RSA NETWITNESS® SUITE

Leitfaden für die ersten Schritte

für Version 11,1

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 Benutzer 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 sollten 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.

Juli 2018

Inhalt

Erste Schritte mit NetWitness Suite

Übersicht

RSA NetWitness-Suite ist eine leistungsstarke Suite zur Erkennung von Bedrohungen, mit der Security Operation Centers (SOCs) Bedrohungen schnell ermitteln, priorisieren und selektieren kann. NetWitness Suite 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 Suite ist leistungsfähiger als je zuvor, aber einfacher für Tier-1-Analysten zu verwenden, da es den Prozess der Identifizierung und Priorisierung von verdächtigen Bedrohungen automatisiert.NetWitness Suite Darüber hinaus können Tier-2- und Tier-3-Analysten Bedrohungen mithilfe neuer Analysetools und der Metadaten- und Rohdaten-Ansichten früherer Versionen von NetWitness-Suite ermitteln und aufspüren.

Architektur

RSA NetWitness Suite ist ein dezentralisiertes und modulares System, das äußerst flexible Bereitstellungsarchitekturen ermöglicht, die anhand der Anforderungen des Unternehmens skaliert werden können. Mit NetWitness Suite können Administratoren drei Arten von Daten aus der Netzwerkinfrastruktur erfassen: Paketdaten, Protokolldaten und Endpunktdaten. Wenn NetWitness Endpoint 4.4, 4.4.0.0 oder höher installiert und konfiguriert ist, werden auch Endpunktereignisdaten gesammelt. 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 Decoders 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 Suite **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 Suite 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.

Das NetWitness Suite 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 Suite-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 Suite-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 Hybrid oder Endpoint Log Hybrid. Der Service „Response Server“ (Antwortserver) ist ebenfalls erforderlich und wird verwendet, um Warnmeldungen zu priorisieren.

Die Tabelle enthält eine Übersicht über jede Hauptkomponente:

Systemkomponente	Beschreibung
Decoder/Log Decoder	• NetWitness Suite sammelt Paket-, Protokoll- und Endpunktdaten. • Paketdaten, d. h. Netzwerkpakete, werden mithilfe des Decoder über den Netzwerkanschluss oder Span-Port erfasst, der normalerweise als Ausgangspunkt in einem Unternehmensnetzwerk festgelegt wird. • Ein Log Decoder kann vier verschiedene Protokolltypen erfassen: Syslog, ODBC, Windows-Ereignisverwaltung und Flatfiles. • Windows-Ereignisverwaltung bezieht sich auf die Windows 2008-Erfassungsmethodologie und Flatfiles können über SFTP abgerufen werden. • Beide Decoder-Typen nehmen Transaktionsrohdaten auf, die erweitert, ausgebucht und im Warehouse oder anderen NetWitness Suite-Komponenten zusammengeführt werden. • Das Verfahren zum Aufnehmen und Analysieren von Transaktionsdaten ist ein dynamisches und offenes Framework.
Endpoint Hybrid oder Endpoint Log Hybrid	• Sammelt und verwaltet Endpunktdaten von Hosts. • Erzeugt Metadaten für Untersuchungen, Analysen, Warnmeldungen und Berichte. • Erfasst Protokolle von Windows-Hosts sowie von allen weiteren Ereignisquellen, die für die Protokollerfassung in der NetWitness Suite unterstützt werden.
Concentrator	• Bietet Index und Abfrage bei NetWitness-Sammlungen. • Kann optional Daten an ESA weiterleiten.
Broker	• Verteilt Zugriff auf die NetWitness-Sammlung auf viele Concentrator oder Archiver, sodass die gesamte NetWitness Suite Enterprise als eine einzelne Sammlung angezeigt wird.

Systemkomponente	Beschreibung
Archiver	• Der Archiver-Service ermöglicht die langfristige Protokollarchivierung durch Indexierung und Komprimierung von Protokolldaten und das Senden der Daten an den Archivierungsspeicher. • Der Archivierungsspeicher wurde für eine langfristige Datenaufbewahrung und Compliance-Reporting optimiert. • Archiver speichert Rohdatenprotokolle und Protokollmetadaten von Log Decoders für die langfristige Aufbewahrung. Zur Speicherung wird DAC (Direct-Attached Capacity) verwendet. **Hinweis:** Rohdatenpakete und Paketmetadaten werden nicht im Archiver gespeichert.
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. • ESA verwendet eine erweiterte Ereignisverarbeitungssprache, mit der Benutzern die Filterung, Aggregation, Verknüpfung, Mustererkennung und Korrelation über mehrere verteilte Ereignisstreams ausdrücken können. • ESA erleichtert die leistungsstarke Erkennung von Incidents und Erzeugung von Warnmeldungen. • Die Funktion der automatisierten Bedrohungserkennung von RSA umfasst vorkonfigurierte ESA Analytics-Module zur Erkennung von Befehls- und Datenverkehr.

Core- und Downstream-Komponenten

In NetWitness Suite 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.

Anmelden bei NetWitness Suite

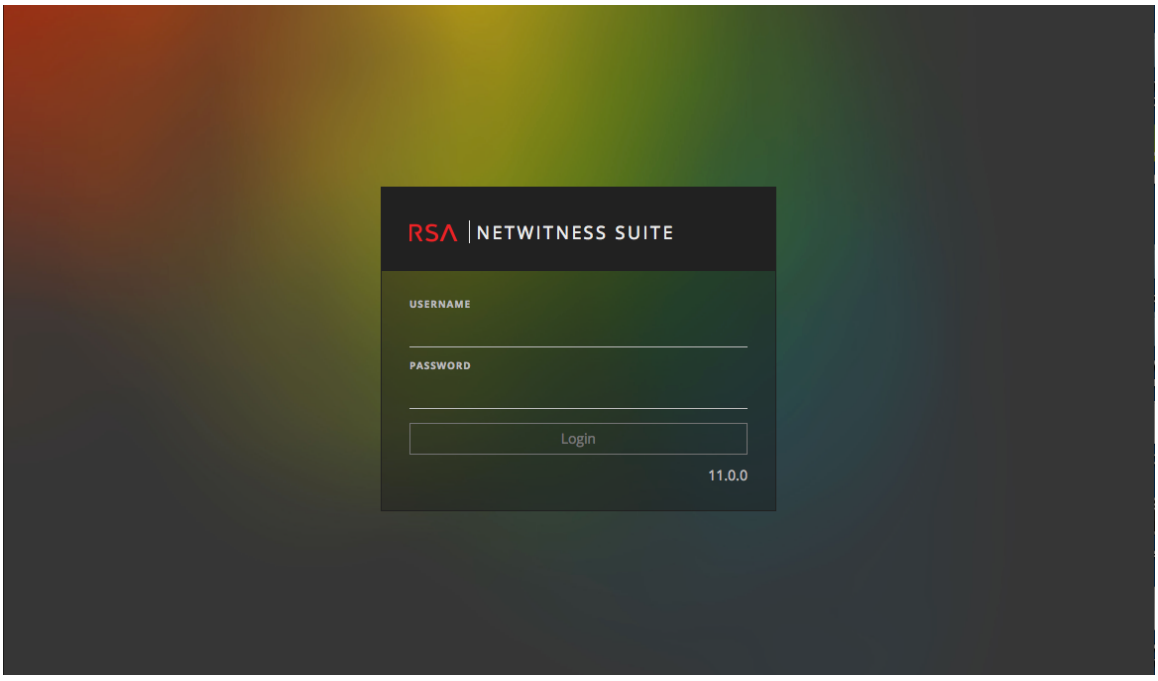
Die Anmeldung bei NetWitness Suite kann je nach Umgebung unterschiedlich sein. Sie können über ein internes Benutzerkonto oder ein externes Benutzerkonto verfügen. Interne Benutzerkonten sind für NetWitness Suite lokal und interne Benutzer können sich bei NetWitness Suite anmelden und erhalten rollenbasierte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

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 Benutzernamen 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.

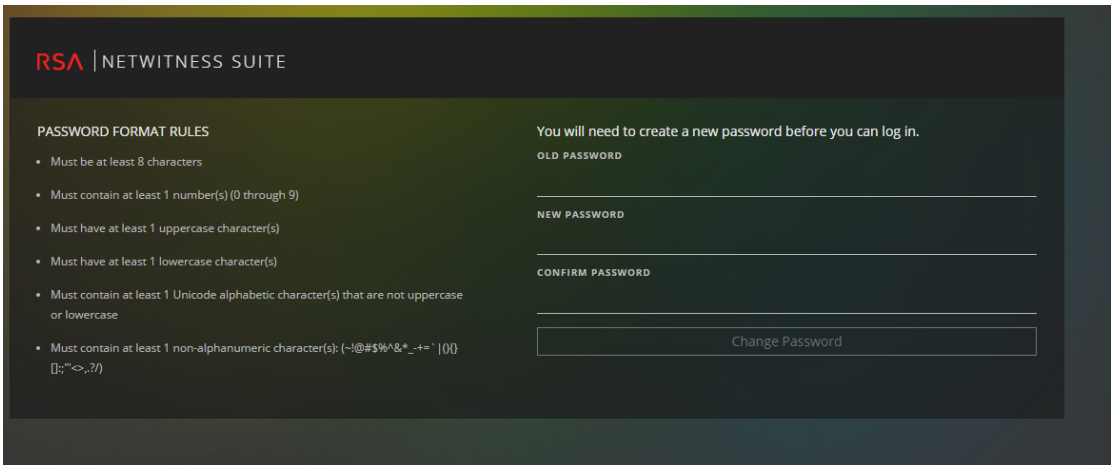
Hinweis: NetWitness Suite unterstützt die neuesten (oder aktuellen) Versionen aktueller Browser.

Wenn Sie gesperrt sind:

Wenn Sie zu oft versuchen, sich mit einem falschen Benutzernamen 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:

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 Suite haben:

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

Abmelden bei NetWitness Suite

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 Benutzereinstellungen auf **Abmelden**.

So melden Sie sich von allen anderen Ansichten ab:

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

Ändern des Passworts

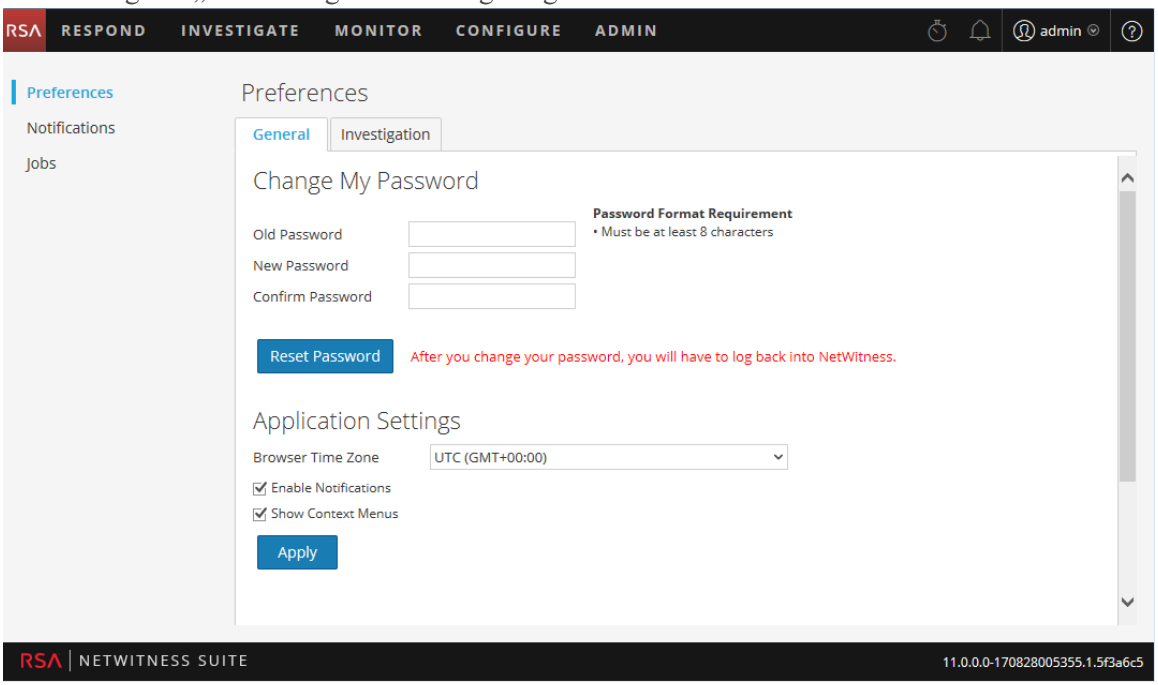
Sie können das Passwort, das Sie für die NetWitness Suite-Authentifizierung verwenden, jederzeit in Ihren Benutzereinstellungen ändern. Ihr Administrator definiert die entsprechenden Anforderungen an die Passwortstärke für Ihr NetWitness Suite-Passwort, wie z B. minimale Passwortlänge und minimale Anzahl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

Hinweis: Geben Sie kein Passwort ein, wenn ein Core-Service eine vertrauenswürdige Verbindung verwendet. Daher ist für Core-Servicekonten keine Aktualisierung erforderlich.

So ändern Sie Ihr Passwort:

1. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie für die meisten Ansichten, z. B. „Untersuchen“, „Überwachen“, „Konfigurieren“ oder „Admin“,  > **Profile** aus.
   - Wählen Sie in der Ansicht „Reagieren“ und einigen „Untersuchen“-Ansichten (Ereignisanalyse, Hosts und Dateien)  und klicken Sie im Dialogfeld „Benutzereinstellungen“ 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 Suite 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 Suite abgemeldet, damit die Änderungen wirksam werden. Das neue Passwort wird bei der nächsten Anmeldung bei NetWitness Suite 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 NetWitness Suite 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

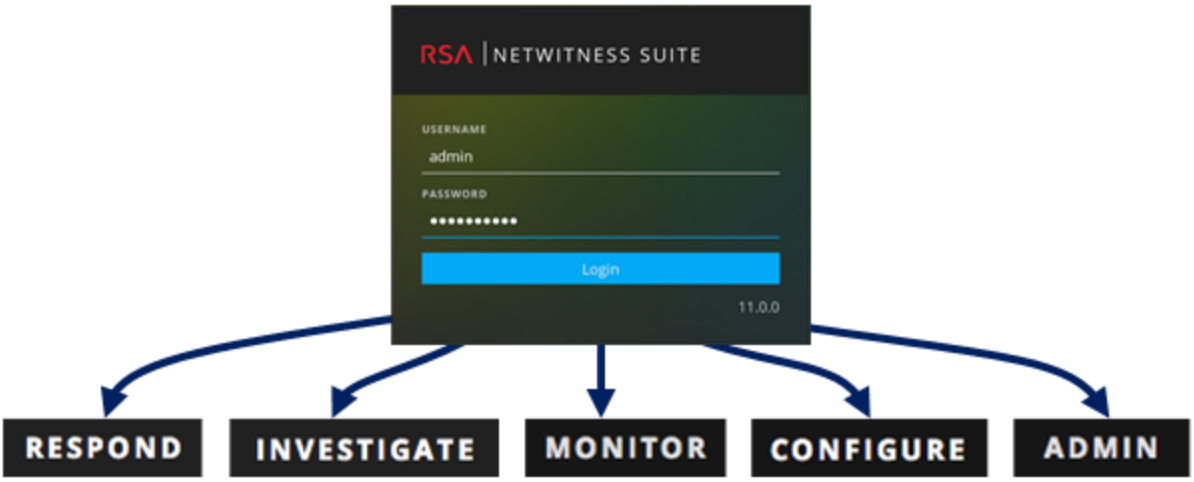
- Installieren und Konfigurieren von Geräten und Software.
- Managen des Benutzerzugriffs
- Monitoring und Anpassen der Performance
- Backup und Wiederherstellen von Daten
- Managen von Speicher und

Archiven

- Aktualisieren der Software
- Erstellen von Berichten zur Einhaltung behördlicher Auflagen

Grundlagen der Navigation in NetWitness Suite

Die NetWitness Suite-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 Suite anzeigen.
  Für Benutzer 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 Suite-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 Benutzer. Sie können verschiedene Bereiche des Dashboards und Berichte je nach Ihren Benutzerberechtigungen anzeigen. NetWitness Suite öffnet diese Ansicht standardmäßig.
  Für Benutzer der Legacy-Version 10.6 ist dies die Ansicht „Dashboard“.
- **Konfigurieren**: Diese Ansicht ist für Mitarbeiter für Bedrohungsinformationen (Inhalt) verfügbar, die Datenquellen und Eingaben in NetWitness Suite konfigurieren. Mitarbeiter für

Bedrohungsinformationen verwenden Sie diesen Bereich zum Herunterladen und Managen von Live-Inhalten. Sie können ebenfalls Incident- und ESA-Regeln erstellen und managen. Benutzer der Legacy-Version 10.6 enthält diese Ansicht „Live“, „Incidents > Konfigurieren“ und „Warnmeldungen > Konfigurieren“ aus der vorherigen Version.

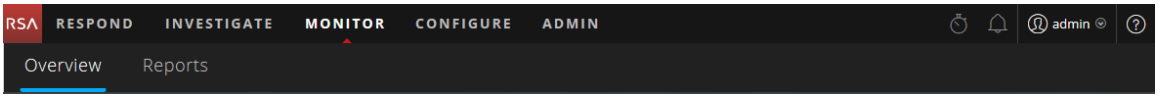
- **ADMIN**: Diese Ansicht ist für Systemadministratoren verfügbar, die die gesamte Anwendung einrichten und verwalten.
  Für Benutzer der Legacy-Version 10.6 entspricht dies der Ansicht „Administration“ ohne die Abschnitte, die zur Ansicht „Konfigurieren“ hinzugefügt wurden.

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.

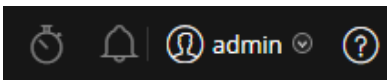
Sekundäre Menüs

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.

