Tenable OT Security 4.6 ユーザーガイド

最終更新日: 2026 年 5 月 11 日

Copyright © 2026 Tenable, Inc.All rights reserved.Tenable、Tenable Nessus、Tenable Lumin、Assure、および Tenable のロゴは、Tenable, Inc.またはその関連会社の登録商標です。その他のすべての製品またはサービスは、それぞれの所有者の商標です。

目次

Tenable OT Security にようこそ **24**

OT Security を使い始める 25

OT Security テクノロジー 25

ソリューションアーキテクチャ 26

OT Security プラットフォームコンポーネント 26

ネットワークコンポーネント 27

Tenable OT Security のハードウェア仕様 28

ICP とセンサーの仕様 28

通常の ICP 28

XL ICP 29

ICP-Mini 31

センサー 32

システム要素 33

資産 33

ポリシーとイベント 33

ポリシーベースの検出 34

異常検出 35

ポリシーカテゴリ 35

グループ 36

イベント 37
OT Security ライセンスコンポーネント 37
Tenable OT Security のライセンシング 37
資産のカウント方法 38
Tenable OT Security コンポーネント 38
ライセンスの流用 39
ライセンス制限の超過 39
期限切れのライセンス 39
運用プレイブック 40
前提条件 40
運用ワークフロー 41
脆弱性の優先順位付けと軽減策 41
目的 41
前提条件 41
ステップ 1: リスクダッシュボードを表示する 41
ステップ 2: 深刻度と資産重要度で優先順位を付ける 42
ステップ 3: 修正オプションを分析する 43
結果 45
ネットワーク脅威に対する調査と対応 45
目的 45
前提条件 45

ステップ 1: イベントアラートをモニタリングする 45
ステップ 2: 対話データを分析する 46
ステップ 3: 対応を開始する 47
結果 48
エラーメッセージ 48
OT Security を使い始める 67
前提条件のチェック 68
OT Security ICP のインストール 69
OT Security の使用 70
OT Security の Tenable One への拡張 70
前提条件 74
ハードウェア要件 74
仮想アプライアンス要件 75
ライセンス要件 75
システム要件 75
OT Security ハードウェア要件 77
OT Security 仮想ハードウェア要件 77
OT Security 仮想センサーの要件 77
ストレージ要件 77
ディスク容量要件 78
ICP システム要件のガイドライン 78

ディスクパーティション要件 79
ネットワークインターフェースの要件 80
NIC の要件 80
アクセス要件 81
インターネット要件 81
ポート要件 82
受信トラフィック 82
送信トラフィック 83
ネットワークに関する考慮事項 83
管理とアクティブクエリのインターフェース 83
管理ロールとアクティブクエリロールの分離 (ポート分割) 84
モニタリングインターフェース 84
ファイヤーウォールに関する考慮事項 84
OT Security Core プラットフォーム 85
OT Security センサー 87
アクティブクエリ 88
OT Security の統合 94
OT エージェント 94
IoT コネクタエージェント 94
OT Security ICP のインストール 95
OT Security ICP ハードウェアアプライアンスのインストール 95

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 97
OT Security ICP 仮想アプライアンスのインストール 104
OT Security のネットワーク接続 106
管理とアクティブクエリ 106
ネットワークモニタリング 106
OT Security ICP の設定 107
Tenable Core のセットアップ 108
Tenable Core ユーザーインターフェースを使う初期設定 108
CLI を使う初期設定 (オプション) 112
Tenable Core への OT Security のインストール 121
セットアップウィザードを使用した OT Security の設定 128
OT Security 管理コンソールへのログイン 129
ユーザー情報 132
デバイス 134
接続して管理とアクティブクエリのポート分割を設定する 135
OT Security ライセンスのアクティベーション 136
OT Security ライセンスのアクティブ化 137
ライセンスをアップデートする 140
ライセンスをオフラインモードでアップデートする 147
ライセンスを再初期化する 153
OT Security の起動 155

OT Security システムの有効化 156
OT Security の使用の開始 157
監視対象ネットワークを設定する 158
ポートを確認して設定する 158
ユーザー、グループ、認証サーバーを設定する 158
ネットワークサービスを追加する 158
アクティブクエリを有効化する 158
Nessus スキャンを作成する 158
バックアップを設定する 159
アップデートを入手する 159
最適化する 159
統合する 159
OT Security センサーのインストール 159
センサーのペアリング 160
センサーのセットアップ 167
設定可能なセンサーのセットアップ 167
DIN レールへの取り付け 167
ラックマウント (設定可能なモデル用) 169
センサーのネットワーク接続 171
センサーセットアップウィザードへのアクセス 171
コンソール接続の確立と初期セットアップ 174

物理接続 176
COM ポートの識別 (Windows) 176
ターミナルの設定 (PuTTY) 176
接続の確立 177
初期ネットワーク設定 178
ユーザーインターフェースへのアクセス 179
OT Security センサーに接続するコンソールケーブル 179
CLI を使用して行うバックアップの復元 181
管理コンソールのユーザーインターフェース要素 182
主なユーザーインターフェース要素 183
ダークモードを有効または無効にする 184
現在のソフトウェアバージョンの確認 184
リソースセンターへのアクセス 186
OT Security のナビゲーション 186
表のカスタマイズ 188
列表示のカスタマイズ (3.19 以前) 188
列表示のカスタマイズ (4.0 以降) 189
リストのカテゴリ別グループ化 (3.19 以前) 190
リストのカテゴリ別グループ化 (4.0 以降) 192
列の並べ替え 194
列のフィルタリング (3.19 以前) 194

列のフィルタリング (4.0 以降) 195
フィルターの保存 197
保存済みフィルターの変更 199
保存済みフィルターの複製 199
すべてのフィルターの削除 200
検索 (3.19 以前) 200
検索 (4.0 以降) 200
データのエクスポート 201
アクションメニュー 201
一括アクション 202
OT Security の概要 203
エグゼクティブレポートの生成 206
インベントリ 207
資産の表示 207
資産タイプ 212
資産の詳細の表示 223
ヘッダーペイン 225
詳細 226
バックプレーンビュー 229
Nessus スキャン情報 229
IEC 61850 231

コードリビジョン 232
バージョンの選択ペイン 233
スナップショットの詳細ペイン 234
バージョン履歴ペイン 235
スナップショットバージョンの比較 235
スナップショットの作成 237
IP証跡 237
攻撃手法 238
攻撃経路を判別する方法 239
推奨軽減ステップ 239
攻撃経路の生成 239
攻撃経路の表示 242
オープンポート 243
オープンポートの更新 244
[オープンポート]タブのその他のアクション 244
スキャンの実行 244
資産ポータルの表示 245
脆弱性 245
イベント 246
ネットワークマップ 250
デバイスポート 251

関連資産 252
ネストされた資産の詳細 253
IEC 61850 255
ソース 257
資産詳細の編集 259
UI による資産詳細の編集 259
CSV のアップロードによる資産詳細の編集 261
資産の非表示 263
診断のエクスポート 264
資産診断レポートのエクスポート 264
Tenable OT Security 診断レポートのエクスポート (Tenable Core) 265
資産のマージ 266
資産をマージすると起きること 270
マージの競合と強制マージ 270
誤ってマージした場合の修正方法 271
資産固有の Tenable Nessus スキャンの実行 271
再同期の実行 272
脆弱性 275
脆弱性の表示 276
プラグイン詳細 278
脆弱性詳細の編集 278

プラグイン出力の表示 279
脆弱性からのプラグイン出力の表示 279
インベントリからのプラグイン出力の表示 280
Tenable Nessus プラグインのプラグイン出力の例 281
OT Security プラグインのプラグイン出力の例 281
検出結果 282
検出結果の詳細の表示 286
ポリシー違反 287
[アクション] メニュー 290
検出結果の解決 290
ポリシーから除外する 291
最新キャプチャファイルをダウンロードする 291
プラグイン詳細 292
イベントを検索する 292
コンプライアンスダッシュボード 292
イベント 297
イベントの表示 297
イベントの詳細の表示 302
イベントクラスタの表示 303
ポリシー除外の作成 304
個々のキャプチャファイルのダウンロード 311

FortiGate ポリシーの作成 312

ネットワーク 313

ネットワーク概要 314

トラフィックと会話の経時変化 314

上位 5 件のソース 315

上位 5 件のデスティネーション 316

プロトコル 317

タイムフレームの設定 318

パケットキャプチャ 319

パケットキャプチャパラメーター 320

パケットキャプチャ表示のフィルタリング 321

パケットキャプチャのオンまたはオフ 322

ファイルのダウンロード 323

対話 323

ネットワークマップ 325

資産のグループ化 328

マップ表示へのフィルターの適用 331

資産の詳細の表示 332

ネットワークベースラインの設定 333

データ収集 334

ポリシー 334

ポリシー設定 334
グループ 335
深刻度レベル 336
イベント通知 336
ポリシーカテゴリとサブカテゴリ 337
ポリシーのタイプ 338
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 338
設定イベント – コントローラー検証イベントのタイプ 338
ネットワークイベントのタイプ 340
ネットワーク脅威イベントのタイプ 343
SCADA イベントのタイプ 344
ポリシーの有効化または無効化 346
ポリシーの表示 348
ポリシーの詳細の表示 350
ポリシーの作成 352
承認されていない書き込みポリシーの作成 362
ポリシーに対するその他のアクション 363
ポリシーの編集 363
ポリシーの複製 365
ポリシーの削除 365
ポリシーの除外の削除 366

アクティブクエリの管理 367
カスタムクエリの作成 370
制限の追加 372
クエリバリエーションの編集 373
クエリバリエーションの複製 374
クエリバリエーションの実行 374
クエリログのダウンロード 375
検出クエリの種類 376
認証情報 378
認証情報の追加 378
認証情報の編集 382
認証情報の削除 382
WMI アカウント 383
Nessus プラグインスキャンの作成 383
Nessus プラグインスキャンの作成 386
Nessus プラグインスキャンの実行 389
データソース 390
センサー 391
センサーの表示 392
受信するセンサーペアリングリクエストを手動で承認 393
アクティブクエリの設定 394

センサーの更新 396
OT エージェント 397
OT エージェントの表示 398
OT エージェントのインストール 400
OT エージェントの設定 405
OT エージェントを使用したスキャンの実行 407
スキャンの中止 408
OT エージェントのアップデート 409
OT エージェントの削除 411
CLI を使用した OT エージェントのインストール 412
OT エージェントのスケジュールスキャンの有効化、無効化、設定 414
OT エージェントとセンサーの比較 415
IoT コネクタの管理 417
IoT コネクタエージェントの要件 418
IoT コネクタエンジン 418
IoT コネクタの追加 418
IoT コネクタにリンクされた資産を表示する 420
IoT 接続をテストする 421
IoT コネクタを編集する 421
IoT コネクタの削除 422
Windows での IoT コネクタエージェントのインストール 422

PCAP プレーヤー 424
PCAP ファイルのアップロード 424
PCAP ファイルの再生 425
手動アップロード 425
CSV を使用した資産詳細の更新 426
手動による資産の追加 426
SCD ファイル 428
Rockwell プロジェクトファイル 429
設定 **431**
システム設定 435
デバイス 435
デバイス名 435
デバイス URL 436
システム時刻 436
ログインセッションタイムアウトの最大値 436
非アクティビティタイムアウトの最大値 436
オープンポートの期限切れ期間 436
ping 要求 436
パケットキャプチャ 437
センサーのペアリングリクエストの自動承認 437
分類バナー 437

収集データの有効化 437
GraphQL Playground 438
ポート設定 438
コンプライアンスダッシュボードの設定 438
アップデート 440
Tenable Nessus プラグインセットのアップデート 441
プラグインの自動クラウドアップデートの設定 441
プラグインアップデートの頻度の編集 441
プラグインの手動クラウドアップデートを実行する 443
オフラインアップデート 443
IDS エンジンルールセットのアップデート 445
IDS エンジンルールセットの自動クラウドアップデートの設定 445
IDS エンジンルールセットのアップデート頻度の編集 445
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 446
オフラインアップデート 447
DFE のクラウドアップデート 449
自動クラウド DFE アップデートの設定 449
DFE アップデートの頻度の編集 449
DFE クラウドアップデートを手動で実行する 450
オフラインアップデート 450
OT Discovery エンジン (OTD) のアップデート 452

証明書 453
HTTPS 証明書の生成 453
HTTPS 証明書のアップロード 454
API キーの生成 455
ICP と Enterprise Manager のペアリング 456
Enterprise Manager と ICP のペアリング解除 459
OT Security EM と ICP ペアリングの解除 460
OT Security と ICP ペアリングの解除 460
ライセンス 460
環境設定 461
ネットワーク定義 461
パッシブモニタリング 461
重複する内部ネットワーク 461
重複するネットワークの追加 462
重複する内部ネットワークに対するアクション 468
SNMP を介した新しい資産の検出 469
IoT 資産の IP アドレスのフェッチ 469
イベントクラスタ 470
モニタリング対象ネットワーク 471
サブネットの追加 472
サブネットの編集 474

ユーザー管理 474
ローカルユーザー 475
ローカルユーザーの表示 476
ローカルユーザーの追加 476
ユーザーアカウントに関するその他のアクション 477
ユーザーグループ 480
ユーザーグループの表示 481
ユーザーグループの追加 481
ユーザーグループに関するその他のアクション 484
ユーザーロール 486
ゾーン 508
ゾーンの作成 508
ゾーンの表示 509
ゾーンの編集 510
ゾーンの削除 511
認証サーバー 511
Active Directory 512
LDAP 514
SAML 516
グループ 517
グループの表示 518

資産グループとタグ 519
タグ 519
資産グループとタグの表示 522
資産グループの作成 524
資産グループとタグの作成 527
E メールグループ 528
E メールグループの表示 529
E メールグループの作成 530
ポートグループ 530
ポートグループの表示 531
ポートグループの作成 531
プロトコルグループ 532
プロトコルグループの表示 533
プロトコルグループの作成 533
スケジュールグループ 534
スケジュールグループの表示 535
スケジュールグループの作成 536
コントローラータググループ 538
コントローラータググループの表示 539
コントローラータググループの作成 539
ルールグループ 541

ルールグループの表示 541
ルールグループの作成 541
グループのアクション 542
グループの詳細の表示 543
グループの編集 544
グループの複製 544
グループを削除する 545
統合 546
Tenable 製品 546
Tenable Security Center 547
Tenable Vulnerability Management 548
Tenable One 548
Palo Alto Networks - 次世代ファイヤーウォール (NGFW) 549
Aruba - ClearPass Policy Manager 549
Tenable One との統合 550
Tenable One の SAML 統合の設定 553
サーバー 564
SMTP サーバー 564
Syslog サーバー 565
FortiGate ファイヤーウォール 567
システムログ 568

付録 – Microsoft Azure とSAML の統合 **570**

手順 1 - Azure で Tenable アプリケーションを作成する 570

手順 2 - 初期設定をする 572

手順 3 - Azure ユーザーを Tenable グループにマッピングする 579

手順 4 - Azure で設定を完成させる 585

手順 5 - 統合をアクティブ化する 587

SSO を使用したサインイン 588

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を実行してください。

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。

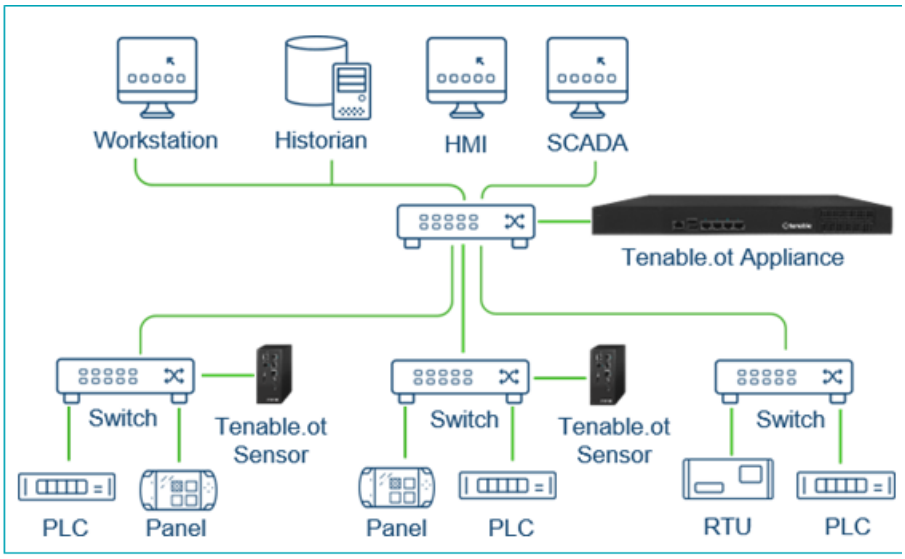
ソリューションアーキテクチャ

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ているので、OT Security はこれらのシステムと資産インベントリ情報を共有することができます。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。

Tenable OT Security のハードウェア仕様

ICP とセンサーの仕様

以下に、Industrial Core Platform (ICP) の OT Security ハードウェアアプライアンスの仕様を示します。

通常の ICP

カテゴリ	通常の ICP
CPU	Intel® Xeon™ D-218dIT、2.0GHz
コア	14
RAM	64GB
ストレージ	256GB SSD 800GB NVMe 2TB HDD
ネットワーク (銅イーサネット)	4 x 1Gbps
ネットワーク (ファイバーイーサネット)	該当なし
電源	単一 110 ~ 220v
フォームファクター	1U ハーフ奥行
寸法 (奥行 x 幅 x 高)	209 x 43 x 376 mm 8.2 x 1.7 x 14.8 インチ
重さ	3.6Kg
動作温度	摂氏 5 ~ 45 度 (華氏 41 ~ 113 度)
相対湿度	8% ~ 90% 結露なし
最大スパンスループット	500Mbps

XL ICP

カテゴリ	XL ICP

CPU	2x Xeon® Silver 4314
コア	2 x 16
RAM	256 GB
ストレージ	960GB SSD SAS FIPS-140 SED 960GB SSD SAS FIPS-140 SED 2 x 2.4TB SAS HDD FIPS-140 SED 注意：ハードウェアはフル暗号化をサポートしており、FIPS-140 に準拠しています。
ネットワーク (銅)	6 x 1Gbps
ネットワーク (ファイバー)	2 x 10GB SFP+
電源	冗長 110-220v、165W
フォームファクター	1U フル奥行
寸法 (幅 x 高 x 奥行)	幅*: 482.0mm (18.98 インチ) x 高：42.8mm (1.69 インチ) x 奥行*: 698mm (27.5 インチ) *寸法はベセルを含みます。
重さ	22kg
動作温度	摂氏 0 ~ 40 度 (華氏 32 ~ 104 度)
保管温度	摂氏 -10 ~ 50 度 (華氏 14 ~ 122 度)
相対湿度	5% ~ 90% 結露なし
証明書	CE / FCC/ RoHS

	CB、CCC、UL、RCM、NOM
最大スパンスループット	1 Gbps

ICP-Mini

カテゴリ	ICP-Mini
CPU	Intel® Core™ i7-1185G7E、1.8 GHz
コア	4
RAM	32 GB
ストレージ	480 GB SSD
ネットワーク (銅)	4 x 2.5 Gbps
ネットワーク (ファイバー)	該当なし
電源	ターミナルブロック 12~28 VDC
フォームファクター	DIN レール
寸法 (mm)	150 x 190 x 81 mm
重さ	1.9 Kg
動作温度	摂氏 0 ~ 40 度 (華氏 32 ~ 104 度)
保管温度	摂氏 -10 ~ 50 度 (華氏 14 ~ 122 度)
相対湿度	10% ~ 95% 結露なし
証明書	CE / FCC / RoHS クラス A

	CB、CCC、UL、ROM、NOM
最大スパンスループット	150 Mbps

センサー

カテゴリ	センサー
CPU	Intel® Core™ 13-8145UE、2.2GHz
コア	2
RAM	4GB
ストレージ	128GB SATA M.2
ネットワーク (銅)	2 x 1Gbps
ネットワーク (ファイバー)	該当なし
電源	ターミナルブロック 12~28 VDC
フォームファクター	極小フォームファクター
寸法 (幅 x 高 x 奥行)	179 x 88 x 34.5 mm 7.05 x 3.46 x 1.36 インチ
重さ	0.72kg
動作温度	摂氏 0 ~ 50 度 (華氏 32 ~ 122 度)
保管温度	摂氏 -40 ~ 60 度 (華氏 -40 ~ 140 度)
相対湿度	20% ~ 80% 結露なし
最大スパンスループット	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。

イベントを解決済みとしてマークできるのは承認されたユーザーです。イベントにコメントを追加することはできます。

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。

> 重要: Tenable 製品を購入するには、Tenable 担当者にご連絡ください。

> 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。

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。

> 注意: OT Security のスタンドアロン購入を Tenable Oneのインスタンスに接続することは可能ですが、それらの資産のライセンスは処理しません。Tenable One のお客様は、OT Security を含む多くの Tenable ソリューションのライセンスを取得していますが、まず Tenable One ライセンスの一部である必要があります。Customer Success Manager (CSM) にご相談の上、適宜アカウントを更新してください。

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。

運用プレイブック

運用プレイブックは、アクションが実行できるワークフローを使用して、お客様が特定のセキュリティ上の成果を達成しやすいように設計されたガイドです。OT組織での自分の役割に関係なく、これらのプレイブックでは、産業用制御システム(ICS)およびSCADA環境をセキュリティ保護するための標準化された手順が用意されています。

これらのプレイブックでは、資産インベントリ、脆弱性管理、脅威の検出を含むOT Securityのマルチエンジン検出機能を使用しており、お客様がレジリエンス態勢を維持するのに役立ちます。

各ワークフローには次の内容が含まれます。

- 達成しようとしている目的または特定の目標
- OT Security インターフェース内のステップバイステップのパス
- ワークフローの実行後の測定可能な結果

前提条件

これらのプレイブックを実行する前に、ネットワークに次のものがあることを確認してください。

- 資産検出: OT Securityがパッシブ検出またはアクティブクエリを使用して1つ以上のネットワークセグメントをモニタリングし、インベントリに入力値があることを確認します。
- ユーザーアクセス許可: ダッシュボードを表示したりスキャンを開始したりするために必要なユーザーロールを自分が持っていることを確認します。

運用ワークフロー

開始するには、次のワークフローを参照してください。

- 脆弱性の優先順位付けと軽減策 – CVSS スコアだけでなく実際の脅威レベル (VPR) に基づいて修正に優先順位を付けます。
- ネットワーク脅威に対する調査と対応 – 異常、マルウェア、不正なネットワークスキャンを検出して調査します。

脆弱性の優先順位付けと軽減策

OT Security は、CVE、脆弱なプロトコル、オープンポートなどの脅威を特定します。脆弱性優先度格付け (VPR) を利用して各脆弱性のリスクスコアを生成するため、チームは共通脆弱性評価システム (CVSS) スコアが高い脆弱性だけでなく、アクティブに悪用される可能性がある高リスクの脆弱性に重点的に対処することができます。

VPR は、脆弱性の技術的な影響と脅威インテリジェンスに基づき Tenable によって計算されたスコアです。VPR および CVSS との違いについての詳細は、こちらのブログを参照してください。

目的

反応型の「すべてをパッチ」アプローチから、リスクベースの戦略に移行します。これにより、運用環境に実際に最大の脅威をもたらす脆弱性を特定して修正します。

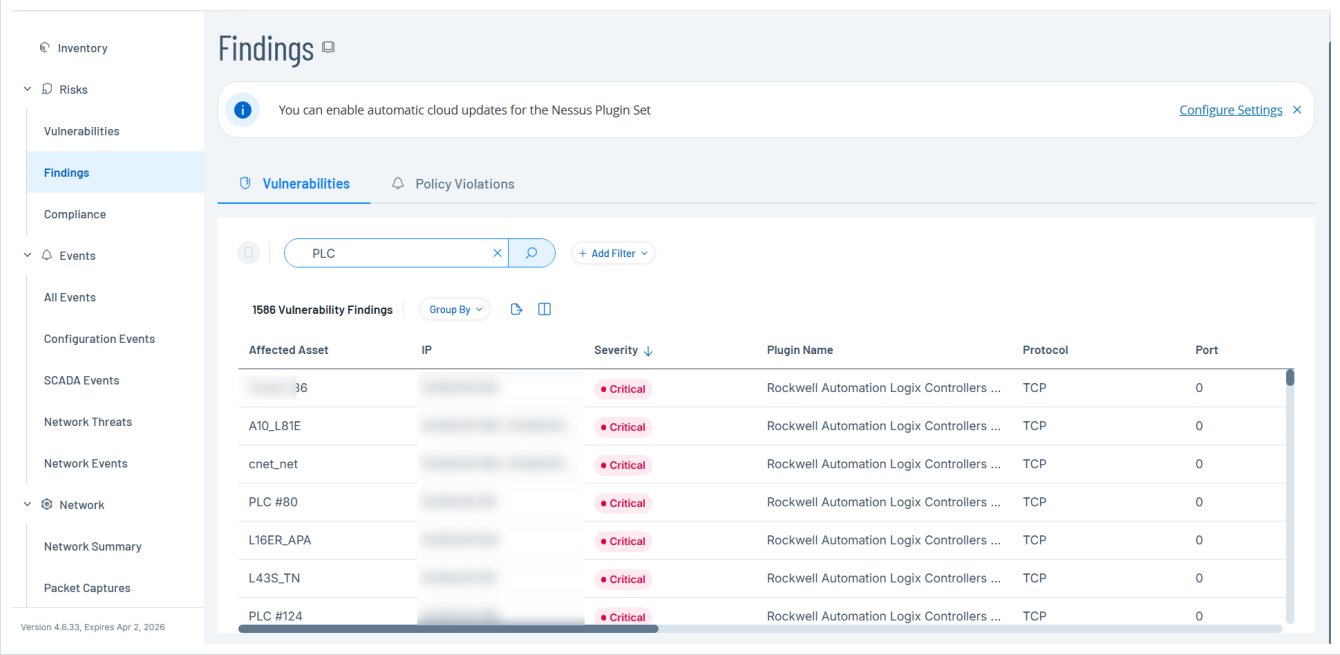
前提条件

- OT Security がパッシブ検出またはアクティブ検出によって資産を特定していなければなりません。
- (オプション) スコアリングを統一するための Tenable Vulnerability Management または Tenable Security Center との統合。

ステップ 1: リスクダッシュボードを表示する

1. OT Security にログインします。
2. 左側のナビゲーションメニューで、[リスク] > [検出結果] をクリックします。

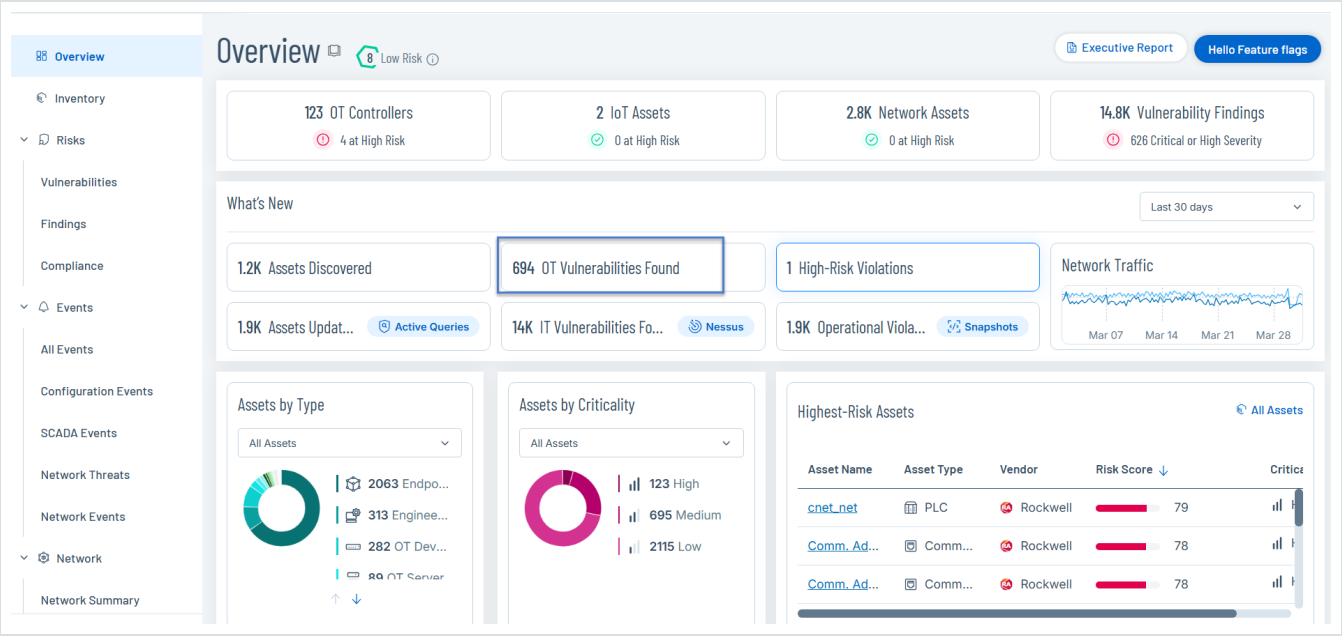
   [検出結果] ページにデフォルトの [脆弱性] タブが表示されます。ここに、CVE や脆弱なプロトコルを含むすべてのネットワーク脅威が表示されます。



ステップ 2: 深刻度と資産重要度で優先順位を付ける

1. 上位の脅威を特定するために、脆弱性リストを VPR または深刻度 ([重大] または [高]) で並べ替えます。
2. コントローラー (PLC) やエンジニアリングステーションなどの重要な資産カテゴリにフォーカスするようビューをフィルタリングするには、[フィルターの追加] ボタンを使用します。

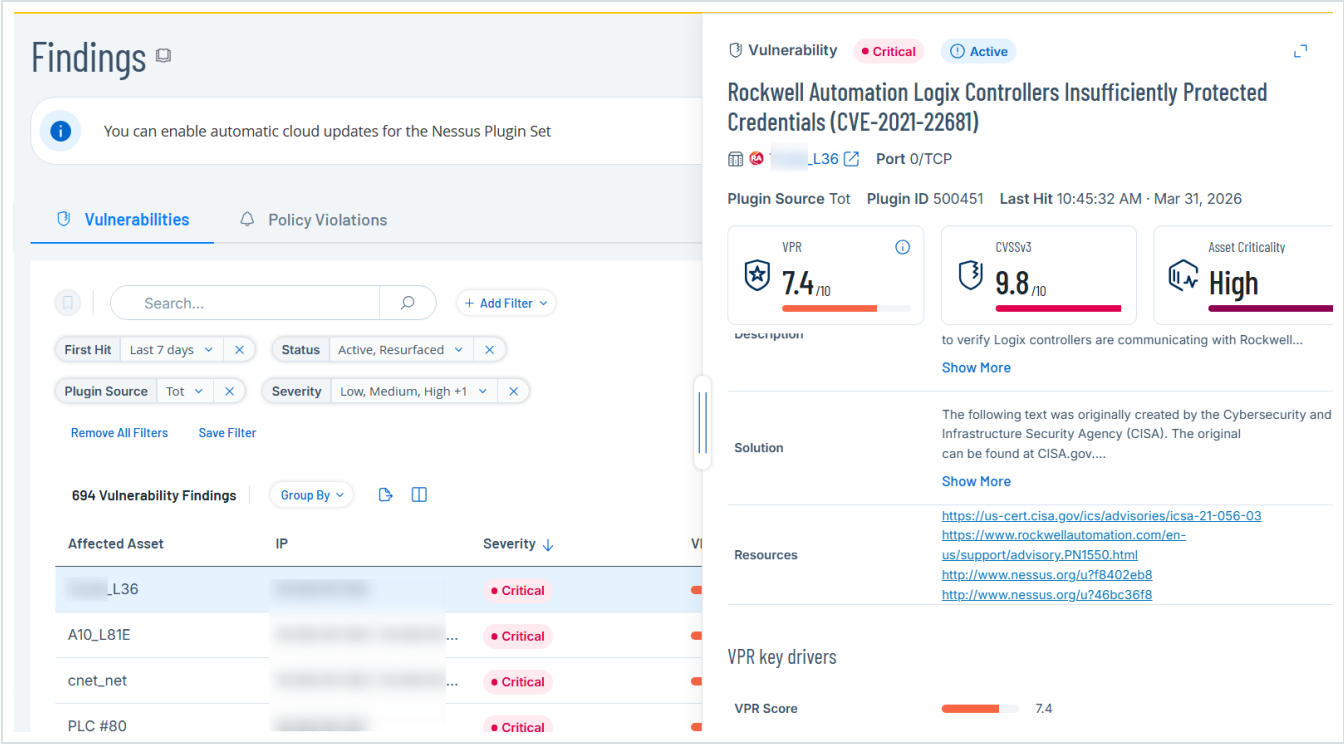
   脆弱性リストに、フィルターが適用された結果が表示されます。
3. または、[概要] ダッシュボードの [脆弱性] ウィジェットを確認して、資産タイプをまたいだ深刻度の分布を見ることができます。



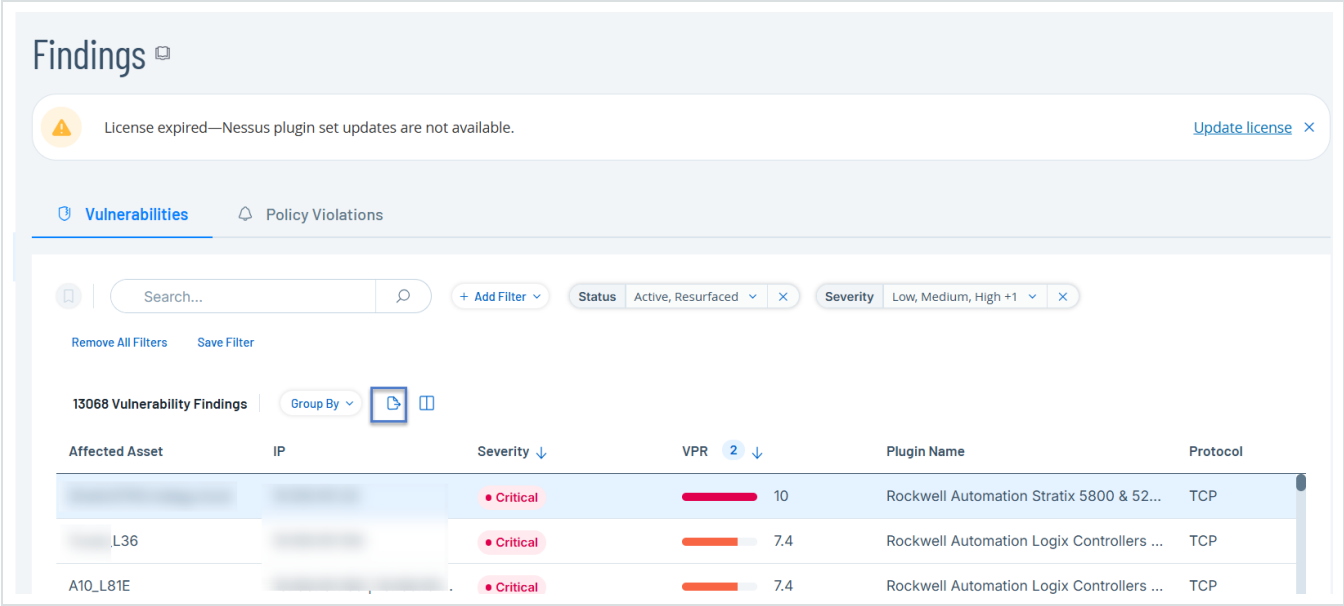
- [OT 脆弱性] ウィジェットをクリックして、[検出結果] ページにドリルダウンします。

ステップ 3: 修正オプションを分析する

1. [検出結果] ページで、特定の資産をクリックして [資産の詳細] パネルを開きます。
2. 特定の脆弱性をクリックすると、その特定の CVE または脆弱性に対して提供されている詳細なインサイトと軽減策の提案を確認できます。



3. [検出結果] ページで [エクスポート] ボタンをクリックすると、データをエクスポートして、他のチームやステークホルダーに共有できます。



ヒント: OT Security を Tenable One または Tenable Security Centerと統合した場合は、これらのアプリケーション内で検出結果をさらに分析できます。Tenable One または Tenable Security Center の統合についての詳細は、統合を参照してください。

結果

ご使用の環境に関連する脆弱性の優先順位が付けられたリストが得られます。これにより、最大のリスクを軽減するためにメンテナンスリソースを効率的に割り当てることができます。

ネットワーク脅威に対する調査と対応

OT Security は、動作異常、署名ベースの検出 (Suricata)、ポリシーベースのルールなど、複数の検出エンジンを採用して、サイバー攻撃の兆候を示すトラフィックを識別します。

目的

不正なスキャン、マルウェアの伝播、プロトコル異常などの疑わしいネットワークアクティビティを検出して調査し、運用の中断を防ぎます。

前提条件

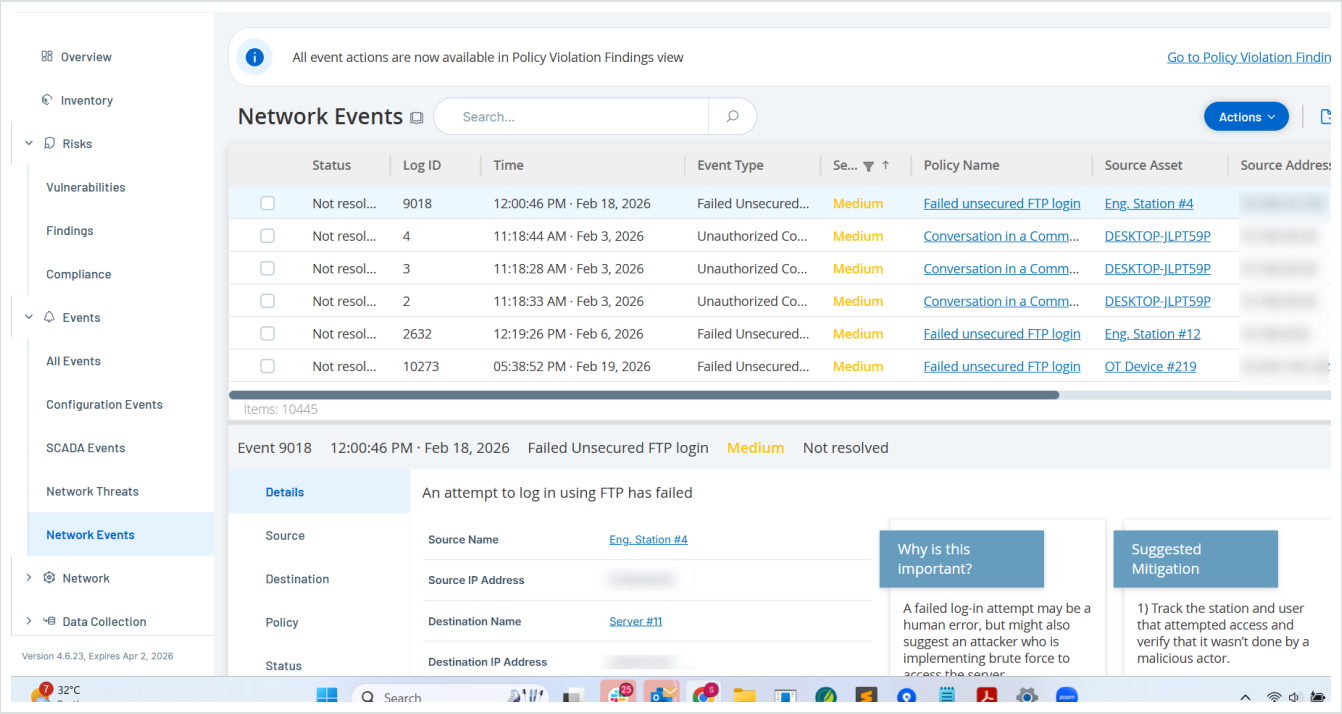
イベントを表示するのに必要なアクセス許可を持っていないければなりません。

以下を設定していることを確認します。

- ネットワークモニタリングを設定する。モニタリング対象ネットワークを参照してください。
- 検出ポリシーを有効化する。ポリシーの有効化または無効化を参照してください。
- (オプション) フォレンジック分析用に PCAP キャプチャを有効にする。個々のキャプチャファイルのダウンロードを参照してください。

ステップ 1: イベントアラートをモニタリングする

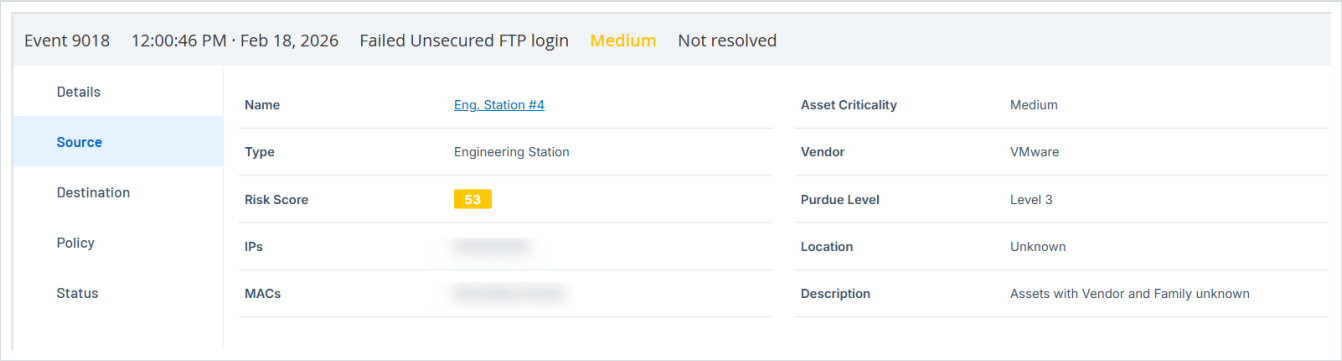
1. OT Security にログインします。
2. 左側のナビゲーションメニューで [イベント] をクリックします。
3. [ネットワーク脅威] または [ネットワークイベント] を選択して、侵入試行や異常なトラフィックに関連するアラートを表示します。



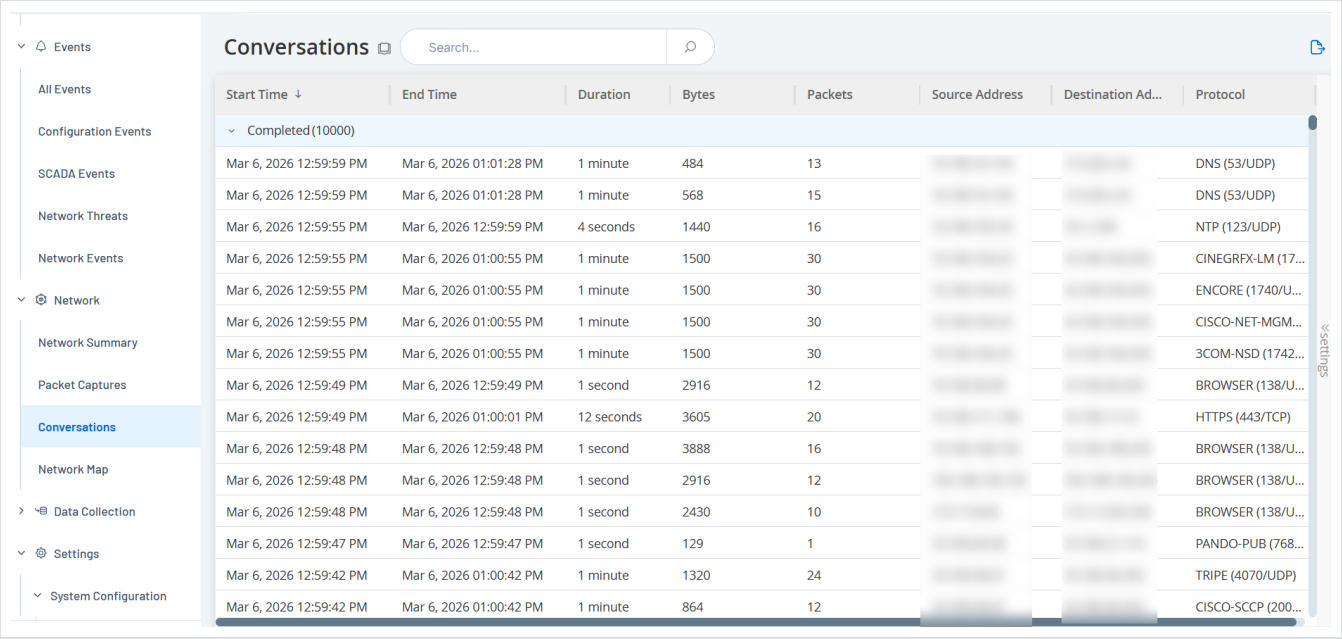
4. 深刻度 ([高] または [重大]) 別にイベントを並べ替え、差し迫った脅威を優先的に処理します。

ステップ 2: 対話データを分析する

1. 特定のイベントを選択して、[イベントの詳細] パネルを表示します。
2. 疑わしいアクティビティに関連するソース資産とデスティネーション資産を特定します。



3. [ネットワーク] > [対話] ページに移動して、これらの資産間の特定のトラフィックフローを表示します。



4. アクセスできる場合は、[パケットキャプチャ] (PCAP) ビューを使用して、生のトラフィックデータを分析し、証拠となるようにします。個々のキャプチャファイルのダウンロードを参照してください。

ステップ 3: 対応を開始する

- [イベントの詳細] セクションで [推奨軽減策] を確認し、対応策を講じます (侵害された資産を隔離するなど)。

- イベントが誤検出の場合は、ポリシー設定を調整し、検出を微調整してノイズを減らします。ポリシーを参照してください。
- [検出結果] > [ポリシー違反] で、イベントを [解決済み] としてマークし、アクティブキューから消去します。ポリシー違反を参照してください。

結果

セキュリティインシデントの「誰が、何を、どこで、いつ」を迅速に特定し、平均対応時間 (MTTR) を最小限に抑えることができます。

エラーメッセージ

次の表は、Tenable OT Security で表示される可能性のあるエラーメッセージを説明しています。

カテゴリ	エラーカテゴリ名	エラーの説明	ユーザーインターフェースメッセージ	推奨アクション
アクティブクエリ管理	NoRoutesForClient	クエリはネットワークからルーティングエラーを受け取りました。	ネットワーク接続に問題がある可能性があります。ネットワーク接続をチェック	ネットワーク接続をチェックし、アクティブクエリを再試行します。

			し、クエリを再試行してください。	
アクティブクエリ管理	InternalError	クエリの試行で内部エラーが発生しました。	予期しないエラーが発生しました。後でもう一度お試しください。問題が解決しない場合、テクニカルサポートにお問い合わせください。	しばらくしてからクエリを再試行します。問題が解決しない場合は Tenable サポートに問い合わせます。
アクティブクエリ管理	DnsError	ターゲット IP の DNS ホスト名が見つかりませんでした。	ターゲット IP の DNS ホスト名が見つかりませんでした。逆引き	逆引き DNS ルックアップが有効になっており、DNS ポインターレコード (PTR) が IP に対して定

			DNS が有効になっており、PTR レコードが IP に対して定義されていることを確認してください。	義されていることを確認する。
アクティブクエリ管理	HostUnreachableError	クエリターゲットに到達できません。ルーティングをチェックしてください。	デバイスに到達できませんでした。これは、ネットワーク接続の問題が原因である可能性があります。ネットワークまたはファイヤー	ネットワーク接続とファイヤーウォールの設定をチェックし、アクティブクエリを再試行します。

			ウォールの設定をチェックし、もう一度お試しください。	
アクティブクエリ管理	TimeoutError	クエリがターゲットから応答を受信していないため、タイムアウトに達しました。	ネットワークタイムアウト。これは、一時的なネットワークの問題、またはデバイスからの応答が遅いことが原因である可能性があります。後でもう一度クエリを実行してください。	しばらくしてからクエリを再試行します。

アクティブクエリ管理	NetworkError	クエリが、ネットワークからエラー応答を受け取りました。	ネットワークエラーが発生しました。これは、一時的なネットワークの問題、またはファイヤーウォールの制限が原因である可能性があります。ネットワーク接続をチェックし、クエリを再試行してください。	ネットワーク接続をチェックし、クエリを再試行します。
アクティブクエリ管理	ProtocolError	クエリがターゲットから予期しない応答を受信し	宛先からのサポートさ	宛先デバイスとの互換性があるかどうかをチェッ

		ました。	れていない応答形式。これは、デバイスのプロトコルのバージョンに互換性がないか、一時的なネットワークの問題が原因である可能性があります。デバイスの互換性をチェックするか、後でクエリを再試行してください。	クするか、しばらくしてからクエリを再試行します。
アクティブクエリ管理	AuthenticationError	クエリで無効な認証情報が使用され	デバイスに認証	認証情報を確認して、クエリを再試

		ました。	できませんでした。認証情報が正しくないか欠落している可能性があります。認証情報を確認してください。	行します。
アクティブクエリ管理	LimitExceededError	OT Securityは、ターゲットに対して失敗したクエリの数の上限に達しています。	クエリの失敗が多すぎるため、このデバイスへのアクティブクエリが一時停止されています。後でもう一度お試しください。問題が解決	デバイスに対して失敗したクエリがいくつかあります。しばらくしてからクエリを再試行します。問題が解決しない場合はテクニカルサポートに問い合わせます。

			しない場合、サポートにお問い合わせください	
アクティブクエリ管理	NoPotentialClients	ターゲットのクエリ範囲(CIDRブロック、資産リスト、またはIP範囲)に有効なクライアントが存在しません。	アクティブクエリは、ターゲット範囲内でアクセス可能なデバイスを見つけることができませんでした。ユーザー適用の制限により、一部のデバイスがブロックされている可能性がありま	ユーザーが適用した制限により、ターゲットデバイスにアクセスできない可能性があります。アクセス制御の設定を確認して、クエリを再試行します。

			す (CIDR ブロック、資産リスト、IP 範囲)。選択とアクセス制御を確認してください。	
アクティブクエリ管理	NoAllowedClients	ターゲットのクエリ範囲 (CIDR ブロック、資産リスト、または IP 範囲) に許可されたクライアントが存在しません。	アクティブクエリが、ターゲット範囲 (CIDR ブロック、資産リスト、IP 範囲) で互換性のあるデバイスを見つけられませんでした。選択とアクセス制御を確	ターゲットデバイスが、OT Security 設定と互換性がない可能性があります。アクセス制御の設定を確認して、クエリを再試行します。

			認してください。	
IoT	ServiceUnavailable	サービスが利用できません。起動時またはリセット後に問題となるかもしれません。	IoT コネクタサービスを利用できないか、問題が発生しました。後でもう一度お試しください。問題が解決しない場合は、サポートにお問い合わせください。	IoT コネクタサービスが一時的にダウンしている可能性があるため、しばらくしてからクエリを再試行します。問題が解決しない場合はテクニカルサポートに問い合わせます。
IoT	IotConnectorSecureModeError	IoT コネクタは、リモートにインストールされている IoT エージェントに接続できません。	IoT コネクタのセキュアモードエラー。リモートシステムに IoT エー	リモートシステムに IoT エージェントを再インストールして、接続を再試行します。

			ジェントを再インストールして、接続を再度許可する必要があります。	
IoT	IotConnectorIpAlreadyExists	ユーザーがすでに存在するIPを使用してコネクタを追加しようとしています。	コネクタの作成に失敗しました。指定されたIPアドレスは、すでに別のコネクタで使用されています。一意のIPアドレスを指定して、もう一度お試しください。	一意のIPアドレスを指定して、コネクタの追加を試行します。

サーバーペアリング: (Enterprise Manager (EM)、外部サーバー、FW)	WrongCertificate	ユーザーが無効な証明書で ICP を EM とペアリングしようとしています。	ペアリングサーバーが無効なセキュリティ証明書を表示しました。サーバー証明書を確認してから、もう一度お試しください。が解決しない場合、サーバー管理者にお問い合わせください。	新しいセキュリティ証明書を生成し、ICP と EM のペアリングを試行します。問題が解決しない場合はサーバー管理者に問い合わせます。
サーバーペアリング: (EM、外部サーバー、FW)	MissingEmAddress	API 経由のみ	ペアリングするサーバーアドレスが指定	接続するサーバーの IP アドレスまたはホスト名を入力して、再試行しま

			されていませんでした。接続するサーバーのIPアドレスまたはホスト名を入力して、もう一度お試しください。	す。
サーバーペアリング:(EM、外部サーバー、FW)	MissingPassword	API経由のみ	指定された認証情報が不完全です。ペアリングサーバーのパスワードを入力して、もう一度お試しください。	サーバーのユーザー名とパスワードを入力して、再試行します。
サーバーペアリング:(EM、外部サー	MissingCredentials	API経由のみ	ペアリングサー	サーバーの有効な認証

バー、FW)			バーの接続認証情報がありません。必要な認証情報(ユーザー名とパスワードなど)を入力して、再試行してください。	情報を入力して、再試行します。
サーバーペアリング:(EM、外部サーバー、FW)	BothApiKeyAndUserCredentials	API 経由のみ	このサーバーとのペアリングに使用できる認証方法は 1 つのみです。API キーまたはユーザー認証情報のどちらかを削	ペアリングに、API キーまたはユーザー認証情報のどちらかのみを使用します。

			除してから、再試行してください。	
OT フィード: PII/Suricata/Nessus	NessusNotReady	サービスが利用できません。起動時またはリセット後に問題となる場合があります。	Nessus サービスを利用できないか、問題が発生しました。後でもう一度お試しください。問題が解決しない場合は、サポートにお問い合わせください。	Nessus サービスがダウンしている可能性があるため、しばらくしてからサービスへのアクセスを試みます。問題が解決しない場合は Tenable サポート に連絡します。
OT フィード: PII/Suricata/Nessus	MissingFile	API 経由のみ	設定ファイルが添付されていません。サポートさ	有効な設定ファイルをアップロードします。

			れている形式の有効な設定ファイルをアップロードしてから、続行してください。	
OT フィード: PII/Suricata/Nessus	InvalidFile	アップロードされたファイルが無効です。	アップロードされたファイルが無効です。これは、サポートされていない形式か、バージョン情報がないことが原因である可能性があります。ド	アップロードするファイルの形式またはバージョンが有効かどうかをチェックしてから、ファイルをアップロードします。

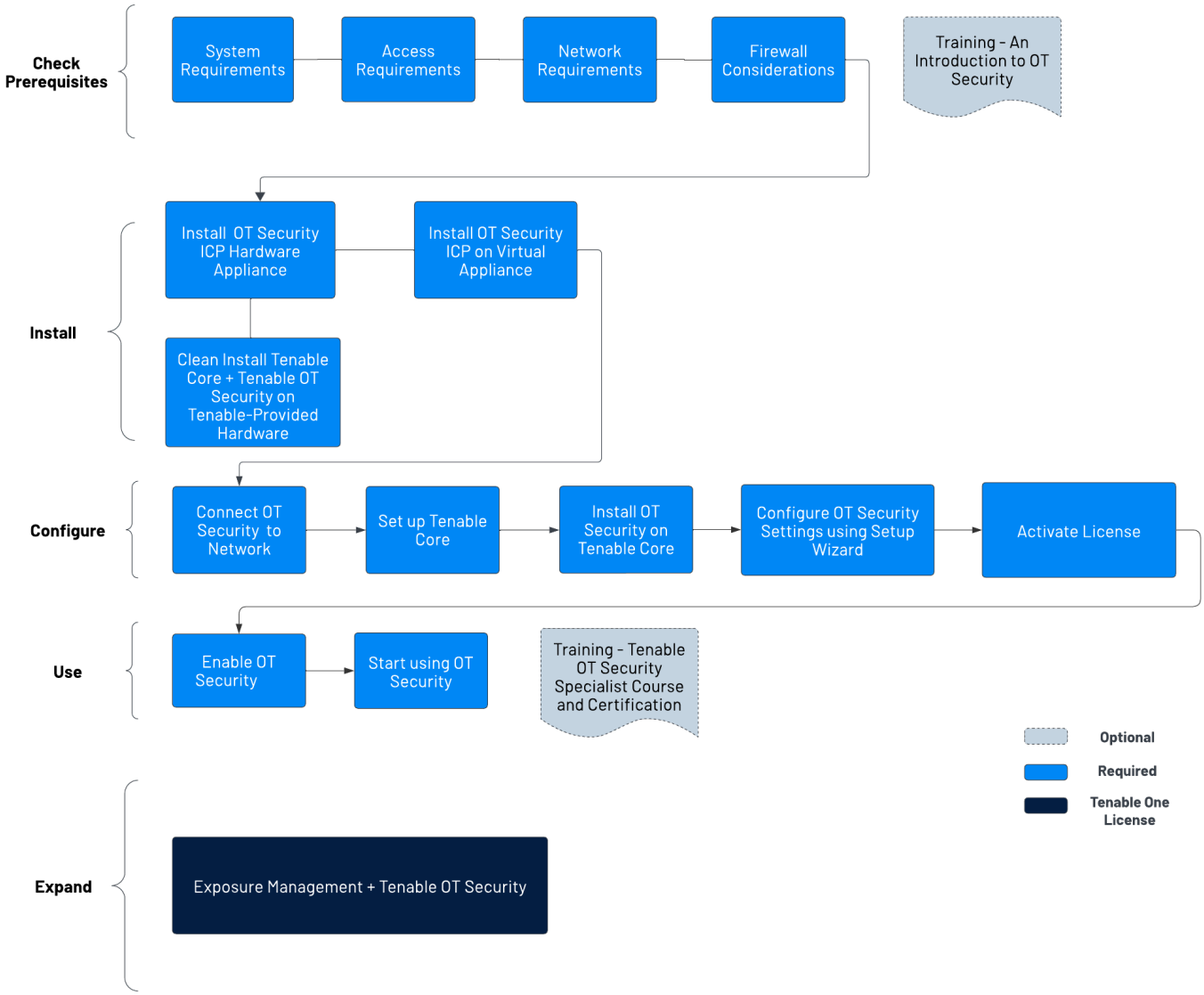
			キュメントのサポートされている形式と必須フィールドを確認し、もう一度お試しください。	
OT フィード: PII/Suricata/Nessus	NoSpaceLeftOnDevice	デバイスにスペースが残っていない状況で、オンラインまたはオフラインモード中にファイルをアップロードしています。	デバイスには、新しい設定ファイルを収容するのに十分なストレージスペースがありません。デバイスの空き容量を確保して、もう一度お試しくだ	デバイスの空き容量を増やして、設定ファイルのアップロードを試行します。

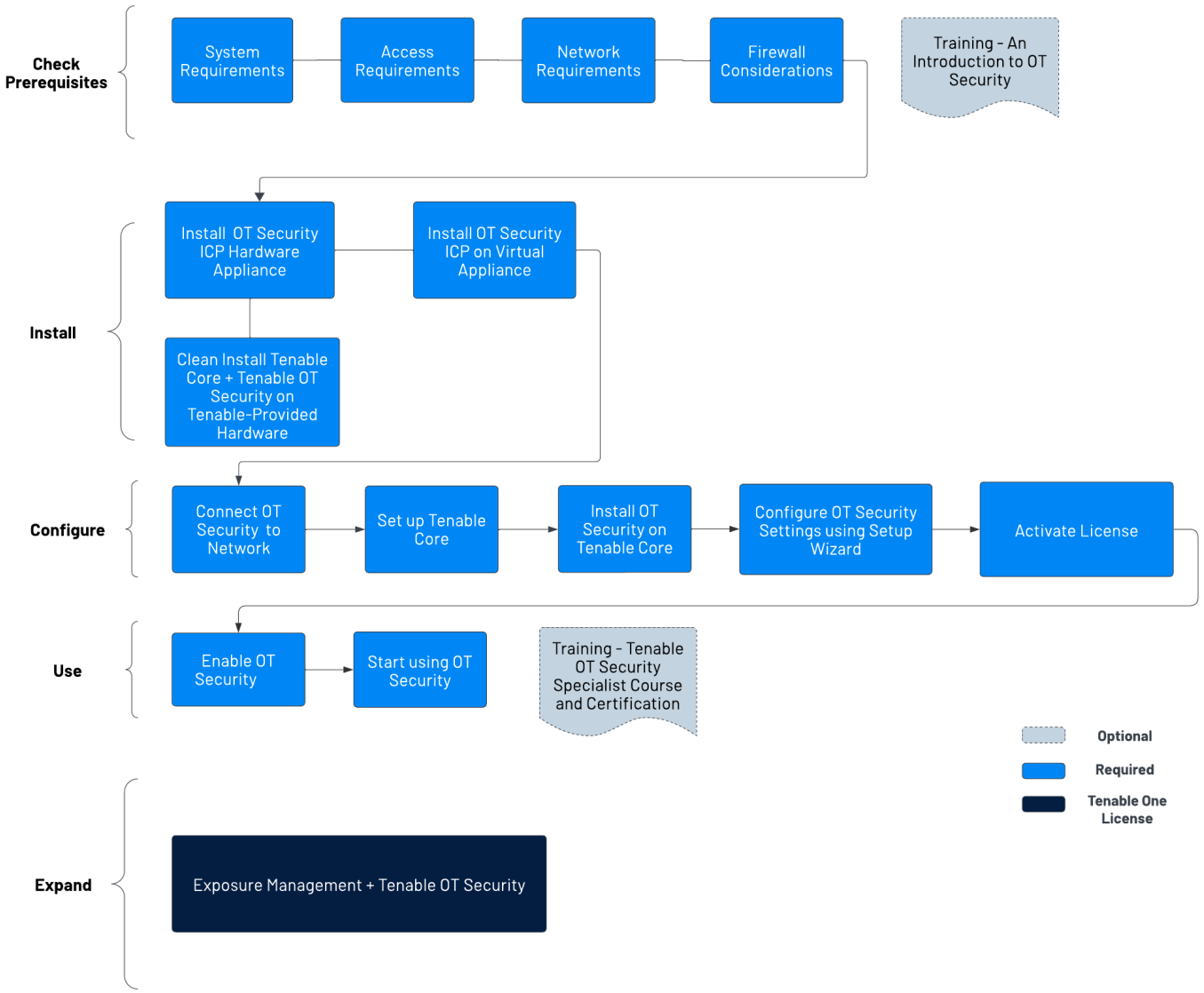
			さい。	
OT フィード: PII/Suricata/Nessus	OldLicense	ユーザーは有効な認証情報のないライセンスを使用しています。	バージョン形式が古いため、アクションを実行できません。サポートされている形式で新しいライセンスを取得し、もう一度お試しください。	OT Security ライセンスをサポートされている形式にアップグレードします。
OT フィード: PII/Suricata/Nessus	UpdateAlreadyInProgress	すでに 1 つのジョブが進行中ですが、ユーザーは現在アップデートを実行しています。同時に実行できるアップデート	このデバイスのアップデートがすでに進行中です。現在のアップデートが完了	現在のアップデートが完了するまで待ってから、再試行します。

		は 1 つのみです。	するまで待ってから、別のアップデートを試行してください。	
OT フィード: PII/Suricata/Nessus	OlderVersionUpdateAttempt	ユーザーが古いバージョンへのダウングレードを試行しています。	新しいバージョンがアクティブなため、ファイルのアップロードに失敗しました。最新のアップデートファイルがあることを確認し、もう一度アップロードをお試しください。	アップロードしようとしているファイルが最新バージョンであることを確認します。

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。





前提条件のチェック

- 前提条件 – OT Security のシステム、ハードウェア、仮想、ライセンスに関する要件を確認します。
  - システム要件 – Tenable Core + OT Security をインストールして実行するための要件を確認します。

- アクセス要件 – Tenable Core + OT Security を実行するためのインターネットとポートに関する要件を確認します。
- ネットワークに関する考慮事項 – OT Security に接続するためのネットワークインターフェースを確認します。
- ファイヤーウォールに関する考慮事項 – 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 - トレーニング資料を読んで、OT Security についての理解を深めます。

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が含まれている事前設定 `.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 を設定します。

    b. Tenable Core への OT Security のインストール - Tenable Core への Tenable OT Security 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、OT Security 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、System Time、ポート分離を設定します。

4. OT Security ライセンスのアクティブ化 – 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

次を起動します: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. の使用の開始OT Security – 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。

OT Security の Tenable One への拡張

注: これには Tenable One ライセンスが必要です。Tenable One の試用版については、Tenable One をご覧ください。

OT Security を Tenable One と統合すると、次の機能を活用できます。

- **[Exposure View]** ページにアクセスして、コンバージドリスクレベルを明らかにしたり、IT と OT の境界を越えて隠れた弱点を明らかにしたりできます。拡張された OT データを使用して、潜在的な脆弱性を継続的にモニタリングし追跡できます。
    - サイバーエクスポージャーカードを表示して管理します。
    - グローバルとオペレーショナルテクノロジーのエクスポージャーカードの CES および CES トレンドデータを表示します。
    - 修正サービスレベル契約 (SLA) データを表示します。
    - Tag Performance のデータを表示します。
- **[Exposure Signals]** ページにアクセスすると、クエリを使用して資産の違反を検索するエクスポージャーシグナルを生成できます。簡単に言えば、クエリに関連する脆弱性の影響を受ける資産は違反と見なされます。これにより、最も重大なリスクシナリオを可視化できます。
    - Tenable Research からの最新フィードを基に、環境内で最もアクティブな脅威を見つけます。
    - クエリと、影響を受ける資産の違反のデータを表示、生成、操作できます。
    - カスタムのエクスポージャーシグナルを作成して、ビジネス固有のリスクと弱点を表示します。
- **[インベントリ]** ページにアクセスして、OT 固有のインサイト (ファームウェアバージョン、ベンダー、モデル、動作状態など) が得られる、情報豊富な資産検出を実行できます。標準的な IT セキュリティツールでは提供できない OT インテリジェンスにアクセスして、次のことができます。

- **[資産]** タブで、次のようにデータを表示および操作します。
  - AD 資産を確認して、インターフェースの戦略的性質を把握します。これは、Tenable サイバーエクスポージャー管理 内でどの機能をいつ使用するかについての予想を立てるのに役立ちます。
  - グローバル資産検索とそのオブジェクトやプロパティについて理解を深めます。後で使用できるようにカスタムクエリをブックマークします。
  - デバイス、ユーザーアカウント、ソフトウェア、クラウド資産、SaaS アプリケーション、ネットワーク、およびその弱点を検出します。
  - **[資産の詳細]** ページにドリルダウンして、資産のプロパティと関連するすべてのコンテキストビューを表示します。
- **[弱点]** タブで、次のようにデータを表示および操作します。
  - 最も効果的な修正判断ができるように、脆弱性と設定ミスに起因する弱点について重要なコンテキストを表示します。
- **[ソフトウェア]** タブで、次のようにデータを表示および操作します。
  - ビジネス全体にデプロイされているソフトウェアを完全に可視化し、関連するリスクをより詳しく把握します。
  - 期限切れになっている可能性のあるソフトウェアと、まもなくサポート終了 (EoL) になるソフトウェアを特定します。
- **[検出結果]** タブで、次のようにデータを表示および操作します。
  - 資産に現れる弱点 (脆弱性または設定ミス) のインスタンスを、プラグイン ID、ポート、プロトコルによって一意に識別して表示します。
  - これらの検出結果に対するインサイト (説明、影響を受ける資産、重大度など) を確

認して潜在的なセキュリティリスクを特定し、十分に活用されていないリソースを可視化し、コンプライアンスの取り組みをサポートします。

- **[攻撃経路]** ページにアクセスし、ウェブアプリ、IT、OT、IoT、アイデンティ、ASM などのアタックサーフェスを通過するリスクの高い攻撃経路を明らかにすることで、リスクの優先順位付けを最適化し、重大な影響を回避します。軽減ガイダンスを使用して、攻撃経路を遮断するためのチョークポイントを特定することで軽減策を効率化し、AI インサイトによって深い専門知識を得ます (FedRAMP 環境ではサポートされていません)。

  - **[ダッシュボード]** タブで、脆弱な資産の概要を表示します。たとえば、重要資産への攻撃経路の数、未解決の攻撃手法の数とその深刻度、ソースノードのエクスポージャースコアと ACR ターゲット値の組み合わせごとに攻撃経路を可視化したマトリクス、トレンドの攻撃経路のリストなどがあります。

    - [上位の攻撃経路マトリクス] を確認し、[上位の攻撃経路] タイルをクリックして、重要資産 (ACR が 7 以上の資産) につながる経路に関する詳細情報を表示します。

    必要に応じてこれらを調整し、最も重大な攻撃経路のデータを表示できます。

  - **[上位の攻撃手法]** タブでは、データを高度なグラフ分析および MITRE ATT&CK® フレームワークと組み合わせて攻撃手法を特定し、1 つ以上の重要資産に至る 1 つ以上の攻撃経路に存在するすべての攻撃手法を確認できます。これにより、資産や情報に対する脅威の影響を引き起こして増幅させる未知の要因を把握し、対処することができます。

  - **[上位の攻撃経路]** タブで、次のように攻撃経路クエリを生成し、潜在的な攻撃経路の一部となっている資産を表示します。

    - ビルトインクエリを使用して攻撃経路を生成する
    - 攻撃経路クエリビルダーを使用して攻撃経路クエリを生成する
    - 資産クエリビルダーを使用して資産クエリを生成する

その後、クエリ結果リストとインタラクティブなグラフから、攻撃経路クエリと資産クエリのデータを表示して操作できます。

- **[MITRE ATT&CK ヒートマップ]** タブを操作し、[ICS] ヒートマップオプションを選択すると、ICS (産業用制御システム) に対する戦術と手法に関する情報が重点的に表示されます

- **[タグ]** ページで、次のようにデータを表示および操作します。
  - 次の設定で、OT 資産に対して新しい動的タグを作成します。
    - 演算子 = Host System Type
    - 値 = PLC
  - タグを作成および管理して、異なる資産クラスをハイライトまたは組み合わせます。
  - **[タグの詳細]** ページを表示して、資産に関連付けられているタグに関する詳細なインサイトを取得します。

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 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 + OT Security または 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。

ヒント: OT Security では、事前にイメージ処理された状態で直接出荷されるターンキーアプライアンスを提供しています。このオプションを選ぶと、使用とデプロイがはるかに容易になり、価値実現までの時間が速まります。ただし、独自のハードウェアを調達して、それに ISO イメージを適用することもできます。自前で用意するまたは弊社のものを使用するいずれの場合でも、Tenable OT ハードウェア仕様をガイドラインまたはベストプラクティスと見なしてください。OT Security のすべてのコンポーネント、ICP EM、センサーは、仕様を満たしているどのハードウェアでも実行できます。

注意: Tenable は、Tenable Core の 1 つのインスタンスに複数のアプリケーションをデプロイすることを推奨していません。Tenable Core に複数のアプリケーションをデプロイする場合は、アプリケーションごとに一意のインスタンスをデプロイしてください。

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	VMware への Tenable Core のデプロイ
	Microsoft Hyper-V	`.zip` ファイル	
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

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。

OT Security ハードウェア要件

特に OT Security または OT Security センサーのハードウェア要件について詳しくは、*General Requirements Guide* の Tenable OT Security Hardware Specifications (Tenable OT Security ハードウェア仕様) を参照してください。

OT Security 仮想ハードウェア要件

エンタープライズネットワークでは、そのパフォーマンス、容量、プロトコル、アクティビティが多岐にわたります。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規模、アプリケーションの設定などがあります。

次のチャートは、仮想環境で Tenable Core + OT Security を運用するための基本的なガイドラインを示しています。

Tenable Core + OT Security には、AVX および AVX2 を搭載した CPU (例: Intel Haswell 以降など) が必要です。

インストールシナリオ	CPU コア	メモリ	ディスク容量
仮想マシン	8 コア	16 GB RAM	205 GB

OT Security 仮想センサーの要件

インストールシナリオ	CPU	メモリ	ディスク容量
センサー	2 つの仮想 CPU	4 GB RAM	60 GB HDD

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では、そのパフォーマンス、容量、プロトコル、アクティビティが多岐にわたります。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ています。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 23Mbps 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 システム要件のガイドライン

最大 SPAN/TAP スルー	CPU コ	メモリ	ストレージ	ネットワークインターフェース

プット (Mbps)	ア[1]	(DDR4)	要件	
50Mbps 以下	4	16 GB RAM	最小 205 GB	最低 2 つのネットワークインターフェース
50 ~ 150 Mbps	16	32 GB RAM	最小 205 GB	最低 2 つのネットワークインターフェース
150 ~ 300 Mbps	32	64 GB RAM	最小 205 GB	最低 2 つのネットワークインターフェース
300 Mbps ~ 1 GB	32-64	128 GB RAM 以上	最小 205 GB	最低 2 つのネットワークインターフェース

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)

標準インストールプロセスでは、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) を付けて設定されている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、大企業のお客様にも RAID ディスクを必須条件にはしていません。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の要件

OT Security をインストールする前に、デバイスに 2 つ (以上) 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 はこのようなインターフェースを自動的に作成します。ISO (Hyper-V など) をインストールする時は、これらのインターフェースを手動で作成します。

注意: Tenable は、10 G 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、10 G ネットワークカードを使用しても 10 G の速度は保証されていません。

NIC の要件

- OT Security が必要とする EM 用の NIC は 1 つのみです。
- OT Security では、ICP 用とセンサー用に最低 2 つの NIC が必要です。
- OT Security では、ICP/EM/センサーに静的 IP アドレスを使用する必要があります。
- センサーと ICP の両方を、複数の SPAN インターフェースをモニタリングするように設定できます。

注意: OT Security 4.1 以降、ネットワークインターフェースのプロファイル名は次のようになっています。

- nic0 – システムポート 1
- nic1 – システムポート 2
- nic2 – システムポート 3
- nic3 – システムポート 4

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またはシステムポート1 (192.168.1.5)とnic3またはシステムポート4 (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またはシステムポート4 (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 + OT Security nic1またはシステムポート2の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アドレスと一致するようにしてください。

詳細については、Manually Configure a Static IP Address (静的IPアドレスの手動設定)、Manage System Networking (システムネットワークの管理)、および *VMwareのドキュメント*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

Tenable Core + OT Securityセンサー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`にアクセスできる必要があります。

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。
	Microsoft Hyper-V	.zip ファイル	
クラウド	Amazon Web Service (AWS)	該当なし	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が必要です。
クラウド	Microsoft Azure	該当なし	
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 Tenable Core + Tenable OT Security センサーの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。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

次の記載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	(デフォルト) Tenable Core インターフェースへの受信 HTTPS 通信。
TCP 8090	バックアップを復元するための受信 HTTPS 通信。 ファイルアップロードサーバーとの受信通信。

送信トラフィック

次の記載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 のアウトバウンド 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) には、インターフェースロールと呼ばれる、いくつかのネットワーク接続が必要です。

管理とアクティブクエリのインターフェース

このインターフェースには、アプライアンスの管理と設定を行うためのネットワークアクセスを許可する IP アドレスが 1 つ設定されています。このインターフェースにより、アプライアンスがアクティブクエリを実行するためにネットワーク上の資産にアクセスできます (推奨だが任意)。

管理ロールとアクティブクエリロールの分離 (ポート分割)

管理とアクティブクエリのロールを 2 つの異なるインターフェースに分離できます。これにより、たとえば、管理目的での IT ネットワークへの接続と、アクティブクエリを使用して OT 資産にアクセスするための OT ネットワークへの接続を分けることができます。

そのためには、それぞれのロール専用の 2 つのインターフェースを用意して接続します。

ICP システムがネットワーク接続を許可している限り、アクティブクエリインターフェースで ICP への基本的な管理接続が許可され、動作します。

OT Security セットアップを終了する際に管理接続が必要になります。ポート分割とアクティブクエリ接続は、後から設定できます。

Tenable 提供のハードウェアアプライアンスでは、OT Security が、デフォルトのインターフェースロールが設定されている (管理ロールとアクティブクエリロールが結合している) 状態で自動的にインストールされます。

> 注意: 両方のインターフェースに同じ IP アドレスを設定する場合、Tenable は管理ロール専用のインターフェースにのみデフォルトゲートウェイを設定することを推奨しています。ポート分割の設定時に、アクティブクエリ専用のゲートウェイを指定できます。

モニタリングインターフェース

1 つ以上のネットワークインターフェースをパッシブネットワーク監視用に使用できます。パッシブモニタリング (SPAN) インターフェース

- 分析のためにトラフィックを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。

> 注意: アプライアンスインターフェースで直接モニタリングできないトラフィックは、OT センサーまたはカプセル化リモート SPAN (ERSPAN) 設定を使用して収集できます。

ファイヤーウォールに関する考慮事項

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、次のポートは開いたままにしてください。

> 注意: EM で一元化されたアップデートが機能するには、ICP がポート 28305 および 8000 (TCP) に到達できる必要があります。

通信方向	ポート	通信先	目的
インバウンド	TCP 443	OT Security アプライアンスのウェブインターフェース	OT Security へのブラウザアクセス
インバウンド	TCP 8000	Tenable Core 用ウェブインターフェース	Tenable Core へのブラウザアクセス
インバウンド	TCP 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 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	TCP 443	Tenable Security Center	統合のためにデータを送信

通信方向	ポート	通信先	目的
ウンド			
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
アウトバウンド*	TCP 389 または 636	AD サーバー	AD LDAP 認証
アウトバウンド*	TCP 443	SAML プロバイダー	シングルサインオン
アウトバウンド*	UDP 161	SNMP サーバー	Tenable Core に対する SNMP 監視
アウトバウンド*	TCP 443	*.tenable.com *.nessus.org	自動プラグイン、アプリケーション、OS アップデート**

通信方向	ポート	通信先	目的
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

通信方向	ポート	通信先	目的
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 28304 (SSH) TCP 443 (HTTPS)	ICP/OT Security センサーペアリングのための SSH 接続。 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。

> 注意: OT Security は、これらのプロトコル全体に対するクエリをサポートしていますが、すべてのクエリがお客様の環境に適用されるわけではありません。最適な結果を得るために、OT Security (または OT Security センサー) と近隣のリモートデバイス間で、リストされているポートの中からできるだけ多くのポートを開いてください。このアクションにより、正確な識別とクエリが可能になります。

プロトコル	ポート	通信先	目的
ICMP		一般/その他	ネットワークレベルの資産検出/ping

プロトコル	ポート	通信先	目的
TCP	21	一般/その他	FTP ファイル転送
TCP/UDP	53	DNS サーバー	ドメインネームシステム (DNS) 解決クエリ
TCP	80	一般/その他	HTTP フィンガープリントおよびウェブインターフェースアクセス
TCP	102	Siemens デバイス	製造メッセージ仕様 (MMS)、IEC 61850 と重複
TCP	102	Siemens デバイス	変電所および SCADA デバイスの IEC 61850/MMS
TCP	102	Siemens デバイス	自動化デバイスの S7/S7+/MMS 通信
UDP	111	Emerson Ovation デバイス	Ovation の RPC サービス登録/検出
TCP	135	Windows デバイス	システムおよびネットワーク管理の WMI クエリ
UDP	137	一般/その他	Windows ネットワーク検出の NetBIOS ネームサービス (NBNS)
UDP	138	一般/その他	Windows ファイル/プリンター共有の NetBIOS データグラムサービス (NBT)
UDP	161	一般/その他	SNMP ポーリングおよびトラップ通信
TCP	443	一般/その他	HTTPS フィンガープリントおよび安全な

プロトコル	ポート	通信先	目的
			ウェブサービス
TCP	445	Windows デバイス	システム管理の WMI/SMB クエリ (一部のケースでは 135 に代わる)
TCP	502	OT デバイス	PLC およびメーターとの Modbus TCP 通信
UDP	1069	Cognex カメラ	Cognex ビジョンシステム検出プロトコル
TCP	1911	BMS コントローラー	Niagara FOX 非暗号化プロトコル
TCP	1962	Phoenix Contact デバイス	PC Worx エンジニアリングおよびコントロール通信
TCP/UDP	2001	Profinet デバイス	コントローラーおよび I/O モジュールの Profinet デバイス通信
TCP	2001	Siemens デバイス	SICAM/PROFINET (レガシーおよび変電所のデバイス)
TCP	2222	Rockwell デバイス	ControlLogix/PLC 通信の PCCC プロトコル
TCP	2404	SCADA デバイス	RTU および変電所通信の IEC 60870-5-104
TCP	3389	Windows デバイス	RDP (リモートデスクトッププロトコル)

プロトコル	ポート	通信先	目的
TCP	3500	Bachmann M1 デバイス	Bachmann M1 コントローラー通信
TCP	4000	Emerson デバイス	Emerson ROC 4000 コントローラーデータ/コントロール
TCP	4444	Schneider Electric	SmartX コントローラー (EcoStruxure Building Operation)
UDP	4800	Moxa デバイス	Moxa デバイス検出プロトコル
TCP	4911	BMS コントローラー	Niagara FOX セキュア (TLS/SSL) プロトコル
TCP	5001	Bosch デバイス	Bosch PSI (プログラマブルシステムインターフェース)
TCP	5002	Mitsubishi デバイス	MELSEC PLC MC プロトコルオーバー TCP
TCP	5007	Mitsubishi デバイス	MELSEC PLC 追加通信ポート
UDP	5009	Mitsubishi デバイス	MELSEC Finder ブロードキャスト (デバイス検出)
TCP	5033	Siemens デバイス	P2 プロトコル (レガシー Siemens 自動化システムで使用)
TCP	5050	Saia-Burgess デバイス	Saia PCD コントローラー通信

プロトコル	ポート	通信先	目的
TCP	5094	HART-IP	スマートインストルメンテーションの HART-IP オーバー TCP
TCP	5313	Yokogawa DCS	CENTUM DCS エンジニアリングインターフェース
TCP	5432	SEL (Schweitzer) デバイス	エネルギーデバイスの PostgreSQL データベースアクセス
TCP	6626	WAGO デバイス	WAGO I/O 通信およびプログラミング
TCP	7700	Schneider Electric	ION パワーメーターおよびエネルギー管理システム
TCP	8000, 8008, 8080, 8443, 8800	一般/その他	共通 HTTP/HTTPS 代替ポート
TCP	9940	Yokogawa DCS	CENTUM ステータスおよび診断
UDP	12321	Honeywell デバイス	Honeywell FTE UDP 検出/冗長性
TCP	18245	Schneider デバイス	M340/M580 PLC の SRTP (Schneider リアルタイムプロトコル)
TCP	18507	Emerson デバイス	Emerson ROC/フローコンピューター (FACE プロトコル)
TCP	18508	Emerson デバイス	Emerson ファームウェアアップグレードサービス (UPGD)

プロトコル	ポート	通信先	目的
TCP	20256	GE デバイス	Proficy iFIX/CIMPLICITY SCADA の PCOM プロトコル
TCP	20547	Procon	PROCON OS リモート管理インターフェース
TCP	24576	ABB デバイス	変電所自動化の ABB ネットワークコントロール (ABB_NC) プロトコル
TCP	34964	Siemens デバイス	PROFINET 接続管理 (PROFINET CM)
TCP	39329	Emerson デバイス	Ovation/VME ベースのコントロールシステム
TCP/UDP	44818	OT デバイス	Rockwell デバイスの CIP (Common Industrial Protocol)
UDP	47808	BMS コントローラー	建物自動化デバイスの BACnet/IP 通信
TCP/UDP	48898	Beckhoff デバイス	コントローラーおよびエンジニアリング通信の ADS/TwinCAT プロトコル
UDP	48899	Beckhoff デバイス	ADS/AMS 検出 (TwinCAT/Beckhoff IPC)
TCP	50000	Siemens デバイス	SIPROTEC 4 リレー通信
TCP	51966	Honeywell デバイス	Honeywell FTE (Fault Tolerant Ethernet) 通信

プロトコル	ポート	通信先	目的
TCP	55553	Honeywell デバイス	Experion PKS の CEE (Control Execution Environment) 通信
TCP	55565	Honeywell デバイス	Experion PKS の冗長性のための FTE (Fault Tolerant Ethernet) 通信

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

OT エージェント

通信方向	ポート	通信先	目的
アウトバウンド	443	OT Security	OT エージェントとの初回ペアリング
アウトバウンド	28306	OT Security	OT エージェントとの接続。

IoT コネクタエージェント

通信方向	ポート	通信先	目的
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
アウトバウンド	TCP 10104 (安全でないポート)	IoT コネクタ	ICP を IoT コネクタエージェントに接続する

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。

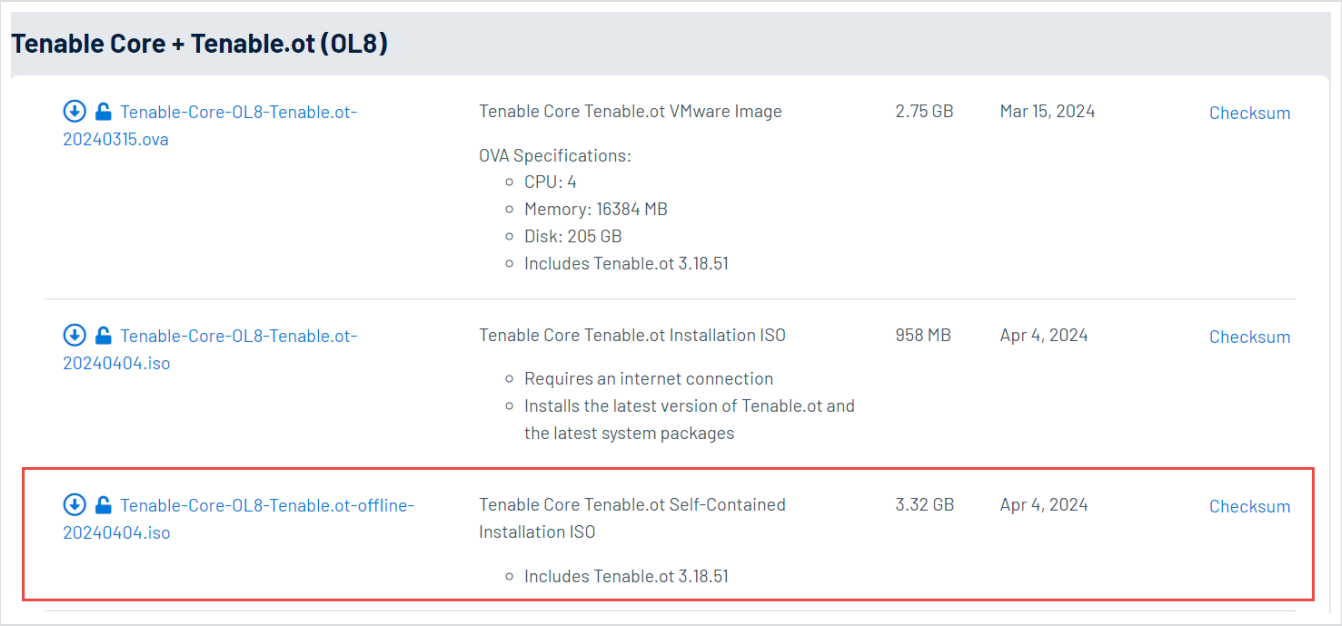
始める前に

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。

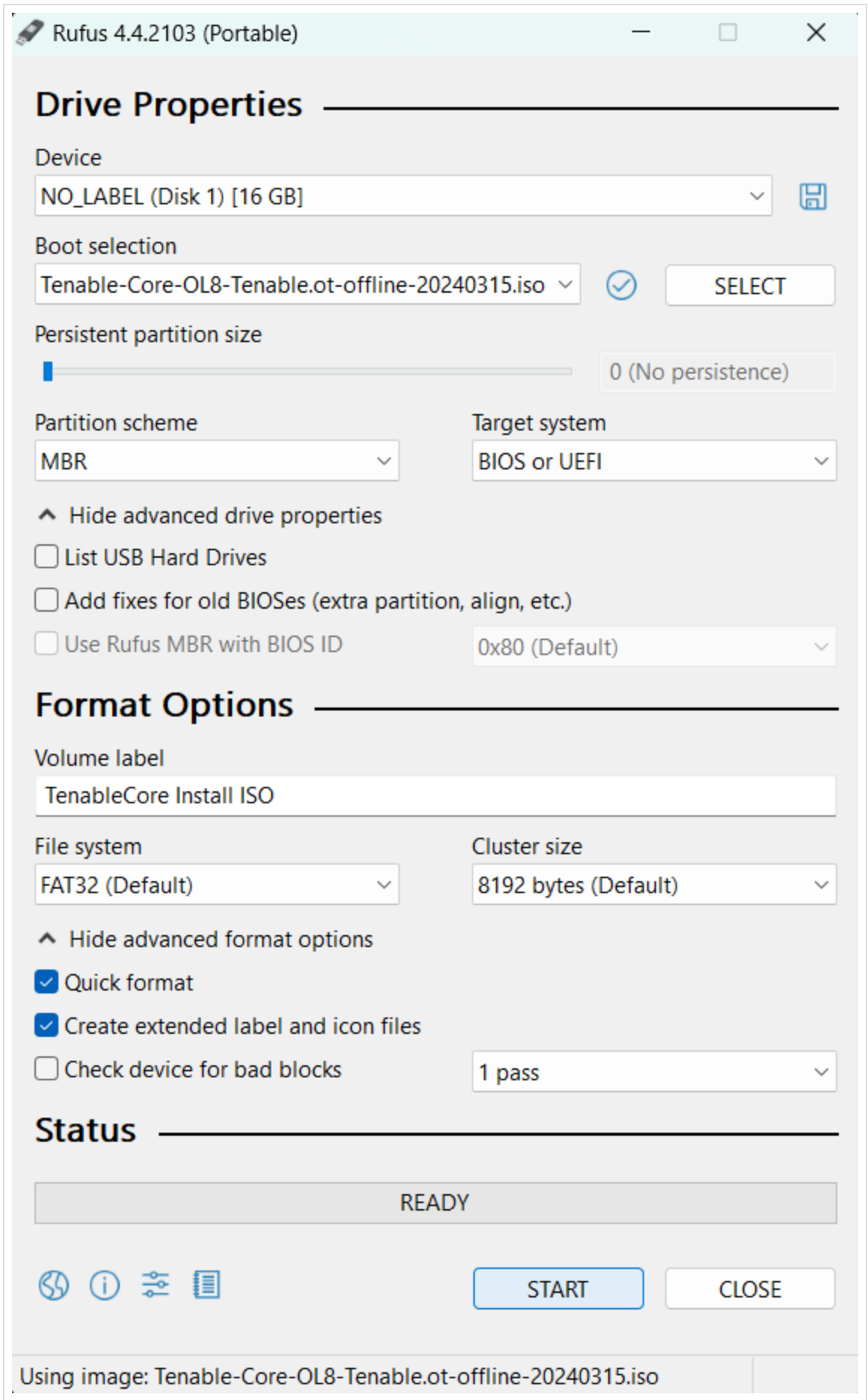
1. Tenable のダウンロードから最新のオフライン ISO ファイルをダウンロードします。

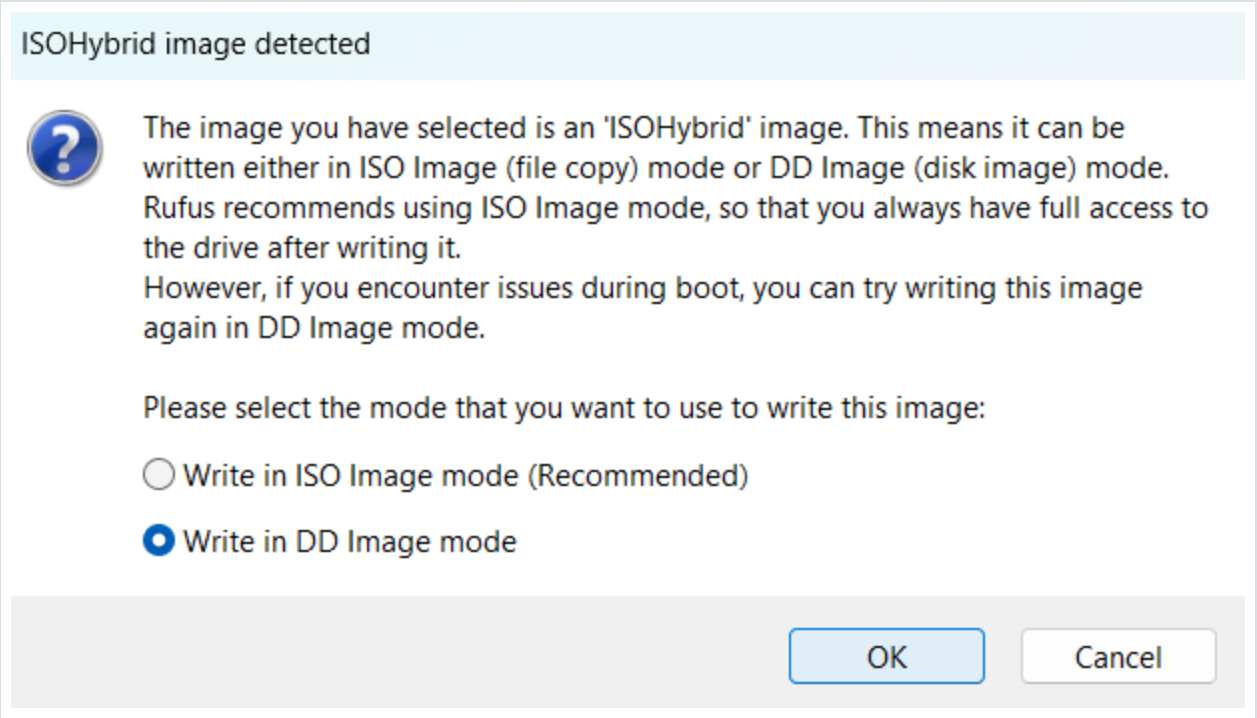


Tenable Core + Tenable.ot (OL8)

Tenable-Core-OL8-Tenable.ot-20240315.ova	Tenable Core Tenable.ot VMware Image OVA Specifications: ○ CPU: 4 ○ Memory: 16384 MB ○ Disk: 205 GB ○ Includes Tenable.ot 3.18.51	2.75 GB	Mar 15, 2024	Checksum
Tenable-Core-OL8-Tenable.ot-20240404.iso	Tenable Core Tenable.ot Installation ISO ○ Requires an internet connection ○ Installs the latest version of Tenable.ot and the latest system packages	958 MB	Apr 4, 2024	Checksum
Tenable-Core-OL8-Tenable.ot-offline-20240404.iso	Tenable Core Tenable.ot Self-Contained Installation ISO ○ Includes Tenable.ot 3.18.51	3.32 GB	Apr 4, 2024	Checksum

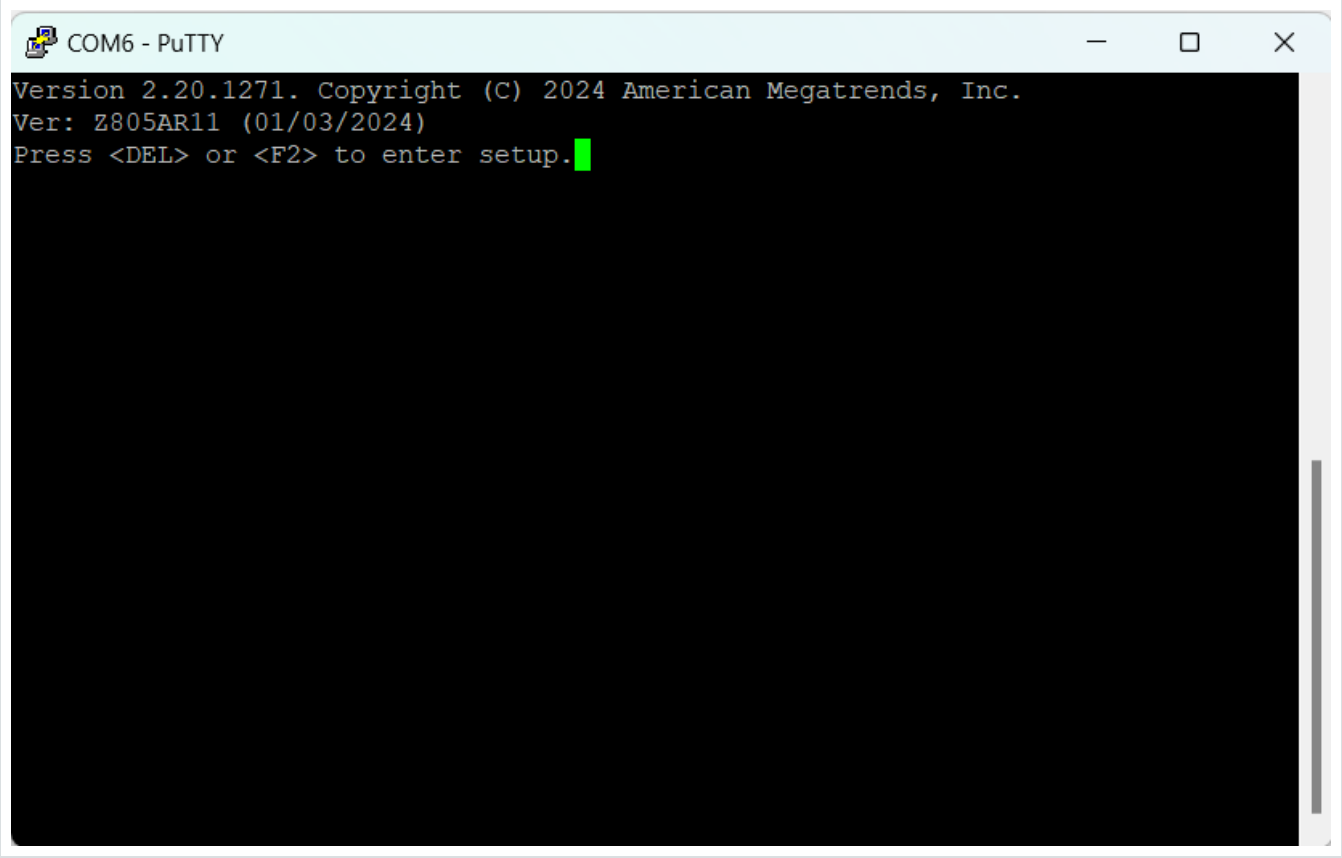
2. USB ドライブを PC に差し込み、ISO を DD モードでフラッシュドライブにフラッシュします。


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



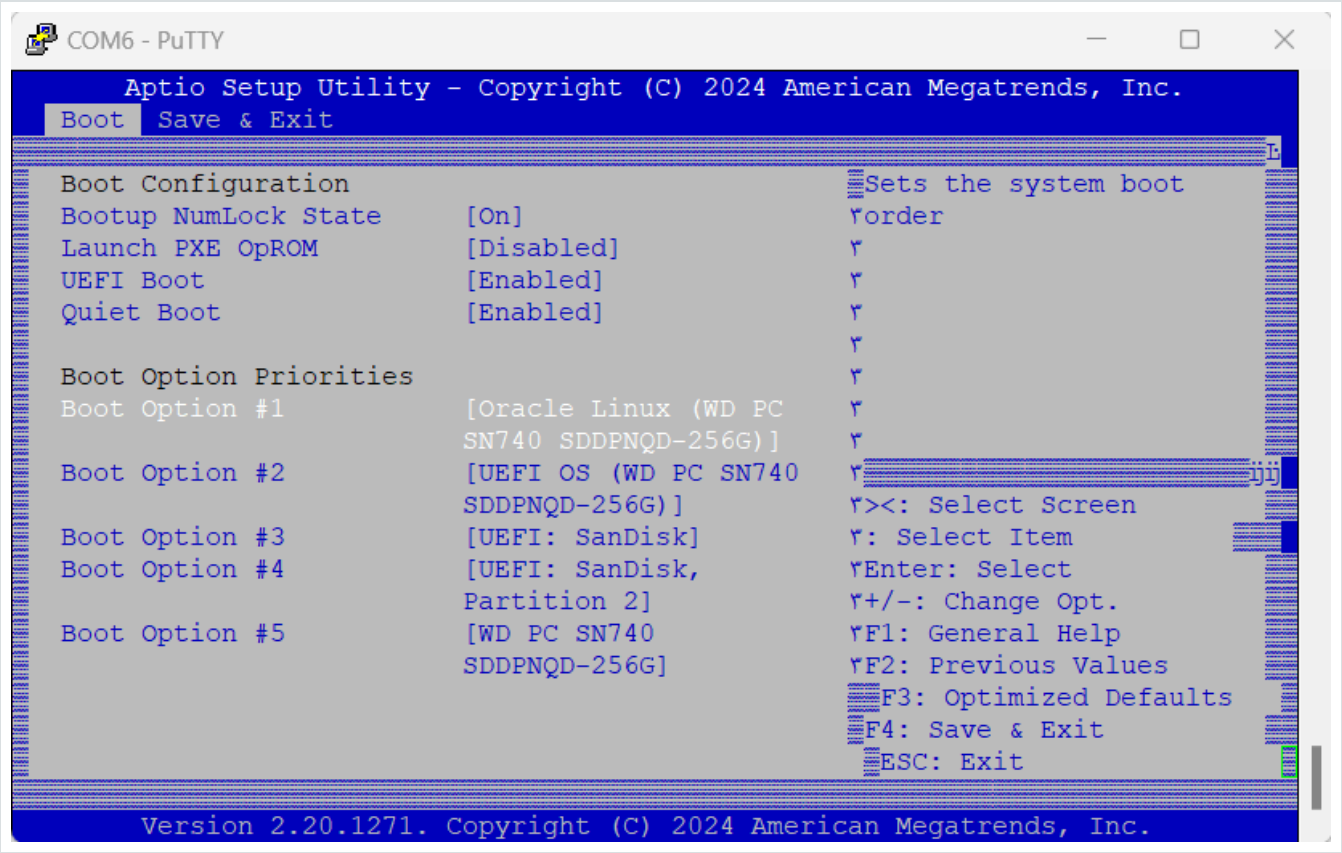
3. 終了したら、USBドライブをOT Securityアプライアンスの USB ポートに差し込みます。

