Tenable OT Security 3.19 ユーザーガイド

最終更新日: 2024 年 10 月 3 日

目次

Tenable OT Security にようこそ

Tenable OT Security (OT Security) (旧 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。脅威の検出と軽減から、資産追跡、脆弱性管理、設定管理、アクティブクエリのチェックに至るまで、OT Security 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、制御性を最大限に高めます。

OT Security は、IT セキュリティ担当者や OT エンジニア向けの、包括的なセキュリティツールとレポート作成機能を提供しています。これにより、コンバージド IT/OT セグメントと ICS アクティビティを可視化し、すべてのサイトとそれぞれの OT 資産 (Windows サーバーから PLC バックプレーンに至るまで) の状況を一元的に把握できるようになります。

以下は OT Security の主な機能です。

- **360 度の可視性** – 攻撃は IT/OT インフラ内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。OT Security は、ご利用の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 IT セキュリティと運用ツールにもネイティブに統合できます。これにより、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。
- **脅威の検出と軽減** – OT Security は、複数の検出のエンジンを利用して、OT 運用に影響を与えかねない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** – 特許取得のテクノロジーを利用する OT Security は、ネットワークレベルだけでなく、デバイスレベルまで、インフラの可視性を提供します。ネットワーク全体で発生してい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 デバイスの両方にクエリをかけます。
- **リスクベースの脆弱性管理** – 包括的かつ詳細な IT/OT 資産追跡機能を使用する OT Security は、予測に基づいた優先順位付けで、産業用制御システム (ICS) ネットワークにある各資産の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、軽減策の提案とともに含まれています。
- **設定管理** – OT Security 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設定変更の詳細な全履歴を提供します。これにより、管理者は

「直近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。

ヒント: *Tenable OT Security ユーザーガイド*とユーザーインターフェースは、英語、日本語、ドイツ語、フランス語、中国語 (簡体字) で提供されています。ユーザーインターフェース言語を変更するには、ローカル設定を参照してください。

Tenable OT Security の詳細情報は、以下の顧客教育用資料を確認してください。

- Tenable OT Security について (Tenable University)

OT Security を使い始める

OT Security の使用を開始するには、OT Security を使い始める に記載されている一連の手順に従ってください。

OT Security テクノロジー

OT Security 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** – OT Security ネットワーク検出テクノロジーは、産業用制御システムに固有の特性と要件に対応するよう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設定変更が含まれます。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許可リストまたはブロックリストに追加し、アラートをトリガーできます。事前定義された状況が発生していないか調べるアクティブクエリチェックをトリガーするようにポリシーを設定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** – OT Security の特許取得済みクエリテクノロジーは、ICS ネットワーク内にある制御デバイスのメタデータを定期的に調査することで、ネットワーク上の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 OT Security 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、設定の詳細、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、安全であり、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

OT Security プラットフォームコンポーネント

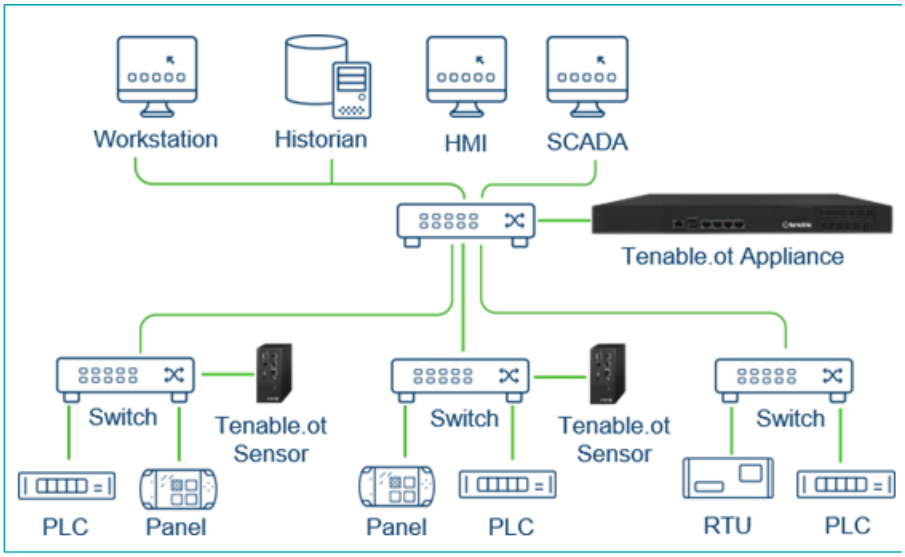
> **注意**: このドキュメントでは、OT Security アプライアンスのことを ICP (Industrial Core Platform) と呼びます。

OT Security ソリューションは次のコンポーネントで構成されています。

- **ICP (OT Security アプライアンス)**– このコンポーネントは、ネットワークから直接 (スパンポートやネットワークタップを介して)、または Tenable OT Security センサー (OT Security センサー) からのデータフィードを使用して (あるいはその両方)、ネットワークトラフィックを収集して分析します。ICP アプライアンスは、ネットワーク検出とアクティブクエリの両方の機能を実行します。

- **OT Security センサー** – これらは、対象のネットワークセグメントに (管理対象スイッチあたり最大 1 つ) デプロイできる小さなデバイスです。OT Security センサーは、すべてのトラフィックをキャプチャして、データを圧縮し、情報を OT Security 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 以降のセンサーでは、それらのセンサーがデプロイさ

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設定できます。



ネットワークコンポーネント

OT Security は、以下のネットワークコンポーネントとのやり取りをサポートしています。

- **OT Security ユーザー(管理)** – ユーザーアカウントを作成して、OT Security 管理コンソールへのアクセスを制御できます。管理コンソールには、ブラウザ(Google Chrome)からセキュアソケットレイヤー認証 (HTTPS) でアクセスできます。

注意: OT Security ユーザーインターフェースには、最新バージョンの Chrome からのみアクセスできます。

- **Active Directory サーバー** – Active Directory などの LDAP サーバーを使用して、ユーザー認証情報をオプションで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** – OT Security イベントログを Syslog プロトコルを使用して SIEM に送信します。
- **SMTP サーバー** – OT Security は、SMTP サーバーを介して、特定のグループの従業員に E メールでイベント通知を送信します。
- **DNS サーバー** – DNS サーバーを OT Security に統合して、資産名の解決を支援します。
- **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 OT Security 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]。

[1]たとえば、OT Security は Palo Alto Networks Next Generation Firewall (NGFW) や Aruba ClearPass との統合をサポートし、OT Security がこれらのシステムと資産インベントリ情報を共有できるようになりました。OT Security は、Tenable Vulnerability Management や Tenable Security Center 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]** で設定します。統合を参照してください。

OT Security ハードウェアコンポーネント

OT Security ハードウェアアプライアンス (ICP)

コンポーネント	説明
電源インジケーター	OT Security 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	サービスまたはローカルアクセス用。8N1 設定で 115200 bps のボーレート。
USB ポート	オフラインモードでのアプライアンスのイメージ再作成またはアップグレード用。
イーサネットポート	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、4 つの GbE ポートが次のように使用されます。 ポート 1 - デフォルトでは、このポートが管理 (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。このポート設定は、セットアップ中にまたは [設定] ページで後から、クエリのみを含むように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) のデスティネーション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化されている場合、このポートは管理(ユーザーインターフェース)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。リモートまたはローカルサポートのために OT Security の Professional Services によって使用されます。

注意: 利用可能なすべてのネットワークインターフェースは、OT Security ICP に対して設定可能です。

リアパネル

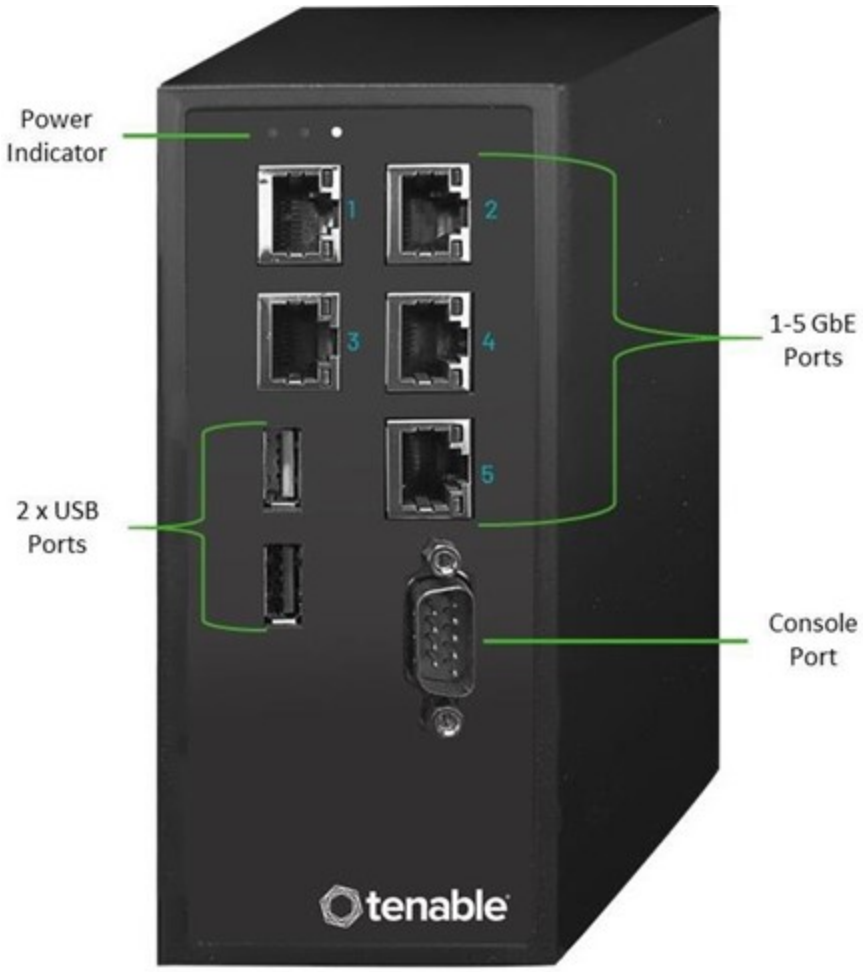
コンポーネント	説明
冷却ファン	2 個の冷却ファン。通風口がふさがれていないことを確認してください。
電源スイッチ	ON/OFF スイッチ(電源を切るには、数秒押し続けます)。
電源	AC 電源コネクタ(AC 100 ~ 240 V)。

パッケージの内容物

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、OT Security 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	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。

OT Security センサーコンポーネント

設定可能なセンサー



注意: 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	サービスまたはローカルアクセス用。 **注意**: 8N1 設定で 115200 bps のボーレート。

USB ポート	オフラインモードでのアプライアンスのイメージ再作成またはアップグレード用。
イーサネットポート	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、5 つの GbE ポートが次のように使用されます。 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) のデスティネーション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。

注意: 利用可能なすべてのネットワークインターフェースは、OT Security センサーに対して設定可能です。

パッケージの内容物

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	

ラックマウントセンサー

注意: 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、Tenable は現在、設定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 *	サービスまたはローカルアクセス用。
USB ポート	オフラインモードでのアプライアンスのイメージ再作成またはアップグレード用。
イーサネットポート	4 つの 1 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 - ミラーポート - ミラーリングセッション (SPAN) のデスティネーション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。

*8N1 設定で 115200 bps のボーレート。

リアパネル

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	AC 電源コネクタ(AC 100 ~ 240 V)。

パッケージの内容物

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	

Enterprise Manager

OT Security EM は、サイトまたはパブリック/プライベートクラウドサーバーにインストールされたアプライアンスとしてデプロイできます。

次の表は、さまざまなデプロイ方法の仕様を示しています。

仕様	オンプレミス	パブリッククラウド
ハードウェア	Intel® Xeon™ D1548、2.0 GHz 2 X 32GB DDR4、2400 MHz データ: 2 x 2TB 固定 SATA3 HDD OS: 1 X 64 GB SSD	AWS

フォームファクター	寸法: 438 x 44 x 321 mm 重さ: 6 kg	該当なし
電源	220W、単一 PS 入力 AC 90V ~ 264V	該当なし
冷却	CPU ヒートシンク、ファンダクト、冷却ファン x 2	該当なし
温度	動作時: 0°C ~ 40°C/32°F ~ 104°F ストレージ: -20 ~ 70º C / -4°F ~ 158°F 湿度: 5% ~ 90%	該当なし

システム要素

資産

資産とは、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、ネットワーク内のハードウェアコンポーネントを指します。OT Security 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、パッチデプロイメント、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

OT Security 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付けられます。

- **イベント** – デバイスに影響を与えたネットワークでのイベント (イベントの深刻度とどれほど最近そのイベントが起きたかに基づく重み付け)。

  > **注意**: 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(古い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)。OT Security 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要度を示す指標。

> **注意**: バックプレーンに接続されている PLC の場合、同じバックプレーンを使用してい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します。特定のポリシーのポリシー定義条件をすべて満たすイベントが発生すると、OT Security でイベントが生成されます。OT Security によりイベントがログに記録され、ポリシーで設定されているポリシーアクションにしたがって通知が送信されます。

ポリシーイベントには次の 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。

このシステムには、事前定義された一連のポリシーがあります(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いて設定することができます。

以下は、可能なポリシー設定の例です。

- **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)** – HMI はコントローラーのファームウェアバージョンをクエリするべきでなく(偵察を示している可能性があります)、コントローラーは稼働中にプログラムされるべきではありません(権限のない悪質な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の変更** – コントローラーロジック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** – 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。
- **資産インベントリの異常または不正な変更** – 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** – 資産ファームウェアまたは状態が変わりました。
- **セットポイントの異常な書き込み** – 特定のパラメーターに変更が加えられると、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、その範囲から外れた場合に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をベースにして、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対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。

- **設定イベントポリシー** – 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化や、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設定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、事前に設定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

OT Security のポリシーの定義で重要な要素は、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、E 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。

OT Security ライセンスコンポーネント

このトピックでは、スタンドアロン製品としての Tenable OT Security のライセンス付与プロセスを説明します。また、資産のカウント方法、購入できるアドオンコンポーネント、ライセンスの流用方法について、およびライセンスが超過または期限切れになるとどうなるかについても説明しています。

ヒント: ライセンスをアップデートまたは再初期化するには、OT Security ライセンスのワークフローを参照してください。

Tenable OT Security のライセンシング

Tenable OT Security は、サブスクリプションまたは永久/メンテナンスバージョンで購入できます。

Tenable OT Security のライセンスを取得する際は、所属する組織のニーズと環境に基づいてライセンスを購入してください。Tenable OT Security はその後、それらのライセンスを*資産*に割り当てます。資産とは、IP アドレスを持つ検出されたデバイスすべてを指し、各 IP アドレスに 1 つのライセンスが割り当てられます。

環境が拡張すると資産数も増えるため、その変化に合わせてライセンスを追加購入する必要があります。Tenable のライセンスは、累進的な価格設定であるため、多く購入するほど単価は安くなります。価格については、Tenable 担当者までお問い合わせください。

資産のカウント方法

Tenable OT Security では、ライセンスは環境内の一意の IP アドレスの数に基づいてカウントされます。資産は、検出された瞬間からライセンス付与されます。

注意: ライブ IP アドレスの背後にある内部ネットワークの資産は、ライセンスとしてカウントされません。たとえば、冗長接続された PLC シャーシに 2 つのライブ IP アドレスがあり、その背後に 10 個のモジュールがある場合、2 つのライブ IP アドレスのみがライセンスとしてカウントされます。

Tenable OT Security コンポーネント

コンポーネントを追加することで、それぞれのユースケースに合わせて Tenable OT Security をカスタマイズできます。一部のコンポーネントは有料のアドオンです。

購入に含まれるもの	アドオンコンポーネント
• 仮想コアアプライアンス • Tenable Security Center.	• Tenable OT Security Enterprise Manager. • Tenable OT Security Configurable Sensor • Tenable OT Security Certified Configurable Sensor • Tenable OT Security Certified Core Platform • Tenable OT Security Core Platform • Tenable OT Security XL Core Platform

ライセンスの流用

ライセンスを購入しても、追加のライセンスを購入しない限り、ライセンスの総数は契約期間中ずっと同じです。ただし Tenable OT Security はユーザーの資産カウントの変化に応じて、リアルタイムでライセンスを流用します。

Tenable OT Security では、次の資産のライセンスが流用されます。

- 非表示の資産
- 30 日以上オフラインになっている資産
- ユーザーインターフェースで削除または非表示にした資産

ライセンス制限の超過

Tenable OT Security では、追加のライセンスを購入しない限り、割り当てられた数のライセンスしか使用できません。

ライセンス数が上限を超えた場合、次のようになります。

- 管理者でないユーザーは Tenable OT Security にアクセスできなくなります。
- ユーザーインターフェースに、ライセンスが超過したことを示すメッセージが表示されます。
- Tenable OT Security 設定から資産を復元できなくなります。
- 脆弱性プラグインや IDS 署名 (フィード更新) を更新できなくなります。

注意: ライセンス制限を超えた場合でも、Tenable OT Security は引き続き新しい資産を検出して追加できます。

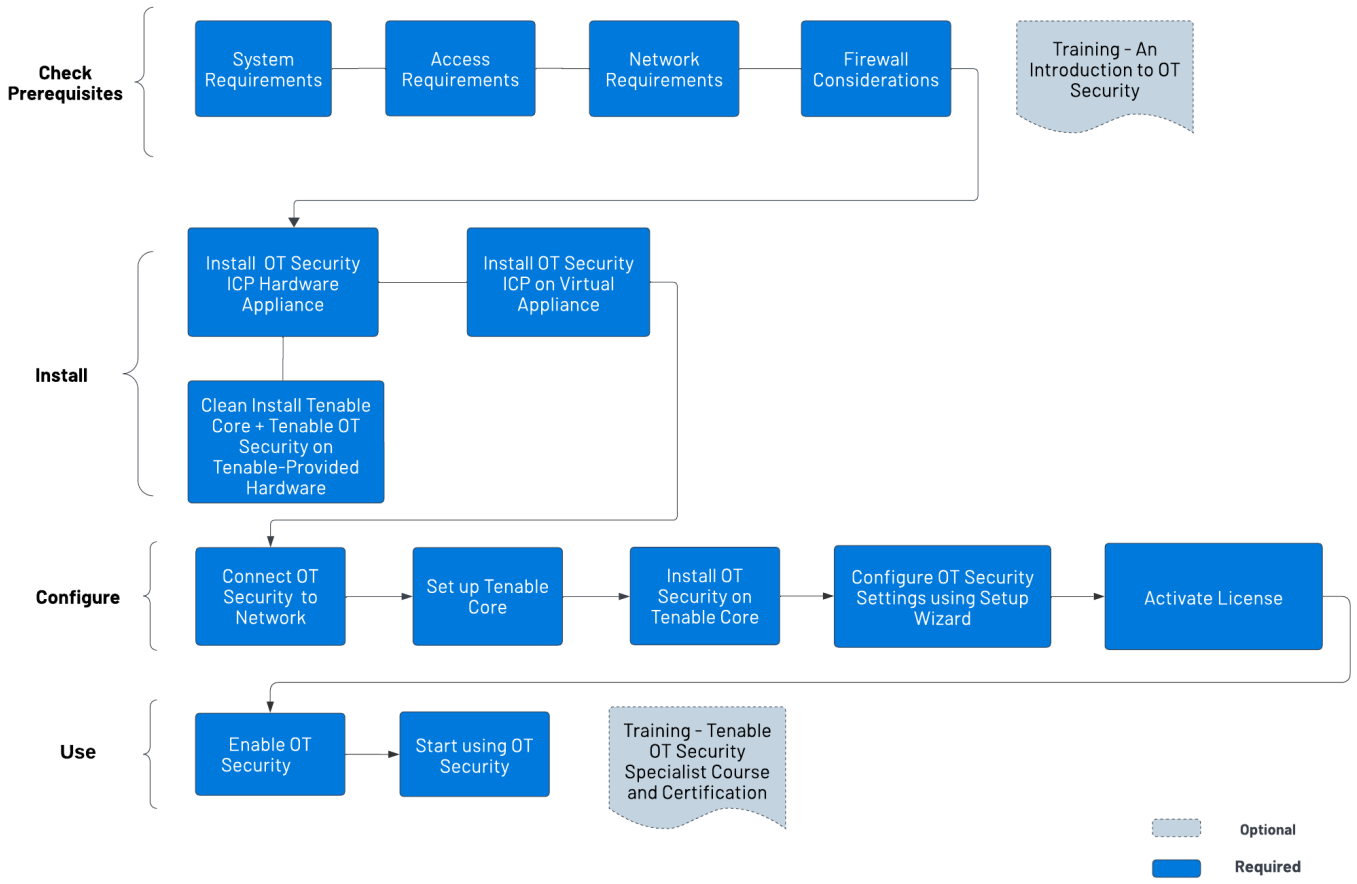
期限切れのライセンス

購入した Tenable OT Security ライセンスは契約期間中ずっと有効です。ライセンスの有効期限が切れる 30 日前になると、ユーザーインターフェースに警告が表示されます。この更新期間中に、Tenable の担当者と連携して、製品の追加や削除、ライセンス数の変更を行ってください。

ライセンスの有効期限が切れると、Tenable OT Security は無効になり、使用できなくなります。

OT Security を使い始める

次の開始手順に従って、OT Security をインストールし、使用を開始します。



始める前に

- 前提条件 – 前提条件 のシステム、ハードウェア、仮想、ライセンス要件を確認します。
  - システム要件 – 要件を確認して、システム要件 + OT Security をインストールして実行します。
  - アクセス要件 – インターネットおよびポート要件を確認して、アクセス要件 + OT Security を実行します。
  - ネットワークに関する考慮事項 – ネットワークインターフェースを確認して、ネットワークに関する考慮事項 に接続します。

- ファイヤーウォールの考慮事項 – OT Security が正しく機能するために開いている必要があるポートを確認します。
- Tenable OT Security の概要 - OT Security を理解するためのトレーニング資料を参照します。

OT Security ICP のインストール

OT Security は、Tenable Core オペレーティングシステム上で実行されるアプリケーションです。そのため、Tenable Core の基本要件に準じていなければなりません。次のガイドラインに従って、Tenable Core + OT Security をインストールして設定します。

OT Security をインストールするには、次のようにします。

1. OT Security ICP のインストール
   - OT Security ICP ハードウェアアプライアンスのインストール - OT Security をハードウェアアプライアンスとしてセットアップします。

     注意: Tenable 提供の Tenable Core ハードウェアには Tenable Core + OT Security がプリインストールされています。古いアプライアンスや旧式のアプライアンスをインストールする場合は、クリーンインストールを選択することもできます。詳細は、Tenable 提供ハードウェアへの Tenable Core + Tenable OT Security のクリーンインストールを参照してください。
   - OT Security ICP 仮想アプライアンスのインストール – 標準の仮想マシン設定を含む、事前設定されている `.ova` ファイルを使用して Tenable Core + OT Security を仮想マシンとしてデプロイするか、インストール `.iso` ファイルを使用してアプライアンスをカスタマイズします。
2. OT Security のネットワーク接続 – OT Security ハードウェアおよび仮想アプライアンスをネットワークに接続します。
3. OT Security ICP の設定
   a. Tenable Core のセットアップ – CLI またはユーザーインターフェースを使用して Tenable Core のセットアップを設定します。
   b. Tenable Core への OT Security のインストール - Tenable Core での Tenable Core への OT Security のインストールのインストールを手動で完了します。

c. セットアップウィザードを使用したOT Securityの設定 – セットアップウィザードを使用して、セットアップウィザードを使用したOT Securityの設定の基本設定を行います。

- OT Securityコンソールにログインし、ユーザー情報、デバイス、システム時刻、ポート分離を設定します。

4. OT Securityライセンスのアクティベーション – OT Securityのインストール完了後、ライセンスをアクティブ化します。

OT Securityの使用

起動OT Security

1. OT Securityの有効化 – ライセンスをアクティブ化した後、OT Securityを有効化します。
2. OT Securityの使用の開始 – 監視対象ネットワーク、ポート分離、ユーザー、グループ、認証サーバーなどを設定して、OT Securityの使用を開始します。

> **ヒント**: 実践的な経験を積み、Tenable OT Securityスペシャリスト認定を取得するには、Tenable OT Securityスペシャリストコースを受講してください。

前提条件

> **目的**: ICPのインストールを成功させるために必要なものがすべて揃っていることを確認します。

Tenable OT Securityは、Tenable Coreオペレーティングシステム上で実行されるアプリケーションです。そのため、Tenable Coreの基本要件に準じていなければなりません。

Tenable Core + Tenable OT Securityは、ハードウェアにデプロイすることも、仮想マシンアプライアンスとしてデプロイすることもできます。仮想マシンのデプロイメントの場合は、ハードウェア要件に記載されている最小要件を満たす必要があります。

ハードウェア要件

複数のサイズのTenable Core + Tenable OT Security専用ハードウェアアプライアンスが利用可能です(別途購入)。ハードウェアの仕様については、Tenable OT Security物理ハードウェアシートを参照してください。

Tenable Core オペレーティングシステムと Tenable OT Security アプリケーションは、提供されているすべてのハードウェアアプライアンスにプリインストールされています。

同じ要件を満たすカスタムハードウェアに Tenable Core + Tenable OT Security をインストールすることもできます。手順については、Tenable サポートまたは Customer Success Manager にお問い合わせください。

Tenable Core + Tenable OT Security の要件に関する詳細については、以下を参照してください。

- システム要件
- アクセス要件

仮想アプライアンス要件

Tenable Core + Tenable OT Security は次の方法でデプロイできます。

- `.ova` ファイルの使用 - このファイルはすぐにデプロイできる状態になっており、標準およびサポートされているすべての仮想マシン設定が含まれています。
- `.iso` ファイルの使用 - これは汎用インストールディスクイメージです。要件を満たし適切に設定された仮想マシンにデプロイしてください。

ライセンス要件

OT Security のライセンスについての一般的な情報は、OT Security ライセンスコンポーネントを参照してください。

ライセンス付与のワークフローについては、OT Security ライセンスのアクティベーションを参照してください。

システム要件

Tenable Core + OT Security または Tenable OT Security センサーをインストールして実行するには、アプリケーションとシステムが次の要件を満たしている必要があります。

注意: インストール中またはデプロイメント中に問題が発生した場合でも、ご使用のホストオペレーティングシステムに関連する問題については、Tenable サポート でサポートすることはできません。

環境	Tenable Core ファイル形式	追加情報

仮想マシン	VMware	.ova ファイル	OT Security ICP 仮想アプライアンスのインストール
ハードウェア Tenable 提供のハードウェア		.iso イメージ	ハードウェアへの Tenable Core のインストール (missing or bad snippet)

注意: パッケージを使用して他の環境で Tenable Core を実行することもできますが、Tenable はその手順に関するドキュメントを提供していません。

(missing or bad snippet)

Tenable Core + OT Security には、最新バージョンの OT Security が含まれています。

ハイパーバイザー[1]に OT Security をインストールすることも、Tenable Core を実行しているユーザー提供のハードウェアに直接インストールすることもできます。

注意: Tenable は、他の Tenable アプリケーションと共有されている環境で Tenable Core + OT Security を実行することをお勧めしません。たとえば、2 つの製品を、同じ仮想マシンや同じ Tenable Core システムにインストールしたりすることです。

ストレージ要件

Tenable では、最高のパフォーマンスを実現するために、ダイレクトアタッチストレージ (DAS) デバイス、できればソリッドステートドライブ (SSD) に OT Security をインストールすることを推奨しています。Tenable は、長期間使用できるように、1 日あたりのドライブ書き込み数 (DWPD) レーティングが高いソリッドステートストレージ (SSS) の使用を強くお勧めします。

Tenable は、ネットワークアタッチストレージ (NAS) デバイスへの OT Security のインストールをサポートしていません。このようなケースでは、ストレージのレイテンシが 10 ミリ秒以下のストレージエリアネットワーク (SAN)、または Tenable ハードウェアアプライアンスを代わりに使用すると良いでしょう。

ディスク容量要件

エンタープライズネットワークのパフォーマンス、容量、プロトコル、アクティビティは、各社で大きく異なります。デプロイメントにあたり検討すべきリソース要件には、ネットワーク理論速度、監視対象ネットワークの

[1]ハイパーバイザーは、VMWare により公式にサポートされており、Hyper-V、KVM で動作することが確認されていなければなりません。

規模、アプリケーションの設定などがあります。プロセッサ、メモリ、ネットワークカードの選択は、これらのデプロイメント設定に大きく依存します。必要なディスク容量は、データ量やシステムにデータを保存する期間に基づく使用状況によって異なります。

OT Security は、監視対象トラフィックのフルパケットキャプチャを実行する必要があります。また、OT Security が保存するポリシーイベントデータのサイズは、デバイスの数と環境の種類によって異なります。

圧縮係数 0.25 に基づいた 1 日あたりのストレージ要件 (GB/日) は、トラフィックレート (Mbps) * 2.7 で計算できます。

2 つのセンサーがそれぞれ 23 Mbps の SPAN トラフィックを受信する場合、1 日あたりのストレージ要件 (GB/日) は、(23*2)*2.7=124 GB と計算し、これがトラフィックストレージの 1 日の容量になります。

注意: コンプライアンスまたはセキュリティ要件により、最大 30 日間のトラフィックを保存する必要がある場合は、この要件を満たすために 3.75 TB の PCAP (パケットキャプチャ) ストレージドライブが必要になります。保存されたトラフィックデータが最大サイズに達すると、OT Security は最も古い PCAP データを上書きし、それを新しいトラフィックに置き換えます。

ICP システム要件ガイドライン (仮想または Tenable Core)

最大 SPAN/TAP スループット (Mbps)	CPU コア[1]	メモリ (DDR4)	ストレージ要件	ネットワークインターフェース
50 Mbps 以下	4	16GB RAM	128 GB	最小 4 x 1 Gbps
50 ~ 150 Mbps	16	32 GB RAM	512 GB	最小 4 x 1 Gbps
150 ~ 300 Mbps	32	64 GB RAM	1 TB	最小 4 x 1 Gbps
300 Mbps ~ 1 GB	32-64	128 GB RAM 以上	2 TB 以上	最小 4 x 1 Gbps

ディスクパーティション要件

OT Security では、次のようにマウントされたパーティションを使用します。

パーティション	コンテンツ

/	オペレーティングシステム
/opt	アプリケーションおよびデータベースファイル
/var/pcap	パケット キャプチャ(フル パケット キャプチャ、イベント 、クエリ)

標準プロセスでは、これらのパーティションを同じディスクに配置します。Tenable では、スループットを向上させるために、これらを別々のディスク上のパーティションに移動することを推奨しています。OT Security はディスクを集中的に使用するアプリケーションなので、SSD などの読み取り/書き込み速度の速いディスクを使用すると、最高のパフォーマンスが得られます。お客様が用意するハードウェアへのインストールで OT Security のパケット キャプチャ機能を使用する場合、Tenable は、DWPD レーティングが高い SSD の使用を推奨しています。

ヒント: 独立ディスクの冗長配列 (RAID 0) を付けた設定でハードウェアプラットフォームに OT Security をデプロイすると、パフォーマンスが大幅に向上します。

ヒント: Tenable は、最大規模のお客様にも RAID ディスクを必須にすることはありません。しかし、100 万件以上の脆弱性を管理するお客様でより高速な RAID ディスクを使用した事例では、クエリの応答時間が数秒から 1 秒未満に短縮されました。

ネットワークインターフェース要件

OT Security をインストールする前に、デバイスに 4 つのネットワークインターフェースが存在している必要があります。Tenable はギガビット インターフェースの使用を推奨しています。VMWare OVA は、これらのインターフェースを自動的に作成します。ISO をお客様のハードウェアにインストールする場合は、これらのインターフェースを手動で作成してください。

注意: Tenable は、10G ネットワークカードの使用で SR-IOV をサポートしておらず、10G ネットワークカードを使用しても 10G の速度は保証されていません。

NIC 要件

ハードウェアまたは仮想環境に Tenable Core + OT Security をインストールした場合、**nic0** (192.168.1.5) と nic3 (192.168.3.3) に静的 IP アドレスが設定されます。他のネットワークインターフェースコントローラー (NIC) は DHCP を使用します。

VMware に Tenable Core + OT Security をデプロイした場合、**nic3** (192.168.3.3) に静的 IP アドレスが設定されます。他の NIC は DHCP を使用します。Tenable Core **nic1** MAC アドレスが、VMware パッシブス

キャン設定の NIC MAC アドレスと一致することを確認してください。必要なら、VMware の設定を変更して Tenable Core MAC アドレスと一致させてください。

詳細については、Manually Configure a Static IP Address (手動による静的 IP アドレスの設定)、Manage System Networking (システムネットワークの管理)、および *VMware* ドキュメントを参照してください。

[1]CPU コアは物理コアを指し、サーバークラスの CPU (Xeon、Opteron) を想定しています。

アクセス要件

デプロイメントは次の要件を満たす必要があります。

- インターネット要件
- ポート要件

インターネット要件

Tenable Core ファイルをダウンロードしてオンラインインストールを実行するには、インターネットアクセスが必要です。

マシンにファイルを転送した後、Tenable Core をデプロイまたはアップデートするためのインターネットアクセスの要件は、ご使用の環境によって異なります。

> **注意**: オンライン ISO からインストールするには (およびオンラインアップデートを入手するには)、`appliance.cloud.tenable.com` にアクセスでき、スキャンジョブを取得するには `sensor.cloud.tenable.com` にアクセスできなければなりません。

環境		Tenable Core 形式	インターネット要件
仮想マシン	VMware	`.ova` ファイル	Tenable Core のデプロイまたはアップデートに、インターネットアクセスは不要です。
ハードウェア		`.iso` イメージ	Tenable Core のインストールまたはアップデートに、インターネットアクセスが必要です。

ヒント: オフラインの .iso ファイルを使ってアップデートをインストールする場合は、インターネットアクセスは不要です。詳細は、Update Tenable Core Offline (Tenable Core のオフラインアップデート) を参照してください。

ポート要件

Tenable Core デプロイメントでは、受信と送信のトラフィック用の特定のポートへのアクセスが必要です。Tenable Security Center には、アプリケーション固有のポートアクセスも必要です。詳細は、(missing or bad snippet)のポート要件を参照してください。OT Securityには、アプリケーション固有のポートアクセスも必要です。詳細は、ファイヤーウォールの考慮事項を参照してください。

受信トラフィック

次のポートへの受信トラフィックを許可します。

注意: 受信トラフィックとは、Tenable Core を設定しているユーザーからのトラフィックを指します。

ポート	トラフィック
TCP 22	受信 SSH 接続
TCP 443	OT Security インターフェースへの受信通信
TCP 8000	Tenable Core インターフェースへの受信 HTTPS 通信

送信トラフィック

次のポートへの送信トラフィックを許可します。

ポート	トラフィック
TCP 22	リモートストレージ接続を含む、送信 SSH 接続
TCP 443	システムアップデート用の `appliance.cloud.tenable.com` と `sensor.cloud.tenable.com` の各サーバーへの送信通信
UDP 53	OT Security および Tenable Core の送信 DNS 通信

ネットワークに関する考慮事項

OT Security アプライアンス(物理と仮想の両方)は、次のネットワークインターフェースに到達する必要があります。

管理とアクティブクエリのインターフェース

- アプライアンスの管理と設定を行うネットワークにアクセスできる IP アドレスで、インターフェースを設定します。
- アプライアンスがネットワーク上の資産にアクセスし、アクティブクエリを実行できるようにします(推奨、ただしオプション)。
- 2 つの異なるネットワークインターフェースで分割できるようにします。個別の管理ポートの接続(ポート分離オプションの場合)を参照してください。

監視インターフェース

- 分析のためにトラフィックをパッシブモニタリングして収集します。
- スイッチのミラーリング、スイッチポートアナライザー(SPAN)、リモートスイッチポートアナライザー(RSPAN)のいずれかのデスティネーションインターフェースに接続されている必要があります。
- (オプション)センサーおよびカプセル化リモート SPAN(ERSPAN)設定を使用して、アプライアンスインターフェースに直接ミラーリングできないトラフィックを監視します。

ファイヤーウォールの考慮事項

OT Security 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に、オープンポートを緻密に計画することは重要です。次の表は、OT Security ICP および OT Security センサーで使用するために予約するポート、アクティブクエリを実行するために必要なポート、Tenable Vulnerability Management や Tenable Security Center との統合に必要なポートを示しています。

注意: ファイヤーウォールの通過を許可する必要がある Tenable のウェブサイトとドメインのリストについては、ナレッジベースの記事を参照してください。

OT Security Core プラットフォーム

OT Security 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 および TCP 28304	OT センサー	センサーの認証、ペアリング、センサー情報の受信。
アウトバウンド	TCP 443 および TCP 28305	OT Security EM	ICP と EM のペアリング
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 28304	ICP/OT Security	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 Security Center	統合のためにデータを送信
アウトバウンド*	TCP 443	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 または 587	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	ポリシーイベントアラートと syslog メッセージを送信する
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	TCP 389 または	AD サーバー	AD LDAP 認証

ンド*	636		
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 *.nessus.org	自動プラグイン、アプリケーション、OS アップデート**
アウトバウンド	TCP 10146 (セキュアポート)	IoT コネクタ	ICP を IoT コネクタエージェントに接続する

*オプションサービス

**オフライン手順が利用可能

OT Security センサー

OT Security 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
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	UDP 53	DNS サーバー	名前解決

ド*			
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
アウトバウンド	TCP 28303	ICP/OT Security センサーから通信を送信、ICP/OT Security で受信	認証されていない、もしくはパッシブのみのセンサー接続
アウトバウンド	TCP 443 および TCP 28304	ICP/OT Security センサーから通信を送信、ICP/OT Security で受信	センサーと ICP 間の認証済み / 安全なトンネル

*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	UDP/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

注意: デバイスが使用するポートは、ベンダーや製品ラインによって異なります。アクティブなクエリを成功させるために必要な、関連するポートとプロトコルのリストについては、識別と詳細のクエリを参照してください。

OT Security の統合

Tenable Vulnerability Management および Tenable Security Center 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 Vulnerability Management の統合
アウトバウンド	TCP 443	Tenable Security Center	Tenable Security Center の統合

識別クエリと詳細クエリ

識別クエリと詳細クエリでは、次のポートを使用できます。

注意: 場合によっては、OT Security またはそのセンサーが資産に関連するポートに到達するために、ファイヤーウォールのポートを開放する必要があります。

ポート	ポート名
21	FTP
80	HTTP
102	Step-7 / S7+

111	Emerson OVATION
135	WMI
161	SNMP
443	HTTPS
502	MODBUS / MMS
1911	Niagara FOX
2001	Profibus
2222	PCCC_AB-ETH
2404	IEC 60870-5
3500	Bachmann
4000	Emerson ROC
4911	Niagara FOX TLS
5002	Mitsubishi MELSEC
5007	Mitsubishi MELSEC
5432	PSQL / SEL
18245	SRTP
20000	DNP3
20256	PCOM
44818	EthernetIP / CIP
47808	BACNET (udp)
48898	ADS
55553	Honeywell CEE
55565	Honeywell FTE

OT Security ICP のインストール

目的: OT Security ICP をインストールして使用できる状態にします。

始める前に

- 前提条件を参照してください。

OT Security ICP をインストールしてネットワークに接続するには、必要に応じて次の手順に従います。

- OT Security ICP ハードウェアアプライアンスのインストール

  注意: Tenable 提供の Tenable Core ハードウェアには Tenable Core + OT Security がプリインストールされています。古いアプライアンスや旧式のアプライアンスをインストールする場合は、クリーンインストールを選択することもできます。詳細は、Tenable 提供ハードウェアへの Tenable Core + Tenable OT Security のクリーンインストールを参照してください。

- OT Security ICP 仮想アプライアンスのインストール

次のステップ

- OT Security のネットワーク接続

OT Security ICP ハードウェアアプライアンスのインストール

OT Security アプライアンスはラックに取り付けるか、または机などの平面に設置できます。

ヒント: Tenable は、アプライアンスをラックやその他の離れた場所に移動する前に、普段使用しているデスクで Tenable Core のセットアップ および OT Security セットアップウィザードで説明されている基本設定とセットアップを実行しておくことをお勧めします。

ラックマウント

OT Security アプライアンスを標準 19 インチラックに取り付けるには、次のようにします。

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。

   注意:
   - 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
   - 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を確認してください

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ネジ (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. 付属の AC 電源ケーブル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

OT Security アプライアンスを平面に設置するには、次のようにします。

1. アプライアンスユニットを、乾いた水平な面 (机など) に置きます。

   注意:
   - 机上が平らで乾いていることを確認してください。
   - 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にある通気孔がふさがれていないことを確認してください
   - 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。

2. 付属の AC 電源ケーブル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。

接続の詳細については、ネットワークに関する考慮事項を参照してください。

次の手順

OT Security のネットワーク接続

Tenable 提供ハードウェアへの Tenable Core + Tenable OT Security のクリーンインストール

Tenable Core + OT Security は、Tenable 提供の公式ハードウェアに標準装備でプリインストールされています。場合によっては、クリーンインストール(再フラッシュとも呼ばれる)が推奨されています。

> **注意**: 新しいアプライアンスを受け取ったばかりの場合は、この手順をスキップできます。

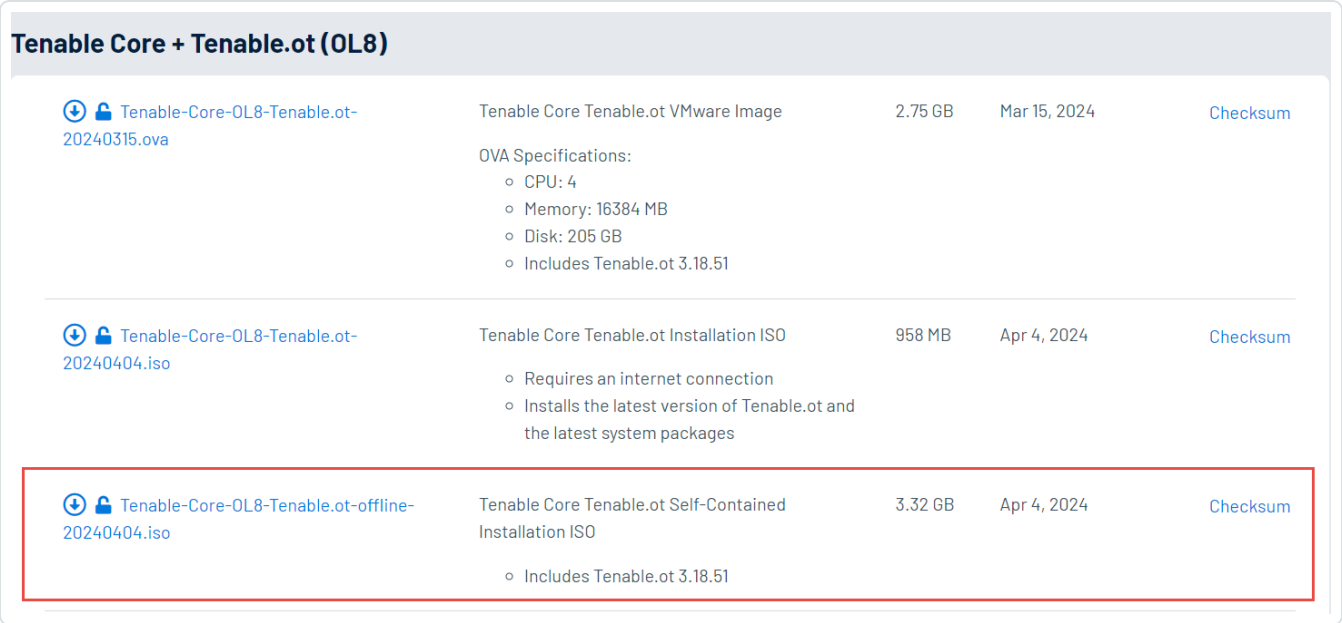
始める前に

以下が揃っていることを確認します。

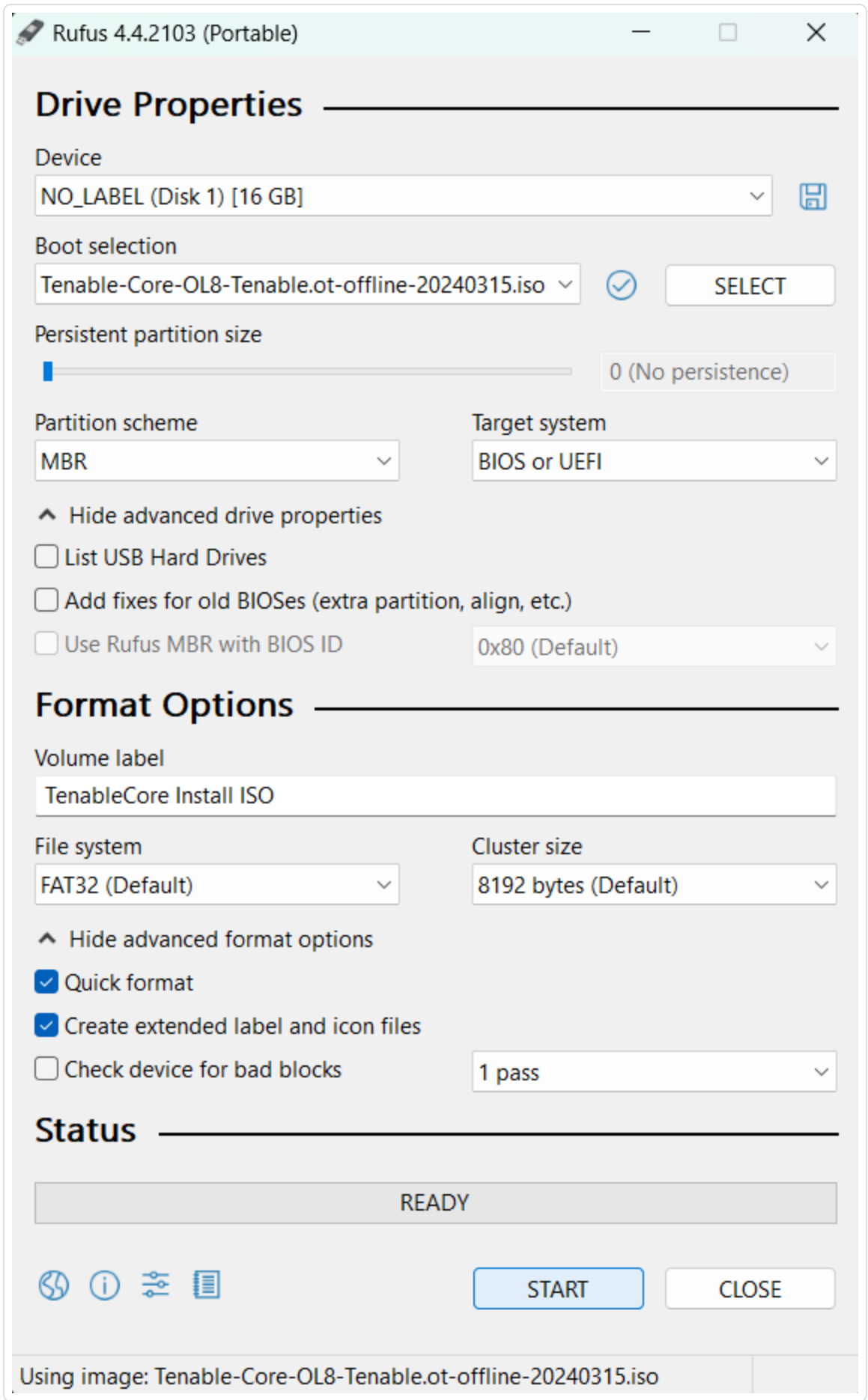
- 起動可能な USB フラッシュドライブをフォーマットして作成するためのアプリケーション(Rufus など)
- シリアルケーブル
- PuTTY などのシリアルターミナルアプリケーション
- 8 GB 以上の USB ドライブ

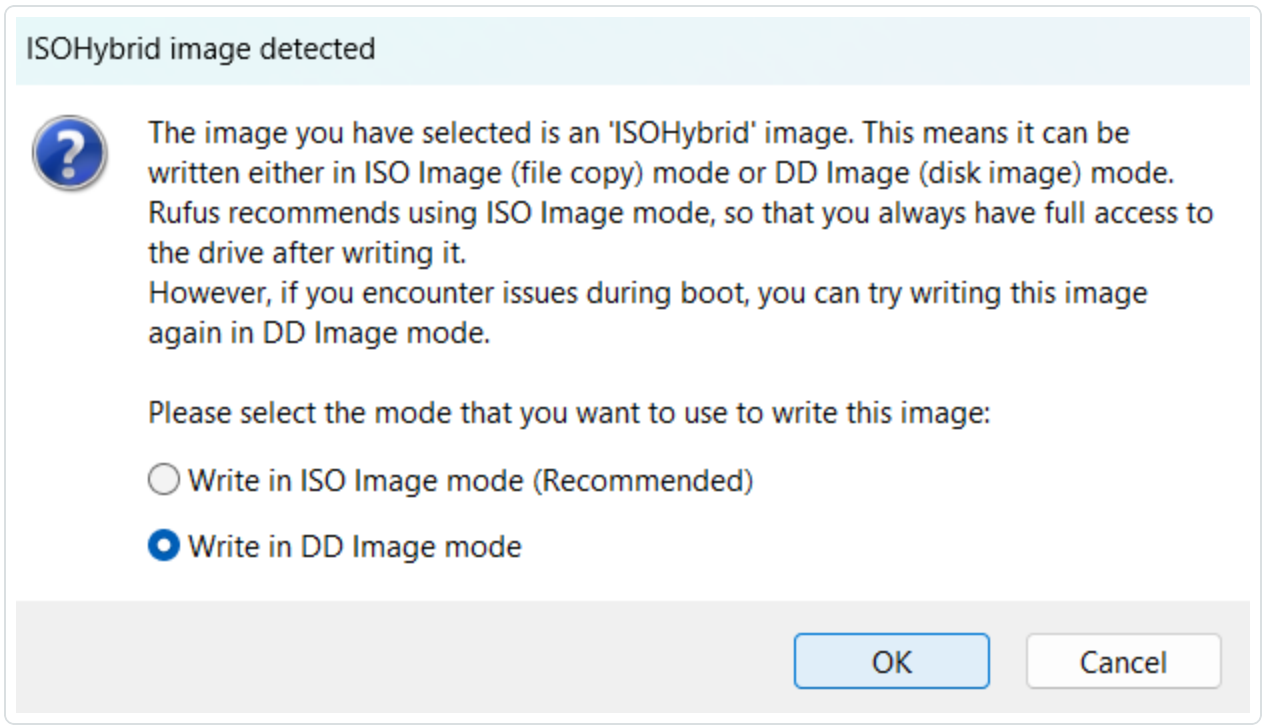
Tenable Core + OT Security ISO ファイルをインストールするには、次のようにします。

1. Tenable のダウンロードから最新のオフライン ISO ファイルをダウンロードします。

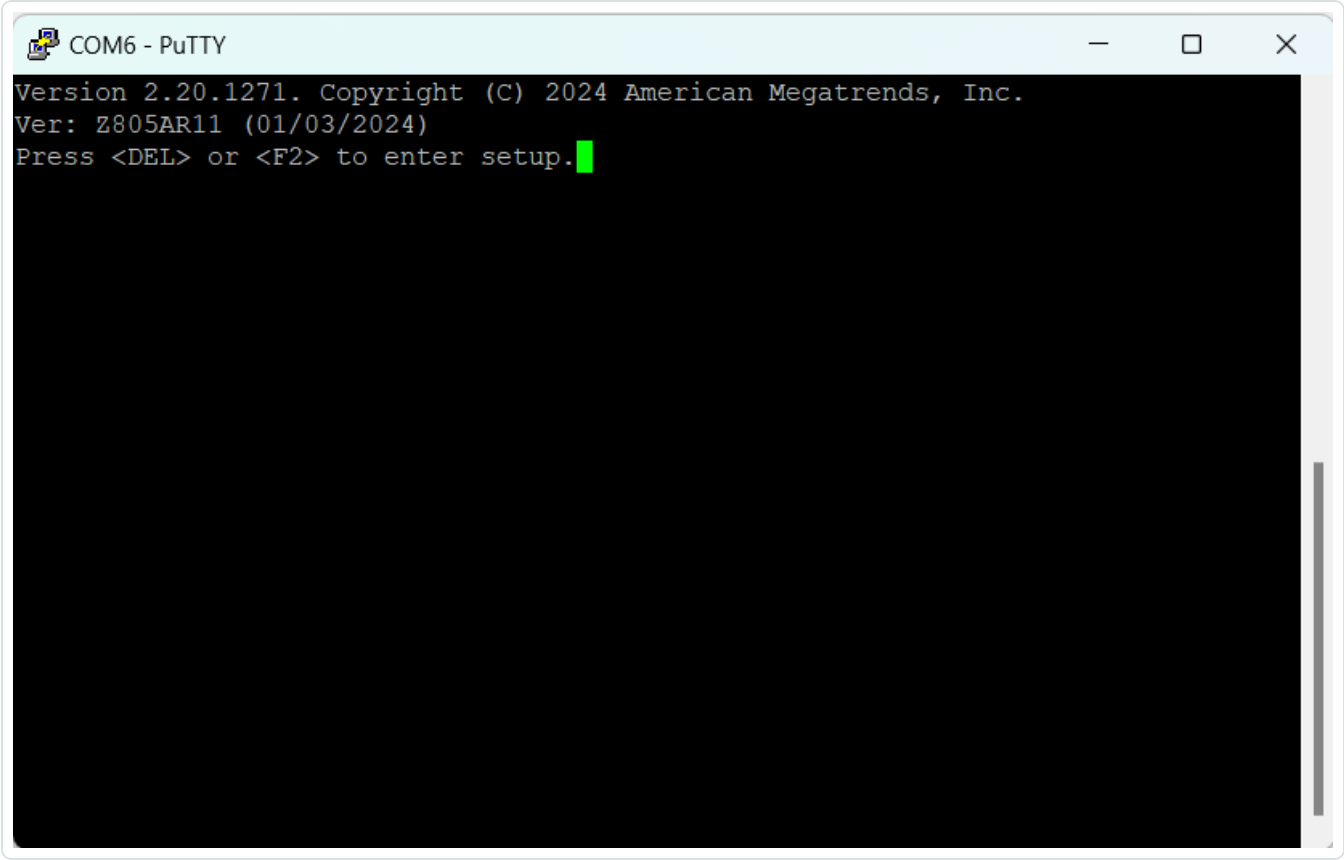


2. USB ドライブを PC に差し込み、ISO を DD モードでフラッシュドライブにフラッシュします。

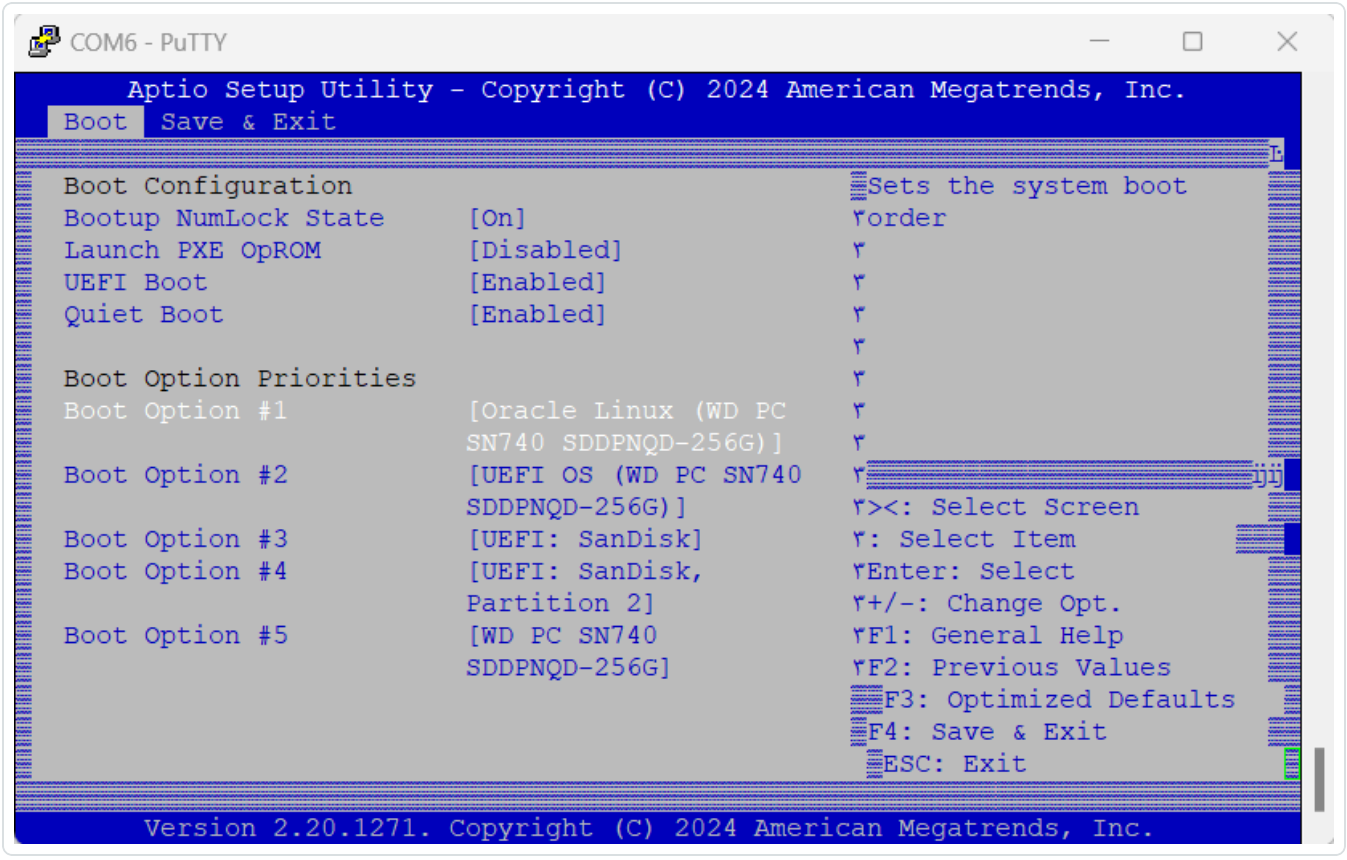

Rufus 4.4.2103 (Portable)
Drive Properties
Device
NO_LABEL (Disk 1) [16 GB]
Boot selection
Tenable-Core-OL8-Tenable.ot-offline-20240315.iso
SELECT
Persistent partition size
0 (No persistence)
Partition scheme
MBR
Target system
BIOS or UEFI
Hide advanced drive properties
List USB Hard Drives
Add fixes for old BIOSes (extra partition, align, etc.)
Use Rufus MBR with BIOS ID
0x80 (Default)
Format Options
Volume label
TenableCore Install ISO
File system
FAT32 (Default)
Cluster size
8192 bytes (Default)
Hide advanced format options
Quick format
Create extended label and icon files
Check device for bad blocks
1 pass
Status
READY
START
CLOSE
Using image: Tenable-Core-OL8-Tenable.ot-offline-20240315.iso



3. 終了したら、USB ドライブを OT Security アプライアンスの USB ポートに差し込みます。
4. コンソールシリアルインターフェースを通してアプライアンスに接続し (8N1 設定で 115200 bps のボーレート)、電源を入れます。

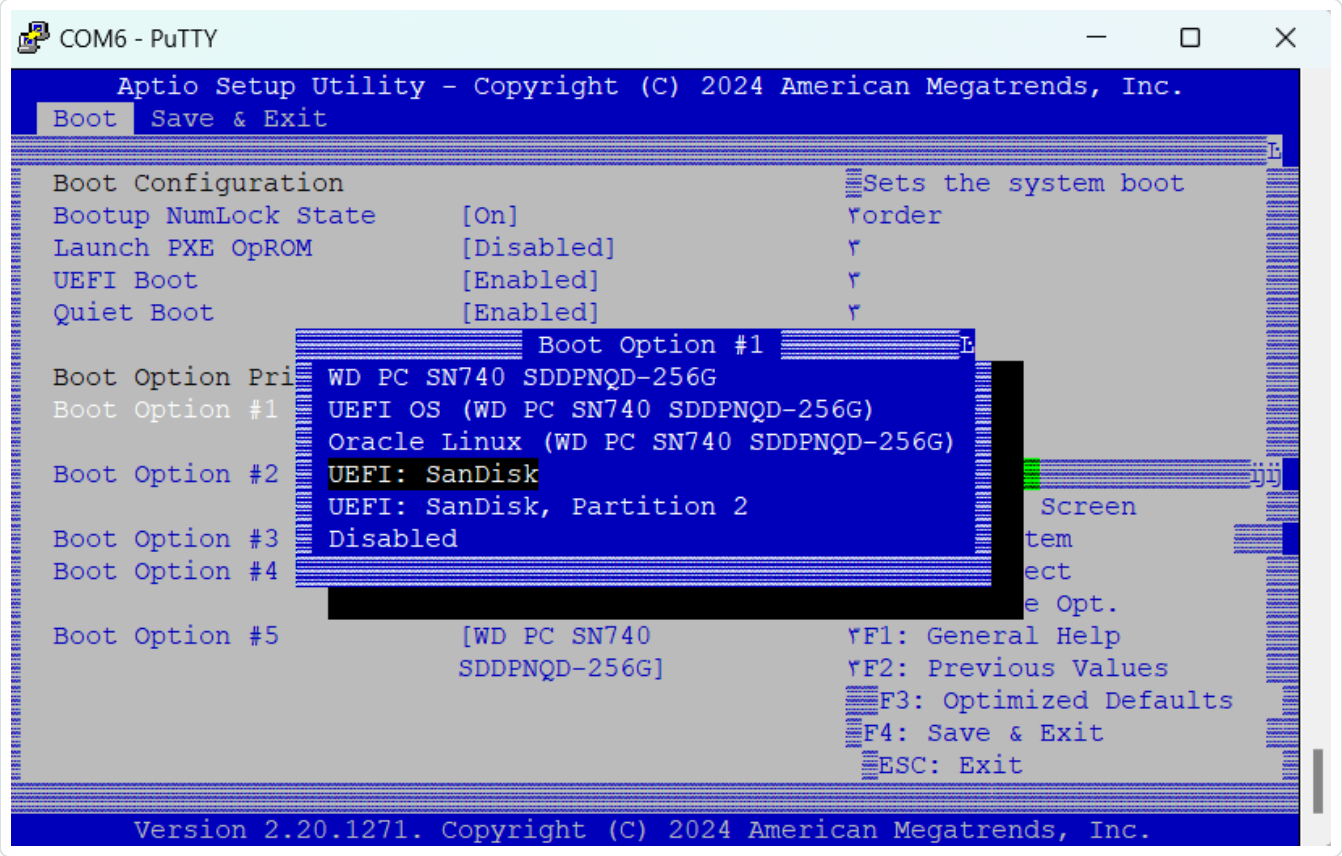


5. プロンプトが表示されたら、<DEL>を押してセットアップに入ります。
6. システムセットアップで、矢印キーを使用して**[Boot]**(起動)セクションに移動します。



7. **[Boot Option #1]**(起動オプション #1)を選択し、USB ドライブに変更します。

> **注意**: UEFI (Unified Extensible Firmware Interface) オプションを使用してください。

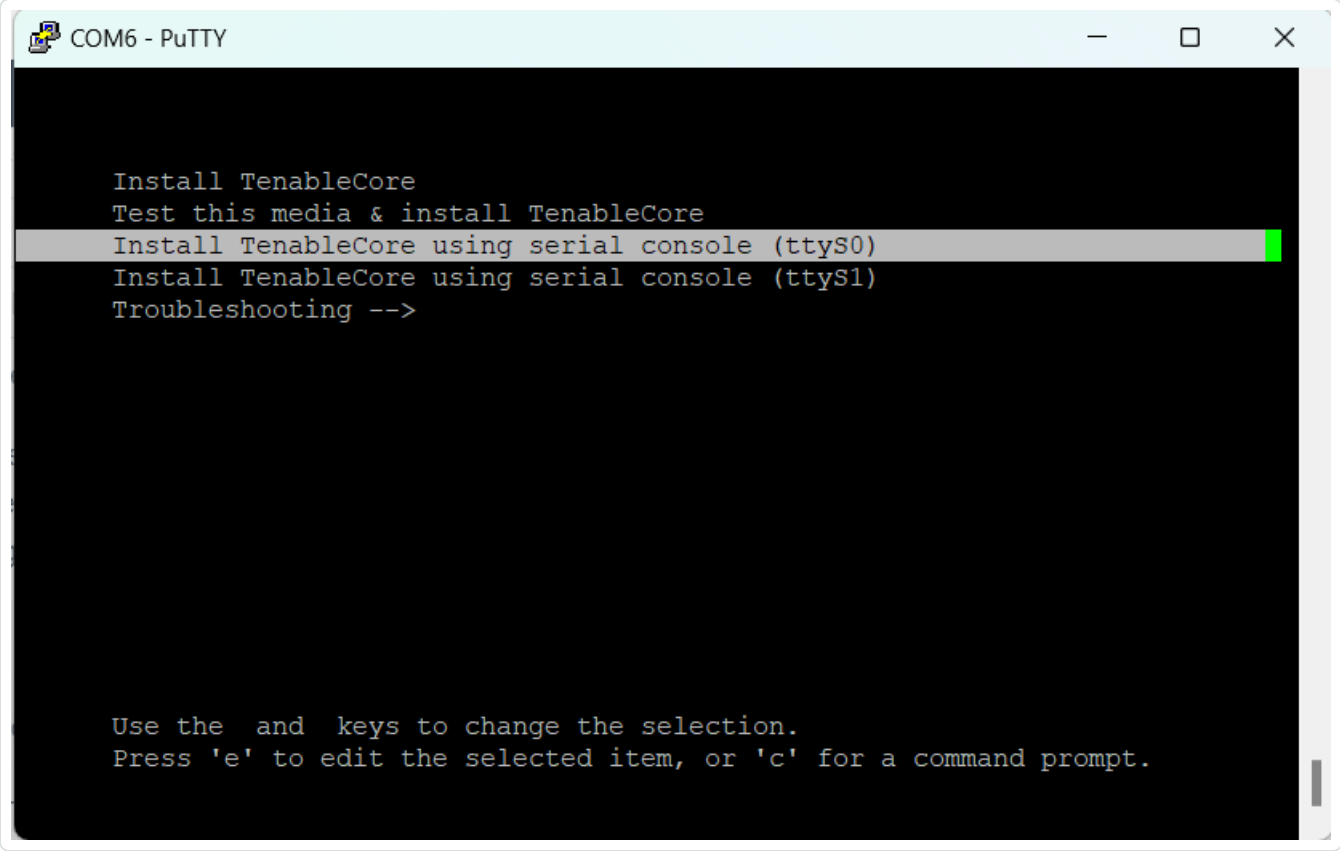


注意: アプライアンスでサポートされているなら「ワンショット起動」機能を使用できます。

8. **[Save & Exit]**(保存して終了)セクションで、**[Save Changes and Reset]**(変更を保存してリセット)を選択します。

9. アプライアンスが再起動した後、プロンプトで **[Install TenableCore using serial console (ttyS0)]**(シリアルコンソール(ttyS0)を使用して TenableCore をインストールする)を選択します。これにより、インストール出力がアプライアンスのシリアルコンソール接続に確実にプッシュされます。

注意: ハードウェアがモニター出力 (VGA、HDMI など)をサポートしている場合は、**[Install TenableCore]**(TenableCore のインストール)オプションを選択できます。このケースでは、インストールの出力は接続したモニターに表示されます。



アプライアンスのインストールが完了するのを待ちます。システムが複数回再起動する場合があります。ログインプロンプトが表示されたら、インストールは完了です。一部のアプライアンスでは、インストール完了後にシステムがシャットダウンすることがあります。

> **注意**: ログインプロンプトが表示された後も、システムがいくつかのインストール手順を実行する場合があります。Tenable では、数分待ってから Tenable Core セットアップウィザードを開始することをお勧めします。

10. インストールが完了してから、USB ドライブを取り外します。

次の手順

[OT Security のネットワーク接続]

OT Security ICP 仮想アプライアンスのインストール

Tenable Core + OT Security を VMware 仮想マシンとしてデプロイするには、Tenable Core + OT Security **.ova** ファイルをダウンロードして、ハイパーバイザーにデプロイする必要があります。

注意: 事前設定されている .ova の代わりに .isoファイルをデプロイする場合は、次のようにしてください。

- Tenable Core + OT Security のシステム要件に従います。
- セットアップ方法を選択するプロンプトが表示されたら、**[Tenable Core のインストール]** を選択します。Tenable Core + Tenable OT Security のクリーンインストールを参照してください。
- 仮想マシンコンソールのインストールユーザーインターフェースを使用してインストールプロセスを実行し、モニタリングします。インストールプロセスは完全に自動化されているため、インストールが完全に完了するまでシステムを操作しないでください。

始める前に

- システム要件に記載されているように、使用環境がインスタンスの使用目的をサポートしていることを確認します。
- アクセス要件で説明されているように、インターネットとポートのアクセスがインスタンスの使用目的をサポートしていることを確認します。

VMware 仮想マシンとして Tenable Core + OT Security をデプロイする手順

1. Tenable ダウンロードページから Tenable Core + OT Security .ova ファイルをダウンロードします。
2. ハイパーバイザーで VMware 仮想マシンを開きます。
3. コンピューターから仮想マシンに、Tenable Core + OT Security VMware .ova ファイルをインポートします。.ova ファイルを仮想マシンにインポートする方法については、VMware ドキュメントを参照してください。
4. セットアッププロンプトで、所属組織のストレージニーズと要件、およびOT Securityシステム要件にある条件を満たすように仮想マシンを設定します。
5. Tenable Core + OT Security インスタンスを起動します。

   ターミナルウィンドウに仮想マシンの起動プロセスが表示されます。起動プロセスの完了には数分かかる場合があります。

   注意: ログインプロンプトが表示された後も、システムがいくつかの最終インストール手順を実行する場合があります。Tenableでは、数分待ってから Tenable Core セットアップウィザードを開始することをお勧めします。

注意: 組織のデータストレージニーズに対応するためにディスク容量を増やしたい場合は、Disk Management (ディスク管理) を参照してください。

次の手順

OT Security のネットワーク接続

OT Security のネットワーク接続

OT Security は、ネットワーク監視とアクティブクエリの両方に使用できます。詳細は、ネットワークに関する考慮事項を参照してください。

- **ネットワーク監視** – 適切なコントローラー/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します。
- **アクティブクエリ** – 適切なコントローラー/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します。

デフォルト設定では、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) を使用します。ただし、初期設定後に管理をポート 3 に設定して、管理ポートをアクティブクエリポートから分離できます。この設定が完了したら、個別の管理ポートの接続 (ポート分離) で説明されているように、ユニットのポート 3 をスイッチの標準ポートに接続して、管理を実行できます。

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

OT Security アプライアンスをネットワークに接続するには、次のようにします。

ハードウェアアプライアンスの場合

1. OT Security 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。

仮想アプライアンスの場合

.ova ファイルを使用してアプライアンスをデプロイした場合、そのアプライアンスには 4 つのネットワークインターフェースが事前設定されています。

.iso ファイルを使用してカスタム仮想アプライアンスをデプロイした場合は、必ずシステム要件で説明されている要件に従って仮想マシンを設定してください。VMware 仮想マシンのネットワーク設定について詳しくは、VMware ドキュメントを参照してください。

OT Security ICP の設定

目的: ソフトウェアのアクティベーションを準備します。

OT Security ICP をインストールしたら、OT Security を設定できます。設定には次の手順が含まれます。

1. Tenable Core のセットアップ – CLI またはユーザーインターフェースを使用して、Tenable Core の初期設定を完了します。
2. Tenable Core への OT Security のインストール – Tenable Core への OT Security のインストールを完了します。
3. セットアップウィザードを使用した OT Security の設定 – セットアップウィザードを使用して、OT Security ICP の基本設定を行います。

Tenable Core のセットアップ

Tenable Core の初期設定は、CLI と Tenable Core ユーザーインターフェースのどちらからでも行うことができます。

仮想アプライアンスのデプロイメントの設定を終了するには、Tenable Core ユーザーインターフェースを使う必要があります。

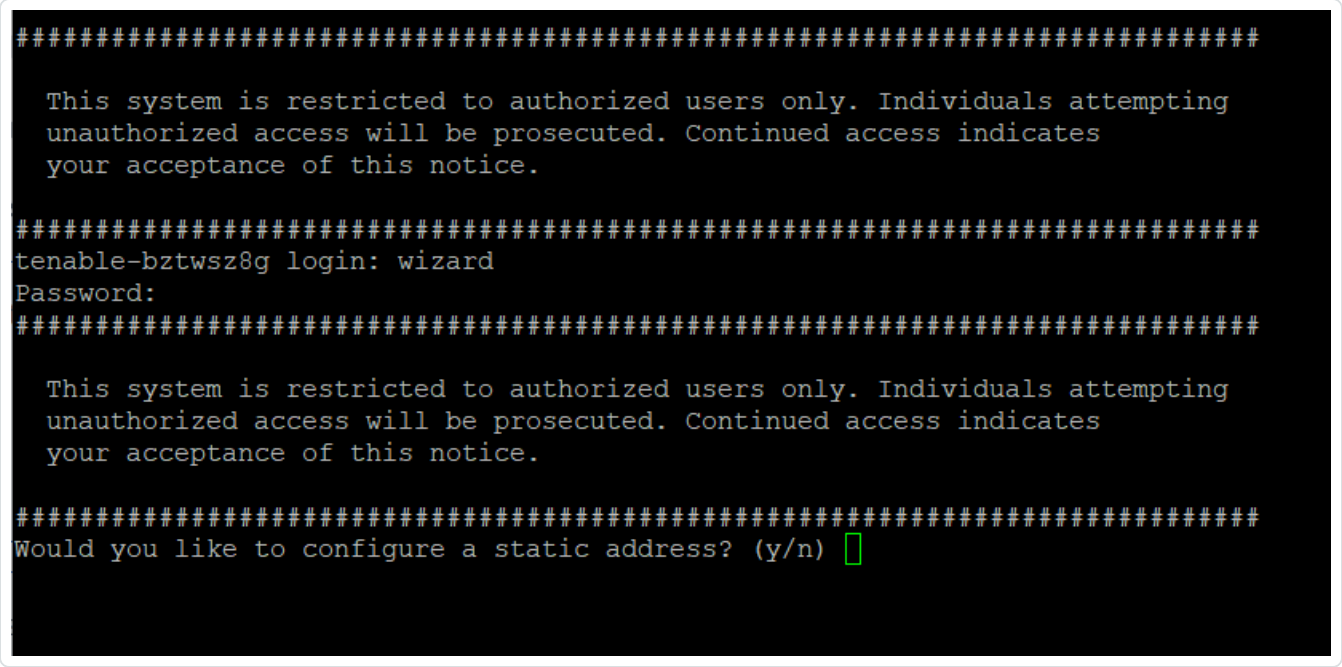
注意: セットアップウィザードが 30 分以内に完了しない場合は、アプライアンスを再起動してください。

CLI を使う初期設定 (オプション)

CLI を使用して Tenable Core を設定するには、次のようにします。

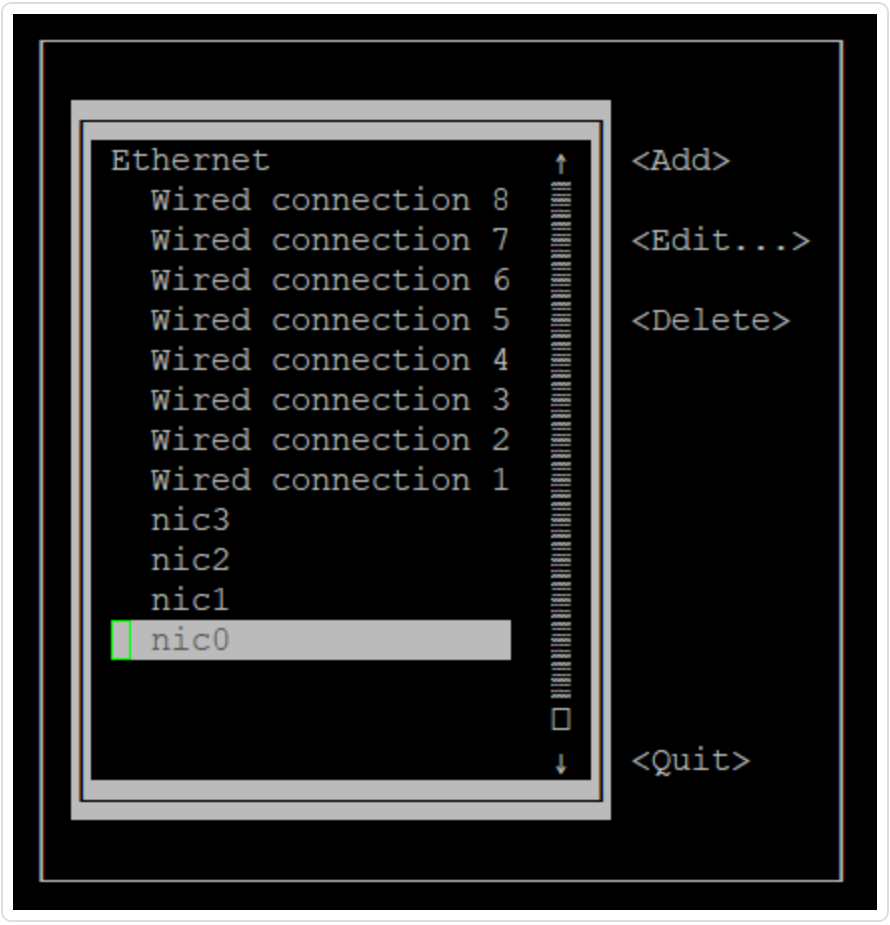
1. Tenable Core + OT Security のクリーンインストールで説明されているように、シリアルコンソールを使用して OT Security アプライアンスに接続します。
2. ユーザー名 `wizard`、パスワード `admin` を使用してログインします。

[ネットワークマネージャー] ターミナルインターフェースが表示されます。



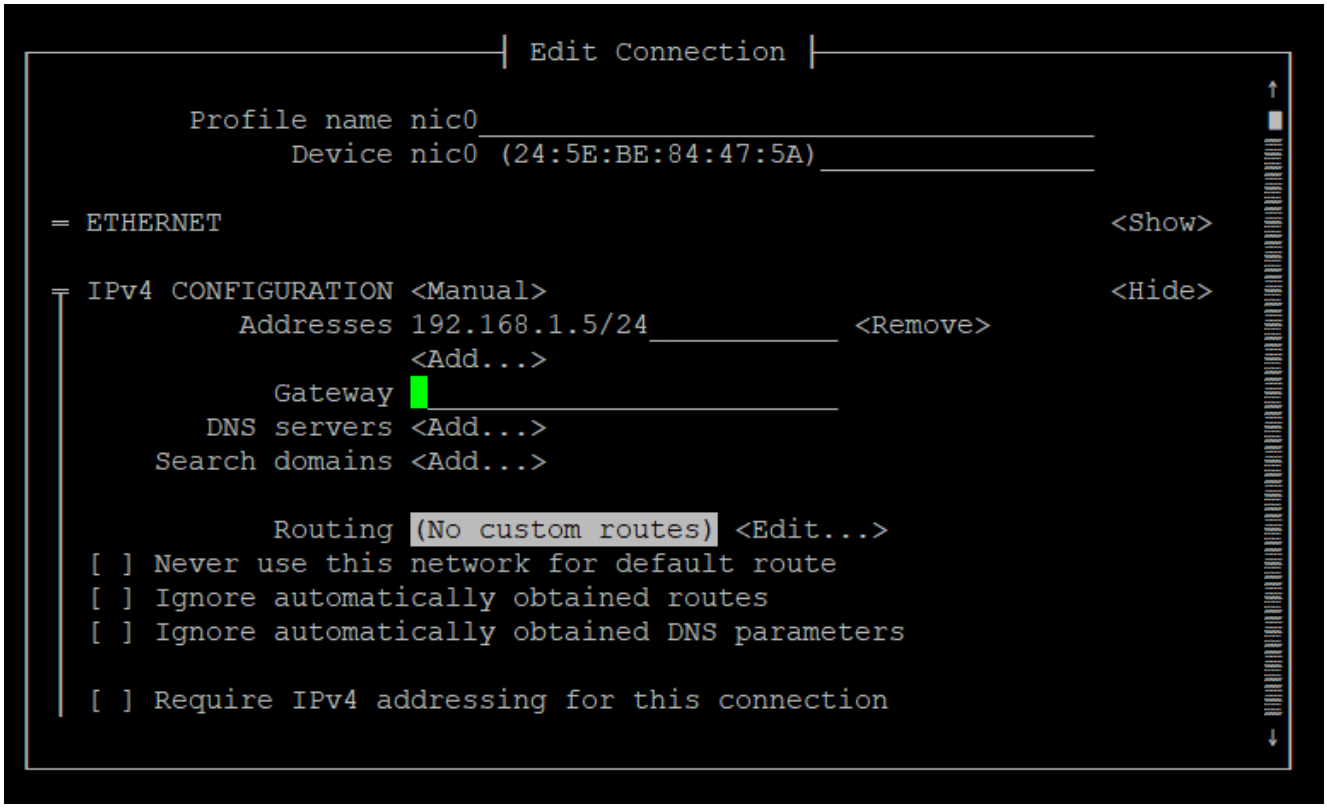
3. (オプション) 管理 IP アドレスを設定するには、**y** と入力します。

