NetWitness® Platform XDR

Version 12.3.0.0

Release Notes

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.

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, 2023

Contents

What's New in 12.3.0.0 Release

The NetWitness 12.3.0.0 Release Notes describe new features, enhancements, security fixes, 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:

- Policy-based Centralized Content Management (CCM)
- Investigate
- Context Hub
- Insight
- SASE Capability
- Springboard
- Respond
- Endpoint Enhancements
- User and Entity Behavior Analytics
- Concentrator, Decoder, and Log Decoder Services
- Log Integrations
- Third-Party Integrations
- Security
- Platform

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.

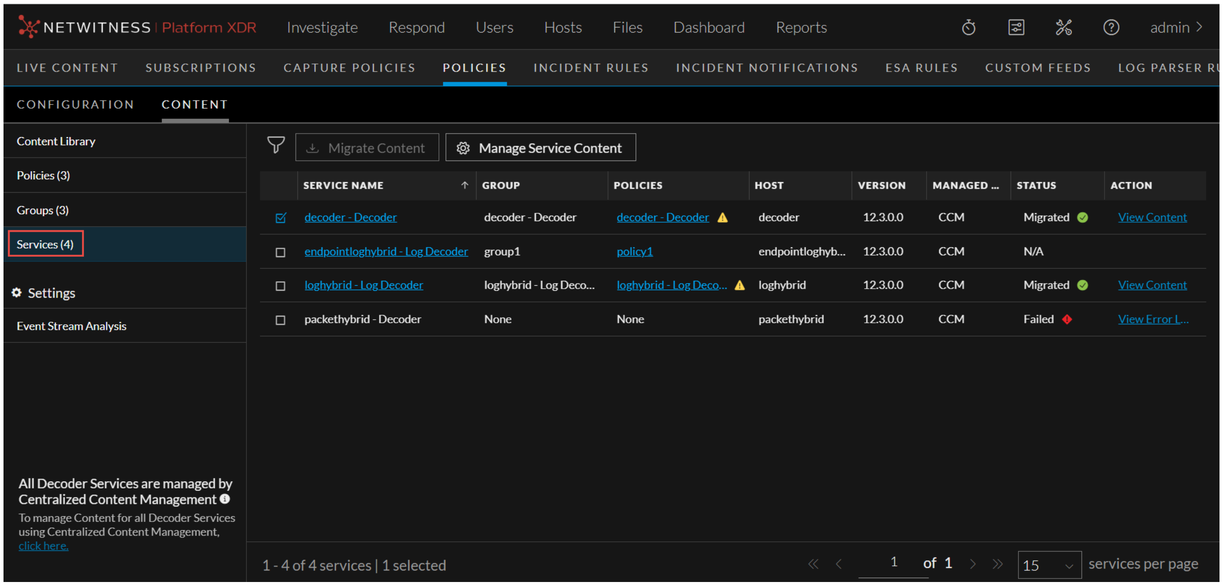
Policy-based Centralized Content Management (CCM)

The following enhancements are made for Policy-based Centralized Content Management in 12.3.0.0 version:

Addition of Services Tab in Content Panel

NetWitness has introduced the **Services** tab to view and manage the 12.3 and above services. The dedicated **Services List** page lists all Decoder and Log Decoder services available in the 12.3+ version. From this page, you can initiate migration, view the content of each service after migration, and conveniently enable or disable CCM for individual services.

- To go to **Services** tab, click **(CONFIGURE)** > **Policies** > **Content** > **Services**.



	SERVICE NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
☑	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
□	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

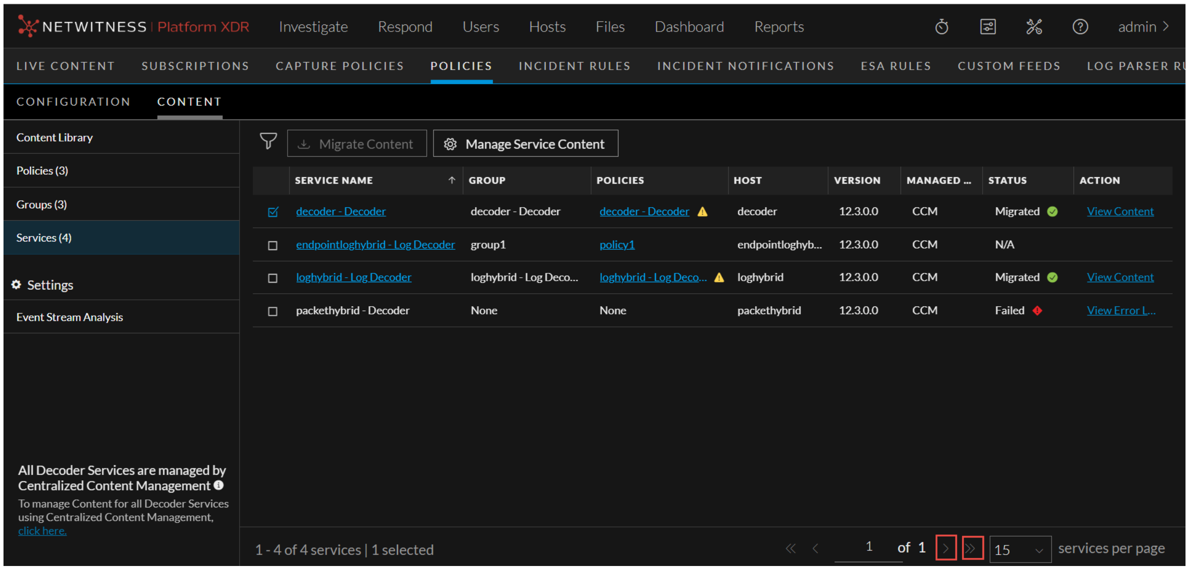
All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 1 selected

1 of 1 15 services per page

- Once you click the **Services** tab:
  - You can view the list of services. By default, 15 services are displayed per page. you can go to the next page by clicking >. You can also directly go to the last page by clicking ≫.



	SERVICE NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
☑	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
□	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

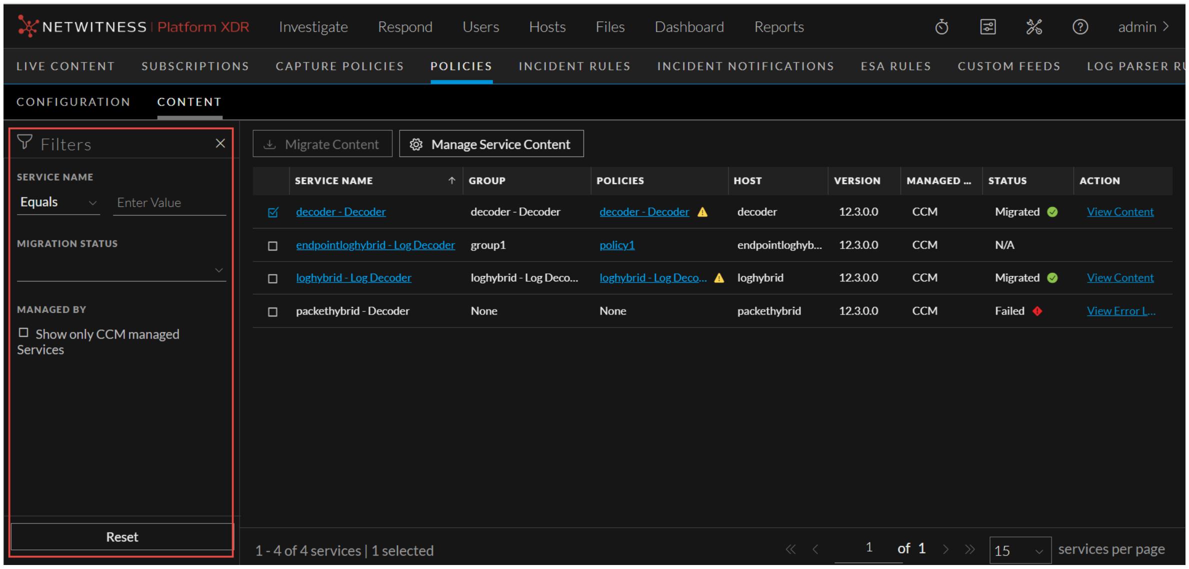
All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 1 selected

1 of 1 15 services per page

  - You can filter the services based on various parameters by clicking .



SERVICE NAME: Equals | Enter Value

MIGRATION STATUS

MANAGED BY

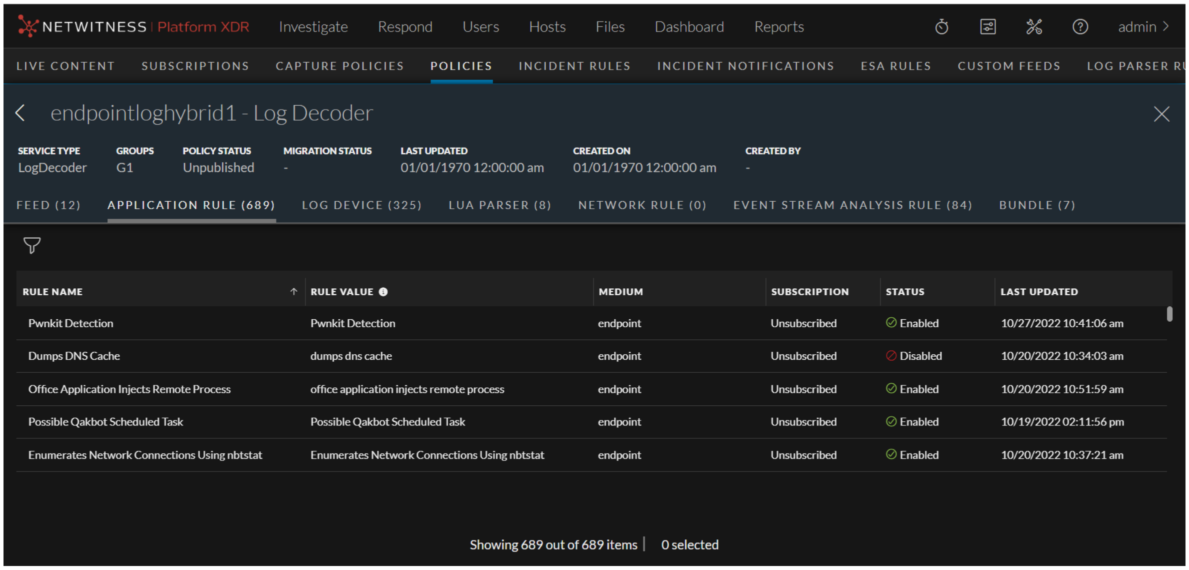
□ Show only CCM managed Services

	SERVICE NAME ↑	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
☑	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
□	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

1 - 4 of 4 services | 1 selected

1 of 1 | 15 services per page

- ○ You can click a service to view the details of the service.



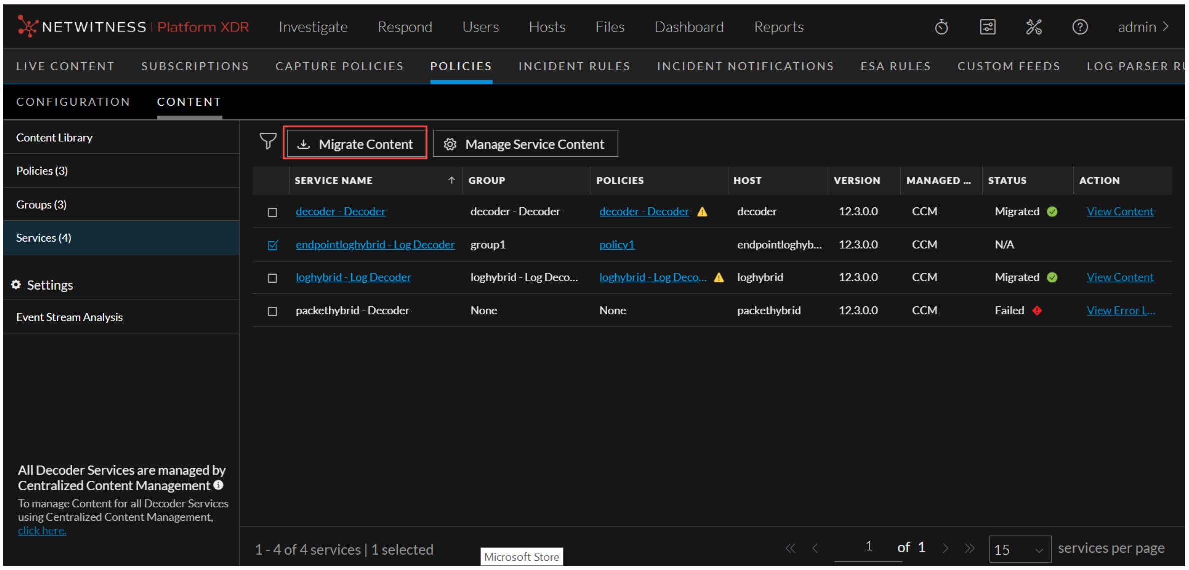
endpointloghybrid1 - Log Decoder

SERVICE TYPE	GROUPS	POLICY STATUS	MIGRATION STATUS	LAST UPDATED	CREATED ON	CREATED BY
LogDecoder	G1	Unpublished	-	01/01/1970 12:00:00 am	01/01/1970 12:00:00 am	-

RULE NAME ↑	RULE VALUE	MEDIUM	SUBSCRIPTION	STATUS	LAST UPDATED
Pwnkit Detection	Pwnkit Detection	endpoint	Unsubscribed	✓ Enabled	10/27/2022 10:41:06 am
Dumps DNS Cache	dumps dns cache	endpoint	Unsubscribed	⊘ Disabled	10/20/2022 10:34:03 am
Office Application Injects Remote Process	office application injects remote process	endpoint	Unsubscribed	✓ Enabled	10/20/2022 10:51:59 am
Possible Qakbot Scheduled Task	Possible Qakbot Scheduled Task	endpoint	Unsubscribed	✓ Enabled	10/19/2022 02:11:56 pm
Enumerates Network Connections Using nbtstat	Enumerates Network Connections Using nbtstat	endpoint	Unsubscribed	✓ Enabled	10/20/2022 10:37:21 am

Showing 689 out of 689 items | 0 selected

- ○ You can automatically migrate content from selected services to CCM Content Library. This feature simplifies the process and saves time by eliminating the need for manual content migration. To migrated content, select the service(s) and click **Migrate Content**.



	SERVICE NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
☑	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

All Decoder Services are managed by Centralized Content Management

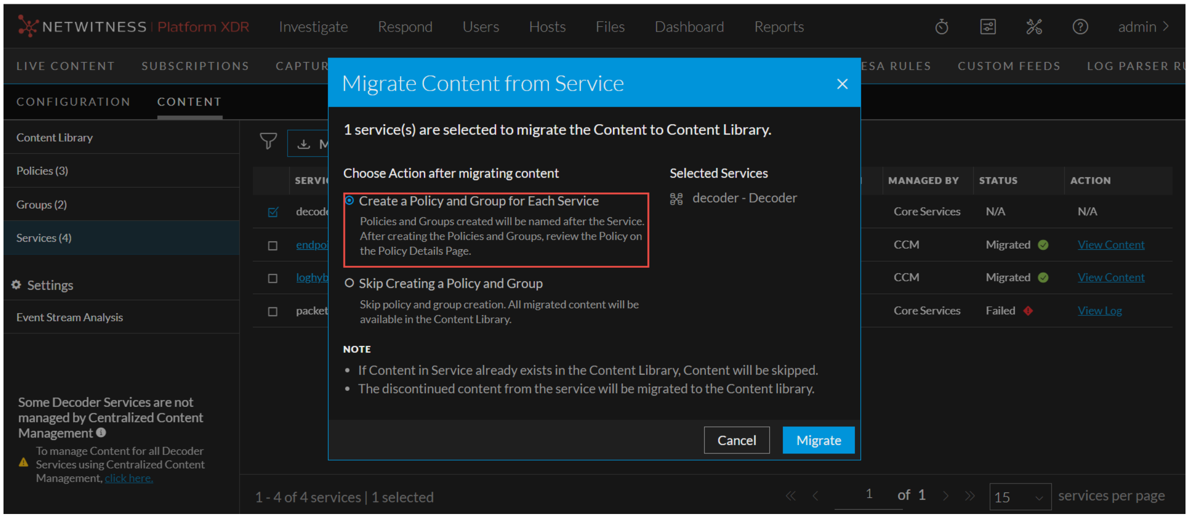
To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 1 selected

1 of 1 | 15 services per page

Note: In this UI, you can migrate Application Rules, Network Rules, LUA Parser, Live Feeds and Live Log Devices. You can continue to manage Custom Feeds and Log Parser Rules from Legacy Custom Feeds UI and Log Parser Rules UI.

- During the migration process, you can create default policy and group for each service selected for migration. Once the migration process is complete, the policy and group will be listed under **Policy Listing** page and **Group Listing** page.



Migrate Content from Service

1 service(s) are selected to migrate the Content to Content Library.

Choose Action after migrating content

● Create a Policy and Group for Each Service

Policies and Groups created will be named after the Service. After creating the Policies and Groups, review the Policy on the Policy Details Page.

○ Skip Creating a Policy and Group

Skip policy and group creation. All migrated content will be available in the Content Library.

Selected Services

decoder - Decoder

NOTE

- If Content in Service already exists in the Content Library, Content will be skipped.
- The discontinued content from the service will be migrated to the Content library.

Cancel | Migrate

	SERVI	MANAGED BY	STATUS	ACTION
☑	decode	Core Services	N/A	N/A
□	endpo	CCM	Migrated ✓	View Content
□	loghyb	CCM	Migrated ✓	View Content
□	packet	Core Services	Failed ◆	View Log

Some Decoder Services are not managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

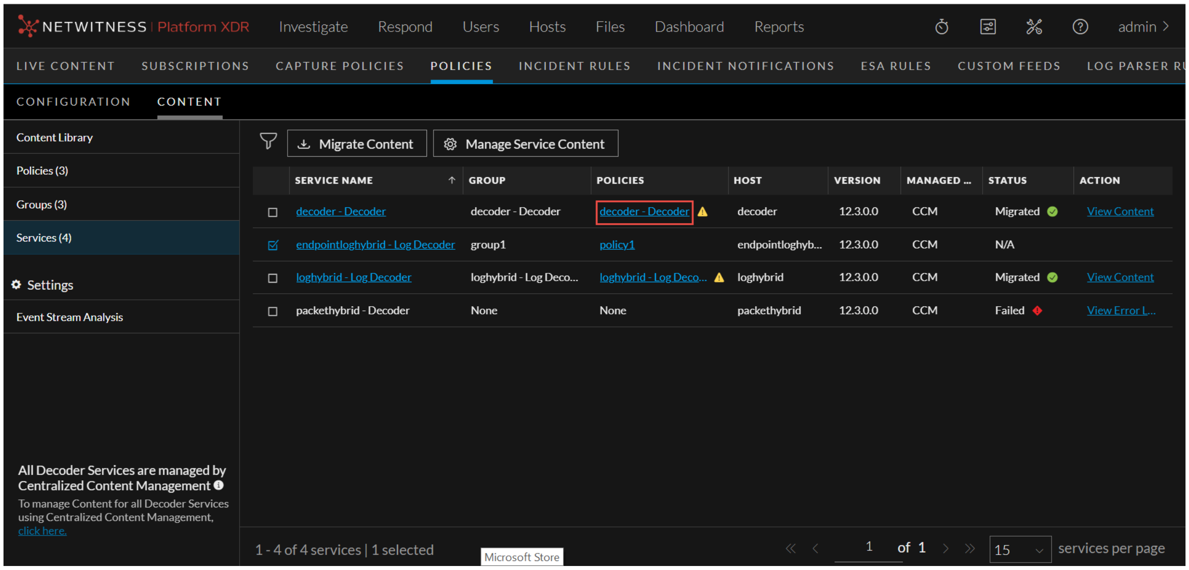
1 - 4 of 4 services | 1 selected

1 of 1 | 15 services per page

Note: The policy and group which is created for the service will be in 'Unpublished' state and it can be published only after it is reviewed. In the **Policy Listing** page, the **Publish** button for such a policy will be disabled. The policy can be published only after reviewing it either from **Policy Details** page or **Edit Policy** Page.

IMPORTANT: While publishing a policy, the content deployed from the policy is merged with the content present in the service. This ensures that duplicate content is overwritten, and unique content present in the service is retained, avoiding unnecessary redundancy and data loss.

- If the migration process is successful and the policy is created successfully for the selected service, you can view the details of the policy. To view the policy details, click policy name under the **Policies** column in **Services List** page.

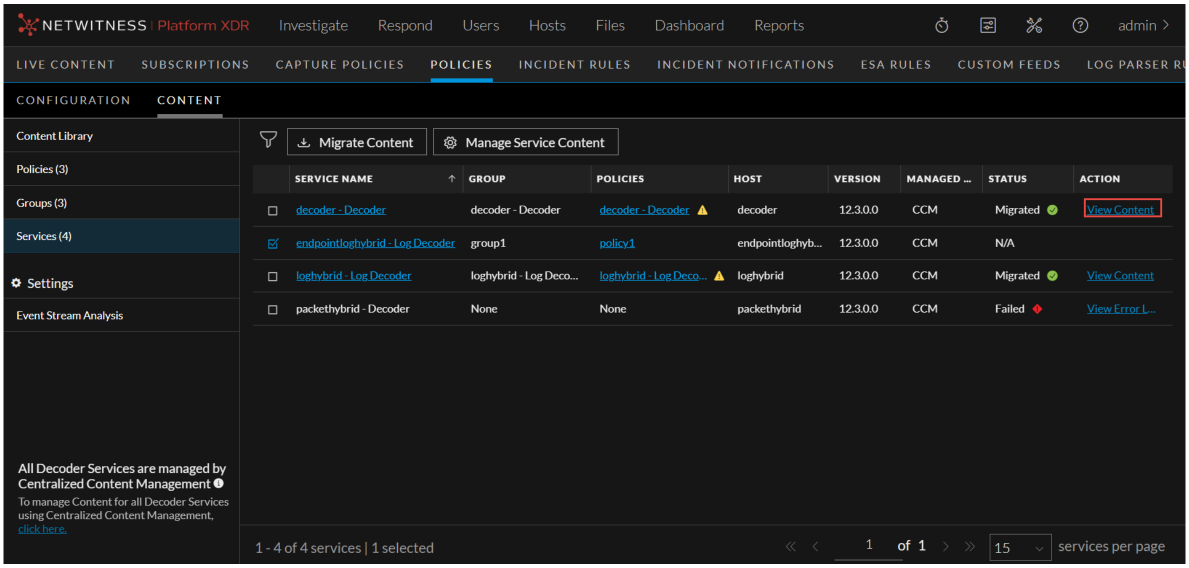


	SERVICE NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
☑	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

All Decoder Services are managed by Centralized Content Management
To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 1 selected « ‹ 1 of 1 › » 15 services per page

- If the migration process is successful, you can view the details of the migrated content. To view the migrated content details, click **View Content** hyperlink under the **Action** column in **Services List** page.

