RSA NETWITNESS® SUITE

Systemsicherheit und Benutzerverwaltung

für Version 11.0

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

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

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

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

Februar 2018

Inhalt

Systemsicherheit und Benutzerverwaltung

Dieser Leitfaden enthält Information über die Einrichtung von Sicherheit und die Kontrolle des Benutzerzugriffs. Der Systemadministrator muss systemweite Einstellungen, Benutzerkonten, Systemrollen, Berechtigungen und den Zugriff auf Services verstehen.

Themen

Einrichten von Systemsicherheit

In diesem Thema wird eine Reihe von End-to-End-Verfahren für die Implementierung von Systemsicherheit vorgestellt. Jeder Schritt in den folgenden Themen erläutert eine systemweite Einstellung. Befolgen Sie die Schritte, um die Sicherheit in NetWitness Suite einzurichten.

Themen

Schritt 1. Konfigurieren der Passwortkomplexität

In diesem Thema wird erläutert, wie die Anforderungen für die systemweite Passowortkomplexität in NetWitness Suite festgelegt werden.

Passwörter sind ein wichtiger Bestandteil Ihrer Strategie für die Netzwerksicherheit. Sie bieten den wichtigen und ersten Schutz für Ihre Computersysteme und verhindern Angriffe und unbefugten Zugriff auf vertrauliche Informationen.

Passwortrichtlinien, die die Sicherheit des Unternehmensnetzwerks verbessern sollen, variieren je nach Branche, Anforderungen des Unternehmens und Bestimmungen. Aufgrund dieser Variationen in den Passwort-Policys können Sie in NetWitness Suite die Anforderungen für die Passwortkomplexität für interne NetWitness Suite-Benutzer konfigurieren, um sie an die Guidelines für Passwort-Policys Ihres Unternehmens anzupassen.

Die Anforderungen an die Komplexität von Passwörtern gelten ausschließlich für interne Benutzer; externe Benutzer sind davon nicht betroffen. Externe Benutzer müssen die Komplexität ihrer Passwörter anhand eigener Methoden und Systeme sicherstellen.

Neben der Angabe des Ablaufzeitraums für globale Standardeinstellungen von Benutzern können Sie festlegen, ob und wann interne Benutzer Benachrichtigungen erhalten, wenn ihre Passwörter in Kürze ablaufen. Die Benachrichtigung über den Passwortablauf wird in einer entsprechenden Meldung gesendet, wenn sich ein Benutzer bei NetWitness Suite anmeldet.

Passwortsicherheit

Sichere Passwörter machen es Angreifern schwerer, Benutzerpasswörter zu erraten, und verhindern unbefugten Zugriff auf das Netzwerk Ihres Unternehmens. Sie können eine angemessene Stufe der Passwortsicherheit für Ihre NetWitness Suite-Benutzer festlegen. Wenn Sie die Einstellungen für die Passwortsicherheit konfigurieren, gelten diese für interne NetWitness Suite-Benutzer, einschließlich der Administratorbenutzer.

Sie können eine beliebige Kombination der folgenden Anforderungen für die Passwortsicherheit erzwingen, die gelten, wenn ein NetWitness Suite-Benutzer ein Passwort erstellt oder ändert:

- Mindestkennwortlänge
- Mindestanzahl an großgeschriebenen Zeichen
- Mindestanzahl an kleingeschriebenen Zeichen
- Mindestanzahl an Dezimalstellen (0 bis 9)
- Mindestanzahl an Sonderzeichen
- Mindestanzahl an nicht lateinischen Buchstaben (inklusive Unicode-Zeichen aus asiatischen

Sprachen)

- Angabe, ob das Passwort den Benutzernamen enthalten darf oder nicht

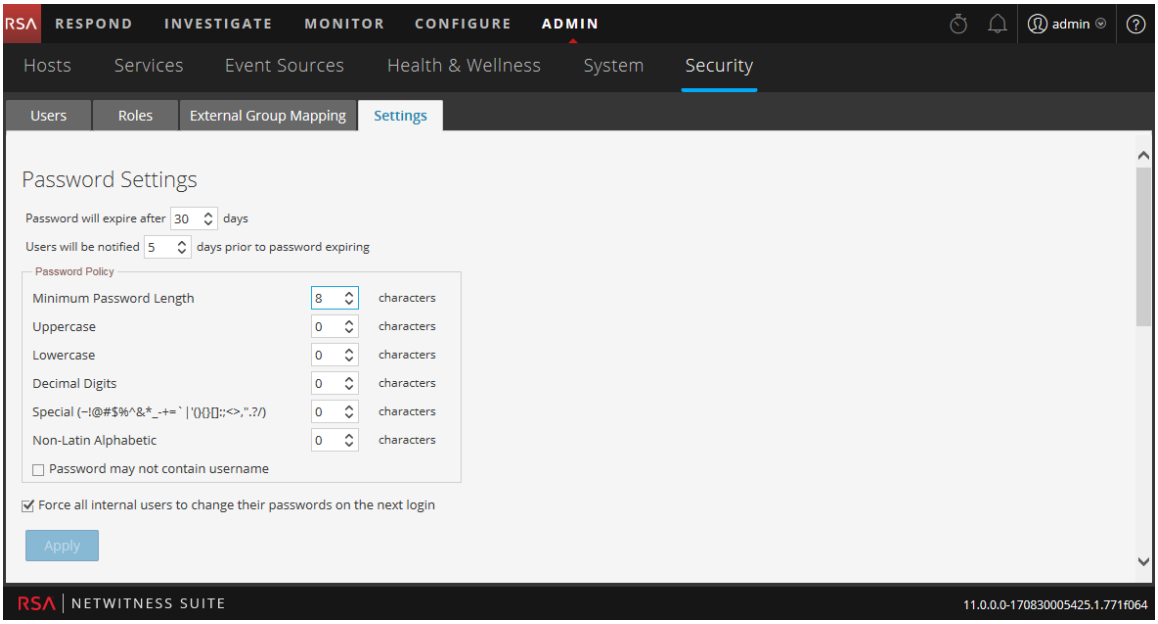
Sie können z. B. eine Anforderung für die Passwortsicherheit erstellen, bei der das Passwort mindestens 8 Zeichen sowie eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten muss und der Benutzername nicht enthalten sein darf.

Wenn Sie eine Mindestanzahl an nicht lateinischen Buchstaben erzwingen möchten, müssen Sie sicherstellen, dass diese Zeichen für die Benutzer bei der Einstellung des Passworts verfügbar sind.

Im Thema „STIG-konforme Passwörter“ im *Systemwartungsleitfaden* finden Sie ein Beispiel einer Policy für sichere Passwörter.

Konfigurieren der Passwortsicherheit

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.



3. Wählen Sie im Abschnitt **Passworteinstellungen** die Anforderungen für die Passwortkomplexität aus, die erzwungen werden sollen, wenn NetWitness Suite-Benutzer ihre Passwörter festlegen, und geben Sie gegebenenfalls die erforderliche Mindestanzahl an Zeichen an. Legen Sie den Wert für die Anforderungen, die Sie nicht erzwingen möchten, auf 0 fest, mit Ausnahme der Mindestpasswortlänge, für die mindestens 4 Zeichen erforderlich sind.

Voraussetzung	Beschreibung
Passwort läuft nach <n> Tagen ab	Die Standardanzahl der Tage, nach denen ein Passwort für alle internen NetWitness Suite-Benutzer abläuft. Beim Wert Null (0) ist der Ablauf der Passwortgültigkeit deaktiviert. Bei Neuinstallationen lautet der Standardwert 30. Für Upgrades wird der vorherige Wert automatisch auf die aktualisierte Installation migriert.
Benutzer werden <n>Tage vor Ablauf des Passworts benachrichtigt	Die Anzahl der Tage vor dem Ablaufdatum der Passwortgültigkeit, um den Benutzer zu benachrichtigen, dass sein Passwort bald abläuft Wenn Benutzer sich bei NetWitness Suite anmelden, wird das Dialogfeld „Meldung bei Passwortablauf“ angezeigt. Der Mindestwert beträgt 1 Tag.
Mindestpasswortlänge	Gibt eine Mindestlänge für das Passwort an. Durch die Angabe einer Mindestpasswortlänge wird verhindert, dass zu kurze Passwörter gewählt werden, die sich leicht erraten lassen. Die Mindestlänge eines Passworts beträgt standardmäßig 4 Zeichen.
Großbuchstaben	Gibt an, wie viele Großbuchstaben das Passwort mindestens enthalten soll. Dazu zählen die Buchstaben europäischer Sprachen von A bis Z, einschließlich diakritischer Zeichen, griechischer und kyrillischer Buchstaben. Beispiel: • Kyrillische Großbuchstaben: Д Ц • Griechische Großbuchstaben: Π Λ
Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben das Passwort mindestens enthalten soll. Dazu zählen die Buchstaben europäischer Sprachen von a bis z, einschließlich diakritischer Zeichen, griechischer und kyrillischer Buchstaben. Beispiel: • Kyrillische Kleinbuchstaben: д ц • Griechische Kleinbuchstaben: π λ
Dezimalstellen	Gibt an, wie viele Dezimalziffern (von 0 bis 9) das Passwort mindestens enthalten soll.

Voraussetzung	Beschreibung
Sonderzeichen (~!@#$%^&*_-+=`|'() {}[]:;<>,".?/)	Gibt an, wie viele Sonderzeichen das Passwort mindestens enthalten soll: ~!@#$%^&*_-+=`|'(){}[]:;<>,".?/
Zeichen aus nicht lateinischen Alphabeten	Gibt an, wie viele Unicode-Zeichen des Alphabets, die weder Groß- noch Kleinbuchstaben sind, mindestens enthalten sein sollen. Dazu zählen Unicode-Zeichen aus asiatischen Sprachen. Beispiel: • Kanji (Japanisch): 頁 (Blatt) 枒 (Baum)
Passwort darf nicht den Benutzernamen enthalten	Gibt an, dass ein Passwort nicht den Benutzernamen des Benutzers enthalten darf (ohne Berücksichtigung von Groß-/Kleinschreibung).

4. Wenn die Änderungen Ihrer Passwort-Policy bei der nächsten Anmeldung anstatt der nächsten Passwortänderung wirksam werden sollen, wählen Sie die Option **Alle internen Benutzer zwingen, bei der nächsten Anmeldung ihr Passwort zu ändern** aus. Beachten Sie, dass diese Einstellung standardmäßig aktiviert ist.
5. Klicken Sie auf **Anwenden**.
   Die Einstellungen für die Passwortsicherheit werden wirksam, wenn interne Benutzer ihre Passwörter erstellen oder ändern. Bei Auswahl der Option **Alle internen Benutzer zwingen, bei der nächsten Anmeldung ihr Passwort zu ändern** müssen alle internen Benutzer ihre Passwörter bei der nächsten Anmeldung bei NetWitness Suite ändern.

Schritt 2. Ändern der Standard-Administratorpasswörter

Dieses Thema enthält Anweisungen zum Ändern des Administratorpassworts für den NetWitness Suite-Service und die Core-Services.

Das Benutzerkonto des Systemadministrators wird mit NetWitness Suite installiert. Der Benutzername lautet **admin** und das Standardpasswort ist das Passwort, das während der Installation der NetWitness Suite in die textbasierte Benutzeroberfläche (TUI) eingegeben wurde. Dem Administrator wird die Rolle **Administratoren** zugewiesen. Diese Rolle verfügt über vollständige Systemberechtigungen zum Steuern, welche Aktionen ein Benutzer ausführen und auf welche Services er zugreifen kann. Die einzige Änderung, die für dieses Konto vorgenommen werden kann, ist die Änderung des Passworts. Im Gegensatz zu anderen NetWitness Suite-Benutzern werden Änderungen am Benutzerpasswort **admin** nicht automatisch an Downstreamservices weitergegeben. Wenn Sie die Einstellungen für die Passwortsicherheit konfigurieren, gelten diese für alle NetWitness Suite-Benutzer, einschließlich des Administratorbenutzers.

Als wichtigem Sicherheitsaspekt von Computern kommt Passwörtern im Hinblick auf den Schutz Ihres Systems die höchste Bedeutung zu. Der **Administratorbenutzer** ist in NetWitness Suite und in jedem Core-Service vorinstalliert. Aus Sicherheitsgründen erstellen Sie die Benutzer und Rollen Ihres Unternehmens in NetWitness Suite und in jedem Core-Service.

Best Practices

RSA empfiehlt die folgenden Best Practices:

- Ändern Sie das **Admin**-Standardpasswort von jedem Service.
- Erstellen Sie ein unterschiedliches Passwort für das **admin**-Konto in jedem Service.

Ändern des Administratorpassworts für die NetWitness Suite

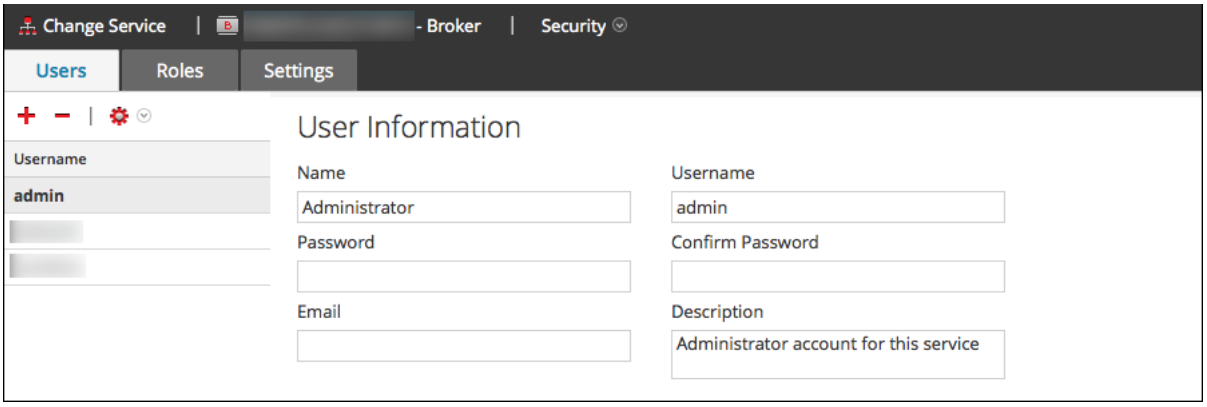
Ändern Sie das **Administratorpasswort** für die NetWitness Suite in der Profilansicht. Weitere Informationen finden Sie unter „Ändern des Passworts“ im *Leitfaden für die ersten Schritte mit NetWitness Suite*. Das Passwort vom **admin**-Benutzer wird nicht an die Core-Services verteilt.

Hinweis: Nachdem Sie das Administratorpasswort geändert haben, müssen Sie eine Datenquelle in der Reporting Engine entfernen und erneut hinzufügen. Weitere Informationen finden Sie im Abschnitt **Entfernen und erneutes Hinzufügen einer Datenquelle in der Reporting Engine** weiter unten.

Ändern des Administratorpassworts für Core-Services

So ändern Sie das Administratorpasswort für einen Core-Service

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Services**.
2. Wählen Sie einen Service und anschließend > **Ansicht > Sicherheit** aus.
3. Wählen Sie auf der Registerkarte **Benutzer** den Benutzer **admin** aus.



4. Geben Sie im Feld **Passwort** ein neues Administratorpasswort für den ausgewählten Service ein.
5. Geben Sie das neue Passwort im Feld **Passwort bestätigen** erneut ein.
6. Klicken Sie auf **Anwenden**.

Hinweis: Nachdem Sie das Administratorpasswort geändert haben, müssen Sie eine Datenquelle in der Reporting Engine entfernen und erneut hinzufügen. Weitere Informationen finden Sie unter **Entfernen und erneutes Hinzufügen einer Datenquelle in der Reporting Engine** weiter unten.

Entfernen und erneutes Hinzufügen einer Datenquelle in der Reporting Engine

Die Reporting Engine überprüft eine Datenquelle anhand des Datenquellen-Benutzernamens und -Passworts. Wenn Sie den Benutzernamen oder das Passwort einer Datenquelle ändern, müssen Sie diese entfernen und erneut hinzufügen.

So entfernen Sie eine Datenquelle in der Reporting Engine und fügen sie erneut hinzu

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Services“ die Reporting Engine und dann > **Ansicht > Konfiguration** aus.
3. Klicken Sie auf die Registerkarte **Quellen**.
4. Wählen Sie den Service aus, den Sie entfernen möchten, und klicken Sie auf .

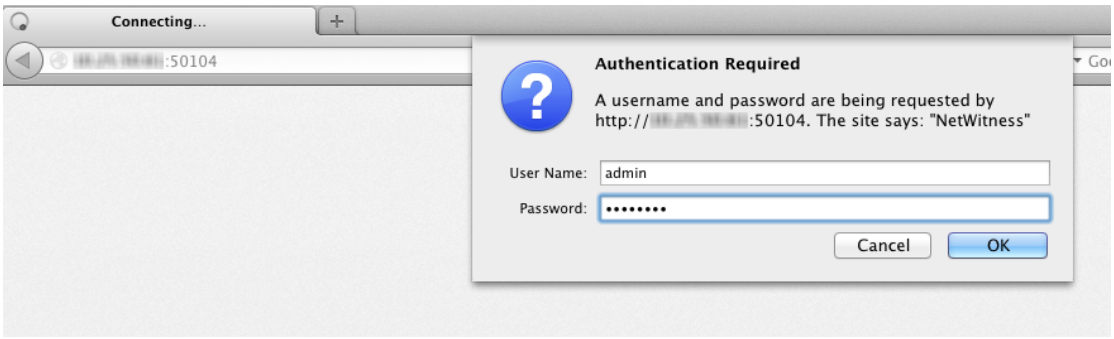
5. Klicken Sie auf + und wählen Sie **Verfügbare Services** aus.
6. Wählen Sie den in Schritt 4 entfernten Service aus und klicken Sie auf **OK**.
7. Geben Sie nach Aufforderung den neuen Benutzernamen und das Passwort für den Service ein.

Ändern des Administratorpassworts für einen Service mithilfe der REST-API

In seltenen Fällen müssen Sie möglicherweise das Administratorpasswort für einen Core-Service außerhalb der NetWitness Suite-Benutzeroberfläche ändern. Dabei handelt es sich um eine weitere Methode, um eine Passwortänderung für den Core-Service durchzuführen. Jedoch ist dies nicht die bevorzugte Methode.

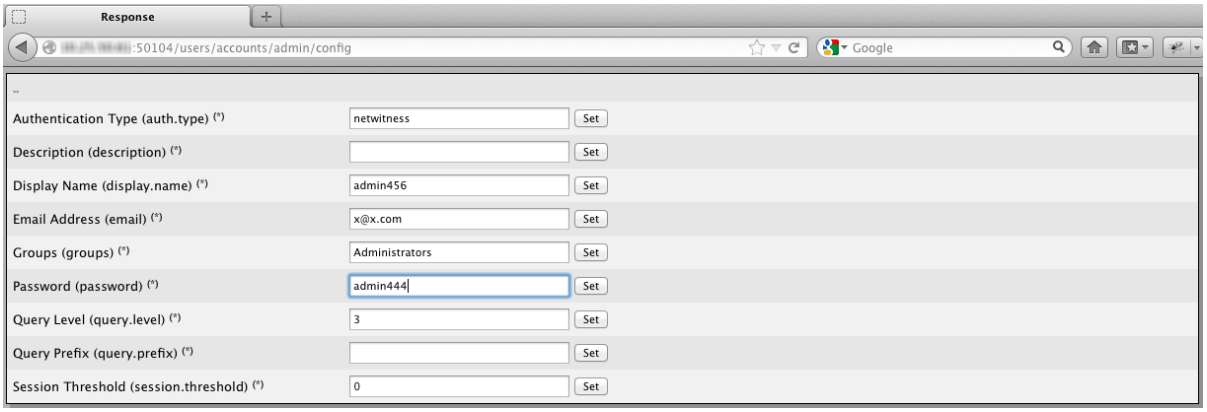
So ändern Sie das Administratorpasswort für den Service mithilfe der REST-Benutzeroberfläche:

1. Öffnen Sie einen Webbrowser und rufen Sie die folgende URL auf:
   <hostname>:<port>
   , wobei **hostname** der Name eines NetWitness Suite-Core-Services und **port** der für die REST-Kommunikation verwendete Port ist. Nachfolgend ist ein Beispiel für einen Decoder angegeben: `http://10.20.30.40:50104`
   Das Dialogfeld „Authentifizierung“ wird angezeigt.



2. Geben Sie im Dialogfeld den für die Authentifizierung als Administrator bei dem Service verwendeten Benutzernamen und das Passwort ein und klicken Sie auf **OK**. Der Standardbenutzername lautet **admin** und das Standardpasswort ist **netwitness**.
   Das REST-Fenster für den Service wird angezeigt.
3. Navigieren Sie durch die Node-Struktur zu **users/accounts/admin/config**.
   Im Browserfenster werden die Benutzerkonfigurationsfelder für den Administrator

angezeigt.



4. Geben Sie im Feld „Passwort“ ein neues Administratorpasswort ein und klicken Sie auf **Festlegen**.

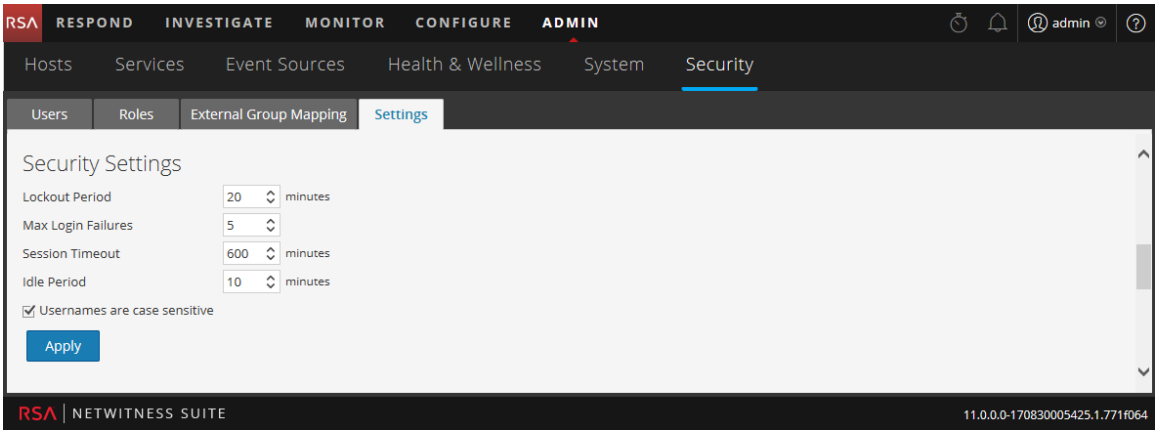
Schritt 3. Konfigurieren von Sicherheitseinstellungen auf Systemebene

In diesem Thema wird das Verfahren zum Einstellen von systemweiten Sicherheitsparametern erklärt.

Die meisten globalen Sicherheitseinstellungen, zum Beispiel die zulässige Höchstanzahl fehlgeschlagener Anmeldeversuche, gelten für alle NetWitness Suite-Benutzer und -Sitzungen. Die Einstellungen für Passwörter im Abschnitt „Passwortsicherheit“, zum Beispiel die Passwortablaufdauer und die Standardanzahl der Tage, nach denen Benutzerpasswörter ablaufen, gelten für interne NetWitness Suite-Benutzer, aber nicht für externe Benutzer.

Konfigurieren von Sicherheitseinstellungen

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.



3. Geben Sie im Abschnitt **Sicherheitseinstellungen** die Werte in die Felder ein, die in der folgenden Tabelle beschrieben werden.

Feld	Beschreibung
Sperrdauer	Gibt an, nach wieviel Minuten ein Benutzer aus NetWitness Suite ausgesperrt wird, nachdem die konfigurierte Anzahl fehlgeschlagener Anmeldungen überschritten wurde. Der Standardwert ist 20 Minuten.
Max. Anmeldungsfehler	Gibt an, nach wie vielen erfolglosen Anmeldeversuchen ein Benutzer gesperrt wird. Der Standardwert ist 5.

Feld	Beschreibung
Sitzungs-Timeout	Gibt die maximale Dauer einer Benutzersitzung bis zum Timeout an (in Minuten). Der Standardwert ist 600. Die Sitzung wird deaktiviert, wenn die konfigurierte Zeit verstrichen ist. Danach muss sich der Benutzer erneut anmelden. Der maximal zulässige Wert beträgt 30.000. **Hinweis:** Wenn Sie ein Upgrade von NetWitness Suite 10.6.x auf Version 11.0 durchgeführt und zuvor für ein unbegrenztes Sitzungs-Timeout den Wert 0 verwendet haben, wurde der Wert automatisch auf 30.000 Minuten zurückgesetzt, da der Wert 0 nicht mehr unterstützt wird.
Leerlaufperiode	Gibt an, nach wieviel Minuten der Inaktivität eine Sitzung deaktiviert wird. Der Standardwert ist 10. Der maximal zulässige Wert beträgt 30.000. **Hinweis:** Wenn Sie ein Upgrade von NetWitness Suite 10.6.x auf Version 11.0 durchgeführt und zuvor für eine unbegrenzte Leerlaufperiode den Wert 0 verwendet haben, wurde der Wert automatisch auf den Standardwert 10 zurückgesetzt, da der Wert 0 nicht mehr unterstützt wird.
Bei Benutzernamen müssen Sie die Groß- und Kleinschreibung beachten.	Wählen Sie diese Option aus, wenn im Feld „Benutzername“ im NetWitness Suite-Anmeldebildschirm die Groß- und Kleinschreibung beachtet werden soll. Beispiel: Wenn bei Benutzernamen die Groß- und Kleinschreibung beachtet wird, können Sie für die Anmeldung bei NetWitness Suite „admin“ verwenden, jedoch nicht „Admin“.

4. Klicken Sie auf **Anwenden**. Die Sicherheitseinstellungen werden umgehend übernommen. Wenn ein Passwort abläuft, empfängt der Benutzer eine Aufforderung zum Ändern des Passworts, wenn er sich bei NetWitness Suite anmeldet.

Schritt 4. (Optional) Konfigurieren der externen Authentifizierung

In diesem Thema werden die von NetWitness Suite unterstützten externen Authentifizierungsmethoden erläutert.

Wenn sich ein Benutzer anmeldet, versucht NetWitness Suite zunächst, eine lokale Authentifizierung durchzuführen. Wenn kein lokaler Benutzer gefunden wird und eine externe Authentifizierungskonfiguration aktiviert ist, wird versucht, die Authentifizierung extern vorzunehmen.

Die externe Authentifizierung ermöglicht es Benutzern, die kein internes NetWitness Suite-Benutzerkonto haben, sich bei NetWitness Suite anzumelden und rollenbasierte Berechtigungen zu erhalten.

NetWitness Suite unterstützt zwei Methoden der externen Authentifizierung: Active Directory und PAM (Pluggable Authentication Modules). Die Themen in diesem Abschnitt beschreiben, wie die Methoden konfiguriert und getestet werden.

Themen

- Konfigurieren von Active Directory
- Konfigurieren der PAM-Anmeldefunktion

Konfigurieren von Active Directory

In diesem Thema wird erläutert, wie Sie NetWitness Suite so konfigurieren, dass externe Benutzeranmeldungen mit Active Directory authentifiziert werden.

Wenn sich ein Benutzer anmeldet, versucht NetWitness Suite zunächst, eine lokale Authentifizierung durchzuführen. Wenn kein lokaler Benutzer gefunden wird und die Active Directory-Konfiguration aktiviert ist, wird versucht, die Authentifizierung mit dem Active Directory-Service vorzunehmen. Im Modul „Administration“ können Sie in der Ansicht „Sicherheit“ auf der Registerkarte „Einstellungen“ Active Directory-Einstellungen konfigurieren, um die Authentifizierung externer Gruppen zu aktivieren.

In einer Umgebung mit mehreren Authentifizierungsservern ermöglicht die LDAP-Weiterleitung ein LDAP-Referral im Anschluss an den AD-Gruppen-Lookup. Die LDAP-Weiterleitung kann den Anmeldevorgang verlängern, da der AD-Gruppen-Lookup auf verbundene Authentifizierungsserver erweitert wird. Wenn Ihre AD-Instanz versucht, Domain-Controller zu kontaktieren, die von Ihrer Firewall blockiert werden, kann bei der Anmeldung bei NetWitness Suite eine Verzögerung von einigen Minuten auftreten. NetWitness Suite verfügt über eine Konfigurationsoption, die angibt, ob eine LDAP-Weiterleitung erfolgt. Standardmäßig sind LDAP-Referrals deaktiviert. Wenn diese Option deaktiviert ist, versucht Ihre AD-Instanz nicht, den Domain-Controller zu kontaktieren, auf den verwiesen wird.

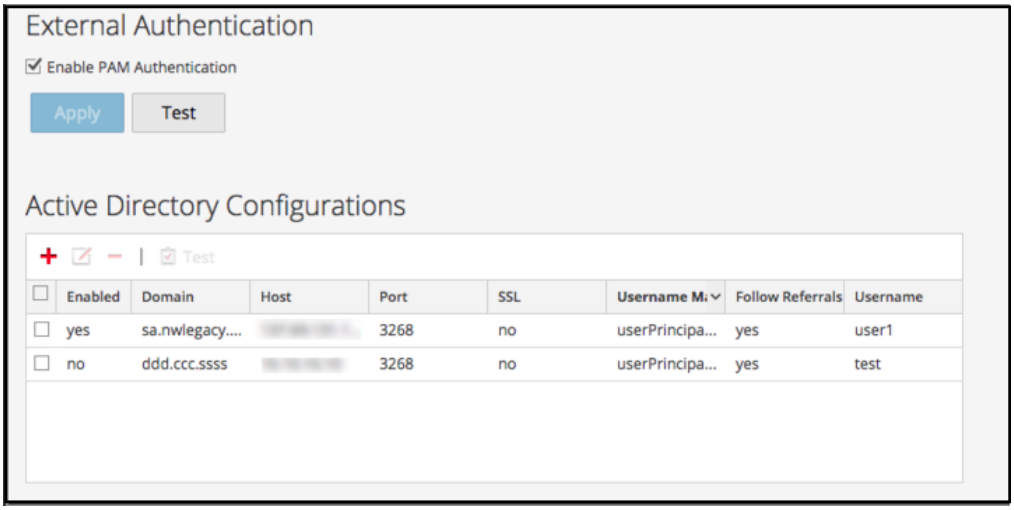
Hinweis: Die Registerkarte „Einstellungen“ bietet auch die Option zum Aktivieren der PAM-Konfiguration, die gleichzeitig mit Active Directory-Konfigurationen verwendet werden kann. Weitere Informationen zum Aktivieren und Konfigurieren der PAM-Authentifizierung finden Sie unter Konfigurieren der PAM-Anmeldefunktion.

Methoden

Konfigurieren der Active Directory-Authentifizierung

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
   Die Liste der Active Directory-Konfigurationen wird im Bereich angezeigt, sodass Sie eine

Konfiguration hinzufügen oder bearbeiten können.



