RSA NETWITNESS® PLATFORM

# Leitfaden für die ersten Schritte

für RSA NetWitness® Platform 11.3

## Kontaktinformationen

Der RSA Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

## Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

## Lizenzvereinbarung



## Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Nutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

## Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren müssen beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

## Verteilung

Dell ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

June 2019

# Inhalt

# Erste Schritte mit NetWitness Platform

## Übersicht

RSA NetWitness® Platform ist eine leistungsstarke Suite zur Erkennung von Bedrohungen, mit der Security Operation Center (SOC) Bedrohungen schnell ermitteln, priorisieren und selektieren können. NetWitness Platform unterstützt Sie beim Isolieren und Beheben von bekannten Bedrohungen sowie von denen, die Ihnen bisher unbekannt waren. Es bietet umfassende Einblicke in Pakete, Protokolle und Endpunkte, die einen bisher unerreichten Einblick in Ihr Unternehmen oder Business liefern.

NetWitness Platform ist trotz seiner Leistungsfähigkeit für Tier-1-Analysten einfacher zu verwenden, da es den Prozess der Identifizierung und Priorisierung von verdächtigen Bedrohungen automatisiert. Tier-2- und Tier-3-Analysten können Bedrohungen ermitteln und aufspüren, indem sie nach Ereignissen suchen, die Ergebnisse filtern und anschließend die Ereignisse mit Rekonstruktions- und Analysetools untersuchen.

## Architektur

RSA NetWitness Platform ist ein dezentralisiertes und modulares System, das äußerst flexible Bereitstellungsarchitekturen ermöglicht, die anhand der Anforderungen des Unternehmens skaliert werden können. Mit NetWitness Platform können Administratoren drei Arten von Daten aus der Netzwerkinfrastruktur erfassen: Paketdaten, Protokolldaten und Endpunktdaten. Die Architektur weist folgende Hauptmerkmale auf:

- **Dezentralisierte Datensammlung**. Die **Decoder** nimmt Paketdaten auf und der **Log Decoder** nimmt Protokolldaten auf. Decoder analysieren und rekonstruieren den gesamten Netzwerkdatenverkehr aus den Schichten 2 bis 7 oder Protokoll- und Ereignisdaten aus Hunderten von Geräten und Ereignisquellen, einschließlich NetWitness Endpoint-Daten (falls installiert und konfiguriert). Der **Concentrator** indiziert aus dem Netzwerk extrahierte Metadaten oder Protokolldaten und stellt sie für unternehmensweite Abfragen und Echtzeitanalysen zur Verfügung. Er erleichtert auch das Reporting und die Erzeugung von Warnmeldungen. Der **Broker** führt die von anderen Geräten und Ereignisquellen erfassten Daten zusammen. Broker führen Daten aus konfigurierten Concentrators zusammen; Concentrators führen Daten aus Decodern zusammen. Somit ist ein Broker ein Bindeglied zwischen mehreren Echtzeitdatenspeichern, die in den verschiedenen Decoder/Concentrator-Paaren in der gesamten Infrastruktur enthalten sind.
- **Warnung in Echtzeit**. Der NetWitness Platform **Event Stream Analysis (ESA)**-Host bietet erweiterte Streamanalysen wie Korrelation und komplexe Ereignisverarbeitung mit hohen Durchsätzen und niedriger Latenz. Er kann große Mengen unterschiedlicher Ereignisdaten aus Concentrators verarbeiten. ESA verwendet eine erweiterte Ereignisverarbeitungssprache, mit der Analysten die Filterung, Zusammenführung, Verkettung, Mustererkennung und Korrelation über mehrere unterschiedliche Ereignisstreams ausdrücken können. Event Stream Analysis unterstützt die Durchführung einer leistungsstarken Erkennung von Incidents und Erzeugung von Warnmeldungen.
- **Echtzeitanalysen** (automatische Analyse von Ereignissen). Die Funktion der automatisierten Bedrohungserkennung von RSA umfasst vorkonfigurierte ESA Analytics-Module zur Erkennung von Befehls- und Datenverkehr.

- **NetWitness-Server**. Das NetWitness-Server bietet Reporting, Ermittlung, Administration und andere Aspekte der Benutzeroberfläche.
- **Kapazität:** NetWitness Platform verfügt über eine mit DACs (Direct-Attached Capacity) oder SANs (Storage Area Network) kompatible Architektur mit modularer Kapazität, die sich an die kurzfristigen Ermittlungsanforderungen sowie die längerfristigen Analyse- und Datenaufbewahrungsanforderungen des Unternehmens anpasst.

NetWitness Platform bietet Flexibilität für große Bereitstellungen. Sie können die Architektur mit mehreren Dutzend physischen Hosts oder einem einzigen physischen Host basierend auf den Besonderheiten der performance- und sicherheitsbezogenen Anforderungen des Kunden entwerfen. Darüber hinaus wurde das gesamte NetWitness Platform-System so optimiert, dass es in einer virtualisierten Infrastruktur ausgeführt werden kann.

Die Systemarchitektur besteht aus folgenden Hauptkomponenten: Decoder, Broker, Concentrator, Archiver, ESA und Warehouse Connector. NetWitness Platform-Komponenten können gemeinsam als ein System oder einzeln verwendet werden.

- Für eine SIEM-Implementierung (Security, Information and Event Management) sind in der Basiskonfiguration folgende Komponenten erforderlich: Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA) und der NetWitness-Server.
- Bei einer Forensikimplementierung erfordert die Basiskonfiguration folgende Komponenten: Decoder, Concentrator, Broker, ESA, Malware Analysis und Endpoint Log Hybrid. Der Antwortserver-Dienst ist ebenfalls erforderlich und wird verwendet, um Warnmeldungen zu priorisieren.

Die Tabelle enthält eine Übersicht über jede Hauptkomponente:

| Systemkomponente | Beschreibung |
|---|---|
| **Decoder/Log Decoder** | • NetWitness Platform sammelt Paket-, Protokoll- und Endpunktdaten.<br>• Paketdaten, d. h. Netzwerkpakete, werden mithilfe des Decoder über den Netzwerkanschluss oder Span-Port erfasst, der normalerweise als Ausgangspunkt in einem Unternehmensnetzwerk festgelegt wird.<br>• Ein Log Decoder kann vier verschiedene Protokolltypen erfassen: Syslog, ODBC, Windows-Ereignisverwaltung und Flatfiles.<br>• Windows-Ereignisverwaltung bezieht sich auf die Windows 2008-Erfassungsmethodologie und Flatfiles können über SFTP abgerufen werden.<br>• Beide Decoder-Typen nehmen Transaktionsrohdaten auf, die erweitert, ausgebucht und im Warehouse oder anderen NetWitness Platform-Komponenten zusammengeführt werden.<br>• Das Verfahren zum Aufnehmen und Analysieren von Transaktionsdaten ist ein dynamisches und offenes Framework. |

| Systemkomponente | Beschreibung |
|---|---|
| **Endpoint Log Hybrid** | • Erfasst und managt Endpunktdaten (Host) von Windows-, Mac- oder Linux-Hosts.<br>• Zeichnet Daten über jede kritische Aktion auf, z. B. Prozesse, Dateien, Änderungen an der Registrierung, Netzwerkverbindungen und Interaktionen mit der Nutzerkonsole.<br>• Sammelt Protokolle von Windows-Hosts, wenn die Sammlung konfiguriert ist.<br>• Erzeugt Metadaten zur Korrelation von Endpunktdaten mit Sitzungen aus anderen Ereignisquellen, z. B. Protokollen und Netzwerk.<br>• Durchführung von Live-Speicheranalysen, Analysen des Netzwerkverkehrs und der Erkennung von verdächtigem Nutzerverhalten |
| **Concentrator** | • Bietet Index und Abfrage bei NetWitness-Sammlungen.<br>• Kann optional Daten an ESA weiterleiten. |
| **Broker** | • Verteilt Zugriff auf die NetWitness-Sammlung auf viele Concentrator oder Archiver, sodass die gesamte NetWitness Platform Enterprise als eine einzelne Sammlung angezeigt wird. |
| **Archiver** | • Der Archiver-Service ermöglicht die langfristige Protokollarchivierung durch Indexierung und Komprimierung von Protokolldaten und das Senden der Daten an den Archivierungsspeicher.<br>• Der Archivierungsspeicher wurde für eine langfristige Datenaufbewahrung und Compliance-Reporting optimiert.<br>• Archiver speichert Rohdatenprotokolle und Protokollmetadaten von Log Decodern für die langfristige Aufbewahrung. Zur Speicherung wird DAC (Direct-Attached Capacity) verwendet.<br>**Hinweis:** Rohdatenpakete und Paketmetadaten werden nicht im Archiver gespeichert. |

| Systemkomponente | Beschreibung |
| --- | --- |
| **Event Stream Analysis (ESA)** | • Der ESA-Service (Event Stream Analysis) bietet Event Stream-Analysen wie Korrelation und komplexe Ereignisverarbeitung mit hohen Durchsätzen und niedriger Latenz. Er kann große Mengen unterschiedlicher Ereignisdaten aus Concentrators verarbeiten.<br>• ESA verwendet eine erweiterte Ereignisverarbeitungssprache, mit der Nutzern die Filterung, Aggregation, Verknüpfung, Mustererkennung und Korrelation über mehrere verteilte Ereignisstreams ausdrücken können.<br>• ESA erleichtert die leistungsstarke Erkennung von Incidents und Erzeugung von Warnmeldungen.<br>• Die Funktion der automatisierten Bedrohungserkennung von RSA umfasst vorkonfigurierte ESA Analytics-Module zur Erkennung von Befehls- und Datenverkehr. |

## Core- und Downstream-Komponenten

In NetWitness Platform nehmen die Core-Services Daten auf und analysieren sie, erzeugen Metadaten und führen dann die erzeugten Metadaten mit den Rohdaten zusammen. Zu den Core-Services zählen Decoder, Log Decoder, Concentrator und Broker. Downstreamsysteme verwenden Daten, die auf Core-Services zu Analysezwecken gespeichert sind. Die Vorgänge von Downstreamservices sind somit abhängig von den Core-Services. Die Downstreamsysteme sind Archiver, ESA, Malware Analysis, Ermittlung und Reporting.

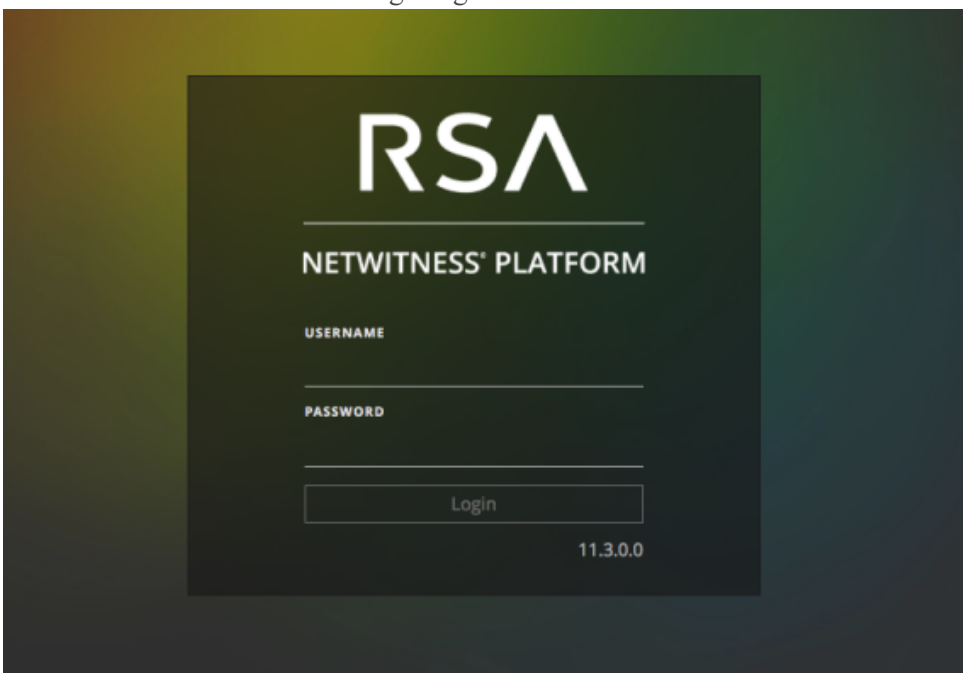
Zwar können die Core-Services auch ohne die Downstreamsysteme eine gute Analyselösung betreiben und bereitstellen, aber die Downstreamkomponenten umfassen zusätzliche Analysefunktionen. ESA bietet eine Echtzeitkorrelation über Sitzungen und Ereignisse hinweg sowie zwischen verschiedenen Typen von Ereignissen, z. B. Protokoll-, Paket- und Endpunktdaten. Ermittlung bietet Möglichkeiten zum Drill-down in Datenbeständen, zum Untersuchen von Ereignissen und Dateien und zum Rekonstruieren von Ereignissen in einer sicheren Umgebung. Der Malware Analysis-Service ermöglicht automatisierte Echtzeitprüfungen auf schädliche Aktivitäten in Netzwerksitzungen und zugehörigen Dateien.

# Anmeldung bei NetWitness Platform

Die Anmeldung bei RSA NetWitness® Platform kann je nach Umgebung unterschiedlich sein. Sie können über ein internes Nutzerkonto oder ein externes Nutzerkonto verfügen. Interne Benutzerkonten sind für NetWitness Platform lokal und interne Nutzer können sich bei NetWitness Platform anmelden und erhalten rollenbasierte Berechtigungen. Externe Benutzerkonten werden außerhalb vonNetWitness Platform authentifiziert und NetWitness Platform-Rollen zugeordnet. Wenn Sie ein externer Nutzer sind und nicht auf NetWitness Platform zugreifen oder die Informationen anzeigen können, die Sie benötigen, wenden Sie sich an Ihren Systemadministrator. Ihr Administrator kann Ihrem Konto die entsprechenden Rollen zuweisen.

**Hinweis:** NetWitness Platform unterstützt moderne (oder aktuelle) Versionen von Google Chrome, Mozilla Firefox und Apple Safari. Es ist möglich, einen anderen Browser zu verwenden, aber einige Funktionen funktionieren möglicherweise nicht wie erwartet.

1. Verwenden Sie ein von Ihrem Administrator bereitgestelltes Symbol oder geben Sie Folgendes in Ihren Webbrowser ein:
   `https://<hostname or IP address>/login`
   wobei `<hostname or IP address>` der Hostname oder die IP-Adresse Ihres NetWitness-Servers ist.
   Der-Anmeldebildschirm wird angezeigt.




2. Geben Sie den Nutzernamen und das Passwort ein und klicken Sie auf **Anmelden**.
   Wenn Ihre Anmeldung erfolgreich ist, werden Sie auf der Landingpage angemeldet, die in Ihren Benutzereinstellungen angegeben ist.

### Wenn Sie gesperrt sind:

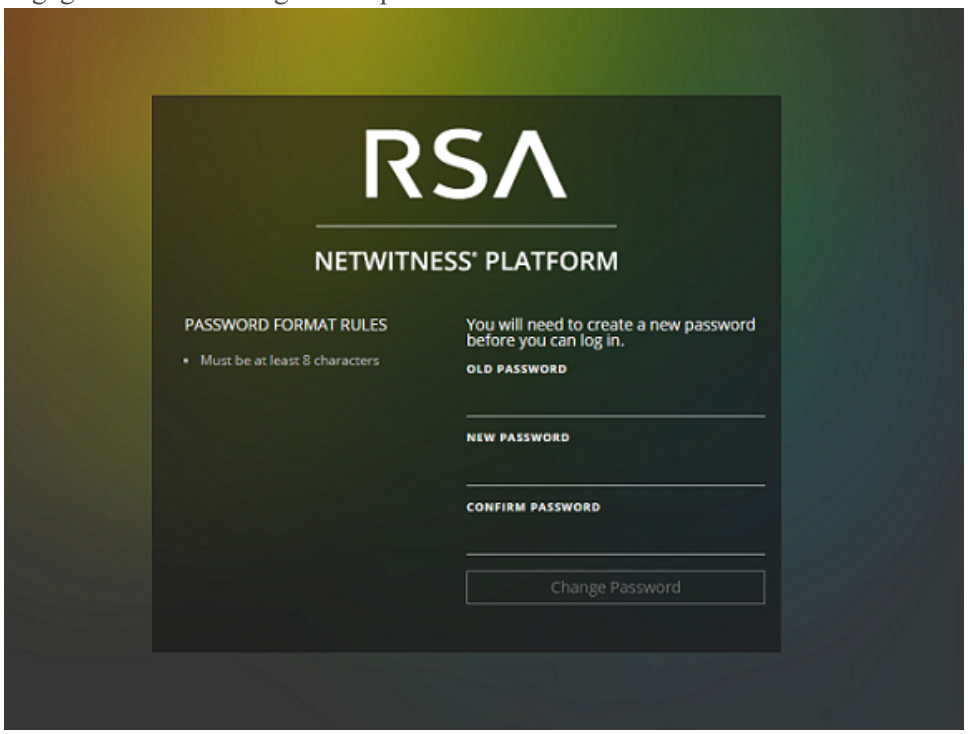
**Hinweis:** Diese Informationen gelten nur für interne Konten. Es gilt nicht für Active Directory- oder PAM-Konten.

Wenn Sie zu oft versuchen, sich mit einem falschen Nutzernamen oder Passwort anzumelden, wird Ihr Konto gesperrt. Wenden Sie sich an Ihren Administrator, um Ihr Konto zu entsperren.

### Wenn Sie ein neues Konto haben oder Ihr Konto abgelaufen ist:

**Hinweis:** Dieses Verfahren gilt nur für interne Konten. Es gilt nicht für Active Directory- oder PAM-Konten.

1. Geben Sie im Dialogfeld zum Erstellen eines neuen Passworts das alte Passwort ein. Geben Sie dann ein neues Passwort ein und bestätigen Sie es. Die Regeln zum Passwortformat (definiert von Ihrem Systemadministrator) finden Sie auf der linken Seite und Ihr neues Passwort muss den angegebenen Formatregeln entsprechen.




2. Klicken Sie auf **Passwort ändern**.

### Wenn Sie nicht den richtigen Zugriff auf NetWitness Platform haben:

Wenn Sie sich erfolgreich anmelden können, die erforderlichen Informationen aber nicht angezeigt werden, muss Ihrem Nutzerkonto möglicherweise eine Nutzerrolle zugewiesen werden. Wenden Sie sich an Ihren Administrator, um Hilfestellung zu erhalten.

## Abmelden von NetWitness Platform

### So melden Sie sich von der Ansicht „Reagieren“ und den „Untersuchen“-Ansichten ab:

1. Wählen Sie im Balken Hauptmenü die Option  aus.
2. Klicken Sie in den Nutzereinstellungen auf **Abmelden**.

### So melden Sie sich von allen anderen Ansichten ab:

Wählen Sie im Balken Hauptmenü die Option  **> Abmelden** aus.

# Ändern des Passworts

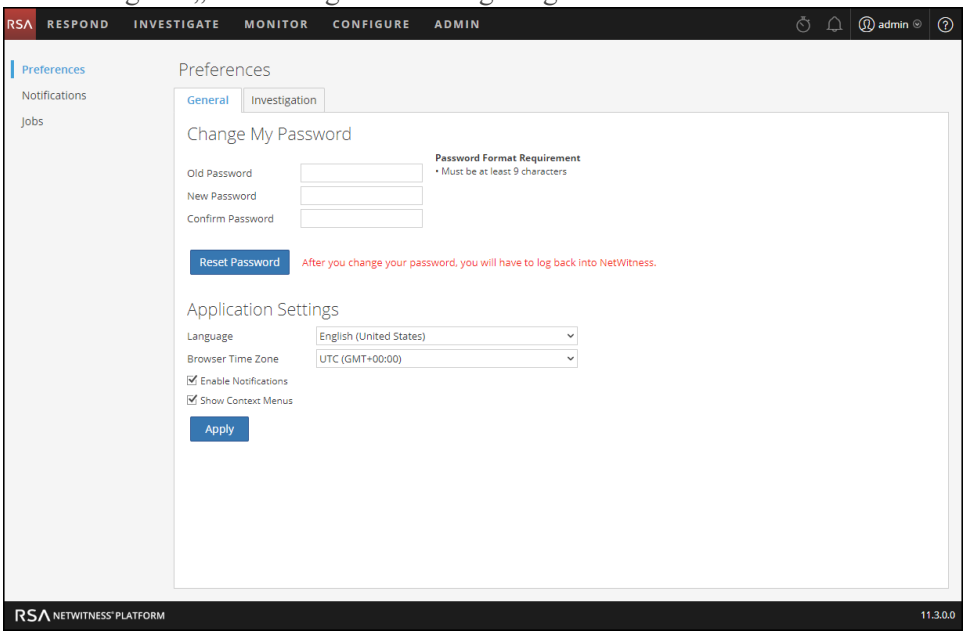
Sie können das Passwort, das Sie für die RSA NetWitness® Platform-Authentifizierung verwenden, jederzeit in Ihren Nutzereinstellungen ändern. Ihr Administrator definiert die entsprechenden Anforderungen an die Passwortstärke für Ihr NetWitness Platform-Passwort, wie z B. minimale Passwortlänge und minimale Anzahl von Großbuchstaben, Kleinbuchstaben, Dezimalstellen, nicht lateinischen Buchstaben und Sonderzeichen. Diese Anforderungen werden angezeigt, wenn Sie Ihr Passwort ändern.

**Hinweis:** Dieses Verfahren gilt nur für interne Konten. Es gilt nicht für Active Directory- oder PAM-Konten.

### So ändern Sie Ihr Passwort:

1. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie für die meisten Ansichten, z. B. „Untersuchen“, „Überwachung“, „Konfigurieren“ oder „Admin“, > **Profil** aus.
   - Wählen Sie in der Ansicht „Reagieren“ und einigen „Untersuchen“-Ansichten (Ereignisanalyse, Hosts, Dateien und Nutzer) aus und klicken Sie im Dialogfeld „Nutzereinstellungen“ auf **Eigenes Passwort ändern**.

   Das Dialogfeld „Einstellungen“ wird angezeigt.




2. Geben Sie im Abschnitt **Eigenes Passwort ändern** das Passwort ein, das Sie zur Authentifizierung in NetWitness Platform verwendet haben in das Feld **Altes Passwort** ein.
3. Geben Sie im Feld **Neues Passwort** das Passwort ein, das Sie bei der nächsten Anmeldung verwenden möchten.
4. Geben Sie das neue Passwort im Feld **Passwort bestätigen** erneut ein.

5. Klicken Sie auf **Passwort zurücksetzen**.
   Sie werden von NetWitness Platform abgemeldet, damit die Änderungen wirksam werden. Das neue Passwort wird bei der nächsten Anmeldung bei NetWitness Platform wirksam.

# Identifizieren Ihrer Rolle

Die hier aufgeführten Rollen sind die typischen Rollen oder Funktionen von Security Operations Center (SOC). Bestimmen Sie die Rolle oder die Rollen, die Sie im SOC durchführen Sie können diese Funktionen als Leitfaden verwenden, um zu entscheiden, wie Sie RSA NetWitness® Platform einrichten und darin navigieren können, damit Sie Ihren Aufgaben effizienter durchführen können.

SOC Team

SOC Manager (SOC Management and Reporting)

- Managen der SOC-Bereitschaft
- Reagieren auf Incidents
- Reagieren auf Datenschutzverletzungen

Data Privacy Officer

- Überwachen und Schützen von datenschutzrelevanten und vertraulichen Informationen

Incident Reponder (T1 Analyst)

- Reagieren auf Incidents
- Korrigieren von Incidents

Threat Hunter (T2/T3 Analyst)

- Ermitteln von Bedrohungen
- Durchführen forensischer Analysen
- Empfehlen von Problemen, die korrigiert werden sollten
- Korrigieren von Problemen

Content Expert (Threat Intelligence)

- Durchführen von Ermittlungen zu neuen Bedrohungsinformationen
- Evaluieren und erstellen neuer Feeds
- Erstellen von Korrelationsregeln zur Markierung von Indikatoren oder Infizierungen

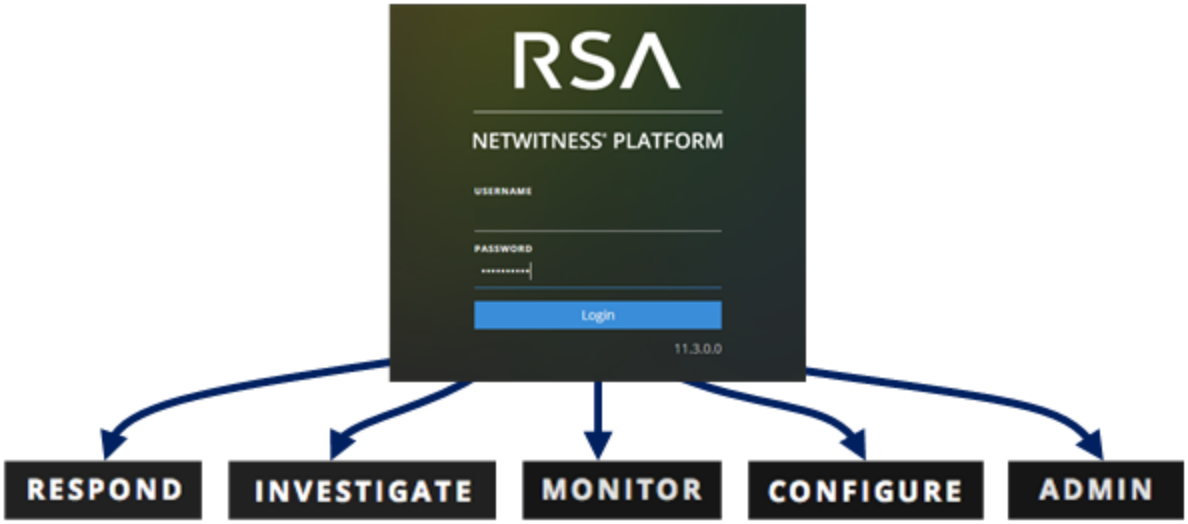
System Administrator

- Installieren und Konfigurieren von Geräten und Software
- Managen des Benutzerzugriffs
- Monitoring und Anpassen der Performance
- Backup und Wiederherstellen von Daten
- Managen von Speicher und Archiven
- Aktualisieren der Software

- Erstellen von Berichten zur Einhaltung behördlicher Auflagen

# Navigation in NetWitness Platform

Die RSA NetWitness® Platform-Anwendung ist in fünf Hauptfunktionsbereiche unterteilt; sogenannten Ansichten, die auf typischen SOC-Rollen (Security Operation Center) basieren.




- **Reagieren**: Diese Ansicht ist für Incident-Experten bestimmt, die eine Liste der priorisierten Incidents zur Selektion anzeigen können. Diese Vorfälle stammen aus Quellen wie ESA-Regeln, NetWitness Endpoint, oder ESA Analytics-Modulen für die automatisierte Bedrohungserkennung. Sie können hier ebenfalls alle Warnmeldungen von NetWitness Platform anzeigen.
  Für Nutzer der Legacy-Version 10.6 wurde diese Ansicht als die Ansicht „Incident-Management“ bezeichnet. Die Liste der Warnmeldungen in der Ansicht „Reagieren“ ersetzt die Ansicht „ESA 10.6-Warnmeldungen > Übersicht“.
- **Ermittlung**: Diese Ansicht ist in erster Linie für Advanced Threat Hunters gedacht, die die manuelle Suche nach Bedrohungen mithilfe von NetWitness Platform-Metadaten, Rohereignisdaten und Ereignisrekonstruktion und -analyse bevorzugen. Incident Responder verwenden diese Ansicht ebenfalls, um Details zu Ereignissen zu dem untersuchten Incident zu erhalten. Threat Hunters und Incident-Experten können die forensische Ereignisrekonstruktion und Ereignisanalysefunktionen in dieser Ansicht verwenden.
- **Monitor**: Diese Ansicht ist für alle Nutzer. Sie können verschiedene Bereiche des Dashboards und Berichte je nach Ihren Nutzerberechtigungen anzeigen. NetWitness Platform öffnet diese Ansicht standardmäßig.
  Für Nutzer der Legacy-Version 10.6 ist dies die Ansicht „Dashboard“.
- **Konfigurieren**: Diese Ansicht ist für Mitarbeiter im Bereich „Bedrohungsdaten“ (Contentexperten) verfügbar, die Datenquellen und Eingaben für NetWitness Platform konfigurieren. Contentexperten nutzen diesen Bereich, um Live-Inhalte herunterzuladen und zu verwalten. Sie können ebenfalls Incident- und ESA-Regeln erstellen und managen.
  Nutzer der Legacy-Version 10.6 enthält diese Ansicht „Live“, „Incidents > Konfigurieren“ und „Warnmeldungen > Konfigurieren“ aus der vorherigen Version.