4. **nic0** (**split-port** 設定を使用する場合は **nic2**) を選択します。



5. **Enter** を押します。

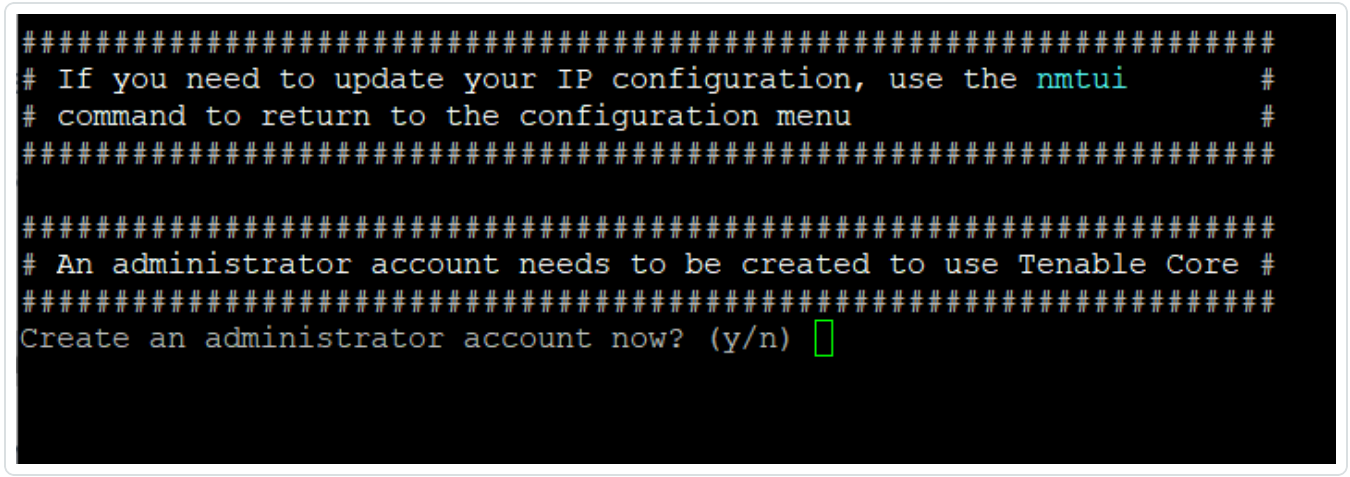
   [Edit Connection](接続の編集)ウィンドウが表示されます。



6. 矢印キーを使用して移動し、必要な IP アドレス、デフォルト ゲートウェイ、DNS サーバーなどを設定します。この設定は後で変更できます。
7. 下矢印で画面の一番下まで移動し、**<OK>** を選択します。

   [Network Manager] (ネットワークマネージャー) ウィンドウが表示されます。
8. **<Quit>** を選択します。

   > **注意**: デフォルトでは、`nic0` は 192.168.1.5/24 の IP アドレスで事前設定されています。この IP アドレスを使用すると、IP ネットワークが到達可能な任意の PC から Tenable Core インターフェース (ポート 8000) を使用してシステムの設定を完了できます。
9. **y** を入力し、プロンプトに従って管理者アカウントを作成します。このアカウントは、Tenable Core (ターミナルコンソール、SSH、Tenable Core ユーザーインターフェース) へのログインにのみ使用します。OT Security アプリケーションには別のアカウントを使用してください。



10. アカウント作成後、そのアカウントを使用して、コンソールからまたはネットワーク接続 (SSH または Tenable Core インターフェース (https://<mgmt-IP>:8000)) を使用して、ターミナルにログインします。

Tenable Core ユーザーインターフェースを使う初期設定

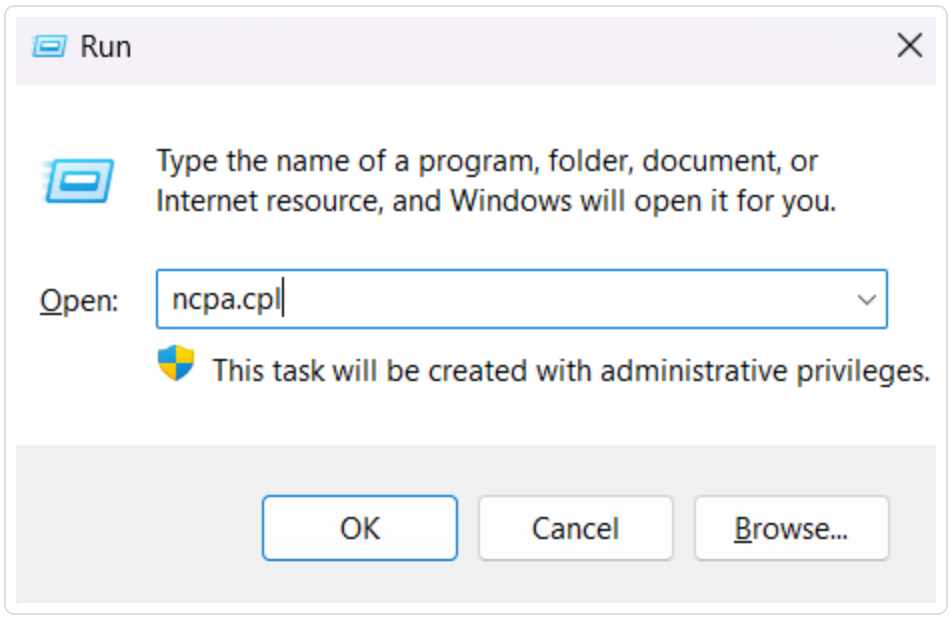
Tenable Core ユーザーインターフェース (https://<mgmt-IP>:8000 でアクセス可能) で初期設定を行うには、アプライアンスへのネットワーク接続が必要です。

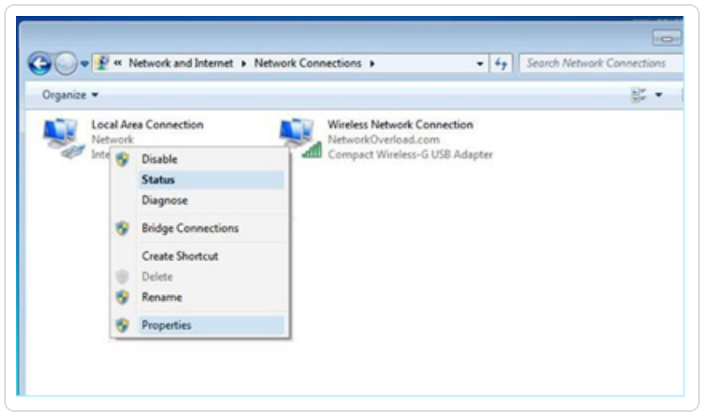
管理 IP アドレスを設定していない場合は、直接接続された PC または適切に設定されたネットワークを使用して、次のいずれかから Tenable Core ユーザーインターフェースにアクセスできます。

- **ポート 1** / **nic0** – IP アドレス 192.168.1.5/24 で事前設定された、デフォルトの管理インターフェース。
- **ポート 4** / **nic3** – IP アドレス 192.168.3.3/24 で事前設定された、エンジニアリングインターフェース。後から変更しない場合は、リカバリプロセスに使用できます。

PC またはノートパソコンから Tenable Core に直接接続するには、次のようにします。

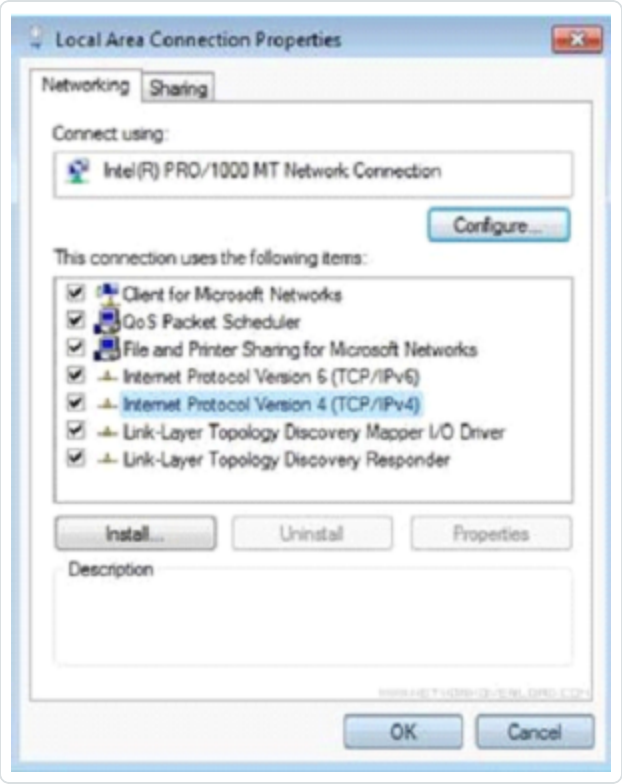
1. PC と OT Security アプライアンスの事前設定されているいずれかのポートをイーサネットケーブルで接続します。
2. Windows で **win+R** キーを押して **[ファイル名を指定して実行]** を開き、`ncpa.cpl` と入力して **[ネットワーク接続]** を開きます。





3. ネットワーク接続 (**[ローカルエリア接続]** という名前) を右クリックし、**[プロパティ]** を選択します。

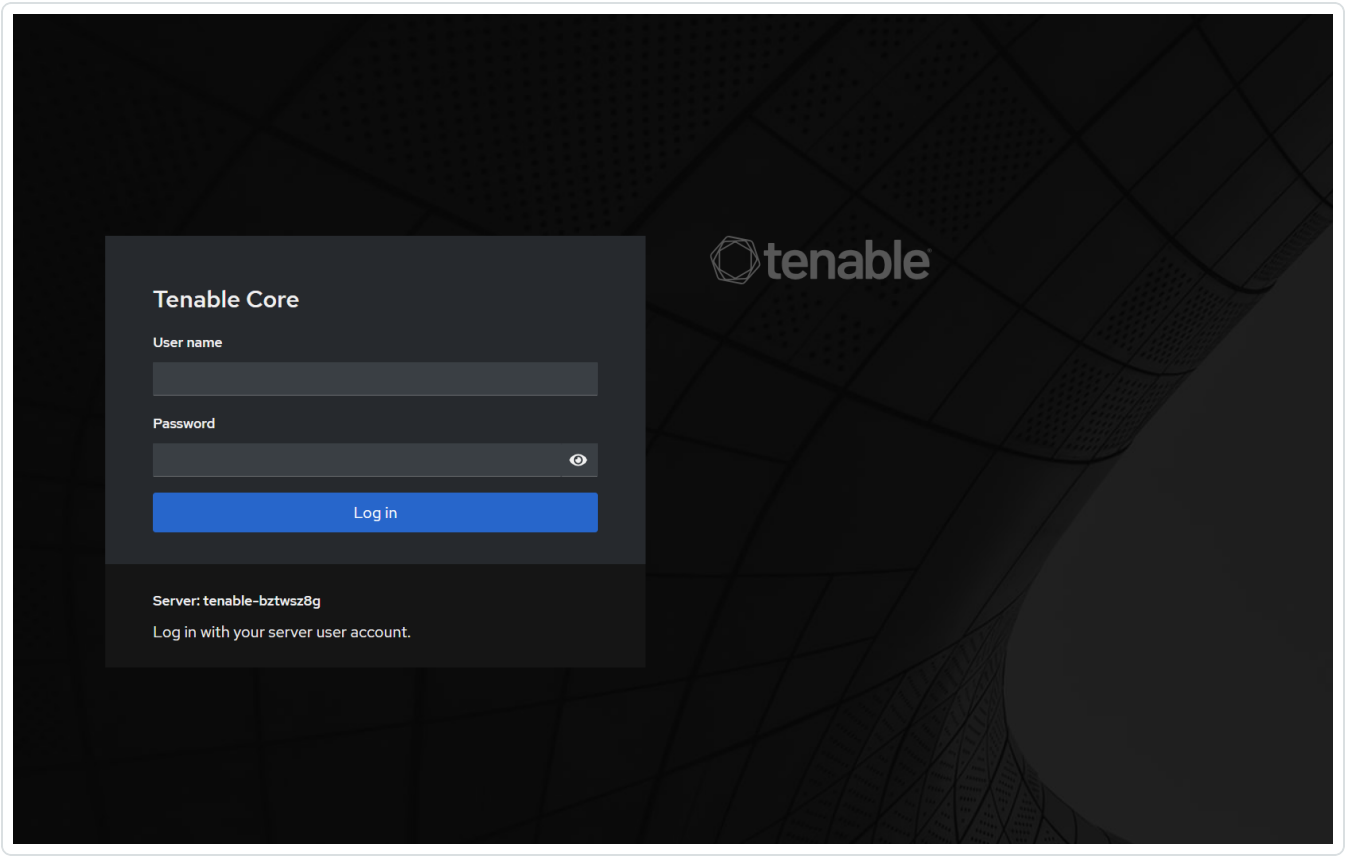
   [ローカルエリア接続プロパティ] ウィンドウが表示されます。



4. **[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) のプロパティ] ウィンドウが表示されます。

5. **[次の IP アドレスを使う]** を選択します。
6. **[IP アドレス]** ボックスに、接続しているインターフェースの適切な IP アドレスを入力します。たとえば、ポート 1 / nic0 のデフォルトアドレスの場合は 192.168.1.10、ポート 4 / nic3 のデフォルトアドレスの場合は 192.168.3.10 です。
7. **[サブネットマスク]** ボックスに、「255.255.255.0」と入力します。
8. **[OK]** をクリックします。
9. Chrome ブラウザから、https://<mgmt-ip>:8000 にアクセスします。



10. 管理者ユーザーアカウントをまだ設定していない場合は、設定を促すプロンプトが表示されます。新しく作成したユーザーで再度ログインします。詳細は、Create and initial Administrator Account (初期管理者ユーザーアカウントの作成) を参照してください。

    管理者アカウント作成後、Tenable では管理 IP アドレスを設定することをお勧めします。**split-port** 設定を使用する場合は、インターフェースが適切なネットワークに到達できることを確認してください。詳細は、ネットワークに関する考慮事項を参照してください。

> **注意**: **split-port** 設定を使用すると、管理がポート 1 (nic0) からポート 3 (nic2) に移動します。接続が失われる可能性があるため、ネットワーク設定によっては、新しい IP アドレスを使用して Tenable Core に再接続する必要があります。

> **注意**: 管理 IP アドレスを設定または変更するには、Tenable Core にログインし直し、管理者権限を有効にして、ネットワーク設定を編集してください。

次の手順

Tenable Core への OT Security のインストール

Tenable Core への OT Security のインストール

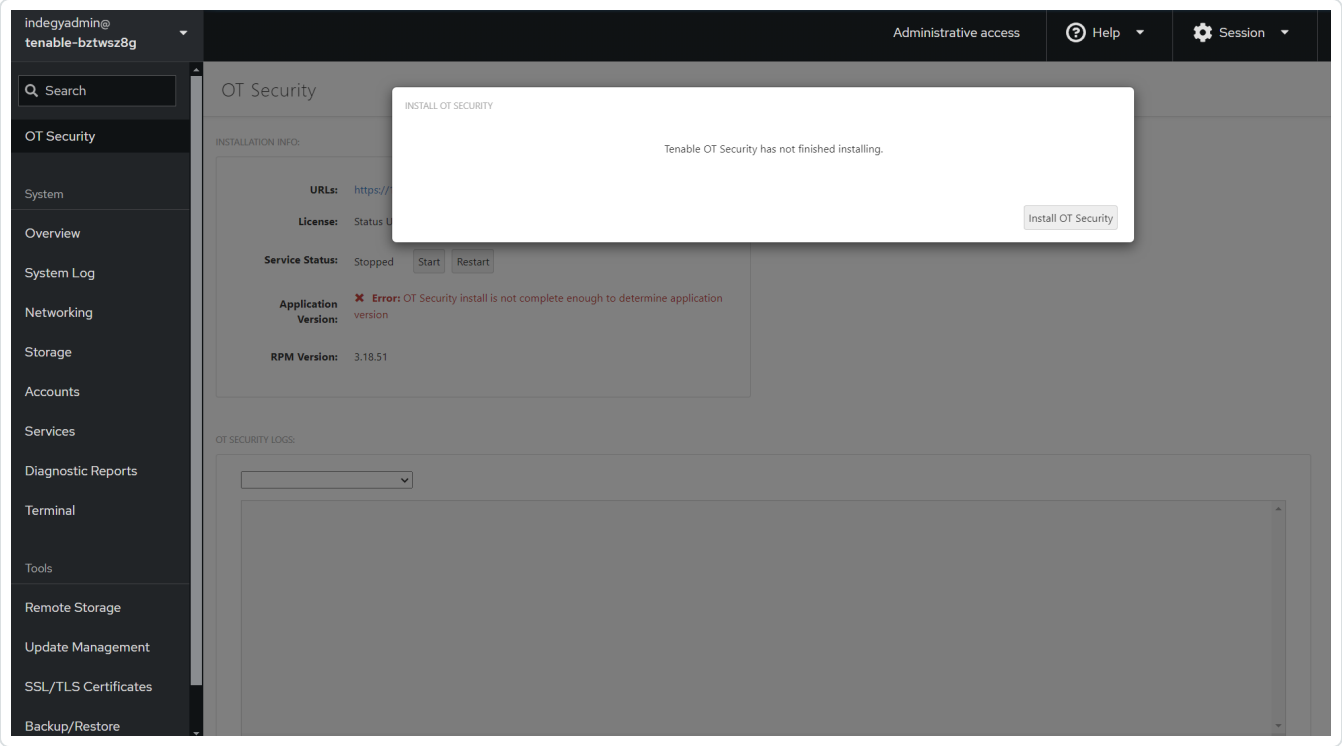
Tenable 提供ではないハードウェアまたは仮想マシンでは、OT Security アプリケーションのインストールを手動で完了する必要があります。

Tenable Core の OT Security をインストールするには、次のようにします。

1. Chrome ブラウザから Tenable Core にログインするには、`https://<mgmt-ip>:8000` にアクセスします。

   > **注意**: 管理者権限があることを確認してください。

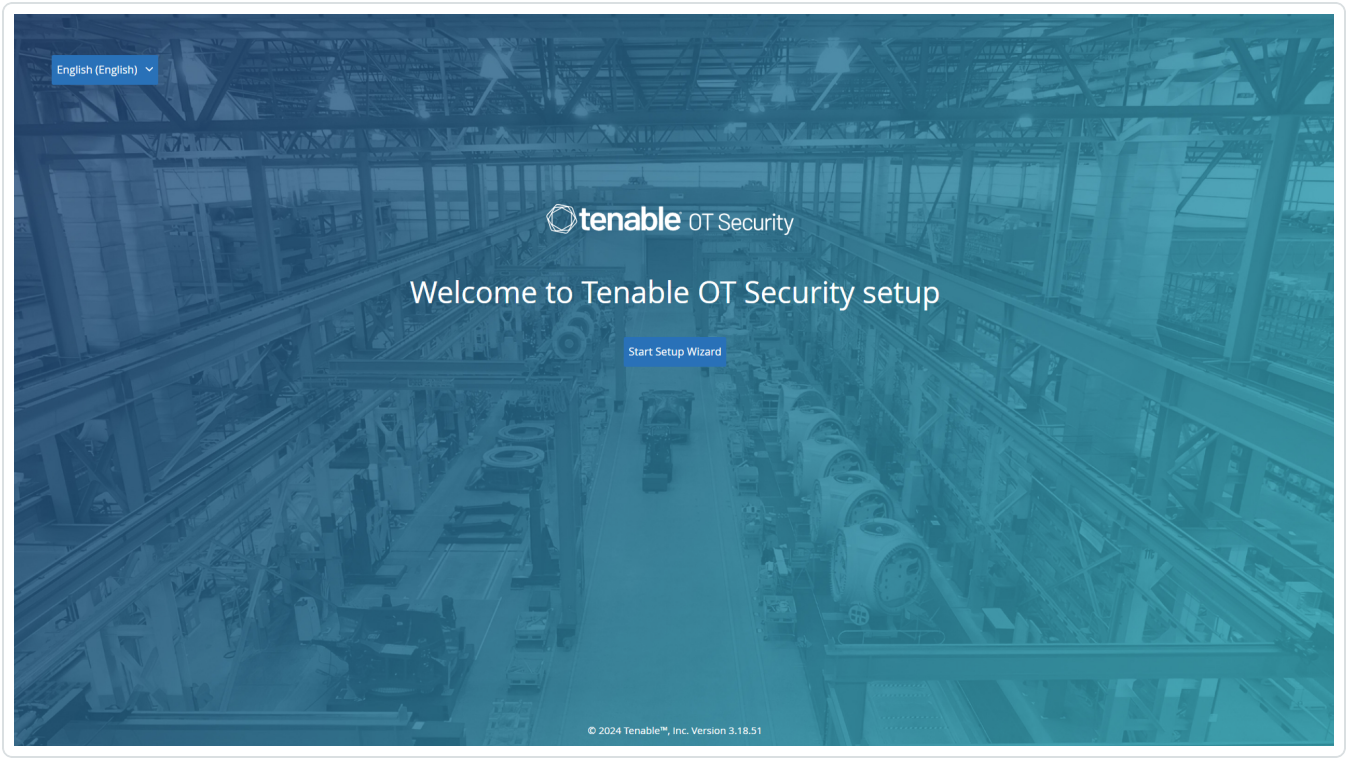
2. OT Security に移動します。
3. インストールのプロンプトで、**[Tenable OT Security のインストール]** をクリックします。



注意: インストールプロセス完了までに時間がかかる場合があります。インストールプロセスを中断しないでください。

インストールが完了したら、`https://<mgmt-ip>` から OT Security ユーザーインターフェースにログインできます。

`mgmt-ip` は、Tenable Core ウィンドウ上部の **URL** フィールドに表示される IP アドレスです。



次の手順

セットアップウィザードを使用した OT Security の設定

セットアップウィザードを使用した OT Security の設定

OT Security セットアップウィザードは、基本的なシステム設定を行うプロセスをガイドします。

> **注意**: この設定は、必要に応じて管理コンソール(ユーザーインターフェース)の**[設定]**画面で変更できます。

セットアップウィザードにアクセスするには、まず OT Security 管理コンソールにログインする必要があります。管理コンソールのログイン方法については、OT Security 管理コンソールへのログインを参照してください。

セットアップウィザードを使用して、以下を設定します。

1. ユーザー情報
2. デバイス
3. システム時刻
4. 個別の管理ポートの接続 (ポート分離)

注意: セットアップウィザード終了後、OT Security からシステムの再起動を求めるメッセージが表示されます。

OT Security 管理コンソールへのログイン

OT Security 管理コンソールにログインするには、次のようにします。

1. 次のいずれかを実行します。

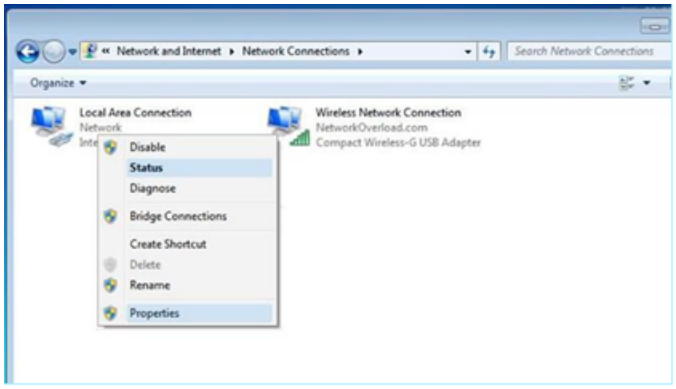
   - イーサネットケーブルを使用して、管理コンソールワークステーション (デスクトップ、ノートパソコンなど) を OT Security アプライアンスのポート 1 に直接接続します。
   - 管理コンソールワークステーションをネットワークスイッチに接続します。

   注意: 管理コンソールワークステーションが、OT Security 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、またはユニットにルーティング可能であることを確認してください。

2. OT Security アプライアンスに接続するため、次の手順で静的 IP を設定します。

   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。

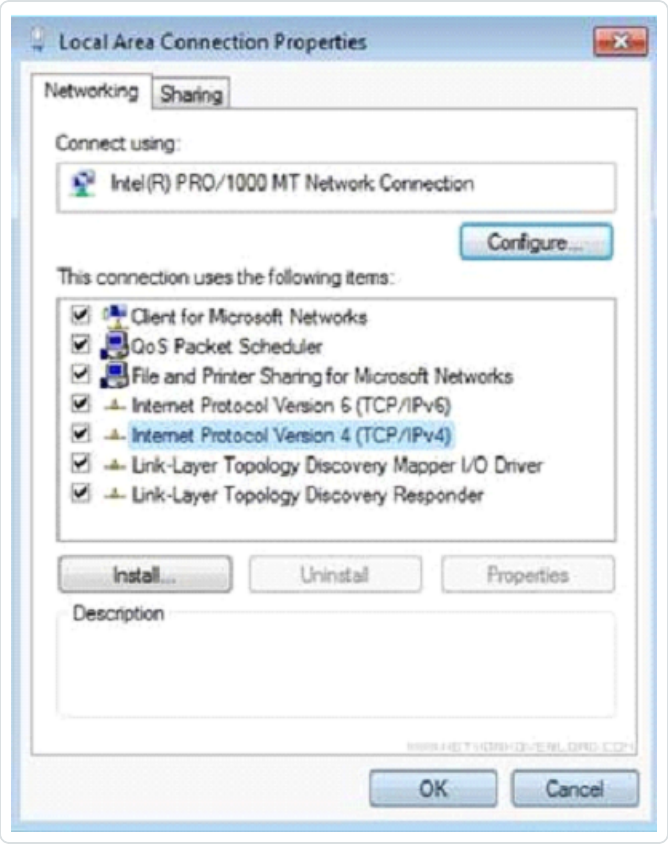
   [ネットワーク接続] 画面が表示されます。

   注意: 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. **[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) のプロパティ] 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]** ボックスに、「192.168.1.10」と入力します。

f. **[サブネット マスク]** ボックスに、「255.255.255.0」と入力します。

g. **[OK]** をクリックします。

OT Security により新しい設定が適用されます。

h. Chrome ブラウザで、https://192.168.1.5 にアクセスします。

セットアップウィザードの **[ようこそ]** 画面が開きます。

注意: ユーザーインターフェースにアクセスするには、最新バージョンの Chrome が必要です。

i. **[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。

次の手順

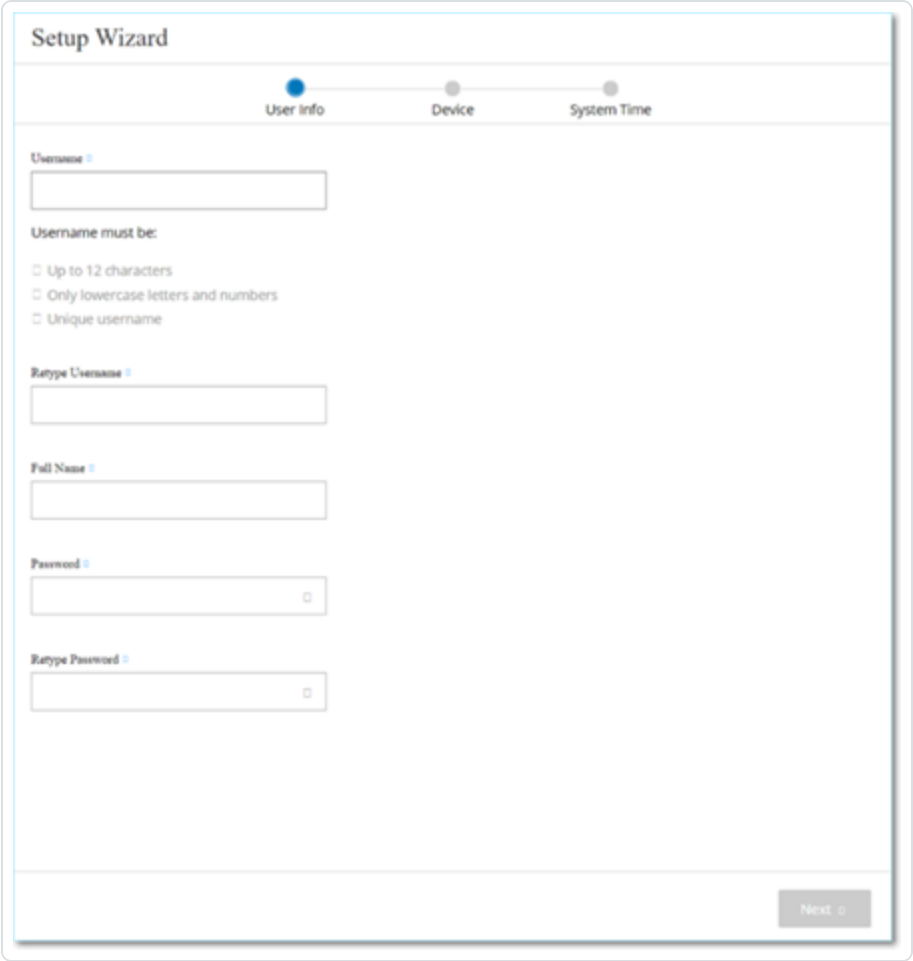
ユーザー情報

ユーザー情報

OT Security セットアップウィザードは、基本的なシステム設定を行うプロセスをガイドします。

注意: この設定は、必要に応じて管理コンソール(ユーザーインターフェース)の**[設定]**画面で変更できます。

ユーザー情報



[ユーザー情報] ページでユーザーアカウント情報を入力します。

注意: 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設定できます。ユーザーインターフェースにログイン後、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]** ボックスに、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]** ボックスに、ユーザー名を再入力します。
3. **[フルネーム]** セクションで、**氏名**を入力します。

   注意: 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]** ボックスに、システムにログインするための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]** ボックスに、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。

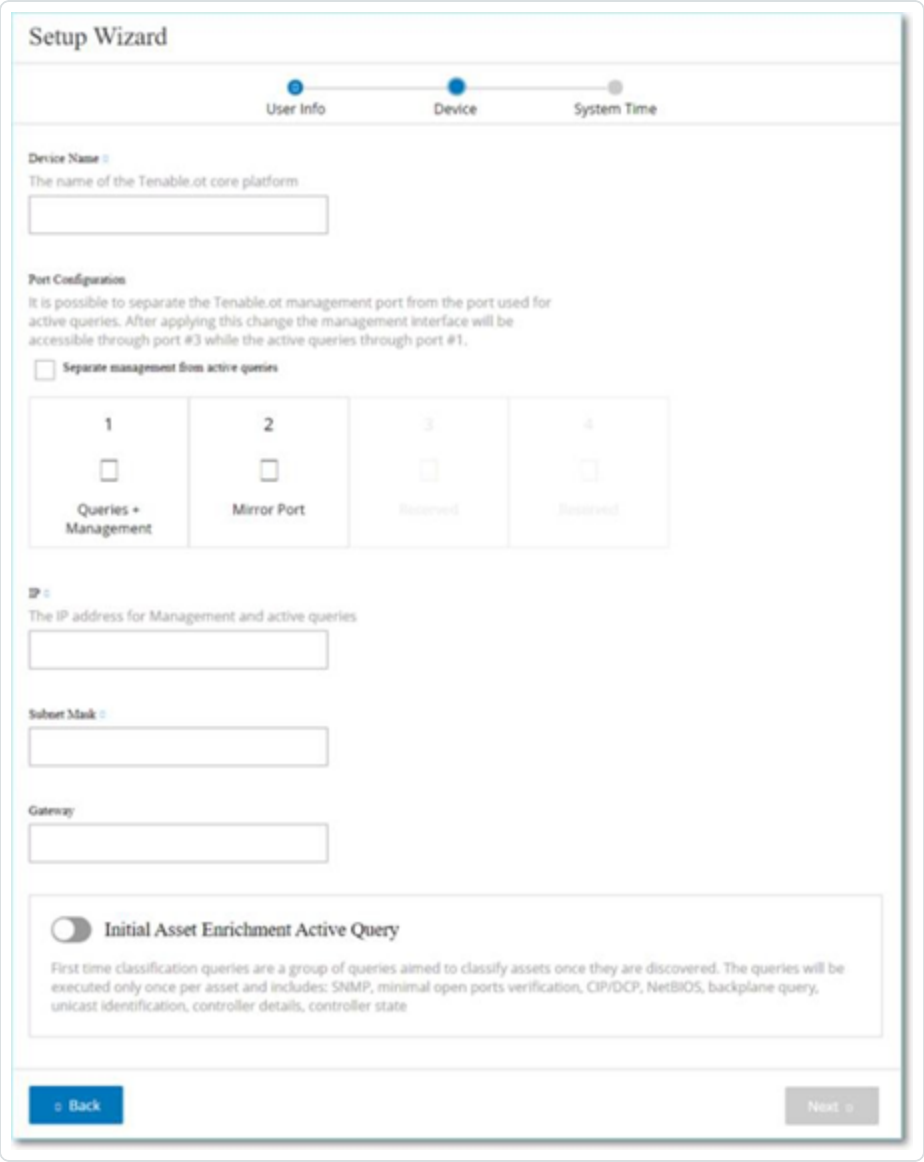
次の手順

デバイスを設定します。

デバイス

OT Security セットアップウィザードは、基本的なシステム設定を行うプロセスをガイドします。

> **注意**: この設定は、必要に応じて管理コンソール(ユーザーインターフェース)の **[設定]** 画面で変更できます。



[デバイス]: ページで、OT Security 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]** ボックスに、OT Security プラットフォームの一意の識別子を入力します。
2. **[ポート設定]** 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、**[管理とアクティブクエリを分離する]** チェックボックスを選択します。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設定されます。

        注意: 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、**[管理とアクティブクエリを分離する]** チェックボックスを選択しないでください。この場合、この手順のステップ 3 をスキップし、ステップ 4 に進みます。

3. **ポート分離**オプションを選択した場合

   a. **[アクティブクエリ IP]** ボックスに、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ポートに接続し、コントローラーに接続またはルーティングできます。OT Security はコントローラーに接続するため、ネットワークサブネット内の IP アドレスが必要です。

   b. **[アクティブクエリのサブネットマスク]** ボックスに、クエリポートのサブネットマスクを入力します。

   c. **[アクティブクエリゲートウェイ]** ボックス (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。

4. **[管理 IP]** ボックスに、OT Security 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 OT Security 管理 IP アドレスになります。ポートを分離しない場合、この IP アドレスはクエリアドレスにもなります。

5. **[管理サブネットマスク]** ボックスに、ネットワークのサブネットマスクを入力します。

6. (オプション) ゲートウェイを設定する場合は、**[管理のゲートウェイ]** ボックスにネットワークのゲートウェイ IP を入力します。

   > **注意**: 管理ゲートウェイ IP を指定しない場合、OT Security はメールサーバーや syslog サーバーなど、サブネット外部の外部コンポーネントと通信できなくなります。

7. **初期資産強化アクティブクエリ**は、システム内で検出された各資産で実行される一連のクエリで構成されています。

   これは、OT Security が資産を分類するのに役立ちます。OT Security によって検出される新しい各資産に対してこれらのクエリを実行するには、**[初期資産強化アクティブクエリ]** トグルをオンにします。

8. **[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。

次の手順

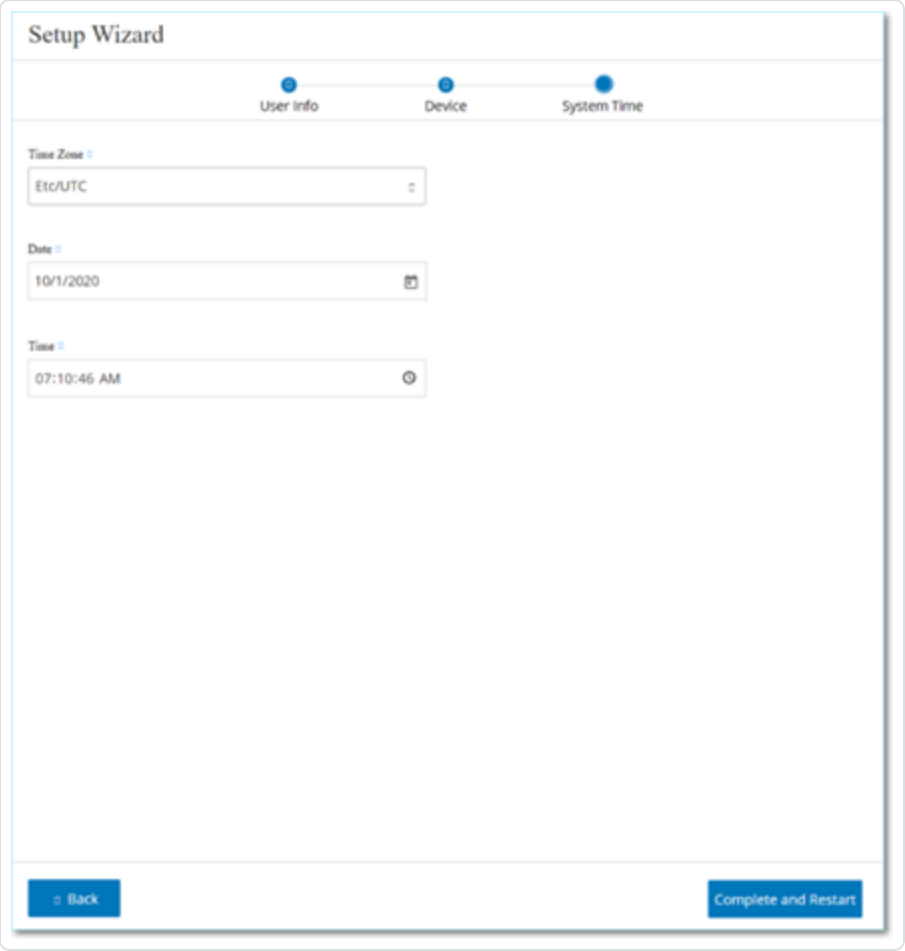
システム時刻の設定を行います。

システム時刻

OT Security セットアップウィザードは、基本的なシステム設定を行うプロセスをガイドします。

> **注意**: この設定は、必要に応じて管理コンソール(ユーザーインターフェース)の**[設定]**画面で変更できます。

システム時刻

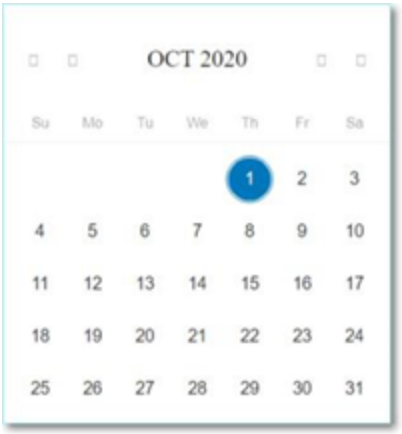


> **注意**: ログとアラートを正確に記録するには、正しい日付と時刻を設定することが重要です。

[システム時刻]ページには、正しい時刻と日付が自動的に表示されます。間違っている場合は、次を実行します。

1. **[タイムゾーン]** ドロップダウンボックスで、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]** ボックスで、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. **[時刻]** ボックスで、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。

   注意: 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]** をクリックした後は、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、ユーザーインターフェースの **[設定]** ページで設定を変更できます。

5. セットアップを完了するには、**[完了して再起動]** をクリックします。

   再起動が完了すると、OT Security により **[ライセンス]** ウィンドウにリダイレクトされます。

   注意: ポート分離オプションを選択した場合は、個別の管理ポートの接続 (ポート分離) の説明に従ってネットワーク接続を変更してください。

次の手順

次を実行します。

- 個別の管理ポートの接続 (ポート分離)
- OT Security ライセンスのアクティベーション

個別の管理ポートの接続 (ポート分離)

[ポート分離]オプションを選択して、クエリを管理から分離する場合は、(管理ポートとなった) OT Security 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。

管理ポートを接続するには、次のようにします。

1. OT Security 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。

次の手順

OT Security ライセンスのアクティベーション

OT Security ライセンスのアクティベーション

目的: ライセンスアクティベーションでシステム機能をロック解除します。

Tenable は、システム内の一意の IP の数に基づいてライセンスを計算します。IP アドレスごとに個別のライセンスが必要です。たとえば、Tenable は、複数のデバイスが同じ IP を共有する場合や、同じバックプレーンに接続された複数のデバイスが同じ 3 つの IP を共有する場合でも、一意の IP の数に基づいてライセンスを決定します。したがって、デバイスの数に関係なく必要なライセンスの数は 3 つになります。

OT Security アプライアンスをインストールした後、ライセンスをアクティブ化できます。

注意: OT Security ライセンスをアップデートまたは再初期化する必要がある場合は、Tenable アカウントマネージャーに連絡してください。Tenable アカウントマネージャーによりライセンスがアップデートされた後、お客様は自分でライセンスのアップデートや再初期化ができるようになります。

Tenable One における Tenable OT Security のデプロイメントやライセンス付与については、Tenable One デプロイメントガイドを参照してください。

始める前に

- OT Security アプライアンスを設置します。
- 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) があることを確認します。

- インターネットにアクセスできることを確認します。OT Security 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。
- Tenable プロビジョニングポータルへのアクセス権があることを確認します。アクセス権については、Tenable Customer Success Manager にお問い合わせください。

OT Security ライセンスのアクティブ化

OT Security ライセンスをアクティブ化し、資産を管理する新しいサイトを作成するための Tenable プロビジョニングポータルを促進することができます。

OT Security ライセンスをアクティブ化するには、次のようにします。

1. コミュニティアカウントを使用して、Tenable プロビジョニングポータルにログインします。

   [プロビジョニング] ページに、お客様がライセンスを持っている製品が表示されます。

2. 左側のペインで、**Tenable OT Security** を選択します。

   OT Security ライセンスと、その購入日、有効期限、ライセンス付与された IP とサイトの数などの詳細が表示されます。

3. **[コード]** 列から、20 桁の OT Security ライセンスコードをコピーします。

4. OT Security で、アクティベーション証明書を生成します。

   a. OT Security の **[ライセンスのアクティベーション]** ページに移動します。

   b. 手順 1 で、**[新しいライセンスコードの入力]** をクリックします。

      [新しい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。

   c. **[ライセンスコード]** ボックスに、プロビジョニングポータルからコピーしたコードを貼り付けます。

   d. **[検証]** をクリックします。

      OT Security は、**[アクティベーション証明書の生成]** セクションを有効にします。

   e. **[証明書の生成]** をクリックします。

      [証明書の生成] パネルが右側に表示されます。

   f. **[テキストをクリップボードにコピー]** をクリックしてから、**[完了]** をクリックします。

OT Security で証明書が生成されます。サイトを追加するには、Tenable プロビジョニングポータルにこの証明書を提供する必要があります。

5. 手順 **3 のアクティベーションコードの入力**で、**[セルフサービス]** リンクをクリックして Tenable プロビジョニングポータルを開きます。

   注意: 評価期間をアクティブ化するには、**[ここをクリック]** リンクをクリックします。

6. [**Tenable OT Security プロビジョニング**] ページに移動し、⊕ **[サイトの追加]** をクリックします。

   [新しい Tenable OT Security サイトの追加] ウィンドウが表示されます。

   a. (オプション) **[ラベル]** ボックスに、サイトの名前を入力します。

   b. **[IP]** ボックスに、このサイトに割り当てる IP アドレスの数を入力します。**[+]** と **[-]** ボタンを使用して、値を増減します。

      ヒント: ライセンスに割り当てられた IP アドレスの数の調整には、**[IP]** ボックスの下にあるスライダーを使用することもできます。

   c. **[アクティベーション証明書]** ボックスに、OT Security でコピーした証明書を貼り付けます。手順 f を参照してください。

   d. **[作成]** をクリックします。

      アクティベーションコードを含むダイアログボックスが表示されます。これは 1 回限り生成されるコードで、OT Security インスタンスにコピーする必要があります。

   e. ⧉ ボタンをクリックし、**[確認]** をクリックします。

7. OT Security インスタンスに戻り、手順 **3 [アクティベーションコードの入力]** セクションで、**[アクティベーションコードの入力]** をクリックします。

   [アクティベーションコードの入力] パネルが右側に表示されます。

8. **[アクティベーションコード]** ボックスに、**Tenable OT Security プロビジョニング**ページからコピーした 1 回限り生成されるコードを貼り付けます。手順 e を参照してください。

9. **[アクティベート]** をクリックします。

   OT Security でシステムが正常にアクティベートされたことを示すメッセージが表示され、OT Security インターフェースが表示されます。

10. **[有効化]**をクリックします。

    OT Security が有効になり、使用できる状態になります。

11. Tenable プロビジョニングポータルに戻り、ワンタイム生成アクティベーションコードのダイアログボックスで、**[この証明書の情報を保存、またはアクティベーション用に Tenable.ot にコピーしました]** チェックボックスをクリックします。

12. **[確認]**をクリックします。

    新しく追加されたサイトが、OT Security の**プロビジョニング**ページに表示されます。

ライセンスをアップデートする

資産の上限を引き上げたり、ライセンス期間を延長したり、ライセンスタイプを変更したりする場合は、ライセンスをアップデートできます。

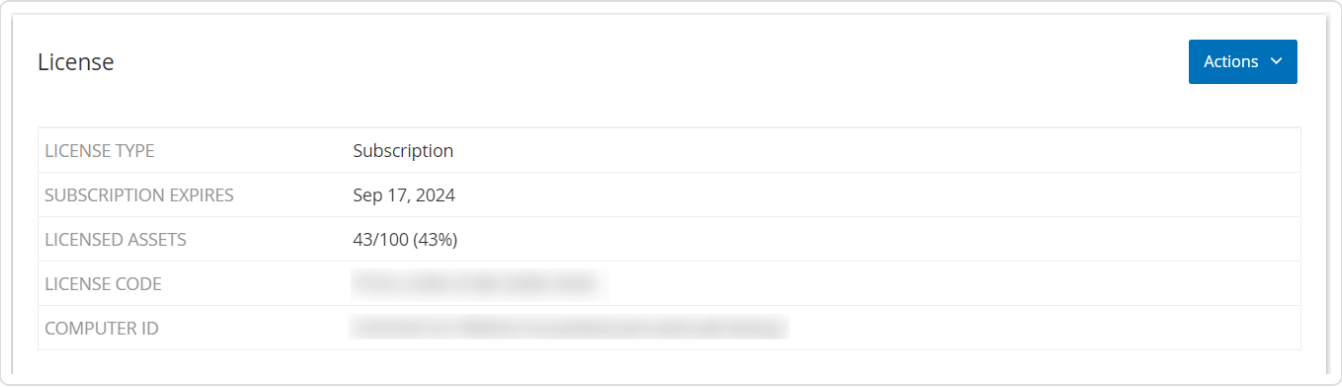
始める前に

- 新しいライセンスのアップデート前に、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すでに更新していなければなりません。
- インターネットへのアクセスが必要です。OT Security デバイスがインターネットに接続できない場合は、任意の PC からライセンスを登録できます。

ライセンスをアップデートするには、次のようにします。

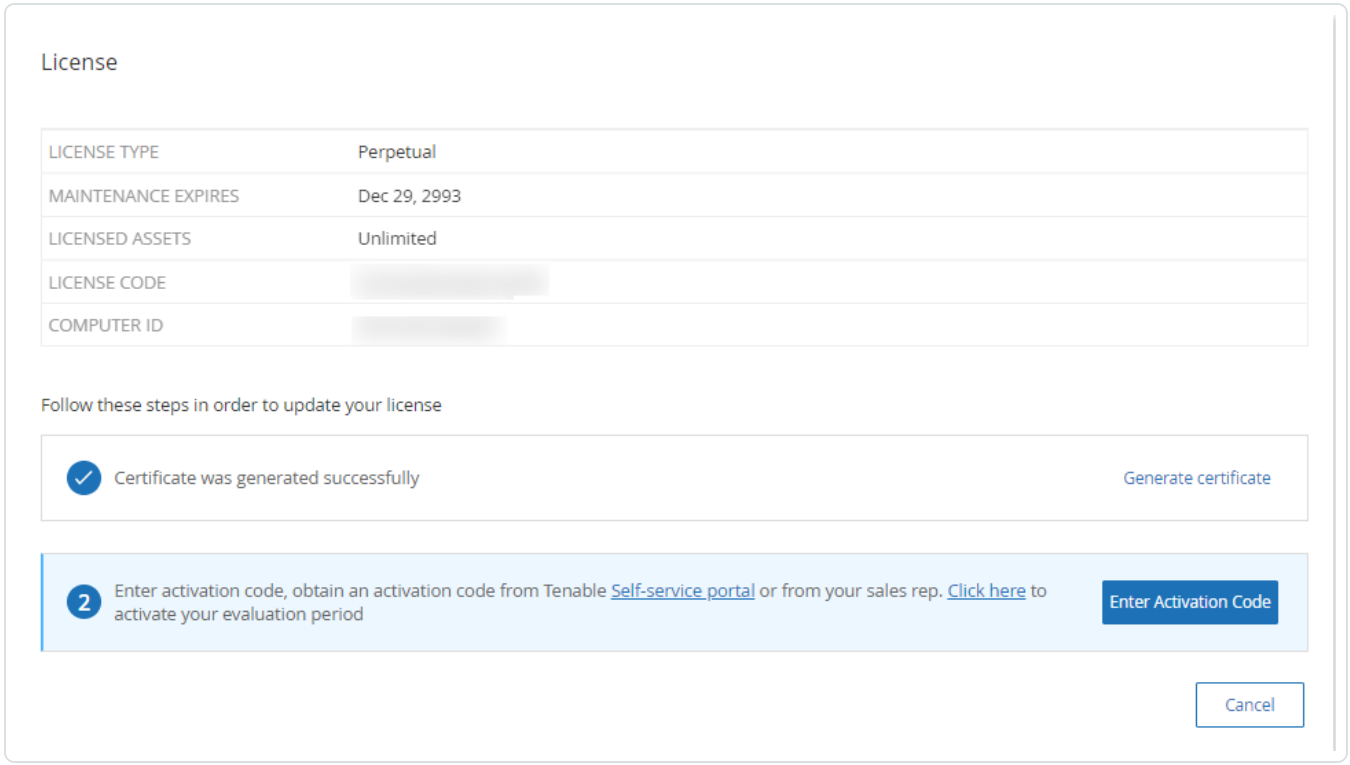
1. **[ローカル設定]** > **[システム設定]** > **[ライセンス]** に移動します。

   [ライセンス] ウィンドウが表示されます。



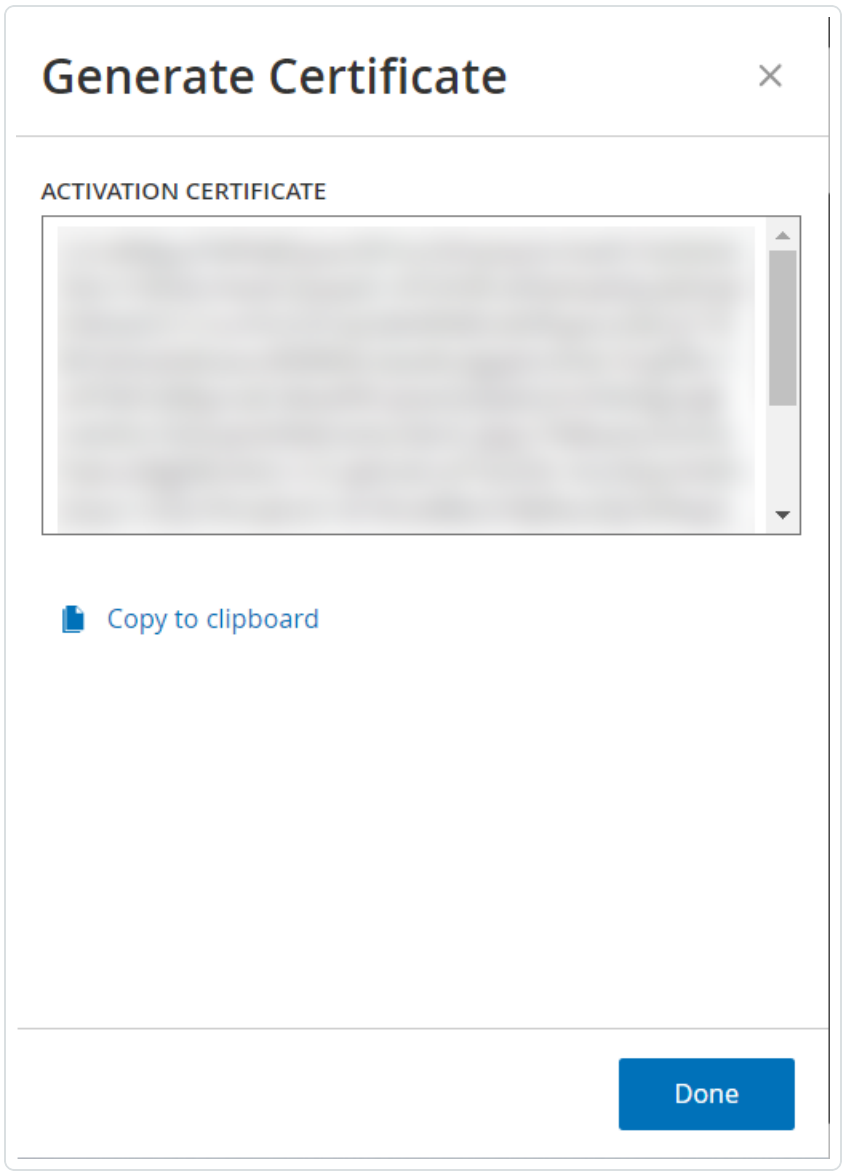
2. **[アクション]** メニューから **[ライセンスのアップデート]** を選択します。

[証明書の生成] および **[アクティベーションコードの入力]** の手順が表示されます。



3. **[(1) アクティベーション証明書の生成]** ボックスで、**[証明書の生成]** をクリックします。

   [証明書の生成] パネルが表示され、このパネルに**アクティベーション証明書**が表示されます。



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

   サイドパネルが閉じます。

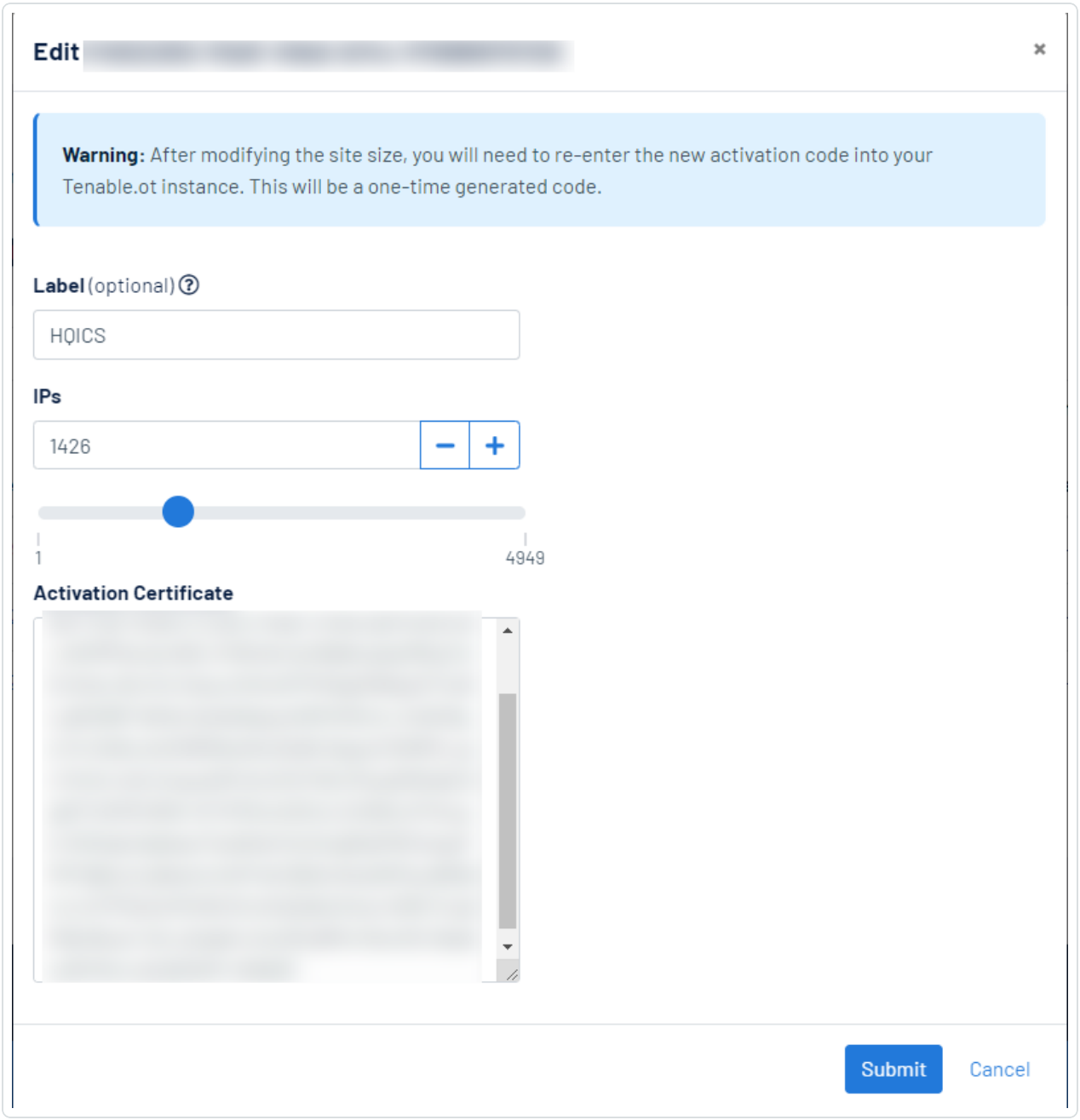
5. Tenable プロビジョニングポータルでサイトの詳細を編集します。

   a. Tenable プロビジョニングポータルで、**[Tenable OT Security プロビジョニング]** ページに移動し、アップデートするサイトの行で、 ボタンをクリックします。

      メニューが表示されます。

   b. **[サイトの編集]** をクリックします。

[サイトの編集]ウィンドウが表示されます。



c. 必要に応じて詳細を調整します。

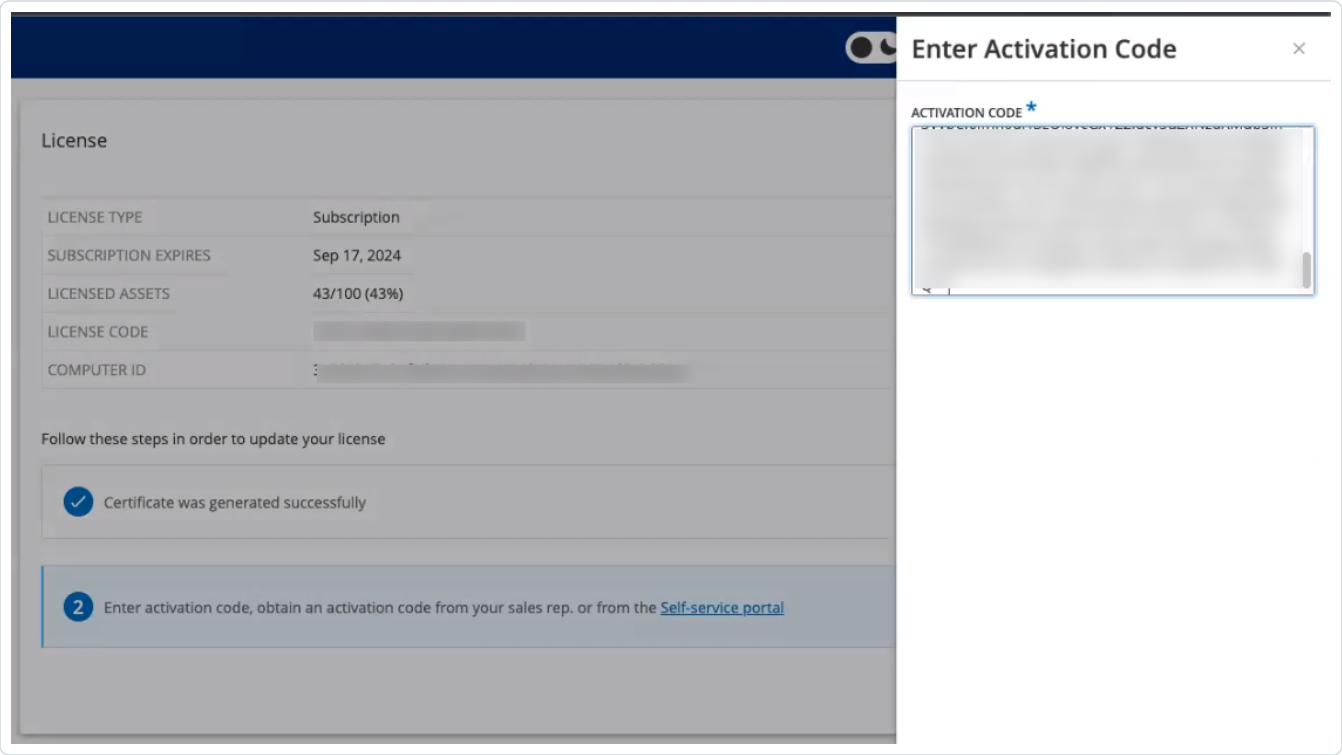
d. **[アクティベーション証明書]**ボックスに、OT Security の**[証明書の生成]**ウィンドウでコピーした証明書を貼り付けます。

e. **[送信]**をクリックします。

ポータルにアクティベーションコードが記載されたダイアログボックスが表示されます。これは1回限り生成されるコードで、OT Security インスタンスにコピーする必要があります。

f. ボタンをクリックし、**[確認]** をクリックします。

6. OT Security インスタンスに戻ります。
7. **[(2) アクティベーションコードの入力]** ボックスで、**[アクティベーションコードの入力]** をクリックします。
8. **[アクティベーションコード]** ボックスに、**Tenable OT Security プロビジョニング**ページからコピーした1回限り生成されるコードを貼り付けます。

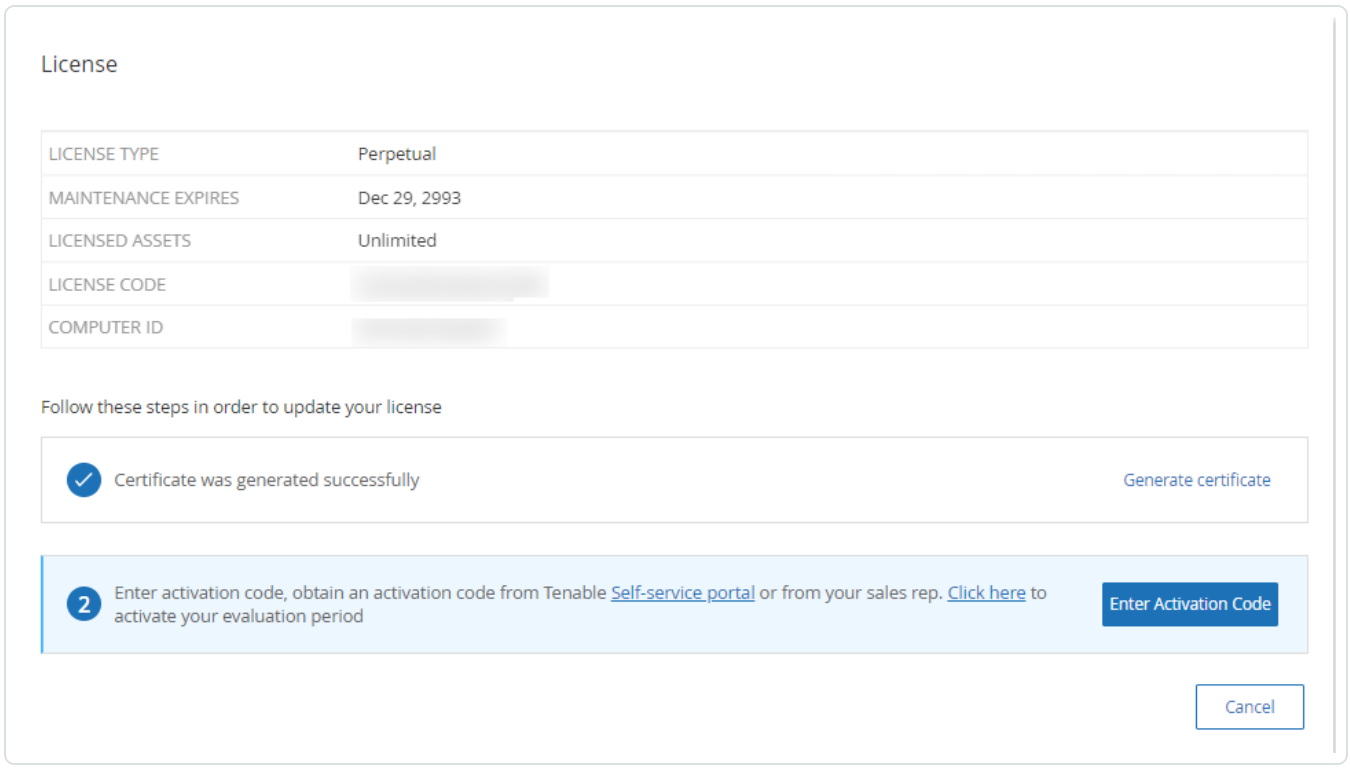


9. **[アクティベート]** をクリックします。

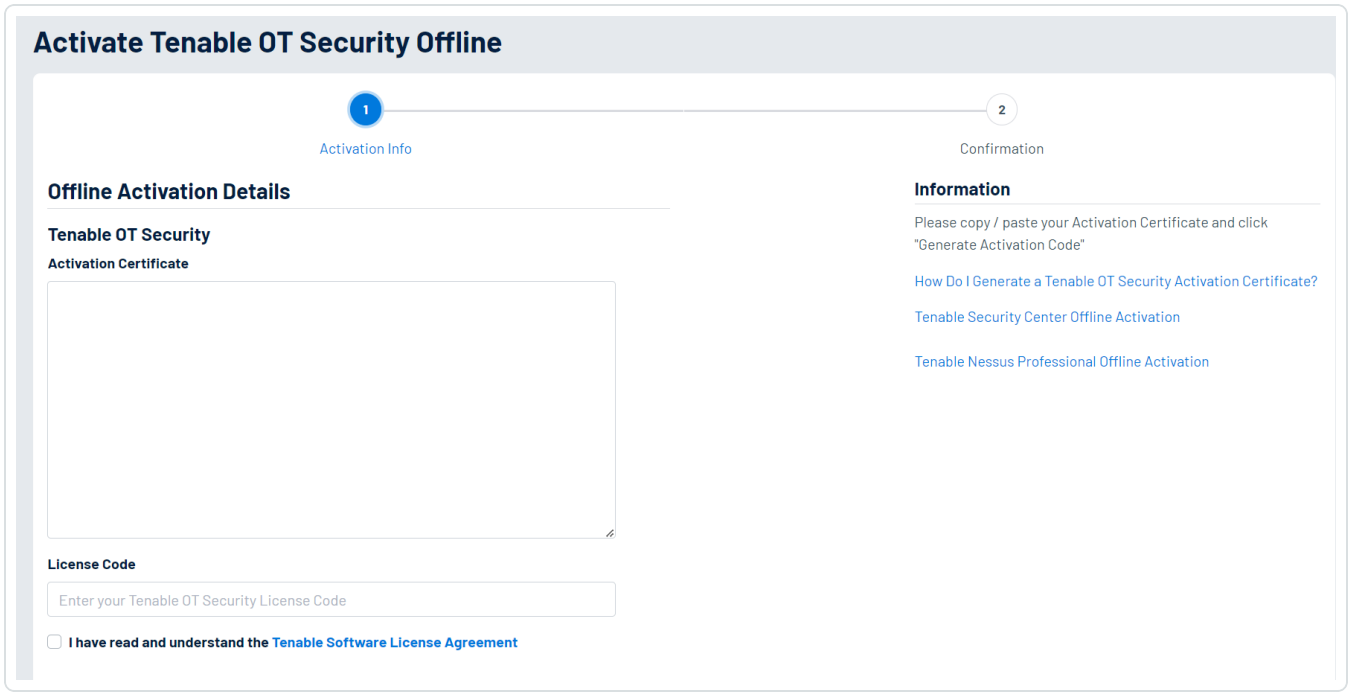
OT Security でシステムが正常にアクティベートしたことを示すメッセージが表示され、**[ライセンス]** ページにアップデートされたライセンスの詳細が表示されます。

ライセンスをオフラインモードでアップデートする

1. ライセンスをアップデートするセクションで説明されている、手順 1 から 4 を実行します。
2. **[(2) アクティベーションコードの入力]** ボックスで、セルフサービスポータルのリンクをクリックします。



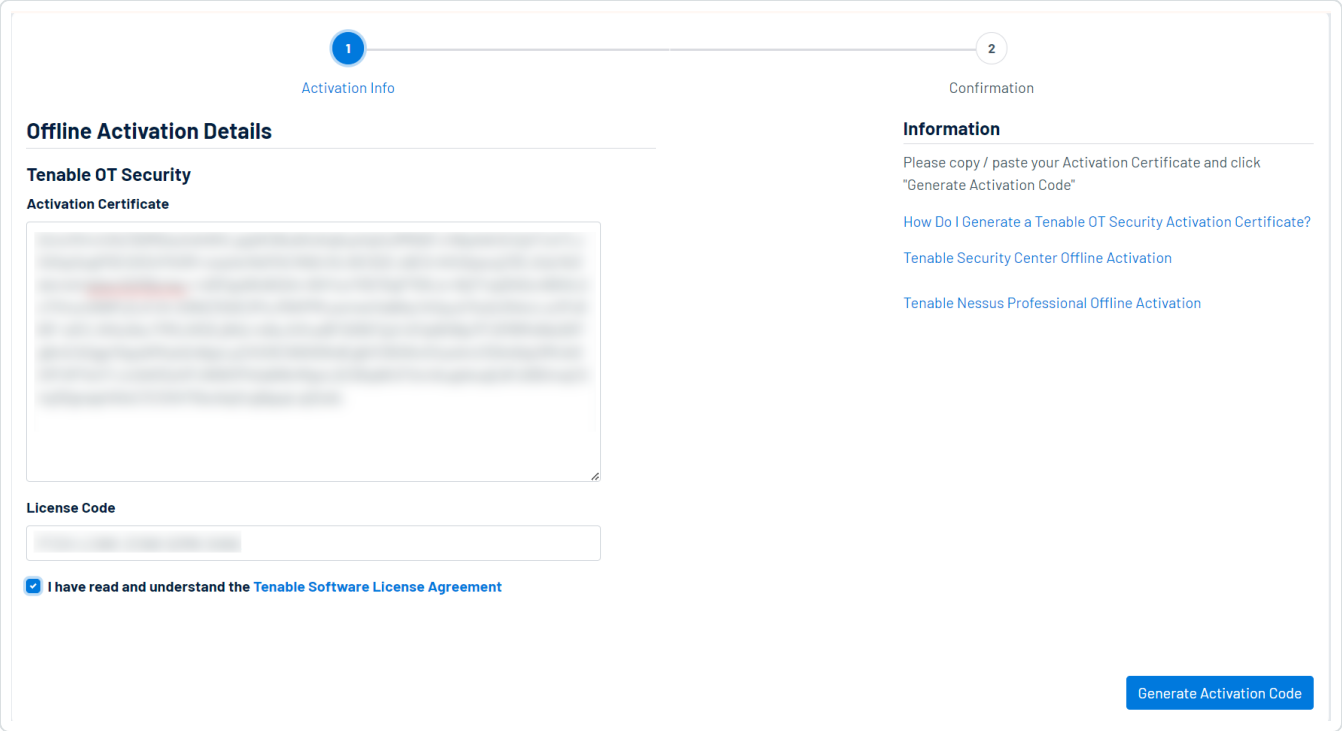
[OT Security をオフラインでアクティブ化] ウィンドウが新しいタブで開きます。



注意: 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[OT Security をオフラインでアクティブ化]画面にアクセスできます。

注意: 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できます。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します。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]**をクリックして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。

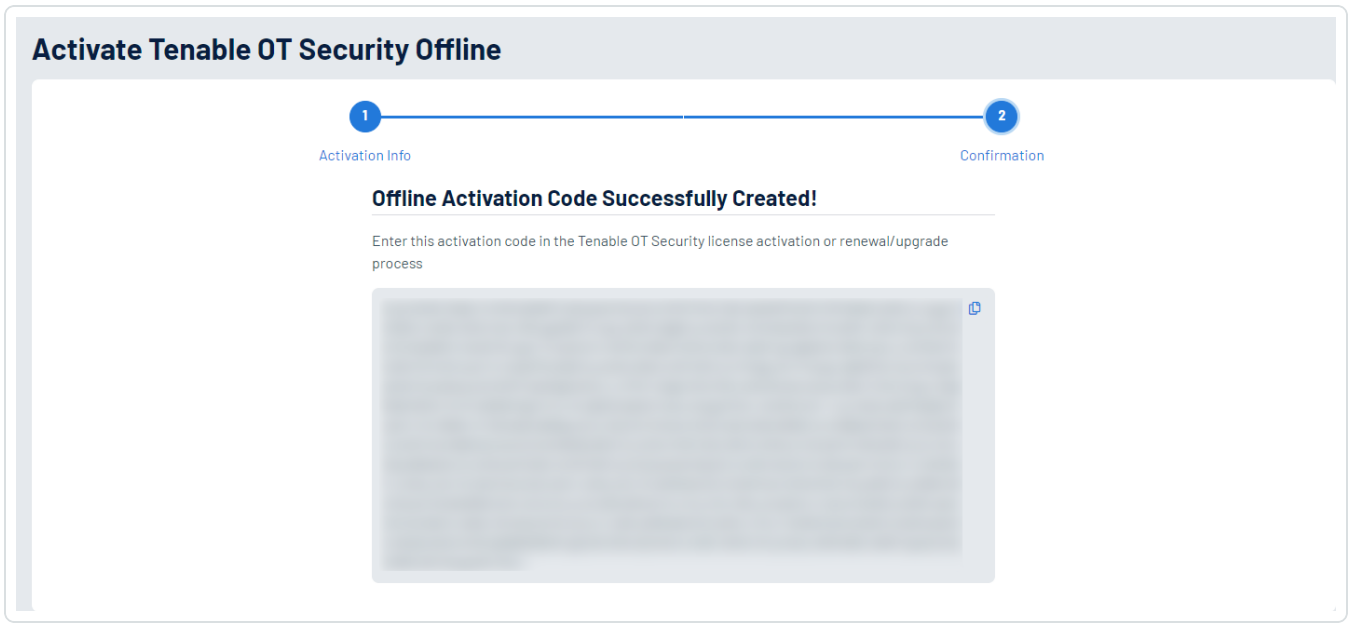
3. **[アクティベーション証明書]**ボックスに、**アクティベーション証明書**を貼り付けます。
4. **[ライセンスコード]**ボックスに、20 文字の**ライセンスコード**を入力します(**[ライセンス]**画面からコピーして貼り付けることができます)。
5. **[Tenable ソフトウェアライセンス契約を読み、理解しました]**チェックボックスをクリックします。



注意: 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。

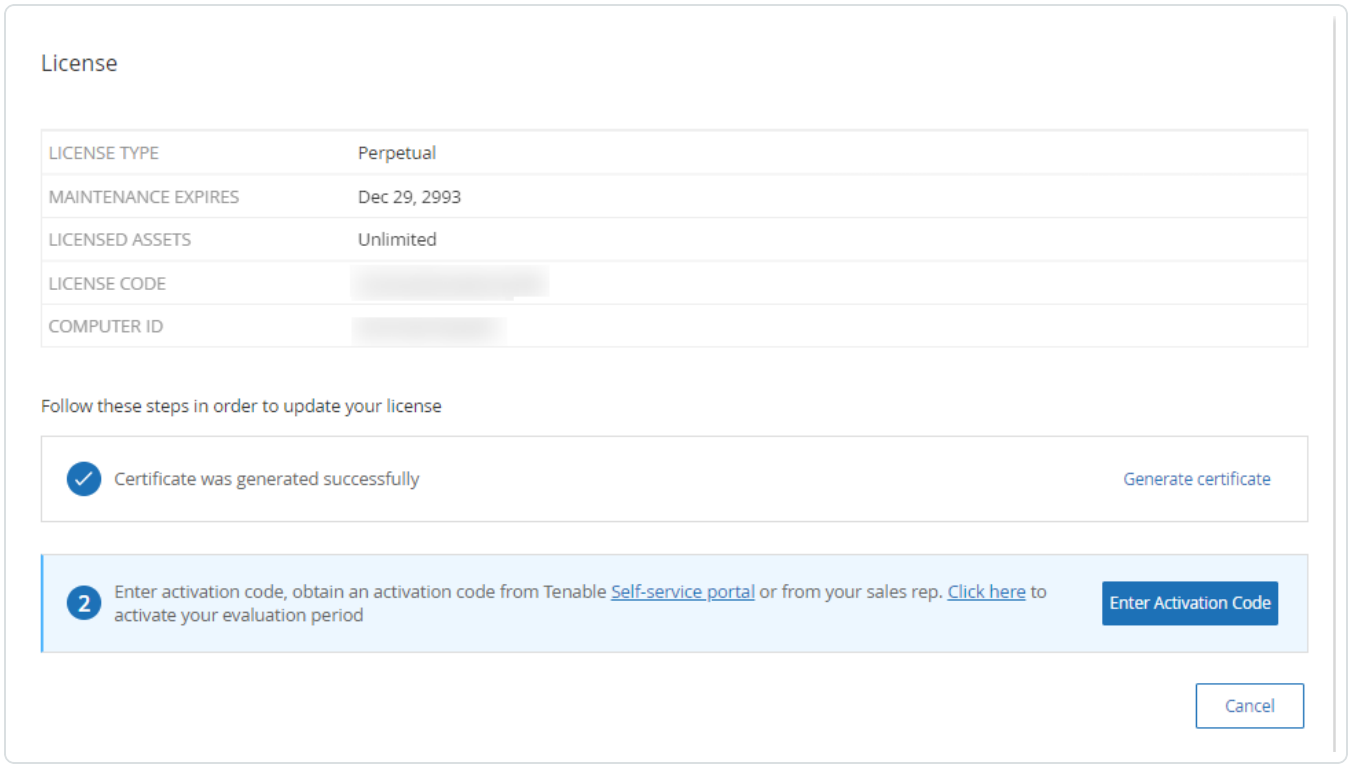
6. **[アクティベーションコードの生成]**をクリックします。

[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!]ウィンドウが表示されます。



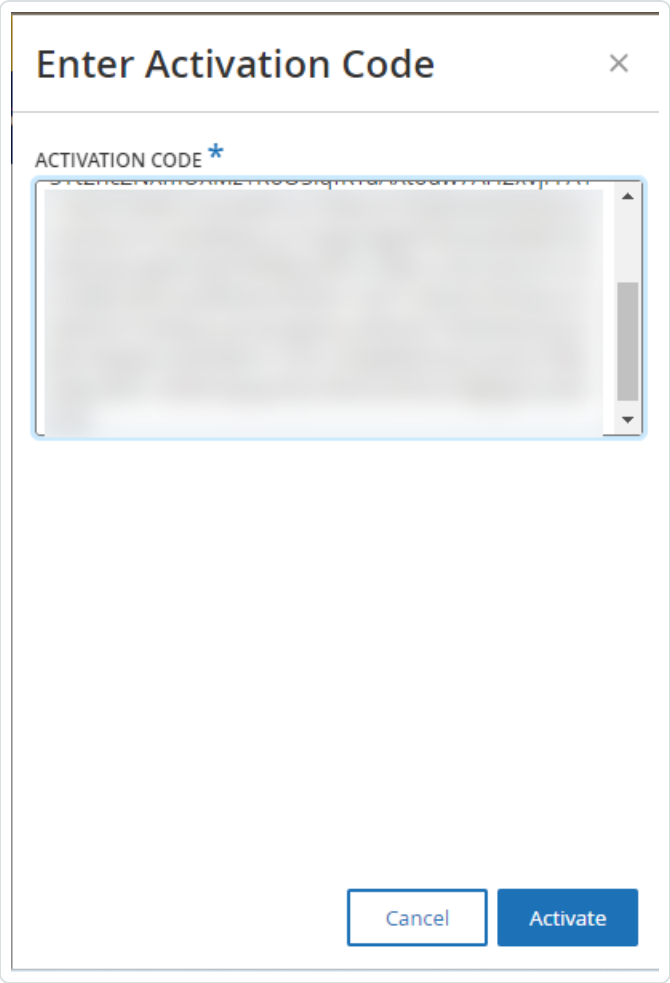
7. ボタンをクリックします。

8. **[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]** 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。

9. **[アクティベーションコード]** ボックスにアクティベーションコードを貼り付け、**[アクティブ化]** をクリックします。



サイドパネルが閉じ、OT Security によりライセンスがアップデートされます。

ライセンスを再初期化する

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 (新しいライセンスを受け取った場合) は、次の手順を実行します。

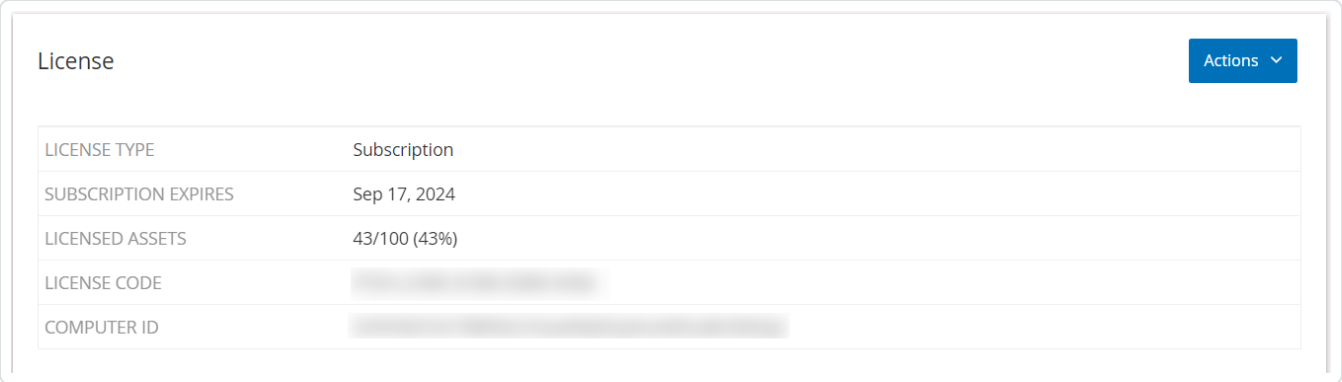
始める前に

- 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。OT Security デバイスをインターネットに接続できない場合は、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するには、次のようにします。