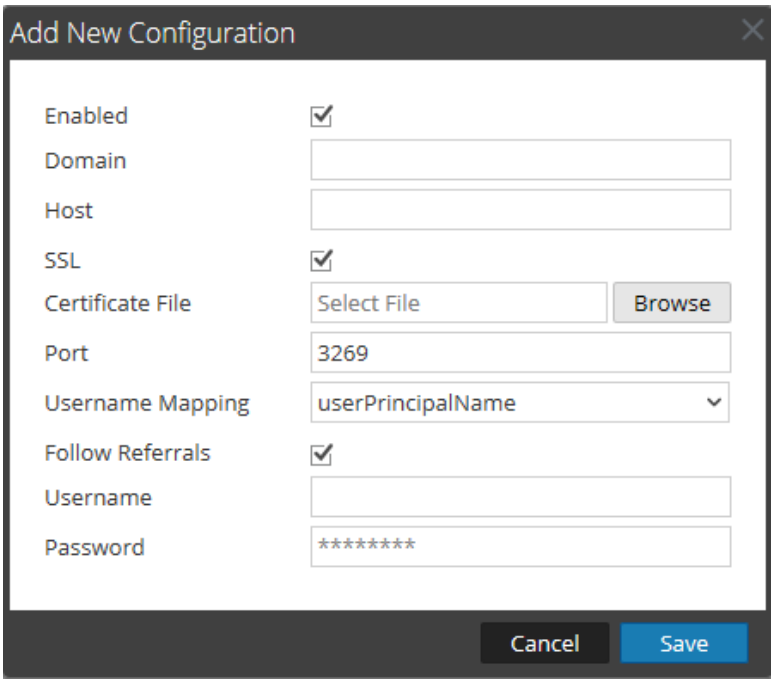
3. Sie können Domains nach Bedarf hinzufügen, bearbeiten oder löschen, wie in den folgenden Abschnitten beschrieben.
   Die Domains, die dieser Liste hinzugefügt wurden, werden automatisch auf der Registerkarte „Externe Gruppenzuordnung“ aufgeführt, sodass Sie jeder Gruppe Sicherheitsrollen zuordnen können.

Hinweis: Wie Sie Sicherheitsrollen für den Active Directory-Zugriff konfigurieren, erfahren Sie unter Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen.

Hinzufügen einer neuen Active Directory-Konfiguration

So fügen Sie der Liste der Active Directory-Konfigurationen eine neue Active Directory-Konfiguration hinzu:

1. Klicken Sie unter „Active Directory-Konfigurationen“ auf +.
   Das Dialogfeld „Neue Konfiguration hinzufügen“ wird angezeigt.



2. Aktivieren Sie das Kontrollkästchen **Aktiviert**.
3. Geben Sie Informationen für **Domain**, **Host** und **Port** für den Active Directory-Service ein.
4. (Optional) Um SSL für diese Konfiguration auszuwählen, aktivieren Sie das Kontrollkästchen **SSL verwenden**. Sie müssen dann eine Zertifikatdatei eingeben. Klicken Sie dazu auf **Durchsuchen** und wählen Sie die gewünschte hochzuladene Datei aus. Wenn der AD-Server ein öffentliches, von der Zertifizierungsstelle signiertes Zertifikat verwendet, müssen Sie kein Zertifikat hochladen. Wenn der AD-Server ein selbstsigniertes Zertifikat verwendet, müssen Sie das Zertifikat der Zertifizierungsstelle oder das selbstsignierte Zertifikat hochladen.
5. Wählen Sie im Feld **Benutzernamenszuordnung** das Active Directory-Suchfeld aus, das Sie für die Benutzernamenszuordnung verwenden möchten. Sie können userPrincipalName (UPN) oder sAMAccountName auswählen.
6. Für Sites mit mehreren Authentifizierungsservern klicken Sie auf **Referrals befolgen**, um die Befolgung von LDAP-Referrals nach AD-Gruppen-Lookups zu aktivieren oder zu deaktivieren.
7. Um Anmeldedaten zur Bindung an den Active Directory-Service während der Suche der Active Directory-Gruppe bereitzustellen, geben Sie die Anmeldedaten in die Felder **Benutzername** und **Passwort** ein.

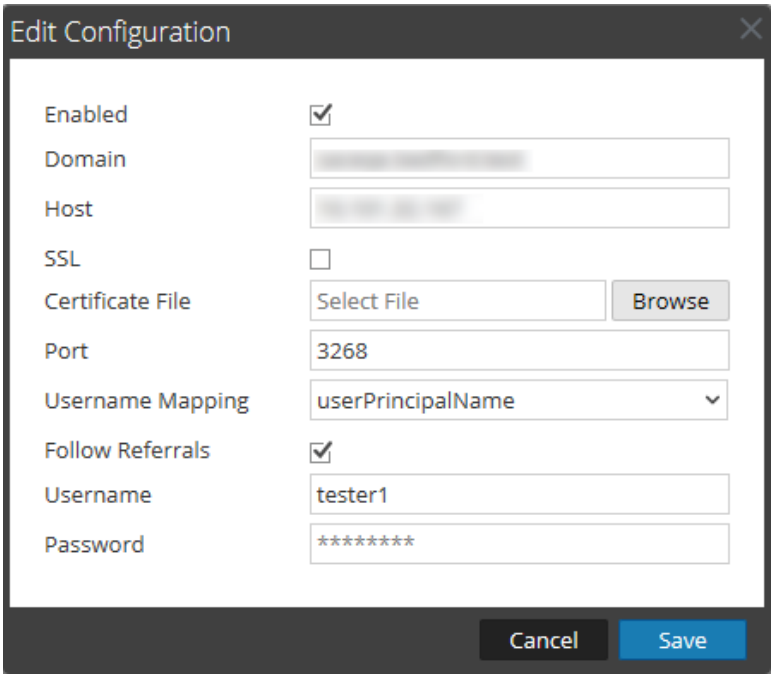
Hinweis: Wenn Sie im Feld **Benutzernamenszuordnung** den Eintrag „sAMAccountName“ ausgewählt haben, müssen Sie zur Authentifizierung den Benutzernamen im Format „Domain\Benutzer“ eingeben.

8. Klicken Sie auf **Speichern**.
   Die neue Konfiguration wird in der Liste der Active Directory-Konfigurationen aufgeführt.

Bearbeiten einer Active Directory-Konfiguration

So bearbeiten Sie eine Active Directory-Konfiguration in der Liste der Active Directory-Konfigurationen:

1. Wählen Sie unter **Active Directory-Konfigurationen** die zu bearbeitende Konfiguration aus und klicken Sie auf .
   Das Dialogfeld „Konfiguration bearbeiten“ wird angezeigt.



2. (Optional) Geben Sie Informationen für **Domain**, **Host** und **Port** für den Active Directory-Service ein.
3. (Optional) Um SSL für diese Konfiguration auszuwählen, aktivieren Sie das Kontrollkästchen **SSL verwenden**. Sie müssen dann eine Zertifikatdatei eingeben. Klicken Sie dazu auf **Durchsuchen** und wählen Sie die gewünschte Datei aus.
4. (Optional) Wählen Sie im Feld **Benutzernamenszuordnung** das Active Directory-Suchfeld aus, das Sie für die Benutzernamenszuordnung verwenden möchten.

5. Zur Angabe des Verhaltens bei der LDAP-Referral-Befolgung in Umgebungen mit mehreren Authentifizierungsservern dient das Kontrollkästchen **Referrals befolgen**.
   a. Wenn Sie die LDAP-Weiterleitung deaktivieren möchten, deaktivieren Sie das Kontrollkästchen.
   b. Wenn Sie die LDAP-Weiterleitung aktivieren möchten, aktivieren Sie das Kontrollkästchen.
6. Um Anmeldedaten zur Bindung an den Active Directory-Service während der Suche der Active Directory-Gruppe bereitzustellen, geben Sie die Anmeldedaten in die Felder **Benutzername** und **Passwort** ein.
7. Klicken Sie auf **Speichern**.
   Die Konfiguration wird in der Liste der Active Directory-Konfigurationen aufgeführt.

Testen einer Active Directory-Konfiguration

So testen Sie eine Active Directory-Konfiguration:

1. Wählen Sie die zu testende Konfiguration aus der Liste der Active Directory-Konfigurationen aus.
2. Klicken Sie in der Symbolleiste auf Test.
   Eine Meldung wird angezeigt, dass der Test erfolgreich war.
3. Wenn der Test fehlgeschlagen ist, überprüfen und bearbeiten Sie die Konfiguration.

Löschen einer Active Directory-Konfiguration

So löschen Sie eine Active Directory-Konfiguration:

1. Wählen Sie unter den Active Directory-Konfigurationen die Konfiguration auf, die aus der Liste der Active Directory-Konfigurationen gelöscht werden soll.
2. Klicken Sie in der Symbolleiste auf −.
   Eine Warnmeldung wird angezeigt, dass alle Benutzer in der ausgewählten Active Directory-Konfiguration sich nicht bei NetWitness Suite anmelden können, werden diese gelöscht wird.
3. Führen Sie einen der folgenden Schritte aus:
   a. Klicken Sie zum Bestätigen des Löschvorgangs auf **Ja**.
   b. Um den Löschvorgang abzubrechen, klicken Sie auf **Nein**.

Konfigurieren der PAM-Anmeldefunktion

In diesem Thema wird erläutert, wie Sie NetWitness Suite so konfigurieren, dass mithilfe von PAM (Pluggable Authentication Modules) externe Benutzeranmeldungen authentifiziert werden können.

Die PAM-Anmeldefunktion umfasst zwei separate Komponenten:

- PAM für die Benutzerauthentifizierung
- NSS für die Gruppenautorisierung

Zusammen bieten sie externen Benutzern die Möglichkeit, sich bei NetWitness Suite anzumelden, ohne ein internes NetWitness Suite-Konto zu haben, und Berechtigungen oder Rollen zu erhalten, die durch Zuordnung der externen Gruppe zu einer NetWitness Suite-Sicherheitsrolle festgelegt wurden. Beide Komponenten sind für eine erfolgreiche Anmeldung erforderlich.

Externe Authentifizierung ist eine Einstellung auf Systemebene. Vor der PAM-Konfiguration sollten Sie alle hierin enthaltenen Informationen aufmerksam lesen.

PAM (Pluggable Authentication Modules)

PAM ist eine von Linux bereitgestellte Bibliothek, die der Authentifizierung von Benutzern gegenüber Authentifizierungsprovidern dient, z. B. RADIUS, Kerberos oder LDAP. Für die Implementierung verwendet jeder Authentifizierungsprovider sein eigenes Modul, das in Form eines Betriebssystempakets (OS), wie etwa pam_ldap bereitgestellt wird. NetWitness Suite verwendet die vom Betriebssystem bereitgestellte PAM-Bibliothek und das Modul, das zur Verwendung durch die PAM-Bibliothek konfiguriert wurde, zur Authentifizierung von Benutzern.

Hinweis: PAM bietet nur die Fähigkeit zur Authentifizierung.

NSS (Name Service Switch)

NSS ist eine Linux-Funktion zur Bereitstellung von Datenbanken, die vom Betriebssystem und den Anwendungen verwendet werden, um Informationen wie Hostnamen und Benutzerattribute (z. B. Stammverzeichnis, primäre Gruppe und Anmeldeshell) zu erkennen und um Benutzer aufzulisten, die einer angegebenen Gruppe angehören. Ähnlich wie PAM kann NSS konfiguriert werden und verwendet Module zur Interaktion mit verschiedenen Anbietertypen. NetWitness Suite verwendet vom Betriebssystem bereitgestellte NSS-Funktionen, um externe PAM-Benutzer zu autorisieren, indem überprüft wird, ob ein Benutzer in NSS bekannt ist. Anschließend werden von NSS die Gruppen abgerufen, bei denen dieser Benutzer Mitglied ist. NetWitness Suite vergleicht die Ergebnisse der Abfrage mit der externen NetWitness Suite-Gruppenzuordnung. Wenn eine entsprechende Gruppe gefunden wird, erhält der Benutzer Zugriff auf die Anmeldung bei NW mit der Sicherheitsebene, die in der externen Gruppenzuordnung definiert wurde.

Hinweis: NSS bietet keine Authentifizierung.

Kombination von PAM und NSS

Sowohl PAM (Authentifizierung) als auch NSS (Autorisierung) müssen erfolgreich sein, damit sich ein externer Benutzer bei NetWitness Suite anmelden darf. Das Verfahren zur Konfiguration und zum Troubleshooting von PAM ist anders als das Verfahren zur Konfiguration und zum Troubleshooting von NSS. Zu den PAM-Beispielen in diesem Leitfaden gehören Kerberos, LDAP und Radius. Zu den NSS-Beispielen gehören Samba, LDAP und UNIX. Welche Kombination von PAM- und NSS-Modul verwendet wird, bestimmen die Anforderungen des Standorts.

Prozessübersicht

Führen Sie zur Konfiguration der PAM-Anmeldefunktion die Anweisungen in diesem Dokument aus:

1. Konfigurieren und testen Sie das PAM-Modul.
2. Konfigurieren und testen Sie den NSS-Service.
3. Aktivieren Sie PAM in NetWitness-Server.
4. Erstellen Sie Gruppenzuordnungen in NetWitness-Server.

Voraussetzungen

Bevor Sie mit der Einrichtung von PAM beginnen, überprüfen Sie abhängig von dem PAM-Modul, das Sie implementieren möchten, das Verfahren und sammeln Sie die Details des externen Authentifizierungsservers.

Bevor Sie mit der Einrichtung von NSS beginnen, überprüfen Sie das Verfahren und identifizieren Sie die Gruppennamen, die Sie in der externen Gruppenzuordnung verwenden werden, und sammeln Sie abhängig von dem verwendeten NSS-Service die Details des externen Authentifizierungsservers.

Bevor Sie damit beginnen, PAM in NetWitness Suite einzurichten, identifizieren Sie die Gruppennamen, die Sie in der externen Gruppenzuordnung verwenden werden. Wenn Rollen zugeordnet werden, muss die Rolle in NetWitness Suite einem Gruppennamen entsprechen, der auf dem externen Authentifizierungsserver vorhanden ist.

Konfigurieren und Testen des PAM-Moduls

Wählen Sie einen der folgenden Abschnitte aus, um die PAM-Komponente einzurichten und zu konfigurieren:

- PAM – Kerberos
- PAM – LDAP

- PAM – RADIUS
- SecurID

PAM – Kerberos

Kerberos-Kommunikationsports – TCP 88

So konfigurieren Sie die PAM-Authentifizierung mithilfe von Kerberos:

1. Führen Sie den folgenden Befehl aus (aber überprüfen Sie zuerst, ob das `krb5-workstation`-Paket in Ihrer Umgebung installiert ist):
   `yum install krb5-workstation pam_krb5`
2. Bearbeiten Sie die folgenden Zeilen in der Kerberos-Konfigurationsdatei `/etc/krb5.conf`. Ersetzen Sie Variablen, die mit <Spitzklammern> abgesetzt sind, durch Ihre Werte und lassen Sie die Spitzklammern weg. Die angegebene Groß- und Kleinschreibung muss befolgt werden.

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 dns_lookup_kdc = true
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = <DOMAIN.COM>
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 <DOMAIN.COM> = {
 kdc = <SERVER.DOMAIN.COM>
 admin_server = <SERVER.DOMAIN.COM>
 }

 [domain_realm]
 <domain.com> = <DOMAIN.COM>
 <.domain.com> = <DOMAIN.COM>
```

3. Testen Sie die Kerberos-Konfiguration mit dem Befehl:
   `kinit <user>@<DOMAIN.COM>`
   Keine Ausgabe nach Eingabe des Passworts bedeutet Erfolg.

4. Bearbeiten Sie die NetWitness-Server-PAM-Konfigurationsdatei `/etc/pam.d/securityanalytics`, um die folgende Zeile hinzuzufügen. Wenn die Datei nicht vorhanden ist, erstellen Sie sie und fügen Sie die folgende Zeile hinzu:
   `auth sufficient pam_krb5.so no_user_check`

Damit ist die Konfiguration für PAM Kerberos abgeschlossen. Fahren Sie jetzt mit dem nächsten Abschnitt *Konfigurieren und Testen des NSS-Services* fort.

PAM – LDAP

LDAP-Kommunikationsports – TCP 389 oder TCP 636

TCP 389 kann für unverschlüsselten und in den meisten Fällen auch für verschlüsselten Datenverkehr verwendet werden und ist in der Regel ausreichend. Die meisten modernen LDAP-Implementierungen unterstützen nach dem Verbinden mit Port 389 den Befehl `start_tls`, mit dem der Status der Verbindung von unverschlüsselt zu verschlüsselt hochgestuft wird. In dieser Instanz beginnen LDAP-URIs immer noch mit `ldap://`, auch wenn sie `start_tls.` verwenden.

TCP 636 wird nur in Instanzen verwendet, in denen der LDAP-Server den Befehl `start_tls` nicht unterstützt. In diesem Fall beginnen LDAP-URIs mit `ldaps://` und der Befehl `start_tls` wird nicht verwendet.

So konfigurieren Sie die PAM-Authentifizierung mithilfe von LDAP:

1. Führen Sie den folgenden Befehl aus (aber überprüfen Sie zuerst, ob das `openldap-clients`-Paket in Ihrer Umgebung installiert ist):
   `yum install nss-pam-ldapd openldap-clients`
2. Bearbeiten Sie die LDAP-Konfigurationsdatei `/etc/nslcd.conf`, wie im folgenden Beispiel gezeigt:

Hinweis: Ersetzen Sie die durch <Spitzklammern> abgesetzten Variablen durch Ihre Werte und entfernen Sie die Spitzklammern. Die angegebene Groß- und Kleinschreibung muss befolgt werden.

Beispiel für Einträge in der Datei `/etc/nslcd.conf`:

```
uri ldap://<server.domain.com>
 base <dc=domain,dc=com>
 binddn <cn=bineuser,dc=domain,dc=com>
 bindpw <secret>
```

3. Führen Sie nach dem Ändern der Datei `/etc/nslcd.conf` den folgenden Befehl aus:
   `systemctl restart nslcd`

4. (Optional) Wenn Sie einen sicheren Transport für die LDAP-Kommunikation mit Peer-Zertifikatüberprüfung (höhere Sicherheit) aktivieren möchten, finden Sie auf der Linux-Manpage für nslcd die korrekte Codeänderung für die Datei `/etc/nslcd.conf`.

   Hinweis: Windows-Domain-Controller ermöglichen standardmäßig keinen sicheren LDAP-Transport. Sie erfordern die Installation eines Serverzertifikats für die Serverauthentifizierung. Abruf und Installation dieses Zertifikat auf dem DC gehen über den Umfang dieses Dokuments hinaus. Einige Informationen dazu sind verfügbar unter https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx.

5. (Optional) Wenn Sie einen sicheren Transport für die LDAP-Kommunikation ohne Peer-Zertifikat aktivieren möchten, finden Sie auf der Linux-Manpage für nslcd die korrekte Codeänderung für die Datei `/etc/nslcd.conf`.

6. Beenden Sie für das Troubleshooting der LDAP-Konfiguration zunächst den `nslcd`-Service, indem Sie den folgenden Befehl eingeben:
   ```
   systemctl stop nlscd
   ```

7. Um Troubleshooting- und Statusinformationen vom Service an die Konsole auszugeben, führen in der Befehlszeile den `nslcd`-Service im Debug-Modus aus:
   ```
   nslcd -d
   ```

8. Bearbeiten Sie die NetWitness-Server-PAM-Konfigurationsdatei `/etc/pam.d/securityanalytics`, um die folgende Zeile hinzuzufügen. Wenn die Datei nicht vorhanden ist, erstellen Sie sie und fügen Sie die folgende Zeile hinzu:
   ```
   auth sufficient pam_ldap.so
   ```

Dadurch wird die Konfiguration für PAM LDAP abgeschlossen. Fahren Sie jetzt mit dem nächsten Abschnitt fort: *Konfigurieren und Testen des NSS-Services*.

PAM – RADIUS

Radius-Kommunikationsports – UDP 1812 oder UDP 1813

Zur Konfiguration der PAM-Authentifizierung mithilfe von Radius müssen Sie den NetWitness-Server zur Clientliste Ihres Radius-Servers hinzufügen und einen gemeinsamen geheimen Schlüssel konfigurieren. Wenden Sie sich hierfür an den Radius-Serveradministrator.

So konfigurieren Sie die PAM-Authentifizierung für RADIUS mithilfe von LDAP:

1. Führen Sie den folgenden Befehl aus (aber überprüfen Sie zuerst, ob das `pam_radius`-Paket in Ihrer Umgebung installiert ist):
   ```
   yum install pam_radius
   ```
2. Bearbeiten Sie die RADIUS-Konfigurationsdatei `/etc/raddb/server` wie folgt:
   ```
   # server[:port] shared_secret  timeout (s)
   server    secret     3
   ```
3. Bearbeiten Sie die NetWitness-Server-PAM-Konfigurationsdatei `/etc/pam.d/securityanalytics`, um die folgende Zeile hinzuzufügen. Wenn die Datei nicht vorhanden ist, erstellen Sie sie und fügen Sie die folgende Zeile hinzu:
   ```
   auth sufficient pam_radius_auth.so
   ```

Achtung: Damit PAM RADIUS verwendet werden kann, muss die Datei `/etc/raddb/server` über Schreibberechtigungen verfügen. Der hierfür erforderliche Befehl lautet: `chown netwitness:netwitness /etc/raddb/server`.

Die PAM-Module und zugehörigen Services geben Informationen nach `/var/log/messages` und `/var/log/secure` aus. Diese Ausgaben können beim Troubleshooting von Konfigurationsproblemen hilfreich sein.

Das folgende Verfahren ist ein Beispiel für die Schritte zum Konfigurieren der PAM-Authentifizierung für RADIUS mithilfe von SecurID:

Hinweis: In den Beispielen für diese Aufgaben wird RSA Authentication Manager als RADIUS-Server verwendet.

1. Führen Sie den folgenden Befehl aus (aber überprüfen Sie zuerst, ob das `pam_radius`-Paket in Ihrer Umgebung installiert ist):
   ```
   yum install pam_radius
   ```
2. Bearbeiten Sie die RADIUS-Konfigurationsdatei `/etc/raddb/server` und aktualisieren Sie sie mit dem Hostnamen der Authentication Manager-Instanz, dem gemeinsamen geheimen Schlüssel und dem Timeout-Wert:
   ```
   # server[:port] shared_secret timeout (s)
   111.222.33.44         secret        1
   #other-server        other-secret 3
   192.168.12.200:6369 securid      10
   ```

Hinweis: Sie müssen die Zeilen `127.0.0.1` und `other-server` auskommentieren und die IP-Adresse der primären Authentication Manager-Instanz mit der RADIUS-Portnummer (z. B. `192.168.12.200:1812`), dem gemeinsamen geheimen RADIUS-Schlüssel und einem Timeout-Wert von 10 hinzufügen.

3. Bearbeiten Sie die NetWitness-Server-PAM-Konfigurationsdatei `/etc/pam.d/securityanalytics`, um die folgende Zeile hinzuzufügen. Wenn die Datei nicht vorhanden ist, erstellen Sie sie und fügen Sie die folgende Zeile hinzu:

   ```
   auth sufficient pam_radius_auth.so
   ```

   Hinweis: Sie können `debug` in der Datei `/etc/pam.d/securityanalytics` an das Ende der oben genannten Zeile hinzufügen, um PAM-Debugging zu aktivieren (z. B. `auth sufficient pam_radius_auth.so debug`).

Die PAM-Module und zugehörigen Services geben Informationen nach `/var/log/messages` und `/var/log/secure` aus. Diese Ausgaben können beim Troubleshooting von Konfigurationsproblemen hilfreich sein.

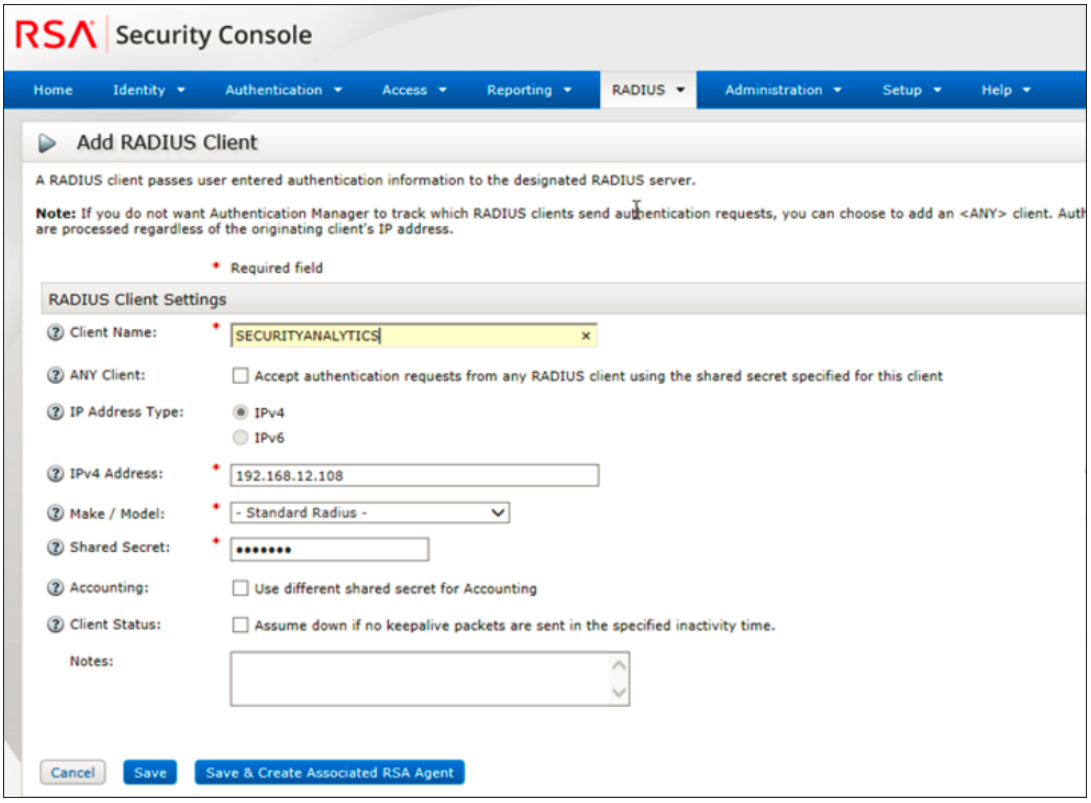
Hinzufügen eines RADIUS-Clients und zugeordneten Agent

Hinweis: In den Beispielen für diese Aufgaben wird RSA Authentication Manager als RADIUS-Server verwendet.
Sie müssen die Anmeldedaten des Administratorkontos verwenden, um sich bei der Sicherheitskonsole von RSA Authentication Manager anzumelden.

So fügen Sie einen RADIUS-Client und zugeordneten Agent hinzu:

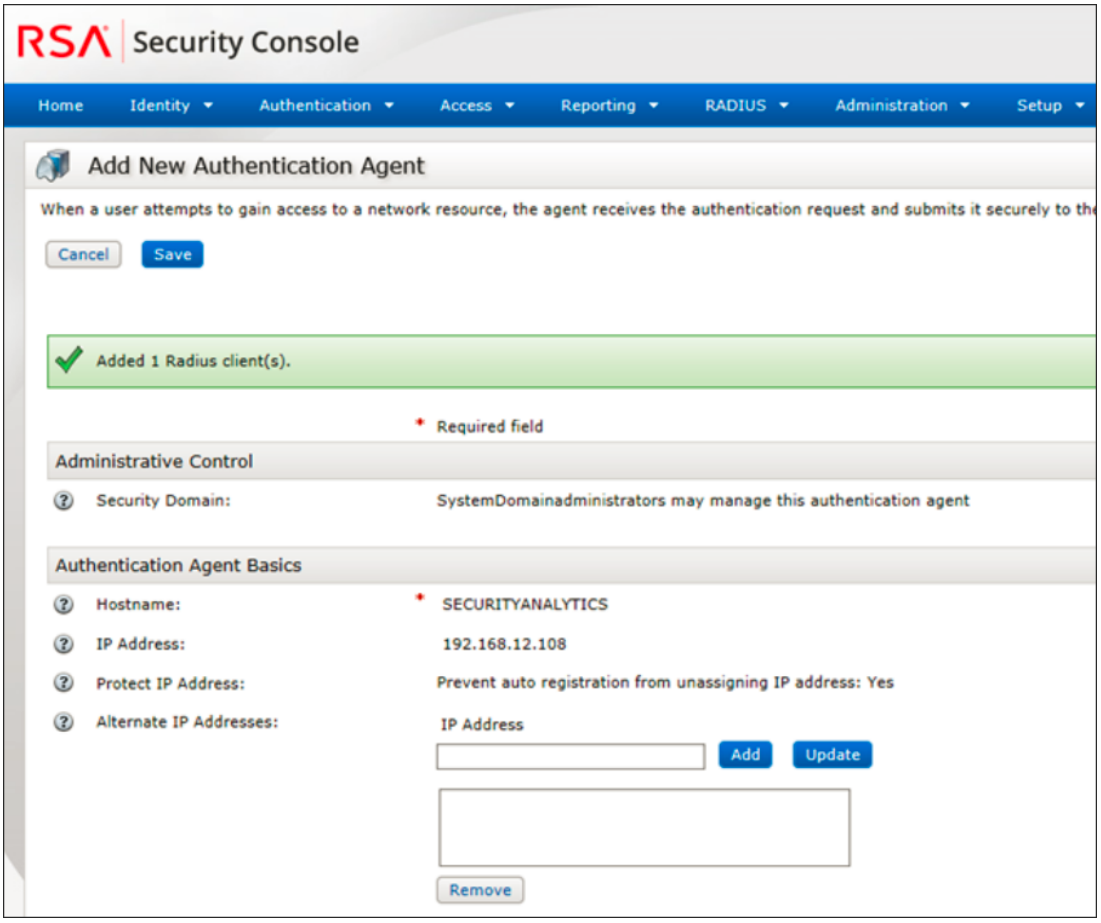
1. Melden Sie sich bei RSA Authentication Manager an.
   Die Sicherheitskonsole wird angezeigt.
2. Klicken Sie in der Sicherheitskonsole auf **RADIUS > RADIUS-Clients > Neue hinzufügen**.

Die Seite „RADIUS-Client hinzufügen“ wird angezeigt.



3. Geben Sie im Bereich „RADIUS-Clienteinstellungen“ folgende Informationen ein:
   a. Geben Sie im Feld **Clientname** den Namen des Clients ein, z. B. „NetWitness Suite“.
   b. Geben Sie im Feld **IPv4-Adresse** die IPv4-Adresse des RADIUS-Clients ein, z. B. 192.168.12.108.
   c. Wählen Sie in der Drop-down-Liste **Marke/Modell** den Typ des RADIUS-Clients aus, z. B. Fortinet.
   d. Geben Sie im Feld **Gemeinsamer geheimer Schlüssel** den freigegebenen Authentifizierungsschlüssel ein.

4. Klicken Sie auf **Zugeordneten RSA-Agent speichern und erstellen**.



5. Klicken Sie auf **Speichern**.

Wenn die Authentication Manager-Instanz den Authentifizierungs-Agent im Netzwerk nicht finden kann, wird eine Seite mit einer Warnmeldung angezeigt. Klicken Sie auf **Ja, Agent speichern**.

Weitere Informationen hierzu finden Sie im Thema „Hinzufügen eines RADIUS-Clients“ im *Administratorhandbuch für RSA Authentication Manager 8.2*.

Damit ist die Konfiguration für PAM RADIUS abgeschlossen. Fahren Sie jetzt mit dem nächsten Abschnitt fort, *Konfigurieren und Testen des NSS-Services*.

PAM-Agent für SecurID

PAM-Kommunikationsport – UDP 5500

Voraussetzungen

Das RSA SecurID PAM-Modul wird nur unter den folgenden Bedingungen unterstützt:

1. Vertrauenswürdige Verbindungen zwischen NetWitness Suite und Core-Services müssen aktiviert und funktionsbereit sein.

Prozessübersicht

Die allgemeinen Schritte zur Konfiguration des SecurID-PAM-Moduls sind:

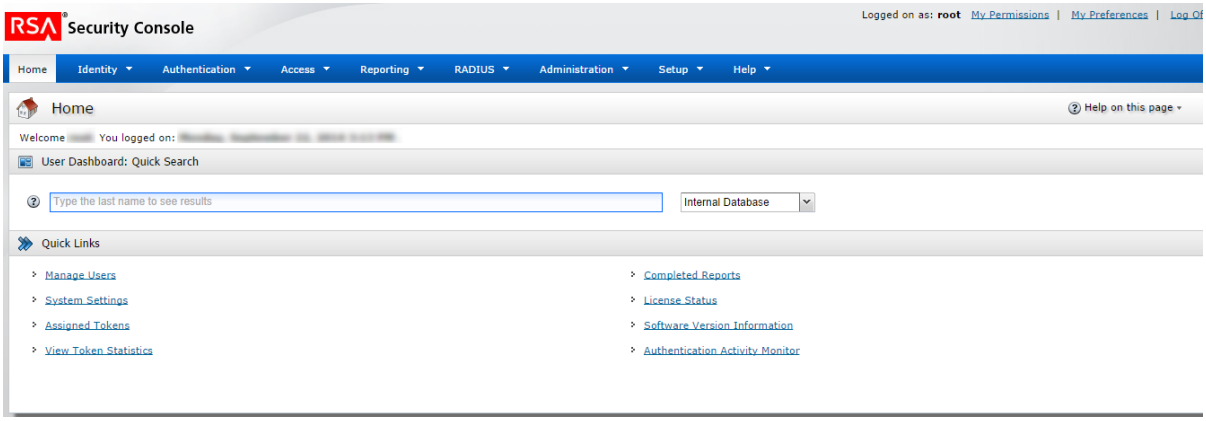
1. Konfigurieren Sie **Authentication Manager**:
   a. Fügen Sie den Authentifizierungs-Agent hinzu.
   b. Konfigurationsdatei herunterladen
2. Konfigurieren Sie **NetWitness-Server**:
   a. Kopieren Sie die Konfigurationsdatei von Authentication Manager und passen Sie sie an.
   b. Installieren Sie das PAM-SecurID-Modul.
3. Testen Sie die Verbindung und die Authentifizierung.

Befolgen Sie dann die übrigen Verfahren in den folgenden Abschnitten:

- Konfigurieren Sie NSS.
- Aktivieren Sie PAM in NetWitness-Server.
- Konfigurieren Sie Gruppenzuordnungen in NetWitness-Server.

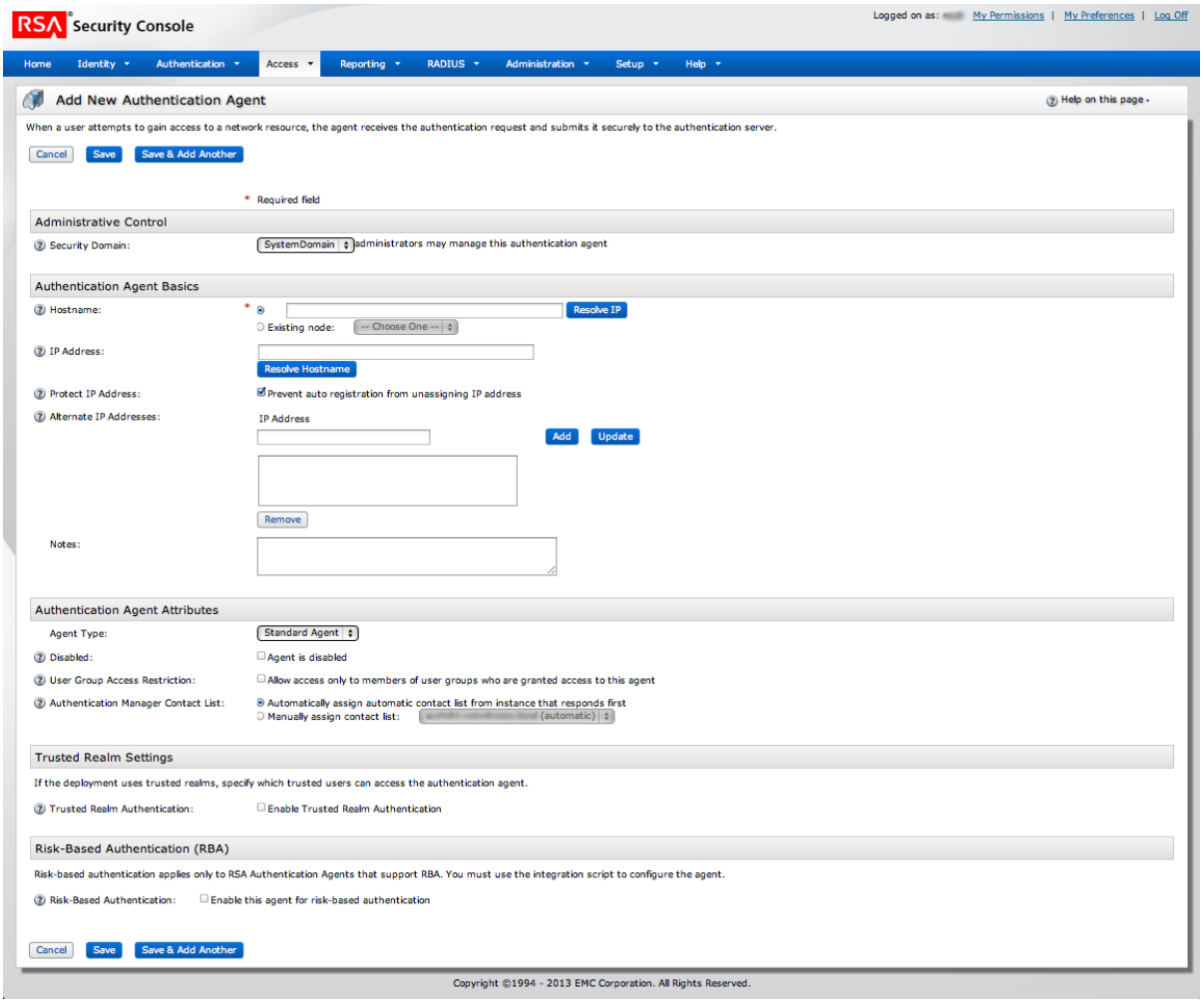
So konfigurieren Sie Authentication Manager:

1. Melden Sie sich bei RSA Authentication Manager an.
   Die Sicherheitskonsole wird angezeigt.

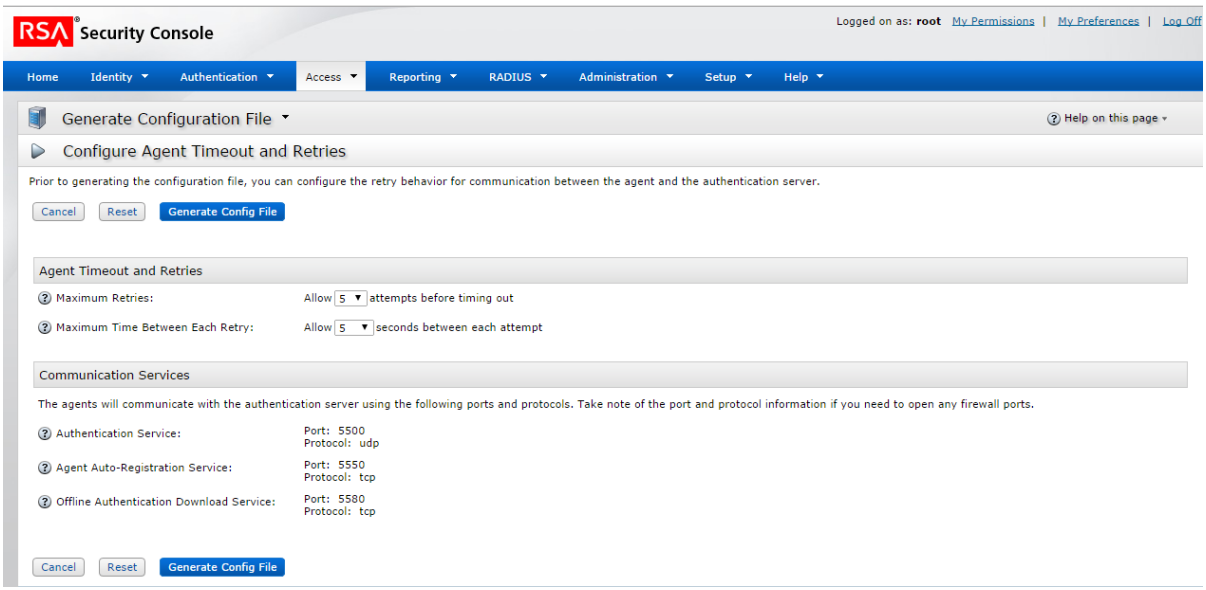


2. Fügen Sie in der Sicherheitskonsole einen neuen Authentifizierungs-Agent hinzu.
   Klicken Sie auf **Zugriff > Authentifizierungs-Agent > Neu hinzufügen**

.Die Seite „Neuen Authentifizierungs-Agent hinzufügen“ wird angezeigt.



3. Geben Sie im Feld **Hostname** den Hostnamen von NetWitness-Server ein.
4. Klicken Sie auf **IP auflösen**.
   Die IP-Adresse von NetWitness-Server wird automatisch im Feld **IP-Adresse** angezeigt.
5. Behalten Sie die Standardeinstellungen bei und klicken Sie auf **Speichern**.
6. Erzeugen Sie eine Konfigurationsdatei.
   Navigieren Sie zu **Zugriff > Authentifizierungs-Agent > Konfigurationsdatei erzeugen**.
   Die Seite „Konfigurationsdatei erzeugen“ wird angezeigt.



7. Behalten Sie die Standardeinstellungen bei und klicken Sie auf **Konfigurationsdatei erzeugen**.
   Dies erzeugt **AM_Config.zip** mit zwei Dateien.
8. Klicken Sie auf **Jetzt herunterladen**.

So installieren und konfigurieren Sie das PAM-SecurID-Modul:

1. Legen Sie auf dem NetWitness-Server ein Verzeichnis an:
   `mkdir /var/ace`
2. Kopieren Sie auf dem NetWitness-Server die Datei `sdconf.rec` aus der ZIP-Datei in das Verzeichnis `/var/ace`.
3. Erstellen Sie die Textdatei `sdopts.rec` im Verzeichnis `/var/ace`.
4. Fügen Sie die folgende Zeile ein:
   `CLIENT_IP=<IP address of NetWitness-Server>`
5. Installieren Sie den SecurID-Autorisierungs-Agent für PAM, der im yum-Repository verfügbar ist:
   `yum install sid-pam-installer`
6. Führen Sie das Installationsskript aus:
   `/opt/rsa/pam-agent-installer/install_pam.sh`
7. Befolgen Sie die Eingabeaufforderungen, um die Standardeinstellungen zu akzeptieren oder zu ändern.

8. Bearbeiten Sie die NetWitness-Server-PAM-Konfigurationsdatei `/etc/pam.d/securityanalytics`, um die folgende Zeile hinzuzufügen. Wenn die Datei nicht vorhanden ist, erstellen Sie sie und fügen Sie die folgende Zeile hinzu:
   `auth sufficient pam_securid.so`

Damit ist die Installation des SecurID-PAM-Moduls abgeschlossen. Testen Sie als Nächstes die Verbindung und die Authentifizierung. Befolgen Sie dann die Verfahren in „Konfigurieren und Testen des NSS-Services“.

Hinweis: Wenn die PAM-SecurID-Konfiguration nicht abgeschlossen ist, kann der Jetty-Server abstürzen und die NetWitness Suite-Benutzeroberfläche wird nicht angezeigt. Sie müssen warten, bis die Konfiguration der PAM-Authentifizierung abgeschlossen ist. Starten Sie dann den Jetty-Server neu.

So testen Sie Verbindung und Authentifizierung:

1. Führen Sie `/opt/pam/bin/64bit/acetest` aus und geben Sie den **Benutzernamen** und **Passcode** ein.
2. (Optional) Wenn acetest fehlschlägt, aktivieren Sie das Debugging:
   `vi/etc/sd_pam.conf`
   `RSATRACELEVEL=15`
3. Führen Sie `/opt/pam/bin/64bit/acestatus` aus. Ausgabe unten