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。



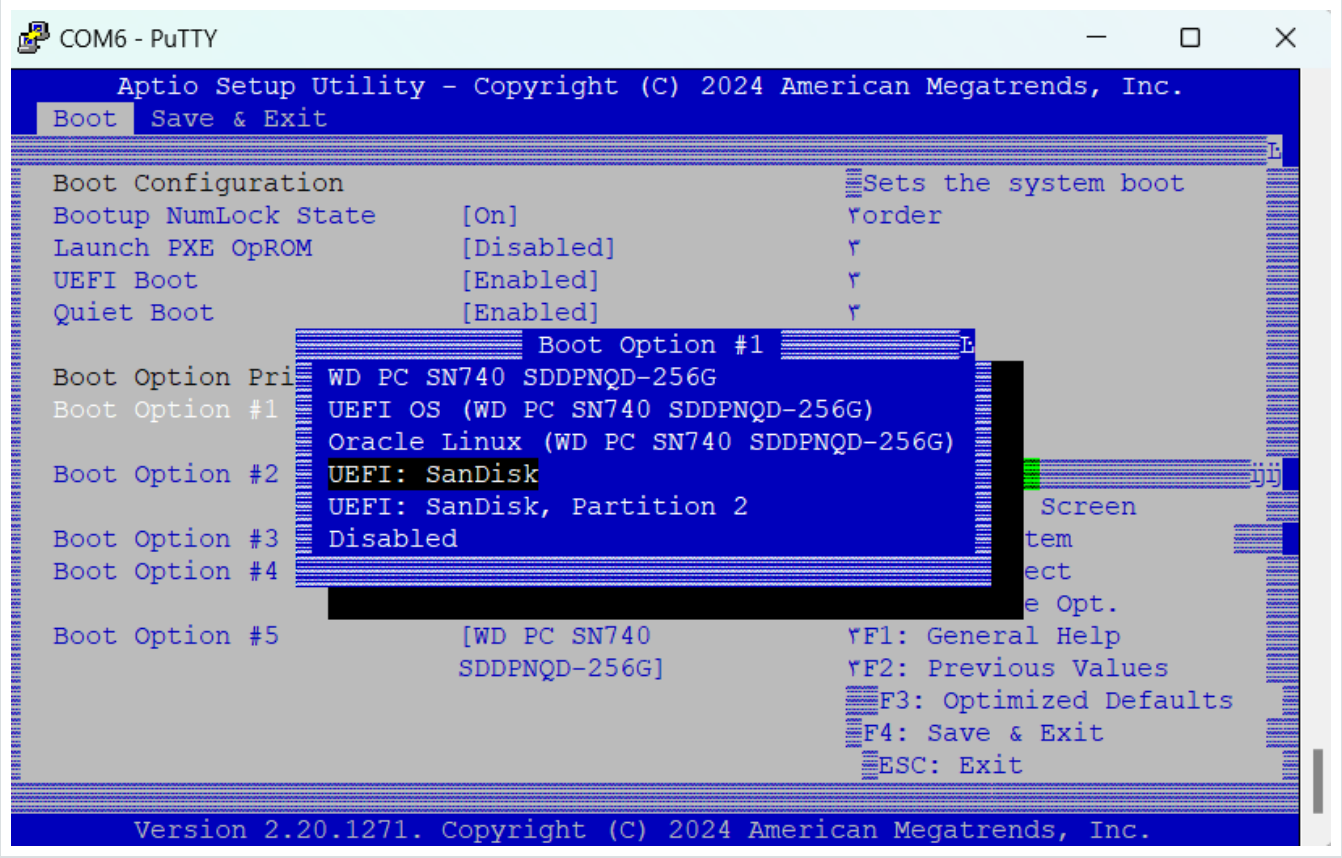
5. プロンプトが表示されたら、<DEL> を押してセットアップに入ります。

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。

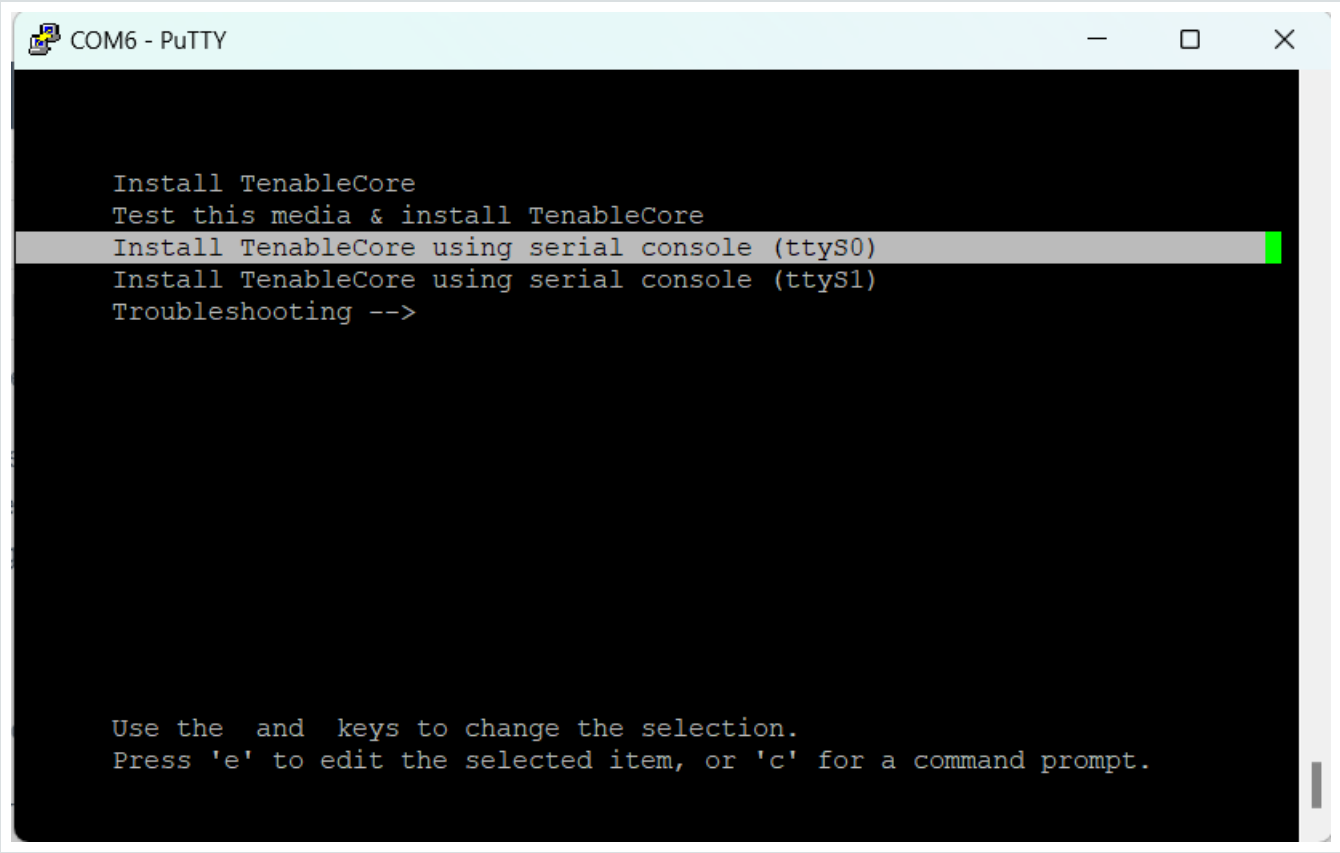


> 注意: アプライアンスでサポートされているなら「ワンショット起動」機能を使用できます。

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: ご使用のハードウェアがモニター出力 (VGA、HDMI) をサポートしている場合は、[Install TenableCore] (TenableCore をインストール) 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。

仮想マシンとして Tenable Core + OT Security をデプロイする方法

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 をインポートします。
   仮想マシンの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。
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ています。

> ヒント: 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、ネットワークモニタリングとアクティブクエリの両方に使用できます。状況に応じてネットワークインフラを準備してください。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。

管理とアクティブクエリ

必要に応じ、選択したネットワークインターフェースを、ICP への管理接続を許可するように設定されたネットワークスイッチインターフェースに接続します。

Tenable Core から、選択した OT Security アプライアンスインターフェースに対して 1 個の IP アドレスとその他の接続設定を設定してください。

管理ロールとアクティブクエリロールを分離する場合は、選択した各インターフェースが専用スイッチインターフェースに接続されていることを確認してください。それぞれに IP アドレスを割り当て、両方の機能でネットワークに到達できるようにスイッチインターフェースを設定します。

詳細については、管理ロールとアクティブクエリロールの分離 (ポート分割) を参照してください。

ネットワークモニタリング

パッシブネットワーク監視用に選択された1つ以上のアプライアンスインターフェースを、ネットワークスイッチの設定済みポートミラーリングデスティネーション (SPAN/RSPAN) インターフェースに接続します。OT ネットワークプロトコルと通信を適切に可視化できるようにポートミラーリングを設定する必要があります。

> 注意: アプライアンスインターフェースで直接モニタリングできないトラフィックは、OT センサーまたはカプセル化リモート SPAN (ERSPAN) 設定を使用してキャプチャできます。

OT Security アプライアンスをネットワークに接続する方法

ハードウェアアプライアンスの場合

Tenable 提供のハードウェアアプライアンスには、さまざまな量やタイプ (RJ45 または SFP) のネットワークインターフェースが付属しています。OT Security には、各ロール用にデフォルトで選択されているインターフェースがプリインストールされています。必要に応じて、この設定を後から変更できます。

Tenable 提供ではないハードウェアでは、各ロール用のインターフェースを選択してから、OT Security インストールプロセスを手動で開始する必要があります。各ロールで利用可能なインターフェースを正しく使用するようにしてください。

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。デプロイメント中または後から、ほかのネットワークアダプターやインターフェースを追加できます。

`.iso` または `.zip` (Hyper-V) 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、必要な数のネットワークインターフェースを設定してください。

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。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 または Hyper-V 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。

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。

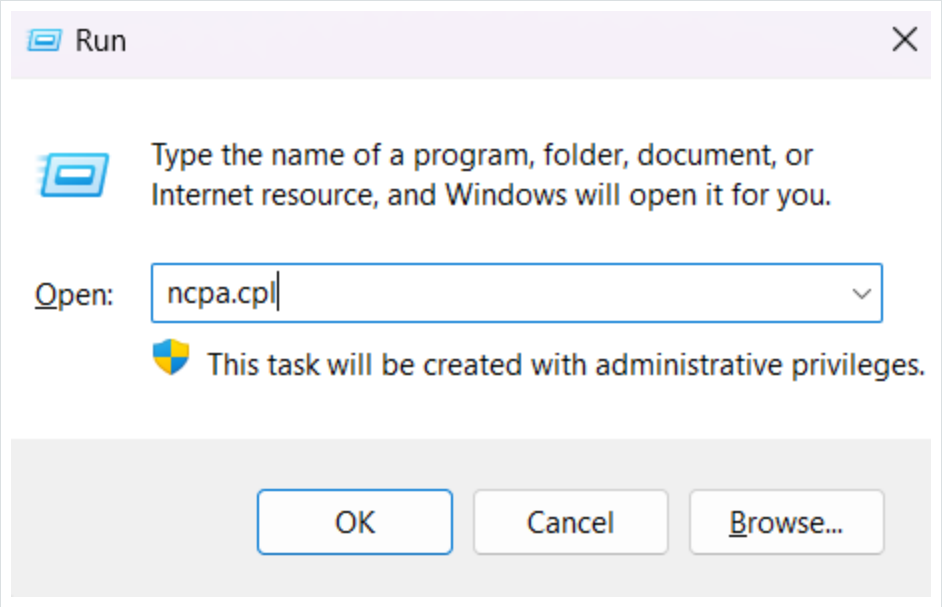
管理 IP アドレスを設定していない場合は、直接接続された PC または適切に設定されたネットワークを使用して、次のいずれかから Tenable Core ユーザーインターフェースにアクセスできます。

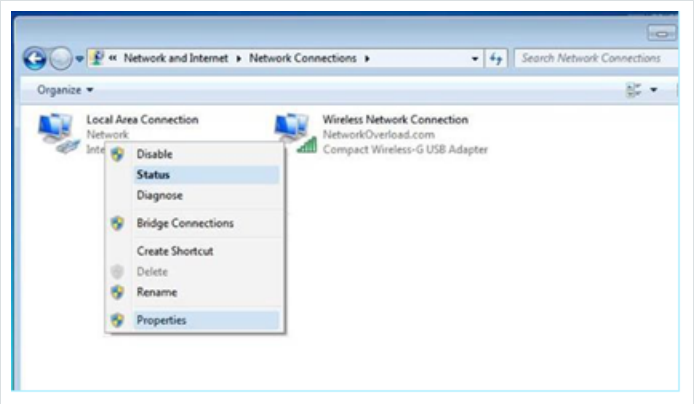
- システムポート 1 – IP アドレス 192.168.1.5/24 で事前設定された、デフォルトの管理インターフェース。
- システムポート 4 – IP アドレス 192.168.3.3/24 で事前設定された、エンジニアリングインターフェース。後から変更しない場合は、リカバリプロセスに使用できます。

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。

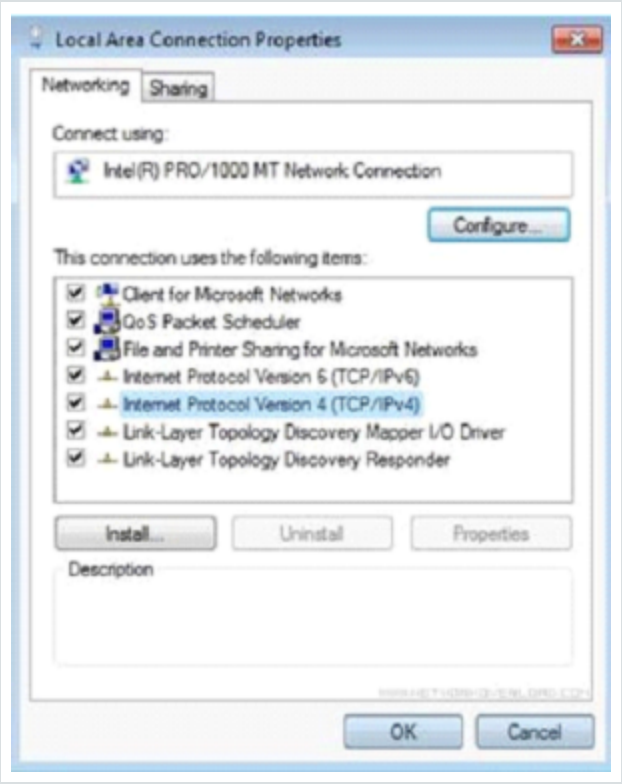
2. Windows で win+R キーを押して [ファイル名 を指 定して実 行] を開き、`ncpa.cpl` と入 力して [ネットワーク接 続] を開きます。





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。

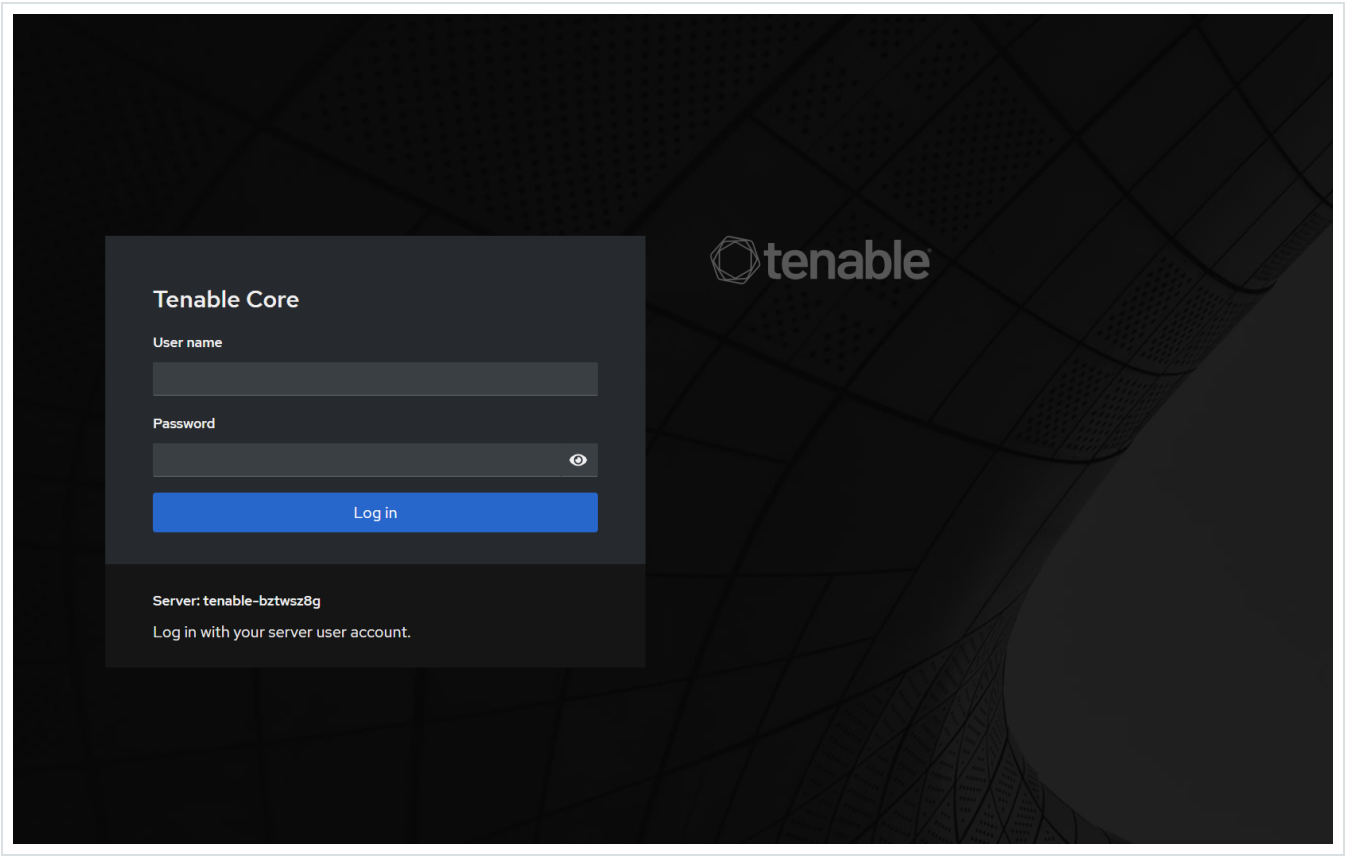
   [ローカルエリア接 続 プロパティ] ウィンドウが表 示されます。



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、システムポート 1 のデフォルトアドレスの場合は 192.168.1.10、システムポート 4 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、すぐに設定できるプロンプトが表示されます。そこから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。

    管理者アカウントを作成したら、Tenable は管理 IP アドレスを設定することをお勧めしています。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: 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、管理者アクセスを有効にして、ネットワーク設定を編集してください。

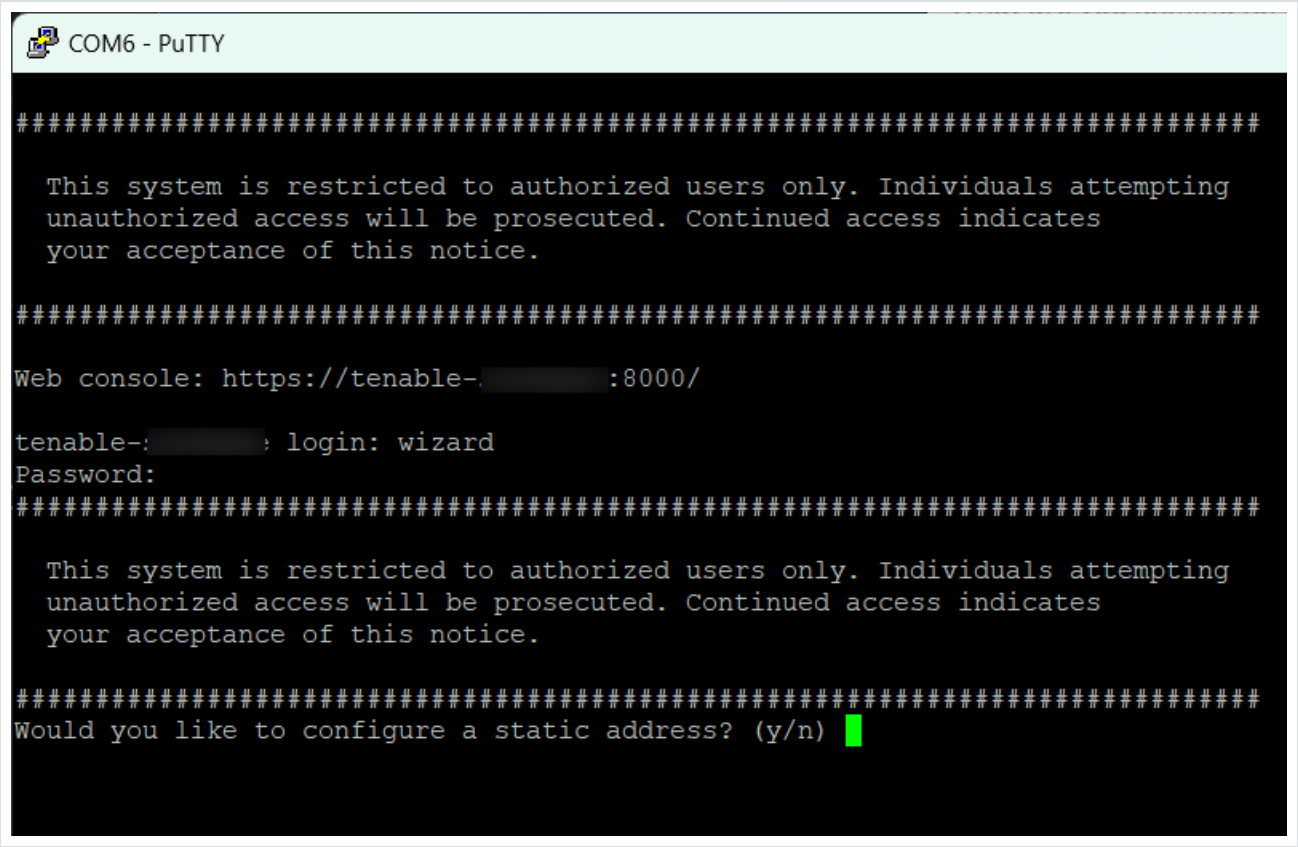
CLI を使う初期設定 (オプション)

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。

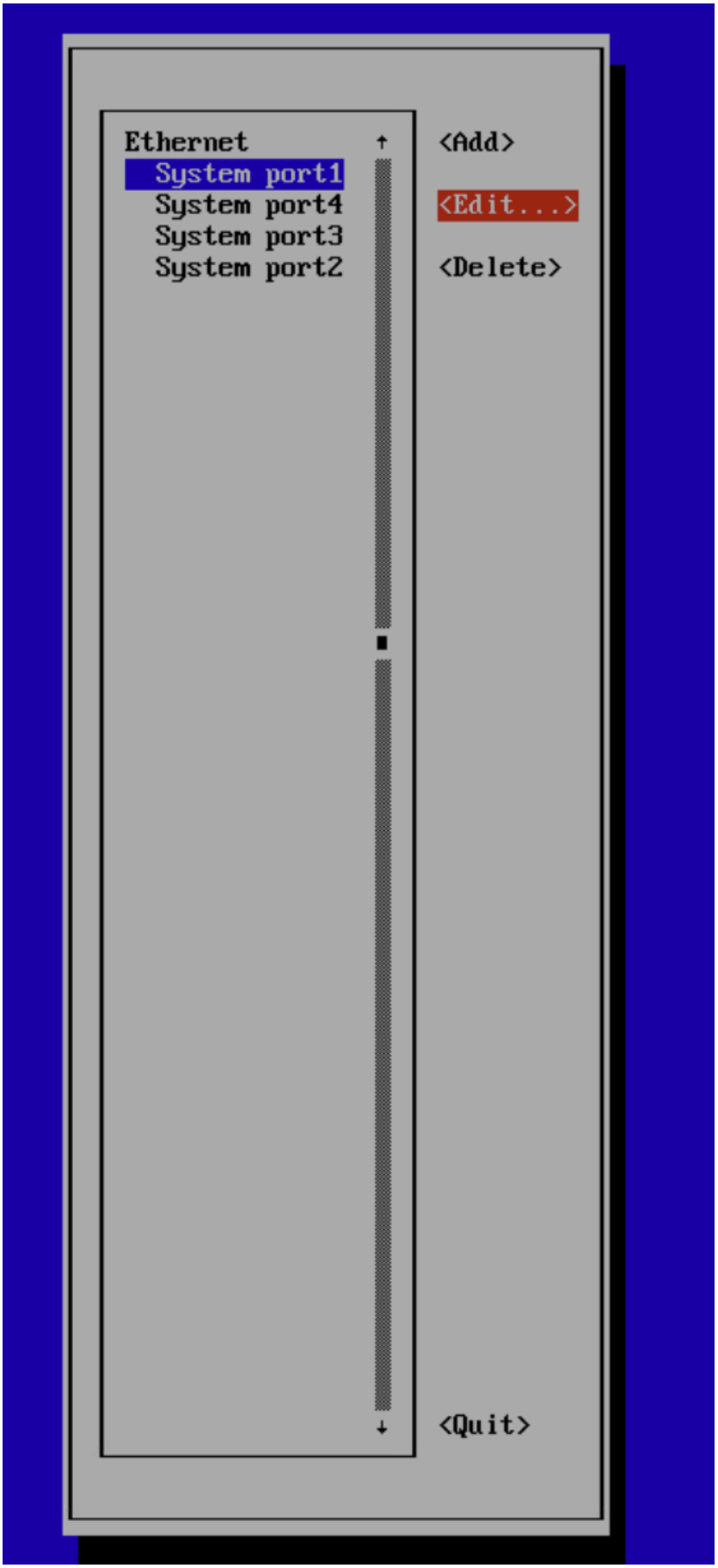
   [ネットワークマネージャー] ターミナルインターフェースが表示されます。



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。

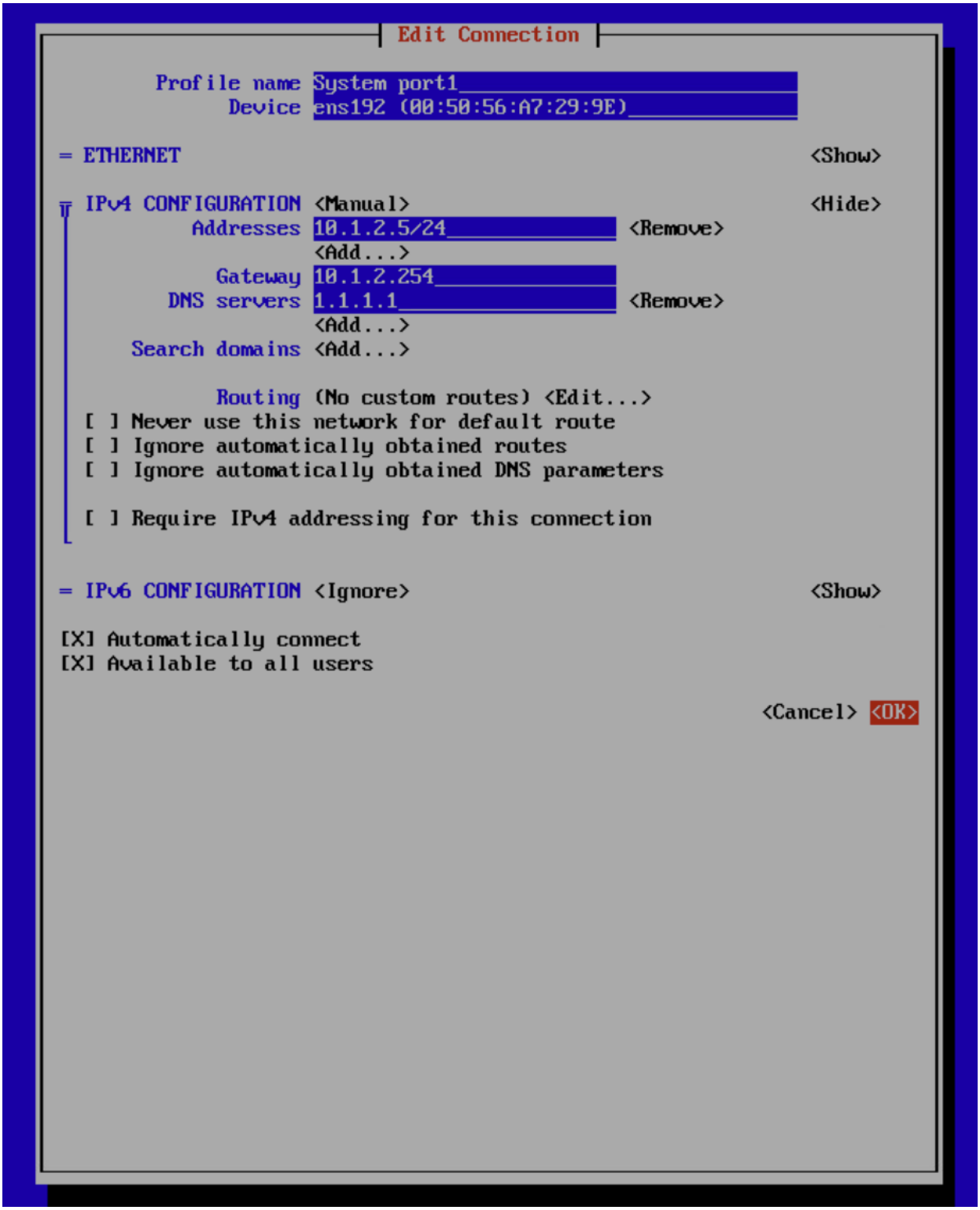
> 注意: この手順をスキップする場合は、`sudo nmtui` コマンドを使用することで、いつでもこのオプションにアクセスできます。

a. [System Port 1] (分割ポート設定を使用している場合は [System Port 3]) を選択します。


Ethernet
System port1
System port4
System port3
System port2
<Add>
<Edit...>
<Delete>
<Quit>

b. Enter を押します。

[接続の編集] ウィンドウが表示されます。



c. [IPV4 設定] ボックスで、オプションを <自動> から <手動> へ変更します。

> 注意:
>
> - 仮想マシンや、Tenable が提供していないハードウェアでは、ポート 1 は自動 IPv4 設定 (DHCP) に事前設定されています。
> - Tenable が提供するアプライアンスでは、ポート 1 は 192.168.1.5/24 に事前設定されています。このポートを使って初期設定のためにアプライアンスへ直接接続し、その後は Tenable Core の UI の [ネットワーキング] タブや、CLI から `sudo nmtui` コマンドを使用して変更できます。

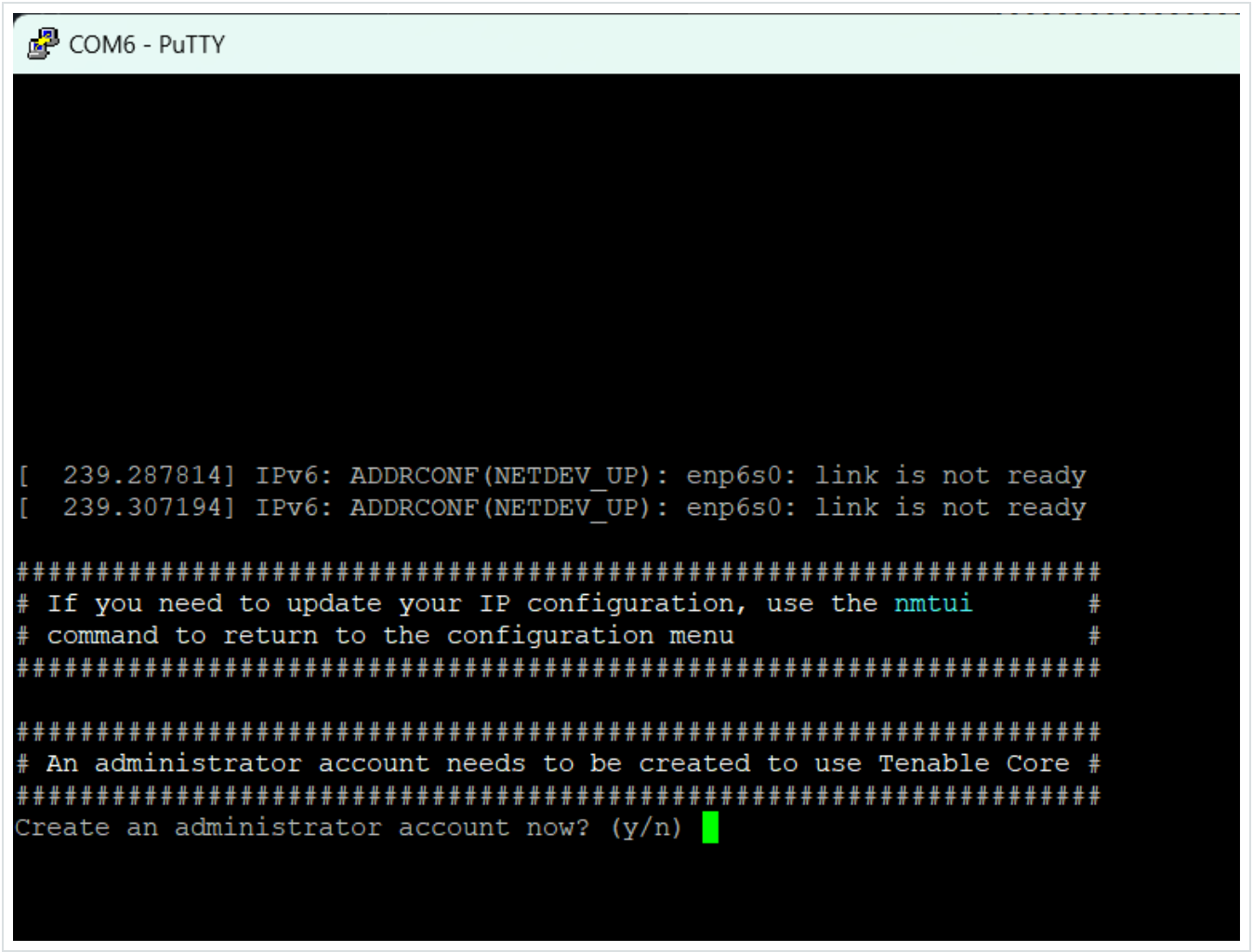
d. 矢印キーを使用して移動し、必要な IP アドレス、デフォルトゲートウェイ、DNS サーバーを設定します。この設定は後で変更できます。

e. 下矢印で画面の一番下まで移動し、<OK> を選択します。

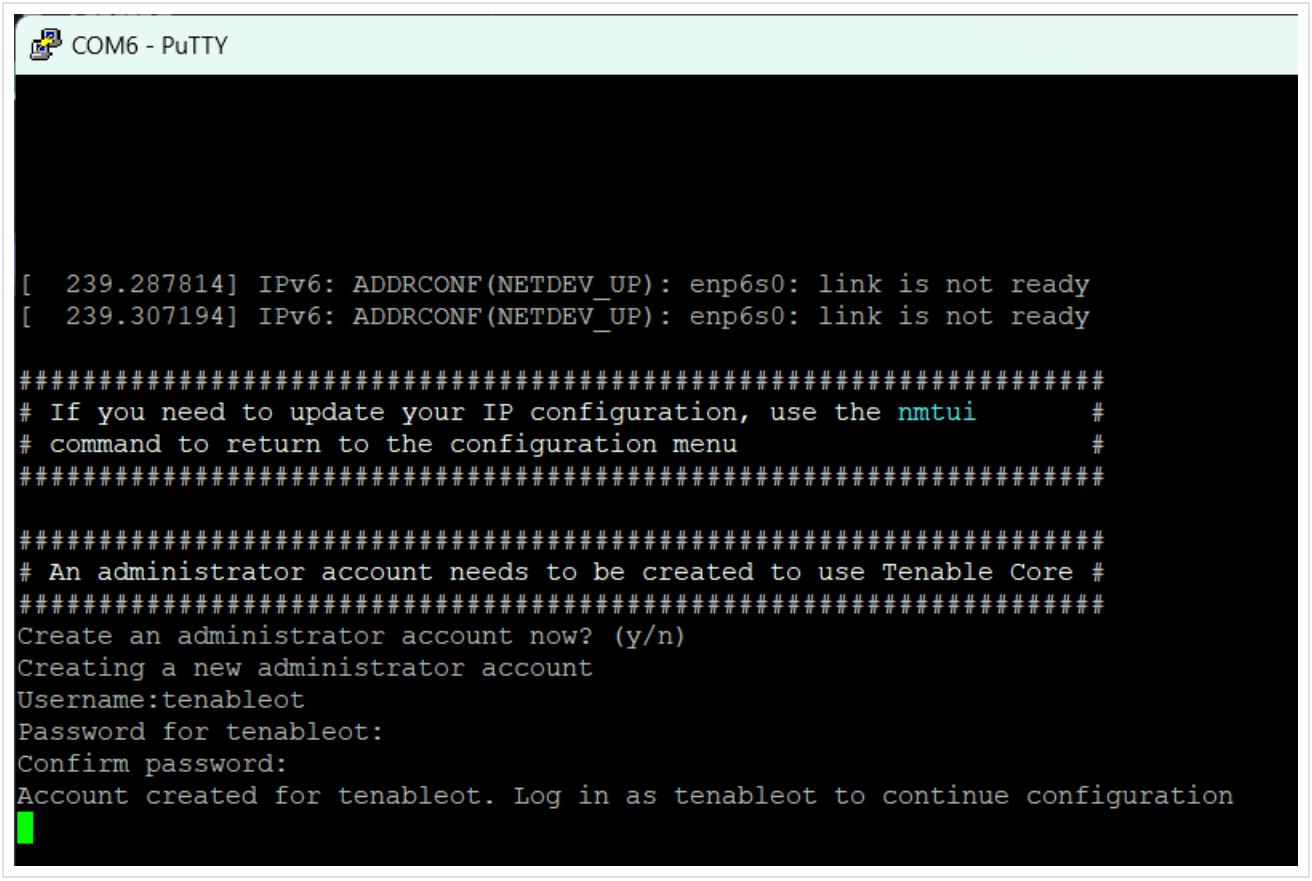
[ネットワークマネージャー] ウィンドウが表示されます。

4. <Quit> を選択します。

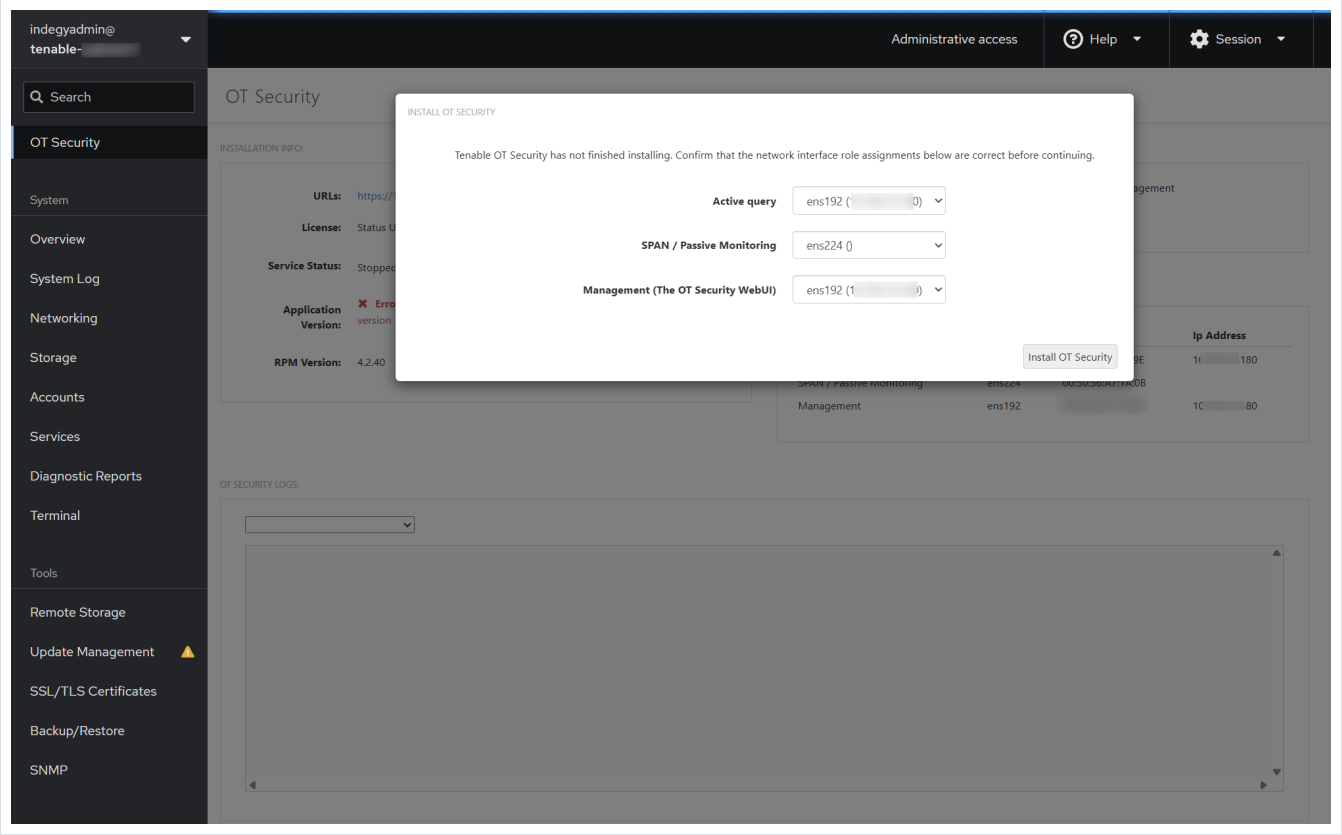
[ネットワークマネージャーターミナル] ウィンドウが表示され、管理者アカウントを作成するためのプロンプトが表示されます。



5. **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。



6. アカウント作成後、コンソール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アクセスし、ログインします。



仮想マシンや Tenable が提供していないハードウェアでは、Tenable Core > **OT Security** ページに OT Security をインストールするためのプロンプトが表示されます。

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 提供のハードウェアアプライアンスには OT Security アプリケーションがプリインストールされています。カスタムハードウェアまたは仮想的に OT Security をデプロイする場合は、インストールプロセスを手動で開始する必要があります。

> **注意:** 各インターフェースにロールを割り当ててから、OT Security アプリケーションのインストールを開始してください。必ず Tenable Core でインターフェースを設定し、適切な接続を許可するようにネットワークインフラを準備してください。詳細については、ネットワークに関する考慮事項と OT Security のネットワーク接続を参照してください。

始める前に

- 管理者アクセスがあることを確認してください。
- Tenable Core 仮想および物理アプライアンスで SSH または Cockpit アクセスがあることを確認してください。

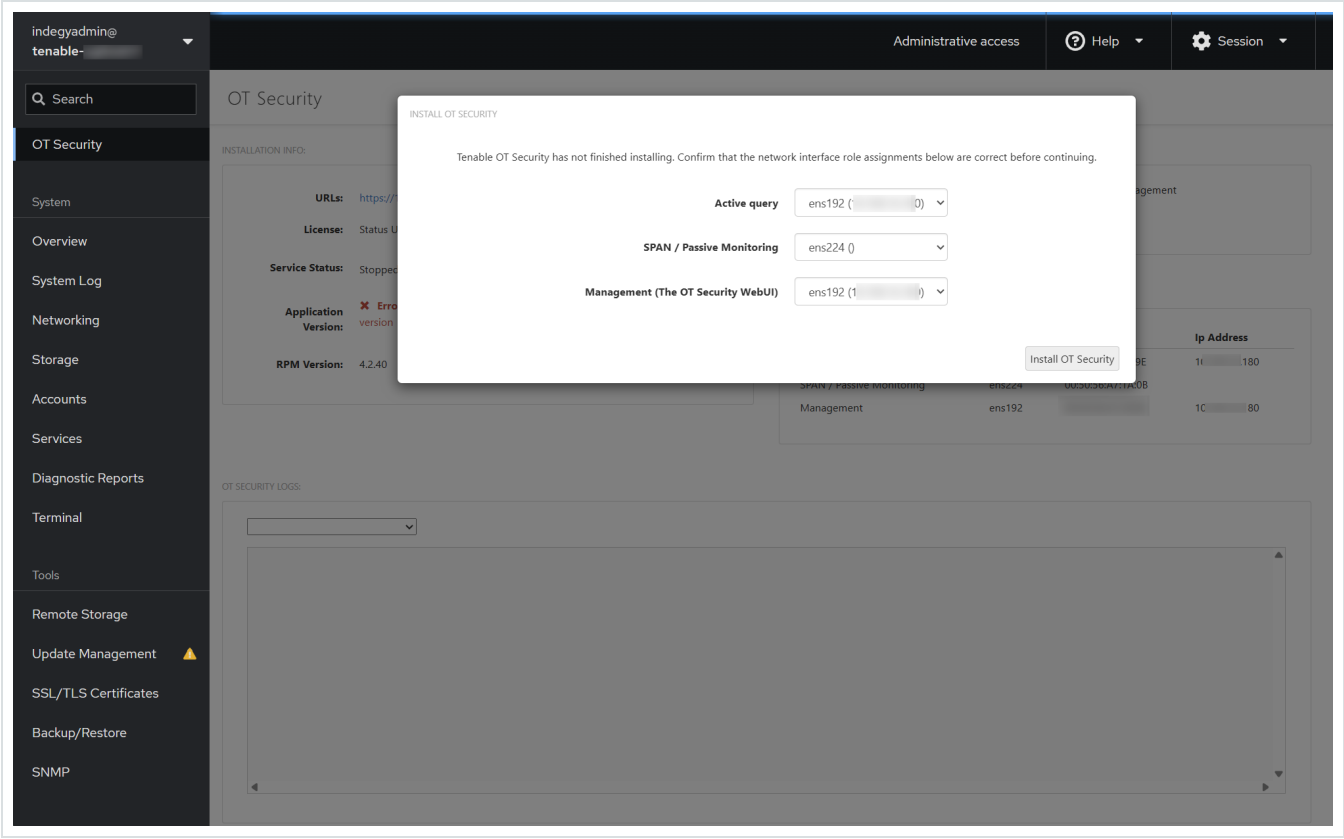
> 注意: 管理者アカウントは、定期的にサインインしてパスワードを更新しないと、アクセスできなくなる可能性があります。パスワードの期限切れにより管理アカウントがロックされた場合は、リモートロック解除ユーティリティを使用してアカウントをロック解除できます。アカウントロックアウトが発生した場合、このユーティリティにより、ICP は接続されたセンサーをリモートでロック解除でき、OT Security Enterprise Manager (EM) は接続された ICP をリモートでロック解除できます。このユーティリティの使用について詳しくは、ナレッジベース記事 Leveraging the Remote Unlock Feature in Tenable Core (Tenable Core のリモートロック解除機能を利用する) を参照してください。

Tenable Core で 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 `https://<mgmt-ip>:8000` にアクセスして、Tenable Core にログインします。
2. **OT Security** に移動します。

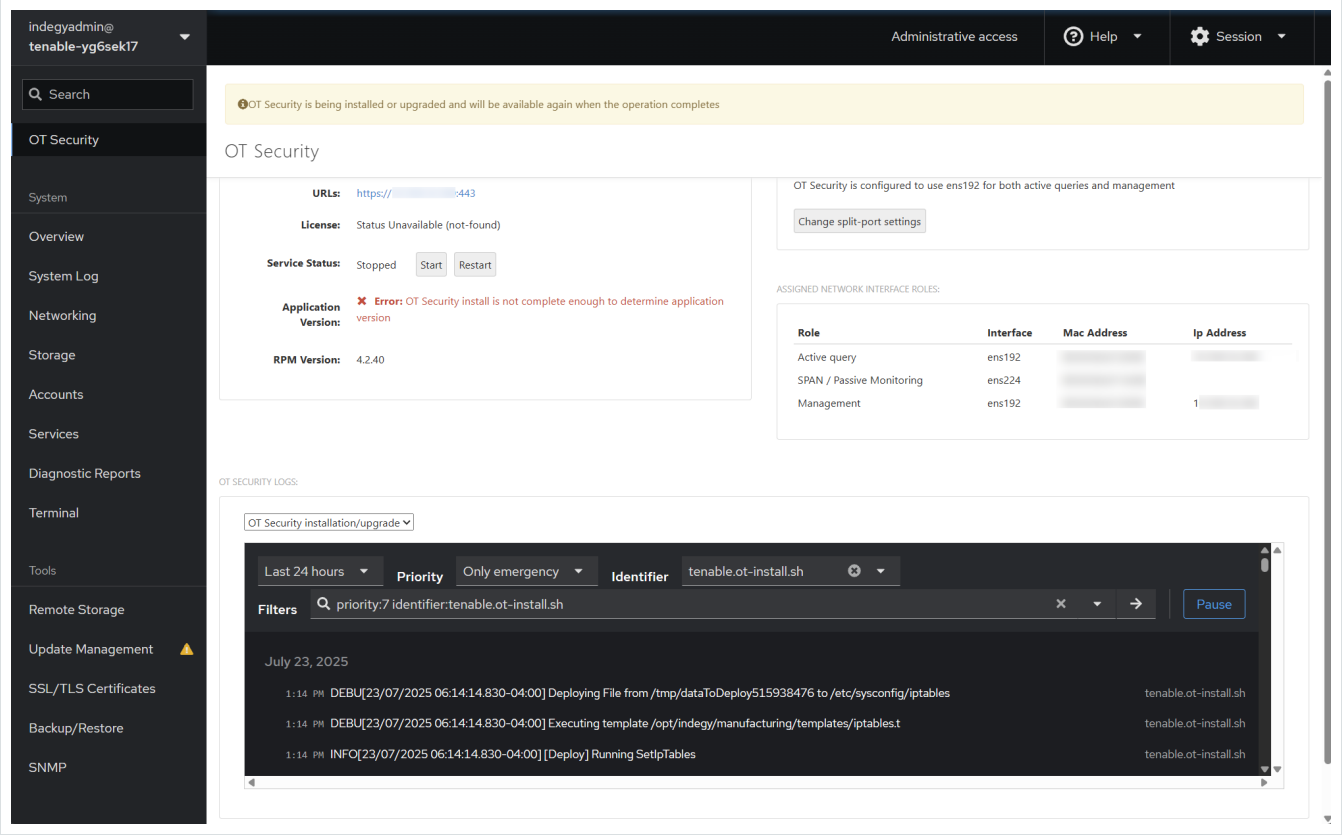
   [OT Security] ページが表示されます。

> 注意: 仮想マシンおよび非 Tenable ハードウェアでは、OT Security をインストールするプロンプトが表示されます。

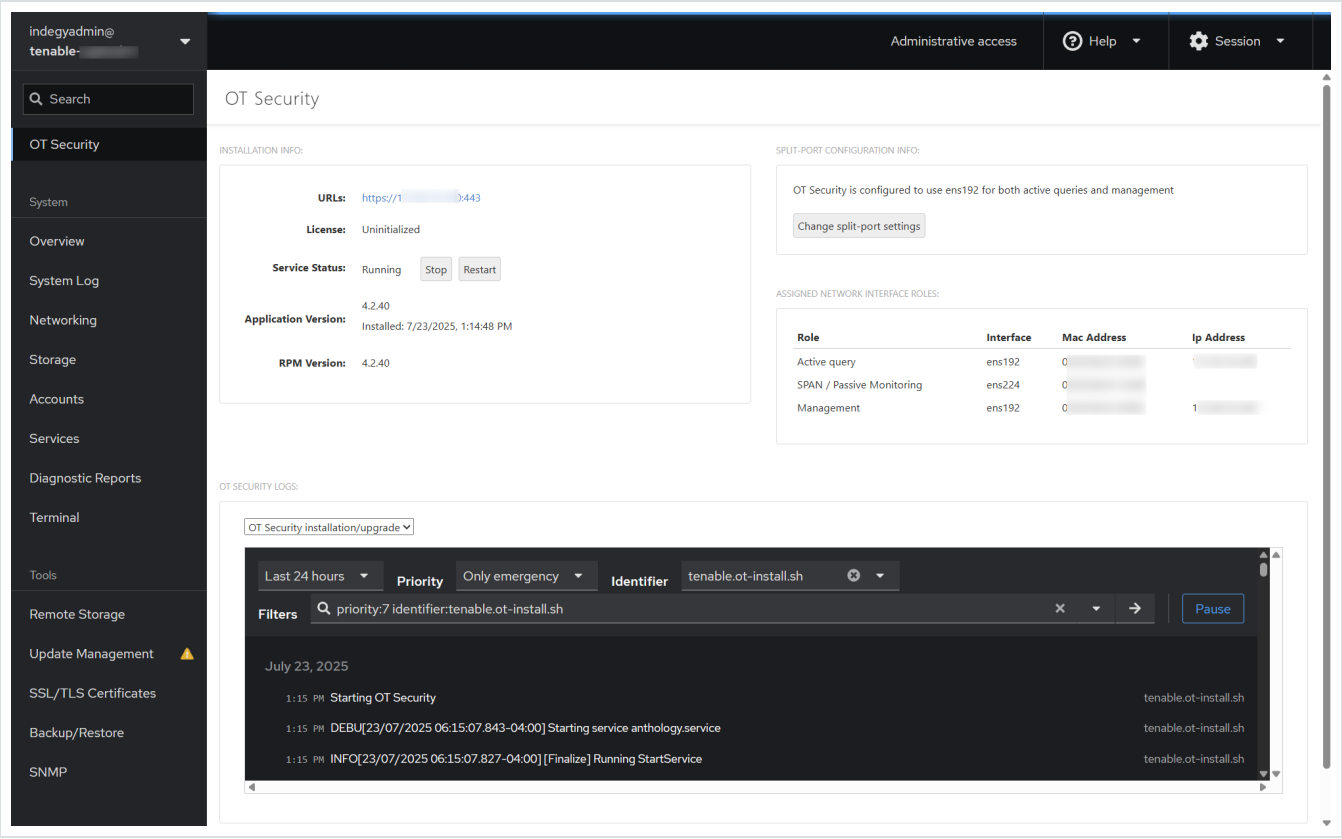


3. [**Tenable OT Security** をインストール] をクリックします。

   Tenable Core はインストールを開始し、黄色のバナーに「`OT Security`がインストール中またはアップグレード中です。この操作が完了してから再び使用できるようになります。」のメッセージが表示されます。

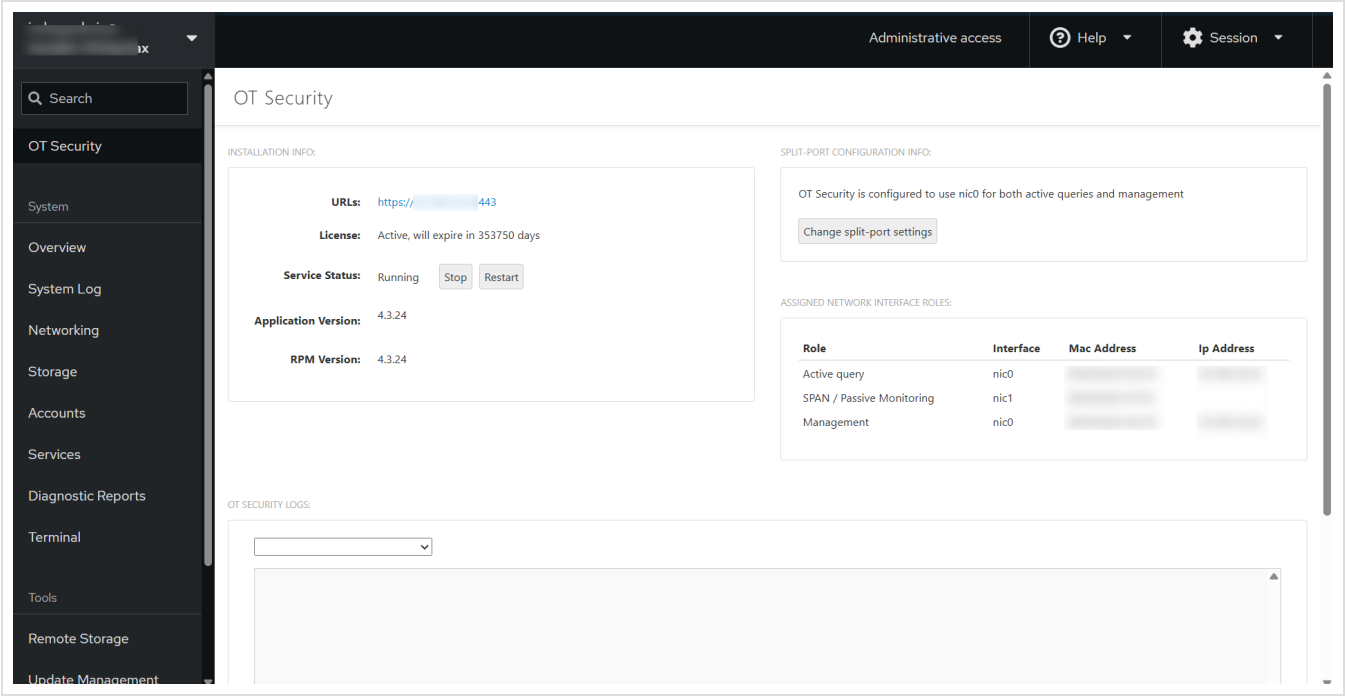


インストールが完了すると、黄色のバナーが消えて、[ライセンス] ステータスが [使用不可] から [未初期化] に変わります。



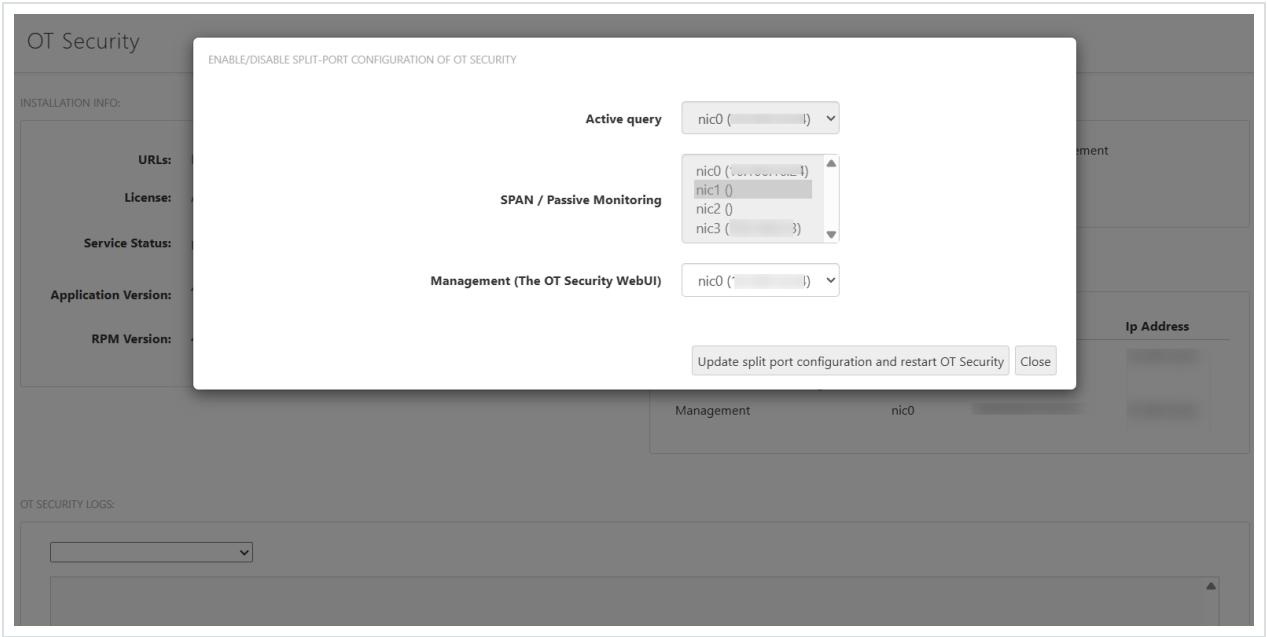
4. (任意) インターフェースロールを選択します。

> 注意: デフォルト設定を維持することもできます。デフォルトのインターフェース設定では、ポート 1 は管理 + アクティブクエリ、ポート 2 はパッシブモニタリングになります。

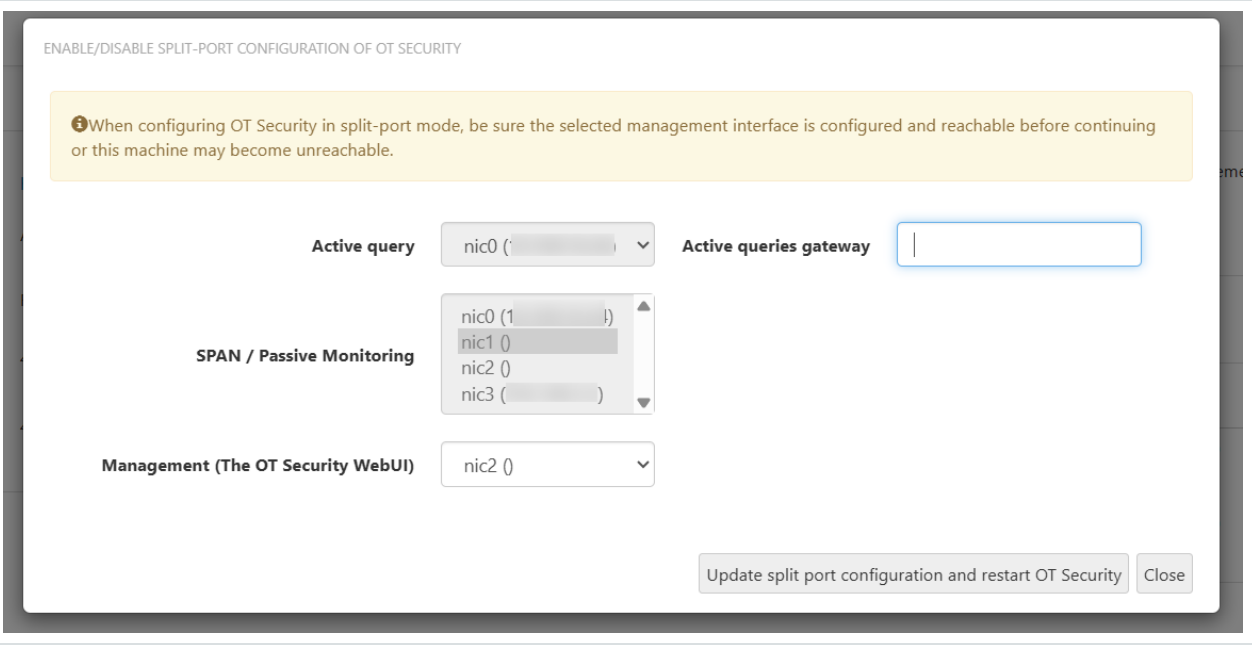


a. [ポート分割の設定情報] セクションで、[ポート分割の設定変更] をクリックします。

[OT Security 分割設定の有効化/無効化] ウィンドウが表示されます。



b. [管理 (**OT Security** WebUI)] ボックスで、管理ポートを別のインターフェース (例: ポート 3) に移動します。



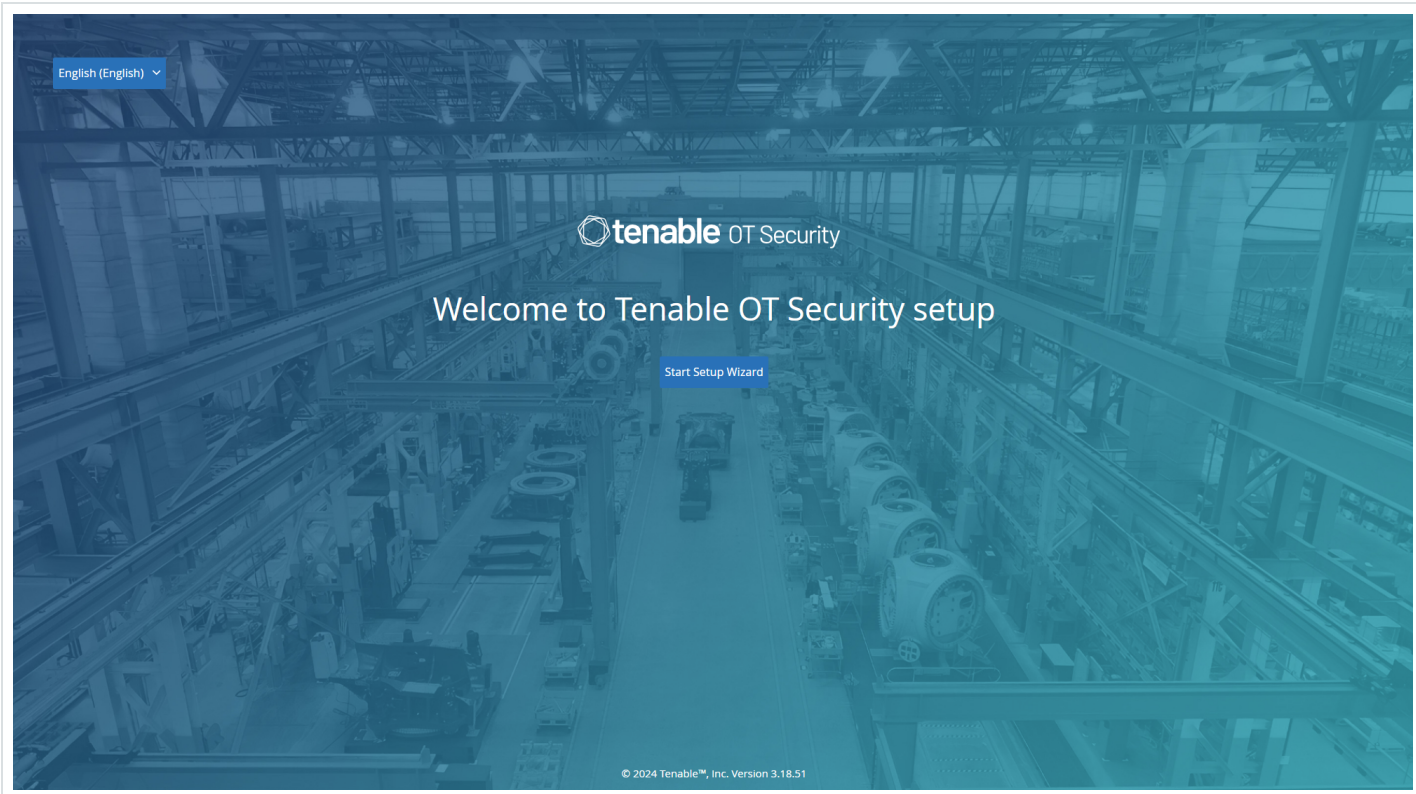
c. (任意) [アクティブクエリゲートウェイ] ボックスに、ゲートウェイ IP アドレスを入力します。

d. [ポート分割設定をアップデートして OT Security を再起動する] をクリックします。

Tenable Core により、必要に応じて再起動またはインストールが開始されます。

注意: この時に、他のアップデートをインストールしたり、再起動したりしないでください。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、[URL] ボックスのリンクをクリックして、OT Security ユーザーインターフェースにログインできます。



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. 接続して管理とアクティブクエリのポート分割を設定する

> 注意: セットアップウィザード終了後、OT Security からシステムを再起動するプロンプトが表示されます。

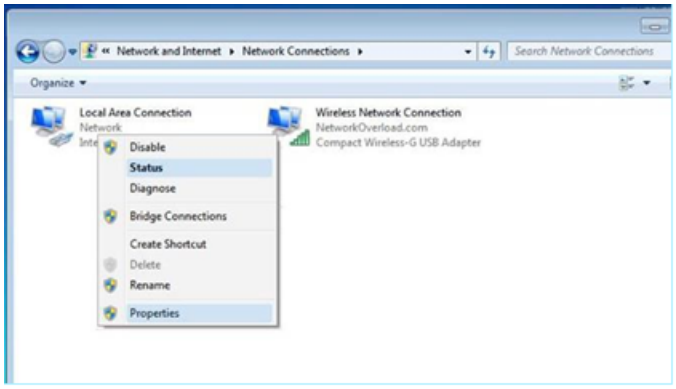
OT Security 管理コンソールへのログイン

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. 次のいずれかを行います。
   - イーサネットケーブルを使用して、管理コンソールワークステーション (デスクトップ、ノートパソコンなど) を 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。

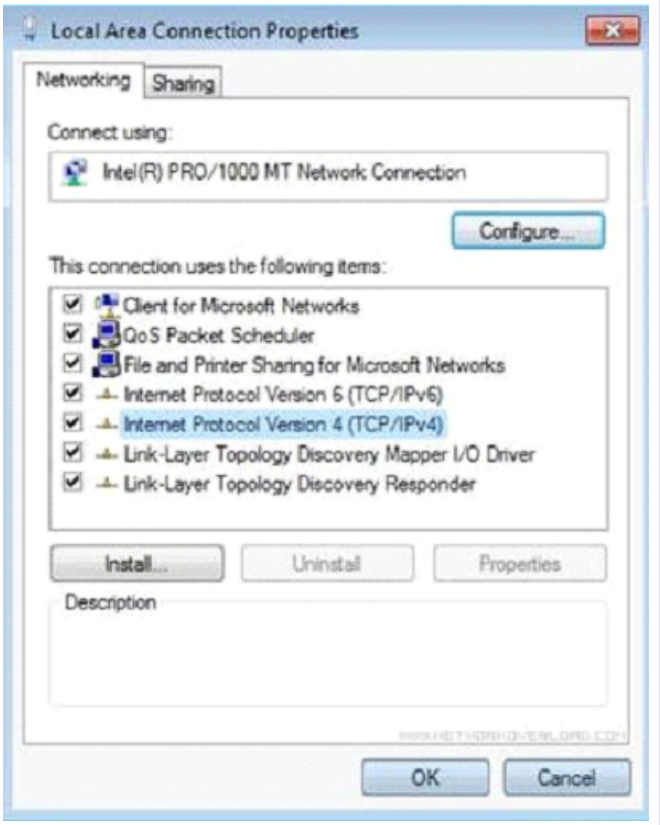
      [ネットワーク接続] 画面が表示されます。



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

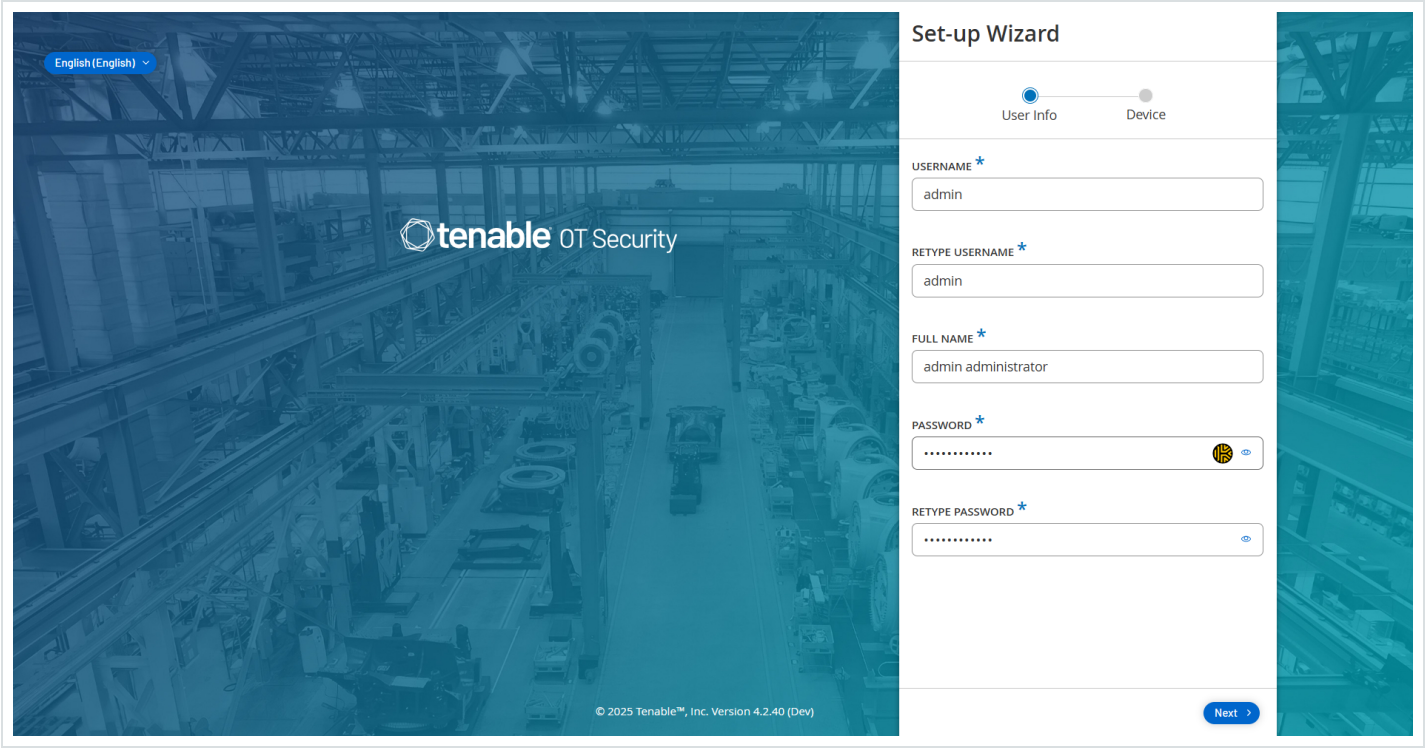
ユーザー情報

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、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。

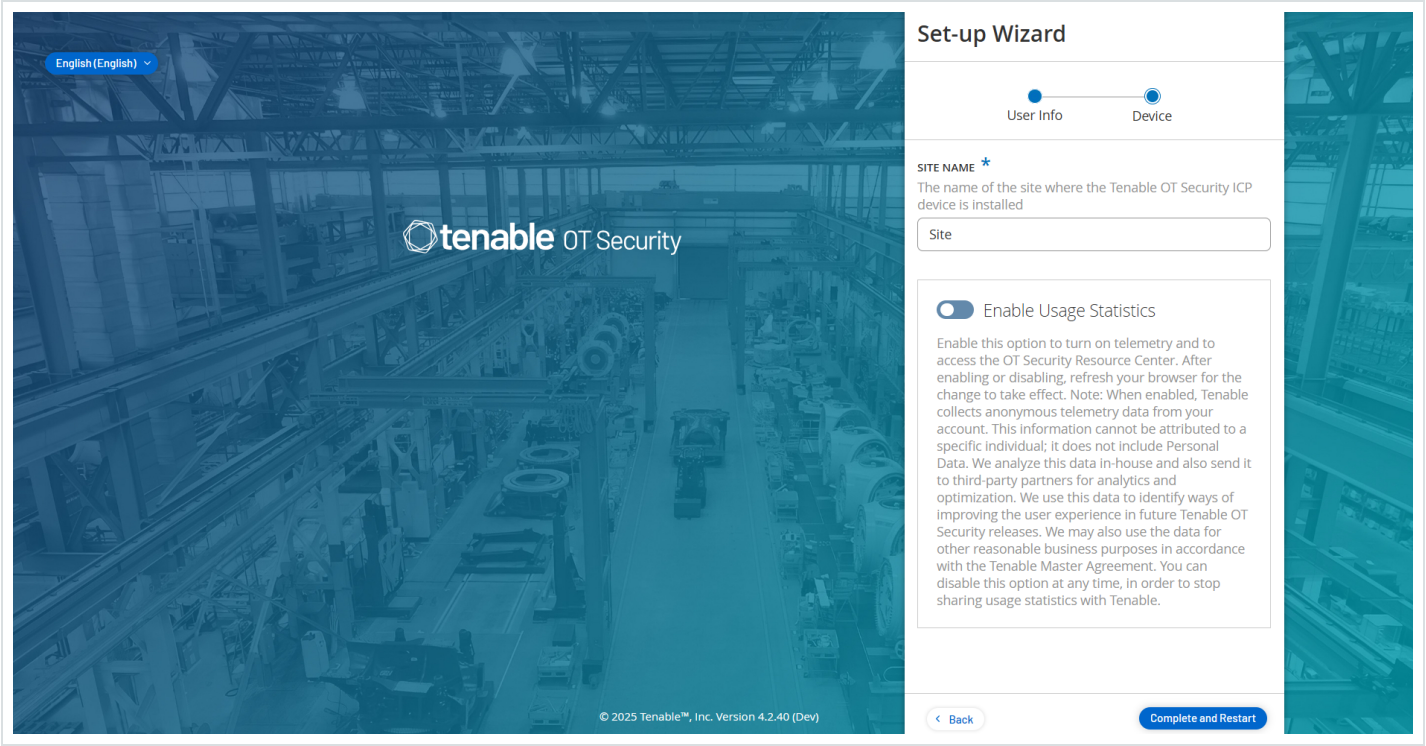
次の手順

デバイスの設定

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. [サイト名] ボックスに、OT Security をインストールしたサイトの名前を入力します。
2. (任意) [収集データの有効化] トグルをクリックして、OT Security がテレメトリデータを収集し、[リソースセンター] にアクセスできるようにします。
3. [完了して再起動] をクリックします。

   OT Security が再起動します。

次の手順

- 接続して管理とアクティブクエリのポート分割を設定する
- OT Security ライセンスのアクティベーション

接続して管理とアクティブクエリのポート分割を設定する

この手順は任意です。ポート分割のオプションを選択した(アクティブクエリインターフェースロールと管理ロールを分離するため)場合、OT Security アプライアンスのセカンダリインターフェースを適切なネットワークスイッチインターフェースに接続できます(Tenable Core でそうしていない場合)。

詳細については、管理ロールとアクティブクエリロールの分離 (ポート分割) を参照してください。

管理ポートに接続する方法

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. そのケーブルをネットワークスイッチのポートに接続します。

OT Security ライセンスのアクティベーション

必要な OT Security ユーザーロール: 管理者

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 Account Management 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すれば、資産を管理する新しいサイトを作成するための Tenable Account Management ポータルを簡単に使用できます。

Account Management ポータルの詳細については、Account Management ポータルドキュメントを参照してください。

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 Account Management ポータルにログインします。

   [アカウント] ページが表示され、表示するアクセス許可があるオプションが表示されます。

2. Tenable OT Security ライセンスをクリックします。

   Tenable OT Security [詳細] ページが表示されます。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. [アクティベーションコード] 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] 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、Account Management ポータルからコピーしたコード (アクティベーションコード) 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 Account Management 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 [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 Account Management ポータルを開きます。

[アカウント管理] ポータルページが表示されます。

> 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. 左のナビゲーションペインで、[製品] をクリックします。

[マイ製品] ページが表示されます。

7. OT Security の 20 桁のライセンスコードを使用して、使用している製品を検索します。

その特定のライセンスコードを持つ OT Security 製品が表示されます。

8. [サイト] タブをクリックします。

[サイト] タブが表示されます。

9. サイトを作成するには、[サイトの管理] > [サイトの作成]をクリックします。

   [新しいサイトの作成] 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。

      ヒント: [ラベル] フィールドを使用して、デバイスまたは ICP の名前を含めることができます。ラベルを付けることにより、さまざまなサイトを区別することができます。

   b. [サイズ] 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。

      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、[サイズ] ボックスの下にあるスライダーを使用できます。

   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。

      ダイアログボックスにアクティベーションコード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ます。

   f. [確認] をクリックします。

10. OT Security インスタンスに戻ります。

11. [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。

12. [アクティベーションコード] ボックスに、Tenable OT Security Account Management 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 8e を参照してください。

13. [アクティブ化] 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。

14. [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。

15. Tenable Account Management ポータルに戻り、1 回限り生成されるアクティベーションコードのダイアログボックスで、[アクティベーションライセンスを保存したことを確認します] チェックボックスをクリックします。

16. [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 [サイト] タブに表示されます。

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。ライセンスをアップデートする場合、既存の 20 桁のライセンスコードを使用します。

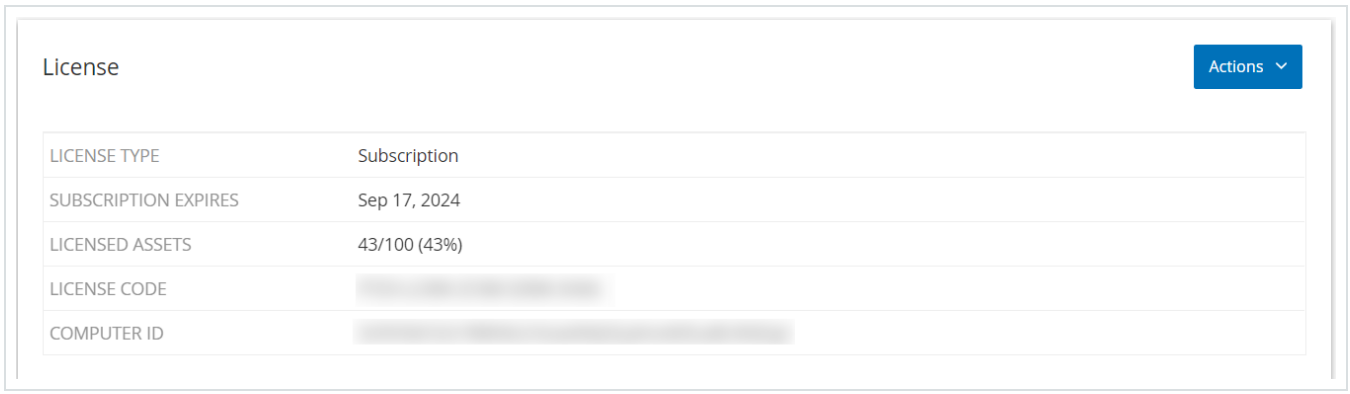
始める前に

- 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。

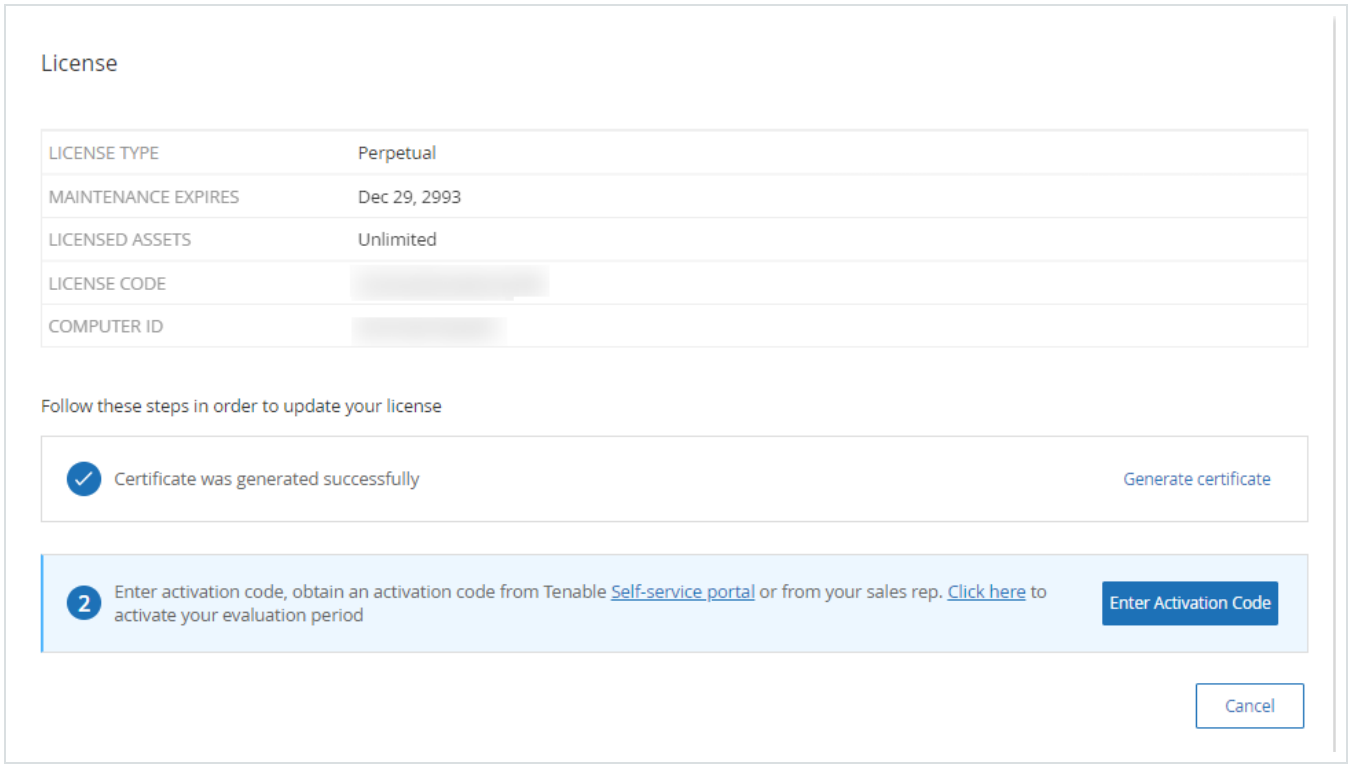
1. [設定] > [システム設定] > [ライセンス] に移動します。

   [ライセンス] ウィンドウが表示されます。



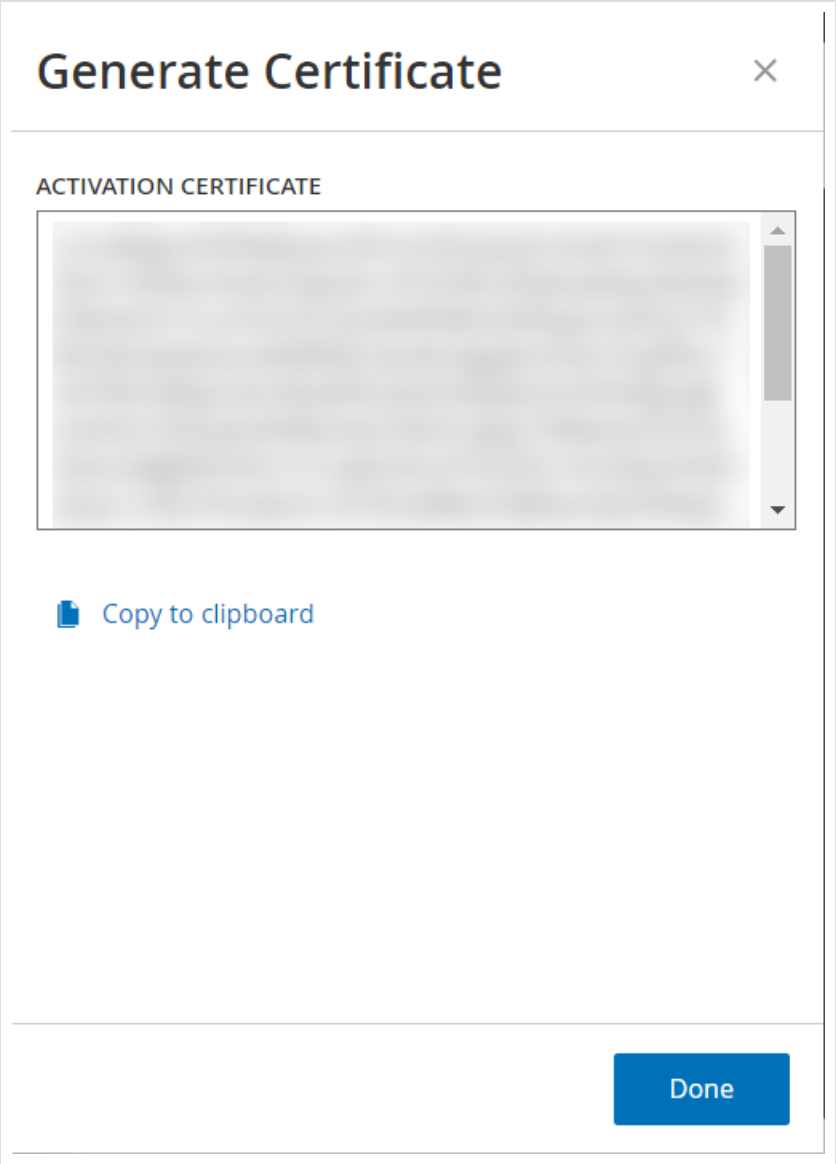
2. [アクション] メニューから [ライセンスのアップデート] を選択します。

   [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. [(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] リンクをクリックします。

   OT Security により、[Tenable アカウント管理] ポータルの [マイアカウント] ページにリダイレクトされます。

注意: 評価期間の場合は、2番目のリンクをクリックしてください。ライセンスをオフラインモードでアップデートするを参照してください。

6. Tenable Account Management ポータルでサイトの詳細を編集します。

   a. 左のナビゲーションペインで、[製品] をクリックします。

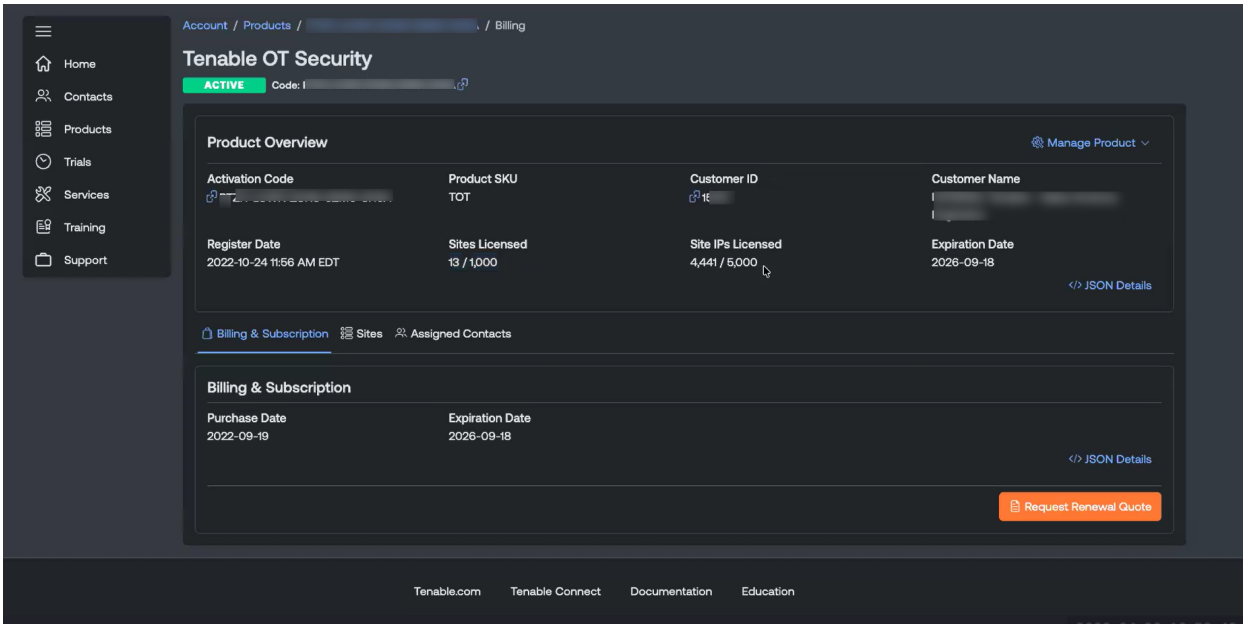
      [マイ製品] ページが表示されます。

   b. OT Security の 20 桁のライセンスコードを使用して、使用している製品を検索します。

      その特定のライセンスコードを持つ OT Security 製品が表示されます。

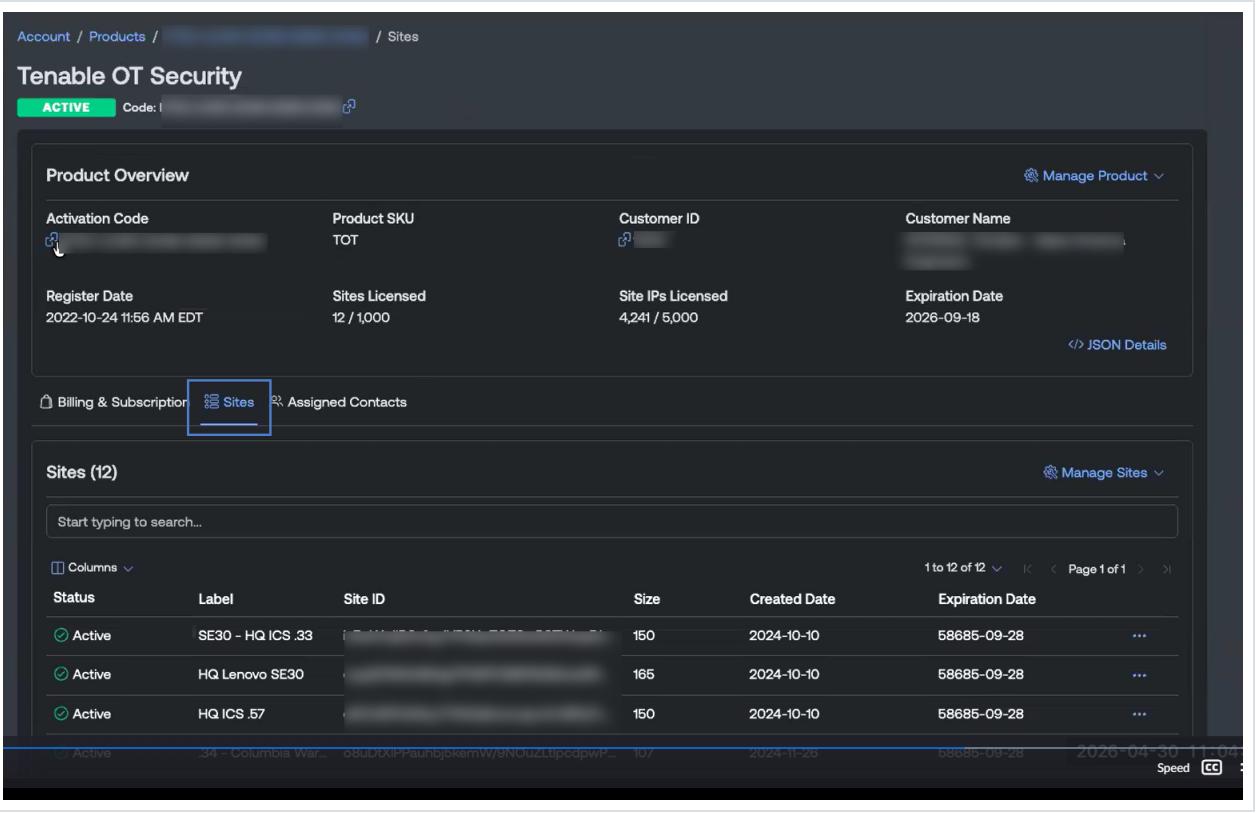
   c. ライセンスコードをクリックして、製品の詳細を表示します。

      Tenable OT Security ページに、製品の概要、請求とサブスクリプション、サイトなどの詳細情報が表示されます。



   d. [サイト] タブをクリックします。

      [サイト] セクションが表示されます。

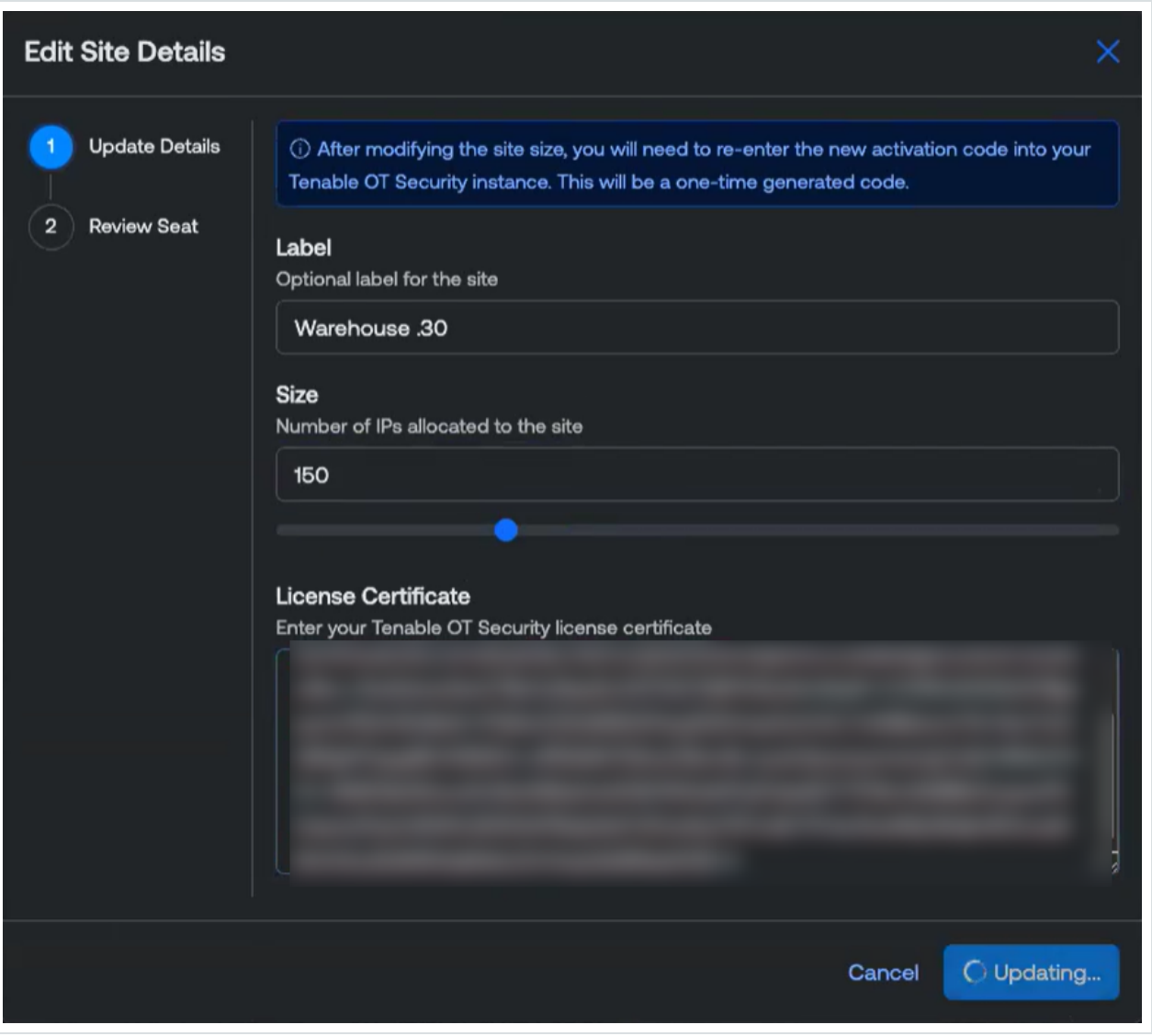


e. 編集するサイトの行にある ··· ボタンをクリックします。

メニューが表示されます。

f. [サイトの編集] をクリックします。

[サイト詳細の編集] ページが表示されます。

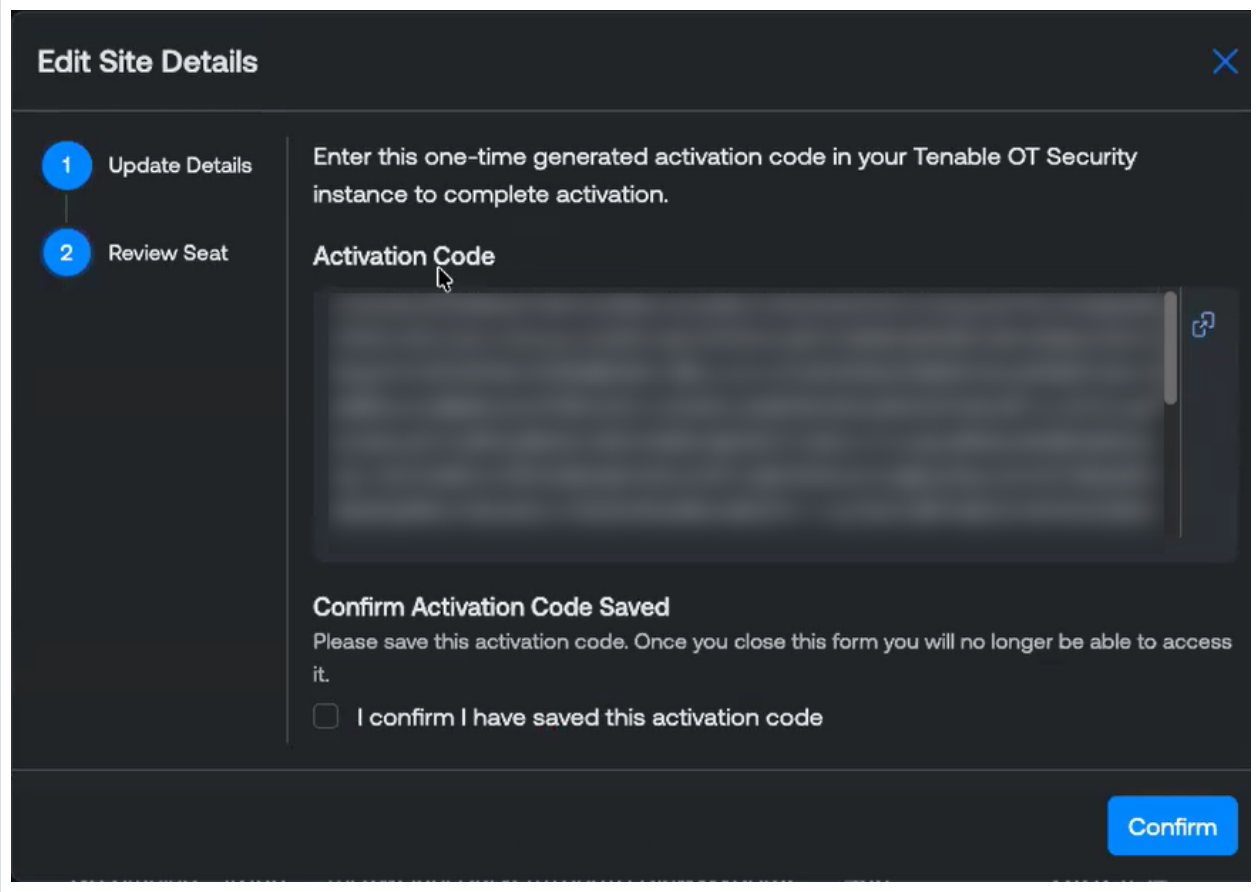


g. 必要に応じて詳細を調整します。

h. [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。

i. [アップデート] 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。

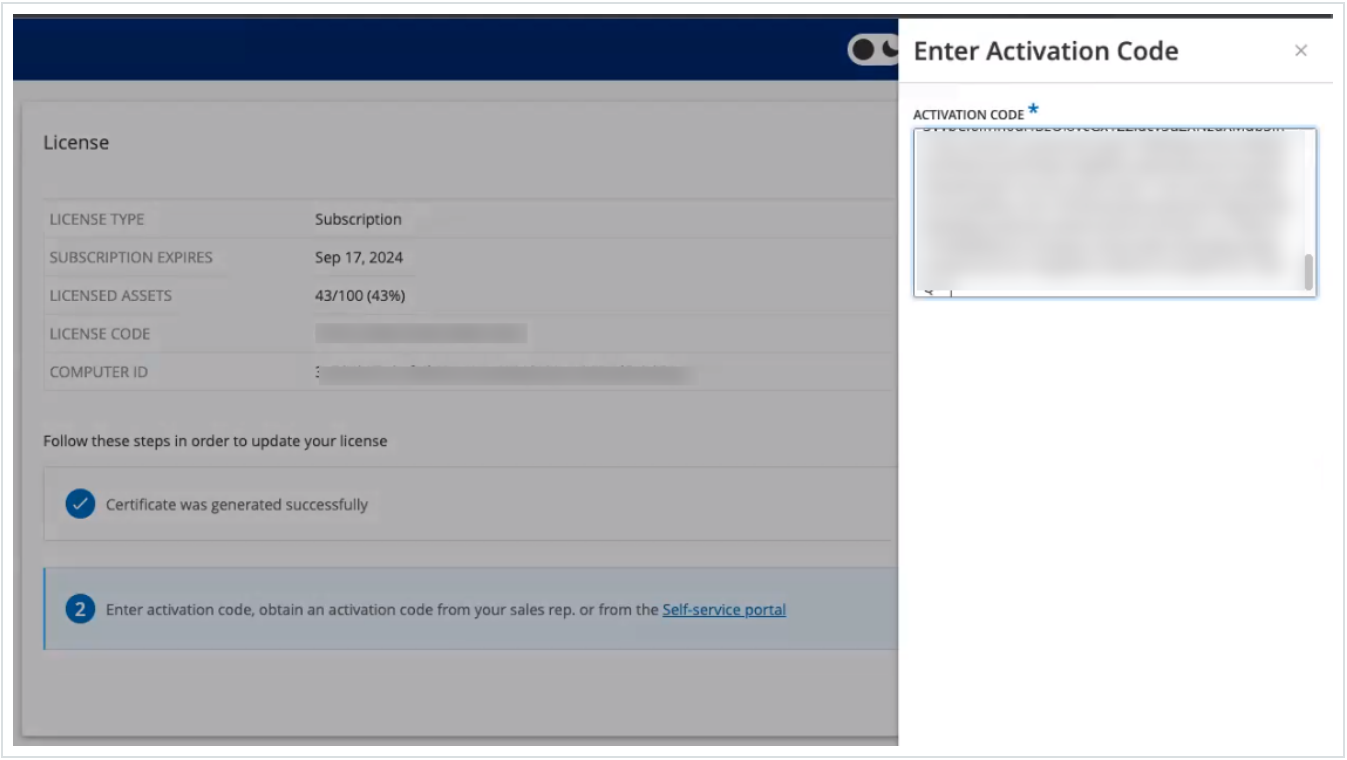


j. ボタンをクリックし、[確認] をクリックします。

7. OT Security インスタンスに戻ります。

8. [(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。

9. [アクティベーションコード] ボックスに、Tenable OT Security Account Management 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。