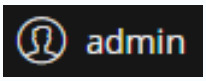
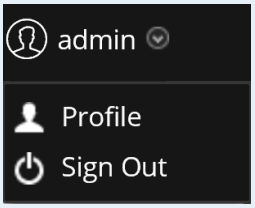


Zusätzliche Optionen

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 Suite-Anwendung in Anspruch nimmt.
	Benachrichtigungen	Klicken Sie auf dieses Symbol, um Benachrichtigungen von der Anwendung anzuzeigen.
	Benutzereinstellungen	Klicken Sie auf dieses Symbol, um Ihre verfügbaren Benutzereinstellungsoptionen anzuzeigen. Sie können Ihre Benutzereinstellungen managen und sich bei NetWitness Suite abmelden.
	Benutzerprofil	Klicken Sie auf Ihr Benutzerprofil, um die verfügbaren Optionen anzuzeigen. Sie können Ihre Benutzereinstellungen managen, Ihr Passwort ändern und sich bei NetWitness Suite abmelden.

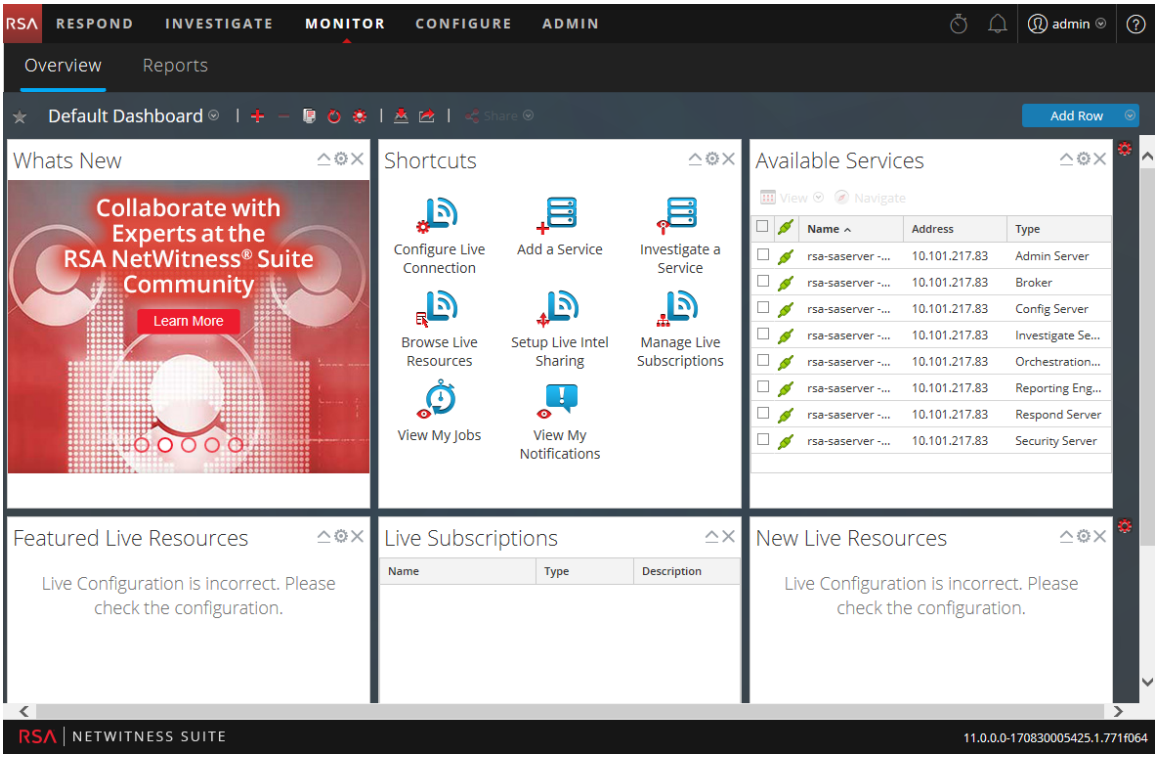
Häufig genutzte Optionen	Name	Beschreibung
	Hilfe	Klicken Sie auf dieses Symbol, um NetWitness Suite-Hilfethemen anzuzeigen.

Hauptansichten

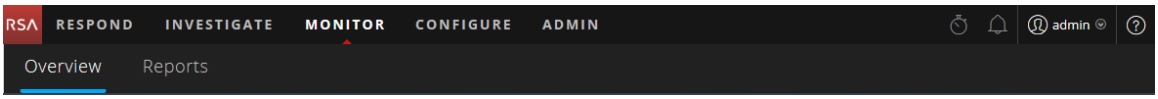
In den folgenden Abschnitten werden die Hauptansichten beschrieben.

Monitor

Die Ansicht Monitor enthält das NetWitness Suite-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 Benutzer 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.

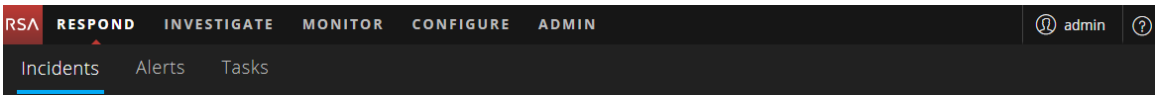
Was kann ich hier tun?	Pfad	Anleitung
Auswählen eines Dashboard	Monitor > Überblick	Siehe Managen von Dashboards.
Erstellen von Dashboards	Monitor > Überblick	Siehe Managen von Dashboards.
Dashboards managen	Monitor > Überblick	Siehe Managen von Dashboards.

Was kann ich hier tun?	Pfad	Anleitung
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.

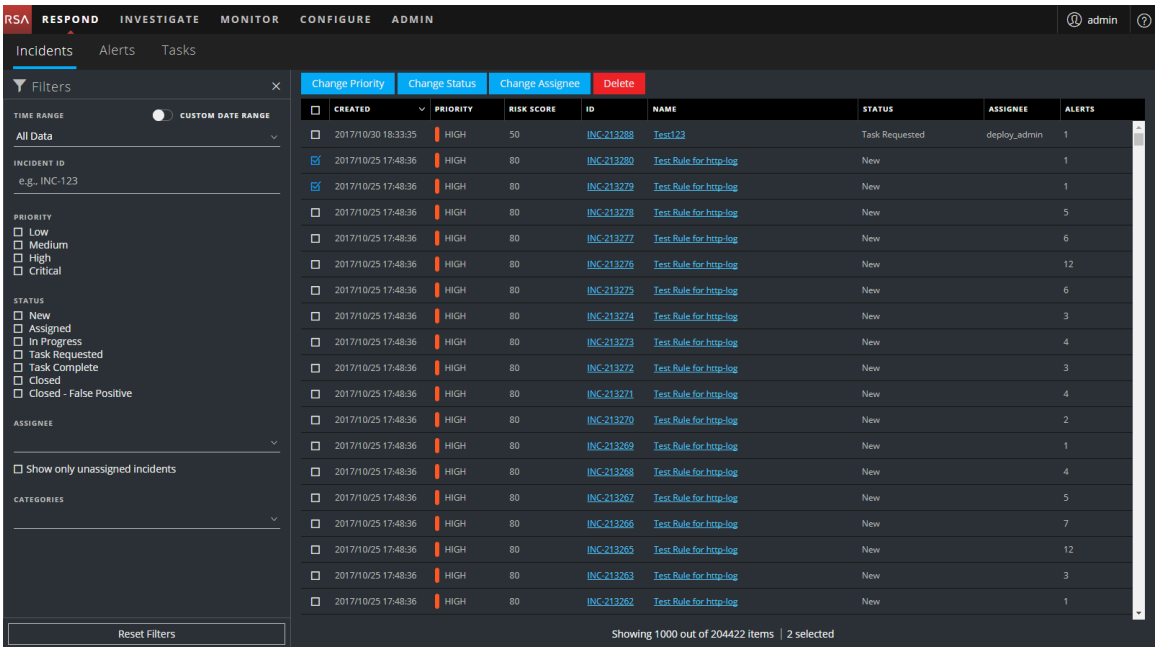
Reagieren-Menü



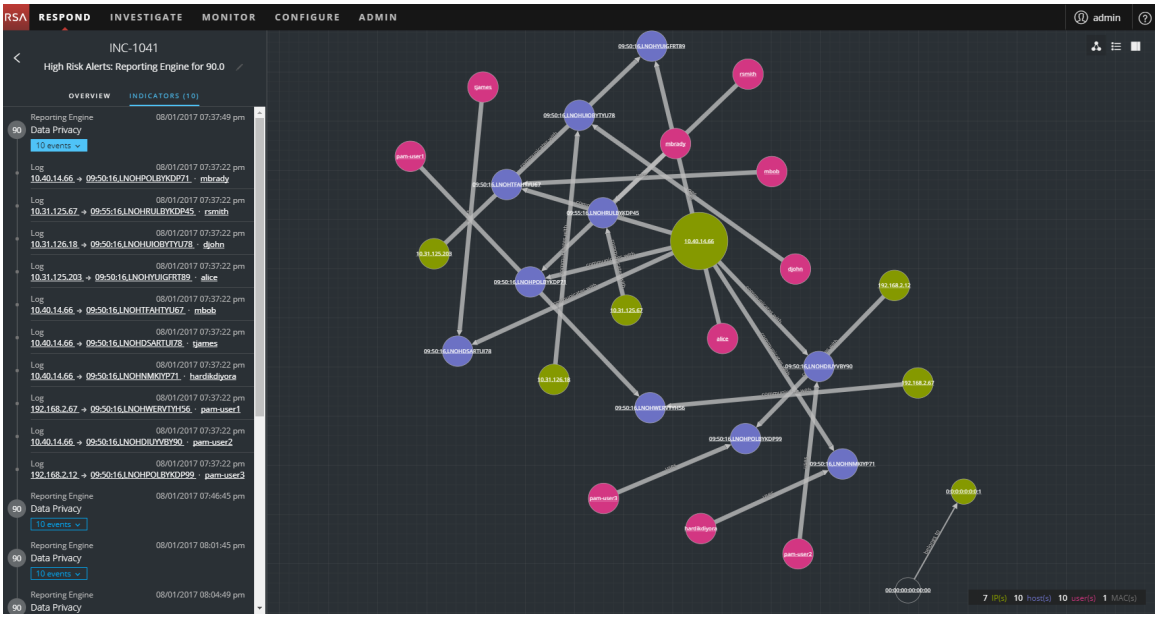
Das Menü Reagieren enthält die folgenden Optionen:

- **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 Suite erhaltenen Bedrohungen und Indikatoren an einem zentralen Speicherort.
- **Aufgaben**: Mit der Ansicht „Aufgabenliste“ können Sie Aufgaben erstellen und bis zum Abschluss nachverfolgen.

Die folgende Abbildung zeigt die Ansicht „Reagieren“ – Ansicht „Incident-Liste“.

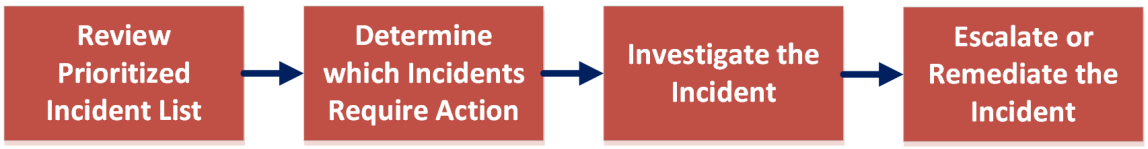


Die folgende Abbildung zeigt ein Beispiel der Ansicht „Reagieren“ – Ansicht „Incident-Details“.



Wenn Sie NetWitness Suite als Vorgangsmanagementtool verwenden, können Sie auch Incidents in dieser Ansicht managen. Neue Incidents werden oben in der Incident-Warteschlange in der Reihenfolge der Priorität angezeigt. Ausgeführte Incidents befinden sich unter neuen Incidents.

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



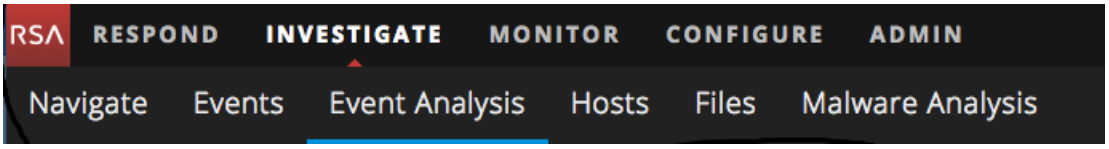
Analysten können in der Ansicht „Reagieren“ die priorisierte Liste der Incidents einsehen und bestimmen, für welche Incidents eine Aktion erforderlich ist. Sie klicken auf einen Incident, um mithilfe unterstützender Details ein klareres Bild von diesem Incident zu erhalten. So können sie den Incident 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*.
Bestimmen, 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 sechs unterschiedliche Ansichten eines Datensatzes, sodass Analysten Metadaten, Endpunktdaten, Protokolle, Ereignisse und 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 sechs „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.

Menü „UNTERSUCHEN“

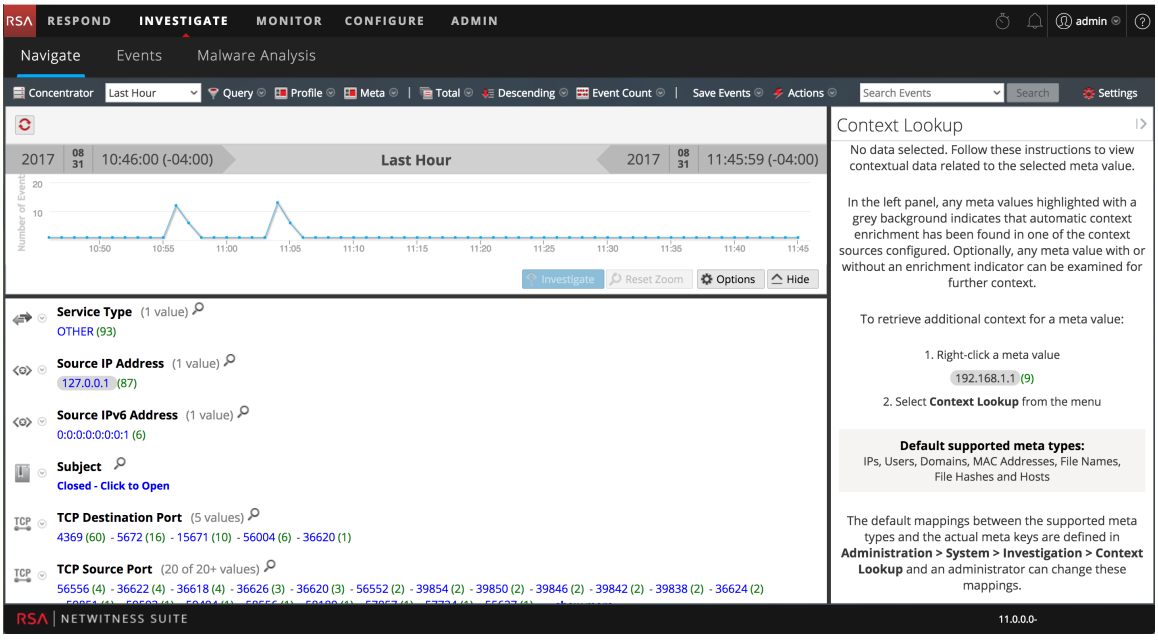


Das Menü Ermittlung enthält die folgenden Optionen:

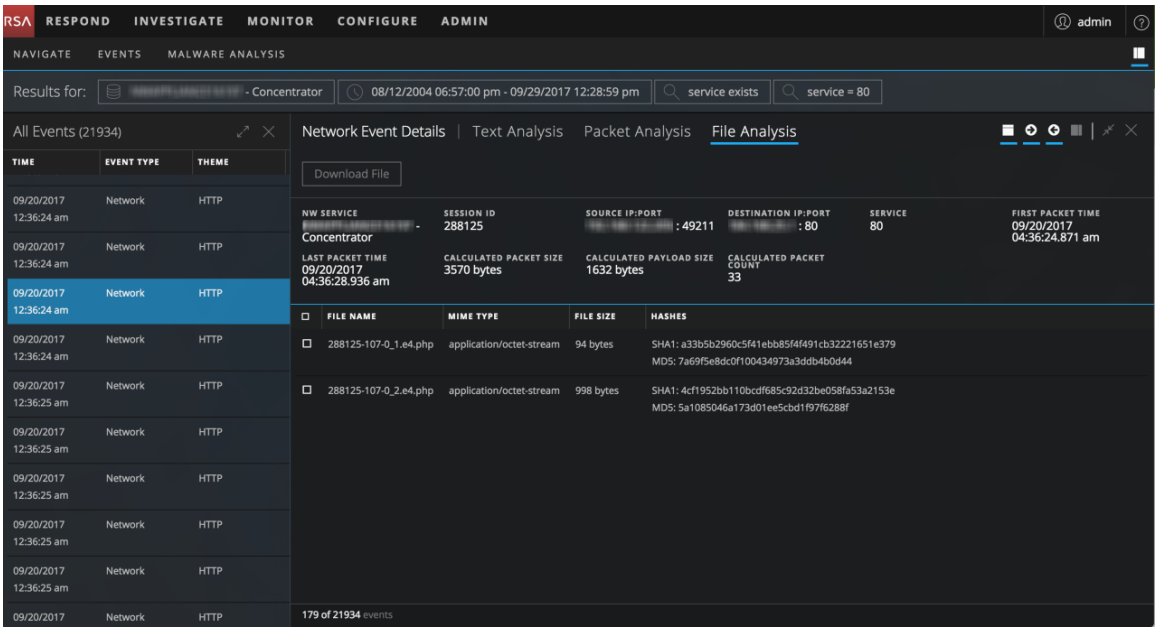
- **Navigieren**: Die Ansicht „Navigation“ enthält eine Liste der Metaschlüssel und Metawerte mit dem Fokus auf Metadaten. Sie können ein Drilldown in die Daten durchführen, ein ausgewähltes Ereignis in der Ansicht „Ereignisse“ oder „Ereignisanalyse“ öffnen, eine Rekonstruktion eines Ereignisses anzeigen, 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 eines Ereignisses anzeigen, eine Ereignisanalyse durchführen und die Einstellungen für die Ereignisansicht 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“ oder zum eigenständigen Endpoint-Modul wechseln, Daten in Live nachschlagen und externe Suchen durchführen.

- **Ansicht „Hosts“**: (Version 11.1 oder höher) Die Ansicht „Hosts“ enthält alle Hosts, auf denen ein NetWitness Endpoint Insights Agent ausgeführt wird. Für jeden Host können Sie Prozesse, Treiber, DLLs, (ausführbare) Dateien, Services und automatische Ausführungen sehen, die gerade aktiv sind, sowie Informationen in Bezug auf angemeldete Benutzer. Von der Ansicht „Hosts“ können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln.
- **Ansicht „Dateien“**: (Version 11.1 oder höher) Die Ansicht „Dateien“ enthält alle eindeutige Dateien, die in Ihrer Bereitstellung gefunden wurden, sowie die zugehörigen Eigenschaften. Für jede Datei können Sie Details wie Dateigröße, Entropie, Format, Firmenname, Signatur und Prüfsumme anzeigen. Von der Ansicht „Dateien“ können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln.
- **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.