```
RSA ACE/Server Limits
 ---------------------
 Configuration Version : 15 Client Retries : 5
 Client Timeout : 5 DES Enabled : Yes

RSA ACE/Static Information
 --------------------------
 Service : securid Protocol : udp Port Number : 5500

RSA ACE/Dynamic Information
 ---------------------------
 Server Release : 8.1.0.0 Communication : 5

RSA ACE/Server List
 -------------------
 Server Name :  auth81.netwitness.local
 Server Address :  192.168.100.10
 Server Active Address : 192.168.100.10
 Master : Yes Slave : No Primary : Yes
 Usage : Available for Authentications
```

4. (Optional) Navigieren Sie zum Beheben von Problemen mit dem Authentication Manager-Server
   zu **Reporting > Echtzeit-Aktivitätsüberwachung > Authentifizierungs-**

Aktivitätsüberwachung.

Klicken Sie dann auf **Überwachung starten**.

5. Wenn Sie die Einstellung geändert haben, setzen Sie RSATRACELEVEL auf 0 zurück:
   `vi/etc/sd_pam.conf`
   `RSATRACELEVEL=0`

Achtung: Überprüfen Sie nach der Installation, ob VAR_ACE in der Datei `/etc/sd_pam.conf` auf den korrekten Speicherort der Datei sdconf.rec verweist. Dies ist der Pfad zu den Konfigurationsdateien. Der hierfür erforderliche Befehl lautet: `chown -R netwitness:netwitness /var/ace`.

Damit ist die Konfiguration des PAM-Agent für SecurID abgeschlossen. Fahren Sie jetzt mit dem nächsten Abschnitt fort: *Konfigurieren und Testen des NSS-Services*.

Konfigurieren und Testen des NSS-Services

Wählen Sie einen NSS-Service aus.

Es stehen drei NSS-Services zur Auswahl: Samba, LDAP und UNIX. Jede der drei Methoden ist mit Vor- und Nachteilen verbunden.

NSS Samba – Vorteile	NSS Samba – Nachteile
Speziell auf Active Directory zugeschnitten	Kann nicht mit anderen als Active Directory-Back-ends verwendet werden
Minimale bis gar keine Konfiguration von Active Directory erforderlich	Konfiguration und Troubleshooting potenziell schwieriger
Keine besonderen Benutzerkonten erforderlich	NW-Server-Rechner muss der Active Directory-Domain hinzugefügt werden
	Verwendet viele Ports für die Kommunikation mit Active Directory; Implementierung über Firewalls und Proxyserver hinweg schwieriger

NSS LDAP – Vorteile	NSS LDAP – Nachteile
Basiskonfiguration einfacher	Kann zusätzliche Konfiguration und Rollen innerhalb von Active Directory erfordern
Kann mit jeder LDAP-Implementation kommunizieren	Erfordert Konfiguration eines LDAP-Bind-Kontos
Verwendet einen einzigen TCP-Port für die Kommunikation - einfacher im Umgang mit Firewalls und Proxyserver	Schwieriger, sicheren Transport zu aktivieren, wenn nicht so konfiguriert, dass Serverzertifikate nicht validiert werden
Hinzufügen des NW-Hosts zur Active Directory-Domain nicht erforderlich	

NSS UNIX

Es ist keine Konfiguration zur Aktivierung des NSS-UNIX-Moduls erforderlich. Dieses ist bereits standardmäßig im Betriebssystem des Hosts aktiviert. Fügen Sie zur Autorisierung eines Benutzers für eine spezifische Gruppe diesen Benutzer einfach zum Betriebssystem und zur Gruppe hinzu:

1. Erstellen Sie eine Betriebssystemgruppe, um Ihren externen Benutzer mit diesem Befehl hinzuzufügen:
   `groupadd <groupname>`
2. Fügen Sie den externen Benutzer mit diesem Befehl dem Betriebssystem hinzu:
   `adduser -G <groupname> -M -N <externalusername>`

Hinweis: Beachten Sie, dass dies NICHT zum Zugriff auf die NW-Server-Konsole berechtigt.

Damit ist die Konfiguration für NSS UNIX abgeschlossen. Fahren Sie fort mit dem Abschnitt „Testen der NSS-Funktion“.

NSS Samba

Active Directory-Winbind-Kommunikationsports

Interne Tests legen nahe, dass mindestens die folgenden Ports geöffnet sein sollten, damit NSS Samba funktioniert. Diese werden nur zur Referenz bereitgestellt.

TCP 88 – Kerberos
TCP 139 – Netbios
TCP 389 – LDAP
UDP 53 – DNS
UDP 88 – Kerberos
UDP 389 – LDAP

Zusätzliche Ports können je nach standortspezifischen Implementierungsanforderungen erforderlich sein. Der folgende Artikel enthält Informationen zu allen Ports, die für die Active Directory-Kommunikation erforderlich sein können: http://technet.Microsoft.com/de-de/library/dd772723%28WS.10%29.aspx.

So konfigurieren Sie NSS Samba:

1. Bearbeiten Sie die Samba-Konfigurationsdatei `/etc/samba/smb.conf` wie folgt. Ersetzen Sie Variablen, die mit <Spitzklammern> abgesetzt sind, durch Ihre Werte und lassen Sie die Spitzklammern weg. Die angegebene Groß- und Kleinschreibung muss befolgt werden.

```
[global]
 workgroup = domain
 netbios name = <NW_APPLIANCE_HOSTNAME>
 password server = <ADSERVER.DOMAIN.COM>
 realm = <DOMAIN.COM>

 local master = no
 security = ads
 syslog only = yes
 log file = /var/log/samba/log.%m
 max log size = 5120
 idmap config * : range = 16777216-33554431
 template shell = /bin/bash
 winbind use default domain = true
 winbind offline logon = false
 winbind enum groups = yes
```

2. Geben Sie die folgenden Befehle ein, um den Windows-Binding-Service `winbind` zu aktivieren und zu starten:

```
systemctl enable winbind
systemctl start winbind
```

3. Bearbeiten Sie die NSS-Konfigurationsdatei, `/etc/nsswitch.conf`. Aktualisieren Sie nur die beiden unten stehenden Einträge und belassen Sie für die anderen die Standardwerte:

```
passwd:     files winbind
group:      files winbind
```

4. Geben Sie für den Beitritt zur Domain den folgenden Befehl ein:
   `net ads join -U <DomainAdminUser>`
5. Geben Sie zum Speichern der Domain-Controller-SID den folgenden Befehl ein:
   `net rpc getsid -S <SERVER.DOMAIN.COM>`
6. Testen Sie die NSS-Funktion, wie im Abschnitt *Testen der NSS-Funktion* beschrieben.
7. Wenn Sie festgestellt haben, dass NSS von der Befehlszeile aus richtig funktioniert, geben Sie den folgenden Befehl ein, um den Host neu zu starten, damit die Änderungen an NSS wirksam werden.
   `reboot`

So führen Sie ein Troubleshooting von NSS Samba durch:

So stellen Sie fest, ob NSS Winbind erfolgreich mit Active Directory kommunizieren kann:

1. Geben Sie die folgenden Befehle ein:
   `wbinfo -u`, um eine Liste der Active Directory-Benutzer zurückzugeben
   `wbinfo -g`, um eine Liste der Active Directory-Gruppen zurückzugeben
2. Wenn keiner der Befehle erfolgreich ist, führen Sie `winbind` im Konsolen-Debug-Modus aus, indem Sie die folgenden Befehle eingeben:
   ```
   systemctl stop winbind
   winbindd -S -F -d <optional debugleve 0-10>
   ```
3. Wiederholen Sie Schritt 1 in einer separaten ssh-Sitzung aus und untersuchen Sie die `winbindd`-Ausgabe auf Hinweise zu dem Problem.
   Erhöhen Sie die Ausführlichkeit von `winbindd` nach Bedarf.
4. Nehmen Sie alle notwendigen Anpassungen an `/etc/samba/smb.conf` vor.
5. Beenden Sie im `winbindd`-Debug-Fenster aus Schritt 2 `winbindd`, indem Sie `CTRL-C` eingeben.
   Wiederholen Sie die Schritte 1 und 2 und fahren Sie mit dem Troubleshooting fort, bis die `wbinfo`-Befehle erfolgreich sind.
6. Wenn die `wbinfo`-Befehle erfolgreich ausgeführt wurden, verwenden Sie die `getent`-Befehle aus dem Abschnitt „Testen der NSS-Funktion“ in diesem Leitfaden, um NSS zu testen.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
7. Wenn `getent` erfolgreich ausgeführt wurde, beenden Sie die Befehlszeile `winbindd`, indem Sie `CTRL-C` eingeben. Geben Sie dann den folgenden Befehl ein, um den Service-

Daemon zu starten:

```
systemctl start winbind
```

Wenn `wbinfo -g` von der Befehlszeile erfolgreich ist, aber die Suche nach externer Gruppenzuordnung keine Active Directory-Gruppen anzeigt:

1. Fügen Sie die folgenden Zeilen zu `/etc/samba/smb.conf` hinzu:
   ```
   allow trusted domains = no
   ```
2. Geben Sie `systemctl restart winbind` ein.

Damit ist die Konfiguration für NSS Samba abgeschlossen. Fahren Sie fort mit dem Abschnitt „Testen der NSS-Funktion“.

NSS LDAP

Hinweis: Diese Anweisungen erfordern, dass für alle Active Directory-PAM-Benutzer- und NSS-Gruppenobjekte die Attribute `uidNumber` und `gidNumber` auf UID- und GID-Nummern im UNIX-Stil festgelegt sind, damit sie von NSS LDAP verwendet werden können. Ältere Active Directory-Schemata verfügen möglicherweise nicht standardmäßig über diese Attribute. Neuere Active Directory-Schemata verfügen möglicherweise über diese Attribute, sie sind aber eventuell nicht in jedem Objekt definiert. Die korrekte Konfiguration dieser Attribute geht über den Rahmen dieses Dokuments hinaus. Wenden Sie sich an Ihren Active Directory-Administrator, um diese Attribute für Ihre PAM-Benutzer und NSS-Gruppen definieren zu lassen.

Ein LDAP-Bind-Benutzer muss in Active Directory erstellt werden, damit NSS verwendet werden kann. Dieser Benutzer muss so konfiguriert werden, dass sein Passwort nicht abläuft. Da diese Anmeldedaten für den NSS LDAP-Service in Klartext angegeben werden müssen, müssen die Berechtigungen von `/etc/nslcd.conf` auf dem Standardwert von 600 belassen werden, damit die Datei von keinen anderen Benutzern des Systems außer Root gelesen werden kann.

LDAP-Kommunikationsports – TCP 389 oder TCP 636

TCP 389 kann für unverschlüsselten und in den meisten Fällen auch für verschlüsselten Datenverkehr verwendet werden und ist in der Regel ausreichend. Die meisten modernen LDAP-Implementierungen unterstützen nach dem Verbinden mit Port 389 den Befehl `start_tls`, mit dem der Status der Verbindung von unverschlüsselt zu verschlüsselt hochgestuft wird. In dieser Instanz beginnen LDAP-URIs immer noch mit `ldap://`, auch wenn sie `start_tls` verwenden.

TCP 636 wird nur in Instanzen verwendet, in denen der LDAP-Server den Befehl `start_tls` nicht unterstützt. In dieser Instanz beginnen LDAP-URIs mit `ldaps://` und der Befehl `start_tls` wird nicht verwendet.

So konfigurieren Sie das NSS-Modul für LDAP mit Active Directory:

1. Rufen Sie das Paket `nss-pam-ldapd` aus dem SMCUPDATE-Repository oder aus dem Update-Repository für den NetWitness-Server ab, wenn der Server mit SMCUPDATE synchronisiert wird. Dies erfordert ein konfiguriertes Live-Konto in NetWitness Suite.
2. Führen Sie für die Installation des Pakets den folgenden Befehl aus:
   ```
   yum install nss-pam-ldapd
   ```
3. Bearbeiten Sie `/etc/nslcd.conf` so, dass die Zeilen unten enthalten sind, und vergewissern Sie sich dabei, dass alle vorhandenen Zeilen in der Datei zunächst mithilfe des Hash-Zeichens # am Anfang der Zeile auskommentiert sind:
   ```
   uid nslcd
   gid ldap
   uri ldap://<server.domain.com>
   base <dc=domain,dc=com>
   binddn <cn=binduser,dc=domain,dc=com
   bindpw <secret>
   ```
   Hinweis: Sie müssen zusätzliche Zuordnungen zwischen den NSS- und LDAP-Suchvorgängen für Ihre spezifische Umgebung hinzufügen. Genaue Details erhalten Sie auf der Linux-Manpage für nslcd.
4. (Optional) Wenn Sie einen sicheren Transport für die LDAP-Kommunikation mit Peer-Zertifikatüberprüfung (höhere Sicherheit) aktivieren möchten, finden Sie auf der Linux-Manpage für nslcd die korrekte Codeänderung für die Datei `/etc/nslcd.conf`.

Hinweis: Windows-Domain-Controller ermöglichen standardmäßig keinen sicheren LDAP-Transport. Sie erfordern die Installation eines Serverzertifikats für die Serverauthentifizierung. Abruf und Installation dieses Zertifikat auf dem DC gehen über den Umfang dieses Dokuments hinaus. Einige Informationen dazu sind verfügbar unter der folgenden URL: https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

5. (Optional) Wenn Sie einen sicheren Transport für die LDAP-Kommunikation ohne Peer-Zertifikat aktivieren möchten, finden Sie auf der Linux-Manpage für nslcd die korrekte Codeänderung für die Datei `/etc/nslcd.conf`.
6. Bearbeiten Sie die NSS-Konfigurationsdatei `/etc/nsswitch.conf`. Aktualisieren Sie nur die beiden unten stehenden Einträge und belassen Sie für die anderen die Standardwerte:
   ```
   passwd:files ldap
   group:files ldap
   ```

7. Geben Sie diese Befehle ein, um den NSLCD-Service zu aktivieren und zu starten:
   ```
   systemctl enable nslcd
   systemctl start nslcd
   ```
8. Testen Sie die NSS-Funktion anhand der Informationen im Abschnitt *Testen der NSS-Funktion*. Wenn die NSS-Tests fehlschlagen, führen Sie ein Troubleshooting von NSS LDAP wie in *Troubleshooting von NSS LDAP* beschrieben durch.
9. Wenn Sie überprüft haben, ob NSS von der Befehlszeile aus richtig funktioniert, starten Sie den Host neu, damit die Änderungen an NSS wirksam werden.
   ```
   reboot
   ```

So führen Sie ein Troubleshooting von NSS LDAP durch:

1. Beenden Sie für das Troubleshooting von NSS LDAP zunächst den nslcd-Service, indem Sie den folgenden Befehl eingeben:
   ```
   systemctl stop nslcd
   ```
2. Um Troubleshooting- und Statusinformationen vom Service an die Konsole auszugeben, führen Sie in der Befehlszeile den nslcd-Service im Debug-Modus aus:
   ```
   nslcd -d
   ```
3. (Optional) Fügen Sie zur Steigerung der Ausführlichkeit des Debuggings zusätzlich mehrmals den Buchstaben „d“ am Ende von „nslcd -d“ hinzu. Geben Sie also zum Beispiel den folgenden Befehl ein:
   ```
   nslcd -ddd
   ```
4. Verwenden Sie von einer separaten ssh-Sitzung aus die `getent`-Befehle aus dem Abschnitt „Testen der NSS-Funktion“ in diesem Leitfaden, um NSS zu testen. Untersuchen Sie die Debug-Ausgabe von nslcd auf Hinweise, wo der Fehler auftritt. Erhöhen Sie die Ausführlichkeit des Debuggings von nslcd nach Bedarf.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
5. Nehmen Sie alle notwendigen Anpassungen an `/etc/nslcd.conf` basierend auf der Ausgabe von Schritt 2 oder 3 vor.
6. Beenden Sie im nslcd-Debug-Fenster aus Schritt 2 oder 3 `nslcd` mit `CTRL-C`. Wiederholen Sie Schritt 2 oder 3 und fahren Sie mit dem Troubleshooting fort, bis der Befehl `getent` erfolgreich ist.
7. Wenn `getent` erfolgreich ist, beenden Sie die Befehlszeile `nslcd` und starten Sie den Service-Daemon:
   ```
   systemctl start nslcd
   ```

Folgende Probleme treten häufiger auf:

- Das SSL-Zertifikat für sicheren LDAP-Transport ist nicht auf dem LDAP/Active Directory-Server installiert.
- Die Überprüfung des CA-Zertifikats ist fehlgeschlagen. Kommentieren Sie die Zeile `tls_cacert` in `/etc/nslcd.conf` aus und versuchen Sie es stattdessen mit `tls_reqcert never`. Wenn das Erfolg hat, wissen Sie, dass die Zertifikatüberprüfung fehlgeschlagen ist.
  - Das Zertifikat der Stammzertifizierungsstelle ist nicht im PEM-Format.
  - Es wird das Zertifikat der ausgebenden Zertifizierungsstelle, nicht der Stammzertifizierungsstelle verwendet.
  - Der Name des SSL-Zertifikats des LDAP-Servers entspricht nicht seinem Hostnamen.
- Basis-DN ist nicht korrekt.
- LDAP-Bind-Benutzer oder -Passwort nicht korrekt angegeben
- Fälschlicherweise ist `ldaps://` statt `ldap://` in Zeile `uri` von `/etc/nslcd.conf` angegeben. `ldaps://` darf nur verwendet werden, wenn LDAPS verwendet wird, jedoch nicht mit dem Befehl `start_tls`.
- Bei Active Directory-Benutzern und -Gruppen ist das Attribut `uidNumber` oder `gidNumber` nicht festgelegt.
- Die Firewall des Netzwerks blockiert die Kommunikation.
- Der Hostname des angegebenen LDAP-Servers kann nicht aufgelöst werden.
  - Falsche DNS-Einstellungen in `/etc/resolv.conf`
  - Falscher Hostname in Zeile `uri` von `/etc/nslcd.conf` angegeben

Damit ist die Konfiguration für NSS LDAP abgeschlossen. Fahren Sie fort mit dem Abschnitt „Testen der NSS-Funktion“.

Testen der NSS-Funktion

Verwenden Sie die folgenden Befehle, um zu testen, ob NSS mit allen vorherigen NSS-Services funktioniert:

```
getent passwd <pamUser>
 getent group <groupOfPamUser>
```

Die Ausgabe sollte ähnlich aussehen wie:

```
[root@~]# getent passwd myuser
 myuser:*:10000:10000::/home/myuser:/bin/sh
```