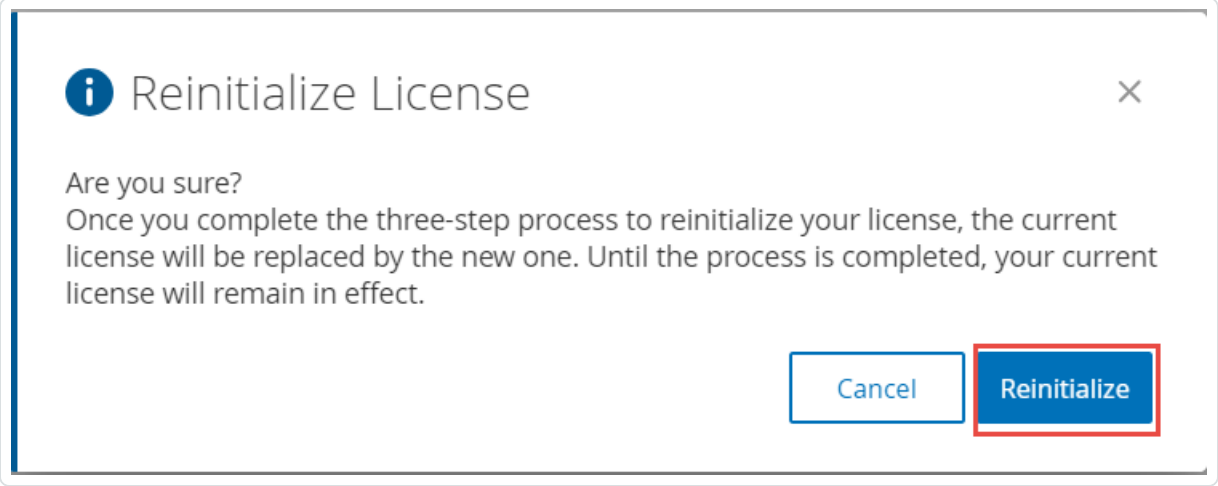
1. **[ローカル設定]** > **[システム設定]** > **[ライセンス]** に移動します。



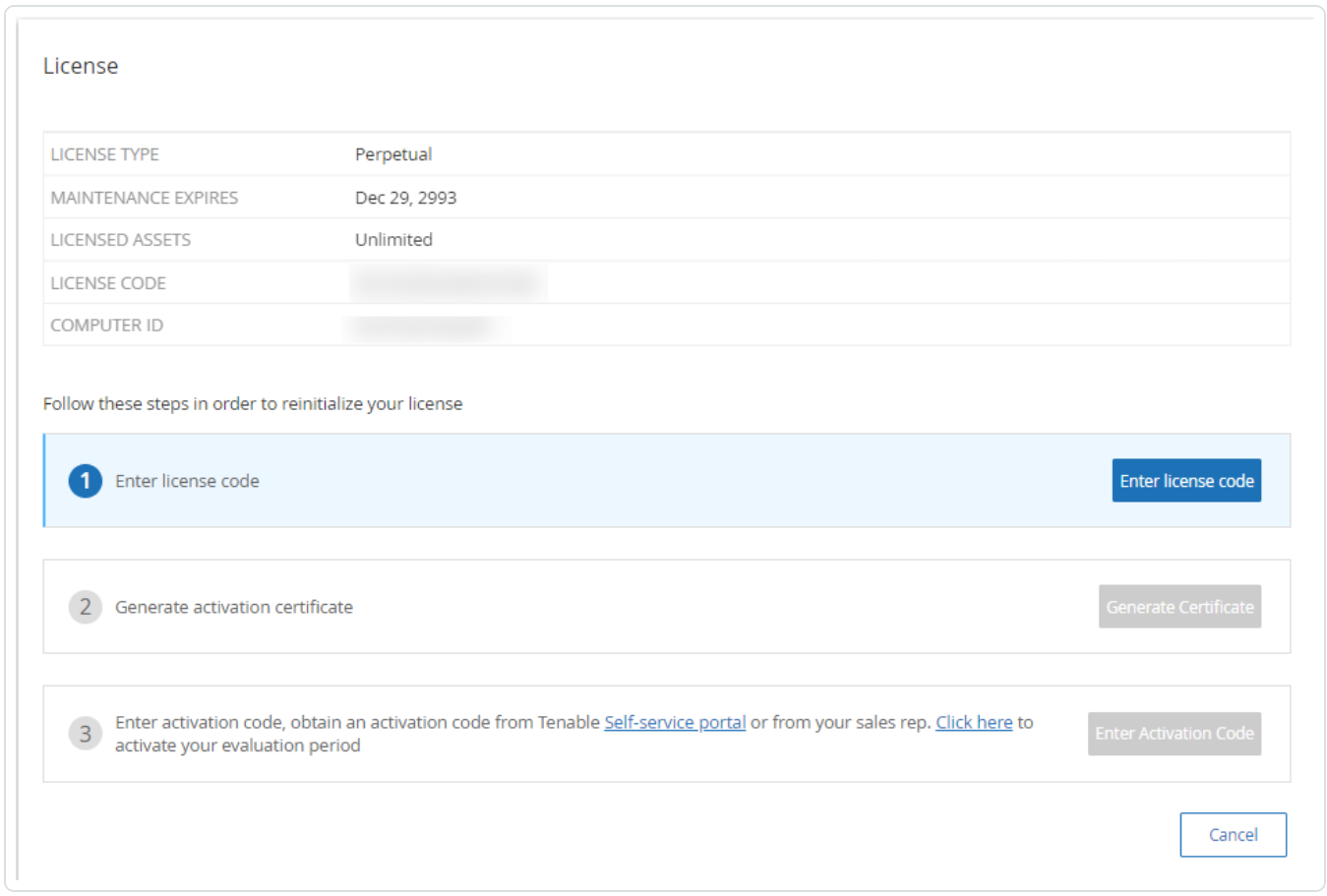
2. **[アクション]** メニューから **[ライセンスの再初期化]** を選択します。

   確認ウィンドウが表示されます。

3. **[再初期化]** をクリックします。



   [ライセンス] ウィンドウに 3 つの再初期化ステップが表示されます。



4. 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ブ化を参照してください。

   アクティベーションコードを入力した後、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。

次の手順

OT Security システムの有効化

OT Security の起動

目的: システムを起動し、OT セキュリティのニーズに合わせて使用を開始します。

Tenable Core + OT Security を設定した後、システムが OT Security の使用を開始できるようにします。

1. OT Security システムの有効化 – ライセンスをアクティベートした後、OT Security システムを有効化します。
2. OT Security の使用 – 監視対象ネットワーク、ポート分離、ユーザー、グループ、認証サーバーなどを設定して、OT Security の使用を開始します。

OT Security 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、OT Security に**[有効化]**ボタンが表示されます。

以下のようなシステムのコア機能をアクティブ化するには、OT Security を有効化してください。

- 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「対話」のログ記録

これらの機能からコンパイルされたすべてのデータと分析をユーザーインターフェースで表示できます。

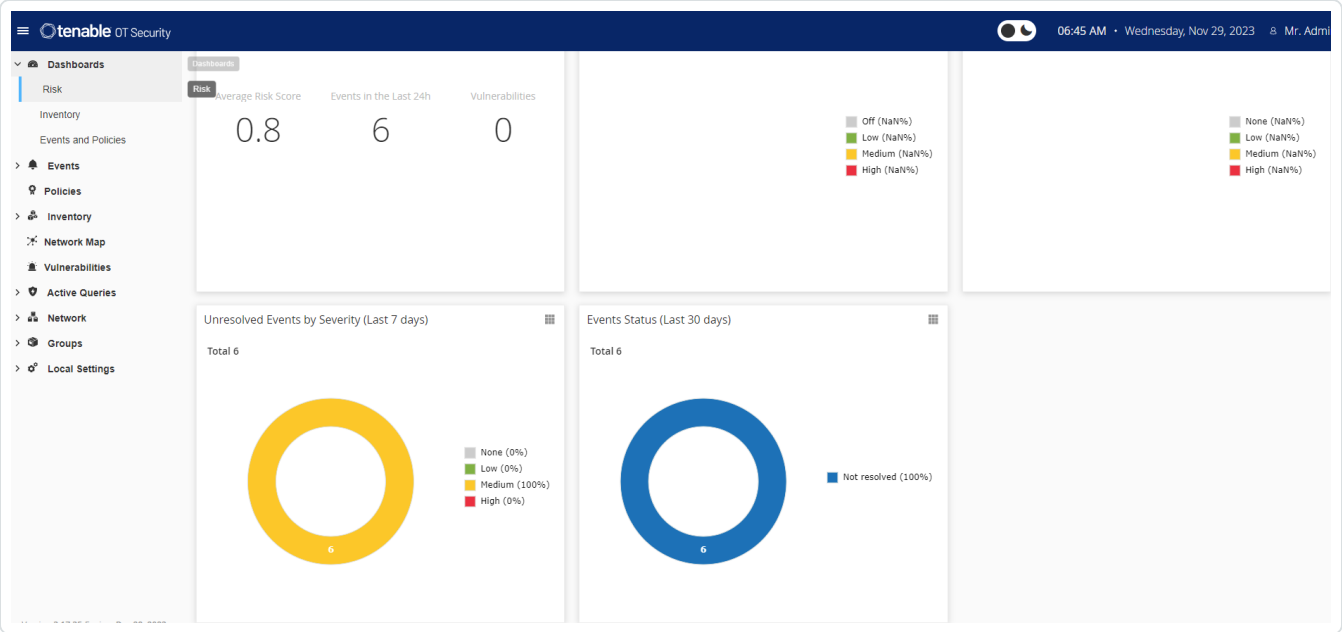
> **注意**: これらは継続的に進行するプロセスであり、完全に更新された結果がユーザーインターフェースに表示されるまでには時間がかかります。

アクティブクエリなど、追加の機能を設定してアクティブ化する場合は、管理コンソール(ユーザーインターフェース)の**[ローカル設定]**ウィンドウで行えます。詳細については、アクティブクエリを参照してください。

OT Security を有効化するには、次のようにします。

1. **[有効化]**をクリックします。

   OT Security によりシステムが有効になり、**[ダッシュボード]** > **[リスク]** ウィンドウが表示されます。



> **注意**: 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。

OT Security の使用の開始

インストール後、OT Security を設定して使用できます。

監視対象ネットワークを設定する

OT Security が監視するネットワークセグメントを設定し、ネットワークに関連するすべてのエリアが含まれるようにします。監視対象ネットワークを参照してください。

> **注意**: 不要な監視対象ネットワークを削除してください。そのネットワークから追加した資産を非表示にできます。詳細は、資産の非表示を参照してください。

ポートを確認して設定する

まだ実行していない場合は、[管理ポートとアクティブクエリポートの分離]を選択できます。

ユーザー、グループ、認証サーバーを設定する

ローカルユーザーとユーザーグループを設定します。外部認証サーバーを設定するか、SAML を利用して SSO ログインを容易にすることができます。

ネットワークサービスを追加する

DNS サーバーと NTP サーバーを追加します。また、すべての重要なイベントを取得するため、Syslog と E メールサーバーを設定できます。

アクティブクエリを有効化する

アクティブクエリは、OT Security の主な利点の 1 つです。資産に直接アクセスして、最も正確でほぼリアルタイムの詳細情報と可視性を得ることができます。詳細については、アクティブクエリを参照してください。

アクティブな資産検出 – サイレントな資産やパッシブモニタリングトラフィックではカバーできない資産を、プロアクティブにプローブして検出します。

Nessus スキャンを作成する

OT Security ネットワークにある IT デバイスに対して実行する Nessus スキャンを設定します。Tenable Nessus スキャンは安全で、検出された IT 資産にのみ影響を与えます。詳細については、Nessus プラグインスキャンの設定を参照してください。

バックアップを設定する

定期的なシステムバックアップを設定し、ローカルに保存するか、リモートストレージにエクスポートするかを選択します。詳細については、Application Data Backup and Restore (アプリケーションデータのバックアップと復元) を参照してください。

アップデートを入手する

フィードとシステムのアップデートを必ず確認してください。システムがオフラインの場合は、必ず定期的に手動アップデートを実行してください。詳細については、アップデートを参照してください。

最適化する

OT Security が起動して実行されたら、生成されたイベントを確認し、環境要件に応じてポリシーを最適化します。

統合する

OT Security を他の Tenable 製品またはサードパーティサービスと統合します。詳細については、統合を参照してください。

OT Security センサーのインストール

注意: このセクションでは、バージョン 3.14 以降のセンサーを設定する手順について説明します。

OT Security センサーのインストールには、センサーと Industrial Core Platform (ICP) とのペアリングが含まれます。センサーと OT Security ICP をペアリングするには、ICP 管理コンソールとセンサーの Tenable コアユーザーインターフェースの両方を使用します。

着信ペアリングリクエストの自動承認を有効にするか、自動承認を無効にして、新しいセンサーのペアリングリクエストごとの手動承認のみを許可することができます。

始める前に

次の条件が満たされていることを確認します。

- センサーハードウェアが適切に設置されている (センサーの設定手順を参照)。
- センサーがネットワークスイッチに接続されている (ネットワークへのセンサーの接続を参照)。
- センサーに独自の静的 IPv4 アドレスがある (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に関する詳細については、Tenable Core + Tenable OT Security ユーザーガイド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 (証明書を参照)。

注意: 接続の切断を回避するために、Tenable では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推奨しています (ローカルユーザーの追加を参照)。新しい管理者ユーザーを追加して、複数のセンサーをペアリングできます。

注意: Tenable Core のマシンにオフライン更新を適用する方法については、Update Tenable Core Offline (Tenable Core のオフラインアップデート) を参照してください。

センサーのペアリング

v.3.14 以降のセンサーと ICP のペアリング手順

1. ICP 管理コンソール(ユーザーインターフェース)で、**[ローカル設定]** > **[センサー]** ウィンドウに移動します。

2. センサーペアリングの自動承認を有効にするには、ページ上部にある **[受信センサーのペアリングリクエストを自動承認する]** スイッチを **[オン]** に切り替えます。オンになっていない場合は、すべてのペアリングリクエストを手動で承認しなければなりません。

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を開きます。

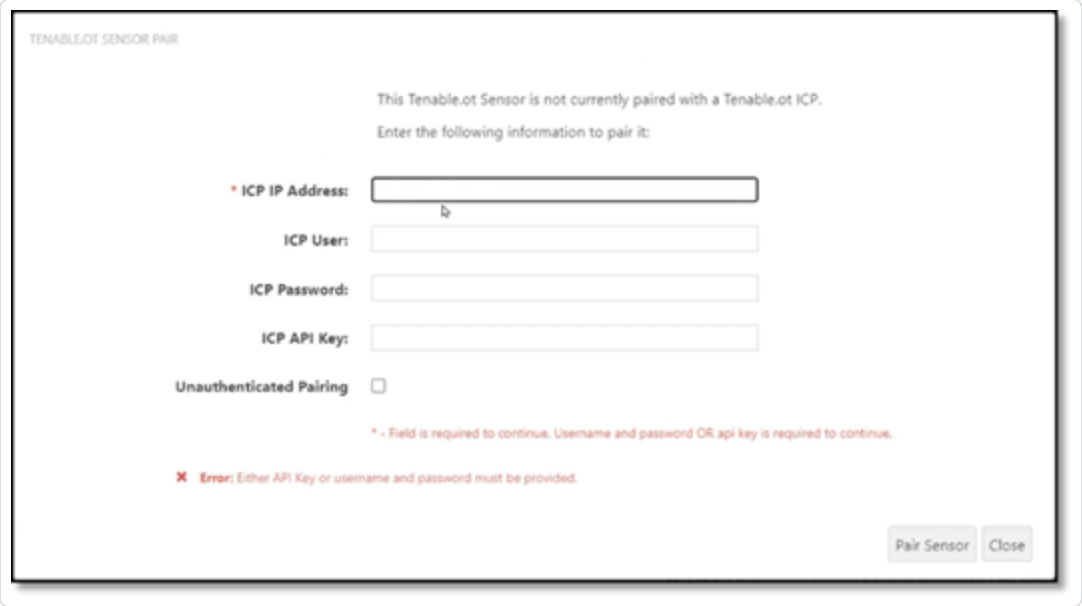
   注意: Tenable Core ユーザーインターフェースには、最新バージョンの Chrome からのみアクセスできます。

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。

   重要: ログイン時に **[特権タスクでパスワードを再利用する]** を選択しないと、センサーサービスを再起動できなくなります。

5. ナビゲーションメニューバーで **[OT Security センサー]** をクリックします。

[OT Security センサーペア] ウィンドウが表示されます。



注意: **[Tenable OT Security センサーペア]** ウィンドウは、ページの初回読み込み時にのみ表示されます。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]** ボックスに、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には、**[認証されていないペアリング]** を選択し、手順 8 に進みます。

注意: **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スキャンすることしかできず、ICP はセンサーを管理してアクティブクエリを送信することができません。

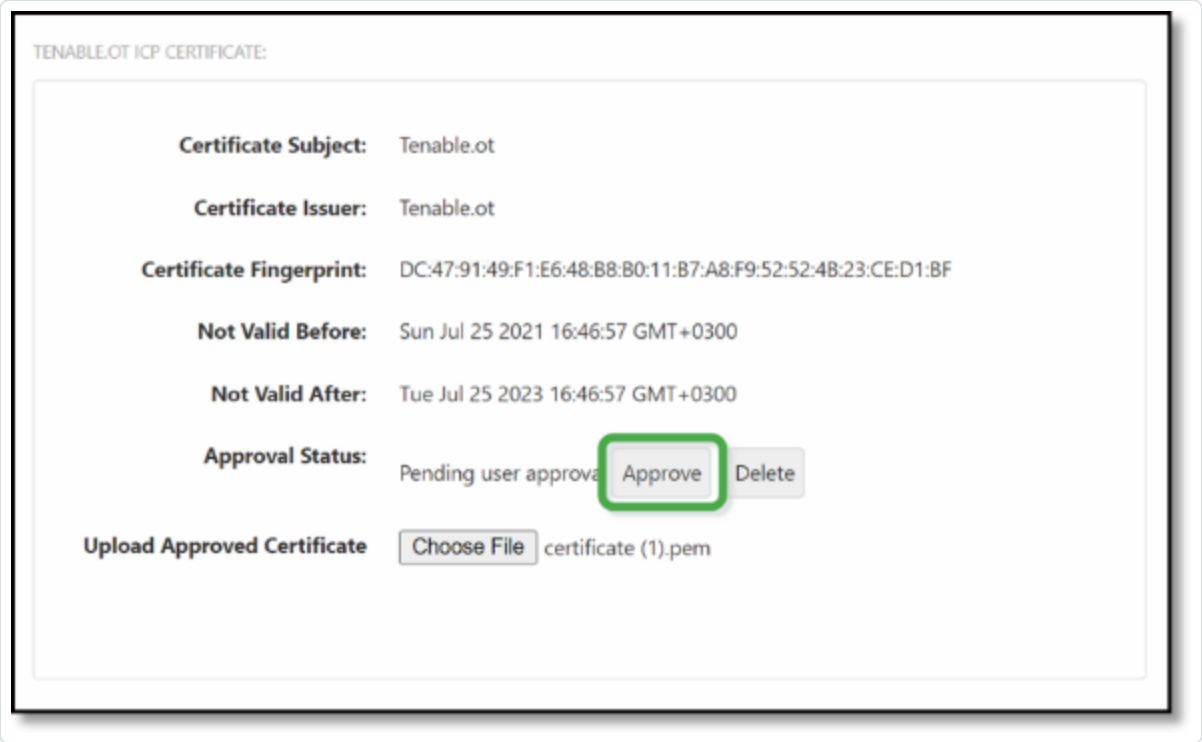
8. ペアリングを認証するには、次のいずれかを実行します。
   - **[ICP ユーザー]** ボックスに ICP ユーザー名を、**[ICP パスワード]** ボックスに ICP パスワードを入力します。
   - **[ICP API キー]** ボックスに ICP の API キーを入力します。

注意: ペアリングプロセス中の接続を確保するために、Tenable では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推奨しています (ローカルユーザーの追加を参照)。

注意: ユーザー名とパスワードを使用する認証方法には、最終的に期限切れになる API キーとは異なり、認証情報が期限切れにならないというメリットがあります。

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** 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ちます。



    b. **[承認]** をクリックして証明書を承認します。

    c. **[Tenable OT Security サーバー証明書の承認の確認]** ウィンドウで、**[この証明書を承認する]** をクリックします。

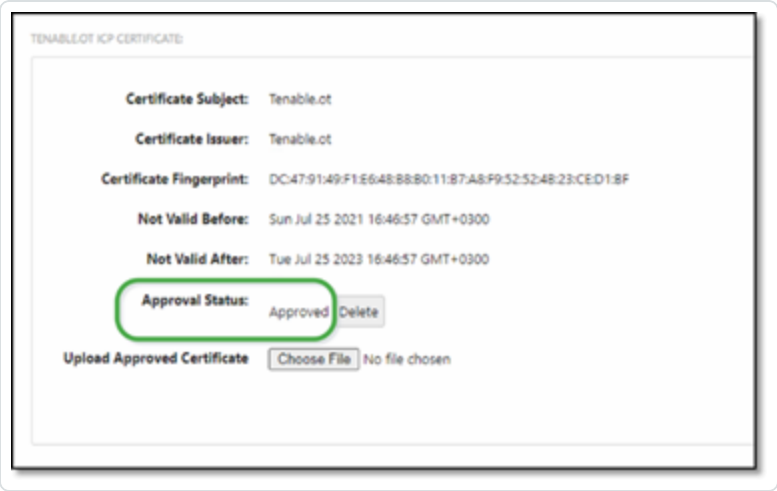
    証明書を手動でアップロードする場合

    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]** 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。

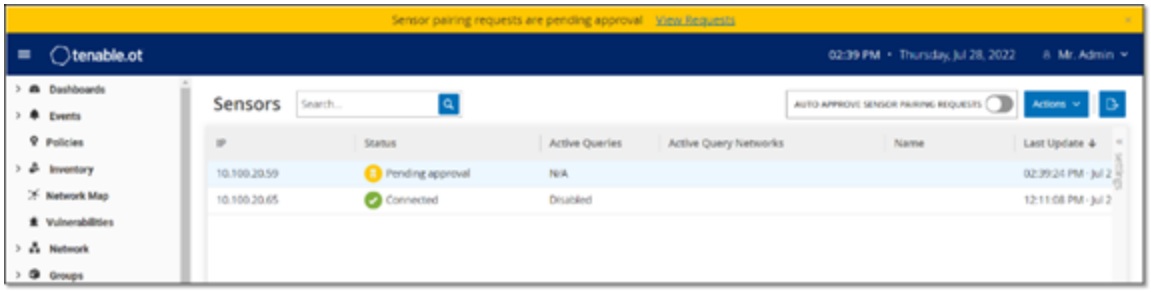
c. アップロードする **.pem** 証明書ファイルに移動します。

有効な証明書が正しく読み込まれると、**[OT Security ICP 証明書]** 表の **[承認ステータス]** が **[認証済み]** と表示されます。

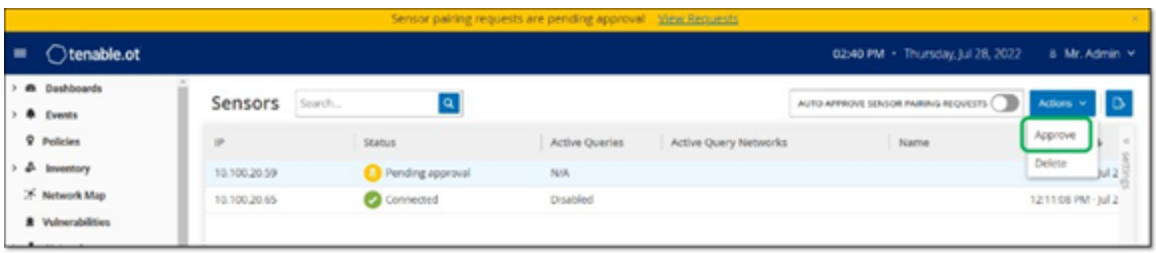


11. ICP ユーザーインターフェースで、**[ローカル設定]** > **[センサー]** に移動します。

OT Security により新しいセンサーが表に表示され、**[ステータス]** が **[承認待ち]** になります。



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。



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が原因である可能性があります。たとえば、トンネルエラーや API の問題です。
- **接続済み (トンネルエラー)** – ペアリングは成功しましたが、トンネル経由の通信を行えません。センサーから ICP へのポート 28304 の接続を確認します。詳細は、ファイヤーウォールの考慮事項を参照してください。

OT Security による認証済みセンサーのペアリングが完了したら、そのセンサーに実行するアクティブクエリを設定できます。アクティブクエリの管理を参照してください。

注意: Tenable は、ペアリングが完了したら Tenable Core ユーザーインターフェースではなく、ICP ページのみを使用してセンサーを管理することを推奨しています。

センサーの設定手順

センサーには、OT Security センサーコンポーネント で説明されているように、ラックマウントセンサーと設定可能なセンサーの 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。設定可能なモデルは、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)。

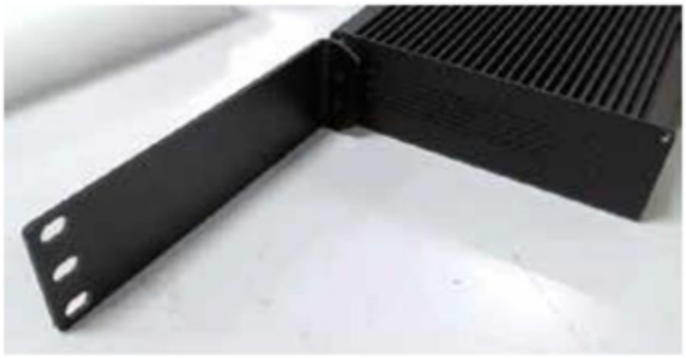
ラックマウントセンサーのセットアップ

センサーは、標準の 19 インチラックに取り付けることも、机などの平面に設置することもできます。

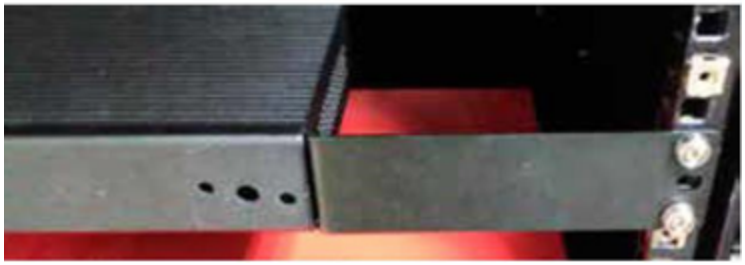
ラックマウント (ラックマウントモデル用)

OT Security 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. 付属のラックマウント用ブラケットをラックマウントに適合するネジ (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。



重要:

- 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
- 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を確認してください

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

OT Security 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。

重要:

- 机上が平らで乾いていることを確認してください
- 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を確認してください

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。

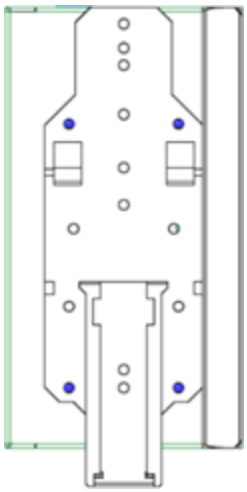
設定可能なセンサーのセットアップ

設定可能なセンサーは、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

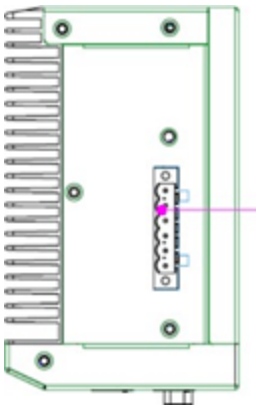
OT Security 設定可能なセンサーの標準 DIN レールへの取り付け手順

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(設定可能なモデル用)

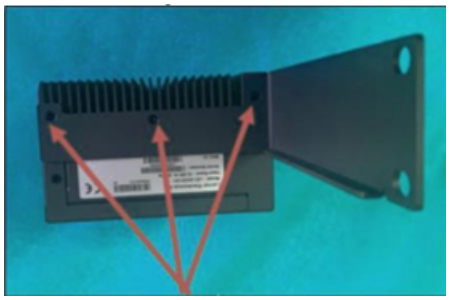
設定可能なセンサーは、付属している「マウントイヤー」を使用して、マウントラックに取り付けることができます。

設定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. 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。



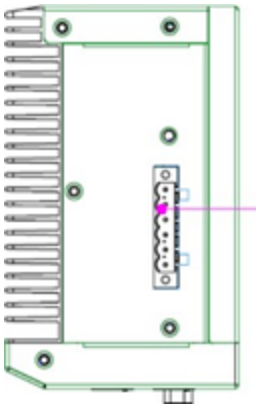
2. サーバーユニットをラックの空いている 1U スロットに挿入します。

> **注意**:
>
> - 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
> - 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を確認してください

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。

センサーのネットワーク接続

OT Security センサーは、ネットワークトラフィックを収集して OT Security 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します。

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します。これは、ネットワーク監視の実行に使用するネットワークとは異なるネットワークでもかまいません。

OT Security 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. OT Security 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。

OT Security 設定可能なセンサーのネットワークへの接続手順

1. OT Security 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。

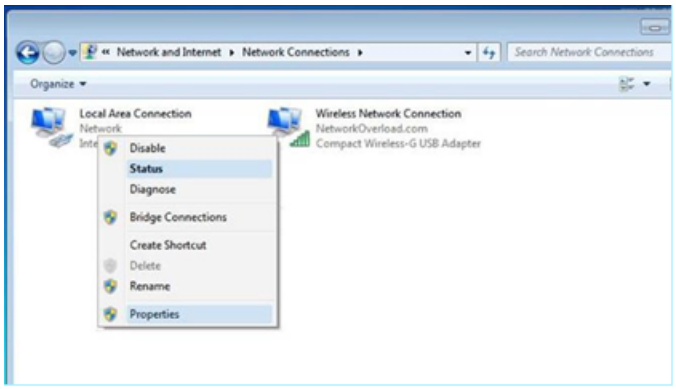
センサーセットアップウィザードへのアクセス

管理コンソールへのログイン手順

1. 次のいずれかを実行します。
   - 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 OT Security 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、OT Security 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(OT Security 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。

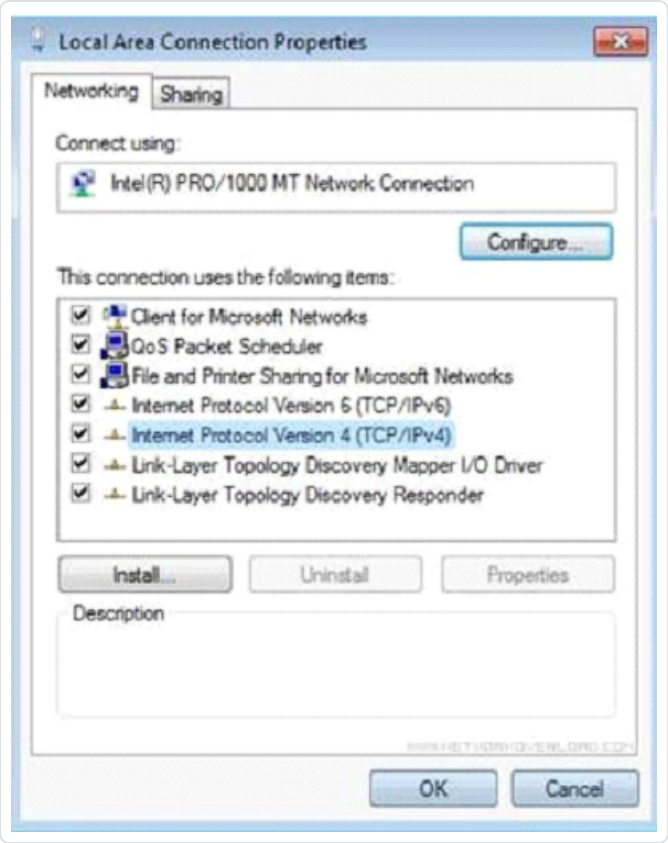
   > **注意**: Windows のバージョンによって、ナビゲーションが若干異なる場合があります。

   [ネットワーク接続] ウィンドウが表示されます。

   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) のプロパティ] 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] ボックスに、「**192.168.1.10**」と入力します。

f. **[サブネット マスク]** ボックスに、「255.255.255.0」と入力します。

g. **[OK]** をクリックします。

OT Security により新しい設定が適用されます。

4. Chrome ブラウザで、https://192.168.1.5:8000 に移動します。

> **注意**: ユーザーインターフェースは Chrome ブラウザからしかアクセスできません。Chrome の最新バージョンを使用してください。

5. センサーをペアリングします。

CLI で行うバックアップの復元

次の方法を使用して、OT Security のバックアップを復元できます。

- Tenable Core ユーザーインターフェースを使用する。Tenable Core + Tenable OT Security ユーザーガイドのバックアップの復元を参照してください。
- `systemd` コマンドを使用する。CLI を使用した復元を参照してください。

注意: 復元できるのは、Tenable Core バックアップユーティリティを使用して作成したバックアップのみです。バージョン 3.18 より前の OT Security からの古いバックアップには互換性がありません。3.18 より前の OT Security の古いバージョンでキャプチャしたバックアップから復元しようとする場合、必要な手順とコマンドについてはサポートにお問い合わせください。

始める前に

- 復元するバックアップ `.tar` ファイルがあることを確認します。SCP (セキュアコピープロトコル) ユーティリティを使用して、`.tar` ファイルを ICP システムにコピーします。

  注意: OT Security のバックアップファイルは、Tenable Core の **[バックアップ/復元]** ページからダウンロードできます。詳細については、バックアップの復元を参照してください。
  OT Security バックアップファイルの例: `tenable-ot-tenable-s2cc78kg-2024-03-21T135648.tar`

CLI を使用して OT Security のバックアップを復元するには、次のようにします。

1. 次のいずれかを実行して、ICP システムにアクセスします。
   - Tenable Core にログインして、ターミナルにアクセスする。
   - SSH を使用してログインする。
2. ターミナルで、次のコマンドを実行します。

   ```
   sudo systemctl start tenablecore.restorelocal@$(systemd-escape <path to backup archive>)
   ```

   注意: バックアップを復元してからコマンドが終了するので、プロセス完了までに時間がかかります。復元の進行状況は、Tenable Core の **[復元]** にリストされているログから確認するか、次のコマンドを実行することで確認できます:
   `journalctl -xf tenablecore.restorelocal@$(systemd-escape <path to backup archive>)`
3. OT Security が実行されていることを確認するには、ブラウザからポート 443 (HTTPS) で OT Security ユーザーインターフェースにログインします。

管理コンソールのユーザーインターフェース要素

管理コンソールのユーザーインターフェースでは、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 OT Security 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。ユーザーインターフェースを使用して、ニーズに応じた OT Security プラットフォーム機能を設定できます。

主なユーザーインターフェース要素

次の表に、主なユーザーインターフェース要素の説明を示します。

ユーザーインターフェース要素	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は、**[バージョン情報]**(ソフトウェア情報を表示)と**[ログアウト]**です。 OT Security のアクティベーションが終わると、**[バージョン情報]**ビューで自分の Tenable カスタマー ID を確認できます。このカスタマー ID は、テクニカルサポートチームまたは Customer Success チームに連絡するときに必要です。
ライセンス情報	OT Security 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した画面が表示されます。
ダーク	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。

モード / デイライトモード	
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。

ダークモードを有効または無効にする

[ダークモード]トグルをオンにすることで、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るようになります。

ダークモードを有効または無効にする手順

1. ウィンドウ上部にある  (ダークモード)トグルをクリックします。

   OT Security により、選択した設定がすべての画面に適用されます。

2. デイライトモード設定に戻すには、  (デイライトモード)トグルをクリックします。

現在のソフトウェアバージョンの確認

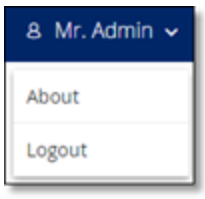
ヘッダーバーの右上隅のユーザープロファイルアイコンを使用して、ソフトウェアのバージョンを確認できます。

現在のソフトウェアバージョンの表示手順

1. メインヘッダーバーの右上隅にある 👤 アイコンをクリックして、メニューを開きます。

   OT Security にユーザーメニューが表示されます。

2. **[バージョン情報]**をクリックします。

OT Security に現在のソフトウェアバージョンが表示されます。

リソースセンターへのアクセス

リソースセンターには、製品のリリース情報、Tenable ブログ投稿、ユーザーガイドドキュメントなど、情報リソースのリストが表示されます。

> **注意**: **リソースセンター**にアクセスするにはインターネットが必要です。

リソースセンターにアクセスする方法

1. 右上の ⓘ ボタンをクリックします。

   [リソースセンター] メニューが表示されます。

2. リソースのリンクをクリックすると、そのリソースに移動します。次のリソースを利用できます。

   - OT Security ナレッジベースを検索
   - 新機能の最新情報

OT Security のナビゲーション

左側のナビゲーションパネルから次のメインページにアクセスできます。

- **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の全体を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、ポリシーにそれぞれ個別のダッシュボードがあります。ダッシュボードを参照してください。
- **イベント** – ポリシー違反の結果として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示す画面と、イベントタイプごとの個別の画面が表示されます。たとえば、設定イベント、SCADA イベント、ネットワーク脅威、ネットワークイベントなどです。イベント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。画面にはすべての資産が表示され、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** – OT Security プラグインによって検出された、ネットワーク内の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資産に対するその他の脅威 (古い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) が含まれます。
- **ネットワーク** – ネットワーク内の資産間で行われた対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。ネットワークを参照してください。
  OT Security では、この情報が 3 つのウィンドウに分けて表示されます。
  - **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。
  - **対話** – ネットワーク内で検出されたすべての対話のリストを、発生した時刻や関連する資産などの詳細とともに表示します。
- **グループ** – ポリシー設定で使用されるグループを表示、作成、編集します。グループ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設定します。ローカル設定を参照してください。

表のカスタマイズ

OT Security ページには、各アイテムのリストを含む表形式でデータが表示されます。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、関連情報に簡単にアクセスできます。

注意: ここで示した例は、**[すべてのイベント]** および **[すべての資産]** ページを対象としていますが、ほとんどのページ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。

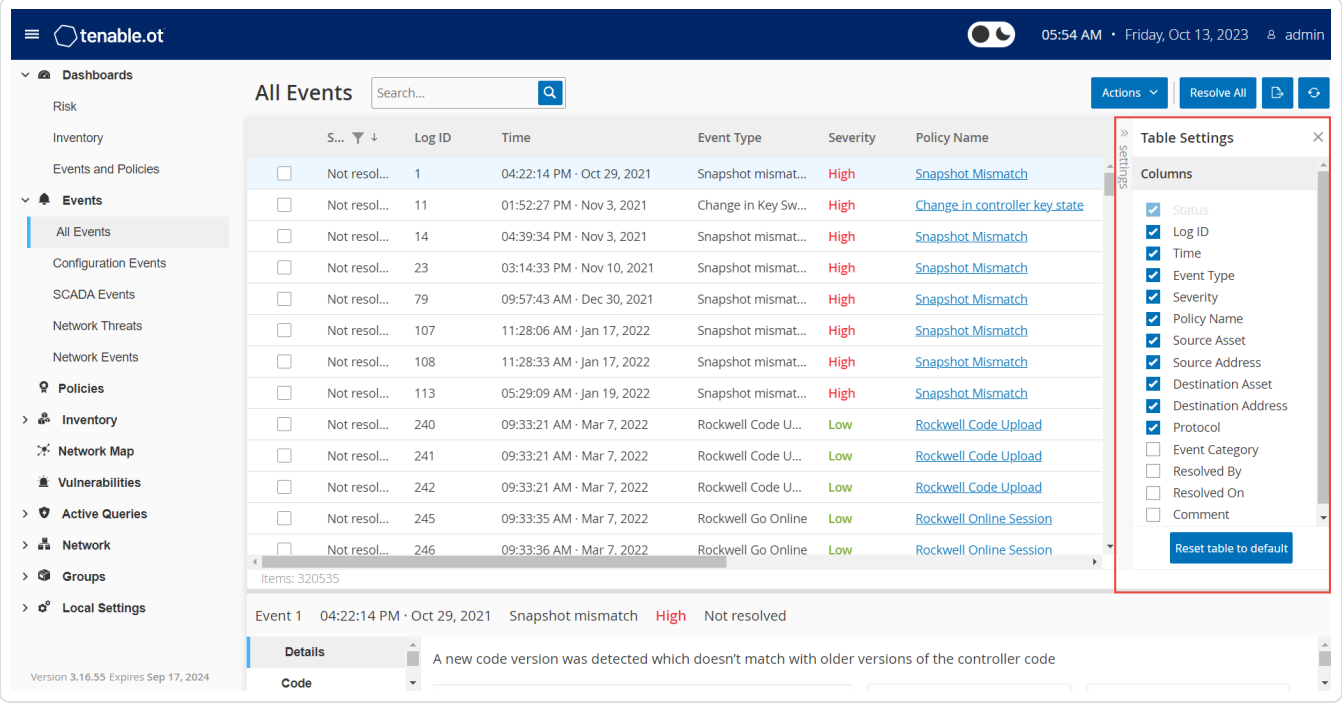
列表示のカスタマイズ

表示する列とその構成方法をカスタマイズできます。

表示する列の指定手順

1. 表の右側にある **[設定]** をクリックします。

   [テーブル設定] パネルが、**[列]** セクションとともに表示されます。



2. **[列]** セクションで、表示する列の横にあるチェックボックスを選択します。
3. 非表示にする列の横にあるチェックボックスのチェックを外します。

OT Security に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. 列のヘッダーをクリックして、目的の位置にドラッグします。

リストのカテゴリ別グループ化

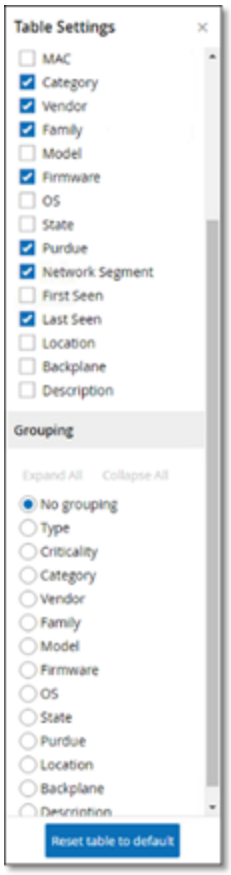
インベントリページで、その特定の画面に関連する各種パラメーターによってリストをグループ化できます。

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。

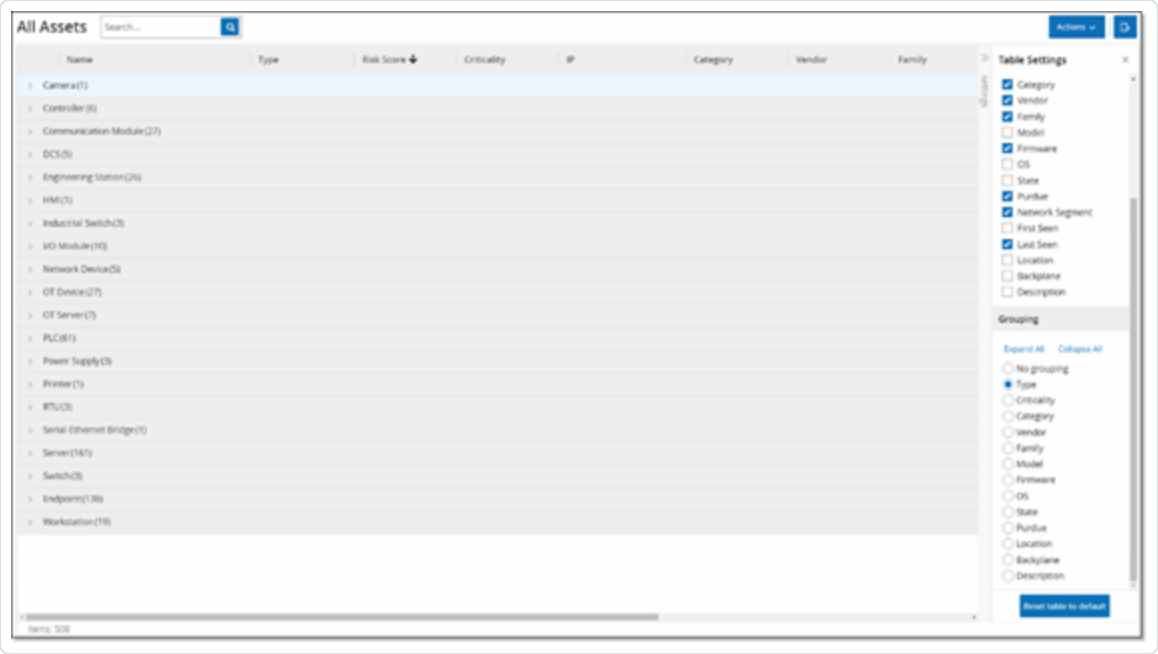
   [テーブル設定] ペインが右側に表示され、**[列]** セクションと **[グループ化]** セクションが表示されます。

2. **[グループ化]** セクションまでスクロールします。



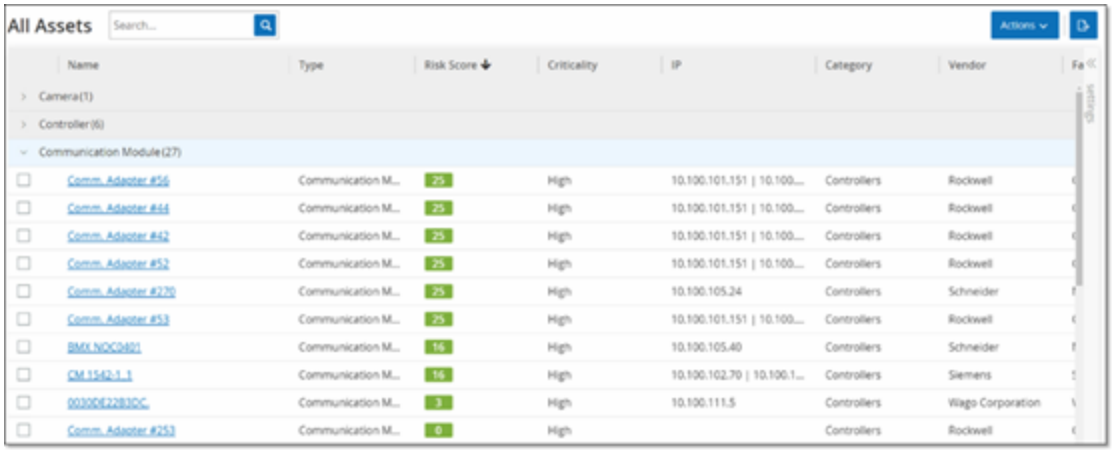
3. リストをグループ化する基準となるパラメーターを選択します。たとえば **[タイプ]** を選択します。

   OT Security は、グループ化されたカテゴリを表示します。



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。



列の並べ替え

リストの並べ替え手順

1. 列の見出しをクリックすると、そのパラメーターで資産が並べ替えられます。たとえば、資産を名前のアルファベット順で表示するには、**[名前]** 見出しをクリックします。
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)。

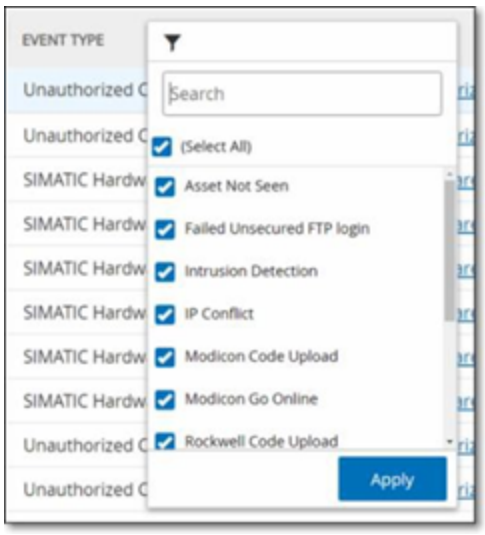
列のフィルタリング

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]** ウィンドウでは、**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横にあるチェックボックスを選択解除します。

   注意: **[すべて選択]** チェックボックスの選択を解除してから、表示する要素を選択します。

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。

   OT Security により、リストが指定された通りにフィルタリングされます。

> 列の見出しの横にあるフィルター ボタンは、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 ボタ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

各ページで、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. ボタ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

OT Security 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。

> **注意**: 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

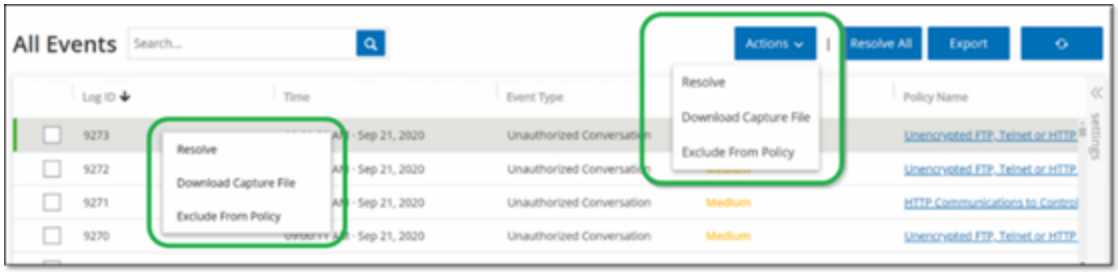
1. データをエクスポートする画面に移動します。
2. ヘッダーバーで **[エクスポート]** をクリックします。

アクションメニュー

各画面には、その画面の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。

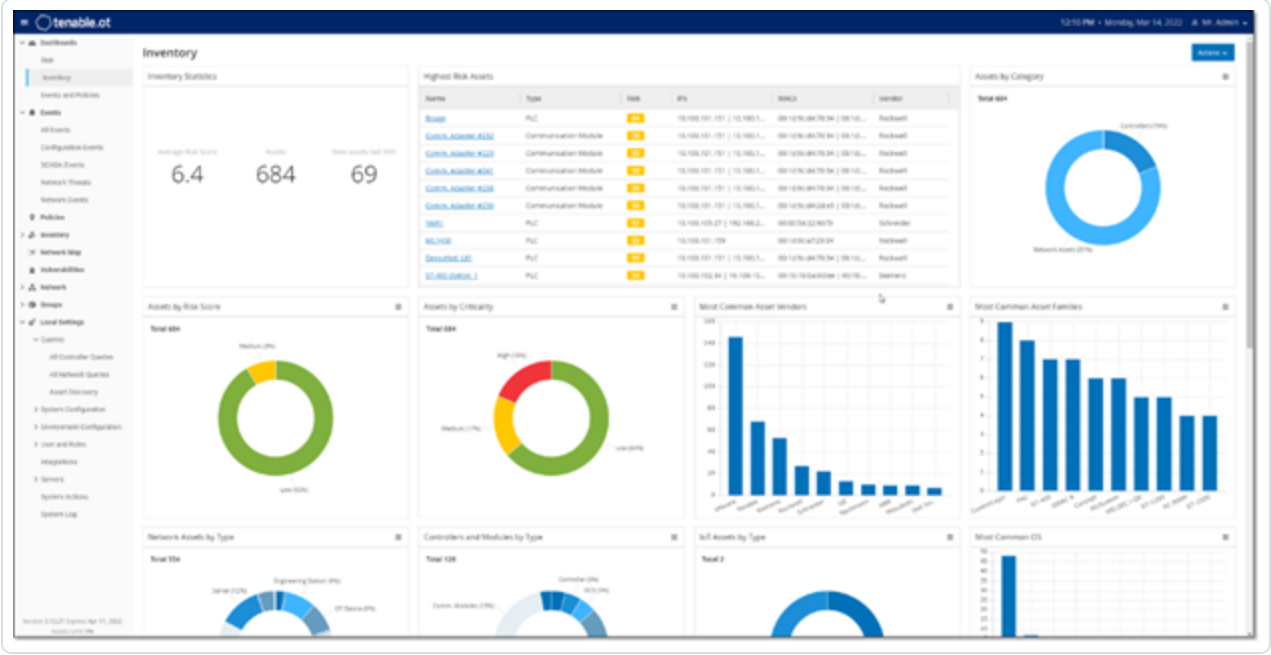
[アクション]メニューにアクセスするには、次のいずれかを行います。

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



ダッシュボード

OT Security には、**[リスク]**、**[インベントリ]**、**[イベントとポリシー]**の 3 つのダッシュボードがあり、ネットワークのインベントリとセキュリティ態勢を一目で確認できます。



ダッシュボードを選択する方法

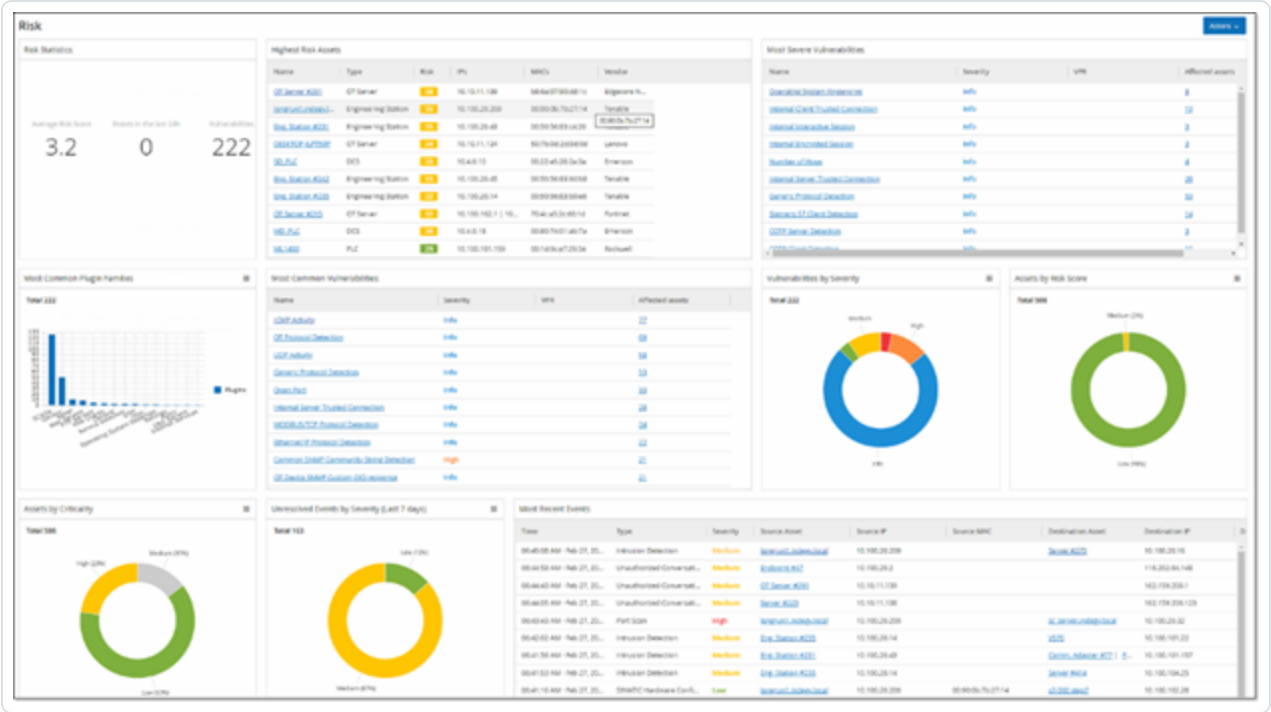
- メインナビゲーションメニューで **[ダッシュボード]** をクリックします。

[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。

表示設定を調整したり、フィルターを設定したりして、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。

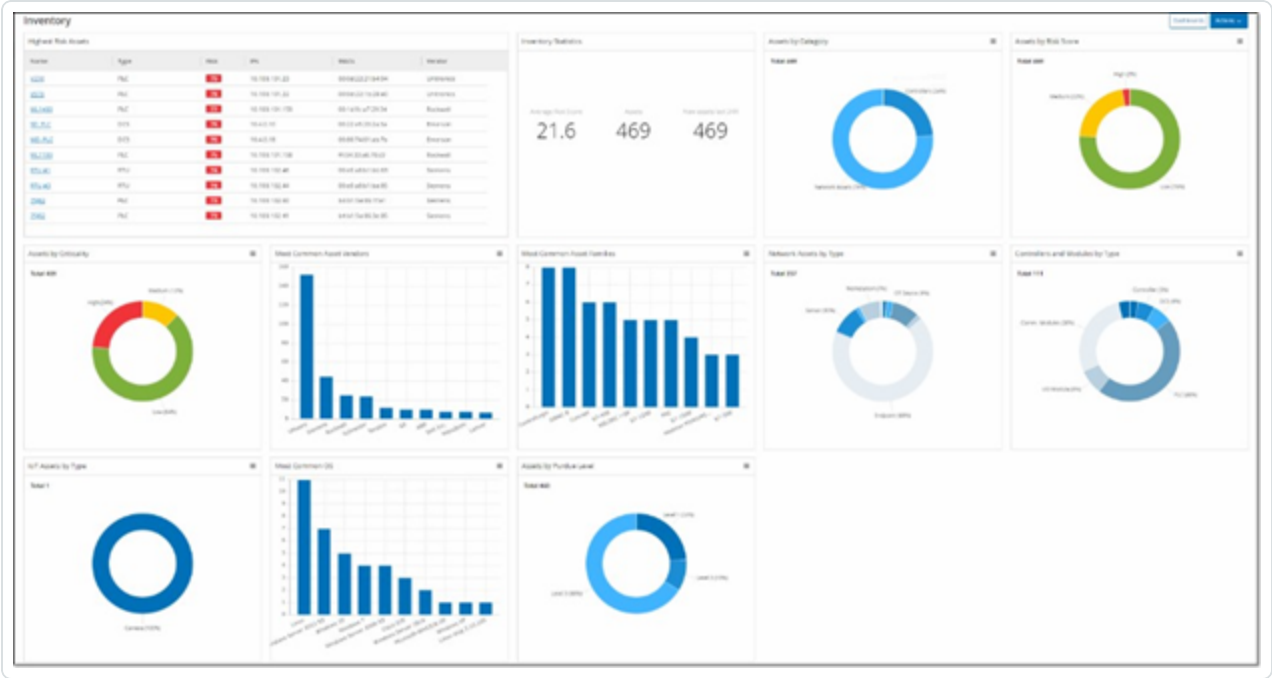


[リスク] ダッシュボードには、[リスク統計]、[リスクスコア別資産]、[資産(重大度別)]、[イベント(深刻度別)]、[最も一般的な脆弱性]などのウィジェットが表示されます。

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。

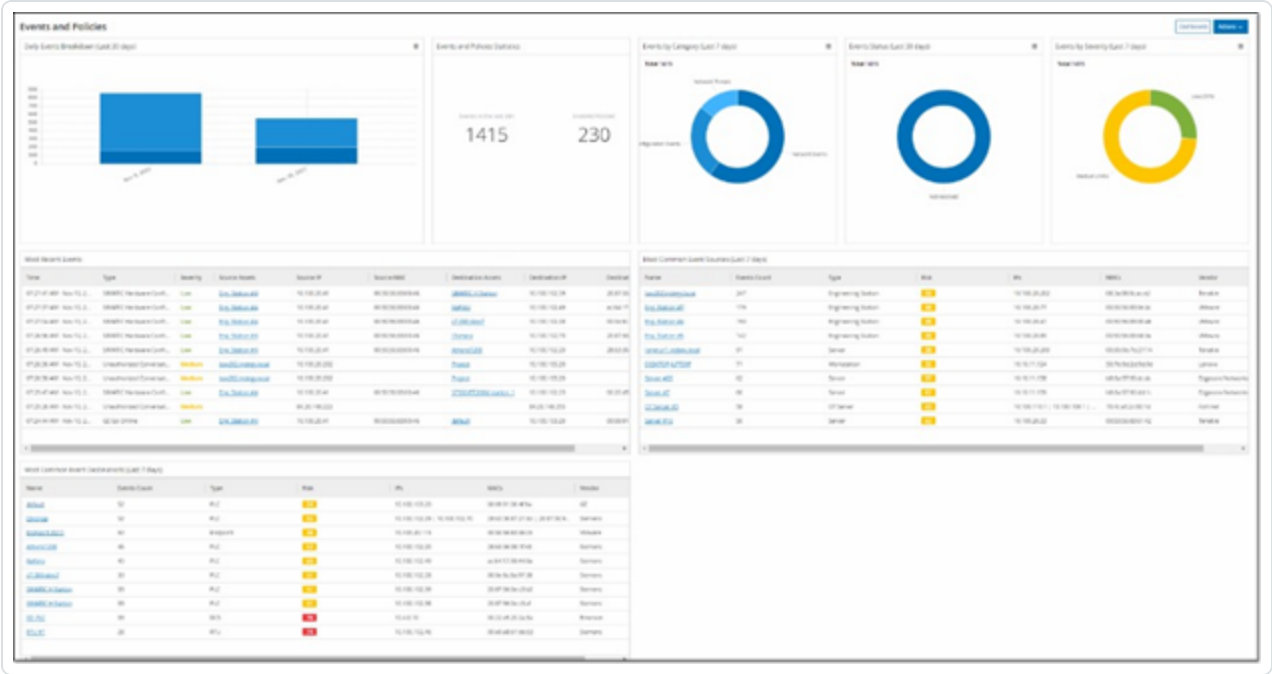


[インベントリ] ダッシュボードには、[リスクの最も高い資産]、[インベントリ統計]、[資産 (リスク別)]、[コントローラーとモジュール (タイプ別)]、[資産 (パデューレベル別)] などのウィジェットが表示されます。

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。

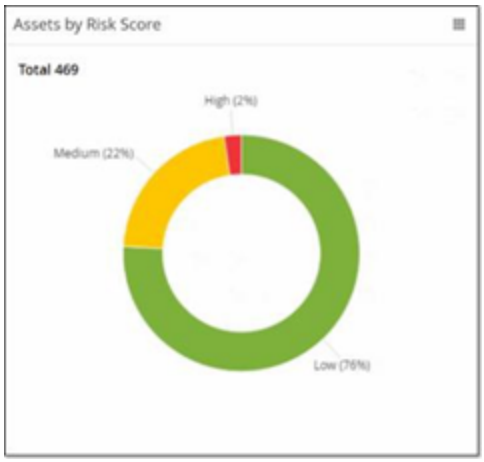
ダッシュボードの操作

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。表示モードが固定されているウィジェットもあれば、モードを切り替えることができるウィジェットもあります。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されます。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。

> **注意**: フィルターを適用できるのは、テーブルモードのみです。

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。

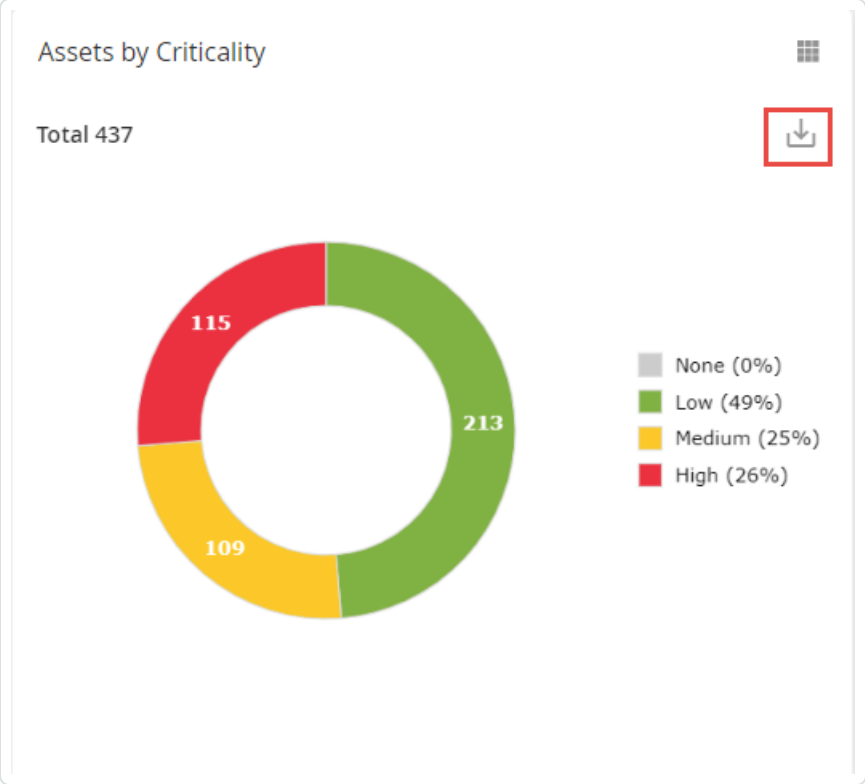


次 のように、ウィジェット を操 作 できます。

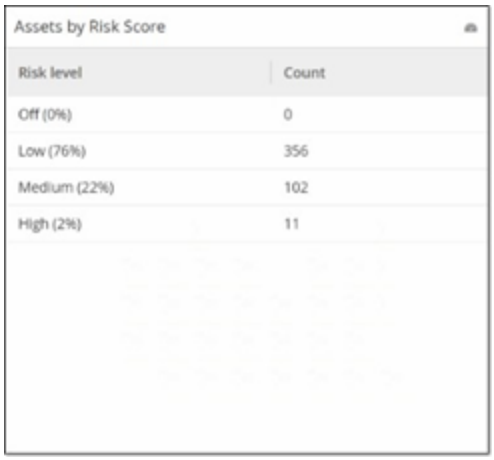
- グラフ上 のポイント にカーソルを合 わせると、グラフのそのセグメント に固 有 のデータを含 むウィンド ウが表 示されます。

- 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 ボタンをクリック

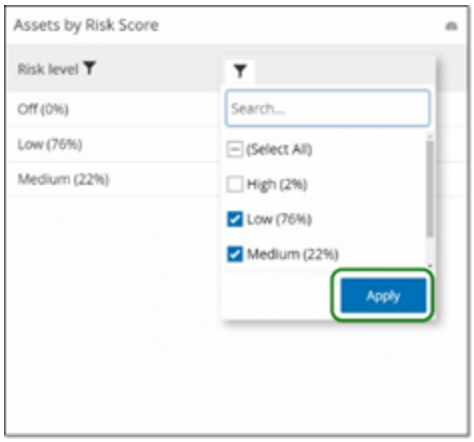
すると、グラフの画像をダウンロードできます。



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、テーブルモードに適用したフィルターはグラフに適用されません。



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使用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。

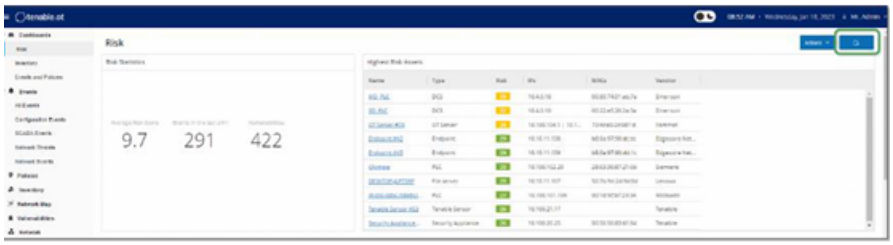
OT Security によりデフォルトのダッシュボードが更新され、次回管理コンソールにアクセスしたときにこのダッシュボードが表示されます。

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. ダッシュボード右上にある **[エクスポート]** 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。

   > **注意**: 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。

コンプライアンスダッシュボード

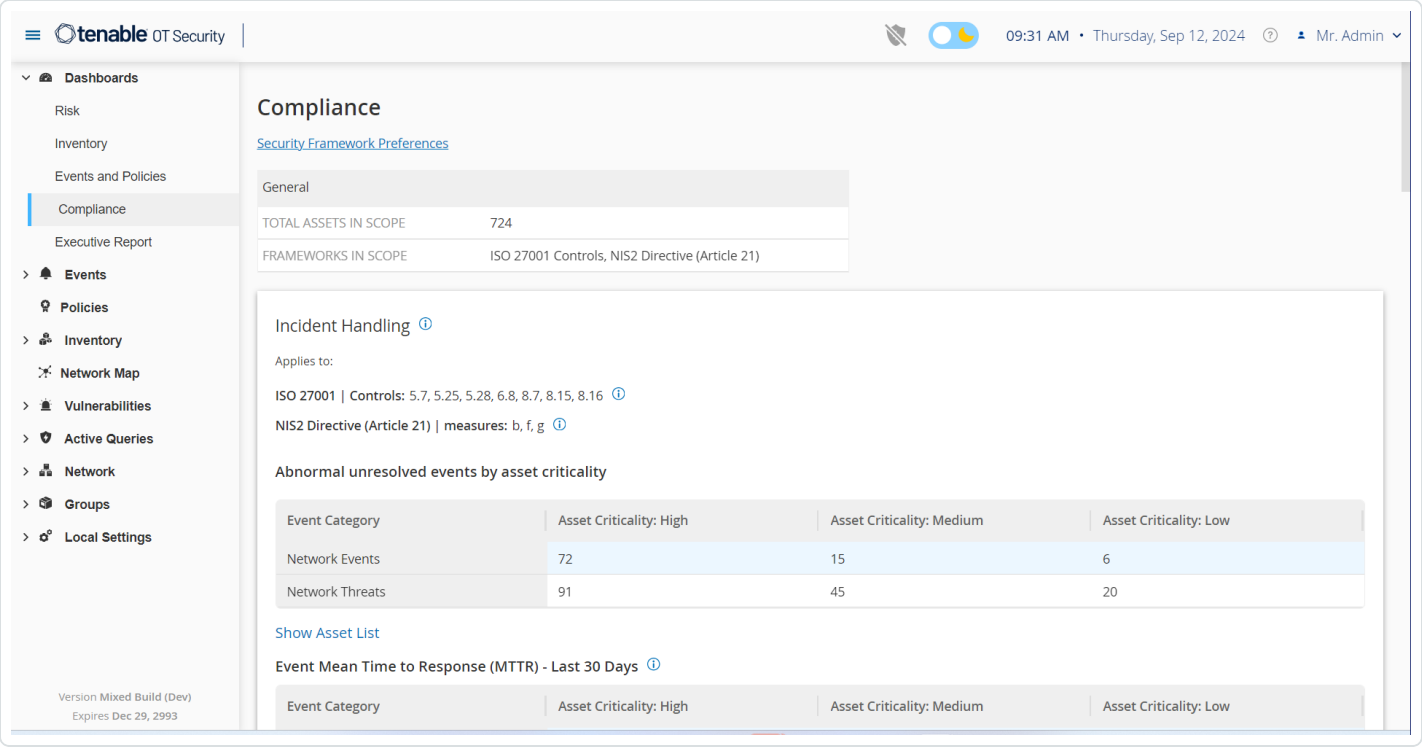
現在、重大なインフラを持つほとんどの企業で、NIS 2 指令や ISO 27001 管理策などのセキュリティフレームワークへのコンプライアンスの監査チェックが行われ、それをクリアすることが義務付けられています。

コンプライアンスフレームワークに対応していくことは、複雑なプロセスになる可能性があり、特殊な知識が必要です。**[コンプライアンス]** ダッシュボードでは、組織の重要な事業運営に影響を与える可能性のあるすべての資産、脆弱性、イベントの全体像を把握することができます。また、監査における次の重要な質問の答えを見つける手助けとなります。

- 疑わしいアクティビティを検出するために、どのセキュリティポリシーを施行しているか
- インシデントの処理にどのくらいの時間がかかるか
- アラートがインシデント対応 (IR) 計画の一部として SOC/SIEM と統合されているか
- 過去 1 週間または過去 1 か月間に、重大な資産で何件のセキュリティイベントが発生したか

[コンプライアンス] ダッシュボードを使用すると、主要なセキュリティ対策を規制要件に適合させたり、進捗状況と改善を経時的に追跡したり、セキュリティ態勢を強化したりできます。

このダッシュボードデータを使用すると、組織がコンプライアンスに対応している分野を特定し、リスクの観点からビジネスに影響を与える分野を改善できます。



[コンプライアンス] ダッシュボードを表示するには、次のようにします。

1. 左側のナビゲーションバーで **[ダッシュボード]** > **[コンプライアンス]** をクリックします。

   [コンプライアンス] ダッシュボードが表示されます。

注意: セキュリティフレームワークの設定を行うには、**[ローカル設定]** > **[システム設定]** > **[コンプライアンス]** に移動します。詳細は、コンプライアンスダッシュボードの設定を参照してください。

ダッシュボードには次のウィジェットが含まれています。

ヒント: 各ウィジェットが対応しているフレームワーク対策の詳細については、ウィジェットセクションの横にある ⓘ アイコンにカーソルを合わせてください。

ウィジェット	説明

インシデント対応	リスクのある資産の概要を、資産の重大度(高、中、低)別に表示します。このデータを使用して、高リスクのセキュリティインシデントに対応できます。 過去 30 日間の重大度が高いイベントの解決に基づいて、OT Security は**イベント平均対応時間 (MTTR)** を記録します。この値は、各重大イベントへの対応に要した平均時間を把握するのに役立ちます。MTTR は重要な KPI であり、MTTR 値が短いほど、インシデント解決プロセスが効率的であることを示します。 **注意**: 疑わしい未対応のイベントがある高リスク資産をすべて表示するには、**[資産リストを表示する]** リンクをクリックします。資産リストを閉じるには、**[資産リストを非表示にする]** をクリックします。
脆弱性対応	すべての脆弱性の概要を、その深刻度と影響を受けている資産タイプ別に表示します。このウィジェットを使用すると、OT、ネットワーク、IoT の脆弱性を継続的に特定、評価、報告、修正できます。 過去 90 日間に修正された脆弱性に基づいて、OT Security は**平均対応時間 (MTTR)** を記録します。MTTR とサービスレベル契約 (SLA) のパラメーターは、各重大脆弱性への対応に要した平均時間を把握し、定義された SLA に基づいて脆弱性軽減に対応するチームの進捗状況を追跡するのに役立ちます。MTTR の値が短いほど、インシデント解決プロセスが効率的であることを示します。 **注意**: アクティブで重大な脆弱性がある高リスク資産をすべて表示するには、**[資産リストを表示する]** をクリックします。資産リストを閉じるには、**[資産リストを非表示にする]** をクリックします。
設定および変更管理	ベースライン設定後の変更など未解決の設定イベントがあるすべての資産と、デバイスの停止などの重大なコントローラーステータスのアクティビティがあるすべての資産の概要を示します。このウィジェットのデータは、不正な変更や重大イベントを検出するのに役立ちます。これにより、サービスの中断時にも、運用継続性と迅速な回復を確保できます。 **注意**: 設定変更イベントのある高リスク資産を表示するには、**[資産リストを表示する]** リンクをクリックします。資産リストを閉じるには、**[資産リストを非表示にする]** をクリックします。
外部エクスポージャーのリ	産業用制御システム (ICS) ネットワークへの外部接続の概要を示します。このウィジェットのデータを使用すると、予期しない外部通信の OT、ネットワーク、IoT 資産を識別、

スク	評価、軽減しやすくなります。ICS 機器および機械ビルダーのベンダーがハイブリッドモデルを使用し、ポータルやエンジニアリングステーションを、外部エクスポージャーの可能性があるクラウドに移行する場合、このデータはサプライチェーンセキュリティのコンプライアンスも確保します。
安全でない暗号	安全でないログインや暗号化されていない認証情報など、安全でない暗号化イベントの概要を提供します。このデータは、安全でない暗号化イベントを監視し検出することで、機密情報の侵害やサービスの中断を防ぐのに役立ちます。 **注意**: 安全でない認証イベントのある高リスク資産をすべて表示するには、**[資産リストを表示する]**をクリックします。資産リストを閉じるには、**[資産リストを非表示にする]**をクリックします。
安全でない通信監視	安全でない通信イベントや不正アクセスのある高リスク資産の概要を提供します。このデータは、機密情報や重大な資産が攻撃者に対して脆弱になる、安全でない通信や疑わしい不正アクセスを回避するのに役立ちます。 **注意**: 安全でない認証イベントのある高リスク資産をすべて表示するには、**[資産リストを表示する]**をクリックします。資産リストを閉じるには、**[資産リストを非表示にする]**をクリックします。
リスク評価	リスクのある資産の概要を重大度別に表示します。このデータは、OT、ネットワーク、IoT 資産に関連付けられているリスクを評価して管理し、潜在的な脅威をプロアクティブに特定して軽減するのに役立ちます。 **注意**: リスクが高い資産をすべて表示するには、**[資産リストを表示する]**リンクをクリックします。資産リストを閉じるには、**[資産リストを非表示にする]**をクリックします。

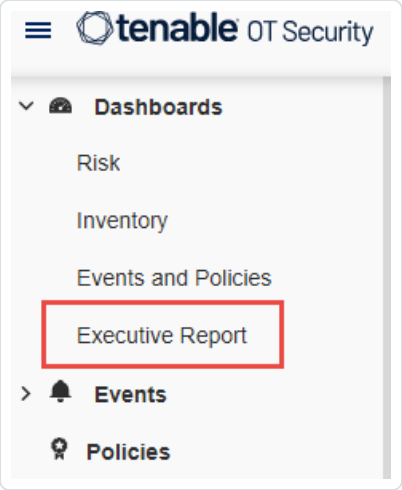
エグゼクティブレポートの生成

過去 30 日間のデータに基づいて、ご利用の環境のリスク評価レポートを生成できます。OT Security は、**[リスク]**、**[インベントリ]**、**[イベントとポリシー]**ダッシュボードの主要ウィジェットを使用して、グラフィカルな概要を作成し、高リスクの資産、重大な脆弱性と一般的な脆弱性、一般的なプラグインファミリー、および最近検出された資産をハイライトします。

レポートのチャート (深刻度別の脆弱性、リスクスコア別の資産、重大度別の資産など) を使用して、過去 30 日間における、環境内の重大な資産と最も深刻な脆弱性を特定します。

マンスリーレポートを生成する方法

1. 左側のナビゲーションバーで、**[ダッシュボード]** > **[エグゼクティブレポート]** に移動します。



   OT Security がブラウザでレポートを開きます。

2. レポートを PDF としてダウンロードするには、ページ上部にある **[PDF で保存する]** をクリックします。

   [印刷] ダイアログボックスが表示されます。

3. **[送信先]** ドロップダウンボックスで、**[PDF に保存]** を選択します。

4. レポートを保存する場所を参照します。

5. **[保存]** をクリックします。

   OT Security は、レポートを PDF 形式で保存します。

ポリシー

OT Security に含まれているポリシーは、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。システムによりイベントが記録され、ポリシーで設定されている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** – OT Security によって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。

OT Security 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できます。

注意: 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 / オフについては、ポリシーを有効または無効にするを参照してください。

ポリシー設定

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設定があります。

グループ

OT Security のポリシーの定義で重要な要素は、グループの使用です。ポリシーを設定する場合、各ポリシー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属しています。これにより、ポリシー設定プロセスが効率化されます。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設定で使用されます。

- **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資産グループを定義する、カスタムのネットワークセグメントを作成することもできます。

- **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します。たとえば、Rockwell コントローラーで開いているポートなどです。
- **プロトコルグループ** – 通信プロトコルを、プロトコルのタイプ別 (Modbus など)、製造元別 (Rockwell 使用可能プロトコルなど) などでグループ化します。
- **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します。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します。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** – Suricata Signature ID (SID) で識別される関連ルールをグループ化します。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、システムで設定されたグループのみです。システムには、事前定義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。グループを参照してください。

注意: 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設定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、さまざまな深刻度レベルの説明を示します。

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。**[イベント]** セクションに **[すべてのイベント]** が表示されます。**[ポリシー]** ページには、イベントをトリガーしたポリシーの下にそのイベントが一覧表示され、**[インベントリ]** ページには、影響を受けている資産の下にイベントがリストされます。さらに、Syslog プロトコルを使用する外部 SIEM または指定された E メール受信者にイベントの通知を送信するように、ポリシーを設定できます。

- **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 OT Security で使用するように設定されています)。Syslog 通知の解釈方法については、OT Security Syslog Integration Guide (OT Security 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、脅威を軽減するための手順が含まれています。

ポリシーカテゴリとサブカテゴリ

OT Security はポリシーを次のカテゴリに分類しています。

- **設定イベント** – 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。次の 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化や、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設定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。イベントを必ず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、スケジュールのブロックリストと許可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** – 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、ネットワークに追加された資産やネットワークから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、懸念要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、事前に設定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、ポリシーによってイベントがトリガーされます。これらのポリシーを、特定のスケジュールや特定の資産に制限できます。ベンダー固有のプロトコルは便宜上ベンターによって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。OT Security には各タイプの事前定義ポリシーがあります。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。

設定イベント – 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。たとえば、ネットワーク内の資産間に実装された「コマンド」などです。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。コントローラーアクティビティタイプは、アクティビティが実行されるコントローラーのタイプと、特定のアクティビティによって定義されます。たとえば、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です。

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。

設定イベント – 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。

> **注意**: 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。
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、ある動作状態から別の状態に変化しました。たとえば、実行中、停止中、テストなどです。
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対する変更です。
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。

注意: 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	[影響を受ける資産グループ] で以前に特定された資産の中から、特定の時間範囲で特定の時間の長さの間ネットワークから削除されているものを検出します。
再発見された資産	非アクティブ、影響を受ける資産、スケジュール	一定期間オフラインになった後にオンラインになった資産または通信を再開した資産を検出します。
USB 設定の変更	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 OT Security により検出された IP 競合に適用されます。
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	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を参照してください。ポリシーは、プロ

	ジュール	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、ネットワークで行われた RDP (リモートデスクトップ接続)。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。

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	OT Security では FTP は安全ではないプロトコルと見なされます。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	OT Security では FTP は安全ではないプロトコルと見なされます。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	OT Security では Telnet は安全ではないプロトコルと見なされます。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	OT Security では Telnet は安全ではないプロトコルと見なされます。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	OT Security では Telnet は安全ではないプロトコルと見なされます。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。

注意: 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設定することもできます。 **注意**: 侵入検知システム(IDS)イベントの**ソース**および**デスティネーション**の資産グループを編集することはできません。
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。

注意: 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。
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設定できます。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	ソース資	MMS 経由で ABB 800xA コントローラーに送信され

き込み	産、デスティネーション資産、スケジュール	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 親ユニットまたは子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。たとえば、選択、操作、ウォーム / コールド再起動などです。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。

