TENABLE.OT

ユーザーガイド

バージョン 3.15

改訂履歴

製品バージョン: Tenable.ot 3.15

ドキュメント改訂履歴:

ドキュメント改訂	日付	説明
1.0	2018 年 10 月 8 日	バージョン 2.5 用ユーザーガイドの最初のバージョンを作成
1.1	2019 年 1 月 28 日	バージョン 2.7 用に更新
1.2	2019 年 8 月 20 日	バージョン 3.1 用に更新
1.3	2019 年 10 月 10 日	現在サポートされている機能に合わせて改訂
1.4	2019 年 1 月 12 日	バージョン 3.3 用に更新
1.5	2020 年 3 月 24 日	バージョン 3.4 用に更新
1.6	2020 年 4 月 6 日	バージョン 3.5 用に更新
1.7	2020 年 4 月 27 日	センサーのドキュメントを追加
1.8	2020 年 6 月 3 日	バージョン 3.6 用に更新
1.9	2020 年 8 月 8 日	バージョン 3.7 用に更新
2.0	2020 年 10 月 11 日	バージョン 3.8 用に更新
2.1	2020 年 12 月 2 日	バージョン 3.9 用に更新
2.2	2021 年 4 月 6 日	バージョン 3.10 用に更新
2.3	2021 年 6 月 30 日	バージョン 3.11 用に更新
2.4	2021 年 12 月 12 日	バージョン 3.12 用に更新
2.5	2022 年 3 月 25 日	バージョン 3.13 用に更新
2.6	2022 年 8 月 22 日	バージョン 3.14 用に更新
2.7	2022 年 9 月 25 日	SAML 統合を追加 (SP1)
2.8	2023 年 1 月 31 日	バージョン 3.15 用に更新

目次

はじめに

Tenable.ot は、サイバー脅威、悪意のある内部関係者、人為的なミスから産業用ネットワークを保護します。脅威の検出と緩和から資産追跡、脆弱性管理、構成管理、アクティブクエリチェックまで、Tenable.ot の ICS セキュリティ機能は、運用環境の可視性、セキュリティ、管理を最大化します。

Tenable.ot は、IT セキュリティ担当者および OT エンジニア向けに、包括的なセキュリティツールおよびレポートを提供しています。これは、コンバージド IT/OT セグメントと ICS アクティビティに対する比類のない可視性を提供し、すべてのサイトとそれぞれの OT 資産 (Windows Servers から PLC バックプレーンまで) にわたって、一元的に非常に明確な状況認識を提供します。

Tenable.ot には、以下の主要な機能があります。

- **360 度の可視性** - 攻撃は IT/OT インフラで容易に伝播する可能性があります。単一のプラットフォームで OT と IT システム全体のサイバーリスクを管理し測定することで、コンバージドアタックサーフェスを完全に可視化できます。Tenable.ot は、セキュリティ情報およびイベント管理 (SIEM) ソリューション、ログ管理ツール、次世代ファイヤーウォール、チケットシステムなどの主要な IT セキュリティおよび運用ツールともネイティブに統合できます。これにより、信頼のエコシステムが構築され、すべてのセキュリティ製品が一体となり、環境の安全を維持できます。
- **脅威の検出と緩和** - Tenable.ot は、マルチ検出エンジンを利用して、OT 操作に影響を与える可能性のある高リスクのイベントと動作を検出します。これらのエンジンには、ポリシー、動作、署名ベースの検出が含まれます。
- **資産インベントリとアクティブ検出** - 特許取得の画期的なテクノロジーを利用する Tenable.ot は、ネットワークレベルだけでなく、デバイスレベルまで、インフラの比類のない可視性を提供します。ネットワークで発生するすべてのアクティビティとアクションを特定するために、ネイティブ通信プロトコルを使用して、ICS 環境の IT デバイスと OT デバイスの両方にアクティブにクエリを行います。
- **リスクベースの脆弱性管理** - 包括的かつ詳細な IT/OT 資産追跡機能を利用する Tenable.ot は、ICS ネットワークの各資産に対して予測に基づいた優先順位付けを使用して、脆弱性とリスクのレベルを生成します。これらのレポートには、リスクスコアと詳細なインサイトが、緩和策の提案とともに含まれています。
- **構成管理** - Tenable.ot は、特定のラダーロジックセグメント、診断バッファ、タグテーブルなどを含む、時間の経過に伴うデバイス構成変更の完全な詳細履歴を提供します。これにより、管理者は「最新の既知の良好な状態」でバックアップスナップショットを確立し、より迅速なリカバリと業界規制へのコンプライアンスを実現できます。

Tenable.ot テクノロジー

Tenable.ot の包括的なソリューションは、2 つの主要な収集テクノロジーで構成されています。

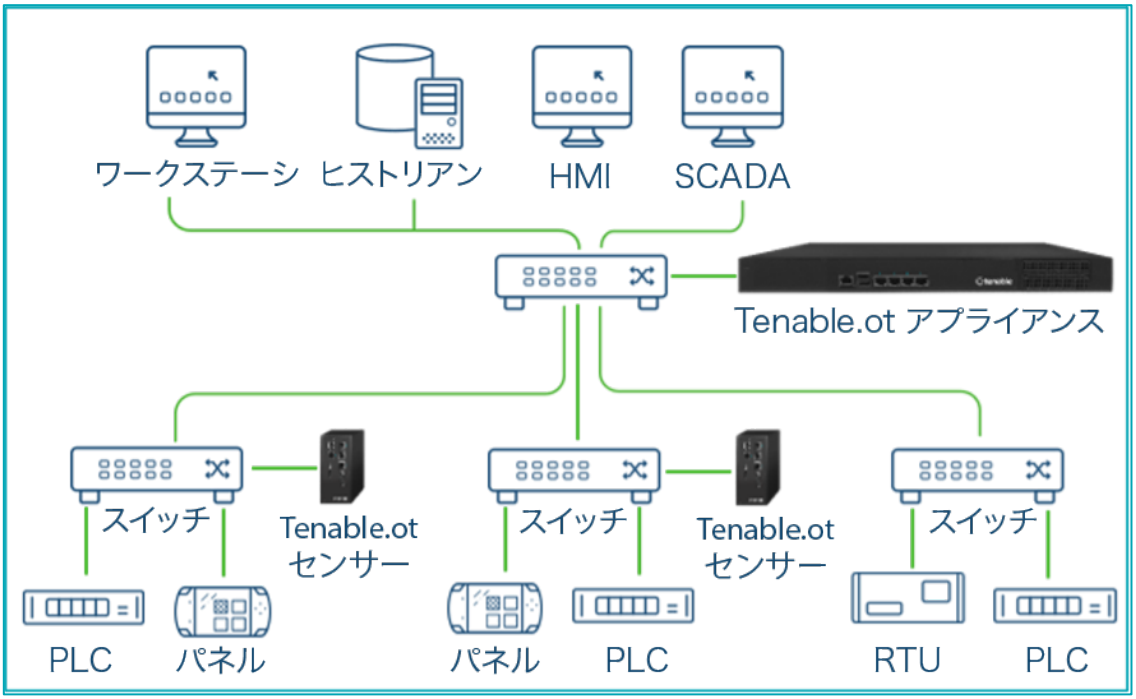
- **ネットワーク検出** - Tenable.ot ネットワーク検出テクノロジーは、産業用制御システム固有の特性と要件に対処するために特別に設計されたパッシブディープパケット検査エンジンです。ネットワーク検出は、エンジニアリングアクティビティに独自の焦点を合わせて、運用ネットワークで実行されたすべてのアクティビティを詳細かつリアルタイムで可視化します。これには、ファームウェアのダウンロード/アップロード、コードの更新、ベンダー独自の通信プロトコルで実行される構成変更が含まれます。ネットワーク検出は、疑わしいまたは認証されていないアクティビティをリアルタイムで警告し、証拠となるデータを含む包括的なイベントログを生成します。ネットワーク検出は、3 種類のアラートを生成します。
    - **ポリシーベース** - 事前定義されたポリシーをアクティブ化するか、カスタムポリシーを作成してサイバー脅威または操作上のミスを示す特定の詳細なアクティビティをホワイトリストまたはブラックリストに追加し、アラートをトリガーできます。ポリシーを設定して、事前定義された状態に関してアクティブクエリチェックをトリガーすることもできます。
    - **動作異常** - システムは、ネットワークトラフィックベースラインからの逸脱を検出します。このベースラインは、指定された時間範囲のトラフィックパターンに基づいて確立されます。また、マルウェアや偵察の挙動を示す疑わしいスキャンも検出します。
    - **署名検出ポリシー** - これらのポリシーは、署名ベースの OT/IT 脅威検出を使用して、侵入の脅威を示すネットワークトラフィックを識別します。検出は、Suricata の脅威エンジンでカタログ化されたルールに基づいています。
- **アクティブクエリ -** Tenable.ot の特許取得済みクエリ技術は、ICS ネットワークの制御デバイスのメタデータを定期的に調査することで、ネットワーク上にあるデバイスを監視します。この機能は、PLC や RTU などの低レベルのデバイスを含むすべての ICS 資産を、それらの資産がネットワークでアクティブでないときでも、自動的に検出して分類する Tenable.ot の能力を強化します。また、デバイスのメタデータ (ファームウェアバージョン、構成の詳細、状態など) にローカルで実装された変更や、デバイスロジックの各コード/機能ブロックの変更も識別されます。ネイティブコントローラー通信プロトコルで読み取り専用クエリを使用するため、完全に安全で、デバイスに影響を与えません。クエリは、事前定義されたスケジュールに基づいて定期的に実行することも、ユーザーがオンデマンドで実行することもできます。

ソリューションアーキテクチャ

Tenable.ot プラットフォームコンポーネント

Tenable.ot ソリューションは 2 つのコンポーネントで構成されています。

- **Tenable.ot アプライアンス** - このコンポーネントは、ネットワークから(スパンポートまたはネットワークタップを介して)直接、および/または Tenable.ot センサーからのデータフィードを使用して、ネットワークトラフィックを収集して分析します。Tenable.ot アプライアンスは、ネットワーク検出機能とアクティブクエリ機能の両方を実行します。
- **Tenable.ot センサー** - 対象のネットワークセグメントに展開できる小さなデバイス(管理対象スイッチごとに最大 1 つのセンサー)です。センサーは、小型ラックマウントまたは DIN レールマウントの 2 つのフォームファクターで利用可能です。Tenable.ot センサーは、すべてのトラフィックをキャプチャして分析し、情報を Tenable.ot アプライアンスに伝達することで、これらのネットワークセグメントを完全に可視化します。バージョン 3.14 以降のセンサーは、それらのセンサーが展開されているネットワークセグメントにアクティブクエリを送信するよう構成することもできます。



Tenable.ot アプライアンスと Tenable.ot センサーのネットワーク展開

ネットワークコンポーネント

Tenable.ot は、以下のネットワークコンポーネントとの相互作用をサポートしています。

- **Tenable.ot ユーザー(管理)** - Tenable.ot 管理コンソールへのアクセスを制御するユーザーアカウントが作成されます。管理コンソールは、セキュアソケットレイヤー認証(HTTPS)を介してウェブブラウザ(Google Chrome)でアクセスされます。

> UI は Chrome ブラウザからしかアクセスできません。また、最新バージョンの Chrome を使用している必要があります。

- **Active Directory サーバー** - Active Directory などの LDAP サーバーを使用して、オプションでユーザー認証情報を割り当てることができます。この場合、ユーザー権限は Active Directory で管理されます。
- **SIEM** - Tenable.ot イベントログは、Syslog プロトコルを使用して SIEM に送信できます。
- **SMTP サーバー** - Tenable.ot イベント通知は、SMTP サーバーを介して、特定のグループの従業員に電子メールで送信できます。
- **DNS サーバー** - DNS サーバーを Tenable.ot に統合して、資産名の解決を支援できます。
- **サードパーティアプリケーション** - 外部アプリケーションは、REST API を使用して Tenable.ot とやり取りしたり、他の特定の統合を使用してデータにアクセスしたりできます。[1]

システム要素

資産

資産は、コントローラー、エンジニアリングステーション、サーバーなどのネットワーク内のハードウェアコンポーネントです。Tenable.ot の自動資産検出、分類、管理は、デバイスに対するすべての変更を継続的に追跡することで、正確な資産インベントリを提供します。これにより、運用の継続性、信頼性、安全性を簡単に維持できるようになります。また、メンテナンスプロジェクトの計画、アップグレードの優先順位付け、パッチ展開、インシデント対応、緩和策においても重要な役割を果たします。

リスク評価

Tenable.ot は、洗練されたアルゴリズムを適用して、ネットワーク上の各資産にもたらされるリスクの程度を評価します。ネットワーク内の資産ごとに *リスクスコア*(0 から 100)が付与されます。リスクスコアは、以下の要因に基づいています。

- **イベント** - デバイスに影響を与えるネットワークで発生したイベント(イベントの深刻度とイベントが起きた時期に基づく重み付け)。

> イベントは新しさに従って重み付けされるため、最近のイベントは古いイベントよりもリスクスコアに大きな影響を与えます。

- **脆弱性** - ネットワークの資産に影響を与える CVE、およびネットワークで特定されたその他の脅威(旧式のオペレーティングシステム、脆弱なプロトコルの使用、脆弱なオープンポートなど)。Tenable.ot では、これらは資産のプラグインヒットとして検出されます。
- **資産重大度** - システムが適切に機能するうえでのデバイスの重大さの指標。

> バックプレーンに接続されている PLC の場合、バックプレーンを共有する他のモジュールのリスクスコアが PLC のリスクスコアに影響を与えます。

ポリシーとイベント

ポリシーは、ネットワークで発生する疑わしいイベント、認証されていないイベント、異常なイベント、またはその他の特筆すべき特定のタイプのイベントを定義するために使用されます。特定のポリシーのすべての *ポリシー定義* 条件に一致

---

[1]たとえば、Tenable.ot は Palo Alto Networks 次世代ファイヤーウォール (NGFW) および Aruba ClearPass との統合をサポートしており、Tenable.ot はこれらのシステムと資産インベントリ情報を共有できます。Tenable.ot は、Tenable.io や Tenable.sc などの他の Tenable プラットフォームと統合することもできます。統合は、**[ローカル設定]** > **[統合]** で構成します。**ローカル設定**を参照してください。

するイベントが発生すると、システムでイベントが生成されます。イベントがシステムに記録され、ポリシーに構成された*ポリシーアクション*に従って通知が送信されます。

ポリシーイベントには 2 つのタイプがあります。

- **ポリシーベースの検出** - 一連のイベント記述子で定義されたポリシーの条件が完全に満たされたときにイベントをトリガーします。
- **異常検出** - ネットワークで異常または不審なアクティビティが識別されたときにイベントをトリガーします。

このシステムは、事前定義された一連のポリシーを備えています (標準装備)。さらに、事前定義されたポリシーを編集したり、新しいカスタムポリシーを定義したりする機能も用意されています。

ポリシーベースの検出

ポリシーベースの検出では、システム内のどのイベントがイベント通知をトリガーするかについて、特定の条件を構成します。ポリシーベースのイベントは、ポリシーの条件が完全に満たされた場合にのみトリガーされます。これにより、システムが ICS ネットワークで発生する実際のイベントを警告するとともに、「誰が」、「何を」、「いつ」、「どこで」、「どのように」に関する意味のある詳細情報を提供するので、誤検出をゼロに抑えます。ポリシーは、さまざまなイベントタイプと記述子に基づく場合があります。以下は、可能なポリシー構成の例です。

- **異常または認証されていない ICS コントロールプレーンのアクティビティ (エンジニアリング):** たとえば、HMI はコントローラーのファームウェアバージョンを照会してはならず (偵察を示している可能性があります)、コントローラーは操作時間中にプログラムされるべきではありません (権限のない悪意のあるアクティビティを示している可能性があります)。
- **コントローラーのコードへの変更:** コントローラーロジックへの変更が特定されました (「スナップショットの不一致」)。
- **異常または不正なネットワーク通信:** たとえば、許可されていない通信プロトコルが 2 つのネットワーク資産間で使用されたか、以前に通信したことがない 2 つの資産間で通信が行われました。
- **資産インベントリへの異常または不正な変更:** たとえば、新しい資産が検出されたか、資産がネットワークでの通信を停止しました。
- **資産プロパティの異常または不正な変更:** たとえば、資産のファームウェアまたは状態が変更されました。
- **設定値の異常な書き込み:** 特定のパラメーターに加えられた変更に対してイベントが生成されます。ユーザーは、パラメーターの許容範囲を定義し、その範囲からの逸脱に対してイベントを生成できます。

異常検出

異常検出ポリシーは、「通常」の動作からの逸脱を検出するシステムのビルトイン機能に基づいて、ネットワークの不審な動作を検出します。次の異常検出ポリシーを使用できます。

- **ネットワークトラフィックベースラインからの逸脱:** ユーザーは、指定された時間範囲のトラフィックマップに基づいて「通常」のネットワークトラフィックのベースラインを定義し、ベースラインからの逸脱に対してアラートを生成します。ベースラインはいつでも更新できます。
- **ネットワークトラフィックの急激な上昇:** ネットワークトラフィックの量または会話数の急激な増加が検出されます。
- **潜在的なネットワークの偵察 / サイバー攻撃のアクティビティ:** IP 競合、TCP ポートスキャン、ARP スキャンなど、ネットワークの偵察やサイバー攻撃のアクティビティを示すイベントが生成されます。

ポリシーカテゴリ

ポリシーは次のカテゴリで構成されています。

  - **構成イベントポリシー** - これらのポリシーは、ネットワークで発生するアクティビティに関連しています。構成イベントポリシーには 2 つのサブカテゴリがあります。
  - **コントローラーの検証** - これらのポリシーは、ネットワークのコントローラーで発生する変更に関連しています。対象となるものには、コントローラーの状態の変更や、ファームウェア、資産プロパティ、コードブロックの変更などがあります。ポリシーは、特定のスケジュール(平日のファームウェアアップグレードなど)および / または特定のコントローラーに制限できます。
  - **コントローラーアクティビティ** - これらのポリシーは、コントローラーの状態と構成に影響を与える特定のエンジニアリングコマンドに関連しています。イベントを常に生成する特定のアクティビティの定義や、イベントを生成するための一連の基準の指定が可能です。たとえば、特定のアクティビティが特定の時間や特定のコントローラーで実行された場合などです。資産、アクティビティ、スケジュールのブラックリストとホワイトリストの両方がサポートされています。

- **ネットワークイベントポリシー** - これらのポリシーは、ネットワーク内の資産および資産間の通信ストリームに関連しています。これには、ネットワークに対して追加または削除された資産が含まれます。また、ネットワークの異常なトラフィックパターンや、懸念される特定の原因を挙げるフラグが立てられたトラフィックパターンも含まれます。たとえば、エンジニアリングステーションが、事前に構成された一連のプロトコルの一部ではないプロトコル(特定のベンダーによって製造されたコントローラーが使用するプロトコルなど)を使用してコントローラーと通信する場合、イベントがトリガーされます。これらのポリシーは、特定のスケジュールや特定の資産に制限される可能性があります。ベンダー固有のプロトコルは便宜上ベンダーごとにまとめられていますが、任意のプロトコルをポリシー定義で使用できます。
- **SCADA イベントポリシー** - これらのポリシーは、産業プロセスに害を及ぼす可能性がある設定値の変更を検出します。この種の変更は、サイバー攻撃やヒューマンエラーに起因する場合があります。
- **ネットワーク脅威ポリシー** - これらのポリシーは、署名ベースの OT/IT 脅威検出を使用して、侵入の脅威を示すネットワークトラフィックを識別します。検出は、Suricata の脅威エンジンでカタログ化されたルールに基づいています。

グループ

Tenable.ot のポリシーの定義で重要なコンポーネントは、*グループ*の使用です。ポリシーを構成する場合、各パラメーターは個々のエンティティではなくグループによって指定します。これにより、ポリシー構成プロセスが大幅に合理化されます。

イベント

ポリシー条件に一致するイベントが発生すると、システムでイベントが生成されます。すべてのイベントはイベント画面に表示され、関連するインベントリおよびポリシー画面からもアクセスできます。各イベントは、イベントによって引き起こされるリスクの程度を示す深刻度レベルでマークされています。通知は、イベントを生成したポリシーのポリシーアクションで指定されているように、電子メール受信者および SIEM に自動的に送信されます。

承認されたユーザーはイベントを解決済みとしてマークでき、コメントを追加することができます。

TENABLE.OT ハードウェアコンポーネント

Tenable.ot アプライアンス

フロントパネル

コンポーネント	説明
電源インジケーター	Tenable.ot アプライアンスがオン(緑)またはオフになったことを示します。
コンソールポート	使用されていません。
USB ポート	使用されていません。
イーサネットポート	4 つの GbE ポートが、次のように管理ネットワークと運用ネットワークに接続するために使用されます。 ポート 1 - デフォルトでは、このポートは管理(ユーザーインターフェース)とアクティブクエリポート(ネットワーク資産との通信)の両方に使用されます。このポート構成は、クエリのみを含むように設定中または設定ページで後から変更することができます。これは、管理インターフェースをコントローラーのネットワークから分離するために行われます。 ポート 2 - ミラーポート - ミラーリングセッション(SPAN)の宛先として使用されます。このポートは、ネットワークトラフィックのコピーを受信します。このポートには IP アドレスがありません。 ポート 3 - ポート分離オプションが有効な場合、このポートは管理(UI)のみに使用され、コントローラーのネットワークの一部ではないネットワークに接続できます。 ポート 4 - 予約済みポートであり、リモートまたはローカルサポートのために Tenable.ot の Professional Services が使用します。

リアパネル

コンポーネント	説明
冷却ファン	2 個の冷却ファン。通風口がふさがれていないことを確認してください。
電源スイッチ	ON/OFF スイッチ(電源を切るには、数秒押し続けます)。
電源ポート	AC 電源コネクタ (AC 100 ～ 240 V)。

パッケージ内容

コンポーネント	説明
2 本のイーサネットケーブル	2 本の標準 RJ45 イーサネットケーブル。これらのケーブルを使用して、Tenable.ot アプライアンスをネットワークスイッチに接続します。
電源ポート	AC 電源コネクタ (AC 100 ～ 240 V)。
マウントブラケット	1U ラックマウントブラケット 2 個。

Tenable.ot センサー

ラックマウントセンサー

ラックマウントセンサーは製造が中止されています。代わりに、構成可能なセンサーモデルをラックマウントに取り付けられるアダプターキットを提供しています。

フロントパネル

コンポーネント	説明
コンソールポート	使用されていません。
USB ポート	使用されていません。
イーサネットポート	4 つの 1GbE ポートが、次のように管理ネットワークと運用ネットワークに接続するために使用されます。 ポート 1 - 管理ポート - デバイスの管理に使用されます。 ポート 2 - ミラーポート - ミラーリングセッション(SPAN)の宛先として使用されます。このポートは、ネットワークトラフィックのコピーを受信します。このポートには IP アドレスがありません。 ポート 3 - 使用されていません。 ポート 4 - 使用されていません。

リアパネル

コンポーネント	説明
電源ボタン	スタンバイモードは赤色、電源オンモードは緑色です。
リセットボタン	電源を切らずにシステムを再起動します。
電源スイッチ	ON/OFF スイッチ(電源を切るには、数秒押し続けます)。
電源ポート	AC 電源コネクタ (AC 100 ～ 240 V)。

パッケージ内容

コンポーネント	説明
イーサネットケーブル	1 本の標準 RJ45 イーサネットケーブル。このケーブルを使用して、センサーをネットワークスイッチに接続します。
電源ケーブル	1 本のその地域の標準 AC 電源ケーブル。
電源	60W AC 電源アダプタ (AC 100 ～ 240 V)。
マウントブラケット	1U L 字型ラックマウントブラケット 2 個。
ネジパック	

構成可能なセンサー

このモデルは、DIN レールまたはマウントラック (アダプターキットを使用) に取り付けられます。以前は、このモデルは DIN レールセンサーと呼ばれていました。

フロントパネル

コンポーネント	説明
電源インジケーター	センサーがオン (緑) またはオフになったことを示します。
コンソールポート	使用されていません。
USB ポート	使用されていません。

コンポーネント	説明
イーサネットポート	5 つの GbE ポートが、次のように管理ネットワークと運用ネットワークに接続するために使用されます。 ポート 1 - 管理ポート - デバイスの管理に使用されます。 ポート 2 - 使用されていません。 ポート 3 - ミラーポート-ミラーリングセッション(SPAN)の宛先として使用されます。このポートは、ネットワークトラフィックのコピーを受信します。このポートには IP アドレスがありません。 ポート 4 - 使用されていません。 ポート 5 - 使用されていません。

パッケージ内容

コンポーネント	説明
電源ケーブル	1 本のその地域の標準 AC 電源ケーブル。
電源	60W AC 電源アダプタ (AC 100 ～ 240 V)。
イーサネットケーブル	1 本の標準 RJ45 イーサネットケーブル。このケーブルを使用して、センサーをネットワークスイッチに接続します。
マウントイヤー	1U L 字型ラックマウントブラケット 2 個(「イヤー」)。
ネジパック	

ファイヤーウォールの考慮事項

Tenable.ot システムを設定する際、Tenable システムが正しく動作するようどのポートを開いたままにしておくかを計画することが重要です。次の表は、Tenable.ot Core プラットフォームおよび Tenable.ot センサーで使用するために開いたままにしておくべきポートを示しています。アクティブクエリの実行や、Tenable.io および Tenable.sc との統合に必要なポートを示すテーブルもあります。

Tenable.ot Core プラットフォーム

Tenable.ot Core プラットフォームとの通信のために、次のポートを開いたままにしておく必要があります。

通信方向	ポート	通信先	目的
インバウンド	TCP 443	Tenable.ot 用ウェブインターフェース	Tenable.ot へのブラウザアクセス
インバウンド	TCP 8000	Tenable Core 用ウェブインターフェース	Tenable Core へのブラウザアクセス
インバウンド	TCP 22	センサー	センサー通信
インバウンド	TCP 22	SSH アクセス用アプライアンス	OS またはアプライアンスへのコマンドラインアクセス
アウトバウンド*	TCP 443	Tenable.sc	統合のためにデータを送信
アウトバウンド*	TCP	cloud.tenable.com	統合のためにデータを送信
アウトバウンド*	さまざまな産業用プロトコル	PLC / コントローラー	アクティブクエリ
アウトバウンド*	TCP 25	アラート用メールサーバー	SMTP(アラートメール、レポート)
アウトバウンド*	UDP 514	Syslog サーバー	Syslog サーバー
アウトバウンド*	UDP 53	DNS サーバー	名前解決
アウトバウンド*	UDP 123	NTP サーバー	タイムサービス
アウトバウンド*	TCP 636	AD サーバー	AD LDAP 認証
アウトバウンド*	TCP 443	SAML プロバイダー	シングルサインオン
アウトバウンド*	UDP 161	SNMP サーバー	Tenable Core に対する SNMP 監視
アウトバウンド*'	TCP\443	*.tenable.com	自動プラグイン、アプリケーション、OS の更新**

*オプションサービス
**オフライン手順が利用可能

Tenable.ot センサー

Tenable.ot センサーとの通信のために、次のポートを開いたままにしておく必要があります。

通信方向	ポート	通信先	目的
インバウンド	TCP 8000	ウェブインターフェース	ユーザー GUI へのブラウザアクセス
アウトバウンド	TCP 22	Tenable.ot アプライアンス	センサー通信

通信方向	ポート	通信先	目的
インバウンド	TCP 22	SSH アクセス用アプライアンス	OS またはアプライアンスへのコマンドラインアクセス
アウトバウンド*	TCP 25	アラート用メールサーバー	SMTP(アラートメール、レポート)
アウトバウンド*	UDP 53	DNS サーバー	名前解決
アウトバウンド*	UDP 123	NTP サーバー	タイムサービス
アウトバウンド*	UDP 161	SNMP サーバー	Tenable Core に対する SNMP 監視

*オプションサービス

アクティブクエリ

アクティブクエリ機能を使用するには、以下のポートを開いたままにしておく必要があります。

通信方向	ポート	通信先	目的
アウトバウンド	TCP 80	OT デバイス	HTTP フィンガープリント
アウトバウンド	TCP 102	OT デバイス	S7 / S7+ プロトコル
アウトバウンド	TCP 443	OT デバイス	HTTPS フィンガープリント
アウトバウンド	TCP 445	OT デバイス	WMI クエリ
アウトバウンド	TCP 502	OT デバイス	Modbus プロトコル
アウトバウンド	TCP 5432	OT デバイス	PostgreSQL クエリ
アウトバウンド	TCP 44818	OT デバイス	CIP プロトコル*
アウトバウンド	TCP/UDP 53	OT デバイス	DNS
アウトバウンド	ICMP	OT デバイス	資産検出
アウトバウンド	UDP 161	OT デバイス	SNMP クエリ
アウトバウンド	UDP 137	OT デバイス	NBNS クエリ
アウトバウンド	UDP 138	OT デバイス	NetBIOS クエリ

*ベンダーによる使用専用
**デバイスのメーカーやモデルによっては、他のポートやプロトコルが必要になる場合があります

Tenable.ot の統合

Tenable.io および Tenable.sc の統合との通信のために、次のポートを開いたままにしておく必要があります。

通信方向	ポート	通信先	目的
アウトバウンド	TCP 443	cloud.tenable.com	Tenable.io の統合
アウトバウンド	TCP 443	Tenable.sc	Tenable.sc の統合

TENABLE.OT アプライアンスの設置

ステップ 1 - Tenable.ot アプライアンスのセットアップ

Tenable.ot アプライアンスは、ラックに取り付けることも、机などの平面に置くこともできます。

ラックマウント

➡ Tenable.ot アプライアンスの標準 (19 インチ) ラックへの取り付け手順

1. サーバーユニットをラックの空いている 1U スロットに挿入します。

   ラックが電気的に接地されていることを確認してください。また、バックパネルにある冷却ファンの通気口とトップパネルの通気孔がふさがれていないことも確認してください。

2. ラックマウント用ブラケット (付属) をラックマウントに適合するねじ (付属していません) でラックフレームに固定し、ユニットをラックに固定します。
3. AC 電源ケーブル (付属) をリアパネルの電源ポートに差し込み、次にケーブルを AC 電源 (主電源) に差し込みます。

平面

➡ Tenable.ot アプライアンスの平面への設置手順

1. アプライアンスユニットを、乾いた水平で安定な面 (机など) に置きます。

   机上が平らで乾いていることを確認してください。
   また、バックパネルにある冷却ファンの通気口とトップパネルの通気孔がふさがれていないことも確認してください。

2. ユニットを他の電気機器と一緒に配置する場合は、バックパネルにある冷却ファンの背後に十分なスペースを確保し、適切な通気と冷却を行います。
3. AC 電源ケーブル (付属) をリアパネルの電源ポートに差し込み、次にケーブルを AC 電源 (主電源) に差し込みます。

ステップ 2 - Tenable.ot のネットワーク接続

Tenable.ot は、ネットワーク監視とアクティブクエリの両方に使用されます。

- **ネットワーク監視の実行 -** 対象のコントローラー / PLC に接続されているネットワークスイッチのミラーリングポートにユニットを接続する必要があります。
- **アクティブクエリの実行 -** 対象のコントローラー / PLC に接続されているネットワークスイッチ上で IP アドレスを持つ通常ポートにユニットを接続する必要があります。

デフォルトでは、アクティブクエリと管理コンソールはユニットの同じポート (ポート 1) を使用するように構成されていますが、初期設定後にポート 3 の管理を構成して管理ポートとアクティブクエリポートに使用するポートを分離できます。この構成後、**ステップ 7 - 個別の管理ポートの接続 (ポート分離オプション用)** で説明されているように、ユニットのポート 3 をスイッチの通常のポートに接続して、管理を実行する必要があります。

初期設定では、ポート 1 をネットワークスイッチの通常のポートに接続し、ポート 2 をミラーリングポートに接続します。

Tenable.ot アプライアンスのネットワークへの接続手順

1. Tenable.ot アプライアンスで、イーサネットケーブル(付属)を **ポート 1** に接続します。
2. ネットワークスイッチの通常のポートにケーブルを接続します。
3. ユニットで、別のイーサネットケーブル(付属)を **ポート 2** に接続します。
4. ネットワークスイッチのミラーリングポートにケーブルを接続します。

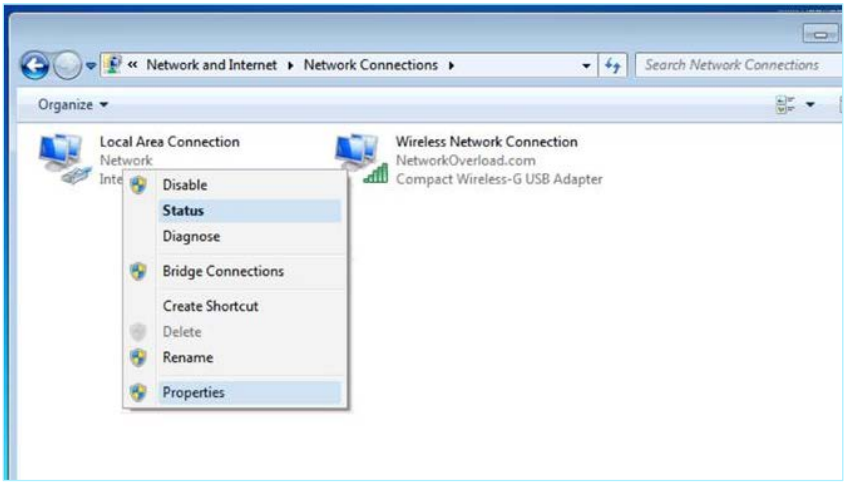
ステップ 3 - 管理コンソールへのログイン

管理コンソールへのログイン手順

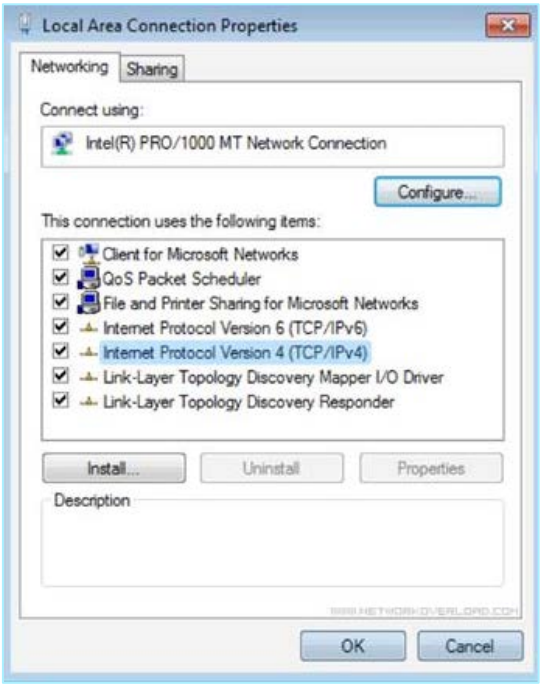
1. 次のいずれかを行います。
   - イーサネットケーブルを使用して、管理コンソールワークステーション(デスクトップ、ノートパソコンなど)を Tenable.ot アプライアンスのポート 1 に直接接続します。
   - 管理コンソールワークステーションをネットワークスイッチに接続します。
2. 管理コンソールワークステーションが、Tenable.ot アプライアンスと同じサブネット(192.168. 1.0/24)の一部であるか、ユニットにルーティング可能であることを確認します。
3. 静的 IP を設定するには、次の手順を実行します(Tenable.ot アプライアンスに接続するには、静的 IP を設定する必要があります)。
   a. **[ネットワークとインターネット]**>**[ネットワークと共有センター]**>**[アダプター設定の変更]** に移動します。

> Windows のバージョンによって、ナビゲーションが若干異なる場合があります。

   b. [ネットワーク接続]画面が表示されます。



c. **[ローカルエリア接続]**を右クリックし、**[プロパティ]**を選択します。
[ローカルエリア接続]ウィンドウが表示されます。



d. **[インターネットプロトコルバージョン4(TCP / IPv4)]**を選択し、**[プロパティ]**をクリックします。
[インターネットプロトコルバージョン4(TCP / IPv4)プロパティ]ウィンドウが表示されます。

e. [次のIPアドレスを使う]を選択します。
f. [IPアドレス]フィールドに、*192.168.1.10*と入力します。
g. [サブネットマスク]フィールドに、*255.255.255.0*と入力します。
h. **[OK]**をクリックします。
新しい設定が適用されます。

4. Chrome ウェブブラウザで、https://192.168.1.5 に移動します。
   セットアップウィザードのようこそ画面が開きます。

> UI は Chrome ブラウザからしかアクセスできません。また、最新バージョンの Chrome を使用している必要があります。

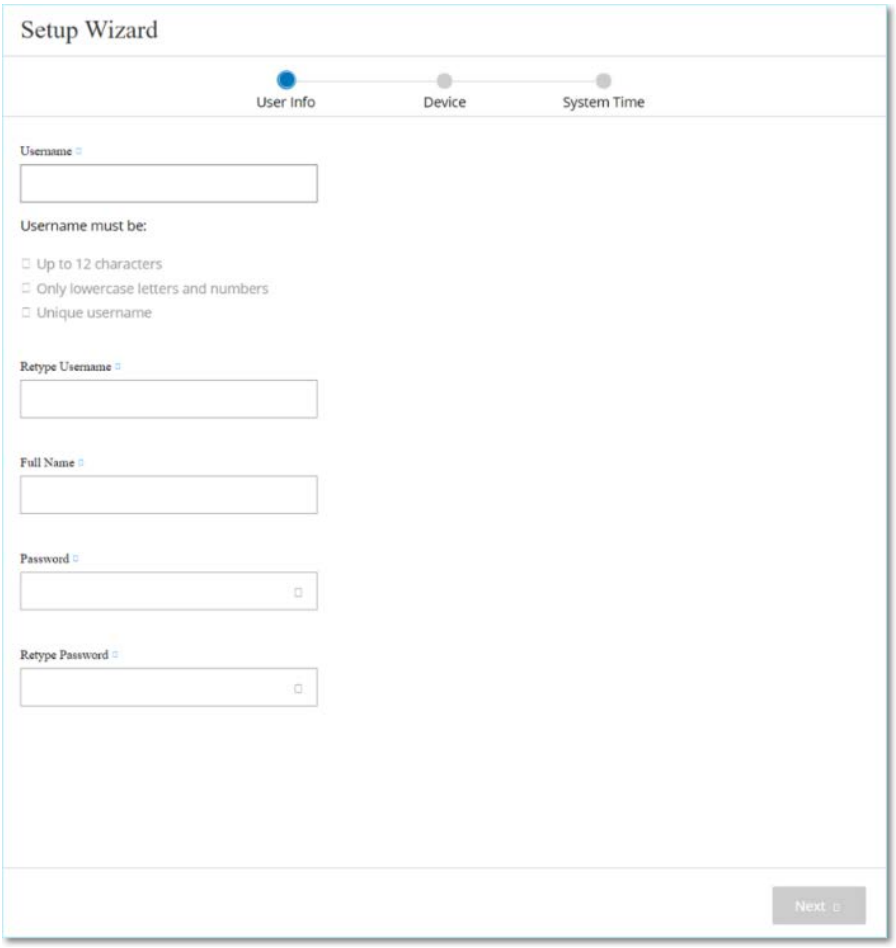
5. **[セットアップウィザードの開始]** をクリックします。
   セットアップウィザードが開き、**[ユーザー情報]** ページが表示されます。

ステップ 4 – セットアップウィザード

Tenable.ot セットアップウィザードは、基本的なシステム設定を構成するプロセスをガイドします。

後で設定を変更する場合は、管理コンソール (UI) の **[設定]** 画面で変更できます。

画面 1 - ユーザー情報



➡ **[ユーザー情報] ページで、次のようにユーザーアカウント情報を入力します。**

セットアップウィザードでは、管理者アカウントの認証情報を構成します。UI にログイン後、追加のユーザーアカウントを作成できます。ユーザーアカウントの詳細については、**ユーザーとロール**セクションを参照してください。

1. **[ユーザー名]** フィールドに、システムへのログインに使用するユーザー名を入力します。ユーザー名の長さは 12 文字まで、使用できる文字は小文字と数字のみとなります。
2. **[ユーザー名の再入力]** フィールドに、同じユーザー名を再入力します。
3. **[氏名]** セクションで、**氏名**を入力します。

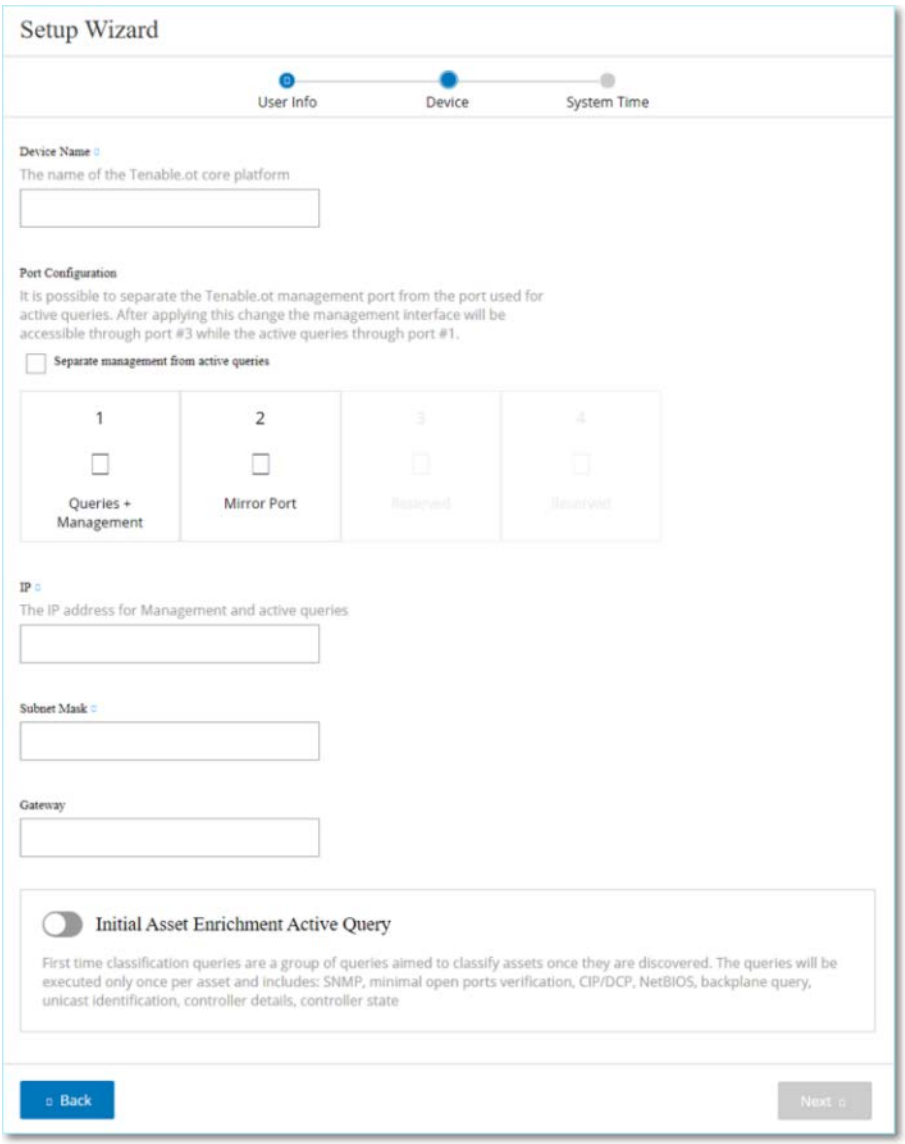
これは、ヘッダーバーとシステムのアクティビティのログに表示される名前です。

4. **[パスワード]** フィールドに、システムへのログインに使用するパスワードを入力します。パスワードには少なくとも以下を含める必要があります。

- 12 文字
- 1 つの大文字
- 1 つの小文字
- 1 つの数字
- 1 つの特殊文字

5. **[パスワードの再入力]** フィールドに、同じパスワードを再入力します。
6. **[次へ]** をクリックします。
   セットアップウィザードの **[デバイス]** ページが開きます。

画面 2 - デバイス



➡ **[デバイス] ページで、次のように Tenable.ot プラットフォームに関する情報を入力します。**

1. **[デバイス名]** フィールドに、Tenable.ot プラットフォームの一意の識別子を入力します。
2. **[ポートの構成]** セクションで、次のいずれかを実行します。
   - **ポート分離** - 1 つのポートを管理用に使用し、別のポートをクエリ用に使用する場合は、**[アクティブクエリから管理を分離]** チェックボックスをオンにします。このオプションを選択すると、*ポート 1* がクエリ*専用*ポートとして、*ポート 3* が管理*専用*ポートとして構成されます。

> 一部のシステムでは、**ポート分離**オプションが利用できない場合があります。サポートが必要な場合は、サポート担当者に連絡してください。

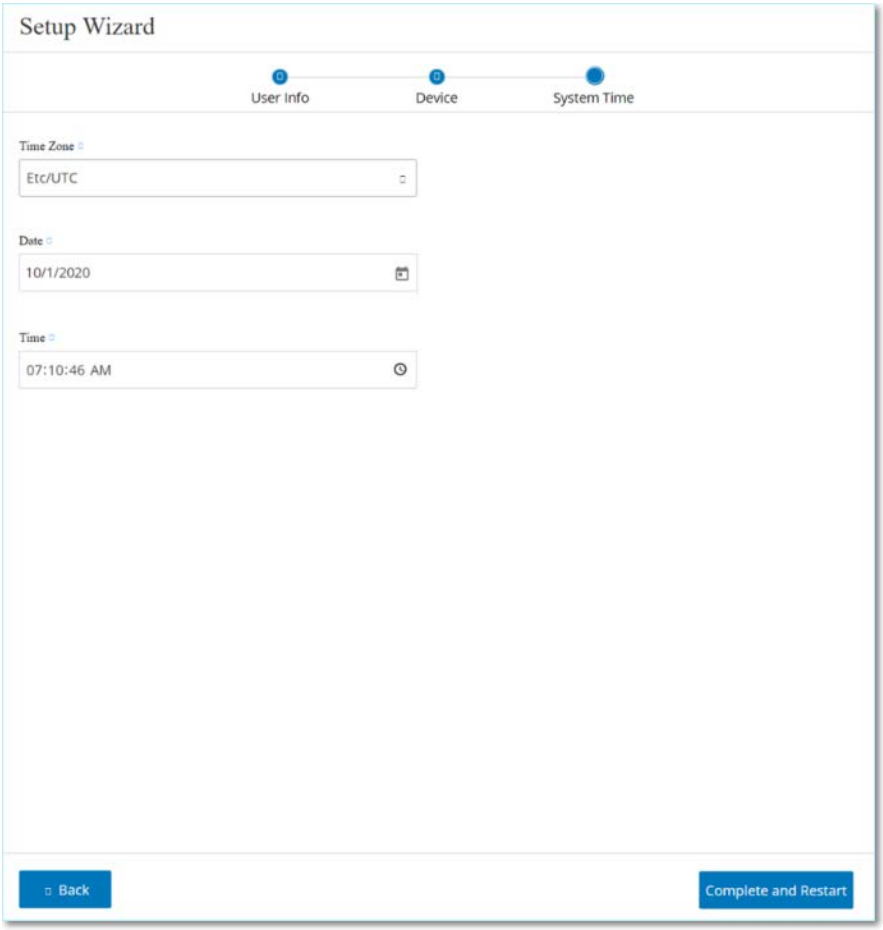
- **分離なし** - クエリと管理を同じポートのままにしたい場合は、**[アクティブクエリから管理を分離]** チェックボックスをオンにしないでください。この場合、この手順の 3 ～ 5 をスキップし、**6 に進みます。**

3. **ポート分離**オプションを選択した場合は、**[アクティブクエリ IP]** フィールドに、ユニットの *クエリポート* の IP アドレスを入力します。このポートは、ネットワークスイッチの通常のポートに接続され、コントローラーと通信できます (つまり、ルーティング可能です)。また、Tenable.ot はコントローラーにアクティブに接続するため、ネットワークサブネット内に IP アドレスが必要です。
4. **ポート分離**オプションを選択した場合は、**[アクティブクエリのサブネットマスク]** フィールドに、*クエリポート* のサブネットマスクを入力します。
5. **ポート分離**オプションを選択した場合は、**[アクティブクエリゲートウェイ]** フィールド (オプション) に、操作ネットワークのゲートウェイの IP アドレスを入力します。
6. **[管理 IP]** フィールドに、Tenable.ot プラットフォームに適用する IP アドレス (ネットワークサブネット内) を入力します。これが Tenable.ot 管理 IP アドレスになります (ポートを分離しない場合、これは *クエリ* アドレスでもあります)。
7. **[管理サブネットマスク]** フィールドに、ネットワークのサブネットマスクを入力します。
8. ゲートウェイ (オプション) を設定する場合は、**[管理ゲートウェイ]** フィールドにネットワークのゲートウェイ IP を入力します。

> このフィールドに入力しないと、Tenable.ot はサブネット外の外部コンポーネント (メールサーバー、syslog サーバーなど) と通信できません。

9. *初期資産強化アクティブクエリ* は、システムで検出された各資産で実行される一連のクエリです。これは、Tenable.ot が資産を分類するのに役立ちます。検出された新しい資産ごとにこれらのクエリを実行する場合は、下部のボックスのトグルスイッチを**オン**にします。
10. **[次へ]** をクリックします。
セットアップウィザードの **[システム時刻]** ページが開きます。

画面 3 - システム時刻



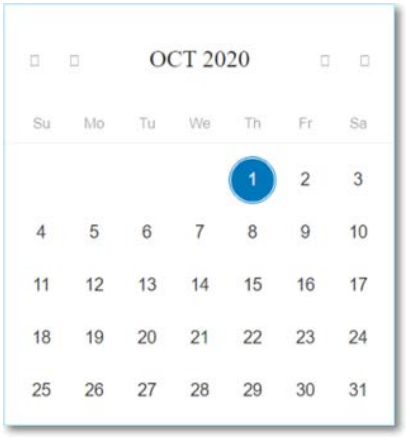
[システム時刻] ページでは、通常、正しい時刻と日付が自動的に設定されます。

ログとアラートを正確に記録するには、正しい日付と時刻を設定することが重要です。

➡ **正しい日付と時刻が設定されていない場合は、次のように情報を入力してください。**

1. **[タイムゾーン]** フィールドで、ドロップダウンリストからサイトの場所のローカルタイムゾーンを選択します。

2. **[日付]** フィールドで、カレンダーアイコン をクリックします。
   ポップアップカレンダーが表示されます。



3. 現在の日付を選択します。
4. **[時間]** フィールドで、**時**、**分**、**秒**、**AM/PM** をそれぞれ選択し、キーボードまたは上矢印と下矢印のいずれかを使用して、正しい数値を入力します。

> セットアップウィザードの前のページを編集する場合は、[戻る] をクリックしてください。[完了して再起動] のクリック後は、セットアップウィザードに戻ることができません。ただし、UI の [設定] ページで構成設定を変更できます。

5. セットアップ手順を完了するには、**[完了して再起動]** をクリックします。
   再起動が完了すると、ライセンス画面にリダイレクトされます。

ステップ 5 - ライセンス

システムをアクティブ化する前に、Tenable.ot ライセンスを登録する必要があります。

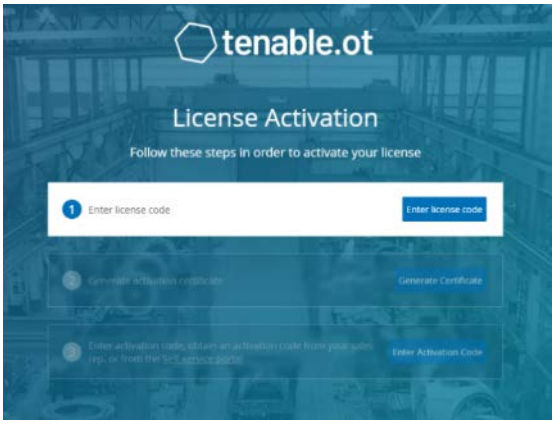
前提条件

- デバイスの注文時に Tenable から受け取ったライセンスコード (20 文字 / 数字)。
- インターネットへのアクセスが必要です。Tenable.ot デバイスがインターネットに接続されていない場合は、任意の PC からライセンスを登録できます。

ライセンスのアクティベーション

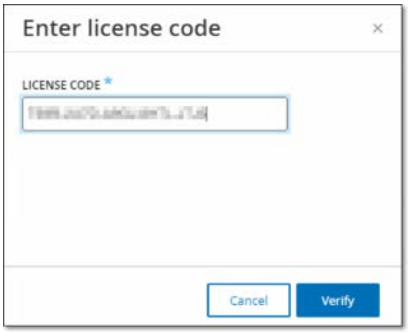
➡ ライセンスのアクティブ化手順

1. **[ライセンスのアクティベーション]** 画面のステップ 1 **[ライセンスコードの入力]** フィールドで、**[ライセンスコードの入力]** ボタンをクリックします。



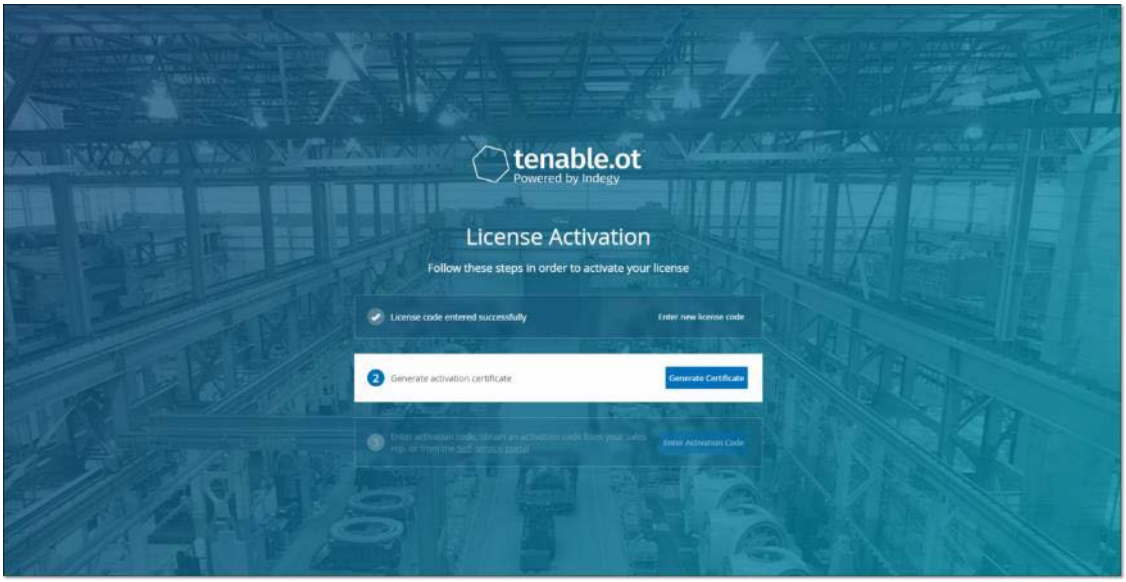
[ライセンスコードの入力] サイドパネルが右側に表示されます。

2. **[ライセンスコード]** フィールドにライセンスコードを入力し、**[確認]** をクリックします。



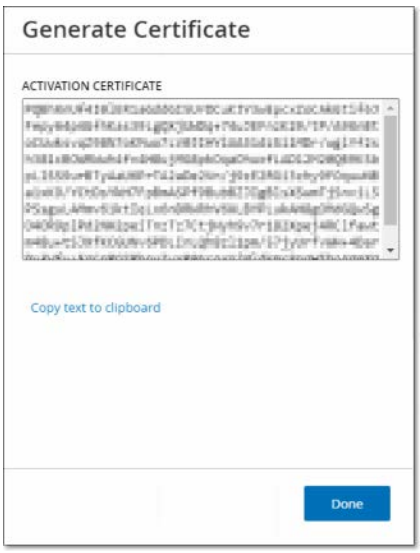
サイドパネルが閉じます。

3. ステップ 2 の **[アクティベーション証明書の生成]** フィールドで、**[証明書の生成]** ボタンをクリックします。



[証明書の生成] サイドパネルがアクティベーション証明書とともに表示されます。

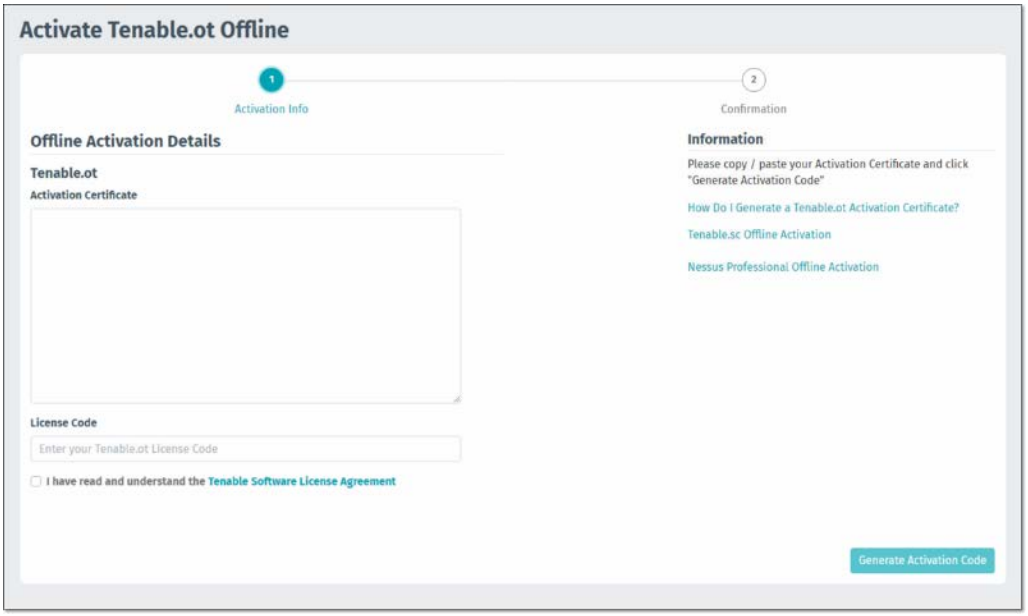
4. **[テキストをクリップボードにコピー]** ボタンをクリックし、**[完了]** をクリックします。



サイドパネルが閉じます。

5. ステップ 3 の **[アクティベーションコードの入力]** フィールドで、**[セルフサービスポータル]** リンクをクリックします。

[Tenable.ot をオフラインでアクティブ化] 画面が新しいタブで開きます。



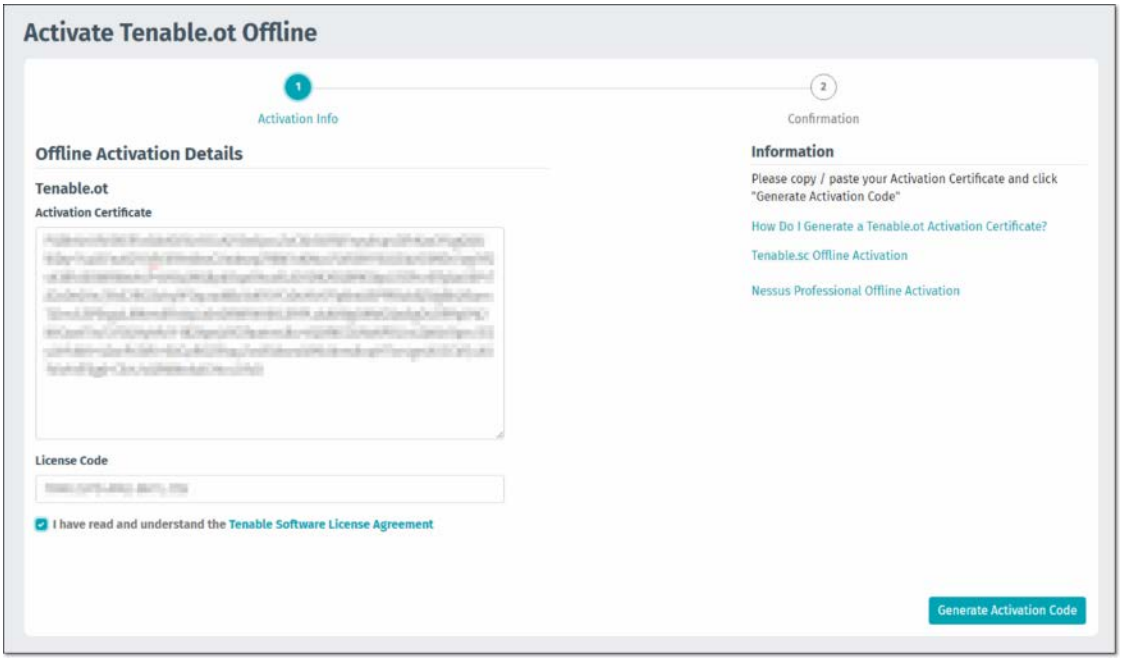
Tenable.ot デバイスがインターネットに接続されていない場合は、インターネットに接続されたデバイスで次の URL から [Tenable.ot をオフラインでアクティブ化] 画面にアクセスする必要があります。
https://provisioning.tenable.com/activate/offline/tenable-ot

現在 tenable.com にログインしていない場合は、メールアドレスとパスワードを使用してログインする必要があります。ログインにはライセンスコードを受け取ったメールアカウントを使用する必要があります。

ログイン認証情報がない場合は、**[パスワードを忘れた場合]** をクリックし、プロンプトに従うか、Tenable アカウントマネージャーに連絡してください。

6. [アクティベーション証明書] フィールドに、アクティベーション証明書を入力します。
7. **[ライセンスコード]** フィールドに、この手順のステップ 2 で入力したものと同じ 20 文字の**ライセンスコード**を入力します。

8. [Tenable ソフトウェアライセンス契約を読み、理解しました]チェックボックスをクリックします。

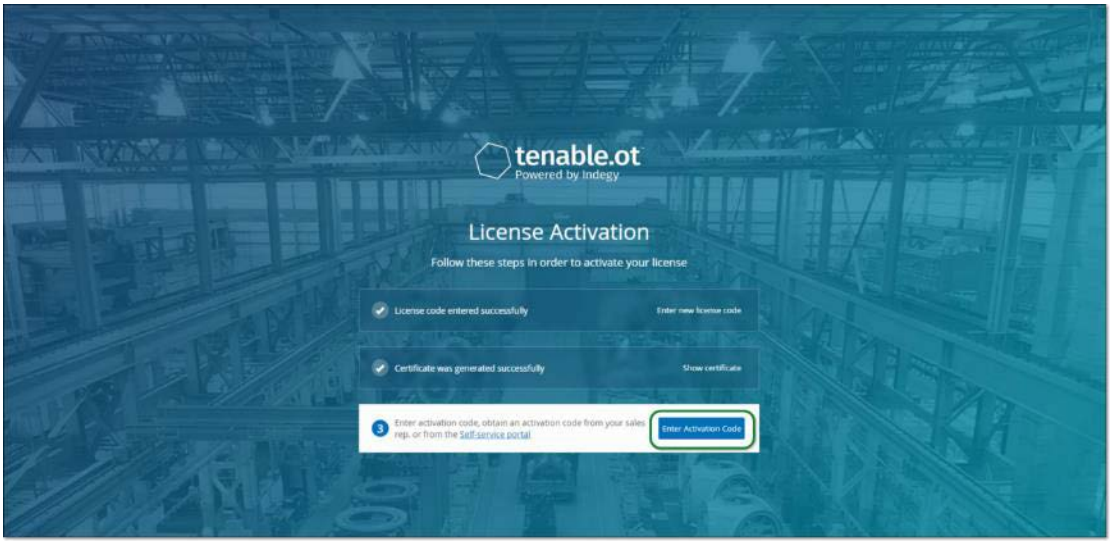


ライセンス契約を表示するには、**[Tenable ソフトウェアライセンス契約]** のリンクをクリックしてください。

9. [アクティベーションコードの生成]ボタンをクリックします。
[オフラインアクティベーションコードが正常に作成されました!]画面が表示されます。

10. [テキストをクリップボードにコピー]をクリックします。

11. Tenable.ot デバイスの**[ライセンスのアクティベーション]**画面に戻り、**[アクティベーションコードの入力]**ボタンをクリックします。



[アクティベーションコードの入力]サイドパネルが表示されます。

12. **[アクティベーションコード]**フィールドにアクティベーションコードを貼り付け、**[アクティブ化]**ボタンをクリックします。

サイドパネルが閉じ、Tenable.ot のホーム画面が表示されます。[有効化]ボタンが表示されます。

ライセンスの更新の詳細については、**ライセンスの更新** を参照してください。

ステップ 6 - システムの有効化

ライセンスのアクティベーションが完了すると、*[有効化]* ボタンが表示されます。

システムの主要な機能をアクティブ化するには、システムを有効化する必要があります。

システムが有効化されると、次の機能がアクティブ化されます。

- ネットワーク内の資産の特定
- すべてのネットワークトラフィックの収集と監視
- ネットワーク上の「会話」のログ記録

上記の機能で蓄積されたすべてのデータと分析は、管理コンソール(UI)で表示できます。

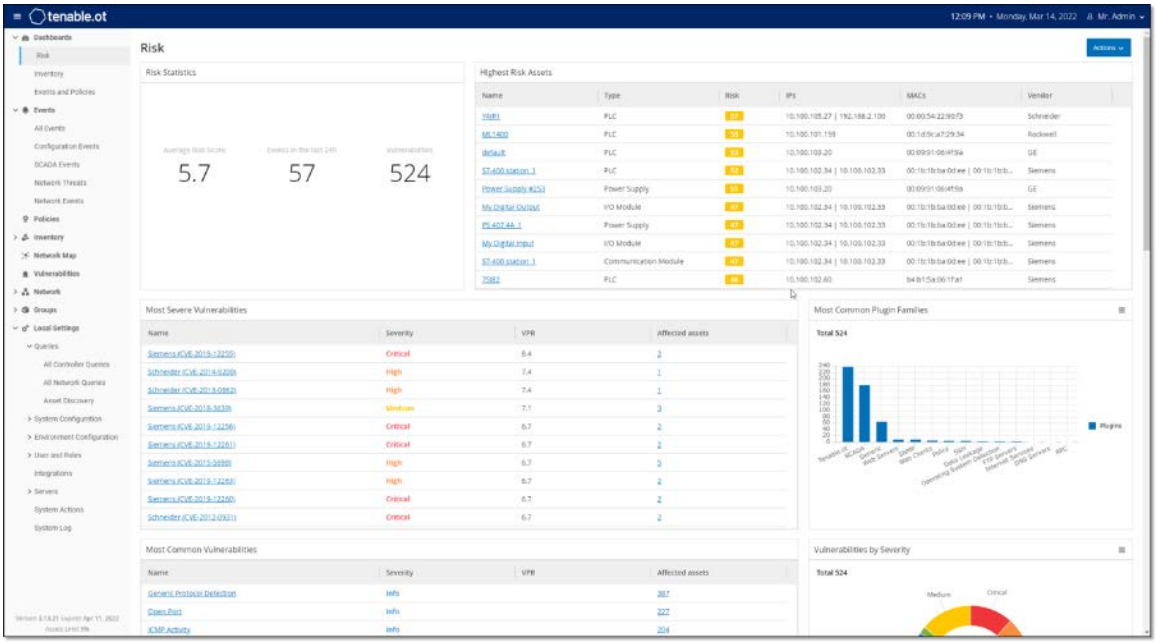
これらは継続的に進行するプロセスであり、UI に表示される結果が完全に更新されるまでには時間がかかります。

アクティブクエリなどの追加機能は、管理コンソール(UI)の **[ローカル設定]** 画面で設定およびアクティブ化できます。

クエリを参照してください。

➡ システムの有効化手順

1. **[有効化]** ボタンをクリックします。
   システムが有効化されます。UI が開き、**[ダッシュボード]**>**[リスク]** 画面が表示されます。



> システムが資産を識別するまでに数分かかります。データの表示を開始するには、ページのリフレッシュが必要な場合があります。

ステップ 7 - 個別の管理ポートの接続 (ポート分離オプション用)

ポート分離オプション (**クエリ**を管理から分離) を選択した場合は、管理ポートとなった Tenable.ot アプライアンスのポート 3 をネットワークスイッチのポートに接続する必要があります。これは、IT ネットワークのネットワークスイッチなど、別のネットワークスイッチにすることもできます。

➡ 管理ポートの接続手順

1. Tenable.ot アプライアンスで、イーサネットケーブル (付属) をポート 3 に接続します。
2. ネットワークスイッチのポートにケーブルを接続します。

TENABLE.OT センサーの設置

センサーと ICP のペアリング

次のセクションでは、バージョン 3.14 以降のセンサーを構成する手順について説明します。以前のモデルのセンサーを構成するには、**付録 1 - センサーのインストール (バージョン 3.13 以前)**に記載されている手順を使用します。

センサーと ICP のペアリングは、ICP 管理コンソールとセンサーの Tenable Core UI の両方を使用して行われます。

新しいセンサーのペアリングリクエストごとに、着信ペアリングリクエストの自動承認を有効にするか、手動承認を必要とするために自動承認を無効にするかを選択できます。

前提条件

- センサーハードウェアが適切に設置されている (**ステップ 1 - センサーの設定**を参照)。
- センサーがネットワークスイッチに接続されている (**ステップ 2 - センサーのネットワーク接続**を参照)。
- センサーに独自の静的 IPv4 アドレスがある (**ステップ 3 - センサーセットアップウィザードへのアクセス**を参照)。
- センサーが Tenable Core プラットフォームに接続され、Core ユーザーインターフェースにログインするためのユーザー名とパスワードがある。Tenable Core ユーザーインターフェースの使用の詳細については、https://docs.tenable.com/tenablecore/Tenableot/Content/TenableCore/Introduction_OT.htm を参照してください。
- ICP コンソールに有効な証明書があることを確認する (**証明書**を参照)。
- 接続の切断を回避するために、センサーのペアリングプロセスに対して管理者ロールを持つ専用 ICP ユーザーを作成することをお勧めします (**ローカルユーザーの追加**を参照)。1 名の新しい管理者ユーザーを、複数のセンサーのペアリングに使用できます。

センサーのペアリング

➡ v.3.14 以降のセンサーと ICP のペアリング

1. ICP 管理コンソール (UI) で、**[ローカル設定]**>**[システム構成]**>**[センサー]**画面に移動します。

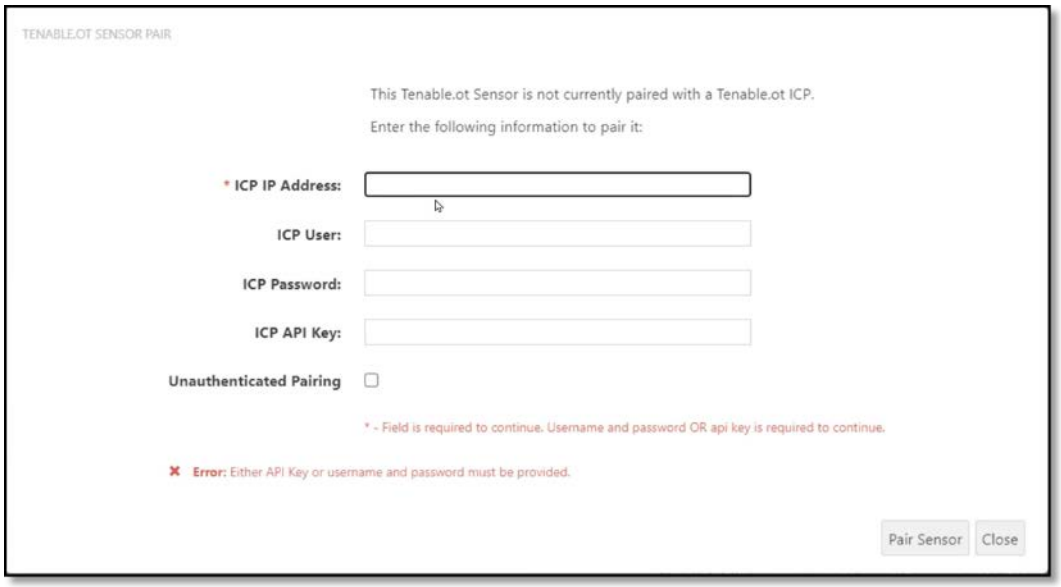
2. センサーペアリングの自動承認を有効にする場合は、画面上部にある**[着信センサーペアリングリクエストの自動承認]**スイッチを**[オン]**に切り替えてください。オフの場合、すべてのペアリングリクエストを手動で承認する必要があります。
3. ICP タブを開いたままで新しいタブを開き、**<Sensor IP>:8000** と入力してセンサーの Tenable Core ユーザーインターフェースにアクセスします。

> UI は Chrome ブラウザからしかアクセスできません。また、最新バージョンの Chrome を使用している必要があります。

4. Tenable Core コンソールのログインウィンドウで、**ユーザー名**と**パスワード**を入力し、**[特権タスクでパスワードを再利用する]**チェックボックスを選択して、**[ログイン]**をクリックします。

ログイン時に **[特権タスクでパスワードを再利用する]** チェックボックスが選択されていない場合、ユーザーはセンサーサービスを再起動できません。

5. ナビゲーションメニューバーで **[Tenable.ot センサー]** をクリックします。
[Tenable.ot センサーペア] ウィンドウが表示されます。



[Tenable.ot センサーペア] ウィンドウは、ページが最初にロードされたときにのみポップアップ表示されます。その後このウィンドウを開くには、**[Tenable Core]** コンソールの **[ペアリング情報]** セクションで ボタンをクリックします。

6. **[ICP IP アドレス]** フィールドに、このセンサーとペアリングする ICP の IPv4 アドレスを入力します。
7. 認証されていない(暗号化されていない)ペアリングを使用する場合は、**[認証されていないペアリング]** チェックボックスをクリックし、ステップ 8 に進みます。

認証されていないペアリングを使用するセンサーは、ネットワークセグメントをパッシブにスキャンすることしかできず、アクティブクエリを送信するために ICP で管理することはできません。

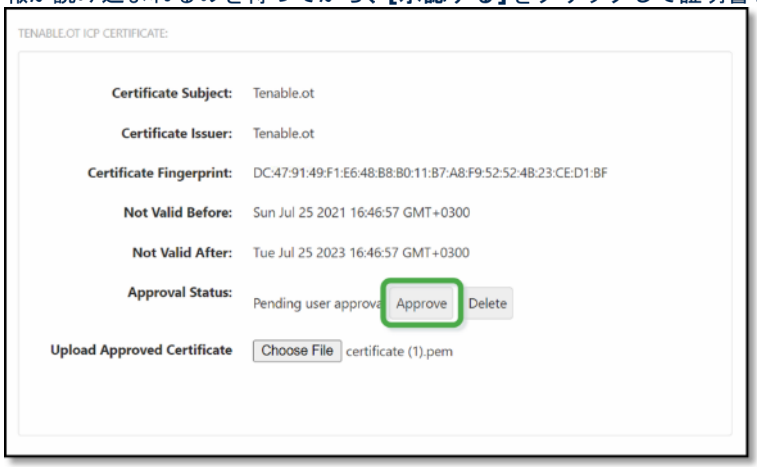
8. ペアリングを認証するには、次のいずれかを実行します。

- **[ICP ユーザー]** フィールドに ICP ユーザー名を、**[ICP パスワード]** フィールドに ICP パスワードを入力します。
- **[ICP API キー]** フィールドに ICP の API キーを入力します。

> ペアリングプロセス中の接続を確保するために、センサーのペアリングに対して専用 ICP ユーザーを作成することをお勧めします (**ローカルユーザーの追加**を参照)。

> ユーザー名とパスワードによる認証方法には、失効する API キーとは反対に、認証情報が失効しないという利点があります。

9. **[センサーのペアリング]** をクリックします。
10. ICP が提供する証明書を使用する場合
    a. **[Tenable Core]** コンソールの **[Tenable ICP 証明書]** セクションにある **[認証ステータス]** に、証明書情報が読み込まれるのを待ってから、**[承認する]** をクリックして証明書を承認します。

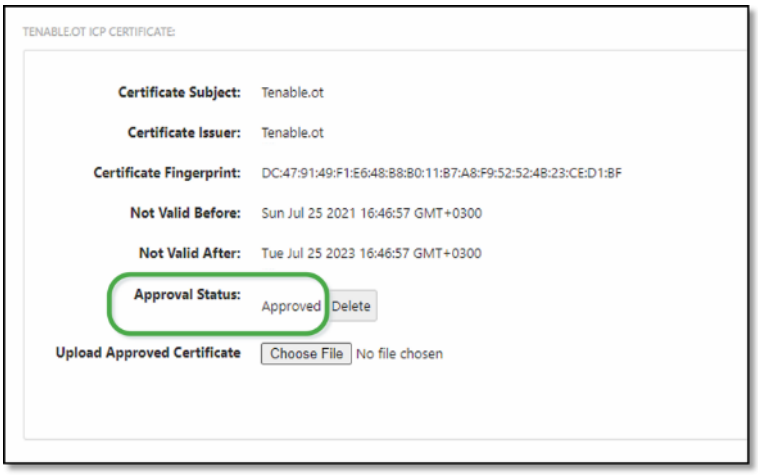


    b. **[Tenable.ot サーバー証明書の承認の確認]** ポップアップウィンドウで、**[この証明書を承認する]** をクリックします。

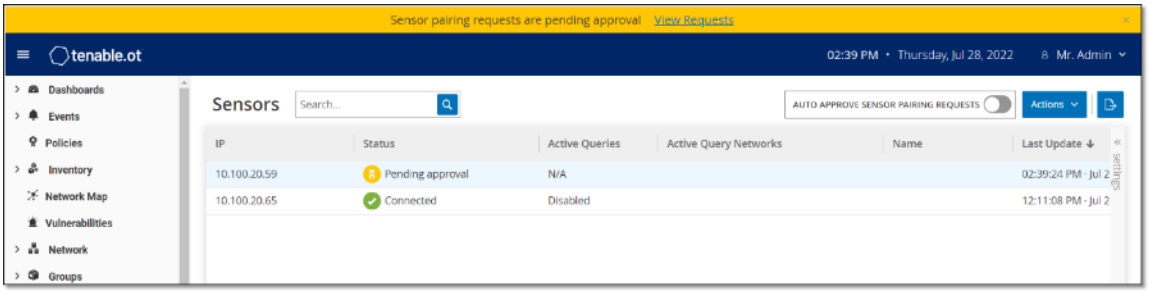
証明書を手動でアップロードする場合

a. **[Tenable ICP]** コンソールで、**HTTPS 証明書の生成**で説明されている手順に従います。
b. **[Tenable Core]** コンソールの **[Tenable ICP 証明書]** セクションにある **[認証済み証明書のアップロード]** で、**[ファイルを選択する]** をクリックします。
c. アップロードする .pem 証明書ファイルに移動します。