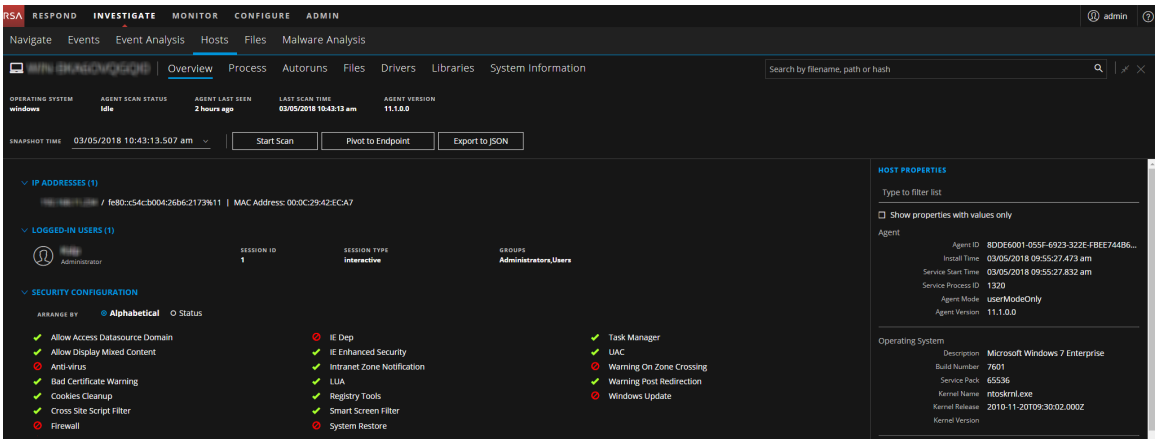
Die folgende Abbildung zeigt die Ansicht „Untersuchen“ – Ansicht „Navigation“.



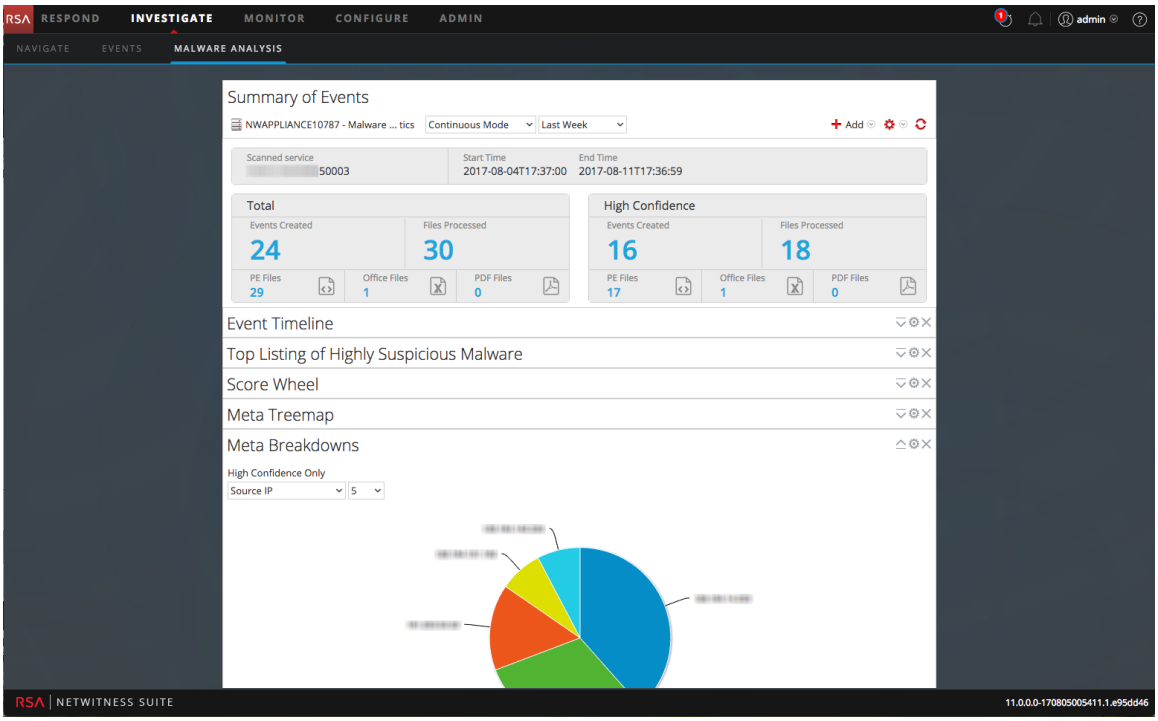
Die folgende Abbildung zeigt die Ansicht „Untersuchen“ – Ansicht „Ereignisanalyse“.



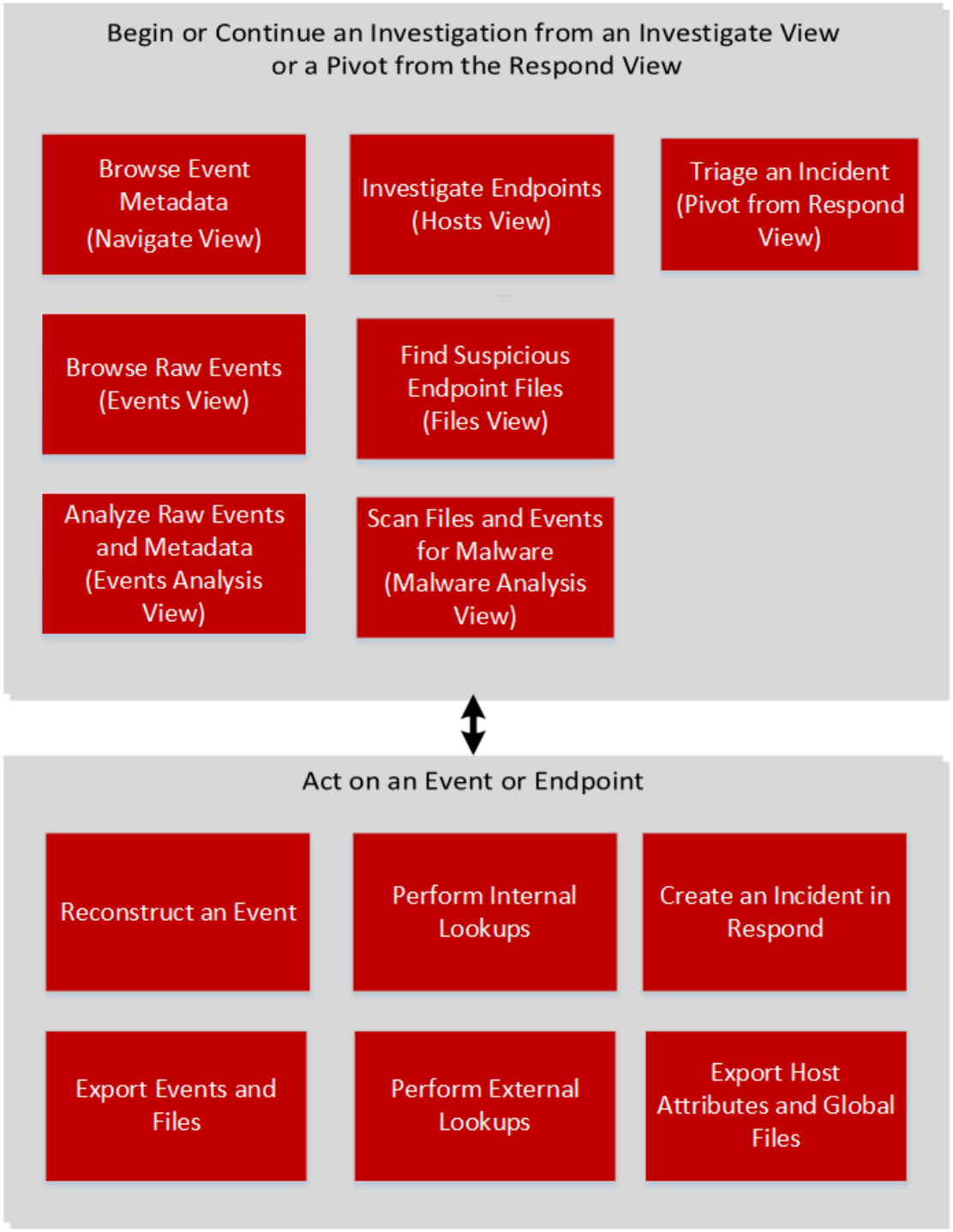
Die folgende Abbildung zeigt die Ansicht „Hosts“ – Ansicht „Details zum Host“.



Die folgende Abbildung zeigt die Malware Analysis-Ereigniszusammenfassung.



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

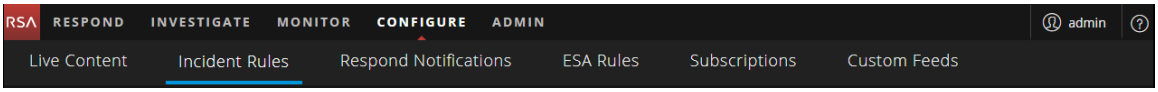

Begin or Continue an Investigation from an Investigate View or a Pivot from the Respond View
Browse Event Metadata (Navigate View)
Investigate Endpoints (Hosts View)
Triage an Incident (Pivot from Respond View)
Browse Raw Events (Events View)
Find Suspicious Endpoint Files (Files View)
Analyze Raw Events and Metadata (Events Analysis View)
Scan Files and Events for Malware (Malware Analysis View)
Act on an Event or Endpoint
Reconstruct an Event
Perform Internal Lookups
Create an Incident in Respond
Export Events and Files
Perform External Lookups
Export Host Attributes and Global Files

Was kann ich hier tun?	Pfad	Anleitung
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 „Untersuchen von Metadaten und Raw-Ereignissen in der Ansicht ‚Ereignisanalyse‘“ im *NetWitness Investigate – Benutzerhandbuch*.
Untersuchen von Endpunkten	Ansicht „Hosts“	Siehe „Untersuchen von Hosts und Dateien“ im *NetWitness Investigate – Benutzerhandbuch*.
Finden verdächtiger Endpunktdateien	Ansicht „Dateien“	Siehe „Untersuchen von Hosts und Dateien“ im *NetWitness Investigate – Benutzerhandbuch*
Dateien und Ereignisse auf Schadsoftware scannen	Ansicht „Malware Analysis“	Siehe „Durchführen von Schadsoftwareanalysen“ im *NetWitness Investigate – Benutzerhandbuch*

Konfigurieren

Die Ansicht „Konfigurieren“ ermöglicht Mitarbeitern für Bedrohungsinformationen (Inhalt) die Konfiguration der Datenquellen und Eingaben in NetWitness Suite 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 Suite, die die Kommunikation und Synchronisation zwischen NetWitness Suite-Services und

einer Bibliothek von Live-Inhalten managt, die RSA NetWitness Suite-Kunden zur Verfügung stehen. Sie können Inhalte aus dem RSA Live-Contentmanagementsystem (CMS) auf NetWitness Suite-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 Benutzer 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 Benutzer 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 Benutzer 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 Suite, um Live-Services in NetWitness Suite einzurichten.
  Für Benutzer 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 leitet die Feeds an ausgewählte Decoders und Log Decoders. Sie können benutzerdefinierte Feeds und Identitätsfeeds einrichten und verwalten.
  NetWitness Suite 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

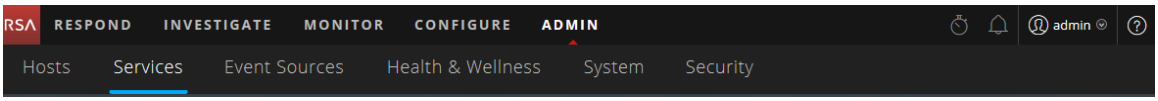
Abgleich werden zusätzliche Metadaten erstellt.
Sie können benutzerdefinierte Feeds zur Bereitstellung von zusätzlichen Metadaten erstellen, z. B. Metadatenextrahierungen, um benutzerdefinierten Netzwerkanwendungen gerecht zu werden.
Für Benutzer der Legacy-Version 10.6 war dies „Live“ > „Feeds“.

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 Suite	Konfigurieren > Abonnement	Siehe *Handbuch zum Management von Live-Services*.
Einrichten und Verwalten von benutzerdefinierten Feeds und Identitätsfeeds	Konfigurieren > Benutzerdefinierte Feeds	Siehe *Handbuch zum Management von Live-Services*.

ADMIN

In der Ansicht „Admin“ können Administratoren Netzwerkhosts und -services managen, die Integrität und den Zustand von NetWitness Suite 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.
- **Integrität und Zustand**: Mit der Ansicht „Integrität und Zustand“ können Sie die Integrität der NetWitness Suite-Hosts und -Services in Ihrer Netzwerkumgebung überwachen.
- **System**: Mit der Ansicht „System“ können Sie globale NetWitness Suite-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 Suite-Versionen managen und den lokalen Lizenzierungsserver konfigurieren.
- **Sicherheit:** Der Bereich „Administrationssicherheit“ bietet die Möglichkeit, Benutzerkonten und Benutzerrollen zu managen, externe Gruppen NetWitness Suite-Rollen zuzuordnen und andere sicherheitsbezogene Systemparameter zu ändern. Diese Funktionen gelten für das NetWitness Suite-System und werden in Verbindung mit den Sicherheitseinstellungen für einzelne Services verwendet.

Was kann ich hier tun?	Pfad	Anleitung
Verwalten von Hosts	ADMIN > Hosts	Siehe *Leitfaden für die ersten Schritte mit Hosts und Services*.

Was kann ich hier tun?	Pfad	Anleitung
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*.
Einrichten und Überwachen von Alarmen für die Hosts und Services in Ihrer NetWitness Suite-Domain	ADMIN > Integrität und Zustand > Alarm	Siehe *Leitfaden Systemwartung*.
Überwachen von Statistiken für die NetWitness Suite-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 Suite-Domain zu unterstützen	ADMIN > Integrität und Zustand > Policys.	Siehe *Leitfaden Systemwartung*.
Festlegen der globalen Konfigurationen für NetWitness Suite	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 Benutzerverwaltung*.
Managen von Systembenutzern mit Rollen und Berechtigungen	ADMIN > Sicherheit	Siehe *Handbuch Systemsicherheit und Benutzerverwaltung*.

Einrichten einer Standardansicht nach SOC-Rolle

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

Die folgende Abbildung zeigt die Hauptansichten in NetWitness Suite.

- **Reagieren**: Diese Ansicht ist für Incident Responders bestimmt, die eine Liste der Incidents zur Priorisierung und Warnmeldungen anzeigen können. Benutzer 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.
- **Überwachen**: 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 für Bedrohungsinformationen (Inhalt) verfügbar, die Datenquellen und Eingaben in NetWitness Suite konfigurieren. Mitarbeiter für Bedrohungsinformationen verwenden Sie diesen Bereich zum Herunterladen und Managen von Live-Inhalten. Sie können ebenfalls Incident- und ESA-Regeln erstellen und managen. Benutzer 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 Suite als Standardansicht auswählen. Zusätzlich zu den Hauptansichten verfügt NetWitness Suite 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“

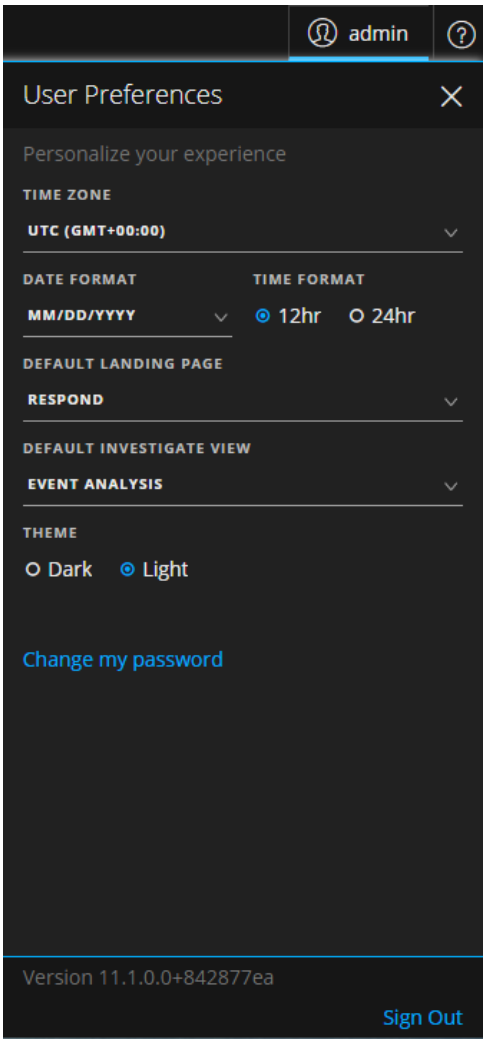
In der folgenden Tabelle sind typische SOC-Rollen und die verfügbaren Ansichten aufgeführt, die Sie als Landingpage in Ihren Benutzereinstellungen basierend auf Ihrer SOC-Rolle auswählen können. Wenn Sie über mehr als eine Administratorrolle verfügen, wählen Sie die Ansicht, die für Sie am besten geeignet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

SOC-Rollen	Rollenbeschreibung	Berücksichtigen dieser standardmäßigen Landingpage
Incident-Experte (Tier-1-Analyst)	Geht Incidents und Warnmeldungen in der Warteschlange an, um sie zu überprüfen und zu minimieren.	**Reagieren**
Threat Hunter (Tier-2-/Tier-3-Analyst)	Führt eine Ermittlung und Erkennung von Advanced Threats durch.	**Ermittlung**
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.

