# NetWitness® Plattform

Version 12.4.0.0

# Versionshinweise

NETWITNESS
Platform

## Contact Information

NetWitness Community auf https://community.netwitness.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Case Management bereitgestellt werden.

## Marken



## Lizenzvereinbarung



## Drittanbieterlizenzen



## Hinweis zu Verschlüsselungstechnologien



## Verteilung



## Sonstiges

März 2024

# Inhalt

# Neuheiten in Version 12.4.0.0

In den Versionshinweisen zu NetWitness 12.4.0.0 werden neue Funktionen, Verbesserungen, Sicherheitsfixes, Upgrade-Pfade, behobene Probleme, bekannte Probleme, Funktionalität, die das Ende der Nutzungsdauer erreicht hat, Build-Nummern und Selbsthilferessourcen beschrieben.

## Verbesserungen

Die folgenden Abschnitte enthalten eine vollständige Liste und Beschreibung der Verbesserungen bestimmter Merkmale:

- Upgrade
- SASE-Merkmale
- Investigate
- Reagieren
- Antwortaktionen
- Insight
- Analyse des Nutzer- und Entitätsverhaltens (UEBA)
- Endpoint
- Policy-basiertes zentralisiertes Contentmanagement (CCM)
- Concentrator-, Decoder-, Log Collector- und Archiver-Services
- Protokollintegrationen
- Sicherheit

Informationen zum Auffinden der Dokumente, auf die in diesem Abschnitt verwiesen wird, finden Sie unter https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246.

Der Abschnitt Produktdokumentation enthält Links zur Dokumentation zu dieser Version.

## Upgrade

Im folgenden Abschnitt wird die neue Erweiterung für Upgrade beschrieben:

### Alma-Betriebssystemmigration

RedHat gab bekannt, dass CentOS Linux 7 am 30. Juni 2024 das Ende seiner Nutzungsdauer (EOL) erreichen wird. Um dieser Änderung Rechnung zu tragen, ist NetWitness Platform jetzt in die neue Version AlmaLinux integriert. Wenn Sie Ihr System auf die Version NetWitness 12.4 aktualisieren, wird es automatisch von CentOS 7.9 zu AlmaLinux 8.9 migriert. Der Upgrade-Prozess für NetWitness Platform 12.4 ist wie alle anderen vorherigen Upgrades einfach und regelmäßig. Sie müssen kein bestimmtes Verfahren für das Upgrade auf das AlmaLinux-Betriebssystem befolgen.
AlmaLinux bietet einige wichtige Vorteile und neue Funktionen:

- Das Upgrade auf AlmaLinux ist ein inhärent automatisierter Prozess, der keine manuelle Eingriffe erfordert.
- Darin enthalten ist ein Pre-Upgrade-Tool, das Administratoren und Administratorinnen dabei hilft, Probleme zu erkennen und zu beheben, bevor der eigentliche Upgrade-Prozess ausgeführt wird.
- Spart Zeit und Verwaltungsaufwand.
- Behält die Kontrolle über installierte Anwendungen.
- Behält die meisten Konfigurationsinformationen bei.

NetWitness Platform rationalisiert den Upgrade-Prozess, spart Zeit und Ressourcen und behält die Kontrolle über installierte Anwendungen und Konfigurationen bei der Migration von CentOS 7.9 zu AlmaLinux 8.9.

## SASE-Merkmale

Im folgenden Abschnitt wird die neue Erweiterung für SASE beschrieben:

### NetWitness SASE-Integrationen

- **NetWitness SASE-Integration in Palo Alto Networks**: Führt die NetWitness-Integration in Palo Alto Prisma SASE ein, um vollständige Netzwerk- und Protokolltransparenz zu bieten. Mit dieser benutzerdefinierten technischen Integration erhalten NetWitness-Nutzer und -Nutzerinnen Einblick in das Verhalten und die Kommunikation zwischen Geräten und Services in Remote-Netzwerken und verteilten Netzwerken in On-Premise-, Hybrid- und Cloud-Bereitstellungen. Die NetWitness-Palo Alto SASE-Integration ermöglicht es Kunden, die SASE-Flexibilität und die damit verbundenen Sicherheitsvorteile zu nutzen und gleichzeitig vollständige Transparenz für Bedrohungserkennung und -abwehr zu erhalten.
- **NetWitness SASE-Integration in Symantec by Broadcom (privater Vorschaumodus)**: Führt die NetWitness-Integration in Symantec by Broadcom SASE ein, um vollständige Netzwerk- und Protokolltransparenz bereitzustellen. Mit dieser benutzerdefinierten technischen Integration erhalten NetWitness-Nutzer und -Nutzerinnen Einblick in das Verhalten und die Kommunikation zwischen Geräten und Services in Remote-Netzwerken und verteilten Netzwerken in On-Premise-, Hybrid- und Cloud-Bereitstellungen. Die NetWitness-Broadcom SASE-Integration ermöglicht es Kunden, die SASE-Flexibilität und die damit verbundenen Sicherheitsvorteile zu nutzen und gleichzeitig vollständige Transparenz für Bedrohungserkennung und -abwehr zu erhalten.

  **Hinweis:** In der Version 12.4 befindet sich die NetWitness SASE-Integration in Symantec by Broadcom im privaten Vorschaumodus.

Weitere Informationen finden Sie im *Broadcom SASE-Konfigurationshandbuch für 12.4* und *Palo Alto Prisma SASE-Konfigurationshandbuch für 12.4*.

### NetWitness SASE Hybrid-Cloud-Konfiguration

Administratoren und Administratorinnen können sich jetzt für ein Hybrid-Cloud-Modell für SASE entscheiden. Die SASE Hybrid-Cloud-Konfiguration ist ein datengesteuertes Design. SASE Hybrid Cloud bietet eine effizientere und sicherere Kommunikation zwischen den NetWitness Platform-Komponenten. Der NetWitness Admin-Server enthält das Skript nw-create-cloud-hybrid, das das NetWitness Overlay Network und die definierten NetWitness Nodes in ihren jeweiligen Regionen in der Google Cloud Platform (GCP) bereitstellt. Das NetWitness Peer-to-Peer-Netzwerk (nw-ppn) bietet sichere, gegenseitig authentifizierte, PKI-basierte Kommunikation zwischen NetWitness-Komponenten.

Weitere Informationen finden Sie im *SASE-Installationshandbuch für 12.4*.