ポリシーを有効または無効にする

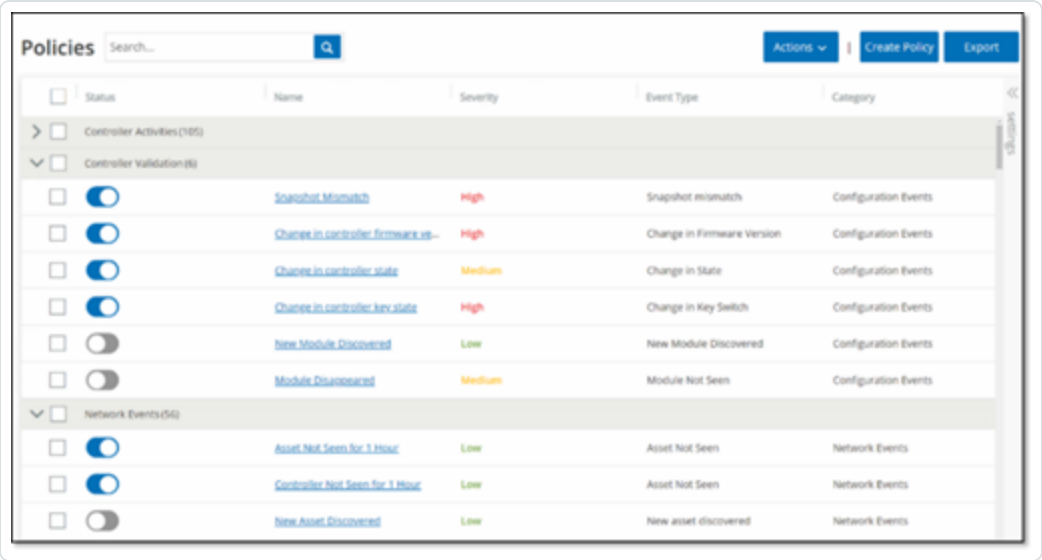
設定されているポリシー(事前設定とユーザー定義の両方)をシステムで有効または無効にできます。個々のポリシーのオンとオフを切り替えたり、複数のポリシーを選択して一括処理でオンとオフを切り替えたりすることができます。

注意: 多くのポリシーは、データを収集するためにクエリを使用します。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。**[アクティブクエリ]** からクエリをアクティブ化できます。アクティブクエリを参照してください。

ポリシーを有効または無効にする

1. **[ポリシー]** に移動します。

   このページには、システムで設定されているすべてのポリシーが、ポリシーカテゴリ別にグループ化されて一覧表示されます。

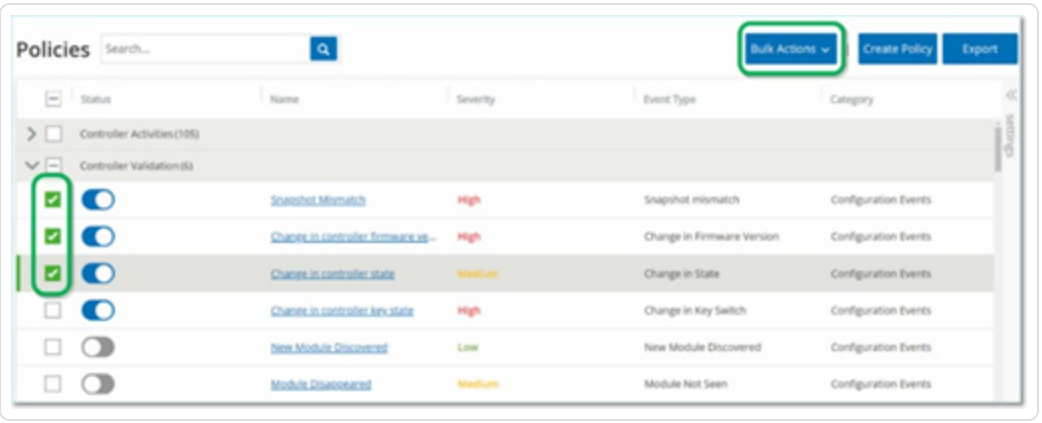


2. ポリシーを有効または無効にするには、該当するポリシーの横にある **[ステータス]** トグルをクリックします。

複数のポリシーのオンとオフの切り替え手順

1. **[ポリシー]** に移動します。

   このページには、システムで設定されているすべてのポリシーが、ポリシーカテゴリ別にグループ化されて一覧表示されます。



2. オンとオフを切り替える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. **[一括アクション]**ドロップダウンボックスから目的のアクション(**[有効化]**または**[無効化]**)を選択します。

   OT Security により、選択したポリシーが有効または無効にされます。

ポリシーの表示

[ポリシー]画面に、システムで設定されているすべてのポリシーが一覧表示されます。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。事前設定ポリシーとユーザー定義のポリシーの両方がこのページに一覧表示されます。各ポリシーには、ポリシーの現在のステータスを示すトグルと、ポリシー設定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。リストのカスタマイズの詳細については、管理コンソールのユーザーインターフェース要素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、トグルの横に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。たとえば、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 などです。
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。

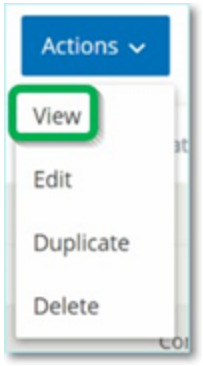
イベントタイプ	このイベントポリシーをトリガーするイベントの特定のタイプ。
カテゴリ	このイベントポリシーをトリガーするイベントタイプの一般カテゴリ。可能な値は、[設定]、[SCADA]、[ネットワーク脅威]、[ネットワークイベント]です。各種カテゴリの詳細については、ポリシーのカテゴリとサブカテゴリを参照してください。
ソース	ポリシー条件。ポリシーが適用されるソース資産グループ / ネットワークセグメント (アクティビティを開始した資産) です。
デスティネーション資産 / 影響を受ける資産	ポリシー条件。ポリシーが適用されるデスティネーション資産グループ / ネットワークセグメント (ア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を記録する Syslog サーバー (SIEM)。
E メール	このポリシーのイベント通知を送信する 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。設定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。さまざまなサブカテゴリの詳細については、ポリシーの表示を参照してください。
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。列をクリックしてリストを並べ替えることができます。これにより、違反 / イベントが最も多いポリシーに集中して取り組むことができます。
除外	各ポリシーに追加された除外の数の一覧表示。詳細は、イベントを参照してください。

ポリシーの詳細の表示

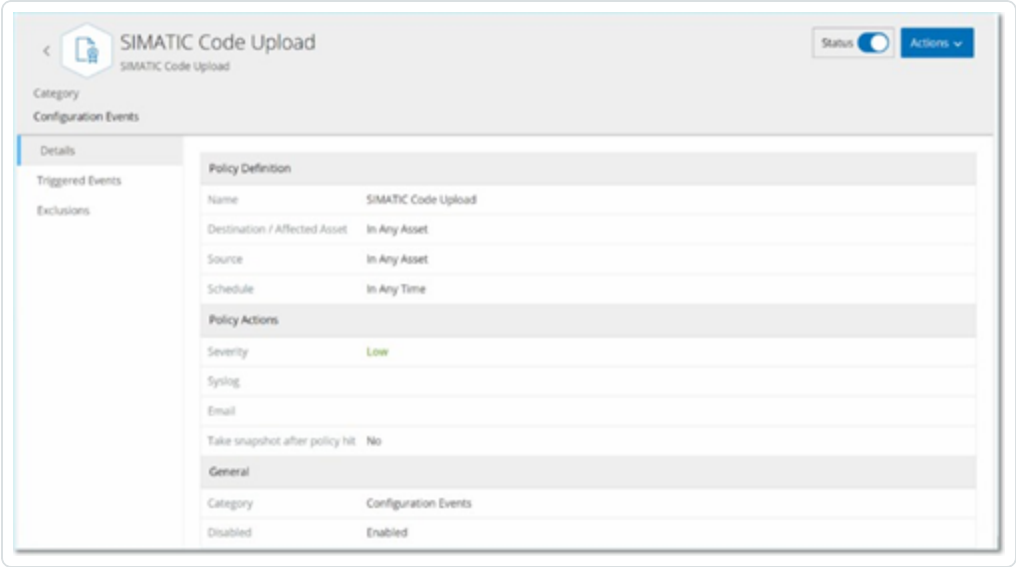
ポリシーの **[ポリシーの詳細]** 画面に、ポリシーに関する追加の詳細が表示されます。このページには、ポリシーによってトリガーされたイベントとポリシー条件がすべて一覧表示されます。

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**ページで、目的のポリシーを選択します。
2. **[アクション]**ドロップダウンボックスから、**[表示]**を選択します。



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。



注意: 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。

ポリシーの詳細ページには、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。このページには、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** – 次のセクションでポリシー設定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、**ポリシーヒット後にスナップショットを取得**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** – 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。また、イベントに関連する資産とイベントの性質に関する詳細も表示されます。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のタブに表示されることを除いて、**イベント**ページ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)。**イベント**ページで除外を追加できます。イベント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と、各除外の固有の除外条件が表示されます。このタブから、除外を削除することもできます (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べきか、通知をどのように配信するかを正確に決定できます。また、各ポリシーにどの程度具体的に、または広範な定義を与えるかについて完全に柔軟な形で決定できます。

> **注意**: ポリシーは、システムで設定されたグループを使用して定義されます。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許可リストに入れるかブロ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許可リストに追加 (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ロックリストに追加 (つまり、ポリシーから除外) します。

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 (すなわち、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。ポリシーの作成のセクションを参照してください。

注意: 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。イベントを参照してください。

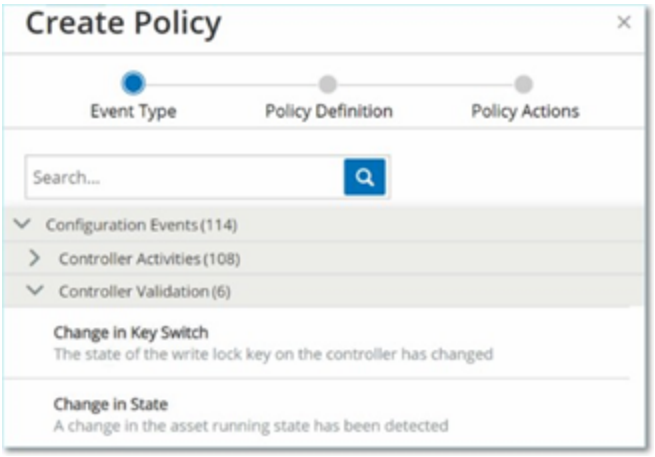
新しいポリシーの作成手順

1. **[プロパティ]** 画面で、**[ポリシーの作成]** をクリックします。

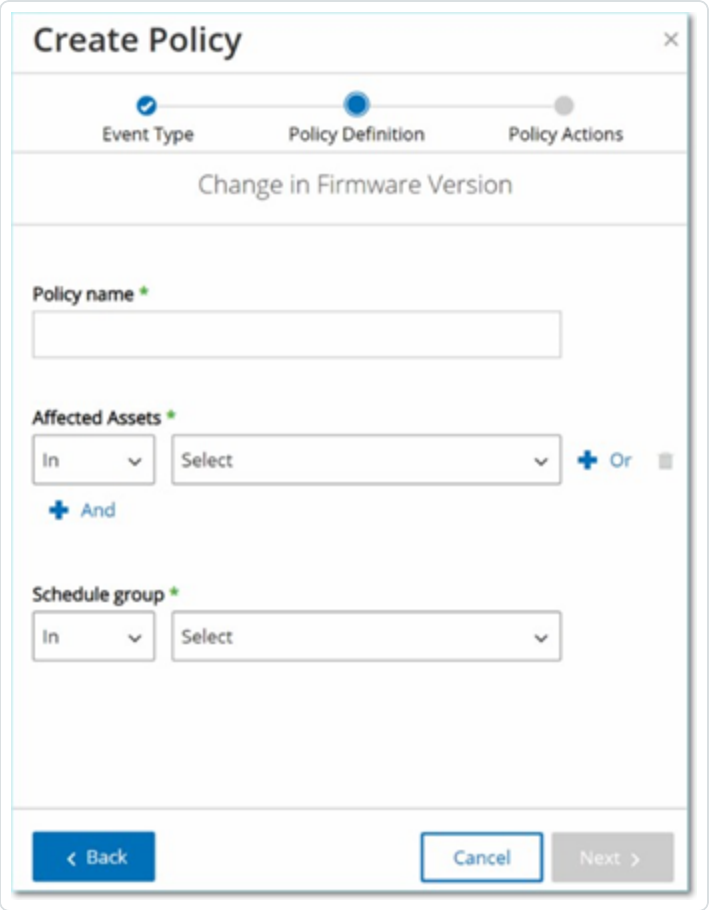
   [ポリシーの作成] ウィザードが開きます。

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。

   > **注意**: 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。

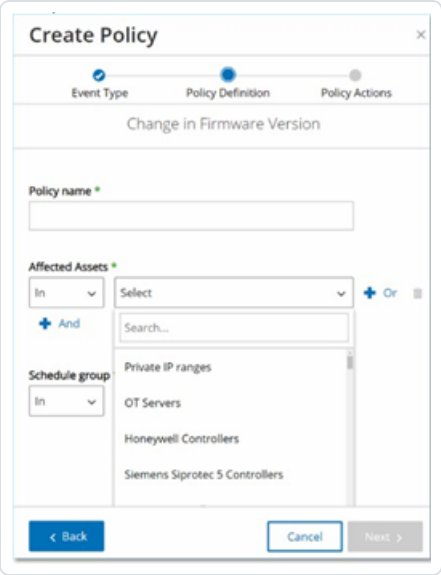
6. 各パラメーターに対して、以下の手順を行います。

   > **重要**: 侵入検知システム (IDS) イベントの **ソース** および **デスティネーション** の資産グループを編集することはできません。

   a. 必要に応じて、選択した要素を許可リストに追加するには **[含める]** (デフォルト) を、選択した要素をブロ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。

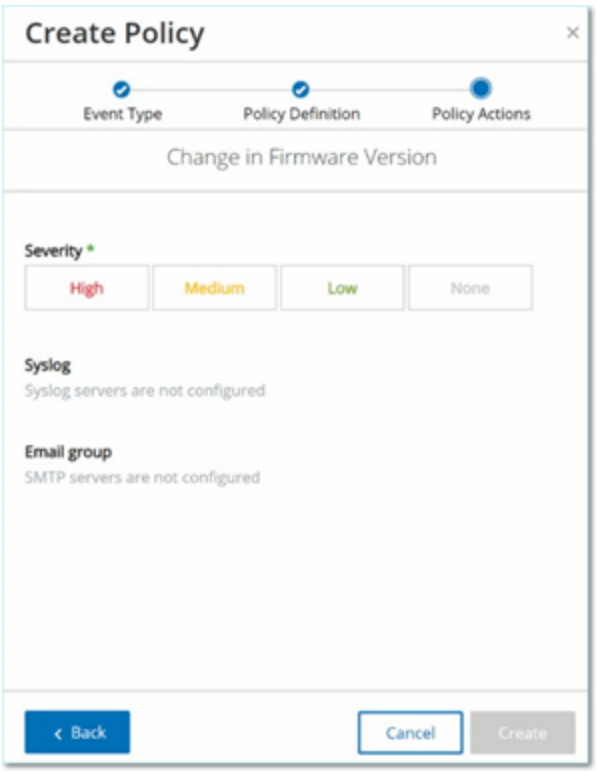
> **注意**: 希望するポリシーの適用に最適なグループ化が存在しない場合は、必要に応じて新しいグループを作成できます。グループを参照してください。

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ます。

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、フィールドの横にある青い**[+ 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ます。

7. **[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。

   注意: 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。

    注意: 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、一部のタイプの設定イベントポリシーに関連しています)。

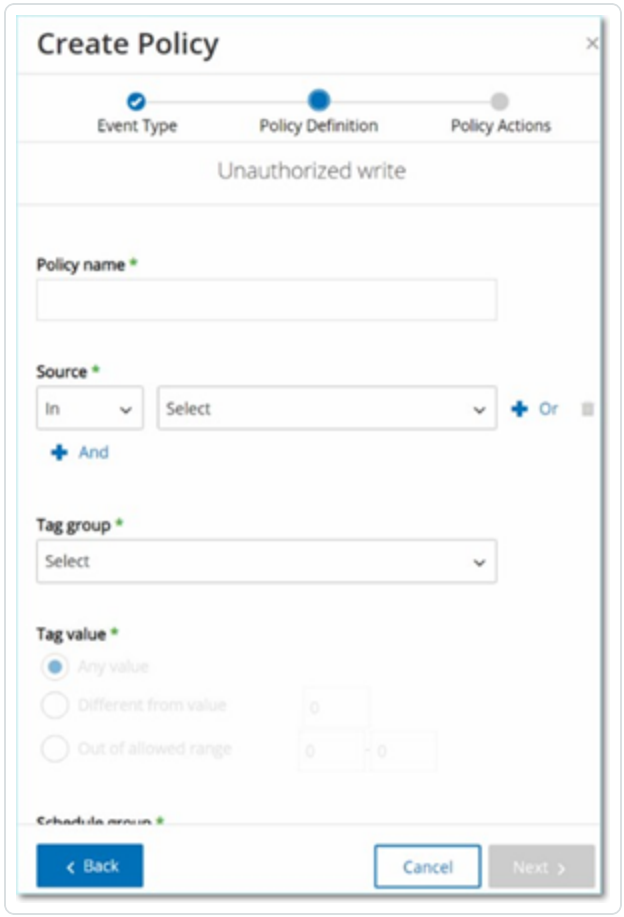
12. **[作成]** をクリックします。新しいポリシーが作成され、自動的にアクティブ化されます。ポリシーが[ポリシー]画面のリストに表示されます。

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。
    - **値と異なる** – 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。

    > **注意**: [値と異なる] 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

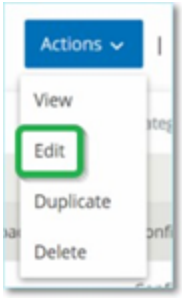
ポリシーの編集

事前定義ポリシーとユーザー定義ポリシーの両方の設定を編集できます。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。

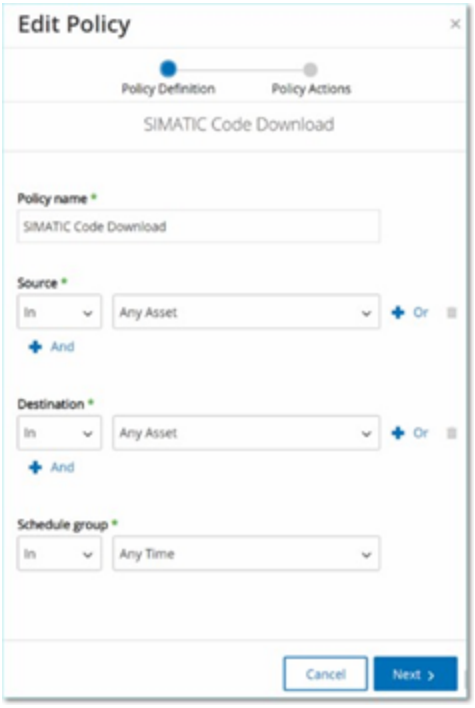
一括アクションで、複数のポリシーの**ポリシーアクション**パラメーターを編集することもできます。

ポリシーの編集手順

1. **[ポリシー]** ウィンドウで、必要な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]** ドロップダウンボックスで、**[編集]** を選択します。



3. **[ポリシーの編集]** ウィンドウに現在の設定が表示されます。



4. 必要に応じて、**ポリシー定義** パラメーターを調整します。

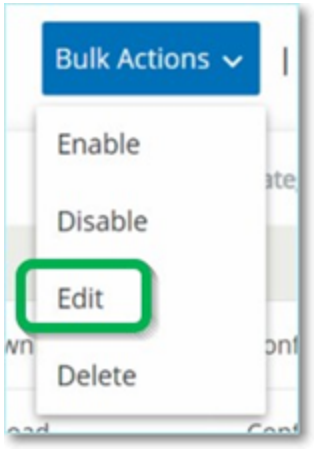
> **注意**: 侵入検知システム (IDS) イベントの **ソース** および **デスティネーション** の資産グループを編集することはできません。

5. **[次へ]** をクリックします。
6. 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。
7. **[保存]** をクリックします。

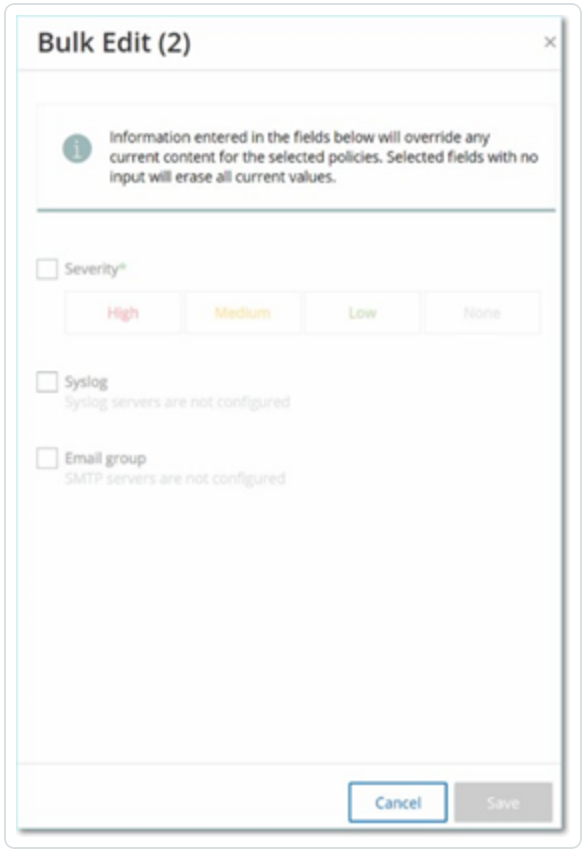
   OT Security に新しい設定でポリシーが保存されます。

複数のポリシーの編集 (一括処理) 手順

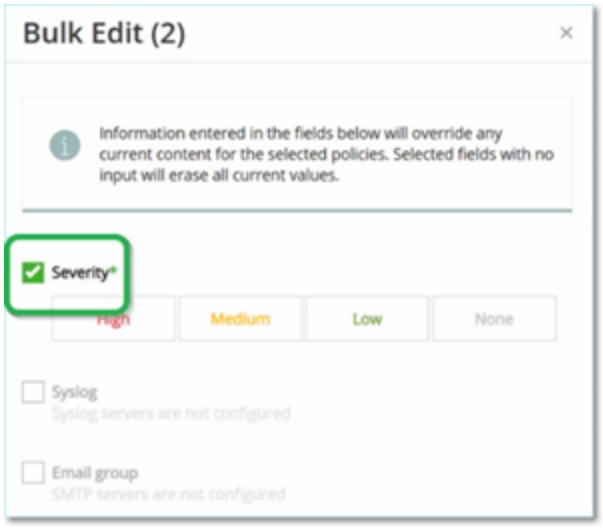
1. **[ポリシー]** ウィンドウで、複数のポリシーの横にあるチェックボックスを選択します。
2. **[一括アクション]** ドロップダウンボックスで、**[編集]** を選択します。



3. **[一括編集]** ウィンドウに、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。



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



5. 各パラメーターを必要に応じて設定します。

   注意: **[一括編集]** ウィンドウに入力された情報は、選択したポリシーの現在の内容を上書きします。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。

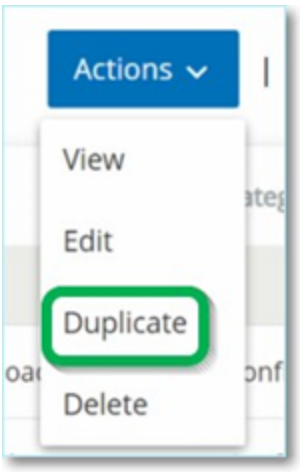
   OT Security に新しい設定でポリシーが保存されます。

ポリシーの複製

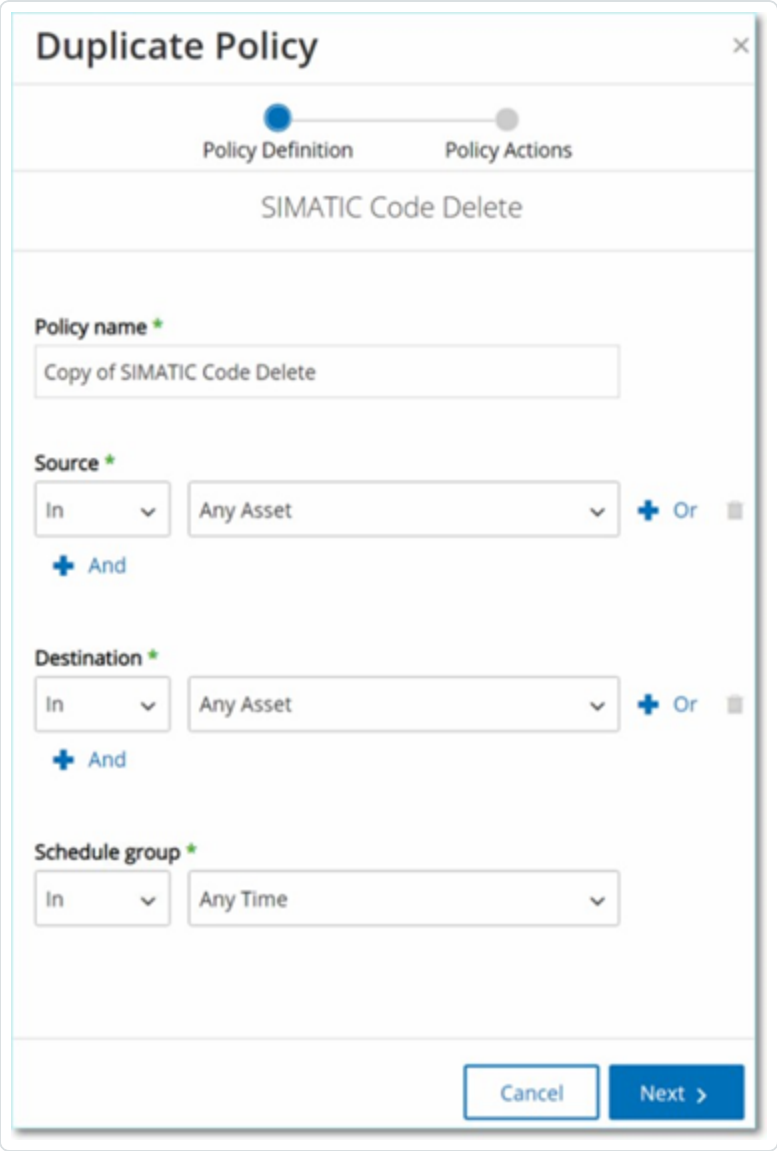
元のポリシーを複製して必要な調整を行うことで、既存のポリシーに類似した新しいポリシーを作成できます。事前定義ポリシーとユーザー定義ポリシーの両方を複製できます (**侵入検知ポリシー**を除く)。

ポリシーの複製手順

1. **[ポリシー]** ウィンドウで、必要な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]** ドロップダウンボックスで、**[複製]** を選択します。



3. **[ポリシーの複製]** ウィンドウに現在の設定が表示され、名前はデフォルトで「*<元のポリシー名> のコピー*」に設定されます。



4. 必要に応じて、**ポリシー定義**パラメーターを調整します。
5. **[次へ]**をクリックします。
6. 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。
7. **[保存]**をクリックします。

   OT Security に新しい設定でポリシーが保存されます。

ポリシーの削除

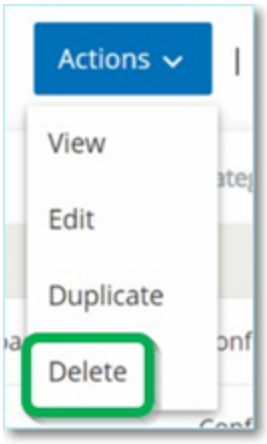
システムからポリシーを削除できます。事前定義ポリシーとユーザー定義ポリシーの両方を削除できます(削除不可能な**侵入検知ポリシー**を除く)。

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。

注意: 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こともできます。

ポリシーを削除する方法

1. **[ポリシー]** ウィンドウで、必要な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]** ドロップダウンボックスで、**[削除]** を選択します。



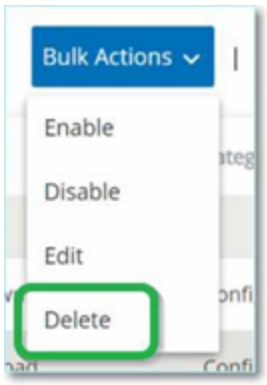
確認ウィンドウが表示されます。

3. **[削除]** をクリックします。

OT Security でシステムからポリシーが削除されます。

複数のポリシーの削除 (一括アクション) 手順

1. **[ポリシー]** ウィンドウで、必要な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]** ドロップダウンボックスで、**[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。

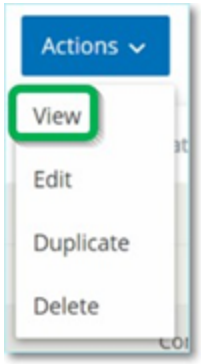
   OT Security でシステムからポリシーが削除されます。

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]** ウィンドウで行うことができます。

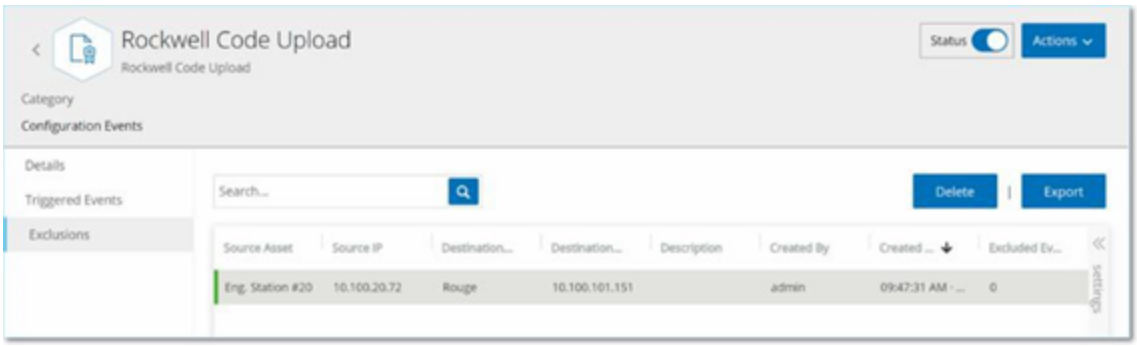
ポリシーの除外の削除手順

1. **[ポリシー]** ウィンドウで、必要なポリシーを選択します。
2. **[アクション]** ドロップダウンボックスで、**[表示]** を選択します。



> **注意**: 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。

   OT Security でシステムから除外が削除されます。

グループ

グループは、ポリシーを構築するための基本的な構成要素です。ポリシーの設定時には、個別のエンティティではなくグループを使用して各ポリシー条件を設定します。OT Security 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。Tenable では、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設定することを推奨しています。

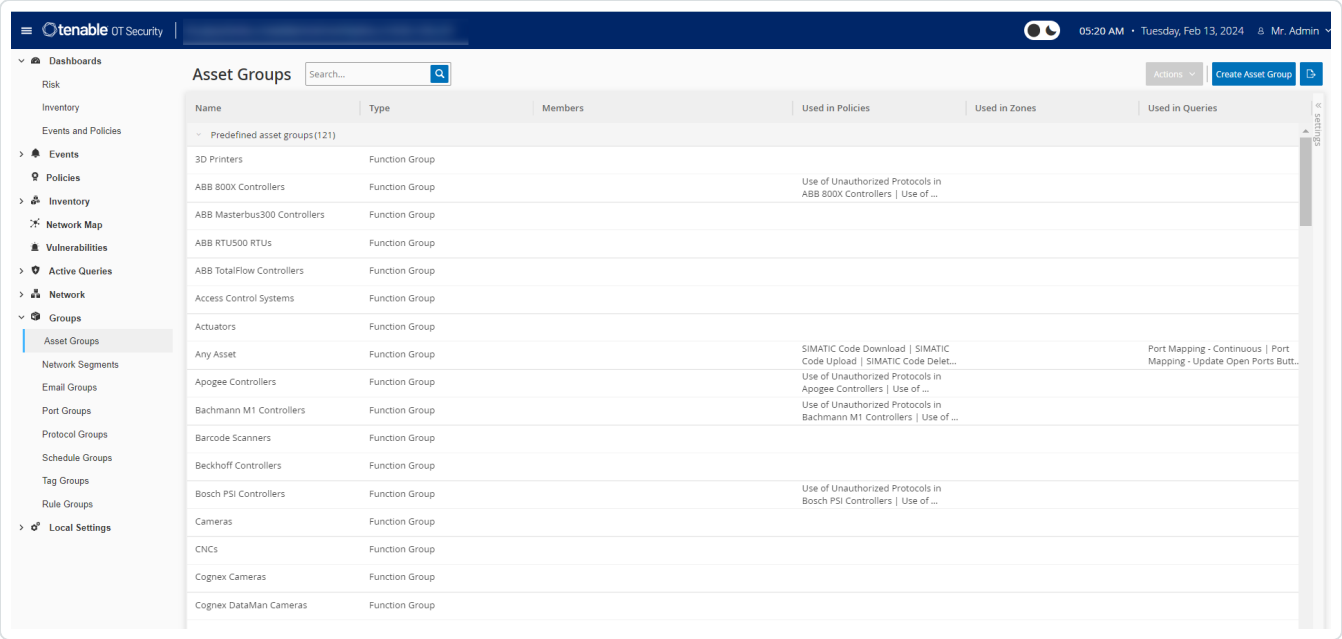
注意: ポリシーパラメーターを設定するときには、グループのみを使用できます。ポリシーを個々のエンティティに適用する場合でも、そのエンティティのみを含むグループを設定する必要があります。

グループの表示

グループを表示するには

1. 左側のナビゲーションバーで **[グループ]** をクリックします。

   [グループ] セクションが展開され、グループタイプが表示されます。



[グループ] で、システムで設定されているすべてのグループを確認できます。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** – 事前設定されているグループで、編集できません。
- **ユーザー定義グループ** – ユーザーが独自に作成および編集できるグループです。

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設定に使用されます。各グループタイプは、[グループ] で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。

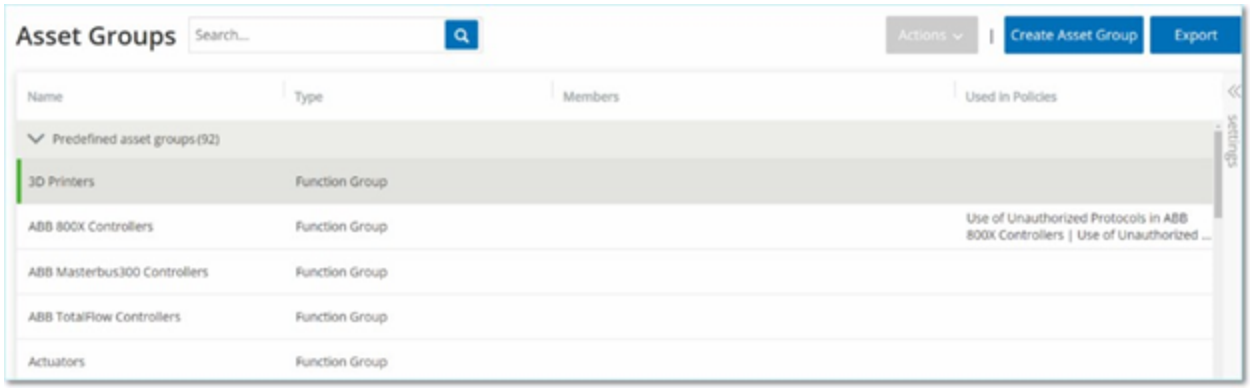
- **プロトコルグループ** – ネットワーク内の資産間で行われる対話に使用されるプロトコルのグループです。**ネットワークイベント**のポリシー条件として使用されます。
- **スケジュールグループ** – スケジュールグループは、指定したイベントが発生する時間がポリシー条件を満たす時間範囲を設定するために使用されます。
- **タググループ** – タグは、特定の操作データを含むコントローラーのパラメーターです。タググループは、SCADA イベントのポリシー条件として使用されます。
- **ルールグループ** – ルールグループは、Suricata Signature ID (SID) 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。**[事前定義資産グループ]** タブには、システムに組み込まれており編集、複製、削除ができないグループが含

まれています。**[ユーザー定義資産グループ]** 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、削除できます。

[資産グループ] テーブルには次の情報が表示されます。

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。詳細については、深刻度レベルの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カテゴリ。可能な値は、[設定]、[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。資産グループは、アクティビティを開始した資産です。
名前	グループを識別する名前。
種類	グループのタイプ。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設定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。
クエリで使用	この資産グループを使用するクエリの名前を表示します。

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

ポリシーの設定時に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。

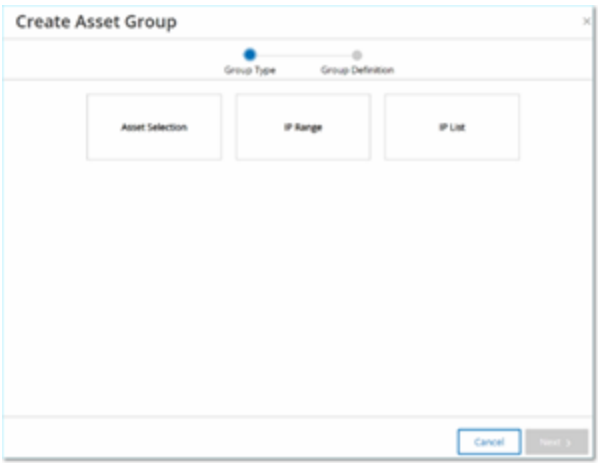
- **資産リスト** – グループに含まれる特定の資産を指定します。
- **IP リスト** – グループに含まれる資産の IP アドレスを指定します。
- **IP 範囲** – グループに含まれる資産の IP アドレスの範囲を指定します。

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

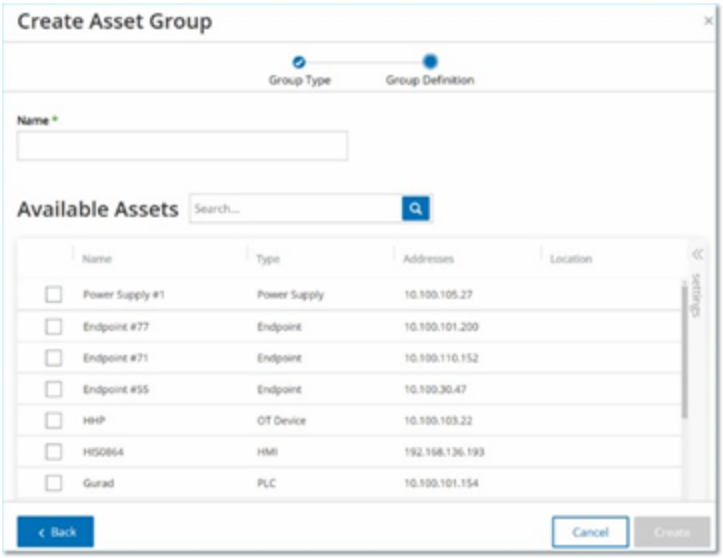
1. **[グループ]** > **[資産グループ]** に移動します。
2. **[資産グループの作成]** をクリックします。

   [資産グループの作成] パネルが表示されます。



3. **[資産選択]** をクリックします。
4. **[次へ]** をクリックします。

   使用可能な資産 のリストが表示されます。



5. **[名前]** ボックスに、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。

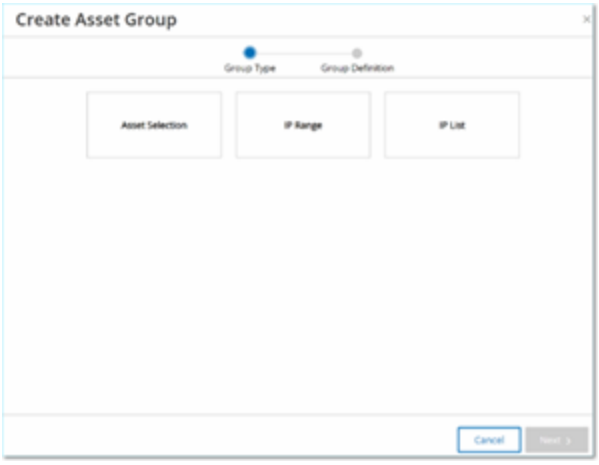
6. グループに含める各資産の横のチェックボックスを選択します。
7. **[作成]** をクリックします。

   OT Security により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、ポリシーを設定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

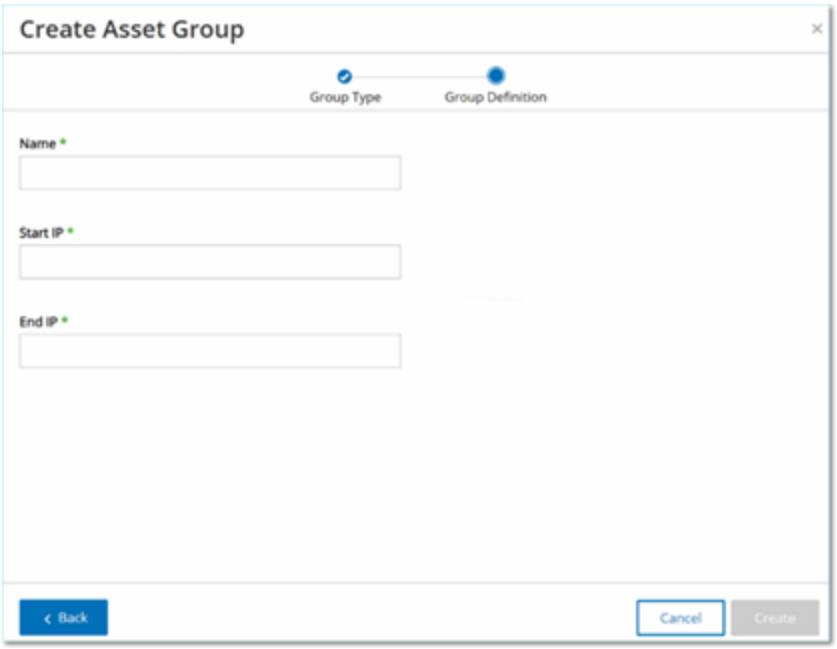
1. **[グループ]** > **[資産グループ]** に移動します。
2. **[資産グループの作成]** をクリックします。

   [資産グループの作成] パネルが表示されます。



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] 選択パネルが表示されます。



5. **[名前]** ボックスに、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]** ボックスに、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]** ボックスに、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。

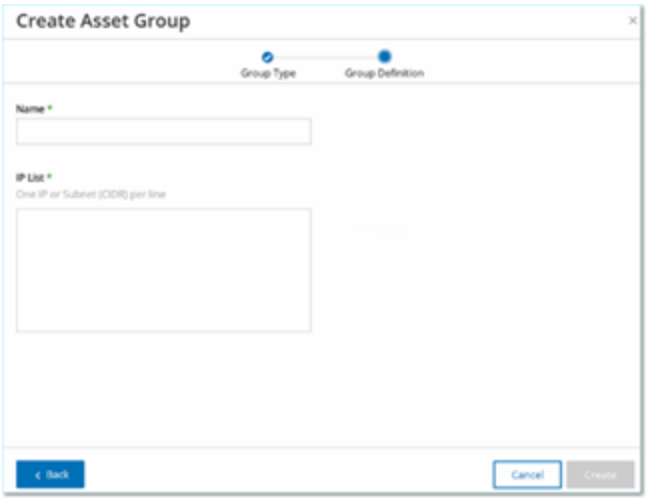
   OT Security により新しい資産グループが作成され、**[資産グループ]** 画面に表示されます。これで、ポリシーを設定するときにこのグループを使用できます。

IP リストタイプの資産グループの作成手順

1. **[グループ]** > **[資産グループ]** に移動します。

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] パネルが表示されます。



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] パネルが表示されます。

5. **[名前]** ボックスに、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。

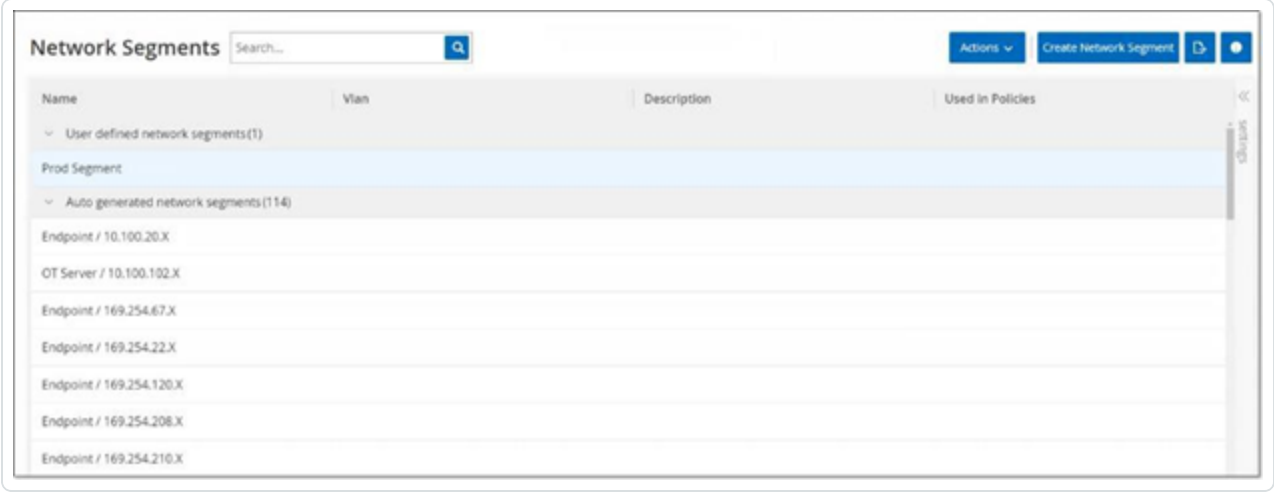
   OT Security により新しい資産グループが作成され、**[資産グループ]** 画面に表示されます。これで、ポリシーを設定するときにこのグループを使用できます。

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を使用すると、関連するネットワーク資産のグループを作成できるため、資産グループを論理的に分離できます。OT Security 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、システムで現在設定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。

[ネットワークセグメント] テーブルには次の詳細が表示されます。

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、**[アクション]** > **[表示]** > **[ポリシーで使用]** タブをクリックします。

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。詳細は、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

ポリシー設定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]** > **[ネットワークセグメント]** に移動します。
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] パネルが表示されます。

3. **[名前]** ボックスに、ネットワークセグメントの名前を入力します。
4. (オプション) **[VLAN]** ボックスに、ネットワークセグメントの VLAN 番号を入力します。
5. (オプション) **[説明]** ボックスに、ネットワークセグメントの説明を入力します。
6. **[作成]** をクリックします。

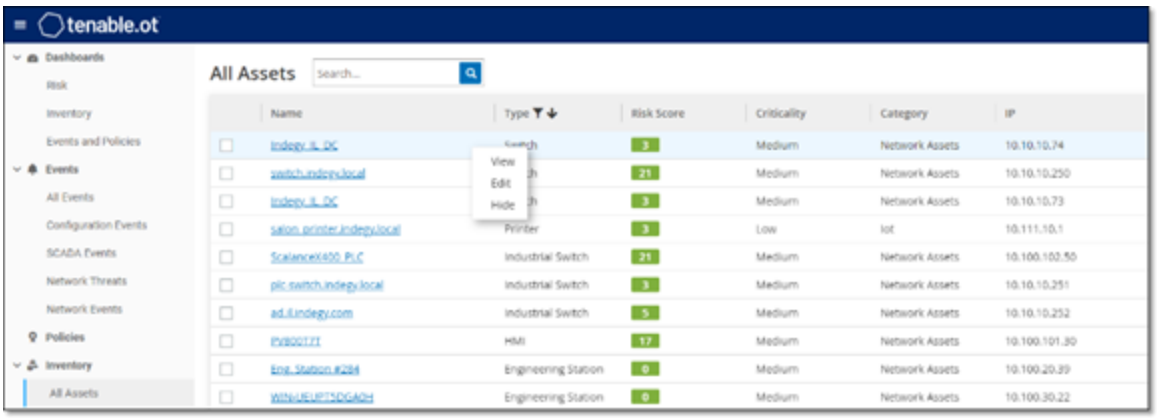
   OT Security により新しいネットワークセグメントが作成され、ネットワークセグメントのリストに表示されます。

7. 新規に作成したネットワークセグメントに資産を割り当てる手順

   a. **[インベントリ]** > **[すべての資産]** に移動します。

   b. 次のいずれかを実行します。

- 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。
- 割り当てる資産にカーソルを合わせ、**[アクション]**メニューから**[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。

8. **[ネットワークセグメント]**ドロップダウンボックスで目的のネットワークセグメントを選択します。

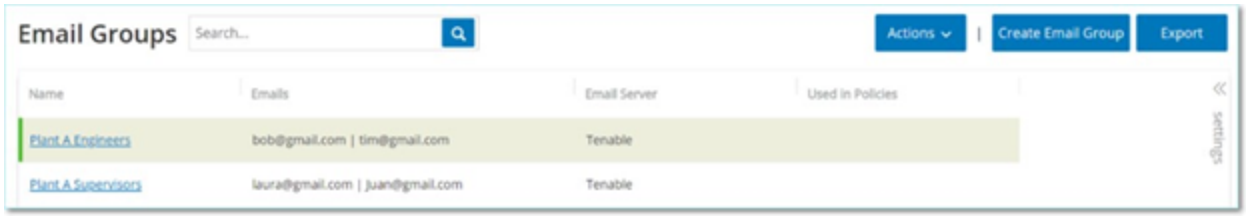
注意: 一部の資産には複数の IP アドレスが関連付けられており、それぞれに必要なネットワークセグメントを選択できます。

OT Security により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、システムで現在設定されているすべての E メールグループが表示されます。

[E メールグループ] テーブルには次の情報が表示されます。

注意: グループを選択し、**[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、**[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	グループに E メールを送信するときに使用される SMTP サーバーの名前です。
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、**[アクション]** > **[表示]** > **[ポリシーで使用]** タブをクリックします。

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。詳細は、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

ポリシー設定で使用する 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。

注意: 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]** > **[E メールグループ]** に移動します。
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] パネルが表示されます。

3. **[名前]** ボックスに、グループの名前を入力します。
4. **[SMTP サーバー]** ドロップダウンボックスで、E メール通知の送信に使用するサーバーを選択します。

   注意: SMTP サーバーがシステムで設定されていない場合は、E メールグループを作成する前に、まずサーバーを設定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]** ボックスで、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。

   OT Security により新しい E メールグループが作成され、**E メールグループ**ページに表示されます。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。

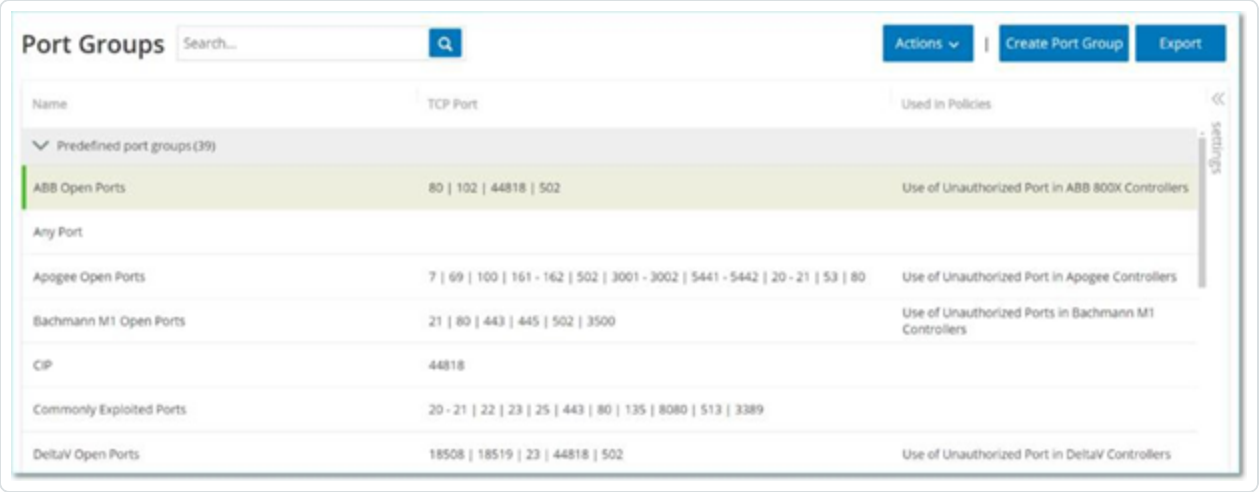
ポートグループ

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ています。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設定が可能になります。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、削除できます。

ポートグループの表示



[ポートグループ]テーブルには、次の詳細が含まれています。

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**: テーブルにグループのすべてのメンバーを表示できない場合は、**[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、**[アクション]** > **[表**

	示] > **[ポリシーで使 用]** タブをクリックします。

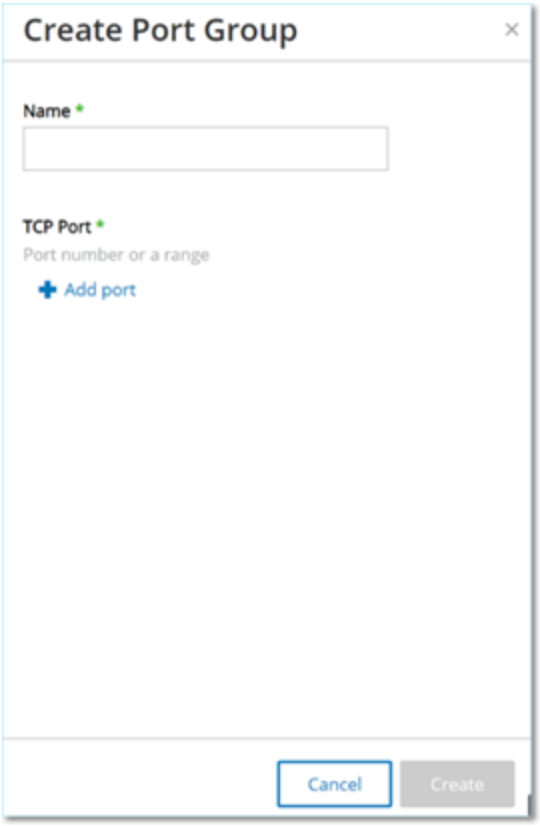
ポートグループの作 成

ポリシーの設 定 で使 用 できるユーザー定 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]** > **[ポートグループ]** に移 動 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] パネルが表 示 されます。



3. **[名 前]** ボックスに、グループの名 前 を入 力 します。
4. **[TCP ポート]** ボックスに、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. ポートをグループに追 加 する手 順

a. **[+ ポートの追加]** をクリックします。

新しい [ポート選択] ボックスが表示されます。

b. **[ポート番号]** ボックスに、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。

OT Security により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、ポリシーを設定するときにこのグループを使用できます。

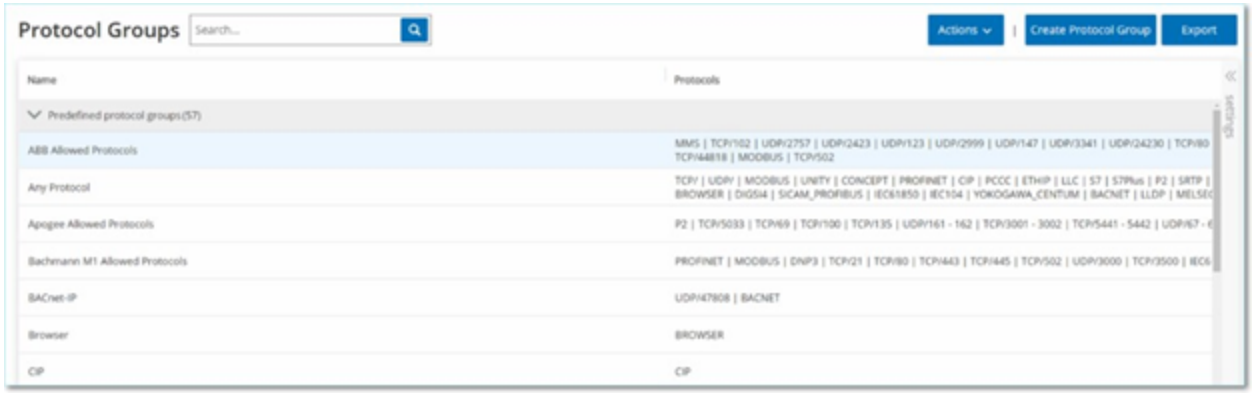
プロトコルグループ

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対話に使用されるプロトコルのセットです。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も定義します。

OT Security 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、これらのグループは編集または削除できません。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

集または削除できませんが、複製は可能です。**[ユーザー定義]**タブには、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、削除できます。

[プロトコルグループ]テーブルには、次の詳細が表示されます。

パラメーター	説明
名前	グループを識別する名前。
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できない場合は、**[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、**[アクション]** > **[表示]** > **[ポリシーで使用]**タブをクリックします。

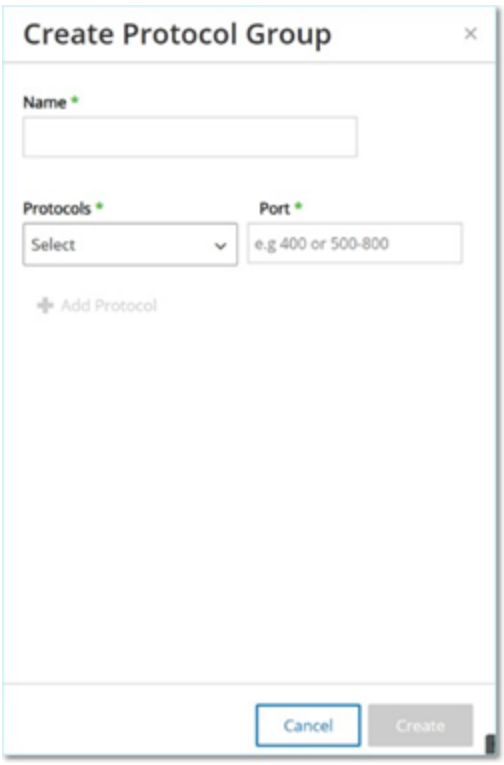
プロトコルグループの作成

ポリシーの設定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]** > **[プロトコルグループ]**に移動します。
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]が表示されます。



3. **[名前]** ボックスに、グループの名前を入力します。
4. **[プロトコル]** ドロップダウンボックスで、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]** ボックス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では、**[ポート]** ボックスに値を入力する必要はありません。
6. プロトコルをグループに追加する手順

   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]** ボックスが表示されます。

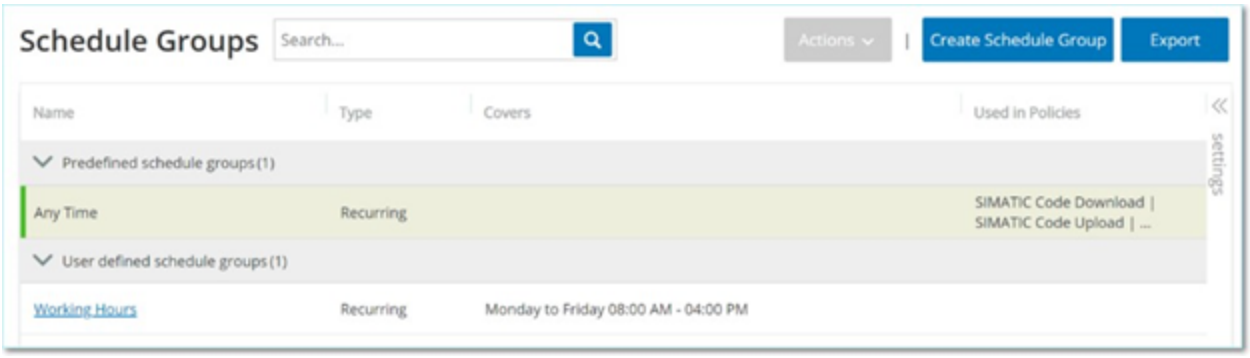
   b. 手順 4 ～ 5 で説明した方法で、新しい**プロトコル選択**を入力します。
7. **[作成]** をクリックします。

   OT Security により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、ポリシーを設定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、システムで現在設定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。**[事前定義スケジュールグループ]** 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、削除できません。**[ユーザー定義スケジュールグループ]** タブには、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、削除できます。

[スケジュールグループ] テーブルには次の詳細が表示されます。

パラメーター	説明
名前	グループを識別する名前。
種類	グループのタイプ。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。 • **定期的** - 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できない場合は、**[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	設定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、**[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

ポリシー設定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期間内に発生するイベントを示すために、共通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。

- **定期的** – 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。

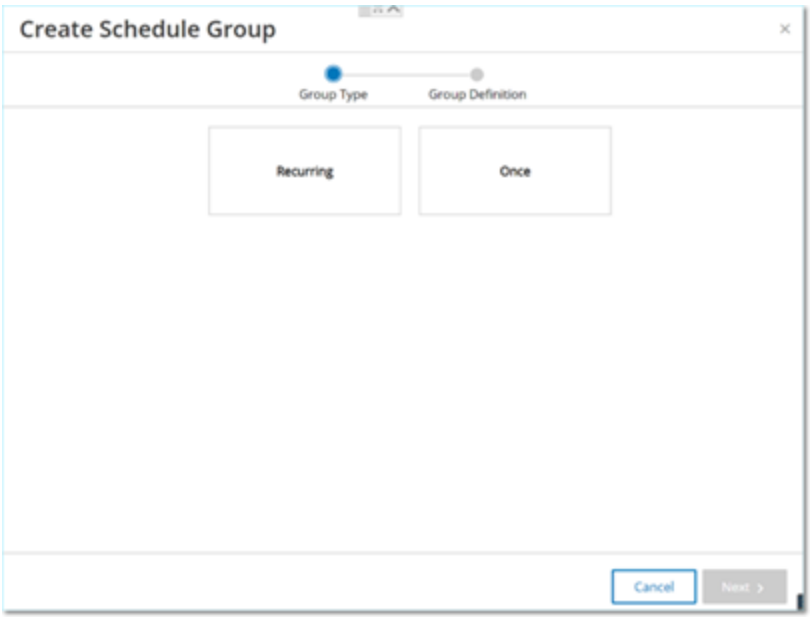
繰り返しタイプのスケジュールグループの作成手順

1. **[グループ]** > **[スケジュールグループ]** に移動します。

   スケジュールグループページが表示されます。

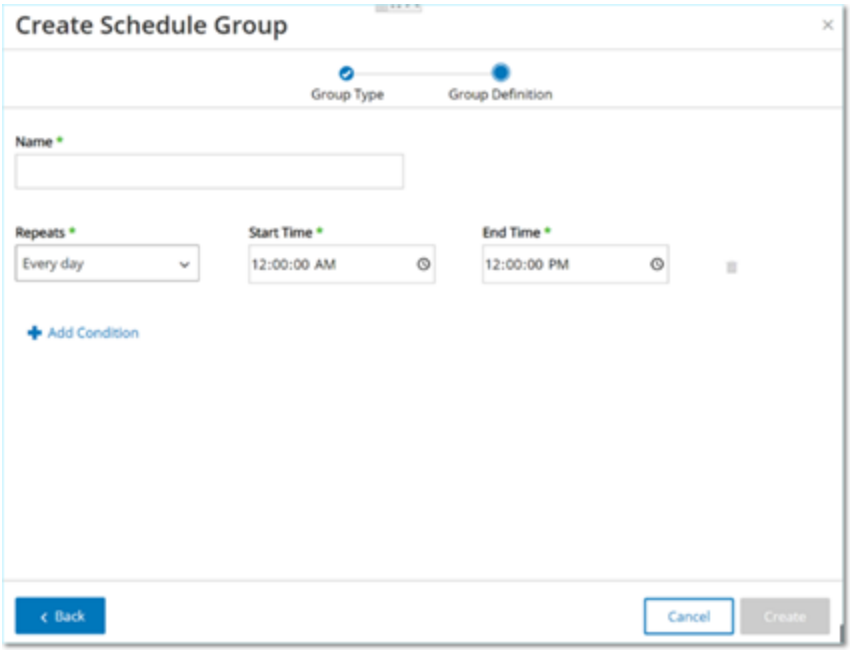
2. **[スケジュールグループの作成]** をクリックします。

   [スケジュールグループの作成] パネルが表示されます。



3. **[定期的]**をクリックします。
4. **[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。



5. **[名前]**ボックスに、グループの名前を入力します。
6. **[繰り返し]**ボックスで、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。

注意: 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。

7. **[開始時刻]** ボックスに、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。
8. **[終了時刻]** ボックスに、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。
9. スケジュールグループに条件 (追加の時間範囲) を追加する手順
    a. **[+ 条件の追加]** をクリックします。

        スケジュール選択パラメーター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。
10. **[作成]** をクリックします。

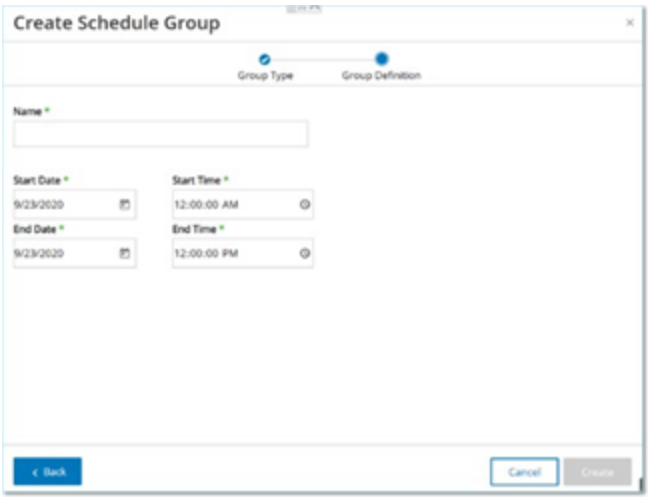
    OT Security により新しいスケジュールグループが作成され、スケジュールグループのリストに表示されます。これで、ポリシーを設定するときにこのグループを使用できます。

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]** > **[スケジュールグループ]** に移動します。
2. **[スケジュールグループの作成]** をクリックします。

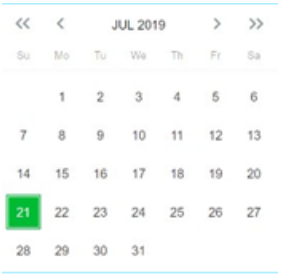
    [スケジュールグループの作成] ウィザードが表示されます。
3. **[時間範囲]** を選択します。
4. **[次へ]** をクリックします。

    時間範囲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]** ボックスに、グループの名前を入力します。
6. **[開始日]** ボックスで、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。デフォルトは現在の日付です。
8. **[開始時刻]** ボックスに、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]** ボックスで、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]** ボックスに、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。

OT Security により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、ポリシーを設定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、システムで現在設定されているすべてのタググループが表示されます。

[タググループ] テーブルには次の詳細が表示されます。

パラメーター	説明
名前	グループを識別する名前。
種類	タグのデータタイプ。可能な値には Bool、Dint、Float、Int、Long、Short、Unknown (OT Security 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できない場合は、**[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	設定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、**[アクション]** > **[表示]** > **[ポリシーで使用]** タブをクリックします。

既存のグループを表示、編集、複製、削除できます。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、削除できます。

新しいタググループの作成手順

1. **[グループ]** > **[タググループ]** に移動します。
2. **[タググループの作成]** をクリックします。

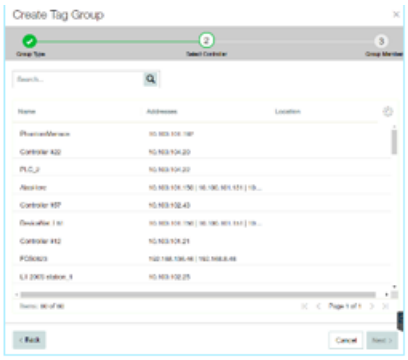
   [タググループの作成] パネルが表示されます。

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。

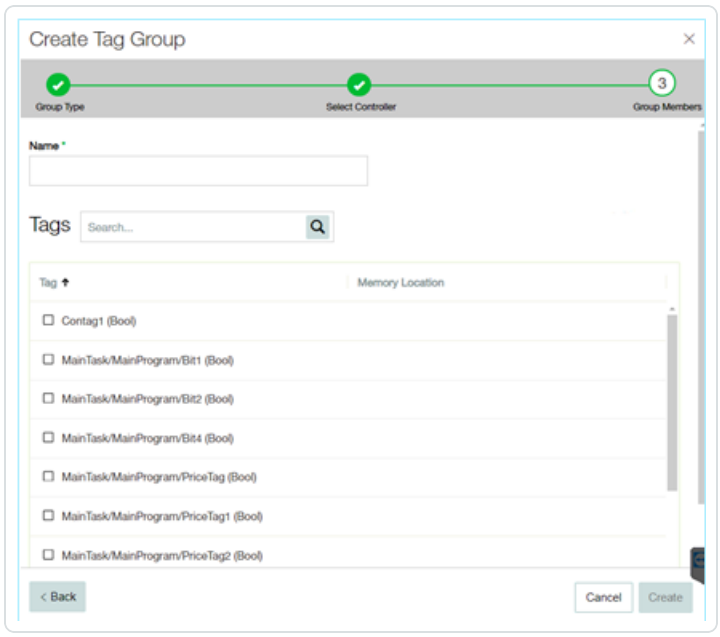
4. **[次へ]** をクリックします。

   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]** ボックスに、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。

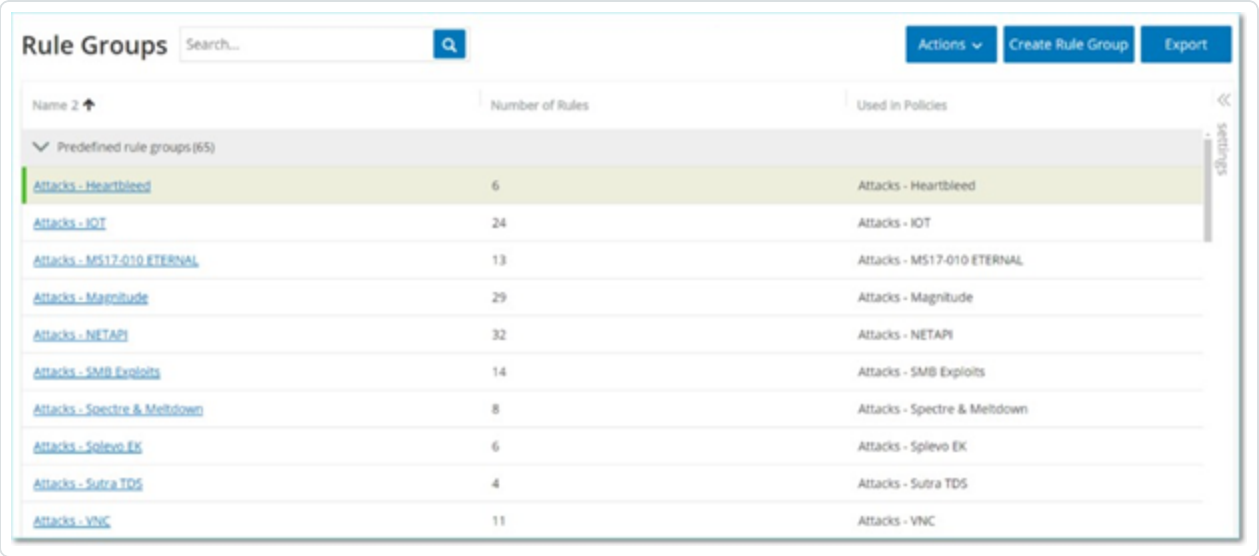
OT Security により新しいタググループが作成され、タググループのリストに表示されます。これで、SCADA イベントポリシーを構成するときにこのグループを使用できます。

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。

OT Security 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、システムで現在設定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、削除できます。

[ルールグループ] テーブルには次の詳細が表示されます。

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。

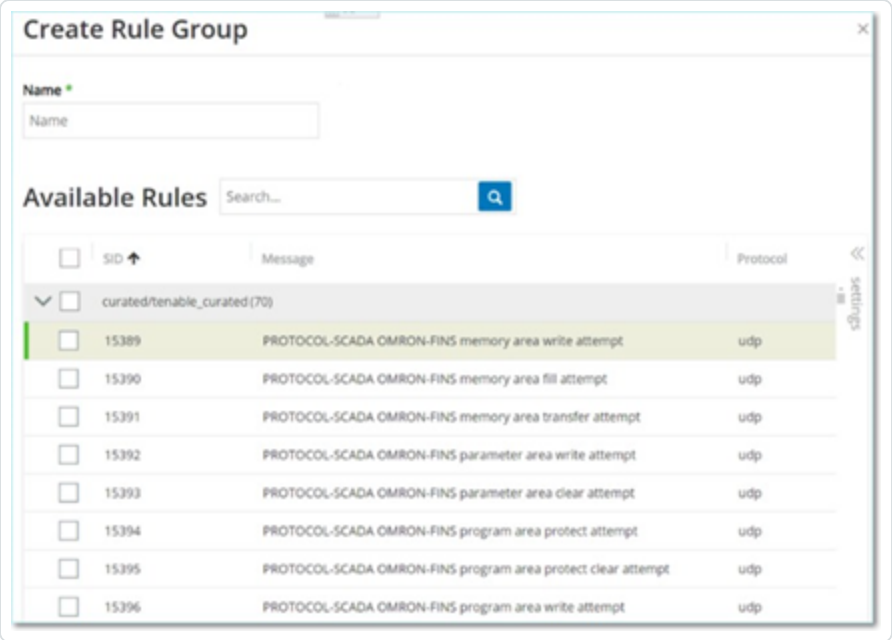
ルールの数	このルールグループを構成するルール(SID)の数。
ポリシーで使用	構成でこのルールグループを使用する各ポリシーのポリシーIDを表示します。 **注意**: このグループが使用されているポリシーの追加情報を表示するには、**[アクション]** > **[表示]** > **[ポリシーで使用]** タブをクリックします。

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]** > **[ルールグループ]** に移動します。
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] パネルが表示されます。



3. **[名前]** ボックスに、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。

   注意: 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。

OT Security により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

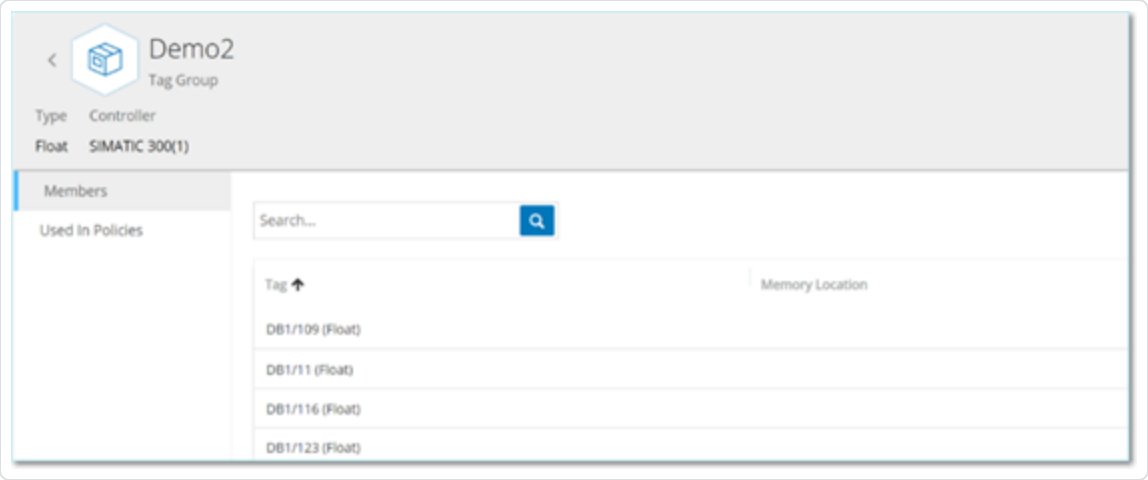
グループ画面のいずれかでグループを選択すると、画面上部の **[アクション]** メニューで次のアクションを実行できます。

- **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。グループの詳細の表示を参照してください。
- **編集** – グループの詳細を編集します。グループを編集するを参照してください。
- **複製** – 指定されたグループと同様の設定で新しいグループを作成します。グループの複製を参照してください。
- **削除** – システムからグループを削除します。グループを削除するを参照してください。

> **注意**: 事前定義グループを編集または削除することはできません。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。

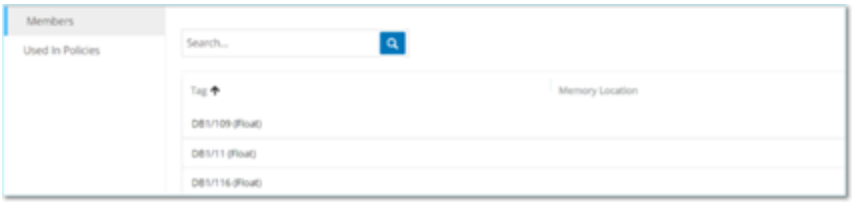
グループの詳細の表示

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。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。

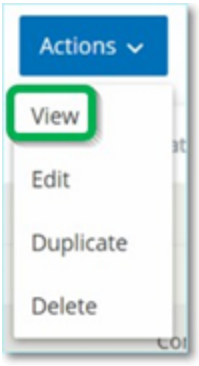


- **ポリシーで使用** – 指定されたグループがポリシー条件として使用されている各ポリシーのリストを表示します。ポリシーのリストには、ポリシーのオン / オフを切り替えるトグルスイッチが含まれています。詳細は、ポリシーの表示を参照してください。

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. 次のいずれかを実行します。
   - **[アクション]** をクリックします。
   - 目的のグループを右クリックします。

     メニューが表示されます。
3. **[表示]** を選択します。



[グループの詳細] 画面が表示されます。

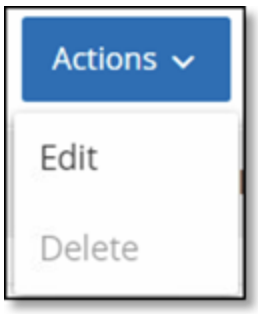
グループを編集する

既存のグループの詳細を編集できます。

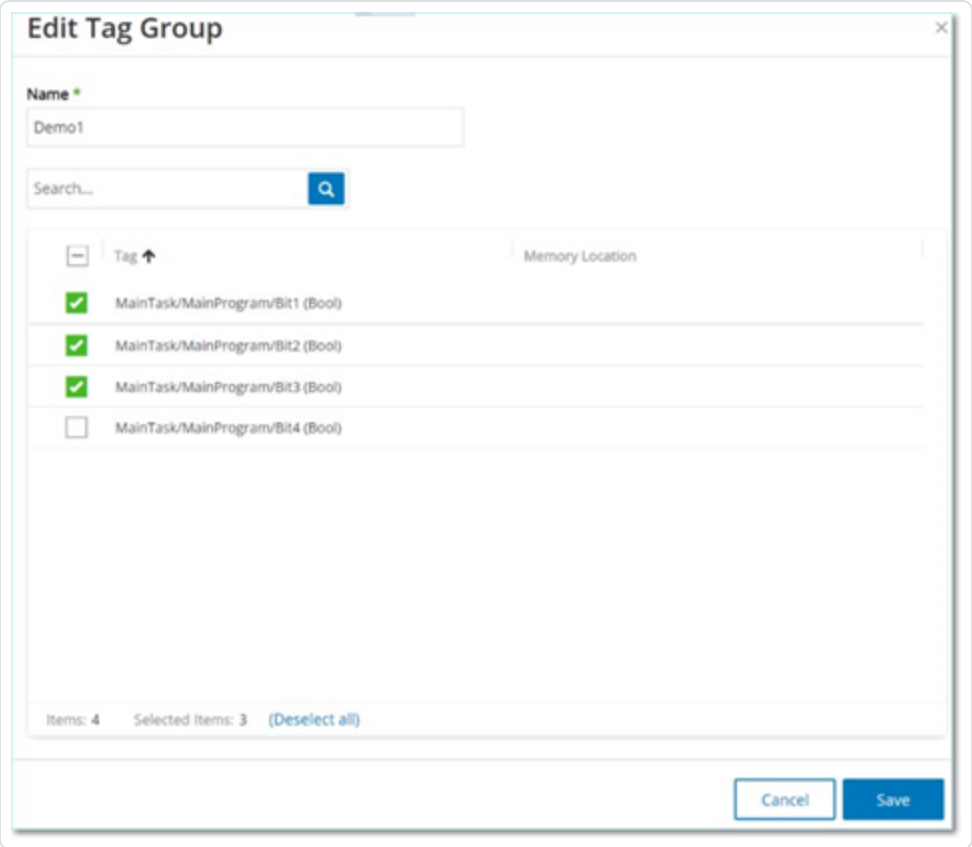
グループの詳細の編集手順

1. **[グループ]** で、目的のグループのタイプを選択します。
2. 次のいずれかを実行します。
   - **[アクション]** をクリックします。
   - 目的のグループを右クリックします。

     メニューが表示されます。
3. **[編集]** を選択します。



4. **[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。



5. 必要に応じて変更します。
6. **[保存]** をクリックします。

   OT Security によりグループが新しい設定で保存されます。

グループの複製

既存のグループと類似する設定を使用して新しいグループを作成するには、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。