SOC-Rollen	Rollenbeschreibung	Berücksichtigen dieser standardmäßigen Landingpage
Contentexperte (Bedrohungsintelligenz)	Konfiguriert Datenquellen und Eingaben in NetWitness Suite.	**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.)
Systemadministrator	Konzentriert sich auf die Konfiguration und die Stabilität der gesamten Anwendung. Managt den Benutzerzugriff.	**Admin**

Einstellen der Standardansicht

1. (Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten) Wählen Sie auf der Hauptmenüleiste  .
   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 Suite 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 Benutzereinstellungen.
3. Wenn Sie überprüfen möchten, ob Sie die richtige Standardansicht sehen, können Sie zum Abmelden auf **Abmelden** klicken und sich dann wieder bei NetWitness Suite anmelden.

Grundlegende Troubleshooting-Tipps für den Benutzersetup

Die folgende Tabelle enthält grundlegende Troubleshooting-Tipps, die möglicherweise hilfreich für den Benutzersetup in NetWitness Suite sein können.

Problem	Troubleshooting-Tipp
Wenn ich mich bei NetWitness Suite anmelde, wird die falsche Standardansicht angezeigt.	Stellen Sie sicher, dass die richtigen Standardansicht im Feld „Standardmäßige Landingpage“ in Ihren Benutzereinstellungen 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.	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 Suite unterstützt die neuesten (oder aktuellen) Versionen aktueller Browser. Installieren Sie eine neuere Browserversion. Wenn Sie kein Upgrade Ihres Browsers durchführen können, können Sie versuchen, das Protokoll TLS 1.2-in Ihrem Browser zu aktivieren: Navigieren Sie zu **Internetoptionen > Erweitert > Einstellungen > Sicherheit**. Vergewissern Sie sich, dass zusätzlich zu Ihren anderen Protokollen auch das Protokoll TLS 1.2 aktiviert ist. Klicken Sie auf **Anwenden**. Laden Sie die Seite erneut.
Wenn ich mich anmelde, wird nichts angezeigt.	Wenden Sie sich an Ihren Administrator. Es muss Ihnen möglicherweise eine Benutzerrolle für Ihr Konto zugewiesen werden oder Sie benötigen zusätzliches Troubleshooting.

Problem	Troubleshooting-Tipp
Ich weiß nicht, wo ich meine standardmäßige Landingpage ändern kann.	Navigieren Sie zu den Benutzereinstellungen in der Ansicht „Reagieren“ oder wenden Sie sich an Ihren Administrator.

Festlegen von Benutzereinstellungen

Sie können Ihre globalen NetWitness Suite-Anwendungseinstellungen in Ihrem Benutzerprofil anzeigen und managen. Ihre globalen Einstellungsoptionen variieren abhängig davon, ob Sie darauf aus der Ansicht „Reagieren“ oder aus anderen Ansichten, z. B. „Überwachung“, „Konfigurieren“, „Admin“ und „Untersuchen“, zugreifen.
Sie können Folgendes tun:

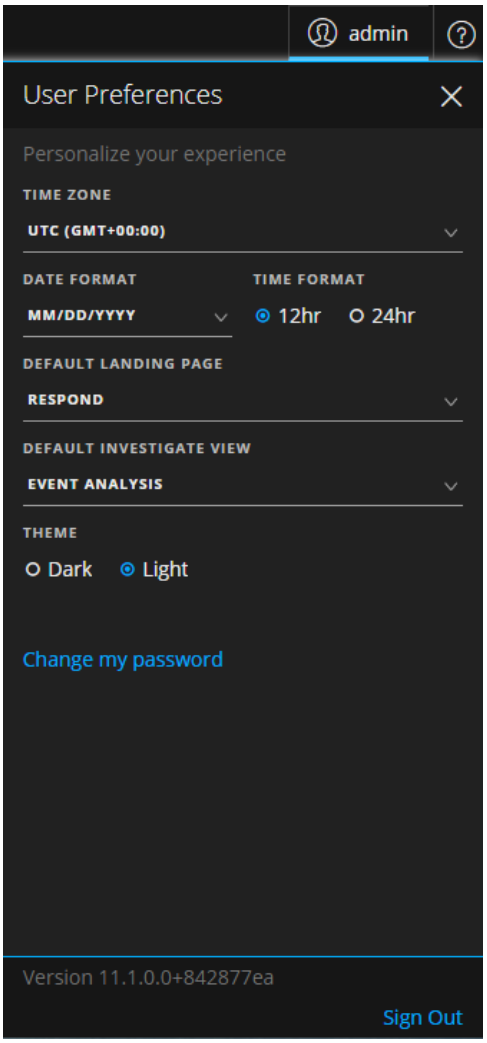
- Festlegen der Zeitzone der Anwendung
- Festlegen des Datums- und Uhrzeitformats der Anwendung*
- Auswählen der standardmäßigen Startansicht für NetWitness Suite*
- Auswählen der standardmäßigen Ansicht „Untersuchen“*
- Auswählen eines dunklen oder hellen Designs für die Anwendung*
- Ihr Passwort ändern (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 und Dateien.

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

Anzeigen der Benutzereinstellungen (Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten)

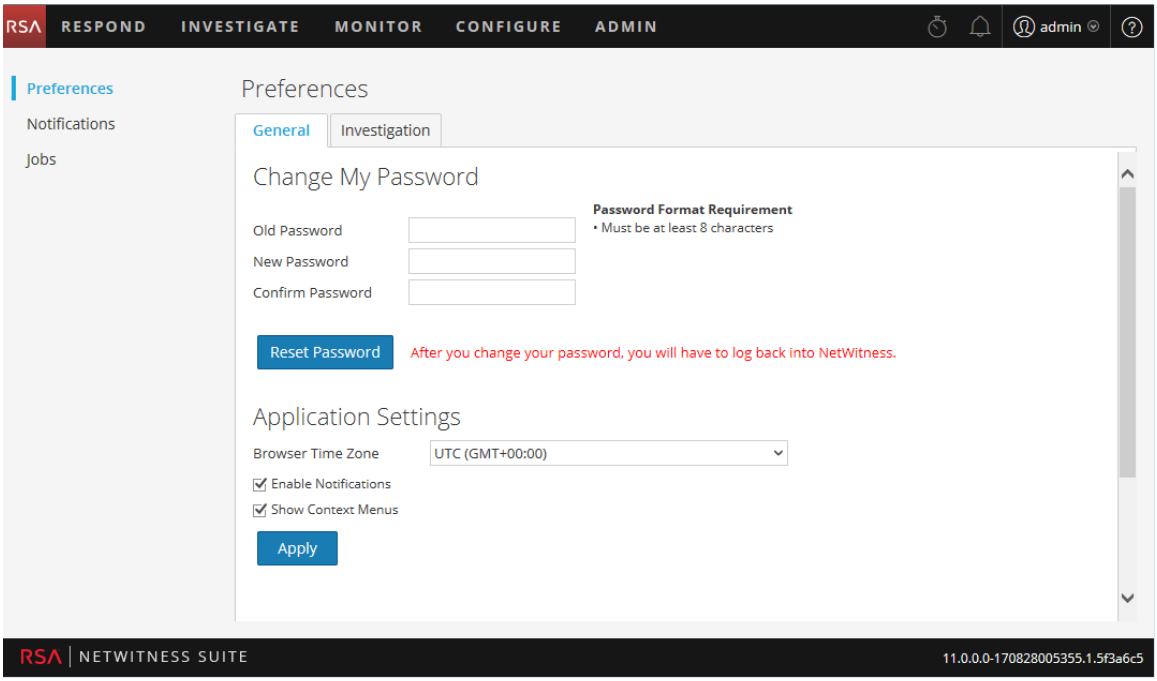
Wählen Sie in der oberen linken Ecke des NetWitness Suite-Browserfensters  aus.
Im Dialogfeld „Benutzereinstellungen“ werden die aktuellen Einstellungen angezeigt, wenn es über die Ansicht „Reagieren“ und folgende „Untersuchen“-Ansichten aufgerufen wird: Ereignisanalyse, Hosts und Dateien.



Die von Ihnen vorgenommenen Einstellungen werden sofort wirksam.

Anzeigen der Benutzereinstellungen (in den meisten Ansichten außer „Reagieren“ und einiger „Untersuchen“-Ansichten)

Bei den meisten der folgenden Ansichten: Untersuchen, Überwachen, Konfigurieren und Admin: Wählen Sie in der oberen linken Ecke des NetWitness Suite-Browserfensters > **Profil** aus. Im Dialogfeld „Einstellungen“ werden die aktuellen Einstellungen angezeigt.



Einstellen von Zeitzone und Datums- und Uhrzeitformat

Sie können die Zeitzone und das Datums und Uhrzeitformat für Ihren Standort ändern.

Hinweis: Sie können die Datums- und Uhrzeiteinstellungen für Ihren Standort nur in der Ansicht „Reagieren“ und einigen „Untersuchen“-Ansichten ändern: Ereignisanalyse, Hosts und Dateien.

1. Wählen Sie im Dialogfeld „Benutzereinstellungen“ Ihre Lokalisierungseinstellungen aus:
   a. **Zeitzone**: Legen Sie die Zeitzone für die Verwendung in NetWitness Suite fest.
   b. **(Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten) 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.

c. **(Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten) 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 der Ansicht „Reagieren“ werden sofort wirksam.

2. **(In den meisten Ansichten außer „Reagieren“ und einiger „Untersuchen“-Ansichten)** Klicken Sie auf **Anwenden**.
   Die Einstellungen werden sofort wirksam.

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

Auswählen der standardmäßigen Startansicht der NetWitness Suite

1. **(Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten)** Öffnen Sie das Dialogfeld „Benutzereinstellungen“.
2. Wählen Sie im Feld **Standardmäßige Landingpage** die Ansicht beim Öffnen aus, die Sie sehen möchten, wenn Sie sich bei NetWitness Suite anmelden. Sie können entsprechend Ihrer Benutzerrolle „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. **(Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten)** Öffnen Sie das Dialogfeld „Benutzereinstellungen“.
2. Legen Sie im Feld **Standardmäßige Ansicht „Untersuchen“** die standardmäßige Landingpage fest, die angezeigt werden soll, wenn Sie sich bei NetWitness Suite anmelden und zu „Untersuchen“ navigieren. Sie können die Ansichten „Navigation“, „Ereignisse“, „Ereignisanalyse“, „Hosts“, „Dateien“ oder „Malware Analysis“ als standardmäßige Ansicht „Untersuchen“ wählen. 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.

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

Auswählen der Darstellung von NetWitness Suite

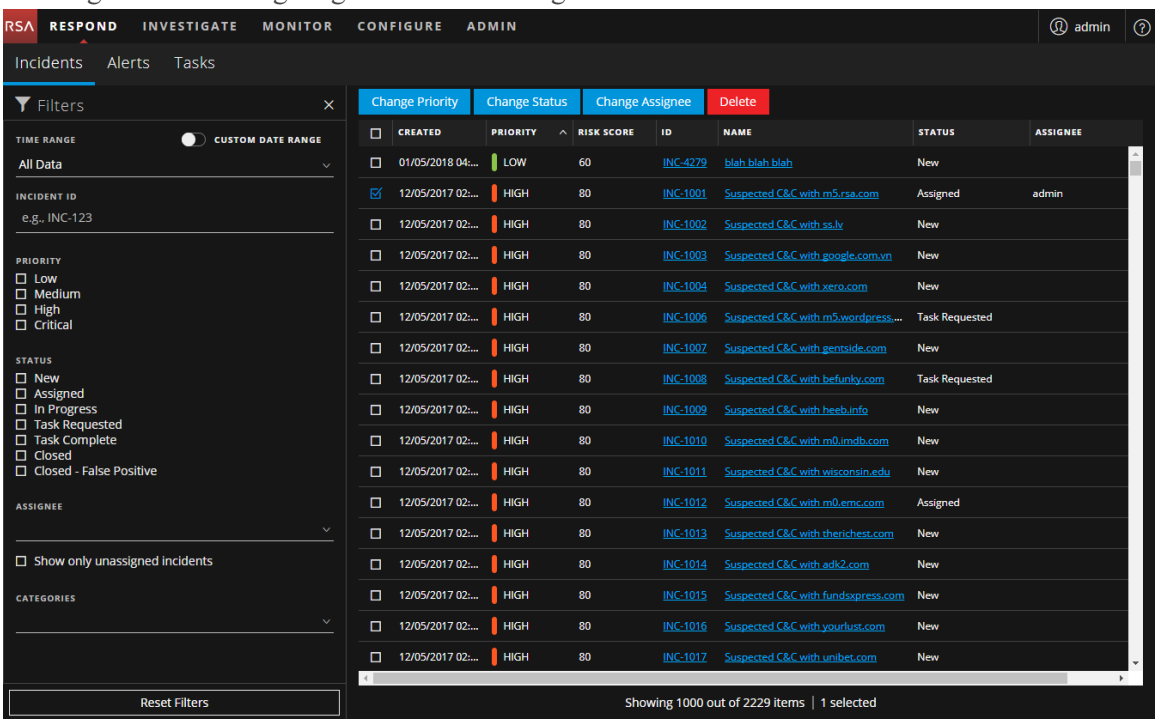
Diese Option ist nur für NetWitness Suite Version 11.1 und höher verfügbar.

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 Suite für Sie dargestellt wird, nicht auf die Darstellung für andere Benutzer.

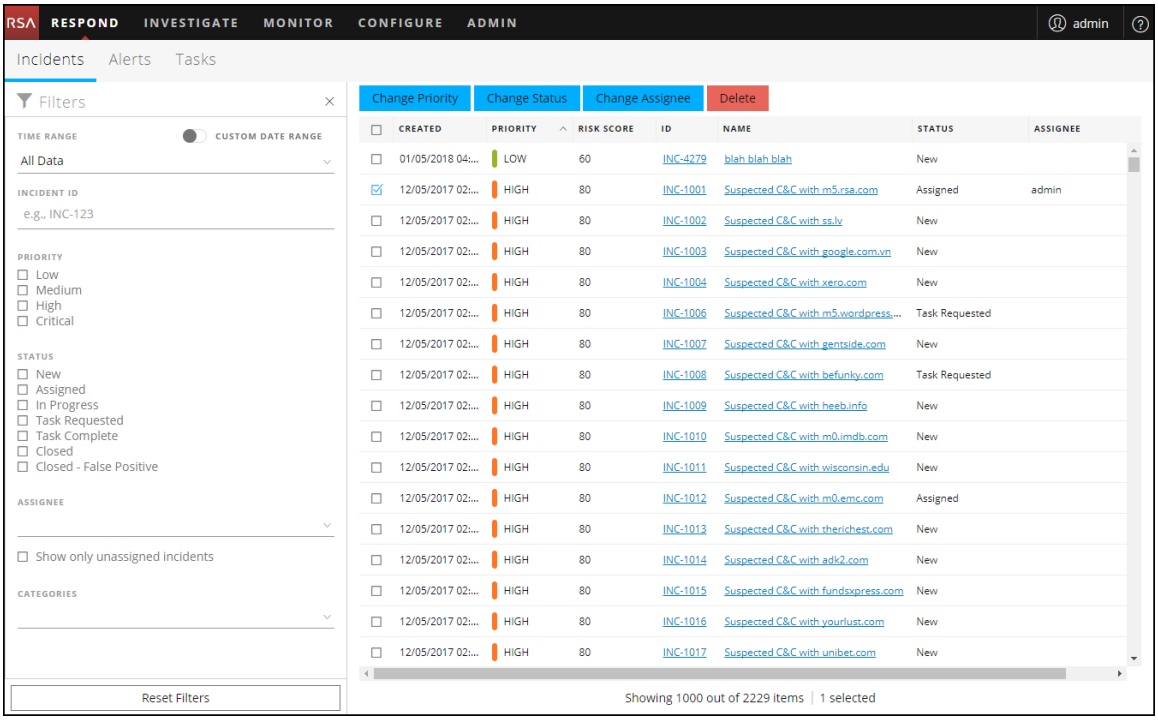
1. **(Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten)** Öffnen Sie das Dialogfeld „Benutzereinstellungen“.
2. Wählen Sie unter **DESIGN** eine der folgenden Optionen aus:
   - **Dunkel**: Das dunkle Design ist am besten für dunklere Umgebungen geeignet oder wenn Sie nicht so viel Kontrast benötigen.
   - **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.



Aktivieren oder Deaktivieren von Systembenachrichtigungen für Ihr Benutzerkonto

(In den meisten Ansichten außer „Reagieren“ und einiger „Untersuchen“-Ansichten) Die NetWitness Suite-Systembenachrichtigungen sind 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 Benutzerkonto 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 Benutzerkonto

(In den meisten Ansichten außer „Reagieren“ und einiger „Untersuchen“-Ansichten) Kontextmenüs sind bei der Erstellung eines neuen Benutzerkontos 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 Benutzerkonto 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.

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 NetWitness Suite können Sie Dashboards zusammensetzen, um allgemeine Informationen und Kennzahlen zu erhalten, die ein Gesamtbild der NetWitness Suite-Bereitstellung darstellen, und nur die wichtigsten Informationen anzeigen, die für den täglichen Betrieb von Bedeutung sind.

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

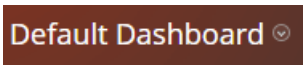
Sie können verschiedene Bereiche des Dashboards und Berichte je nach Ihren Benutzerberechtigungen anzeigen. Sie können ein vorkonfiguriertes Dashboard auswählen, ein Dashboard importieren oder Ihr eigenes angepasstes Dashboard erstellen. Mit den Dashboards können Sie schnell und einfach Berichte anzeigen. 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 standardmäßigen Landingpage zur Anmeldung bei NetWitness Suite ist, wird Ihnen nach Abschluss des Anmeldeprozesses immer das Standarddashboard oder das aktuell konfigurierte Dashboard angezeigt. Wählen Sie zum Zurückkehren zum Dashboard von einer anderen NetWitness Suite-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 Suite-Symbolleiste angezeigt.

Ein Dashboard verfügt über Folgendes:

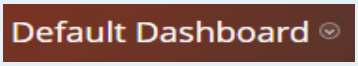
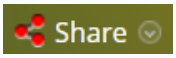
- die Dashboard-Symbolleiste
- den Dashboard-Titel und die Dashboards-Auswahlliste

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.