有効な証明書が承認されると、**[Tenable.ot ICP 証明書]** テーブルの **[承認ステータス]** が **[認証済み]** と表示されます。

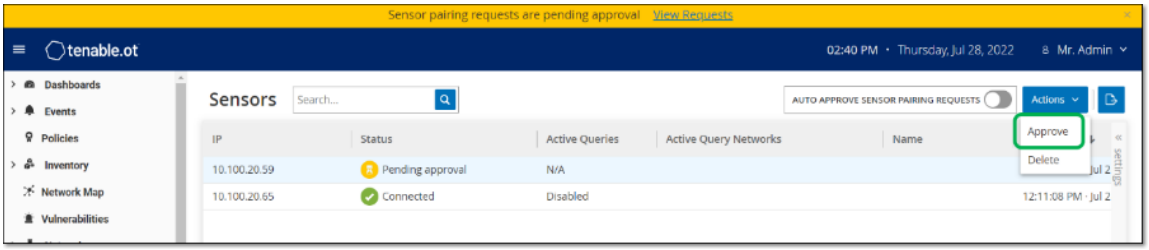


11. ICP UI で、**[ローカル設定]>[システム構成]>[センサー]**画面に戻ります。



新しいセンサーがテーブルに表示され、ステータスが*[承認待ち]*になるはずです。

12. センサーの行をクリックし、**[アクション]**ボタンをクリック(または行を右クリック)して、**[承認]**を選択します。



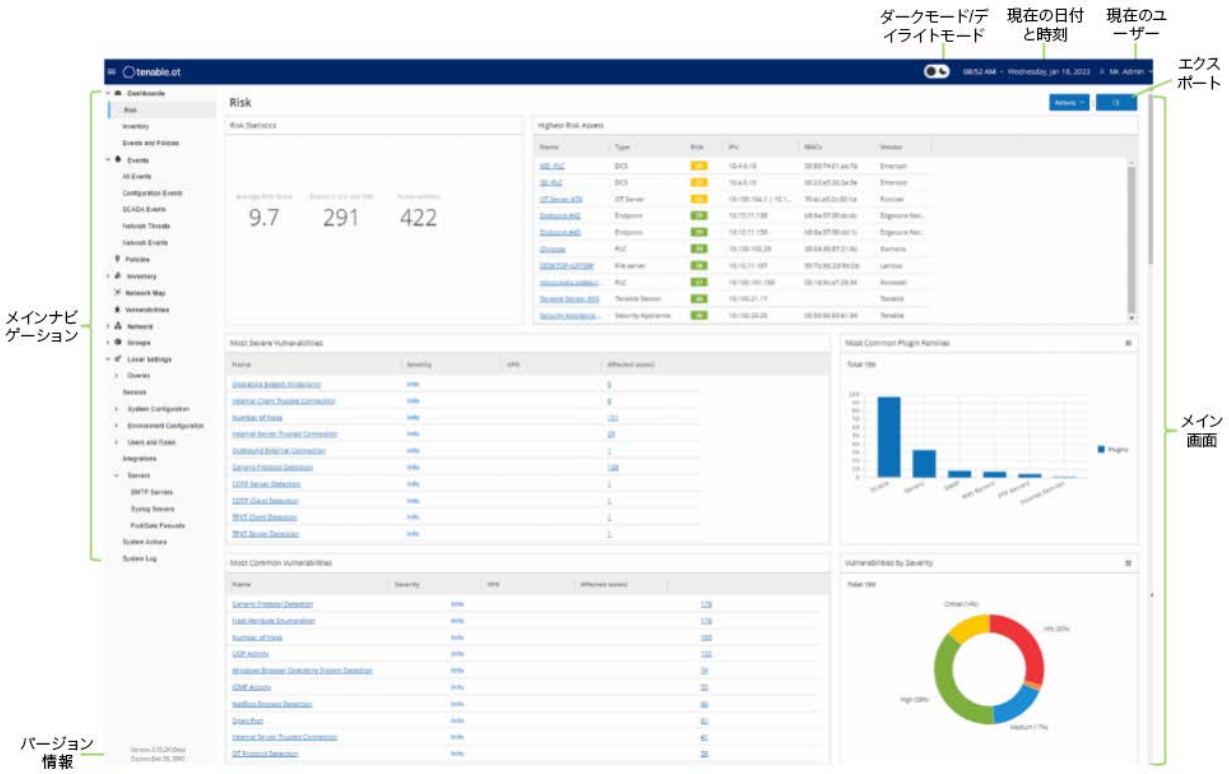
13. ペアリングが成功すると、ステータスが*[接続済み]*に切り替わります。その他のステータスは次のとおりです。
    - *接続済み(未認証)* - センサーは未認証モードで接続されています。センサーは、パッシブネットワーク検出のみを実行できます。
    - *一時停止* - センサーは適切に接続されていますが、一時停止しています。
    - *切断* - センサーは接続されていません。認証されたセンサーの場合、ペアリングプロセスのエラー(トンネルエラー、API の問題など)に起因する可能性があります。
14. 認証済みセンサーのペアリングが完了したら、そのセンサーで実行するアクティブクエリを構成できます。**アクティブクエリの構成**を参照してください。

> ペアリングが完了したら、Tenable Core UI ではなく ICP ページのみを使用してセンサーを管理することをお勧めします。

管理コンソールの UI 要素

管理コンソールの UI は、資産管理、ネットワークアクティビティ、セキュリティイベントに関連する Tenable.ot によって検出された重要なデータに簡単にアクセスできます。UI を使用して、ニーズに応じた Tenable.ot プラットフォーム機能を構成できます。この章では、UI 要素の概要を説明します。特定の UI 機能の詳細については、続く章で説明します。

メイン UI 要素



次の表は、常に表示されるメイン UI 要素を説明しています。

UI 要素	説明
メインナビゲーション	メインナビゲーションメニュー。アイコンをクリックして、ナビゲーションメニューの表示/非表示を切り替えます。
現在の日付と時刻	システムに登録されている現在の日付と時刻を表示します。
現在のユーザー名	現在システムにログインしているユーザーの名前を表示します。選択メニューの下矢印をクリックします。メニューオプションには、[バージョン情報]と[ログアウト]があります。
ライセンス情報	Tenable.ot ソフトウェアのバージョンとライセンスの有効期限を表示します。
メイン画面	メインナビゲーションで選択された画面を表示します。

UI 要素	説明
ダークモード/デイライトモード	表示カラースキームをダークモードまたはデイライトモードに変更します。
エクスポート	ダッシュボードの PDF をダウンロードします。

ダークモードをオン / オフにする

ユーザーは、ダークモードスイッチを切り替えることで、すべての画面でダークモードカラースキームを使用できます。

➡ ダークモードをオン / オフにする方法

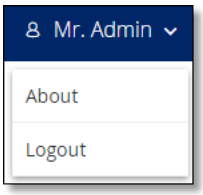
1. 画面上部の **[ダークモード]** ボタン  をクリックして、ダークモードをオンにします。
   設定がすべての画面に適用され、**[デイライトモード]** ボタン  が表示されます。
2. デイライトモード設定に戻すには、**[デイライトモード]** ボタンをクリックします。

現在のソフトウェアバージョンの確認

ユーザーは、ヘッダーバーの右上にあるユーザー名ボタンを使用して、ソフトウェアのバージョンを確認できます。

➡ 現在のソフトウェアバージョンの表示手順

1. メインのヘッダーバーで、右上隅のユーザー名ボタンをクリックしてメニューを開きます。
   

   ユーザーメニューが表示されます。
   

2. メニューで、**[バージョン情報]** をクリックします。
   現在のソフトウェアのバージョンが表示されます。
   

メイン画面

UI にはいくつかのメイン画面があり、**メインナビゲーション**からアクセスできます。以下は、各種画面の簡単な説明です。各画面については、続く章でさらに詳しく説明します。

- **ダッシュボード** - ネットワークのインベントリとセキュリティ体制を一目で確認できるグラフとテーブルを含むウィジェットを表示します。*リスク*、*インベントリ*、*イベントとポリシー*にそれぞれ個別のダッシュボードがあります。**ダッシュボード**の章を参照してください。
- **イベント** - ポリシーヒットの結果として、システムで発生したすべてのイベントが表示されます。*すべてのイベント*を表示する画面と、特定のタイプ(構成イベント、SCADA イベント、ネットワーク脅威、ネットワークイベント)のイベントを表示するための個別の画面があります。**イベント**の章を参照してください。
- **ポリシー** - システムのポリシーを表示、編集、アクティブ化します。**ポリシー**の章を参照してください。
- **インベントリ** - 検出されたすべての資産のインベントリが表示されるため、包括的な資産管理、各資産の状況の監視、関連するイベントの表示が可能になります。*すべての資産*を表示する画面と、特定のタイプの資産(*コントローラーとモジュール*、*ネットワーク資産*、*IoT*)を表示する個別の画面があります。**インベントリ**の章を参照してください。
- **ネットワークマップ** - ネットワーク資産とその接続を視覚的に表示します。
- **脆弱性** - Tenable.ot プラグインによって検出された、ネットワーク内におけるすべての脅威の詳細なリストを表示し、推奨される修正手順を提供します。このセクションには、CVE およびネットワークの資産に対するその他の脅威が含まれます(旧式のオペレーティングシステム、脆弱なプロトコルの使用、脆弱なオープンポートなど)。
- **ネットワーク** - ネットワーク内の資産間で行われた会話に関するデータの推移を表示することで、ネットワークトラフィックの包括的なビューを提供します。 **ネットワーク**の章を参照してください。
  この情報は、3 つの別々の画面に表示されます。
  - **ネットワークサマリー** - ネットワークトラフィックの概要を表示します。
  - **パケットキャプチャ** - ネットワークトラフィックのフルパケットキャプチャを表示します。
  - **会話** - ネットワークで検出されたすべての会話のリストを、発生した時刻、関連する資産などの詳細とともに表示します。
- **グループ** - ポリシー構成で使用されるグループを表示、作成、編集します。**グループ**の章を参照してください。
- **ローカル設定** - システム設定を表示および構成します。**ローカル設定**の章を参照してください。

リストの操作

さまざまな Tenable.ot 画面が、各画面に関連するデータを、テーブル形式で各項目のリストとともに表示します。これらのテーブルには標準化されたカスタマイズ機能があり、ユーザーは関連情報に簡単にアクセスできます。以下のセクションでは、カスタマイズ機能について説明します。

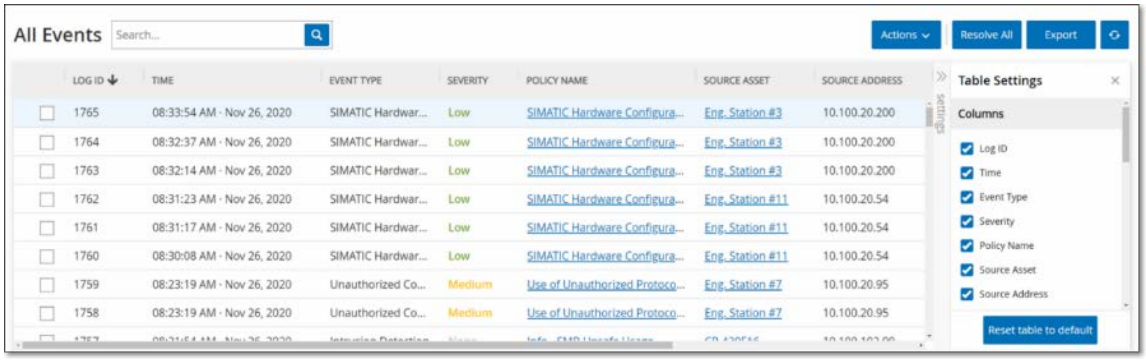
> [すべてのイベント] および [すべての資産] 画面の例が表示されていますが、UI のほとんどの画面で同様の機能を利用できます。
>
> **[設定]** > **[テーブルをデフォルトにリセット]** をクリックして、いつでもデフォルトの表示設定に戻すことができます。

列表示のカスタマイズ

表示する列とその構成方法をカスタマイズできます。

➡ 表示する列の選択手順

1. テーブルの右端にある **[設定]** タブをクリックします。
   [テーブル設定] ペインが画面の右側に表示され、**[列]** セクションが表示されます。



2. **[列]** セクションで、表示する各列の横のチェックボックスを選択します。
3. 非表示にする各列の横のチェックボックスを選択解除します。
   選択した列のみが表示されます。
4. 「**x**」(または **[設定]** タブ) をクリックして、*[テーブル設定]* ウィンドウを閉じます。

➡ 列の表示順序の調整手順

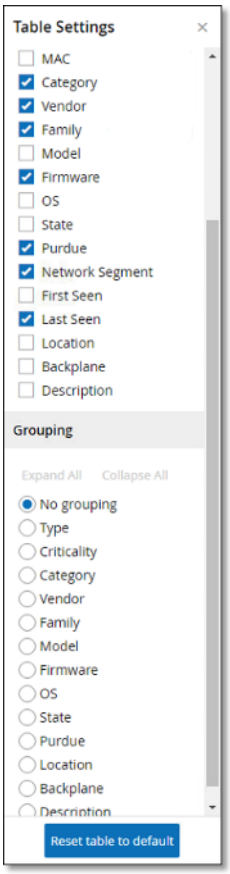
1. 列をクリックして、目的の位置にドラッグします。

グループ化

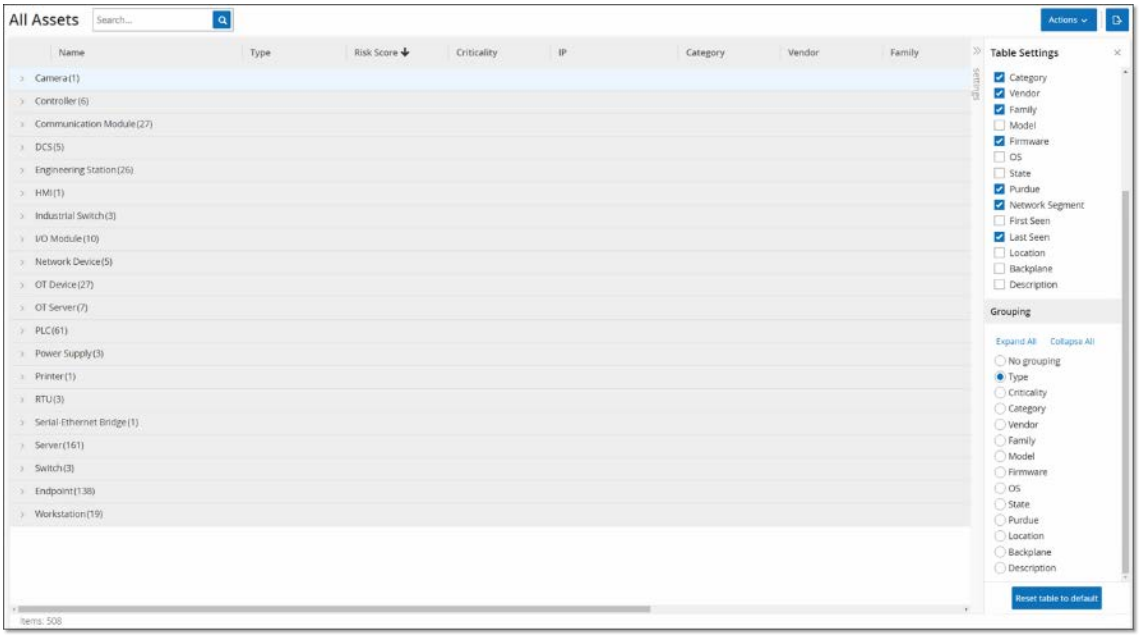
各インベントリ画面で、その特定の画面に関連する各種パラメーターによってリストをグループ化できます。

➡ リストのグループ化手順

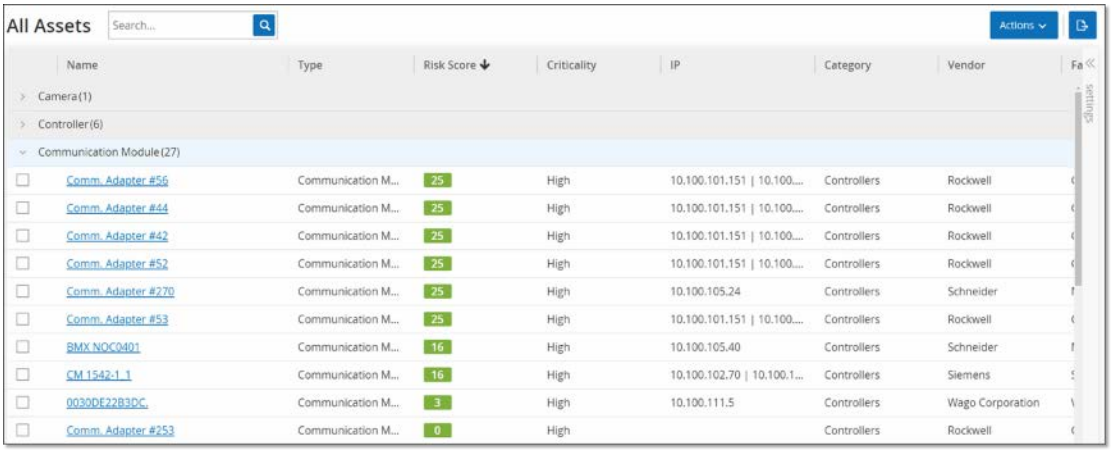
1. テーブルの右端にある **[設定]** タブをクリックします。
   [テーブル設定] ペインが画面の右側に表示され、**[列]** と **[グループ化]** セクションが表示されます。
2. **[グループ化]** セクションまでスクロールします。



3. リストをグループ化するパラメーターの横にあるラジオボタンを選択します (例 : タイプ)。
   グループカテゴリがメインウィンドウに表示されます。



4. 「**x**」(または**[設定]**タブ)をクリックして、*[テーブル設定]*ウィンドウを閉じます。
5. カテゴリの横の矢印をクリックして、そのカテゴリのすべてのインスタンスを表示します。



並べ替え

➡ リストの並べ替え手順

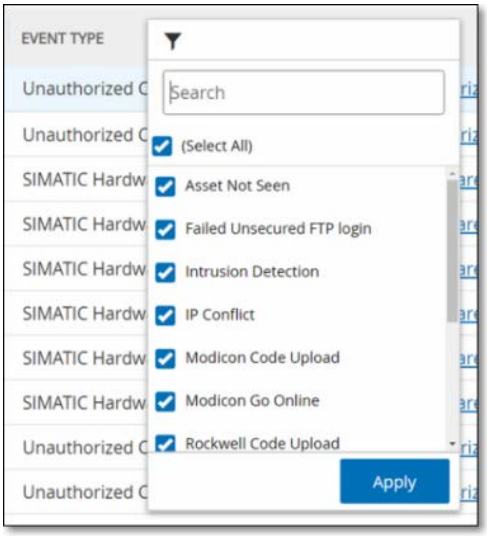
1. 列の見出しをクリックして、そのパラメーターで資産を並べ替えます(例:[**名前**]の見出しをクリックして、資産を名前のアルファベット順に表示します)。
2. 表示順序を逆にしたい場合は、列の見出しをもう一度クリックします(つまり、A → Z、Z → A)。

フィルタリング

1つ以上の列の見出しに対してフィルターを設定できます。累積的にフィルターがかかるため、すべてのフィルター基準を満たすリストのみが表示されます。フィルターオプションは各列の見出しに対して固有です。各画面には、関連するフィルターの選択肢が表示されます。たとえば、[コントローラーインベントリ]画面では、*名前*、*アドレス*、*タイプ*、*バックプレーン*、*ベンダー*などでフィルタリングできます。

➡ リストのフィルタリング手順

1. 列の見出しにカーソルを合わせて、フィルターアイコン を表示します。
2. フィルターアイコン をクリックします。
   フィルターオプションのリストが表示されます。オプションは各パラメーターに対して固有です。



3. 表示する要素を選択し、非表示にする要素の選択を解除します。

[すべて選択]チェックボックスを選択解除してから、表示する要素を選択できます。

4. フィルターのリストを検索し、フィルターを選択または選択解除できます。
5. **[適用]**をクリックします。
   リストは指定された通りにフィルターされます。
6. 列の見出しの横にあるフィルターアイコン は、結果がそのパラメーターでフィルタリングされていることを示します。

➡ フィルターの削除手順

1. フィルターアイコン をクリックします。
2. *[すべて選択]*チェックボックスをクリックして、すべての選択を解除します。
3. *[すべて選択]*チェックボックスを**もう一度**クリックして、すべての要素を選択します。
4. **[適用]**をクリックします。

検索

各画面で、特定のレコードを検索できます。

➡ リストの検索手順

1. [検索]ボックスに検索テキストを入力します。
2. アイコンをクリックします。
3. 検索テキストをクリアするには、「**x**」をクリックします。

データのエクスポート

Tenable.ot UI に表示されている任意のリスト(イベント、インベントリなど)からデータを CSV ファイルとしてエクスポートできます。

> フィルターが現在の表示に適用されている場合でも、エクスポートされたファイルにはそのページのすべてのデータが含まれます。

➡ データのエクスポート手順

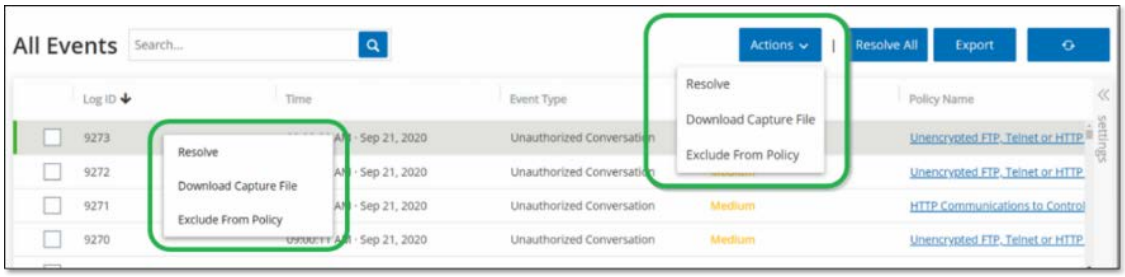
1. データをエクスポートする画面に移動します。
2. ヘッダーバーで**[エクスポート]**をクリックします。

アクションメニュー

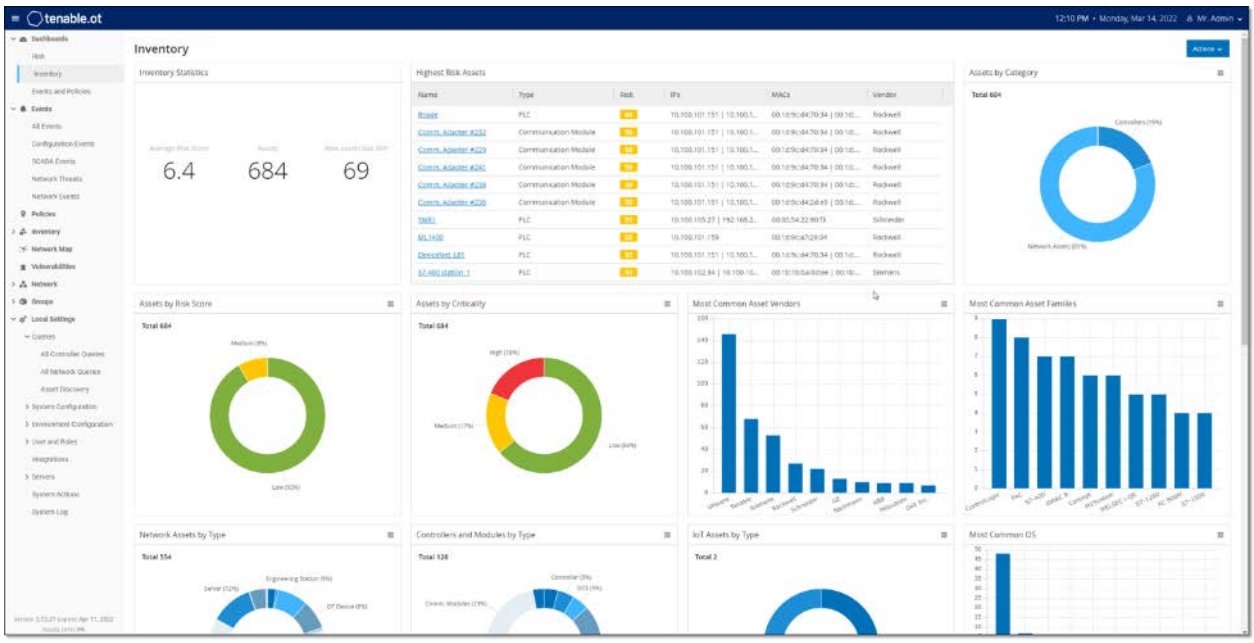
各画面には、その画面にリストされている要素に対して実行できる一連のアクションがあります。たとえば、[ポリシー]画面では、ポリシーの*表示*、*編集*、*複製*、*削除*ができます。[イベント]画面では、イベントの*解決*または*キャプチャファイルのダウンロード*ができます。

[アクション]メニューにアクセスするには、2 つの方法があります。

- 要素を選択してから、ヘッダーバーの**[アクション]**ボタンをクリック
- 要素を右クリック



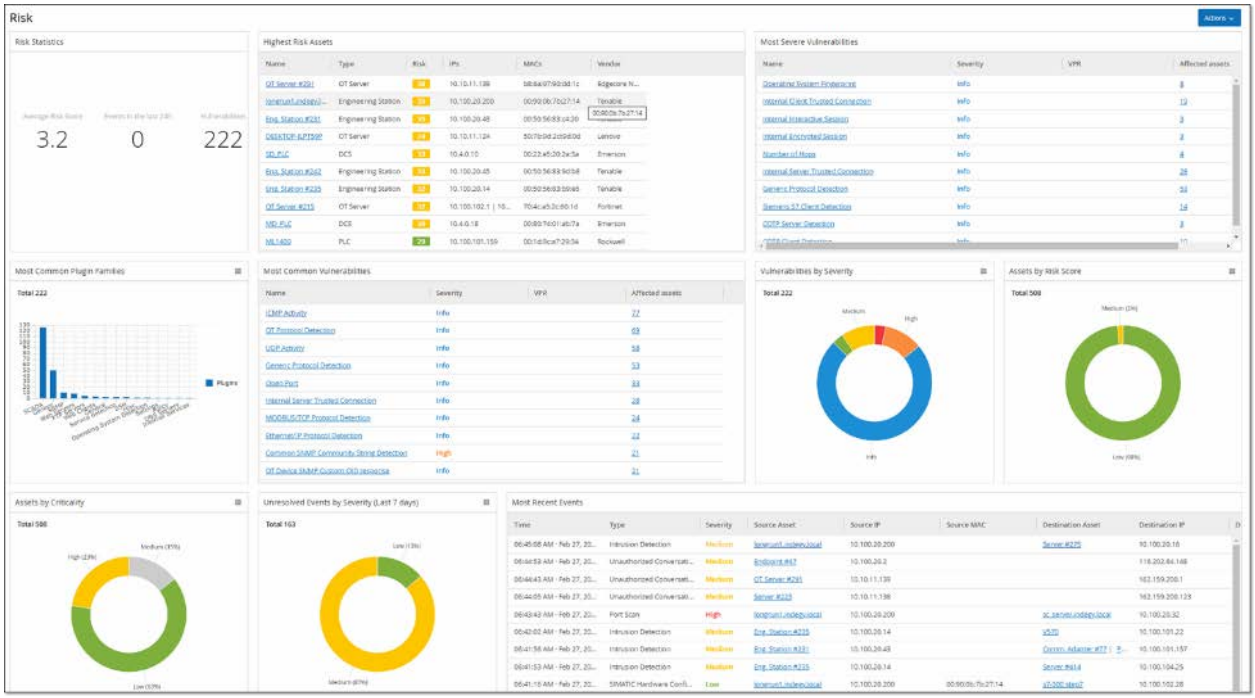
ダッシュボード



[リスク]、*[インベントリ]*、*[イベントとポリシー]*という 3 つのダッシュボードがあります。ダッシュボードには、ネットワークのインベントリとセキュリティ体制を一目で確認できるウィジェットが含まれます。ダッシュボードは、メインナビゲーションから選択するか、右上隅の**[ダッシュボード]**ボタンをクリックして表示されるメニューから選択することで、選択できます。*[リスク]*ダッシュボードは初期デフォルトビューです。デフォルトビューは別のダッシュボードに変更できます。

表示設定を調整しフィルターを設定して、ダッシュボードを操作できます。「**ダッシュボードの操作**」を参照してください。

リスクダッシュボード

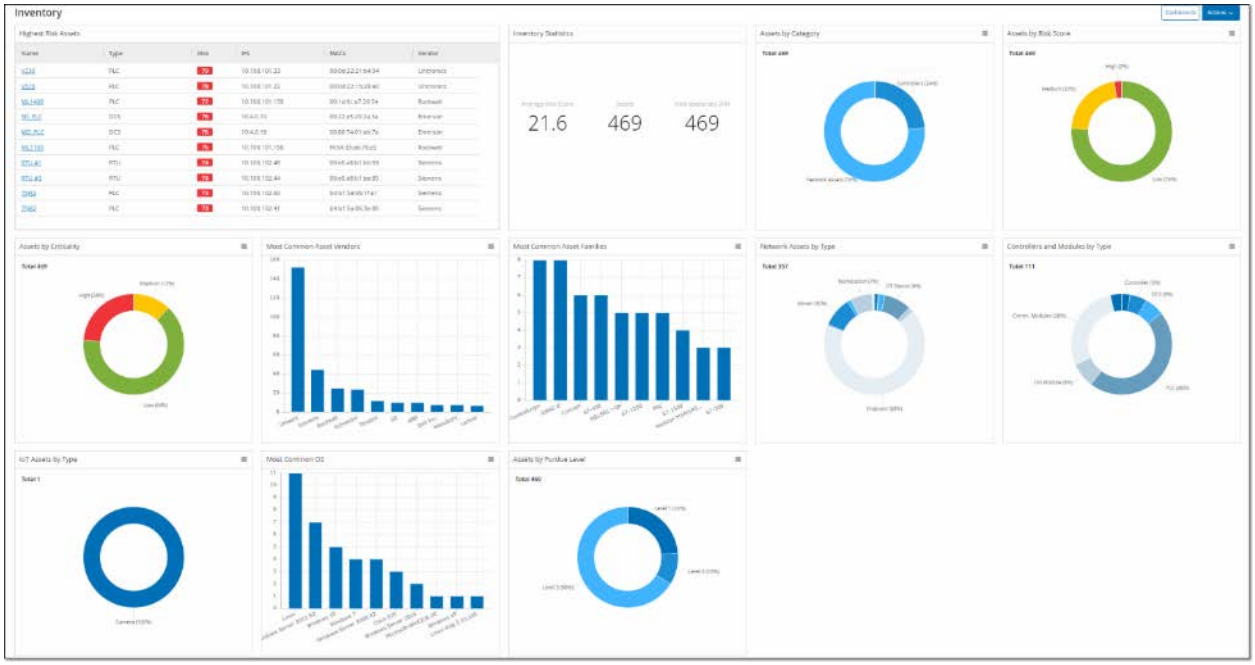


[リスク]ダッシュボードでは、資産リスクスコアと脆弱性管理指標を詳しく確認して、ネットワークのサイバー露出に関するインサイトを得られます。

[リスク]ダッシュボードには、[リスク統計]、[リスクスコア別資産]、[資産(重大度別)]、[イベント(深刻度別)]、[最も一般的な脆弱性]などのウィジェットが表示されます。

資産または脆弱性のリンクをクリックすると、それぞれ[インベントリ]または[脆弱性]画面の対応する要素に移動します。

インベントリダッシュボード

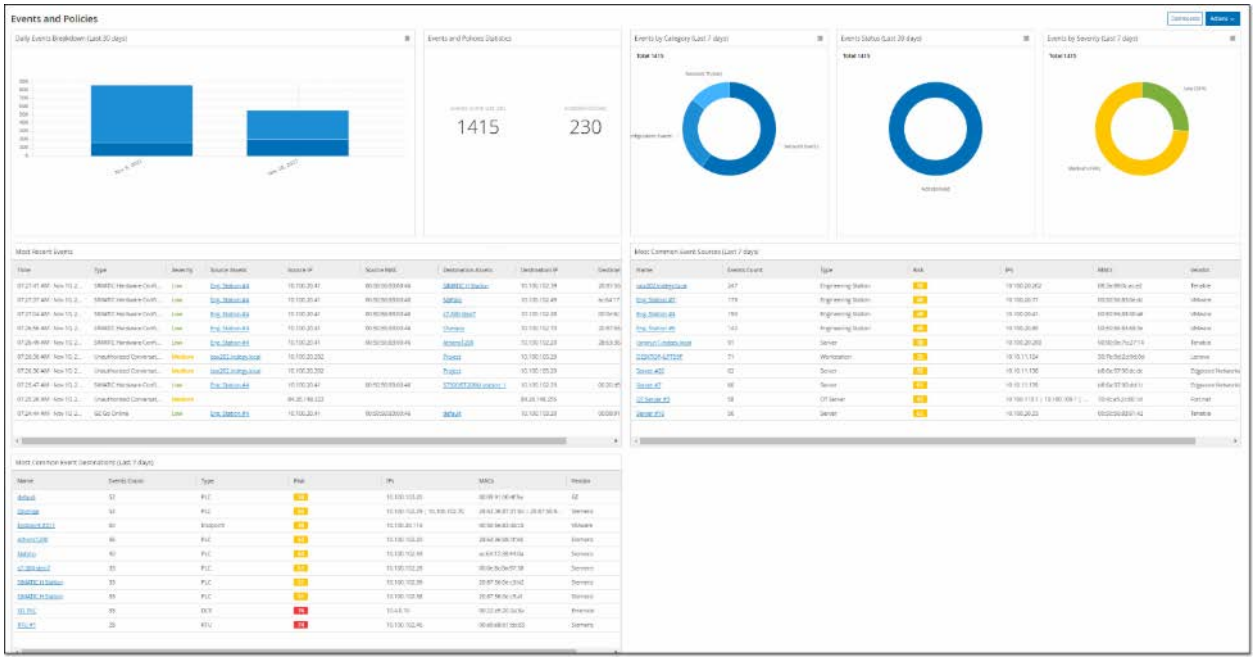


[インベントリ]ダッシュボードでは、資産インベントリを視覚的に捉え、資産の管理と追跡を容易にします。

[インベントリ]ダッシュボードには、[リスクの最も高い資産]、[インベントリ統計]、[資産(リスク別)]、[コントローラーとモジュール(タイプ別)]、[資産(パデューレベル別)]などのウィジェットが表示されます。

資産リンクをクリックすると、[インベントリ]画面の対応する資産に移動します。

イベントとポリシーダッシュボード



[イベントとポリシー]ダッシュボードでは、識別されたイベントとそれらが生成するポリシー違反を監視し、ネットワークの脅威を検出する手段を提供します。

[イベントとポリシー]ダッシュボードには、[毎日のイベントの内訳]、[イベントとポリシーの統計]、[イベントのステータス]、[最も一般的なイベントデスティネーション]などのウィジェットが表示されます。

資産またはイベントのリンクをクリックすると、それぞれ[インベントリ]または[イベント]画面の対応する要素に移動します。

ダッシュボードの操作

ウィジェットを操作することで、ダッシュボードの表示を調整できます。ダッシュボードにデータを表示するモードには、グラフとテーブルという 2 つのモードがあります。一部のウィジェットでは表示モードが固定されていますが、一部のウィジェットではモード間を行ったり来たりすることができます。右上に記号のあるウィジェットは、グラフモードまたはテーブルモードで表示できます。テーブル / グラフの記号をクリックして、モードを切り替えます。

フィルターはテーブルモードでのみ設定できます。フィルターが設定されると、グラフモードでも適用されます。

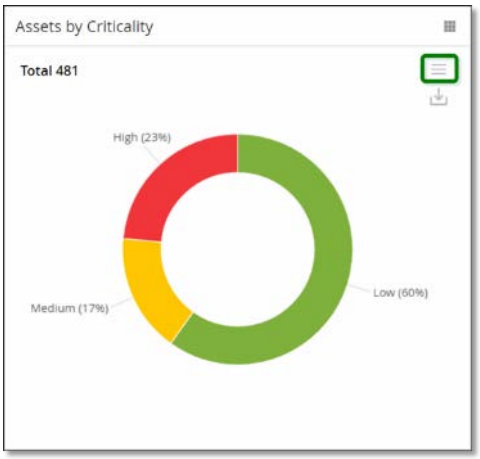
グラフモード

グラフモードは、ウィジェットデータをグラフィック表示します。

次のように、ウィジェットを操作できます。

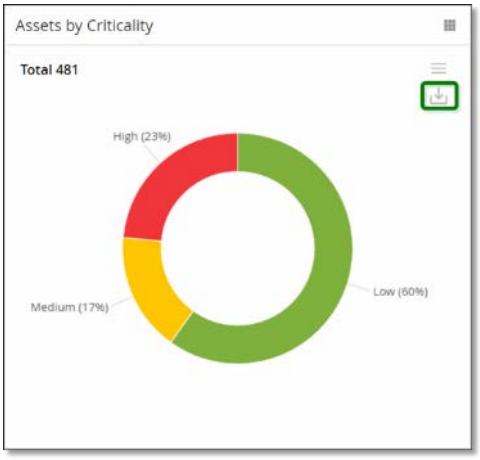
- グラフ上のポイントにカーソルを合わせると、グラフのそのセグメントに固有のデータを含むポップアップウィンドウが表示されます。

右上の**[設定]**ボタンをクリックすることで、表示に使用するチャートのタイプを調整できます。



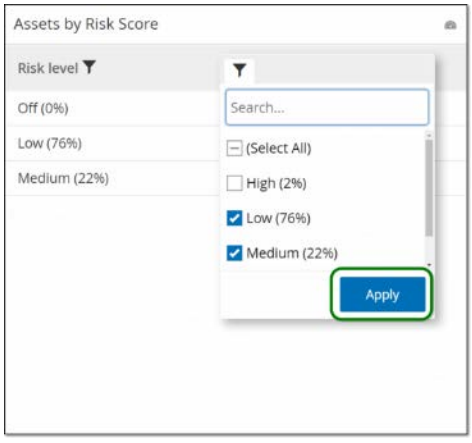
[設定]メニューから他のチャートタイプの1つを選択できます。

- グラフモードでウィジェットを表示している場合、ウィジェットにカーソルを合わせて**[ダウンロード]**アイコンをクリックすると、グラフの画像をダウンロードできます。



テーブルモード

テーブルモードでウィジェットを表示している場合、列ヘッダーにカーソルを合わせ、フィルターアイコンをクリックし、フィルターを選択してから、**[適用]**をクリックすることで、各列をフィルタリングできます。グラフモードに切り替えた場合、フィルターはグラフにも適用されます。

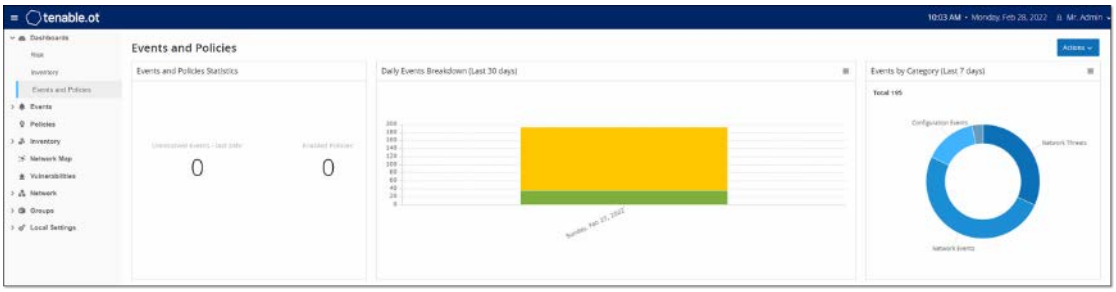


デフォルトのダッシュボードの変更

リスクダッシュボードは、管理コンソールの初期デフォルトビューです。別のダッシュボードをデフォルトビューとして表示するように指定できます。

➡ デフォルトのダッシュボードビューの変更手順

1. デフォルトビューとして設定するダッシュボードに移動します。



2. **[アクション]**>**[デフォルトにする]**をクリックします。

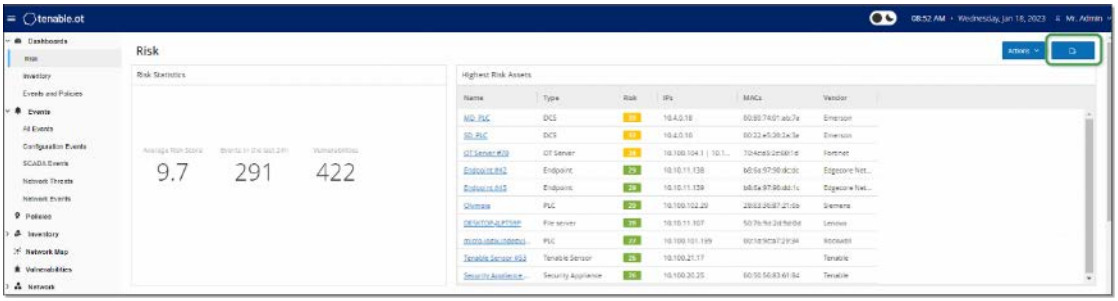
デフォルトのダッシュボードが更新されます。次回の管理コンソールアクセス時、このダッシュボードが表示されます。

ダッシュボードのエクスポート

ダッシュボード画面の[エクスポート]ボタンは、各ダッシュボードウィジェットを個別のページに表示した PDF をエクスポートします。

➡ ダッシュボードのエクスポート手順

1. ダッシュボードの右上の**[エクスポート]**ボタンをクリックします( )。



PDF はデフォルトのダウンロードフォルダに自動的にダウンロードされます。

> PDF ダウンロードの進行中 (2〜3 秒) は、ブラウザで [ダッシュボード] タブを開いたままにしてください。

2. ファイルのダウンロードが完了したら、ダウンロードしたばかりのファイルに移動して、そのファイルを表示または共有します。

ポリシー

ポリシーは、ネットワークで発生する疑わしいイベント、認証されていないイベント、異常なイベント、またはその他の特筆すべき特定のタイプのイベントを定義するために使用されます。特定のポリシーのすべての*ポリシー定義*条件を満たすイベントが発生すると、システムでイベントが生成されます。イベントがシステムに記録され、ポリシーに構成された*ポリシーアクション*に従って通知が送信されます。

ポリシーイベントには 2 つのタイプがあります。

- **ポリシーベースの検出** - 一連のイベント記述子で定義されたポリシーの条件が正確に満たされた場合にイベントをトリガーします。
- **異常検出** - ネットワークで異常または不審なアクティビティが識別されたときにイベントをトリガーします。

このシステムは、事前定義された一連のポリシーを備えています(標準装備)。さらに、事前定義されたポリシーを編集したり、新しいカスタムポリシーを定義したりする機能も用意されています。

デフォルトでは、*ほとんどの* ポリシーがオンになっています。ポリシーのオン / オフを切り替えるには、「**ポリシーのオンとオフ**」を参照してください。

ポリシーの構成

各ポリシーは、ネットワーク内における特定のタイプの動作を定義する一連の条件で構成されています。これには、アクティビティ、関連する資産、イベントのタイミングなどの考慮事項が含まれます。ポリシーで設定された**すべて**のパラメーターに適合するイベントのみが、そのポリシーのイベントをトリガーします。各ポリシーには、イベントの深刻度、通知方法、ログ記録を定義する指定されたポリシーアクション構成があります。

グループ

Tenable.ot のポリシーの定義で重要なコンポーネントは、*グループ*の使用です。ポリシーを構成する場合、各パラメーターは個々のエンティティではなくグループによって指定します。これにより、ポリシー構成プロセスが大幅に合理化されます。たとえば、*ファームウェアの更新*というアクティビティが 1 日の特定の時間(勤務時間中など)にコントローラーで実行されたときに疑わしいアクティビティと見なされる場合、ネットワーク内のコントローラーごとに個別のポリシーを作成する代わりに、資産グループ*コントローラー*に適用される単一のポリシーを作成できます。

次のタイプのグループがポリシー構成の一部として使用されます。

- **資産グループ** - システムには、資産タイプに基づいた事前定義の資産グループがあります。場所、部門、重大度などの他の要素に基づいてカスタムグループを追加できます。
- **ネットワークセグメント** - システムは、資産タイプと IP 範囲に基づいて自動生成されるネットワークセグメントを作成します。同様の通信パターンを持つ必要がある資産グループを定義するカスタムネットワークセグメントを作成できます。
- **メールグループ** - 特定のイベントのメール通知を受信する複数のメールアカウントをグループ化できます。たとえば、役割、部門などによるグループ化です。
- **ポートグループ** - 同様の方法で使用されるポートをグループ化できます。たとえば、Rockwell コントローラーで通常開いているポートなどです。
- **プロトコルグループ** - 通信プロトコルは、プロトコルのタイプ(Modbus など)、製造元(Rockwell 使用可能プロトコルなど)などでグループ化できます。
- **スケジュールグループ** - いくつかの時間範囲を、特定の共通の特性を持つスケジュールグループとしてグループ化できます。たとえば、勤務時間、週末などです。

- **タググループ** - さまざまなコントローラーで類似の操作データを含むタグをグループ化できます。たとえば、ファーネスの温度を制御するタグです。
- **ルールグループ** - ルールグループは、Suricata Signature ID (SID) で識別される関連ルールのグループで構成されます。これらのグループは、侵入検知ポリシーを定義するためのポリシー条件として使用されます。

ポリシーの定義で使用できるのは、システムで構成されたグループのみです。システムには、事前定義されたグループのセットがあります。これらのグループを編集したり、独自のグループを追加したりできます。**グループ**の章を参照してください。

> ポリシーパラメーターはグループを使用して**のみ**設定できます。ポリシーを個々のエンティティに適用する場合でも、そのエンティティのみを含むグループを構成する必要があります。

深刻度レベル

各ポリシーには、イベントをトリガーした状況によってもたらされるリスクの程度を示す特定の深刻度レベルが割り当てられています。次の表に、さまざまなイベントレベルの意味を示します。

深刻度	説明
なし	このイベントは問題ありません。
低	現時点では心配はありませんが、都合の良いときに確認する必要があります。
中	潜在的に害のあるアクティビティが発生したことに対する中程度の深刻度レベルで、都合の良いときに対処する必要があります。
高	潜在的に害のあるアクティビティが発生したことに対する深刻度の高いレベルで、すぐに対処する必要があります。

イベント通知

ポリシー条件に一致するイベントが発生すると、イベントがトリガーされます。すべてのイベントが [イベント] に表示されます (各イベントは、[ポリシー] 画面のイベントをトリガーしたポリシーの下、および [インベントリ] 画面のイベントの影響を受けた資産の下にも一覧表示されます)。さらに、ポリシーは、Syslog プロトコルおよび / または指定された電子メール受信者を使用して、イベントの通知を外部 SIEM に送信するように構成できます。

- **Syslog 通知** - Syslog メッセージは、標準キーとカスタムキーの両方がある CEF プロトコルを使用します (これらは Tenable.ot で使用するように構成されています)。Syslog 通知の解釈方法の説明については、**Tenable.ot Syslog 統合ガイド**を参照してください。
- **メール通知** - メールメッセージには、通知を生成したイベントの詳細と、脅威を緩和するために実行する必要がある手順の提案が含まれています。

ポリシーカテゴリとサブカテゴリ

ポリシーは次のカテゴリで構成されています。

- **構成イベントポリシー** - これらのポリシーは、ネットワークで発生するアクティビティに関連しています。構成イベントポリシーには 2 つのサブカテゴリがあります。
    - **コントローラーの検証** - これらのポリシーは、ネットワークのコントローラーで発生する変更に関連しています。対象となるものには、コントローラーの状態の変更や、ファームウェア、資産プロパティ、

コードブロックの変更などがあります。ポリシーは、特定のスケジュール(平日のファームウェアアップグレードなど)および / または特定のコントローラーに制限できます。

- **コントローラーアクティビティ** - これらのポリシーは、コントローラーの状態と構成に影響を与える特定のエンジニアリングコマンドに関連しています。イベントを常に生成する特定のアクティビティの定義や、イベントを生成するための一連の基準の指定が可能です。たとえば、特定のアクティビティが特定の時間や特定のコントローラーで実行された場合などです。資産、アクティビティ、スケジュールのブラックリストとホワイトリストの両方がサポートされています。

- **ネットワークイベントポリシー** - これらのポリシーは、ネットワーク内の資産および資産間の通信ストリームに関連しています。これには、ネットワークに対して追加または削除された資産が含まれます。また、ネットワークに異常なトラフィックパターンや、懸念される原因を挙げるフラグが立てられたトラフィックパターンも含まれます。たとえば、エンジニアリングステーションが、事前に構成された一連のプロトコルの一部ではないプロトコル(特定のベンダーによって製造されたコントローラーが使用するプロトコルなど)を使用してコントローラーと通信する場合、イベントがトリガーされます。これらのポリシーは、特定のスケジュールや特定の資産に制限される可能性があります。ベンダー固有のプロトコルは便宜上ベンダーごとにまとめられていますが、任意のプロトコルをポリシー定義で使用できます。
- **SCADA イベントポリシー** - これらのポリシーは、産業プロセスに害を及ぼす可能性がある設定値の変更を検出します。この種の変更は、サイバー攻撃やヒューマンエラーに起因する場合があります。
- **ネットワーク脅威ポリシー** - これらのポリシーは、署名ベースの OT/IT 脅威検出を使用して、侵入の脅威を示すネットワークトラフィックを識別します。検出は、Suricata の脅威エンジンでカタログ化されたルールに基づいています。

ポリシーのタイプ

各カテゴリおよびサブカテゴリ内には、一連の異なるタイプのポリシーがあります。システムには、各タイプの定義済みポリシーがありますが、各タイプの独自のカスタムポリシーを作成することもできます。次の表は、カテゴリ別にグループ化されたさまざまなポリシータイプを説明しています。

構成イベント - コントローラーアクティビティのイベントタイプ

*コントローラーアクティビティ*は、ネットワークで発生するアクティビティに関連しています(つまり、ネットワークの資産間に実装された「コマンド」)。コントローラーアクティビティイベントには、さまざまなタイプがあります。各タイプは、アクティビティが実行されるコントローラーのタイプ、および指定される特定のアクティビティ(Rockwell PLC の停止、SIMATIC コードのダウンロード、Modicon オンラインセッションなど)によって定義されます。

コントローラーアクティビティイベントに適用されるポリシー定義パラメーター(ポリシー条件)は、*ソース資産*、*デスティネーション資産*、*スケジュール*です。

構成イベント - コントローラー検証イベントのタイプ

次の表では、さまざまなタイプのコントローラー検証イベントについて説明します。

> 影響を受ける資産、ソース、またはデスティネーションに関連するポリシー条件は、*資産グループ*または*ネットワークセグメント*のいずれかを選択することで指定できます。

イベントタイプ	ポリシー条件	説明
キースイッチの変更	影響を受ける資産、スケジュール	物理的なキーの位置を調整することで、コントローラーの状態が変更されました(現在 Rockwell コントローラーでのみサポートされています)。

イベントタイプ	ポリシー条件	説明
状態の変化	影響を受ける資産、スケジュール	コントローラーが、ある動作状態(実行中、停止中、テストなど)から別の状態に変化しました。
ファームウェアバージョンの変更	影響を受ける資産、スケジュール	コントローラーで実行しているファームウェアに変更が加えられました。
確認されないモジュール	影響を受ける資産、スケジュール	バックプレーンから取り外された、以前に識別されたモジュールを検出します。
検出された新しいモジュール	影響を受ける資産、スケジュール	既存のバックプレーンに追加された新しいモジュールを検出します。
スナップショットの不一致	影響を受ける資産、スケジュール	コントローラーの最新のスナップショット(コントローラーに展開されたプログラムの現在の状態をキャプチャしたもの)が、そのコントローラーの以前のスナップショットと同一ではありませんでした。

ネットワークイベントのタイプ

次の表では、さまざまなタイプのネットワークイベントについて説明します。

影響を受ける資産、ソース、またはデスティネーションに関連するポリシー条件は、*資産グループ*または*ネットワークセグメント*のいずれかを選択することで指定できます。

イベントタイプ	ポリシー条件	説明
確認されない資産	確認されていない、影響を受ける資産、スケジュール	指定された時間範囲内の特定の時間帯において、ネットワークから削除された、*[影響を受ける資産]*グループで以前に特定された資産を検出します。
USB 構成の変更	影響を受ける資産、スケジュール	USB デバイスが Windows ベースのワークステーションに接続または取り外されたことを検出します。ポリシーは、指定された時間範囲内に影響を受ける資産グループの資産の変更に適用されます。
IP の競合	スケジュール	同じ IP アドレスを使用しているネットワーク内の複数の資産を検出します。これは、サイバー攻撃を示しているか、ネットワーク管理が不適切なために発生している可能性があります。ポリシーは、指定された時間範囲内に検出された IP 競合に適用されます。

イベントタイプ	ポリシー条件	説明
ネットワークベースラインの逸脱	ソース、デスティネーション、プロトコル、スケジュール	ネットワークベースラインのサンプリング中に、互いに通信しなかった資産間の新しい接続を検出します。このオプションは、システムにネットワークベースラインが設定された後にのみ利用可能です。初期ネットワークベースラインを設定したり、ネットワークベースラインを更新したりするには、**ネットワークベースラインの設定**セクションで説明されている手順に従ってください。ポリシーは、プロトコルグループからのプロトコルを使用して、指定された時間範囲内のソース資産グループの資産からデスティネーション資産グループの資産への通信に適用されます。
検出された新しい資産	影響を受ける資産、スケジュール	指定された時間範囲内にネットワークに出現する、*ソース*資産グループの指定されたタイプの新しい資産を検出します。
オープンポート	影響を受ける資産、ポート	ネットワークで新しいオープンポートを検出します。未使用のオープンポートは、セキュリティリスクをもたらす可能性があります。このポリシーは、影響を受ける資産グループの資産およびポートグループのポートに適用されます。
ネットワークトラフィックの急激な上昇	時間枠、機密性レベル、スケジュール	ネットワークトラフィック量の異常な急増を検出します。このポリシーは、指定された時間枠に関連し、指定された機密性レベルに基づく急激な上昇に適用されます。また、指定された時間範囲に制限されます。
会話の急激な上昇	時間枠、機密性レベル、スケジュール	ネットワーク内の会話数の異常な急増を検出します。このポリシーは、指定された時間枠に関連し、指定された機密性レベルに基づく急激な上昇に適用されます。また、指定された時間範囲に制限されます。
RDP 接続(認証済み)	ソース、デスティネーション、スケジュール	認証資格情報を使用してネットワークで RDP(リモートデスクトップ接続)が行われました。このポリシーは、指定された時間範囲内に*デスティネーション*資産グループの資産に接続する、*ソース*資産グループの資産に適用されます。
RDP 接続(未認証)	ソース、デスティネーション、スケジュール	認証資格情報を使用せずに、ネットワークで RDP(リモートデスクトップ接続)が行われました。このポリシーは、指定された時間範囲内に*デスティネーション*資産グループの資産に接続する、*ソース*資産グループの資産に適用されます。

イベントタイプ	ポリシー条件	説明
認証されていない会話	ソース、デスティネーション、プロトコル、スケジュール	ネットワーク内の資産間で送信された通信を検出します。このポリシーは、プロトコルグループからの *プロトコル* を使用して、指定された時間範囲内の *ソース* 資産グループの資産から *デスティネーション* 資産グループの資産へ送信される通信に適用されます。
安全でない FTP ログインの成功	ソース、デスティネーション、スケジュール	FTP は安全でないプロトコルと見なされています。このポリシーは、FTP を使用したログインの成功を検出します。
安全でない FTP ログインの失敗	ソース、デスティネーション、スケジュール	FTP は安全でないプロトコルと見なされています。このポリシーは、FTP を使用して失敗したログイン試行を検出します。
安全でない Telnet ログインの成功	ソース、デスティネーション、スケジュール	Telnet は安全でないプロトコルと見なされています。このポリシーは、Telnet を使用したログインの成功を検出します。
安全でない Telnet ログインの失敗	ソース、デスティネーション、スケジュール	Telnet は安全でないプロトコルと見なされています。このポリシーは、Telnet を使用して失敗したログイン試行を検出します。
安全でない Telnet ログイン試行	ソース、デスティネーション、スケジュール	Telnet は安全でないプロトコルと見なされています。このポリシーは、Telnet を使用したログイン試行を検出します (結果ステータスが検出されなかったログイン)。

ネットワーク脅威イベントのタイプ

次の表では、さまざまなタイプのネットワーク脅威イベントについて説明します。

影響を受ける資産、ソース、またはデスティネーションに関連するポリシー条件は、*資産グループ* または *ネットワークセグメント* のいずれかを選択することで指定できます。

イベントタイプ	ポリシー条件	説明
侵入検知	ソース、影響を受ける資産、ルールグループ、スケジュール	侵入検出ポリシーポリシーは、署名ベースの OT/IT 脅威検出を使用して、侵入の脅威を示すネットワークトラフィックを識別します。検出は、Suricata の脅威エンジンでカタログ化されたルールに基づいています。このルールは、カテゴリ (例: ICS 攻撃、サービス拒否、マルウェアなど) とサブカテゴリ (例: ICS 攻撃 - Stuxnet、ICS 攻撃 - Black Energy など) にグループ化されます。システムには、関連ルールの事前定義グループのセットがあります。さまざまなルールの独自のカスタムグループを構成することもできます。

イベントタイプ	ポリシー条件	説明
ARP スキャン	影響を受ける資産、スケジュール	ネットワークで実行されている ARP スキャン(ネットワーク偵察アクティビティ)を検出します。このポリシーは、指定された時間範囲内に*影響を受ける*資産グループでブロードキャストされた効果を持つスキャンに適用されます。
ポートスキャン	ソース資産、デスティネーション資産、スケジュール	オープン(脆弱)ポートを検出するためのネットワークで実行されている SYN スキャン(ネットワーク偵察アクティビティ)を検出します。このポリシーは、指定された時間範囲内のソース資産グループの資産からデスティネーション資産グループの資産への通信に適用されます。

SCADA イベントのタイプ

次の表では、さまざまなタイプの SCADA イベントについて説明します。

> 影響を受ける資産、ソース、またはデスティネーションに関連するポリシー条件は、*資産グループ*または*ネットワークセグメント*のいずれかを選択することで指定できます。

イベントタイプ	ポリシー条件	説明
Modbus の不正なデータアドレス	ソース資産、デスティネーション資産、スケジュール	Modbus プロトコルの「不正なデータアドレス」エラーコードを検出します。このポリシーは、指定された時間範囲内のソース資産グループの資産からデスティネーション資産グループの資産への通信に適用されます。
Modbus の不正なデータ値	ソース資産、デスティネーション資産、スケジュール	Modbus プロトコルの「不正なデータ値」エラーコードを検出します。このポリシーは、指定された時間範囲内のソース資産グループの資産からデスティネーション資産グループの資産への通信に適用されます。
Modbus の不正な関数	ソース資産、デスティネーション資産、スケジュール	Modbus プロトコルの「不正な関数」エラーコードを検出します。このポリシーは、指定された時間範囲内のソース資産グループの資産からデスティネーション資産グループの資産への通信に適用されます。

イベントタイプ	ポリシー条件	説明
承認されていない書き込み	ソース資産、タググループ、タグ値、スケジュール	指定のソース資産グループのコントローラー(現在 Rockwell および S7 コントローラーがサポートされています)上の指定のタグへの承認されていないタグ書き込みを検出します。このポリシーは、新しい書き込み、指定値からの変更、または指定範囲外の値を検出するように構成できます。このポリシーは、指定された時間範囲にのみ適用されます。
ABB - 承認されていない書き込み	ソース資産、デスティネーション資産、スケジュール	MMS 経由で ABB 800xA コントローラーに送信される、許可された範囲外の書き込みコマンドを検出します。
IEC 60870-5-104 コマンド(データ転送の開始 / 停止、問い合わせコマンド、カウンター問い合わせコマンド、クロック同期コマンド、プロセスリセットコマンド、時間タグ付きテストコマンド)	ソース資産、デスティネーション資産、スケジュール	リスクがあると考えられる IEC-104 マスターまたはスレーブユニットに送信された特定のコマンドを検出します。
DNP3 コマンド	ソース資産、デスティネーション資産、スケジュール	DNP3 プロトコルを使用して送信されたすべてのメインコマンドを検出します(例: 選択、操作、ウォーム / コールド再起動)。また、サポートされていない関数コードやパラメーターエラーなどの内部インジケーターに起因するエラーも検出します。

ポリシーのオンとオフの切り替え

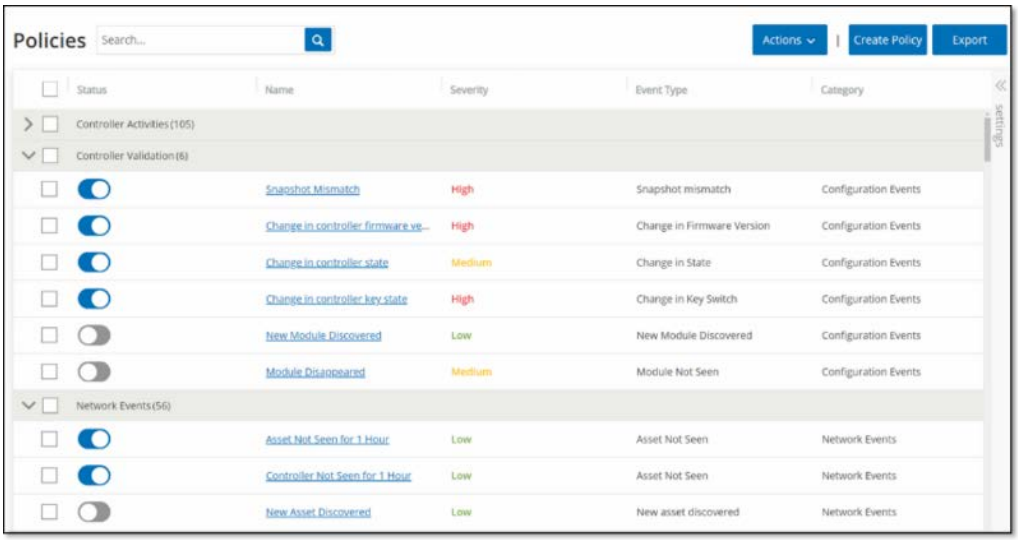
システムですでに構成済みのポリシー(事前構成済みとユーザー定義済みの両方)を簡単にオンまたはオフにできます。一つ一つのポリシーのオン / オフを切り替えたり、複数のポリシーを選択して一括処理でオン / オフを切り替えたりすることができます。

多くのポリシーは、データを収集するためのクエリの使用に依存しています。クエリ機能の一部またはすべてが無効の場合、関連するポリシーは有効になりません。**[ローカル設定]** > **[クエリ]** に移動すると、クエリをアクティブ化できます。

クエリを参照してください。

ポリシーのオン / オフ手順

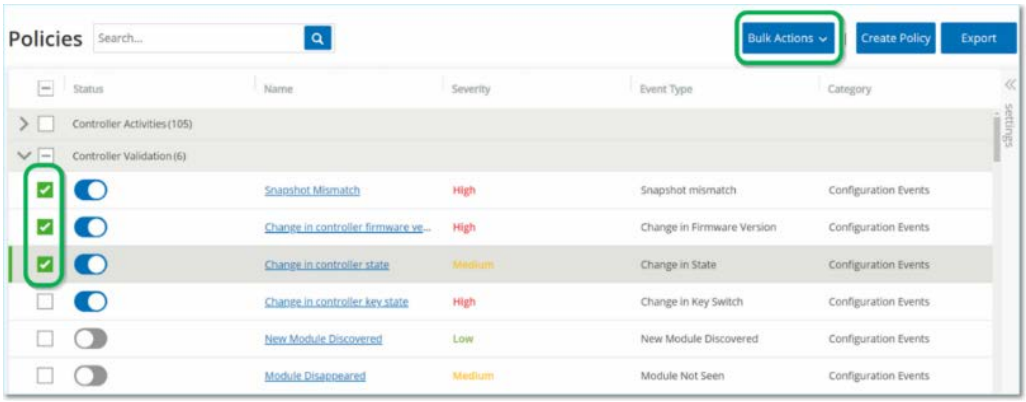
1. **[ポリシー]**画面に移動します。
   システムで構成されている各ポリシーのリストが表示されます。ポリシーリストはポリシーカテゴリごとにグループ化されています。



2. 関連する[ポリシーの**オン / オフ**]の横の**[ステータス]**スイッチを切り替えます。

複数のポリシーのオン / オフ手順

1. **[ポリシー]**画面に移動します。
   システムで構成されている各ポリシーのリストが表示されます。ポリシーリストはポリシーカテゴリごとにグループ化されています。



2. オン / オフを切り替えたい各ポリシーの横にあるチェックボックスを選択します。次の選択方法のいずれかを実行します。
   - **個々のポリシーを選択** - 特定のポリシーの横にあるチェックボックスをクリックします。
   - **ポリシータイプを選択** - [ポリシータイプ]の見出しの横のチェックボックスをクリックします。
   - **すべてのポリシーを選択** - テーブルの上部にあるタイトルバーのチェックボックスをクリックします。
3. ヘッダーバーの**[一括アクション]**ボタンをクリックします。
4. ドロップダウンリストから目的のアクション([**有効**]または[**無効**])を選択します。
   選択したすべてのポリシーがオン / オフになります。

ポリシーの表示

[**ポリシー**]画面には、システムで構成されている各ポリシーのリストが表示されます。リストは、ポリシーカテゴリごとに別々のタブでグループ化されています。事前に構成されたポリシーとユーザー定義のポリシーの両方がこの画面に一覧表示されます。各ポリシーのリストには、ポリシーの現在のステータスを示すトグルスイッチと、ポリシー構成を示すいくつかのパラメーターが含まれています。

列を表示 / 非表示にしたり、資産リストをソートおよびフィルタリングしたり、キーワードを検索したりできます。カスタマイズ機能の説明については、**リスト**を参照してください。

次の表で、ポリシーパラメーターについて説明します。

パラメーター	説明
ステータス	ポリシーがオンかオフかを示します。生成するイベントが多すぎるためにポリシーがシステムによって自動的に無効にされた場合、警告アイコンが表示されます。 ステータススイッチを切り替えて、ポリシーをオン / オフにします。
ポリシー ID	システム内のポリシーの一意の識別子。ポリシー ID は、カテゴリごとに異なるプレフィックスを持つカテゴリ別にグループ化されます (例 : コントローラーアクティビティの P1、ネットワークイベントの P2 など)。
名前	ポリシーの名前。
深刻度	イベントの深刻度。可能な値は、なし、低、中、高です。**深刻度レベル**の説明については、「深刻度レベル」セクションを参照してください。
イベントタイプ	このイベントポリシーをトリガーするイベントの特定のタイプ。
カテゴリ	このイベントポリシーをトリガーするイベントのタイプの一般カテゴリ。可能な値は、構成、SCADA、ネットワーク脅威、ネットワークイベントです。各種カテゴリの説明については、**ポリシーカテゴリとサブカテゴリ**を参照してください。
ソース	ポリシー条件。ポリシーが適用されるソース資産グループ / ネットワークセグメント (アクティビティを開始した資産) です。
デスティネーション / 影響を受ける資産	ポリシー条件。ポリシーが適用されるデスティネーション資産グループ / ネットワークセグメント (アクティビティを受け取る資産) です。単一の資産 (ソースとデスティネーションを指定しない) を含むポリシーの場合、このパラメーターはイベントの影響を受けた資産を表示します。
スケジュール	ポリシー条件。ポリシーが適用される時間範囲です。
Syslog	このポリシーのイベントが記録される Syslog サーバー (SIEM)。
メール	このポリシーのイベント通知が送信される E メールグループ。
サブカテゴリ	イベントのサブカテゴリ分類。*構成イベント*のカテゴリは、*コントローラーアクティビティ*や*コントローラーの検証*といったサブカテゴリで構成されています。各種サブカテゴリの説明については、**ポリシーカテゴリとサブカテゴリ**を参照してください。

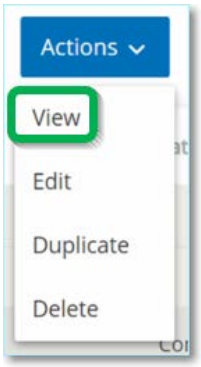
パラメーター	説明
ポリシーあたりのイベント数	それぞれのポリシーによって生成されたイベント数の一覧表示。列をクリックすると、リストをソートして、違反 / イベントが最も多いポリシーに焦点を当てることができます。
除外	各ポリシーに追加された除外の数の一覧表示。詳細については、**ポリシー除外の作成**を参照してください。

ポリシーの詳細の表示

ポリシーの [ポリシーの詳細] 画面を開いて、ポリシーに関する追加の詳細を表示できます。この画面には、すべてのポリシー条件の完全なリストが表示されます。選択したポリシーによってトリガーされたすべてのイベントのリストも表示されます。

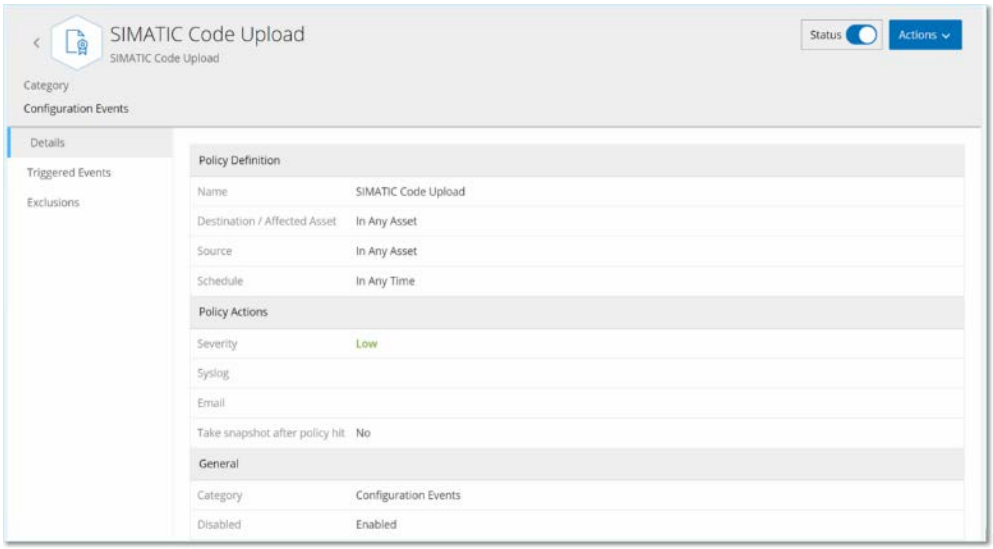
➡ 特定のポリシーの [ポリシーの詳細] 画面を開く手順

1. **[ポリシー]** 画面で、目的のポリシーを選択します。
2. **[アクション]** メニューをクリックし、ドロップダウンリストから **[表示]** を選択します。



> または、関連するポリシーを右クリックして [アクション] メニューにアクセスすることもできます。

選択したポリシーの [ポリシーの詳細] 画面が表示されます。



[ポリシーの詳細]画面には、以下の要素があります。

- **ヘッダーバー** - ポリシーの名前、タイプ、カテゴリが表示されます。また、ポリシーのオン / オフを切り替えるトグルスイッチと、利用可能なアクション(編集、複製、削除)のドロップダウンリストもあります。
- **[詳細]タブ** - 次の 3 つのセクションでポリシー構成の詳細を表示します。
    - **ポリシー定義** - すべてのポリシー条件を表示します。これには、そのポリシータイプのすべての関連フィールドが含まれます。
    - **ポリシーアクション** - 深刻度レベルとイベント通知の宛先(Syslog、E メール)を表示します。また、*初回ヒット後に無効化*機能がアクティブ化されているかどうかを示します。
    - **一般** - ポリシーのカテゴリとステータスを表示します。
- **[トリガーされたイベント]タブ** - このポリシーによってトリガーされたイベントのリストが表示されます。イベントごとに、イベントに関連する資産およびイベントの性質に関する情報が表示されます。このタブに表示される情報は、指定したポリシーのイベントのみがここに表示されることを除いて、**イベント画面に表示される情報と同じ**です。イベント情報の説明については、**イベントの表示**を参照してください。**[除外]タブ** - ポリシーが、セキュリティ脅威をもたらさない特定の条件に対してイベントを生成していることが判明した場合は、それらの条件をポリシーから*除外*できます(これらの特定の条件に対するイベントの生成を停止できます)。これは[イベント]画面で行われます。**ポリシー除外の作成**を参照してください。[除外]タブには、このポリシーに適用されているすべての除外が表示され、除外ごとに、除外された特定の条件が表示されます。このタブから、除外を削除できます(指定した条件でイベントの生成を再開できるようにします)。

ポリシーの作成

ICS ネットワークの特定の考慮事項に基づいて、カスタムポリシーを作成できます。どのタイプのイベントをスタッフに通知するか、通知をどのように配信するかを正確に決定できます。各ポリシーに与える定義の程度をどれほど特定または広範なものにするかについて、完全な柔軟性があります。

ポリシーの定義は、システムで構成されたグループを使用して行います。特定のパラメーターのドロップダウンリストにポリシーを適用したい特定のグループ化が表示されない場合は、必要に応じて新しいグループを作成できます。グループを参照してください。

新しいポリシーを作成する場合、まず作成したいポリシーの*カテゴリ*と*タイプ*を選択します。*[ポリシー作成]*ウィザードがセットアッププロセスをガイドします。各ポリシータイプには、関連するポリシー条件パラメーターの独自のセットがあります。[ポリシー作成]ウィザードは、選択したポリシーのタイプの関連するポリシー条件パラメーターを表示します。

ソース、*デスティネーション*、*スケジュール*のパラメーターでは、指定したグループをホワイトリストに入れるかブラックリストに入れるかを指定できます。

- **[含む]**を選択して、指定したグループをホワイトリストに追加(つまり、ポリシーに含める)、または
- **[含まない]**を選択して、指定したグループをブラックリストに追加(つまり、ポリシーから除外)

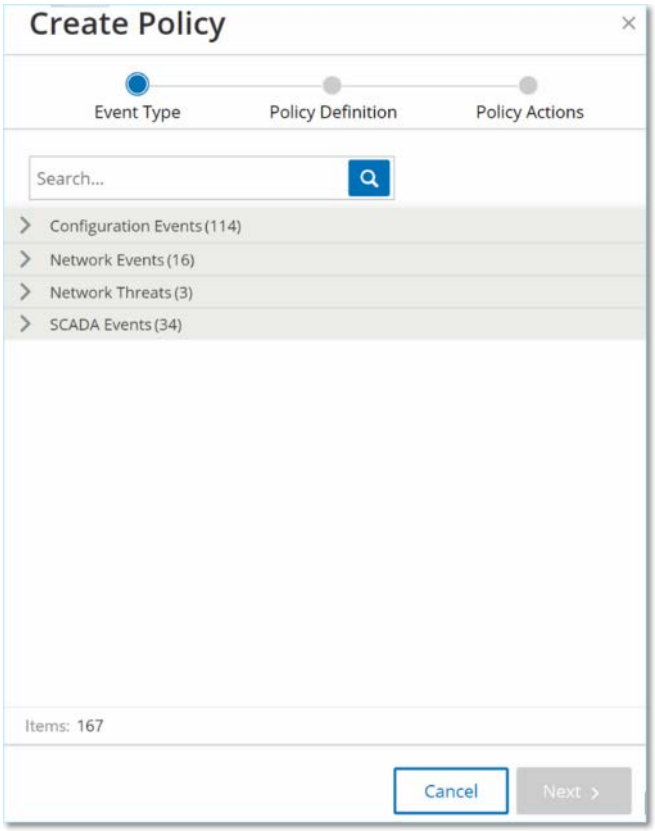
資産グループとネットワークセグメントのパラメーター(例:*ソース*、*デスティネーション*、*影響を受ける資産*)では、論理演算子(AND/OR)を使用して、事前定義されたグループのさまざまな組み合わせまたはサブセットにポリシーを適用できます。たとえば、*ICS デバイス*または *ICS サーバー*のいずれかのデバイスにポリシーを適用する場合は、[*ICS デバイス*]**または**[*ICS サーバー*]を選択します。ポリシーを*工場 A* にある*コントローラーのみに適用する場合は、コントローラーと工場 A デバイスを選択します*。

既存のポリシーと同様のパラメーターで新しいポリシーを作成したい場合は、元のポリシーを*複製*して必要な変更を行うことができます。「**ポリシーの複製**」のセクションを参照してください。

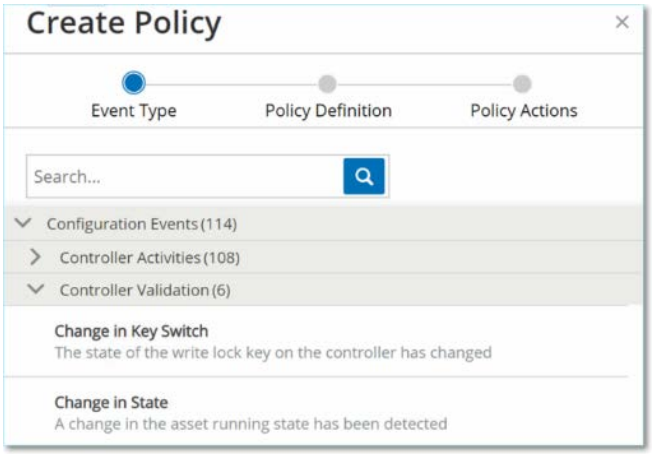
> ポリシーを作成した後、注意を必要としない状況でポリシーがイベントを生成していることが判明した場合は、ポリシーから特定の条件を除外できます。**ポリシー除外の作成**を参照してください。

新しいポリシーの作成手順

1. **[プロパティ]**画面で、**[ポリシーの作成]**をクリックします。
   [ポリシーの作成]ウィザードが開きます。

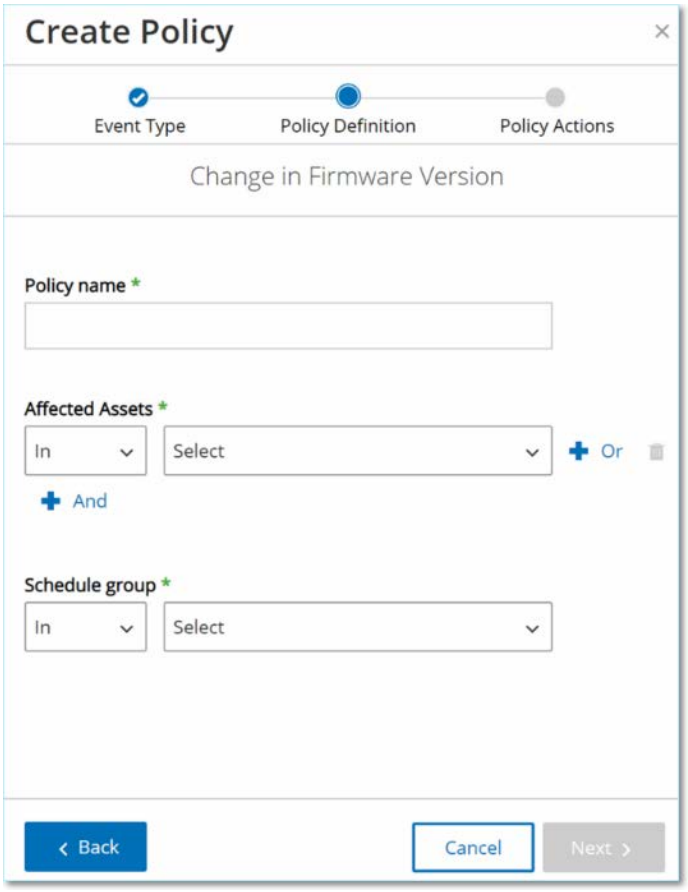


2. **[ポリシーカテゴリ]**をクリックして、サブカテゴリおよび / またはポリシータイプを表示します。
   そのカテゴリに含まれるすべてのサブカテゴリおよび / またはタイプのリストが表示されます。



3. [ポリシーのタイプ]を選択します。
4. **[次へ]**をクリックします。
   ポリシーを定義するための一連のパラメーターが表示されます。これには、選択したポリシータイプに関連する