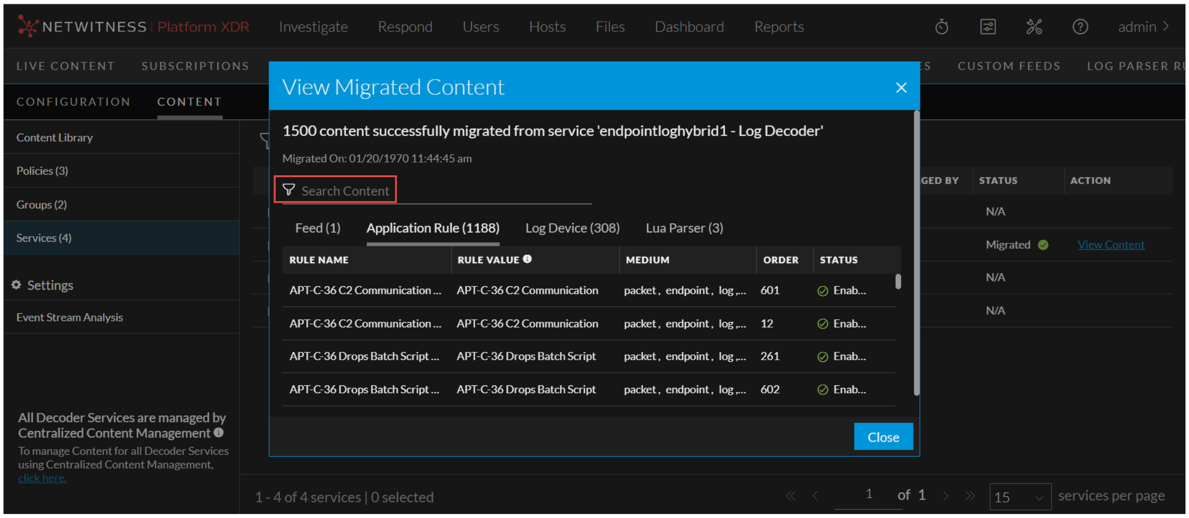

	SERVICE NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
☑	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

All Decoder Services are managed by Centralized Content Management
To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 1 selected « ‹ 1 of 1 › » 15 services per page

- You can search the migrated content based on various parameters.

Note:
- For Application Rule and Network Rule, the search is based on **Rule Name** and **Rule Value**.
- For Feeds, Log Device and LUA Parser, the search is based on the **Name**.



View Migrated Content

1500 content successfully migrated from service 'endpointloghybrid1 - Log Decoder'

Migrated On: 01/20/1970 11:44:45 am

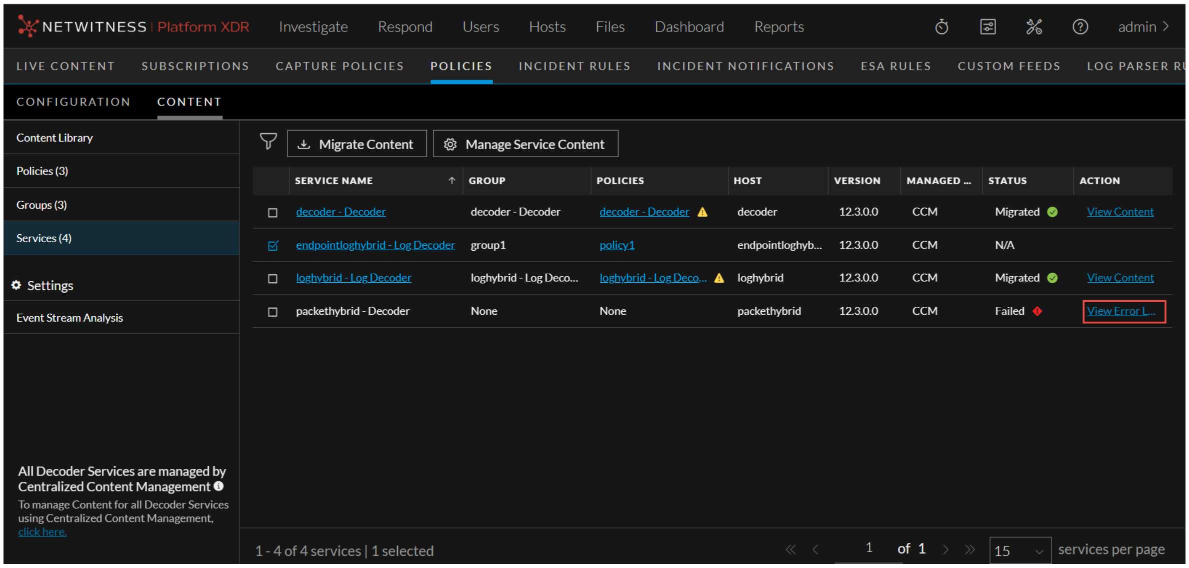
RULE NAME	RULE VALUE	MEDIUM	ORDER	STATUS
APT-C-36 C2 Communication ...	APT-C-36 C2 Communication	packet , endpoint , log ,...	601	✓ Enab...
APT-C-36 C2 Communication ...	APT-C-36 C2 Communication	packet , endpoint , log ,...	12	✓ Enab...
APT-C-36 Drops Batch Script ...	APT-C-36 Drops Batch Script	packet , endpoint , log ,...	261	✓ Enab...
APT-C-36 Drops Batch Script ...	APT-C-36 Drops Batch Script	packet , endpoint , log ,...	602	✓ Enab...

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 0 selected   1 of 1

- If the migration has failed due to some reason, then you can view the logs. To view the logs, click **View Error Log** hyperlink under the **Action** column in **Services List** page.



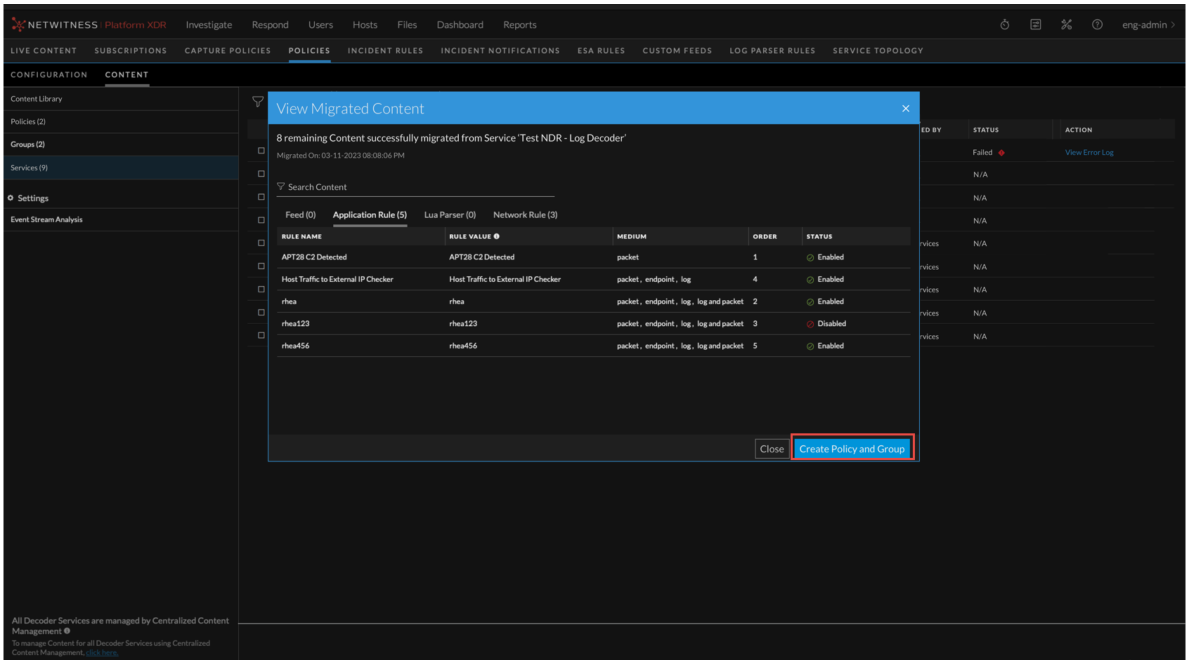
	SERVICE NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
☑	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 1 selected   1 of 1

- Even if only some content from a service is migrated to Content Library, NetWitness has also provided you an option to create policy and group for such a service. To create policy and group for such partially migrated service, click **View Error Log -> View Migrated Content -> Create Policy and Group**.



View Migrated Content

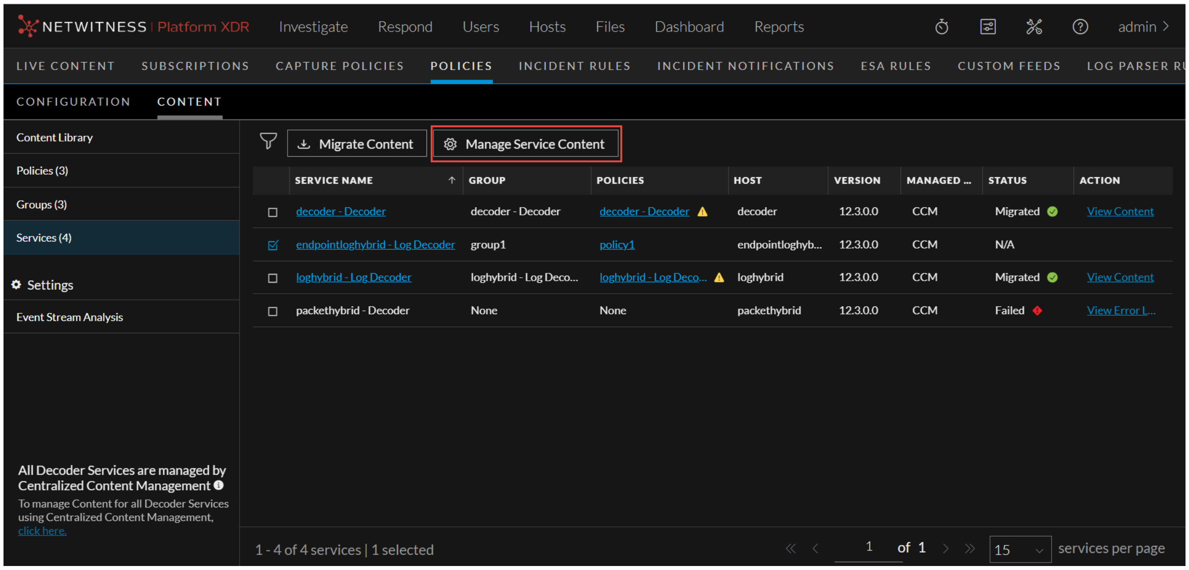
8 remaining Content successfully migrated from Service 'Test NDR - Log Decoder'

Migrated On: 03-11-2023 08:08:06 PM

Feed (0) | Application Rule (5) | Lua Parser (0) | Network Rule (3)

RULE NAME	RULE VALUE	MEDIUM	ORDER	STATUS
APT28 C2 Detected	APT28 C2 Detected	packet	1	Enabled
Host Traffic to External IP Checker	Host Traffic to External IP Checker	packet , endpoint , log	4	Enabled
rhea	rhea	packet , endpoint , log , log and packet	2	Enabled
rhea123	rhea123	packet , endpoint , log , log and packet	3	Disabled
rhea456	rhea456	packet , endpoint , log , log and packet	5	Enabled

- You can enable or disable CCM for individual Decoder Service. To enable or disable CCM, select the service and click **Manage Service Content**.



	SERVICE NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
☑	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

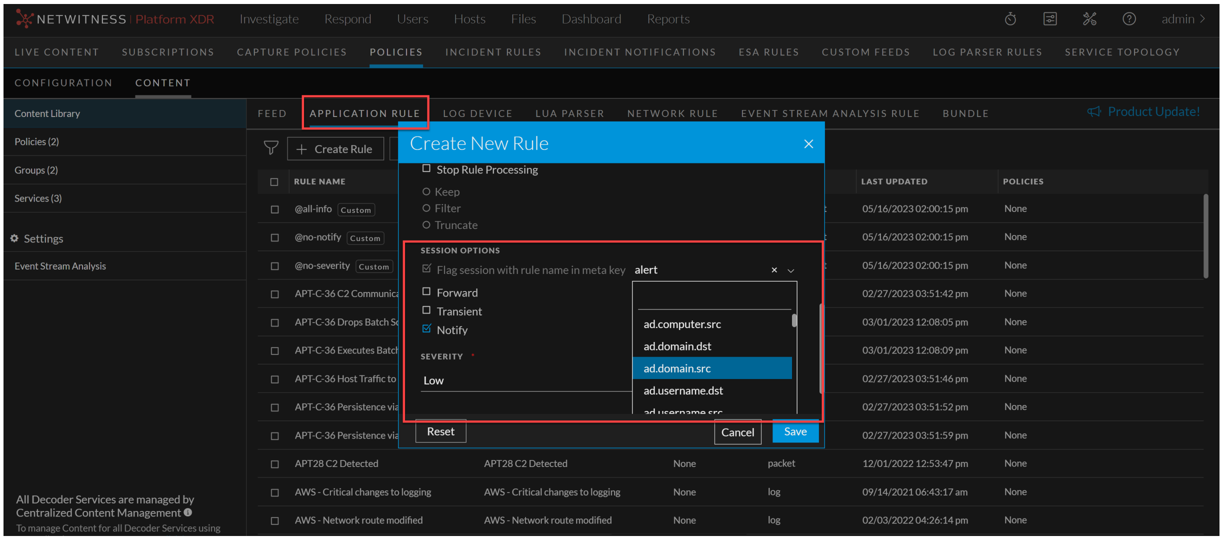
1 - 4 of 4 services | 1 selected

For more information, see the **Manage Services** in the see Policy-based Centralized Content Management Guide.

Application and Network Rule Enhancements

NetWitness has enhanced the Application and Network Rules to help administrators manage the rules efficiently by adding the following improvements:

- Under Session Options, the option **Alert on** is renamed to **Flag session with rule name in meta key** in the Application Rule tab. With this enhancement, administrators can now select a custom meta key from the drop-down, and a meta value corresponding to the rule name will be generated when the session metadata matches the rule.



Create New Rule

☐ Stop Rule Processing

○ Keep
○ Filter
○ Truncate

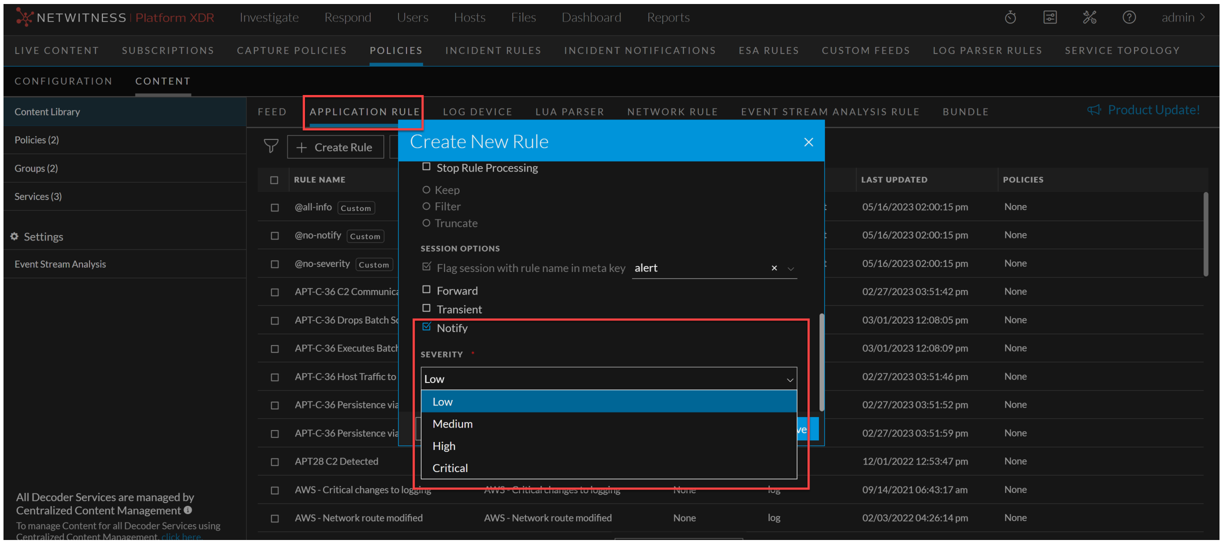
SESSION OPTIONS

☑ Flag session with rule name in meta key: alert

☐ Forward
☐ Transient
☑ Notify

SEVERITY *: Low

- Administrators can now select the **Notify** option to trigger alert generation and choose the **Severity** level while creating or modifying the Application Rules. The severity levels are **Critical**, **High**, **Medium**, and **Low**.



Create New Rule

☐ Stop Rule Processing

○ Keep
○ Filter
○ Truncate

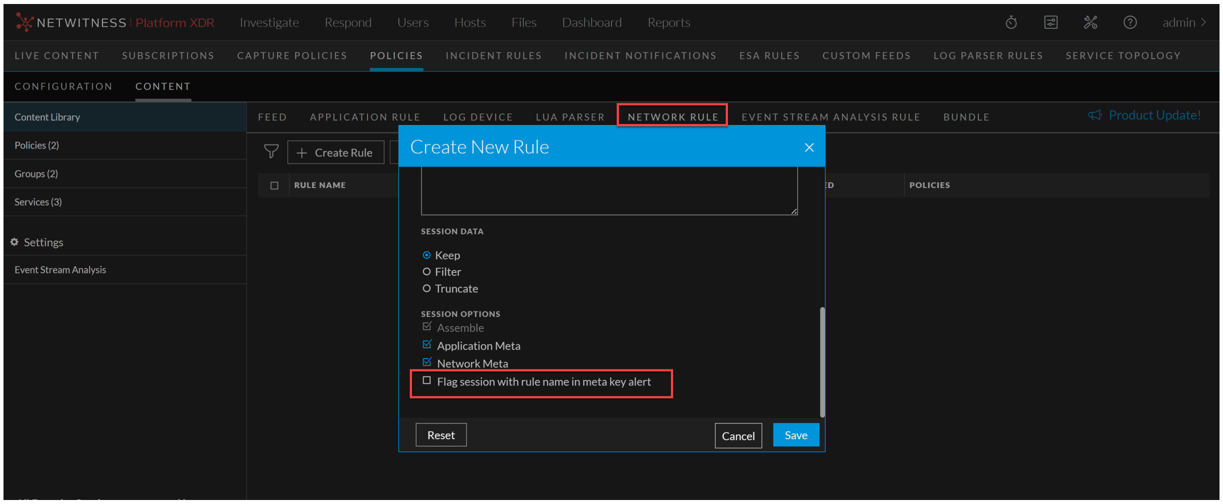
SESSION OPTIONS

☑ Flag session with rule name in meta key: alert

☐ Forward
☐ Transient
☑ Notify

SEVERITY *: Low

- Under Session Options, the option **Alert on** is renamed to **Flag session with rule name in meta key alert** in the Network Rule tab.



SESSION DATA

● Keep
○ Filter
○ Truncate

SESSION OPTIONS

☑ Assemble
☑ Application Meta
☑ Network Meta
□ Flag session with rule name in meta key alert

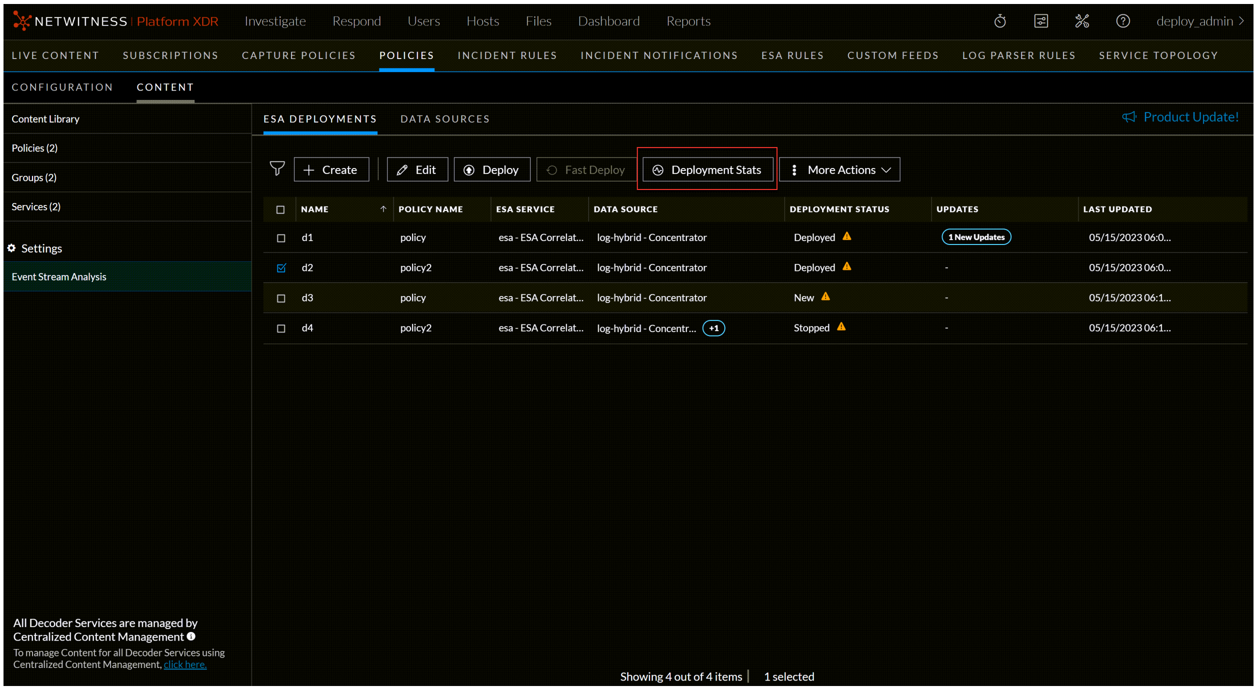
For more information, see the **Create an Application Rule** and **Create a Network Rule** topics in the *Policy-based Centralized Content Management Guide*.