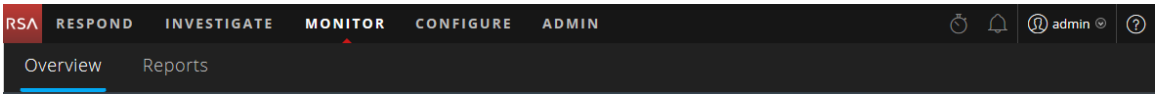
- **ADMIN**: Diese Ansicht ist für Systemadministratoren verfügbar, die die gesamte Anwendung einrichten und verwalten.
  Für Nutzer der Legacy-Version 10.6 entspricht dies der Ansicht „Administration“ ohne die Abschnitte, die zur Ansicht „Konfigurieren“ hinzugefügt wurden.

## Zugriff auf Hauptansichten

Die Optionen, mit denen die Hauptansichten geöffnet werden, werden oben im Browserfenster aufgeführt. Mit den entsprechenden Berechtigungen können Sie auf die folgenden Ansichten oben im Browserfenster jederzeit zugreifen.

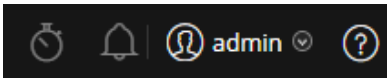

## Sekundäre Menüs

Einige Ansichten verfügen über sekundäre Kontextmenüs mit weiteren Ansichten, die Sie auswählen können. Diese Ansichten unterscheiden sich entsprechend der Aufgaben, die Sie durchführen können. Das folgende Beispiel zeigt das Menü Monitor.



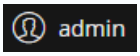
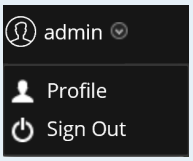

## Zusätzliche Optionen

Neben den drei Ansichten stehen zusätzliche Optionen oben im Browserfenster zur Verfügung, die für die gesamte Anwendung anwendbar sind.




In der folgenden Tabelle werden diese häufig genutzten Optionen beschrieben:

| Häufig genutzte Optionen | Name | Beschreibung |
|---|---|---|
|  | Jobs | Klicken Sie in den Ansichten Ermittlung, Monitor, Konfigurieren und ADMIN auf dieses Symbol, um Ihre Jobs in der Jobkurzübersicht anzuzeigen und zu managen. Jobs sind nach Bedarf oder geplante Aufgaben, deren Abschluss einige Zeit in der NetWitness Platform-Anwendung in Anspruch nimmt. |

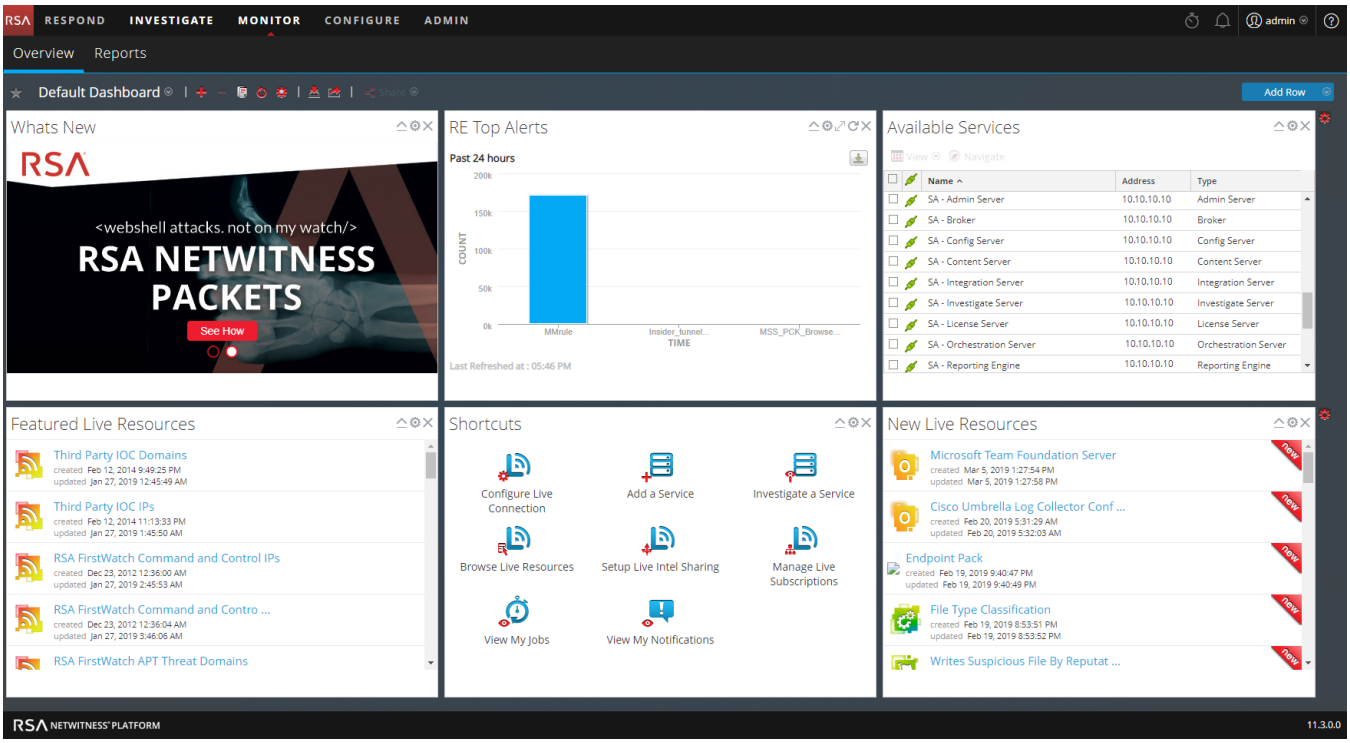
| Häufig genutzte Optionen | Name | Beschreibung |
|---|---|---|
|  | Benachrichtigungen | Klicken Sie auf dieses Symbol, um Benachrichtigungen von der Anwendung anzuzeigen. |
|  | Nutzereinstellungen | Klicken Sie auf dieses Symbol, um Ihre verfügbaren Nutzereinstellungsoptionen anzuzeigen. Sie können Ihre Nutzereinstellungen managen und sich bei NetWitness Platform abmelden. |
|  | Nutzerprofil | Klicken Sie auf Ihr Nutzerprofil, um die verfügbaren Optionen anzuzeigen. Sie können Ihre Nutzereinstellungen managen, Ihr Passwort ändern und sich bei NetWitness Platform abmelden. |
|  | Hilfe | Klicken Sie auf dieses Symbol, um NetWitness Platform-Hilfethemen anzuzeigen. |

## Hauptansichten

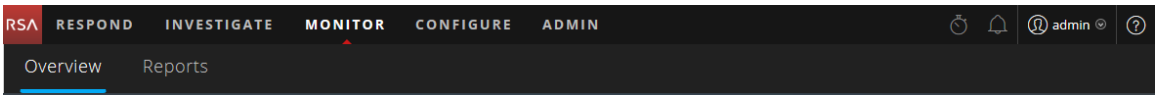
In den folgenden Abschnitten werden die Hauptansichten beschrieben.

## Monitor

Die Ansicht Monitor enthält das NetWitness Platform-Dashboard. „Überwachen“ bietet vorkonfigurierte Dashboards und Berichte, die Sie verwenden können. Sie können aber auch Ihre eigenen erstellen.




## Monitor-Menü




Das Menü Monitor enthält die folgenden Optionen:

- **Überblick**: Mit der Ansicht „Überblick“ können Sie Ihre Dashboards anzeigen und managen. Sie können die folgenden vorkonfigurierten Dashboards auswählen:
  - Standard
  - Identität
  - Investigation
  - Vorgänge – Dateianalyse
  - Vorgänge – Protokolle
  - Vorgänge – Netzwerk
  - Vorgänge – Protokollanalyse
  - Übersicht
  - RSA SecurID
  - Bedrohung – Suche

- Bedrohung – Angriff
- Bedrohung – Malwareindikatoren

Für Nutzer der Legacy-Version 10.6 war dies die Ansicht „Dashboard“.

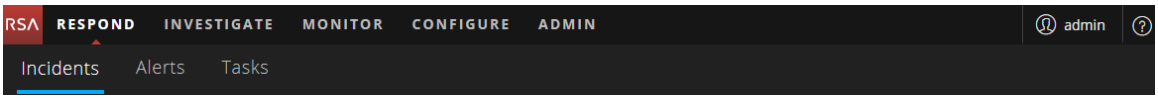
- **Berichte**: Mit der Ansicht „Berichte“ können Sie relevante Berichte für Ihre SOC-Rolle gemäß Ihren zugewiesenen Berechtigungen anzeigen und managen.

| Was kann ich hier tun? | Pfad | Anleitung |
|---|---|---|
| Auswählen eines Dashboard | Monitor > Überblick | Siehe Managen von Dashboards. |
| Erstellen von Dashboards | Monitor > Überblick | Siehe Managen von Dashboards. |
| Dashboards managen | Monitor > Überblick | Siehe Managen von Dashboards. |
| Anzeigen eines Berichts | Monitor > Berichte > Ansicht | Siehe *Reporting-Leitfaden*. |
| Berichte managen | Monitor > Berichte > Managen | Siehe *Reporting-Leitfaden*. |

# Reagieren

In der Ansicht „Reagieren“ wird Analysten eine Warteschlange mit Incidents in der Reihenfolge des Schweregrads angezeigt. Wenn Sie einen Incident in der Warteschlange auswählen, erhalten Sie relevante zugehörige Daten, damit Sie den Incident untersuchen können. Dort können Sie den Umfang des Incident ermitteln und ihn nach Bedarf eskalieren oder korrigieren.

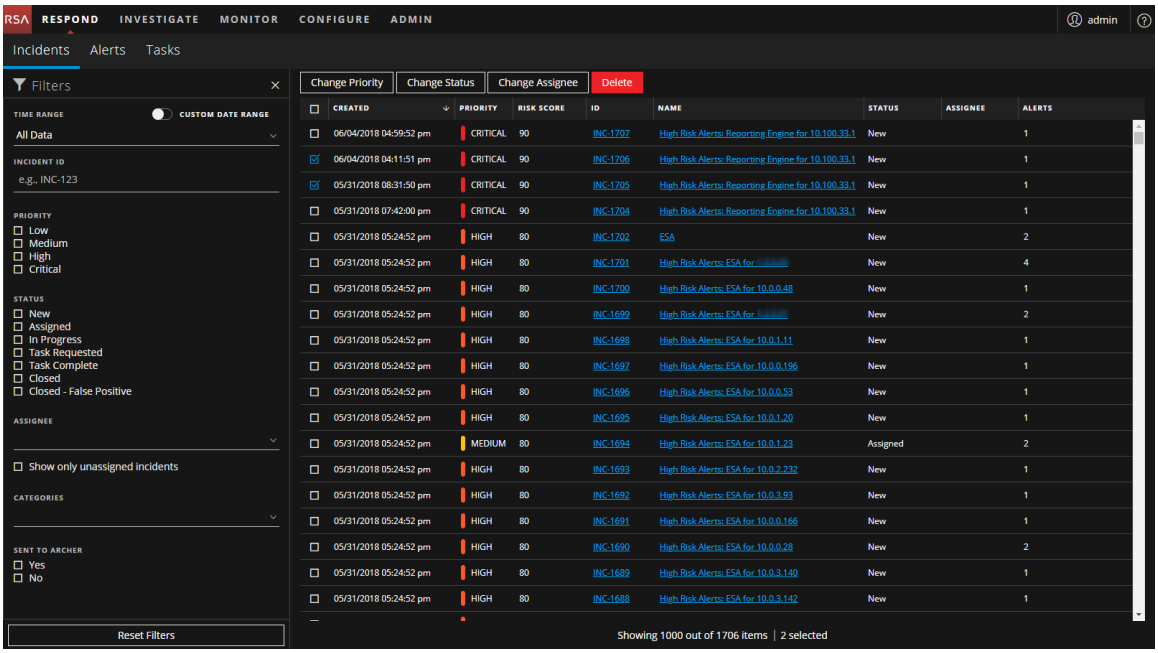
## Reagieren-Menü




Das Menü Reagieren enthält die folgenden Optionen:

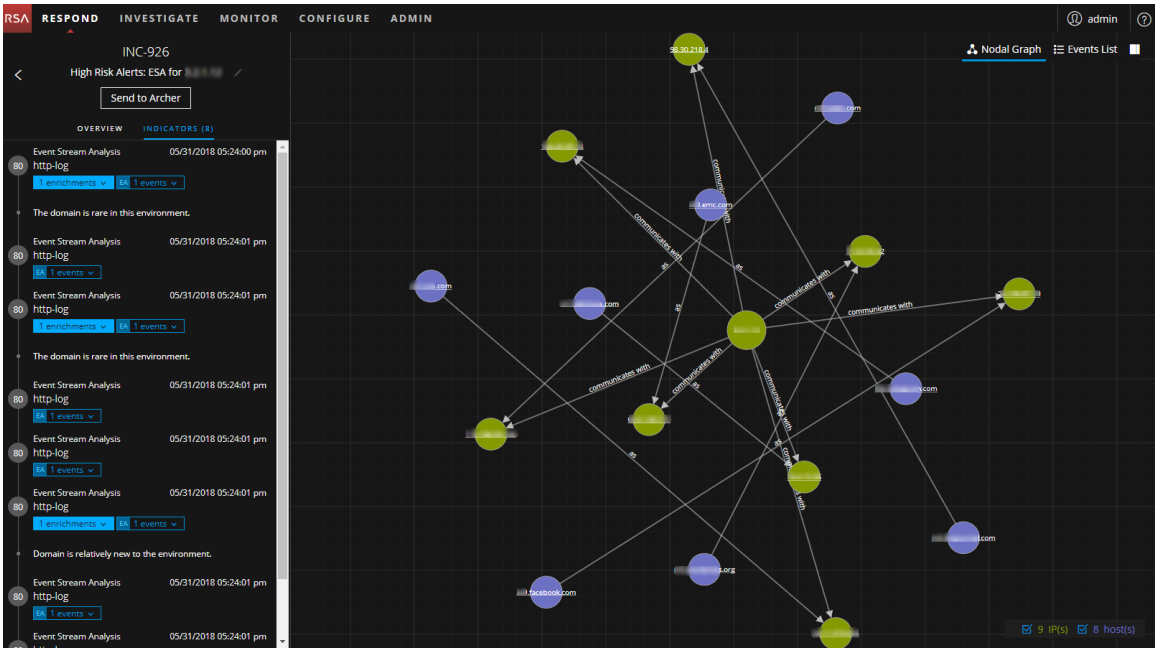
- **Incidents**: Die Listenansicht „Incidents“ enthält eine Liste aller Incidents mit grundlegenden Informationen. Die Ansicht „Incident-Details“ bietet umfassende Details zu einem Incident.
- **Warnmeldungen**: Die Ansichten „Warnmeldungsliste“ und „Warnmeldungsdetails“ bieten Informationen zu allen von NetWitness Platform erhaltenen Bedrohungen und Indikatoren an einem zentralen Speicherort.
- **Aufgaben**: Mit der Ansicht „Aufgabenliste“ können Sie Aufgaben erstellen und bis zum Abschluss nachverfolgen.

Auf der folgenden Abbildung ist die Liste der priorisierten Incidents in der Ansicht „Reagieren“ – Ansicht „Incident-Liste“ zu sehen.

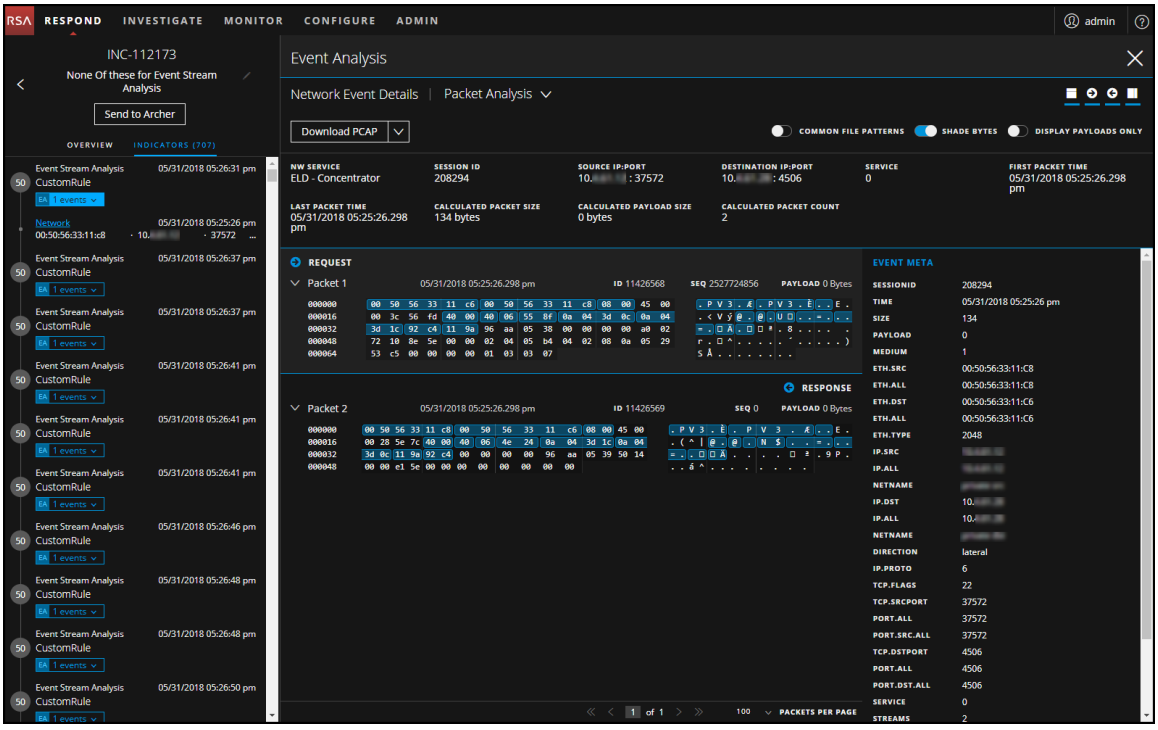



Wenn Sie NetWitness Platform als Vorgangsmanagementtool verwenden, können Sie auch Incidents in dieser Ansicht managen. Neue Incidents werden oben in der Incident-Warteschlange angezeigt.

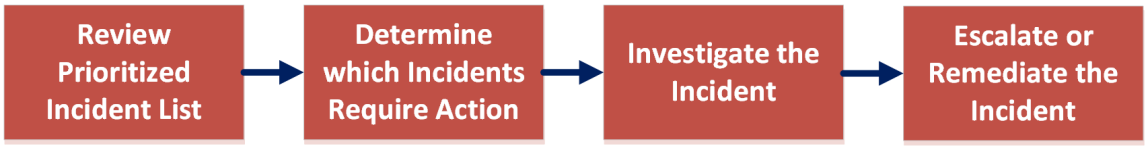
Die folgende Abbildung zeigt ein Beispiel der Ansicht „Reagieren“ – Ansicht „Incident-Details“, in der Details für einen ausgewählten Incident zu sehen sind.




Die Ansicht „Reagieren“ soll die Bewertung von Incidents, die Kontextualisierung von Daten, die Zusammenarbeit mit anderen Analysten und bei Bedarf den Wechsel zu einer detaillierten Untersuchung vereinfachen. In der folgenden Abbildung ist ein Beispiel einer Ereignisanalyse in der Ansicht „Incident-Details“ zu sehen.



Die folgende Abbildung zeigt den allgemeinen Workflow der Ansicht „Reagieren“.



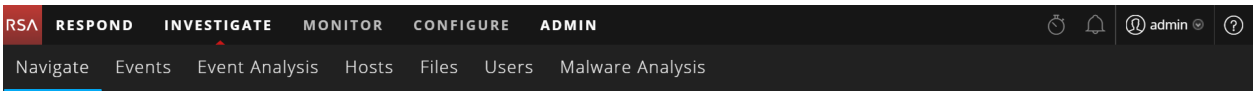

Analysten können in der Ansicht „Reagieren“ die priorisierte Liste der Incidents einsehen und bestimmen, für welche Incidents eine Aktion erforderlich ist. Sie klicken auf einen Incident, um mithilfe unterstützender Details ein klareres Bild von diesem Incident zu erhalten. So können sie den Incident weiter untersuchen. Dann können Analysten bestimmen, wie Sie auf die Bedrohung reagieren, indem sie ihn eskalieren oder korrigieren.

| Was kann ich hier tun? | Pfad | Anleitung |
|---|---|---|
| Anzeigen priorisierte Incident-Listen | Reagieren > Incidents (Ansicht „Incident-Liste“) | Siehe *NetWitness Respond – Benutzerhandbuch*. |
| Ermitteln, welche Incidents eine Aktion erfordern (Priorisieren eines Incident) | Reagieren > Incidents (Ansicht „Incident-Details“) | Siehe *NetWitness Respond – Benutzerhandbuch*. |
| Untersuchen des Incident | Reagieren > Incidents (Ansicht „Incident-Details“) | Siehe *NetWitness Respond – Benutzerhandbuch*. (Sie können auch zur Ansicht „Untersuchen“ wechseln.) |
| Eskalieren oder Korrigieren des Incident | Reagieren > Incidents (Ansicht „Incident-Details“) und Reagieren > Aufgaben (Ansicht „Aufgabenliste“) | Siehe *NetWitness Respond – Benutzerhandbuch*. |
| Überprüfen von Warnmeldungen | Reagieren > Warnmeldungen (Ansichten „Warnmeldungsliste“ und „Warnmeldungsdetails“) | Siehe *NetWitness Respond – Benutzerhandbuch*. |

## Ermittlung

Die Ansicht „Untersuchen“ bietet sieben unterschiedliche Ansichten eines Datensatzes, sodass Analysten Metadaten und Rohdaten für Endpunkte, Protokolle und Ereignisse sowie potenzielle Indikatoren für eine Gefährdung einsehen können. Sie können nicht nur über die Daten zu einem bestimmten Service, sondern auch über „Reagieren“, die Ansicht „Überwachung“, einen Eintrag in einem von der Reporting Engine generierten Bericht oder eine ordnungsgemäß konfigurierte Anwendung eines Drittanbieters zu „Untersuchen“ wechseln. Ihre Untersuchung können Sie in einer der sieben „Untersuchen“-Ansichten beginnen und dann in einer anderen „Untersuchen“-Ansicht fortsetzen. Die Art und Weise, wie Sie vorgehen, hängt davon ab, welche Fragestellung Sie untersuchen möchten. Wenn Sie auf ein Ereignis stoßen, das eine Reaktion erfordert, können Sie in Respond einen Incident anlegen, damit ein Incident-Experte weitere Maßnahmen ergreifen kann. Im *NetWitness Investigate – Benutzerhandbuch* finden Sie detaillierte Informationen.

## Ermittlung-Menü




Das Menü Ermittlung enthält die folgenden Optionen:

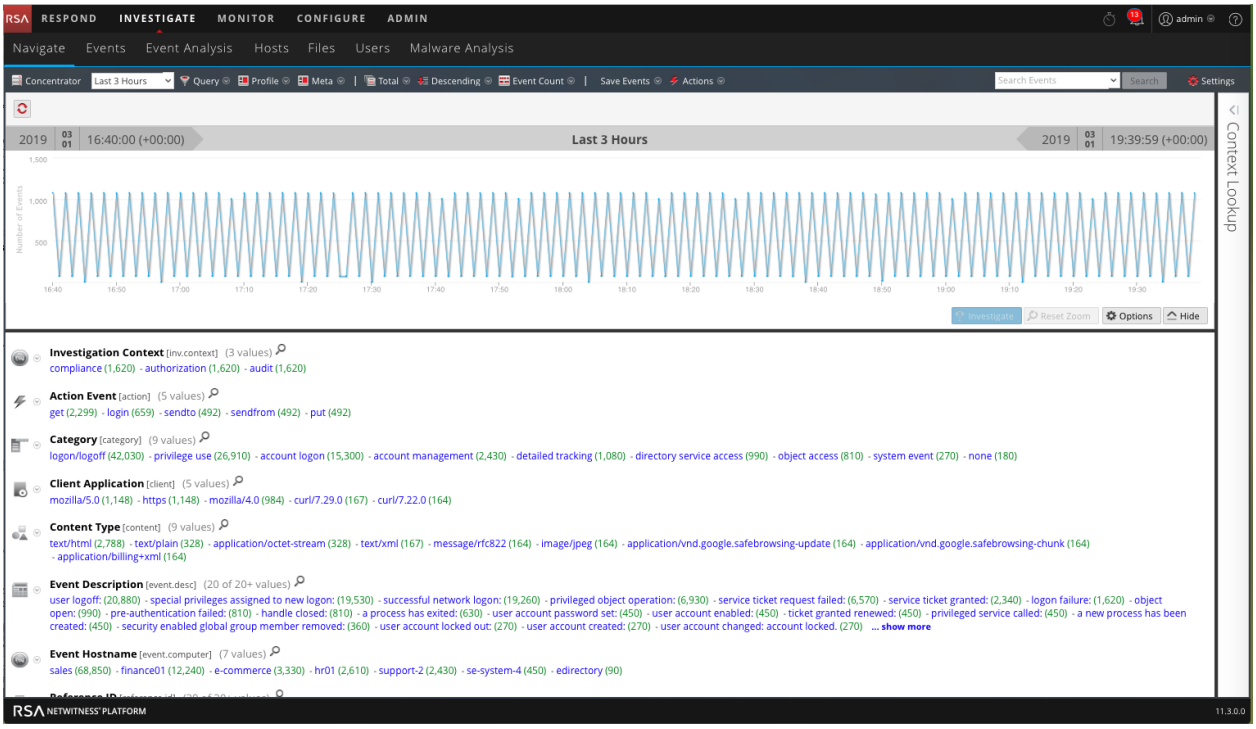
- **Navigieren**: Die Ansicht „Navigation“ enthält eine Liste der Metaschlüssel und Metawerte mit dem Fokus auf Metadaten. Sie können ein Drilldown in die Daten durchführen, ein ausgewähltes Ereignis in der Ansicht „Ereignisse“ oder „Ereignisanalyse“ öffnen, eine Rekonstruktion eines Ereignisses anzeigen, nach Ereignissen suchen, zusätzlichen Kontext im Context-Hub-Service suchen und die Einstellungen für die Ansicht „Navigation“ konfigurieren.
- **Ereignisse**: Die Ansicht „Ereignisse“ enthält eine Liste von Ereignissen mit dem Fokus auf Rohdaten. Sie können eine einfache Liste, eine detaillierte Liste und eine Protokollliste der Ereignisse durchsuchen. Sie können nach Ereignissen suchen, ein ausgewähltes Ereignis in der Ansicht „Ereignisanalyse“ öffnen, eine Rekonstruktion des Ereignisses anzeigen, nach zusätzlichen Kontexten im Context-Hub-Service suchen und die Einstellungen für die Ansicht „Ereignisse“ konfigurieren.
- **Ereignisanalyse**: Die Ansicht „Ereignisanalyse“ enthält eine Liste der Ereignisse mit dem Fokus auf Metadaten und Rohdaten. Sie können eine Rekonstruktion anzeigen, die hilfreiche Hinweise bietet, um interessante Punkte in einer Rekonstruktion zu identifizieren, zur Ansicht „Hosts“ navigieren, nach zusätzlichen Kontexten im Context-Hub-Service suchen (ab Version 11.2), nach Daten in Live suchen und externe Suchen durchführen.
- **Ansicht „Hosts“**: (Version 11.1 und höher) Die Ansicht „Hosts“ enthält alle Hosts, auf denen ein NetWitness Endpoint Agent ausgeführt wird. Für jeden Host können Sie Scandetails anzeigen, Ereignisse in Bezug auf Warnmeldungen, Anomalien, Prozessdetails und Informationen zu angemeldeten Nutzern nachverfolgen. Von der Ansicht „Hosts“ können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ und „Nutzer“ wechseln.
- **Ansicht „Dateien“**: (Version 11.1 und höher) Die Ansicht „Dateien“ bietet eine ganzheitliche Ansicht aller Dateien in Ihrer Bereitstellung. Sie können verschiedene Filter anwenden, Dateien in unterschiedliche Status sortieren und kategorisieren, um die Anzahl der Dateien für die Analyse zu reduzieren und verdächtige oder schädliche Dateien zu identifizieren. Von der Ansicht Dateien können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln.
- **Ansicht „Nutzer“**: (ab Version 11.2) Mit der Ansicht „Nutzer“ von RSA NetWitness UEBA wird die Transparenz von riskantem Nutzerverhalten in Ihrem Unternehmen gewährleistet. Sie können eine Liste der Nutzer mit hohem Risiko und eine Zusammenfassung der wichtigsten Warnmeldungen für riskantes Verhalten für Ihre Umgebung anzeigen. Dann können Sie einen Nutzer oder eine Benachrichtigung auswählen und Details über das riskante Verhalten und eine Zeitleiste anzeigen, in der die Verhaltensweisen aufgetreten sind.

