RSA NETWITNESS® PLATFORM

システム セキュリティとユーザ管 理ガイド

バージョン 11.2

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、Dellが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事上の責任が課せられる可能性があります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、これらの使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

この資料に記載される情報は、発行日時点で正確であるとみなされます。この情報は予告なく変更されることがあります。

2月 2019

目次

システム セキュリティとユーザ管 理

このガイドでは、セキュリティの設 定とユーザ アクセス制 御について説 明します。システム管 理者は、システム全 体の設 定、ユーザ アカウント、システム ロール、権 限、サービスへのアクセスについて理 解している必 要があります。

トピック

システム セキュリティの設 定

このトピックでは、システム セキュリティの実 装 手 順 について説 明します。次 のトピックの各 ステップでは、システム全 体 の設 定 について説 明します。NetWitness Platformにセキュリティを構 成 するには、このトピックの手 順 を実 行します。

トピック

ステップ1. パスワードの複 雑 性 の構 成

このトピックでは、システム全 体 のNetWitness Platformパスワードの複 雑 性 の要 件 について説 明 しま す。

パスワードはネット ワーク セキュリティ戦 略 上 、重 要 なロールを担 います。パスワードによって、コンピュー ター システムの最 前 線 で重 要 な保 護 を行 い、秘 密 情 報 への攻 撃 と不 正 アクセスを防 ぎます。

パスワード ポリシーは企 業 ネット ワークのセキュリティを向 上 させます。パスワード ポリシーは業 界 や企 業 の要 件 、規 制 などに応 じて異 なります。さまざまなパスワード ポリシーに対 応 するため、NetWitness Platformでは、NetWitness Platform内 部 ユーザ向 けのパスワードの複 雑 性 の要 件 を構 成 できます。こ れによって、企 業 のパスワード ポリシー ガイドラインに対 応 することができます。

パスワードの複 雑 性 の要 件 は、内 部 ユーザのみに適 用 され、外 部 ユーザには強 制 されません。外 部 ユーザは、外 部 認 証 システムの方 法 とシステムによってパスワードの複 雑 性 が管 理 されます。

また、グローバルのデフォルト ユーザ パスワード有 効 期 間 を設 定 し、パスワードの有 効 期 限 が近 くなった 内 部 ユーザに通 知 を送 信 するか否 か、送 信 する場 合 はそのタイミングを指 定 できます。パスワードの有 効 期 限 に関 する通 知 は、NetWitness Platformへのログオン時 に表 示 されるパスワード有 効 期 限 に関 するメッセージで構 成 されます。

パスワードの強 度

強 力 なパスワードにより、攻 撃 者 がユーザのパスワードを推 測 することがより困 難 になり、組 織 のネット ワークへの不 正 なアクセスを防 ぐのに役 立 ちます。NetWitness Platformユーザに対 して、適 切 なレベル のパスワード強 度 を定 義 することができます。パスワードの強 度 設 定 を構 成 すると、その設 定 がadmin ユーザを含 む内 部 NetWitness Platformユーザに適 用 されます。

管 理 者 は、次 のパスワード強 度 要 件 を任 意 に組 み合 わせ、NetWitness Platformユーザがパスワードの 作 成 や変 更 を行 う時 に強 制 することができます。

- 最 小 パスワード長
- 大 文 字 の最 小 数
- 小 文 字 の最 小 数
- 数 字 (0～9) の最 小 数
- 特 殊 文 字 の最 小 数
- 非 ラテン アルファベット 文 字 (アジア言 語 のUnicode文 字 を含 む) の最 小 数
- パスワードにユーザ名 を含 むことができるかどうか

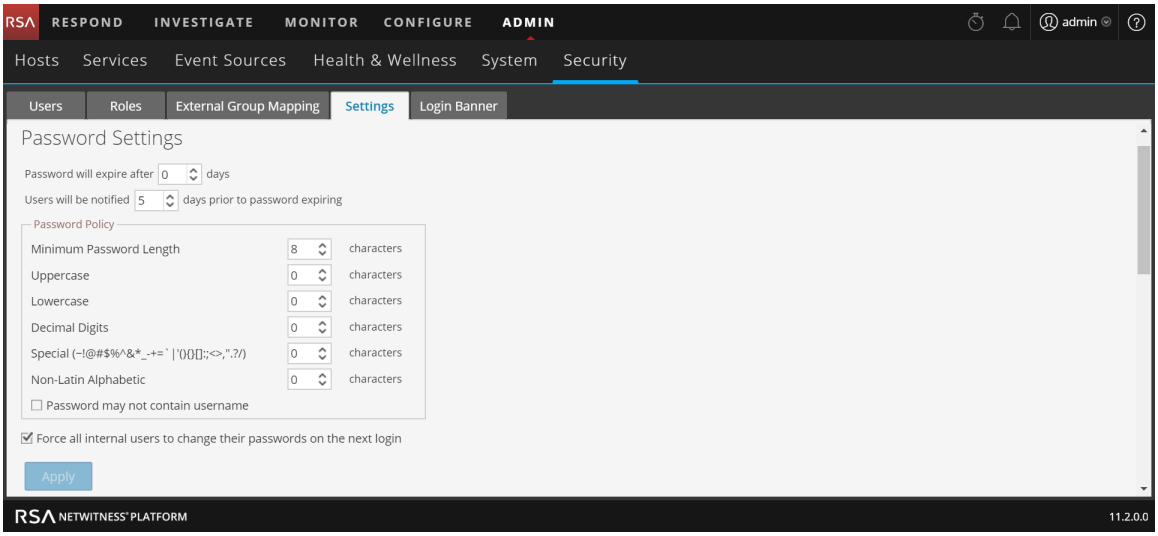
たとえば、最 小 8文 字 、ユーザのユーザ名 を含 むことは不 可 、大 文 字 と小 文 字 と数 字 と特 殊 文 字 を含 む、という強 力 なパスワード要 件 を設 定 できます。

非 ラテン アルファベット 文 字 の最 小 数 の要 件 を適 用 する場 合 には、ユーザがパスワードを設 定 する際 に それらの文 字 を使 用 できることを確 認 してください。

「*システム メンテナンス ガイド*」のトピック「STIG準 拠 パスワード」では、強 力 なパスワード ポリシーの例 を 提 示 しています。

パスワード強 度 の構 成

1. NetWitness Platformで、[管 理] > [セキュリティ]に移 動します。
   [セキュリティ]ビューが表 示され、[ユーザ]タブが開きます。
2. [設 定]タブをクリックします。



3. [パスワード設 定]セクションで、NetWitness Platformユーザが自 分 のパスワードを設 定 する際 に適 用 される、パスワードの複 雑 性 要 件 を選 択 し、必 要 な場 合 、最 小 文 字 数 要 件 を設 定 します。要 件 を適 用 しない場 合 は、最 小 値 が4文 字 の[最 小 パスワード長]を除 いて、値 を0に設 定 します。

要 件	説 明
パスワードの有 効 期 限 : <n>日	NetWitness Platform内 部 ユーザのデフォルトのパスワード有 効 期 間 の日 数 。値 にゼロ(0) を指 定 すると、パスワードの有 効 期 限 が無 効 化 されます。新 規 インスト ールの場 合 、デフォルト値 は0です。アップグレードの場 合 は、以 前 の値 は自 動 的 にアップグレード インストールに移 行 します。
パスワードの有 効 期 限 が切 れる<n>日 前 にユーザに通 知	パスワードの有 効 期 限 の何 日 前 になったら、ユーザにまもなくパスワードの有 効 期 限 が切 れることを通 知 するか。ユーザがNetWitness Platformにログインするとき に[パスワード有 効 期 限 切 れメッセージ]ダイアログが表 示 されます。最 小 値 は1 日 です。
最 小 パスワード長	パスワードの最 小 の長 さを指 定 します。最 小 パスワード長 を設 定 すると、ユーザ が、推 測 が容 易 な短 いパスワードを設 定 するのを防 ぐことができます。デフォルト で必 要 な最 小 パスワード長 は4文 字 です。
大 文 字	パスワードに含 める大 文 字 の最 小 数 を指 定 します。これにはAからZ(ダイアクリ ティカルマーク付 きを含 む) 、ギリシャ文 字 、キリル文 字 が含 まれます。例 : • キリル文 字 の大 文 字 : Д Ц • ギリシャ文 字 の大 文 字 : Π Λ

要件	説明
小文字	パスワードに含める小文字の最小数を指定します。これにはaからz(ダイアクリティカルマーク付きを含む) 、ギリシャ文字、キリル文字が含まれます。例 : • キリル文字の小文字 : д ц • ギリシャ文字の小文字 : π λ
数字	パスワードに使用する数字(0～9) の最小数を指定します。
特殊文字	パスワードに使用する特殊文字の最小数を指定します。次の特殊文字を使用できます。 ~!@#$%^&*_-+=`|'(){}[]:;<>,".?/
非ラテン アルファベット文字	大文字小文字以外のUnicode文字の最小数を指定します。これにはアジア言語のUnicode文字を含みます。例 : • 漢字(日本語) : 頁(leaf) 枒(tree)
パスワードにユーザ名を含めることを禁止	パスワードにユーザのユーザ名 (大文字と小文字を区別しない) を含むことを禁止します。

4. パスワード ポリシーの変更を次回のパスワード変更時ではなく次回のログイン時に反映させる場合は、[**すべての内部ユーザに次回ログイン時にパスワードの変更を強制**]を選択します。この設定は、デフォルトで選択されています。
5. [**適用**]をクリックします。
パスワードの強度設定は、内部ユーザがパスワードを作成または変更するときに有効になります。[**すべての内部ユーザに次回ログイン時にパスワードの変更を強制**]を選択した場合は、すべての内部ユーザがNetWitness Platformに次回ログオンするときにパスワードを変更する必要があります。

ステップ2. デフォルト のAdminパスワード の変 更

このトピックでは、NetWitness Platformサービスおよびコア サービスのadminパスワード の変 更 手 順 につい て説 明します。

NetWitness Platformではシステム管 理 者 のユーザ アカウント がインスト ールされています。ユーザ名 は **admin**です。デフォルト パスワード は、NetWitness Platformのインスト ール処 理 中 にTUI(テキスト ベース のユーザ インタフェース) に入 力 されたパスワード です。adminには**Administrators**ロール**ル**が割り当 てられ ています。このロールには、ユーザが実 行 できる操 作 とアクセスできるサービスを制 御 する完 全 なシステ ム権 限 があります。このアカウント に対 して実 行 できる変 更 は、パスワード の変 更 のみです。他 の NetWitness Platformユーザと異 なり、**admin**ユーザ パスワード の変 更 はダウンストリーム サービスに自 動 的 に伝 播 されません。パスワード の強 度 設 定 を構 成 すると、その設 定 がadminユーザを含 むすべての NetWitness Platformユーザに適 用 されます。

パスワード は、システムを保 護 するための最 も重 要 な要 素 となります。**admin**ユーザは、NetWitness Platformおよび各 コア サービスにプリインスト ールされています。セキュリティ確 保 のため、組 織 に必 要 な ユーザとロールをNetWitness Platformおよび各 コア サービスで作 成 します。

ベスト プラクティス

RSAでは、以 下 の項 目 を推 奨 しています。

- 各 サービスの**admin**パスワード をデフォルト から変 更 します。
- 各 サービスの**admin**アカウント に対 して異 なるパスワード を作 成 します。

NetWitness Platformのadminパスワード の変 更

NetWitness Platformの**admin**パスワード を[プロファイル]ビューで変 更 します。「*NetWitness Platform スタート ガイド*」の「パスワード の変 更 」を参 照 してください。**admin**ユーザのパスワード はコア サービスに伝 播 しません。

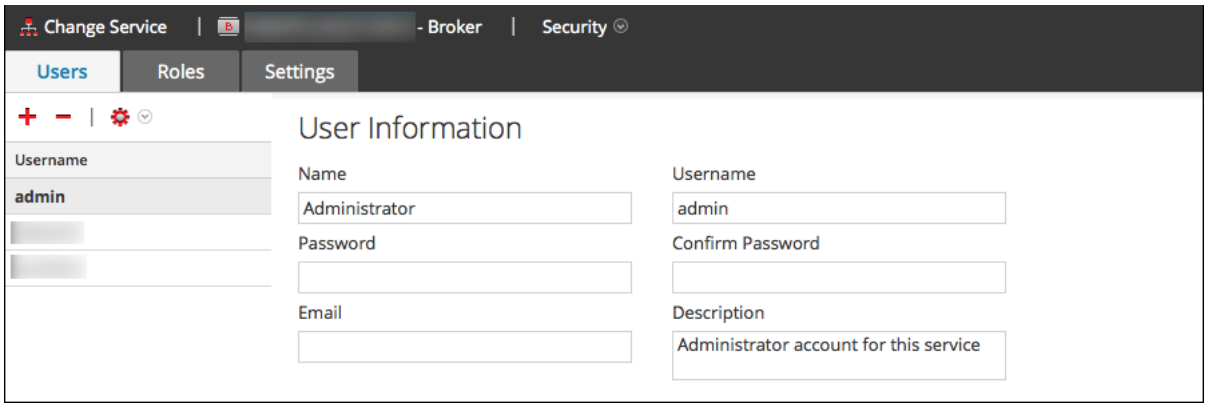
注 : adminパスワード を変 更 した後 で、Reporting Engineでデータ ソースを削 除 して、再 追 加 する必 要 があります。詳 細 については、「**Reporting Engineでのデータ ソースの削 除 と再 追 加** 」セクションを参 照 してください。

コア サービスのadminパスワード の変 更

コア サービスのadminパスワード を変 更 するには、次 の手 順 を実 行 します。

1. NetWitness Platformで、**[管 理]＞[サービス]**に移 動 します。
2. サービスを選 択 し、 **＞[表 示]＞[セキュリティ]**を選 択 します。

3. [**ユーザ**]タブで、**admin**ユーザを選 択します。



4. [**パスワード**]フィールドに、選 択したサービスの新しいadminパスワードを入 力します。
5. [**パスワードの確 認**]フィールドに、新しいパスワードを再 入 力します。
6. [**適 用**]をクリックします。

注 : adminパスワードを変 更した後 で、Reporting Engineでデータ ソースを削 除して、再 追 加する必 要 があります。詳 細については、下 記の「**Reporting Engineでのデータ ソースの削 除と再 追 加**」を参 照 してください。

Reporting Engineでのデータ ソースの削 除と再 追 加

Reporting Engineでは、データ ソースの検 証に、そのデータ ソースのユーザ名 とパスワードが使 用されます。データ ソースのユーザ名 またはパスワードを変 更した場 合 は、そのデータ ソースを削 除して、再 追 加する必 要 があります。

Reporting Engineでデータ ソースを削 除して再 追 加するには、次 の手 順を実 行します。

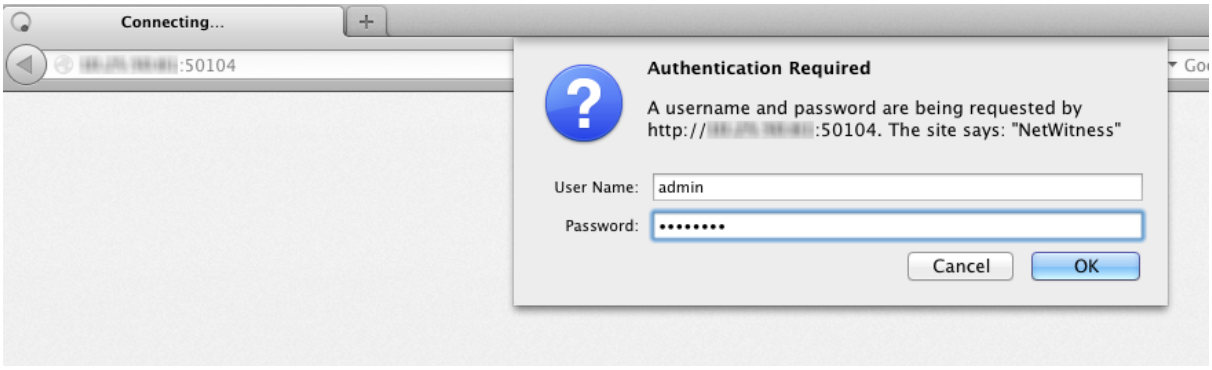
1. NetWitness Platformで、[**管 理**]＞[**サービス**]に移 動します。
2. [サービス]ビューでReporting Engineを選 択し、 [**表 示**]＞[**構 成**]を選 択します。
3. [**ソース**]タブをクリックします。
4. 削 除するサービスを選 択し、 をクリックします。
5. をクリックし、[**使 用 可 能なサービス**]を選 択します。
6. ステップ4で削 除したサービスを選 択し、[**OK**]をクリックします。
7. プロンプトが表 示されたら、サービスの新しいユーザ名 とパスワードを入 力します。

REST APIを使 用したサービスのadminパスワードの変 更

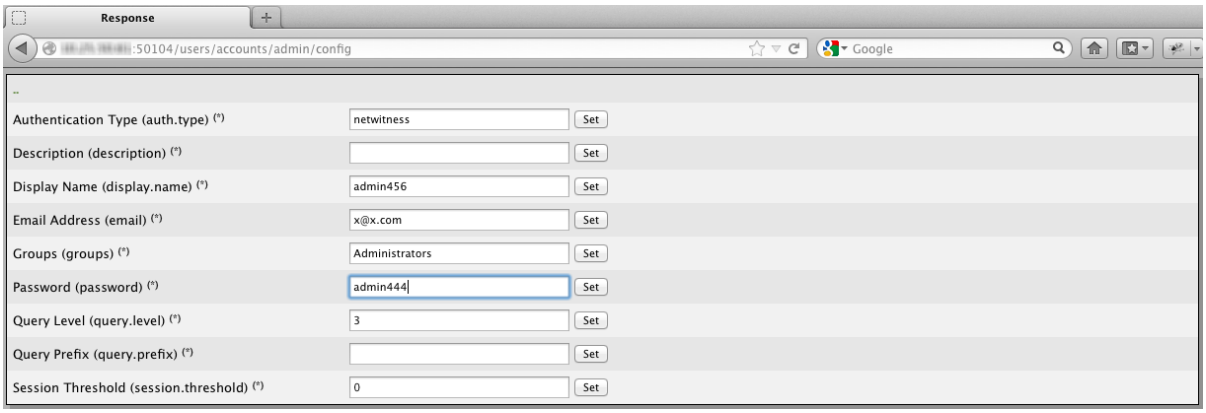
まれに、NetWitness Platformのユーザ インタフェースを使 用 せずに、コア サービスのadminパスワードを変 更しなければならないケースがあります。これは、コア サービスのパスワードを変 更する代 替 の方 法に過 ぎず、推 奨される方 法ではありません。

RESTユーザ インタフェースを使 用してサービスのadminパスワードを変 更するには、次 の手 順を実 行します。

1. Webブラウザを開き、次のURLに移 動します。
   <hostname>:<port>
   ここで、**hostname**はNetWitness Platformコア サービスの名 前 、**port**はREST通 信 に使 用されるポー トです。たとえば、Decoderに接 続 する場 合 は次 のようになります。
   `http://10.20.30.40:50104`
   認 証 ダイアログが表 示されます。



2. ダイアログで、サービスのadminとして認 証 に使 用されるユーザ名 とパスワードを入 力し、[**OK**]をク リックします。デフォルト のユーザ名 は**admin**、デフォルト のパスワード は**netwitness**です。
   サービスのRESTウィンド ウが表 示されます。
3. ノード ツリーで[**users**]＞[**accoutns**]＞[**admin**]＞[**config**]に移 動します。
   adminのユーザ構 成 フィールド がブラウザ ウィンド ウに表 示されます。



4. [パスワード]フィールド で、新しいadminパスワードを入 力し、[**設 定**]をクリックします。

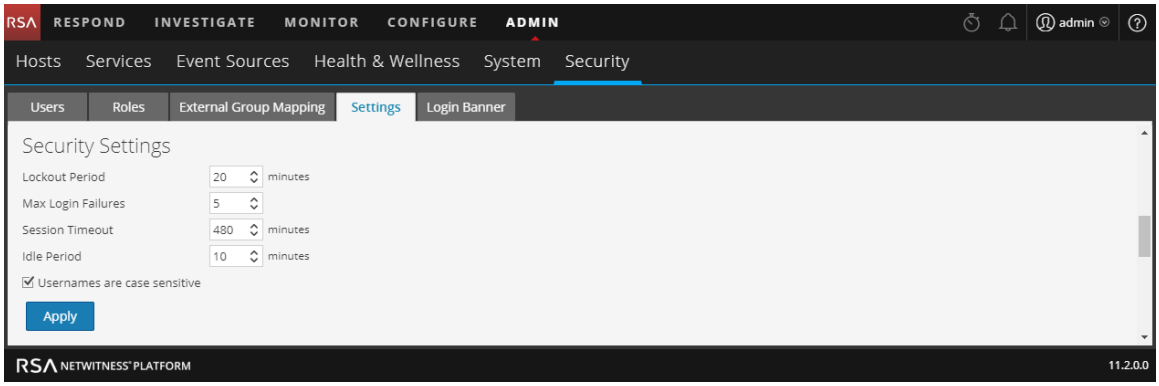
ステップ3. システム レベルのセキュリティ設 定 の構 成

このトピックでは、システム全 体 のセキュリティ パラメータを設 定 する方 法 について説 明します。

ログインの最 大 失 敗 回 数などの大 半 のグローバル セキュリティ設 定 は、NetWitness Platformのすべての ユーザとセッションに適 用されます。パスワード の有 効 期 間 やユーザ パスワード の有 効 期 限 が切 れるま でのデフォルト の日 数 のように、[パスワード の強 度]セクションにあるパスワード 関 連 の設 定 は、内 部 の NetWitness Platformユーザには適 用されますが、外 部 ユーザには適 用されません。

セキュリティ設 定 の構 成

1. NetWitness Platformで、**[管 理]＞[セキュリティ]**に移 動します。
   [セキュリティ]ビューが表 示され、[**ユーザ**]タブが開きます。
2. [**設 定**]タブをクリックします。



3. [**セキュリティ設 定**]セクションで、次 の表 の説 明 に従 って各 フィールド の値 を指 定します。

フィールド	説 明
ロックアウト 期 間	ユーザが最 大 ログイン失 敗 回 数 を超 過 した後 、NetWitness Platformからロックアウ トされる期 間 (分) 。デフォルト 値 は20分 です。
最 大 ログイ ン失 敗 回 数	ユーザがログインを失 敗 できる最 大 回 数 。ユーザは、ここで指 定 した回 数 ログイン に失 敗 するとロックアウト されます。デフォルト 値 は5です。
セッション タ イムアウト	タイムアウト するまでに許 可 されるユーザ セッションの最 長 期 間 (分 単 位) 。デフォル ト値 は480です。設 定 された時 間 が経 過 すると、セッションがタイムアウトし、ユーザ は再 度 ログインする必 要 があります。許 可 された最 大 値 は30,000です。 **注 :** NetWitness Platformをバージョン10.6.xから11.xに移 行 し、以 前 は無 制 限 の セッション タイムアウト を示 す値 0を使 用していた場 合 、その値 は自 動 的 に30,000 分 にリセット されました(値 0はサポート されなくなったため) 。

フィールド	説 明
アイド ル期 間	セッションがタイムアウト するまでのアイド ル状 態 の期 間(分) 。デフォルト 値 は10で す。許 可 された最 大 値 は30,000です。 **注 :** NetWitness Platformをバージョン10.6.xから11.xに移 行し、以 前 は無 制 限 の アイド ル期 間 を示 す値 0を使 用していた場 合 、その値 は自 動 的にデフォルト 値 10 にリセット されました(値 0はサポート されなくなったため) 。
ユーザ名 は 大 文 字 と小 文 字 が区 別 されま す。	NetWitness Platformログイン画 面 のユーザ名 フィールド で大 文 字 と小 文 字 を区 別 する場 合 は、このオプションを選 択 します。たとえば、ユーザ名 が大 文 字 と小 文 字 を 区 別 する場 合 、NetWitness Platformへのログオンにadminを使 用 することはでき ますが、Adminを使 用 することはできません。

4. [**適 用**]をクリックします。セキュリティ設 定 はすぐに反 映 されます。パスワード の有 効 期 限 が切 れる と、パスワード を変 更 するよう求 めるプロンプト がNetWitness Platformへのログオン時 に表 示 されま す。

ステップ4. (オプション) 外 部 認 証 の構 成

このトピックでは、NetWitness Platformでサポートされる外 部 認 証 方 法を紹 介しています。

ユーザがログインを試 行 すると、NetWitness Platformはまずローカル認 証を試みます。ローカル ユーザが見 つからず、外 部 認 証の構 成が有 効な場 合 、外 部 認 証を試 行します。

外 部 認 証を使 用 すると、NetWitness Platformの内 部 ユーザ アカウントを持 たないユーザでもNetWitness Platformにログオンし、ロールに基 づいた権 限を持 つことができます。

NetWitness Platformでサポートされる外 部 認 証 方 法は、Active DirectoryとPAM(Pluggable Authentication Module) の2つです。それぞれの認 証 方 法の構 成とテストの方 法について、このセクションの各トピックで説 明します。

トピック

- Active Directoryの構 成
- PAMのログイン機 能 の構 成

Active Directoryの構成

このトピックでは、Active Directoryを使用して外部ユーザを認証するようNetWitness Platformを構成する方法について説明します。

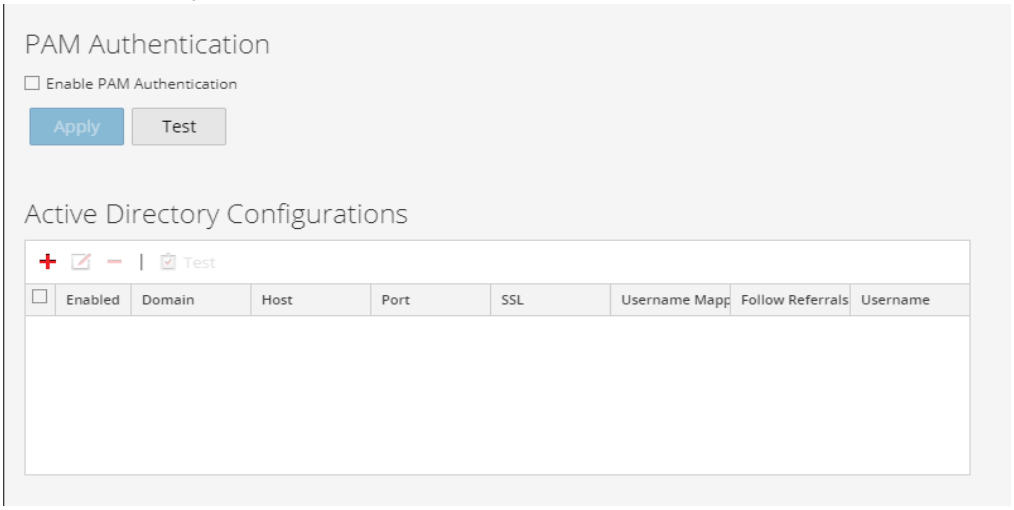
ユーザがログインを試行すると、NetWitness Platformはまずローカル認証を試みます。ローカル ユーザが検出されず、Active Directory構成が有効である場合、Active Directoryサービスでの認証が試行されます。[管理]＞[セキュリティ]ビュー＞[設定]タブで、Active Directoryを設定し、外部グループの認証を有効にすることができます。

複数の認証サーバを使用する環境では、LDAP転送により、ADグループ検索のためのLDAPリフェラルの利用が可能になります。LDAP転送を使用すると、ログオンにかかる時間が長くなる可能性があります。これは、ADグループ検索が、接続済みの認証サーバへと拡張されるためです。ADインスタンスがファイアウォールでブロックされているドメイン コントローラに接続を試みると、ユーザがNetWitness Platformへログオンする際に数分の遅延が発生する可能性があります。NetWitness Platformには、LDAP転送を実行するかどうか指定する構成オプションがあります。デフォルトでLDAPリフェラルは無効になっています。LDAPリフェラルが無効の場合、ADインスタンスは参照先のドメイン コントローラに接続を試みません。

注：[設定]タブには、PAM構成を有効化するオプションもあります。PAM構成は、Active Directory構成と同時に使用できます。PAM認証を有効化および構成する方法については、「PAMのログイン機能の構成」を参照してください。

Active Directory認証の構成

1. **[管理]＞[セキュリティ]**に移動します。
   [セキュリティ]ビューが表示され、[**ユーザ**]タブが開きます。
2. [**設定**]タブをクリックします。
   Active Directory構成リストがパネルに表示され、構成を追加または編集できます。



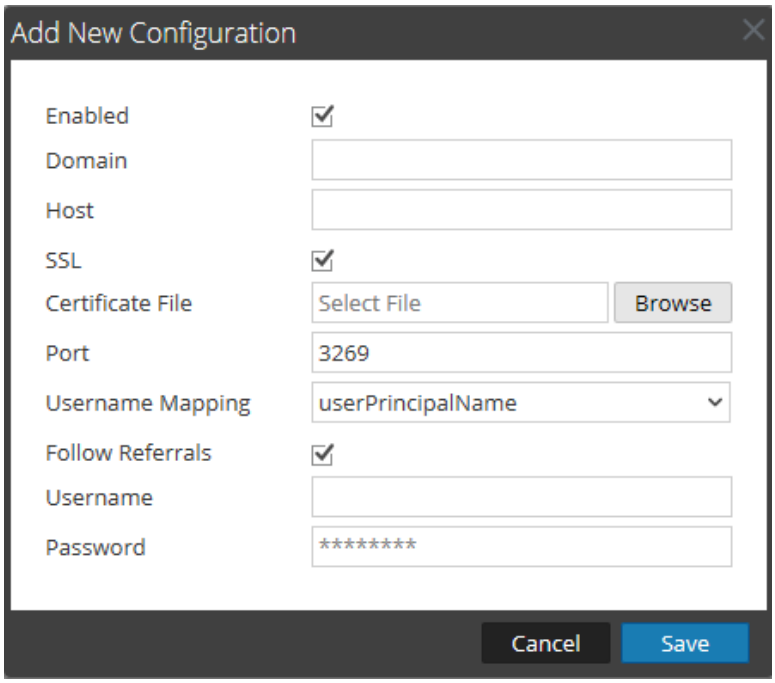
3. 必要に応じて、以下のセクションの説明に従ってドメインを追加、編集、または削除します。
   このリストに追加されたドメインは[外部グループ マッピング]タブに自動的に表示され、セキュリティロールを各グループに割り当てることができます。

