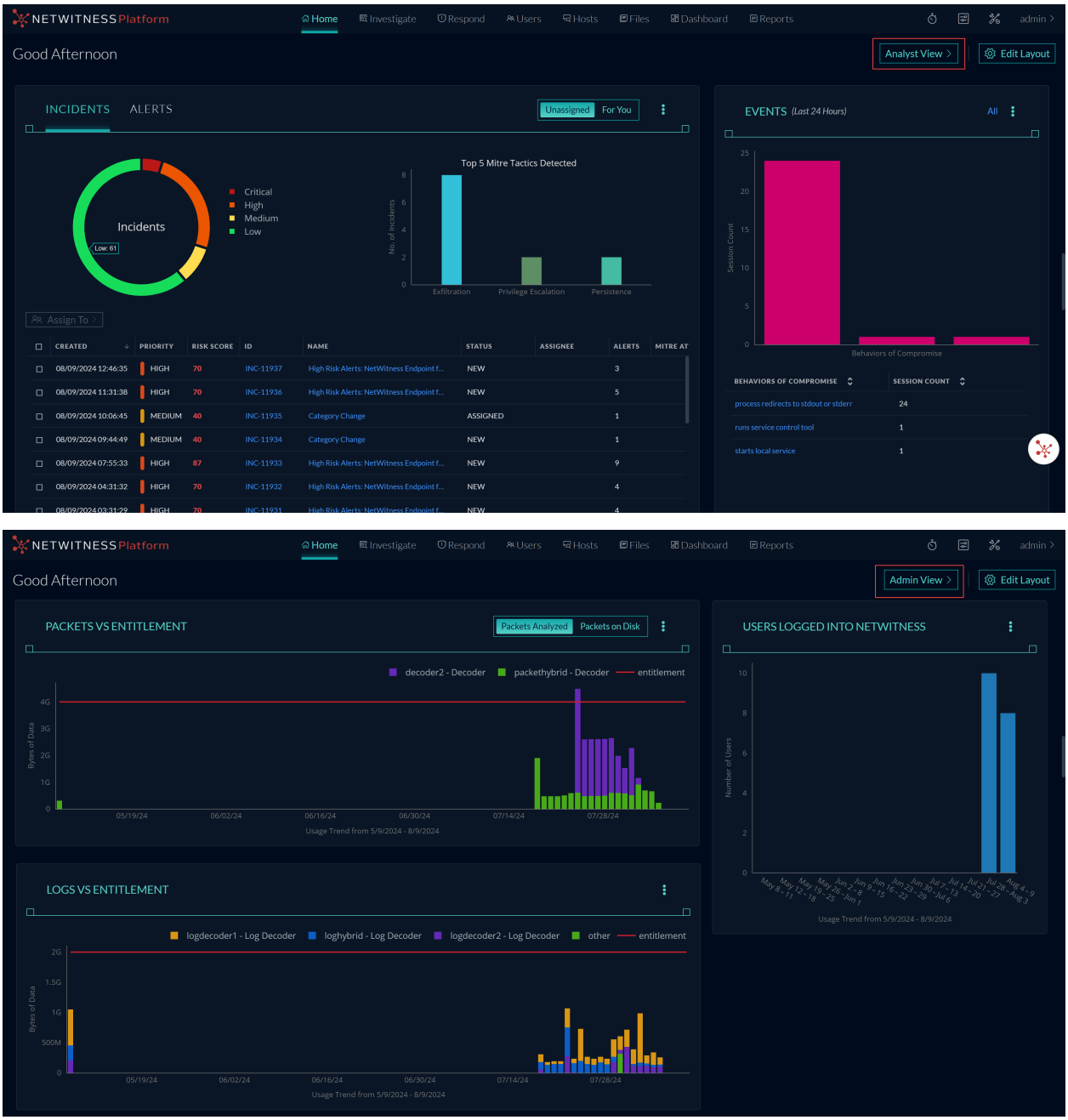
The following section describes the new enhancements for the Dashboard component:

New Home Pages

NetWitness introduces a new **Home** page menu that consists of **Admin**, **Analyst**, and **Manager** views. Each home page is comprised of multiple widgets. Administrators, Analysts, and SOC Managers can access the respective widgets that display certain data in graphical form. The data can be associated with Endpoints, Users, Assets, Content, Incidents, Alerts, MITRE ATT&CK, Retention, and many more.


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
INCIDENTS
9
NEW INCIDENTS
8
CLOSED INCIDENTS
0
ALERTS
40
MEAN TIME TO RESOLVE
0 Sec
MITRE ATT&CK® OVERVIEW
MEDIUM
CONTENT TYPE
EXPAND ALL SUB TECHNIQUES
Deployed
Partially Deployed
Not Deployed
Unavailable
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
5 of 10 techniques
2 of 8 techniques
7 of 10 techniques
7 of 14 techniques
15 of 20 techniques
13 of 14 techniques
25 of 43 techniques
7 of 17 techniques
16 of 32 techniques
3 of 9 techniques
9 of 17 techniques
7 of 17 techniques
6 of 9 techniq


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
MEAN TIME TO DETECT (MTTD)
Critical
High
Medium
Low
Weekly Trend
MEAN TIME TO RESOLVE (MTTR)
Critical
High
Medium
Low
Weekly Trend
INCIDENT TREND OVER TIME
Critical
High
Avg. Incident Count
100
50
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
ALERT TREND OVER TIME
Critical
High
Medium
Low
Avg. Alert Count
4000
3000
2000
1000
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
INCIDENT SLAS (Last 90 Days)
Mean Time To Resolve
SLA
Severity
Low
Medium
High
Critical
INCIDENT STATUS BY PRIORITY (Last 90 Days)
Critical
High
Medium
Low
No. of Incidents
6k
4k
2k
0
New
Reopen
Assigned
In Progress
Task Requested
Task Complete
Closed
Closed False Positive



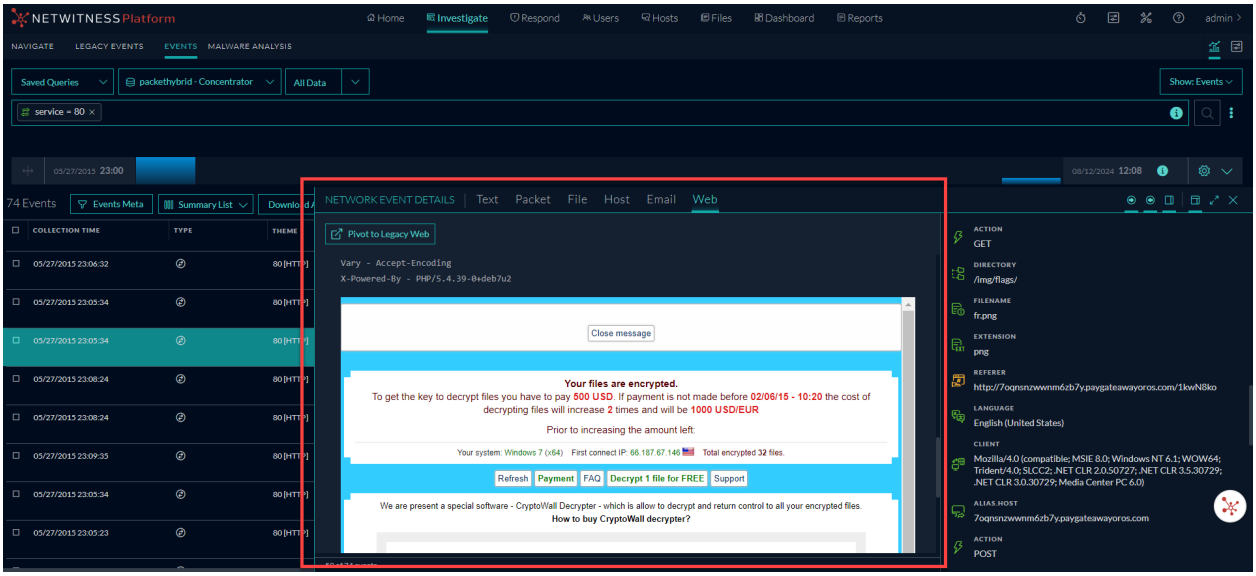
For more information, see **Manage Home Widgets** topic in the NetWitness Getting Started Guide for 12.5.

Investigate

The following section describes the new enhancements for the Investigate component:

Web Reconstruction from Events View

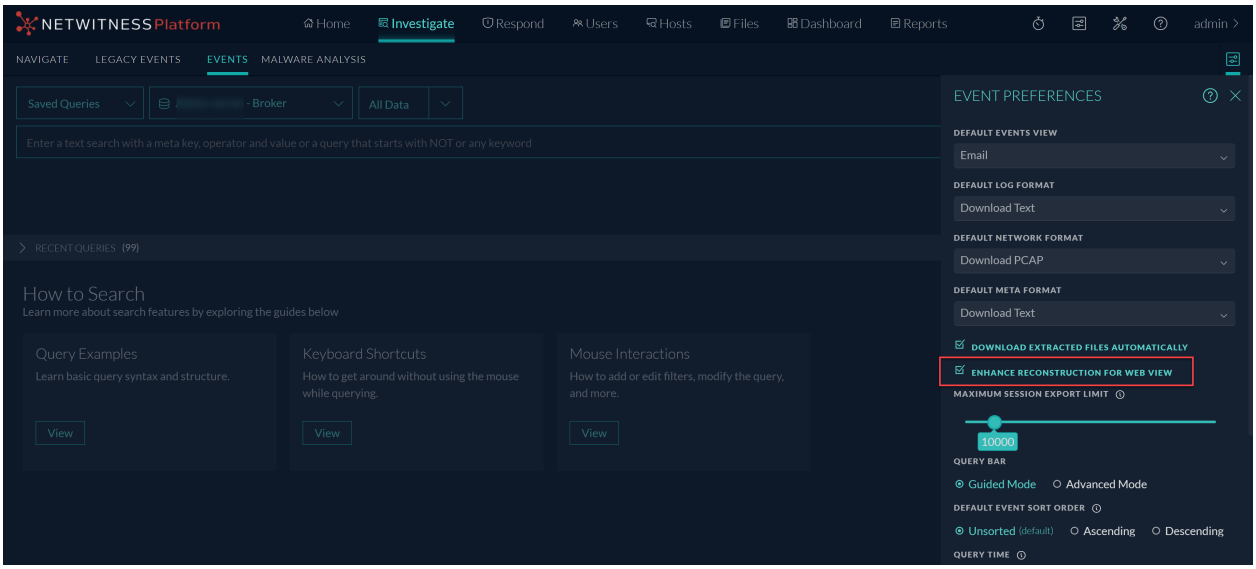
Analysts can safely reconstruct the web view of the target event from the **Events > Web Reconstruction** view if a user has visited web pages related to a particular event. NetWitness can reconstruct the same web page by using the data available in packets, displaying the web page, and relating it to the images and CSS styles as accurately as possible. This web reconstruction process enables analysts to gain valuable insights into the web activity performed, facilitating effective analysis and investigation.



For more information, see the **Web Reconstruction** section of the **Examine Event Details in the Events View** topic in the NetWitness Investigate User Guide for 12.5.