Option	Beschreibung
	Zeigt die Liste der verfügbaren Dashboards an, aus denen Sie auswählen können.
	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 Benutzer.
	Ermöglicht Benutzern, dem Dashboard basierend auf den Anforderungen Zeilen und Spalten hinzuzufügen. 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 Suite 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:

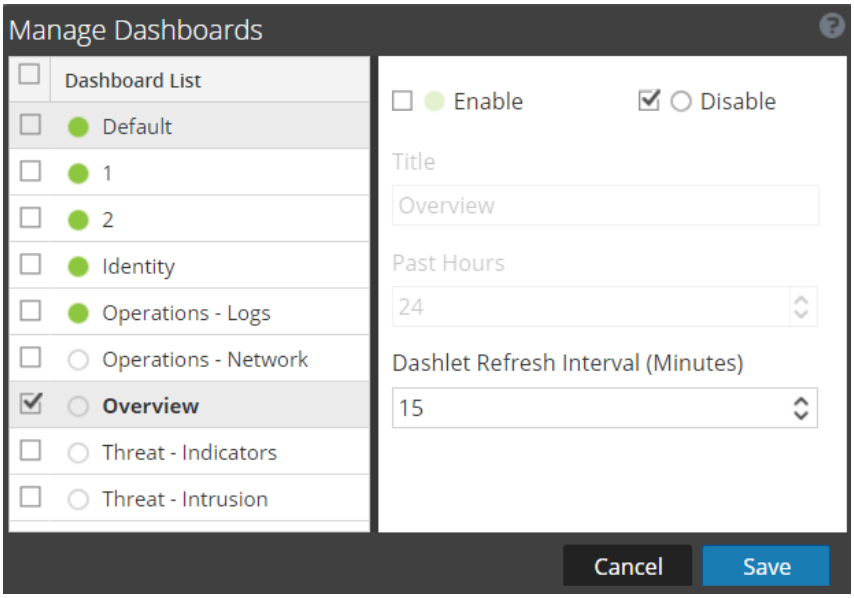
- Bearbeiten eines Dashboards
- Exportieren eines Dashboards
- Freigeben eines Dashboards
- Löschen eines Dashboard

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

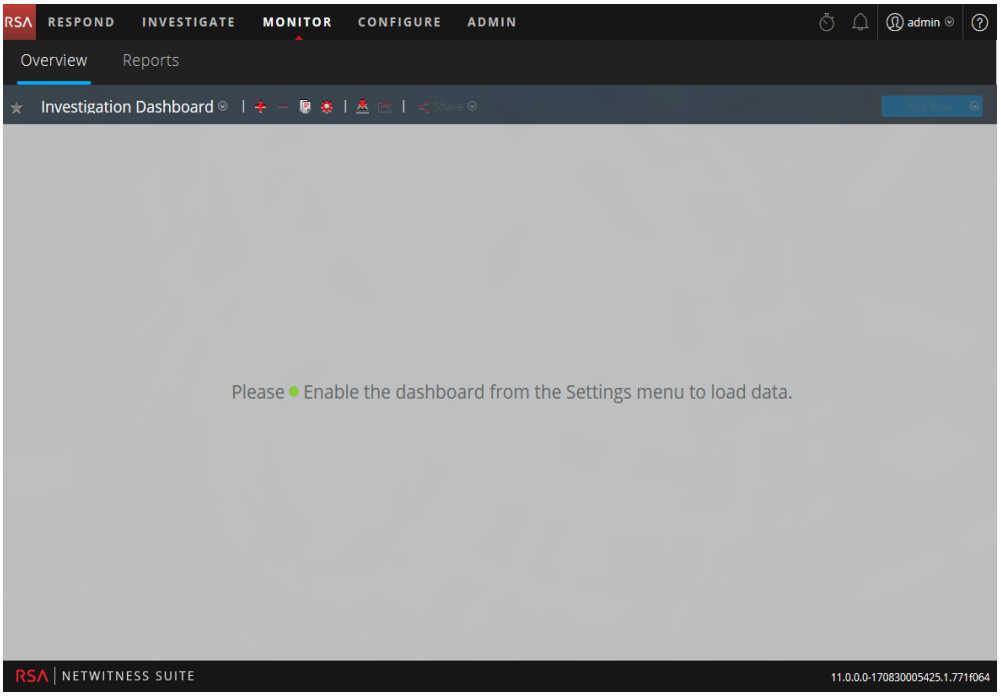


Name	Beschreibung
Dashboardliste	Zeigt eine Liste der standardmäßigen, vorkonfigurierten und benutzerdefinierten Dashboards an.
Enable	Zeigt an, ob das ausgewählte Dashlet aktiviert ist.
Disable	Zeigt an, ob das ausgewählte Dashlet deaktiviert ist.
Titel	Zeigt den Titel des ausgewählten Dashlet. Sie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

Name	Beschreibung
Dashlet-Aktualisierungsintervall (Minuten)	Zeigt das Aktualisierungsintervall eines Dashlet an.

Aktivieren eines Dashboards

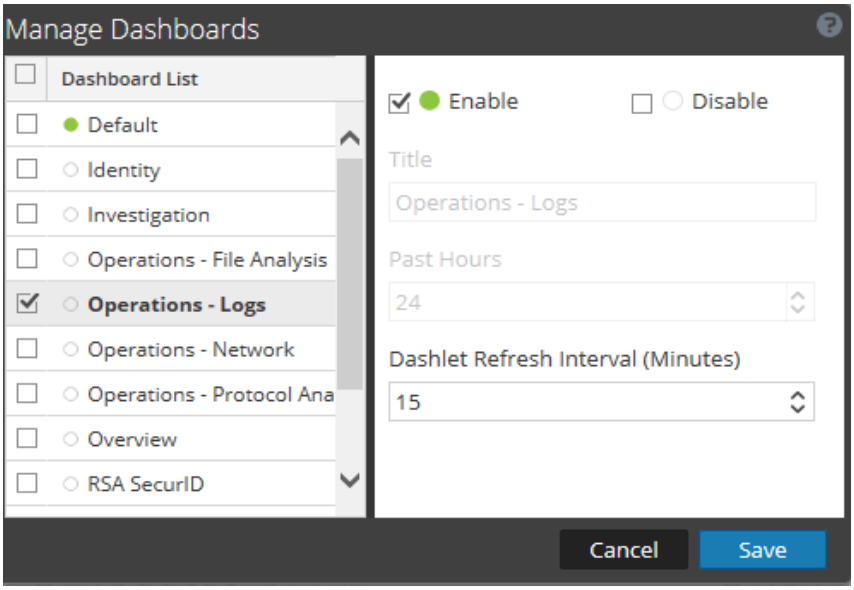
Wenn Sie ein Dashboard auswählen, das nicht aktiviert ist, wird ein maskierter Bildschirm angezeigt.



So aktivieren Sie ein oder mehrere Dashboard(s):

1. Navigieren Sie zu dem Dashboard, das aktiviert werden soll.
2. Klicken Sie in der Dashboardsymbolleiste auf  .

3. Wählen Sie die Option **Dashboard managen** aus.
   Das Dialogfeld „Dashboards managen“ wird angezeigt.



4. Wählen Sie aus der Dashboardliste das bzw. die zu aktivierende(n) Dashboard(s) aus.
5. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
6. Klicken Sie auf **Speichern**.

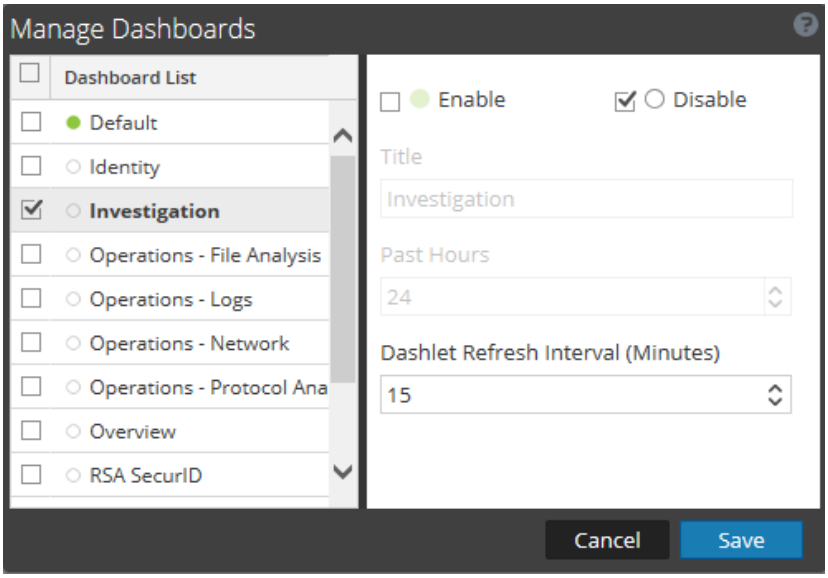
Deaktivieren eines Dashboards

So deaktivieren Sie ein oder mehrere Dashboard(s):

1. Navigieren Sie zu dem Dashboard, das deaktiviert werden soll.
2. Klicken Sie in der Dashboardsymbolleiste auf  .

3. Wählen Sie die Option **Dashboard managen** aus.

   Das Dialogfeld „Dashboards managen“ wird angezeigt.



4. Wählen Sie aus der Dashboardliste das bzw. die zu deaktivierende(n) Dashboard(s) aus.
5. Aktivieren Sie das Kontrollkästchen **Deaktivieren**.
6. Klicken Sie auf **Speichern**.

Einstellen eines Dashboards als Favoriten

Sie können zum Anpassen der Ansichten in NetWitness Suite ein vorkonfiguriertes oder benutzerdefiniertes Dashboard als Favoriten festlegen. Das NetWitness Suite-Dashboard stellt, wie der Name schon vermuten lässt, alle NetWitness Suite-Dashlets bereit. Das Dialogfeld „Favorit“ legt ein spezifisches Dashboard als Ihr bevorzugtes Dashboard fest. Jedes Mal, wenn Sie sich bei NetWitness Suite anmelden, wird dieses Dashboard als Favorit aufgeführt.

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

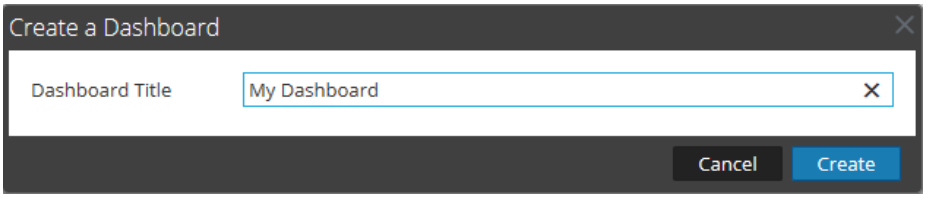
   Wenn das bevorzugte Symbol in der Farbe Rot angezeigt wird, bedeutet dies, dass das ausgewählte Dashboard als Favorit festgelegt und oberhalb der Zeile aufgeführt wird.

Erstellen von benutzerdefinierten Dashboards

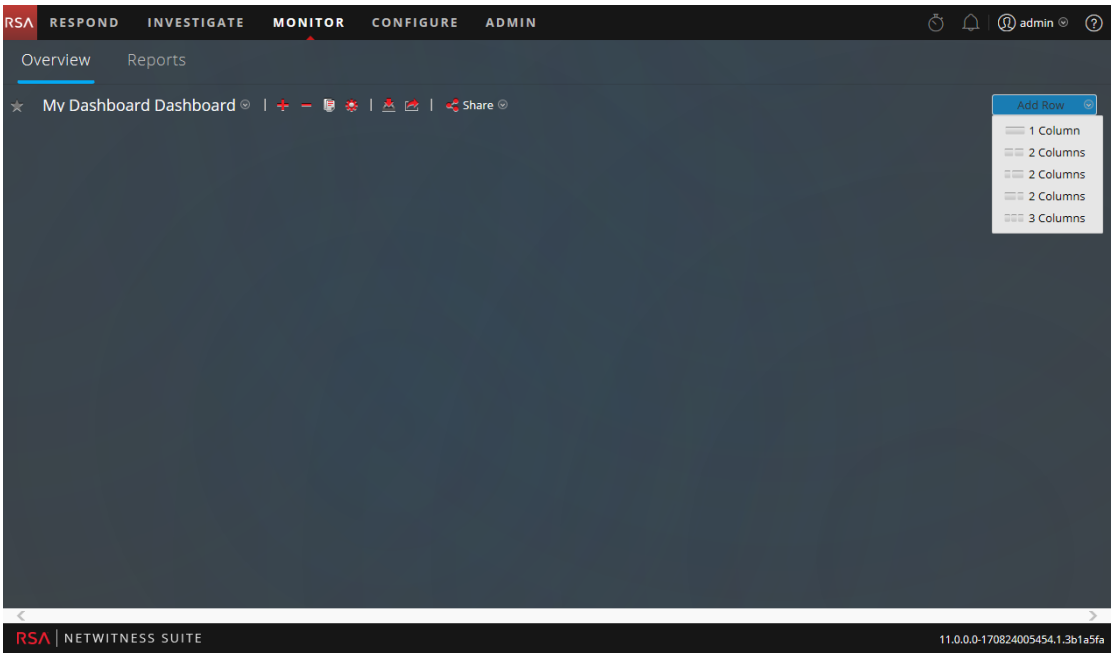
Sie können ein Dashboard für einen bestimmten Zweck anpassen, zum Beispiel, um einen bestimmten geografischen oder funktionalen Bereich des Netzwerks darzustellen. Jedes definierte Dashboard wird der Dashboardauswahlliste hinzugefügt.

So erstellen Sie ein angepassten Dashboard:

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



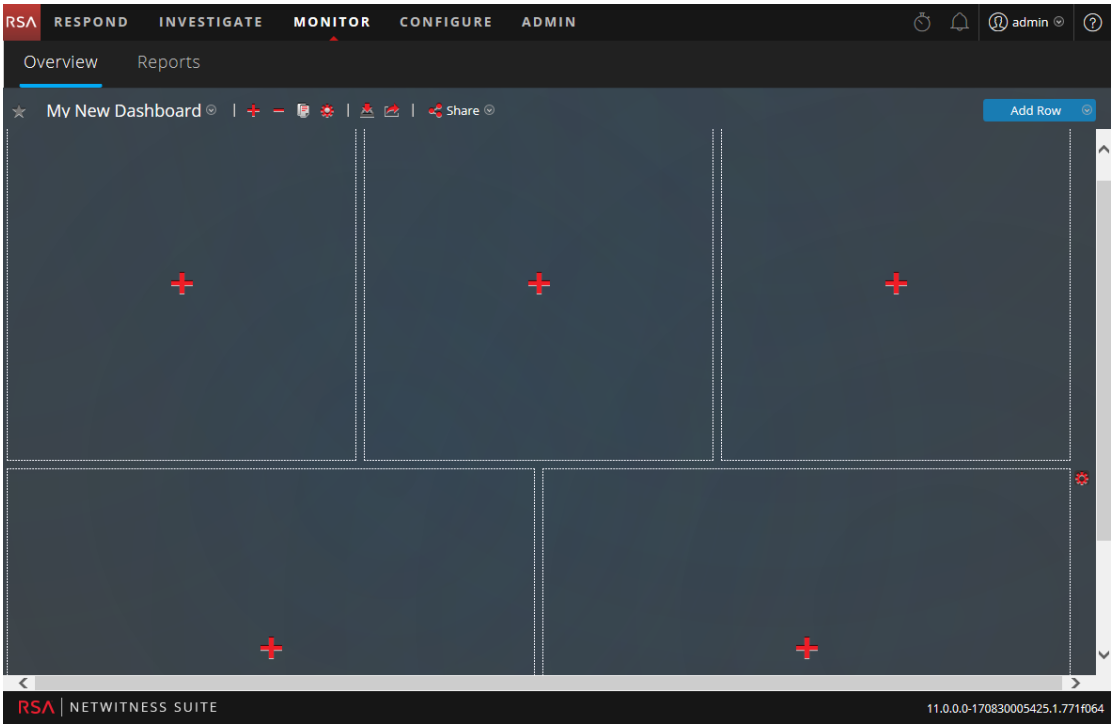
2. Geben Sie einen Titel für das neue Dashboard ein und klicken Sie auf **Erstellen**.
   Das neue Dashboard wird als leerer Bildschirm angezeigt.



3. Fügen Sie mit dem Steuerelement **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 auf das  in einem leeren Platzhalter in einer Zeile 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 Dashboardauswahlliste auswählen.
- benutzerdefinierte Dashboards löschen.
- ein Dashboard importieren oder exportieren.

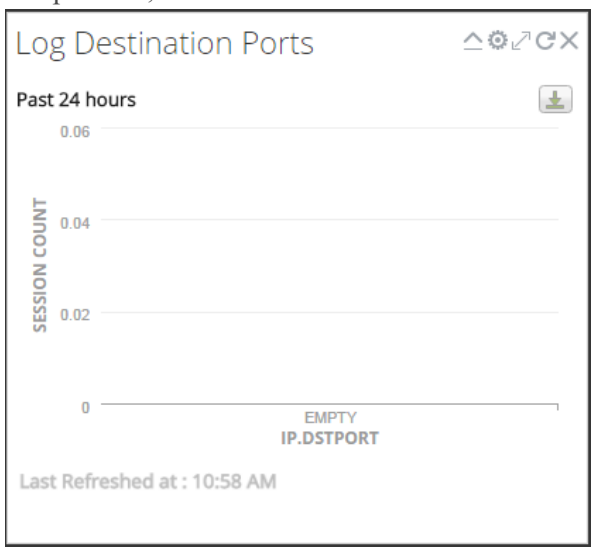
Jedes Dashboard verfügt über:

- die Dashboard-Symbolleiste
- einen Dashboard-Titel und die Dashboard-Auswahlliste
- 0 oder mehrere Dashlets

Arbeiten mit Dashlets

NetWitness Suite 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.

Symbol	Name	Beschreibung
	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. **Hinweis:** Diese Funktion ist nur verfügbar für das Echtzeitdiagramm-Dashlet und die vorkonfigurierten Dashboards im NetWitness Suite 11.0 oder höher.