Deployment Statistics

Introducing the new enhanced statistics feature **Deployment Stats** which provides users with comprehensive insights into the performance and status of their deployments.

IMPORTANT: The old legacy **Services** tab has been deprecated, making the CCM the primary location for accessing and managing statistics.

- The statistics associated with engines, rules, and alerts have been moved to the new Centralized Content Management (CCM) pages as part of the ongoing migration.



□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
□	d1	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed ⚠	1 New Updates	05/15/2023 06:0...
☑	d2	policy2	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed ⚠	-	05/15/2023 06:0...
□	d3	policy	esa - ESA Correlat...	log-hybrid - Concentrator	New ⚠	-	05/15/2023 06:1...
□	d4	policy2	esa - ESA Correlat...	log-hybrid - Concentr... +1	Stopped ⚠	-	05/15/2023 06:1...

Showing 4 out of 4 items | 1 selected

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

- Users can easily access and analyze deployment statistics, including engine, rule, and alert metrics, to monitor the effectiveness and efficiency of their configurations.
- The ability to enable and disable rules at the runtime of the engine provides greater flexibility and control over rule execution.
- Users can now view the timestamp indicating when the statistics were last fetched, ensuring the accuracy and relevance of the displayed information.
- On-demand stats fetching allows users to retrieve the latest statistics anytime, keeping them updated with the system's performance.
- In addition to the existing statistics, users can now view individual data source statistics for each engine, enabling a more granular analysis of data source performance.

Create and Edit ESA Rules from CCM (Redirection to ESA Rules Tab)

Introduced a new redirection feature, The ESA rule creation, and editing features have been seamlessly integrated into the existing CCM design, providing a consistent experience and optimizing usability.

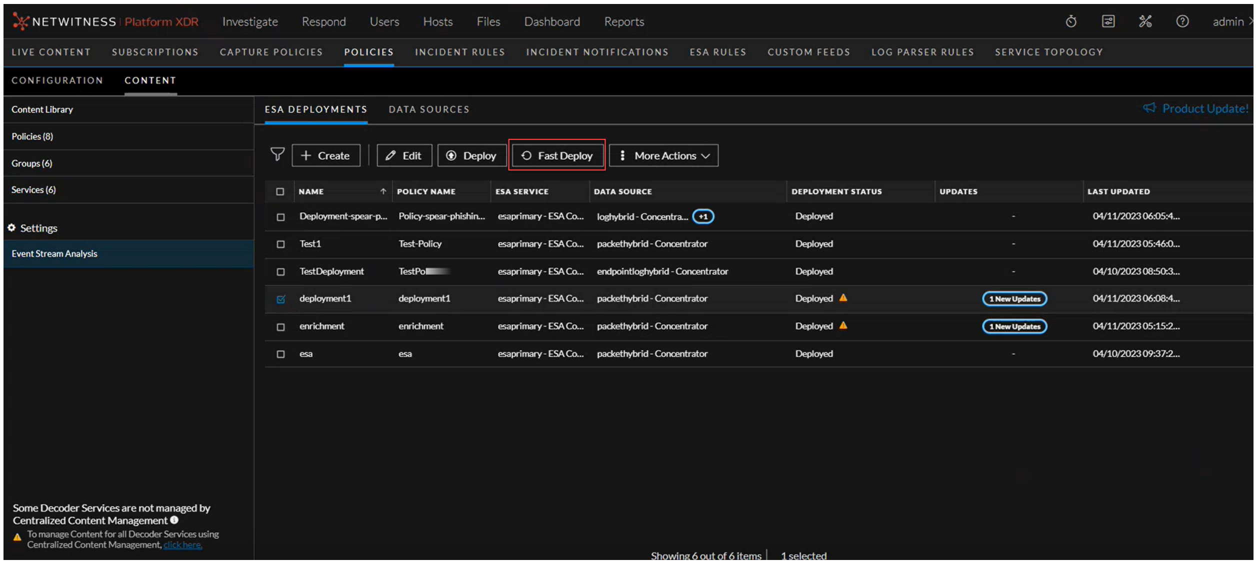
Users can now create and edit ESA rules within the streamlined workflow making necessary modifications to rules minimizing the clicks redirecting to the **ESA Rules Tab**, ensuring a smoother experience.

Endpoint Rule Management

Users can now enable or disable endpoint rules per deployment, allowing them to tailor rule execution to specific deployment requirements.

Fast Deployment Support

Fast Deploy is supported, which allows users to expedite the deployment process for compatible configurations, saving time and effort.



☐	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
☐	Deployment-spear-p...	Policy-spear-phishin...	esaprimary - ESA Co...	loghybrid - Concentra... +1	Deployed	-	04/11/2023 06:05:4...
☐	Test1	Test-Policy	esaprimary - ESA Co...	packethybrid - Concentrator	Deployed	-	04/11/2023 05:46:0...
☐	TestDeployment	TestPo	esaprimary - ESA Co...	endpointloghybrid - Concentrator	Deployed	-	04/10/2023 08:50:3...
☑	deployment1	deployment1	esaprimary - ESA Co...	packethybrid - Concentrator	Deployed ⚠	1 New Updates	04/11/2023 06:08:4...
☐	enrichment	enrichment	esaprimary - ESA Co...	packethybrid - Concentrator	Deployed ⚠	1 New Updates	04/11/2023 05:15:2...
☐	esa	esa	esaprimary - ESA Co...	packethybrid - Concentrator	Deployed	-	04/10/2023 09:37:2...

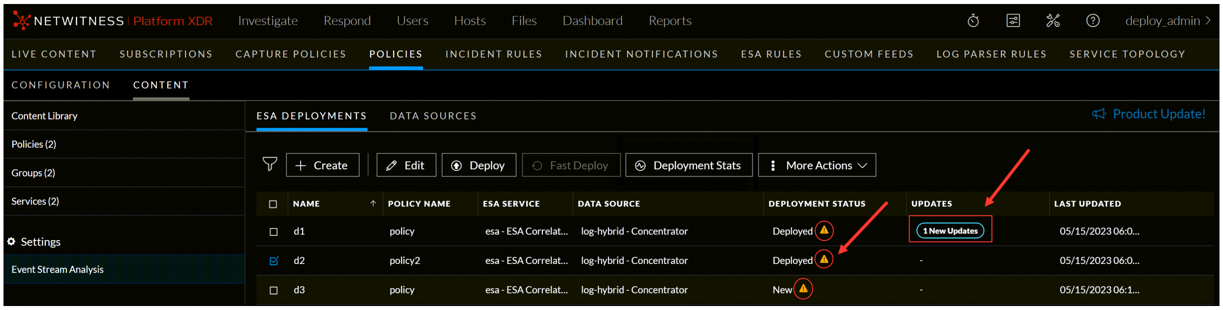
Some Decoder Services are not managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 6 out of 6 items | 1 selected

Deployment Updates, Indicators and Notifications

- Users can easily track updates made to deployments, with a clear indicator signaling the presence of updates.
- Stay informed and effortlessly monitor the status and progress of your deployments.
- Users will be notified if another user is currently editing a deployment, preventing conflicts and ensuring smooth collaboration.
- Notifications and severity configurations for rules in a deployment can be easily viewed, enabling users to stay informed about rule behavior and potential security threats.



□	NAME ↑	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
□	d1	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed ⚠	1 New Updates	05/15/2023 06:0...
☑	d2	policy2	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed ⚠	-	05/15/2023 06:0...
□	d3	policy	esa - ESA Correlat...	log-hybrid - Concentrator	New ⚠	-	05/15/2023 06:1...

For more information on the enhancements, see Policy-based Centralized Content Management Guide.

Investigate

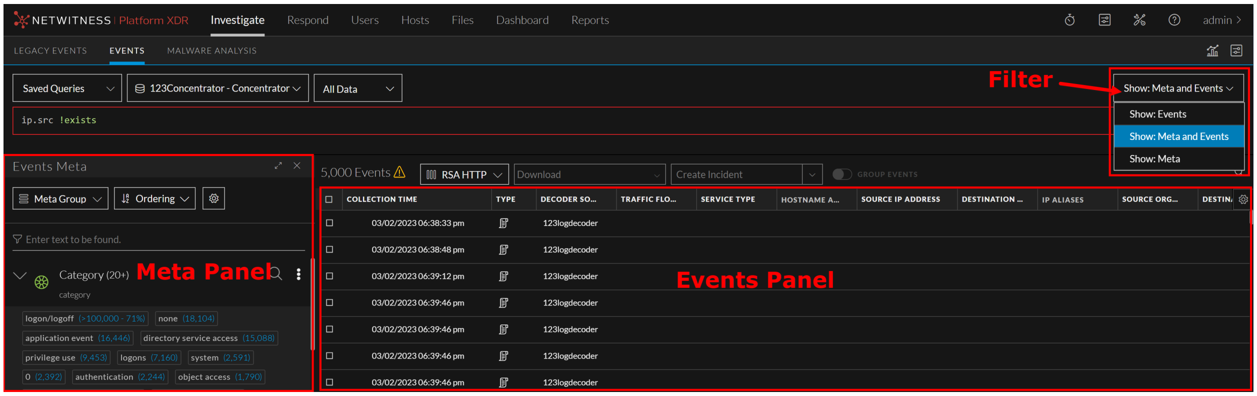
The following section describes the new enhancements for the Investigate component:

NetWitness enhancements in the **Investigate** > **Events** view provide increased flexibility and improved investigative workflow. These enhancements empower analysts to complete investigations and increase efficiency of administrators.

Select Query Results Panel Layout

The **Query Builder** allows you to select the **Query Results** panel layout before executing the query.

For example, if you select, **Show: Meta and Events** option from the dropdown menu, the query results are by default displayed in two separate panels, i.e., **Meta** and **Events**.



```
ip.src !exists
```

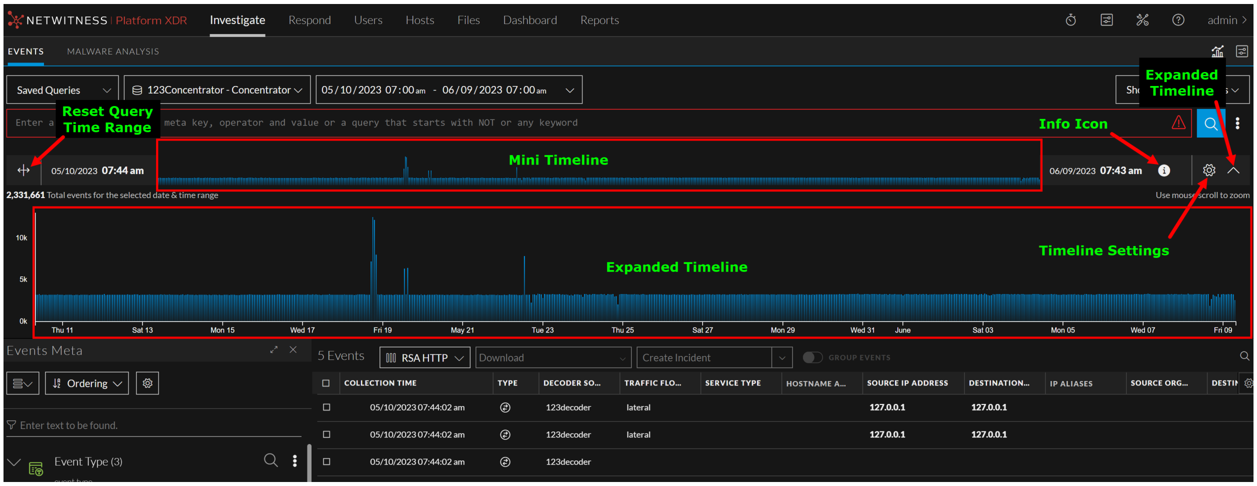
□	COLLECTION TIME	TYPE	DECODER SO...	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP ADDRESS	DESTINATION ...	IP ALIASES	SOURCE ORG...	DESTIN...
□	03/02/2023 06:38:33 pm		123logdecoder								
□	03/02/2023 06:38:48 pm		123logdecoder								
□	03/02/2023 06:39:12 pm		123logdecoder								
□	03/02/2023 06:39:46 pm		123logdecoder								
□	03/02/2023 06:39:46 pm		123logdecoder								
□	03/02/2023 06:39:46 pm		123logdecoder								
□	03/02/2023 06:39:46 pm		123logdecoder								

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

Timeline Enhancements

The enhanced **Timeline** displays activity for the specified service and time range as a bar chart. This allows analysts to detect significant spikes that could indicate anomalies. Using the visual representation, analysts can conduct a more detailed investigation of the events that occurred during that specific period.

With the enhanced timeline, analyst can now expand the timeline, zoom into the interested zone in the timeline, change the axis settings, or reset the query to the original requested form.



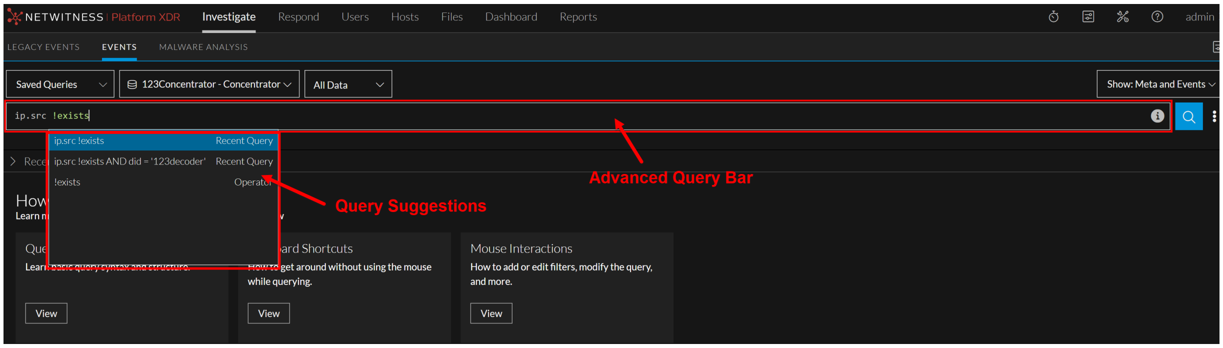
□	COLLECTION TIME	TYPE	DECODER SO...	TRAFFIC FLO...	SERVICE TYPE	HOSTNAME A...	SOURCE IP ADDRESS	DESTINATION...	IP ALIASES	SOURCE ORG...	DESTIN
□	05/10/2023 07:44:02 am		123decoder	lateral			127.0.0.1	127.0.0.1			
□	05/10/2023 07:44:02 am		123decoder	lateral			127.0.0.1	127.0.0.1			
□	05/10/2023 07:44:02 am		123decoder								

For more information, see **Timeline** topic in the *NetWitness Investigate User Guide*.

Introducing Advanced Query Bar

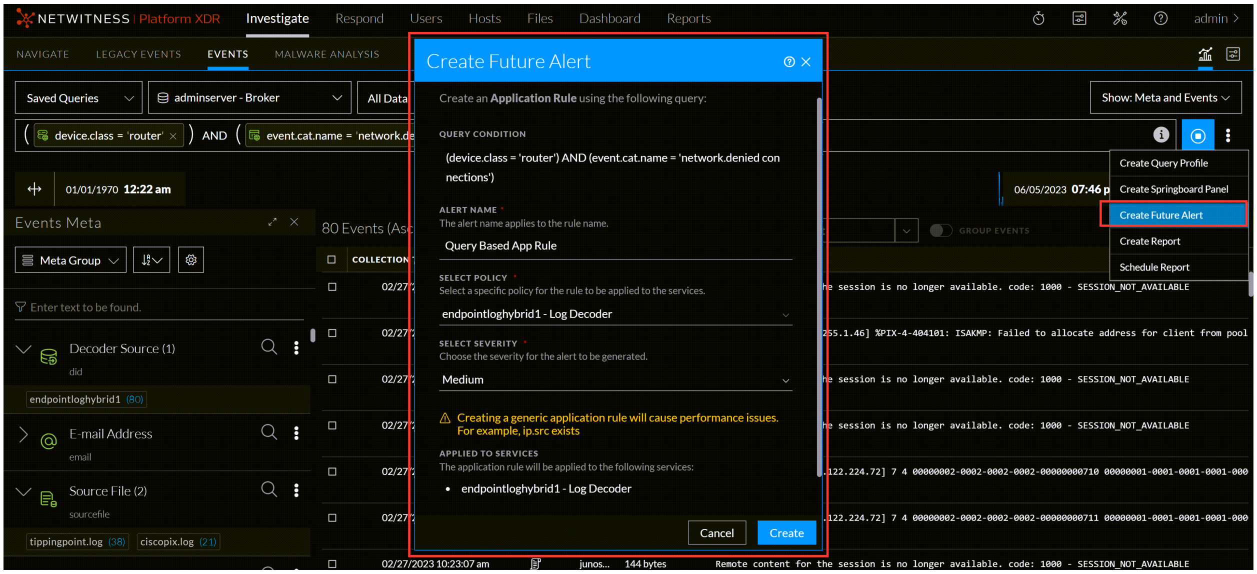
NetWitness introduces the new Advanced Query Bar under **Investigate** > **Events** panel to provide a seamless experience to the users while they write queries. Advanced Query Bar provides a search bar with the ability to accept a query construction in text form just like an Integrated Development Environment (IDE), instead of the pill-based entry of Guided Mode. Advanced Query Bar provides following benefits:

- **Syntax or error highlighting**: The syntax of each query is validated and a red outline marks invalid filters.
- **Auto suggestions**: Suggestions such as meta key, an alias for medium, an operator in a drop-down list to help in query construction.
- **Recent queries**: Displays recent queries.


NETWITNESS | Platform XDR
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
LEGACY EVENTS
EVENTS
MALWARE ANALYSIS
Saved Queries
123Concentrator - Concentrator
All Data
Show: Meta and Events
ip.src !exists
ip.src !exists Recent Query
ip.src !exists AND did = '123decoder' Recent Query
!exists Operator
Advanced Query Bar
Query Suggestions
ard Shortcuts
How to get around without using the mouse while querying.
Mouse Interactions
How to add or edit filters, modify the query, and more.
View
View
View

Create Future Alert using Events Query

During the investigation, administrators and analysts can now create an application rule for any suspicious activity from the **Investigate** > **Events** view. You can create application rules with a flexible query that covers a wide set of events and system information from your network, including suspected breach activities and misconfigured servers. Once the rule is applied to a matched policy with Decoder services, it generates alerts whenever a match occurs and helps analysts to triage, investigate, and respond to threats.



Create Future Alert

Create an **Application Rule** using the following query:

QUERY CONDITION

(device.class = 'router') AND (event.cat.name = 'network.denied connections')

ALERT NAME *

The alert name applies to the rule name.

Query Based App Rule

SELECT POLICY *

Select a specific policy for the rule to be applied to the services.

endpointloghybrid1 - Log Decoder

SELECT SEVERITY *

Choose the severity for the alert to be generated.

Medium

⚠ Creating a generic application rule will cause performance issues. For example, ip.src exists

APPLIED TO SERVICES

The application rule will be applied to the following services:

- endpointloghybrid1 - Log Decoder

For more information, see the **Create a Future Alert from Events View** topic in the *NetWitness Investigate User Guide*.

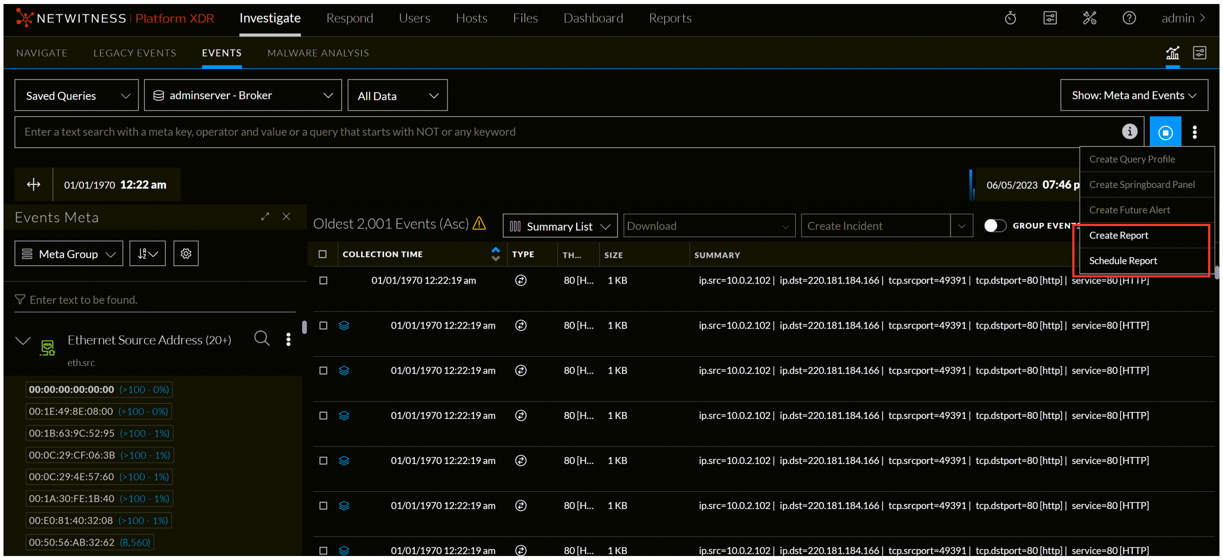
Generate Custom Reports from Investigate Events View

NetWitness Investigate Events view has been enhanced with integrated reporting capabilities enabling increased flexibility and streamlined workflow. Administrators and analysts can now convert their investigation queries into adhoc and schedule reports seamlessly from the **Investigate** > **Events** view. This eliminates the need to switch back to the reporting pages and reconfigure queries, saving time and effort.