注 : Active Directoryで認 証 するユーザに適 用 するセキュリティ ロールを構 成 する場 合 は、「ステップ5. (オプション) 外 部 グループへのユーザ ロールの割り当 て」を参 照してください。

新しいActive Directory構 成 の追 加

Active Directory構 成 リストに新しいActive Directory構 成 を追 加 するには、次 の手 順 を実 行します。

1. [Active Directory構 成]で+をクリックします。
   [新しい構 成 の追 加]ダイアログが表 示されます。



2. [**有 効**]チェックボックスを選 択します。
3. Active Directoryサービスの**ドメイン**、**ホスト**、**ポート**情 報を入 力します。
4. (オプション) この設 定 でSSLを選 択 するには、[**SSL**]チェックボックスをオンにします。次 に、[**参 照**]をクリックし、アップロードするファイルを選 択 することで、Active Directoryサーバの証 明 書 ファイルを入 力する必 要 があります。
5. [**ユーザ名 マッピング**]フィールドで、ユーザ名 マッピングに使 用 するActive Directory検 索 フィールドを選 択します。UPN(userPrincipalName) またはsAMAccountNameを選 択 できます。
6. 複 数 の認 証 サーバがあるサイトの場 合 、[**リフェラルのフォロー**]をクリックして、ADグループ検 索 のためのLDAP参 照 のリフェラルを有 効 または無 効 にします。
7. Active Directoryグループの検 索 時 に、Active Directoryサービスにバインドするための認 証 情 報 を提 供 するには、[**ユーザ名**]フィールドと[**パスワード**]フィールドに認 証 情 報 を入 力します。

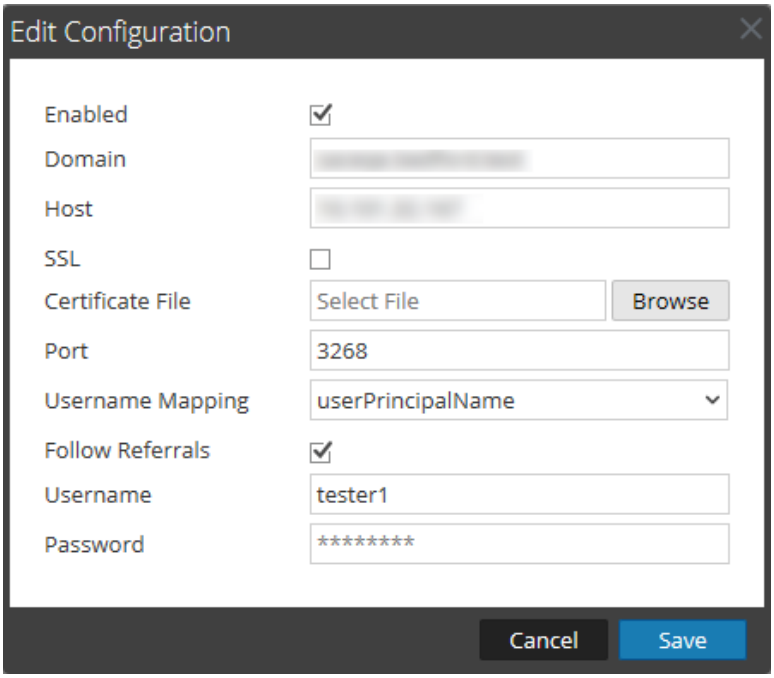
注 : [**ユーザ名 マッピング**]フィールドでsAMAccountNameを選 択 した場 合 は、認 証 に使 用 するユーザ名 を「ドメイン\ユーザ」の形 式 で入 力する必 要 があります。

8. [**保 存**]をクリックします。
   新しい構 成 がActive Directory構 成 リストに表 示されます。

Active Directory構成の編集

Active Directory構成リストのActive Directory構成を編集するには、次の手順を実行します。

1. [**Active Directory構成**]で、編集する構成を選択して をクリックします。
   [構成の編集]ダイアログが表示されます。



2. (オプション) Active Directoryサービスの**ドメイン**、**ホスト**、**ポート**情報を入力します。
3. (オプション) この設定でSSLを選択するには、[**SSL**]チェックボックスをオンにします。次に、[**参照**]をクリックし、アップロードするファイルを選択することで、Active Directoryサーバの証明書ファイルを入力する必要があります。
4. (オプション) [**ユーザ名 マッピング**]フィールドで、ユーザ名マッピングに使用するActive Directory検索フィールドを選択します。
5. 複数の認証サーバがある環境でLDAPリフェラルのフォローを指定するには、[**リフェラルのフォロー**]チェックボックスをオンにします。
   a. LDAP転送を無効化する場合は、ボックスをオフにします。
   b. LDAP転送を有効にする場合は、ボックスをオンにします。
6. Active Directoryグループの検索時に、Active Directoryサービスにバインドするための認証情報を提供するには、[**ユーザ名**]フィールドと[**パスワード**]フィールドに認証情報を入力します。
7. [**保存**]をクリックします。
   構成がActive Directory構成リストに表示されます。

Active Directory構 成 のテスト

Active Directory構 成をテストするには、次 の手 順を実 行します。

1. Active Directory構 成リストからテストする構 成を選 択します。
2. ツールバーで Test をクリックします。
   テストに成 功したことを示 すメッセージが表 示されます。
3. テストが成 功しない場 合 は、構 成を確 認して編 集します。

Active Directory構 成 の削 除

Active Directory構 成を削 除するには、次 の手 順を実 行します。

1. [Active Directory構 成]で、Active Directory構 成リストから削 除する構 成を選 択します。
2. ツールバーで ー をクリックします。
   選 択したActive Directory構 成を削 除すると、その構 成 のすべてのユーザがNetWitness Platformに ログインできなくなることを警 告するメッセージが表 示されます。
3. 次 のいずれかを実 行します。
   a. 削 除を確 定するには、[**はい**]をクリックします。
   b. 削 除をキャンセルするには、[**いいえ**]をクリックする。

PAMのログイン機能の構成

このトピックでは、PAM(Pluggable Authentication Module) を使用して外部ユーザを認証するようNetWitness Platformを構成する方法について説明します。

PAMログイン機能は次の2つの別々のコンポーネントで構成されます。

- ユーザ認証用のPAM
- グループ認証用のNSS

この2つの組み合わせによって、外部ユーザは内部のNetWitness Platformアカウントを持っていなくても、NetWitness Platformにログインし、外部グループとNetWitness Platformセキュリティ ロールのマッピングによって指定された権限やロールの付与を受けることができます。ログインに成功するには、両方のコンポーネントが必要です。

外部認証はシステム レベルの設定です。PAMを構成する前に、ここに示すすべての情報を確認しておいてください。

Pluggable Authentication Module

PAMは、Linuxが提供しているライブラリの1つで、ユーザをRADIUS、Kerberos、LDAPなどの認証プロバイダーに対して認証する機能を提供します。実装では、認証プロバイダーごとに専用のモジュールが使用されます。このモジュールは、pam_ldapのようなオペレーティング システム(OS) パッケージの形式になっています。NetWitness Platformでは、OSが提供するPAMライブラリと、そのPAMライブラリを使用するように構成されたモジュールを使用して、ユーザを認証します。

注 : PAMが提供するのは認証機能のみです。

ネーム サービス スイッチ

NSSはLinuxの機能の1つで、OSとアプリケーションはNSSが提供するデータベースを使用して、ホスト名などの情報、ホーム ディレクトリ、プライマリ グループ、ログイン シェルなどのユーザ属性を検出し、また、特定のグループに属するユーザの一覧を取得したりします。PAMと同様、NSSも設定可能で、モジュールを使用してさまざまなタイプのプロバイダーとやり取りします。NetWitness Platformでは、OSが提供するNSS機能を使用して外部PAMユーザに権限を付与します。具体的には、そのユーザがNSSに既知であるかどうかを検索し、ユーザが属しているグループをNSSにリクエストします。NetWitness Platformはリクエストの結果をNetWitness Platformの外部グループ マッピングと比較し、一致するグループが見つかれば、外部グループ マッピングで定義されているセキュリティ レベルでNetWitness Platformにログオンするためのアクセス権をユーザに付与します。

注 : NSSでは認証を提供しません。

PAMとNSSの組み合わせ

外部ユーザがNetWitness Platformへのログインを許可されるには、PAM(認証) とNSS(権限付与) の両方に成功する必要があります。PAMの構成とトラブルシューティングの手順は、NSSの構成とトラブルシューティングの手順と異なります。このガイドでは、PAMの例として、Kerberos、LDAP、RADIUSを取り上げています。また、NSSの例として、LDAPとUNIXを取り上げています。使用されるPAMとNSSのモジュールの組み合わせは、組織の要件によって決定されます。

プロセスの概 要

PAMログイン機 能を構 成 するには、このド キュメント の説 明に従って、各 ステップを実 行してください。

1. PAMモジュールの構 成 とテスト
2. NSSサービスの構 成 とテスト
3. NetWitness ServerでのPAMの有 効 化
4. NetWitness Serverでのグループ マッピングの作 成

前 提 条 件

PAMの構 成 を開 始 する前 に、実 装 するPAMモジュールに応 じて、手 順 を確 認 し、外 部 認 証 サーバの詳 細 情 報 を収 集 してください。

NSSの構 成 を開 始 する前 に、使 用 するNSSサービスに応 じて手 順 を確 認 し、外 部 グループ マッピングで使 用 するグループ名 を特 定 して、外 部 認 証 サーバの詳 細 情 報 を収 集 してください。

NetWitness PlatformでPAMの構 成 を開 始 する前 に、外 部 グループ マッピングで使 用 するグループ名 を特 定 してください。ロールをマッピングする際 、NetWitness Platform内 のロールが、外 部 の認 証 サーバに存 在 するグループ名 と一 致 する必 要 があります。

PAMモジュールの構 成 とテスト

以 下 のセクションのいずれかを選 択 して、PAMコンポーネント のセット アップと構 成 を実 行 してください。

- PAM Kerberos
- PAM RADIUS
- SecurID向 けPAMエージェント

PAM Kerberos

Kerberos通信ポート : TCP 88

Kerberosを使用するPAM認証を構成するには、以下のステップを実行します。

1. 次のコマンドを実行します(ただし、まずはkrb5-workstationパッケージがお客様の環境にインストールされていることを確認します) 。
   ```
   yum install krb5-workstation pam_krb5
   ```
2. Kerberos設定ファイル/etc/krb5.confで以下の行を編集します。変数(山括弧<>で囲まれた部分) は、実際の値に置き換えてください。大文字で表記されている部分は、実際の値を大文字で入力する必要があります。

   ```
   # 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. 次のコマンドを使用して、Kerberos構成をテストします。
   ```
   kinit <user>@<DOMAIN.COM>
   ```
   パスワードの入力後に何も出力されない場合は、成功したことを示しています。
4. NetWitness ServerのPAM構成ファイル/etc/pam.d/securityanalyticsを編集して、次の行を追加します。ファイルが存在しない場合は、ファイルを作成し、次の行を追加します。
   ```
   auth sufficient pam_krb5.so no_user_check
   ```

PAM Kerberosの構 成 はこれで完 了 です。次 のセクション「NSSサービスの設 定 とテスト 」に進 みます。

PAM RADIUS

RADIUS通 信 ポート : UDP 1812またはUDP 1813

RADIUSを使 用 するPAM認 証 を構 成 するには、NetWitness ServerをRADIUSサーバのクライアント リストに追 加 し、共 有 シークレットを構 成 する必 要 があります。これを実 行 する手 順 については、RADIUSサーバ管 理 者 に問い合 わせてください。

RADIUSを使 用 してPAM認 証 を設 定 するには、以 下 のステップを実 行 します。

1. 次 のコマンドを実 行 します(ただし、まずはpam_radius_authパッケージがお客 様 の環 境 にインストールされていることを確 認 します) 。
   ```
   yum install pam_radius_auth
   ```
2. RADIUS構 成 ファイル/etc/raddb/serverを以 下 のように編 集 します。
   ```
   # server[:port] shared_secret  timeout (s)
   server     secret      3
   ```
3. NetWitness ServerのPAM構 成 ファイル/etc/pam.d/securityanalyticsを編 集 して、次 の行 を追 加 します。ファイルが存 在 しない場 合 は、ファイルを作 成 し、次 の行 を追 加 します。
   ```
   auth sufficient pam_radius_auth.so
   ```
4. 次 のコマンドを実 行 して、RADIUSライブラリをコピーします。
   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```

注 意 : PAM RADIUSを機 能 させるには、/etc/raddb/serverファイルに書 き込 み権 限 が必 要 です。これに必 要 なコマンドは次 のとおりです : `chown netwitness:netwitness /etc/raddb/server`。

注 意 : PAM RADIUSに対 して上 記 の変 更 を行 った後 は、Jettyサーバを再 起 動 する必 要 があります。これに必 要 なコマンドは次 のとおりです。
```
systemctl restart jetty
```

PAMモジュールおよび関 連 サービスは/var/log/messagesと/var/log/secureに情 報 を出 力 します。これらの出 力 は、設 定 問 題 のトラブルシューティングを支 援 するために使 用 できます。

次 の手 順 では、SecurIDを使 用 してRADIUSのPAM認 証 を構 成 する例 を示 します。

注 : これらのタスクの例 では、RADIUSサーバとしてRSA Authentication Managerを使 用 します。

1. 次 のコマンドを実 行 します(ただし、まずはpam_radius_authパッケージがお客 様 の環 境 にインストールされていることを確 認 します) 。
   ```
   yum install pam_radius_auth
   ```
2. RADIUS構 成 ファイル/etc/raddb/serverを編 集 し、Authentication Managerインスタンスのホスト名 、共 有 シークレット、タイムアウト値 を使 用 して更 新 します。
   ```
   # server[:port] shared_secret timeout (s)
    111.222.33.44         secret        1
    #other-server        other-secret 3
    192.168.12.200:6369 securid      10
   ```

注 : 127.0.0.1とother-serverの行をコメント アウトし、Authentication Managerプライマリ インスタンスのIPアドレス、RADIUSポート番 号(たとえば192.168.12.200:1812) 、RADIUS共 有シークレット 、タイムアウト 値(10) を追 加する必 要 があります。

3. NetWitness ServerのPAM構 成ファイル/etc/pam.d/securityanalyticsを編 集して、次 の行を追 加します。ファイルが存 在しない場 合 は、ファイルを作 成し、次 の行を追 加します。

   ```
   auth sufficient pam_radius_auth.so
   ```

   注 : /etc/pam.d/securityanalyticsファイル内 にある前 述 の行 の最 後 にdebugを追 加 することで、PAMのデバッグ機 能(たとえばauth sufficient pam_radius_auth.so debug) を有 効化 することができます。

4. 次 のコマンドを実 行して、RADIUSライブラリをコピーします。

   ```
   cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
   ```

PAMモジュールおよび関 連 サービスは/var/log/messagesと/var/log/secureに情 報を出 力します。これらの出 力 は、構 成 問 題 のトラブルシューティングを支 援 するために使 用 できます。

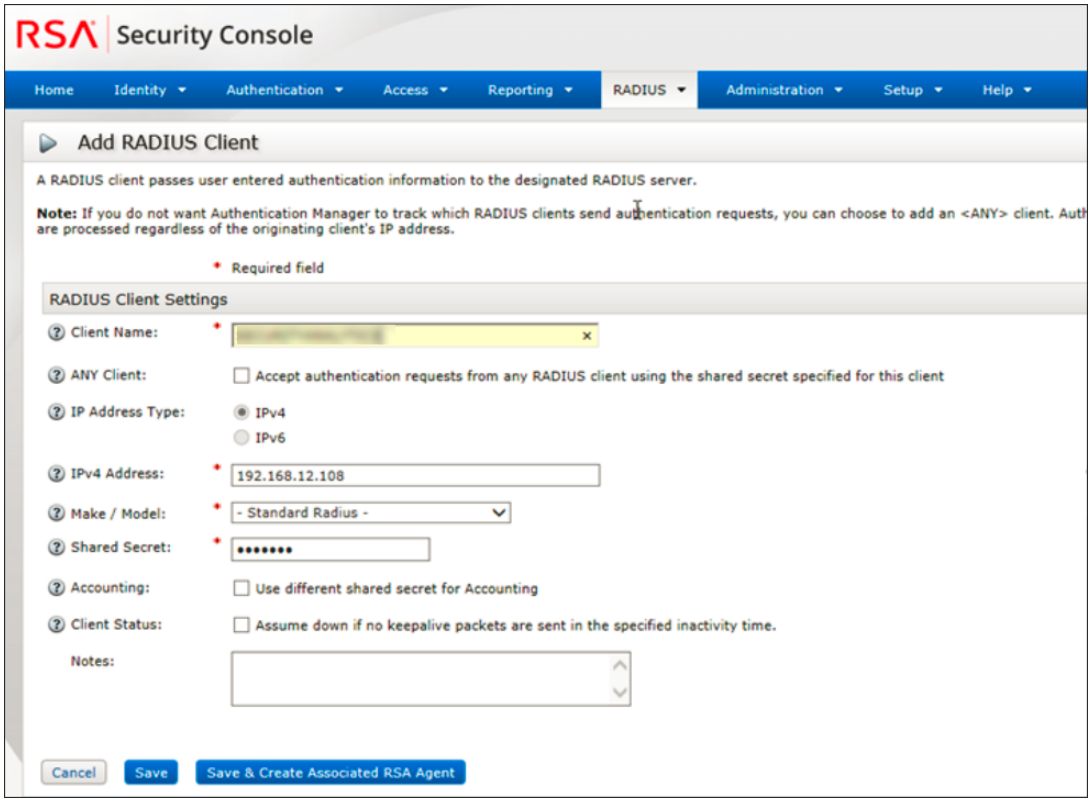
RADIUSクライアントと関 連 エージェントの追 加

注 : これらのタスクの例 では、RADIUSサーバとしてRSA Authentication Managerを使 用します。管 理 者 アカウントの認 証 情 報 を使 用して、RSA Authentication Manager Security Consoleにログオンする必 要 があります。

RADIUSクライアントと関 連 エージェントを追 加 するには、次 のステップを実 行します。

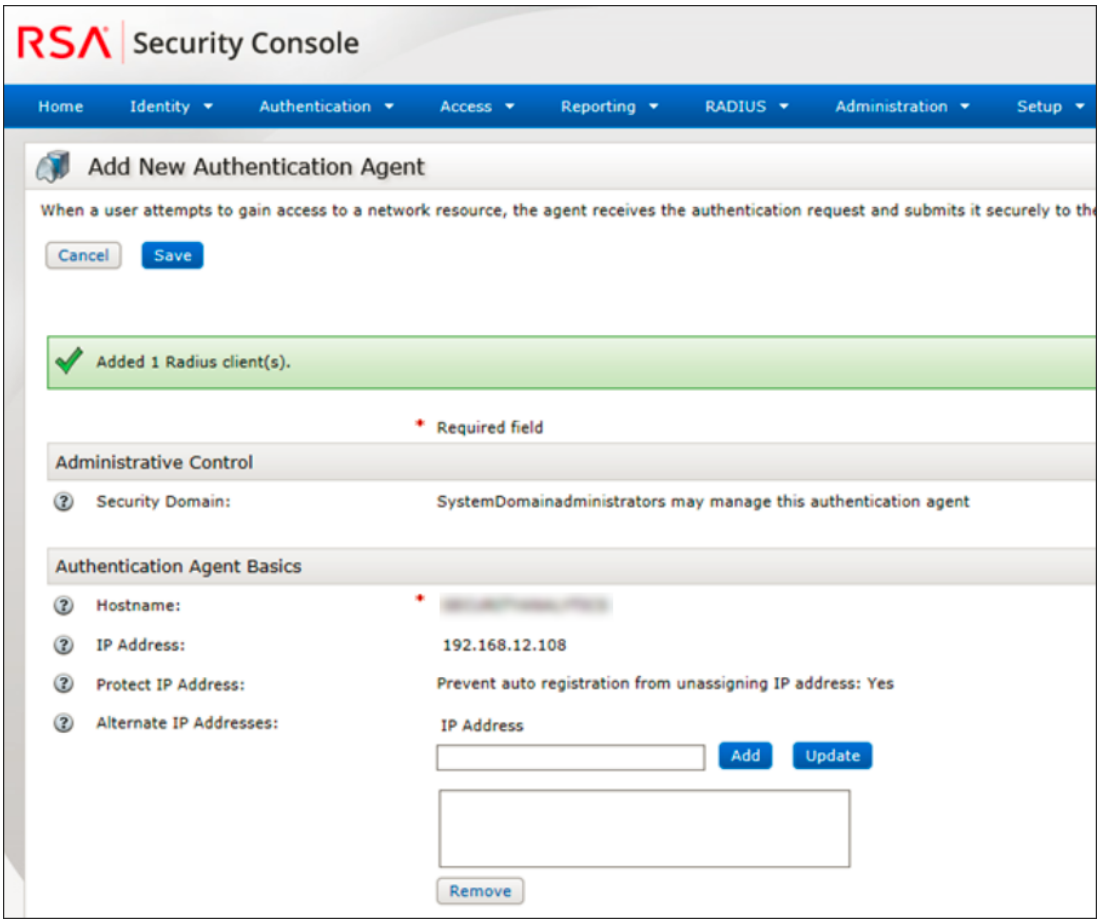
1. RSA Authentication Managerにログオンします。
   Security Consoleが表 示されます。

2. Security Consoleで、[**RADIUS**]＞[**RADIUSクライアント**]＞[**新規追加**]の順にクリックします。
[RADIUSクライアントの追加]ページが表示されます。



3. [RADIUSクライアントの設定]で、次の情報を指定します。
   a. [**クライアント名**]フィールドに、クライアントの名前(たとえば、NetWitness Platform)を入力します。
   b. [**IPv4アドレス**]フィールドに、RADIUSクライアントのIPv4アドレス(たとえば、192.168.12.108)を入力します。
   c. [**製造元/モデル**]ドロップダウンリストで、RADIUSクライアントのタイプ(たとえば、Fortinet)を選択します。
   d. [**共有シークレット**]フィールドに、認証共有シークレットを入力します。

4. [**保存と関連するRSAエージェントの作成**]をクリックします。



5. [**保存**]をクリックします。

Authentication Managerインスタンスがネットワーク上の認証エージェントを見つけることができない場合、警告ページが表示されます。[**はい、エージェントを保存します**]をクリックします。

詳細については、『*RSA Authentication Manager 8.2管理者ガイド*』の「RADIUSクライアントの追加」のトピックを参照してください。

PAM RADIUSの構成はこれで完了です。次のセクション「NSSサービスの設定とテスト」に進みます。

SecurID向 けPAMエージェント

PAM通信ポート - UDP 5500

前提条件

RSA SecurID PAMモジュールは、以下の条件が満たされている場合にのみサポートされます。

- 信頼接続がNetWitness Platformとコア サービス間で有効になり、機能していなければなりません。

プロセスの概要

SecurID PAMモジュールのおおまかな設定ステップは次のとおりです。

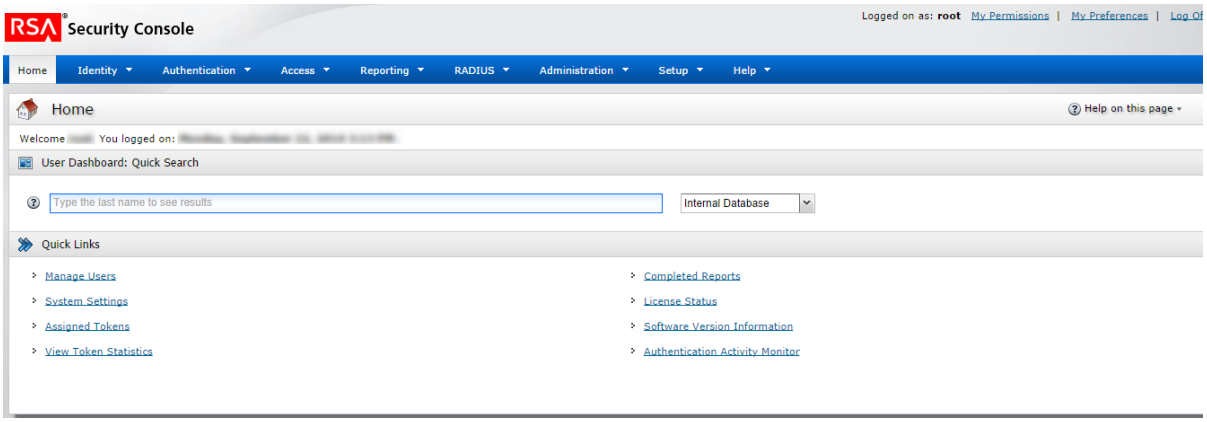
1. **Authentication Manager**を設定します。
   a. AuthenticationAgentを追加します。
   b. 設定ファイルを作成してダウンロードします。
2. **NetWitness Server**を設定します。
   a. Authentication Managerから設定ファイルをコピーしてカスタマイズします。
   b. PAM SecurIDモジュールをインストールします。
3. 接続と認証をテストします。

後述の残りの手順を実行します。

- NSSサービスの設定とテスト
- NetWitness ServerでのPAMの有効化
- NetWitness Serverでのグループ マッピングの作成

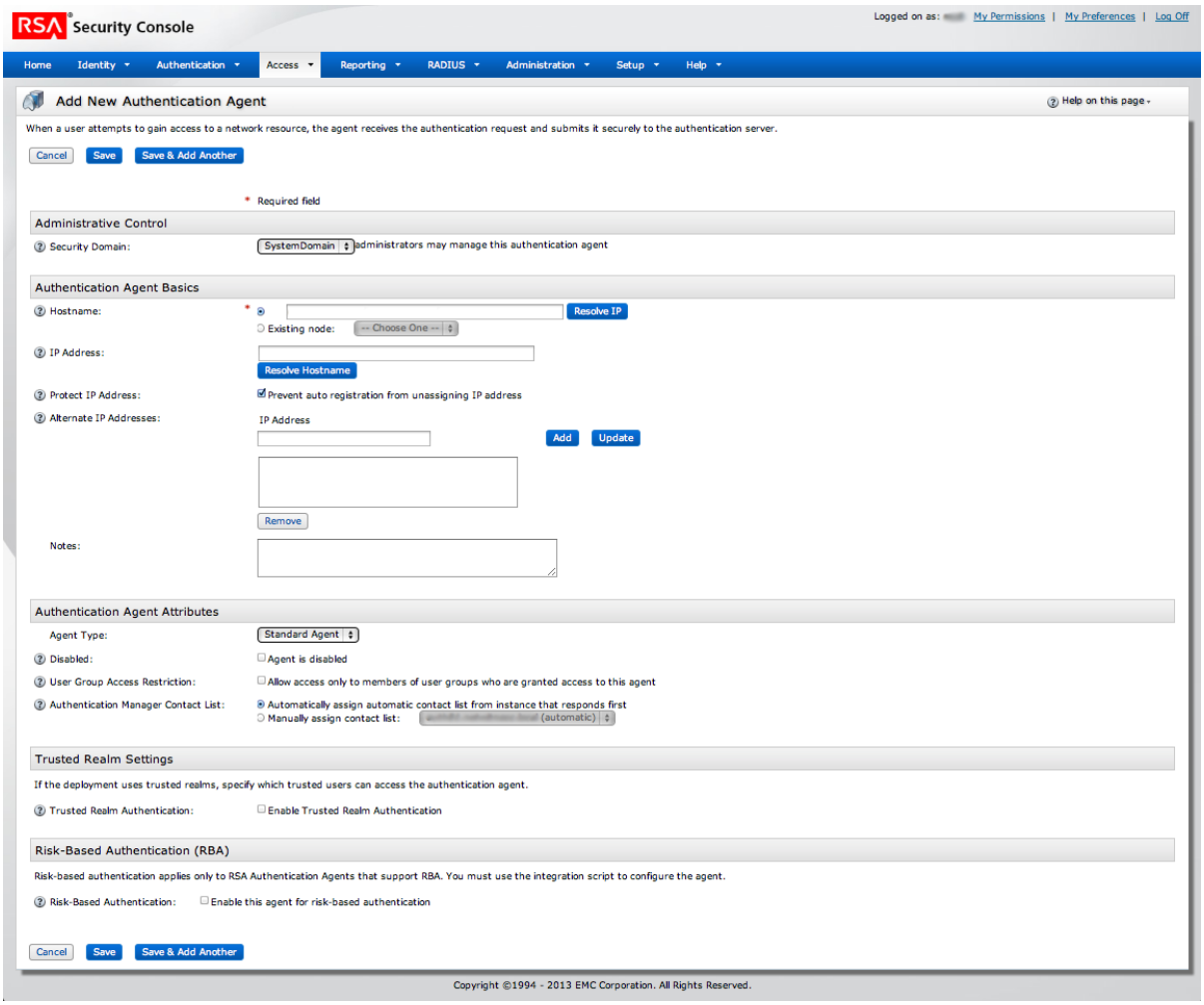
Authentication Manageを構成する方法

1. RSA Authentication Managerにログオンします。
   Security Consoleが表示されます。



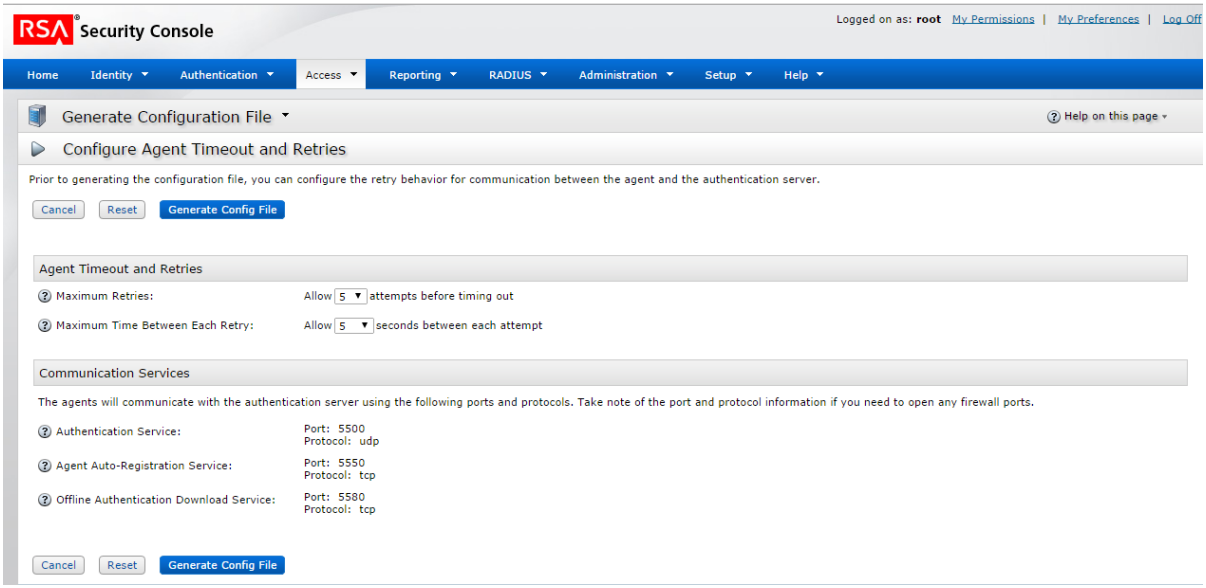
2. Security Consoleで、新しい認証エージェントを追加します。
   [アクセス]＞[認証エージェント]＞[新規追加]

をクリックします。[新しい認 証エージェントの追 加]ページが表 示されます。



3. [**ホスト名**]フィールドに、NetWitness Serverのホスト名を入 力します。
4. [**IPの解 決**]をクリックします。
   NetWitness ServerのIPアドレスが[**IPアドレス**]フィールドに自 動 的に表 示されます。
5. デフォルト設 定をそのまま維 持して、[**保 存**]をクリックします。
6. 構 成ファイルを生 成します。
   [アクセス]＞[認 証エージェント]＞[構 成ファイルの生 成]に移 動します。

[構 成ファイルの生 成]ページが表 示されます。



7. デフォルト設 定をそのまま維 持して、[**構 成ファイルの生 成**]をクリックします。
   2つのファイルを含 んだ**AM_Config.zip**が作 成されます。
8. [**Download Now(今 すぐダウンロード)**]をクリックします。

PAM SecurIDモジュールをインストールして構 成する方 法

1. NetWitness Serverで、次 のディレクトリを作 成します。
   `mkdir /var/ace`
2. NetWitness Serverで、`sdconf.rec`を.zipファイルから`/var/ace`にコピーします。
3. テキスト ファイル`sdopts.rec`を`/var/ace`ディレクトリに作 成します。
4. 次 の行を挿 入します。
   `CLIENT_IP=<IP address of NetWitness Server>`
5. 次 のyumリポジトリにあるPAM向 けSecurID認 証エージェントをインストールします。
   `yum install sid-pam-installer`
6. 次 のインストール スクリプトを実 行します。
   `/opt/rsa/pam-agent-installer/install_pam.sh`
7. プロンプトに従 ってデフォルトをそのまま使 用するか変 更します。
8. NetWitness ServerのPAM構 成ファイル`/etc/pam.d/securityanalytics`を編 集して、次 の行を追 加します。ファイルが存 在しない場 合 は、ファイルを作 成し、次 の行を追 加します。
   `auth sufficient pam_securid.so`

SecurID PAMモジュールのインストールはこれで完 了 です。次 に、接 続と認 証をテストした後 で、「NSS サービスの設 定とテスト」の手 順に従います。

注 : PAM SecurIDのセットアップが完 了していない場 合 、Jettyサーバをクラッシュさせる可 能 性 があり、NetWitness PlatformのUIは表 示されません。PAM認 証の構 成が完 了するまで待 機し、Jettyサーバを再 起 動する必 要 があります。

接続と認証をテストする方法

1. /opt/pam/bin/64bit/acetestを実行し、**ユーザ名**と**パスコード**を入力します。
2. (オプション) acetestが失敗した場合は、デバッグを有効にします。
   vi/etc/sd_pam.conf
   RSATRACELEVEL=15
3. /opt/pam/bin/64bit/acestatusを実行します。出力は以下のように表示されます。