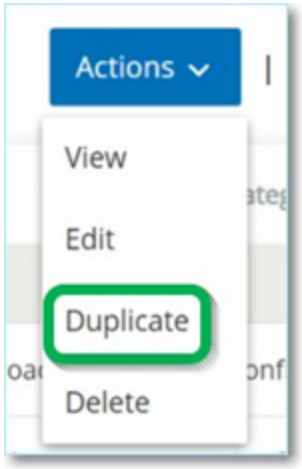
グループの複製手順

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. 次のいずれかを実行します。

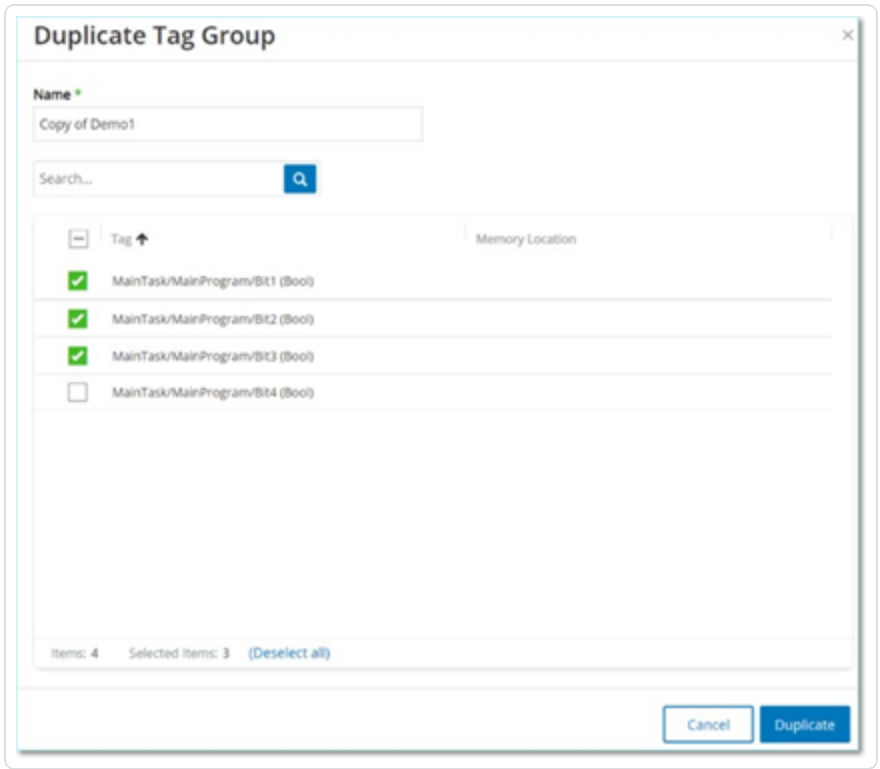
- **[アクション]** をクリックします。
- 目 的 のグループを右 クリックします。

  メニューが表 示されます。

4. **[複 製]** を選 択します。



[Duplicate Group (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。



5. **[名前]** ボックスに、新規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「コピー - (元のグループ名)」という形式の名前になります。
6. グループ設定に必要な変更を加えます。
7. **[複製]** をクリックします。

   OT Security により、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。

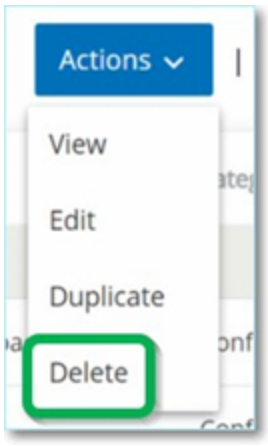
グループを削除する

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、ユーザー定義ポリシーが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、そのポリシーは削除できません。

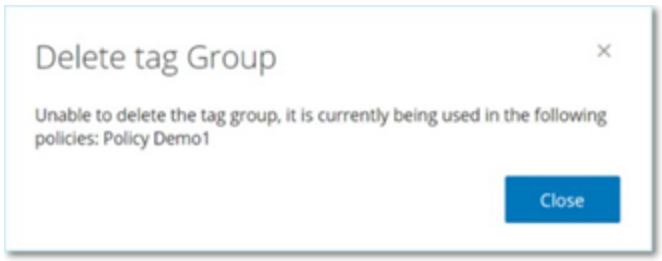
グループの削除手順

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. 次のいずれかを実行します。
   - **[アクション]** をクリックします。
   - 目的のグループを右クリックします。

     メニューが表示されます。
4. [**Delete**] を選択します。



   確認ウィンドウが表示されます。



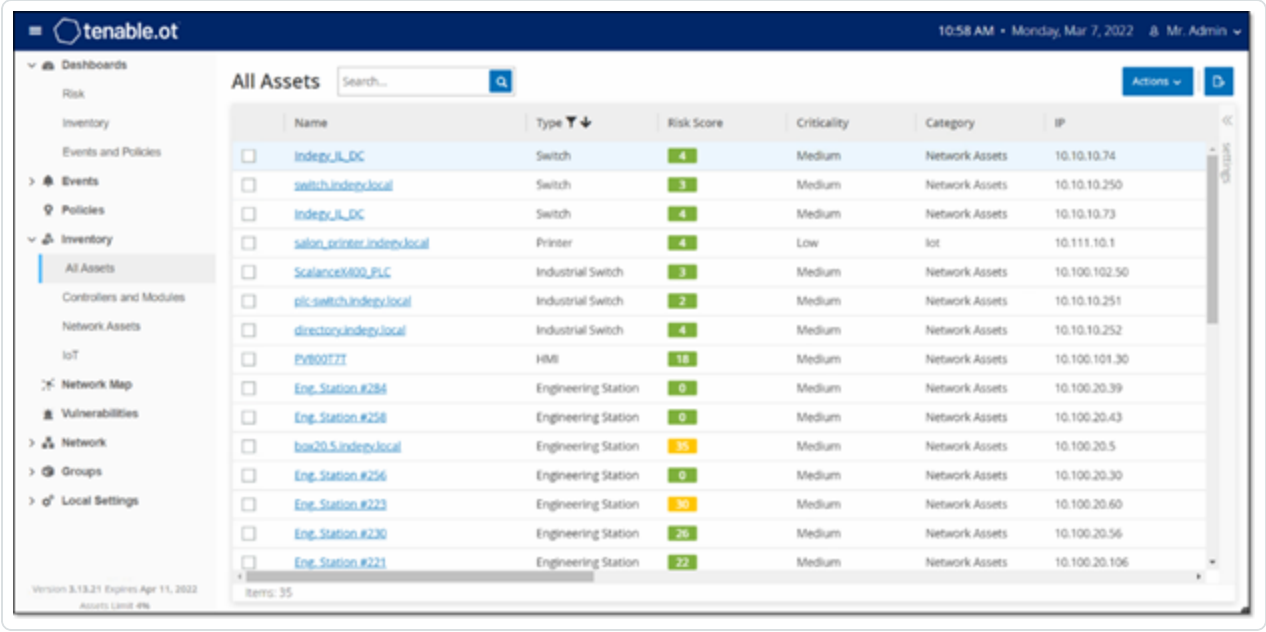
5. **[削除]**をクリックします。

   OT Security により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

OT Security 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、パッチデプロイメント、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]**ページに表示されます。[インベントリ]ページには、資産に関する詳細が含まれるため、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

のステータスもモニタリングできます。OT Security は、ネットワーク検出機能とアクティブクエリ機能を使用してこのデータを収集します。**[すべて]** ページには、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、**[コントローラーとモジュール]**、**[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。

> **注意**: [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。

各資産ページ (**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**) で、表示される列と各列の位置を調整して、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。表のカスタマイズ方法については、管理コンソールのユーザーインターフェース要素を参照してください。

次の表では、**[インベントリ]** ページの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]** ページ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 [資産詳細] 画面を表示します (インベントリ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、管理コンソールのユーザーインターフェース要素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。
種類	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	OT Security の資産詳細でユーザーが入力した資産の場所。インベントリを参照してください。
最終確認日	デバイスが OT Security 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。
説明	OT Security の資産詳細でユーザーが設定した、資産の簡単な説明。インベントリ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、OT Security 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、OT Security 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
				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、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
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、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。		OT サーバー
				ヒストリアン

				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	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。		サーバー
				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
		プリンタ
		UPS
		IP 電話
		スマートセンサー
		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

資産詳細ページには、選択した資産について OT Security が検出し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。

特定の資産の**資産詳細**ページへのアクセス手順

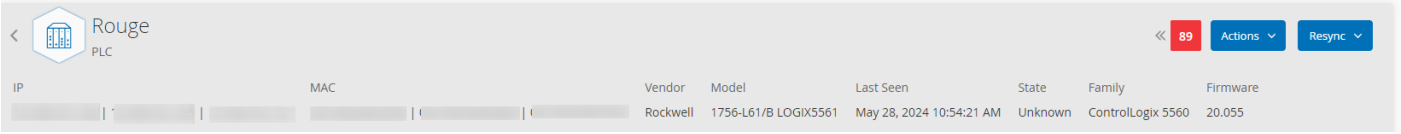
1. 次のいずれかを実行します。
    - 資産名がリンクとして表示されているいずれかのページ (**[インベントリ]**、**[イベント]**、または**[ネットワーク]**) で資産名をクリックします。
    - **インベントリ**ページで、**[アクション]** > **[表示]** をクリックします。

関連する資産タイプの**[資産詳細]**ウィンドウには、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) – OT Security 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、脆弱なプロトコルの使用、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オープンな通信ポートなど、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です。
- **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。

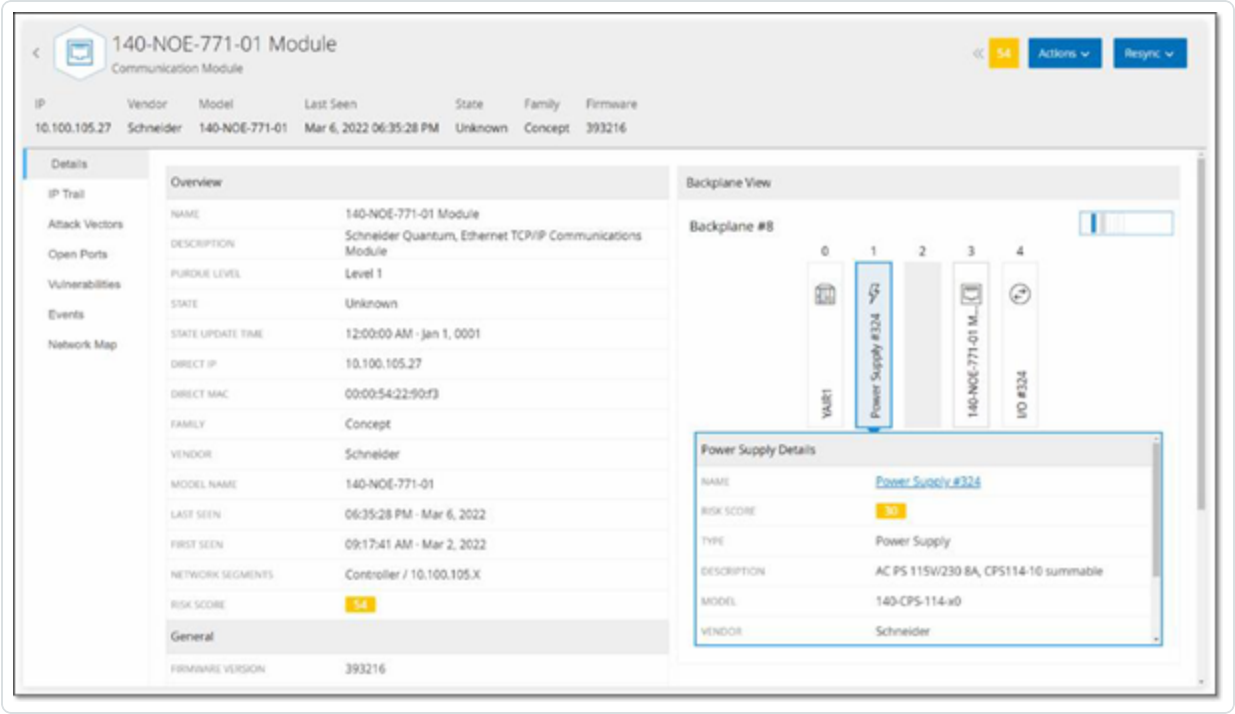


この表示には、次の要素が含まれます。

- **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、Tenable 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。ヘッダーペイン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、OT Security 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。

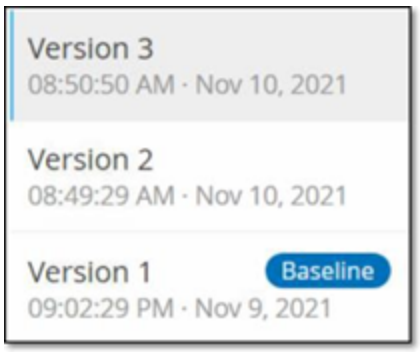
スナップショットは次の方法でトリガーできます。

- **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」ポリシーを設定して、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。設定イベント – 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。

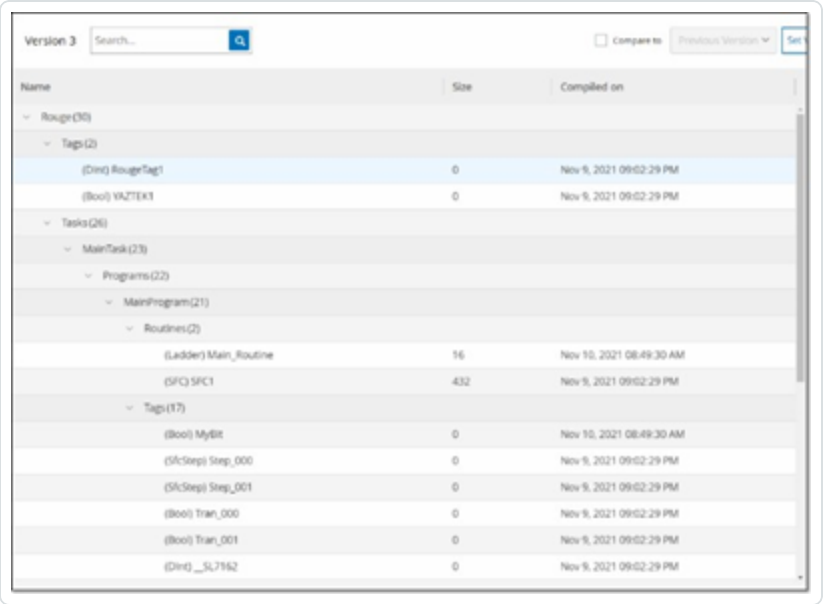
続くセクションでは、コードリビジョン表示のさまざまなセクションと、異なる「スナップショット」バージョンを比較する方法について説明します。

バージョンの選択ペイン



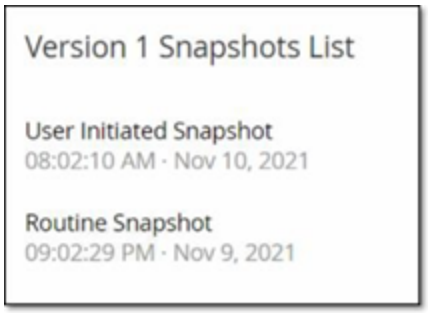
このペインには、このコントローラーのコードリビジョンの利用可能なすべてのバージョンのリストが表示されます。バージョンごとに、そのバージョンの稼働が開始したと認識されている開始時刻が表示されます。以前の「スナップショット」からの変更が検出されるたびに、新しいバージョンが作成されます。「ベースライン」タグは、比較の目的でベースラインバージョンとして現在設定されているバージョンを示します。バージョンを選択して、[スナップショットの詳細] ペインにコードリビジョンを表示します。

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。

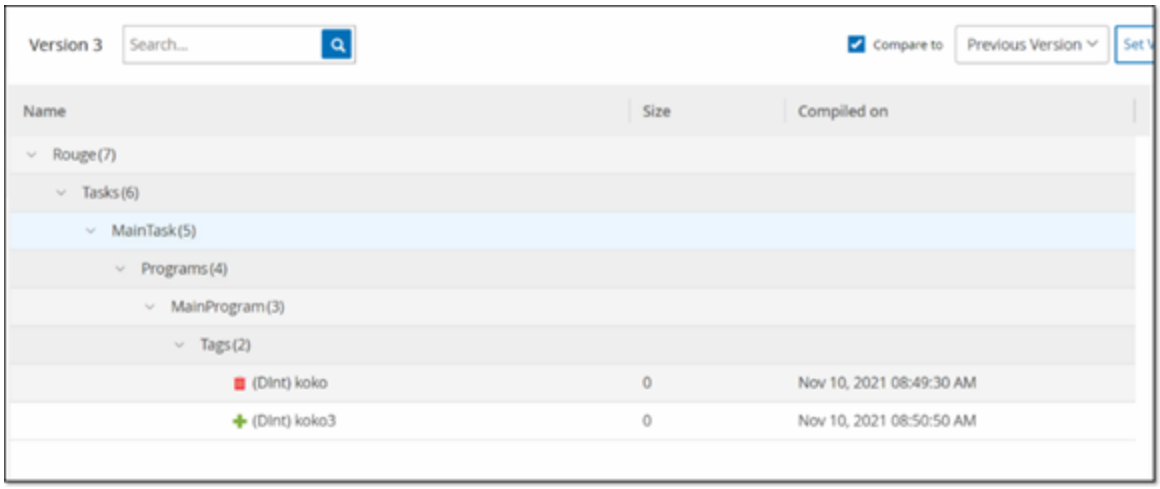
削除済み - 選択したバージョンで削除されたコード。

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。

   > **注意**: 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。[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。
7. [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。

攻撃手法

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。
- 通信経路の過程を調査し、プロセスへの関連を検証する。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** – OT Security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、OT Securityは、ターゲット資産へのアクセスに利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

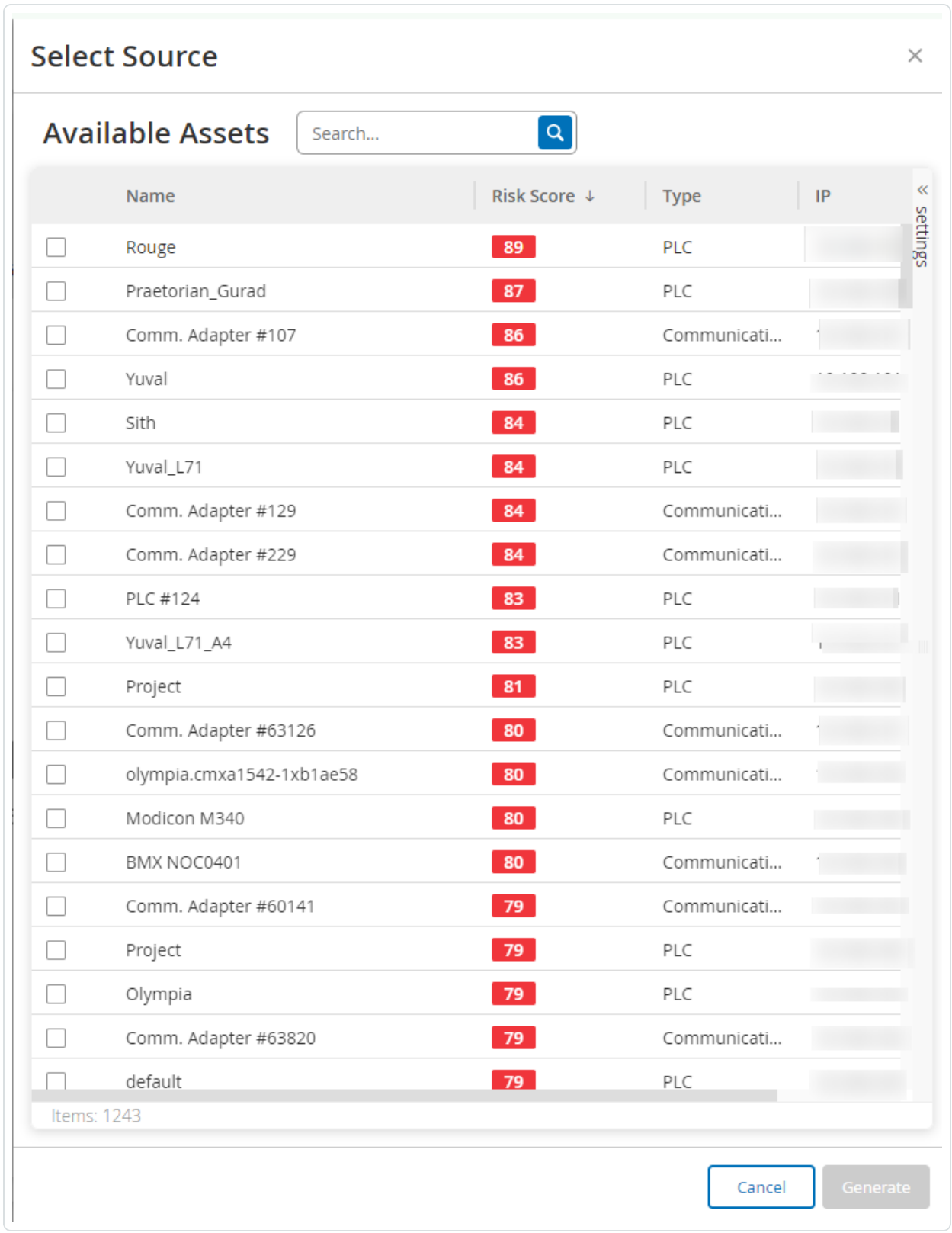
1. 目的のターゲット資産の**資産詳細**ページに移動し、**[攻撃経路]**タブをクリックします。
2. **[生成]**をクリックし、ドロップダウンリストから**[ソースを自動的に選択]**をクリックします。

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。


Select Source
Available Assets
Search...
Name
Risk Score
Type
IP
settings
Rouge 89 PLC
Praetorian_Gurad 87 PLC
Comm. Adapter #107 86 Communicati...
Yuval 86 PLC
Sith 84 PLC
Yuval_L71 84 PLC
Comm. Adapter #129 84 Communicati...
Comm. Adapter #229 84 Communicati...
PLC #124 83 PLC
Yuval_L71_A4 83 PLC
Project 81 PLC
Comm. Adapter #63126 80 Communicati...
olympia.cmxa1542-1xb1ae58 80 Communicati...
Modicon M340 80 PLC
BMX NOC0401 80 Communicati...
Comm. Adapter #60141 79 Communicati...
Project 79 PLC
Olympia 79 PLC
Comm. Adapter #63820 79 Communicati...
default 79 PLC
Items: 1243
Cancel
Generate

注意: 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。

注意: [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。

開いているポート

[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、対話、Tenable Nessus Network Monitor または Tenable 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。[オープンポートの期限切れ期間] の長さを調整するには、デバイスを参照してください。

オープンポートスキャンのパラメーターは、[アクティブクエリ] で設定します。選択した資産に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 / ネットワーク資産]** 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 / ネットワーク資産]** 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。

   OT Security 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

> **注意**: 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。

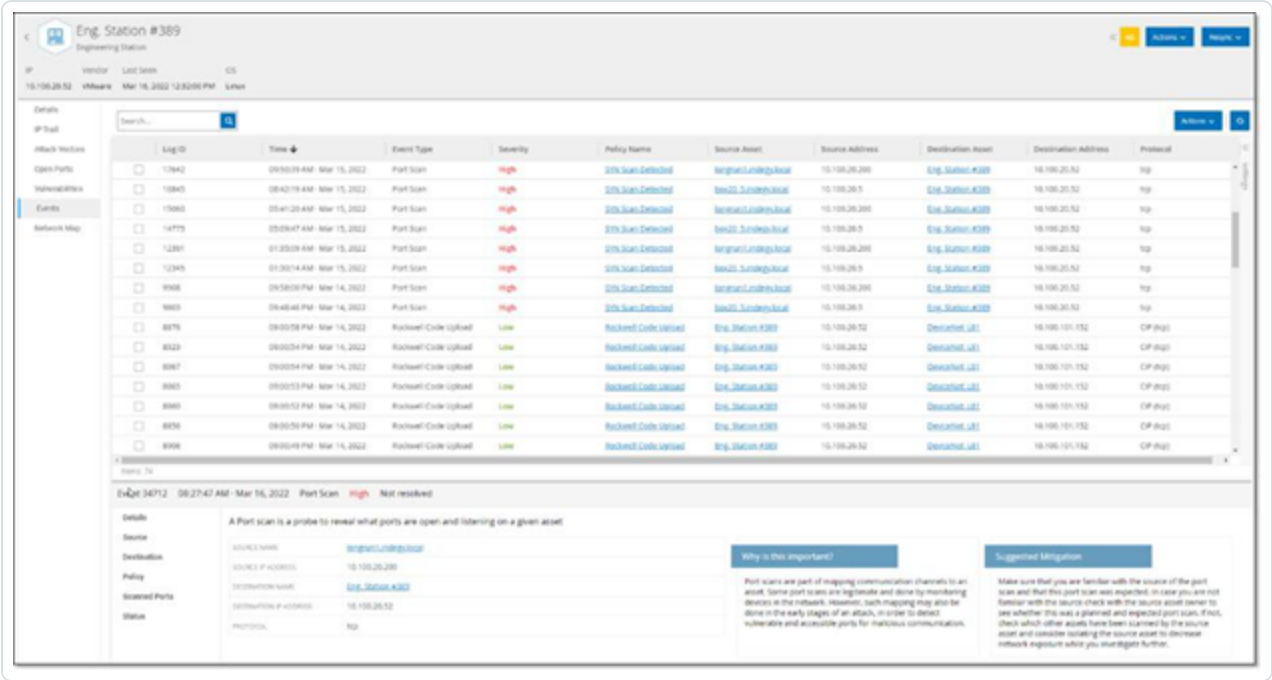
   [資産詳細] 画面が表示されます。
2. **[オープンポート]** タブをクリックします。
3. 特定のポートを選択します。
4. **[アクション]** メニューをクリックします。
5. ドロップダウンメニューから、**[表示]** を選択します。

   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、OT Security 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、OT Security 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、管理コンソールのユーザーインターフェース要素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。
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、ポリシーカテゴリとサブカテゴリを参照してください)。 • 設定イベント - 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詳細画面に移動します。

デバイスポート

[デバイスポート] タブはネットワークスイッチから表示でき、ネットワークスイッチのポートに関する詳細が含まれています。OT Security は、スイッチに対する SNMP クエリを使用してこのデータを収集します。表示される各ポートの詳細には、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、説明などの情報があります。

MAC	Name	Status	Admin Status	Alias	Description	Type	Time of Query
	P1.11	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P0.2	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.15	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.1	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.1	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.3	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.7	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.8	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.3	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.5	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.6	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.4	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.6	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	vlan1	Up	Up	vlan1	Siemens, SIMATIC NE...	L3ipvlan	04:34:37 AM · May 28...
	P1.16	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.2	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...

Items: 31

注意: このタブを表示するには、アカウントでこの機能を有効にします。この機能をアクティブ化するには、Tenable サポート に連絡してください。

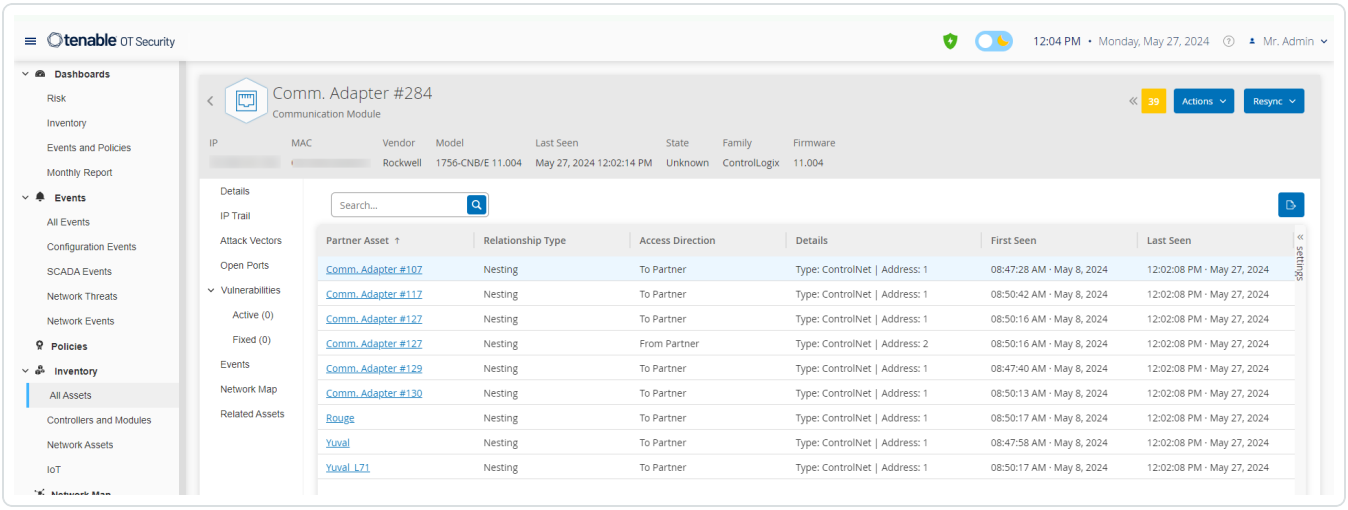
関連資産

資産の**[関連資産]**ページには、ネストされたすべての資産のリストが表示されます。

[関連資産]ページにアクセスする方法

1. **[インベントリ]** > **[すべての資産]**テーブルで、資産をクリックして資産の詳細ページを開きます。
2. 左側のナビゲーションペインで**[関連資産]**をクリックします。

   [関連資産]ページが表示されます。

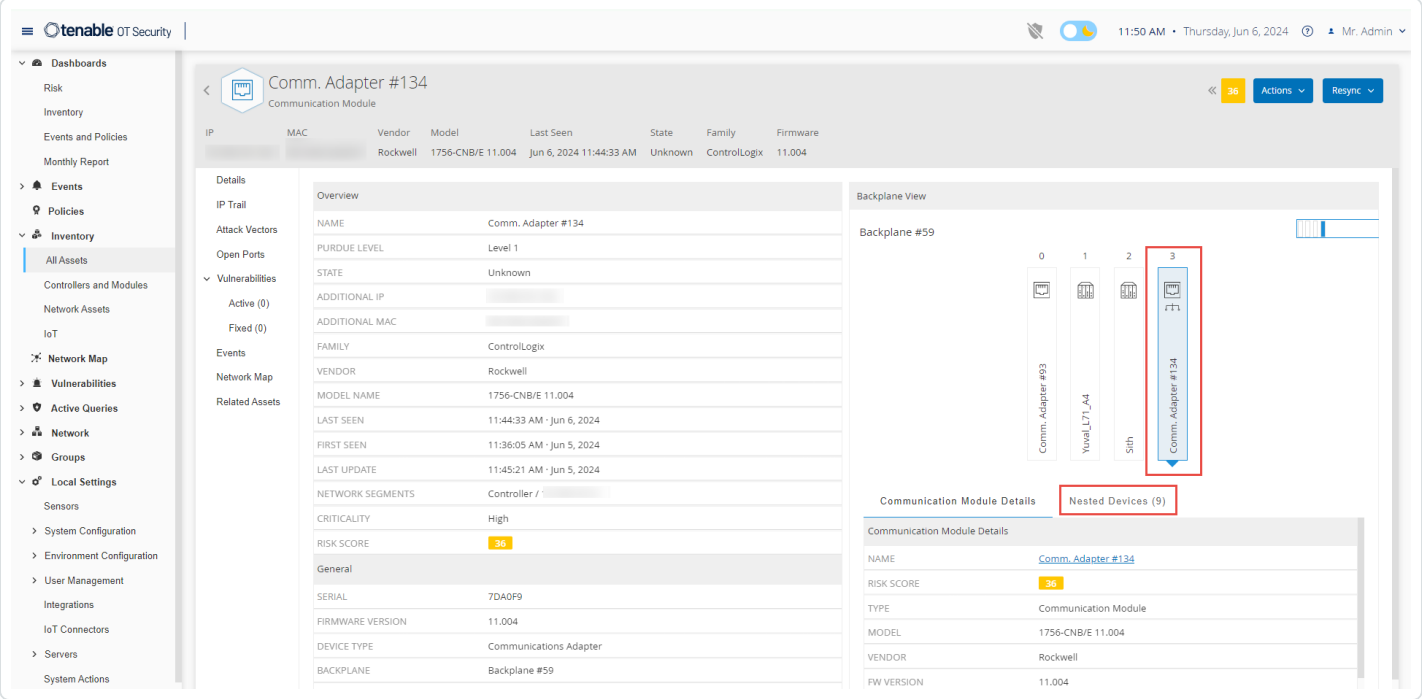


次の詳細を含む**[関連資産]**ページが表示されます。

列	説明
パートナー資産	関連資産の名前。
関係タイプ	関連資産との関係のタイプ: ネスト。
アクセス方向	資産とそのパートナーの間のアクセスの方向。
詳細	資産タイプの詳細。たとえば、ControlNet または IP。
初回確認日	OT Security がこの資産を最初に発見した日付。
最終確認日	OT Security がこの資産を最後に検出した日付。

ネストされた資産の詳細

ネストされたデバイスとは、プログラマブルロジックコントローラー(PLC)のバックプレーンやデバイスの背後で接続されているPLCまたはその他の産業用制御システム(ICS)モジュールのことです。これは、通信アダプターに直接接続された可変周波数ドライブ(VFD)に似ています。ネストされた資産の詳細を表示するには、**[関連資産]**ページで、ネストされた資産のリンクをクリックします。OT Securityは アイコンを使用してネストされたデバイスを示します。



[ネストされた資産の詳細]ページに次の詳細情報が表示されます。

セクション	説明
概要	名前、パデューレベル、状態、追加IPなどの資産の詳細が含まれます。
全般	シリアル番号、ファームウェアバージョン、デバイスタイプ、バックプレーン番号、スロット番号などの詳細が含まれます。
バックプレーンビュー	バックプレーンのグラフィックビューが表示されます。バックプレーンビューにあるデバイス名をクリックすると、**[通信モジュールの詳細]**タブと**[ネストされたデバイス]**タブが表示されます。

資産詳細の編集

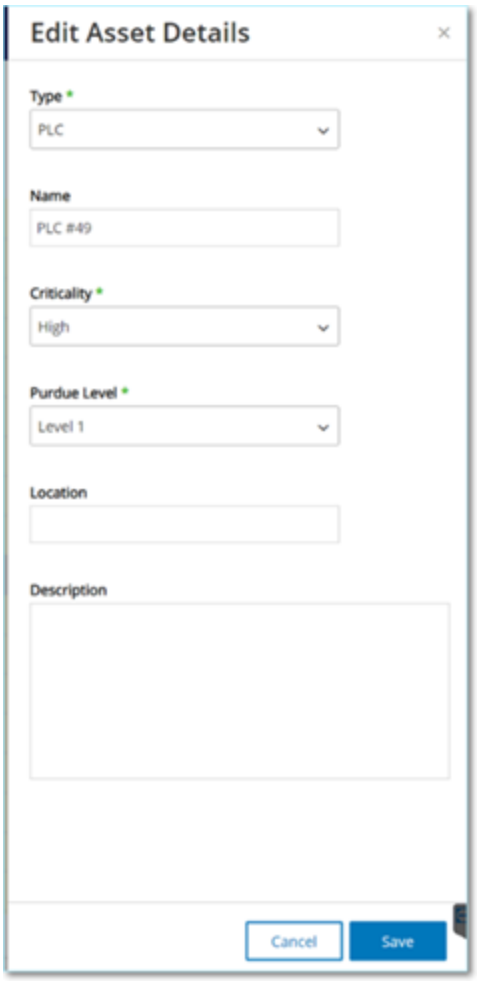
OT Security は、内部データとネットワークでのアクティビティに基づいて、資産のタイプと名前を自動的に識別します。システムがこの情報を収集できない場合や自動識別が正確でないと思われる場合は、直接 UI から、または CSV ファイルをアップロードすることでこれらのパラメーターを編集できます。資産の一般的な説明とユニットの場所の説明を追加することもできます。

UI による資産詳細の編集

1 つの資産の資産詳細を編集するには、次のようにします。

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、OT Security 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。

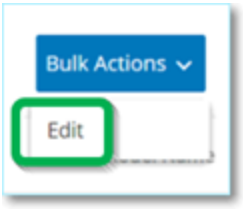
編集した詳細がその資産に保存されます。

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。

   > **注意**: 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。

   > **注意**: 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。

   > **注意**: [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。

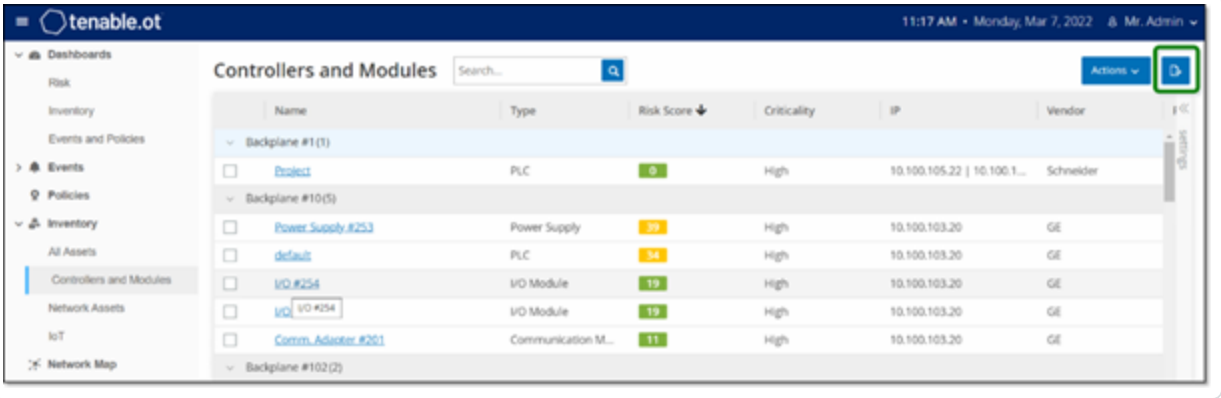
   資産が新しい設定で保存されます。

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。

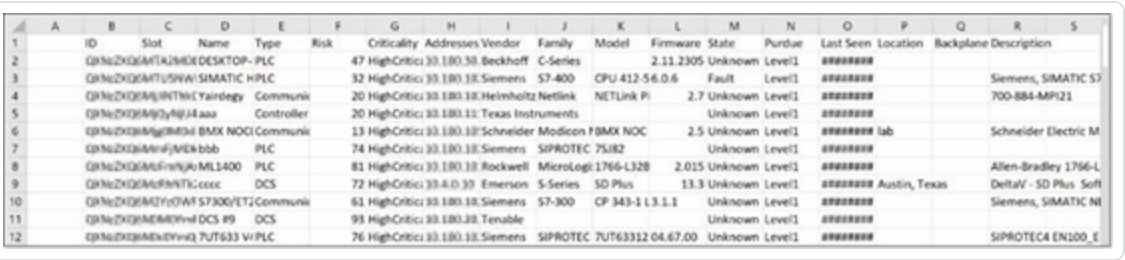
CSV で資産詳細を編集する手順

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。



4. セルの内容を変更して、編集可能なパラメーターを編集します(編集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)。

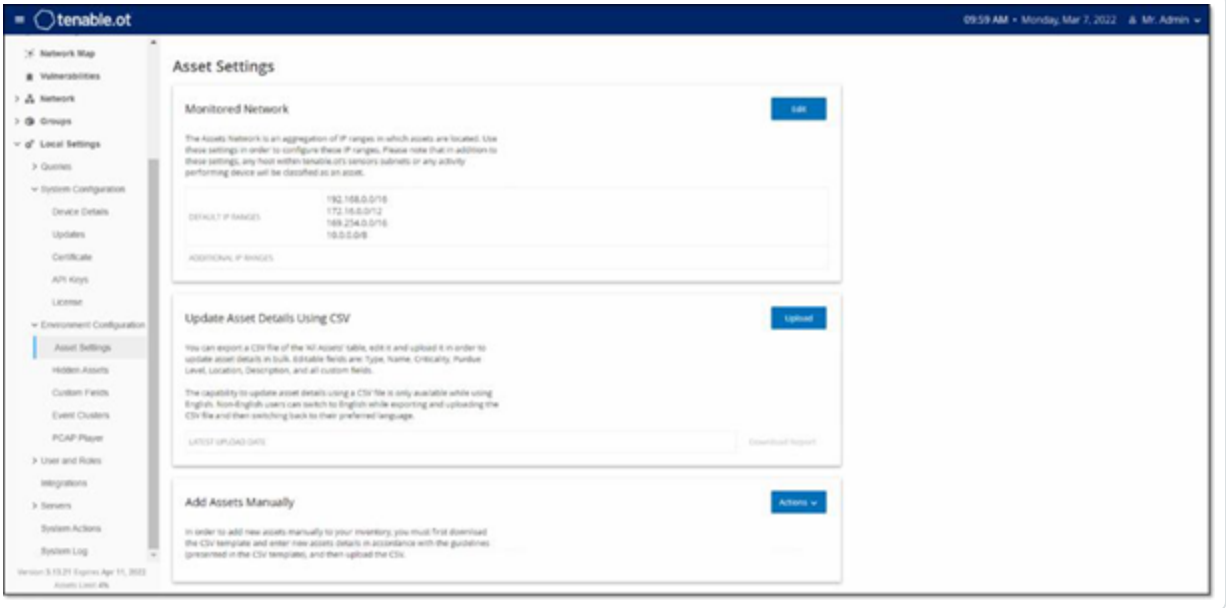
> **注意**: 特定のオプションを必要とするパラメーター(タイプ、重大度、パデューレベルなど)には有効なデータを入力する必要があります。有効なデータでない場合、対応する資産は更新されません。

5. ファイルを csv ファイルタイプとして保存します。

注意: 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。

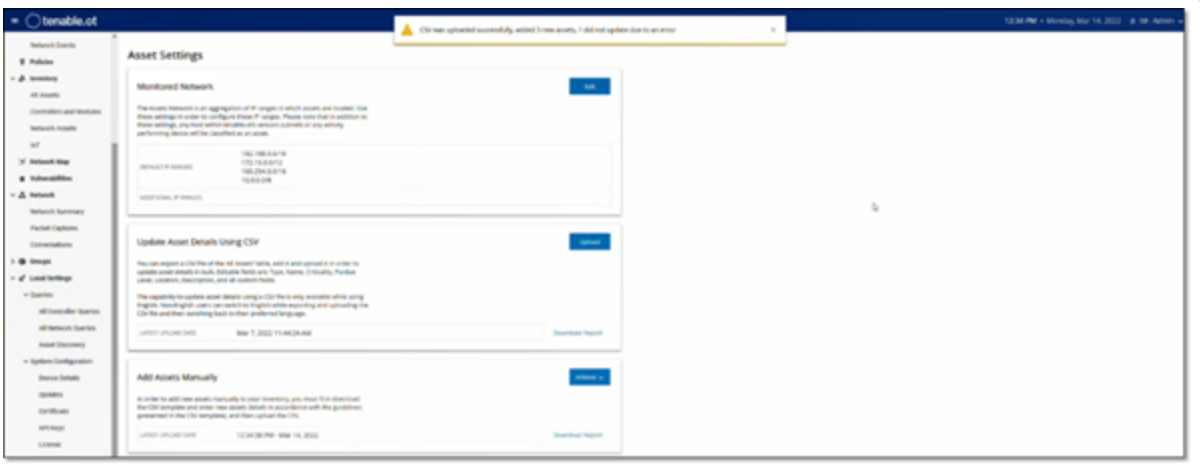
6. **[ローカル設定]** で、**[環境構成]** > **[資産設定]** に移動します。

   [資産設定] 画面が表示されます。



7. **[CSV を使用して資産の詳細をアップデート]** 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。

   更新された行数を示す確認メッセージが表示されます。



[CSV を使用して資産の詳細をアップデート] セクションの **[最終アップロード日]** ボックスが更新されます。

9. アップロードの結果に関する詳細を確認するには、**[CSV を使用して資産の詳細をアップデート]** 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。

   OT Security は、アップデートされた資産 ID とアップデートに失敗した資産 ID をリストした csv ファイルをダウンロードします。

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、非表示の資産のイベントとネットワークアクティビティは、引き続き表示されます。

非表示の資産は、**[ローカル設定]** > **[環境設定]** > **[非表示の資産]** ページから復元できます。

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. ヘッダーバーで、**[アクション]** をクリックします。

   メニューが表示されます。

4. **[資産を非表示にする]** を選択します。

   [非表示の資産] ページが表示されます。

5. (オプション) **[コメント]** ボックスで、資産に関するテキストコメントを追加します。

   > **注意**: コメントは、**[ローカル設定]** > **[環境設定]** > **[非表示の資産]** ページの、削除された資産のリストで表示されます。

6. **[非表示]** をクリックします。

   OT Security **[インベントリ]** ページと **[グループ]** ページで当該資産が非表示になります。

診断のエクスポート

資産または資産グループの診断レポートをエクスポートしてダウンロードできます。このレポートから、誤検出やその他の問題を知ることができます。このレポートを Tenable サポート に共有して、詳細な分析を行うことができます。

診断レポートをエクスポートする方法

1. 左側のナビゲーションバーで、**[インベントリ]** > **[すべての資産]** の順に移動します。

   [すべての資産] ページが表示されます。

2. [すべての資産] テーブルで、診断レポートのエクスポートに含める 1 つまたは複数の資産を選択します。

3. 次のいずれかを行います。

   - 1 つの資産の場合: 右上にある **[アクション]** > **[診断のエクスポート]** をクリックします。
   - 複数の資産の場合: 右上にある **[一括アクション]** > **[診断のエクスポート]** をクリックします。

   OT Security により、選択した 1 つまたは複数の資産の診断レポートがダウンロードされます。診断レポートは tar.gz ファイルで、資産の詳細は .json ファイルに含まれています。

   診断レポートの名前には、資産の名前、タイムスタンプ、OT Security のバージョンが含まれます。たとえば、次のようになります。

   1 つの資産の場合: `TOTS_Rouge_3.19.15_2024-06-03T07_05_27.tar.gz`

   複数の資産の場合: `TOTS_AssetsReport_3.19.15_2024-06-03T07_17_54.tar.gz`

4. 診断レポートを抽出し、詳細な分析のために Tenable サポート に共有します。

資産固有の Tenable Nessus スキャンの実行

Tenable 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ツールです。OT Security では、OT ネットワーク内の特定の IT 資産に対して、Tenable Nessus の**基本ネットワークスキャン**を実行できます。これは、サーバーとネットワークデバイスの脆弱性に関してさらに多くの情報を収集するための、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 と SNMP の認証情報があればそれを使用します。この操作は、関連する PC ベースのマシンでのみ実行できます。スキャン結果には、[脆弱性] ページからアクセスできます。カスタマイズし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に対して特定の Tenable Nessus プラグインのセットを実行することもできます。Tenable Nessusプラグインスキャンを参照してください。

注意: Tenable Nessus は、IT 環境で最適に動作する侵入型ツールです。Tenable では、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。

特定の資産に Tenable Nessus スキャンを実行する手順

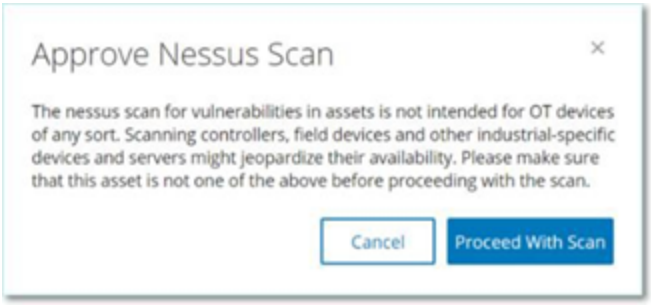
1. **[インベントリ]** > **[ネットワーク資産]** に移動します。

   [ネットワーク資産] ページが表示されます。

2. スキャンする 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. 右上の **[アクション]** > **[Nessus スキャン]** をクリックします。

   [Nessus スキャンの承認] ダイアログボックスが表示されます。



4. **[スキャンに進む]** をクリックします。

   OT Security が Nessus スキャンを実行します。

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]** > **[コントローラーとモジュール]** ページの **[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、資産を識別します。

- **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使用される 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 が有効な資産の設定の詳細を取得します。
- **状態** – 資産の現在のステータス(**実行中**、**停止中**、**障害**、**不明**、**テスト**)を検出します。
- **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]** セクションに表示されます。

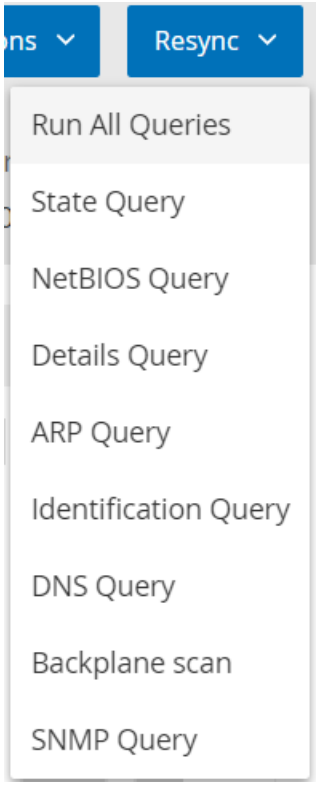
特定の条件下で、**[再同期]** ボタンが無効になる可能性があります。考えられる理由は次のとおりです。

- デバイスに到達できないか、使用できるクエリがない
- **アクティブクエリ**ページで設定されたアクセス許可により、管理者以外のアカウントによる特定のクエリの開始が制限されている可能性がある
- この OT Security デプロイメントでは、クエリが有効になっていない
- **[アクティブクエリ]** > **[手動]** セクションのすべてのクエリが無効になっている
- 資産にクエリ用の既知の IP アドレスがない

資産データの再同期の実行手順

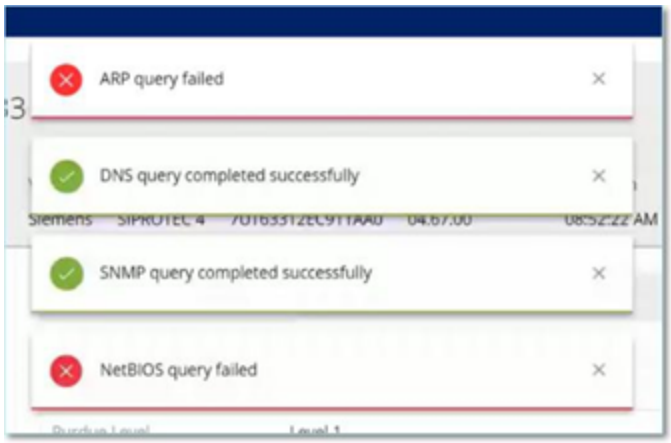
1. 目的の資産の **資産詳細**ページで、右上にある **[再同期]** をクリックします。

   クエリのドロップダウンリストが表示されます。



2. 実行するクエリをクリックするか、**[すべてのクエリを実行]**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。

   各クエリが実行されると、クエリのステータスを知らせる通知が表示されます。



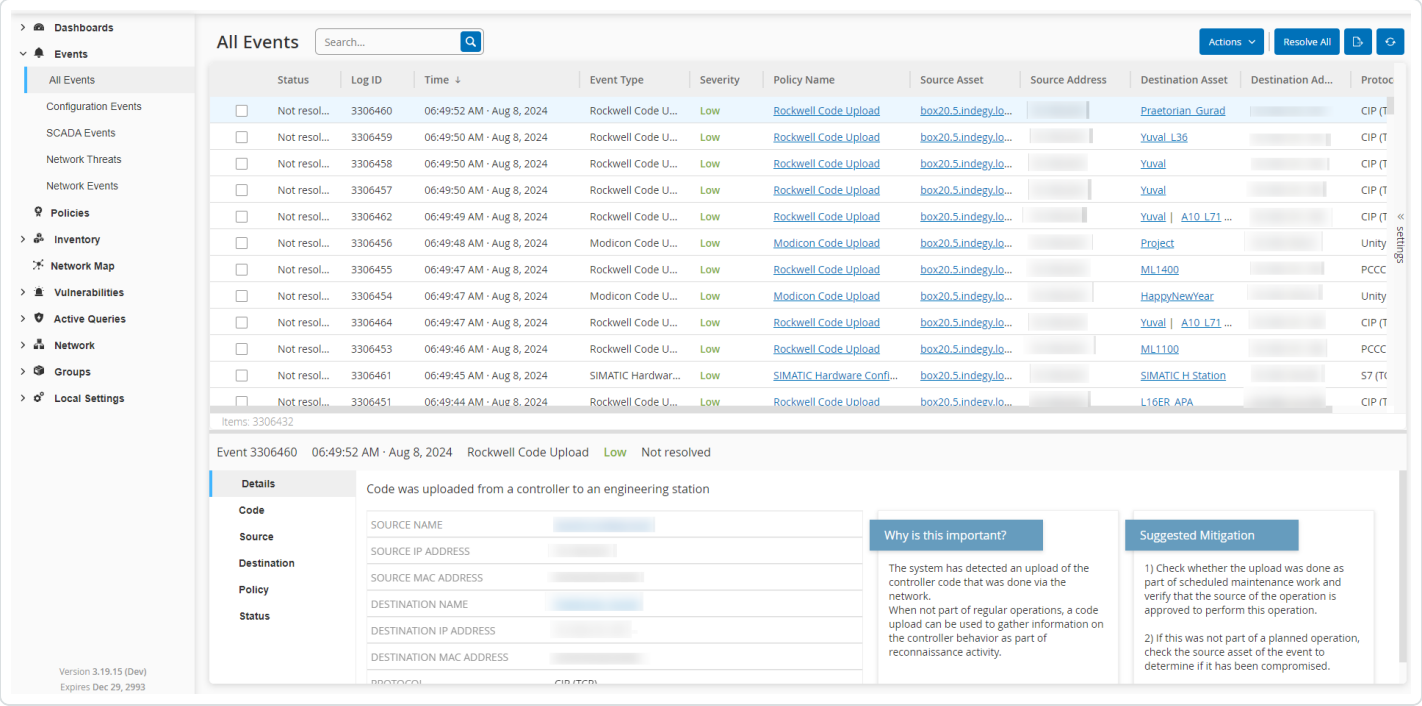
クエリが終了するたびに、OT Security はその資産のシステムデータを新しいデータに基づいて更新します。

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。OT Security システムで設定したポリシーは、設定イベント、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イベントを生成します。OT Security は深刻度レベルを各ポリシーに割り当て、イベントの深刻度を示します。

ポリシーをアクティブ化すると、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]** ページに表示されます。イベントの特定のサブセットが、**設定イベント**、**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ウィンドウに表示されます。

イベントページのそれぞれのイベント (設定イベント、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選択することで、表示設定をカスタマイズできます。イベントは、イベントタイプ、深刻度、ポリシー名などに基づいてグループ化できます。イベントリストの並べ替え、フィルタリング、検索も可能です。カスタマイズ機能の詳細については、表のカスタマイズを参照してください。

ヘッダーバーの **[アクション]** ボタンを使用して、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。

ページの下部には、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。

注意: 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。

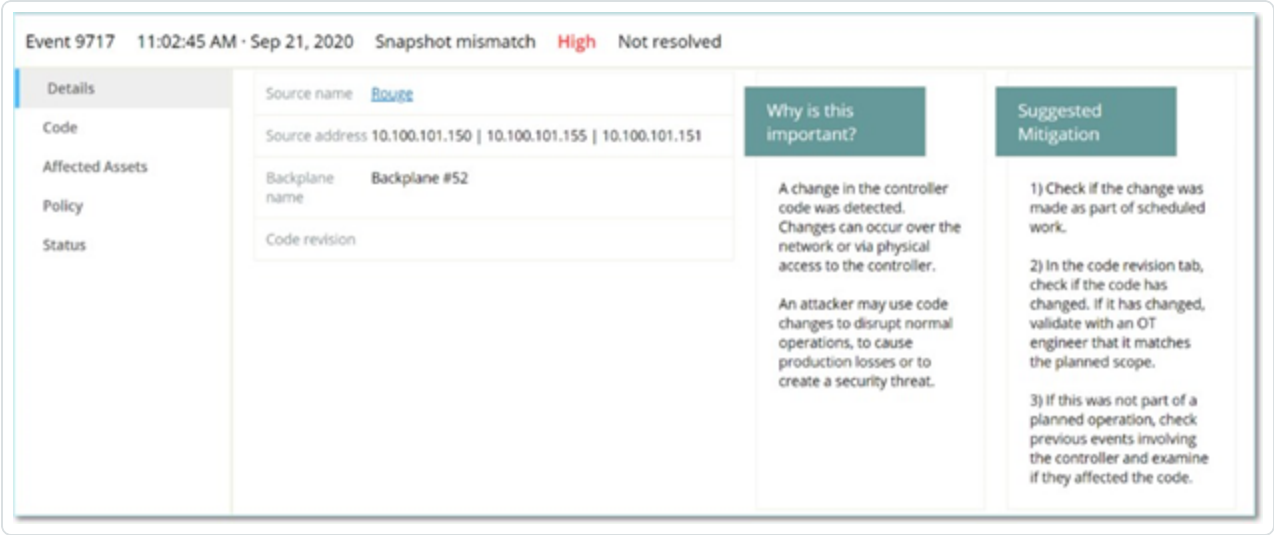
各イベントに関連するパケットキャプチャファイルをダウンロードできます。ネットワークを参照してください。各イベントリストに表示される情報について、次の表で説明します。

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。インベントリ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	OT Security の資産詳細でユーザーが入力した資産の場所。インベントリを参照してください。

最終確認日	デバイスが OT Security 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。
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、ポリシーカテゴリとサブカテゴリを参照してください)。 • 設定イベント - 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。

イベントの詳細の表示

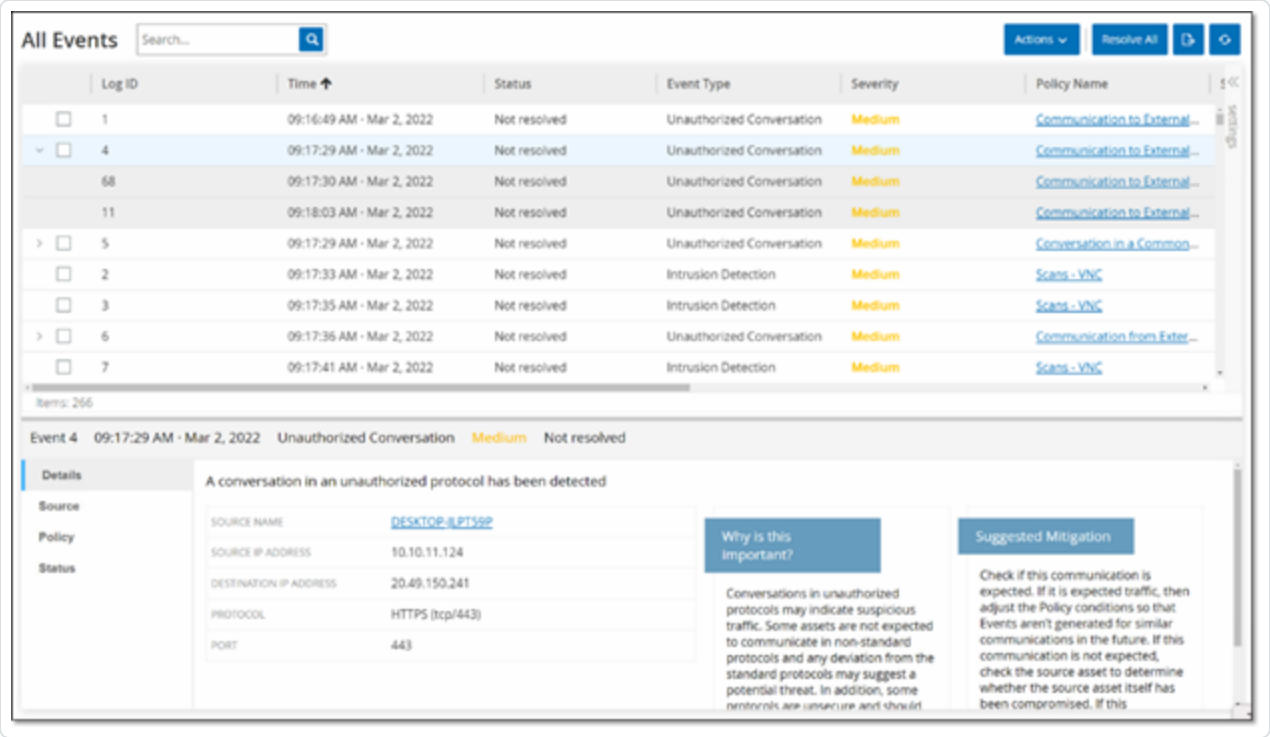


イベント画面の下部に、選択したイベントの追加詳細が表示されます。情報は複数のタブに分割されています。選択したイベントに関連するタブのみが表示されます。詳細情報には、関連エンティティに関する追加情報へのリンクが含まれています(ソース資産、デスティネーション資産、ポリシー、グループなど)。

- **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 設定、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設定の詳細については、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、問題を解決するために必要な手順を実行するか、対応が不要であると判断した場合は、そのイベントは**解決済み**としてマークされます。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、一括処理で**解決済み**としてマークすることもできます。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**ページ（設定イベント、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. ヘッダーバーで、**[アクション]** をクリックします。

   ドロップダウンメニューが表示されます。

   > **注意**：複数のイベントを**解決済み**としてマークする場合、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. **[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. (オプション) **[コメント]** ボックスに、問題を解決するための緩和策を説明するコメントを追加できます。
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**としてマークされます。

すべてのイベントの解決

[すべて解決] アクションは、現在の表示に適用されているフィルターに基づいて、現在のページのすべてのイベントに適用されます。たとえば、**設定イベント**ページが開いている場合に **[すべて解決]** を選択すると、設定イベントは解決しますが、SCADA イベントなどは解決しません。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**ページ (設定イベント、SCADA イベント、ネットワーク脅威、ネットワークイベント) で、ヘッダーバーで **[すべて解決]** をクリックします。

   [すべてのイベントの解決] ウィンドウが表示され、解決するイベントの数が表示されます。

2. (オプション) **[コメント]** ボックスで、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。
3. **[解決]** をクリックします。

   OT Security に警告メッセージが表示されます。
4. **[解決]** をクリックします。

   OT Security は、現在表示されているすべてのイベントを**解決済み**としてマークします。

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)。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。

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**ページから除外を作成できます。ポリシーから除外する特定のイベントの条件を指定できます。

指定した条件のイベントの生成を後で再開するために、除外を削除できます。ポリシーを参照してください。

ポリシーの除外の作成手順

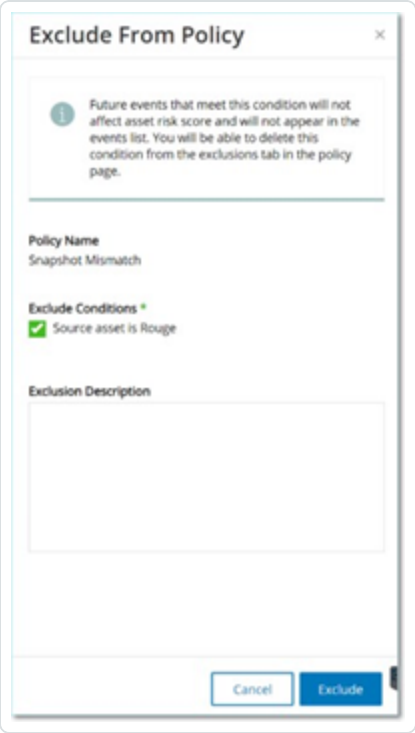
1. 関連する**イベント**ページ(設定イベント、SCADA イベント、ネットワーク脅威、ネットワークイベント)で、除外を作成するイベントを選択します。
2. ヘッダーバーで、**[アクション]**をクリックするか、イベントを右クリックします。

   [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、指定された条件のいずれかを満たす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する各条件の横にあるチェックボックスを解除できます。

   > **注意**: たとえば、以下に示すウィンドウで、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 対話に引き続き適用するには、「プロトコルは UDP です」を選択解除する必要があります。



注意: 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。次の表を参照してください。

5. (オプション) **[除外の説明]** ボックスで、除外に関するコメントを追加できます。
6. **[除外]** をクリックします。

   OT Security が除外を作成します。

   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	設定イベント (アクティビティ)	• 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 • 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 • 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

OT Security 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(たとえば Wireshark など)を使用してダウンロードおよび分析できます。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。ネットワークを参照してください。

注意: 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]** > **[システム設定]** > **[パケットキャプチャ]** 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**ページで、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. ヘッダーバーで、**[アクション]** をクリックします。

   [アクション] メニューが表示されます。
3. **[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 OT Security 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、OT Security 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自動的に適用されるよう設定されます。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。

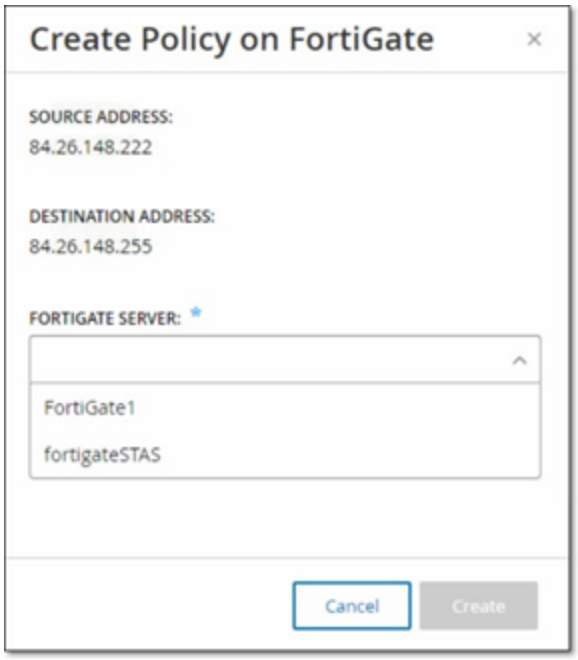
FortiGate ポリシーを提案する前に、FortiGate ファイヤーウォールサーバーと OT Security の統合を設定する必要があります。FortiGate ファイヤーウォールを参照してください。

FortiGate ポリシーの提案手順

1. 関連する **イベント** ページ (設定イベント、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. ヘッダーバーで、**[アクション]** をクリックするか、イベントを右クリックします。

   ドロップダウンメニューが表示されます。
3. **[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。OT Security 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]** のドロップダウンボックスで、必要なサーバーを選択します。

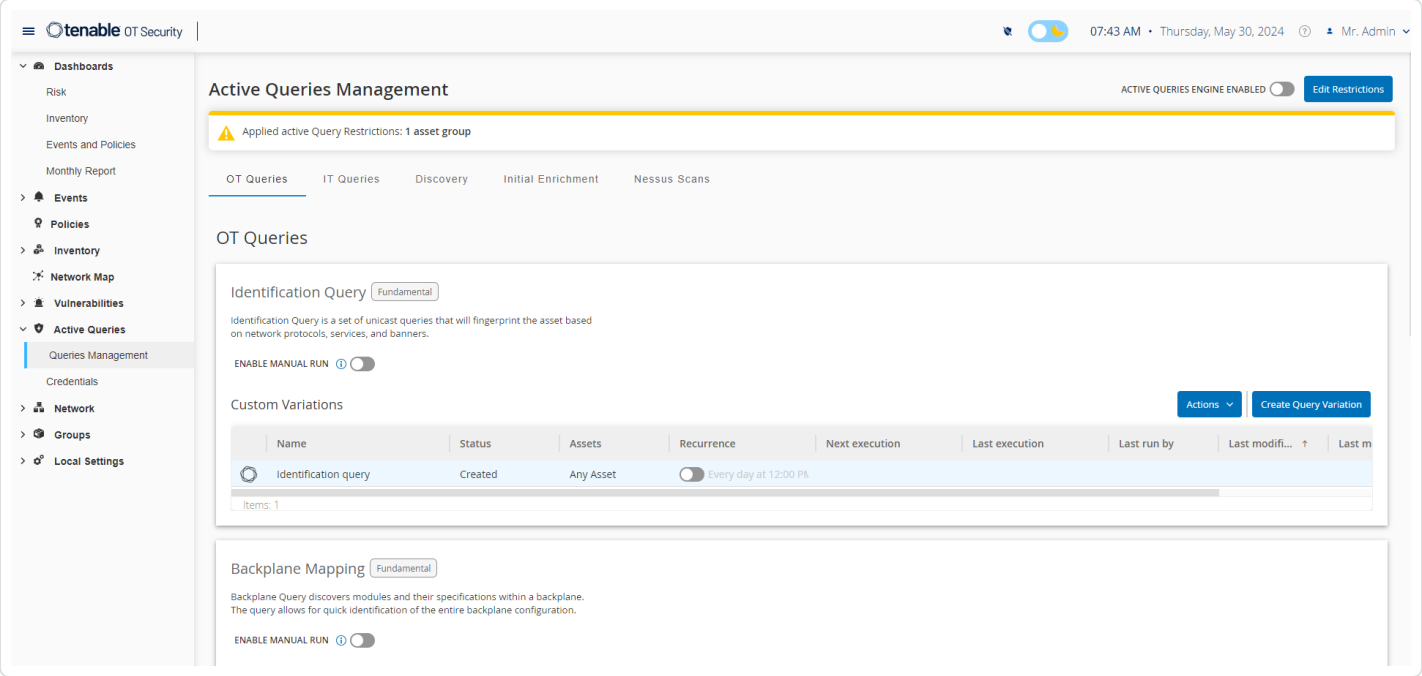


5. **[作成]**をクリックします。

   ポリシーが FortiGate で作成され、パネルが閉じます。FortiGate アプリケーションで新しいポリシーを表示できます。FortiGate 管理者は、必要に応じて設定を調整できます。

アクティブクエリの管理

[アクティブクエリ管理]ページでは、アクティブクエリを設定して有効にすることができます。Tenable は、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を推奨していますが、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や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、クエリカードにある**[手動実行を有効化]**トグルを有効にすることで、クエリをオンデマンドで開始できます。**[手動実行を有効化]**オプションを無効にした場合、**[資産の詳細]**ページ (**[インベントリ]** > **[すべての資産]**) で 再同期の実行 を選択すると、OT Security はこのオプションをオーバーライドするかどうかのプロンプトが表示されます。

クエリテクノロジーの詳細については、OT Security テクノロジーを参照してください。

注意: クエリを無効にすると、OT Security が資産の特定に失敗する場合があります。OT Security は、パッシブモニタリングとアクティブクエリによってデバイスを追跡します。

ヒント: アクティブクエリを機能させるには、**[アクティブクエリエンジンを有効にする]**トグルをクリックします。アクティブクエリを有効にした後、OT Security はヘッダーに を表示し、クエリエンジンが実行中であることを示します。アクティブクエリを実行するには、各クエリを個別に有効化する必要があります。

[アクティブクエリ管理]ページでは、クエリが次のタイプに分類されます。クエリタイプごとに個別のクエリタブがあり、そのクエリのリストが表示されます。

- **OT クエリ** – 専用プロトコルを使用して、コントローラーと埋込デバイスを安全にポーリングして詳細情報を取得するように設計されたクエリです。OT Security は、読み取り専用クエリを実行して、PLC の実行状態や、バックプレーンに接続されているその他のモジュールなどのデバイス情報を収

集します。OT Security がサポートする専用プロトコルをリッスンしているデバイスにクエリをかけます。クエリタイプには、**識別情報のクエリ**、**バックプレーンマッピング**、**詳細のクエリ**、**状態のクエリ**、および**コードスナップショット**があります。

- **IT クエリ** – OT Security が観察した IT タイプの監視対象資産から追加のデータポイントをフェッチするためのクエリです。NetBIOS を除き、IT タイプのクエリには認証情報が必要です。
    - **NetBIOS クエリ**は、OT Security センサーまたは OT Security 自体のブロードキャスト範囲で NetBIOS をリッスンしているデバイスの検出を試みます。このクエリのタイプは、近くにある Windows デバイスを特定するのに適しています。
    - **SNMP クエリ**は、SNMP v2 または SNMP v3 の認証情報を使用して、SNMP をサポートするネットワークインフラまたはネットワーク接続デバイスに対して識別詳細情報を求めます。OT Security は、SNMP システムの説明やその他のパラメーターを求めるクエリを実行し、資産文脈の追加やフィンガープリントの取得が簡単にできるようにします。
    - **WMI 詳細クエリ**は、Windows ベースのシステムからさまざまな重要データポイントをフェッチします。これには、OT Security がクエリをかけるシステムに、Windows Management Instrumentation (WMI) サービスをポーリングするのに十分なアクセス許可を持つ Windows アカウント (ローカルまたはドメイン) がなければなりません。
    - **WMI USB 状態**クエリは、エンジニアリングワークステーションやサーバーなどの Windows デバイスに、USB ドライブやポータブルハードドライブなどのリムーバブルメディアが接続されているかどうかを判別します。このクエリは、**Windows マシンの USB 設定の変更**ポリシーが正しく機能するための前提条件となっており、このポリシーと密接に関連しています。
    - **Nessus 基本スキャン**は、IP アドレス、FQDN、オペレーティングシステム、オープンポートなどのシステムの詳細をフェッチします。
    - **ARP クエリ**(アドレス解決プロトコルクエリ) は、同じブロードキャストドメイン内にある IP 接続デバイスのネットワークインターフェースのハードウェアアドレスまたは MAC アドレスをフェッチします。
- **検出** – これらのクエリは、OT Security が監視するネットワークにある資産をリアルタイムで検出します。
    - **資産検出** – インターネット制御メッセージプロトコル (ICMP) または ping を使用して、ライブ IP アドレスや応答する IP アドレスを検出します。

- **アクティブ資産追跡** – 既知の監視対象資産が稼働していて利用可能であることを確認するために、その資産に対して定期的に ping を試行します。
- **コントローラー検出** – 一連のマルチキャストパケットをネットワークに送信して、コントローラーまたは ICS デバイスに対し、それぞれの情報を OT Security に直接返信するように促します。
- **Ping クエリ** – インターネット制御メッセージプロトコル(ICMP) の ping を送信して、資産が到達可能かどうかを検証します。
- **DNS ルックアップ** – DNS サーバーの詳細をフェッチします。
- **ポートマッピング** – 監視対象資産のオープンポートに関する詳細をフェッチします。

- **初期強化** – 特定の基準または条件に基づく自動 OT Security クエリです。資産強化ベースのクエリは、Tenable が初めてデバイスをパッシブまたはアクティブに観察したときに実行されます。資産強化により、OT Security はデバイスがネットワーク上に現れると直ちにそのデバイスのフィンガープリントを取得して識別します。
- **Nessus スキャン** – Tenable Nessus プラグインスキャンは高度な Nessus スキャンを起動します。このスキャンでは、CIDR と IP アドレスのリストで指定されている資産に対し、ユーザー定義リストに載っているプラグインを実行します。詳細は、Nessus プラグインスキャンの作成を参照してください。

カスタムクエリの作成

各クエリタイプには、定期的にまたはオンデマンドで実行することができるシステムのデフォルトのバリエーションがあります。その他にも、異なるプロジェクトや機能に対して固有の設定をして、クエリごとのバリエーションを追加で作成することができます。

たとえば、次のシナリオに対応したカスタムクエリを設定できます。

- 工場内の複数の場所でメンテナンス時間が異なる
- 複数の資産でプロジェクトと重大度が異なる
- OT 部門と IT 部門でクエリが異なる

クエリバリエーションを作成する方法

1. **[アクティブクエリ]** > **[クエリ管理]** に移動します。

   [アクティブクエリ管理] ページが表示されます。

2. 必要なクエリタイプのタブをクリックします。

   OT Security がクエリタイプと利用可能なクエリのリストを表示します。

3. 必要なクエリタイプセクションで、**[クエリバリエーションの作成]** をクリックします。

   [クエリバリエーションの作成] パネルが表示されます。

4. **[名前]** ボックスにクエリの名前を入力します。

5. **[資産]** ドロップダウンボックスで資産グループを選択します。

   > **注意**: **[検索]** ボックスを使用して、特定のグループを検索することもできます。

6. クエリを繰り返し実行する場合は、**[定期実行]** トグルをクリックします。

   OT Security は、**[繰り返し間隔]** セクションを有効にします。

7. 数字を入力して、ドロップダウンボックスから **[日]** または **[週]** を選択します。特定のクエリでは **[分]** と **[時間]** を設定することもできます。

   [週] を選択した場合は、クエリを実行する曜日を指定します。

8. **[時刻]** ボックスで、時計アイコンをクリックして時刻を選択するか手動で時刻を入力して、クエリを実行する時刻 (HH:MM:SS) を設定します。

9. (資産検出のみ) **[IP 範囲]** ボックスに、資産の IP アドレスを入力します。

10. (検出クエリのみ) **[同時にポーリングする資産の数]** ドロップダウンボックスで、資産の数 (10、20、または 30) を選択します。

11. (検出クエリのみ) **[検出クエリの間隔]** ドロップダウンボックスで、検出クエリ間の間隔 (1 ~ 3 秒) を選択します。

12. **[保存]** をクリックします。

    OT Security により、クエリが **[カスタムバリエーション]** テーブルに追加されます。

    クエリバリエーションの実行を参照してください。

制限の追加

特定の資産グループ(IP 範囲、OT サーバー、タブレット、医療機器、ドメインコントローラーなど)に対してクエリが実行されないようにブロックすることができます。特定のプロトコル(クライアント)に制限を適用することもできます。

制限を追加する方法

1. **[アクティブクエリ]** > **[クエリ管理]** に移動します。

   [アクティブクエリ管理] ページが表示されます。

2. 右上の **[制限の追加]** をクリックします。

   [制限の追加] パネルが表示されます。

3. **[ブロックされた資産]** ドロップダウンボックスでブロックする資産グループを選択します。

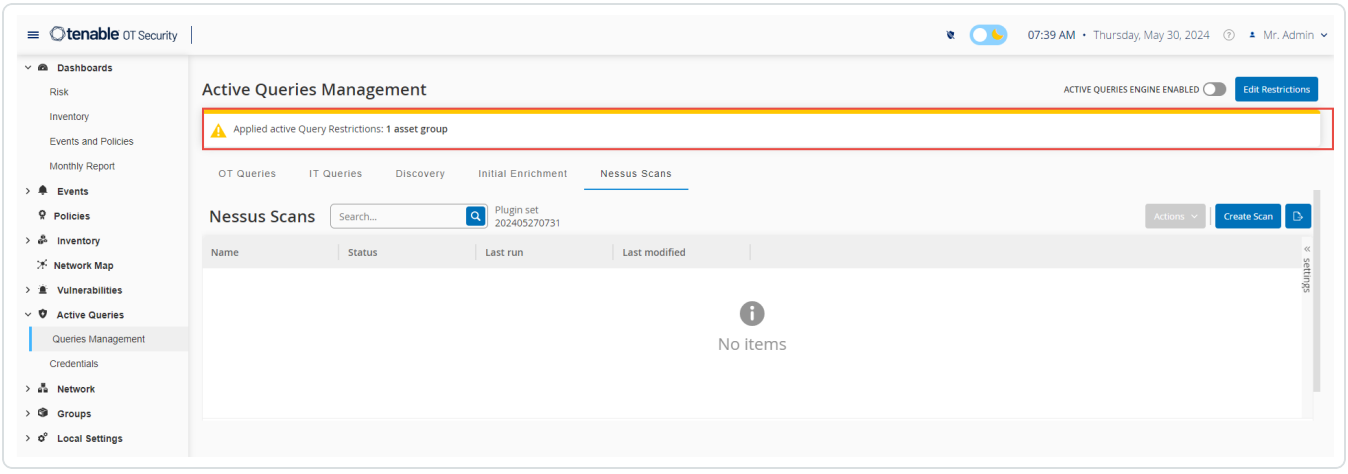
   > **注意**: 検索ボックスを使用して、特定の資産グループを検索できます。

4. **[制限されたクライアント]** ドロップダウンボックスで、目的のクライアントを選択します。

5. **[ブラックアウト期間]** ドロップダウンボックスで、アクティブクエリをブロックする期間を選択します。選択可能なオプションは、スケジュールグループに応じて変わります。デフォルトで表示されるオプションは、**[なし]** と **[勤務時間]** です。

6. **[保存]** をクリックします。

   OT Security により、特定のクライアントと資産グループに制限が適用されます。各タブの上部に、制限があることを示すバナーが表示されます。



クエリバリエーションの編集

クエリの詳細を編集する方法

1. **[アクティブクエリ]** > **[クエリ管理]** に移動します。

   [アクティブクエリ管理] ウィンドウが表示されます。

2. クエリのリストから編集するクエリを選択し、次のいずれかを行います。

   - クエリを右クリックし、**[編集]** を選択します。
   - クエリを選択し、**[アクション]** > **[編集]** をクリックします。

   [クエリの編集] パネルが表示されます。

3. 必要に応じてクエリを変更します。

4. **[保存]** をクリックします。

   OT Security により、クエリバリエーションへの変更が保存されます。

クエリバリエーションの複製

1. **[アクティブクエリ]** > **[クエリ管理]** に移動します。

   [クエリ管理] ページが表示されます。

2. クエリのリストからコピーを作成するクエリを選択し、次のいずれかを実行します。

   - クエリを右クリックし、**[複製]** を選択します。
   - クエリを選択し、**[アクション]** > **[複製]** をクリックします。

   [クエリの複製] パネルが表示され、このパネルにクエリの詳細が表示されます。

3. 必要に応じてクエリの名前と詳細を変更します。

4. **[保存]** をクリックします。

   OT Security によりクエリが保存され、[クエリ] テーブルに表示されます。

クエリバリエーションの実行

必要な場合にはアクティブクエリを実行できます。

クエリを実行する方法

1. **[アクティブクエリ]** > **[クエリ管理]** に移動します。

   [クエリ管理] ページが表示されます。

2. クエリのリストから実行するクエリを選択し、次のいずれかを行います。

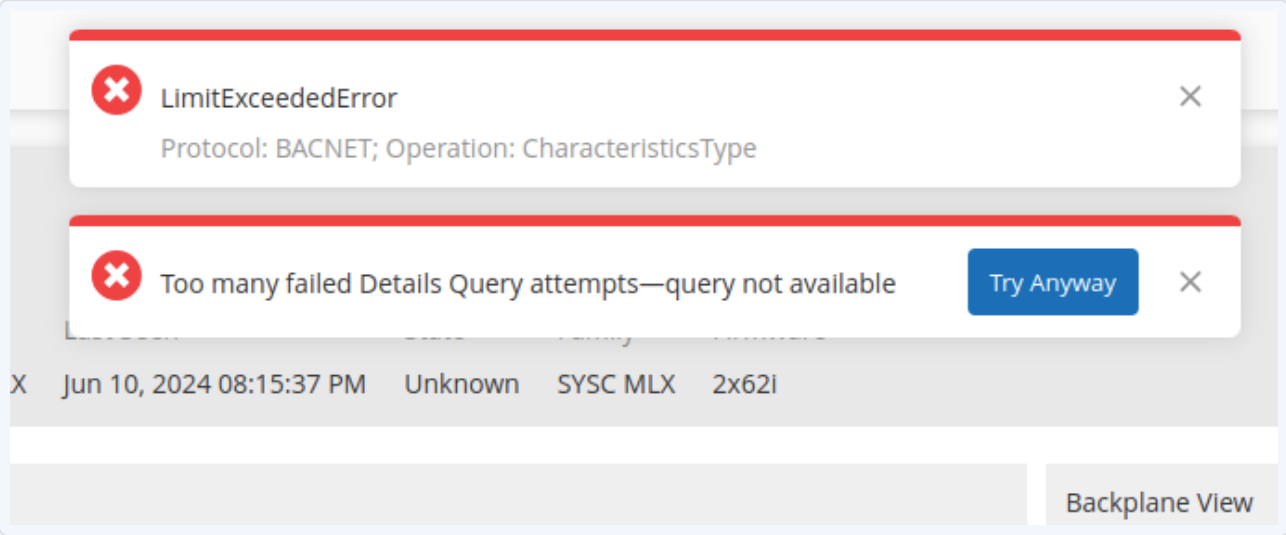
   - クエリを右クリックし、**[今すぐ実行]** を選択します。
   - **[アクション]** メニューで、**[今すぐ実行]** をクリックします。