The following are the key benefits of generating reports from the **Events** view:

- Quickly configure and generate the reports.
- Share generated reports directly with administrators or other analysts by configuring email IDs, facilitating efficient communication and collaboration.
- Report generation now adopts preconfigured settings by default, reducing the need for manual configuration and accelerating the reporting process.
- Generated reports can be used to monitor security incidents and malware activity.
- Set up scheduled reports to run at regular intervals and trigger an email with events each time they

run.

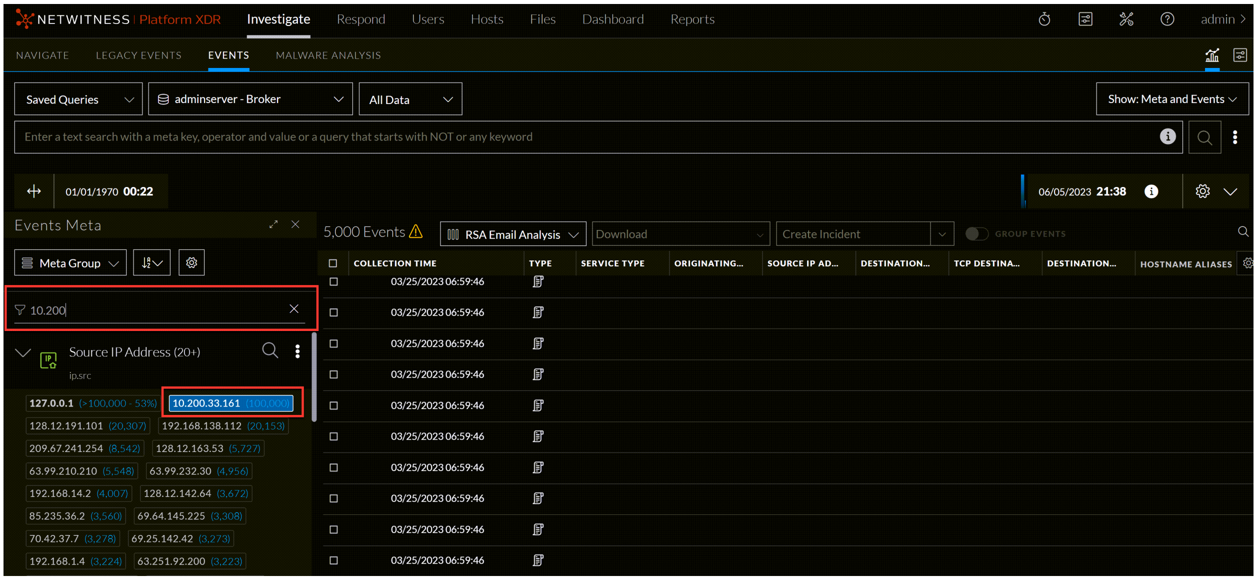


COLLECTION TIME	TYPE	TH...	SIZE	SUMMARY
01/01/1970 12:22:19 am		80 [H...	1 KB	ip.src=10.0.2.102 | ip.dst=220.181.184.166 | tcp.srcport=49391 | tcp.dstport=80 [http] | service=80 [HTTP]
01/01/1970 12:22:19 am		80 [H...	1 KB	ip.src=10.0.2.102 | ip.dst=220.181.184.166 | tcp.srcport=49391 | tcp.dstport=80 [http] | service=80 [HTTP]
01/01/1970 12:22:19 am		80 [H...	1 KB	ip.src=10.0.2.102 | ip.dst=220.181.184.166 | tcp.srcport=49391 | tcp.dstport=80 [http] | service=80 [HTTP]
01/01/1970 12:22:19 am		80 [H...	1 KB	ip.src=10.0.2.102 | ip.dst=220.181.184.166 | tcp.srcport=49391 | tcp.dstport=80 [http] | service=80 [HTTP]
01/01/1970 12:22:19 am		80 [H...	1 KB	ip.src=10.0.2.102 | ip.dst=220.181.184.166 | tcp.srcport=49391 | tcp.dstport=80 [http] | service=80 [HTTP]
01/01/1970 12:22:19 am		80 [H...	1 KB	ip.src=10.0.2.102 | ip.dst=220.181.184.166 | tcp.srcport=49391 | tcp.dstport=80 [http] | service=80 [HTTP]
01/01/1970 12:22:19 am		80 [H...	1 KB	ip.src=10.0.2.102 | ip.dst=220.181.184.166 | tcp.srcport=49391 | tcp.dstport=80 [http] | service=80 [HTTP]

For more information, see the **Generate Reports from Events View** topic in the *NetWitness Investigate User Guide*.

Search Meta Information Quickly from Events Meta Panel

Analysts can now search for meta keys and meta values quickly from the **Events Meta** panel using the newly added **Filter** option. This enhancement allows analysts to refine their search results by entering specific meta values or keys and the results are highlighted with blue indicator and helps analysts to investigate seamlessly rather than scrolling through a long list of metadata.

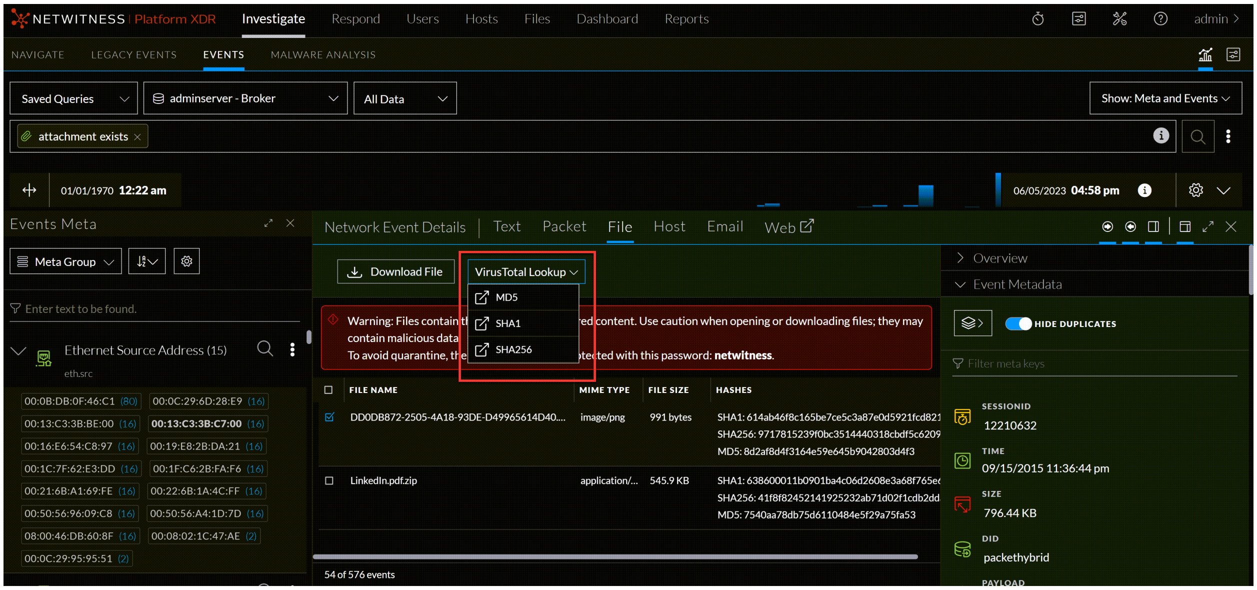


COLLECTION TIME	TYPE	SERVICE TYPE	ORIGINATING...	SOURCE IP AD...	DESTINATION...	TCP DESTINA...	DESTINATION...	HOSTNAME ALIASES
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								
03/25/2023 06:59:46								

For more information, see the **Filter Meta Information using Events Meta Panel** topic in the *NetWitness Investigate User Guide*.

Support for VirusTotal Hashes Lookup from Events View

NetWitness now includes files and file hashes VirusTotal Lookup capabilities from the **Investigate** > **Events** view. With this enhancement, analysts can perform a VirusTotal Lookup on files with file hashes (**MD5**, **SHA1**, and **SHA256**) to get more information about the file, which automatically redirects them to VirusTotal's website. Once the hashes match VirusTotal's recognized types, they undergo a malware scan. The results are returned to determine if a file is malicious or not. This enhancement makes it easier for analysts to identify viruses, malware, and other malicious files with VirusTotal Lookup and helps them to perform investigation more effectively.



00:0B:DB:0F:46:C1 (80) 00:0C:29:6D:28:E9 (16)
00:13:C3:3B:BE:00 (16) 00:13:C3:3B:C7:00 (16)
00:16:E6:54:C8:97 (16) 00:19:E8:2B:DA:21 (16)
00:1C:7F:62:E3:DD (16) 00:1F:C6:2B:FA:F6 (16)
00:21:6B:A1:69:FE (16) 00:22:6B:1A:4C:FF (16)
00:50:56:96:09:C8 (16) 00:50:56:A4:1D:7D (16)
08:00:46:DB:60:8F (16) 00:08:02:1C:47:AE (2)
00:0C:29:95:95:51 (2)

Warning: Files contain th… …red content. Use caution when opening or downloading files; they may contain malicious data.
To avoid quarantine, the… …otected with this password: **netwitness**.

☐	FILE NAME	MIME TYPE	FILE SIZE	HASHES
☑	DD0DB872-2505-4A18-93DE-D49965614D40....	image/png	991 bytes	SHA1: 614ab46f8c165be7ce5c3a87e0d5921fcd821 SHA256: 9717815239f0bc3514440318cbdf5c6209 MD5: 8d2af8d4f3164e59e645b9042803d4f3
☐	LinkedIn.pdf.zip	application/...	545.9 KB	SHA1: 638600011b0901ba4c06d2608e3a68f765e SHA256: 41f8f82452141925232ab71d02f1cdb2dd MD5: 7540aa78db75d6110484e5f29a75fa53

54 of 576 events

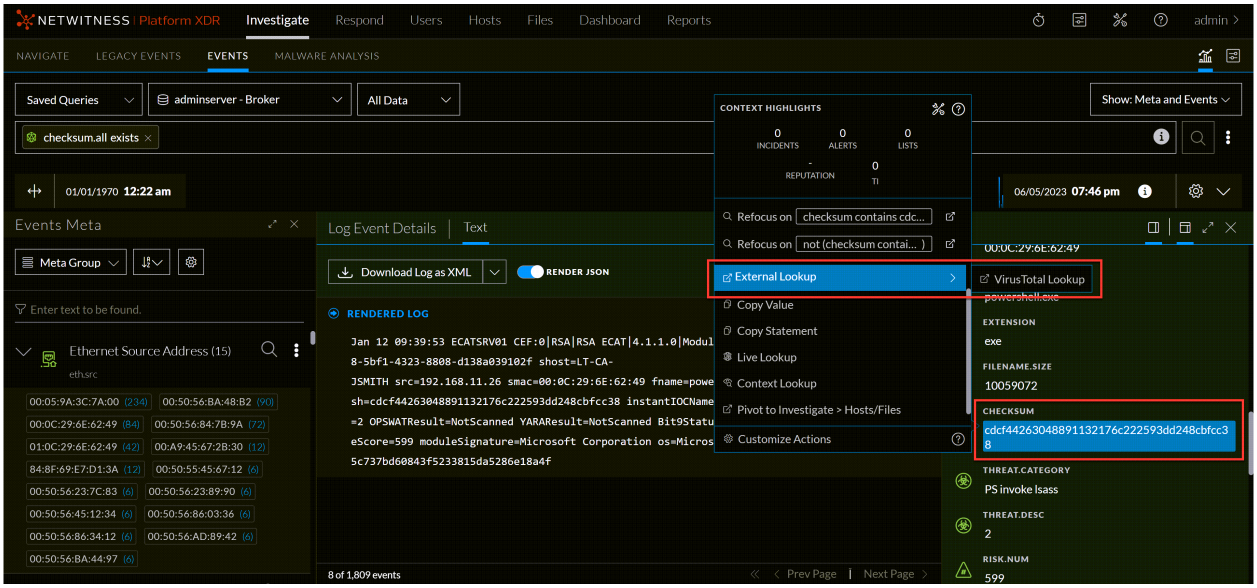
SESSIONID
12210632

TIME
09/15/2015 11:36:44 pm

SIZE
796.44 KB

DID
packethybrid

PAYLOAD



00:05:9A:3C:7A:00 (234) 00:50:56:BA:48:B2 (90)
00:0C:29:6E:62:49 (84) 00:50:56:84:7B:9A (72)
01:0C:29:6E:62:49 (42) 00:A9:45:67:2B:30 (12)
84:8F:69:E7:D1:3A (12) 00:50:55:45:67:12 (6)
00:50:56:23:7C:83 (6) 00:50:56:23:89:90 (6)
00:50:56:45:12:34 (6) 00:50:56:86:03:36 (6)
00:50:56:86:34:12 (6) 00:50:56:AD:89:42 (6)
00:50:56:BA:44:97 (6)

```
Jan 12 09:39:53 ECATSRV01 CEF:0|RSA|RSA ECAT|4.1.1.0|Modul
8-5bf1-4323-8808-d138a039102f shost=LT-CA-
JSMITH src=192.168.11.26 smac=00:0C:29:6E:62:49 fname=powe
sh=cdcf44263048891132176c222593dd248cbfcc38 instantIOCName
=2 OPSWATResult=NotScanned YARAResult=NotScanned Bit9Statu
eScore=599 moduleSignature=Microsoft Corporation os=Micros
5c737bd60843f5233815da5286e18a4f
```

8 of 1,809 events

00:0C:29:6E:62:49
powershell.exe

EXTENSION
exe

FILENAME.SIZE
10059072

CHECKSUM
cdcf44263048891132176c222593dd248cbfcc38

THREAT.CATEGORY
PS invoke lsass

THREAT.DESC
2

RISK.NUM
599

For more information, see **Launch a VirusTotal Lookup for a File** and **Perform Lookups of Meta Values in Events** topics in the *NetWitness Investigate User Guide*.

Introducing Meta Settings Panel

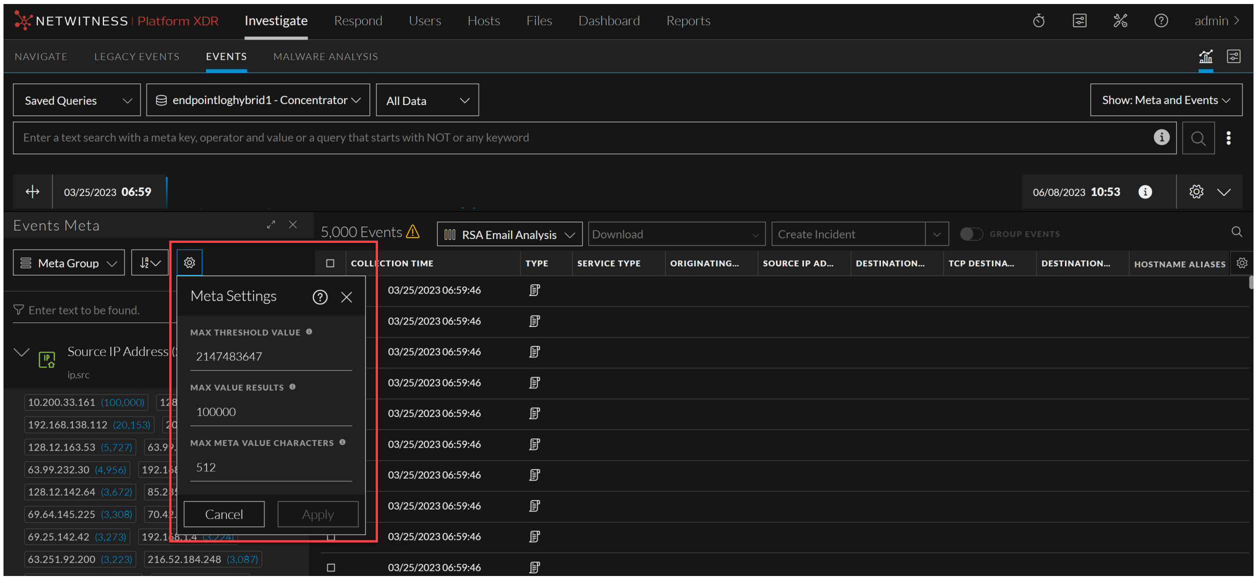
NetWitness introduces the new **Meta Settings** panel under the **Investigate** > **Events** > **Events Meta** view to allow analysts to configure the number of sessions required for the specific meta key value within the Events view. This enhancement provides analysts with the following configuration options:

- **Max Threshold Value**: This option allows analysts to set the maximum number of sessions that are loaded for a meta key value in the Events panel. If you set a higher threshold, you will get more accurate counts, but it will take longer to load the data. The Max Threshold Value should be between 1 - 2147483647. The default value is 100,000.

- **Max Value Results**: This option allows analysts to set the maximum number of values to load in the Events view when the Max Results option is selected in the Meta Key Menu for an open Meta Key. The Max Value Results should be between 100-100000. The default value is 1000.

- **Max Meta Value Characters**: This option allows analysts to set the maximum number of characters in a meta value name displayed in the Events Meta panel. The Max Meta Value Characters should be between 60-512. The default value is 60.

These new configuration options give analysts more control over how metadata is displayed and loaded in the Events view. This helps analysts to perform the investigation more efficiently.



Meta Settings

MAX THRESHOLD VALUE: 2147483647

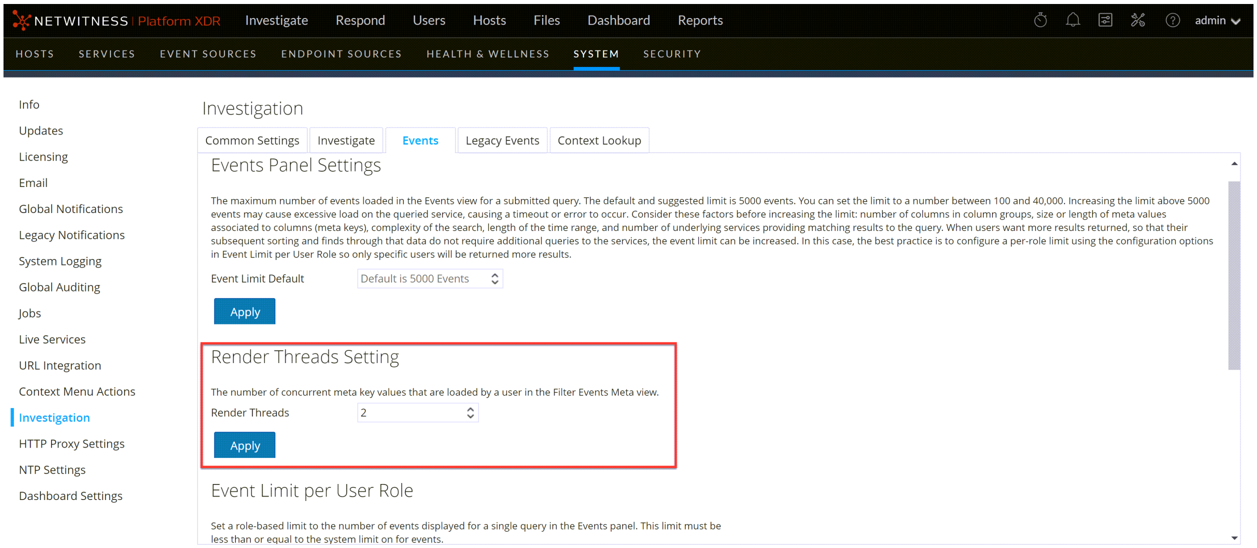
MAX VALUE RESULTS: 100000

MAX META VALUE CHARACTERS: 512

For more information, see **Configure Events View Meta Value Loading Parameters** topic in the *NetWitness Investigate User Guide*.

Render Threads Setting for Events Meta Value

NetWitness now allows analysts to set the Render Threads value under the **System** > **Investigation** > **Events** tab > **Render Threads Setting**. This setting controls the number of concurrent meta key values that are loaded by the user in the Events Meta panel. By increasing the number of render threads, the meta values within the Events Meta panel are loaded concurrently. The Render Threads value should be between 1-8. The default value is 2.



Investigation

Events Panel Settings

The maximum number of events loaded in the Events view for a submitted query. The default and suggested limit is 5000 events. You can set the limit to a number between 100 and 40,000. Increasing the limit above 5000 events may cause excessive load on the queried service, causing a timeout or error to occur. Consider these factors before increasing the limit: number of columns in column groups, size or length of meta values associated to columns (meta keys), complexity of the search, length of the time range, and number of underlying services providing matching results to the query. When users want more results returned, so that their subsequent sorting and finds through that data do not require additional queries to the services, the event limit can be increased. In this case, the best practice is to configure a per-role limit using the configuration options in Event Limit per User Role so only specific users will be returned more results.

Event Limit Default: Default is 5000 Events

Render Threads Setting

The number of concurrent meta key values that are loaded by a user in the Filter Events Meta view.