```
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. (オプション) Authentication Managerサーバをトラブルシューティングするには、次の手順を実行します。
   [レポート] > **[リアルタイム アクティビティ モニタ]** > **[認証アクティビティ モニタ]**に移動します。
   次に、**[モニタの開始]**をクリックします。
5. 設定を変更した場合は、RSATRACELEVELを0にリセットします。
   vi/etc/sd_pam.conf
   RSATRACELEVEL=0

注意：インストールが完了したら、/etc/sd_pam.confファイルのVAR_ACEがsdconf.recファイルの正しい場所を参照していることを確認します。これは構成ファイルのパスです。これに必要なコマンドは次のとおりです：chown -R netwitness:netwitness /var/ace。

SecurID向けPAMエージェントの構成はこれで完了です。次のセクション「NSSサービスの設定とテスト」に進みます。

NSSサービスの設定とテスト

NSS UNIX

NSS UNIXモジュールを有効化するために必要な構成はありません。ホストのオペレーティング システムによってデフォルトで有効化されています。特定のグループのユーザに権限を付与するには、そのユーザをオペレーティング システムに追加し、グループに追加します。

1. 次のコマンドを使用して、外部ユーザを追加する際に使用するOSグループを作成します。
   groupadd <groupname>

2. 次のコマンドを使 用して、外 部ユーザをOSに追 加します。
   ```
   adduser -G <groupname> -M -N <externalusername>
   ```

注 : この操 作だけではまだ、NetWitness Serverコンソールへのアクセスは許 可されません。

NSS UNIXの構 成はこれで完 了です。次に、NSS機 能のテストに進みます。

NSS機 能のテスト

NSSが前 述のNSSサービスのすべてと連 携しているかどうかをテストするには、次のコマンドを使 用します。

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

出 力は次のようになります。

```
[root@~]# getent passwd myuser
 myuser:*:10000:10000::/home/myuser:/bin/sh
[root@~]# getent group mygroup
 mygroup:*:10000:myuser3
```

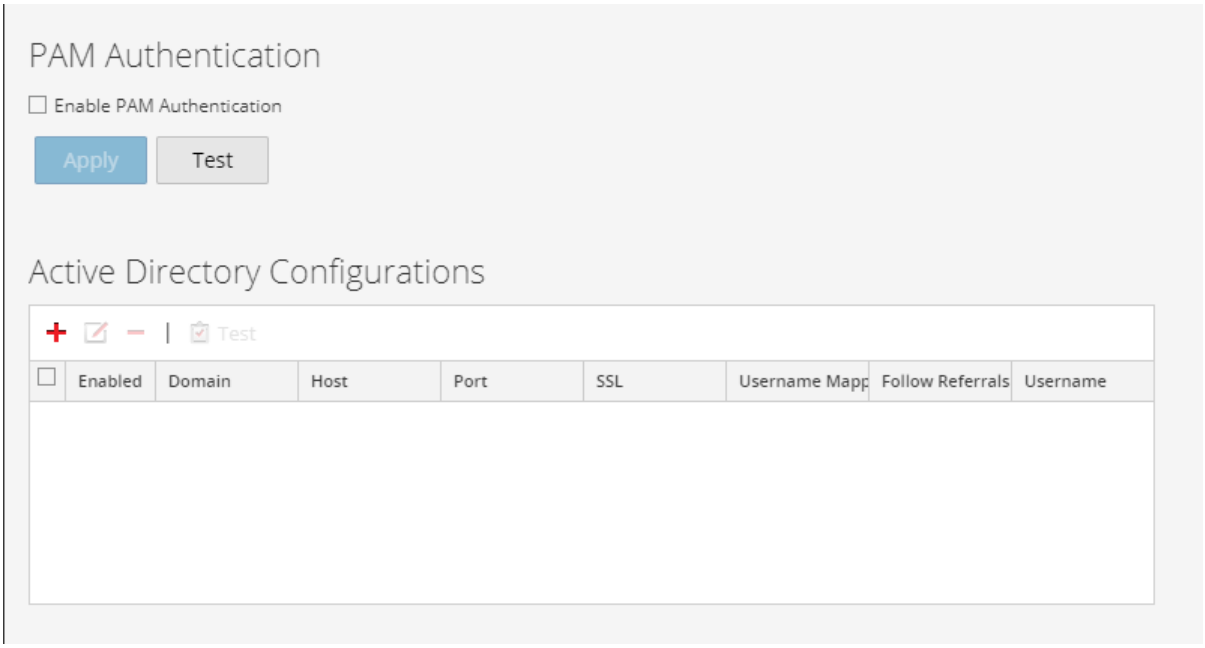
- どのコマンドも出 力を生 成しない場 合、NSSの外 部権 限認 可は正 常に機 能していません。このドキュメントに記 載されているNSSモジュールのトラブルシューティング ガイダンスを参 照してください。
- `getent`コマンドが成 功し、`/var/log/secure`で認 証の成 功が確 認できているにも関 わらず、NetWitness Platformが外 部ユーザにログインを許 可できない場 合 :
  - NW外 部グループ マッピングでNSSグループに正 しいグループ名を指 定していない可 能 性があります。後 述の「PAMの有 効 化とグループ マッピングの作 成」を参 照してください。
  - NSS構 成に加えた変 更がNetWitness Platformに反 映されていない可 能 性があります。NetWitness Platformホストを再 起 動すると、NSS構 成に加えた変 更がNetWitness Platformに反 映されます。Jettyサーバの再 起 動だけでは不 十 分です。

次のセクション「NetWitness ServerでのPAMの有 効 化」に進みます。

NetWitness ServerでのPAMの有 効 化

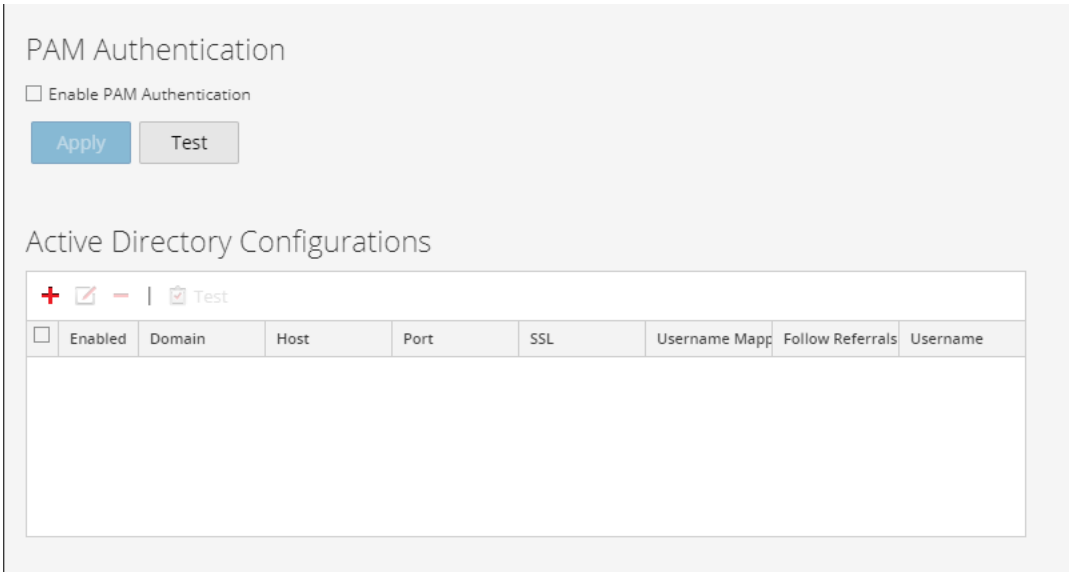
1. NetWitness Platformで、**[管 理]**>**[セキュリティ]**に移 動します。
   [管 理]>[セキュリティ]ビューが表 示され、[ユーザ]タブが開きます。
2. **[設 定]**タブをクリックします。

3. [**PAM認証**]で、[**PAM認証の有効化**]を選択し、[**適用**]をクリックします。

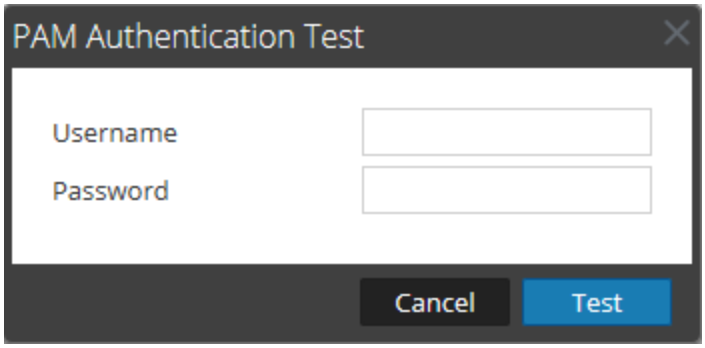


PAMの外部認証のテスト

1. [**管理**]>[**セキュリティ**]に移動します。
   [セキュリティ]ビューが表示され、[**ユーザ**]タブが開きます。
2. [**設定**]タブをクリックします。
3. [**PAM認証**]で、[**PAM認証の有効化**]を選択します。



4. [**PAM認 証**]オプションで、[**テスト**]をクリックします。
   [**PAM認 証テスト**]ダイアログが表 示されます。



5. PAM構 成を使 用して認 証をテストするユーザ名 とパスワードを入 力します。
6. [**テスト**]をクリックします。
   接 続 性を確 認 するために外 部 認 証 がテストされます。
7. テストが成 功しない場 合 は、構 成を確 認して編 集します。

PAMが有 効 化され、Active Directory構 成も有 効のままになります。セキュリティ ロールを各 グループにマッピングできるように、PAM構 成 が[外 部 グループ マッピング]タブに自 動 的に表 示されます。

NetWitness Serverでのグループ マッピングの作 成

PAMのアクセスに使 用されるセキュリティ ロールを構 成 するには、ステップ5. (オプション) 外 部 グループへのユーザ ロールの割り当 て

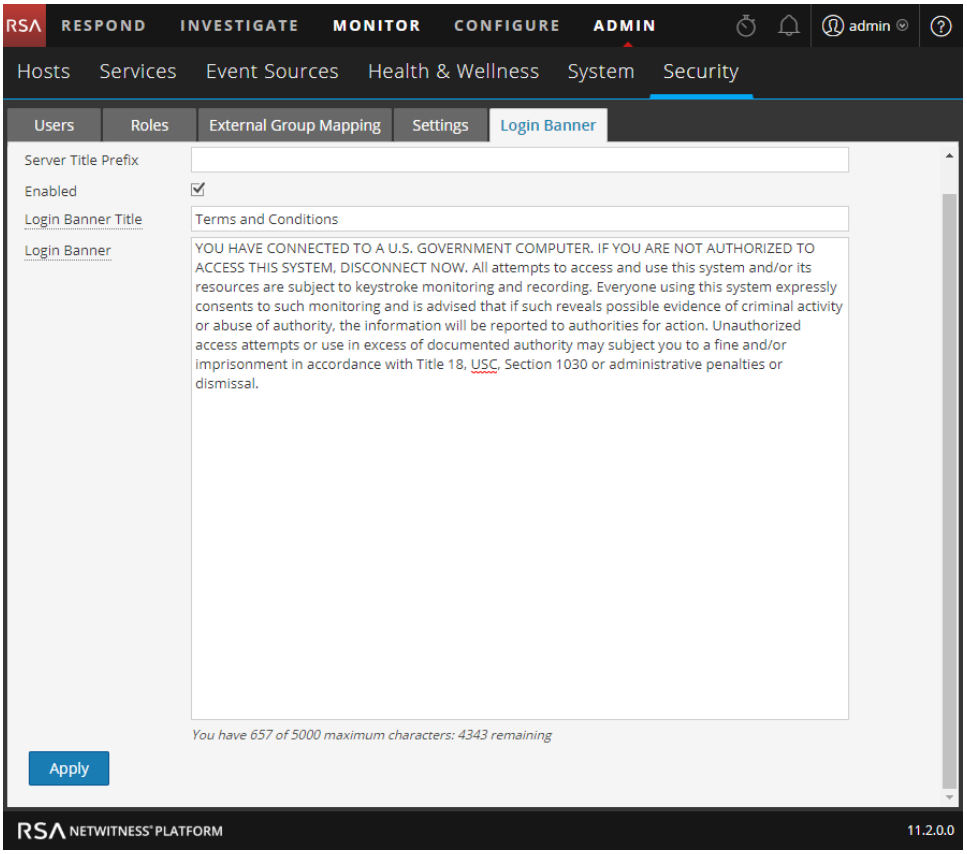
ステップ5. (オプション) カスタム ログイン バナーの作 成

このトピックでは、ユーザがNetWitness Platformにログオンする前に表 示されるログイン バナーを作 成 するための手 順について説 明します。

ユーザがログインする前に条 件に同 意 することを求 めるカスタマイズされたバナーを利 用 できます。同 意 しないユーザはログオンできません。

カスタム ログイン バナーの作 成と有 効 化

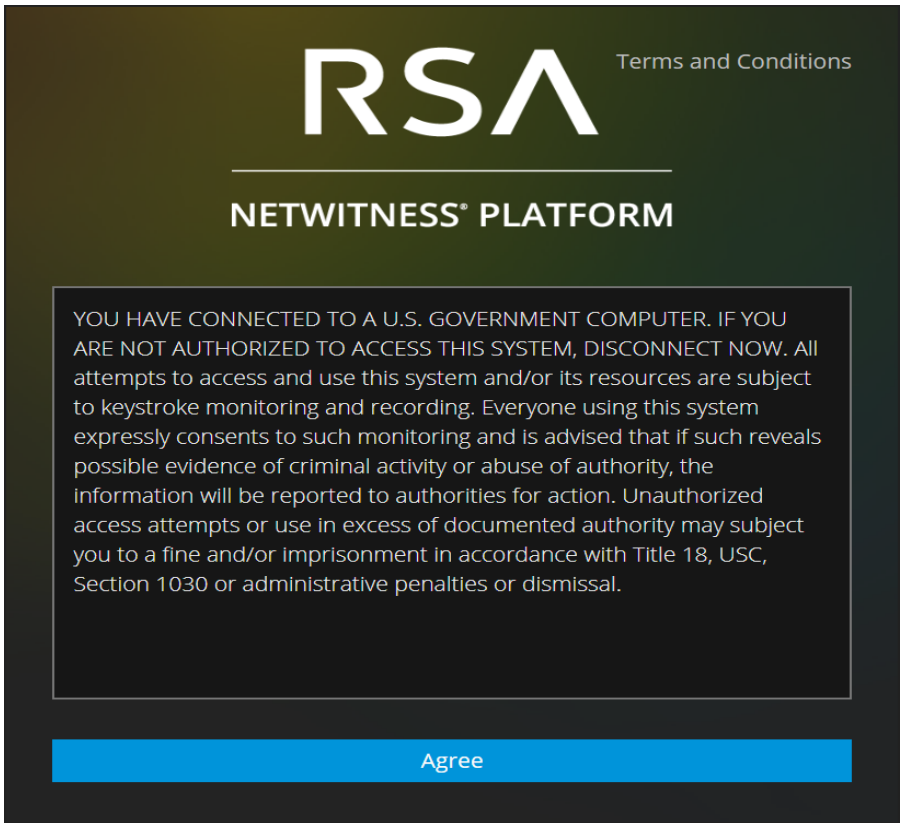
1. [**管 理**] > [**セキュリティ**]に移 動します。
   [セキュリティ]ビューが表 示され、[ユーザ]タブが開きます。
2. [**ログイン バナー**]タブをクリックして[**有 効**]チェックボックスを選 択し、バナーの有 効 化と無 効 化を切り替 えます。
   [有 効]を選 択 すると、[ログイン バナーのタイト ル]フィールドと[ログイン バナー]フィールドがアクティブになり、デフォルト のコンテンツが適 切に設 定されます。



3. デフォルト のコンテンツを使 用 するか、バナーのカスタム タイト ルおよびコンテンツを入 力し、[**適 用**]をクリックします。
   バナーが有 効 化され、即 座にアクティブになります。

注 : 平 文とHTMLタグ付きテキストの両 方が許 可されていますが、疑わしいタグは削 除されます。たとえば、すべてのリンクは「https」プロトコルを使 用する必 要 があります。

4. バナーをテストするには、ログアウトします。NetWitness Platformの認 証 情 報を入 力するためのフィールド の前 にバナーが表 示されます。



5. [**同 意**]をクリックします。
バナーが閉じ、ログオン情 報を入 力することができます。

ロール ベースのアクセス制御の仕組み

このトピックでは、NetWitness Serverとコア サービスとの間に信 頼 接 続 がある場 合 のRBAC(ロール ベースのアクセス制 御) について説 明します。

RSA NetWitness® Platformでは、ロールはユーザが実 行 可 能 な操 作を定 義します。ロールには権 限 が割り当 てられており、各 ユーザにロールを割り当 てる必 要 があります。これにより、ユーザはロールで許 可 されている操 作を実 行 できます。

事 前 構 成されたロール

ロールの作 成と権 限 の割り当 てのプロセスをシンプルにするために、NetWitness Platformには事 前 構 成されたロールがあります。組 織 でカスタムのロールを追 加 することもできます。

次 の表 は、事 前 構 成されたそれぞれのロールと割り当 てられた権 限 を示しています。Administrators ロールにはすべての権 限 が割り当 てられています。他 のそれぞれのロールには権 限 のサブセット が割り当 てられています。

ロール	権 限
Administrators	完 全 なシステム アクセス権 を持ちます。デフォルト では、System Administratorsペルソナにはすべての権 限 が付 与 されています。
Respond_ Administrator	すべての対 応 権 限 にアクセスします。Respond Administratorペルソナは、応 答 のシステム構 成 に重 点 を置 いています。
Data_Privacy_ Officers	DPO(Data Privacy Officer) ペルソナは、Administratorsと類 似 していますが、システム内 の機 密 データの難 読 化 および表 示 を管 理 する設 定 オプションに焦 点 を当 てた権 限 が追 加 されています(『*データ プライバシー管 理 ガイド*』を参 照) 。DPOロールを持 つユーザは、どのメタ キーに難 読 化 のフラグが付 いているかを確 認 でき、難 読 化 されているメタ キーおよびフラグが付 いているメタ キーの値 を確 認 することもできます。
SOC_ Managers	Analystsと同 じアクセス権 に加 えて、インシデント の処 理 に必 要 な権 限 を持ちます。SOC Managersペルソナは、対 応 に構 成 に必 要 な権 限 以 外 は、Analystsと同 一 です。
Operators	構 成 へのアクセス権 を持ちますが、メタおよびセッションのコンテンツへのアクセス権 は持ちません。System Operatorsペルソナは、システム設 定 に焦 点 を当 てていますが、Investigation、ESA、Alerting、Reporting、Respondには焦 点 を当 てていません。
Malware_ Analysts	Investigationとマルウェア イベント へのアクセス権 を持ちます。Malware Analystsペルソナには、Malware Analysisモジュールへのアクセス権 だけが付 与 されています。
Analysts	メタおよびセッションのコンテンツへのアクセス権 を持ちますが、構 成 へのアクセス権 は持ちません。SOC(セキュリティ オペレーション センター) のAnalystsペルソナは、Investigation、ESA、Alerting、Reporting、Respondに焦 点 を当 てていますが、システム設 定 には焦 点 を当 てていません。

ロール	権限
UEBA_ Analysts	[**調査**] > [**ユーザ**]ビューで、RSA NetWitness UEBAサービスにアクセスします。NetWitness UEBAは、ネットワーク環境内のすべてのエンティティにおける危険な行動を検出、調査、監視するための高度な分析ソリューションです。 **注**:このロールに特定の権限を設定する必要はありません。必要な操作はこのロールをユーザに割り当てることだけです。そのユーザはNetWitness UEBAにアクセスできるようになります。

サーバとサービスとの間の信頼接続

信頼接続では、サービスはNetWitness Serverを明示的に信頼し、ユーザの管理と認証を行います。認証されたユーザは各コア サービスでローカルに定義される必要がないため、各サービスにおける管理を軽減できます。

次の表が示すように、すべてのユーザ管理タスクはサーバで行います。

タスク	場所
ユーザの追加	サーバ
ユーザ名の管理	サーバ
パスワードの管理	サーバ
内部NetWitness Platformユーザの認証	サーバ
(オプション) 外部ユーザの認証: - Active Directory - PAM	 サーバ サーバ
PAMのインストールと構成	サーバ

信頼接続とユーザの一元管理のメリットは次のとおりです。

- すべてのユーザ管理タスクはNetWitness Serverサーバでのみ1度だけ行います。
- サービスへのアクセスを制御でき、ユーザの認証をサービスで設定する必要はありません。
- ユーザはNetWitness Platformのログインでパスワードを一度だけ入力すると、サーバによって認証されます。
- サーバで認証済みのユーザは、パスワードを入力せずに、[管理]>[サービス]にあるすべてのコアサービスにアクセスできます。

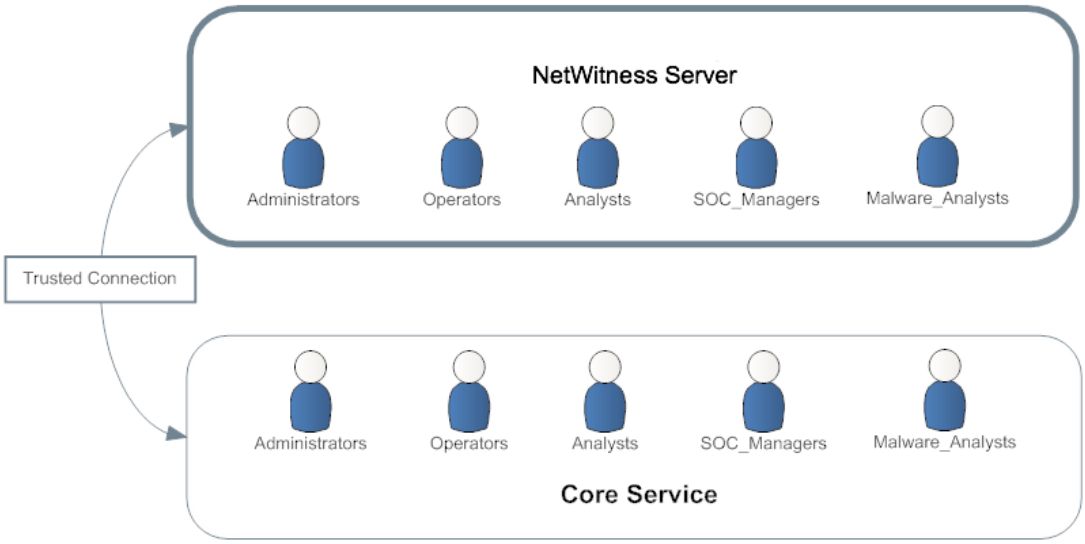
信頼接続の確立

11.xをインストールするかまたはこのバージョンにアップグレードすると、デフォルトで次の2つの設定を使用して信頼接続が確立されます。

- SSLが有効になります。
- コア サービスはSSLポートに接続し、通信が暗号化されます。

サーバおよびサービスにおける共通のロール名

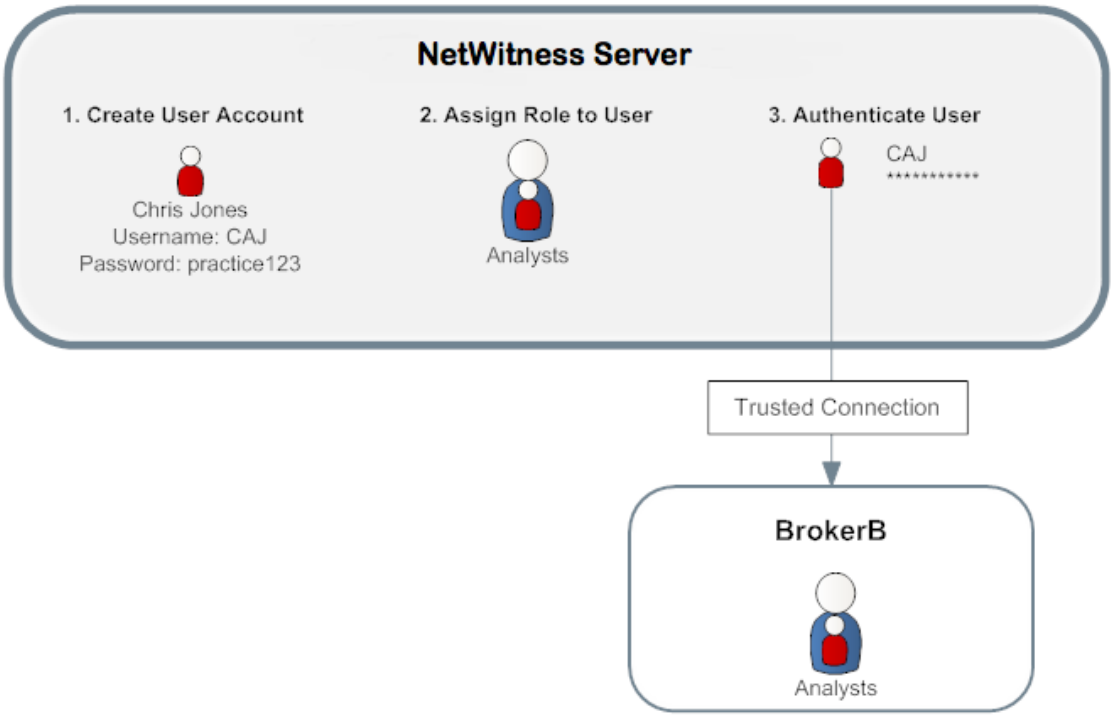
信頼接続は、サーバおよびサービスで共通のロール名に依存しています。新規インストール環境では、NetWitness Platformは5つの事前構成されたロールがサーバと各コア サービスにインストールされます。