すべてのポリシー条件が含まれます。

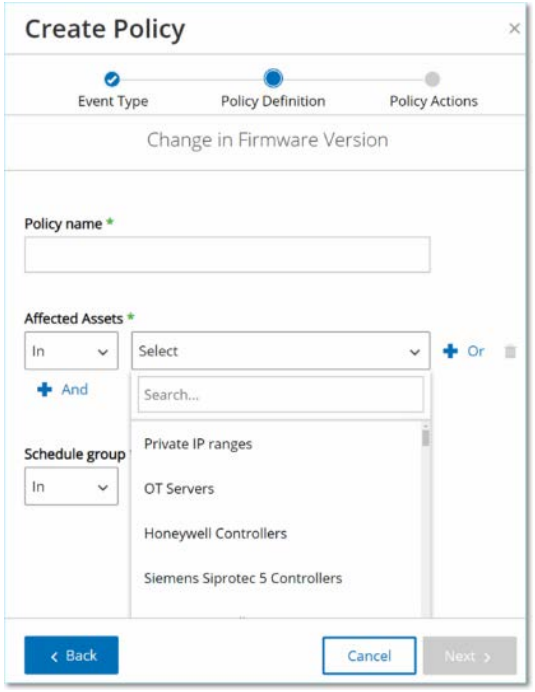


5. **[ポリシー名]**フィールドに、このポリシーの名前を入力します。

> ポリシーに検出させるイベントのタイプに関する特定の性質を説明する名前を選択してください。

6. 表示される各パラメーターについて:
    a. 必要に応じて、選択した要素をホワイトリストに追加するには**[含める]**(デフォルト)を、選択した要素をブラックリストに追加するには**[含まない]**を選択します。

b. **[選択]**をクリックします。
関連する要素(資産グループ、ネットワークセグメント、ポートグループ、スケジュールグループなど)のドロップダウンリストが表示されます。



c. 目的の要素を選択します。

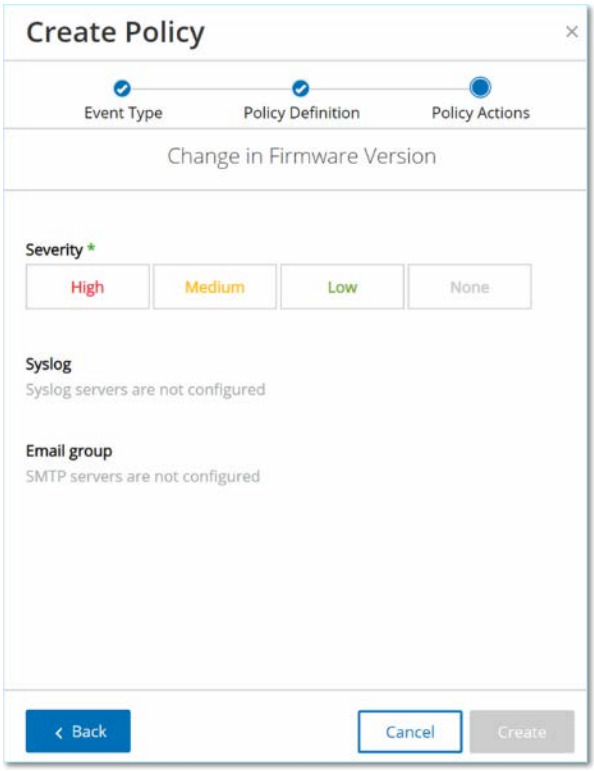
> 希望するポリシーの適用に最適なグループ化が存在しない場合は、必要に応じて新しいグループを作成できます。**グループ**を参照してください。

d. 資産パラメーター(例: *ソース*、*デスティネーション*、*影響を受ける資産*)で、「Or」条件を使って資産グループ / ネットワークセグメントを追加したい場合は、フィールドの横にある青い**[+ Or]**ボタンをクリックし、別の資産グループ / ネットワークセグメントを選択してください。

e. 資産パラメーター(例: *ソース*、*デスティネーション*、*影響を受ける資産*)で、「And」条件を使って資産グループ / ネットワークセグメントを追加したい場合は、フィールドの下にある青い**[+ And]**ボタンをクリックし、別の資産グループ / ネットワークセグメントを選択してください。

7. すべてのフィールドに入力したら、**[次へ]**をクリックします。
一連のポリシーアクションパラメーター(つまり、ポリシーヒットが発生したときにシステムによって実行され

るアクション)が表示されます。



8. **[深刻度]**セクションで、このポリシーに設定する深刻度レベルをクリックします。
9. イベントログを 1 つ以上の Syslog サーバーに送信する場合は、**[Syslog]**セクションで、イベントログを送信する各サーバーの横にあるチェックボックスを選択します。

> Syslog サーバーを追加するには、**Syslog サーバー**を参照してください。

10. イベントのメール通知を送信する場合は**[E メールグループ]**フィールドで、ドロップダウンリストから通知する E メールグループを選択します。

> SMTP サーバーを追加するには、**SMTP サーバー**を参照してください。

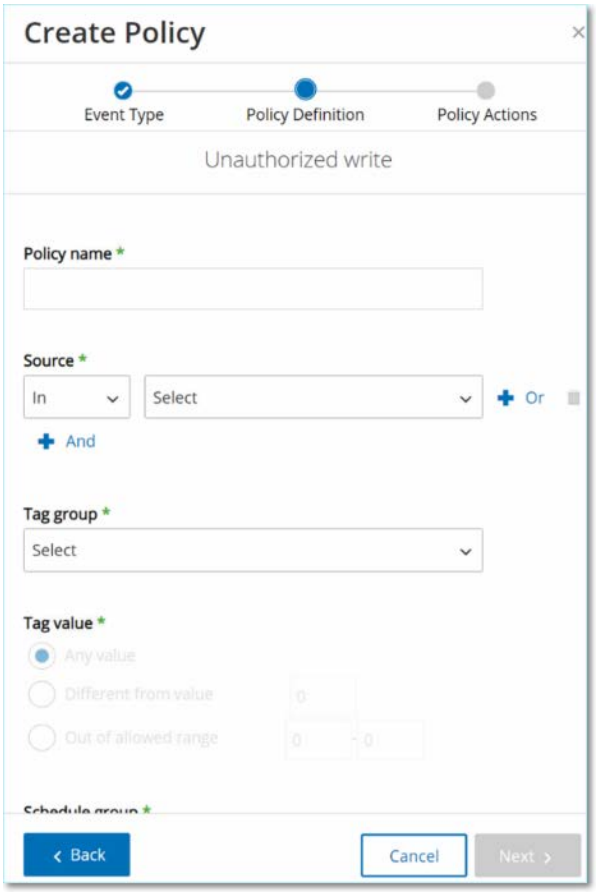
11. **[その他のアクション]**セクションで、指定されたアクションが関連している場合
    - ポリシーヒットが初めて発生した後にポリシーを無効にしたい場合は、**[初回ヒット後にポリシーを無効化]**チェックボックスを選択します(このアクションは、一部のタイプのネットワークイベントポリシーおよび一部のタイプの SCADA イベントポリシーに関連しています)。
    - ポリシーヒットが検出されるたびに、影響を受ける資産の自動スナップショットを開始したい場合は、**[ポリシーヒット後にスナップショットを作成]**チェックボックスを選択します(このアクションは、一部のタイプの*構成イベント*ポリシーに関連しています)。
12. すべてのフィールドに入力したら、**[作成]**をクリックします。
    新しいポリシーが作成され、自動的にアクティブ化されます。ポリシーが[ポリシー]画面のリストに表示されます。

承認されていない書き込みポリシーの作成

このタイプのポリシーは、コントローラータグへの承認されていない書き込みを検出します。ポリシー定義では、関連するタググループとポリシーヒットを生成する書き込みのタイプを指定する必要があります。

承認されていない書き込みポリシーへのポリシー定義の設定手順

1. **ポリシーの作成**の説明に従って、新しい承認されていない書き込みポリシーを作成します。



2. [ポリシー定義]セクションの**[タググループ]**フィールドで、このポリシーが適用されるタググループを選択します。
3. [**タグ値**]セクションで、ラジオボタンをクリックして希望のオプションを選択し、必要なフィールドに入力します。オプションは次のとおりです。
   - **任意の値** - このオプションを選択すると、タグ値へのすべての変更を検出します。
   - **異なる値** - このオプションを選択すると、指定した値以外のすべての値を検出します。この選択肢の横にあるフィールドに、指定した値を入力します。
   - **許容範囲外** - このオプションを選択すると、指定された範囲外のすべての値を検出します。この選択肢の横にある許容範囲の下限と上限のそれぞれのフィールドに、値を入力します。

> *[異なる値]* と *[許容範囲外]* オプションは、標準のタグタイプ (整数、ブール値など) でのみ利用でき、カスタマイズされたタグや文字列では利用できません。

4. **ポリシーの作成**の説明に従って、ポリシー作成手順を完了します。

ポリシーに対するその他のアクション

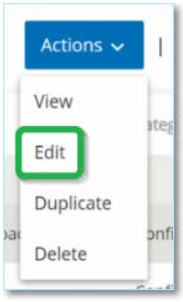
ポリシーの編集

定義済みのポリシーとユーザー定義ポリシーの両方の構成を編集できます。ほとんどのポリシーでは、ポリシー定義パラメーター(ポリシー条件)とポリシーアクションパラメーターの両方を調整できます。侵入検知ポリシーの場合、調整できるのはポリシーアクションパラメーターのみです。

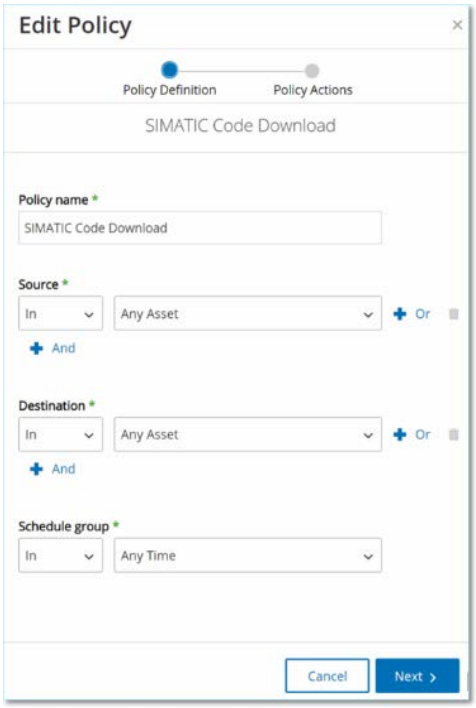
一括アクションで、複数のポリシーのポリシーアクションパラメーターを編集することもできます。

➡ ポリシーの編集手順

1. **[ポリシー]**画面で、目的のポリシーの横にあるチェックボックスを選択します。
2. **[アクション]**メニューをクリックし、ドロップダウンリストから**[編集]**を選択します。



現在の構成が入力された**[ポリシーの編集]**画面が表示されます。

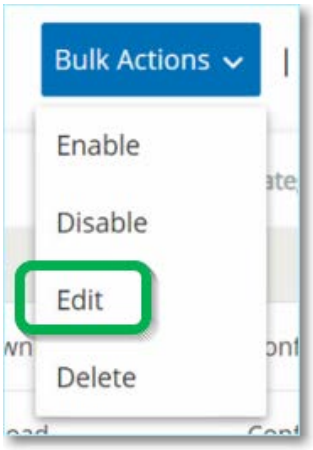


3. 必要に応じて、*ポリシー定義*パラメーターを調整します。
4. **[次へ]**をクリックします。
5. 必要に応じて、*ポリシーアクション*パラメーターを調整します。
6. **[保存]**をクリックします。
   ポリシーが新しい構成で保存されます。

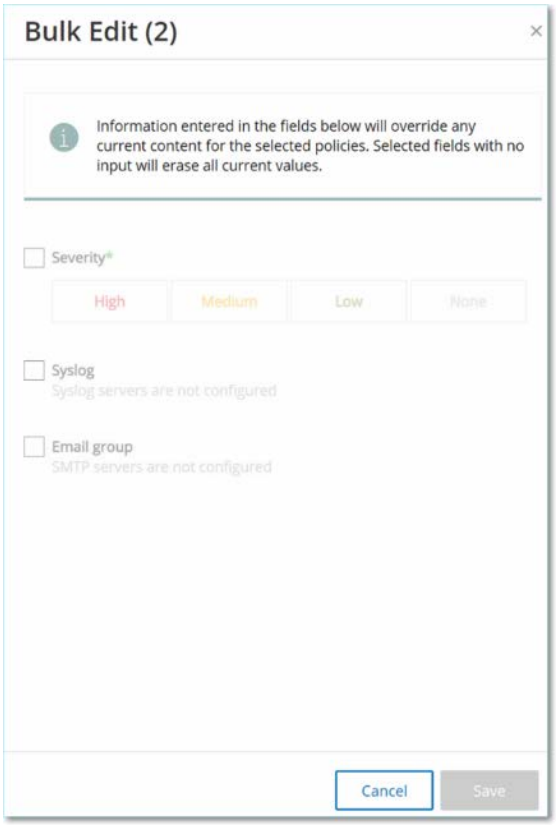
➡ 複数のポリシーの編集 (一括処理) 手順

1. **[ポリシー]**画面で、ポリシーの横にあるチェックボックスを複数選択します。

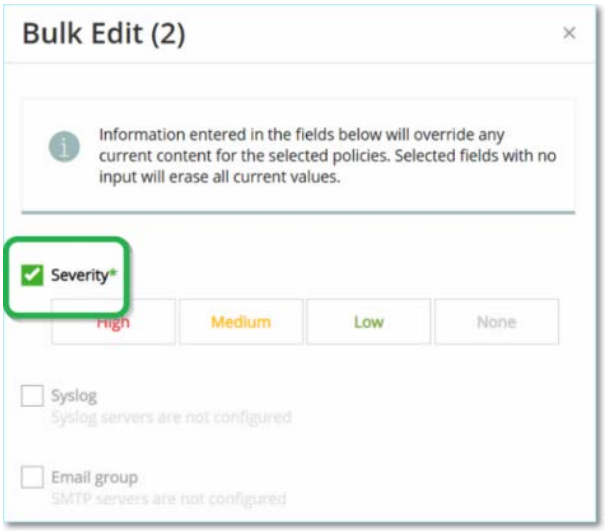
2. **[一括アクション]**メニューをクリックし、ドロップダウンリストから**[編集]**を選択します。



[一括編集]画面で、一括編集に利用できるポリシーアクションが表示されます。



3. 編集する各パラメーター(*深刻度*、*Syslog*、*E メールグループ*)の横にあるチェックボックスを選択します。



4. 各パラメーターを必要に応じて設定します。

> [一括編集] フィールドに入力された情報で、選択されたポリシーの現在の内容が上書きされます。パラメーターの横のチェックボックスを選択して、選択を入力しない場合でも、そのパラメーターの現在の値は消去されます。

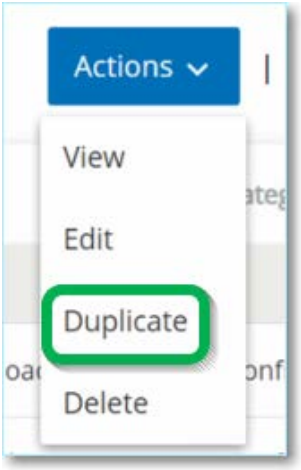
5. **[保存]**をクリックします。
   ポリシーが新しい構成で保存されます。

ポリシーの複製

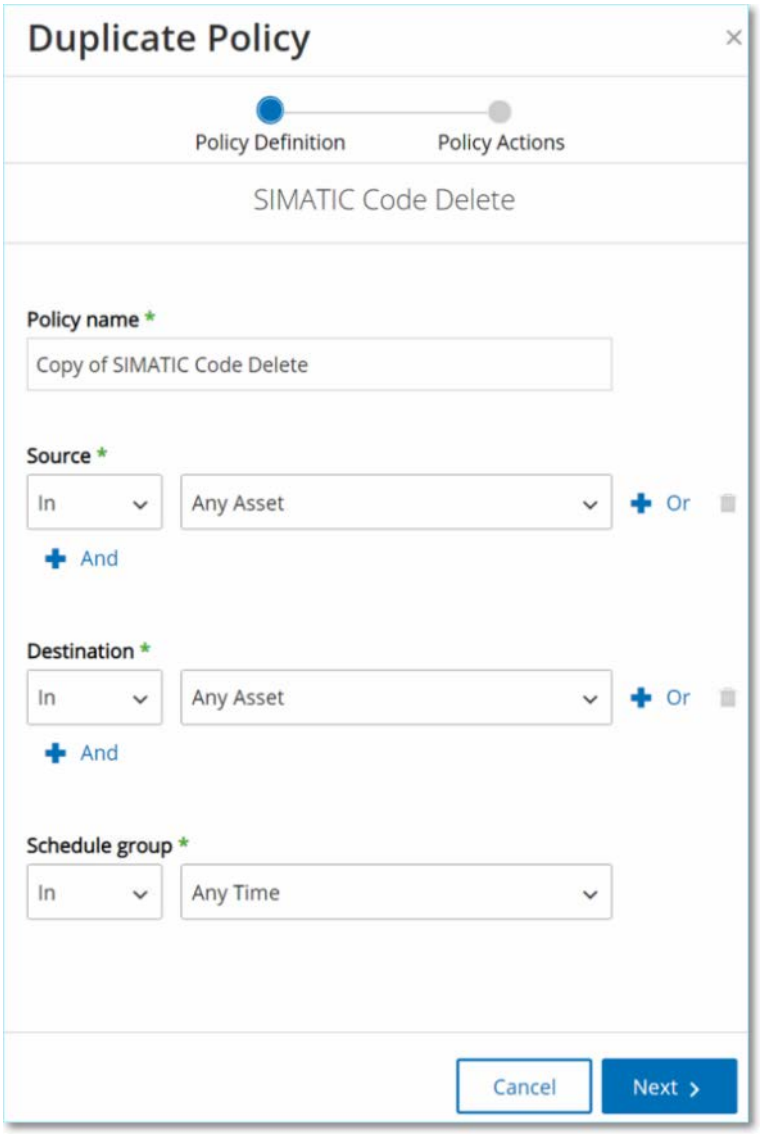
元のポリシーを*複製*して必要な調整を行うことで、既存のポリシーに類似した新しいポリシーを作成できます。事前定義されたポリシーとユーザー定義のポリシーの両方を複製できます(侵入検知ポリシーを除く)。

➡ ポリシーの複製手順

1. **[ポリシー]**画面で、目的のポリシーの横にあるチェックボックスを選択します。
2. **[アクション]**メニューをクリックし、ドロップダウンリストから**[複製]**を選択します。



[ポリシーの複製] 画面が現在の構成が入力された状態で表示され、名前はデフォルトで「<元のポリシー名> のコピー」と設定されます。



3. 必要に応じて、*ポリシー定義*パラメーターを調整します。
4. **[次へ]** をクリックします。
5. 必要に応じて、*ポリシーアクション*パラメーターを調整します。
6. **[保存]** をクリックします。
   ポリシーが新しい構成で保存されます。

ポリシーの削除

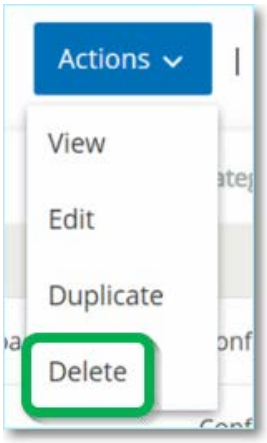
システムからポリシーを削除できます。事前定義されたポリシーとユーザー定義のポリシーの両方を削除できます(削除不可能な侵入検知ポリシーを除く)。

一括アクションで複数のポリシーを削除することもできます。

> システムからポリシーを削除すると、再度アクティブ化することはできません。別のオプションとして、ステータスをオフに切り替えて一時的にアクティブ化を解除し、オプションを予約して後で再度アクティブ化する方法があります。

ポリシーの削除手順

1. **[ポリシー]**画面で、目的のポリシーの横にあるチェックボックスを選択します。
2. **[アクション]**メニューをクリックし、ドロップダウンリストから**[削除]**を選択します。

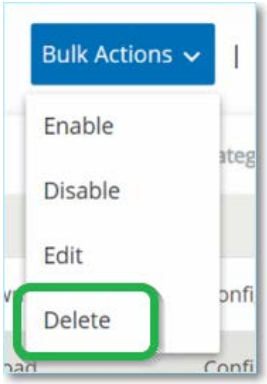


確認ウィンドウが表示されます。

3. **[削除]**をクリックします。
ポリシーがシステムから削除されます。

複数のポリシーの削除(一括アクション)手順

1. **[ポリシー]**画面で、目的の各ポリシーの横にあるチェックボックスを選択します。
2. **[一括アクション]**メニューをクリックし、ドロップダウンリストから**[削除]**を選択します。



確認ウィンドウが表示されます。

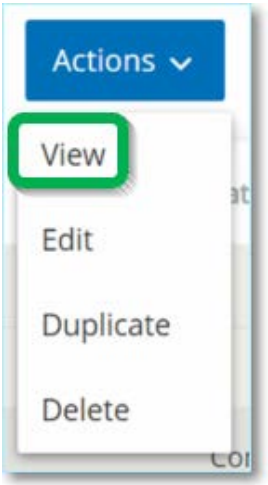
3. **[削除]**をクリックします。
ポリシーがシステムから削除されます。

ポリシーの除外の削除

特定のポリシーに適用されている除外を削除する場合は、[ポリシー]画面で行うことができます。

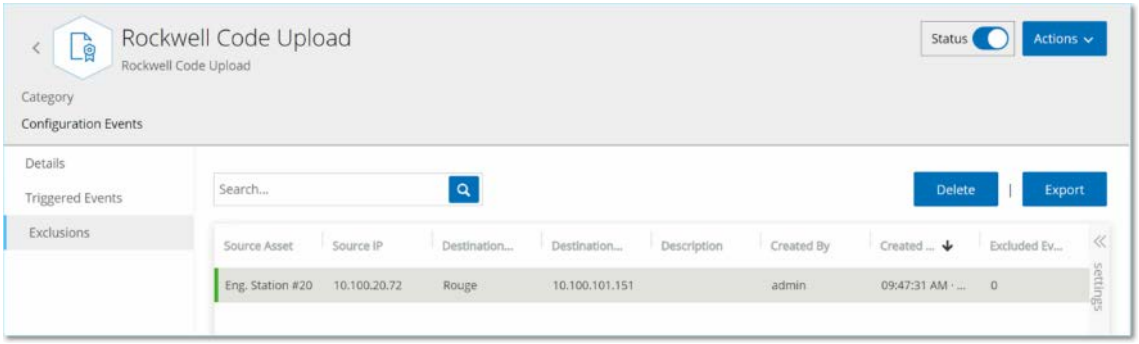
➡ ポリシーの除外の削除手順

1. **[ポリシー]**画面で、目的のポリシーを選択します。
2. **[アクション]**メニューをクリックし、ドロップダウンリストから**[表示]**を選択します。



または、関連するポリシーを右クリックして[アクション]メニューにアクセスすることもできます。

3. **[除外]**タブをクリックします。



除外のリストが表示されます。

4. 削除するポリシーの除外を選択します。
5. **[削除]**をクリックします。
   確認ウィンドウが表示されます。
6. 確認ウィンドウで、**[削除]**をクリックします。
   除外がシステムから削除されます。

グループ

グループは、ポリシーを構築するために使用される基本的な構成要素です。ポリシーを構成する場合、各ポリシー条件は個々のエンティティではなくグループを使用して指定されます。システムには、いくつかの事前定義グループがあります。独自のユーザー定義グループを作成することもできます。したがって、ポリシーの編集と作成のプロセスを合理化するために、事前に必要なグループを構成することをお勧めします。

ポリシーパラメーターは、グループを使用してのみ設定できます。ポリシーを個々のエンティティに適用する場合でも、そのエンティティのみを含むグループを構成する必要があります。

[**グループ**] で、システムで構成されたすべてのグループを表示できます。グループは 2 つのカテゴリに分類されます。

- **事前定義グループ** - システムで事前構成されており、編集することができません。
- **ユーザー定義グループ** - エンドユーザーによって作成され、編集することができます。

いくつかの異なるタイプのグループがあり、それぞれがさまざまなポリシータイプの構成に使用されます。各グループタイプは、グループの下に、別の画面で表示されます。グループのタイプは次のとおりです。

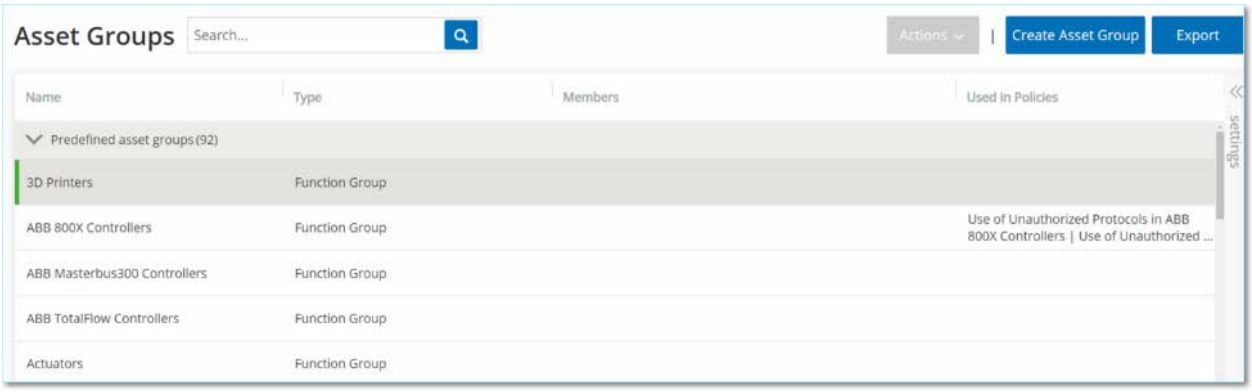
- **資産グループ** - 資産はネットワーク内のハードウェアエンティティです。資産グループは、幅広いポリシータイプのポリシー条件として使用されます。
- **ネットワークセグメント** - ネットワークセグメンテーションは、関連するネットワーク資産のグループを作成する方法で、ある資産グループを別の資産グループから論理的に分離するのに役立ちます。
- **E メールグループ** - ポリシーイベントの発生時に通知される E メールのグループです。すべてのポリシータイプに使用されます。
- **ポートグループ** - ネットワーク内の資産によって使用されるポートのグループです。オープンポートを識別するポリシーに使用されます。
- **プロトコルグループ** - ネットワーク内の資産間で行われる会話に使用されるプロトコルのグループです。ネットワークイベントのポリシー条件として使用されます。
- **スケジュールグループ** - スケジュールグループは、指定したイベントが発生する時間がポリシー条件を満たす時間範囲を構成するために使用されます。
- **タググループ** - タグは、特定の操作データを含むコントローラーのパラメーターです。タググループは、SCADA イベントのポリシー条件として使用されます。
- **ルールグループ** - ルールグループは、Suricata Signature ID (SID) で識別される関連ルールのグループで構成されます。これらのグループは、侵入検知ポリシーを定義するためのポリシー条件として使用されます。

次のセクションでは、各タイプのグループを作成する手順について説明します。また、既存のグループを表示、編集、複製、削除することもできます。**グループのアクション**を参照してください。

資産グループ

資産はネットワーク内のハードウェアエンティティです。類似の資産をグループ化すると、グループ内のすべての資産に適用されるポリシーを作成できます。たとえば、資産グループ*コントローラー*を使用して、任意のコントローラーに対するファームウェアの変更をアラートするポリシーを作成できます。資産グループは、幅広いポリシータイプのポリシー条件として使用されます。資産グループを使用して、さまざまなポリシータイプの *ソース*資産、*デスティネーション*資産、*影響を受ける資産*を指定できます。

資産グループの表示



[資産グループ]画面には、システムで現在構成されているすべての資産グループが表示されます。*[事前定義]*タブには、システムに組み込まれている編集、複製、削除ができないグループが含まれています。*[ユーザー定義]*タブには、ユーザーが作成したカスタムグループが含まれています。これらのグループは、編集、複製、削除することができます。

この画面に表示される情報について、次の表で説明します。

パラメーター	説明
ステータス	ポリシーがオンかオフかを示します。生成するイベントが多すぎるためにポリシーがシステムによって自動的に無効にされた場合、警告アイコンが表示されます。 ステータススイッチを切り替えて、ポリシーをオン / オフにします。
名前	ポリシーの名前。
深刻度	イベントの深刻度。可能な値は、なし、低、中、高です。深刻度レベルの説明については、**深刻度レベル**セクションを参照してください。
イベントタイプ	このイベントポリシーをトリガーするイベントの特定のタイプ。
カテゴリ	このイベントポリシーをトリガーするイベントのタイプの一般カテゴリ。可能な値は、構成、SCADA、ネットワーク脅威、ネットワークイベントです。各種カテゴリの説明については、**ポリシーカテゴリとサブカテゴリ**を参照してください。
ソース	ポリシー条件。ポリシーが適用されるソース資産グループ(アクティビティを開始した資産)。
名前	グループの識別に使用される名前。

パラメーター	説明
タイプ	グループのタイプを示します。オプションは次のとおりです。 • 関数 - 特定の関数を提供するために作成された事前定義の資産グループ • 資産リスト - グループに含まれる指定された資産 • IP リスト - 指定された IP アドレスを持つ資産 • IP 範囲 - IP アドレスの指定された範囲内の資産
メンバー	このグループに含まれている資産のリストを表示します。関数グループの値は表示されません。 **注意:** この行にすべての資産を表示するスペースがない場合は、**[テーブルアクション]>[表示]>[メンバー]**タブをクリックします。
ポリシーで使用	この資産グループを構成で使用する各ポリシーの名前を表示します。 **注意:** グループが使用されているポリシーの詳細を表示するには、**[テーブルアクション]>[表示]>[ポリシーで使用]**タブをクリックします。

次のセクションでは、さまざまなタイプの資産グループを作成する手順について説明します。また、既存のグループを表示、編集、複製、削除することもできます。**グループのアクション**を参照してください。

資産グループの作成

ポリシーの構成で使用するカスタム資産グループを作成できます。類似の資産をグループ化して、グループ内のすべての資産に適用されるポリシーを作成できます。

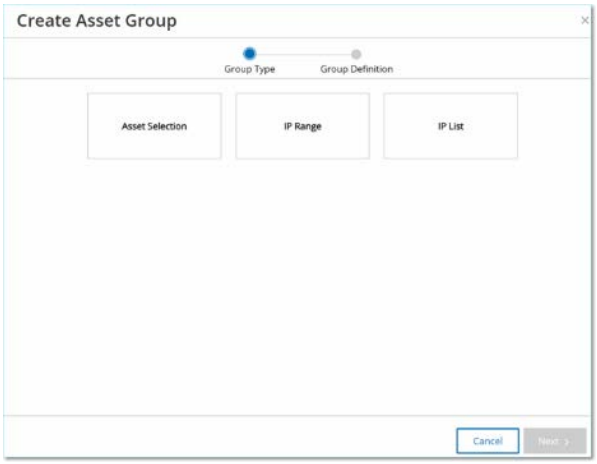
ユーザー定義の資産グループには 3 つのタイプがあります。

- **資産リスト** - グループに含まれる特定の資産を指定します。
- **IP リスト** - グループに含まれる資産の IP アドレスを指定します。
- **IP 範囲** - グループに含まれる資産の IP アドレスの範囲を指定します。

各タイプの資産グループを作成する手順は異なります。

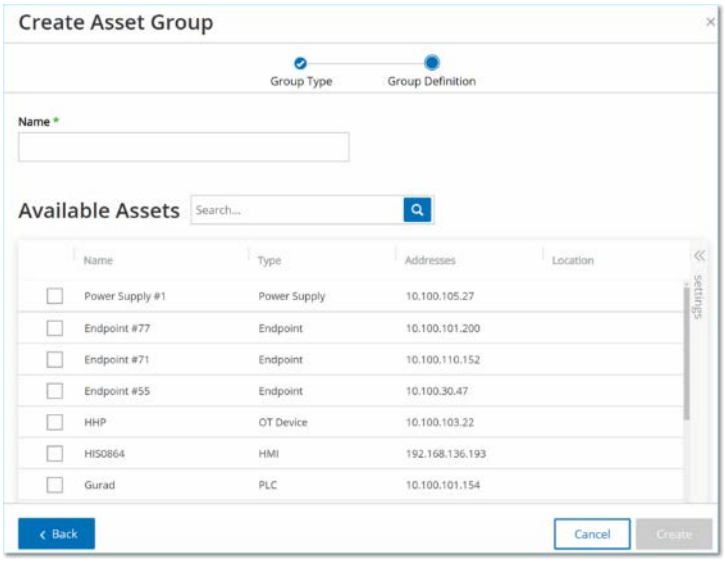
➡ 資産選択タイプの資産グループの作成手順

1. [グループ] で、[資産グループ] を選択します。
2. [資産グループの作成] をクリックします。
   [資産グループの作成] ウィザードが表示されます。



3. [資産選択] をクリックします。

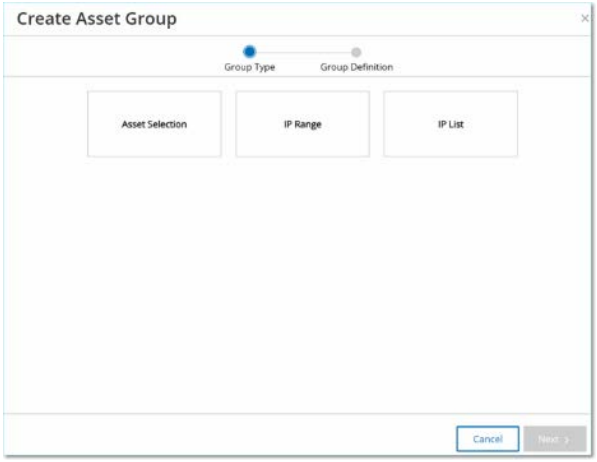
4. **[次へ]**をクリックします。
   利用可能な資産のリストが表示されます。



5. **[名前]**フィールドに、グループの名前を入力します。
   グループに含まれる資産を分類する共通要素を説明する名前を選択します。
6. グループに含める各資産の横のチェックボックスを選択します。
7. 選択が完了したら、**[作成]**をクリックします。
   新しい資産グループが作成され、[資産グループ]画面に表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

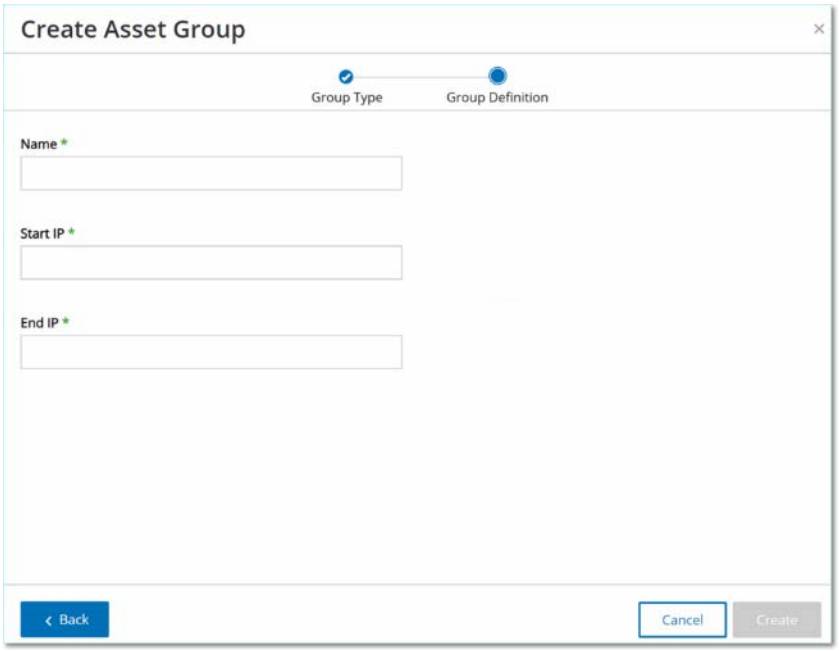
IP 範囲タイプの資産グループの作成手順

1. [グループ]で、[資産グループ]を選択します。
2. [資産グループの作成]をクリックします。
   [資産グループの作成]ウィザードが表示されます。



3. **[IP 範囲]**をクリックします。

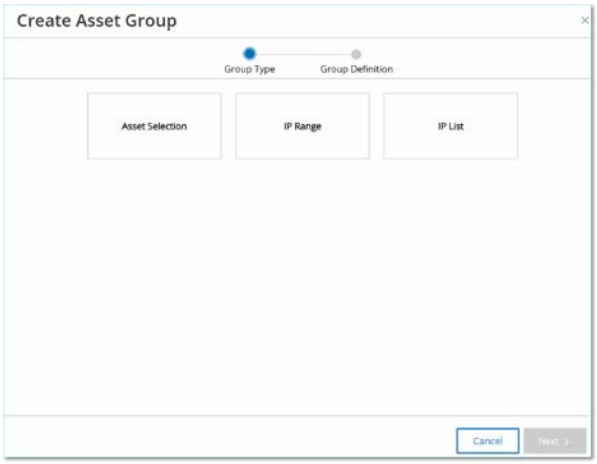
4. **[次へ]**をクリックします。
   IP 範囲選択パラメーターが表示されます。



5. **[名前]**フィールドに、グループの名前を入力します。
   グループに含まれる資産を分類する共通要素を説明する名前を選択します。
6. **[開始 IP]**フィールドに、含めたい範囲の最初の IP アドレスを入力します。
7. **[終了 IP]**フィールドに、含めたい範囲の最後の IP アドレスを入力します。
8. **[作成]**をクリックします。
   新しい資産グループが作成され、[資産グループ]画面に表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

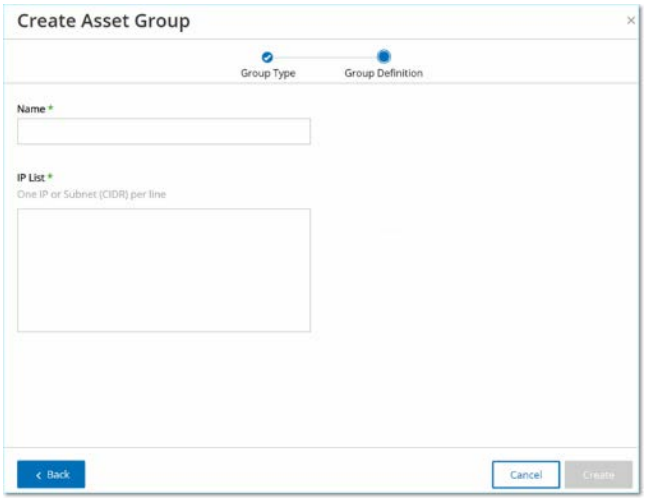
IP リストタイプの資産グループの作成手順

1. [グループ]で、[資産グループ]を選択します。
2. [資産グループの作成]をクリックします。
   [資産グループの作成]ウィザードが表示されます。



3. **[IP リスト]**をクリックします。

4. **[次へ]**をクリックします。
   IP リストパラメーターが表示されます。



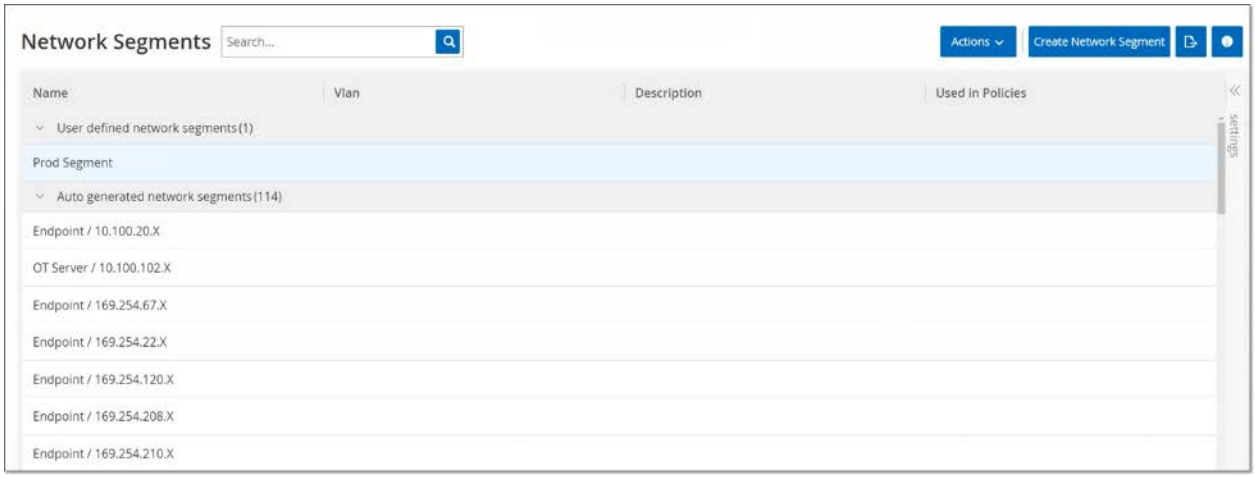
5. **[名前]**フィールドに、グループの名前を入力します。
   グループに含まれる資産を分類する共通要素を説明する名前を選択します。
6. **[IP リスト]**ボックスに、グループに含める IP アドレスまたはサブネットを入力します。
7. さらに資産をグループに追加するには、追加の IP アドレスまたはサブネットをそれぞれ別の行に入力します。
8. **[作成]**をクリックします。
   新しい資産グループが作成され、[資産グループ]画面に表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

ネットワークセグメント

ネットワークセグメンテーションは、関連するネットワーク資産のグループを作成する方法で、ある資産グループを別の資産グループから論理的に分離するのに役立ちます。Tenable.ot は、ネットワーク内の資産に関連付けられている各 IP アドレスをネットワークセグメントに自動的に割り当てます(複数の IP アドレスを持つ資産の場合、各 IP はネットワークセグメントに関連付けられます)。自動生成された各セグメントには、同じクラス C ネットワークアドレス(IP の最初の 24 ビットが同じ)の IP を持つ特定のカテゴリ(コントローラー、OT サーバー、ネットワークデバイスなど)のすべての資産が含まれます。

ユーザー定義のネットワークセグメントを作成し、そのセグメントに割り当てる資産を指定できます。[インベントリ]画面には各資産のネットワークセグメントを表示する列があり、ネットワークセグメントで資産を簡単にソートおよびフィルタリングできます。

ネットワークセグメントの表示



[ネットワークセグメント]画面には、システムで現在構成されているすべてのネットワークセグメントが表示されます。*[自動生成]*タブには、システムによって自動的に生成されるネットワークセグメントが含まれています。*[ユーザー定義]*タブには、ユーザーが作成したカスタムネットワークセグメントが含まれています。

この画面に表示される情報について、次の表で説明します。

パラメーター	説明
名前	ネットワークセグメントの識別に使用される名前。
VLAN	ネットワークセグメントの VLAN 番号。(オプション)
説明	ネットワークセグメントの説明。(オプション)
ポリシーで使用	このネットワークセグメントに適用されるポリシーの名前を表示します。 **注意:** ネットワークセグメントが使用されているポリシーの詳細を表示するには、**[テーブルアクション]>[表示]>[ポリシーで使用]**タブをクリックします。

次のセクションでは、ネットワークセグメントを作成する手順について説明します。また、既存のネットワークセグメントを表示、編集、複製、削除することもできます。**グループのアクション**を参照してください。

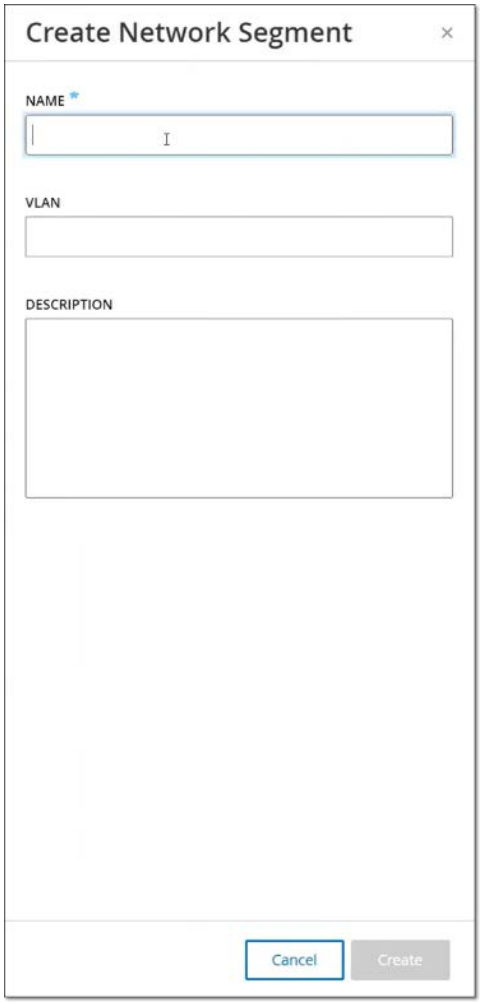
ネットワークセグメントの作成

ポリシーの構成で使用するネットワークセグメントを作成できます。関連するネットワーク資産をグループ化することで、そのセグメント内の資産の許容可能なネットワークトラフィックを定義するポリシーの作成が可能になります。

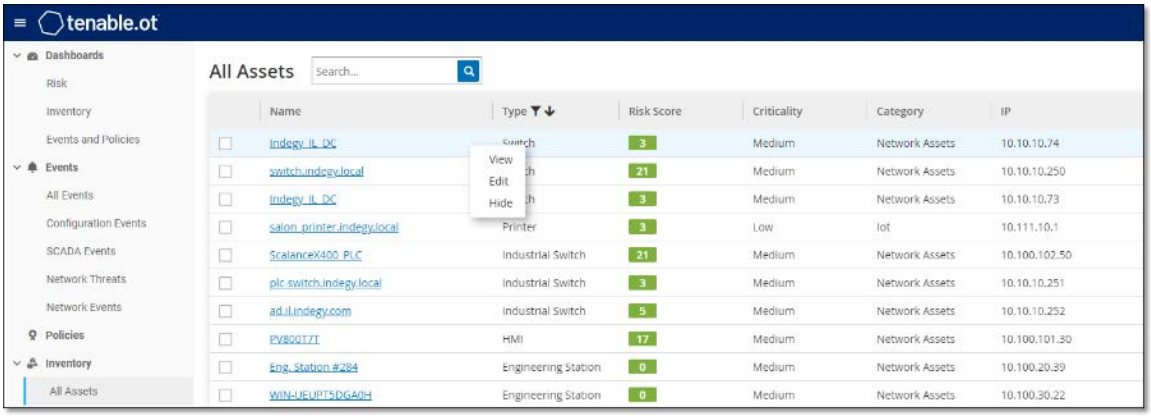
➡ ネットワークセグメントの作成手順

1. **[グループ]**で、**[ネットワークセグメント]**を選択します。
2. **[ネットワークセグメントの作成]**をクリックします。

[ネットワークセグメントの作成]ウィザードが表示されます。

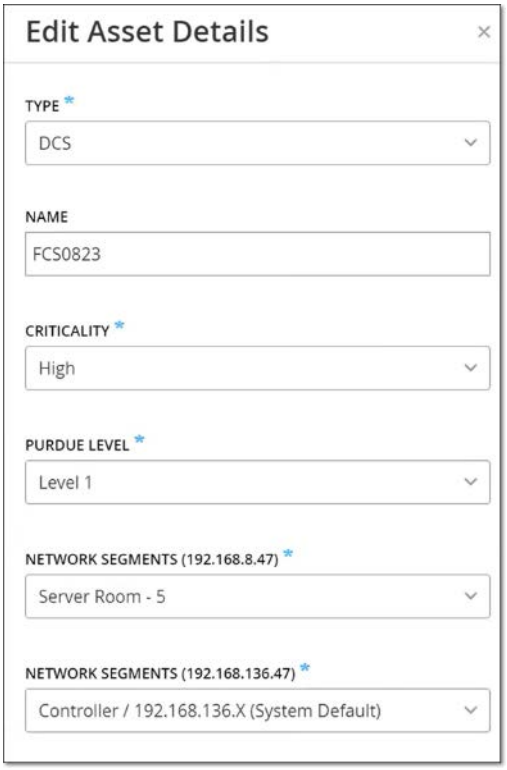


3. **[名前]**フィールドに、ネットワークセグメントの名前を入力します。
4. **[VLAN]**フィールドに、ネットワークセグメントの VLAN 番号を入力します。(オプション)
5. **[説明]**フィールドに、ネットワークセグメントの説明を入力します。(オプション)
6. **[作成]**をクリックします。
   新しいネットワークセグメントが作成され、ネットワークセグメントのリストに表示されます。
7. **[インベントリ]**で、**[すべての資産]**を選択します。
8. 新しく作成したネットワークセグメントに割り当てる資産を右クリックし、**[編集]**を選択します。



[資産詳細の編集]ウィンドウが開きます。

9. **[ネットワークセグメント]** フィールドで、ドロップダウンリストから適切なネットワークセグメントを選択します。



一部の資産には複数の IP アドレスが関連付けられており、それぞれに適切なネットワークセグメントを選択できます。

ネットワークセグメントが資産に適用され、ネットワークセグメント列に表示されます。これで、ポリシーを構成するときにこのネットワークセグメントを使用できます。

E メールグループ

E メールグループは、関連する当事者の E メールのグループです。E メールグループは、特定のポリシーによってトリガーされるイベント通知の受信者を指定するために使用されます。たとえば、ロール、部門などでグループ化すると、特定のポリシーイベントの通知を関連する当事者に送信できます。

E メールグループの表示

[E メールグループ] 画面には、システムで現在構成されているすべての E メールグループが表示されます。

この画面に表示される情報について、次の表で説明します。

グループを選択し、**[テーブルアクション]** > **[表示]** をクリックすることで、特定のグループに関する追加の詳細を表示できます。

パラメーター	説明
名前	グループの識別に使用される名前。
E メール	グループに含まれる E メールのリスト。 **注意:** グループのすべてのメンバーを表示するスペースがない場合は、**[テーブルアクション]>[表示]>[メンバー]** タブをクリックします。
E メールサーバー	このグループに E メールを送信するために使用される、SMTP サーバーに割り当てられた名前。
ポリシーで使用	通知がこのグループに送信されるポリシーの名前を表示します。 **注意:** グループが使用されているポリシーの詳細を表示するには、**[テーブルアクション]>[表示]>[ポリシーで使用]** タブをクリックします。

次のセクションでは、E メールグループを作成する手順について説明します。また、既存のグループを表示、編集、複製、削除することもできます。**グループのアクション**を参照してください。

E メールグループの作成

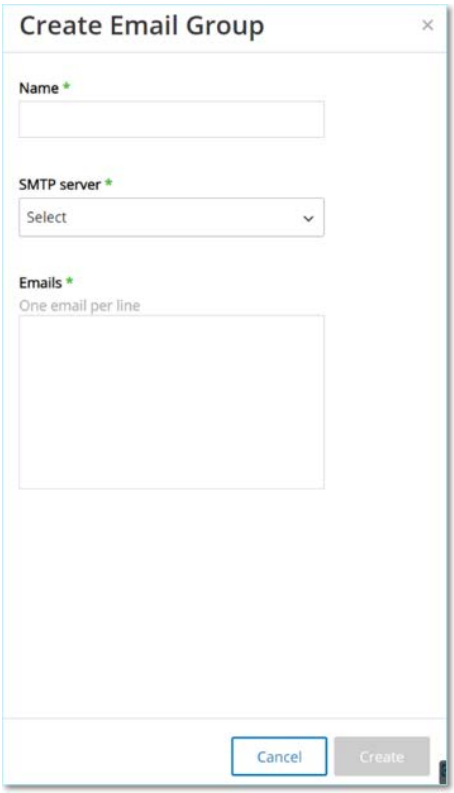
ポリシーの構成で使用する E メールグループを作成できます。関連する E メールをグループ化することで、すべての関連する担当者に送信されるポリシーイベント通知を設定します。

各ポリシーに割り当てることができる E メールグループは 1 つのみです。したがって、適切なグループを各ポリシーに割り当てることができるように、特定の制限されたグループと広範で包括的なグループの両方を作成すると便利です。

➡ E メールグループの作成手順

1. **[グループ]** で、**[E メールグループ]** を選択します。
2. **[E メールグループの作成]** をクリックします。

[E メールグループの作成] ウィザードが表示されます。



3. **[名前]** フィールドに、グループの名前を入力します。
4. **[SMTP サーバー]** フィールドで、E メール通知の送信に使用するサーバーをドロップダウンリストから選択します。

> SMTP サーバーがシステムで構成されていない場合は、E メールグループを作成する前に、まずサーバーを構成する必要があります。**SMTP サーバー**を参照してください。

5. **[E メール]** フィールドで、グループの各メンバーの E メールを別々の行に入力します。
6. **[作成]** をクリックします。
   新しい E メールグループが作成され、[E メールグループ] 画面に表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

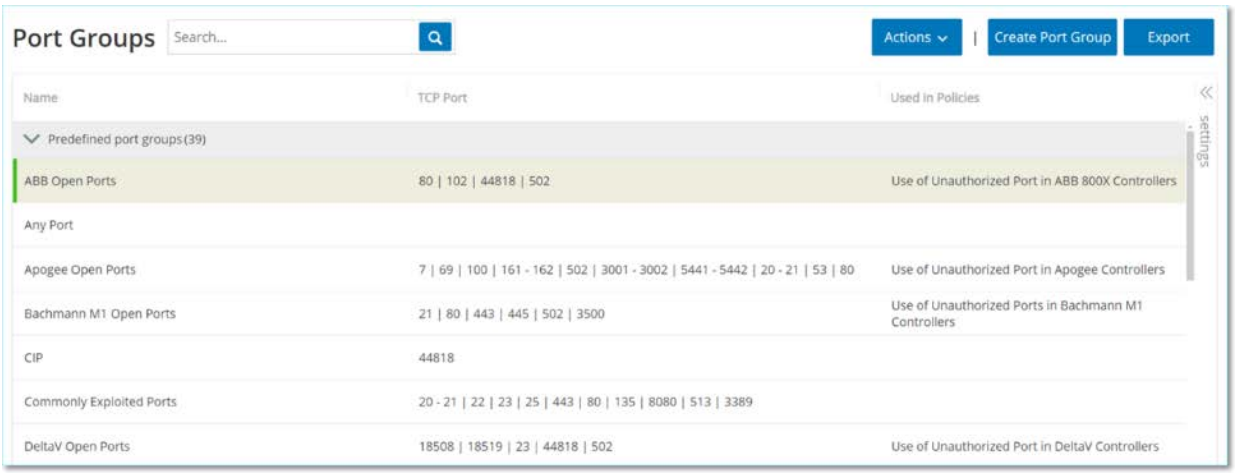
ポートグループ

ポートグループは、ネットワークの資産によって使用されるポートのグループです。ポートグループは、**オープンポート**ネットワークイベントポリシーを定義するためのポリシー条件として使用され、ネットワークでオープンポートを検出します。

[事前定義] タブには、システムで事前定義されているポートグループが表示されます。これらのグループは、特定のベンダーのコントローラーで開かれることが想定されているポートで構成されます。たとえば、Group Siemens PLC のオープンポートには、20、21、80、102、443、502 が含まれています。これにより、そのベンダーからのコントローラーに対して開かれることが想定されていないオープンポートを検出するポリシーの構成が可能になります。これらのグループは、編集や削除はできませんが、複製することができます。

[ユーザー定義] タブには、ユーザーが作成したカスタムグループが含まれています。これらのグループは、編集、複製、削除することができます。

ポートグループの表示



この画面に表示される情報について、次の表で説明します。

パラメーター	説明
名前	グループの識別に使用される名前。
TCP ポート	グループに含まれるポートおよび / またはポートの範囲のリスト。 **注意:** グループのすべてのメンバーを表示するスペースがない場合は、**[テーブルアクション]>[表示]>[メンバー]**タブをクリックします。
ポリシーで使用	構成でこのポートグループを使用する各ポリシーの名前を表示します。**注意:** グループが使用されているポリシーの追加情報を表示するには、**[テーブルアクション]>[表示]>[ポリシーで使用]**タブをクリックします。

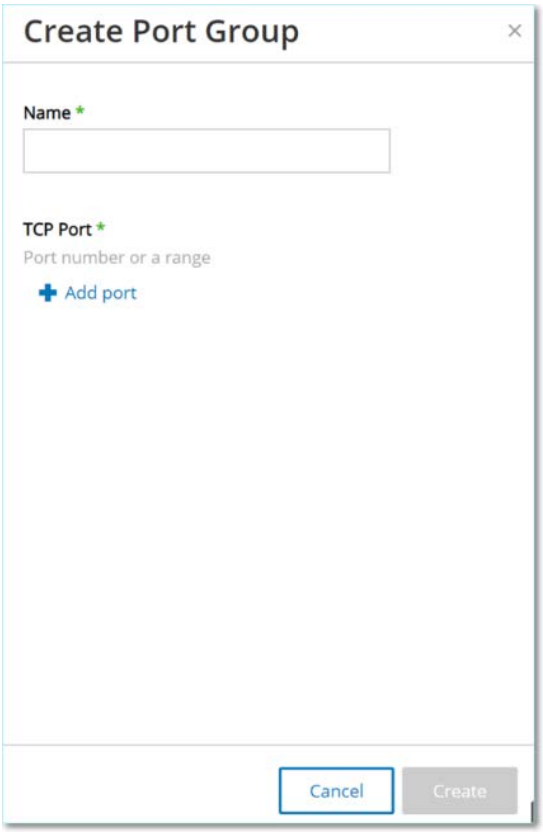
ポートグループの作成

ポリシーの構成で使用するユーザー定義のポートグループを作成できます。類似のポートをグループ化することで、特定のセキュリティリスクを引き起こすオープンポートを警告するポリシーの作成が可能になります。

➡ ポートグループの作成手順

1. **[グループ]**で、**[ポートグループ]**を選択します。
2. **[ポートグループの作成]**をクリックします。

[ポートグループの作成]ウィザードが表示されます。



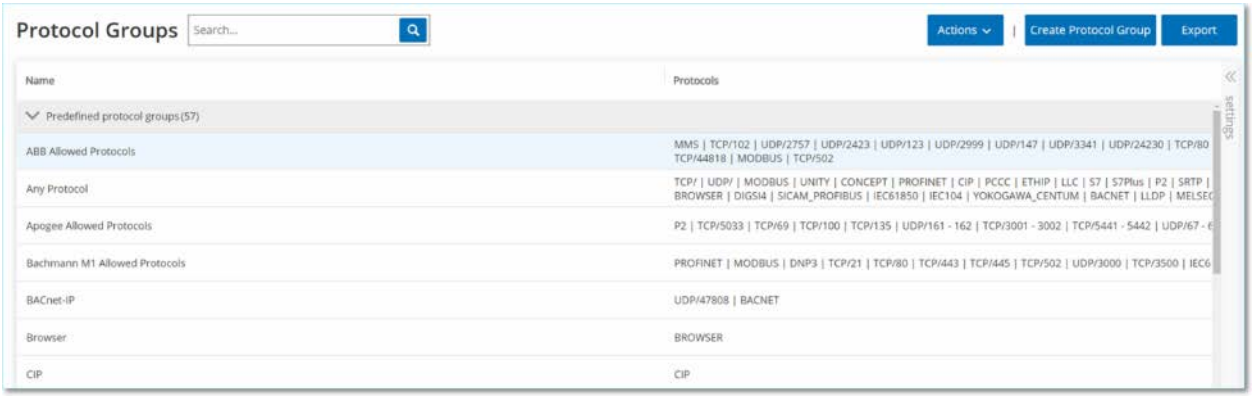
3. **[名前]**フィールドに、グループの名前を入力します。
4. **[TCP ポート]**フィールドに、グループに含める単一のポートまたはポートの範囲を入力します。
5. さらにポートをグループに追加する場合は、ポートを追加するたびに次の手順を実行します。
    a. **[+ポートの追加]**をクリックします。
    新しい[ポート選択]フィールドが表示されます。
    b. **[ポート番号]**フィールドに、グループに含める単一のポートまたはポートの範囲を入力します。
6. **[作成]**をクリックします。
新しいポートグループが作成され、ポートグループのリストに表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

プロトコルグループ

プロトコルグループは、ネットワーク内の資産間で行われる会話に使用されるプロトコルのグループです。プロトコルグループはネットワークポリシーのポリシー条件として使用され、特定の資産間で使用されるどのプロトコルがポリシーをトリガーするかを定義します。

Tenable.ot には、関連するプロトコルを構成する一連の定義済みプロトコルグループがあります。これらのグループは、ポリシーで使用できますが、編集や削除はできません。プロトコルは、特定のベンダーによって許可されているプロトコルによってグループ化できます。たとえば、Schneider で許可されているプロトコルには、TCP:80(HTTP)、TCP:21(FTP)、Modbus、Modbus_UMAS、Modbus_MODICON、TCP:44818(CIP)、UDP:69(TFTP)、UDP:161(SNMP)、UDP:162(SNMP)、UDP:44818、UDP:67-68(DHCP)があります。プロトコルのタイプ(Modbus、PROFINET、CIP など)でグループ化することもできます。独自のユーザー定義プロトコルグループを作成することもできます。

プロトコルグループの表示



[プロトコルグループ]画面には、システムで現在構成されているすべてのプロトコルグループが表示されます。*[事前定義]*タブには、システムに組み込まれているグループが表示されます。これらのグループは、編集や削除はできませんが、複製することができます。*[ユーザー定義]*タブには、ユーザーが作成したカスタムグループが表示されます。これらのグループは、編集、複製、削除することができます。

この画面に表示される情報について、次の表で説明します。

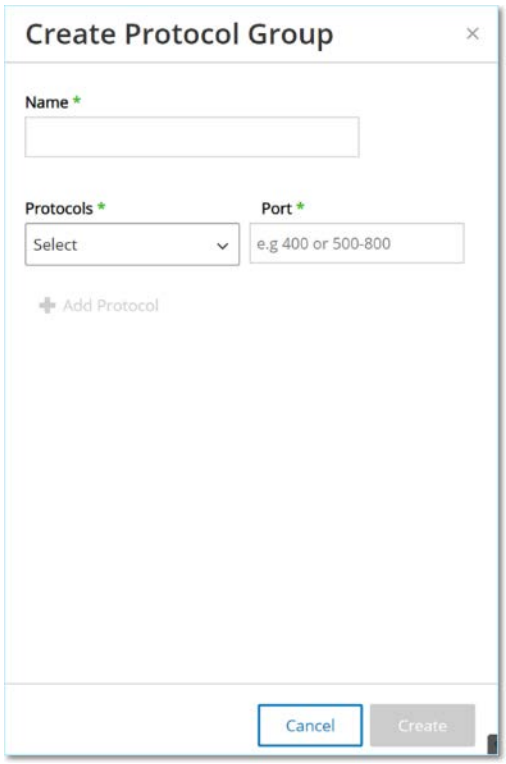
パラメーター	説明
名前	グループの識別に使用される名前。
プロトコル	グループに含まれるプロトコルのリスト。 **注意:** グループのすべてのメンバーを表示するスペースがない場合は、**[テーブルアクション]>[表示]>[メンバー]**タブをクリックします。
ポリシーで使用	構成でこのプロトコルグループを使用する各ポリシーの名前を表示します。 **注意:** このグループが使用されているポリシーの追加情報を表示するには、**[テーブルアクション]>[表示]>[ポリシーで使用]**タブをクリックします。

プロトコルグループの作成

ポリシーの構成で使用するカスタムプロトコルグループを作成できます。類似のプロトコルをグループ化することで、疑わしいプロトコルを定義するポリシーの作成が可能になります。

➡ プロトコルグループの作成手順

1. **[グループ]**で、**[プロトコルグループ]**を選択します。
2. **[プロトコルグループの作成]**をクリックします。
   [プロトコルグループの作成]ウィザードが表示されます。

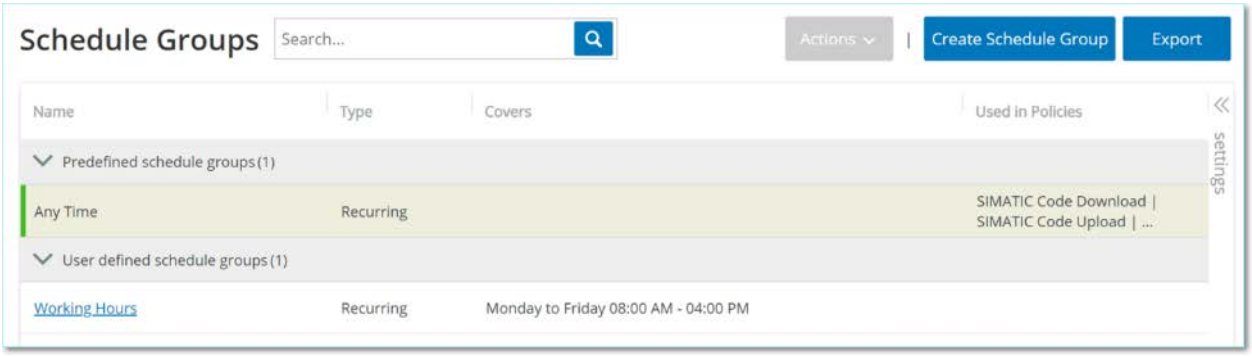


3. **[名前]**フィールドに、グループの名前を入力します。
4. **[プロトコル]**フィールドで、ドロップダウンメニューからプロトコルタイプを選択します。
5. 選択したプロトコルが *TCP* または *UDP* の場合、**[ポート]**フィールドにポート番号またはポートの範囲を入力します。その他のプロトコルタイプの場合、**[ポート]**フィールドに値は入力しません。
6. さらにプロトコルをグループに追加する場合は、プロトコルを追加するたびに次の手順を実行します。
   a. **[+プロトコルの追加]**をクリックします。
      新しい**[プロトコル選択]**フィールドが表示されます。
   b. 手順４～５で説明した方法で、新しいプロトコル選択を入力します。
7. **[作成]**をクリックします。
   新しいプロトコルグループが作成され、プロトコルグループのリストに表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

スケジュールグループ

スケジュールグループは、スケジュール設定された期間内に発生するアクティビティを注目に値する特性を持った時間範囲または時間範囲のグループを定義します。たとえば、特定のアクティビティは勤務時間中に発生することが予想され、他のアクティビティはダウンタイム中に発生することが予想されます。

スケジュールグループの表示



[スケジュールグループ]画面には、システムで現在構成されているすべてのスケジュールグループが表示されます。*[事前定義]*タブには、システムに組み込まれているグループが含まれます。これらのグループは、編集、複製、削除することができません。*[ユーザー定義]*タブには、ユーザーが作成したカスタムグループが表示されます。これらのグループは、編集、複製、削除することができます。

この画面に表示される情報について、次の表で説明します。

パラメーター	説明
名前	グループの識別に使用される名前。
タイプ	グループのタイプを示します。オプションは次のとおりです。 • 機能 - 特定の機能を提供するために作成された事前定義のスケジュールグループ。 • 繰り返し - 毎日または毎週繰り返されるスケジュール。たとえば、勤務時間のスケジュールを月曜日から金曜日の午前 9 時から午後 5 時と定義できます。 • 間隔 - 特定の日付または日付の範囲で発生するスケジュール。たとえば、工場改修のスケジュールは、6 月 1 日から 8 月 15 日までの期間と定義できます。
対象範囲	スケジュール設定のサマリー。 **注意:** グループのすべてのメンバーを表示するスペースがない場合は、**[テーブルアクション]>[表示]>[メンバー]**タブをクリックします。
ポリシーで使用	構成でこのスケジュールグループを使用する各ポリシーのポリシー ID を表示します。 **注意:** このグループが使用されているポリシーの追加情報を表示するには、**[テーブルアクション]>[表示]>[ポリシーで使用]**タブをクリックします。

スケジュールグループの作成

ポリシーの構成で使用するカスタムスケジュールグループを作成できます。スケジュールグループは、スケジュール設定された期間内に発生するイベントを注目に値するものとする、共有の特性を持つ時間範囲または時間範囲のグループを指定します。

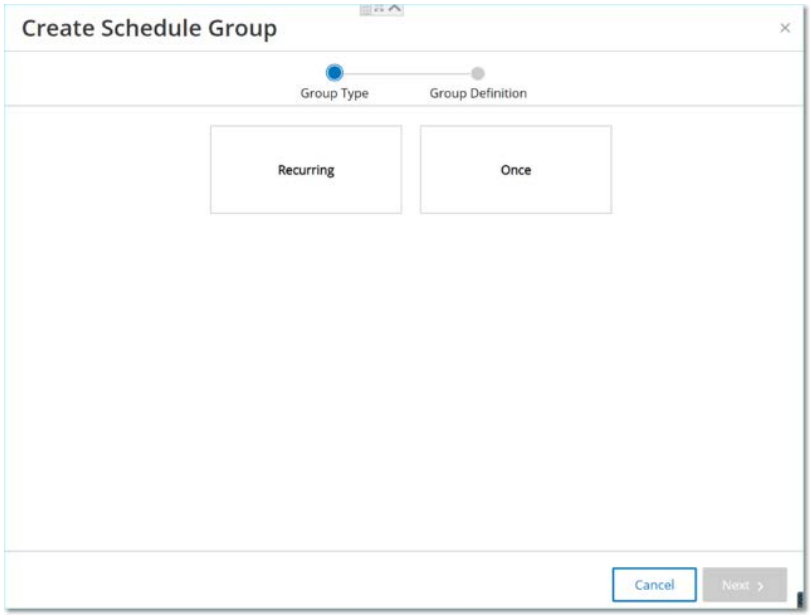
スケジュールグループには 2 つのタイプがあります。

- **繰り返し** - 毎週繰り返されるスケジュール。たとえば、勤務時間のスケジュールを月曜日から金曜日の午前 9 時から午後 5 時と定義できます。
- **1回** - 特定の日付または日付の範囲で発生するスケジュール。たとえば、工場改修のスケジュールは、6 月 1 日から 8 月 15 日までの期間と定義できます。各タイプのスケジュールグループを作成する手順は異なります。

各タイプのスケジュールグループを作成する手順は異なります。

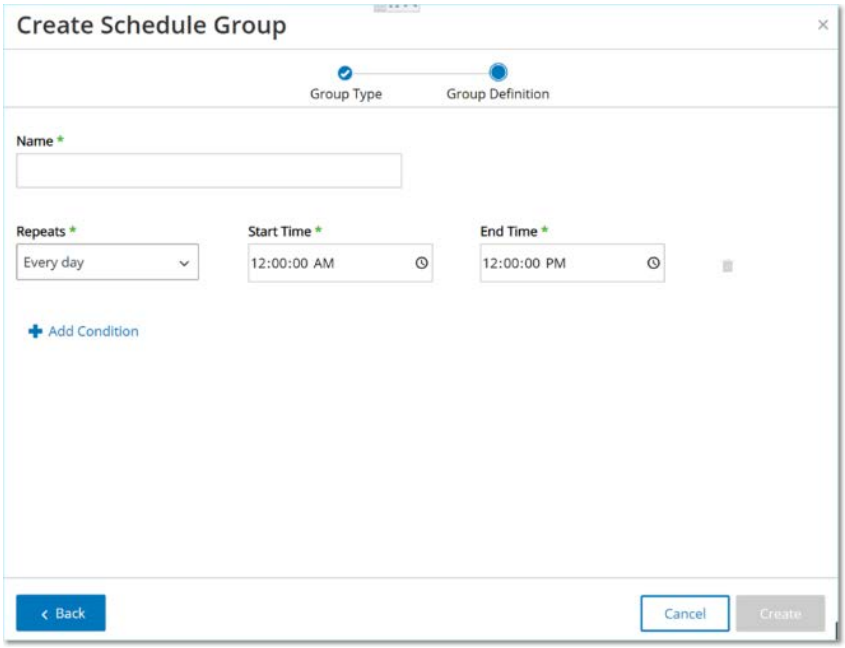
➡ 繰り返しタイプのスケジュールグループの作成手順

1. **[グループ]** で、**[スケジュールグループ]** を選択します。
2. **[スケジュールグループの作成]** をクリックします。
3. **[スケジュールグループ]** 画面で、**[スケジュールグループの作成]** をクリックします。
   [スケジュールグループの作成] ウィザードが表示されます。



4. **[繰り返し]** を選択します。

5. **[次へ]**をクリックします。
   繰り返しスケジュールグループを定義するためのパラメーターが表示されます。



6. **[名前]**フィールドに、グループの名前を入力します。
7. **[繰り返し]**フィールドで、スケジュールグループに含める曜日を選択します。オプションは*毎日*、*月曜日から金曜日*、または特定の曜日です。

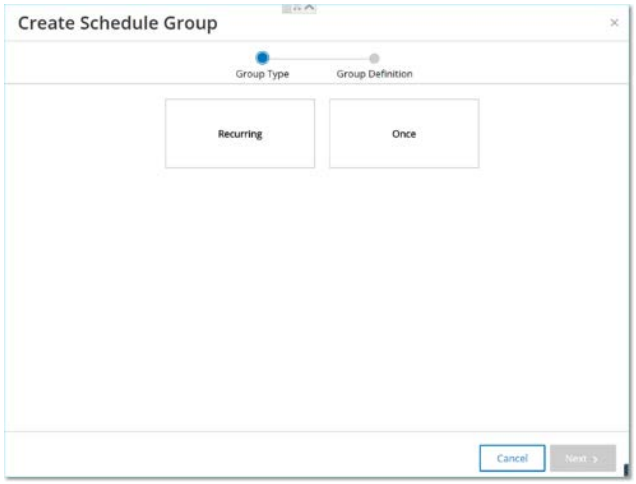
> 月曜日と水曜日など、特定の曜日のみを含める場合は、曜日ごとに個別の条件を追加する必要があります。

8. **[開始時刻]**フィールドに、スケジュールグループに含まれる時間範囲の開始時刻(HH:MM:SS AM/PM)を入力します。
9. **[終了時刻]**フィールドに、スケジュールグループに含まれる時間範囲の終了時刻(HH:MM:SS AM/PM)を入力します。
10. さらに条件(追加の時間範囲)をスケジュールグループに追加する場合は、条件を追加するたびに次の手順を実行します。
    a. **[+条件の追加]**をクリックします。
       [スケジュール選択]フィールドの新しい行が表示されます。
    b. 上記の手順5～7に従って、スケジュールフィールドに入力します。
11. **[作成]**をクリックします。
    新しいスケジュールグループが作成され、スケジュールグループのリストに表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

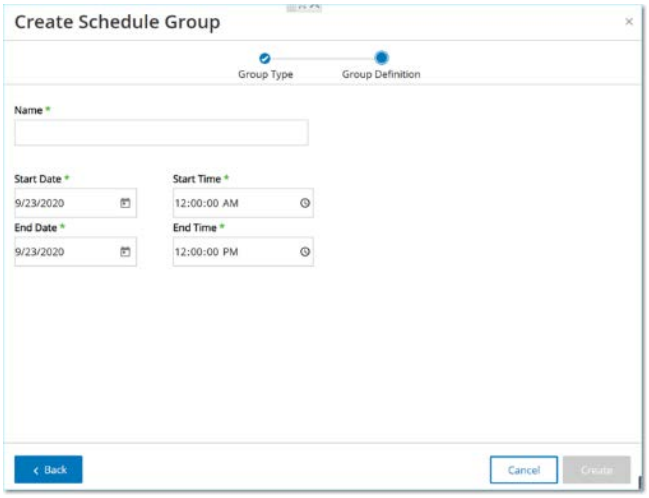
1回限りのスケジュールグループの作成手順

1. **[グループ]**で、**[スケジュールグループ]**を選択します。
2. **[スケジュールグループの作成]**をクリックします。

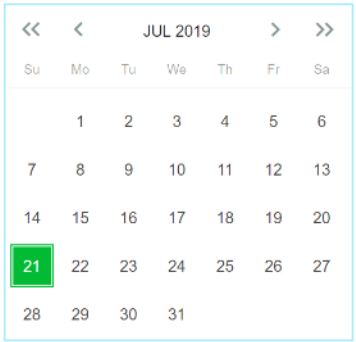
[スケジュールグループの作成]ウィザードが表示されます。



3. **[1回]**を選択します。
4. **[次へ]**をクリックします。
   1回限りのスケジュールグループを定義するためのパラメーターが表示されます。



5. **[名前]**フィールドに、グループの名前を入力します。
6. **[開始日]**フィールドで、カレンダーアイコン をクリックします。
   カレンダーウィンドウが開きます。



7. スケジュールグループが開始する日付を選択します。(デフォルト : 現在の日付)
8. **[開始時刻]**フィールドに、スケジュールグループに含まれる時間範囲の開始時刻(HH:MM:SS AM/PM)を入力します。
9. **[終了日]**フィールドで、カレンダーアイコン をクリックします。
   カレンダーウィンドウが開きます。
10. スケジュールグループが終了する日付を選択します。(デフォルト : 現在の日付)

11. **[終了時刻]**フィールドに、スケジュールグループに含まれる時間範囲の終了時刻(HH:MM:SS AM/PM)を入力します。
12. **[作成]**をクリックします。
    新しいスケジュールグループが作成され、スケジュールグループのリストに表示されます。これで、ポリシーを構成するときにこのグループを使用できます。

タググループ

タグは、特定の操作データを含むコントローラーのパラメーターです。タググループは、**SCADA イベントポリシー**のポリシー条件として使用されます。同様の役割を担うタグをグループ化することで、指定されたパラメーターに対する疑わしい変更を検出するポリシーを作成できます。たとえば、ファーネスの温度を制御するタグをグループ化することで、ファーネスに害を及ぼす可能性のある温度変化を検出するポリシーを作成できます。

タググループの表示

[タググループ]画面には、システムで現在構成されているすべてのタググループが表示されます。

この画面に表示される情報について、次の表で説明します。

パラメーター	説明
名前	グループの識別に使用される名前。
タイプ	タグのデータタイプ。可能な値には *Bool*、*Dint*、*Float*、*Int*、*Long*、*Short*、*Unknown*(Tenable.ot が識別できないタイプのタグの場合)、*Any Type*(異なるタイプのタグを含めることができます)があります。
コントローラー	タグが監視されているコントローラー。
タグ	グループに含まれている各タグと、各タグがあるコントローラーの名前を表示します。 **注意:** この行にすべてのタグを表示するスペースがない場合は、**[テーブルアクション]>[表示]>[メンバー]**タブをクリックします。
ポリシーで使用	構成でこのスケジュールグループを使用する各ポリシーのポリシー ID を表示します。 **注意:** このグループが使用されているポリシーの追加情報を表示するには、**[テーブルアクション]>[表示]>[ポリシーで使用]**タブをクリックします。

次のセクションでは、ポートグループを作成する手順について説明します。また、既存のグループを表示、編集、複製、削除することもできます。**グループのアクション**を参照してください。

タググループの作成

ポリシー構成で使用するカスタムタググループを作成できます。類似のタグをグループ化すると、グループ内のすべてのタグに適用されるポリシーを作成できるようになります。類似するタイプのタグを選択し、タグの共通要素を表す名前を付けます。

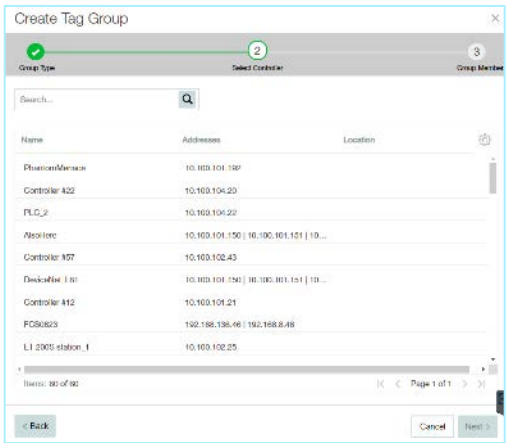
*[任意のタイプ]*オプションを選択することで、異なるタイプのタグを含むグループを作成することもできます。この場合、このグループに適用されるポリシーが検出できるのは指定のタグの「*任意の値*」の変更であり、特定の値を検出するように設定することはできません。

タググループは、編集、複製、削除することができます。

➡ 新しいタググループの作成手順

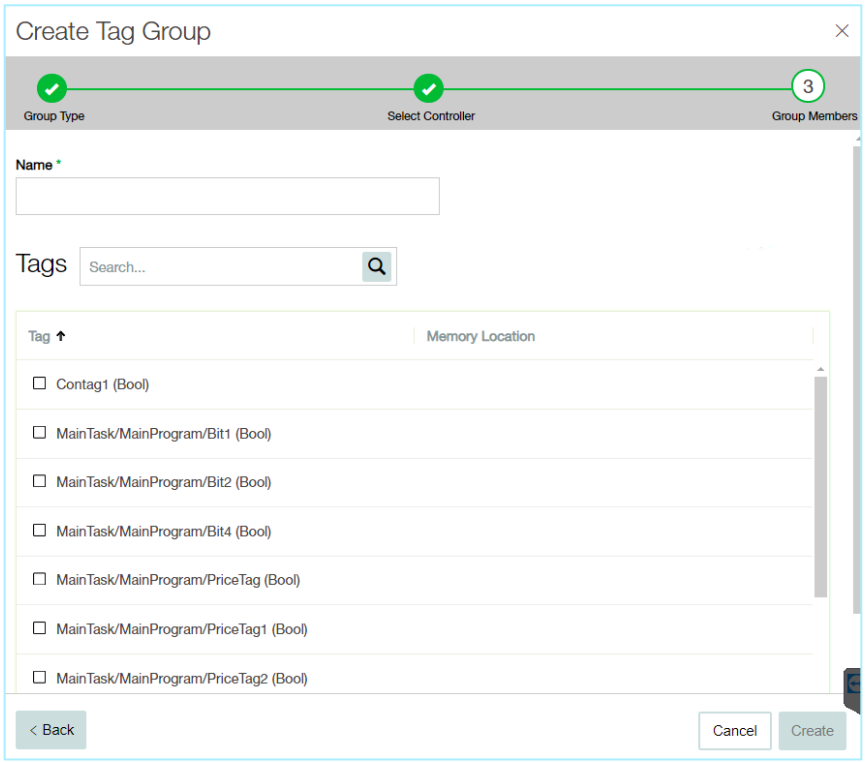
1. **[グループ]**で、**[タググループ]**を選択します。
2. **[タググループの作成]**をクリックします。
   [タググループの作成]ウィザードが表示されます。

3. タグタイプを選択します。オプションには 。*Bool*、*Dint*、*Float*、*Int*、*Long*、*Short* または *Any Type*(異なるタイプのタグを含めることができます)があります。
4. **[次へ]**をクリックします。
   ネットワーク内のコントローラーのリストが表示されます。