Render Threads: 2

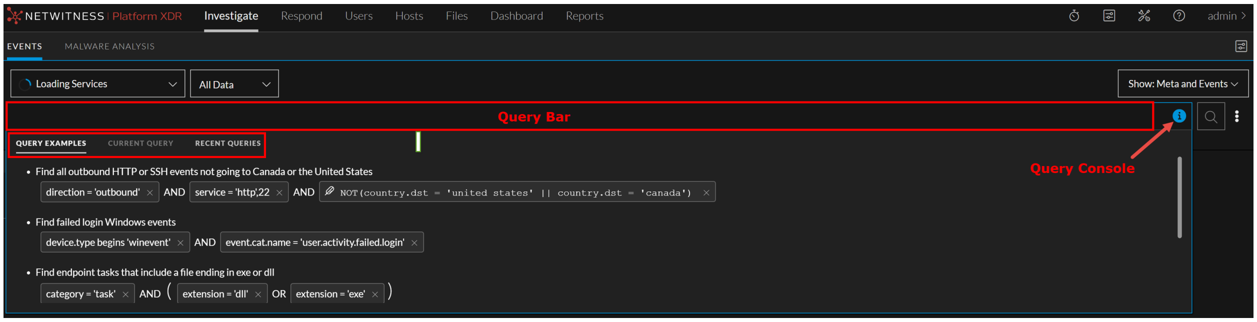
Event Limit per User Role

Set a role-based limit to the number of events displayed for a single query in the Events panel. This limit must be less than or equal to the system limit on for events.

For more information, see the **Configure Events View Settings** topic in the *System Configuration Guide*.

Enhanced Query Console

The **Query Console** has been enhanced to help the analysts with query construction on the **Investigate** > **Events** view. Analysts can now quickly view the Query Examples, Current Query, or Recent Queries on the **Query Console** directly.



- Find all outbound HTTP or SSH events not going to Canada or the United States

  direction = 'outbound' AND service = 'http',22 AND NOT(country.dst = 'united states' || country.dst = 'canada')

- Find failed login Windows events

  device.type begins 'winevent' AND event.cat.name = 'user.activity.failed.login'

- Find endpoint tasks that include a file ending in exe or dll

  category = 'task' AND (extension = 'dll' OR extension = 'exe')

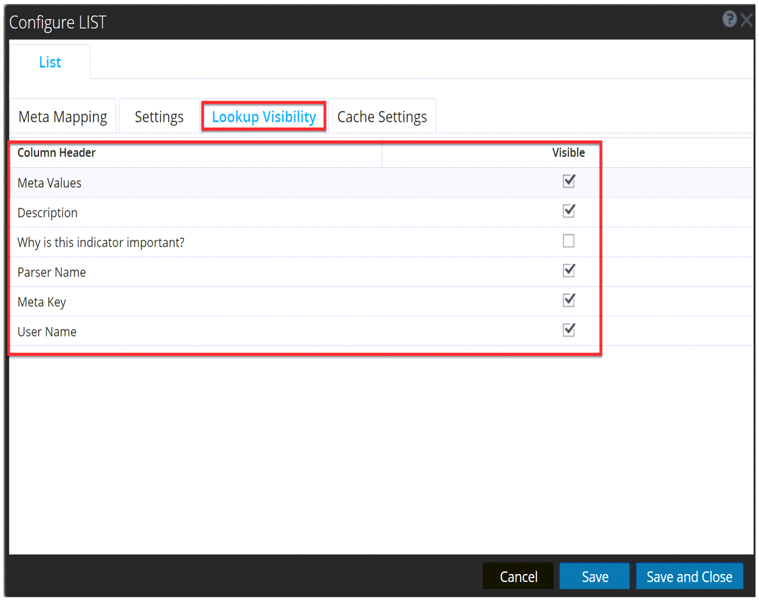
For more information, see **Query Console** topic in the *NetWitness Investigate User Guide*.

Context Hub

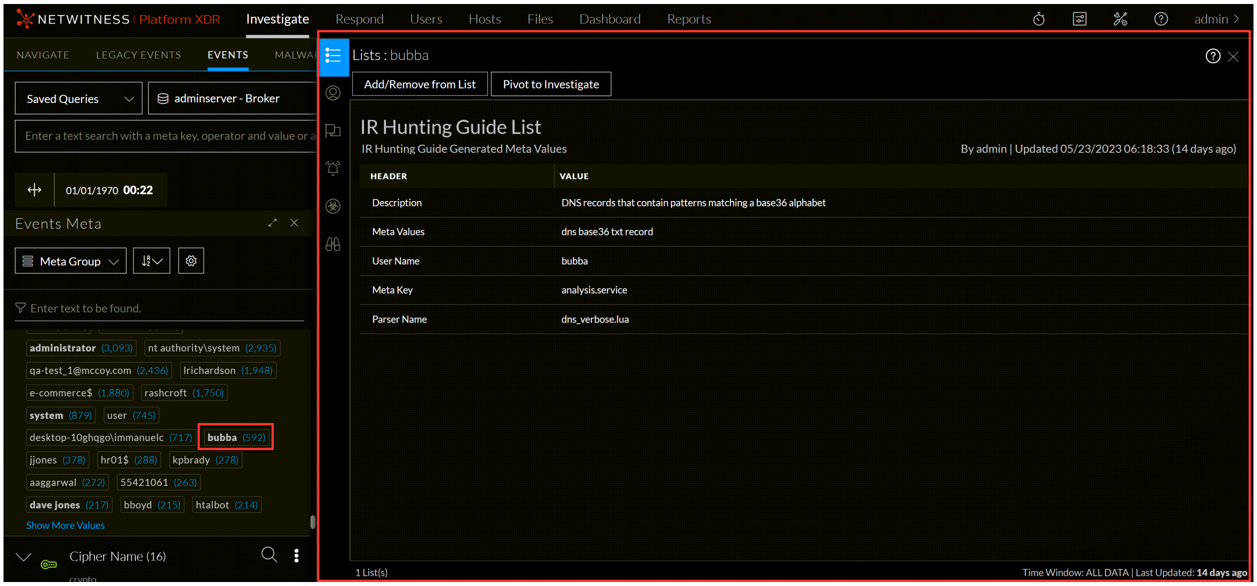
The following section describes the new enhancements for Context Hub component:

Additional Data for Context Lookup Lists Panel

Administrators can now configure additional data of interest from the lists on the Context Hub **Lists** page. These additional details from the lists are reflected in the Context Lookup **Lists** panel when you view the context for an event on the **Events** or **Respond** view. This helps analysts with better visibility for further analysis and investigation.



Column Header	Visible
Meta Values	☑
Description	☑
Why is this indicator important?	□
Parser Name	☑
Meta Key	☑
User Name	☑



IR Hunting Guide List

IR Hunting Guide Generated Meta Values

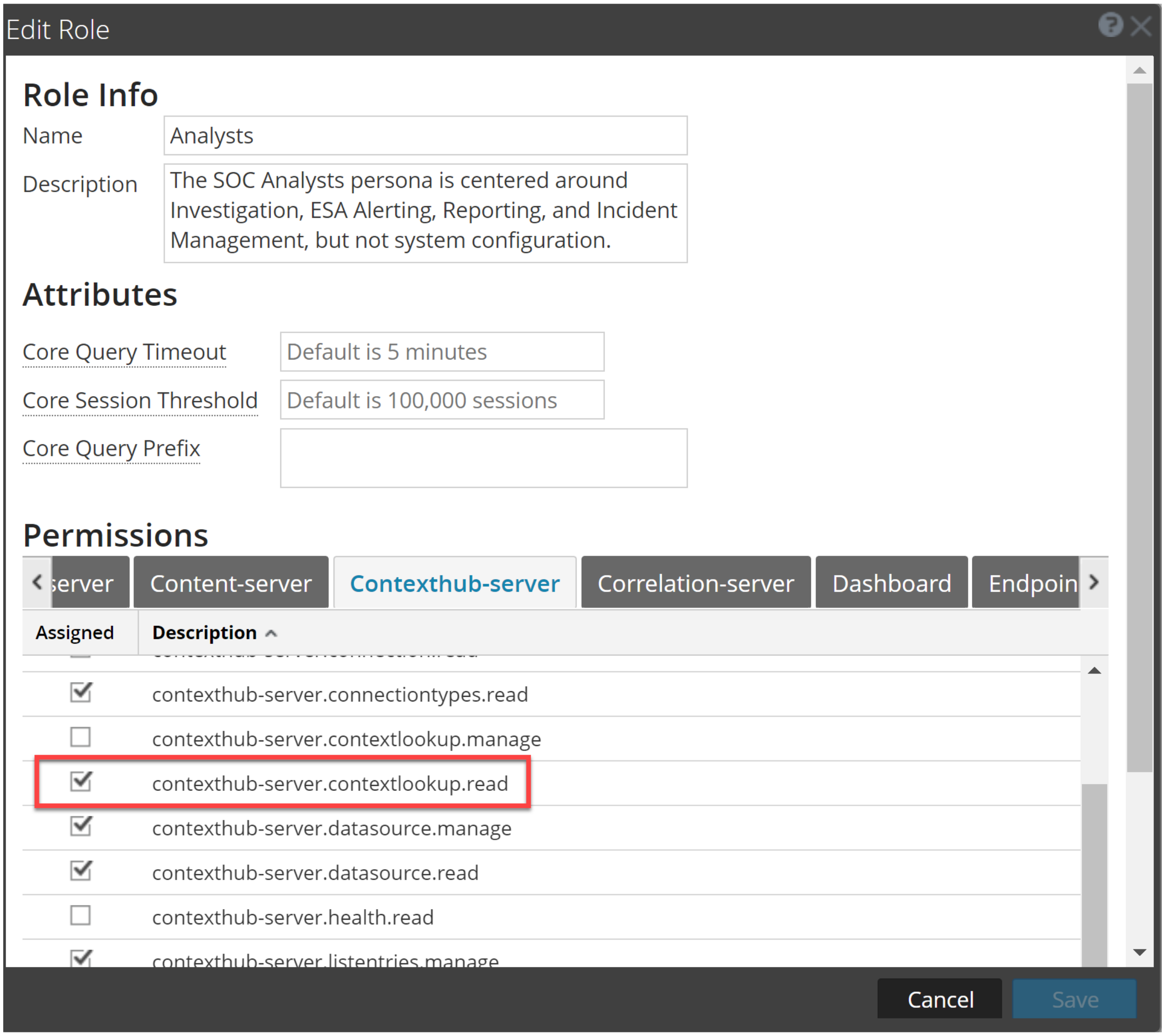
By admin | Updated 05/23/2023 06:18:33 (14 days ago)

HEADER	VALUE
Description	DNS records that contain patterns matching a base36 alphabet
Meta Values	dns base36 txt record
User Name	bubba
Meta Key	analysis.service
Parser Name	dns_verbose.lua

For more information, see the **Manage Meta values for Context Hub Lists** topic in the *Context Hub Configuration Guide*.

New Permission at the Users Level for Context Lookup

NetWitness introduces a new permission named **contexthub-server.contextlookup.read** for Context Lookup. This permission is enabled only for administrators, analysts, malware analysts, SOC managers, and Respond administrators. With this enhancement, administrators can now assign role permissions that prevent users from viewing context enrichment that is not relevant to them or performing the Add/Remove from List actions. Additionally, this can prevent unauthorized users from accessing sensitive information.



Edit Role

Role Info

Name: Analysts

Description: The SOC Analysts persona is centered around Investigation, ESA Alerting, Reporting, and Incident Management, but not system configuration.

Attributes

Core Query Timeout: Default is 5 minutes

Core Session Threshold: Default is 100,000 sessions

Core Query Prefix:

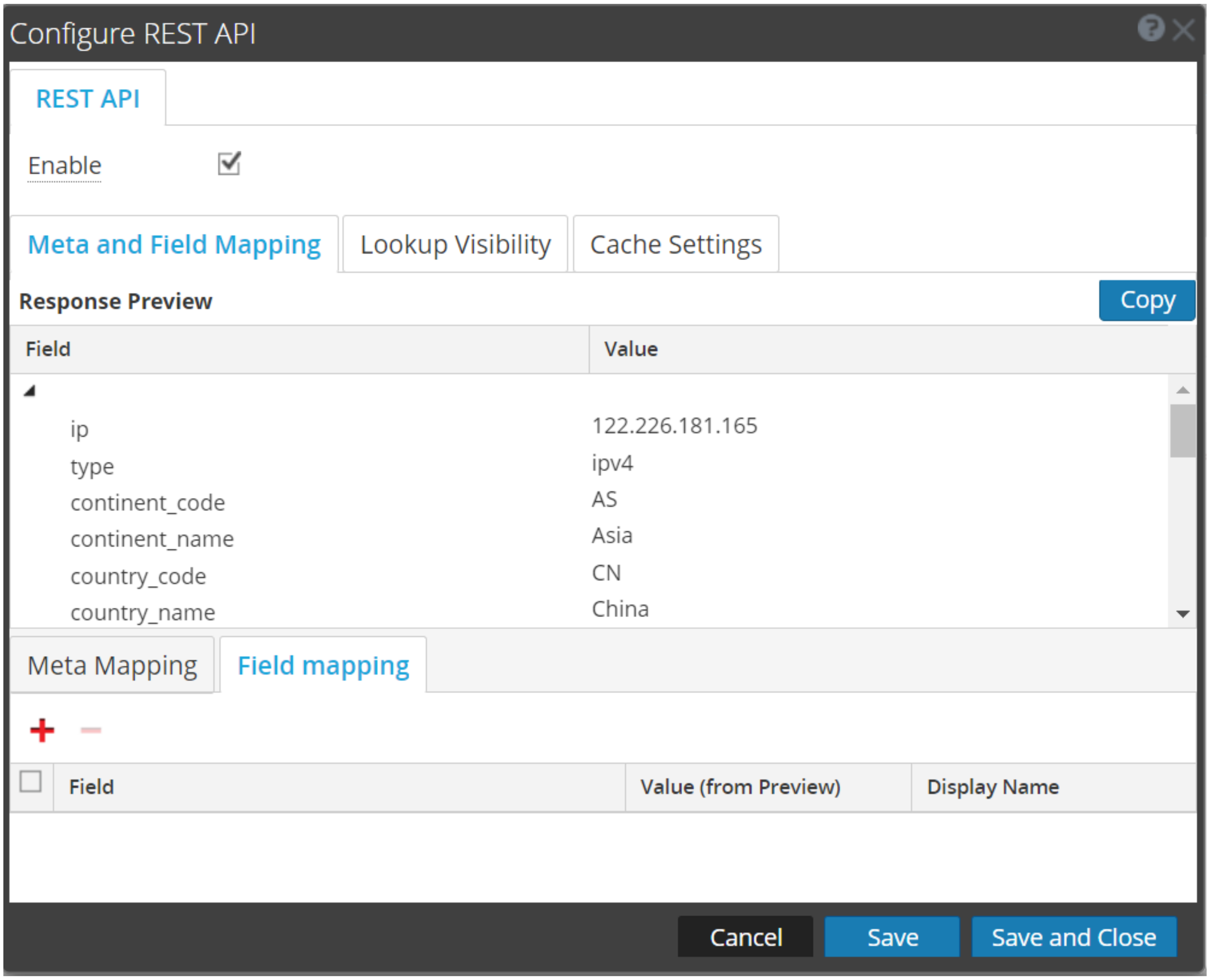
Permissions

Assigned	Description
☑	contexthub-server.connectiontypes.read
□	contexthub-server.contextlookup.manage
☑	contexthub-server.contextlookup.read
☑	contexthub-server.datasource.manage
☑	contexthub-server.datasource.read
□	contexthub-server.health.read
☑	contexthub-server.listentries.manage

For more information, see **Role Permissions** topic in the *System Security and User Management Guide*.

REST API Data Source Enhancements

Administrators can now view the data for Responsive Preview under the **Meta and Field Mapping** and perform **Field mapping** operations for REST API data sources with or without authentication. This enhancement helps administrators to avoid reconfiguring the REST API data source and saves time.



Enable ☑

Response Preview

Field	Value
ip	122.226.181.165
type	ipv4
continent_code	AS
continent_name	Asia
country_code	CN
country_name	China

□	Field	Value (from Preview)	Display Name

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

Insight

Introducing NetWitness Insight

NetWitness Insight is a SaaS solution available as an extension for a NetWitness Network, Detection & Response (NDR) customer. NetWitness Insight is an advanced analytics solution that leverages unsupervised machine learning to empower the response of the Security Operations Center (SOC) team. NetWitness Insight continuously examines network data collected by the Decoder to discover, profile, categorize, characterize, prioritize, and track all assets. NetWitness Insight identifies the assets in the enterprise to alert analysts of their presence. The discovered assets are automatically categorized into groups of similar servers and prioritized based on their network profiles. These assets are presented to analysts in a Springboard panel to guide them to focus on certain assets to protect their organization. Contextual information about the asset is available anywhere analysts interact with IP addresses in **Respond** and **Investigate** workflows. Incidents and alerts can be created based on asset changes.

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

SASE Capability

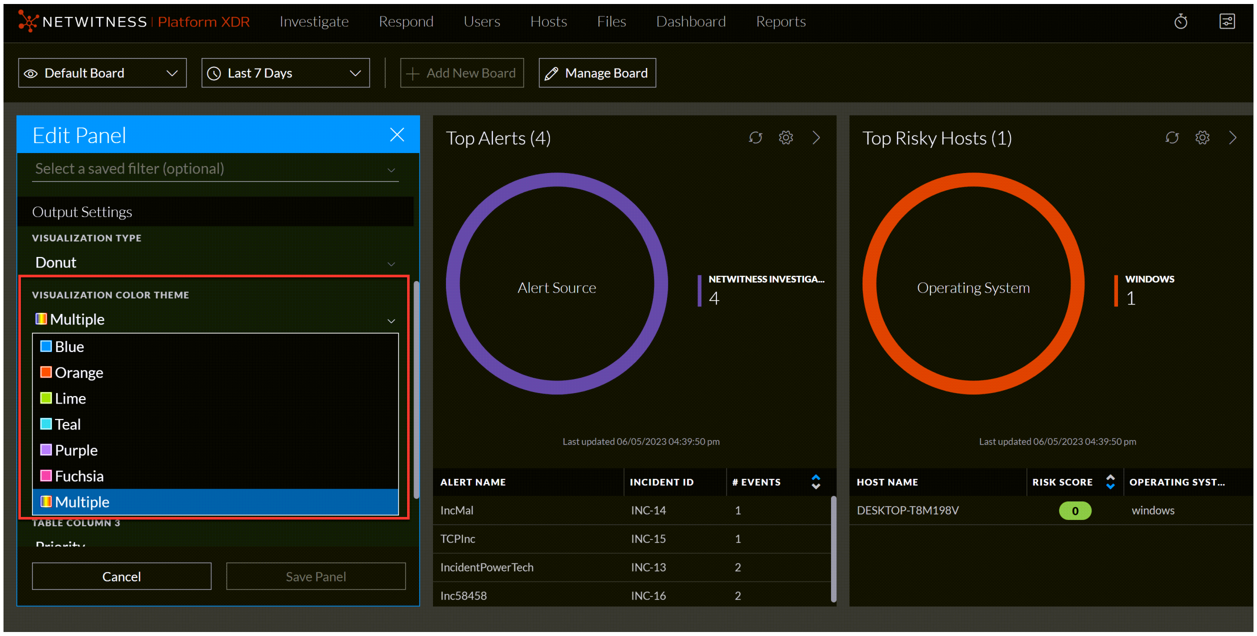
Available in preview mode, this new integration with major SASE vendors provides further network visibility for NetWitness Network (NDR) customers. Previously limited to logs, these integrations deliver original network traffic to NetWitness, providing analysts with deep network visibility and detection for SASE remote communications. Please contact your account representative to get a preview.

Springboard

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

Improved Color Visualization for Springboard Panels

NetWitness Springboard now allows analysts to choose from a variety of color palettes when creating or editing panels using the new **Visualization Color Theme** option. This enhancement gives analysts more control over the appearance of their panels, making them more visually appealing and easier to understand. As a result, analysts can visualize the data better and perform analysis and investigations more efficiently.