  **Hinweis:** Die Ansicht „Nutzer“ ist nur verfügbar, wenn Ihnen die Rolle des Administrators oder UEBA-Analysten zugewiesen wird.

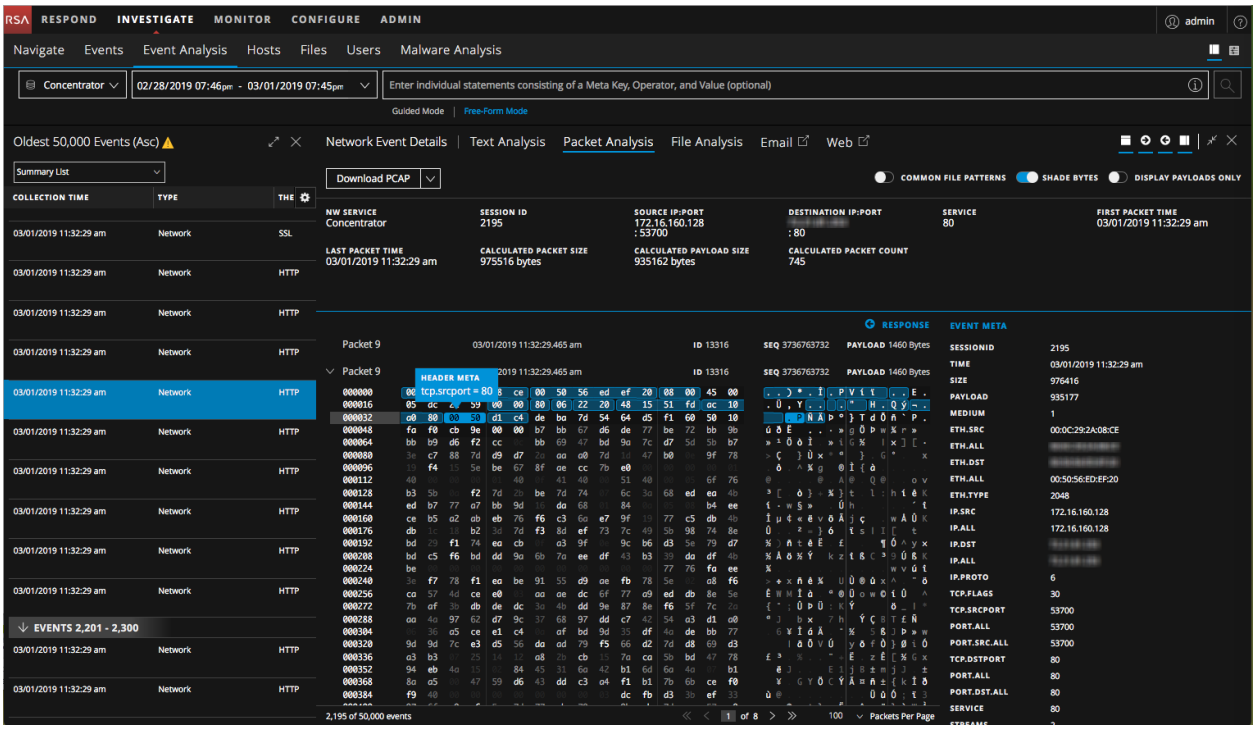
- **Malware Analysis**: Malware Analysis ist eine automatisierte Verarbeitungssoftware zur Analyse von Schadsoftware, die bestimmte Typen von Dateiobjekten analysiert (z. B. Windows PE, PDF und MS

Office), um die potenzielle Schädlichkeit einer Datei zu bewerten. Mit Malware Analysis können Sie von den zahlreichen erfassten Dateien die Dateien priorisieren, von denen potenziell die größte Gefahr ausgeht.

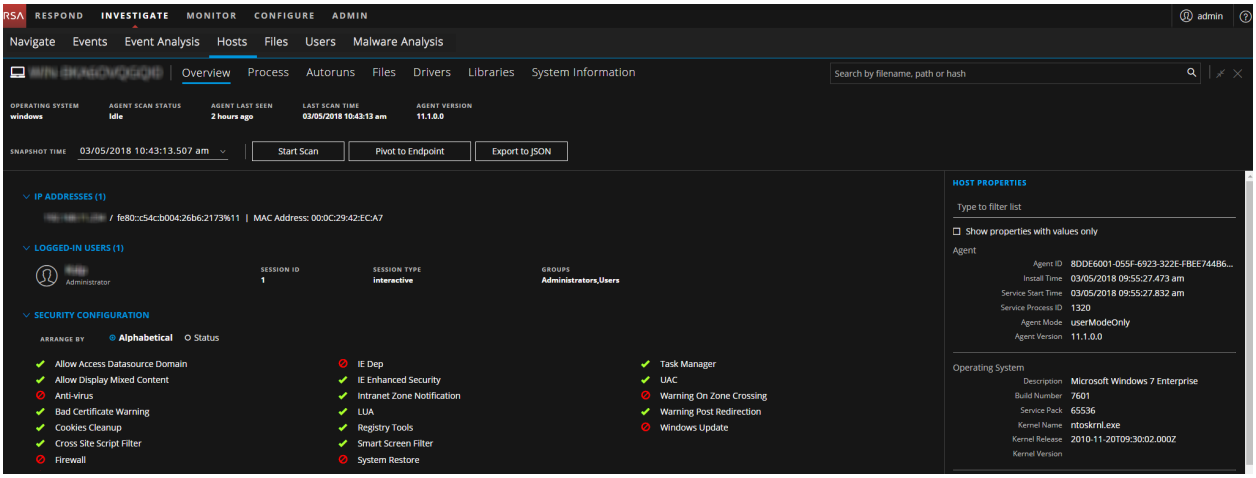
Die folgende Abbildung zeigt die Ansicht „Navigation“.



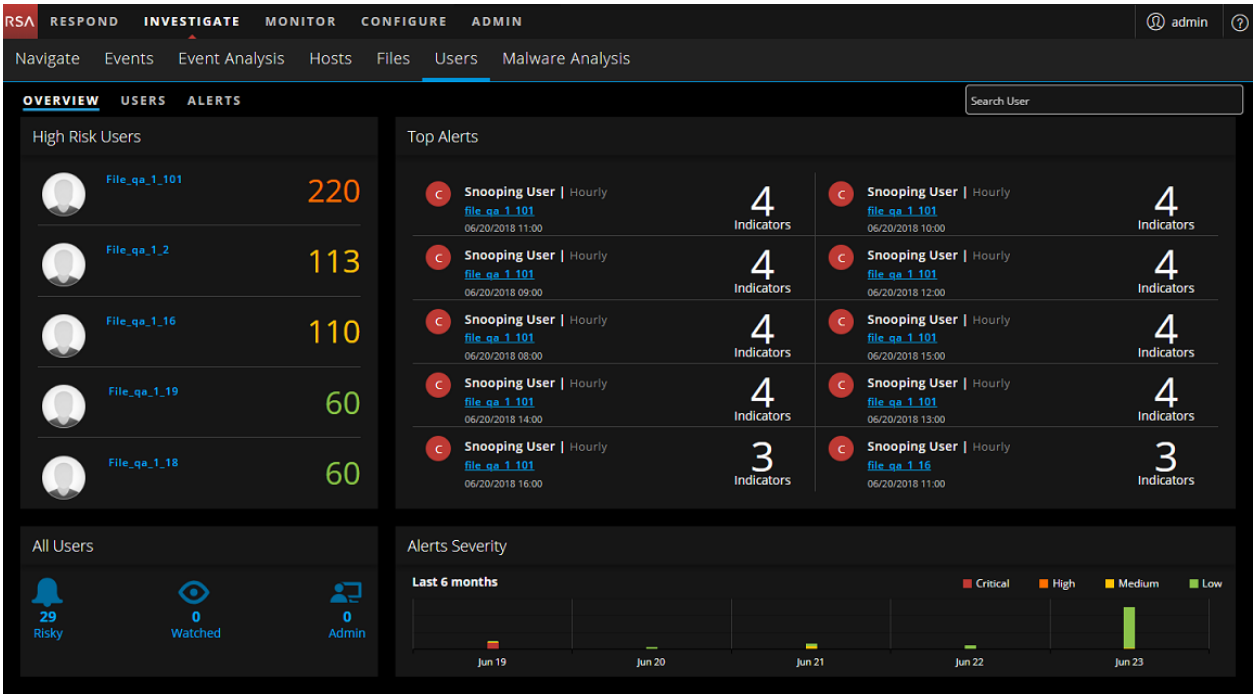

Die folgende Abbildung zeigt die Ansicht „Ereignisanalyse“.



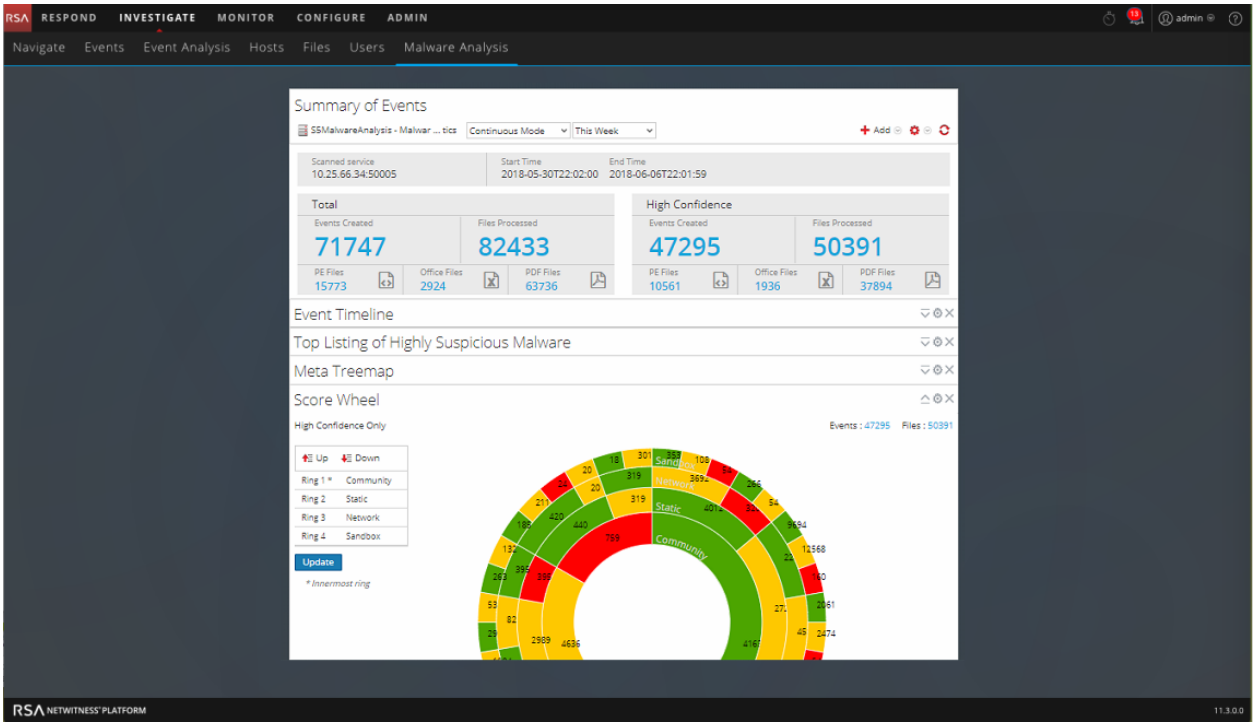
Die folgende Abbildung zeigt die Ansicht „Hosts“ – Ansicht „Details zum Host“.



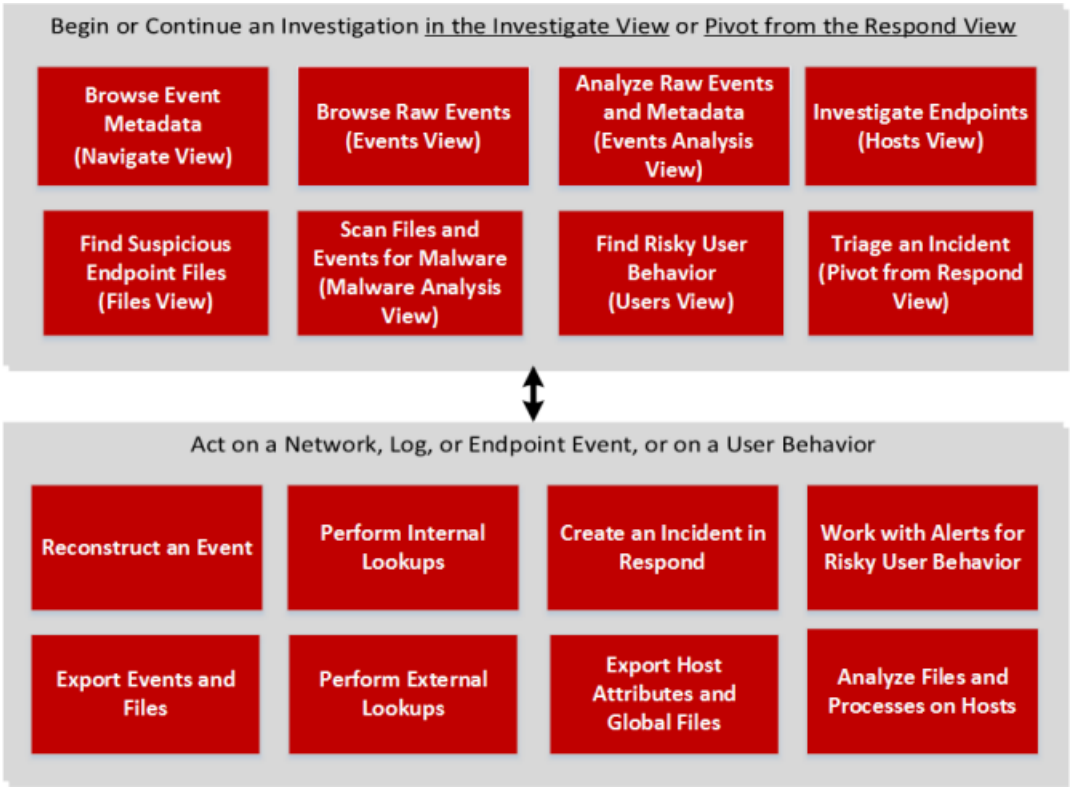

Die folgende Abbildung zeigt die Ansicht „Nutzer“.



Die folgende Abbildung zeigt die Malware Analysis-Ereigniszusammenfassung.




In der folgenden Abbildung ist der Typ der Ermittlung für jede Ansicht im oberen Block dargestellt. Der untere Block zeigt Aufgaben, die Sie als Teil einer Ermittlung durchführen können.

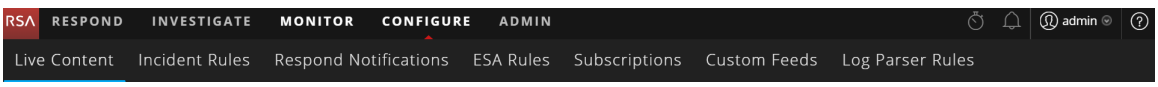


| Was kann ich hier tun? | Pfad | Anleitung |
|---|---|---|
| Konfigurieren von Ermittlungsansichten und -einstellungen | Ansicht Ermittlung | Siehe „Konfigurieren von Ansichten und Voreinstellungen von NetWitness Investigate“ im *NetWitness Investigate – Benutzerhandbuch*. |
| Durchsuchen von Ereignismetadaten | Ansicht „Navigation“ | Siehe „Untersuchen von Metadaten in der Ansicht ‚Navigieren‘“ im *NetWitness Investigate – Benutzerhandbuch*. |
| Durchsuchen von Raw-Ereignissen | Ansicht „Ereignisse“ | Siehe „Untersuchen von Raw-Ereignissen in der Ansicht ‚Ereignisse‘“ im *NetWitness Investigate – Benutzerhandbuch*. |
| Analyse von Raw-Ereignissen und Metadaten | Ansicht „Ereignisanalyse“ | Siehe „Analysieren von Raw-Ereignissen und Metadaten“ *NetWitness Investigate – Benutzerhandbuch*. |
| Untersuchen von Endpunkten | Ansicht „Hosts“ | Weitere Informationen finden sie im *NetWitness Endpoint-Benutzerhandbuch*. |
| Finden verdächtiger Endpunktdateien | Ansicht „Dateien“ | Siehe *NetWitness Endpoint-Benutzerhandbuch*. |
| Dateien und Ereignisse auf Schadsoftware scannen | Ansicht „Malware Analysis“ | Weitere Informationen finden Sie im *Leitfaden zur Malware Analysis*. |
| Riskantes Nutzerverhalten suchen | Ansicht „Nutzer“ | Siehe *NetWitness UEBA – Benutzerhandbuch*. |
| Priorisieren eines Incidents | Aus der Ansicht „Reagieren" wechseln | Siehe *NetWitness Respond – Benutzerhandbuch*. |

## Konfigurieren

Die Ansicht „Konfigurieren“ ermöglicht Mitarbeitern für Bedrohungsinformationen (Contentexperten) die Konfiguration der Datenquellen und Eingaben in NetWitness Platform an einem zentralen Ort.

### Konfigurieren-Menü




Das Menü Konfigurieren enthält die folgenden Optionen:

- **Live-Inhalt**: (Live-Services) Mit der Ansicht „Live-Inhalt“ können Sie nach Live-Services-Ressourcen suchen und diese abonnieren. Live-Services ist die Komponente der NetWitness Platform, die die Kommunikation und Synchronisation zwischen NetWitness Platform-Services und

einer Bibliothek von Live-Inhalten managt, die RSA NetWitness Platform-Kunden zur Verfügung stehen. Sie können Inhalte aus dem RSA Live-Contentmanagementsystem (CMS) auf NetWitness Platform-Services und -Software anzeigen, suchen, bereitstellen und abonnieren. Wenn Sie eine Ressource abonnieren, geben Sie an, dass Sie regelmäßig Aktualisierungen von RSA Live-Services erhalten möchten.
Für Nutzer der Legacy-Version 10.6 war dies „Live > Suche“.

- **Incident-Regeln**: Mit der Ansicht „Incident-Regeln“ können Sie Incident-Regeln mit unterschiedlichen Kriterien erstellen, um Incidents automatisch zu erstellen. Sie können sich in der Ansicht „Reagieren“ die priorisierten Incidents anzeigen lassen.
  Für Nutzer der Legacy-Version 10.6 war dies Incidents > Konfigurieren. In 11.1 oder höher werden Aggregationsregeln als Incident-Regeln bezeichnet.
- **Auf Benachrichtigungen antworten**: In der Ansicht „Auf Benachrichtigungen antworten“ können Sie automatisch E-Mail-Benachrichtigungen an SOC-Manager und die mit den Incidents verknüpften Analysten senden, wenn Incidents erstellt oder aktualisiert werden.
- **ESA-Regeln**: Mit der Ansicht „ESA-Regeln“ können Sie die ESA-Regeln (Event Stream Analysis) managen, mit denen die Kriterien für Problemverhalten oder bedrohliche Ereignisse in Ihrem Netzwerk bestimmt werden. Wenn ESA eine Bedrohung entdeckt, die Regelkriterien entspricht, wird eine Warnmeldung erzeugt.
  Sie können ESA-Regeln selbst erstellen oder von Live-Services herunterladen. Die Regelbibliothek enthält alle erstellten oder heruntergeladenen ESA-Regeln. Zum Aktivieren von Regeln müssen Sie diese zu einer Bereitstellung hinzufügen. Die Bereitstellung ordnet Regeln aus Ihrer Regelbibliothek den entsprechenden ESA-Services zu.
  Für Nutzer der Legacy-Version 10.6 war dies „Warnmeldungen > Konfigurieren“.
- **Abonnements**: (Live-Services) In der Ansicht „Abonnements“ können Sie den Live-Inhalt verwalten, den Sie in der Ansicht „Live-Inhalt“ abonniert haben. Konfigurieren Sie die Verbindung und die Synchronisation zwischen dem CMS-Server und NetWitness Platform, um Live-Services in NetWitness Platform einzurichten.
  Für Nutzer der Legacy-Version 10.6 war dies Live > Konfigurieren.
- **Benutzerdefinierte Feeds**: (Live-Services) Die Ansicht „Benutzerdefinierte Feeds“ optimiert die Aufgabe der Erstellung und des Managements benutzerdefinierter Feeds und füllt die Feeds an ausgewählte Decoder und Log Decoder. Sie können benutzerdefinierte Feeds und Identitätsfeeds einrichten und verwalten.
  NetWitness Platform verwendet Feeds zum Erstellen von Metadaten, die auf extern definierten Metadatenwerten beruhen. Ein Feed ist eine Liste von Daten, die bei der Erfassung oder Verarbeitung von Sitzungen mit diesen abgeglichen werden. Bei jedem erfolgreichen Abgleich werden zusätzliche Metadaten erstellt.
  Sie können benutzerdefinierte Feeds zur Bereitstellung von zusätzlichen Metadaten erstellen, z. B. Metadatenextrahierungen, um benutzerdefinierten Netzwerkanwendungen gerecht zu werden.
  Für Nutzer der Legacy-Version 10.6 war dies „Live > Feeds“.
- **Protokoll-Parser-Regeln**: Auf der Registerkarte „Protokoll-Parser-Regeln“ werden Informationen zu einzelnen Protokollparsern angezeigt sowie der Standardparser „Alle analysieren“, mit dem Protokolle analysiert werden können, die keinem bestimmten Protokoll-Parser zugeordnet sind. Auf

dieser Registerkarte finden Sie folgende Informationen:

- Sie können die Regeln für einen bestimmten Ereignisquelltyp anzeigen, einschließlich des Standardsarsers.
- Sie können die Namen, Literale, Muster und Metadaten für jeden konfigurierten Protokollparser anzeigen.
- Sie können Protokollparser hinzufügen.
- Sie können benutzerdefinierte Regeln für Protokollparser hinzufügen, bearbeiten und löschen.

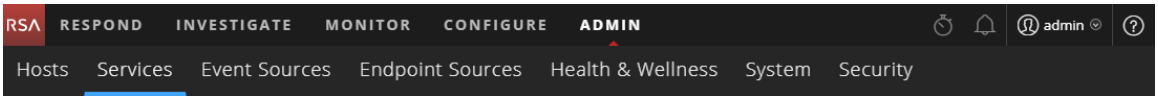
**Hinweis:** Die Registerkarte „Protokoll-Parser-Regeln“ ist ab Version 11.2 im Menü „Konfigurieren“ verfügbar. Bei früheren Versionen ist sie unter „Administration > Ereignisquellen“ zu finden.

| Was kann ich hier tun? | Pfad | Anleitung |
|---|---|---|
| Erstellen eines Live-Services-Kontos | RSA Live-Registrierungsportal: https://cms.netwitness.com/registration/ | Siehe *Handbuch zum Management von Live-Services*. |
| Suchen und Bereitstellen von Live-Services-Ressourcen | Konfigurieren > Live-Inhalt | Siehe *Handbuch zum Management von Live-Services*. |
| Automatisches Erstellen von Incidents | Konfigurieren > Incident-Regeln | Siehe den *Konfigurationsleitfaden für NetWitness Respond*. |
| Konfigurieren von „Auf Benachrichtigungen antworten“ | Konfigurieren > Auf Benachrichtigungen antworten | Siehe den *Konfigurationsleitfaden für NetWitness Respond*. |
| Konfigurieren von Warnmeldungen | Konfigurieren > ESA-Regeln | Siehe *Warnmeldungen mit ESA-Korrelationsregeln – Benutzerhandbuch*. |
| Einrichten von Live-Services-Services in NetWitness Platform | Konfigurieren > Abonnement | Siehe das *Handbuch zum Management von Live-Services*. |
| Einrichten und Verwalten von benutzerdefinierten Feeds und Identitätsfeeds | Konfigurieren > Nutzerdefinierte Feeds | Siehe *Handbuch zum Management von Live-Services*. |
| Zeigen Sie Protokollparser und Protokoll-Parser-Regeln an und bearbeiten Sie sie. | Konfigurieren > Protokoll-Parser-Regeln | Siehe das *Handbuch für Protokollparser-Anpassungen*. |

# ADMIN

In der Ansicht „Admin“ können Administratoren Netzwerkhosts und -services managen, die Integrität und den Zustand von NetWitness Platform überwachen und die Systemebenensicherheit managen. Sie können auch globale Systemressourcen konfigurieren und Ereignisquellen managen.

## ADMIN-Menü




Das Menü ADMIN enthält die folgenden Optionen:

- **Hosts**: In der Ansicht „Hosts“ können Sie Hosts einrichten und verwalten. Ein Host ist der Computer, auf dem Services ausgeführt werden. Ein Host kann ein physischer Rechner oder eine virtuelle Maschine sein.
- **Services**: Mit der Ansicht „Services“ können Sie Services managen, Servicebenutzer und -rollen managen, Service-Servicekonfigurationsdateien verwalten und Serviceeigenschaften durchsuchen und bearbeiten. Ein Service führt eine eindeutige Funktion aus, z. B. erfasst ein Decoder-Service Netzwerkdaten im Paketformat.
- **Ereignisquellen**: Mit der Ansicht „Ereignisquellen“ können Sie Ereignisquellen verwalten und Warnmeldungsrichtlinien für diese konfigurieren. Typischerweise überwachen Unternehmen ihre Ereignisquellen aufgeteilt in Gruppen, in Abhängigkeit davon, wie kritisch die einzelnen Ereignisquellen sind. Sie können Überwachungsrichtlinien für jede Ereignisquellengruppe erstellen und sie basierend auf ihrer Priorität ordnen.
- **Endpunktquellen**: In der Ansicht Endpunktquellen können Sie Endpunkt-Konfigurationen über Gruppen managen und aktualisieren und das Verhalten der Agents mithilfe von Richtlinien managen. Sie können die Standardrichtlinien verwenden oder diese Richtlinien anpassen.
- **Integrität und Zustand**: Mit der Ansicht „Integrität und Zustand“ können Sie die Integrität der NetWitness Platform-Hosts und -Services in Ihrer Netzwerkumgebung überwachen.
- **System**: In der Ansicht „System“ können Sie globale NetWitness Platform-Konfigurationen festlegen. Sie können Auditprotokollierung, E-Mail, Systemprotokollierung, Jobs, RSA Live-Services, URL-Integration, Investigation, Event Stream Analysis (ESA), ESA Analytics und erweiterte Leistungseinstellungen global konfigurieren. Außerdem können Sie NetWitness Platform-Versionen managen und den lokalen Lizenzierungsserver konfigurieren.
- **Sicherheit:** Der Bereich „Administrationssicherheit“ bietet die Möglichkeit, Nutzerkonten und Nutzerrollen zu managen, externe Gruppen NetWitness Platform-Rollen zuzuordnen und andere sicherheitsbezogene Systemparameter zu ändern. Diese Funktionen gelten für das NetWitness Platform-System und werden in Verbindung mit den Sicherheitseinstellungen für einzelne Services verwendet.

**Hinweis:** Ab Version 11.2 befindet sich die Registerkarte „Ereignisquellen > Protokoll-Parser-Regeln“ in der Ansicht „Konfigurieren“.

| Was kann ich hier tun? | Pfad | Anleitung |
|---|---|---|
| Verwalten von Hosts | ADMIN > Hosts | Siehe *Leitfaden für die ersten Schritte mit Hosts und Services*. |
| Managen von Services wie das Management von Servicebenutzerzugriff und Sicherheit | ADMIN > Services | Siehe *Leitfaden für die ersten Schritte mit Hosts und Services*. |
| Verwalten von Ereignisquellen und Konfigurieren von Warnmeldungsrichtlinien für diese | ADMIN > Ereignisquellen | Siehe *Leitfaden für das Ereignisquellenmanagement*. |
| Verwalten von Endpunktquellen und Konfigurieren von Warnmeldungsrichtlinien für diese | ADMIN > Endpunktquellen | Siehe *Leitfaden für das Ereignisquellenmanagement*. |
| Einrichten und Überwachen von Alarmen für die Hosts und Services in Ihrer NetWitness Platform-Domain | ADMIN > Integrität und Zustand > Alarm | Siehe *Leitfaden Systemwartung*. |
| Überwachen von Statistiken für die NetWitness Platform-Hosts und die auf diesen Hosts ausgeführten Services | ADMIN > Integrität und Zustand > Überwachung | Siehe *Leitfaden Systemwartung*. |
| Erstellen und Anwenden von Richtlinien auf Ihre Hosts und Services, um die Erhaltung der Integrität und des Zustands Ihrer NetWitness Platform-Domain zu unterstützen | ADMIN > Integrität und Zustand > Richtlinien | Siehe *Leitfaden Systemwartung*. |
| Festlegen der globalen Konfigurationen für NetWitness Platform | ADMIN > System | Siehe den *Systemkonfigurationsleitfaden*. |
| Konfigurieren der globalen Auditprotokollierung | ADMIN > System > Globales Auditing | Siehe den *Systemkonfigurationsleitfaden*. |
| Einrichten von Systemsicherheit | ADMIN > Sicherheit | Siehe *Handbuch Systemsicherheit und Nutzerverwaltung*. |
| Managen von Systembenutzern mit Rollen und Berechtigungen | ADMIN > Sicherheit | Siehe *Handbuch Systemsicherheit und Nutzerverwaltung*. |
| Einrichten der PKI-Authentifizierung (Public Key Infrastructure) PKI ist in NetWitness Platform 11.3 und höher verfügbar. | ADMIN > Sicherheit | Siehe *Handbuch Systemsicherheit und Nutzerverwaltung*. |

# Einrichten einer Standardansicht nach SOC-Rolle

Sie können die Navigation in der Anwendung nach der Anmeldung bei RSA NetWitness® Platform leichter gestalten, indem Sie Ihre Standardansicht basierend auf Ihrer SOC-Rolle (Security Operations) einrichten. Sie können Ihre Standardansicht – auch bekannt als Landingpage – in Ihren Nutzereinstellungen festlegen.