Improved Reconstruction of Events in Web View

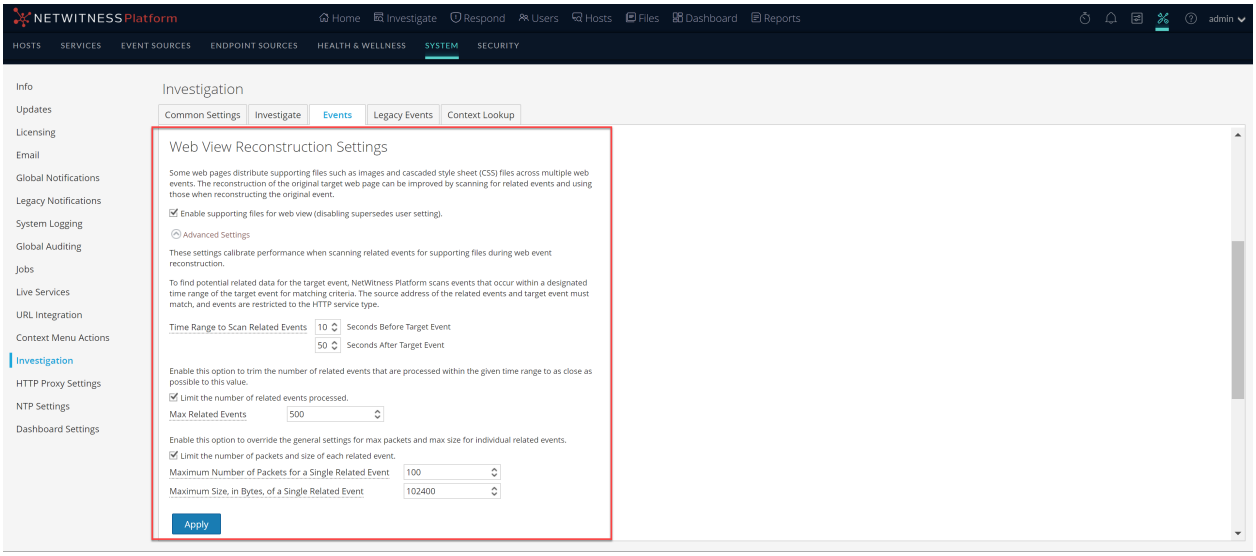
A new user preference, **Enhance Reconstruction for Web View**, has been added to the **Events Preferences** panel in the **Investigate** > **Events** view. This preference is enabled by default for all users. This option improves the reconstruction of websites that reconstruct an event by using CSS, images, and links to format the view in an effective way, thus allowing analysts to better understand the context and details of the events they are reconstructing. This enhancement allows analysts to conduct a more informed and accurate analysis and take appropriate actions.



For more information, see the **Set User Preferences for the Events View** topic in the *NetWitness Investigate User Guide*.

Introducing Web View Reconstruction Settings from System View

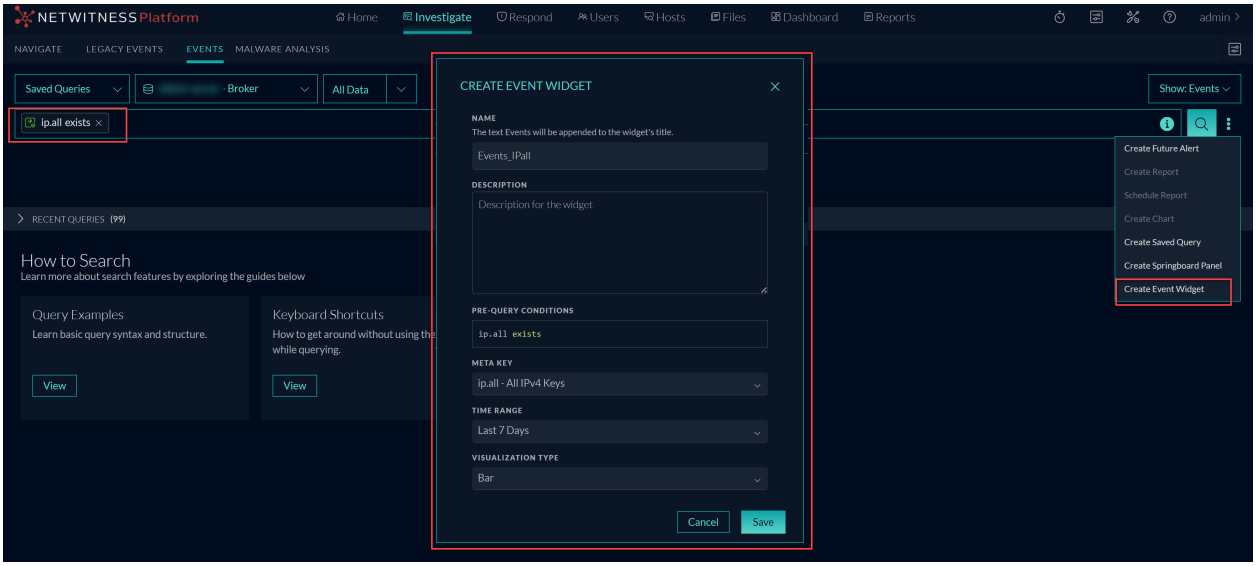
NetWitness introduces the new **Web View Reconstruction Settings** from the **(Admin)** > **System** > **Investigation** view. This setting from the **Events** tab allows administrators to enhances the reconstruction of web views by scanning and reconstructing related events with the same supporting files. When reconstructing a web view spanning multiple events, the system can improve the target event's reconstruction by including related events that contain relevant images and CSS files. Only HTTP service-type events with the same source address as the target event and a timestamp within a specified time range before and after the target event will be scanned. Administrators can also configure the maximum number of related events to scan, providing greater flexibility and precision in web view reconstruction. The Advanced Settings option displays all configurable settings in this section.



For more information, see the **Web View Reconstruction Settings** section of the **Investigation Configuration Panel** topic in the *System Configuration Guide*.

Create Custom Events Widget from Query

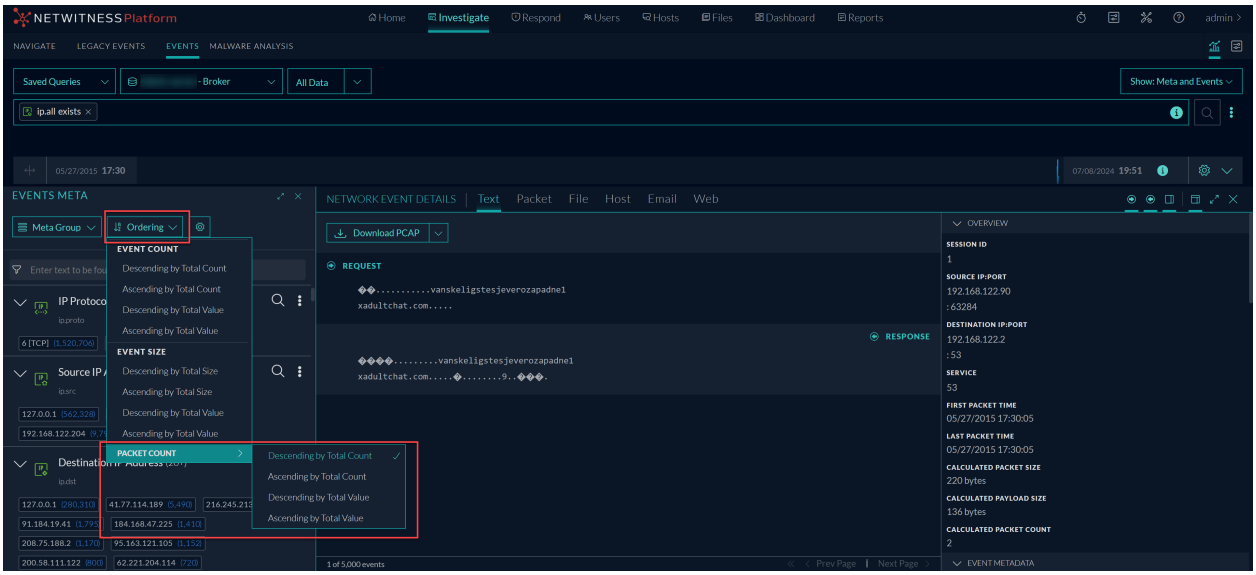
During the investigation, administrators and analysts can now create an Event widget from the **Investigate** > **Events** view. Users can add any number of filters to the query search bar and convert these searches into Event widgets for improved detection and monitoring. The newly created widget will be saved for quick access under the Home page library. Users can then add the Event widget to the Dashboard Layout view (**Admin**, **Analyst**, or **Manager**) under the Home page and customize its configuration to suit their needs. This feature enhances the monitoring and analysis of events, allowing users to track and watch relevant and important events in real time.



For more information, see the **Create Events Widget from Investigate View** topic in the NetWitness Investigate User Guide for 12.5.

Sort Meta Key Results by Packet Count

Analysts can now sort the results of each meta key by the number of packets in the session on the **Investigate** > **Events** page. You can sort the results by Value or Total and in ascending or descending order. By sorting the meta key results by packet count, you can easily find the most or least frequent meta values that occurred in the user environment and can be used for further investigation or analysis.



For more information, see the **Set the Ordering Method for Meta Values** section of the **Drill into Metadata in the Events View** topic in the NetWitness Investigate User Guide for 12.5.

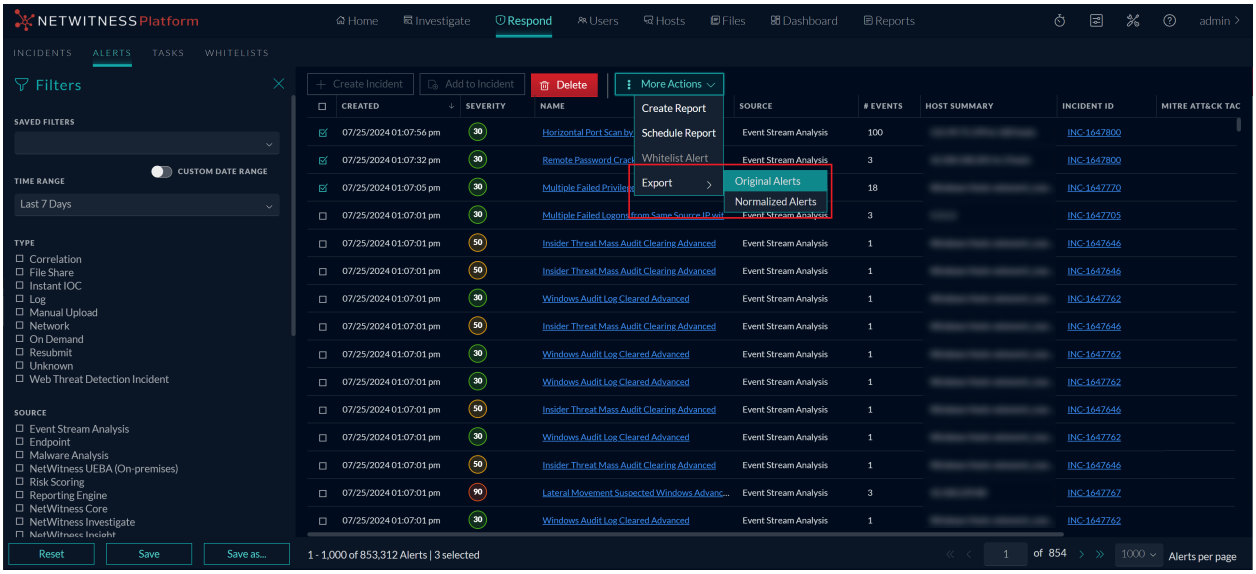
Respond

The following section describes the new enhancements for the Respond component:

Alerts View Enhancement

The **Export** option in **Respond** > **Alerts** > Select an alert > **More Actions** allows you to export and download the original and normalized alerts along with the events in JSON format. NetWitness Platform allows you to export up to **1000** alerts at a time for offline investigation.