VISUALIZATION TYPE
Donut

VISUALIZATION COLOR THEME
Multiple

NETWITNESS INVESTIGA...
4

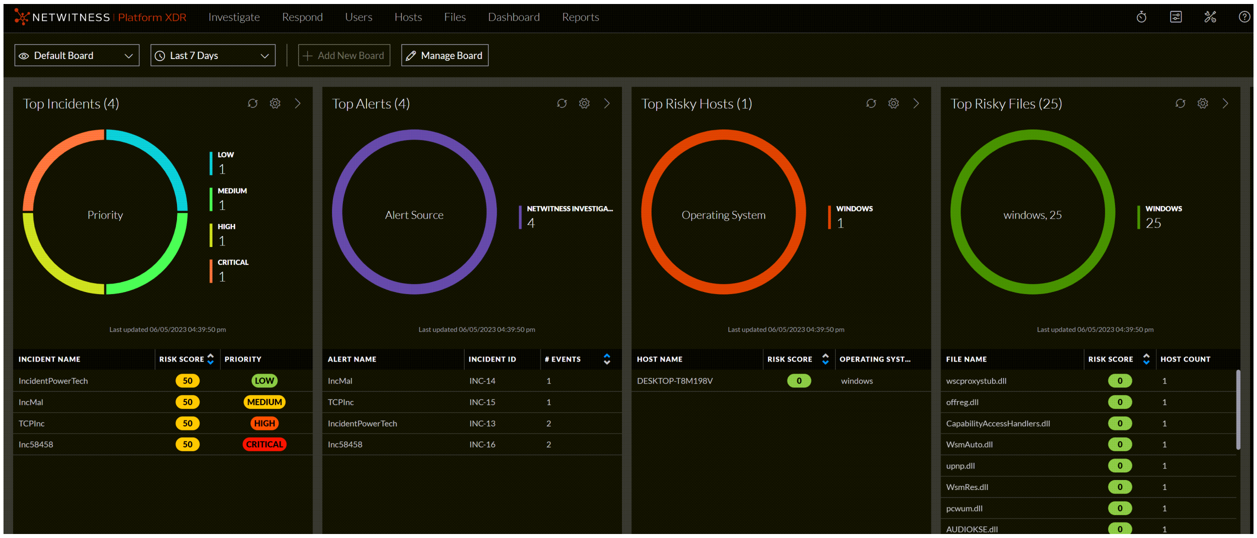
Last updated 06/05/2023 04:39:50 pm

ALERT NAME	INCIDENT ID	# EVENTS
IncMal	INC-14	1
TCPInc	INC-15	1
IncidentPowerTech	INC-13	2
Inc58458	INC-16	2

WINDOWS
1

Last updated 06/05/2023 04:39:50 pm

HOST NAME	RISK SCORE	OPERATING SYST...
DESKTOP-T8M198V	0	windows



INCIDENT NAME	RISK SCORE	PRIORITY
IncidentPowerTech	50	LOW
IncMal	50	MEDIUM
TCPInc	50	HIGH
Inc58458	50	CRITICAL

ALERT NAME	INCIDENT ID	# EVENTS
IncMal	INC-14	1
TCPInc	INC-15	1
IncidentPowerTech	INC-13	2
Inc58458	INC-16	2

HOST NAME	RISK SCORE	OPERATING SYST...
DESKTOP-T8M198V	0	windows

FILE NAME	RISK SCORE	HOST COUNT
wscproxystub.dll	0	1
offreg.dll	0	1
CapabilityAccessHandlers.dll	0	1
WsmAuto.dll	0	1
upnp.dll	0	1
WsmRes.dll	0	1
pcwum.dll	0	1
AUDIOKSE.dll	0	1

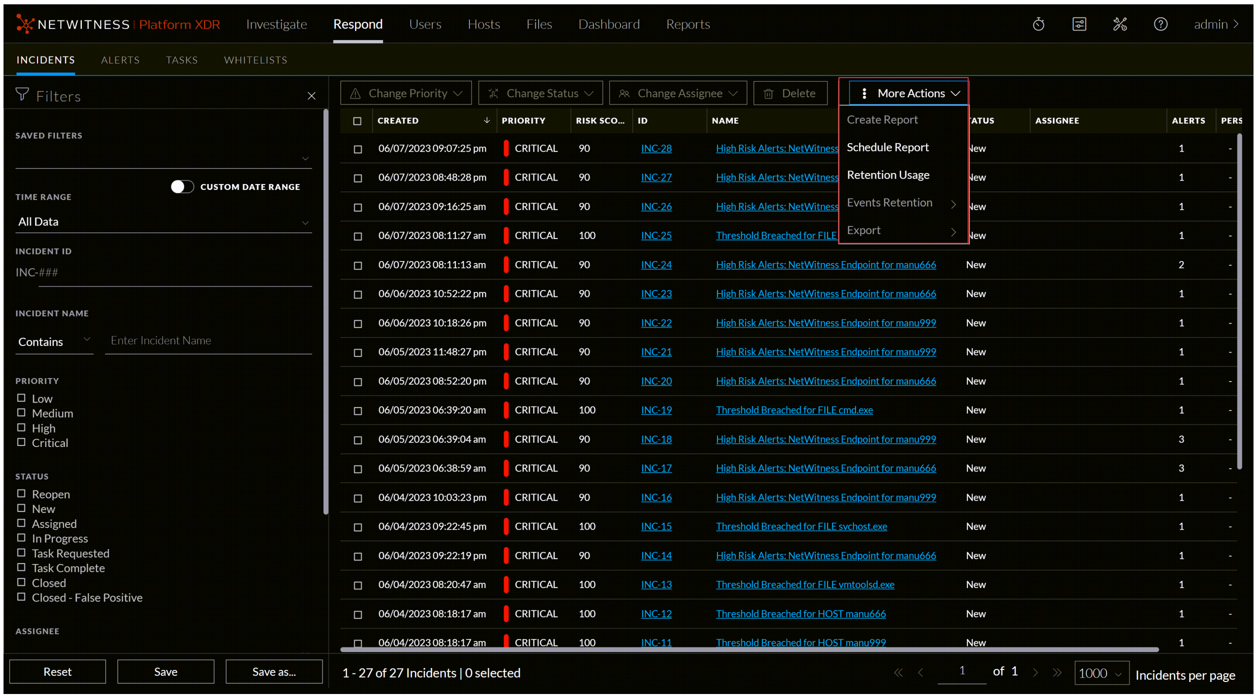
For more information, see **Managing the Springboard** topic in the *NetWitness Getting Started Guide*.

Respond

NetWitness latest enhancements to reporting capabilities in **Respond** view provide users with increased flexibility and streamlined workflows. These improvements address the challenges you face during investigation and reporting. The following enhancements are made to the **Respond** component.

Respond Reporting Enhancements

With the new upgrades to **Respond** reporting, administrators and analysts can efficiently capture, analyze, and share their findings with management, resulting in enhanced reporting experience within NetWitness.



SAVED FILTERS

TIME RANGE

All Data

CUSTOM DATE RANGE

INCIDENT ID

INC-###

INCIDENT NAME

Contains

Enter Incident Name

PRIORITY

- □ Low
- □ Medium
- □ High
- □ Critical

STATUS

- □ Reopen
- □ New
- □ Assigned
- □ In Progress
- □ Task Requested
- □ Task Complete
- □ Closed
- □ Closed - False Positive

ASSIGNEE

□	CREATED	PRIORITY	RISK SCO...	ID	NAME	ATUS	ASSIGNEE	ALERTS	PERS
□	06/07/2023 09:07:25 pm	CRITICAL	90	INC-28	High Risk Alerts: NetWitness	New		1	-
□	06/07/2023 08:48:28 pm	CRITICAL	90	INC-27	High Risk Alerts: NetWitness	New		1	-
□	06/07/2023 09:16:25 am	CRITICAL	90	INC-26	High Risk Alerts: NetWitness	New		1	-
□	06/07/2023 08:11:27 am	CRITICAL	100	INC-25	Threshold Breached for FILE	New		1	-
□	06/07/2023 08:11:13 am	CRITICAL	90	INC-24	High Risk Alerts: NetWitness Endpoint for manu666	New		2	-
□	06/06/2023 10:52:22 pm	CRITICAL	90	INC-23	High Risk Alerts: NetWitness Endpoint for manu666	New		1	-
□	06/06/2023 10:18:26 pm	CRITICAL	90	INC-22	High Risk Alerts: NetWitness Endpoint for manu999	New		1	-
□	06/05/2023 11:48:27 pm	CRITICAL	90	INC-21	High Risk Alerts: NetWitness Endpoint for manu999	New		1	-
□	06/05/2023 08:52:20 pm	CRITICAL	90	INC-20	High Risk Alerts: NetWitness Endpoint for manu666	New		1	-
□	06/05/2023 06:39:20 am	CRITICAL	100	INC-19	Threshold Breached for FILE cmd.exe	New		1	-
□	06/05/2023 06:39:04 am	CRITICAL	90	INC-18	High Risk Alerts: NetWitness Endpoint for manu999	New		3	-
□	06/05/2023 06:38:59 am	CRITICAL	90	INC-17	High Risk Alerts: NetWitness Endpoint for manu666	New		3	-
□	06/04/2023 10:03:23 pm	CRITICAL	90	INC-16	High Risk Alerts: NetWitness Endpoint for manu999	New		1	-
□	06/04/2023 09:22:45 pm	CRITICAL	100	INC-15	Threshold Breached for FILE svchost.exe	New		1	-
□	06/04/2023 09:22:19 pm	CRITICAL	90	INC-14	High Risk Alerts: NetWitness Endpoint for manu666	New		1	-
□	06/04/2023 08:20:47 am	CRITICAL	100	INC-13	Threshold Breached for FILE vmtoolsd.exe	New		1	-
□	06/04/2023 08:18:17 am	CRITICAL	100	INC-12	Threshold Breached for HOST manu666	New		1	-
□	06/04/2023 08:18:17 am	CRITICAL	100	INC-11	Threshold Breached for HOST manu999	New		1	-

1 - 27 of 27 Incidents | 0 selected

1 of 1 1000 Incidents per page

- Integrated reporting capabilities into the events and respond views allow administrators and analysts to seamlessly tie their investigations to reports to capture and report their findings to the management.
- Users can review incidents and alerts within the **Respond** view and generate comprehensive reports directly from the interface. Analysts and administrators can document their analysis and share detailed reports with stakeholders.
- Reports generated from the **Respond** view now leverage the powerful filtering capabilities available within **Respond**, ensuring that the reports accurately reflect the specific incidents or alerts reviewed.
- Introduced a simplified workflow driven by customizable templates, this feature eliminates the complexity of the current reporting workflow and reduces the input required from analysts and administrators.
- Report creation now defaults to preconfigured settings, minimizing the need for manual configuration and expediting the reporting process.
- Analysts can now email the generated reports directly to administrators or other analysts, facilitating efficient communication and collaboration.

For more information, see the **Generate Reports from Respond View** topic in the NetWitness Respond User Guide.

Respond Server Support for Core Alerts and Insight Alerts

The Respond Server support for **NetWitness Core Alerts** and **NetWitness Insight Alerts** update improves your security by helping you detect and respond to incidents more effectively. This includes improvements that make managing and analyzing core and insight alerts within the NetWitness platform easier.

- **Normalisation Support:** We have added support for normalizing these alerts, enabling the detection of suspicious logs and network traffic patterns. This enhancement helps you proactively identify potential security threats and take swift action.

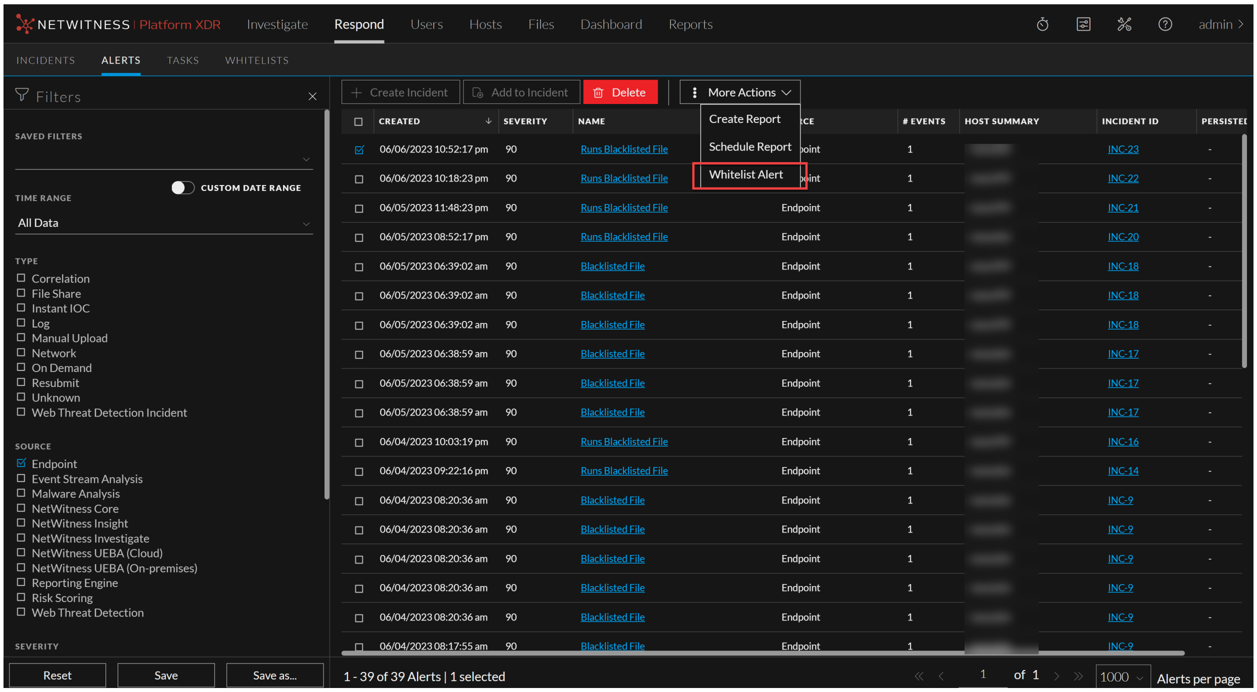
- **Filtering Support:** Improved the filtering on alerts, providing a more detailed and comprehensive view empowering you to make faster and more informed decisions.

- **OOTB Incident Aggregation Rule for Core Alerts and Insight Alerts:**To simplify incident response, we have included an Out-of-the-Box (OOTB) incident aggregation rule specifically designed for core alerts and insight alerts. This rule automates grouping related core alerts and insight alerts into a single incident, streamlining your incident management process and saving valuable time.

For more information, see the **Respond Server Support** topic in the NetWitness Respond User Guide.

Alerts View Enhancements

The **Respond** > **Alerts** view is enhanced with the **Whitelist Alert** feature to help administrators and analysts whitelist the non-suspicious Endpoint alerts. You can select the entities such as File, User, and Host and define the Whitelist condition to avoid triggering of the unwanted alerts for the required entities.



TIME RANGE
All Data

TYPE
- □ Correlation
- □ File Share
- □ Instant IOC
- □ Log
- □ Manual Upload
- □ Network
- □ On Demand
- □ Resubmit
- □ Unknown
- □ Web Threat Detection Incident

SOURCE
- ☑ Endpoint
- □ Event Stream Analysis
- □ Malware Analysis
- □ NetWitness Core
- □ NetWitness Insight
- □ NetWitness Investigate
- □ NetWitness UEBA (Cloud)
- □ NetWitness UEBA (On-premises)
- □ Reporting Engine
- □ Risk Scoring
- □ Web Threat Detection

SEVERITY

□	CREATED	SEVERITY	NAME	CE	# EVENTS	HOST SUMMARY	INCIDENT ID	PERSISTED
☑	06/06/2023 10:52:17 pm	90	Runs Blacklisted File	oint	1	[redacted]	INC-23	-
□	06/06/2023 10:18:23 pm	90	Runs Blacklisted File	oint	1	[redacted]	INC-22	-
□	06/05/2023 11:48:23 pm	90	Runs Blacklisted File	Endpoint	1	[redacted]	INC-21	-
□	06/05/2023 08:52:17 pm	90	Runs Blacklisted File	Endpoint	1	[redacted]	INC-20	-
□	06/05/2023 06:39:02 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-18	-
□	06/05/2023 06:39:02 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-18	-
□	06/05/2023 06:39:02 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-18	-
□	06/05/2023 06:38:59 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-17	-
□	06/05/2023 06:38:59 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-17	-
□	06/05/2023 06:38:59 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-17	-
□	06/04/2023 10:03:19 pm	90	Runs Blacklisted File	Endpoint	1	[redacted]	INC-16	-
□	06/04/2023 09:22:16 pm	90	Runs Blacklisted File	Endpoint	1	[redacted]	INC-14	-
□	06/04/2023 08:20:36 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-9	-
□	06/04/2023 08:20:36 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-9	-
□	06/04/2023 08:20:36 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-9	-
□	06/04/2023 08:20:36 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-9	-
□	06/04/2023 08:20:36 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-9	-
□	06/04/2023 08:17:55 am	90	Blacklisted File	Endpoint	1	[redacted]	INC-9	-

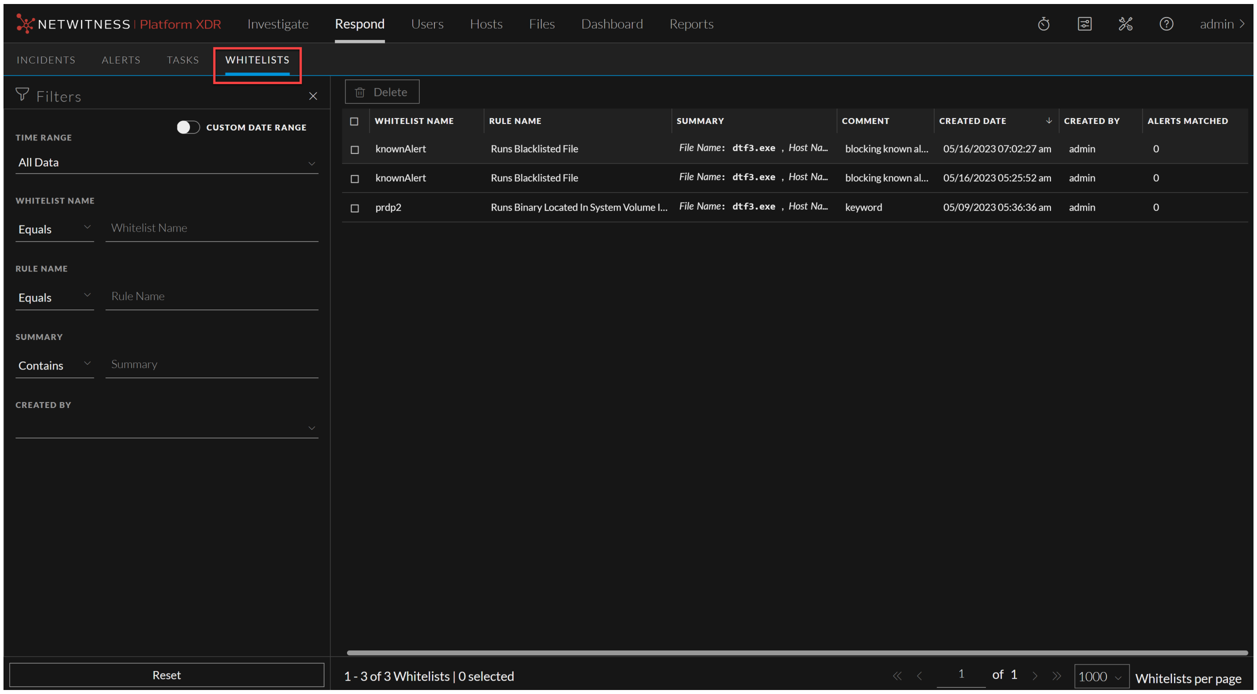
1 - 39 of 39 Alerts | 1 selected

1 of 1 | 1000 Alerts per page

For more information, see **Whitelist Endpoint Alerts** topic in the NetWitness Respond User Guide.

Respond View Enhancements

The new **Whitelists** tab added in the **Respond** view enables you to view and manage the Endpoint Whitelists created after whitelisting the non-suspicious Endpoint alerts.



TIME RANGE
All Data

WHITELIST NAME
Equals | Whitelist Name

RULE NAME
Equals | Rule Name

SUMMARY
Contains | Summary

CREATED BY

□	WHITELIST NAME	RULE NAME	SUMMARY	COMMENT	CREATED DATE	CREATED BY	ALERTS MATCHED
□	knownAlert	Runs Blacklisted File	*File Name*: `dtf3.exe` , *Host Na...*	blocking known al...	05/16/2023 07:02:27 am	admin	0
□	knownAlert	Runs Blacklisted File	*File Name*: `dtf3.exe` , *Host Na...*	blocking known al...	05/16/2023 05:25:52 am	admin	0
□	prdp2	Runs Binary Located In System Volume I...	*File Name*: `dtf3.exe` , *Host Na...*	keyword	05/09/2023 05:36:36 am	admin	0

1 - 3 of 3 Whitelists | 0 selected

1 of 1 | 1000 Whitelists per page

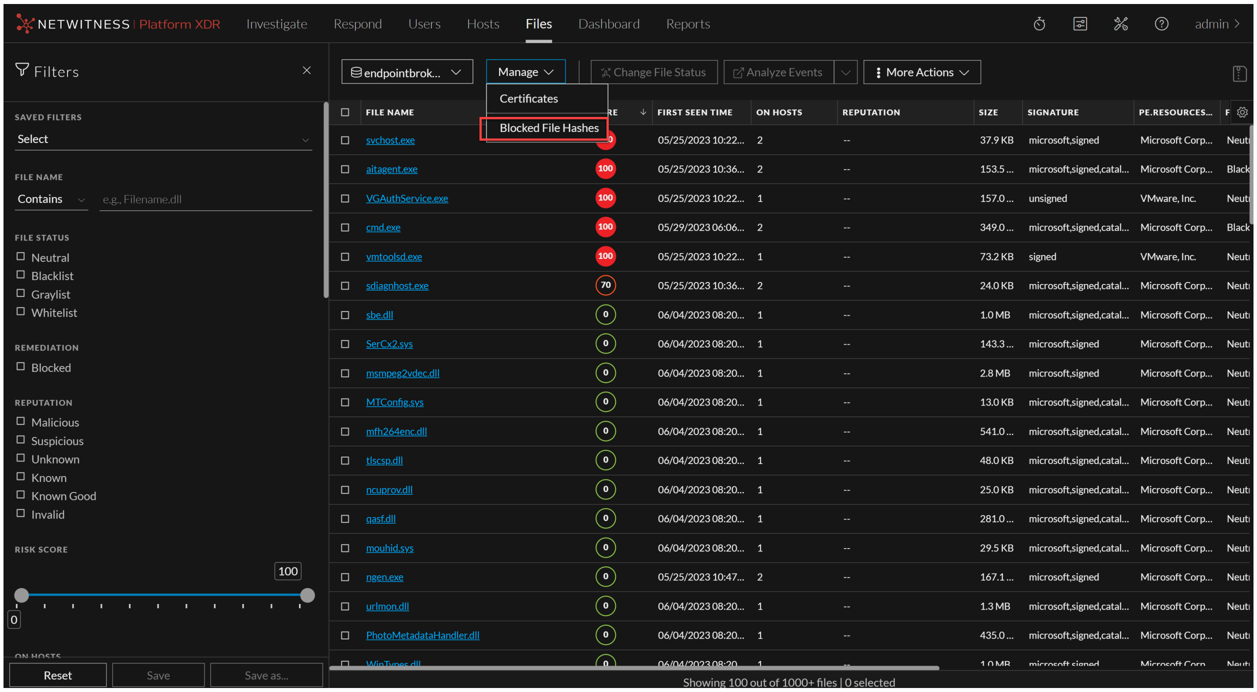
For more information, see **Whitelist Endpoint Alerts** topic in the NetWitness Respond User Guide.