Die folgende Abbildung zeigt die Hauptansichten in NetWitness Platform.


- **Reagieren**: Diese Ansicht ist für Incident Responders bestimmt, die eine Liste der Incidents zur Priorisierung und Warnmeldungen anzeigen können. Nutzer der Legacy-Version 10.6 kennen diese Ansicht als die Ansicht „Incident-Management“. Die Ansicht „Reagieren > Warnmeldungen“ ersetzt die Ansicht „Warnmeldungen > Zusammenfassung“ in ESA 10.6.
  „Reagieren“ ist die standardmäßige Startansicht. Wenn Sie nicht über die Berechtigung zum Anzeigen der Ansicht „Reagieren“ verfügen, wird Ihnen als Standardansicht „Überwachen“ angezeigt.
- **Untersuchen**: Diese Ansicht ist für Threat Hunters, die Advanced Threats ermitteln und aufspüren. Andere Analysten wie beispielsweise Incident-Experten können zur detaillierteren Analyse eines Incidents zu dieser Ansicht wechseln.
- **Ermittlung**: Diese Ansicht steht allen Benutzern zur Verfügung. Es handelt sich um die Standardansicht für vorherige Anwendungsversionen. Sie können verschiedene Bereiche des Dashboards und Berichte je nach Ihren Benutzerberechtigungen anzeigen. Sie können ein vorkonfiguriertes Dashboard auswählen, ein Dashboard importieren oder Ihr eigenes angepasstes Dashboard erstellen.
- **Konfigurieren**: Diese Ansicht ist für Mitarbeiter im Bereich „Bedrohungsdaten“ (Contentexperten) verfügbar, die Datenquellen und Eingaben für NetWitness Platform konfigurieren. Contentexperten nutzen diesen Bereich, um Live-Inhalte herunterzuladen und zu verwalten. Sie können ebenfalls Incident- und ESA-Regeln erstellen und managen.
  Nutzer der Legacy-Version 10.6 kennen diese Ansicht als die Ansicht „Live“, Incidents > Konfigurieren und Warnmeldungen > Konfigurieren.
- **Admin**: Diese Ansicht ist für Systemadministratoren verfügbar, die die gesamte Anwendung einrichten und verwalten.

Sie können eine der Hauptansichten für NetWitness Platform als Standardansicht auswählen. Zusätzlich zu den Hauptansichten verfügt NetWitness Platform über vordefinierte Dashboards, die Sie in der Ansicht „Überwachen“ abhängig von den Aufgaben, die Sie durchführen, auswählen können:

- Standard-Dashboard
- Dashboard „Identität“
- Vorgänge – Dashboard „Protokolle“
- Vorgänge – Dashboard „Netzwerk“

- Übersichts-Dashboard
- Bedrohung – Dashboard „Indikatoren“
- Bedrohung – Dashboard „Angriff“

In der folgenden Tabelle sind typische SOC-Rollen und die verfügbaren Ansichten aufgeführt, die Sie als Landingpage in Ihren Nutzereinstellungen basierend auf Ihrer SOC-Rolle auswählen können. Wenn Sie über mehr als eine Administratorrolle verfügen, wählen Sie die Ansicht, die für Sie am besten geeignet ist, wenn Sie sich bei NetWitness Platform anmelden.

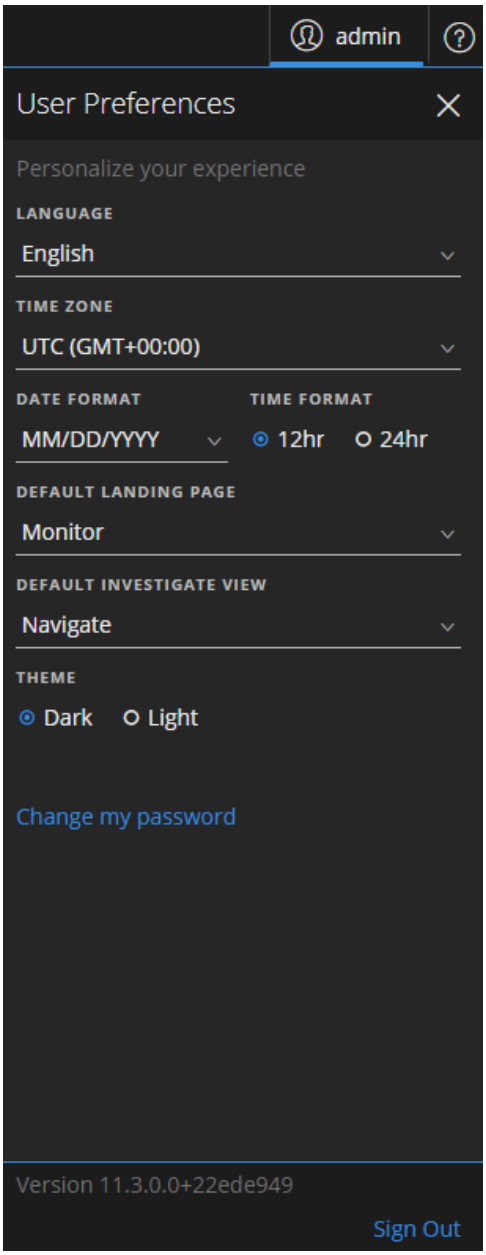
| SOC-Rollen | Rollenbeschreibung | Berücksichtigen dieser standardmäßigen Landingpage |
|---|---|---|
| Incident-Experte (Tier-1-Analyst) | Kümmert sich um Incidents und Warnmeldungen in der Warteschlange, um sie zu überprüfen und einzudämmen. | **Reagieren** |
| Threat Hunter (Tier-2-/Tier-3-Analyst) | Führt eine Ermittlung und Erkennung von Advanced Threats durch. | **UNTERSUCHEN**<br>Informationen zur Auswahl der standardmäßigen Untersuchen-Ansicht finden Sie im *NetWitness Investigate – Benutzerhandbuch*. |
| SOC-Manager (SOC-Management und -Reporting) | Managt die SOC-Bereitschaft und reagiert auf Incidents und Datensicherheitsverletzungen. | **Monitor** (Dashboard befindet sich in der Ansicht Monitor. Wenn Sie sich anmelden, wählen Sie das entsprechende vordefinierte Dashboard für Ihre SOC-Rolle aus. Sie können auch ein Dashboard importieren oder Ihr eigenes Dashboard erstellen. |
| Contentexperte (Bedrohungsintelligenz) | Konfiguriert Datenquellen und Eingaben in NetWitness Platform. | **Monitor** oder **Konfigurieren** (Dashboard befindet sich in der Ansicht Monitor. Wenn Sie sich anmelden, wählen Sie das entsprechende vordefinierte Dashboard für Ihre SOC-Rolle aus. Sie können auch ein Dashboard importieren oder Ihr eigenes Dashboard erstellen. Wenn Sie sich dafür entscheiden, Monitor als Standardansicht auszuwählen, können Sie vom Hauptmenü zur Ansicht Konfigurieren navigieren.) |
| Datenschutzbeauftragter (DPO) | Ähnlich wie bei einem Administrator; ein DPO überwacht und schützt jedoch datenschutzrelevante Informationen. | **Monitor** (Dashboard befindet sich in der Ansicht Monitor. Wenn Sie sich anmelden, wählen Sie das entsprechende vordefinierte Dashboard für Ihre SOC-Rolle aus. Sie können auch ein Dashboard importieren oder Ihr eigenes Dashboard erstellen.) |

| SOC-Rollen | Rollenbeschreibung | Berücksichtigen dieser standardmäßigen Landingpage |
|---|---|---|
| Systemadministrator | Konzentriert sich auf die Konfiguration und die Stabilität der gesamten Anwendung. Managt den Benutzerzugriff. | **Admin** |

## Festlegen der Standardansicht

1. (Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten) Wählen Sie auf der Hauptmenüleiste  aus.

   Im Dialogfeld „Benutzereinstellungen“ werden die aktuellen Einstellungen angezeigt.




2. Wählen Sie im Feld **Standardmäßige Landingpage** die Standardansicht aus, die Sie sehen möchten, wenn Sie sich bei NetWitness Platform anmelden. Verwenden Sie in die obige Tabelle, um Ihre Auswahl basierend auf Ihrer SOC-Rolle vorzunehmen. Wenn Sie beispielsweise ein Incident-Experte sind, können Sie **Reagieren** auswählen und wenn Sie ein Threat Hunter sind, können Sie **Untersuchen** auswählen.

   Die Einstellungen werden sofort wirksam. Sie können Ihre standardmäßige Landingpage jederzeit ändern. Informationen über andere Einstellungen finden Sie unter Festlegen von Nutzereinstellungen.

3. Wenn Sie überprüfen möchten, ob Sie die richtige Standardansicht sehen, können Sie zum Abmelden auf **Abmelden** klicken und sich dann wieder bei NetWitness Platform anmelden.

## Grundlegende Troubleshooting-Tipps für den Benutzersetup

Die folgende Tabelle enthält grundlegende Troubleshooting-Tipps, die möglicherweise hilfreich für das Nutzersetup in NetWitness Platform sein können.

| Problem | Troubleshooting-Tipp |
|---|---|
| Wenn ich mich bei NetWitness Platform anmelde, wird die falsche Standardansicht angezeigt. | Stellen Sie sicher, dass die richtigen Standardansicht im Feld „Standardmäßige Landingpage“ in Ihren Nutzereinstellungen festgelegt ist. Bei Auswahl der Ansicht Monitor können Sie das vordefinierte Dashboard auswählen, das am besten zu Ihrer SOC-Rolle passt. Sie können auch ein Dashboard importieren oder Ihr eigenes Dashboard erstellen. |
| Die richtige Ansicht wird angezeigt, aber die Metadaten werden nicht geladen. | Stellen Sie sicher, dass Sie die neueste Version des Browsers verwenden. Wenn das nicht funktioniert, versuchen Sie es mit einem anderen Browser. Wenn Sie beispielsweise Safari verwenden, versuchen Sie es mit Firefox oder Chrome. |
| Ich verwende Internet Explorer 10 und die folgende Fehlermeldung wird angezeigt: `The page can't be displayed.` | NetWitness Platform unterstützt aktuelle Versionen von Firefox, Chrome und Safari. Wenn Sie Internet Explorer verwenden, funktionieren nicht alle Funktionen wie vorgesehen. Versuchen Sie, einen der unterstützten Browser zu verwenden. |
| Wenn ich mich anmelde, wird nichts angezeigt. | Wenden Sie sich an Ihren Administrator. Es muss Ihnen möglicherweise eine Nutzerrolle für Ihr Konto zugewiesen werden oder Sie benötigen zusätzliche Troubleshooting-Maßnahmen. |
| Ich weiß nicht, wo ich meine standardmäßige Landingpage ändern kann. | Navigieren Sie zu den Nutzereinstellungen in der Ansicht „Reagieren“ oder wenden Sie sich an Ihren Administrator. |

# Festlegen von Nutzereinstellungen

Sie können Ihre globalen RSA NetWitness® Platform-Anwendungseinstellungen in Ihrem Benutzerprofil anzeigen und managen. Es gibt zwei globale Dialogfelder mit Nutzereinstellungen, die unterschiedliche Optionen aufweisen. Das Dialogfeld „Nutzereinstellungen“ kann über die Ansicht „Reagieren“ und folgende „Untersuchen“-Ansichten aufgerufen werden: Ereignisanalyse, Hosts, Dateien und Nutzer. Das Dialogfeld „Einstellungen“ kann von meisten anderen Ansichten aus aufgerufen werden. Welches Dialogfeld Sie sehen, hängt davon ab, von wo aus Sie auf die Nutzereinstellungen zugreifen.

Sie haben folgende Möglichkeiten:

- Ändern der Sprache der Anwendung
- Festlegen der Zeitzone der Anwendung
- Festlegen des Datums- und Uhrzeitformats der Anwendung*
- Auswählen der standardmäßigen Startansicht für NetWitness Platform*
- Auswählen der standardmäßigen Ansicht „Untersuchen“*
- Auswählen eines dunklen oder hellen Designs für die Anwendung*
- Ihr Passwort ändern (weitere Informationen siehe Ändern des Passworts)
- Aktivieren oder Deaktivieren von Benachrichtigungen**
- Aktivieren oder Deaktivieren von Kontextmenüs**

* Sie können diese Änderung im Dialogfeld **Benutzereinstellungen** vornehmen, das sich über „Reagieren“ und einige „Untersuchen“-Ansichten aufrufen lässt: Ereignisanalyse, Hosts, Dateien und Nutzer.

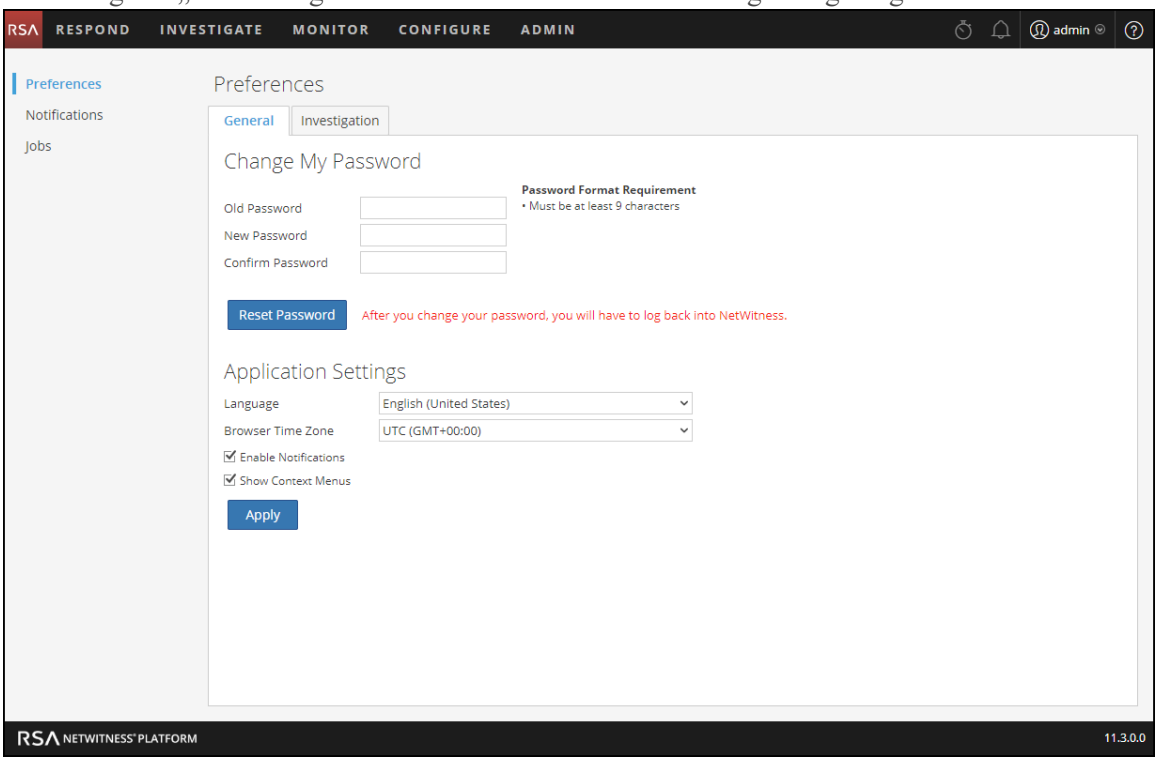
** Sie können diese Änderung im Dialogfeld **Einstellungen** vornehmen, das sich über die meisten Ansichten aufrufen lässt (außer „Reagieren“ und folgende „Untersuchen“-Ansichten: Ereignisanalyse, Hosts, Dateien und Nutzer).

## Einstellungen (in den meisten Ansichten außer „Reagieren“ und einiger „Untersuchen“-Ansichten)

In diesem Abschnitt finden Sie Anweisungen für verschiedene Aufgaben, die im Dialogfeld „Einstellungen“ ausgeführt werden können. Es ist über die meisten Ansichten aufrufbar, mit Ausnahme von „Reagieren“ und einigen „Untersuchen“-Ansichten.

## Anzeigen der Einstellungen

Wählen Sie in der oberen rechten Ecke des NetWitness Platform-Browserfensters > **Profil** aus. Im Dialogfeld „Einstellungen“ werden die aktuellen Einstellungen angezeigt.




## Festlegen von Sprache und Zeitzone

**Hinweis:** Die Einstellung der Sprache ist ab NetWitness Platform 11.2 verfügbar.

Sie können die Sprache für NetWitness Platform ändern. Die Standardsprache ist Englisch (USA).

1. Wählen Sie im Dialogfeld „Benutzereinstellungen“ Ihre Lokalisierungseinstellungen aus:
   a. **Sprache**: Wählen Sie Ihre bevorzugte Sprache für NetWitness Platform aus.
   b. **Zeitzone**: Legen Sie die Zeitzone für die Verwendung in NetWitness Platform fest.
2. Klicken Sie auf **Anwenden**.
   Die Einstellungen werden sofort wirksam.

**Hinweis:** Wenn für die ausgewählte Zeitzone des aktuell angemeldeten Nutzers die Sommerzeit gilt, wird in der Benutzeroberfläche automatisch die korrekte Zeit angezeigt.

## Aktivieren oder Deaktivieren von Systembenachrichtigungen für Ihr Nutzerkonto

Die NetWitness Platform-Systembenachrichtigungen werden bei der Erstellung eines neuen Benutzerkontos standardmäßig aktiviert. Sie können diese Benachrichtigungen jederzeit deaktivieren und aktivieren.

1. Im Dialogfeld „Voreinstellungen“:
   - Aktivieren Sie zum Aktivieren von Benachrichtigungen für Ihr Nutzerkonto das Kontrollkästchen **Benachrichtigungen aktivieren**.
   - Deaktivieren Sie zum Deaktivieren von Benachrichtigungen das Kontrollkästchen **Benachrichtigungen aktivieren**.
2. Klicken Sie auf **Anwenden**.
   Ihre neue Einstellung wird sofort wirksam.

### Aktivieren oder Deaktivieren von Kontextmenüs für Ihr Nutzerkonto

Bei der Erstellung eines neuen Nutzerkontos sind Kontextmenüs standardmäßig aktiviert. Durch Klicken mit der rechten Maustaste in einer Ansicht werden Kontextmenüs mit weiteren Funktionen für bestimmte Ansichten geöffnet.

1. Im Dialogfeld „Voreinstellungen“:
   - Aktivieren Sie zur Aktivierung von Kontextmenüs für Ihr Nutzerkonto das Kontrollkästchen **Kontextmenüs aktivieren**.
   - Deaktivieren Sie zur Deaktivierung von Kontextmenüs das Kontrollkästchen **Kontextmenüs aktivieren**.
2. Klicken Sie auf **Anwenden**.
   Ihre neue Einstellung wird sofort wirksam.

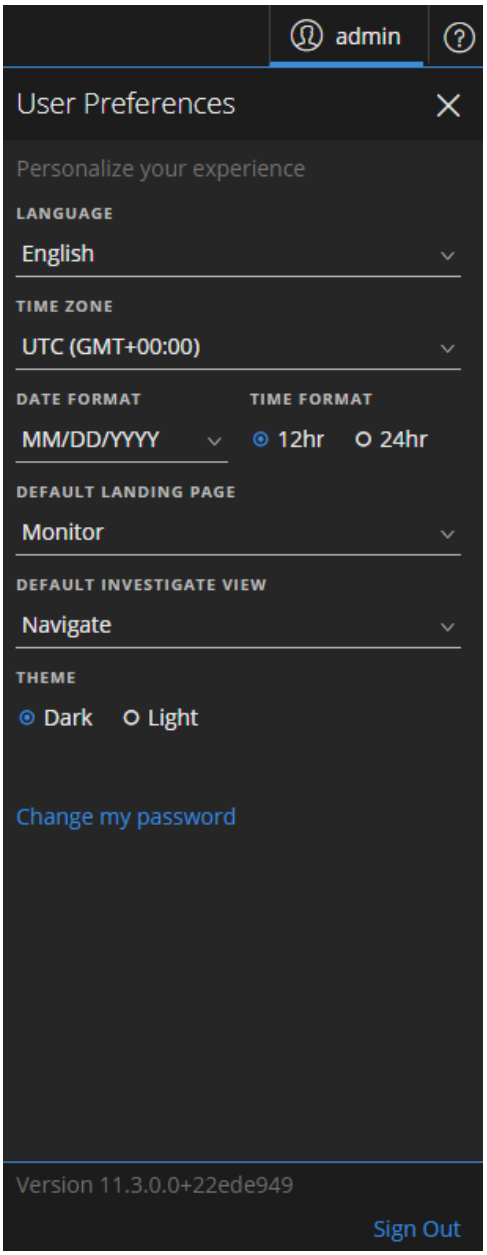
**Hinweis:** Die auf der Registerkarte „Untersuchen“ im Dialogfeld „Einstellungen“ verfügbaren Einstellungen sind im *NetWitness Investigate – Benutzerhandbuch* dokumentiert.

## Nutzereinstellungen (Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten)

In diesem Abschnitt finden Sie Anweisungen für verschiedene Aufgaben, die im Dialogfeld „Nutzereinstellungen“ ausgeführt werden können. Es ist über die „Reagieren“-Ansicht und einige „Untersuchen“-Ansichten aufrufbar.

### Anzeigen der Nutzereinstellungen

Wählen Sie in der rechten oberen Ecke des NetWitness Platform-Browserfensters  aus.
Im Dialogfeld „Nutzereinstellungen“ werden die aktuellen Einstellungen angezeigt, wenn es über die Ansicht „Reagieren“ und folgende „Untersuchen“-Ansichten aufgerufen wird: Ereignisanalyse, Hosts, Dateien und Nutzer.




Die von Ihnen vorgenommenen Einstellungen werden sofort wirksam.

## Einstellen von Sprache, Zeitzone und Datums- und Zeitformat

**Hinweis:** Die Einstellung der Sprache ist ab NetWitness Platform 11.2 verfügbar.

Sie können die Sprache für NetWitness Platform ändern. Die Standardsprache ist Englisch (USA). Sie können auch die Zeitzone und das Datums- und Uhrzeitformat für Ihren Standort ändern.

1. Öffnen Sie das Dialogfeld „Nutzereinstellungen“.
2. Wählen Sie im Dialogfeld „Benutzereinstellungen“ Ihre Lokalisierungseinstellungen aus:
   a. **Sprache**: Wählen Sie Ihre bevorzugte Sprache für NetWitness Platform aus.
   b. **Zeitzone**: Legen Sie die Zeitzone für die Verwendung in NetWitness Platform fest.
   c. **Datumsformat**: Legt das Format für die Reihenfolge der Anzeige von Monat (MM), Tag (TT) und Jahr (JJJJ) fest. Das Format MM/TT/JJJJ zeigt beispielsweise das Datum als 05/11/2017 an.
   d. **Zeitformat**: Legen Sie die Uhrzeit als 12- oder 24-Stunden-Uhrzeit fest. 2:00 Uhr im 12-Stunden-Zeitformat ist z. B. 14:00 Uhr im 24-Stunden-Zeitformat.

   Änderungen in den Ansichten „Reagieren“ und „Untersuchen“ werden sofort wirksam.

**Hinweis:** Wenn für die ausgewählte Zeitzone des aktuell angemeldeten Nutzers die Sommerzeit gilt, wird in der Benutzeroberfläche automatisch die korrekte Zeit angezeigt.

## Auswählen der standardmäßigen Startansicht der NetWitness Platform

1. Öffnen Sie das Dialogfeld „Nutzereinstellungen“.
2. Wählen Sie im Feld **Standardmäßige Landingpage** die Ansicht beim Öffnen aus, die Sie sehen möchten, wenn Sie sich bei NetWitness Platform anmelden. Sie können entsprechend Ihrer Nutzerrolle „Reagieren“, „Untersuchen“, „Überwachen“, „Konfigurieren“ und „Admin“ auswählen. Beispielsweise können Sie „Reagieren“ auswählen, um direkt zum entsprechenden Abschnitt der Anwendung für Incident-Experten zu wechseln. Unter Einrichten einer Standardansicht nach SOC-Rolle erhalten Sie Informationen zur Auswahl der geeigneten Standardansicht.
   Diese Auswahl wird die Standardansicht für die gesamte Anwendung. Die Änderungen werden sofort wirksam.

## Festlegen der standardmäßigen Ansicht „Untersuchen“

1. Öffnen Sie das Dialogfeld „Nutzereinstellungen“.
2. Legen Sie im Feld **Standardmäßige Ansicht „Untersuchen“** die standardmäßige Landingpage fest, die angezeigt werden soll, wenn Sie sich bei NetWitness Platform anmelden und zu „Untersuchen“ navigieren. Sie können die Ansicht „Navigieren“, „Ereignisse“, „Ereignisanalyse“, „Hosts“, „Dateien“, „Nutzer“ oder „Malware Analysis“ als standardmäßige „Untersuchen“-Ansicht auswählen. Beispielsweise können Sie „Ereignisse“ als standardmäßige Ansicht „Untersuchen“ wählen, um direkt zu „Ereignisse“ zu gehen und die für einen Service generierten Ereignisse anzuzeigen. Unter Einrichten einer Standardansicht nach SOC-Rolle erhalten Sie Informationen zur Auswahl der geeigneten Standardansicht. Weitere Informationen finden Sie im *NetWitness Investigate – Benutzerhandbuch*.

**Hinweis:** Nachdem Sie die Änderung in der Drop-down-Liste angewendet haben, kann es manchmal einige Sekunden dauern, bis sie wirksam wird.

## Festlegen der Darstellung der NetWitness Platform

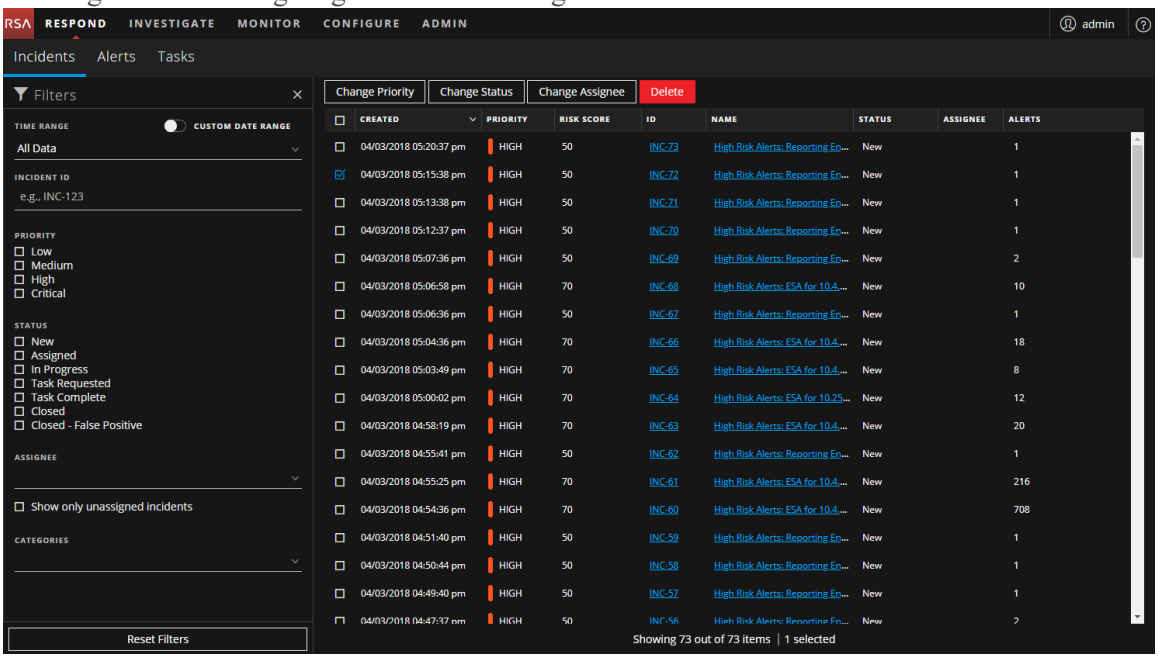
**Hinweis:** Diese Option ist nur für NetWitness Platform Version 11.1 und höher verfügbar.