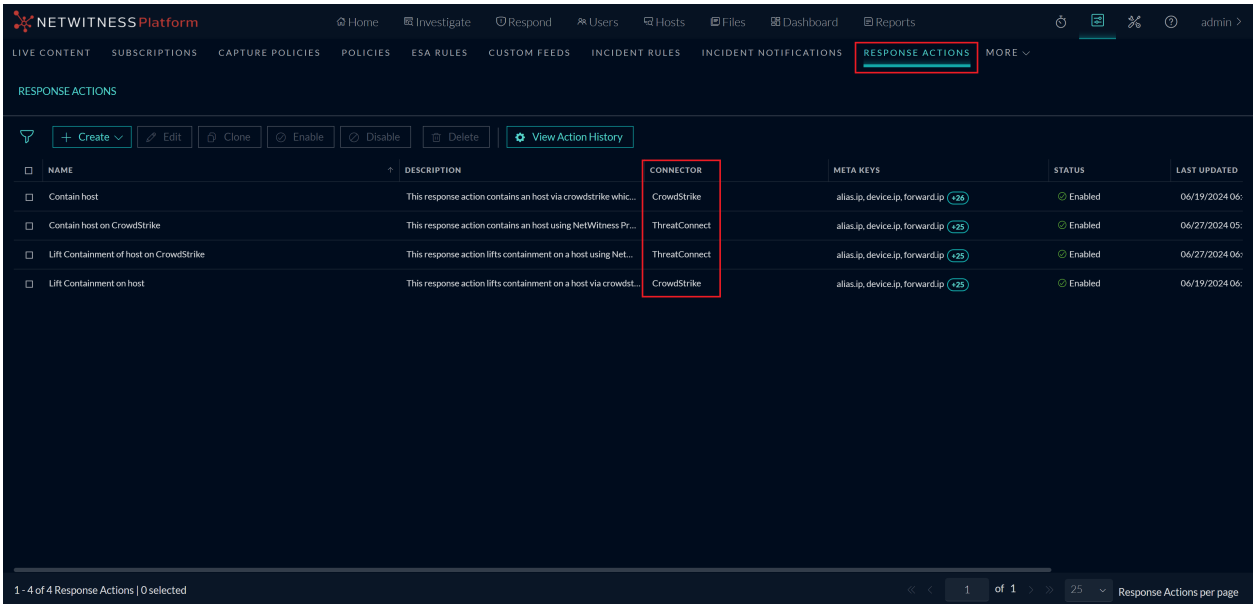
For more information, see **Export Alerts Data** in *NetWitness Respond User Guide for 12.5*.



OOTB Response Actions

Introduction of Out of the Box (OOTB) actions as part of the Response Actions Service. The OOTB actions "Contain Host" and "Lift Containment on Host" are enabled for CrowdStrike and CrowdStrike integrated through NetWitness Orchestrator. This enhancement allows analysts to manually execute response actions after reviewing an incident or automatically as part of a triggered incident. The Response Actions with CrowdStrike are available directly or through NetWitness Orchestrator.

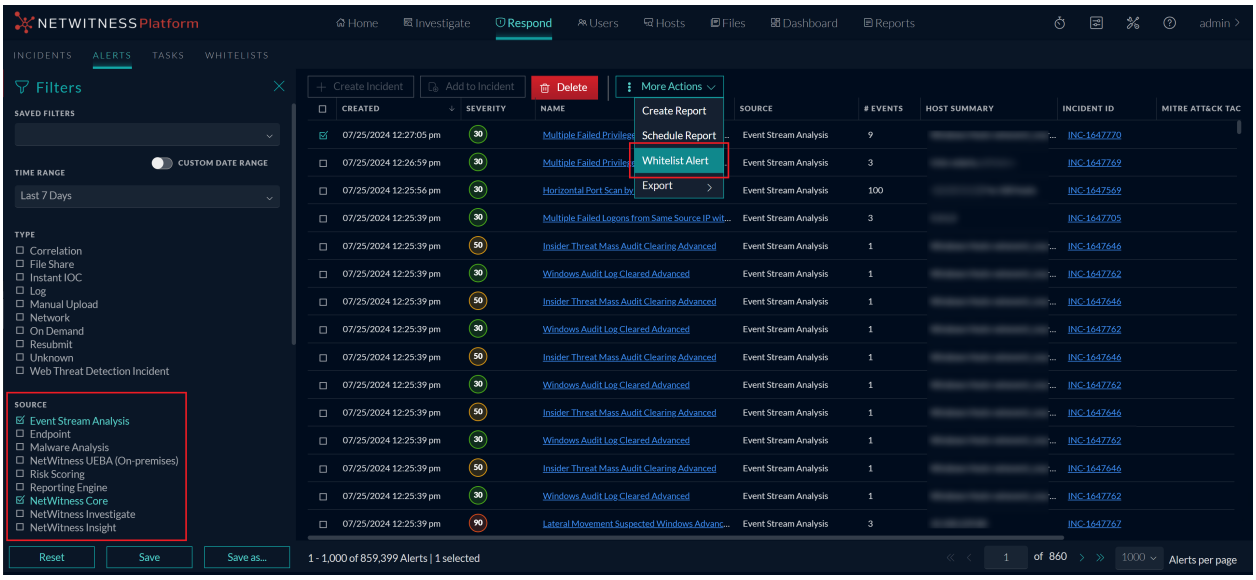
For more information, see **Response Actions** in *NetWitness Response Actions Configuration Guide for 12.5*.



Whitelist Enhancement

The Whitelist feature has been enhanced to include alerts for Event Stream Analysis and NetWitness Core services. You can now whitelist unwanted and recurring non-suspicious alerts for these services. This allows you to select specific entities and set whitelist conditions to prevent unwanted alerts for those entities.

For more information, see **Whitelists List View** in *NetWitness Respond User Guide for 12.5*.

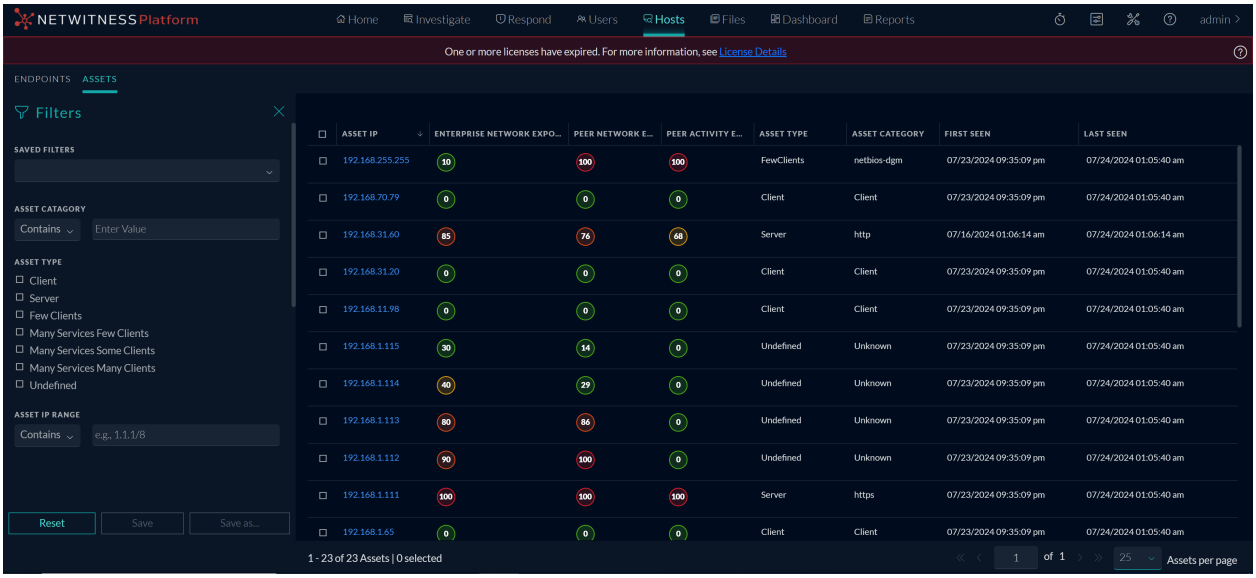


Insight

The following section describes the new enhancements for the Insight component:

New Assets View for Network Assets Detection and Investigation

NetWitness introduces a new Assets view within the **Hosts > Assets** menu. This view provides a centralized location where all the Network assets are detected within your environment along with their associated details, such as the asset IP, asset type, asset category, enterprise network exposure, peer network exposure, peer activity exposure, first seen, and last seen. You can use filters to narrow down the assets by different criteria. This view helps analysts to easily identify and prioritize assets behaving abnormally or unfamiliar assets, enabling them to take immediate action to mitigate any potential security risks.

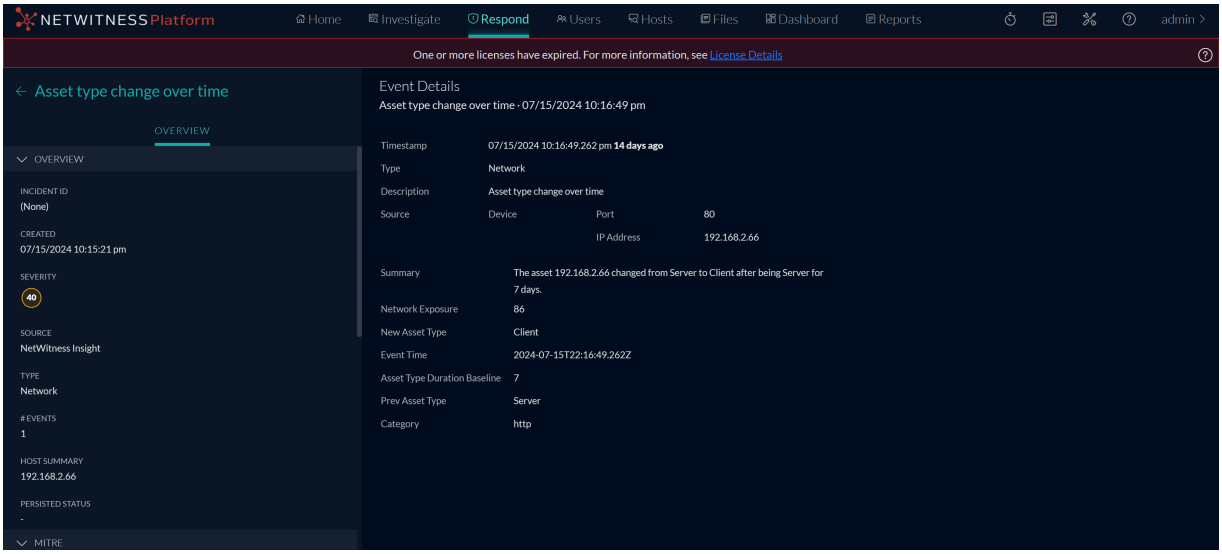


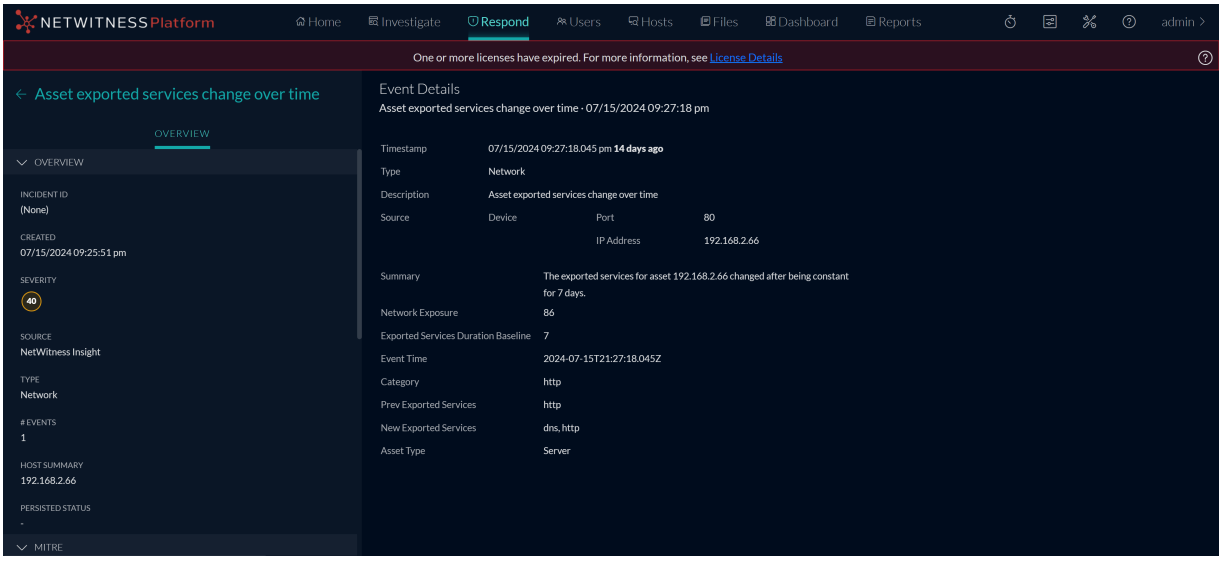
New Insight Alerts for Network Assets

NetWitness introduces two new Insight alerts to help you monitor and respond to changes in your network assets. These alerts are available in the **Respond** > **Alerts** view and are based on the asset type and the exported services of each asset.