Endpoint Enhancements

The following section describes the new enhancements for Endpoint component:

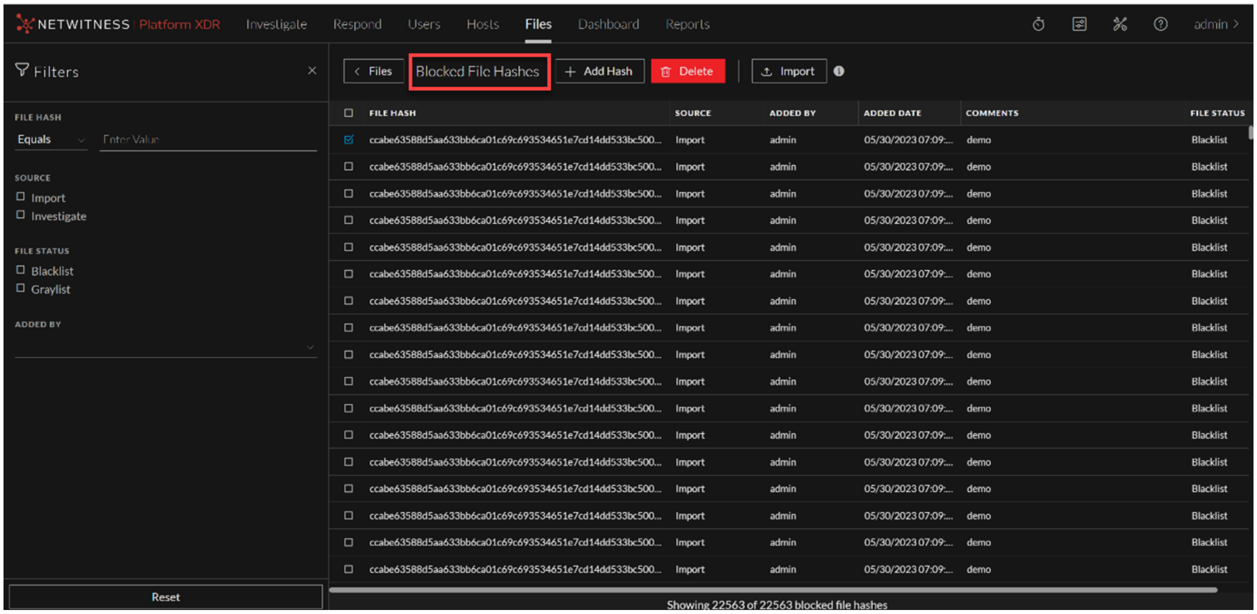
Files View Enhancements

The **Files** view is enhanced to help administrators and analysts block the new file hashes and manage the existing blocked file hashes. You can block up to a maximum of 50,000 file hashes using this feature.



☐	FILE NAME	RE	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES...	F
☐	svchost.exe	0	05/25/2023 10:22...	2	--	37.9 KB	microsoft,signed	Microsoft Corp...	Neut
☐	aitagent.exe	100	05/25/2023 10:36...	2	--	153.5 ...	microsoft,signed,catal...	Microsoft Corp...	Black
☐	VGAuthService.exe	100	05/25/2023 10:22...	1	--	157.0 ...	unsigned	VMware, Inc.	Neut
☐	cmd.exe	100	05/29/2023 06:06...	2	--	349.0 ...	microsoft,signed,catal...	Microsoft Corp...	Black
☐	vmtoolsd.exe	100	05/25/2023 10:22...	1	--	73.2 KB	signed	VMware, Inc.	Neut
☐	sdiagnhost.exe	70	05/25/2023 10:36...	2	--	24.0 KB	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	sbe.dll	0	06/04/2023 08:20...	1	--	1.0 MB	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	SerCx2.sys	0	06/04/2023 08:20...	1	--	143.3 ...	microsoft,signed	Microsoft Corp...	Neut
☐	msmpeg2vdec.dll	0	06/04/2023 08:20...	1	--	2.8 MB	microsoft,signed	Microsoft Corp...	Neut
☐	MTConfig.sys	0	06/04/2023 08:20...	1	--	13.0 KB	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	mfh264enc.dll	0	06/04/2023 08:20...	1	--	541.0 ...	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	tlscsp.dll	0	06/04/2023 08:20...	1	--	48.0 KB	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	ncuprov.dll	0	06/04/2023 08:20...	1	--	25.0 KB	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	qasf.dll	0	06/04/2023 08:20...	1	--	281.0 ...	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	mouhid.sys	0	06/04/2023 08:20...	1	--	29.5 KB	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	ngen.exe	0	05/25/2023 10:47...	2	--	167.1 ...	microsoft,signed	Microsoft Corp...	Neut
☐	urlmon.dll	0	06/04/2023 08:20...	1	--	1.3 MB	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	PhotoMetadataHandler.dll	0	06/04/2023 08:20...	1	--	435.0 ...	microsoft,signed,catal...	Microsoft Corp...	Neut
☐	WinTypes.dll	0	06/04/2023 08:20...	1	--	1.0 MB	microsoft,signed	Microsoft Corp...	Neut

Showing 100 out of 1000+ files | 0 selected



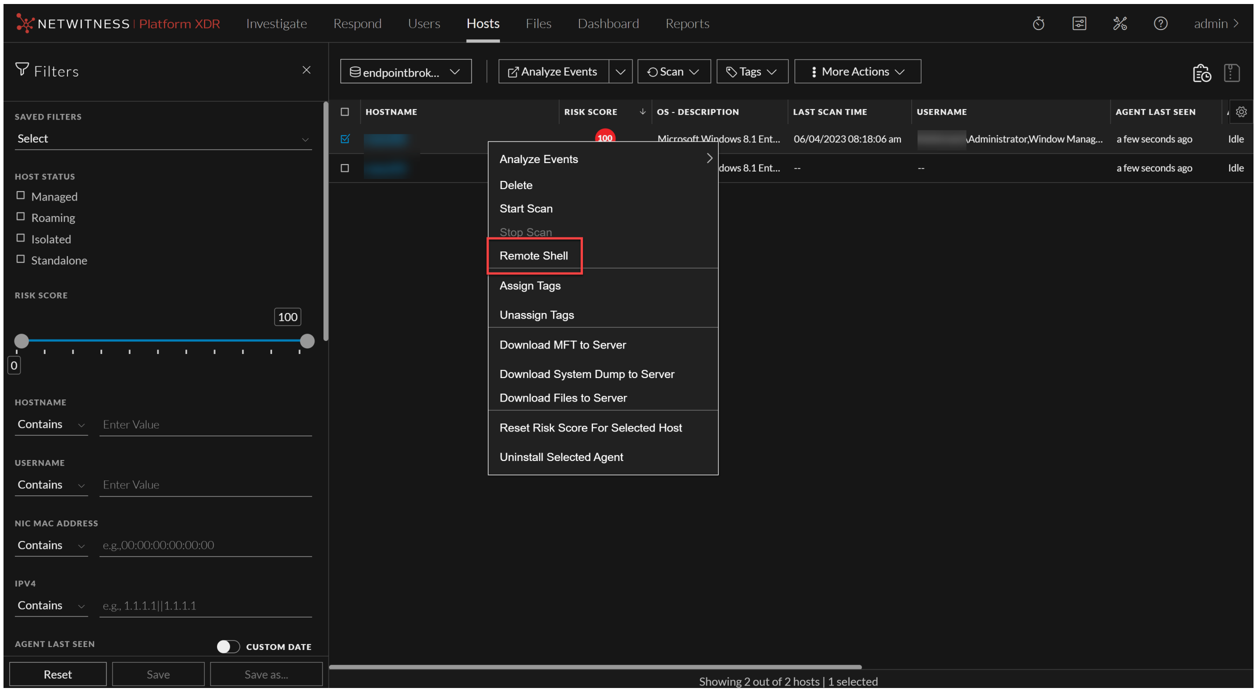
☐	FILE HASH	SOURCE	ADDED BY	ADDED DATE	COMMENTS	FILE STATUS
☑	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist
☐	ccabe63588d5aa633bb6ca01c69c693534651e7cd14dd533bc500...	Import	admin	05/30/2023 07:09:...	demo	Blacklist

Showing 22563 of 22563 blocked file hashes

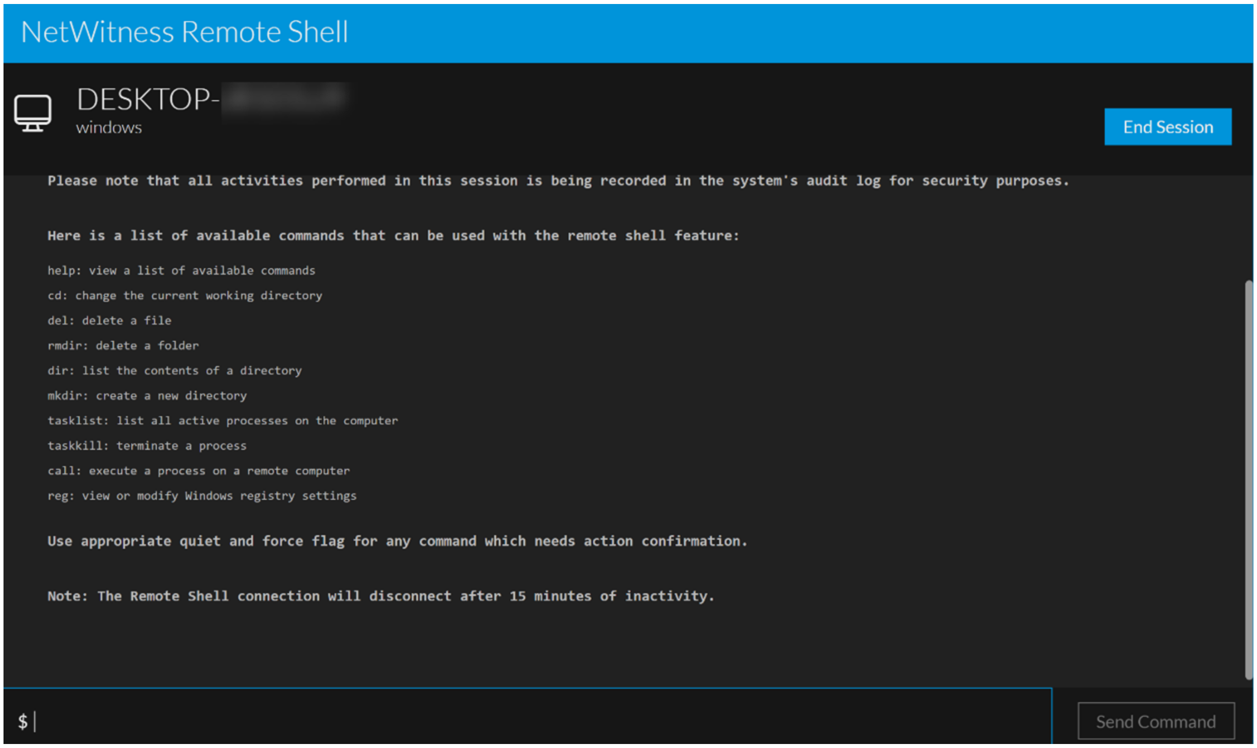
For more information, see **Manage Blocked File Hashes** topic in the NetWitness Endpoint User Guide.

Hosts View Enhancements

The **Hosts** view is enhanced with the **Remote Shell** feature to help administrators and analysts access the remote agents and perform remediation actions during investigation. You can execute the commands only in the quiet mode.



	HOSTNAME	RISK SCORE	OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	
☑	[redacted]	100	Microsoft Windows 8.1 Ent...	06/04/2023 08:18:06 am	[redacted]\Administrator,Window Manag...	a few seconds ago	Idle
□	[redacted]		dows 8.1 Ent...	--	--	a few seconds ago	Idle



```
Please note that all activities performed in this session is being recorded in the system's audit log for security purposes.

Here is a list of available commands that can be used with the remote shell feature:

help: view a list of available commands
cd: change the current working directory
del: delete a file
rmdir: delete a folder
dir: list the contents of a directory
mkdir: create a new directory
tasklist: list all active processes on the computer
taskkill: terminate a process
call: execute a process on a remote computer
reg: view or modify Windows registry settings

Use appropriate quiet and force flag for any command which needs action confirmation.

Note: The Remote Shell connection will disconnect after 15 minutes of inactivity.

$ |
```

For more information, see **Remote Shell** topic in the NetWitness Endpoint User Guide.

Advanced Linux Agent - File Event Tracking Enhancement

Linux Agent - File Event Tracking is introduced to help analysts view the file related activities by an executable, such as `writetoexecutable`. Analysts can view and monitor file events to detect threats on Linux machines.

For more information, see **Introduction to Endpoint Investigation** topic in the NetWitness Endpoint User Guide.

File Log Collection Enhancement

NetWitness Platform XDR supports collection of **MicrosoftIIS** logs. You can select **MicrosoftIIS** from the **Log File Type** drop-down list in **(Admin)** > **Endpoint Sources** > **Policies** > **Define File Policy Settings** to collect and monitor **MicrosoftIIS** file logs.

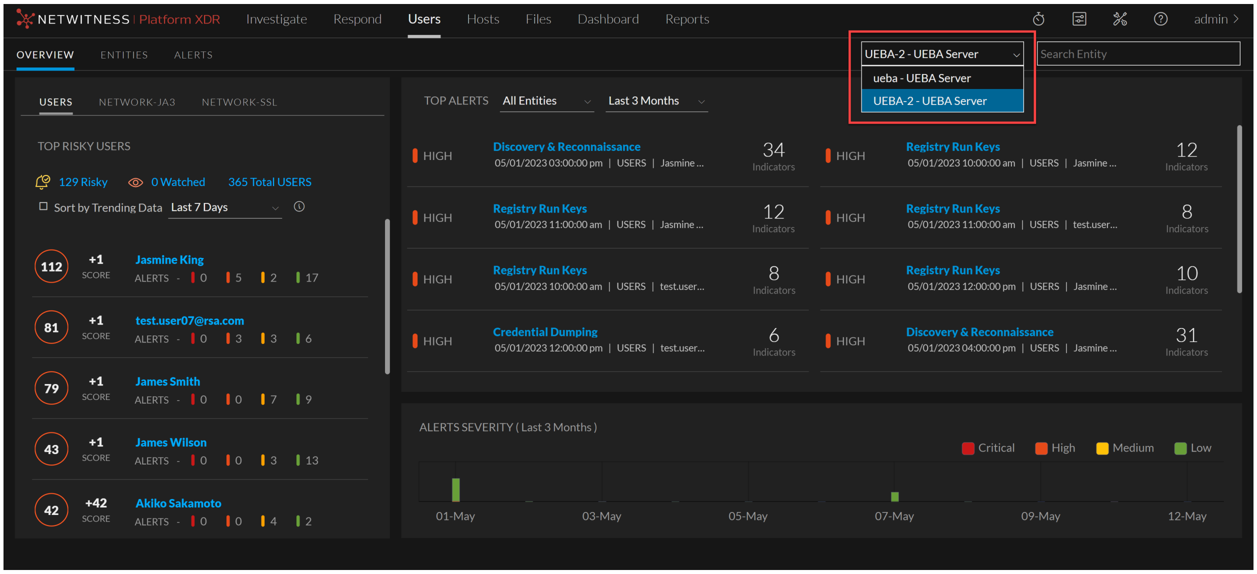
For more information, see **Appendices** topic in the NetWitness Endpoint Configuration Guide.

User and Entity Behavior Analytics

The following section describes the new enhancements for UEBA component:

Enhanced Configuration Support for Multiple UEBA Servers

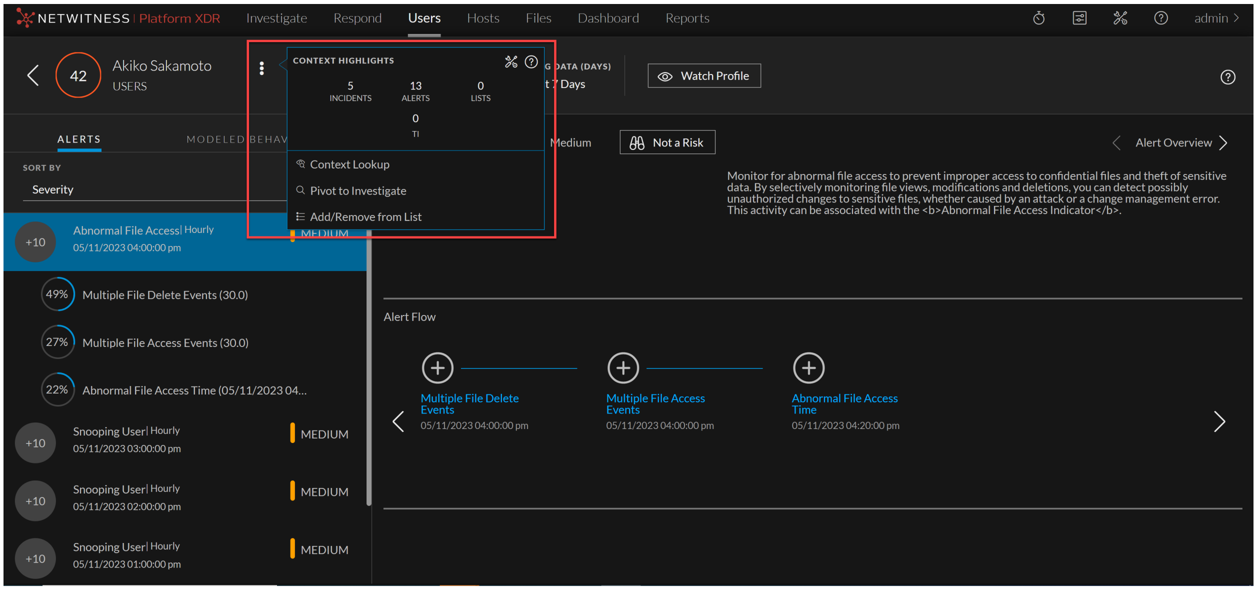
NetWitness introduces the ability to deploy multiple UEBA servers in your environment, providing increased flexibility and control. With this enhancement, administrators can distribute the UEBA server deployment across dedicated servers, such as one server for Logs and Endpoint data and another for Network (TLS) data. This data segregation ensures that each server can focus on its designated data type, resulting in faster and more streamlined processing. With the data segregation, analysts can now select the specific data type using the drop-down option provided for Multiple UEBA servers. This feature helps analysts to focus on the relevant users, network entities, and alerts associated with each UEBA server.


NETWITNESS | Platform XDR
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
OVERVIEW
ENTITIES
ALERTS
UEBA-2 - UEBA Server
ueba - UEBA Server
UEBA-2 - UEBA Server
Search Entity
USERS
NETWORK-JA3
NETWORK-SSL
TOP RISKY USERS
129 Risky
0 Watched
365 Total USERS
Sort by Trending Data
Last 7 Days
112 +1 SCORE Jasmine King ALERTS - 0 5 2 17
81 +1 SCORE test.user07@rsa.com ALERTS - 0 3 3 6
79 +1 SCORE James Smith ALERTS - 0 0 7 9
43 +1 SCORE James Wilson ALERTS - 0 0 3 13
42 +42 SCORE Akiko Sakamoto ALERTS - 0 0 4 2
TOP ALERTS
All Entities
Last 3 Months
HIGH Discovery & Reconnaissance 05/01/2023 03:00:00 pm | USERS | Jasmine ... 34 Indicators
HIGH Registry Run Keys 05/01/2023 10:00:00 am | USERS | Jasmine ... 12 Indicators
HIGH Registry Run Keys 05/01/2023 11:00:00 am | USERS | Jasmine ... 12 Indicators
HIGH Registry Run Keys 05/01/2023 11:00:00 am | USERS | test.user... 8 Indicators
HIGH Registry Run Keys 05/01/2023 10:00:00 am | USERS | test.user... 8 Indicators
HIGH Registry Run Keys 05/01/2023 12:00:00 pm | USERS | Jasmine ... 10 Indicators
HIGH Credential Dumping 05/01/2023 12:00:00 pm | USERS | test.user... 6 Indicators
HIGH Discovery & Reconnaissance 05/01/2023 04:00:00 pm | USERS | Jasmine ... 31 Indicators
ALERTS SEVERITY (Last 3 Months)
Critical
High
Medium
Low
01-May
03-May
05-May
07-May
09-May
12-May

For more information, see the **Configure Multiple UEBA Servers** topic in the *NetWitness UEBA Configuration Guide*.

Introducing Contextual Information for Users

Analysts can now view contextual information about users on the NetWitness **Users** page. This enhancement enables analysts to make better decisions and take appropriate actions. A single place contains contextual information about users to help analysts identify and prioritize areas of investigation. The **Context Highlights** panel enables analysts to view contextual information for selected users, including total Respond alerts and incidents associated with them. Moreover, analysts can also switch to the **Investigate** view for a deeper look at users for focused analysis and investigation.



Monitor for abnormal file access to prevent improper access to confidential files and theft of sensitive data. By selectively monitoring file views, modifications and deletions, you can detect possibly unauthorized changes to sensitive files, whether caused by an attack or a change management error. This activity can be associated with the <b>Abnormal File Access Indicator</b>.

For more information, see the **View Contextual Information for Users** topic in the *NetWitness UEBA Users Guide*.

UEBA Performance Improvement

NetWitness UEBA (On-premises) has been enhanced to improve the performance of its data processing capabilities by updating the adaptor task and effectively allocating available free memory on UEBA services. This results in faster processing time and better performance for all UEBA tasks.

