NetWitness® Platform

Version 12.4.0.0

Release Notes

NETWITNESS

Platform

Contact Information

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

Trademarks

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

Miscellaneous

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

April, 2024

Contents

What's New in 12.4.0.0 Release

The NetWitness 12.4.0.0 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:

- Upgrade
- Investigate
- Event Stream Analysis (ESA)
- Respond
- Response Actions
- Insight
- User and Entity Behavior Analytics
- Endpoint
- Policy-based Centralized Content Management (CCM)
- Concentrator, Decoder, Log Collector, and Archiver Services
- Log Integrations
- Security

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.

Upgrade

The following section describes the new enhancement for Upgrade:

Alma OS Migration

RedHat announced that CentOS Linux 7 will reach the end of life (EOL) on June 30, 2024. To address this change, NetWitness Platform is now integrated with the new version, AlmaLinux. When you upgrade to the NetWitness 12.4 version, you will be automatically migrated from CentOS 7.9 to AlmaLinux 8.9. The NetWitness Platform 12.4 upgrade process is easy and regular, like any other previous upgrades. You do not have to follow any specific procedure for upgrading to AlmaLinux OS. AlmaLinux provides several key benefits and new features:

- The upgrade to AlmaLinux is an inherently automated process with zero manual intervention.
- It comes with a pre-upgrade tool that helps administrators discover and mitigate issues before running the actual upgrade process.
- Saves time and administrative efforts.
- Retains control over installed applications.
- Preserves most of the configuration information.

NetWitness Platform streamlines the upgrade process, saves time and resources, and maintains control over installed applications and configurations when migrating from CentOS 7.9 to AlmaLinux 8.9.

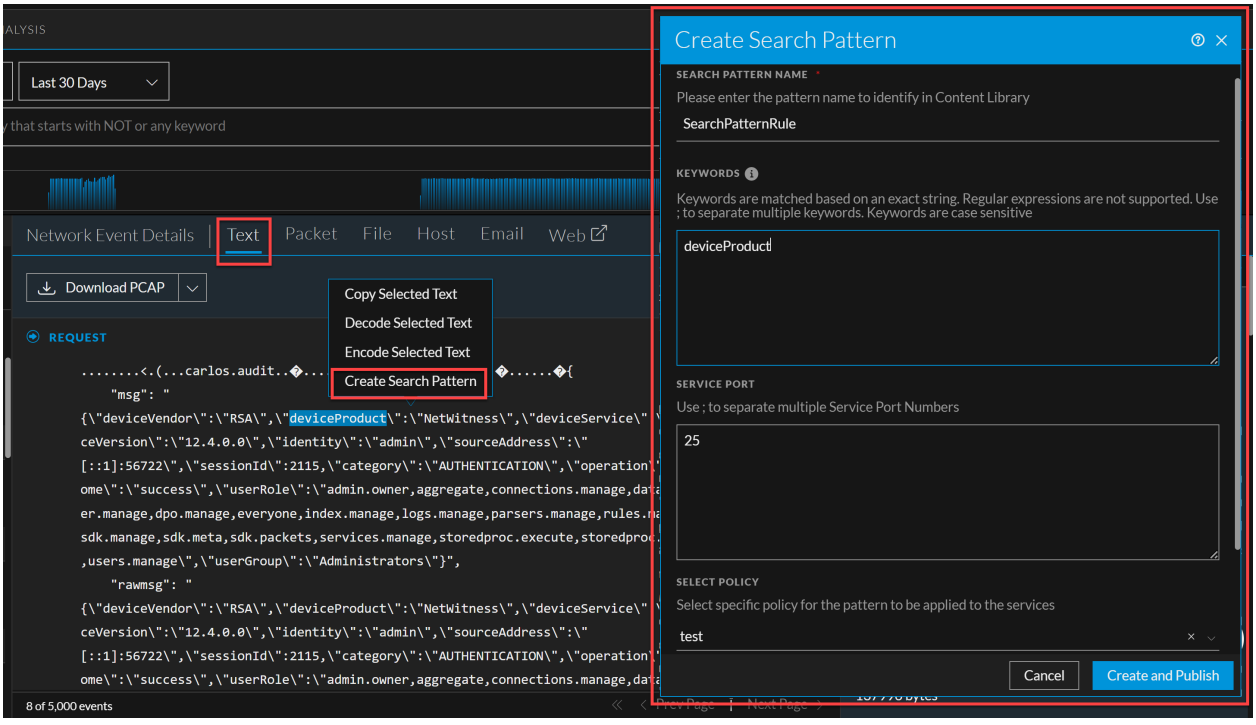
Investigate

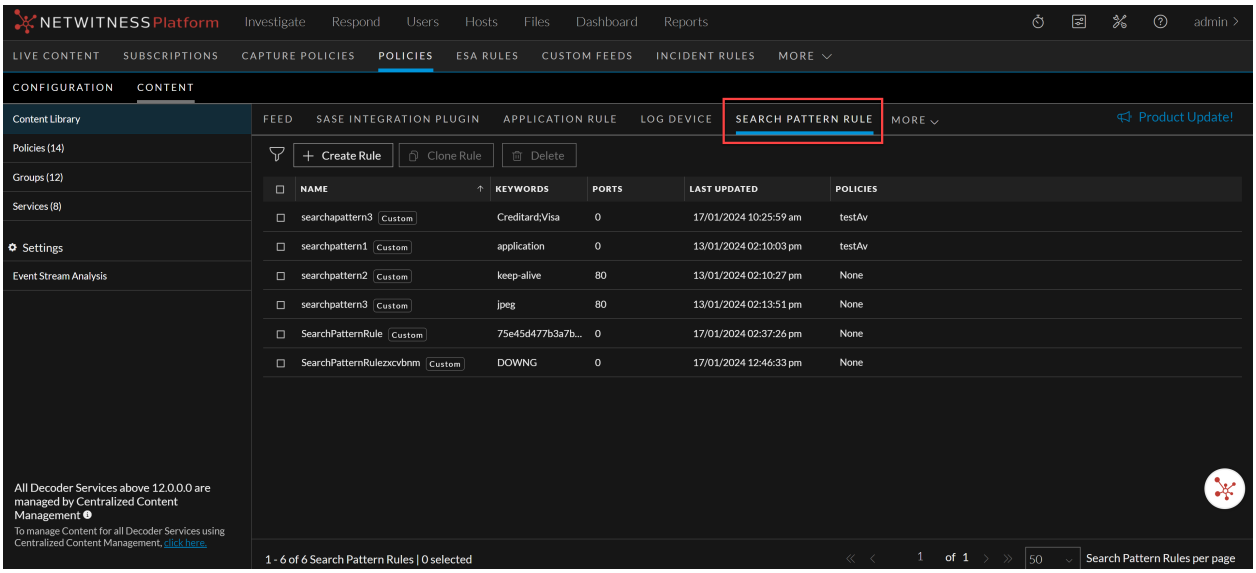
The following section describes the new enhancements for the Investigate component:

Interactive Network Parser Creation

In the **Investigate** > **Events** view, users can convert the exact patterns selected or keywords found in the network traffic they review in text session reconstruction into a network parser. This streamlined process allows the user to generate meta to trigger an incident (e.g., a future detection) without understanding how to create the parser.