JuniorAnalystsなどのカスタム ロールを追加している場合は、ArchiverAやBrokerBなどの各サービスにそのロールを追加する必要があります。ロール名では、大文字と小文字が区別され、空白文字を含むことはできず、厳密に同一である必要があります。たとえば、JuniorAnalyst(単数)とJuniorAnalysts(複数)は共通のロール名の要件を満たしていません。

ユーザの構 成 とサービス アクセスのエンド ツー エンド のワークフロー

このワークフローでは、NetWitness ServerとサービスBrokerBとの間に信 頼 接 続 がある場 合 のロール ベースのアクセス制 御 の仕 組 みを示しています。



1. NetWitness Serverで、新しいユーザのアカウントを作 成します。
   名 前 : Chris Jones
   ユーザ名 : CAJ
   パスワード : practice123
2. Chris Jonesに割り当 てるのは事 前 構 成されたロールかカスタム ロールかを決 めます。
   - **事 前 構 成されたロール**
     a. **Analystsのロール**に割り当 てられたデフォルト の権 限 を維 持 または変 更します。これには、Alerting、Investigation、Malwareモジュールへのアクセスなどの権 限 が含 まれます。
     b. Chris JonesにAnalystsのロールを割り当 てます。
   - **カスタム ロール**
     a. JuniorAnalystsなど、カスタムロールを作 成します。
     b. **JuniorAnalystsのロール**に権 限 を割り当 てます。
     c. Chris JonesにJuniorAnalystsのロールを割り当 てます。
     d. JuniorAnalystsのロールをBrokerBなどのサービスに追 加します。

3. ユーザChris JonesはNetWitness Serverにログオンします。
   ユーザ名 : CAJ
   パスワード : practice123
4. サーバはChrisを認 証します。
5. 信 頼 接 続により、認 証 ユーザであるChrisは、別 のパスワードを入 力 せずに、BrokerBにアクセスできます。

詳 細な説 明 や手 順については、「ロールと権 限 によるユーザの管 理 」を参 照してください。

関 連トピック

- ロールの権 限

ロールの権 限

このトピックでは、NetWitness Platformに事 前 定 義されたシステム ロールを割り当 てられたユーザが、デフォルト でアクセス可 能なユーザ インタフェースについて説 明します。

NetWitness Platformでは、各 モジュール、ダッシュレット 、ビューへのユーザ アクセスは、このトピックで説明されている権 限に基 づいて制 御されます。これらのロールの権 限 は、[管 理] > [セキュリティ] > [ロール] タブからアクセスできる[ロールの追 加] または[ロールの編 集] ダイアログにあります。

[ロールの追 加] または[ロールの編 集] ダイアログで、[権 限] セクションのタブはNetWitness Platformのさまざまな領 域を表し、それらの領 域 で使 用できる権 限を示します。たとえば、[管 理] タブには、[管 理] ビューで使 用 可 能な権 限を示します。

注 : [ロールの追 加]/[ロールの編 集] ダイアログには、[構 成] ビューに対 応 する[構 成] タブはありません。[構 成] ビューの権 限を割り当 てるには、[構 成] ビューに含 まれる各 ビューの権 限を割り当 てます。このようなビューは、[Liveコンテンツ] (Live) 、[インシデント ルール] (インシデント) 、[対 応 の通 知] (インシデント 、Respond Server、Integration Server) 、[ESAルール] (アラート) 、[サブスクリプション] (Live) 、[カスタムFeed] (Live) です。

注 : [Admin-server] タブの左 側 には、アスタリスク(*) のタブがあります。このタブは、バックエンド サービスのみの管 理 へのアクセスを示します。

次 の表 に、各 NetWitness Platformユーザ ロールに割り当 てられるデフォルト 権 限を示します。

- Administrators
- Respond Administrators
- Data Privacy Officers
- SOC Managers
- Operators
- Malware Analysts
- Analysts

Administratorsロールはデフォルト ですべての権 限を持っているため、この表 には含 まれていません。

新しいサービスのサービス権 限 の形 式

一 部 の新しいNetWitness Platformサービスのサービス権 限 は、次 の3つの要 素 で構 成されています。

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

たとえば、**investigate-server.metrics.read**権 限 の場 合 は次 のような意 味 になります。

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

この権 限を割り当 てられたユーザは、investigate-serverサービスが公 開するすべてのメトリックを表 示することができます。

管理

次の表に、各ロールに割り当てられる[管理]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorsロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
管理モジュールへのアクセス	可	可	可	可	可
ヘルスモニタへのアクセス	可	可	可	可	可
システム更新の適用	可				
Liveインテリジェンス共有にオプトイン可能	可				
詳細設定の管理	可				
ATD設定の管理	可				
監査の管理	可				可
Eメールの管理	可				
グローバル監査の管理	可				可
ヘルスモニタ ポリシーの管理	可				
LLSの管理	可				
ログの管理	可				可
通知の管理	可				
プラグインの管理	可				
クエリ条件の管理	可				
再構築の管理	可				
セキュリティの管理	可				可
サービスの管理	可				可
システム設定の管理	可				
ESA設定の変更	可				
イベント ソースの変更	可				
ホストの変更	可				
サービスの変更	可				可

権 限	Operators	Analysts	SOC Managers	MA	DPO
イベント ソースの表 示	可		可		
ヘルスモニタ ポリシーの表 示	可	可	可		
ヘルスモニタ統 計 ブラウザの表 示	可	可	可		可
ホスト の表 示	可				可
サービスの表 示	可				可

Admin-server

次 の表 に、[Admin-server] タブの権 限 を示 します。Administratorsロールはすべての権 限 を持 ち、デフォルト で権 限 が付 与 される唯 一 のロールです。

権 限	説 明
admin-server.configuration.manage	すべてのサービス構 成 パラメータを変 更 する権 限
admin-server.health.read	サービスが公 開 するすべての稼 働 状 態 通 知 を表 示 する権 限
admin-server.logs.manage	ログ関 連 の構 成 を変 更 する権 限
admin-server.metrics.read	サービスが公 開 するすべてのメトリックを表 示 する権 限
admin-server.process.manage	サービスを開 始 および停 止 する権 限
admin-server.security.manage	セキュリティ関 連 のリソース(パスワード 、キーなど) を編 集 する権 限
admin-server.security.read	セキュリティ関 連 のリソースを表 示 する権 限

アラート

次 の表 に、各 ロールに割 り当 てられる[アラート] タブの権 限 を示 します。空 白 のフィールド は、ロールに権 限 がないことを示 します。Administratorsロールはデフォルト ですべての権 限 を持 っているため、この表 には含 まれていません。

権 限	Operators	Analysts	SOC Managers	MA	DPO
アラート モジュールへのアクセス	可	可	可		可
ルールの管 理			可		可
アラート の表 示	可	可	可		可
ルールの表 示			可		可

Cloud-gateway-server

次の表に、[Cloud Gateway-Server]タブの権限を示します。Administratorsロールはすべての権限を持ち、デフォルトで権限が付与される唯一のロールです。

権限	説明
cloud-gateway-server.configuration.manage	Cloud Gatewayサービスのすべてのパラメータを変更する権限
cloud-gateway-server.health.read	サービスが公開するすべての稼働状態通知を表示する権限
cloud-gateway-server.logs.manage	ログ関連の構成を変更する権限
cloud-gateway-server.metrics.read	サービスが公開するすべてのメトリックを表示する権限
cloud-gateway-server.process.manage	サービスを開始および停止する権限
cloud-gateway-server.security.manage	セキュリティ関連のリソース(パスワード、キーなど) を編集する権限
cloud-gateway-server.security.read	セキュリティ関連のリソースを表示する権限
cloud-gateway-server.uploadstream.manage	uploadstreamの構成を編集する権限
cloud-gateway-server.uploadstream.read	uploadstreamの構成を表示する権限

Config-server

次の表に、[Config-server]タブの権限を示します。Administratorsロールはすべての権限を持ち、デフォルトで権限が付与される唯一のロールです。

権限	説明
config-server.*	すべての権限(以下のすべて)
config-server.configuration.manage	すべてのサービス構成パラメータを変更する権限
config-server.health.read	サービスが公開するすべての稼働状態通知を表示する権限
config-server.logs.manage	ログ関連の構成を変更する権限
config-server.metrics.read	サービスが公開するすべてのメトリックを表示する権限
config-server.process.manage	サービスを開始および停止する権限
config-server.security.manage	セキュリティ関連のリソース(パスワード、キーなど) を編集する権限
config-server.security.read	セキュリティ関連のリソースを表示する権限

Content-server

次 の表 に、[Content-server]タブの権 限を示します。

権 限	説 明
content-server*	すべての権 限(以 下 のすべて)
content-server.logparser.manage	ログParser構 成を管 理する権 限
content-server.logparser.read	ログParser構 成を表 示する権 限

次 の表 に、各 ロールに割り当 てられている[Content-server]タブの権 限を示します。空 白 のフィールドは、ロールに権 限 がないことを示します。Administratorロールはデフォルト ですべての権 限を持っているため、この表 には含 まれていません。

権 限	Operators	Analysts	SOC Managers	MA	DPO
content-server.*	可				可
content-server.logparser.manage	可				可
ontent-server.logparser.read	可	可	可		可

Contexthub-server

次 の表 に、[Contexthub-server]タブの権 限を示します。

権 限	説 明
contexthub-server.*	すべての権 限(以 下 のすべて)
contexthub-server.configuration.manage	すべてのサービス構 成 パラメータを変 更する権 限
contexthub-server.connection.manage	すべての接 続 設 定を変 更する権 限
contexthub-server.connection.read	すべての接 続 設 定を表 示する権 限
contexthub-server.connectiontypes.read	構 成されているすべての接 続 タイプを表 示する権 限
contexthub-server.datasource.manage	データ ソース設 定を変 更する権 限
contexthub-server.datasource.read	データ ソース設 定を表 示する権 限
contexthub-server.health.read	サービスが公 開するすべての稼 働 状 態 通 知を表 示する権 限
contexthub-server.listentries.manage	リスト エントリーを変 更する権 限
contexthub-server.logs.manage	ログ関 連 の構 成を変 更する権 限

権限	説明
contexthub-server.metrics.read	サービスが公開するすべてのメトリックを表示する権限
contexthub-server.process.manage	サービスを開始および停止する権限
contexthub-server.query.read	クエリを表示する権限
contexthub-server.security.manage	セキュリティ関連のリソース(パスワード、キーなど) を編集する権限
contexthub-server.security.read	セキュリティ関連のリソースを表示する権限
contexthub-server.stix.read	STIX設定を表示する権限
contexthub-server.taxiidatasource.manage	TAXIIデータ ソース設定を変更する権限
contexthub-server.taxiidatasource.read	TAXIIデータ ソース設定を表示する権限

次の表に、各ロールに割り当てられている[Contexthub-server]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
contexthub-server.*					可
contexthub-server.configuration.manage					
contexthub-server.connection.manage					
contexthub-server.connection.read		可	可	可	
contexthub-server.connectiontypes.read			可		
contexthub-server.datasource.manage		可	可	可	
contexthub-server.datasource.read		可	可	可	
contexthub-server.health.read					
contexthub-server.listentries.manage		可	可	可	
contexthub-server.logs.manage					
contexthub-server.metrics.read					
contexthub-server.process.manage					
contexthub-server.query.read		可	可	可	
contexthub-server.security.manage					

権限	Operators	Analysts	SOC Managers	MA	DPO
contexthub-server.security.read					
contexthub-server.stix.read		可	可	可	
contexthub-server.taxiidatasource.manage		可	可	可	
contexthub-server.taxiidatasource.read		可	可	可	

ダッシュボード

次の表に、各ロールに割り当てられる[ダッシュボード]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorsロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
Dashlet Access - Admin Device List Dashlet	可	可	可		可
Dashlet Access - Admin Device Monitor Dashlet					可
Dashlet Access - Admin News Dashlet	可	可	可		可
Dashlet Access - Alert Variance Dashlet		可	可		可
Dashlet Access - Alerting Recent Alerts Dashlet		可	可		可
Dashlet Access - Investigation Jobs Dashlet		可	可		可
Dashlet Access - Investigation Top Values Dashlet		可	可		可
Dashlet Access - Live Featured Resources Dashlet	可	可	可		可
Dashlet Access - Live New Resources Dashlet	可	可	可		可
Dashlet Access - Live Subscriptions Dashlet	可	可	可		可
Dashlet Access - Live Updated Resources Dashlet	可	可	可		可
Dashlet Access - Malware Jobs Dashlet		可	可		可

権限	Operators	Analysts	SOC Managers	MA	DPO
Dashlet Access - Reporting Recent Report Dashlet		可	可		可
Dashlet Access - Reporting Charts Dashlet		可	可		可
Dashlet Access - Top Alerts Dashlet		可	可		可
Dashlet Access - Unified RSA First Watch Dashlet	可	可	可		可
Dashlet Access - Unified Shortcuts Dashlet	可	可	可		可

Endpoint-server

次の表に、[Endpoint-server]タブの権限を示します。Administratorsロールはデフォルトですべての権限を持っています。

権限	説明
endpoint-server*	すべての権限(以下のすべて)
endpoint-server.agent.manage	エージェント パッケージ構成をダウンロードおよび管理する権限
endpoint-server.agent.read	エージェント パッケージ構成を表示する権限
endpoint-server.ca.manage	エージェント パッケージを生成してダウンロードする権限
endpoint-server.ca.read	エージェント パッケージを生成してダウンロードする権限
endpoint-server.configuration.manage	すべてのエンドポイント構成パラメータを変更する権限
endpoint-server.dataretention.manage	データ保存ポリシーを構成する権限
endpoint-server.dataretention.read	データ保存ポリシーを表示する権限
endpoint-server.filter.manage	フィルタを削除する権限
endpoint-server.filter.read	フィルタを表示する権限
endpoint-server.health.read	サービスが公開するすべての稼働状態通知を表示する権限
endpoint-server.logs.manage	ログ関連の構成を変更する権限
endpoint-server.machine.manage	ホストを削除する権限
endpoint-server.machine.read	ホストを表示する権限

権限	説明
endpoint-server.metrics.read	サービスが公 開するすべてのメトリックを表 示する権限
endpoint-server.policy.manage	スキャン スケジュール構 成を更 新および保 存する権限
endpoint-server.policy.read	既 存のスキャン スケジュール構 成を表 示する権限
endpoint-server.process.manage	サービスを開 始および停 止する権限
endpoint-server.scan.manage	エンドポイント スキャンを実 行する権限
endpoint-server.scan.read	エンドポイント スキャン データを表 示する権限
endpoint-server.security.manage	セキュリティ関 連のリソース(パスワード 、キーなど) を編 集する権限
endpoint-server.security.read	セキュリティ関 連のリソースを表 示する権限

次 の表 に、各 ロールに割り当 てられている[Endpoint-server]タブの権 限を示します。空 白 のフィールドは、ロールに権 限 がないことを示します。Administratorロールはデフォルト ですべての権 限を持っているため、この表 には含 まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
endpoint-server*	可				
endpoint-server.agent.manage					
endpoint-server.agent.read					
endpoint-server.ca.manage					
endpoint-server.ca.read					
endpoint-server.configuration.manage					
endpoint-server.dataretention.manage					
endpoint-server.dataretention.read					
endpoint-server.filter.manage		可			
endpoint-server.filter.read		可			
endpoint-server.health.read					
endpoint-server.logs.manage					
endpoint-server.machine.manage		可			
endpoint-server.machine.read		可			
endpoint-server.metrics.read					
endpoint-server.policy.manage	可				

権限	Operators	Analysts	SOC Managers	MA	DPO
endpoint-server.policy.read	可				
endpoint-server.process.manage					
endpoint-server.scan.manage		可			
endpoint-server.scan.read		可			
endpoint-server.security.manage					
endpoint-server.security.read					

Esa-analytics-server

次の表に、[Esa-Analytics-server]タブの権限を示します。AdministratorsロールおよびOperatorsロールはすべての権限を持ち、これらのロールのみがデフォルトで権限を付与されています。

権限	説明
esa-analytics-server.*	すべての権限(以下のすべて)
esa-analytics-server.analytics.manage	ESA Analyticsを変更する権限
esa-analytics-server.analytics.read	ESA Analyticsを表示する権限
esa-analytics-server.configuration.manage	すべてのサービス構成パラメータを変更する権限
esa-analytics-server.health.read	サービスが公開するすべての稼働状態通知を表示する権限
esa-analytics-server.logs.manage	ログ関連の構成を変更する権限
esa-analytics-server.metrics.read	サービスが公開するすべてのメトリックを表示する権限
esa-analytics-server.model.manage	ESAモデルを変更する権限
esa-analytics-server.model.read	ESAモデルを表示する権限
esa-analytics-server.process.manage	サービスを開始および停止する権限
esa-analytics-server.security.manage	セキュリティ関連のリソースを変更する権限
esa-analytics-server.security.read	セキュリティ関連のリソースを表示する権限

インシデント

次の表に、各ロールに割り当てられる[インシデント]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorsロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
インシデント モジュールへのアクセス		可	可	可	可
インシデント管理統合の構成			可		可
アラートとインシデントの削除					可
アラート処理ルールの管理			可		可
インシデントの表示および管理		可	可	可	可

Integration-server

(Integration-serverの権限は、NetWitness Platformバージョン11.1以降で使用できます。)

次の表に、[Integration-server]タブの権限を示します。

権限	説明
integration-server.*	すべての権限(以下のすべて)
integration-server.api.access	サード パーティ アプリケーションからの外部リクエストを承認する権限
integration-server.configuration.manage	すべてのサービス統合構成パラメータを表示および変更する権限
integration-server.health.read	サービスが公開するすべての稼働状態通知を表示する権限
integration-server.logs.manage	ログ関連の統合構成を変更する権限
integration-server.metrics.read	サービスが公開するすべてのメトリックを表示する権限
integration-server.notification.manage	グローバル通知構成(SMTPサーバなど) を変更する権限
integration-server.notification.read	グローバル通知構成(SMTPサーバなど) を表示する権限
integration-server.notification.send	通知(Eメールなど) を送信する権限
integration-server.process.manage	サービスを開始および停止する権限
integration-server.security.manage	セキュリティ関連のリソース(パスワード、キーなど) を編集する権限
integration-server.security.read	セキュリティ関連のリソースを表示する権限
integration-server.template.manage	通知テンプレートを変更する権限
integration-server.template.read	通知テンプレートを表示する権限

次の表に、各ロールに割り当てられている[Integration-server]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
integration-server.*					可
integration-server.api.access					
integration-server.configuration.manage					
integration-server.health.read					
integration-server.logs.manage					
integration-server.metrics.read					
integration-server.notification.manage	可		可		
integration-server.notification.read	可		可		
integration-server.notification.send	可		可		
integration-server.process.manage					
integration-server.security.manage					
integration-server.security.read					
integration-server.template.manage	可		可		
integration-server.template.read	可		可		

調査

次の表に、各ロールに割り当てられる[調査]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorsロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
調査モジュールへのアクセス		可	可	可	可
コンテキスト ルックアップ		可	可	可	
調査からのインシデントの作成		可	可	可	
調査からのリストの管理		可	可	可	
イベントのナビゲート		可	可	可	可
値のナビゲート		可	可	可	可

Investigate-server

次 の表 に、[Investigate-server]タブの権 限を示 します。Administrators、Analysts、SOC Managers、Malware Analysts、Data Privacy Officersのロールはすべての権 限を持 ち、これらのロールのみがデフォルト で権 限を付 与 されています。

権 限	説 明
investigate-server.*	[イベント分 析]ビューのすべての権 限(以 下 すべて)
investigate-server.configuration.manage	サービスの構 成プロパティを変 更 する権 限
investigate-server.content.export	サービスからコンテンツをエクスポート する権 限
investigate-server.content.reconstruct	サマリー ビュー、パケット 、パケット マップ、テキスト 、ログ、ファイルの再 構 築 、パケット 数 を表 示 する権 限
investigate-server.event.read	サービスが公 開 するイベント を表 示 する権 限
investigate-server.health.read	サービスが公 開 するすべての稼 働 状 態 通 知 を表 示 する権 限
investigate-server.logs.manage	ログ関 連 の構 成を変 更 する権 限
investigate-server.metagroup.manage	メタ グループを管 理 する権 限
investigate-server.metagroup.read	メタ グループを表 示 および使 用 する権 限
investigate-server.metrics.read	サービスが公 開 するすべてのメトリックを表 示 する権 限
investigate-server.process.manage	サービスを開 始 および停 止 する権 限
investigate-server.security.manage	セキュリティ関 連 のリソース(パスワード 、キーなど) を編 集 する権 限
investigate-server.security.read	セキュリティ関 連 のリソースを表 示 する権 限

Live

次 の表 に、各 ロールに割 り当 てられる[Live]タブの権 限を示 します。空 白 のフィールド は、ロールに権 限 がないことを示 します。Administratorsロールはデフォルト ですべての権 限を持 っているため、この表 には含 まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
Live					
Liveモジュールへのアクセス	可	可	可		可
Liveシステム設定の管理	可				
リソース					
Liveリソースの導入	可				可
Live Feedの管理	可				可
Liveリソースの管理	可				可
Liveリソースの検索	可	可	可		可
Liveリソースの詳細の表示	可	可	可		可

マルウェア

次の表に、各ロールに割り当てられる[マルウェア]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorsロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
マルウェア ファイルのダウンロード		可	可	可	可
Malware Analysisスキャンの開始		可	可	可	可
Malware Analysisイベントの表示		可	可	可	可

Orchestration-server

次の表に、[Orchestration-server]タブの権限を示します。Administrators、Operators、およびData Privacy Officersのロールはすべての権限を持ち、これらのロールのみがデフォルトで権限を付与されています。

権限	説明
orchestration-server.*	すべての権限(以下のすべて)
orchestration-server.configuration.manage	すべてのサービス構成パラメータを変更する権限
orchestration-server.file.read	ファイルを表示する権限
orchestration-server.health.read	サービスが公開するすべての稼働状態通知を表示する権限
orchestration-server.logs.manage	ログ関連の構成を変更する権限

権限	説明
orchestration-server.metrics.read	サービスが公 開するすべてのメトリックを表 示する権 限
orchestration-server.process.manage	サービスを開 始 および停 止する権 限
orchestration-server.security.manage	セキュリティ関 連 のリソース(パスワード 、キーなど) を編 集する権 限
orchestration-server.security.read	セキュリティ関 連 のリソースを表 示する権 限

レポート

次 の表 に、各 ロールに割 り当 てられる[レポート]タブの権 限 を示します。空 白 のフィールド は、ロールに権 限 がないことを示します。Administratorsロールはデフォルト ですべての権 限 を持っているため、この表 には含 まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
アラート					
REアラート の定 義		可	可		可
REアラート 定 義 のエクスポート		可	可		可
REアラート の管 理		可	可		可
REアラート の表 示		可	可		可
スケジュール設 定 されたREアラート の表 示		可	可		可
チャート					
チャート の定 義		可	可		可
チャート の削 除		可	可		可
チャート 定 義 のエクスポート		可	可		可
チャート の管 理		可	可		可
チャート の表 示		可	可		可
リスト					
リスト の定 義		可	可		可
リスト の削 除		可	可		可
リスト のエクスポート		可	可		可
リスト の管 理		可	可		可
レポート					

権限	Operators	Analysts	SOC Managers	MA	DPO
レポートの定義		可	可		可
レポートの削除		可	可		可
レポートのエクスポート		可	可		可
レポートの管理		可	可		可
レポートの表示		可	可		可
レポート					
構成へのアクセス		可	可		可
レポート モジュールへのアクセス		可	可		可
レポート検索へのアクセス		可	可		可
ビューへのアクセス		可	可		可
ルール					
ルールからのREアラート定義の追加		可	可		可
ルールの定義		可	可		可
ルールの削除		可	可		可
ルールのエクスポート		可	可		可
ルールの管理		可	可		可
ルールの用途の表示		可	可		可
スケジュール					
スケジュールの定義		可	可		可
スケジュールの削除		可	可		可
スケジュールの表示		可	可		可
Warehouse Analytics					
ジョブの定義		可	可		可
ジョブの削除		可	可		可
ジョブの管理		可	可		可
ジョブの表示		可	可		可

Respond-server

次の表に、[Respond-server]タブ権限を示します。

権限	説明
respond-server.*	すべての権限(以下のすべて)
respond-server.alert.delete	アラートを削除する権限
respond-server.alert.manage	アラートを作成、更新、または削除する権限
respond-server.alert.read	アラートを表示する権限
respond-server.alertrule.manage	アラート統合ルールを作成、更新、または削除する権限
respond-server.alertrule.read	アラート統合ルールを表示する権限
respond-server.configuration.manage	サービスの構成プロパティを変更する権限
respond-server.health.read	サービスが公開するすべての稼働通知を表示する権限
respond-server.incident.delete	インシデントを削除する権限
respond-server.incident.manage	インシデントを作成、更新、または削除する権限
respond-server.incident.read	インシデントを表示する権限
respond-server.journal.manage	インシデントのジャーナル エントリーを作成、更新、または削除する権限
respond-server.journal.read	インシデントのジャーナル エントリーを表示する権限
respond-server.logs.manage	ログ関連の構成を変更する権限
respond-server.metrics.read	サービスが公開するすべてのメトリックを表示する権限
respond-server.notification.manage	(この権限は、NetWitness Platformバージョン11.1以降で使用できます)。 メール サーバ、SOCマネージャ、通知の送信先(割り当て先とSOCマネージャ)などを選択し、対応の通知を構成する権限。
respond-server.notification.read	(この権限はNetWitness Platformバージョン11.1以降で使用できます)。 対応の通知設定を表示する権限。
respond-server.process.manage	サービスを開始および停止する権限
respond-server.remediation.manage	改善タスクを作成、更新、または削除する権限
respond-server.remediation.read	改善タスクを表示する権限

権限	説明
respond-server.security.manage	セキュリティ関連のリソース(パスワード 、キーなど) を編集する権限
respond-server.security.read	セキュリティ関連のリソースを表示する権限

次の表に、各ロールに割り当てられる[Respond-server]タブの権限を示します。空白のフィールドは、ロールに権限がないことを示します。Administratorsロールおよび Respond Administratorロールはデフォルトですべての権限を持っているため、この表には含まれていません。

権限	Operators	Analysts	SOC Managers	MA	DPO
respond-server.*					可
respond-server.alert.delete					
respond-server.alert.manage		可	可	可	
respond-server.alert.read		可	可	可	
respond-server.alertrule.manage			可		
respond-server.alertrule.read			可		
respond-server.configuration.manage					
respond-server.health.read					
respond-server.incident.delete					
respond-server.incident.manage		可	可	可	
respond-server.incident.read		可	可	可	
respond-server.journal.manage		可	可	可	
respond-server.journal.read		可	可	可	
respond-server.logs.manage					
respond-server.metrics.read					
respond-server.notification.manage			可		
respond-server.notification.read			可		
respond-server.process.manage					
respond-server.remediation.manage		可	可	可	
respond-server.remediation.read		可	可	可	
respond-server.security.manage					

権限	Operators	Analysts	SOC Managers	MA	DPO
respond-server.security.read					

対応の通知の設定の権限

注 : (対応の通知の設定の権限は、NetWitness Platformバージョン11.1以降で使用できます) 。NetWitness Platformバージョン11.0から11.1以降に更新する場合は、既存の標準提供のNetWitness Platformユーザ ロールに権限を追加する必要があります。11.1以降へのすべてのアップグレードでは、カスタム ロールに権限を追加する必要があります。

Respond Administrators、Data Privacy Officers、SOC Managersには、対応の通知の設定([構成] > [対応の通知]) にアクセスするため、次の権限を追加する必要があります。

[インシデント]タブ:

- インシデント管理統合の構成

[Respond-server]タブ:

- respond-server.notification.manage
- respond-server.notification.read

[Integration-server]タブ:

- integration-server.notification.read
- integration-server.notification.manage

対応のイベント分析権限

注 : [対応]ビューの[イベント分析]パネルは、NetWitness Platformバージョン11.2以降で使用できます。

[対応」ビューの[イベント分析]パネルには、特定のインジケータのイベントについて[調査]の[イベント分析]ビューが表示されます。[対応]ビューにイベント分析を表示するには、Investigate Serverの次の権限が必要です。

[Investigate-server]タブ:

- investigate-server.event.read
- investigate-server.content.reconstruct
- investigate-server.content.export

Security-server

次の表に、[Security-server]タブの権限を示します。Administrators、Operators、およびData Privacy Officersのロールはすべての権限を持ち、これらのロールのみがデフォルトで権限を付与されています。

権限	説明
security-server.*	すべての権限(以下のすべて)

権限	説明
security-server.account.manage	NetWitness Platformローカル アカウントを表示、作成、変更または削除する権限
security-server.account.read	NetWitness Platformローカル アカウントを表示する権限
security-server.ca.manage	NetWitness Platform導入環境のPKIパラメータ(証明書への署名など)を管理する権限
security-server.ca.read	NetWitness Platform導入環境のPKIパラメータを表示する権限
security-server.configuration.manage	すべてのサービス構成パラメータを変更する権限
security-server.health.read	サービスが公開するすべての稼働状態通知を表示する権限
security-server.logs.manage	ログ関連の構成を変更する権限
security-server.metrics.read	サービスが公開するすべてのメトリックを表示する権限
security-server.permission.manage	NetWitness Platformの権限を作成または削除する権限
security-server.process.manage	サービスを開始および停止する権限
security-server.role.manage	NetWitness Platformのロールを作成、変更または削除する権限(ロール権限の追加など)
security-server.role.read	NetWitness Platformのロールの定義を表示する権限
security-server.security.manage	セキュリティ関連のリソース(パスワード、キーなど)を編集する権限
security-server.security.read	セキュリティ関連のリソースを表示する権限
security-server.user.manage	NetWitness Platformユーザ プロファイルを表示、作成、変更または削除する権限
security-server.user.read	NetWitness Platformユーザ プロファイルの詳細(ロール、ログイン時間など)を表示する権限

Source-server(将来の使用)

次の表に、[Source-server]タブの権限を示します。

権限	説明
source-server*	すべての権限(以下のすべて)
source-server.group.manage	USMグループを作成および管理する権限
source-server.group.read	USMグループを表示する権限

権 限	説 明
source-server.policy.manage	USMポリシーを作 成 および管 理 する権 限
source-server.policy.read	USMポリシーを表 示 する権 限
source-server.grouppolicy.read	基 準 のグループとポリシーを表 示 する権 限

ロールと権 限によるユーザの管 理

このトピックでは、NetWitness Platformでユーザを管 理するための各 手 順について説 明します。これらのステップでは、NetWitness Platformでユーザを追 加する方 法について、さらにユーザが実 行できる操 作を制 御する方 法について説 明します。

トピック

- 「ステップ1. 事 前 構 成されたNetWitness Platformロールの確 認」
- 「ステップ2. (オプション) ロールの追 加と権 限の割り当 て」
- 「ステップ3. ロールごとのクエリおよびセッションの属 性の検 証」
- 「ステップ4. ユーザの設 定」
- 「ステップ5. (オプション) 外 部グループへのユーザ ロールの割り当 て」

ステップ1. 事前構成されたNetWitness Platformロールの確認

ロールの作成と権限の割り当てのプロセスを簡単にするために、NetWitness Platformには事前構成されたロールがあります。

ロール	権限
Administrators	完全なシステム アクセス権を持ちます。デフォルトでは、System Administratorsペルソナにはすべての権限が付与されています。
Respond_ Administrator	すべての対応権限にアクセスします。Respond Administratorペルソナは、応答のシステム構成に重点を置いています。
Data_Privacy_ Officers	DPO(Data Privacy Officer) ペルソナは、Administratorsと類似していますが、システム内の機密データの難読化および表示を管理する設定オプションに焦点を当てた権限が追加されています(『*データ プライバシー管理ガイド*』を参照) 。DPOロールを持つユーザは、どのメタ キーに難読化のフラグが付いているかを確認でき、難読化されているメタ キーおよびフラグが付いているメタ キーの値を確認することもできます。
SOC_ Managers	Analystsと同じアクセス権に加えて、インシデントの処理に必要な権限を持ちます。SOC Managersペルソナは、対応に構成に必要な権限以外は、Analystsと同一です。
Operators	構成へのアクセス権を持ちますが、メタおよびセッションのコンテンツへのアクセス権は持ちません。System Operatorsペルソナは、システム設定に焦点を当てていますが、Investigation、ESA、Alerting、Reporting、Respondには焦点を当てていません。
Malware_ Analysts	Investigationとマルウェア イベントへのアクセス権を持ちます。Malware Analystsペルソナには、Malware Analysisモジュールへのアクセス権だけが付与されています。
Analysts	メタおよびセッションのコンテンツへのアクセス権を持ちますが、構成へのアクセス権は持ちません。SOC(セキュリティ オペレーション センター) のAnalystsペルソナは、Investigation、ESA、Alerting、Reporting、Respondに焦点を当てていますが、システム設定には焦点を当てていません。
UEBA_ Analysts	[**調査**] > [**ユーザ**]ビューで、RSA NetWitness UEBAサービスにアクセスします。NetWitness UEBAは、ネットワーク環境内のすべてのエンティティにおける危険な行動を検出、調査、監視するための高度な分析ソリューションです。 **注**:このロールに特定の権限を設定する必要はありません。必要な操作はこのロールをユーザに割り当てることだけです。そのユーザはNetWitness UEBAにアクセスできるようになります。

管理者はカスタムのロールを追加できます。

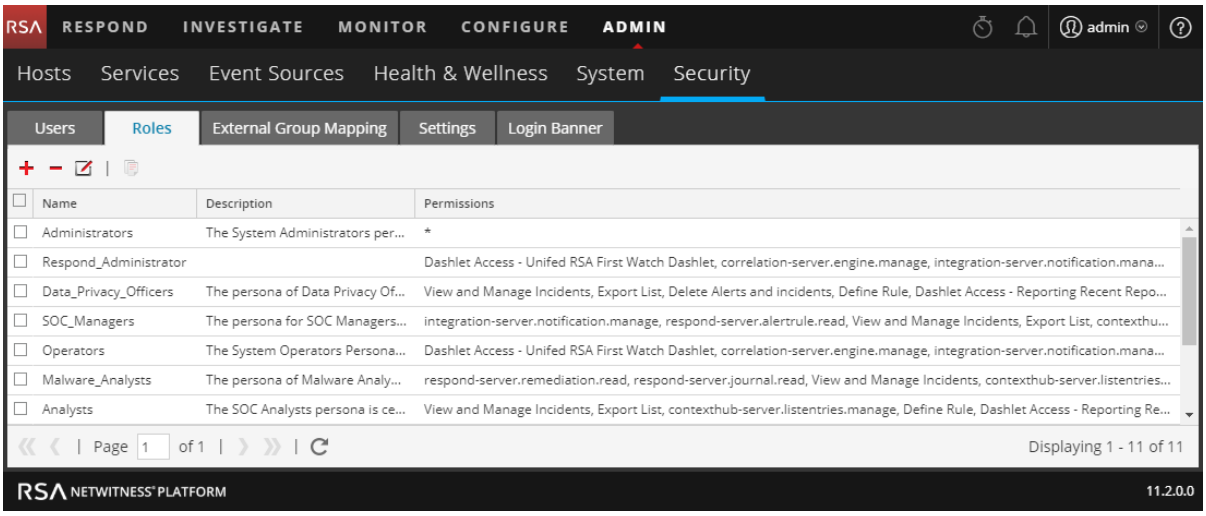
ステップ2. (オプション) ロールの追 加と権 限 の割り当 て

NetWitness Platformには事 前 構 成されたロールがありますが、カスタムのロールを追 加 することもできます。たとえば、事 前 構 成されたAnalystsロールに加 えて、AnalystsEuropeおよびAnalystsAsiaというカスタム ロールを追 加 できます。権 限 の詳 細なリストについては、「ロールの権 限 」を参 照してください。

[**ロール**]タブで次 の手 順を開 始します。

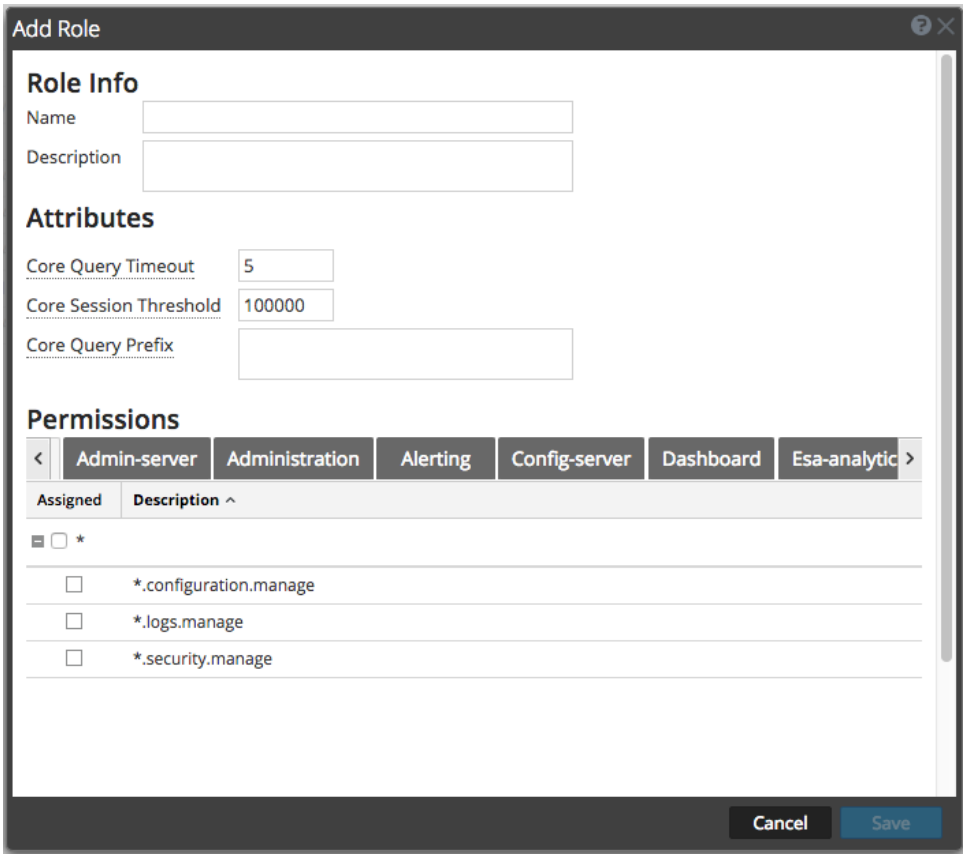
[ロール]タブに移 動する方 法

1. [**管 理**]＞[**セキュリティ**]に移 動します。
   [セキュリティ]ビューが表 示され、[**ユーザ**]タブが開きます。
2. [**ロール**]タブをクリックします。



ロールの追 加と権 限 の割り当 て

1. [**ロール**]タブで、ツールバーの+をクリックします。
2. [**ロールの追 加**]ダイアログが表 示されます。



3. [**ロール情報**]セクションで、次 の情 報を入 力します。
   - **名 前**
   - (オプション) **説 明**
4. [**属 性**]セクションで、各 属 性の目 的の値を入 力します。属 性の詳 細については、ステップ3. ロールごとのクエリおよびセッションの属 性の検 証
5. [**権 限**]セクションで次 の操 作を実 行します。
   - < および > をクリックして、モジュールのリストをスクロールします。
   - ロールでアクセスするモジュールを選 択します。
   - ロールに付 与 する権 限を1つずつ選 択します。

6. ロールに割り当 てるすべての権 限を選 択 するまで繰り返します。
7. [**保 存**]をクリックして新しいロールを追 加します。このロールは即 座に有 効になります。これで、作 成したロールをユーザに割り当 てることができます。

ロールの複 製

新しいロールを追 加する効 率 的な方 法として、既 存 のロールを複 製して新しい名 前で保 存し、割り当 てられている権 限を編 集する方 法 があります。

1. [**ロール**]タブで、複 製するロールを選 択して、をクリックします。
2. 新しいロール名 を入 力し、[**保 存**]をクリックします。
3. 権 限を変 更するには、次 の手 順に従ってください。

ロールに割り当 てられた権 限 の変 更

1. [**ロール**]タブで、ロールを選 択してをクリックします。
   [**ロールの編 集**]ダイアログが表 示されます。
2. [**権 限**]セクションで次 の操 作を実 行します。
   - および をクリックして、モジュールのリストをスクロールします。
   - 権 限を編 集するモジュールを選 択します。
   - 各 権 限を選 択または選 択 解 除します。
3. ロールに必 要な権 限 が割り当 てられるまで、このステップを繰り返します。
4. [**保 存**]をクリックします。編 集 後 の権 限 がすぐに有 効になります。

ロールの削 除

ユーザに割り当 てられていないロールは削 除 できます。

1. [**ロール**]タブで、ロールを選 択して をクリックします。
2. ロールを削 除するかどうかの確 認を求 めるダイアログが開きます。**はい**をクリックします。

ステップ3. ロールごとのクエリおよびセッションの属性の検証

このトピックでは、クエリおよびセッションの属性について説明し、ユーザ ロールに対してこれらの属性を設定する手順を紹介します。また、ロールの設定がユーザ個別の設定にどのように影響を及ぼすか、またユーザが複数のロールに属している場合はどうなるのかについても説明します。

ユーザ ロールを定義したら、各ロールに設定されているクエリおよびセッションの属性を確認することが重要です。これらの設定は、要件に応じて調整できます。

クエリおよびセッションの属性

クエリおよびセッションの属性によって、ユーザが実行するクエリの処理方法が決まります。これらの属性を使用すると、ユーザが取得できる情報を制限できます。これらの属性は、ロールに割り当てられたユーザのすべてのセッションに適用されます。

要件に応じて、次のクエリ属性を、ユーザ ロールに対して指定できます。

- [**Coreクエリ タイムアウト**]は、NetWitness Platformのコア サービスに対して適用されるオプションの設定です。これにより、ユーザがクエリを実行できる最長時間が分単位で指定されます。この値を設定する場合は、ゼロ(0) 以上にする必要があります。ゼロを指定するとタイムアウトしません。デフォルト値は5分です。
- [**Coreセッション閾値**]は必須の設定です。この値はゼロ(0) 以上でなければなりません。デフォルトは、100000です。ここで指定した制限は、Investigate表示設定で定義された[**最大セッション エクスポート**]値を上書きします。この閾値がゼロより大きい場合は、セッション カウントが閾値を超えると、クエリの最適化により、セッション カウントの合計が推定されます。クエリが返したメタ値が閾値に達すると、システムでは以下の動作を行います。
  - セッションのカウントを停止する
  - 閾値と、閾値に達するまでに要したクエリ時間の割合を表示する
- [**Coreクエリ プレフィックス**]は、ユーザが実行するクエリに適用されるオプションのフィルタです。プレフィックスによって、ユーザに表示されるクエリの結果が制限されます。たとえば、クエリ プレフィックスに `'service' = 80` を指定した場合、ユーザが実行するクエリの先頭にこの条件が付加され、ユーザは、HTTPセッションのメタデータにしかアクセスできなくなります。

注 : バージョン11.1以降では、Coreクエリ プレフィックスで、設定済みのメタ エンティティを使用できます。メタ エンティティの設定の詳細については、『*コア データベース チューニング ガイド*』を参照してください。

ユーザに適用されるクエリ操作属性は、ユーザに割り当てられたロールにより異なります。ロールのクエリ属性の設定を確認することが重要です。

ユーザへのクエリ属性の適用順序

ユーザが複数のロールに属している場合、そのユーザには次のロジックが適用されます。

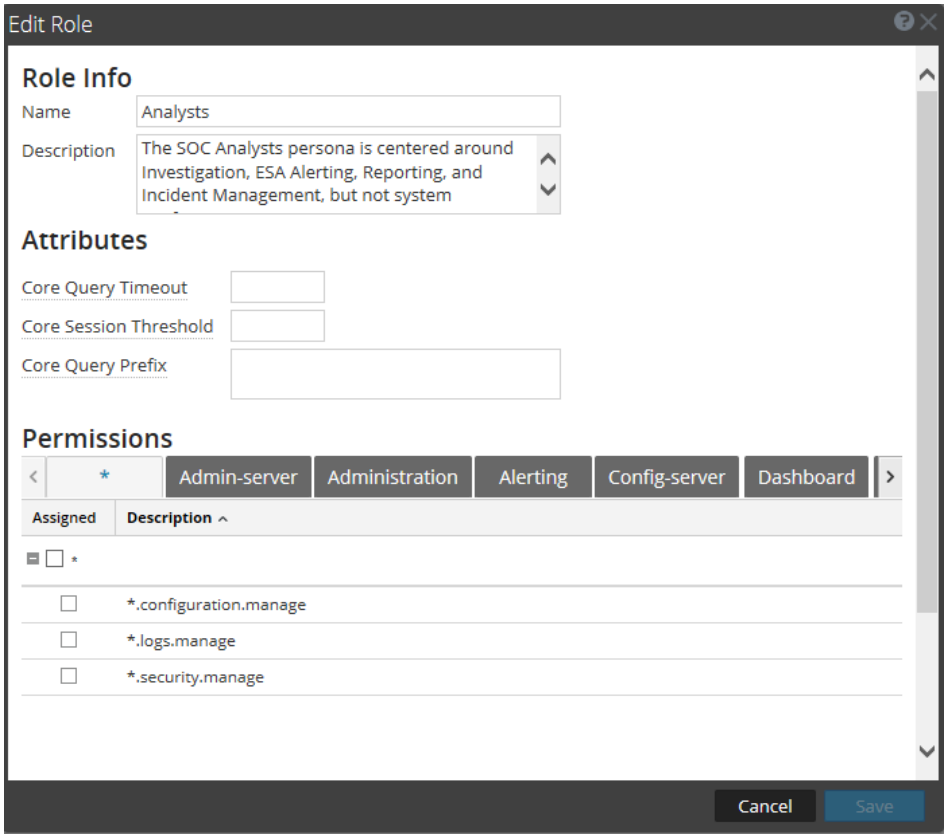
- **クエリ タイムアウト** : ユーザに割り当てられたすべてのロールの中の最も許容範囲が広い値(最大値) 。

- **クエリ プレフィックス**: 各 ユーザ ロールのクエリ プレフィックスはANDで連 結 されます。
- **セッション閾 値** : ユーザに割り当 てられたすべてのロールの中 の最 大 値 。

ユーザ ロールのクエリ属 性 の設 定

1. **[管 理]** > **[セキュリティ]**に移 動します。
   [セキュリティ]ビューが表 示 され、[**ユーザ**]タブが開きます。

2. [**ロール**]タブをクリックします。ロールを追 加 する場 合 は、 をクリックします。ロールを編 集 する場 合 は、ロールを選 択 し、 をクリックします。
   [ロールの追 加]または[ロールの編 集]ダイアログが表 示 されます。



3. ロールの属 性 を設 定 するには、[**属 性**]セクションで次 の操 作 を行います。
   - (オプション) [**Coreクエリ タイムアウト**]フィールドに、ユーザがクエリを実 行 できる最 長 時 間 を分 単 位 で入 力 します。このタイムアウトは、Investigationから実 行 されるクエリに適 用 されます。
   - (オプション) [**Coreセッション閾 値**]フィールドに、システムによるセッションのカウントを停 止 する閾 値 を入 力 します。
   - (オプション) **Coreクエリ プレフィックス**を入 力 して、ロール メンバの[調 査]の[ナビゲート]ビュー、[イベント]ビュー、[イベント分 析]ビューに表 示 されるクエリ結 果 をフィルタ処 理 します。特 定 のロールを持 つユーザによって実 行 されるすべてのクエリの前 に付 加 されるクエリを指 定 できます。たとえば、クエリ プレフィックスに`'service' = 80` を指 定 した場 合 、このロールのユーザが実 行 す

るクエリの先 頭 にこの条 件 が付 加 され、ユーザは、HTTPセッションのメタデータにしかアクセスでき なくなります。ユーザがHTTP以 外 のイベントに移 動しようとすると、ビューは表 示 されません。

4. ［**保 存**］をクリックします。

ステップ4. ユーザの設 定

このトピックでは、新しいユーザを設 定する手 順について説 明します。

トピック

- ユーザの追 加とロールの割り当 て
- ユーザ アカウントの有 効 化 、ロック解 除 、削 除

ユーザの追加とロールの割り当て

このトピックでは、ローカル ユーザまたは外部ユーザの各タイプの新しいユーザを追加する方法について説明します。ロールをローカル ユーザに割り当てる方法についても説明します。

すべてのNetWitness Platformユーザは、ローカル ユーザ アカウントまたは外部ユーザ アカウントを持つ必要があります。

ローカル ユーザ アカウントおよび外部ユーザ アカウントを管理する場合には、次の考慮事項が重要になります。

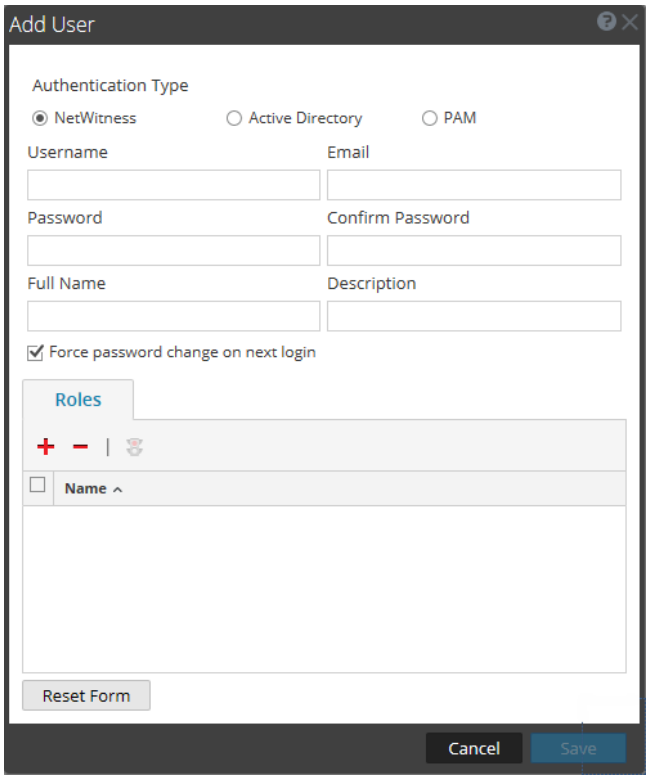
ローカル ユーザ アカウント	外部ユーザ アカウント
NetWitness Platform内で管理されます。	外部で管理され、このドキュメントの範囲外です。
ロールは、直接割り当てられます。	ロールは、外部グループ マッピングによって割り当てられます。
このトピックで説明するように、ユーザに割り当てられた各ロールから権限が継承されます。	アカウントの外部ユーザ グループに割り当てられた各ロールから権限が継承されます。詳細については、「ステップ5. (オプション) 外部グループへのユーザ ロールの割り当て」を参照してください。
NetWitness Platformがすべてのユーザ情報を管理します。	NetWitness PlatformはユーザIDのみを管理します。この値には、ユーザ名、名前、メールが含まれます。

以下に説明する手順はすべて、[ユーザ]タブから実行します。[ユーザ]タブに移動するには、**[管理]＞[セキュリティ]**に移動します。[セキュリティ]ビューが表示され、[ユーザ]タブが開きます。

ローカル ユーザの追加

ローカル ユーザ アカウントを追加し、ユーザにロールを割り当てるには、次の手順を実行します。

1. [**ユーザ**]タブで、ツールバーの＋をクリックします。
   [**ユーザの追加**]ダイアログが表示されます。



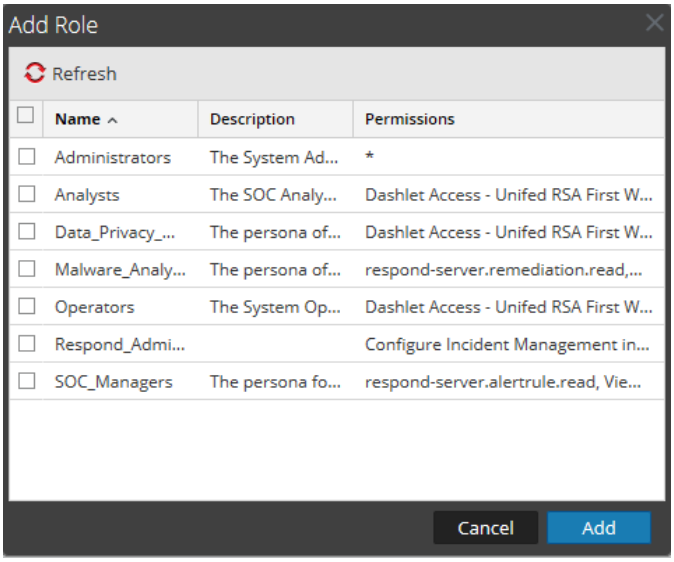
2. 新しいユーザについて次のアカウント情報を入力します。
   - **Authentication Type**: [**NetWitness**] がデフォルトで選択されています。これはローカル ユーザを追加する場合の適切な選択肢です。このオプションは、ADまたはPAM構成が設定されていて、その認証タイプが選択できる場合にのみ表示されます。

注: ADまたはPAM構成がない場合、認証タイプは自動的に[NetWitness]に設定され、それ以外のオプションは使用できません。

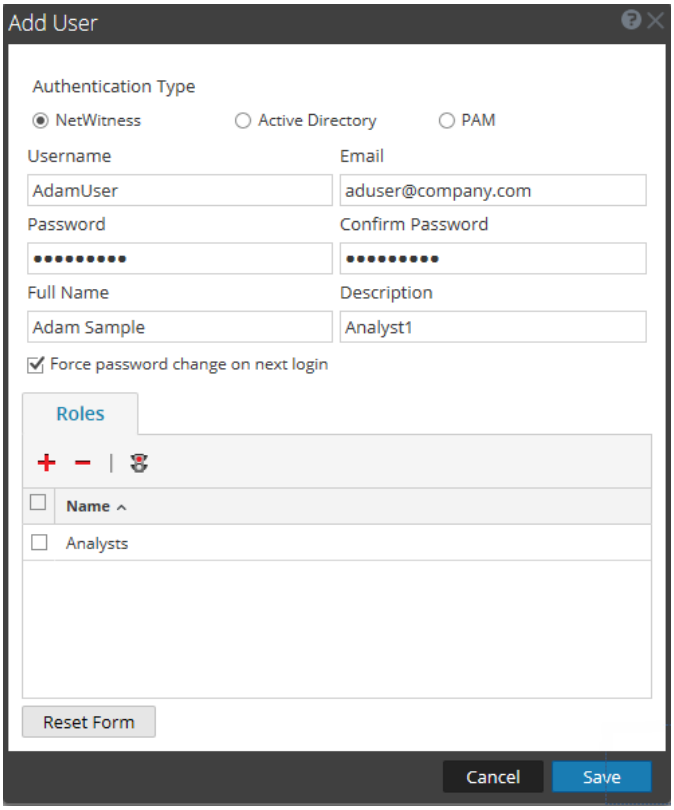
   - NetWitness Platformにログオンするための**ユーザ名**
   - **メール** アドレス
   - NetWitness Platformにログオンするためのパスワード ([**パスワード**] フィールドと[**パスワードの確認**] フィールド)
   - 新しいユーザの**フルネーム**
   - (オプション) ユーザ アカウントの**説明**

3. ユーザが次回ログオンしたときに、パスワードを期限切れにするには、[**次回ログイン時にパスワードの変更を強制**] を選択します。
   アクティブなユーザ セッションには影響しません。ユーザのパスワードが期限切れになったことを示す がユーザ行に表示されます。パスワードを期限切れにした後で、それを元に戻すことはできません。このチェックボックスは、次回のユーザ アカウント編集時にオフになります。

4. ロールをユーザに割り当 てるには、[**ロール**]タブの**+**をクリックします。
[**ロールの追 加**]選 択ダイアログに、使 用 可 能なロールのリストが表 示されます。

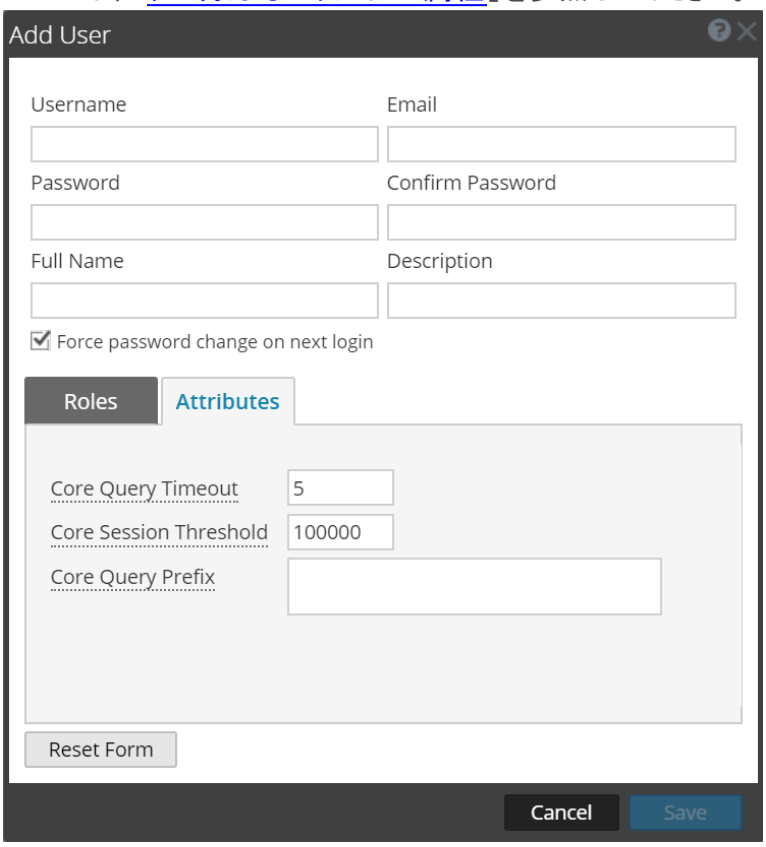


5. 割り当 てるロールをそれぞれ選 択して、[**追 加**]をクリックします。
[**ユーザの追 加**]ダイアログに、ユーザに割り当 てるロールがすべて表 示されます。