- **Asset type change over time**: This alert is generated when there is a change in an asset's type (for example, client to server) after the same type was observed for 7 consecutive days.
- **Asset exported services change over time**: This alert is generated if there is a change in the number of services exported by an asset after the same number of services was observed for 7 consecutive days, even if the asset category remains unchanged.

  These alerts help analysts to identify and investigate any potential anomalies or threats in their environment.





For more information, see the **NetWitness Insight** section in the *NetWitness Documentation Portal*.

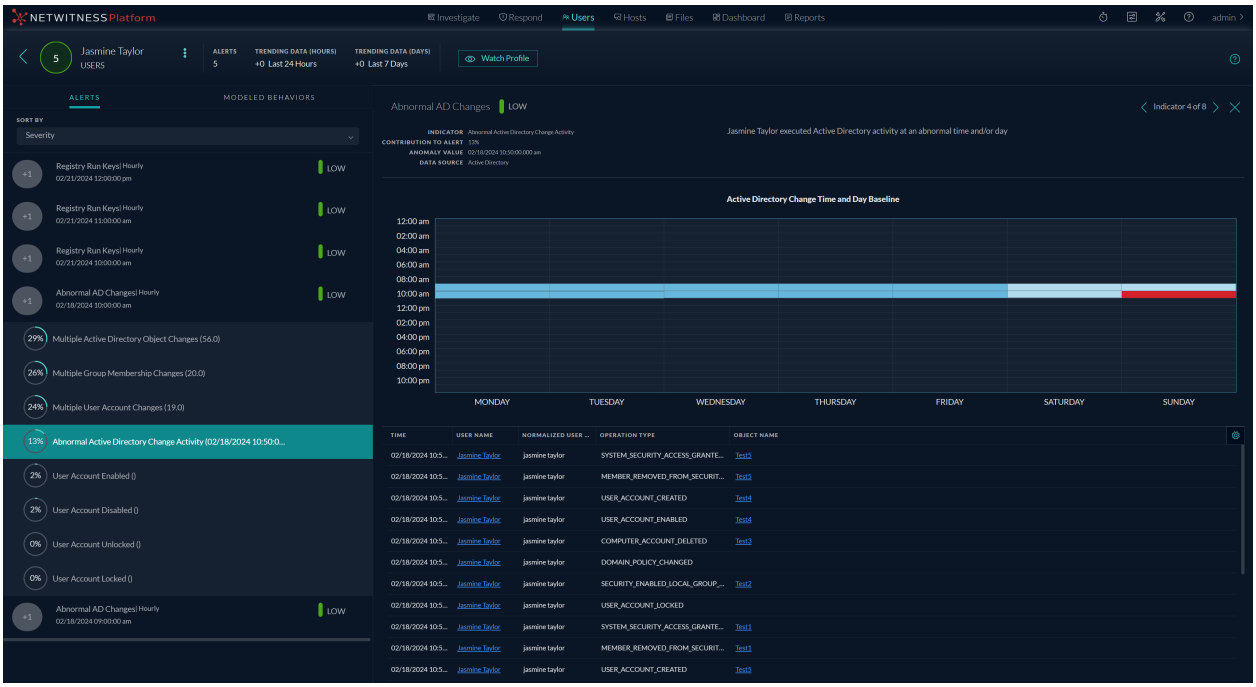
User and Entity Behavior Analytics

The following section describes the new enhancements for UEBA component:

UEBA Anomaly Detection using Day of the Week

NetWitness UEBA enhances its anomaly detection capabilities by introducing the Day of the Week feature. This feature enables the detection of non-standard access patterns that may indicate a compromised account or an insider threat. When a monitored user or a network entity activity on a particular day of the week differs from its usual baseline, UEBA flags it as an anomaly, generates a Non-Standard Access or Non-Standard Activity alert, and notifies the analysts for further investigation and verification. For further information on the monitored activities tracked for Non-Standard Access and Non-Standard Activity, please see the topic **Alert Types** in the *NetWitness UEBA User Guide*.

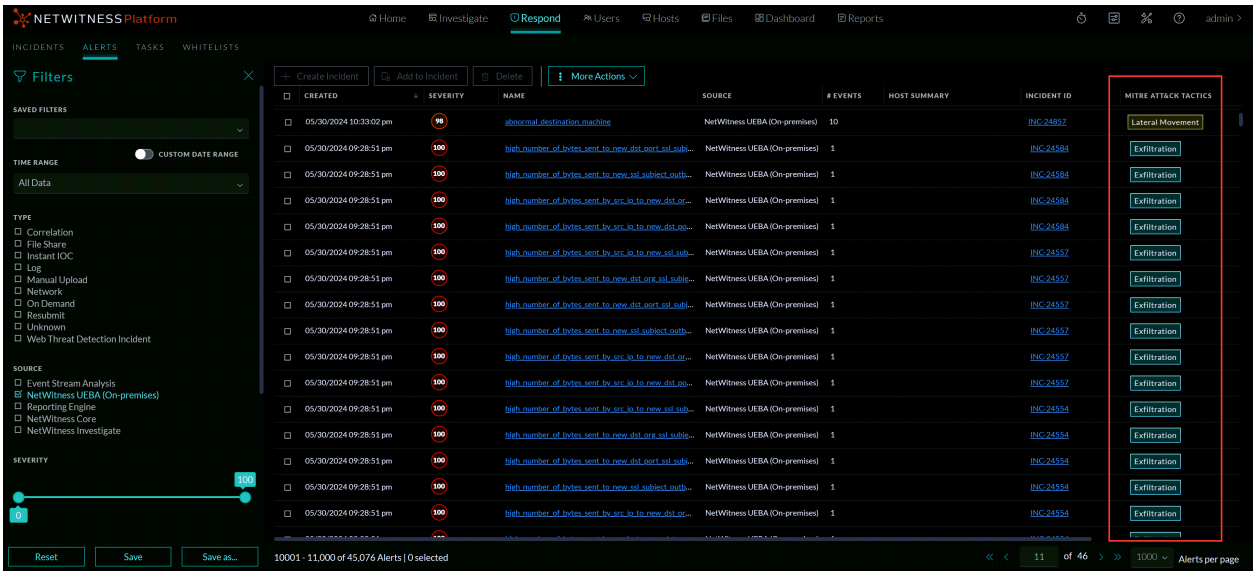
For example, the user accessed the Active Directory on an abnormal day. The user typically works from Monday to Friday, but they logged in on a Sunday and made active directory changes. This behavior was detected as an anomaly by NetWitness UEBA based on the day of the week enhancement, which indicates that this is an unusual day for this user to make changes in AD, generating an alert for the analysts to investigate.



MITRE ATT&CK Mapping for UEBA

NetWitness now integrates MITRE ATT&CK framework mapping for UEBA alerts and incidents. This mapping helps analysts understand the attacker's potential tactics, techniques, and sub-techniques behind detected activities by correlating them with known behaviors. When investigating UEBA alerts and incidents, analysts can see a list of mapped tactics and techniques from the **Respond** view, along with a dedicated **ATT&CK Explorer** panel that provides further context and related information, which eliminates the need to visit MITRE's website for ATT&CK information. This enhancement provides valuable insights into threat severity and nature, enabling faster and more informed response decisions.

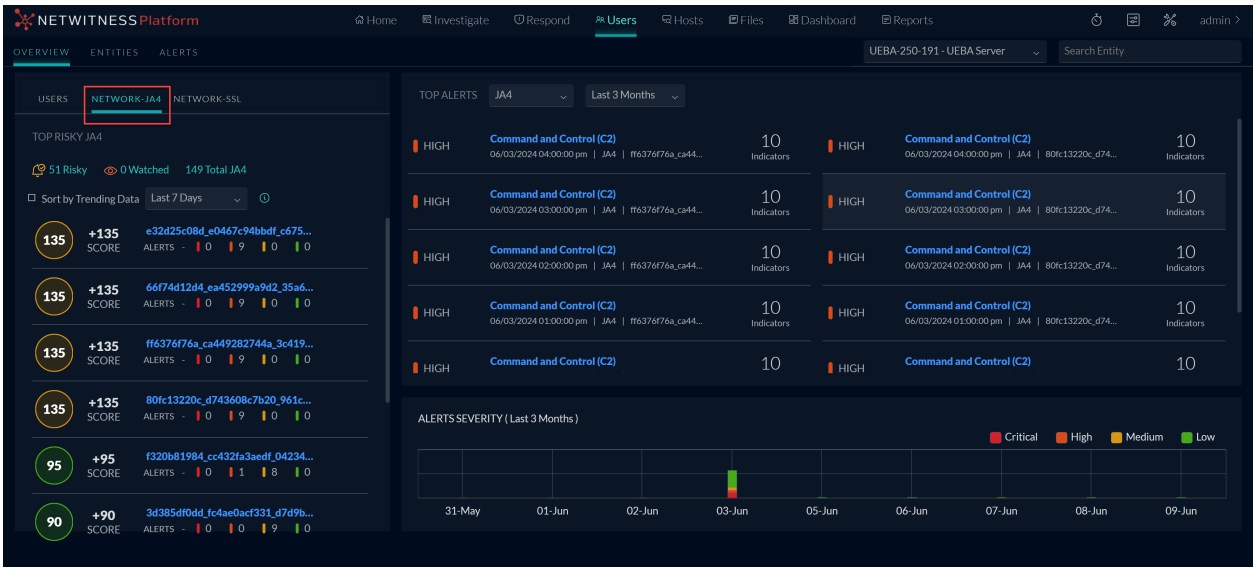
For example, A UEBA alert identified suspicious remote access behavior from a user account. This behavior aligns with the MITRE ATT&CK tactic of **Lateral Movement** and technique using **Remote Services**, alerting analysts to investigate a possible attempt to obtain data and take necessary actions.



For more information on the Mitre ATT&CK framework usage for UEBA, see the topic **Use MITRE ATT&CK® Framework** in the NetWitness Respond Guide 12.5.

Added JA4 Support in UEBA for Improved Client Identification and Threat Detection

NetWitness has added support for the JA4 fingerprint and is the default for UEBA from the 12.5 version or later. This change is implemented because JA4 is identified as the most reliable and improved client identification method. JA4 leverages TLS Client Hello packets to identify application-specific traffic patterns and create unique fingerprints for each application. This reduces the total number of unique fingerprints for modern browsers. As a result, a single client will have only one JA4 fingerprint instead of multiple ones, making it easier to track and monitor. This improvement in UEBA with JA4 helps to identify the fingerprints of malicious applications and enables analysts to proactively identify and mitigate threats hidden within encrypted traffic.