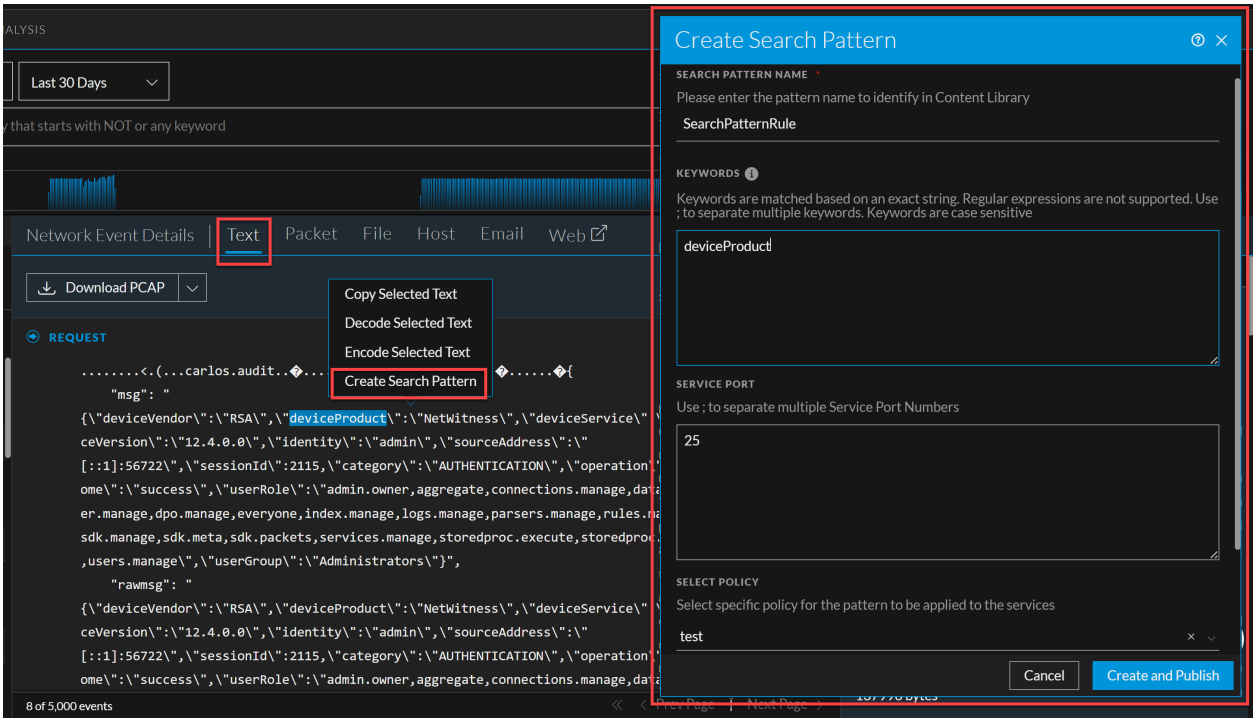
## Investigate

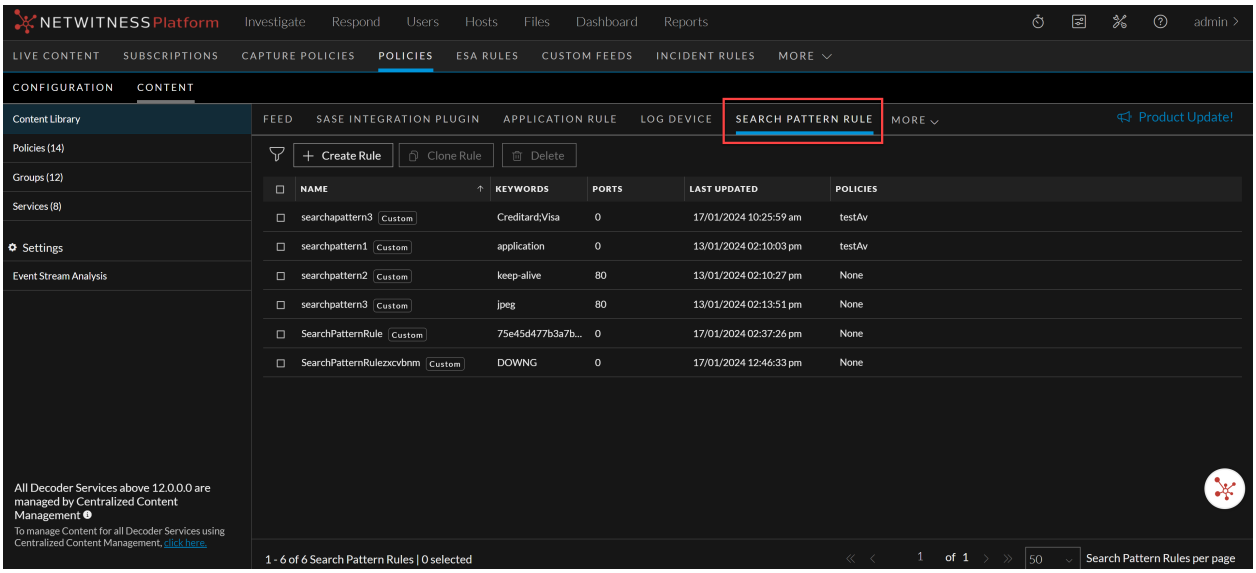
Im folgenden Abschnitt werden die neuen Erweiterungen für die Investigate-Komponente beschrieben:

### Erstellung eines interaktiven Netzwerk-Parsers

In der Ansicht **Investigate** > **Ereignisse** können Nutzer und Nutzerinnen die genauen ausgewählten Muster oder die Schlüsselwörter, die sie in dem bei der Rekonstruktion von Textsitzungen überprüften Datenverkehr finden, in einen Netzwerk-Parser umwandeln. Dieser optimierte Prozess ermöglicht es Nutzern und Nutzerinnen, Metadaten zu generieren, um einen Vorfall (z. B. eine zukünftige Erkennung) auszulösen, ohne zu wissen, wie der Parser erstellt wird.

Nutzern und Nutzerinnen können auch einen Netzwerkparser mit Schlüsselwörtern in der Sicht  **(Konfigurieren)** > **Policys** > **Inhaltsbibliothek** > **Mehr** > **Suchmusterregel** erstellen.

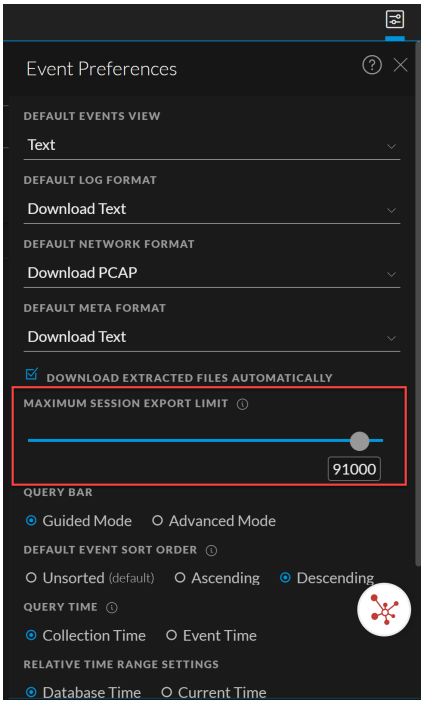





Weitere Informationen finden Sie im Thema **Erstellen eines Suchmusters auf der Registerkarte „Text“** im *NetWitness Investigate-Benutzerhandbuch* und im Thema **Verwalten von Suchmusterregeln** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

## Herunterladen von mehr Sitzungen, als in der Ereignistabelle angezeigt werden

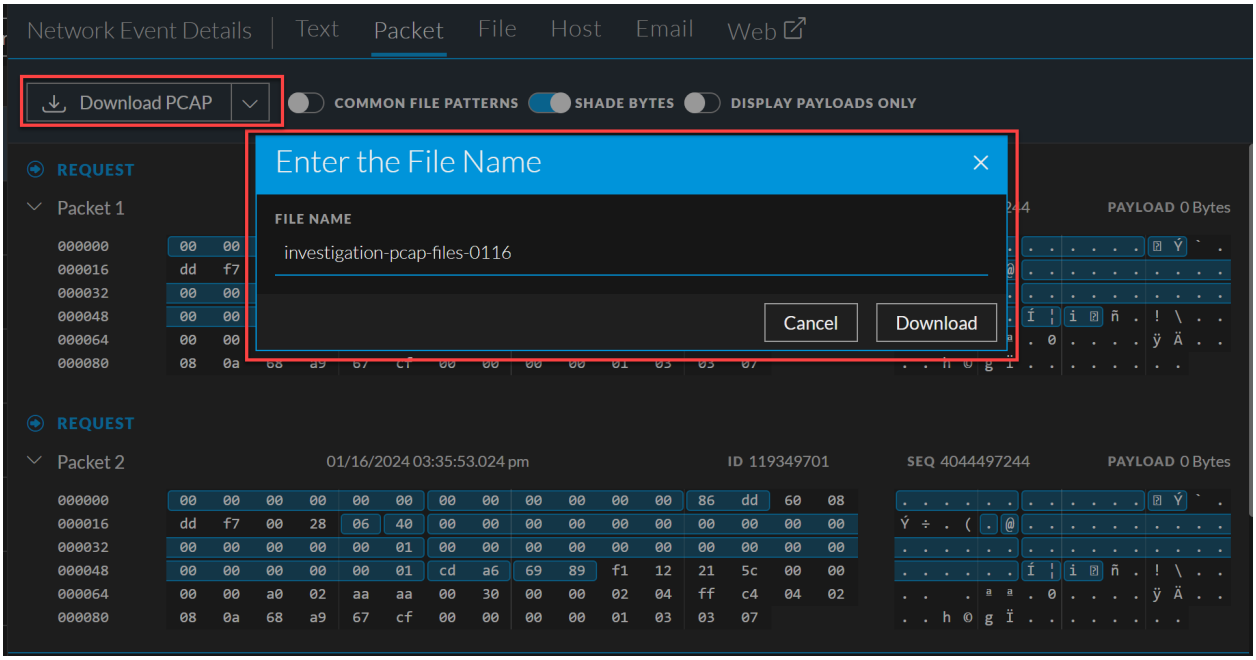
Die neue Benutzereinstellung **Maximales Sitzungsexportlimit** wurde dem Bereich **Ereigniseinstellungen** in der Ansicht **Investigate** > **Ereignisse** hinzugefügt. Analysten und Analystinnen können mit dieser Einstellung die Anzahl der verfügbaren Sitzungen für den Export mithilfe der Menüoptionen **Alle herunterladen** anpassen. Durch diese Verbesserung ist die Anzahl der exportierten Sitzungen unabhängig von der Anzahl der in der Ereignistabelle angezeigten Sitzungen.



Weitere Informationen finden Sie im Thema **Festlegen von Benutzereinstellungen für die Ereignisansicht** im *NetWitness Investigate – Benutzerhandbuch*.