5. タグをグループに含めるコントローラーを選択します。
6. **[次へ]**をクリックします。

指定したコントローラーの指定したタイプのタグのリストが表示されます。



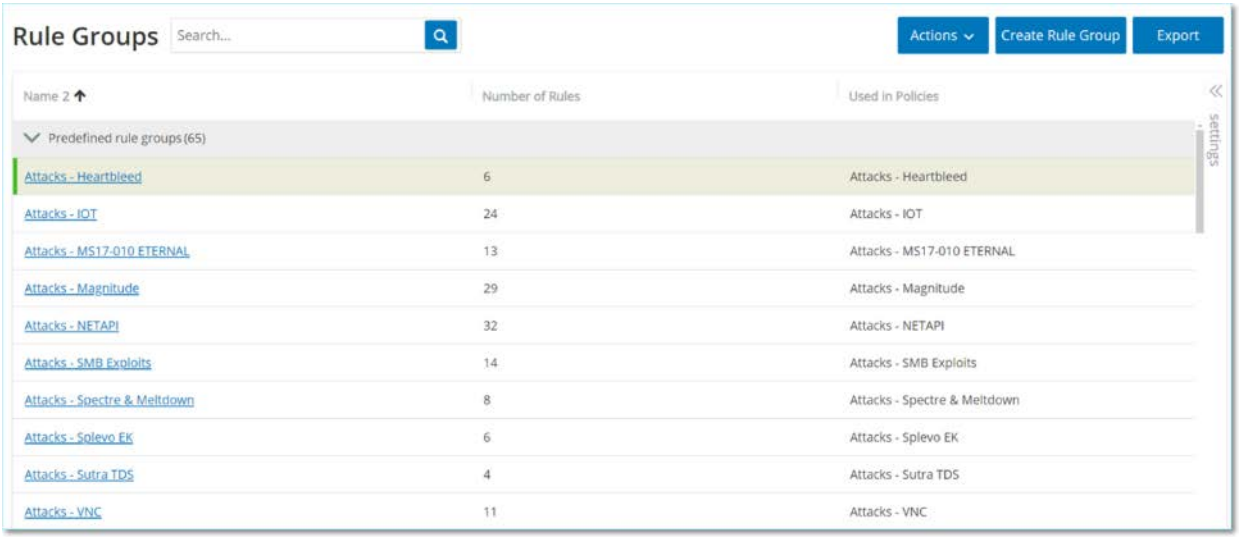
7. **[名前]** フィールドに、グループの名前を入力します。
8. グループに含める各タグの横のチェックボックスを選択します。
9. **[作成]** をクリックします。
   新しいタググループが作成され、タググループのリストに表示されます。これで、SCADA イベントポリシーを構成するときにこのグループを使用できます。

ルールグループ

ルールグループは、Suricata Signature ID (SID) で識別される関連ルールのグループで構成されます。これらのグループは、侵入検知ポリシーを定義するためのポリシー条件として使用されます。

Tenable.ot は、関連する脆弱性の定義済みグループのセットを提供します。さらに、提供する脆弱性のリポジトリから個別のルールを選択し、独自のカスタムルールグループを作成できます。

ルールグループの表示



[ルールグループ] 画面には、システムで現在構成されているすべてのルールグループが表示されます。*[事前定義]* タブには、システムに組み込まれているグループが含まれます。これらのグループは、編集、複製、削除することができません。*[ユーザー定義]* タブには、ユーザーが作成したカスタムグループが表示されます。これらのグループは、編集、複製、削除することができます。

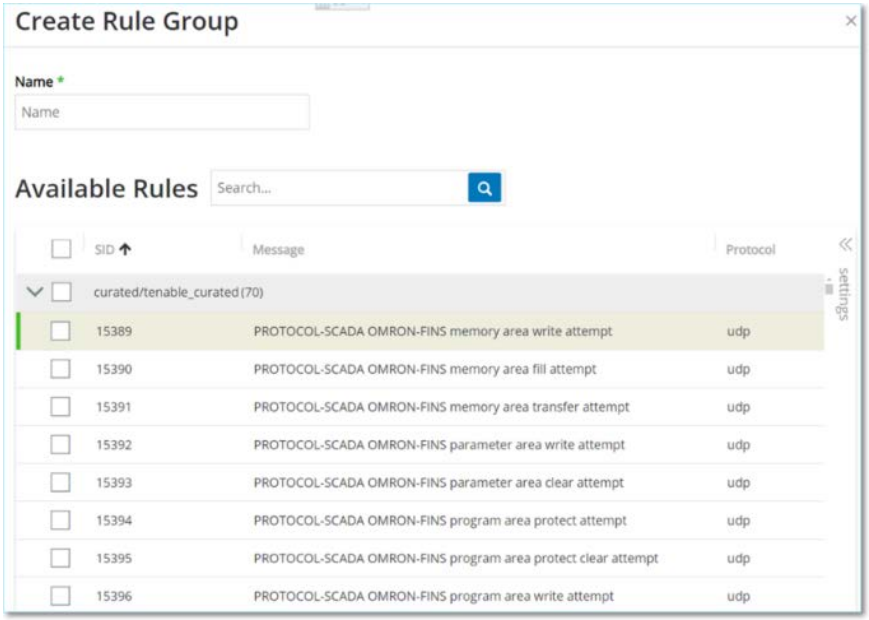
この画面に表示される情報について、次の表で説明します。

パラメーター	説明
名前	グループの識別に使用される名前。
ルールの数	このルールグループを構成するルール(SID)の数。
ポリシーで使用	構成でこのルールグループを使用する各ポリシーのポリシー ID を表示します。 **注意:** このグループが使用されているポリシーの追加情報を表示するには、**[テーブルアクション]**>**[表示]**>**[ポリシーで使用]** タブをクリックします。

ルールグループの作成

➡ 新しいルールグループの作成手順

1. **[グループ]** で、**[ルールグループ]** を選択します。
2. **[ルールグループの作成]** をクリックします。
   [ルールグループの作成] ウィザードが表示されます。



3. **[名前]** フィールドに、グループの名前を入力します。
4. **[使用可能なルール]** セクションで、グループに含める各ルールの横のチェックボックスを選択します。

> 検索ボックスを使用して、目的のルールを検索します。

5. **[作成]** をクリックします。
   新しいルールグループが作成され、ルールグループのリストに表示されます。これで、侵入検知ポリシーを構成するときにこのグループを使用できます。

グループのアクション

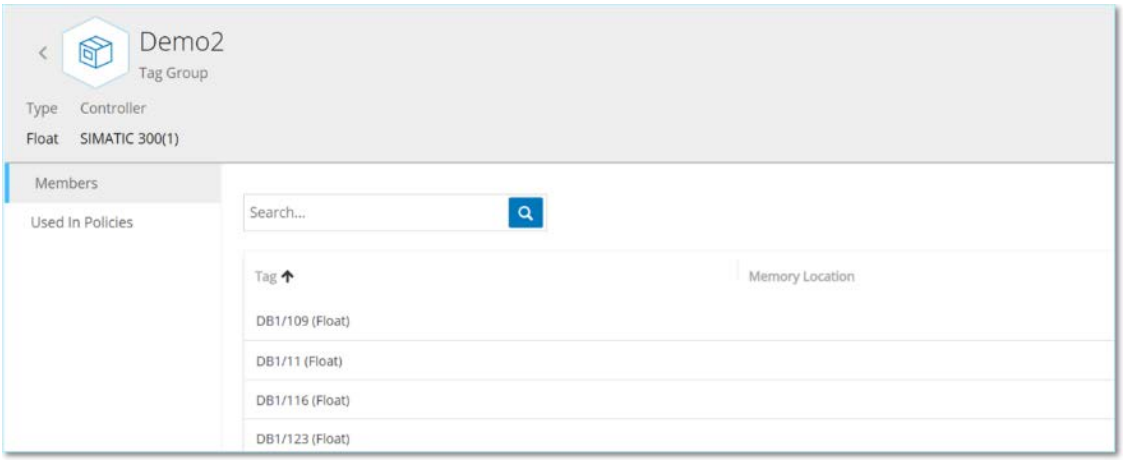
グループ画面のいずれかでグループを選択すると、画面上部の[アクション]メニューで次のアクションを実行できます。

- **表示** - グループに含まれているエンティティや、グループをポリシー条件として使用しているポリシーなど、選択したグループに関する詳細が表示されます。
- **編集** - グループの詳細を編集します。
- **複製** - 指定されたグループと同様の構成で新しいグループを作成します。
- **削除** - システムからグループを削除します。

> 事前定義グループは、編集や削除はできません。一部の事前定義グループでは複製もできません。
>
> アクションメニューは、グループを右クリックしてアクセスすることもできます。

グループの詳細の表示

グループを選択して**[アクション]**>**[表示]**をクリックすると、選択したグループの*[グループの詳細]*画面が表示されます。



[グループの詳細]画面には、グループの名前とタイプを表示するヘッダーバーがあります。また、次の 2 つのタブがあります。

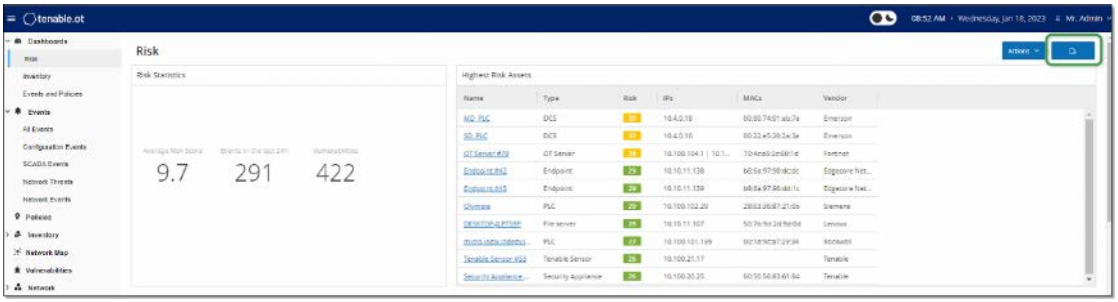
- **メンバー** - グループの全メンバーのリストを表示します。

- **ポリシーで使用** - 指定されたグループがポリシー条件として使用されている各ポリシーのリストを表示します。ポリシーのリストには、ポリシーのオン / オフを切り替えるトグルスイッチが含まれています。ポリシーリストに表示される情報については、ダッシュボードのエクスポート

ダッシュボード画面の[エクスポート]ボタンは、各ダッシュボードウィジェットを個別のページに表示した PDF をエクスポートします。

ダッシュボードのエクスポート手順

1. ダッシュボードの右上の**[エクスポート]**ボタンをクリックします( )。

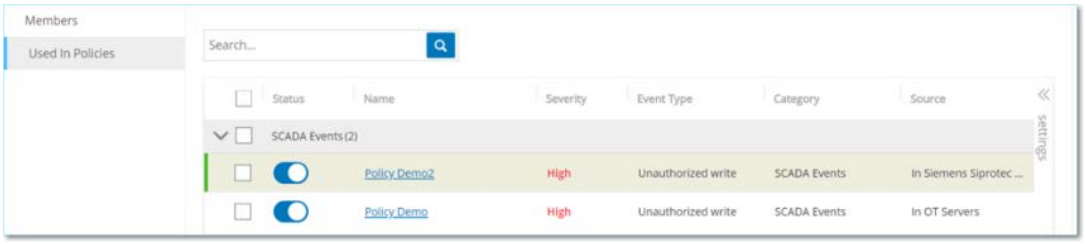


PDF はデフォルトのダウンロードフォルダに自動的にダウンロードされます。

2. PDF ダウンロードの進行中 (2〜3 秒) は、ブラウザで [ダッシュボード] タブを開いたままにしてください。

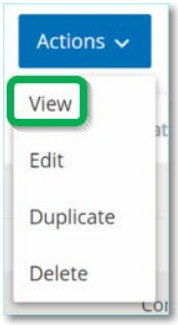
3. ファイルのダウンロードが完了したら、ダウンロードしたばかりのファイルに移動して、そのファイルを表示または共有します。

- ポリシー。



グループの詳細の表示手順

1. **[グループ]**で、目的のグループのタイプを選択します。
2. 目的のグループを選択します。
3. **[アクション]**をクリックします(またはグループを右クリックします)。
4. ドロップダウンメニューから、**[表示]**を選択します。



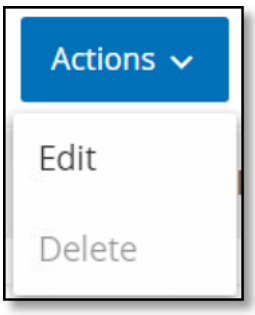
[グループの詳細]画面が表示されます。

グループの編集

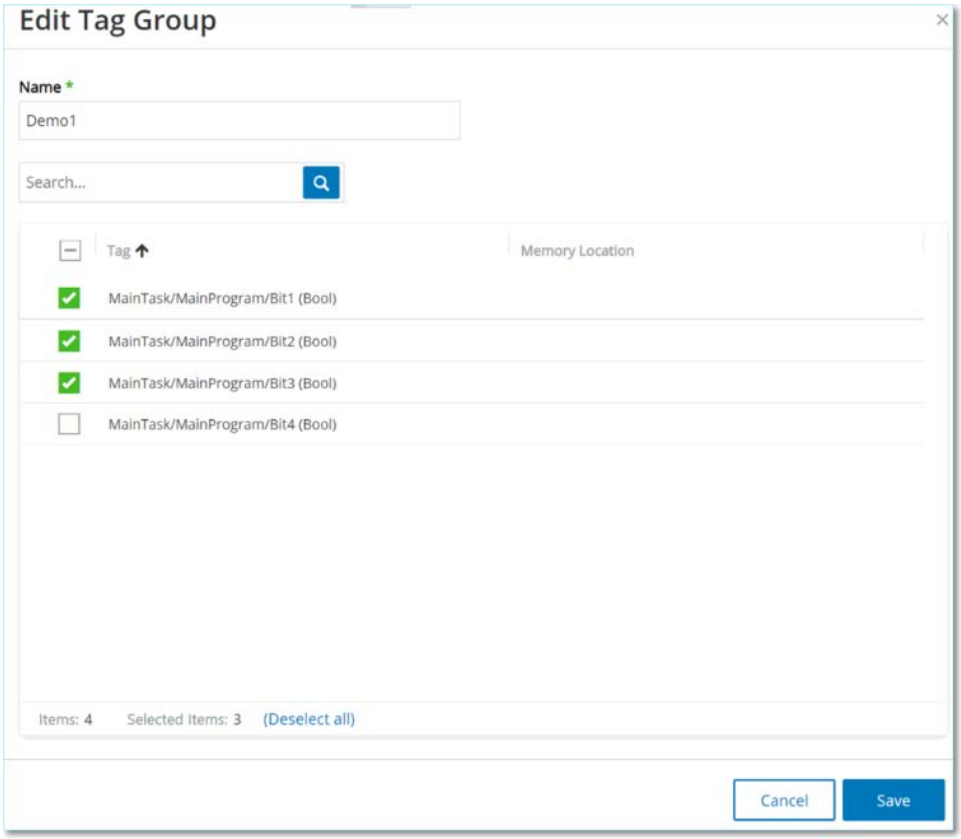
既存のグループの詳細を編集できます。

グループの詳細の編集手順

1. **[グループ]**で、目的のグループのタイプを選択します。
2. 目的のグループを選択します。
3. **[アクション]**をクリックします(またはグループを右クリックします)。
4. ドロップダウンメニューから、**[編集]**を選択します。



5. **[グループの編集]**ウィンドウが表示され、指定したグループタイプに関連するパラメーターが表示されます。



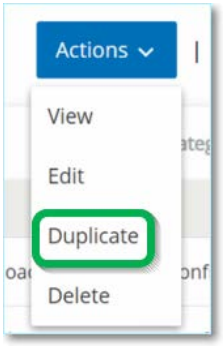
6. 必要な変更を行います。
7. **[保存]**をクリックします。
   グループが新しい設定で保存されます。

グループの複製

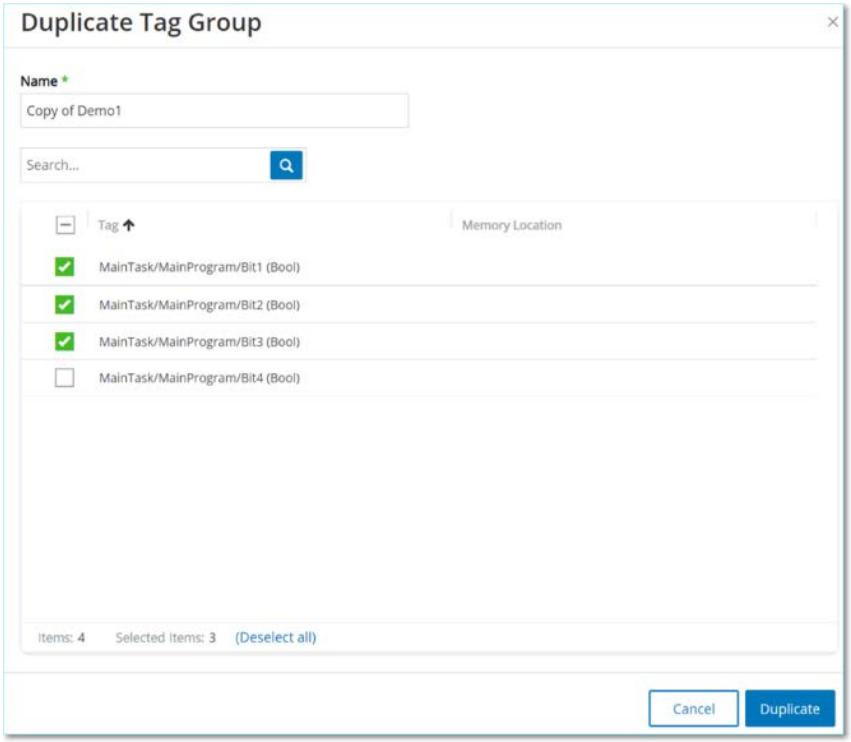
既存のグループと似たような設定で新しいグループを作成する場合は、既存のグループを「複製」できます。グループを複製すると、元のグループに加えて、新しいグループが新しい名前で保存されます。

グループの複製手順

1. **[グループ]**で、目的のグループのタイプを選択します。
2. 新しいグループのベースにする既存のグループを選択します。
3. **[アクション]**をクリックします(またはグループを右クリックします)。
4. ドロップダウンメニューから、**[複製]**を選択します。



5. **[グループの複製]**ウィンドウが表示され、指定したグループタイプに関連するパラメーターが表示されます。



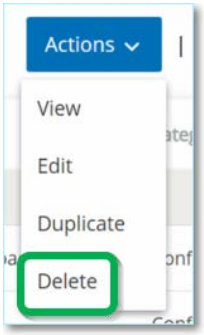
6. **[名前]**フィールドに、新しいグループの名前を入力します(デフォルトでは、新しいグループは元のグループ名「のコピー」という名前になります)。
7. グループ設定に必要な変更を加えます。
8. **[複製]**をクリックします。
   既存のグループに加えて、新しいグループが新しい設定で保存されます。

グループの削除

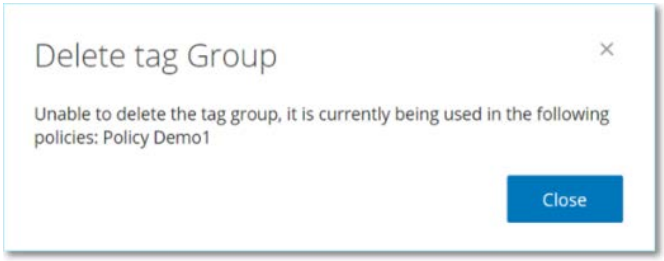
ユーザー定義グループは削除できますが、事前定義グループは削除できません。また、ユーザー定義グループが 1 つ以上のポリシーのポリシー条件として使用されている場合、そのグループは削除できません。

➡ グループの削除手順

1. **[グループ]** で、目的のグループのタイプを選択します。
2. 削除するグループを選択します。
3. **[アクション]** をクリックします (またはグループを右クリックします)。
4. ドロップダウンメニューから、**[削除]** を選択します。



5. 確認ウィンドウが表示されます。

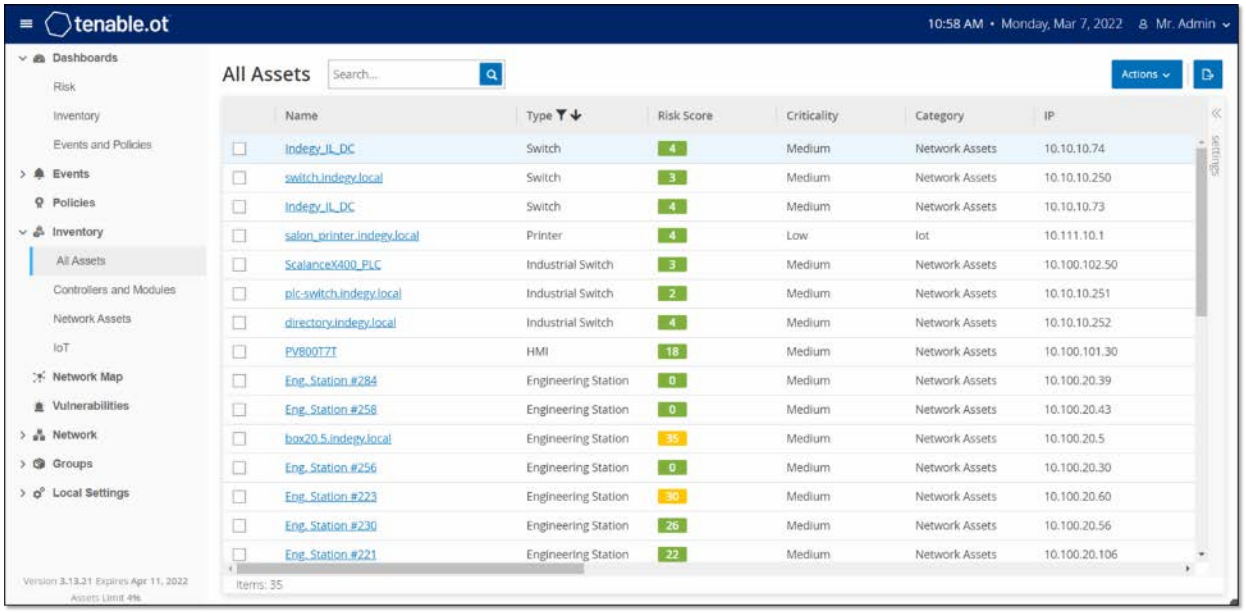


6. **[削除]** をクリックします。
   グループがシステムから完全に削除されます。

インベントリ

Tenable.ot の自動資産検出、分類、管理は、デバイスに対するすべての変更を継続的に追跡することで、正確な最新の資産インベントリを提供します。これにより、運用の継続性、信頼性、安全性を簡単に維持できるようになります。また、メンテナンスプロジェクトの計画、アップグレードの優先順位付け、パッチ展開、インシデント対応、緩和策においても重要な役割を果たします。

資産の表示



ネットワーク内のすべての資産が、インベントリ画面に表示されます。各資産に関する詳細なデータが表示されるため、包括的な資産管理が可能になるだけでなく、各資産とその関連イベントのステータスも監視できます。インベントリ画面に表示されるデータは、Tenable.ot のネットワーク検知およびアクティブクエリ機能を使用して収集されます。**[すべて]** 画面には、すべてのタイプの資産のデータが表示されます。さらに、資産の特定のサブセットが、**[コントローラーおよびモジュール]**、**[ネットワーク資産]**、**[IoT]** の各資産タイプの個別の画面に表示されます。

> *[ネットワーク資産]* 画面には、*[コントローラーとモジュール]* や *[IoT]* 画面に含まれていないすべてのタイプの資産が含まれています。

各資産画面(*すべて*、*コントローラーとモジュール*、*ネットワーク資産*、*IoT*)は、表示される列と各列の位置を調整することで、表示設定をカスタマイズできます。また、資産リストをソートおよびフィルタリングしたり、検索を実行したりすることもできます。カスタマイズ機能の説明については、**リスト**を参照してください。

次の表では、インベントリ画面に表示されるパラメーターについて説明します。

「*」が付いているパラメーターは、[コントローラー]画面にのみ表示されます。

パラメーター	説明
名前	ネットワーク内の資産の名前。資産の名前をクリックして、その資産の[資産の詳細]画面を表示します(**資産詳細の表示**を参照してください)。
IP	資産の IP アドレス。 **注意:** 資産には複数の IP アドレスがある場合があります。 **注意:** Direct のラベルが付いた IP アドレスは、Tenable が直接接続を確立したアドレスです。ラベルがない場合は、Tenable が直接通信せずに IP を検出したことを意味します。 **注意:** 資産は IP 範囲でフィルタリングできます。フィルタリングの詳細については、**フィルタリング**を参照してください。
MAC	資産の MAC アドレス。
ネットワークセグメント	この資産の IP が割り当てられるネットワークセグメント。
タイプ	資産のタイプ。*コントローラー*、*I/O*、*通信*など。**資産タイプ**を参照してください。
バックプレーン*	資産が接続されているバックプレーンユニット。バックプレーン構成に関する追加の詳細が、[資産詳細]画面に表示されます。
スロット*	バックプレーン上にある資産の場合、資産が取り付けられているスロットの番号が表示されます。
ベンダー	資産ベンダー。
ファミリー*	資産ベンダーによって定義された製品のファミリー名。
ファームウェア	現在資産にインストールされているファームウェアのバージョン。
場所	Tenable.ot の資産詳細でユーザーが入力した資産の場所。資産詳細の編集を参照してください。
最終確認時間	デバイスが Tenable.ot によって最後に確認された時間。これは、デバイスがネットワークに接続された、またはアクティビティを実行した最後の時間です。
OS	資産で実行されている OS。
モデル名	資産のモデル名。
状態*	デバイスの状態。可能な値は次のとおりです。 バックアップ - コントローラーはプライマリコントローラーのバックアップとして実行されています。 障害 - コントローラーは障害モードです。 構成なし - コントローラーに構成が設定されていません。 実行中 - コントローラーは実行中です。 停止 - コントローラーは実行されていません。 不明 - 状態は不明です。

パラメーター	説明
説明	Tenable.ot の資産詳細でユーザーが構成した、資産の簡単な説明。資産詳細の編集を参照してください。
リスク	資産に関連するリスクの程度を 0(リスクなし)から 100(非常に高いリスク)の範囲で示す指標。リスクスコアの計算方法の説明については、リスク**評価**を参照してください。
重大度	システムが適切に機能するうえでの資産の重大さの指標。資産タイプに基づいて、各資産に値が自動的に割り当てられます。値は手動で調整できます。
パデューレベル	資産のパデューレベル(0 = 物理プロセス、1 = インテリジェントデバイス、2 = コントロールシステム、3 = 製造オペレーションシステム、4 = ビジネスロジスティクスシステム)。
カスタムフィールド	カスタムフィールドを作成して、資産に関連情報をタグ付けできます。カスタムフィールドは、外部リソースへのリンクにすることができます。

資産タイプ

次の表では、Tenable.ot によって特定されるさまざまな種類の資産について説明します。また、Tenable.ot 管理コンソール(ネットワークマップ画面など)では、各資産タイプを表すアイコンも表示されます。

カテゴリ	デフォルトの重大度レベル / パデューレベル	説明	サブタイプ	
コントローラー	高 / 1	入力デバイスの状態を継続的に監視し、カスタムプログラムに基づいて意思決定を行い、出力デバイスの状態を制御する産業用コンピューター制御システム。このカテゴリには、すべてのタイプのコントローラーとその関連コンポーネントが含まれます。		コントローラー
				PLC
				DCS
				IED
				RTU
				BMS コントローラー
				ロボット
				通信モジュール
				I/O モジュール
				CNC

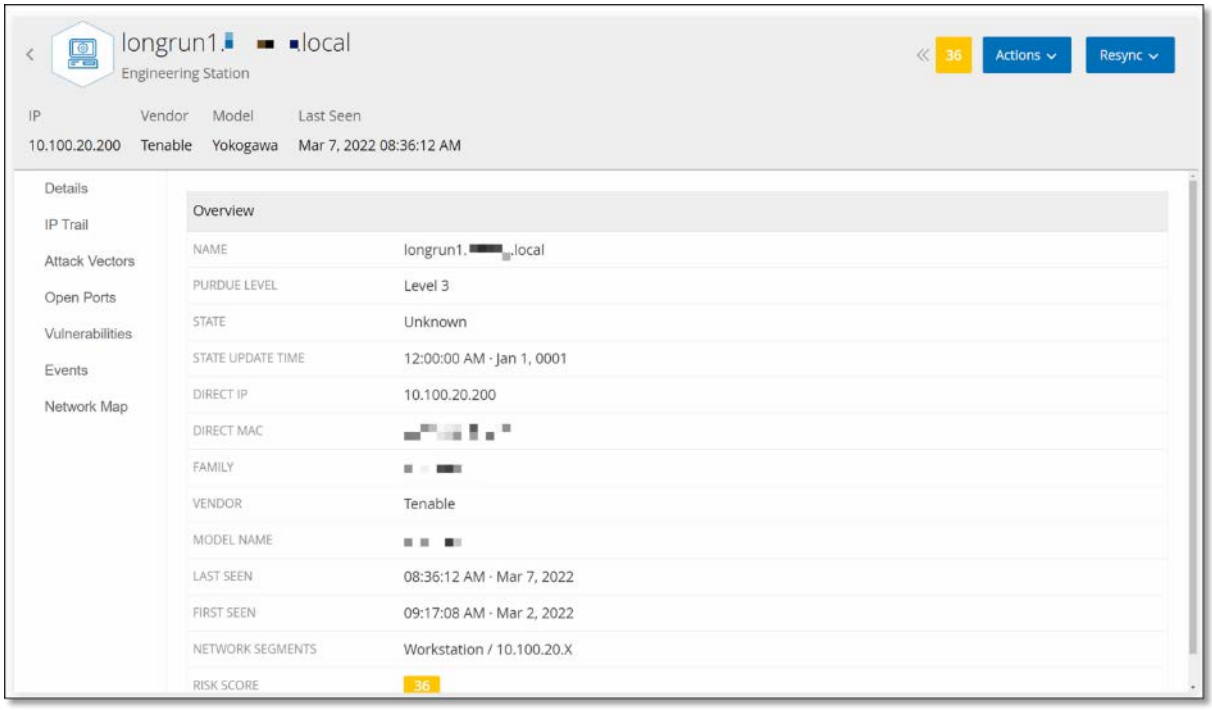
カテゴリ	デフォルトの重大度レベル / パデューレベル	説明	サブタイプ	
				電源
				バックプレーンモジュール
フィールドデバイス	高 / 1	産業用プロトコルを使用して情報を ICS システムに送信する産業用デバイス (センサー、アクチュエーター、電気モーターなど)。		フィールドデバイス
				パワーメーター
				リモート I/O
				リレー
				インバーター
				産業用センサー
				ドライブ
				アクチュエーター
OT デバイス	中 / 2	このカテゴリには、あらゆるタイプの OT デバイスが含まれます。		OT デバイス
				産業用ルーター
				産業用スイッチ
				産業用ゲートウェイ
				産業用ネットワークデバイス
				産業用プリンター
OT サーバー	中 / 2	産業用データにアクセスするために使用されるコンピューター / デバイス。このカテゴリには、		OT サーバー
				ヒストリアン

カテゴリ	デフォルトの重大度レベル / パデューレベル	説明	サブタイプ	
		すべてのタイプの OT サーバーとその関連コンポーネントが含まれます。		HMI
				データロガー
ネットワークデバイス	中 / 3	ネットワークデバイス (スイッチやルーターなど)。このカテゴリには、すべてのタイプのネットワークデバイスとその関連コンポーネントが含まれます。		ネットワークデバイス
				ルーター
				スイッチ
				シリアルイーサネットブリッジ
				ゲートウェイ
				ハブ
				ワイヤレスアクセスポイント
				ファイヤーウォール
				コンバーター
				リピーター
				ラジオ
ワークステーション	低 / 3	ネットワークに接続され、PLC の制御に使用されるコンピューター。このカテゴリには、すべてのタイプのワークステーションとその関連コンポーネントが含まれます。		ワークステーション
				OT ワークステーション
				エンジニアリングステーション
				仮想ワークステーション
サーバー	低 / 3			サーバー

カテゴリ	デフォルトの重大度レベル / パデューレベル	説明	サブタイプ	
		このカテゴリには、さまざまなタイプの IT サーバーが含まれます。		ファイルサーバー
				ウェブサーバー
				仮想サーバー
				セキュリティアプライアンス
				Tenable ICP
				Tenable EM
				Tenable センサー
				ドメインコントローラー
				IoT
IoT	低 / 3	このカテゴリには、さまざまなタイプの相互関連デバイスが含まれます。		カメラ
				パネル
				プロジェクター
				VOIP デバイス
				3D プリンター
				プリンター
				UPS
				IP 電話
				スマートセンサー

カテゴリ	デフォルトの重大度レベル / パデューレベル	説明	サブタイプ	
				バーコードスキャナー
				アクセス制御システム
				照明制御
				HVAC モジュール
				スマートハブ
				スマート TV
				医療機器
				タブレット
				モバイルデバイス
				ストレージデバイス
エンドポイント	低 / 3	ネットワーク内の未識別 IP アドレス。		エンドポイント

資産詳細の表示



[資産詳細]画面には、選択した資産について Tenable.ot によって検出されたすべてのデータに関する包括的な詳細が表示されます。詳細は、ヘッダーバーと一連のタブおよびサブセクションに表示されます。一部のタブとサブセクションは、特定の資産タイプにのみ関連しています。

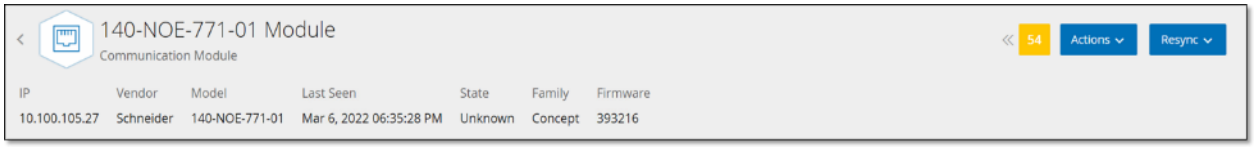
特定の資産に関する[資産詳細]画面にアクセスするには、管理コンソールでリンクとして表示される資産の名前(例:インベントリ、イベント、ネットワークなど)をクリックするか、関連する**[インベントリ]**画面で**[アクション]**>**[表示]**をクリックします。

関連する資産タイプの[資産詳細]画面には、次の要素が含まれています。

- **ヘッダーペイン** – 資産およびその現在の状態に関する重要な情報の概要を表示します。また、その資産のリストを編集できる*[アクション]*メニューも含まれています。
- **詳細** – 詳細情報をさまざまな資産タイプに関連する特定のデータを含むサブセクションに分割して表示します。
- コードリビジョン(コントローラーのみ) – Tenable.ot の「スナップショット」機能により検出された、現在および以前のコードリビジョンに関する情報を表示します。これには、コードに導入された特定の変更に関するすべての詳細、つまり、追加、削除、変更されたセクション(コードブロック / ラング)が含まれます。
- **IP 証跡** – 資産に関連するすべての現在および過去の IP を表示します。
- **攻撃経路** – 脆弱性攻撃経路、つまり攻撃者がこの資産へのアクセスを取得するために使用できるルートを示します。攻撃経路を自動的に生成して、最も重要な攻撃経路を表示したり、特定の資産からの攻撃経路を手動で生成したりできます。
- **オープンポート** – 資産のオープンポートに関する情報を表示します。
- **脆弱性** – 旧式の Windows オペレーティングシステム、特定のタイプのデバイスにとって危険または重要でないことが分かっている脆弱なプロトコルとオープンな通信ポートの使用など、選択した資産に対してシステムが特定した脆弱性を表示します。「**脆弱性**」を参照してください。
- **イベント** – 資産に関連するネットワーク内のイベントのリスト。

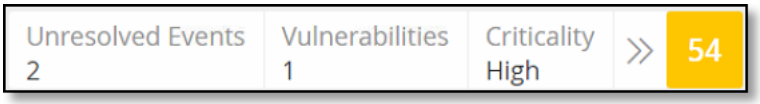
- **ネットワークマップ** - 資産のネットワーク接続をグラフィックで表示します。
- **デバイスポート** (ネットワークスイッチ用) - ネットワークスイッチのポートに関する情報を表示します。

ヘッダーペイン



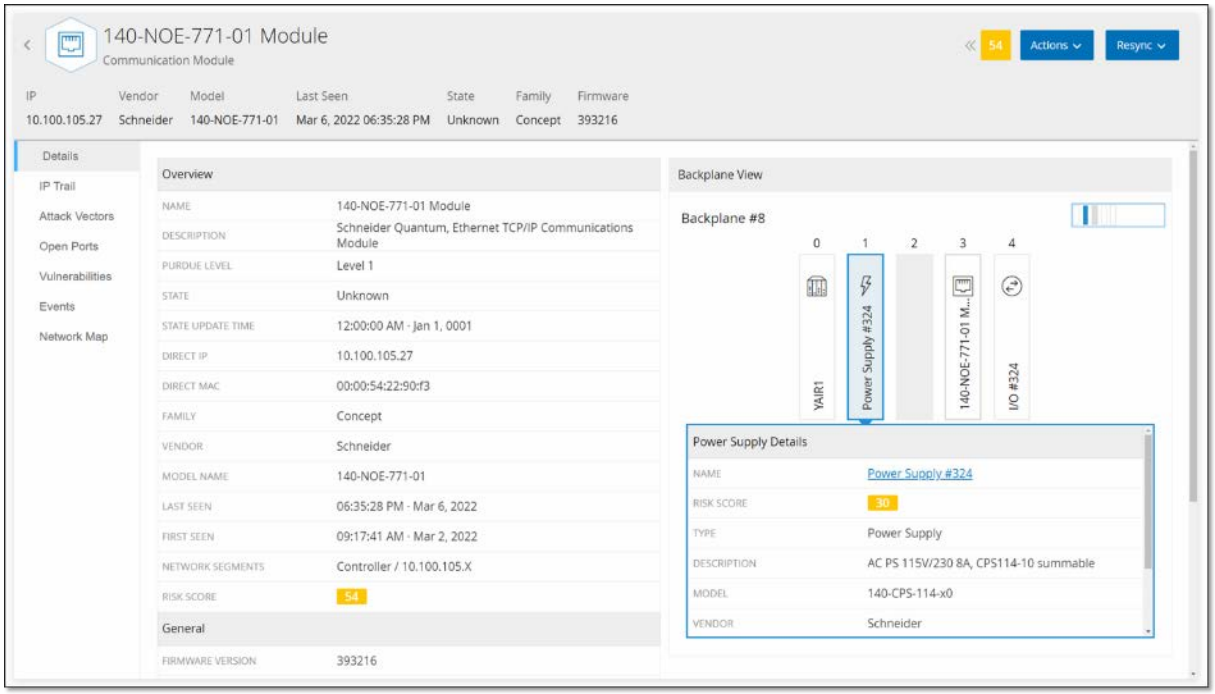
ヘッダーペインには、資産の現在の状態の概要が表示されます。この表示には、次の要素が含まれます。

- **名前** - 資産の名前。
- **戻る (リンク)** - この資産画面にアクセスした画面に戻ります。
- **資産タイプ** - 資産タイプのアイコンと名前を表示します。
- **資産の概要** - IP、ベンダー、ファミリー、モデル、ファームウェア、最終確認時間 (日付と時刻) を含む、資産に関する重要な情報を表示します。
- **リスクスコアウィジェット** - 資産のリスクスコアを表示します。リスクスコアは、資産にもたらされる脅威の程度の評価 (1 ～ 100) です。この値の決定方法の説明については、**リスク評価** を参照してください。[リスクスコア] インジケーターをクリックすると、拡張ウィジェットが表示され、リスクレベルの評価に寄与する要素 (未解決のイベント、脆弱性、重大度) の内訳が表示されます。

  一部の要素は、その要素の詳細を表示する関連画面へのリンクです。
- **アクションメニュー** - 資産詳細を編集したり、Nessus スキャンを実行したりできます。
- **再同期ボタン** - このボタンをクリックして、この資産で利用可能な 1 つ以上のクエリを手動で実行します。**再同期の実行** を参照してください。

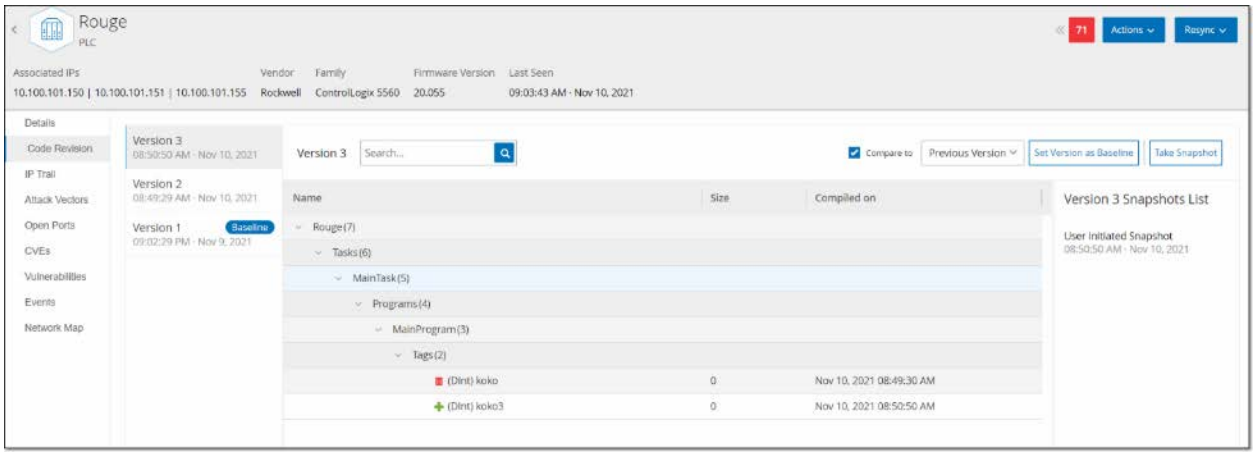
[詳細] タブ



[詳細]タブには、選択した資産に関する追加の詳細が表示されます。情報はいくつかのセクションに分割され、指定した資産のさまざまなタイプのシステムデータおよび構成データが表示されます。指定した資産に関連するセクションのみが表示されます。以下は、さまざまなタイプの資産に対して表示される可能性があるすべてのセクションカテゴリのリストです。*概要*、*一般*、*プロジェクト*、*メモリ*、*イーサネット*、*Profinet*、*OS*、*システム*、*ハードウェア*、*デバイスとドライブ*、*USB デバイス*、*インストールされているソフトウェア*、*IEC -61850*、*インターフェースの状態*。

バックプレーンに接続されている資産の場合、*[バックプレーンビュー]*セクションもあり、接続されている各デバイスのスロット位置を含む、バックプレーン構成をグラフィカルに表示します。デバイスを選択して、下部のペインに詳細を表示します。

コードリビジョン



[コードリビジョン]タブ(コントローラーのみ)には、Tenable.ot の「スナップショット」によってキャプチャされたコントローラーのコードのさまざまなバージョンが表示されます。各「スナップショット」バージョンには、「スナップショット」が作成された時点でのコードリビジョンに関する情報が含まれています。これには、特定のセクション(コードブロック / 実行)とタグに関する詳細が含まれます。「スナップショット」がそのコントローラーの以前の「スナップショット」と同一でない場合は常にコードリビジョンの新しい*バージョン*が作成されます。バージョンを比較して、コントローラーコードに加えられた変更を確認できます。

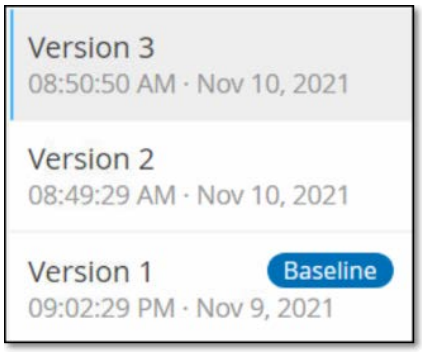
スナップショットは次の方法でトリガーできます。

- **ルーチン** - スナップショットは、システム設定画面でユーザーが設定したとおり、定期的に取得されます。
- **アクティビティ検出** - 特定のコードアクティビティが検出されたときに、システムがスナップショットをトリガーします(例: コードのダウンロード)。
- **ユーザー開始** - ユーザーは、特定の資産の**[スナップショットを作成]**ボタンをクリックすることで、スナップショットを手動でトリガーできます。

「スナップショットの不一致」ポリシーを構成して、コントローラーのコードに加えられた追加、削除、変更を検出できます。**構成イベント - コントローラー検証イベントのタイプ**を参照してください。

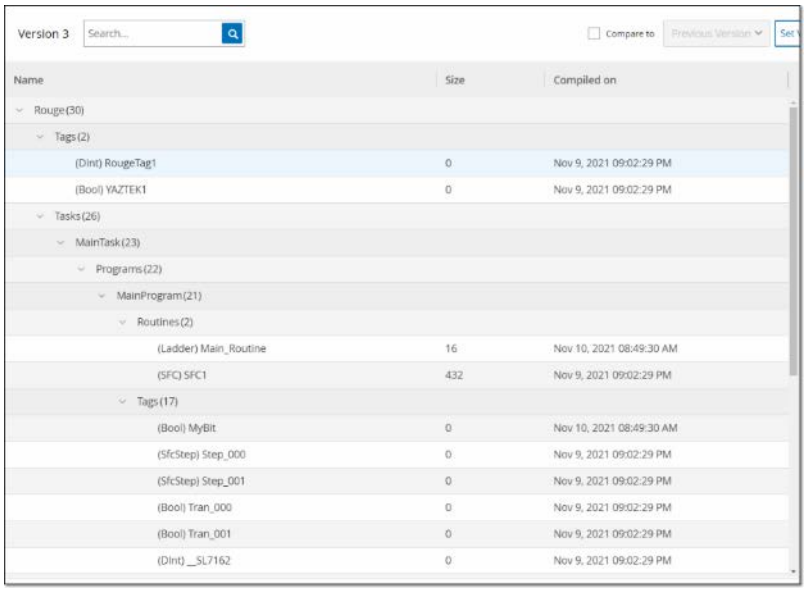
続くセクションでは、コードリビジョン表示のさまざまなセクションと、異なる「スナップショット」バージョンを比較する方法について説明します。

バージョンの選択ペイン



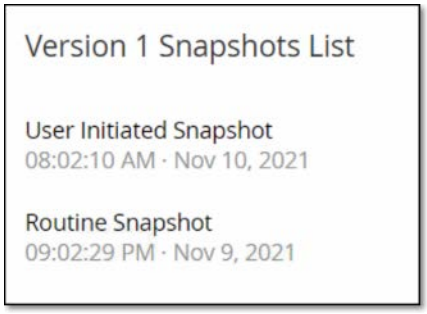
このペインには、このコントローラーのコードリビジョンの利用可能なすべてのバージョンのリストが表示されます。バージョンごとに、そのバージョンの稼働が開始したと認識されている*開始*時刻が表示されます。以前の「スナップショット」からの変更が検出されるたびに、新しいバージョンが作成されます。「ベースライン」タグは、比較の目的でベースラインバージョンとして現在設定されているバージョンを示します。バージョンを選択して、**[スナップショットの詳細]**ペインにコードリビジョンを表示します。

スナップショットの詳細ペイン



詳細ペインには、選択したスナップショットバージョンの特定のコードブロック、ラング、タグに関する詳細情報が表示されます。コード要素は、表示される詳細を展開 / 最小化するための矢印付きのツリー構造で表示されます。各要素について、名前、サイズ、コンパイルした日時が表示されます。選択したバージョンを以前のバージョンまたは「ベースライン」バージョンと比較して、変更内容を確認できます。**スナップショットバージョンの比較**を参照してください。

バージョン履歴ペイン



このペインには、選択されたバージョンをキャプチャした「スナップショット」に関する詳細が表示されます。これには、キャプチャが開始された方法やキャプチャされた日時も含まれます。

スナップショット間で変更が行われなかった場合、複数のスナップショットが単一のバージョンとしてグループ化されます。すべての同一のスナップショットが、そのバージョンの[スナップショット履歴]ペインに一覧表示されます。

スナップショットバージョンの比較

スナップショットバージョンを*以前*のバージョンまたは*ベースライン*のバージョンと比較できます。比較が実行されると、スナップショットの詳細ペインに、2 つのスナップショット間でコントローラーのコードに加えられた変更が表示されます。

変更は次のようにマークされます。

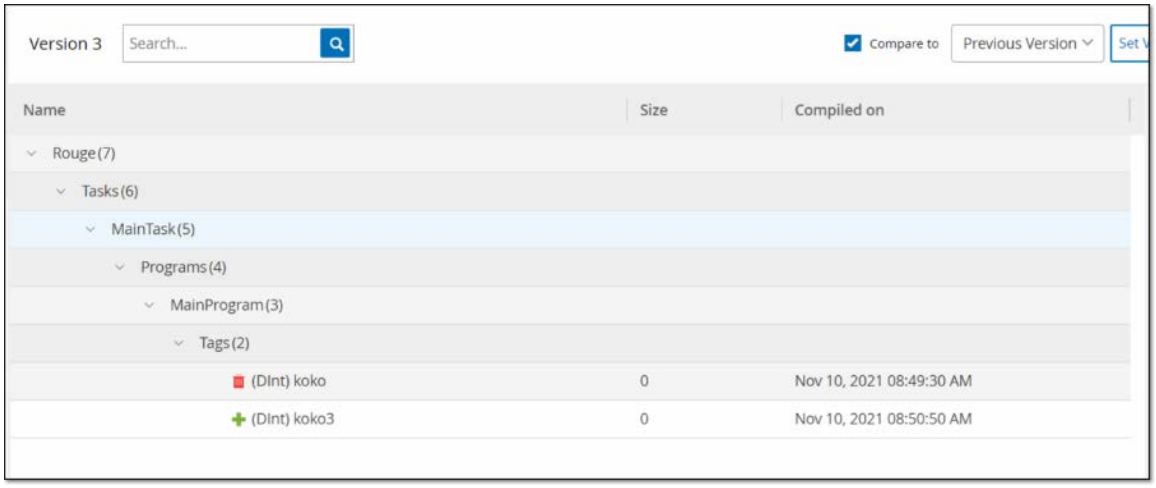
追加済み - 選択したバージョンで追加された新しいコード。

削除済み - 選択したバージョンで削除されたコード。

編集済み - 選択したバージョンで編集されたコード。

スナップショットのバージョンを直前のバージョンと比較する手順

1. **[インベントリ]**>**[コントローラー]**画面で、目的のコントローラーを選択します。
2. **[コードリビジョン]**タブをクリックします。
3. **[バージョンの選択]**ペインで、分析するバージョンを選択します。
4. **[スナップショットの詳細]**ペインの上部にある比較フィールドで、ドロップダウンメニューから**[以前のバージョン]**を選択します。
5. **[比較対象]**チェックボックスをクリックします。
   [スナップショットの詳細]ペインに、2 つのバージョン間のすべての違いが表示されます。変更ごとに、発生した変更のタイプがアイコンで示されます。



スナップショットのバージョンを旧バージョン (直前のバージョン以外) と比較する手順

1. **[インベントリ]**>**[コントローラー]**画面で、目的のコントローラーを選択します。
2. **[コードリビジョン]**タブをクリックします。
3. **[バージョンの選択]**ペインで、比較のベースラインとして使用するバージョンを選択します。
4. **[スナップショットの詳細]**ペインの上部で、**[バージョンをベースラインに設定]**をクリックします。
   選択したバージョンに**[ベースライン]**タグが表示され、ベースラインバージョンとして設定されていることが示されます。

バージョンをベースラインとして設定した場合に影響するのは、その画面を使用した比較だけです。これは、*スナップショットの不一致*をチェックするポリシーには影響しません。

5. **[バージョンの選択]**ペインで、ベースラインと比較するバージョンを選択します。
6. **[比較対象]**チェックボックスをクリックします。
7. [比較対象]チェックボックスの横のフィールドで、ドロップダウンメニューから**[ベースラインバージョン]**を選択します。
   [スナップショットの詳細]ペインに、2 つのバージョン間のすべての違いが表示されます。変更ごとに、発生した変更のタイプがアイコンで示されます。

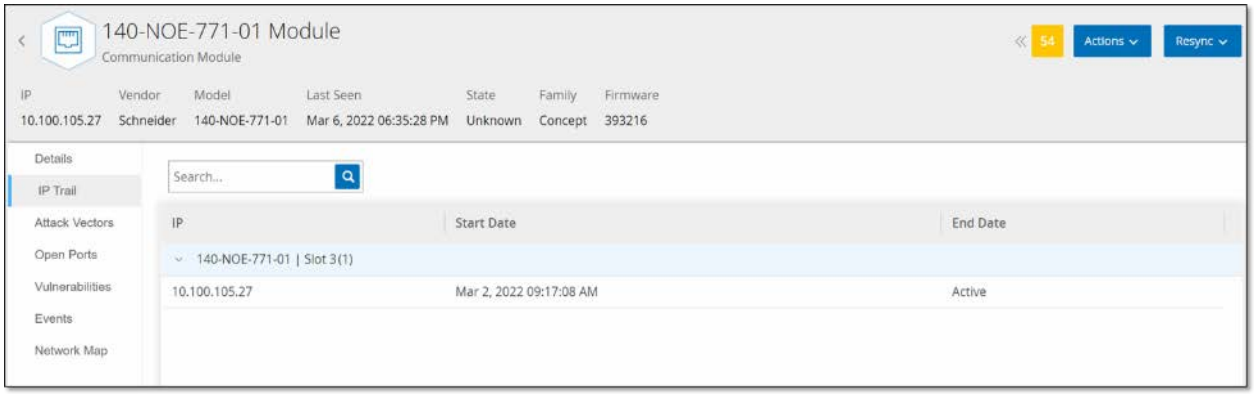
スナップショットの作成

スナップショットは、ユーザーが手動で開始することができます。たとえば、技術者がコントローラーの保守・メンテナンスを行う前後にスナップショットを実行することをお勧めします。

➡ コントローラーのスナップショットの作成手順

1. **[インベントリ]**>**[コントローラー]**画面で、目的のコントローラーを選択します。
2. **[コードリビジョン]**タブをクリックします。
3. **[スナップショットの詳細]**ペインの右上にある**[スナップショットを作成]**をクリックします。
   ユーザーが開始したスナップショットが作成されます。
4. 変更が識別されない場合、新しいユーザー識別スナップショットが最新バージョンの[リビジョン履歴]ペインに追加されます。変更が識別された場合、コードリビジョンの変更を示す新しいバージョンが作成されます。

IP 証跡



[IP 証跡]タブには、この資産に関連するすべての IP が表示されます。[ネットワークカード]列には、この資産で使用されるネットワークカードのリストが表示されます。ネットワークカードの横の矢印をクリックしてリストを展開し、共有バックプレーンに接続されているすべての資産の IP を表示します。

リストには、IP アドレスの使用の開始日と終了日が含まれます。終了日のオプションは次のとおりです。

- **アクティブ** - 現在、IP アドレスはこの資産に使用されています。
- **{日付 / 時間}** - IP アドレスがこの資産に対してアクティブだった最後の日時(過去 30 日以内にアクティブだった場合)。
- **{日付 / 時間}(非アクティブ)** - IP アドレスがこの資産に対してアクティブだった最後の日時(過去 30 日以上非アクティブだった場合)。
- **非アクティブ** - IP アドレスは別の資産によって使用されています。

攻撃経路

攻撃者は、ネットワークの脆弱性、つまり「弱点」を利用して重要な資産にアクセスすることで、重要なアクセスを侵害することができます。重要な資産は攻撃の対象(デスティネーション)であり、*攻撃経路*は攻撃者がその資産にアクセスするために使用するルートです。

攻撃経路を判別する方法

ターゲット資産が指定されると、システムは、この資産へのアクセスを可能にする可能性があるすべての潜在的な攻撃経路を計算し、この資産を危険にさらすリスクが最も高い経路を特定します。最も重大な攻撃経路を特定するため、計算には複数のパラメーターを利用し、リスクベースのアプローチを使用します。使用されるパラメーターを次に示します。

- 資産リスクレベル
- パスの長さ
- 資産間の通信方法
- 外部通信(インターネット / 社内)と内部通信の比較

推奨軽減ステップ

選択した経路を使用して、潜在的な攻撃のリスクを最小限に抑える推奨軽減ステップには以下が含まれます。

- 攻撃経路に含まれる資産の関連リスクスコアおよび個別リスクスコアを低減する。
- 外部ネットワーク(インターネットまたは社内ネットワーク)へのネットワークアクセスを最小化または除去する。
- サプライチェーンの通信経路を調査し、プロセスに対する妥当性を検証する。それほど重要でないものは、潜在的な攻撃経路をなくすために削除する(ポートのクローズ、サービスの除去など)。

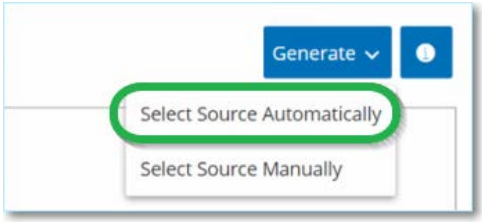
攻撃経路の生成

攻撃経路は、関連するターゲット資産ごとに手動で生成する必要があります。これは、目的のターゲット資産の[攻撃経路]タブで行われます。攻撃経路を生成するには 2 つの方法があります。

- **自動** – Tenable.ot はすべての潜在的な攻撃経路を評価し、最も脆弱な経路を特定します。
- **手動** – 特定のソース資産を指定すると、Tenable.ot は、ターゲット資産にアクセスするために使用できる潜在的な経路(存在する場合)を表示します。

➡ 自動の攻撃経路の生成手順

1. 目的のターゲット資産の**[資産詳細]**ページに移動し、**[攻撃経路]**タブをクリックします。
2. **[生成]**をクリックし、ドロップダウンリストから**[ソースを自動的に選択]**をクリックします。

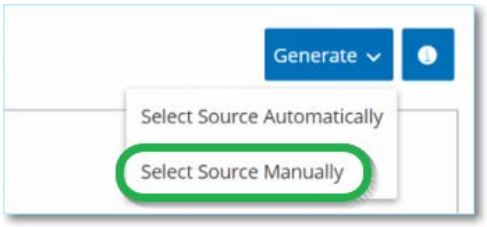


攻撃経路が自動的に生成され、**[攻撃経路]**タブに表示されます。

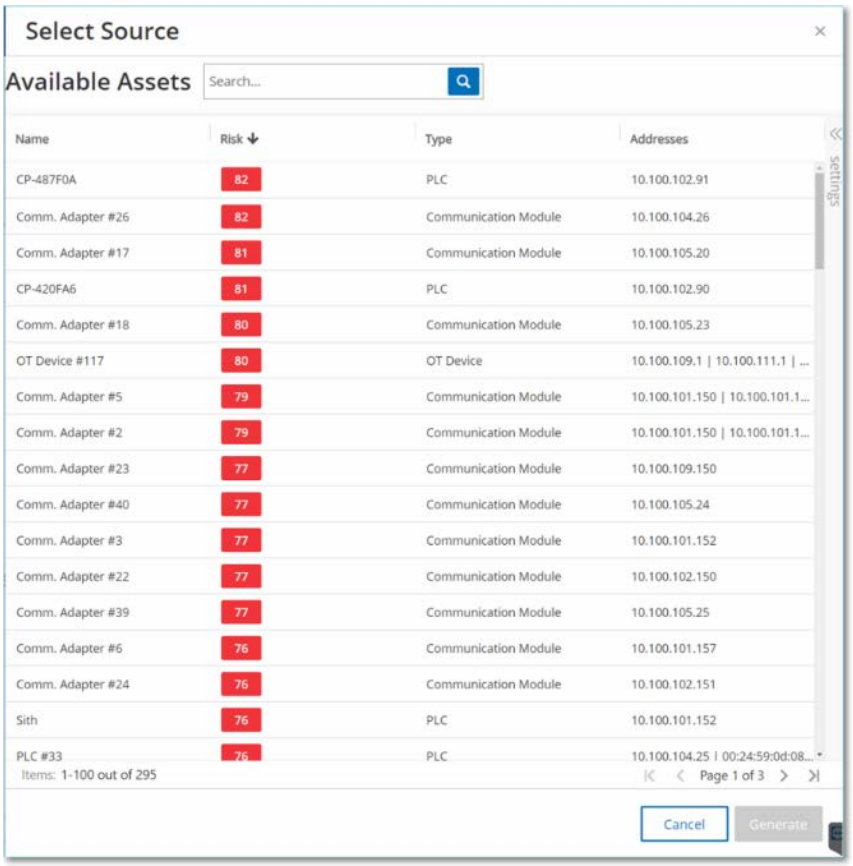
➡ 手動の攻撃経路の生成手順

1. 目的のターゲット資産の**[資産詳細]**ページに移動し、**[攻撃経路]**タブをクリックします。

2. **[生成]**をクリックし、ドロップダウンリストから**[ソースを手動で選択]**をクリックします。



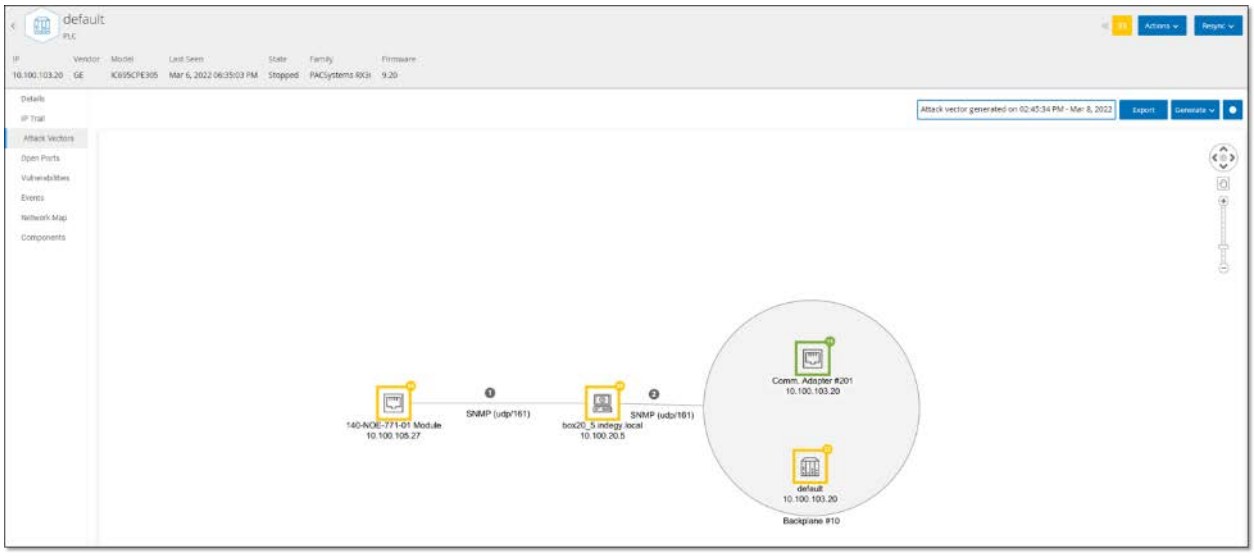
[ソースの選択]ウィンドウが表示されます。



デフォルトでは、ソース資産はリスクスコア順に並んでいます。表示設定を調整したり、目的の資産を検索したりできます。

3. 目的のソース資産を選択します。
4. **[生成]**をクリックします。
   攻撃経路が生成され、**[攻撃経路]**タブに表示されます。

攻撃経路の表示

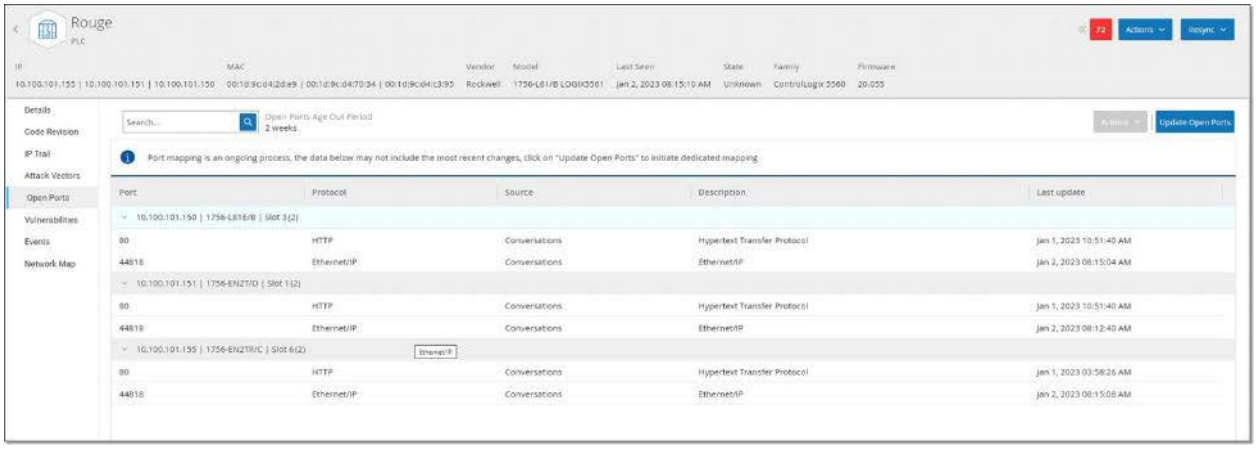


[攻撃経路] タブには、指定されたターゲット資産に対して生成された最も新しい攻撃経路の図が表示されます。[生成] ボタンの横のボックスには、表示された攻撃経路の生成日時が表示されます。攻撃経路の図には、次の要素が含まれます。

- 攻撃経路に含まれる各資産について、リスクレベルと IP アドレスが表示されます。資産アイコンをクリックして、そのリスク要因に関する追加の詳細を表示します。
- ネットワーク接続ごとに、通信プロトコルが表示されます。
- バックプレーンを共有する資産の場合、資産は円で囲まれています。

[攻撃経路] タブの右上にあるヘルプボタンをクリックすると、攻撃経路機能の説明が表示されます。

オープンポート



[オープンポート] タブには、この資産のオープンポートのリストが表示されます。オープンポートごとに、使用するプロトコル、機能の説明、データが最後に更新された日時、ポートが開いていることを示す情報ソース (アクティブクエリ、ポートマッピング、会話、NNM または Nessus スキャン) に関する詳細が提供されます。資産で利用可能な IP ごとに、オープンポートの個別のリストが表示されます (共有バックプレーンを通じてアクセスされるポートも含みます)。IP の横の矢印をクリックしてリストを開き、オープンポートを表示します。

オープンポートのタイムアウト期間経過後、ポートがまだ開いていることを示す情報を受信しない場合、オープンポートのリストからそのポートが自動的に削除されます。デフォルトの期間は 2 週間です。オープンポートのタイムアウト期間の長さを調整するには、**デバイス**を参照してください。

オープンポートのスキャンパラメーターは、**[ローカル設定]** タブで構成されます。**すべてのコントローラークエリ**を参照してください。選択した資産の手動クエリを実行して、オープンポートのリストを更新することもできます。

➡ オープンポートのリストの手動更新手順

1. **[インベントリ]>[コントローラー / ネックワーク資産]** 画面で、目的の資産を選択します。
   [資産詳細] 画面が表示されます。
2. **[オープンポート]** タブをクリックします。
3. [オープンポート] ペインの右上にある **[オープンポートの更新]** をクリックします。
   新しいスキャンが実行され、このコントローラーに表示されているオープンポートが更新されます。

[オープンポート] タブのその他のアクション

特定の資産の [オープンポート] タブで、特定のオープンポートに対して次のアクションも実行できます。

- スキャン - 選択したポートのスキャンを実行します。
- 表示 - デバイスのウェブインターフェースにアクセスすることで、デバイスに関するその他の詳細と診断を表示します。

➡ 特定のポートでのスキャンの実行手順

1. **[インベントリ]>[コントローラー / ネックワーク資産]** 画面で、目的の資産を選択します。
   [資産詳細] 画面が表示されます。
2. **[オープンポート]** タブをクリックします。
3. 特定のポートを選択します。
4. **[アクション]** メニューをクリックします。
5. ドロップダウンメニューから、**[スキャン]** を選択します。
   Tenable.ot は選択されたポートでスキャンを実行します。

➡ 資産のポータルの表示手順

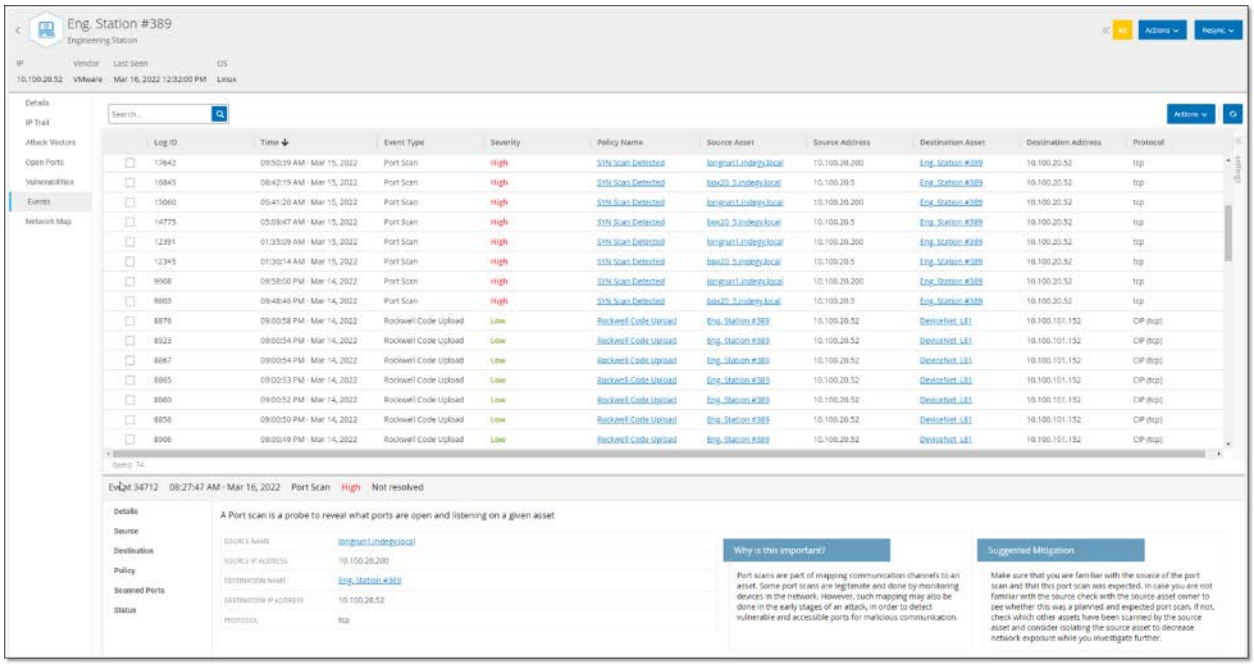
このオプションは、ポート 80 (ウェブアクセスに使用) がオープンポートの 1 つである場合にのみ使用できます。

1. **[インベントリ]>[コントローラー / ネックワーク資産]** 画面で、目的の資産を選択します。
   [資産詳細] 画面が表示されます。
2. **[オープンポート]** タブをクリックします。
3. 特定のポートを選択します。
4. **[アクション]** メニューをクリックします。
5. ドロップダウンメニューから、**[表示]** を選択します。
   新しいブラウザタブが開き、その資産の資産ポータルが表示されます。

脆弱性

[脆弱性]タブには、Tenable.ot プラグインによって検出された、指定された資産に影響を与えるすべての脆弱性のリストが表示されます。システムは、旧式の Windows オペレーティングシステム、特定のタイプのデバイスにとって危険または重要でないことが分かっている脆弱なプロトコルとオープンな通信ポートの使用などの脆弱性を特定します。各リストには、脅威の性質とその深刻度に関する詳細が表示されます。このタブに表示される情報は、指定した資産に関連する脆弱性のみがここに表示されることを除いて、**[リスク]>[脆弱性]画面に表示される情報と同じ**です。脆弱性情報の説明については、**脆弱性**を参照してください。

イベント



[イベント]タブには、Tenable.ot プラグインによって検出された、資産に関連するネットワーク内のイベントの詳細リストが表示されます。表示される列と各列の位置を調整することで、表示設定をカスタマイズできます。イベントは、さまざまなカテゴリ(イベントタイプ、深刻度、ポリシー名など)に従ってグループ化できます。また、イベントリストをソートおよびフィルタリングしたり、検索を実行したりすることもできます。カスタマイズ機能の説明については、**リスト**を参照してください。

画面の下部には、選択されたイベントに関する詳細情報がタブに分割されて表示されます。選択したイベントのイベントタイプに関連するタブのみが表示されます。イベントの詳細については、**イベント**を参照してください。

ペインの上部に**[アクション]**ボタンがあり、選択したイベントで次のアクションを実行できます。

- 解決 - このイベントを解決済みとしてマークします。
- PCAP のダウンロード - このイベントの PCAP ファイルをダウンロードします。
- 除外 - このイベントのポリシー除外を作成します。

これらのアクションの詳細については、**イベント**の章を参照してください。

各イベントリストに表示される情報について、次の表で説明します。

パラメーター	説明
ログ ID	イベントを参照するためにシステムによって生成される ID。
時間	イベントが発生した日時。
イベントタイプ	イベントをトリガーしたアクティビティのタイプの説明。イベントは、システムに設定されているポリシーによって生成されます。さまざまなタイプのポリシーの説明については、**ポリシーのタイプ**を参照してください。
深刻度	イベントの深刻度レベルを表示します。以下は、可能な値の説明です。 なし - 心配は不要です。 情報 - 現時点では心配はありませんが、都合の良いときに確認する必要があります。 警告 - 潜在的に害のあるアクティビティが発生したことに対する中程度の深刻度レベルで、都合の良いときに対処する必要があります。 重大 - 潜在的に害のあるアクティビティが発生したことに対する深刻度の高いレベルで、すぐに対処する必要があります。
ポリシー名	イベントを生成したポリシーの名前。名前は、ポリシーリストへのリンクになっています。
ソース資産	イベントを開始した資産の名前。このフィールドは、資産リストへのリンクになっています。
ソースアドレス	イベントを開始した資産の IP または MAC。
デスティネーション資産	イベントの影響を受けた資産の名前。このフィールドは、資産リストへのリンクになっています。
デスティネーションアドレス	イベントの影響を受けた IP または MAC。
プロトコル	関連する場合は、このイベントを生成した会話に使用されたプロトコルを示します。

イベントカテゴリ	イベントの一般的なカテゴリを表示します。 **注意:** [すべてのイベント] 画面には、すべてのタイプのイベントが表示されます。それぞれの特定のイベント画面には、指定されたカテゴリのイベントのみが表示されます。 以下は、イベントカテゴリの簡単な説明です (詳細な説明については、**ポリシーカテゴリ**を参照してください)。 • 構成イベント - 2 つのサブカテゴリが含まれます。 • コントローラー検証イベント - これらのポリシーは、ネットワークのコントローラーで発生する変更を検出します。 • コントローラーアクティビティイベント - アクティビティポリシーは、ネットワークで発生するアクティビティに関連しています (つまり、ネットワークの資産間に実装された「コマンド」)。 • SCADA イベント - コントローラーのデータプレーンに加えられた変更を識別するポリシーです。 • ネットワーク脅威イベント - これらのポリシーは、侵入の脅威を示すネットワークトラフィックを特定します。 • ネットワークイベント - ネットワーク内の資産および資産間の通信ストリームに関連したポリシーです。
ステータス	イベントが解決済みとしてマークされているかどうかを示します。
解決者	解決済みイベントについて、どのユーザーがイベントを解決済みとしてマークしたかを示します。
解決日	解決済みイベントについて、いつイベントが解決済みとしてマークされたかを示します。
コメント	イベントの解決時に追加されたコメントを表示します。

ネットワークマップ

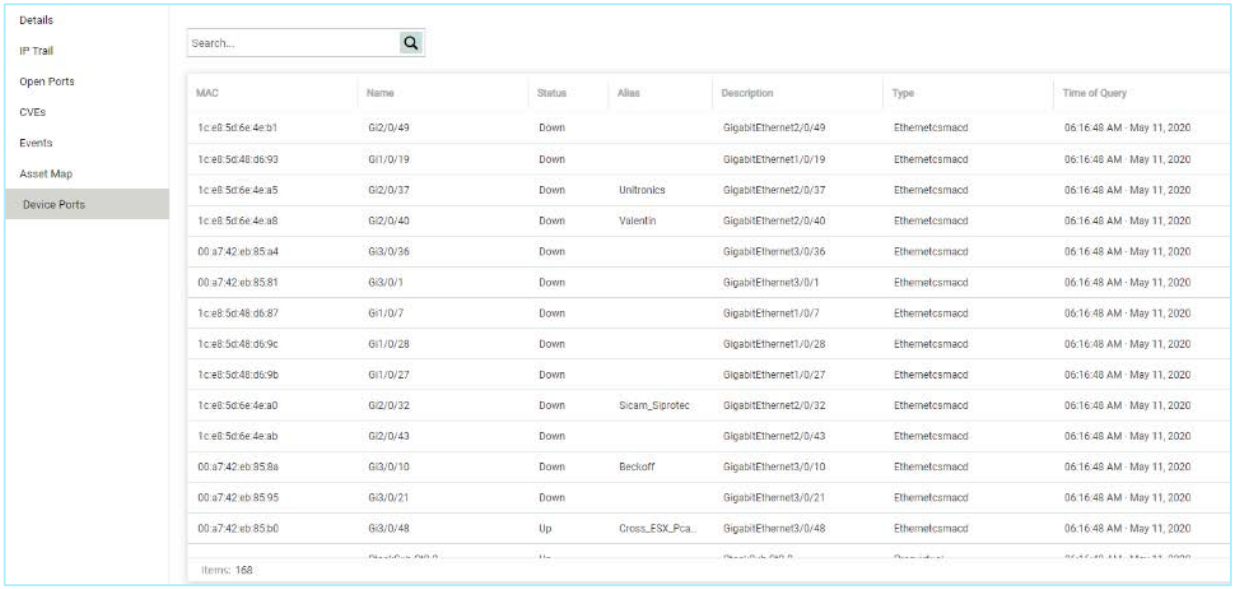
[ネットワークマップ]タブは、資産のネットワーク接続をグラフィックで表示します。このビューには、選択した資産が過去 30 日間に行ったすべての接続が表示されます。

このタブに表示される情報は、**[ネットワークマップ]**画面に表示される情報と類似していますが、ここに表示される情報はこの特定の資産に関連する接続に限定されます。また、この画面には、ネットワークマップのメイン画面に示されているような資産のグループへの接続ではなく、個々の資産への接続が表示されます。このタブに表示される情報の説明については、**ネットワークマップ**を参照してください。

すべての資産のネットワークマップを表示するには、**[ネットワークマップに移動]**ボタンをクリックします。クリックすると、ネットワークマップが動的に拡大し、この資産にフォーカスして、他の資産グループへの接続を表示します。

マップ上の接続された資産のいずれかをクリックするとその資産の詳細が表示され、資産名のリンクをクリックすると選択した資産の詳細画面に移動します。

デバイスポート



ネットワークスイッチの［**デバイスポート**］タブが表示されます。ネットワークスイッチのポートに関する詳細情報が表示されます。このデータは、スイッチに対する SNMP クエリを使用して収集されます。各ポートについて、*MAC* アドレス、*名前*、接続ステータス（アップまたはダウン）、*エイリアス*、*説明*の情報が表示されます。