Users can also create a network parser using keywords from the **(Configure)** > **Policies** > **Content Library** > **More** > **Search Pattern Rule** view.

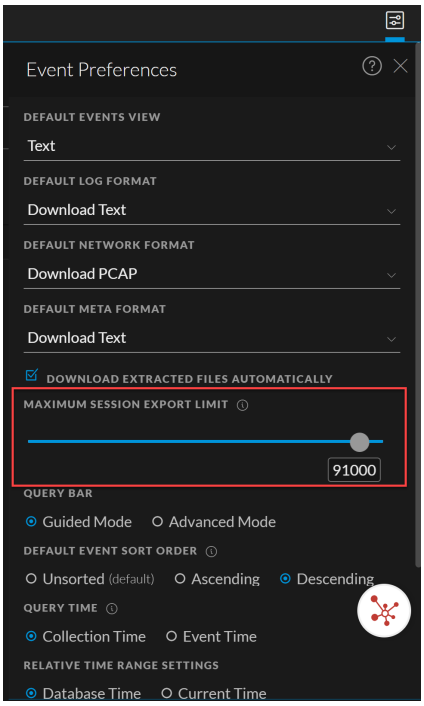




For more information, see **Create a Search Pattern in the Text Tab** topic in the *NetWitness Investigate User Guide* and **Manage Search Pattern Rule** topic in the *Policy-based Centralized Content Management Guide*.

Download More Sessions than Displayed in Events Table

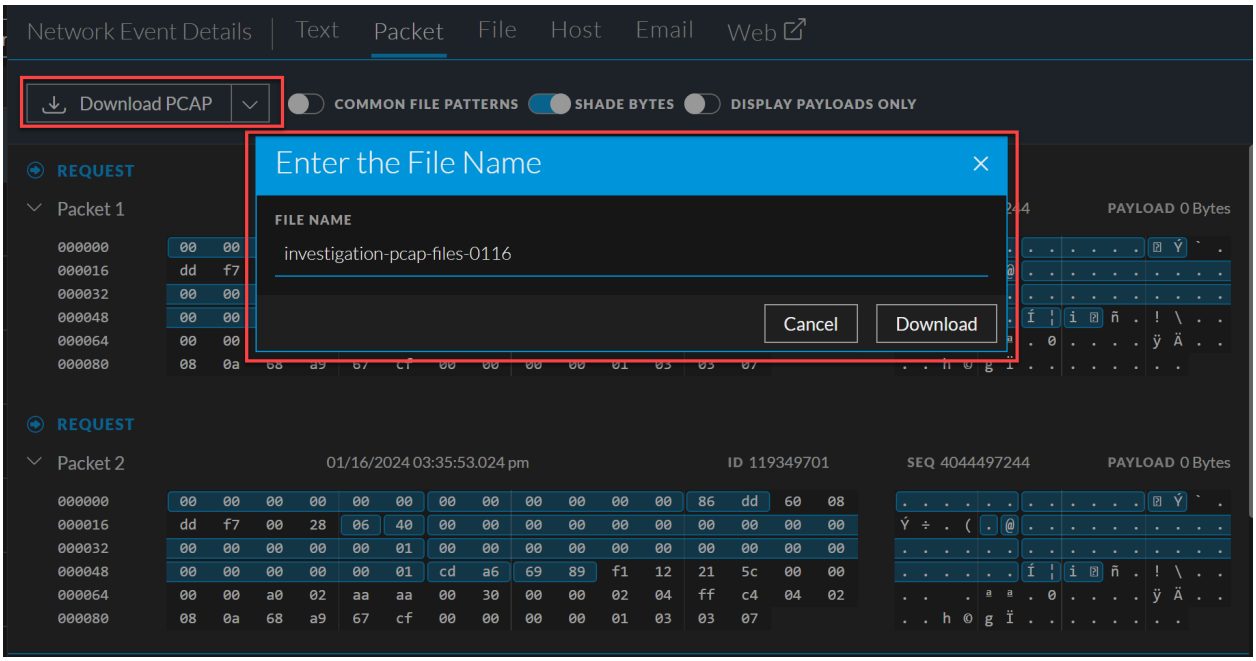
A new user preference, **Maximum Session Export Limit**, has been added to the **Events Preferences** panel in the **Investigate** > **Events** view. Analysts can use this setting to adjust the number of available sessions for exporting using the **Download All** menu options. This enhancement makes the number of exported sessions independent from the number of sessions displayed in the Events table.



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

Option to Download Files with Custom Names

Analysts can now use custom names when downloading event files from the **Events** panel view. Custom names make it easier to organize and manage downloaded event files, saving analysts time and effort.



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

Event Stream Analysis (ESA)

The following section describes the new enhancement for the ESA component:

Migrate custom scripts for notifications

You can migrate custom scripts to set up notifications. If a custom script needs file(s) to be accessed for read/write/execute operation, then file(s) must be in /tmp or /var/tmp directories.