### Option zum Herunterladen von Dateien mit benutzerdefinierten Namen

Analysten und Analystinnen können jetzt benutzerdefinierte Namen verwenden, wenn sie Ereignisdateien aus der Panelansicht **Ereignisse** herunterladen. Benutzerdefinierte Namen erleichtern die Organisation und Verwaltung heruntergeladener Ereignisdateien und sparen Zeit und Mühe.




Weitere Informationen finden Sie im Thema **Herunterladen von Daten in der Ereignisansicht** im *NetWitness Investigate – Benutzerhandbuch*.

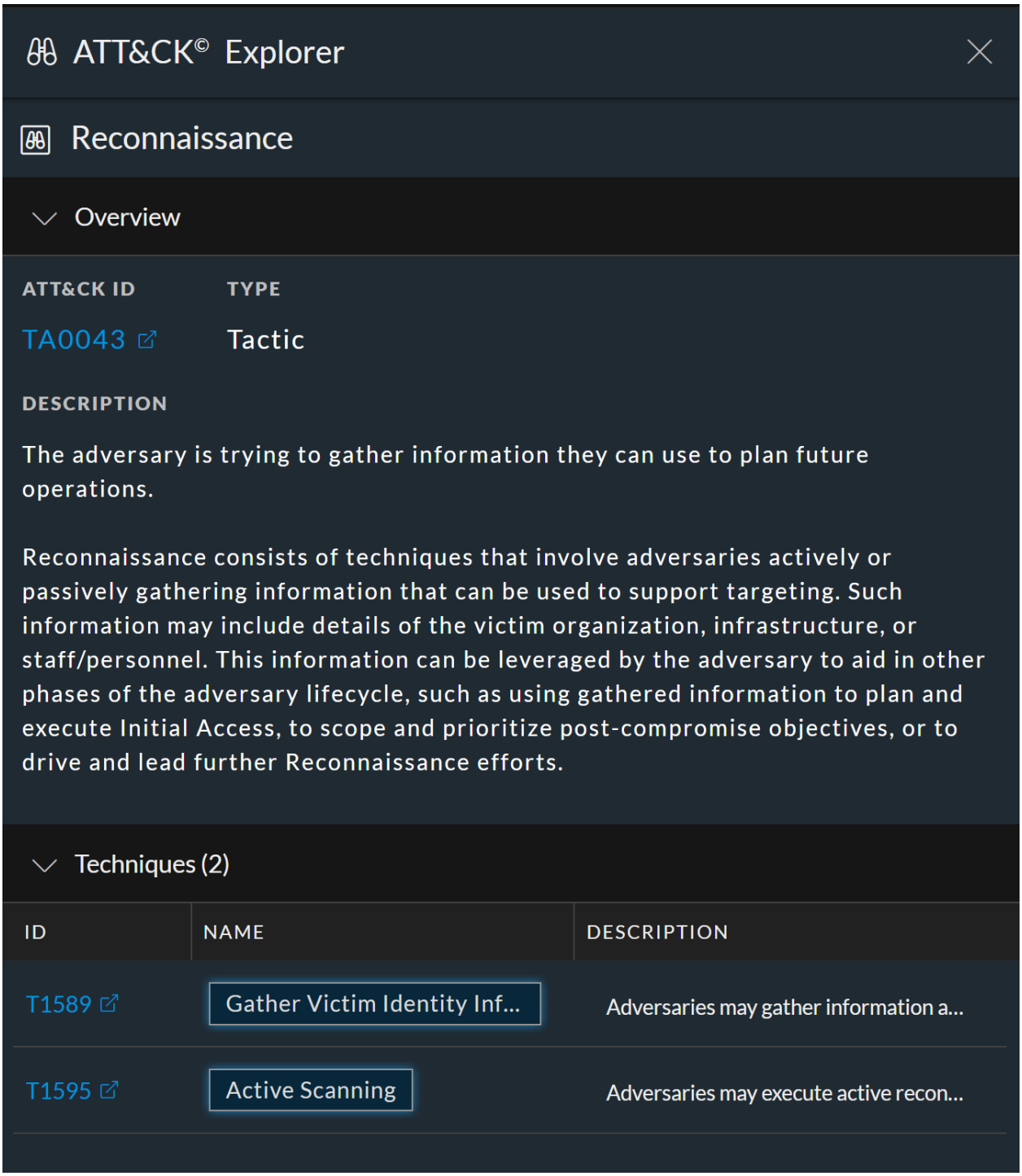
## Reagieren

In den folgenden Abschnitten werden die neuen Erweiterungen für die Respond-Komponente beschrieben:

### MITRE ATT&CK®-Integration in NetWitness

MITRE ATT&CK® ist eine kuratierte Wissensdatenbank über Techniken und Taktiken von Gegnern. Es bietet eine angemessene Kategorisierungsebene für gegnerische Aktionen und spezifische Möglichkeiten, sich dagegen zu verteidigen. Analysten und Analystinnen können die übergeordnete Liste der angegebenen Taktiken, Techniken und Untertechniken sowie deren Details anzeigen und erfahren, in welcher Beziehung potenzielle Bedrohungen und Schwachstellen in ihrer Umgebung zum MITRE ATT&CK-Framework stehen.

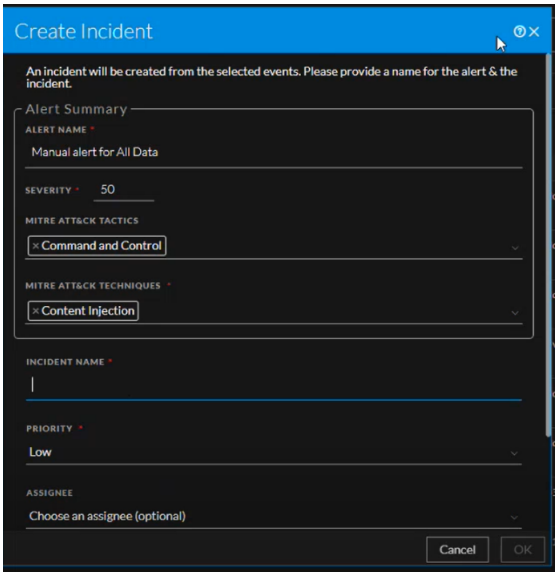
Der neue Bereich **ATT&CK© Explorer** bietet Informationen zu den Taktiken und Techniken von Gegnern im Zusammenhang mit den Vorfällen in der Ansicht **Respond**.



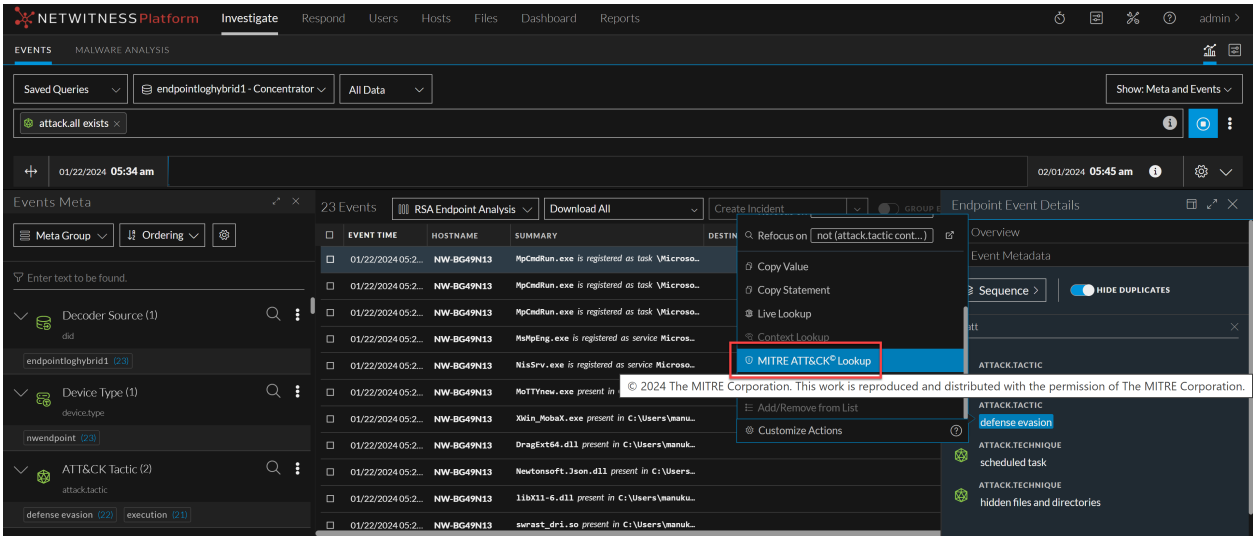

NetWitness Live ist in das MITRE ATT&CK-Framework integriert, um Analysten und Analystinnen dabei zu helfen, die MITRE ATT&CK-Taktiken und -Techniken anzuzeigen, die mit den **Anwendungsregeln** und **Event Stream Analysis-Regeln** verknüpft sind. Der rechte Bereich „Servicedetails“ (**(Konfigurieren)** > **Policys** > **Inhalt** > **Inhaltsbibliothek** > **Anwendungsregel** oder **Event Stream Analysis Regel** > auf eine Zeile klicken > Servicedetails, rechter Bereich) wird erweitert, um Informationen über die MITRE ATT&CK-Taktiken und -Techniken bereitzustellen.