```
[root@~]# getent group mygroup
 mygroup:*:10000:myuser3
```

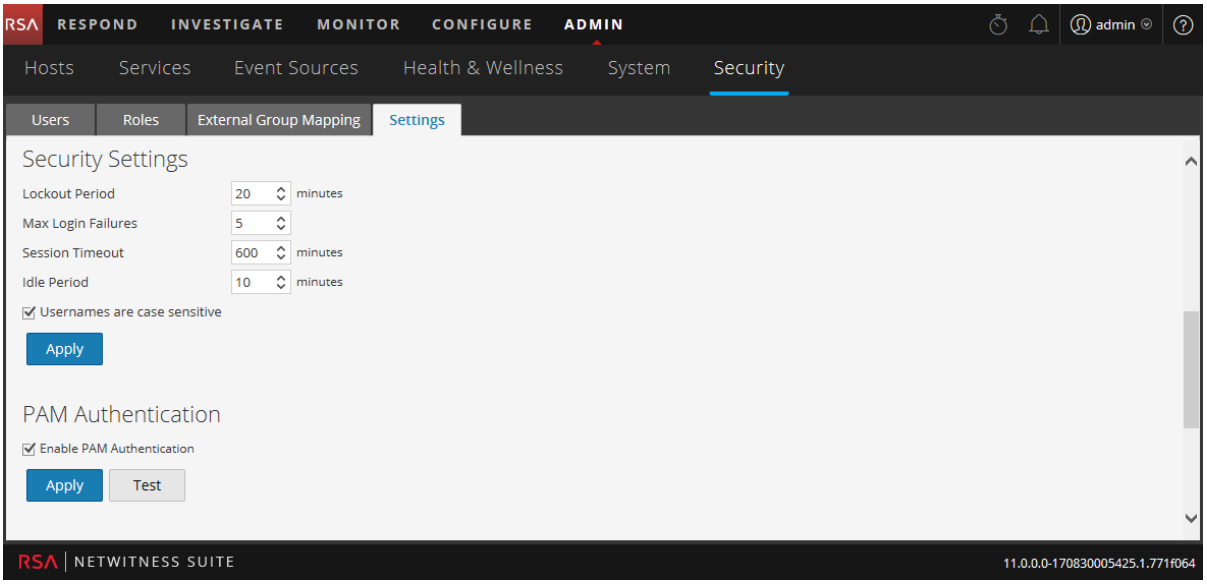
- Wenn keiner der Befehle eine Ausgabe generiert, funktioniert NSS für die externe Autorisierung nicht einwandfrei. Konsultieren Sie die Troubleshooting-Informationen für Ihr NSS-Modul in diesem Dokument.
- Wenn die `getent`-Befehle erfolgreich ausgeführt wurden und die erfolgreiche Authentifizierung in `/var/log/secure` bestätigt wird, NetWitness Suite jedoch die Anmeldung externer Benutzer weiterhin nicht zulässt:
  - Wurde der richtige Gruppenname für die NSS-Gruppe in der externen Gruppenzuordnung von NW angegeben? Siehe „Aktivieren von PAM“ und „Erstellen von Gruppenzuordnungen“ unten.
  - Es ist möglich, dass die NSS-Konfiguration geändert wurde und NetWitness Suite die Änderung nicht übernommen hat. Nach einem Neustart des NetWitness Suite-Hosts werden die Änderungen an der NSS-Konfiguration in NetWitness Suite wirksam. Ein Neustart von `jetty` ist nicht ausreichend.

Fahren Sie mit dem nächsten Abschnitt fort: „Aktivieren von PAM in NetWitness-Server“.

Aktivieren Sie PAM in NetWitness-Server.

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Administration > Sicherheit“ wird mit geöffneter Registerkarte „Benutzer“ angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.

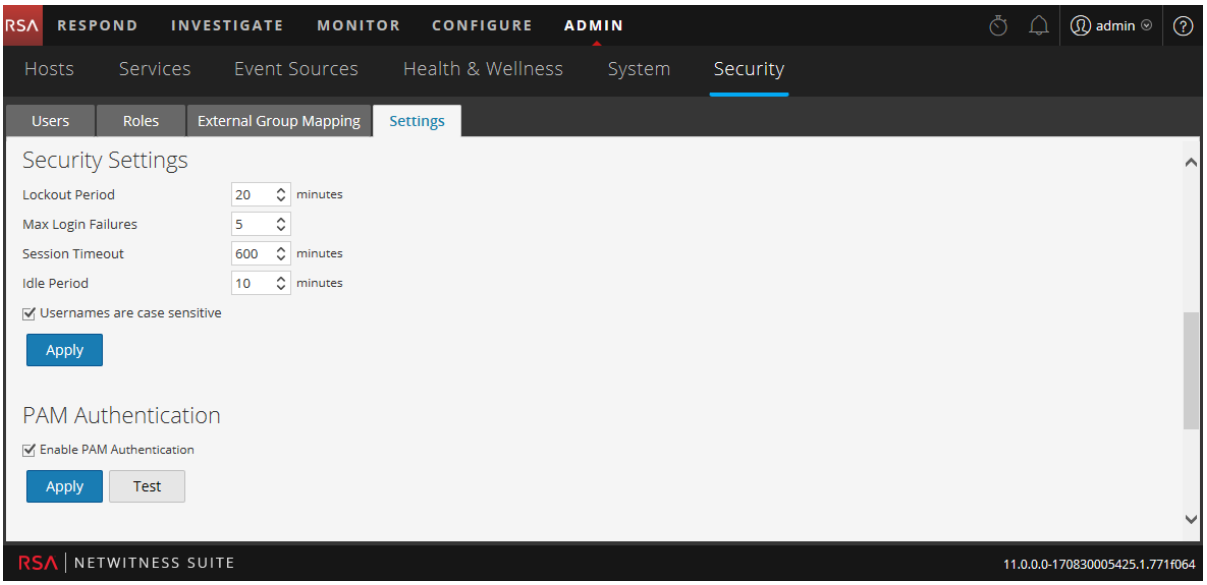
3. Wählen Sie unter **PAM-Authentifizierung** die Option **PAM-Authentifizierung aktivieren** aus und klicken Sie auf **Anwenden**.



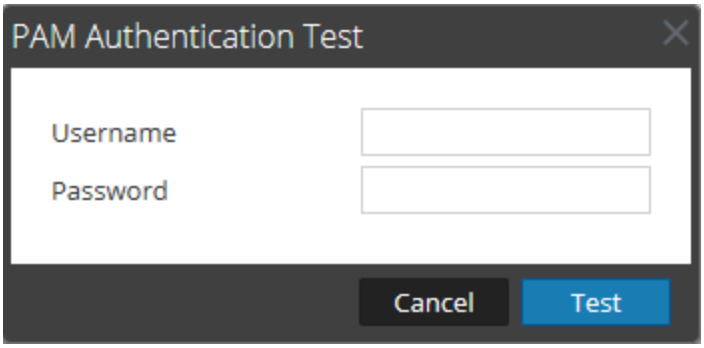
Testen der PAM-Authentifizierung

So testen Sie die externe Authentifizierung für PAM:

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie unter **PAM-Authentifizierung** die Option **PAM-Authentifizierung aktivieren** aus.



4. Klicken Sie unter **PAM-Authentifizierung** auf **Testen**.
   Das Dialogfeld **PAM-Authentifizierungstest** wird angezeigt.



5. Geben Sie einen Benutzernamen und ein Passwort ein, die Sie zur Authentifizierung mit der aktuellen PAM-Konfiguration testen möchten.
6. Klicken Sie auf **Testen**.
   Die externe Authentifizierungsmethode wird getestet, um die Konnektivität sicherzustellen
7. Wenn der Test fehlgeschlagen ist, überprüfen und bearbeiten Sie die Konfiguration.

PAM wurde aktiviert und die Active Directory-Konfigurationen bleiben ebenfalls aktiviert. PAM-Konfigurationen werden automatisch auf der Registerkarte „Externe Gruppenzuordnung“ aufgeführt, sodass Sie jeder Gruppe Sicherheitsrollen zuordnen können. Wie Sie Sicherheitsrollen für den PAM-Zugriff konfigurieren, erfahren Sie unter Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen.

So funktioniert Role-Based Access Control

In diesem Thema wird die Role-Based Access Control (RBAC, rollenbasierte Zugriffskontrolle) erläutert, bei der eine vertrauenswürdige Verbindung zwischen NetWitness-Server und einem Core-Service besteht.

In RSA NetWitness® Suite legen Rollen fest, welche Aktionen Benutzer ausführen können. Einer Rolle sind Berechtigungen zugewiesen. Sie müssen jedem Benutzer eine Rolle zuweisen. Der Benutzer hat dann die Berechtigung, zu tun, was die Rolle erlaubt.

Vorkonfigurierte Rollen

Um die Erstellung von Rollen und die Zuweisung von Berechtigungen zu vereinfachen, gibt es in NetWitness Suite vorkonfigurierte Rollen. Sie können auch Rollen hinzufügen, die an Ihr Unternehmen angepasst wurden.

Die folgende Tabelle listet alle vorkonfigurierten Rollen und die zugewiesen Berechtigungen auf. Alle Berechtigungen sind der Administratorrolle zugewiesen. Allen anderen Rollen ist ein Teilsatz der Berechtigungen zugewiesen.

Rolle	Berechtigung
Administratoren	Voller Systemzugriff. Der Rolle des Systemadministrators sind standardmäßig alle Berechtigungen zugewiesen.
Operatoren	Zugriff auf die Konfigurationen, aber nicht auf Meta- und Sitzungsinhalte. Die Rolle des System Operators konzentriert sich auf die Systemkonfiguration, umfasst jedoch nicht Investigation, ESA, Alerting, Reporting und Respond.
Analysten	Zugriff auf Meta- und Sitzungsinhalte, aber nicht auf Konfigurationen. Die Rolle des SOC-Analysten (Security Operation Center) konzentriert sich auf Investigation, ESA, Alerting, Reporting und Respond, umfasst jedoch nicht die Systemkonfiguration.
Respond_ Administrator	Zugriff auf alle Respond-Berechtigungen.

Rolle	Berechtigung
SOC_Managers	Gleicher Zugriff wie Analysten sowie zusätzliche Berechtigung für das Verarbeiten von Incidents. Die Rolle des SOC-Managers ist identisch mit der des Analysten, umfasst jedoch die zur Konfiguration von Respond erforderlichen Berechtigungen.
Malware_ Analysts	Zugriff auf Ermittlungen und Schadsoftware-Ereignisse. Die Rolle des Schadsoftwareanalysten erlaubt nur den Zugriff auf das Malware Analysis-Modul.
Data_Privacy_ Officers	Die Rolle des DPO (Data Privacy Officer, Datenschutzbeauftragter) ist ähnlich der des Administrators, mit zusätzlichem Fokus auf Konfigurationsoptionen, die Verschleierung und die Anzeige sensibler Daten innerhalb des Systems managen (siehe *Datenschutzmanagement*). Benutzer mit der Rolle DPO können sehen, welche Metaschlüssel zur Verschleierung markiert sind, und sie sehen auch verborgene Metaschlüssel und Werte, die für die markierten Metaschlüssel erstellt wurden.

Vertrauenswürdige Verbindung zwischen Server und Service

In einer vertrauenswürdigen Verbindung vertraut ein Service explizit NetWitness-Server, um Benutzer zu managen und zu authentifizieren. Hierdurch wird der Verwaltungsaufwand für den jeweiligen Service reduziert, da authentifizierte Benutzer nicht lokal in den einzelnen Core-Services definiert werden müssen.

Wie die folgende Tabelle zeigt, werden alle Benutzermanagementaufgaben auf dem Server durchgeführt.

Aufgabe	Location
Hinzufügen von Benutzern	Server
Benutzernamen verwalten	Server
Passwörter verwalten	Server

Aufgabe	Location
Interne Benutzer von NetWitness Suite authentifizieren	Server
(Optional) Externe Benutzer authentifizieren mit:	
- Active Directory	Server
- PAM	Server
PAM installieren und konfigurieren	Server

Vertrauenswürdige Verbindung und zentrales Benutzermanagement haben folgende Vorteile:

- Sie führen alle Benutzermanagementaufgaben nur einmal und nur auf NetWitness-Server durch.
- Sie haben die Kontrolle über den Zugriff auf Services, müssen aber keine Benutzer für die Services einrichten und authentifizieren.
- Benutzer geben Passwörter nur einmal bei der Anmeldung bei NetWitness Suite an und werden vom Server authentifiziert.
- Benutzer, die bereits vom Server authentifiziert wurden, können in „ADMIN > Services“ auf alle Core-Services zugreifen, ohne ein Passwort einzugeben.

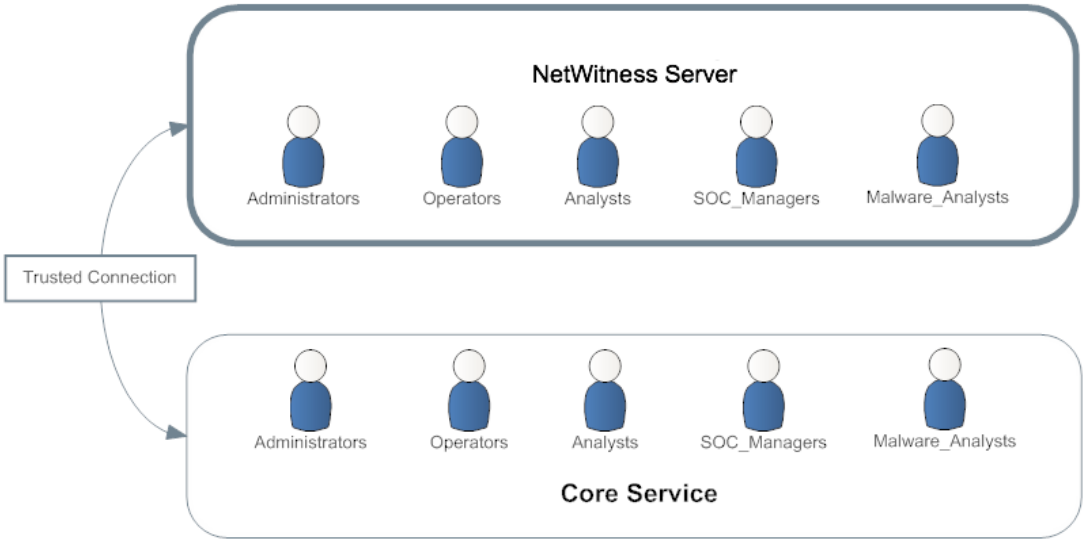
So werden vertrauenswürdige Verbindungen hergestellt

Wenn Sie die Version 11.0 installieren oder ein Upgrade auf diese Version durchführen, werden vertrauenswürdige Verbindungen standardmäßig mit zwei Einstellungen hergestellt:

1. SSL ist aktiviert.
2. Der Core-Service ist mit einem verschlüsselten SSL-Port verbunden.

Gemeinsame Rollennamen auf dem Server und bei Services

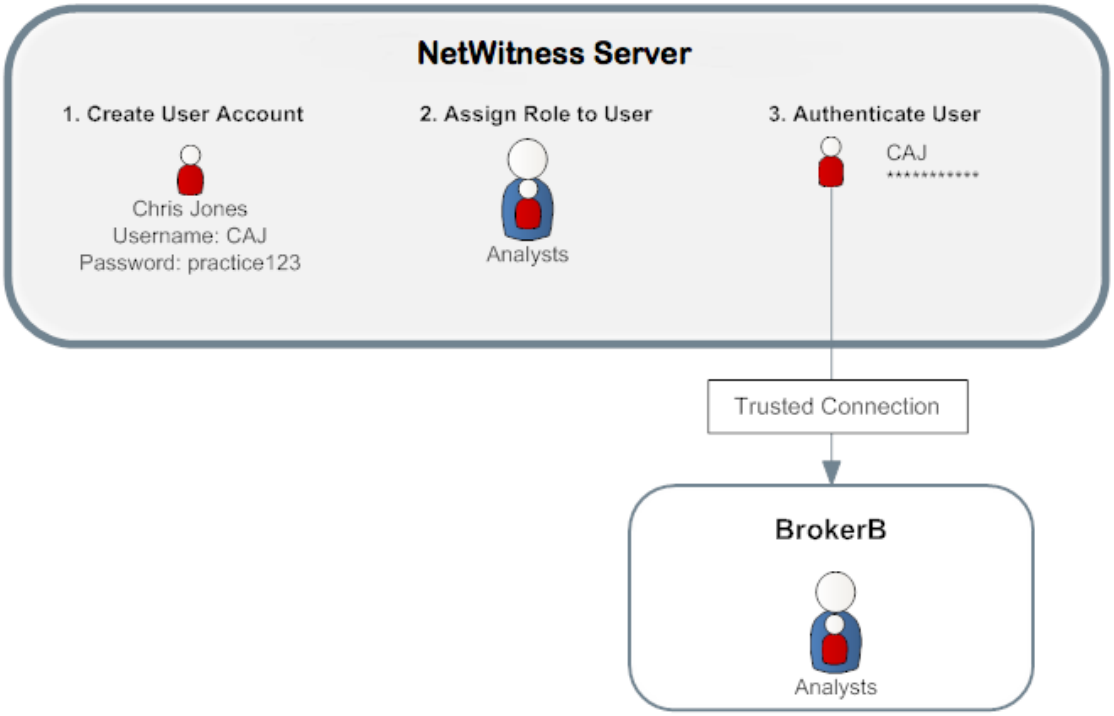
Vertrauenswürdige Verbindungen funktionieren nur, wenn die Rollennamen auf dem Server und beim Service gleich sind. Bei einer Neuinstallation installiert NetWitness Suite die fünf vorkonfigurierten Rollen auf dem Server und jedem Core-Service.



Wenn Sie eine benutzerdefinierte Rolle wie „JuniorAnalysts“ hinzufügen, müssen Sie die Rolle für jeden Dienst wie ArchiverA und BrokerB. Bei Rollennamen wird zwischen Groß-/Kleinschreibung unterschieden, sie dürfen keine Leerzeichen enthalten und müssen identisch sein. Beispiel: „JuniorAnalyst“ (Singular) und „JuniorAnalysts“ (Plural) erfüllen nicht die Anforderungen für gleiche Rollennamen.

End-to-End-Workflow für Benutzer-Setup und Servicezugriff

In diesem Workflow wird gezeigt, wie der rollenbasierte Zugriff funktioniert, wenn eine vertrauenswürdige Verbindung zwischen NetWitness-Server und dem BrokerB-Service besteht.



1. Erstellen Sie auf NetWitness-Server ein Konto für einen neuen Benutzer:
   Name: Chris Jones
   Benutzername: CAJ
   Passwort: practice123
2. Entscheiden Sie, ob Sie Chris Jones eine vorkonfigurierte oder benutzerdefinierte Rollen zuweisen möchten:
   - **Vorkonfigurierte Rolle**
     a. Behalten Sie die Standardberechtigungen bei, die der Rolle **Analysts** zugewiesen sind, oder ändern Sie sie. Hierzu gehören Berechtigungen wie der Zugriff auf die Module Alerting, Investigation und Malware.
     b. Weisen Sie Chris Jones die Rolle des Analysten zu.
   - **Benutzerdefinierte Rolle**
     a. Erstellen Sie die benutzerdefinierte Rolle, z. B. „JuniorAnalysts“.
     b. Weisen Sie der Rolle **JuniorAnalysts** Berechtigungen zu.
     c. Weisen Sie Chris Jones die Rolle „JuniorAnalysts“ zu.
     d. Fügen Sie die Rolle JuniorAnalysts dem Service hinzu, z. B. BrokerB.

3. Der Benutzer Chris Jones meldet sich bei NetWitness-Server an:
   Benutzername: CAJ
   Passwort: practice123
4. Der Server authentifiziert Chris.
5. Die vertrauenswürdige Verbindung erlaubt dem authentifizierten Benutzer Chris den Zugriff auf BrokerB ohne Eingabe eines weiteren Passworts.

Detailliertere Beschreibungen und Verfahren finden Sie unter Managen von Benutzern mit Rollen und Berechtigungen.

Verwandtes Thema

- Rollenberechtigungen

Rollenberechtigungen

In diesem Thema werden die Zugriffsrechte auf die Benutzeroberfläche beschrieben, die Benutzer mit vordefinierten NetWitness Suite-Systemrollen standardmäßig haben.

In NetWitness Suite ist der Benutzerzugriff auf Module, Dashlets und Ansichten von den zugewiesenen Berechtigungen abhängig, die in diesem Thema beschrieben werden. Sie können diese Rollenberechtigungen im Dialogfeld „Rollen hinzufügen“ oder „Rollen bearbeiten“ auf der Registerkarte „Administration > Sicherheit > Rollen“ suchen.

Im Dialogfeld „Rolle hinzufügen“ oder „Rolle bearbeiten“ stellen die Registerkarten im Abschnitt „Berechtigungen“ verschiedene Bereiche von NetWitness Suite dar und es werden die verfügbaren Berechtigungen für diese Bereiche angezeigt. Auf der Registerkarte „Administration“ werden beispielsweise die verfügbaren Berechtigungen in der Administrationsansicht angezeigt.

Hinweis: In den Dialogfeldern „Rolle hinzufügen“ und „Rolle bearbeiten“ gibt keine Registerkarte „Konfiguration“, die der Konfigurationsansicht entspricht. Um Berechtigungen in der Konfigurationsansicht zuzuweisen, weisen Sie sie den in der Konfigurationsansicht enthaltenen Ansichten zu: Live-Inhalte (Live), Regeln des Vorfalls (Incidents), ESA-Regeln (Altering), Abonnements (Live) und benutzerdefinierte Feeds (Live).

Hinweis: Links neben der Registerkarte „Administration“ befindet sich eine mit einem Sternchen (*) gekennzeichnete Registerkarte. Auf dieser Registerkarte wird nur der Zugriff auf das Management der Back-end-Services angezeigt.

In den folgenden Tabellen sind die Standardberechtigungen angegeben, die der jeweiligen NetWitness Suite-Benutzerrolle zugewiesen sind:

- Administratoren
- Operatoren
- Analysten
- Respond-Administrator
- SOC-Manager
- Malware Analysts (MA)
- Data Privacy Officers (DPO)

Da die Administratorrolle standardmäßig alle Berechtigungen besitzt, wird sie nicht in den Tabellen aufgeführt.

Format der Serviceberechtigungen für neue Services

Die Serviceberechtigungen für einige neue NetWitness Suite-Services enthalten drei Komponenten im folgenden Format:

```
<service name>.<resource>.<action>
```

Beispiel für die Berechtigung **investigate-server.metrics.read**:

- service name = **investigate-server**
- resource = **metrics**
- action = **read**

Benutzer, denen diese Berechtigung zugewiesen wurde, können alle Metriken lesen, die der Service „investigate-server“ bereitstellt.

Administration

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Administration“ aufgeführt: Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Auf Administration-Modul zugreifen	Ja	Ja	Ja	Ja	Ja
Zugreifen auf Integrität und Zustand	Ja	Ja	Ja	Ja	Ja
Systemupdates anwenden	Ja				
Teilnahme an der Live-Intelligence-Freigabe	Ja				
Globales Auditing managen	Ja				Ja
Managen der Integritäts- und Zustandsrichtlinie	Ja				

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Erweiterte Einstellungen managen	Ja				
Auditing managen	Ja				Ja
E-Mail managen	Ja				
LLS managen	Ja				
Protokolle managen	Ja				Ja
Benachrichtigungen managen	Ja				
Plug-ins managen	Ja				
Prädikate managen	Ja				
Rekonstruktion managen	Ja				
Sicherheit managen	Ja				Ja
Services managen	Ja				Ja
Systemeinstellungen managen	Ja				
Einstellungen für ESA ändern	Ja				
Ereignisquellen ändern	Ja				
Hosts ändern	Ja				
Services ändern	Ja				Ja
Ereignisquellen anzeigen	Ja		Ja		
Anzeigen der Integritäts- und Zustandsrichtlinie	Ja	Ja	Ja		

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Anzeigen des Statistikbrowsers von Integrität und Zustand	Ja	Ja	Ja		Ja
Hosts anzeigen	Ja				Ja
Services anzeigen	Ja				Ja

Admin-server

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte „Admin-server“ aufgeführt. Die Administratorrolle verfügt über sämtliche Berechtigungen und ist die einzige Rolle mit standardmäßig erteilten Berechtigungen.

Berechtigung	Beschreibung
admin-server.configuration.manage	Berechtigung zum Anzeigen und Ändern aller Servicekonfigurationsparameter
admin-server.health.read	Berechtigung zum Lesen von Benachrichtigungen zur Integrität, die der Service bereitstellt
admin-server.logs.manage	Berechtigung zum Ändern von protokollbezogenen Konfigurationen
admin-server.metrics.read	Berechtigung zum Lesen von Metriken, die der Service bereitstellt
admin-server.process.manage	Berechtigung zum Starten und Beenden des Services
admin-server.security.manage	Berechtigung zum Bearbeiten von sicherheitsbezogenen Ressourcen (Passwörter, Schlüssel usw.)
admin-server.security.read	Berechtigung zum Lesen von sicherheitsbezogenen Ressourcen

Alerting

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Alerting“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Auf Alerting-Modul zugreifen	Ja	Ja	Ja		Ja
Regeln managen	Ja		Ja		Ja
Warnmeldungen anzeigen		Ja	Ja		Ja
Regeln anzeigen	Ja		Ja		Ja

Config-server

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte „Config-server“ aufgeführt. Die Administratorrolle verfügt über sämtliche Berechtigungen und ist die einzige Rolle mit standardmäßig erteilten Berechtigungen.

Berechtigung	Beschreibung
config-server.*	Alle Berechtigungen (alle unten genannten Berechtigungen)
config-server.configuration.manage	Berechtigung zum Anzeigen und Ändern aller Servicekonfigurationsparameter
config-server.health.read	Berechtigung zum Lesen von Benachrichtigungen zur Integrität, die der Service bereitstellt
config-server.logs.manage	Berechtigung zum Ändern von protokollbezogenen Konfigurationen
config-server.metrics.read	Berechtigung zum Lesen von Metriken, die der Service bereitstellt

Berechtigung	Beschreibung
config-server.process.manage	Berechtigung zum Starten und Beenden des Services
config-server.security.manage	Berechtigung zum Bearbeiten von sicherheitsbezogenen Ressourcen (Passwörter, Schlüssel usw.)
config-server.security.read	Berechtigung zum Lesen von sicherheitsbezogenen Ressourcen

Dashboard

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Dashboard“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Dashlet-Zugriff – Admin-Geräteliste	Ja	Ja	Ja		Ja
Dashlet-Zugriff – Admin-Geräteüberwachung	Ja				Ja
Dashlet-Zugriff – Administration-Neuigkeiten	Ja	Ja	Ja		Ja
Dashlet-Zugriff – Warnmeldungsvarianz		Ja	Ja		Ja
Dashlet-Zugriff – Alerting-Dashlet „Aktuelle Warnmeldungen“		Ja	Ja		Ja
Dashlet-Zugriff – Investigation – Dashlet „Jobs		Ja	Ja		Ja

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Dashlet-Zugriff – Ermittlungen Top-Werte		Ja	Ja		Ja
Dashlet-Zugriff – Betroffene Live-Ressourcen	Ja	Ja	Ja		Ja
Dashlet-Zugriff – Live – Dashlet „Neue Ressourcen	Ja	Ja	Ja		Ja
Dashlet-Zugriff – Live – Dashlet „Abonnements	Ja	Ja	Ja		Ja
Dashlet-Zugriff – Live – Dashlet „Aktualisierte Ressourcen	Ja	Ja	Ja		Ja
Dashlet-Zugriff – Schadsoftwarejobs		Ja	Ja		Ja
Dashlet-Zugriff– Reporting-Dashlet „Kürzlich ausgeführte Berichte“		Ja	Ja		Ja
Dashlet-Zugriff – Reporting-Dashlet „Diagramme“		Ja	Ja		Ja
Dashlet-Zugriff – Top-Warnmeldungen		Ja	Ja		Ja
Dashlet-Zugriff – Unified-Dashlet „RSA First Watch“	Ja	Ja	Ja		Ja
Dashlet-Zugriff – Unified-Dashlet „Verknüpfungen“	Ja	Ja	Ja		Ja

Esa-Analytics-server

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte „Esa-Analytics-server“ aufgeführt. Die Administrator- und die Operatorrolle verfügen über sämtliche Berechtigungen und sind die einzigen Rollen mit standardmäßig erteilten Berechtigungen.

Berechtigung	Beschreibung
esa-analytics-server.*	Alle Berechtigungen (alle unten genannten Berechtigungen)
esa-analytics-server.analytics.manage	Berechtigung zum Anzeigen und Ändern von ESA Analytics
esa-analytics-server.analytics.read	Berechtigung zum Anzeigen von ESA Analytics
esa-analytics-server.configuration.manage	Berechtigung zum Anzeigen und Ändern aller Servicekonfigurationsparameter
esa-analytics-server.health.read	Berechtigung zum Lesen von Benachrichtigungen zur Integrität, die der Service bereitstellt
esa-analytics-server.logs.manage	Berechtigung zum Ändern von protokollbezogenen Konfigurationen
esa-analytics-server.metrics.read	Berechtigung zum Lesen von Metriken, die der Service bereitstellt
esa-analytics-server.model.manage	Berechtigung zum Anzeigen und Ändern von ESA-Modellen
esa-analytics-server.model.read	Berechtigung zum Anzeigen von ESA-Modellen
esa-analytics-server.process.manage	Berechtigung zum Starten und Beenden des Services
esa-analytics-server.security.read	Berechtigung zum Lesen von sicherheitsbezogenen Ressourcen

Incidents

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Incidents“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Auf Incident-Modul zugreifen		Ja	Ja	Ja	Ja
Incident Management-Integration konfigurieren			Ja		Ja
Warnmeldungen und Incidents löschen					Ja
Regeln zum Umgang mit Warnmeldungen managen			Ja		Ja
Incidents anzeigen und managen		Ja	Ja	Ja	Ja

Ermittlung

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Untersuchen“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Auf Investigation-Modul zugreifen		Ja	Ja	Ja	Ja
Kontextabfrage		Ja	Ja	Ja	
Incidents aus Investigation erstellen		Ja	Ja	Ja	

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Listen aus Investigation managen		Ja	Ja	Ja	
In Ereignissen navigieren		Ja	Ja	Ja	Ja
In Werten navigieren		Ja	Ja	Ja	Ja

Investigate-server

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte „Investigate-server“ aufgeführt.

Berechtigung	Beschreibung
investigate-server.*	Alle Berechtigungen (alle unten genannten Berechtigungen)
investigate-server.configuration.manage	Berechtigung zum Ändern von Konfigurationseigenschaften für den Server
investigate-server.health.read	Berechtigung zum Lesen von Benachrichtigungen zur Integrität, die der Service bereitstellt
investigate-server.logs.manage	Berechtigung zum Ändern von protokollbezogenen Konfigurationen
investigate-server.metrics.read	Berechtigung zum Lesen von Metriken, die der Service bereitstellt
Investigate-server.process.manage	Berechtigung zum Starten und Beenden des Services
investigate-server.security.manage	Berechtigung zum Bearbeiten von sicherheitsbezogenen Ressourcen (Passwörter, Schlüssel usw.)
investigate-server.security.read	Berechtigung zum Lesen von sicherheitsbezogenen Ressourcen

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Investigate-server“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
investigate-server.*		Ja	Ja	Ja	Ja
investigate-server.configuration.manage					
investigate-server.health.read					
investigate-server.logs.manage					
investigate-server.metrics.read					
investigate-server.process.manage					
investigate-server.security.manage					
investigate-server.security.read					

Live

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Live“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Live					
Auf Live-Modul zugreifen	Ja	Ja	Ja		Ja
Live-Systemeinstellungen managen	Ja				

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Ressourcen					
Live-Ressourcen bereitstellen	Ja				Ja
Live-Feeds managen	Ja				Ja
Live-Ressourcen managen	Ja				Ja
Live-Ressourcen durchsuchen	Ja	Ja	Ja		Ja
Live-Ressourcendetails anzeigen	Ja	Ja	Ja		Ja

Orchestration-server

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte „Orchestration-server“ aufgeführt. Die Administrator-, Operator- und Data Privacy Officers-Rolle verfügen über sämtliche Berechtigungen und sind die einzigen Rollen mit standardmäßig erteilten Berechtigungen.

Berechtigung	Beschreibung
orchestration-server.*	Alle Berechtigungen (alle unten genannten Berechtigungen)
orchestration-server.configuration.manage	Berechtigung zum Anzeigen und Ändern aller Servicekonfigurationsparameter
orchestration-server.health.read	Berechtigung zum Lesen von Benachrichtigungen zur Integrität, die der Service bereitstellt
orchestration-server.logs.manage	Berechtigung zum Ändern von protokollbezogenen Konfigurationen
orchestration-server.metrics.read	Berechtigung zum Lesen von Metriken, die der Service bereitstellt

Berechtigung	Beschreibung
orchestration-server.process.manage	Berechtigung zum Starten und Beenden des Services
orchestration-server.security.manage	Berechtigung zum Bearbeiten von sicherheitsbezogenen Ressourcen (Passwörter, Schlüssel usw.)
orchestration-server.security.read	Berechtigung zum Lesen von sicherheitsbezogenen Ressourcen

Schadsoftware

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Schadsoftware“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Malware-Dateien herunterladen		Ja	Ja	Ja	Ja
Malware Analysis-Scan initiieren		Ja	Ja	Ja	Ja
Malware Analysis-Ereignisse anzeigen		Ja	Ja	Ja	Ja

Berichte

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Berichte“ aufgeführt. Die Administratorrolle besitzt standardmäßig alle Berechtigungen und wird daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Warnmeldung					

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
RE-Warnmeldung definieren		Ja	Ja		Ja
RE-Warnmeldungsdefinition exportieren		Ja	Ja		Ja
RE-Warnmeldungen managen		Ja	Ja		Ja
RE-Warnmeldungen anzeigen		Ja	Ja		Ja
Anzeigen von geplanten RE-Warnmeldungen		Ja	Ja		Ja
Diagramm					
Diagramm definieren		Ja	Ja		Ja
Diagramm löschen		Ja	Ja		Ja
Diagrammdefinition exportieren		Ja	Ja		Ja
Diagramme managen		Ja	Ja		Ja
Diagramme anzeigen		Ja	Ja		Ja
Liste					
Listen definieren		Ja	Ja		Ja
Liste löschen		Ja	Ja		Ja
Exportieren von Listen		Ja	Ja		Ja
Listen managen		Ja	Ja		Ja
Bericht					
Bericht definieren		Ja	Ja		Ja
Bericht löschen		Ja	Ja		Ja

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Bericht exportieren		Ja	Ja		Ja
Berichte managen		Ja	Ja		Ja
Berichte anzeigen		Ja	Ja		Ja
Berichte					
Auf Konfiguration zugreifen		Ja	Ja		Ja
Auf Reporter-Modul zugreifen		Ja	Ja		Ja
Auf Reporter-Suche zugreifen		Ja	Ja		Ja
Auf Ansicht zugreifen		Ja	Ja		Ja
Regel					
RE-Warnmeldungsdefinition aus Regel hinzufügen		Ja	Ja		Ja
Regel definieren		Ja	Ja		Ja
Regel löschen		Ja	Ja		Ja
Regel exportieren		Ja	Ja		Ja
Regeln managen		Ja	Ja		Ja
Regelnutzung anzeigen		Ja	Ja		Ja
Planungen					
Plan definieren		Ja	Ja		Ja
Plan löschen		Ja	Ja		Ja
Zeitpläne anzeigen		Ja	Ja		Ja
Warehouse Analytics					

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
Jobs definieren		Ja	Ja		Ja
Jobs löschen		Ja	Ja		Ja
Jobs managen		Ja	Ja		Ja
Jobs anzeigen		Ja	Ja		Ja

Respond-server

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte „Respond-server“ aufgeführt.

Berechtigung	Beschreibung
respond-server.*	Alle Berechtigungen (alle unten genannten Berechtigungen)
respond-server.alert.delete	Berechtigung zum Löschen von Warnmeldungen
respond-server.alert.manage	Berechtigung zum Erstellen, Aktualisieren oder Löschen von Warnmeldungen
respond-server.alert.read	Berechtigung zum Anzeigen von Warnmeldungen
respond-server.alertrule.manage	Berechtigung zum Erstellen, Aktualisieren oder Löschen von Aggregationsregeln für Warnmeldungen
respond-server.alertrule.read	Berechtigung zum Anzeigen von Aggregationsregeln für Warnmeldungen
respond-server.configuration.manage	Berechtigung zum Ändern von Konfigurationseigenschaften für den Service
respond-server.health.read	Berechtigung zum Lesen von Benachrichtigungen zur Integrität, die der Service bereitstellt

Berechtigung	Beschreibung
respond-server.incident.delete	Berechtigung zum Löschen von Incidents
respond-server.incident.manage	Berechtigung zum Erstellen, Aktualisieren oder Löschen von Incidents
respond-server.incident.read	Berechtigung zum Anzeigen von Incidents
respond-server.journal.manage	Berechtigung zum Erstellen, Aktualisieren oder Löschen von Journaleinträgen für einen Incident
respond-server.journal.read	Berechtigung zum Anzeigen von Journaleinträgen für einen Incident
respond-server.logs.manage	Berechtigung zum Ändern von protokollbezogenen Konfigurationen
respond-server.metrics.read	Berechtigung zum Lesen von Metriken, die der Service bereitstellt
respond-server.process.manage	Berechtigung zum Starten und Beenden des Services
respond-server.remediation.manage	Berechtigung zum Erstellen, Aktualisieren oder Löschen von Korrekturaufgaben
respond-server.remediation.read	Berechtigung zum Anzeigen von Korrekturaufgaben
respond-server.security.manage	Berechtigung zum Bearbeiten von sicherheitsbezogenen Ressourcen (Passwörter, Schlüssel usw.)
respond-server.security.read	Berechtigung zum Lesen von sicherheitsbezogenen Ressourcen

In der folgenden Tabelle sind die zur jeweiligen Rolle zugewiesenen Berechtigungen der Registerkarte „Respond-server“ aufgeführt. Die Administrator- und Respond-Administratorrollen besitzen standardmäßig alle Berechtigungen und werden daher nicht aufgelistet.

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
respond-server.*					Ja
respond-server.alert.delete					
respond-server.alert.manage		Ja	Ja	Ja	
respond-server.alert.read		Ja	Ja	Ja	
respond-server.alertrule.manage			Ja		
respond-server.alertrule.read			Ja		
respond-server.configuration.manage					
respond-server.health.read					
respond-server.incident.delete					
respond-server.incident.manage		Ja	Ja	Ja	
respond-server.incident.read		Ja	Ja	Ja	
respond-server.journal.manage		Ja	Ja	Ja	
respond-server.journal.read		Ja	Ja	Ja	
respond-server.logs.manage					
respond-server.metrics.read					
respond-server.process.manage					

Berechtigung	Operatoren	Analysten	SOC-Manager	MA	DPO
respond-server.remediation.manage		Ja	Ja	Ja	
respond-server.remediation.read		Ja	Ja	Ja	
respond-server.security.manage					
respond-server.security.read					

Security-server

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte „Security-server“ aufgeführt. Die Administrator-, Operator- und Data Privacy Officers-Rolle verfügen über sämtliche Berechtigungen und sind die einzigen Rollen mit standardmäßig erteilten Berechtigungen.

Berechtigung	Beschreibung
security-server.*	Alle Berechtigungen (alle unten genannten Berechtigungen)
security-server.account.manage	Berechtigung zum Anzeigen, Erstellen, Ändern oder Entfernen von lokalen NetWitness Suite-Konten
security-server.account.read	Berechtigung zum Anzeigen von lokalen NetWitness Suite-Konten
security-server.configuration.manage	Berechtigung zum Anzeigen und Ändern aller Servicekonfigurationsparameter
security-server.health.read	Berechtigung zum Lesen von Benachrichtigungen zur Integrität, die der Service bereitstellt
security-server.logs.manage	Berechtigung zum Ändern von protokollbezogenen Konfigurationen

Berechtigung	Beschreibung
security-server.metrics.read	Berechtigung zum Lesen von Metriken, die der Service bereitstellt
security-server.permission.manage	Berechtigung zum Erstellen oder Entfernen von NetWitness Suite-Berechtigungen
security-server.process.manage	Berechtigung zum Starten und Beenden des Services
security-server.role.manage	Berechtigung zum Erstellen, Ändern oder Entfernen von NetWitness Suite-Rollen (z. B. Rollenberechtigungen hinzufügen)
security-server.role.read	Berechtigung zum Anzeigen von Rollendefinitionen für NetWitness Suite
security-server.security.manage	Berechtigung zum Bearbeiten von sicherheitsbezogenen Ressourcen (Passwörter, Schlüssel usw.)
security-server.security.read	Berechtigung zum Lesen von sicherheitsbezogenen Ressourcen
security-server.user.manage	Berechtigung zum Anzeigen, Erstellen, Ändern oder Entfernen von NetWitness Suite-Benutzerprofilen
security-server.user.read	Berechtigung zum Anzeigen der Details von NetWitness Suite-Benutzerprofilen (z. B. Rollen, Anmeldezeiten usw.)

Managen von Benutzern mit Rollen und Berechtigungen

In diesem Thema wird eine Reihe von End-to-End-Verfahren zum Managen von Benutzern in NetWitness Suite vorgestellt. Diese Schritte erläutern, wie Sie einen Benutzer in NetWitness Suite hinzufügen und dann festlegen, welche Aktionen der Benutzer ausführen kann.

Themen

Schritt 1. Überprüfen der vorkonfigurierten NetWitness-Rollen

Zur Vereinfachung der Erstellung von Rollen und der Zuweisung von Berechtigungen gibt es in NetWitness Suite vorkonfigurierte Rollen.

Rolle	Berechtigung
Administratoren	Voller Systemzugriff
Operatoren	Zugriff auf die Konfigurationen, aber nicht auf Meta- und Sitzungsinhalte
Analysten	Zugriff auf Meta- und Sitzungsinhalte, aber nicht auf Konfigurationen
Respond_ Administrator	Zugriff auf sämtliche Berechtigungen für Respond-Server und Incidents
SOC_Managers	Gleicher Zugriff wie Analysten sowie zusätzliche Berechtigung für das Verarbeiten von Incidents
Malware_ Analysts	Zugriff auf Schadsoftwareereignisse und Meta- sowie Sitzungsinhalt
Data_Privacy_ Officers	Zugriff auf Metadaten und Sitzungsinhalte sowie auf Konfigurationsoptionen für das Management der Verschleierung und Anzeige sensibler Daten innerhalb des Systems (siehe „Datenschutzmanagement“)

Der Administrator kann auch angepasste Rollen hinzufügen.