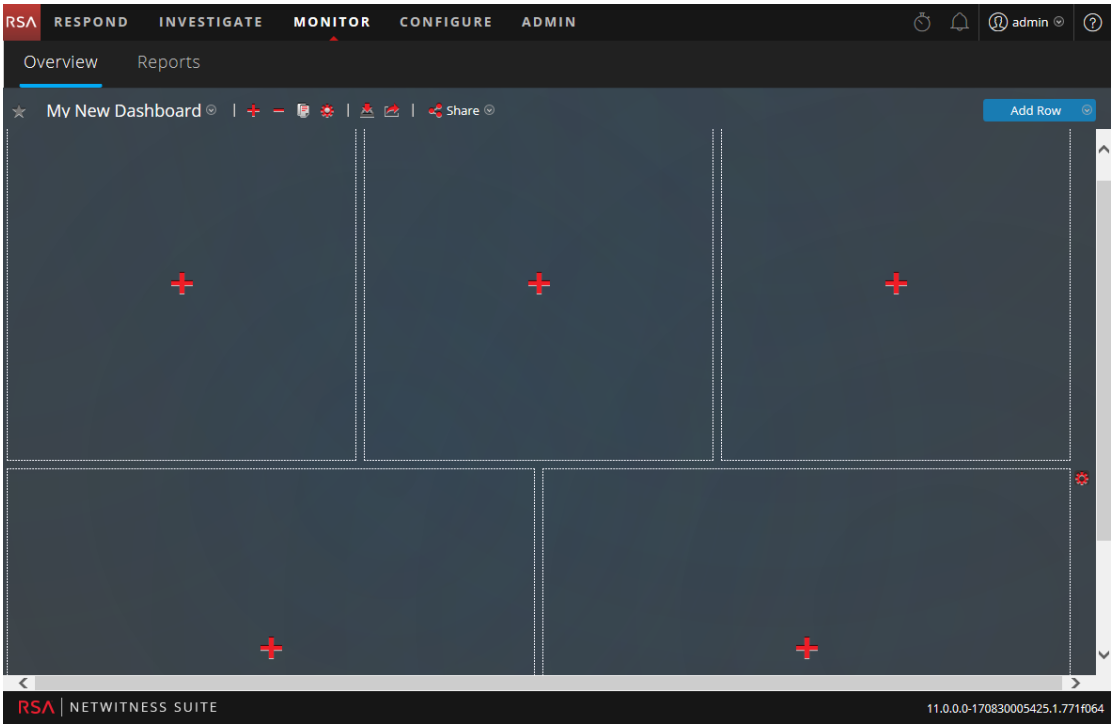
Sie können dem Standard-Dashboard Dashlets hinzufügen oder ein benutzerdefiniertes Dashboard mit Ihrem eigenen nützlichen Satz Dashlets erstellen, um Ihren Workflow effizienter zu gestalten.

Dashlet hinzufügen

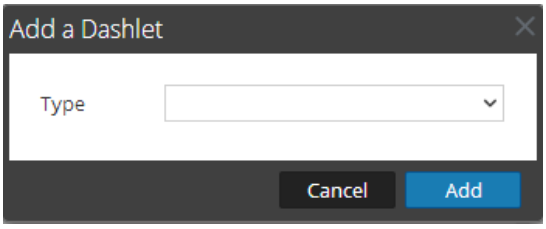
Zum Anpassen der Ansichten in NetWitness Suite können Sie im Standarddashboard Dashlets hinzufügen oder benutzerdefinierte Dashboards erstellen. Sie können vorkonfigurierten Dashboards jedoch keine Dashlets hinzufügen.

So fügen Sie ein Dashlet hinzu:

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

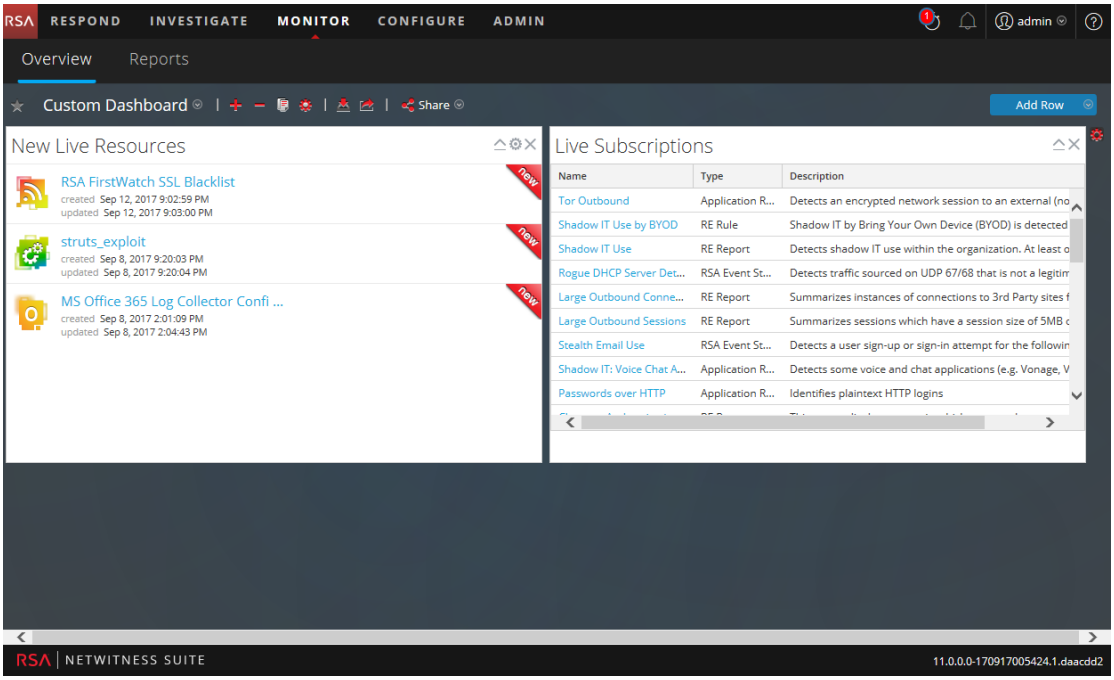


2. Klicken Sie auf  auf dem Platzhalter, an dem Sie das Dashlet hinzufügen möchten.
   Das Dialogfeld „Dashlet hinzufügen“ wird angezeigt.



3. Klicken Sie auf die Dashlet-Auswahlliste **Typ**, um die verfügbaren Dashlets anzuzeigen, und wählen Sie den Typ des Dashlet 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 Benutzer 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.

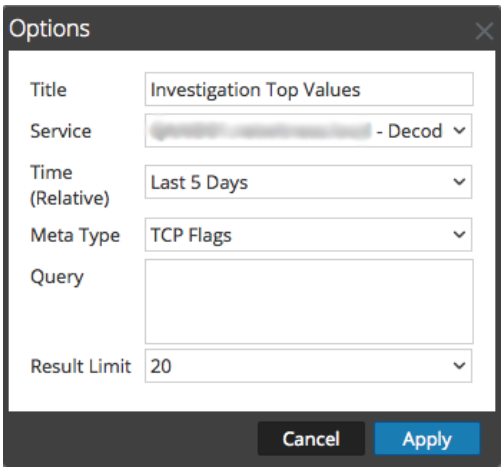
Wenn ein Dashlet keine bearbeitbaren Eigenschaften hat, z. B. das Dashlet „Live-Abonnements“, wird die Einstellungsoption nicht in der Titelleiste angezeigt. Viele Dashlets haben einen bearbeitbaren Titel, in dem Sie die folgenden Eigenschaften bearbeiten können:

- 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 ( ).

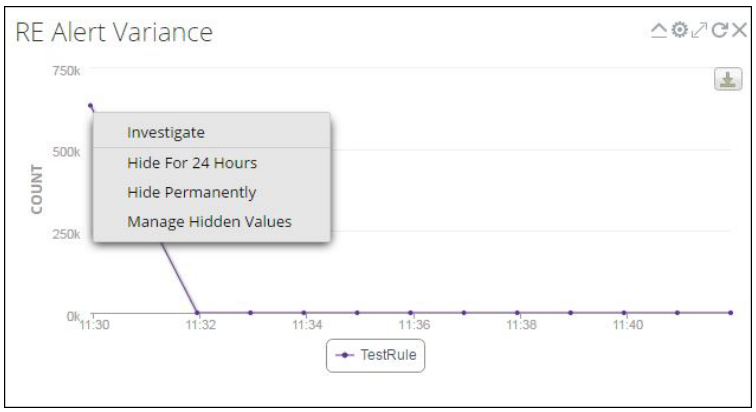
   Das Dialogfeld **Optionen** wird angezeigt.



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**.

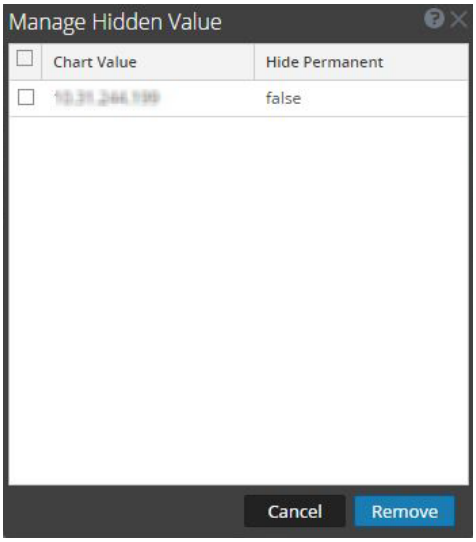
Einige Dashlets enthalten Konfigurationsoptionen, mit denen Sie die Darstellung oder den Inhalt des Dashlet anpassen können. Die folgenden Optionen stehen durch Linksklick für die Top-RE-Warnmeldungen, RE-Warnmeldungsvarianz und RE-Echtzeitdiagramm-Dashlets zur Verfügung:

- **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 auf dem 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.



Hinweis: 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 Benutzern 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 Benutzer dasselbe Übersichtsdashboard aufruft, wird der Wert weiterhin angezeigt. Dasselbe gilt für ein benutzerdefiniertes Dashboard. Wenn Sie einen Wert im benutzerdefinierten Dashboard ausblenden und dasselbe Dashboard für einen anderen Benutzer freigeben, werden die Werte weiterhin angezeigt werden, obwohl das Dashboard freigegeben ist.

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

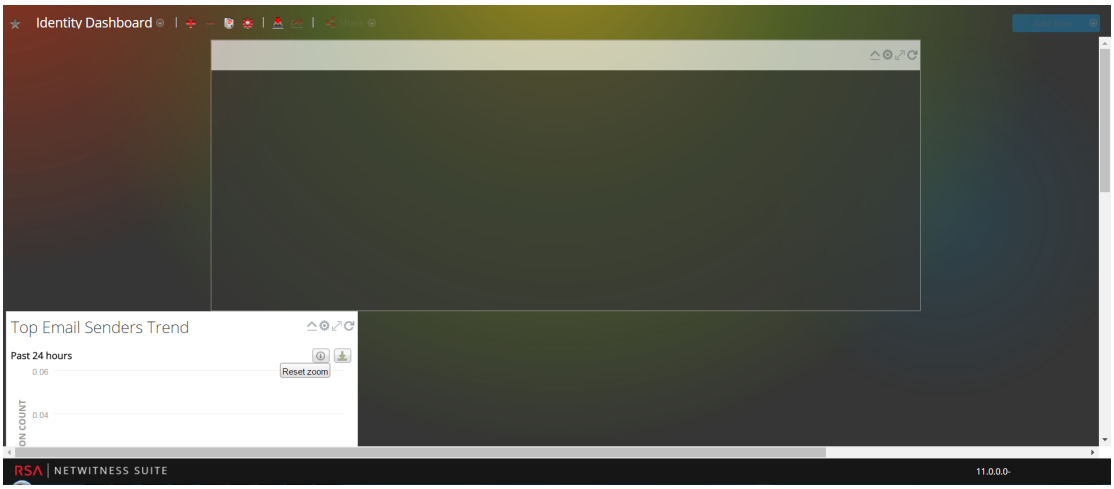
Neuanordnung eines Dashlet

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.



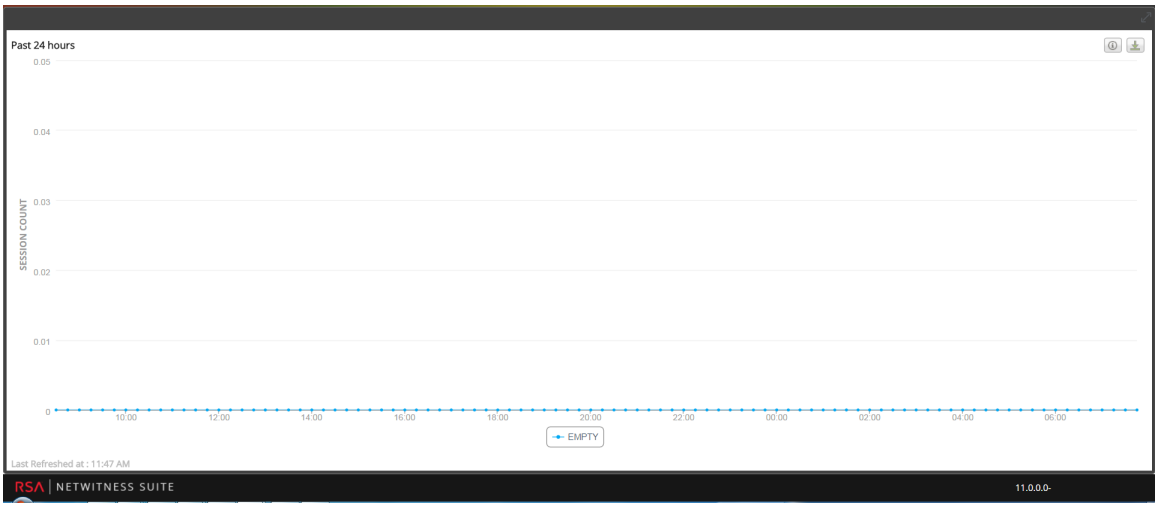
3. Lassen Sie die Maustaste los, wenn sich das Dashlet an der gewünschten Position befindet.
   Das Dashlet, das sich zurzeit an dieser Position befindet, wird nach unten verschoben.

Maximieren eines einzelnen Dashlets

In diesem Abschnitt wird erläutert, wie Sie ein Dashlet im gesamten Bereich des Hauptdashboards in NetWitness Suite mit demselben Dashlet-Titel öffnen. 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.

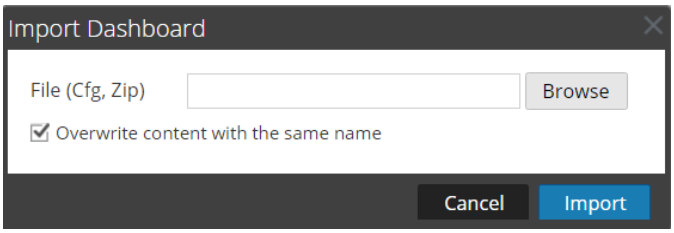
Importieren und Exportieren von Dashboards

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 Suite importieren.

Importieren eines Dashboard

1. Wählen Sie in der Dashboardsymbolleiste **Dashboard importieren** aus.

   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 **Dashboard importieren**.
   Das Dashboard wird in NetWitness Suite angezeigt

Hinweis: Wenn Sie ein Dashboard aus Security Analytics 10.6.x in NetWitness Suite11.x importieren, müssen das Dashboard und die zugehörigen Regeln und Diagramme separat importiert werden. Wenn Sie jedoch ein Dashboard von NetWitness Suite11.x in NetWitness Suite importieren, werden das Dashboard und alle 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 Suite-Instanz funktionieren. Es ist auch möglich, Ihre benutzerdefinierten Dashboards für andere Benutzer 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.

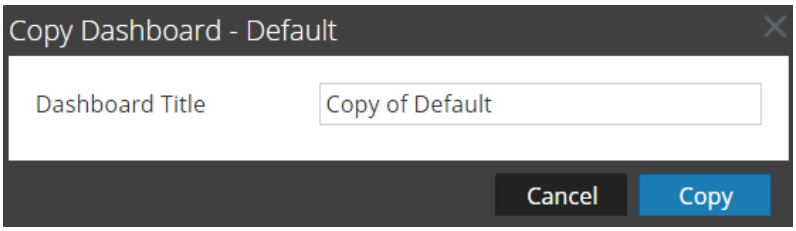
Kopieren eines Dashboards

Zum Anpassen der Ansichten in NetWitness Suite können Sie Dashboards in das NetWitness-Dashboard oder ein benutzerdefiniertes Dashboard kopieren. Das NetWitness Suite-Dashboard stellt, wie der Name schon vermuten lässt, alle NetWitness Suite-Dashlets bereit. Das Dialogfeld „Dashboard kopieren“ erstellt ein Duplikat des Dashboards, das angepasst werden kann. Wenn Sie ein Dashboard kopieren, enthält der Standardname das Präfix „Kopie von“. Beispielsweise wird der Standardtitel des kopierten Dashboards „Kopie von XYZ“ lauten, wenn der Name des ursprünglichen Dashboards „XYZ“ ist.

So kopieren Sie ein Dashboard:

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

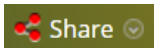
   Das Dialogfeld „Dashboard kopieren – Standard“ wird angezeigt. Der folgende Screenshot ist ein Beispiel für das Kopieren eines Dashboards.



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

Freigeben eines Dashboards

In NetWitness Suite können Sie als Administrator Dashboards zum Anzeigen mit anderen Rollen, wie Administrator, Analyst, Operator usw., freigeben. Wenn Sie ein Dashlet freigeben, können die Benutzer das Dashboard 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 NetWitness Suite Aufgaben, nach Bedarf oder geplant, die einige Minuten erfordern. Das NetWitness Suite-Jobsystem erlaubt Ihnen, eine Aufgabe mit langer Laufzeit zu beginnen und fortzufahren, andere Teile von NetWitness Suite 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 Suite arbeiten, können Sie über die NetWitness Suite-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.

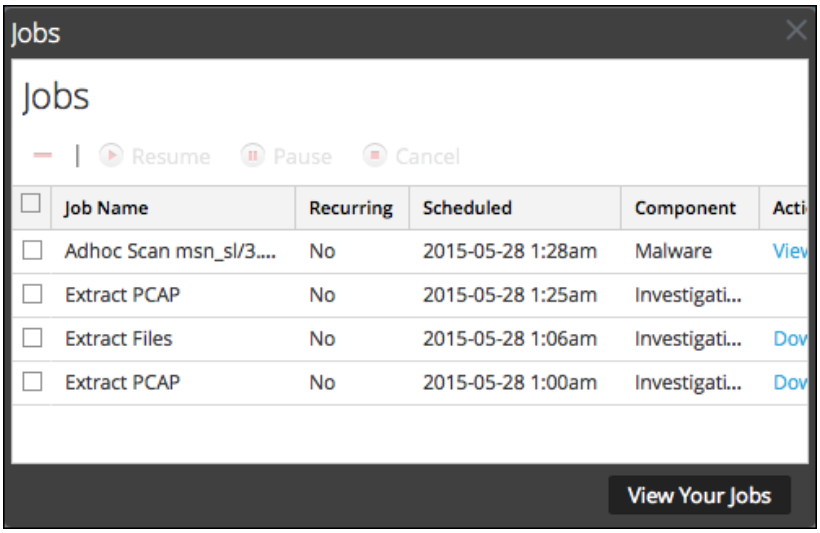
- In der Ansicht Profil finden Sie dieselben Jobs in einem vollständigen Bereich. Dies sind nur Ihre Jobs.
- In der Ansicht System können Benutzer mit Administratorrechten alle Jobs für alle Benutzer in einem einzigen Jobfenster anzeigen und managen.