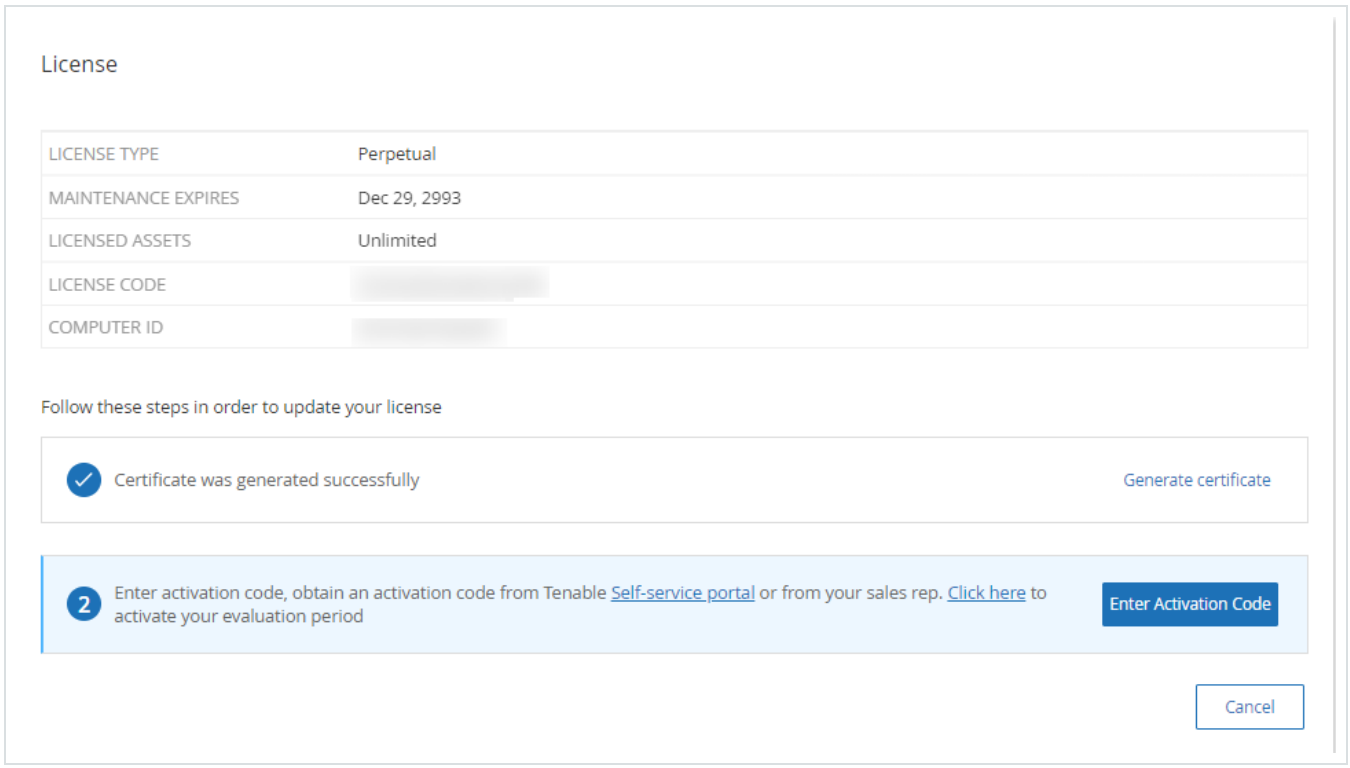


10. [アクティブ化] をクリックします。

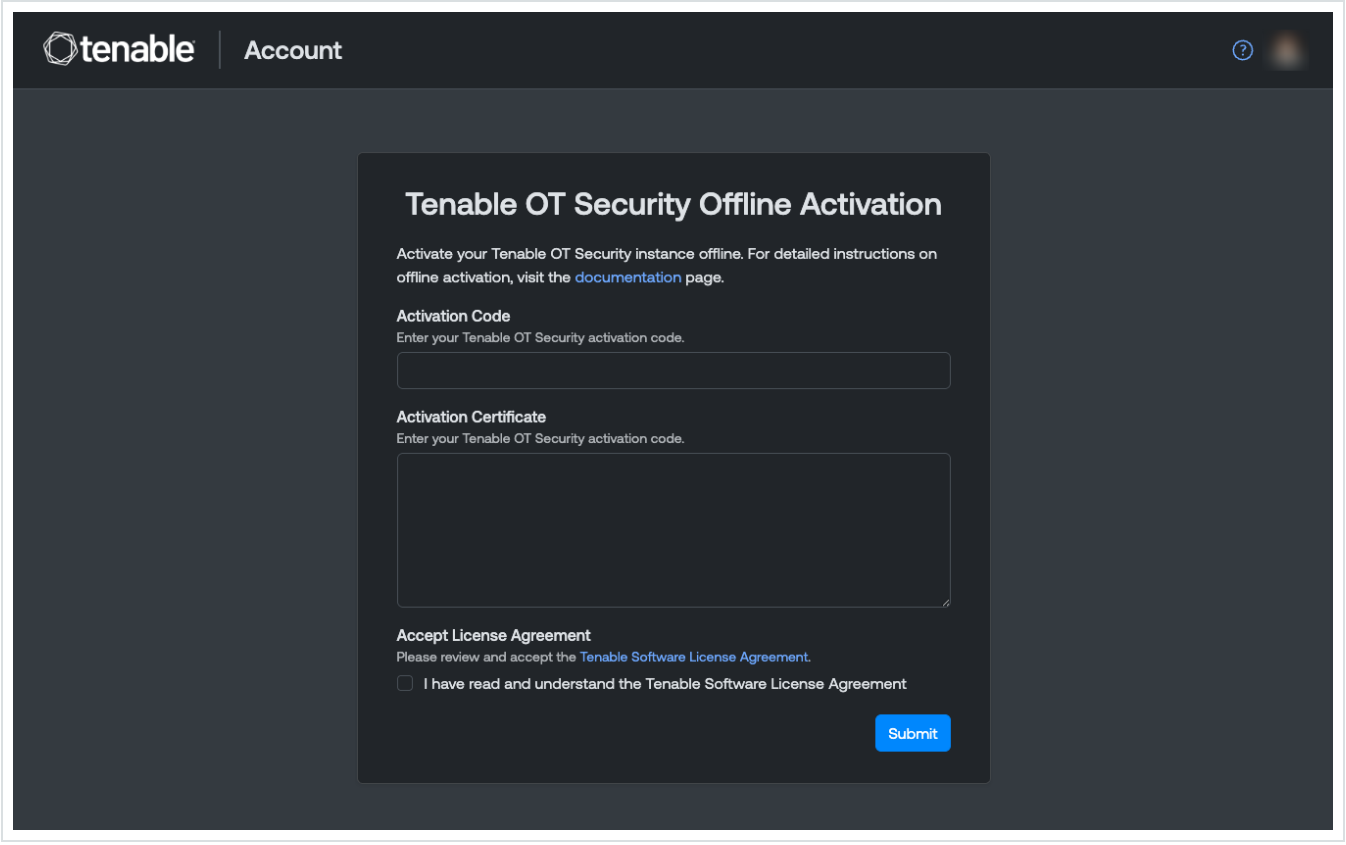
    OT Security でシステムが正常にアクティベートしたことを示すメッセージが表示され、[ライセンス] ページにアップデートされたライセンスの詳細が表示されます。

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。



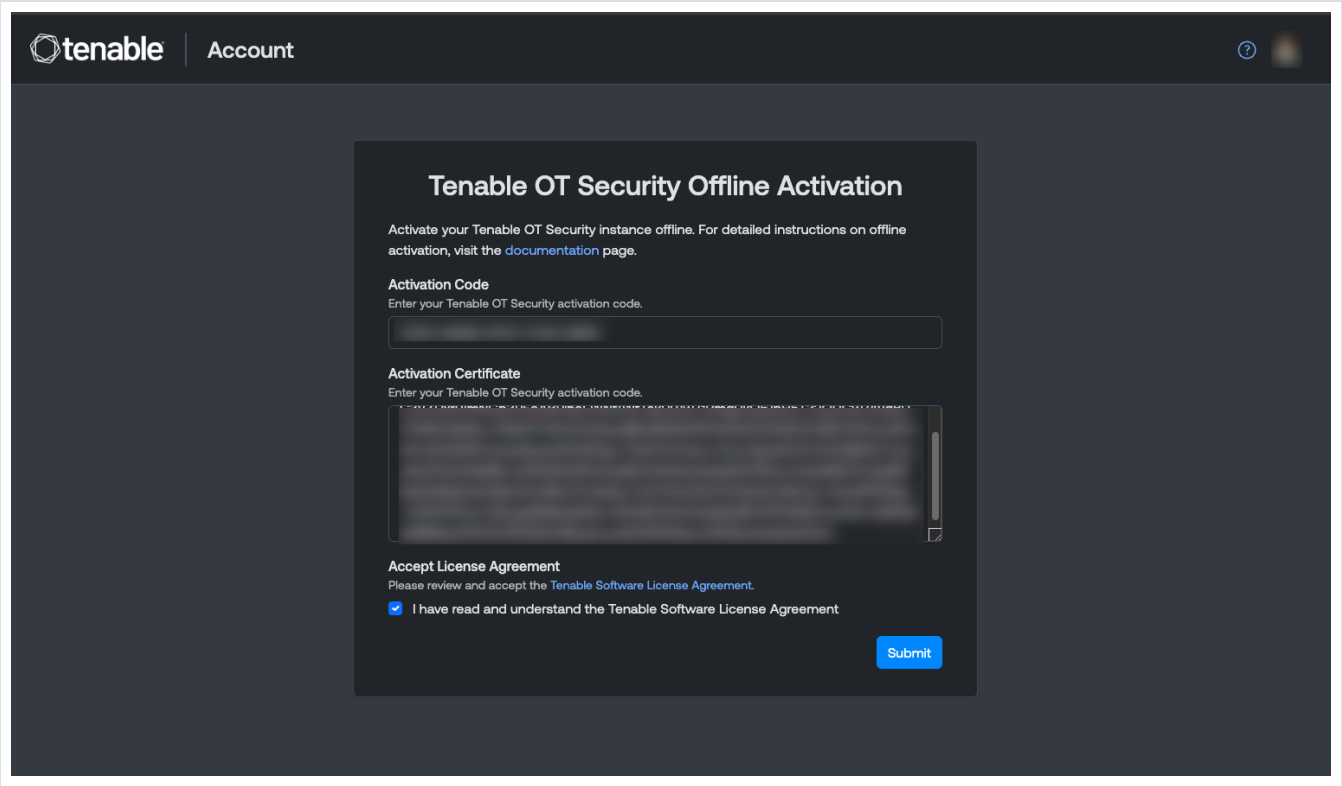
注意: URL https://account.tenable.com/offline-activation/ot-security を使用して、インターネットに接続されたデバイスから [OT Security をオフラインでアクティブ化] 画面にアクセスできます。

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] ウィンドウからコピーして貼り付けることができます)。

4. [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。

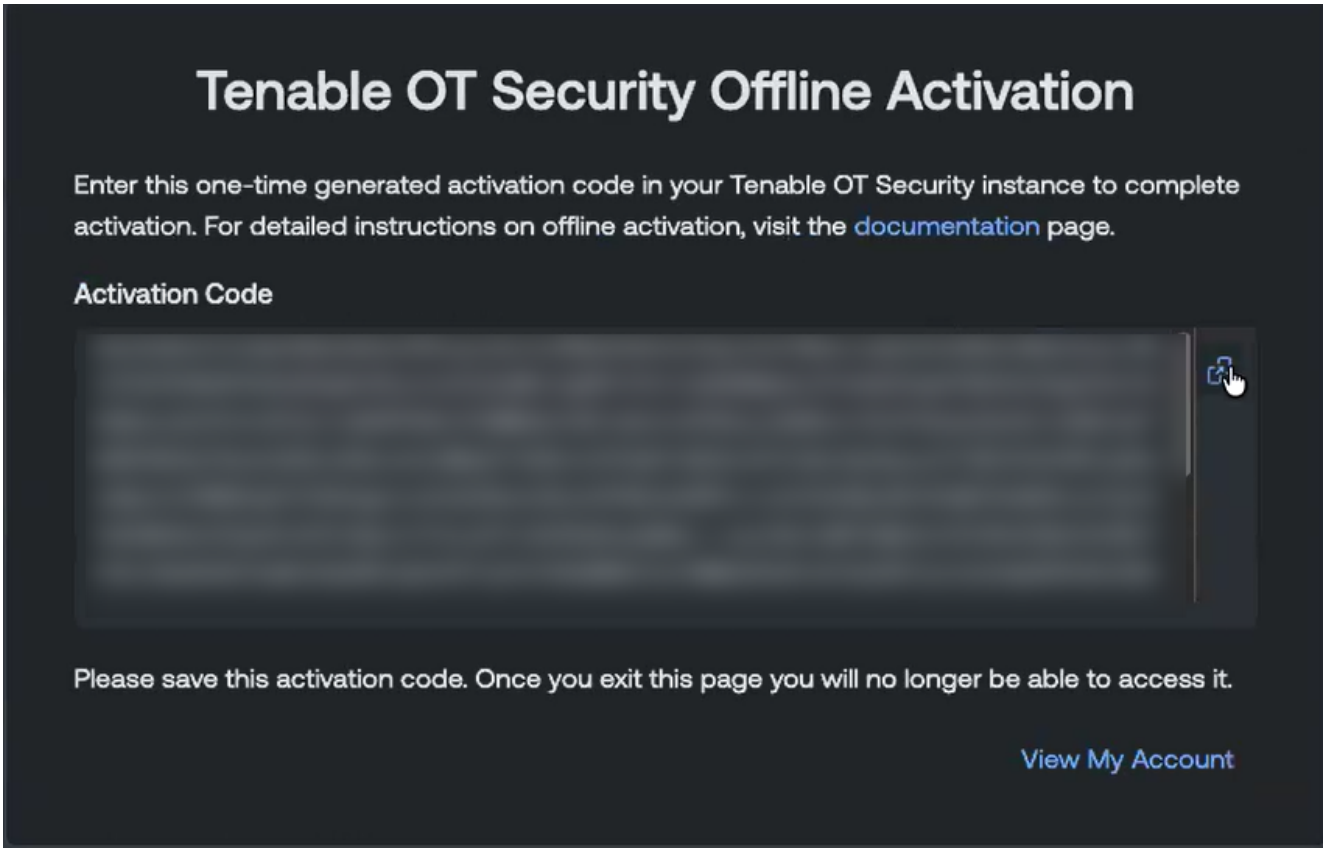
5. [Tenable ソフトウェアライセンス契約を読み、理解しました] チェックボックスをクリックします。



> 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。

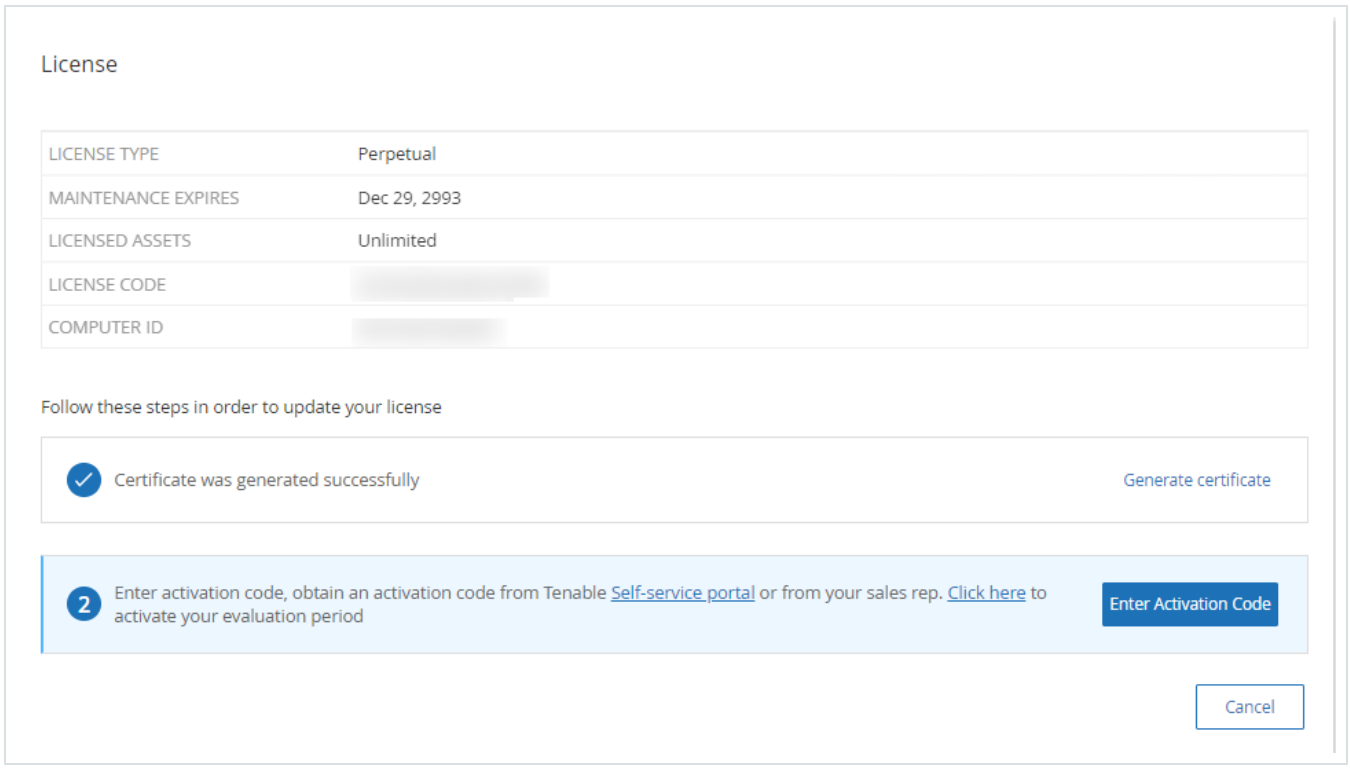
6. [送信] をクリックします。

   OT Security はアクティベーションコードを生成します。



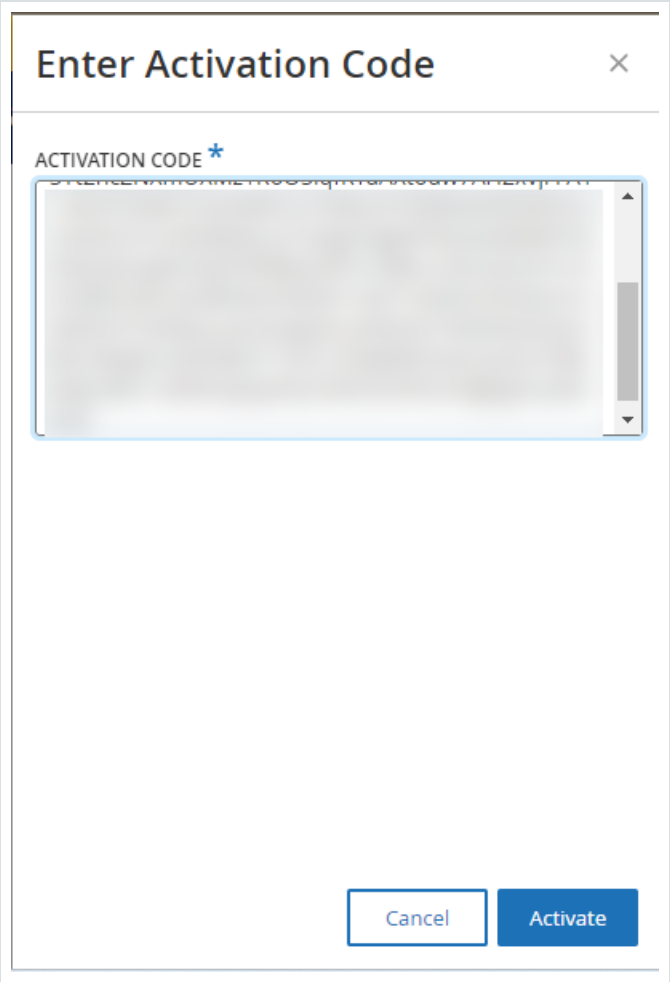
7. アクティベーションコードをコピーするには、 ボタンをクリックします。

8. OT Security の [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。

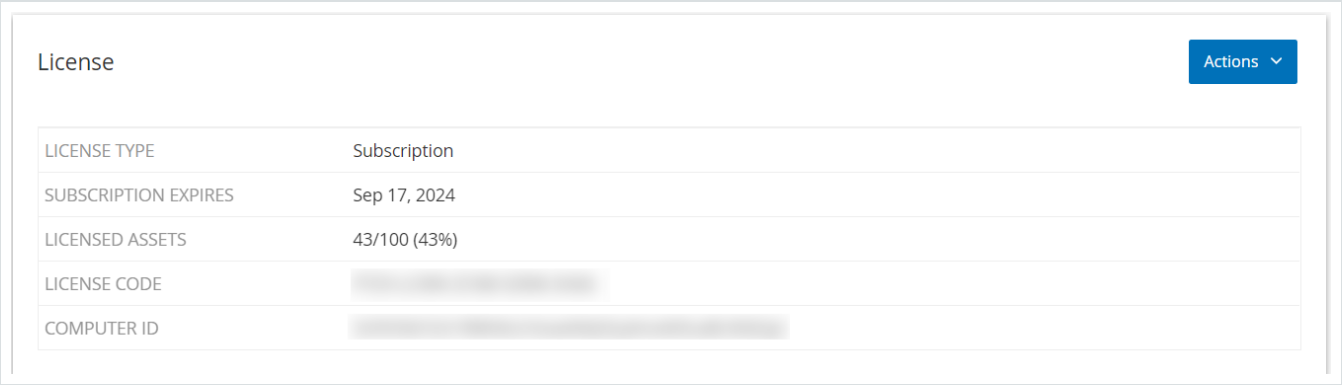
> 注意: 評価ライセンスまたは一時ライセンスには、必ず一意のライセンスコードがあります。

始める前に

- 担当の Tenable アカウントマネージャーが、システムであなたの新しいライセンスをすでに発行し、ライセンスコード (20 英数字) をあなたに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。

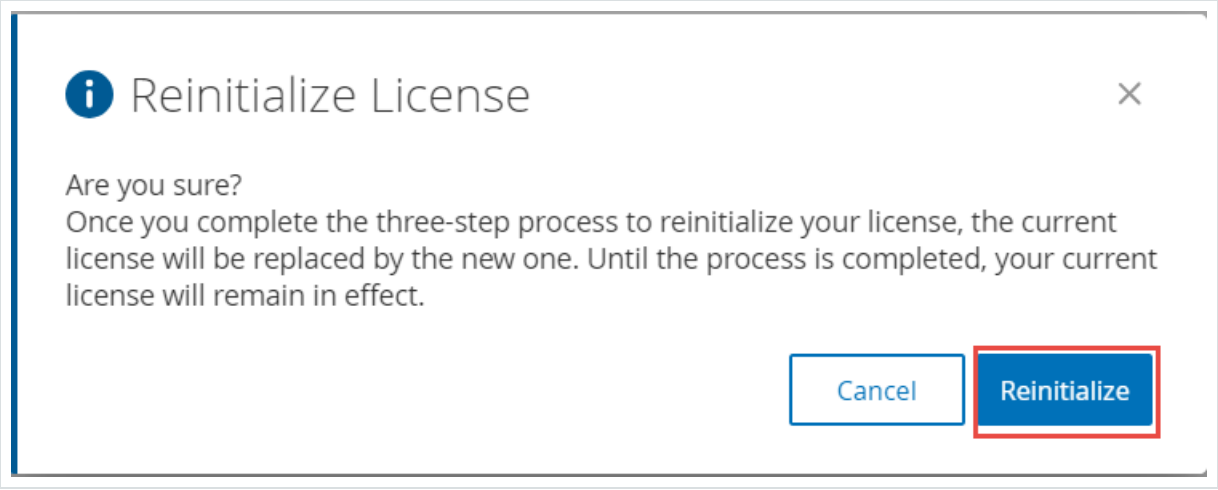
1. 設定] > [システム設定] > [ライセンス] に移動します。



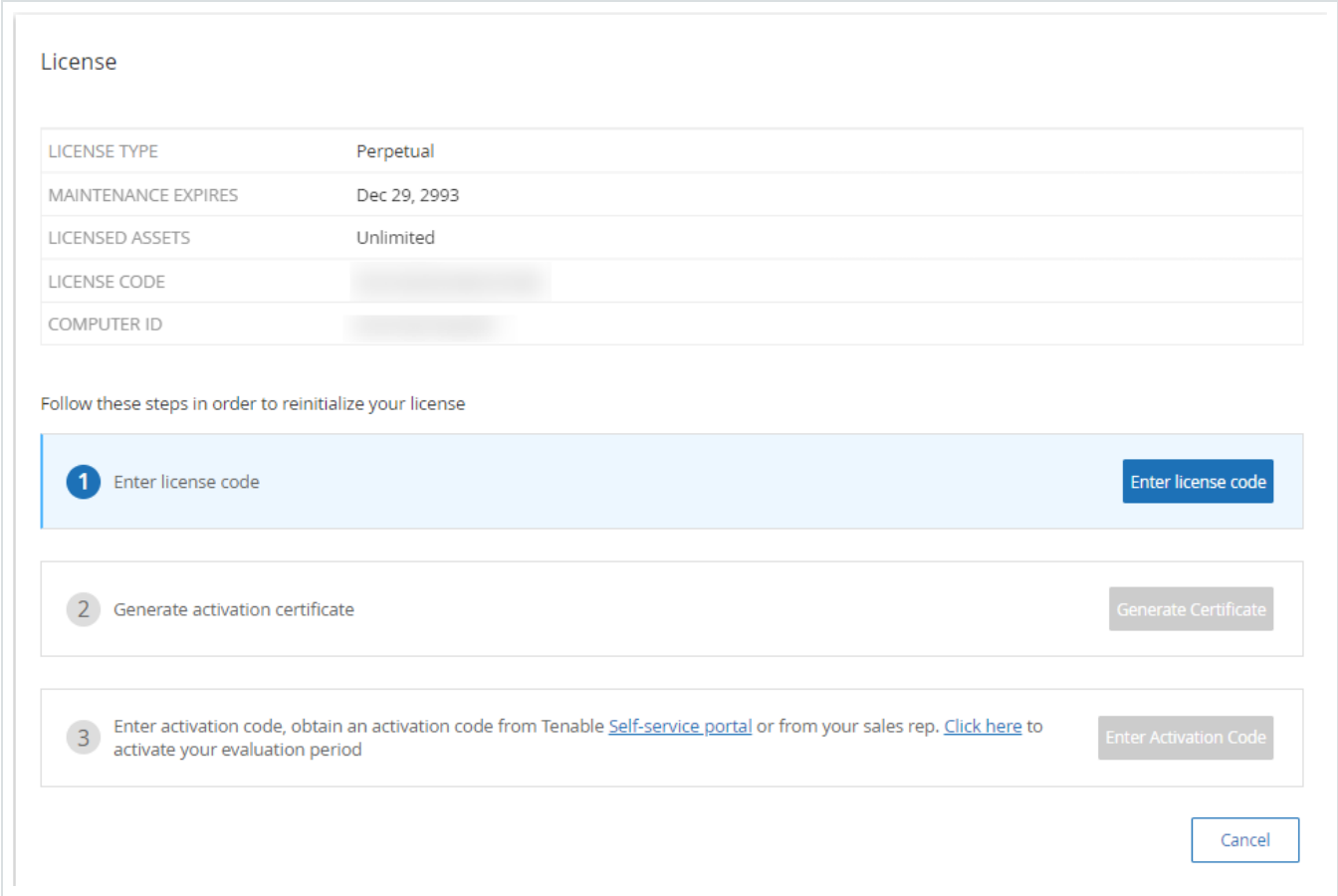
2. [アクション] メニューから [ライセンスの再初期化] を選択します。

   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. [ライセンスのアクティベーション] セクションで、システム起動手順 (ステップ 1 ~ 17) に従って、ライセンスをアクティブ化します。

   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

> 必要な OT Security ユーザーロール: 管理者

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。

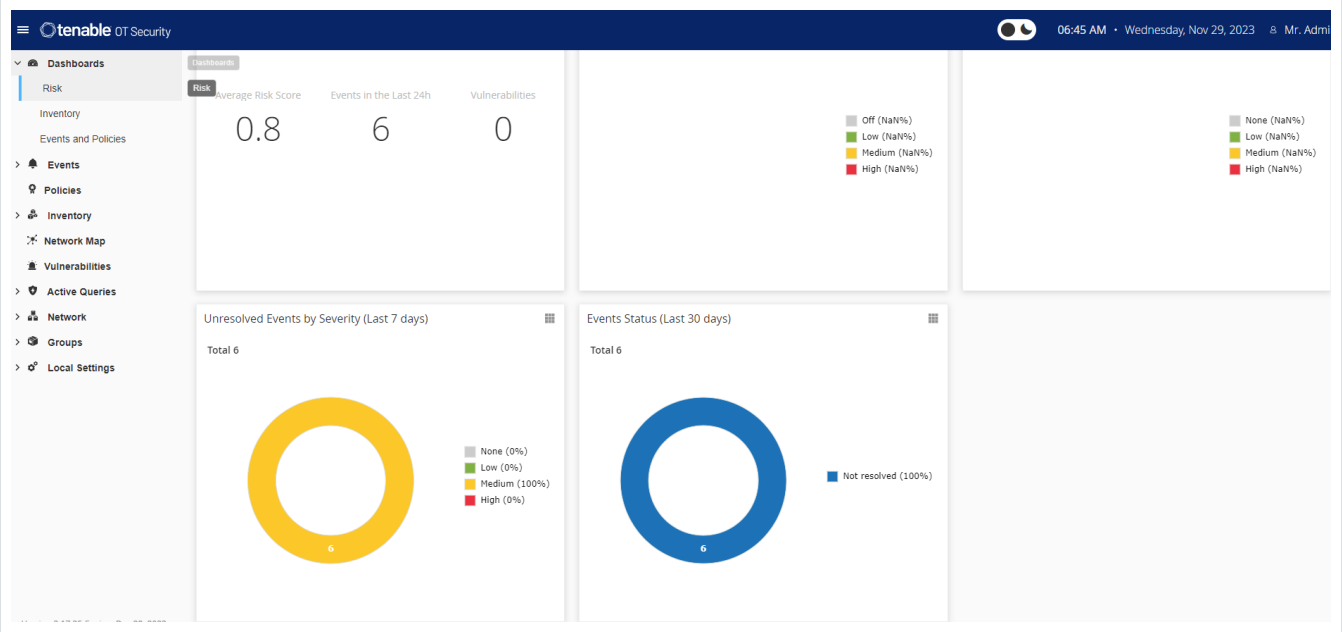
管理コンソール(ユーザーインターフェース)の設定]ウィンドウで、アクティブクエリなど、追加の機能を設定してアクティブ化することができます。詳細については、アクティブクエリを参照してください。

> 重要:バージョン4.4以降では、アラートの過負荷を減らすためにOT Securityを有効にすると、パッシブモニタリングはデフォルトで無効になります。パッシブモニタリングを有効にするには、[設定]>[ネットワーク定義]ページに移動し、[パッシブモニタリング]トグルをクリックして有効にします。ヘッダーのパッシブモニタリング アイコンは、パッシブモニタリングが有効か無効かを示します。

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かもしれません。

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。環境設定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 (センサーのセットアップを参照)。
- 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)。

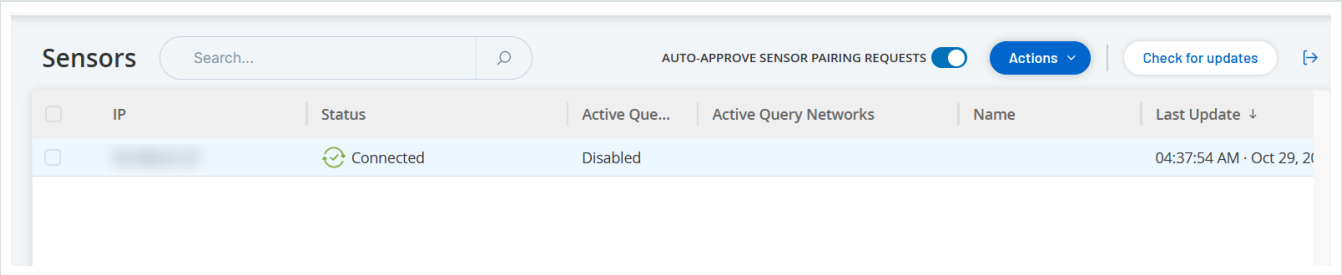
注意: 接続の切断を回避するために、Tenable ではセンサーのペアリングプロセスに対して管理者ロールを持つ専用 ICP ユーザーを作成することを推奨しています (ローカルユーザーの追加を参照)。新しい管理者ユーザーを追加して、複数のセンサーをペアリングできます。

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、設定] > [センサー] ウィンドウに移動します。

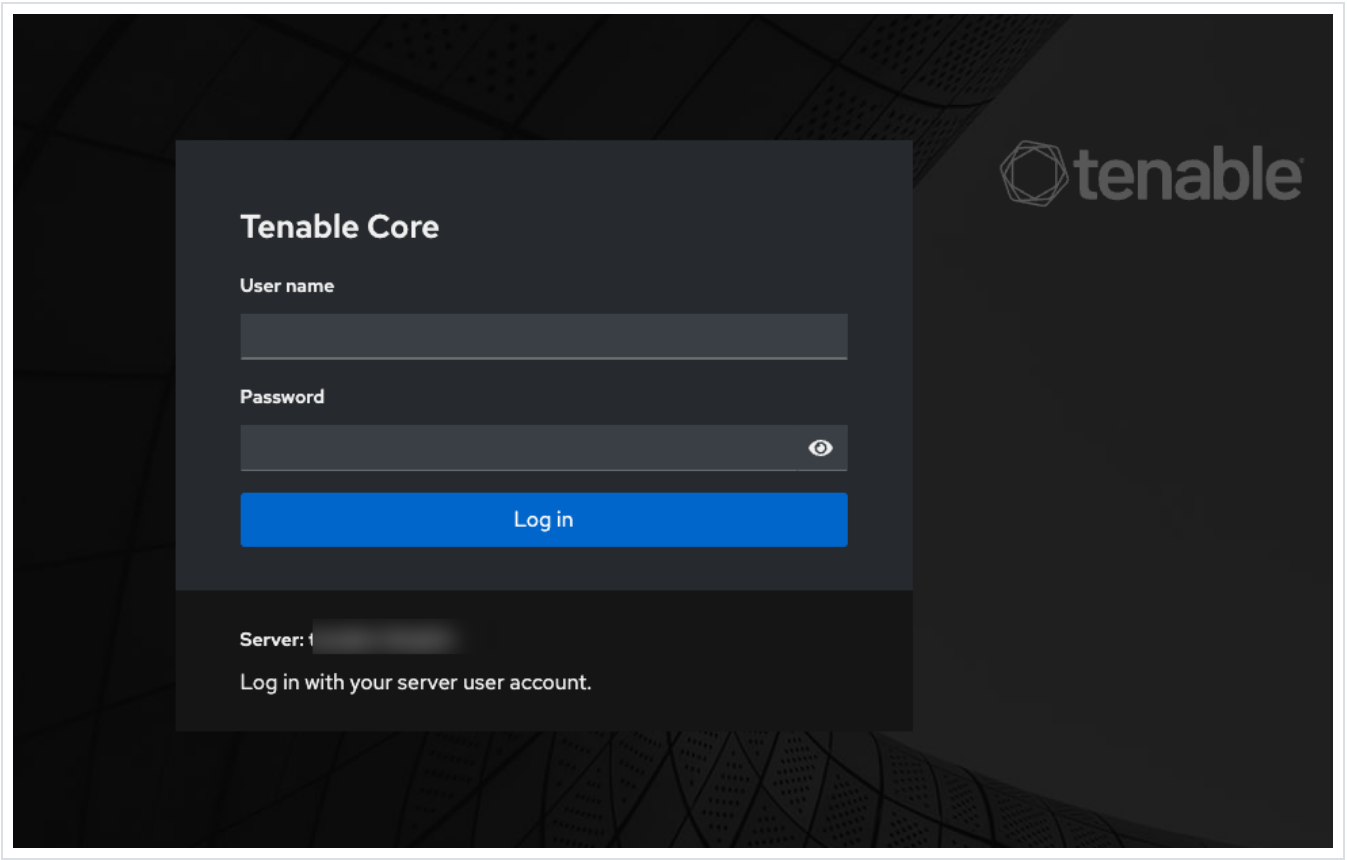


2. センサーペアリングの自動承認を有効にするには、ページ上部にある [受信センサーのペアリングリクエストを自動承認する] スイッチを [オン] に切り替えます。オンになっていない場合は、すべてのペアリングリクエストを手動で承認しなければなりません。

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。

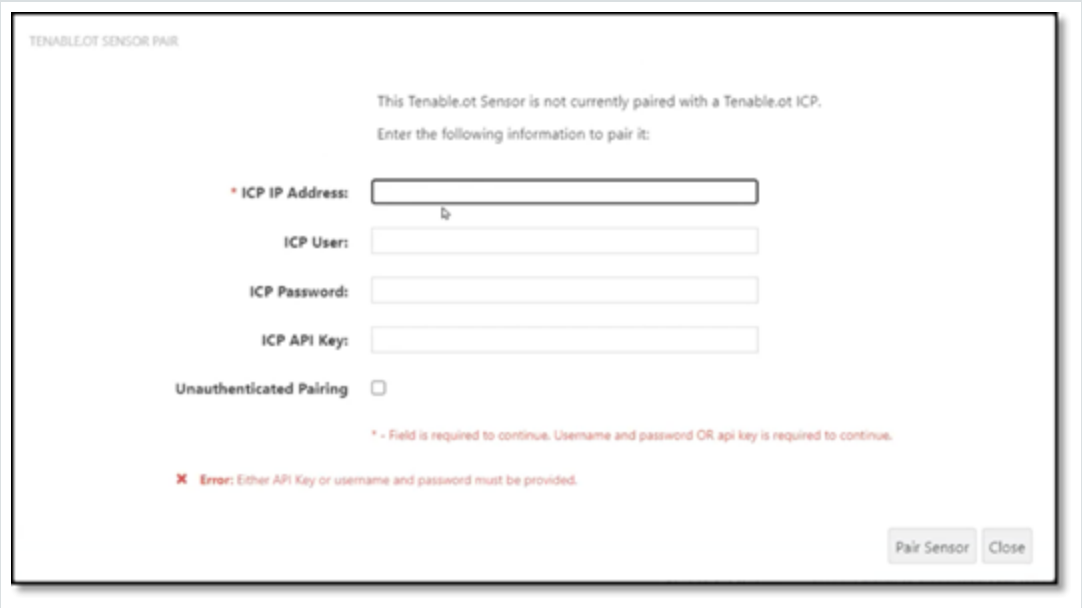
4. Tenable Core コンソールのログインウィンドウで、ユーザー名とパスワードを入力し、[特権タスクでパスワードを再利用する] チェックボックスを選択して、[ログイン] をクリックします。



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。

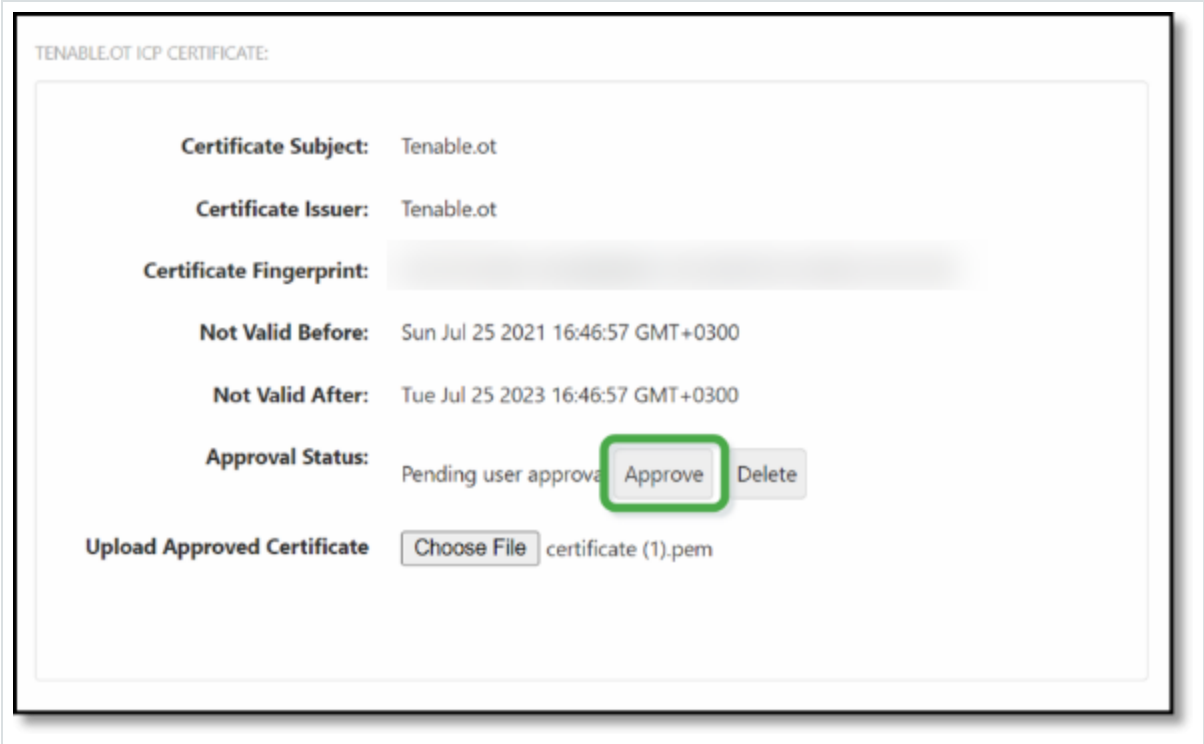
> 注意: ペアリングプロセス中の接続を確保するために、Tenable ではセンサーのペアリングに対して専用 ICP ユーザーを作成することを推奨しています (ローカルユーザーの追加を参照)。

> 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。

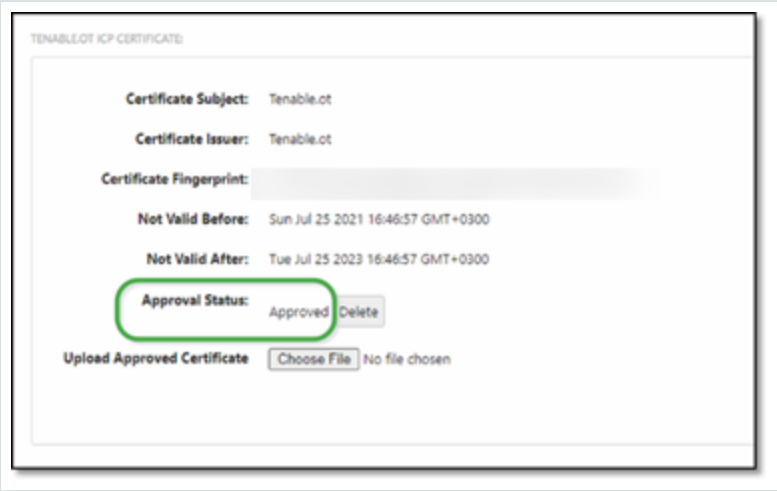
    証明書を手動でアップロードする場合

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。

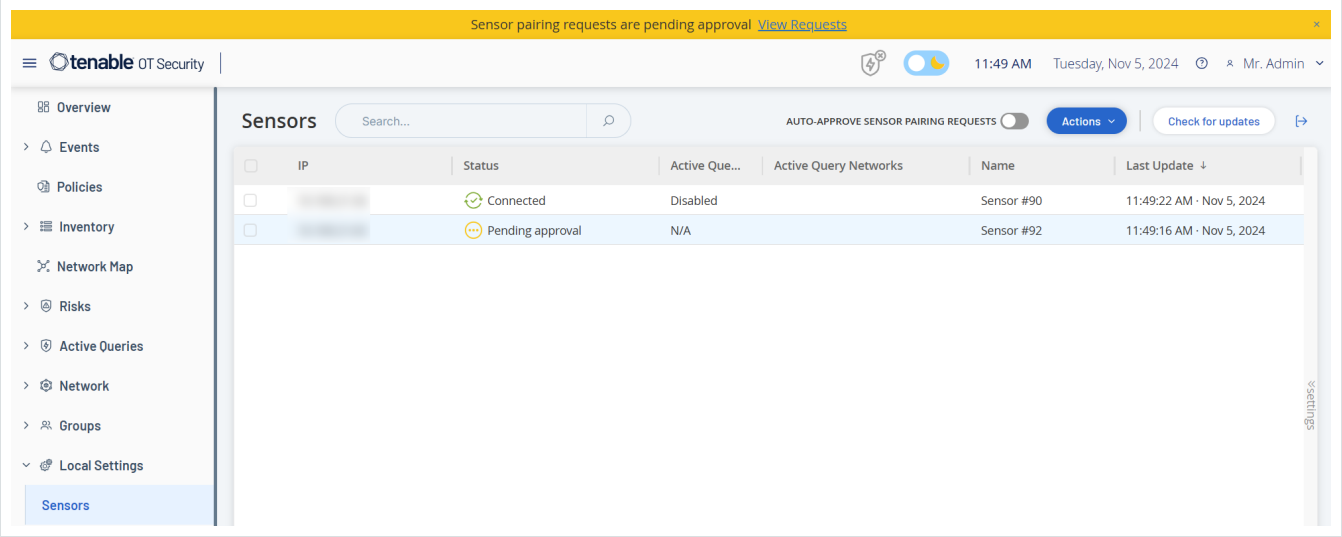
c. アップロードする `.pem` 証明書ファイルに移動します。

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。

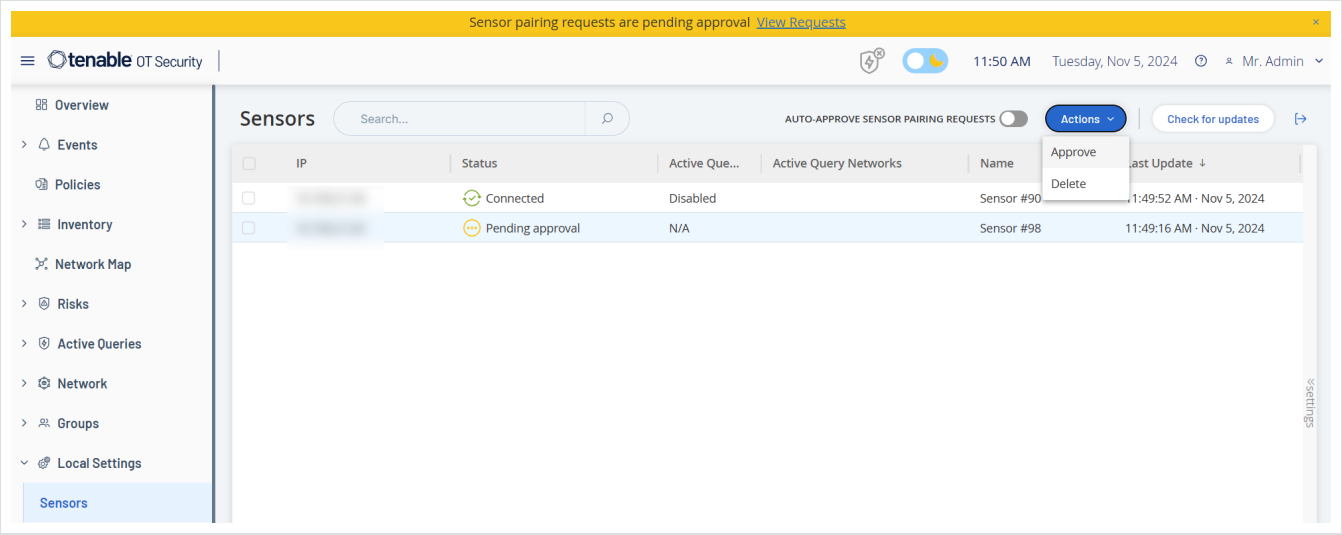


11. ICP ユーザーインターフェースで、[ローカル設定] > [センサー] に移動します。

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に関する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。

センサーのセットアップ

設定可能なモデルセンサーは、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)。

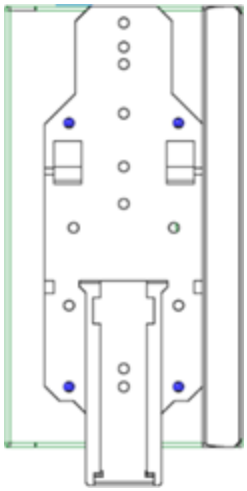
設定可能なセンサーのセットアップ

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

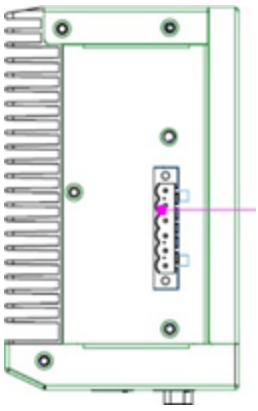
OT Security 設定可能なセンサーの標準 DIN レールへの取り付け手順

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。

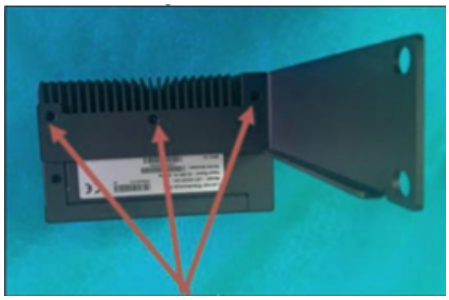
次に、AC 電源ケーブル(付属)を電源ユニットに挿入し、もう一方の端を AC コンセントに差し込みます。

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。

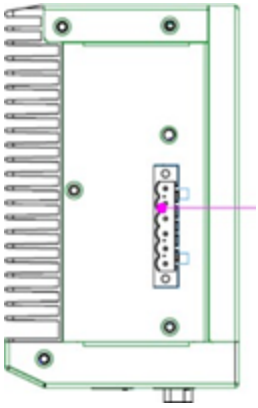
注意:

- 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、ネットワークモニタリング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 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. 次のいずれかを行います。

   - イーサネットケーブルを使用して、管理コンソールワークステーション (デスクトップ、ノートパソコンなど) を 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。

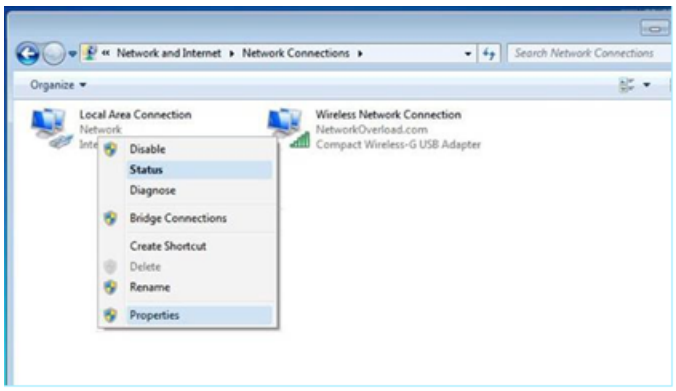
2. 管理コンソールワークステーションが、OT Security センサーと同じサブネット (192.168.1.5) の一部であるか、ユニットにルーティング可能であることを確認します。

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。

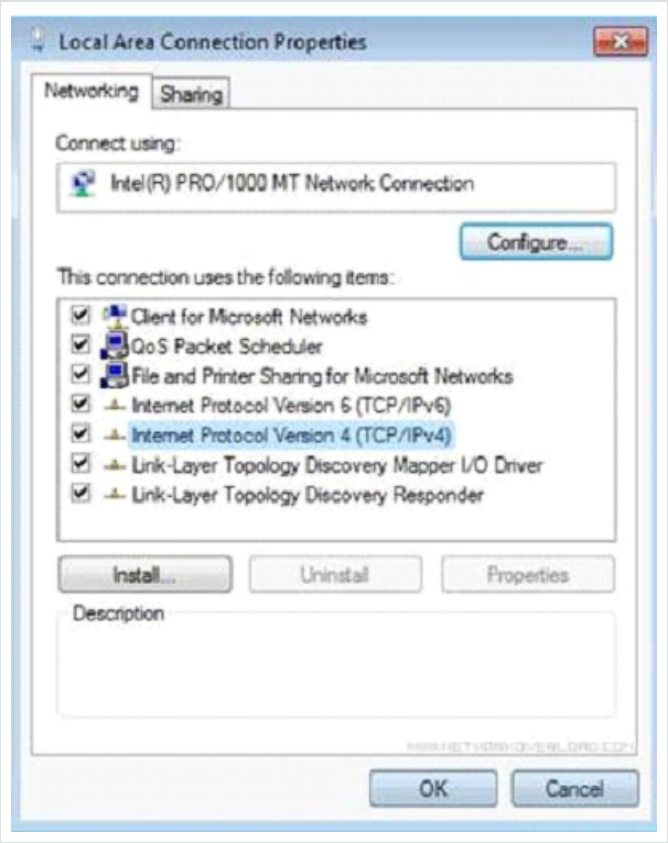
      > 注意: Windows のバージョンによって、ナビゲーションが若干異なる場合があります。

      [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。

コンソール接続の確立と初期セットアップ

このトピックでは、ローカルシリアルコンソールを OT Securityアプライアンス (ICP およびセンサー) に接続する方法について説明します。この接続方法は、初期 IP 設定、ネットワークのトラブルシューティング、または管理 IP にアクセスできない場合の復旧に使用します。

始める前に

以下のソフトウェアおよびハードウェアを準備してください。

ソフトウェア

- ターミナルエミュレーター: PuTTY、Tera Term、Serial、Minicom などのユーティリティ。
- ドライバー: 特定の USB ケーブルやアダプター用のドライバー (FTDI や PL2303 など) がインストールされていることを確認します。

ハードウェアとケーブル接続オプション

適切なケーブル接続方法を選択するため、使用しているアプライアンスのタイプを確認してください。

- **Tenable OT Security** または **Tenable** ICP (Industrial Core Platform) コンソール
  - ポートタイプ: RJ-45 コンソール
  - 推奨ケーブル: USB-RJ45 コンソールケーブル

> 注意: 通常、アプライアンスの梱包には水色の Cisco スタイルのコンソールケーブルが入っています。これは標準的なケーブル (約 10 ドル) で、ネットワークスイッチで一般的に使用されています。

- **Tenable センサー:** センサーには 2 つのハードウェアバリエーションがあります。使用するデバイスの物理ポートを確認してください。
  - RJ-45 コンソールポート: USB-RJ45 コンソールケーブルを使用します。
  - DB9 (シリアル) ポート: USB-DB9 シリアルケーブルを使用します。

> ヒント: Tenable では、接続の問題を最小限に抑えるために複数部品のアダプターではなく、USB-DB9 メスコネクタの直結ケーブル (単一構成) の使用を推奨しています。

代替方法 (レガシーアダプター)

USB-コンソールケーブルの代わりに標準的なシリアル-USBアダプターを使用する場合は、回線内にヌルモデムアダプターまたはカプラーを使用する必要があります。

> ヒント: 接続失敗は多くの場合、標準のシリアルアダプターがヌルモデムなしでは送信ピンや受信ピンを正しくクロス接続できないために発生します。

物理接続

1. ケーブルの USB 側をワークステーションに接続します。
2. もう一方の端 (RJ-45 または DB9) をアプライアンスに接続します。
    - ラベル付きポート: [コンソール] ラベル、またはモニターや IOIOI のような記号が付いたポートを見つけます。
    - ラベルのないポート: ポートにラベルがない場合は、USB ポートの左側にある単一の RJ-45 ポートに接続します。
3. ケーブルが確実に差し込まれていることを確認してください。

COM ポートの識別 (Windows)

Windows によってケーブルに割り当てられた通信ポート (COM) を識別する必要があります。

1. Windows マシンでスタートを右クリックし、[デバイス マネージャー] を選択します。

    [デバイス マネージャー] ウィンドウが表示されます。
2. [ポート (COM と LPT)] を展開します。
3. デバイス (例: USB シリアルポート) を見つけて、番号 (例: COM3) を書き留めます。

ターミナルの設定 (PuTTY)

ターミナルエミュレーター (PuTTY など) を起動し、次の Tenable TTY 設定でセッションを設定します。

PuTTY で、[接続] > [シリアル] に移動し、次の設定を行います。

設定	値
接続タイプ	シリアル
シリアルライン:	使用している COM ポート (例: COM3)
速度 (ボー)	115200
データビット	8
ストップビット	1
パリティ	なし
フロー制御	なし 注意: フロー制御が XON/XOFF に設定されていないことを確認してください。

ヒント: [セッション] ページでこれらの設定を「Tenable OT コンソール」として保存しておくと、後で使用できます。

接続の確立

1. [開く] をクリックして、セッションを開始します。
2. ターミナルウィンドウが表示されたら Enter を 2 回押して、コンソールを起動します。

3. 以下のプロンプトが表示されることを確認します。

```
################################################################################

  This system is restricted to authorized users only. Individuals attempting
  unauthorized access will be prosecuted. Continued access indicates
  your acceptance of this notice.

################################################################################
```

4. プロンプトでログインします。

初期ネットワーク設定

管理インターフェースには静的 IP が必要です。DHCP はサポートされていません。

1. ネットワークマネージャーツールを実行します。

```
sudo nmtui
```

2. [接続の編集] を選択します。

3. 管理インターフェース (通常は、nic0 や eth0 など最初のインターフェース) を選択します。

> 警告: 2 番目のインターフェース (多くの場合 nic1) を設定しないでください。これはパッシブモニタリング用の SPAN またはミラーポートであり、IP アドレスは必要ありません。

4. IPv4 設定を <Manual> に設定します。

5. <Show> を選択し、以下を入力します。

   - アドレス: 静的 IP または CIDR (例: 192.168.1.50/24)
   - ゲートウェイ: ゲートウェイ IP アドレス。
   - DNS サーバー: DNS IP アドレス

6. 下部に移動し、<OK> を選択して保存します。

7. [終了] を選択します。

ユーザーインターフェースへのアクセス

IP を設定した後、次の操作を行います。

1. 管理ポートからネットワークスイッチにネットワークケーブルを接続します。

2. ブラウザを開き、ポート 8000 を指定して https://<YOUR_STATIC_IP> :8000 にアクセスします。

   OT Security のログインページが表示されます。これで [セットアップ] ウィザードに進むことができます。セットアップウィザードを使用した OT Security の設定を参照してください。

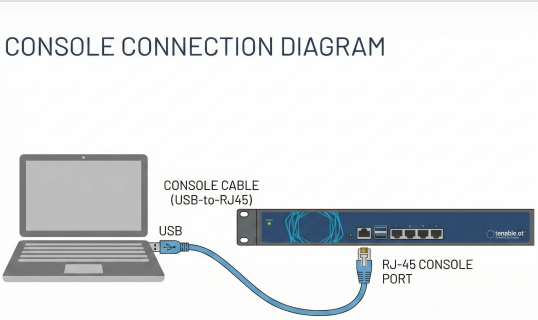
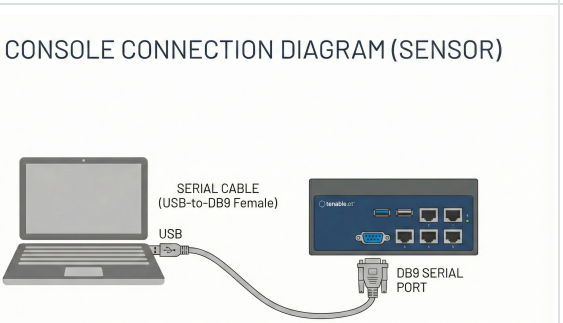
関連項目

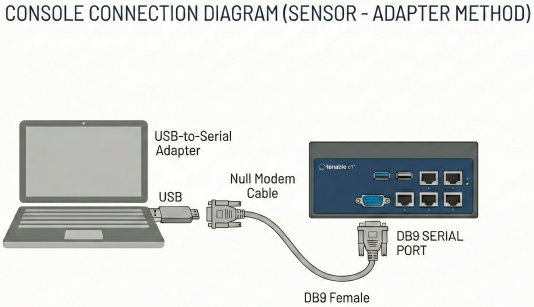
OT Security センサーに接続するコンソールケーブル

OT Security センサーに接続するコンソールケーブル

以下のケーブルを使用して、ラップトップを OT Security センサーに接続できます。

ケーブル	画像	コンソール接続図

コンソールケーブル (USB-RJ45)		
シリアルケーブル (USB-DB9 メス)		

ヌルモデムケーブル		

CLI を使用して行うバックアップの復元

CLI または Tenable Core インターフェースを使用して、OT Security を復元できます。Tenable Core ユーザーインターフェースを使ったバックアップの復元のについて詳しくは、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。CLI を使用して復元するには、次の手順を実行します。