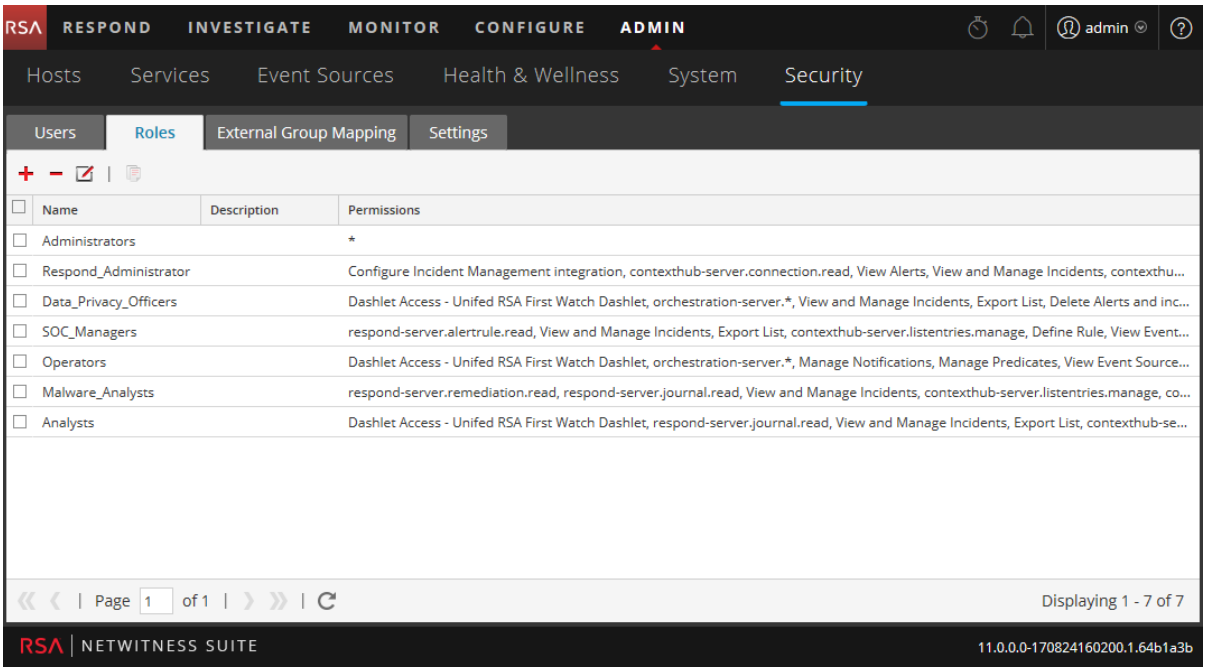
Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen

Obwohl NetWitness Suite über fünf vorkonfigurierte Rollen verfügt, können Sie benutzerdefinierte Rollen hinzufügen. Beispielsweise könnten Sie zusätzlich zur vorkonfigurierten Rolle Analyst benutzerdefinierte Rollen für AnalystEuropa und AnalystsAsien hinzufügen. Eine detaillierte Liste von Berechtigungen erhalten Sie unter Rollenberechtigungen.

Jedes der folgenden Verfahren beginnt auf der Registerkarte **Rollen**.

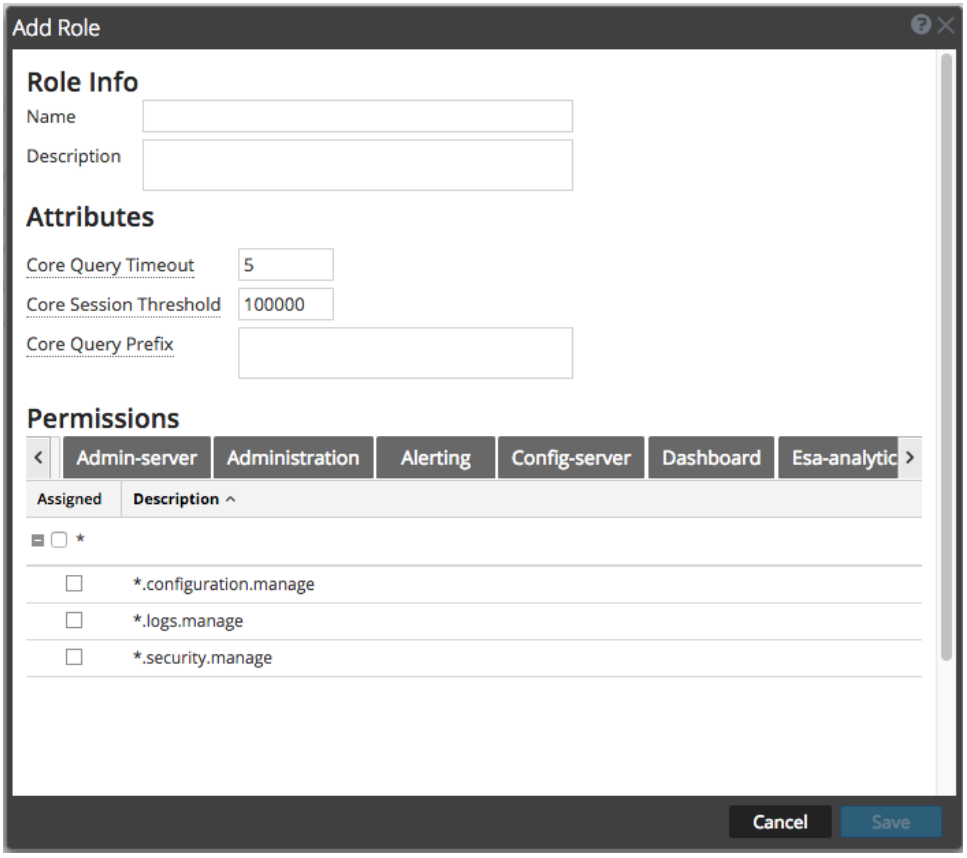
So navigieren Sie zur Registerkarte Rollen:

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Rollen**.



Hinzufügen einer Rolle und Zuweisen von Berechtigungen

1. Klicken Sie auf der Registerkarte **Rollen** in der Symbolleiste auf ✚.
2. Das Dialogfeld **Rolle hinzufügen** wird angezeigt.



3. Geben Sie im Abschnitt **Rolleninfo** die folgenden Informationen zu der Rolle ein:
   - **Name**
   - (Optional) **Beschreibung**
4. Geben Sie im Abschnitt **Attribute** die gewünschten Werte für jedes Attribut ein. Weitere Informationen zu den Attributen finden Sie unter Schritt 3. Überprüfen von Abfrage- und Sitzungsattributen pro Rolle.
5. Im Abschnitt **Berechtigungen**:
   - Klicken Sie auf ‹ und › , um durch die Module zu blättern.
   - Wählen Sie ein Modul aus, auf das die Rolle zugreifen wird.
   - Wählen Sie eine Berechtigung aus, die die Rolle haben soll.

6. Wiederholen Sie den vorherigen Schritt, bis alle Berechtigungen ausgewählt sind, die der Rolle zugewiesen werden sollen.
7. Klicken Sie auf **Speichern**, um die neue Rolle hinzuzufügen, die sofort wirksam ist. Sie können die neue Rolle jetzt Benutzern zuweisen.

Duplizieren von Rollen

Eine effiziente Methode, eine neue Rolle hinzuzufügen, ist es, eine ähnliche Rolle zu duplizieren, sie unter einem neuen Namen zu speichern und die bereits zugewiesenen Berechtigungen zu bearbeiten.

1. Wählen Sie auf der Registerkarte **Rollen** die Rolle aus, die Sie duplizieren möchten, und klicken Sie auf  .
2. Geben Sie einen neuen Namen für die Rolle ein und klicken Sie auf **Speichern**.
3. Führen Sie zur Änderung der Berechtigungen die Schritte des nächsten Verfahrens aus.

Ändern der einer Rolle zugewiesenen Berechtigungen

1. Wählen Sie auf der Registerkarte **Rollen** die Rolle aus und klicken Sie auf  .
   Das Dialogfeld **Rolle bearbeiten** wird angezeigt.
2. Im Abschnitt **Berechtigungen**:
   - Klicken Sie auf  und  , um durch die Module zu blättern.
   - Wählen Sie ein Modul aus, um für es die Berechtigungen zu bearbeiten.
   - Aktivieren oder deaktivieren Sie jede Berechtigung.
3. Wiederholen Sie den vorherigen Schritt, bis die Rolle die erforderlichen Berechtigungen hat.
4. Klicken Sie auf **Speichern**. Die überarbeiteten Berechtigungen sind sofort wirksam.

Löschen einer Rolle

Sie können eine Rolle löschen, wenn sie keinem Benutzer zugewiesen ist.

1. Wählen Sie auf der Registerkarte **Rollen** eine Rolle aus und klicken Sie auf .
2. Ein Dialogfeld fordert Sie auf, zu bestätigen, dass Sie die Rolle löschen möchten. Klicken Sie auf **Yes**.

Schritt 3. Überprüfen von Abfrage- und Sitzungsattributen pro Rolle

Dieses Thema beschreibt die Funktion von Abfrage- und Sitzungsattributen und enthält Anweisungen zum Festlegen dieser Attribute in Benutzerrollen. Außerdem wird in diesem Thema erläutert, welchen Effekt die Rolleneinstellungen auf die einzelnen Benutzereinstellungen haben und was geschieht, wenn ein Benutzer Mitglied mehrerer Rollen ist.

Nach der Definition der Benutzerrollen ist es wichtig, die Abfrage- und Sitzungsattribute zu überprüfen, die den einzelnen Rollen zugeordnet sind. Sie können diese Einstellungen gemäß Ihren Anforderungen anpassen.

Abfrage- und Sitzungsattribute

Abfrage- und Sitzungsattribute legen fest, wie vom Benutzer ausgeführte Abfragen verarbeitet werden. Diese Attribute ermöglichen Ihnen das Sperren von Informationen, die die Benutzer abrufen können. Die Attribute gelten für alle Sitzungen von Benutzern, die einer Rolle zugewiesen sind.

Je nach Ihren Anforderungen können Sie die folgenden Abfragebehandlungsattribute für eine Benutzerrolle festlegen:

- **Core-Abfragetimeout** ist eine optionale Einstellung, die für Core-Services von NetWitness Suite 10.5 und höher gilt. Sie gibt die maximale Dauer in Minuten an, in der ein Benutzer eine Abfrage ausführen kann. Wenn dieser Wert festgelegt wird, muss er null (0) oder größer sein. Beim Wert 0 tritt kein Timeout ein.
- **Core-Sitzungsschwellenwert** ist eine erforderliche Einstellung. Dieser Wert muss null (0) oder größer sein. Bei einem Schwellenwert größer als null extrapoliert die Abfrageoptimierung die Gesamtsitzungsanzahl, die diesen Schwellenwert übersteigt. Wenn der von der Abfrage zurückgegebene Metawert den Schwellenwert erreicht, führt das System Folgendes aus:
  - Beendet die Ermittlung der Sitzungsanzahl.
  - Zeigt den Schwellenwert und den Prozentsatz der Abfragezeit, der zum Erreichen des Schwellenwertes verwendet wurde, an.
- **Core-Abfragepräfix** ist ein optionaler Filter, der auf die vom Benutzer ausgeführten Abfragen angewendet wird. Durch das Präfix werden die Ergebnisse eingeschränkt, die der Benutzer sieht. Beispiel: Das Abfragepräfix `'service' = 80` wird allen Abfragen

vorangestellt, die vom Benutzer ausgeführt werden. Daher kann der Benutzer nur auf Metadaten von HTTP-Sitzungen zugreifen.

Welche Abfragebehandlungsattribut-Einstellungen für einen Benutzer gelten, hängt davon ab, welche Rollenmitgliedschaften der Benutzer besitzt. Daher ist es wichtig, die Abfragebehandlungsattribut-Einstellungen für Ihre Rollen zu überprüfen.

Gültigkeit von Abfragebehandlungsattribut-Einstellungen für einzelne Benutzer

Falls ein Benutzer Mitglied in mehreren Rollen ist, gilt die folgende Systematik:

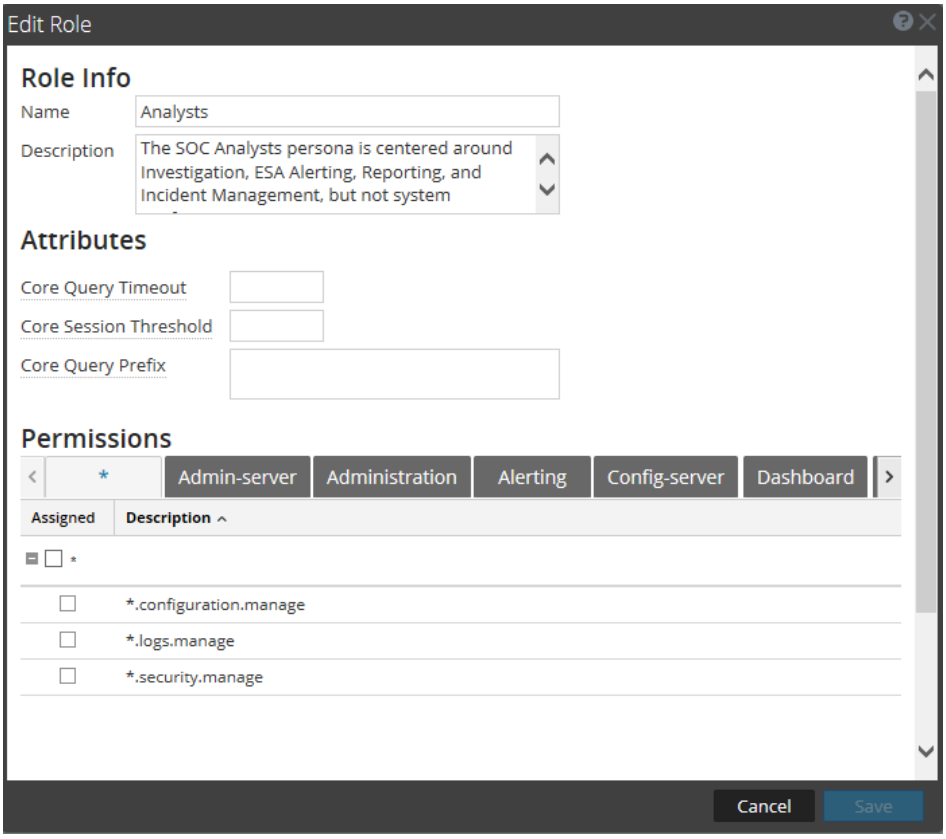
- **Timeout für Abfrage:** Für den Benutzer gilt der großzügigste (höchste) Wert aller zugewiesenen Rollen.
- **Abfragepräfix:** Die Abfragepräfixe aller Benutzerrollen werden durch AND miteinander verknüpft.
- **Sitzungsschwellenwert:** Für den Benutzer gilt der höchste Wert aller zugewiesenen Rollen.

Verfahren

So legen Sie Abfragebehandlungsattribute für eine Benutzerrolle fest:

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Rollen**. Wenn Sie eine Rolle hinzufügen, klicken Sie auf . Wenn Sie eine Rolle bearbeiten, wählen Sie die Rolle aus und klicken Sie auf .

Das Dialogfeld „Rolle hinzufügen“ oder „Rolle bearbeiten“ wird angezeigt.



3. Zum Festlegen der Attribute für die Rolle führen Sie im Bereich **Attribute** die folgenden Schritte aus:

   - (Optional) Geben Sie im Feld **Core-Abfragetimeout** die maximale Anzahl von Minuten an, die eine Abfrage von einem Benutzer ausgeführt werden kann. Der Standardwert beträgt 5 Minuten. Dieses Timeout gilt nur für Abfragen, die von Investigation aus durchgeführt werden. Die Core-Services von NetWitness Suite 10.5 und höher verwenden dieses Feld.
     Wenn in den Rollen kein Wert festgelegt ist, werden bei einer Migration auf NetWitness Suite 10.5 und höher standardmäßig 5 Minuten eingetragen.
   - Geben Sie einen **Core-Sitzungsschwellenwert** ein, um die Ermittlung der Sitzungsanzahl durch das System zu beenden. Der Standardwert ist `100000`. Der hier angegebene Grenzwert setzt den Wert **Max. Sitzungsexport** außer Kraft, der in den Ermittlung-Anzeigeeinstellungen festgelegt wurde.
   - (Optional) Geben Sie ein **Core-Abfragepräfix** ein, um die Abfrageergebnisse zu filtern, die den Rollenmitgliedern angezeigt werden. Dies ist standardmäßig leer.

> **Hinweis:** Werte in kursiver Schrift sind Standardwerte, z. B. *5*. Nicht kursive Werte weisen auf eine Änderung des Standardwerts hin, z. B. `1200`.

4. Klicken Sie auf **Speichern**.

Schritt 4. Einrichten eines Benutzers

Dieses Thema bietet Verfahren zum Einrichten eines neuen Benutzers.

Themen

- Hinzufügen eines Benutzers und einer Rolle
- Aktivieren, Entsperren und Löschen von Benutzerkonten

Hinzufügen eines Benutzers und einer Rolle

In diesem Thema wird erklärt, wie Sie einen neuen Benutzer zu jedem Benutzerkontotypen, lokal und extern, hinzufügen. Es wird außerdem erklärt, wie eine Rolle auf einen lokalen Benutzer zugeteilt wird.

Alle NetWitness Suite-Benutzer müssen ein lokales oder externes Benutzerkonto haben.

Die folgenden Punkte sind beim Verwalten von lokalen und externen Benutzerkonten wichtig.

Lokales Benutzerkonto	Externes Benutzerkonto
In NetWitness Suite verwaltet	Extern und außerhalb dieses Dokumentumfangs verwaltet
Direkt zugeteilte Rollen	Durch externe Gruppenzuordnung zugewiesene Regeln
Leitet Berechtigungen von jeder Rolle ab, die dem Benutzer zugewiesen wurde, wie in diesem Thema beschrieben.	Leitet Berechtigungen von der jeweiligen Rolle ab, die dem Konto der externen Benutzergruppe zugeordnet wurde, wie erläutert wird in Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen.
NetWitness Suite verwaltet alle Benutzerinformationen.	NetWitness Suite verwaltet nur die Benutzeridentifikation. Dies umfasst den Benutzernamen, den Vor- und Nachnamen und die E-Mail-Adresse.

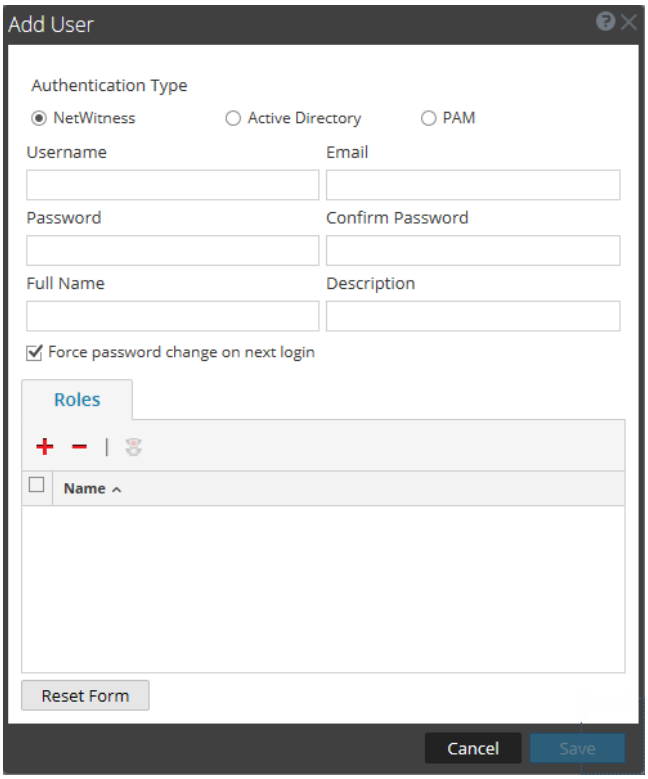
Methoden

Jedes der folgenden Verfahren beginnt auf der Registerkarte „Benutzer“.Um zu dieser Registerkarte zu navigieren, wählen Sie **ADMIN >Sicherheit** aus. Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte „Benutzer“ angezeigt.

Hinzufügen eines Benutzers und einer Rolle

So fügen Sie ein lokales Benutzerkonto hinzu und weisen einem Benutzer eine Rolle zu:

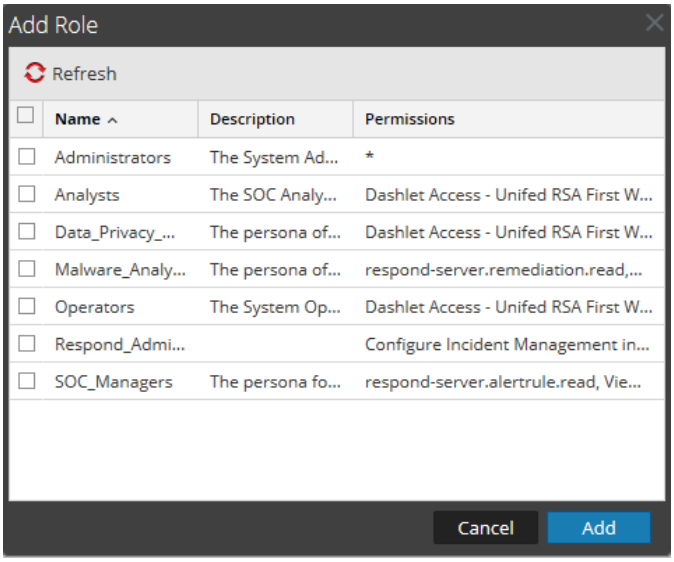
1. Klicken Sie auf der Registerkarte **Benutzer** in der Symbolleiste auf  .
   Das Dialogfeld **Benutzer hinzufügen** wird angezeigt.



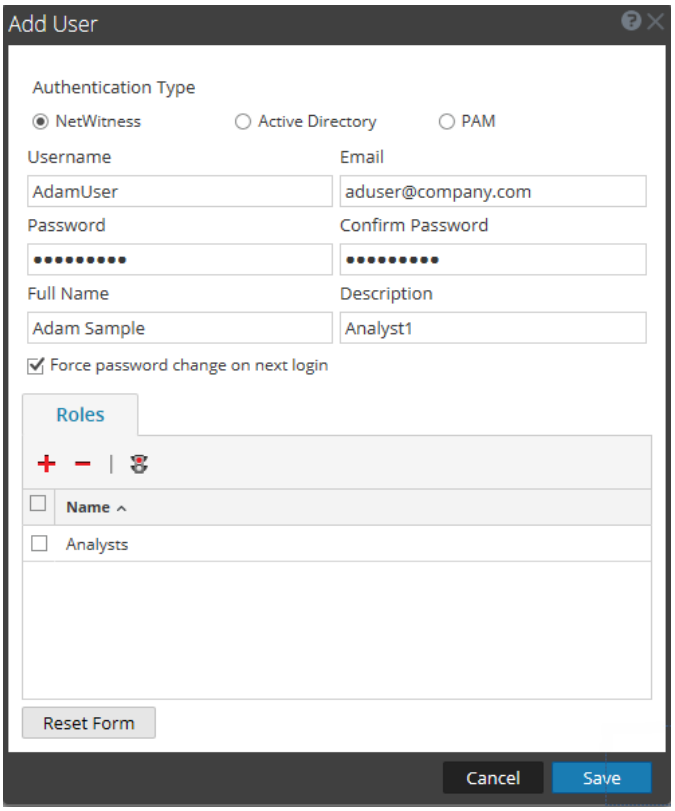
2. Geben Sie die folgenden Kontoinformationen für den neuen Benutzer ein:
   - **Authentication Type**: **NetWitness** ist standardmäßig ausgewählt und die richtige Wahl beim Hinzufügen eines lokalen Benutzers. Diese Option wird nur angezeigt, wenn Active Directory- oder PAM-Konfigurationen eingerichtet wurden, damit dieser Authentifizierungstyp ausgewählt werden kann. Wenn keine Active Directory- oder PAM-Konfigurationen vorhanden sind, ist der Authentifizierungstyp automatisch auf „NetWitness“ festgelegt und es stehen keine weiteren Optionen zur Verfügung.
   - **Benutzername** für die Anmeldung bei NetWitness Suite
   - **E-Mail**-Adresse
   - Passwort zur Anmeldung in NetWitness Suite, in den Feldern **Passwort** und **Passwort bestätigen**
   - **Vor- und Nachname** des neuen Benutzers
   - (Optional) **Beschreibung** des Benutzerkontos
3. Damit der Benutzer beim nächsten Anmeldevorgang sein Passwort durch ein neues ersetzen muss, wählen Sie **Passwortänderung bei nächster Anmeldung erzwingen** aus.
   Dies wirkt sich nicht auf aktive Benutzersitzungen aus. Das Symbol wird in der

Benutzerzeile angezeigt, um darauf hinzuweisen, dass das Benutzerpasswort abgelaufen ist. Sie können dies nicht rückgängig machen, nachdem das Passwort abgelaufen ist. Das Kontrollkästchen wird deaktiviert, wenn Sie das Benutzerkonto das nächste Mal bearbeiten.

4. Um dem Benutzer eine Rolle zuzuweisen, klicken Sie auf + auf der Registerkarte **Rollen**. Im Auswahldialogfeld **Rolle hinzufügen** wird die Liste der verfügbaren Rollen angezeigt.

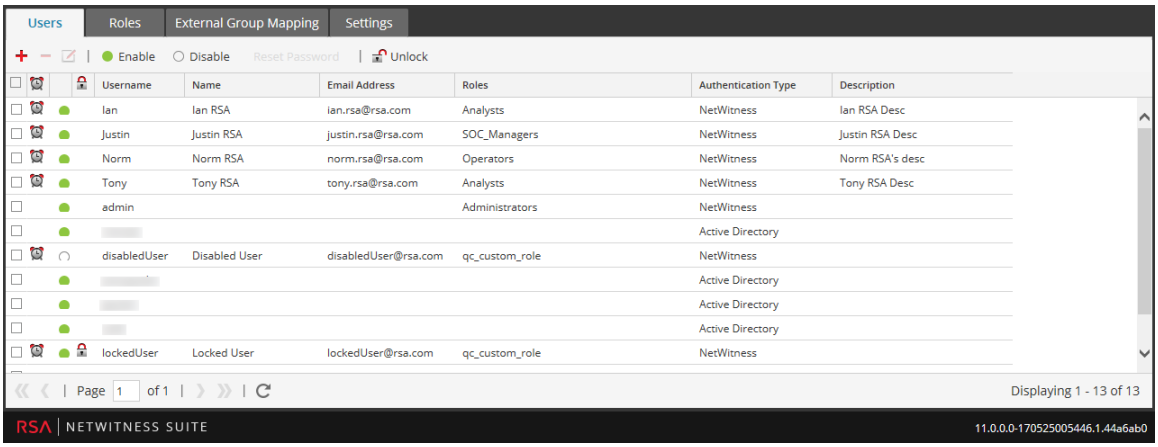


5. Wählen Sie alle Rollen aus, die Sie zuweisen möchten, und klicken Sie auf **Hinzufügen**. Im Dialogfeld **Benutzer hinzufügen** werden alle Rollen angezeigt, die dem Benutzer zugewiesen wurden.



6. (Optional) Wählen Sie eine Rolle aus und klicken Sie auf , um für die Regel **alle Berechtigungen anzuzeigen**.

7. Klicken Sie auf **Speichern**.
   Die Registerkarte **Benutzer** zeigt die neuen Benutzer und alle dem Benutzer zugewiesenen Rollen an. Das Konto ist sofort aktiv.



Hinzufügen eines Benutzers für die externe Authentifizierung

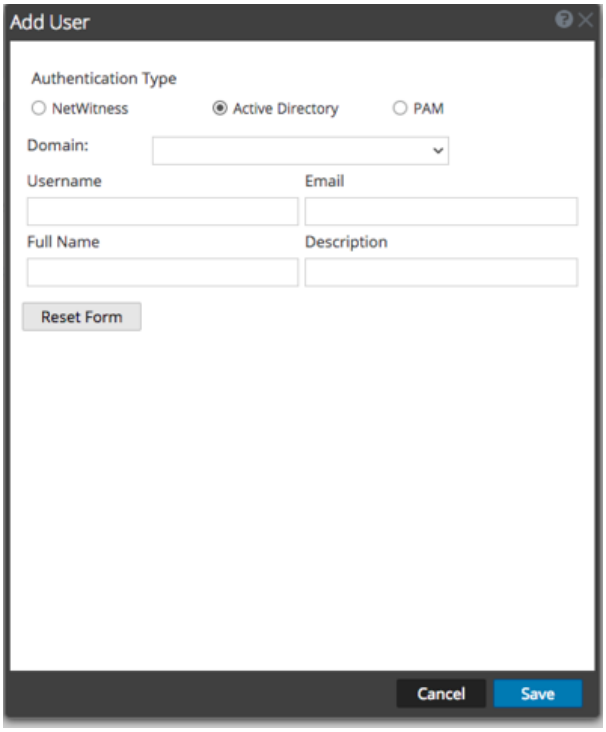
Voraussetzung: Externe Authentifizierung muss konfiguriert werden. Weitere Informationen erhalten Sie unter Schritt 4. (Optional) Konfigurieren der externen Authentifizierung.

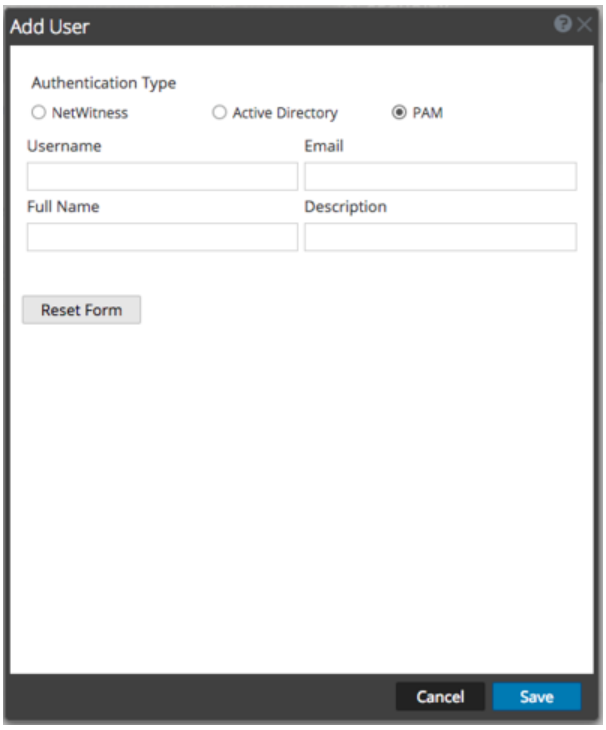
So fügen Sie einen Benutzer hinzu, der extern (außerhalb von NetWitness Suite) authentifiziert ist:

1. Klicken Sie auf der Registerkarte **Benutzer** in der Symbolleiste auf +.

   Das Dialogfeld **Benutzer hinzufügen** wird angezeigt.

2. Wählen Sie unter **Authentifizierungstyp** entweder **Active Directory** oder **PAM** aus. Das Dialogfeld wird aktualisiert und zeigt nun die Pflichtfelder für den ausgewählten externen Authentifizierungstyp an.





3. Geben Sie die folgenden Informationen ein:
   - **Domain** (wenn nur „Active Directory“ als Authentifizierungstyp ausgewählt wurde): Wählen Sie in der Drop-down-Liste der verfügbaren Domains die Active Directory-Domain für den Benutzer aus.
   - **Benutzername** für die Anmeldung bei NetWitness Suite
   - **E-Mail**-Adresse
   - **Vor- und Nachname** des neuen Benutzers
   - (Optional) **Beschreibung** des Benutzerkontos
4. Klicken Sie auf **Speichern**. Auf der Registerkarte „Benutzer“ wird das neue Benutzerkonto angezeigt, dem noch eine Rolle und Berechtigungen zugeordnet werden müssen.
5. Anweisungen zum Zuordnen einer Rolle zum neuen Benutzer erhalten Sie in Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen.

Ändern der Benutzerinformationen oder Rollen

So ändern Sie die Kontoinformationen oder zugeteilten Rollen eines Benutzers:

1. Wählen Sie in der Registerkarte **Benutzer** einen Benutzer aus und klicken Sie in der Symbolleiste auf 
   .Das Dialogfeld **Benutzer bearbeiten** wird angezeigt.
2. Um Benutzerinformationen zu bearbeiten, ändern Sie eines der folgenden Felder:
   - **E-Mail**
   - **Vor- und Nachname**
   - **Beschreibung**
3. Damit der Benutzer beim nächsten Anmeldevorgang sein **internes** Passwort durch ein neues ersetzen muss, wählen Sie **Passwortänderung bei nächster Anmeldung erzwingen** aus. Dies wirkt sich nicht auf aktive Benutzersitzungen aus. Das Symbol  wird in der Benutzerzeile angezeigt, um darauf hinzuweisen, dass das Benutzerpasswort abgelaufen ist. Sie können dies nicht rückgängig machen, nachdem das Passwort abgelaufen ist. Das Kontrollkästchen wird deaktiviert, wenn Sie das Benutzerkonto das nächste Mal bearbeiten.
4. Im Abschnitt **Rollen** :
   - Um eine andere Rolle zuzuweisen, klicken Sie auf  , wählen eine Rolle aus und klicken auf **Hinzufügen**.
   - Um eine zugewiesene Rolle zu entfernen, wählen Sie eine Rolle aus und klicken Sie auf .
5. Klicken Sie auf **Speichern**.

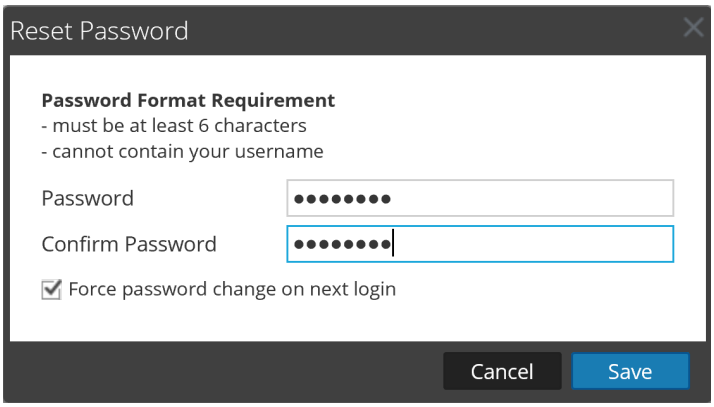
Benutzer löschen

1. Wählen Sie in der Registerkarte **Benutzer** einen Benutzer aus.
2. Klicken Sie in der Symbolleiste auf .
3. Klicken Sie auf **Speichern**.

Hinweis: Um einen Benutzer, der extern durch Active Directory authentifiziert wurde, komplett zu löschen, müssen Sie den Benutzer auch von der AD-Gruppe löschen.

Zurücksetzen eines Benutzerpassworts

1. Wählen Sie in der Registerkarte **Benutzer** einen Benutzer aus.
2. Klicken Sie in der Symbolleiste auf **Passwort zurücksetzen**.



   Im Bereich **Passwortformatanforderungen** sind die speziellen Anforderungen für das Passwort aufgeführt. Administratoren können diese Anforderungen für alle internen Benutzer in der Passwort-Policy anpassen. Anweisungen hierzu erhalten Sie in Schritt 1. Konfigurieren der Passwortkomplexität.

3. Sie können auswählen, ob der Benutzer bei der nächsten Anmeldung bei NetWitness Suite sein Passwort ändern muss.
4. Klicken Sie auf **Speichern**.

Aktivieren, Entsperren und Löschen von Benutzerkonten

Dieses Thema bietet Anleitungen zum Aktivieren, Entsperren und Löschen von Benutzerkonten.

Alle Benutzer von NetWitness Suite müssen entweder über ein lokales Benutzerkonto mit Benutzername und Passwort oder über ein externes Benutzerkonto verfügen. In NetWitness Suite können lokale Benutzerkonten aktiviert, deaktiviert und gelöscht werden.

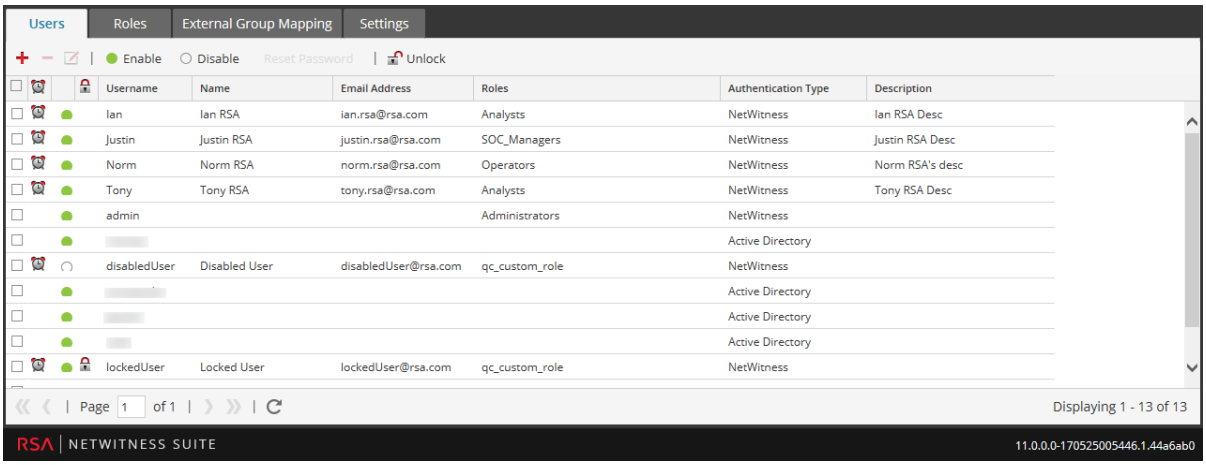
Wenn sich ein externer Benutzer zum ersten Mal bei NetWitness Suite anmeldet, wird automatisch ein neuer Benutzereintrag mit NetWitness Suite erstellt.NetWitness Suite verwaltet nur Informationen zur Identifizierung des Benutzer; wie z. B. den vollständigen Namen und die E-Mail-Adresse.

Sie können gesperrte Konten für lokale und externe Benutzer entsperren.

Aktivieren von deaktivierten NetWitness Suite-Benutzerkonten

So aktivieren Sie deaktivierte NetWitness Suite-Benutzerkonten:

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.



2. Wählen Sie im Raster **Benutzer** ein oder mehrere Konten aus.
3. Klicken Sie auf Enable.
   In einem Dialogfeld werden Sie zur Bestätigung aufgefordert.
4. Wenn Sie die Konten aktivieren möchten, klicken Sie auf **Ja**.
   Die Konten werden aktiviert und der Benutzer kann sich bei NetWitness Suite anmelden.

Deaktivieren von NetWitness Suite-Benutzerkonten

Sie können den Zugriff von Benutzern blockieren, indem Sie sie deaktivieren. Beim Deaktivieren des Benutzers werden die Benutzereinstellungen nicht gelöscht. Mit dieser Aktion wird der Benutzerzugriff blockiert, ohne die Benutzereinstellungen zu löschen. Daher bleiben nach einer erneuten Aktivierung der Benutzer deren Einstellungen intakt. Sie können Benutzer erneut aktivieren, um den Benutzerzugriff wiederherzustellen. Es können nur lokale Benutzer deaktiviert werden, jedoch nicht externe Benutzer.

So deaktivieren Sie NetWitness Suite-Benutzerkonten:

1. Wählen Sie im Raster **Benutzer** ein oder mehrere Konten aus.
2. Klicken Sie auf Disable.
   In einem Dialogfeld werden Sie zur Bestätigung aufgefordert.
3. Wenn Sie die Konten deaktivieren möchten, klicken Sie auf **Ja**.
   Die Konten werden deaktiviert und der Benutzer kann sich nicht mehr bei NetWitness Suite anmelden.

Entsperren von gesperrten NetWitness Suite-Benutzerkonten

Nach mehreren aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen wird ein Benutzer für einen Zeitraum gesperrt. So entsperren Sie NetWitness Suite-Benutzerkonten, die aufgrund mehrerer fehlgeschlagener Anmeldeversuche gesperrt wurden:

1. Wählen Sie im Raster **Benutzer** ein oder mehrere Konten aus.
2. Klicken Sie auf Unlock.
   In einem Dialogfeld werden Sie zur Bestätigung aufgefordert.
3. Wenn Sie die Konten entsperren möchten, klicken Sie auf **Ja**.
   Die Konten werden entsperrt und der Benutzer kann sich bei NetWitness Suite anmelden.