Sie können je nach persönlicher Präferenz ein dunkles oder ein helles Design für Ihre Anwendung auswählen. Wenn Sie das Design ändern, übernehmen die Ansicht „Reagieren“ und einige Ansichten „Untersuchen“ das helle oder dunkle Design. Ihre Auswahl wirkt sich nur darauf aus, wie NetWitness Platform für Sie dargestellt wird, nicht auf die Darstellung für andere Nutzer.

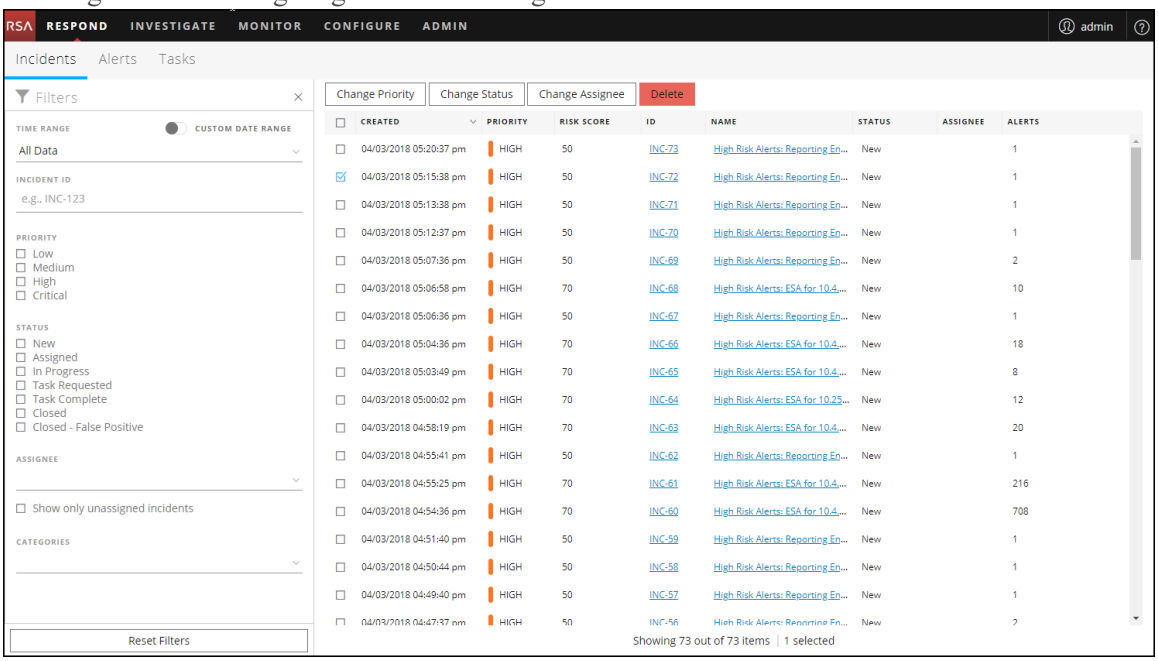
1. Öffnen Sie das Dialogfeld „Nutzereinstellungen“.
2. Wählen Sie unter **DESIGN** eine der folgenden Optionen aus:
   - **Dunkel**: Das dunkle Design ist am besten für dunklere Umgebungen geeignet oder wenn Sie nicht so viel Kontrast benötigen.
   - **Hell**: Das helle Design ist am besten für hellere Umgebungen geeignet, wenn Sie mehr Kontrast benötigen oder wenn Sie die Anwendung projizieren, damit andere sie sehen können. Da einige Ansichten von den Designänderungen nicht betroffen sind, wird empfohlen, für eine einheitliche Anzeige das hellere Design auszuwählen.

Die Änderungen werden sofort wirksam.

Die folgende Abbildung zeigt das dunkle Design.



Die folgende Abbildung zeigt das helle Design.



# Managen von Dashboards

Ein Dashboard besteht aus einer Gruppe von Dashlets, mit denen Sie bedeutende Snapshots verschiedener Komponenten, die Sie als wichtig erachten, in einem Bereich anzeigen können. In RSA NetWitness® Platform können Sie Dashboards zusammensetzen, um allgemeine Informationen und Kennzahlen zu erhalten, die ein Gesamtbild der NetWitness Platform-Bereitstellung darstellen, und nur die wichtigsten Informationen anzeigen, die für den täglichen Betrieb von Bedeutung sind.

Standardmäßig wird das NetWitness Platform-Dashboard angezeigt, wenn Sie sich bei NetWitness Platform anmelden. Es enthält einige nützliche Dashlets, die Sie bei Ihren ersten eigenen Anpassungen unterstützen. Die Dashboards für alle NetWitness Platform-Komponenten können dem Standard-NetWitness Platform-Dashboard oder einem benutzerdefinierten NetWitness Platform-Dashboard hinzugefügt werden.

Sie können verschiedene Bereiche des Dashboards und Berichte je nach Ihren Benutzerberechtigungen anzeigen. Sie können ein vorkonfiguriertes Dashboard auswählen, ein Dashboard importieren oder Ihr eigenes angepasstes Dashboard erstellen. Mit den Dashboards können Sie schnell und einfach Berichte anzeigen. Sie können Dashboards so konfigurieren, dass die Informationen angezeigt werden, die Ihren Workflow unterstützen. In diesem Thema werden die allgemeinen Aufgaben beschrieben, die durchgeführt werden können, wenn Sie ein Dashboard einrichten.

## Dashboard-Grundlagen

Wenn die Ansicht „Überwachung“ Ihre standardmäßige Landingpage nach der Anmeldung bei NetWitness Platform ist, wird Ihnen immer das Standarddashboard oder das aktuell konfigurierte Dashboard nach erfolgter Anmeldung angezeigt. Wählen Sie zum Zurückkehren zum Dashboard von einer anderen NetWitness Platform-Komponente die Optionen **Überwachung** > **Übersicht**.

### Dashboard-Titel

Der Dashboard-Titel bezieht sich auf das aktive Dashboard, zum Beispiel das Standard-Dashboard.


### Dashboard-Auswahlliste

Mithilfe der Dashboardauswahlliste können Sie auf vorkonfigurierte und benutzerdefinierte Dashboards zugreifen. Wenn Sie ein Dashboard auswählen, wird der Titel neben der NetWitness Platform-Symbolleiste angezeigt.


Ein Dashboard verfügt über Folgendes:

- die Dashboard-Symbolleiste
- den Dashboard-Titel und die Dashboards-Auswahlliste

## Dashboard-Symbolleiste

Die Dashboardsymbolleiste ist neben dem Titel des ausgewählten Dashboards verfügbar. Mit der Dashboard-Symbolleiste können verschiedene Funktionen für das Dashboard und die Dashlets ausgeführt werden.


**Hinweis:** Die Optionen „Kopieren“, „Löschen“, „Importieren“, „Exportieren“, „Freigeben“ und „Zeile hinzufügen“ sind für vorkonfigurierte Dashboards deaktiviert.

| Option | Beschreibung |
|---|---|
| ★ | Legt das ausgewählte Dashboard als Favoriten fest. |
| Default Dashboard | Zeigt die Liste der verfügbaren Dashboards an, aus denen Sie auswählen können. |

| Option | Beschreibung |
|---|---|
|  | Das Dialogfeld „Dashboard erstellen“ wird angezeigt. Hier können Sie ein benutzerdefiniertes Dashboard erstellen oder hinzufügen. |
|  | Löscht ein benutzerdefiniertes Dashboard. Das Standard-Dashboard kann nicht gelöscht werden. |
|  | Ermöglicht Ihnen das Kopieren eines Dashboards. |
|  | Zeigt das Dialogfeld „Dashlet managen“. |
|  | Exportiert ein Dashboard als ZIP-Datei. |
|  | Importiert ein Dashboard als ZIP- oder CFG-Datei. |
|   | Ermöglicht Ihnen die Freigabe eines Dashboards für einen anderen Nutzer. |
|   | Ermöglicht Benutzern, dem Dashboard basierend auf den Anforderungen Zeilen und Spalten hinzuzufügen.<br>Klicken Sie auf das  -Symbol in einer Zeile, um ein Dashlet hinzufügen. |

### Das Standard-Dashboard

Das Standard-Dashboard ist so konfiguriert, dass bestimmte Dashlets in einer bestimmten Anordnung angezeigt werden. Das Standard-Dashboard stellt ein Beispiel für eine Zusammensetzung eines Dashboard dar und bietet den Ausgangspunkt für die benutzerdefinierte Anpassung.

- Sie können die Informationen auf dem Standarddashboard durch Bearbeiten, Hinzufügen, Löschen, Verschieben und Maximieren von Dashlets anpassen.
- Nachdem Sie das Standarddashboard (  ) bearbeitet haben, können Sie dieses wieder in das ursprüngliche Layout zurücksetzen.
- Das Standarddashboard kann nicht gelöscht oder freigegeben werden.

## Auswählen eines vorkonfigurierten Dashboards

Bei der Installation von NetWitness Platform Suite werden die folgenden vorkonfigurierten Dashboards automatisch aktiviert und stehen Ihnen zur Verfügung:

- Standard
- Identität
- Investigation

- Vorgänge – Dateianalyse
- Vorgänge – Protokolle
- Vorgänge – Netzwerk
- Vorgänge – Protokollanalyse
- Übersicht
- RSA SecurID
- Bedrohung – Suche
- Bedrohung – Angriff
- Bedrohung – Malwareindikatoren

Sie können in einem vorkonfigurierten Dashboard die folgenden Aktionen nicht ausführen:

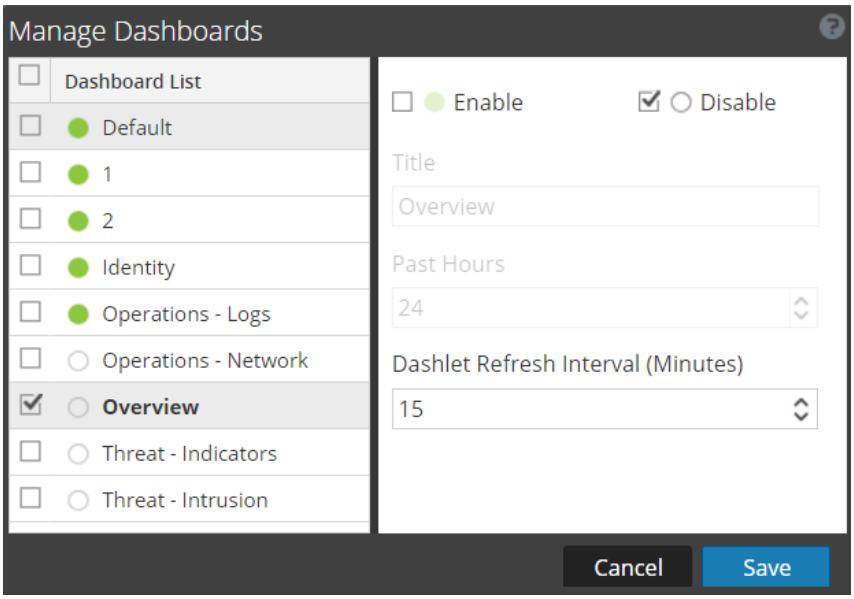
- Bearbeiten eines Dashboards
- Exportieren eines Dashboards
- Freigeben eines Dashboards
- Löschen eines Dashboard

Weitere Informationen zu den einzelnen vorkonfigurierten Dashboards, finden Sie im Dashboardkatalog im Bereich RSA Content auf RSA Link.

## Aktivieren oder Deaktivieren von Dashboards

Wenn Sie ein Dashboard aktivieren oder deaktivieren, werden alle Dashlets im Dashboard mit den zugehörigen Diagrammen aktiviert oder deaktiviert, es sei denn, sie werden in einem anderen Dashboard genutzt.

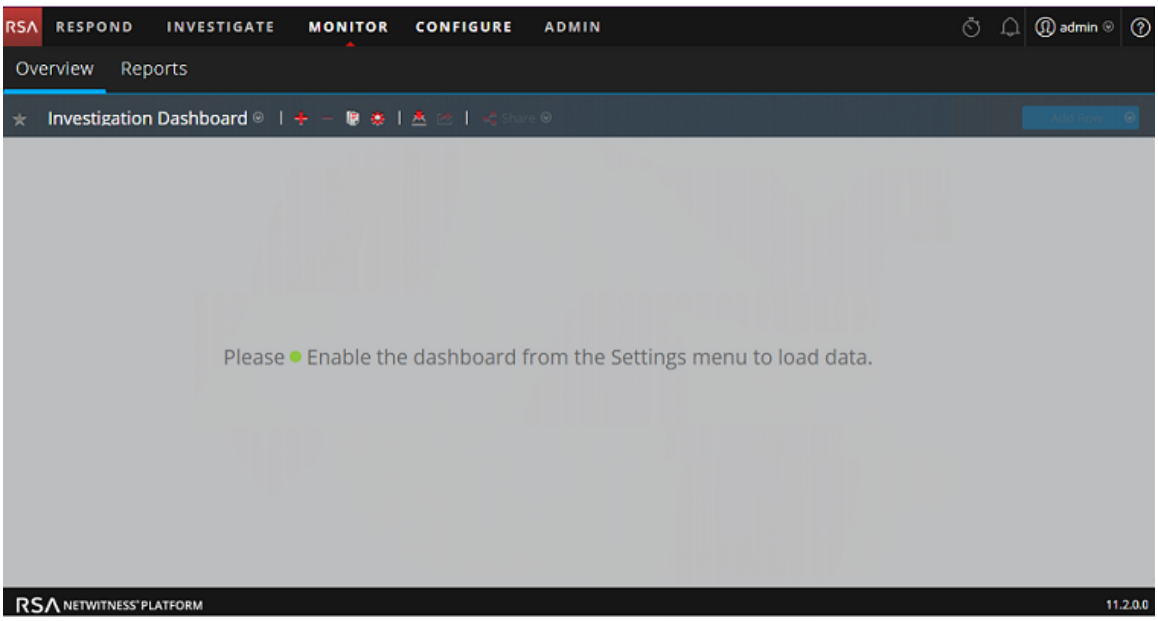
NetWitness Platform-Module können nur die Dashlets anzeigen, die im Dialogfeld „Dashlet managen“ zur Verfügung stehen. Das Haupt-Dashboard bietet alle NetWitness Platform-Dashlets. Dies ist ein Beispiel für aktuell verfügbare Dashlets.




| Name | Beschreibung |
|---|---|
| Dashboardliste | Zeigt eine Liste der standardmäßigen, vorkonfigurierten und benutzerdefinierten Dashboards an. |
| Enable | Zeigt an, ob das ausgewählte Dashlet aktiviert ist. |
| Disable | Zeigt an, ob das ausgewählte Dashlet deaktiviert ist. |
| Titel | Zeigt den Titel des ausgewählten Dashlets an. Sie können auch das Dashboard umbenennen. |
| Vergangene Stunden | Zeigt den Zeitpunkt, zu dem die Daten erfasst werden. |
| Dashlet-Aktualisierungsintervall (Minuten) | Zeigt das Aktualisierungsintervall eines Dashlets an. |

## Aktivieren eines Dashboards

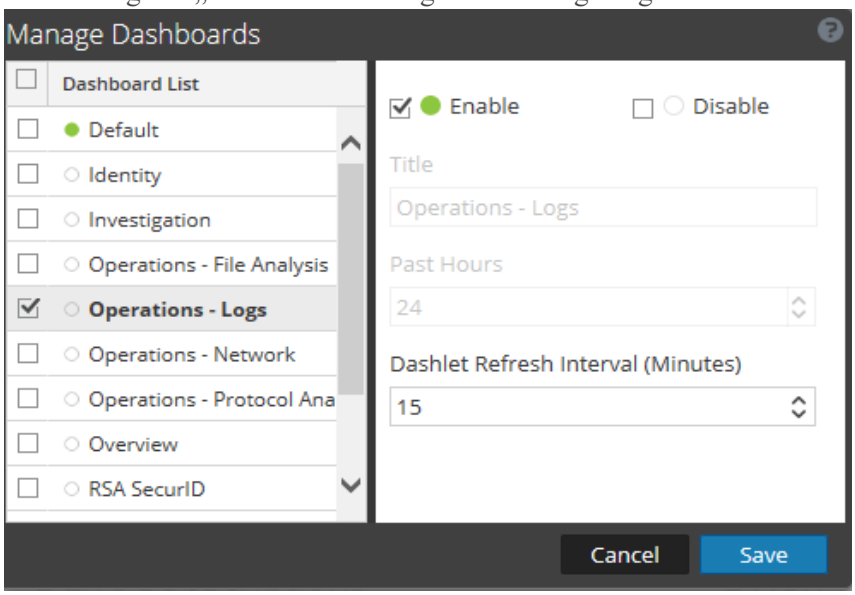
Wenn Sie ein Dashboard auswählen, das nicht aktiviert ist, wird ein maskierter Bildschirm angezeigt.




So aktivieren Sie ein oder mehrere Dashboard(s):

1. Navigieren Sie zu dem Dashboard, das aktiviert werden soll.

2. Klicken Sie in der Dashboard-Symbolleiste auf  (Dashboards managen).
Das Dialogfeld „Dashboards managen“ wird angezeigt.




3. Wählen Sie aus der Dashboardliste die zu aktivierenden Dashboards aus.

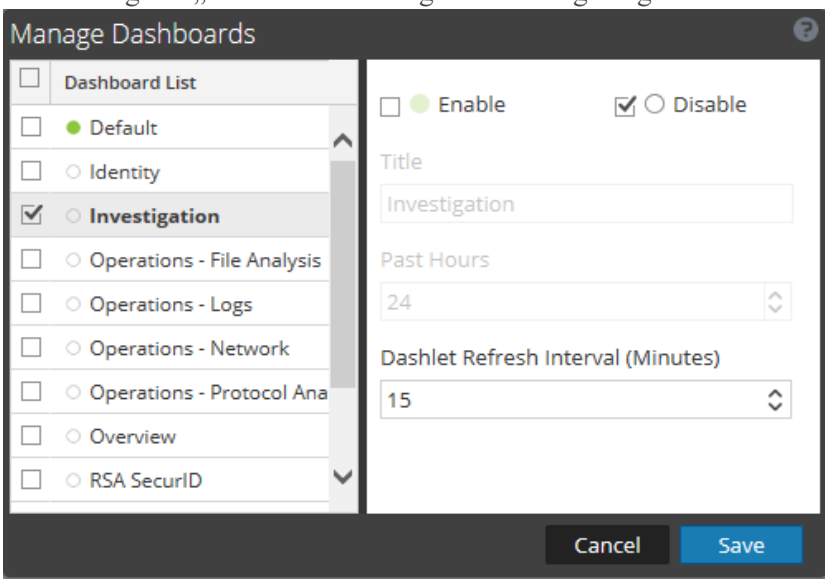
4. Aktivieren Sie das Kontrollkästchen **Aktivieren**.

5. Klicken Sie auf **Speichern**.

### Deaktivieren eines Dashboards

So deaktivieren Sie ein oder mehrere Dashboards:

1. Navigieren Sie zu dem Dashboard, das deaktiviert werden soll.
2. Klicken Sie in der Dashboard-Symbolleiste auf  (Dashboards managen).
   Das Dialogfeld „Dashboards managen“ wird angezeigt.




3. Wählen Sie aus der Dashboardliste die zu deaktivierenden Dashboards aus.
4. Aktivieren Sie das Kontrollkästchen **Deaktivieren**.
5. Klicken Sie auf **Speichern**.

## Einstellen eines Dashboards als Favoriten

Sie können zum Anpassen der Ansichten in NetWitness Platform ein vorkonfiguriertes oder benutzerdefiniertes Dashboard als Favoriten festlegen. Das NetWitness Platform-Dashboard bietet alle NetWitness Platform-Dashlets. Im Dialogfeld „Favorit“ wird ein spezifisches Dashboard als Ihr bevorzugtes Dashboard festgelegt. Jedes Mal, wenn Sie sich bei NetWitness Platform anmelden, wird dieses Dashboard als Favorit angezeigt.

1. Navigieren Sie zu einem beliebigen Dashboard.
2. Klicken Sie in der Dashboard-Symbolleiste auf  .

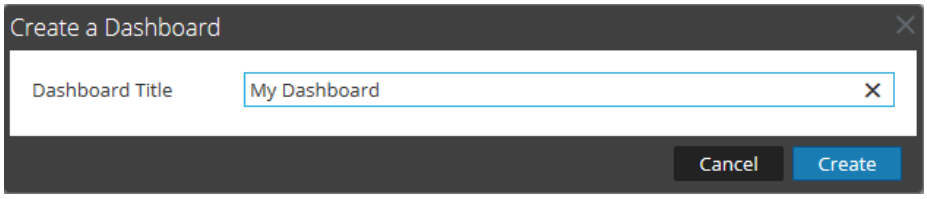
   Wenn das „Favorit“-Symbol in der Farbe Rot angezeigt wird, bedeutet dies, dass das ausgewählte Dashboard als Favorit festgelegt und oberhalb der Zeile aufgeführt wird.

## Erstellen von benutzerdefinierten Dashboards

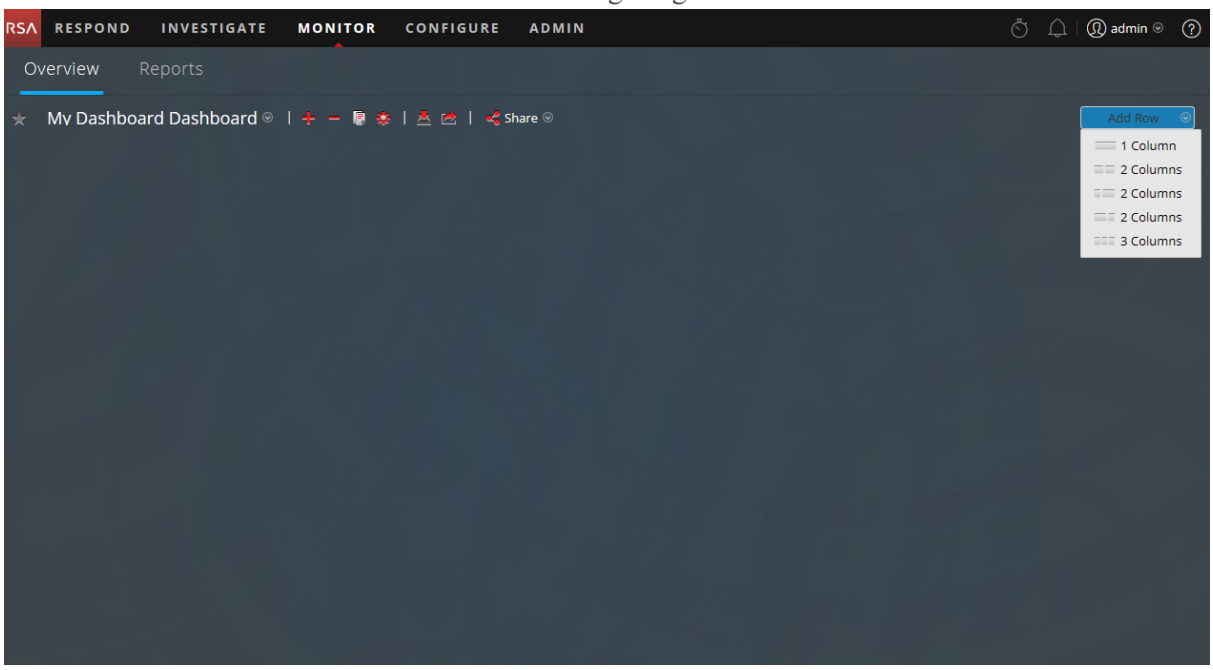
Sie können ein Dashboard für einen bestimmten Zweck anpassen, zum Beispiel, um einen bestimmten geografischen oder funktionalen Bereich des Netzwerks darzustellen. Jedes definierte Dashboard wird der Dashboardauswahlliste hinzugefügt.

So erstellen Sie ein angepassten Dashboard:

1. Klicken Sie in der Dashboardsymbolleiste auf  .
   Das Dialogfeld „Dashboard erstellen“ wird angezeigt.



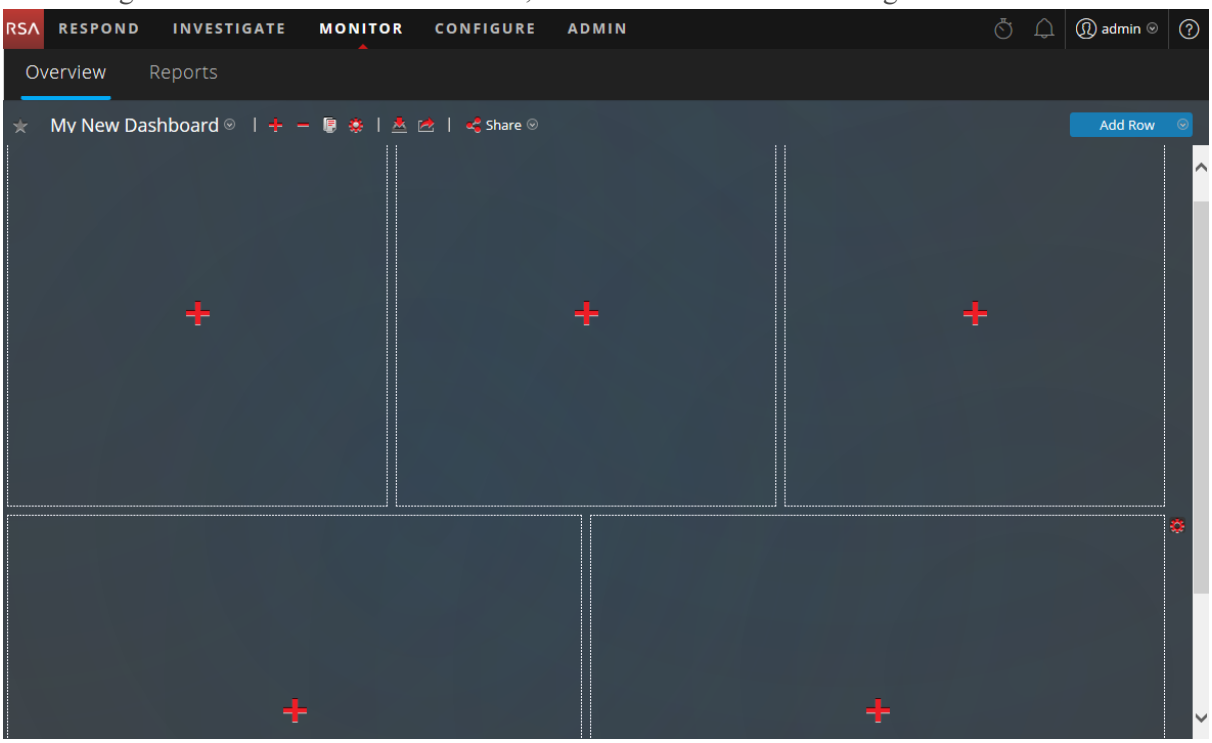

2. Geben Sie einen Titel für das neue Dashboard ein und klicken Sie auf **Erstellen**.
   Das neue Dashboard wird als leerer Bildschirm angezeigt.




3. Fügen Sie mit der Option **Zeile hinzufügen** auf der rechten Seite des Bildschirms ( 

) Zeilen mit einer oder mehreren Spalten hinzu. Klicken Sie auf die gewünschten Spaltenkonfiguration in der Drop-down-Liste, um dem Dashboard eine Zeile mit der ausgewählten Anzahl von Spalten

hinzuzufügen. Wiederholen Sie den Prozess, um weitere Zeilen hinzuzufügen.




4. Sie können jetzt alle gewünschten Dashlets zum Dashboard hinzufügen, indem Sie in einem leeren Platzhalter in einer Zeile auf + klicken. Weitere Informationen zum Hinzufügen und Managen von Dashlets, finden Sie unter Arbeiten mit Dashlets.

Sobald Sie benutzerdefinierte Dashboards erstellt haben, können Sie:

- zwischen Dashboards wechseln, indem Sie eine Option aus der Dashboard-Auswahlliste auswählen.
- benutzerdefinierte Dashboards löschen.
- ein Dashboard importieren oder exportieren.