> 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。

> 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、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。
> 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 /home/admin/my-tc-ot-backup.tar)
```

各部の説明

- `/home/admin/my-tc-ot-backup.tar` は、実際のバックアップファイルの場所です。

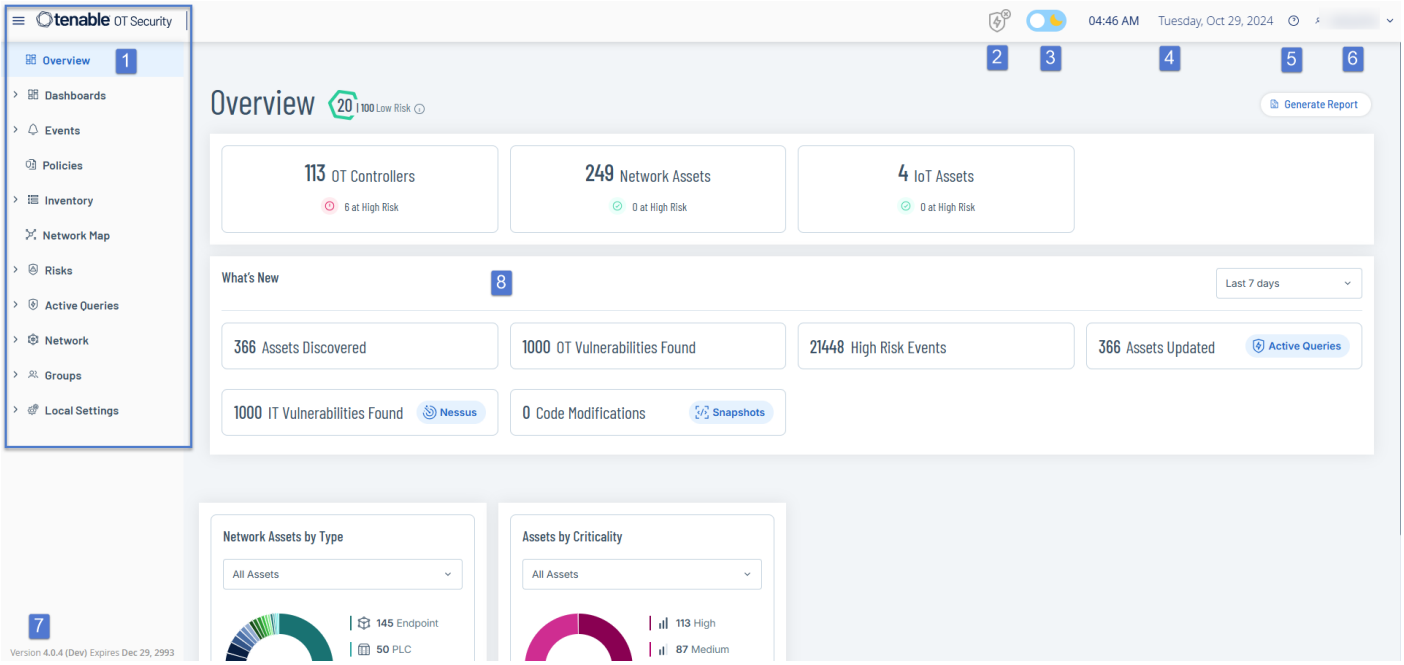
> 注意: バックアップを復元してからコマンドが終了するので、プロセス完了までに時間がかかります。次の場所から復元の進行状況を確認できます:
> Tenable Core ユーザーインターフェースの [バックアップ/復元] > [バックアップ/復元ログ] > [復元] のログ。あるいは、次のコマンドを実行します。
>
> `journalctl -xf tenablecore.restorelocal@$(systemd-escape /home/admin/my-tc-ot-backup.tar)`
>
> ここで `/home/admin/my-tc-ot-backup.tar` は実際のバックアップファイルの場所です。

OT Security が復元され、アプリケーションにアクセスできるようになります。OT Security が実行中であ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。

シリアル番号	ユーザーインターフェース要素	説明
1	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、メインナビゲーションメニューの表示/非表示を切り替えます。
2	アクティブクエリ	アクティブクエリが有効か無効かを示します。
3	ダークモード/デイライト	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

	モード	更します。
4	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。
5	リソースセンター	OT Security リソースセンター。
6	現在のユーザー名	システムに現在ログインしているユーザーの名前を表示します。下矢印をクリックすると次のメニューオプションが表示されます: [バージョン情報] (ソフトウェア情報を表示) と [ログアウト]。 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。
7	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。
8	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。

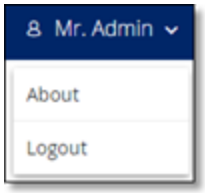
現在のソフトウェアバージョンの確認

ヘッダーバーの右上隅のユーザープロフィー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ます。

OT Security によりユーザーメニューが表示されます。



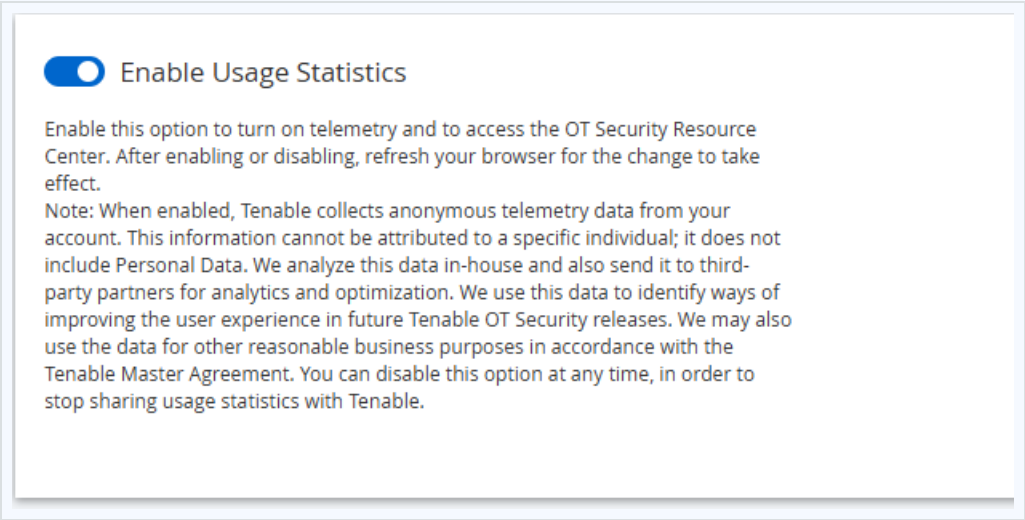
2. [バージョン情報] をクリックします。

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] ⓘ はデフォルトでは無効になっています。[リソースセンター] を有効にするには、[設定] > [システム設定] > [デバイス] に移動し、[収集データの有効化] トグルをクリックして有効にします。



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。

- 概要 – ネットワークのインベントリとセキュリティポスチャーの全体像を示すウィジェットを表示します。OT Security の概要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] ページに、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。[すべての資産] には、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含まれます。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。ネットワークマップを参照してください。
- リスク – CVE、脆弱なプロトコル、脆弱なオープンポートなどを含め、OT Security によって検出されたすべてのネットワーク脅威を、推奨される修正手順とともに表示します。脆弱性を参照してください。
- アクティブクエリ – 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。アクティブクエリの管理を参照してください。
- 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経時的なデータを表示することで、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、ネットワーク情報が次の 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。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。

> 重要: OT Security バージョン 4.0 以降では、いくつかの UI 変更が導入されていますが、アプリケーションのすべてのページがアップデートされているわけではありません。このバージョンでは、[インベントリ] および [脆弱性に関する検出結果] のページでのみ、カスタマイズ、フィルター、並べ替え、検索を行う方法が改善されています。これらの手順については、4.0 用のマークが付いている見出しのセクションに記載されています。例: OT Security 4.0 以降の列表示のカスタマイズ。

> 注意: ここでは、[すべてのイベント] および [すべての資産] ページが例として挙げられていますが、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。OT Security 4.0 以降では、[表示されている列] > [デフォルトにリセット] をクリックします。

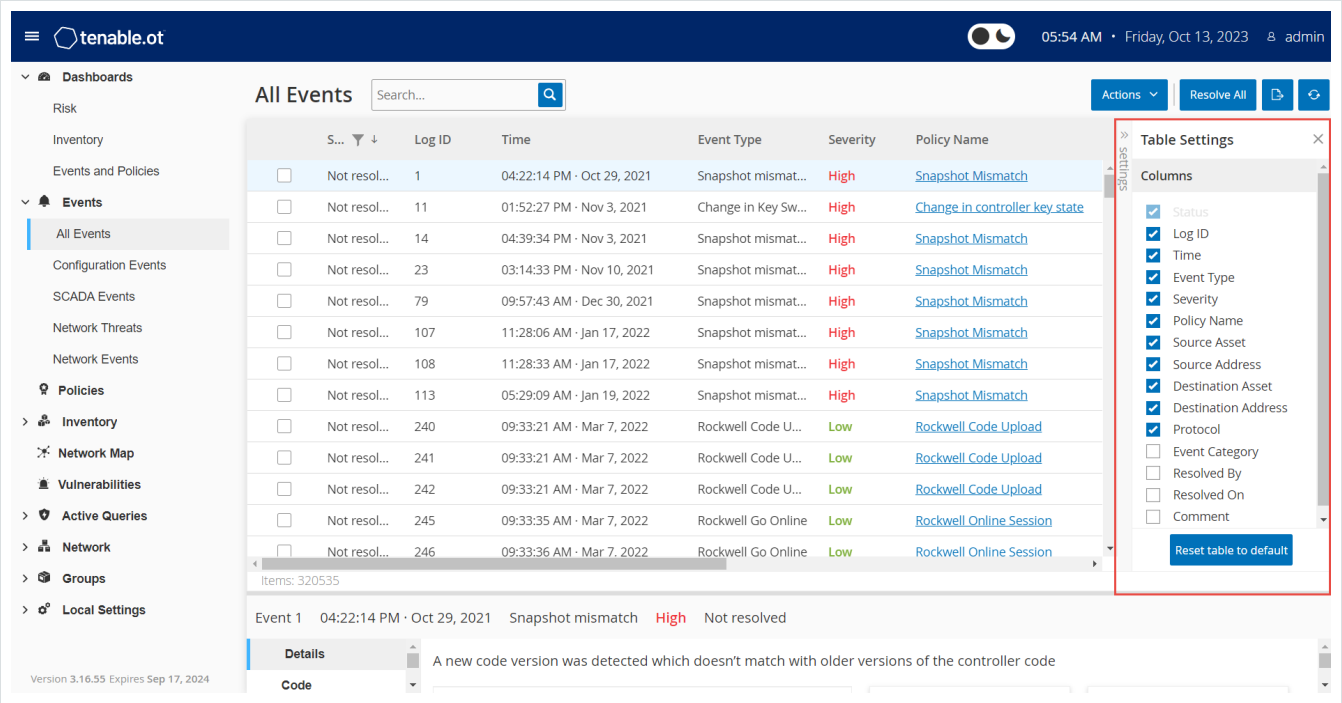
列表示のカスタマイズ (3.19 以前)

表示する列とその編成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] パネルが表示され、そこに [列] セクションがあります。



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 により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。

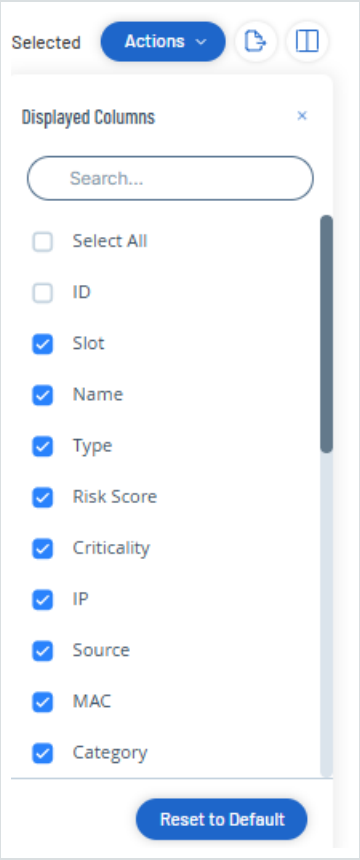
列の表示順序の調整手順

1. 列ヘッダーをクリックして、目的の位置にドラッグします。

列表示のカスタマイズ (4.0 以降)

1. ヘッダーバーで、 ボタンをクリックします。

   [表示されている列] パネルが表示されます。



2. 表示する列の横にあるチェックボックスを選択します。

   注意: 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。

   ヒント: [検索] ボックスを使用して、特定の列を検索します。

3. ✕ ボタンをクリックして、[表示されている列] パネルを閉じます。

   OT Security により選択した列のみが表示されます。

リストのカテゴリ別グループ化 (3.19 以前)

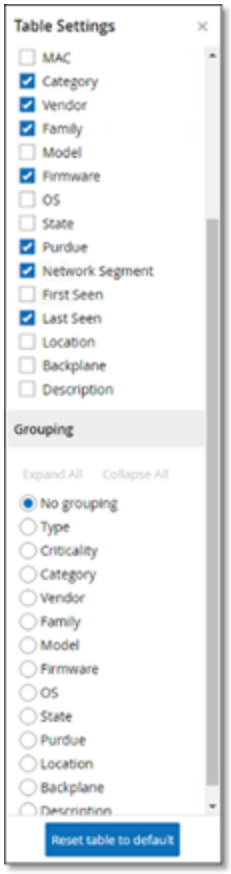
[インベントリ] ページでは、その特定の画面に関連するさまざまなパラメーターを基準に、リストをグループ化できます。

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。

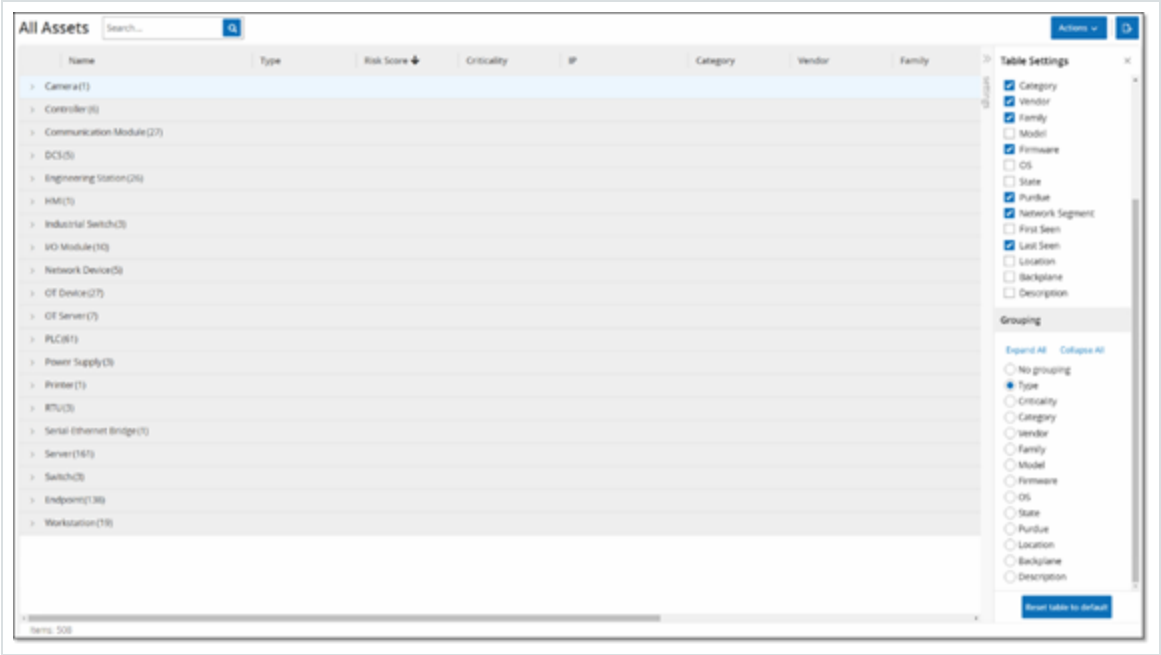
   [テーブル設定] ペインが右側に表示され、[列] セクションと [グループ化] セクションが表示されます。

2. [グループ化] セクションまでスクロールします。



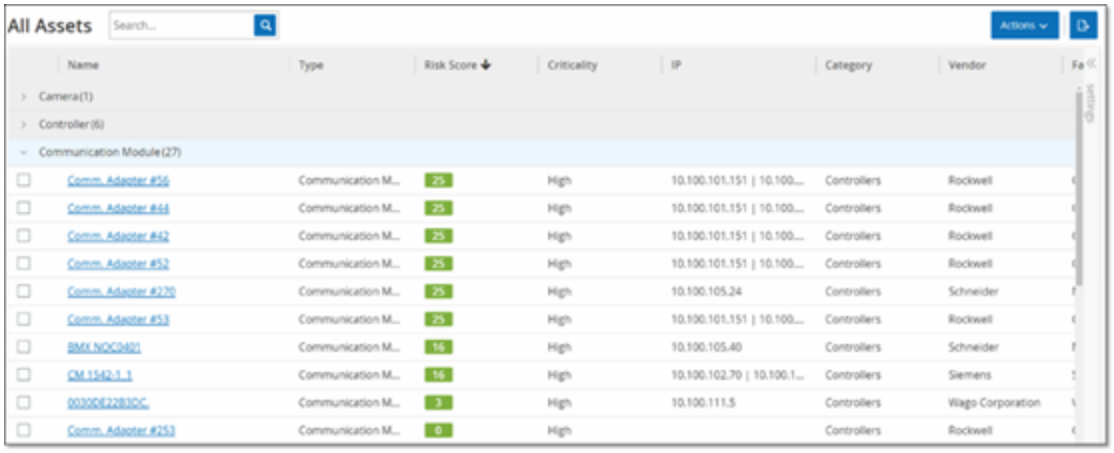
3. リストをグループ化する基準となるパラメーターを選択します。たとえば [タイプ] を選択します。

   OT Security は、グループ化されたカテゴリを表示します。



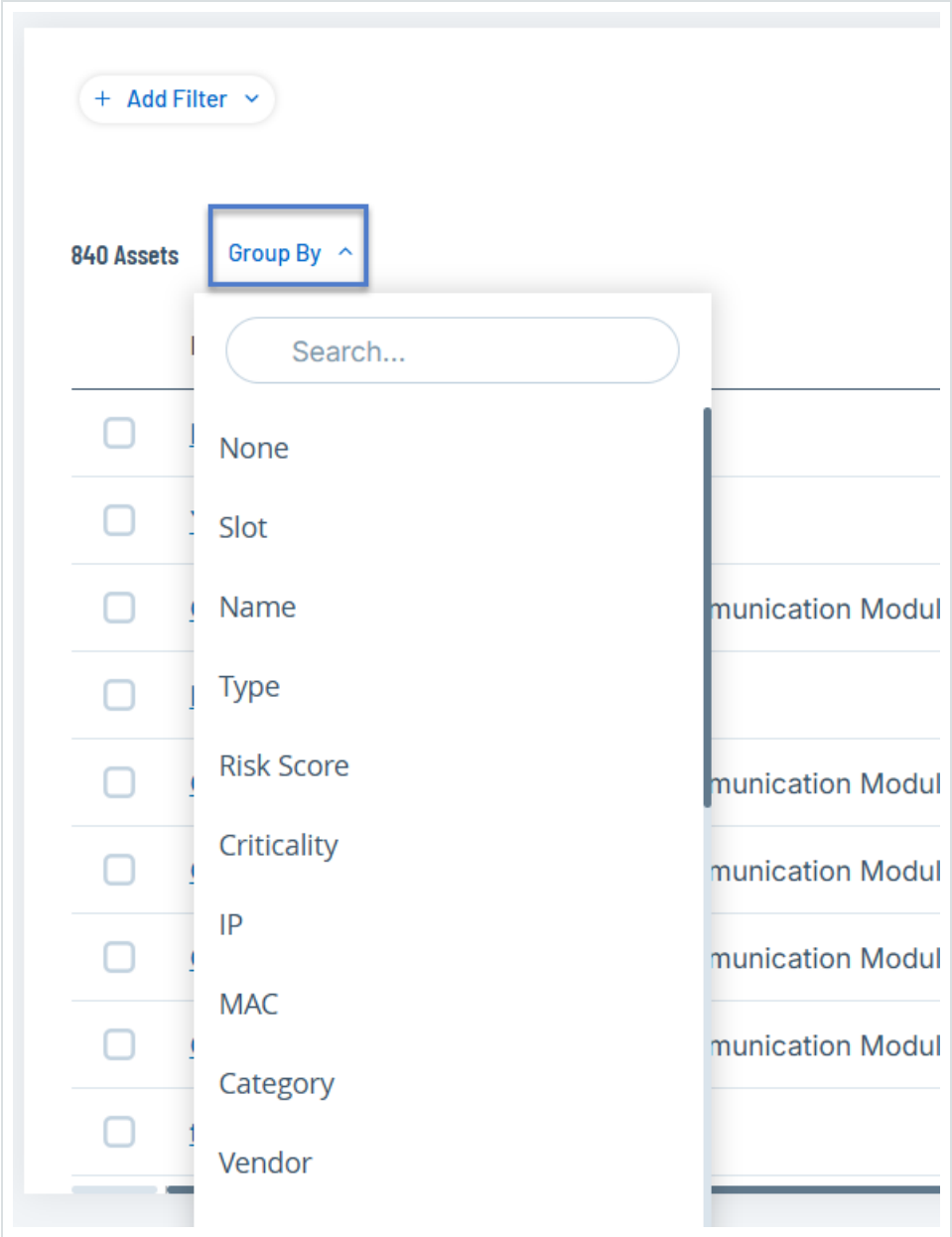
4. [x] または [設 定] タブをクリックして、[テーブル設 定] ウィンドウを閉じます。

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。



リストのカテゴリ別 グループ化 (4.0 以降)

1. テーブルのヘッダーで、[グループ化 の基 準] ドロップダウンリストをクリックします。



2. リストのグループ化に使用するパラメーターを選択します。例: 名前。

> ヒント: [検索] ボックスを使用して、特定のパラメーターを検索します。

OT Security は、選択したパラメーターでリストをグループ化します。

> 注意: リストを展開または折りたたむには、それぞれ [すべて展開] または [すべて折りたたむ] ボタンを使用します。

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)。

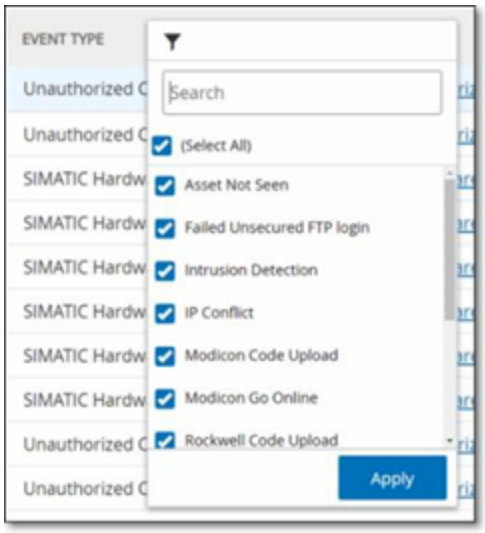
列のフィルタリング (3.19 以前)

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。各ページには、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] 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固有です。



3. 表示する要素を選択し、非表示にする要素のチェックボックスの選択を解除します。

> 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することができます。

4. フィルターのリストを検索し、フィルターを選択または選択解除できます。

5. [適用] をクリックします。

   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。

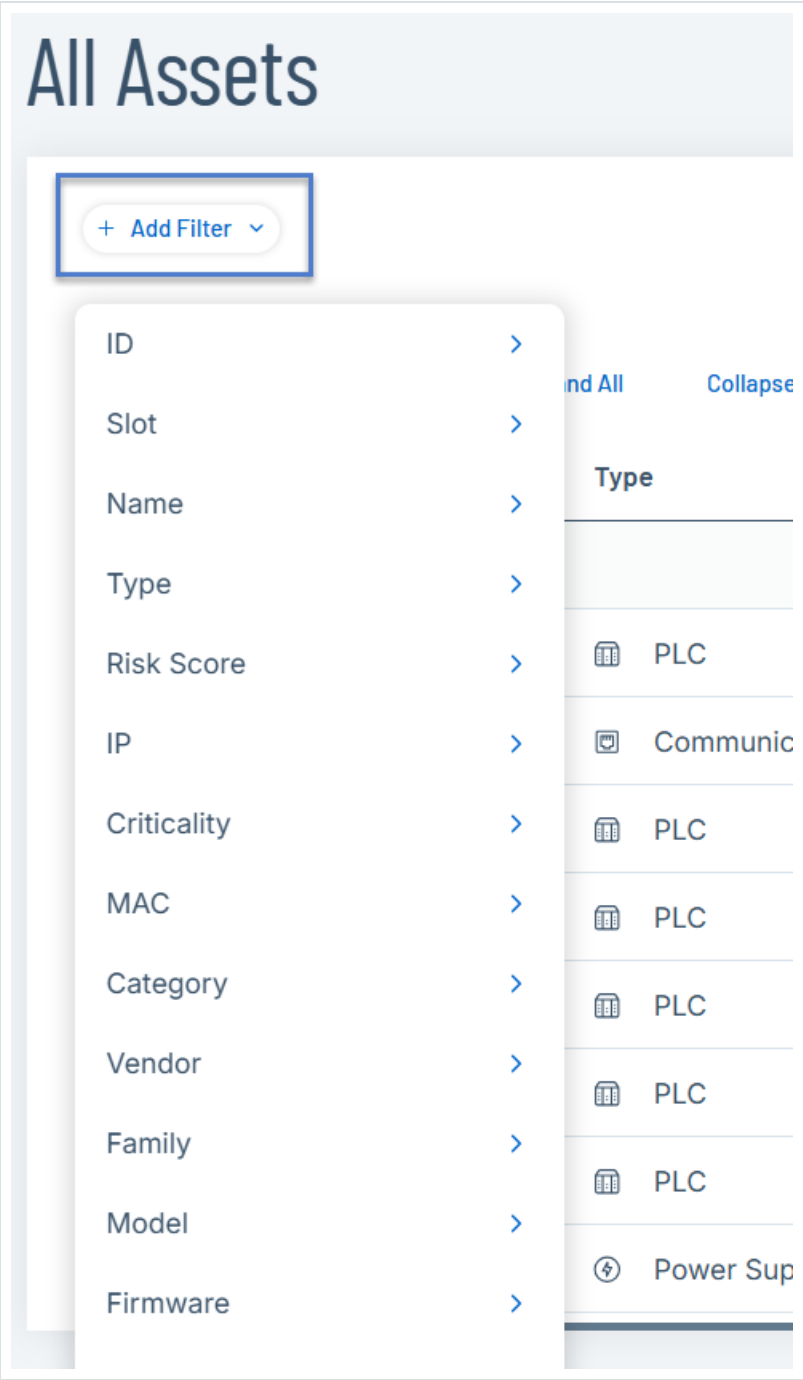
3. [すべて選択] チェックボックスをもう一度クリックして、すべての要素を選択します。

4. [適用] をクリックします。

列のフィルタリング (4.0 以降)

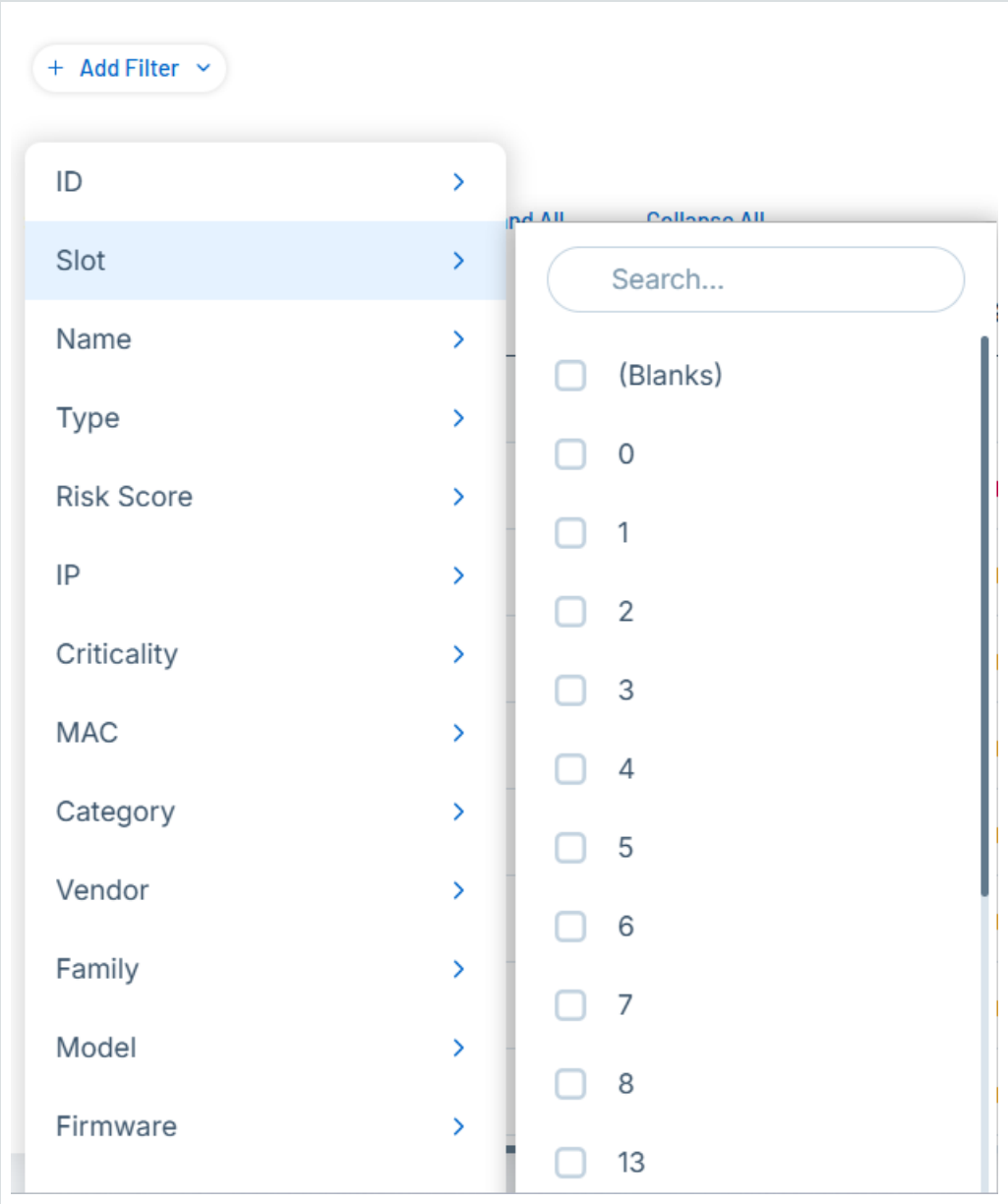
1. テーブルのヘッダーで、＋ [フィルターを追加]ドロップダウンリストをクリックします。

   利用可能なフィルター要素を含むドロップダウンメニューが表示されます。



2. フィルタリングの基準となる要素を選択します。

フィルターオプションのリストが表示されます。

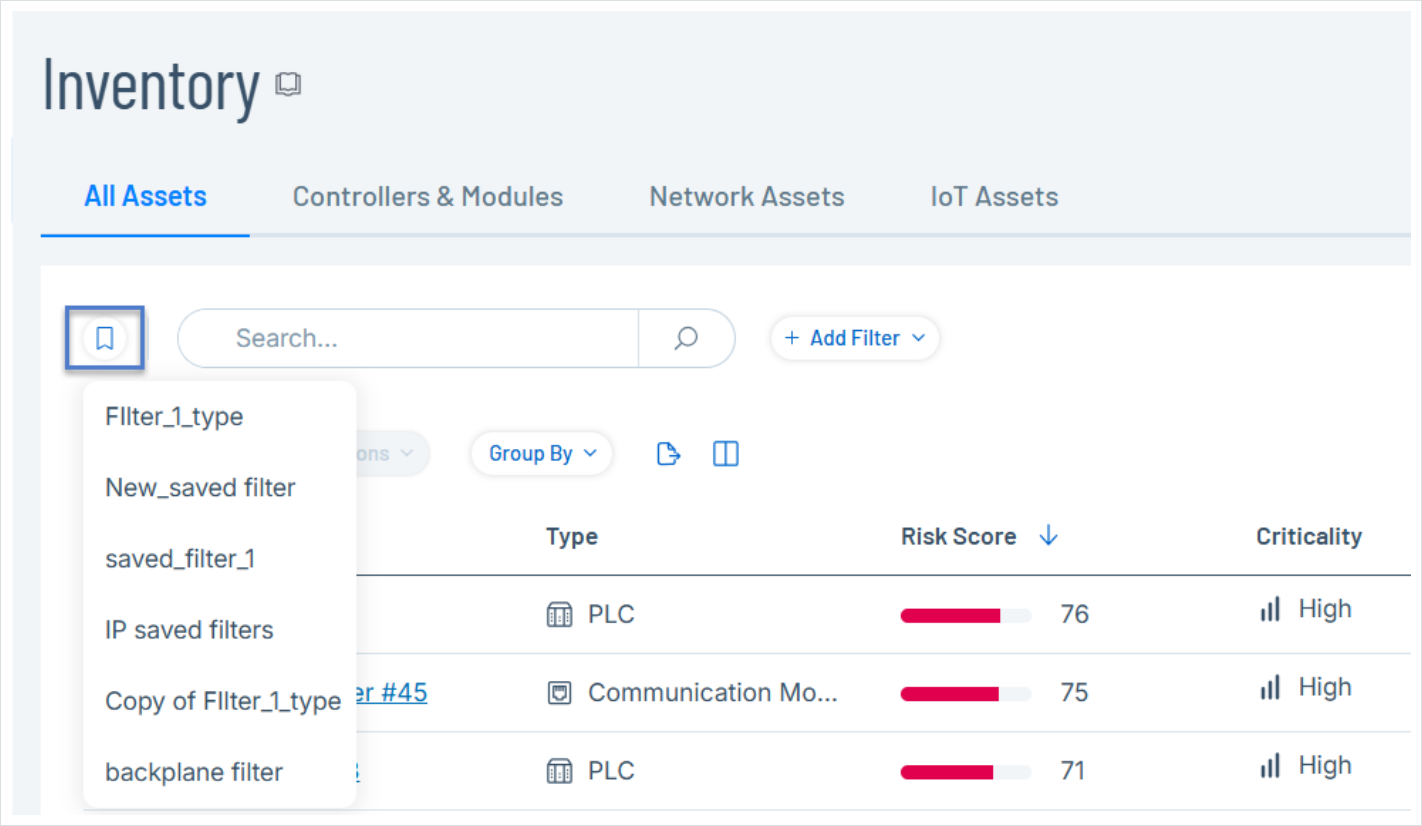


3. フィルタリングするオプションの隣にあるチェックボックスを選択します。

> ヒント: [検索] ボックスを使用して、特定のフィルターオプションを検索します。

フィルターの保存

頻繁に使用するフィルターを保存しておき、必要に応じて [保存済みフィルター] からアクセスできます。これにより、特定のフィルタリングされたビューを保存し、すぐにそのビューに戻ることができます。



注意: フィルターの保存機能は、[インベントリ]、[検出結果] > [脆弱性]、[検出結果] > [ポリシー違反] のページで利用できます。

頻繁に使用するフィルターを保存する方法

1. テーブルのヘッダーで、 + [フィルターを追加] ドロップダウンリストをクリックします。

   利用可能なフィルター要素を含むドロップダウンメニューが表示されます。

2. 目的のフィルター要素を選択します。

3. [フィルターの適用] をクリックします。

   OT Security はフィルタリングされた結果を表示します。

4. フィルターを保存するには、[フィルターを保存] をクリックします。

[フィルターを保存] パネルが表示されます。

5. [名前] ボックスにフィルターの名前を入力します。
6. [保存] をクリックします。

   OT Security によりフィルターが保存されます。
7. 保存済みフィルターにアクセスするには、 ボタンをクリックします。

   保存済みフィルターのリストが表示されます。
8. 目的のフィルターをクリックし、フィルタリングされた結果を表示します。

保存済みフィルターの変更

既存の保存済みフィルターに変更を加えることができます。

既存の保存済みフィルターの変更方法

1. テーブルのヘッダーで ボタンをクリックします。

   保存済みフィルターのリストが表示されます。
2. 変更する保存済みフィルターをクリックします。
3. 必要に応じてフィルター要素を追加または削除します。
4. [フィルターを保存] をクリックし、[変更を保存] を選択します。

   OT Security によりフィルターの変更が保存されます。

保存済みフィルターの複製

保存済みフィルターを複製して、新しいフィルターとして保存できます。

保存済みフィルターを複製して新しい名前で保存する方法

1. テーブルのヘッダーで ボタンをクリックします。

   保存済みフィルターのリストが表示されます。

2. コピーする既存の保存済みフィルターをクリックします。

3. [フィルターを保存] をクリックし、[コピーとして保存] を選択します。

   [フィルターを保存] パネルが表示されます。

4. [名前] ボックスで、フィルター名を変更します。

5. [保存] をクリックします。

   OT Security によりフィルターが保存されます。

すべてのフィルターの削除

適用されているすべてのフィルターをクリアし、表をフィルタリングされていない元の状態に戻す方法

- テーブルのヘッダーで、[すべてのフィルターを削除] をクリックします。

検索 (3.19 以前)

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] ボタンをクリックします。

検索 (4.0 以降)

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、 ボタンをクリックします。

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

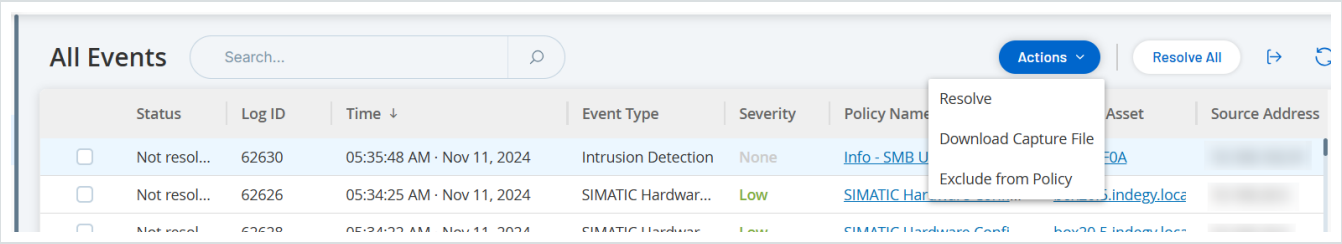
1. データをエクスポートするページに移動します。
2. ヘッダーバーで ボタンをクリックします。

   OT Security がデータを CSV 形式でダウンロードします。

アクションメニュー

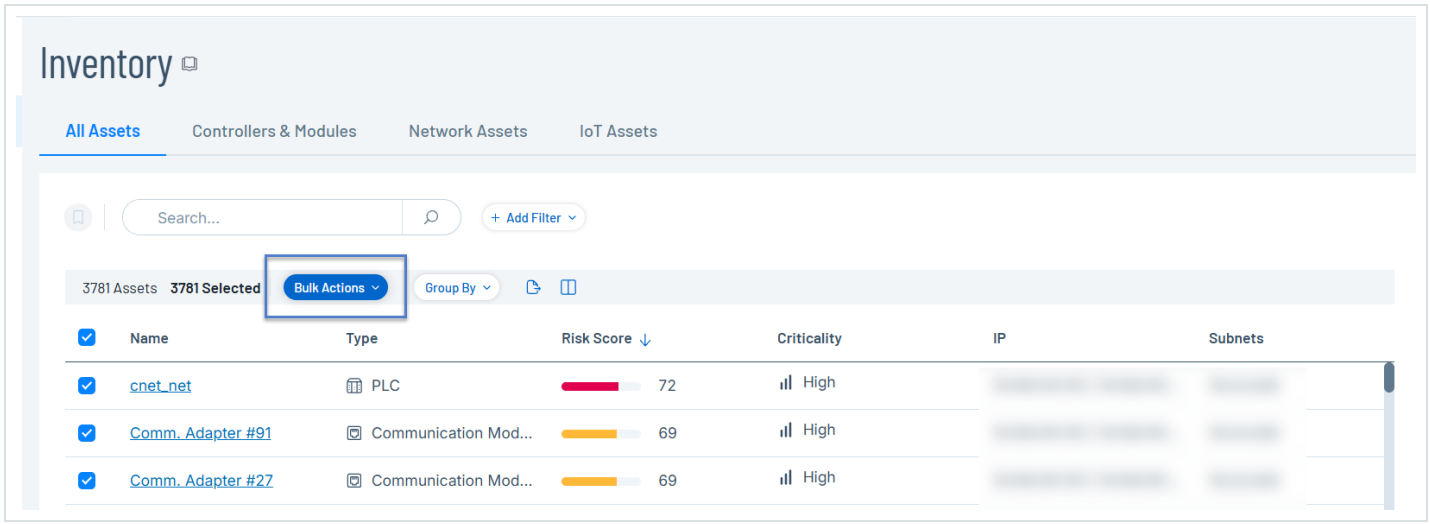
各画面には、その画面の要素に対して実行できる一連のアクションがあります。たとえば、[ポリシー] 画面では、ポリシーの **[表示]**、**[編集]**、**[複製]**、**[削除]** ができます。[イベント] 画面では、イベントの **[解決]** または **[キャプチャファイルのダウンロード]** ができます。

[アクション] メニューにアクセスする方法

- 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。
- 

一括アクション

ページで複数の要素を選択すると、OT Security でヘッダーの [一括アクション] オプションが有効になります。



OT Security の概要

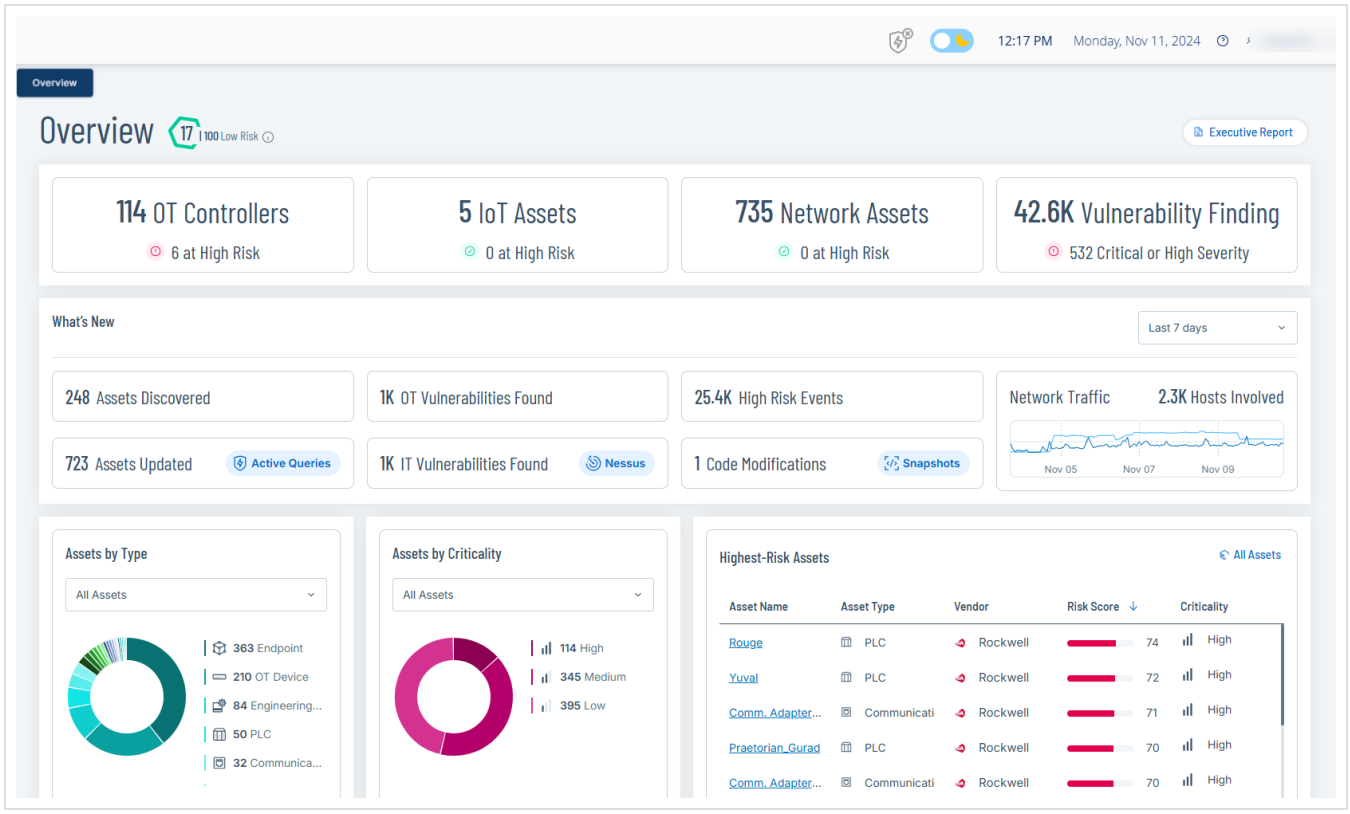
[概要] ページを使用して、インタラクティブなウィジェットで OT 環境の主要なインサイトを表示できます。このページのウィジェットから、環境に関する次のようなリアルタイムのインサイトが得られます。

- 環境のセキュリティ返信に関する情報
- 最後ログイン以降に生じた直近の変化のサマリー
- インベントリ内のさまざまなタイプの資産の内訳
- 資産と脆弱性の現在の状態。
- 最も高いリスクをもたらす資産
- 最終コードリビジョンのタイムスタンプ

[概要] ページにアクセスする方法

1. 左側のナビゲーションバーで、[概要] をクリックします。

   [概要] ページが表示されます。



[概要] ページには以下のウィジェットが含まれています。

ウィジェット	説明
リスクスコア	[リスクスコアの平均] は、環境内のすべての資産スコアの平均です。スコアの内訳を表示するには、値にカーソルを合わせます。 [リスクスコアの平均] は、次のカラーコードでリスクの深刻度を示します。 • 低 (緑): 0 ~ 29 • 中 (黄色): 30 ~ 69 • 高 (赤): 70 ~ 100

	OT Security は、時間とともに変化する次の要素 (要因、ファームウェア、状態の変化) に基づいて資産スコアを計算します。 • 重大度 - 資産タイプとパデューレベルに基づく。たとえば、PLC は実働環境をコントロールするため重要と見なされますが、カメラは通常それより重要度が低いと見なされます。 • 脆弱性 - VPR (脆弱性優先度格付け) 資産に基づく。 • イベント - 資産に関連付けられているイベントに基づく。ポリシーはイベントをトリガーし、各ポリシーは深刻度を定義します。深刻度は、イベントの数、その深刻度、およびイベントが存在していた期間に基づいて計算されます。古いイベントがスコアに与える影響は、新しいイベントよりも少ないです。 • バックプレーン - バックプレースに存在する資産は、その隣接資産のスコアに影響を与えます。たとえば、1 つのモジュールが脆弱である場合、そのバックプレーン全体も脆弱です。
資産と脆弱性	環境内の資産と脆弱性の現在の状態。資産タイプ (OT コントローラー、ネットワーク資産、IoT 資産) ごとに個別のウィジェットがあり、そのカテゴリにある資産の数と高リスクの資産の数が表示されます。 注意: リスクスコアが 70 以上の資産は、高リスクと見なされます。
新機能	新しい資産、脆弱性、高リスクイベントなど、最後ログイン以降に生じた変化のサマリー。ドリルダウンしてそれぞれの資産、イベント、または脆弱性のページを開き、フィルタリングされた資産、脆弱性、イベントを表示できます。 新しい資産、脆弱性、高リスクの違反、運用上の違反など、最終ログイン以降に生じた変化のサマリー。ドリルダウンしてそれぞれの資産、検出結果、脆弱性のページを開き、フィルタリングされた資産、脆弱性、イベントを表示できます。 フィルタードロップダウンを使用して、[過去 1 日]、[過去 7 日] (デフォルト)、または [過去 30 日] で結果をフィルタリングできます。

資産 (タイプ別)	タイプ (エンドポイント、PLC、OT デバイスなど) 別の資産の数。
資産 (重大度別)	重大度 (高、中、低) 別の資産の数。
リスクの最も高い資産	すべての高リスク資産を、資産名、タイプ、ベンダー、リスクスコア、重大度などの詳細とともにリストします。[すべての資産] ページに移動するには、右上にある [すべての資産] リンクをクリックします。
エグゼクティブレポート	OT 環境のリスク評価レポートを生成します。詳細は、エグゼクティブレポートの生成を参照してください。

エグゼクティブレポートの生成

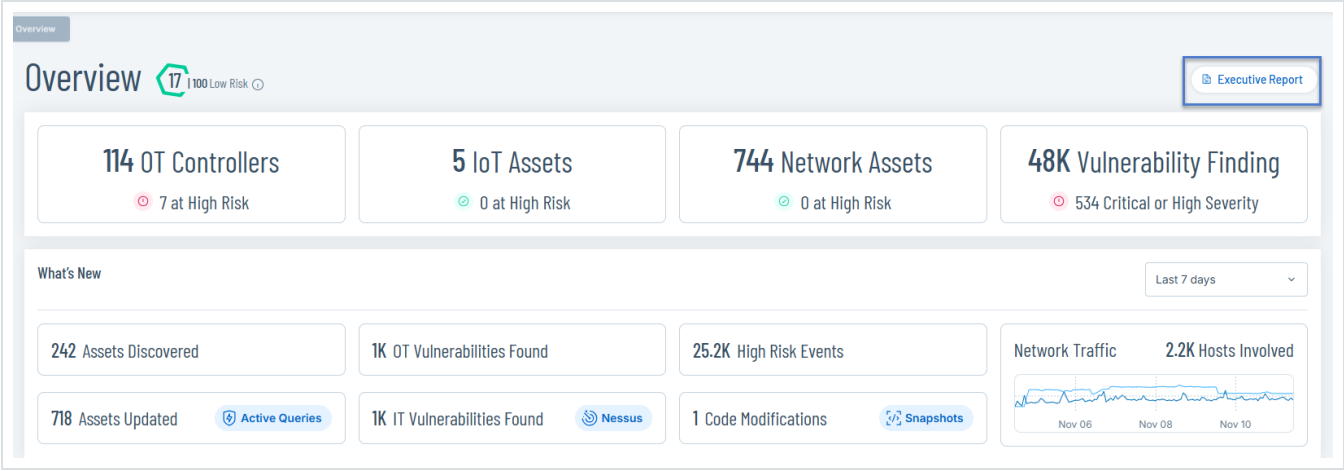
過去 30 日間のデータに基づいて、ご利用の環境のリスク評価レポートを生成できます。OT Security は、[リスク]、[インベントリ]、[イベントとポリシー] ダッシュボードの主要ウィジェットを使用して、グラフィカルな概要を作成し、高リスクの資産、重大な脆弱性と一般的な脆弱性、一般的なプラグインファミリー、および最近検出された資産をハイライトします。

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、[概要] に移動します。

   [概要] ページが表示されます。



2. 右上の [エグゼクティブレポート] をクリックします。

   OT Security がブラウザでレポートを開きます。

3. 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。

4. [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。

5. レポートを保存する場所を参照します。

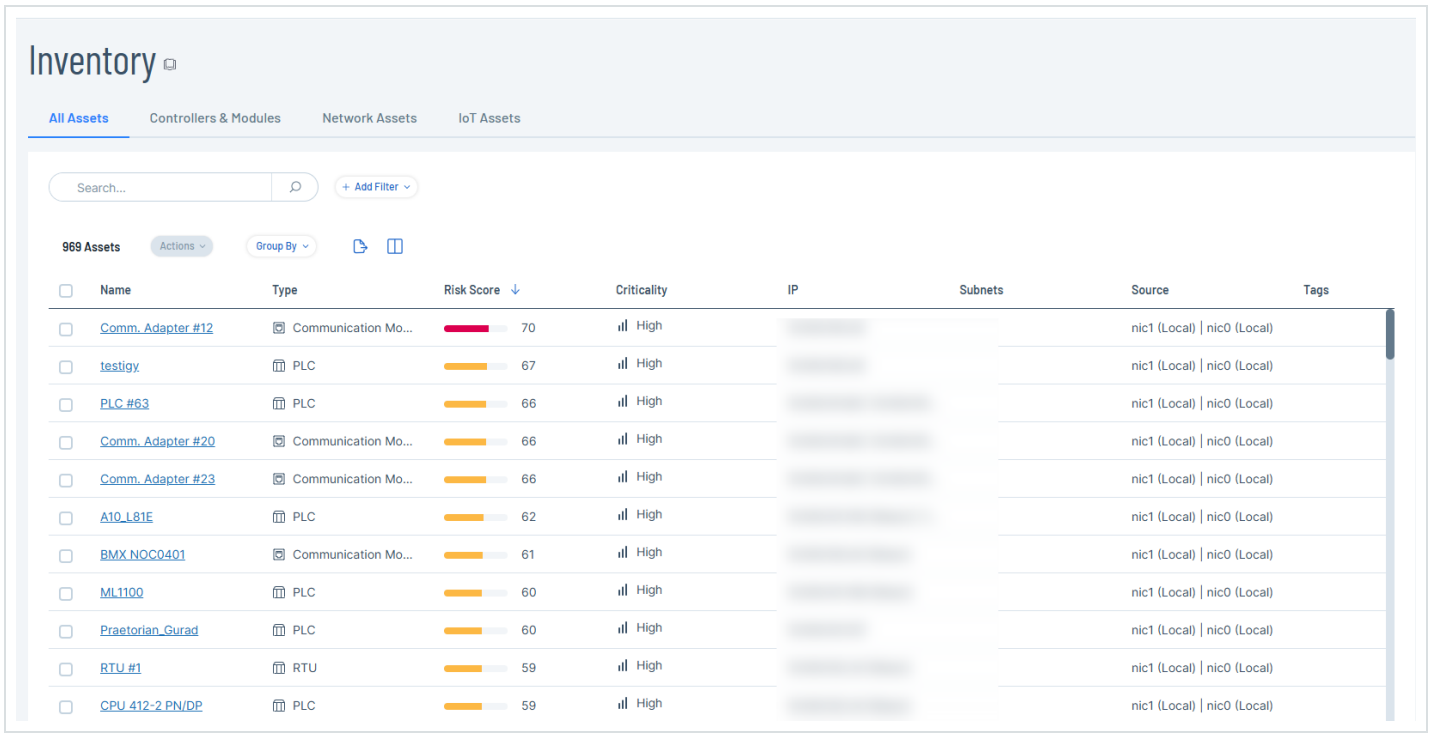
6. [保存] をクリックします。

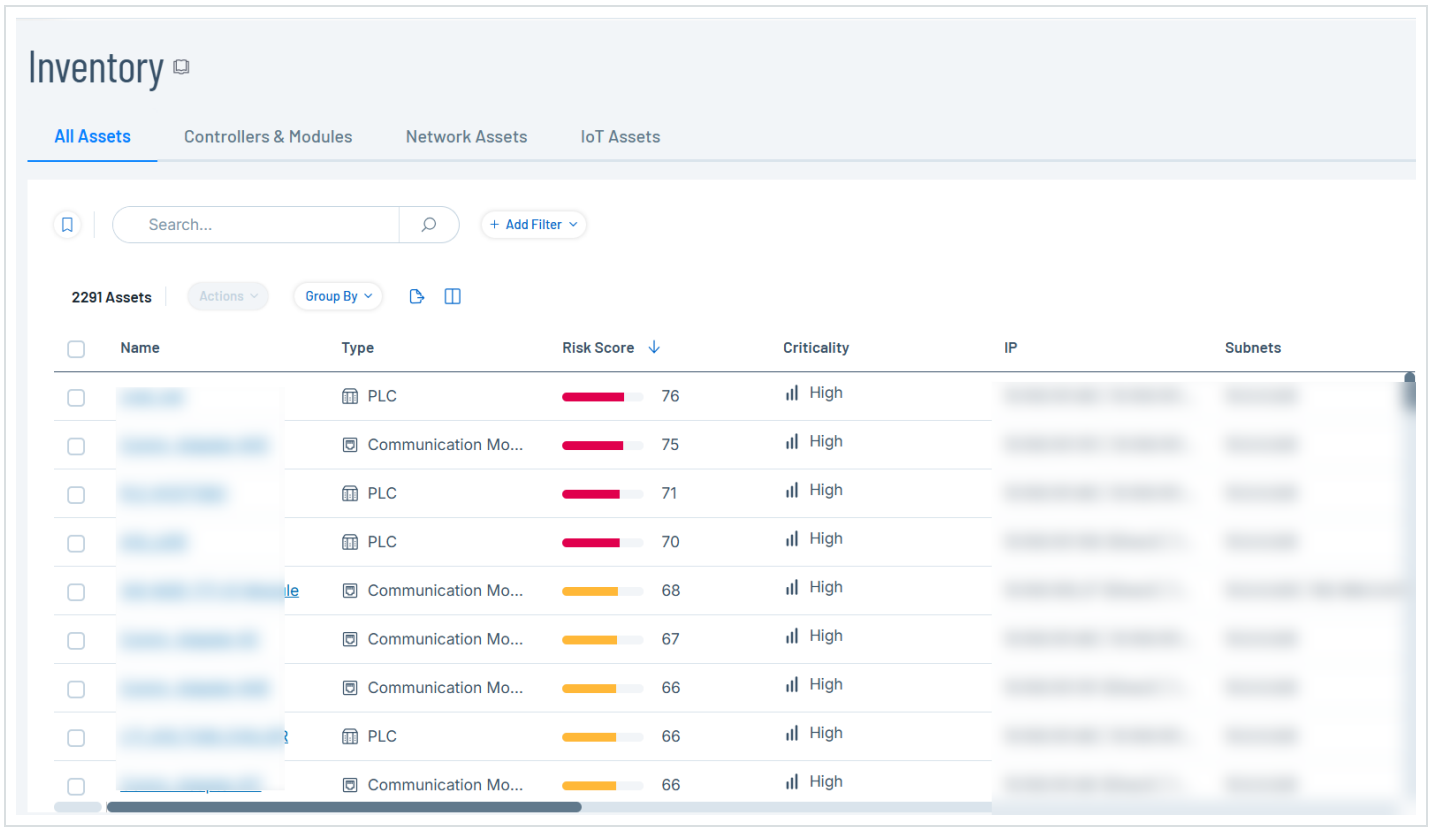
   OT Security によりレポートが PDF 形式で保存されます。

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。
サブネット	SNMP を介してネットワークデバイスにクエリを実行することで検出されたサブネット

パラメーター	説明
ソース	ソースの名前。例: ローカルソースの場合は nic 1 または nic 2、ソースがセンサーの場合はセンサー名。
MAC	資産の MAC アドレス。
タグ	[資産グループとタグ] ページで資産に対して作成したタグ。
ネットワークセグメント	この資産の IP が割り当てられるネットワークセグメント。
タイプ	資産のタイプ。コントローラー、I/O、通信など。資産タイプを参照してください。
バックプレーン*	資産が接続されているバックプレーンユニット。バックプレーン構成に関する追加の詳細が、[資産詳細] 画面に表示されます。
スロット*	バックプレーン上にある資産の場合、資産が取り付けられているスロットの番号が表示されます。
ベンダー	資産ベンダー。
ファミリー*	資産ベンダーによって定義された製品のファミリー名。
ファームウェア	現在資産にインストールされているファームウェアのバージョン。
場所	OT Security の資産詳細でユーザーが入力した資産の場所。資産詳細の編集を参照してください。
最終確認日	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。

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

資産タイプ

次の表では、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

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	
				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

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	
				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

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	
				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

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	
				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

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	
				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

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	
				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

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	
				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

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	
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

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	

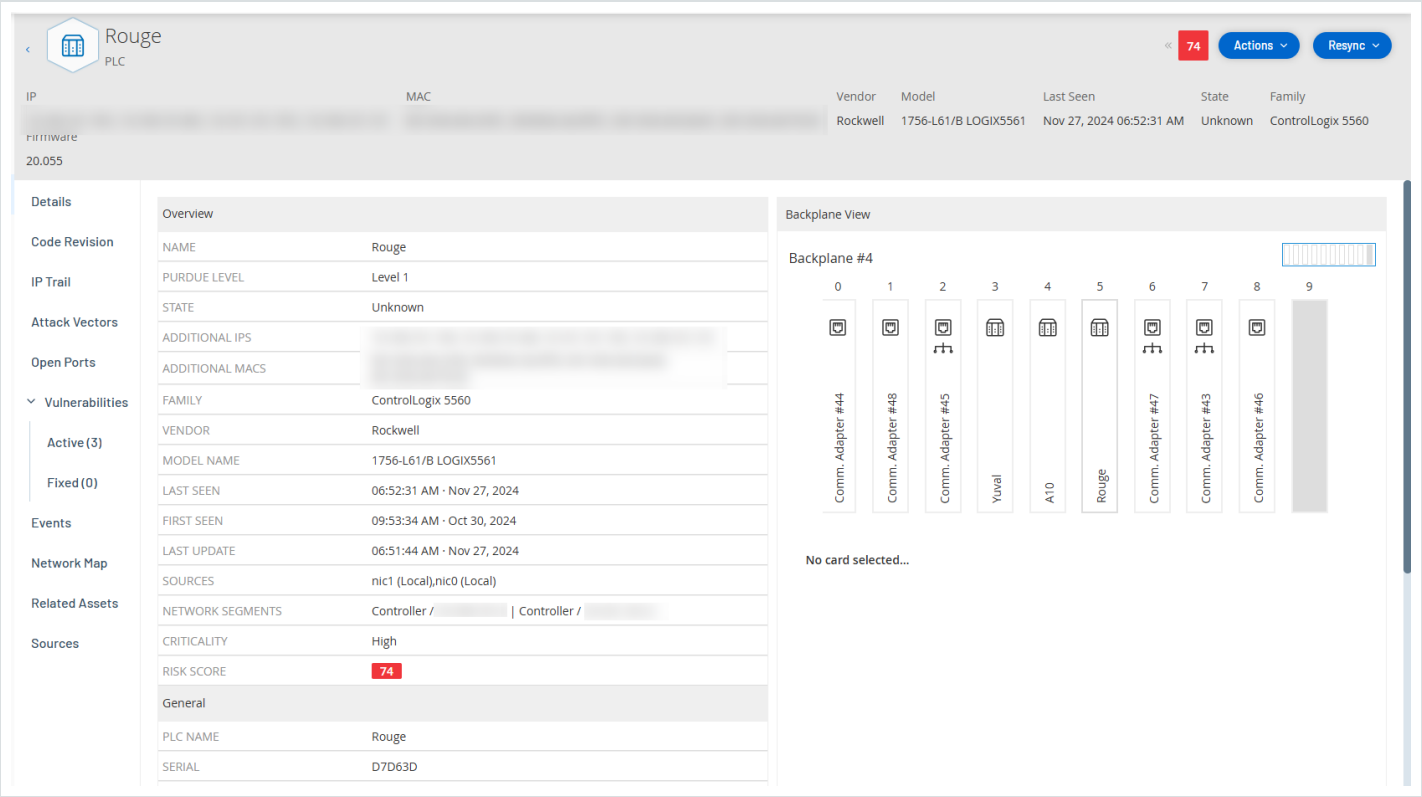
カテゴリ	デフォルトの重大度レベル / パデューレベル	説明	サブタイプ	
				IP 電話
				スマートセンサー
				バーコードスキャナー
				アクセス制御システム
				照明制御
				HVAC モジュール
				スマートハブ

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	
				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

資産の詳細の表示

必要な OT Security ユーザーロール: 管理者、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

[資産の詳細] 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. 次のいずれかを行います。

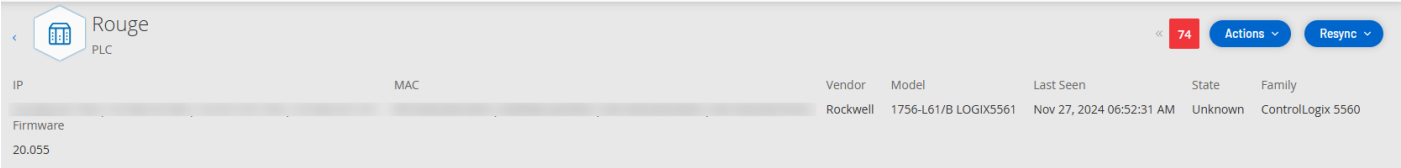
   - 資産名がリンクとして表示されているいずれかのページ ([インベントリ]、[イベント]、または [ネットワーク]) で資産名をクリックします。
   - インベントリページで、[アクション] > [表示] をクリックします。

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、選択した資産に関してシステムが特定した脆弱性 (修正済みとアクティブ) を表示します。脆弱性を参照してください。
- イベント – 資産が関係して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。
- 関連資産 – ネストされたすべての資産のリストが表示されます。
- ソース – 場所、タイプ、資産の IP アドレスと MAC アドレス、初回報告時刻と最終報告時刻など、資産のソースに関連するすべての情報が表示されます。

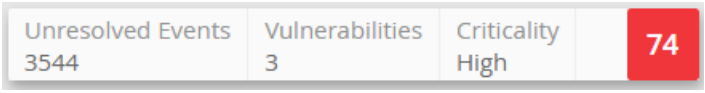
ヘッダーペイン

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元の画面に戻ります。
- 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 - クリックしてこの資産で利用可能な 1 つ以上のクエリを手動で実行します。再同期の実行を参照してください。

詳細

[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、指定した資産の各種のシステムデータと設定データが表示されます。OT Security は、指定された資産に関連するセクションのみを表示します。次のリストには、さまざまな資産タイプで表示される可能性があるすべてのセクションカテゴリが含まれています: 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。

> 注意: OT Security は資産から抽出した詳細のみを表示します。すべての資産ですべてのセクションが表示されるわけではありません。たとえば、[全般]、[Nessus スキャン情報] などです。

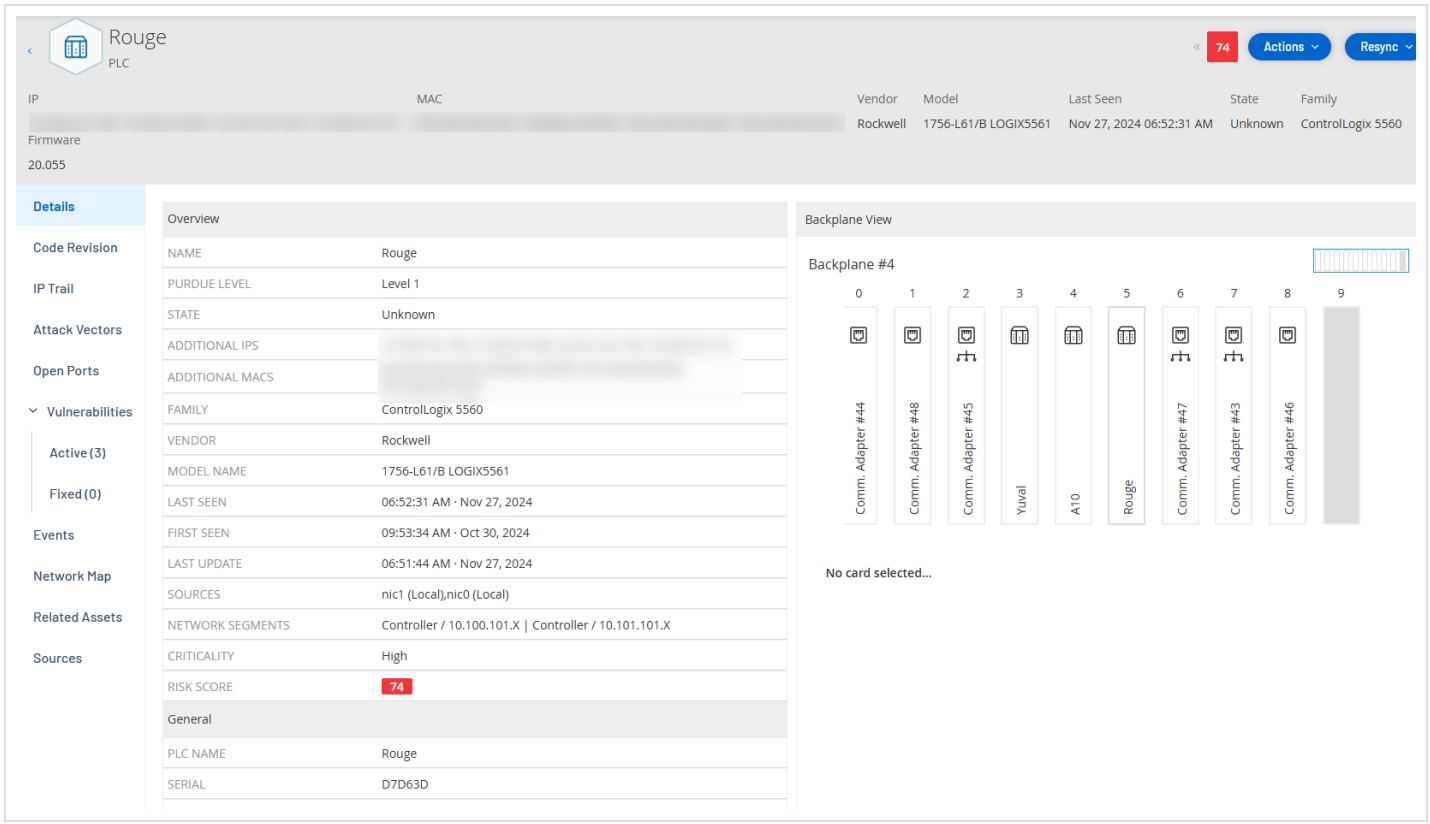
次の表は、[概要] セクションの詳細を示しています。

セクション	説明
名前	パッシブモニタリングまたはアクティブクエリによって取得、または資産タイプと一意の識別子を使用して自動的に生成される資産名。
説明	ユーザーからの資産の説明。
パデューレベル	資産に割り当てられたパデューモデルレベル。
状態	資産の現在の運用ステータス。このフィールドは、特定の資産タイプ (通常はコントローラー) に関連しています。
Direct IP	その特定の資産またはモジュールに存在する、または設定されている IP アドレス。
Direct Mac	その特定の資産またはモジュールに物理的に存在する、または設定されている Mac アドレス。
追加の IP	資産に間接的にアクセスするために使用される、資産とバックプレーンまたは類似のインフラを共有する他のモジュールに関連付けられた IP アドレス。 たとえば、PLC (コントローラーモジュール) には独自のネットワークインターフェースがなく、

セクション	説明
	別のスロットにインストールされた通信モジュールに設定されたIPアドレス経由でアクセスされる場合があります。資産にはバックプレーン以外の接続がある可能性があります。
追加のMac	資産に間接的にアクセスするために使用される、バックプレーンまたは類似のインフラを共有する他のモジュールに関連付けられたMacアドレス。
ファミリー	資産が属するデバイスファミリーまたは製品ライン。
ベンダー	資産の製造者またはサプライヤー。
モデル名	資産の特定のモデル番号。
最終確認日	OT Securityが資産を最後に検出した日時。 OT Securityは、PCAP (トラフィックキャプチャファイル) を再生するとき、または同様の分析を実行したときに、このフィールドを更新する場合があります。
初回確認日	資産が最初に検出された日時。[最終確認日]の値と同じか、それよりも前のはずです。
最終更新日	資産のいずれかの詳細の最新更新日時。 注意: 説明の更新など、資産情報を手動で変更すると、資産が現在アクティブかどうか、最近検出されたかどうかに関わらず、この値が更新されます。
ソース	資産に特定された、または資産に関連付けられているソース (センサー、PCAP、ローカルインターフェースなど)。
ネットワークセグメント	資産に割り当てられた、または関連付けられたネットワークセグメント。

セクション	説明
重大度	[高]、[中]、[低] で評価された資産の重大度。
リスクスコア	資産に関連するリスクがもたらす潜在的な影響を反映。スコアは、重大度、脆弱性、未解決のイベント (およびその期間)、関連資産 (バックプレーン経由など)、その他の関連する考慮事項などの要因の影響を受けます。
タグ	資産に関連付けられているタグ資産グループとタグを参照してください。

バックプレーンビュー



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ます。このセクションには、接続されている各デバイスのスロット位置など、バックプレーン設定がグラフィカルに表示されます。デバイスを選択して、下部のペインにその詳細を表示します。

Nessus スキャン情報

Nessus スキャン情報は次のことに役立ちます。

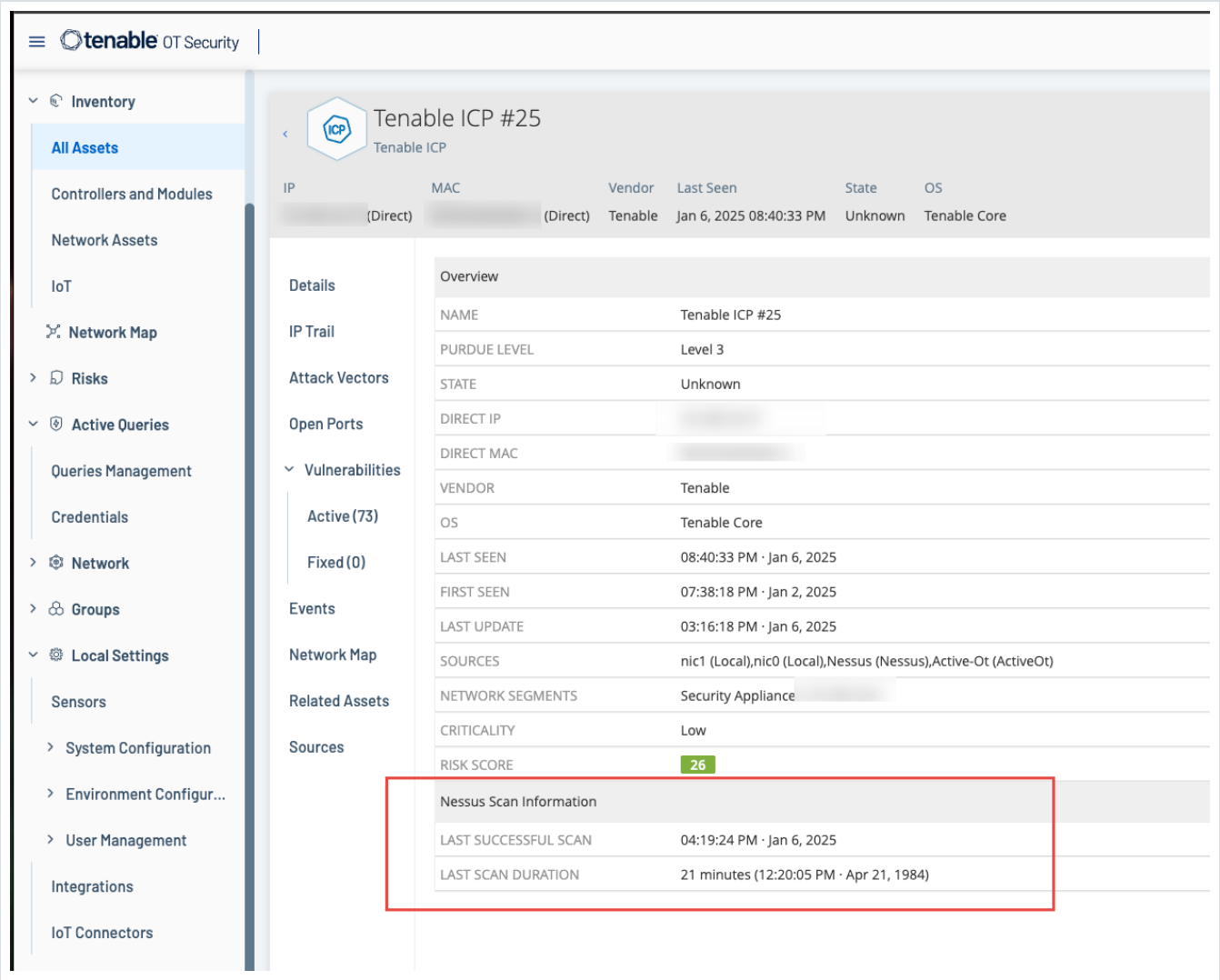
- 評価済み資産と未評価の資産を把握する。
- 資産が認証スキャンと非認証スキャンのどちらの対象になっているのかを把握する。
- スキャンと脆弱性管理に関するベストプラクティスを実行する。たとえば、Windows、Linux を実行している IT タイプの資産に対して脆弱性評価スキャンを実行できます。認証情報の有無にかかわらず、スキャンは組織のどの程度のアタックサーフェスが内部と外部の両方で露出されているかを評価するのに役立ちます。

Nessus スキャンの詳細については、Nessus プラグインスキャンの作成を参照してください。

[詳細] ページの [Nessus スキャン情報] セクションには、次の詳細が表示されます。

- 最後の正常なスキャン
- 最終認証スキャン

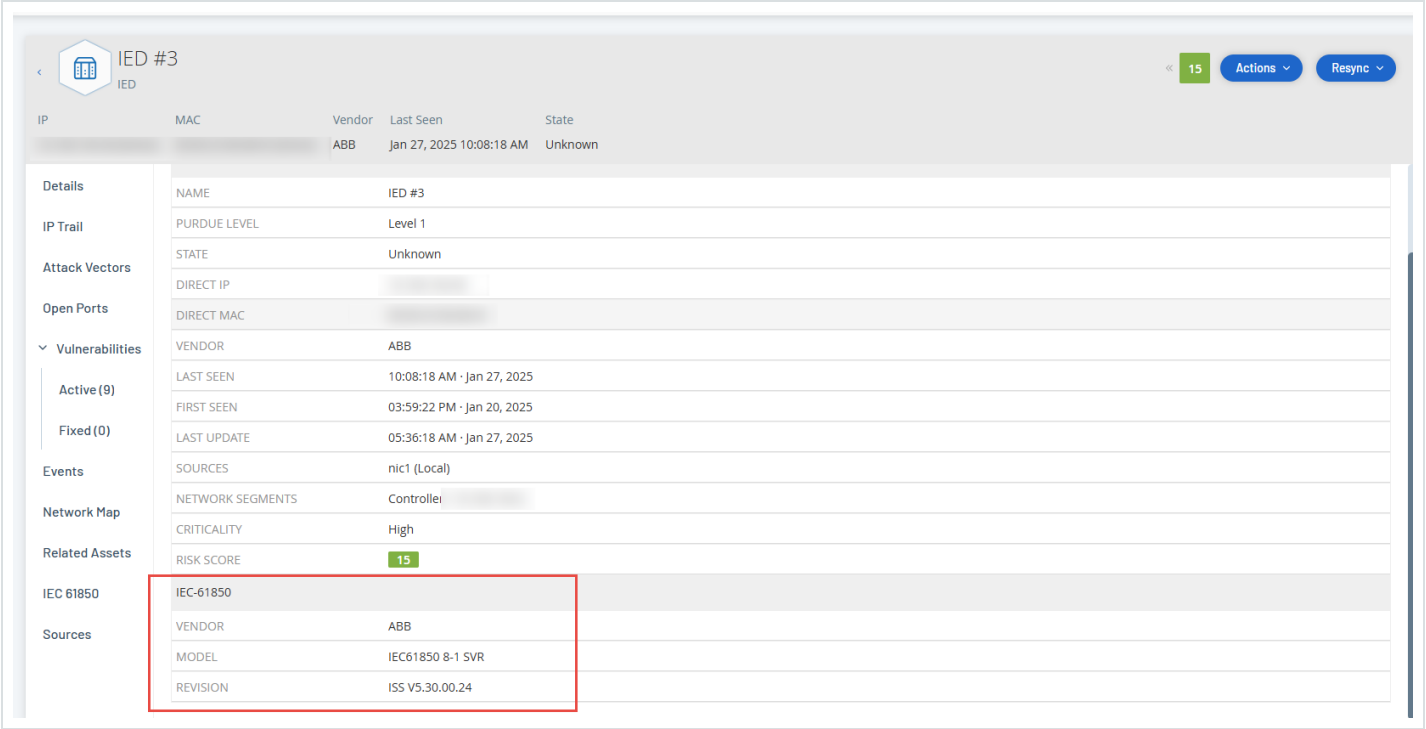
- 最後のスキャン所要時間



IEC 61850

[詳細] ページの IEC 61850 セクションには、特定の IED 資産に関する次の設定が表示されます。

- ベンダー
- モデル
- リビジョン

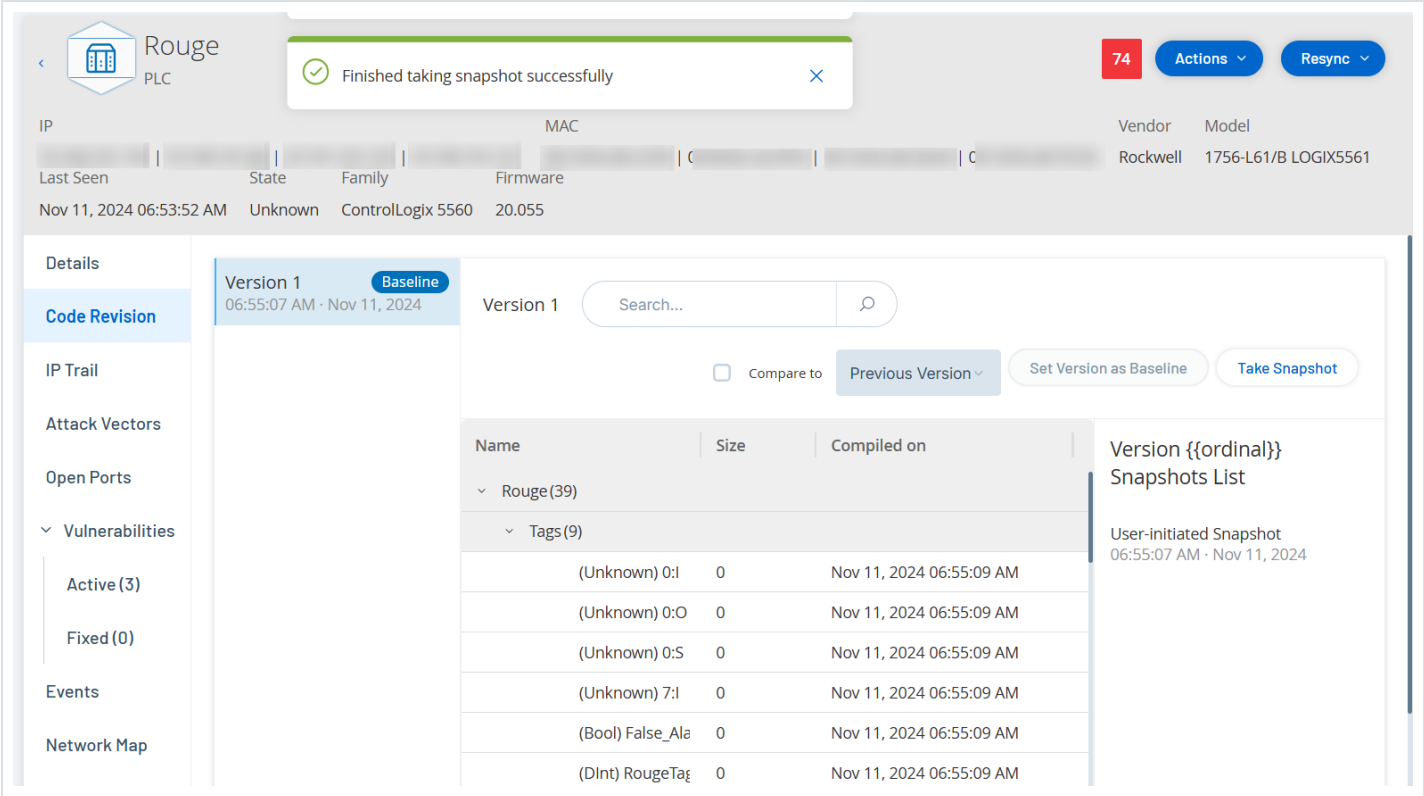


SCD ファイルの詳細については、以下を参照してください。

- SCD ファイル
- IEC 61850

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各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 / ラング) 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。



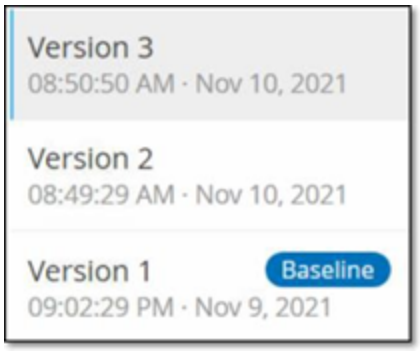
スナップショットは次の方法でトリガーできます。

- 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。

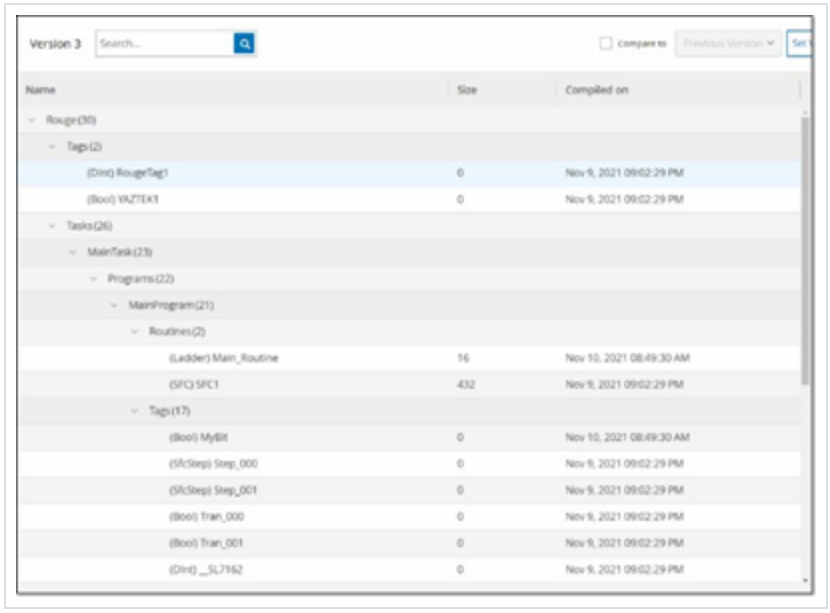
続くセクションでは、コードリビジョン表示のさまざまなセクションと、異なる「スナップショット」バージョンを比較する方法について説明します。

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。

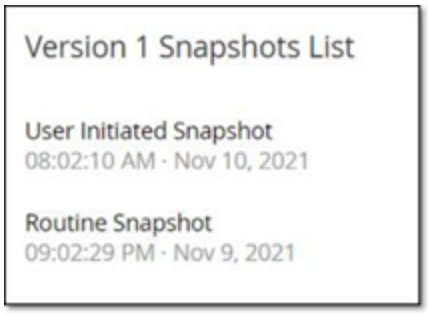
スナップショットの詳細ペイン



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。同一のスナップショットはすべて、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前のバージョンや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。

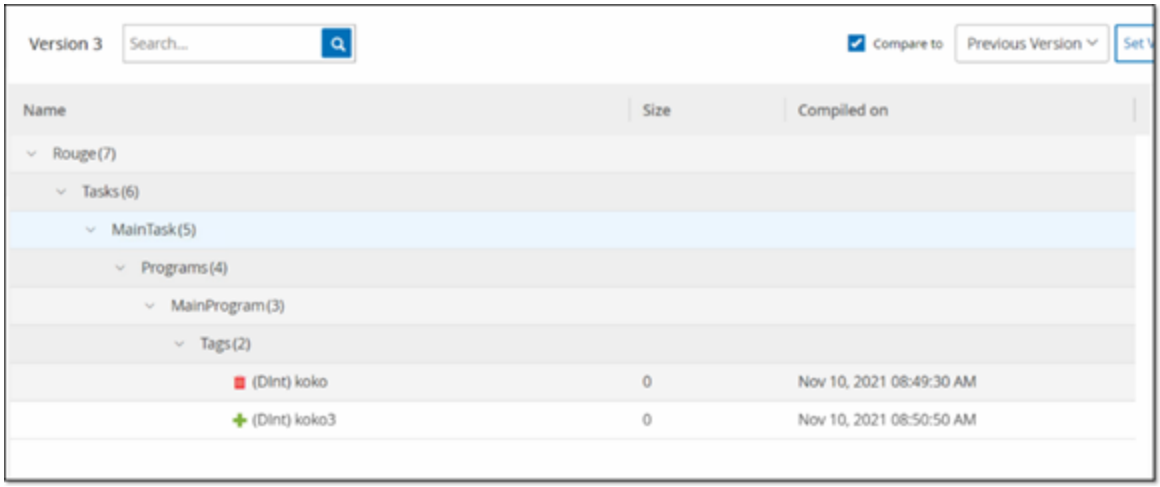
削除済み - 選択したバージョンで削除されたコード。

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. [次と比較:] 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. [次と比較:]チェックボックスをクリックします。
7. [次と比較:]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[ベースラインのバージョン]を選択します。

   [スナップショットの詳細]ペインに、2つのバージョン間のすべての違いが表示されます。変更ごとに、発生した変更のタイプがアイコンで示されます。

スナップショットの作成

スナップショットは手動で開始できます。Tenableは、技術者によるコントローラーの修正作業の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方法

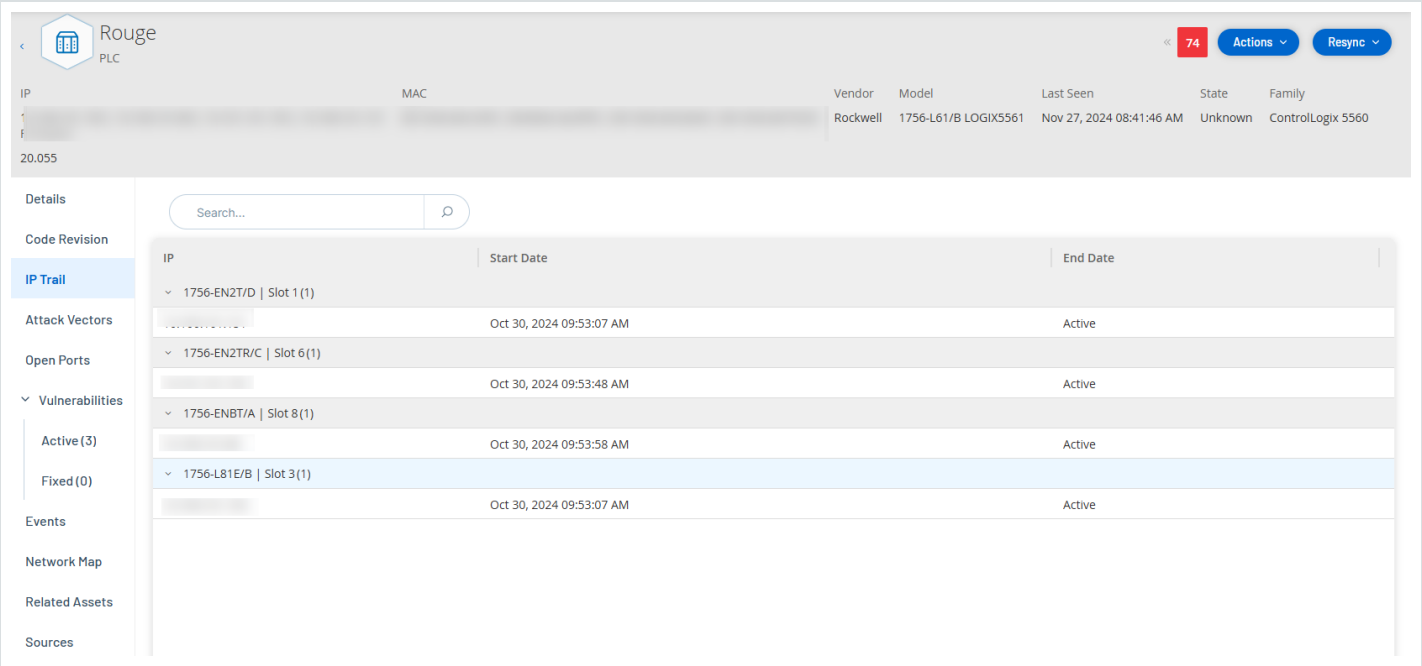
1. [インベントリ] > [コントローラー]画面で、目的のコントローラーを選択します。
2. [コードリビジョン]タブをクリックします。
3. [スナップショットの詳細]ペインの右上にある[スナップショットを作成]をクリックします。

   ユーザーが開始したスナップショットが作成されます。

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。次のパラメーターがあります。

- 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)。

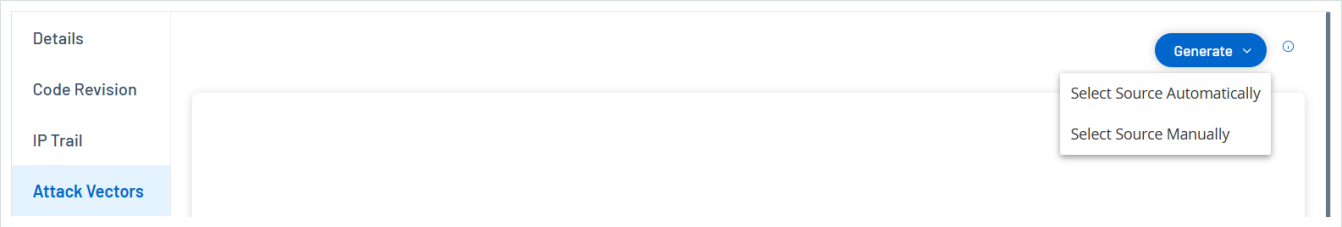
攻撃経路の生成

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。

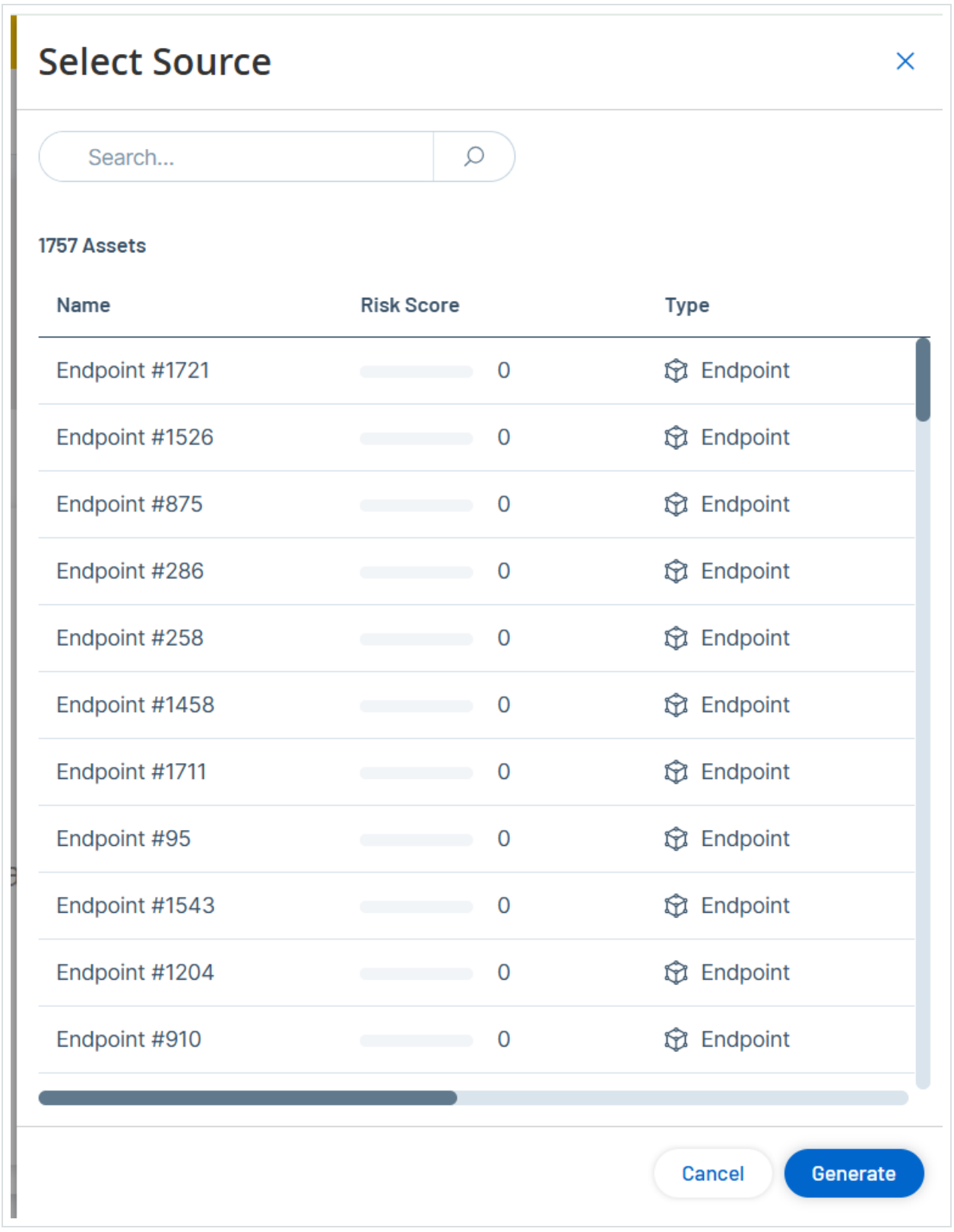


攻撃経路が自動的に生成され、[攻撃経路] タブに表示されます。

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。

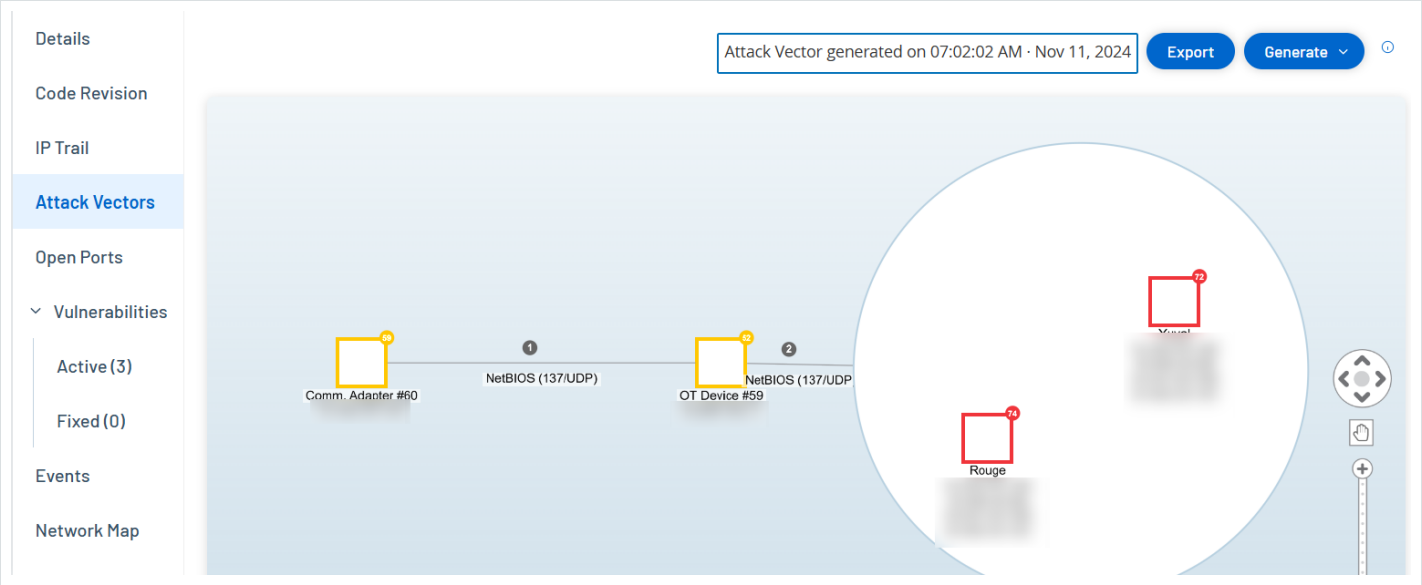

Select Source
Search...
1757 Assets
Name
Risk Score
Type
Endpoint #1721
0
Endpoint
Endpoint #1526
0
Endpoint
Endpoint #875
0
Endpoint
Endpoint #286
0
Endpoint
Endpoint #258
0
Endpoint
Endpoint #1458
0
Endpoint
Endpoint #1711
0
Endpoint
Endpoint #95
0
Endpoint
Endpoint #1543
0
Endpoint
Endpoint #1204
0
Endpoint
Endpoint #910
0
Endpoint
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. 必要な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



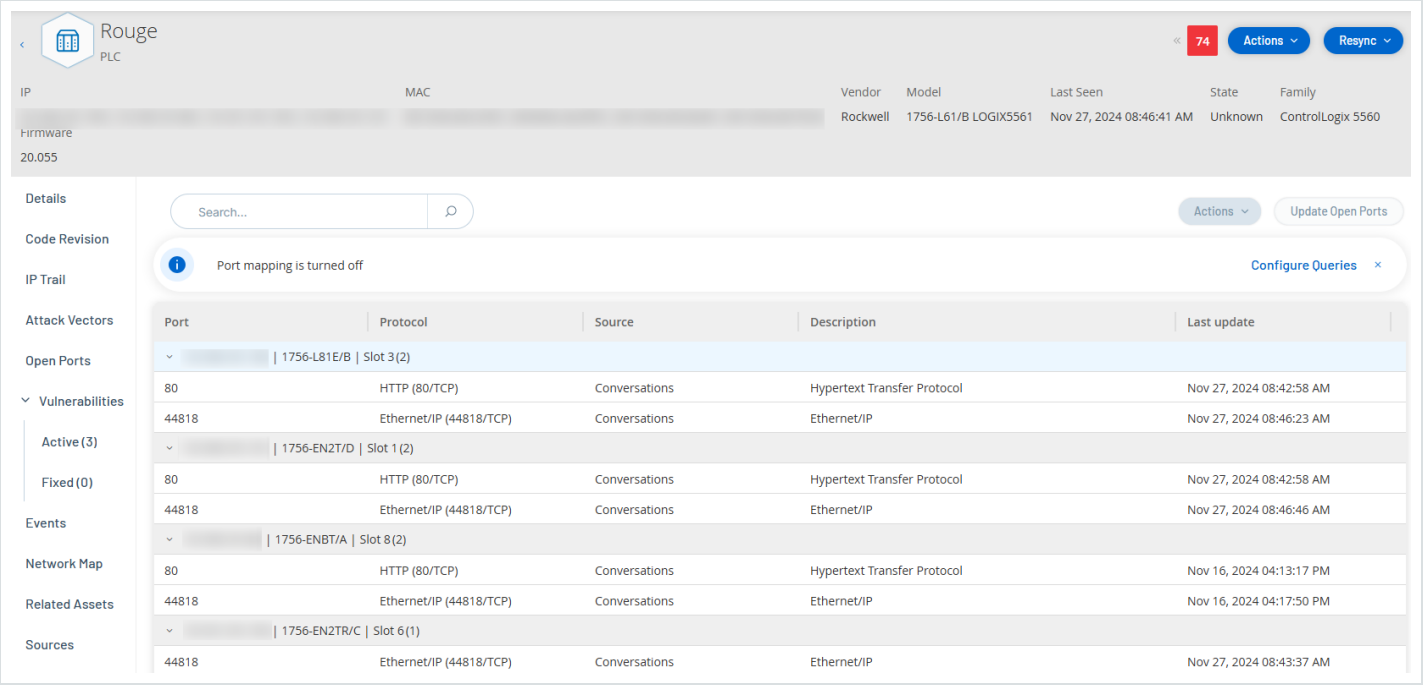
[攻撃経路] タブには、指定されたターゲット資産に対して生成された最も新しい攻撃経路の図が表示されます。[生成] ボタンの横のボックスには、表示された攻撃経路の生成日時が表示されます。攻撃経路の図には、次の要素が含まれます。

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

オープンポート

[オープンポート] タブには、この資産のオープンポートのリストが表示されます。オープンポートごとに、使用するプロトコル、機能の説明、データが最後に更新された日時、ポートが開いていることを示す情報ソース (アクティブクエリ、ポートマッピング、対話、Tenable 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、リストからそのオープン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。選択した資産の手動クエリを実行して、オープンポートのリストを更新することもできます。

オープンポートの更新

必要な OT Security ユーザーロール: 管理者、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

オープンポートのリストの手動更新方法

1. [インベントリ] > [コントローラー / ネックワーク資産] 画面で、目的の資産を選択します。

   [資産詳細] 画面が表示されます。

2. [オープンポート] タブをクリックします。

3. [オープンポート] ペインの右上にある [オープンポートの更新] をクリックします。

   新しいスキャンが実行され、このコントローラーに表示されているオープンポートが更新されます。

[オープンポート] タブのその他のアクション

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

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

スキャンの実行

特定のポートでのスキャンの実行方法

1. [インベントリ] > [コントローラー / ネックワーク資産] 画面で、目的の資産を選択します。

   [資産詳細] 画面が表示されます。

2. [オープンポート] タブをクリックします。

3. 特定のポートを選択します。

4. [アクション] メニューをクリックします。

5. ドロップダウンメニューから、[スキャン] を選択します。

   OT Security は選択されたポートでスキャンを実行します。

資産ポータルの表示

資産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。

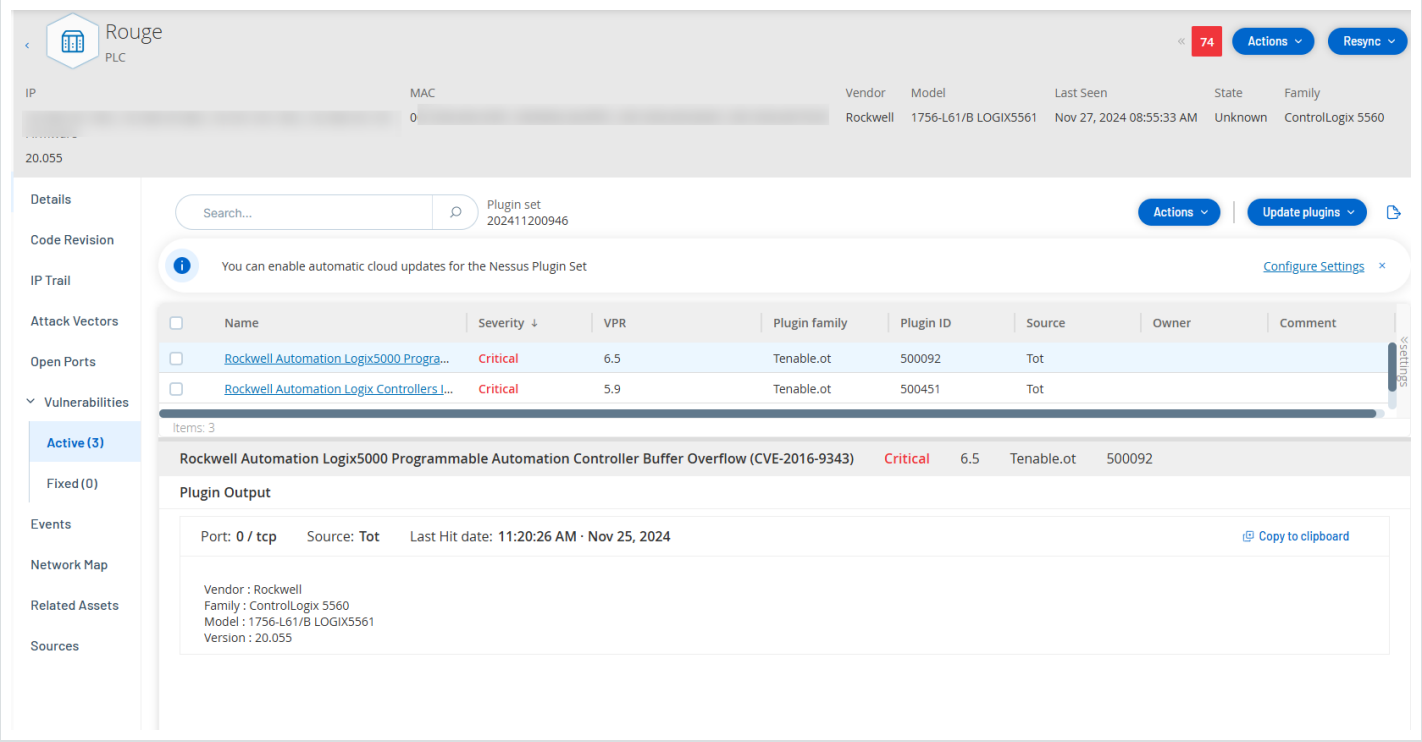
4. [アクション] メニューをクリックします。

5. ドロップダウンメニューから、[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。

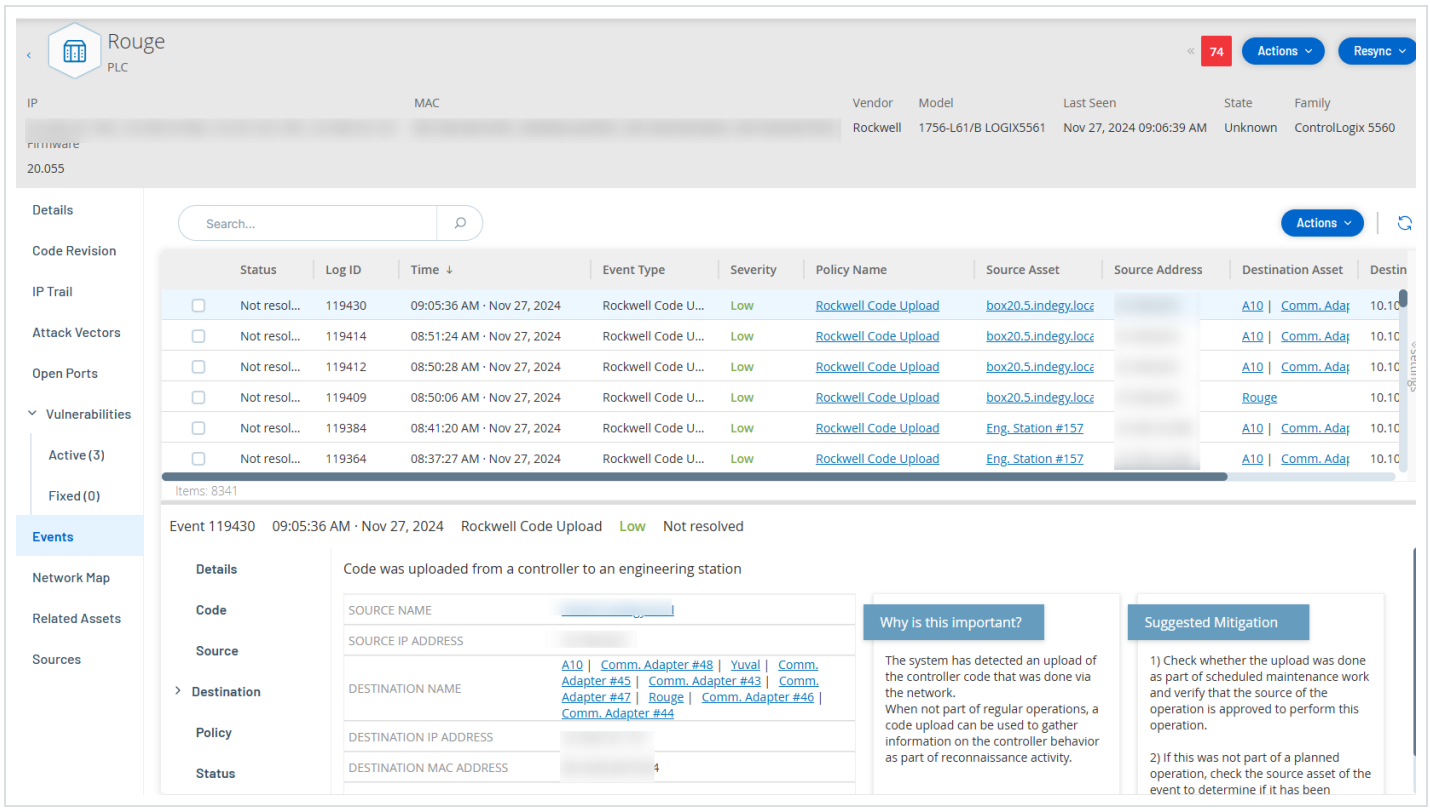
脆弱性

[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、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とオープンな通信ポートなどの脆弱性を特定します。脆弱性は、アクティブと修正済みの 2 つのカテゴリに分けてリストされます。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、指定された資産に関連する脆弱性だけがこのページに表示されることを除いて、[リスク] > [脆弱性] ページ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。



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。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]ボタンがあります。このボタンを使って、選択したイベントに対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。
- キャプチャファイルのダウンロード - このイベントの PCAP ファイルをダウンロードします。
- ポリシーから除外 - 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。

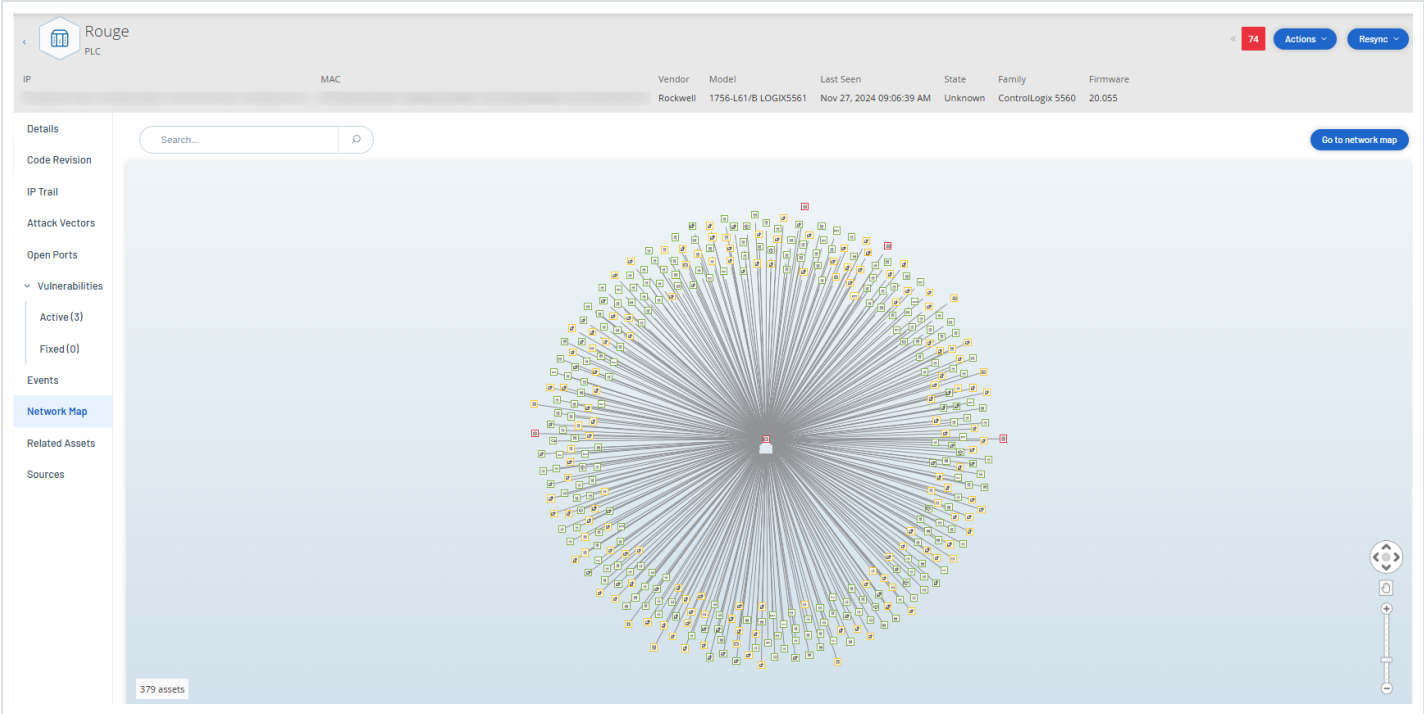
パラメーター	説明
ログ ID	イベントを参照するためにシステムによって生成される ID。
時間	イベントが発生した日時。
イベントタイプ	イベントをトリガーしたアクティビティのタイプの説明。イベントは、システムに設定されているポリシーによって生成されます。さまざまなタイプのポリシーの説明については、ポリシーのタイプを参照してください。
深刻度	イベントの深刻度レベルを表示します。以下は、可能な値の説明です。 • なし - 心配は不要です。 • 情報 - 現時点では心配はありませんが、都合の良いときに確認する必要があります。 • 警告 - 潜在的に害のあるアクティビティが発生したことに対する中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。

パラメーター	説明
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。

パラメーター	説明
	• ネットワーク脅威イベント - これらのポリシーは、侵入の脅威を示すネットワークトラフィックを特定します。 • ネットワークイベント - ネットワーク内の資産および資産間の通信ストリームに関連したポリシーです。
ステータス	イベントが解決済みとしてマークされているかどうかを示します。
解決者	解決済みイベントについて、どのユーザーがイベントを解決済みとしてマークしたかを示します。
解決日	解決済みイベントについて、いつイベントが解決済みとしてマークされたかを示します。
コメント	イベントの解決時に追加されたコメントを表示します。

ネットワークマップ

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



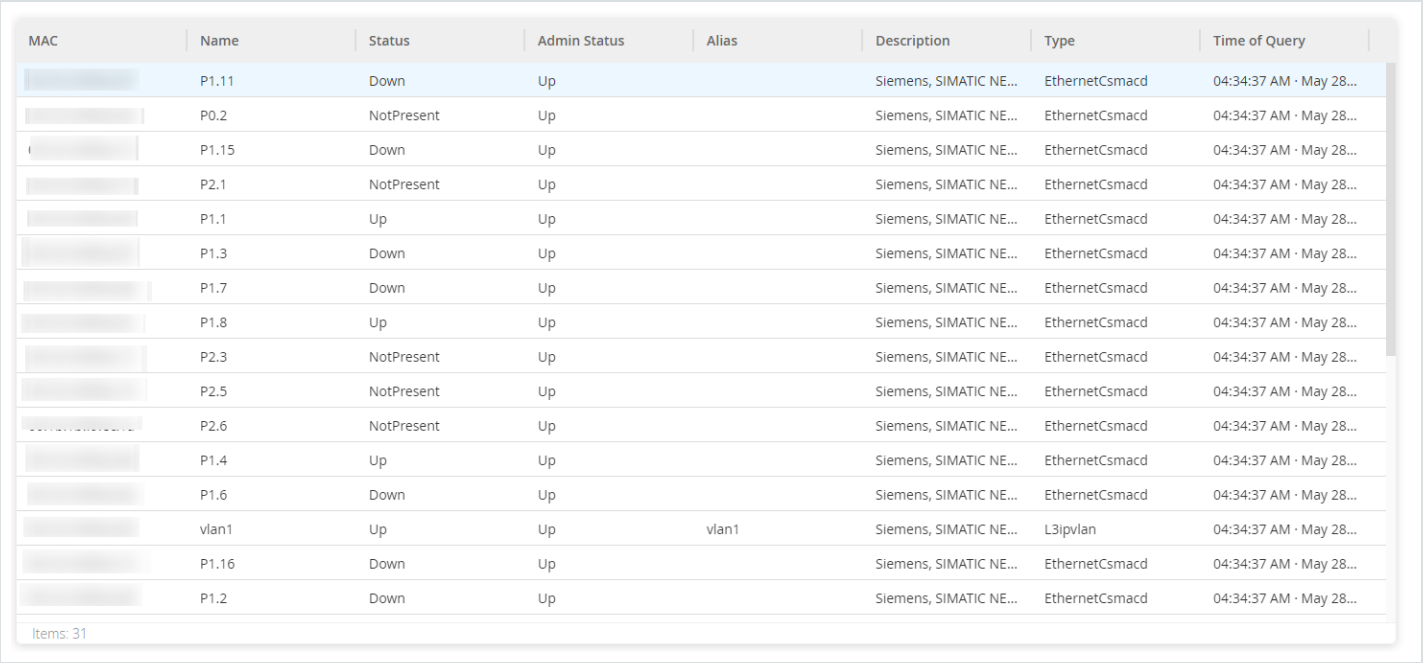
このタブに表示される情報は、[ネットワークマップ] 画面に表示される情報と類似していますが、ここに表示される情報はこの特定の資産に関連する接続に限定されます。また、この画面には、ネットワークマップのメイン画面に示されているような資産のグループへの接続ではなく、個々の資産への接続が表示されます。このタブに表示される情報の説明については、ネットワークマップを参照してください。

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

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

デバイスポート

[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。

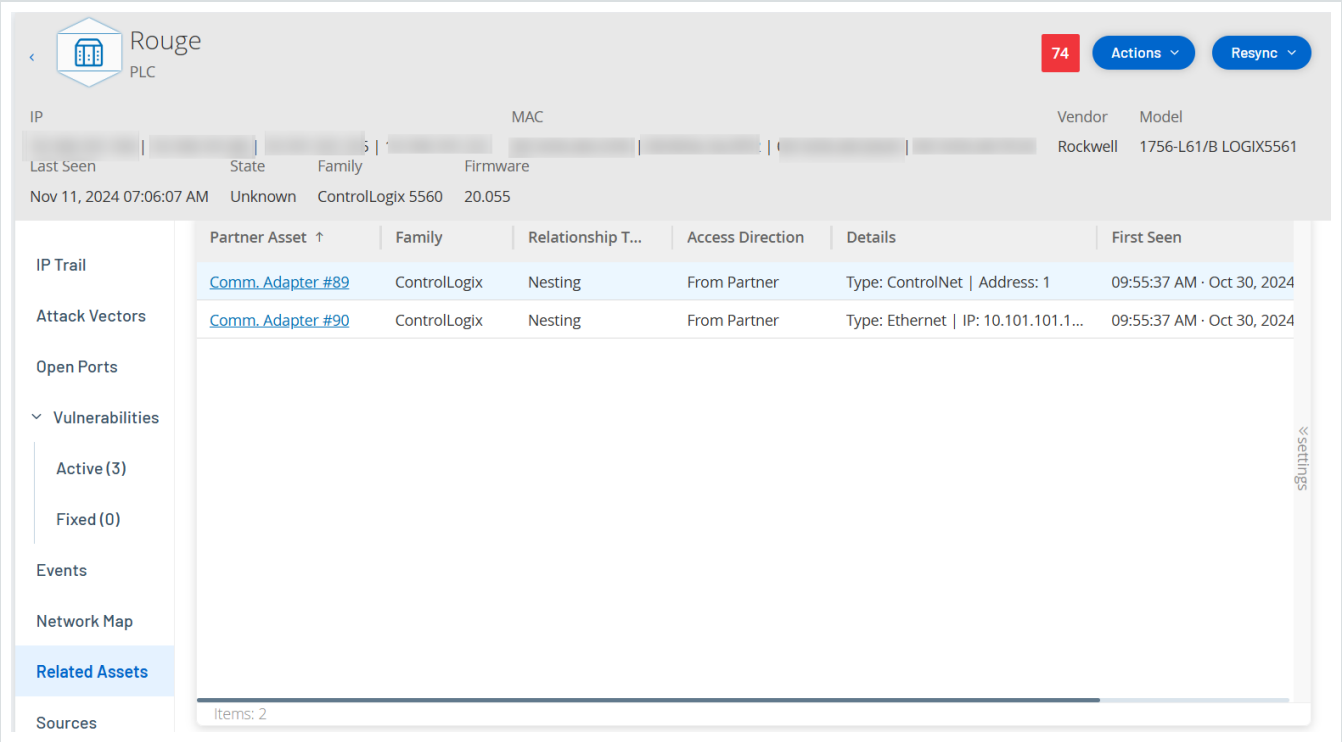
関連資産

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。

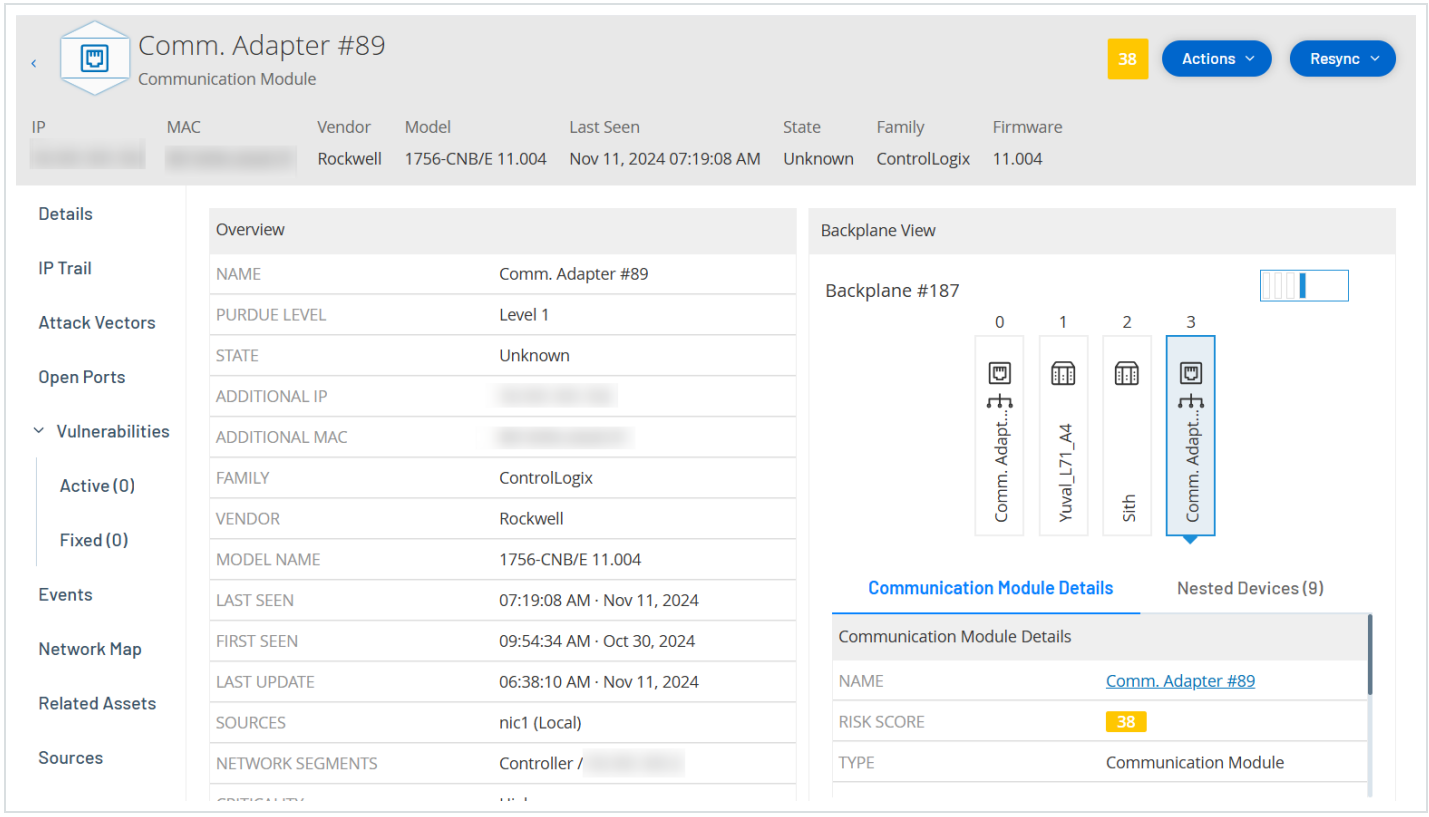


次の詳細を含む [関連資産] ページが表示されます。

縦棒	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。
一般	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	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のデバイス名をク

レーンビュー	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。

IEC 61850

アップロードされた Substation Configuration Description (SCD) ファイルに基づいて、OT Security は製造メッセージ仕様 (MMS) レポートのリストを生成します。これらのレポートは、変電所資産間の通信について説明しています。OT Security は、SCD ファイル設定で認証されていないアクセスを検出すると、エラーメッセージを表示します。SCD ファイルのアップロードの詳細については、SCD ファイルを参照してください。

IEC 61850 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] に移動します。

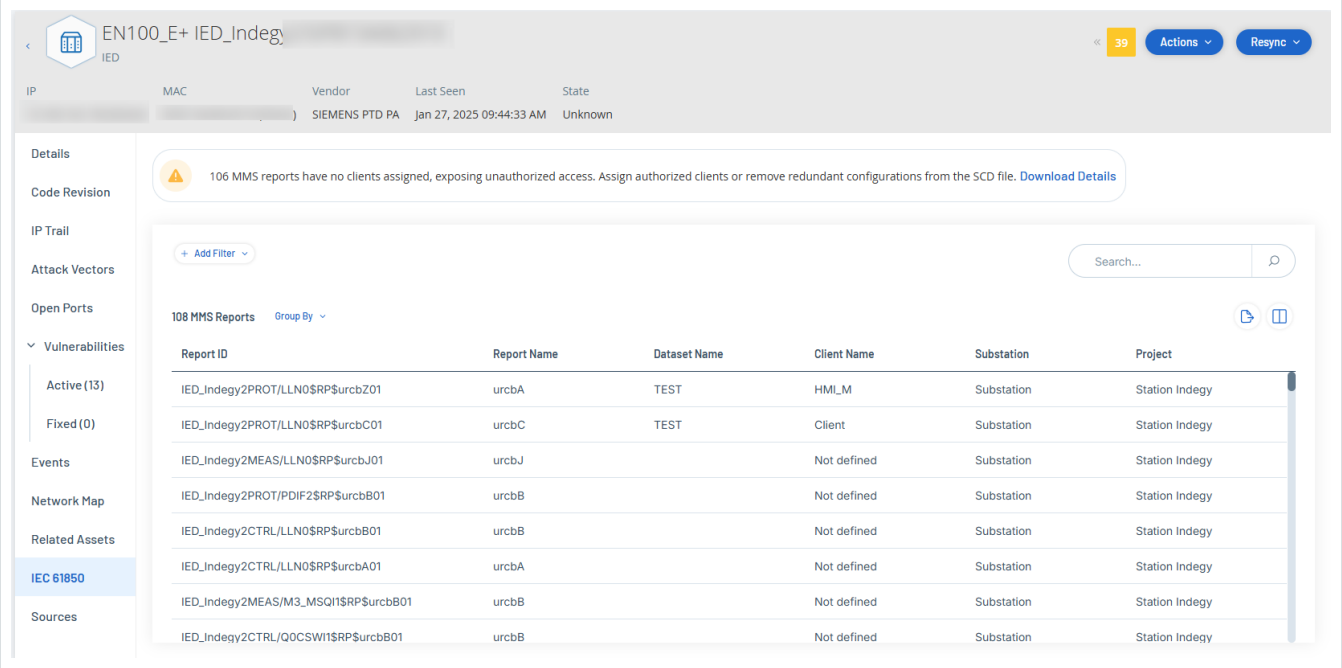
   [すべての資産] ページが表示されます。

2. IEC 61850 設定を表示する対象の資産または変電所を検索して選択します。

   資産の詳細ページが表示されます。

3. 左側のナビゲーションバーで、[IEC 61850] を選択します。

表示された [IEC 61850] ページには、次の詳細が含まれています。

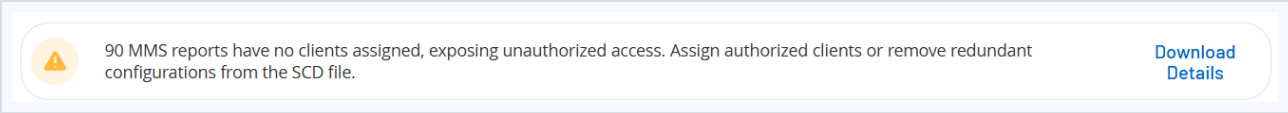


縦棒	説明
レポート ID	レポートの一意の識別子として機能する MMS レポート ID。
レポート名	レポートの一意の識別子として機能する MMS レポート名。
データセット名	レポートに含まれるデータポイントのグループを定義する、MMS レポートにリンクされたデータセットの名前。
クライアント名	レポートをサブスクリプション登録して受信するクライアントアプリケーションまたはシステムの名前。
変電所	MMS レポートを生成する IED (インテリジェント電子デバイス) が設置されている変電所。

プロジェクト	レポートとその関連コンポーネントが属する、包括的な IEC 61850 プロジェクトまたはシステム設定。

4. OT Security が検出した検出結果の詳細を表示する方法: ページ上部にあるエラーメッセージで、[詳細のダウンロード] をクリックします。

   OT Security は詳細を CSV 形式でダウンロードします。

   > **注意: エラーメッセージ内の MMS レポートの数は特定の資産に適用されますが、ダウンロードされた CSV ファイルにはすべての資産の詳細が含まれます。**
   >
   > 
   >

ソース

資産の [ソース] ページには、場所、タイプ、最初と最後に報告された時間など、資産のソースに関連するすべての情報が表示されます。資産のソースは、[インベントリ] > [すべての資産] ページの [ソース] 列でも見ることができます。

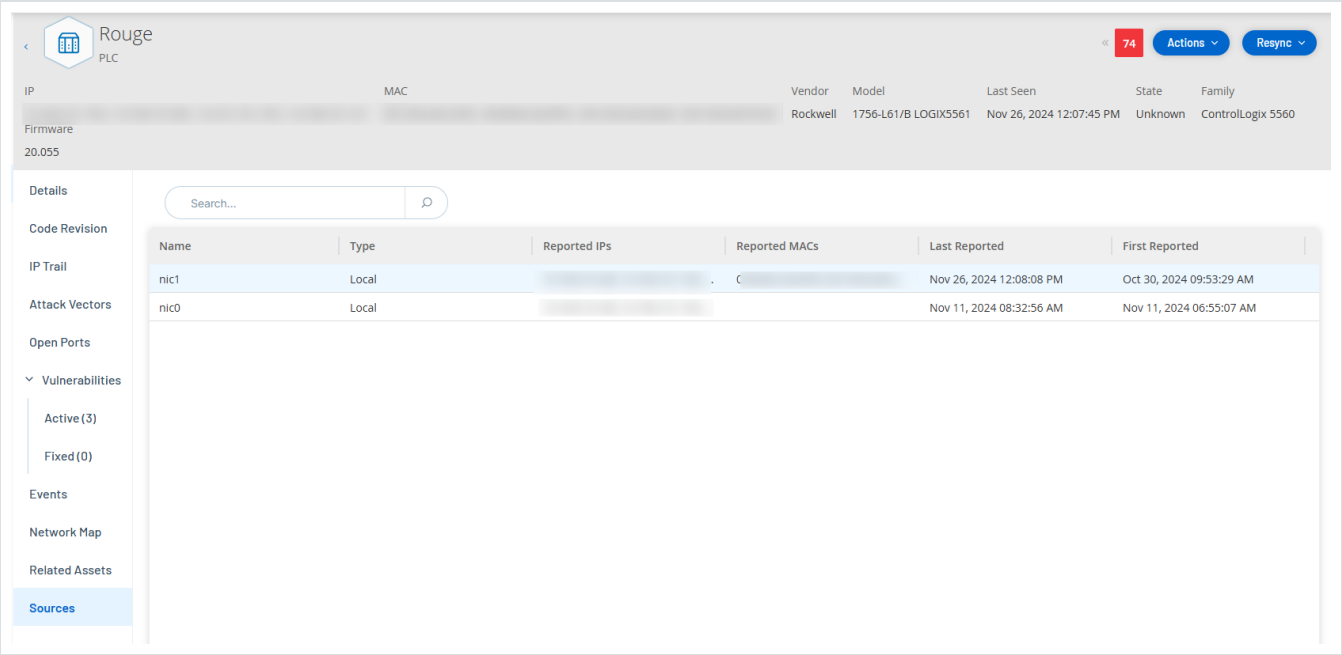
[ソース] ページにアクセスする方法

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。

   資産の詳細ページが表示されます。

2. 左側のナビゲーションペインで [ソース] をクリックします。

[ソース] ページが表 示されます。



[ソース] ページが次 の詳 細とともに表 示されます。

縦棒	説明
名 前	ソースの名 前 (例: ローカルソースの場 合 は nic 1 または nic 2、ソースがセンサーの場 合 はセンサー名)。
タイプ	ソースのタイプ (ローカル ICP またはセンサー)
報 告さ れた IP	ソース資 産 を発 生 元とする IP アドレス。
報 告さ れた MAC	ソース資 産 を発 生 元とする MAC アドレス。センサーが資 産 を観 察 できるほど接 近 した場 合 、OT Security は MAC アドレスを報 告します。センサーが資 産 から遠く離 れていても、センサー間 の会 話 を観 察 している場 合 、OT Security は観 察 された IP アドレスのみを報 告します。
最 後 報 告	ソース資 産 が最 後 に報 告された時 刻 。

初回報告	ソース資産が最初に報告された時刻。

資産詳細の編集

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、サイトオペレーター

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. 必要な資産を選択します。
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] ボックスで、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] ボックスに、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] ボックスに、システムにとってのこの資産の重大度のレベルを入力します。