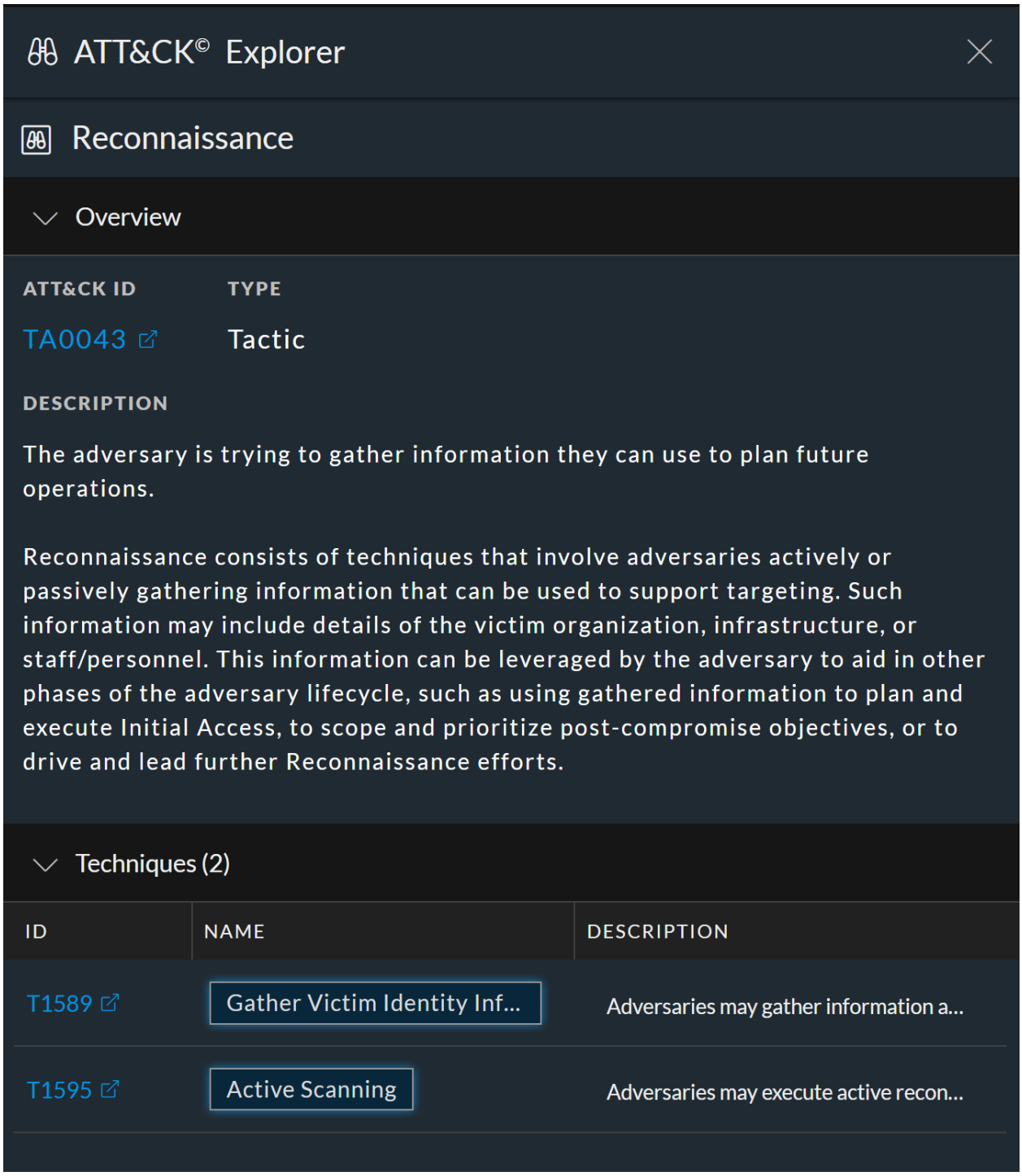
Respond

The following sections describe the new enhancements for the Respond component:

MITRE ATT&CK® Integration with NetWitness

MITRE ATT&CK® is a curated knowledge base of adversary Techniques and Tactics. It provides an appropriate level of categorization for adversary action and specific ways of defending against it. Analysts can view the high-level list of specified tactics, techniques, and sub-techniques, along with their details, and learn how potential threats and vulnerabilities in their environment are associated with the MITRE ATT&CK framework.

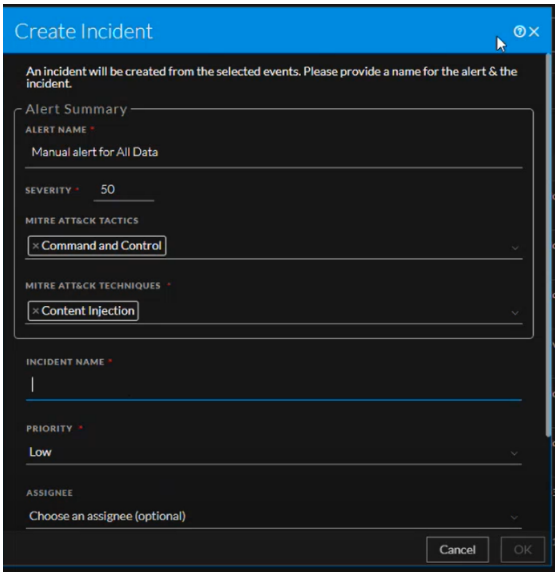
The new **ATT&CK© Explorer** Panel provides information about the adversary tactics and techniques associated with the Incidents in the **Respond** view.



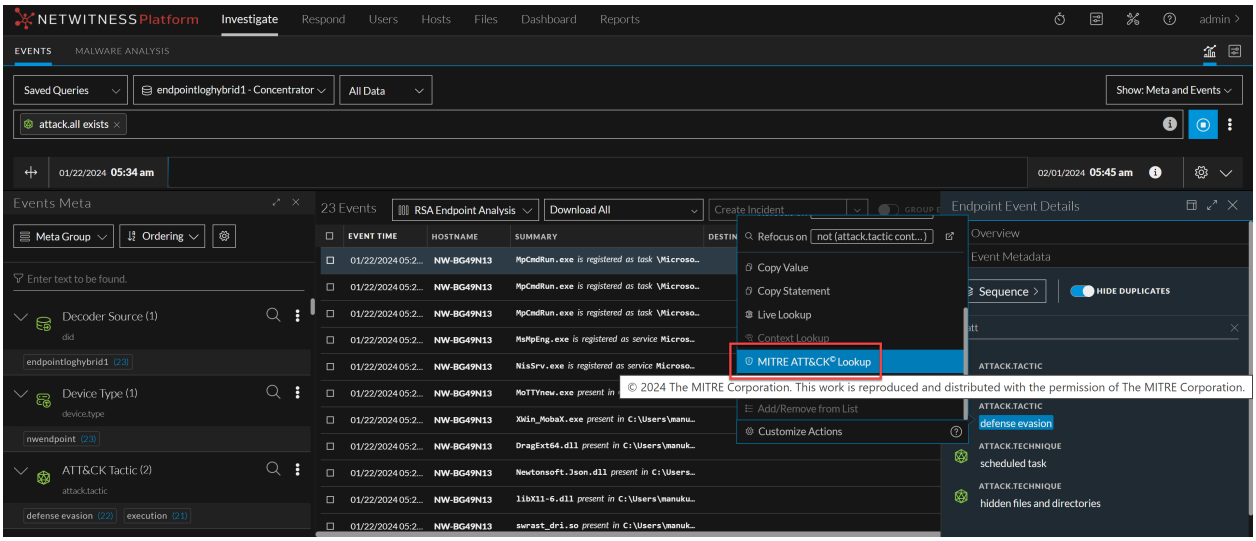
NetWitness Live is integrated with MITRE ATT&CK framework to help analysts to view the MITRE ATT&CK Tactics and Techniques associated with the **Application Rules** and **Event Stream Analysis Rules**. The Service Details Right panel (**(Configure)** > **Policies** > **Content** > **Content Library** > **Application Rule** or **Event Stream Analysis Rule** > click a row > Service Details Right panel) is enhanced to provide information about the MITRE ATT&CK Tactics and Techniques.