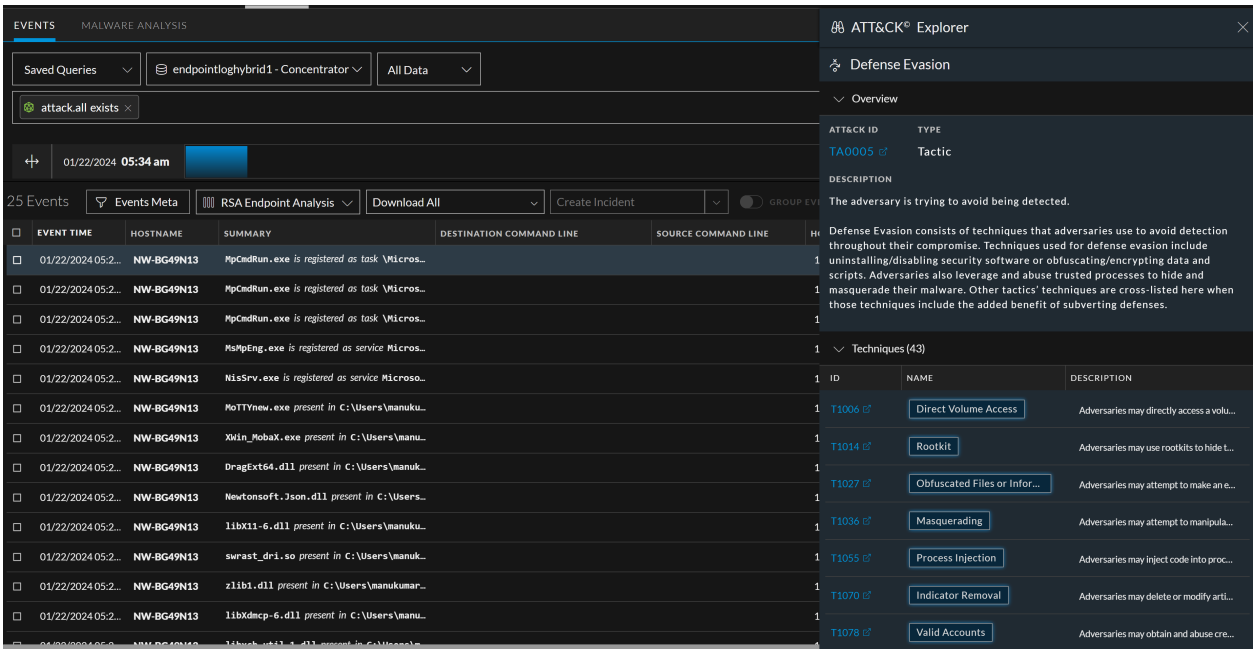
Sie können MITRE ATT&CK-Taktiken und -Techniken mit Tags kennzeichnen, während Sie eine benutzerdefinierte **Anwendungsregel** oder **Event Stream Analysis-Regel** erstellen.

Zudem können Sie die MITRE ATT&CK-Taktiken und -Techniken auswählen, während Sie einen Vorfall in der Ansicht **Investigate** > **Ereignisse** erstellen.




Dadurch werden die Metaschlüssel **ATTACK.TACTIC** und **ATTACK.TECHNIQUE** im Bereich **Ereignismetadaten** um die **MITRE ATT&CK© Lookup**-Integration erweitert, damit Sie mehr Informationen über die spezifische Taktik und Technik im Zusammenhang mit dem Ereignis erhalten.






Der neue Bereich **ATT&CK© Explorer** wird angezeigt, wenn Sie auf **MITRE ATT&CK© Lookup** klicken.

Weitere Informationen finden Sie im NetWitness Respond-Benutzerhandbuch für 12.4, *NetWitness Investigate-Benutzerhandbuch* und *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

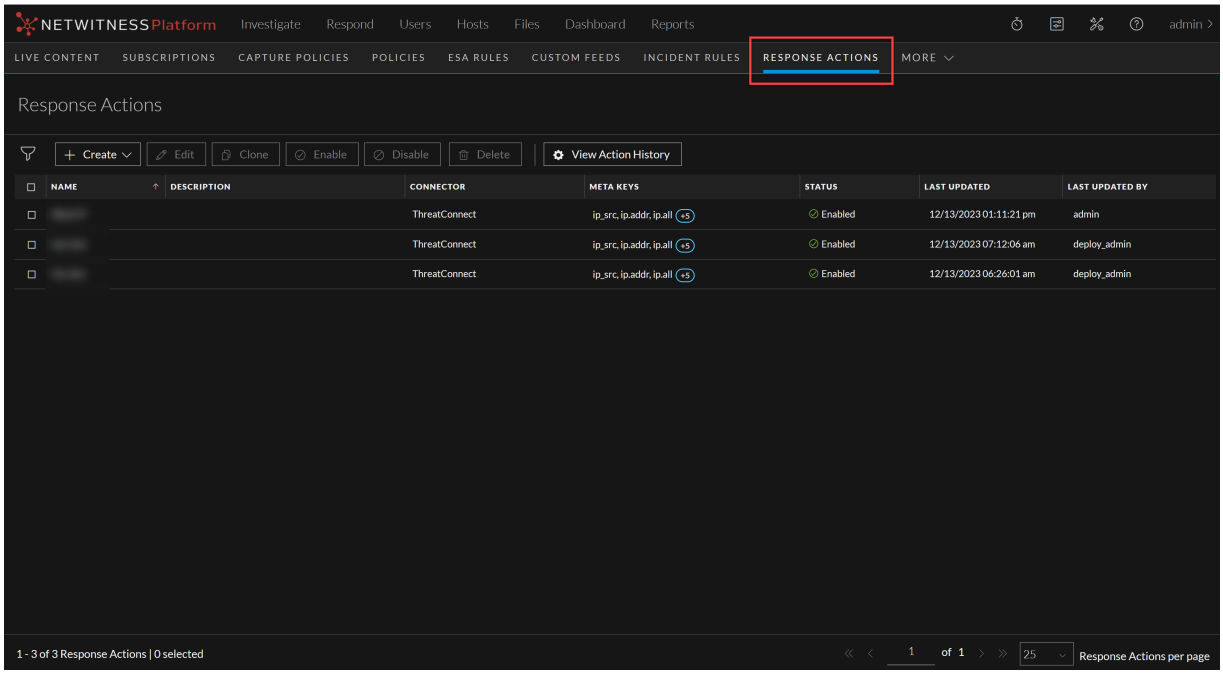
## Antwortaktionen

Antwortaktionen sind die reaktiven Vorgänge, die nach der Triage eines Ereignisses mit einem Tool oder Connector eines Drittanbieters wie ThreatConnect an konfigurierten Metas ausgeführt werden.

**Antwortaktionen**, die neue Funktion in **(KONFIGURIEREN)** > **Mehr** ermöglicht Ihnen, die folgenden Aktionen auszuführen:

- Erstellen und verwalten Sie Antwortaktionen für die unterstützten Metadaten, die in der Ansicht **Respond**, **Investigate**, **Hosts** und **Benutzer** verfügbar sind.
- Führen Sie Schnellaktionen für die konfigurierten Metadaten durch und senden Sie die Metadaten mit

zusätzlichen Parametern an den Connector, um weitere Aktionen durchzuführen.




Weitere Informationen finden Sie im *Aktionskonfigurationsleitfaden für NetWitness Respond 12.4*.

## Insight

In den folgenden Abschnitten werden die neuen Erweiterungen für die Insight-Komponente beschrieben:

### Whitelist für Insight-Warnungen in der Respond-Ansicht

Administratoren und Administratorinnen sowie Analysten und Analystinnen können jetzt unerwünschte und wiederkehrende Insight-Warnungen, die in der Ansicht **Respond** > **Warnmeldungen** generiert werden, auf die Whitelist setzen. Diese Erweiterung bietet die Möglichkeit, bestimmte Werte wie IP-Adresse und Asset-Typ auszuwählen und eine Whitelist-Bedingung zu definieren, um zu verhindern, dass unerwünschte Warnungen für diese Werte generiert werden. Mithilfe dieser Erweiterung können Analysten und Analystinnen den Managementprozess für Warnmeldungen optimieren, indem sie bestimmte IP-Adressen oder Asset-Typen ausschließen, die als zuverlässig und sicher gelten. Diese Optimierung minimiert unnötige Warnmeldungen, die in der Ansicht **Respond** > **Warnmeldungen** generiert werden, und reduziert so den mit der Überprüfung und Analyse der Warnmeldungen verbundenen Zeit- und Arbeitsaufwand.