Löschen von NetWitness Suite-Benutzerkonten

Wenn keine externe Authentifizierung verwendet wird, kann sich ein Benutzer mit einem lokalen Konto bei NetWitness Suite anmelden. Diese lokalen Konten werden direkt mithilfe von NetWitness Suite gemanagt. Um den Zugriff für einen lokalen Benutzer zu entziehen, deaktivieren Sie das Konto oder löschen Sie es ganz aus dem System.

Hinweis: Hierdurch werden alle Benutzereinstellungen des Kontos aus NetWitness Suite gelöscht. Wenn dies nicht beabsichtigt wird, deaktivieren Sie den Benutzer einfach anstatt ihn zu löschen.

So löschen Sie NetWitness Suite-Benutzerkonten:

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Wählen Sie in der Liste „Benutzer“ ein oder mehrere Konten aus.
3. Klicken Sie auf .
   In einem Warnmeldungsdialogfeld werden Sie zur Bestätigung aufgefordert.
4. Wenn Sie die Konten löschen möchten, klicken Sie auf **Ja**.
   Die Konten werden aus NetWitness Suite gelöscht und die Benutzer können sich nicht mehr bei NetWitness Suite anmelden.

Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen

In diesem Thema werden die Methoden für die Zuordnung von NetWitness Suite-Benutzerrollen zu externen Gruppen beschrieben.

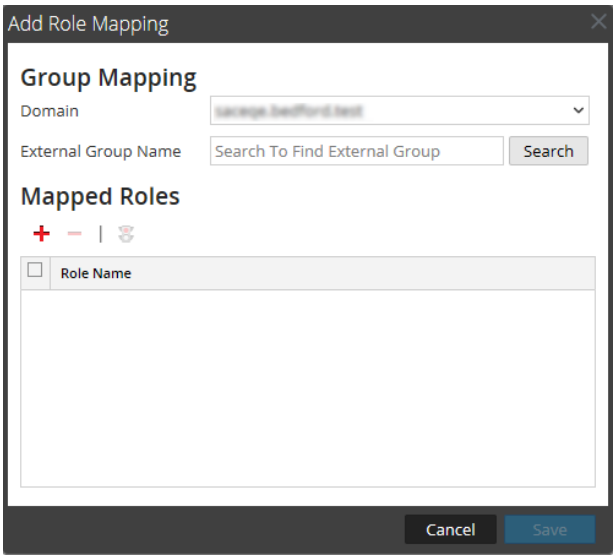
In NetWitness Suite leiten externe Gruppen Berechtigungen für verschiedene Module und Ansichten von NetWitness Suite-Benutzerrollen, die zugewiesene Berechtigungen haben, ab. Ordnen Sie externen Gruppen Benutzerrollen zu, um ihnen Zugriff zu verschaffen. Um den Zugriff externer Gruppen zu ändern, bearbeiten Sie die Rollen, die ihnen zugeordnet wurden. Fahren Sie mit dem Hinzufügen und Löschen von Rollen fort, bis die externe Gruppe über den erforderlichen Zugriff verfügt. Die Änderungen werden sofort übernommen.

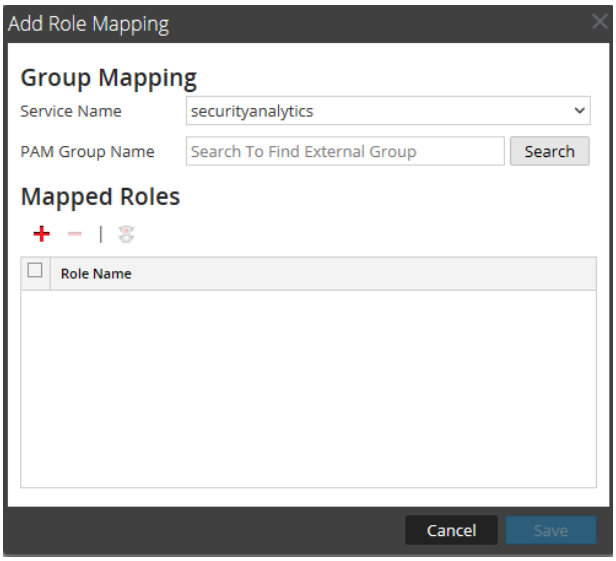
Voraussetzungen

Richten Sie in der Registerkarte Einstellungen eine Authentifizierungsmethode für externe Benutzer ein, um externe Gruppen in NetWitness Suite anzuzeigen.

Hinzufügen einer Rollenzuordnung zu externen Gruppen

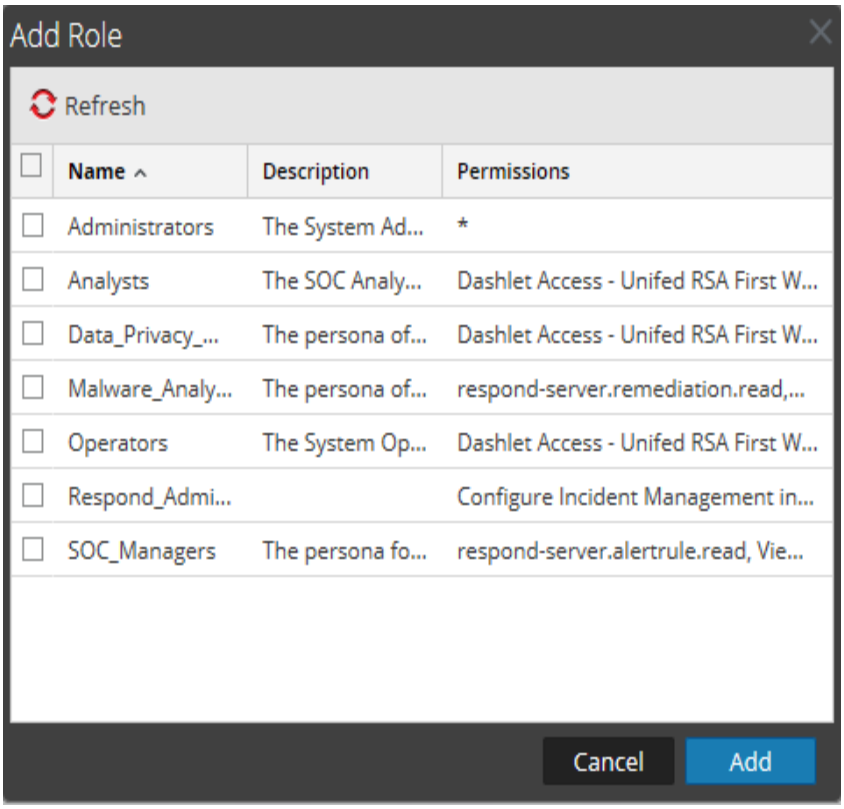
1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Externe Gruppenzuordnung**.
3. Klicken Sie in der Symbolleiste auf +.
   Das Dialogfeld **Rollenzuordnung hinzufügen** für die ausgewählte externe Authentifizierungsmethode wird angezeigt.





4. Klicken Sie auf **Suchen** und suchen Sie im Dialogfeld Suchen nach externen Gruppen nach dem Namen einer externen Gruppe. Wählen Sie diesen dann aus.

5. Um Rollen zu der Gruppenzuordnung hinzuzufügen, klicken Sie auf + im Abschnitt **Zugeordnete Rollen**.
   Das Dialogfeld **Rolle hinzufügen** wird angezeigt.



6. Klicken Sie auf das Kontrollkästchen in der Titelleiste, um alle Rollen auszuwählen, oder wählen Sie die Rollen einzeln aus.
7. Zum Hinzufügen der Rollen zum Abschnitt **Zugeordnete Rollen** im Dialogfeld „Rollenzuordnung hinzufügen“ klicken Sie auf **Hinzufügen**.
   Das Dialogfeld wird geschlossen und die ausgewählten Rollen werden im Abschnitt „Zugeordnete Rollen“ angezeigt.
8. Wenn Sie Rollen aus dem Abschnitt **Zugeordnete Rollen** löschen möchten, wählen Sie diese aus und klicken Sie auf − .
9. Wenn im Dialogfeld **Rollenzuordnung hinzufügen** die Rollenzuordnung angezeigt wird, die Sie für die Gruppe definieren möchten, klicken Sie auf **Speichern**.
   Das Dialogfeld „Rollenzuordnung hinzufügen“ wird geschlossen und die neue Rollenzuordnung wird in der Liste der Registerkarte „Externe Gruppenzuordnung“ aufgeführt.

Bearbeiten der Rollenzuordnung einer Gruppe

1. Klicken Sie in der Aktionsleiste **Externe Gruppenzuordnung** auf **Bearbeiten**.
   Das Dialogfeld **Rollenzuordnung** bearbeiten wird mit dem Gruppennamen im Feld **Name der externen Gruppe** angezeigt.
2. Um Rollen zu der Zuordnung hinzuzufügen, klicken Sie auf + im Abschnitt **Zugeordnete Rollen**.
   Das Dialogfeld Rolle hinzufügen wird angezeigt.
3. Klicken Sie auf das Kontrollkästchen in der Titelleiste, um alle Rollen auszuwählen, oder wählen Sie die Rollen einzeln aus.
4. Zum Hinzufügen der Rollen zum Abschnitt **Zugeordnete Rollen** im Dialogfeld **Rollenzuordnung hinzufügen** klicken Sie auf **Hinzufügen**.
   Das Dialogfeld wird geschlossen und die ausgewählten Rollen werden im Abschnitt „Zugeordnete Rollen“ angezeigt.
5. Wenn Sie Rollen aus dem Abschnitt **Zugeordnete Rollen** löschen möchten, wählen Sie diese aus und klicken Sie auf − .
6. Wenn im Dialogfeld **Rollenzuordnung bearbeiten** die Rollenzuordnung angezeigt wird, die Sie für die Gruppe definieren möchten, klicken Sie auf **Speichern**.
   Das Dialogfeld wird geschlossen und die bearbeitete Rollenzuordnung wird auf der Registerkarte „Externe Gruppenzuordnung“ aufgelistet.

Verwandtes Thema

- Suchen nach externen Gruppen

Suchen nach externen Gruppen

Dieses Thema enthält Anweisungen für die Suche nach externen Gruppen, denen NetWitness Suite-Benutzerrollen zugeordnet sind.

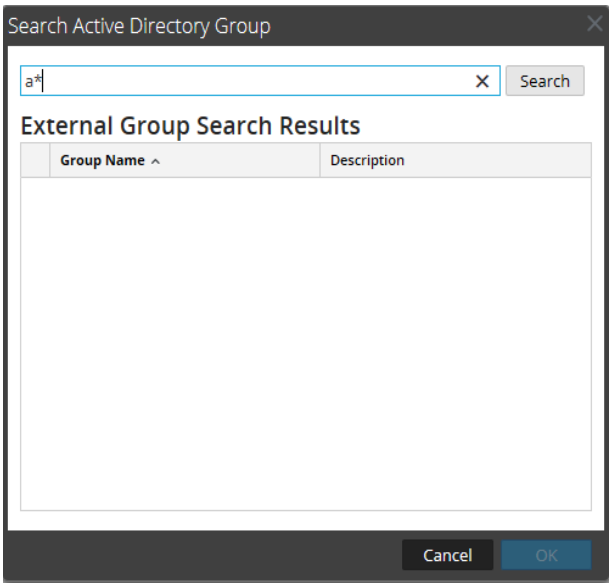
Voraussetzungen

Eine Methode für die externe Benutzerauthentifizierung muss aktiviert sein.

Verfahren

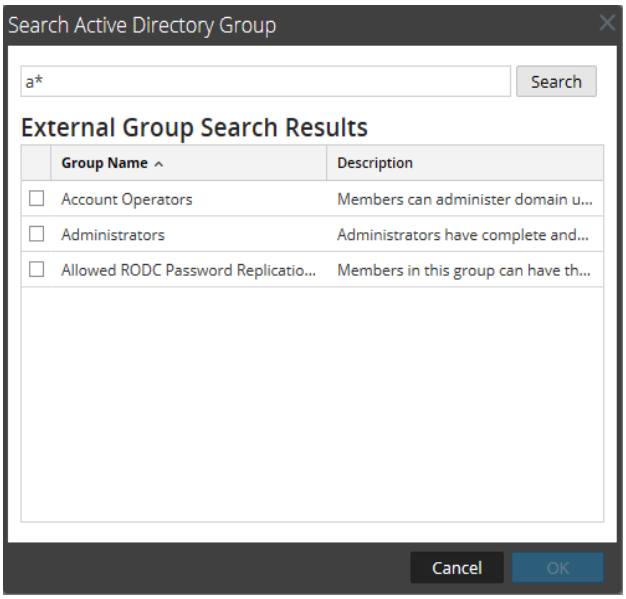
So suchen Sie nach einer externen Gruppe:

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Externe Gruppenzuordnung**.
3. Klicken Sie in der Symbolleiste auf + oder ✎.
   Das Dialogfeld **Rollenzuordnung hinzufügen** für die ausgewählte externe Authentifizierungsmethode wird angezeigt.
4. Der Abschnitt **Gruppenzuordnung** hängt von der ausgewählten externen Authentifizierungsmethode ab.
   - Wählen Sie für **Active Directory** eine **Domain** aus. Klicken Sie dann neben **Name der externen Gruppe** auf **Suchen**.
   - Klicken Sie für **PAM** neben **Name der PAM-Gruppe** auf **Suchen**.
     Das Dialogfeld **Externe Gruppen durchsuchen** wird angezeigt.
5. Geben Sie im Feld **Gemeinsamer Name** einen Gruppennamen oder einen Teil eines Gruppennamens mit dem Platzhalterzeichen (*) ein.



6. Klicken Sie auf **Suchen**.

   Die Ergebnisse werden im Abschnitt **Externe Gruppen - Suchergebnisse** angezeigt.



7. Wählen Sie die Gruppe aus, der Sie Rollen zuweisen möchten, und klicken Sie auf **OK**.

Referenzen

Dieses Thema enthält eine Sammlung von Referenzen zur Systemsicherheit und zum Benutzermanagement in NetWitness Suite.

Themen

Ansicht „Administration-Sicherheit“

In diesem Thema werden die Benutzeroberflächenelemente in der Ansicht Sicherheit unter Administration sowie in allen zugehörigen Dialogfeldern und Registerkarten beschrieben. Die Komponenten der Schnittstelle sind alphabetisch aufgelistet.

Der Bereich Administration > Sicherheit 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.

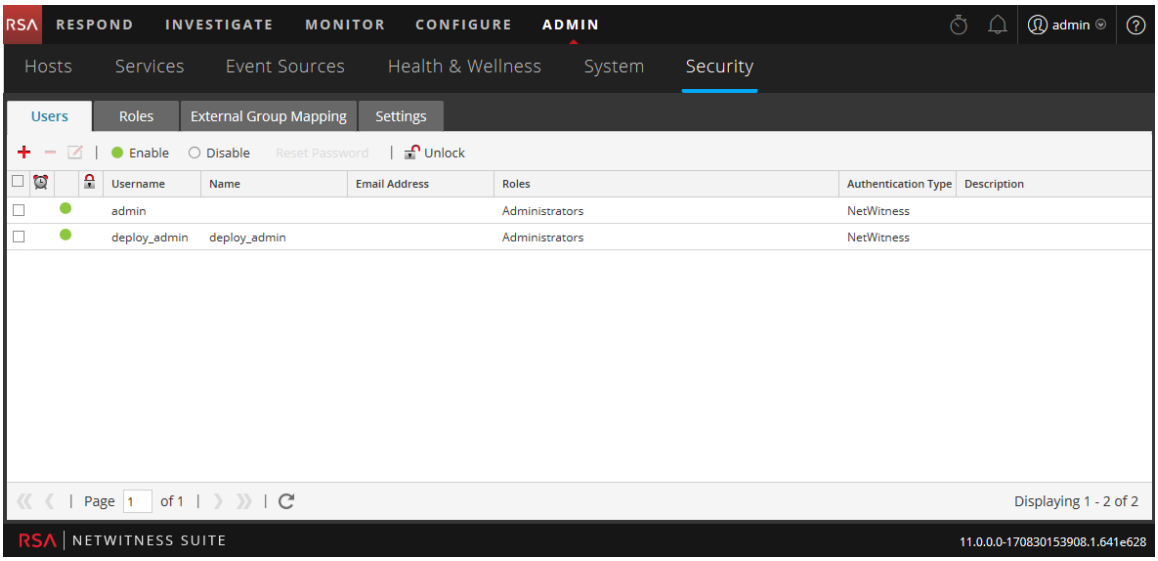
Was möchten Sie tun?

Rolle	Ich möchte...	Details anzeigen
Administrator	Managen von Benutzern	Schritt 4. Einrichten eines Benutzers
Administrator	Verwalten von Rollen	Schritt 1. Überprüfen der vorkonfigurierten NetWitness-Rollen Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen
Administrator	(Optional) Konfigurieren der externen Gruppenzuordnungen	Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen
Administrator	Einstellungen konfigurieren	Schritt 3. Konfigurieren von Sicherheitseinstellungen auf Systemebene

Verwandte Themen

- Registerkarte Benutzer
- Registerkarte Rollen
- Registerkarte Externe Gruppenzuordnung
- Registerkarte Einstellungen

Um die Ansicht Admin Sicherheit anzuzeigen, gehen Sie zu **ADMIN > Sicherheit**.



Der Bereich Administration > Sicherheit umfasst fünf Registerkarten:

- Mit der Registerkarte **Benutzer** können Benutzerkonten verwaltet werden.
- Mit der Registerkarte **Rollen** können Sicherheitsrollen definiert und Rollen zu Benutzerkonten zugeordnet werden.
- Mit der Registerkarte **Externe Gruppenzuordnung** können Zugriffsparameter für LDAP-Gruppen verwaltet werden.
- Mit Registerkarte **Einstellungen** können Komplexität und Ablaufen von Passwörtern für interne NetWitness Suite-Benutzer und das Systemverhalten bei fehlgeschlagenen Anmeldungen und Inaktivität konfiguriert werden. Außerdem bietet Sie eine Möglichkeit zum Konfigurieren der externen Authentifizierung.

Registerkarte Benutzer

In diesem Thema werden die Funktionen zum Einrichten eines Benutzerkontos in der Ansicht Administration > Sicherheit > Registerkarte Benutzer beschrieben.

Jeder NetWitness Suite-Benutzer muss über ein Benutzerkonto verfügen. Auf der Registerkarte Benutzer können Sie Benutzerkonten erstellen, bearbeiten, löschen, aktivieren/deaktivieren und entsperren.

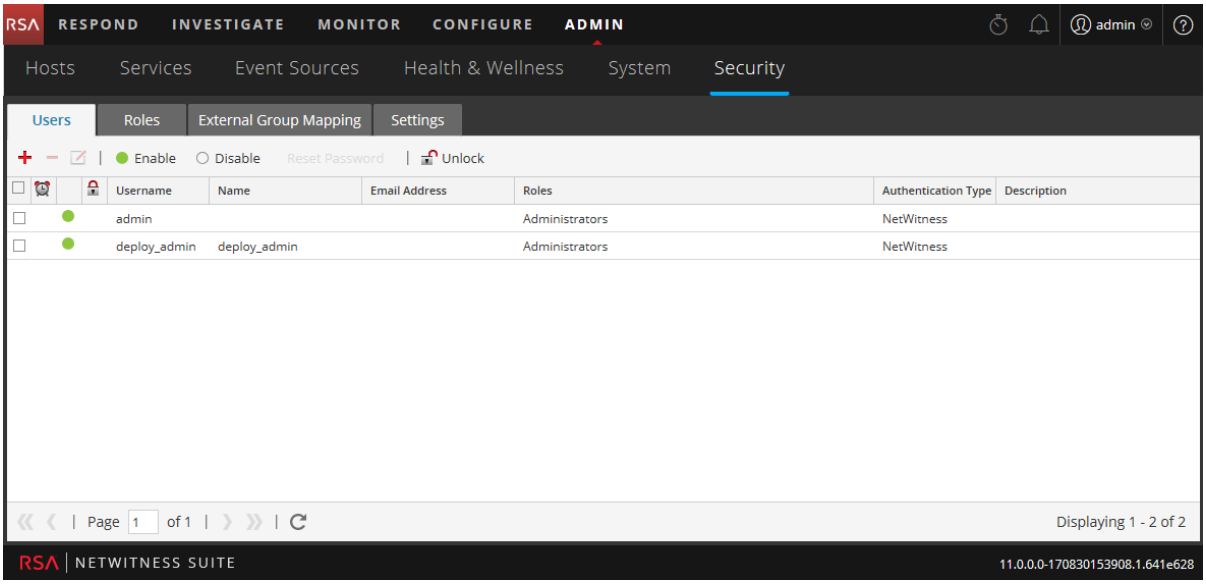
Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Einrichten eines neuen Benutzers	Schritt 4. Einrichten eines Benutzers Hinzufügen eines Benutzers und einer Rolle
Administrator	Managen von Benutzerkonten	Aktivieren, Entsperren und Löschen von Benutzerkonten

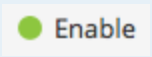
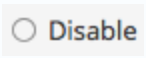
Verwandte Themen

- Dialogfeld „Benutzer hinzufügen“ oder „Benutzer bearbeiten“

Um auf diese Ansicht zuzugreifen, gehen Sie zu **ADMIN > Sicherheit**. Die Ansicht Sicherheit öffnet standardmäßig mit der Registerkarte **Benutzer**.



Die Registerkarte „Benutzer“ besteht aus der Benutzerliste mit einer Symbolleiste im oberen Bereich. Im Folgenden werden die Symbolleistenfunktionen beschrieben.

Funktion	Beschreibung
	Öffnet das Dialogfeld Benutzer hinzufügen.
	Löscht den ausgewählten Benutzer.
	Öffnet das Dialogfeld Benutzer bearbeiten für den ausgewählten Benutzer.
	Aktiviert ein deaktiviertes Benutzerkonto, wobei alle Einstellungen erhalten bleiben.
	Sperrt den Benutzerzugriff, ohne Benutzereinstellungen zu löschen, sodass beim erneuten Aktivieren des Benutzerkontos die Einstellungen erhalten bleiben.
Passwort zurücksetzen	Öffnet das Dialogfeld Passwort zurücksetzen, in dem Sie das Kennwort für den ausgewählten Benutzer ändern können. Dieses Dialogfeld enthält die Anforderungen an das Passwortformat, um das Passwort zu ändern. Hier können Sie auch den Benutzer zum Ändern seines Passworts bei der nächsten Anmeldung zwingen.
 Entsperren	Entsperrt ein Benutzerkonto, das aufgrund von zu vielen fehlgeschlagenen Anmeldeversuchen gesperrt wurde.

Das Liste **Benutzer** besteht aus folgenden Spalten.

Spalte	Beschreibung
	Wenn dieses Symbol in einer Zeile angezeigt wird, bedeutet dies, dass das Benutzerpasswort abgelaufen ist.
Benutzername	Benutzername für die Anmeldung bei NetWitness Suite.
Name	Name des Benutzers, zu dem das Konto gehört

Spalte	Beschreibung
E-Mail-Adresse	E-Mail-Adresse des Benutzers
Rollen	Die dem Benutzer zugewiesene Rolle
Extern	Authentifizierungsmethode, z. B. extern durch Active Directory oder PAM oder intern durch NetWitness Suite.
Beschreibung	Beschreibung des Benutzerkontos

Dialogfeld „Benutzer hinzufügen“ oder „Benutzer bearbeiten“

In diesem Thema werden die Dialogfelder „Benutzer hinzufügen“ und „Benutzer bearbeiten“ vorgestellt, auf die über die Ansicht „Admin“ > „Sicherheit“ Registerkarte „Benutzer“ zugegriffen werden kann.

Alle Benutzer müssen entweder über ein lokales Benutzerkonto mit Benutzernamen und Passwort verfügen oder ein externes Benutzerkonto besitzen, das NetWitness Suite zugeordnet ist.

Was möchten Sie tun?

Rolle	Ich möchte...	Details anzeigen
Administrator	Hinzufügen eines Benutzers und einer Rolle	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen
Administrator	Benutzerinformationen ändern	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen
Administrator	Zurücksetzen eines Benutzerpassworts	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen
Administrator	Hinzufügen eines Benutzers für die externe Authentifizierung	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen

Verwandte Themen

- Managen von Benutzern mit Rollen und Berechtigungen
- Aktivieren, Entsperren und Löschen von Benutzerkonten

Benutzereinstellungen

So zeigen Sie das Dialogfeld **Benutzer hinzufügen** bzw. **Benutzer bearbeiten** an:

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Aktionsleiste auf  .
     Das Dialogfeld **Benutzer hinzufügen** wird angezeigt.

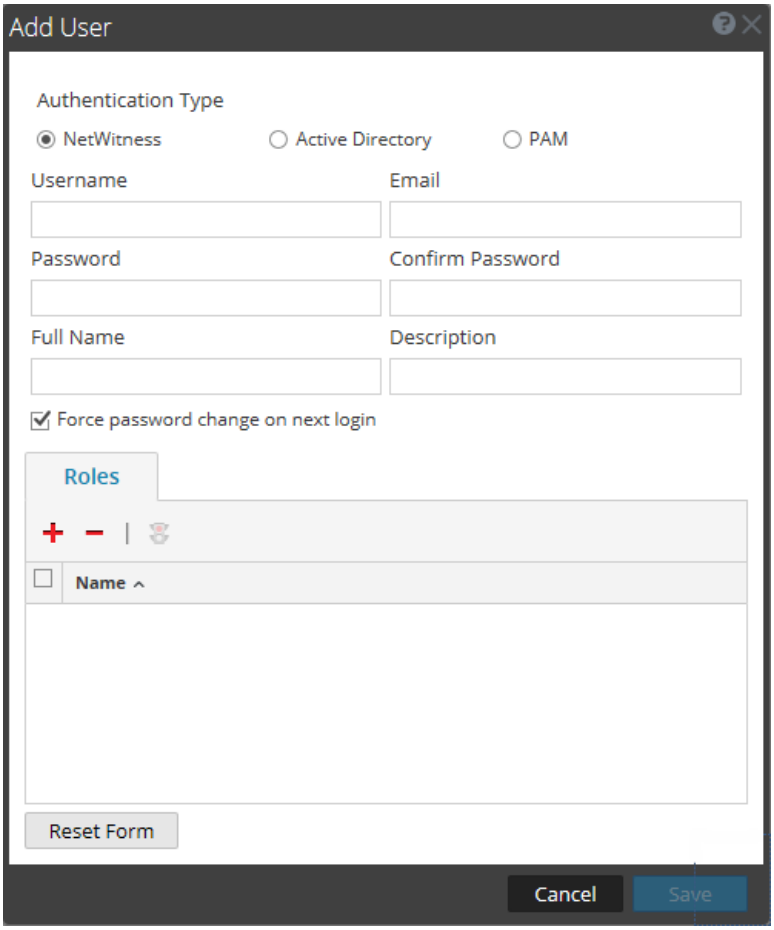
- Wählen Sie einen Benutzer aus und klicken Sie in der Aktionsleiste auf .

  Das Dialogfeld **Benutzer bearbeiten** wird angezeigt.

Die Dialogfelder Benutzer hinzufügen und Benutzer bearbeiten, sind identisch mit der Ausnahme, dass das Dialogfeld Benutzer Hinzufügen zusätzlich die Felder **Passwort** und **Passwort bestätigen** enthält. Sie können im Dialogfeld Benutzer hinzufügen ein Passwort für einen neuen Benutzer hinzufügen. Benutzer können nur ihre eigenen Passwörter in den Benutzereinstellungen ändern. Sie können ein Passwort für einen Benutzer direkt von der Registerkarte Benutzer zurücksetzen.

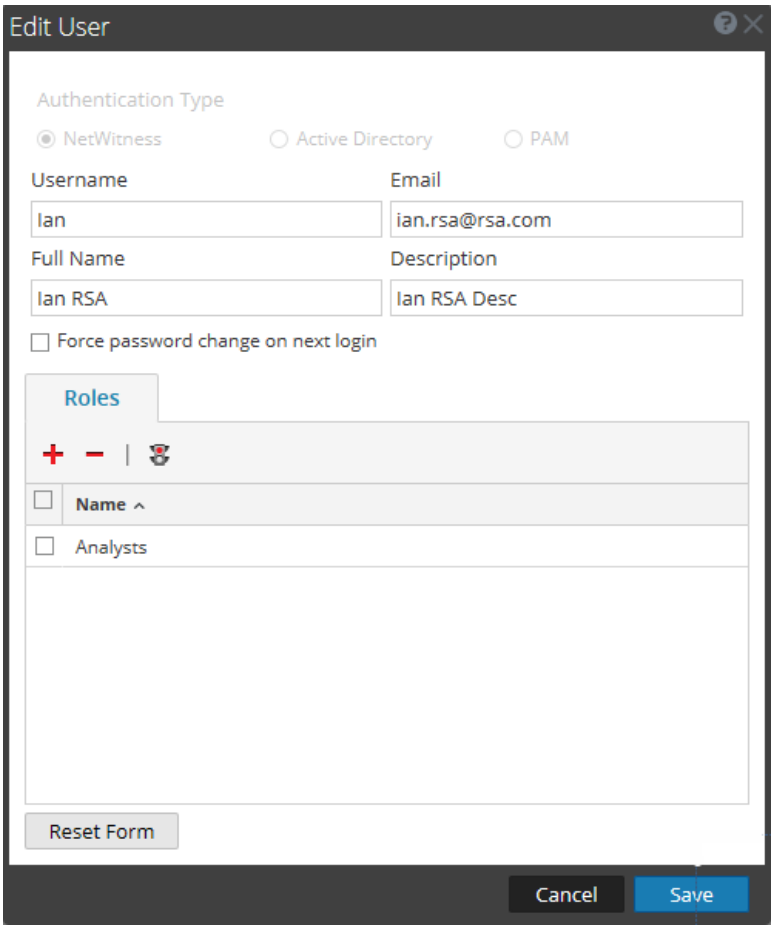
Dialogfeld Benutzer hinzufügen

Hierbei handelt es sich um das Dialogfeld Benutzer hinzufügen für einen internen Benutzer.



Dialogfeld Benutzer bearbeiten

Hierbei handelt es sich um das Dialogfeld Benutzer bearbeiten für einen internen Benutzer.



Die Dialogfelder Benutzer hinzufügen und Benutzer bearbeiten enthalten folgende Angaben:

- Authentication type
- Benutzerinformationen
- Rollen des Benutzers

Benutzerinformationen

Die folgende Tabelle enthält Beschreibungen der Benutzerinformationen.

Feld	Beschreibung
Authentifizierungstyp	Der Authentifizierungstyp für den Benutzer. Standardauswahl ist NetWitness, was einen internen Benutzer ausweist. Optionen für externe Benutzer sind Active Directory und PAM. Dieses Feld ist deaktiviert, wenn Sie einen Benutzer bearbeiten.

Feld	Beschreibung
Benutzername	Benutzername für das Benutzerkonto von NetWitness Suite.
Vor- und Nachname	Name des Benutzers
Passwort	(Nur Dialogfeld Benutzer hinzufügen) Passwort zur Anmeldung NetWitness Suite.
Passwort bestätigen	(Nur Dialogfeld Benutzer hinzufügen) Passwortbestätigung für das Hinzufügen des Benutzerpassworts.
E-Mail	E-Mail-Adresse des Benutzers
Beschreibung	(Optional) Beschreibung des Benutzers.
Passwortänderung bei nächster Anmeldung erzwingen	Das Benutzerpasswort läuft ab, wenn der Benutzer sich das nächste Mal bei NetWitness Suite anmeldet. Dies wirkt sich nicht auf aktive Benutzersitzungen aus. In der Benutzerzeile wird ⏰ angezeigt, um darauf hinzuweisen, dass das Benutzerpasswort abgelaufen ist. Sie können dies nicht rückgängig machen, nachdem das Passwort abgelaufen ist. Das Kontrollkästchen wird deaktiviert, wenn Sie das Benutzerkonto das nächste Mal bearbeiten.
Formular zurücksetzen	Entfernt alle aktuellen Änderungen.

Registerkarte Rollen

Die folgende Tabelle enthält Beschreibungen der Optionen in der Registerkarte Rollen. Die Registerkarte Rollen zeigt die Rollen, die dem Benutzer zugewiesen sind.

Option	Beschreibung
	Öffnet das Dialogfeld Rolle hinzufügen. Darin sind die Rollen aufgelistet, die Sie dem Benutzer zuweisen können.
	Entfernt die ausgewählte Rolle, sodass sie dem Benutzer nicht zugewiesen wird.
	Zeigt Berechtigungen für die ausgewählte Rolle an.
Name	Listet die einzelnen, dem Benutzer zugewiesenen Rollen auf

Registerkarte Rollen

In diesem Thema werden die Funktionen der Ansicht „Administration“ > „Sicherheit“ > Registerkarte „Rollen“ erläutert.

Rollen werden allenNetWitness Suite-Benutzern zugewiesen. Benutzer erhalten die von den Rollen erlaubten Berechtigungen. Auf der Registerkarte „Rollen“ können Sie eine Rolle erstellen, duplizieren, bearbeiten und löschen. Außerdem können Sie eine Liste aller Rollen mit den entsprechenden Berechtigungen anzeigen.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Vorkonfigurierte Rollen anzeigen	Schritt 1. Überprüfen der vorkonfigurierten NetWitness-Rollen
Administrator	Neue Rolle erstellen	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen

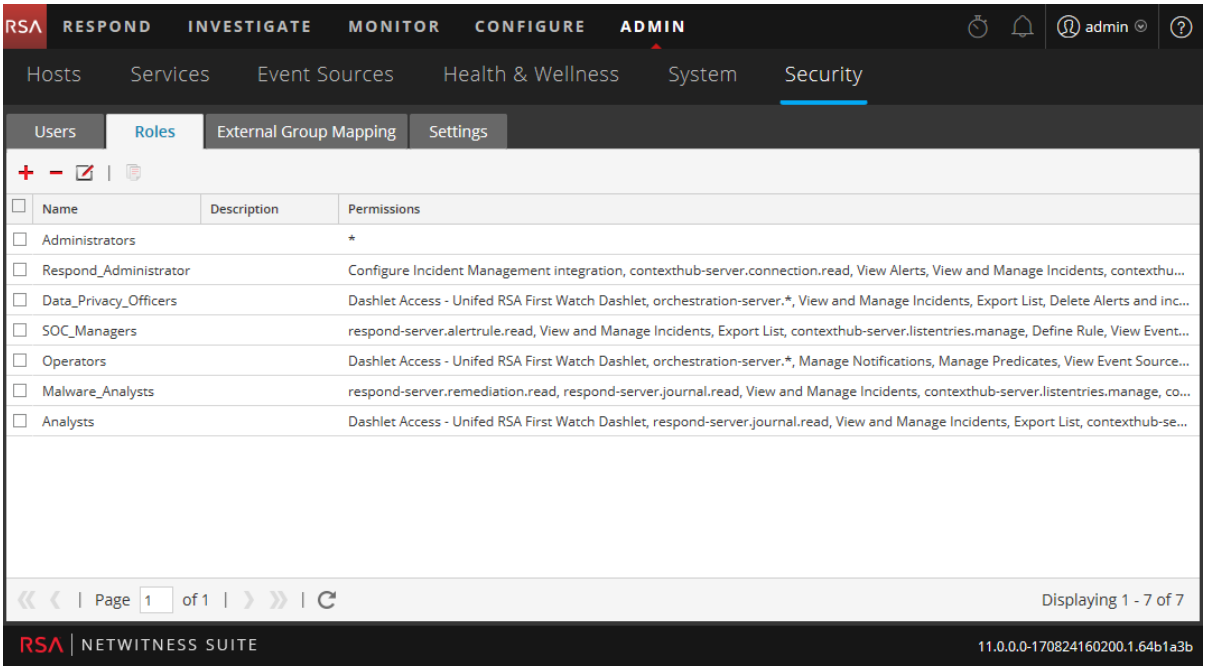
Verwandte Themen

- Dialogfeld „Rolle hinzufügen“ oder „Rolle bearbeiten“

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht Sicherheit wird standardmäßig mit geöffneter Registerkarte **Benutzer** angezeigt.

2. Klicken Sie auf die Registerkarte **Rollen**.



Die Registerkarte Rollen besteht aus der Rollenliste mit einer Symbolleiste ganz oben.

In der folgenden Tabelle werden die Funktionen der Symbolleiste beschrieben.

Funktion	Beschreibung
+	Zeigt das Dialogfeld Rolle hinzufügen an.
✎	Zeigt das Dialogfeld Rolle bearbeiten an.
−	Zeigt eine Warnmeldung an und bittet um Bestätigung, dass Sie eine Rolle löschen möchten.
⧉	Dupliziert eine Rolle, um sie unter einem anderen Namen zu speichern.

In der folgenden Tabelle sind die Funktionen der Rollenliste beschrieben.

Spalte	Beschreibung
Name	Zeigt den Namen einer Rolle an, die einem Benutzer gegeben werden kann.
Beschreibung	Zeigt eine Beschreibung der Rolle an.

Spalte	Beschreibung
Berechtigungen	Zeigt die Berechtigungen an, die einer Rolle zugewiesen wurden.

Dialogfeld „Rolle hinzufügen“ oder „Rolle bearbeiten“

Dieses Thema bietet eine Einführung in die Dialogfelder „Rolle hinzufügen“ und „Rolle bearbeiten“, auf die von der Ansicht „Administration“ > „Sicherheit“ > Registerkarte „Rollen“ aus zugegriffen werden kann.

In den Dialogfeldern „Rolle hinzufügen“ und „Rolle bearbeiten“ können Sie eine Rolle sowie die zugewiesenen Berechtigungen hinzufügen oder bearbeiten. Sie können auch die Attribute zur Abfragebehandlung für Rollenmitglieder angeben, um die Informationen zu sperren, die sie abrufen können. Die Struktur der Dialogfelder ist identisch. Der einzige Unterschied besteht darin, dass Sie entweder eine neue Rolle hinzufügen oder eine bestehende Rolle zu ändern.

Wenn Sie die Berechtigungen für eine Rolle ändern, wird die Änderung sofort auf alle Benutzer angewendet, denen diese besondere Rolle zugewiesen wurde, nachdem die Rolle gespeichert wurde.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Vorkonfigurierte Rollen anzeigen	Schritt 1. Überprüfen der vorkonfigurierten NetWitness-Rollen
Administrator	Neue Rolle erstellen	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen
Administrator	Bearbeiten einer Regel	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen
Administrator	Löschen einer Rolle	Schritt 2. (Optional) Hinzufügen einer Rolle und Zuweisen von Berechtigungen

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht Sicherheit wird standardmäßig mit geöffneter Registerkarte **Benutzer**

angezeigt.

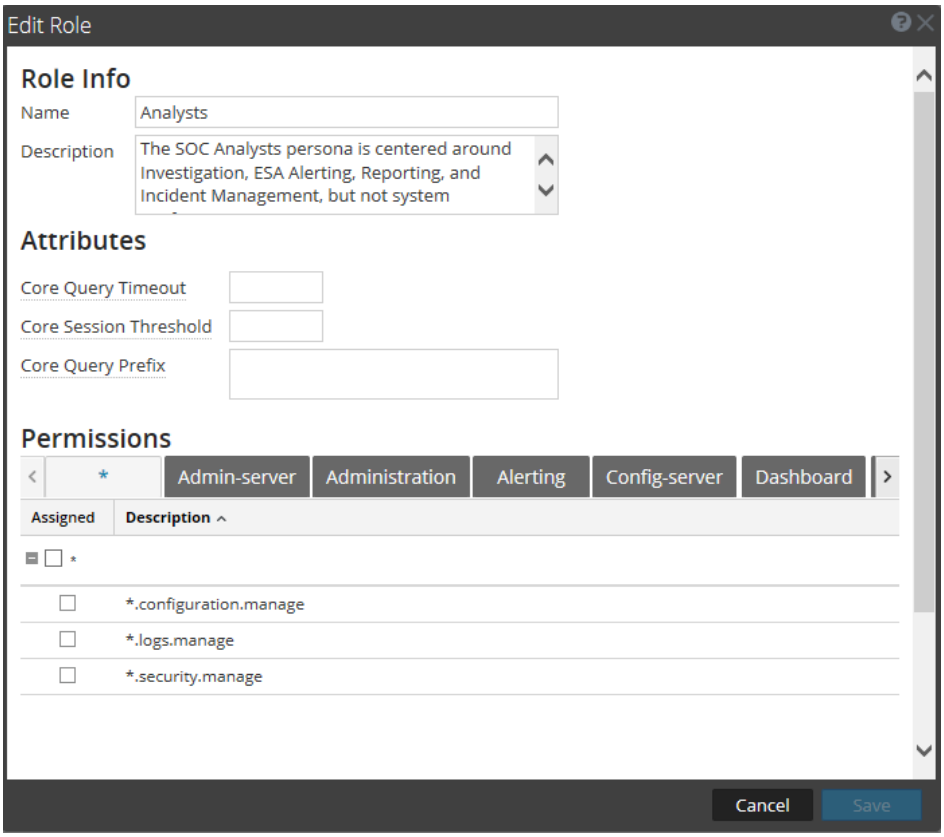
2. Klicken Sie auf die Registerkarte **Rollen**.
3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie in der Aktionsleiste auf  .