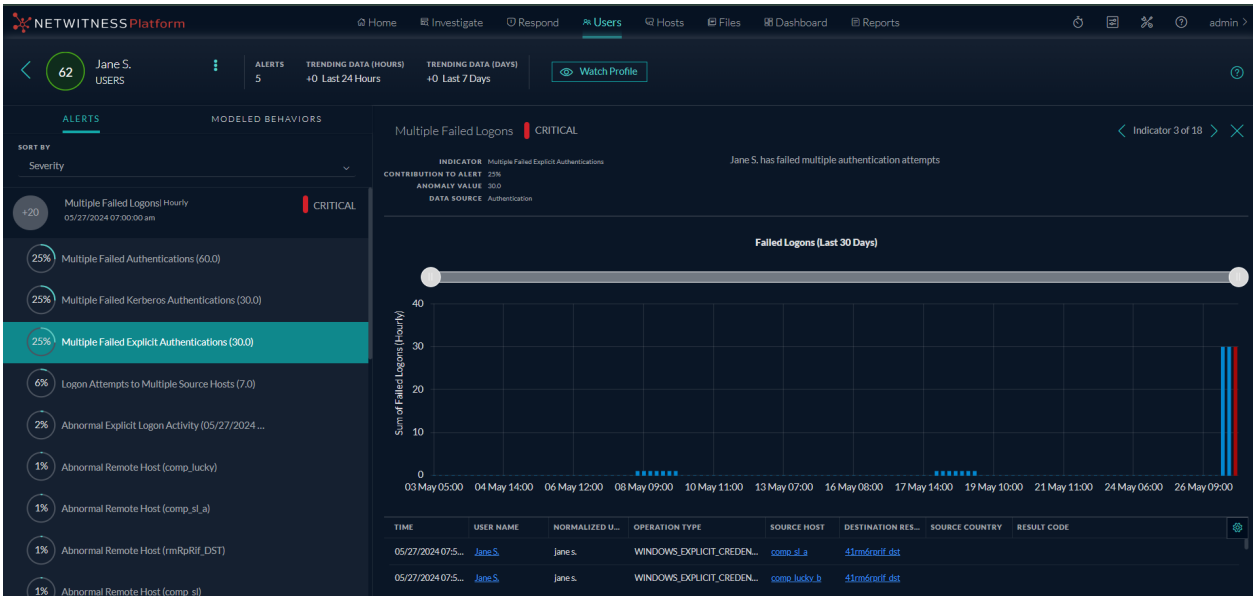


For more information on JA4 support, see NetWitness UEBA User Guide for 12.5.

Enhanced UEBA for Detection of Kerberos and Explicit Logon Activity

NetWitness UEBA has enhanced its detection capabilities for logon activities by introducing two new indicators and modeled behaviors specifically for **Kerberos** and **Explicit** Logons. This enhancement allows for more precise differentiation between various logon events within your environment, significantly reducing false positives and inconsistencies related to Kerberos and Explicit logon activities. By separating these logon types, analysts can more effectively identify abnormal logon behaviors and protect their environment from possible threats. These new indicators provide deeper insights into logon activities, helping analysts effectively monitor and investigate any suspicious or malicious behavior.

For example, A **Multiple Failed Logons** alert can be triggered when anomalous activity is identified for multiple failed authentication attempts in both **Kerberos** and **Explicit Logon** activity.



For more information, see the **Logon Activity Indicators** section of the **NetWitness UEBA Use Cases** topic in the NetWitness UEBA User Guide for 12.5.

SASE Capability

The following section describes the new enhancement for SASE:

NetWitness SASE Integration with Netskope (Private Preview Mode)

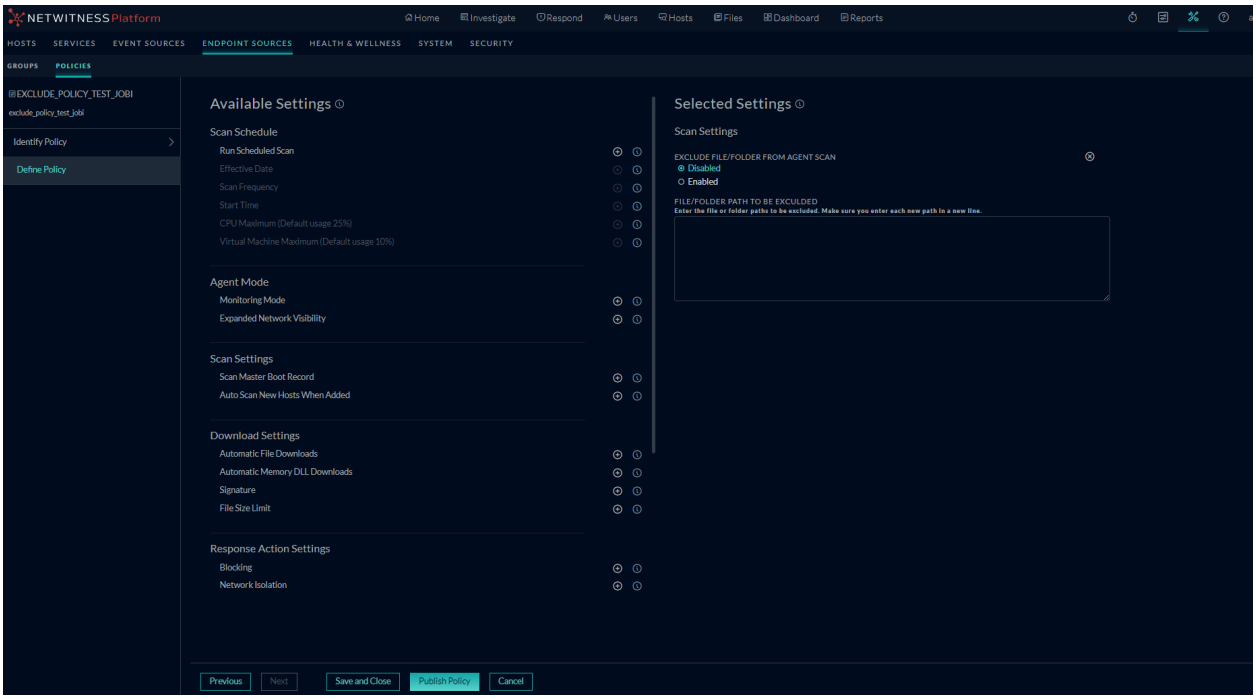
Introduces NetWitness integration with Netskope SASE to provide complete network and logs visibility. With this custom technical integration, NetWitness users gain insight into behavior and communication among devices and services in remote and distributed networks across on-premises, hybrid, and cloud deployments. The NetWitness-Netskope SASE integration enables customers to leverage SASE flexibility and its inherent security advantages while retaining complete visibility for threat detection and response. In 12.5 release, NetWitness SASE integration with Netskope is in Private Preview Mode.

Endpoint

The following section describes the new enhancements for Endpoint component

Exclusion of Specific Files and Folders from Agent Full System Scans

You can configure the NetWitness Platform to exclude specific files and folders from NetWitness Endpoint Agent full system scans. When you exclude files or folders, the NetWitness Endpoint Agent ignores them when it scans for security risks. If you exclude files and folders with large sizes, you might find that Endpoint Agent scan time is reduced. Excluding a file or folder from the NetWitness Endpoint Agent scans reduces the protection level of hosts on your network. It should be used only if you have a specific need and are confident the items are not infected. You can exclude files and folders only from a Full System Scan.



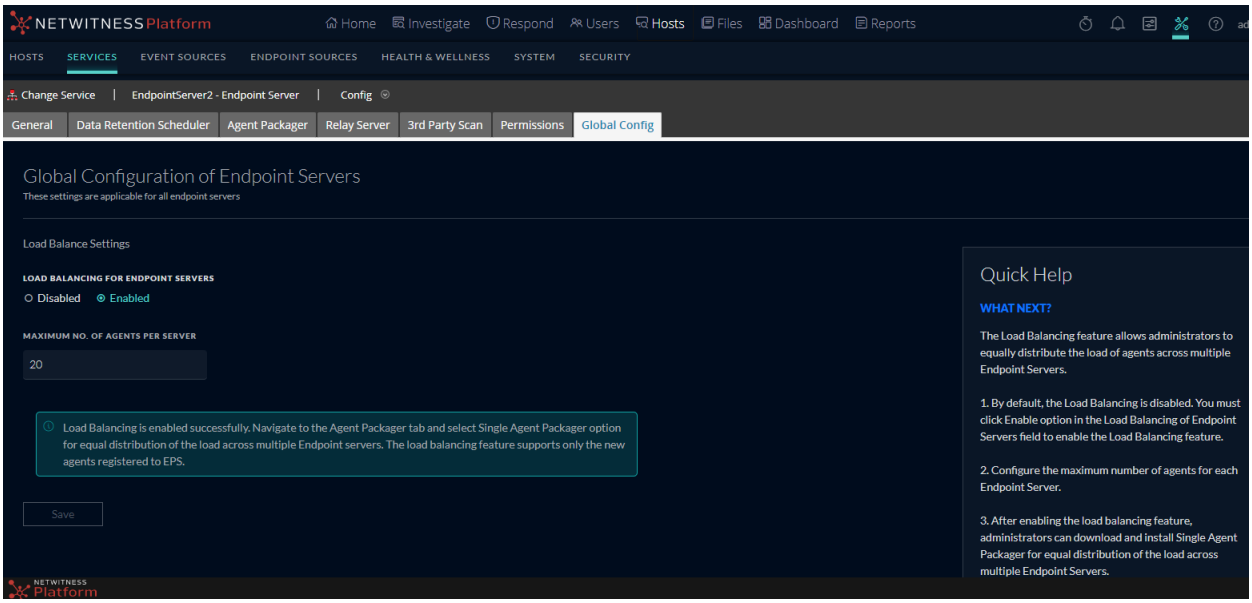
For more information on how to exclude files and folders from NetWitness Agent Full System Scan, see NetWitness Endpoint Configuration Guide.

Optimizing Performance: Load Balancing Capabilities in Endpoint Servers

The newly introduced load balancing feature enables administrators to distribute agents' loads equally across the endpoint servers in the environment.

When organizations become larger, the need to add new agents for deployments increases, and distributing agents across Endpoint Servers becomes difficult. Administrators must download a different Packager for each endpoint server and use policies to distribute the load based on conditions. Using the load balancing feature, customers only need to download one agent packager and push it to all the endpoint agents. Based on the defined load and parameters, the agents will be equally distributed across Endpoint Servers.