Weitere Informationen finden Sie im Abschnitt **NetWitness Insight** im *NetWitness-Dokumentationsportal*.

## Analyse des Nutzer- und Entitätsverhaltens (UEBA)

Im folgenden Abschnitt werden die neue Erweiterungen der UEBA-Komponente beschrieben:

### Unterstützung für Cisco Adaptive Security Appliance (ASA) und Fortinet VPN-Geräte

NetWitness UEBA wurde Unterstützung für die Cisco ASA- und Fortinet VPN-Geräte hinzugefügt. Dank dieser Erweiterung kann UEBA nun Cisco ASA- und Fortinet VPN-Protokolle verarbeiten, wodurch die Erfassung und Analyse von Benutzeraktivitätsinformationen erleichtert wird.

Weitere Informationen finden Sie im Abschnitt **Von der UEBA unterstützte Quellen nach Schema** im *UEBA-Konfigurationshandbuch*.

### Verbesserung der UEBA-Performance

Die folgenden Leistungsverbesserungen wurden für UEBA in der Version 12.4.0.0 vorgenommen:

- Die Aggregations- und Akkumulationsmodelle wurden optimiert, sodass Modelle parallel generiert und gespeichert werden.
- Die stündliche Aggregationsaufgabe für die Punktzahl wurde optimiert, sodass die Aggregation und Bewertung parallel erfolgt.

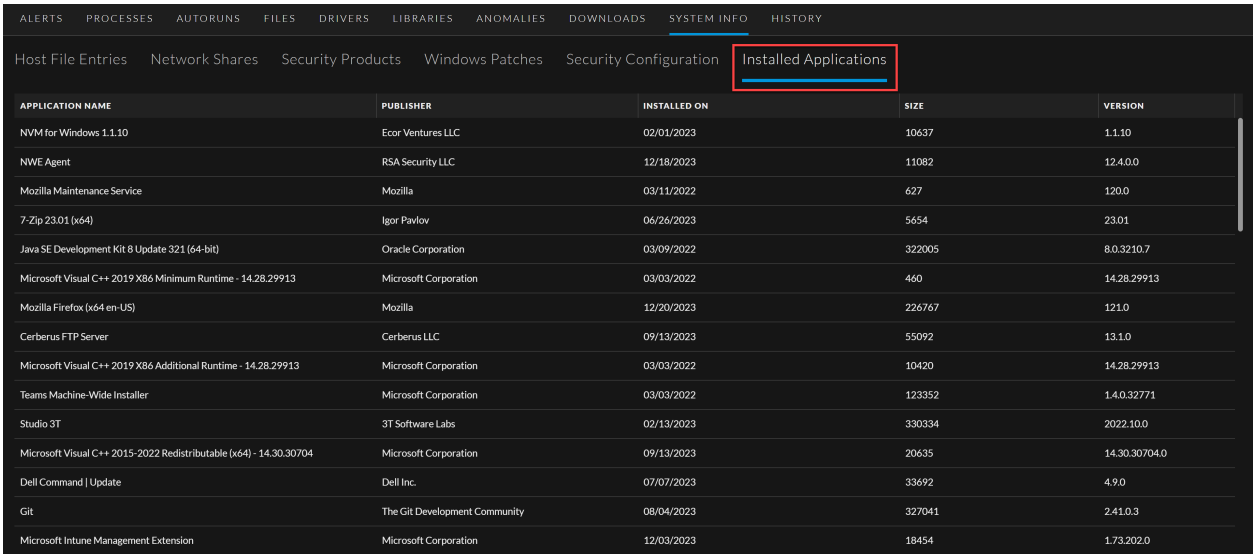
Weitere Informationen zur unterstützten Skala finden Sie im Thema **Learning Period Per Scale for 12.4** im *UEBA-Konfigurationshandbuch*.

## Endpoint

Im folgenden Abschnitt werden die neue Erweiterungen der Endpoint-Komponente beschrieben:

### Anzeigen installierter Anwendungen

Die Ansicht **Hostdetails** > **Systeminformationen** wurde erweitert, sodass Analysten und Analystinnen die Informationen zu den verschiedenen auf einem Windows-Computer installierten Anwendungen anzeigen können.

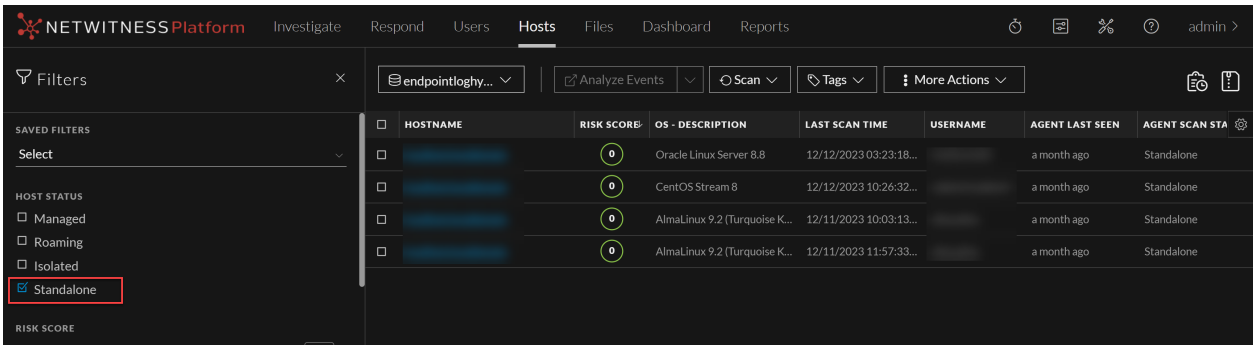



| APPLICATION NAME | PUBLISHER | INSTALLED ON | SIZE | VERSION |
|---|---|---|---|---|
| NVM for Windows 1.1.10 | Ecor Ventures LLC | 02/01/2023 | 10637 | 1.1.10 |
| NWE Agent | RSA Security LLC | 12/18/2023 | 11082 | 12.4.0.0 |
| Mozilla Maintenance Service | Mozilla | 03/11/2022 | 627 | 120.0 |
| 7-Zip 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 |

Weitere Informationen finden Sie im *NetWitness Endpoint-Benutzerhandbuch für 12.4*.

## Eigenständiger Scan für Linux-Agenten

Administratoren und Administratorinnen können Offline- oder Standalone-Scans auf Linux-Hosts durchführen, um eine Bedrohungsanalyse auf den Linux-Computern mit Air Gap durchzuführen.



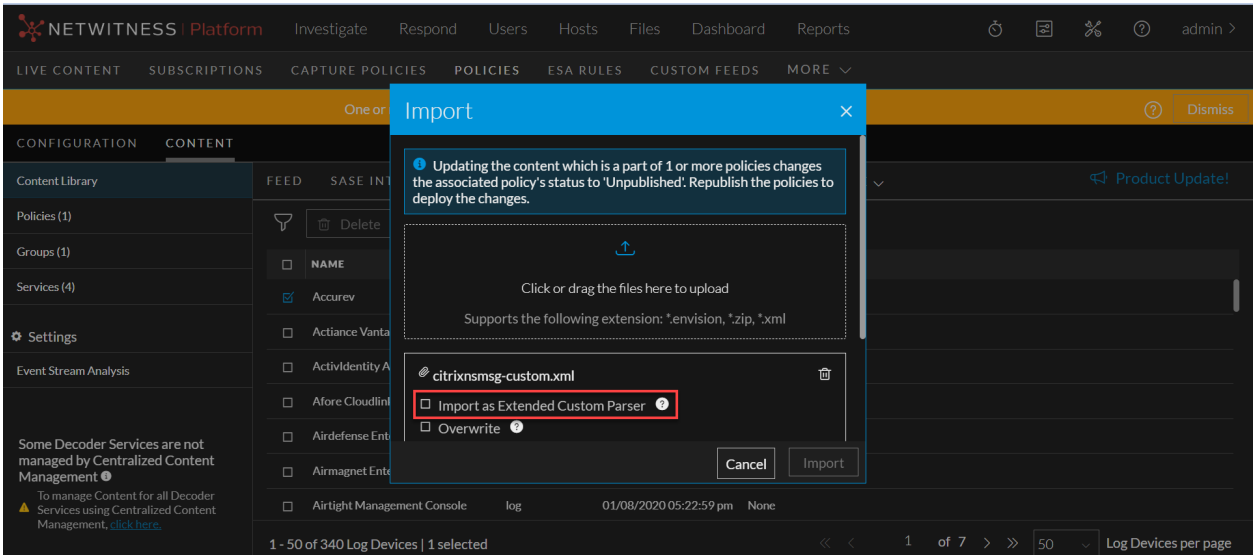

Weitere Informationen finden Sie im *NetWitness Endpoint-Benutzerhandbuch für 12.4*.