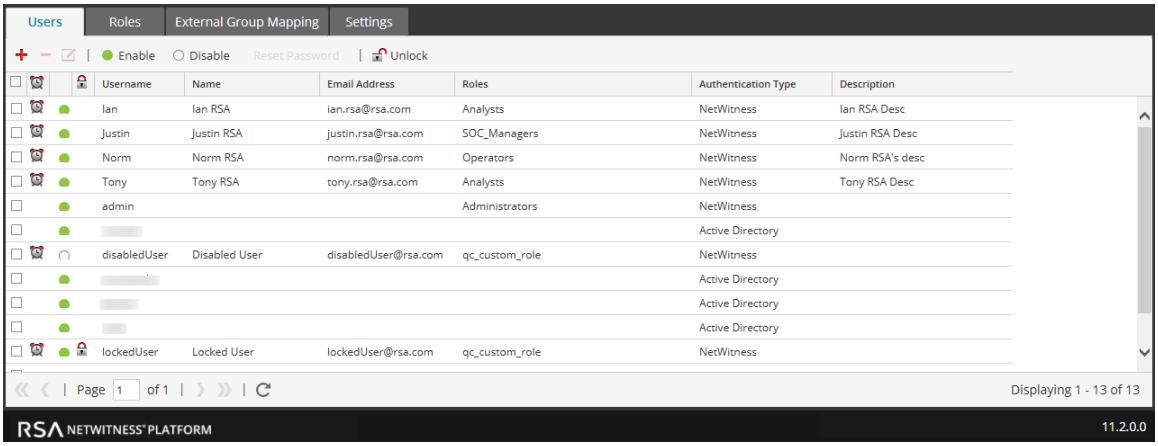


6. (オプション) ユーザに属 性を割り当 てるには、[**属 性**]に移 動し、適 切な値を変 更します。これらの属 性はユーザに固 有であり、ロール内の属 性に対してすべて同じ規 則に従います。属 性の詳 細に

ついては、「クエリおよびセッションの属 性」を参 照してください。



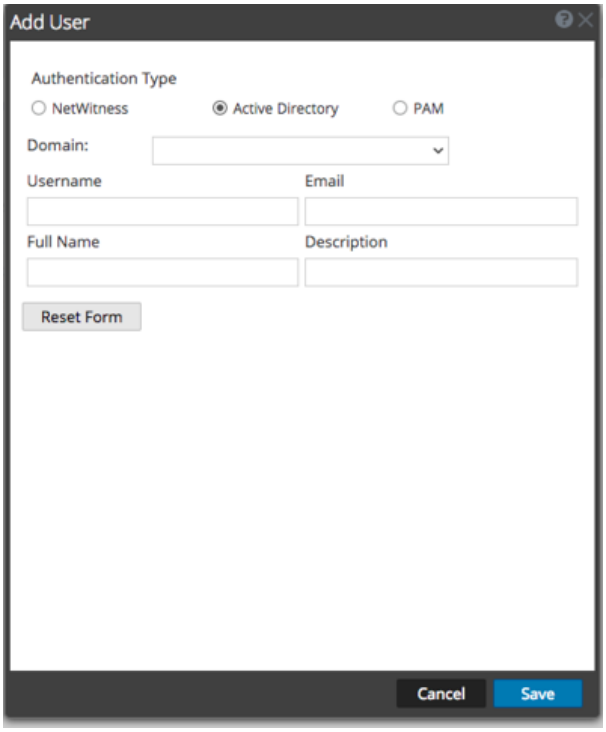
7. (オプション) ロールを選 択し、をクリックして、そのロールに関 する**すべての権 限を表 示**します。
8. [**保 存**]をクリックします。
[**ユーザ**] タブに、新 しいユーザおよびこのユーザに割り当 てられた各 ロールが表 示されます。このアカウントは即 座にアクティブになります。

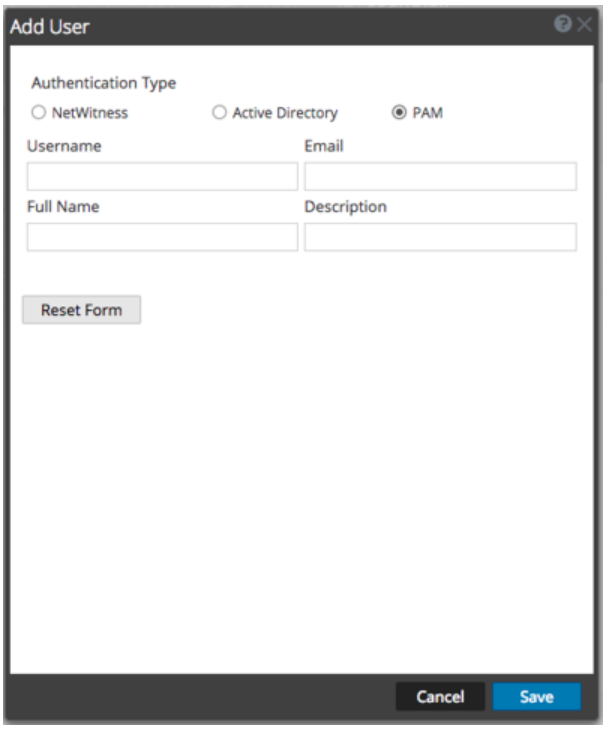


外 部 認 証 のためのユーザの追 加

前 提 条 件 : 外 部 認 証 を構 成 しておく必 要 があります。「ステップ4. (オプション) 外 部 認 証 の構 成 」を参 照 してください。

1. [**ユーザ**] タブで、ツールバーの＋をクリックします。
   [**ユーザの追 加**] ダイアログが表 示 されます。
2. [**認 証 タイプ**] で、[**Active Directory**] または [**PAM**] のいずれかを選 択 します。ダイアログが更 新 され、選 択 した外 部 認 証 タイプの必 須 入 力 フィールド が表 示 されます。





3. 次の情報を入力します。
   - **ドメイン**(Active Directory認証を選択した場合のみ) : 使用可能なドメインのドロップダウン リストからユーザのActive Directoryドメインを選択します。
   - NetWitness Platformにログオンするための**ユーザ名**
   - **メール** アドレス
   - 新しいユーザの**フルネーム**
   - (オプション) ユーザ アカウントの**説明**
4. [**保存**]をクリックします。[ユーザ]タブに、ロールと権限が必要な新しいユーザ アカウントが表示されます。
5. 新しいユーザにロールを割り当てる場合は、「ステップ5. (オプション) 外部グループへのユーザ ロールの割り当て」を参照してください。

ユーザ情報またはロールの変更

ユーザのアカウント情報または割り当てられたロールを変更するには、次の手順を実行します。

1. [**ユーザ**] タブで、ユーザを選択し、ツールバーの  をクリックします。
   [**ユーザの編集**]ダイアログが表示されます。
2. ユーザ情報を編集するには、次の任意のフィールドを変更します。
   - **メール**
   - **名前**

- **説明**

3. **内部**ユーザが次回ログオンしたときにそのユーザのパスワードを期限切れにするには、[**次回のログイン時にパスワードの変更を強制**]を選択します。アクティブなユーザ セッションには影響しません。
   ユーザのパスワードが期限切れになったことを示す  がユーザ行に表示されます。パスワードを期限切れにした後で、それを元に戻すことはできません。このチェックボックスは、次回のユーザ アカウント編集時にオフになります。
4. [**ロール**]セクションで次の操作を実行します。
   - 別のロールを割り当てるには、➕をクリックし、ロールを選択して[**追加**]をクリックします。
   - 割り当てられたロールを削除するには、ロールを選択して➖をクリックします。
7. [**保存**]をクリックします。

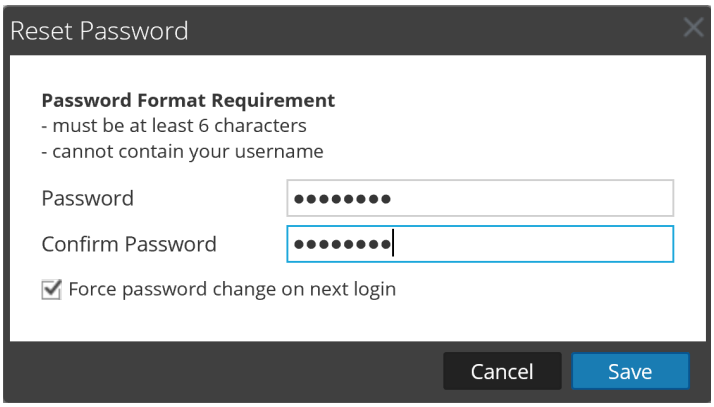
ユーザの削除

1. [**ユーザ**]タブで、ユーザを選択します。
2. ツールバーで➖をクリックします。
3. [**保存**]をクリックします。

注：Active Directoryによって外部で認証されるユーザを完全に削除するには、そのユーザをADグループからも削除する必要があります。

ユーザ パスワードのリセット

1. [**ユーザ**]タブで、ユーザを選択します。
2. ツールバーで[**パスワードのリセット**]をクリックします。



   [**パスワード形式の要件**]セクションには、パスワードの具体的な要件のリストが表示されます。管理者は、パスワード ポリシーですべての内部ユーザについてこれらの要件を調整できます。「ステップ1. パスワードの複雑性の構成」を参照してください。
3. ユーザがNetWitness Platformに次回ログインするときにパスワードの変更を強制するかどうかを選択します。
4. [**保存**]をクリックします。

ユーザ アカウントの有 効 化 、ロック解 除 、削 除

このトピックでは、ユーザ アカウントを有 効 化 、ロック解 除 、削 除 するための手 順 について説 明します。

NetWitness Platformのすべてのユーザは、ユーザ名 とパスワードを持 つローカル ユーザ アカウントを持 つか、または外 部 ユーザ アカウントを持 つ必 要 があります。NetWitness Platformで、ローカル ユーザ アカウントの有 効 化 、無 効 化 、削 除 を行うことができます。

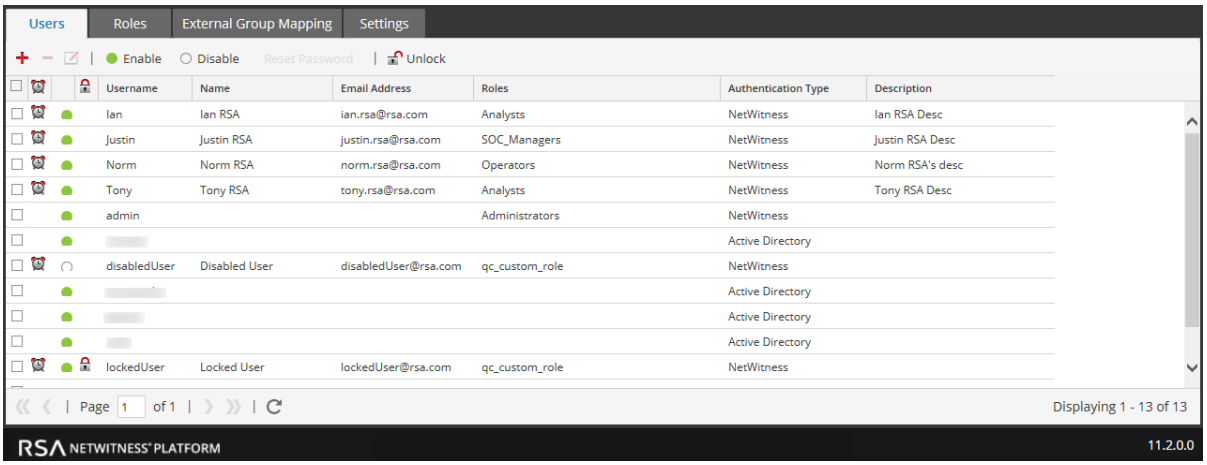
外 部 ユーザが最 初 にNetWitness Platformへログインする際 には、新 しいユーザ エントリーがNetWitness Platformによって自 動 的 に作 成 されます。NetWitness Platformはユーザ情 報 (たとえば名 前 やメール など) のみを管 理 します。

また、ローカルおよび外 部 の両 方 のユーザについて、ロックされたアカウントのロックを解 除 できます。

無 効 化 されたNetWitness Platformユーザ アカウントの有 効 化

無 効 化 されたNetWitness Platformユーザ アカウントを有 効 にするには、次 の手 順 を実 行 します。

1. NetWitness Platformで、[**管 理**] > [**セキュリティ**]に移 動 します。
   [セキュリティ]ビューが表 示 され、[**ユーザ**]タブが開きます。



2. [**ユーザ**] グリッド で、1つ以 上 のアカウントを選 択 します。
3. Enableをクリックします。
   確 認 のダイアログが表 示 されます。
4. アカウントを有 効 化 する場 合 は、[**はい**]をクリックします。
   アカウントが有 効 になり、ユーザがNetWitness Platformにログインできます。

NetWitness Platformユーザ アカウントの無 効 化

ユーザを無 効 化 することにより、ユーザ アクセスをブロックできます。ユーザを無 効 化 してもユーザ環 境 設 定 は削 除 されません。このアクションは、ユーザ環 境 設 定 を保 持 したまま、ユーザのアクセスをブロックします。ユーザを再 度 有 効 にすると、ユーザ環 境 設 定 はそのまま維 持 されます。ユーザに再 度 アクセスを許 可 するには、ユーザ アカウントを有 効 化 します。ユーザの無 効 化 はローカル ユーザのみ実 行 することができます。外 部 ユーザは無 効 化 できません。

NetWitness Platformユーザ アカウントを無効化するには、次の手順を実行します。

1. [**ユーザ**] グリッドで、1つ以上のアカウントを選択します。
2. Disableをクリックします。
   確認のダイアログが表示されます。
3. アカウントを無効化する場合は、[**はい**]をクリックします。
   アカウントが無効になり、ユーザがNetWitness Platformにログインできなくなります。

ロックされたNetWitness Platformユーザ アカウントのロックの解除

ユーザは、指定した回数ログインに失敗すると、一定期間ロックアウトされます。ロックされたNetWitness Platformユーザ アカウントのロックを解除するには、次の手順を実行します。

1. [**ユーザ**] グリッドで、1つ以上のアカウントを選択します。
2. Unlockをクリックします。
   確認のダイアログが表示されます。
3. アカウントのロックを解除する場合は、[**はい**]をクリックします。
   アカウントのロックが解除され、ユーザがNetWitness Platformにログオンできます。

NetWitness Platformユーザ アカウントの削除

外部認証を使用しない場合、ユーザはローカル アカウントを使用してNetWitness Platformにログオンできます。これらのローカル アカウントは、NetWitness Platformを使用して直接管理します。ローカル ユーザのアクセスを拒否するには、アカウントを無効にするか、システムからアカウントを完全に削除します。

注：これによって、NetWitness Platformからアカウントのすべての環境設定が削除されます。環境設定を破棄したくない場合には、ユーザを削除するのではなく、ユーザを無効にします。

NetWitness Platformユーザ アカウントを削除にするには、次の手順を実行します。

1. [**管理**] > [**セキュリティ**]に移動します。
   [セキュリティ]ビューが表示され、[**ユーザ**]タブが開きます。
2. [ユーザ]リストで、1つ以上のアカウントを選択します。
3. をクリックします。
   警告ダイアログで、確認が要求されます。
4. アカウントを削除する場合は、[**はい**]をクリックします。
   アカウントがNetWitness Platformから削除され、ユーザがNetWitness Platformにログインできなくなります。

ステップ5. (オプション) 外 部 グループへのユーザ ロールの割り当 て

このトピックでは、NetWitness Platformユーザ ロールを外 部 グループに割り当 てる方 法 について説 明しま す。

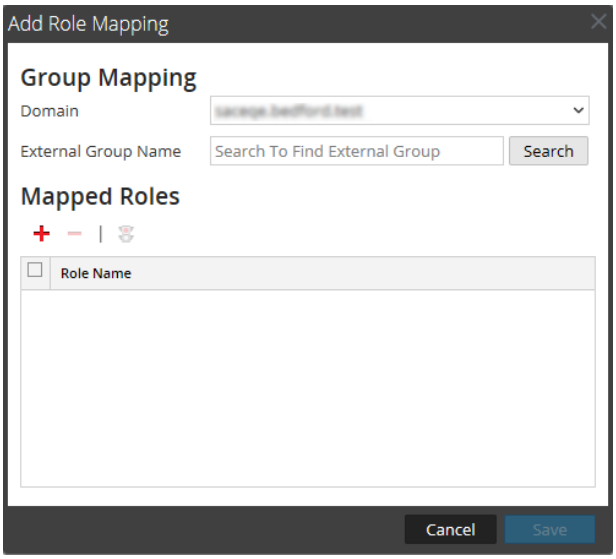
NetWitness Platformでは、外 部 グループは、権 限を割り当 てられたNetWitness Platformユーザ ロール から各 種 モジュールとビューの権 限を継 承します。外 部 グループがSecurity Analyticsシステムにアクセス できるようにするには、外 部 グループにユーザ ロールを割り当 てます。外 部 グループのアクセスを変 更 す るには、割り当 てられているロールを編 集します。外 部 グループによるアクセスに必 要 な権 限の割り当 て が完 了 するまで、ロールを追 加 および削 除します。変 更 は即 座 に有 効になります。

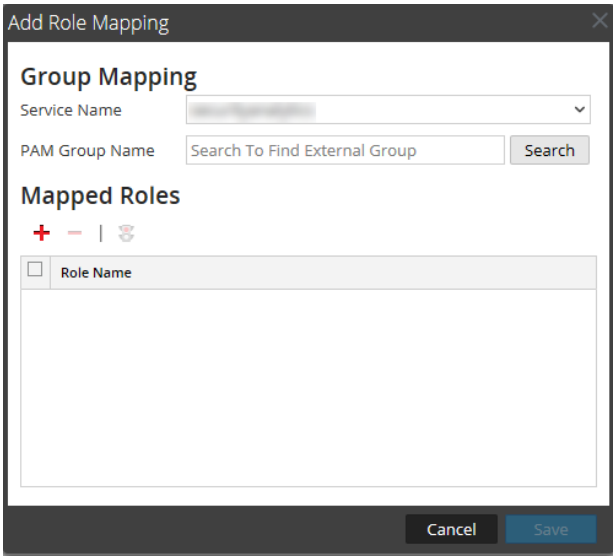
前 提 条 件

[設 定]タブで、外 部 ユーザ認 証 のための方 法 を設 定し、外 部 グループがNetWitness Platformに表 示さ れるようにします。

外 部 グループのロール マッピングの追 加

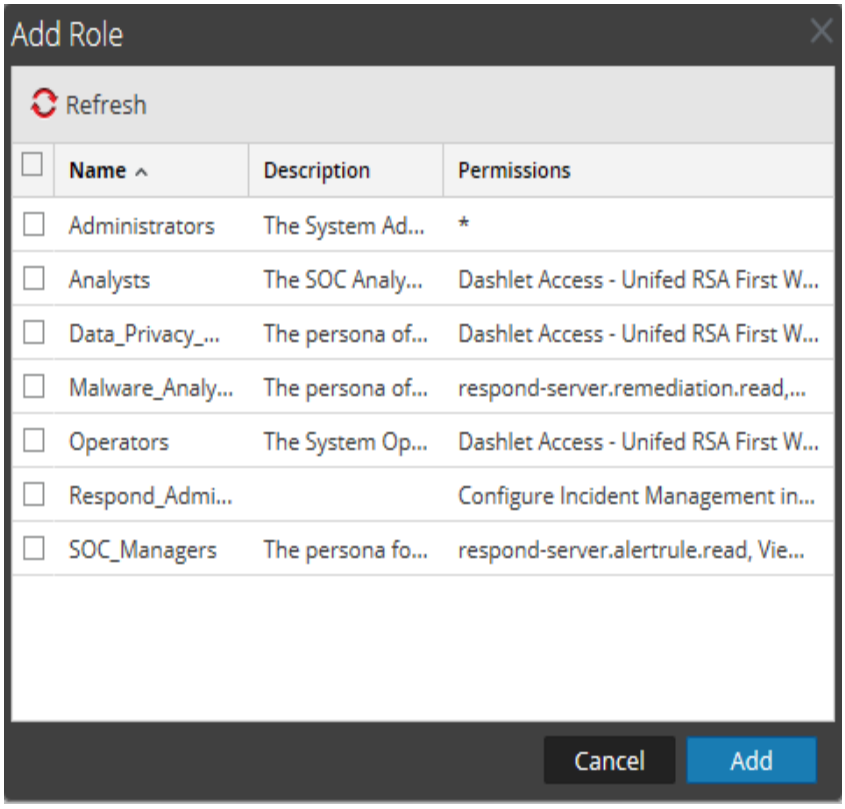
1. NetWitness Platformで、[**管 理**]＞[**セキュリティ**]に移 動します。
   [セキュリティ]ビューが表 示され、[**ユーザ**]タブが開きます。
2. [**外 部 グループ マッピング**]タブをクリックします。
3. ツールバーで＋をクリックします。
   選 択した外 部 認 証 方 法に対 応した[**ロール マッピングの追 加**]ダイアログが表 示されます。





4. [**検 索**]をクリックし、[外 部 グループの検 索]で外 部 グループ名 を検 索して選 択します。

5. グループ マッピングにロールを追 加 するには、[**マップされたロール**] セクションの＋をクリックします。
[**ロールの追 加**] ダイアログが表 示 されます。



6. タイト ル バーのチェックボックスをオンにして、すべてのロールを選 択 するか、または個 別 にロールを選 択 します。
7. [ロール マッピングの追 加] ダイアログの[**マップされたロール**] セクションにロールを追 加 するには、[**追 加**] をクリックします。
ダイアログが閉じ、選 択 したロールが[マップされたロール] セクションに表 示 されます。
8. [**マップされたロール**] セクションからロールを削 除 する場 合 は、ロールを選 択 し、 － をクリックします。
9. [**ロール マッピングの追 加**] ダイアログで、グループに定 義 するロール マッピングが完 了 したら、[**保 存**] をクリックします。
[ロール マッピングの追 加] ダイアログが閉じ、新しいロール マッピングが[外 部 グループ マッピング] タブ リストに示 されます。

グループのロール マッピングの編 集

1. [**外 部 グループ マッピング**] アクション バーで、[**編 集**] をクリックします。
[**ロール マッピングの編 集**] ダイアログが開き、[**外 部 グループ名**] フィールドにグループ名 が表 示 されます。
2. マッピングにロールを追 加 するには、[**マップされたロール**] セクションの＋をクリックします。
[ロールの追 加] ダイアログが表 示 されます。

3. タイトル バーのチェックボックスをオンにして、すべてのロールを選 択 するか、または個 別 にロールを選 択します。
4. [**ロール マッピングの追 加**]ダイアログの[**マップされたロール**]セクションにロールを追 加 するには、[**追 加**]をクリックします。
   ダイアログが閉じ、選 択したロールが[マップされたロール]セクションに表 示されます。
5. [**マップされたロール**]セクションからロールを削 除 する場 合 は、ロールを選 択し、 をクリックします。
6. [**ロール マッピングの編 集**]ダイアログで、グループに定 義 するロール マッピングが完 了したら、[**保 存**]をクリックします。
   ダイアログが閉じ、編 集したロール マッピングが[外 部 グループ マッピング]タブに示 されます。

関 連トピック

- 外 部 グループの検 索

外 部 グループの検 索

このトピックでは、NetWitness Platformのユーザ ロールをマッピングする外 部 グループを検 索 する手 順 について説 明します。

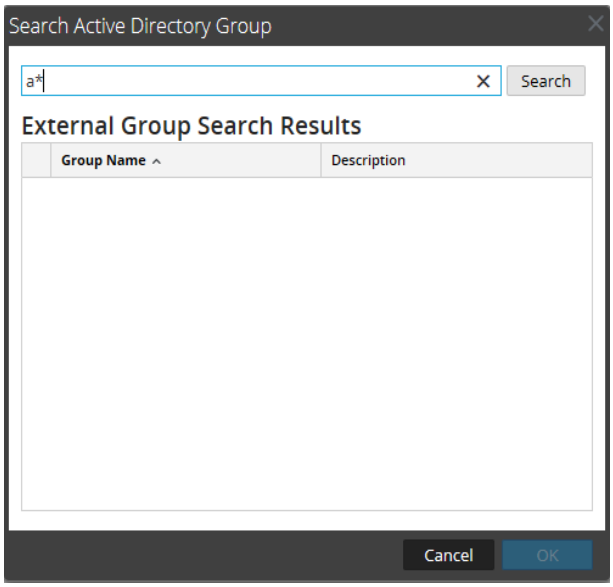
前提条件

外 部 ユーザの認 証 方 法 が有 効 に設 定されている必 要 があります。

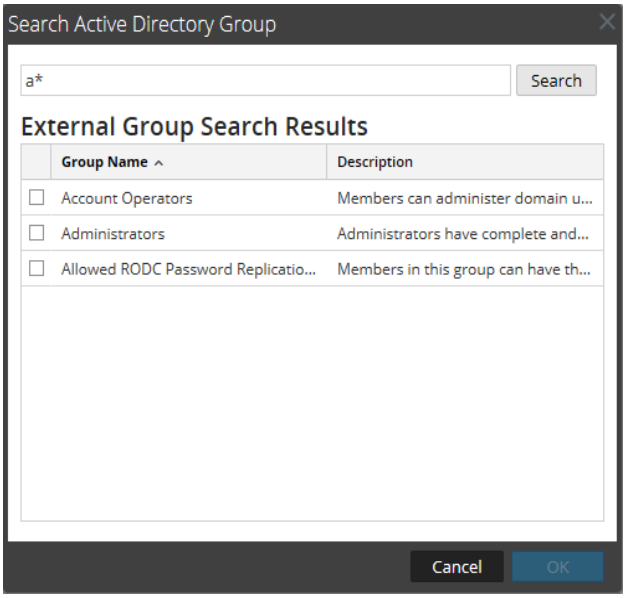
手順

外部グループを検索する方法

1. NetWitness Platformで、**[管 理]＞[セキュリティ]**に移 動します。
   [セキュリティ]ビューが表 示され、[**ユーザ**]タブが開きます。
2. [**外 部 グループ マッピング**]タブをクリックします。
3. ツールバーで、＋または をクリックします。
   選 択した外 部 認 証 方 法 に対 応した[**ロール マッピングの追 加**]ダイアログが表 示されます。
4. [**グループ マッピング**]セクションの内 容 は、選 択されている外 部 認 証 方 法 によって異 なります。
   - **Active Directory**の場 合 は、**ドメイン**を選 択してから、[**外 部 グループ名**]の横 の[**検 索**]をクリック します。
   - **PAM**の場 合 は、[**PAMグループ名**]の横 の[**検 索**]をクリックします。
     [**外 部 グループの検 索**]ダイアログが表 示されます。
5. [**共 通 名**]に、グループ名 を入 力 するか、グループ名 の一 部 をワイルド カード 文 字 (*) とともに入 力 し ます。



6. [**検索**]をクリックします。
   [**外部グループの検索結果**]セクションに結果が表示されます。



7. ロールを割り当てるグループを選択し、[**OK**]をクリックします。

参考情報

このトピックでは、NetWitness Platformにおけるシステム セキュリティとユーザ管 理に関する参考事例をまとめています。

- [管 理]の[セキュリティ]ビュー
- [ユーザ]タブ
- [ユーザの追 加]または[ユーザの編 集]ダイアログ
- [ロール]タブ
- [ロールの追 加]または[ロールの編 集]ダイアログ
- [ログイン バナー]タブ
- [外 部 グループ マッピング]タブ
- [ロール マッピングの追 加]ダイアログ
- [外 部 グループの検 索]ダイアログ
- [設 定]タブ

[管理]の[セキュリティ]ビュー

このトピックでは、[**管理**]>[**セキュリティ**]ビューおよび関連するダイアログやタブのユーザー インターフェイス構成要素について説明します。インタフェース構成要素をアルファベット順に説明します。

[**管理**]>[**セキュリティ**]ビューでは、ユーザー アカウントの管理、ユーザー ロールの管理、NetWitness Platformロールへの外部グループのマッピング、その他のセキュリティ関連のシステム パラメーターの変更などを実行できます。これらの設定はNetWitness Platformシステムに適用され、個々のサービスのセキュリティ設定とあわせて使用されます。

実行したいことは何ですか?