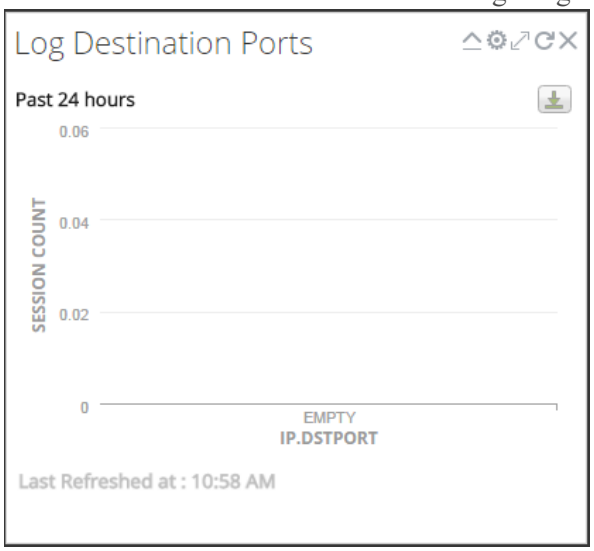
Jedes Dashboard verfügt über:

- die Dashboard-Symbolleiste
- den Dashboard-Titel und die Dashboards-Auswahlliste
- kein oder mehrere Dashlets

## Arbeiten mit Dashlets

NetWitness Platform verwendet Dashlets, um zielgerichtete Untergruppen von Systeminformationen, Services, Jobs, Ressourcen, Abonnements, Regeln und andere Informationen anzuzeigen.

Die Steuerelemente eines Dashlet befinden sich in der Titelleiste. Alle Dashlets besitzen einen gemeinsamen Satz von Steuerelementen. Nur diejenigen, die dem bestimmten Dashlet entsprechen, werden in der Titelleiste des Dashlets angezeigt.




In der folgenden Tabelle werden die Symbole beschrieben, die im Dashboard angezeigt werden.

| Symbol | Name | Beschreibung |
|---|---|---|
| | Vertikal ausblenden | Das Dashlet wird vertikal ausgeblendet, sodass nur der Titel sichtbar ist. |
| | Vertikal einblenden | Das Dashlet wird in Originalgröße eingeblendet. |
| | Neu laden | Das Dashlet wird neu geladen. |
| | Einstellungen | Zeigt die konfigurierbaren Einstellungen für das Dashlet an. |
| | Maximieren | Bei manchen Dashlets mit Inhalten, die nicht horizontal in das Dashlet passen, können Sie ein Diagramm maximieren oder das Dashlet im Vollbildmodus anzeigen. |
| | Löschen | Löscht das Dashlet aus dem Dashboard |
| Letzte Aktualisierung | | Zeigt den Zeitpunkt, an dem die Daten über das zugehörige Diagramm abgefragt wurden. |
| Mehr anzeigen | | Führt beim Anklicken zum entsprechenden Dashboard, das mit dem Haupt-Dashlet verknüpft ist, und zeigt weitere Informationen an. Wenn Sie das Dashboard nicht mit einem bestehenden Dashlet verknüpft haben, steht Ihnen dieser Link bei diesem Dashlet nicht zur Verfügung. Klicken Sie zur Konfiguration dieser Option auf und wählen Sie im Feld „Dashboard-Verknüpfung“ eine verbundene Dashboardansicht aus, um weitere Informationen zum bestimmten Dashlet anzuzeigen. |

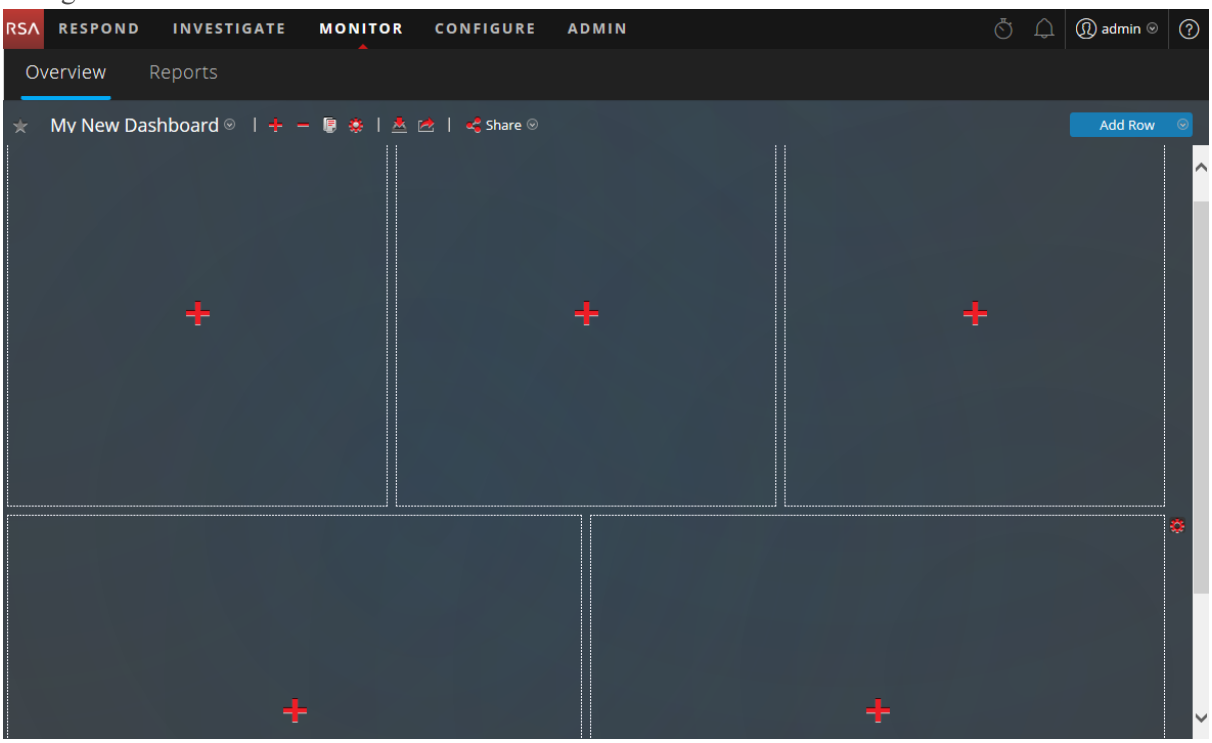
Sie können dem Standard-Dashboard Dashlets hinzufügen oder ein benutzerdefiniertes Dashboard mit Ihrem eigenen nützlichen Satz Dashlets erstellen, um Ihren Workflow effizienter zu gestalten.

## Dashlet hinzufügen

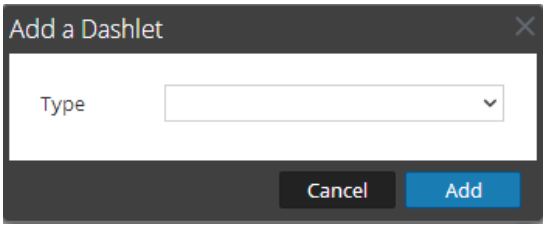
Zum Anpassen der Ansichten in NetWitness Platform können Sie im Standarddashboard Dashlets hinzufügen oder benutzerdefinierte Dashboards erstellen. Sie können vorkonfigurierten Dashboards jedoch keine Dashlets hinzufügen.

So fügen Sie ein Dashlet hinzu:

1. Navigieren Sie zu einem Dashboard oder erstellen Sie ein neues Dashboard.

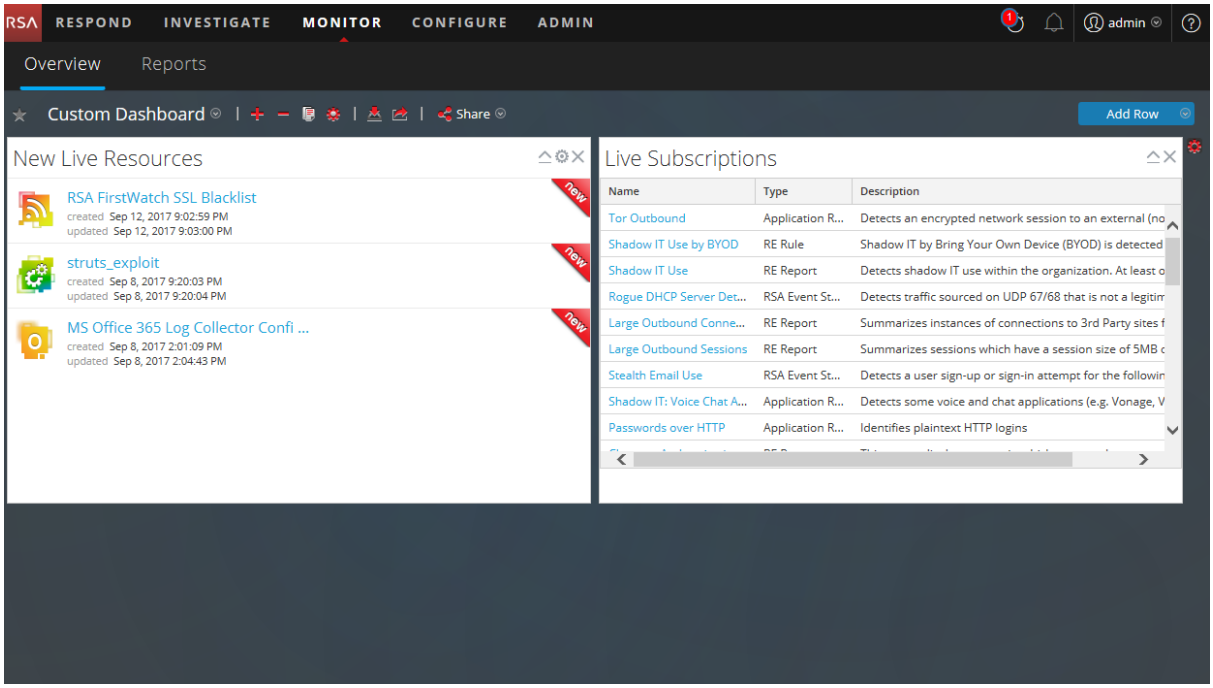



2. Klicken Sie auf  auf dem Platzhalter, an dem Sie das Dashlet hinzufügen möchten.
Das Dialogfeld „Dashlet hinzufügen“ wird angezeigt.




3. Klicken Sie auf die Auswahlliste **Typ**, um die verfügbaren Dashlets anzuzeigen, und wählen Sie den Typ des Dashlets aus, den Sie hinzufügen möchten. Je nach Typ des Dashlet, den Sie hinzufügen, werden einige konfigurierbare Felder im Dialogfeld **Dashlet hinzufügen** angezeigt.
4. Geben Sie einen Titel für das Dashlet ein. Der Titel kann Buchstaben, Ziffern, Sonderzeichen und Leerstellen umfassen.

5. Wenn weitere konfigurierbare Felder für dieses Dashlet angezeigt werden, legen Sie die entsprechenden Werte fest.
6. Klicken Sie auf **Hinzufügen**, wenn alle Pflichtfelder konfiguriert wurden.
   Das Dashlet wird dem Dashboard im ausgewählten Platzhalter hinzugefügt und wird automatisch gespeichert.




## Bearbeiten der Dashlet-Eigenschaften

Alle vorkonfigurierten Dashlets sind schreibgeschützt und die Eigenschaften können nicht bearbeitet werden. Andere Dashlets sind bearbeitbar, damit Nutzer einige Aspekte der im Dashlet angezeigten Daten anpassen können. Ein Dashlet mit bearbeitbaren Eigenschaften verfügt über eine Einstellungsoption ( ⚙ ), die alle Bearbeitungsoptionen anzeigt.

Nachdem die Dashlets hinzugefügt wurden, können Sie sie per Drag-and-drop verschieben und austauschen.

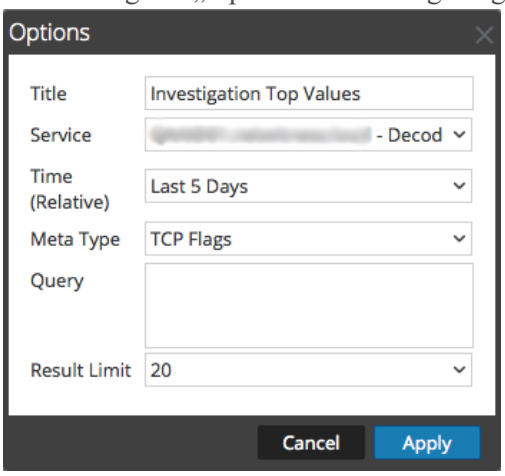
Wenn ein Dashlet keine bearbeitbaren Eigenschaften hat, z. B. das Dashlet „Live-Abonnements“, wird die Einstellungsoption nicht in der Titelleiste angezeigt. Viele Dashlets haben einen bearbeitbaren Titel, in dem Sie die folgenden Eigenschaften bearbeiten können:

- Dashlet-Anzeigetitel.
- Art der zu überwachenden Services, z. B. können Sie nur Decoder überwachen oder Decoder und Concentrators überwachen

Andere Dashlets haben Parameter, die Sie definieren, um die Art und die Menge der Informationen anzugeben, die im Dashlet angezeigt werden sollen. Beispielsweise verfügt ein Echtzeitdiagramm-Dashlet über die Einstellungsoption.

1. Klicken Sie zum Anzeigen und Ändern der Optionen für ein Dashlet in einer Dashlet-Titelleiste auf Einstellungen ( ⚙ ).

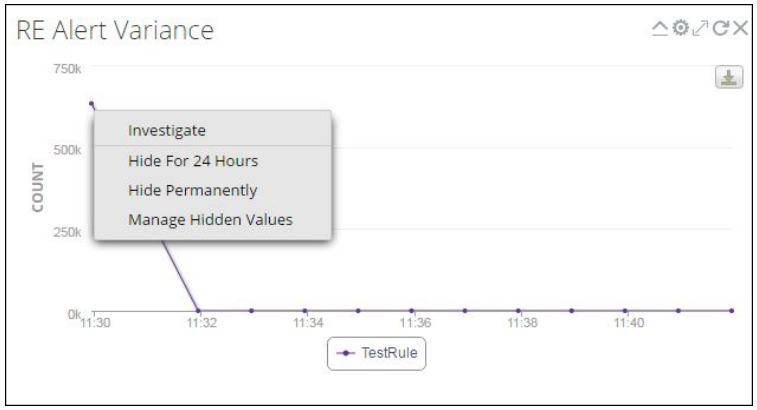
Das Dialogfeld „Optionen“ wird angezeigt.




2. Bearbeiten Sie die gewünschten angezeigten Eigenschaften. Sie können zum Beispiel im Dashlet „Investigation Top-Werte“ den „Ergebnisgrenzwert“ von 20 in 40 ändern.
3. Klicken Sie auf **Anwenden**.

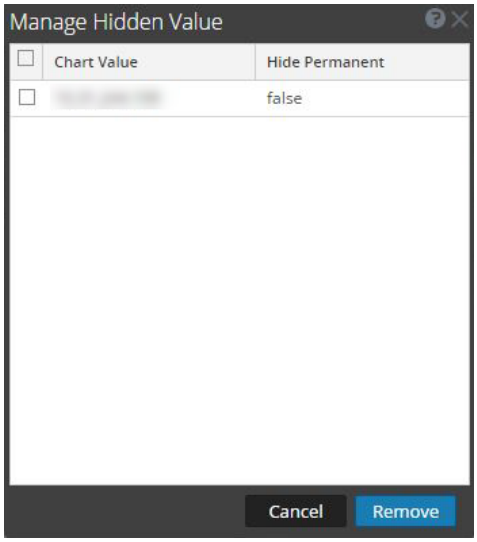
Einige Dashlets enthalten Konfigurationsoptionen, mit denen Sie die Darstellung oder den Inhalt des Dashlet anpassen können. Die folgenden Optionen stehen durch Linksklick für die Top-RE-Warnmeldungen, RE-Warnmeldungsvarianz und RE-Echtzeitdiagramm-Dashlets zur Verfügung:

- **Für 24 Stunden ausblenden**: Mit dieser Option können Sie den ausgewählten Wert für die nächsten 24 Stunden ausblenden. Nach 24 Stunden werden die Daten automatisch im Dashlet angezeigt, wenn der Wert konfiguriert und oben aufgelistet wird.
- **Permanent ausblenden**: Mit dieser Option können Sie den ausgewählten Wert dauerhaft ausblenden, bis Sie ihn erneut mit der Option „Ausgeblendete Werte managen“ hinzufügen.




- **Ausgeblendete Werte managen**: Diese Option zeigt eine Liste aller ausgeblendeten Werte an. Sie können das Kontrollkästchen für einen Wert auswählen und auf **Entfernen** klicken, um die Daten

wieder auf dem Diagramm anzuzeigen.




Die Optionen zum Ausblenden für 24 Stunden, zum permanenten Ausblenden und zum Managen ausgeblendeter Werte sind für Geomap-Diagramme nicht verfügbar.

**Hinweis:** Wenn Sie einen Wert in einem vorkonfigurierten Dashboard bearbeiten, ist dies eine benutzerspezifische Änderung. Die Änderungen an einem vorkonfigurierten Dashboard gelten nur für Ihr Dashboard und können nicht von anderen Nutzern angezeigt werden, die dasselbe vorkonfigurierte Dashboard verwenden. Wenn Sie beispielsweise einen Wert in einem Übersichtsdashboard ausblenden, gelten die Änderungen nur für Ihr Dashboard. Wenn ein anderer Nutzer dasselbe Übersichtsdashboard aufruft, kann er den Wert weiterhin sehen. Dasselbe gilt für ein benutzerdefiniertes Dashboard. Wenn Sie einen Wert im benutzerdefinierten Dashboard ausblenden und das Dashboard für einen anderen Nutzer freigeben, ist der Wert für ihn weiterhin zu sehen, auch wenn das Dashboard freigegeben ist.

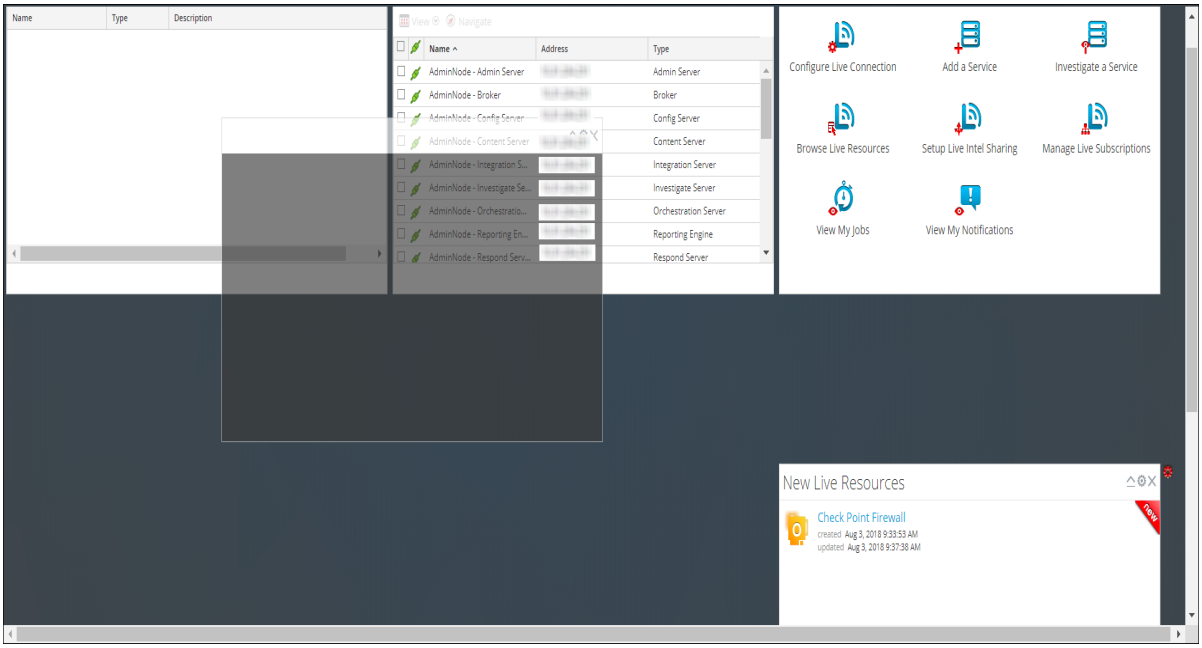
Weitere Informationen zu den einzelnen verfügbaren Dashboards, finden Sie im Dashboardkatalog im Bereich RSA Content auf RSA Link.

## Neuanordnung eines Dashlet

Sie können Dashlets durch Ziehen und Ablegen (Drag-and-drop) in einer anderen Reihenfolge im Dashboard anordnen.

1. Bewegen Sie zum Verschieben eines Dashlet den Mauszeiger auf die Titelleiste eines Dashlet, das Sie verschieben möchten.
   Der Verschieben-Cursor wird am Dashlet angezeigt. Klicken Sie auf die Titelleiste eines Dashlet, das Sie verschieben möchten, und halten Sie die Maustaste gedrückt.

2. Halten Sie die linke Maustaste weiter gedrückt und ziehen Sie das Fenster an die neue Position. Die Abbildung unten zeigt ein Dashlet, während es neu angeordnet wird.



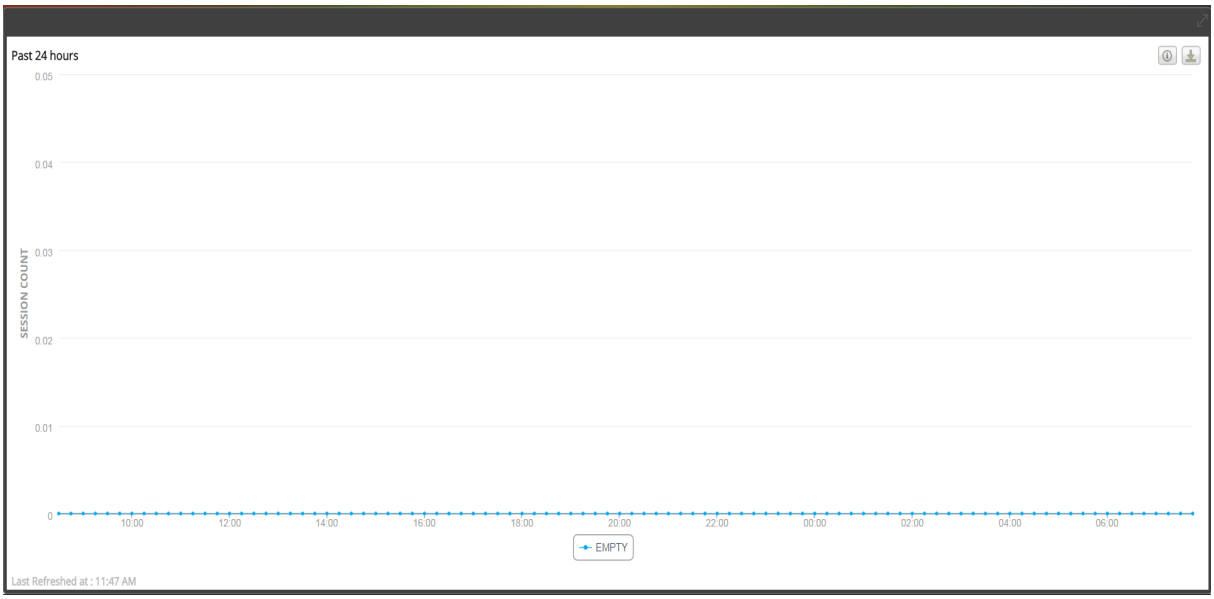

3. Lassen Sie die Maustaste los, wenn sich das Dashlet an der gewünschten Position befindet. Das Dashlet, das sich zurzeit an dieser Position befindet, wird nach unten verschoben.

## Maximieren eines einzelnen Dashlets

In diesem Abschnitt wird erläutert, wie Sie ein Dashlet so öffnen, dass es den gesamten Bereich des NetWitness Platform-Dashboards ausfüllt. Dashlets mit vielen Spalten oder Diagrammen, z. B. einige Reporting-Dashlets, sind einfacher zu betrachten, wenn sie maximiert sind, sodass der gesamte Inhalt ohne Bildlauf sichtbar ist.

Klicken Sie zum Maximieren eines Diagramm- oder Warnmeldungs-Dashlet auf das Symbol zum Maximieren in der Dashlet-Titelleiste: ⤢. Das Dashlet wird auf dem gesamten Bildschirm angezeigt.

Klicken Sie zum Minimieren eines Dashlet auf das Symbol in der Titelleiste des Dashlet: ⤢. Das Dashlet wird in der vorherigen Größe wiederhergestellt.




### Löschen von Dashlets

1. Klicken Sie in der Titelleiste auf ✕:
   .Ein Pop-up-Fenster wird angezeigt, in dem Sie bestätigen müssen, ob Sie das Dashlet löschen möchten.
2. Klicken Sie auf **Ja**, wenn Sie es löschen möchten. Das Dashlet wird aus dem Dashboard entfernt.
   Klicken Sie auf **Nein**, wenn Sie es nicht löschen möchten.

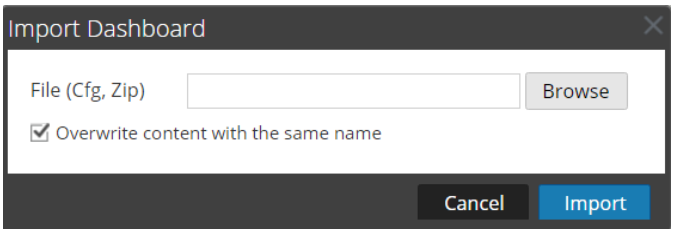
**Hinweis:** Nachdem Sie das Dashlet entfernt haben, wird der leere Bereich durch einen Platzhalter ersetzt, in dem Sie ein anderes Dashlet mithilfe des oben beschriebenen Verfahrens „Dashlet hinzufügen“ hinzufügen können.

## Importieren und Exportieren von Dashboards

Die Möglichkeit, Dashboards an sich ändernde Bedingungen anzupassen, kann zu einer großen Anzahl von Dashboards führen, von denen nicht alle täglich benötigt werden. Anstatt jedes Mal von vorne anzufangen, wenn Sie ein bestimmtes benutzerdefiniertes Dashboard neu erstellen möchten, können Sie die Dashboards exportieren, die zurzeit nicht verwendet werden. Wenn Sie ein zuvor exportiertes Dashboard verwenden möchten, können Sie es in NetWitness Platform importieren.

### Importieren eines Dashboard

1. Klicken Sie in der Dashboardsymbolleiste auf (Dashboard importieren).
   Das Dialogfeld „Dashboard importieren“ wird angezeigt.




2. Navigieren Sie im Dialogfeld **Dashboard importieren** zur Dashboard-Datei. Sie können CFG- und ZIP-Dateien importieren.
3. Klicken Sie auf **Importieren**.
   Das Dashboard wird in NetWitness Platform angezeigt

**Hinweis:** Wenn Sie ein Dashboard aus Security Analytics 10.6.x in NetWitness Platform11.x importieren, müssen das Dashboard und die zugehörigen Regeln und Diagramme separat importiert werden. Wenn Sie jedoch ein Dashboard von NetWitness Platform11.x in NetWitness Platform importieren, werden das Dashboard und alle mit ihm verbundenen Regeln und Diagramme im ZIP-Format importiert.

### Exportieren eines Dashboard

**Hinweis:** Wenn Sie das Dashboard „Reporter-Echtzeitdiagramm“ exportieren, werden auch die zugehörigen Reporting Engine-Inhalte exportiert.

Exportierte Dashboards sind so konzipiert, dass sie in derselben NetWitness Platform-Instanz funktionieren. Es ist auch möglich, Ihre benutzerdefinierten Dashboards für andere Nutzer in Ihrem Unternehmen freizugeben, vorausgesetzt, dass sie über gleichwertige Berechtigungen verfügen.

Zum Exportieren eines Dashboards muss es geöffnet sein, damit Sie im Drop-down-Menü Bearbeiten auf das Dialogfeld Dashboard exportieren zugreifen können.

1. Navigieren Sie zu dem Dashboard, das Sie exportieren möchten. Sämtliche vorhandene Dashboards werden im Drop-down-Menü **Dashboard-Auswahlliste** im zurzeit angezeigten Dashboard angezeigt.
2. Klicken Sie in der Dashboardsymbolleiste auf  (Dashboard exportieren).
   Die exportierte Datei wird im ZIP-Format gespeichert.

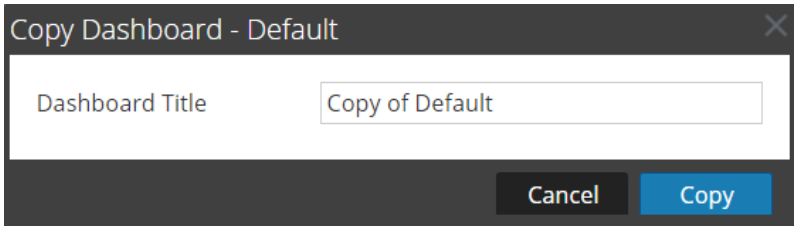
**Hinweis:** Die Exportfunktion gilt nicht für vorkonfigurierte Dashboards.