# Policy-basiertes zentralisiertes Contentmanagement (CCM)

Die folgenden Verbesserungen wurden beim CCM in der Version 12.4.0.0 vorgenommen:

## Verbesserungen der ordnungsgemäßen Funktion und Bereitstellung benutzerdefinierter Parser in Services über CCM

Einführung der Möglichkeit, einzelne XML-Inhalte (Protokollgeräte-Inhaltstyp) in die Inhaltsbibliothek zu importieren. Sie können entweder die Basisparser oder die erweiterten Parser als eigenständige XML-Datei hochladen. Beim Importieren von XML-Dateien können Sie diese optional mit dem entsprechenden Basisparser verknüpfen und sie so effektiv als Erweiterungsparser behandeln. Um ein eigenständiges XML als erweiterten Parser zu importieren, wählen Sie **Als erweiterten benutzerdefinierten Parser importieren** im Bildschirm **Importieren** aus.



Die Inhaltsbibliothek zeigt jetzt Basisparser und Erweiterungsparser als unterschiedliche Elemente an und bietet somit Nutzern und Nutzerinnen eine klare und organisierte Ansicht. Durch diese Trennung wird sichergestellt, dass Nutzer und Nutzerinnen beide Arten von Parsern innerhalb der Bibliothek problemlos identifizieren und verwalten können. Wenn einer Policy ein Erweiterungsparser hinzugefügt wird, wird der entsprechende Basisparser überdies automatisch auch in die Policy einbezogen. Diese optimierte Integration vereinfacht den Prozess für Nutzer und Nutzerinnen und macht die manuelle Verknüpfung von Basis- und Erweiterungsparsern beim Erstellen oder Bearbeiten von Richtlinien überflüssig.

Weitere Informationen finden Sie im Abschnitt **Importieren von Inhalten in die Inhaltsbibliothek** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

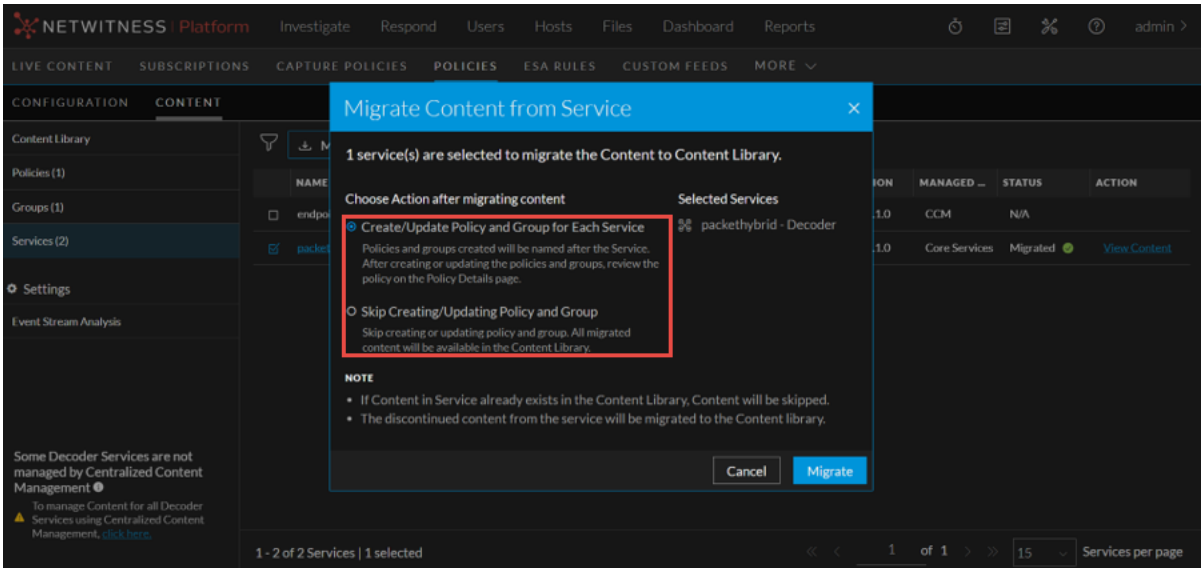
## Verbesserungen beim Entfernen eines Dienstes aus einer Gruppe

Beim Entfernen eines Dienstes aus einer Gruppe können Sie entweder den Inhalt aus dem Service löschen und dann den Service aus der Gruppe entfernen oder den Service aus der Gruppe entfernen, ohne den Inhalt zu löschen.

Weitere Informationen finden Sie in den Abschnitten **Bearbeiten einer Gruppe**, **Bearbeiten einer Policy** und **Löschen einer Policy** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

## Möglichkeit zur erneuten Migration von Inhalten aus dem Service

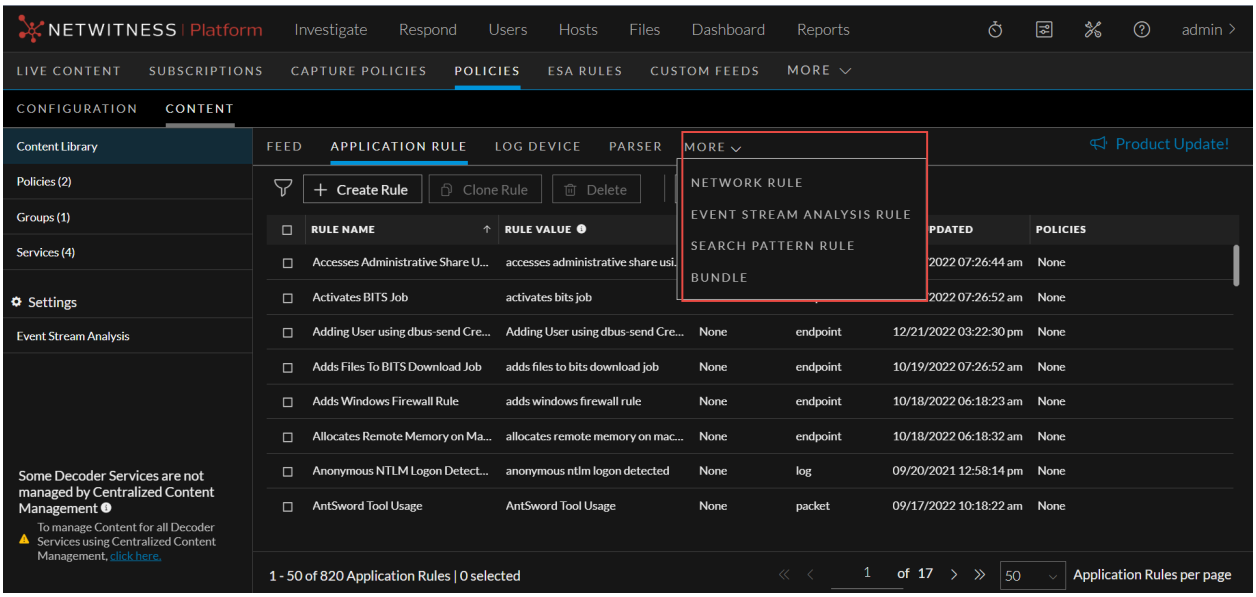
CCM wurde erweitert, um Inhalte von einem Service erneut zu migrieren, selbst wenn diese bereits migriert und/oder Gruppen und Policys zugewiesen wurden. Beim Migrieren von Inhalten von einem Service, der bereits einer Policy zugeordnet ist, können Sie optional die zugehörige Policy mit migrierten Inhalten aktualisieren. Um die vorhandene Policy und Gruppe für den Service nach der erneuten Migration des Service zu aktualisieren, werden die auf der Seite **Inhalt vom Service migrieren** verfügbaren Optionen in **Policy und Gruppen für jeden Service erstellen/aktualisieren** und **Erstellen/Aktualisieren einer Policy und Gruppe überspringen** aktualisiert.




Weitere Informationen finden Sie im Abschnitt **Migrieren von Inhalten in die Inhaltsbibliothek** im *Leitfaden zum Policy-basierten zentralisierten Contentmanagement*.