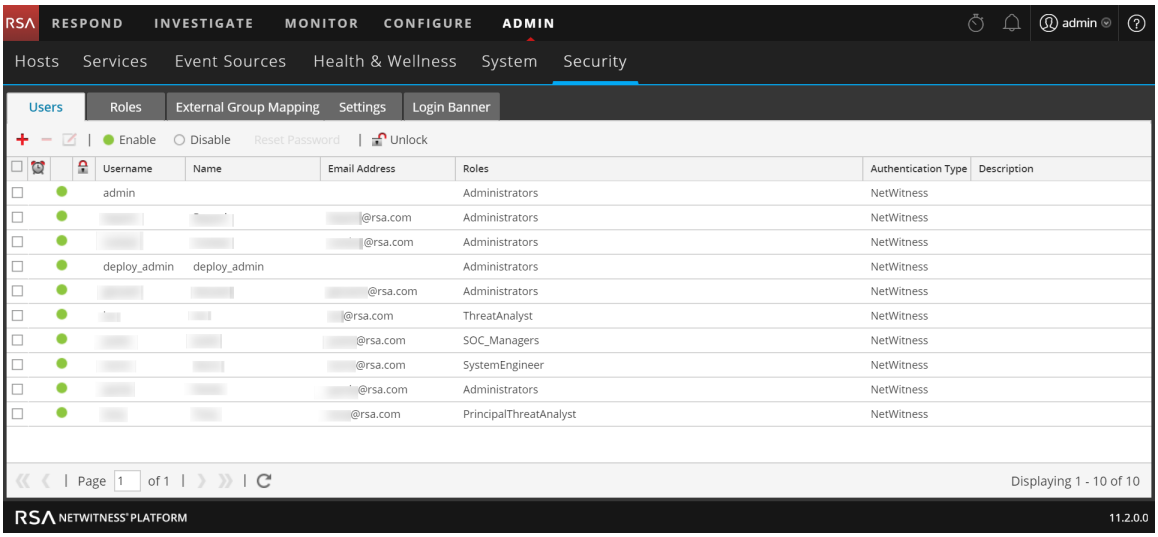
ロール	実行したいこと	手順
管理者	ユーザの管理	ステップ4. ユーザの設定
管理者	ロールの管理	ステップ1. 事前構成されたNetWitness Platformロールの確認 ステップ2. (オプション) ロールの追加と権限の割り当て
管理者	(オプション) 外部グループ マッピングの構成	ステップ5. (オプション) 外部グループへのユーザ ロールの割り当て
管理者	設定の構成	ステップ3. システム レベルのセキュリティ設定の構成
管理者	(オプション) ログイン条件の設定	ステップ5. (オプション) カスタム ログイン バナーの作成

関連トピック

- [ユーザ]タブ
- [ロール]タブ
- [外部グループ マッピング]タブ
- [設定]タブ
- [ログイン バナー]タブ

簡単な説明

[管理]の[セキュリティ]ビューを表示するには、[**管理**]>[**セキュリティ**]に移動します。



[**管 理**] > [**セキュリティ**]ビューには、次 の5個 のタブがあります。

- [**ユーザー**]タブでは、ユーザー アカウントを管 理します。
- [**ロール**]タブでは、セキュリティ ロールの定 義 およびユーザー アカウント へのロールの割り当 てを行います。
- [**外 部 グループ マッピング**]では、LDAPグループのアクセス パラメータを管 理します。
- [**設 定**]タブでは、NetWitness Platform内 部 ユーザのパスワード の複 雑 性 の要 件 と有 効 期 限 を構 成 し、ログイン失 敗 やアイド ル期 間 が連 続 した場 合 のシステムの動 作 を構 成 します。また、外 部 認 証 も構 成 します。
- 事 前 構 成 されたNetWitness Platformロールの確 認
- [**ログイン バナー**]タブでは、ログイン画 面 にアクセスする前 に同 意 する必 要 のある条 件 を設 定 します。

[ユーザ]タブ

このトピックでは、[管理]>[セキュリティ]ビュー>[ユーザ]タブでユーザ アカウントを設定するための機能について説明します。

各NetWitness Platformユーザにはユーザ アカウントが必要です。[ユーザ]タブでは、ユーザ アカウントを作成、編集、削除、有効化/無効化、ロック解除できます。

実行したいことは何ですか?

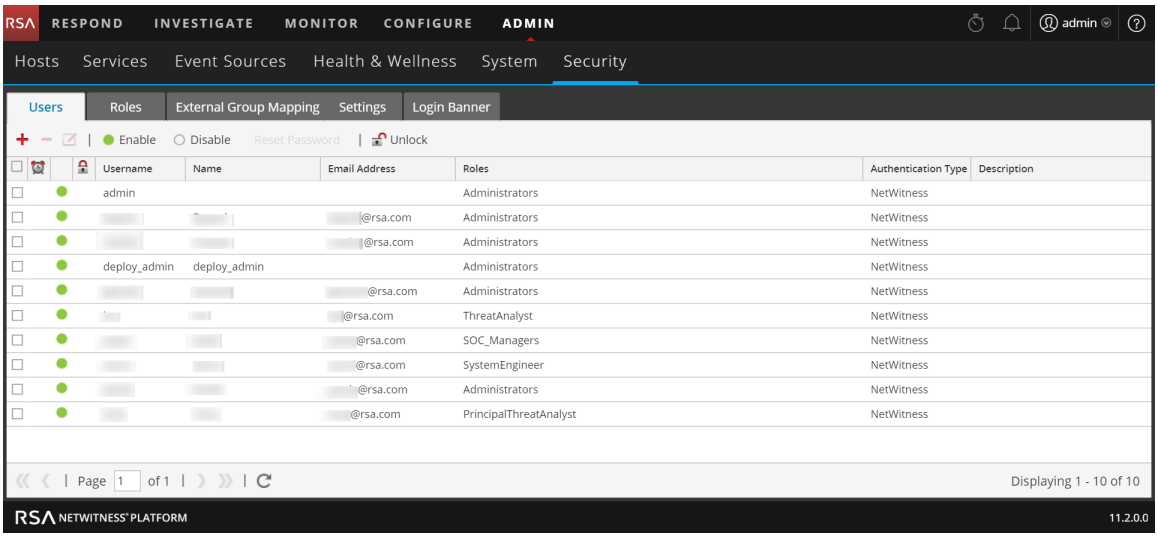
ロール	実行したいこと	手順
管理者	新しいユーザの設定	ステップ4. ユーザの設定 ユーザの追加とロールの割り当て
管理者	ユーザ アカウントの管理	ユーザ アカウントの有効化、ロック解除、削除

関連トピック

- [ユーザの追加]または[ユーザの編集]ダイアログ

簡単な説明

このビューにアクセスするには、**[管理]>[セキュリティ]**に移動します。[セキュリティ]ビューが開き、デフォルトで[**ユーザ**]タブが表示されます。



[ユーザ]タブには[ユーザ]リストが表示され、その上部にツールバーがあります。ツールバーの機能を次に示します。

機 能	説 明
+	[ユーザの追 加]ダイアログを開きます。
−	選 択したユーザを削 除します。
	選 択したユーザの[ユーザの編 集]ダイアログを開きます。
	無 効になっているユーザ アカウントを有 効にします。
	ユーザ環 境 設 定を削 除することなく、ユーザのアクセスをブロックします。ユーザ環 境 設 定を維 持したまま、ユーザを再 度 有 効にすることができます。
パスワードのリセット	[パスワード のリセット]ダイアログが開き、選 択したユーザのパスワードを変 更することができます。このダイアログには、新しいパスワード の要 件 が一 覧 表 示され、次 回 ログイン時 のパスワード の変 更をユーザに強 制 することもできます。
 ロック解 除	指 定された回 数 ログインに失 敗したためにロックされたユーザ アカウント のロック状 態 を解 除します。

[**ユーザ**] リスト には次 の列 があります。

列	説 明
	このアイコンが[ユーザ] 列 に表 示された場 合 、そのユーザのパスワード の有 効 期 限 が切れていることを示しています。
ユーザ名	NetWitness Platformにログ オンするためのユーザ名 。
名 前	ユーザの名 前 。
メール アドレス	ユーザのメール アドレス。
ロール	ユーザに割 り当 てられたロール。
認 証タイプ	認 証 方 法(Active DirectoryまたはPAMによる外 部 認 証 、またはNetWitness Platformによる内 部 認 証) 。
説 明	ユーザ アカウント の説 明 。

[ユーザの追加]または[ユーザの編集]ダイアログ

このトピックでは、[管理]>[セキュリティ]ビュー>[ユーザ]タブからアクセスできる、[ユーザの追加]ダイアログと[ユーザの編集]ダイアログについて説明します。

すべてのユーザには、ユーザ名とパスワードを持つローカル ユーザ アカウント、またはNetWitness Platformにマッピングされた外部ユーザ アカウントが必要です。

実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	ユーザの追加とロールの割り当て	ユーザの追加とロールの割り当て
管理者	ユーザ情報の変更	ユーザ情報またはロールの変更
管理者	ユーザ パスワードのリセット	ユーザ パスワードのリセット
管理者	外部認証のユーザの追加	外部認証のためのユーザの追加

関連トピック

- ロールと権限によるユーザの管理
- ユーザ アカウントの有効化、ロック解除、削除

簡単な説明

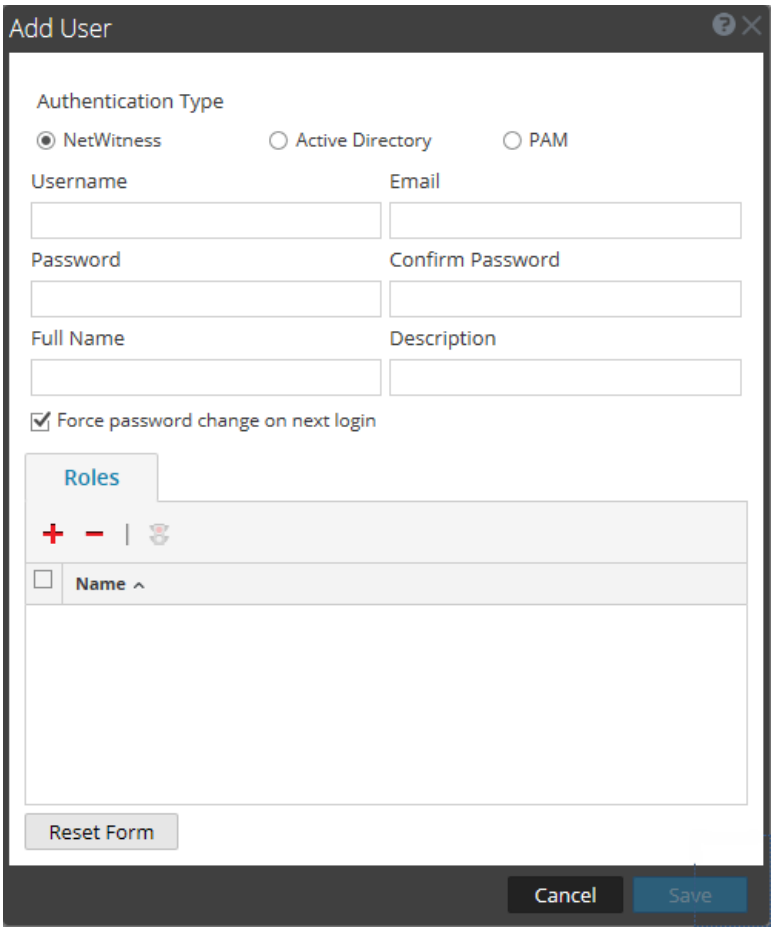
[**ユーザの追加**]または[**ユーザの編集**]ダイアログを表示するには、次の手順を実行します。

1. NetWitness Platformで、[**管理**]>[**セキュリティ**]に移動します。
   [セキュリティ]ビューが表示され、[**ユーザ**]タブが開きます。
2. 以下のいずれかの操作を実行します。
   - アクション バーで、  をクリックします。
     [**ユーザの追加**]ダイアログが表示されます。
   - ユーザを選択し、アクション バーで  をクリックします。
     [**ユーザの編集**]ダイアログが表示されます。

[ユーザの追加]と[ユーザの編集]のダイアログの違いは、[ユーザの追加]ダイアログのみに[**パスワード**]フィールドと[**パスワードの確認**]フィールドが表示される点です。それ以外は同じです。[ユーザの追加]ダイアログでは、新しいユーザのパスワードを設定できます。ユーザは、ユーザ環境設定で自分のパスワードを変更できます。ユーザのパスワードは[ユーザ]タブから直接リセットすることができます。

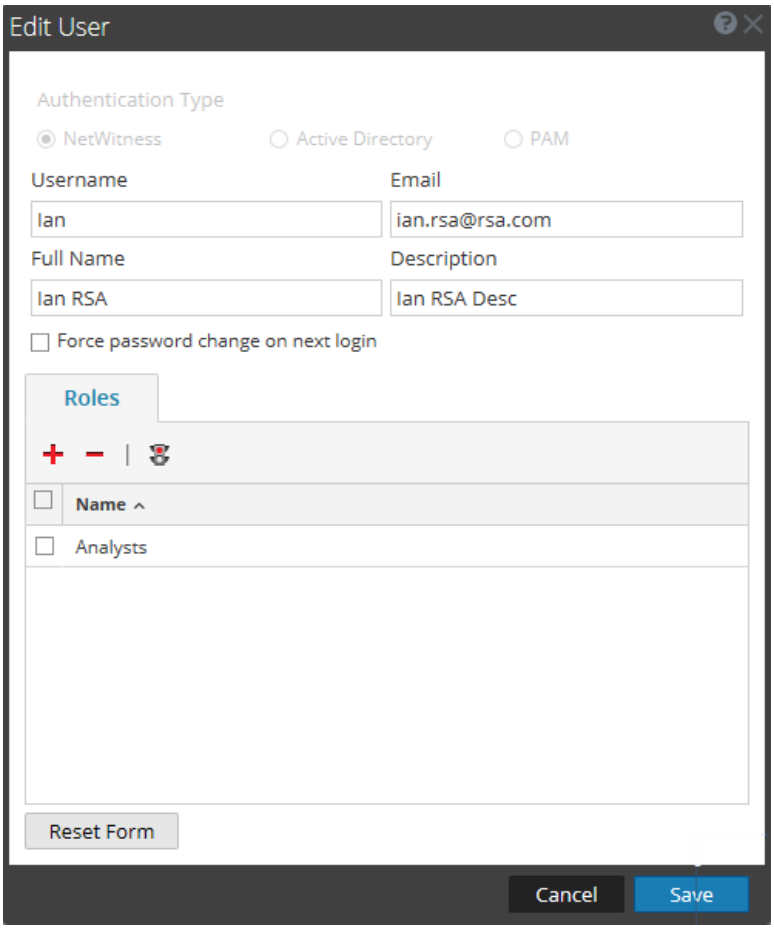
[ユーザの追加]ダイアログ

これは、内部ユーザの[ユーザの追加]ダイアログです。



[ユーザの編 集] ダイアログ

これは、内 部 ユーザの[ユーザの編 集] ダイアログです。



[ユーザの追 加]と[ユーザの編 集]ダイアログには、次 の情 報 が表 示されます。

- 認 証タイプ
- ユーザ情 報
- ユーザが所 属 するロール

ユーザ情 報

次 の表 にユーザ情 報 の説 明を示します。

フィールド	説 明
認 証タイプ	ユーザの認 証タイプ。デフォルト の選 択 は、NetWitnessです。これは、内 部 ユーザを意 味します。外 部 ユーザ用 のオプションは、Active DirectoryとPAMです。ユーザを編 集 するときは、このフィールド は無 効 です。
ユーザ名	NetWitness Platformユーザ アカウント のユーザ名 。
名 前	ユーザの名 前 。
パスワード	([ユーザの追 加]ダイアログのみ) NetWitness Platformにログオンするパスワード 。

フィールド	説 明
パスワード の確 認	([ユーザの追 加] ダイアログのみ) ユーザ パスワード の追 加 のためのパス ワード 確 認 。
メール	ユーザのメール アドレス。
説 明	(オプション) ユーザの説 明 。
次 回 ログイン時 にパスワー ドの変 更 を強 制	ユーザが次 回 NetWitness Platformにログオンしたときにユーザのパス ワードを期 限 切 れにします。このフィールド は内 部 ユーザにのみ適 用 さ れます。アクティブなユーザ セッションには影 響 しません。ユーザのパス ワード が期 限 切 れになったことを示 す がユーザ行 に表 示 されます。 パスワードを期 限 切 れにした後 で、それを元 に戻 すことはできません。 このチェックボックスは、次 回 のユーザ アカウント 編 集 時 にオフになりま す。
リセット	変 更 をクリアします。

[ロール] タブ

次 の表 に、[ロール] タブの各 オプションの説 明 を示 します。[ロール] タブでは、ユーザに割 り当 てられて いるロールを示 します。

オプショ ン	説 明
+	[ロールの追 加] ダイアログが開 き、ユーザに割 り当 てることのできるロールの一 覧 が表 示 さ れます。
−	選 択 したロールがユーザから削 除 されます。
	選 択 したロールの権 限 が表 示 されます。
名 前	ユーザに割 り当 てられているロールが一 覧 表 示 されます。

[ロール]タブ

このトピックでは、[管理]>[セキュリティ]ビュー>[ロール]タブの機能について説明します。

ロールは、すべてのユーザに割り当てられます。ユーザには、ロールで許可される権限が付与されます。[ロール]タブでは、ロールを作成、複製、編集、削除できます。すべてのロールおよびそれらの個々の権限のリストを表示することもできます。

実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	事前構成済みのロールを表示します。	ステップ1. 事前構成されたNetWitness Platformロールの確認
管理者	新しいロールの作成	ステップ2. (オプション) ロールの追加と権限の割り当て

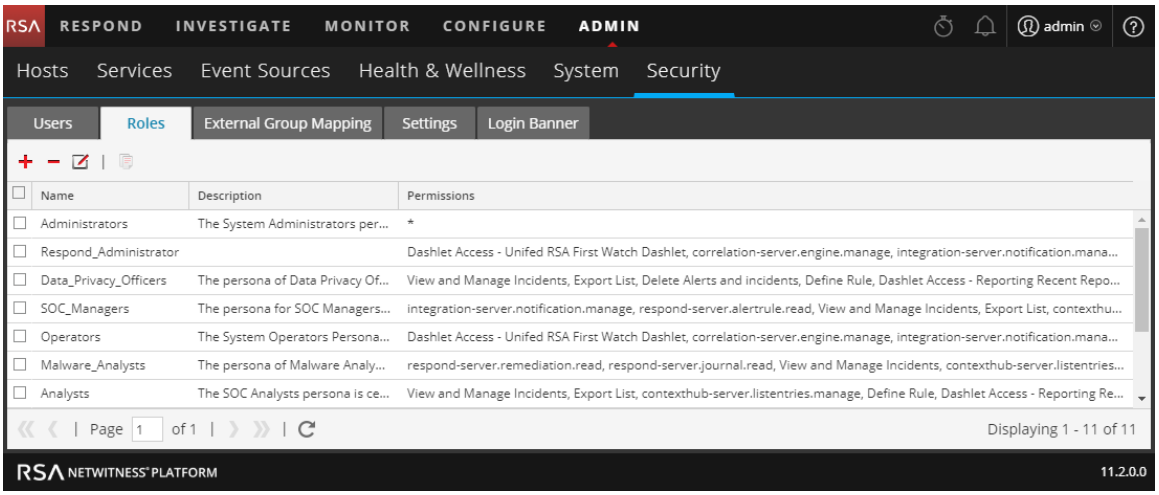
関連トピック

- [ロールの追加]または[ロールの編集]ダイアログ

簡単な説明

このビューにアクセスするには、次の手順を実行します。

1. **[管理]>[セキュリティ]**に移動します。
   [セキュリティ]ビューが開き、デフォルトで[**ユーザ**]タブが表示されます。
2. [**ロール**]タブをクリックします。



[ロール]タブには[ロール]リストが表示され、上部にはツールバーがあります。

次の表は、ツールバーの機能について説明しています。

機 能	説 明
	[ロールの追 加]ダイアログを表 示します。
	[ロールの編 集]ダイアログを表 示します。
	ロールを削 除します。確 認 のダイアログが表 示されます。
	ロールを複 製し、別 の名 前 で保 存します。

次 の表 は、ロールのリストについての説 明 です。

列	説 明
名 前	ユーザに付 与 できるロールの名 前 を表 示します。
説 明	ロールの説 明 を表 示します。
権 限	ロールに割 り当 てられている権 限 を表 示します。

[ロールの追加]または[ロールの編集]ダイアログ

このトピックでは、[**管理**]>[**セキュリティ**]**ビュー**>[**ロール**]タブからアクセスできる、[ロールの追加]および[ロールの編集]ダイアログについて説明します。

[ロールの追加]ダイアログおよび[ロールの編集]ダイアログでは、ロールを追加したり、ロールに割り当てられた権限を編集することができます。ロールのメンバーに対してクエリ処理属性を指定して、メンバーが取得できる情報を制限することもできます。これらのダイアログの構造は同じです。唯一の違いは、新しいロールを追加するか、既存のロールを変更するかです。

ロールの権限を変更すると、ロールの保存後ただちに、そのロールに割り当てられているユーザに適用されます。

実行したいことは何ですか?

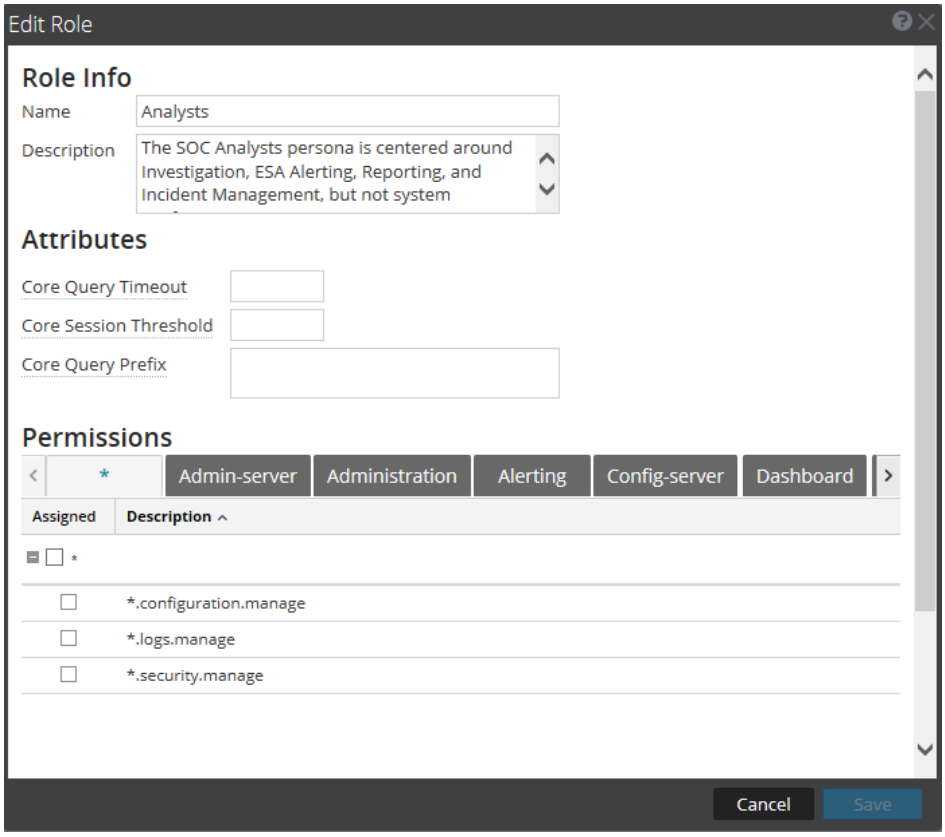
ロール	実行したいこと	手順
管理者	事前構成済みのロールを表示します。	ステップ1. 事前構成されたNetWitness Platformロールの確認
管理者	新しいロールの作成	ステップ2. (オプション) ロールの追加と権限の割り当て
管理者	ルールの編集	ステップ2. (オプション) ロールの追加と権限の割り当て
管理者	ロールの削除	ステップ2. (オプション) ロールの追加と権限の割り当て

簡単な説明

このビューにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[**管理**]>[**セキュリティ**]に移動します。
   [セキュリティ]ビューが開き、デフォルトで[**ユーザ**]タブが表示されます。
2. [**ロール**]タブをクリックします。
3. 以下のいずれかの操作を実行します。
   - アクション バーで、  をクリックします。
     [**ロールの追加**]ダイアログが表示されます。

- ロールを選 択し、アクション バーで をクリックします。
  [**ロールの編 集**]ダイアログが表 示されます。



[ロールの追 加]ダイアログと[ロールの編 集]ダイアログには、それぞれ [**ロール情 報**]、[**属 性**]、[**権 限**]の3つのセクションがあります。

ロール情 報

次 の表 は[**ロール情 報**]セクションの情 報 です。

機 能	説 明
名 前	ユーザ ロールの名 前 。
説 明	ユーザ ロールに関 する説 明 。オプションです。

属 性

次 の表 は[**属 性**]セクションの情 報について説 明しています。詳 細は、ステップ3. ロールごとのクエリおよびセッションの属 性 の検 証を参 照してください。

機能	説明
Coreクエリタイムアウト	(オプション) ユーザがクエリを実行できる最長時間(分)を指定します。デフォルト値は5分です。このタイムアウトは、Investigationから実行されるクエリにのみ適用されます。この値を設定する場合は、ゼロ(0)以上にする必要があります。ゼロを指定するとタイムアウトしません。
Coreセッション閾値	サービスがメタ値をスキャンする時にセッションをカウントする方法を制御します。この値はゼロ(0)以上にする必要があります。この閾値がゼロより大きい場合は、セッション カウントが閾値を超えると、クエリの最適化により、セッション カウントの合計を推定します。クエリが返したメタ値が閾値に達すると、システムでは以下の動作が行われます。 • セッションのカウントを停止する • 閾値と、閾値に達するまでに要したクエリ時間の割合を表示する デフォルト値は`100000`です。ここで指定した制限は、調査の表示設定で定義された**最大セッション エクスポート**値よりも優先されます。
Coreクエリプレフィックス	(オプション) クエリ結果をフィルタして、ロール メンバーに表示される情報を制限します。デフォルトでは、空白です。たとえば、クエリプレフィックスに`'service' = 80`を指定した場合、ユーザが実行するクエリの先頭にこの条件が付加され、ユーザは、HTTPセッションのメタにしかアクセスできなくなります。

権限

次の表は[**権限**]セクションの情報について説明しています。権限については、「ロールの権限」を参照してください。

機能	説明
[**モジュール**]タブ	各モジュールに1個ずつ、合計15個のデフォルト タブがあります(管理、Admin-server、アラート、Config-server、インシデント、調査、Investigation-server、Integration-server、Live、マルウェア、Orchestration-server、レポート、Response-server、Security-server、ダッシュボード)。インストール状況によっては、追加のタブが表示される場合があります。それぞれのタブにモジュールの権限が一覧表示されます。
[**説明**]列	モジュールのすべての権限のリスト。
[**割り当て済み**]列	モジュールの権限がロールに割り当てられていることを示すチェックボックスがあります。
保存	選択した権限を割り当てた状態でロールを保存します。
キャンセル	設定をキャンセルして、ダイアログを閉じます。

[ログイン バナー]タブ

[ログイン バナー]タブでは、NetWitness Platformログイン画 面 にバナーを追 加 できます。これにより、ユーザは条 件 に同 意 するまでログ オンできなくなります。複 数 のNetWitness Serverを導 入 している場 合 は、[サーバ タイトル プレフィックス]を追 加 すると、現 在 のタブのNetWitness Serverを識 別 できるようになります。ログイン バナーのデフォルト のタイトルとテキストをカスタマイズできます。バナーは、デフォルト では無 効 化 されています。

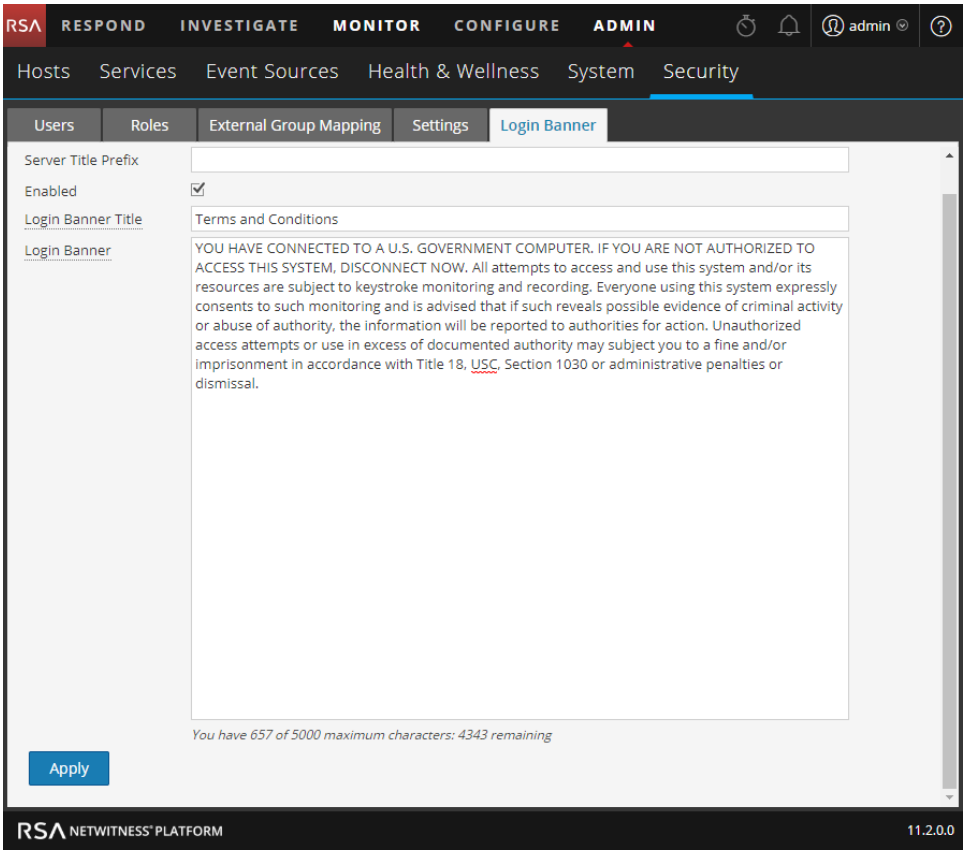
実 行 したいことは何 ですか?