このタブは、アカウントでアクティブ化されている場合にのみ使用できます。この機能をアクティブ化するには、サポート担当者に連絡してください。

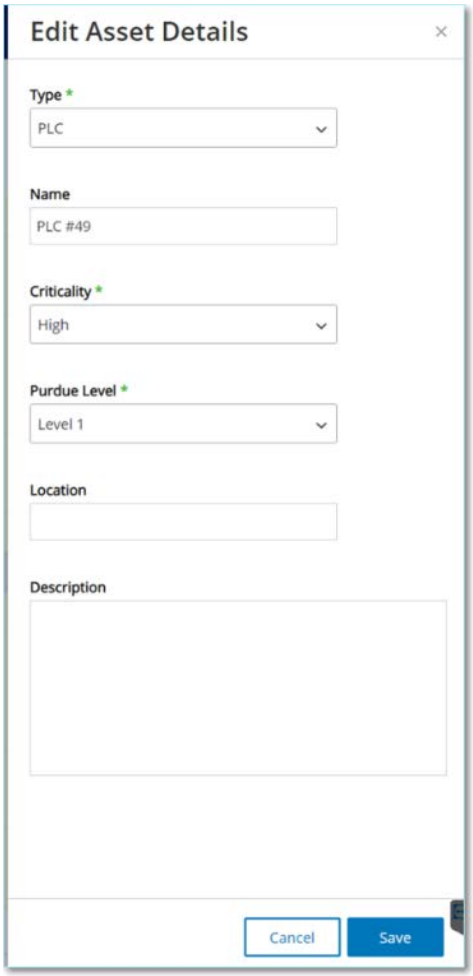
資産詳細の編集

Tenable.ot は、内部データとネットワークでのアクティビティに基づいて、資産のタイプと名前を自動的に識別します。システムがこの情報を収集できない場合や自動識別が正確でないと思われる場合は、直接 UI から、または CSV ファイルをアップロードすることでこれらのパラメーターを編集できます。資産の一般的な説明とユニットの場所の説明を追加することもできます。

UI による資産詳細の編集

➡ 1 つの資産の資産詳細の編集手順

1. **[インベントリ]** で、**[コントローラー]** または **[ネットワーク資産]** をクリックします。
2. 目的の資産を選択します。
3. ヘッダーバーの **[アクション]** ボタンをクリックします。
4. ドロップダウンリストから、**[編集]** を選択します。
   [資産詳細の編集] ウィンドウが開きます。



5. **[タイプ]** フィールドで、ドロップダウンリストから資産タイプを選択します。
6. **[名前]** フィールドに、Tenable.ot UI で資産を識別するための名前を入力します。
7. **[重大度]** フィールドに、システムにとってのこの資産の重大度レベルを入力します。
8. **[パデューレベル]** フィールドに、資産タイプに基づいたパデューレベルを入力します。
9. **[バックプレーン]** フィールド(コントローラー用)に、資産がインストールされているバックプレーンの名前を入力します。
10. **[場所]** フィールドに、資産の場所の説明を入力します。これはオプションのフィールドです。データは、資産テーブルとこの資産の[資産詳細]画面に表示されます。

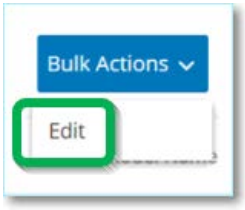
11. **[説明]** フィールドに、資産の説明を入力します。これはオプションのフィールドです。データは、この資産の [資産詳細] 画面に表示されます。
12. **[保存]** をクリックします。
    編集した詳細がその資産に保存されます。

複数の資産の編集 (一括プロセス) 手順

1. **[インベントリ]** で、**[コントローラー]** または **[ネットワーク資産]** をクリックします。
2. 目的の各資産の横にあるチェックボックスを選択します。

> または、目的の各資産をクリックしながら **Shift** キーを押すことで、複数の資産を選択できます。

3. **[一括アクション]** メニューをクリックし、ドロップダウンリストから **[編集]** を選択します。



[一括編集] 画面で、一括編集に利用できるパラメーターが表示されます。

4. 編集する各パラメーター (*タイプ*、*重大度*、*パデューレベル*、*ネットワークセグメント*、*場所*、*説明*) の横にあるチェックボックスを選択します。

> ネットワークセグメントを一括編集する場合、まず資産をタイプでフィルターし、次に一括編集する資産を選択します。
> 複数の IP アドレスを持つ資産は、ネットワークセグメントの一括編集に含めることができません。各資産を手動で編集する必要があります。

5. 各パラメーターを必要に応じて設定します。

> [一括編集] フィールドに情報を入力すると、選択された資産の現在の内容が上書きされます。パラメーターの横のチェックボックスを選択して、選択を入力しない場合でも、そのパラメーターの現在の値は消去されます。

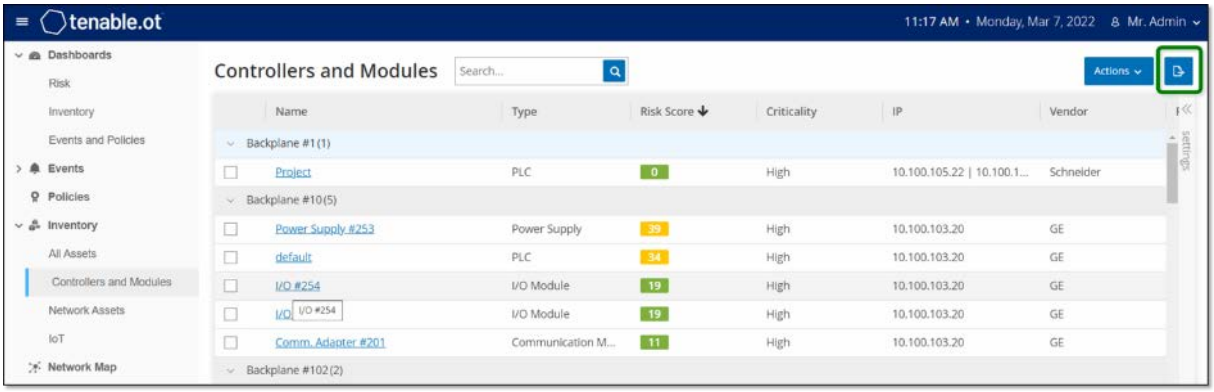
6. **[保存]** をクリックします。
    資産が新しい構成で保存されます。

CSV のアップロードによる資産詳細の編集

この方法で資産詳細を編集すると、UI で手動で編集する代わりに、csv ファイルで数多くの資産を編集できます。この方法を使用して、*タイプ*、*名前*、*重大度*、*パデューレベル*、*場所*、*説明*、カスタムフィールドの詳細を編集できます。

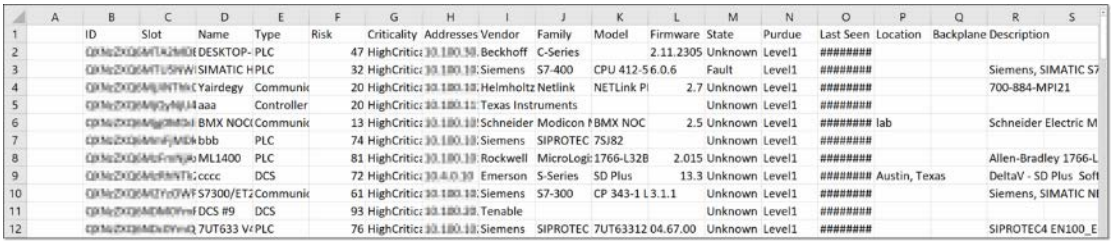
➡ CSV で資産詳細を編集する手順

1. **[インベントリ]**で、**[すべての資産]**、**[コントローラー]**と**[モジュール]**、または**[ネットワーク資産]**をクリックします。
2. **[エクスポート]**ボタンをクリックします。



インベントリの csv ファイルがダウンロードされます。

3. ダウンロードしたばかりのファイルに移動して開きます。



	ID	Slot	Name	Type	Risk	Criticality	Addresses	Vendor	Family	Model	Firmware	State	Purdue	Last Seen	Location	Backplane	Description
2			DESKTOP-	PLC		47	HighCritic	Beckhoff	C-Series		2.11.2305	Unknown	Level1	########			
3			SIMATIC H	PLC		32	HighCritic	Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	########			Siemens, SIMATIC S7
4			Yairdegy	Communic		20	HighCritic	Helmholtz	Netlink	NETLink PI	2.7	Unknown	Level1	########			700-884-MPI21
5			aaa	Controller		20	HighCritic	Texas Instruments				Unknown	Level1	########			
6			BMX NOC	Communic		13	HighCritic	Schneider	Modicon I	BMX NOC	2.5	Unknown	Level1	########	lab		Schneider Electric M
7			bbb	PLC		74	HighCritic	Siemens	SIPROTEC	7SJ82		Unknown	Level1	########			
8			ML1400	PLC		81	HighCritic	Rockwell	MicroLogi	1766-L32B	2.015	Unknown	Level1	########			Allen-Bradley 1766-L
9			cccc	DCS		72	HighCritic	Emerson	S-Series	SD Plus	13.3	Unknown	Level1	########	Austin, Texas		DeltaV - SD Plus Soft
10			S7300/ET2	Communic		61	HighCritic	Siemens	S7-300	CP 343-1 L	3.1.1	Unknown	Level1	########			Siemens, SIMATIC NI
11			DCS #9	DCS		93	HighCritic	Tenable				Unknown	Level1	########			
12			7UT633 V4	PLC		76	HighCritic	Siemens	SIPROTEC	7UT63312	04.67.00	Unknown	Level1	########			SIPROTEC4 EN100_E

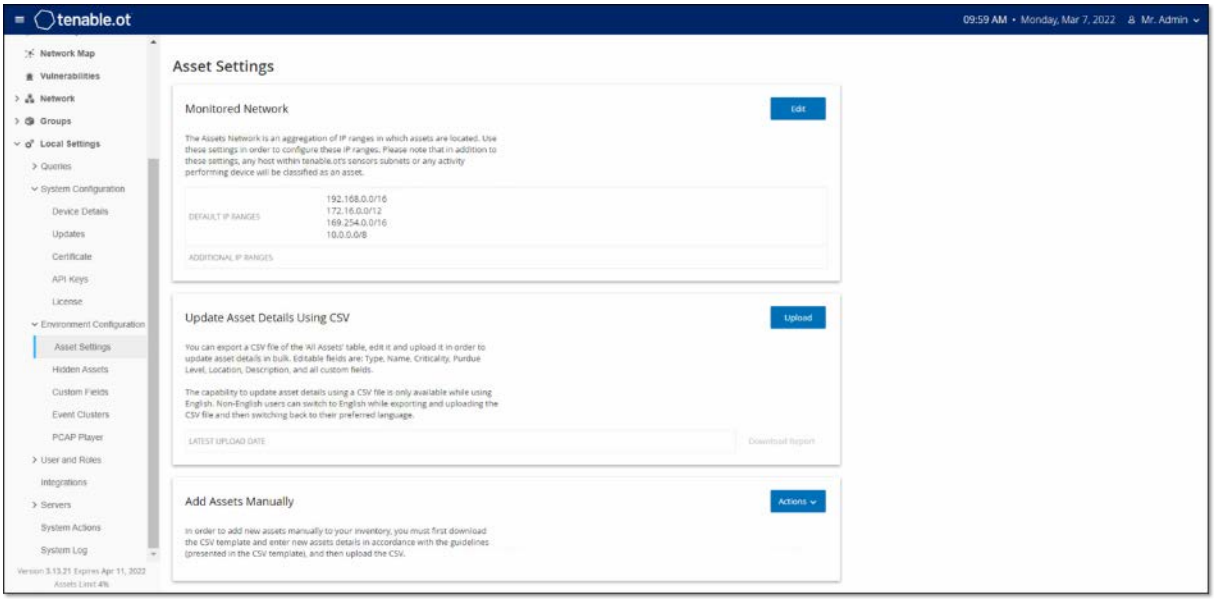
4. セルの内容を変更して、許容可能なパラメーターを編集します(許容可能なパラメーターは、*タイプ*、*名前*、*重大度*、*パデューレベル*、*場所*、*説明*、カスタムフィールドです)。

> 特定のオプション(タイプ、重大度、パデューレベルなど)を必要とするパラメーターには有効なデータを入力する必要があります。入力しないと、対応する資産は更新されません。

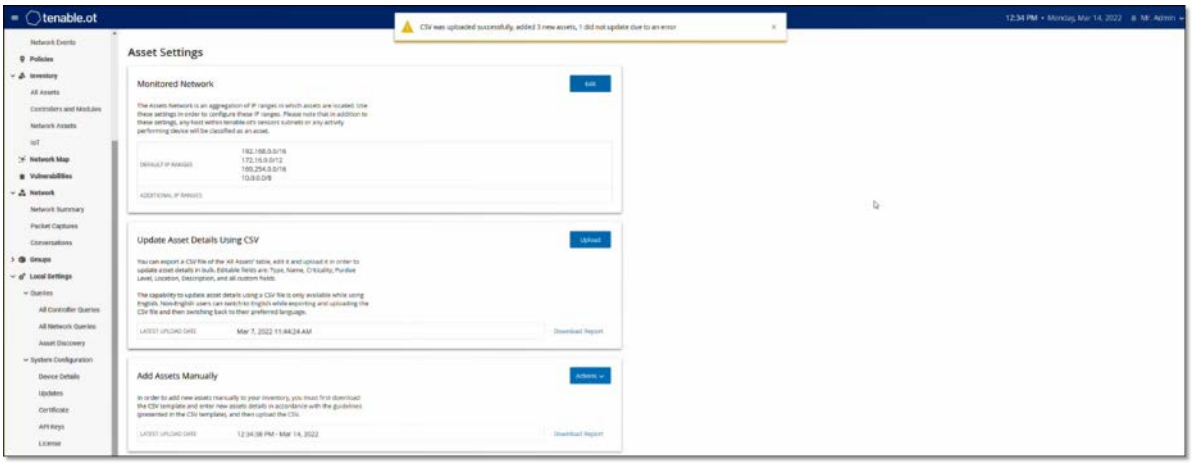
5. ファイルを csv ファイルタイプとして保存します。

> 変更した資産のみがシステムで更新されます。csv に含まれていない資産、または変更していない行は、システムで変更されません。また、この方法を使用して資産を削除することはできません。

6. **[ローカル設定]**で、**[環境構成]**>**[資産設定]**に移動します。
   [資産設定]画面が表示されます。



7. **[CSV を使用して資産詳細を更新]**セクションで、**[アップロード]**をクリックします。
8. デバイスのナビゲーションプロンプトに従って、保存したばかりの csv ファイルをアップロードします。
   正常に更新された行数を示す確認が表示されます。



   [CSV を使用して資産詳細を更新]セクションの**[最終アップロード日]**フィールドが更新されます。
9. アップロードの結果に関する詳細情報を表示するには、**[CSV を使用して資産の詳細を更新]**セクションで、**[レポートのダウンロード]**をクリックします。
   正常に更新された資産 ID と失敗した資産 ID を詳述する csv ファイルがダウンロードされます。

資産の非表示

1 つ以上の資産を資産インベントリから非表示にすることができます。非表示にした資産は、インベントリに表示されず、グループから削除されます。ただし、非表示の資産についても引き続き、イベントとネットワークアクティビティが表示されます。

非表示にした資産は、**[ローカル設定]**>**[資産]**>**[非表示の資産]**画面から復元できます。 **ローカル設定**を参照してください。

➡ 1 つ以上の資産を非表示にする手順

1. **[インベントリ]**で、**[コントローラー]**または**[ネットワーク資産]**をクリックします。
2. 削除する 1 つ以上の資産の横のチェックボックスを選択します。

3. ヘッダーバーの**[アクション]**ボタンをクリックします。
4. ドロップダウンリストから、**[資産を非表示にする]**を選択します。
   [非表示の資産]ウィンドウが開きます。
5. **[コメント]**フィールドで、資産に関する自由形式テキストのコメントを追加できます。(オプション)

> **[ローカル設定]** > **[資産]** > **[非表示の資産]** 画面の削除された資産のリストにコメントが表示されます。

6. **[非表示]**をクリックします。
   資産は、インベントリおよびグループから非表示になります。

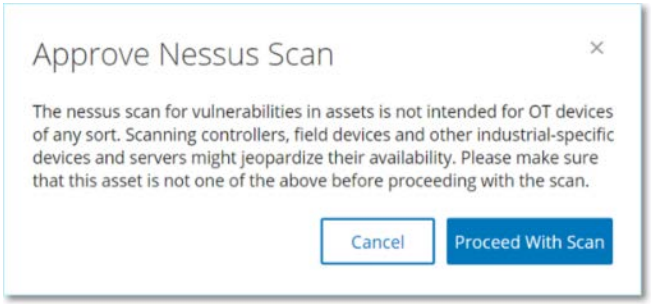
資産特定 Nessus スキャンの実行

Nessus は、脆弱性を検出するために IT デバイスをスキャンする Tenable ツールです。Tenable.ot は、OT ネットワーク内の特定の IT 資産で Nessus の「基本ネットワークスキャン」を実行できます。これは、サーバーデバイスおよびネットワークデバイスの脆弱性に関する追加情報を収集するアクティブなフルシステムスキャンです。このスキャンでは、WMI および SNMP の認証情報がユーザーによって提供されている場合、その情報を使用します。このアクションは、関連する PC ベースのマシンでのみ利用可能です。スキャンの結果が、**[脆弱性]**画面に表示されます。また、カスタマイズされたスキャンを作成して、特定のネットワーク資産のセットで Nessus プラグインの特定のセットを実行することもできます。**Nessus プラグインスキャン**を参照してください。

> Nessus は、IT 環境で最適に動作する侵入型ツールです。通常の動作に干渉する可能性があるため、OT デバイスでの使用はお勧めしません。

➡ Nessus スキャンを手動で実行する手順

1. **[インベントリ]**で、**[ネットワーク資産]**をクリックします。
2. 目的の資産を選択します。
3. ヘッダーバーの**[アクション]**ボタンをクリックします。
4. ドロップダウンリストから、**[Nessus スキャン]**を選択します。
   [Nessus スキャンの承認]確認ウィンドウが表示されます。



5. **[スキャンに進む]**をクリックします。
   Nessus スキャンが実行されます。

再同期の実行

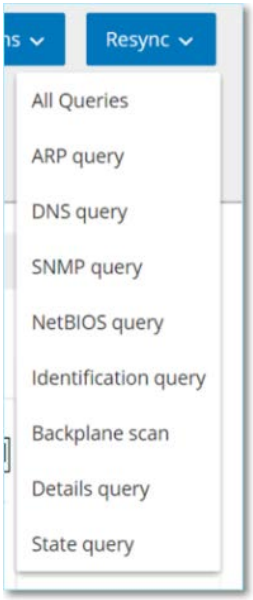
再同期機能は、この資産の最新情報を取得するために、ネットワークとコントローラーに対して 1 つ以上のクエリを開始します。利用可能なすべてのクエリを実行することも、特定のクエリを選択して実行することもできます。以下は、「再同期」で利用可能なクエリです。

- **バックプレーンスキャン** - バックプレーン内のモジュールとその仕様を検出します。

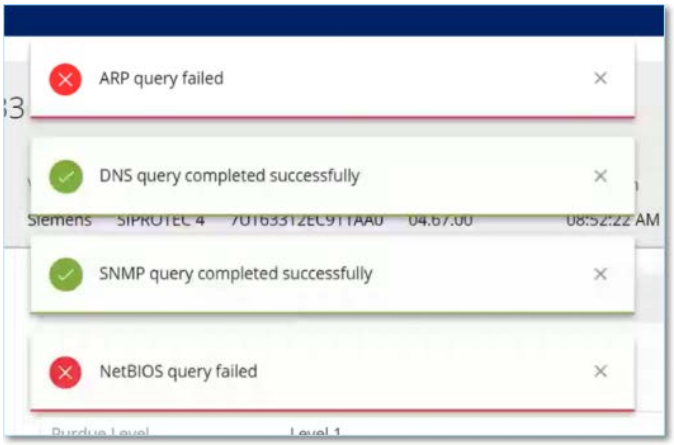
- **DNS スキャン** - ネットワーク内の資産の DNS 名を検索します。
- **詳細クエリ** – コントローラーのハードウェアとファームウェアの詳細を取得します。結果は、**[資産]>[コントローラー]** 画面の **[ファームウェア]** フィールドに表示されます。
- **識別クエリ** – 複数のプロトコルを使用して、資産の識別を試みます。
- **NetBIOS クエリ** - ネットワーク内の Windows マシンの分類と検出のために送信される NetBIOS ユニキャストパケットを送信します。
- **SNMP クエリ** (SNMP が有効な資産用) – SNMP が有効な資産の構成の詳細を取得します。
- **状態** – 資産の現在のステータスを検出します (実行中、停止中、障害、構成なし、テスト)。
- **ARP** - ネットワークで検出された新しい IP の MAC アドレスを取得します。結果は、**[詳細]>[概要]** 画面の **[MAC]** フィールドに表示されます。

資産データの再同期の実行手順

1. 目的の資産の **[資産詳細]** 画面で、[ヘッダー] ペインの **[再同期]** ボタンをクリックします。
2. クエリのドロップダウンリストが表示されます。



3. 実行するクエリをクリックするか、*[すべてのクエリ]* をクリックして利用可能なすべてのクエリを実行します。
4. 各クエリが実行されると、ポップアップ通知にクエリのステータスが表示されます。



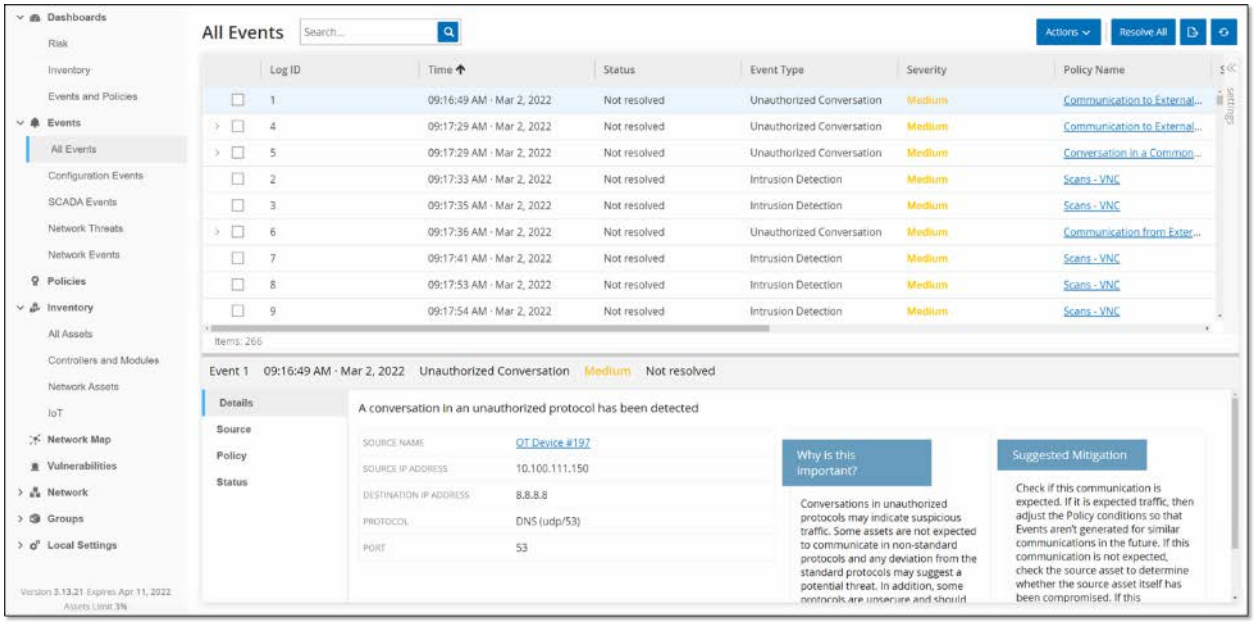
クエリが正常に実行されるたびに、この資産のシステムデータは新しいデータに基づいて更新されます。

イベント

イベントは、ネットワーク内の潜在的に危険なアクティビティに対する注意を促すためにシステムで生成された通知です。イベントは、*構成イベント*、*SCADA イベント*、*ネットワーク脅威*、*ネットワークイベント*のいずれかのカテゴリでシステムに設定されたポリシーによって生成されます。深刻度レベルが各ポリシーに割り当てられ、イベントの深刻度を示します。

ポリシーがアクティブ化されると、そのポリシーの条件に適合するシステム内のイベントがイベントログをトリガーします。同じ特性を持つ複数のイベントが、1つにクラスター化されます。

イベントの表示



システムで発生したすべてのイベントが、**[すべてのイベント]**画面に表示されます。イベントの特定のサブセットが、**構成イベント**、**SCADA イベント**、**ネットワーク脅威**、**ネットワークイベント**の各イベントカテゴリの別々の画面に表示されます。

画面の上部には、各イベントのリストが表示されます。イベント画面のそれぞれのイベント(構成イベント、SCADA イベント、ネットワーク脅威、ネットワークイベント)は、表示する列と各列の位置を調整することで、表示設定をカスタマイズできます。イベントは、さまざまなカテゴリ(イベントタイプ、深刻度、ポリシー名など)に従ってグループ化できます。また、イベントリストをソートおよびフィルタリングしたり、検索を実行したりすることもできます。カスタマイズ機能の説明については、**リスト**を参照してください。

ヘッダーバーに**[アクション]**ボタンがあり、選択したイベントで次のアクションを実行できます。

- 解決 – このイベントを解決済みとしてマークします。
- PCAP のダウンロード – このイベントの PCAP ファイルをダウンロードします。
- 除外 – このイベントのポリシー除外を作成します。

これらのアクションの詳細情報は、次のセクションに示されています。

画面の下部には、選択されたイベントに関する詳細情報がタブに分割されて表示されます。選択したイベントのイベントタイプに関連するタブのみが表示されます。さまざまなタイプのイベントに対して、*詳細*、*コード*、*ソース*、*デスティネーション*、*ポリシー*、*スキャン済みポート*、*ステータス*のタブが表示されます。

パネル分割を上下にドラッグして、下部パネルの表示を拡大 / 縮小できます。

各イベントに関連するパケットキャプチャファイルをダウンロードできます。**ファイルのダウンロード**を参照してください。

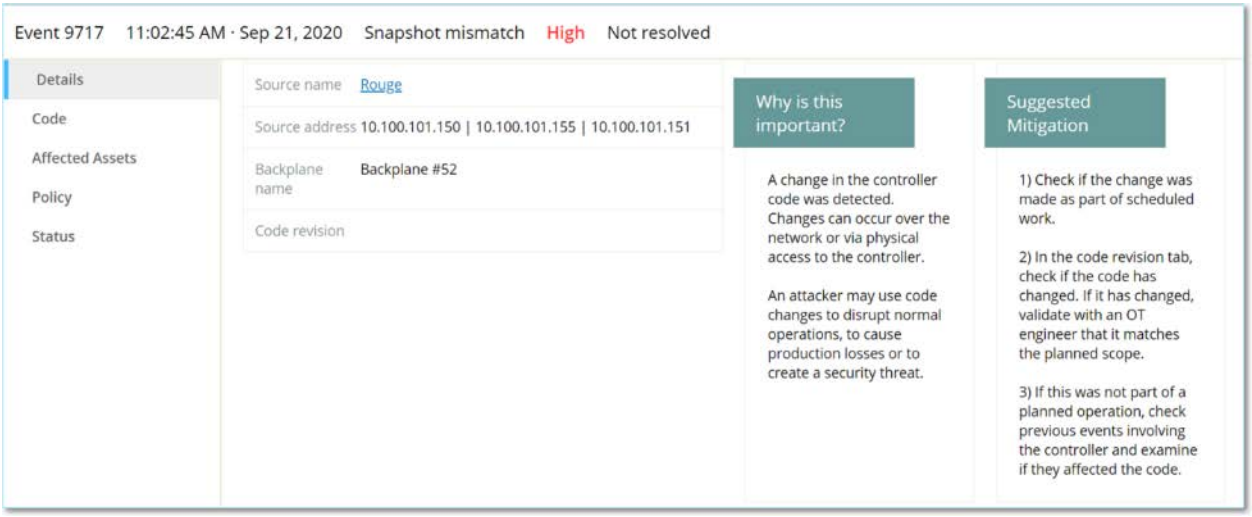
各イベントリストに表示される情報について、次の表で説明します。

パラメーター	説明
名前	ネットワーク内のデバイスの名前。資産の名前をクリックして、その資産の[資産詳細]画面を表示します。 **資産詳細の表示**を参照してください。
アドレス	資産の IP および / または MAC アドレス。 **注意:** 資産には複数の IP アドレスがある場合があります。
タイプ	資産タイプ。さまざまな資産タイプの説明については、**資産タイプ**を参照してください。
バックプレーン	コントローラーが接続されているバックプレーンユニット。バックプレーン構成に関する追加の詳細が、[資産詳細]画面に表示されます。
スロット	バックプレーン上にあるコントローラーの場合、コントローラーが取り付けられているスロットの番号が表示されます。
ベンダー	資産ベンダー。
ファミリー	コントローラーベンダーによって定義された製品のファミリー名。
ファームウェア	現在コントローラーにインストールされているファームウェアのバージョン。
場所	Tenable.ot の資産詳細でユーザーが入力した資産の場所。**資産詳細の編集**を参照してください。
最終確認時間	デバイスが Tenable.ot によって最後に確認された時間。これは、デバイスがネットワークに接続された、またはアクティビティを実行した最後の時間です。
OS	資産で実行されている OS。
ログ ID	イベントを参照するためにシステムによって生成される ID。
時間	イベントが発生した日時。
イベントタイプ	イベントをトリガーしたアクティビティのタイプの説明。イベントは、システムに設定されているポリシーによって生成されます。さまざまなタイプのポリシーの説明については、**ポリシーのタイプ**を参照してください。

パラメーター	説明
深刻度	イベントの深刻度レベルを表示します。以下は、可能な値の説明です。 なし - 心配は不要です。 **情報** - 現時点では心配はありませんが、都合の良いときに確認する必要があります。 **警告** - 潜在的に害のあるアクティビティが発生したことに対する中程度の深刻度レベルで、都合の良いときに対処する必要があります。 **重大** - 潜在的に害のあるアクティビティが発生したことに対する深刻度の高いレベルで、すぐに対処する必要があります。
ポリシー名	イベントを生成したポリシーの名前。名前は、ポリシーリストへのリンクになっています。
ソース資産	イベントを開始した資産の名前。このフィールドは、資産リストへのリンクになっています。
ソースアドレス	イベントを開始した資産の IP または MAC。
デスティネーション資産	イベントの影響を受けた資産の名前。このフィールドは、資産リストへのリンクになっています。
デスティネーションアドレス	イベントの影響を受けた IP または MAC。
プロトコル	関連する場合は、このイベントを生成した会話に使用されたプロトコルを示します。
イベントカテゴリ	イベントの一般的なカテゴリを表示します。 **注意:** [すべてのイベント] 画面には、すべてのタイプのイベントが表示されます。それぞれの特定のイベント画面には、指定されたカテゴリのイベントのみが表示されます。 以下は、イベントカテゴリの簡単な説明です (詳細な説明については、**ポリシーカテゴリ** を参照してください)。 • 構成イベント - 2 つのサブカテゴリが含まれます。 • コントローラー検証イベント - これらのポリシーは、ネットワークのコントローラーで発生する変更を検出します。 • コントローラーアクティビティイベント - アクティビティポリシーは、ネットワークで発生するアクティビティに関連しています (つまり、ネットワークの資産間に実装された「コマンド」)。 • SCADA イベント - コントローラーのデータプレーンに加えられた変更を識別するポリシーです。 • ネットワーク脅威イベント - これらのポリシーは、侵入の脅威を示すネットワークトラフィックを特定します。 • ネットワークイベント - ネットワーク内の資産および資産間の通信ストリームに関連したポリシーです。
ステータス	イベントが解決済みとしてマークされているかどうかを示します。
解決者	解決済みイベントについて、どのユーザーがイベントを解決済みとしてマークしたかを示します。
解決日	解決済みイベントについて、いつイベントが解決済みとしてマークされたかを示します。

パラメーター	説明
コメント	イベントの解決時に追加されたコメントを表示します。

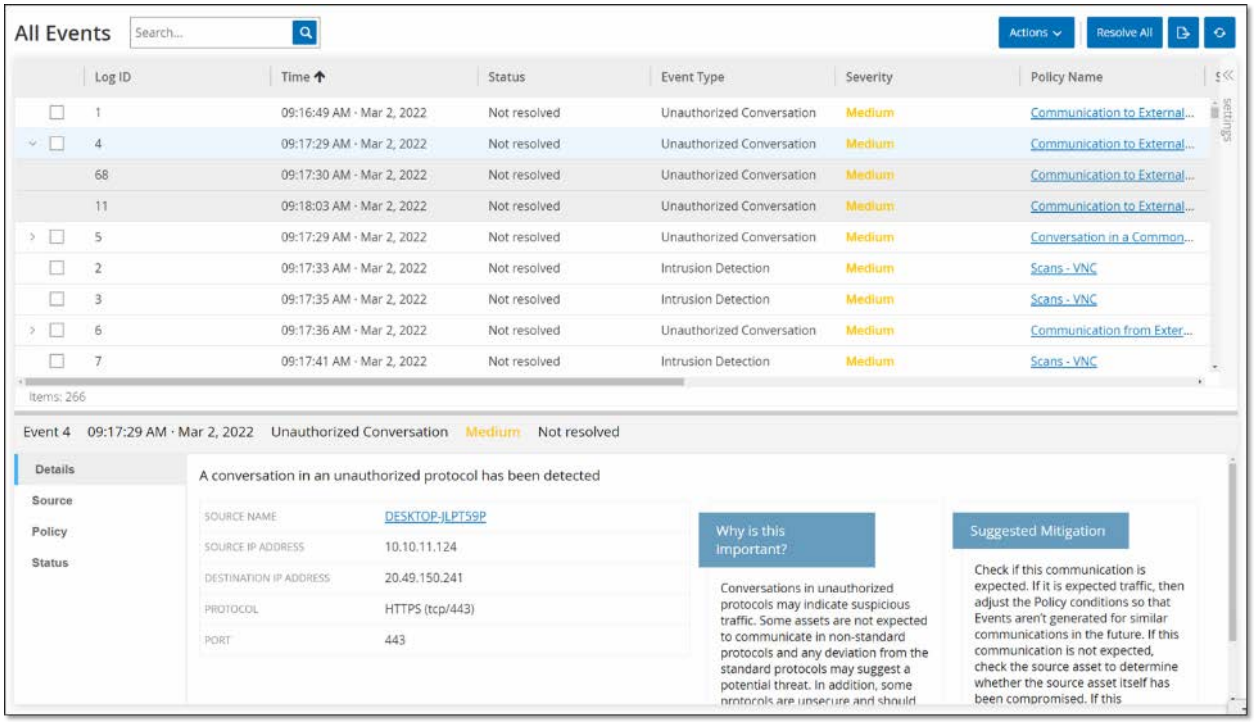
イベントの詳細の表示



イベント画面の下部に、選択したイベントの追加詳細が表示されます。情報は複数のタブに分割されています。選択したイベントに関連するタブのみが表示されます。詳細情報には、関連エンティティに関する追加情報へのリンクが含まれています(ソース資産、デスティネーション資産、ポリシー、グループなど)。

- **ヘッダー** - イベントに関する重要な情報の概要を表示します。
- **詳細** - イベントの簡単な説明、およびこの情報が重要である理由の説明とイベントによる潜在的な被害を緩和するための推奨手順が記載されています。さらに、イベントに関連するソース資産とデスティネーション資産も表示されます。
- **ルールの詳細**(侵入検出イベント用)- イベントに適用される Suricata ルールに関する情報を表示します。
- **コード** - このタブは、コードのダウンロードとアップロード、HW 構成、コードの削除などのコントローラーアクティビティで表示されます。特定のコードブロック、ラング、タグなど、関連コードに関する詳細情報が表示されます。コード要素は、表示される詳細を展開 / 最小化するための矢印付きのツリー構造で表示されます。
- **ソース** - このイベントのソース資産に関する詳細情報を表示します。
- **デスティネーション** - このイベントのデスティネーション資産に関する詳細情報を表示します。
- **影響を受ける資産** - このイベントによって影響を受ける資産に関する詳細情報を表示します。
- **スキャン済みポート**(ポートスキャンイベント用) - スキャンされたポートを表示します。
- **スキャン済みアドレス**(ARP スキャンイベント用) - スキャンされたアドレスを表示します。
- **ポリシー** - イベントをトリガーしたポリシーに関する詳細情報を表示します。
- **ステータス** - イベントが解決済みとしてマークされているかどうかを示します。解決済みのイベントについては、どのユーザーが解決済みとしてマークしたか、いつ解決されたかに関する詳細を表示します。

イベントクラスターの表示



イベントの監視を容易にするために、同じ特性を持つ複数のイベントが、1つにクラスター化されます。クラスタリングは、イベントタイプ(同じポリシーを共有するなど)、ソース資産とデスティネーション資産、イベントが発生する時間範囲に基づいて行われます。イベントクラスターの構成の詳細については、**イベントクラスター**を参照してください。

クラスター化されたイベントは、ログ ID の横に矢印で示されます。クラスターの個々のイベントを表示するには、レコードをクリックしてリストを展開します。

イベントの解決

許可された技術者がイベントを評価し、問題対処に必要とされる措置が講じたか、対処不要と判断した後、イベントを*解決済み*としてマークする必要があります。クラスターの一部である1つのイベントが解決されると、そのクラスター内のすべてのイベントが解決済みとしてマークされます。複数のイベントを選択して、バッチプロセスで解決済みとしてマークすることができます。また、すべてのイベント(または特定のカテゴリのすべてのイベント)を一度に解決済みとしてマークすることもできます。

個々のイベントの解決

➡ 特定のイベントを解決済みとしてマークする手順

1. 関連する**[イベント]**画面(構成イベント、SCADA イベント、ネットワーク脅威、ネットワークイベント)で、解決済みとしてマークする1つ以上のイベントの横にあるチェックボックスを選択します。
2. ヘッダーバーの**[アクション]**ボタンをクリックします。

> 複数のイベントを解決済みとしてマークする場合でも、選択されたイベントをすべて解決済みにするには、*[すべて解決]* ボタン**ではなく**、*[解決]* ボタンをクリックする必要があります。*[すべて解決]* ボタンは、選択されていないものも含めて、すべてのイベントを解決するために使用されます。

3. ドロップダウンメニューで、**[解決]** を選択します。
   [イベントの解決] ウィンドウが表示されます。

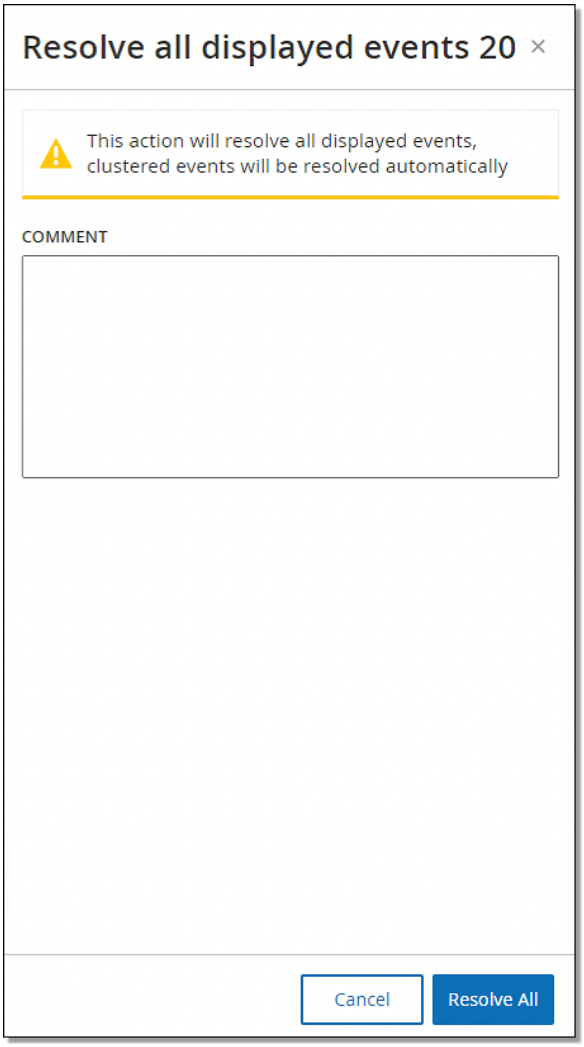
4. **[コメント]** フィールドに、問題を解決するために講じた緩和策を説明するコメントを追加できます。(オプションフィールド)
5. **[解決]** をクリックします。
   選択したイベントのステータスが*解決済み*とマークされます。

すべてのイベントの解決

[すべて解決]アクションは、画面に現在適用されているフィルターに基づいて、現在の画面に表示されているすべてのイベントに適用されます(つまり、[構成イベント]画面が開いている場合、[すべて解決]は構成イベントを解決済みにしますが SCADA イベントなどは解決済みにしません)。クラスター化されたイベントの場合、クラスター内のすべてのイベントが解決済みとしてマークされます。

➡ すべてのイベントを解決済みとしてマークする手順

1. 関連する**イベント**画面(構成イベント、SCADA イベント、ネットワーク脅威、ネットワークイベント)のヘッダーバーで、**[すべて解決]**をクリックします。
2. **[すべてのイベントを解決]**ウィンドウが表示され、解決するイベントの数が右上隅に表示されます。



3. **[コメント]**フィールドで、解決されるイベントのグループに関するコメントを追加できます。(オプションフィールド)
4. **[解決]**をクリックします。
   警告メッセージが表示されます。
5. **[解決]**をクリックします。
   現在表示されているすべてのイベントが解決済みとしてマークされます。

ポリシー除外の作成

ポリシーが、セキュリティ脅威をもたらさない特定の条件に対してイベントを生成していることが判明した場合は、それらの条件をポリシーから*除外*できます(つまり、それらの特定の条件に対するイベントの生成を停止できます)。たとえ

ば、勤務時間中に発生するコントローラー状態の変更を検出するポリシーがあったとしても、特定のコントローラーではその時間中に状態が変化することは正常であると判断した場合、そのコントローラーをポリシーから*除外*できます。

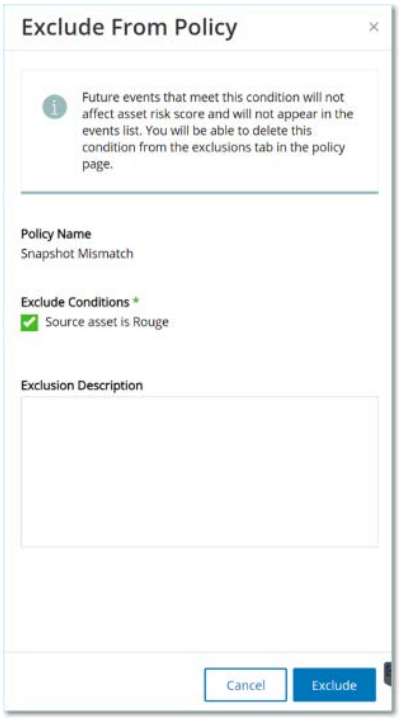
除外は、ポリシーによって生成されたイベントに基づいて、イベント画面から作成します。特定のイベントのどの条件をポリシーから除外するかを指定できます。

指定した条件のイベントの生成を後で再開する場合は、除外を削除できます。**ポリシーの除外の削除**を参照してください。

➡ ポリシーの除外の作成手順

1. 関連する**イベント**画面(構成イベント、SCADA イベント、ネットワーク脅威、ネットワークイベント)で、除外を作成するイベントを選択します。
2. ヘッダーバーの**[アクション]**ボタンをクリックします(またはイベントを右クリックします)。
   [アクション]メニューが表示されます。
3. **[ポリシーから除外]**をクリックします。
   [ポリシーから除外]ウィンドウが開きます。
4. **[条件の除外]**セクションでは、デフォルトですべての条件が選択されています(これにより、指定した条件の*いずれか*で、トリガーされるイベントがポリシーから除外されます)。イベントの生成を継続したい各条件の横にあるチェックボックスを**解除解除**できます。

> たとえば、以下に示すダイアログで、指定したソース資産とデスティネーション資産および IP をこのポリシーから除外したいものの、このポリシーをネットワーク内の他の資産間の UDP 会話に引き続き適用したい場合は、「プロトコルは UDP です」を選択解除する必要があります。



> 除外できる条件のセットは、ポリシーのタイプによって異なります。以下の表を参照してください。

5. **[除外の説明]**フィールドで、除外に関するコメントを追加できます(オプション)。
6. **[除外]**をクリックします。
   除外が作成されます。

次の表は、イベントのタイプごとに除外できる条件を示しています。

ポリシーカテゴリ	イベントタイプ	除外条件
コントローラーアクティビティ	構成イベント(アクティビティなど)	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP
コントローラー検証	キー状態の変化	• ソース資産
	コントローラー状態の変化	• ソース資産
	FW バージョンの変更	• ソース資産
	確認されないモジュール	• ソース資産
	スナップショットの不一致	• ソース資産
ネットワーク	確認されない資産	• ソース資産
	USB 構成の変更	• ソース資産 • USB デバイス ID
	IP の競合	• MAC アドレス • IP アドレス
	ネットワークベースラインの逸脱	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP • プロトコル
	オープンポート	• ソース資産 • ソース IP • ポート
	RDP 接続	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP
	認証されていない会話	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP • プロトコル
	FTP ログイン(失敗および成功)	• ソース資産 • ソース IP • デスティネーション資産

ポリシーカテゴリ	イベントタイプ	除外条件
		• デスティネーション IP
	Telnet ログイン(試行、失敗、成功)	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP
ネットワーク脅威	侵入検知	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP • SID
	ARP スキャン	• ソース資産 • ソース IP
	ポートスキャン	• ソース資産 • ソース IP
SCADA	Modbus の不正なデータアドレス	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP
	Modbus の不正なデータ値	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP
	Modbus の不正な関数	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP
	承認されていない書き込み	• ソース資産 • デスティネーション資産 • タグ名
	IEC60870-5-104 StartDT IEC60870-5-104 StopDT	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP
	IEC60870-5-104 関数コードベースのイベント	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP

ポリシーカテゴリ	イベントタイプ	除外条件
		• COT
	DNP3 イベント	• ソース資産 • ソース IP • デスティネーション資産 • デスティネーション IP • ソース DNP3 アドレス • デスティネーション DNP3 アドレス

個々のキャプチャファイルのダウンロード

Tenable.ot は、ネットワーク内の各イベントに関連するパケットキャプチャデータを保存します。データは PCAP ファイルとして保存され、ネットワークプロトコル分析ツール(Wireshark など)を使用してダウンロードおよび分析できます。このセクションでは、個々のイベントに関連する PCAP ファイルをダウンロードする方法について説明します。ネットワーク全体の PCAP ファイルをダウンロードすることもできます。**パケットキャプチャ**を参照してください。

PCAP ファイルは、パケットキャプチャ機能がアクティブ化されている場合にのみ利用できます。パケットキャプチャ機能は、**[ローカル設定]** > **[システム構成]** > **[パケットキャプチャ]** 画面からアクティブ化できます。 **パケットキャプチャ**を参照してください。

PCAP ファイルは、コントローラーアクティビティ、ネットワーク脅威、SCADA イベント、一部のタイプのネットワークイベントなど、ネットワークアクティビティに関連するイベントでのみ使用できます。

PCAP ファイルのダウンロード

➡ PCAP ファイルのダウンロード手順

1. **[イベント]** 画面で、PCAP ファイルをダウンロードするイベントの横にあるチェックボックスを選択します。
2. ヘッダーバーの **[アクション]** ボタンをクリックします。
3. ドロップダウンメニューで、**[キャプチャファイルのダウンロード]** を選択します。
   zip 圧縮された PCAP ファイルがローカルマシンにダウンロードされます。

FortiGate ポリシーの作成

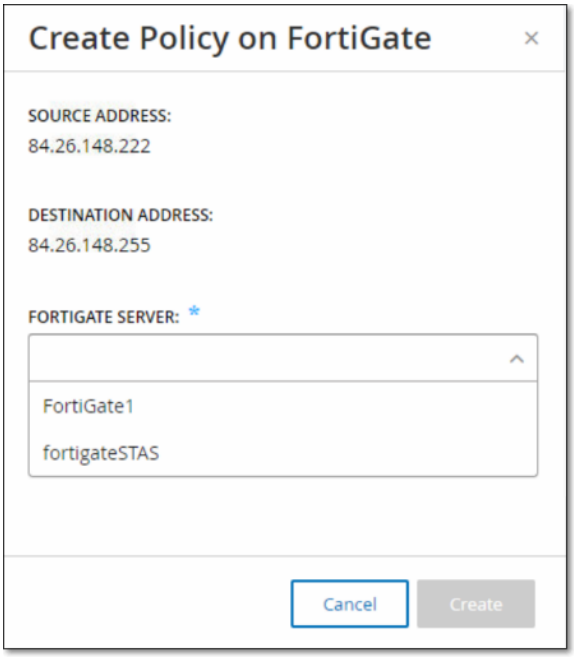
FortiGate 統合により、特定の Tenable.ot イベントを使用して、FortiGate 次世代ファイヤーウォールでファイヤーウォールポリシー / ルールを作成できます。この機能を許可するイベントのタイプ(サポートされているイベント)は、*ベースラインの逸脱*、*認証されていない会話*、*侵入検知*、*RDP 接続(認証あり、認証なし)*です。FortiGate ポリシーは、Tenable.ot イベントに関連するソース資産とデスティネーション資産に適用されるように自動的に設定されます。デフォルトでは、このポリシーにより、FortiGate は指定されたタイプのトラフィックを拒否(ブロック)します。FortiGate 管理者は、FortiGate アプリケーションのポリシー設定を調整できます。

FortiGate ポリシーを提案できるようになる前に、FortiGate ファイヤーウォールサーバーと Tenable.ot の統合を設定する必要があります。**FortiGate ファイヤーウォール**を参照してください。

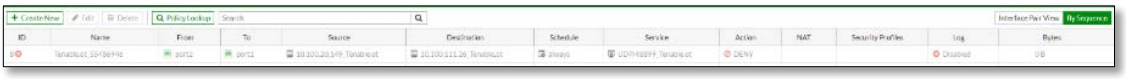
➡ FortiGate ポリシーの提案手順

1. 関連する**イベント** 画面(*構成イベント*、*SCADA イベント*、*ネットワーク脅威*、*ネットワークイベント*)で、FortiGate ポリシーを作成するイベントを選択します。
2. ヘッダーバーの **[アクション]** ボタンをクリックします(またはイベントを右クリックします)。
3. ドロップダウンメニューで、**[FortiGate ポリシーの作成]** を選択します。
   FortiGate パネルで **[ポリシーの作成]** が開きます。Tenable.ot イベントに関連する資産の**ソースアドレス**と**デスティネーションアドレス**はすでに入力されています。

4. **[FortiGate サーバー]** フィールドのドロップダウンメニューで、目的のサーバーを選択します。



5. **[作成]** をクリックします。
   ポリシーが FortiGate で作成され、パネルが閉じます。
6. FortiGate アプリケーションで新しいポリシーを表示できます。



7. FortiGate 管理者は、必要に応じて設定を調整できます。

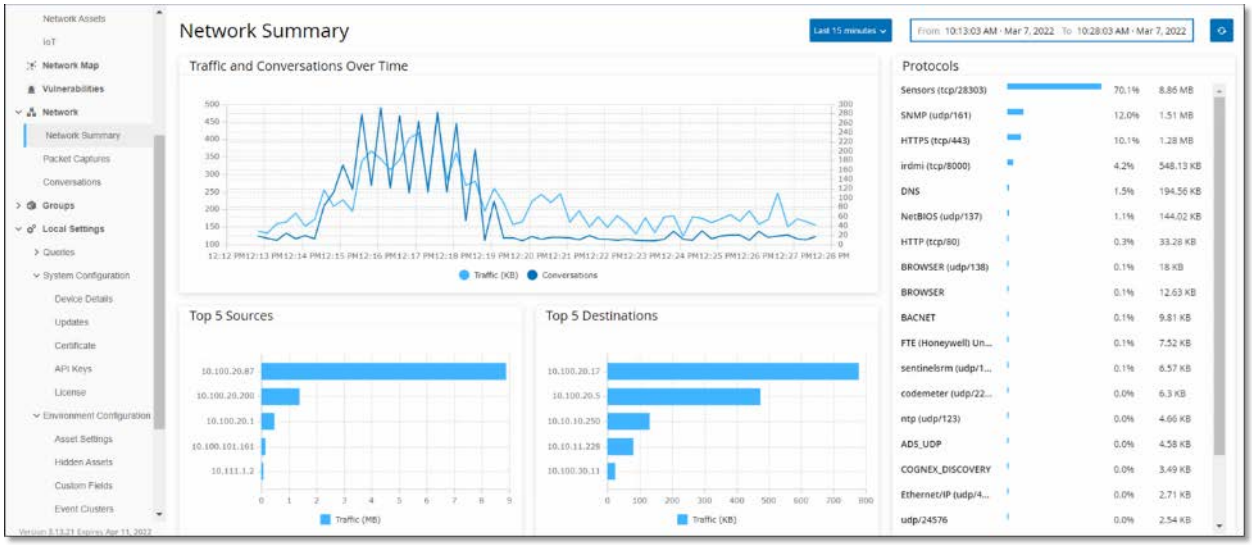
ネットワーク

Tenable.ot は、ネットワークのすべてのアクティビティを監視します。この情報は、UI の **[ネットワーク]** セクションに表示されます。

ネットワークデータが 3 つの画面に表示されます。

- **ネットワークサマリー** - ネットワークアクティビティの概要を表示します。
- **パケットキャプチャ** - システムによってキャプチャされた PCAP ファイルのリストを表示します。
- **会話** - ネットワークで検出されたすべての会話のリストを、発生した時刻、関連する資産などの詳細とともに表示します。

ネットワークサマリー



[ネットワークサマリー] 画面は、ネットワークアクティビティをまとめたビジュアルグラフを表示します。データを表示するタイムフレームを設定したり、ウィジェットを操作して、追加の詳細を表示したりすることができます。

画面には 4 つのウィジェットが含まれています。

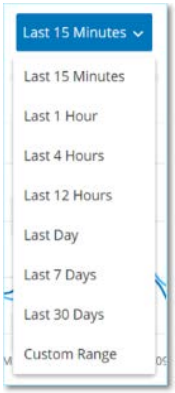
- **トラフィックと会話の経時変化** - GB/MB 単位でトラフィック量を表示し、ネットワークで発生している会話の数を表示するグラフ。
- **上位 5 件のソース** - ネットワークアクティビティを最も多く開始した 5 つのソース資産を表示する横棒グラフ。各ソースについて、グラフはトラフィック量を表すバーを表示します。グラフにカーソルを合わせると、会話の数がツールチップに表示されます。
- **上位 5 件のデスティネーション** - ネットワークアクティビティを最も多く受信した 5 つのデスティネーション資産を表示する横棒グラフ。各ソースについて、グラフは着信トラフィック量を表すバーを表示します。グラフにカーソルを合わせると、会話の数がツールチップに表示されます。
- **プロトコル** - ネットワークで使用されている通信プロトコルを周波数順に表示した棒グラフ。各プロトコルについて、グラフには、プロトコルが使用された割合 (総トラフィックのパーセンテージ) とトラフィック量が表示されます。

タイムフレームの設定

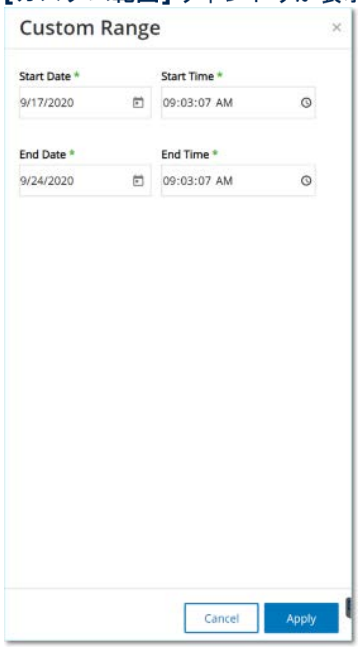
[ネットワーク]画面に表示されるすべてのデータは、指定されたタイムフレームにおけるネットワークのアクティビティを表します。現在表示されているデータの時間範囲がヘッダーバーに表示されます。デフォルトのタイムフレームは、*過去 15 分間*に設定されています。選択したタイムフレームの*開始*時間と*終了*時間がヘッダーバーに表示されます。

タイムフレームの設定手順

1. ヘッダーバーの**[タイムフレーム選択]**をクリックします(デフォルトは過去 15 分間)。
   タイムフレームオプションのあるドロップダウンメニューが表示されます。

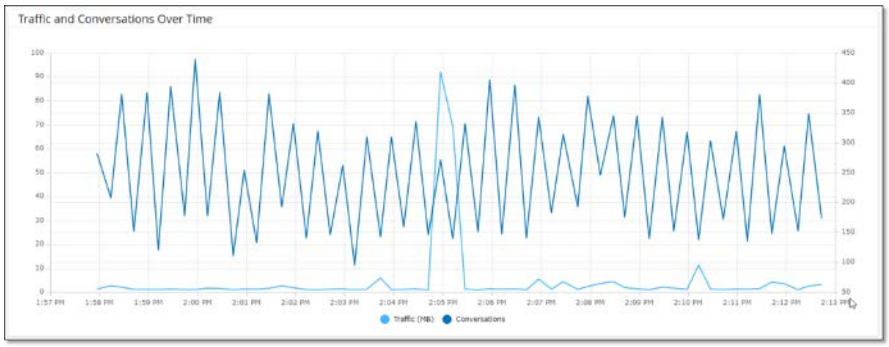


2. 次のいずれかの方法で時間範囲を選択します。
   - 希望する範囲をクリックして、事前設定の時間範囲を選択します(オプションは、過去 15 分、過去 1 時間、過去 4 時間、過去 12 時間、過去 1 日間、過去 7 日間、過去 30 日間)。
   - 次の手順を使用して、カスタムの時間範囲を設定します。
     a. **[カスタム範囲]**をクリックします。
        [カスタム範囲]ウィンドウが表示されます。



     b. 適切なフィールドに**開始日**と**開始時間**、**終了日**と**終了時間**を入力します。
     c. **[適用]**をクリックします。
        タイムフレームが設定されます。開始日と開始時間、終了日と終了時間は、ヘッダーバーのタイムフレーム選択の横に表示されます。画面がリフレッシュされ、選択したタイムフレームのデータのみが表示されます。

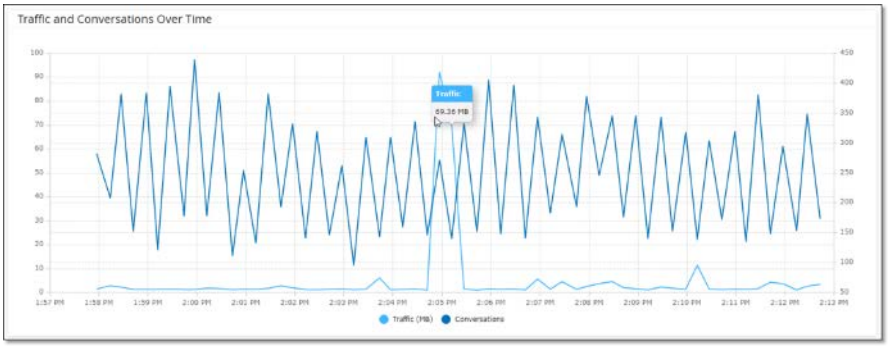
トラフィックと会話の経時変化



折れ線グラフが、トラフィックの量(KB/MB/GB で測定)とネットワークで発生した会話の数を時間の経過に伴う変化で表示します。表示キーがグラフの上部に表示されます。

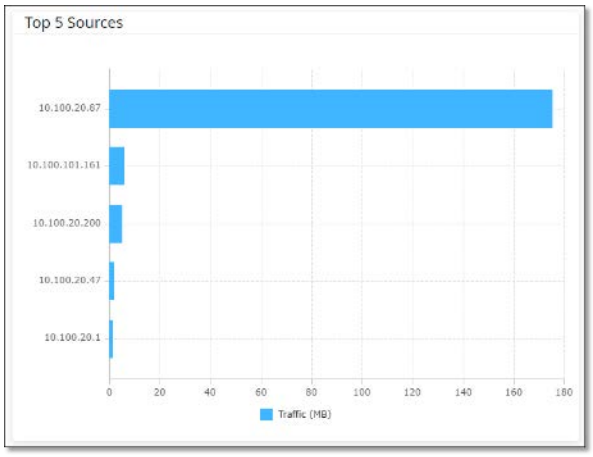
➡ 特定の時間セグメントのデータを表示する手順

1. グラフ上のポイントにカーソルを合わせると、その時間セグメント中に発生したトラフィックと会話に関する特定のデータを含むポップアップウィンドウが表示されます。



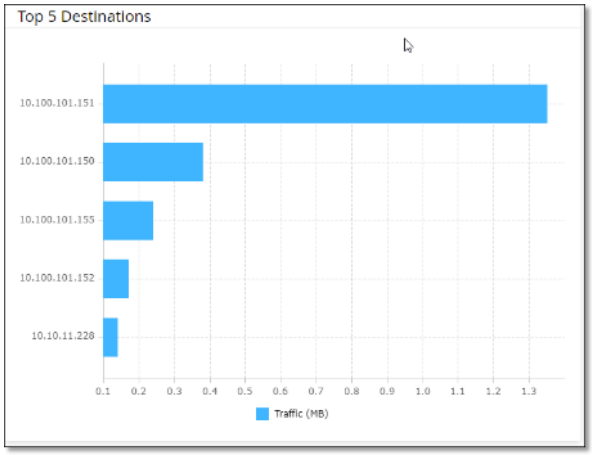
表示されている時間セグメントの長さは、表示されている時間スケールに応じて調整されます (たとえば、15 分のタイムフレームのデータは、1 分ごとに個別に表示されますが、30 日のタイムフレームの場合は、6 時間のセグメントで表示されます)。

上位 5 件のソース



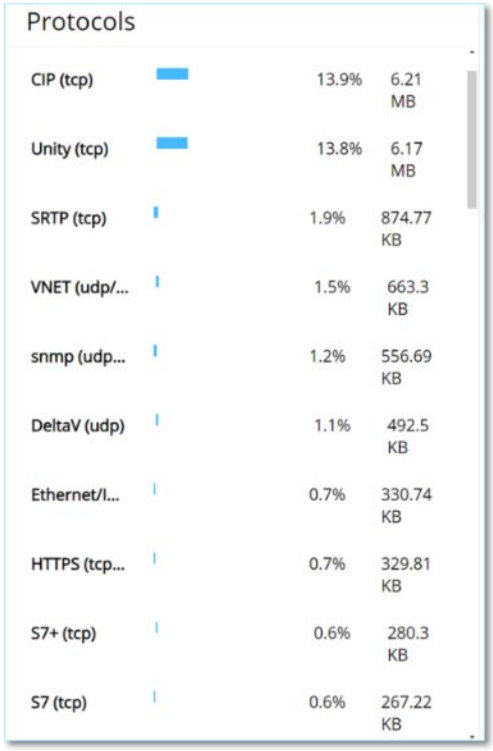
[上位 5 件のソース] ペインには、指定されたタイムフレームの間にネットワーク経由で通信を送信した上位 5 件の資産それぞれの会話数とトラフィック量が表示されます。ソース資産は IP アドレスで識別されます。棒グラフにカーソルを合わせると、その資産から送信された会話の数とトラフィックの量が表示されます。

上位 5 件のデスティネーション



[上位 5 件のデスティネーション] ペインには、指定されたタイムフレームの間にネットワーク経由で通信を受信した上位 5 件の資産それぞれの会話数とトラフィック量が表示されます。デスティネーション資産は IP アドレスで識別されます。棒グラフにカーソルを合わせると、その資産が受信した会話の数とトラフィックの量が表示されます。

プロトコル



[プロトコル] ペインには、指定されたタイムフレームにおけるネットワーク内の通信のさまざまなプロトコルの使用状況に関するデータが表示されます。プロトコルは、使用頻度の高いもの(上)から使用頻度の低いもの(下)の順番に一覧表示されています。プロトコルごとに、次の情報が表示されます。

- 使用率を示す棒グラフ(完全な長さの棒グラフは上位のプロトコルの使用率、それより短い棒グラフは使用されている上位のプロトコルに対する使用率の割合を示します)
- 使用率
- 通信の総量

パケットキャプチャ

システムは、ネットワーク内の完全なアクティビティのネットワークパケットキャプチャを含むファイルを保存します。データはPCAPファイルとして保存され、ネットワークプロトコル分析ツール(Wiresharkなど)を使用して分析できます。これにより、重要なイベントの詳細なフォレンジック分析が可能になります。システムのストレージ容量(1.8 TB)を超えると、システムは古いファイルを削除します。

[パケットキャプチャ]画面に、システム内のすべてのパケットキャプチャファイルが表示されます。*[完了]*タブには、ダウンロード可能な各完了ファイルのリストが表示されます。*[進行中]*タブには、システムで現在進行中のパケットキャプチャに関する詳細が表示されます。

ヘッダーバーには、システムでまだ利用可能な最も古いキャプチャ済みファイルが表示されます。また、ファイルをダウンロードしたり、現在のパケットキャプチャを手動で閉じたりするためのボタンも含まれています。

ファイルリストテーブルで、列の表示 / 非表示、リストのソートおよびフィルタリング、キーワードの検索ができます。カスタマイズ機能の説明については、 **リスト**を参照してください。

> **[イベント]**画面から個々のイベントのPCAPファイルをダウンロードすることもできます。**ファイルのダウンロード**を参照してください。

パケットキャプチャパラメーター

次の表で、パケットキャプチャリストで表示されるパラメーターについて説明します。

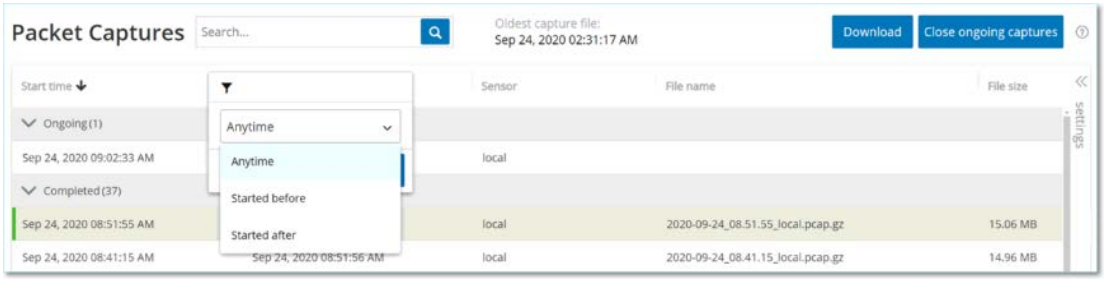
パラメーター	説明
開始時刻	パケットキャプチャが開始した日時。
終了時刻	パケットキャプチャが終了した日時。
ステータス	キャプチャのステータス。可能な値: *完了*または*進行中*。
センサー	パケットをキャプチャしたTenable.otセンサー。Tenable.otアプライアンスによって直接キャプチャされたパケットの場合、値は*ローカル*になります。
ファイル名	ファイルの名前。
ファイルサイズ	KB/MB単位のファイルのサイズ。

パケットキャプチャ表示のフィルタリング

開始時間や終了時間のパラメーターを入力して**パケットキャプチャ**の表示をフィルタリングし、特定のPCAPを見つけることができます。

➡ パケットキャプチャのフィルタリング手順

1. **[ネットワーク]**で、**[パケットキャプチャ]**を選択します。
2. 開始時間でフィルターするには、**[開始時間]**にカーソルを合わせ、表示されるメニューアイコンをクリックします。
   ドロップダウンメニューが開きます。

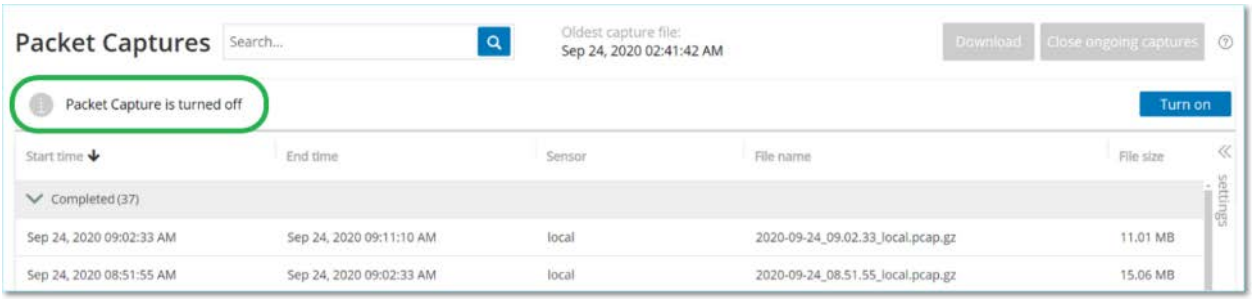


   フィルターを次のように設定します。
   a. ドロップダウンリストからフィルターオプションを選択します。オプションは*[日時指定なし]*(デフォルト)、*[次の時点より前に開始]*、または*[次の時点より後に開始]*です。
   b. **[次の時点より前に開始]**または**[次の時点より後に開始]**が選択された場合、**[日付]**および**[時刻]**フィールドのあるウィンドウが開き、希望の日付と時刻を選択できます。
   c. **[適用]**をクリックします。
3. 終了時間でフィルターするには、**[終了時刻]**の横にある**[フィルター]**アイコンをクリックします。
   ドロップダウンメニューが開きます。フィルターを次のように設定します。
   a. ドロップダウンリストからフィルターオプションを選択します。オプションは*[日時指定なし]*(デフォルト)、*[次の時点より前に開始]*、または*[次の時点より後に開始]*です。
   b. **[次の時点より前に開始]**または**[次の時点より後に開始]**が選択された場合、**[日付]**および**[時刻]**フィールドのあるウィンドウが開き、希望の日付と時刻を選択できます。
   c. **[適用]**をクリックします。
   フィルターが適用され、選択したタイムフレーム内に生成されたファイルのみが表示されます。

パケットキャプチャのアクティブ化 / アクティブ化解除

パケットキャプチャは、**[ローカル設定]**>**[デバイスの詳細]**画面でアクティブ化 / アクティブ化解除できます。**パケットキャプチャ**を参照してください。

パケットキャプチャ機能がオフの場合、**[パケットキャプチャ]**画面にオフであることを通知するメッセージが表示されます。

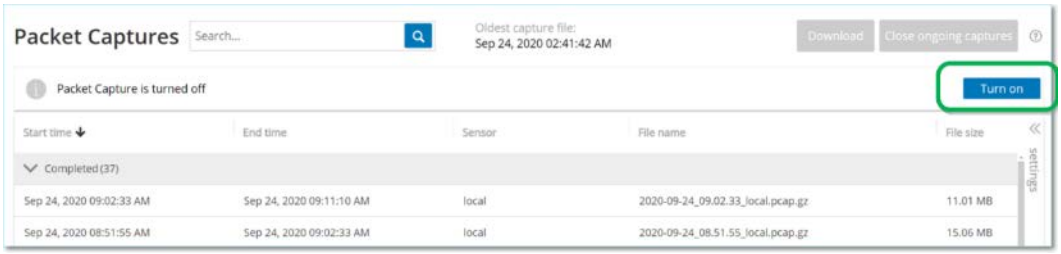


[ネットワーク]>**[パケットキャプチャ]**画面からパケットキャプチャをアクティブ化できます(ただし、アクティブ化解除はできません)。

➡ パケットキャプチャ画面からパケットキャプチャをアクティブ化する手順

1. **[ネットワーク]**で、**[パケットキャプチャ]**を選択します。

2. **ヘッダー**バーで、**[オンにする]**をクリックします。



システムはパケットキャプチャを開始します。

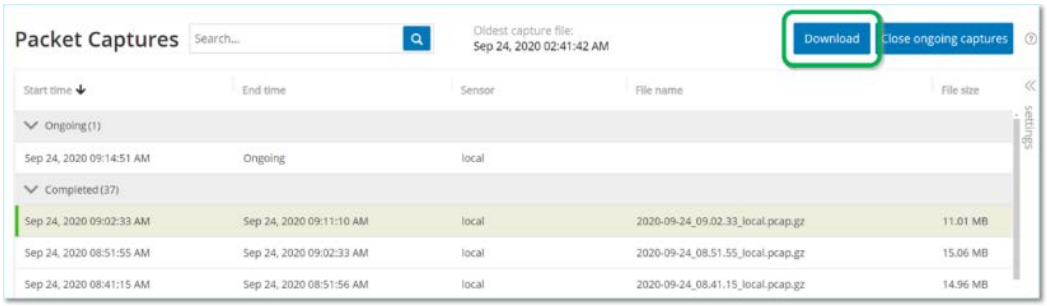
ファイルのダウンロード

任意の*完成した*PCAP ファイルをローカルマシンにダウンロードできます。ダウンロードした PCAP ファイルは、ネットワークプロトコル分析ツール(Wireshark など)を使用して分析できます。

まだ進行中のファイルキャプチャはダウンロードできません。進行中のキャプチャを手動で閉じ、現在のファイルを閉じることで、新しいファイルの情報のキャプチャを開始することができます。

➡ 完成したファイルのダウンロード手順

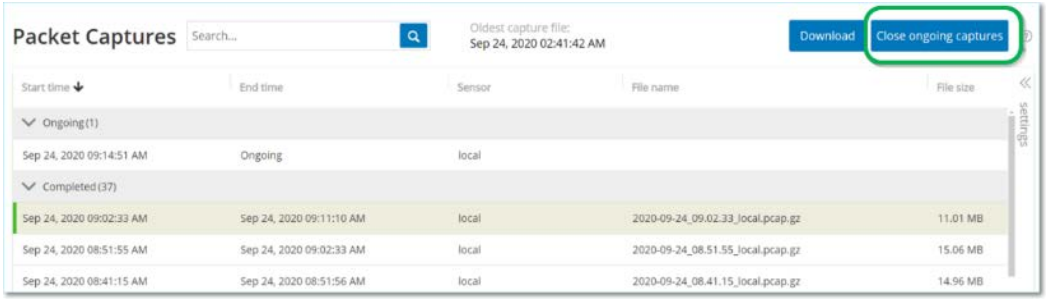
1. **[ネットワーク]**で、**[パケットキャプチャ]**を選択します。
2. パケットキャプチャリストから目的のファイルを選択します。
3. **ヘッダー**バーで、**[ダウンロード]**をクリックします。



zip 圧縮された PCAP ファイルがローカルマシンにダウンロードされます。

➡ 現在のパケットキャプチャを手動で閉じる手順

1. **[ネットワーク]**で、**[パケットキャプチャ]**を選択します。
2. **ヘッダー**バーで、**[進行中のキャプチャを閉じる]**をクリックします。



現在のキャプチャが停止し、ファイルをダウンロードできるようになります。新しいパケットキャプチャが自動的に開始されます。

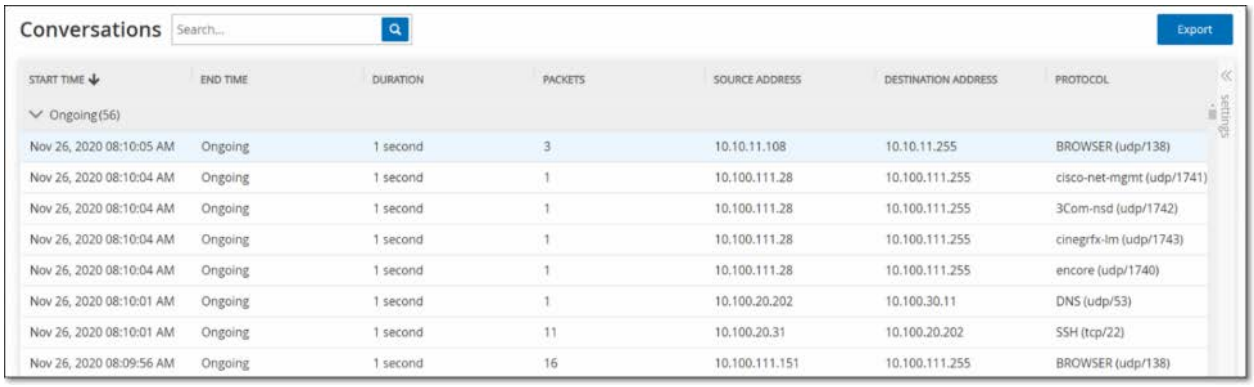
会話

会話は、ソースとデスティネーションの 2 つの資産間のネットワーク通信です。たとえば、エンジニアリングワークステーションと PLC の間、または 2 台のサーバー間のやり取りです。**[会話]** 画面には、会話に関する詳細情報を含む、現在および過去の会話のリストが表示されます。

会話画面には、以下の追加機能があります。

- **検索** - **[検索]** ボックスに識別情報を入力して、特定の会話を検索します。
- **エクスポート** - **[エクスポート]** をクリックすると、すべてのデータが [会話] タブからローカルマシンに .csv ファイルとしてエクスポートされます。

[会話] テーブルには、最新の 10,000 個のネットワーク会話が表示されます。

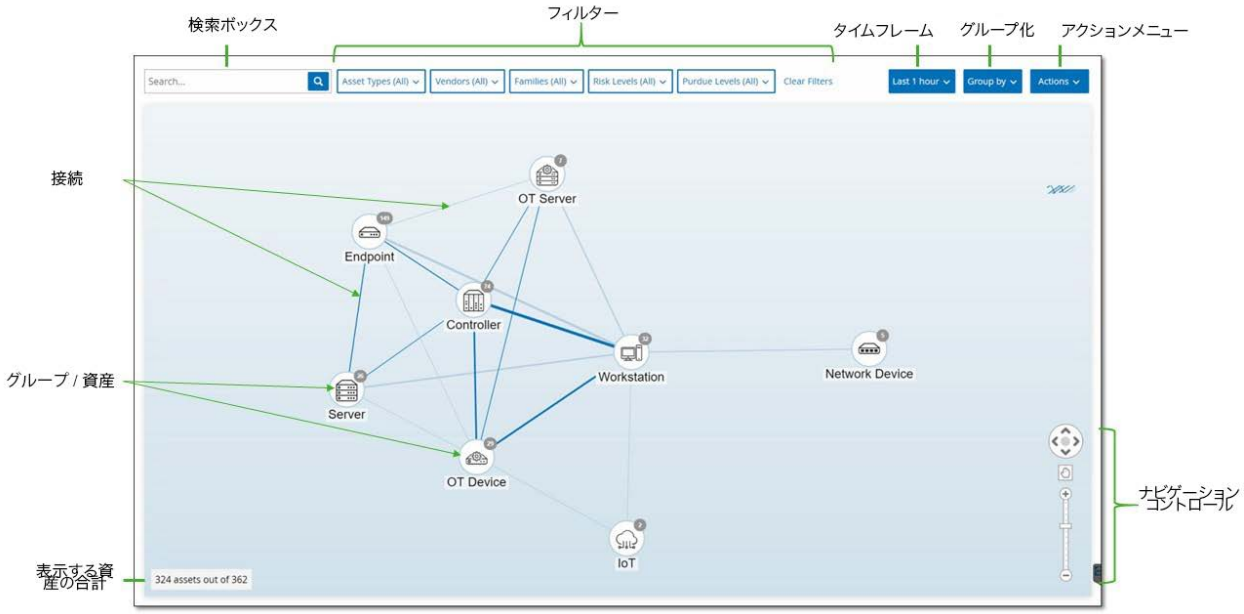


[会話] タブに表示される情報について、以下の表で説明します。

パラメーター	説明
開始時刻	会話が開始した時刻。
終了時刻	会話が終了した時刻。進行中の会話は、*[進行中]* と表示されます。
期間	会話が進行中であった時間。
パケット	送信されたデータパケットの数。
ソースアドレス	データを送信した資産の IP。
デスティネーションアドレス	データを受信した資産の IP。
プロトコル	通信に使用されたプロトコル。

ネットワークマップ

[ネットワークマップ]画面は、Tenable.ot のネットワーク検出機能によって検出されたとおりに、ネットワーク資産とその接続を時間に沿って視覚的に表示します。ネットワーク検出は、コントロールプレーンのエンジニアリングアクティビティに独自の焦点を合わせて、運用ネットワークで実行されたすべてのアクティビティを詳細かつリアルタイムで可視化します。たとえば、ベンダー独自の特定プロトコルで実行される、ファームウェアのダウンロード / アップロード、コードの更新、構成変更です。資産は、関連する資産のグループごとに、または個別の資産として表示できます。