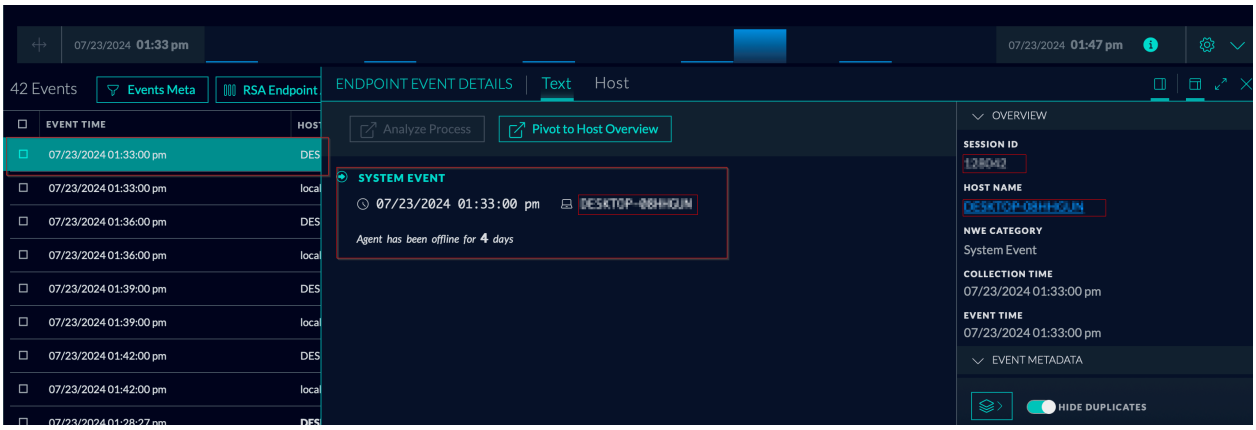
By implementing load balancing, organizations can ensure that their deployment scales efficiently, reducing the risk of overloading any single endpoint server and maintaining optimal performance across the network. To use the load balancing capability, you need to enable load balancing.



For more information on load balancing, see “About Load Balancing” “Enable Load Balancing” topics in the *NetWitness Endpoint User Guide.*

Ability to Monitor Endpoint Agents' Last-seen Details

NetWitness Platform enables administrators and analysts to regularly create reports detailing the number of endpoint agents that haven't reported for a specified number of days, ensuring compliance and governance in the organization. Understanding when the endpoint agent was last active provides insights into the overall performance of the endpoint devices. Monitoring the endpoint agents’ last-seen status is crucial for ensuring security, compliance, operational efficiency, and effective resource management within an organization.



For more information, see “Monitor Endpoint Agents' Last-seen Details” topic in the NetWitness Endpoint User Guide.

Supported Operating System Enhancements

Administrators have the option to deploy Endpoint agents on the following version of Windows Operating System:

- **Windows 11 (up to version 23H2)**

For more information, see **Introduction to Endpoint Agent Installation** topic in the *NetWitness Endpoint Agent Installation Guide*.

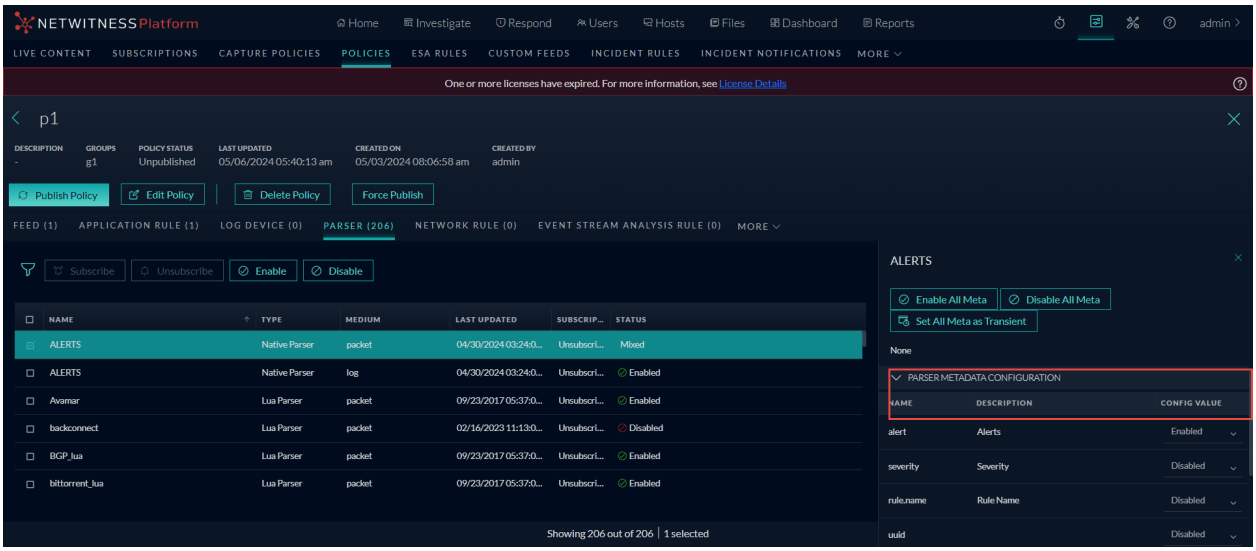
Policy-based Centralized Content Management (CCM)

The following enhancements are made for CCM in 12.5.0.0 version:

Support for Native Parsers

View Parser Metadata Configuration

The **Policy Details** > **Parser** view has been enhanced to view the **Parser Metadata Configuration** on the right hand side panel displaying all the Metas for selected Parser.

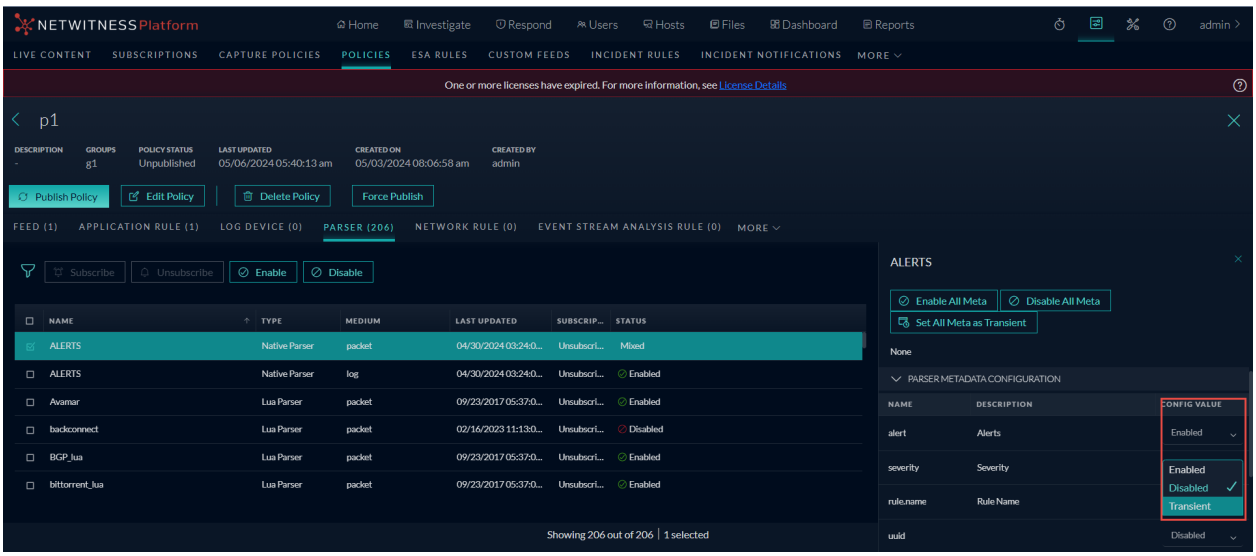


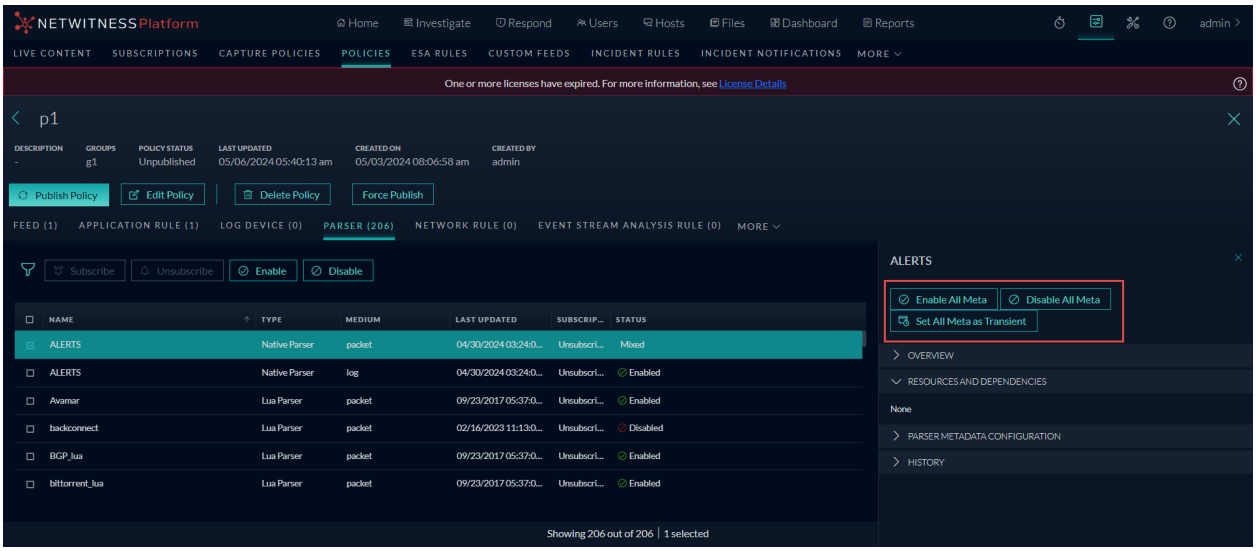
For more information, see **View a Policy** topic in the *Policy-based Centralized Content Management Guide*.

Enable or Disable Parser Meta

The **Policy Details** > **Parser** view has been enhanced to enable or disable specific parser meta giving you the capability to decide whether to user native parsers or not. You can:

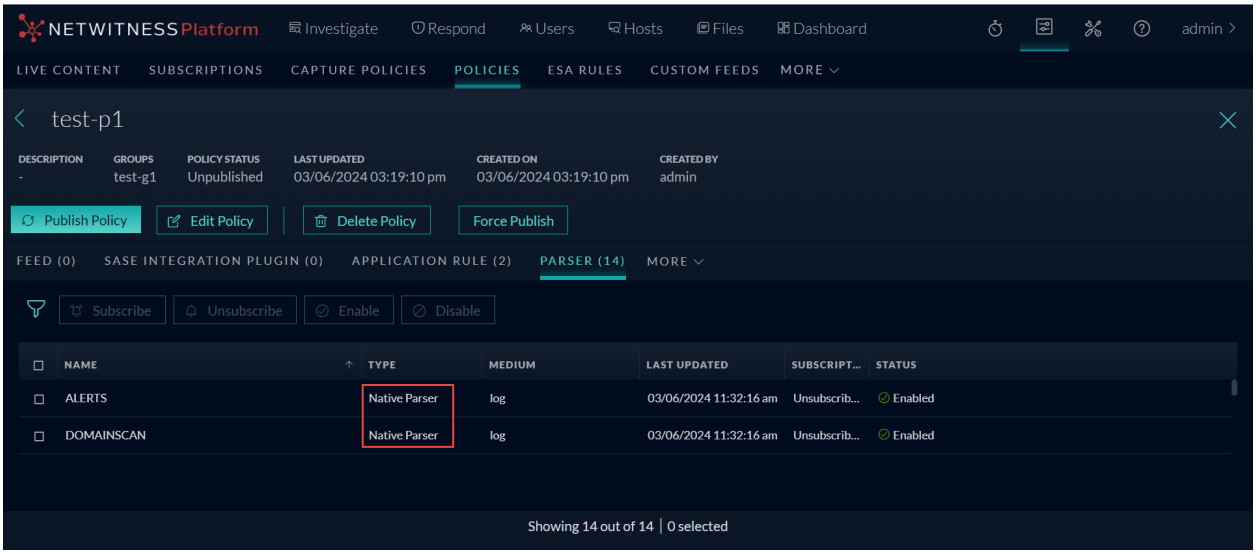
- Enable all meta
- Disable all meta
- Make all meta as transient
- Enable individual meta
- Disable individual meta
- Make individual meta as transient