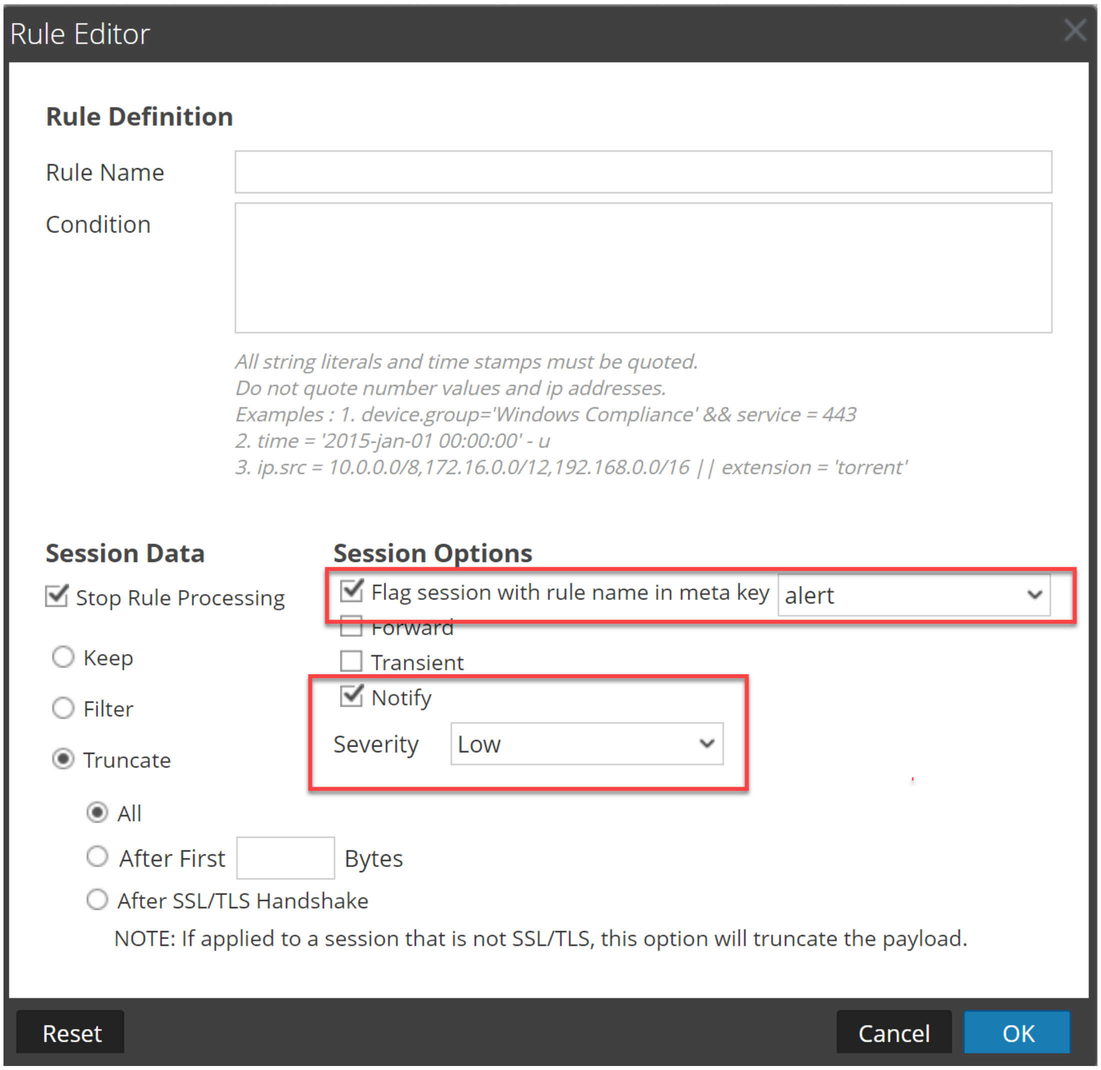
For more information on the supported scale, see the **Learning Period Per Scale for 12.3** topic in the *UEBA Configuration Guide*.

Concentrator, Decoder, and Log Decoder Services

Application Rule Enhancements

NetWitness has enhanced the Application Rules to help administrators manage the rules efficiently by adding the following improvements:

- Under Session Options, the option **Alert on** is renamed to **Flag session with rule name in meta key** in the Application Rule tab. With this enhancement, administrators can now select a custom meta key from the drop-down, and a meta value corresponding to the rule name will be generated when the session metadata matches the rule.
- Administrators can now select the **Notify** option to trigger alert generation and choose the **Severity** level while creating or modifying the Application Rules. The severity levels are **Critical**, **High**, **Medium**, and **Low**.



Rule Editor

Rule Definition

Rule Name

Condition

All string literals and time stamps must be quoted.
Do not quote number values and ip addresses.
Examples : 1. device.group='Windows Compliance' && service = 443
2. time = '2015-jan-01 00:00:00' - u
3. ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 || extension = 'torrent'

Session Data

☑ Stop Rule Processing

○ Keep
○ Filter
● Truncate
● All
○ After First Bytes
○ After SSL/TLS Handshake

NOTE: If applied to a session that is not SSL/TLS, this option will truncate the payload.

Session Options

☑ Flag session with rule name in meta key: alert
□ Forward
□ Transient
☑ Notify
Severity: Low

For more information, see the **Configure Application Rules** topic in the *Decoder and Log Decoder Configuration Guide*.

Core Database Tuning

Improved optimized storage efficiency for maintaining high-speed access to both raw and metadata. With this latest update, NetWitness offers the option to utilize ZSTD compression, for your data storage needs.

- **ZSTD Compression for Data Storage:** ZSTD compression now supports storing raw and metadata separately. This feature saves considerable storage space while ensuring swift access to your data. You can now balance data compression and access performance excellently.

- **Configurable Compression Ratio:** Users can configure the compression ratio to tailor the balance between compression efficiency and data access speed. This flexibility lets you fine-tune the compression settings based on your specific use cases and requirements.

For more information, see the **Database Configuration Nodes** topic in the *Core Database Tuning Guide*.

Logstash Event Sources

Introducing NetWitness JDBC Logstash Input plugin support to collect logs from the following databases.

- Oracle 11g, 12c, 18c, and 19c
- IBMDB2

You can also use **Custom Typespec** to collect logs from databases that are not supported out of the box.

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

Log Integrations

NetWitness Platform XDR supports the integration of the following event sources to collect and parse logs. Unless specified, these services are supported on NetWitness Platform XDR 11.7.0.0 or later.

- As a launch partner for AWS AppFabric, NetWitness empowers customers to use this simplified, standardized method of securing new and existing AWS apps. For more information, see S3 Universal Connector.
- FluentD
- Jamf Protect
- JDBC Oracle 11g, 12c, 18c, and 19c (Supported from 12.3 onwards)
- JDBC IBMDB2 (Supported from 12.3 onwards)
- Custom JDBC Typespec (Supported from 12.3 onwards)
- Microsoft Azure Log Analytics (Support for Azure Kubernetes logs)
- OPSWAT Meta Access Cloud
- S3 Universal Connector (Support for Cloudflare RBI logs)
- Symantec Data Center Security (Symantec DCS)
- VMware Unified Access Gateway (UAG)

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

Third-Party Integrations

- **Splunk Integration**: Bidirectional workflow allows data flow between NetWitness and Splunk for additional context and increased efficiency. The NetWitness Query App for Splunk connects to a NetWitness Concentrator, facilitating regular polling of the NetWitness API to gather new session meta data. The collected meta data can be subsequently indexed by Splunk, ensuring timely analysis and processing. For more information, see NetWitness Query App for Splunk.

Security

Customers can use keytool to import certificates to JVM trust. This has helped them to move away from communicating over untrusted channel.

For more information on using keytool to import certificates to JVM trust, see the article *Custom Certificate Issue in CCM*.

Platform

The following section describes the new enhancements for Platform component:

Backup and Restore Improvements

- The Passwordless remote copying feature allows administrators to avoid entering the password in the Command Line Interface (CLI) while exporting and importing the data using the NetWitness Recovery Tool (NRT) and the NetWitness Recovery Wrapper Tool.

  For more information, see Recovery Tool User Guide.

- NetWitness Platform XDR allows the non-root users to perform backup and recovery of data using the NetWitness Recovery tool (NRT) and the NetWitness Recovery Wrapper tool.

  For more information, see Recovery Tool User Guide.

- NetWitness Recovery Wrapper Tool is enhanced with the following options to allow administrators to backup group of the hosts:

  - **Category Group**: This group allows you to create a backup of all the hosts specific to a given category such as Log Hybrid, Log Collector, Standalone Broker in the environment.

  - **Host Group**: This group allows you to create a backup of all the hosts specific to a given group created on the **/admin/appliances** page.
    You can use the backup to restore any of the hosts in case of configuration issues or catastrophic failures.

    For more information, see Recovery Tool User Guide.

Service Topology Export

NetWitness Platform XDR allows the Administrators to view details of the service aggregation flow map and export the relationship map for IT use cases.

Security Fixes

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 12.3.0.0

- NetWitness 12.2.0.1 to 12.3.0.0
- NetWitness 12.2.0.0 to 12.3.0.0
- NetWitness 12.1.1.0 to 12.3.0.0
- NetWitness 12.1.0.1 to 12.3.0.0
- NetWitness 12.1.0.0 to 12.3.0.0
- NetWitness 12.0.0.0 to 12.3.0
- NetWitness 11.7.3.0 to 12.3.0.0
- NetWitness 11.7.2.0 to 12.3.0.0
- NetWitness 11.7.1.2 to 12.3.0.0
- NetWitness 11.7.1.1 to 12.3.0.0
- NetWitness 11.7.1.0 to 12.3.0.0
- NetWitness 11.7.0.2 to 12.3.0.0
- NetWitness 11.7.0.1 to 12.3.0.0
- NetWitness 11.7.0.0 to 12.3.0.0

For more information on upgrading to 12.3.0.0, see Upgrade Guide for NetWitness 12.3.0.0

Warning: Before upgrading the UEBA host to 12.3.0.0, you must perform the backup of your Elasticsearch data such as Users, Entities, Alerts, and Indicators to retain them post upgrade. For more information, see NetWitness UEBA Configuration Guide *for 12.3.0.0*.

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 (11.7 to 12.2.0.1)

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-11-7-to-12-1-1/ta-p/695650.

Fixed Issues in 12.3.0.0 Release

This section lists issues fixed in 12.3.0.0 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.

Reporting Engine Fixes

Tracking Number	Description
ASOC-128177	After upgrading to the 12.1 version, Reporting Engine cannot forward logs to SFTP server after finishing the queries due to script issues. As a result, reporting engine report is not saved in the SFTP server.
ASOC-127736	An error message is displayed on the Report page after enabling **Push to Decoder** in an alert for a NetWitness Platform Database rule in Reporting Engine. As a result, Report page cannot push the rule to the decoder on the Report page.
ASOC-127577	Test chart feature in Reports (**Reports** > **Charts** > **Add new chart** > **Test Chart**) is unable to load with certain time ranges such as 1hr, 3hr, 6hr, 12hr, and 24hr. This issue occurs because Start and End dates are set as required request parameters.

Endpoint Fixes

Tracking Number	Description
ASOC-127545	In Endpoint, the **Hosts** tab is not loading because of the presence of huge bash history for a few agents. As a result, you can see timeouts or delays in **mongo.db**
ASOC-127319	Process Tree is not displayed in the **Respond** Service for high and critical Endpoint alerts (**Host**> **Event Details** > **View alert Details**). This issue occurs when the session ID of the event exceeds the integer limit of 32 bits. As a result, you cannot investigate the events.

SA Services

Tracking Number	Description
ASOC-127584	While filtering app rules under **Decoder** (**Admin** > **Services** > **Decoder** > **config**), the enable and disable functionality is not working correctly. As a result, the display order of any row remains the same and does not update after filtering the rules.
SADOCS-2392	If you download a file from the Events page with Korean characters in the file name, an underscore replaces the Korean characters in the file name. The fix converts the Korean characters of the UTF character set. But the Korean characters of the Non-UTF character set depends on JVM 20 or 21. This will be addressed in future releases.

Threat Intelligence

Tracking Number	Description
ASOC-100727	On failover, recurring custom feeds created before the failover are failing and not getting pushed to the core.

Core Services (Broker, Concentrator, Decoder, Archiver) Fixes

Tracking Number	Description
ASOC-113643	When the log decoder forwards the logs in RFC-3164 format to the other sources, the event destination receives the logs in the format which is specified for higher-order AppRule.
SACE-19321	While applying an aggregation filter on Archiver to archiver aggregation, all data aggregates because the aggregation filter does not function. This issue is fixed and Archiver to Archiver aggregation now supports query filters to filter out certain meta keys from sessions during aggregation.
ASOC-124102	For **rabbitmq.log**, queue exchange and its binding is not getting created. Hence, it triggers an alarm 'LogCollector Event Process Queue with no Bindings'. In the 12.3 version, the binding commands are part of NetWitness platform.

Administration Fixes

Tracking Number	Description
ASOC-121321	NwLogDecoder service frequently receives error messages in **/var/log/messages** because the message upload cannot recognize parameters such as **finalCount**.
ASOC-128043	The Jobs (**Admin** > **System** > **Jobs**) with lengthy queries take longer to load. As a result, the load time of the Jobs page is impacted.

SMS Fixes

Tracking Number	Description
ASOC-126357	Unable to establish a secure connection between ESM and Log Decoders because the certificates that ESM service uses are not available on the Log Decoder nodes. As a result, SMS fails to upload ESM feed files to the connected Log Decoders.

ESA Fixes

Tracking Number	Description
ASOC-127546	When the user sends an event to ESPER, and then it throws an exception runtime, the details need to be captured and moved to **Mongo.DB**. But, if the user gets frequent exceptions, the process becomes slow due to many databases writes.

Warehouse Connector Fixes

Tracking Number	Description
ASOC-133986	Avro file processing in the warehouse connector is extremely slow due to large data that causes Avro files to pile up and duplicate.
ASOC-133988	After rebooting Network Decoder or Log Decoder, an alarm is triggered in Health & Wellness to indicate a Lockbox failure.

Known Issues in 12.3.0.0 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 12.3.0.0 Components

The following table lists the build numbers for various components of NetWitness 12.3.0.0

Component	Version Number
NetWitness Admin Server	rsa-nw-admin-server-12.3.0.0-230530014857.5.c0e2a19.el7.centos.noarch.rpm
NetWitness Advanced Analytics Content	rsa-nw-advanced-analytics-content-12.3.0.0-230613124604.5.4770638.el7.centos.noarch.rpm
NetWitness Advanced Analytics Server	rsa-nw-advanced-analytics-server-12.3.0.0-230613124531.5.4770638.el7.centos.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Appliance Nonfips	rsa-nw-appliance-nonfips-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Audit Plugin	rsa-audit-plugins-12.3.0.0-4853.5.dace80b86.el7.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.3.0.0-4853.5.dace80b86.el7.x86_64.rpm
NetWitness Bootstrap	rsa-nw-bootstrap-12.3.0.0-2306160858.5.492a0d1.el7.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Broker Nonfips	rsa-nw-broker-nonfips-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.3.0.0-2770.5.4ee93683a.el7.x86_64.rpm
NetWitness Cloud	rsa-nw-cloud-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Cloud Connector Server	rsa-nw-cloud-connector-server-12.3.0.0-230523142637.5.432d8ef.el7.centos.noarch.rpm
NetWitness Cloud Link Server	rsa-nw-cloud-link-server-12.3.0.0-230511090224.5.d2efa6f.el7.centos.noarch.rpm
NetWitness Collectd	rsa-collectd-12.3.0.0-4853.5.dace80b86.el7.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.3.0.0-4853.5.dace80b86.el7.x86_64.rpm
NetWitness Component Descriptor	rsa-nw-component-descriptor-12.3.0.0-2307041631.5.0d0a586.el7.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Concentrator Nonfips	rsa-nw-concentrator-nonfips-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-12.3.0.0-2306160859.5.e5dbb35.el7.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-12.3.0.0-230614082002.5.4bec355.el7.centos.noarch.rpm

NetWitness Console	rsa-nw-console-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Content Server	rsa-nw-content-server-12.3.0.0-230612030617.5.6429c13.el7.centos.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-12.3.0.0-230614055744.5.e2e01bf.el7.centos.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-12.3.0.0-230516090433.5.d0c3976.el7.centos.noarch.rpm
NetWitness Dashboard Content	rsa-nw-dashboard-content-20230616110614-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Decoder Content	rsa-nw-decodercontent-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Decoder Analytics Content	rsa-nw-decoder-analytics-content-20230616110614-5.noarch.rpm
NetWitness Decoder Nonfips	rsa-nw-decoder-nonfips-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Decoder Content	rsa-nw-decodercontent-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-12.3.0.0-2306160900.5.2395b51.el7.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-12.3.0.0-2306141519.5.2d421f9.el7.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-12.3.0.0-230614010041.5.29afaf8.el7.centos.noarch.rpm
NetWitness Endpoint Decoder Analytics Content	rsa-nw-endpointdecoder-analytics-content-20230616110614-5.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-12.3.0.0-230620020656.5.8351980.el7.centos.noarch.rpm
NetWitness Esper Enterprise	rsa-nw-esper-enterprise-12.3.0.0-2303231741.5.04c15de.el7.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-12.3.0.0-230531075324.5.6dc4898.el7.centos.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-12.3.0.0-230530001121.5.ab3a460.el7.centos.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-12.3.0.0-230630083209.5.b2aa0d7.el7.centos.noarch.rpm
NetWitness License Server	rsa-nw-license-server-12.3.0.0-230404045616.5.72437bd.el7.centos.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.3.0.0-15098.5.c66d461f9.el7.x86_64.rpm
NetWitness Log Collector Content	rsa-nw-logcollectorcontent-20230614103642-5.el7.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.3.0.0-15098.5.c66d461f9.el7.x86_64.rpm
NetWitness Log Collector Tools	rsa-nw-logcollector-tools-12.3.0.0-15098.5.c66d461f9.el7.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm

NetWitness Log Decoder Analytics Content	rsa-nw-logdecoder-analytics-content-20230616110614-5.noarch.rpm
NetWitness Log Decoder Base Content	rsa-nw-logdecoder-base-content-20230614103642-5.el7.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-12.3.0.0-230630091956.5.260a353.el7.centos.x86_64.rpm
NetWitness Metrics Server	/rsa-nw-metrics-server-12.3.0.0-230511053142.5.23b4ed1.el7.centos.noarch.rpm
NetWitness Node Infra Server	rsa-nw-node-infra-server-12.3.0.0-230509040518.5.15a12b7.el7.centos.noarch.rpm
NetWitness Orchestration Cli	rsa-nw-orchestration-cli-12.3.0.0-2306160903.5.e98afa6.el7.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-12.3.0.0-230614065500.5.1242be3.el7.centos.noarch.rpm
NetWitness Placeholder	rsa-nw-placeholder-12.3.0.0-2306160901.5.500d706.el7.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.3.0.0-2306221221.5.8ac7e19.el7.noarch.rpm
NetWitness Presidio Config Server	rsa-nw-presidio-configserver-12.3.0.0-2306221221.5.8ac7e19.el7.noarch.rpm
NetWitness Presidio Core	rsa-nw-presidio-core-12.3.0.0-2306221221.5.8ac7e19.el7.noarch.rpm
NetWitness Presidio Elastic Search Init	rsa-nw-presidio-elasticsearch-init-12.3.0.0-2306221221.5.8ac7e19.el7.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.3.0.0-2306221240.5.2d6feb8.el7.noarch.rpm
NetWitness Presidio Flume	rsa-nw-presidio-flume-12.3.0.0-2306221238.5.a31ce74.el7.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-12.3.0.0-2306221221.5.8ac7e19.el7.noarch.rpm
NetWitness Presidio Output	rsa-nw-presidio-output-12.3.0.0-2306221221.5.8ac7e19.el7.noarch.rpm
NetWitness Presidio UI	rsa-nw-presidio-ui-12.3.0.0-2306221243.5.5f6c77a.el7.noarch.rpm
NetWitness Protobufs	rsa-protobufs-rt-12.3.0.0-939.5.755aa1cca.el7.x86_64.rpm
NetWitness Recovery Tools	rsa-nw-recovery-tool-12.3.0.0-2306160903.5.15c08f7.el7.noarch.rpm
NetWitness Relay Server	rsa-nw-relay-server-12.3.0.0-230614011121.5.136f258.el7.centos.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-12.3.0.0-5985.5.43c875596.el7.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-12.3.0.0-230621025346.5.992ecd5.el7.centos.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-12.3.0.0-2306160904.5.c752734.el7.noarch.rpm
NetWitness SA Tools	rsa-sa-tools-12.3.0.0-2306160905.5.e2a3b05.el7.noarch.rpm
NetWitness Security Cli	rsa-nw-security-cli-12.3.0.0-2306160906.5.bc29f90.el7.noarch.rpm
NetWitness Security Server	rsa-nw-security-server-12.3.0.0-230616073026.5.d03c80d.el7.centos.noarch.rpm

NetWitness Shell	rsa-nw-shell-12.3.0.0-230614131040.5.1df56af.el7.centos.noarch.rpm
NetWitness SOS Report Plugins	rsa-nw-sosreport-plugins-12.3.0.0-2306160906.5.801926f.el7.noarch.rpm
NetWitness SMS Runtime	rsa-sms-runtime-rt-12.3.0.0-4853.5.dace80b86.el7.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-12.3.0.0-4853.5.dace80b86.el7.x86_64.rpm
NetWitness Source Server	rsa-nw-source-server-12.3.0.0-230704021941.5.fb09470.el7.centos.noarch.rpm
NetWitness Source Server Content	rsa-nw-sourceserver-content-20230614103642-5.el7.x86_64.rpm
NetWitness Thing	rsa-nw-thing-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm
NetWitness User Interface	rsa-nw-ui-12.3.0.0-230630035034.5.f29f5bfd7a.el7.centos.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.3.0.0-12777.5.8c90c3468.el7.x86_64.rpm

Getting Help with NetWitness Platform XDR

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 12.3.0.0 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.3.0.0 Upgrade Guide	https://community.netwitness.com/t5/netwitness-platform-online/upgrade-guide-for-12-2/ta-p/696583

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 XDR documentation.