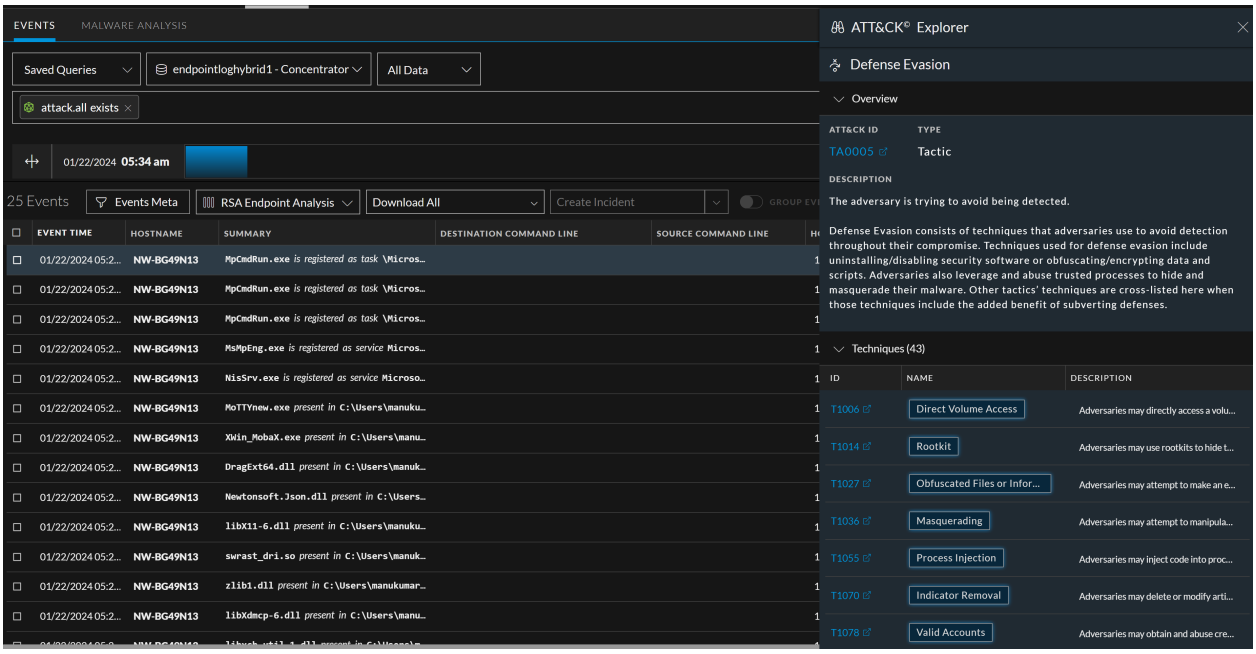
You can tag MITRE ATT&CK Tactics and Techniques while creating a custom **Application Rule** or **Event Stream Analysis Rule**.

You can also select the MITRE ATT&CK Tactics and Techniques while creating an incident from the **Investigate** > **Events** view.



With this, the **ATTACK.TACTIC** and **ATTACK.TECHNIQUE** metakeys in the **Events Metadata** panel has been enhanced with **MITRE ATT&CK© Lookup** integration to help you gain more information on the specific tactic and technique associated with the event.





The new **ATT&CK© Explorer** Panel is displayed when you click **MITRE ATT&CK© Lookup**.

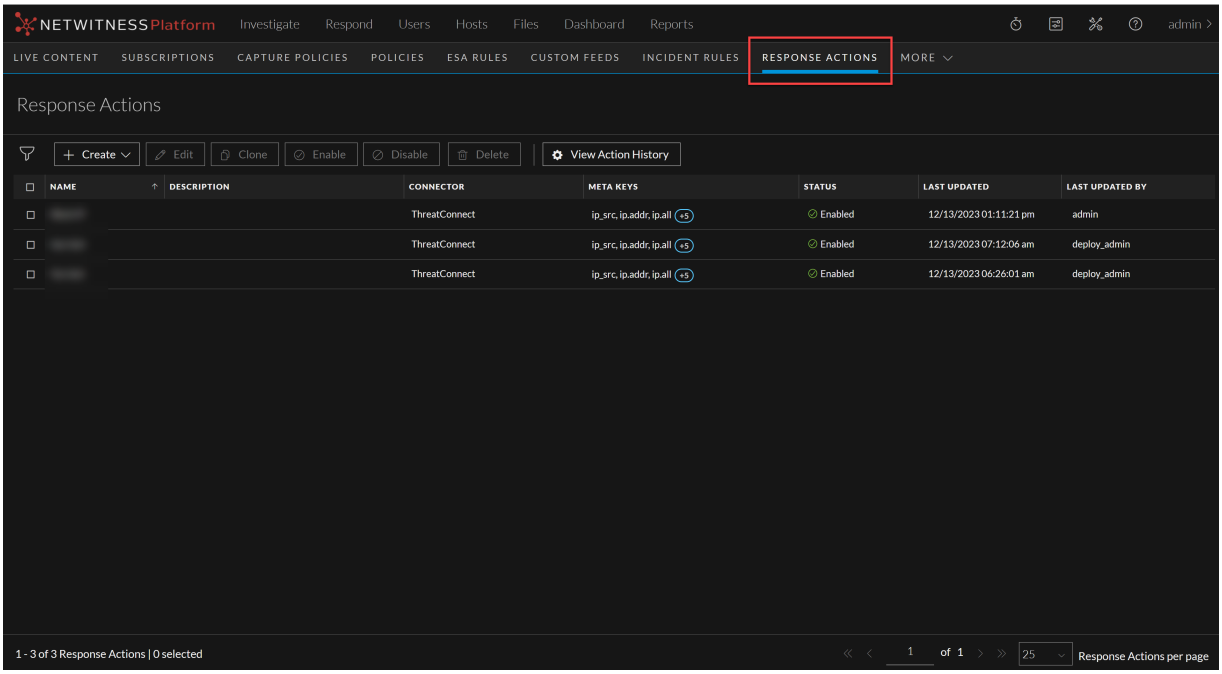
For more information, see NetWitness Respond User Guide for 12.4, *NetWitness Investigate User Guide*, and *Policy-based Centralized Content Management Guide*.