ネットワークマップには、指定されたタイムフレーム内に検出されたすべての資産と接続が表示されます。

以下は、ネットワークマップ画面に表示される要素の説明です。

- **検索ボックス** - 検索テキストを入力して、表示されている資産を検索します。検索結果は、検索テキストに一致するものが見つかったすべてのグループを強調表示することで示されます。各グループにドリルダウンして、関連する資産を表示できます。
- **フィルター** - *資産タイプ*、*ベンダー*、*ファミリー*、*リスクレベル*、*パデューレベル*の 1 つ以上の指定されたカテゴリでマップ表示をフィルターできます。資産タイプの説明については、**資産タイプ**を参照してください。
- **タイムフレーム** - ネットワークマップには、指定されたタイムフレーム内に検出されたすべての資産とネットワーク接続が表示されます。デフォルトのタイムフレームは、*過去 1 か月*に設定されています。**[タイムフレーム選択]**をクリックして、ドロップダウンメニューから別のタイムフレームを選択します。
- **グループ化** - 表示で資産をグループ化するカテゴリを指定できます。オプションは、*[資産タイプ]*、*[パデューレベル]*、*[リスクレベル]*、*[グループ化なし]*です。*[すべてのグループを折りたたむ]*オプションは、現在のグループ化選択を維持したまま、開かれているすべてのグループを折りたたみます。
- **アクション** - ドロップダウンメニューから次のアクションを選択できます。
    - **ベースラインとして設定** - 異常なネットワークアクティビティの検出に使用されるベースラインを設定します。**ネットワークベースラインの設定**を参照してください。
    - **自動配置** - 現在表示されているエンティティのマップ表示を自動的に最適化します。
- **グループ / 資産** - 資産の各グループはマップ上のアイコンで表され、各資産タイプは異なるアイコンで表されます(**資産タイプ**で説明)。グループの場合、アイコンの上部の数字は、そのグループに含まれる資産の数を示しま

す。個々の資産アイコンに達するまで、ドリルダウンして各サブグループの個別のアイコンを表示できます。個々の資産の場合、資産周囲のフレームの色(赤、黄、緑)はリスクレベルを示します。

グループと資産をドラッグして再配置して、資産とその接続を見やすく表示することができます。

- **接続** - 現在マップに表示されている粒度の程度に応じた、資産のグループおよび / または個々の資産間の各通信です。線の太さは、その接続を介した通信量を示します。
- **表示された資産の合計** - 指定されたタイムフレームと資産フィルターに基づいて、ネットワークで検出された(およびマップに表示された)資産の数を表示します。この数は、ネットワークで検出された資産の総数と関連させて表示されます。
- **ナビゲーションコントロール** - 画面上のコントロールを使用するか標準のマウスコントロールを使用して、表示を拡大および縮小したり、移動して目的の要素を表示したりできます。

資産のグループ化

ネットワークマップは、さまざまな異なるカテゴリでグループ化された資産を表示できます。資産のグループ間の接続が表示されます。資産をクリックすると、そのグループに含まれる要素にドリルダウンできます。複数のグループを同時にドリルダウンできます。Tenable.ot には埋め込みグループの複数のレイヤーが含まれているため、ドリルダウンするたびに、含まれている資産をより詳細に表示できます。

以下は、メイン表示に適用できるグループ化と選択されたグループ化のドリルダウンオプションです。

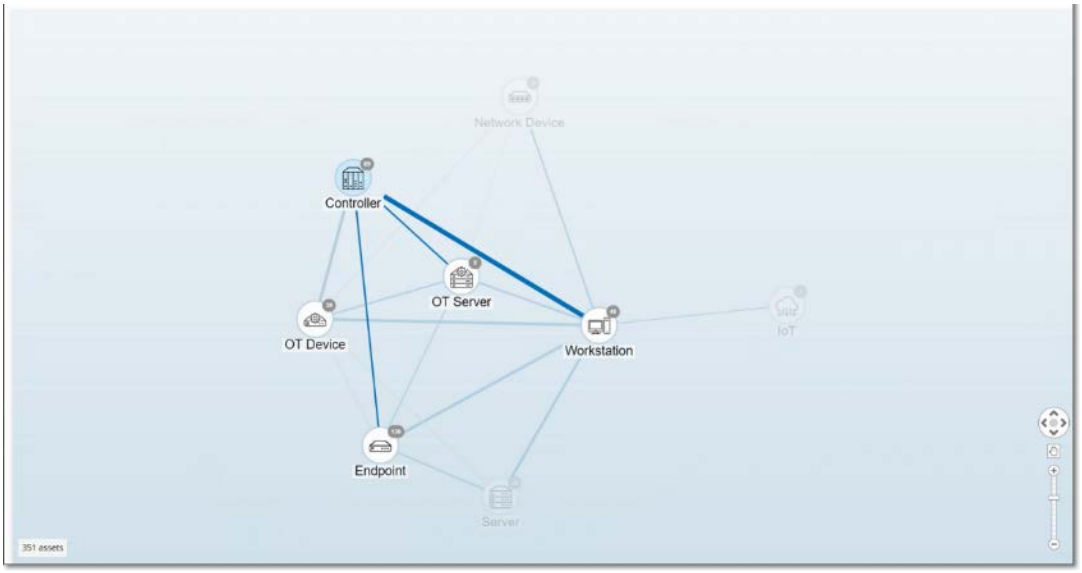
マップ表示が *[資産タイプ]*(デフォルト)でグループ化されている場合、ドリルダウン階層は次のようになります。**[資産タイプ]**>**[ベンダー]**>**[ファミリー]**>**[個別資産]**。

マップ表示が *[リスクレベル]* または *[パデューレベル]* でグループ化されている場合、資産タイプのグループ化の*上*にさらにレベルが追加され、階層は次のようになります。**[パデューレベル / リスクレベル]**>**[資産タイプ]**>**[ベンダー]**>**[ファミリー]**>**[個別資産]**。すべてのレベルは、含まれているグループ / 資産を囲む円で表されます。

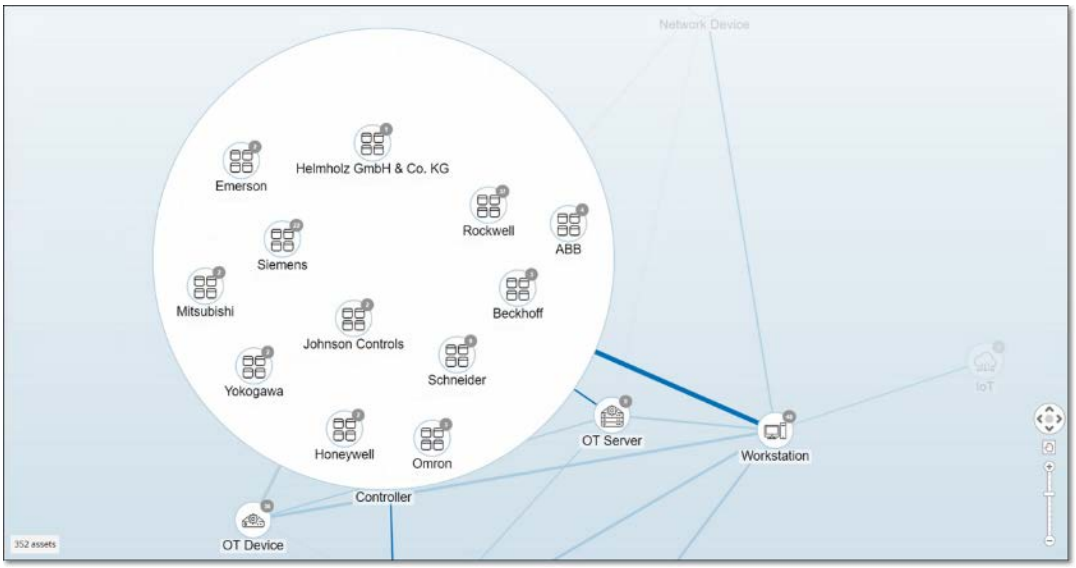
次の例は、表示をドリルダウンする方法を示しています。

➡ 資産タイプグループにドリルダウンする手順

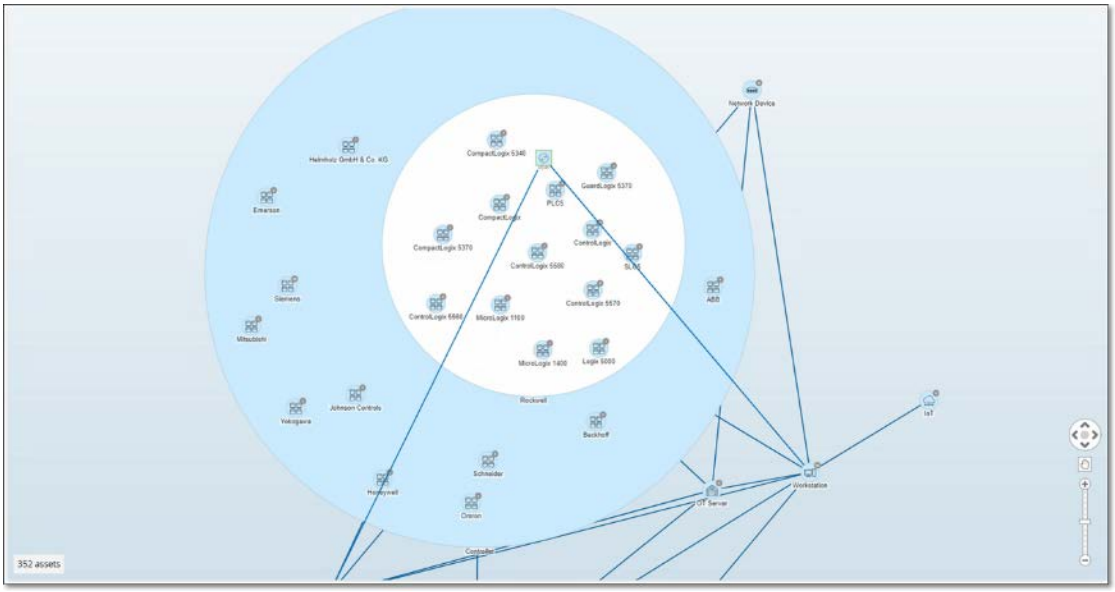
1. デフォルトでは、**[ネットワークマップ]**画面を開くと、*[資産タイプ]*別にグループ化された資産が表示されます。



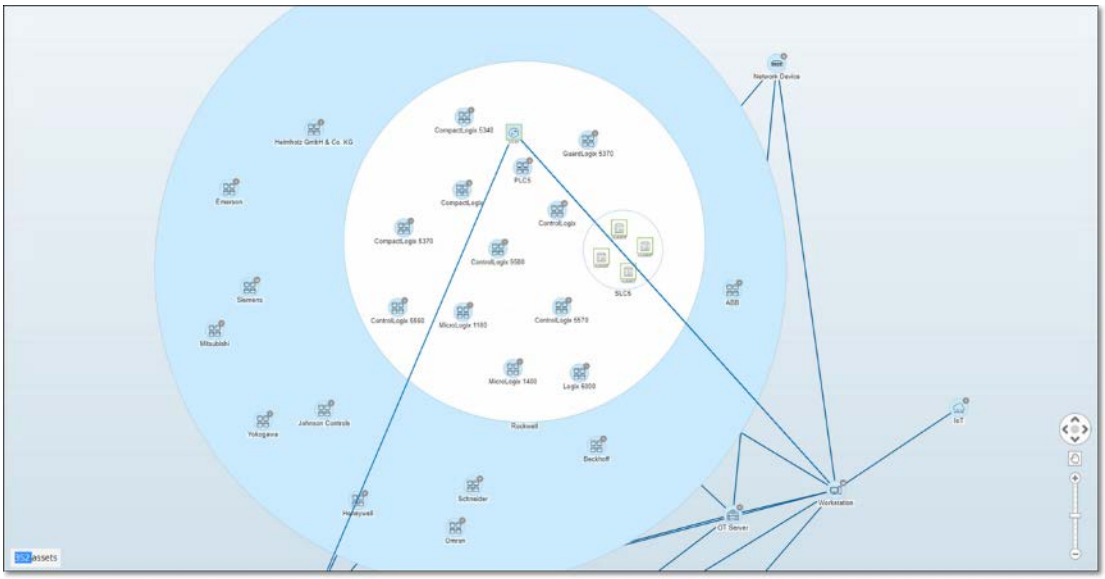
2. ドリルダウンするグループアイコン(例 : **コントローラー**)をダブルクリックします。
グループが展開され、そのグループ内の ベンダーグループが表示されます。



3. さらにドリルダウンするには、ベンダーグループ(例 : Rockwell)をクリックします。



4. さらにドリルダウンするには、ファミリーグループ(例 : SLC5)をクリックします。
5. そのグループ内の個々の資産が表示されます。



6. これで、特定の資産をクリックすると、その資産とその接続の詳細を確認できるようになりました。**資産詳細の表示**を参照してください。

➡ 表示の折りたたみ手順

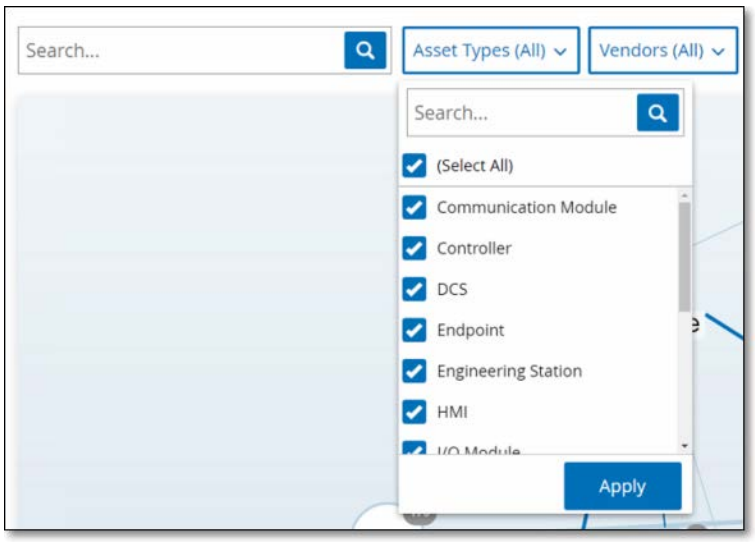
1. **[グループ化]**をクリックします。
2. **[すべてのグループを折りたたむ]**をクリックします。
   表示は最上位レベルのグループの表示に戻ります。

➡ すべてのグループ化の削除手順

1. **[グループ化基準]**ボタンをクリックします。
2. **[グループ化しない]**を選択します。
   マップはグループ化が適用されず、すべての個々の資産が表示されます。

マップ表示へのフィルターの適用

資産タイプ、ベンダー、ファミリー、リスクレベル、パデューレベルの 1 つ以上の指定されたカテゴリでマップ表示をフィルターできます。



フィルターのマップへの適用手順

1. 必要なフィルターカテゴリをクリックします。
2. 表示に含める / 除外する各要素のチェックボックスを選択 / 選択解除します。

> デフォルトでは、すべての要素がフィルターに含まれています。

3. **[すべて選択]** チェックボックスをクリックしてすべての値の選択を解除してから、必要な値を追加できます。
4. フィルター検索ボックスで検索を実行して、フィルターウィンドウで特定の値を検索できます。
5. 必要に応じて、各フィルターカテゴリに対してこのプロセスを繰り返します。
6. **[適用]** をクリックします。
   選択した要素のみがマップに表示されます。

資産詳細の表示

特定の資産をクリックすると、リスクレベル、IP アドレス、資産タイプ、ベンダー、ファミリーなど、資産とそのネットワークアクティビティに関する基本情報が表示されます。マップには、選択した資産から、その資産と通信している他のすべての資産への接続が表示されます。次に、資産名のリンクをクリックすると、**[資産の詳細]**画面に移動し、資産に関するより詳細な情報を表示できます。

ネットワークベースラインの設定

ネットワークベースラインは、指定された期間にネットワーク内の資産間で行われたすべての会話のマップです。ネットワークベースラインは、ネットワーク内の異常な会話を警告する*ネットワークベースライン逸脱*ポリシーで使用されます。**ネットワークイベントのタイプ**を参照してください。

ベースラインサンプル中に相互作用しなかった資産間の各会話により、ポリシーアラートがトリガーされます(指定されたポリシー条件の範囲内であることが前提です)。ネットワークベースライン逸脱ポリシーを作成できるようにするには、[ネットワークマップ]画面で最初のネットワークベースラインを作成する必要があります。ネットワークベースラインは、新しいネットワークベースラインを設定することで、いつでも更新できます。新しい資産または接続がネットワークに追加されるたびに、新しいネットワークベースラインを設定する必要があります。

➡ ネットワークベースラインの設定手順

1. **[ネットワークマップ]**画面で、画面上部の**[タイムフレーム選択]**を使用して、ネットワークベースラインに含める会話の時間範囲を選択します。
   選択したタイムフレームの**ネットワークマップ**が画面に表示されます。
2. 画面上部の**[アクション]**>**[ベースラインとして設定]**をクリックします。
   新しいネットワークベースラインがシステムで構成され、すべてのネットワークベースライン逸脱ポリシーに適用されます。

脆弱性

Tenable.ot は、ネットワークの資産に影響を与えるさまざまなタイプの脅威を識別します。新しい脆弱性に関する情報が発見され一般公開されているドメインで公表されると、Tenable, Inc. の研究スタッフは Nessus がその脆弱性を検出できるようにプログラムを設計します。

これらのプログラムは *プラグイン*という名前で、*Nessus Attack Scripting Language* (NASL) と呼ばれる Nessus 独自のスクリプト言語で記述されています。プラグインは、CVE、およびネットワークの資産に影響を与える可能性がある他の脅威を検出します(旧式のオペレーティングシステム、脆弱なプロトコルの使用、脆弱なオープンポートなど)。

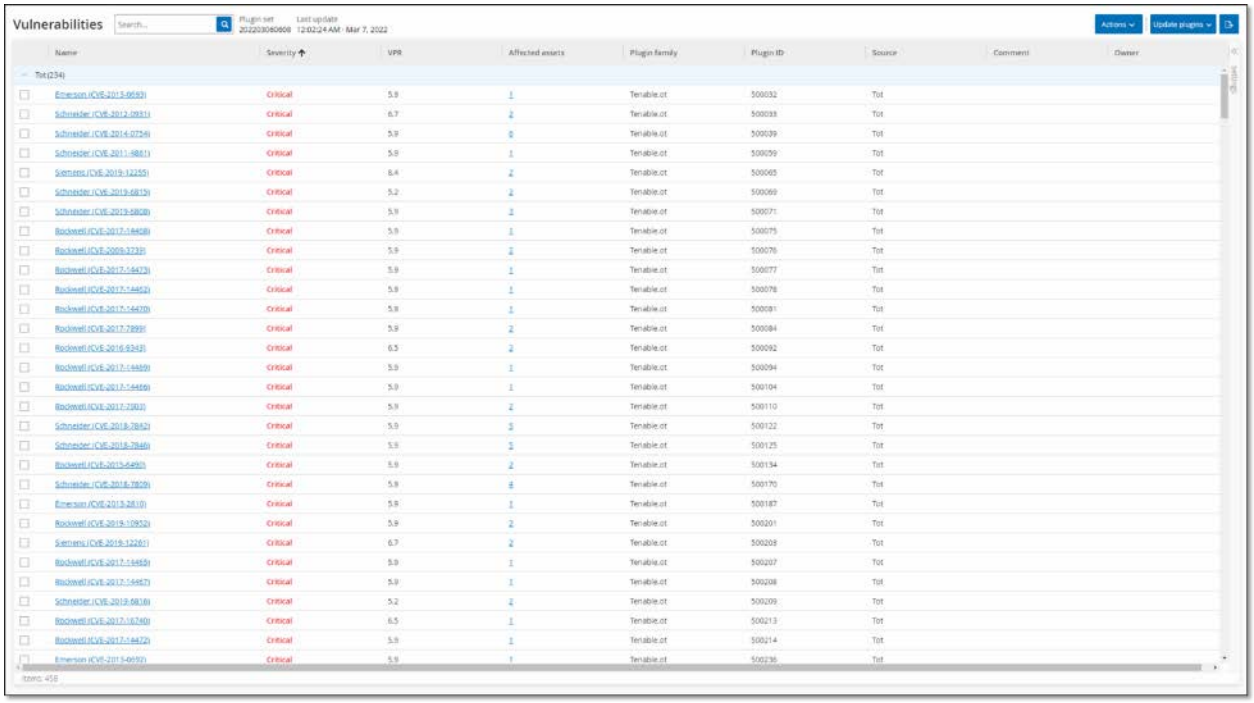
プラグインには、脆弱性情報、修復アクションの一般的なセット、セキュリティ問題の存在をテストするアルゴリズムが含まれています。

プラグインセットの更新については、**更新**を参照してください。

脆弱性画面

[脆弱性] 画面には、ネットワークと資産に影響を与える、Tenable プラグインによって検出されたすべての脆弱性のリストが表示されます。

表示される列と各列の位置を調整することで、表示設定をカスタマイズできます。カスタマイズ機能の説明については、**リスト**を参照してください。



[脆弱性] タブに表示される情報について、次の表で説明します。

パラメーター	説明
名前	脆弱性の名前。名前は、完全な脆弱性リストを表示するリンクになっています。
深刻度	このスコアは、このプラグインによって検出された脅威の深刻度を示します。可能な値は、*情報*、*低*、*中*、*高*です。
VPR	Vulnerability Priority Rating (VPR: 脆弱性優先度評価) は、深刻度レベルの動的インジケーターであり、脆弱性の現在の悪用可能性に基づいて常に更新されます。この値は、脆弱性による技術的な影響と脅威を評価する Tenable の予測に基づいた優先順位付けの出力として Tenable によって生成されます。 VPR の値の範囲は 0.1 から 10.0 で、値が大きいほど悪用の可能性が高くなります。
プラグイン ID	プラグインの一意の識別子。
影響を受ける資産	この脆弱性の影響を受けるネットワーク内の資産の数。
プラグインファミリー	このプラグインが関連付けられているファミリー (グループ)。
コメント	このプラグインに関する自由形式テキストのコメントを追加できます。

プラグインの詳細

プラグイン名をクリックすると、そのプラグインに関する詳細情報が表示されます。

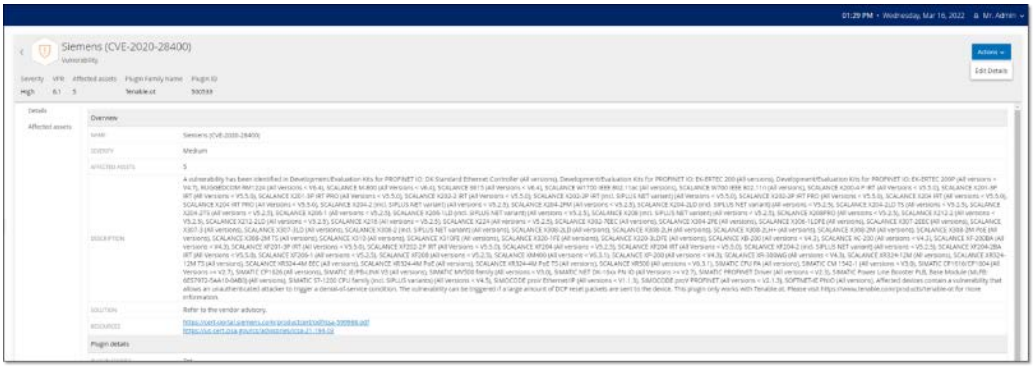
この画面には 3 つの要素があります。

- **ヘッダーバー** - 指定された脆弱性に関する基本情報を表示し、脆弱性の詳細を編集できる **[アクション]** ボタンが含まれています。**脆弱性詳細の編集** を参照してください。
- **詳細タブ** - 脆弱性の完全な説明を表示し、関連するリソースへのリンクを提供します。
- **影響を受ける資産タブ** - 特定の脆弱性の影響を受けるすべての資産のリストを表示します。各リストには、資産に関する詳細情報、およびその資産の [資産詳細] ウィンドウを表示するためのリンクが含まれています。

脆弱性詳細の編集

脆弱性詳細の編集手順

1. 関連する**[脆弱性の詳細]**ページで、右上にある**[アクション]**ボタンをクリックします。
   [アクション]メニューが表示されます。



2. **[アクション]**メニューで、**[詳細の編集]**をクリックします。
   [脆弱性詳細の編集]サイドパネルが表示されます。

3. **[コメント]**フィールドに、脆弱性に関するコメントを入力します。
4. **[所有者]**フィールドに、脆弱性に対処するために割り当てられたユーザーの名前を入力します。
5. **[保存]**をクリックします。

ローカル設定

さまざまな設定画面が、メインナビゲーションの**[ローカル設定]**の下に一覧表示されます。

以下は、各タブで表示される情報と利用可能なアクションの簡単な説明です。

- **クエリ** - クエリ機能をアクティブ化 / アクティブ化解除し、その頻度と設定を調整します。クエリは、*資産検出*、*コントローラー*、*ネットワーク*の別々の画面に分割されます。
- クエリを参照してください。
- **システム構成**
    - **デバイス** - デバイスの詳細とネットワーク情報を表示および編集します(例 : システム時間、DNS サーバー、自動ログアウト(非アクティブタイムアウト))。
    - **センサー** - センサーを表示および管理し、着信センサーのペアリングリクエストを承認または削除し、センサーによって実行されるアクティブクエリを構成します。**センサー**を参照してください。
    - **ポート構成** - デバイスのポートの構成方法を表示します。ポート構成の詳細については、Tenable.ot アプライアンスのインストール > ステップ 4 - セットアップウィザード > **画面 2 – デバイスを参照してください。**
    - **更新** - プラグインの更新をクラウドまたはオフラインで、自動または手動で実行します。
    - **証明書** – HTTPS 証明書に関する情報を表示し、システムで新しい HTTPS 証明書を生成するか独自の HTTPS 証明書をアップロードすることで、安全な接続を確保します。**証明書**を参照してください。
    - **API キー** – API キーを生成して、サードパーティアプリが API 経由で Tenable.ot にアクセスできるようにします。すべてのユーザーが API キーを作成できます。API キーは、それを作成したユーザーのロールに応じて、そのユーザーと同じアクセス許可を持ちます。API キーは、最初に生成されたときに一度表示されます。ユーザーは後で使用するためにそのキーを安全な場所に保存する必要があります。
    - **ライセンス** - ライセンスの表示、更新、再作成を行えます。**ライセンス**を参照してください。
- **環境構成**
    - **資産設定** -
        - **監視対象ネットワーク** – システムが資産を分類する IP 範囲の集約を表示および編集します。
        - **CSV を使用して資産詳細を更新** – CSV テンプレートを使用して資産の詳細を更新します。
        - **資産を手動で追加** – CSV テンプレートを使用して、資産リストに新しい資産を追加します。

NNM に送信できる IP 範囲の最大数は 128 であるため、この制限を超えないことをお勧めします。

指定された IP 範囲に加えて、Tenable.ot プラットフォームのサブネット内のホストまたは任意のアクティビティを実行しているデバイスが資産として分類されます。

- **非表示**の資産 - システムで非表示になっている資産のリストを表示します(ユーザーが資産リストから削除することを選択したものなど)。**資産の非表示**を参照してください。この画面から非表示の資産を復元できます。
- **カスタムフィールド** - カスタムフィールドを作成して、資産に関連情報をタグ付けできます。カスタムフィールドはプレーンテキストにすることも、外部リソースへのリンクにすることもできます。
- **イベントクラスター** - イベントの監視を容易にするために、指定された時間範囲内で発生する複数の類似のイベントをクラスター化できます。**イベントクラスター**を参照してください。
- **PCAP プレーヤー** - 記録されたネットワークアクティビティを含む PCAP ファイルをアップロードし、それを Tenable.ot で「再生」し、データをシステムに読み込むことができます。**PCAP プレーヤー」**を参照してください。

- **ユーザーおよびロール** - すべてのユーザーアカウントに関する情報を表示、編集、エクスポートします。

  - **ユーザー設定** - 現在システムにログインしているユーザーに関する情報(フルネーム、ユーザー名、パスワード)を表示および編集し、ユーザーインターフェースで使用する言語(英語、日本語、中国語、フランス語、ドイツ語)を変更します。
  - **ローカルユーザー** - 管理者ユーザーは、特定のユーザー用のローカルユーザーアカウントを作成し、そのアカウントにロールを割り当てることができます。**ローカルユーザー**を参照してください。
  - **ユーザーグループ** - 管理ユーザーは、ユーザーグループを表示、編集、追加、削除できます。**ユーザーグループ**を参照してください。
  - **認証サーバー** - Active Directory などの LDAP サーバーを使用して、オプションでユーザー認証情報を割り当てることができます。この場合、ユーザー権限は Active Directory で管理されます。**認証サーバー**を参照してください。

- **統合** - 他のプラットフォームとの統合を設定します。Tenable.ot は現在、Palo Alto Networks 次世代ファイヤーウォール(NGFW)と Aruba ClearPass、およびその他の Tenable 製品(Tenable.sc と Tenable.io)との統合をサポートしています。**統合**を参照してください。
- **サーバー** - システムで構成されたサーバーを表示、作成、編集します。以下の 3 つに対して個別の画面が表示されます。

  - **SMTP サーバー** - SMTP サーバーにより、イベント通知を電子メールで送信できます。
  - **Syslog サーバー** - Syslog サーバーにより、イベントログを外部 SIEM に記録できます。
  - **FortiGate ファイヤーウォール** - Tenable.ot と FortiGate の統合により、ユーザーは Tenable.ot ネットワークイベントに基づいてファイヤーウォールポリシーの提案を FortiGate ファイヤーウォールに送信できます。

- **システムアクション** - システムアクティビティのサブメニューを表示します。サブメニューには次のオプションがあります。

  - **システムバックアップ** - Tenable.ot アプライアンスをバックアップできます(パケットキャプチャデータを除く)。バックアップファイルからシステムを復元するには、https://www.tenable.com/products/tenable-ot に連絡してください。バックアップ処理中、すべてのユーザーが Tenable.ot を使用できなくなることに注意してください。
  - **エクスポート設定** - Tenable.ot プラットフォーム構成設定を .ndg ファイルとしてローカルコンピューターにエクスポートします。これは、システムをリセットする場合や、新しい Tenable.ot プラットフォームにインポートする場合のバックアップとして機能します。
  - **インポート設定** - .ndg ファイルとしてローカルコンピューターに保存された Tenable.ot プラットフォーム構成設定をインポートします。
  - **診断データをダウンロード** - 診断データを含むファイルを Tenable.ot プラットフォームに作成し、ローカルコンピューターに保存します。
  - **再起動** - Tenable.ot プラットフォームを再起動します。これは、特定の構成変更のアクティベーションに必要です。
  - **無効化** - すべての監視アクティビティを無効化します。監視アクティビティはいつでも再度アクティブ化できます。
  - **シャットダウン** - Tenable.ot プラットフォームをシャットダウンします。電源を入れるには、Tenable.ot アプライアンスの電源ボタンを押します。

- **出荷時の設定にリセット** - すべての設定を出荷時のデフォルト設定に戻します。警告 : この操作は元に戻すことができず、システム内のすべてのデータが失われます。

- **システムログ** - システムで発生したすべてのシステムイベント(オンになっているポリシー、編集済みポリシー、解決済みイベントなど)のログを表示します。ログは CSV ファイルとしてエクスポートすることも、Syslog サーバーに送信することもできます。**システムログ**を参照してください。

クエリ

[Tenable.ot クエリ]画面では、クエリ機能を構成してアクティブ化できます。クエリテクノロジーの一般的な説明については、**Tenable.ot テクノロジー**を参照してください。初期セットアップの一部として、すべてのクエリ機能をアクティブ化することが推奨されていましたが、いつでも、任意のクエリ機能をアクティブ化 / 非アクティブ化できます。また、クエリを実行するタイミングと方法の設定を調整することもできます。

定期的に実行される自動クエリに加えて、ほとんどのクエリは、クエリの横にある**[今すぐ実行]**ボタンをクリックすることで、ユーザーがオンデマンドで開始できます。

Log4J および Ripple20 脆弱性スキャンは**手動**でのみ実行でき、定期的なスケジュールでは実行できません。これらは、**[ローカル設定]** > **[クエリ]** > **[ネットワーク]** 画面からアクティブ化されます。 **ネットワーククエリ機能テーブル**を参照してください。

クエリをオフにすると、システムがネットワークで重要なイベントを検出できなくなります。これにより、多くの機能が使用できなくなります。

クエリのアクティブ化と構成は、**[ローカル設定]**>**[クエリ]**で行います。クエリは 3 つの画面に分割されます。次のセクションでは、さまざまなタイプのクエリについて説明し、各タイプのクエリをアクティブ化および構成する手順を示します。

すべてのコントローラークエリ

➡ コントローラークエリのアクティブ化手順

1. **[ローカル設定]**で、**[クエリ]**>**[コントローラー]**画面に移動します。
2. **[すべてのコントローラークエリ]**のスイッチを**オン**に切り替えます。
3. クエリのタイプごとにステータスの**オン / オフ**を切り替えることで、特定のタイプのクエリをアクティブ化 / アクティブ化解除します。さまざまなタイプのコントローラークエリの説明については、**コントローラークエリ機能テーブル**を参照してください。
4. 次の手順を使用して、各コントローラークエリタイプの設定を編集できます。
    a. 目的のクエリタイプの横にある**[編集]**をクリックします。
    b. クエリの頻度とスケジュールを調整します(利用可能な設定オプションの説明については、**コントローラークエリ機能テーブル**を参照してください)。
    c. **[保存]**をクリックします。

コントローラークエリ機能テーブル

機能	説明	頻度 (最小～最大)
すべてのコントローラークエリ	以下で説明するように、コントローラーに関連するすべてのクエリ機能をアクティブ化します。	該当なし

機能	説明	頻度 (最小～最大)
定期スナップショット	各コントローラーに展開されている現在のプログラムをキャプチャします。スナップショットを定期的に取得することにより、変更がネットワークを介して送信されなくても、Tenable.ot はコントローラーのプログラムに加えられた変更を検出できます。	1 日 1 回 ～ 6 週間に 1 回
ポリシートリガースナップショット	ユーザーがポリシーを構成して、ポリシーの条件が満たされたときにスナップショットをトリガーできるようにします。	該当なし
コントローラー検出	新しいコントローラーを検索し、不明な資産の分類を支援するブロードキャスト。	1 時間 1 回 ～ 6 週間に 1 回
コントローラー状態クエリ	現在の PLC ステータスを検出します (オプション : *実行中*、*停止中*、*障害*、*構成なし*、*テスト*)。	5 分に 1 回 ～ 1 時間に 1 回
診断バッファクエリ	Siemens コントローラーで定義された診断バッファイベントログのクエリ。	1 日 1 回 ～ 6 週間に 1 回
コントローラー詳細クエリ	コントローラーのハードウェアとファームウェアの詳細を取得します。	1 時間 1 回 ～ 6 週間に 1 回
バックプレーンクエリ	バックプレーン内のモジュールとその仕様を検出します。クエリにより、バックプレーン全体の構成を迅速に特定できます。	15 分に 1 回 ～ 1 週間 1 回

すべてのネットワーククエリ

➡ ネットワーククエリのアクティブ化手順

1. **[ローカル設定]** で、**[クエリ]**>**[ネットワーク]** 画面に移動します。
2. **[すべてのネットワーククエリ]** のスイッチを**オン**に切り替えます。
3. アクティブ化したいクエリのタイプごとにステータスの**オン / オフ**を切り替えることで、特定のタイプのクエリをアクティブ化 / アクティブ化解除します。さまざまなネットワーククエリ機能の説明については、**ネットワーククエリ機能テーブル**を参照してください。
4. 次の手順を使用して、各ネットワーククエリタイプの設定を編集できます。
    a. 目的のクエリタイプの横にある **[編集]** をクリックします。
    b. クエリの頻度とスケジュールを調整します (利用可能な設定オプションの説明については、**ネットワーククエリ機能テーブル**を参照してください)。
    c. **[保存]** をクリックします。

ネットワーククエリ機能テーブル

機能	説明	設定
すべてのネットワーククエリ	以下で説明するように、非コントローラーネットワーク資産に関連するすべてのクエリ機能をアクティブ化します。	該当なし
ポートマッピング	ネットワーク資産のすべてのオープンポートを特定します。これにより、未使用のポートを閉じることで、セキュリティリスクを最小限に抑えることができます。	マッピング範囲 - マッピングがすべてのポートに対して行われるか、最も頻繁に使用される 1,000 個のポートに対してのみ行われるかを設定します。 マッピングレート - デフォルトで毎秒マッピングされるポート数と、オンデマンドマッピングの最大レートを設定します。

機能	説明	設定
SNMP クエリ	ネットワークの SNMP 対応資産から構成情報を収集します。	SNMP v2 コミュニティ文字列 SNMP v3 ユーザー名 頻度とスケジュール - 1 日 1 回 ～ 6 週間に 1 回
DNS クエリ	ネットワーク内の資産の DNS 名を検索します。	該当なし
ARP クエリ	ネットワークで検出された新しい IP の MAC アドレスを取得します。	該当なし
NetBIOS	このクエリは、ネットワーク内の Windows マシンの分類と検出に使用される NetBIOS ユニキャストパケットを送信します。	頻度とスケジュール - 1 時間 1 回 ～ 6 週間に 1 回
アクティブ資産追跡	指定された期間にわたってネットワーク内の非アクティブな資産を検出し、それら資産をポーリングしてまだアクティブであるかどうかを検証します。	頻度とスケジュール - 5 分に 1 回 ～ 1 週間 1 回
WMI クエリ	ネットワーク内の Windows マシンに関する情報を収集します。	WMI ユーザー名 - IT 提供 パスワード - IT 提供 頻度とスケジュール - 1 日 1 回 ～ 6 週間に 1 回 IP アドレスのテスト - [IP アドレスのテスト] をクリックし、ネットワーク内の既知の Windows マシンの IP を入力してから、画面の下部にある [IP アドレスのテスト] をクリックすると、WMI 構成をテストできます。次に、その資産の「資産詳細」を開くことで、WMI 情報が追加されたことを確認できます。
USB 接続クエリ	ネットワーク内の Windows PC への USB/DoK デバイスの接続を検出します。	頻度とスケジュール - 1 日 1 回 ～ 6 週間に 1 回
Ripple20 の脆弱性スキャン	このスキャンは、Ripple20 の脆弱性に関連する CVE を特定します。Nessus プラグインを使用します。 **注意:** このスキャンは**手動**で実行する必要があり、指定された IP アドレスや CIDR 内の資産でのみ実行されます。	IP アドレスまたは CIDR
Log4J の脆弱性スキャン	このスキャンは、Log4J の脆弱性に関連する CVE を特定します。Nessus プラグインを使用します。 **注意:** このスキャンは手動で実行する必要があり、指定された IP アドレスや CIDR 内の資産でのみ実行されます。	IP アドレスまたは CIDR

資産検出

Tenable.ot は、ネットワークを介した他の資産とのやり取りを検出することで、ネットワーク内の資産を自動的に識別します。Tenable.ot には、ネットワークでアクティブでない資産や、**資産検出**クエリを使用するミラーリングポートによって通信ストリームがキャプチャされない資産を識別する追加機能があります。クエリが自動的に実行される頻度を設定することもでき、この画面からいつでも手動でクエリを実行することもできます。

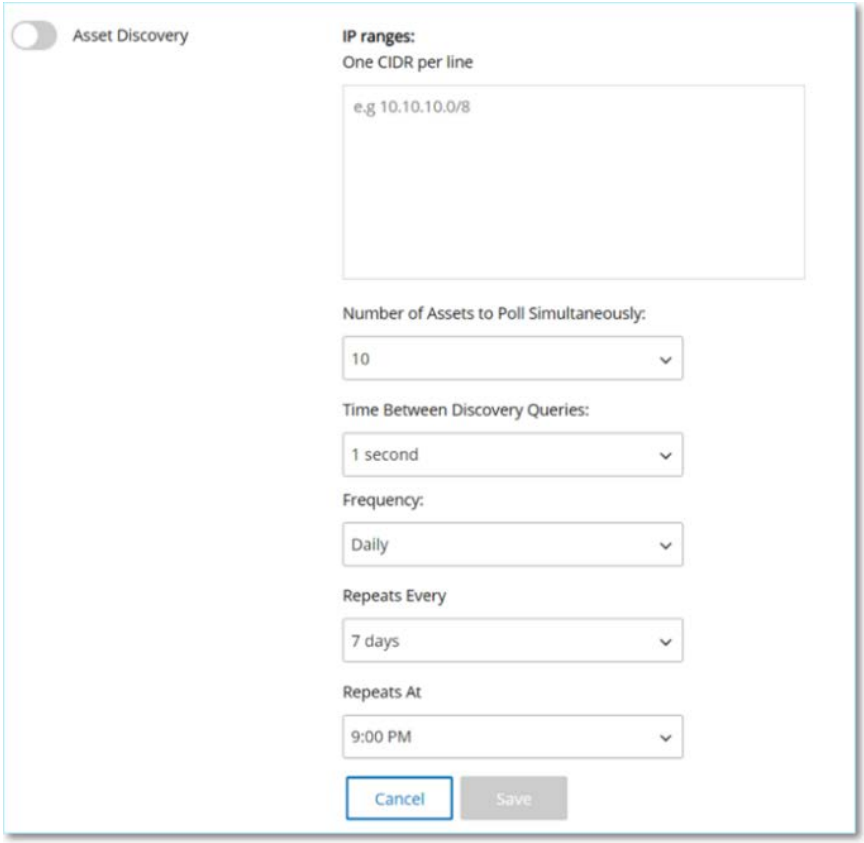
新しい資産が検出されると、**初期資産強化**機能が次のクエリを実行して、資産に関する正確な情報を判断します。SNMP、最小オープンポート検証、CIP / DCP、NetBIOS、バックプレーンクエリ、ユニキャスト識別、コントローラー詳細、コントローラー状態。

> **資産設定**で監視対象ネットワークとして定義されている IP のみがスキャンに含まれます。

> クエリをオフにすると、システムがネットワークで重要なイベントを検出できなくなります。これにより、多くの機能が使用できなくなります。

資産検出クエリのアクティブ化手順

1. **[ローカル設定]**で、**[クエリ]**>**[資産検出]**画面に移動します。
2. **[資産検出]**セクションで**[編集]**をクリックします。
   一連の構成フィールドが表示されます。



3. **[IP 範囲]**ボックスに、1 つ以上の IP 範囲を入力します(各範囲を別々の行に入力)。

ミラーポートによって監視されているネットワークのセグメントを入力する必要はありません。Tenable.ot によって自動的にクエリされます。ミラーポートで監視されていないネットワークの**追加**セグメントで資産検出クエリを実行する場合は、それらのセグメントの IP の範囲をこのボックスに入力します。

4. ドロップダウンメニューから値を選択することで、以下の構成設定(オプション)を調整できます。
   - **同時にポーリングする資産の数**(オプション: 10、20、30)
   - **検出クエリ間の時間**(オプション: 1 ～ 3 秒)
   - **繰り返し** - クエリの頻度の設定に使用される間隔のタイプを設定(日次または週次)
   - **繰り返し頻度** - クエリの頻度を設定(日次: 1～31 日、週次: 1～6 週間)
   - **曜日** - 週次間隔の場合、クエリを実行する曜日を設定
   - **時刻** - クエリを実行する時刻を設定
5. **[保存]**をクリックします。
6. **[資産検出]**スイッチを**オン**に切り替えます。

➡ 初期資産強化のアクティブ化手順

1. **[ローカル設定]**で、**[クエリ]**>**[資産検出]**画面に移動します。
2. **[初期資産強化]**のスイッチを**オン**に切り替えます。

Nessus プラグインスキャン

Nessus プラグインスキャンは、CIDR と IP アドレスのリストで指定された資産でプラグインのユーザー定義リストを実行する高度な Nessus スキャンを起動します。

スキャンは、指定された CIDR 内の応答する資産で実行されます。ただし、OT デバイスを保護するために、特定の範囲(PLC 以外)で確認されたネットワーク資産のみがスキャンされます。「エンドポイント」タイプの資産はスキャンされません。

Nessus は、IT 環境で最適に動作する侵入型ツールです。通常の動作に干渉する可能性があるため、OT デバイスでの使用はお勧めしません。

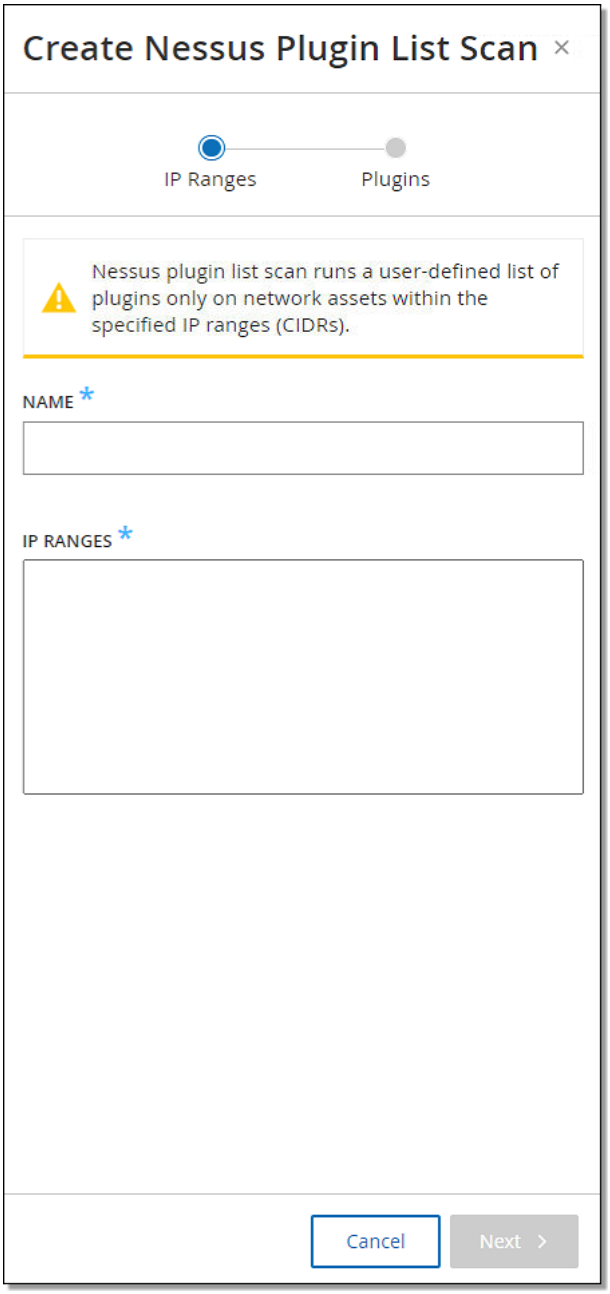
任意の 1 つの資産で基本 Nessus スキャンを実行するには、**資産特定 Nessus スキャンの実行**を参照してください。

基本スキャンは、「エンドポイント」タイプの資産で実行できます。

➡ Nessus プラグインスキャンの作成手順

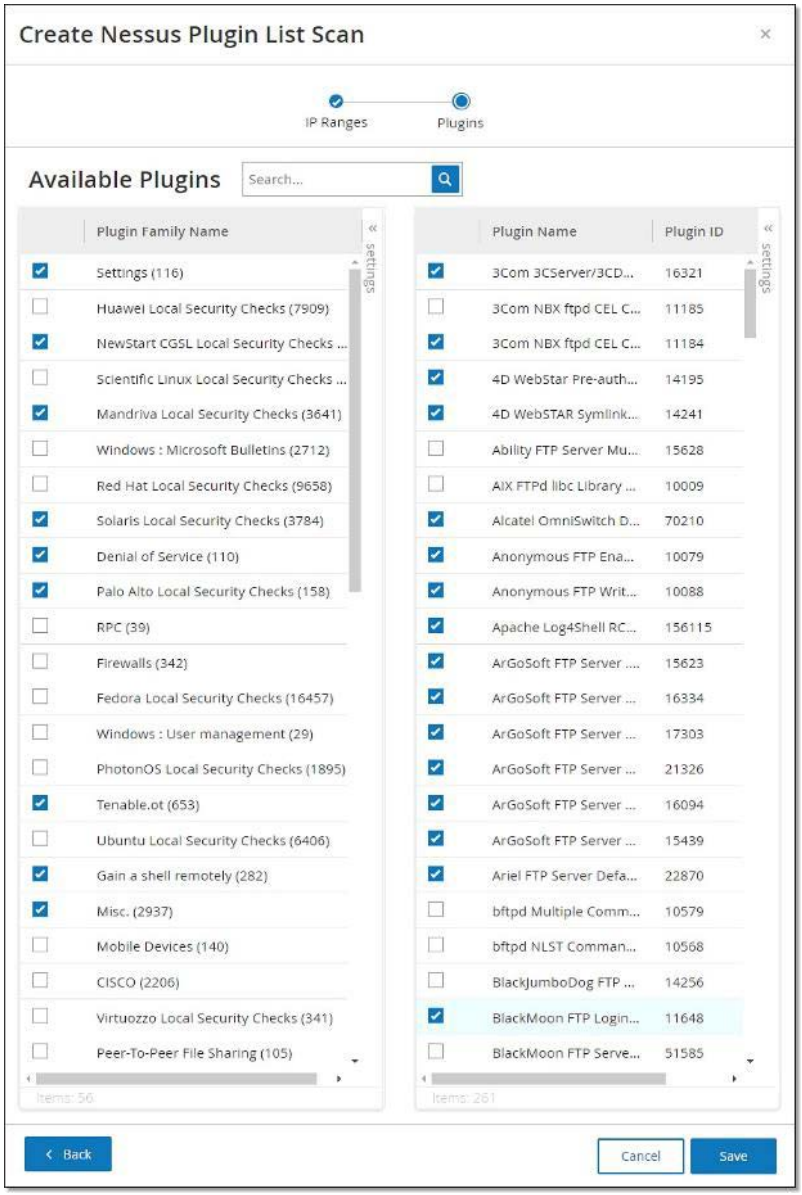
1. **[ローカル設定]**>**[クエリ]**>**[Nessus スキャン]**に移動します。

2. **[スキャンの作成]**ボタンをクリックします。
   [Nessus プラグインリストスキャンの作成]サイドパネルが表示されます。



3. **[名前]**フィールドに、Nessus スキャンの名前を入力します。
4. **[IP 範囲]**フィールドに、IP または CIDR の範囲を入力します。

5. **[次へ]**をクリックします。
   [プラグイン]ペインが表示されます。



> 表示されるプラグインはデバイス固有です。新しいプラグインを受信するには、ライセンスが最新の状態である必要があります。ライセンスを更新するには、**ライセンスの更新**を参照してください。

6. 左側の列で必要に応じてプラグインファミリーを選択してスキャンに含め、右側の列で必要に応じて個々のプラグインの選択を解除します。

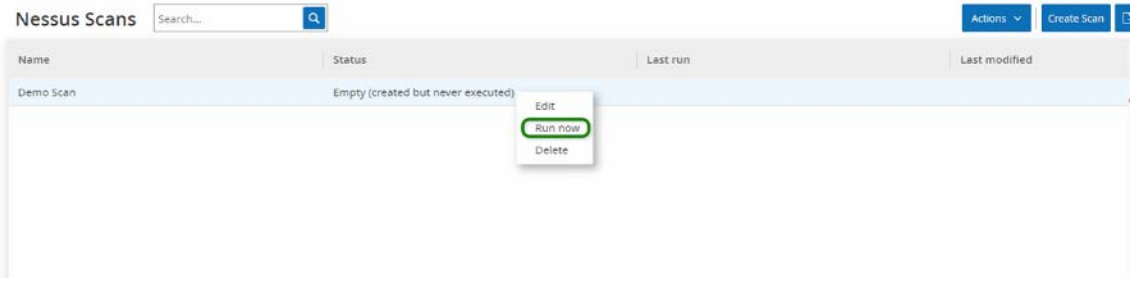
> Nessus プラグインファミリーの詳細については、https://www.tenable.com/plugins/nessus/families を参照してください。

7. **[保存]**をクリックします。
   新しい Nessus スキャンが**[Nessus スキャン]**画面に表示されます。

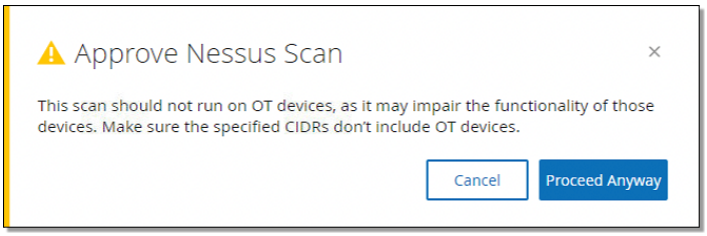
> 既存の Nessus スキャンを編集または削除するには、対象のスキャン行を右クリックし、**[編集]** または **[削除]** を選択します。

Nessus プラグインスキャンの実行手順

1. **[Nessus スキャン]** 画面で、対象のスキャン行を選択し、右クリックして **[今すぐ実行]** を選択するか、**[アクション]>[今すぐ実行]** をクリックします。



[Nessus スキャンの承認] ダイアログが表示されます。



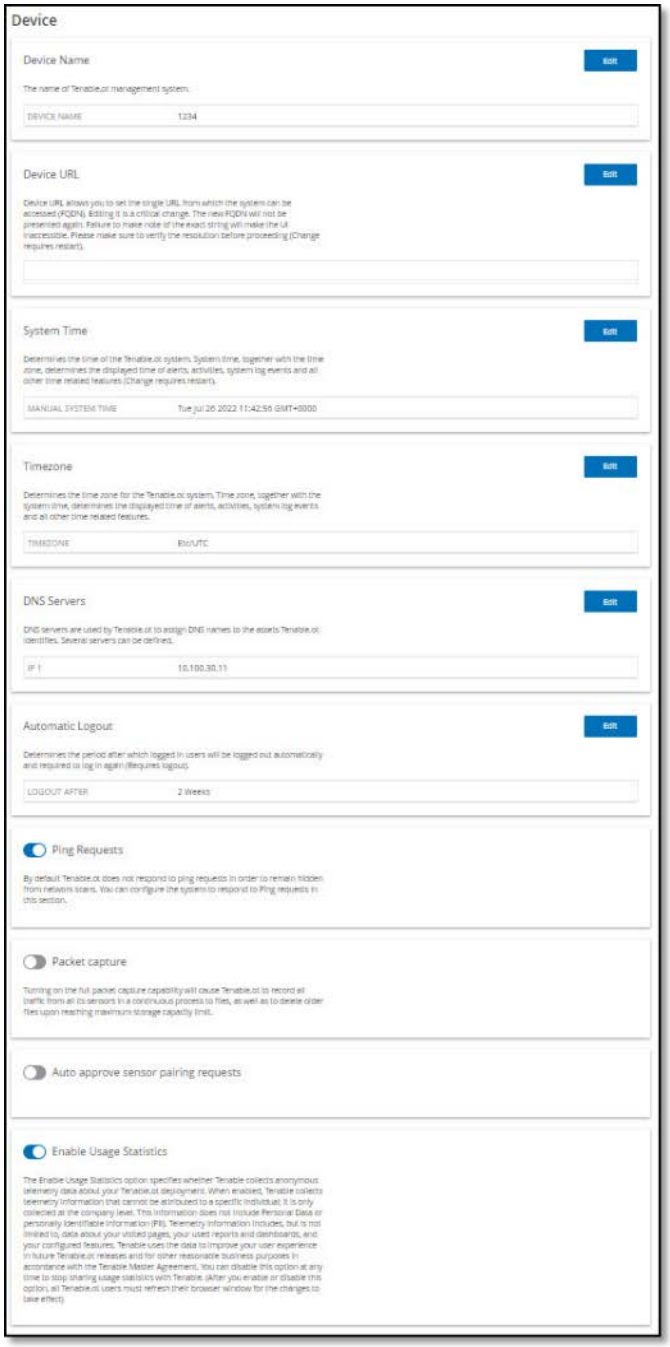
2. スキャンに OT デバイスが含まれていないことがわかっている場合は、**[続行]** をクリックします。
   ダイアログが閉じ、スキャンが保存されます。
3. スキャンを実行するには、もう一度スキャン行を右クリックし、**[今すぐ実行]** を選択します。
   [Nessus スキャンの承認] ダイアログが再び表示されます。
4. **[続行]** をクリックします。
   スキャンが実行されます。スキャンは、現在のステータスに基づいて、一時停止 / 再開、停止、中止される可能性があります。

システム構成

Tenable.ot のシステム構成画面を使用すると、プラグインの更新を自動的に構成したり、プラグインの更新を手動で実行できたりするほか、デバイス、HTTPS 証明書、API キー、ライセンスに関する詳細を表示および更新できます。

デバイス

この画面には、Tenable.ot 構成に関する詳細情報が表示されます。この画面で情報を表示し、構成を編集できます。



次の情報が表示されます。

- **デバイス名** - Tenable.ot アプライアンスの一意の識別子。
- **デバイス URL** – システムにアクセスできる 1 つの URL を設定できます(FQDN)。

デバイス URL の編集は重要な変更です。新しい FQDN は再度表示されません。そのため、文字列を正確にメモしておかないと UI にアクセスできなくなります。続行する前に、必ず解決が正しいかどうか確認してください。

- **システム時刻** – 通常、正しい時刻と日付が自動的に設定されますが、編集も可能です。

ログとアラートを正確に記録するには、正しい日付と時刻を設定することが重要です。

- **タイムゾーン** – ドロップダウンリストからサイトの場所のローカルタイムゾーンを選択します。
- **DNS サーバー** – DNS サーバーは、Tenable.ot が特定する資産に DNS 名を割り当てるため Tenable.ot システムによって使用されます。複数のサーバーを指定できます。
- **自動ログアウト** – ログインユーザーが自動的にログアウトされて再ログインを要求されるようになるまでの時間を決定します。
- **オープンポートのタイムアウト期間** - ここで指定した期間が経過してもポートがまだ開いていることを示す情報を受信しない場合、そのオープンポートのリストが個々の[資産の詳細]画面から削除されます。デフォルト設定は 2 週間です。詳細は、**オープンポート**を参照してください。

ping 要求

ping 要求をオンにすると、ping 要求に対する Tenable.ot プラットフォームの自動応答がアクティブ化されます。

➡ ping 要求のアクティブ化手順

1. **[ローカル設定]**>**[システム構成]**>**[デバイス]**画面に移動します。
2. **[ping 要求]**スイッチを**オン**に切り替えます。

パケットキャプチャ

フルパケットキャプチャ機能をオンにすると、ネットワーク内のすべてのトラフィックのフルパケットキャプチャの連続記録がアクティブ化されます。これにより、トラブルシューティングとフォレンジック調査機能を拡張できます。ストレージ容量(1.8 TB)を超えると、システムは古いファイルを削除します。利用可能なファイルは、**[ネットワーク]**>**[パケットキャプチャ]**画面で表示およびダウンロードできます。**パケットキャプチャ**セクションを参照してください。

➡ パケットキャプチャのアクティブ化手順

1. **[ローカル設定]**>**[システム構成]**>**[デバイス]**画面に移動します。
2. **[パケットキャプチャ]**スイッチを**オン**に切り替えます。

スイッチを**オフ**に切り替えることで、パケットキャプチャ機能をいつでも停止できます。

センサーペアリングリクエストの自動承認

着信センサーペアリングリクエストの自動承認を有効にすると、管理者が追加の手順を実行することなく、すべてのセンサーペアリングリクエストが承認されるようになります。このオプションを選択しない場合、新しいセンサーをネットワークに接続するには、最終的な手動承認が必要です。

着信センサーペアリングリクエストの自動承認を有効にする手順

1. **[ローカル設定]**>**[システム構成]**>**[デバイス]**画面に移動します。
2. **[着信センサーペアリングリクエストの自動承認]**スイッチを**オン**に切り替えます。

スイッチを**オフ**に切り替えることで、着信センサーペアリングリクエストの自動承認をいつでも許可できます。

使用状況統計の有効化

[使用状況統計の有効化]オプションにより、Tenable が Tenable.ot デプロイメントについての匿名のテレメトリデータを収集するかどうかを指定します。有効にすると、Tenable は特定の個人に帰属しないテレメトリ情報を収集します。この情報は会社レベルでのみ収集され、個人データや個人を特定できる情報(PII)は含まれません。テレメトリ情報とは、アクセスしたページ、使用したレポートとダッシュボード、設定済み機能に関するデータを指しますが、これらに限定されません。Tenable は、Tenable 基本契約書に従って、将来の Tenable.ot リリースでユーザーエクスペリエンスを改善するためおよびその他の合理的なビジネス上の目的でデータを使用します。この設定はデフォルトで有効です。

使用状況統計を有効にする手順

1. **[ローカル設定]**>**[システム構成]**>**[デバイス]**画面に移動します。
2. **[使用状況統計の有効化]**スイッチを**オン**に切り替えます。

スイッチを**オフ**に切り替えることで、使用状況統計の共有をいつでも無効にできます。

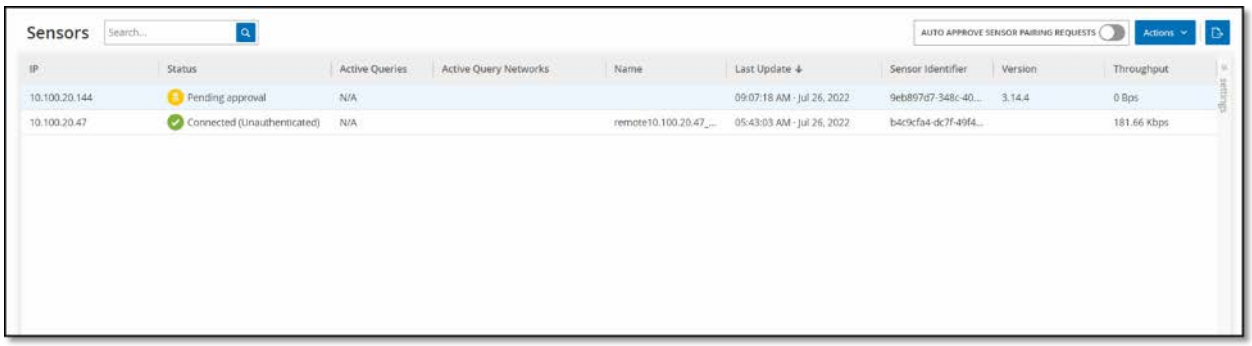
センサー

Tenable Core UI を使用してセンサーをペアリングすると、**[アクション]**メニューで編集機能、一時停止機能、削除機能を使用して、新しいペアリングを承認したりセンサーを表示および管理することができます。トグルスイッチを使用して、センサーペアリングリクエストの自動承認を有効にすることもできます。

バージョン 2.214 よりも前のセンサーモデルは、ICP センサー ページに表示されません。ただし、これまで通り未認証モードで使用できます。

センサー画面の表示

[センサー]テーブルには、システム内の v. 2.214 以降のすべてのセンサーのリストが表示されます。



画面に表示される情報について、次の表で説明します。

パラメーター	説明
IP	センサーの IPv4 アドレス。
ステータス	センサーのステータス: 接続済み、接続済み(未認証)、承認保留中、切断済み、または一時停止。
アクティブクエリ	センサーのアクティブクエリ送信機能(有効、無効、該当なし)。
アクティブクエリネットワーク	センサーが割り当てられているネットワークセグメント。
名前	システム内のセンサーの名前。
最終更新日	センサー情報が最後に更新された日時。
センサー識別子	UUID(Sensor Universal Unique Identifier)。インターネット上のオブジェクトまたはエンティティを一意に識別するために使用される 128 ビットの値。
バージョン	センサーのバージョン。
スループット	センサーを介してストリーミングされているデータ量の測定値(KB/秒)。

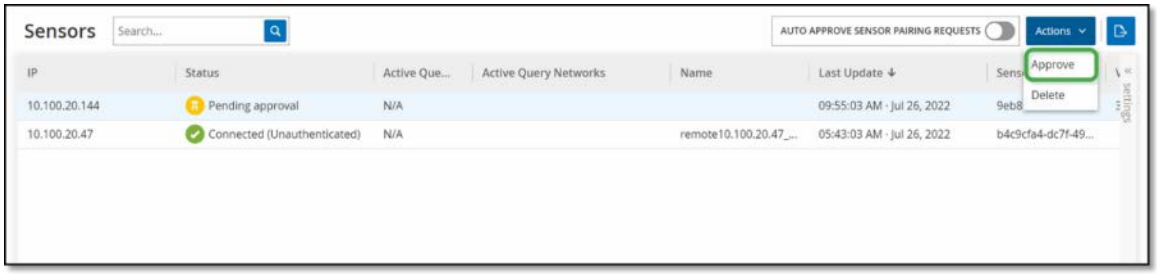
受信センサーペアリングリクエストの手動承認

[センサーのペアリングリクエストの自動承認]設定が**オフ**に切り替えられている場合、受信センサーのペアリングリクエストを手動で承認しないと正常に接続されません。

➡ センサーペアリングリクエストを手動で承認する手順

1. **[ローカル設定]**>**[システム構成]**>**[センサー]画面**に移動します。
2. ステータスが**[承認保留中]**のテーブル内の行をクリックします。

3. **[アクション]**>**[承認]**をクリックするか、右クリックして右クリックメニューから**[承認]**を選択します。



センサーを削除する場合は、**[アクション]**>**[削除]**をクリックするか、右クリックして右クリックメニューから**[削除]**を選択します。

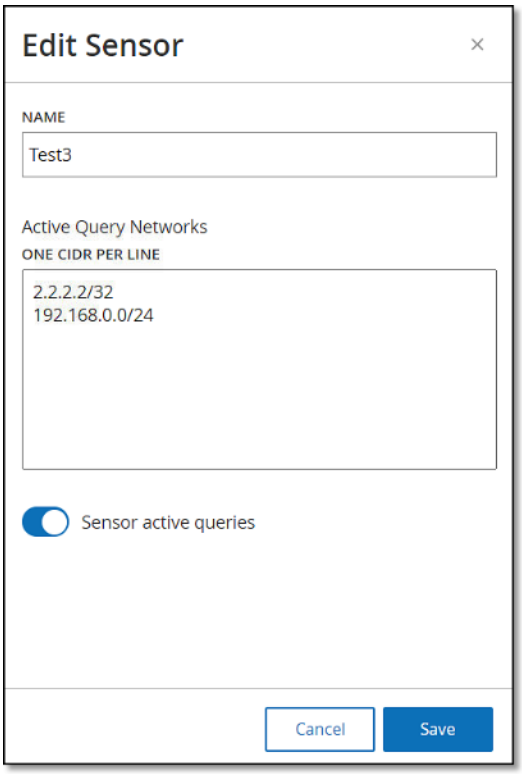
アクティブクエリの構成

センサーが*認証*モードで接続されると、割り当てられているネットワークセグメントでアクティブクエリを実行するようにセンサーを構成できます。クエリするネットワークセグメントを指定する必要があります。

センサーは、この構成に関係なく、利用可能なすべてのセグメントでパッシブネットワーク検出を実行します。

アクティブクエリの構成手順

1. **[ローカル設定]**で、**[システム構成]**>**[センサー]**に移動します。
2. ステータスが**[接続済み]**のテーブル内の行をクリックします。
3. **[アクション]**>**[編集]**をクリックするか、右クリックして右クリックメニューから**[編集]**を選択します。
   [センサーの編集]パネルが表示されます。



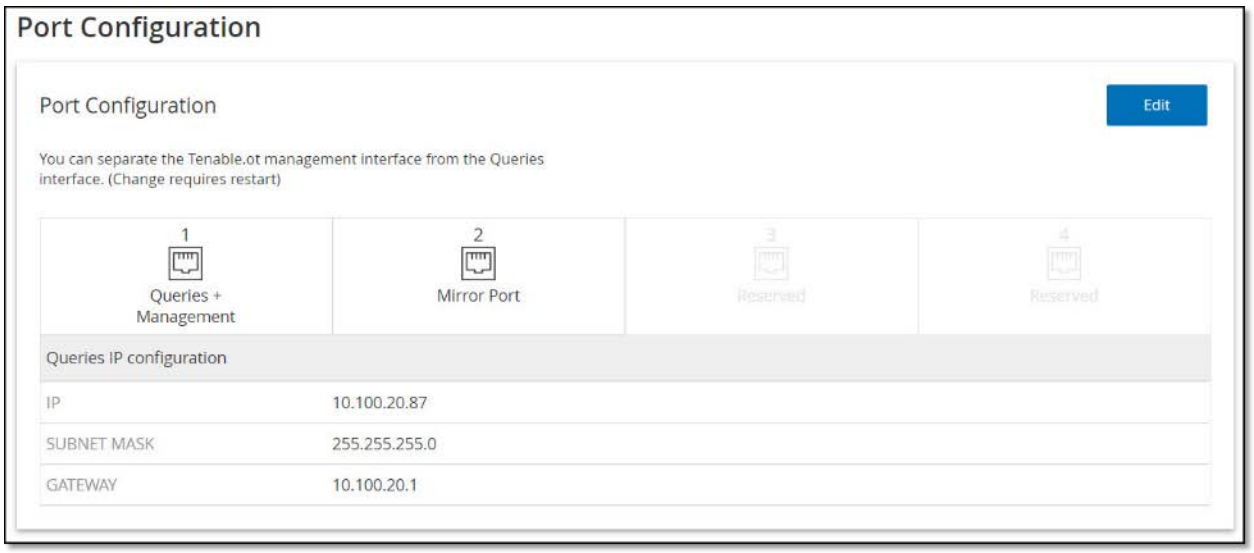
4. センサーの名前を変更する場合は、**[名前]**フィールドのテキストを編集します。
5. **[アクティブクエリネットワーク]**フィールドで、CIDR 表記を使用し個々の行で各サブネットワークを追加して、センサーがアクティブクエリを送信する関連ネットワークセグメントを追加または編集します。

クエリは、監視対象のネットワーク範囲に含まれる CIDR でのみ実行できます。このセンサーを介してアクセス可能な CIDR のみを追加するようにしてください。アクセスできない CIDR を追加すると、ICP が他の手段でこれらのセグメントをクエリする機能が妨げられる可能性があります。

6. **[センサーアクティブクエリ]** スイッチを**オン**に切り替えて、アクティブクエリを有効にします。
7. **[保存]** をクリックします。
   パネルが閉じます。
   [センサー] テーブルの **[アクティブクエリ]** の見出しで、有効なセンサーが **[有効]** と表示されます。

ポート構成

[ポート構成] 画面は、デバイスのポートの構成方法を表示します。ポート構成の詳細については、**Tenable.ot アプライアンスのインストール** > **ステップ 4 - セットアップウィザード** > **画面 2 – デバイス** を参照してください。



更新

プラグインおよび IDS エンジンルールセットを最新の状態に保つことで、資産の最新の既知の脆弱性をすべて確実に監視できます。更新は、クラウドを通じて自動および手動の両方で実行でき、オフラインでも実行できます。

[脆弱性] 画面で **[プラグインの更新]** ボタンをクリックして、更新を実行することもできます。

ユーザーライセンスの有効期限が切れると、新しい更新をダウンロードするオプションがブロックされ、ユーザーはプラグインを更新できなくなります。

Nessus プラグインセットの更新

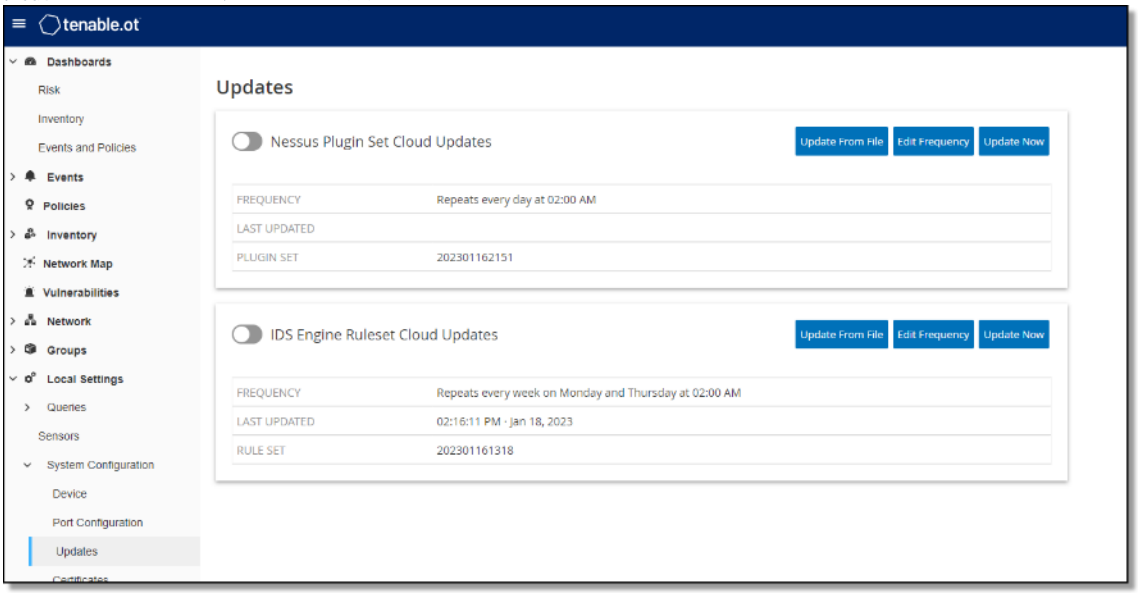
クラウド更新

インターネット接続のあるユーザーは、クラウドを通じてプラグインを更新できます。自動更新がオンの場合、プラグインはユーザーが設定した時間と頻度で更新します(デフォルトは毎日午前 2 時)。

プラグインの自動クラウド更新の設定

➡ プラグインの自動更新を有効にする手順

1. **[ローカル設定]**で、**[システム構成]**>**[更新]**に移動します。
   Nessus プラグインセットのクラウド更新で**[更新]**画面が表示され、プラグインセットの番号、最終更新日時、更新スケジュールが表示されます。

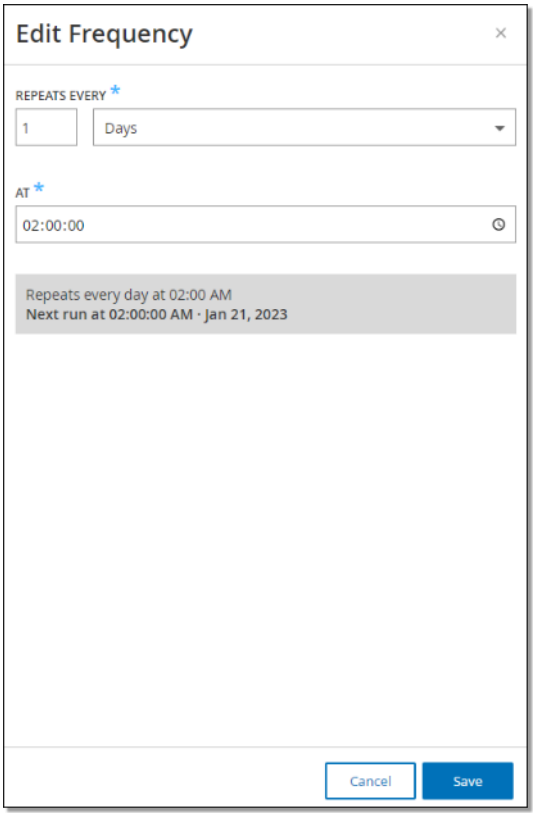


2. トグルスイッチがオンになっていない場合は、クリックして自動更新をオンにします。

➡ プラグインの自動更新スケジュールを編集する手順

1. **[ローカル設定]**で、**[システム構成]**>**[更新]**に移動します。
   Nessus プラグインセットのクラウド更新で**[更新]**画面が表示され、プラグインセットの番号、最終更新日時、更新スケジュールが表示されます。

2. **[頻度の編集]**ボタンをクリックします。
   [頻度の編集]サイドパネルが表示されます。



3. **[繰り返し頻度]**で、数字を入力し、ドロップダウンメニューから時間の単位(日または週)を選択することで、プラグインを更新する時間間隔を設定します。
4. **[週]**を選択した場合は、プラグインで週次更新を実行する曜日を選択します。
5. **[時刻]**で、[時計アイコン]をクリックして時間を選択するか手動で時間を入力して、プラグインを更新する時刻(HH:MM:SS)を設定します。
6. **[保存]**をクリックします。
   頻度の更新が成功したことを通知するダイアログが表示されます。

プラグインの手動クラウド更新の実行

➡ プラグインを手動で更新する手順

1. **[ローカル設定]**で、**[システム構成]**>**[更新]**に移動します。
   Nessus プラグインセットのクラウド更新で**[更新]**画面が表示され、プラグインセットの最終更新バージョン、最終更新日時、更新スケジュールが表示されます。
2. **[今すぐ更新]**ボタンをクリックします。
   更新が開始したことを通知するダイアログが表示されます。更新が完了すると、**[プラグインセット]**フィールドに現在のプラグインセットの番号が表示されます。

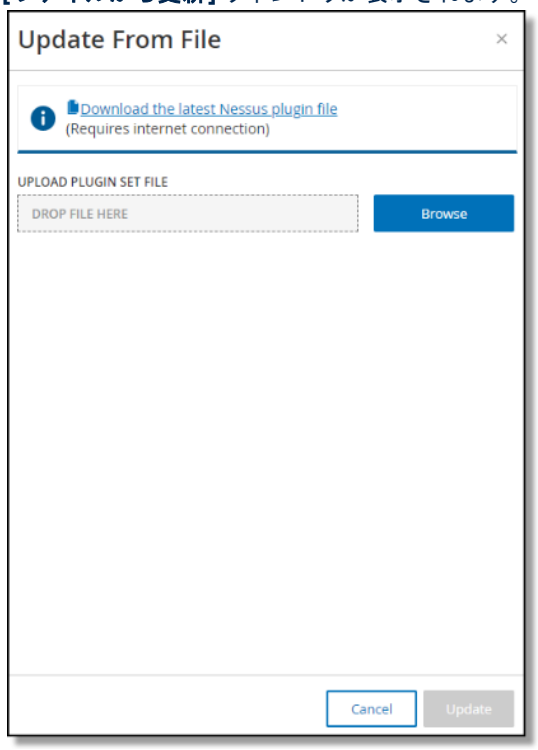
プラグインセットの更新の進行中は、ブラウザウィンドウを開いたままにしてページを更新しないでください。

オフライン更新

Tenable.ot デバイスにインターネット接続がないユーザーは、Tenable Customer Portal から最新のプラグインセットをダウンロードし、ファイルをアップロードすることで、プラグインを手動で更新できます。

➡ プラグインをオフラインで更新する手順

1. **[ローカル設定]** で、**[システム構成]** > **[更新]** に移動します。
   Nessus プラグインセットのクラウド更新 で **[更新]** 画面が表示され、プラグインセットの番号、最終更新日時、更新スケジュールが表示されます。
2. **[ファイルから更新]** ボタンをクリックします。
   [ファイルから更新] ウィンドウが表示されます。



3. まだダウンロードを行っていない場合は、リンクをクリックして最新のプラグインファイルをダウンロードしてから、**[ファイルから更新]** ウィンドウに戻ります。

> リンクから最新のプラグインファイルをダウンロードできるのは、インターネットに接続された PC などのインターネット接続を介した場合のみです。

4. **[参照]** をクリックし、Tenable.ot Customer Portal からダウンロードしたプラグイン設定ファイルに移動します。
5. **[更新]** をクリックします。

IDS エンジンルールセットの更新

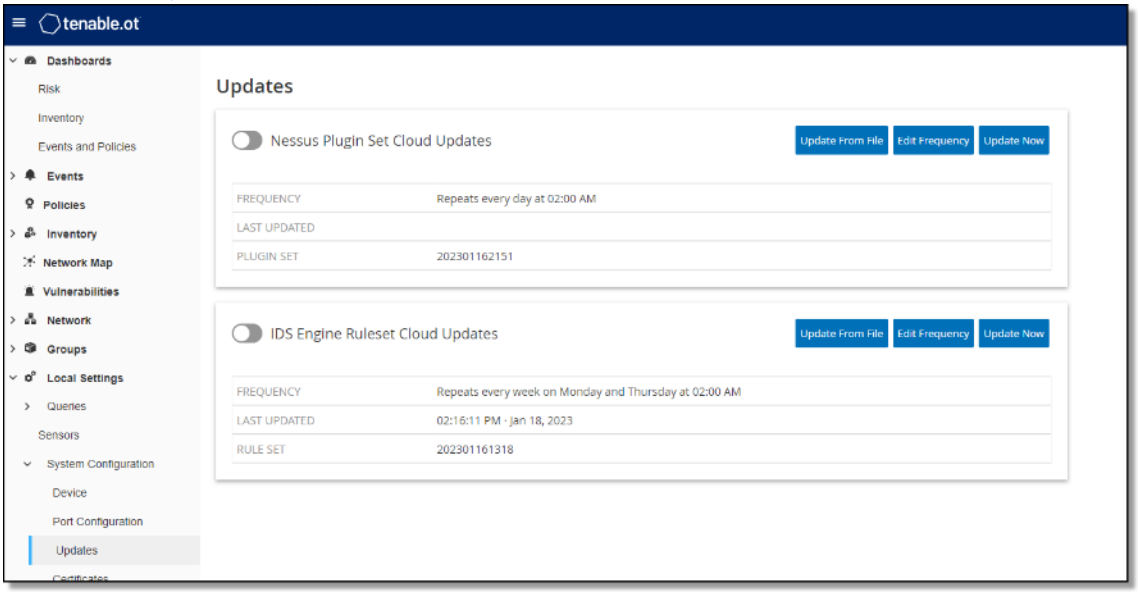
クラウド更新

インターネット接続のあるユーザーは、クラウドを通じて IDS エンジンルールセットを更新できます。自動更新がオンの場合、IDS エンジンルールセットはユーザーが設定した時間と頻度で更新します(デフォルトでは毎週月曜日と火曜日の午前 2 時)。