View Native Parsers Enabled for Services and Attached to Policy

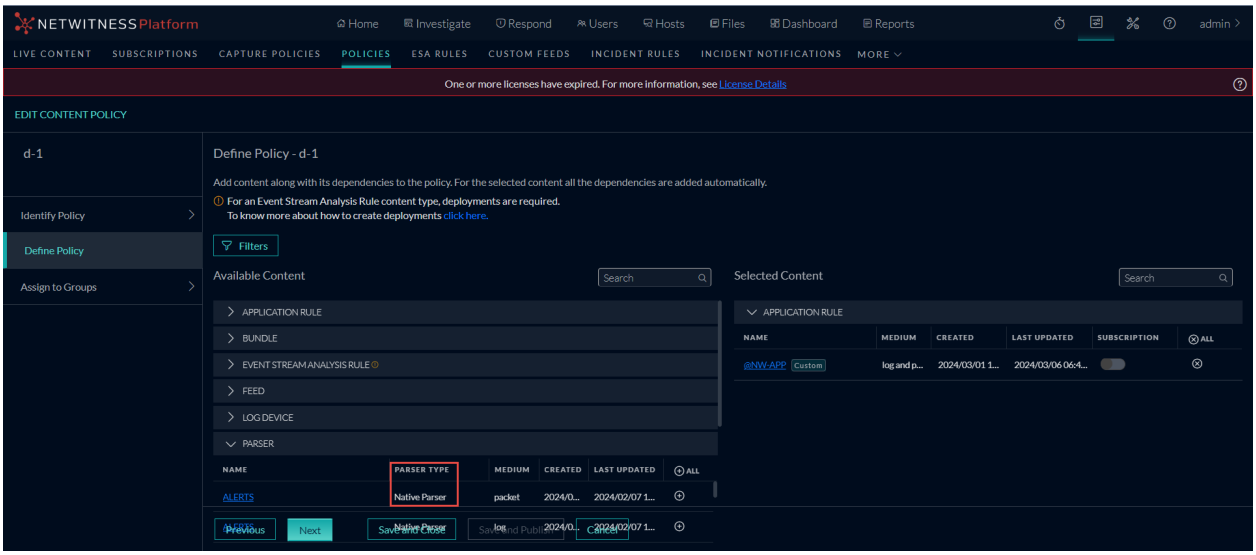
You can easily view the Native Parsers enabled for services and attached to a policy as they are automatically displayed in the **Policy Details** page.



For more information, see **View a Policy** topic in the *Policy-based Centralized Content Management Guide*.

Distinguish between Native Parsers and LUA Parsers while Creating a Policy

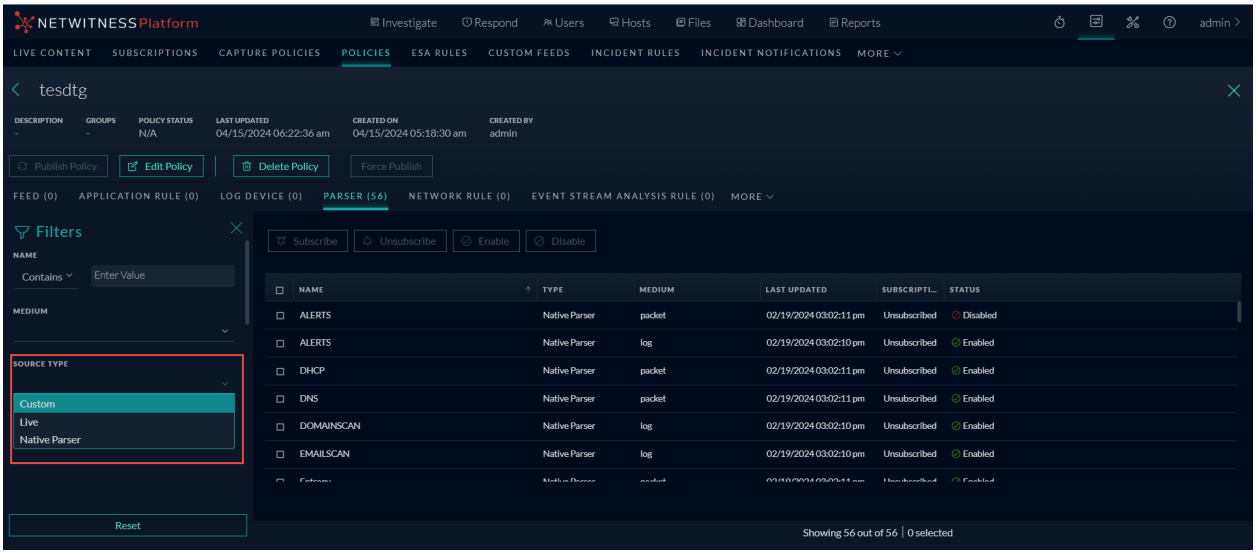
A distinguishable identifier is created for native parser in the **Create Policy** or **Edit Policy** page to help you distinguish between native parser and LUA parser while creating a policy.



For more information, see **Create and Publish Policies** topic in the *Policy-based Centralized Content Management Guide*.

Filter Native Parsers

You can filter the native parsers in the **Create Policy**, **Edit Policy** and **Policy Details** page enabling you to easily select or view the native parsers required for the policy. This will streamline the process and enable you to easily add or remove native parsers during policy creation or modification.



For more information, see **Create and Publish Policies** topic in the *Policy-based Centralized Content Management Guide*.

Concentrator, Decoder, Log Collector, and Archiver Services

The following enhancements are made for Concentrator, Decoder, Log Collector, and Archiver Services in 12.5.0.0 version:

Introducing JA4 TLS Fingerprinting

JA4 identifies application-specific traffic patterns by analyzing the TLS handshake negotiations (Client Hello), thus enhancing the UEBA threat detection capabilities.

For more information, see **Support for the JA4 Entity for UEBA** topic in the *Decoder Configuration Guide*.

Logstash Event Sources

Introduced NetWitness JDBC Logstash Input plugin support to collect logs from MSSQL, IBMDB2, and Oracle databases.

For more information, see **Configure Logstash Event Sources in NetWitness** topic in the *Log Collection Guide*.

Extended Meta

An optional configuration to increase the length of values that can be stored in the meta database to provide better accuracy when it comes to certain use cases requiring matches of long strings.

Extended Meta provides a way to selectively configure certain meta keys to support values greater than 256 bytes. With this feature, meta values previously truncated by the 256 bytes limit can now be extended up to 4,096 bytes in length.

For more information, see the Extended Meta Guidelines mentioned in the *NetWitness Extended Meta User Guide for 12.5*.

Application Rule Tracking

Counts how often an application rule is matched as well as the ability to reset the counter for troubleshooting purposes.

For more information, see the *API Guide for 12.5*.

Log Integrations

NetWitness Platform supports the integration of the following event sources to collect and parse logs. Unless specified, these services are supported on NetWitness Platform 12.2.0.0 or later.

- Amazon AWS CloudWatch
- Okta Workforce Identity Cloud

For more information on integrating the parser services, see NetWitness Platform Integrations Guide.

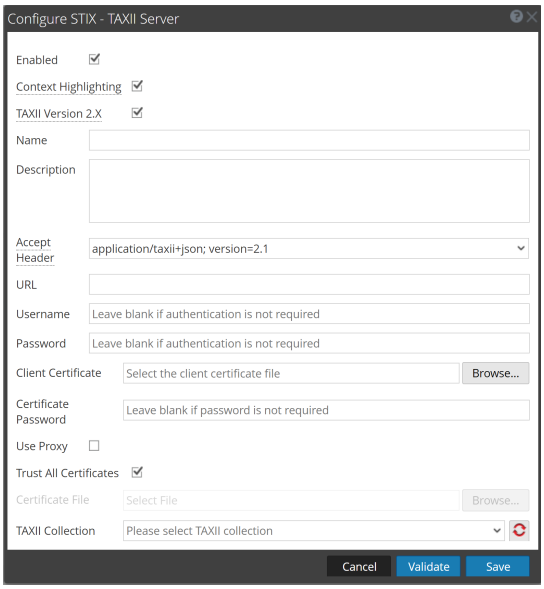
Context Hub

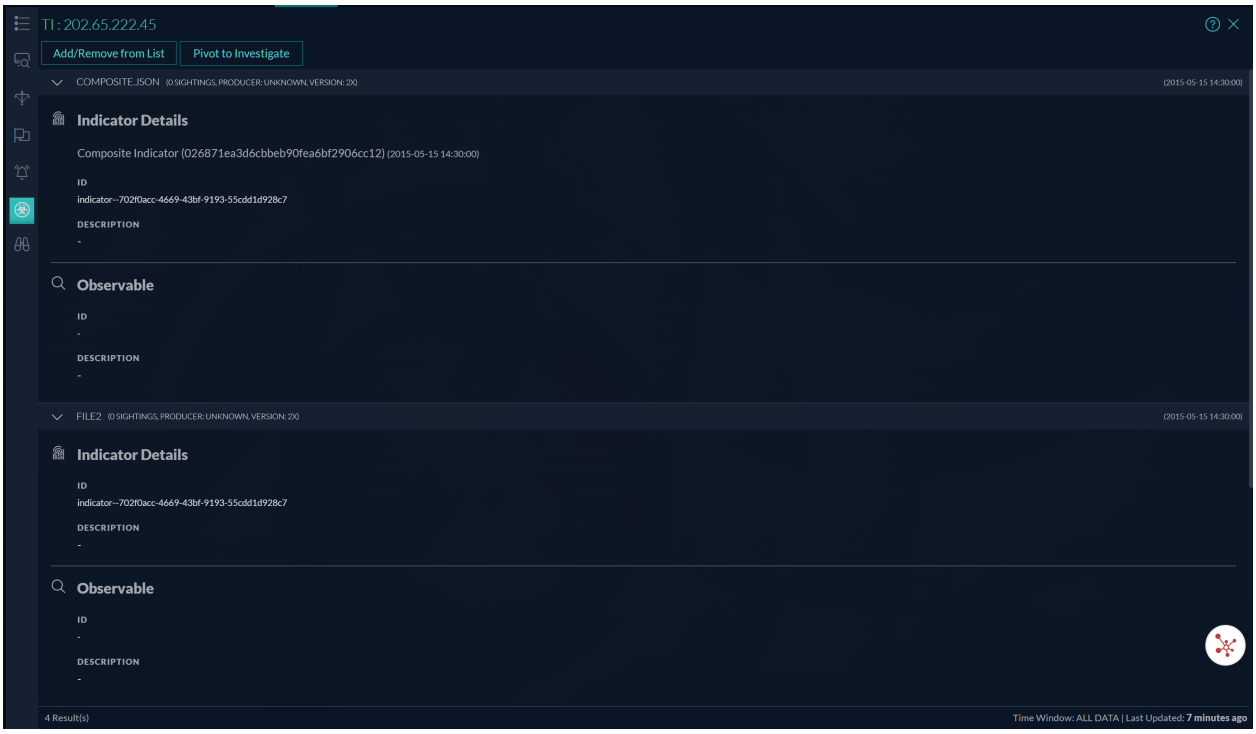
The following section describes the new enhancements for the Context Hub component:

Improved Threat Intelligence with STIX 2.x Integration

NetWitness has enhanced its threat detection and security monitoring capabilities by integrating support for STIX 2.x feeds, including versions 2.0 and 2.1. Administrators can now utilize STIX 2.x (JSON format) to configure File, REST, and TAXII Server as data source indicators for Context Hub. This enhancement allows you to create custom feeds using STIX 2.x data sources. The NetWitness platform analyzes data in the background to extract valuable threat intelligence and identify malicious patterns, providing enriched context through Context Lookup on the **Investigate** and **Respond** pages and helping analysts to conduct investigations more effectively.