## Verbesserungen an der Benutzeroberfläche

Das Navigationsmenü **MEHR** wurde der CCM-Benutzeroberfläche hinzugefügt, um standardmäßig Bundles, Suchmuster und Integrationen anzuzeigen. Wenn Sie den Inhaltstyp aus dem Menü **MEHR** auswählen, wird dieser Inhaltstyp auf der linken Seite des Menüs **MEHR** angezeigt.

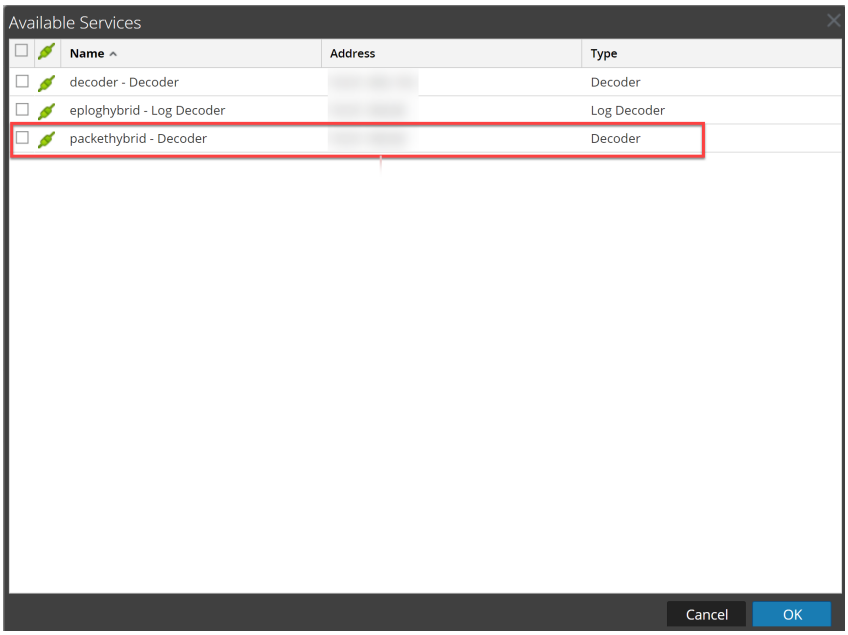


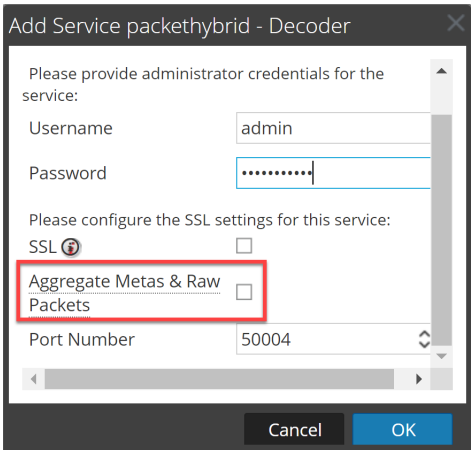

# Concentrator-, Decoder-, Log Collector- und Archiver-Services

Die folgenden Verbesserungen wurden für Concentrator-, Decoder-, Log Collector- und Archiver-Services in der Version 12.4.0.0 vorgenommen:

## Selektive Aufbewahrung für Packet Decoder

Diese Version bietet NDR-Kunden eine selektive Aufbewahrungsoption, mit der sie die erforderlichen Aufbewahrungsanforderungen drastisch senken und gleichzeitig wichtige Beweise aufbewahren können, um weiterhin führend in der Forensik und bei der Suche nach Bedrohungen zu sein. Dies wird dadurch erreicht, dass Administratoren und Administratorinnen den Packet Decoder-Host für Archiver jetzt nahtlos über die Registerkarte **(Admin)** > **Services** > **Konfiguration** Ansicht > **Allgemein** als Datenquelle konfigurieren können. Darüber hinaus können Administratoren und Administratorinnen jetzt mit der neuen Option **Metadaten und Rohpakete aggregieren** den gewünschten Aggregationstyp auswählen. Auf diese Weise können Administratoren und Administratorinnen wählen, ob der Decoder-Service nur auf Basis von Metadatenwerten oder sowohl auf Metadatenwerten als auch auf Rohpaketen aggregiert werden soll.




Weitere Informationen erhalten Sie im Thema **Hinzufügen von Packet Decoder als Datenquelle zu Archiver** im *Archiver-Konfigurationsleitfaden*.

## Möglichkeit, die Verwendung von IP-Adressen für die Standardauthentifizierung zu verwerfen

Netwitness hat die Verwendung von IP-Adressen für die Standardauthentifizierung der Windows-Sammlung eingestellt. Jetzt müssen Sie den FQDN in der Ereignisquellenadresse verwenden und beim Konfigurieren der Standardauthentifizierung einen Eintrag mit demselben FQDN in „/etc/hosts“ hinzufügen.

### Neues Dienstprogramm zum Streamen von Metadaten von Decodern an Tools von Drittanbietern

Einführung eines Beta-Dienstprogramms zum Streamen von Metadaten von Netzwerkdecodern an andere Tools von Drittanbietern, sodass die Integration von NetWitness Platform in andere Produkte vereinfacht wird. Alle oder eine Teilmenge der Metadaten können gestreamt werden, um je nach Anwendungsfall die an das Drittanbietertool gesendete Menge zu begrenzen.

Weitere Informationen finden Sie im *Installations- und Konfigurationshandbuch für Meta Export*.

## Protokollintegrationen

NetWitness Platform unterstützt die Integration der folgenden Ereignisquellen zum Sammeln und Analysieren von Protokollen. Sofern nicht anders angegeben, werden diese Services in NetWitness Platform 12.2.0.0 oder höher unterstützt.

- Zugriff auf Palo Alto Prisma
- VMware vSphere
- DeepInspect
- GCP-Windows-VM-Protokolle (über das GCP-Plug-in)

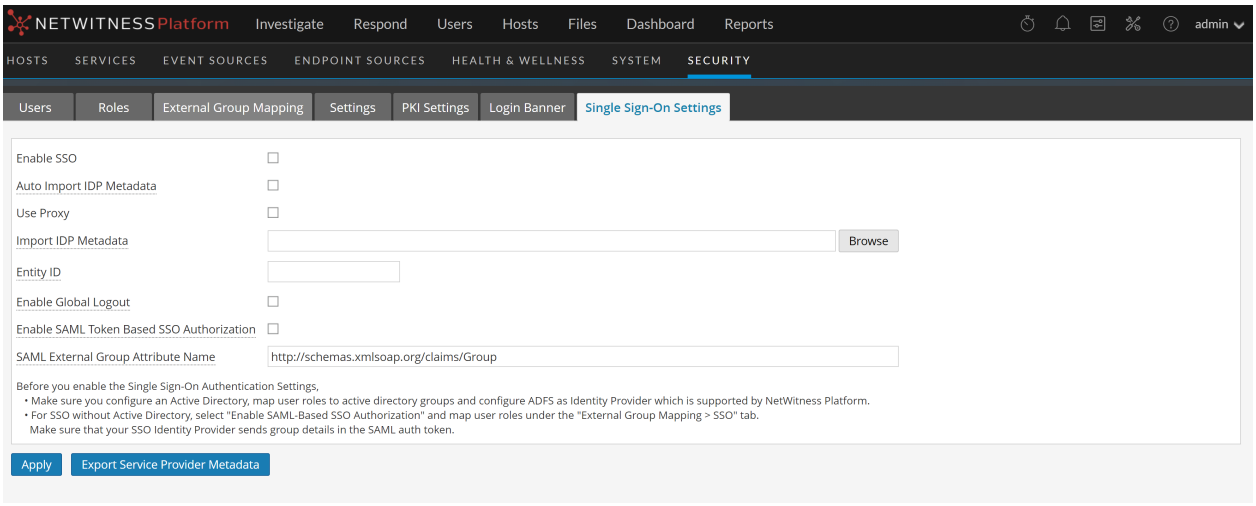
**Hinweis:** Ab Version 12.4 steht auch das VMWare-Plug-in zur Erfassung von VMWare-Ereignissen und -Aufgaben zur Verfügung.

Weitere Informationen zur Integration der Parser-Services finden Sie im NetWitness Platform – Integrationshandbuch.

## Sicherheit

### Single Sign-On (SSO)-Authentifizierung unabhängig von der Active Directory (AD)-Konfiguration in NetWitness

Ab NetWitness Platform Version 12.4 bietet NetWitness SSO, die unabhängig von der AD-Konfiguration in NetWitness ist. Es ermöglicht die Benutzerautorisierung durch Verwendung der Liste der Benutzergruppen, die in das von ADFS empfangene SAML-Authentifizierungstoken eingebettet ist, und durch Überprüfung dieser Gruppen anhand der bereits in NetWitness eingerichteten Benutzergruppen. Dadurch müssen Nutzer und Nutzerinnen keine Active Directory-Einstellungen innerhalb von NetWitness für die Benutzerauthentifizierung konfigurieren oder sich auf diese verlassen. NetWitness unterstützt jetzt sowohl Azure ADFS als auch Microsoft ADFS.