ロール	実 行 したいこと	手 順
管 理 者	ログイン バナーの作 成 または有 効 化	ステップ5. (オプション) カスタム ログイン バナーの作 成

簡 単 な説 明

[ログイン バナー]タブにアクセスするには、次 の手 順 を実 行 します。

1. **[管 理]>[セキュリティ]**に移 動 します。
   [セキュリティ]ビューが開き、デフォルト で[**ユーザ**]タブが表 示 されます。
2. [**ログイン バナー**]タブをクリックします。



バナーを有効化すると、ログイン画面に表示されます。

次の表に、[ログイン バナー]タブの機能を示します。

機能	説明
サーバ タイトル プレフィックス	タイトル バーにNetWitness Serverのプレフィックスを表示します。
有効	ログイン バナーが有効化されているかどうかを示すチェックボックス。このボックスはデフォルトでオフに設定されています。
ログイン バナー タイトル	ログイン条件を表示するダイアログ ボックスのタイトルを示します。
ログイン バナー	ユーザが同意しなければならない条件を示します。

[外 部 グループ マッピング]タブ

外 部 ユーザの認 証を設 定した場 合 、ユーザ ロールを外 部 グループに割り当 てることができます。[外 部 グループ マッピング]タブには、ロールを割り当 てた各 外 部 グループに関 する情 報 が表 示されます。

実 行したいことは何 ですか?

ロール	実 行したいこと	手 順
管 理 者	外 部 グループへのロールの割り当 て	ステップ5. (オプション) 外 部 グループへのユーザ ロールの割り当 て
管 理 者	外 部 グループの検 索	外 部 グループの検 索

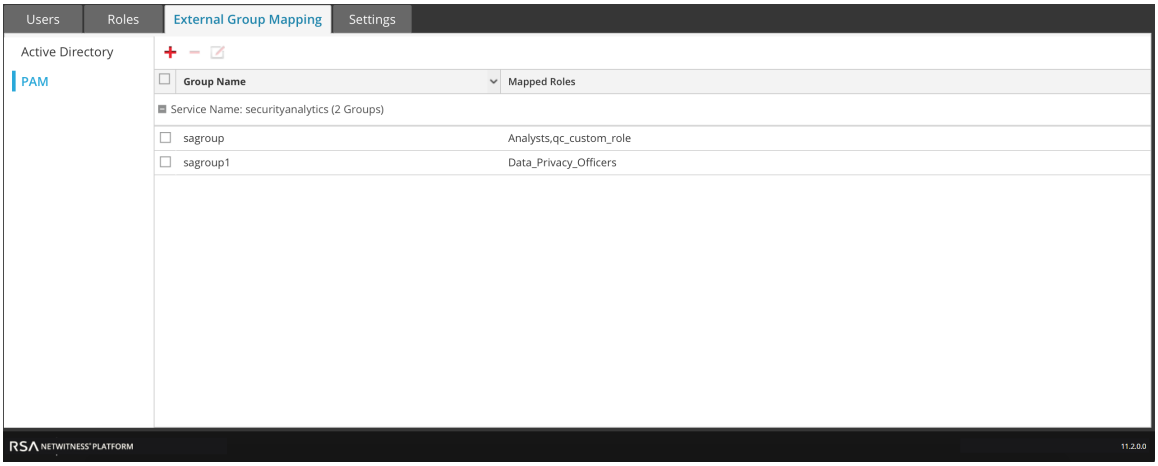
関 連トピック

- [ロール マッピングの追 加]ダイアログ
- [外 部 グループの検 索]ダイアログ

簡 単な説 明

このビューにアクセスするには、次 の手 順を実 行します。

1. NetWitness Platformで、**[管 理]＞[セキュリティ]**に移 動します。
   [セキュリティ]ビューが表 示され、[**ユーザ**]タブが開きます。
2. [**外 部 グループ マッピング**]タブをクリックします。



[外 部 グループ マッピング]タブはツールバーとリストで構 成されています。

リストには次 の機 能 があります。

機能	説明
グループ タイプ	左側の列で[**Active Directory**]または[**PAM**]のいずれかをクリックすると、選択したタイプのグループが表示されます。
選択ボックス	各行のグループを選択します。タイトル バーの選択ボックスは、すべてのグループを選択します。
グループ名	NetWitness Platformにアクセスできる外部グループの名前が表示されます。
マップされたロール	外部グループに割り当てられているNetWitness Platformのロールが表示されます。

ツールバーには次の機能があります。

機能	説明
	[ロール マッピングの追加]ダイアログが表示されます。このダイアログでは、外部グループを選択してのロールに割り当てることができます。
	警告メッセージが表示され、外部グループに割り当てられているNetWitness Platformのすべてのロールを削除するかどうかの確認を求められます。
	[ロール マッピングの編集]ダイアログが表示されます。このダイアログでは、NetWitness Platformのロールを外部グループに追加したり、削除することができます。

[ロール マッピングの追 加]ダイアログ

このトピックでは、[管 理]＞[セキュリティ]＞[外 部 グループ マッピング]タブ＞[ロール マッピングの追 加]ダイアログの機 能 について説 明します。

NetWitness Platformでは、各 ユーザー ロールに権 限 が関 連づけられます。1つ以 上 のロールを外 部 グループにマッピングして、各 ロールと同じ権 限 セットをそのグループに付 与 することができます。

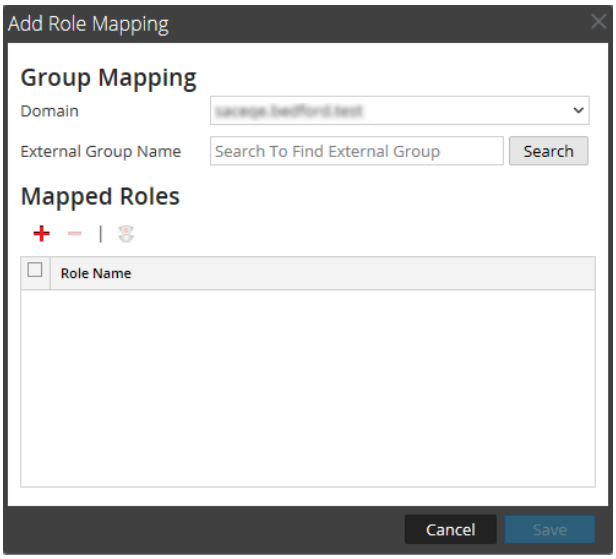
実 行したいことは何 ですか?

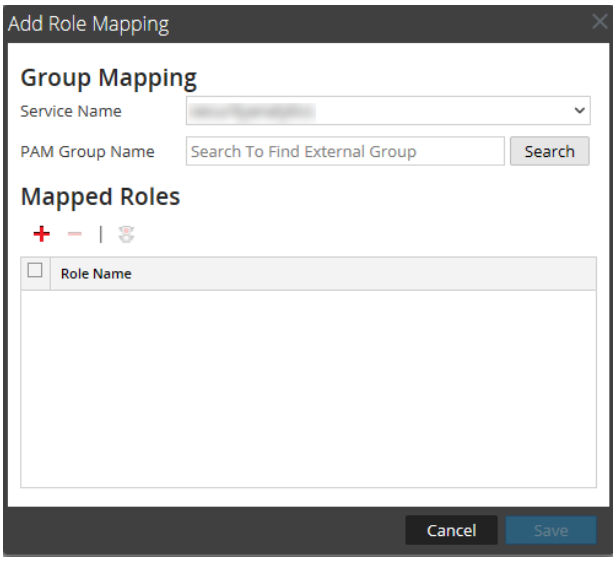
ロール	実 行したいこと	手 順
管 理 者	外 部 グループへのロールの割り当 て	ステップ5. (オプション) 外 部 グループへのユーザ ロールの割り当 て
管 理 者	外 部 グループの検 索	外 部 グループの検 索

簡 単な説 明

このダイアログにアクセスするには、次 の手 順 を実 行します。

1. NetWitness Platformで、**[管 理]＞[セキュリティ]**に移 動します。
2. [**外 部 グループ マッピング**]タブをクリックします。
3. ツールバーで＋をクリックします。
   設 定した外 部 認 証 方 法 に対 応した[ロール マッピングの追 加]ダイアログが表 示されます。





[ロール マッピングの追 加]ダイアログと[ロール マッピングの編 集]ダイアログはほぼ同 一 です。唯 一 の違いは、[ロール マッピングの編 集]ダイアログでは検 索 が実 行 できません。

グループ マッピング

[**グループ マッピング**]セクションには次 の機 能 があります。

機 能	説 明
ドメイン	Active Directoryを外 部 ユーザの認 証 用 に設 定 している場 合 に表 示 されます。ロールをマッピングする外 部 のActive Directoryグループのドメイン名 です。
外 部 グループ名	Active Directoryを外 部 ユーザの認 証 用 に設 定 している場 合 に表 示 されます。ロールをマッピングする外 部 グループです。

機 能	説 明
PAMグループ名	PAMを外 部ユーザの認 証 用に構 成している場 合に表 示されます。ロールをマッピングする外 部グループの名 前です。
検 索	検 索 用のダイアログが表 示され、外 部グループを検 索できます。検 索機 能は[ロール マッピングの編 集]ダイアログでは使 用できません。

マップされたロール

[**マップされたロール**]セクションには次の機 能があります。

機 能	説 明
+	[ロールの追 加]ダイアログが表 示され、追 加できる構 成 済みのNetWitness Platformユーザー ロールが一 覧 表 示されます。
−	選 択したロールを[マップされたロール]グリッド から削 除します。
名 前	NetWitness Platformユーザ ロールの名 前が表 示されます。
権 限	NetWitness Platformユーザ ロールに関 連づけられている権 限が表 示されます。
キャンセル	新 規のグループ マッピングまたはグループ マッピングの変 更をキャンセルして、ダイアログを閉じます。
保 存	新 規のグループ マッピングまたはグループ マッピングの変 更を保 存して、ダイアログを閉じます。

[外部グループの検索]ダイアログ

このトピックでは、[管理]>[セキュリティ]ビュー>[外部グループ マッピング]タブの[外部グループの検索]ダイアログの機能について説明します。

ユーザの外部認証を設定した場合、NetWitness Platformユーザ ロールを外部グループにマッピングすることができます。外部グループを検索して、NetWitness Platformロールをマッピングするグループを選択します。

実行したいことは何ですか?

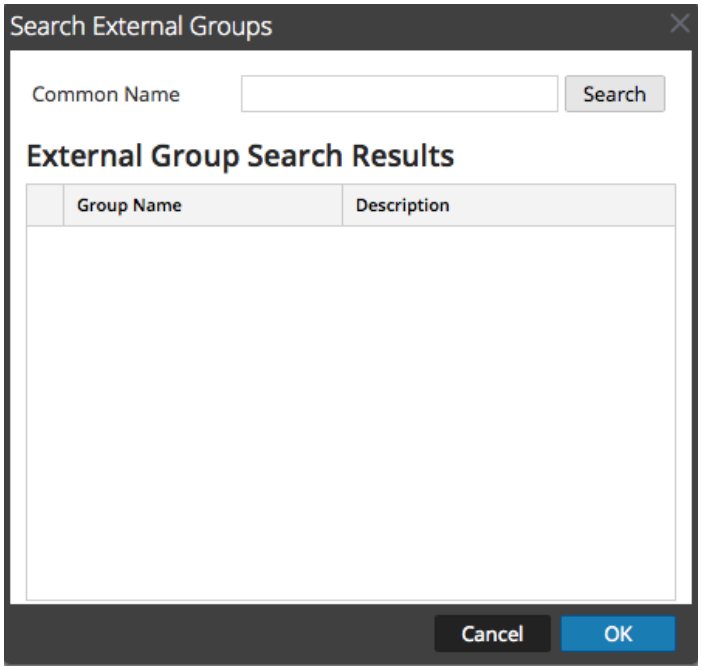
ロール	実行したいこと	手順
管理者	外部グループへのロールの割り当て	ステップ5. (オプション) 外部グループへのユーザ ロールの割り当て
管理者	外部グループ マッピングの表示	[外部グループ マッピング]タブ
管理者	外部グループの検索	外部グループの検索

簡単な説明

このダイアログにアクセスするには、次の手順を実行します。

1. **[管理]>[セキュリティ]**に移動します。
   [セキュリティ]ビューが表示され、[**ユーザ**]タブが開きます。
2. [**外部グループ マッピング**]タブをクリックします。
3. ツールバーで+をクリックします。
   設定した外部認証方法に対応した[ロール マッピングの追加]ダイアログが表示されます。
4. [グループ マッピング]セクションで、[**ドメイン**]を選択します。

5. [グループ マッピング] セクションで、[**検索**] をクリックします。
   [**外部グループの検索**] ダイアログが表示されます。



次の表は、[外部グループの検索] ダイアログの機能について説明しています。

機能	説明
共通名	検索するグループ名。正確な名前のほか、ワイルド カード文字 (*) を使用できます。
グループ名	ロールをマッピングする外部グループ。
説明	グループに関するオプションのテキスト。
OK	選択した外部グループが追加された [ロール マッピングの追加] ダイアログが表示されます。
キャンセル	ダイアログを閉じます。

[設定]タブ

このトピックでは、[管理]>[セキュリティ]ビュー>[設定]タブについて説明します。[設定]タブでは、NetWitness Platformの内部ユーザ向けのパスワードの複雑性の要件とシステム全体のセキュリティ パラメータを構成します。

NetWitness Platformセキュリティの構成の詳細については、「システム セキュリティの設定」を参照してください。

パスワードの複雑性の要件は、内部ユーザのみに適用され、外部ユーザには強制されません。外部ユーザは、外部認証システムの方法とシステムによってパスワードの複雑性が管理されます。

実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	パスワードの複雑性の構成	ステップ1. パスワードの複雑性の構成
管理者	システム レベルのセキュリティ設定の構成	ステップ3. システム レベルのセキュリティ設定の構成
管理者	(オプション) 外部認証の構成	ステップ4. (オプション) 外部認証の構成

関連トピック

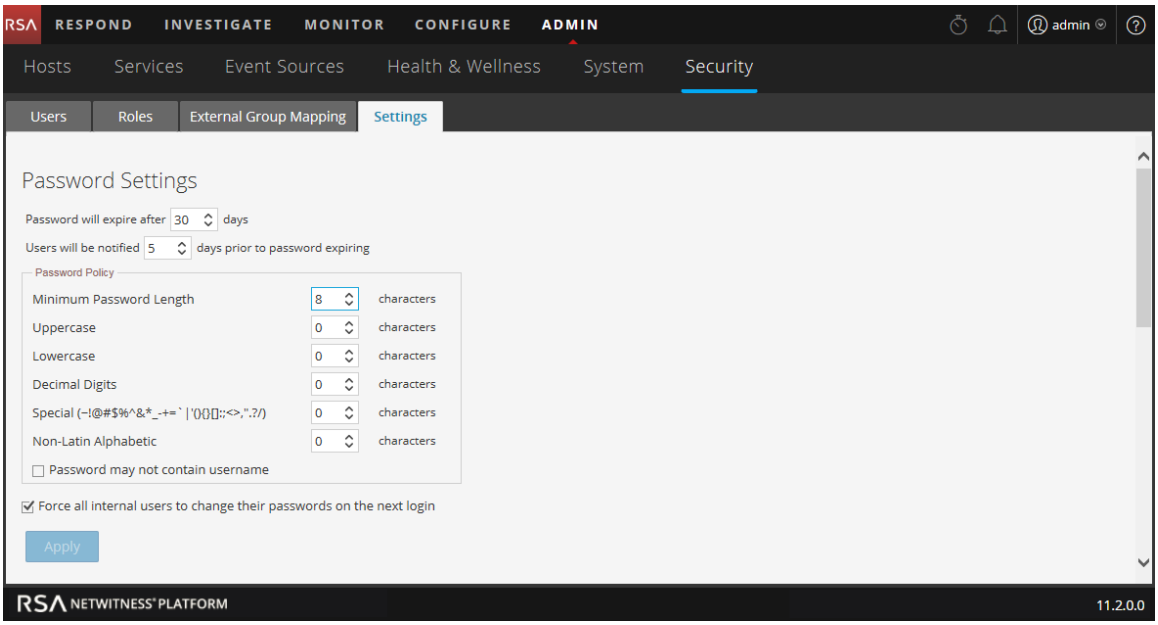
- システム セキュリティの設定

簡単な説明

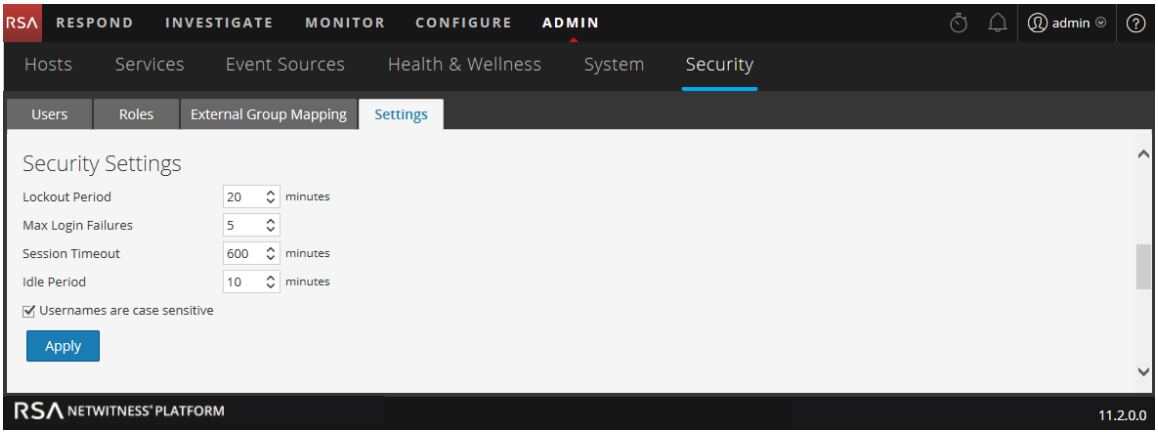
[設定]タブにアクセスするには、次の手順を実行します。

1. **[管理]>[セキュリティ]**に移動します。
   [セキュリティ]ビューが表示され、[**ユーザ**]タブが開きます。
2. [**設定**]タブをクリックします。

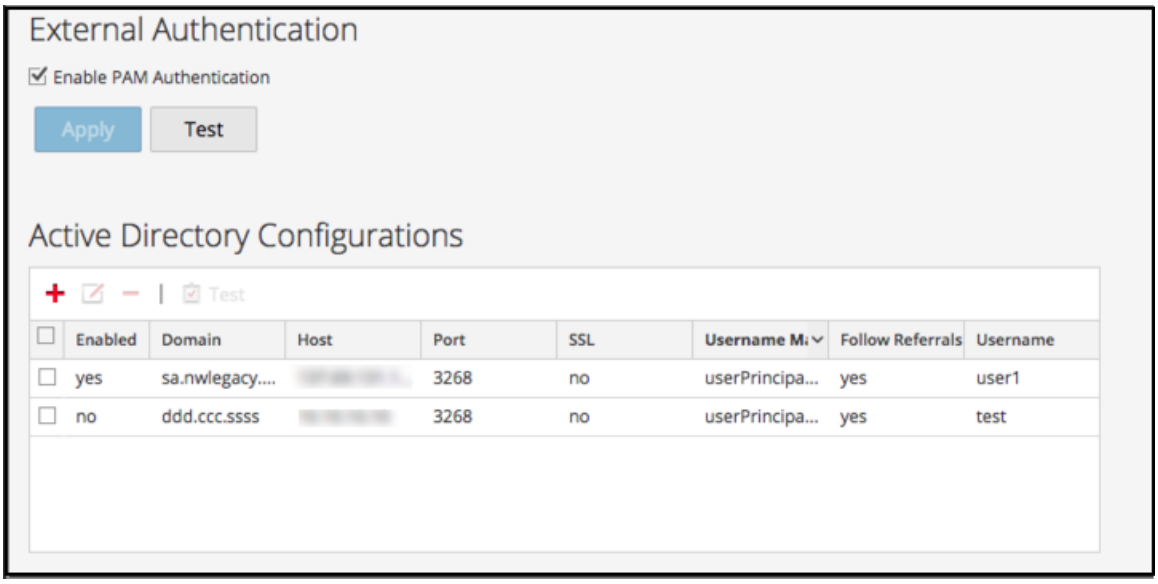
次の図は、[設定]タブの[パスワード設定]セクションを示します。



次の図は、[設定]タブの[セキュリティ設定]セクションを示します。



次の図は、[設定]タブの[PAM認証]セクションと[Active Directory構成]セクションを示しています。



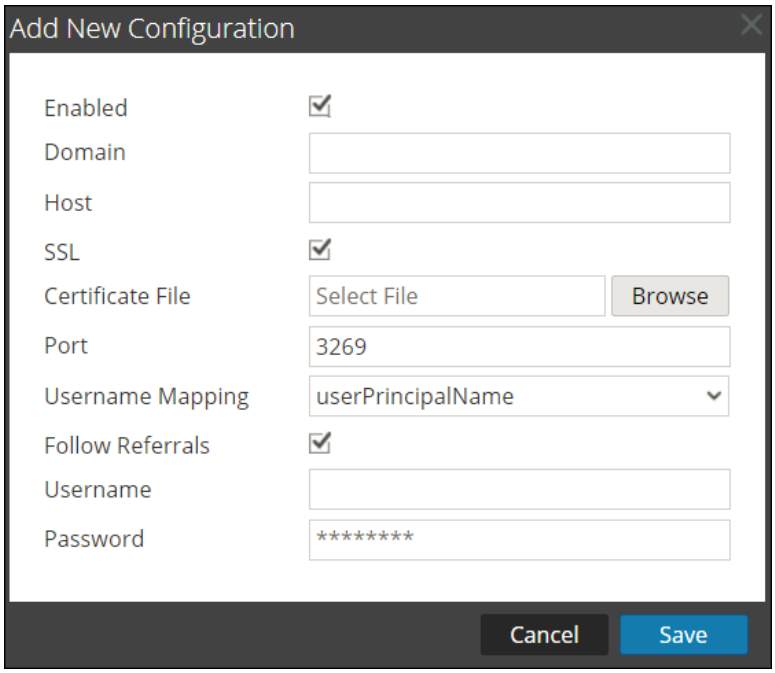
パスワード設 定

[パスワード ポリシー] セクションでは、NetWitness Platformの内 部ユーザがパスワードを設 定する際に満たす必 要のあるパスワードの複 雑 性の要 件を構 成できます。

オプション	説 明
パスワードの有 効 期 限 : <n> 日	NetWitness Platform内 部ユーザのデフォルトのパスワード有 効 期 間の日 数。値にゼロ(0) を指 定すると、パスワードの有 効 期 限が無 効 化されます。新 規インストールの場 合 、デフォルト値 は30です。アップグレードの場 合 、既 存の値が自 動 的に維 持されます。
ユーザに通 知 : <n>日 前	パスワードの有 効 期 限の何 日 前になったら、ユーザにまもなくパスワードの有 効 期 限が切れることを通 知するか。ユーザは、パスワードの有 効 期 限が切れる前の指 定された日 付に、1回 限りの通 知メールを受 け取ります。また、NetWitness Platformへのログオン時には、パスワード有 効 期 限 切 れメッセージ ダイアログも表 示されます。最 小 値 は1日 です。
最 小 パスワード長	NetWitness Platformユーザ パスワードの最 低 限 必 要な長さを指 定します。最 小 パスワード長を設 定すると、ユーザが、推 測が容 易な短いパスワードを設 定するのを防ぐことができます。
大 文 字	パスワードに含 める大 文 字の最 小 数を指 定します。これにはAからZ(ダイアクリティカルマーク付きを含む) 、ギリシャ文 字 、キリル文 字が含まれます。例 : • キリル文 字の大 文 字 : Д Ц • ギリシャ文 字の大 文 字 : Π Λ
小 文 字	パスワードに含 める小 文 字の最 小 数を指 定します。これにはaからz(ダイアクリティカルマーク付きを含む) 、ギリシャ文 字 、キリル文 字が含まれます。例 : • キリル文 字の小 文 字 : д ц • ギリシャ文 字の小 文 字 : π λ

オプション	説 明
数 字	パスワードに使 用する数 字(0～9) の最 小 数を指 定します。
特 殊 文 字 (~!@#$%^&*_ -+=`|'(){} []:;<>,".?/)	パスワードに使 用する特 殊 文 字の最 小 数を指 定します。次の特 殊 文 字を使 用できます。 ~!@#$%^&*_-+=`|'(){}[]:;<>,".?/
非ラテン アル ファベット 文 字	大 文 字 小 文 字 以 外のUnicode文 字の最 小 数を指 定します。これにはアジア言 語のUnicode文 字を含みます。例 : • 漢 字(日 本 語) : 頁(leaf) 枒(tree)
パスワードに ユーザ名 を含 めることを禁 止	パスワードにユーザのユーザ名 (大 文 字と小 文 字を区 別しない) を含むことを禁 止します。
すべての内 部 ユーザに次 回 ログイン時 にパ スワード の変 更を強 制	すべての内 部ユーザに対して、パスワード の作 成時 または変 更時ではなく、次 回NetWitness Platformにログオンするときにパスワード の変 更を要 求します。この設 定がデフォルト でオンになっていることに注 意してください。
適 用	パスワード の強 度 設 定は、NetWitness Platformユーザが自 分のパスワードを作 成 または変 更するときに有 効となります。[**すべての内 部ユーザに次 回ログイン時 にパスワード の変 更を強 制**]を選 択した場 合、すべての内 部ユーザは次 回NetWitness Platformログイン時 にパスワードを変 更する必 要があります。

次の図は、[設 定]タブの[Active Directory構 成]セクションにある[新しい構 成の追 加]ダイアログを示しています。



セキュリティ設定

[セキュリティ設定]セクションでは、NetWitness Platformユーザのグローバル セキュリティ設定を構成できます。

オプション	説明
ロックアウト期間	ユーザが最大ログイン失敗回数を超過した後、NetWitness Platformからロック アウトされる期間(分)。デフォルト値は20分です。
最大ログイン失敗回数	ユーザがログインを失敗できる最大回数。ユーザは、ここで指定した回数ログインに失敗するとロックアウトされます。デフォルト値は5です。
セッション タイムアウト	タイムアウトするまでに許可されるユーザ セッションの最長期間(分単位)。デフォルト値は600です。この値が0の場合、セッションの最長期間は設定されません。この値を設定すると、指定した期間が経過した後、セッションがタイムアウトします。ユーザは再度ログインする必要があります。
アイドル期間	セッションがタイムアウトするまでのアイドル状態の期間(分)。デフォルト値は10です。値が0の場合、セッションはタイムアウトしません。
ユーザ名は大文字と小文字が区別されます	NetWitness Platformログイン画面のユーザ名フィールドで大文字と小文字を区別する場合は、このオプションを選択します。たとえば、ユーザ名が大文字と小文字を区別する場合、NetWitness Platformへのログオンにadminを使用することはできますが、Adminを使用することはできません。これは必須フィールドです。
パスワード	Active Directoryのセキュリティ設定を追加または編集する場合は、パスワードを入力します。これは必須フィールドです。
適用	設定がすぐに反映されます。

PAM認証

[PAM認証]セクションでは、NetWitness Platformが外部ユーザを認証する方法としてPAMを構成し、ログインのテストを実施することができます。

オプション	説明
PAM認証の有効化	NetWitness Platformが外部ユーザのログオンの認証にPAM(Pluggable Authentication Modules) を使用できるようになります。
適用	PAM構成設定が保存され、次回のログオン時から設定が有効になります。
テスト	ユーザ名とパスワードのプロンプトを表示した後、現在有効なPAM認証方法をテストします。

Active Directory構成

[Active Directory構成]セクションでは、NetWitness Platformが外部ユーザをログイン時に認証する方法としてActive Directoryを構成します。

オプション	説 明
有 効	NetWitness Platformユーザのの Active Directoryによる認 証を有 効にします。
ドメイン	Active Directoryサービスのドメイン名 。
ホスト	Active Directoryサービスを実 行 するホストの名 前またはIPアドレス。
ポート	Active Directoryサービスを実 行 するホストのポート 。
SSL	Active Directoryサービスが SSL(Secure Sockets Layer) を使 用 するかどうかを示 します。SSLを有 効にして、Active Directoryサービスと NetWitness Platformの バージョン11.1以 降 が通 信 するには、Active Directoryのサーバ証 明 書をアップ ロードする必 要 があります。
ユーザ名 マッピング	ユーザ名 をマッピングするActive Directoryのフィールドを指 定します。UPN (userPrincipalName) またはsAMAccountNameを指 定 できます。
リフェラルのフォ ロー	Active Directoryによって作 成されたLDAPリフェラルをがフォローするかどうかを指 定します。
ユーザ名	ユーザ名 を指 定した場 合 、Active Directoryグループを検 索するときに、指 定さ れたユーザ名 でActive Directoryサービスにバインドします。この認 証 情 報は他 の 用 途には使 用されません。