This enhancement simplifies the utilization of structured threat intelligence by eliminating many previous constraints, allowing for more descriptive and effective reporting of sightings. This integration involves the conversion of structured threat intelligence from STIX format into a format that the SIEM system can easily understand and use, thus enhancing its effectiveness in protecting against threats.





For more information, see **Configure STIX as a Data Source** topic in the Context Hub Configuration Guide.

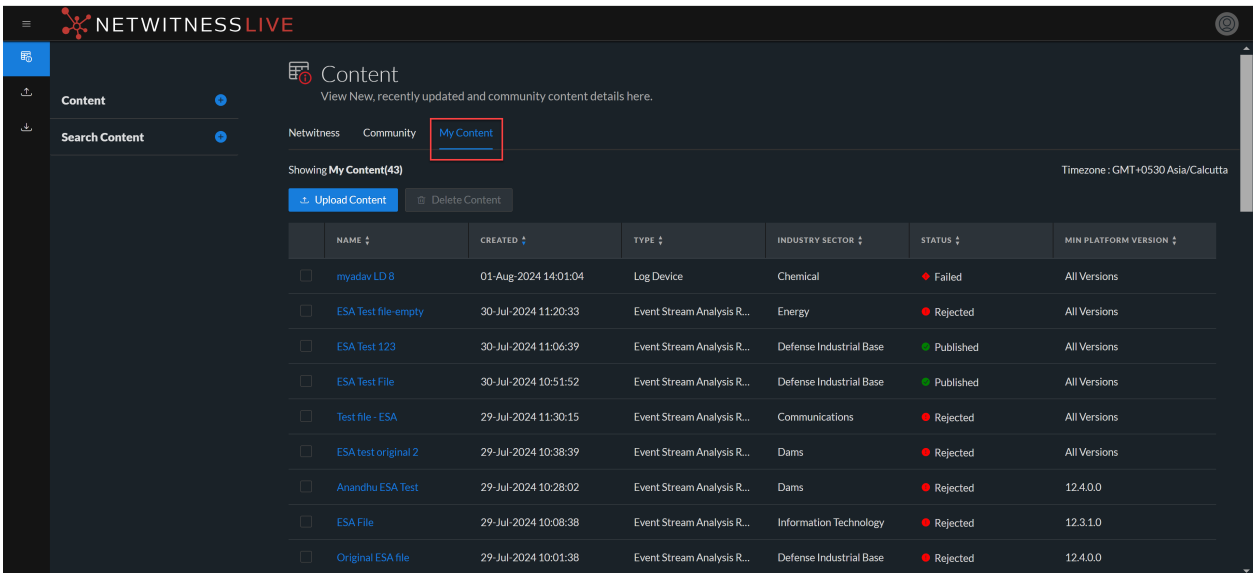
Live Cloud Service

The following section describes the new enhancements for the Live Cloud Service component:

Manage Custom Community Content on NetWitness Live

NetWitness introduces the new My Content feature, allowing users to seamlessly manage custom content directly from the NetWitness Live UI. This includes uploading, deleting, and downloading user-created content like Log Devices, Event Stream Analysis rules, parsers, feeds, etc. This feature provides users with a more efficient way to share useful and relevant custom content among users, reducing the time and effort required to publish content through content publication teams. Users can choose from a range of content options that suit their needs and use cases.

Note: NetWitness Live My Content feature supports only Log Device and ESA contents in this release.



For more information, see the **Manage Custom Content** topic in the NetWitness Live Services Management Guide.

Security Updates

Addresses the latest security vulnerabilities reported against various libraries the NetWitness Platform uses, including one critical (CVE-2016-1000027), 35 major, 103 Moderate, and 16 minor vulnerabilities.

For more information on Security Fixes, see https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#security.

Upgrade Paths

The following upgrade paths are supported for NetWitness 12.5.0.0

- NetWitness 12.4.2.0 to 12.5.0.0
- NetWitness 12.4.1.0 to 12.5.0.0
- NetWitness 12.4.0.0 to 12.5.0.0
- NetWitness 12.3.1.0 to 12.5.0.0
- NetWitness 12.3.0.0 to 12.5.0.0
- NetWitness 12.2.0.1 to 12.5.0.0
- NetWitness 12.2.0.0 to 12.5.0.0

For more information on upgrading to 12.5.0.0, see Upgrade Guide for NetWitness 12.5.0.0

IMPORTANT: NetWitness advises users to check their software versions, noting that versions up to 12.2 have reached End of Life (EOL) as of March 31, 2024. For more information, see https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. To take advantage of the latest features and security updates, NetWitness recommends upgrading to version 12.5.

IMPORTANT: If you want to upgrade from 11.7.x or 11.7.x.x versions to 12.5.0.0 version, you must first upgrade to 12.2.0.0 or 12.3.0.0 version before upgrading to 12.5.

IMPORTANT: The Warehouse connector uses a lockbox to store credentials securely for data integration sources and destinations. However, users upgrading from earlier versions to the 12.5 version cannot start the configured streams without migrating their existing credentials in the new lockbox. As a result, users must manually create a new lockbox key and then refresh the password for their sources and destinations configured in Warehouse Connector, wherever applicable. For detailed instructions on creating the new lockbox key, refer to the **Warehouse Connector** section under the **Post Upgrade Tasks** in the Upgrade Guide for NetWitness 12.5.0.0.

Product Version Life Cycle for NetWitness Platform

See for Product Version Life Cycle for NetWitness Platform a list of versions that reach End of Primary Support (EOPS).

What's New in Previous Releases

The section provides new features and enhancements for all supported previous releases.

For more information, see https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-12-x/ta-p/695650.

Fixed Issues in 12.5.0.0 Release

This section lists issues fixed in 12.5.0.0 version.

For additional information on fixed issues, see the Fixed Version column in the NetWitness® Platform Known Issues list (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) on NetWitness Community Portal.

Endpoint Fixes

Tracking Number	Description
SACE-21629	The polling mechanism on the Endpoint server was not timing out as expected when checking the relay server's message queue, due to an excessive timeout limit.

Home Page Fixes

Tracking Number	Description
ASOC-148336	Users can now select "Home Page" as their default landing page under the User Preferences setting option without encountering a blank screen.

Platform Fixes

Tracking Number	Description
ASOC- 146908	During upgrade, the host fails to boot into el8 kernel after OS Migration is complete.

Decoder Fixes

Tracking Number	Description
ASOC-147188	On running the optional Prune command as part of the DPDK migration, continuous failure messages related to some interfaces on the logs are displayed.
ASOC-144467	When reloading the Hosted plugin, the plugin instance gets deleted instead of reloading from the decoder/hosted tree.
ASOC-154781	Decoder upgrade to 12.4.x eventually fills up /var/netwitness/decoder partition with parsestatdb data.

Known Issues in 12.5.0.0 Release

Issues that remain unresolved in this release are documented in the NetWitness® Platform Known Issues list on the NetWitness community portal: https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

Build Numbers for 12.5.0.0 Components

The following table lists the build numbers for various components of NetWitness 12.5.0.0

Component	Version Number
NetWitness Admin Server	rsa-nw-admin-server-12.5.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Advanced Analytics Content	rsa-nw-advanced-analytics-content-12.5.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Advanced Analytics Server	rsa-nw-advanced-analytics-server-12.5.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Audit Plugin	rsa-audit-plugins-12.5.0.0-4892.5.9d0750b41.el8.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Bootstrap	rsa-nw-bootstrap-12.5.0.0-2401240926.5.a3d68ef.el8.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.5.0.0-2787.5.721a8daa7.el7.x86_64.rpm
NetWitness Cloud	rsa-nw-cloud-12.5.0.0-12867.5.957818c84.el8.x86_64.rpm
NetWitness Cloud Connector Server	rsa-nw-cloud-connector-server-12.5.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Cloud Link Server	rsa-nw-cloud-link-server-12.5.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm
NetWitness Collectd	rsa-collectd-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Component Descriptor	rsa-nw-component-descriptor-12.5.0.0-2402280945.5.4c3391a.el8.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-12.5.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-12.5.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
NetWitness Console	rsa-nw-console-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Content Server	rsa-nw-content-server-12.5.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-12.5.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-12.5.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Dashboard Content	rsa-nw-dashboard-content-20231220155210-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Decoder Analytics Content	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Decoder Content	rsa-nw-decodercontent-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-12.5.0.0-2402150604.5.dbd95e3.el8.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-12.5.0.0-2402061657.5.db93b9a.el8.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-12.5.0.0-240103053136.5.8430874.el8.alma.noarch.rpm
NetWitness Endpoint Decoder Analytics Content	rsa-nw-endpointdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-12.5.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm
NetWitness Esper Enterprise	rsa-nw-esper-enterprise-12.5.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-12.5.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-12.5.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-12.5.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm
NetWitness License Server	rsa-nw-license-server-12.5.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Collector Content	rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm

NetWitness Log Collector Tools	rsa-nw-logcollector-tools-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Log Decoder Analytics Content	rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Log Decoder Base Content	rsa-nw-logdecoder-base-content-20240124060008-5.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-12.5.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm
NetWitness Meta Export Utility	rsa-nw-metaexport-utility-12.5.0.0-110124.5.el8.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-12.5.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm
NetWitness Node Infra Server	rsa-nw-node-infra-server-12.5.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm
NetWitness Orchestration Cli	rsa-nw-orchestration-cli-12.5.0.0-2401091103.5.7317baa.el8.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-12.5.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitness Placeholder	rsa-nw-placeholder-12.5.0.0-2310040926.5.cebd204.el8.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Config Server	rsa-nw-presidio-configserver-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Core	rsa-nw-presidio-core-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Elastic Search Init	rsa-nw-presidio-elasticsearch-init-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.5.0.0-2401151152.5.18bd06b.el8.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Output	rsa-nw-presidio-output-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio UI	rsa-nw-presidio-ui-12.5.0.0-2402270745.5.0844250.el8.noarch.rpm

NetWitness Protobufs	rsa-protobufs-rt-12.5.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitness Recovery Tools	rsa-nw-recovery-tool-12.5.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitness Relay Server	rsa-nw-relay-server-12.5.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-12.5.0.0-5996.5.b76234be4.el8.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-12.5.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Response Actions Server	rsa-nw-response-actions-server-12.5.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-12.5.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness SA Tools	rsa-sa-tools-12.5.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitness Security Cli	rsa-nw-security-cli-12.5.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitness Security Server	rsa-nw-security-server-12.5.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitness Shell	rsa-nw-shell-12.5.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitness SOS Report Plugins	rsa-nw-sosreport-plugins-12.5.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness SMS Runtime RT	rsa-sms-runtime-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Source Server	rsa-nw-source-server-12.5.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitness Source Server Content	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
NetWitness User Interface	rsa-nw-ui-12.5.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.4.5.0-12866.5.1aefe557c.el8.x86_64.rpm

Getting Help with NetWitness Platform

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
NetWitness Platform Master Table of Contents	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.4.0.0 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.4.0.0 Upgrade Guide	https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308
NetWitness Analytics on Cloud	To learn more about new features and enhancements in NetWitness Analytics on Cloud releases, check the following What's New section: For UEBA Cloud, see https://docs.netwitness.com/netwitnessueba/release_information/whats_new/. For Insight, see https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/.

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, contact NetWitness Support.

Contact NetWitness Support

If you contact NetWitness Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the NetWitness Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW Update	https://update.netwitness.com/
LiveUI	https://live.netwitness.com

NetWitness Educational Services

Sign up for access to NetWitness courses and additional resources on the NetWitness Educational Services and Training.

NetWitness Education Portal	https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog
NetWitness Educational Services Course Catalog	https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training
NetWitness Educational Services Training Schedule	https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826
NetWitness Educational Services Support Contact	education.support@netwitness.com

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.