8. [パデューレベル] ボックスに、資産タイプに応じたパデューレベルを入力します。

9. [バックプレーン] ボックス (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] ボックスに、資産の場所の説明を入力します。これは任意のフィールドです。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] ボックスに、資産の説明を入力します。これは任意のフィールドです。データは、この資産の [資産詳細] ページに表示されます。

12. [保存] をクリックします。

    OT Security により、編集された詳細が保存されます。

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。

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] でフィルターしてから、一括編集する資産を選択してください。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] フィールドに入力した情報は、選択された資産の現在の内容をすべてオーバーライドします。パラメーターの横のチェックボックスを選択し、選択内容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。

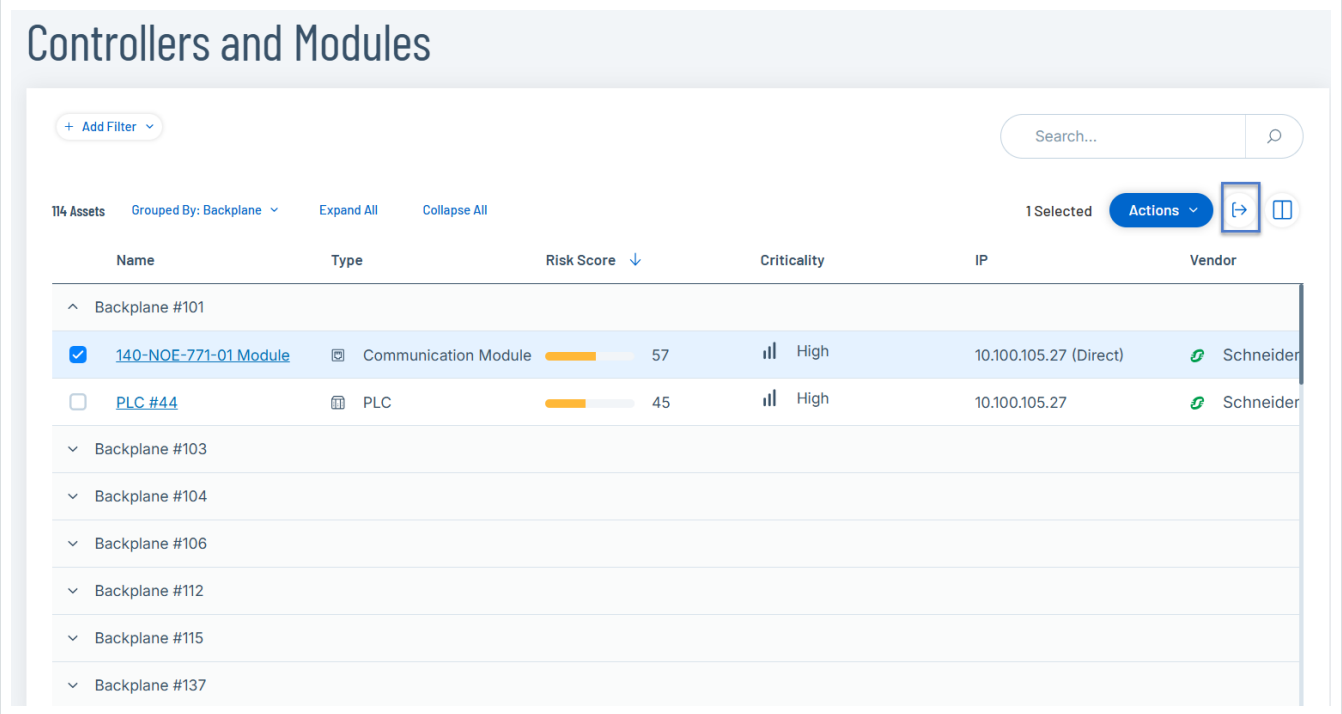
   OT Security により、新しい設定でポリシーが保存されます。

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。

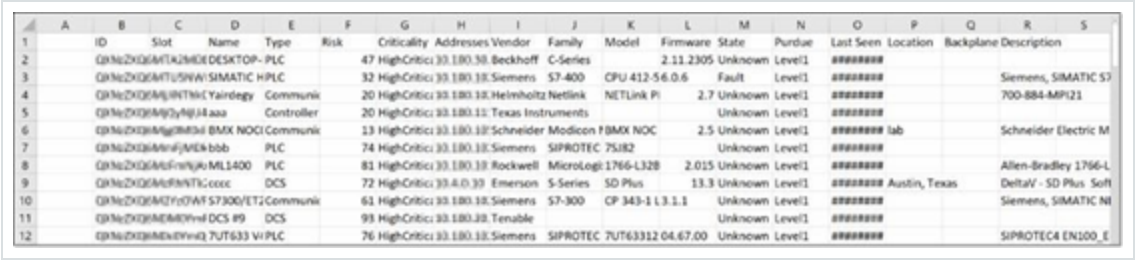
CSV で資産詳細を編集する手順

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]、[ネットワーク資産] のいずれかをクリックします。
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。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1		ID	Slot	Name	Type	Risk	Criticality	Addresses	Vendor	Family	Model	Firmware	State	Purdue	Last Seen	Location	Backplane	Description	
2		[illegible]		DESKTOP-	PLC		47 High	10.180.50.	Beckhoff	C-Series		2.11.2305	Unknown	Level1	########				
3		[illegible]		SIMATIC H	PLC		32 High	10.180.10.	Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	########			Siemens, SIMATIC S7	
4		[illegible]		Yairdegy	Communic		20 High	10.180.10.	Helmholtz	Netlink	NETLink PI	2.7	Unknown	Level1	########			700-884-MPI21	
5		[illegible]		aaa	Controller		20 High	10.180.11.	Texas Instruments				Unknown	Level1	########				
6		[illegible]		BMX NOCI	Communic		13 High	10.180.10.	Schneider	Modicon F	BMX NOC	2.5	Unknown	Level1	########	lab		Schneider Electric M	
7		[illegible]		bbb	PLC		74 High	10.180.10.	Siemens	SIPROTEC	7SJ82		Unknown	Level1	########				
8		[illegible]		ML1400	PLC		81 High	10.180.10.	Rockwell	MicroLogi	1766-L32B	2.015	Unknown	Level1	########			Allen-Bradley 1766-L	
9		[illegible]		cccc	DCS		72 High	10.4.0.10	Emerson	S-Series	SD Plus	13.3	Unknown	Level1	########	Austin, Texas		DeltaV - SD Plus Soft	
10		[illegible]		S7300/ET2	Communic		61 High	10.180.10.	Siemens	S7-300	CP 343-1 L	3.1.1	Unknown	Level1	########			Siemens, SIMATIC NI	
11		[illegible]		DCS #9	DCS		93 High	10.180.10.	Tenable				Unknown	Level1	########				
12		[illegible]		7UT633 V4	PLC		76 High	10.180.10.	Siemens	SIPROTEC	7UT63312	04.67.00	Unknown	Level1	########			SIPROTEC4 EN100_E	

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。

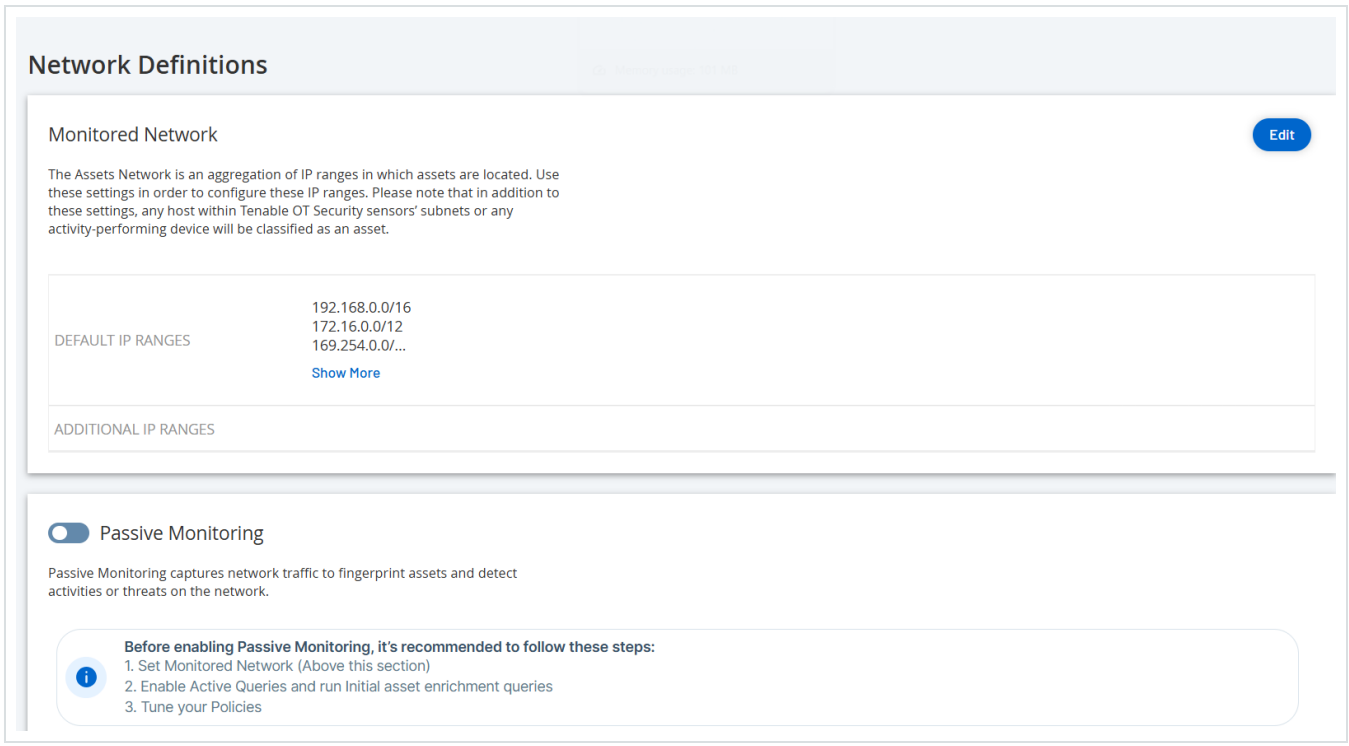
   > 注意: 特定のオプションを必要とするパラメーター (タイプ、重大度、パデューレベルなど) には有効なデータを入力する必要があります。有効なデータでない場合、対応する資産は更新されません。

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. 設定] で、[環境設定] > [ネットワーク定義] に移動します。

   [ネットワーク定義] ページが表示されます。



7. [CSV を使用した資産詳細の更新] セクションで、[アップロード] をクリックします。
8. デバイスのナビゲーションプロンプトに従って、保存したばかりの csv ファイルをアップロードします。

   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 を使用した資産詳細の更新] 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 を使用した資産詳細の更新] セクションで、[レポートのダウンロード] をクリックします。

   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。

非表示の資産の復元は、設定] > [環境**設定]** > [非表示の資産] ページからできます。

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、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 により、[インベントリ] ページと [グループ] ページで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。それぞれのニーズに応じて、資産インベントリから直接、または Tenable Core 管理インターフェースから診断をプルできます。

資産診断レポートのエクスポート

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、さらに分析するために Tenable サポート に共有します。

Tenable OT Security 診断レポートのエクスポート (Tenable Core)

トラブルシューティングのために、Tenable Core から Tenable OT Security 固有の診断レポートを生成してエクスポートすることができます。

始める前に

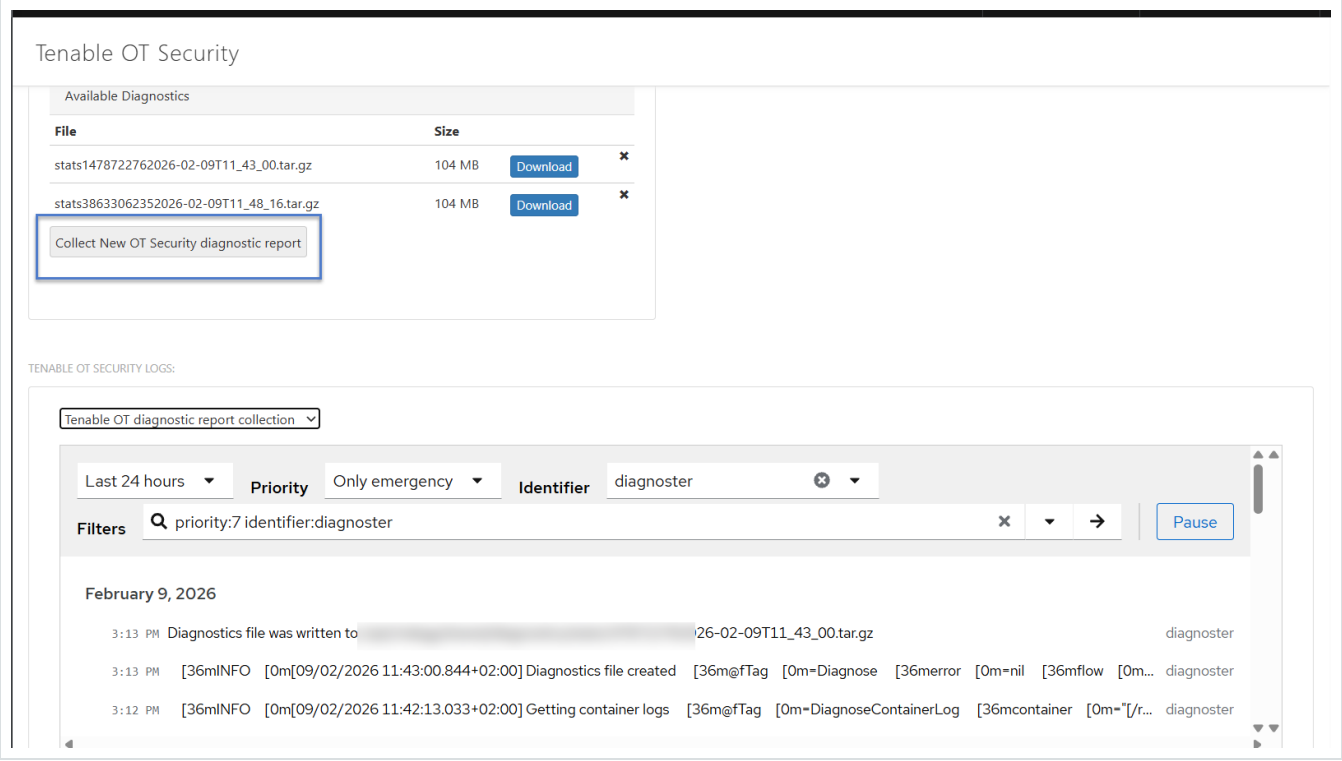
- 管理者アクセスがあることを確認してください。

診断レポートを生成する方法

1. Tenable Core にログインします。
2. 左側のナビゲーションバーで [**Tenable OT Security**] をクリックします。

   [**Tenable OT Security**] ページが表示されます。
3. [OT 診断] セクションで、[新しい OT セキュリティ診断レポートの収集] をクリックします。

   システムにより診断レポートが生成されます。



4. ダウンロードするレポートの横にある [ダウンロード] をクリックします。

   Tenable Core によりレポートがシステムにダウンロードされます。Tenable Core がログを生成した後、データがデバッグログに表示されるまでに数分かかる場合があります。

資産のマージ

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、サイトオペレーター

ネットワーク内のデバイスが、OT Security で 2 つ以上の別々の資産として表示される場合があります。これは、パッシブトラフィックの観察、ルーティング設定、資産情報の不足などにより、内部で資産を自動的にマージできないことが原因です。

たとえば、ワークステーション、サーバー、コントローラーなどのマルチホーム型デバイスには通常、さまざまなネットワーク間で通信できるように複数の IP アドレスがあります。または、スイッチ、ルーター、ファイヤーウォールの仮想ネットワークインターフェースも考えられます。これらは 1 つの物理ネットワークデバイスの仮想的な拡張であるにもかかわらず、それぞれが異なる資産として登録される可能性があります。

そのような場合、[資産のマージ] オプションを使用して 2 つの資産をマージし、重複を削除できます。このオプションには、[インベントリ] ページまたは 1 つの資産の詳細ページからアクセスできます。

> 注意: このアクションは元に戻すことができません。

資産をマージする方法

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

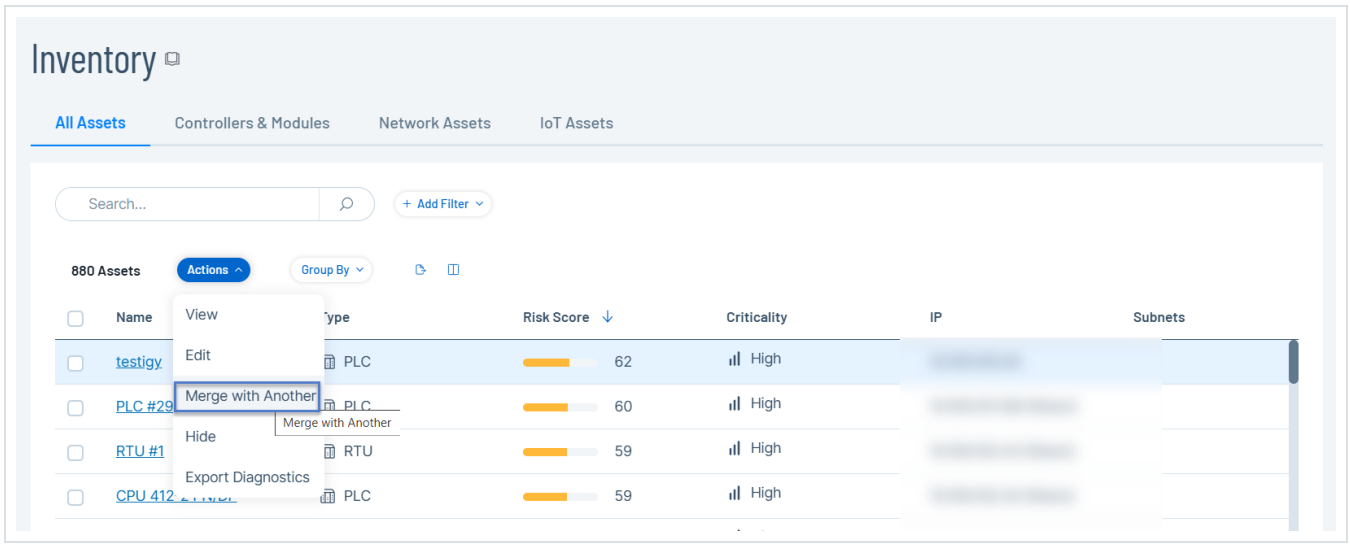
   [すべての資産] ページが表示されます。

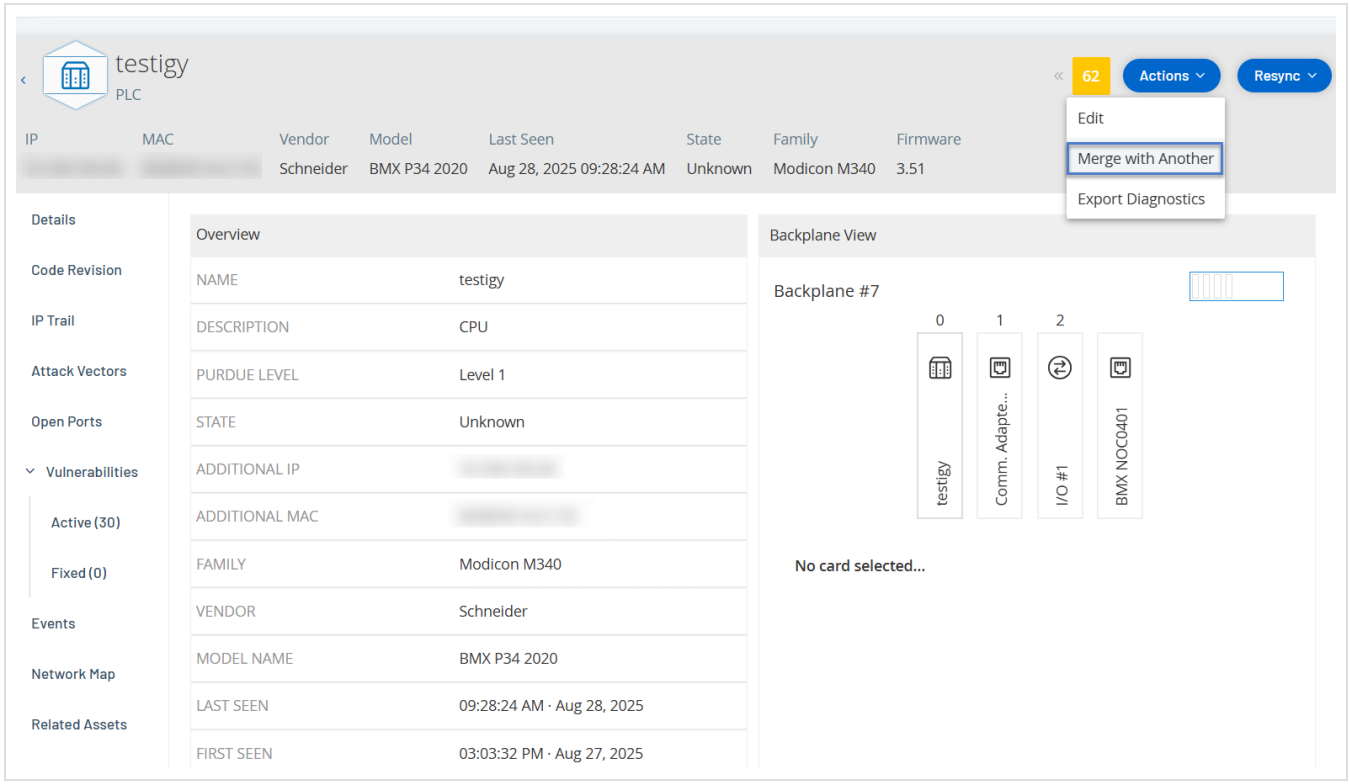
2. [すべての資産] テーブルで、次のいずれかを行います。

   - マージするターゲット資産を選択します。
   - 資産リンクをクリックして、[資産の詳細] ページを開きます。

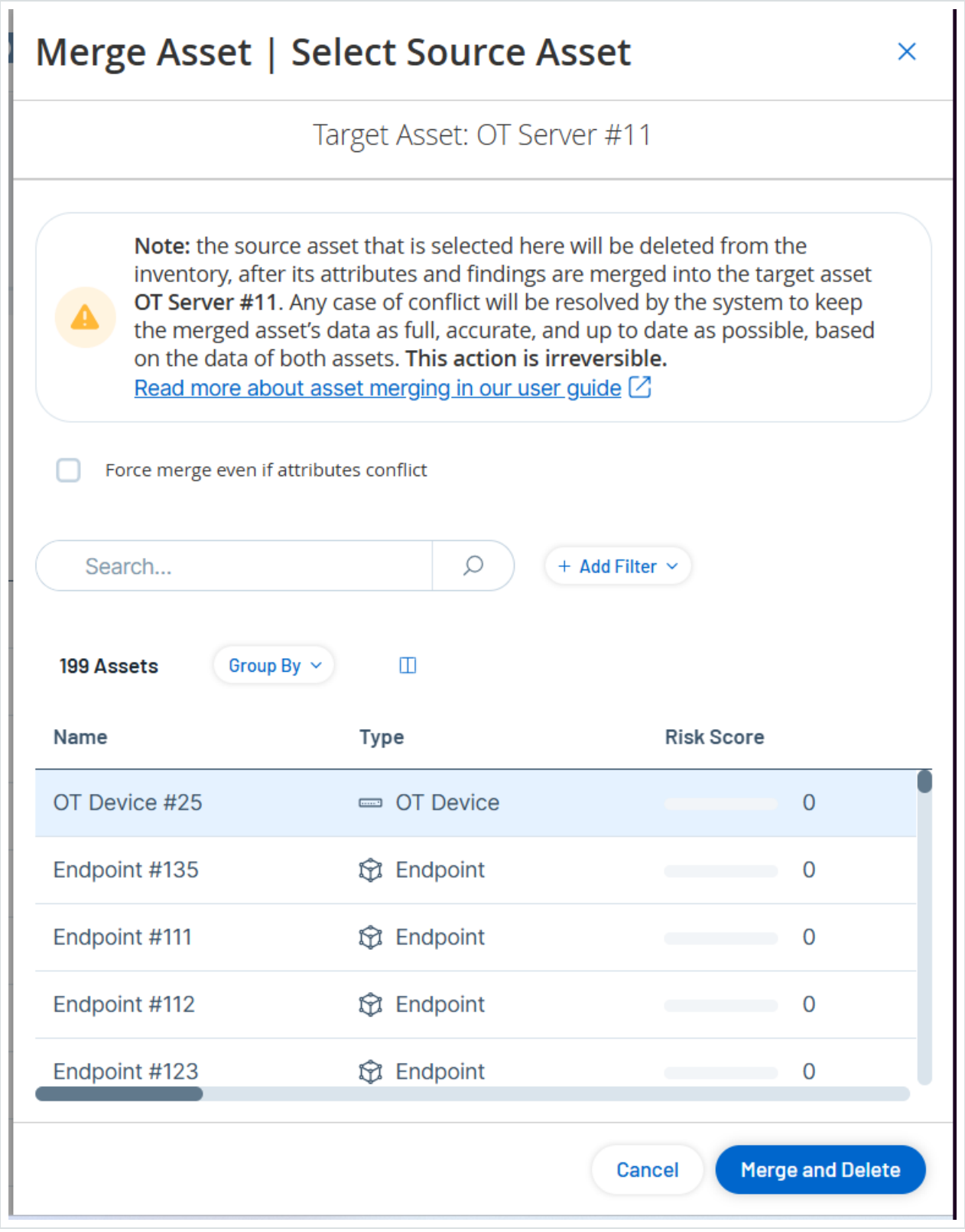
   OT Security で [アクション] が有効になります。

3. [アクション] > [別の資産とマージ] をクリックします。





[資産のマージ | ソース資産の選択] パネルが表示されます。



4. ソース資 産をフィルタリングまたは検 索します。

5. ターゲット資産とマージするソース資産を選択します。
6. (オプション) [属性が競合する場合でも強制的にマージする] チェックボックスを選択すると、競合を無視してマージできます。
7. [マージして削除] をクリックします。

   OT Security でソース資産が削除され、その属性と検出結果がターゲット資産にマージされます。

資産をマージすると起きること

資産マージプロセスでは、システム全体のデータの整合性を維持しながら、2 つの資産を 1 つのエンティティに結合します。

この操作には、次の主な段階が含まれます。

- 資産プロパティの統合: 資産がマージされると、そのプロパティはデスティネーション資産にマージされます。同じプロパティに対して両方の資産の値が異なる場合、システムは優先順位のメカニズムを使用して、どちらの値を保持するかを決定します。これにより、マージされた資産に最も正確または最新の情報が保持されます。
- 接続の保持: 以前にどちらかの資産に紐づいていたネットワーク接続は、マージ後の資産を参照するようになります。これには次のものが含まれます。
  - 他のデバイスへの直接接続
  - バックプレーン内のスロットベースの接続
  - IP アドレスと MAC アドレスを含む、ネットワークインターフェースのマッピング。システムは、過去のすべてのアドレス情報を保持し、重複するエントリを削除します。
- 検出結果の統合: システムは、すべての検出結果、脆弱性、セキュリティイベントをマージ後の新しい資産の下に統合します。これにより、完全なセキュリティ履歴が維持されます。

マージの競合と強制マージ

次の資産はマージできません。

- ICP、センサー、ブロードキャスト資産などの特殊な資産
- 異なるバックプレーンに属する資産 (そのうちの 1 つだけがバックプレーンを持つことが許可されます)
- 異なるスロットを持つ資産 (両方の資産にスロットがある場合は同じスロットであることが必要です)
- 異なるシリアル番号を持つ資産

強制マージ: [強制マージ] チェックボックスを選択すると、バックプレーン、スロット、シリアルの競合に関するシステムのチェックがバイパスされます。このオプションを使っても、必ずしもマージが成功するわけではありません。マージエンジンが無効な操作をブロックする可能性はありますが、システムはブロックされる前にマージを続行します。

誤ってマージした場合の修正方法

誤って資産をマージしてしまった場合や、両方の資産をマージ前の状態に戻したい場合は、資産を削除します。削除することで、システムはマージ前の個々の資産を再検出できます。OT Security から単一の資産または資産グループを削除する方法については、このナレッジベースの記事を参照してください。

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。

OT Security の Nessus スキャンは、Tenable Nessus、Tenable Security Center、Tenable Vulnerability Management の基本ネットワークスキャンと同じポリシー設定を使用します。唯一の違いは、OT Security

のパフォーマンスオプションです。以下は、OT Security の Nessus スキャンのパフォーマンスオプションです。これらのオプションは、[アクティブクエリ管理] ページから起動する [Nessus スキャン] にも適用されます。

- 同時に存在するホスト 5 個 (最大)
- ホストあたりの同時チェック 2 件 (最大)
- ネットワーク読み取りのタイムアウト 15 秒

> 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

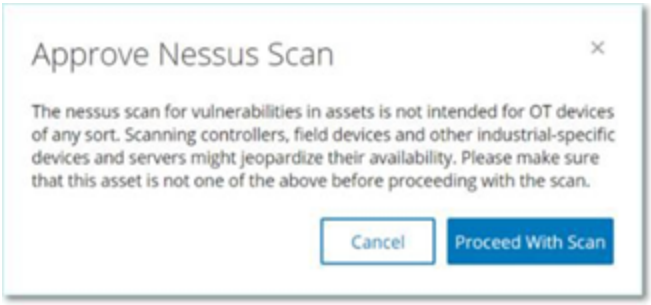
1. [インベントリ] > [ネットワーク資産] に移動します。

   [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

必要な OT Security ユーザーロール: 管理者、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

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。

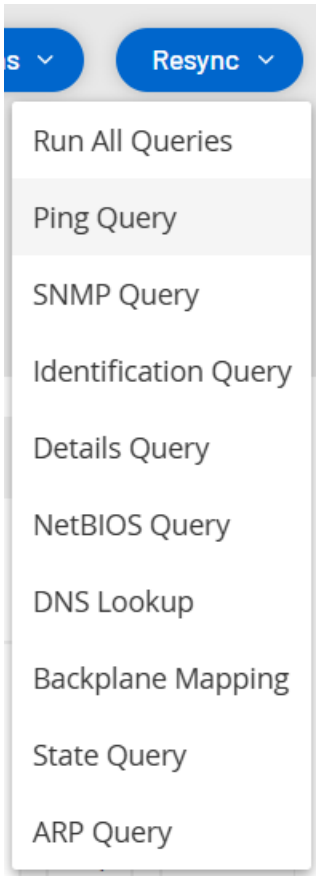
- デバイスに到達できないか、使用できるクエリがない
- アクティブクエリページで設定されたアクセス許可により、管理者以外のアカウントによる特定のクエリの開始が制限されている可能性がある
- この OT Security デプロイメントでは、クエリが有効になっていない

- [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

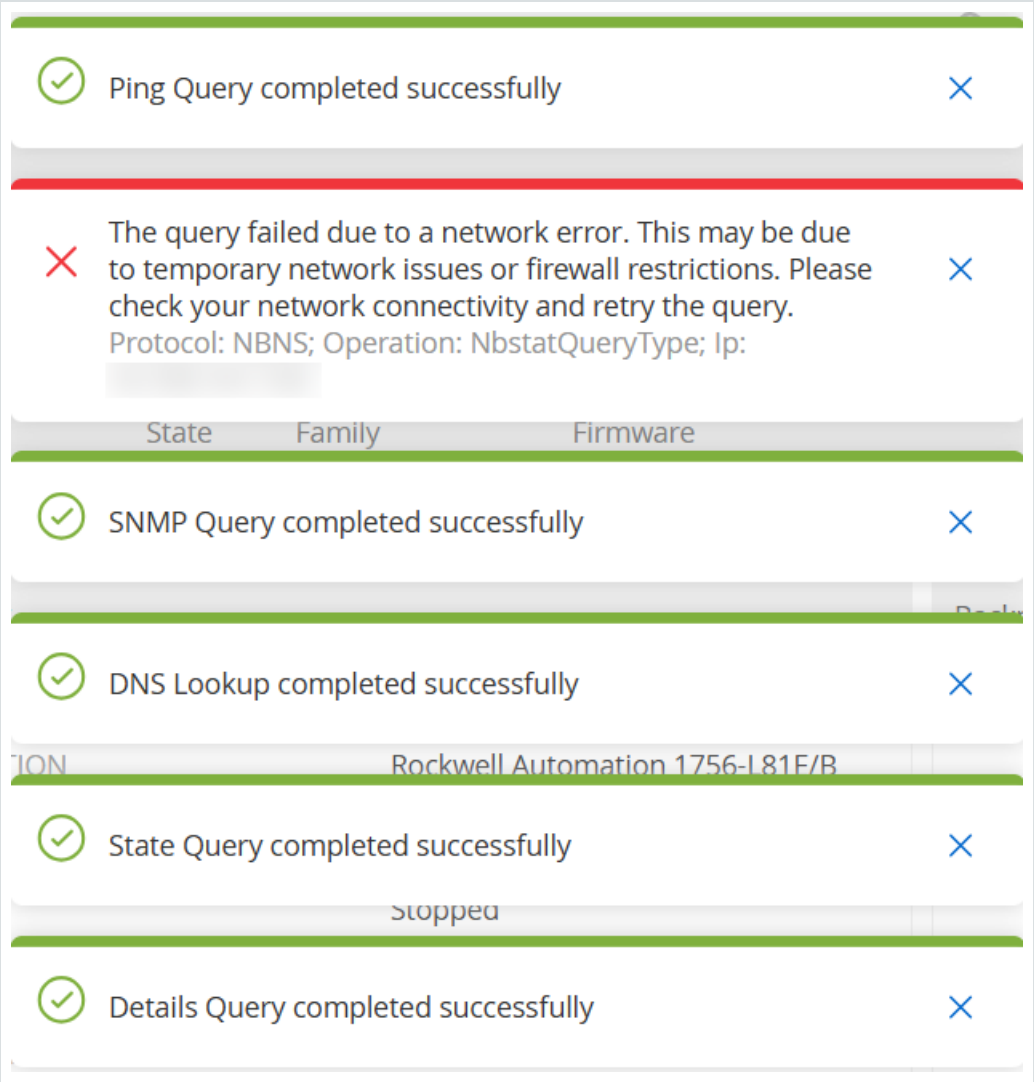
1. 必要な資産の [資産詳細] ページで、右上にある [再同期] をクリックします。

   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 は新しいデータに基づいてその資産のシステムデータを更新します。

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 リサーチスタッフは 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、プラグインと呼ばれ、Tenable Nessus Attack Scripting Language (NASL) という 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 (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) を検出します。

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。

脆弱性の表示

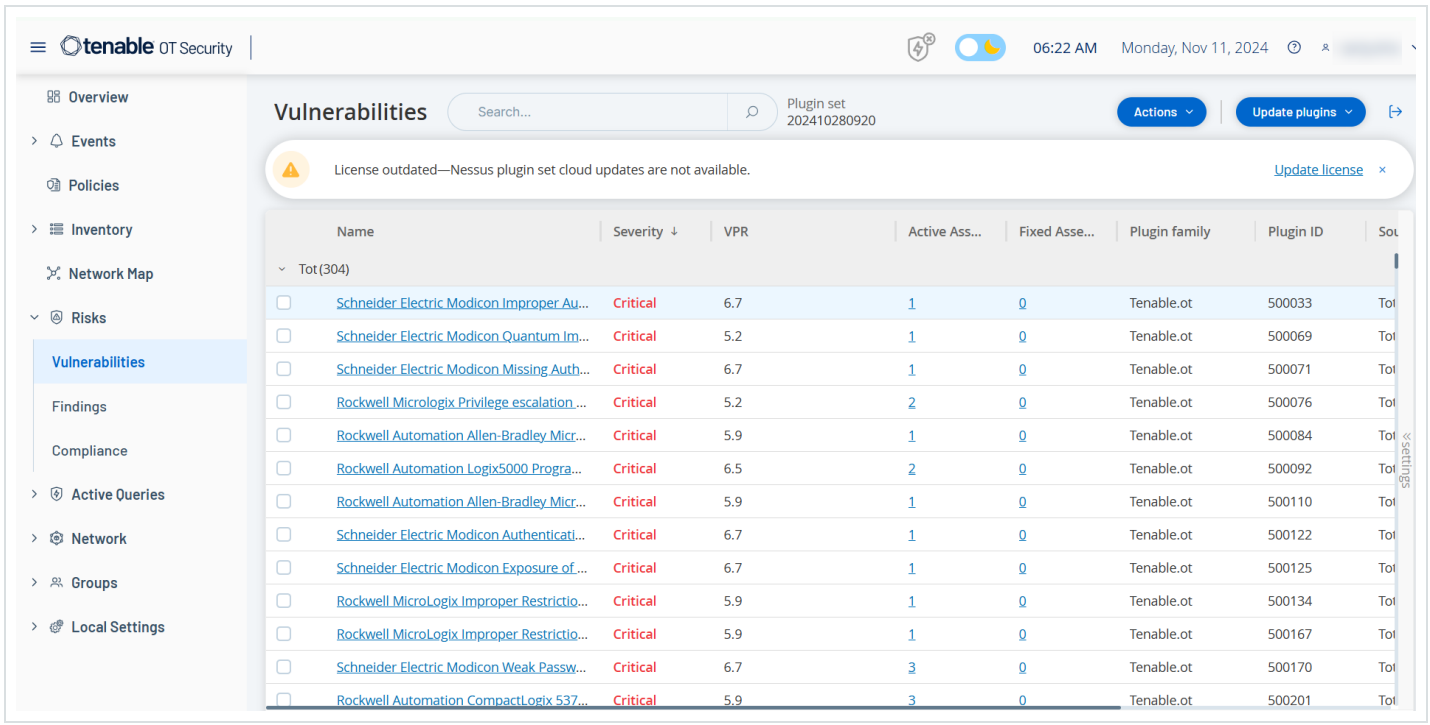
必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー、セキュリティアナリスト、サイトオペレーター、読み取り専用

[脆弱性] ページには、Tenable プラグインによって検出され、ネットワークと資産に影響を及ぼしている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。

(バージョン 3.19 のみ) 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) 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。

アクティブ資産	現在この脆弱性の影響を受けているネットワーク内の資産の数。
修正資産	定義された期間 (デフォルトでは 1 年) において、この脆弱性の影響を受け、最近修正されたネットワーク内の資産の数。この期間をカスタマイズするには、Tenable サポート に連絡してください。
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てい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

必要な OT Security ユーザーロール: 管理者、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

脆弱性の詳細を編集する手順

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人の名前を入力します。

5. [保存] をクリックします。

プラグイン出力の表示

資産のプラグイン出力で、資産で特定のプラグインが報告された理由に関する背景や説明を見ることができます。

脆弱性からのプラグイン出力の表示

[脆弱性] ページからプラグイン出力の詳細を表示する方法

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あるわけではありません。

インベントリからのプラグイン出力の表示

[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方法

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。

   [資産の詳細]ページが表示されます。

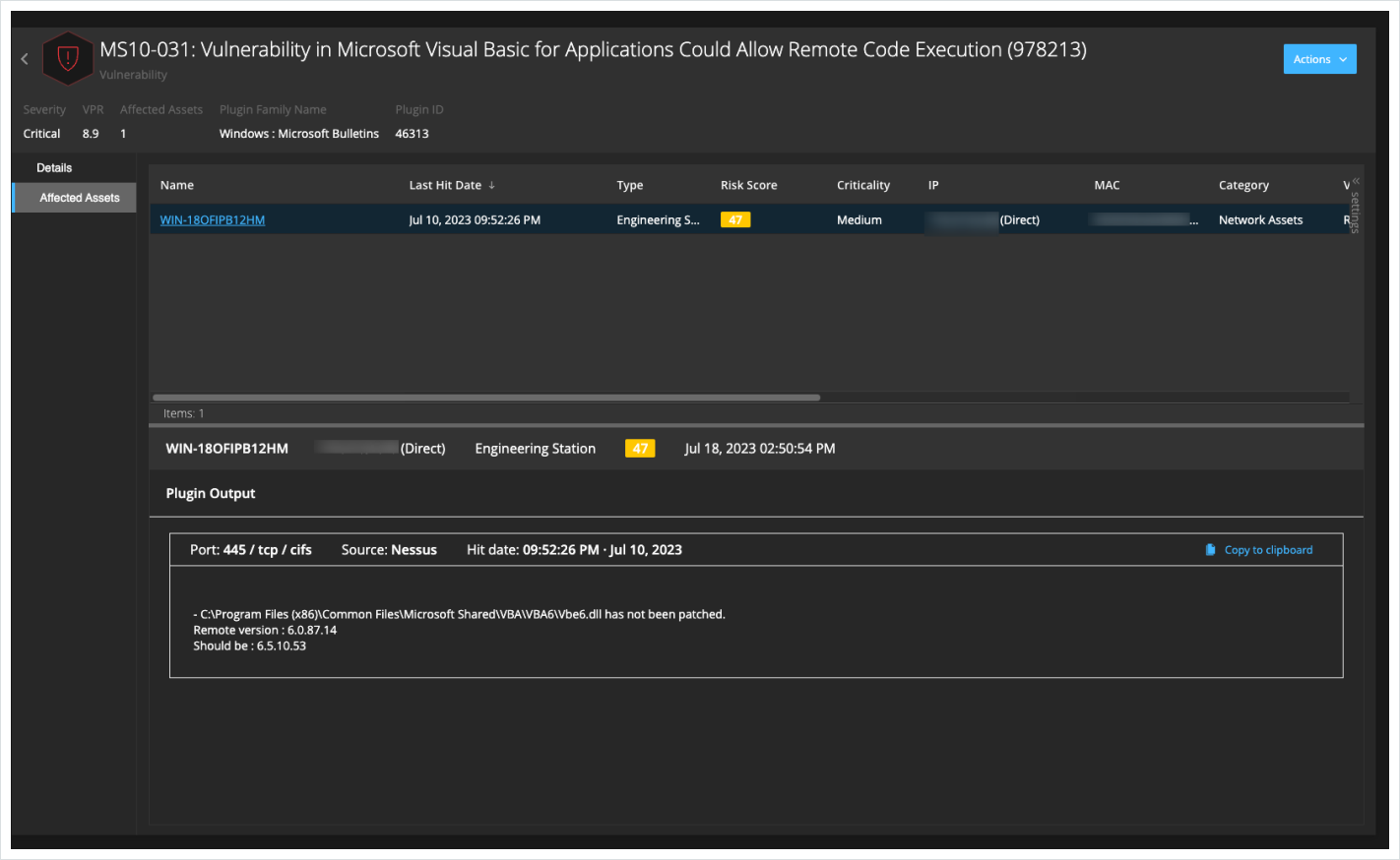
3. [脆弱性]タブをクリックします。

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。

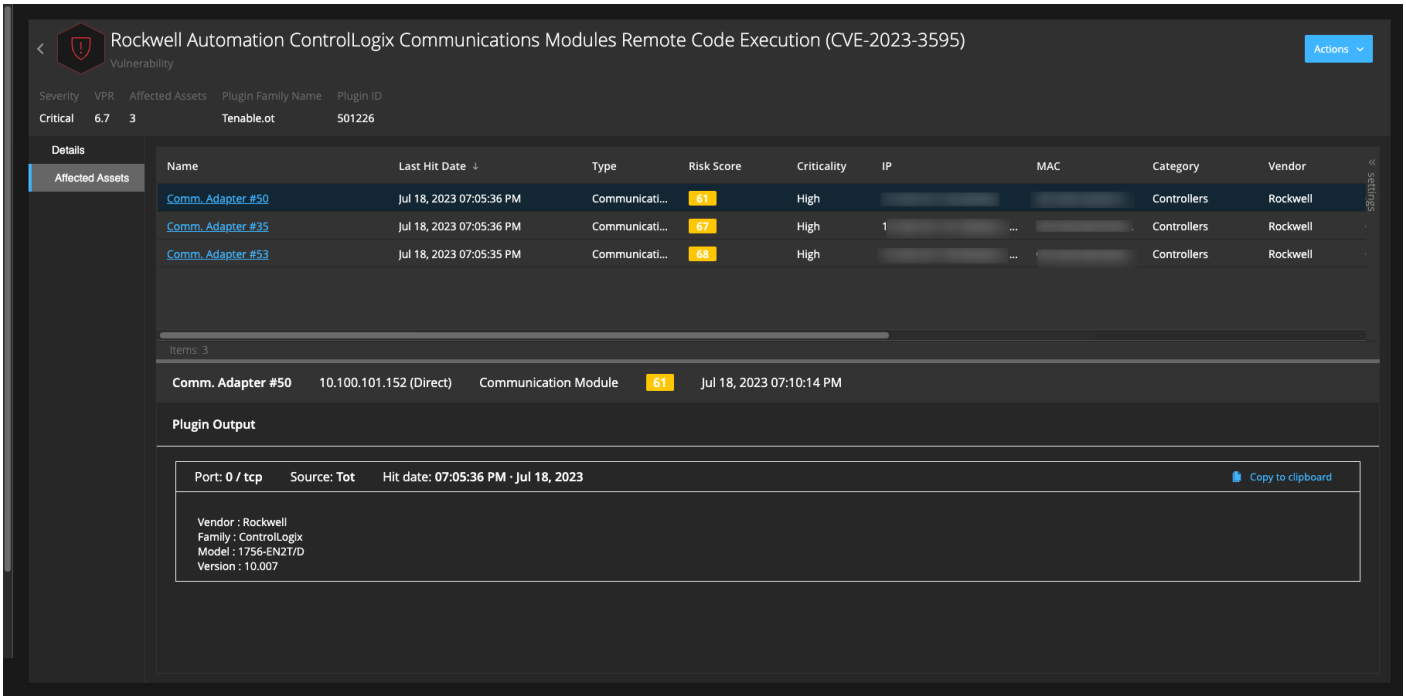
- ヒット日
- ソース
- ポート
- プラグイン出力

> 注意: すべてのプラグインでプラグイン出力があ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



検出結果

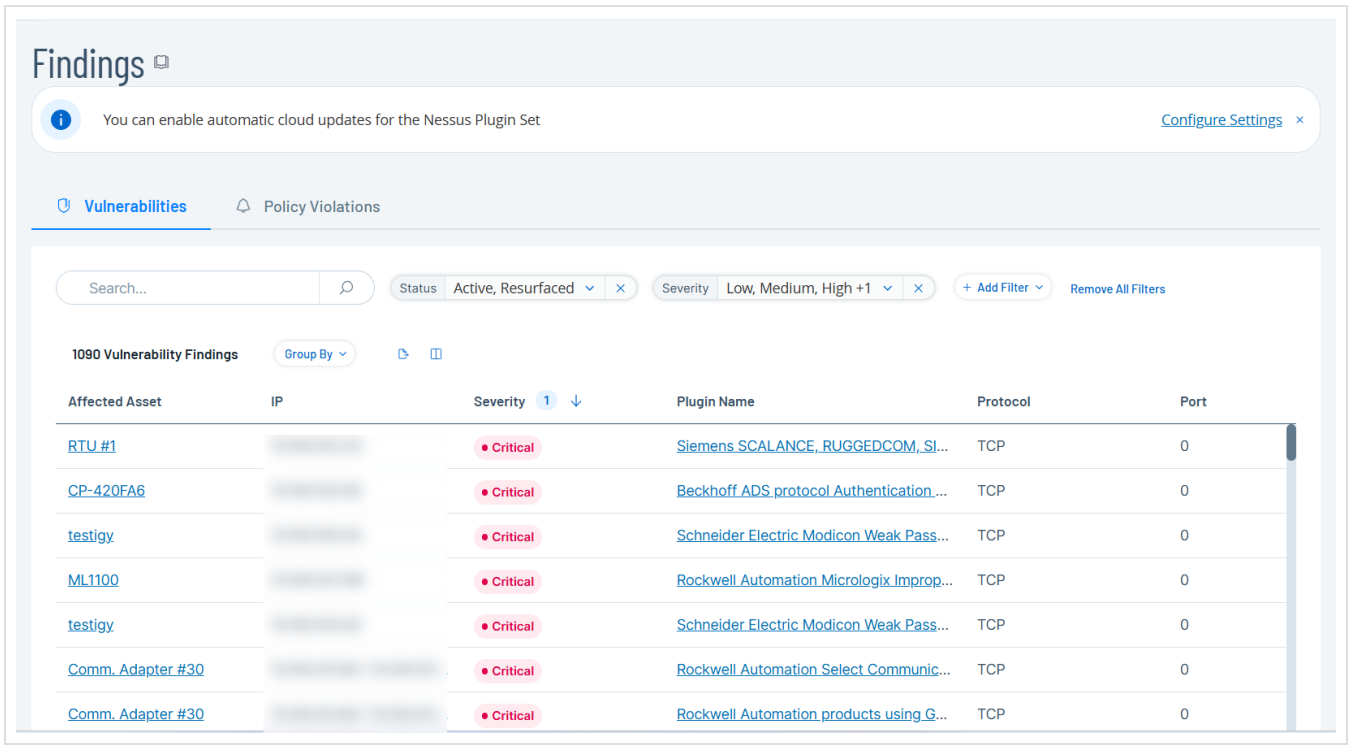
[検出結果] ページを使用して、環境に影響を与える脆弱性の個別のインスタンスのリストを資産ごとに確認します。[検出結果] ページでは、次の操作を実行できます。

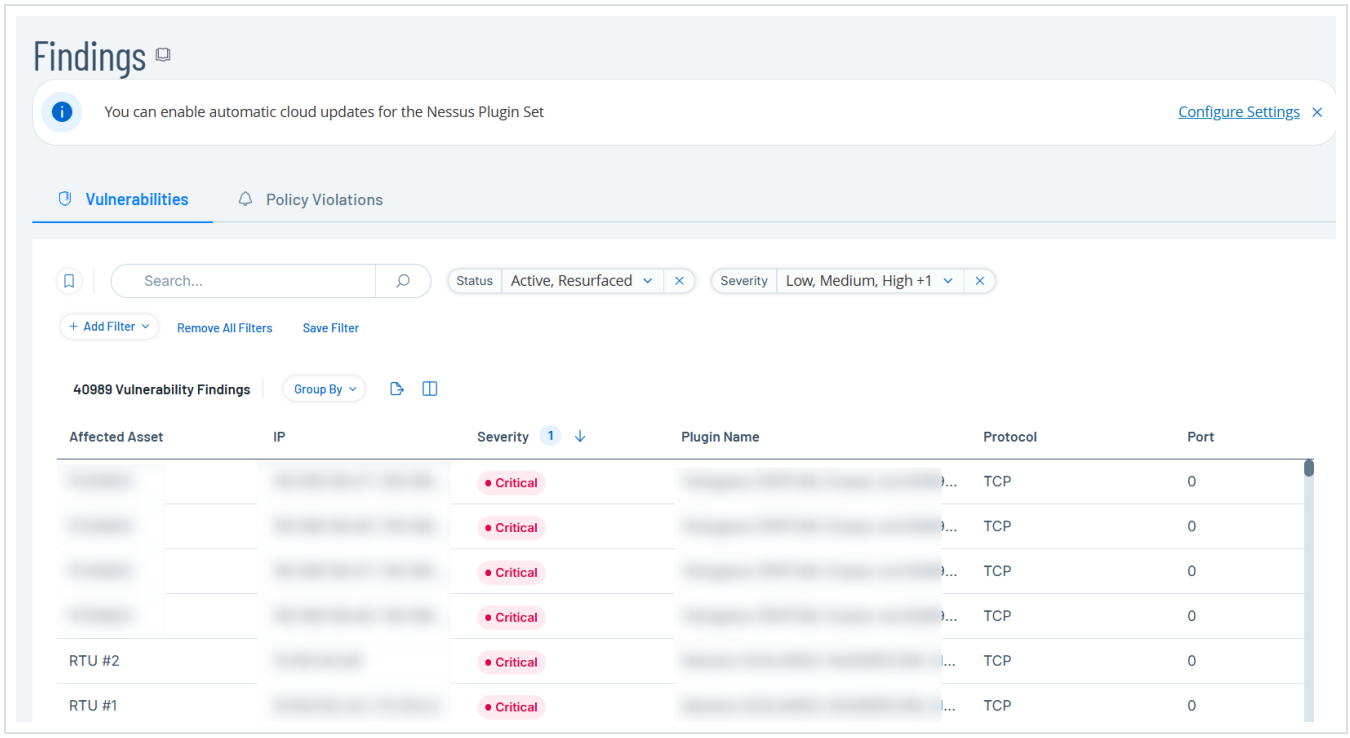
- 環境内の脆弱性のそれぞれ固有の「ヒット」に関する詳細な証拠を表示します。
- プラグインのプロパティ、影響を受けている資産、ステータス、最終ヒットなどの特定のインスタンス、またはプロパティの任意の組み合わせのいずれかで脆弱性のリストをフィルタリングします。
- フィルタリングされた検出結果のリストをエクスポートし、修正するために検出結果を割り当てます。

[検出結果] ページにアクセスする方法

1. 左側のナビゲーションメニューで、[リスク] > [検出結果] に移動します。

   [検出結果] ページが表示され、脆弱性が表形式で表示されます。





[検出結果] の表には、次の詳細が含まれています。

縦棒	説明
影響を受けている資産	脆弱性が検出された資産。
IP	資産のIPアドレス。
深刻度	脆弱性の深刻度: 重大、中、低、情報。
プラグイン名	脆弱性を検出したプラグイン。
プラグインID	プラグインのID。
ポート	脆弱性が検出されたポート。
プロトコル	資産との通信に使用されるプロトコル。
VPR	脆弱性のVulnerability Priority Rating。
ステータス	脆弱性のステータス。可能な値は次のとおりです。 アクティブ - 脆弱性が最初の検出以来継続的に発生していることを示します。 修正済み - 脆弱性が最初に現れた後は消失し、再び表面化しなかったことを示します。 再表面化 - 脆弱性が現れ、その後消失し、再び出現したことを示します。
プラグインソース	プラグインソース。
初回ヒット	脆弱性が最初に検出された時刻。
最終ヒット	脆弱性が最後に検出された時刻。

縦棒	説明
資産タグ	資産に関連付けられているタグ資産タグとグループを参照してください。
修正時刻	脆弱性が修正された時刻。
プラグインファミリー	プラグインのファミリー。
資産タイプ	資産タイプ (PLC、OT デバイスなど)。
資産リスクスコア	資産のリスクスコア。
資産カテゴリ	資産が属するカテゴリ(コントローラー、ネットワーク資産など)。
資産ベンダー	資産のベンダーの名前。
資産重大度	脆弱性の深刻度に基づく資産の重大度 (高重大度、中重大度、低重大度)。
資産ファミリー	資産のファミリー。
資産モデル	資産のモデル。
ファームウェア	資産のファームウェア。
OS	資産が実行されるオペレーティングシステム。
資産状態	資産の現在の状態。
パデューレベル	資産のパデューレベル
ネットワークセグメント	資産が属するネットワークセグメント。
場所	資産の場所。
バックプレーン名	脆弱性が検出されたバックプレーンの名前。

検出結果の詳細の表示

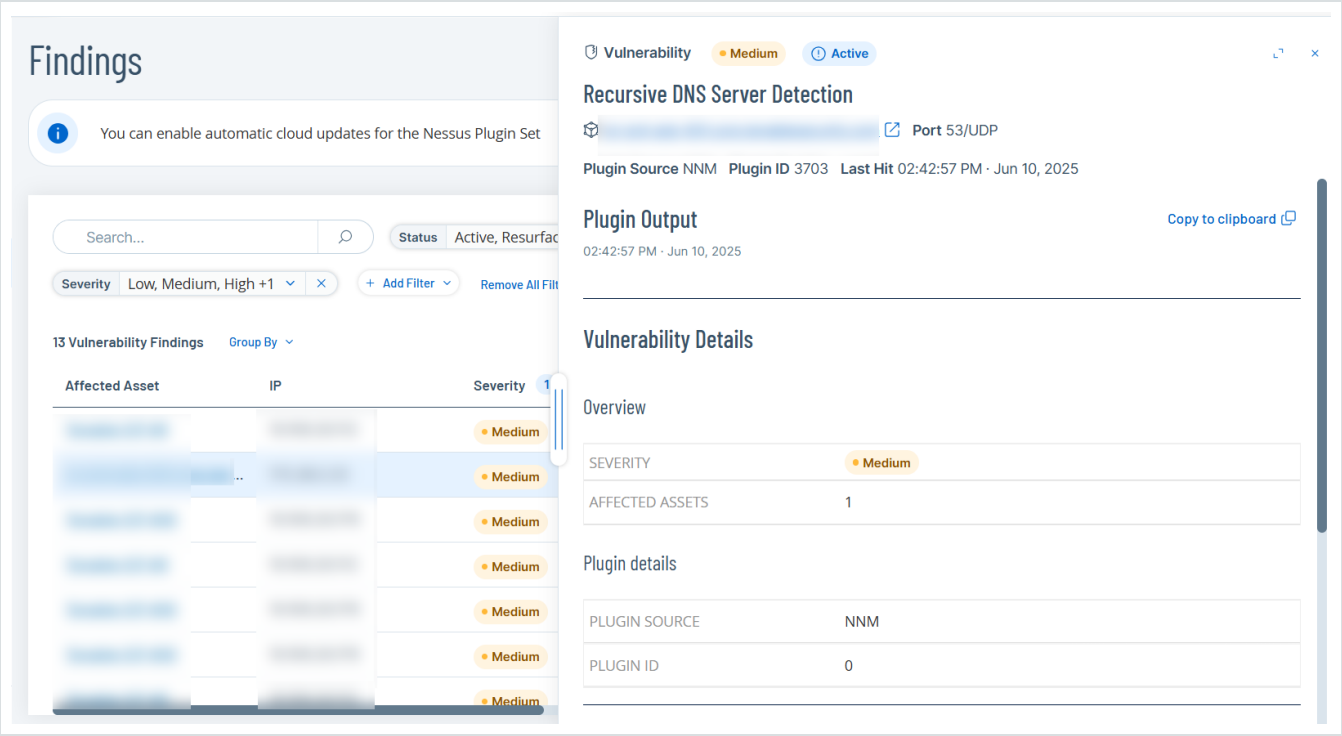
検出結果の詳細には、以下が含まれます。

- プラグイン出力
- 脆弱性の詳細
- 影響を受ける資産の詳細

検出結果の詳細を表示する方法

1. [検出結果] ページで、[影響を受ける資産] または [プラグイン名] 列にあるリンクをクリックします。

   [脆弱性の詳細] パネルが表示されます。



   次の詳細を表示できます。

   - 深刻度
   - 影響を受ける資産

- プラグインソース
- プラグイン ID
- 影響を受ける資産の詳細 (例: 名前、タイプ、重要度、リスクスコア、IP アドレス、パデューレベル)

- [脆弱性の詳細] パネルを展開するには、右上の ボタンをクリックします。
- パネルを閉じるには、右上の × ボタンをクリックします。
- 資産の全詳細情報を表示するには、[影響を受ける資産] セクションで、[資産の詳細をすべて表示] をクリックします。
- OT Security により別のブラウザタブが開き、そこに表示される [インベントリ] ページに 1 つの資産の詳細が表示されます。

ポリシー違反

[ポリシー違反] ページを使用して、同じポリシー、ソース、デスティネーションに関連付けられているすべてのイベントを表示します。ページにある各検出結果は、同じソースとデスティネーションを共有する同じポリシーヒットから生じた複数のイベントの集約です。

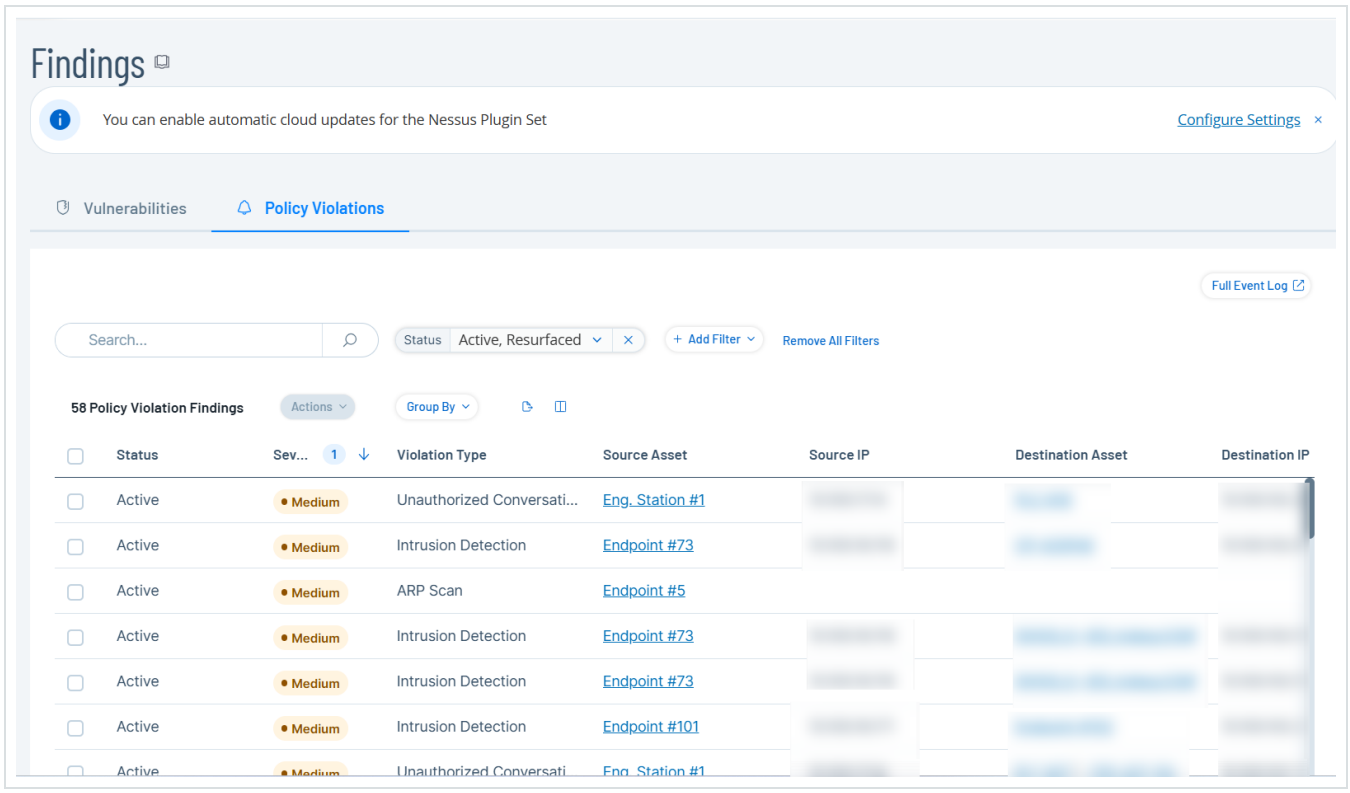
[ポリシー違反] ページにアクセスする方法

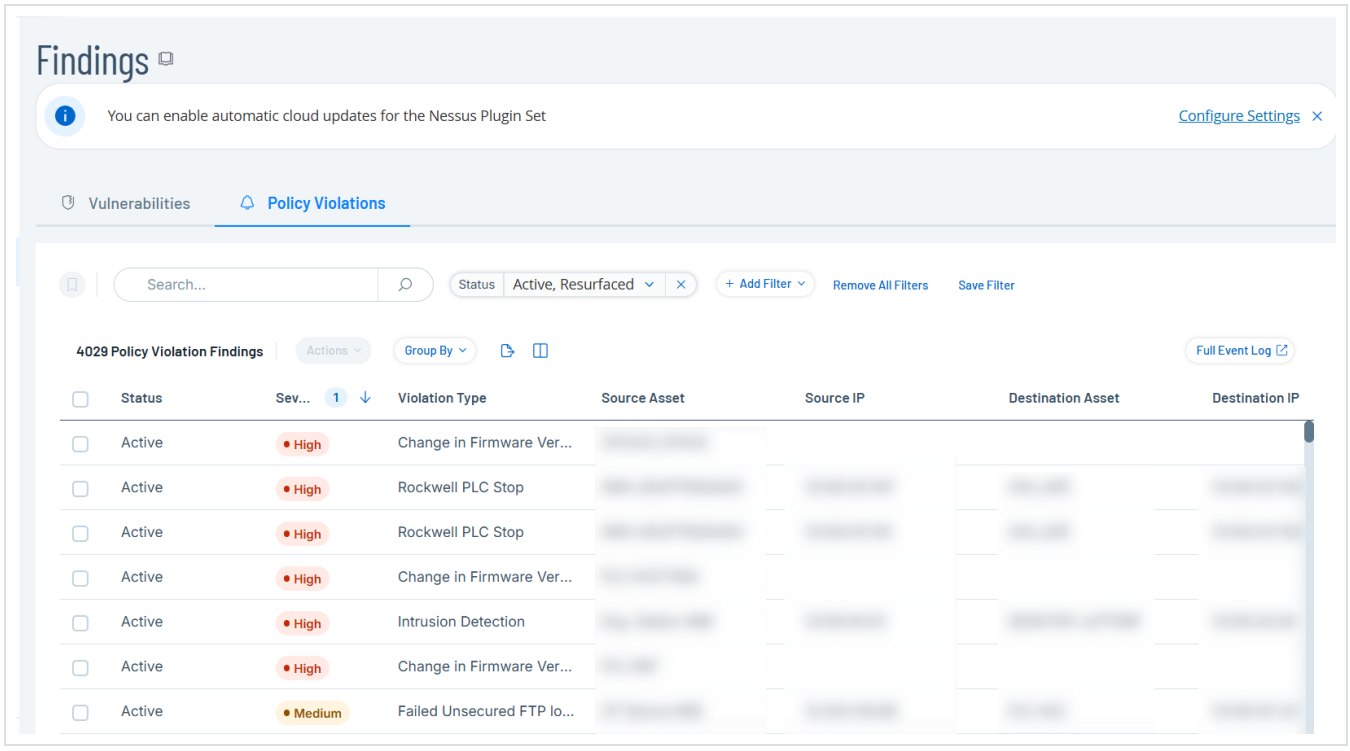
1. 左側のナビゲーションメニューで、[リスク] > [検出結果] をクリックします。

   [検出結果] ページが表示されます。

2. [ポリシー違反] タブをクリックします。

   [ポリシー違反] ページが、イベントのリストとともに表示されます。





[ポリシー違反] タブには以下の詳細が含まれます。

縦棒	説明
ID	違反のID
ステータス	違反のステータス: アクティブ、再表面化、解決済み
深刻度	違反の深刻度レベル: [高]、[中]、[低]
違反のタイプ	違反の種類 (たとえば、認証されていない会話や侵入検知)
違反カテゴリ	違反タイプが属するカテゴリ
ポリシー	違反の原因となったポリシー
プラグイン名	違反に関連付けられているプラグイン
Mitre ICS 戦術	産業用制御システム (ICS) に対する特定のMitre 攻撃手法の背後にある理由
Mitre ICS 技術	攻撃者が戦術目標を達成する方法
ソース資産	違反が発生した資産
ソースIP	ソース資産のIP アドレス
デスティネーション資産	違反が終了した資産
デスティネーションIP	デスティネーション資産のIP アドレス
プロトコル	違反に関連付けられているプロトコル
初回ヒット	違反が最初に検出された時刻

縦棒	説明
最終ヒット	違反が最後に検出された時刻
アクティブヒット	違反を引き起こしたイベントの数
資産タイプ	違反が検出された資産のタイプ
資産重大度	資産の重大度
資産ベンダー	資産に関連付けられたベンダー
資産ファミリー	資産が属するファミリー
資産タグ	資産に関連付けられているタグ
パデューレベル	資産のパデューレベル
資産の場所	資産が配置されている地域
解決日	違反が解決された日付
解決者	違反を解決したユーザー
コメント	違反の解決時にユーザーが追加したコメント

3. (オプション) [違反] ページで以下の操作を実行できます。

    - 表のカスタマイズの説明に従って列をカスタマイズします。
    - 検出結果の表にフィルターを適用します。表でのフィルター適用を参照してください。
    - データを CSV 形式でエクスポートします。

[アクション] メニュー

検出結果の解決

- 検出結果を解決する方法

    a. 検出結果の行を選択し、[アクション] > [解決] をクリックします。

    [解決] パネルが表示されます。

    b. 検出結果を解決するコメントを入力します。

    c. [保存] をクリックします。

    OT Security が検出結果を解決し、[プラグインの詳細] パネルにステータスが [解決済み]と表示されます。

    > 注意: イベントが再発すると、OT Security は検出結果を再度開き、ステータスが [再表面化] と表示されます。

ポリシーから除外する

- 検出結果をポリシーから除外する方法

    a. 検出結果の行を選択し、[アクション] > [ポリシーから除外] をクリックします。

    [ポリシーから除外] パネルが表示されます。

    b. 除外条件を選択します。

    > 注意: 除外条件は、直近のイベントに基づいています。

    c. [除外の説明] を入力します。

    d. [保存] をクリックします。

    OT Security は、直近のイベントをポリシーから除外します。

最新キャプチャファイルをダウンロードする

- 最新キャプチャファイルをダウンロードする方法

    a. 検出結果の行を選択し、[アクション] > [最新キャプチャファイルのダウンロード] をクリックします。

    OT Security は、直近のイベントのキャプチャファイルをダウンロードします。

プラグイン詳細

検出結果のプラグインの詳細を表示する方法

1. [ポリシー違反] タブで検出結果の行をクリックすると、プラグインの詳細が表示されます。

    プラグイン詳細パネルに、OT Security プラグインページから違反の詳細が表示されます。

    パネルは、4 つのタブ ([詳細]、[ソース]、[デスティネーション]、[ポリシー]) で、違反の詳細を表示します。

イベントを検索する

違反を引き起こした特定のイベントを検索する方法

a. 特定の検出結果のイベントを検索するには、[検出結果 ID をコピー] をクリックします。

b. [イベント] ページに移動するには、[完全なイベントログ] リンクをクリックします。

    [すべてのイベント] ページが表示されます。

c. [検索] ボックスに、先ほどコピーした検出結果 ID を貼り付けます。

    OT Security は、特定の検出結果のイベントを一覧表示します。

コンプライアンスダッシュボード

必要な OT Security ユーザーロール: 管理者、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

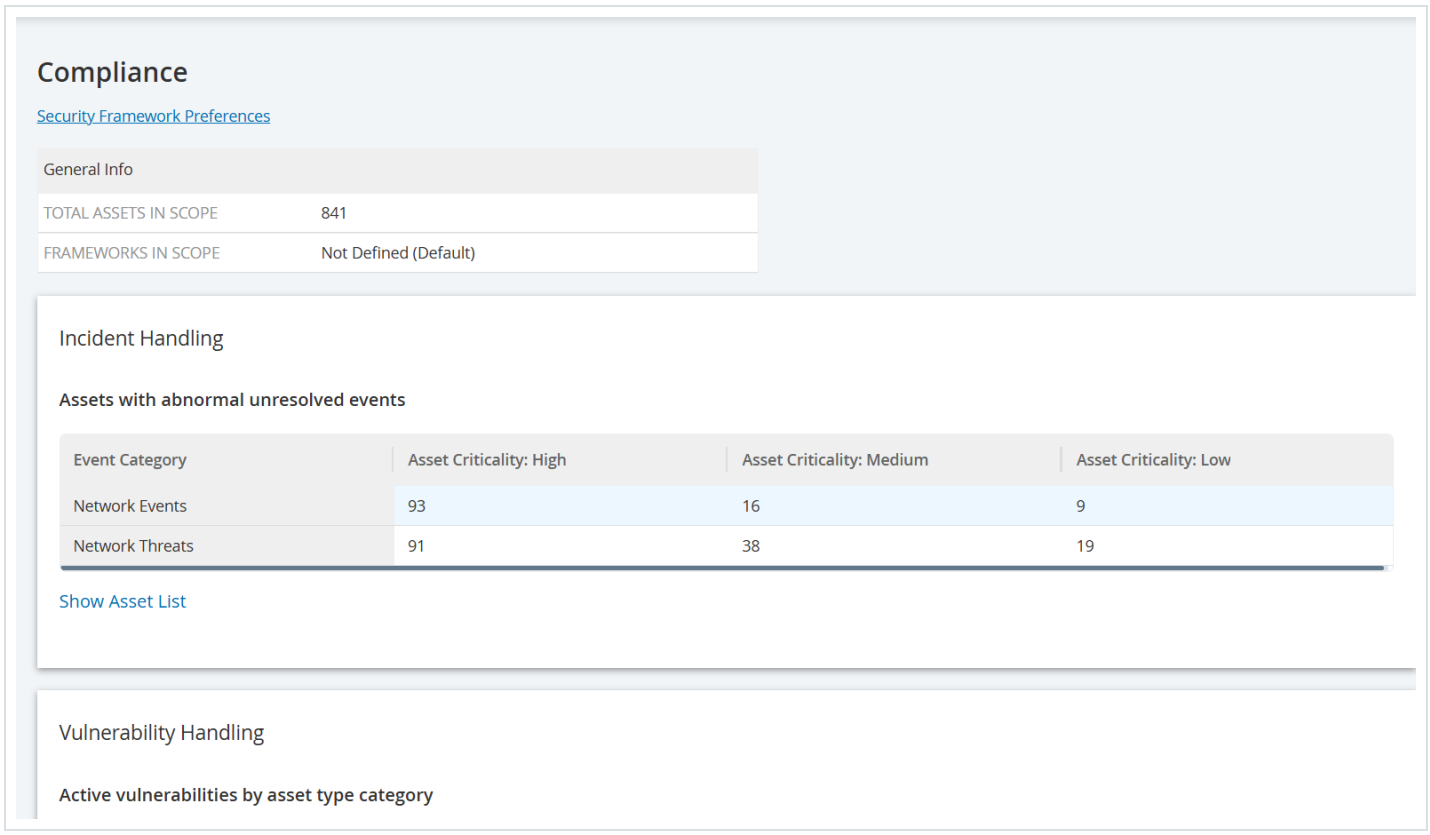
現在、重大なインフラを持つほとんどの企業で、NIS 2 指令や ISO 27001 管理策などのセキュリティフレームワークへのコンプライアンスの監査チェックが行われ、それをクリアすることが義務付けられています。

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。

2. 左側のナビゲーションバーで [リスク] > [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

ウィジェット	説明
	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スク	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、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

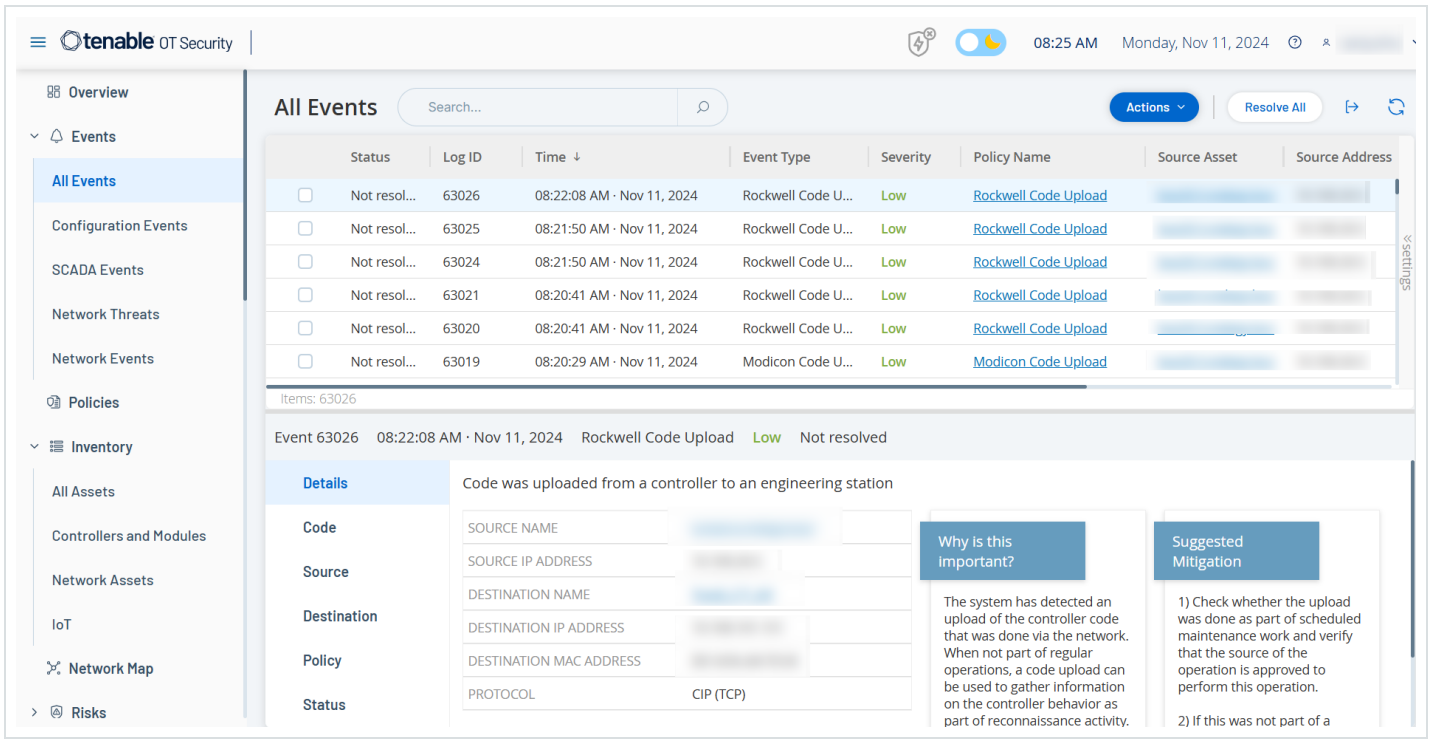
ウィジェット	説明
	ブに特定して軽減するのに役立ちます。 注意: リスクが高い資産をすべて表示するには、[資産リストを表示する] リンクをクリックします。資産リストを閉じるには、[資産リストを非表示にする] をクリックします。

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。

各イベントページ (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。イベントタイプ、深刻度、ポリシー名などに基づいて、イベントをグループ化することができます。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。

パラメーター	説明
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	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。

パラメーター	説明
ン資産	
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

パラメーター	説明
	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] ページの下部に、選択したイベントのさらに詳しい情報が表示されます。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)。

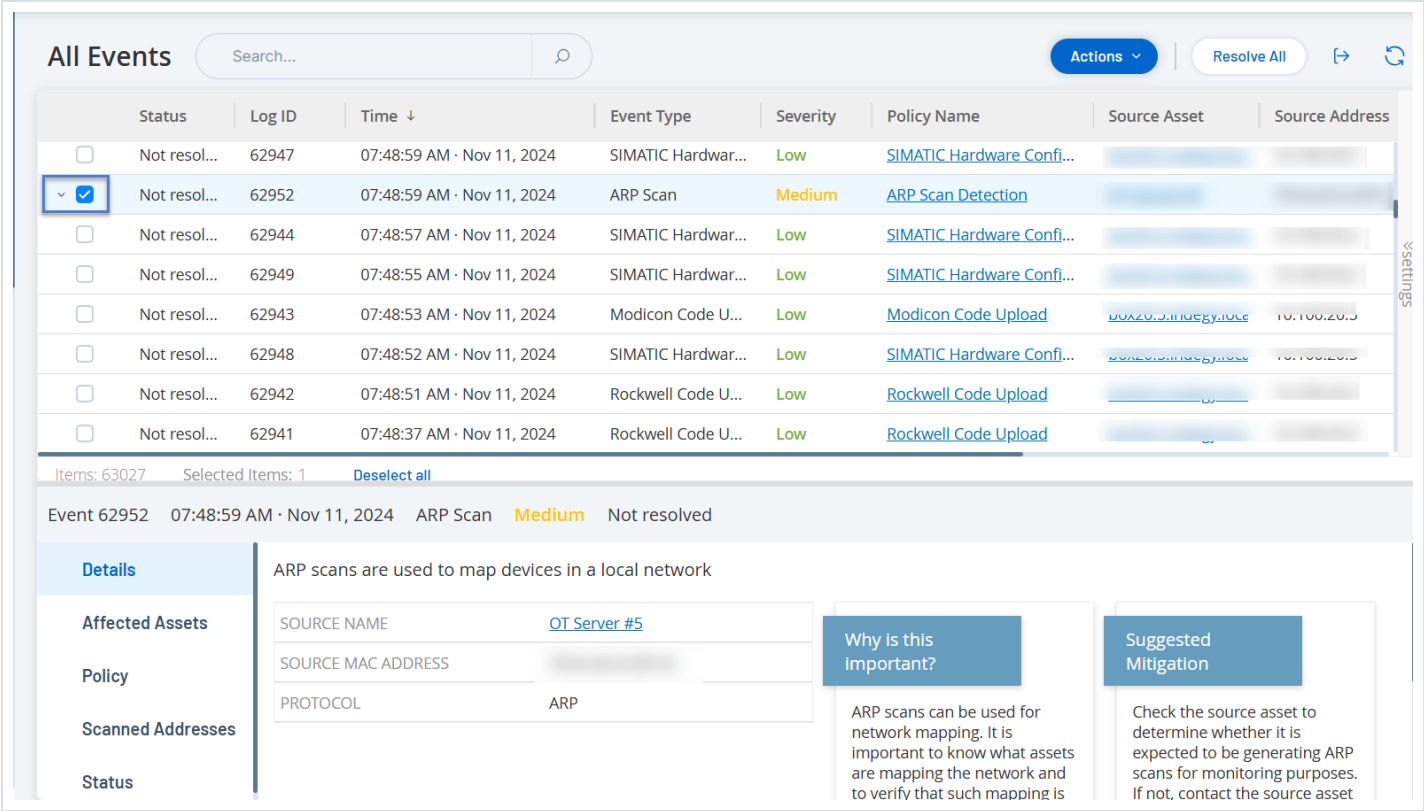
- ヘッダー - イベントに関する重要な情報の概要を表示します。
- 詳細 - イベントの簡単な説明、およびこの情報が重要である理由の説明とイベントによる潜在的な被害を緩和するための推奨手順が記載されています。さらに、イベントに関連するソース資産とデスティネーション資産も表示されます。
- ルールの詳細 (侵入検出イベント用) - イベントに適用される Suricata ルールに関する情報を表示します。

- 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。

イベントクラスタの表示

イベントのモニタリング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 つのクラスタにまとめられます。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。イベントクラスタの設定の詳細については、イベントクラスタを参照してください。

クラスタ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。



ポリシー除外の作成

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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。

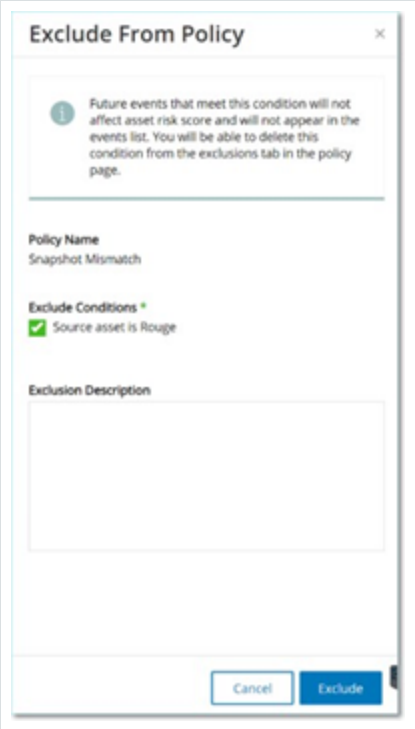
3. [ポリシーから除外] をクリックします。

   [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

ポリシーカテゴリ	イベントタイプ	除外条件
	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

ポリシーカテゴリ	イベントタイプ	除外条件
		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

ポリシーカテゴリ	イベントタイプ	除外条件
	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

ポリシーカテゴリ	イベントタイプ	除外条件
	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

ポリシーカテゴリ	イベントタイプ	除外条件
		• 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

必要な OT Security ユーザーロール: 管理者、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

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ます。これらのファイルをダウンロードし、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。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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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。

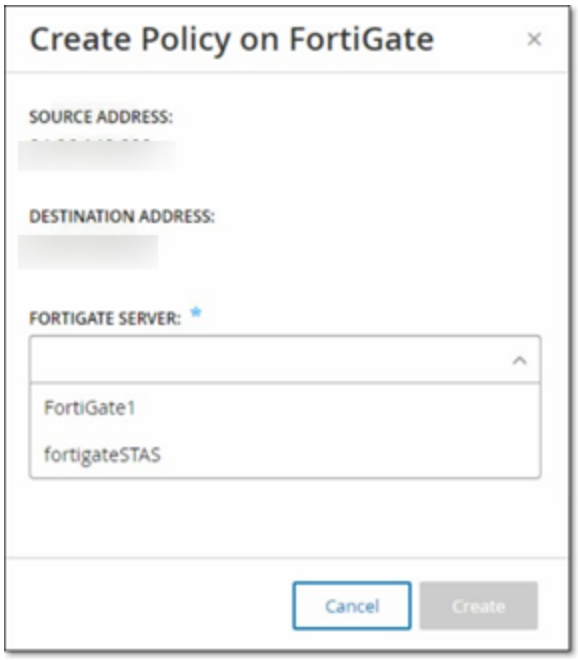
FortiGate ポリシーを提案する前に、FortiGate ファイヤーウォールサーバーと OT Security の統合を設定する必要があります。FortiGate ファイヤーウォールを参照してください。

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。

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。

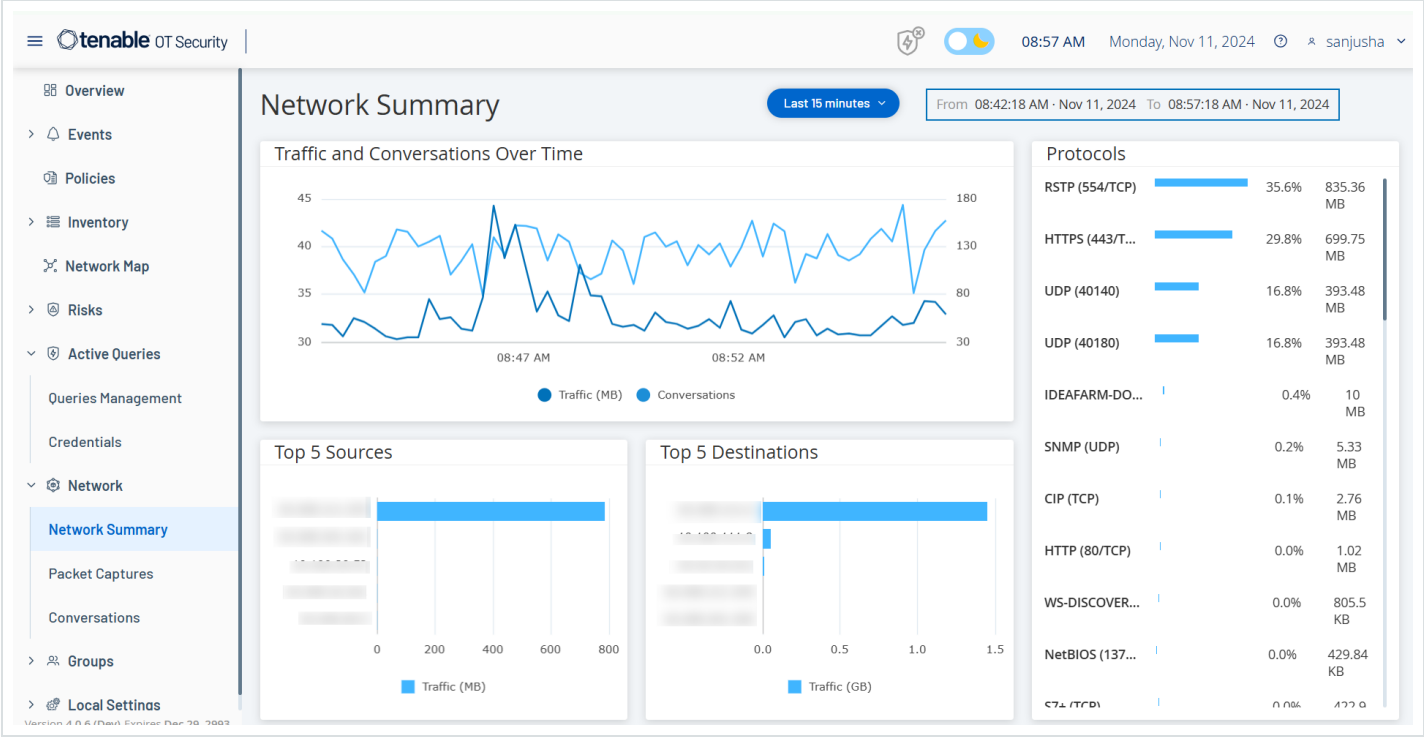
[ネットワーク] ページにアクセスする方法

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

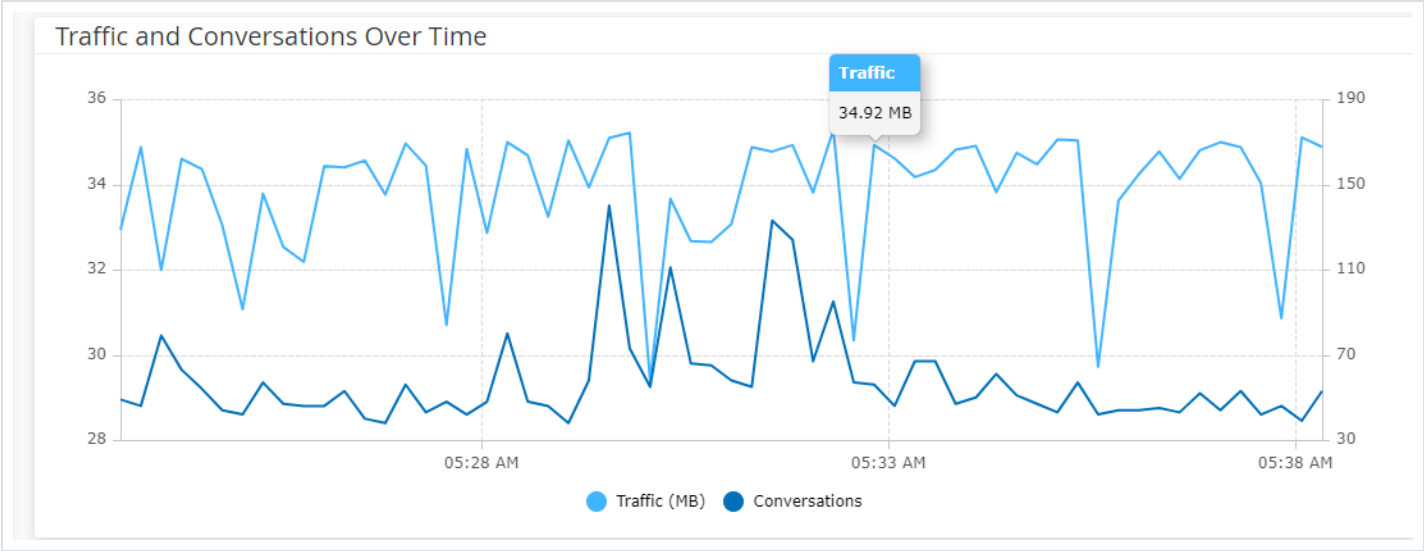
[ネットワーク概要] ページには、ネットワークアクティビティをまとめたビジュアルグラフが表示されます。特定の時間枠のデータを表示できます。



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

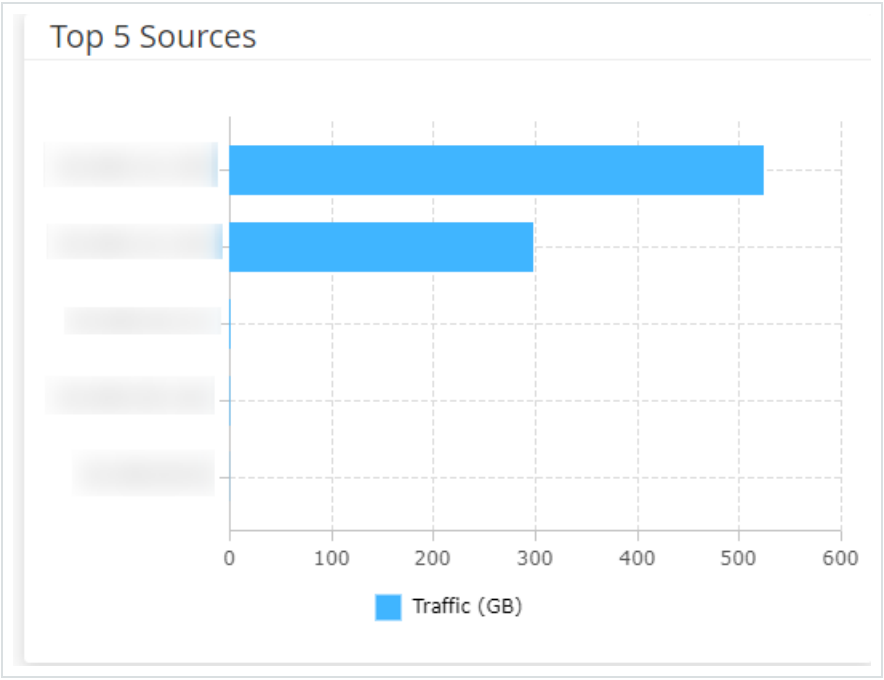
折れ線グラフが、ネットワーク内のトラフィックの量 (KB/MB/GB で測定) と対話の数の推移を表示します。凡例キーがグラフの上部に表示されます。グラフ上のポイントにカーソルを合わせると、その時間セグメント中に発生したトラフィックと対話に関する特定のデータが表示されます。



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。

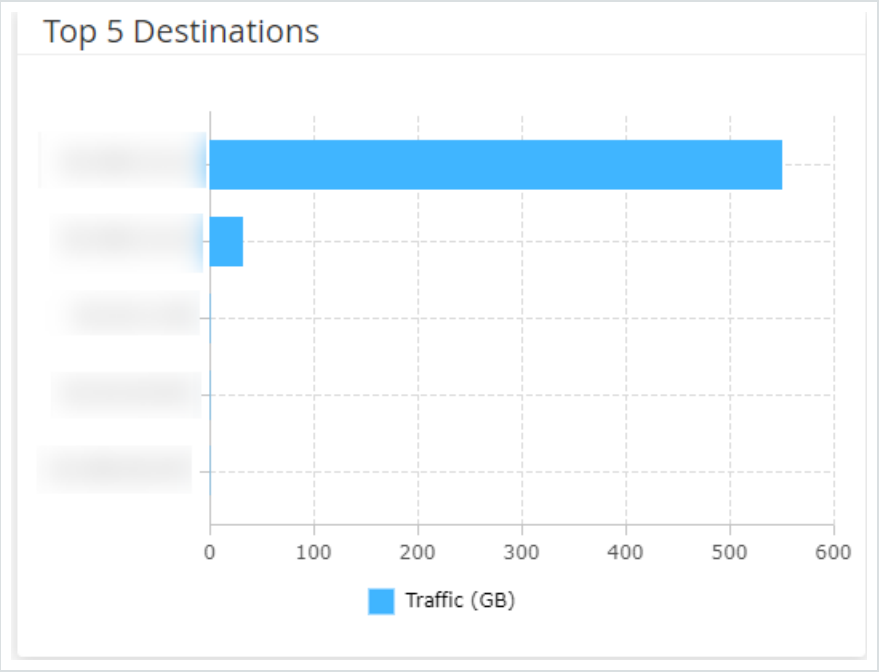
上位 5 件のソース

[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。



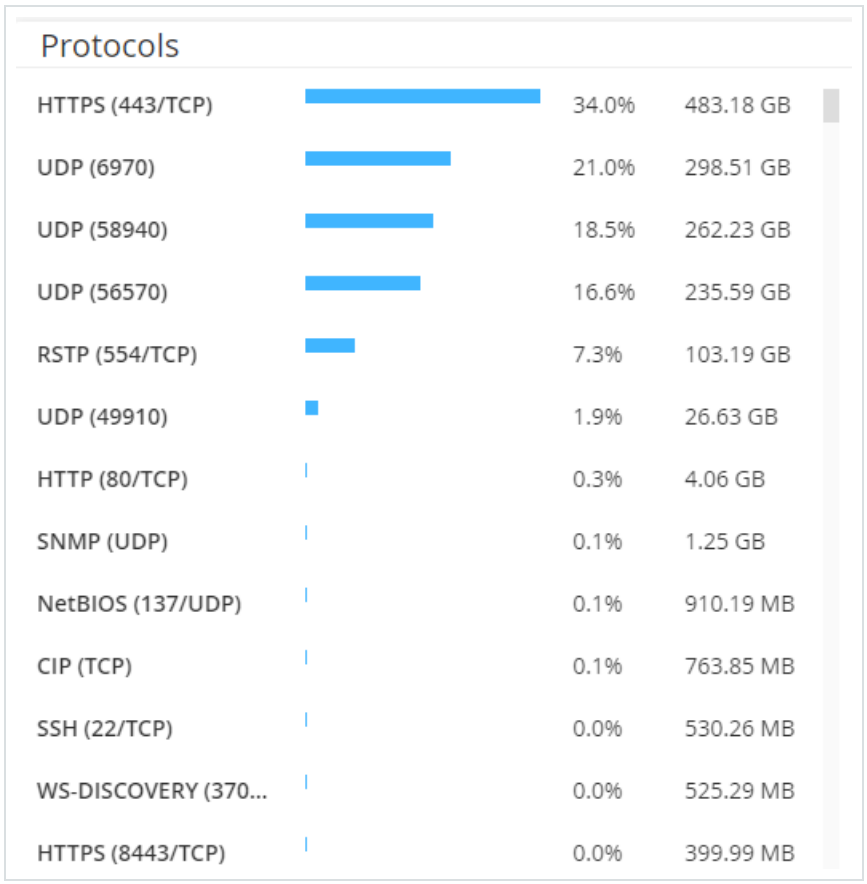
上位 5 件のデスティネーション

[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。

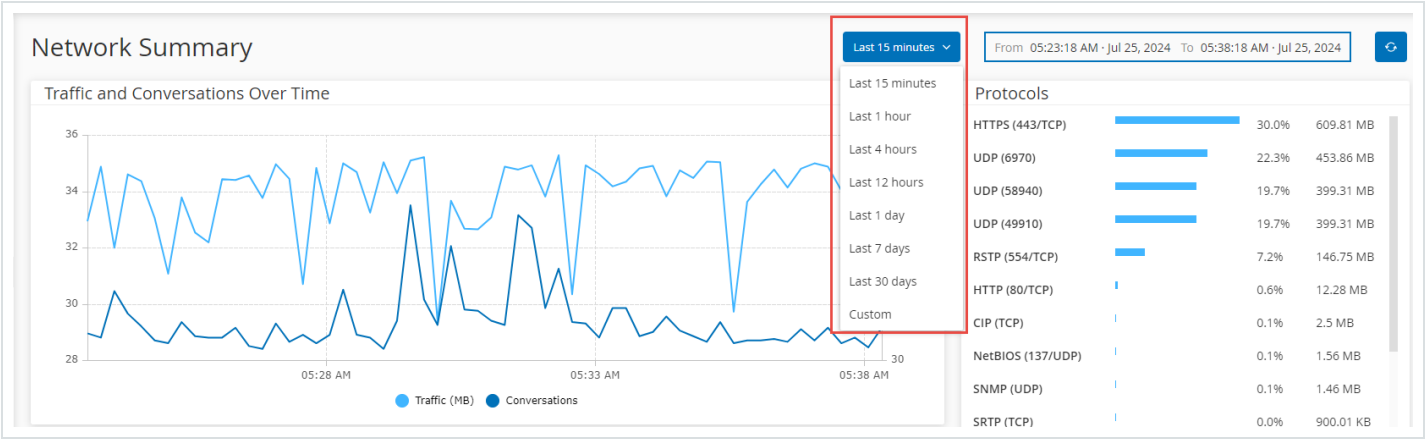
タイムフレームの設定

[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 によりページがリフレッシュされ、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。

> 注意: 読み取り専用およびサイトオペレーターのロールには、進行中のキャプチャを停止したり、保存されたパケットキャプチャをダウンロードしたりするアクセス許可がありません。

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	パケットキャプチャが終了した日時。

刻	
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

> 必要な OT Security ユーザーロール: 管理者、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

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。

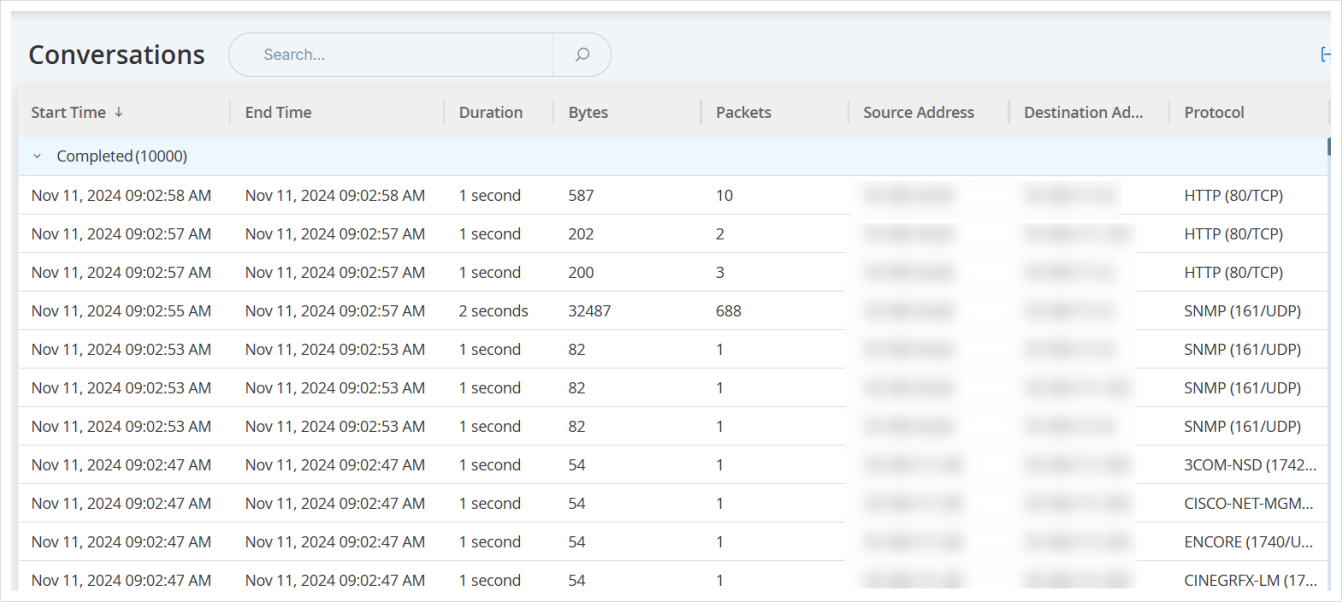
- 検索 – [検索] ボックスを使用し、識別情報を入力することで特定の対話を検索します。
- エクスポート – [エクスポート] ボタンを使用して、[対話] タブにあるすべてのデータを、ローカルマシンの .csv ファイルにエクスポートします。

> 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。



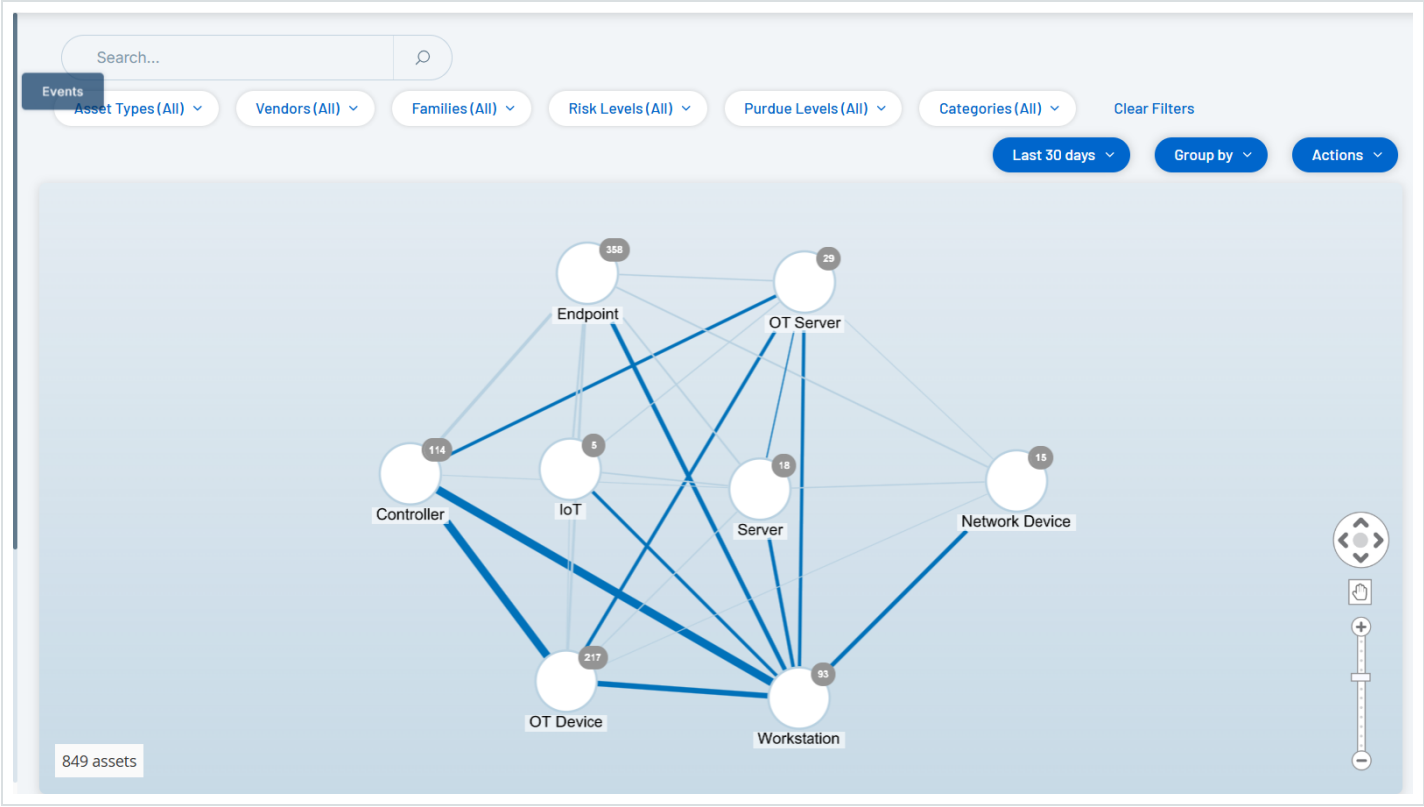
   [対話] ページには、次の詳細が表示されます。

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	通信に使用されるプロトコル。

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、資産のグループ間または個々の資産間 (またはその両方) の各通信です。線の太さは、その接続を通して行われている通信量を示します。

    ネットワークマップでは、カラーコードを使用して IT プロトコルと OT プロトコルを区別しています。

    - 灰色の線は、IT 専用プロトコル (DNS、HTTP、FTP など) を示します。

    - 青い線は、OT プロトコル (HTTP、MODBUS、CIP、FTP など) の存在を示します。

- 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。

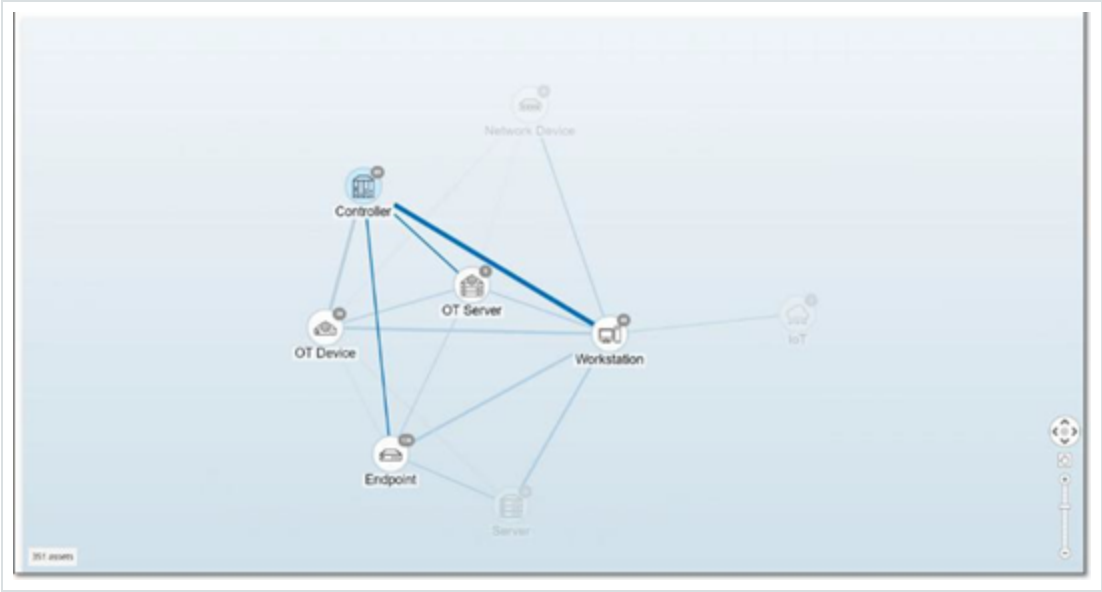
マップ表示が [資産タイプ] (デフォルト) でグループ化されている場合、ドリルダウン階層は次のようになります。[資産タイプ] > [ベンダー] > [ファミリー] > [個別資産]。

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。

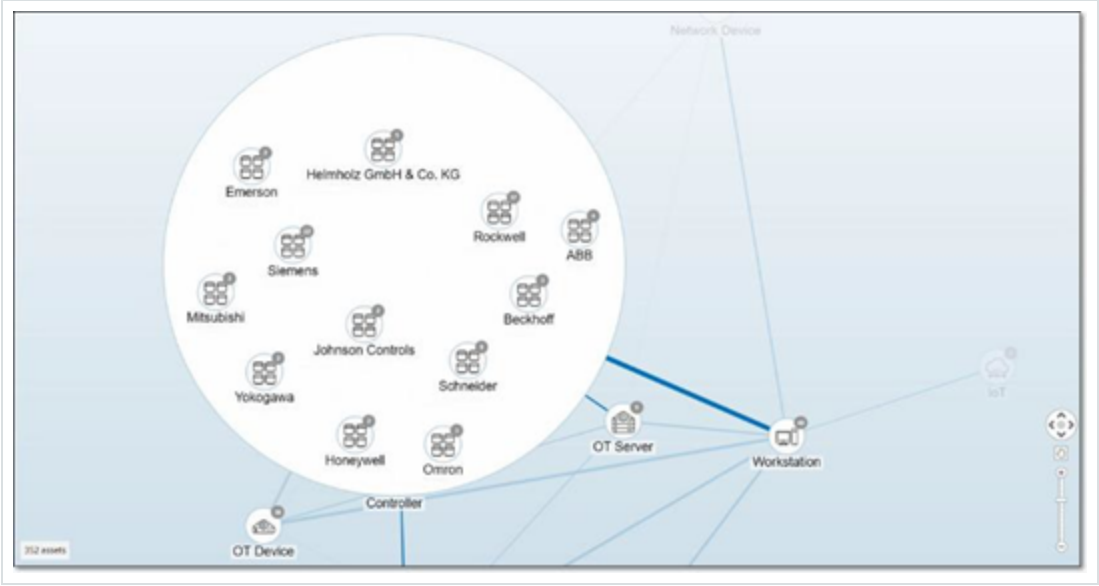
資産タイプグループにドリルダウンする手順

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。

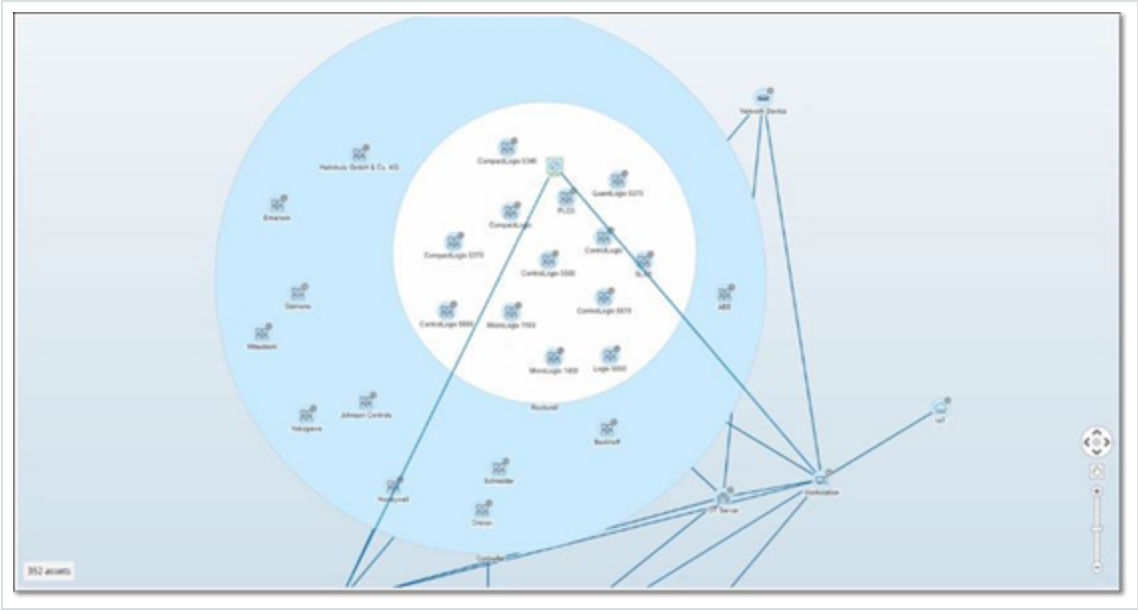


2. ドリルダウンするグループアイコン (例 : コントローラー) をダブルクリックします。

   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。

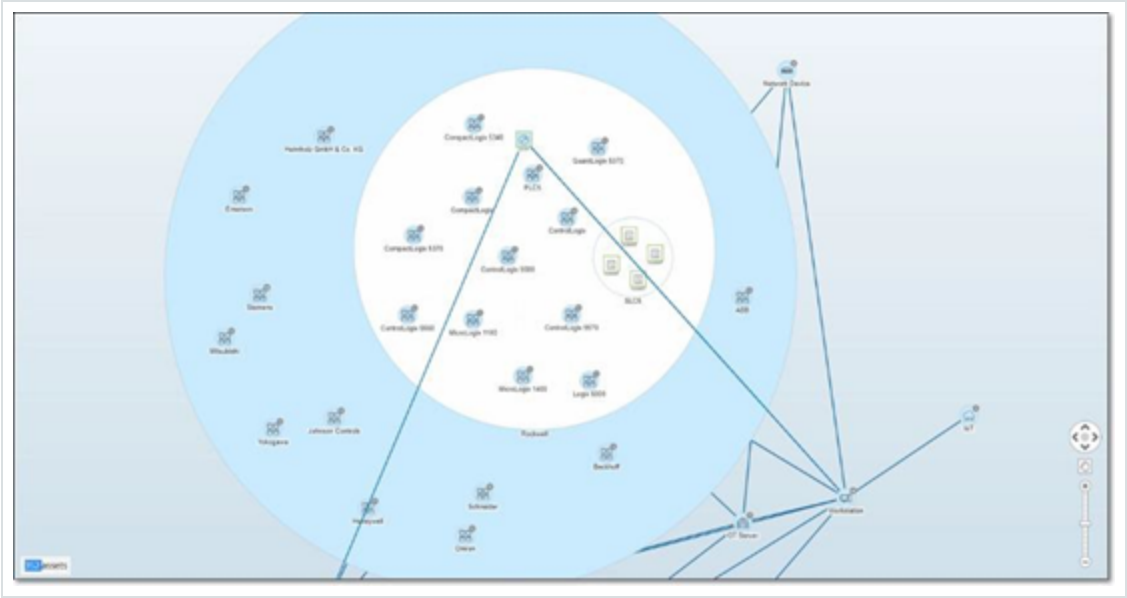


3. さらにドリルダウンするには、ベンダーグループ (例 : Rockwell) をクリックします。



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。

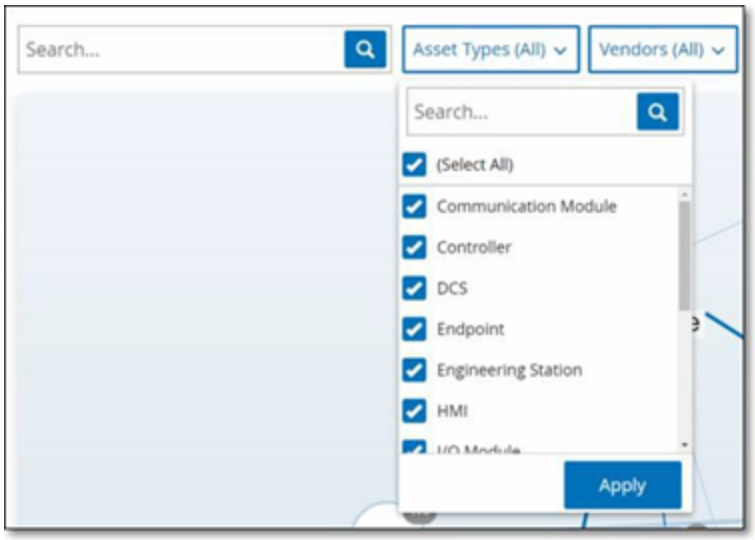
すべてのグループ化の削除手順

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、パデューレベルの中から 1 つ以上の指定し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。

資産の詳細の表示

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、当該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、そのベースラインが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。

データ収集

OT Security の [データ収集] セクションには、次の設定ページが含まれます。

- ポリシー
- アクティブクエリの管理
- データソース

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。システムはイベントをログに記録し、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、ポリシーの有効化または無効化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。
- E 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、職務別、部門別でグループ化します。
- ポートグループ – 似たような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) 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、テストです。
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	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

	産、スケジュール	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、スケジュール	ネットワークベースラインのサンプリング中に、互いに通信しなかった資産間の新しい接続を検出します。このオプションは、システムにネットワークベースラインが設定された後にのみ利用可能です。初期ネットワークベースラインを設定したり、ネットワークベースラインを更新したりするには、ネットワークベースラインの設定を参照してください。ポリシーは、プロトコルグループからのプロトコルを使用して、指定された時間範囲内のソース資産グループの資産からデスティネーション資産グループの資産への通信に適用されます。
検出された新しい資産	影響を受ける資産、スケジュール	指定された時間範囲内にネットワークに出現する、ソース資産グループの指定されたタイプの新しい資産を検出します。
オープンポート	影響を受ける資産、ポート	ネットワークで新しいオープンポートを検出します。未使用のオープンポートは、セキュリティリスクをもたらす可能性があります。このポリシーは、影響を受ける資産グループの資産およびポートグループのポートに適用されます。
ネットワークトラフィックの急激な上昇	時間枠、機密性レベル、スケジュール	ネットワークトラフィック量の異常な急増を検出します。このポリシーは、指定された時間枠に関連し、指定された機密性レベルに基づく急激な上昇に適用されます。また、指定された時間範囲に制限されます。

会話の急激な上昇	時間枠、機密性レベル、スケジュール	ネットワーク内の会話数の異常な急増を検出します。このポリシーは、指定された時間枠に関連し、指定された機密性レベルに基づく急激な上昇に適用されます。また、指定された時間範囲に制限されます。
RDP 接続 (認証済み)	ソース、デスティネーション、スケジュール	認証資格情報を使用してネットワークで RDP (リモートデスクトップ接続) が行われました。このポリシーは、指定された時間範囲内にデスティネーション資産グループの資産に接続する、ソース資産グループの資産に適用されます。
RDP 接続 (未認証)	ソース、デスティネーション、スケジュール	認証資格情報を使用せずに、ネットワークで行われた 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	ポリシー	説明

タイプ	条件	
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(ICS攻撃、サービス拒否、マルウェア)とサブカテゴリ(ICS攻撃 - Stuxnet、ICS攻撃 - Black Energy)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き込み	ソース資産、デスティネーション資産、スケジュール	MMS 経由で ABB 800xA コントローラーに送信される、許可された範囲外の書き込みコマンドを検出します。
IEC 60870-5-104 コマンド (データ転送の開始 / 停止、問い合わせコマンド、カウンター問い合わせコマンド、クロック同期コマンド、プロセスリセットコマンド、時間タグ付きテストコマンド)	ソース資産、デスティネーション資産、スケジュール	リスクがあると考えられる IEC-104 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から発生しているエラーも検出します。

ポリシーの有効化または無効化

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

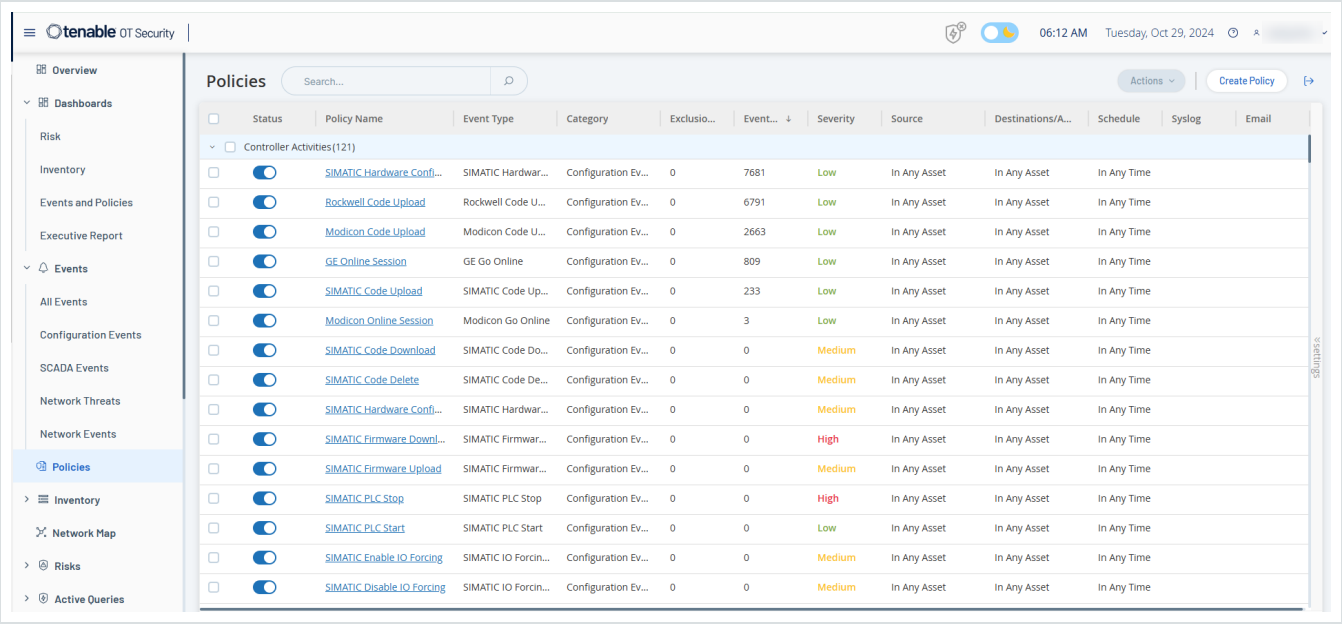
設定されているポリシー (事前設定とユーザー定義の両方) をシステムで有効または無効にできます。個々のポリシーのオンとオフを切り替えたり、複数のポリシーを選択して一括処理でオンとオフを切り替えたりすることができます。

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分けされて一覧表示されます。

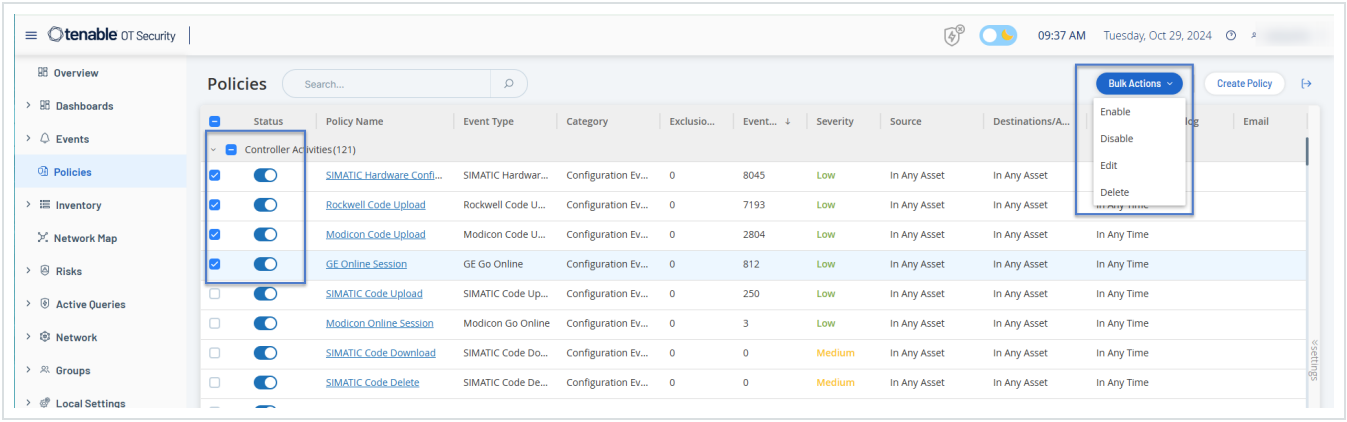


2. ポリシーを有効または無効にするには、該当するポリシーの横にある [ステータス] トグルをクリックします。

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分けされて一覧表示されます。



2. 有効/無効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 – 表のトップ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

> **必要な OT Security ユーザーロール:** 管理者、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

[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 はカテゴリ別にグループ化され、カテゴリごとに異なるプレフィックスが付けられます。たとえば、コントローラーアクティビティの場合は P1、ネットワークイベントの場合は P2 となります。
名前	ポリシーの名前。
深刻度	イベントの深刻度。可能な値は、[なし]、[低]、[中]、[高] です。深刻度レベルの説明については、深刻度レベルセクションを参照してください。
イベントタイプ	このイベントポリシーをトリガーするイベントの特定のタイプ。
カテゴリ	このイベントポリシーをトリガーするイベント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	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

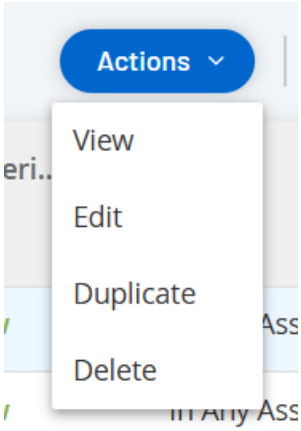
資産 / 影響を受ける資産	指定しない) を含むポリシーの場合、このパラメーターはイベントの影響を受けた資産を表示します。
スケジュール	ポリシー条件。ポリシーが適用される時間範囲です。
Syslog	このポリシーのイベントを記録する Syslog サーバー (SIEM)。
E メール	このポリシーのイベント通知を送信する E メールグループ。
サブカテゴリ	イベントのサブカテゴリ分類。設定イベントのカテゴリは、コントローラーアクティビティやコントローラーの検証といったサブカテゴリで構成されています。さまざまなサブカテゴリの詳細については、ポリシーの表示を参照してください。
ポリシーあたりのイベント数	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

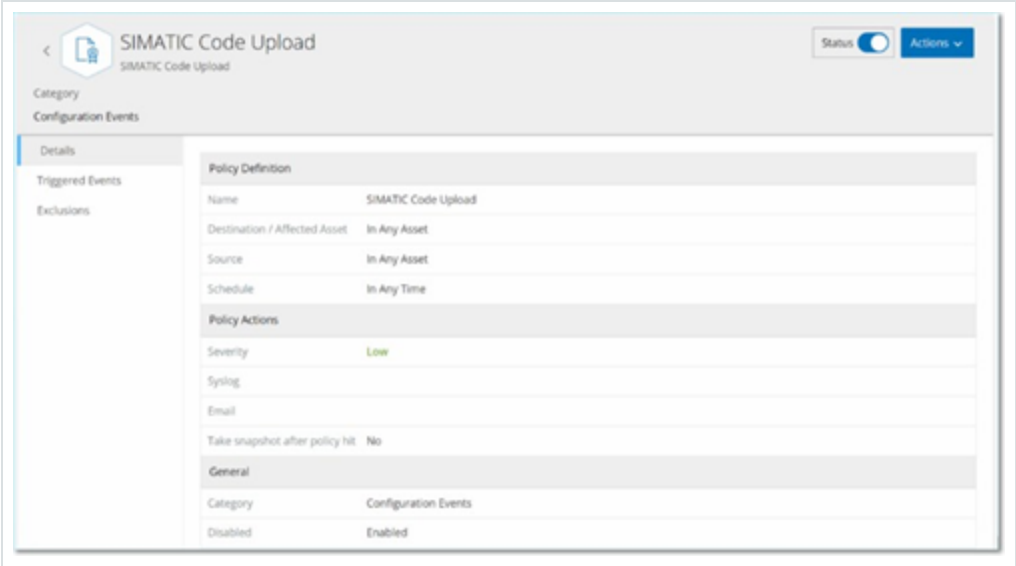
ポリシーの [ポリシーの詳細] 画面に、ポリシーに関する追加の詳細が表示されます。このページには、ポリシーによってトリガーされたイベントとポリシー条件がすべて一覧表示されます。