     Das Dialogfeld **Rolle hinzufügen** wird angezeigt.

   - Wählen Sie eine Rolle aus und klicken Sie in der Aktionsleiste auf  .

     Das Dialogfeld **Rolle bearbeiten** wird angezeigt.



Die Dialogfelder „Rolle hinzufügen“ und „Rolle bearbeiten“ umfassen drei Abschnitte: **Rolleninfo**, **Attribute** und **Berechtigungen**.

Rolleninfo

Diese Informationen finden Sie im Abschnitt **Rolleninfo**.

Funktion	Beschreibung
Name	Der Name der Benutzerrolle

Funktion	Beschreibung
Beschreibung	Kurze Beschreibung der Benutzerrolle

Merkmale

Dies sind die Informationen im Bereich **Attribute**. Ein Wert in kursiver Schrift stellt einen Standardwert dar, z. B. *5*. Nicht kursive Werte weisen auf eine Änderung des Standardwerts hin, z. B. `1200`. Schritt 3. Überprüfen von Abfrage- und Sitzungsattributen pro Rolle.

Funktion	Beschreibung
Core-Abfragetimeout	(Optional) Gibt die maximale Dauer in Minuten an, in der ein Benutzer eine Abfrage ausführen kann. Der Standardwert ist 5 Minuten. Dieser Timeout gilt nur für Abfragen, die aus Investigation durchgeführt werden. Wenn dieser Wert festgelegt ist, muss er null (0) oder mehr betragen. Beim Wert 0 tritt kein Timeout ein. Wenn in den Rollen kein Wert festgelegt ist, werden bei einer Migration auf NetWitness Suite 10.5 und höher standardmäßig 5 Minuten eingetragen. **Hinweis:** Dieses Feld wird für NetWitness Suite Core-Services der Version 10.5 und höher verwendet.

Funktion	Beschreibung
Core-Sitzungsschwellenwert	Steuert, wie der Service Metadatenwerte scannt, um die Sitzungsanzahl festzustellen. Dieser Wert muss null (0) oder mehr betragen. Wenn dieser Wert größer als null ist, wird eine Abfrageoptimierung die Gesamtsitzungsanzahl ableiten, die den Schwellenwert überschreitet. Wenn der von der Abfrage zurückgegebene Metawert den Schwellenwert erreicht, führt das System Folgendes aus: • Beendet die Ermittlung der Sitzungsanzahl. • Zeigt den Schwellenwert und den Prozentsatz der Abfragezeit, der zum Erreichen des Schwellenwertes verwendet wurde, an. Der Standardwert ist `100000`. Der hier angegebene Grenzwert setzt den Wert **Max. Sitzungsexport** außer Kraft, der in den Ermittlung-Anzeigeeinstellungen festgelegt wurde.
Core-Abfragepräfix	(Optional) Filtert Abfrageergebnisse, um die Anzeige für Rollenmitglieder zu beschränken. Standardmäßig ist dies leer. Das Abfragepräfix `'service' = 80` steht vor allen Abfragen, die vom Benutzer ausgeführt werden, und der Benutzer kann nur auf Metadaten von HTTP-Sitzungen zugreifen.

Berechtigungen

Diese Informationen finden Sie im Abschnitt **Berechtigungen**. In Rollenberechtigungen werden die Berechtigungen beschrieben.

Feature	Beschreibung
Registerkarten **Module**	Insgesamt gibt es acht Registerkarten, eine für jedes Modul: Administration, Alerting, Incidents, Investigation, Live, Malware, Reporting und Dashboard. In jeder Registerkarte werden die Berechtigungen für ein Modul aufgeführt.
Spalte **Beschreibung**	Liste aller Berechtigungen für das Modul.

Feature	Beschreibung
Spalte **Zugewiesen**	Ein Kontrollkästchen, das anzeigt, ob der Rolle eine Modulberechtigung zugewiesen wurde.
Speichern	Speichert die Rolle mit den ausgewählten Berechtigungen.
Abbrechen	Bricht sämtliche Aktionen ab und schließt das Dialogfeld.

Registerkarte Externe Gruppenzuordnung

Wenn Sie die Authentifizierung für externe Benutzer einrichten, können Sie einer externen Gruppe NetWitness Suite-Benutzerrollen zuordnen. Die Registerkarte Externe Gruppenzuordnung enthält Informationen über jede externe Gruppe, der Sie Rollen zugeordnet haben.

Was möchten Sie tun?

Rolle	Ich möchte...	Details anzeigen
Administrator	Einer externen Gruppe eine Rolle zuordnen	Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen
Administrator	Nach einer externen Gruppe suchen	Suchen nach externen Gruppen

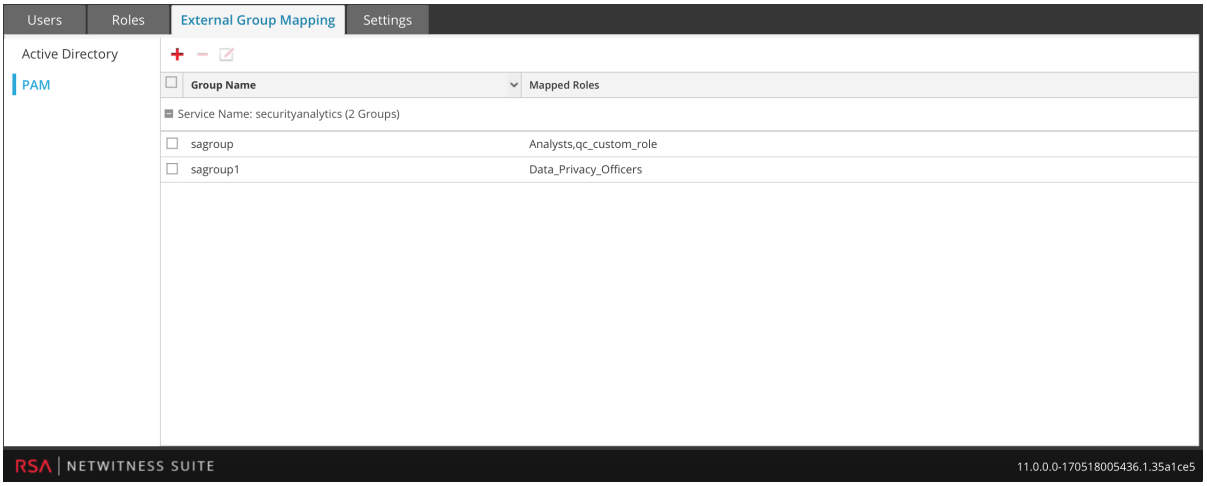
Verwandte Themen

- Dialogfeld Rollenzuordnung hinzufügen
- Dialogfeld Externe Gruppen durchsuchen

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.

2. Klicken Sie auf die Registerkarte **Externe Gruppenzuordnung**.



Die Registerkarte „Externe Gruppenzuordnung“ umfasst eine Symbolleiste und eine Liste.

Die Liste umfasst folgende Funktionen:

Funktion	Beschreibung
Gruppentyp	Klicken Sie in der Spalte auf der linken Seite entweder auf **Active Directory** oder **PAM**, um Gruppen für den ausgewählten Typ anzuzeigen.
Auswahlfeld	In einer Zeile wird die Auswahl eines Gruppennamens aktiviert bzw. deaktiviert. In der Titelliste wird die Auswahl aller Gruppennamen aktiviert bzw. deaktiviert.
Gruppenname	Zeigt den Namen der externen Gruppe an, die Zugriff auf NetWitness Suite hat.
Zugeordnete Rollen	Zeigt die NetWitness Suite-Rollen an, die der externen Gruppe zugeordnet sind.

Die **Symbolleiste** umfasst folgende Funktionen:

Funktion	Beschreibung
	Zeigt das Dialogfeld Rollenzuordnung hinzufügen an, in dem Sie eine externe Gruppe auswählen und einer NetWitness Suite-Rolle zuordnen können.

Funktion	Beschreibung
	Zeigt eine Warnung an und fordert auf, das Entfernen aller der externen Gruppe zugeordneten NetWitness Suite-Rollen zu bestätigen.
	Zeigt das Dialogfeld Rollenzuordnung bearbeiten an, in dem Sie der externen Gruppe NetWitness Suite-Rollen zuordnen oder sie daraus entfernen können.

Dialogfeld Rollenzuordnung hinzufügen

In diesem Thema werden die Funktionen des Dialogfelds Admin > Sicherheit > Registerkarte Externe Gruppenzuordnung > Rollenzuordnung hinzufügen erläutert.

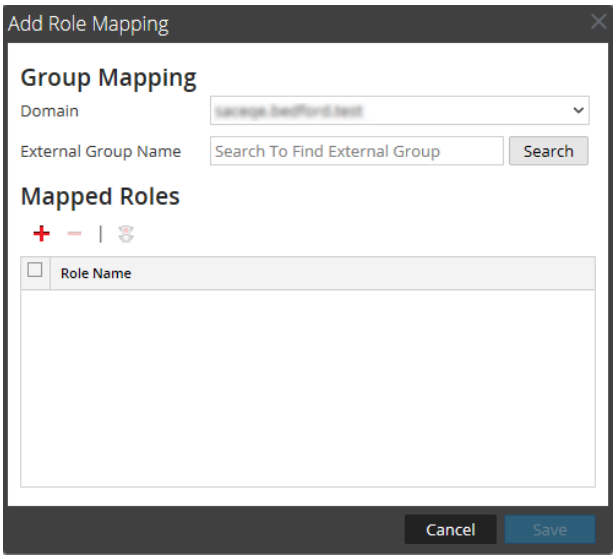
In NetWitness Suite hat jede Benutzerrolle ihre eigenen Berechtigungen. Sie können eine oder mehrereNetWitness Suite-Rollen einer externen Gruppe zuordnen. Dadurch erhält die Gruppe dieselben Berechtigungen, die jede Rolle hat.

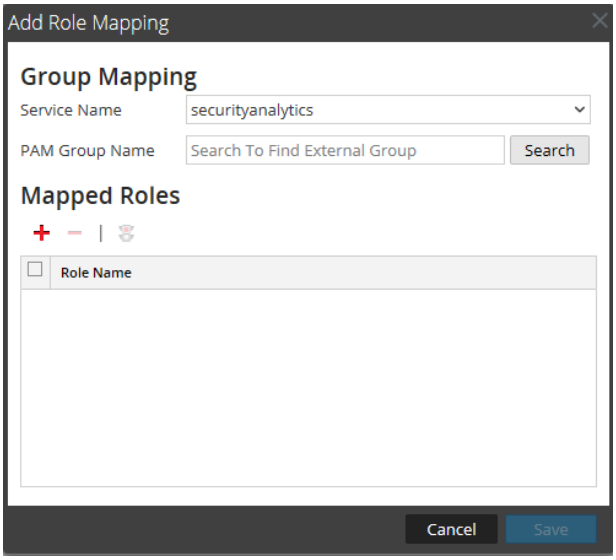
Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Einer externen Gruppe eine Rolle zuordnen	Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen
Administrator	Nach einer externen Gruppe suchen	Suchen nach externen Gruppen

So rufen Sie dieses Dialogfeld auf:

1. Navigieren Sie in NetWitness Suite zu **ADMIN > Sicherheit**.
2. Klicken Sie auf die Registerkarte **Externe Gruppenzuordnung**.
3. Klicken Sie in der Symbolleiste auf +.
   Das Dialogfeld **Rollenzuordnung hinzufügen** für die erstellte externe Authentifizierungsmethode wird angezeigt.





Die Dialogfelder Rollenzuordnung hinzufügen und Rollenzuordnung bearbeiten sind nahezu identisch. Der einzige Unterschied besteht darin, dass Sie im Dialogfeld Rollenzuordnung bearbeiten nicht suchen können.

Gruppenzuordnung

Der Abschnitt **Gruppenzuordnung** hat die folgenden Funktionen:

Funktion	Beschreibung
Domain	Wird angezeigt, wenn Sie Active Directory zur Authentifizierung externer Benutzer einrichten. Der Domainname der externen AD-Gruppe, der Rollen zugeordnet werden.

Funktion	Beschreibung
Name der externen Gruppe	Wird angezeigt, wenn Sie Active Directory zur Authentifizierung externer Benutzer einrichten. Die externe Gruppe, der Rollen zugeordnet werden.
Name der PAM-Gruppe	Wird angezeigt, wenn Sie PAM zur Authentifizierung externer Benutzer konfiguriert haben. Der Name der externen Gruppe, der Rollen zugeordnet werden.
Suchen	Zeigt einen Suchdialog an, in dem Sie nach externen Gruppen suchen können. Die Suche ist im Dialogfeld Rollenzuordnung bearbeiten nicht verfügbar.

Zugeordnete Rollen

Der Abschnitt **Zugeordnete Rollen** hat die folgenden Funktionen:

Funktion	Beschreibung
	Öffnet das Dialogfeld Rolle hinzufügen, in dem konfigurierte NetWitness Suite-Benutzerrollen, die hinzuzufügen sind, aufgelistet sind.
	Entfernt ausgewählte Rollen aus dem Raster Zugeordnete Rollen.
Name	Zeigt den Namen der NetWitness Suite-Benutzerrolle an.
Berechtigungen	Zeigt die der NetWitness Suite-Benutzerrolle zugeordneten Berechtigungen an.
Abbrechen	Bricht die Erstellung einer neuen Gruppenzuordnung oder die Änderung einer Gruppenzuordnung ab und schließt das Dialogfeld.
Speichern	Speichert die neue Gruppenzuordnung oder die Änderung einer Gruppenzuordnung und schließt das Dialogfeld.

Dialogfeld Externe Gruppen durchsuchen

In diesem Thema werden die Funktionen in der Ansicht „Admin“ > „Sicherheit“ Dialogfeld „Externe Gruppen durchsuchen“ beschrieben.

Wenn Sie eine Authentifizierung für externe Benutzer einrichten, können Sie externen Gruppen eine NetWitness Suite-Benutzerrolle zuordnen. Suchen Sie nach externen Gruppen, um die Gruppen auszuwählen, denen Sie eine NetWitness Suite-Rolle zuordnen möchten.

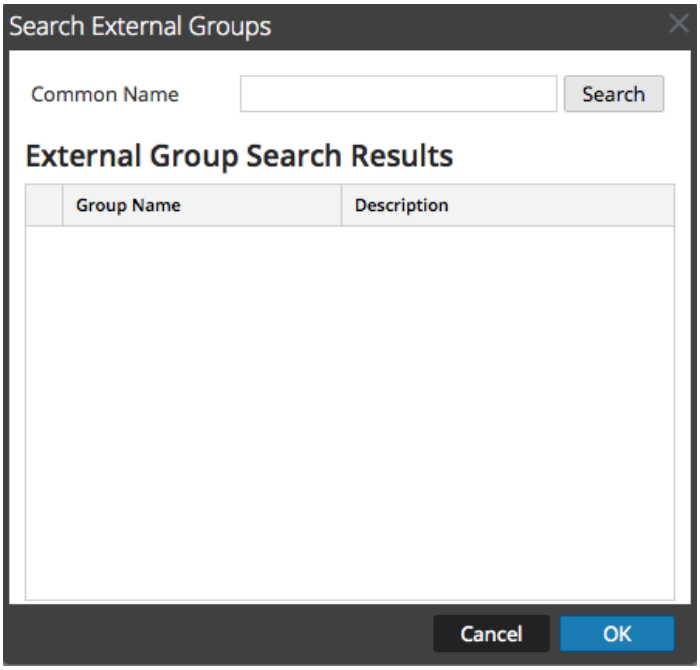
Was möchten Sie tun?

Rolle	Ich möchte...	Details anzeigen
Administrator	Einer externen Gruppe eine Rolle zuordnen	Schritt 5. (Optional) Zuordnen von Benutzerrollen zu externen Gruppen
Administrator	Externe Gruppenzuordnungen anzeigen	Registerkarte Externe Gruppenzuordnung
Administrator	Suchen nach externen Gruppen	Suchen nach externen Gruppen

So rufen Sie dieses Dialogfeld auf:

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Externe Gruppenzuordnung**.
3. Klicken Sie in der Symbolleiste auf +.
   Das Dialogfeld „Rollenzuordnung hinzufügen“ für die erstellte externe Authentifizierungsmethode wird angezeigt.
4. Wählen Sie im Bereich „Gruppenzuordnung“ eine **Domain** aus.

5. Klicken Sie im Bereich Gruppenzuordnung auf **Suchen**.
   Das Dialogfeld **Externe Gruppen durchsuchen** wird angezeigt.



In der folgenden Tabelle sind die Funktionen im Dialogfeld Externe Gruppen durchsuchen beschrieben.

Funktion	Beschreibung
Common Name	Gruppenname, nach dem Sie suchen. Kann dem exakten Namen entsprechen oder ein Sternchen(*) als Platzhalter enthalten, der für jedes beliebige Zeichen steht.
Gruppenname	Externe Gruppe, der Sie Rollen zuordnen können.
Beschreibung	Optionaler Text, der die Gruppe beschreibt.
OK	Das Dialogfeld Rollenzuordnung hinzufügen für die ausgewählte externe Gruppe wird angezeigt.
Abbrechen	Schließt das Dialogfeld.

Registerkarte Einstellungen

In diesem Thema wird die Ansicht Admin > Sicherheit > Registerkarte Einstellungen erläutert. In der Registerkarte Einstellungen konfigurieren Sie die Komplexität von Passwörtern für interne NetWitness Suite-Benutzer sowie systemweite Sicherheitsparameter.

Informationen zur Konfiguration der NetWitness Suite-Sicherheit finden Sie unter Einrichten von Systemsicherheit.

Die Anforderungen an die Komplexität von Passwörtern gelten ausschließlich für interne Benutzer; externe Benutzer sind davon nicht betroffen. Externe Benutzer müssen die Komplexität ihrer Passwörter anhand eigener Methoden und Systeme sicherstellen.

Was möchten Sie tun?

Rolle	Ich möchte...	Details anzeigen
Administrator	Konfigurieren der Passwortkomplexität	Schritt 1. Konfigurieren der PasswortkomplexitätKonfigurieren der Passwortkomplexität
Administrator	Konfigurieren von Sicherheitseinstellungen auf Systemebene	Schritt 3. Konfigurieren von Sicherheitseinstellungen auf Systemebene
Administrator	(Optional) Konfigurieren der externen Authentifizierung	Schritt 4. (Optional) Konfigurieren der externen Authentifizierung

Verwandte Themen

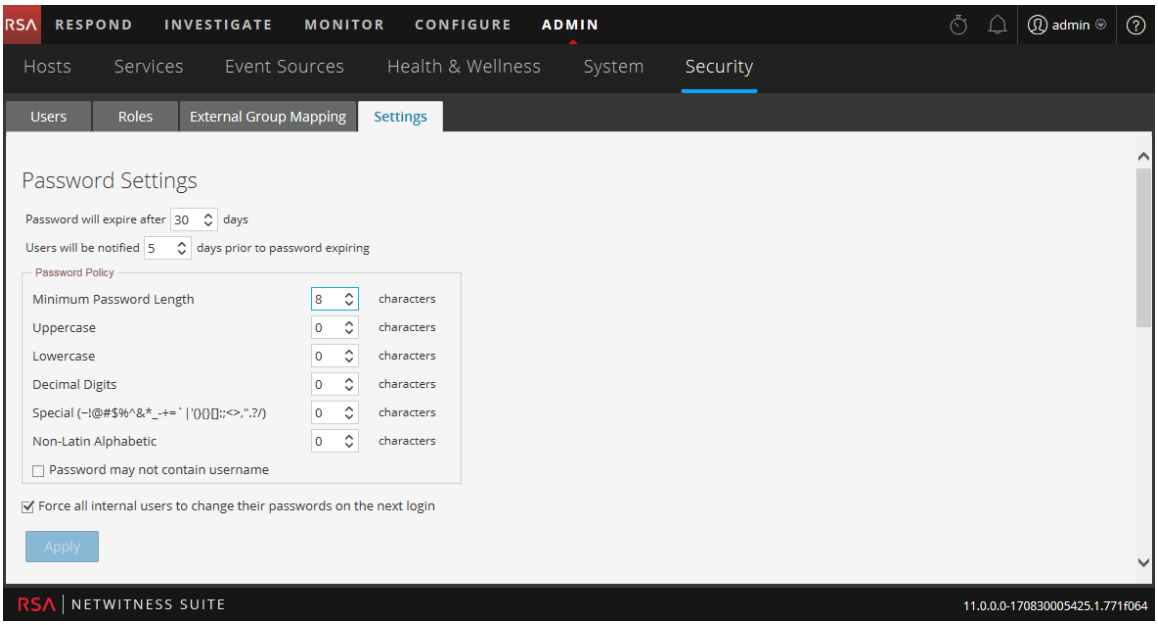
- Einrichten von Systemsicherheit

Ansicht Admin > Sicherheit > Registerkarte Einstellungen

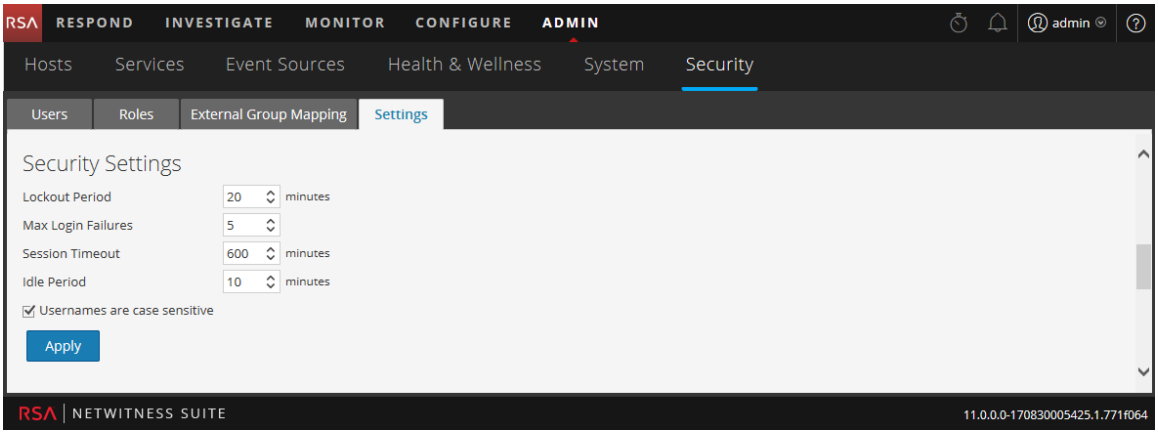
So rufen Sie die Registerkarte Einstellungen auf:

1. Navigieren Sie zu **ADMIN > Sicherheit**.
   Die Ansicht „Sicherheit“ wird mit geöffneter Registerkarte **Benutzer** angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.

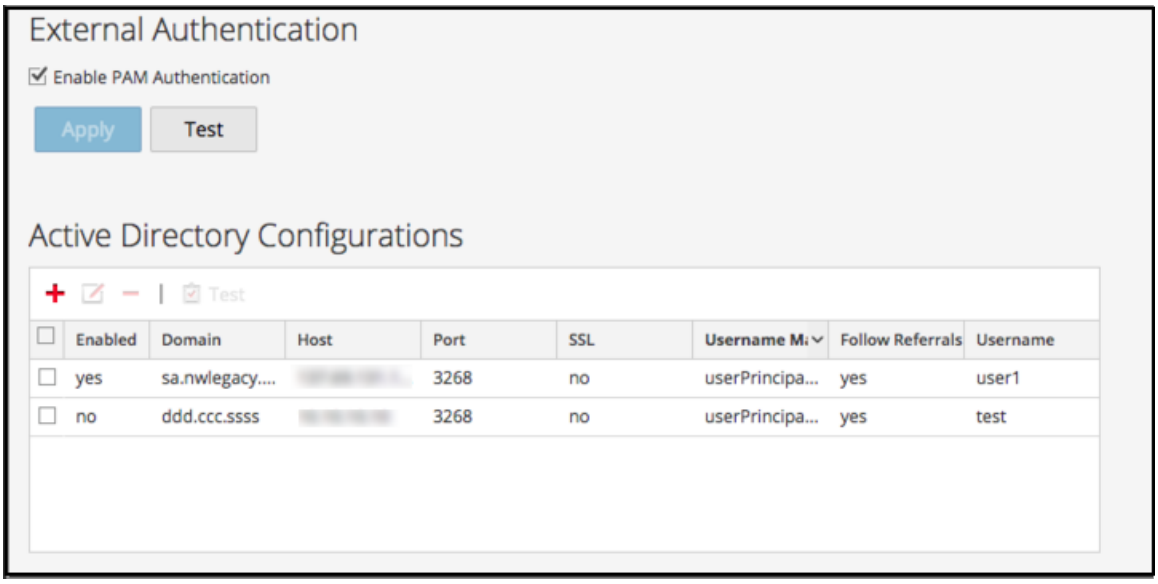
Die folgende Abbildung zeigt den Abschnitt Passworteinstellungen auf der Registerkarte „Einstellungen“.



Die folgende Abbildung zeigt den Abschnitt Sicherheitseinstellungen auf der Registerkarte Einstellungen.



Die folgende Abbildung zeigt die Abschnitte „PAM-Authentifizierung“ und „Active Directory-Konfigurationen“ auf der Registerkarte „Einstellungen“.



Passworteinstellungen

Im Abschnitt Passwortrichtlinie lassen sich die Anforderungen an die Komplexität von Passwörtern für interne Benutzer von NetWitness Suite konfigurieren, wenn diese ihre Passwörter festlegen.

Option	Beschreibung
Passwort läuft nach <n> Tagen ab	Die Standardanzahl der Tage, nach denen ein Passwort für alle internen NetWitness Suite-Benutzer abläuft. Beim Wert Null (0) ist der Ablauf der Passwortgültigkeit deaktiviert. Bei Neuinstallationen lautet der Standardwert 30. Für Upgrades wird der vorherige Wert automatisch auf die aktualisierte Installation migriert.
Benutzer werden <n> Tage vor Ablauf des Passworts benachrichtigt	Die Anzahl der Tage vor dem Ablaufdatum der Passwortgültigkeit, um den Benutzer zu benachrichtigen, dass sein Passwort bald abläuft Die Benutzer erhalten am angegebenen Datum vor dem Ablauf ihres Passworts einmalig eine E-Mail. Wenn Benutzer sich bei NetWitness Suite anmelden, wird das Dialogfeld „Meldung bei Passwortablauf“ angezeigt. Der Mindestwert ist 1 Tag.

Option	Beschreibung
Mindestkennwortlänge	Enthält die Anforderung an die Mindestkennwortlänge für NetWitness Suite-Benutzerpasswörter. Durch die Angabe einer Mindestkennwortlänge wird verhindert, dass zu kurze Kennwörter gewählt werden, die sich leicht erraten lassen.
Großbuchstaben	Gibt an, wie viele Großbuchstaben das Passwort mindestens enthalten soll. Dazu zählen die Buchstaben europäischer Sprachen von A bis Z, einschließlich diakritischer Zeichen, griechischer und kyrillischer Buchstaben. Beispiel: • Kyrillische Großbuchstaben: Д Ц • Griechische Großbuchstaben: Π Λ
Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben das Passwort mindestens enthalten soll. Dazu zählen die Buchstaben europäischer Sprachen von a bis z, scharfes s (ß) sowie diakritische Zeichen, griechische und kyrillische Buchstaben. Beispiel: • Kyrillische Kleinbuchstaben: д ц • Griechische Kleinbuchstaben: π λ
Dezimalstellen	Gibt an, wie viele Dezimalziffern (von 0 bis 9) das Passwort mindestens enthalten soll.
Sonderzeichen (~!@#$%^&*_-+=`|'() {}[]:;<>,".?/)	Gibt an, wie viele Sonderzeichen das Passwort mindestens enthalten soll: `~!@#$%^&*_-+=`|'(){}[]:;<>,".?/`
Zeichen aus nicht lateinischen Alphabeten	Gibt an, wie viele Zeichen des Unicode-Alphabets, die weder Groß- noch Kleinbuchstaben sind, mindestens enthalten sein sollen. Dazu zählen Unicode-Zeichen aus asiatischen Sprachen. Beispiel: • Kanji (Japanisch): 頁 (Blatt) 枒 (Baum)

Option	Beschreibung
Passwort darf nicht den Benutzernamen enthalten	Gibt an, dass ein Passwort nicht den Benutzernamen des Benutzers enthalten darf (ohne Berücksichtigung von Groß-/Kleinschreibung).
Alle internen Benutzer zwingen, bei der nächsten Anmeldung ihr Passwort zu ändern	Fordert alle internen Benutzer auf, ihr Kennwort bei der nächsten Anmeldung bei NetWitness Suite zu ändern. Beachten Sie, dass diese Einstellung standardmäßig aktiviert ist.
Anwenden	Die Einstellungen für die Passwortsicherheit werden wirksam, wenn NetWitness Suite-Benutzer ihre Passwörter erstellen oder ändern. Wenn **Alle internen Benutzer zwingen, bei der nächsten Anmeldung ihr Passwort zu ändern** ausgewählt ist, müssen alle internen Benutzer bei der nächsten Anmeldung in NetWitness Suite ihr Passwort ändern.

Sicherheitseinstellungen

Im Abschnitt Sicherheitseinstellungen können Sie globale Sicherheitseinstellungen für Benutzer von NetWitness Suite konfigurieren.

Option	Beschreibung
Sperrdauer	Gibt an, nach wieviel Minuten ein Benutzer aus NetWitness Suite ausgesperrt wird, nachdem die konfigurierte Anzahl fehlgeschlagener Anmeldungen überschritten wurde. Der Standardwert ist 20 Minuten.
Max. Anmeldungsfehler	Gibt an, nach wie vielen erfolglosen Anmeldeversuchen ein Benutzer gesperrt wird. Der Standardwert ist 5

Option	Beschreibung
Sitzungs-Timeout	Gibt die maximale Dauer einer Benutzersitzung bis zum Timeout an (in Minuten). Der Standardwert ist 600. Wenn der Wert 0 ist, gibt es keine Beschränkung für die Sitzungsdauer. Wenn der Wert eine positive Ganzzahl ist, wird die Sitzung deaktiviert, wenn die konfigurierte Zeit verstrichen ist. Der Benutzer muss sich dann erneut anmelden.
Leerlaufperiode	Gibt an, nach wieviel Minuten der Inaktivität eine Sitzung deaktiviert wird. Der Standardwert ist 10. Wenn der Wert 0 ist, wird die Sitzung nicht aufgrund eines Timeout deaktiviert.
Bei Benutzernamen müssen Sie die Groß- und Kleinschreibung beachten.	Wählen Sie diese Option aus, wenn im Feld „Benutzername“ im NetWitness Suite-Anmeldebildschirm die Groß- und Kleinschreibung beachtet werden soll. Beispiel: Wenn bei Benutzernamen die Groß- und Kleinschreibung beachtet wird, können Sie für die Anmeldung bei NetWitness Suite „admin“ verwenden, jedoch nicht „Admin“.
Anwenden	Übernimmt die Einstellungen mit sofortiger Wirkung.

PAM-Authentifizierung

Im Abschnitt PAM-Authentifizierung können Sie NetWitness Suite so konfigurieren, dass die Authentifizierung und Prüfung von Anmeldungen externer Benutzer durch Active Directory oder PAM erfolgt.

Option	Beschreibung
PAM-Authentifizierung aktivieren	Ermöglicht NetWitness Suite die Verwendung von PAM (Pluggable Authentication Modules) zur Authentifizierung externer Benutzeranmeldungen.
Anwenden	Übernimmt die PAM-Einstellungen bei der nächsten Anmeldung.
Test	Fordert einen Benutzernamen und ein Passwort an und testet dann die derzeit aktivierte PAM-Authentifizierungsmethode.

Active Directory-Konfigurationen

Im Abschnitt Active Directory-Konfiguration können Sie NetWitness Suite so konfigurieren, dass die Authentifizierung von Anmeldungen externer Benutzer durch Active Directory erfolgt.

Option	Beschreibung
Aktiviert	Aktiviert die Active Directory-Authentifizierung für Benutzer von NetWitness Suite.
Domain	Name der Domain, in der sich der Active Directory-Service befindet.
Host	Name des Hosts oder IP-Adresse, auf dem oder an der sich der Active Directory-Service befindet.
Port	Port am Host, der zur Active Directory-Serviceauthentifizierung verwendet wird.
SSL	Gibt an, ob der Active Directory-Service SSL verwendet.
Benutzernamenszuordnung	Gibt das in Active Directory für die Benutzernamenszuordnung verwendete Suchfeld an. Sie können dafür specify userPrincipalName (UPN) oder sAMAccountName angeben.
Referrals befolgen	Gibt an, obNetWitness Suite von Active Directory erzeugte LDAP-Referrals befolgt.
Benutzername	Wenn hier ein Benutzername angegeben wird, wird er mit dem Active Directory-Service verbunden, während Active Directory-Gruppen durchsucht werden. Diese Anmeldeinformation wird zu keinem anderen Zweck verwendet.