Response Actions

Response Actions are the reactive operations performed on configured metas using a third-party tool or connector such as ThreatConnect after triaging an event. **Response Actions**, the new feature added in **(CONFIGURE)** > **More** allows you to perform the following actions:

- Create and manage Response Actions for the supported metas available in **Respond**, **Investigate**, **Hosts**, and **Users** view.
- Perform Quick Actions on the configured meta and post the meta with additional parameters to the

connector for taking further actions.



For more information, see NetWitness Response Actions Configuration Guide for 12.4.

Insight

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

Whitelist Insight Alerts in Respond View

Administrators and analysts can now whitelist unwanted and recurring Insight alerts generated in the **Respond** > **Alerts** view. This enhancement provides the ability to select specific values, such as IP Address and Asset Type, and define a Whitelist condition to prevent unwanted alerts from being generated for these values. Using this enhancement, analysts can streamline the alert management process by excluding specific IP addresses or asset types that are known to be reliable and secure. This optimization minimizes unnecessary alerts generated on the **Respond** > **Alerts** view, reducing the time and effort required to review and analyze alerts.

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

User and Entity Behavior Analytics

The following section describes the new enhancements for UEBA component:

Support for Cisco Adaptive Security Appliance (ASA) and Fortinet VPN Devices

NetWitness UEBA has added support for the Cisco ASA and Fortinet VPN devices. With this enhancement, UEBA can now process Cisco ASA and Fortinet VPN logs, which helps to gather and analyze user activity information.

For more information, see the **UEBA Supported Sources by Schema** section in the *UEBA Configuration Guide*.

UEBA Performance Improvements

The following performance improvements are made for UEBA in the 12.4.0.0 version:

- Optimized the aggregation and accumulation models to generate and store models in parallel.
- Optimized the hourly score aggregation task to aggregate and score in parallel.

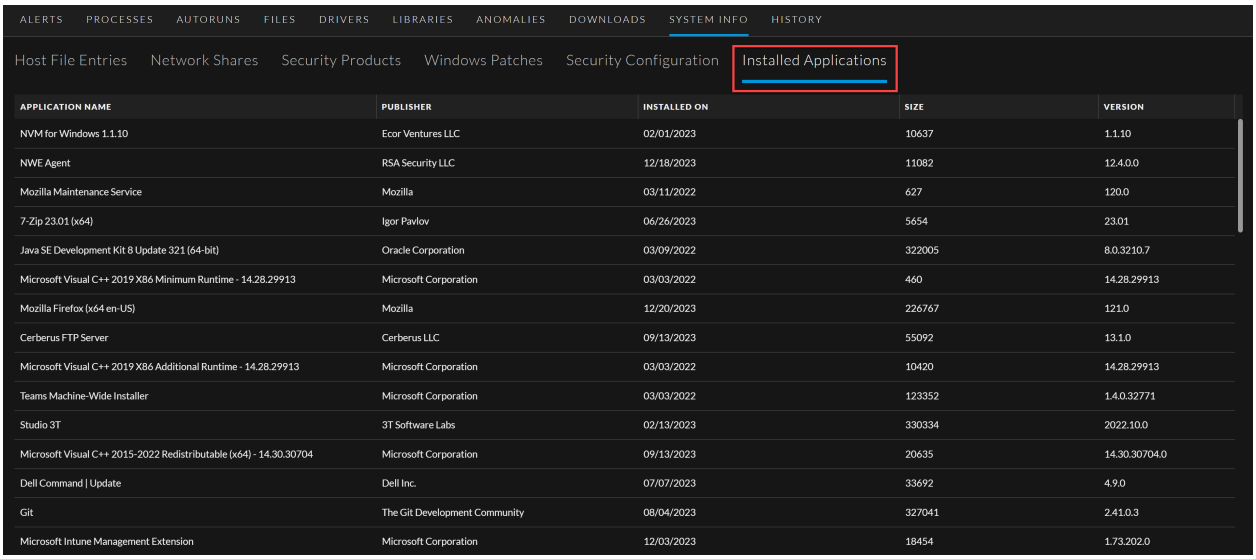
For more information on the supported scale, see the **Learning Period Per Scale for 12.4** topic in the *UEBA Configuration Guide*.

Endpoint

The following section describes the new enhancements for Endpoint component:

View Installed Applications

The **Hosts** details > **System Info** view has been enhanced to allow analysts to view the information about the various applications installed on a Windows machine.

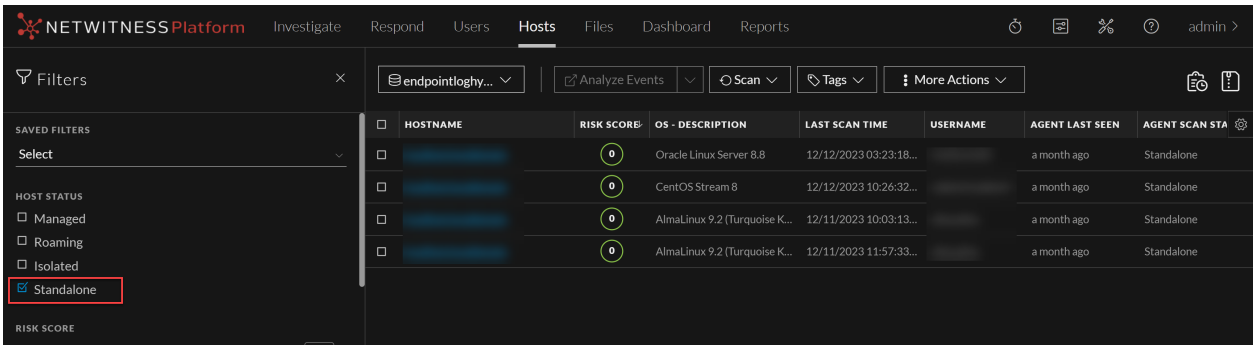


APPLICATION NAME	PUBLISHER	INSTALLED ON	SIZE	VERSION
NVM for Windows 1.1.10	Ecor Ventures LLC	02/01/2023	10637	1.1.10
NWE Agent	RSA Security LLC	12/18/2023	11082	12.4.0.0
Mozilla Maintenance Service	Mozilla	03/11/2022	627	120.0
7-Zip 23.01 (x64)	Igor Pavlov	06/26/2023	5654	23.01
Java SE Development Kit 8 Update 321 (64-bit)	Oracle Corporation	03/09/2022	322005	8.0.3210.7
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29913	Microsoft Corporation	03/03/2022	460	14.28.29913
Mozilla Firefox (x64 en-US)	Mozilla	12/20/2023	226767	121.0
Cerberus FTP Server	Cerberus LLC	09/13/2023	55092	13.1.0
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29913	Microsoft Corporation	03/03/2022	10420	14.28.29913
Teams Machine-Wide Installer	Microsoft Corporation	03/03/2022	123352	1.4.0.32771
Studio 3T	3T Software Labs	02/13/2023	330334	2022.10.0
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.30.30704	Microsoft Corporation	09/13/2023	20635	14.30.30704.0
Dell Command | Update	Dell Inc.	07/07/2023	33692	4.9.0
Git	The Git Development Community	08/04/2023	327041	2.41.0.3
Microsoft Intune Management Extension	Microsoft Corporation	12/03/2023	18454	1.73.202.0

For more information, see *NetWitness Endpoint User Guide for 12.4*.