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] ページが表示されます。



> 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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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。

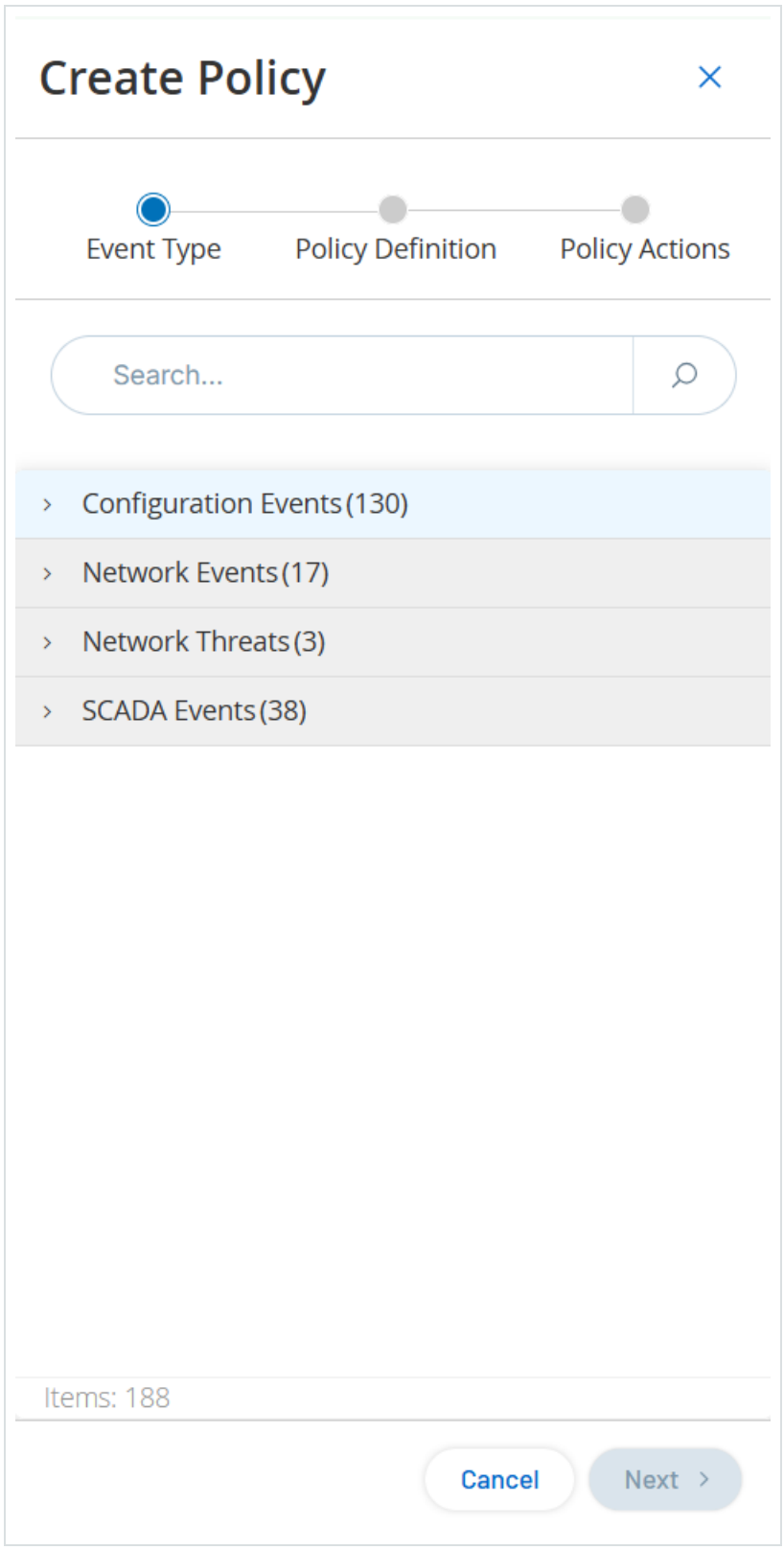
既存のポリシーと同様のパラメーターで新しいポリシーを作成したい場合は、元のポリシーを複製して必要な変更を行うことができます。ポリシーの作成のセクションを参照してください。

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

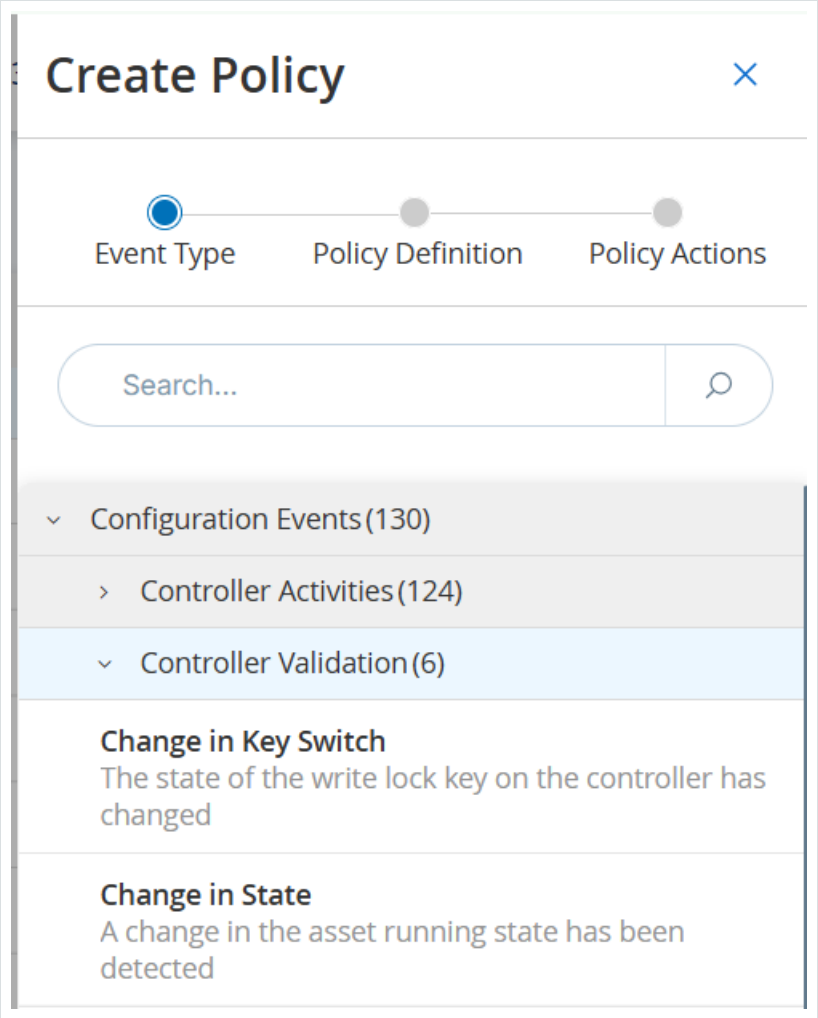
1. [プロパティ] 画面で、[ポリシーの作成] をクリックします。

   [ポリシーの作成] ウィザードが開きます。

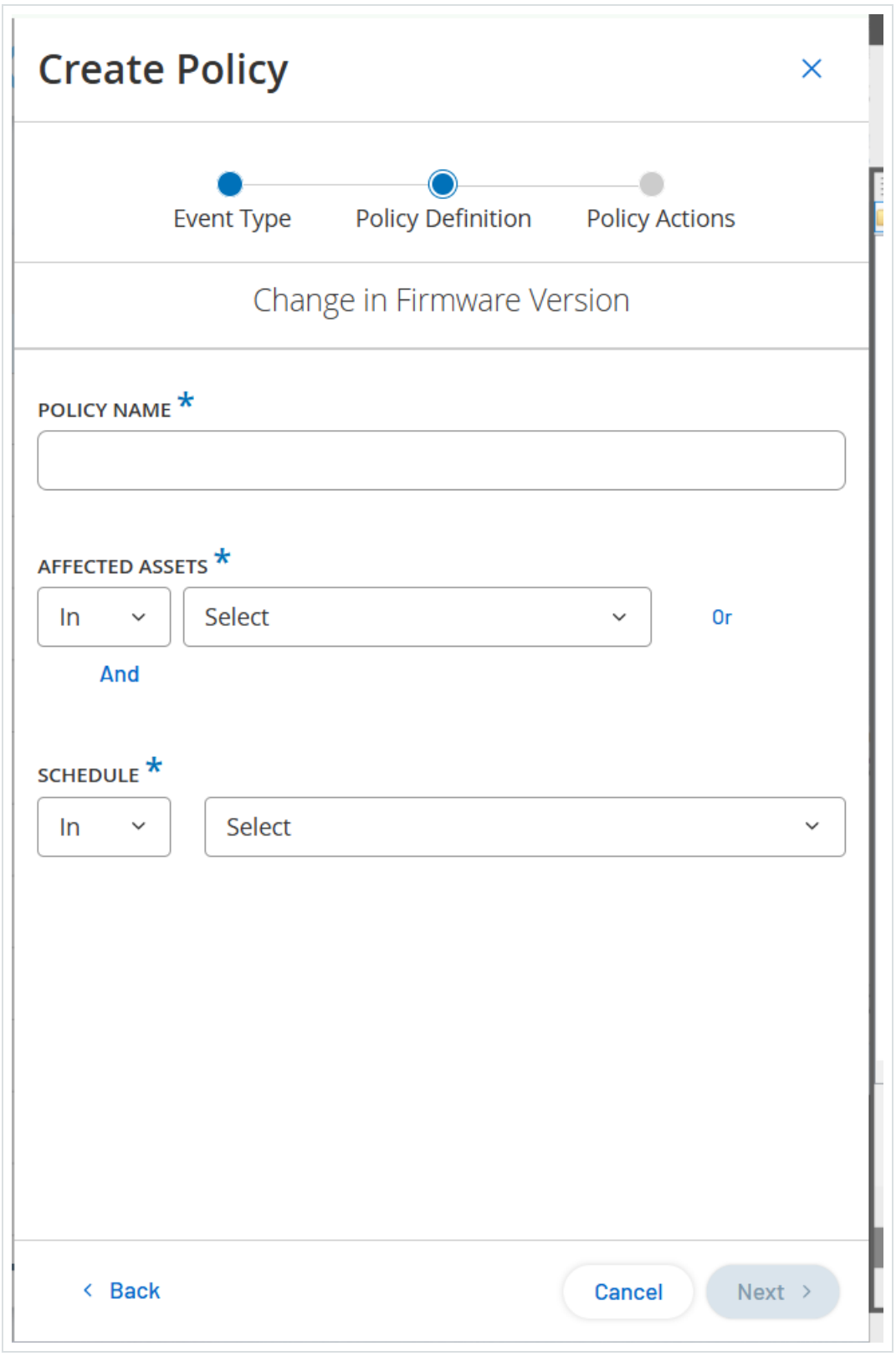

Create Policy
Event Type
Policy Definition
Policy Actions
Search...
Configuration Events (130)
Network Events (17)
Network Threats (3)
SCADA Events (38)
Items: 188
Cancel
Next

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。


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
POLICY NAME *
AFFECTED ASSETS *
In
Select
Or
And
SCHEDULE *
In
Select
Back
Cancel
Next

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。

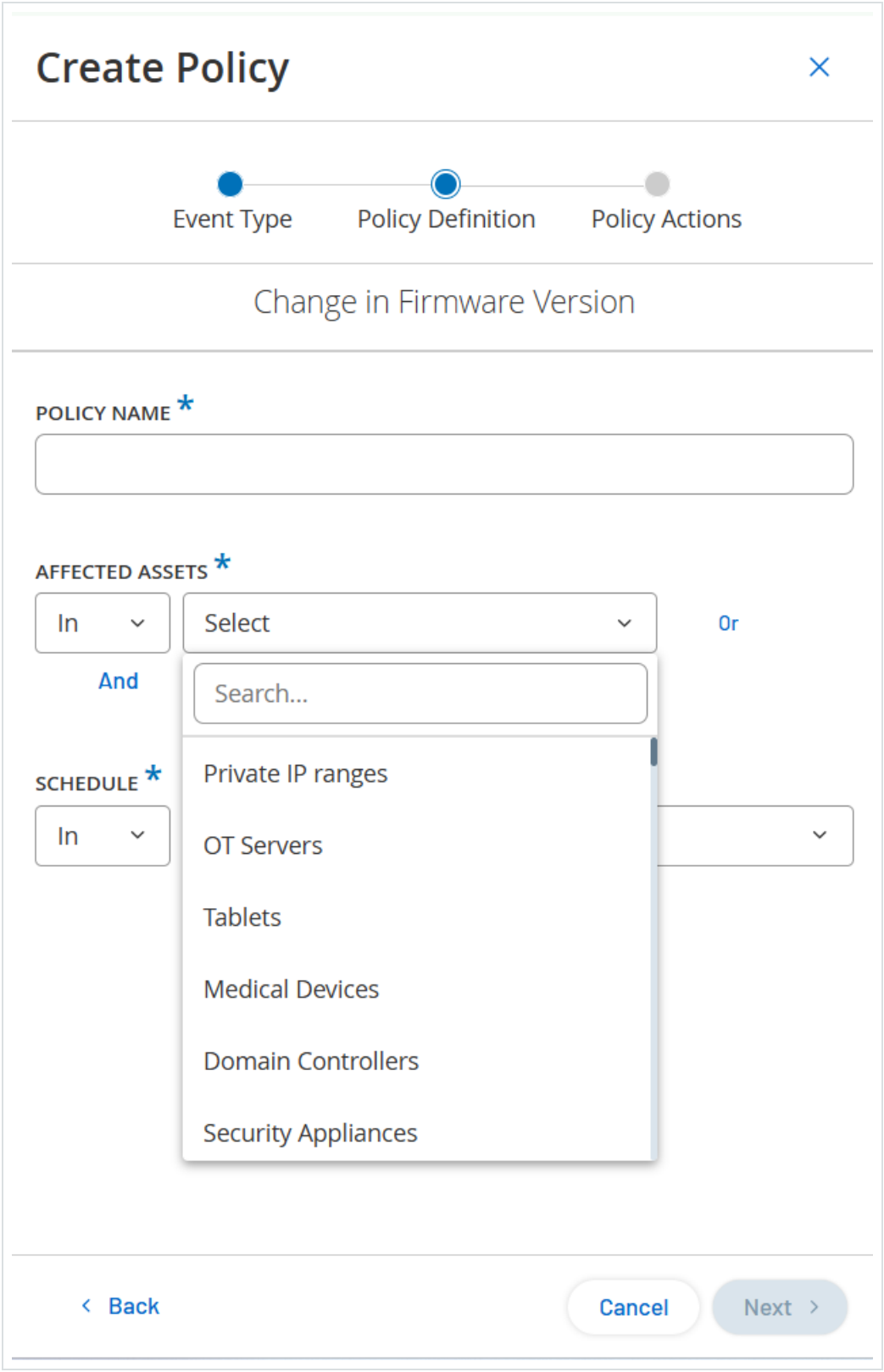
   > 注意: 侵入検知システム (IDS) イベントの [ソース] および [デスティネーション] の資産グループを編集することはできません。

   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 [含まれる] (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 [含まれない] 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。

      > 注意: すべての資産グループの中から選択することができますが、ルールセットに次の資産プロパティのいずれかを持つ動的資産グループは除きます。
      > - リスクスコア
      > - バックプレーン名
      > - ソース
      > - タグ
      > - ハードウェアの状態
      > - ライフサイクルの状態
      > - 代替製品


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
POLICY NAME *
AFFECTED ASSETS *
In
Select
Or
And
Search...
Private IP ranges
OT Servers
Tablets
Medical Devices
Domain Controllers
Security Appliances
SCHEDULE *
In
Back
Cancel
Next

c. 目的の要素を選択します。

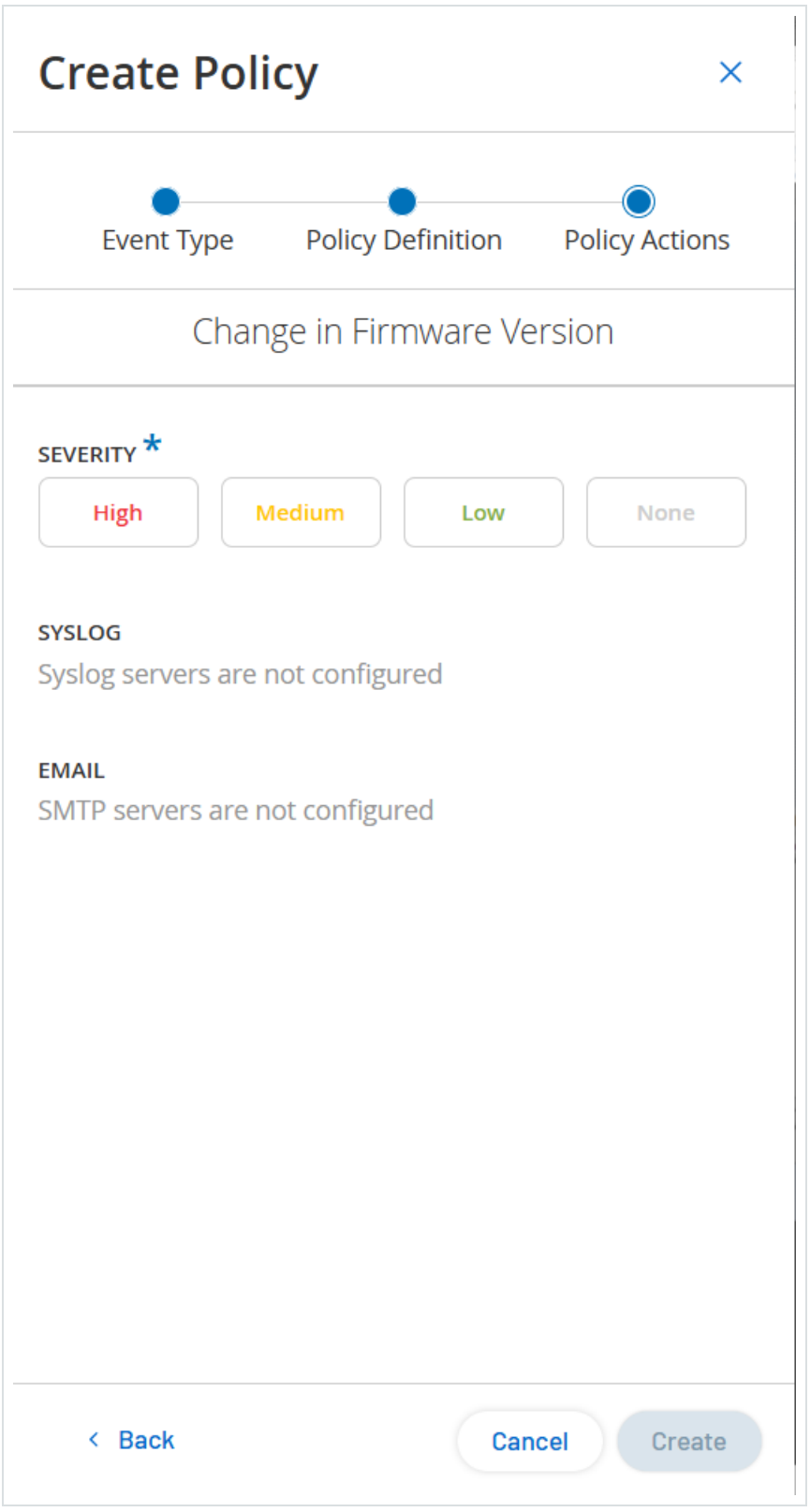
> 注意: 希望するポリシーの適用に最適なグループ化が存在しない場合は、必要に応じて新しいグループを作成できます。グループを参照してください。

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。


Create Policy
Event Type
Policy Definition
Policy Actions
Change in Firmware Version
SEVERITY *
High
Medium
Low
None
SYSLOG
Syslog servers are not configured
EMAIL
SMTP servers are not configured
Back
Cancel
Create

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

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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すべてオーバーライドします。パラメーターの横のチェックボックスを選択し、選択内容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。

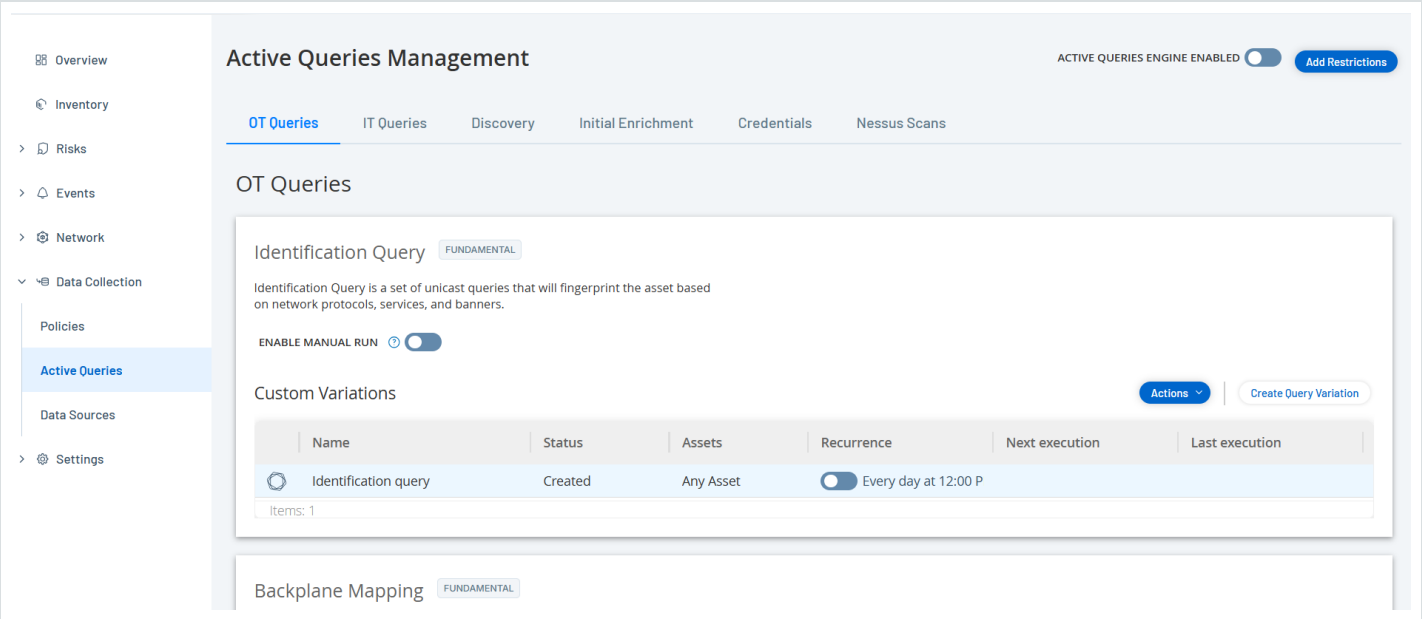
   確認ウィンドウが表示されます。

6. 確認ウィンドウで、[削除] をクリックします。

   OT Security によりシステムから除外が削除されます。

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。

さらに、OT Security には、SNMP クエリを活用するために以下のオプションが用意されています。

- SNMP ポートの状態 – [SNMP ポートの状態] トグルを有効にして資産のネットワークポート状態を取得し、[隣接するものを取得する] トグルを有効にします。
- 隣接するものを取得する – このオプションを有効にすると、OT Security は SNMP を介して隣接するデバイスの MAC アドレスと IP アドレスを収集します。これらの資産をインベントリに追加するには、[設定] > [環境設定] > [ネットワーク定義] > [SNMP 経由で新しい資産を検出] を有効にします。

- 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。

- サブネット自動検出 – SNMP を使用してネットワークデバイスにクエリを実行することで、サブネットを検出します。[インベントリ] ページの [サブネット] 列には、資産の IP アドレスが属しているサブネットが表示されます。特定のサブネット内の資産をフィルタリングすることもできます。
- 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

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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. [データ収集] > [アクティブクエリ] 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) [複数の検出クエリの間隔] ドロップダウンボックスで、検出クエリの間隔 (1 ~ 3 秒) を選択します。
12. (重複するネットワークのみ) [関連するセンサー] ボックスで、関連するセンサーを選択します。
13. [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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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。

注意: 検出 (ICMP) クエリとオープンポートチェック (資産強化) クエリには制限は適用されません。

制限を追加する手順

1. データ収集] > [アクティブクエリ] 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。

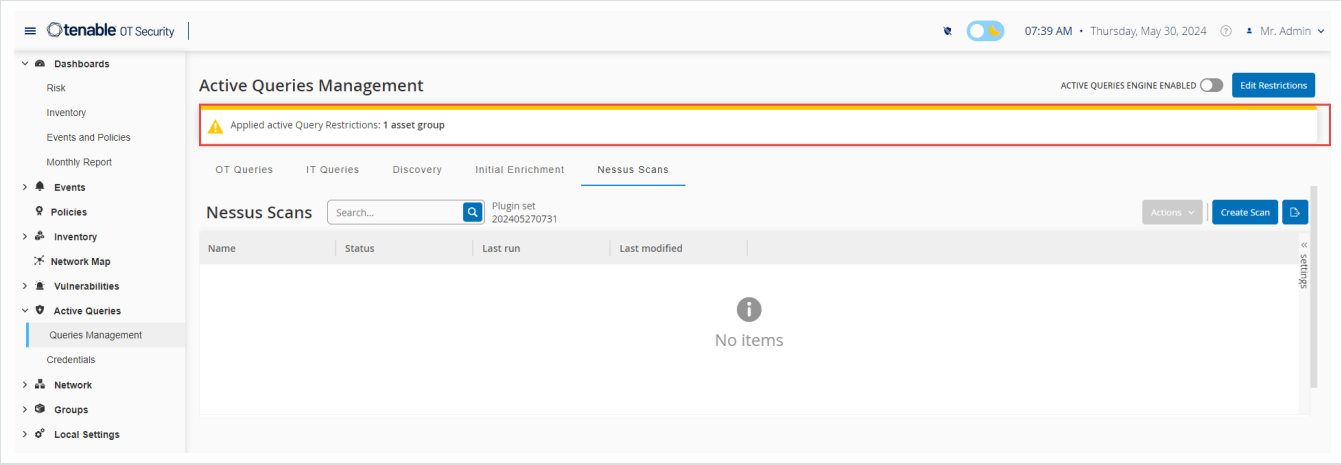
> 注意: 検索ボックスを使用して、特定の資産グループを検索できます。

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

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

クエリの詳細を編集する方法

1. データ収集] > [アクティブクエリ] 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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー

1. データ収集] > [アクティブクエリ] 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 OT Security ユーザーロール: 管理者、スーパーバイザー

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. データ収集] > [アクティブクエリ] 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。

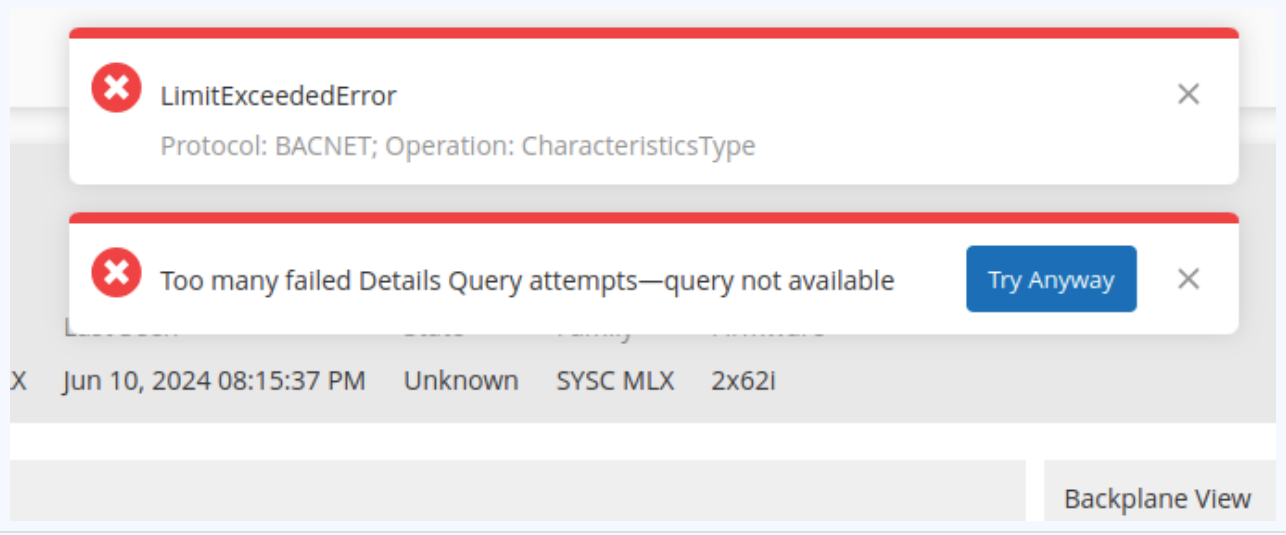
   - クエリを右クリックし、[今すぐ実行] を選択します。
   - [アクション] メニューで、[今すぐ実行] をクリックします。

   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。

   OT Security により、選択したクエリが実行されます。

   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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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. データ収集] > [アクティブクエリ] 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、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。

検出クエリの種類

OT Security は、さまざまなネットワークやデバイスタイプでデータ収集を行うための資産検出に、以下のクエリを使用します。

クエリのタイプ	説明
SnmpType (SNMP クエリ)	スイッチやルーターなど、管理対象のネットワークデバイスからのシステムデータの収集を標準化します。このクエリは、Simple Network Management Protocol (SNMP) を使用して、ハードウェアの詳細、インターフェースのステータス、基本的なシステム設定を取得します。
ArpType (レイヤー 2 ARP ブロードキャスト)	Layer 2 の Address Resolution Protocol (ARP) ブロードキャストを使用して、ローカルネットワークセグメント上のアクティブなデバイスを検出します。これは、ゲートウェイを越えて通信していない近隣の資産を特定す

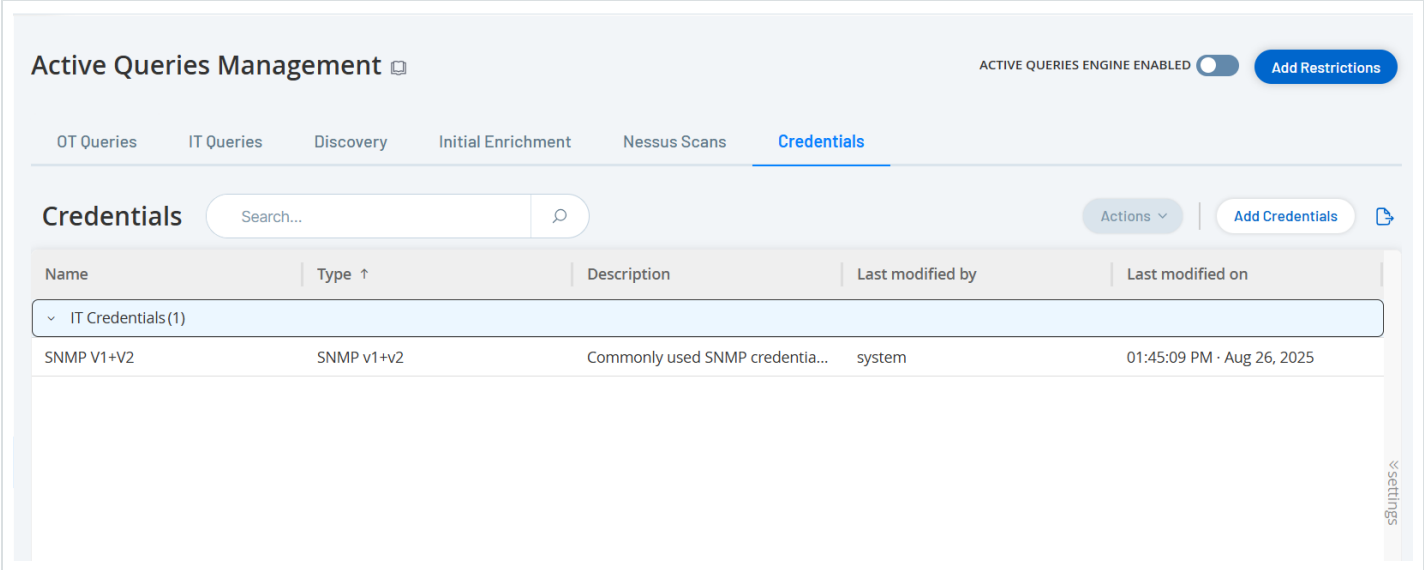
	るために重要です。
IdentificationType (識別クエリ)	デバイスに対して基本的な識別情報を照会することで、主要なフィンガープリンティングツールとして機能します。このクエリは、製造元、モデル、ファームウェアバージョンを取得し、ベースラインの資産プロファイルを確立します。
CharacteristicsType (詳細クエリ)	独自の産業用プロトコルを使用して、より深いレベルのメタデータを取得します。このクエリは、標準的な識別クエリでは取得できない詳細なハードウェアおよびソフトウェア情報を提供します。
BpScanType (バックプレーンスキャン)	モジュール型ハードウェアにおいて、物理シャーシ上のすべてのモジュール、カード、サブコンポーネントを列挙します。このクエリは、PLC やコントローラーの内部アーキテクチャ全体を把握するために使用します。
RunStatusType (コントローラー状態クエリ)	PLC、IED、コントローラーの動作モードを監視します。たとえば、RUN、STOP、FAULT といったモードがあります。このクエリは、プロセスがアクティブかどうか、またはデバイスが脆弱なプログラミング状態に移行しているかどうかを判断する上で重要です。
NbstatQueryType (NetBIOS 検出)	NetBIOS ネームサービスを照会して、Windows ベースのシステムと互換性のあるその他のデバイスを特定します。このクエリは、ローカルサブネットにある資産のホスト名とワークグループ情報を解決するために使用します。
WmiType (WMI 詳細クエリ)	認証済みの Windows Management Instrumentation (WMI) を使用して、Windows エンドポイントの詳細な監査を実行します。このクエリは、インストールされているソフトウェア、OS パッチ、アクティブユーザー、システム修正プログラムに関する正確なデータを収集するために使用します。
WmiUsbType (WMI USB または HID クエリ)	接続された物理周辺機器の監査に特化した WMI リクエスト。このクエリは、サムドライブなどのリムーバブルメディアや HID デバイスを検出して記

	録します。こうしたデバイスは、エアギャップ環境にマルウェアを持ち込む一般的な経路となります。
DnsType (DNS ルックアップ)	設定済みの DNS サーバーを使用して、IP アドレスを完全修飾ドメイン名 (FQDN) に解決します。これにより、管理コンソール内で、人間が識別しやすいネットワーク名で資産が表示されます。

認証情報

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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. [データ収集] > [アクティブクエリ] に移動します。

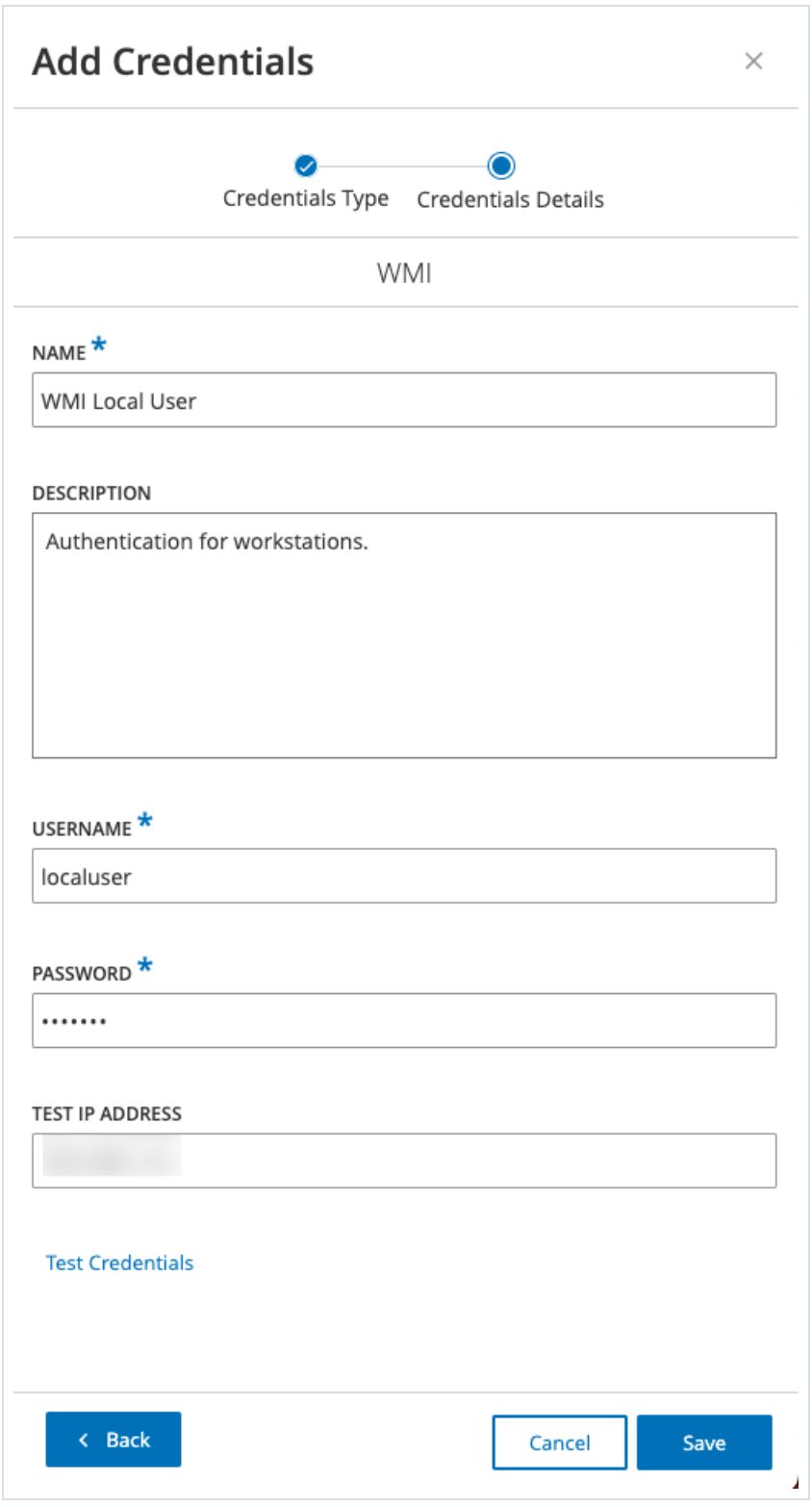
   [アクティブクエリ管理] ページが表示されます。

2. [Credentials] (認証情報) タブをクリックします。

   [認証情報] ページが表示されます。

3. 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。


Add Credentials
Credentials Type
Credentials Details
WMI
NAME *
WMI Local User
DESCRIPTION
Authentication for workstations.
USERNAME *
localuser
PASSWORD *
TEST IP ADDRESS
Test Credentials
Back
Cancel
Save

4. [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

5. [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。

6. 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

7. [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。
8. (重複するネットワークのみ) [複製 (センサー)] ボックスで、関連するセンサーを選択します。
9. [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. [データ収集] > [アクティブクエリ] 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. [Credentials] (認証情報) タブをクリックします。

   [認証情報] ページが表示されます。
3. 次のいずれかを行います。
   - 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。
4. 必要に応じて詳細を変更します。
5. [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. [データ収集] > [アクティブクエリ] 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. [Credentials] (認証情報) タブをクリックします。

   [認証情報] ページが表示されます。

3. 次のいずれかを行います。

   - 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。

   OT Security により、選択した認証情報が削除されます。

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

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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。

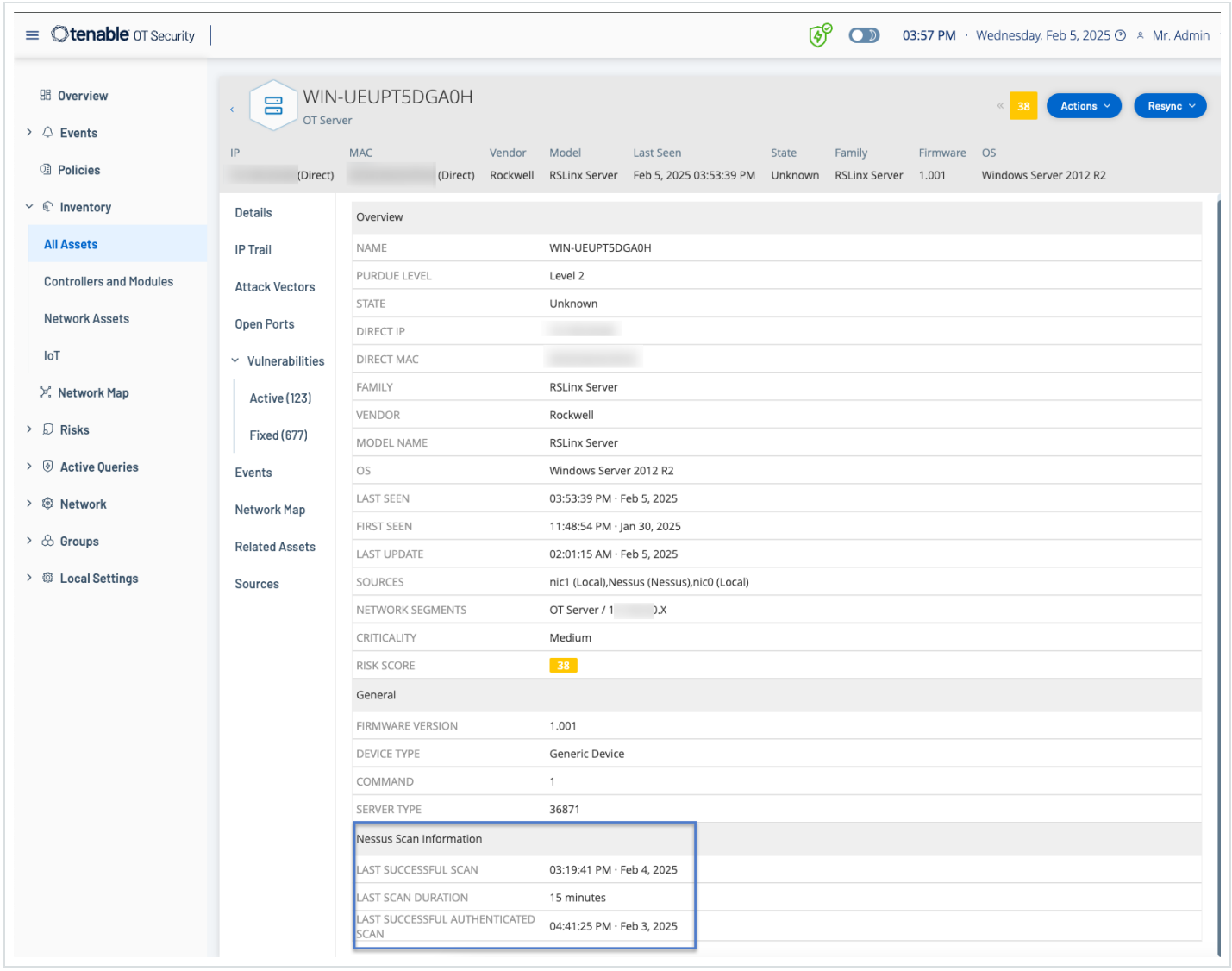
OT Security は、指定された CIDR 内の応答する資産に対してスキャンを実行します。ただし、OT デバイスを保護するために、OT Security は特定の範囲 (PLC 以外) で確認されたネットワーク資産のみをスキャンします。OT Security は、スキャンからエンドポイントタイプの資産を除外します。

OT Security 4.1 以降では、以下のオプションを使用して新しいスキャンを作成できます。

- 徹底的なテストを実行する – このオプションでは、Nessus はプラグインを含む詳細なスキャンを実行できます。これにより、スキャンにかかる時間が長くなる可能性がありますが、JAR ファイルやインストールされている Python ライブラリなど、より詳細な情報を発見するのに役立ちます。
- 高い冗長性の処理 - このオプションにより、スキャンは脆弱性に関する追加の詳細情報を提供できるようになります。この情報を使用してスキャン検出結果のトラブルシューティングを行うことができます。また、このオプションにより、Attack Path Analysis は Nessus スキャン接続データを活用できます。
- ネットワークタイムアウト (秒単位) – ホストからの応答を取得するまで Nessus が待機しなければならない最大時間。低速ホストでスキャンしている場合は、秒数を増やすことができます。デフォルトは 15 秒です。
- ホストあたりの最大同時チェック数 – Nessus がホストに対して実行する必要があるチェックの最大数。デフォルトのチェック数は 2 です。
- スキャンあたりの最大同時ホスト数 – Nessus が同時にスキャンできるホストの最大数。デフォルトのホスト数は 10 です。

認証スキャンの Nessus スキャン情報には、次の詳細が含まれます。

- 最後の正常なスキャン
- 最後のスキャン所要時間
- 最後の正常な認証スキャン



Nessus スキャン情報は次のことに役立ちます。

- 評価済み資産と未評価の資産を把握する。
- 資産が認証スキャンと非認証スキャンのどちらの対象になっているのかを把握する。
- スキャンと脆弱性管理に関するベストプラクティスを実行する。たとえば、Windows、Linux を実行している IT タイプの資産に対して脆弱性評価スキャンを実行できます。認証情報の有無にかかわらず、スキャンは組織のどの程度のアタックサーフェスが内部と外部の両方で露出されているかを評価するのに役立ちます。

OT Security の Nessus スキャンは、Tenable Nessus、Tenable Security Center、Tenable Vulnerability Management の基本ネットワークスキャンと同じポリシー設定を使用します。唯一の違いは、OT Security のパフォーマンスオプションです。以下は、OT Security の Nessus スキャンのパフォーマンスオプションです。これらのオプションは、[インベントリ] > [すべての資産] ページから起動する [Nessus 基本スキャン] にも適用されます。

- 同時に存在するホスト 5 個 (最大)
- ホストあたりの同時チェック 2 件 (最大)
- ネットワーク読み取りのタイムアウト 15 秒

> 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。

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. [データ収集] > [アクティブクエリ] に移動します。

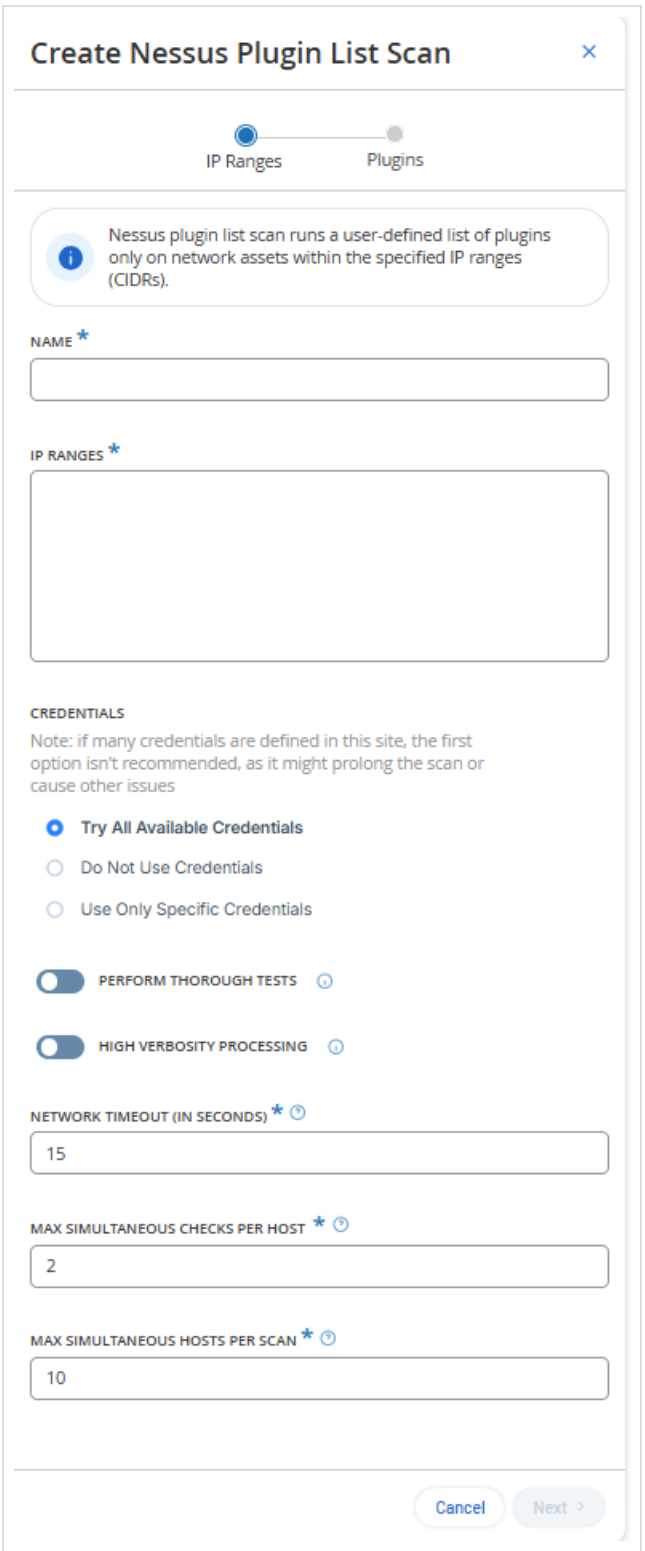
   [アクティブクエリ管理] ページが表示されます。

3. [Nessus スキャン] タブをクリックします。

   [Nessus スキャン] ページが表示されます。

4. 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。


Create Nessus Plugin List Scan
IP Ranges
Plugins
Nessus plugin list scan runs a user-defined list of plugins only on network assets within the specified IP ranges (CIDRs).
NAME *
IP RANGES *
CREDENTIALS
Note: if many credentials are defined in this site, the first option isn't recommended, as it might prolong the scan or cause other issues
Try All Available Credentials
Do Not Use Credentials
Use Only Specific Credentials
PERFORM THOROUGH TESTS
HIGH VERBOSITY PROCESSING
NETWORK TIMEOUT (IN SECONDS) *
15
MAX SIMULTANEOUS CHECKS PER HOST *
2
MAX SIMULTANEOUS HOSTS PER SCAN *
10
Cancel
Next

> 注意: 画像は新しい Nessus スキャンを作成するためのデフォルト値を示しています。デフォルト値でスキャンを実行する場合、スキャンはそれ以前のスキャンと同じ設定で実行されます。

5. [名前] ボックスに Nessus スキャンの名前を入力します。
6. [IP 範囲] ボックスに、IP または CIDR の範囲を入力します。
7. 次のいずれかのオプションを選択して、Nessus スキャンの認証情報を割り当てます。
    - 認証情報を使用しない - 非認証スキャンを実行する場合は、このオプションを選択します。

      > ヒント: 複数の設定済みの認証情報がある場合、これを選択するとスキャンが長くなる可能性があるため、このオプションをスキップしてください。

    - 利用可能なすべての認証情報を試す – スキャンで利用可能なすべての認証情報を試す場合は、このオプションを選択します。
    - 特定の認証情報のみを使用する
        a. [特定の認証情報のみを使用する] を選択した場合は、ICP で定義されているすべての認証情報のリストから必要な認証情報を選択します。
8. (オプション) [徹底的なテスト] トグルをクリックして、詳細スキャンを有効にします。

> 注意: [徹底的なテスト] オプションには、スキャン時間が長くなる可能性のあるプラグインが含まれますが、JAR ファイルやインストールされている Python ライブラリなど、より詳細な情報を Nessus スキャンが発見するのに役立ちます。

9. (オプション) [より高い冗長性] トグルをクリックしてスキャンを有効にし、脆弱性に関する追加の詳細を提供します。

> 注意: [より高い冗長性] を有効にすることにより、スキャンは脆弱性に関する追加の詳細情報を提供します。これを、スキャン検出結果のトラブルシューティングに役立てることができます。また、このオプションにより、Attack Path Analysis は Nessus スキャン接続データを活用できます。

10. [ネットワークタイムアウト (秒単位)] ボックスで、ホストからの応答を取得するまで Nessus が待機しなければならない最大時間を入力します。低速ホストでスキャンしている場合は、秒数を増やすことができます。デフォルトのタイムアウトは 15 秒です。

11. [ホストあたりの最大同時チェック数] に、Nessus がホストに対して実行する必要があるチェックの最大数を入力します。デフォルトのチェック数は 2 です。

12. [スキャンあたりの最大同時ホスト数] ボックスで、Nessus が同時にスキャンできるホストの最大数を入力します。デフォルトのホスト数は 10 です。

13. [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。

14. [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。

15. [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。

データソース

OT Security の [データソース] セクションには、次の設定ページが含まれます。

- 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。
- エージェント – OT エージェントを作成して、センサーをインストールできないリモートの Windows マシンをスキャンします。OT エージェントを参照してください。
- IoT コネクタ – すべての管理対象モノのインターネット (IoT) デバイスをそれぞれのアプリケーションサーバーにマッピングします。IoT コネクタの管理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。
- 手動アップロード
  - CSV を使用した資産詳細の更新 – CSV テンプレートを使用して資産の詳細を更新します。[CSV を使用した資産詳細の更新] を参照してください。
  - 手動による資産の追加 – 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。
  - SCD ファイル – Substation Configuration Description (SCD) ファイルを OT Security にアップロードして、資産に対する可視性、IEC 61850 設定、お使いの環境に関するセキュリティインサイトを取得します。SCD ファイルを参照してください。
  - Rockwell プロジェクトファイル - `Rockwell .L5X` ファイルをアップロードすることで、資産を作成し、資産の詳細を充実させ、エアギャップ環境や可視性が制限された環境で資産間の関係を構築できます。Rockwell プロジェクトファイル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。

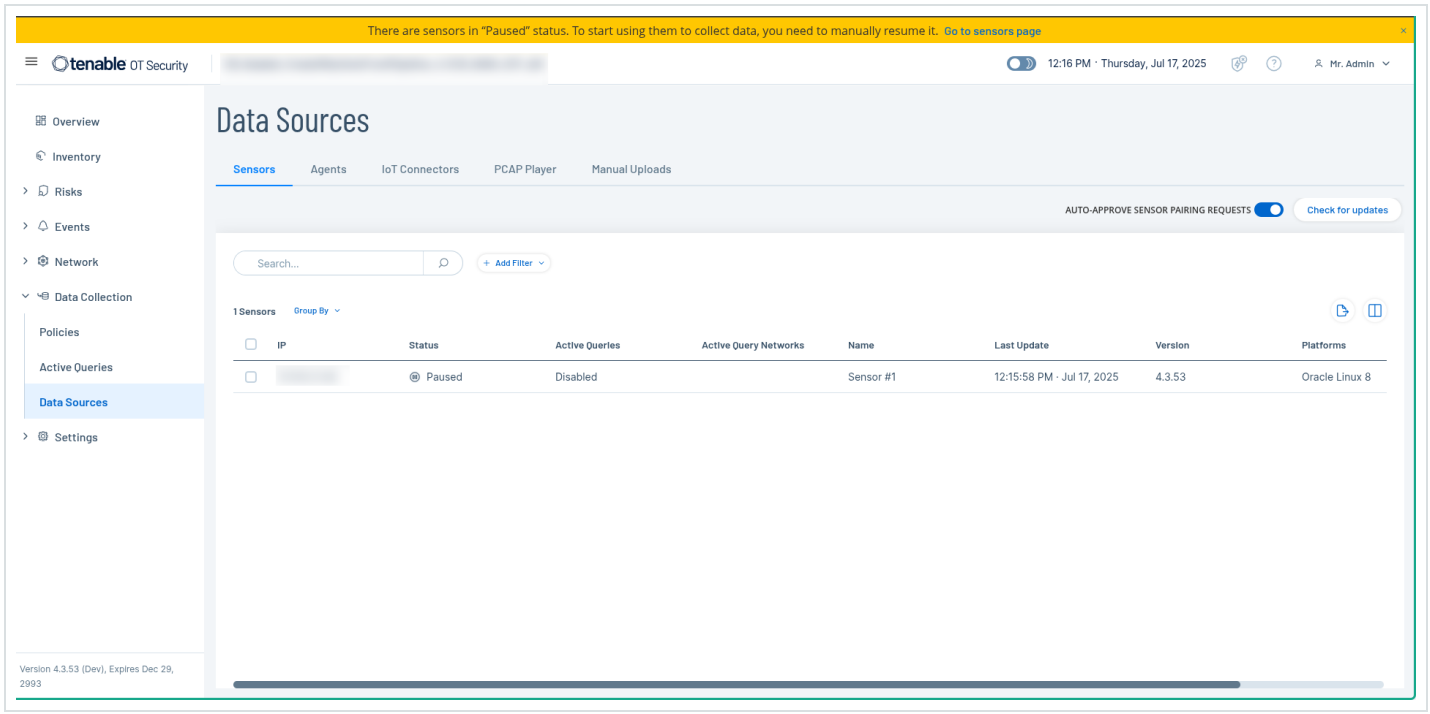
> 注意: ICP とペアリングできるセンサーの数に制限はありませんが、アプライアンスごとに合計 SPAN (Switched Port Analyzer) トラフィック量に上限があります。たとえば、10 のセンサーそれぞれで 10 ~ 20Mbps の速度で送信できますが、トラフィック全体で ICP の制限を超えてはなりません。詳細について

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

必要な OT Security ユーザーロール: 管理者、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

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



[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)]、[承認待ち]、[切断]、また

	は[一時停止]。 重要: ペアリングが完了すると、すべてのセンサーのステータスが[一時停止]と表示されます。 • 認証されたセンサーのステータスを変更するには、次の手順を行います。OT Security でセンサーを右クリックし、ステータスを[一時停止]から[接続済み]に変更してアクティブにします。 • 認証されていないセンサーのステータスを変更するには、次の手順を行います。Tenable Core + OT Security センサーで、[OT Security センサー] > [ペアリング情報] セクションに移動し、[データ転送の再開] をクリックして[接続ステータス]を変更します。
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)。

受信するセンサーペアリングリクエストを手動で承認

必要な OT Security ユーザーロール: 管理者

[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、受信するセンサー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。

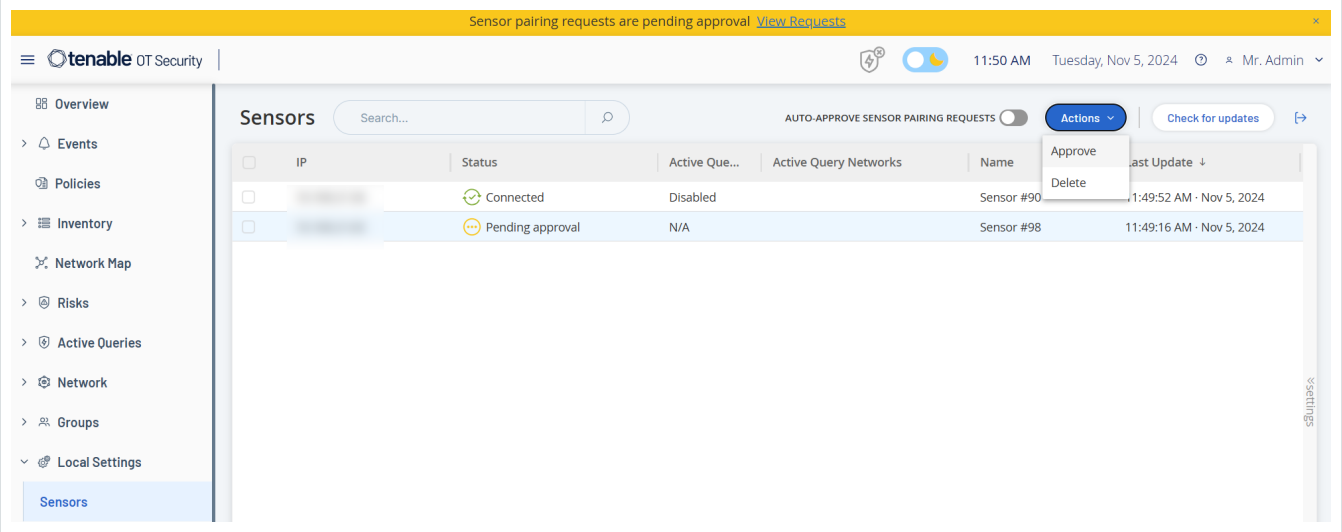
センサーペアリングリクエストを手動で承認する方法

1. [データ収集] > [データソース] ページで、[センサー] タブをクリックします。

   [センサー] ページが表示されます。

2. ステータスが [承認待ち] 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

必要な OT Security ユーザーロール: 管理者

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。

アクティブクエリを設定する方法

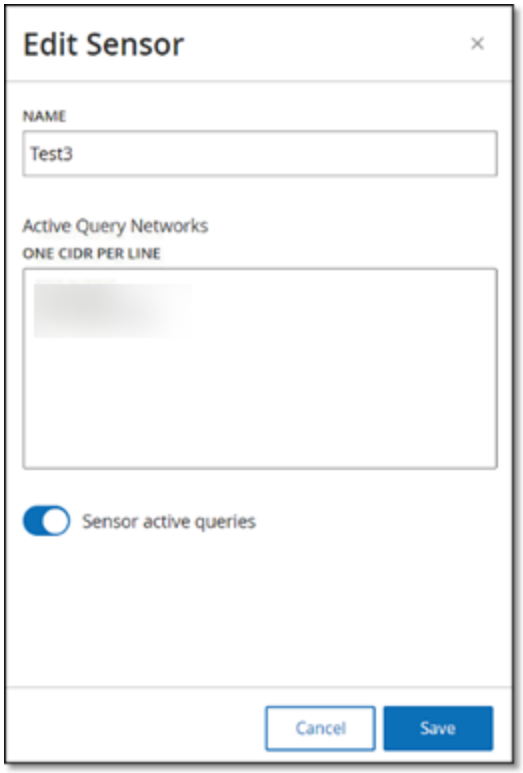
1. [データ収集] > [データソース] ページで、[センサー] タブをクリックします。

   [センサー] ページが表示されます。

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。

   > 注意: センサーが重複するネットワークの一部である場合、重複するネットワークの IP アドレスが [アクティブクエリネットワーク] ボックスに表示され、編集不可になっています。

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

> 必要な OT Security ユーザーロール: 管理者

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。

> 注意: OT Security は、一元化された更新にオフライン ISO を使用しています。ICP に取り付けられているすべての認証されたセンサーを一元更新するには、ICP の `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` に ICP / センサーオフライン ISO を配置します。

> 注意: (OT Security EM ユーザーのみを対象としています)。OT Security は、一元化された更新にオフライン ISO を使用しています。EM を介して ICP に取り付けられているすべての認証されたセンサーを一元更新するには、EM の `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` に EM オフライン ISO を配置します。

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。ペアリングに関する詳細は、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. [データ収集] > [データソース]ページで、[センサー]タブをクリックします。

   [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。

OTエージェント

OT エージェントは、リモート Windows マシンにインストールできるソフトウェアコンポーネントです。センサーのインストールが不可能または実際的でない環境の OT Security 資産をアクティブに照会して検出できます。OT エージェントは、アクティブクエリを活用して、[監視対象ネットワーク] にリストされている複製ネットワークやアクティブクエリネットワークをスキャンします。これにより、Windows ベースのゲートウェイ、エンジニアリングワークステーション、またはヒューマンマシンインターフェース (HMI) で実行されているエージェントが、重要な OT/IoT およびネットワーク上の組み込みデバイスを特定できます。

OT エージェントによって検出される各 OT 資産は、その検出ソースとなった該当エージェントに関連付けられます。これにより、ネットワーク内の資産特定のトレーサビリティが得られます。

ネットワークをスキャンするには、まず OT エージェントをインストールして設定します。以下のセクションでは、OT エージェントをインストールして設定し、OT エージェントを使用してスキャンを実行する方法について説明します。

1. OT エージェントのダウンロード
2. OT エージェントのインストール
3. OT エージェントの設定
4. スキャンの実行

OT エージェントの表示

[OT エージェント] ページは、ネットワークをモニタリングするためにユーザーがデプロイするエージェントをモニタリングおよび設定するための中央ハブとして機能します。

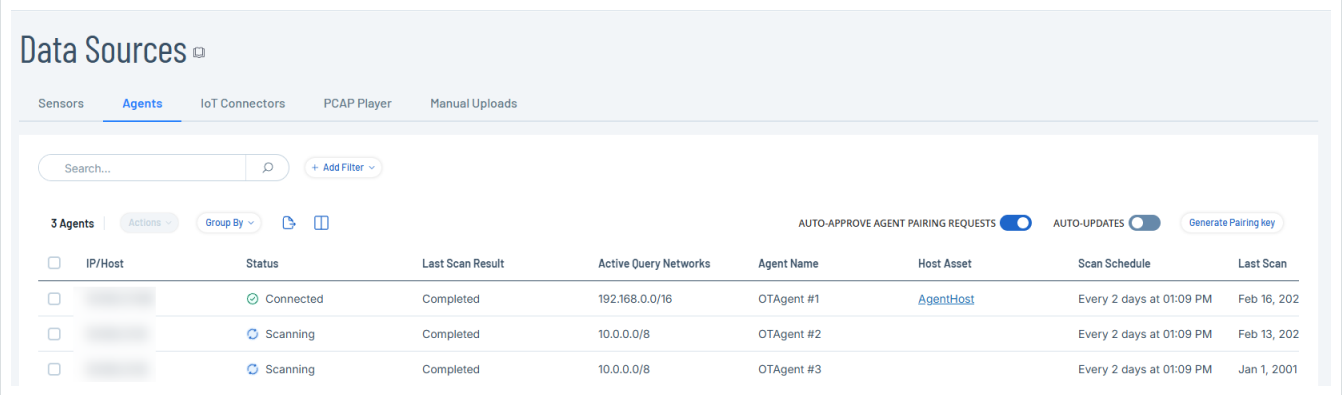
[OT エージェント] ページにアクセスする方法

1. 左側のナビゲーションメニューで、[データ収集] > [データソース] をクリックします。

   [データソース] ページが表示されます。

2. [エージェント] タブをクリックします。

   [エージェント] ページが表示され、デプロイした OT エージェントのリストが表示されます。



[エージェント] ページには、次の詳細が表示されます。

パラメーター	説明
IP/ホスト	OT エージェントがインストールされているマシンの IPv4 アドレス。
ステータス	エージェントのステータス。 • 接続済み • 一時停止済 • 切断 • 保留中の設定 • 承認待ち • 接続準備中 • 接続の待機中 • 更新中 • スキャン中
最終スキャン結果	最終スキャンのステータス: 完了または失敗。

アクティブクエリネットワーク	OT エージェントが現在のスキャンでターゲットにしている特定のネットワークセグメント。
エージェント名	OT エージェントに割り当てられた一意の名前。
ホスト資産	ホスト資産の詳細ページへの直接リンク。
スキャンスケジュール	設定されたスキャンの頻度。スケジュールがない場合、列に[無効]と表示されます。
最終スキャン	直近のスキャンが開始された日時。
最終スキャンの所要時間	最終スキャンの完了にかかった時間。
認証情報	エージェントがデバイスをスキャンするために使用する認証情報。
報告された資産	スキャンで検出された資産の数。
エージェントバージョン	OT エージェントのバージョン。
OTD バージョン	OT Discovery エンジンのバージョン。
ホスト OS	ホストマシンのオペレーティングシステム。

OT エージェントのインストール

> 必要な OT Security ユーザーロール: 管理者

Windows マシンに OT エージェントをインストールして、OT 環境をスキャンします。

始める前に

- Tenable ダウンロードポータルから OT エージェントをダウンロードします。
- Windows マシンで管理者のアクセス許可を持っていることを確認します。

注意: ペアリングおよび接続用のデフォルトのポートは、それぞれ 443 および 28306 です。ポートについては、ファイヤーウォールに関する考慮事項を参照してください。

OT エージェントのインストール方法

1. インストールファイル (`Tenable-OT-Agent-version.msi`) を Windows マシンに移します。
2. `.msi` インストールファイルをクリックし、インストールウィザードを開きます。
3. [OT エージェントセットアップウィザード] ウィンドウで、[次へ] をクリックします。

   [ICP 詳細の入力] ウィンドウが表示されます。
4. 次のいずれかを選択します。

   - **ペアリングキーを使用する**

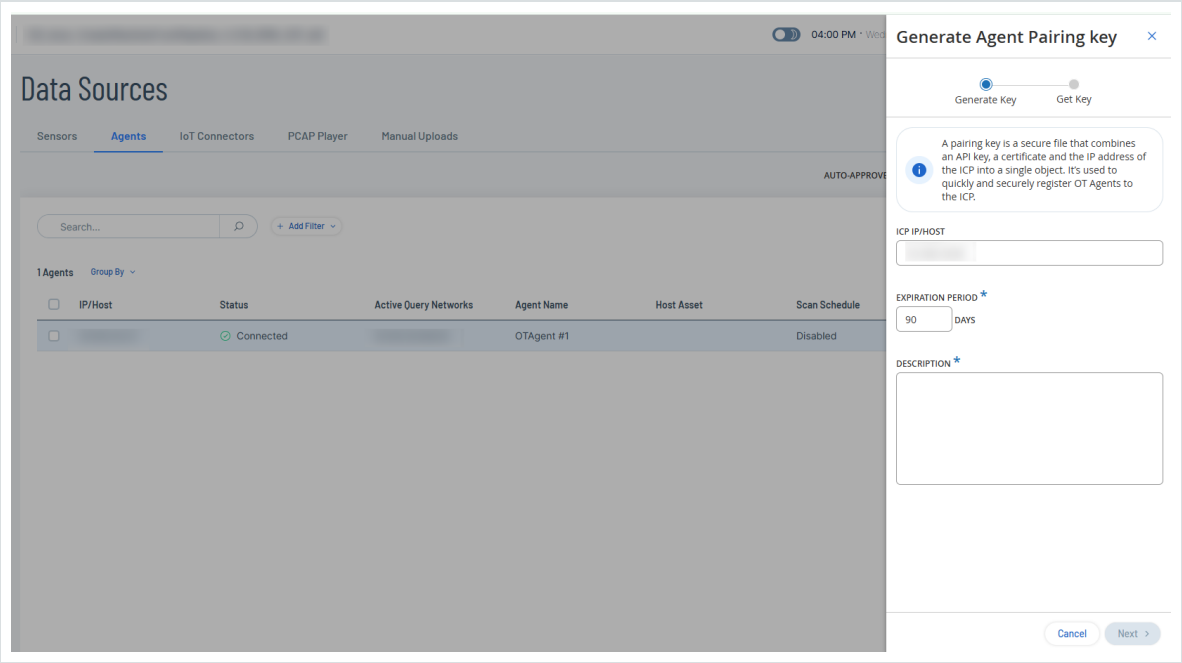
     これはデフォルトのオプションです。このオプションを選択した場合は、次の手順を実行します。

     1. OT Security で、[データ収集] > [データソース] に移動します。

        [データソース] ページが表示されます。
     2. [エージェント] タブをクリックします。

        [エージェント] ページが表示されます。
     3. 右上の [ペアリングキーの生成] をクリックします。

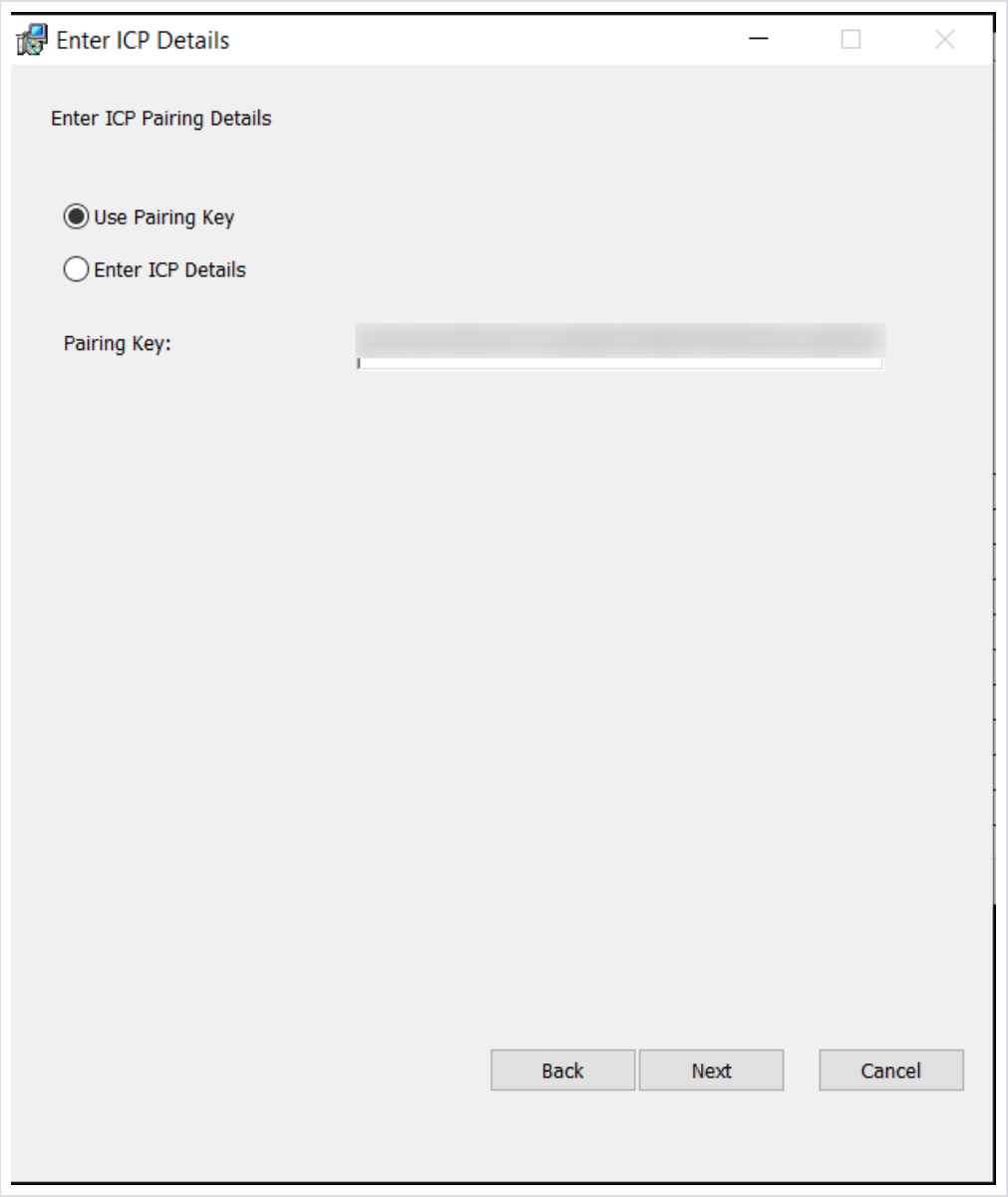
        [エージェントペアリングキーの生成] パネルが表示されます。



4. [ICP IP/ホスト] ボックスに、ICP の IP アドレスまたはホスト名を入力します。
5. [有効期間] ドロップダウンボックスで、デフォルトの 90 日間のままにするか、キーが期限切れになるまでの日数を指定します。
6. [説明] ボックスに、キーの説明を入力します。
7. [次へ] をクリックします。

   OT Security によりペアリングキーが生成されます。
8. ボタンをクリックし、ペアリングキーをコピーします。
9. [完了] をクリックします。

   OT Security によりパネルが閉じます。
10. Windows ホストマシンに戻ります。
11. [ペアリングキー] ボックスに、ICP からコピーしたペアリングキーを貼り付けます。



- ICP 詳細を入力する

  このオプションを選択すると、関連フィールドが表示され、ICP に必要な詳細を入力できます。

  1. [ICP アドレス] ボックスに、ICP の IP アドレスを入力します。
  2. [ICP ユーザー名] ボックスに、ICP マシンの名前を入力します。

3. [ICP パスワード] ボックスに、ICP マシンのパスワードを入力します。
4. [API キー] ボックスに、ICP から生成された API キーを入力します。API キーの生成を参照してください。
5. [証明書フィンガープリント] ボックスに、ICP から生成されたフィンガープリントを入力します。証明書を参照してください。

> 注意: ペアリングキーと証明書は、ペアリングプロセスでのみ必要です。ペアリング完了後、必要に応じてペアリングキーと証明書を削除できます。

5. [次へ] をクリックします。

   [宛先フォルダー] ウィンドウが表示されます。

6. [OT エージェントのインストール先] ボックスで、デフォルトのインストール先のままにするか、OT エージェントをインストールするパスを指定して、[次へ] をクリックします。
7. [インストール] をクリックします。

   インストーラーが OT エージェントをインストールし、OT Security の [エージェント] タブのリストに載せます。この時のステータスは [保留中の設定] です。

8. [終了] をクリックして、インストーラーを閉じます。

> 注意: ペアリングに問題がある場合は、OT エージェントインストールウィザードの [修復] オプションを使用して、ペアリングの詳細を再入力できます。

9. ペアリングリクエストを自動的に承認するには、[エージェントペアリングのリクエストを自動承認する] トグルをクリックして有効にします。

   このオプションが有効になっていない場合は、以下を実行します。

   - 新しく追加された OT エージェントを右クリックします。

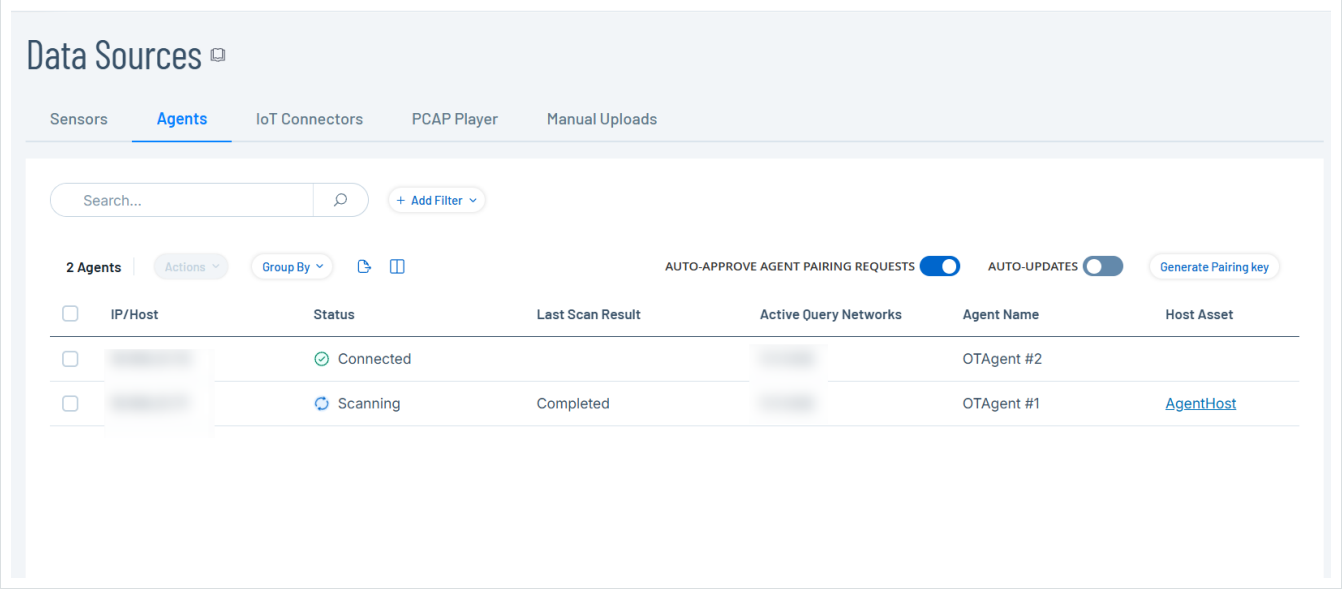
     メニューが表示されます。

- OT エージェントの横にあるチェックボックスを選択します。

  OT Security は、[アクション] > [承認] メニューを有効にします。

10. [承認] をクリックします。

    OT Security はエージェントのペアリングを承認し、ステータスを [保留中の設定] に変更します。



> 注意: OT エージェントを実行する前に、[エージェントペアリングのリクエストを自動承認する] オプションが有効になっている場合でも、OT エージェントの設定が完了していることを確認してください。

次の手順

OT エージェントの設定

OT エージェントの設定

> 必要な OT Security ユーザーロール: 管理者

OT エージェントをインストールした後、その名前を定義し、スキャンするネットワークを指定し、アクティブクエリのスケジュールを設定します。

始める前に

- OT エージェントをインストールします。

OT エージェントの設定方法

1. [エージェント] タブで、次のいずれかを行います。

   - 新しく追加された OT エージェントを右クリックします。

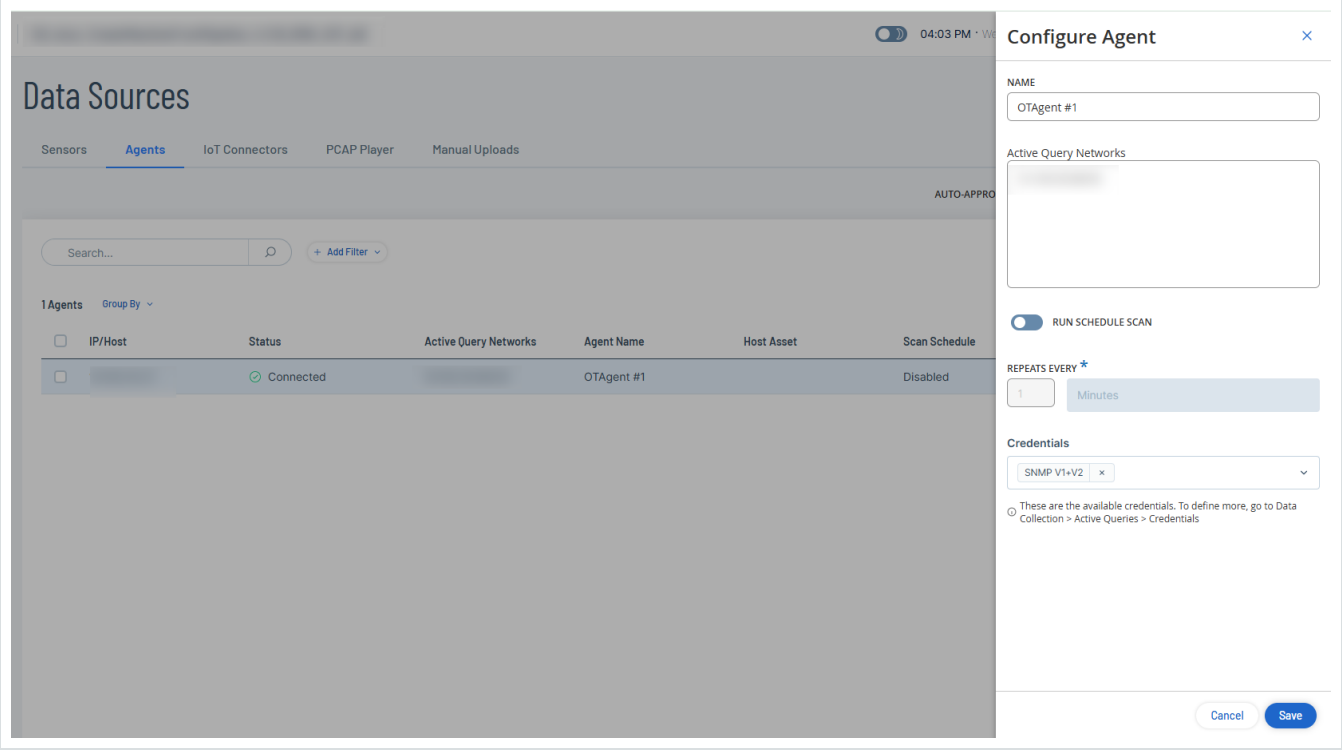
     メニューが表示されます。

   - OT エージェントの横にあるチェックボックスを選択します。

     OT Security は、[アクション] > [設定] メニューを有効にします。

2. [設定] をクリックします。

   [エージェントの設定] パネルが表示されます。



3. [名前] ボックスに、エージェントの名前を入力します。

4. [アクティブクエリ] ボックスに、スキャンするネットワークの IP アドレスを入力します。

> 注意: OT エージェントは、モニタリング対象ネットワーク ([環境設定] > [ネットワーク定義] > [監視対象ネットワーク]) に含まれている、アクティブクエリネットワークの IP アドレスのみをスキャンします。

5. (オプション) スケジュールスキャンを有効にするには、[スケジュールスキャンの実行] トグルをクリックします。

   OT Security は、[繰り返し間隔] ドロップダウンボックスを有効にします。

6. (オプション) 必要に応じて、分、時間、日、週を指定します。

7. [認証情報] ドロップダウンボックスで、必要な認証情報を選択します。

   > 注意: [アクティブクエリ] > [認証情報] で作成した認証情報のみがこのリストに表示されます。詳細は、認証情報 を参照してください。

8. [保存] をクリックします。

   OT Security は、OT エージェントのステータスを [接続済み] に更新します。

次の手順

スキャンの実行

OT エージェントを使用したスキャンの実行

> 必要な OT Security ユーザーロール: 管理者

エージェントスキャンを開始すると、次のアクティブクエリがトリガーされます。

- 検出: 監視対象ネットワークのライブ資産を検出します。
- オープンポートチェック: アクティブクエリクライアントで最も頻繁に使用されるポートをスキャンします。
- 初期強化: Dynamic Fingerprinting Engine (DFE) で新しく検出された資産を特定します。

- OT クエリ: 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。
- IT クエリ: OT Security によりモニタリングされている IT デバイスからデータを取得します。

詳細は、アクティブクエリの管理を参照してください。

エージェントスキャンを実行する方法

1. [データソース] > [エージェント] タブで、次のいずれかを行います。
    - 新しく追加された OT エージェントを右クリックします。

      メニューが表示されます。
    - OT エージェントの横にあるチェックボックスを選択します。

      OT Security により、ヘッダーの [アクション] ボタンが有効になります。

    > 注意: 複数のエージェントのスキャンを開始するには、複数の OT エージェントを選択し、[一括アクション] > [今すぐスキャン] をクリックします。

2. [アクション] > [今すぐスキャン] をクリックします。

    エージェントのステータスが [スキャン中] に変わり、指定されたネットワークでスキャンが開まります。スキャンが完了した後、エージェントテーブルの [報告された資産] 列にあるリンクをクリックすると、[インベントリ] ページでフィルタリングされた結果が表示されます。

スキャンの中止

> 必要な OT Security ユーザーロール: 管理者

進行中のスキャンを停止する必要がある場合は、次のようにします。

1. [データソース] > [エージェント] タブで、次のいずれかを行います。

    - エージェントを右クリックし、[スキャンの中止] を選択します。
    - エージェントの横にあるチェックボックスを選択し、[アクション] > [スキャンの中止] をクリックします。

    OT Security によりスキャンが停止され、[最終スキャン結果] 列に [失敗] と表示されます。

OT エージェントのアップデート

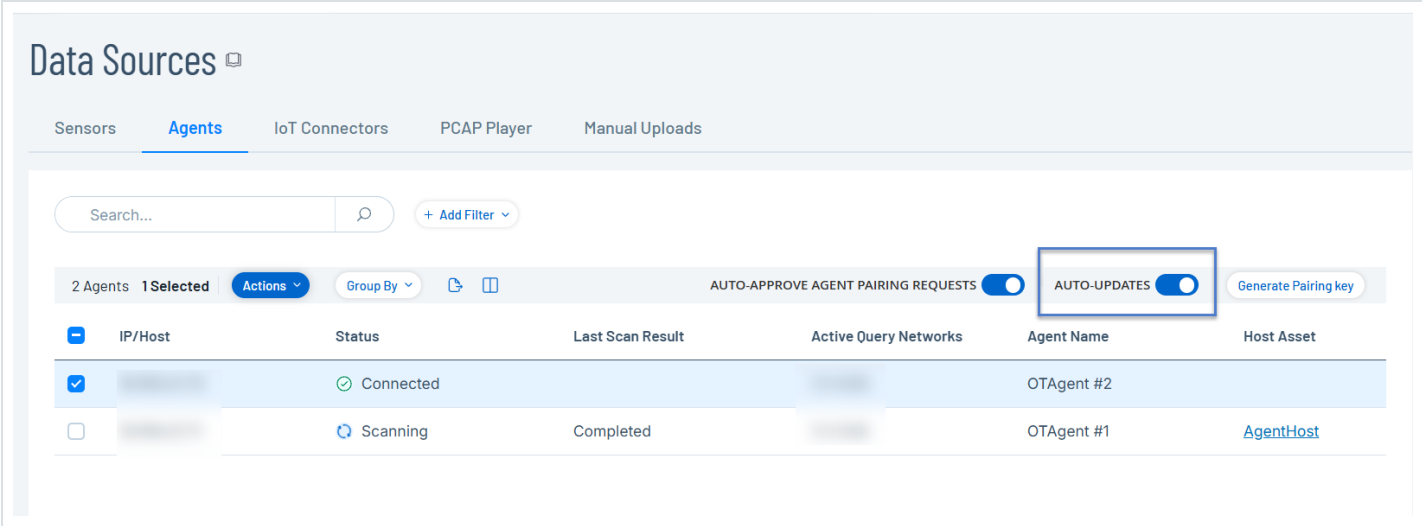
必要な OT Security ユーザーロール: 管理者

ファイルをアップロードするのに必要な **OT Security** ユーザーロール: 管理者、スーパーバイザー、セキュリティアナリスト

OT エージェントは、OT Discovery (OTD) エンジンを使用して環境を能動的にスキャンします。[エージェント] ページから手動または自動で OT Discovery エンジンをアップデートできます。

自動アップデート

ICP の更新がリリースされたときに OTD バージョンを自動的にアップデートするには、[自動アップデート] トグルを有効にします。このトグルはデフォルトでは無効になっています。[自動アップデート] を有効にすると、OT Security は新しいリリースが利用可能になると、接続されたエージェントに最新の OTD エンジンバージョンを自動的にプッシュします。



手動アップデート

公式リリースの合間にOTD エンジンをアップデートする必要がある、または複数のエージェントを同時に一括更新する必要がある場合は、手動アップデートを使用します。

始める前に

- OT Discovery エンジン (OTD) のアップデートにある説明に従い、[システム設定] > [アップデート]> [OT Discovery Engine (OTD) のアップデート] セクションで、OTD ファイルをアップロードします。
- OT エージェントがオンラインで、ステータスが [接続済み] であることを確認します。

OTD エンジンを手動でアップデートする方法

1. 左側のナビゲーションバーで、[データソース] > [エージェント] をクリックします。

   [エージェント] タブが表示されます。

2. エージェントをアップデートするには、以下のいずれかを行います。

   - アップデートするエージェントを右クリックします。

     メニューが表示されます。

   - アップデートするエージェントの横にあるチェックボックスを選択します。

OT Security により [アクション] メニューが有効になります。

> 注意: OTD エンジンを一括でアップデートするには、複数のエージェントを選択してから、[一括アクション] >[アップデート] をクリックします。

3. [アクション] > [アップデート] をクリックします。

   [OTD バージョンのアップデート] ダイアログボックスが表示されます。

4. [アップデート] をクリックして確定します。

   OT Security は OT Discovery エンジンを最新バージョンにアップデートします。

OT エージェントの削除

> 必要な OT Security ユーザーロール: 管理者

Windows マシンから OT エージェントをアンインストールすると、OT Security でエージェントのステータスが [切断] に変更されます。

OT エージェントの削除方法

1. Windows マシンでインストーラーを開き、[削除] をクリックします。
2. ウィザードの手順に従って、エージェントをアンインストールします。

   OT エージェントが Windows マシンからアンインストールされます。

3. OT Security の [データソース] > [エージェント] タブに移動します。

   OT Security はエージェントのステータスを [切断] に変更します。

4. 次のいずれかを行います。

   - 新しく追加された OT エージェントを右クリックします。

     メニューが表示されます。

- OT エージェントの横にあるチェックボックスを選択します。

  OT Security は、[アクション] > [削除] メニューを有効にします。

  > 注意: OT エージェントを一括で削除するには、複数の OT エージェントを選択し、[一括アクション] > [削除] をクリックします。

5. [削除] をクリックします。

   OT Security により OT エージェントが削除されます。

   > 注意: 関連する複製ネットワークがある場合は、エージェントを削除する前に、まずそれらのネットワークを削除する必要があります。

CLI を使用した OT エージェントのインストール

> 必要な OT Security ユーザーロール: 管理者

CLI コマンドを使用して、ペアリングキー、ICP 認証情報、または API キーを使って OT エージェントをインストールできます。CLI で OT エージェントをアンインストールすることもできます。

始める前に

- Tenable ダウンロードポータルから OT エージェントのインストーラーをダウンロードします。

ペアリングキーを使用して OT エージェントをインストールするには、次のコマンドを実行します。

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn PAIRING_KEY="<PairingKey>"
```