Weitere Informationen finden Sie im Thema **Einrichten der Single-Sign-On-Authentifizierung** im *Handbuch zur Systemsicherheit und Benutzerverwaltung*.

# Sicherheitskorrekturen

Weitere Informationen zu Sicherheitskorrekturen finden Sie unter https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#security.

# Upgradepfade

Die folgenden Upgradepfade werden für NetWitness 12.4.0.0 unterstützt:

- NetWitness 12.3.1.0 zu 12.4.0.0
- NetWitness 12.3.0.0 zu 12.4.0.0
- NetWitness 12.2.0.1 zu 12.4.0.0
- NetWitness 12.2.0.0 zu 12.4.0.0

Weitere Informationen zum Upgrade auf 12.4.0.0 finden Sie unter Upgrade-Leitfaden für NetWitness 12.4.0.0

**WICHTIG:** Wenn Sie ein Upgrade von den Versionen 11.7.x (Service Packs) oder 11.7.x.x (Patches) auf die Version 12.4.0.0 durchführen möchten, müssen Sie zunächst ein Upgrade auf die Version 12.2.0.0 oder 12.3.0.0 durchführen, bevor Sie auf 12.4 aktualisieren.

# Lebenszyklus der Produktversion von NetWitness Platform

Eine Liste der Versionen, die das Ende des Primärsupports (EOPS) erreichen, finden Sie unter Produktversionslebenszyklus von NetWitness Platform.

# Neuheiten in früheren Versionen (11.7 bis 12.3.1.0)

Der Abschnitt enthält neue Funktionen und Verbesserungen für alle unterstützten Vorgängerversionen.

Weitere Informationen finden Sie unter https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-7-to-12-1-1/ta-p/695650.

# In Version 12.4.0.0 behobene Probleme

In diesem Abschnitt werden in der Version 12.4.0.0 behobene Probleme aufgeführt.

Weitere Informationen zu behobenen Problemen finden Sie in der Spalte „Behobene Version“ in der Liste bekannter Probleme in NetWitness® Platform (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) im NetWitness Community Portal.

## Korrekturen beim policy-basierten zentralisierten Content-Management (CCM)

| Rückverfolgungsnummer | Beschreibung |
|---|---|
| ASOC-142018 | Die von CCM veröffentlichten Protokollgeräte-Contents werden nicht deaktiviert, wenn Contents für einen Dienst gelöscht werden. |
| ASOC-141524 | Die ESA-Regeln konnten durch Bearbeiten oder Aktualisieren der ESA-Regel nicht gespeichert werden. In den NetWitness-UI- und SA-Protokollen wurde beim Speichern der Regel eine Laufzeitausnahme angezeigt. Außerdem wurde beim Troubleshooting festgestellt, dass der **RSA OSINT Non-IP Threat Intel Feed** keine eindeutige ID mit der Policy verknüpft hatte und in mehreren Dokumenten in den Content-Policy-Sammlungen vorkam. |

# Bekannte Probleme in Version 12.4.0.0

Probleme, die in dieser Version weiterhin ungelöst sind, sind in der Liste der bekannten Probleme der NetWitness® Platform im NetWitness-Community-Portal dokumentiert:
https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

# Build-Nummern für 12.4.0.0-Komponenten

Die folgende Tabelle enthält die Build-Nummern für die verschiedenen Komponenten von NetWitness Platform 12.4.0.0.

| Komponente | Versionsnummer |
|---|---|
| NetWitness Admin-Server | rsa-nw-admin-server-12.4.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm |
| NetWitness Inhalte zu erweiterten Analysen | rsa-nw-advanced-analytics-content-12.4.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm |
| NetWitness Erweiterter Analyseserver | 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-Service | 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 Beschreibung der Komponente | rsa-nw-component-descriptor-12.4.0.0-2402080831.5.a403c19.el8.noarch.rpm |
| NetWitness Concentrator | rsa-nw-concentrator-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Konfigurationsmanagement | rsa-nw-config-management-12.4.0.0-2402050947.5.b7e9f64.el8.noarch.rpm |
| NetWitness Konfigurationsserver | rsa-nw-config-server-12.4.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm |
| NetWitness-Konsole | 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 Korrelationsserver (ESA) | rsa-nw-correlation-server-12.4.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm |
| NetWitness Dashboard-Inhalt | 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-Analyseinhalte | 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 Bereitstellung-Upgrade | rsa-nw-deployment-upgrade-12.4.0.0-2402050945.5.1903a3b.el8.noarch.rpm |
| NetWitness Endpoint-Agenten | 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 Endpunkt-Decoder-Analyseinhalte | 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 Integrationsserver | 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-Webserver | rsa-nw-legacy-web-server-12.4.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm |
| NetWitnessLizenzserver | 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-Inhalte | 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-Analyseinhalte | rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm |
| NetWitness Log Decoder-Basisinhalte | 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-Exportdienstprogramm | rsa-nw-metaexport-utility-12.4.0.0-110124.5.el8.x86_64.rpm |
| NetWitness Server für Messwerte | 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 Orchestrierungs-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 Platzhalter | 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-Konfigurationsserver | 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-Ausgabe | rsa-nw-presidio-output-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm |
| NetWitness Presidio-Benutzeroberfläche | 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 Wiederherstellungstools | 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 Antwortserver | rsa-nw-respond-server-12.4.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm |
| NetWitness Antwortaktionsserver | 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 Sicherheits-CLI | rsa-nw-security-cli-12.4.0.0-2401091103.5.18ab320.el8.noarch.rpm |
| NetWitness Sicherheitsserver | 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-Berichts-Plugins | rsa-nw-sosreport-plugins-12.4.0.0-2401162235.5.af21a76.el8.noarch.rpm |
| NetWitness SMS-Laufzeit 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 Quellserver | rsa-nw-source-server-12.4.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm |
| NetWitness Quellserverinhalt | rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm |
| NetWitness-Benutzeroberfläche | 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 |

# Hilfe zu NetWitness Platform

## Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

| Dokumentation | Standort-URL |
|---|---|
| NetWitness Platform – Masterinhaltsverzeichnis | https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation |
| NetWitness Platform 12.4.0.0 Produktdokumentation | https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation |
| Leitfaden zum Upgrade auf NetWitness Platform 12.4.0.0 | https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308 |
| NetWitness Analytics in der Cloud | Weitere Informationen zu neuen Funktionen und Verbesserungen in Versionen von NetWitness Analytics in der Cloud finden Sie im folgenden Abschnitt „Neuheiten“:<br>Informationen zu UEBA Cloud finden Sie unter https://docs.netwitness.com/netwitnessueba/release_information/whats_new/.<br>Informationen zu Insight finden Sie unter https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/. |

## Ressourcen zur Selbsthilfe

Es gibt mehrere Optionen, die Ihnen bei der Installation und Verwendung von NetWitness bei Bedarf Hilfestellung bieten:

- Weitere Informationen zu allen Aspekten von NetWitness finden Sie hier: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Benutzen Sie die Felder **Search** und **Create a Post** im NetWitness Community-Portal, um hier spezifische Informationen zu finden: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- Weitere Informationen finden Sie in der NetWitness Wissensdatenbank: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- Weitere Informationen finden Sie im Abschnitt „Troubleshooting” in den Leitfäden.

- Siehe auch NetWitness® Platform-Blogbeiträge.
- Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den NetWitness Support.

## NetWitness Support kontaktieren

Wenn Sie den NetWitness-Support kontaktieren, sollten Sie sich an Ihrem Computer befinden. Bereiten Sie sich darauf vor, die folgenden Informationen zu geben:

- Die Versionsnummer des verwendeten NetWitness Platform-Produkts oder der Appliance.
- Typ der verwendeten Hardware

Verwenden Sie die folgenden Kontaktinformationen, wenn Sie Fragen haben oder Unterstützung benötigen.

| | |
|---|---|
| NetWitness Community Portal | https://community.netwitness.com<br>Klicken Sie im Hauptmenü auf **Support > Portal für Support-Fälle > Meine Fälle anzeigen**. |
| Internationale Kontakte (So kontaktieren Sie den 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

Melden Sie sich an, um Zugang zu NetWitness-Kursen und zusätzlichen Ressourcen zu NetWitness Educational Services und Schulungen zu erhalten.

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

# Feedback zur Produktdokumentation

Sie können eine E-Mail an feedbacknwdocs@netwitness.com senden, um Feedback zu den Dokumentation der NetWitness Platform zu geben.