## Kopieren eines Dashboards

Zum Anpassen der Ansichten in NetWitness Platform können Sie Dashboards in das NetWitness-Dashboard oder ein benutzerdefiniertes Dashboard kopieren. Das NetWitness Platform-Dashboard stellt, wie der Name schon vermuten lässt, alle NetWitness Platform-Dashlets bereit. Das Dialogfeld „Dashboard kopieren“ erstellt ein Duplikat des Dashboards, das angepasst werden kann. Wenn Sie ein Dashboard kopieren, wird dem Standardnamen `Copy of` vorangestellt. Wenn der Name des Originaldashboards zum Beispiel `XYZ` ist, lautet der Standardname des kopierten Dashboards `Copy of XYZ`.

So kopieren Sie ein Dashboard:

1. Navigieren Sie zu einem beliebigen Dashboard.
2. Klicken Sie in der Dashboardsymbolleiste auf .
   Das Dialogfeld „Dashboard kopieren“ wird angezeigt. Der folgende Screenshot ist ein Beispiel für das Kopieren eines Dashboards.




3. Geben Sie den Dashboard-Titel ein.
4. Klicken Sie auf **Copy**.

## Freigeben eines Dashboards

In NetWitness Platform können Sie als Administrator Dashboards für andere Rollen wie Administrator, Analyst, Operator usw. freigeben. Wenn Sie ein Dashlet freigeben, können die Nutzer das Dashboard nur anzeigen, als Favoriten festlegen, kopieren und exportieren. Im Falle von anderen Rollen wie Analyst, Operator usw. können Sie das Dashboard nur für ähnliche Rollen freigeben. Beispielsweise kann ein Analyst ein Dashboard nur für andere Analysten freigeben.

1. Navigieren Sie zu einem beliebigen Dashboard.
2. Klicken Sie in der Dashboardsymbolleiste auf 

und wählen Sie das Kontrollkästchen für die Rolle aus, für die Sie das Dashboard freigeben möchten.

**Hinweis:** Deaktivieren Sie das Kontrollkästchen der Rolle, wenn Sie das Dashboard nicht freigeben möchten.

# Managen von Jobs

Zwangsläufig gibt es in RSA NetWitness® Platform Aufgaben (bedarfsorientiert oder geplant), die einige Minuten dauern. Das NetWitness Platform-Jobsystem erlaubt Ihnen, eine Aufgabe mit langer Laufzeit zu beginnen und fortzufahren, andere Teile von NetWitness Platform zu verwenden, während der Job ausgeführt wird. Sie können nicht nur den Fortschritt der Aufgabe überwachen, sondern auch Benachrichtigungen zum Abschluss der Aufgabe und deren Erfolg bzw. Misserfolg empfangen.

Während Sie in NetWitness Platform arbeiten, können Sie über die Symbolleiste eine kurze Übersicht Ihrer Jobs öffnen. Sie können sich diese jederzeit ansehen. Wenn ein Jobstatus geändert wurde, wird das Symbol Jobs ( ) mit der Anzahl der gerade ausgeführten Jobs markiert. Sobald alle Jobs abgeschlossen sind, verschwindet diese Zahl.

Sie können die Jobs auch in diesen beiden Ansichten anzeigen:

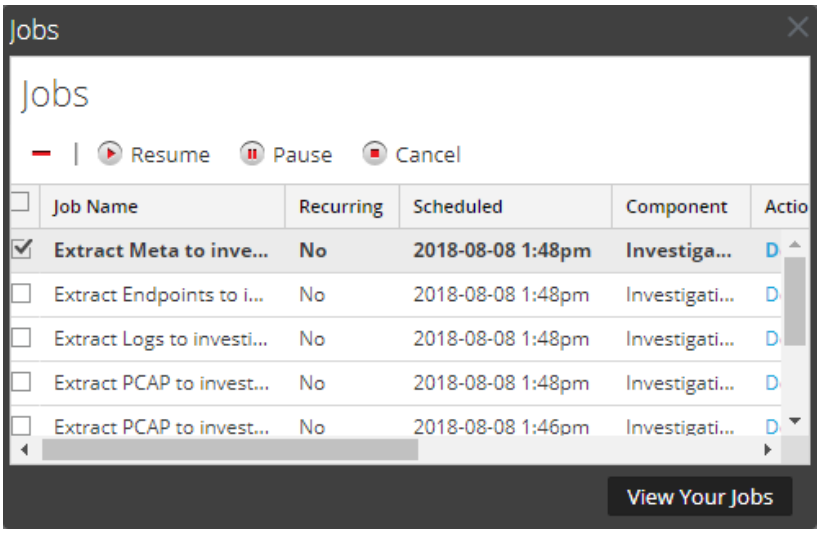
- Im Bereich „Jobs“ des Nutzerprofils finden Sie dieselben Jobs in einem eigenen Bereich. Dies sind nur Ihre Jobs.
- In der Ansicht System können Nutzer mit Administratorrechten alle Jobs für alle Nutzer in einem einzigen Jobfenster anzeigen und managen.

Der Aufbau des Jobfensters ist in allen Ansichten identisch.

## Anzeigen der Jobkurzübersicht

Klicken Sie in der NetWitness Platform-Symbolleiste auf das Symbol „Jobs“ ( ).

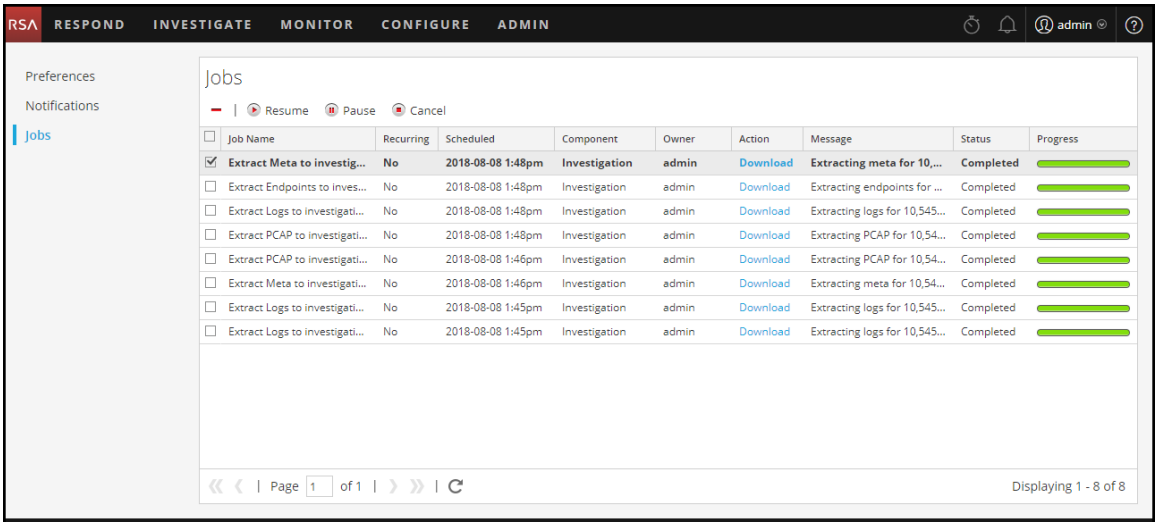
Die Jobkurzübersicht wird angezeigt.




In der Jobkurzübersicht werden alle wiederkehrenden und nicht wiederkehrenden Jobs angezeigt, deren Eigentümer Sie sind. Dabei steht nur eine Teilmenge der Spalten zur Verfügung, die im Bereich „Jobs“ verfügbar sind. Ansonsten sind die Jobkurzübersicht und der Bereich „Jobs“ des Nutzerprofils gleich. In der Ansicht „Administration“ > „System“ enthält der Bereich „Jobs“ Informationen über alle NetWitness Platform-Jobs für alle Nutzer.

## Anzeigen aller Jobs

Um eine umfassende Ansicht Ihrer Jobs anzuzeigen, klicken Sie in der Jobkurzübersicht auf **Ihre Jobs anzeigen**.
Der Bereich „Jobs“ wird angezeigt.




## Anhalten und Fortsetzen der geplanten Ausführung eines wiederkehrenden Jobs

Die Optionen Anhalten und Fortsetzen gelten nur für wiederkehrende Jobs. Sie können einen wiederkehrenden Job, der ausgeführt wird, anhalten. Allerdings hat dies keine Auswirkungen auf diese Ausführung. Die nächste Ausführung des Jobs (vorausgesetzt der Job ist noch angehalten) wird übersprungen.

1. Um die nächste Ausführung eines wiederkehrenden Jobs zu stoppen, wählen Sie den Job in einem beliebigen **Jobs**-Fenster aus und klicken Sie auf **Pause**.
   Die nächste Ausführung des Jobs wird übersprungen und die Planung wird angehalten, bis Sie auf Fortsetzen klicken.
2. Um die Ausführung pausierter wiederkehrender Jobs neu zu starten, wählen Sie den Job aus und klicken Sie auf **Fortsetzen**.
   Die nächste Ausführung des Jobs findet wie geplant statt und die Planung für den Job wird wieder aufgenommen.

## Abbrechen eines Jobs

Um Jobs zu beenden, die gerade ausgeführt werden oder sich in der Warteschlange befinden, gehen Sie wie folgt vor:

1. Wählen Sie in der **Jobkurzübersicht** oder im Bereich **Jobs** einen oder mehrere Jobs aus.
2. Klicken Sie auf **Abbrechen**.
   Ein Bestätigungsdialogfeld wird angezeigt.

3. Klicken Sie auf **Ja**.
   Die Jobs werden abgebrochen und die Einträge verbleiben mit dem Status **Abgebrochen** in der Liste.

   Wenn Sie einen wiederkehrenden Job abbrechen, wird die aktuelle Ausführung des Jobs abgebrochen. Beim der nächsten geplanten Ausführung des Jobs wird dieser normal ausgeführt.

## Löschen eines Jobs

**Achtung:** Wenn Sie einen Job löschen, wird er umgehend aus der Liste gelöscht. Es wird kein Bestätigungsdialogfeld angezeigt. Wenn Sie einen wiederkehrenden Job löschen, werden alle künftigen Ausführungen ebenfalls gelöscht.

Nutzer können ihre eigenen Jobs vor, während oder nach der Ausführung löschen. Administratoren können jeden Job löschen. So löschen Sie Jobs:

1. Wählen Sie einen oder mehrere Jobs aus.

2. Klicken Sie auf  .
   Die Jobs werden aus der Liste gelöscht.

## Herunterladen eines Jobs

Wenn ein Job den Status Download in der Spalte Aktion aufweist, können Sie das Ergebnis des Jobs herunterladen. Wenn Sie in der Ansicht „Untersuchen“ arbeiten und die Paketdaten für eine Sitzung als PCAP-Datei entpacken oder die Nutzdatendateien (z. B Word-Dokumente und Bilder) einer Sitzung extrahieren, wird eine Datei erstellt. Klicken Sie auf **Herunterladen**, um die Datei auf das lokale System herunterzuladen.

# Anzeigen und Löschen von Benachrichtigungen

Während Sie in RSA NetWitness® Platform arbeiten, können Sie aktuelle Systembenachrichtigungen einsehen, ohne den Bereich zu verlassen, in dem Sie gerade arbeiten. Sie können eine kurze Übersicht der Benachrichtigungen in der NetWitness Platform-Symbolleiste öffnen. Sie können diese jederzeit einsehen. Bei Empfang einer neuen Benachrichtigung wird das Benachrichtigungssymbol entsprechend markiert ( ).

Beispiele für Benachrichtigungen sind:

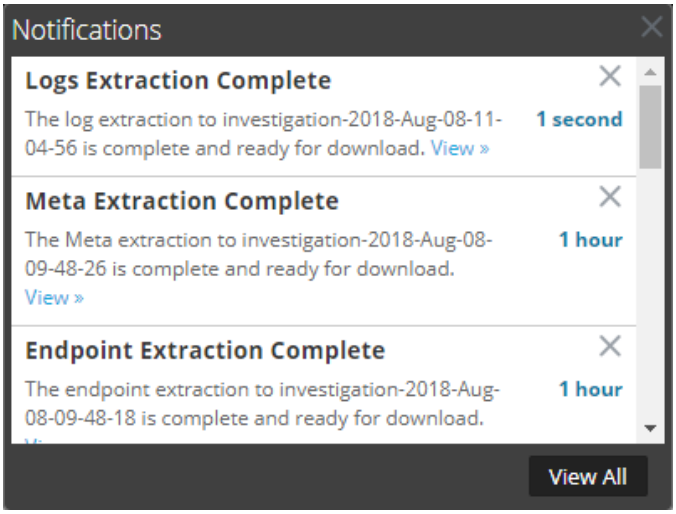
- Ein Upgrade eines Hosts wurde abgeschlossen.
- Ein Parser-Push zu den Decoders wurde abgeschlossen.
- Es ist eine neuere Softwareversion verfügbar.

In diesen beiden Ansichten werden Benachrichtigungen angezeigt:

- Im Benachrichtigungsbereich sehen Sie die aktuellen Benachrichtigungen.
- Im Bereich „Profilbenachrichtigungen“ werden alle Benachrichtigungen für den Nutzer angezeigt.

## Anzeigen aktueller Benachrichtigungen

Klicken Sie auf das Symbol „Benachrichtigungen“ ( ), um aktuelle Benachrichtigungen aufzurufen. Die Taskleiste Benachrichtigungen wird angezeigt.

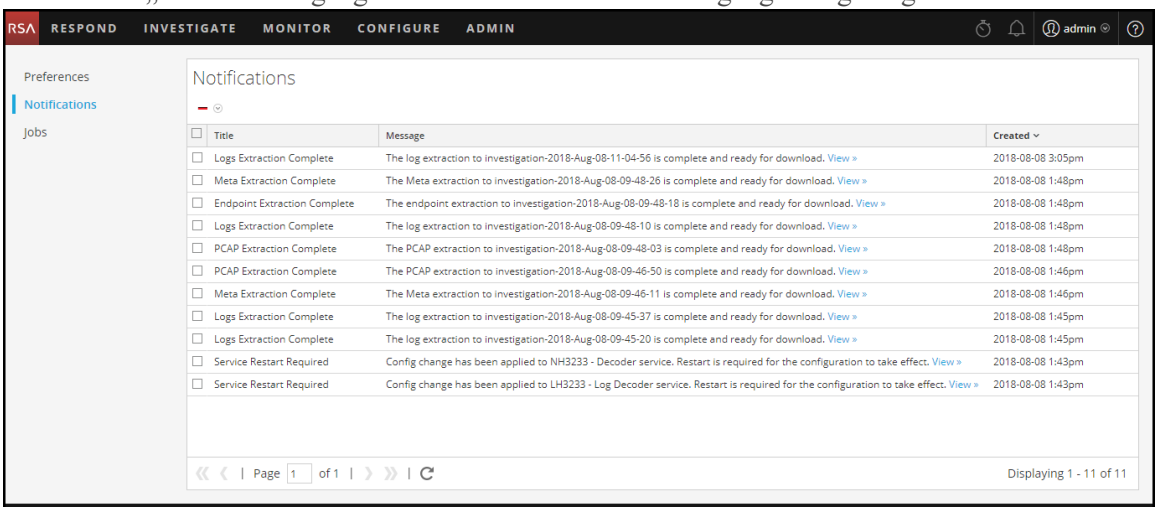


## Anzeigen aller Benachrichtigungen

Gehen Sie wie folgt vor, um alle Benachrichtigungen anzuzeigen:

- Klicken Sie auf , um den Benachrichtigungsbereich zu öffnen, und klicken Sie dann auf **Alle anzeigen**.
- Wählen Sie in der oberen rechten Ecke des NetWitness Platform-Browserfensters > **Profil** aus und wählen Sie dann im Bereich „Optionen“ des Dialogfelds „Einstellungen“ die Option **Benachrichtigungen** aus.

Im Bereich „Benachrichtigungen“ werden alle Benachrichtigungen angezeigt.




## Löschen von Benachrichtigungsdatensätzen

So löschen Sie Benachrichtigungsdatensätze:

1. Wählen Sie in der Liste **Profilbenachrichtigungen** die Benachrichtigungen aus, die Sie löschen möchten.
2. Klicken Sie auf .

   Die ausgewählten Benachrichtigungen werden aus der Liste und aus dem Benachrichtigungsbereich gelöscht.

# Anzeigen der Hilfe in der Anwendung

Sie haben verschiedene Möglichkeiten, für die Verwendung von RSA NetWitness® Platform Hilfestellung zu erhalten. Dafür stehen Ihnen die Inlinehilfe, Kurzinformationen und Onlinehilfelinks zur Verfügung.

## Anzeigen der Inlinehilfe

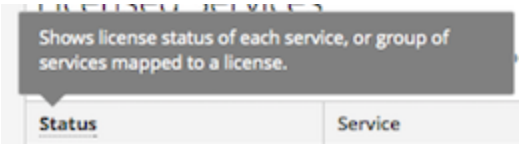
Die Inlinehilfe bietet zusätzliche Informationen darüber, was in Abschnitten oder Feldern zu tun ist, die derzeit in der NetWitness Platform-Benutzeroberfläche angezeigt werden. Bewegen Sie den Mauszeiger zum Anzeigen der Inlinehilfe auf . In der Inlinehilfe wird eine kurze Beschreibung des Elements angezeigt.

Beispiel für Inlinehilfe:


## Anzeigen von Kurzinformationen

Kurzinformationen bieten eine schnelle Möglichkeit, eine Beschreibung des Texts oder zusätzliche Informationen über eine Aktion, ein Feld oder einen Parameter anzuzeigen. Kurzinformationen werden als unterstrichener Text angezeigt. Bewegen Sie die Maus zur Anzeige der Kurzinformation und einer kurzen Beschreibung des Ausdrucks über den unterstrichenen Text.

Beispiel für eine Kurzinformation:

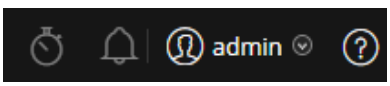



## Anzeigen der Onlinehilfe

Onlinehilfelinks führen Sie aus NetWitness Platform heraus zur RSA Link-Onlinedokumentation. Diese Website bietet eine vollständige Dokumentation für NetWitness Platform und die Links führen Sie direkt zu dem Thema, in dem der aktuell angezeigte Teil der Benutzeroberfläche beschrieben wird.

Klicken Sie zur Anzeige des Onlinehilfethemas für den aktuellen Bereich der Benutzeroberfläche auf in der NetWitness Platform-Symbolleiste oder in einem Dialogfeld. Das entsprechende Hilfethema wird in einem anderen Browserfenster angezeigt. Das Thema beschreibt die Funktionen der aktuellen Ansicht oder des Dialogfelds. Von diesem Thema aus können Sie schnell zu den zugehörigen Verfahren navigieren.

In der folgenden Abbildung ist ein Beispiel für das Onlinehilfesymbol in der NetWitness Platform-Symbolleiste gezeigt.



# Suchen nach Dokumenten auf RSA Link

Die RSA NetWitness® Platform-Dokumentation befindet sich auf RSA Link, dem RSA-Supportportal bzw. der Supportcommunity. RSA Link vereint alle Ihre RSA-Ressourcen an einem zentralen Ort. Es umfasst Ratgeber, Produktdokumentationen, Wissensdatenbankartikel, Downloads und Schulungen. Eine *geführte Tour durch RSA Link* finden Sie unter https://community.rsa.com/videos/21554.

## Suchen nach der NetWitness Platform-Dokumentation

Die Dokumentation zu NetWitness Platform Logs and Networks finden Sie unter folgendem Link: https://community.rsa.com/docs/DOC-40370

### So navigieren Sie zur Dokumentation von NetWitness Platform Logs and Networks:

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS PLATFORM**.
2. Klicken Sie auf der Seite zu RSA NetWitness Platform auf **DOCUMENTATION** und wählen Sie **RSA NETWITNESS LOGS AND NETWORK** aus.

### So navigieren Sie zur Dokumentation für NetWitness Endpoint 4.x:

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS PLATFORM**.
2. Klicken Sie auf der Seite zu RSA NetWitness Platform auf **DOCUMENTATION** und wählen Sie **RSA NETWITNESS ENDPOINT** aus.

## Suchen nach RSA-Inhalt

RSA-Inhalt finden Sie unter folgendem Link: https://community.rsa.com/community/products/netwitness/rsa-content

### So navigieren Sie zum RSA-Inhalt:

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS PLATFORM**.
2. Klicken Sie auf der Seite zu RSA NetWitness Platform auf **DOCUMENTATION** und wählen Sie **ADDITIONAL RESOURCES** > **RSA LIVE CONTENT** aus.

## Suchen nach von RSA unterstützten Ereignisquellen

Von RSA unterstützte Ereignisquellen finden Sie unter folgendem Link: https://community.rsa.com/community/products/netwitness/parser-network/event-sources

**So navigieren Sie zu von RSA unterstützten Ereignisquellen:**

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS PLATFORM**.
2. Klicken Sie auf der Seite zu RSA NetWitness Platform auf **DOCUMENTATION** und wählen Sie **ADDITIONAL RESOURCES** > **EVENT SOURCE CONFIGURATION** aus.

## Suchen nach Handbüchern zur Hardwarekonfiguration

Die Handbücher zur Hardwarekonfiguration finden Sie unter folgendem Link:
https://community.rsa.com/community/products/netwitness/hardware-setup-guides

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS PLATFORM**.
2. Klicken Sie auf der Seite zu RSA NetWitness Platform auf **DOCUMENTATION** und wählen Sie **ADDITIONAL RESOURCES** > **HARDWARE SETUP GUIDES** aus.

## Suchen nach Dokumenten mit dem NetWitness-Navigator

Sie können mit dem Tool NetWitness-Navigator nach der gewünschten RSA NetWitness Platform-Dokumentation in RSA Link suchen.

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS PLATFORM**.
2. Klicken Sie unter PRODUKTRESSOURCEN (rechts auf der Seite) auf **RSA NetWitness Navigator**.
3. Wählen Sie die gewünschten Suchkriterien aus den verfügbaren Optionen aus. Bei der Suche nach Dokumentation sollten Sie **Benutzerdokumentation** als Contenttyp auswählen. Darüber hinaus wird die Option „Kosten“ für die Benutzerdokumentation ignoriert.
4. Klicken Sie zum Anzeigen einer Liste der übereinstimmenden Dokumente auf **ERGEBNISSE ANZEIGEN**.
5. Klicken Sie zum Löschen Ihrer vorherigen Suchoptionen auf **OPTIONEN ZURÜCKSETZEN**.

## Nachverfolgen von Content für Updates

Sie können Seiten oder Dokumente nachverfolgen, um über Änderungen informiert zu werden.

1. Melden Sie sich bei RSA Link an.
2. Navigieren Sie zu einer Seite oder einem Dokument und wählen Sie in der oberen rechten Ecke entweder **Folgen** oder **Aktionen** > **Folgen** aus.

## Senden Ihres Feedbacks an RSA

Ihr Feedback ist uns sehr wichtig und hilft uns dabei, für unsere Kunden eine bessere Erfahrung zu bieten. Bitte senden Sie Ihre Vorschläge an sahelpfeedback@rsa.com.

# Referenzen für die ersten Schritte in NetWitness Platform

Der folgende Abschnitt enthält die Referenzinformationen zur Benutzerschnittstelle in Bezug auf Erste Schritte mit der NetWitness Platform-Anwendung.

# Nutzereinstellungen

Um RSA NetWitness® Platform an Ihre Umgebung und Arbeitsabläufe anzupassen, können Sie eigene globale Anwendungseinstellungen festlegen. Sie können Folgendes tun:

- Ändern der Sprache der Anwendung
- Festlegen der Zeitzone der Anwendung
- Festlegen des Datums- und Uhrzeitformats
- Auswählen der standardmäßigen Startansicht für NetWitness Platform*
- Auswählen der standardmäßigen Ansicht „Untersuchen“
- Auswählen eines dunklen oder hellen Designs für die Anwendung
- Ändern des Passworts
- Benachrichtigungen aktivieren
- Aktivieren von Kontextmenüs
- Ändern von Investigate-Einstellungen – wird im *NetWitness Investigate – Benutzerhandbuch* beschrieben.

Ihre globalen Einstellungsoptionen variieren abhängig davon, ob Sie darauf aus der Ansicht „Reagieren“ oder aus anderen Ansichten, z. B. „Untersuchen“, „Überwachung“, „Konfigurieren“ und „Admin“ zugreifen. Es gibt zwei Dialogfelder für globale Nutzereinstellungen, die über die Hauptmenüleiste aufgerufen werden können:

- Dialogfeld **Nutzereinstellungen**: Aufrufbar über „Reagieren“ und folgende „Untersuchen“-Ansichten: Ereignisanalyse, Hosts, Dateien und Nutzer.
- Dialogfeld **Einstellungen**: Über die meisten anderen Ansichten aufrufbar.

## Was möchten Sie tun?

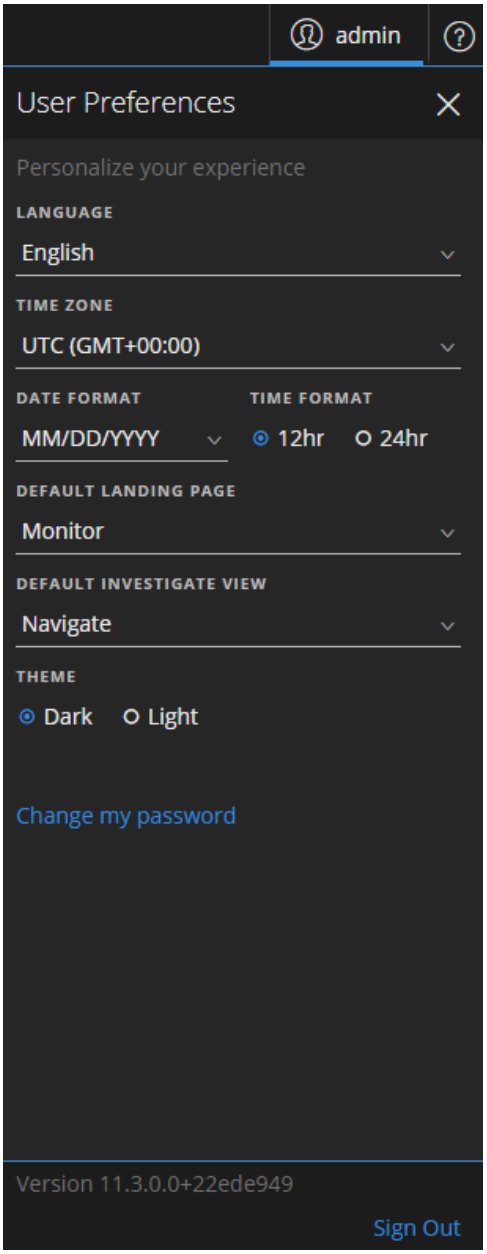
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Alle | eigenes Passwort ändern | Eigenes Passwort ändern |
| Alle | Meine standardmäßige Landingpage auswählen | Einrichten einer Standardansicht nach SOC-Rolle |
| Alle | Meine Nutzereinstellungen festlegen | Festlegen von Nutzereinstellungen |

## Verwandte Themen

- Navigation in NetWitness Platform

## Nutzereinstellungen (Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten)

Um auf Ihre Einstellungen zuzugreifen, klicken Sie auf .
Im Dialogfeld „Nutzereinstellungen“ werden die aktuellen Einstellungen und die NetWitness Platform-Version angezeigt.