各部の説明

- `OtAgentInstaller.msi` はインストールファイルです。
- `PairingKey` は、OT Security の [データ収集] > [データソース] > [エージェント] タブから生成するキーです。

例:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn PAIRING_
KEY="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxoxxxxxxxxxxxx"
```

ユーザー名とパスワードを使用して OT エージェントをインストールするには、次のコマンドを実行します。

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn ICP_ADDRESS="<IpAddress>" ICP_USERNAME="<Username>" ICP_
PASSWORD="<Password>" ICP_FINGERPRINT="<CertFingerprint>"
```

各部の説明

- `OtAgentInstaller.msi` はインストールファイルです。
- `IpAddress` は ICP の IP アドレスです。
- `Username` は ICP にログインするためのユーザー名です。
- `Password` は ICP のパスワードです。
- `CertFingerprint` は OT Security で生成する証明書です。

例:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="XX.XXX.XX.XX" ICP_USERNAME="admin" ICP_
PASSWORD="xxxxxxx" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
```

API キーを使用してインストールするには、次のコマンドを実行します。

```
msiexec.exe /i "<OtAgentInstaller.msi>" /qn ICP_ADDRESS="<IpAddress>" ICP_APIKEY="<APIKey>" ICP_
FINGERPRINT="<CertFingerprint>"
```

(任意のパラメーター) `INSTALLBASE='"<FullDirPath>"'`

各部の説明

- `OtAgentInstaller.msi` はインストールファイルです。
- `IpAddress` は ICP の IP アドレスです。

- APIKey は ICP から生成された API キーです。
- CertFingerprint は ICP から生成された証明書です。
- FullDirPath はインストールディレクトリのパスです。

例 1:

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="XX.XXX.XX.XX" ICP_APIKEY="kxxxxxxxxxxxxxxxx_
xxxxxxxx=" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
```

例 2: INSTALLBASE パラメーターを使用する

```
msiexec.exe /i "OtAgentInstaller.msi" /qn ICP_ADDRESS="xx.xxx.xx.xx" ICP_APIKEY="xxxxxxxxxxxxxxx_
xxxxxxxxxxx=" ICP_FINGERPRINT="XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX"
INSTALLBASE='"C:\Program Files\AAA"'
```

OT エージェントのアンインストール方法

```
msiexec.exe /x "<OtAgentInstaller.msi>" /qn
```

各部の説明

- OtAgentInstaller.msi はインストールファイルです。

OT エージェントのスケジュールスキャンの有効化、無効化、設定

[一括アクション] オプションを使用して、複数の OT エージェントのスケジュールスキャンを同時に有効または無効にします。

始める前に

- OT エージェントがオンラインであり、[ステータス] 列に [接続済み] と表示されていることを確認します。

スケジュールエージェントスキャンで一括アクションを実行する方法

1. [エージェント] テーブルで、スキャン対象の OT エージェントを複数選択します。

   OT Security により、ヘッダーの [一括アクション] ボタンが有効になります。

2. 次のいずれかのオプションを選択します。

一括アクションのオプション	説明
スケジュールスキャンを有効にする	スケジュール設定されたエージェントスキャンを有効にするには、このオプションを選択します。スケジュールスキャンはデフォルトで 1 分ごとに実行されます。
スケジュールスキャンを無効にする	スケジュール設定されたエージェントスキャンを無効にするには、このオプションを選択します。
スケジュールスキャンを設定する	a. スケジュールスキャンを設定するには、[一括アクション] > [スケジュールスキャンの設定] をクリックします。 [スケジュールの設定] パネルが表示されます。 b. [繰り返し間隔] ボックスで、スキャンを繰り返す回数を選択します。 c. 必要に応じて、分数、時間数、日数、週数を指定します。 注意: ここで指定したスケジュールは、エージェントの既存のスケジュールよりも優先されます。 d. [保存] をクリックします。

OT エージェントとセンサーの比較

機能	OT エージェント	センサー

ターゲットユースケース	評価、PoV、柔軟な Windows ベースの OT 環境向け	トラフィックの検査と制御が必要なフルデプロイメント向け
デプロイメントタイプ	Windows マシン (HMI、ワークステーション、ジャンプボックス) にインストール	Tenable Core オペレーティングシステムをベースとするハードウェアまたは VM にインストール
ICP の依存関係	ICP とのペアリングが必要だが、独立してデータ収集が可能 (サポート + スクリプトが必要)	ICP に完全に依存
インストールの複雑さ	軽量で柔軟性があり、一括デプロイメントが可能	物理または仮想デプロイメントと設定が必要
ICP へのデータフロー	スキャン完了後に結果がプッシュされる	連続データストリーム (アクティブ + パッシブ)
実行タイプ	アクティブスキャンのみ	アクティブスキャンとパッシブスキャン
スキャン管理 UI	[エージェント] ページからのみ管理	[アクティブクエリ] ページと [インベントリ] ページからトリガーされるクエリ
Nessus の統合	サポート対象外	Nessus クエリはセンサーを経由してルーティング可能
脆弱性マッチング	ICP に組み込まれた Nessus をマッチングに使用	ICP に組み込まれた Nessus をマッチングとアクティブスキャンの両方に使用
スキャンのスケジューリング	サポート対象 (1 回または継続)	サポート対象 (1 回または継続)

資産の可視性	インベントリに表示されるが、インベントリからクエリ不可能な資産	インベントリから完全にクエリ可能な資産
認証情報の範囲	エージェントごとに設定された専用認証情報を使用	ICP のグローバル認証情報を使用
複製ネットワークのサポート	サポート対象	サポート対象
グローバル制限を守る	バージョン 4.3 ではサポート対象外	サポート対象
ペアリング方法	ペアリングキー (1 つの blob に API キー + 証明書 + ICP IP)	API キー、証明書、IP の手動設定が必要
ハードウェア	なし - 既存の Windows マシンで実行	専用ハードウェアまたは VM が必要
パッシブトラフィックキャプチャ	サポート対象外	完全サポート

IoT コネクタの管理

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

OT Security では、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それぞれのアプリケーションサーバーにマッピングできます。これを行うには、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します。

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、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 コネクタエージェントの要件

要件カテゴリ	最小要件
オペレーティングシステム	• Windows XP、7、10、11。Windows Server 2003、2008、2012、2016、2019、2022 • Ubuntu 20.x または 22.x
メモリ	1GB
ディスク容量	1GB
CPU	専用の CPU 能力が 10% 以上あるハードウェア。

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、管理対象のすべてのデバイスをインポートします。

IoT コネクタに関して次のタスクを実行できます。

IoT コネクタの追加

1. [データ収集] > [データソース] ページで、[IoT コネクタ] タブをクリックします。

   [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. [サーバーの IP アドレス] 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. データベースでホストされている VMS に接続するには、[VMS 認証情報] トグルをクリックして有効にします。

     OT Security は、VMS 認証情報に必要な関連フィールドを有効にします。
  4. [データベースの IP アドレス] ボックスに、VMS をホストしているデータベースの IP アドレスを追加します。
  5. [データベースポート] ボックスに、サーバーへの接続用のポート番号を追加します。
  6. [ユーザー名] ボックスに、データベースのユーザー名を入力します。
  7. [パスワード] ボックスに、データベースのパスワードを入力します。
  8. [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。

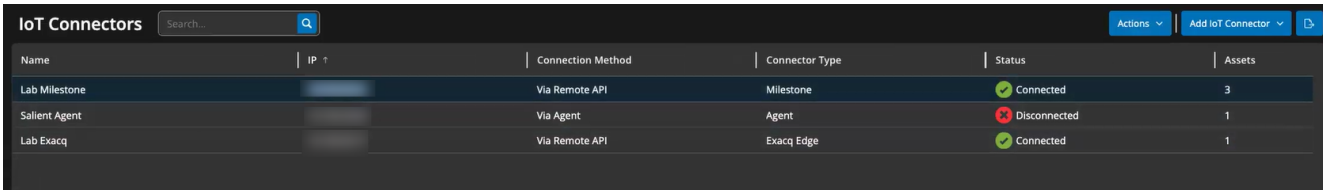
- **リモート API 経由**

  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 により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。

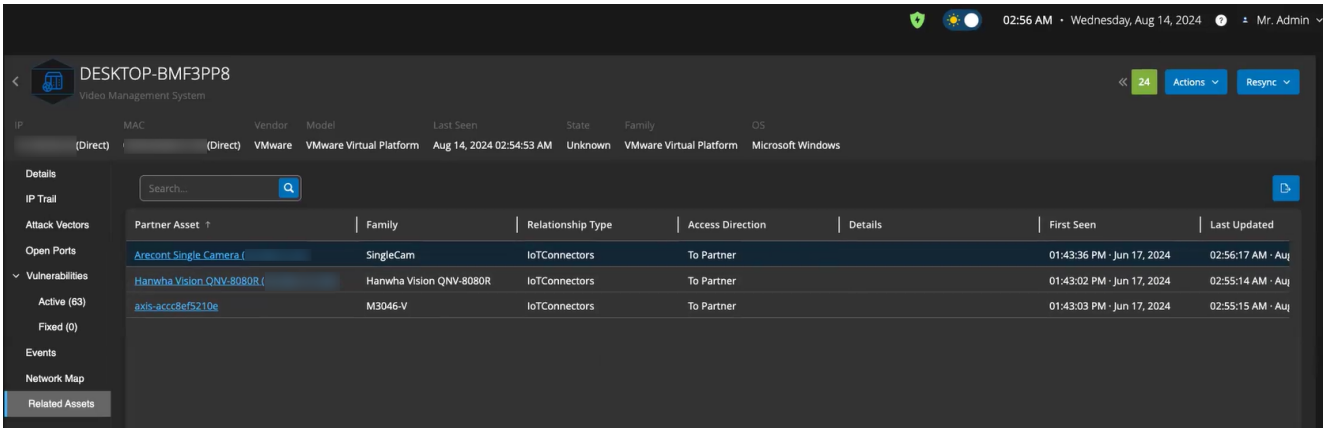
サーバーによって管理されているすべてのデバイスを表示する方法

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 コネクタの削除

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。同じ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。

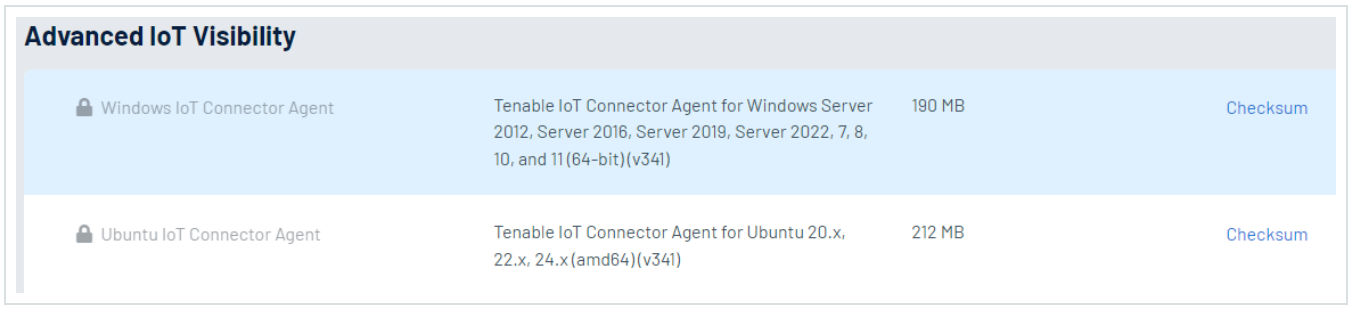
Windows での IoT コネクタエージェントのインストール

> 必要なロール: 管理者

OT Security では、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それぞれのアプリケーションサーバーにマッピングできます。これを行うには、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。

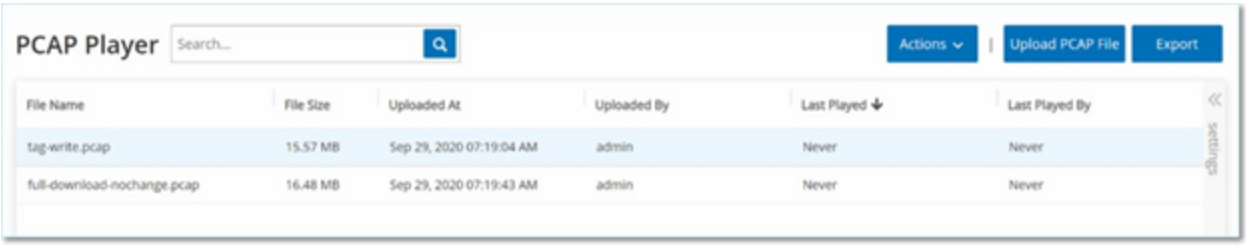
b. 現在実行中のサービスのリストに **OT Security** IoT コネクタエージェント が表示されていることを確認します。

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。

PCAP プレーヤー

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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. [データ収集] > [データソース] ページで、[PCAP プレーヤー] タブをクリックします。

   [PCAP プレーヤー] ページが表示されます。

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. [データ収集] > [データソース] ページで、[PCAP プレーヤー] タブをクリックします。

   [PCAP プレーヤー] ページが表示されます。

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: ファイルの再生中に別の PCAP ファイルを再生することはできません。

手動アップロード

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、サイトオペレーター

[手動アップロード] タブには以下が含まれます。

- CSV を使用した資産詳細の更新
- 手動による資産の追加
- SCD ファイル
- Rockwell プロジェクトファイル

CSV を使用した資産詳細の更新

[すべての資産] 表を CSV ファイルでエクスポートし、編集を加えてからアップロードできます。タイプ、名前、重大度、パデューレベル、ロケーション、説明、およびすべてのカスタムフィールドを編集できます。

言語が英語に設定されている場合のみ、CSV ファイルを使用して資産の詳細を更新できます。非英語圏のユーザーは、CSV ファイルをエクスポートしてアップロードしている間は一時的に英語に切り替え、その後、ご希望の言語に戻すことができます。

資産の詳細の CSV ファイルをアップロードする方法

1. [データ収集] > [データソース] ページで、[手動アップロード] タブをクリックします。
2. [CSV を使用した資産詳細の更新] セクションで、[アップロード] をクリックします。
3. CSV ファイルがある場所を参照してアップロードします。

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くても、インベントリを追跡するために、所有している他の資産を表示させたいと思うかもしれません。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、システム内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、システムはその資産を通常の資産として扱うようになります。

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方法

1. [データ収集] > [データソース] に移動します。

   [データソース] ページが表示されます。

2. [手動アップロード] タブで、[資産を手動で追加] セクションに移動します。

3. [アクション] メニューから [CSV テンプレートをダウンロード] 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。

4. `tot_Assets` テンプレートドキュメントを開きます。

5. ファイルにある指示に正確に従って `tot_Assets` テンプレートを編集し、列ヘッダー (名前、タイプなど) と入力した値だけになるようにします。

6. 編集したファイルを保存します。

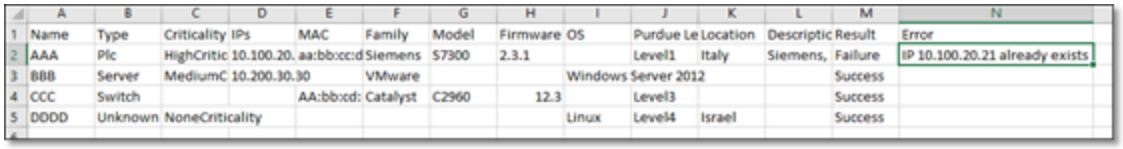
7. [資産設定] ページに戻ります。

8. [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。

9. [資産を手動で追加] で、[レポートのダウンロード] をクリックします。

   レポートを含む CSV ファイルが表示され、[結果] 列に成功と失敗が示されます。エラーの詳細は、

[エラー] 列に表示されます。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Name	Type	Criticality	IPs	MAC	Family	Model	Firmware	OS	Purdue Le	Location	Descriptic	Result	Error
2	AAA	Plc	HighCritic	10.100.20.	aa:bb:cc:d	Siemens	S7300	2.3.1		Level1	Italy	Siemens,	Failure	IP 10.100.20.21 already exists
3	BBB	Server	MediumC	10.200.30.	30	VMware			Windows	Server 2012			Success	
4	CCC	Switch			AA:bb:cd:	Catalyst	C2960	12.3		Level3			Success	
5	DDDD	Unknown	NoneCriticality						Linux	Level4	Israel		Success	

SCD ファイル

Substation Configuration Description (SCD) ファイルには、変電所の通信関連の全詳細情報が含まれています。SCD ファイルを OT Security にアップロードして、資産、IEC 61850 設定に対する可視性、およびお使いの環境に関するセキュリティインサイトを得ることができるようになりました。

SCD ファイルの情報に基づいて、OT Security は変電所の設定ミスに関連する次のような検出結果を報告します。

- 認証されていないクライアントからの製造メッセージ仕様 (MMS) レポートへのアクセス。
- SCD ファイルに記載されていない認証されていないクライアントが、MMS レポートをサブスクリプション登録しようとしています。

> 注意: OT Security は、SCD ファイルの次の形式のみをサポートします。
>
> - Substation Configuration Language (SCL) バージョン 1.0 および 2.0
> - 変電所が 1 つだけの SCD ファイル

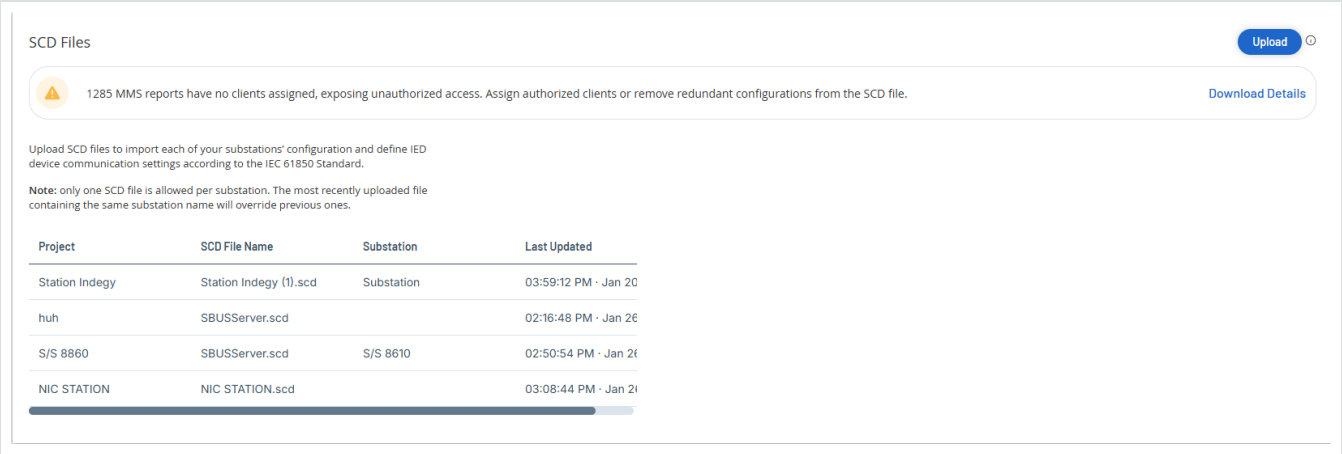
SCD ファイルをアップロードする方法

1. [データ収集] > [データソース] に移動します。

   [データソース] ページが表示されます。

2. [手動アップロード] タブで、[SCD ファイル] セクションに移動します。

3. [SCD ファイル] セクションで、[アップロード] をクリックします。



> 注意: 変電所ごとに 1 つの SCD ファイルのみアップロードできます。同じ変電所名を含む直近にアップロードされたファイルが、その前のファイルをオーバーライドします。

4. アップロードするファイルを参照して選択します。

   OT Security は SCD ファイルをアップロードし、[インベントリ] > [詳細] タブと [IEC 61850] タブで資産の詳細が表示されます。SCD ファイルに設定ミスがあるとイベントがトリガーされ、[詳細] ページと [IEC 61850] ページの上部に不正アクセスのエラーメッセージが表示されます。

5. (オプション) 検出結果の詳細をダウンロードするには、エラーメッセージで [詳細のダウンロード] をクリックします。

   OT Security は詳細を CSV 形式でダウンロードします。

Rockwell プロジェクトファイル

Rockwell `.L5X` ファイルをアップロードすることで、資産を作成し、資産の詳細を充実させ、エアギャップ環境や可視性が制限された環境で資産間の関係を構築できます。プロジェクトのファイルサイズは最大 50 MiB です。

> 重要: デフォルトでは、`ProjectFilePopulatePrimaryLayerAssetIPs` は `True` に、`ProjectFilePopulateNonPrimaryLayerAssetIPs` は `False` に設定されています。同一の IP アドレスを持つ資産を含む複数のプロジェクトファイルをアップロードする場合、`ProjectFilePopulateNonPrimaryLayerAssetIPs` 構成パラメーターを `True` に設定することで、資産の重複を解消できます。これにより、システムは非プライマリレイヤーにある資産の IP アドレスを表示できる

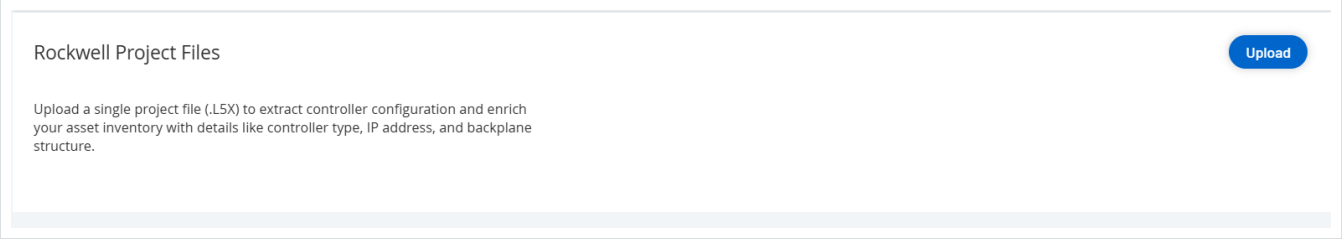
ようになり、同じ IP アドレスを持つ資産を 1 つの資産として解決して、同じバックプレーンに正しく配置することができます。設定の変更については、Tenable サポートにお問い合わせください。

Rockwell ファイルをアップロードする方法

1. [データ収集] > [データソース] に移動します。

   [データソース] ページが表示されます。

2. [手動アップロード] タブで、[Rockwell プロジェクトファイル] セクションに移動します。



3. [アップロード] をクリックします。

4. アップロードするファイルを参照して選択します。

   OT Security は Rockwell プロジェクトファイルをアップロードし、[インベントリ] > [詳細] タブで資産の詳細が表示されます。

設定

OT Security の設定] 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。

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。API キーの生成を参照してください。

- ライセンス – ライセンスの表示、アップデート、再作成ができます。ライセンスを参照してください。

- **ネットワーク定義**
  - パッシブモニタリング – パッシブモニタリングを有効にして、OT Security が資産を検出できるようにします。パッシブモニタリングを参照してください。
  - CSV を使用した資産詳細の更新 – CSV テンプレートを使用して資産の詳細を更新します。[CSV を使用した資産詳細の更新] を参照してください。
  - 手動による資産の追加 – 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 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。

- 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。モニタリング対象ネットワークを参照してください。
- 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 – 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化できます。イベントクラスタ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。ユーザー管理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。ユーザー管理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。ユーザー管理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。

- 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に戻します。出荷時の設定にリセットできるのは、管理者またはセキュリティマネージャーのみです。

  > 警告: この操作は元に戻せません。システムのすべてのデータが失われます。

  以下のオプションが、Tenable Core から選択可能になりました。

  - 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 を使用して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。

- 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。

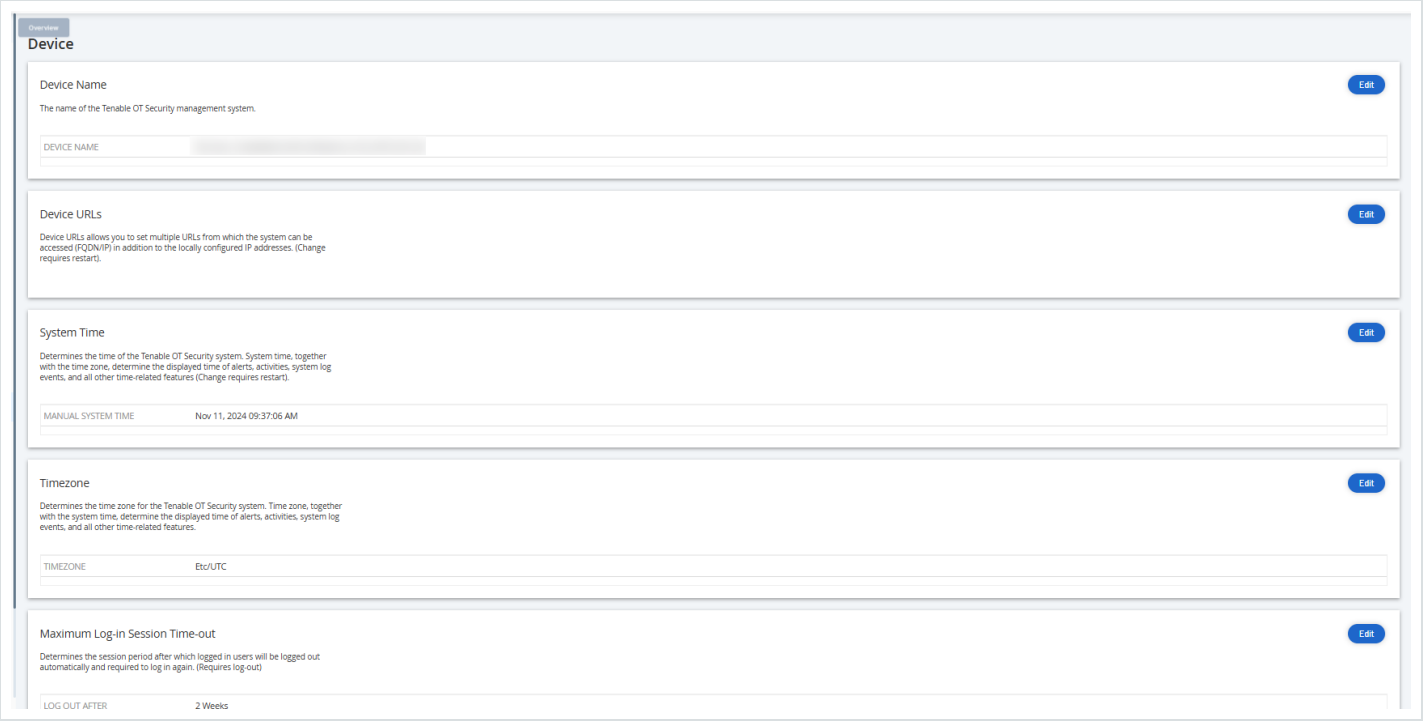
システム設定

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

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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。

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

バージョン 4.1 以降、ポート 8000 の Tenable Core インターフェースの分割ポートを表示して設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

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

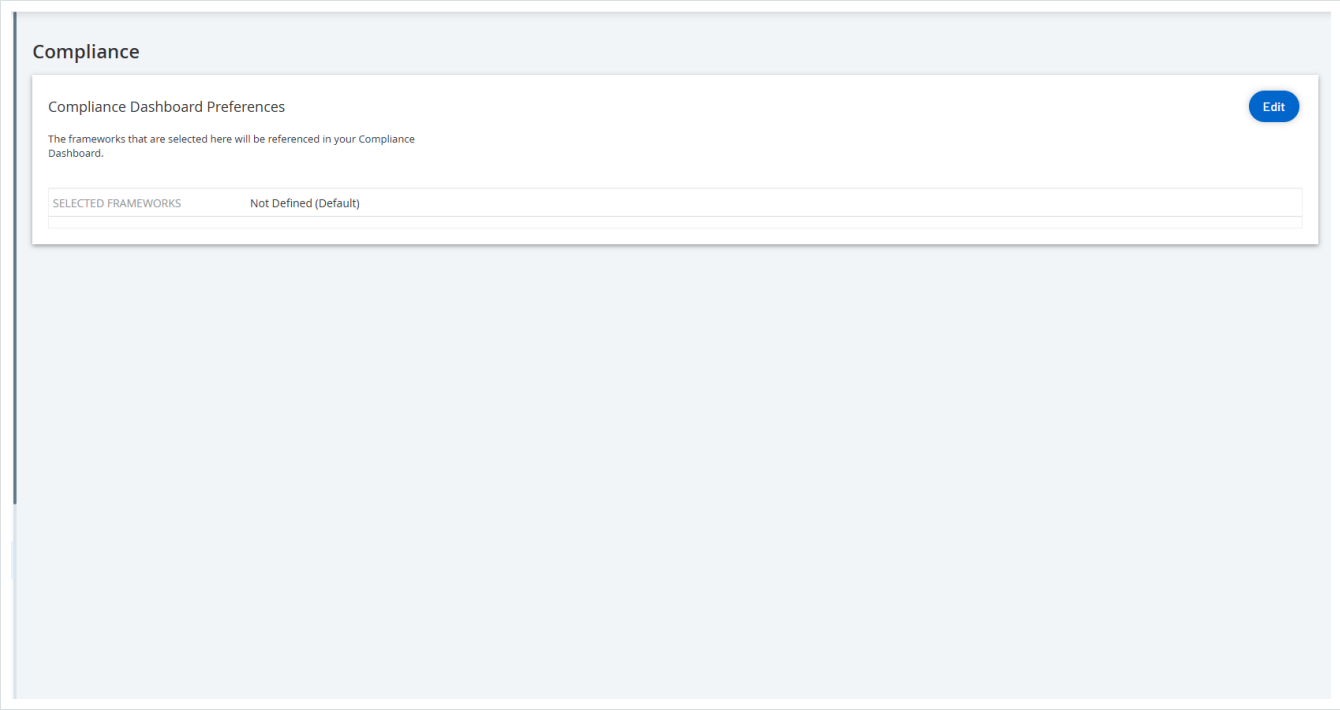
データを生成するときに [コンプライアンス] ダッシュボードが参照するセキュリティフレームワークを指定することができます。

[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。

   - 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)
- NERC-CIP 要件
- IEC-62443-3-3 要件

4. [保存] をクリックします。

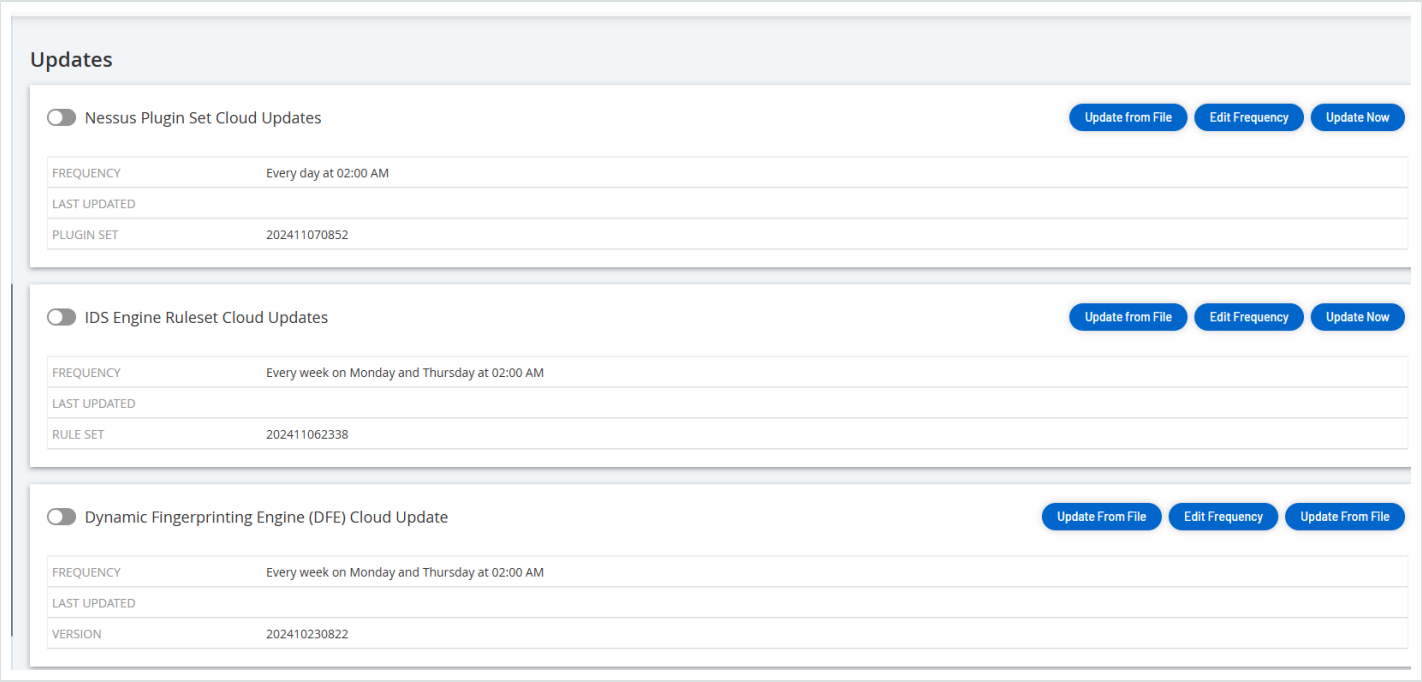
   OT Security は、コンプライアンスフレームワークの設定を保存し、指定された設定と照らして組織のコンプライアンスをチェックします。OT Security は、コンプライアンスチェックの結果を [コンプライアンス] ダッシュボードに表示します。

アップデート

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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 が資産をモニタリングして、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 には、DFE (Dynamic Fingerprinting Engine) のクラウドアップデートで、分類、ファミリー、カバレッジをアップデートするオプションがあります。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の設定

プラグインの自動アップデートを有効にする手順

1. 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。

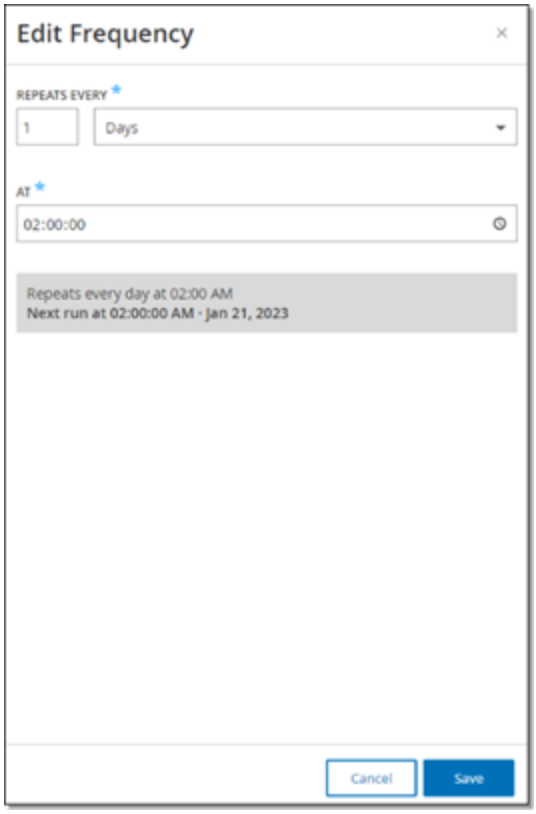
プラグインアップデートの頻度の編集

1. 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. 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. 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。

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の設定

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. 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の編集

1. 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. 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。

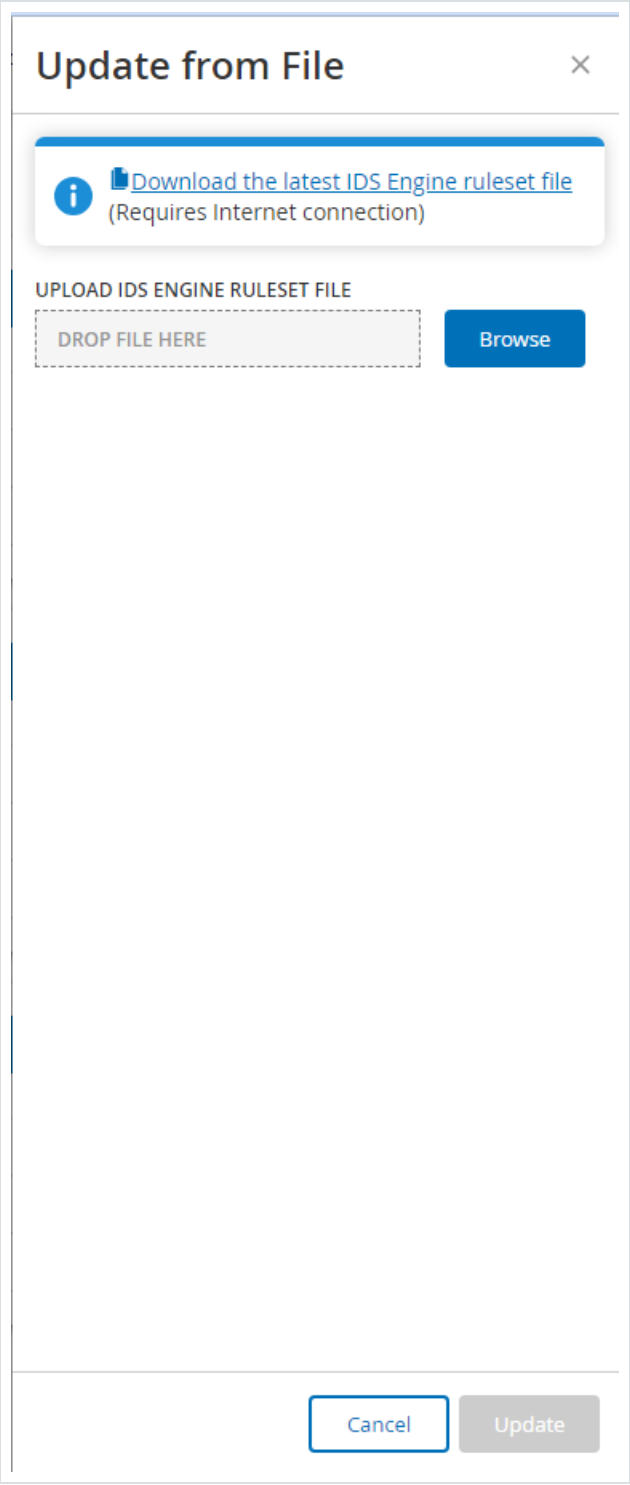
IDS エンジンルールセットをオフラインでアップデートする手順

1. 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 アップデートの設定

自動 DFE アップデートを有効にする方法

1. 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の編集

1. 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. 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。

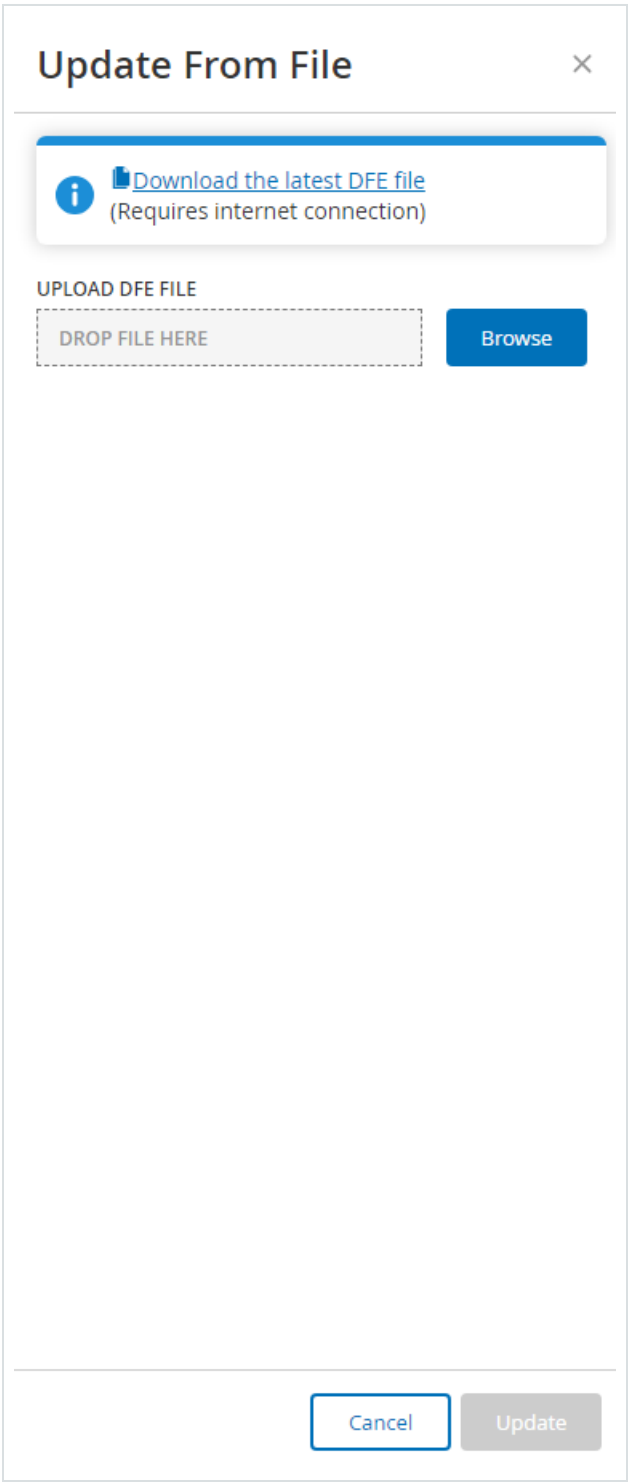
オフラインで DFE アップデートを実行する方法

1. 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。

OT Discovery エンジン (OTD) のアップデート

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティアナリスト

OT エージェントは、OT Discovery (OTD) エンジンを使用して環境をスキャンします。[データソース] >[エージェント] ページから手動または自動で OTD エンジンをアップデートできます。OTD エンジンをアップデートする前に、まず最新の OTD ファイルを OT Security にアップロードする必要があります。

始める前に

- ダウンロードポータルから OT Discovery (OTD) エンジンファイルをダウンロードします。

OTD エンジンファイルをアップロードする方法

1. [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。

2. [OT Discovery Engine (OTD) のアップデート] セクションで、[アップロード] をクリックします。

   [ファイルのアップロード] パネルが表示されます。

3. [参照] をクリックし、Tenable ダウンロードポータルからダウンロードした OTD エンジンファイルに移動します。

4. [アップロード] をクリックします。

5. OTD エンジンをアップデートするには、OT エージェントのアップデートの手順に従ってください。

証明書

必要な OT Security ユーザーロール: 管理者

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。

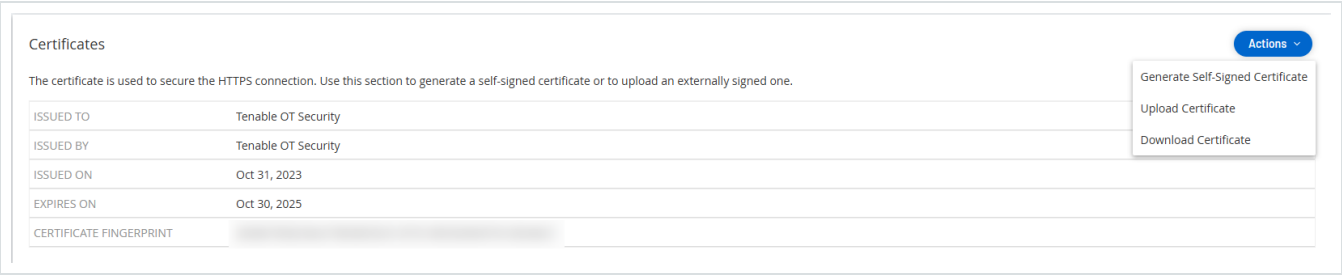
注意: 新しい証明書を生成すると、現在の証明書は上書きされます。

自己署名証明書の生成方法

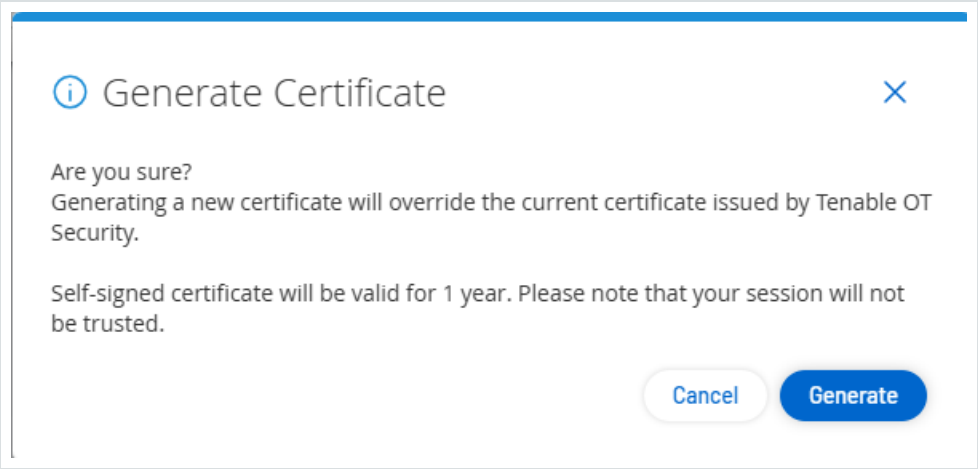
1. 設定] > [システム設定] > [証明書] に移動します。

   [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、[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. 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 証明書が確実にアップデートされるように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。

API キーの生成

> 必要な OT Security ユーザーロール: 管理者、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

API キーを生成することで、OT Security を組織内の他のセキュリティツールやシステムに統合しやすくなります。

OT Security で API キーを生成する方法

1. [設定] > [システム設定] > [API キー] に移動します。

   [API キー] ページが表示されます。

2. 右上の [キーの生成] をクリックします。

   [キーの生成] パネルが表示されます。

3. [有効期限] ボックスで、API キーが期限切れになるまでの日数を選択します。

4. [説明] ボックスで、API キーの説明を入力します。

5. [生成] をクリックします。

   [キーの生成] パネルに [ID] と [API キー] が表示されます。

6. ボタンをクリックし、API キーをコピーします。

7. [完了] をクリックします。

   [API キー] ページが表示され、新しく追加された API キー ID が表示されます。

ICP と Enterprise Manager のペアリング

必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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 をペアリングすれば、すべてのサイトを管理できます。

注意: EM とペアリングしたら、サイトとそのセンサーが最新バージョンのアップデートを受け取るように、すべてのアップデートを EM レベルで実行する必要があります。

始める前に

次のことを確認してください。

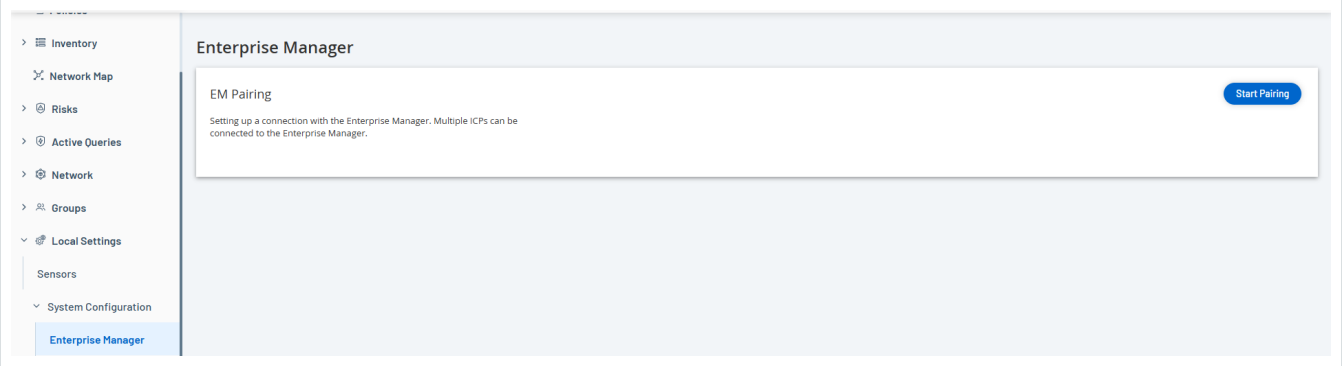
- OT Security EM は API を通して ICP に接続できる
- ICP から OT Security EM への通信用に TCP 443 と TCP 28305 が開かれている
- ICP と OT Security EM の間に HTTPS 接続が存在している
- (オプション) OT Security EM で API キーを生成する

  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、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 からアクセスした ICP インスタンスのヘッダーには ICP ラベルが表示されます。詳細については、Tenable OT Security Enterprise Manager ユーザーガイドの ICP をご覧ください。

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 のペアリング解除

必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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 と ICP ペアリングの解除

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 により、OT Security とのペアリングが解除されます。

OT Security と ICP ペアリングの解除

1. OT Security で、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 により、OT Security EM とのペアリングが解除されます。

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

ネットワーク定義

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー、サイトオペレーター

[ネットワーク定義] ページには、次のセクションが含まれます。

- パッシブモニタリング
- 重複する内部ネットワーク
- SNMP を介した新しい資産の検出
- IoT 資産の IP アドレスのフェッチ

パッシブモニタリング

パッシブモニタリングは、OT Security の初期設定中に無効になります。Tenable では、パッシブモニタリングを有効にする前に、監視対象ネットワークの設定を完了するよう推奨しています。これにより、初期段階で大量のアラートやセキュリティイベントが発生するのを抑え、アラートの過剰発生を防ぐことができます。

重複する内部ネットワーク

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

重複するIP範囲は、同じIPアドレスが複数のデバイスに割り当てられている時に発生します。重複するIP範囲は製造環境全体で共通のものになります。これにより、資産を正確に特定して追跡することが困難になり、可視性のギャップや不適切な資産の関連付けが発生します。IPアドレスが異なるセグメントにまたがって再利用されている場合でも、OT Securityに対して重複するネットワークを定義すれば、資産を正確に追跡することができます。

> 注意: 重複するネットワーク内の資産がセンサーと別のソース(別のセンサーやローカルのICP)の両方によって検出された場合、OT Securityインターフェースはそれを1つの資産に統合します。ただし、ライセンス数としては2つの資産としてカウントされます。これを防ぐために、Tenableでは重複するネットワーク範囲を調整してそのような資産を除外することを推奨しています。

重複するネットワークの追加

始める前に

- 認証されたセンサーがペアリングされていることを確認してください。

  > 注意: OT Securityは、認証されていないセンサーの重複するネットワークをサポートしていません。

環境内の重複ネットワークを定義する方法

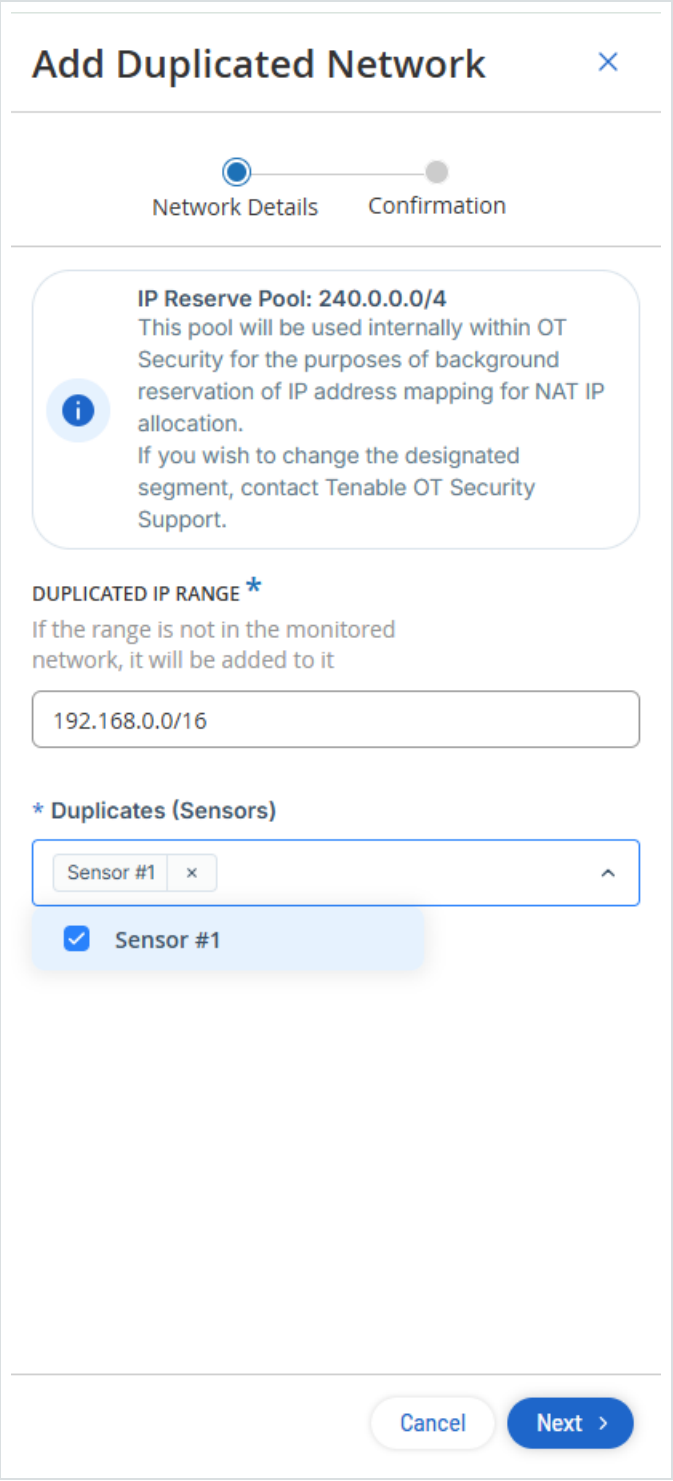
1. [設定] > [環境設定] > [ネットワーク定義]に移動します。

   [ネットワーク定義]ページが表示されます。

2. [重複する内部ネットワーク]セクションで、[ネットワークの追加]をクリックします。

   [重複するネットワークの追加]パネルが[ネットワークの詳細]とともに表示されます。

   > 注意: OT Securityは、IPアドレスをNAT IP割り当てにマッピングするための内部予約プールとして、240.0.0.0/4 IP範囲を使用します。この予約プール範囲を変更するには、Tenableサポートに連絡してください。

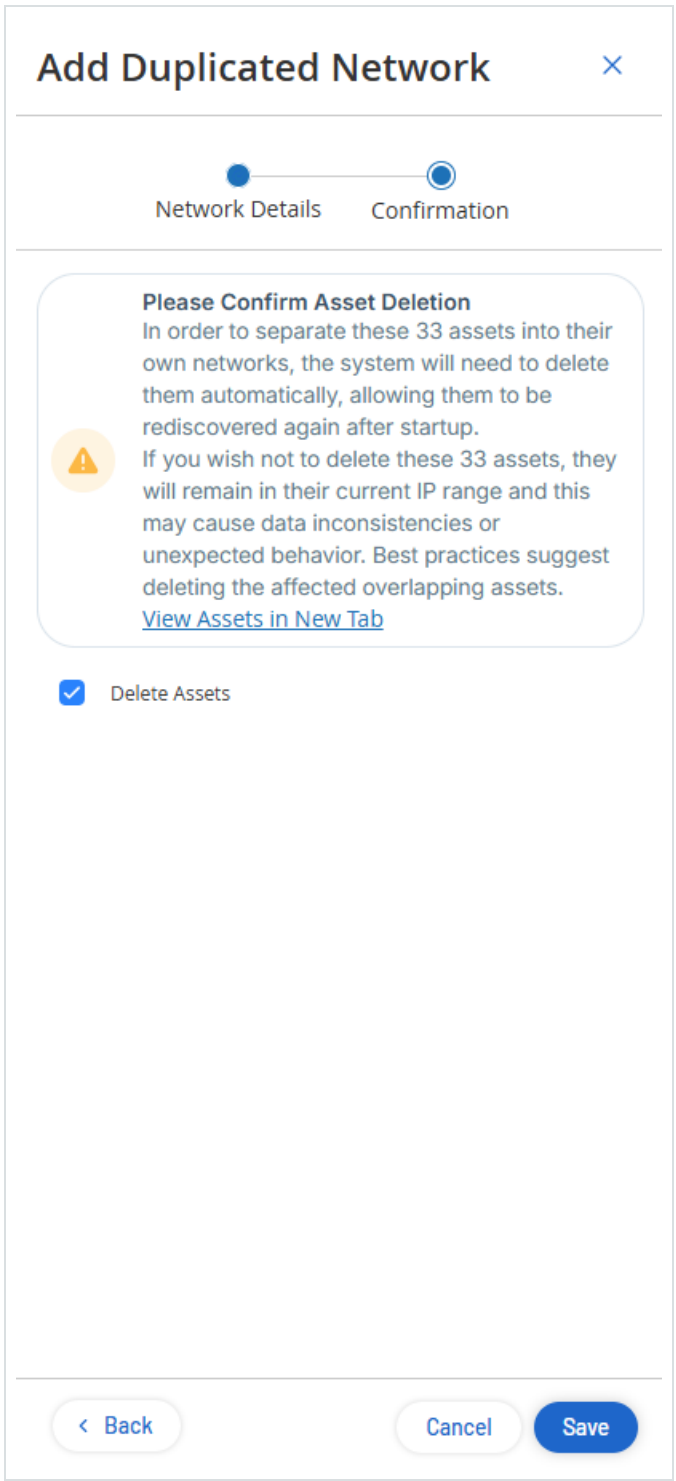


3. [重複する IP 範囲] ボックスに、IP 範囲を CIDR 形式で入力します (例: 192.168.0.0/24)。

4. [重複 (センサー)] ドロップダウンボックスから、重複する IP 範囲に関連付けるセンサーを選択します。

5. [次へ] をクリックします。

   [確認] パネルが表示されます。

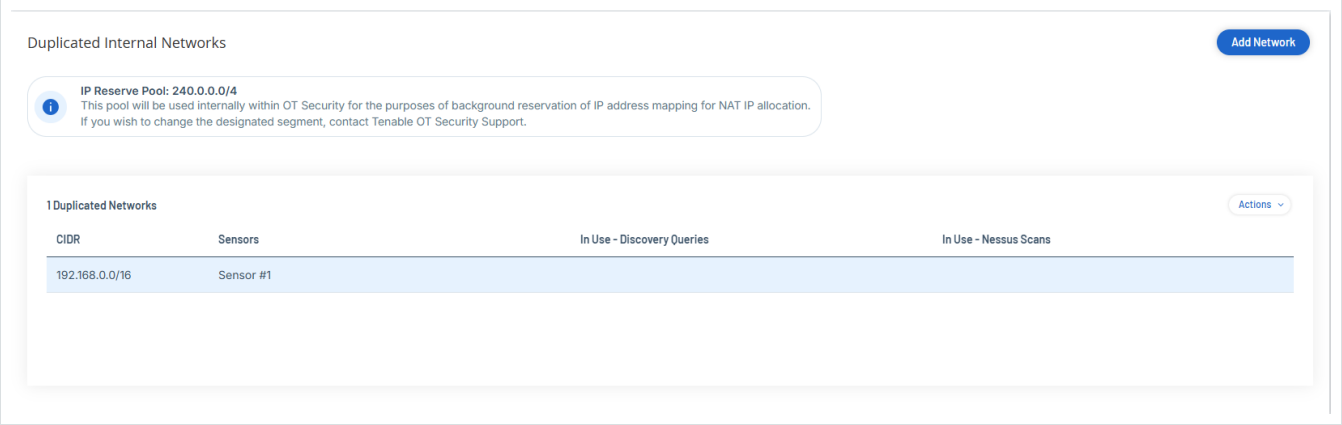


6. (オプション) [資 産 の削 除] チェックボックスを選 択します。

ヒント: 選択されたすべての資産を独自のネットワークに分離するために、Tenable は、OT Security が資産を削除して、起動後にそれらを再検出できるようにすることを推奨しています。[資産の削除] チェックボックスを選択しない場合、資産は現在の IP 範囲内にとどまり、不一致や予期しない動作が起きる可能性があります。

7. [保存] をクリックします。

   OT Security により重複 IP 範囲が保存され、[重複する内部ネットワーク] テーブルに表示されます。



重要: 重複するネットワークの設定が完了したら、Tenable は、OT Security を再起動してからセンサーを有効にすることを推奨しています。

8. OT Security を再起動します。

9. センサーを有効にするには、設定] > [センサー] に移動します。

   注意: アクティブクエリの IP 範囲 (CIDR) は、[重複する内部ネットワーク] で設定したものです。

   1. 次のいずれかを行います。

      - 単一のセンサー: センサーを右クリックし、[編集] をクリックします。[センサーの編集] パネルで、[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。
      - 複数のセンサー: 必要なセンサーをすべて選択します。ヘッダーで、[一括アクション] > [アクティブクエリの有効化] を選択します。

2. センサーを右クリックし、ステータスを [一時停止] から [接続済み] に変更してアクティブにします。

次のステップ

重複するネットワークを設定して OT Security を再起動した後、資産は実際の IP とともに [すべての資産] テーブルに表示されます。さらに、重複するネットワークに割り当てられた IP を入力する場合は、対応するセンサーも選択する必要があります (たとえば、[アクティブクエリ] > [検出] / [Nessus スキャン] > [スキャンを作成]、または [認証情報] > [認証情報のテスト])。

- [インベントリ] > [すべての資産] で、[すべての資産] テーブルの資産の実際の IP アドレスと [ソース] を表示します。たとえば、同じ IP アドレスを共有しているが、異なるセンサーに関連付けられている 2 つの資産があるとします。
- [アクティブクエリ] > [クエリ管理] > [検出] または [Nessus スキャン] > [スキャンを作成] で、重複するネットワークを含むアクティブクエリを設定する際に、その IP 範囲の [関連するセンサー] を選択します。これにより、その他のセンサーを除外しながら、特定のセンサーに関連付けられた資産を求めるクエリを実行できます。

  > 注意: OT Security は、重複するネットワークの IP 範囲に対してのみ、[関連するセンサー] ボックスを有効にします。他のすべての IP 範囲では無効のままです。

- [アクティブクエリ] > [認証情報] > [認証情報のテスト] で認証情報を設定する際に、重複するネットワークの IP 範囲を入力する場合は、[複製 (センサー)] ボックスで関連するセンサーも選択する必要があります。
- 重複するネットワークの資産部分に対して [資産グループ] を作成するには、[資産選択] オプションを使用し、[資産] テーブルの [ソース] 列に基づいて特定の IP を指定します。

[重複する内部ネットワーク] テーブル

[重複する内部ネットワーク] テーブルには次の詳細が表示されます。

縦棒	説明
CIDR	重複するネットワークの IP 範囲。
センサー	重複するネットワークの IP 範囲に関連付けられているセンサー。
使用中 - 検出クエリ	CIDR が少なくとも 1 つの資産検出 (アクティブクエリ) で使用中かどうかを示します。使用中の場合、CIDR アクティブ検出を削除してから、その CIDR を含む重複するネットワークを削除します。
使用中 - Nessus スキャン	CIDR が 1 つ以上の Nessus スキャンで使用中かどうかを示します。使用中の場合、Nessus スキャンから CIDR を削除してから、その CIDR を含む重複するネットワークを削除します。

重複する内部ネットワークに対するアクション

重複するネットワークの編集

必要に応じて、重複するネットワーク設定を変更できます。

重複するネットワークを編集する方法

1. [重複する内部ネットワーク] セクションで、変更対象である重複するネットワークを選択します。
2. 次のいずれかを行います。
    - 重複するネットワークを右クリックし、[編集] を選択します。
    - セクションの右上で、[アクション] > [編集] を選択します。

    [重複するネットワークの編集] パネルが表示され、そこに選択した重複するネットワークの詳細情報も表示されます。
3. 必要に応じて値を変更します。
4. [次へ] をクリックします。

5. [確認] パネルで、[保存] をクリックします。

   OT Security により、重複するネットワークの変更が保存されます。

重複するネットワークの削除

不要になった重複するネットワークを削除できます。

重複するネットワークを削除する方法

1. [重複する内部ネットワーク] セクションで、削除対象である重複するネットワークを選択します。
2. 次のいずれかを行います。
   - 重複するネットワークを右クリックし、[削除] を選択します。
   - セクションの右上で、[アクション] > [削除] を選択します。

OT Security により重複するネットワークが削除されます。

重複するネットワークで使用中のセンサーの削除

重複するネットワークで使用中のセンサーを削除する方法

1. Nessus スキャン/アクティブ検出から CIDR を削除します。
2. 重複するネットワーク設定からセンサーを削除します。
3. 置き換える場合は、API を使用して新しいセンサー ID を設定し、古いセンサーを置き換えます。
4. [センサー] ページで、古いセンサーを削除します。

SNMP を介した新しい資産の検出

[SNMP を介して新しい資産を検出する] オプションを有効にすると、OT Security は SNMP クエリによって検出された資産を資産インベントリに追加します。

IoT 資産の IP アドレスのフェッチ

デフォルトでは、IoT コネクタから資産をインポートすると、OT Security はデバイスの MAC アドレスとともに IP アドレスもインポートします。MAC アドレスのみをインポートするには、[IoT 資産の IP アドレスをフェッチする] オプションを無効にします。詳細は、IoT コネクタの管理を参照してください。

イベントクラスタ

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

イベントのモニタリング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 つのクラスタにまとめられます。このクラスタ化は、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、デスティネーション資産に基づいて行われます。

イベントをクラスタ化するには、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、クラスタには含まれません。

クラスタリングを有効化する方法

1. [設定] > [環境設定] > [イベントクラスタ] に移動します。

   [イベントクラスタ] ページが表示されます。

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。

モニタリング対象ネットワーク

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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。

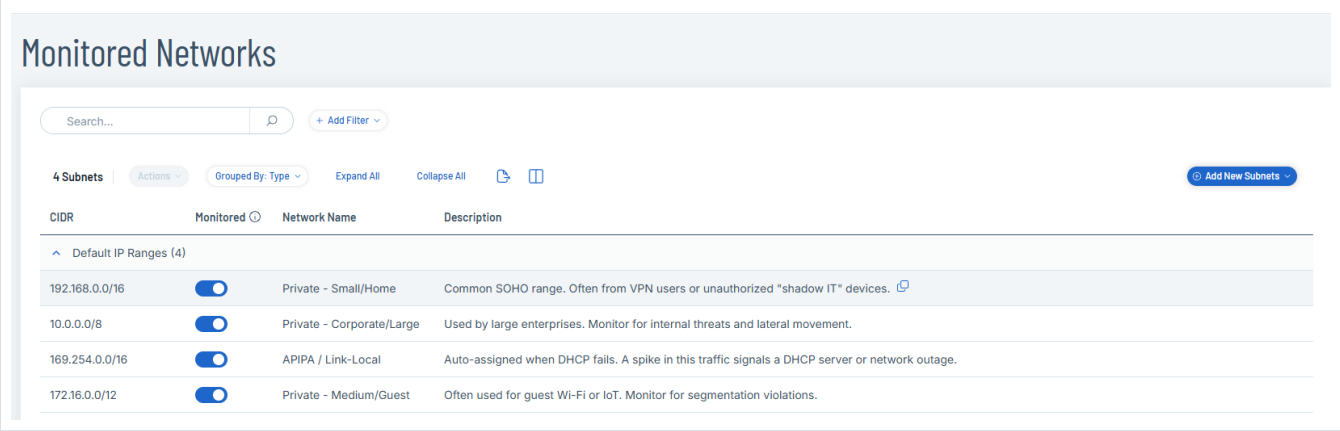
デフォルトでは、OT Security は 3 つのデフォルトのパブリック範囲 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、およびリンクローカル範囲 (APIPA) 169.254.0.0/16 を設定します。

> 注意: 5,000 個を超えるモニタリング対象サブネットを設定した場合、OT Security はリストの最初の 5,000 個エントリに切り捨てます。この切り捨てが発生しても、システムからの通知はありません。
> Nessus Network Monitor (NNM) コンポーネントの場合、OT Security は最初の 128 エントリのみを処理します。

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. [設定] > [環境設定] > [モニタリング対象ネットワーク] に移動します。

   [モニタリング対象ネットワーク] ページが表示されます。



2. 必要に応じてテーブルをカスタマイズします。テーブルのカスタマイズを参照してください。

3. [モニタリング対象ネットワーク] テーブルには、次の詳細が含まれています。

列	説明
デフォルトの IP 範囲およびカスタム IP 範囲	[デフォルトの IP 範囲] セクションには、OT Security で設定されたデフォルトの IP 範囲が表示されます。 [カスタム IP 範囲] セクションには、ユーザー自身が作成した IP 範囲が表示されます。
CIDR	[CIDR] 列には、モニタリング対象の IP アドレスが表示されます。
モニタリング対象	クリックして、設定済みの IP アドレスのモニタリングを有効または無効にします。
ネットワーク名	ネットワークの名前。
説明	IP 範囲に関する説明。
	パラメーターの横にあるコピーボタンを使用して、値をコピーします。

サブネットの追加

モニタリングするサブネットまたはサブネットのリストを追加できます。

新しいサブネットを追加する方法

1. 左側ナビゲーションメニューで、[設定] > [環境設定] > [モニタリング対象ネットワーク] をクリックします。

   [モニタリング対象ネットワーク] ページが表示されます。

2. 右上の [新しいサブネットの追加] をクリックします。

   メニューが表示されます。

3. 次のいずれかを選択します。

   - 1つのサブネットの追加 – このオプションを選択して、1つのサブネットを追加します。
   - サブネットリストの追加 – このオプションを選択して、サブネットのリストを追加します。

   [サブネットの追加] パネルが表示されます。

4. [1つのサブネットの追加] を選択した場合

   a. [CIDR] ボックスに、IP アドレス範囲を入力します。(例: `192.168.1.0/24`)。

   b. [モニタリング対象] トグルをクリックして OT Security を有効にし、トラフィックをキャプチャし、IP 範囲内でアクティブクエリを実行します。

   > 注意: [モニタリング対象] トグルはデフォルトで有効になっています。モニタリングをオフにするには、[モニタリング対象] トグルをクリックして無効にします。

   c. (オプション) [ネットワーク名] ボックスに、ネットワークの名前を入力します。

   d. (オプション) [説明] ボックスに、サブネットの説明を入力します。

   e. [保存] をクリックします。

5. [サブネットリストの追加]を選択した場合、[サブネットの追加] パネルで次の操作を行います。

a. [CIDR] ボックスに、CIDR のリストを 1 行に 1 つずつ入力します。

b. [モニタリング対象 (追加されたすべてのサブネット)] トグルをクリックして、OT Security がトラフィックをキャプチャし、リストされたすべてのサブネットのアクティブクエリを実行することを許可します。

> 注意: [モニタリング対象] トグルはデフォルトで有効になっています。モニタリングをオフにするには、[モニタリング対象 (追加されたすべてのサブネット)] トグルをクリックして無効にします。

c. [保存] をクリックします。

OT Security によりサブネットが保存され、[モニタリング対象ネットワーク] ページに表示されます。

サブネットの編集

サブネットを編集して変更することができます。

1. サブネットを編集するには、次のいずれかを行います。

   - [モニタリング対象ネットワーク] テーブルで、編集する IP 範囲の行にカーソルを合わせます。

     OT Security により [アクション] メニューが有効になります。

   - [モニタリング対象ネットワーク] テーブルで、編集する IP 範囲の行を右クリックします。

     メニューが表示されます。

2. [サブネットの編集] を選択します。

   [サブネットの編集] パネルが表示されます。

3. 必要な変更を行います。

4. [保存] をクリックします。

   OT Security により、サブネットの変更が保存されます。

ユーザー管理

OT Security コンソールへのアクセスは、そのユーザーに提供され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]、および [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あります。カスタムの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 – アイデンティティプロバイダー (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

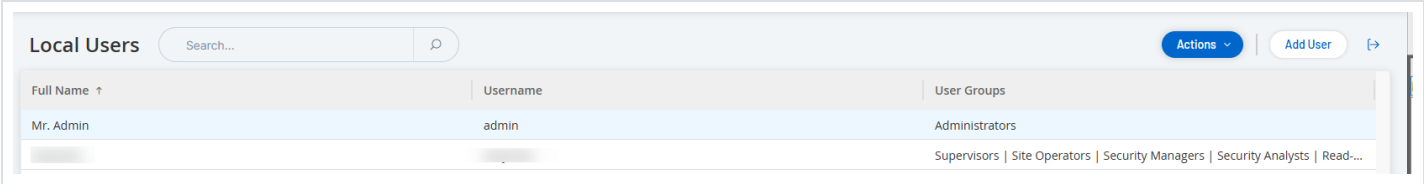
必要な OT Security ユーザーロール: 管理者

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. 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]、および [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あります。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. 設定] > [ユーザー管理] > [ローカルユーザー] に移動します。

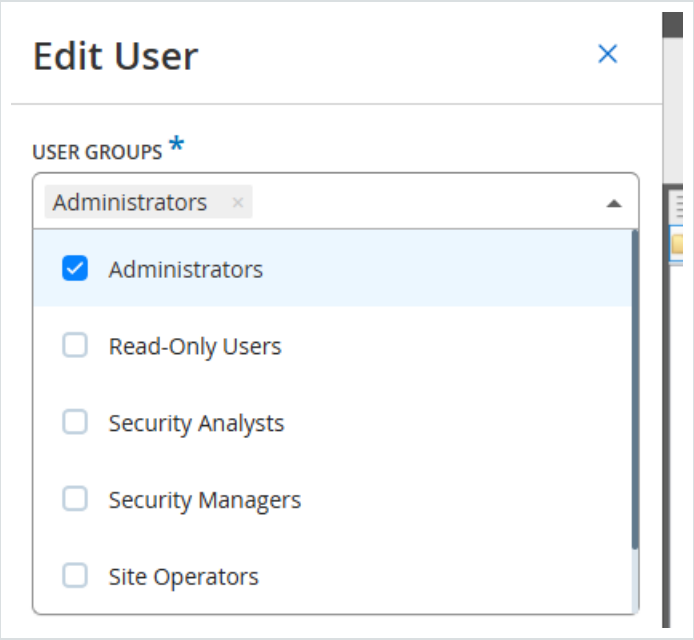
   [ローカルユーザー] ページが表示されます。

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. 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] ページが表示されます。

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. 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] ページが表示されます。

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

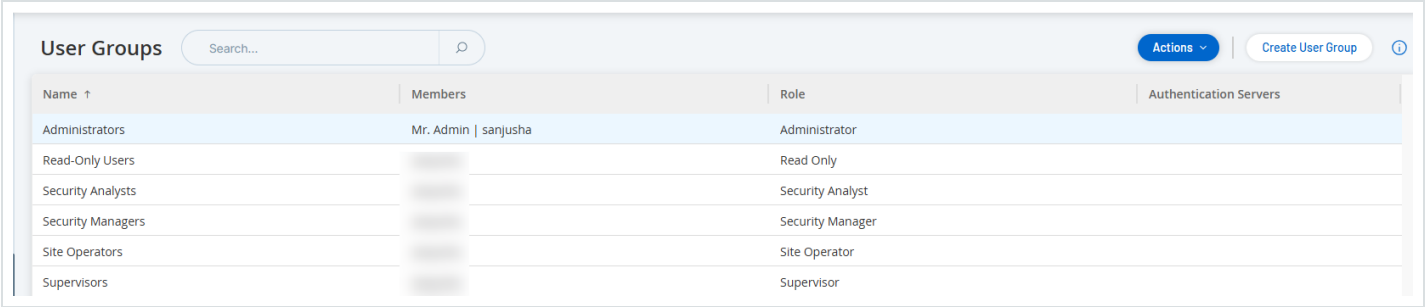
> 必要な OT Security ユーザーロール: 管理者

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、1 つ以上のユーザーグループに割り当てられます。それにより、そのユーザーに割り当てられるロールが決まります。

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]、および [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あります。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。

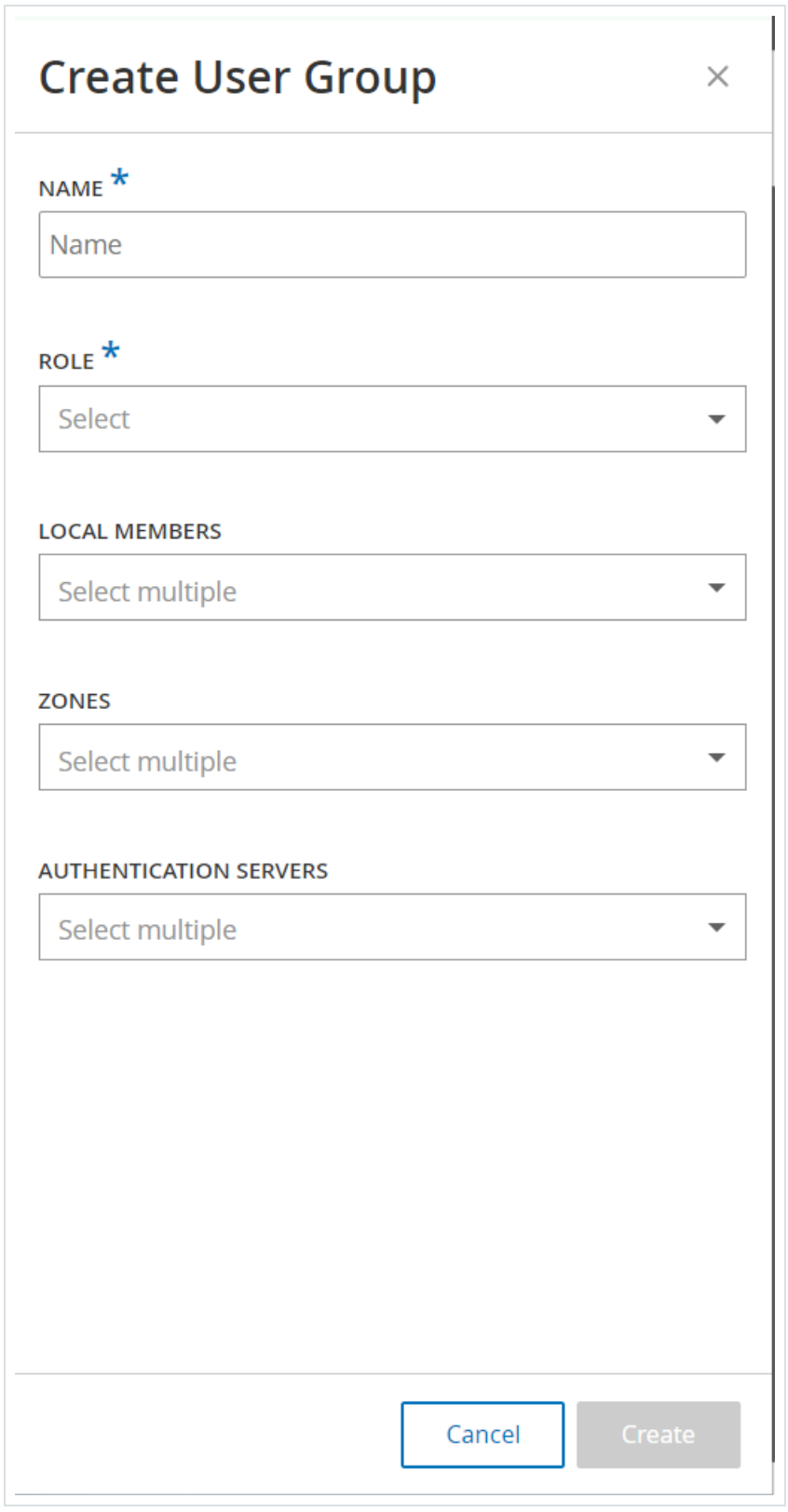
ユーザーグループを作成する方法

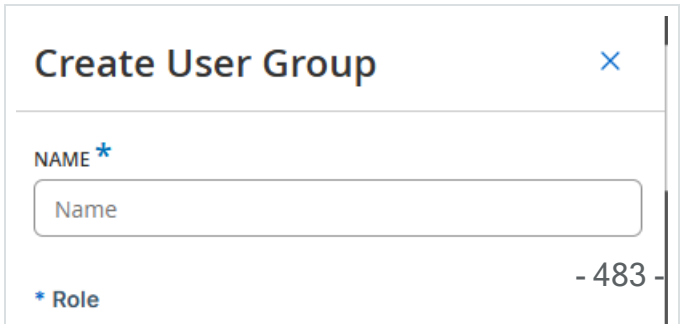
1. 設定] > [ユーザー管理] > [ユーザーグループ] に移動します。

   [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。


Create User Group
NAME *
Name
ROLE *
Select
LOCAL MEMBERS
Select multiple
ZONES
Select multiple
AUTHENTICATION SERVERS
Select multiple
Cancel
Create


Create User Group
NAME *
Name
* Role

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. 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. 次のいずれかを行います。

   - 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. 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. 次のいずれかを行います。

   - 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)	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る	✓	✓	✓	✓	✗	✗	✗
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	✓	✓	✓	✓	✓	✓	✓

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
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	✓	✓	✓	✗	✗	✓	✗

アクセス許可	管理者 (ローカル)	管理者 (外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
(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	✓	✓	✓	✓	✓	✓	✓

アクセス許可	管理者 (ローカル)	管理者 (外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
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							

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
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	✓	✓	✓	✓	✓	✓	✓

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
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	✓	✓	✓	✓	✓	✓	✓

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
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	✓	✓	✓	✗	✗	✗	✗

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
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	✓	✓	✓	✗	✗	✗	✗

アクセス許可	管理者(ローカル)	管理者(外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
スタ							
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)

アクセス許可	管理者 (ローカル)	管理者 (外部/AD)	スーパーバイザー	セキュリティマネージャー	セキュリティアナリスト	サイトオペレーター	読み取り専用
システムアクション	✓	✓出荷時設定へのリセットなし	✓バックアップと診断のみ	✓診断のみ	✗	✗	✗
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	✓	✓	✓	✗	✗	✗	✗

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る	✓	✓
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	✓	✓
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る	✓	✓	✗	✗	✗
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	✓	✗	✗	✗	✗
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

必要な OT Security ユーザーロール: 管理者

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. 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. 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。

縦棒	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. [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. [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. 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

> 必要な OT Security ユーザーロール: 管理者

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、統合をセットアップしてから、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]、および [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あります。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. 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。

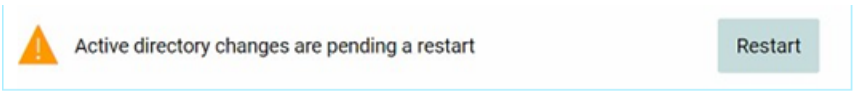
   > 注意: これらのフィールドはオプションです。フィールドが入力されていない場合、AD ユーザーはそのユーザーグループに割り当てられません。マッピングされたグループなしでも統合を設定できますが、その場合、少なくとも 1 つのグループマップの ping を追加するまで、ユーザーはシステムにアクセスできません。