Standalone Scan for Linux Agents

Administrators can execute offline or standalone scans on Linux hosts to perform threat analysis on the Air-gapped Linux machines.



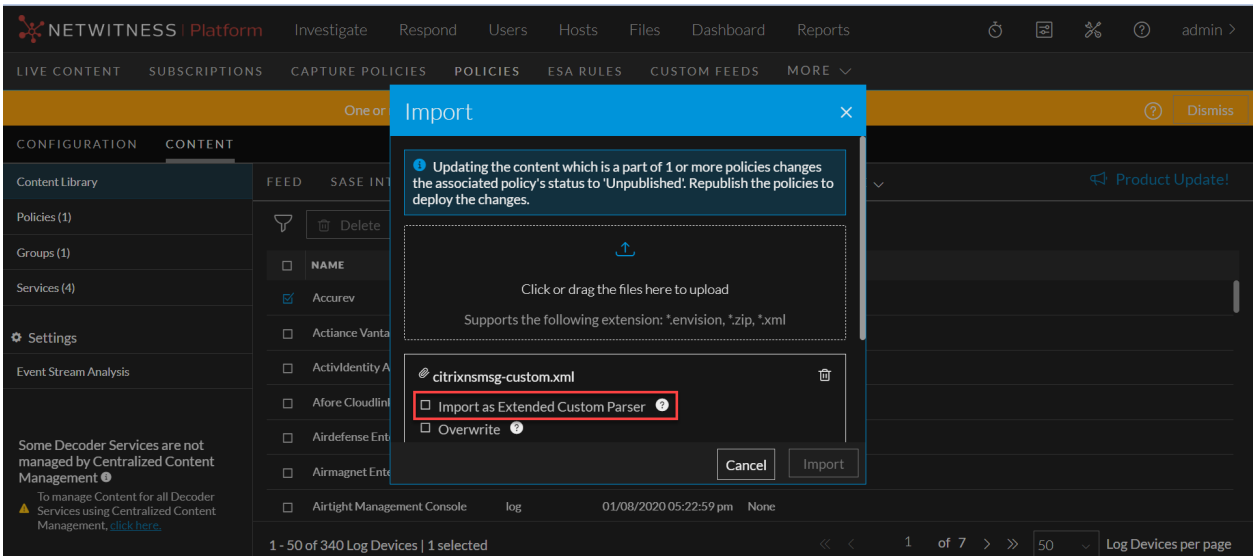
For more information, see *NetWitness Endpoint User Guide for 12.4*.

Policy-based Centralized Content Management (CCM)

The following enhancements are made for CCM in 12.4.0.0 version:

Enhancements for Proper Functioning and Deployment of Custom Parsers into Services through CCM

Introduced the capability to import individual XML (Log Device content type) to Content Library. You can upload either the base parsers or extended parsers as a standalone XML file. While importing XML files, you can optionally associate it with its corresponding base parser, effectively treating it as an extension parser. To import a standalone XML as an extended parser, select **Import as Extended Custom Parser** in the **Import** screen.



The Content Library now displays base parsers and extension parsers as distinct items, providing a clear and organized view for users. This separation ensures that users can easily identify and manage both types of parsers within the library. Furthermore, when an extension parser is added to a policy, the corresponding base parser is automatically included in the policy as well. This streamlined integration simplifies the process for users, eliminating the need to manually link base and extension parsers when creating or editing policies.

For more information, see the **Import Content to Content Library** section in the *Policy-based Centralized Content Management Guide*.

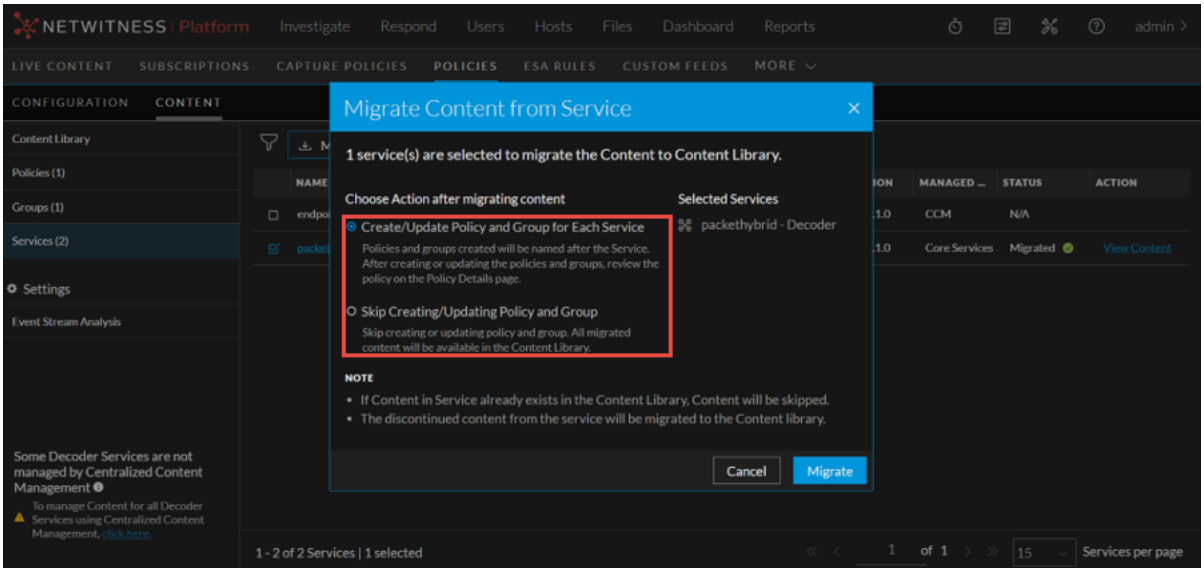
Enhancements during Removal of a Service from Group

While removing a service from the group, you can opt to either delete the content from service and then remove the service from the group or remove the service from the group without deleting the content.