Der Aufbau des Jobfensters ist in allen Ansichten identisch.

Anzeigen der Jobkurzübersicht

Klicken Sie in der NetWitness Suite-Symbolleiste auf das Symbol „Jobs“:  .

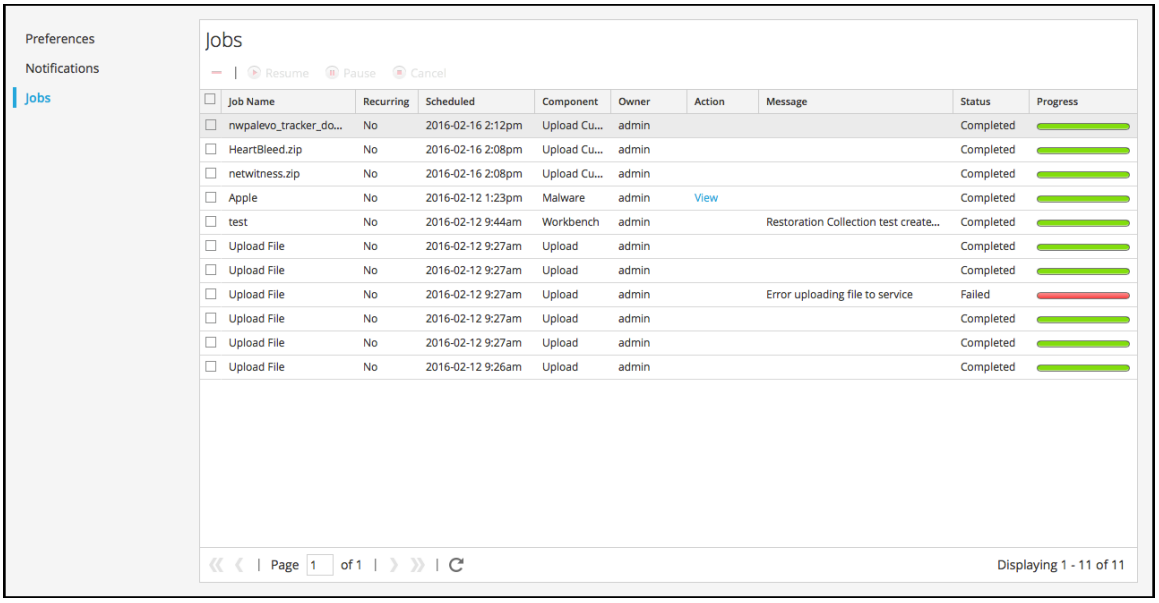
Die Jobkurzübersicht wird angezeigt.



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“ in der Ansicht „Profil“ gleich. In der Ansicht Administration > System enthält der Bereich Jobs Informationen über alle NetWitness Suite-Jobs für alle Benutzer.

Anzeigen Ihrer Jobs im Bereich der Ansicht Profil > Jobs

Klicken Sie zum Anzeigen einer umfassenderen Ansicht Ihrer Jobs auf **Ihre Jobs anzeigen**. Der Bereich „Jobs“ in der Ansicht „Profil“ 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 **Jobfenster** aus und klicken Sie auf **Anhalten**.

   Die nächste Ausführung des Jobs wird übersprungen und die Planung wird angehalten, bis Sie auf Fortsetzen klicken.

2. Um die Ausführung angehaltener 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** im Raster.

   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 der Job umgehend aus dem Raster gelöscht. Es wird kein Bestätigungsdialogfeld angezeigt. Wenn Sie einen wiederkehrenden Job löschen, werden alle künftigen Ausführungen ebenfalls gelöscht.

Benutzer können ihre eigenen Jobs vor, während oder nach der Ausführung löschen. Benutzer mit der Rolle ADMIN können einen beliebigen Job löschen. So löschen Sie Jobs:

1. Wählen Sie einen oder mehrere Jobs aus.
2. Klicken Sie auf **Delete**.
3. Die Jobs werden aus dem Raster gelöscht.

Herunterladen eines Jobs

Wenn ein Job den Status Download in der Spalte Aktion aufweist, können Sie das Ergebnis des Jobs herunterladen. Wenn Sie im Modul Investigation arbeiten und die Paketdaten für eine Sitzung als PCAP-Datei entpacken oder die Nutzlastdateien (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 NetWitness Suite arbeiten, können Sie aktuelle Systembenachrichtigungen einsehen, ohne das Modul zu verlassen, in dem Sie arbeiten. Sie können eine kurze Übersicht der Benachrichtigungen in der NetWitness Suite-Symbolleiste öffnen. Sie können diese jederzeit einsehen. Bei Empfang einer neuen Benachrichtigung wird das Benachrichtigungssymbol angezeigt.

Beispiele für Benachrichtigungen sind:

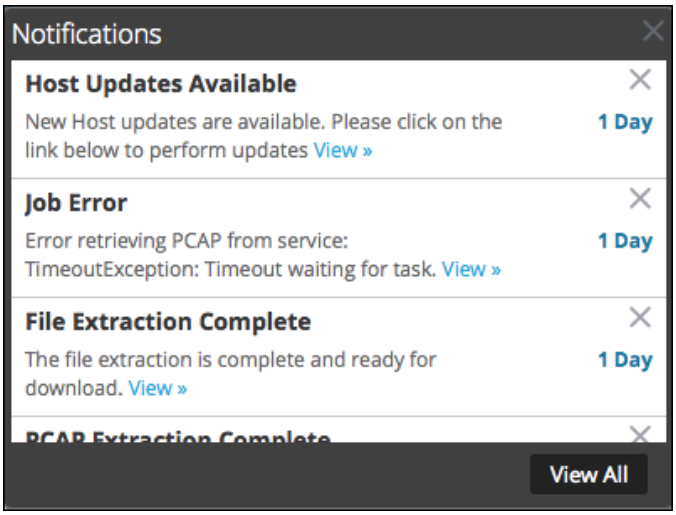
- Ein Upgrade eines Hosts wurde abgeschlossen.
- Ein Parser-Push zu den Decoders wurde abgeschlossen.
- Es ist eine neuere Softwareversion verfügbar.

Sie können alle Benachrichtigungen in einem vollständigen Benachrichtigungsbereich in den folgenden zwei Ansichten anzeigen.

- In der Ansicht „Profil“ werden nur Ihre Benachrichtigungen angezeigt.
- In der Ansicht „System“ können Benutzer mit Administratorrechten alle Benachrichtigungen für alle Benutzer in einem einzigen Bereich anzeigen und managen.

Benachrichtigungen anzeigen

Klicken Sie auf das Symbol „Benachrichtigungen“ (), um den Benachrichtigungsbereich anzuzeigen.

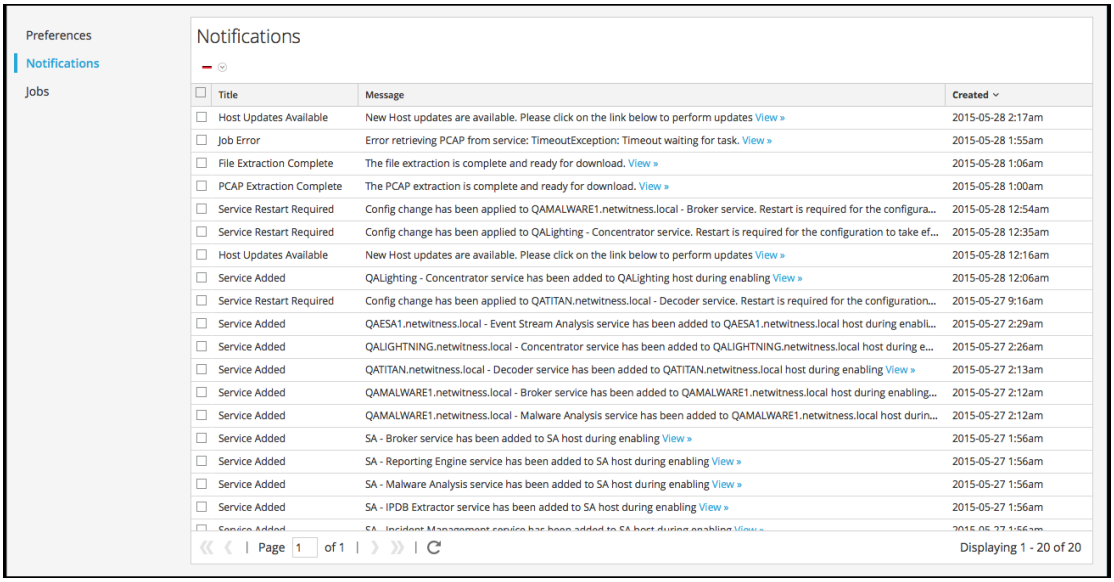


Alle Benachrichtigungen anzeigen

Gehen Sie wie folgt vor, um alle Benachrichtigungen anzuzeigen:

1. Navigieren Sie zu **Profil** und wählen Sie dann im Bereich „Optionen“ der Ansicht „Profil“ die Option **Benachrichtigungen** aus.
2. Navigieren Sie zu **ADMIN > System** und wählen Sie im Bereich „Optionen“ der Ansicht „System“ die Option **Benachrichtigungen** aus.
3. Klicken Sie auf  , um den Benachrichtigungsbereich zu öffnen, und klicken Sie dann im Benachrichtigungsbereich auf **Alle anzeigen**.

   Der Bereich „Benachrichtigungen“ wird angezeigt. Hier werden alle Benachrichtigungen angezeigt und das Format unterscheidet sich von dem Format des Benachrichtigungsbereichs.



Löschen von Benachrichtigungsdatensätzen

So löschen Sie Benachrichtigungsdatensätze:

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

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

Anzeigen der Hilfe in der Anwendung

Es gibt verschiedene Möglichkeiten, bei der Verwendung von NetWitness Suite Hilfe zu erhalten. Sie können die Inlinehilfe, die Kurzinformationen und Onlinehilfelinks verwenden.

Anzeigen der Inlinehilfe

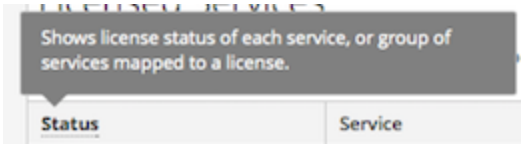
Die Inlinehilfe bietet zusätzliche Informationen darüber, was in Abschnitten oder Feldern zu tun ist, die derzeit in der NetWitness Suite-Benutzeroberfläche angezeigt werden. Bewegen Sie den Mauszeiger zum Anzeigen der Inlinehilfe auf . In der Inlinehilfe wird eine kurze Beschreibung des Elements angezeigt.

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:

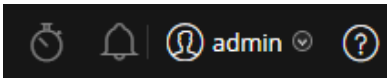


Anzeigen der Onlinehilfe

Onlinehilfelinks führen Sie aus NetWitness Suite heraus zur RSA Link-Onlinedokumentation. Diese Website bietet eine vollständige Dokumentation für NetWitness Suite 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 Teil der Benutzeroberfläche auf  in der NetWitness Suite-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 Suite-Symbolleiste gezeigt.



Suchen nach Dokumenten auf RSA Link

Die RSA NetWitness® Suite-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 Suite-Dokumentation

Die Dokumentation von NetWitness Suite Logs and Packets finden Sie unter folgendem Link: https://community.rsa.com/docs/DOC-40370

So navigieren Sie zur Dokumentation von NetWitness Suite Logs and Packets:

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS SUITE**.
2. Klicken Sie auf der Seite RSA NetWitness Suite auf **DOKUMENTATION** und wählen Sie **RSA NETWITNESS LOGS AND PACKETS** 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 SUITE**.
2. Klicken Sie auf der Seite RSA NetWitness Suite auf **DOKUMENTATION** 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 SUITE**.
2. Klicken Sie auf der Seite RSA NetWitness Suite auf **DOKUMENTATION** und wählen Sie **WEITERE RESSOURCEN** > **RSA-INHALT** 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 SUITE**.
2. Klicken Sie auf der Seite RSA NetWitness Suite auf **DOKUMENTATION** und wählen Sie **WEITERE RESSOURCEN** > **EREIGNISQUELLENKONFIGURATION** 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 SUITE**.
2. Klicken Sie auf der Seite RSA NetWitness Suite auf **DOKUMENTATION** und wählen Sie **WEITERE RESSOURCEN** > **HARDWAREKONFIGURATIONSLEITFÄDEN** aus.

Suchen nach Dokumenten mit dem NetWitness-Navigator

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

1. Klicken Sie auf der Startseite von RSA Link (https://community.rsa.com) auf **RSA NETWITNESS SUITE**.
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.

Erste Schritte mit NetWitness Suite – Referenzen

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

- Benutzereinstellungen
- Bereich „Benachrichtigungen“ und Benachrichtigungsbereich
- Bereich „Jobs“ und Jobkurzübersicht

Benutzereinstellungen

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

- Festlegen der Zeitzone der Anwendung
- Festlegen des Datums- und Uhrzeitformats
- Auswählen der standardmäßigen Startansicht für NetWitness Suite
- 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 Benutzereinstellungen, die über die Hauptmenüleiste aufgerufen werden können:

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

Was möchten Sie tun?

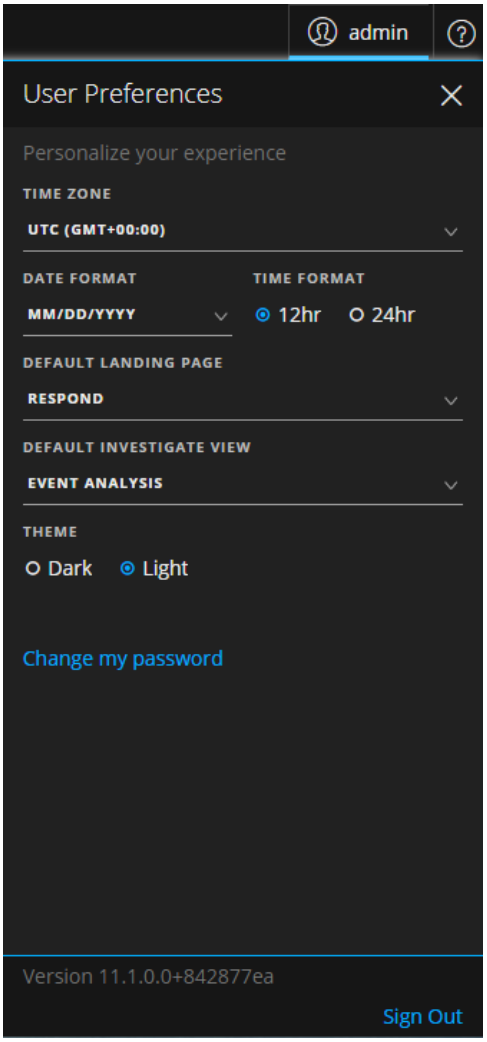
Rolle	Ziel	Details anzeigen
Alle	eigenes Passwort ändern	Eigenes Passwort ändern
Alle	Meine standardmäßige Landingpage auswählen	Einrichten einer Standardansicht nach SOC-Rolle
Alle	Meine Benutzereinstellungen festlegen	Festlegen von Benutzereinstellungen

Verwandte Themen

- Grundlagen der Navigation in NetWitness Suite

Benutzereinstellungen (Ansicht „Reagieren“ und einige „Untersuchen“-Ansichten)

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



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

Option	Beschreibung
Zeitzone	Legt die Zeitzone für die Verwendung in NetWitness Suite 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 Suite die Auswahl einer Standardansicht. Sie können entsprechend Ihrer Benutzerrolle „Reagieren“, „Investigate“, „Überwachen“, „Konfigurieren“ und „Admin“ auswählen. Beispielsweise können Sie „Reagieren“ auswählen, um direkt zum entsprechenden Abschnitt der Anwendung für Incident-Experten zu wechseln. Diese Auswahl legt die Standardansicht für die gesamte Anwendung fest.
Standardmäßige Ansicht „Untersuchen“	(Diese Option gilt für NetWitness Suite 11.1 oder höher.) Wählen Sie die standardmäßige Landingpage für die Ansicht „Untersuchen“ aus. Sie können die Ansichten „Navigation“, „Ereignisse“, „Ereignisanalyse“, „Hosts“, „Dateien“ oder „Malware Analysis“ als standardmäßige Ansicht „Untersuchen“ wählen. Beispielsweise können Sie „Ereignisse“ als standardmäßige Ansicht „Untersuchen“ wählen, um direkt zu „Ereignisse“ zu gehen und die für einen Service generierten Ereignisse anzuzeigen.

Option	Beschreibung
Design	(Diese Option gilt für NetWitness Suite 11.1 und höher.) Ändert die Darstellung der Ansicht „Reagieren“ und einige Untersuchen-Ansichten, die in der Anwendung angezeigt werden. Sie können helle oder dunkle Designs auswählen. • **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. Ihre Auswahl wirkt sich nur darauf aus, wie NetWitness Suite für Sie dargestellt wird, nicht auf die Darstellung für andere Benutzer.
Eigenes Passwort ändern	Öffnet das Dialogfeld „Einstellungen“, in dem Sie Ihr Passwort ändern können.
Version	Zeigt die NetWitness Suite-Version an.
Abmelden	Ermöglicht es Ihnen, sich von NetWitness Suite abzumelden.