   クエリを実行するかどうかの確認を求めるメッセージが表示されます。

3. **[OK]** をクリックします。

   選択したクエリが OT Security により実行されます。

   注意: **[とにかく試してみる]** オプションを使用して、アクティブクエリ試行回数の制限を無視して、デバイスまたはネットワークでアクティブクエリを続行できます。



クエリログのダウンロード

クエリバリエーションの前回の実行ログをダウンロードできます。ログを使用して、アクティブクエリに含まれる資産やプロトコルに関する問題のトラブルシューティングを行うことができます。

直近のクエリログをダウンロードする方法

1. **[アクティブクエリ]** > **[クエリ管理]** に移動します。

   [クエリ管理] ウィンドウが表示されます。

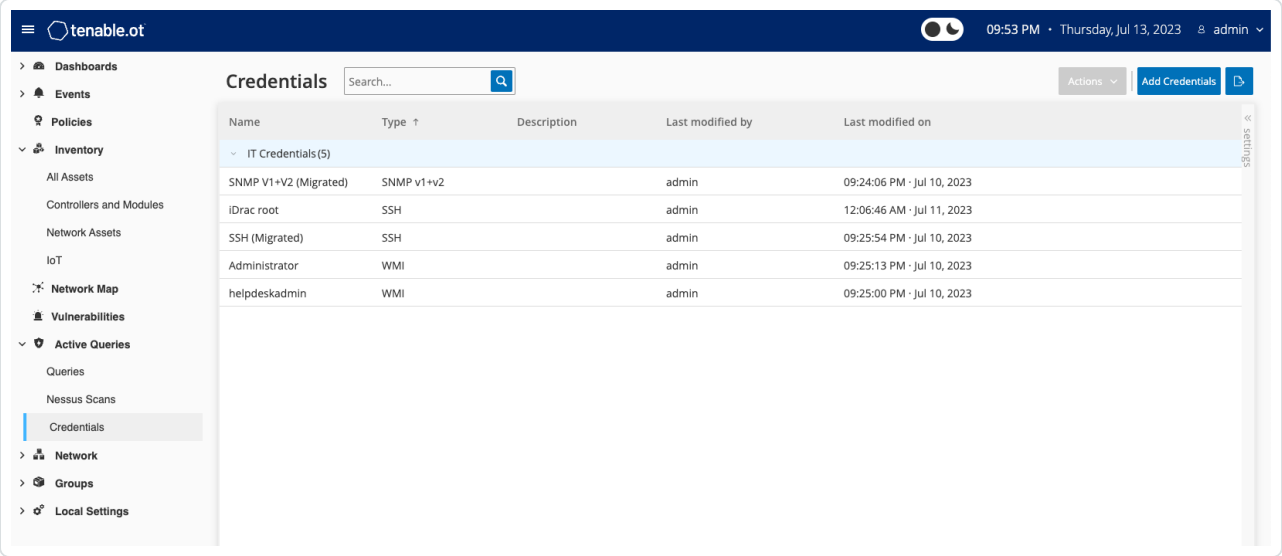
2. クエリのリストから、ログをダウンロードするクエリを選択し、次のいずれかを行います。

    - クエリを右クリックし、**[直近の実行ログをダウンロード]** を選択します。
    - **[アクション]** メニューで、**[直近の実行ログをダウンロード]** をクリックします。

OT Security は、直近のアクティブクエリのログをダウンロードします。

認証情報

必要に応じて、**[認証情報]** ページでデバイス認証情報を設定します。ネイティブのネットワークプロトコル、または独自のプロトコルで通信する場合、デバイスは認証情報を要求しません。ただし、OT Security がサポートする特定のデバイスは、資産検出を実行するために認証情報を要求する場合があります。



認証情報の追加

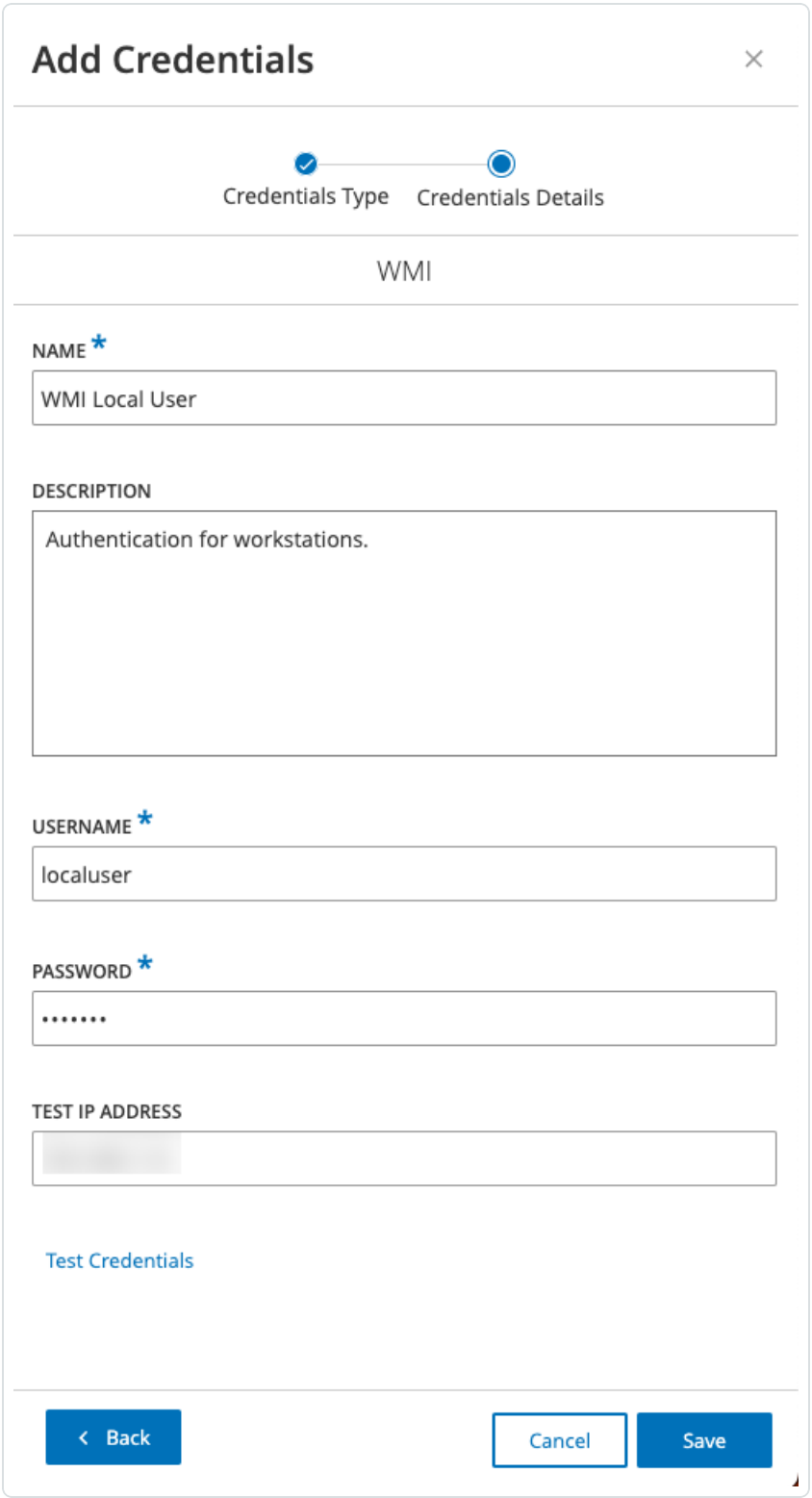
認証情報の追加手順

1. **[アクティブクエリ]** > **[認証情報]** に移動します。

    [認証情報] ページが表示されます。

2. 右上の **[認証情報の追加]** をクリックします。

[認証情報の追加]パネルが表示されます。



3. **[認証情報タイプ]** セクションで、デバイスタイプをクリックして選択します。使用できるオプションは次のとおりです。

    - ABB RTU 500
    - Bachmann
    - コンセプト
    - Sel
    - SicamA8000
    - SIPROTEC 5
    - SNMP v1+v2
    - SNMP v3
    - SSH
    - WMI

4. **[次へ]** をクリックします。

    [認証情報の詳細] パネルが表示されます。

5. 次の詳細を指定します。

    - **名前** – 認証情報の名前
    - **説明** – 認証情報の説明
    - **ユーザー名** – デバイスのユーザー名
    - **パスワード** – デバイスのパスワード
    - **テスト IP アドレス** – デバイスの IP アドレス

6. **[認証情報のテスト]** をクリックして、OT Security がその認証情報を使用してデバイスに到達できるかどうかを確認します。

7. **[保存]** をクリックします。

    OT Security により認証情報が保存され、**[認証情報]** ページに表示されます。

認証情報の編集

認証情報の詳細を編集できます。

認証情報の編集手順

1. **[アクティブクエリ]** > **[認証情報]** に移動します。

   [認証情報] ページが表示されます。

2. 次のいずれかを実行します。

   - 目的の認証情報を右クリックし、**[編集]** を選択します。
   - 目的の認証情報を選択し、**[アクション]** メニューから **[編集]** を選択します。

   [認証情報の編集] パネルが表示されます。

3. 必要に応じて詳細を変更します。

4. **[保存]** をクリックします。

認証情報の削除

不要になった認証情報は削除できます。

認証情報の削除手順

1. **[アクティブクエリ]** > **[認証情報]** に移動します。

   [認証情報] ウィンドウが表示されます。

2. 次のいずれかを実行します。

   - 目的の認証情報を右クリックし、**[削除]** を選択します。
   - 目的の認証情報を選択し、**[アクション]** メニューから **[削除]** を選択します。

   選択した認証情報が OT Security により削除されます。

WMI アカウント

WMI アカウントを設定することで、OT Security で Windows Management Instrumentation (WMI) クエリを実行できるようになります。OT Security は、Windows システムに関する詳細な情報を得るために、WMI クエリに依存しています。

OT Security は、WMI クエリを実行する際に Tenable Nessus と同じ WMI メソッドに依存しています。スキャンするために WMI アカウントを設定するには、Tenable Nessus ユーザーガイドのローカルおよびリモート監査の Window ログインを有効にするセクションを参照してください。

Nessus プラグインスキャンの作成

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に対し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。

OT Security は、指定された CIDR 内の応答する資産に対してスキャンを実行します。ただし、OT デバイスを保護するために、OT Security は特定の範囲 (PLC 以外) で確認されたネットワーク資産のみをスキャンします。OT Security は、スキャンから**エンドポイント**タイプの資産を除外します。

> **注意**: Tenable Nessus は、IT 環境で最適に動作する侵入型ツールです。Tenable では、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 Tenable Nessus の使用はお勧めしません。

任意の 1 つの資産に Nessus 基本スキャンを実行する場合は、資産固有の Tenable Nessus スキャンの実行を参照してください。

> **注意**: 基本スキャンは、**エンドポイント**タイプの資産に実行できます。

Nessus プラグインスキャンの作成

Nessus プラグインスキャンの作成手順

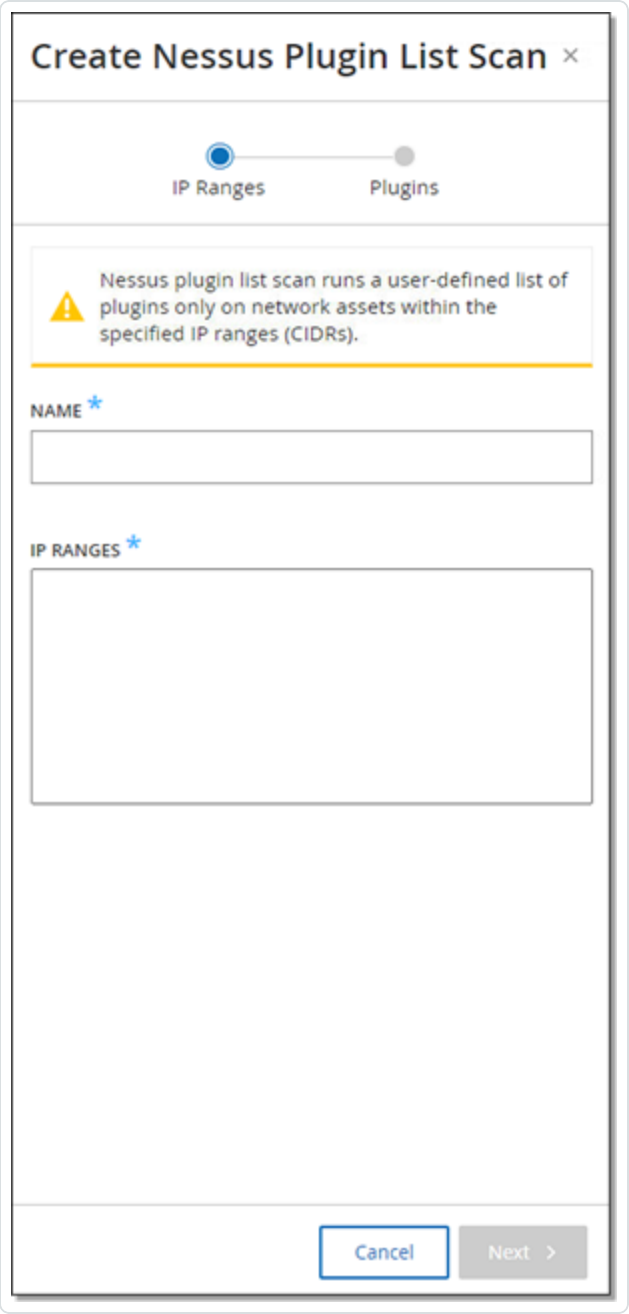
1. **[アクティブクエリ]** > **[クエリ管理]** に移動します。

   [アクティブクエリ管理] ページが表示されます。

2. **[Nessus スキャン]** タブをクリックします。

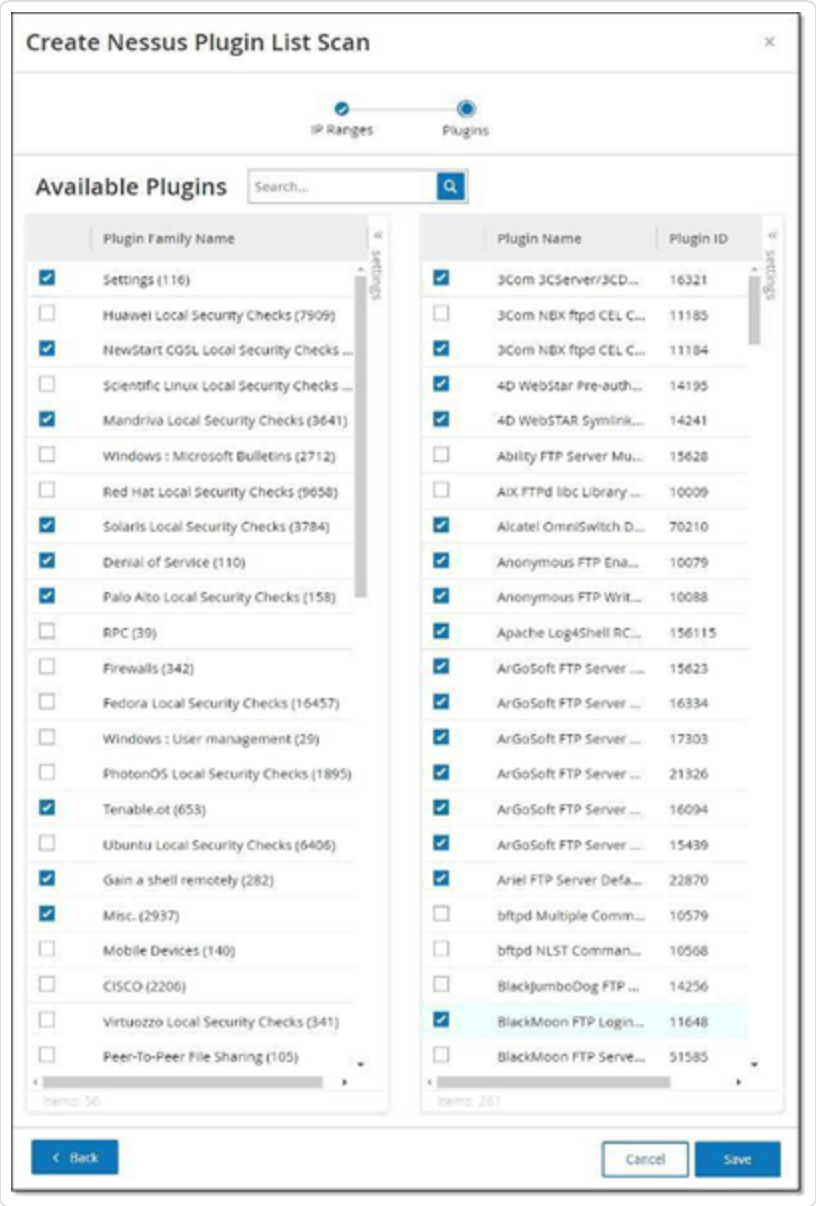
3. 右上の **[スキャンを作成]** をクリックします。

   [Nessus プラグインリストスキャンの作成] パネルが表示されます。



4. **[名前]** ボックスに Nessus スキャンの名前を入力します。
5. **[IP 範囲]** ボックスに、IP または CIDR の範囲を入力します。
6. **[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。



注意: OT Security はそのデバイスに固有のプラグインのみをリスト表示します。新しいプラグインを受け取るには、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。

7. **[プラグインファミリー名]** 列で、必要なプラグインファミリーを選択してスキャンに含めます。必要に応じて、右側の列で個々のプラグインのチェックボックスをオフにします。

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

8. **[保存]** をクリックします。

   新しい Nessus スキャンが **[Nessus スキャン]** ページに表示されます。

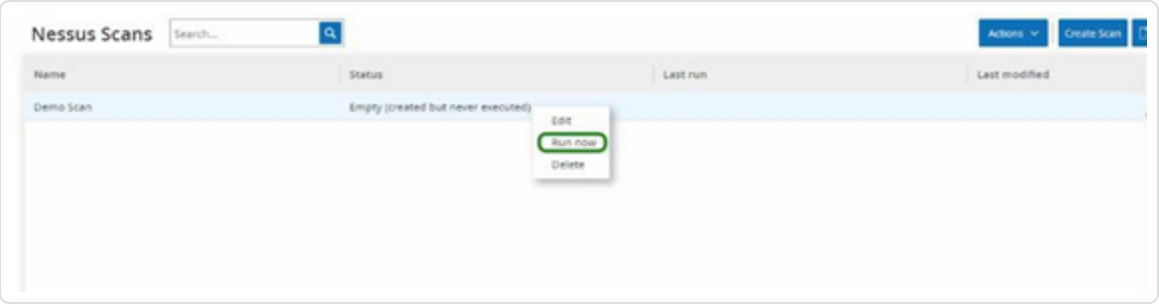
   > **注意**: 既存の Tenable Nessus スキャンを編集または削除するには、そのスキャンを右クリックし、**[編集]** または **[削除]** を選択します。

Nessus プラグインスキャンの実行

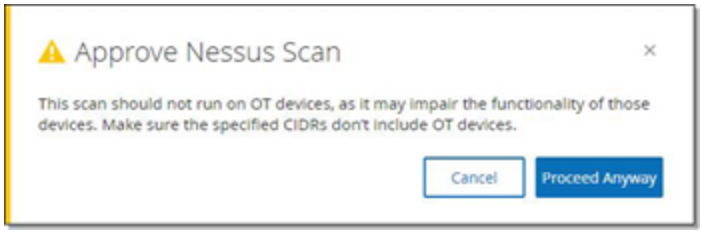
Nessus プラグインスキャンの実行手順

1. **[Nessus スキャン]** ページで、次のいずれかを実行します。

   - スキャンを右クリックし、**[今すぐ実行]** を選択します。
   - 実行するスキャンを選択し、**[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、**[このまま続行する]** をクリックします。

   ダイアログが閉じ、OT Security がスキャンを保存します。

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. **[このまま続行する]** をクリックします。

   OT Security がスキャンを実行します。現在のステータスに応じて、スキャンを一時停止/再開、停止、または強制終了できます。

ネットワーク

OT Security はネットワーク内のすべてのアクティビティを監視し、次のページにデータを表示します。

- **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。パケットキャプチャを参照してください。
- **対話** – ネットワーク内で検出されたすべての対話のリストを、発生した時刻や関連する資産などの詳細とともに表示します。対話を参照してください。

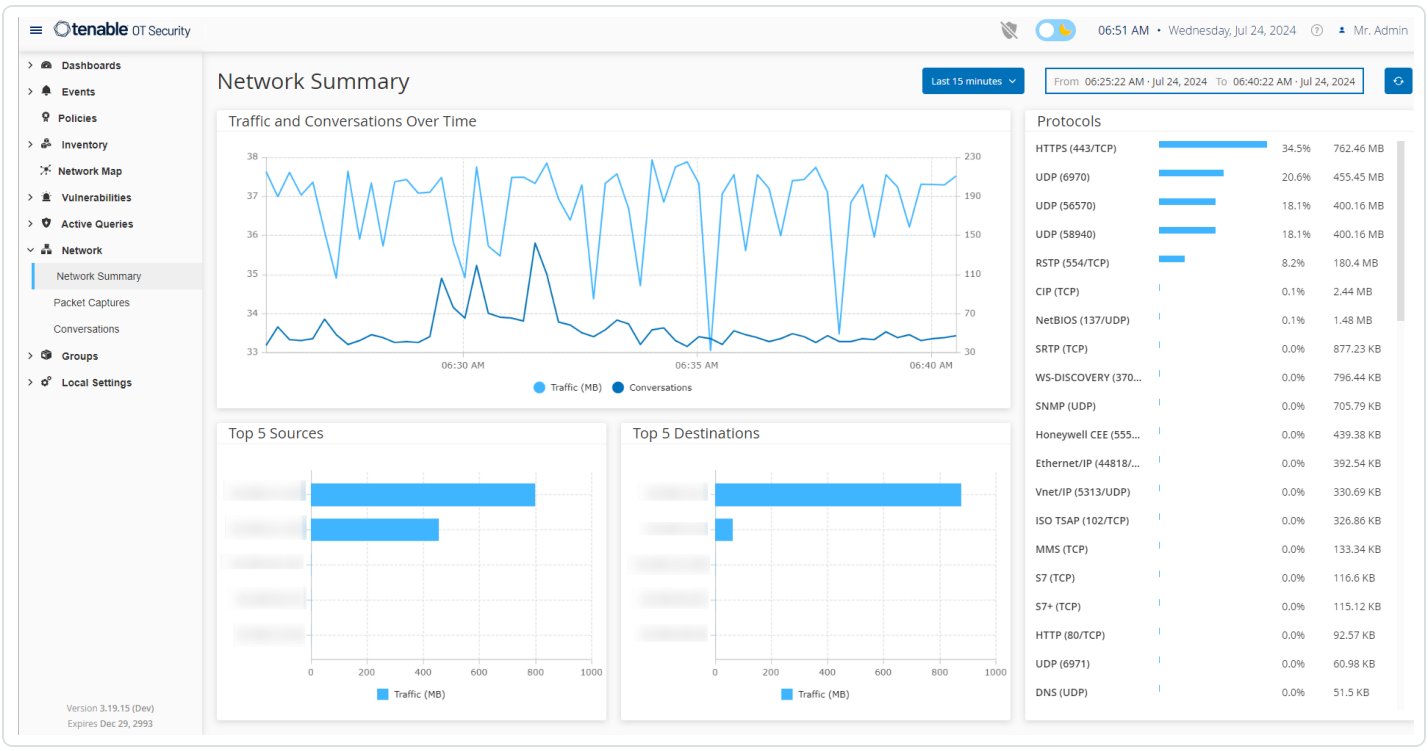
[ネットワーク] ページにアクセスする方法

1. 左側のナビゲーションペインで、**[ネットワーク]** を選択します。

   [ネットワーク概要] ページが表示されます。

ネットワーク概要

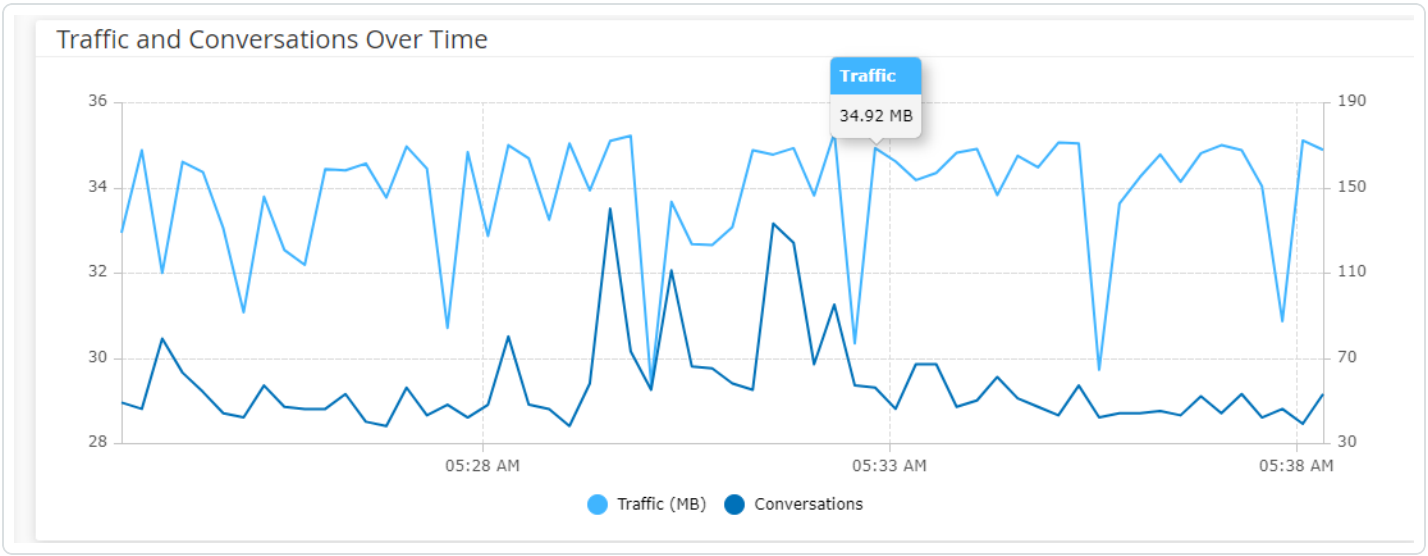
[ネットワーク概要] ページには、ネットワークアクティビティをまとめたビジュアルグラフが表示されます。特定の時間枠のデータを表示できます。



次のウィジェットを操作して、追加の詳細を表示します。

トラフィックと会話の経時変化

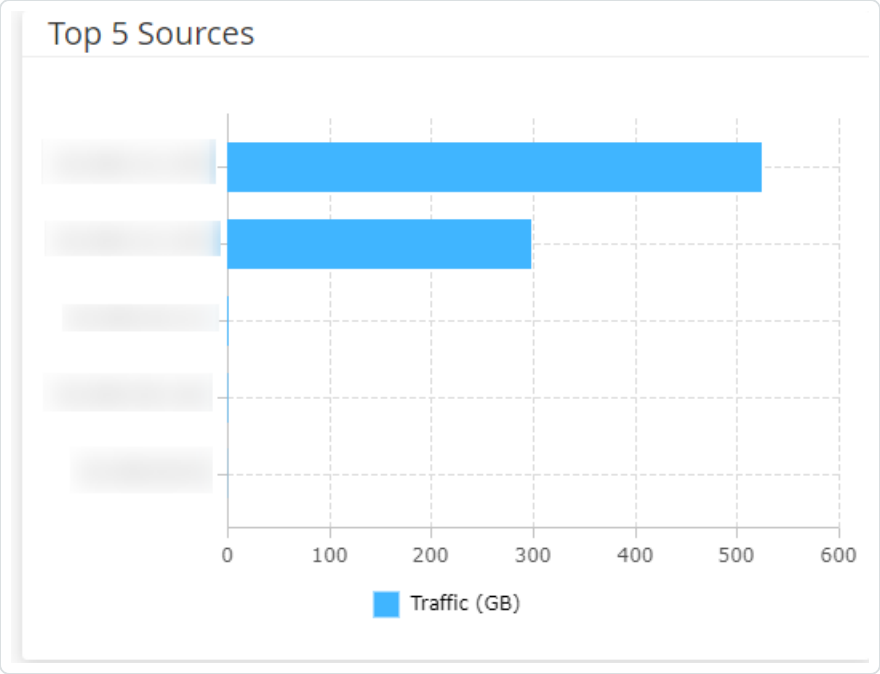
折れ線グラフが、ネットワーク内のトラフィックの量 (KB/MB/GB で測定) と対話の数の推移を表示します。凡例キーがグラフの上部に表示されます。グラフ上のポイントにカーソルを合わせると、その時間セグメント中に発生したトラフィックと対話に関する特定のデータが表示されます。



注意: 時間セグメントの長さは、グラフに表示される時間スケールに従って調整されます。たとえば、15 分のタイムフレームでは 1 分ごとのデータが個別に表示され、30 日のタイムフレームでは 6 時間セグメントのデータが表示されます。

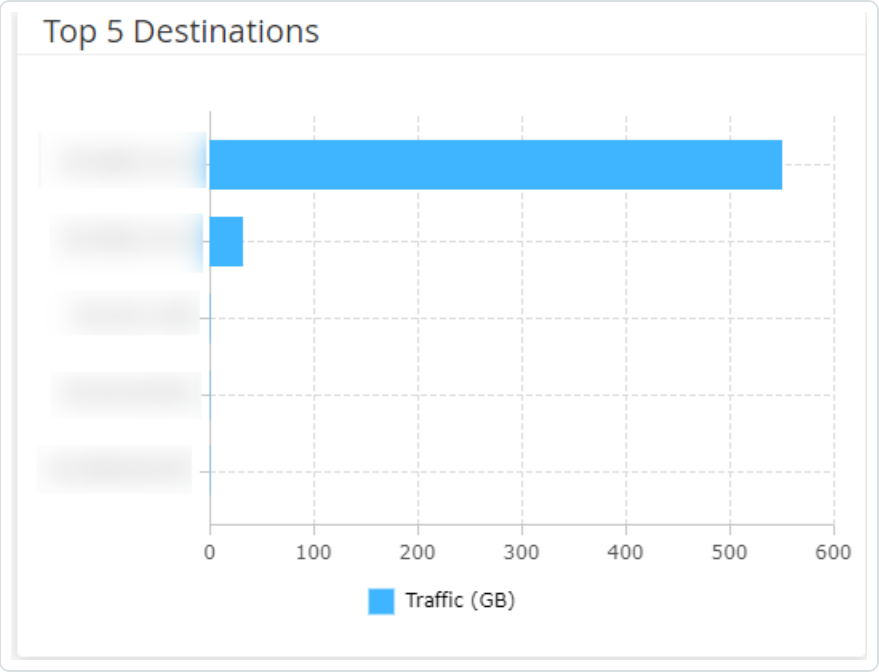
上位 5 件のソース

[上位 5 件のソース] ウィジェットには、特定の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対話数とトラフィック量が表示されます。ソース資産は IP アドレスで識別することができます。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対話の数とトラフィックの量が表示されます。



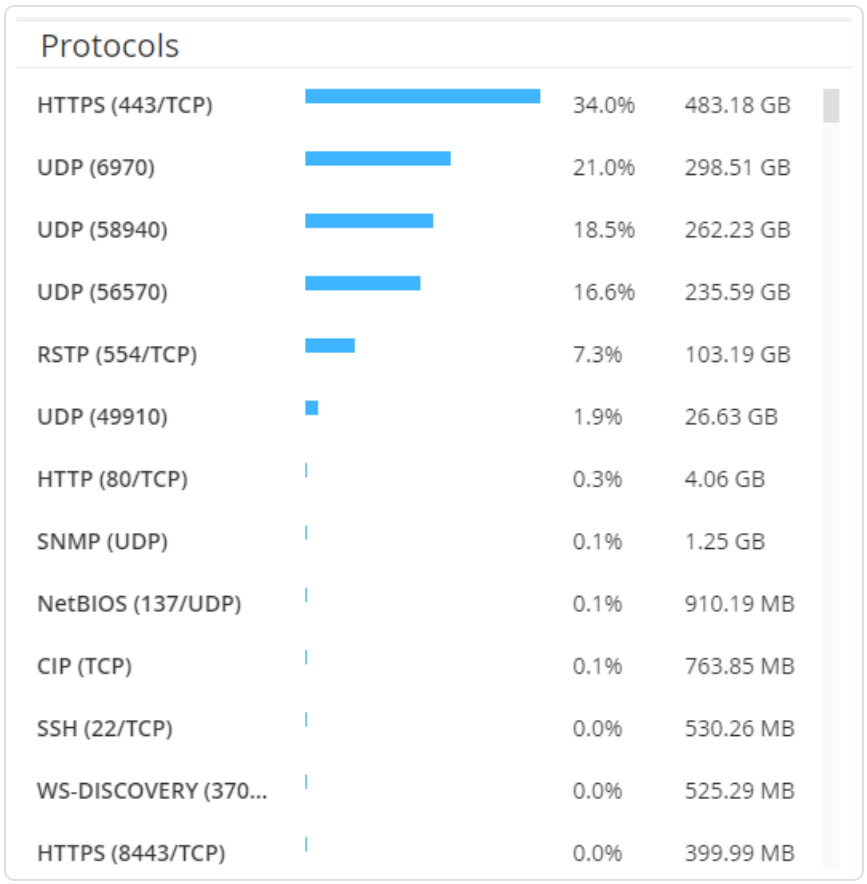
上位 5 件のデスティネーション

[上位 5 件のデスティネーション] ウィジェットには、特定の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対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 アドレスで識別することができます。棒グラフにカーソルを合わせると、その資産が受信した対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] ウィジェットには、特定の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)の順に表示されます。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(フルの長さの棒は使用率の最も高いプロトコルを表し、それより短い長さの棒は使用率の最も高いプロトコルに対する使用率の程度を示します)。
- 使用率。
- 通信の総量。

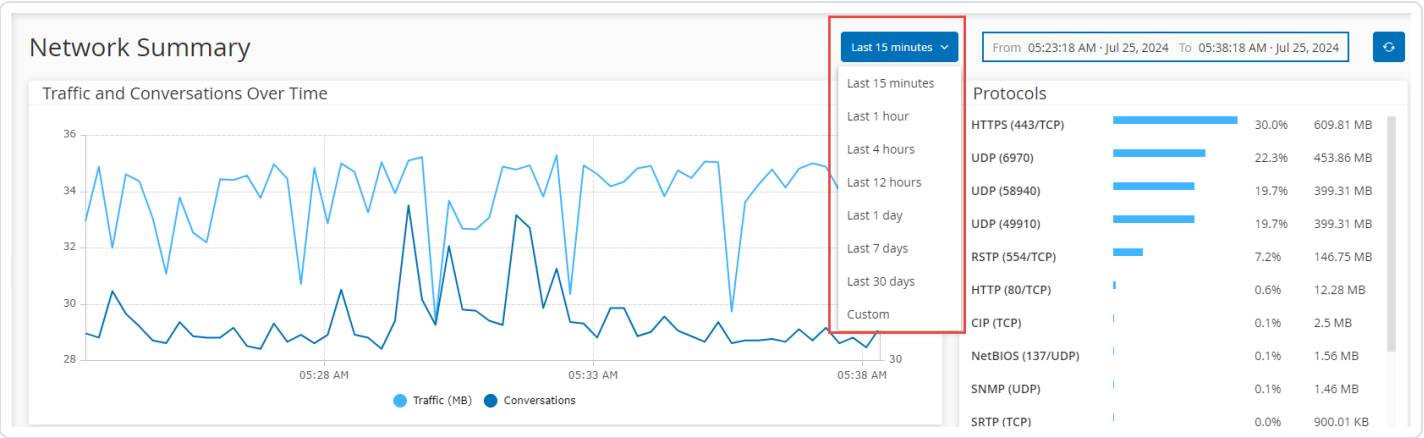
タイムフレームの設定

[ネットワーク概要] ページに表示されるすべてのデータは、特定の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。ヘッダーバーには、現在のデータ表示の時間範囲が示されています。デフォルトのタイムフレームは、**[過去 15 分]** です。ヘッダーバーには、タイムフレームの開始時刻と終了時刻も表示されます。

タイムフレームを設定する方法

ヘッダーバーで、タイムフレームのドロップダウンをクリックします。デフォルトは **[過去 15 分]** です。

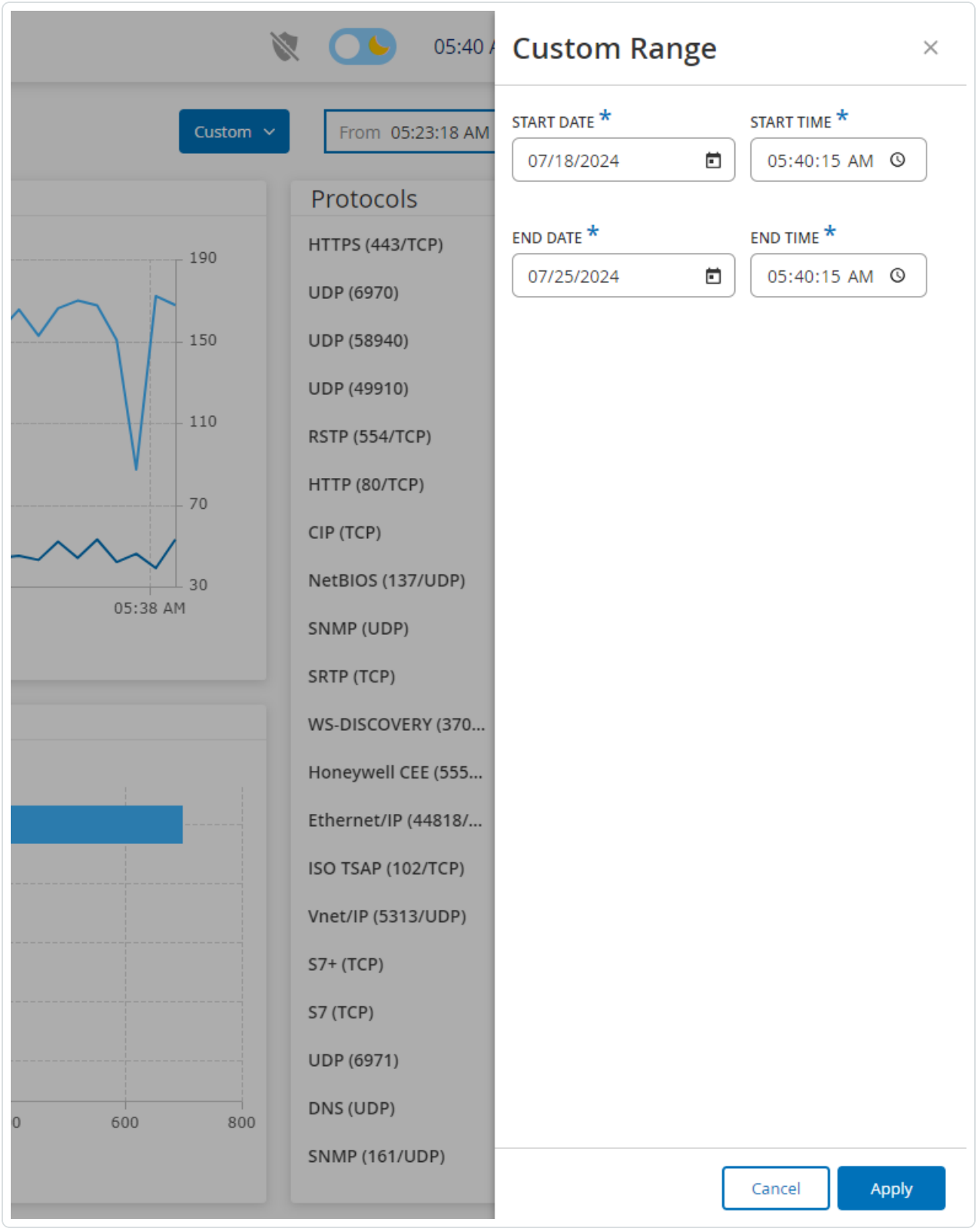
ドロップダウンボックスに利用可能なオプションがリストされます。



次のいずれかの方法で時間範囲を選択します。

- 必要な範囲をクリックして、現在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 日間です。
- カスタムの時間範囲を設定する方法
- **[カスタム]** をクリックします。

  [カスタムの範囲] ウィンドウが表示されます。



- **[開始日]**、**[開始時刻]**、**[終了日]**、**[終了時刻]**を入力します。

- **[適用]**をクリックします。

  タイムフレームを設定すると、ヘッダーバーのタイムフレーム選択の横に開始日時と終了日時が表示されます。OT Security によりページが更新され、選択したタイムフレーム内のデータが表示されます。

パケットキャプチャ

OT Security は、ネットワーク内の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 (パケットキャプチャ) ファイルとして保存されます。これは、ネットワークプロトコル分析ツール (Wireshark など) を使用して分析することができます。これにより、重大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が 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] ページに、システム内のすべての PCAP ファイルが表示されます。**[完了]** セクションには、ダウンロード可能なすべて完了ファイルがリストされます。**[進行中]** セクションには、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、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オプションもあります。

パケットキャプチャテーブルでは、列の表示/非表示、並べ替え、リストのフィルタリング、キーワードの検索ができます。テーブルのカスタマイズについては、表のカスタマイズを参照してください。

> **注意**: **[イベント]** ページ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

[パケットキャプチャ] リストには次の詳細が表示されます。

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: **[完了]** または **[進行中]**。
センサー	パケットをキャプチャした OT Security センサー。OT Security 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、値はローカルとして表示されます。
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

開始時刻や終了時刻のパラメーターを入力することにより、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]** > **[パケットキャプチャ]** に移動します。
2. 開始時刻でフィルタリングするには、**[開始時刻]** にカーソルを合わせ、▽ アイコンをクリックします。

   ドロップダウンメニューが表示されます。

   1. フィルターを設定する方法

      a. ドロップダウンメニューから、必要なフィルター (**[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]**) を選択します。

      b. **[次の時点より前に開始]** または **[次の時点より後に開始]** を選択した場合、**[日付]** および **[時刻]** ボックスのあるウィンドウが開き、そこで日付と時刻を選択できます。

      c. **[適用]** をクリックします。
3. 終了時刻でフィルタリングするには、**[終了時刻]** にカーソルを合わせ、▽ アイコンをクリックします。

   ドロップダウンメニューが表示されます。

1. フィルターを設定する方法

    a. 必要なフィルターを **[日時指定なし](デフォルト)**、**[次の時点より前に終了]**、または **[次の時点より後に終了]** から選択します。

    b. **[次の時点より前に終了]** または **[次の時点より後に終了]** を選択した場合、**[日付]** および **[時刻]** ボックスのあるウィンドウが開き、そこで日付と時刻を選択できます。

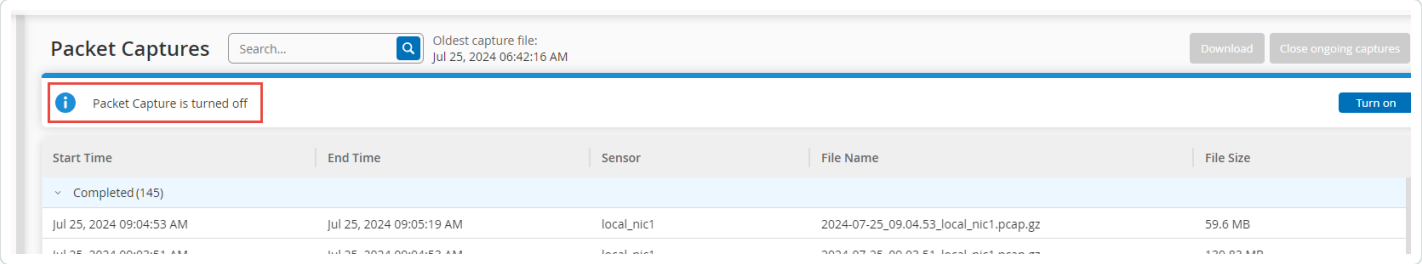
    c. **[適用]** をクリックします。

    OT Security によりフィルターが適用され、指定したタイムフレーム内で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オンまたはオフ

パケットキャプチャ機能は、**[ローカル設定]** > **[システム設定]** > **[デバイス]** からオンまたはオフにできます。

パケットキャプチャ機能がオフになると、オフになったことを通知するメッセージが **[パケットキャプチャ]** 画面に表示されます。



重要: **[ネットワーク]** > **[パケットキャプチャ]** からパケットキャプチャをオンにできますが、オフにはできません。

パケットキャプチャをオンにする方法

1. **[ネットワーク]** > **[パケットキャプチャ]** に移動します。
2. **ヘッダーバー**で、**[オンにする]** をクリックします。

    OT Security によりパケットキャプチャが開始されす。

ファイルのダウンロード

完了した PCAP ファイルをローカルマシンにダウンロードできます。その後、Wireshark などのネットワークプロトコル分析ツール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、新しいファイルでの情報キャプチャを開始することができます。

完了したファイルのダウンロード手順

1. **[ネットワーク]** > **[パケットキャプチャ]** に移動します。
2. パケットキャプチャリストから必要な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。

   OT Security により zip 形式の 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方法

1. **[ネットワーク]** > **[パケットキャプチャ]** に移動します。
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。

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

対話

対話とは、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 台のサーバー間のインタラクションです。**[対話]** ページには対話に関する詳細情報を含む、現在および過去の対話のリストが表示されます。

[対話] ページから、次のアクションを実行できます。

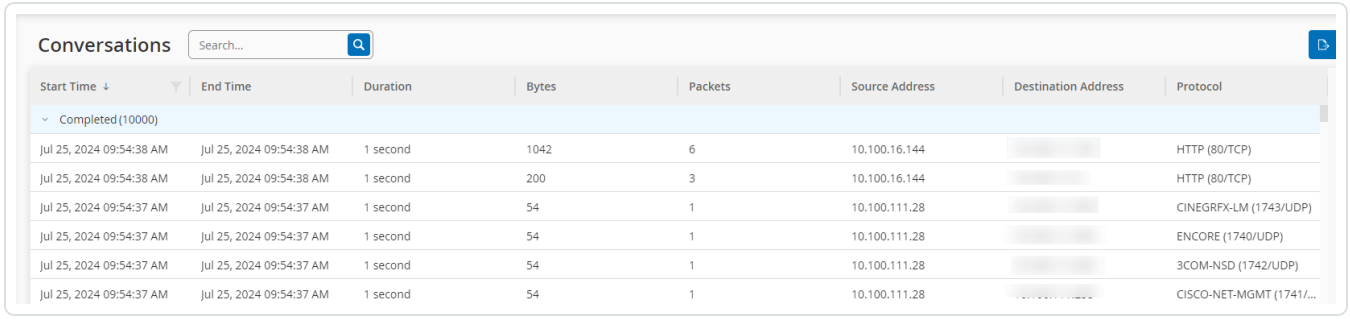
- **検索** – **[検索]** ボックスを使用し、識別情報を入力することで特定の対話を検索します。
- **エクスポート** –  [エクスポート] ボタンを使用して、**[対話]** タブにあるすべてのデータを、ローカルマシンの `.csv` ファイルにエクスポートします。

  注意: [対話] テーブルには、直近の 10,000 件のネットワーク対話が表示されます。

[対話] ページにアクセスする方法

1. **[ネットワーク]** > **[対話]** に移動します。

   [対話] ページが表示されます。

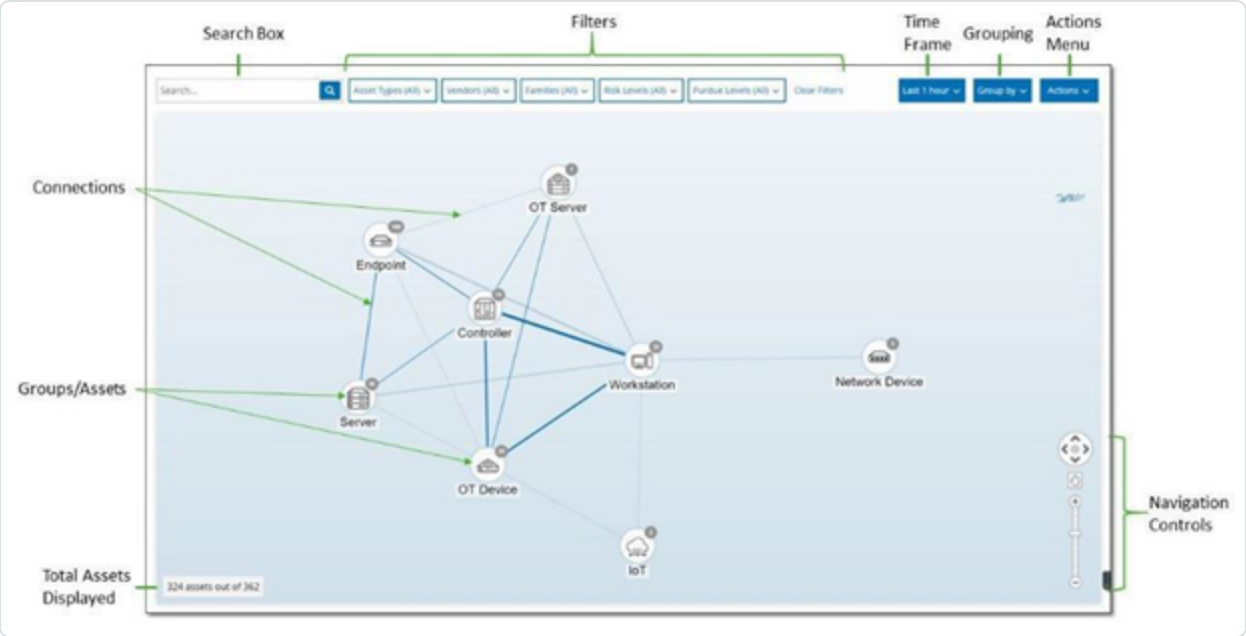


[対話]ページには、次の詳細が表示されます。

パラメーター	説明
開始時刻	対話の開始時刻。
終了時刻	対話の終了時刻。進行中の会話は、**[進行中]**と表示されます。
期間	対話の継続時間。
パケット	対話中に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アドレス。
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、OT Security のネットワーク検出機能によって検出された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(ファームウェアのダウンロードまたはアップロード、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設定変更など)に焦点を合わせて、運用ネットワークでの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。[ネットワークマップ]には、資産が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されます。



[ネットワークマップ] には、指定したタイムフレーム内に Tenable により検出されたすべての資産と接続が表示されます。

ネットワークマップページには次の詳細が表示されます。

- **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。ネットワークマップに検索結果が表示され、検索テキストに一致するすべてのグループが強調表示されます。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、指定し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 30 日]** に設定されています。タイムフレームのドロップダウンボックスで、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ために使用されるカテゴリを指定します。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表示したまま、開かれているその他の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** – マップ上のアイコンは各資産グループを表し、各資産タイプがアイコンによって示されます。各資産タイプについては資産タイプで説明しています。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。

  注意: 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、拡大および縮小して表示を調整したり、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ページには、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。また、複数のグループを同時にドリルダウンできます。OT Security 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、ドリルダウンすることで、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、選択したグループ化のドリルダウンオプションです。

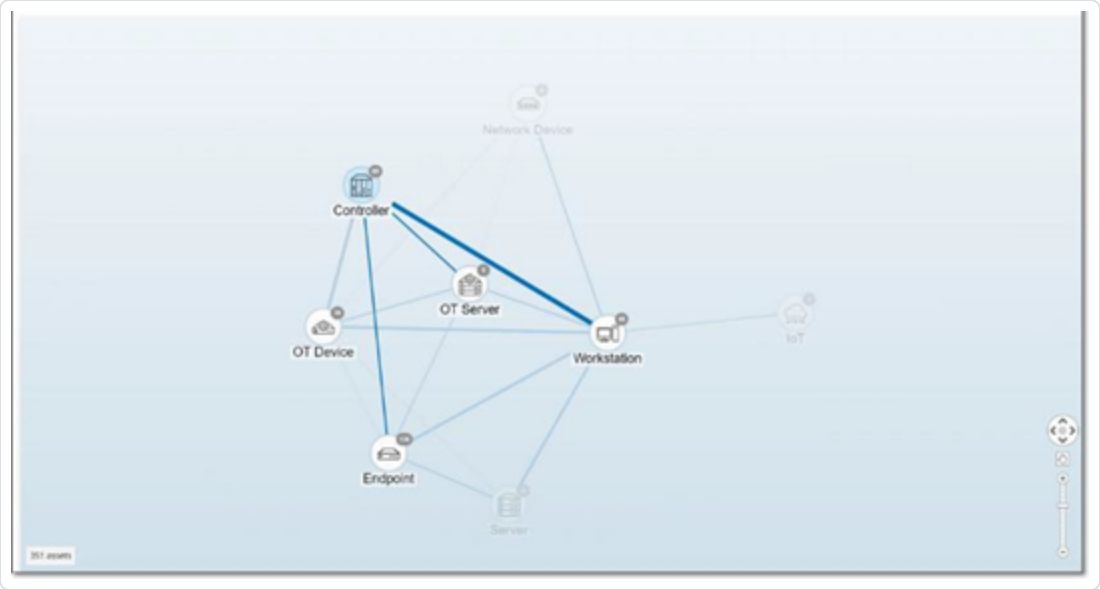
マップ表示が**[資産タイプ]**(デフォルト)でグループ化されている場合、ドリルダウン階層は次のようになります。**[資産タイプ]** > **[ベンダー]** > **[ファミリー]** > **[個別資産]**。

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]**。各レベルは、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。

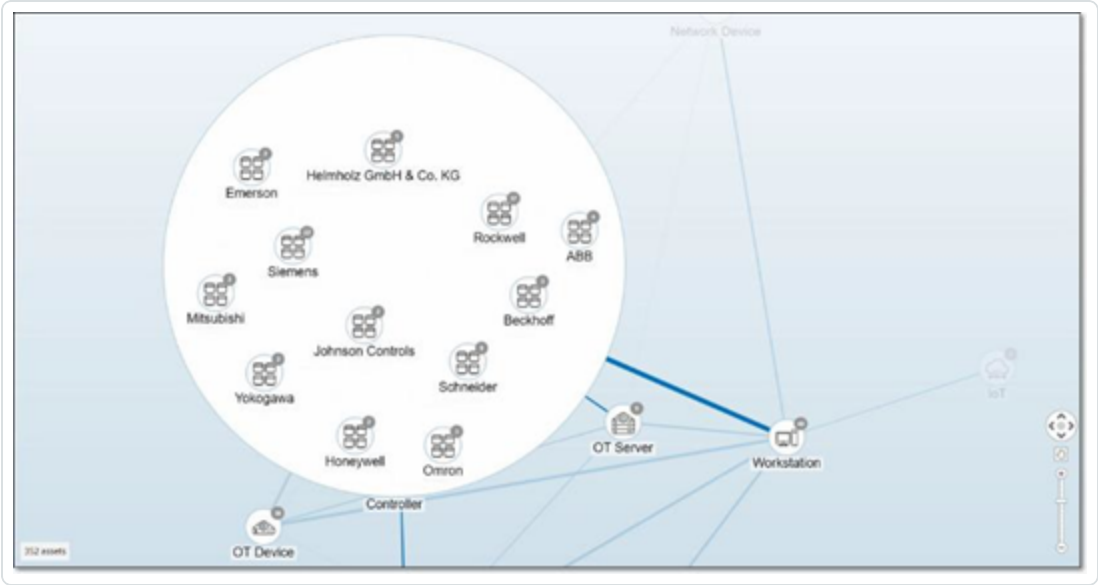
資産タイプグループにドリルダウンする手順

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。

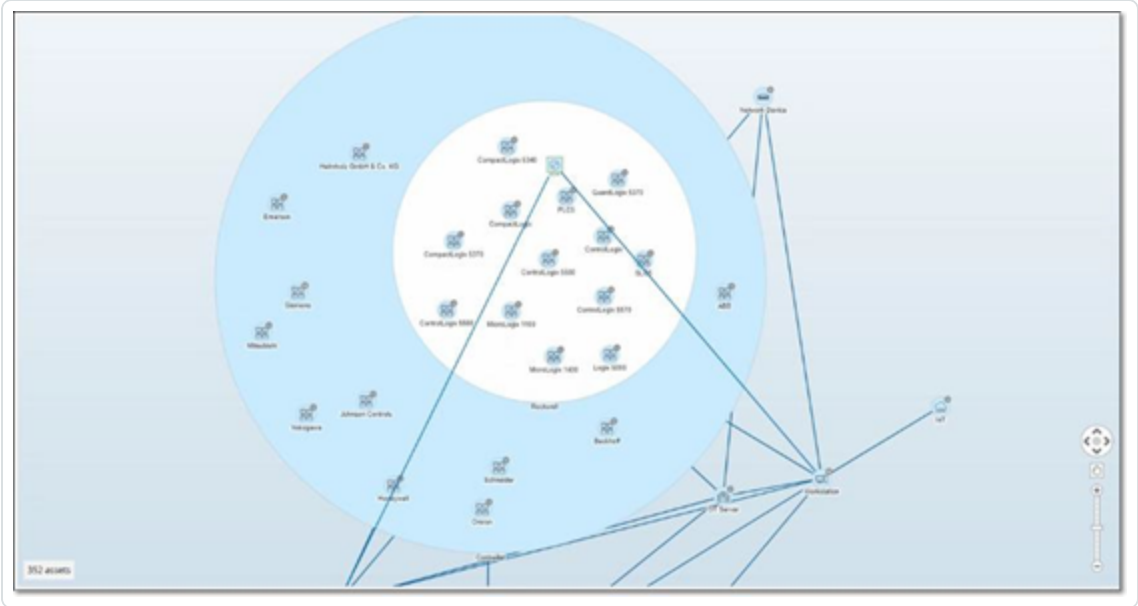


2. ドリルダウンするグループアイコン(例:コントローラー)をダブルクリックします。

   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。

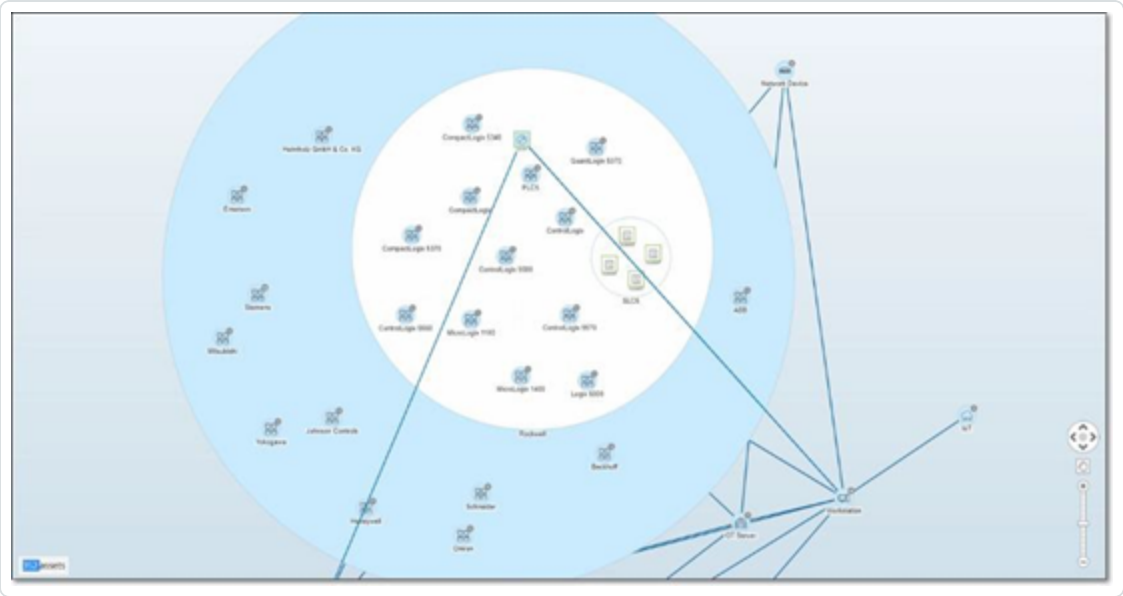


3. さらにドリルダウンするには、ベンダーグループ (例 : Rockwell) をクリックします。



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。

   そのグループ内の個々の資産が表示されます。



5. 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。[インベントリ]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。

   最上位レベルのグループが再び表示されます。

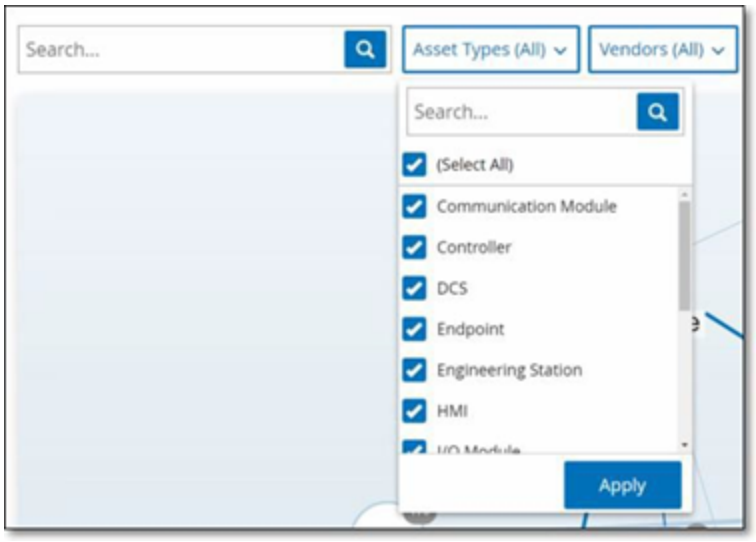
すべてのグループ化の削除手順

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。

   マップには、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. 目的のフィルターカテゴリをクリックします。
2. 表示または非表示にする各要素のチェックボックスを選択または選択解除します。

   注意: デフォルトでは、フィルターにはすべての要素が含まれています。

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、**[資産詳細]** 画面に移動し、資産に関するより詳細な情報を確認できます。

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対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やり取りがなかった資産により、各対話について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。

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対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. 右上で**[アクション]**>**[ベースラインとして設定]**を選択します。

   OT Securityにより新しいネットワークベースラインが設定され、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

OT Security 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てパブリックドメインで一般公開されると、Tenable Research スタッフは Tenable Nessus がその脆弱性を検出できるようにプログラムを作成します。

これらのプログラムはプラグインという名前で、Tenable Nessus Attack Scripting Language (NASL) と呼ばれる Tenable 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 (古い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、一般的な修正処置のセットに加えて、セキュリティ問題が存在しないか検査するアルゴリズムが含まれています。

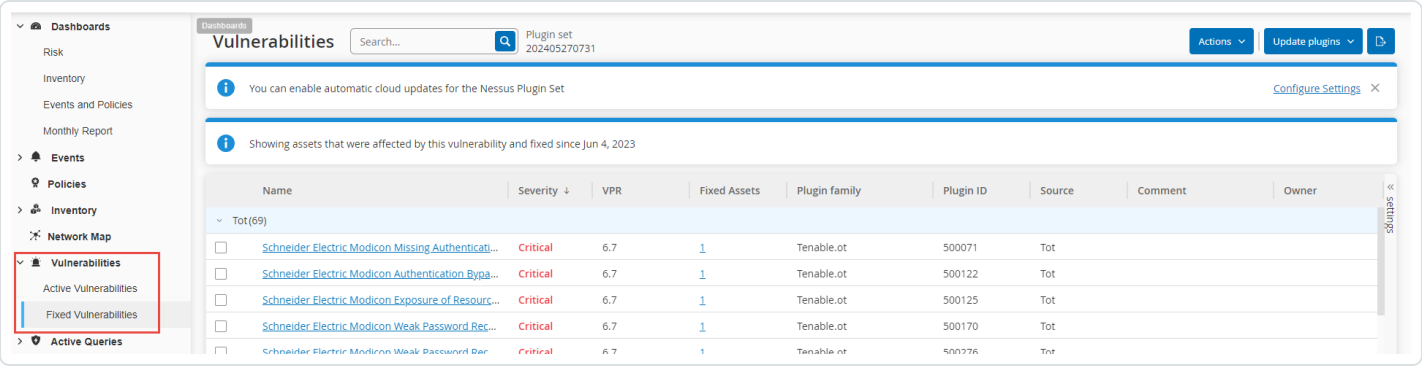
プラグインセットのアップデートについては、環境設定を参照してください。

脆弱性

[脆弱性] ページには、ネットワークと資産に影響がある、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、管理コンソールのユーザーインターフェース要素を参照してください。

左側のナビゲーションバーにある **[アクティブな脆弱性]** と **[修正された脆弱性]** のオプションを使用すると、未解決の脆弱性と修正済みの脆弱性をそれぞれ表示できます。



注意: OT Security では、修正された脆弱性は、期限切れになるまで 1 年間保持されます。

[脆弱性]ページには、次の詳細が表示されます。

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]、[重大]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される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される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

プラグインの詳細を表示する手順

1. 詳細を表示する脆弱性の行で、脆弱性の名前をクリックします。

   [脆弱性の詳細]ウィンドウが表示されます。

[脆弱性の詳細]ウィンドウには、次の詳細が表示されます。

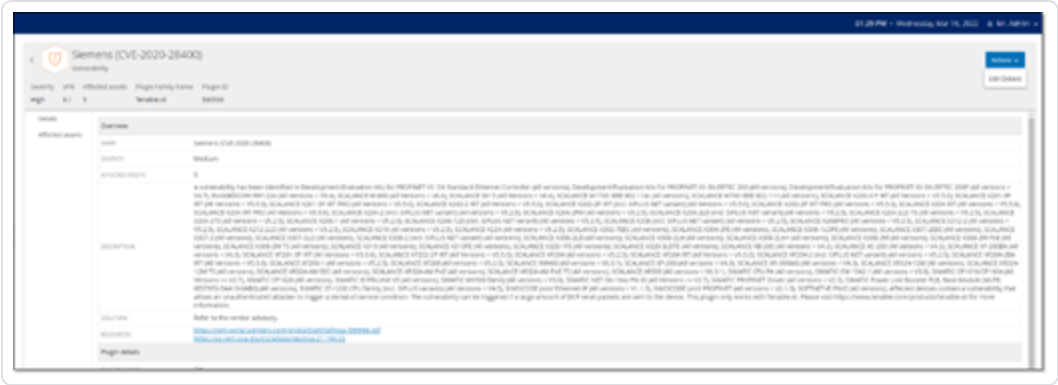
- **ヘッダーバー** – 指定された脆弱性に関する基本情報が表示されます。脆弱性の詳細を編集するには、**[アクション]**メニューから**[詳細の編集]**を選択します。脆弱性詳細の編集を参照してください。
- **[詳細]タブ** – 脆弱性の完全な説明を表示し、関連するリソースへのリンクを提供します。
- **[影響を受ける資産]タブ** – 特定の脆弱性の影響を受けるすべての資産のリストを表示します。各リストには、資産に関する詳細情報、およびその資産の[資産詳細]ウィンドウを表示するためのリンクが含まれています。

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]**メニューをクリックします。

   [アクション]メニューが表示されます。



2. **[詳細の編集]** をクリックします。

   [脆弱性詳細の編集] パネルが表示されます。

3. **[コメント]** ボックスに、脆弱性に関するコメントを入力します。
4. **[所有者]** ボックスに、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。

プラグインの出力表示

資産のプラグイン出力は、資産について特定のプラグインが報告された理由に関する文脈または説明を提供します。

脆弱性ページからプラグイン出力の詳細を表示する手順

1. **[脆弱性]** に移動します。

   脆弱性 ページが表示されます。

2. 脆弱性のリストで詳細を表示する脆弱性を選択し、次のいずれかを行います。

   - 脆弱性のリンクをクリックします。
   - 脆弱性を右クリックし、**[表示]** を選択します。
   - **[アクション]** ドロップダウンボックスから、**[表示]** を選択します。

   脆弱性の詳細ページに **[プラグイン出力]** パネルが表示され、次の情報が表示されます。

   - ヒット日
   - ソース
   - ポート
   - プラグイン出力

   > **注意**: すべてのプラグインでプラグイン出力が利用できるわけではありません。

インベントリページからプラグイン出力の詳細を表示する手順

1. **[インベントリ]** > **[すべての資産]** に移動します。

   インベントリ ページが表示されます。

2. 資産のリストで詳細を表示する資産を選択し、次のいずれかを行います。

   - 資産のリンクをクリックします。
   - 資産を右クリックし、**[表示]** を選択します。
   - 資産の横にあるチェックボックスを選択し、**[アクション]** ドロップダウンボックスから **[表示]** を選択します。

   資産詳細ページが表示されます。

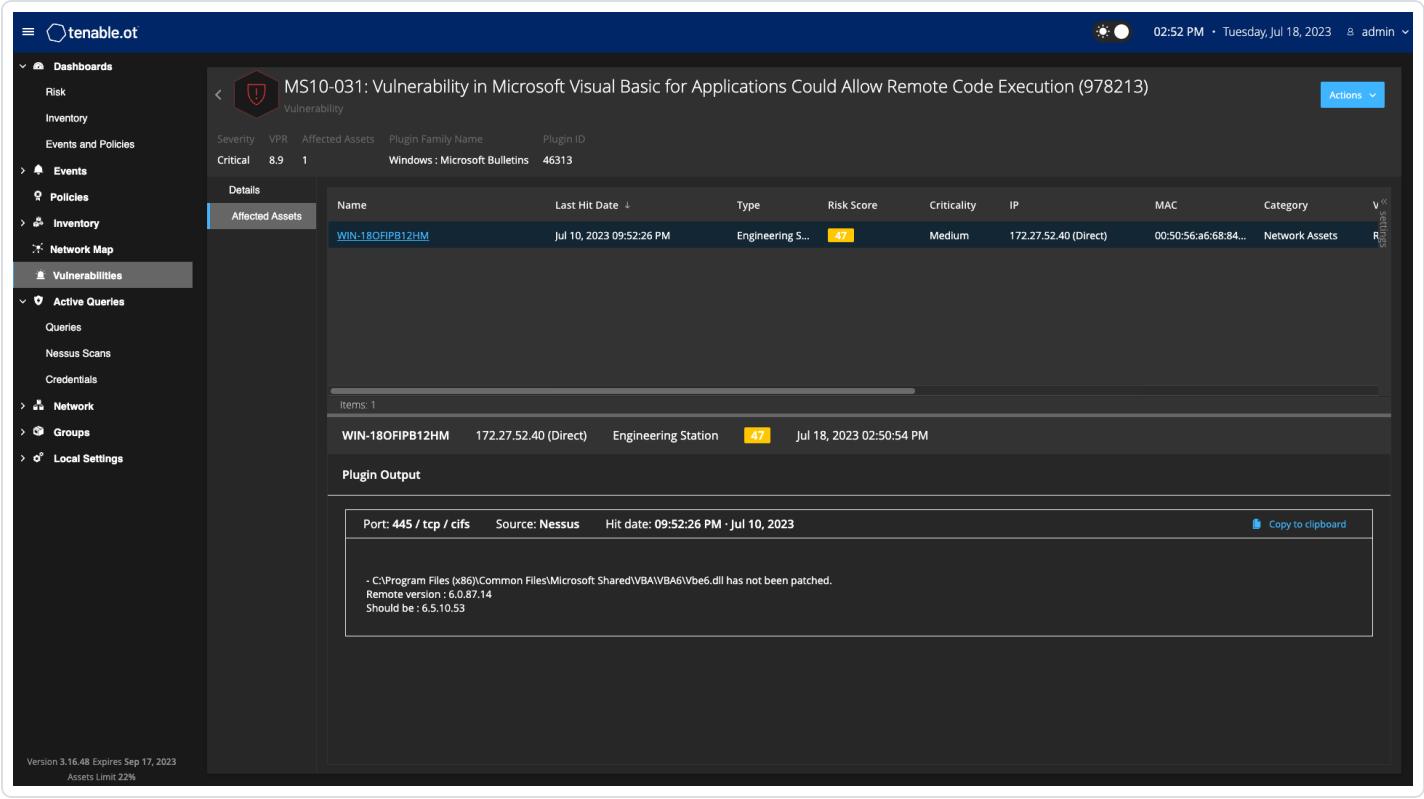
3. **[脆弱性]** タブをクリックします。

   脆弱性のリストが表示され、**[プラグイン出力]** パネルに次の情報が表示されます。

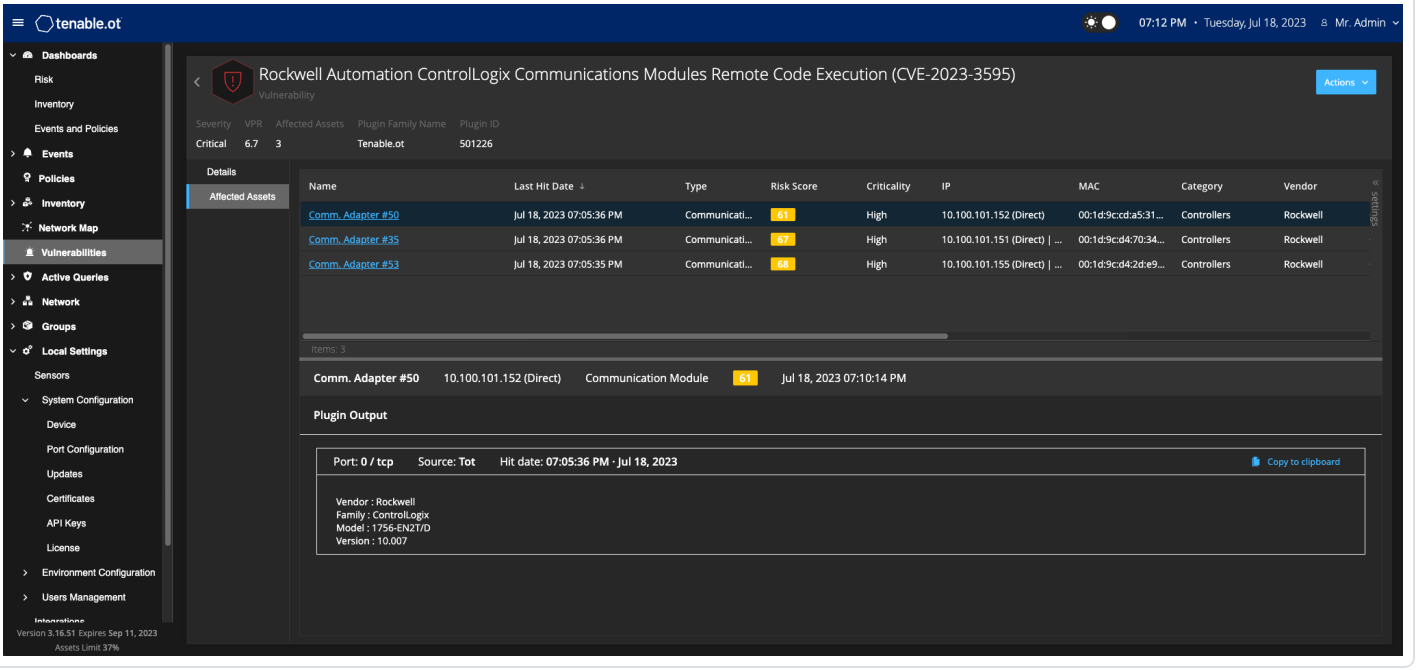
   - ヒット日
   - ソース
   - ポート
   - プラグイン出力

> **注意**: すべてのプラグインでプラグイン出力が利用できるわけではありません。

Tenable Nessus プラグインのプラグイン出力の例



OT Security プラグインのプラグイン出力の例


tenable.ot
07:12 PM • Tuesday, Jul 18, 2023
Mr. Admin
Dashboards
Risk
Inventory
Events and Policies
Events
Policies
Inventory
Network Map
Vulnerabilities
Active Queries
Network
Groups
Local Settings
Sensors
System Configuration
Device
Port Configuration
Updates
Certificates
API Keys
License
Environment Configuration
Users Management
Version 3.16.51 Expires Sep 11, 2023
Assets Limit 37%
Rockwell Automation ControlLogix Communications Modules Remote Code Execution (CVE-2023-3595)
Vulnerability
Actions
Severity VPR Affected Assets Plugin Family Name Plugin ID
Critical 6.7 3 Tenable.ot 501226
Details
Affected Assets
Name Last Hit Date Type Risk Score Criticality IP MAC Category Vendor
Comm. Adapter #50 Jul 18, 2023 07:05:36 PM Communicati... 61 High 10.100.101.152 (Direct) 00:1d:9c:cd:a5:31... Controllers Rockwell
Comm. Adapter #35 Jul 18, 2023 07:05:36 PM Communicati... 67 High 10.100.101.151 (Direct) | ... 00:1d:9c:d4:70:34... Controllers Rockwell
Comm. Adapter #53 Jul 18, 2023 07:05:35 PM Communicati... 68 High 10.100.101.155 (Direct) | ... 00:1d:9c:d4:2d:e9... Controllers Rockwell
Items: 3
Comm. Adapter #50 10.100.101.152 (Direct) Communication Module 61 Jul 18, 2023 07:10:14 PM
Plugin Output
Port: 0 / tcp Source: Tot Hit date: 07:05:36 PM · Jul 18, 2023
Copy to clipboard
Vendor : Rockwell
Family : ControlLogix
Model : 1756-EN2T/D
Version : 10.007

ローカル設定

OT Security の **[ローカル設定]** セクションには、OT Security の設定ページのほとんどが含まれています。**[ローカル設定]** から以下のページにアクセスできます。

アクティブクエリ – クエリ機能をアクティブ化または非アクティブ化し、その頻度と設定を調整します。アクティブクエリをご覧ください。

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設定します。センサーを参照してください。

システム設定

- **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。たとえば、システム時刻、自動ログアウト (非アクティブタイムアウト) などです。

  > **注意**: DNS サーバーは、Tenable Core で設定できます。詳細については、Tenable Core + Tenable OT Security ユーザーガイドの「静的 IP アドレスを手動で設定する」を参照してください。

- **ポート設定** - デバイスのポートがどのように設定されているかを表示します。ポート設定の詳細については、デバイスを参照してください。
- **アップデート** – プラグインのアップデートを、クラウドまたはオフラインで、自動的に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。システム設定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 OT Security 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。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。

環境設定

- **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。監視対象ネットワークを参照してください。
  - **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。手動による資産の追加を参照してください。

    注意: Tenable Nessus Network Monitor に送信できる IP 範囲の最大数は 128 であるため、Tenable はこの制限を超えないことをお勧めしています。指定された IP 範囲に加えて、OT Security 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** – システムの非表示の資産のリストを表示します。これらは、資産リストから削除された資産です。インベントリを参照してください。このページ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** – イベントを監視するために、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 OT Security 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。ユーザーとロールを参照してください。

- **ユーザーグループ** – 管理者ユーザーは、ユーザーグループを表示、編集、追加、削除できます。ユーザーとロール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。ユーザーとロール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。OT Security 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 Security Center と Tenable Vulnerability Management) 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** – システムで設定されたサーバーを表示、作成、編集します。以下の 3 つに対応する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 E 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** – OT Security と FortiGate の統合により、OT Security 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することができます。
- **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** –3.18 以降、Tenable Core の **[バックアップ/復元]** ページを使用して、OT Security のバックアップと復元を行うことができます。詳細については、Application Data Backup and Restore (アプリケーションデータのバックアップと復元) を参照してください。CLI を使用して復元する場合は、CLI で行うバックアップの復元を参照してください。
  - **エクスポート設定** - OT Security プラットフォーム設定を .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 OT Security 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。
  - **設定のインポート** – .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 OT Security プラットフォーム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 OT Security 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** – OT Security プラットフォームを再起動します。これは、特定の設定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** – OT Security 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、OT Security 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:

  警告: この操作は元に戻せません。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のログを表示します。たとえば、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です。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。

センサー

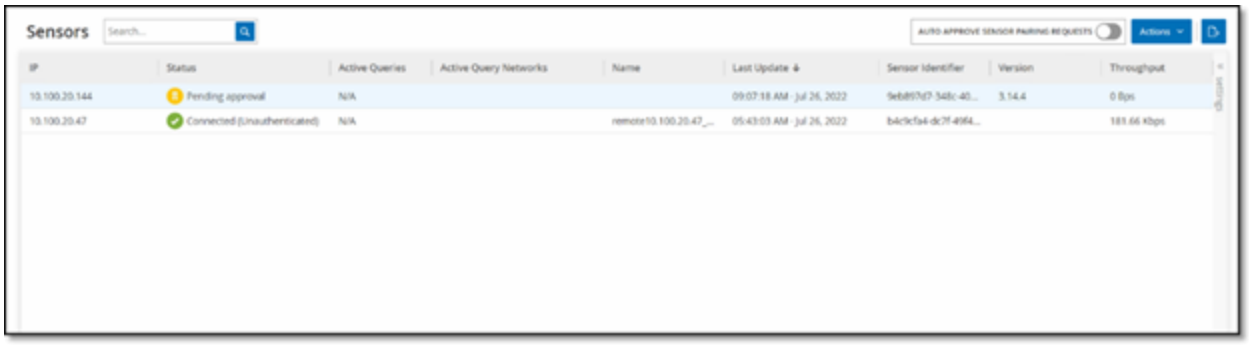
Tenable Core ユーザーインターフェースを使用してセンサーをペアリングすると、**[アクション]** メニューで**編集**機能、**一時停止**機能、**削除**機能を使用して、新しいペアリングを承認したり、センサーを表示および管理したりすることができます。**[センサーのペアリングリクエストの自動承認]** トグルを使用して、センサーペアリングリクエストの自動承認を有効にすることもできます。