For more information, see the **Edit a Group**, **Edit a Policy** and **Delete a Policy** sections in the *Policy-based Centralized Content Management Guide*.

Capability to Remigrate Content from Service

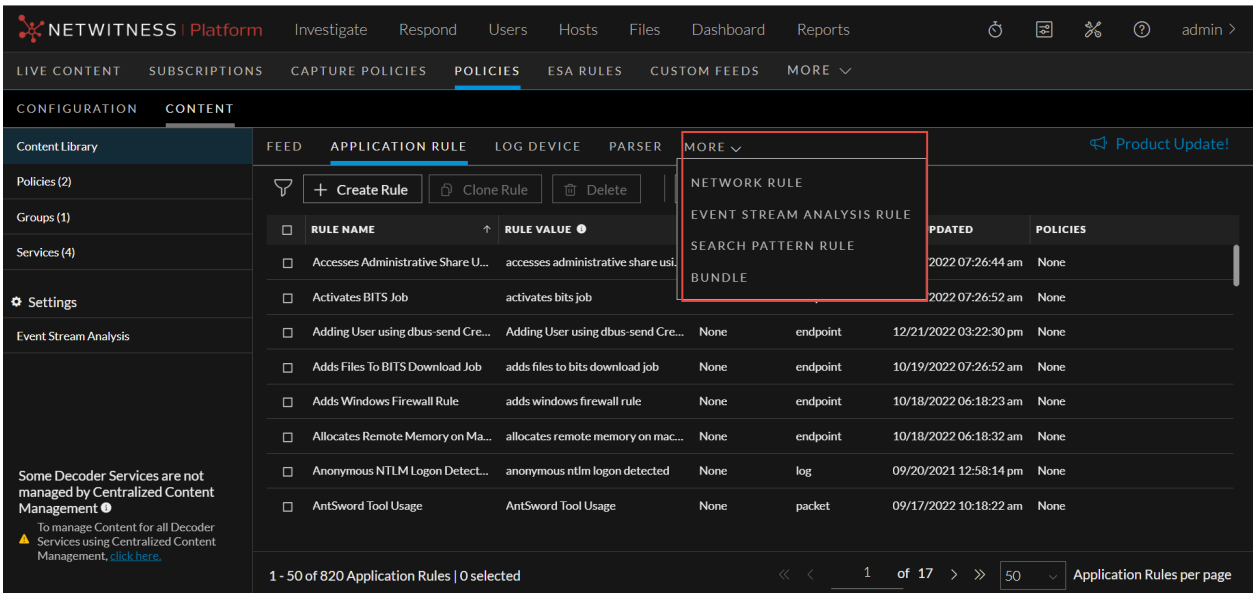
CCM is enhanced to re-migrate content from a service even if it is already migrated and/or assigned to Groups and Policies.While migrating content from a service already associated to a policy, you can optionally update the associated policy with migrated content. To update the existing policy and group for service after remigrating the service, the options available in the **Migrate Content from Service** page are updated to **Create/Update Policy and Group for Each Service** and **Skip Creating/Updating a Policy and Group**.



For more information, see the **Migrate Content from Service** section in the *Policy-based Centralized Content Management Guide*.

UI Enhancements

The **MORE** navigation menu is added to the CCM UI to view Bundles, Search Patterns, and Integrations by default. As you select the content type from the **MORE** menu, that content type appears on the left of the **MORE** menu.



Concentrator, Decoder, Log Collector, and Archiver Services

The following enhancements are made for Concentrator, Decoder, Log Collector, and Archiver Services in 12.4.0.0 version:

Capability to Deprecate the Use of IP Address for Basic Authentication

Netwitness has deprecated the use of IP address for Windows Collection Basic Authentication. Now, you must use the FQDN in the Event Source Address and add an entry of the same FQDN in '/etc/hosts' while configuring Basic Authentication.

New Utility to Stream Meta From Decoders to 3rd Party Tools

Introduced a beta utility to stream meta from network decoders to other 3rd party tools, making it easy to integrate NetWitness Platform with other products. All or a subset of meta data can be streamed to limit the amount sent to the 3rd party tool depending on the use case.

For more information, see Meta Export Installation and Configuration Guide.

Log Integrations

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

- Palo Alto Prisma Access
- VMware vSphere
- DeepInspect
- GCP Windows VM Logs (via GCP Plugin)

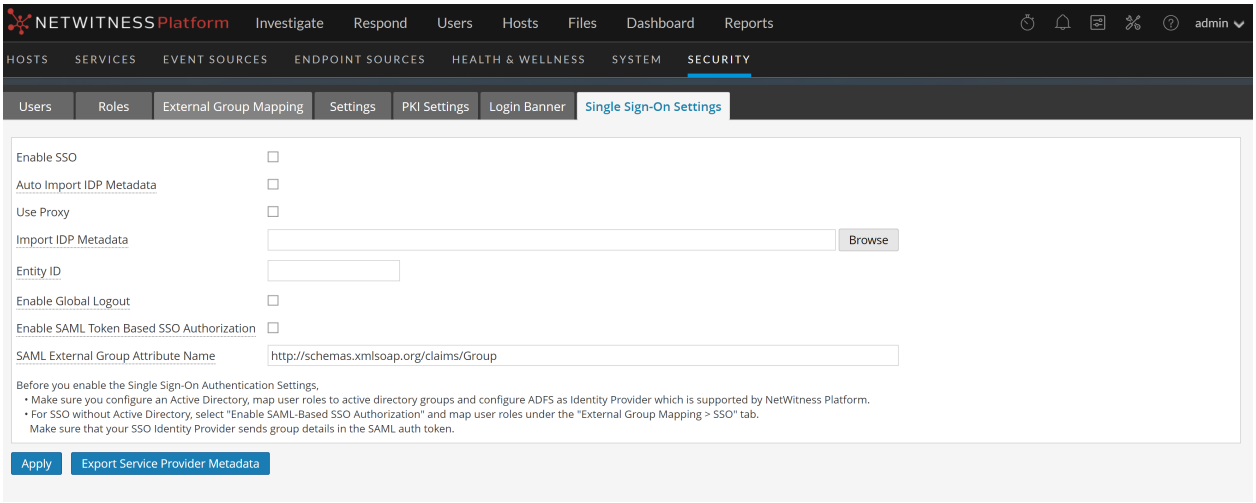
Note: From 12.4 onwards, VMWare plugin is also available for the collection of VMWare events and tasks.