IDS エンジンルールセットの自動クラウド更新の設定

➡ IDS エンジンルールセットの自動クラウド更新を設定する手順

1. **[ローカル設定]** で、**[システム構成]**>**[更新]** に移動します。
   IDS エンジンルールセットのクラウド更新 で **[更新]** 画面が表示され、ルールセットの番号、最終更新日時、更新スケジュールが表示されます。

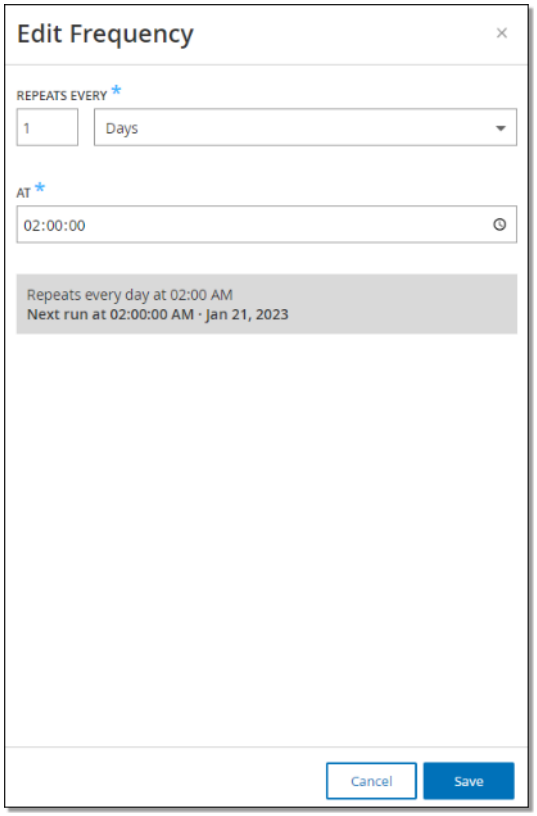


2. トグルスイッチがオンになっていない場合は、クリックして自動更新をオンにします。

➡ IDS エンジンルールセットの自動更新スケジュールを編集する手順

1. **[ローカル設定]** で、**[システム構成]**>**[更新]** に移動します。
   IDS エンジンルールセットのクラウド更新 で **[更新]** 画面が表示され、ルールセットの番号、最終更新日時、更新スケジュールが表示されます。

2. **[頻度の編集]**ボタンをクリックします。
   [頻度の編集]サイドパネルが表示されます。



3. **[繰り返し頻度]**で、数字を入力し、ドロップダウンメニューから時間の単位(日または週)を選択することで、ルールセットを更新する時間間隔を設定します。
4. **[週]**を選択した場合は、ルールセットで週次更新を実行する曜日を選択します。
5. **[時刻]**で、[時計アイコン]をクリックして時間を選択するか手動で時間を入力して、IDS エンジンルールセットを更新する時刻(HH:MM:SS)を設定します。
   [保存]をクリックします。
   頻度の更新が成功したことを通知するダイアログが表示されます。

IDS エンジンルールセットの手動クラウド更新の実行

➡ IDS エンジンルールセットを手動で更新する手順

1. **[ローカル設定]**で、**[システム構成]**>**[更新]**に移動します。
   IDS エンジンルールセットのクラウド更新で**[更新]**画面が表示され、ルールセットの番号、最終更新日時、更新スケジュールが表示されます。
2. **[今すぐ更新]**ボタンをクリックします。
   更新が開始したことを通知するダイアログが表示されます。更新が完了すると、**[ルールセット]**フィールドに現在のルールセットの番号が表示されます。

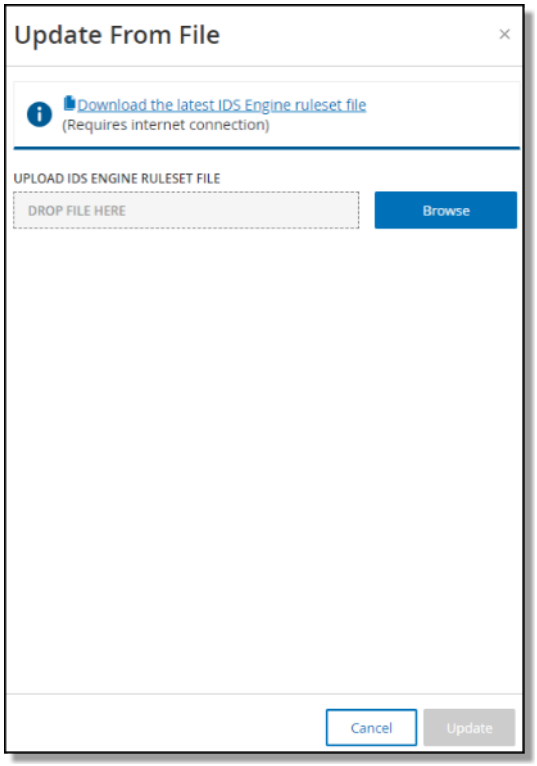
オフライン更新

Tenable.ot デバイスにインターネット接続がないユーザーは、Tenable Customer Portal から最新のルールセットをダウンロードしてそのファイルをアップロードすることで、IDS エンジンルールセットを手動で更新できます。

➡ IDS エンジンルールセットをオフラインで更新する手順

1. **[ローカル設定]**で、**[システム構成]**>**[更新]**>**[IDS エンジンルールセットのクラウド更新]**に移動します。
   [更新]画面が表示され、ルールセットの番号、最終更新日時、更新スケジュールが表示されます。

2. **[ファイルから更新]**ボタンをクリックします。
   [ファイルから更新]ウィンドウが表示されます。



3. まだ最新の IDS エンジンルールセットファイルをダウンロードしていない場合は、リンクをクリックしてダウンロードします。

> リンクから最新の IDS エンジンルールセットファイルをダウンロードできるのは、インターネットに接続された PC などのインターネット接続を介した場合のみです。

4. **[参照]**をクリックし、Tenable.ot Customer Portal からダウンロードした IDS エンジンルールセット設定ファイルに移動します。
5. **[更新]**をクリックします。

証明書

HTTPS 証明書の生成

HTTPS 証明書により、システムが Tenable.ot アプライアンスおよびサーバーへの安全な接続を使用していることが保証されます。最初の証明書は 2 年で有効期限が切れます。新しい自己署名証明書はいつでも生成でき、有効期限は 1 年間です。

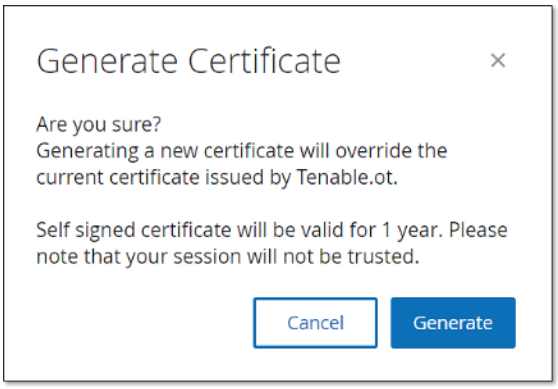
> 新しい証明書を生成すると、現在の証明書は上書きされます。

➡ 自己署名証明書の生成手順

1. **[ローカル設定]**で、**[システム構成]**>**[証明書]**画面に移動します。

2. **[アクション]** ボタンをクリックし、**[自己署名証明書の生成]** を選択します。

[証明書の生成]確認ウィンドウが表示されます。



3. **[生成]** をクリックします。
   自己署名証明書が生成され、**[ローカル設定]**>**[システム構成]**>**[証明書]** 画面で表示できます。

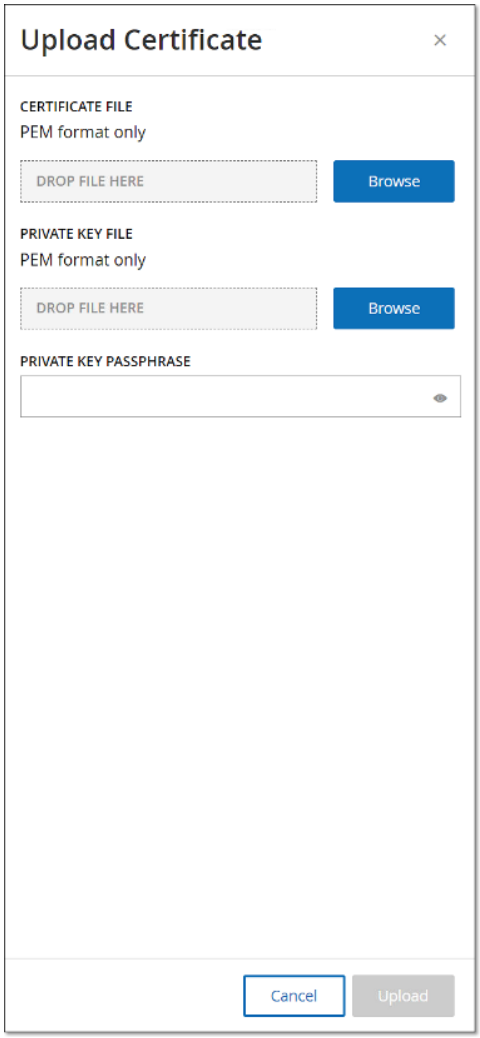
HTTPS 証明書のアップロード

自己署名の HTTPS 証明書の生成に加えて、ユーザーは UI([ローカル設定]>[システム構成]>[証明書])から自分自身の HTTPS 証明書をアップロードできます。証明書は、ICP と IM などの間の他のデバイス(ブラウザを含む)への HTTPS 接続を保護するために使用されます。

➡ HTTPS 証明書のアップロード手順

1. **[ローカル設定]** で、**[システム構成]**>**[証明書]** 画面に移動します。
2. **[アクション]** ボタンをクリックし、**[証明書のアップロード]** を選択します。

[証明書のアップロード]サイドパネルが表示されます。



3. **[証明書ファイル]**で**[参照]**ボタンをクリックし、アップロードする証明書ファイルに移動します。
4. **[秘密鍵ファイル]**で**[参照]**ボタンをクリックし、アップロードする秘密鍵ファイルに移動します。
5. **[秘密鍵のパスフレーズ]**フィールドに秘密鍵のパスフレーズを入力します。
6. **[アップロード]**ボタンをクリックして、ファイルをアップロードします。
   サイドパネルが閉じます。

証明書を置き換えた後、ブラウザタブをリロードして、HTTP 証明書の更新が正常に行われたかどうかを確認することをお勧めします。証明書の更新に失敗した場合、警告通知が表示されます。

ライセンス

場合によっては、Tenable.ot ライセンスを更新または再初期化する必要があります。Tenable アカウントマネージャーに連絡した後、次のいずれかの手順に従って、ライセンスを更新または再初期化する必要があります。

ライセンスの更新

既存のライセンスを更新する必要がある場合 (資産制限を増やす、ライセンス期間を延長する、ライセンスタイプを変更するなど)、次の手順に従ってください。

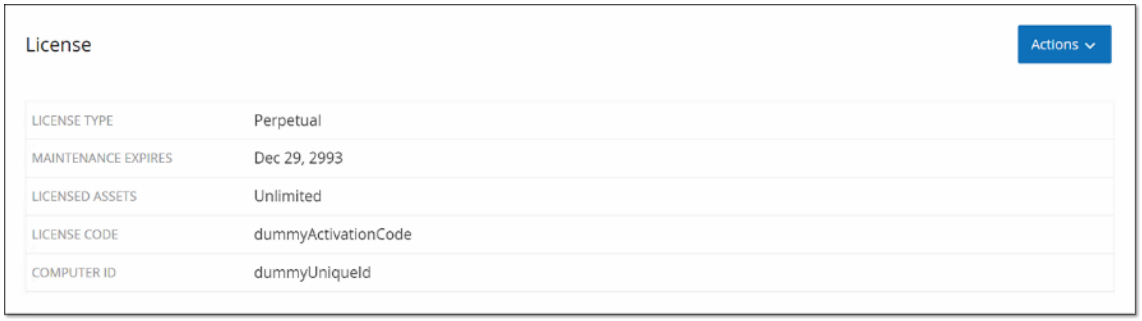
前提条件

- 新しいライセンスの登録前に、Tenable アカウントマネージャーがシステムのライセンス情報を更新しておく必要があります。
- インターネットへのアクセスが必要です。Tenable.ot デバイスがインターネットに接続されていない場合は、任意の PC からライセンスを登録できます。

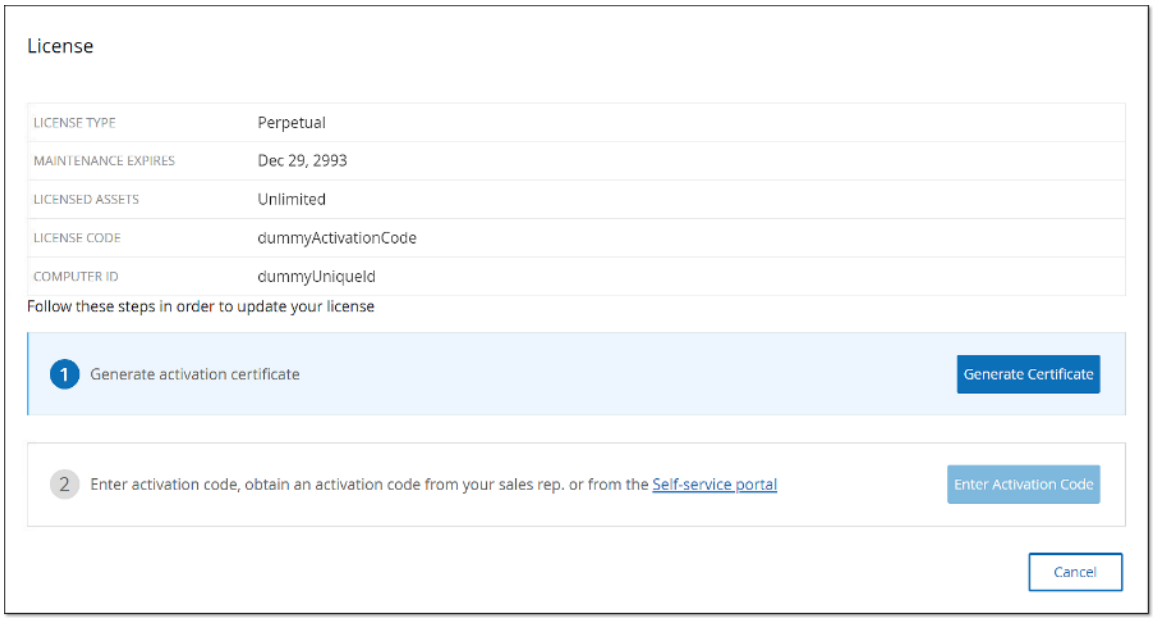
新しいライセンスの登録

➡ ライセンスの登録手順

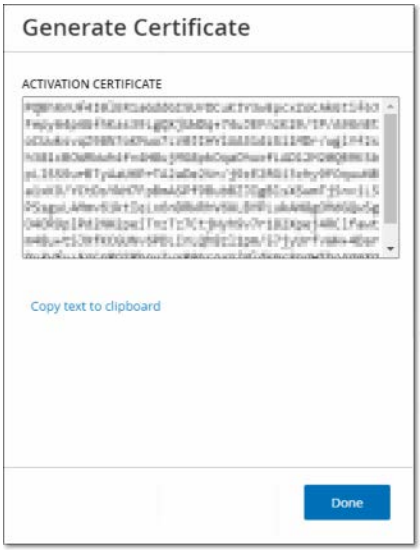
1. **[ローカル設定]** で、**[システム構成]**>**[ライセンス]** に移動します。
   [ライセンス] 画面が表示されます。



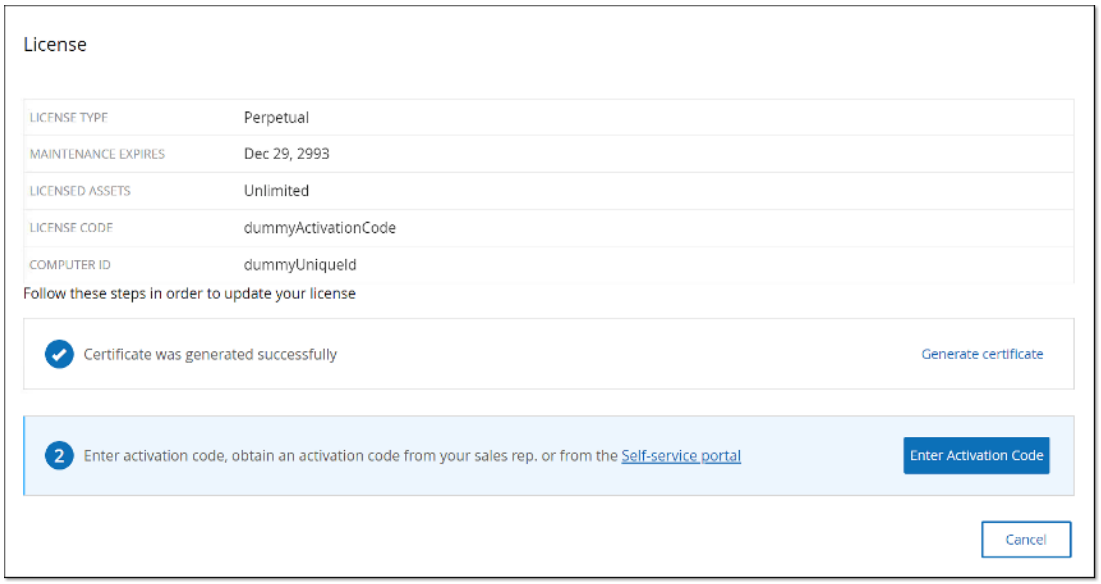
2. **[アクション]** ボタンをクリックし、**[ライセンスの更新]** を選択します。
   [証明書の生成] および **[アクティベーションコードの入力]** のステップが表示されます。



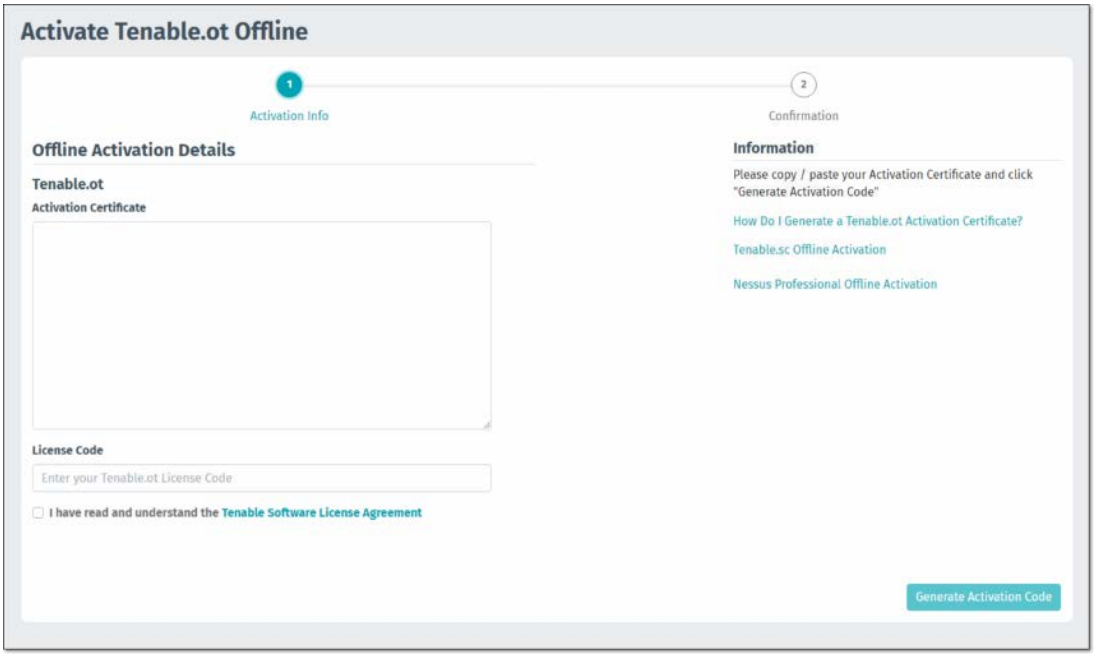
3. **[(1) アクティベーション証明書の生成]** フィールドで、**[証明書の生成]** ボタンをクリックします。
   [証明書の生成] サイドパネルがアクティベーション証明書とともに表示されます。



4. **[テキストをクリップボードにコピー]** ボタンをクリックし、**[完了]** をクリックします。
   サイドパネルが閉じます。
5. **[(2) アクティベーションコードの入力]** フィールドで、セルフサービスポータルのリンクをクリックします。



[Tenable.ot をオフラインでアクティブ化] 画面が新しいタブで開きます。



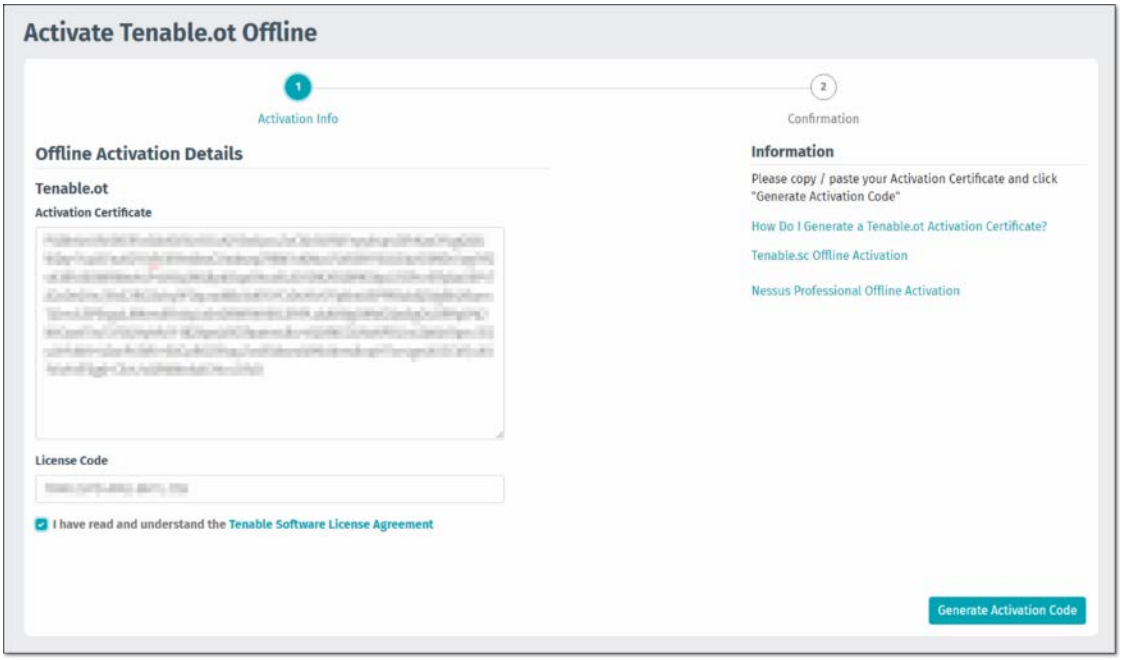
URL https://provisioning.tenable.com/activate/offline/tenable-ot を使用して、インターネットに接続されたデバイスから [Tenable.ot をオフラインでアクティブ化] 画面にアクセスする必要があります。

現在 tenable.com にログインしていない場合は、メールアドレスとパスワードを使用してログインする必要があります。ログインにはライセンスコードを受け取ったメールアカウントを使用する必要があります。

ログイン認証情報がない場合は、**[パスワードを忘れた場合]** をクリックし、プロンプトに従うか、Tenable アカウントマネージャーに連絡してください。

6. **[アクティベーション証明書]** フィールドに、アクティベーション証明書を入力します。
7. **[ライセンスコード]** フィールドに、20 文字の**ライセンスコード**を入力します (**[ライセンス]** 画面からコピーして貼り付けることができます)。

8. **[Tenable ソフトウェアライセンス契約を読み、理解しました]**チェックボックスをクリックします。

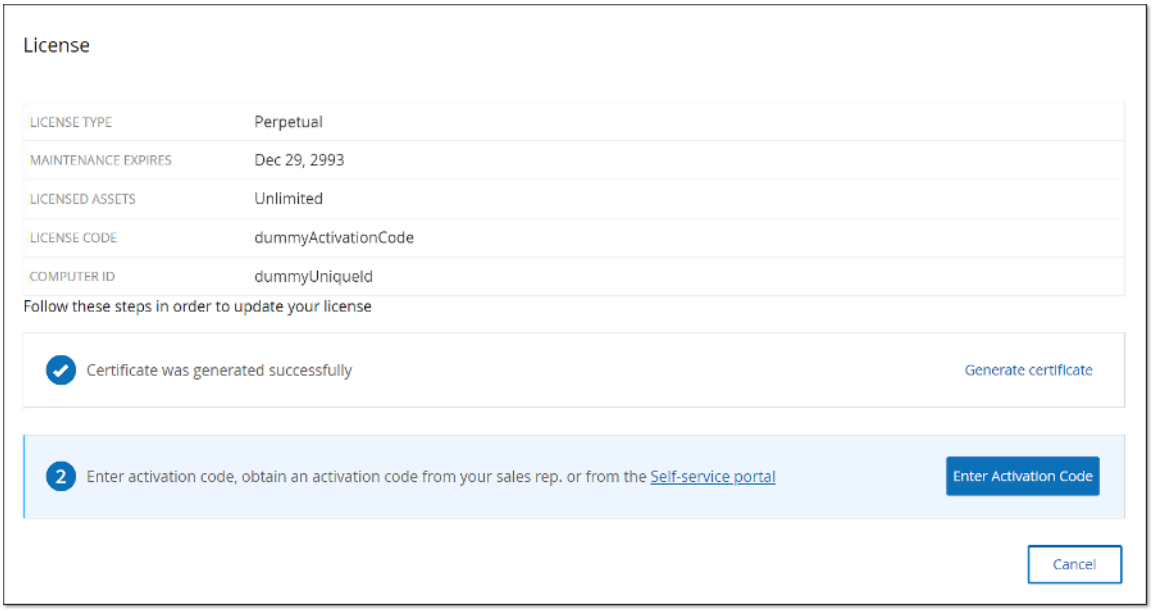


ライセンス契約を表示するには、**[Tenable ソフトウェアライセンス契約]**のリンクをクリックしてください。

9. **[アクティベーションコードの生成]**ボタンをクリックします。
[オフラインアクティベーションコードが正常に作成されました!]画面が表示されます。

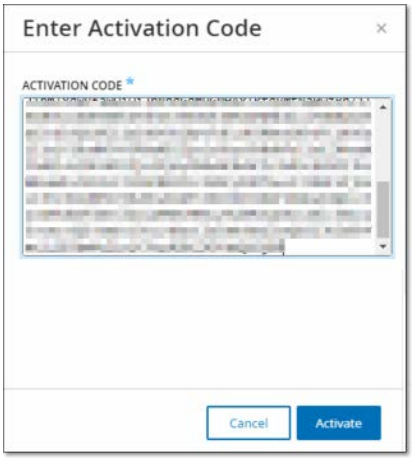
10. **[テキストをクリップボードにコピー]**をクリックします。

11. **[ライセンス]**タブに戻り、**[アクティベーションコードの入力]**ボタンをクリックします。



[アクティベーションコードの入力]サイドパネルが表示されます。

12. **[アクティベーションコード]**フィールドにアクティベーションコードを貼り付け、**[アクティブ化]**ボタンをクリックします。



サイドパネルが閉じ、ライセンスが更新されます。

ライセンスの再初期化

ライセンスを再初期化すると、システム起動時のライセンスアクティベーションと同様に、システムから現在のライセンスが削除され、新しいライセンスがアクティブ化されます。ライセンスを再初期化する必要がある場合(新しいライセンスが発行された場合)は、次の手順を実行します。

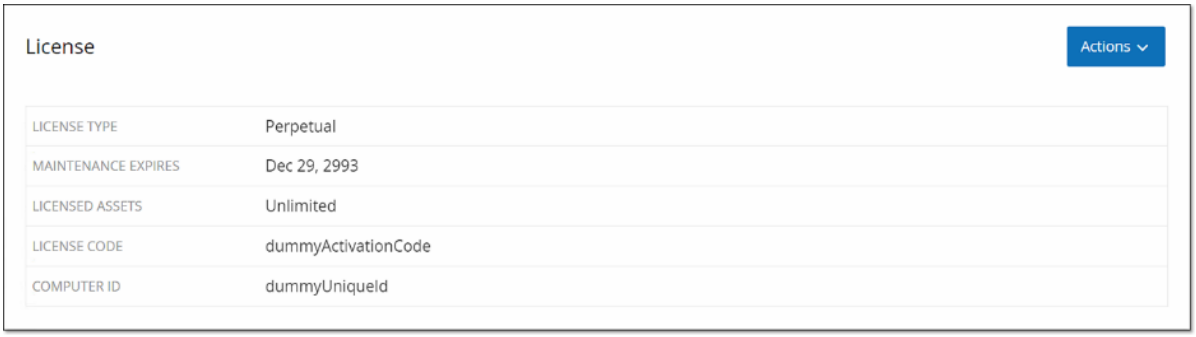
前提条件

- Tenable アカウントマネージャーが、システムで新しいライセンスをすでに発行し、ライセンスコード(20 文字の文字 / 数字)を提供している必要があります。
- インターネットへのアクセスが必要です。Tenable.ot デバイスがインターネットに接続されていない場合は、任意の PC からライセンスを登録できます。

ライセンスの再初期化

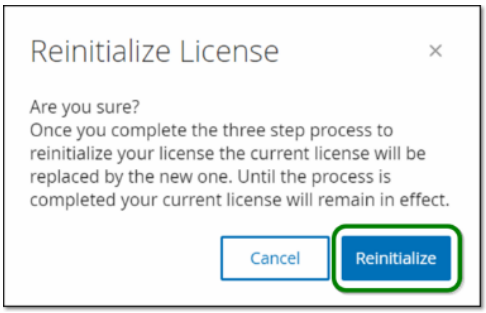
ライセンスの再初期化手順

1. **[ローカル設定]**で、**[システム構成]**>**[ライセンス]**に移動します。

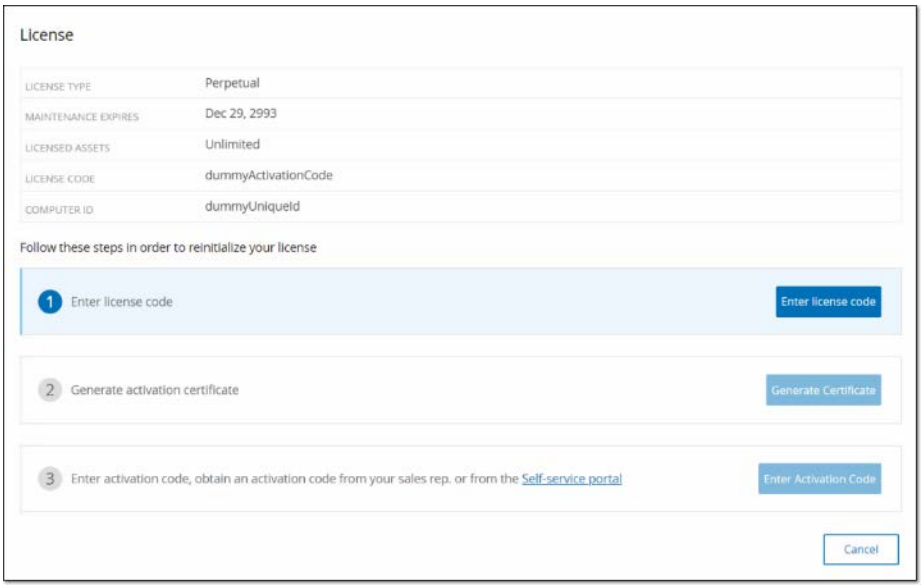


[アクション]ボタンをクリックし、**[ライセンスの再初期化]**を選択します。
確認ウィンドウが表示されます。

2. **[再初期化]**をクリックします。



[ライセンス]画面に 3 つの再初期化ステップが表示されます。



3. システム起動手順に従って、ライセンスをアクティブ化します。**ライセンスのアクティベーション**を参照してください。
アクティベーションコードを入力すると、現在のライセンスは新しいライセンスに置き換えられます。

ライセンスの計算

Tenable アカウントのライセンスは、システム内の一意の IP の数に基づいて計算されます。IP ごとに個別のライセンスが必要です。したがって、複数のデバイスが同じ複数の IP を共有する場合(例: 同じ 3 つの IP を共有する同じバックプレーンに接続された複数のデバイス)でも、デバイスの数に関係なく、ライセンスは IP の数(この場合は 3 つのライセンス)に基づきます。

環境構成

資産設定

資産を手動で追加

Tenable.ot でまだ検出されていないとしても、インベントリを追跡しやすくするために、所有している追加の資産を表示したほうが良いこともあります。その場合は、CSV ファイルをダウンロードして編集し、ファイルをシステムにアップロードすることで、これらの資産をインベントリに手動で追加できます。

ユーザーがアップロードできるのは、システムの既存の資産によってまだ使用されていない IP を持つ資産のみです。同じ IP でネットワークを介して通信している資産をシステムが検出した場合、システムは検出された資産について取得した情報を使用し、以前にアップロードした情報を上書きします。ネットワークで資産が通信していることをシステムが検出すると、システムは資産を通常のものとして処理し始めます。

アップロードされた資産の IP アドレスは、システムライセンスの一部としてカウントされます。

アップロードされた資産は、システムによって検出されるまで、リスクスコア 0 を表示します。

> 資産を手動で追加した場合、Tenable.ot がネットワークでの資産の通信を検出するまで、これらの資産のイベントは検出されません。

➡ 資産を手動で追加する手順

1. **[ローカル設定]** で、**[環境構成]**>**[資産設定]** に移動します。
   [資産設定] 画面が表示されます。
2. **[資産を手動で追加]** で、**[アクション]** ボタンをクリックし、**[CSV テンプレートのダウンロード]** を選択します。
3. tot_Assets テンプレートドキュメントがダウンロードされます。
4. tot_Assets テンプレートドキュメントを開きます。
5. ファイルにある指示に従って tot_Assets テンプレートを正確に編集し、列ヘッダー(名前、タイプなど)と入力した値のみを残します。
6. 編集したファイルを保存します。
7. **[資産設定]** 画面に戻ります。
8. **[アクション]** ボタンをクリックし、**[CSV をアップロード]** を選択し、目的の CSV ファイルに移動して開き、アップロードします。
9. **[資産を手動で追加]** で、**[レポートのダウンロード]** をクリックします。
   レポートを含む CSV ファイルが表示され、[結果]列に成功と失敗が示されます。エラーの詳細は、[エラー]列に表示されます。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Name	Type	Criticality	IPs	MAC	Family	Model	Firmware	OS	Purdue Le	Location	Descriptic	Result	Error
2	AAA	Plc	HighCritic	10.100.20.	aa:bb:cc:d	Siemens	S7300	2.3.1		Level1	Italy	Siemens,	Failure	IP 10.100.20.21 already exists
3	BBB	Server	MediumC	10.200.30.30		VMware			Windows Server 2012				Success	
4	CCC	Switch			AA:bb:cd:	Catalyst	C2960	12.3		Level3			Success	
5	DDDD	Unknown	NoneCriticality						Linux	Level4	Israel		Success	

イベントクラスター

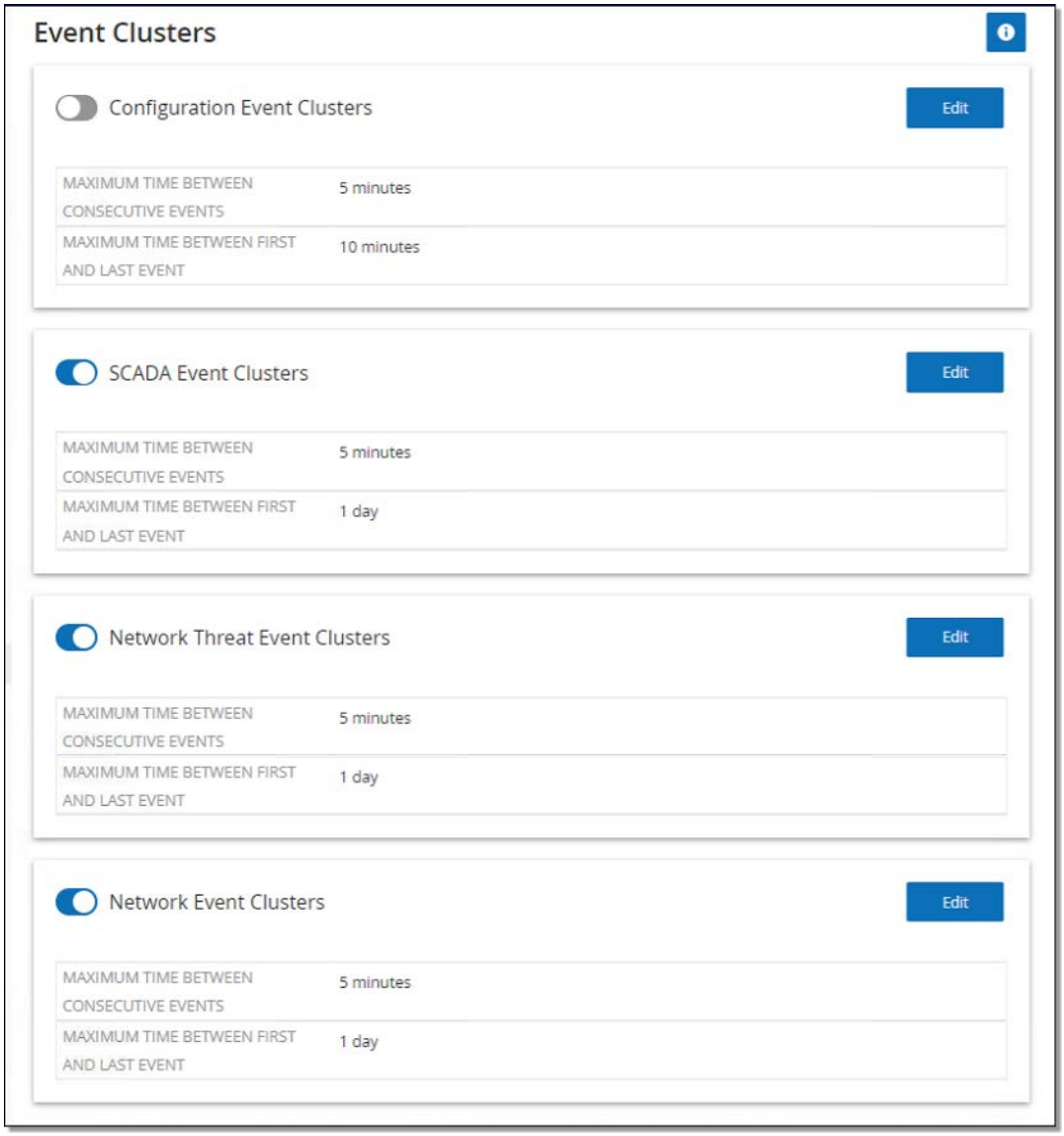
イベントの監視を容易にするために、同じ特性を持つ複数のイベントが、1 つにクラスター化されます。クラスタリングは、イベントタイプ(同じポリシーを共有するなど)、ソース資産とデスティネーション資産などに基づいて行われます。

イベントをクラスター化するには、次の構成された時間間隔内にイベントを生成する必要があります。

- **連続するイベント間の最大時間** - イベント間の最大時間間隔を設定します。この時間が経過すると、連続するイベントはクラスター化されません。
- **最初と最後のイベント間の最大時間** - すべてのイベントがクラスターとして表示される最大時間間隔を設定します。この時間間隔の後に生成されるイベントは、クラスターには含まれません。

クラスタリングの有効手順

1. **[ローカル設定]** で、**[環境構成]** > **[イベントクラスター]** に移動します。
   [イベントクラスター] 画面が表示されます。

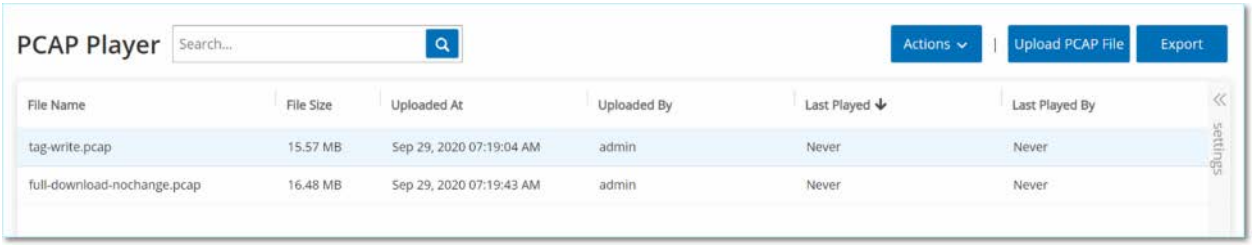


2. トグルをクリックして、クラスタリングに必要なカテゴリを有効にします。
3. カテゴリの時間間隔を構成するには、**[編集]** ボタンをクリックします。
   [構成の編集] ウィンドウが表示されます。
4. 数値フィールドに目的の数値を入力し、ドロップダウンリストを使用して時間の単位を調整します。

> クラスタリングおよび時間間隔の詳細については、ボタンをクリックしてください。

5. **[保存]** をクリックします。

PCAP プレーヤー



Tenable.ot では、記録されたネットワークアクティビティを含む PCAP ファイルをアップロードし、Tenable.ot で「再生」することができます。PCAP ファイルを「再生」すると、Tenable.ot はネットワークトラフィックを監視し、まるでネットワーク内でトラフィックが発生したかのように、検出された資産、ネットワークアクティビティ、脆弱性に関するすべての情報を記録します。この機能は、シミュレーションの目的で使用したり、ネットワークの外部(リモートプラントなど)で発生する Tenable.ot 展開によって監視されているトラフィックを分析したりするために使用できます。

この機能でサポートされているファイルタイプは、.pcap、.pcapng、.pcap.gz、.pcapng.gz です。Tenable.ot またはその他のネットワーク監視ツールのインスタンスによって記録されたファイルを使用できます。

PCAP ファイルのアップロード

PCAP ファイルのアップロード手順

1. **[ローカル設定]** で、**[環境構成]**>**[PCAP プレーヤー]** に移動します。
2. **[PCAP ファイルのアップロード]** をクリックします。
   ファイルエクスプローラーが開きます。
3. 目的の PCAP 記録を選択します。
4. **[開く]** をクリックします。
   PCAP ファイルがシステムにアップロードされます。

PCAP ファイルの再生

PCPAP ファイルの再生手順

1. **[ローカル設定]** で、**[環境構成]**>**[PCAP プレーヤー]** に移動します。
2. 再生する PCAP 記録を選択します。
3. **[アクション]**>**[再生]** をクリックします。
4. **[PCAP の再生]** ウィザードが表示されます。
5. **[再生速度]** フィールドで、システムがファイルを再生する速度をドロップダウンリストから選択します。オプションは、*1X*、*2X*、*4X*、*8X*、*16X* です。

   PCAP ファイルを再生するとデータがシステムに挿入されます。実行されると、この操作を元に戻したり停止することはできません。

6. **[再生]** をクリックします。
   PCAP ファイルがシステムで「再生」されます。PCAP ファイルのすべてのネットワークアクティビティがシステムに登録され、システムによって識別された資産が資産インベントリに追加されます。

ファイルの再生中は、別の PCAP ファイルを再生できません。

ユーザーとロール

Tenable.ot コンソール(UI)へのアクセスは、そのユーザーが利用できる権限を指定するユーザーアカウントによって制御されます。ユーザーの権限は、ユーザーが割り当てられているユーザーグループによって決定されます。各ユーザーグループには、そのメンバーが利用できる一連の権限を定義するロールが割り当てられます。したがって、たとえば、*サイトオペレーター*ユーザーグループに *サイトオペレーター*のロールがある場合、そのグループに割り当てられているすべてのユーザーに *サイトオペレーター*ロールに関連付けられた一連の権限が付与されます。

システムには、利用可能な各ロール(*管理者*ユーザーグループ > *管理者*ロール、*サイトオペレーター*ユーザーグループ > *サイトオペレーター*ロールなど)に対応する一連の事前定義されたユーザーグループが用意されています。カスタムユーザーグループを作成して、メンバーのロールを指定することもできます。

システムでユーザーを作成するには、3 つの方法があります。

- **ローカルユーザーの追加** - ユーザーアカウントを作成して、個々のユーザーがシステムにアクセスすることを承認します。ロールを定義するユーザーグループにユーザーを割り当てます。
- **認証サーバー** - 所属組織の認証サーバー(Active Directory、LDAP など)を使用して、ユーザーがシステムにアクセスすることを承認します。Active Directory の既存のグループに基づいて、Tenable.ot ロールを割り当てることができます。
- **SAML** - ID プロバイダー(Azure Active Directory など)との統合をセットアップし、ユーザーを Tenable.ot アプリケーションに割り当てます。

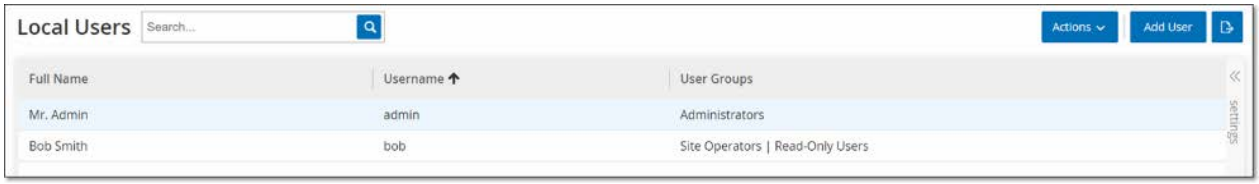
ローカルユーザー

管理者ユーザーは、新しいユーザーアカウントを作成したり既存のアカウントを編集したりできます。各ユーザーは、ユーザーに割り当てられたロールを決定する 1 つ以上のユーザーグループに割り当てられます。

ユーザーのアカウントまたはユーザーグループの作成 / 編集中でも、ユーザーをユーザーグループに追加できます。

ローカルユーザーの表示

[ローカルユーザー]画面に、システム内のすべてのローカルユーザーのリストが表示されます。



この画面に表示される情報について、次の表で説明します。

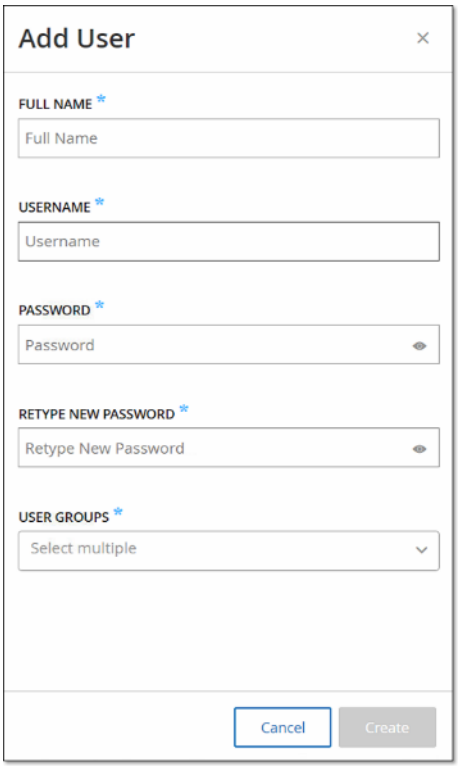
パラメーター	説明
フルネーム	ユーザーのフルネーム。
ユーザー名	ログインに使用されるユーザーのユーザー名。
ユーザーグループ	ユーザーが割り当てられているユーザーグループ。

ローカルユーザーの追加

ユーザーアカウントを作成して、個々のユーザーがシステムにアクセスすることを承認します。各ユーザーは、1つ以上のユーザーグループに割り当てられる必要があります。

➡ ユーザーアカウントの作成手順

1. **[ローカル設定]**で、**[ユーザー管理]**>**[ローカルユーザー]**画面に移動します。
2. **[ユーザーの追加]**ボタンをクリックします。
   [ユーザーの追加]ペインが表示されます。



3. **[フルネーム]**フィールドで、姓名を入力します。

> 入力した名前は、ユーザーのサインイン時にヘッダーバーに表示されます。

4. **[ユーザー名]**フィールドに、システムへのログインに使用するユーザー名を入力します。
5. **[パスワード]**フィールドに、パスワードを入力します。
6. **[パスワードの再入力]**フィールドに、同じパスワードを入力します。

> これは、ユーザーが最初のログインに使用するパスワードです。ユーザーは、システムにログインした後に**[設定]**画面でパスワードを変更できます。

7. **[ユーザーグループ]** フィールドをクリックし、このユーザーを割り当てる各ユーザーグループのチェックボックスを選択します。

> システムには、利用可能な各ロール (*管理者*ユーザーグループ > *管理者*ロール、*サイトオペレーター*ユーザーグループ > *サイトオペレーター*ロールなど) に対応する一連の事前定義されたユーザーグループが用意されています。利用可能なロールの説明については、**ユーザーロール**を参照してください。

8. **[作成]** をクリックします。
新しいユーザーアカウントがシステムで作成され、**[ローカルユーザー]** タブに表示されるユーザーのリストに追加されます。

ユーザーアカウントに関するその他のアクション

ユーザーアカウントの編集

ユーザーをさらに別のユーザーグループに割り当てたり、グループからユーザーを削除したりできます。

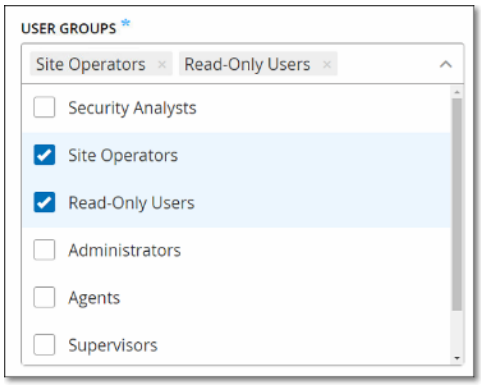
➡ ユーザーのユーザーグループの変更手順

1. **[ローカル設定]** で、**[ユーザー管理]** > **[ローカルユーザー]** 画面に移動します。
[ローカルユーザー] 画面が表示されます。
2. 目的のユーザーを右クリックし、メニューから **[ユーザーの編集]** を選択します。

> または、ユーザーを選択して、**[アクション]** ボタン > **[ユーザーの編集]** をクリックすることもできます。

3. **[ユーザーの編集]** ペインが表示され、ユーザーが割り当てられているユーザーグループが示されます。

4. **[ユーザーグループ]** フィールドをクリックします。
ユーザーグループのリストが表示されます。



5. 目的のユーザーグループを選択 / 選択解除します。
6. **[保存]** をクリックします。

ユーザーのパスワードの変更

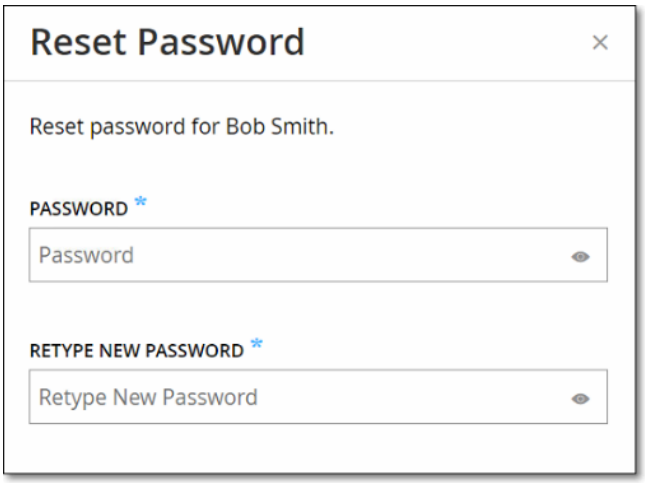
以下は、管理者ユーザーがシステムの任意のアカウントのパスワードを変更する際に使用する手順です。ユーザーが自身のパスワードを変更する場合は、**[ローカル設定]** > **[ユーザー]** に移動して変更できます。

ユーザーのパスワードの変更手順

1. **[ローカル設定]** で、**[ユーザー管理]** > **[ローカルユーザー]** 画面に移動します。
   [ローカルユーザー] 画面が表示されます。
2. 目的のユーザーを右クリックし、メニューから **[パスワードのリセット]** を選択します。

   または、ユーザーを選択して、**[アクション]** ボタン > **[パスワードのリセット]** をクリックすることもできます。

   [パスワードのリセット] ウィンドウが表示されます。



3. **[新しいパスワード]** フィールドに、新しいパスワードを入力します。
4. **[新しいパスワードの再入力]** フィールドに、新しいパスワードを再入力します。
5. **[リセット]** をクリックします。
   新しいパスワードが、指定されたユーザーアカウントに適用されます。

ローカルユーザーの削除

ユーザーアカウントの削除手順

1. **[ローカル設定]** で、**[ユーザー管理]** > **[ローカルユーザー]** 画面に移動します。
   [ローカルユーザー] 画面が表示されます。
2. 目的のユーザーを右クリックし、メニューから **[ユーザーの削除]** を選択します。

   または、ユーザーを選択して、**[アクション]** ボタン > **[ユーザーの削除]** をクリックすることもできます。

   確認ウィンドウが表示されます。
3. **[削除]** をクリックします。
   ユーザーアカウントがシステムから削除されます。

ユーザーグループ

管理者ユーザーは、新しいユーザーグループを作成したり、既存のグループを編集したりできます。各ユーザーは、ユーザーに割り当てられたロールを決定する1つ以上のユーザーグループに割り当てられます。

システムには、利用可能な各ロール(*管理者*ユーザーグループ > *管理者*ロール、*サイトオペレーター*ユーザーグループ > *サイトオペレーター*ロールなど)に対応する一連の事前定義されたユーザーグループが用意されています。利用可能なロールの説明については、**ユーザーロール**を参照してください。

ユーザーグループの表示

[ユーザーグループ]画面に、システム内のすべてのユーザーグループのリストが表示されます。

この画面に表示される情報について、次の表で説明します。

パラメーター	説明
名前	ユーザーグループの名前。
メンバー	グループに割り当てられたすべてのメンバーのリスト。
ロール	このグループに与えられるロール。各ロールに関連付けられているアクセス許可の説明については、**ユーザーロールテーブル**を参照してください。

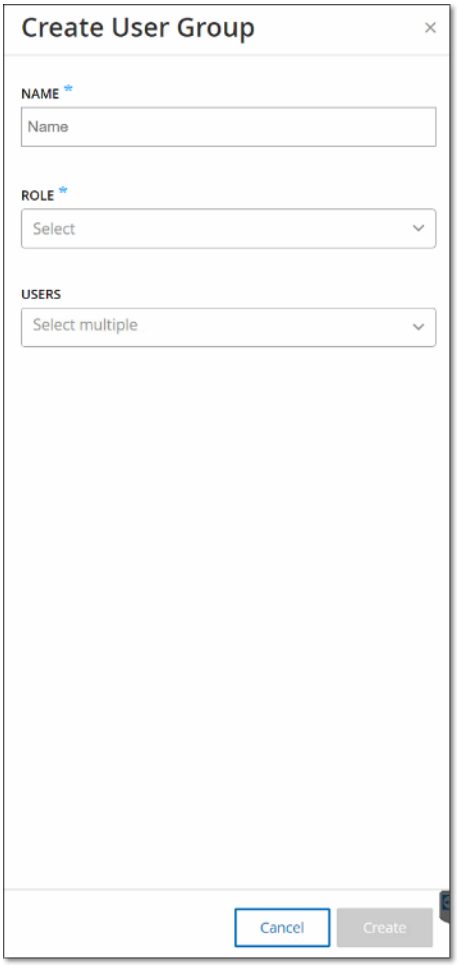
ユーザーグループの追加

新しいユーザーグループを作成し、そのグループにユーザーを割り当てることができます。

➡ ユーザーアカウントの作成手順

1. **[ローカル設定]**で、**[ユーザー管理]**>**[ユーザーグループ]**画面に移動します。
   [ユーザーグループ]画面が表示されます。

2. **[ユーザーグループの作成]**ボタンをクリックします。
   [ユーザーグループの作成]ペインが表示されます。



3. **[名前]**フィールドに、グループの名前を入力します。
4. **[ロール]**フィールドで、このグループに割り当てるロールをドロップダウンリストから選択します。
5. **[ユーザー]**フィールドで、このグループに割り当てる1人以上のユーザーをドロップダウンリストから選択します。
6. **[作成]**をクリックします。
   新しいユーザーグループがシステムで作成され、**[ユーザーグループ]**画面に表示されるグループのリストに追加されます。

ユーザーグループに関するその他のアクション

ユーザーグループの編集

グループを編集することで、設定を編集し、既存のユーザーグループにメンバーを追加したり、削除したりできます。

> または、ユーザーを選択して、**[アクション]** ボタン > **[ユーザーの削除]** をクリックすることもできます。

➡ ユーザーグループの編集手順

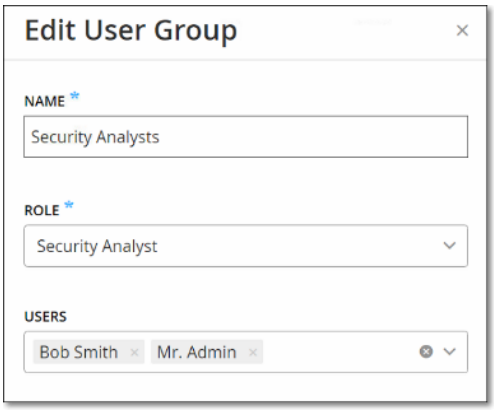
1. [ローカル設定] で、[ユーザー管理] > [ユーザーグループ] 画面に移動します。
   [ユーザーグループ] 画面が表示されます。

2. 目的のユーザーを右クリックし、メニューから［**ユーザーグループの編集**］を選択します。

> または、ユーザーを選択して、［**アクション**］ボタン > ［**ユーザーグループの編集**］をクリックすることもできます。

3. ［**ユーザーグループの編集**］ペインが表示され、グループの設定が表示されます。

4. **名前**と**ロール**を変更できます。**ユーザー**を選択 / 選択解除して、ユーザーをグループに追加 / 削除することもできます。



5. **[保存]** をクリックします。

ユーザーグループの削除

> 削除できるのは、現在ユーザーが誰も割り当てられていないユーザーグループのみです。ユーザーがグループに割り当てられている場合は、グループを削除する前に、まずユーザーをグループから削除する必要があります。

➡ ユーザーグループの削除手順

1. **[ローカル設定]** で、**[ユーザー管理]** > **[ユーザーグループ]** 画面に移動します。
   [ユーザーグループ] 画面が表示されます。

2. 目的のユーザーグループを右クリックし、メニューから［**ユーザーグループの削除**］を選択します。
   確認ウィンドウが表示されます。

> または、ユーザーを選択して、［**アクション**］ボタン > ［**ユーザーグループの削除**］をクリックすることもできます。

3. **[削除]** をクリックします。
   ユーザーグループがシステムから削除されます。

ユーザーロール

以下は、利用可能なロールの簡単な説明です。

- **管理者** - システムのすべての操作タスクおよび管理タスク(新しいユーザーアカウントの作成を含む)を行うための最大の権限を持ちます。
- **読み取り専用** - データ(資産インベントリ、イベント、ネットワークトラフィック)の表示はできますが、システム内のアクションの実行はできません。
- **セキュリティアナリスト** - システム内のデータの表示およびセキュリティイベントの解決ができます。
- **セキュリティマネージャー** - セキュリティ関連の機能の管理(ポリシーの構成、システム内のデータの表示、イベントの解決を含む)ができます。
- **サイトオペレーター** - システム内のデータの表示および資産インベントリの管理ができます。
- **スーパーバイザー** - システムのすべての操作タスクおよび限定された一部の管理タスク(新しいユーザーの作成や他の機密性の高いアクティビティを除く)を行うためのすべての権限を持ちます。

ユーザーロールテーブル

次の表は、各ロールで有効になっている権限の詳細な内訳を示しています。

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
イベント							
イベントを表示	✓	✓	✓	✓	✓	✓	✓
解決	✓	✓	✓	✓	✓	X	X
キャプチャファイルのダウンロード	✓	✓	✓	✓	✓	✓	✓
ポリシーから除外	✓	✓	✓	✓	X	X	X
すべて解決	✓	✓	✓	✓	✓	X	X
エクスポート	✓	✓	✓	✓	✓	✓	✓
FortiGate でのポリシーの作成	✓	✓	✓	✓	X	X	X
更新	✓	✓	✓	✓	✓	✓	✓
ポリシー							
ポリシーの表示	✓	✓	✓	✓	✓	✓	✓
有効化 / 無効化	✓	✓	✓	✓	X	X	X
アクションの表示	✓	✓	✓	✓	✓	✓	✓
編集	✓	✓	✓	✓	X	X	X

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
複製	✓	✓	✓	✓	X	X	X
削除	✓	✓	✓	✓	X	X	X
ポリシーの作成	✓	✓	✓	✓	X	X	X
エクスポート	✓	✓	✓	✓	✓	✓	✓
資産							
資産の表示	✓	✓	✓	✓	✓	✓	✓
アクションの表示	✓	✓	✓	✓	✓	✓	✓
編集	✓	✓	✓	X	X	✓	X
削除	✓	✓	✓	X	X	✓	X
インポート(csvで新しい資産をアップロード)	✓	✓	✓	X	X	✓	X
非表示	✓	✓	✓	X	X	✓	X
エクスポート	✓	✓	✓	✓	✓	✓	✓
再同期	✓	✓	✓	✓	✓	✓	X
Nessus スキャン	✓	✓	✓	✓	✓	✓	X
スナップショットの作成(単一の資産)	✓	✓	✓	✓	✓	✓	X
開いているポートの更新(単一の資産)	✓	✓	✓	✓	✓	X	X
ポート状態の更新(単一の資産)	✓	✓	✓	✓	✓	X	X
ブラウザで表示(単一の資産)	✓	✓	✓	✓	✓	✓	✓

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
メイン資産マップで表示(単一の資産)	✓	✓	✓	✓	✓	✓	✓
攻撃経路の生成(単一の資産)	✓	✓	✓	✓	✓	✓	✓
脆弱性(プラグイン)							
プラグインヒットの表示	✓	✓	✓	✓	✓	✓	✓
アクションの表示	✓	✓	✓	✓	✓	✓	✓
コメントの編集	✓	✓	✓	✓	✓	X	X
プラグインセットの更新	✓	✓	✓	✓	X	X	X
エクスポート	✓	✓	✓	✓	✓	✓	✓
ネットワーク							
パケットキャプチャをオンにする	✓	✓	✓	X	X	X	X
進行中のキャプチャを閉じる	✓	✓	✓	✓	✓	✓	X
PCAP ファイルのダウンロード	✓	✓	✓	✓	✓	✓	✓
会話テーブルのエクスポート	✓	✓	✓	✓	✓	✓	✓
ベースラインとして設定	✓	✓	✓	✓	X	X	X
マップの生成	✓	✓	✓	✓	✓	✓	✓
マップの更新	✓	✓	✓	✓	✓	✓	✓
グループ							
グループの表示	✓	✓	✓	✓	✓	✓	✓
アクションの表示	✓	✓	✓	✓	✓	✓	✓

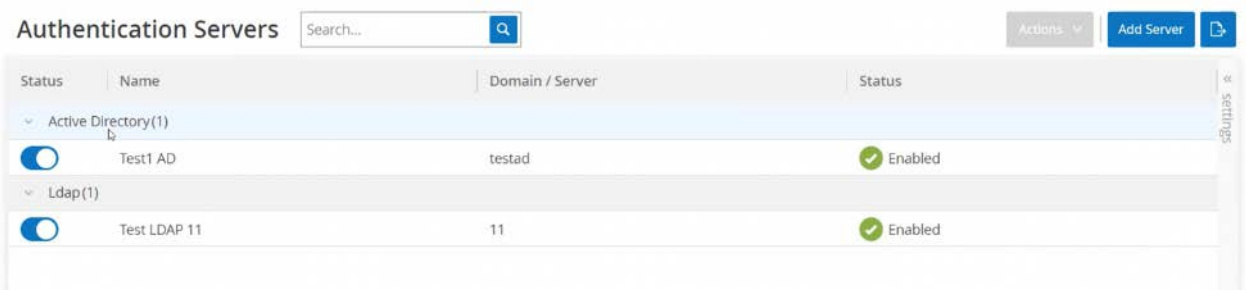
アクセス許可	管理者 (ローカル)	管理者 (外部 / AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
編集	✓	✓	✓	✓	X	X	X
複製	✓	✓	✓	✓	X	X	X
削除	✓	✓	✓	✓	X	X	X
グループの作成	✓	✓	✓	✓	X	X	X
エクスポート	✓	✓	✓	✓	✓	✓	✓
レポート							
レポートの表示	✓	✓	✓	✓	✓	✓	✓
生成	✓	✓	✓	✓	✓	✓	✓
ダウンロード	✓	✓	✓	✓	✓	✓	✓
エクスポート	✓	✓	✓	✓	✓	✓	✓
ネットワークセグメント							
ネットワークセグメントの表示	✓	✓	✓	✓	✓	✓	✓
編集	✓	✓	✓	✓	X	X	X
削除	✓	✓	✓	✓	X	X	X
作成	✓	✓	✓	✓	X	X	X
エクスポート	✓	✓	✓	✓	✓	✓	✓
詳細情報	✓	✓	✓	✓	✓	✓	✓
ローカル設定							
クエリ	✓	✓	✓	X	X	X	X
システム構成 - デバイスの詳細	✓	✓	✓	X	X	X	X

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
システム構成 - センサー	✓	✓	(アクションなし)	(アクションなし)	(アクションなし)	(アクションなし)	(アクションなし)
システム構成 - ポート構成	✓	✓	✓	X	X	X	X
システム構成 - 更新	✓	✓	✓	X	X	X	X
システム構成 - 証明書(HTTPS)	✓	✓	X	X	X	X	X
システム構成 - API キー	✓	X	✓(ローカルユーザーのみ)	✓(ローカルユーザーのみ)	✓(ローカルユーザーのみ)	✓(ローカルユーザーのみ)	✓(ローカルユーザーのみ)
システム構成 - ライセンス	✓	✓	X	X	X	X	X
環境構成 - 資産設定	✓	✓	✓	X	X	X	X
環境構成 - 非表示の資産	✓	✓	✓	✔ - 復元なし	✔ - 復元なし	✓	✔ - 復元なし
環境構成 - カスタムフィールド	✓	✓	✓	X	X	X	X
環境構成 - イベントクラスター	✓	✓	✓	X	X	X	X
環境構成 - PCAP プレーヤー	✓	✓	✓	X	X	X	X
ユーザーとロール - ユーザー設定	✓	✓	✓	X	X	X	X
ユーザーとロール - ローカルユーザー	✓	X	X	X	X	X	X
ユーザーとロール - ユーザーグループ	✓	X	X	X	X	X	X
ユーザーとロール - Active Directory	✓	X	X	X	X	X	X
統合	✓	✓	X	X	X	X	X

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
サーバー	✓	✓	✓	(アクションなし)	(アクションなし)	(アクションなし)	(アクションなし)
システムアクション	✓	✔ - 出荷時設定へのリセットなし	✔ - バックアップと診断のみ	✔ - 診断のみ	X	X	X
システムログ	✓	✓	✓	✓	✓	✓	✔ - syslog なし
有効化(セットアップ時および無効化後)	✓	✓	X	X	X	X	X
資産を削除	✓	✓	✓	X	X	X	X

認証サーバー

認証サーバー画面には、認証サーバーとの既存の統合が表示されます。**[サーバーの追加]**ボタンをクリックして、サーバーを追加できます。



Active Directory

Tenable.ot を所属組織の Active Directory と統合できます。これにより、ユーザーは自分の Active Directory 認証情報を使用してシステムにログインできるようになります。構成には、統合のセットアップと、AD のグループの Tenable.ot のユーザーグループへのマッピングが含まれます。

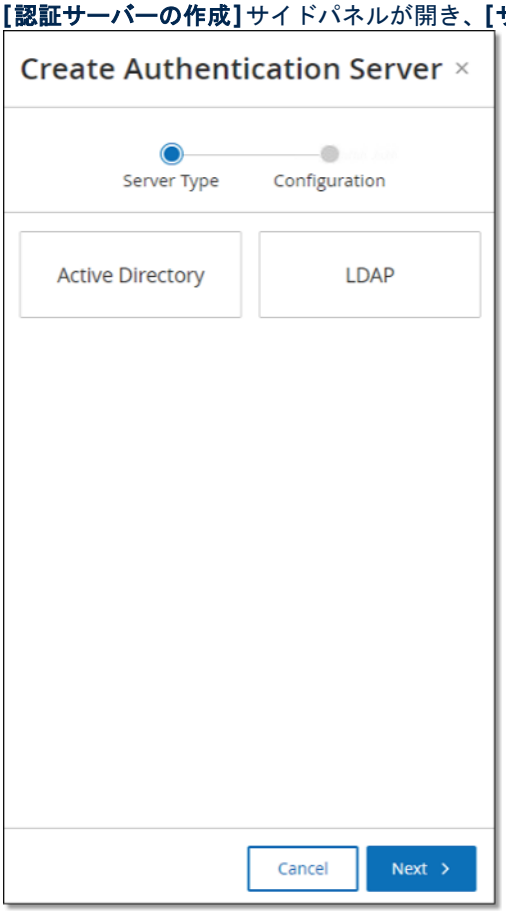
システムには、利用可能な各ロール(*管理者*ユーザーグループ > *管理者*ロール、*サイトオペレーター*ユーザーグループ > *サイトオペレーター*ロールなど)に対応する一連の事前定義されたユーザーグループが用意されています。利用可能なロールの説明については、**ユーザーロール**を参照してください。

Active Directory の構成手順

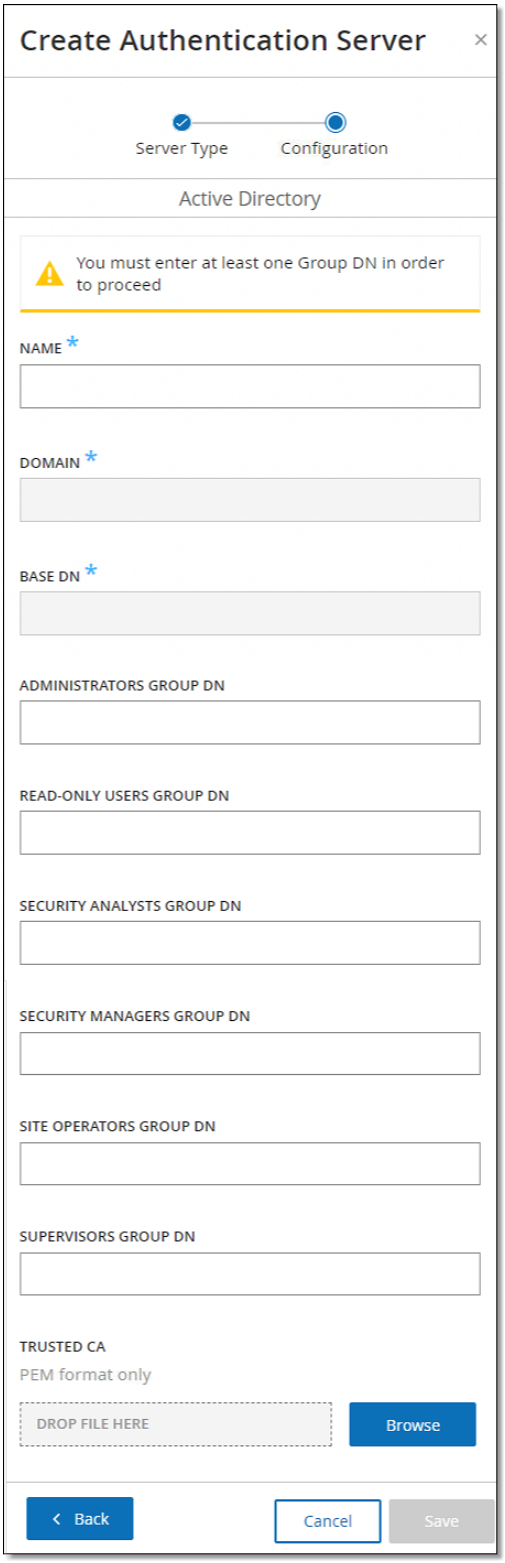
1. **オプションで**、所属組織の CA またはネットワーク管理者から CA 証明書を取得し、ローカルマシンに読み込むこともできます。

> システムには、利用可能な各ロール (*管理者*ユーザーグループ > *管理者*ロール、*サイトオペレーター*ユーザーグループ > *サイトオペレーター*ロールなど) に対応する一連の事前定義されたユーザーグループが用意されています。利用可能なロールの説明については、**ユーザーロール**を参照してください。

2. **[ローカル設定]** で、**[ユーザーとロール]**>**[認証サーバー]** 画面に移動します。
3. **[サーバーの追加]** をクリックします。
   [認証サーバーの作成] サイドパネルが開き、**[サーバータイプ]** ペインが表示されます。



4. **[Active Directory]** をクリックします。
   [Active Directory の構成] ペインが表示されます。



5. **[名前]** フィールドに、ログイン画面で使用する名前を入力します。
6. **[ドメイン名]** フィールドに、組織のドメインの FQDN (例 : company.com) を入力します。

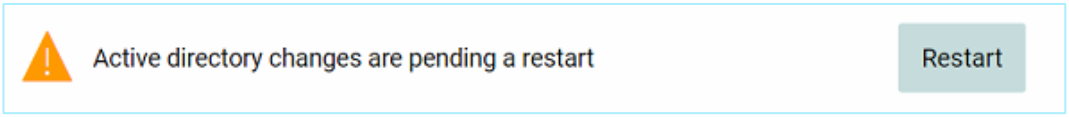
ドメイン名がわからない場合は、Windows CMD / コマンドラインで「set」コマンドを入力すると確認できます。「USERDNSDOMAIN」属性に付与される値が、ドメイン名です。

7. **[ベース DN]** フィールドに、ドメインの識別名を入力します。この値の形式は、「DC={第 2 レベルドメイン},DC={トップレベルドメイン}」です (例: DC=company, DC=com)。
8. AD グループから Tenable.ot ユーザーグループにマップする各グループについて、適切なフィールドに AD グループの DN を入力します。たとえば、ユーザーのグループを管理者ユーザーグループに割り当てるには、管理者権限を割り当てる Active Directory グループの DN を **[管理者グループ DN]** フィールドに入力します。

Tenable.ot 権限を割り当てたいグループの DN がわからない場合は、Windows CMD / コマンドラインにコマンド「dsquery group -name Users*」を入力して、ユーザーを含む Active Directory で構成されているすべてのグループのリストを表示できます。割り当てるグループの名前は、表示されている名前と同じ形式でフィールドに入力する必要があります (例: 「CN=IT_Admins, OU=Groups, DC=Company, DC=Com」)。ベース DN も、各 DN の末尾に含める必要があります。

これらのフィールドは必須ではありません。フィールドが入力されていない場合、AD ユーザーはそのユーザーグループに割り当てられません。マッピングされたグループなしでも統合を設定できますが、その場合、少なくとも 1 つのグループマッピングを追加するまで、ユーザーはシステムにアクセスできません。

9. **[信頼されている CA]** セクションで、**[参照]** をクリックし、所属組織の CA 証明書 (CA またはネットワーク管理者から入手したもの) を含むファイルに移動します。(オプション)
10. **[Active Directory を有効にする]** チェックボックスを選択します。
11. **[保存]** をクリックします。
ポップアップウィンドウが表示され、Active Directory をアクティブ化するためにユニットを再起動するように求められます。



12. **[再起動]** をクリックします。
ユニットが再起動します。再起動すると、Active Directory の設定がアクティブ化されます。指定されたグループに割り当てられたユーザーは、自分の組織の認証情報を使用して Tenable.ot プラットフォームにアクセスできます。

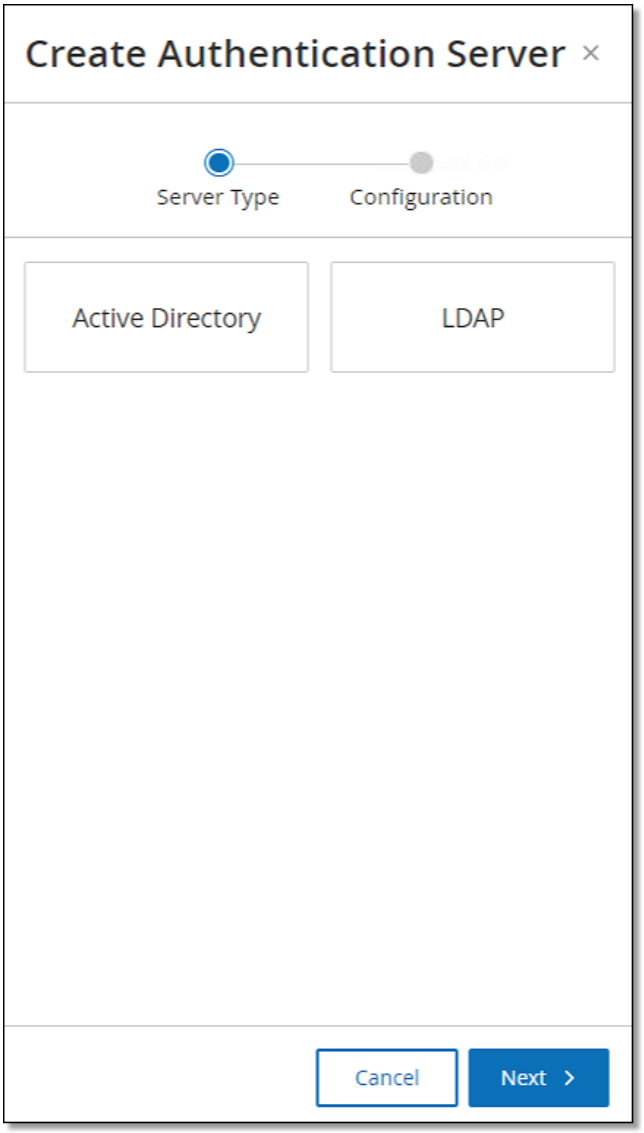
Active Directory を使用してログインするには、ログインページでユーザープリンシパル名 (UPN) を使用する必要があります。ユーザー名に @<domain>.com を追加するだけでよい場合もあります。

LDAP

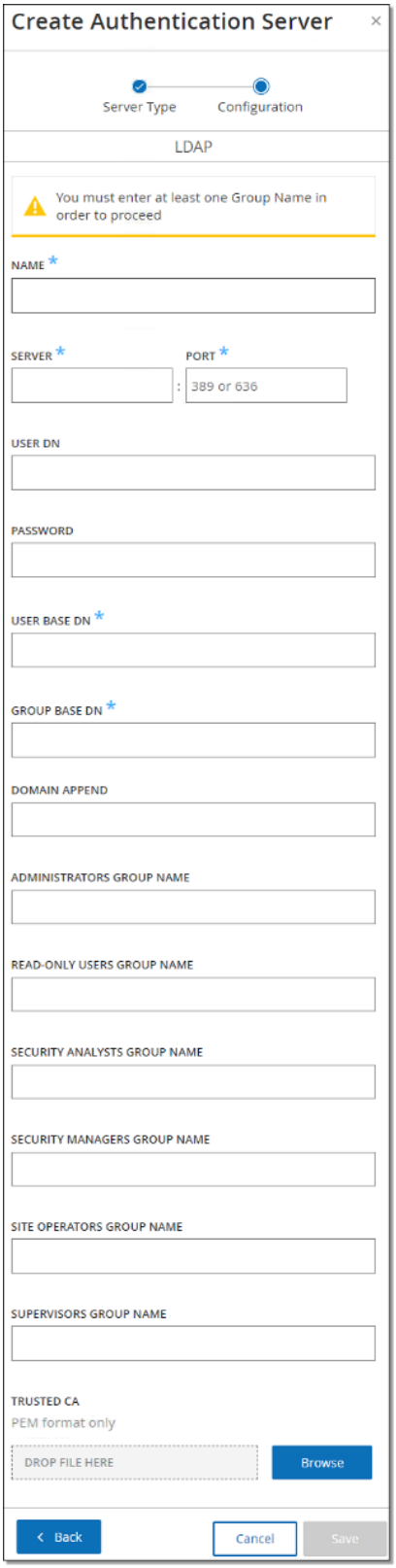
Tenable.ot を所属組織の LDAP と統合できます。これにより、ユーザーは自分の LDAP 認証情報を使用して Tenable.ot にログインできるようになります。構成には、統合のセットアップと、AD のグループの Tenable.ot のユーザーグループへのマッピングが含まれます。