In der folgenden Tabelle sind die Optionen für globale Anwendungseinstellungen beschrieben, auf die Sie über das Dialogfeld „Nutzereinstellungen“ zugreifen können.

| Option | Beschreibung |
|---|---|
| Sprache | (Diese Option ist ab NetWitness Platform 11.2 verfügbar.)<br>Legt die bevorzugte Sprache für NetWitness Platform fest. Die Standardsprache ist Englisch (USA). |

| Option | Beschreibung |
|---|---|
| Zeitzone | Legt die Zeitzone für die Verwendung in NetWitness Platform fest. |
| Datumsformat | Legt das Format für die Reihenfolge der Anzeige von Monat (MM), (TT) Tag und Jahr (JJJJ) fest. Das Format MM/TT/JJJJ zeigt beispielsweise das Datum als 05/11/2017 an. |
| Zeitformat | Legt die Uhrzeit als 12- oder 24-Stunden-Uhrzeit fest. 2:00 Uhr im 12-Stunden-Zeitformat ist z. B. 14:00 Uhr im 24-Stunden-Zeitformat. |
| Standardmäßige Landingpage | Ermöglicht bei der Anmeldung bei NetWitness Platform die Auswahl einer Standardansicht. Sie können entsprechend Ihrer Nutzerrolle „Reagieren“, „Investigate“, „Überwachen“, „Konfigurieren“ und „Admin“ auswählen. Beispielsweise können Sie „Reagieren“ auswählen, um direkt zum entsprechenden Abschnitt der Anwendung für Incident-Experten zu wechseln.<br>Diese Auswahl legt die Standardansicht für die gesamte Anwendung fest. |
| Standardmäßige Ansicht „Untersuchen“ | (Diese Option gilt für NetWitness Platform 11.1 oder höher.) Wählen Sie die standardmäßige Landingpage für die Ansicht „Untersuchen“ aus. Sie können die Ansicht „Navigieren“, „Ereignisse“, „Ereignisanalyse“, „Hosts“, „Dateien“, „Nutzer“ oder „Malware Analysis“ als standardmäßige „Untersuchen“-Ansicht auswählen. Beispielsweise können Sie „Ereignisse“ als standardmäßige Ansicht „Untersuchen“ wählen, um direkt zu „Ereignisse“ zu gehen und die für einen Service generierten Ereignisse anzuzeigen. |
| Design | (Diese Option gilt für NetWitness Platform 11.1 und höher.)<br>Ändert die Darstellung der Ansicht „Reagieren“ und einige Untersuchen-Ansichten, die in der Anwendung angezeigt werden. Sie können helle oder dunkle Designs auswählen.<br>• **Dunkel**: Das dunkle Design ist am besten für dunklere Umgebungen geeignet oder wenn Sie nicht so viel Kontrast benötigen.<br>• **Hell**: Das helle Design ist am besten für hellere Umgebungen geeignet, wenn Sie mehr Kontrast benötigen oder wenn Sie die Anwendung projizieren, damit andere sie sehen können. Da einige Ansichten von den Designänderungen nicht betroffen sind, wird empfohlen, für eine einheitliche Anzeige das hellere Design auszuwählen.<br>Ihre Auswahl wirkt sich nur darauf aus, wie NetWitness Platform für Sie dargestellt wird, nicht auf die Darstellung für andere Nutzer. |
| Eigenes Passwort ändern | Öffnet das Dialogfeld „Einstellungen“, in dem Sie Ihr Passwort ändern können. |
| Version | Zeigt die NetWitness Platform-Version an. |
| Abmelden | Ermöglicht es Ihnen, sich von NetWitness Platform abzumelden. |

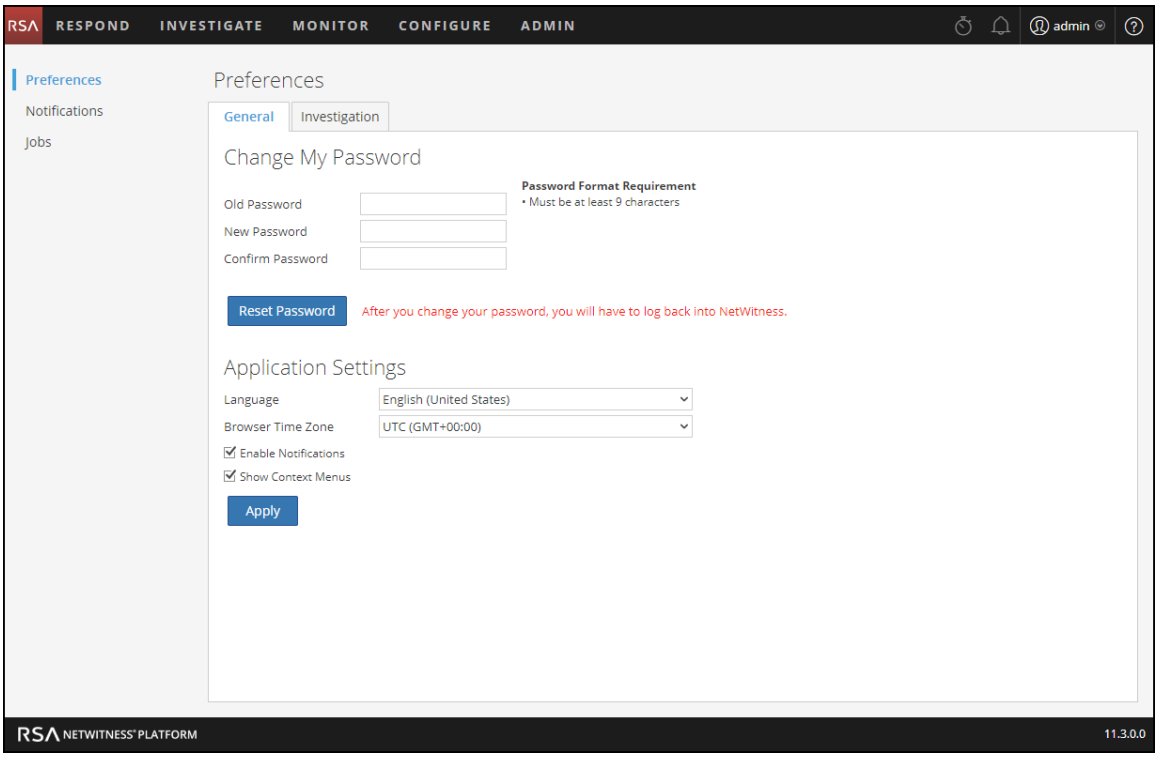
Die von Ihnen vorgenommenen Einstellungen werden sofort wirksam.

## Einstellungen

Um auf weitere globale Nutzereinstellungen zuzugreifen, führen Sie einen der folgenden Schritte aus:

- In den meisten Ansichten, z. B. „Untersuchen“, „Überwachung“, „Konfigurieren“ und „Admin“, navigieren Sie zu > **Profil**.
- Wählen Sie in der Ansicht „Reagieren“ und einigen „Untersuchen“-Ansichten (Ereignisanalyse, Hosts, Dateien und Nutzer) aus und klicken Sie im Dialogfeld „Nutzereinstellungen“ auf **Eigenes Passwort ändern**.

Im Dialogfeld „Einstellungen“ werden die aktuellen Einstellungen angezeigt.




In der folgenden Tabelle sind die Optionen für globale Anwendungseinstellungen beschrieben, auf die Sie über das Dialogfeld „Einstellungen“ zugreifen können.

## Eigenes Passwort ändern

In diesem Abschnitt können Sie Ihr Passwort ändern. Ihr Administrator definiert die entsprechenden Anforderungen an die Passwortstärke für Ihr NetWitness Platform-Passwort, wie z. B. minimale Passwortlänge und minimale Anzahl von Großbuchstaben, Kleinbuchstaben, Dezimalstellen, nicht-lateinischen Buchstaben und Sonderzeichen. Diese Anforderungen werden angezeigt, wenn Sie Ihr Passwort ändern.

In den folgenden Tabellen sind die Optionen im Abschnitt „Eigenes Passwort ändern“ beschrieben.

| Option | Beschreibung |
|---|---|
| Altes Passwort | Geben Sie das Passwort ein, das Sie zur Anmeldung bei NetWitness Platform verwenden. |

| Option | Beschreibung |
|---|---|
| Neues Passwort | Geben Sie das Passwort ein, das Sie für die nächste Anmeldung verwenden möchten. |
| Passwort bestätigen | Geben Sie das neue Passwort erneut ein. |
| Passwort zurücksetzen | Aktualisiert Ihr Nutzerprofil mit dem neuen Passwort. Sie werden von NetWitness Platform abgemeldet, damit die Änderungen wirksam werden. Das neue Passwort wird bei der nächsten Anmeldung bei NetWitness Platform wirksam. Die Passwortänderung wird für Ihre Systemanmeldung und für alle NetWitness Platform-Services angewendet, zu denen Ihr Konto hinzugefügt wurde. |

Wenn Sie Ihr Passwort geändert haben, werden Sie von NetWitness Platform abgemeldet, damit die Änderungen wirksam werden. Das neue Passwort wird bei der nächsten Anmeldung bei NetWitness Platform wirksam.

### Anwendungseinstellungen

In der folgenden Tabelle sind die Optionen im Abschnitt „Anwendungseinstellungen“ beschrieben.

| Option | Beschreibung |
|---|---|
| Sprache | (Diese Option ist ab NetWitness Platform 11.2 verfügbar.)<br>Legt die bevorzugte Sprache für NetWitness Platform fest. Die Standardsprache ist Englisch (USA). |
| Browserzeitzone | Legt die Zeitzone für die Verwendung in NetWitness Platform fest. Ihre Zeitzoneneinstellung wird auf der Symbolleiste angezeigt. |
| Benachrichtigungen aktivieren | Mit diesem Kontrollkästchen werden Benachrichtigungen für Ihr Nutzerkonto aktiviert und deaktiviert. Die NetWitness Platform-Systembenachrichtigungen werden bei der Erstellung eines neuen Benutzerkontos standardmäßig aktiviert. |
| Aktivieren von Kontextmenüs | Mit diesem Kontrollkästchen werden Kontextmenüs für Ihr Nutzerkonto aktiviert und deaktiviert. Bei der Erstellung eines neuen Benutzerkontos werden die Kontextmenüs standardmäßig aktiviert. Durch Klicken mit der rechten Maustaste in einer Ansicht werden Kontextmenüs mit weiteren Funktionen für bestimmte Ansichten geöffnet. |
| Anwenden | Aktualisiert die Einstellungen und wendet die Änderungen sofort an. |

# Bereich „Benachrichtigungen“ und Benachrichtigungsbereich

RSA NetWitness® Platform stellt Systembenachrichtigungen bereit, um Nutzer über bestimmte Aktionen oder Bedingungen zu informieren.

- Ein Upgrade eines Hosts wurde abgeschlossen.
- Ein Parser-Push zu den Decodern wurde abgeschlossen.
- Ein Service ist ausgefallen (kritisches Protokoll eines bestimmten Typs).
- Eine Visualisierung wurde abgeschlossen.
- Ein Bericht wurde abgeschlossen.
- Es ist eine neuere Softwareversion verfügbar.

Während Sie in NetWitness Platform arbeiten, können Sie aktuelle Systembenachrichtigungen einsehen, ohne den Bereich zu verlassen, in dem Sie gerade arbeiten. Sie können eine kurze Übersicht der Benachrichtigungen in der NetWitness Platform-Symbolleiste öffnen. Sie können diese jederzeit einsehen. Bei Empfang einer neuen Benachrichtigung wird das Benachrichtigungssymbol entsprechend markiert (  ).

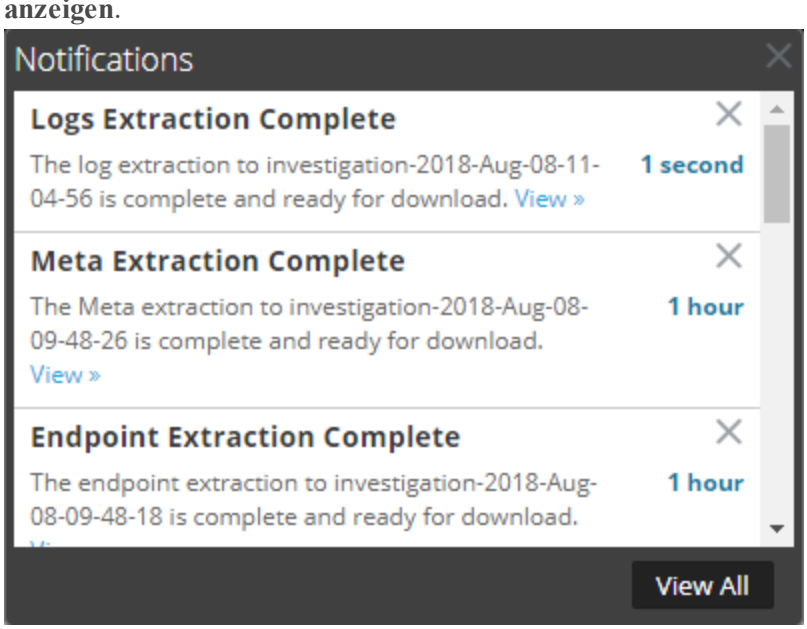
Wenn Sie Benachrichtigungen im Benachrichtigungsbereich anzeigen, werden nur aktuelle Benachrichtigungen angezeigt. Sie können über Ihr Nutzerprofil und den Benachrichtigungsbereich auf alle Ihre Benachrichtigungen zugreifen, indem Sie die Option „Alle anzeigen“ auswählen. Anleitungen für die Anzeige von Benachrichtigungen finden Sie unter Anzeigen und Löschen von Benachrichtigungen.

## Was möchten Sie tun?

| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Alle | alle Benachrichtigungen anzeigen | Anzeigen und Löschen von Benachrichtigungen |
| Alle | Benachrichtigung löschen | Anzeigen und Löschen von Benachrichtigungen |

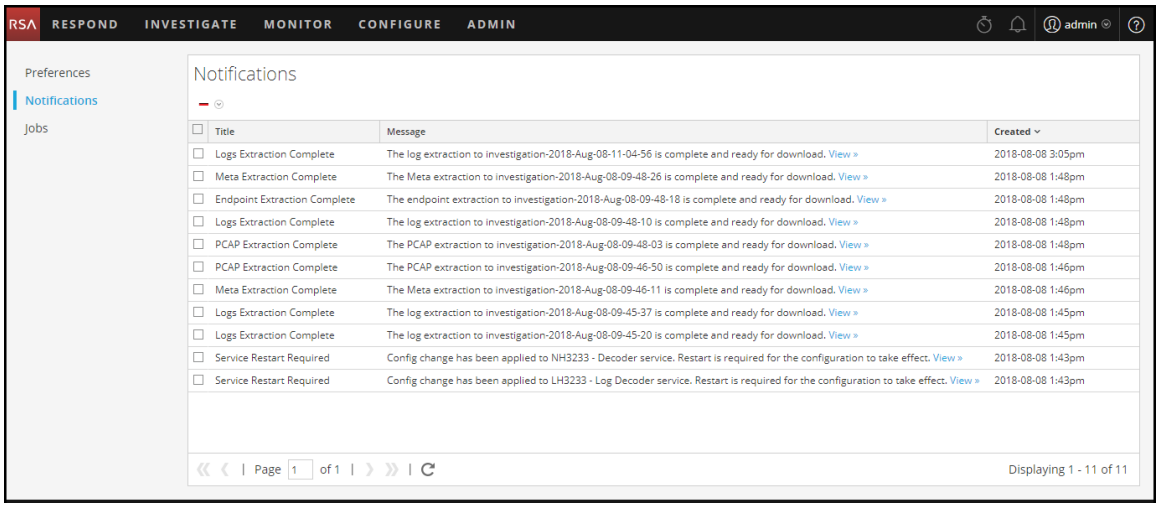
Führen Sie zum Öffnen des Bereichs „Benachrichtigungen“ eine der folgenden Aktionen aus:

- Klicken Sie auf , um den Benachrichtigungsbereich zu öffnen, und klicken Sie dann auf **Alle anzeigen**.




- Wählen Sie in der oberen rechten Ecke des NetWitness Platform-Browserfensters > **Profil** aus und wählen Sie dann im Bereich „Optionen“ des Dialogfelds „Einstellungen“ die Option **Benachrichtigungen** aus.

  Der Bereich „Benachrichtigungen“ wird angezeigt.




Im Benachrichtigungsbereich sehen Sie die aktuellen Benachrichtigungen. Er enthält einen Teil der Informationen aus dem Bereich „Benachrichtigungen“. Im Bereich „Benachrichtigungen“ werden alle Benachrichtigungen angezeigt. In der folgenden Tabelle werden die Funktionen des Bereichs „Benachrichtigungen“ und des Benachrichtigungsbereichs beschrieben.

| Funktion | Beschreibung |
|---|---|
|  | (nur Bereich „Benachrichtigungen“) Zeigt ein Drop-down-Menü an, in dem Sie die ausgewählte Benachrichtig oder sämtliche Benachrichtigungen im Bereich „Benachrichtigungen“ und im Benachrichtigungsbereich löschen können. |
| Titel | Der Titel der Benachrichtigung, z. B. **Protokollextraktion abgeschlossen**. |
| Meldung | Die gesamte Meldung, z. B. **Die Protokollextraktion für die Untersuchung ist abgeschlossen und steht zum Herunterladen zur Verfügung.** |
| Anzeigen | Einige Meldungen enthalten einen Link, der eine **Ansicht** öffnet, in der Sie Maßnahmen ergreifen können. Wenn beispielsweise eine Datei herunterzuladen ist, öffnet ein Klick auf diesen Link den Bereich „Jobs“, die Ansicht, in der Sie die Datei herunterladen können. |
| Erstellt | Datum und Uhrzeit der Erstellung der Benachrichtigung.<br>Im Benachrichtigungsbereich wird die Anzahl der Stunden oder Tage seit Erstellung der Benachrichtigung angezeigt. |
| Alle anzeigen | (nur Benachrichtigungsbereich) Öffnet den Bereich „Benachrichtigungen“, in dem alle Ihre Benachrichtigungen aufgelistet sind. |

# Bereich „Jobs“ und Jobkurzübersicht

Jobs werden von verschiedenen RSA NetWitness® Platform-Komponenten gestartet, beispielsweise durch das herunterladen von CMS-Ressourcen (Content Management System) von Live-Services und das Extrahieren von Protokollen, Metadateien und PCAP-Dateien aus NetWitness Investigate.

In der Ansicht „Administration > System“ können Administratoren alle NetWitness Platform-Jobs im Bereich „Jobs“ managen. Andere Nicht-Administrator-Nutzer können ihre eigenen Jobs im Bereich „Jobs“ des Nutzerprofils anzeigen.

Während Sie in NetWitness Platform arbeiten, können Sie über die NetWitness Platform-Symbolleiste eine Schnellansicht Ihrer Jobs öffnen. Wenn ein Jobstatus geändert wird, wird das Symbol Jobs (  ) mit der Anzahl der gerade ausgeführten Jobs markiert. Sobald alle Jobs abgeschlossen sind, verschwindet diese Zahl.

Im Bereich Jobs können Sie:

- die Jobs anzeigen und sortieren
- einen Job anhalten oder fortsetzen
- Abbrechen eines Jobs
- einen Job löschen
- einen Job herunterladen

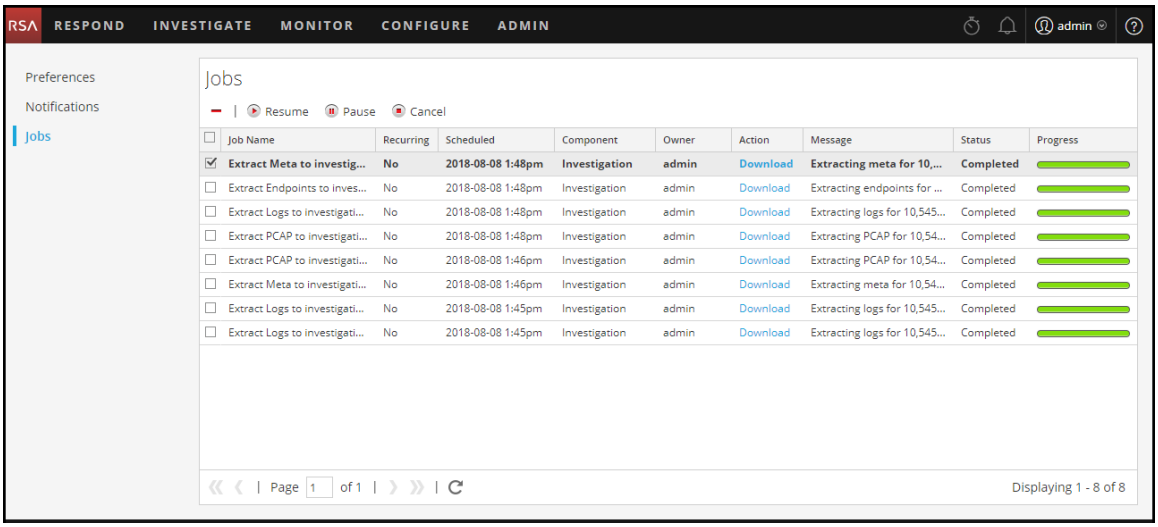
Der Aufbau des Jobfensters ist in allen Ansichten identisch.

## Was möchten Sie tun?

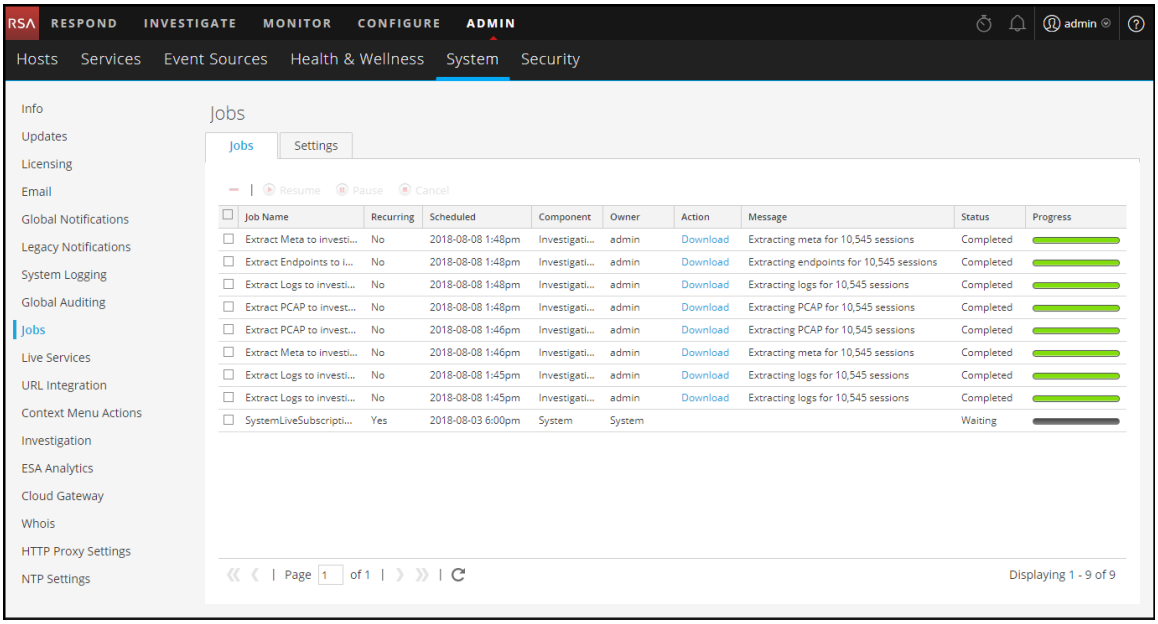
| Rolle | Ziel | Details anzeigen |
|---|---|---|
| Alle | einen geplanten Job anhalten und fortsetzen | Managen von Jobs |
| Alle | einen Job abbrechen oder löschen | Managen von Jobs |
| | einen Job herunterladen | Managen von Jobs |

Führen Sie zum Öffnen des Bereichs „Jobs“ eine der folgenden Aktionen aus:

- Wählen Sie in der oberen rechten Ecke des NetWitness Platform-Browserfensters  > **Profil** aus und wählen Sie dann im Bereich „Optionen“ des Dialogfelds „Einstellungen“ die Option **Jobs** aus. Der Bereich „Jobs“ wird angezeigt. Er zeigt die Jobs eines bestimmten Nutzers an.

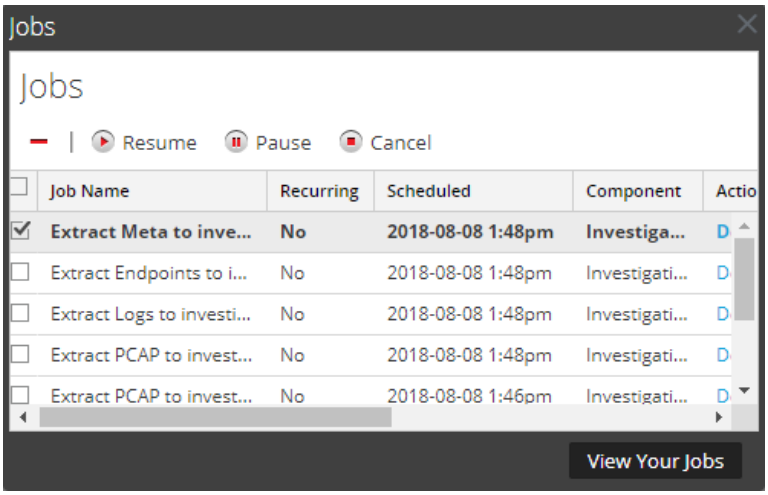



- Navigieren Sie zu **ADMIN > System** und wählen Sie im Bereich „Optionen“ die Option **Jobs** aus. Der Bereich „Jobs“ in der Ansicht „Administration > System“ wird angezeigt. Er zeigt die Jobs für alle Nutzer an.




Im Bereich „Jobs“ werden Informationen zu Jobs in einer Liste dargestellt. Die Spalten enthalten einen Fortschrittsbalken für den Job, den Jobnamen, eine Anzeige dazu, ob der Job wiederkehrend oder nicht wiederkehrend ist, die NetWitness Platform-Komponente, die den Job steuert, den Jobeigentümer, den Status, zugeordnete Nachrichten und eine Schaltfläche an, mit der Erfassungsdateien und Nutzlastdateien für die Jobpakete heruntergeladen werden können.

Um die Jobkurzübersicht anzuzeigen, klicken Sie auf das Symbol **Jobs** .




In der Jobkurzübersicht werden unter Verwendung einer Teilmenge der im Bereich **Jobs** verfügbaren Spalten alle Jobs aufgelistet, deren Eigentümer Sie sind. Ansonsten sind die Jobkurzübersicht und der Bereich „Jobs“ des Nutzerprofils gleich. In der Ansicht „Administration > System“ enthält der Bereich „Jobs“ Informationen über alle NetWitness Platform-Jobs für alle Nutzer.

In der folgenden Tabelle sind die im Bereich „Jobs“ verfügbaren Optionen beschrieben.

| Option | Beschreibung |
|---|---|
| Resume | Die Option Fortsetzen gilt nur für wiederkehrende Jobs, die angehalten wurden. Wenn Sie einen angehaltenen Job fortsetzen, wird die nächste Ausführung des Jobs wie geplant stattfinden. |
| Pause | Die Option Anhalten gilt nur für wiederkehrende Jobs. Wenn Sie einen wiederkehrenden Job, der ausgeführt wird, anhalten, hat dies keine Auswirkungen auf diese Ausführung. Die nächste Ausführung des Jobs (vorausgesetzt der Job ist noch angehalten) wird übersprungen. |
| Cancel | Bricht einen wiederkehrenden oder nicht wiederkehrenden Job ab. Sie können einen Job abbrechen, während er ausgeführt wird. Wenn Sie einen wiederkehrenden Job abbrechen, wird die aktuelle Ausführung des Jobs abgebrochen. Beim der nächsten geplanten Ausführung des Jobs wird dieser normal ausgeführt. |
| − | Löscht einen wiederkehrenden oder nicht wiederkehrenden Job aus dem Bereich Jobs. Wenn Sie einen Job löschen, wird der Job umgehend aus dem Bereich Jobs gelöscht. Es wird kein Bestätigungsdialogfeld angezeigt. Wenn Sie einen wiederkehrenden Job löschen, werden alle künftigen Ausführungen ebenfalls gelöscht. |

In dieser Tabelle sind die Spalten der Jobkurzübersicht und des Bereichs „Jobs“ beschrieben.

| Funktion | Beschreibung |
|---|---|
| Auswahlfeld | Ermöglicht die Auswahl von einem oder von mehreren Jobs. |
| Jobname | Zeigt den Namen des Jobs an, z. B. **Dateien extrahieren** oder **Upgrade für Service durchführen**. |
| Wiederkehrend | Gibt an, ob der Job wiederkehrend oder nicht wiederkehrend ist. **Ja** = wiederkehrend, **Nein** = nicht wiederkehrend. |
| Geplant | Gibt die geplante Startzeit und das Startdatum des Jobs an. |
| Komponente | Zeigt die Komponente an, aus der der Job stammt, z. B. **Investigation** oder **Administration**. |
| Eigentümer | Gibt den Besitzer des Jobs an. Der Besitzer des Jobs wird standardmäßig nicht in der **Jobkurzübersicht** angezeigt, da hier nur die Jobs des aktuellen Nutzers zu sehen sind. Die Spalte kann aber hinzugefügt werden. |
| Aktion | Zeigt den Job in einer anderen Ansicht an oder lädt Jobdateien für den Job in das standardmäßige Verzeichnis **Downloads** auf dem lokalen System herunter. Nur für erfolgreich abgeschlossene Jobs wird der Link **Anzeigen** in der Spalte **Aktion** angezeigt. Nur für Jobs, mit denen eine Datei erstellt wird, wird der Link **Download** in der Spalte **Aktion** angezeigt. |
| Meldung | Zeigt zusätzliche Informationen zum Job an, z. B. **Dateien werden extrahiert** oder **Keine Sitzungen gefunden**. |
| Status | Gibt den Status des Jobs an. Standardwerte sind **Unterbrochen**, **Wird ausgeführt**, **Abgebrochen**, **Fehlgeschlagen**, **Abgeschlossen**. Weitere Statuswerte können hinzugefügt werden. |
| Fortschritt | Zeigt an, wie viel Prozent des Jobs abgeschlossen sind. |
| Ihre Jobs anzeigen | (nur Jobkurzübersicht) Zeigt Ihre Jobs im Bereich **Jobs** an. |