注意: 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。

注意: ICP とペアリングできるセンサーの数に制限はありませんが、アプライアンスごとに合計 SPAN (Switched Port Analyzer) トラフィック量に上限があります。たとえば、10 のセンサーそれぞれで 10 ~ 20 Mbps の速度で送信できますが、トラフィック全体で ICP の制限を超えてはなりません。詳細については、Tenable Core + OT Security ユーザーガイドの システム要件とライセンス要件を参照してください。

センサーの表示

[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。



[センサー] テーブルには、次の詳細が含まれています。

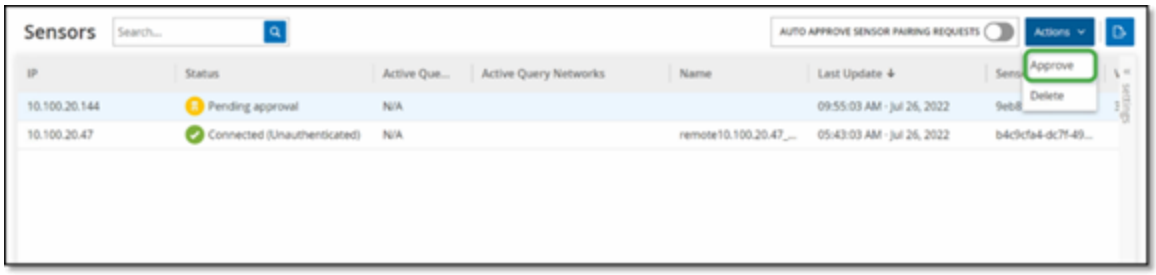
パラメーター	説明
IP	センサーの IPv4 アドレス。
ステータス	センサーのステータス: **接続済み**、**接続済み (未認証)**、**承認保留中**、**切断済み**、または一時停止。
アクティブクエリ	センサーのアクティブクエリ送信機能: **有効**、**無効**、**該当なし**。
アクティブクエリネットワーク	センサーが割り当てられているネットワークセグメント。
名前	システム内のセンサーの名前。
最終更新日	センサー情報が最後に更新された日時。
センサー識別子	UUID (Sensor Universal Unique Identifier)。インターネット上のオブジェ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)。

受信センサーのペアリングリクエストを手動で承認

[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]** > **[センサー]** 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、右クリックメニューから **[承認]** を選択します。



> **注意**: 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 **[削除]** を選択します。

アクティブクエリの設定

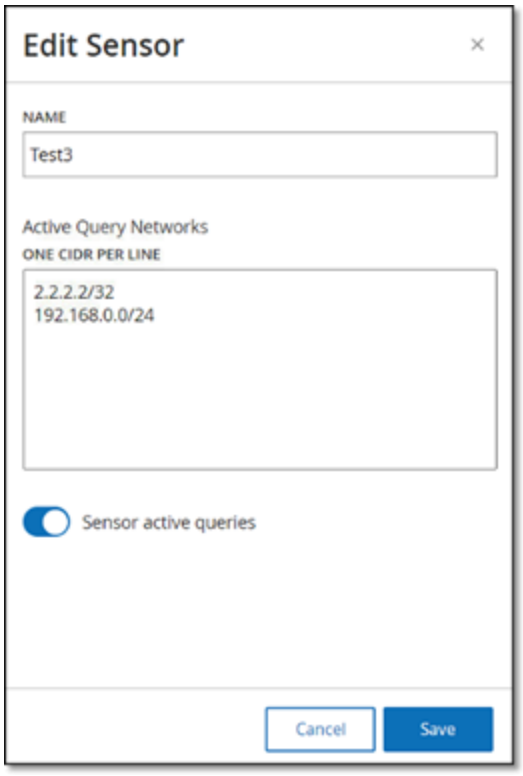
センサーが認証モードで接続されると、割り当てられているネットワークセグメントでアクティブクエリを実行するようにセンサーを設定できます。クエリするネットワークセグメントを指定する必要があります。

> **注意**: センサーは、この設定に関係なく、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設定手順

1. **[ローカル設定]** で、**[システム設定]** > **[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 **[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には、**[名前]** ボックス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]** ボックスで、CIDR 表記を使用して個々の行で各サブネットワークを追加し、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。

   注意: 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。このセンサーからアクセスできる 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 が別の方法でそれらのセグメントをクエリする機能に支障をきたす可能性があります。
6. **[センサーアクティブクエリ]** トグルをクリックして、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]** 列に、有効なセンサーが **[有効]** と表示されます。

センサーの更新

バージョン 3.16 以降の OT Security センサーは、対象を管理している ICP からソフトウェアとセキュリティの更新プログラムを受け取ります。認証とペアリングされたセンサーは、必要な OS とソフトウェアの更新を提供するときにこのサイトを使用します。センサーがソフトウェアの更新を受け取るために必要なのは、

OT Security に到達できることだけです。OT Security の一元化された **センサー**ページから、すべてのセンサーを更新できます。

センサーに更新が必要な場合には、以下の時点でアラートを受け取ります。

- 起動時
- センサーと ICP 間のペアリングの完了時
- 定期チェック
- **[更新の確認]** オプションの使用時

注意: リモートセンサーを更新するには、認証によってセンサーを OT Security とペアリングする必要があります。ペアリングの詳細については ICP とセンサーのペアリングを参照してください。

ICP を使用して認証済みセンサーをバージョン 3.16 以降に更新する手順

1. **[ローカル設定]** > **[センサー]** に移動します。

   センサーページが表示されます。

2. **[バージョン]** 列をチェックして、バージョンが最新かどうか、または更新が必要かどうかを確認します。
3. バージョンの更新が必要な場合は、次のいずれかを行います。

1 つのセンサーを更新する場合

- 目的のセンサーを右クリックし、**[更新]** を選択します。
- 目的のセンサーの横にあるチェックボックスを選択し、**[アクション]** メニューから **[更新]** を選択します。

複数のセンサーを更新する場合

- 更新が必要な 1 つ以上のセンサーを選択し、**[アクション]** メニューから **[更新]** を選択します。

選択したセンサーが OT Security により更新されます。

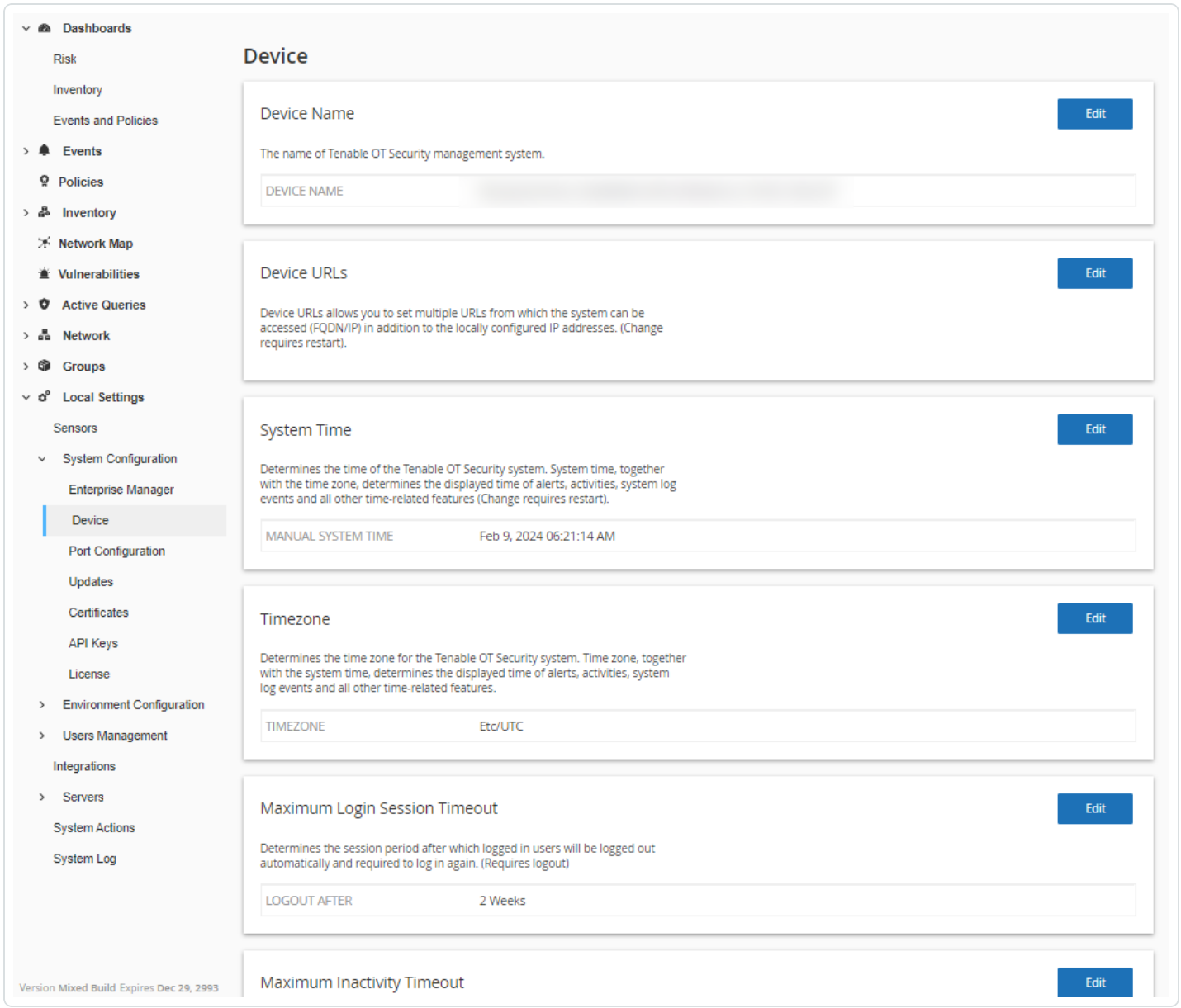
注意: 更新中は、センサーを利用できないことがあります。

システム設定

OT Security の**システム設定**ページでは、プラグインの更新を自動的に設定したり、プラグインの更新を手動で実行したりできるほか、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

デバイスページには、OT Security 設定に関する詳細情報が表示されます。このページで設定を確認して編集できます。



デバイス名

OT Security アプライアンスの一意の識別子です。

デバイス URL

システムにアクセスできる 1 つの URL (FQDN) を設定できます。

重要: 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ユーザーインターフェースにアクセスできなくなります。続行する前に、必ず解決されることを確認してください。

システム時刻

正しい時刻と日付が自動的に設定されますが、編集することもできます。

注意: 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。タイムゾーンを変更するには、**[編集]** をクリックします

ログインセッションタイムアウトの最大値

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セッション期間です。ログインセッションのタイムアウト期間を変更するには、**[編集]** をクリックします。利用できる期間のオプションは、2 週間、30 分、1 時間、4 時間、12 時間、1 日、1 週間、2 週間です。

非アクティビティタイムアウトの最大値

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非アクティビティ期間です。非アクティビティ期間を変更するには、**[編集]** をクリックします。

オープンポートの期限切れ期間

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、インベントリ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 OT Security 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 要求をアクティブ化するには、**[ping 要求]**トグルをクリックして ping 要求を有効にします。

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。ストレージ容量が 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]** ページで表示およびダウンロードできます。ネットワークのセクションを参照してください。

パケットキャプチャをアクティブ化するには、**[パケットキャプチャ]**トグルをクリックしてパケットキャプチャを有効にします。

> **注意**: 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。

センサーのペアリングリクエストの自動承認

受信センサーのペアリングリクエストの自動承認を有効にすると、追加の管理者なしで、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。

受信センサーのペアリングリクエストの自動承認を有効にするには、**[受信センサーのペアリングリクエストを自動承認]**トグルをクリックして自動承認を有効にします。

分類バナー

OT Security にバナーを追加して、ソフトウェアを通してデータにアクセスできることを示します。

バナーを追加するには、**[編集]**をクリックします。バナーを追加したら、**[分類バナー]**トグルをクリックして有効にします。

収集データの有効化

[収集データの有効化]オプションを使って、Tenable が OT Security 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 OT Security リリースでユーザーエクスペリエンスを改善するため、また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。

テレメトリ収集を有効にするには、**[使用状況に関する統計情報の有効化]**トグルをクリックします。

> **注意**: このトグルのスイッチをクリックすることで、収集データの共有をいつでも無効にできます。

GraphQL Playground

ブラウザ内の GraphQL IDEです。本番環境で Playground を使用して API クエリをテストするには、このトグルを有効または無効にします。

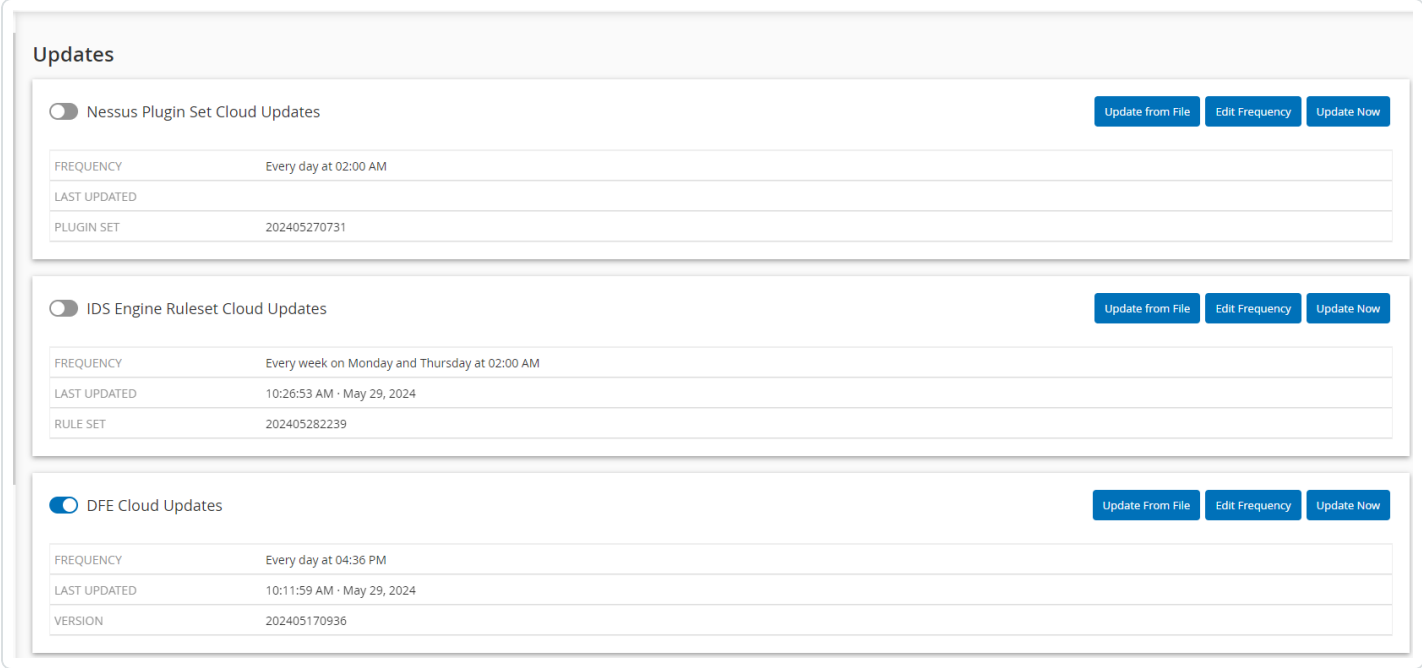
ポート設定

[ポート設定]ページは、デバイスのポートがどのように設定されているかを表示します。ポート設定の詳細については、デバイスを参照してください。

アップデート

Tenable Nessus プラグインと侵入検知システム(IDS)エンジンルールセットを最新バージョンにアップデートすると、OT Security が資産を監視して、最新の既知の脆弱性がないかすべてチェックしてくれます。OT Security は、Dynamic Fingerprinting Engine (DFE) のクラウドアップデートを通じて、分類、ファミリー、カバレッジなどをアップデートするオプションを提供しています。アップデートは、クラウドを通じて自動でも手動で実行でき、オフラインでも実行できます。

注意: Tenable Core の更新の詳細については、Tenable Core + OT Security ユーザーガイドの更新の管理を参照してください。



注意: **[脆弱性]** > **[プラグインのアップデート]** からアップデートを実行することもできます。

注意: ユーザーライセンスの有効期限が切れると、新しいアップデートをダウンロードするオプションがブロックされ、プラグインをアップデートできなくなります。

Tenable Nessus プラグインセットのアップデート

プラグインの自動クラウドアップデートを設定する

インターネット接続がある場合は、クラウドを通じてプラグインをアップデートできます。自動アップデートを有効にしている場合、プラグインはユーザーが設定した時間と頻度でアップデートされます(デフォルトは毎日午前 2 時)。

プラグインの自動アップデートを有効にする手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ウィンドウが表示されます。**[Nessus プラグインセットのクラウドアップデート]** セクションに、プラグインセットの数、最終アップデート日、アップデートスケジュールが表示されます。

2. **[Nessus プラグインセットのクラウドアップデート]** トグルをクリックして、自動アップデートを有効にします。

プラグインアップデートの頻度を編集する

プラグインの自動アップデートスケジュールを編集する手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ウィンドウが表示されます。**[Nessus プラグインセットのクラウドアップデート]** セクションに、プラグインセットの数、最終アップデート日、アップデートスケジュールが表示されます。

2. **[頻度の編集]** 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]** セクションで、数値を入力してドロップダウンボックスから時間の単位（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。

   [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。

4. **[時刻]** セクションで、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。

5. **[保存]** をクリックします。

   頻度が正常に変更されたことを示すメッセージが表示されます。

プラグインの手動クラウドアップデートを実行する

プラグインを手動でアップデートする手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページの **[Nessus プラグインセットのクラウドアップデート]** セクションに、プラグインセットの数、最終更新日、アップデートスケジュールが表示されます。

2. **[今すぐアップデート]** をクリックします。

   アップデートが進行していることを確認するメッセージが表示されます。アップデートが完了すると、**[プラグインセット]** に現在のプラグインセットの数が表示されます。

   > **ヒント**: **プラグインセット** のアップデートの進行中は、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。

オフラインアップデート

OT Security デバイスにインターネット接続がない場合は、Tenable Community 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アップデートできます。

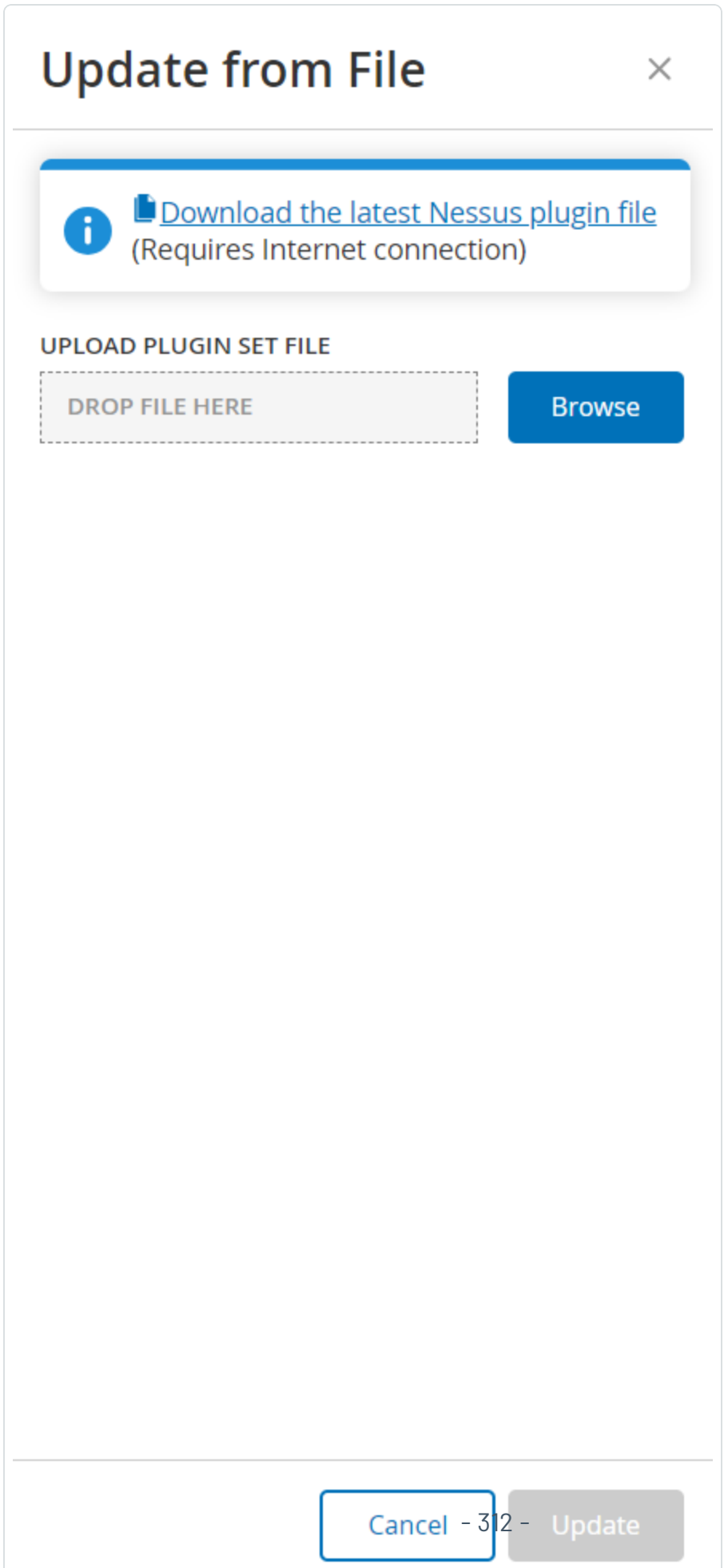
プラグインをオフラインでアップデートする手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページが表示されます。**[Nessus プラグインセットのクラウドアップデート]** セクションに、プラグインセットの数、最終アップデート日、アップデートスケジュールが表示されます。

2. **[ファイルからアップデート]** をクリックします。

[ファイルからアップデート] ウィンドウが表示されます。


Update from File
Download the latest Nessus plugin file
(Requires Internet connection)
UPLOAD PLUGIN SET FILE
DROP FILE HERE
Browse
Cancel
Update

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。

   注意: 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、OT Security 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. **[アップデート]** をクリックします。

IDS エンジンルールセットのアップデート

IDS エンジンルールセットの自動クラウドアップデートを設定する

インターネット接続がある場合は、クラウドを通じて IDS エンジンルールセットをアップデートできます。自動アップデートを有効にすると、ユーザーが設定した時間と頻度で IDS エンジンルールセットをアップデートできます (デフォルトでは毎週月曜日と木曜日の午前 2 時に繰り返されます)。

IDS エンジンルールセットの自動クラウドアップデートを設定する手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページが表示されます。**[IDS エンジンルールセットのクラウドアップデート]** に、ルールセットの数、最終アップデート日、アップデートスケジュールが表示されます。

2. **[IDS エンジンルールセットのクラウドアップデート]** トグルをクリックして、自動アップデートを有効にします。

IDS エンジンルールセットのアップデート頻度を編集する

IDS エンジンルールセットの自動アップデートのスケジュールを編集する手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページが表示されます。**[IDS エンジンルールセットのクラウドアップデート]** に、ルールセットの数、最終アップデート日、アップデートスケジュールが表示されます。

2. **[頻度の編集]** 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. **[繰り返し間隔]** セクションで、数値を入力してドロップダウンボックスから時間の単位 (日または週) を選択することで、ルールセットをアップデートする時間間隔を設定します。

   [週] を選択した場合は、ルールセットの週次アップデートを実行する曜日を選択します。

4. **[時間]** セクションで、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アップデートする時刻 (HH:MM:SS) を設定します。

5. **[保存]** をクリックします。

   頻度が正常に変更されたことを示すメッセージが表示されます。

IDS エンジンルールセットのクラウドアップデートを手動で実行する

IDS エンジンルールセットを手動でアップデートする手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページが表示されます。**[IDS エンジンルールセットのクラウドアップデート]** に、ルールセットの数、最終アップデート日、アップデートスケジュールが表示されます。

2. **[今すぐアップデート]** をクリックします。

   アップデートが進行していることを確認するメッセージが表示されます。アップデートが完了すると、**[ルールセット]** ボックスに現在の IDS エンジンルールセットの数が表示されます。

オフラインアップデート

OT Security デバイスにインターネット接続がない場合は、Tenable Customer Portal から最新のルール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、IDS エンジンルールセットを手動でアップデートできます。

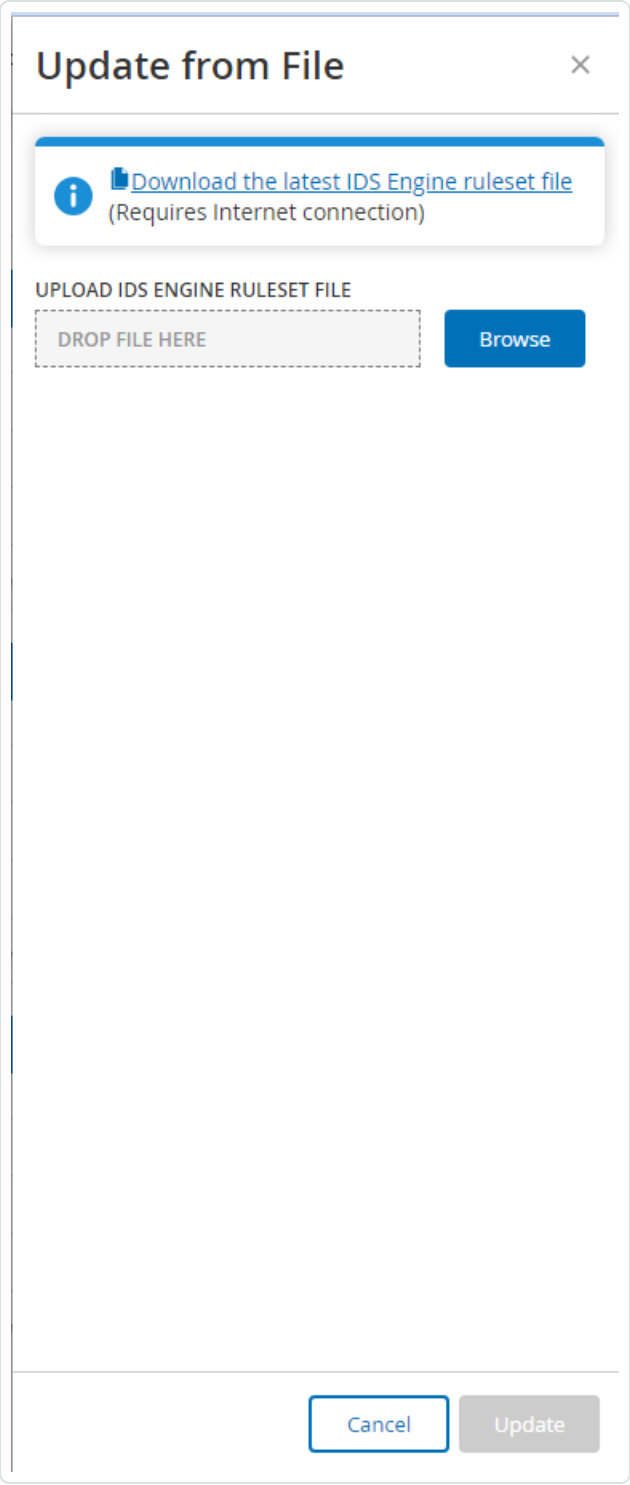
IDS エンジンルールセットをオフラインでアップデートする手順

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ウィンドウが表示されます。**[IDS エンジンルールセットのクラウドアップデート]** に、ルールセットの数、最終アップデート日、アップデートスケジュールが表示されます。

2. **[ファイルからアップデート]** をクリックします。

   [ファイルからアップデート] 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。

> **注意**: リンクから最新の IDS エンジンルールセットファイルのダウンロードするには、インターネットに接続された PC など、インターネット接続が必要になります。

4. **[参照]** をクリックし、OT Security Customer Portal からダウンロードした IDS エンジンルールセットファイルに移動します。
5. **[アップデート]** をクリックします。

DFE のクラウドアップデート

[Dynamic Fingerprinting Engine (DFE) のアップデート] セクションを使用して、OT Security システムの変更を更新したり、新しい分類を追加したりできます。

自動クラウド DFE アップデートを設定する

インターネット接続を使用しクラウドから IDS エンジンルールセットをアップデートできます。自動アップデートを有効にすると、設定した時間と頻度で IDS エンジンルールセットをアップデートできます (デフォルトでは毎週月曜日と木曜日の午前 2 時に繰り返されます)。

自動 DFE アップデートを有効にする方法

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページが表示されます。**[DFE のクラウドアップデート]** セクションには、自動アップデートの頻度設定、最終更新日、アップデートの現在のバージョンが表示されます。
2. 自動アップデートを有効にするには、**[DFE のクラウドアップデート]** トグルをクリックします。

DFE アップデートの頻度を編集する

自動 DFE アップデートのスケジュールを編集する方法

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページが表示されます。**[DFE のクラウドアップデート]** セクションには、自動アップデートの頻度設定、最終更新日、アップデートの現在のバージョンが表示されます。
2. **[頻度の編集]** 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. **[繰り返し間隔]** セクションで、数値を入力してドロップダウンボックスから時間の単位 (日または週) を選択することで、DFE アップデートの時間間隔を設定します。

   [週]を選択した場合は、DFE を毎週アップデートする曜日を選択します。

4. **[時間]** セクションで、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、DFE をアップデートする時刻 (HH:MM:SS) を設定します。

5. **[保存]** をクリックします。

   頻度が正常にアップデートされたことを確認するメッセージが表示されます。

DFE クラウドアップデートを手動で実行する

DFE を手動でアップデートする方法

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ページが表示されます。**[DFE のクラウドアップデート]** セクションには、自動アップデートの頻度設定、最終更新日、アップデートの現在のバージョンが表示されます。

2. **[今すぐアップデート]** をクリックします。

   アップデートが進行していることを確認するメッセージが表示されます。アップデートが完了すると、**[バージョン]** ボックスに現在の DFE バージョンが表示されます。

オフラインアップデート

OT Security デバイスにインターネット接続がない場合は、Tenable Customer Portal から最新のバージョンをダウンロードし、ファイルをアップロードすることで、DFE を手動でアップデートできます。

オフラインで DFE アップデートを実行する方法

1. **[ローカル設定]** > **[システム設定]** > **[アップデート]** に移動します。

   [アップデート] ウィンドウが表示されます。**[DFE のクラウドアップデート]** セクションには、自動アップデートの頻度設定、最終更新日、アップデートの現在のバージョンが表示されます。

2. **[ファイルからアップデート]** をクリックします。

   [ファイルからアップデート] ウィンドウが表示されます。

3. まだダウンロードしていない場合は、リンクをクリックして、最新のデバイス署名ファイルをダウンロードします。

注意: 最新のデバイス署名ファイルのリンクからのダウンロードは、インターネットに接続された PC など、インターネット接続を介してのみ行えます。

4. **[参照]** をクリックし、OT Security Customer Portal からダウンロードしたデバイス署名ファイルに移動します。
5. **[アップデート]** をクリックします。

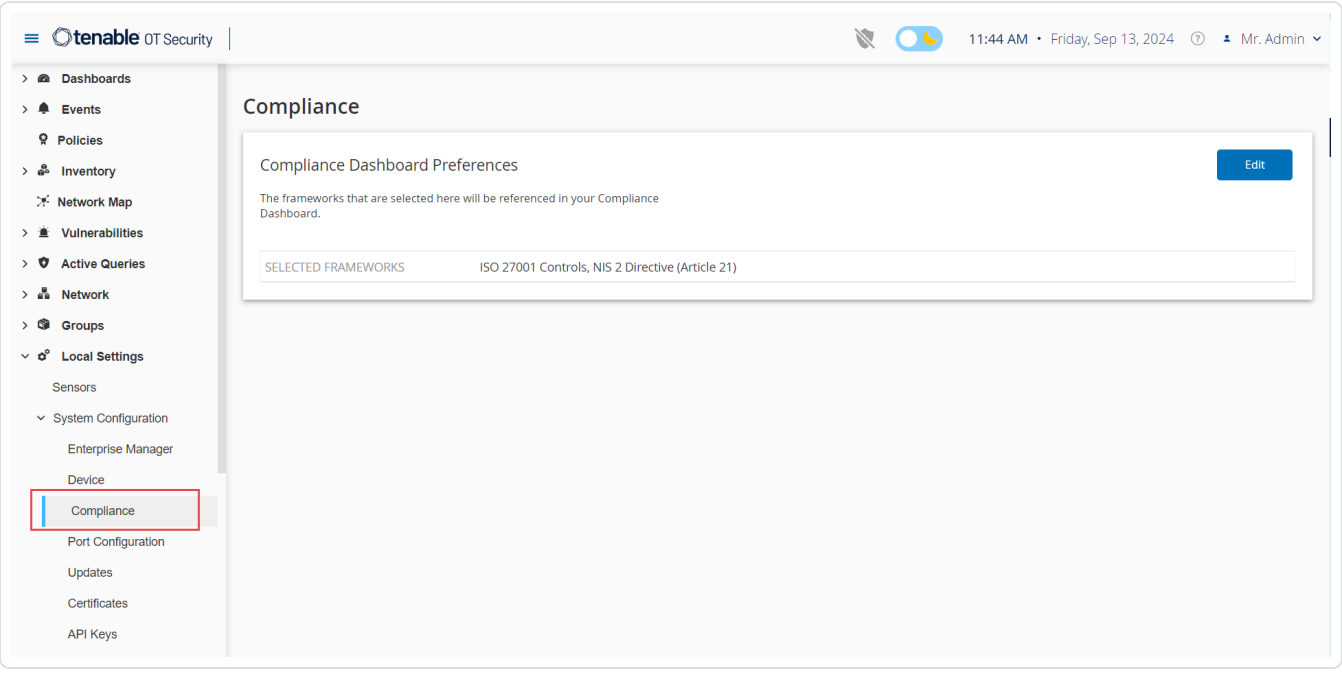
コンプライアンスダッシュボードの設定

ウィジェットでデータを生成するときに **[コンプライアンス]** ダッシュボードが参照するセキュリティフレームワークを指定することができます。

[コンプライアンス] ダッシュボードの設定を行うには、次のようにします。

1. 次のいずれかを行います。
   - **[ローカル設定]** > **[システム設定]** > **[コンプライアンス]** に移動します。
   - **[コンプライアンス]** ダッシュボードページで、**[セキュリティフレームワークの設定]** リンクをクリックします。

   [コンプライアンス] 設定ページが表示されます。



2. **[コンプライアンスダッシュボードの設定]** セクションで、**[編集]** をクリックします。

[参照されるコンプライアンスフレームワークの編集] ペインが表示されます。

3. 必要なコンプライアンスフレームワークを選択します。次のオプションから選択できます。
   - **ISO 27001 管理策**
   - **CAF 原則**
   - **OTCC サブドメイン**
   - **NIS2 指令 (第 21 条)**
4. **[保存]** をクリックします。

   OT Security は、コンプライアンスフレームワークの設定を保存し、指定された設定と照らして組織のコンプライアンスをチェックします。OT Security は、コンプライアンスチェックの結果を [コンプライアンスダッシュボード] に表示します。

証明書

HTTPS 証明書の生成

HTTPS 証明書により、システムが OT Security 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。

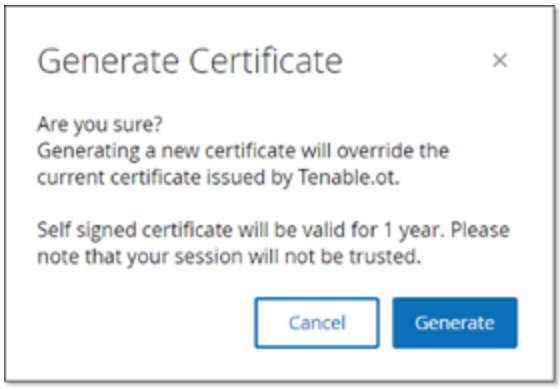
> **注意**: 新しい証明書を生成すると、現在の証明書は上書きされます。

自己署名証明書の生成手順

1. **[ローカル設定]** > **[システム設定]** > **[証明書]** に移動します。

   [証明書] ウィンドウが表示されます。
2. **[アクション]** メニューから **[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。

   OT Security により自己署名証明書が生成され、**[ローカル設定]**>**[システム設定]**>**[証明書]**ページで確認できます。

HTTPS 証明書のアップロード

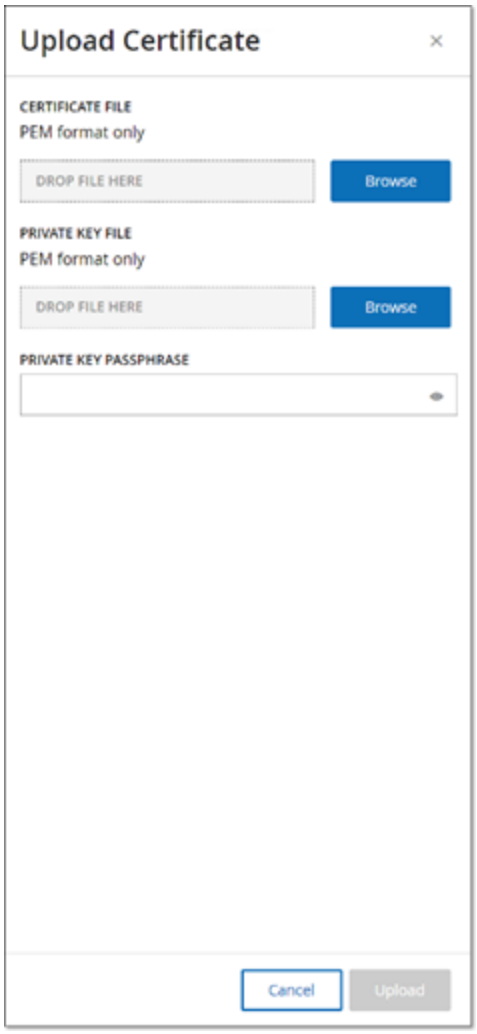
HTTPS 証明書のアップロード手順

1. **[ローカル設定]**>**[システム設定]**>**[証明書]**に移動します。

   [証明書]ウィンドウが表示されます。

2. **[アクション]**メニューから**[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]** セクションで **[参照]** 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]** セクションで **[参照]** 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. **[秘密鍵パスフレーズ]** ボックスに秘密鍵のパスフレーズを入力します。
6. **[アップロード]** 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。

   注意: Tenable では、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推奨しています。アップロードが失敗した場合、OT Security により警告メッセージが表示されます。

ICP と Enterprise Manager のペアリング

注意: このフローは、OT Security 3.18 以降で利用可能です。

Industrial Core Platform (ICP) と OT Security EM をペアリングして、すべてのサイトを管理できます。

始める前に

次のことを確認してください。

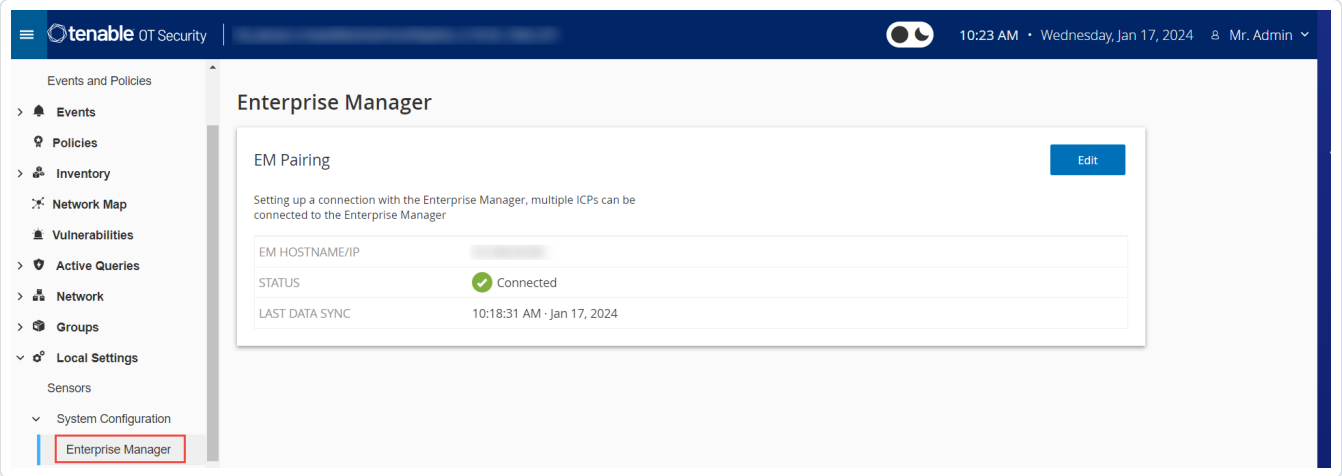
- OT Security EM は API を通して ICP に接続できる
- ICP から OT Security EM への通信用に TCP 443 と TCP 28305 が開かれている
- ICP と OT Security EM の間に HTTPS 接続が存在している
- (オプション) OT Security EM で API キーを生成する

  注意: これは、API キーオプションを使用してペアリングする場合にのみ必須です。

ICP と OT Security EM をペアリングするには

1. OT Security で、**[ローカル設定]** > **[システム設定]** > **[Enterprise Manager]** に移動します。

   Enterprise Manager ページが表示されます。



2. **[EM ペアリング]** セクションで、**[ペアリングの開始]** をクリックします。

   [EM ペアリング設定] パネルが表示されます。

3. 次のいずれかを選択します。

- **ユーザー名とパスワードを使ったペアリング**
- **API シークレットを使ったペアリング**

選択	アクション
ユーザー名とパスワードを使ったペアリング	1. **[ホスト名/IP]** ボックスに、EM のホスト名または IP アドレスを入力します。 2. **[ユーザー名]** ボックスに、EM の管理者のユーザー名を入力します。 3. **[パスワード]** ボックスに、EM のパスワードを入力します。 4. **[EM 証明書フィンガープリント]** に、EM の **[証明書]** ページからコピーした証明書を貼り付けます。 **ヒント**: この手順をスキップして、**EM ペアリング**ページから証明書を手動で承認することもできます。 **注意**: OT Security EM の **[ローカル設定]** > **[システム設定]** から **証明書**ページにアクセスできます。
API キーを使用してペアリング	1. **[ホスト名/IP]** ボックスに、EM のホスト名または IP アドレスを入力します。 2. **[API シークレット]** ボックスに、EM からコピーした API キーを貼り付けます。 3. **[EM 証明書フィンガープリント]** に、EM の **[証明書]** ページからコピーした証明書を貼り付けます。 **ヒント**: この手順をスキップして、**EM ペアリング**ページから証明書を手動で承認することもできます。 **注意**: OT Security EM の **[ローカル設定]** > **[システム設定]** から **証明書**ページにアクセスできます。

4. **[ペアリング]** をクリックします。

OT Security が **EM ペアリング**ページにペアリングステータスを表示します。

> **注意**: ステータスは、**[証明書の承認待ち]**(証明書が提供されていない場合)または**[EM の承認待ち]**(ペアリングリクエストの自動承認が無効の場合)と表示されます。

5. (オプション) ステータスが**[証明書の承認待ち]**の場合

   a. **[証明書の表示]**をクリックします。

      [証明書の承認]パネルが表示されます。

   b. パネルのフィンガープリントが EM の**証明書**ページのものと同じであることを確認します。

      [承認]をクリックします。

      OT Security によって証明書が承認されると、EM ペアリングページでステータスが**[EM の承認待ち]**に変わります。

6. ステータスが**[EM の承認待ち]**と表示されている場合、**[自動承認 ICP ペアリングリクエスト]**が無効になっています。有効にするには次の手順を実行してください。

> **ヒント**: OT Security EM でペアリングリクエストを自動的に承認するには、OT Security EM の **ICP** ページで**[自動承認 ICP ペアリングリクエスト]**を有効にします。

   a. OT Security EM の左側のナビゲーションバーで、**[ICP]**を選択します。

      ICP ページが表示されます

   b. ペアリングするシステムの行にカーソルを合わせ、次のいずれかを実行します。

      - **[ステータス]**列を右クリックし、**[承認]**を選択します。
      - 右上の**[アクション]** > **[承認]**をクリックします。

OT Security EM がペアリングを承認し、**[接続済み]**のステータスが表示されます。

> **ヒント**: ペアリングが完了すると、OT Security EM に以下が表示されます。
>
> - ICP のデータを EM **ダッシュボード**で表示します。
> - 新たにペアリングされた ICP が**[ICP]**ページに表示されます。
> - **[ICP]**ページの ICP 名をクリックして、ICP にアクセスします。EM からアクセスされた ICP インスタンスでは、ヘッダーに **ICP** ラベルが表示されます。詳細は、ICPsを参照してください。

OT Security で、**Enterprise Manager** ページのステータスが **[接続済み]** と表示されます。**[編集]** をクリックして、EM ペアリング設定を変更できます。

Enterprise Manager と ICP のペアリングの解除

ペアリングが不要になったら、EM または ICP から ICP ペアリングを解除できます。

OT Security EM から ICP ペアリングを解除するには

1. OT Security EM の左側のナビゲーションバーで、**[ICP]** を選択します。

   ICP ページが表示されます

2. 削除する ICP の行にカーソルを合わせ、次のいずれかを実行します。

   - **[ステータス]** 列を右クリックし、**[削除]** を選択します。
   - [ICP] の行をクリックします。これにより、行が強調表示され、**[アクション]** ボタンが有効になります。

3. **[削除]** をクリックします。

OT Security EM が OT Security とのペアリングを解除します。

OT Security から ICP ペアリングを解除するには

1. OT Security で、**[ローカル設定]** > **[システム設定]** > **[Enterprise Manager]** に移動します。

   Enterprise Manager ページが表示されます。

2. [EM ペアリング] セクションで、**[編集]** をクリックします。

   [EM ペアリング] パネルが表示されます。

3. **[ペアリングなし]** をクリックします。

4. **[ペアリング]** をクリックします。

   OT Security が OT Security EM とのペアリングを解除します。

ライセンス

OT Security ライセンスを更新または再初期化する必要がある場合は、Tenable アカウントマネージャーに連絡してください。Tenable アカウントマネージャーによりライセンスがアップデートされたら、お客様は自分

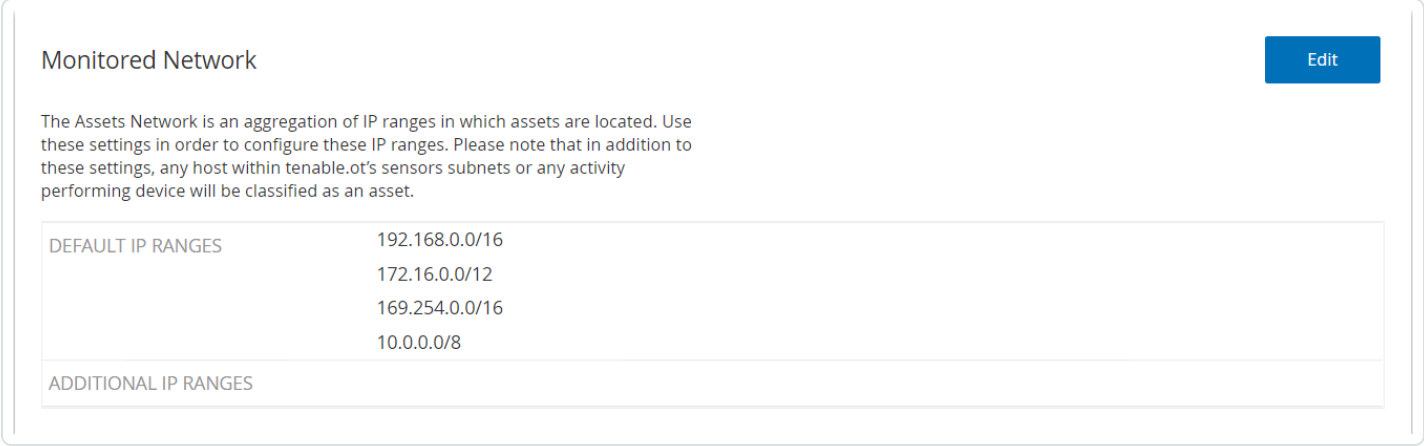
でライセンスのアップデートや再初期化ができます。詳細は、OT Security ライセンスのアクティベーションを参照してください。

環境設定

監視対象ネットワーク

監視対象ネットワークの設定には、OT Security のモニタリング境界を定義する一連の IP 範囲 (CIDR/サブネット) が含まれます。OT Security は、設定された範囲外の資産を無視します。

デフォルトでは、OT Security は 3 つのデフォルトのパブリック範囲 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、およびリンクローカル範囲 (APIPA) 169.254.0.0/16 を設定します。



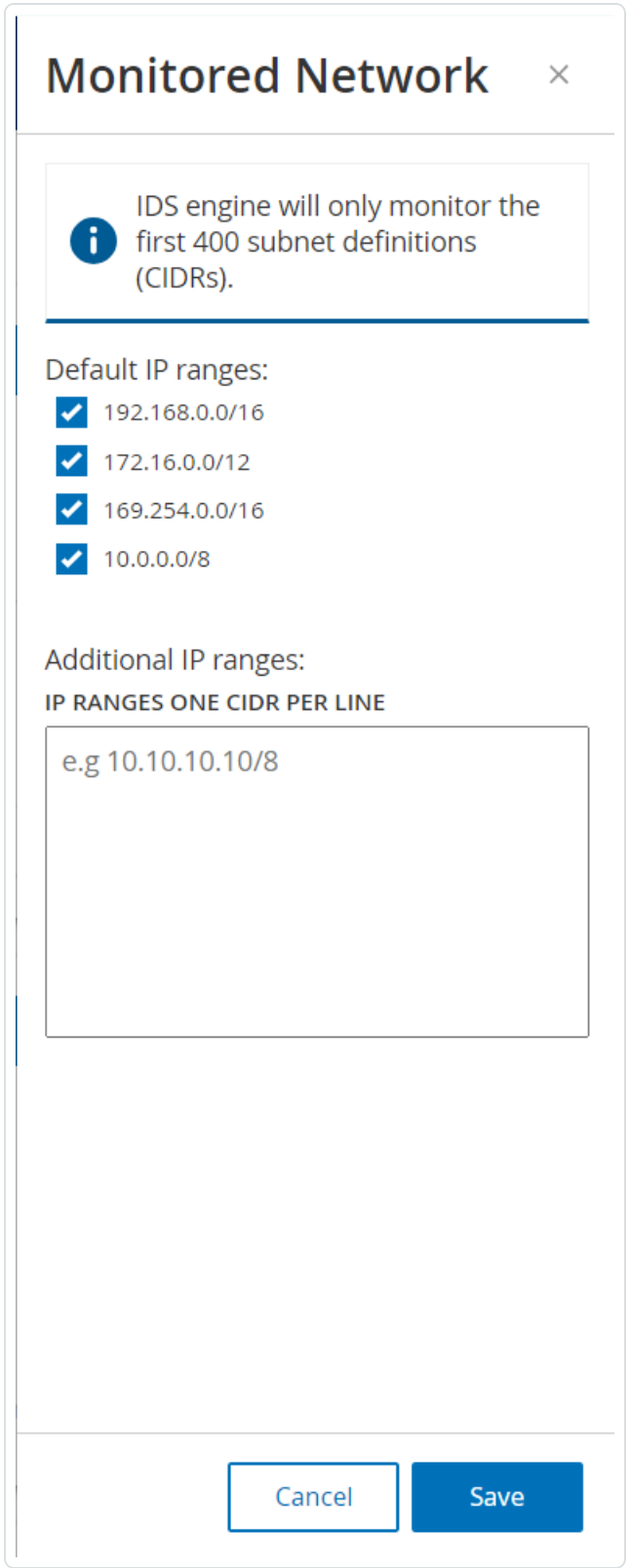
デフォルトの範囲のいずれかを無効にする、または使用しているネットワークに適した範囲を追加するには、次のようにします。

1. **[ローカル設定]** > **[環境設定]** > **[資産設定]** に移動します。

   [資産設定] ウィンドウが表示されます。

2. **[編集]** をクリックします。

[監視対象ネットワーク] パネルが表示されます。



3. 必要な **[既定の IP 範囲]** を選択するか、指定されたテキストボックスに **[追加の IP 範囲]** (1 行につき 1 つの IP 範囲) を追加します。
4. **[保存]** をクリックします。

   OT Security が監視対象ネットワーク設定を保存します。

手動による資産の追加

OT Security でまだ資産が検出されていないとしても、インベントリを追跡するために、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。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のリスクスコアは、OT Security によって検出されるまでは 0 と表示されます。

> **注意**: 資産を手動で追加した場合、OT Security 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には、次のようにします。

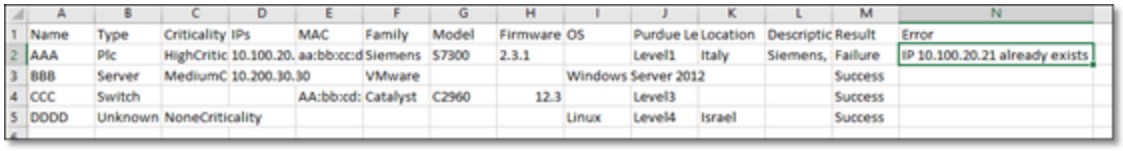
1. **[ローカル設定]** > **[環境設定]** > **[資産設定]** に移動します。

   [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]** メニューから **[CSV テンプレートのダウンロード]** を選択します。

   OT Security により 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。
3. tot_Assets テンプレートドキュメントを開きます。
4. 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。
5. 編集したファイルを保存します。

6. **[資産設定]** 画面に戻ります。
7. **[アクション]** メニューから **[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。
8. **[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イベントなど)、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。

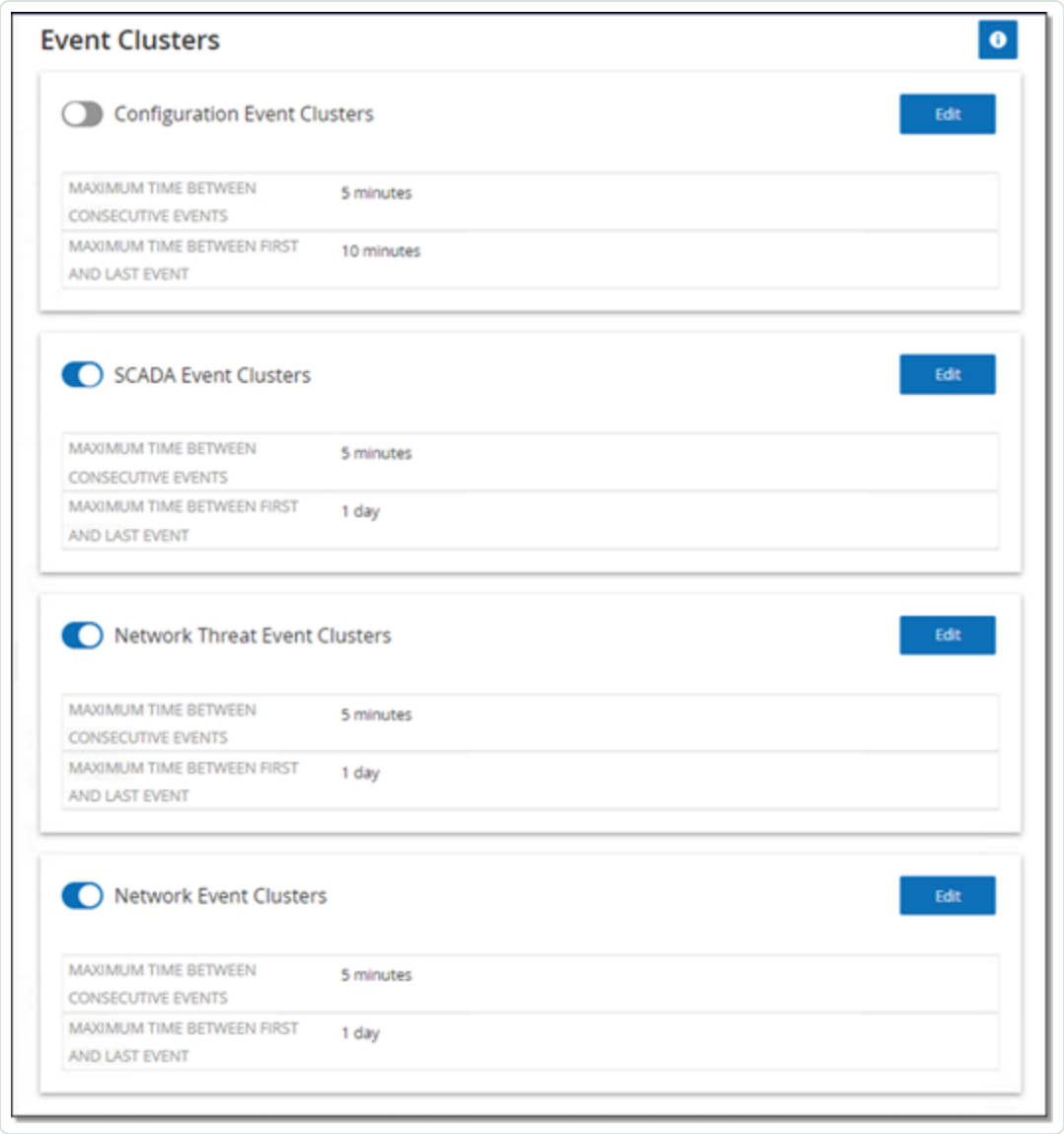
イベントをクラスター化するには、次の設定された時間間隔内にイベントを生成する必要があります。

- **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]** に移動し、**[環境設定]** > **[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。

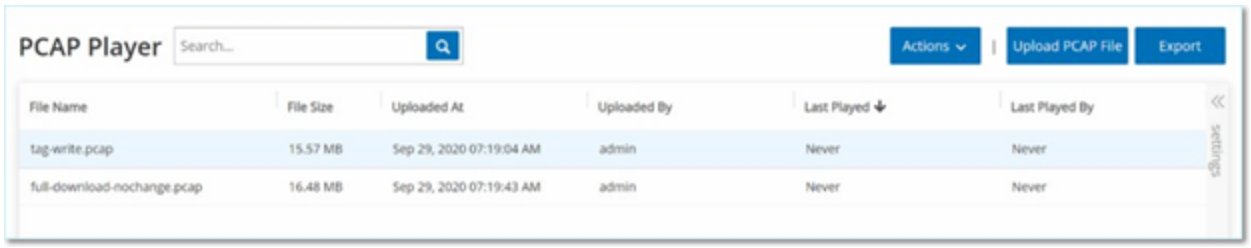


2. トグルをクリックして、クラスタリングに必要なカテゴリを有効にします。
3. カテゴリの時間間隔を設定するには、**[編集]**をクリックします。

   [設定の編集]ウィンドウが表示されます。
4. 数値ボックスに目的の数値を入力し、ドロップダウンボックスを使用して時間の単位を選択します。

   > **注意**: クラスタリングおよび時間間隔の詳細については、 アイコ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



OT Security では、記録されたネットワークアクティビティを含む PCAP (パケットキャプチャ) ファイルをアップロードし、OT Security で「再生」することができます。PCAP ファイルを「再生」すると、OT Security 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で発生する OT Security 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。たとえば、遠隔地の工場などです。t

注意: PCAP プレーヤー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。OT Security 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]** > **[環境設定]** > **[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。

   OT Security により 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

PCAP ファイルの再生手順

1. **[ローカル設定]** > **[環境設定]** > **[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。

   [PCAP の再生] ウィザードが表示されます。

4. **[再生速度]** ドロップダウンボックスで、システムがファイルを再生する速度を選択します。

   オプションは、1X、2X、4X、8X、16X です。

   > **注意**: 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。この操作を元に戻すことはできず、実行されると停止できません。

5. **[再生]** をクリックします。

   PCAP ファイルが再生されます。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。

   > **注意**: 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

OT Security コンソールへのアクセスは、そのユーザーが利用できるアクセス許可を指定するユーザーアカウントによって制御されます。ユーザーのアクセス許可は、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アクセス許可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アクセス許可が付与されます。

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、OT Security ロールを割り当てることができます。

- **SAML** – ID プロバイダー (Microsoft Entra ID など) との統合をセットアップし、ユーザーを OT Security アプリケーションに割り当てます。

ローカルユーザー

ユーザーグループ

ユーザーロール

ゾーン

認証サーバー

SAML

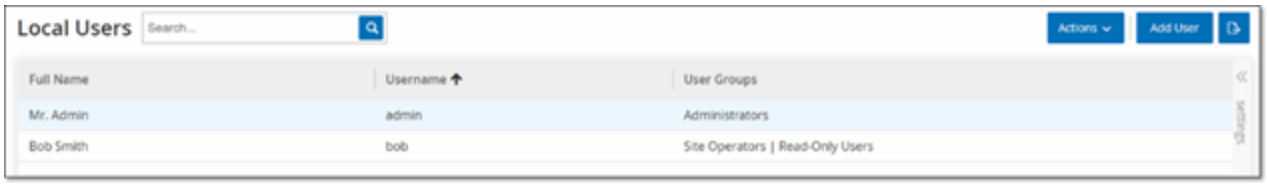
ローカルユーザー

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。

注意: ユーザーのアカウントまたはユーザーグループの作成中または編集中に、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] ウィンドウに、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。



[ローカルユーザー] ウィンドウには、次の詳細が表示されます。

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。

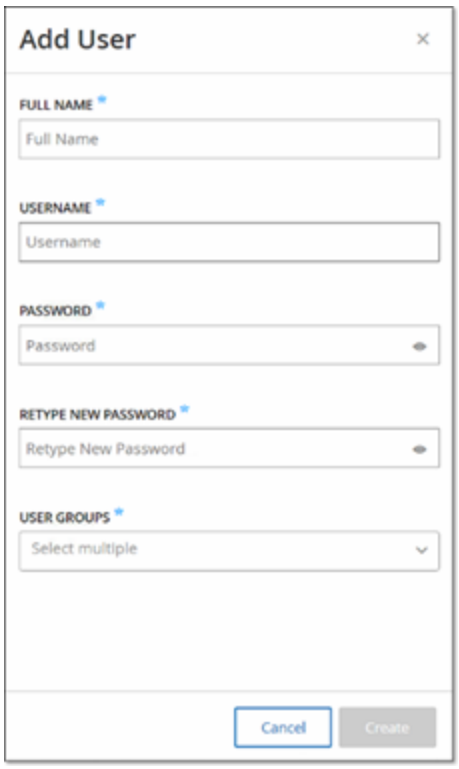
ローカルユーザーの追加

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]** > **[ユーザー管理]** > **[ローカルユーザー]** に移動します。
2. **[ユーザーの追加]** 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]** ボックスに姓と名を入力します。

   > **注意**: 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]** ボックスに、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]** ボックスで、パスワードを入力します。
6. **[パスワードの再入力]** ボックスに、同じパスワードを入力します。

注意: 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]**ウィンドウでパスワードを変更できます。

7. **[ユーザーグループ]**ドロップダウンボックスで、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。

   注意: 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、ローカルユーザーを参照してください。

8. **[作成]**をクリックします。

   OT Security により新しいユーザーアカウントがシステムに作成され、**[ローカルユーザー]**のユーザー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]** > **[ユーザー管理]** > **[ローカルユーザー]**に移動します。

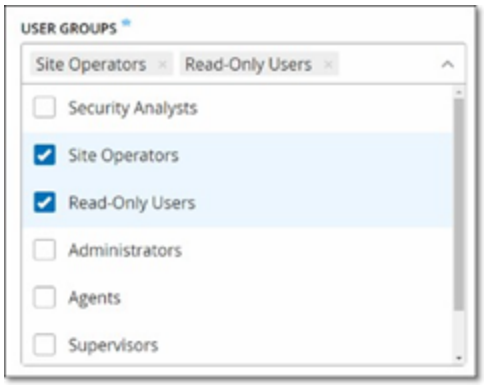
   [ローカルユーザー]画面が表示されます。

2. 目的のユーザーを右クリックし、**[ユーザーの編集]**を選択します。

   注意: あるいは、ユーザーを選択して、**[アクション]**メニューから**[ユーザーの編集]**を選択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]** ドロップダウンボックスで、目的のユーザーグループを選択または選択解除します。



5. **[保存]** をクリックします。

ユーザーのパスワードの変更

> **注意**: これは、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]** > **[ユーザー管理]** > **[ローカルユーザー]** 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、**[パスワードのリセット]** を選択します。

   > **注意**: あるいは、ユーザーを選択して、**[アクション]** メニューから **[パスワードのリセット]** を選択することもできます。

   [パスワードリセット] ウィンドウが表示されます。

3. **[新しいパスワード]** ボックス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]** ボックスに新しいパスワードをもう一度入力します。
5. **[リセット]** をクリックします。

   OT Security により、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]** > **[ユーザー管理]** > **[ローカルユーザー]** 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、**[ユーザーの削除]** を選択します。

   > **注意**: あるいは、ユーザーを選択して、**[アクション]** メニューから **[ユーザーの削除]** を選択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。

   OT Security により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

ユーザーグループページに、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。

ユーザーグループページでは次の詳細を確認できます。

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。

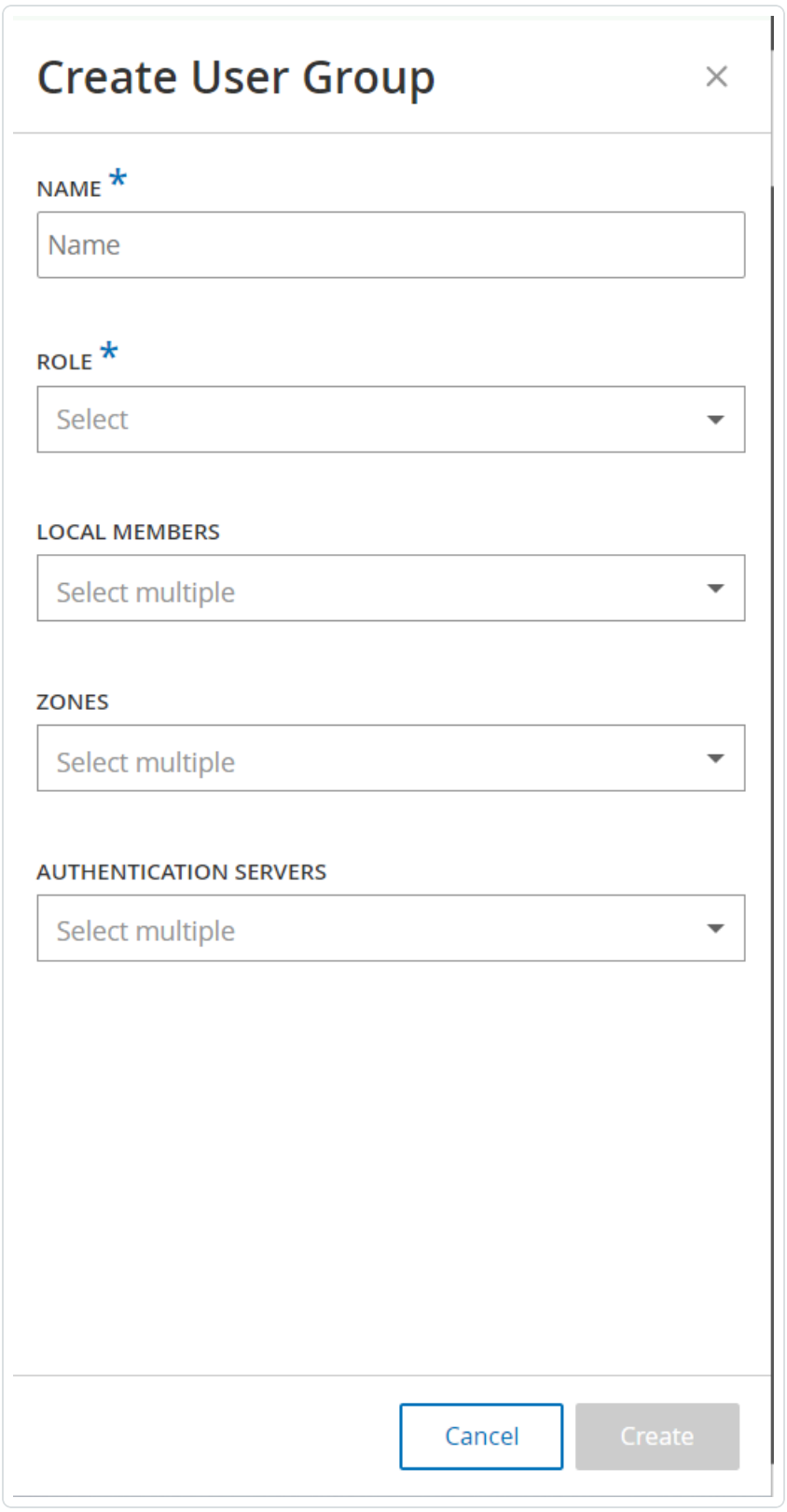
ユーザーグループを作成する方法

1. **[ローカル設定]** > **[ユーザー管理]** > **[ユーザーグループ]** 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]** 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]**ボックスに、グループの名前を入力します。

4. **[ロール]**ドロップダウンボックスのドロップダウンリストから、このグループに割り当てるロールを選択します。選択可能なロールは次のとおりです。

    - 読み取り専用
    - 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

5. **[ローカルメンバー]**ドロップダウンボックスで、グループに割り当てるユーザーアカウントを選択します。
6. **[ゾーン]**ドロップダウンボックスで、ユーザーグループに割り当てるゾーンを選択します。
7. **[認証サーバー]**ドロップダウンボックスで、ユーザーグループに割り当てるサーバーを選択します。
8. **[作成]**をクリックします。

    OT Security により新しいユーザーグループが作成され、**[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。

注意: あるいは、ユーザーを選択して、**[アクション]**メニューから**[ユーザーの削除]**を選択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]** > **[ユーザー管理]** > **[ユーザーグループ]**に移動します。

    [ユーザーグループ]画面が表示されます。

2. 次のいずれかを実行します。

- 目的のユーザーグループを右クリックし、**[編集]**を選択します。
- 編集するユーザーグループを選択します。**[アクション]**メニューが表示されます。**[アクション]** > **[編集]**を選択します。

[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。

3. **名前とロール**を変更します。グループにユーザーを追加または削除するには、ユーザーを選択または選択解除します。

4. 必要に応じてパラメーターを変更します。
5. **[保存]**をクリックします。

ユーザーグループの削除

注意: 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]** > **[ユーザー管理]** > **[ユーザーグループ]**に移動します。

   [ユーザーグループ]画面が表示されます。

2. 次のいずれかを実行します。

- 目的のユーザーグループを右クリックし、**[削除]**を選択します。
- 削除するユーザーグループを選択します。**[アクション]**メニューが表示されます。**[アクション]** > **[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。

OT Security により**ユーザーグループ**が削除されます。

ユーザーロール

利用可能なロールは次のとおりです。

- **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、システム内でアクションを実行することはできません。
- **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(ポリシーの設定、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)
イベント		
イベントを表示	✓	✓
解決	✓	✓

キャプチャファイルのダウンロード	✓	✓
ポリシーから除外	✓	✓
すべて解決	✓	✓
エクスポート	✓	✓
FortiGateでポリシーを作成	✓	✓
更新	✓	✓
ポリシー		
ポリシーの表示	✓	✓
有効化 / 無効化	✓	✓
アクションの表示	✓	✓
編集	✓	✓
複製	✓	✓
削除	✓	✓
ポリシーの作成	✓	✓
エクスポート	✓	✓
資産		
資産の表示	✓	✓
アクションの表示	✓	✓
編集	✓	✓
削除	✓	✓
インポート (csv で新しい資産をアップロード)	✓	✓

非表示	✓	✓
エクスポート	✓	✓
再同期	✓	✓
Nessus スキャン	✓	✓
スナップショットの作成（単一の資産）	✓	✓
開いているポートの更新（単一の資産）	✓	✓
ポート状態の更新（単一の資産）	✓	✓
ブラウザで表示（単一の資産）	✓	✓
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	✓	✓
プラグインセットの更新	✓	✓
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	✓	✓
進行中のキャプチャを閉じる	✓	✓
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	✓	✓

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	✓	✓
編集	✓	✓
複製	✓	✓
削除	✓	✓
グループの作成	✓	✓
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	✓	✓
削除	✓	✓
作成	✓	✓
エクスポート	✓	✓
詳細情報	✓	✓

ローカル設定		
クエリ	✓	✓
システム設定 - デバイスの詳細	✓	✓
システム設定 - センサー	✓	✓
システム設定 - ポート設定	✓	✓
システム設定 - 更新	✓	✓
システム設定 - 証明書 (HTTPS)	✓	✓
システム設定 - API キー	✓	✗
システム設定 - ライセンス	✓	✓
環境設定 - 資産設定	✓	✓
環境設定 - 非表示の資産	✓	✓
環境設定 - カスタムフィールド	✓	✓
環境設定 - イベントクラスター	✓	✓
環境設定 - PCAP プレーヤー	✓	✓
ユーザーとロール - ユーザー設定	✓	✓
ユーザーとロール - ローカルユーザー	✓	✗
ユーザーとロール - ユーザーグループ	✓	✗
ユーザーとロール - Active Directory	✓	✗
統合	✓	✓
サーバー	✓	✓
システムアクション	✓	✓出荷時設定へのリセットなし

システムログ	✓	✓
有効化（セットアップ時および無効化後）	✓	✓
資産の削除	✓	✓

アクセス許可	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	✓	✓	✓	✗	✗
キャプチャファイルのダウンロード	✓	✓	✓	✓	✓
ポリシーから除外	✓	✓	✗	✗	✗
すべて解決	✓	✓	✓	✗	✗
エクスポート	✓	✓	✓	✓	✓
FortiGateでポリシーを作成	✓	✓	✗	✗	✗
更新	✓	✓	✓	✓	✓
ポリシー					
ポリシーの表示	✓	✓	✓	✓	✓
有効化 / 無効化	✓	✓	✗	✗	✗
アクションの表示	✓	✓	✓	✓	✓
編集	✓	✓	✗	✗	✗
複製	✓	✓	✗	✗	✗

削除	✓	✓	✗	✗	✗
ポリシーの作成	✓	✓	✗	✗	✗
エクスポート	✓	✓	✓	✓	✓
資産					
資産の表示	✓	✓	✓	✓	✓
アクションの表示	✓	✓	✓	✓	✓
編集	✓	✗	✗	✓	✗
削除	✓	✗	✗	✓	✗
インポート (csv で新しい資産をアップロード)	✓	✗	✗	✓	✗
非表示	✓	✗	✗	✓	✗
エクスポート	✓	✓	✓	✓	✓
再同期	✓	✓	✓	✓	✗
Nessus スキャン	✓	✓	✓	✓	✗
スナップショットの作成 (単一の資産)	✓	✓	✓	✓	✗
開いているポートの更新 (単一の資産)	✓	✓	✓	✗	✗
ポート状態の更新 (単一の資産)	✓	✓	✓	✗	✗
ブラウザで表示 (単一の資産)	✓	✓	✓	✓	✓
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	✓	✓	✓	✗	✗
プラグインセットの更新	✓	✓	✗	✗	✗
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	✓	✗	✗	✗	✗
進行中のキャプチャを閉じる	✓	✓	✓	✓	✗
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	✓	✓	✗	✗	✗
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	✓	✓	✓	✓	✓
編集	✓	✓	✗	✗	✗
複製	✓	✓	✗	✗	✗
削除	✓	✓	✗	✗	✗
グループの作成	✓	✓	✗	✗	✗
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	✓	✓	✗	✗	✗
削除	✓	✓	✗	✗	✗
作成	✓	✓	✗	✗	✗
エクスポート	✓	✓	✓	✓	✓
詳細情報	✓	✓	✓	✓	✓
ローカル設定					
クエリ	✓	✗	✗	✗	✗
システム設定 - デバイスの詳細	✓	✗	✗	✗	✗

システム設定 - 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)
システム設定 - ポート設定	✓	✗	✗	✗	✗
システム設定 - 更新	✓	✗	✗	✗	✗
システム設定 - 証明書 (HTTPS)	✗	✗	✗	✗	✗
システム設定 - API キー	✓(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)
システム設定 - ライセンス	✗	✗	✗	✗	✗
環境設定 - 資産設定	✓	✗	✗	✗	✗
環境設定 - 非表示の資産	✓	✓- 復元なし	✓- 復元なし	✓	✓- 復元なし
環境設定 - カスタムフィールド	✓	✗	✗	✗	✗
環境設定 - イベントクラスター	✓	✗	✗	✗	✗
環境設定 - PCAP プレーヤー	✓	✗	✗	✗	✗
ユーザーとロール - ユーザー設定	✓	✗	✗	✗	✗
ユーザーとロール - ローカルユーザー	✗	✗	✗	✗	✗
ユーザーとロール -	✗	✗	✗	✗	✗

ユーザーグループ					
ユーザーとロール - Active Directory	✗	✗	✗	✗	✗
統合	✗	✗	✗	✗	✗
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	✓バックアップと診断のみ	✓診断のみ	✗	✗	✗
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)	✗	✗	✗	✗	✗
資産の削除	✓	✗	✗	✗	✗

ゾーン

ゾーンは、特定のユーザーグループが閲覧できる資産、イベント、脆弱性を制御します。特定のユーザーグループは、そのゾーン内にある資産とそれに関連する脆弱性、イベント、接続だけを閲覧できます。管理者以外のアカウントを特定のグループとゾーンに割り当てて、関連する資産だけを閲覧できるように制限できます。

ゾーンの作成

ゾーンを作成するには

1. **[ローカル設定]** > **[ユーザー管理]** > **[ゾーン]** に移動します。

   ゾーンページが表示されます。

2. 右上の**[作成]**をクリックします。

   [ゾーンの作成] パネルが表示されます。

3. **[名前]** ボックスにゾーンの名前を入力します。
4. **[資産グループ]** ボックスで、ゾーンに割り当てるグループを選択します。検索ボックスを使用して、特定の資産グループを検索できます。
5. **[ユーザーグループ]** ボックスで、ゾーンに割り当てるユーザーグループを選択します。
6. (オプション) **[説明]** ボックスに、ゾーンの説明を入力します。
7. **[作成]** をクリックします。

   OT Security によりゾーンが作成され、**ゾーン**ページに表示されます。

ゾーンの表示

1. **[ローカル設定]** > **[ユーザー管理]** > **[ゾーン]** に移動します。

   ゾーンページが表示されます。**ゾーン**ページには、ゾーンが表形式で表示され、次の詳細が含まれます。

列	説明
名前	ゾーンの名前
資産グループ	ゾーンに割り当てられた資産グループ
ユーザーグループ	ゾーンに割り当てられたユーザーグループ
説明	ゾーンの説明
最終変更者	ゾーンを最後に変更したユーザー
最終変更日	ゾーンが最後に変更された日付

ゾーンの編集

1. **[ローカル設定]** > **[ユーザー管理]** > **[ゾーン]** に移動します。

   ゾーンページが表示されます。

2. 編集するゾーンの行をクリックし、次のいずれかを実行します。

- ゾーンを右クリックし、**[編集]**を選択します。
- ヘッダーバーで、**[アクション]** > **[編集]**をクリックします。

[ゾーンの編集]パネルが表示されます。

3. 必要に応じて設定を変更します。
4. **[保存]**をクリックします。

OT Securityによりゾーンが更新されます。

ゾーンの複製

1. **[ローカル設定]** > **[ユーザー管理]** > **[ゾーン]**に移動します。

ゾーンページが表示されます。

2. 複製するゾーンの行をクリックし、次のいずれかを実行します。
   - ゾーンを右クリックし、**[複製]**を選択します。
   - ヘッダーバーで、**[アクション]** > **[複製]**をクリックします。

[ゾーンの複製]パネルが表示されます。

3. **[名前]**ボックスにゾーンの名前を入力します。

デフォルト値は、元のゾーン名に「のコピー」という末尾が付いたものとなります。

4. 必要に応じて設定を変更します。
5. **[複製]**をクリックします。

OT Securityにより、ゾーンの複製が作成されます。

ゾーンの削除

不要になったゾーンは削除できます。

> **注意**: 関連するユーザーグループが存在する場合、ゾーンを削除することはできません。

1. **[ローカル設定]** > **[ユーザー管理]** > **[ゾーン]**に移動します。

ゾーンページが表示されます。

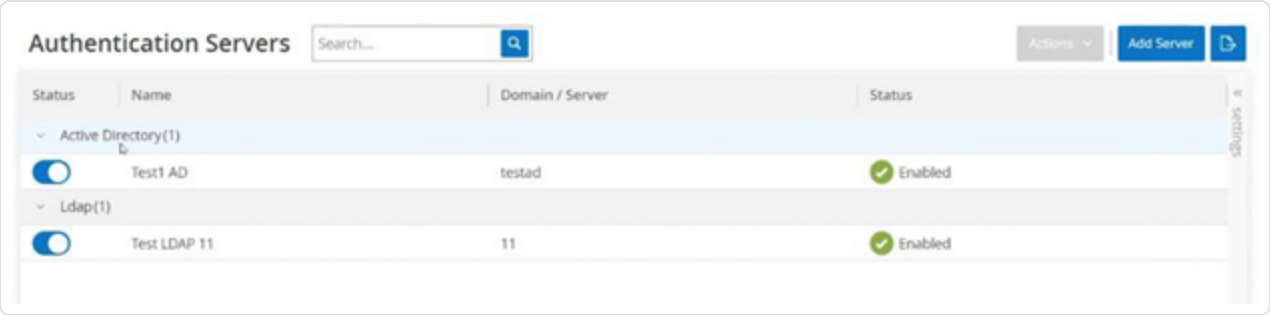
2. 削除するゾーンの行をクリックし、次のいずれかを実行します。

   - ゾーンを右クリックし、**[削除]** を選択します。
   - ヘッダーバーで、**[アクション]** > **[削除]** をクリックします。

   OT Security により、ゾーンが削除されます。

認証サーバー

認証サーバーページには、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

OT Security を所属組織の Active Directory (AD) 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 OT Security にログインできるようになります。設定には、統合のセットアップと、AD のグループを OT Security のユーザーグループにマッピングすることが含まれます。