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

Security

Single Sign-On (SSO) Authentication Independent of Active Directory (AD) Configuration in NetWitness

Starting from NetWitness Platform version 12.4, NetWitness offers SSO that is independent of AD configuration in NetWitness. It allows user authorization by using the list of user groups embedded in the SAML authentication token received from ADFS and verifying them against user groups already set up in NetWitness. This eliminates the need for users to configure or rely on Active Directory settings within NetWitness for user authentication. NetWitness now supports both Azure ADFS and Microsoft ADFS.



For more information, see **Set Up Single Sign-On Authentication** topic in the *System Security and User Management Guide*.

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 12.4.0.0

- NetWitness 12.3.1.0 to 12.4.0.0
- NetWitness 12.3.0.0 to 12.4.0.0

- NetWitness 12.2.0.1 to 12.4.0.0
- NetWitness 12.2.0.0 to 12.4.0.0

For more information on upgrading to 12.4.0.0, see Upgrade Guide for NetWitness 12.4.0.0

IMPORTANT: When adding users at the OS level during or after an upgrade to NetWitness version 12.4.0.0 or later, the admin server may encounter issues with new users or groups related to a few NetWitness accounts. These issues may result in incorrect LDAP mapping IDs and prevent affected users from logging in using LDAP after the upgrade.

IMPORTANT: The Warehouse connector uses a lockbox to store credentials securely for data integration sources and destinations. However, users upgrading from earlier versions to the 12.4 version cannot start the configured streams without migrating their existing credentials in the new lockbox. As a result, users must manually create a new lockbox key and then refresh the password for their sources and destinations configured in Warehouse Connector, wherever applicable. For detailed instructions on creating the new lockbox key, refer to the **Warehouse Connector** section under the **Post Upgrade Tasks** in the Upgrade Guide for NetWitness 12.4.0.0.

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

What's New in Previous Releases

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

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

Fixed Issues in 12.4.0.0 Release

This section lists issues fixed in 12.4.0.0 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.

Policy-based Centralized Content Management (CCM) Fixes

Tracking Number	Description
ASOC-142018	The Log device contents published from CCM are not disabled when contents are deleted for a service.
ASOC-141524	The ESA rules could not be saved by editing or updating the ESA rule. NetWitness UI and SA logs showed a run time exception while saving the rule. Also, on troubleshooting, the **RSA OSINT Non-IP Threat Intel Feed** did not have a unique ID associated with the policy, and occurred in multiple documents in the content policy collections.

Known Issues in 12.4.0.0 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 12.4.0.0 Components

The following table lists the build numbers for various components of NetWitness 12.4.0.0

Component	Version Number
NetWitness Admin Server	rsa-nw-admin-server-12.4.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Advanced Analytics Content	rsa-nw-advanced-analytics-content-12.4.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Advanced Analytics Server	rsa-nw-advanced-analytics-server-12.4.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Audit Plugin	rsa-audit-plugins-12.4.0.0-4892.5.9d0750b41.el8.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Bootstrap	rsa-nw-bootstrap-12.4.0.0-2401240926.5.a3d68ef.el8.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.4.0.0-2787.5.721a8daa7.el7.x86_64.rpm
NetWitness Cloud	rsa-nw-cloud-12.4.0.0-12867.5.957818c84.el8.x86_64.rpm
NetWitness Cloud Connector Server	rsa-nw-cloud-connector-server-12.4.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Cloud Link Server	rsa-nw-cloud-link-server-12.4.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm
NetWitness Collectd	rsa-collectd-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Component Descriptor	rsa-nw-component-descriptor-12.4.0.0-2402280945.5.4c3391a.el8.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-12.4.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-12.4.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
NetWitness Console	rsa-nw-console-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Content Server	rsa-nw-content-server-12.4.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-12.4.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-12.4.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Dashboard Content	rsa-nw-dashboard-content-20231220155210-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Decoder Analytics Content	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Decoder Content	rsa-nw-decodercontent-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-12.4.0.0-2402150604.5.dbd95e3.el8.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-12.4.0.0-2402061657.5.db93b9a.el8.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-12.4.0.0-240103053136.5.8430874.el8.alma.noarch.rpm
NetWitness Endpoint Decoder Analytics Content	rsa-nw-endpointdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-12.4.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm
NetWitness Esper Enterprise	rsa-nw-esper-enterprise-12.4.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-12.4.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-12.4.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-12.4.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm
NetWitness License Server	rsa-nw-license-server-12.4.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Collector Content	rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm

NetWitness Log Collector Tools	rsa-nw-logcollector-tools-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Log Decoder Analytics Content	rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Log Decoder Base Content	rsa-nw-logdecoder-base-content-20240124060008-5.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-12.4.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm
NetWitness Meta Export Utility	rsa-nw-metaexport-utility-12.4.0.0-110124.5.el8.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-12.4.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm
NetWitness Node Infra Server	rsa-nw-node-infra-server-12.4.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm
NetWitness Orchestration Cli	rsa-nw-orchestration-cli-12.4.0.0-2401091103.5.7317baa.el8.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-12.4.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitness Placeholder	rsa-nw-placeholder-12.4.0.0-2310040926.5.cebd204.el8.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Config Server	rsa-nw-presidio-configserver-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Core	rsa-nw-presidio-core-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Elastic Search Init	rsa-nw-presidio-elasticsearch-init-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.4.0.0-2401151152.5.18bd06b.el8.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Output	rsa-nw-presidio-output-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio UI	rsa-nw-presidio-ui-12.4.0.0-2402270745.5.0844250.el8.noarch.rpm

NetWitness Protobufs	rsa-protobufs-rt-12.4.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitness Recovery Tools	rsa-nw-recovery-tool-12.4.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitness Relay Server	rsa-nw-relay-server-12.4.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-12.4.0.0-5996.5.b76234be4.el8.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-12.4.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Response Actions Server	rsa-nw-response-actions-server-12.4.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-12.4.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness SA Tools	rsa-sa-tools-12.4.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitness Security Cli	rsa-nw-security-cli-12.4.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitness Security Server	rsa-nw-security-server-12.4.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitness Shell	rsa-nw-shell-12.4.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitness SOS Report Plugins	rsa-nw-sosreport-plugins-12.4.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness SMS Runtime RT	rsa-sms-runtime-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Source Server	rsa-nw-source-server-12.4.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitness Source Server Content	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
NetWitness User Interface	rsa-nw-ui-12.4.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

Getting Help with NetWitness Platform

Product Documentation

The following documentation is provided with this release.

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

Self-Help Resources

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

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

Contact NetWitness Support

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

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

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

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

NetWitness Educational Services

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

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

Feedback on Product Documentation

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