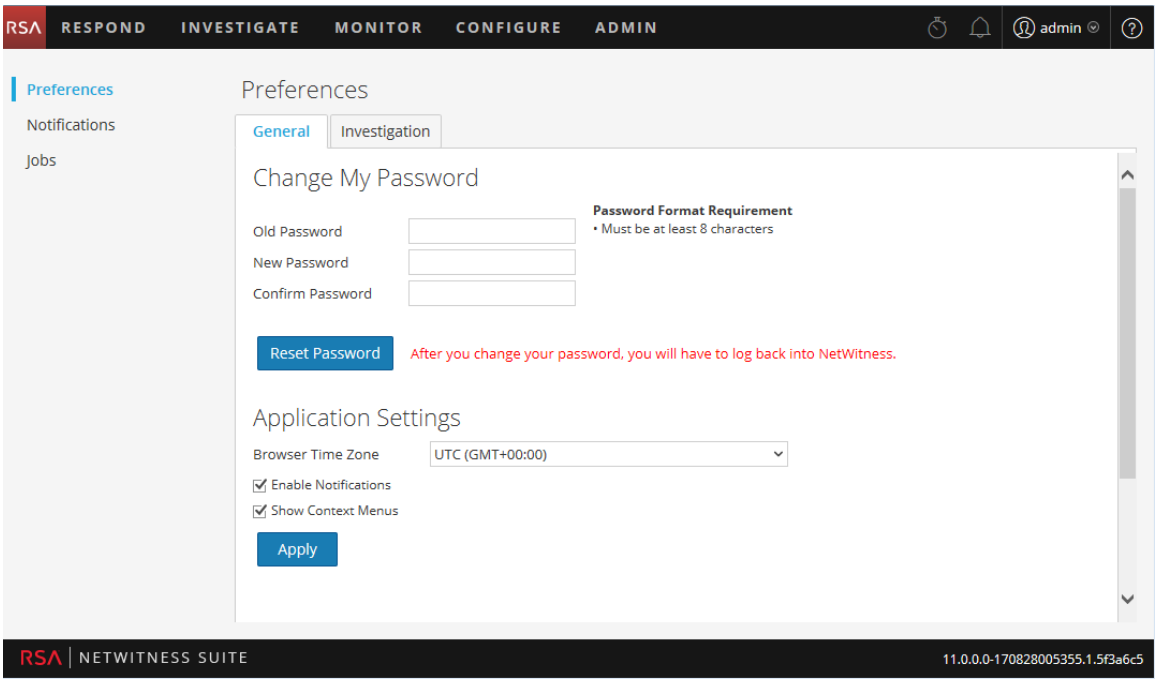
Die von Ihnen vorgenommenen Einstellungen werden sofort wirksam.

Einstellungen

Um auf weitere globale Benutzereinstellungen 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 und Dateien)  und klicken Sie im Dialogfeld „Benutzereinstellungen“ 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 Suite-Passwort, wie z B. minimale Passwortlänge und minimale Anzahl von Großbuchstaben, Kleinbuchstaben, Dezimalstellen, nicht lateinische 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 Suite verwenden.
Neues Passwort	Geben Sie das Passwort ein, das Sie für die nächste Anmeldung verwenden möchten.
Passwort bestätigen	Geben Sie das neue Passwort erneut ein.

Option	Beschreibung
Passwort zurücksetzen	Aktualisiert Ihr Benutzerprofil mit dem neuen Passwort. Sie werden von NetWitness Suite abgemeldet, damit die Änderungen wirksam werden. Das neue Passwort wird bei der nächsten Anmeldung bei NetWitness Suite wirksam. Die Passwortänderung wird für Ihre Systemanmeldung und für alle NetWitness Suite-Services angewendet, zu denen Ihr Konto hinzugefügt wurde.

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

Anwendungseinstellungen

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

Option	Beschreibung
Browserzeitzone	Legt die Zeitzone für die Verwendung in NetWitness Suite fest. Ihre Zeitzoneneinstellung wird auf der Symbolleiste angezeigt.
Benachrichtigungen aktivieren	Mit diesem Kontrollkästchen werden Benachrichtigungen für Ihr Benutzerkonto aktiviert und deaktiviert. Die NetWitness Suite-Systembenachrichtigungen werden bei der Erstellung eines neuen Benutzerkontos standardmäßig aktiviert.
Aktivieren von Kontextmenüs	Mit diesem Kontrollkästchen werden Kontextmenüs für Ihr Benutzerkonto aktiviert und deaktiviert. Bei der Erstellung eines neuen Benutzerkontos sind 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

NetWitness Suite stellt Systembenachrichtigungen bereit, um Benutzer 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 Suite arbeiten, können Sie aktuelle Systembenachrichtigungen einsehen, ohne das Modul zu verlassen, in dem Sie arbeiten. Sie können eine kurze Übersicht der Benachrichtigungen in der NetWitness Suite-Symbolleiste öffnen. Sie können diese jederzeit einsehen. Bei Empfang einer neuen Benachrichtigung wird das Benachrichtigungssymbol angezeigt.

Wenn Sie Benachrichtigungen im Benachrichtigungsbereich anzeigen, werden nur aktuelle Benachrichtigungen angezeigt. Sie können alle Benachrichtigungen in der Profilansicht oder der Systemansicht in einem Tabellenformat anzeigen. Anleitungen für die Anzeige von Benachrichtigungen finden Sie unter Anzeigen und Löschen von Benachrichtigungen.

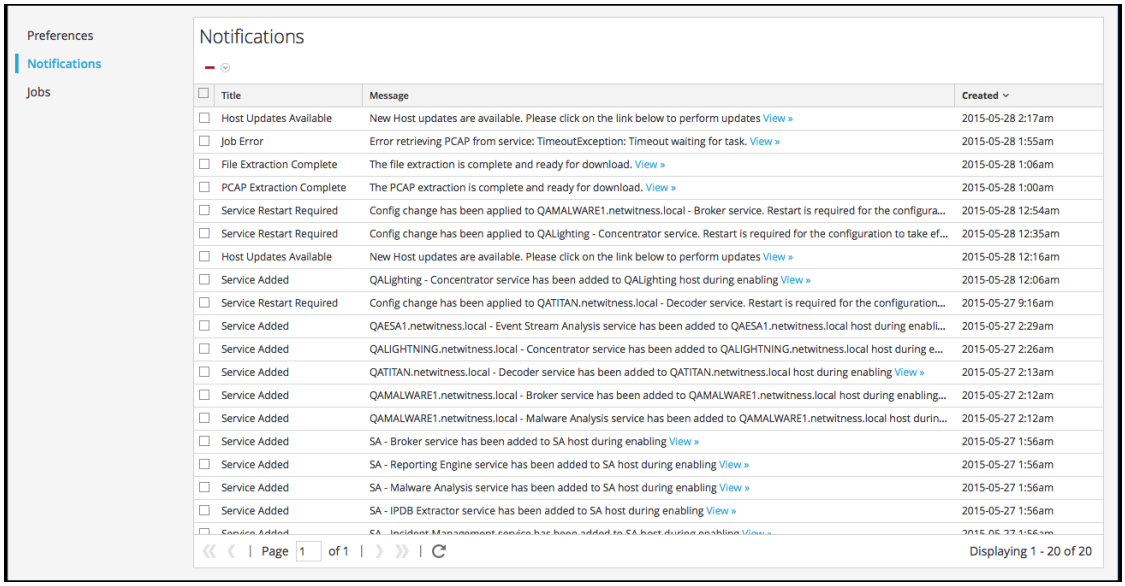
Was möchten Sie tun?

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

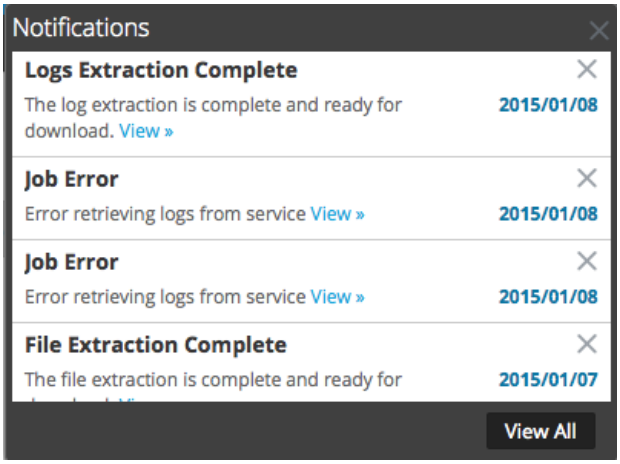
Führen Sie zum Öffnen des Bereichs „Benachrichtigungen“ eine der folgenden Aktionen aus:

- Navigieren Sie zu **Profil** und wählen Sie im Bereich „Optionen“ der Ansicht „Profil“ die Option **Benachrichtigungen** aus.

- Navigieren Sie zu **ADMIN > System** und wählen Sie im Bereich „Optionen“ der Ansicht „System“ die Option **Benachrichtigungen** aus.



- Klicken Sie auf  und klicken Sie dann im Benachrichtigungsbereich auf **Alle anzeigen**.



Der Bereich „Benachrichtigungen“ verfügt über eine Symbolleiste und eine Tabelle. Der Benachrichtigungsbereich ist eine Teilmenge der Informationen im Bereich „Benachrichtigungen“. In der folgenden Tabelle werden die Funktionen des Benachrichtigungsbereichs beschrieben.

Funktion	Beschreibung
	Zeigt ein Drop-down-Menü an, in dem Sie die ausgewählten Benachrichtigungsdatensätze oder sämtliche Benachrichtigungsdatensätze in der Tabelle **Benachrichtigungen** und im Bereich „Benachrichtigungen“ löschen können.
Titel	Der Titel der Benachrichtigung, z. B. **Dateiextraktion abgeschlossen**.
Meldung	Die gesamte Meldung, z. B. **Die Dateiextraktion ist abgeschlossen und zum Download bereit**.
Ansicht	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. Im Benachrichtigungsbereich ist dies die Spalte, die die Anzahl der Tage seit Erstellung der Benachrichtigung enthält.
Alle anzeigen	Zeigt die Tabelle „Benachrichtigungen“ in der Profilansicht an.

Bereich „Jobs“ und Jobkurzübersicht

Jobs werden von unterschiedlichen NetWitness Suite-Modulen gestartet. Das Live-Modul kann z. B. CMS-Ressourcen herunterladen, das Modul „Administration“ kann einen Feed zu einem Service hochladen und das Modul „Investigation“ kann Pakete in Paketerfassungsdateien analysieren und rekonstruieren.

In der Ansicht „Administration > System“ können Benutzer in der Gruppe ADMIN alle NetWitness Suite-Jobs im Bereich „Jobs“ managen. Andere Nicht-Administrator-Benutzer können ihre eigenen Jobs in der Profilansicht anzeigen.

Während Sie in NetWitness Suite arbeiten, können Sie über die NetWitness Suite-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

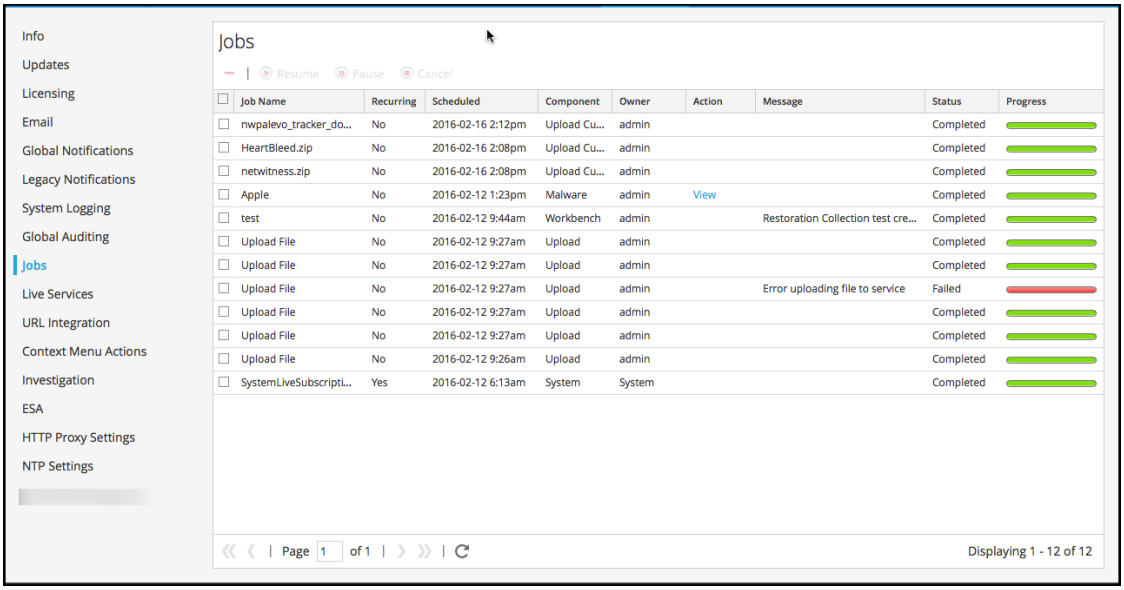
Der Aufbau des Jobfensters ist in allen Ansichten identisch.

Was möchten Sie tun?

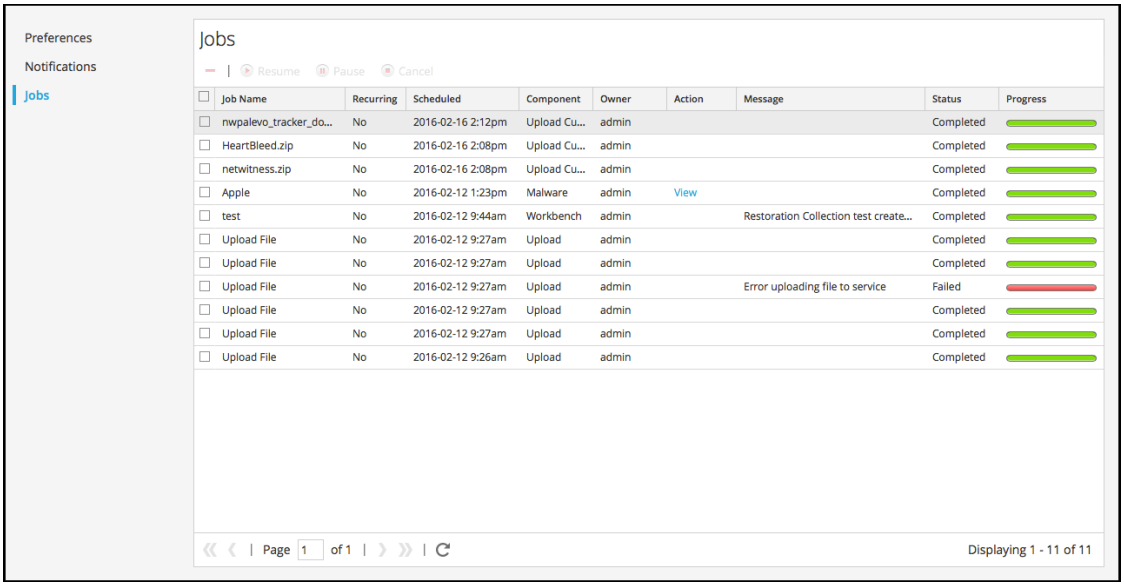
Rolle	Ziel	Details anzeigen
Alle	einen geplanten Job anhalten und fortsetzen	Managen von Jobs
Alle	einen Job abbrechen oder löschen	Managen von Jobs
	einen Job herunterladen	Managen von Jobs

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

- Navigieren Sie zu **ADMIN > System** und wählen Sie im Bereich „Optionen“ **Jobs** aus.

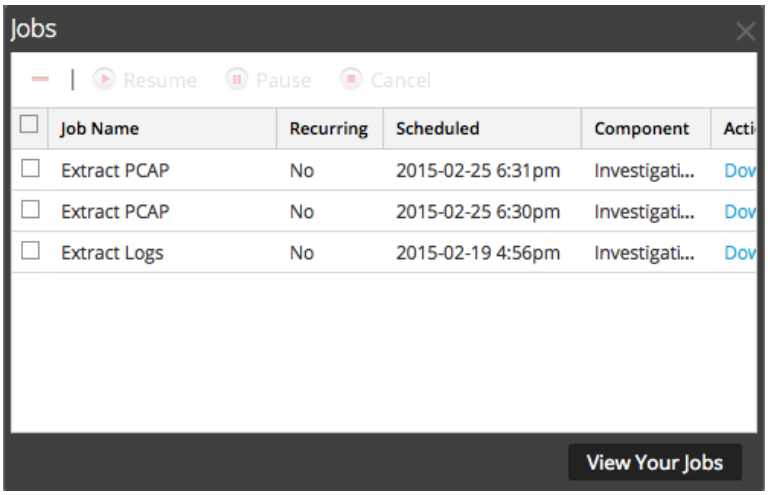


- Navigieren Sie zu **Profil** und wählen Sie im Bereich „Optionen“ **Jobs** aus.



Im Bereich Jobs werden Informationen zu Jobs in einem Raster dargestellt. Die Spalten enthalten einen Fortschrittsbalken für den Job, den Jobnamen, eine Anzeige dazu, ob der Job wiederkehrend oder nicht wiederkehrend ist, das NetWitness Suite-Modul, das 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 die Ansicht „Profil“ > Bereich „Jobs“ gleich. In der Ansicht Administration > System enthält der Bereich Jobs Informationen über alle NetWitness Suite-Jobs für alle Benutzer.

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

Funktion	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.

Funktion	Beschreibung
	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 Funktionen der Jobkurzübersicht und des Bereichs „Jobs“ beschrieben.

Funktion	Beschreibung
Auswahlfeld	Klicken Sie in dieses Feld, um einen oder mehrere Jobs auszuwählen.
Progress	Zeigt an, wie viel Prozent des Jobs abgeschlossen sind.
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.
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 Benutzers zu sehen sind. Die Spalte kann aber hinzugefügt werden.
Status	Gibt den Status des Jobs an. Standardwerte sind **Unterbrochen**, **Wird ausgeführt**, **Abgebrochen**, **Fehlgeschlagen**, **Abgeschlossen**. Weitere Statuswerte können hinzugefügt werden.
Meldung	Zeigt zusätzliche Informationen zum Job an, z. B. **Dateien werden extrahiert** oder **Keine Sitzungen gefunden**.

Funktion	Beschreibung
Aktion	Zeigt Jobs in der Malware Analysis-Ansicht Investigation 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.
Ihre Jobs anzeigen	Zeigt Ihre Jobs unter der **Ansicht „Profil“ > Bereich „Jobs“** an.
Geplant	Gibt die geplante Startzeit und das Startdatum des Jobs an.