注意: 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、認証サーバーを参照してください。

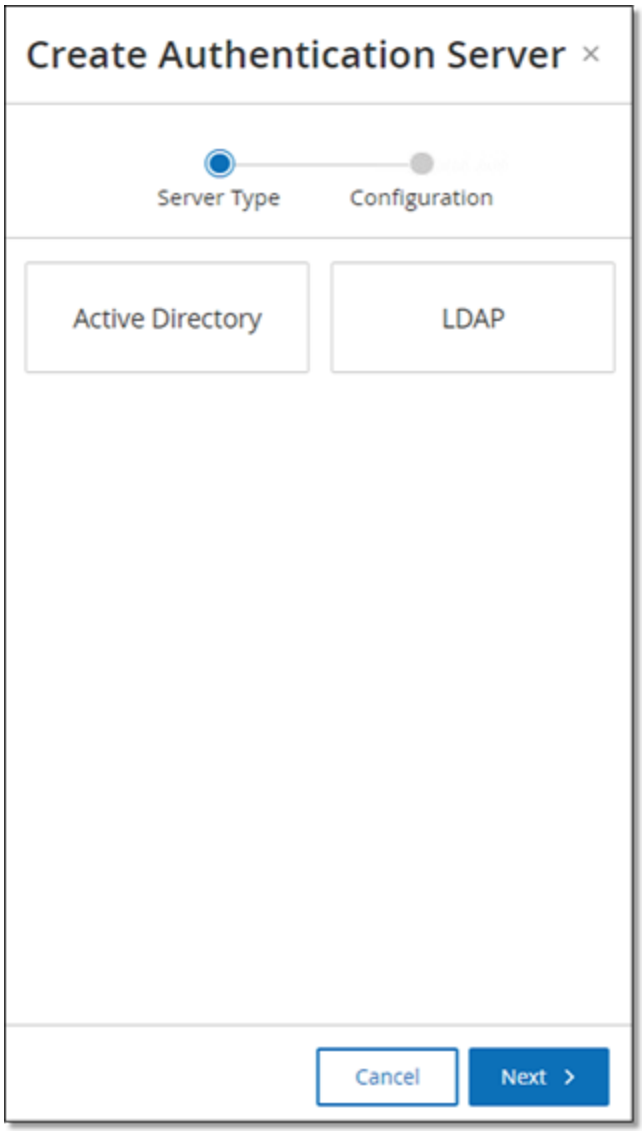
Active Directory の設定手順

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。
2. **[ローカル設定]** > **[ユーザー管理]** > **[認証サーバー]** に移動します。

   [認証サーバー] ウィンドウが表示されます。

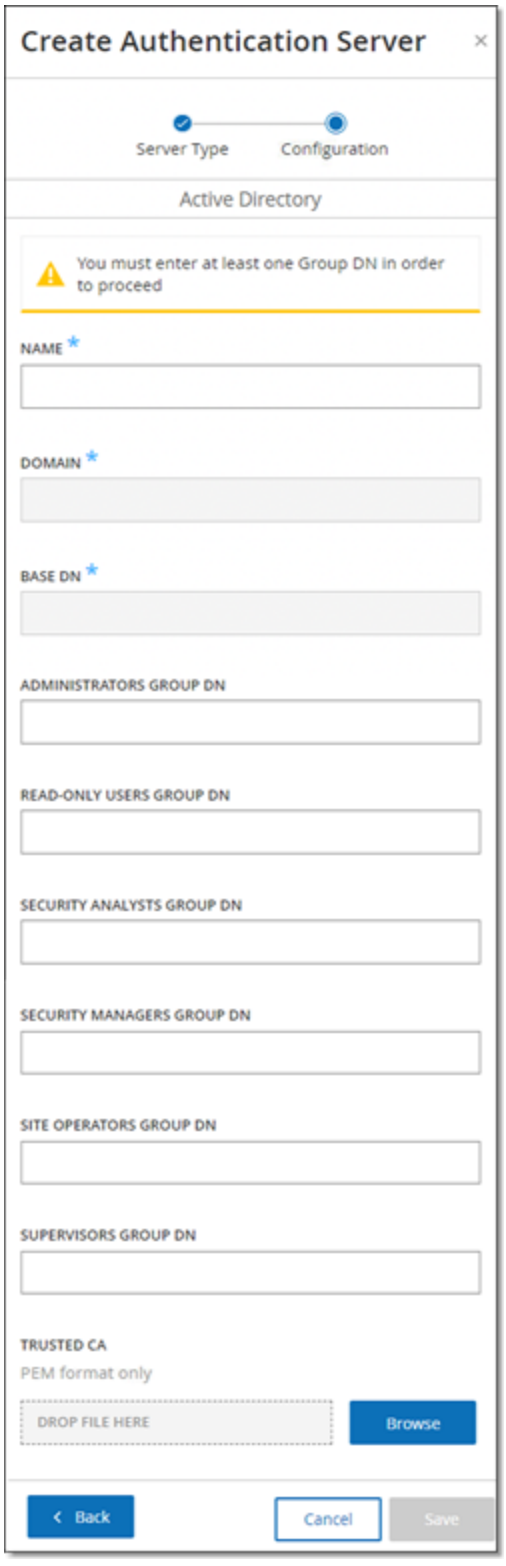
3. **[サーバーの追加]** をクリックします。

   [認証サーバーの作成] パネルが開き、**[サーバータイプ]** が表示されます。



4. **[Active Directory]** をクリックしてから **[次へ]** をクリックします。

   [Active Directory] 設定ペインが表示されます。



5. **[名前]**ボックスに、ログイン画面で使用する名前を入力します。
6. **[ドメイン]**ボックスに、組織ドメインの FQDN (例 : company.com) を入力します。

注意: ドメインがわからない場合は、Windows CMD またはコマンドラインで「set」コマンドを入力すると確認できます。「USERDNSDOMAIN」属性に付与されている値がドメイン名です。

7. **[ベース DN]** ボックスに、ドメインの識別名を入力します。この値の形式は、「DC={セカンドレベルドメイン},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 OT Security ユーザーグループにマップする各グループについて、適切なボックスに 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、管理者権限の割り当て先となる Active Directory グループの DN を **[管理者グループ DN]** ボックスに入力します。

   注意: OT Security 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 またはコマンドラインにコマンド `dsquery group -name Users` を入力すれば、ユーザーを含む Active Directory で設定されているすべてのグループのリストが表示されます。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。

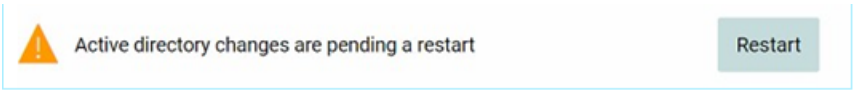
   注意: これらのフィールドはオプションです。フィールドが入力されていない場合、AD ユーザーはそのユーザーグループに割り当てられません。マッピングされたグループなしでも統合を設定できますが、その場合、少なくとも 1 つのグループマップの ping を追加するまで、ユーザーはシステムにアクセスできません。

9. (オプション) **[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。

10. **[Active Directory の有効化]** 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。

    メッセージが表示され、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、OT Security により Active Directory の設定が有効になります。指定されたグループに割り当てられたユーザーは、自分の所属組織の認証情報を使用して OT Security プラットフォームにアクセスできます。

注意: 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。

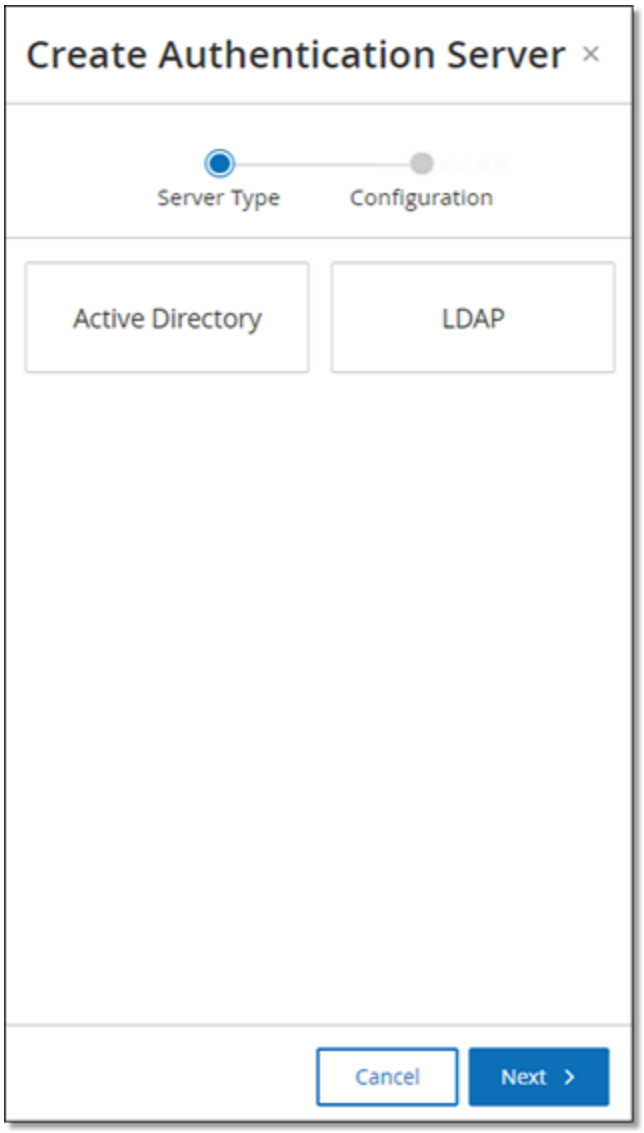
LDAP

OT Security 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 OT Security にログインできるようになります。設定には、統合のセットアップと、AD のグループを OT Security のユーザーグループにマッピングすることが含まれます。

LDAP を設定するには

1. **[ローカル設定]** > **[ユーザー管理]** > **[認証サーバー]** 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] パネルが開き、**[サーバータイプ]** が表示されます。



3. **[LDAP]** を選択してから、**[次へ]** をクリックします。

   [LDAP 設定] ペインが表示されます。

4. **[名前]** ボックスに、ログイン画面で使用する名前を入力します。

   > **注意**: 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 の両方が設定されている場合、ログイン画面の異なる設定を区別するのはログイン名のみです。

5. **[サーバー]** ボックスに、FQDN またはログインアドレスを入力します。

注意: 安全な接続を使用している場合、Tenable は 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。

注意: ホスト名を使用している場合、OT Security 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。[システム設定] > [デバイス] で確認してください。

6. **[ポート]** ボックスに、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。

   注意: 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]** ボックスに、DN を DN 形式のパラメーターを使って入力します。たとえば、adsrv1.tenable.com というサーバー名の場合、ユーザー DN は `CN=Administrator,CN=Users,DC=adsrv1,DC=tenable,DC=com` となります。

8. **[パスワード]** ボックスに、ユーザー DN のパスワードを入力します。

   注意: LDAP を使用した OT Security 設定は、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、OT Security 設定も更新する必要があります。

9. **[ユーザーベース DN]** ボックスに、ベースドメイン名を DN 形式で入力します。たとえば、adsrv1.tenable.com というサーバー名の場合、ユーザーベース DN は `OU=Users,DC=adsrv1,DC=tenable,DC=com` となります。

10. **[グループベース DN]** ボックスに、グループベースドメイン名を DN 形式で入力します。たとえば、adsrv1.tenable.com というサーバー名の場合、グループベース DN は `OU=Groups,DC=adsrv1,DC=tenable,DC=com` となります。

11. **[ドメイン追加]** ボックスに、ユーザーが自分がメンバーとして所属しているドメインを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のボックスに、ユーザーが LDAP 設定で使用する Tenable グループ名を入力します。

13. 設定にポート 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。

OT Security によりサーバーが**無効**モードで起動されます。

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]** をクリックしてすぐに再起動して設定を適用するか、**[後で再起動]** をクリックして新しい設定なしでシステムの使用を一時的に続行します。

    > **注意**: LDAP 設定の有効化 / 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。

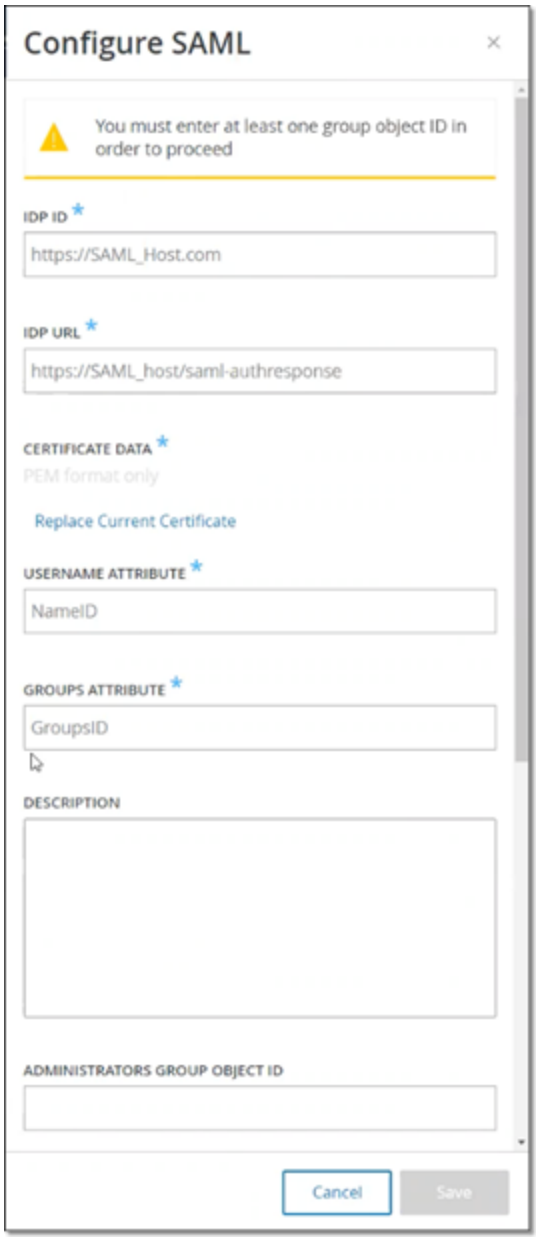
SAML

OT Security 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、ユーザーはアイデンティティプロバイダーを使用して認証を行うことができます。設定では、ID プロバイダー内で OT Security アプリケーションを作成し、作成した OT Security 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 OT Security の **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 OT Security 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。OT Security と Microsoft Azure の統合に関する詳細なチュートリアルについては、付録 – Microsoft Entra ID の SAML 統合を参照してください。

SAML を設定するには

1. **[ローカル設定]** > **[ユーザー管理]** > **[SAML]** に移動します。
2. **[設定]** をクリックします。

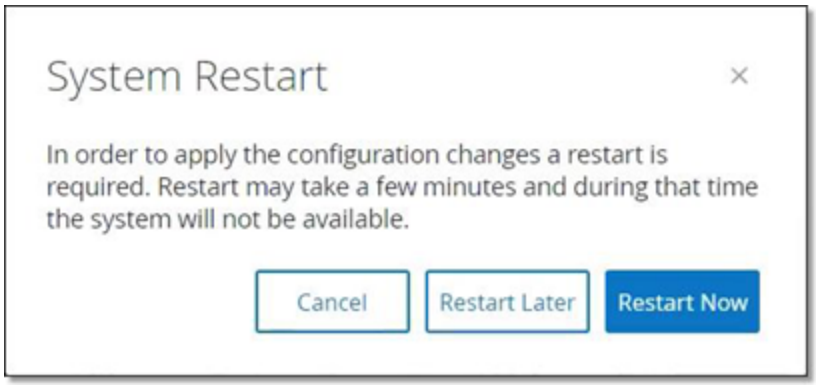
   [SAML の設定] パネルが表示されます。



3. **[IDP ID]** ボックスに、OT Security アプリケーションのアイデンティティプロバイダーの ID を入力します。
4. **[IDP URL]** フィールドに、OT Security アプリケーションのアイデンティティプロバイダーの URL を入力します。
5. **[証明書データ]** で、**[ここにファイルをドロップ]** をクリックし、OT Security 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]** ボックスに、OT Security アプリケーションのアイデンティティプロバイダーのユーザー名属性を入力します。

7. **[グループ属性]** ボックスに、OT Security アプリケーションのアイデンティティプロバイダーのグループ属性を入力します。
8. (オプション) **[説明]** ボックスに説明を入力します。
9. 設定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 OT Security 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]** ウィンドウで **[SAML シングルサインオンログイン]** トグルをクリックして、シングルサインオンログインを有効にします。

    [システムの再起動] 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 設定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 設定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 OT Security に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 OT Security プラットフォームにアクセスできます。

統合

OT Security 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するため、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

OT Security は Tenable Security Center および Tenable Vulnerability Management と統合できます。OT Security は、これらの統合により、他のプラットフォームとデータを共有します。同期されたデータには、OT の脆弱性と、OT Security から開始された IT タイプの Tenable Nessus スキャンによって検出されたデータが含まれます。

注意: OT Security は、統合を介して**非表示**アセットのデータを Tenable Security Center と Tenable Vulnerability Management に送信することはありません。

注意: プラットフォームを統合するには、OT Security がポート 443 を介して Tenable Security Center または Tenable Vulnerability Management にアクセスできる必要があります。Tenable では、Tenable Security Center または Tenable Vulnerability Management で特定のユーザーを作成し、OT Security への統合ユーザーとして使用することを推奨しています。

Tenable Security Center

Tenable Security Center を統合するには、OT Security データを保存する**ユニバーサルリポジトリ**を Tenable Security Center に作成し、リポジトリ ID をメモします。詳細については、ユニバーサルリポジトリを参照してください。

注意: Tenable では、OT Security との統合に使用される特定のユーザーを Tenable Security Center で作成することを推奨しています。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 Security Center を統合するには

1. **[ローカル設定]** > **[統合]** に移動します。

   統合ページが表示されます。

2. 右上の **[統合モジュールの追加]** をクリックします。

   [統合モジュールの追加] パネルが表示されます。

3. **[モジュールタイプ]** セクションで、[Tenable Security Center] を選択します。

4. **[次へ]**をクリックします。

   関連するフィールドを含む**[モジュール定義]**パネルが表示されます。

5. **[ホスト名/IP]**ボックスに、Tenable Security Center のホスト名または IP を入力します。
6. **[ユーザー名]**ボックスに、アカウントのユーザー ID を入力します。
7. **[パスワード]**ボックスにアカウントのパスワードを入力します。
8. **[リポジトリ ID]**に、ユニバーサルリポジトリ ID を指定します。
9. **[同期頻度]**ドロップダウンボックスで、データを同期する頻度を設定します。
10. **[保存]**をクリックします。

    OT Security は統合を作成し、統合ページに新しい統合を表示します。

11. 新しい統合を右クリックし、**[同期]**をクリックします。

Tenable Vulnerability Management

注意: 最初に、Tenable Vulnerability Management 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]**)。統合の設定時に OT Security 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。

Tenable Vulnerability Management を統合するには

1. **[ローカル設定]** > **[統合]**に移動します。

   統合ページが表示されます。

2. 右上の**[統合モジュールの追加]**をクリックします。

   [統合モジュールの追加]パネルが表示されます。

3. **[モジュールタイプ]**セクションで、[Tenable Vulnerability Management]を選択します。
4. **[次へ]**をクリックします。

   関連するフィールドを含む**[モジュール定義]**パネルが表示されます。

5. **[アクセスキー]**ボックスで、アクセスキーを入力します。

6. **[シークレットキー]** ボックスに、秘密鍵を入力します。
7. **[同期頻度]** ドロップダウンボックスで、データを同期する頻度を選択します。

Tenable One

Tenable One と統合するには、Tenable One との統合 の手順に従ってください。

Palo Alto Networks - 次世代ファイヤーウォール(NGFW)

OT Security 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。

OT Security を Palo Alto Networks 次世代ファイヤーウォール(NGFW) と統合するには

1. **[ローカル設定]** > **[統合]** に移動します。

   統合 ページが表示されます。
2. 右上の **[統合モジュールの追加]** をクリックします。

   [統合モジュールの追加] パネルが表示されます。
3. **[モジュールタイプ]** セクションで、[Palo Alto Networks NGFW] を選択します。
4. **[次へ]** をクリックします。
5. **[ホスト名/IP]** ボックスに、Palo Alto NGFW アカウントのホスト名または IP アドレスを入力します。
6. **[ユーザー名]** ボックスに、NGFW アカウントのユーザー名を入力します。
7. **[パスワード]** ボックスに NGFW アカウントのパスワードを入力します。
8. **[保存]** をクリックします。

   OT Security が統合を保存します。

Aruba - ClearPass Policy Manager

OT Security 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。

OT Security を Aruba ClearPass アカウントと統合するには

1. **[ローカル設定]** > **[統合]** に移動します。

   統合 ページが表示されます。

2. 右上の **[統合モジュールの追加]** をクリックします。

   [統合モジュールの追加] パネルが表示されます。

3. **[モジュールタイプ]** セクションで、[Aruba Networks ClearPass] を選択します。

4. **[次へ]** をクリックします。

5. **[ホスト名/IP]** ボックスに、Aruba Networks ClearPass アカウントのホスト名または IP アドレスを入力します。

6. **[ユーザー名]** ボックスに、Aruba Networks ClearPass アカウントのユーザー名を入力します。

7. **[パスワード]** ボックスに Aruba Networks ClearPass アカウントのパスワードを入力します。

8. **[クライアント ID]** ボックスに Aruba Networks ClearPass アカウントのクライアント ID を入力します。

9. **[API クライアントシークレット]** ボックスに Aruba ClearPass アカウントの API クライアントシークレットを入力します。

10. **[保存]** をクリックします。

    OT Security が統合を保存します。

Tenable One との統合

OT Security を Tenable One と統合して、資産とリスクスコアのデータを Tenable Vulnerability Management に送信できます。Tenable One と統合するには、まず Tenable Vulnerability Management でリンクキーを生成して、それを OT Security に提供する必要があります。Tenable One は、前回の同期以降に行われた資産の変更により、定期的に更新されます。

始める前に

- Tenable Vulnerability Management でリンクキーが生成されていることを確認します。詳細については、Tenable Vulnerability Management ユーザーガイドの OT コネクタを参照してください。

  注意: Tenable Vulnerability Management 内で生成されたリンクキーは、単一の OT Security サイトに対してのみ使用できます。

Tenable One との統合手順

1. **[ローカル設定]** > **[統合]** に移動します。

   統合ページが表示されます。

2. 右上の **[統合モジュールの追加]** をクリックします。

   [統合モジュールの追加] パネルが表示されます。

3. **[モジュールタイプ]** セクションで、[**Tenable One**] をクリックします。

4. **[次へ]** をクリックします。

   [モジュール定義] セクションが表示されます。

5. **[クラウドサイト]** ボックスにクラウドサイト名を入力します。

   > **注意**: リンクキーを生成した後、クラウドサイト名が Tenable Vulnerability Management の **[OT コネクタの追加]** ウィンドウに表示されます。

6. **[リンクキー]** ボックスに、Tenable Vulnerability Management から生成したリンクキーを入力します。

7. **[保存]** をクリックします。

   OT Security に統合が成功したことを示すメッセージが表示されます。統合が完了すると、**統合**ページでリンクされたサイトを表示できます。Tenable One では、**[センサー]** > **[OT コネクタ]** ページに、OT Security でそのサイト用に設定されたデバイス名が表示されます。

   サイトのデバイス名については、**[システム設定]** > **[デバイス]** ページの **[デバイス名]** セクションを参照してください。

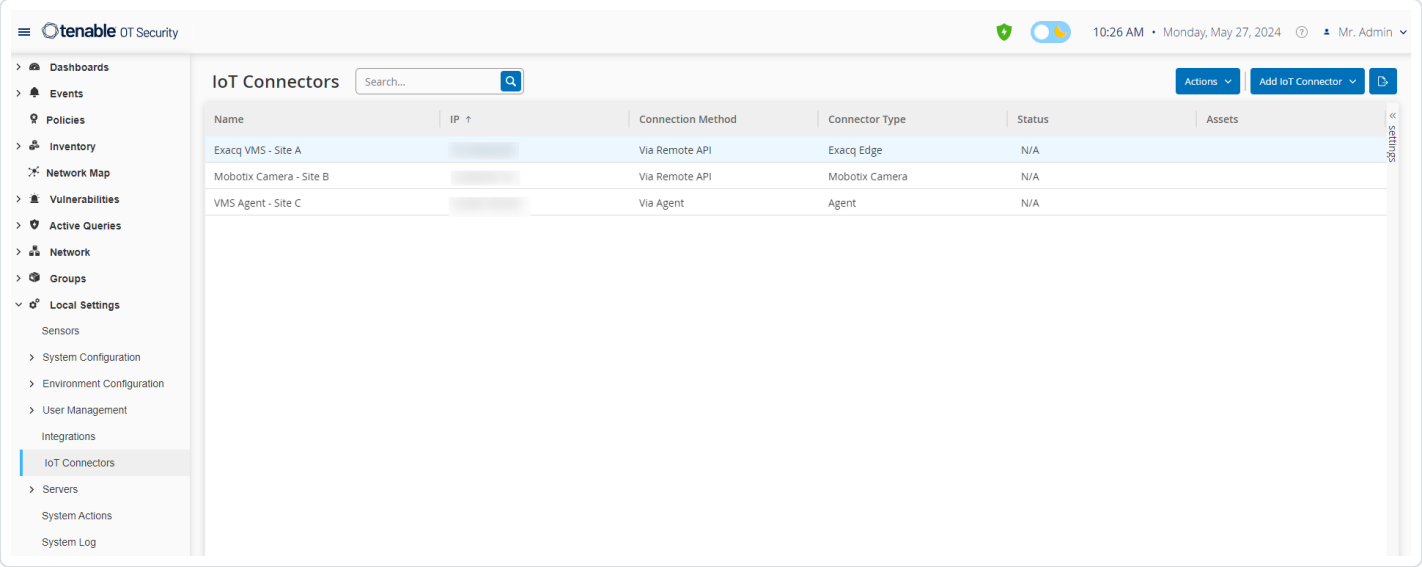
   > **注意**: 既にペアリングされているサイトの名前を OT Security で変更した場合、センサー名を新しいサイト名と一致するよう Tenable Vulnerability Management 内で手動で変更できます。または、OT Security と Tenable Vulnerability Management の両方で統合を削除し、再度ペアリングすればサイト名の変更を自動的に更新できます。

Tenable One の Tenable OT Security をデプロイしてライセンスを付与する全手順については、Tenable One デプロイメントガイドを参照してください。

IoT コネクタ

OT Security では、IoT コネクタエンジンを設定し、特定のアプリケーションサーバーから資産を同期することで、管理されているモノのインターネット (IoT) のすべてのデバイスを特定のアプリケーションサーバーにマッピングできます。

たとえば、IP カメラの場合、それを管理するビデオ管理システム (VMS) サーバーが表示されます。OT Security の **[インベントリ]** ページで、VMS アプリケーションサーバーに移動すると、**[インベントリ]** > **[関連資産]** ページに、そのサーバーが管理しているすべてのカメラが表示されます。



注意: デフォルトでは、IoT コネクタから資産をインポートする場合、OT Security はデバイスの MAC アドレスとともに IP アドレスをインポートします。MAC アドレスのみをインポートするには、**[ローカル設定]** > **[環境設定]** > **[資産設定]** に移動し、**[IoT 資産の IP アドレスをフェッチ]** オプションを無効にします。

IoT コネクタエンジン

OT Security には、ご使用の IoT/VMS サーバーと統合できる IoT コネクタエンジンが含まれています。

このエンジンは 2 つの接続方法をサポートしています。リモートアプリケーション API サービス経由の認証とエージェント経由の接続です。アプリケーションサーバーとエンジンを統合すると、OT Security は、カメラ、バッジアクセスシステム、火災パネルなど、アプリケーションサーバーが管理するすべてのデバイスをインポートします。

IoT コネクタを追加する

リモート API サービスかエージェントを使用して、IoT コネクタを OT Security と統合できます。

始める前に

- (**エージェント経由の接続の場合のみ**) アプリケーションサーバーに OT Security IoT コネクタエージェントがインストールされていることを確認します。詳細は、Windows での IoT コネクタエージェントのインストールを参照してください。

1. 左側のナビゲーションバーで、**[ローカル設定]** > **[IoT コネクタ]** に移動します。

   [IoT コネクタ] ページが表示されます。

2. 右上の **[IoT コネクタの追加]** をクリックします。

   ドロップダウンメニューが表示されます。

3. 次のいずれかのオプションを選択します。

   - **エージェント経由**

     1. **[コネクタ名]** ボックスに、コネクタの名前を入力します。
     2. **[IP]** ボックスに、追加するコネクタの IP アドレスを入力します。
     3. **[保存]** をクリックします。

        注意: アプリケーションサーバーに OT Security IoT コネクタエージェントがインストールされていない場合、接続は失敗し、OT Security はエラーメッセージを表示します。

   - **リモート API 経由**

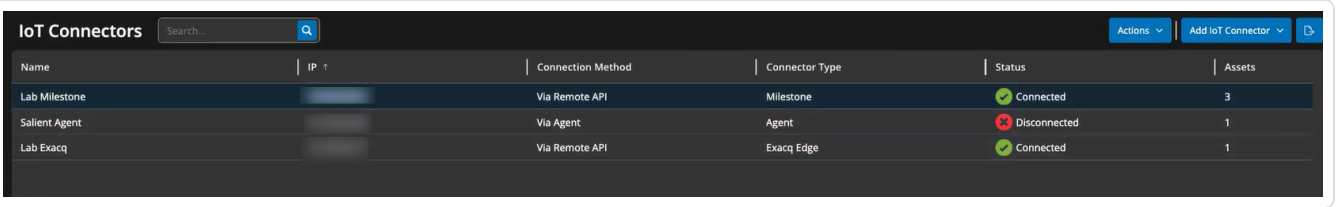
     1. **[コネクタタイプ]** セクションで、追加する IoT コネクタを選択します。
     2. **[次へ]** をクリックします。

        [コネクタの詳細] セクションが表示されます。

     3. **[コネクタ名]** ボックスに、コネクタの名前を入力します。
     4. **[IP]** ボックスに、コネクタの IP アドレスを入力します。
     5. **[ポート]** ボックスに、OT Security が接続に使用するポート番号を入力します。デフォルトのポート番号は 22609 です。

6. **[ユーザー名]** ボックスに、コネクタへのログインに使 用するユーザー名を入 力します。
7. **[パスワード]** ボックスに、コネクタのパスワードを入 力します。
8. **[保 存]** をクリックします。

OT Security によってコネクタが保 存され、**[IoT コネクタ]** ページに表 示されます。



IoT コネクタにリンクされた資 産を表 示する

アプリケーションサーバーに接 続すると、アプリケーションサーバーによって管 理されている関 連する資 産 やサービスを表 示できます。

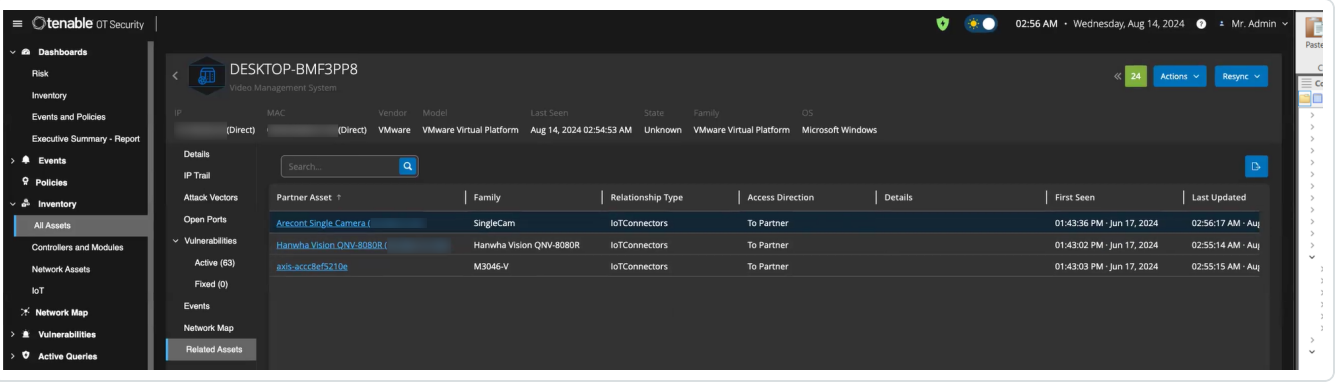
サーバーによって管 理されているすべてのデバイスを表 示する方 法

1. **[インベントリ]** > **[すべての資 産]** に移 動します。

   [すべての資 産] ページが表 示されます。

2. **[検 索]** ボックスを使 用して、アプリケーションサーバーを検 索します。

   選 択したアプリケーションサーバーのページが、管 理するデバイスのリストとともに表 示されます。



IoT 接 続をテストする

IoT コネクタを追 加 後 、OT Security が到 達できるかどうかをテスト できます。

1. [IoT コネクタ] テーブルで、次のいずれかを実行します。

   - テストする IoT コネクタの行を右クリックし、**[テスト接続]** を選択します。
   - テストする IoT コネクタを選択し、**[アクション]** > **[テスト接続]** をクリックします。

   OT Security は、テストを実行してコネクタに到達できるかどうかを検証します。

IoT コネクタを編集する

1. [IoT コネクタ] テーブルで、次のいずれかを実行します。

   - 編集する IoT コネクタの行を右クリックし、**[編集]** を選択します。
   - 編集する IoT コネクタを選択し、**[アクション]** > **[編集]** をクリックします。

   [エージェント/リモート API 経由で IoT コネクタを編集] パネルが表示されます。

2. 必要に応じて詳細を変更します。
3. **[保存]** をクリックします。

   OT Security が IoT コネクタの更新内容を保存します。

IoT コネクタを削除する

1. [IoT コネクタ] テーブルで、次のいずれかを実行します。

   - 削除する IoT コネクタの行を右クリックし、**[削除]** を選択します。
   - 削除する IoT コネクタを選択し、**[アクション]** > **[削除]** をクリックします。

   OT Security は IoT コネクタを削除します。

   > **注意**: IoT コネクタを削除すると、OT Security はアプリケーションサーバーから IoT コネクタエージェントをアンインストールします。アプリケーションサーバーをエージェント経由で接続するには、OT Security IoT コネクタエージェント を再インストールする必要があります。

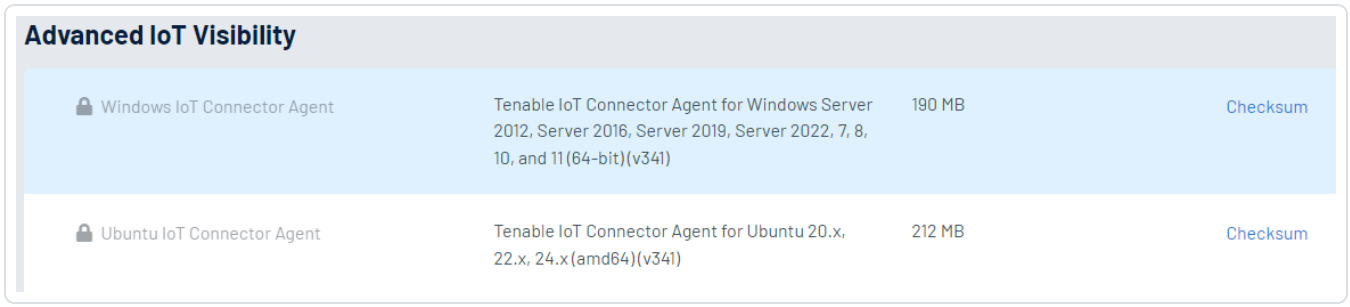
Windows での IoT コネクタエージェントのインストール

> **必要なロール**: 管理者

OT Security では、IoT コネクタエンジンを設定し、特定のアプリケーションサーバーから資産を同期することで、管理されているモノのインターネット (IoT) のすべてのデバイスを特定のアプリケーションサーバーにマッピングできます。アプリケーションサーバーをエージェント経由で接続するには、OT Security IoT コネクタエージェントをインストールする必要があります。

OT Security IoT コネクタエージェントをインストールするには

1. [Tenable ダウンロード] ページにログインします。
2. **OT Security** ページに移動します。
3. **[高度な IoT の可視性]** セクションから、**Windows IoT コネクタエージェント** パッケージをダウンロードします。



4. ダウンロードした **Windows IoT コネクタエージェント** パッケージを、インストールするアプリケーションサーバーにコピーします。
5. **[Tenable IoT コネクタエージェント]** ウィザードを実行します。

   コネクタエージェント ウィザードが初期化中であることを示すメッセージが表示され、**[Tenable IoT コネクタエージェントのセットアップウィザードにようこそ]** ウィンドウが表示されます。
6. **[次へ]** をクリックします。

   [ライセンス契約] ウィンドウが表示されます。
7. **[契約に同意します]** を選択し、**[次へ]** をクリックします。

   [宛先ディレクトリを選択] ウィンドウが表示されます。
8. IoT コネクタエージェントをインストールするディレクトリを指定し (またはデフォルトのディレクトリを使用)、**[次へ]** をクリックします。

   Tenable IoT コネクタエージェントのインストールが開始されます。

9. インストールが完了したら、Tenable IoT コネクタエージェント サービスが実行されていることを確認します。

   a. **[実行]** コマンドウィンドウで、`services.msc` と入力します。

      [サービス] ウィンドウが開きます。

   b. 現在実行中のサービスのリストに **OT Security IoT コネクタエージェント** が表示されていることを確認します。

インストールが完了したら、アプリケーションサーバーを OT Security に接続できます。リモート エージェントを介してアプリケーションサーバーに接続する方法の詳細については、エージェント経由で IoT コネクタを追加するを参照してください。

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 E 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、OT Security 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。

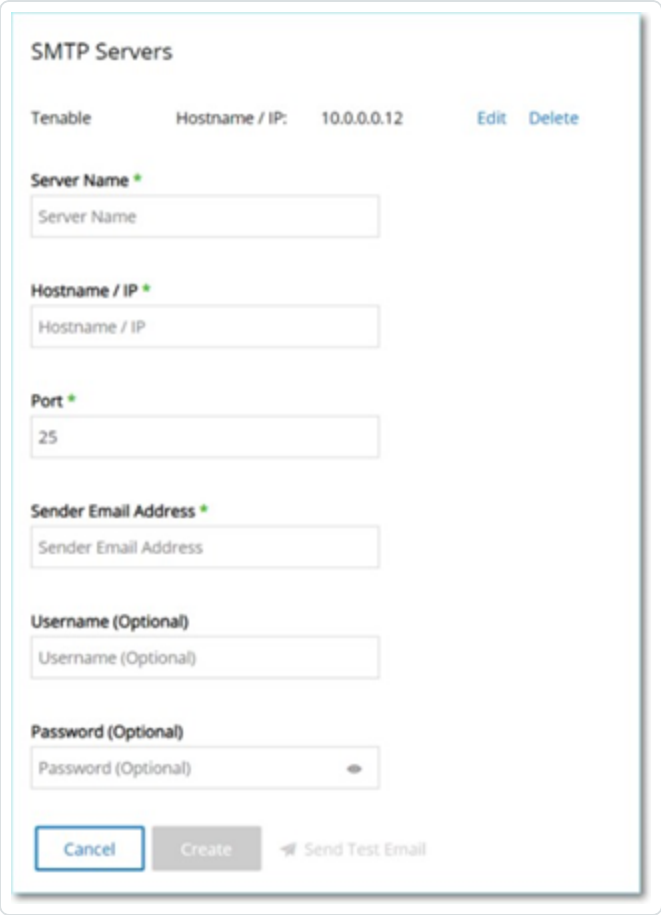
SMTP サーバー

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、イベントが生成されるたびにメール通知を送信することはできません。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(ユーザーインターフェース) で表示できます。

SMTP サーバーの設定手順

1. **[ローカル設定]** > **[サーバー]** > **[SMTP サーバー]** 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] 設定ウィンドウが表示されます。



3. **[サーバー名]** ボックスに、E メール通知に使用する SMTP サーバーの名前を入力します。
4. **[ホスト名 \IP]** ボックスに、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]** ボックスに、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]** ボックスに、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. (オプション) **[ユーザー名]** ボックスと **[パスワード]** ボックスに、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。
8. テスト E メールを送信して設定が正しく行われたことを確認するには、**[テスト E メールの送信]** をクリックし、送信先の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。

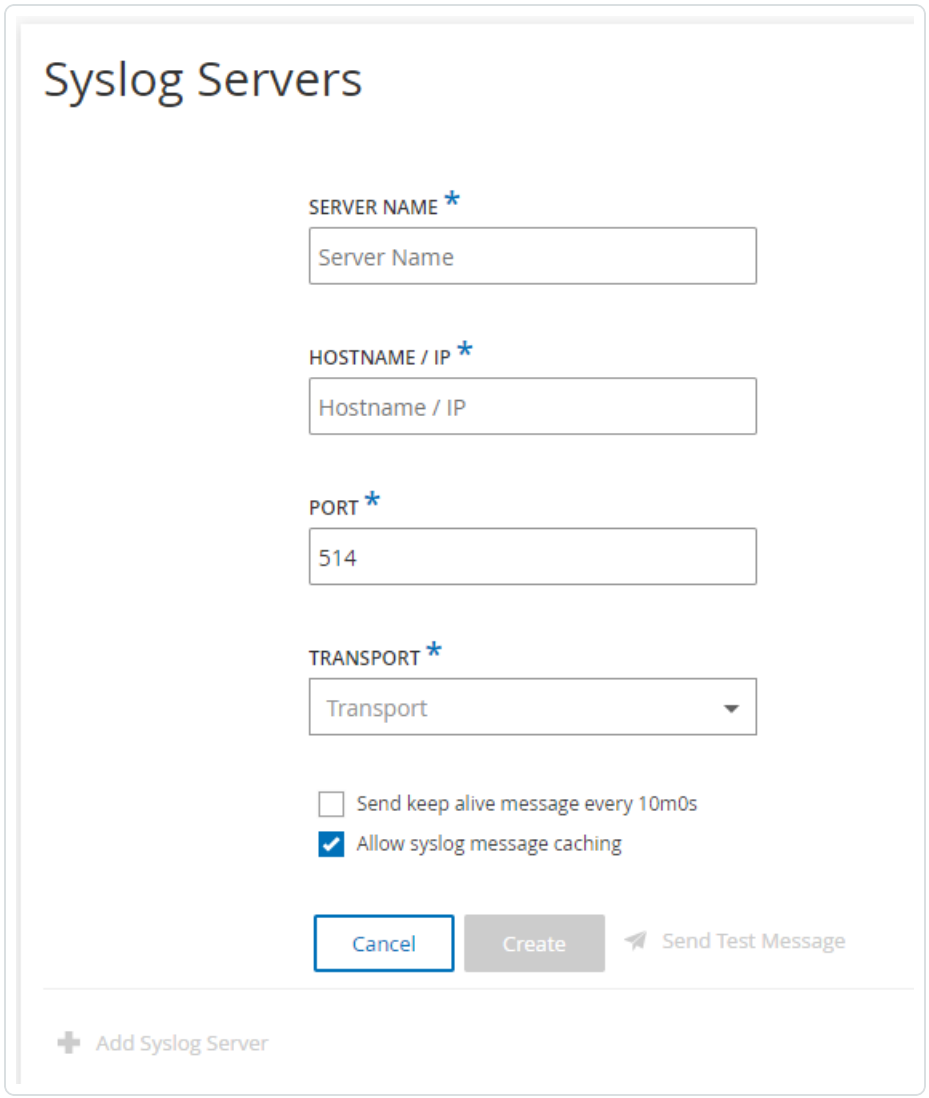
追加の SMTP サーバーを設定するには、この手順を繰り返します。

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、システムで 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 OT Security プラットフォームのみに保存されます。

Syslog サーバーの設定手順

1. **[ローカル設定]** > **[サーバー]** > **[Syslog サーバー]** 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]** 設定ウィンドウが表示されます。



3. **[サーバー名]** ボックスに、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]** ボックスに、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]** ボックスに、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]** ドロップダウンボックスで、使用するトランスポートプロトコルを選択します。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設定が成功したことを確認するには、**[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. (オプション) 接続を頻繁にチェックするには、**[10 分ごとにキープアライブメッセージを送信する]** オプションを選択します。
9. (オプション) TCP syslog の場合、**[syslog メッセージのキャッシュを許可する]** オプションを選択して、接続が中断したときにイベントをキャッシュし、接続が復元されたらイベントを送信します。

   > **注意**: UDP syslog メッセージには状態の認識がなく、接続が中断された場合に失われる可能性があります。

10. **[保存]** をクリックします。

    追加の Syslog サーバーを設定するには、この手順を繰り返します。

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]** > **[サーバー]** > **[FortiGate ファイヤーウォール]** に移動します。
2. **[ファイヤーウォールの追加]** をクリックします。

   [FortiGate ファイヤーウォールの追加] 設定ウィンドウが表示されます。

3. **[サーバー名]** ボックスに、使用する FortiGate サーバーの名前を入力します。
4. **[ホスト名/IP]** ボックスに、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]** ボックスに、FortiGate から生成した API トークンを入力します。

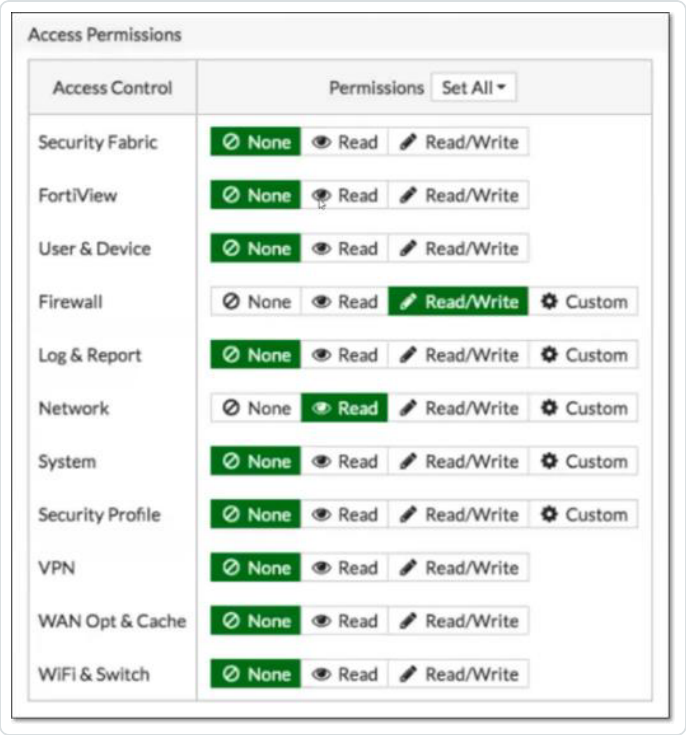
   注意: FortiGate API トークンを生成する手順については、次のページを参照してください。
   https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token

6. **[追加]** をクリックします。

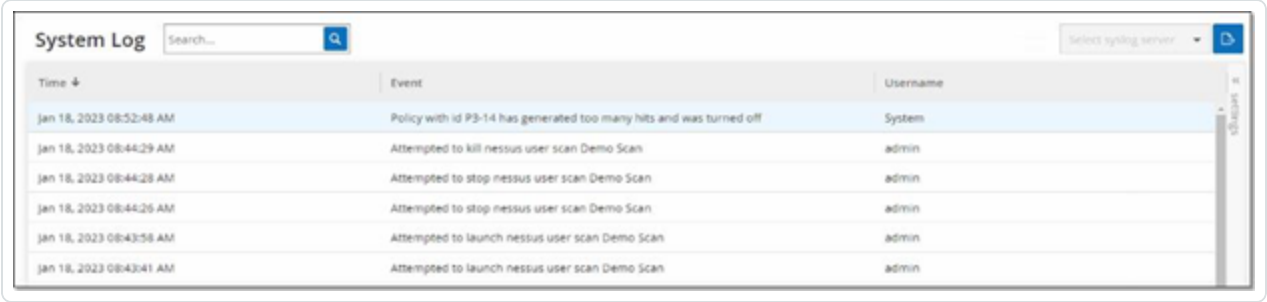
   OT Security により FortiGate ファイヤーウォールサーバーが作成されます。

   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、OT Security ユニットの IP アドレスを使用してください。

   OT Security 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許可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設定することもできます。

ログに記録された各イベントには、次の詳細が含まれています。

パラメーター	説明

時刻	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設定する手順

1. **[ローカル設定]** > **[システムログ]** に移動します。
2. 右上のドロップダウンボックスをクリックしてサーバーのリストを表示します。

   注意: 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。

   OT Security により、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 – Microsoft Entra ID の SAML 統合

OT Security では、SAML プロトコルを使用した Microsoft Entra ID との統合がサポートされています。これにより、OT Security に割り当てられていた Azure ユーザーが、SSO を介して OT Security 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、OT Security でロールを割り当てることができます。

このセクションでは、OT Security と Microsoft Entra ID のシングルサインオン (SSO) 統合を設定するフロー全体について説明します。この設定では、Microsoft Entra ID で OT Security アプリケーションを作成し、作成した OT Security アプリケーションに関する情報を入力し、アイデンティティプロバイダーの証明書を OT Security SAML ページにアップロードし、アイデンティティプロバイダーのグループを OT Security 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。

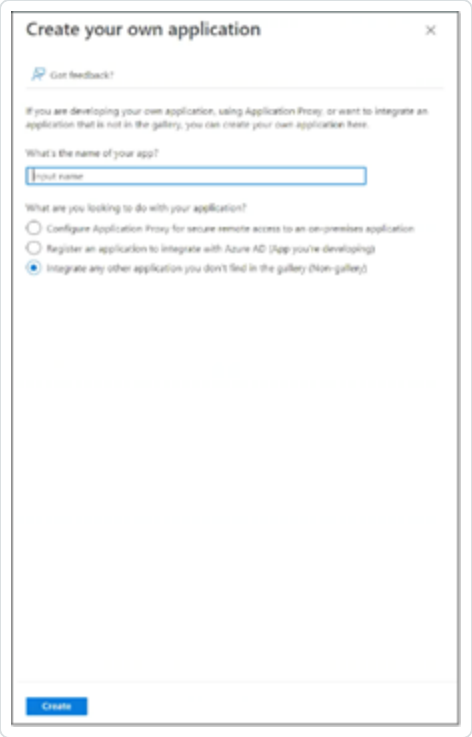
この設定を行うには、Microsoft Entra ID と OT Security の両方に管理ユーザーとしてログインする必要があります。

手順 1 - Microsoft Entra ID で Tenable アプリケーションを作成する

Microsoft Entra ID での Tenable アプリケーションの作成手順

1. Microsoft Entra ID で、[Microsoft Entra ID] > **[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 **[Microsoft Entra ID 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. **[アプリケーションの名前]** 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。

手順 2 - 初期設定を行う

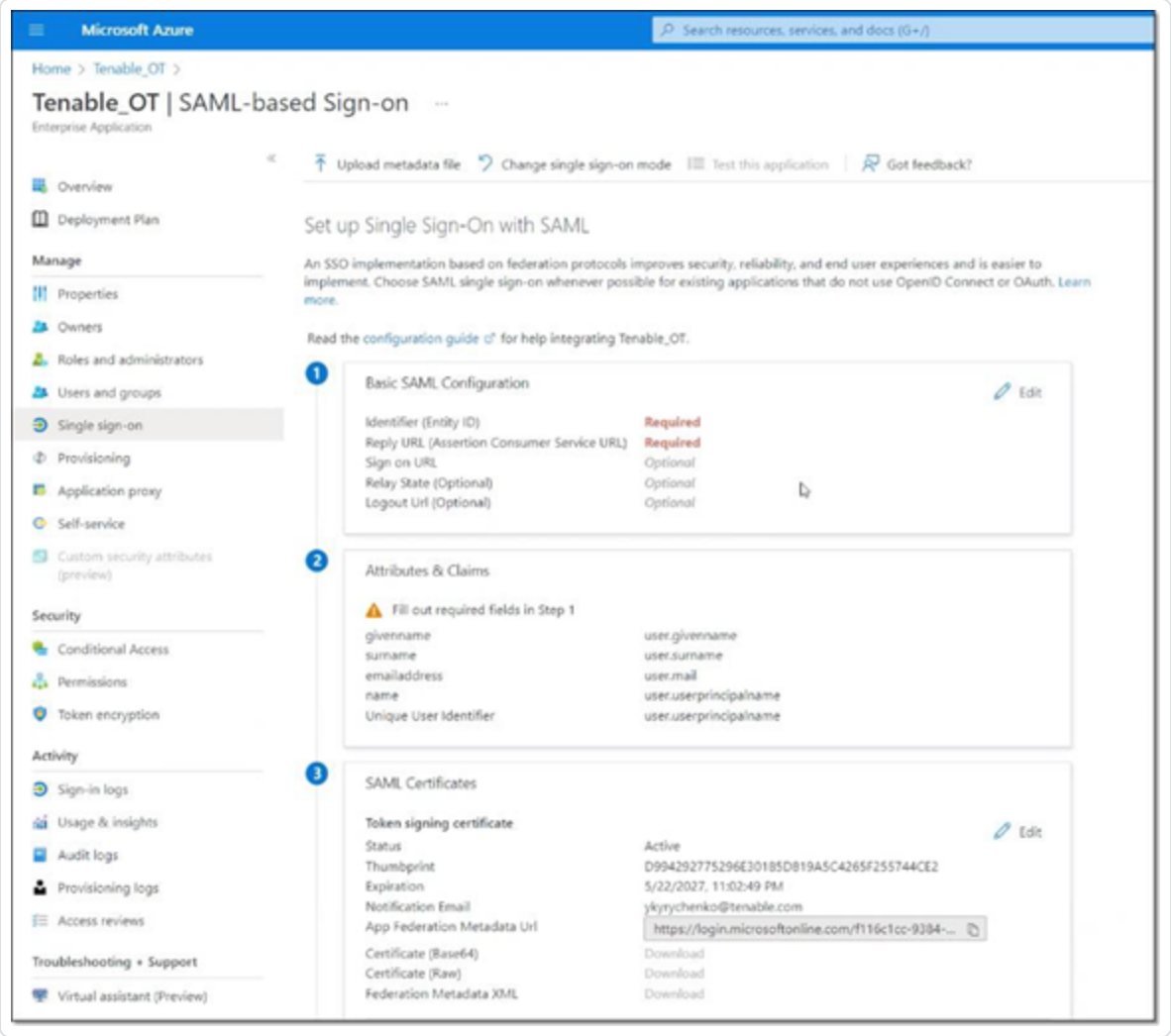
この手順では Azure の OT Security アプリケーションの初期設定を行います。必要な証明書のダウンロードを可能にするために、[基本 SAML 設定] の値の識別子および応答 URL の一時的な値を作成します。

> **注意**: この手順で指定されているフィールドのみを設定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。

初期設定の手順

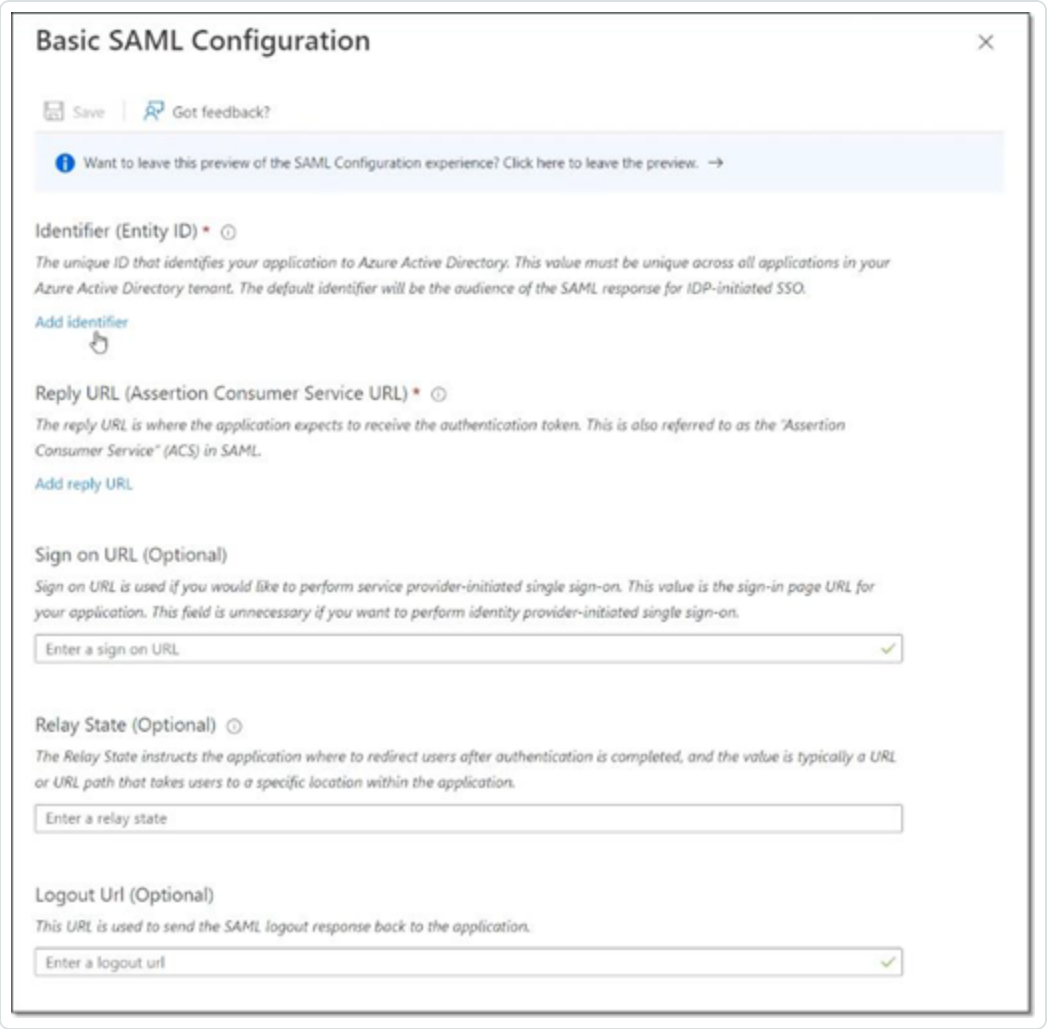
1. Microsoft Entra ID ナビゲーションメニューで、**[シングルサインオン]** をクリックし、シングルサインオンの方法として [SAML] を選択します。

   [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 の **[基本 SAML 設定]** で、 [編集] をクリックします。

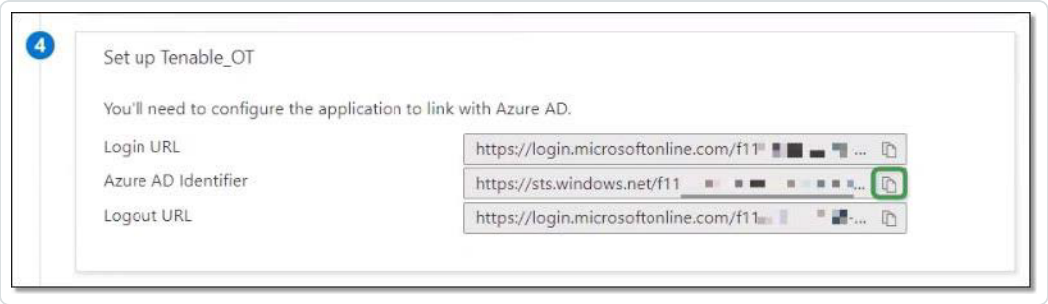
   [基本 SAML 設定] サイドパネルが表示されます。



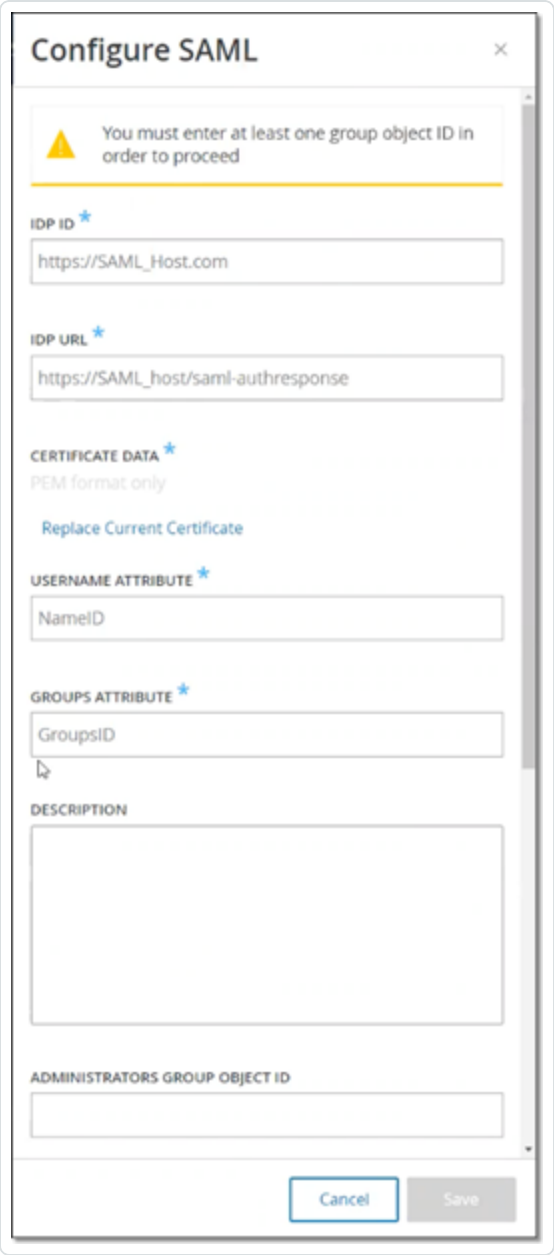
3. **[識別子 (エンティティ ID)]** フィールドに、Tenable アプリケーションの一時 ID (tenable_ot など) を入力します。
4. **[応答 URL (アサーションコンシューマサービス URL)]** フィールドに、有効な URL (例: https://OT Security) を入力します。

   注意: 識別子と応答 URL のどちらも、この後の設定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 設定]** サイドパネルを閉じます。
6. セクション 4 の **[セットアップ]** で、**[コピー]** アイコンをクリックして **[Microsoft Entra ID 識別子]** をコピーします。



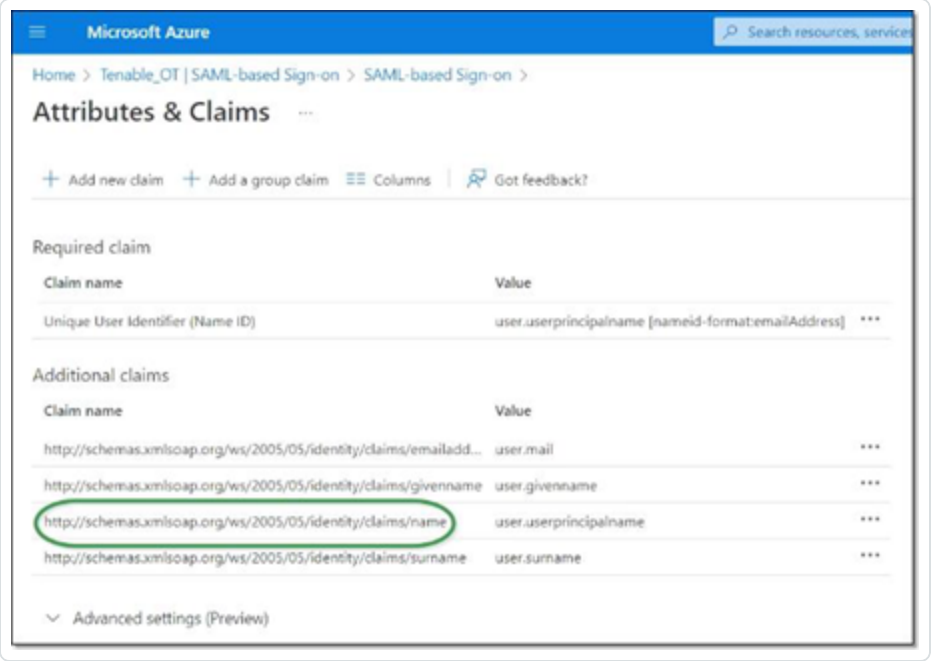
7. OT Security コンソールに切り替え、**[ユーザーとロール]** > **[SAML]** に移動します。
8. **[設定]** をクリックして **[SAML の設定]** サイドパネルを表示し、コピーした値を **[IDP ID]** フィールドに貼り付けます。



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. **OT Security** 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 の **[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. **OT Security** 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。

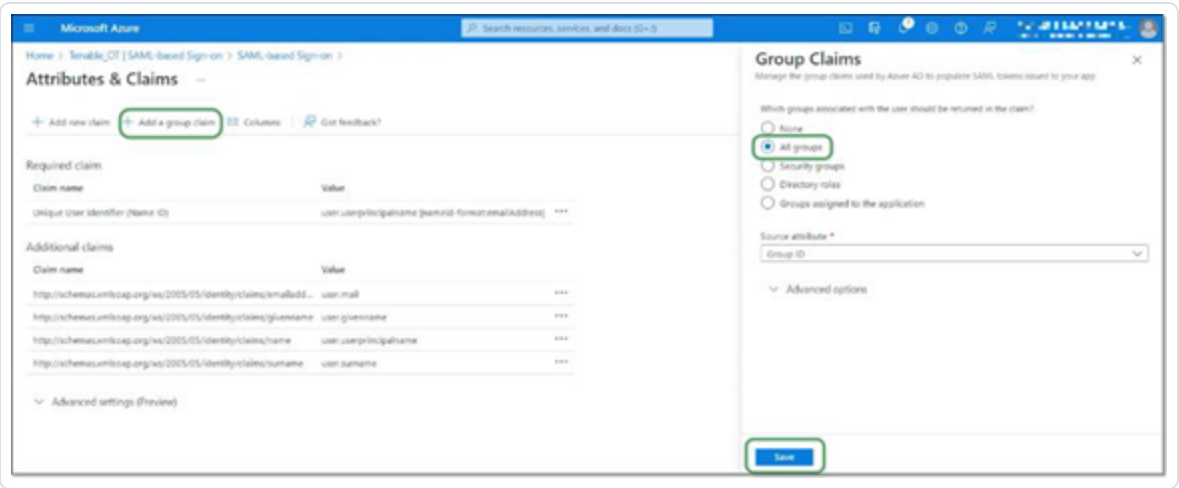
13. **Azure** コンソールのセクション 2 の **[属性とクレーム]** で、 **[編集]** をクリックします。

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。



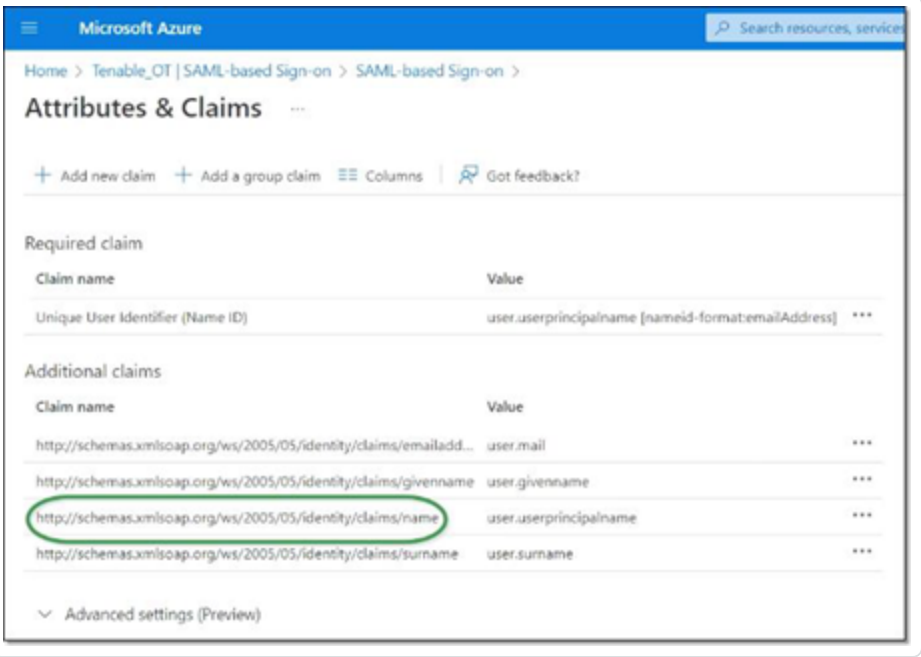
15. **Tenable** コンソールに戻り、この URL を **[ユーザー名属性]** フィールドに貼り付けます。

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。



注意: 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]** の 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 設定の説明を追加する場合は、**[説明]** フィールドに入力します。

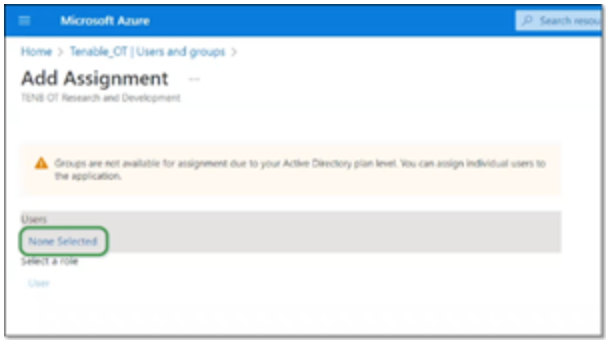
手順 3 - Azure ユーザーを Tenable グループにマッピングする

この手順では、Microsoft Entra ID ユーザーが OT Security 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 OT Security 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。OT Security 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。詳細は、ユーザーとロールを参照してください。各 Azure ユーザーは、OT Security 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。

注意: 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、それらの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 OT Security にマッピングする手順

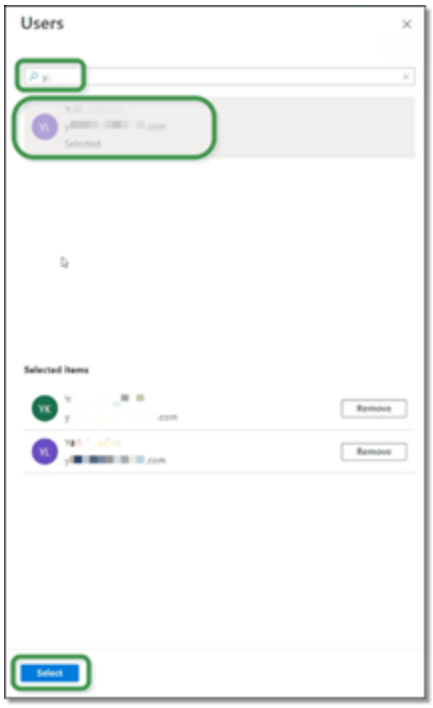
1. **Microsoft Azure** で、**[ユーザーとグループ]** ページに移動し、**[+ ユーザー/グループの追加]** をクリックします。
2. **[割り当ての追加]** 画面の **[ユーザー]** で、**[選択なし]** をクリックします。



[ユーザー] サイドパネルが表示されます。

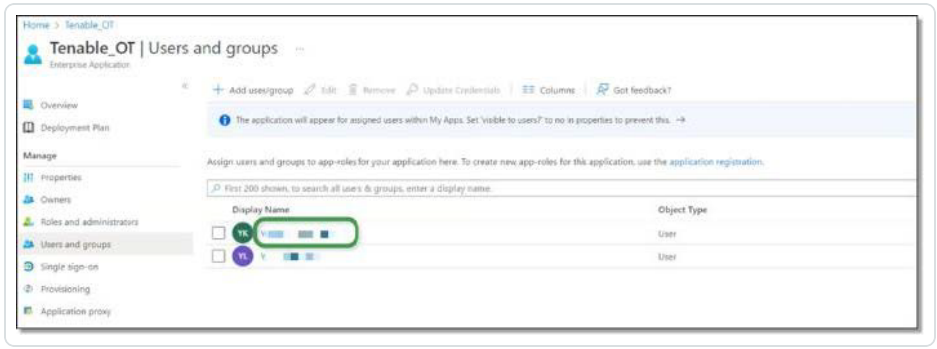
注意: Microsoft Azure でグループ設定が有効になっていて、[すべてのグループ] ではなく **[アプリケーションに割り当てられているグループ]** を以前に選択していた場合は、個々のユーザーではなくグループを割り当てることができます。

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。



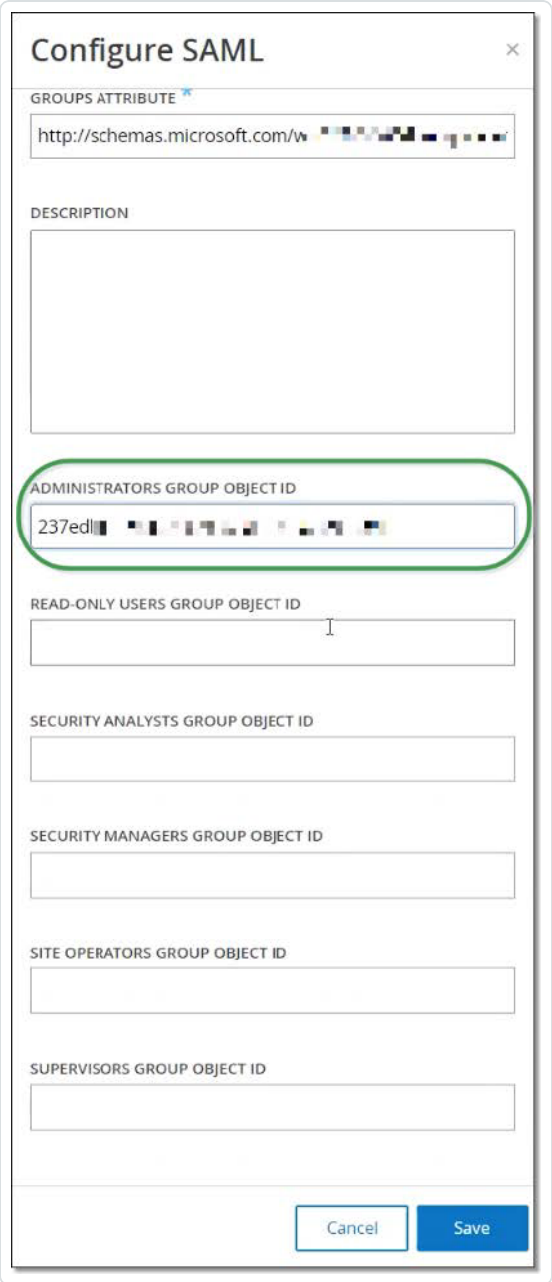
[ユーザーとグループ] ページが表示されます。

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)のプロフィールを表示します。

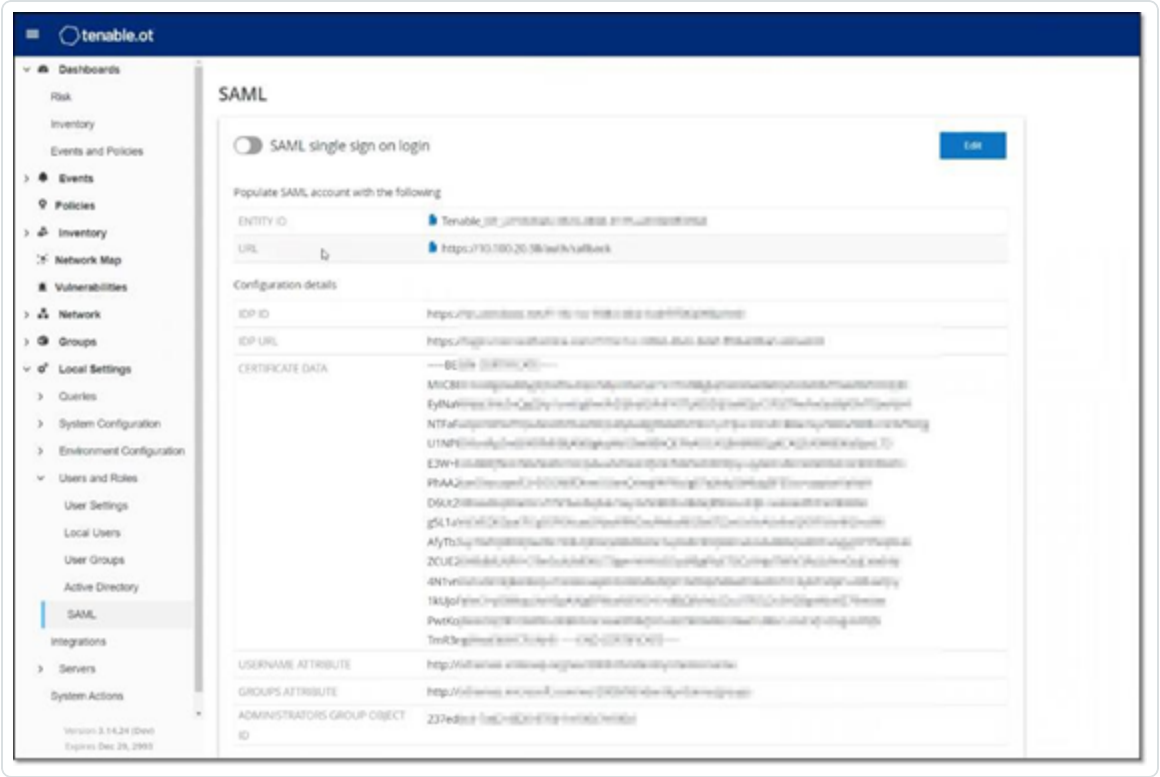


5. **[プロフィール]** 画面の左側のナビゲーションバーで、**[グループ]** を選択して **[グループ]** 画面を表示します。
6. **[オブジェクト ID]** で、Tenable にマッピングされるグループの値をハイライト表示してコピーします。

7. **OT Security** 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. OT Security のそれぞれのユーザーグループにマッピングする各グループで、手順 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。



OT Security コンソールに[SAML]画面が表示され、この画面に設定された情報が表示されます。



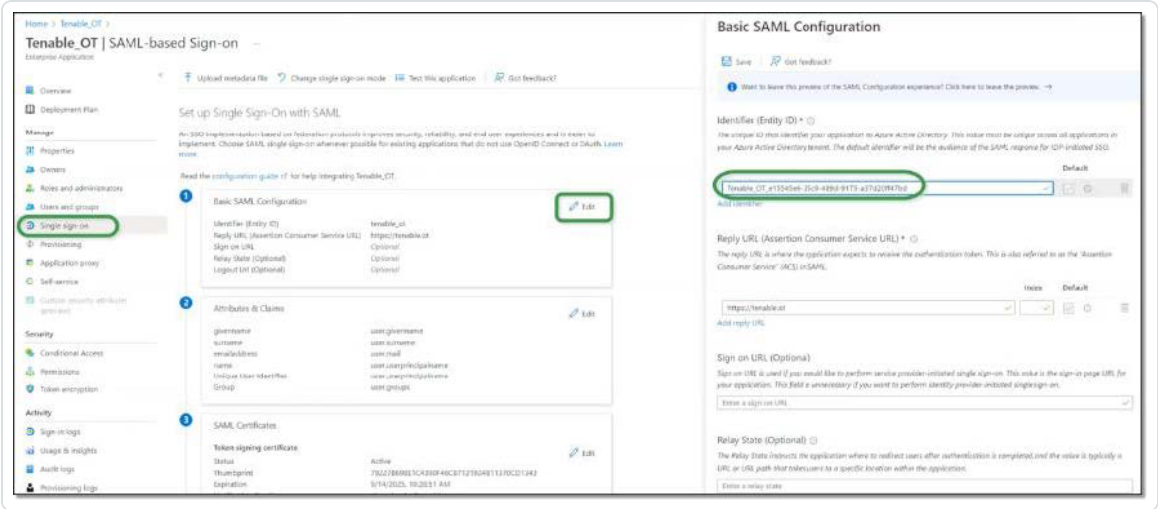
手順 4 - Azure で設定を終了する

Azure で設定を終了する手順

1. OT Security 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 の **[基本 SAML 設定]** 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. OT Security 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 設定]** 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]** をクリックして設定を保存し、サイドパネルを閉じます。

   設定が完了し、接続が **[Azure Enterprise アプリケーション]** 画面に表示されます。

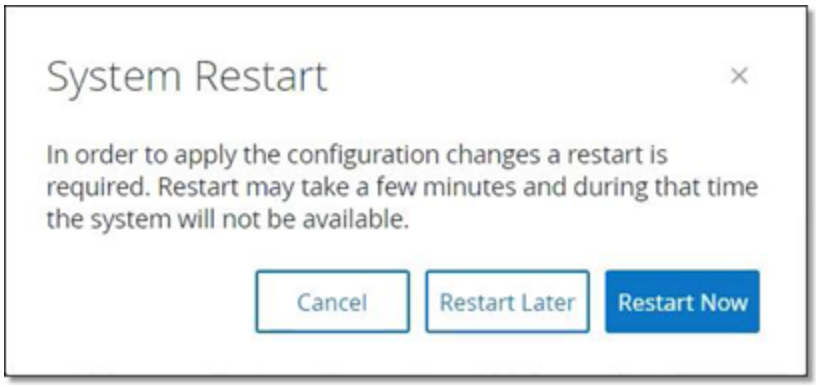
手順 5 - 統合をアクティブ化する

SAML 統合をアクティブ化するには、OT Security 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. OT Security 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。

   [システムの再起動] 通知ウィンドウが表示されます。



2. **[今すぐ再起動]** をクリックしてシステムを再起動し、SAML 設定をすぐに適用するか、**[後で再起動]** をクリックして、次にシステムを再起動したときに SAML 設定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、**OT Security** 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。OT Security 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 OT Security にログインできます。

SSO を使用したサインイン手順

1. **OT Security** 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、OT Security 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、そこでログインに使用するアカウントを選択できます。

改訂履歴

製品バージョン: OT Security 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
2.9	2023 年 7 月 25 日	バージョン 3.16 用に更新
3.0	2023 年 9 月 11 日	バージョン 3.17 用に更新
3.1	2024 年 3 月 15 日	バージョン 3.18 用に更新
3.2	2024 年 7 月 30 日	バージョン 3.19 用に更新