LDAP の構成手順

1. [ローカル設定]で、[ユーザーとロール]>**[認証サーバー]**画面に移動します。
2. **[サーバーの追加]**をクリックします。
   [認証サーバーの追加]サイドパネルが開き、**[サーバータイプ]**ペインが表示されます。



3. **[LDAP]** を選択します。
   [LDAP の構成] ペインが表示されます。



4. **[名前]** フィールドに、ログイン画面で使用する名前を入力します。

ログイン名は区別でき、LDAP に使用されていることが分かるようにする必要があります。LDAP と Active Directory の両方が構成されている場合、ログイン画面の異なる構成を区別するのはログイン名のみです。

5. **[サーバー]** フィールドに、FQDN またはログインアドレスを入力します。

安全な接続を使用している場合、IP アドレスではなく FQDN を使用して、提供された安全な証明書が検証されるようにすることをお勧めします。

ホスト名を使用している場合、Tenable.ot システムの DNS サーバーのリストに含まれている必要があります。**[システム構成]** > **[デバイス]** を参照してください。

6. **[ポート]** フィールドに、安全ではない接続を使用する場合は 389、安全な SSL 接続を使用する場合は 636 を入力します。

ポート 636 を選択した場合、統合を完了するには証明書が必要です。

7. **[ユーザー DN]** フィールドに、DN 形式のパラメーターで DN を入力します (例: AD_1.qa.com のサーバー名の場合、ユーザー DN は CN=Administrator,CN=Users,DC=qa,DC=com となります)。
8. **[パスワード]** フィールドに、ユーザー DN のパスワードを入力します。

LDAP を使用した Tenable.ot 構成は、ユーザー DN パスワードが現在も有効である場合に限り使用できます。したがって、ユーザー DN のパスワードが変更または期限切れになった場合は、Tenable.ot 構成も更新する必要があります。

9. **[ユーザーベース DN]** フィールドに、ベースドメイン名を DN 形式で入力します (例: DC=qa,DC=com)。
10. **[グループベース DN]** フィールドに、グループベースドメイン名を DN 形式で入力します。
11. **[ドメイン追加]** フィールドに、ユーザーがメンバーとなっているドメインをユーザーが適用しなかった場合に、認証リクエストに追加されるデフォルトのドメインを入力します。
12. 関連するグループ名フィールドに、ユーザーが LDAP 構成で使用する Tenable グループ名を入力します。
13. 構成にポート 636 を使用する場合は、**[信頼できる CA]** で **[参照]** をクリックし、有効な PEM 証明書ファイルに移動します。
14. **[保存]** をクリックします。
    サーバーが無効モードで起動します。
15. 構成を適用するには、トグルスイッチをクリックして**オン**にします。
    [システム再起動] ダイアログが表示されます。
16. **[今すぐ再起動する]** をクリックしてすぐに再起動して構成を適用するか、**[後で再起動する]** をクリックして新しい構成なしでシステムの使用を一時的に続行します。

LDAP 構成の有効化 / 無効化は、システムが再起動されるまで完了しません。システムをすぐに再起動しない場合は、再起動する準備ができたときに画面上部にあるバナーの **[再起動]** ボタンをクリックしてください。

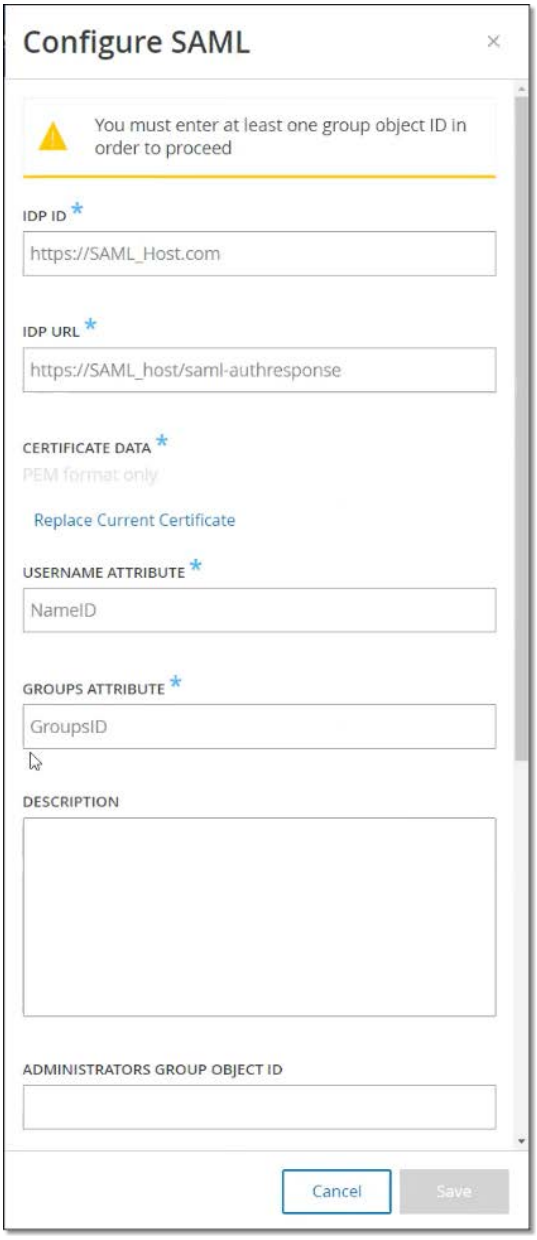
SAML

Tenable.ot を所属組織の ID プロバイダー(Microsoft Azure など)と統合できます。これにより、ユーザーは ID プロバイダー経由で認証を行うことができます。構成では、ID プロバイダー内で Tenable.ot アプリケーションを作成し、作成した Tenable.ot アプリケーションに関する情報を入力し、ID プロバイダーの証明書を Tenable.ot **SAML** ページにアップロードしてから、ID プロバイダーのグループを Tenable.ot のユーザーグループにマッピングして統合をセットアップする必要があります。Tenable.ot を Microsoft Azure と統合するための詳細なチュートリアルについては、付録 **2-AZURE ACTIVE DIRECTORY** の **SAML** 統合を参照してください。

SAML の構成手順

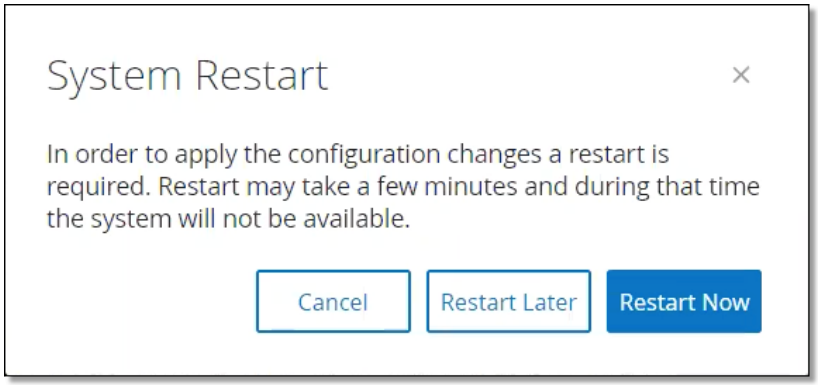
1. **[ローカル設定]** で、**[ユーザーとロール]**>**[SAML]** 画面に移動します。

2. **[構成]** をクリックします。
   [SAML の構成] サイドパネルが表示されます。



3. **[IDP ID]** フィールドに、Tenable.ot アプリケーションの ID プロバイダーの ID を入力します。
4. **[IDP URL]** フィールドに、Tenable.ot アプリケーションの ID プロバイダーの URL を入力します。
5. **[証明書データ]** で、**[現在の証明書の置き換え]** をクリックし、Tenable.ot アプリケーションで使用するためにダウンロードした ID プロバイダーの証明書ファイルに移動して開きます。
6. **[ユーザー名属性]** フィールドに、Tenable.ot アプリケーションの ID プロバイダーからのユーザー名属性を入力します。
7. **[グループ属性]** フィールドに、Tenable.ot アプリケーションの ID プロバイダーからのグループ属性を入力します。
8. **[説明]** フィールドに、説明を入力します。(オプション)
9. 構成するグループマッピングごとに、ユーザーのグループの ID プロバイダーの**グループオブジェクト ID** にアクセスし、それを対象の **[グループオブジェクト ID]** フィールドに入力して、対象の Tenable.ot ユーザーグループにマッピングします。
10. **[保存]** をクリックして保存し、サイドパネルを閉じます。

11. **[SAML]** 画面で、**[SAML シングルサインオンログイン]** ボタンをクリックして **オン**に切り替えます。
[システム再起動] の通知ウィンドウが表示されます。



12. **[今すぐ再起動する]** をクリックしてシステムを再起動し、SAML 構成をすぐに適用するか、**[後で再起動する]** をクリックして、次にシステムを再起動したときに SAML 構成が適用されるようにします。後で再起動することを選択した場合、再起動が完了するまで次のバナーが表示されます。

再起動すると、設定が有効になり、指定されたグループに割り当てられているユーザーは、ID プロバイダーの認証情報を使用して Tenable.ot プラットフォームにアクセスできます。

統合

Tenable.ot を他のサイバーセキュリティプラットフォームと同期できるように、他のサポートされているプラットフォームとの統合を設定できます。

Tenable 製品

Tenable.ot を Tenable.sc および Tenable.io と統合できます。これにより、Tenable.ot は他のプラットフォームとデータを共有できます。同期されたデータには、OT の脆弱性と、Tenable.ot から開始された IT タイプの Nessus スキャンによって検出されたデータが含まれます。

Tenable.ot で「非表示」になっている資産のデータは、統合を通じて Tenable.sc と Tenable.io に送信されません。

プラットフォームを統合するには、Tenable.ot がポート 443 を介して Tenable.sc や Tenable.io にアクセスできる必要があります。Tenable.ot への統合ユーザーとして使用される特定のユーザーを Tenable.sc や Tenable.io で作成することをお勧めします。

Tenable.sc

Tenable.sc を統合するには、Tenable.ot データ用の新しいエージェントリポジトリを作成します。リポジトリ ID を書き留めます。Tenable.ot で、新しい統合を作成し、Tenable.sc システムの IP またはホスト名、アカウント認証情報、リポジトリ ID を入力し、同期頻度を設定します。次に、新しく追加された統合を右クリックし、[同期] をクリックします。

Tenable.ot との統合に使用される Tenable.sc で特定のユーザーを作成することをお勧めします。このユーザーは、*セキュリティマネージャー* / *セキュリティアナリスト*または*脆弱性アナリスト*のロールを持ち、「フルアクセス」グループに割り当てる必要があります。

Tenable.io

Tenable.io と統合するには、アクセスキーとシークレットキーを入力し、同期頻度を設定します。

最初に、Tenable.io コンソールで API キーを生成する必要があります (**[設定]** > **[マイアカウント]** > **[API キー]** > **[生成]**)。統合を構成するときに、Tenable.ot コンソールで入力するアクセスキーとシークレットキーが与えられます。

Palo Alto Networks - 次世代ファイヤーウォール (NGFW)

Tenable.ot が検出した資産インベントリ情報を Palo Alto システムと共有できます。

Tenable.ot を Palo Alto NGFW と統合するには、Palo Alto NGRW の IP またはホスト名、および NGRW アカウントにアクセスするための認証情報を入力してください。

Aruba - ClearPass Policy Manager

Tenable.ot が検出した資産インベントリ情報を Aruba システムと共有できます。

Tenable.ot を Aruba ClearPass システムと統合するには、Aruba ClearPass システムの IP またはホスト名、および Aruba ClearPass アカウントにアクセスするための認証情報を入力してください。

サーバー

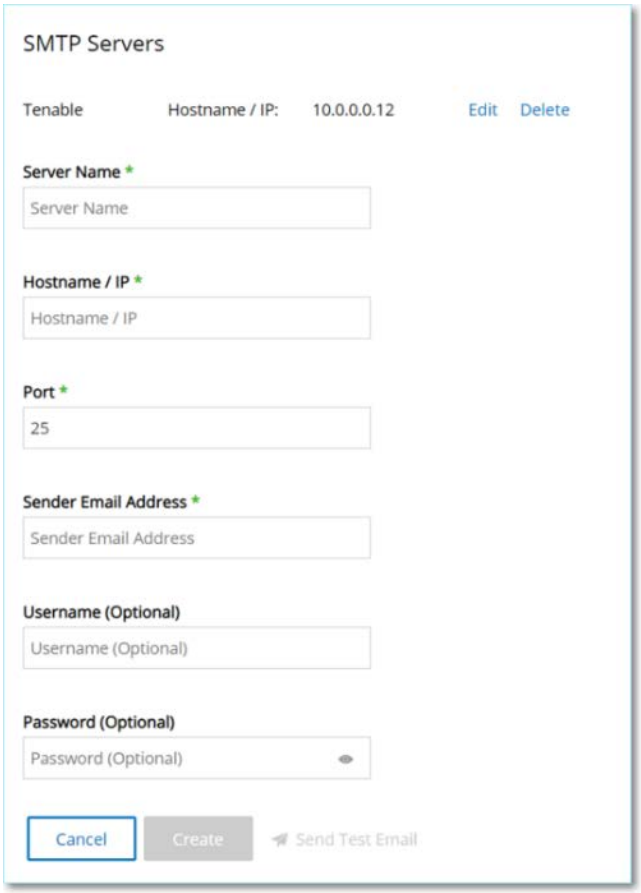
システムで SMTP サーバーと Syslog サーバーを設定して、イベント通知を電子メールで送信したり、SIEM に記録したりすることができます。また、FortiGate ファイヤーウォールを設定して、Tenable.ot ネットワークイベントに基づいてファイヤーウォールポリシーの提案を FortiGate に送信することもできます。

SMTP サーバー

E メールを介して関係者にイベント通知を送信できるようにするには、システムに *SMTP サーバー*を設定する必要があります。SMTP サーバーを設定しない場合、システムによって生成されたイベントを E メールで送信できません。どのような状況でも、すべてのイベントは、イベント画面の管理コンソール(UI)で表示できます。

➡ SMTP サーバーの設定手順

1. **[ローカル設定]** で、**[サーバー]**>**[SMTP サーバー]** 画面に移動します。
2. **[SMTP サーバーの追加]** をクリックします。
   [SMTP サーバー構成] ウィンドウが表示されます。



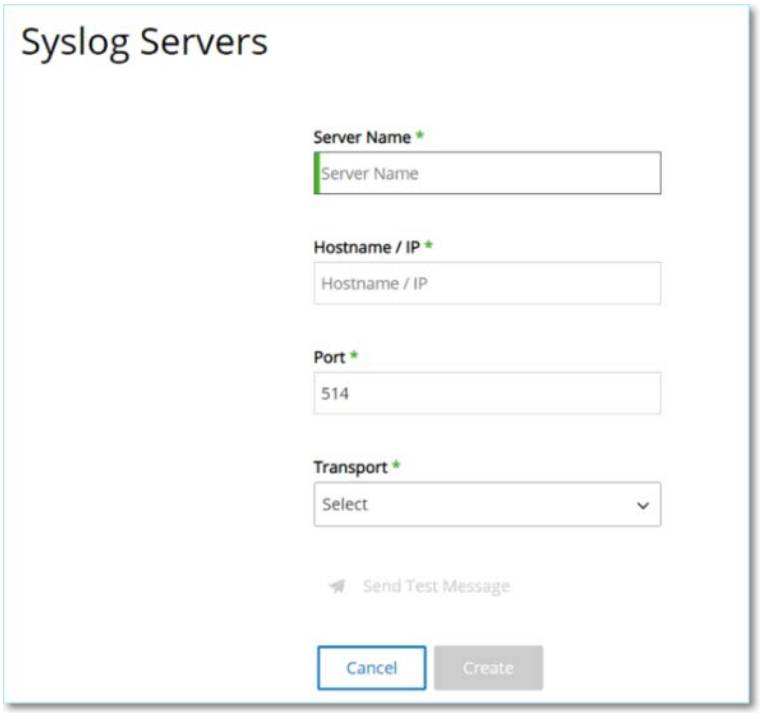
3. **[サーバー名]** フィールドに、E メール通知に使用される SMTP サーバーの名前を入力します。
4. **[ホスト名 / IP]** フィールドに、SMTP サーバーのホスト名または IP アドレスを入力します。
5. **[ポート]** フィールドに、イベントをリッスンする SMTP サーバーのポート番号を入力します(デフォルトは 25)。
6. **[送信者 E メールアドレス]** フィールドに、イベント通知メールの送信者として表示される E メールアドレスを入力します。
7. **[ユーザー名]** および **[パスワード]** フィールドに、SMTP サーバーへのアクセスに使用するユーザー名とパスワードを入力します。これらのフィールドはオプションです。
8. この時点で、テスト E メールを送信して、構成が成功したことを確認できます。**[テスト E メールの送信]** をクリックし、送信先の E メールアドレスを入力して、受信ボックスをチェックし、メールが届いたかどうかを確認します。E メールが届かない場合は、トラブルシューティングを行って問題の原因を特定し、修正します。
9. **[保存]** をクリックします。
   上記の手順を繰り返すことで、追加の SMTP サーバーを設定できます。

Syslog サーバー

外部サーバーでログイベントの収集を有効にするには、システムに *Syslog* サーバーを設定する必要があります。Syslog サーバーを設定しない場合、イベントログは Tenable.ot プラットフォームにのみ保存されます。

Syslog サーバーの設定手順

1. **[ローカル設定]** で、**[サーバー]**>**[Syslog サーバー]** 画面に移動します。
2. **[+ Syslog サーバーの追加]** をクリックします。
   [Syslog サーバー構成] ウィンドウが表示されます。



3. **[サーバー名]** フィールドに、システムイベントのログに使用する Syslog サーバーの名前を入力します。
4. **[ホスト名 / IP]** フィールドに、Syslog サーバーのホスト名または IP アドレスを入力します。
5. **[ポート]** フィールドに、イベントが送信される Syslog サーバーのポート番号を入力します (デフォルトは 514)。
6. **[トランスポート]** フィールドで、使用するトランスポートプロトコルをドロップダウンリストから選択します。オプションは *TCP* または *UDP* です。
7. テストメッセージを送信して構成が成功したことを確認する場合は、**[テストメッセージの送信]** をクリックし、メッセージが届いたかどうかを確認します。メッセージが届かない場合は、トラブルシューティングを行って問題の原因を特定し、修正します。
8. **[保存]** をクリックします。
   上記の手順を繰り返すことで、追加の Syslog サーバーを設定できます。

FortiGate ファイヤーウォール

FortiGate サーバーの設定手順

1. **[ローカル設定]** で、**[サーバー]** > **[FortiGate ファイヤーウォール]** 画面に移動します。
2. **[ファイヤーウォールの追加]** ボタンをクリックします。
   [FortiGate ファイヤーウォールの追加] 構成ウィンドウが表示されます。

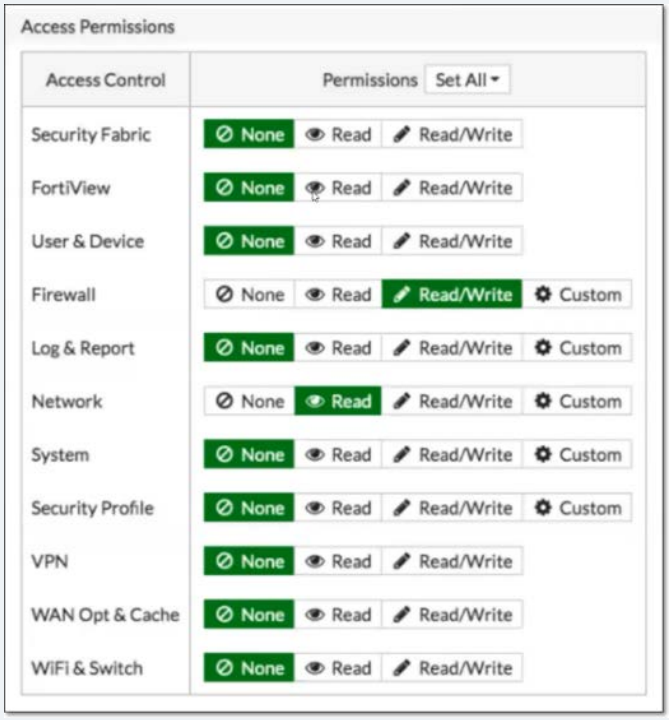
3. **[サーバー名]** フィールドに、使用する FortiGate サーバーの名前を入力します。
4. **[ホスト / IP]** フィールドに、FortiGate サーバーのホスト名または IP アドレスを入力します。
5. **[API キー]** フィールドに、FortiGate から生成した **API トークン**を入力します。詳細については、以下の注意を参照してください。
6. **[追加]** をクリックします。
   FortiGate ファイヤーウォールサーバーが作成されます。

FortiGate API トークンを生成する手順については、次のページを参照してください。
https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token

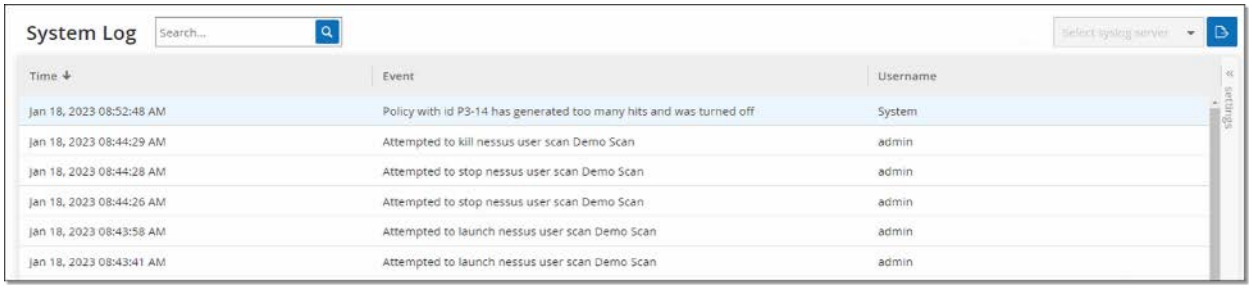
注意:

- ソースアドレス(API トークンを信頼できるホストからのみ使用可能とするために必要)には、Tenable.ot ユニットの IP アドレスを使用してください。

Tenable.ot の管理者プロファイルを作成するときは、次の設定に従ってアクセス権限を必ず適用してください。



システムログ



[システムログ]画面は、システムで発生したすべてのシステムイベント(ポリシーがオンにされた、ポリシーが編集された、イベントが解決されたなど)のリストを表示します。このログには、ユーザーが開始したイベントと自動的に発生するシステムイベント(ヒットが多すぎるためにポリシーが自動的にオフになったなど)の両方が含まれます。このログには、*[イベント]*画面に表示されるポリシー生成イベントは**含まれません**。ログは CSV ファイルとしてエクスポートできます。システムログイベントを Syslog サーバーに送信するようにシステムを構成することもできます。

ログに記録される各イベントに表示される情報について、次の表で説明します。

パラメーター	説明
時間	イベントが発生した日時。
イベント	発生したイベントの簡単な説明。
ユーザー名	イベントを開始したユーザーの名前。自動的に発生するイベントの場合、ユーザー名は与えられません。

Syslog サーバーへのシステムログの送信

➡ システムイベントを Syslog サーバーに送信するようにシステムを構成する手順

1. **[ローカル設定]**>**[システムログ]**画面に移動します。
2. ヘッダーバーで、**[Syslog サーバーの選択]**をクリックします。
   サーバーのドロップダウンリストが表示されます。

> Syslog サーバーを追加するには、**Syslog サーバー**を参照してください。

3. 目的のサーバーを選択します。
   システムログイベントが、指定された Syslog サーバーに送信されます。

付録 1 - センサーのインストール (バージョン 3.13 以前)

次の手順は、バージョン v.3.13 以前のセンサーを構成するためのフロー全体を説明しています。一部の初期ステップは、新しいセンサーにも関連しています。ただし、セットアップウィザードは、**センサーのペアリング**で説明されているペアリング手順に置き換えられています。

ステップ 1 - センサーの設定

センサーには、**Tenable.ot センサー**セクションで説明されているように、ラックマウントセンサーと構成可能なセンサーの 2 つのモデルがあります。ラックマウントモデルは、標準の 19 インチラックに取り付けるか、平面に置くことができます。構成可能なモデルは、DIN レールに設置するか、標準の 19 インチラックに取り付けることができます (「マウントイヤー」アダプターキットを使用)。

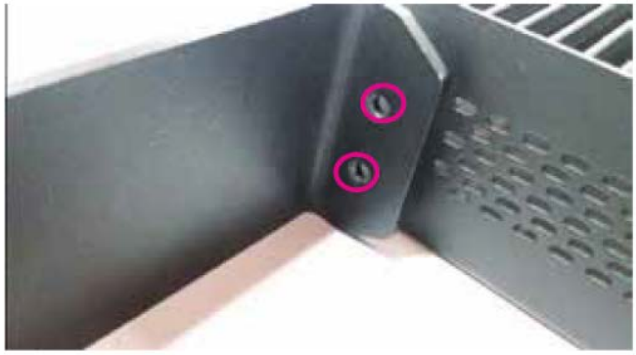
ラックマウントセンサーのセットアップ

ラックマウントセンサーは、標準の 19 インチラックに取り付けることも、机などの平面に置くこともできます。

ラックマウント (ラックマウントモデル用)

➡ **Tenable.ot センサーの標準 (19 インチ) ラックへの取り付け手順**

1. 下の画像に示すように、L 字型ブラケットをセンサーの両側のネジ穴に取り付けます。



2. 両側に 2 本のネジを挿入し、ドライバーでネジを締めてブラケットを所定の位置に固定します。
3. ブラケット付きのセンサーをラックの空いている 1U スロットに挿入します。

4. ラックマウント用ブラケット(付属)をラックマウントに適合するねじ(付属していません)でラックフレームに固定し、ユニットをラックに固定します。

ラックが電気的に接地されていることを確認してください。また、バックパネルにある冷却ファンの通気口とトップパネルの通気孔がふさがれていないことも確認してください。

5. AC 電源ケーブル(付属)をリアパネルの電源ポートに差し込み、次にケーブルを AC 電源(主電源)に差し込みます。

平面

➡ Tenable.ot センサーの平面への設置手順

1. センサーを、乾いた水平で安定な面(机など)に置きます。

机上が平らで乾いていることを確認してください。
また、バックパネルにある冷却ファンの通気口とトップパネルの通気孔がふさがれていないことも確認してください。

2. ユニットを他の電気機器と一緒に配置する場合は、バックパネルにある冷却ファンの背後に十分なスペースを確保し、適切な通気と冷却を行います。
3. AC 電源ケーブル(付属)をリアパネルの電源ポートに差し込み、次にケーブルを AC 電源(主電源)に差し込みます。

構成可能なセンサーのセットアップ

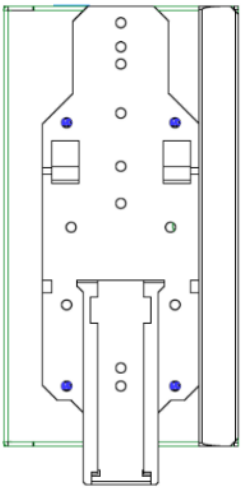
構成可能なセンサーは、DIN レールに設置することも、標準の 19 インチラックに取り付けることもできます(「マウントイヤー」アダプターキットを使用)。

DIN レールへの取り付け

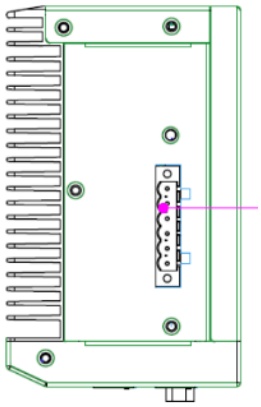
構成可能なモデルは、次の手順で DIN レールに取り付けられます。

Tenable.ot 構成可能なセンサーの標準 DIN レールへの取り付け手順

1. センサーの裏側にあるブラケットを使用して、センサーを DIN レールに取り付けます。



2. 次のいずれかの方法で電源を接続します。
   - **DC 電源** - 12-36V DC 6 ピン Phoenix Contact コネクタをセンサーユニットの側面に挿入し、コネクタの上部と下部にある埋め込み型ネジを締めて、DC 電源コードをセンサーに接続します。次に、コードのもう一方の端を DC 電源に接続します。



   - **AC 電源** - 12-36V DC 6 ピン Phoenix Contact コネクタをセンサーユニットの側面に挿入し、コネクタの上部と下部にある埋め込み型ネジを締めて、AC 電源をセンサーに接続します。

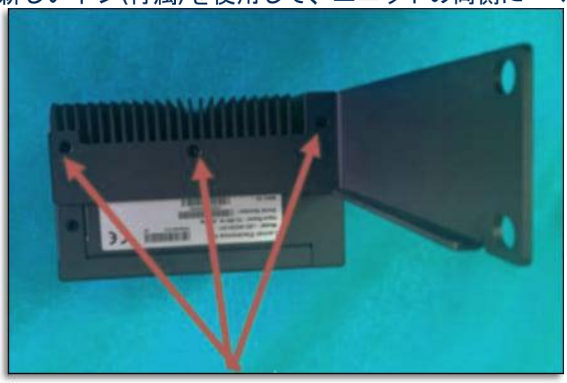
次に、AC 電源ケーブル (付属) を電源ユニットに挿入し、もう一方の端を AC コンセントに差し込みます。

ラックマウント (構成可能なモデル用)

構成可能なセンサーは、付属している「マウントイヤー」を使用して、マウントラックに取り付けることができます。

➡ 構成可能なセンサーの標準 (19 インチ) ラックへの取り付け手順

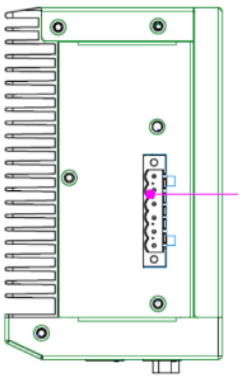
1. 次のように、ラックマウント用にユニットを準備します。
    a. ユニットの両側から 3 本のネジを外します。
    b. 新しいネジ (付属) を使用して、ユニットの両側に「マウントイヤー」を取り付けます。



2. サーバーユニットをラックの空いている 1U スロットに挿入します。

> ラックが電気的に接地されていることを確認してください。また、バックパネルにある冷却ファンの通気口とトップパネルの通気孔がふさがれていないことも確認してください。

3. 取り付けネジ (付属) を使用して、「マウントイヤー」をラックフレームに固定することにより、ユニットをラックに固定します。
4. 次のいずれかの方法で電源を接続します。
    - **DC 電源** - 12-36V DC 6 ピン Phoenix Contact コネクタをセンサーユニットの側面に挿入し、コネクタの上部と下部にある埋め込み型ネジを締めて、DC 電源コードをセンサーに接続します。次に、コードのもう一方の端を DC 電源に接続します。



    - **AC 電源** - 12-36V DC 6 ピン Phoenix Contact コネクタをセンサーユニットの側面に挿入し、コネクタの上部と下部にある埋め込み型ネジを締めて、AC 電源をセンサーに接続します。

次に、AC 電源ケーブル(付属)を電源ユニットに挿入し、もう一方の端を AC コンセントに差し込みます。

ステップ 2 - センサーのネットワーク接続

Tenable.ot センサーは、ネットワークトラフィックを収集して Tenable.ot アプライアンスに転送するために使用されます。ネットワーク監視を実行するには、対象のコントローラー / PLC に接続されているネットワークスイッチのミラーリングポートにユニットを接続する必要があります。

センサーを管理するには、ユニットをネットワークに接続する必要があります(ネットワークの監視に使用するネットワークとは別のネットワークを使用できます)。

➡ Tenable.ot ラックマウントセンサーのネットワークへの接続手順

1. Tenable.ot センサーで、イーサネットケーブル(付属)を**ポート 1** に接続します。
2. ネットワークスイッチの通常のポートにケーブルを接続します。
3. ユニットで、別のイーサネットケーブル(付属)を**ポート 2** に接続します。
4. ネットワークスイッチのミラーリングポートにケーブルを接続します。

➡ Tenable.ot 構成可能なセンサーのネットワークへの接続手順

1. Tenable.ot センサーで、イーサネットケーブル(付属)を**ポート 1** に接続します。
2. ネットワークスイッチの通常のポートにケーブルを接続します。
3. ユニットで、別のイーサネットケーブル(付属)を**ポート 3** に接続します。
4. ネットワークスイッチのミラーリングポートにケーブルを接続します。

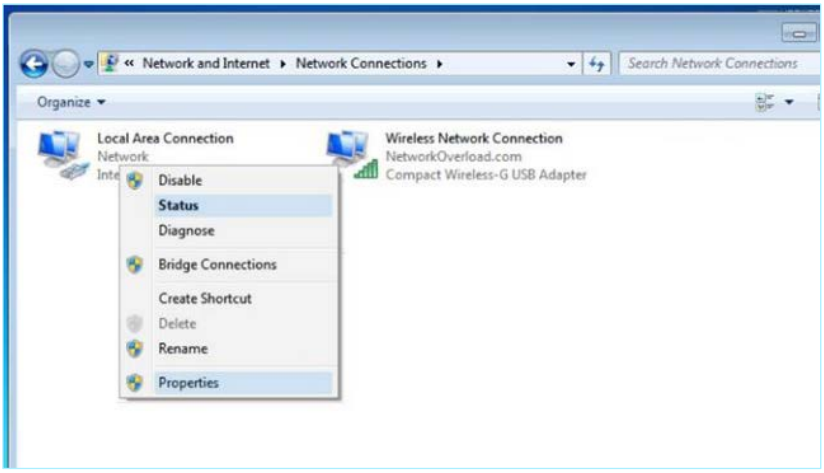
ステップ 3 - センサーセットアップウィザードへのアクセス

➡ 管理コンソールへのログイン手順

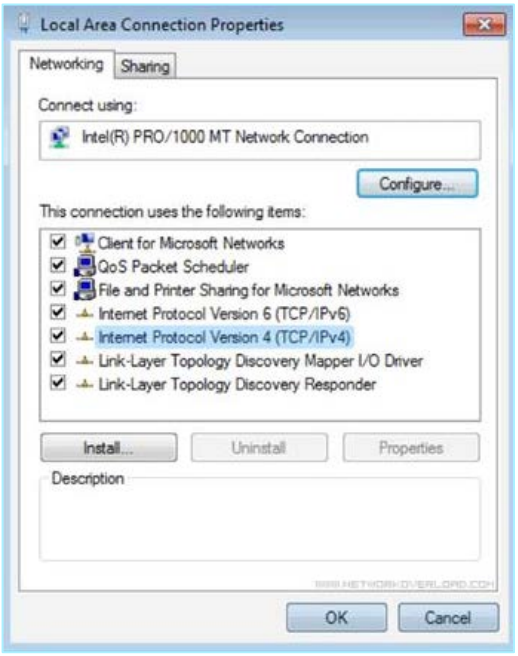
1. 次のいずれかを行います。
   - イーサネットケーブルを使用して、管理コンソールワークステーション(デスクトップ、ノートパソコンなど)を Tenable.ot センサーのポート 1 に直接接続します。
   - 管理コンソールワークステーションをネットワークスイッチに接続します。
2. 管理コンソールワークステーションが、Tenable.ot センサーと同じサブネット(192.168.1.5)の一部であるか、ユニットにルーティング可能であることを確認します。
3. 静的 IP を設定するには、次の手順を実行します(Tenable.ot センサーに接続するには、静的 IP を設定する必要があります)。
   a. **[ネットワークとインターネット]**>**[ネットワークと共有センター]**>**[アダプター設定の変更]** に移動します。

Windows のバージョンによって、ナビゲーションが若干異なる場合があります。

[ネットワーク接続]画面が表示されます。



b. **[ローカルエリア接続]**を右クリックし、**[プロパティ]**を選択します。
[ローカルエリア接続]ウィンドウが表示されます。



c. **[インターネットプロトコルバージョン4 (TCP / IPv4)]**を選択し、**[プロパティ]**をクリックします。
[インターネットプロトコルバージョン4 (TCP / IPv4) プロパティ]ウィンドウが表示されます。

d. [次の IP アドレスを使う]を選択します。
e. [IP アドレス]フィールドに、*192.168.1.10* と入力します。
f. [サブネットマスク]フィールドに、*255.255.255.0* と入力します。
g. **[OK]**をクリックします。
新しい設定が適用されます。

4. Chrome ウェブブラウザで、192.168.1.5 に移動します。

> UI は Chrome ブラウザからしかアクセスできません。また、最新バージョンの Chrome を使用している必要があります。

セットアップウィザードのようこそ画面が開きます。

5. **[セットアップウィザードの開始]**をクリックします。
セットアップウィザードが開き、**[ユーザー情報]**ページが表示されます。

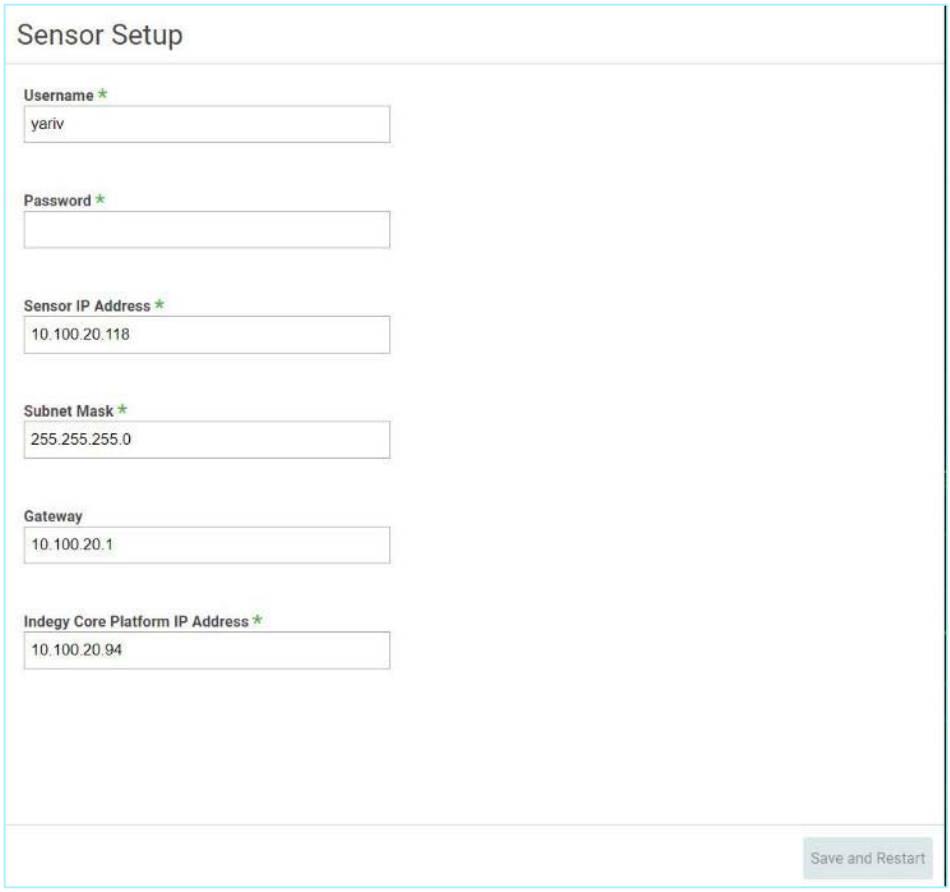
ステップ 4 – センサーセットアップウィザード

Tenable.ot セットアップウィザードは、基本的なシステム設定を構成するプロセスをガイドします。

後で構成を変更する場合は、管理コンソール (UI) の **[設定]** 画面で変更できます。

センサーの設定手順

1. ようこそ画面で、**[セットアップの開始]** をクリックします。
   セットアップ画面が表示されます。



2. **[ユーザー名]** フィールドに、システムへのログインに使用するユーザー名を入力します。ユーザー名の長さは 12 文字まで、使用できる文字は小文字と数字のみとなります。
3. **[パスワード]** フィールドに、システムへのログインに使用するパスワードを入力します。パスワードには少なくとも以下を含める必要があります。
   - 12 文字
   - 1 つの大文字
   - 1 つの小文字
   - 1 つの数字
   - 1 つの特殊文字
4. **[パスワードの再入力]** フィールドに、同じパスワードを再入力します。
5. **[センサー IP アドレス]** フィールドに、Tenable.ot センサーに適用する IP アドレス (ネットワークサブネット内) を入力します。デフォルトの IP アドレスを変更することを強くお勧めします。
6. **[サブネットマスク]** フィールドに、ネットワークのサブネットマスクを入力します。

7. ゲートウェイ (オプション) を設定する場合は、**[ゲートウェイ]** フィールドにネットワークのゲートウェイ IP を入力します。
8. **[IP アドレス]** フィールドに、Tenable.ot プラットフォームの IP アドレスを入力します。
9. **[保存して再起動]** をクリックします。
   センサーは再起動を実行します。

10. 再起動プロセスに続いて、ネットワークトラフィックは Tenable.ot プラットフォームに転送されます。構成を変更する場合は、構成済みの IP アドレスと構成済みの認証情報を使用してセンサーにログインできます。

付録 2 - AZURE ACTIVE DIRECTORY の SAML 統合

Tenable.ot は、SAML プロトコルを介した Microsoft Azure Active Directory との統合をサポートしています。これにより、Tenable.ot に割り当てられていた Azure ユーザーが、SSO を介して Tenable.ot にログインできるようになります。グループマッピングを使用して、Azure でユーザーが割り当てられているグループに従って、Tenable.ot でロールを割り当てることができます。

統合のセットアップ

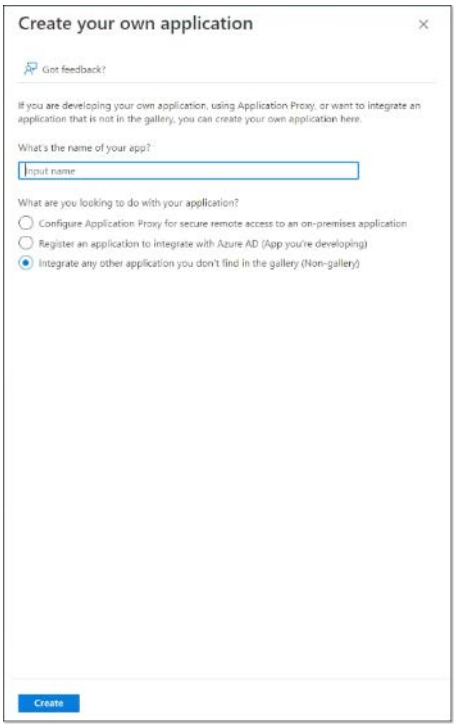
このセクションでは、Tenable.ot と Microsoft Azure Active Directory をシングルサインオン(SSO)統合するためのフロー全体について説明します。構成では、Azure Active Directory で Tenable.ot アプリケーションを作成し、作成した Tenable.ot アプリケーションに関する情報を入力し、ID プロバイダーの証明書を Tenable.ot SAML ページにアップロードしてから、ID プロバイダーのグループを Tenable.ot のユーザーグループにマッピングして統合を設定する必要があります。

構成をセットアップするには、Azure Active Directory と Tenable.ot の両方に管理ユーザーとしてログインする必要があります。

ステップ 1 - Azure での Tenable アプリケーションの作成

➡ Azure での Tenable アプリケーションの作成手順

1. **Microsoft Azure Active Directory** で、**[Azure Active Directory]** > **[エンタープライズアプリケーション]** に移動し、**[+ 新しいアプリケーション]** をクリックして **[Azure AD Gallery を参照]** を表示し、**[+ 自分のアプリケーションを作成]** をクリックします。
   [自分のアプリケーションを作成] サイドパネルが表示されます。



2. **[アプリの名前は何と言いますか]** フィールドで、アプリケーションの名前(Tenable_OT など)を入力し、**[ギャラリーにない他のアプリケーションを統合する(ギャラリー以外)](デフォルトで選択)** を選択し、**[作成]** をクリックしてアプリケーションを追加します。

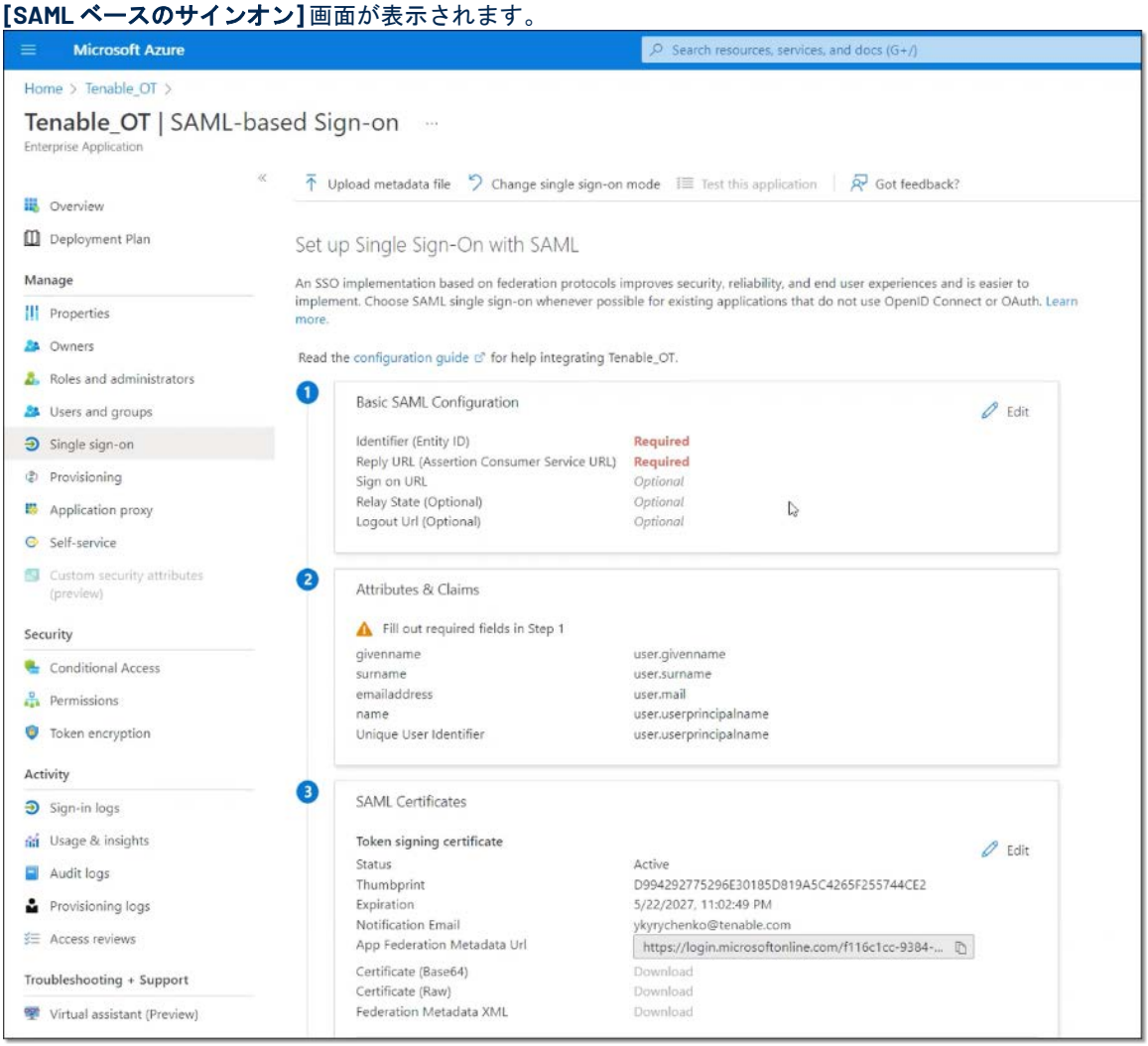
ステップ 2 - 初期構成

このステップは、Azure での Tenable.ot アプリケーションの初期構成であり、必要な証明書のダウンロードを有効にするために、基本 SAML 構成値識別子および応答 URL の一時的な値の作成で構成されています。

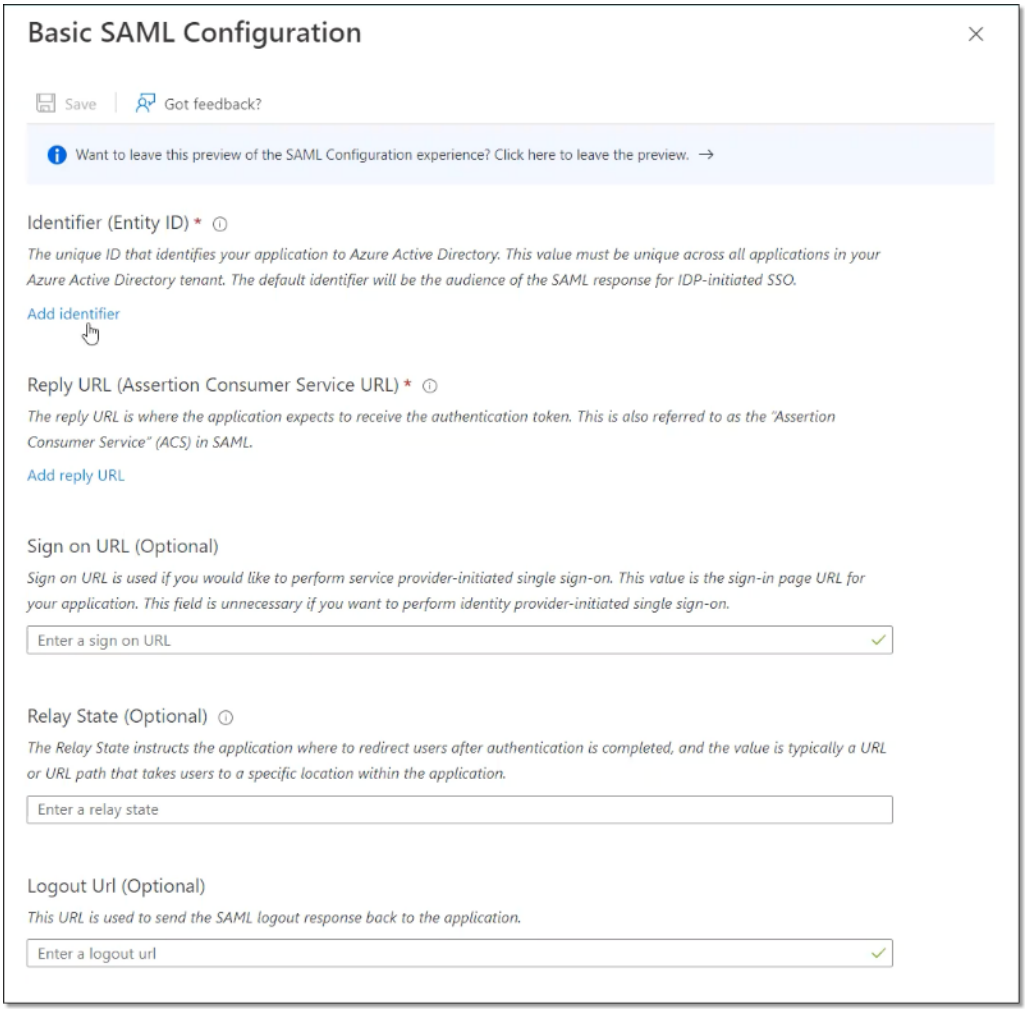
> この手順で指定されているフィールドのみを構成する必要があります。その他のフィールドは、デフォルト値のままにしておきます。

初期構成の手順

1. **Microsoft Azure Active Directory** ナビゲーションメニューで、**[シングルサインオン]** をクリックし、シングルサインオンの方法として **[SAML]** を選択します。
   [SAML ベースのサインオン] 画面が表示されます。



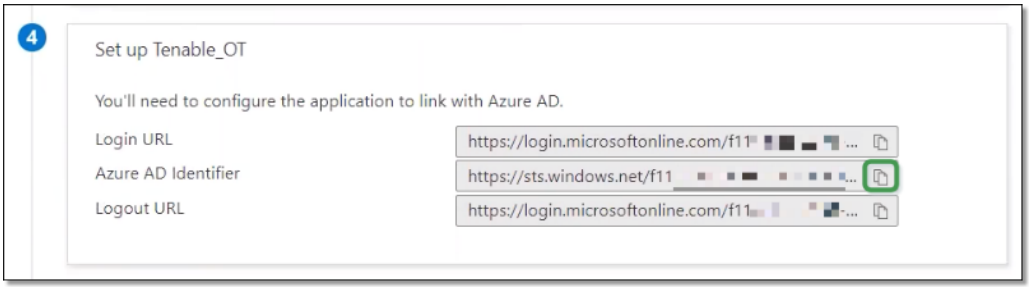
2. セクション 1 - **[基本 SAML 構成]** で、[編集] をクリックします。
[基本 SAML 構成] サイドパネルが表示されます。



3. **[識別子 (エンティティ ID)]** フィールドに、Tenable アプリケーションの一時 ID (tenable_ot など) を入力します。
4. **[応答 URL (アサーションコンシューマサービス URL)]** フィールドに、有効な URL (例: https://tenable.ot) を入力します。

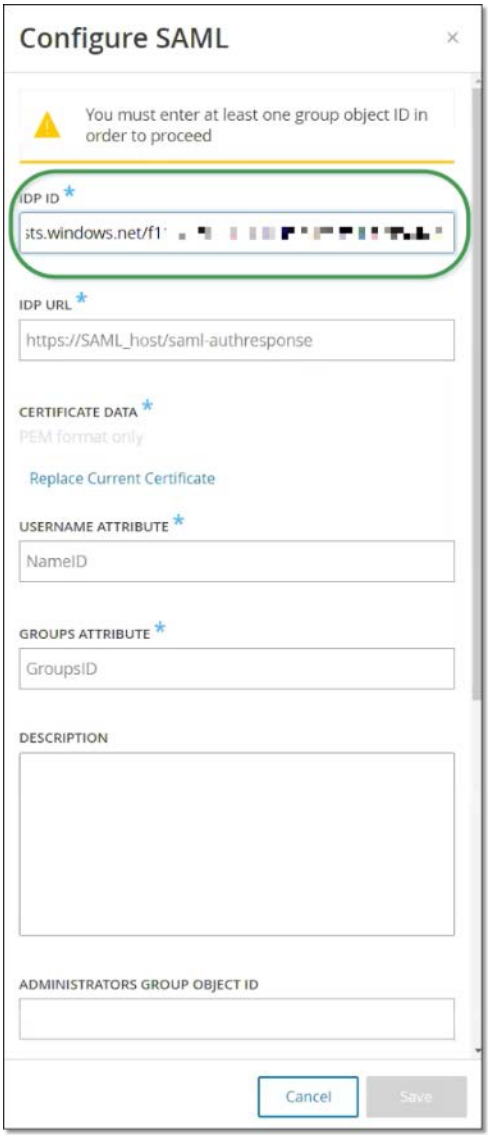
> 識別子と応答 URL の両方は、この後の構成プロセスで変更されます。

5. **[保存]** をクリックして一時的な値を保存し、**[基本 SAML 構成]** サイドパネルを閉じます。
6. セクション 4 - **[セットアップ]** で、**[コピー]** アイコンをクリックして **[Azure AD 識別子]** をコピーします。



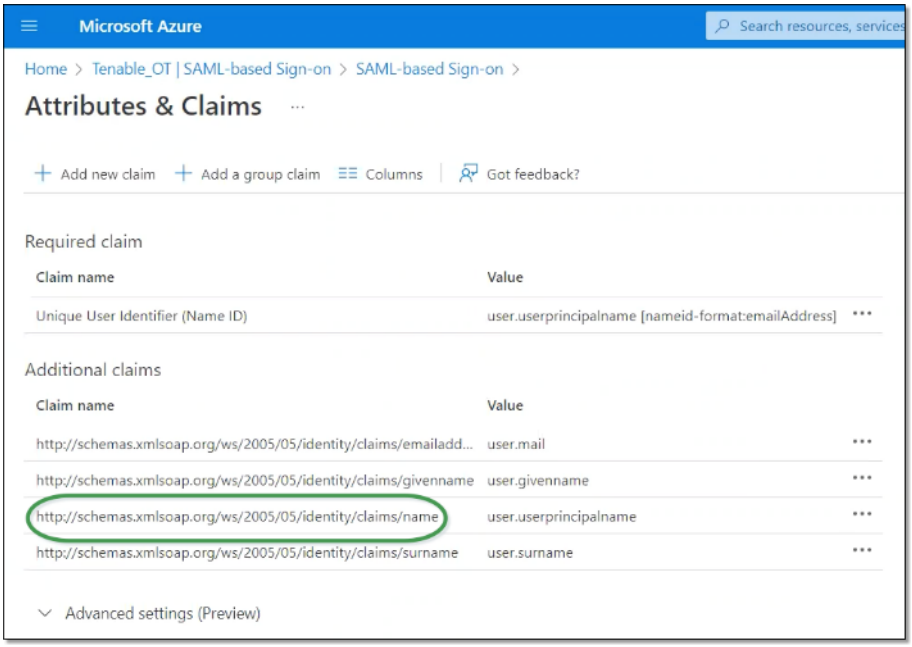
7. **Tenable.ot** コンソールに切り替え、**[ユーザーとロール]** > **[SAML]** に移動します。

8. **[構成]** をクリックして **[SAML の構成]** サイドパネルを表示し、コピーした値を **[IDP ID]** フィールドに貼り付けます。

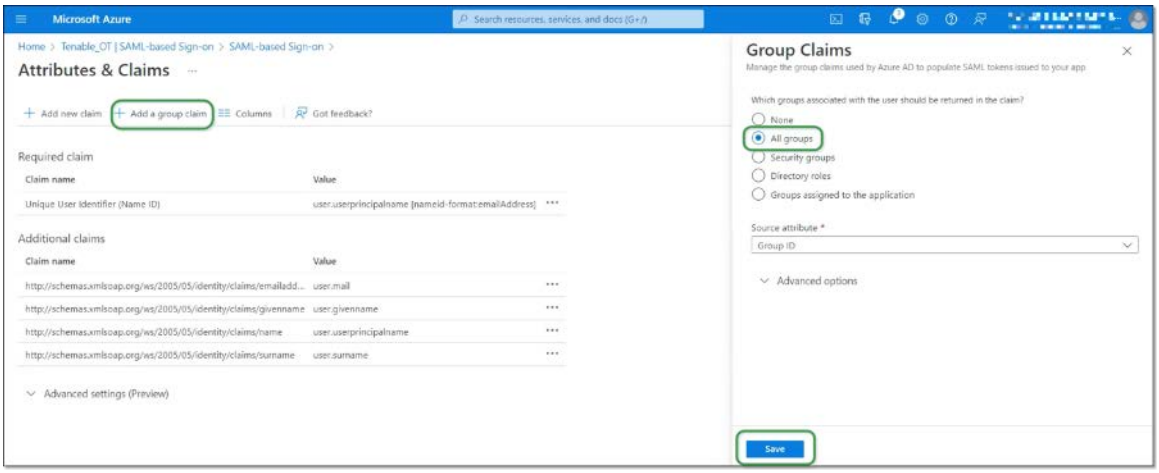


9. **Azure** コンソールで、アイコンをクリックして **[ログイン URL]** をコピーします。
10. **Tenable.ot** コンソールに戻り、コピーした値を **[IDP URL]** フィールドに貼り付けます。
11. **Azure** コンソールのセクション 3 - **[SAML 証明書]** (**証明書 (Base64)** 用) で、**[ダウンロード]** をクリックします。
12. **Tenable.ot** コンソールに戻り **[証明書データ]** で **[参照]** をクリックし、セキュリティ証明書ファイルに移動して選択します。
13. **Azure** コンソールのセクション 2 - **[属性とクレーム]** で、**[編集]** をクリックします。

14. **[追加のクレーム]** で、値 **user.userprincipalname** に対応する **[クレーム名]** の URL を選択してコピーします。

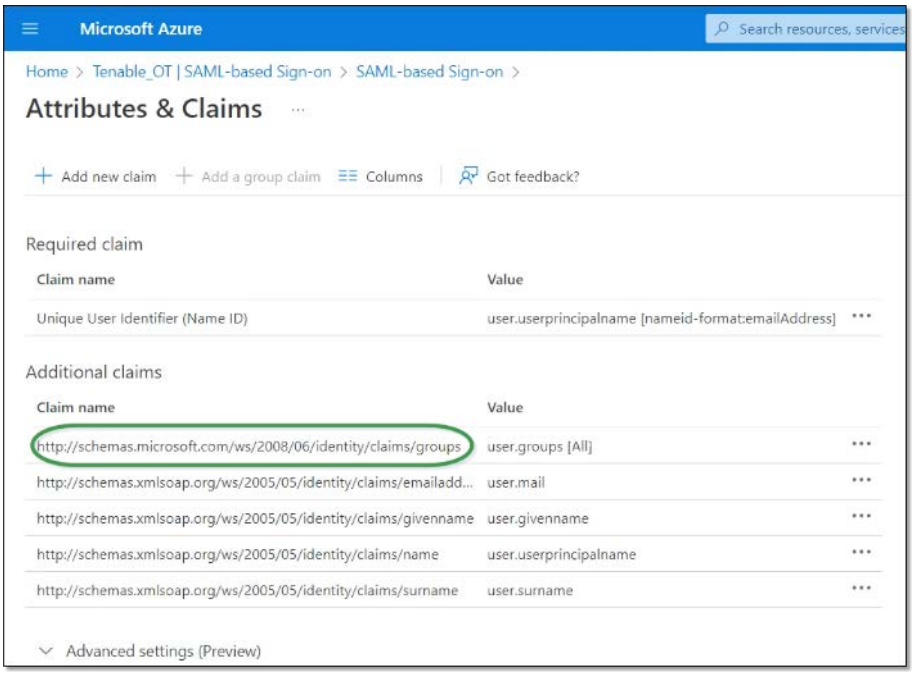


15. **Tenable** コンソールに戻り、この URL を **[ユーザー名属性]** フィールドに貼り付けます。
16. Azure コンソールで、**[+ グループのクレームを追加]** をクリックして **[グループのクレーム]** サイドパネルを表示し、**[クレームでユーザーに関連付けられているどのグループを返す必要がありますか]** で **[すべてのグループ]** を選択し、**[保存]** をクリックします。



Microsoft Azure でグループ設定が有効になっている場合は、**[すべてのグループ]** ではなく **[アプリケーションに割り当てられているグループ]** を選択すると、Azure はアプリケーションに割り当てられているユーザーグループのみを提供します。

17. **[追加のクレーム]** で、値 user.groups [All] に関連付けられた **[クレーム名]** URL をハイライト表示してコピーします。



18. **Tenable** コンソールに戻り、コピーした URL を **[グループ属性]** フィールドに貼り付けます。
19. SAML 構成の説明を追加する場合は、**[説明]** フィールドに入力します。

ステップ 3 - Azure ユーザーの Tenable グループへのマッピング

このステップでは、Azure Active Directory ユーザーが Tenable.ot アプリケーションに割り当てられます。各ユーザーに付与されたアクセス許可は、当該ユーザーが割り当てられている Azure グループと、関連付けられたロールと一連のアクセス許可を持つ事前定義された Tenable.ot ユーザーグループとの間のマッピングによって指定されます。Tenable.ot の事前定義されたユーザーグループは、*管理者*、*読み取り専用ユーザー*、*セキュリティアナリスト*、*セキュリティマネージャー*、*サイトオペレーター*、*スーパーバイザー*です。詳細については、**ユーザーグループ**を参照してください。各 Azure ユーザーは、Tenable.ot ユーザーグループにマッピングされる少なくとも 1 つのグループに割り当てられる必要があります。

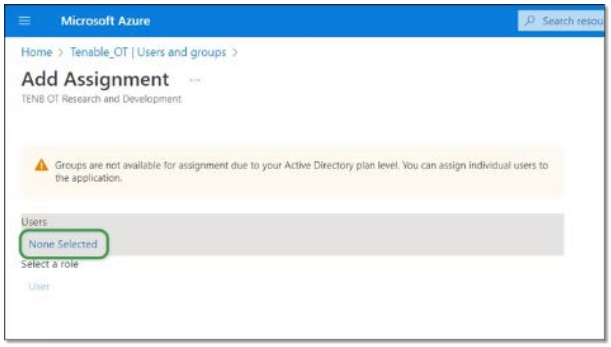
SAML 経由でログインした管理者ユーザーは、管理者 (外部) ユーザーと見なされ、ローカル管理者の持つすべての権限は付与されていません。

複数のユーザーグループに割り当てられたユーザーには、グループの中から最高のアクセス許可が与えられます。

➡ Azure ユーザーを Tenable.ot にマッピングする手順

1. **Microsoft Azure** で、**[ユーザーとグループ]** ページに移動し、**[+ ユーザー / グループの追加]** をクリックします。

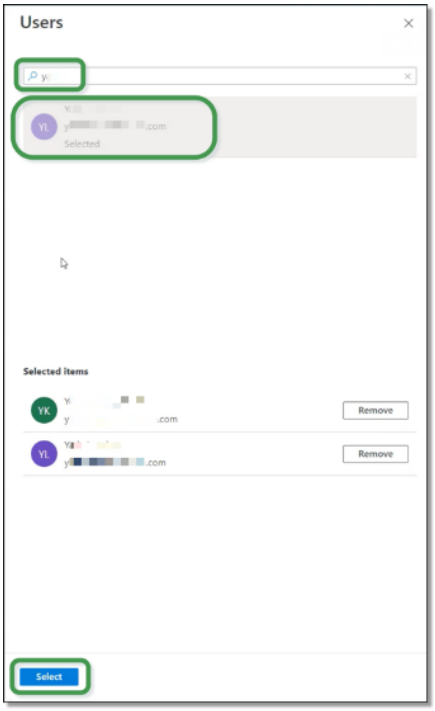
2. **[割り当ての追加]**画面の**[ユーザー]**で、**[選択なし]**をクリックします。



[ユーザー]サイドパネルが表示されます。

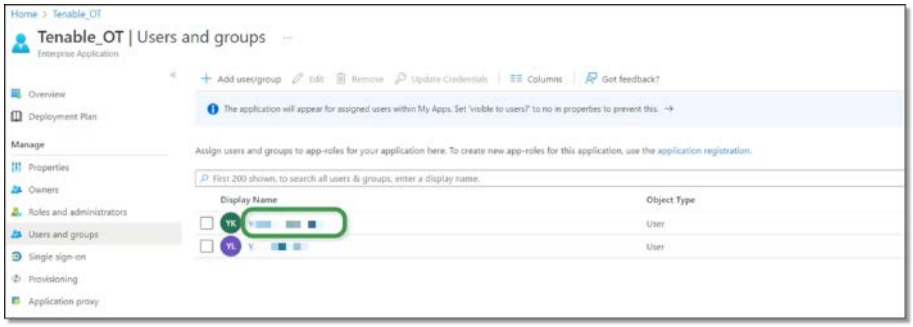
> Microsoft Azure でグループ設定が有効になっていて、すべてのグループではなく**アプリケーションに割り当てられているグループ**を選択する場合、個々のユーザーではなくグループを割り当てることができます。

3. すべての対象ユーザーを検索してクリックし、**[選択]**をクリックしてから**[割り当て]**をクリックして、ユーザーをアプリケーションに割り当てます。



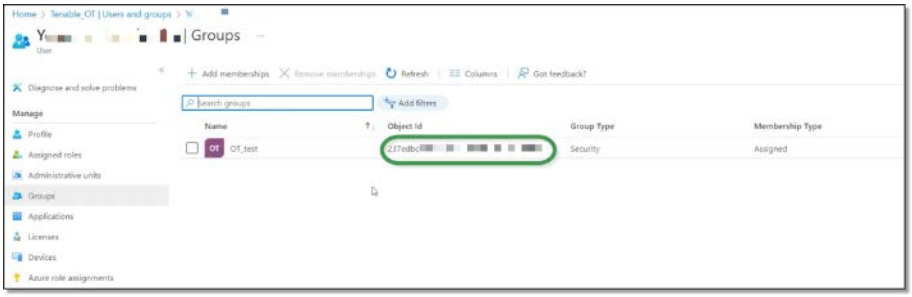
[ユーザーとグループ]ページが表示されます。

4. ユーザー(またはグループ)の**表示名**をクリックして、そのユーザー(またはグループ)のプロファイルを表示します。

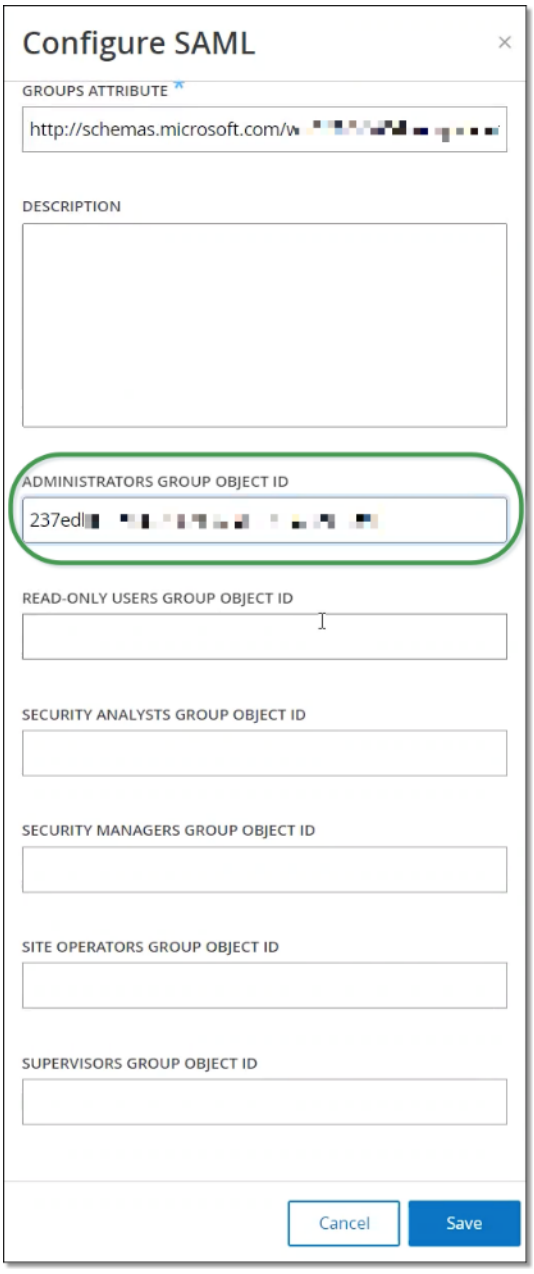


5. **[プロファイル]**画面の左側のナビゲーションバーで、**[グループ]**を選択して**[グループ]**画面を表示します。

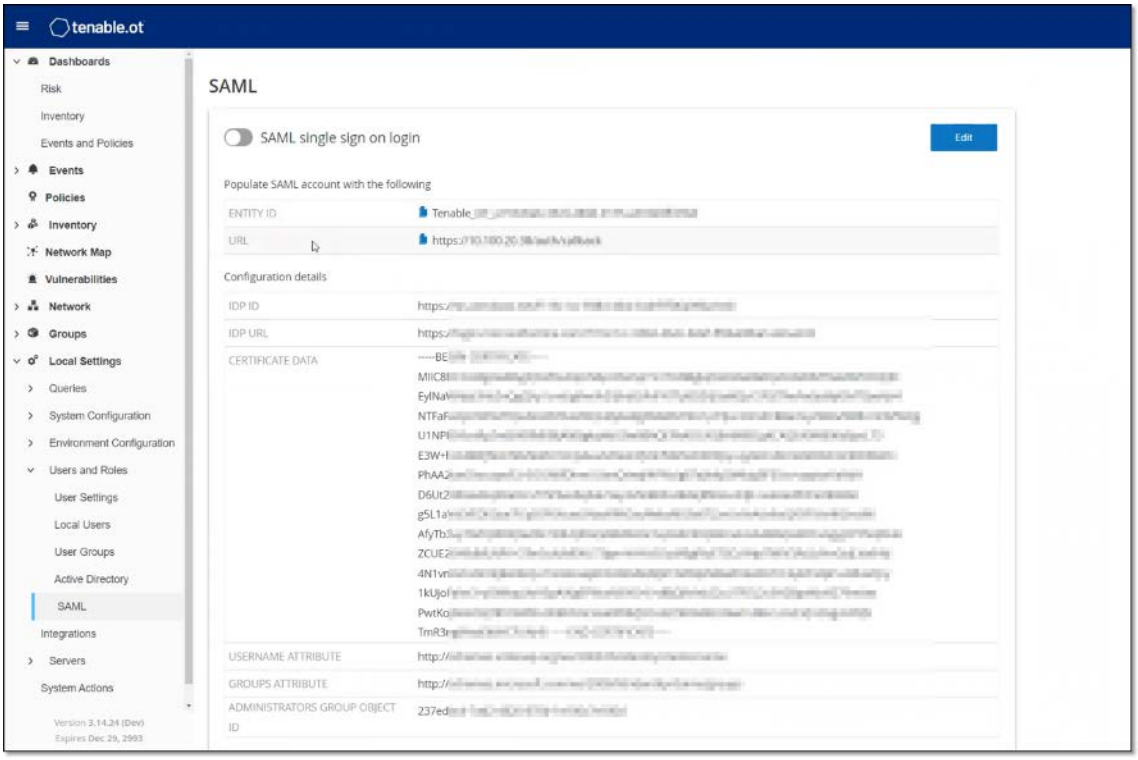
6. **[オブジェクト ID]** で、Tenable にマッピングされるグループの値をハイライト表示してコピーします。



7. **Tenable.ot** コンソールに戻り、コピーした値を対象の **[グループオブジェクト ID]** フィールド (例: 管理者グループオブジェクト ID) に貼り付けます。
8. Tenable.ot で異なるユーザーグループにマッピングするグループごとに、ステップ 1~7 を繰り返します。
9. **[保存]** をクリックして保存し、サイドパネルを閉じます。



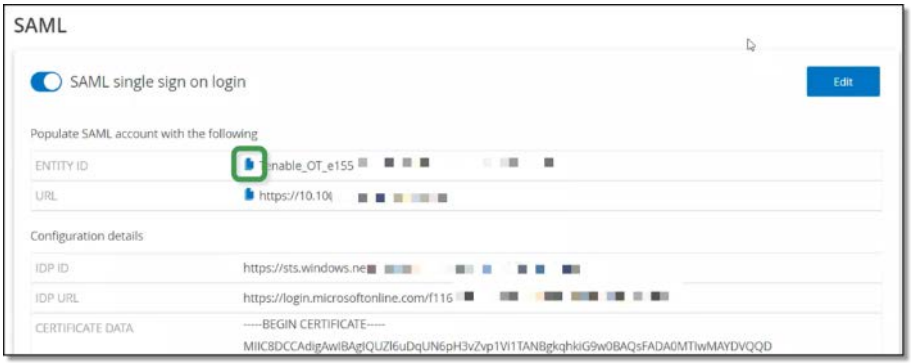
[SAML] 画面が、構成された情報とともに Tenable.ot コンソールに表示されます。



ステップ 4 - Azure での構成の終了

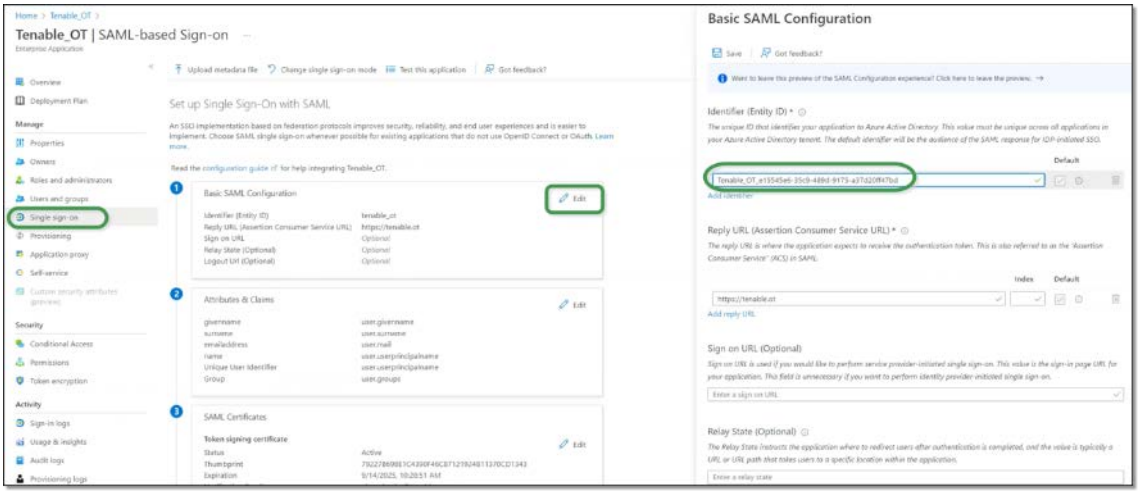
➡ Azure で構成を終了する手順

1. Tenable.ot の **[SAML]** 画面の **[エンティティ ID]** で、コピーアイコンをクリックします。



2. **[Azure]** 画面に切り替え、左側のナビゲーションメニューで **[シングルサインオン]** をクリックして、**[SAML ベースのサインオン]** ページを開きます。

3. セクション 1 - **[基本 SAML 構成]** で、**[編集]** をクリックし、コピーした値を **[識別子 (エンティティ ID)]** フィールドに貼り付けて、以前に入力した一時的な値を置き換えます。



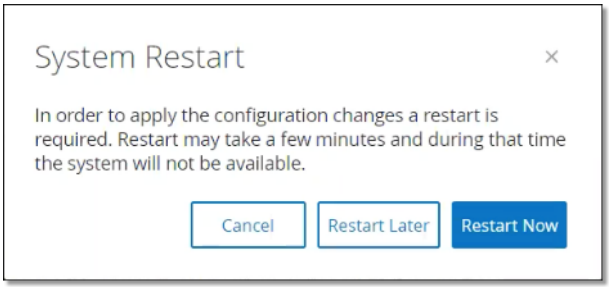
4. Tenable.ot の **[SAML]** 画面に戻り、**[URL]** で、コピーアイコンをクリックします。
5. **Azure** コンソールの **[基本 SAML 構成]** サイドパネルの **[応答 URL (アサーションコンシューマサービス URL)]** で、コピーした URL を貼り付け、以前入力した一時的な URL を置き換えます。
6. **[保存]** をクリックして構成を保存し、サイドパネルを閉じます。
   構成が完了し、接続が **[Azure Enterprise アプリケーション]** 画面に表示されます。

ステップ 5 - 統合のアクティブ化

SAML 統合をアクティブ化するには、Tenable.ot を再起動する必要があります。ユーザーは、システムをすぐに再起動するか、後で再起動するかを選択できます。

➡ 統合をアクティブ化する手順

1. Tenable.ot コンソールの **[SAML]** 画面で、**[SAML シングルサインオンログイン]** ボタンをクリックして **オン** に切り替えます。
   [システム再起動] の通知ウィンドウが表示されます。



2. **[今すぐ再起動する]** をクリックしてシステムを再起動し、SAML 構成をすぐに適用するか、**[後で再起動する]** をクリックして、次にシステムを再起動したときに SAML 構成が適用されるようにします。後で再起動することを選択した場合、再起動が完了するまで次のバナーが表示されます。

SSO を使用したサインイン

再起動すると、**Tenable.ot** ログインウィンドウでは、ログインボタンの下に新しい **[SSO からサインイン]** リンクが表示されます。Tenable.ot に割り当てられた Azure ユーザーは、Azure アカウントを使用して Tenable.ot にログインできます。

➡ SSO を使用したサインイン手順

1. **Tenable.ot** ログイン画面で、**[SSO からサインイン]** リンクをクリックします。

Azure にすでにログインしている場合は、Tenable.ot コンソールに直接移動します。まだログインしていない場合は、Azure サインインページにリダイレクトされます。
複数のアカウントを持つユーザーは、Microsoft の **[アカウントの選択]** ページにリダイレクトされ、ログインに使用するアカウントを選択できます。