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、統合をセットアップしてから、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. 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

> 必要な OT Security ユーザーロール: 管理者

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 Azure と SAML の統合を参照してください。

SAML を設定するには

1. 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] 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 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、使用しているアイデンティティ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。

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

必要な OT Security ユーザーロール: 管理者、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

グループを表示するには

1. [設定] > [グループ] に移動します。

   [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。次のグループのタイプがあります。

- 資産グループとタグ – 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。
- 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、ポリシー条件を満たすためにイベントが発生しなければならない時刻を設定するために使用する時間範囲です。
- コントローラータググループ – 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。

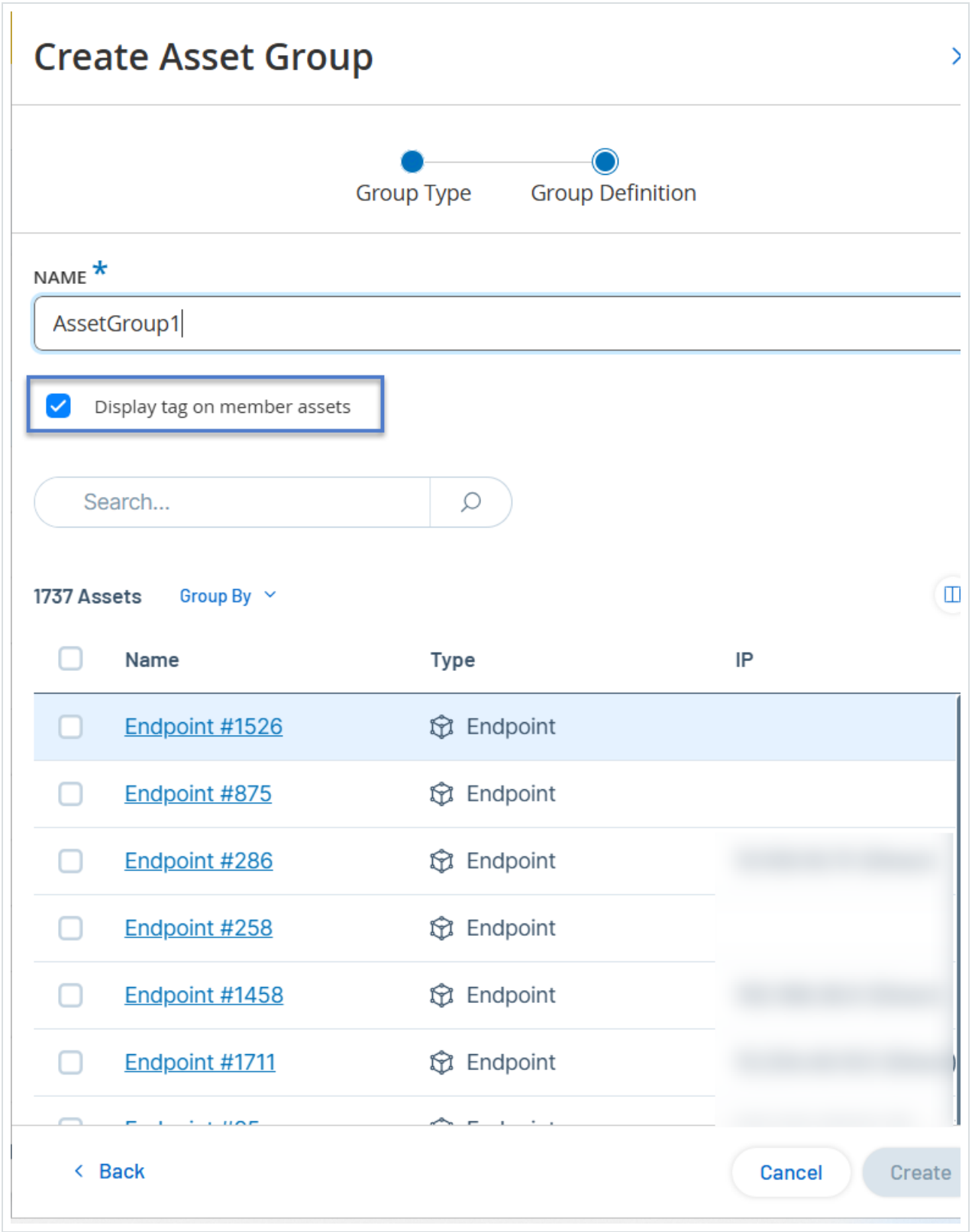
資産グループとタグ

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。

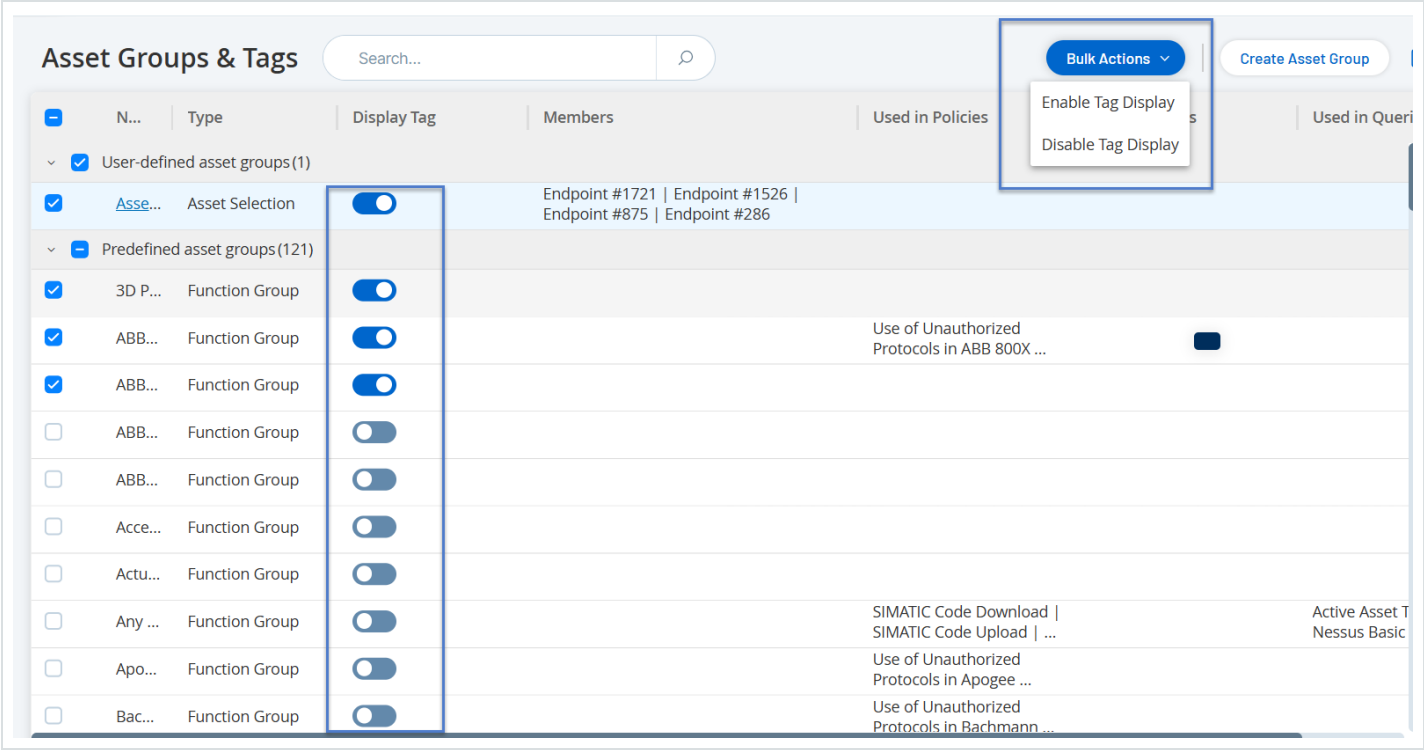
タグ

タグは、特定の基準に基づいて資産をグループ化するのに役立ちます。これにより、さまざまなワークフローを合理化し、優先順位を付けることができます。グループを作成すると、OT Security はグループを資産のタグとして変換します。

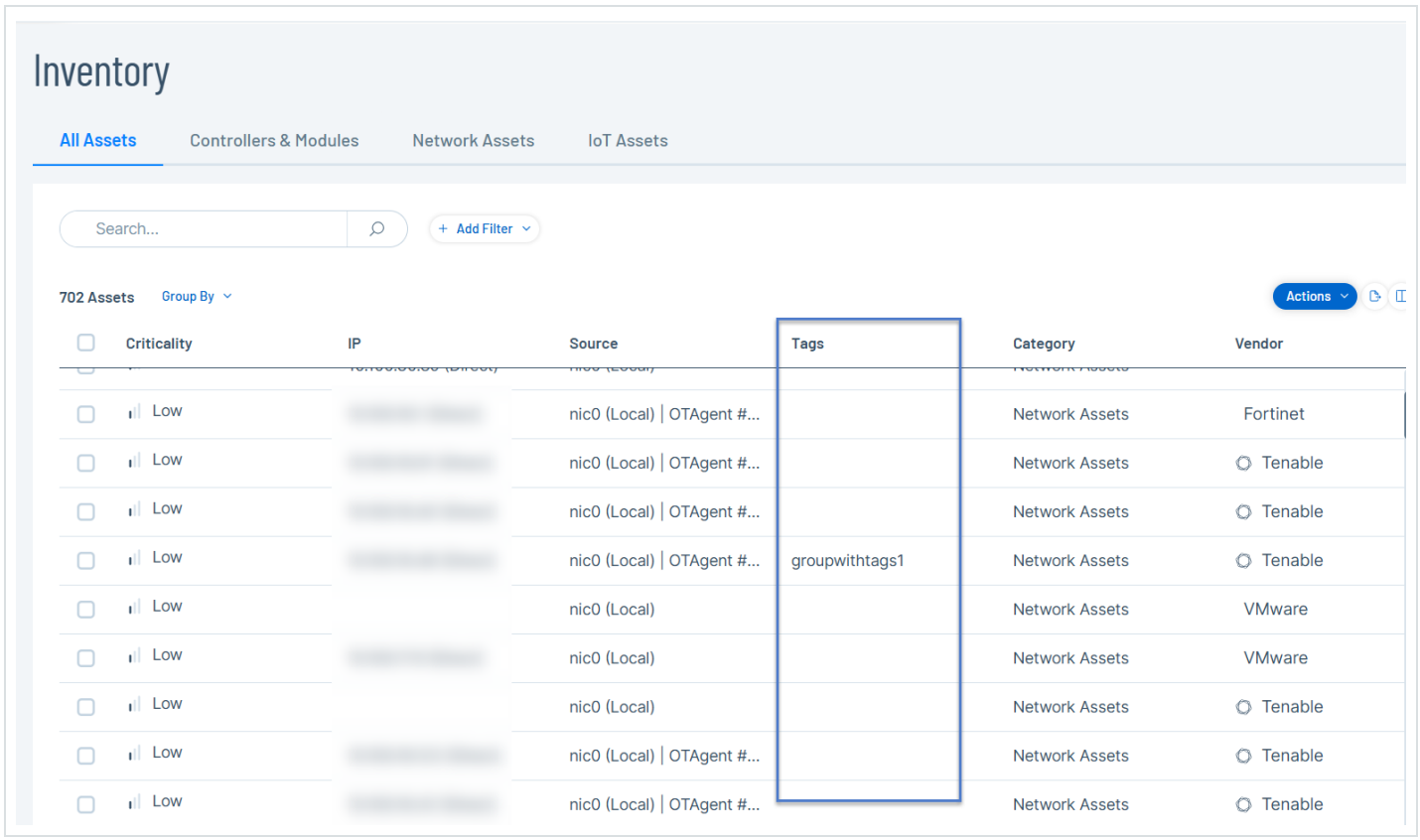
資産のタグを表示するには、資産グループの作成時に[メンバー資産にタグを表示]チェックボックスを選択します。



複数の資産のタグ表示を有効または無効にするには、複数の資産を選択し、[一括アクション] メニューから必要に応じて [タグ表示の有効化] または [タグ表示の無効化] を選択します。各資産の [タグを表示] 列にあるトグルを有効または無効にすることもできます。



これらの資産グループは、[インベントリ] > [すべての資産] ページの [タグ] 列に表示されます。



資産グループとタグの表示

[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。

ID	資産グループに割り当てられたID。
名前	ポリシーの名前。
タグを表示	[インベントリ] > [すべての資産] ページでタグの表示を有効にするトグル。
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、深刻度レベルセクションを参照してください。
発生元	資産グループの発生元: ユーザー定義またはシステム定義。
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。
タイプ	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にある資産。
タイプ	グループのタイプ。オプションは [静的] または [動的] です。
メン	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

バー	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。
ゾーンで使用	この資産グループを使用するゾーン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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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。

- 資産選択 – 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。

注意: 重複するネットワークの場合は、[資産選択] オプションを使用して資産グループを作成します。

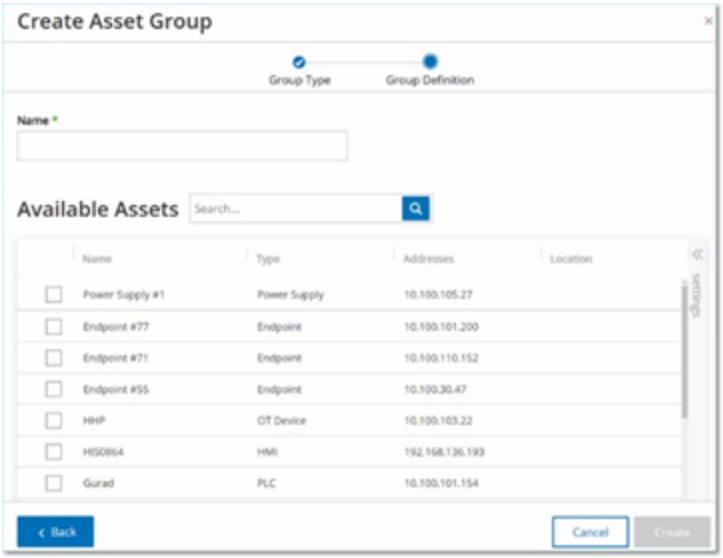
各タイプで資産グループを作成する手順は異なります。

資産選択タイプの資産グループの作成手順

1. [設定] > [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. 資産のタグを表示するには、[メンバー資産にタグを表示] チェックボックスを選択します。

   > 注意: このオプションが選択されている場合、OT Security は [インベントリ] > [すべての資産] ページの [タグ] 列にタグを表示します。

6. [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。
7. グループに含める各資産の横にあるチェックボックスを選択します。

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. [設定] > [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. [設定] > [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。

資産グループとタグの作成

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。必要な資産を選択するか、特定のカテゴリの資産をグループ化するフィルタールールを設定することで、グループを作成できます。選択した基準に基づいて資産を動的にグループ化することで、優先順位付けやレポート作成などのプロセスの効率化や拡張がしやすくなります。

資産グループを作成する方法

1. [グループ] > [資産グループとタグ] に移動します。

   [資産グループとタグ] ページが表示されます。
2. 資産グループを作成するには、[資産グループの作成] をクリックします。

   [資産グループの作成] ウィンドウが表示されます。

3. [グループのタイプ] セクションで、次のいずれかを選択します。

    - 静的 (手動選択) – 静的資産グループは、手動で資産を選択してグループに追加することで定義されます。いったんグループを設定すると、編集しない限り、そのメンバーは変更されません。

    - 動的 (ルールベース) – 動的資産グループは、ルールを使って資産インベントリをフィルタリングします。継続的な資産検出や情報更新に伴ってグループのメンバーは自動的に追加または削除され、グループは常に最新の状態に保たれます。

4. [次へ] をクリックします。

    [グループの定義] パネルが表示されます。

5. [名前] ボックスに、資産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. [静的] を選択した場合は、次の操作を行います。

    a. グループに含める資産の横にあるチェックボックスを選択します。

7. [動的] を選択した場合は、[フィルターを追加] をクリックしてグループ作成のルールを有効にします。資産のフィルタリングを参照してください。

    > 注意: グループ作成を有効にするには、少なくとも 1 つのフィルターを追加する必要があります。

8. 各資産のタグを表示するには、[メンバー資産にタグを表示] チェックボックスを選択します。このオプションはデフォルトで選択されています。

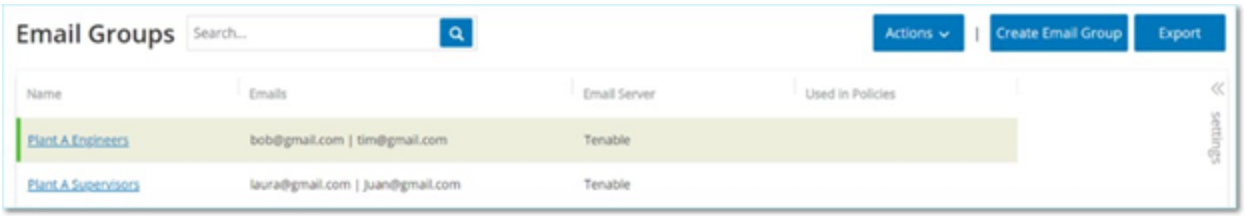
9. [作成] をクリックします。

    OT Security により資産グループが作成され、[資産グループとタグ] ページに表示されます。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。

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、職務や部門別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

必要なOT Securityユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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. [設定] > [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、ポリシーを設定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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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. [設定] > [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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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. [設定] > [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。
タイプ	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	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。

で使用	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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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. [設定] > [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. [設定] > [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。

コントローラータググループ

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。コントローラータググループは、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の不審な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、ファーネスに有害な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。

コントローラータググループの表示

[コントローラータググループ] ページには、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。

コントローラー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。
タイプ	タグのデータ型。可能な値には Bool、Dint、Float、Int、Long、Short、Unknown (OT Security が識別できない型のタグ)、Any Type (異なる型のタグを含めることが可能) があります。
コントローラー	タグがモニタリング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、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。

コントローラータググループの作成

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

ポリシー設定で使用するカスタムのコントローラー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することができます。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、指定されたタグの任意の値の変更だけです。特定の値を検出するように設定することはできません。

コントローラー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方法

1. [設定] > [グループ] > [コントローラータググループ] に移動します。
2. [コントローラータググループの作成] をクリックします。

   [コントローラー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、コントローラー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設定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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

新しいルールグループの作成手順

1. [設定] > [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

必要な OT Security ユーザーロール: 管理者、スーパーバイザー、セキュリティマネージャー

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。グループの編集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、目的のグループタイプを選択します。

   選択したグループタイプのページが表示されます

2. 表示するグループを選択します。

   OT Security は、[アクション] ボタンを有効にします。

3. 次のいずれかを行います。

   - [アクション] をクリックし、[表示]を選択します。
   - 目的のグループを右クリックし、[表示] を選択します。

4. [表示] を選択します。

   [グループの詳細] ページが表示されます。

グループの編集

既存のグループの詳細を編集できます。

グループの詳細の編集手順

1. [グループ] で、目的のグループタイプを選択します。

   選択したグループタイプのページが表示されます

2. [グループ] ページで、編集するグループを選択します。

   OT Security は、[アクション] ボタンを有効にします。

3. 次のいずれかを行います。

   - [アクション] をクリックし、[編集] を選択します。
   - 目的のグループを右クリックし、[編集] を選択します。

4. [編集] を選択します。

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

6. 必要に応じて変更します。

7. [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、目的のグループタイプを選択します。

   選択したグループタイプのページが表示されます。

2. 複製するグループを選択します。

   OT Security は、[アクション] ボタンを有効にします。

3. 次のいずれかを行います。

   - [アクション] をクリックし、[複製] を選択します。
   - 目的のグループを右クリックし、[複製] を選択します。

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。

グループを削除する方法

1. [グループ] で、目的のグループタイプを選択します。

   選択したグループタイプのページが表示されます

2. 削除するグループを選択します。

   OT Security は、[アクション] ボタンを有効にします。

3. 次のいずれかを行います。

   - [アクション] をクリックし、[削除] を選択します。
   - 目的のグループを右クリックし、[削除] を選択します。

4. [削除] 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。

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資産のデータを 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

必要な OT Security ユーザーロール: 管理者

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 を統合する方法

1. Tenable OT Security インターフェースで、[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

必要なOT Securityユーザーロール: 管理者

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を統合する方法

1. Tenable OT Securityインターフェースで、[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

必要な OT Security ユーザーロール: 管理者

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)

必要な OT Security ユーザーロール: 管理者

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) と統合する方法

1. Tenable OT Security インターフェースで、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 により、統合が保存されます。

Aruba - ClearPass Policy Manager

必要な OT Security ユーザーロール: 管理者

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方法

1. Tenable OT Security インターフェースで、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 により、統合が保存されます。

Tenable One との統合

OT Security を Tenable One と統合することで、Tenable サイバーエクスポージャー管理上で資産とリスクスコアのデータを確認できます。

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。

統合後、OT Security は Tenable One に次のデータを送信します。

- OT Security は、すべての資産と資産属性を、[サイバーエクスポージャー管理] > [インベントリ] ページと同期します。これらの属性には、ベンダー、メーカー、モデル、状態、ファームウェア、シリアル番号が含まれます。同期の対象となるフィールドは次の通りです。
    - OT_BACKPLANE_ID
    - OT_BACKPLANE_NAME
    - OT_CATEGORY
    - OT_CRITICALITY
    - OT_DESCRIPTION
    - OT_FAMILY
    - OT_FIRMWARE
    - OT_ID
    - OT_LOCATION
    - OT_MODEL
    - OT_SERIAL_NUMBER
    - OT_SLOT
    - OT_STATE
    - OT_VENDOR

- OT_SENSOR_NAME
- OT_DIRECT_IP_ADDRESSES
- OT_RISK

- プラグイン ID、プラグイン名、プラグイン出力など、資産に関連付けられているすべての脆弱性の検出結果。Tenable One はこのデータを使用して、各資産の脆弱性ステータスが [アクティブ] か [修正済み] であるかを追跡します。
- (バージョン 4.4 以降) 各資産に関連付けられているすべてのポリシー違反の検出結果。このデータには、ポリシーイベントタイプ、イベントを説明する詳細なプラグイン出力、関係する資産が含まれます。また、観察されたアクティビティに関連する MITRE ATT&CK 戦術、技術、手順 (TTP) も含まれます。
- (バージョン 4.5 以降) 資産に関連付けられたすべての動的タグ。これらは Tenable One では外部タグとして表示されます。

> 注意: OT Security の検出結果は Tenable Vulnerability Management には表示されません。ただし、Tenable Vulnerability Management と OT Security を統合している場合、スキャンで OT Discovery エンジンを使用している場合は除きます。

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 との統合方法

1. Tenable OT Security インターフェースで、[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。

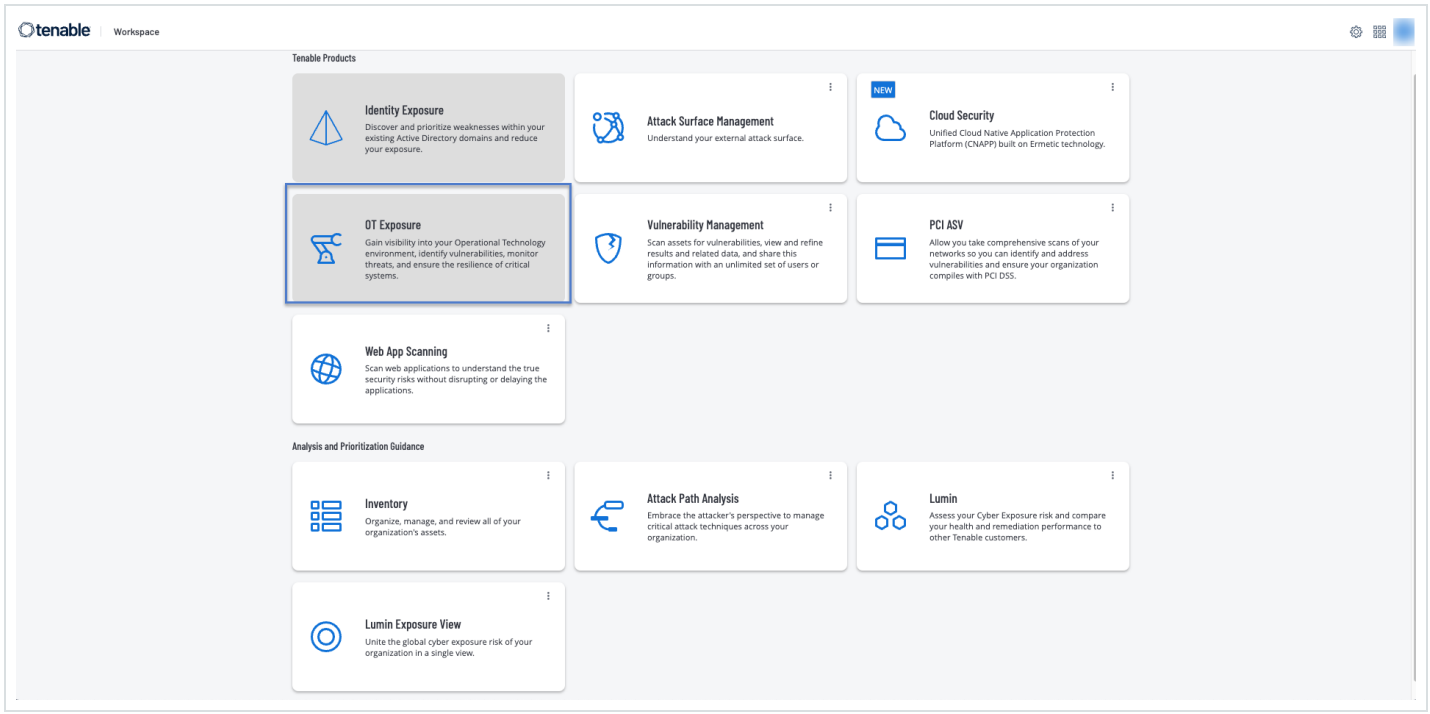
   > **注意:** 既にペアリングされているサイトの名前を OT Security で変更した場合、センサー名を新しいサイト名と一致するよう Tenable Vulnerability Management 内で手動で変更できます。または、OT Security と Tenable Vulnerability Management の両方で統合を削除し、再度ペアリングすればサイト名の変更を自動的に更新できます。

Tenable One に 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。

Tenable One の SAML 統合の設定

SSO を使用して OT Security にアクセスするように Tenable One インスタンスで SAML を設定します。

Tenable One [ワークスペース] ページの [OT エクスポージャー] タイルは、デフォルトでは無効になっています。[OT エクスポージャー] タイルを有効にするには、まず Tenable One の SAML を設定する必要があります。



始める前に

- 有効な Tenable One および OT Security のライセンスがあることを確認してください。

Tenable OT Security の SAML を設定する方法

1. Tenable One から SAML アイデンティティプロバイダー (IDP) の詳細とグループオブジェクト ID を取得します。

   a. サポートされているブラウザで https://cloud.tenable.com にログインし、[ワークスペース] ページにアクセスします。

   b. 右上の ⚙ ボタンをクリックします。

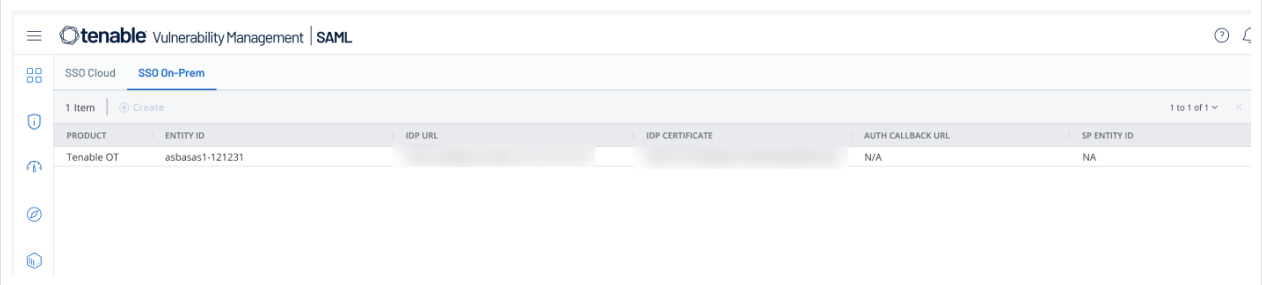
   [設定] ページが表示されます。

c. [SAML] タイルをクリックします。

[SAML] ページが表 示されます。

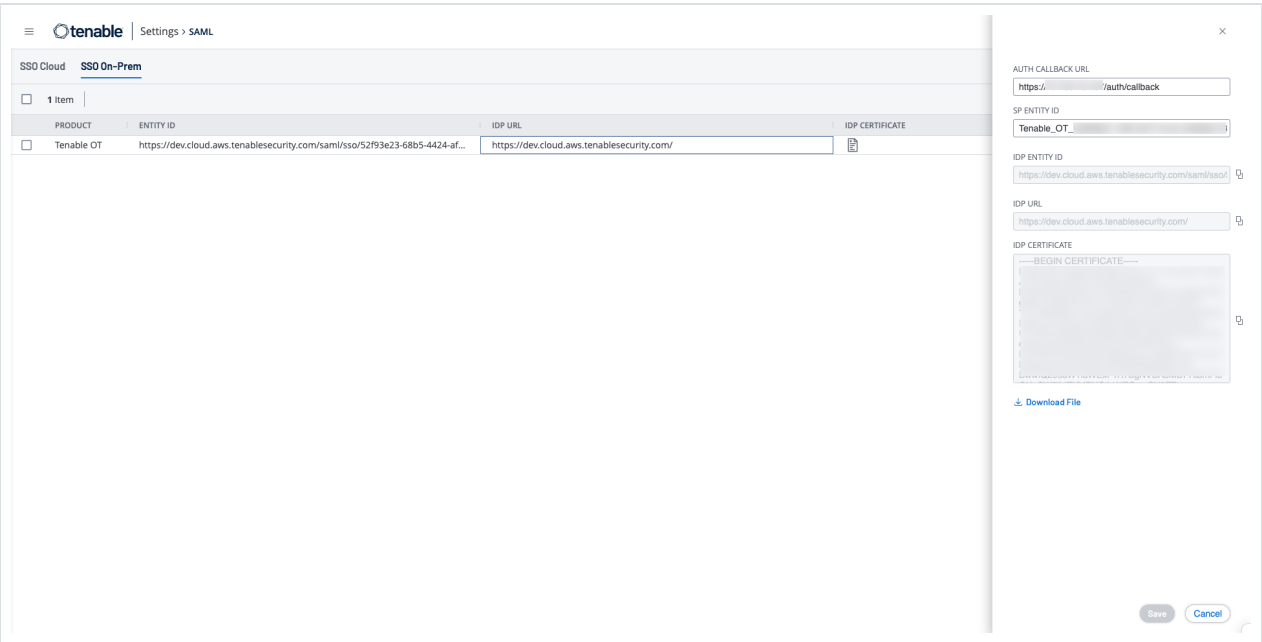
d. [SSO オンプレミス] タブをクリックします。

[SSO オンプレミス] ページが表 示され、Tenable OT Securityの SSO 設 定 が表 示されます。



e. Tenable OT Security 行 にカーソルを合 わせてクリックします。

右 側 に IDP の詳 細 パネルが表 示されます。



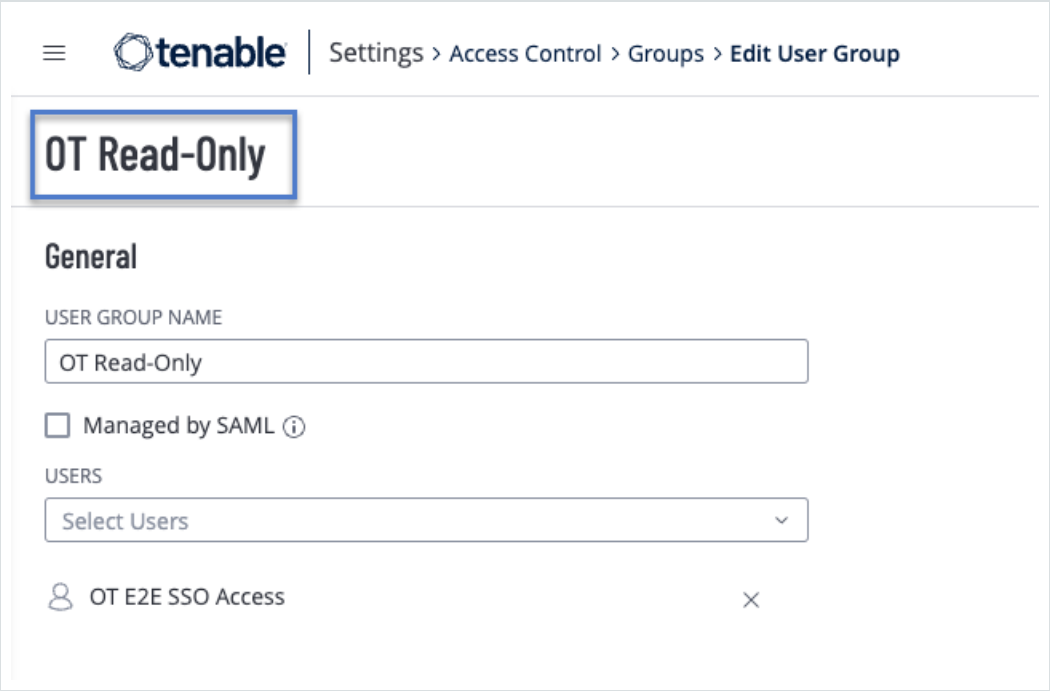
f. ボタンを使 用して、次 の詳 細をコピーします。

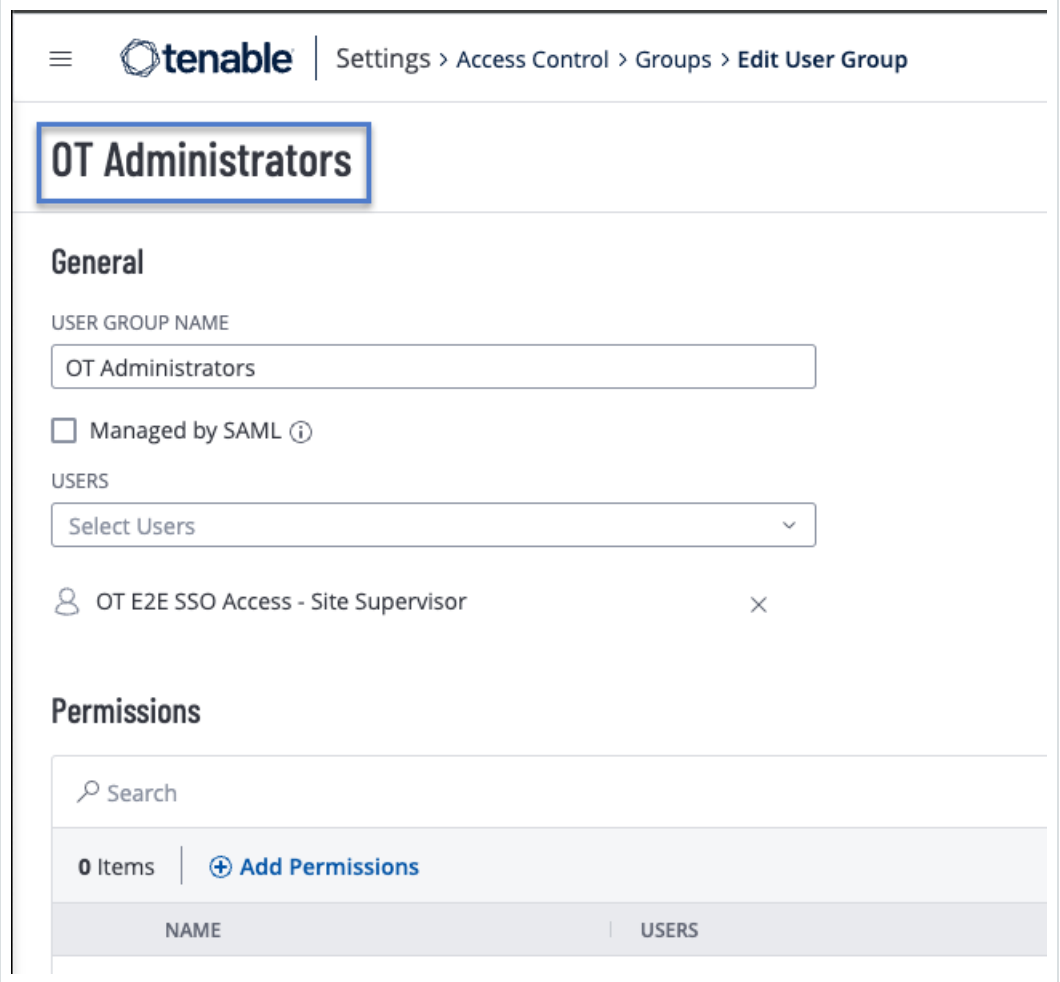
- IDP エンティティ ID
- IDP URL
- IDP 証明書

g. [ファイルのダウンロード] をクリックして、ローカルシステムに証明書をダウンロードします。

h. グループのマッピングデータを取得します。グループオブジェクト ID 情報を表示するには、[設定] > [アクセス制御] > [グループ] に移動し、関連するグループを見つけるか追加します。

たとえば、Tenable One で、[OT 管理者] と [OT 読み取り専用] の 2 つのグループを作成します。OT Security のユーザーロールにマッピングするには、これらのグループ名を、OT Security [SAML] ページの [管理者グループオブジェクト ID] フィールドと [読み取り専用ユーザーグループオブジェクト ID] フィールドにそれぞれ追加します。


Settings > Access Control > Groups > Edit User Group
OT Read-Only
General
USER GROUP NAME
OT Read-Only
Managed by SAML
USERS
Select Users
OT E2E SSO Access


Settings > Access Control > Groups > Edit User Group
OT Administrators
General
USER GROUP NAME
OT Administrators
Managed by SAML
USERS
Select Users
OT E2E SSO Access - Site Supervisor
Permissions
Search
0 Items
Add Permissions
NAME
USERS

2. OT Security で SAML を次のように設定します。

    a. OT Security にログインします。

    b. 設定] > [ユーザー管理] > [SAML] に移動します。

    [SAML] ページが表示されます。

    c. [設定]、既存の設定を編集する場合は [編集] をクリックします。

    [SAML の設定] ページが表示されます。

    d. Tenable One [SAML] > [SSO オンプレミス] ページからコピーした次の詳細を入力します。

        a. [IDP ID] ボックスに、Tenable One SAML ページからコピーした [IDP エンティティ ID] を貼り付けます。

        b. [IDP URL] ボックスに、Tenable One SAML ページからコピーした [IDP URL] を貼り付けます。

        c. [証明書データ] ボックスで、証明書ファイルをダウンロードした場所を参照し、そのファイルをアップロードします。

        d. [ユーザー名属性] ボックスに次の情報を入力します。

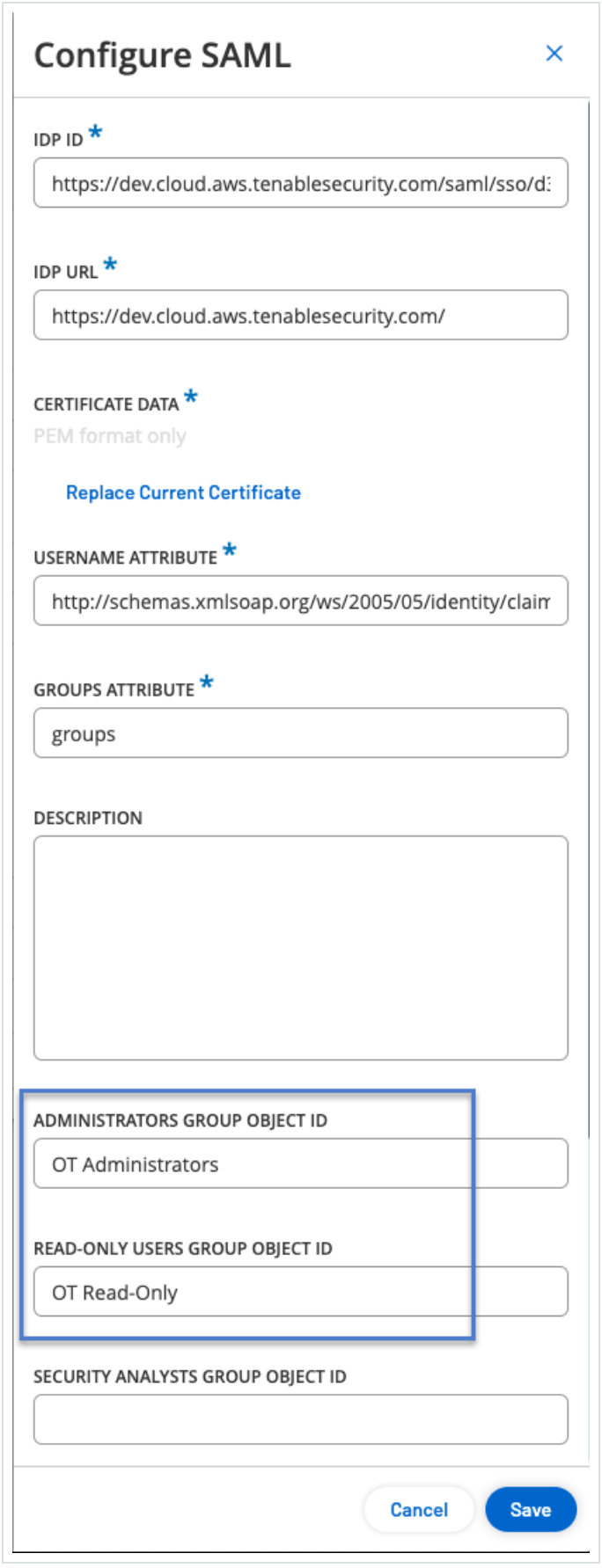
        ```
        http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
        ```

        e. [グループ属性] ボックスに、**groups** と入力します (Groups ではなく、小文字にする必要があります)。

        f. Tenable One から取得したグループオブジェクト ID 情報を入力します。

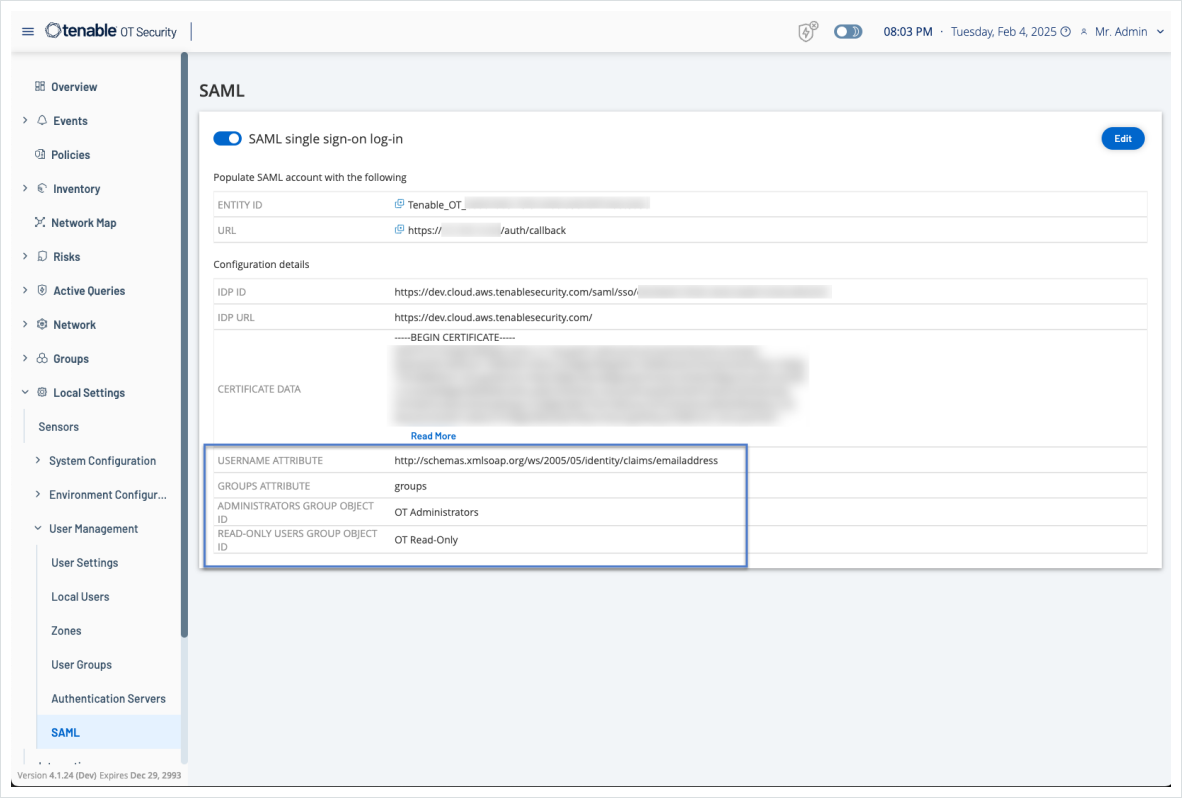
        たとえば、ステップ h で、[OT 管理者] と [OT 読み取り専用] の 2 つのグループを Tenable One で作成しました。これらのグループ名を、[SAML の設定] ページの [管理

者 グループオブジェクト ID] フィールドと [読み取り専用ユーザーグループオブジェクト ID] フィールドにそれぞれ追加します。


Configure SAML
IDP ID *
https://dev.cloud.aws.tenablesecurity.com/saml/sso/d
IDP URL *
https://dev.cloud.aws.tenablesecurity.com/
CERTIFICATE DATA *
PEM format only
Replace Current Certificate
USERNAME ATTRIBUTE *
http://schemas.xmlsoap.org/ws/2005/05/identity/claim
GROUPS ATTRIBUTE *
groups
DESCRIPTION
ADMINISTRATORS GROUP OBJECT ID
OT Administrators
READ-ONLY USERS GROUP OBJECT ID
OT Read-Only
SECURITY ANALYSTS GROUP OBJECT ID
Cancel
Save

g. [保存] をクリックします。

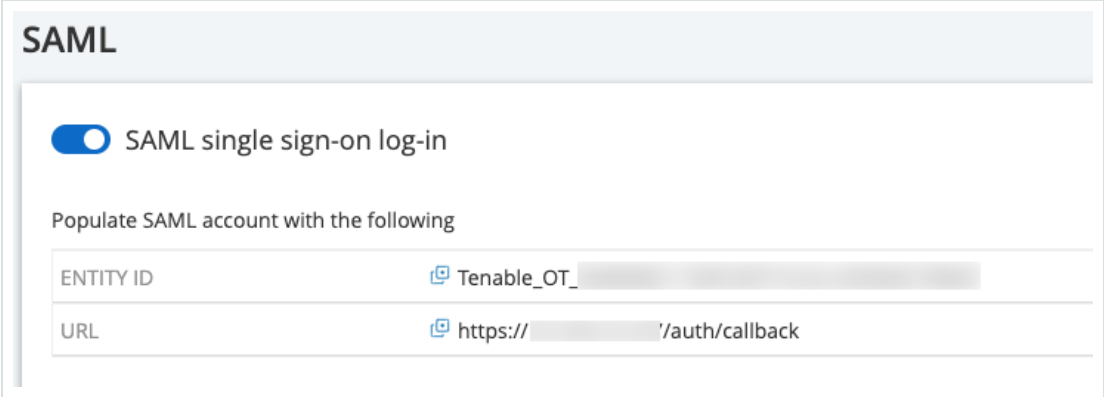
OT Security により設定が保存され、次の情報が表示されます。



> 重要: 設定の保存後は再起動しないでください。OT Security とTenable One の両方で設定手順を完了してから、再起動してください。

h. [SAML] ページで、次の値をコピーします。これらの値は、Tenable One の最終的な設定で必要になります。

- エンティティ ID
- URL



3. Tenable One で最終的な設定を完了します。

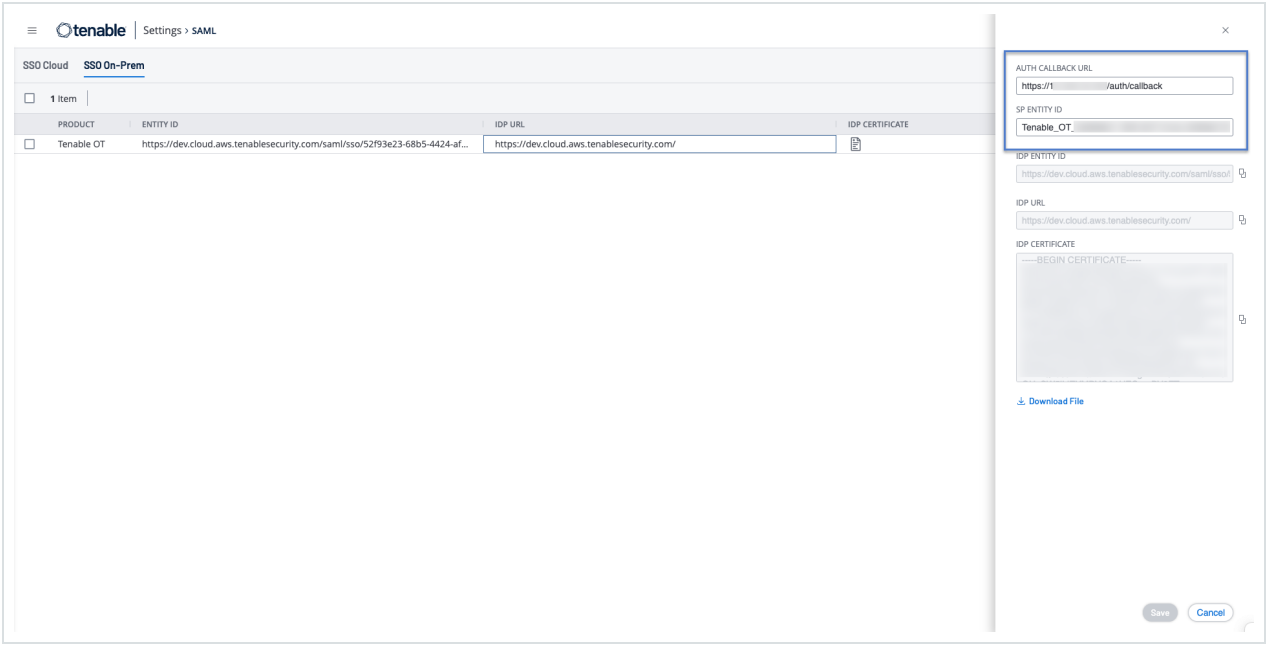
   a. Tenable One で、[設定] > [SAML]> [SSO オンプレミス] ページに移動します。

      [SSO オンプレミス] ページが表示され、Tenable OT Securityの SSO 設定が表示されます。

   b. OT Security 行をクリックします。

      OT Security 設定の詳細パネルが表示されます。

   c. [認証コールバック URL] と [SP エンティティ ID] に、OT Security の [SAML] ページでコピーした詳細を入力します。



d. [保存] をクリックします。

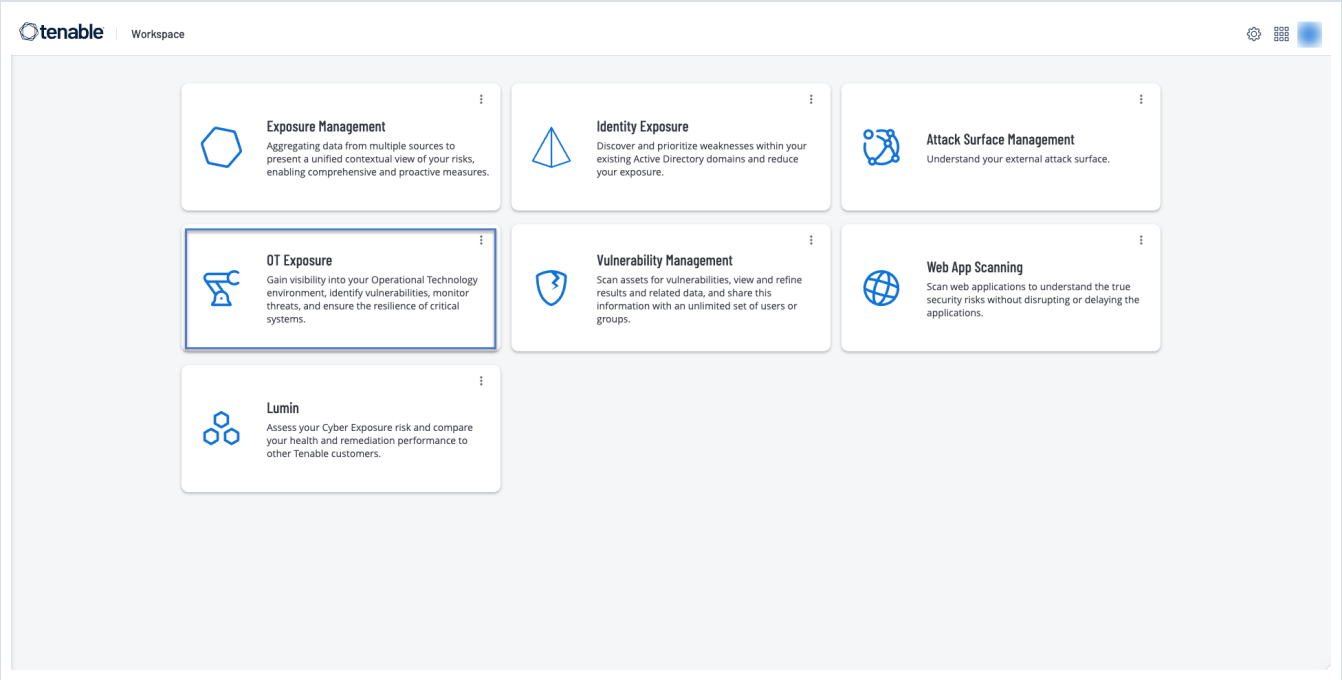
OT Security により SAML 設定が保存されます。

4. [SAML シングルサインオンログイン] トグルをクリックして SAML を有効にします。

OT Security により再起動を促すメッセージが表示されます。

5. OT Security を再起動します。

Tenable が、[ワークスペース] ページの [OT エクスポージャー] タイルを有効にします。[OT エクスポージャー] タイルをクリックし、OT Security にアクセスします。



サーバー

> 必要な OT Security ユーザーロール: 管理者、スーパーバイザー

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. 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。

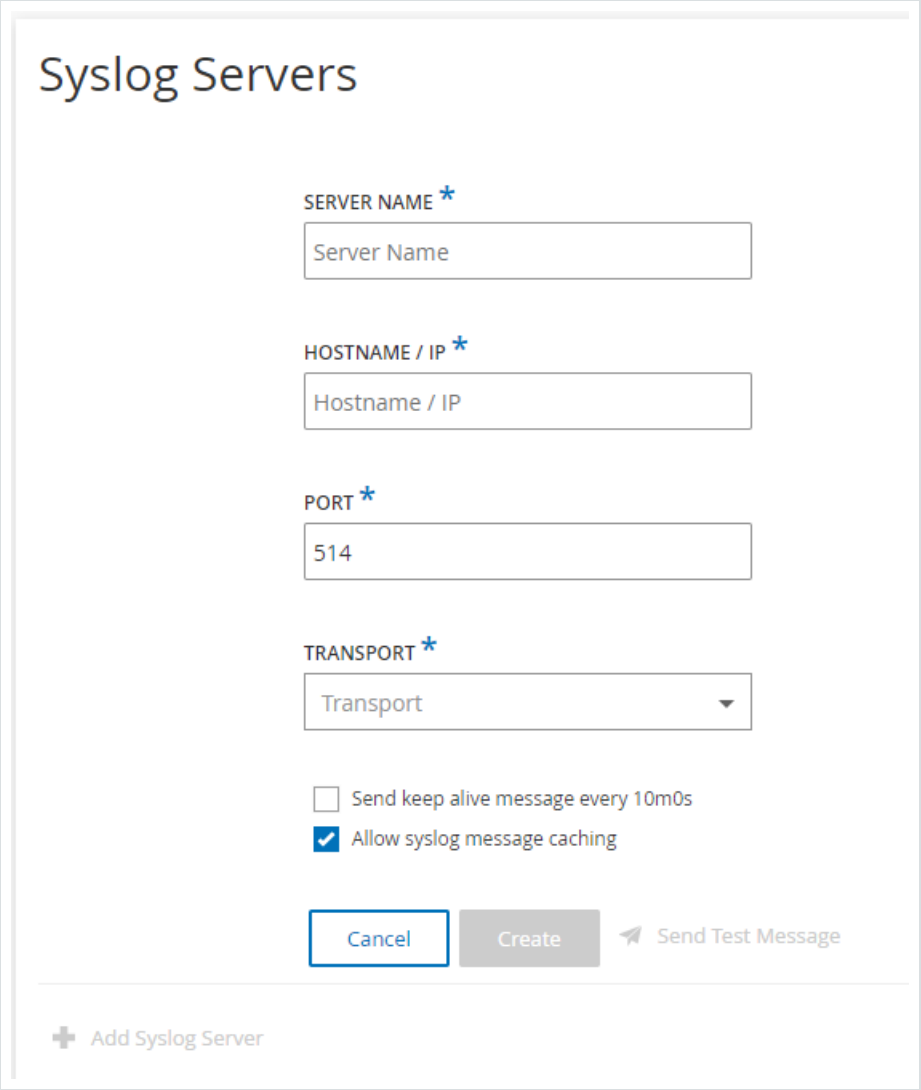
   追加の SMTP サーバーを設定するには、この手順を繰り返します。

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. 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 メッセージは状態を認識せず、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. [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。

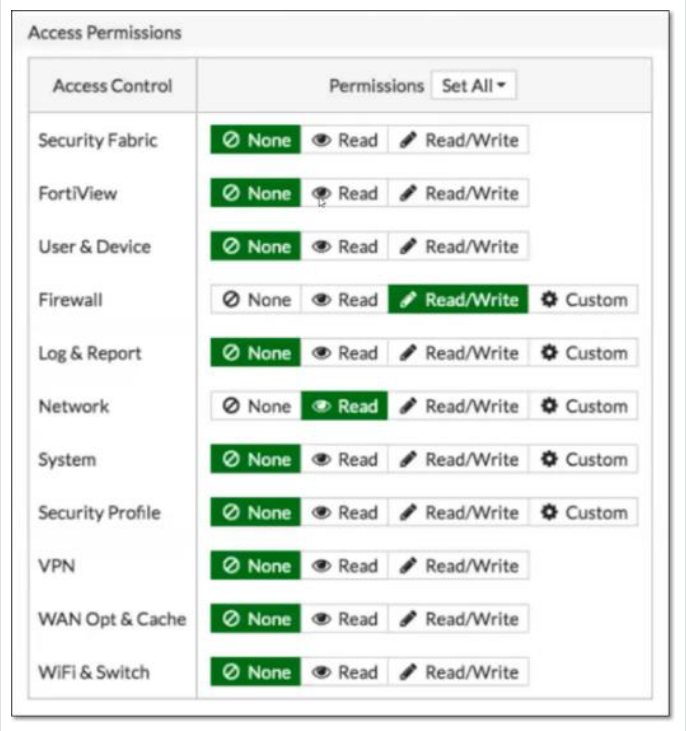
> 注意: FortiGate API トークンを生成する手順については、次のページを参照してください。
> https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token

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

> 必要な OT Security ユーザーロール: 管理者

[システムログ] ページでは、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) がリスト表示されます。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。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。

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、ユーザー名はありません。

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. 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. 必要な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 Azure とSAML の統合

OT Security では、SAML プロトコルを使用した Azure 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る Azure ユーザーが、シングルサインオン (SSO) で 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合わせて、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 Azure の SSO 統合を設定するフロー全体について説明します。それには、Azure で OT Security アプリケーションを作成して統合を設定することも含まれます。その後、この新しく作成された OT Security アプリケーションに関する情報を提供し、ご利用の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できます。グループをアイデンティティプロバイダーから OT Security のユーザーグループにマッピングして、設定を完了させます。

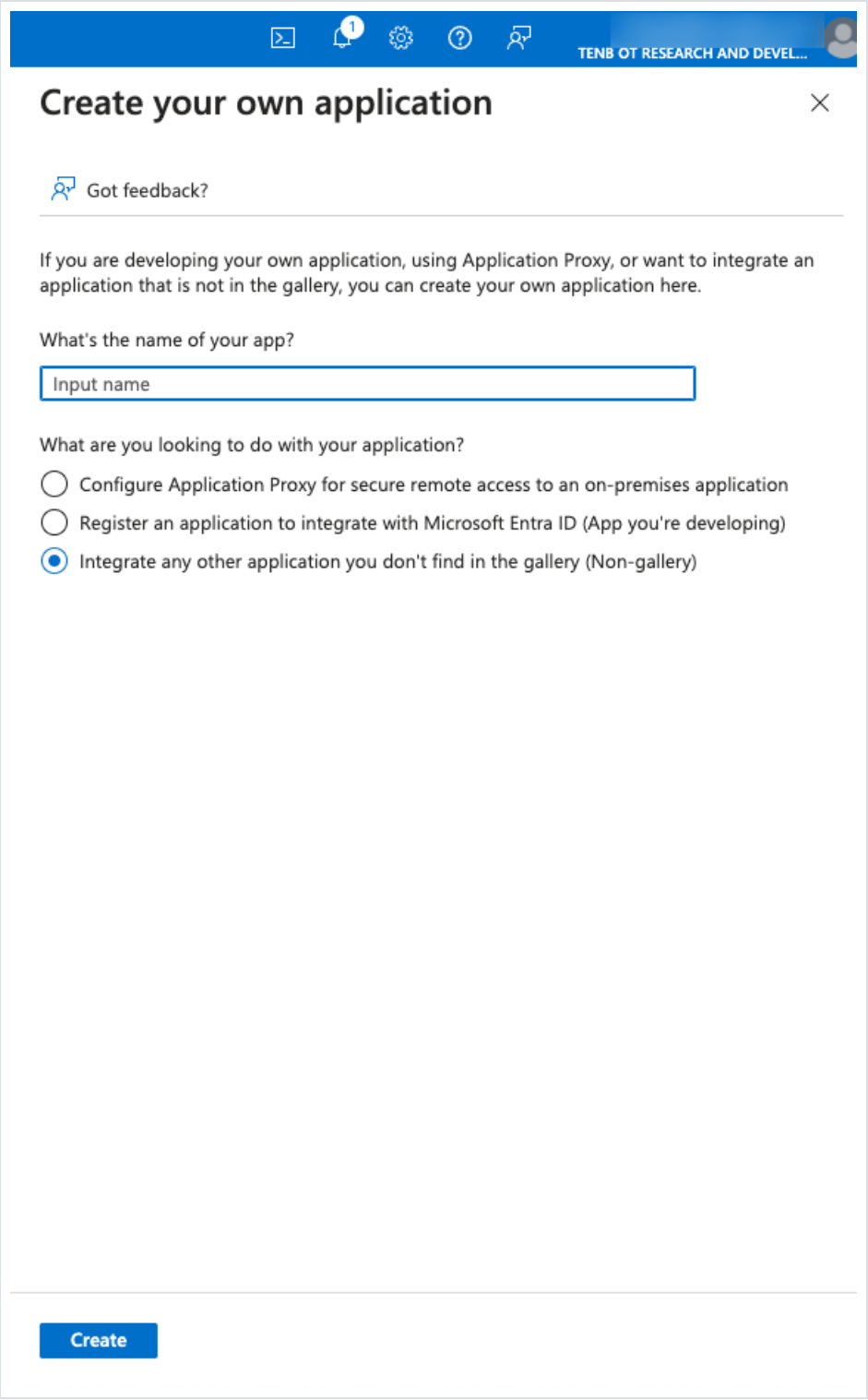
この設定を行うには、Microsoft Azure と OT Security の両方に管理ユーザーとしてログインする必要があります。

手順 1 - Azure で Tenable アプリケーションを作成する

Azure で Tenable アプリケーションを作成する方法

1. Azure で、Microsoft Entra ID > [Enterprise Applications](エンタープライズアプリケーション) に移動し、[+ New application](+ 新しいアプリケーション) をクリックします。

   [Browse Microsoft Entra ID Gallery](Microsoft Entra ID ギャラリーを参照する) ページが表示されます。



2. [+ Create your own application](+ 自分のアプリケーションを作成する) をクリックします。

   [Create your own application](自分のアプリケーションを作成する) サイドパネルが表示されます。

3. [What's the name of your app?](アプリケーションの名前) ボックスで、アプリケーションの名前 (Tenable_OT など) を入力し、[Integrate any other application you don't find in the gallery (Non-gallery)](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) 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 - 初期設定をする

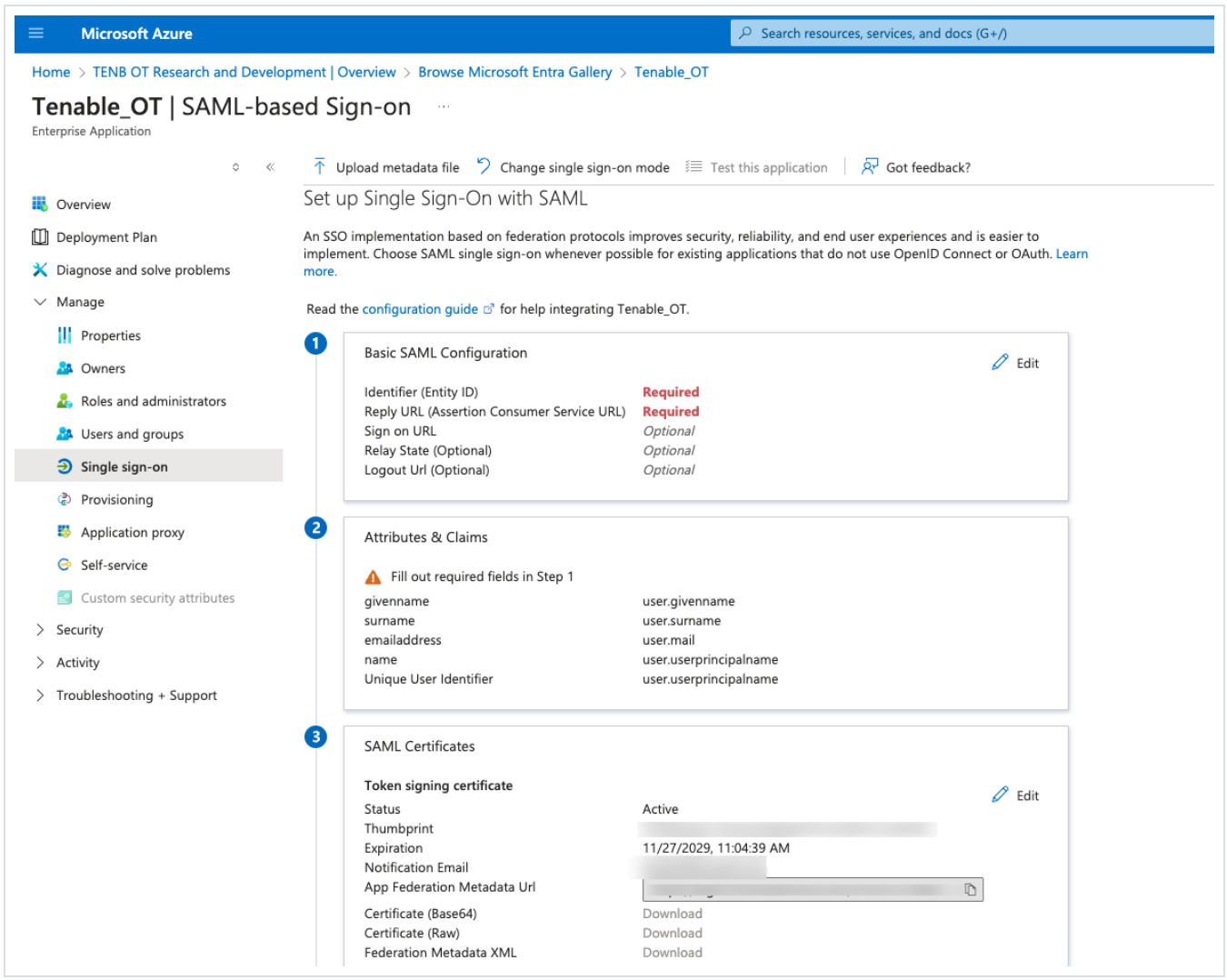
この手順では、Azure で OT Security アプリケーションの初期設定を行います。これには、基本 SAML 設定値 (識別子および応答 URL) の一時的な値を作成して、必要な証明書をダウンロードすることが含まれます。

> 注意: この手順で記載されているパラメーターのみを設定してください。その他のパラメーターはデフォルト値のままにします。

初期設定を実行する方法

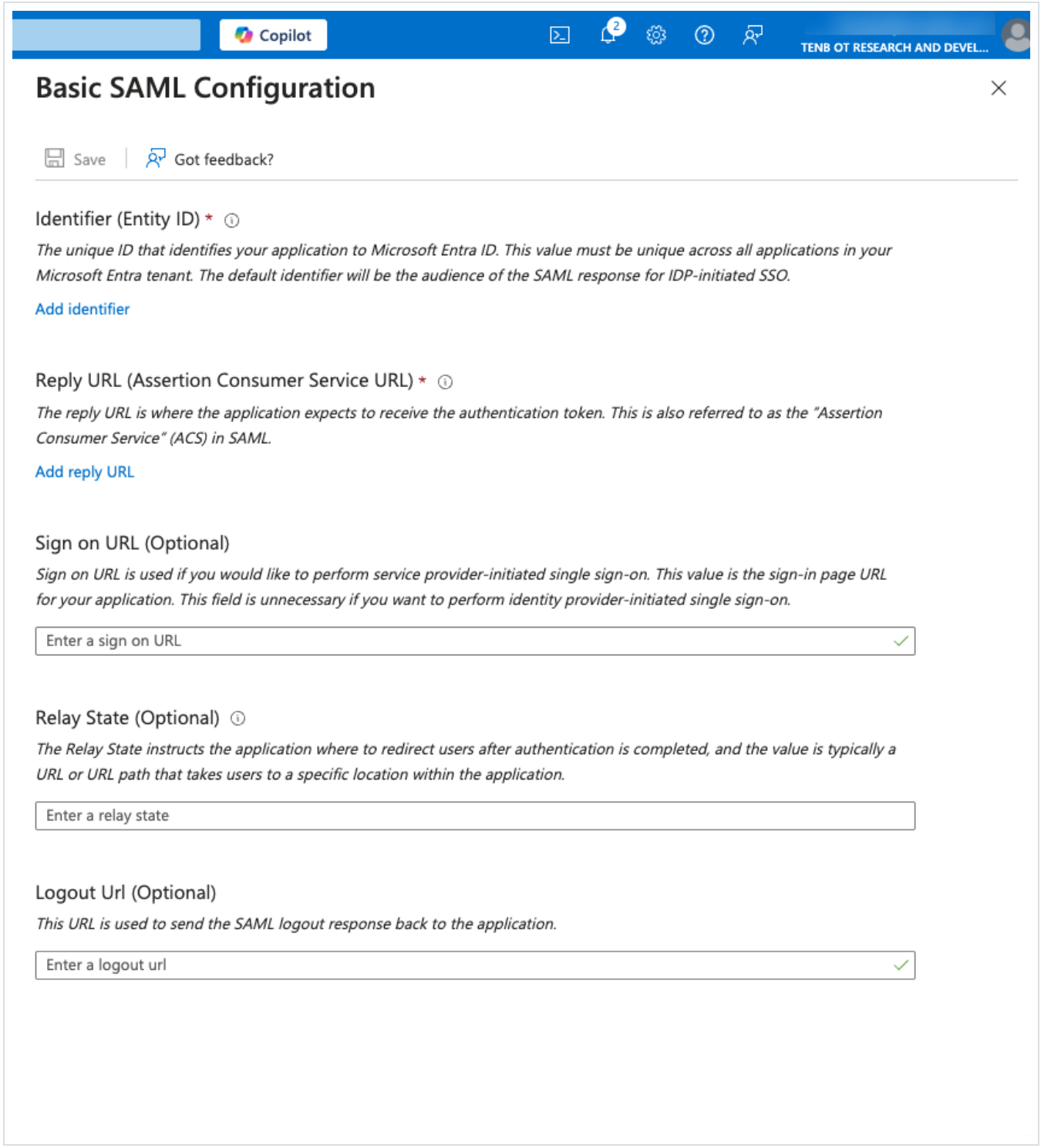
1. Azure ナビゲーションメニューで、[Single sign-on](シングルサインオン) をクリックし、シングルサインオンの方法として SAML を選択します。

   [SAML-based Sign-on](SAML ベースのサインオン) ページが表示されます。



2. セクション 1 [Basic SAML Configuration](基本 SAML 設定) の [編集] をクリックします。

[Basic SAML Configuration](基本 SAML 設定) サイドパネルが表示されます。



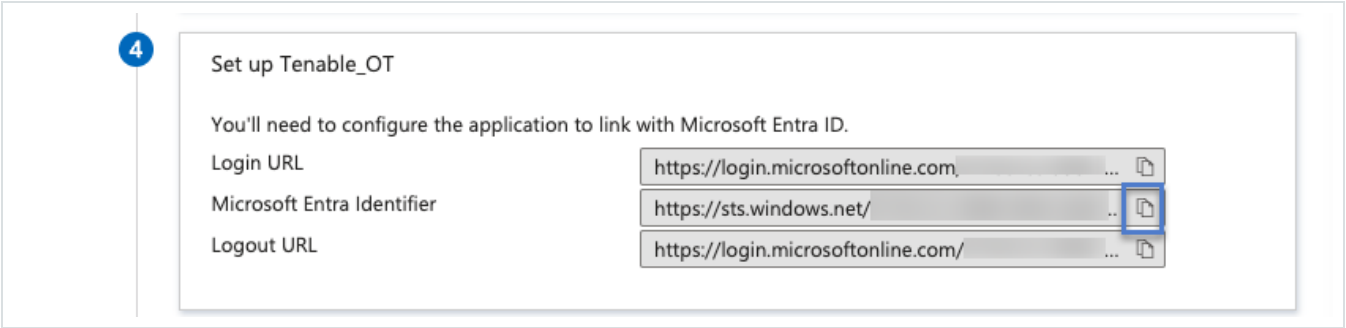
3. [識別子 (エンティティ ID)] ボックスに、Tenable アプリケーションの一時 ID (例: `tenable_ot`) を入力します。

4. [Reply URL (Assertion Consumer Service URL)](応答 URL (アサーションコンシューマサービス URL)) ボックスに、有効な URL (例: `https://OT Security`) を入力します。

   > 注意: [識別子] と [応答 URL] の値は一時的な値であり、その後の設定プロセスで変更可能です。

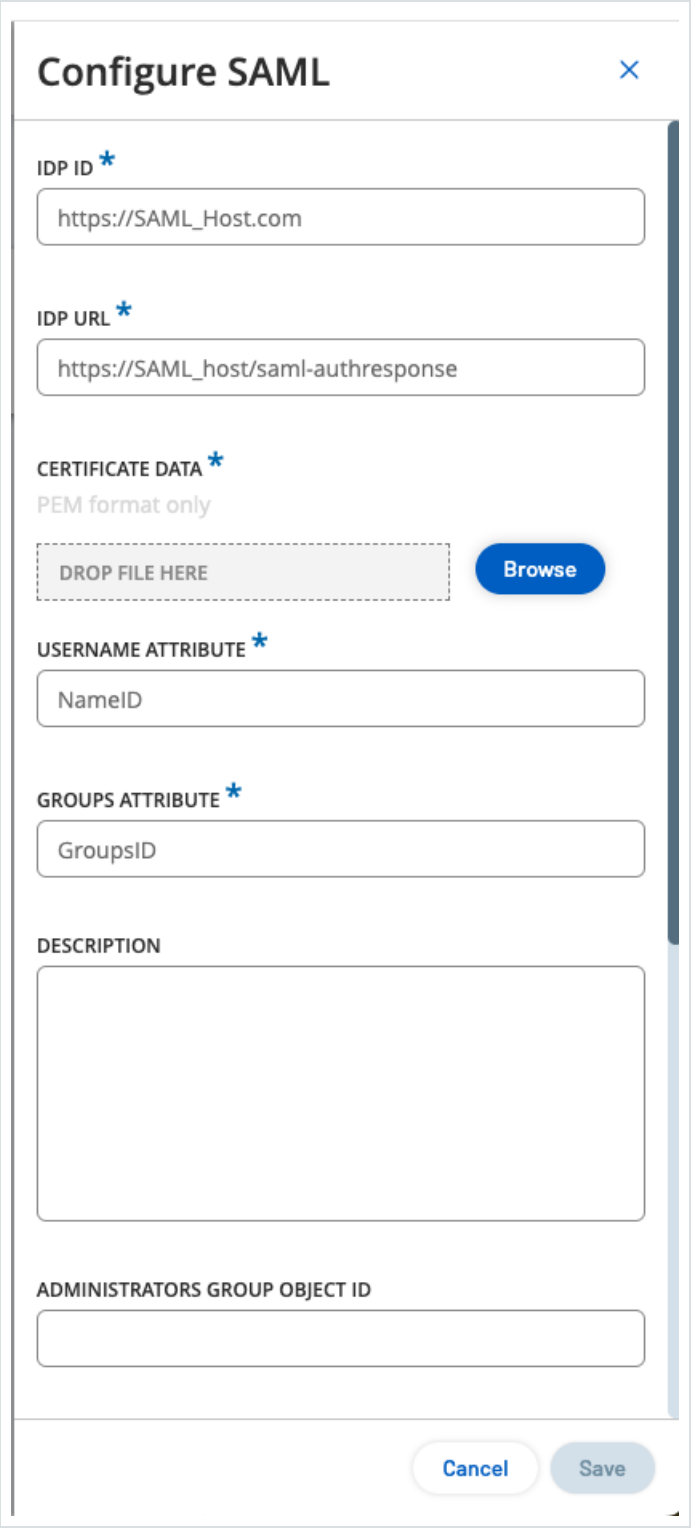
5. [保存] をクリックして一時的な値を保存し、[Basic SAML Configuration](基本 SAML 設定) サイドパネルを閉じます。

6. セクション 4 [セットアップ] で、ボタンをクリックして [Microsoft Entra ID Identifier](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、[ユーザー管理] > [SAML] に移動します。

8. [Configure](設定) をクリックして [Configure SAML](SAML の設定) サイドパネルを表示し、コピーした値を [IDP ID] ボックスに貼り付けます。



9. Microsoft Azure コンソールで、 ボタンをクリックして [ログイン URL] をコピーします。

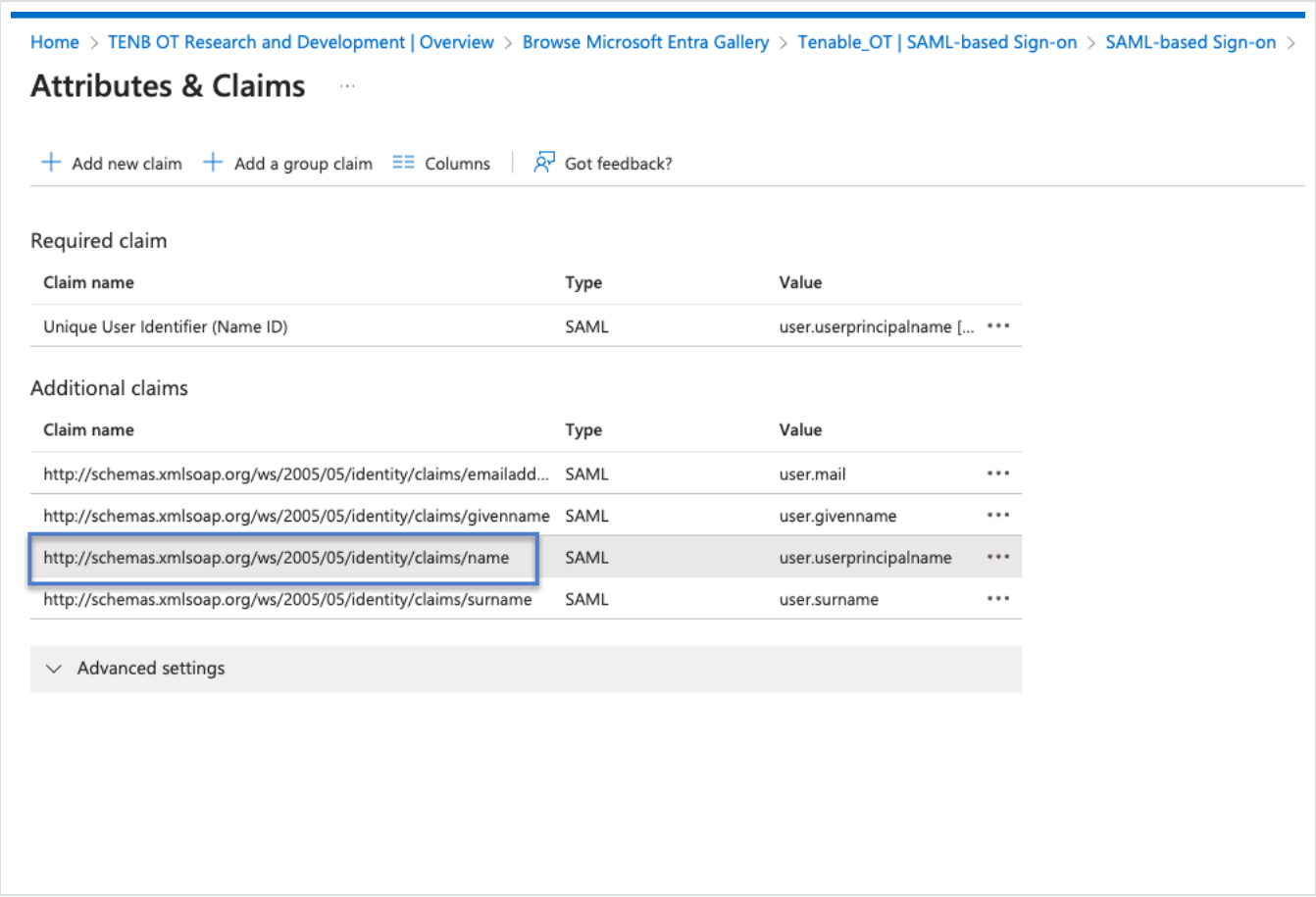
10. OT Security コンソールに戻り、コピーした値を [IDP URL] ボックスに貼り付けます。

11. Azure コンソールのセクション 3 [SAML Certificates](SAML 証明書) で、[Certificate (Base64)](証明書 (Base64)) の [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、[Certificate Data](証明書データ) セクションで、セキュリティ証明書ファイルを参照して選択します。

13. Azure コンソールのセクション 2 [Attributes & Claims](属性とクレーム) の [編集] をクリックします。

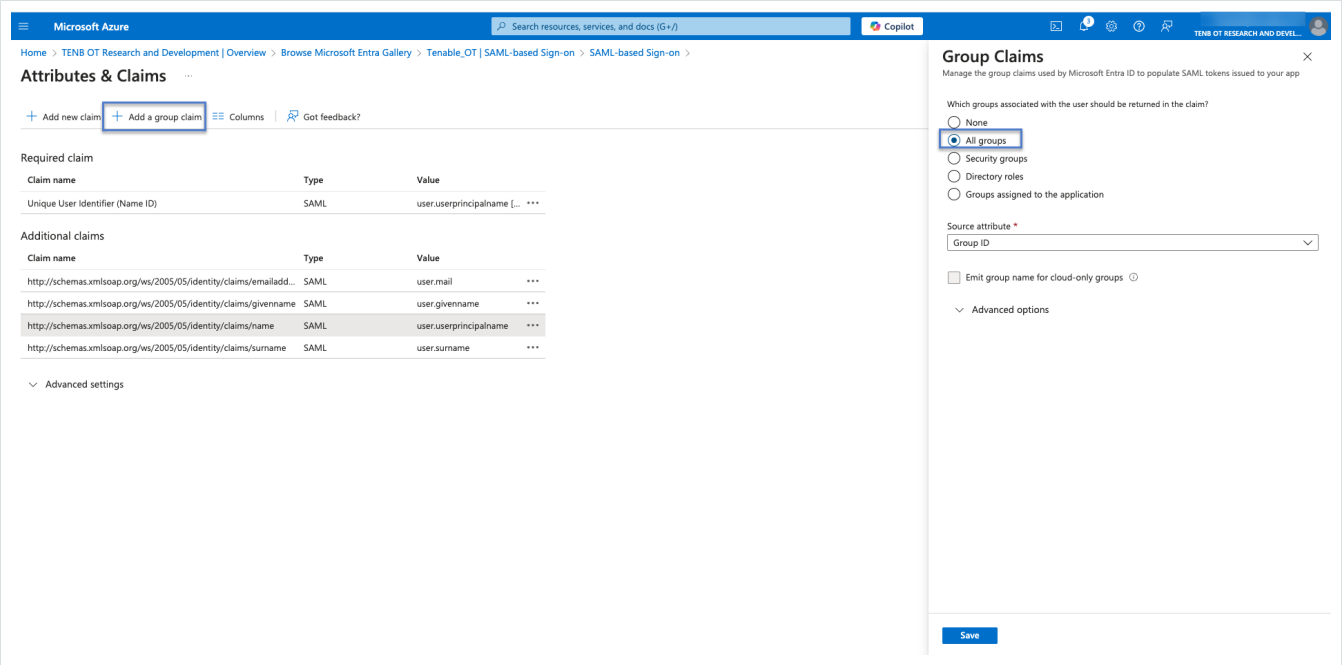
14. [Additional claims](追加のクレーム) セクションで、[値] が user.userprincipalname になっている [Claim name](クレーム名) の URL を選択してコピーします。



15. OT Security コンソールに戻り、この URL を [Username Attribute](ユーザー名属性) ボックスに貼り付けます。

16. Azure コンソールで、[+ Add a group claim](+ グループクレームを追加する) をクリックします。

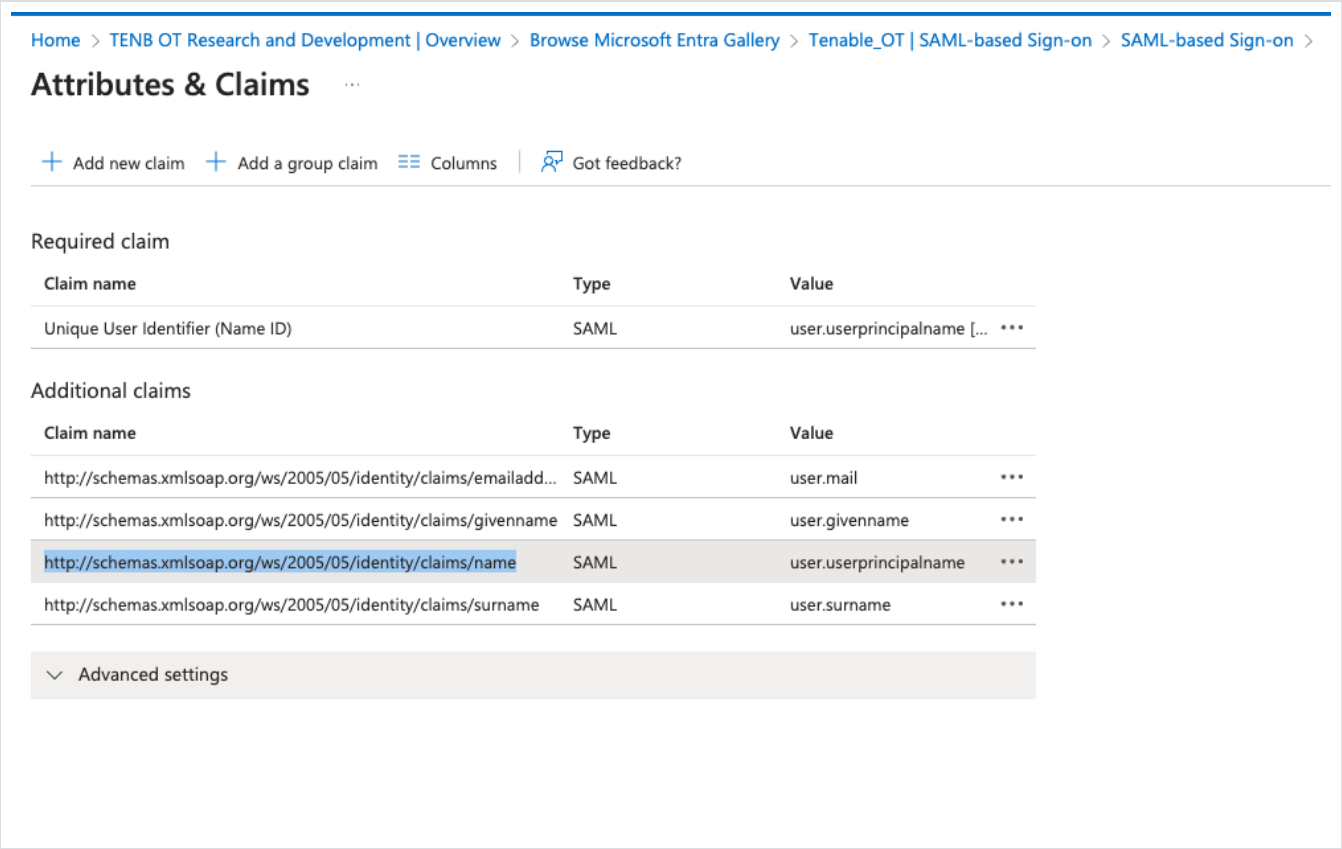
    [Group Claims](グループクレーム) サイドパネルが表示されます。



17. [Which groups associated with the user should be returned in the claim?] セクションで、[すべてのグループ] を選択し、[保存] をクリックします。

    > 注意: 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 [Groups assigned to the application](アプリケーションに割り当てられているグループ) を選択することができます。こうすると、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だけを提供します。

18. [Additional claims](追加のクレーム) セクションで、[値] が user.groups [すべて] になっている [Claim name](クレーム名) の URL をハイライト表示してコピーします。



19. OT Security コンソールに戻り、コピーした URL を [Groups Attribute](グループ属性) ボックスに貼り付けます。

20. (オプション) [説明] ボックスに SAML 設定の説明を追加します。

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、Azure ユーザーを OT Security アプリケーションに割り当てます。各ユーザーに付与されるアクセス許可は、その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の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、ユーザー管理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ている少なくとも 1 つのグループに割り当てられる必要があります。

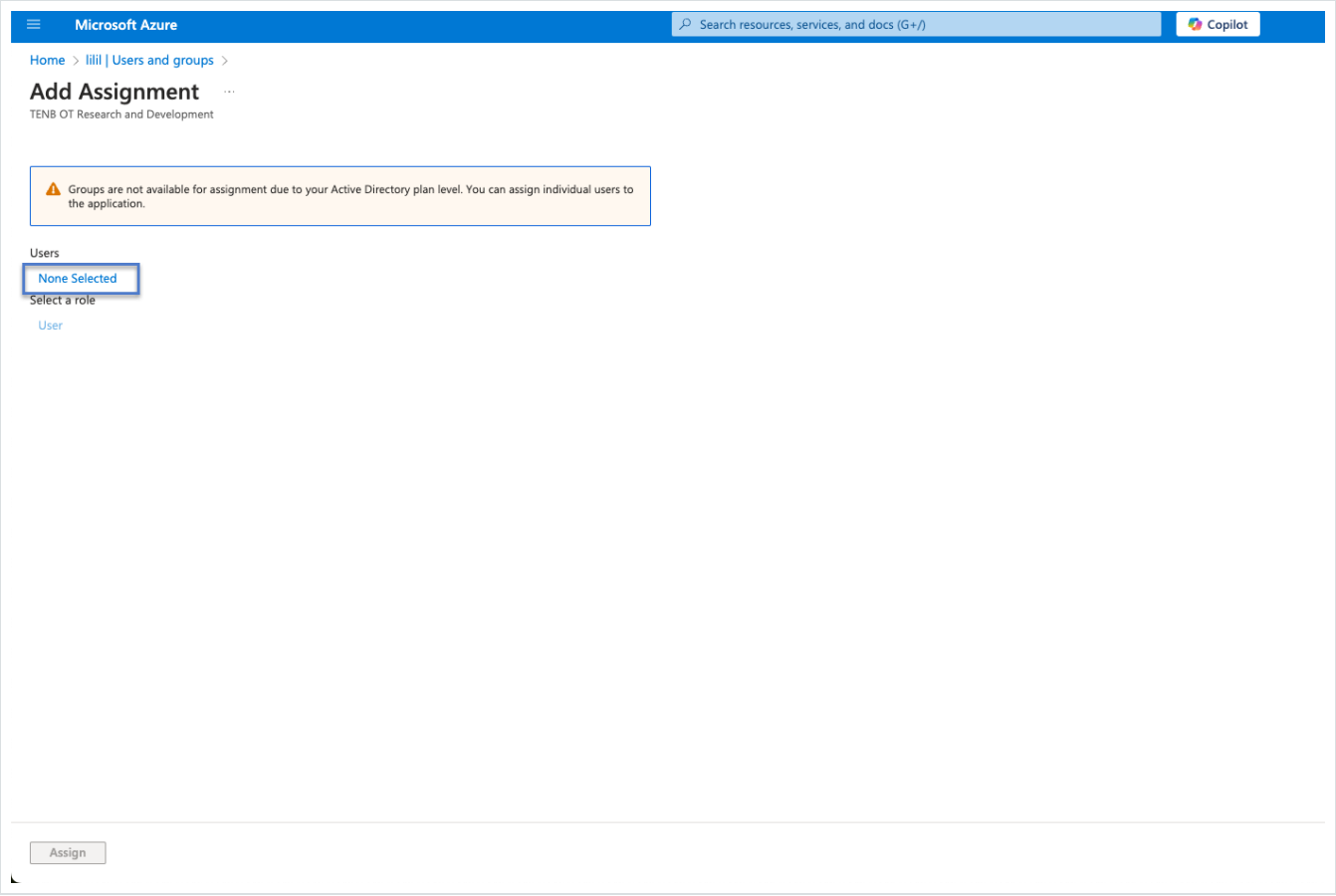
注意: SAML 経由でログインした管理者ユーザーは、管理者 (外部) ユーザーと見なされ、ローカル管理者のすべての権限は付与されません。複数のユーザーグループに割り当てられたユーザーには、それらのグループの中から最高のアクセス許可が付与されます。

Azure ユーザーを OT Security にマッピングする方法

1. Azure で、[ユーザーとグループ] ページに移動し、[+ Add user/group](+ ユーザー/グループの追加) をクリックします。

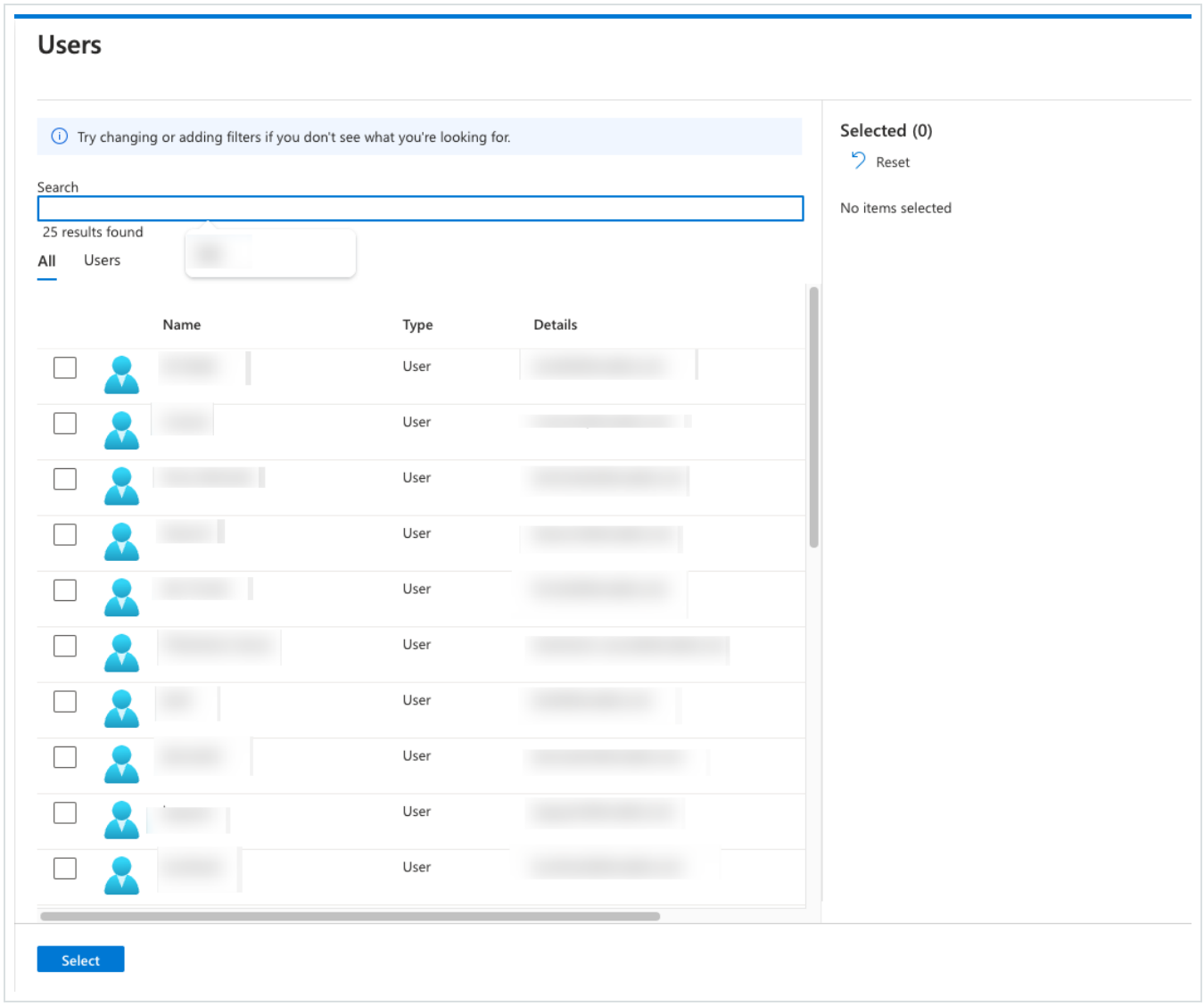
2. [割り当ての追加] ページの [ユーザー] で、[選択なし] をクリックします。

   [ユーザー] ページが表示されます。



注意: Azure でグループ設定を有効にし、[すべてのグループ] ではなく [Groups assigned to the application]([アプリケーションに割り当てられているグループ) を選択した場合は、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。

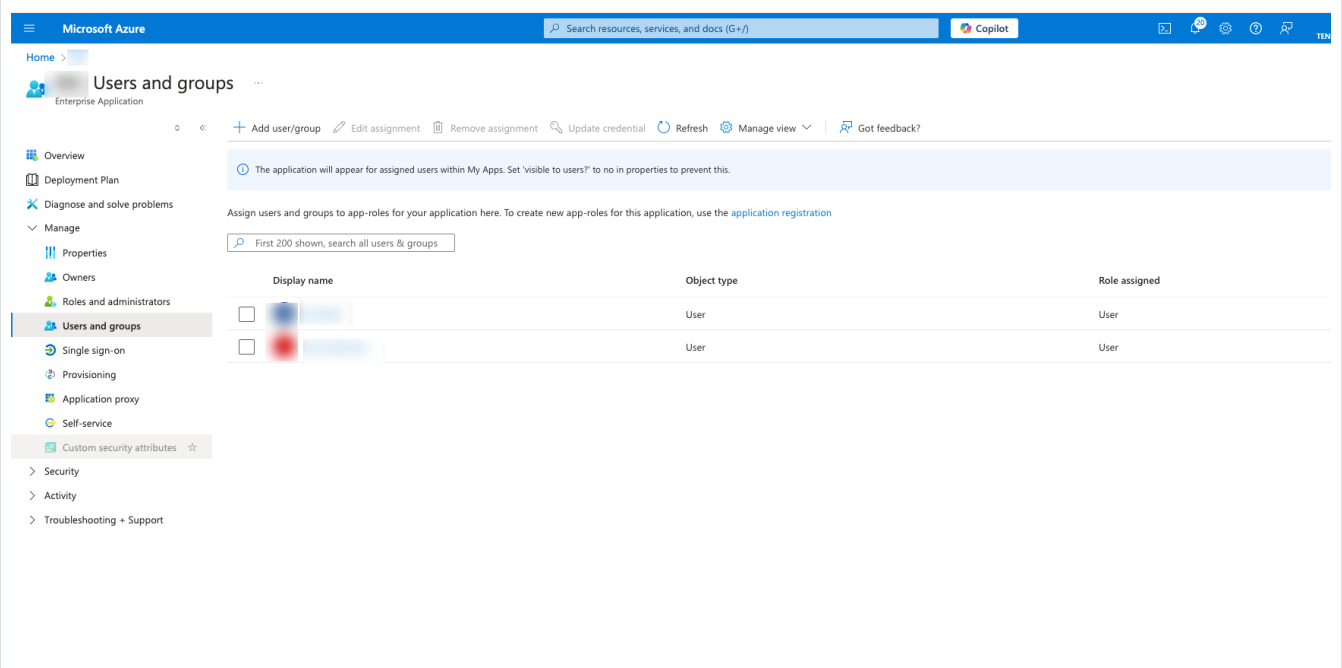
3. 必要なすべてのユーザーを検索して選択し、[選択] をクリックします。



4. [割り当て] をクリックして、それらの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。

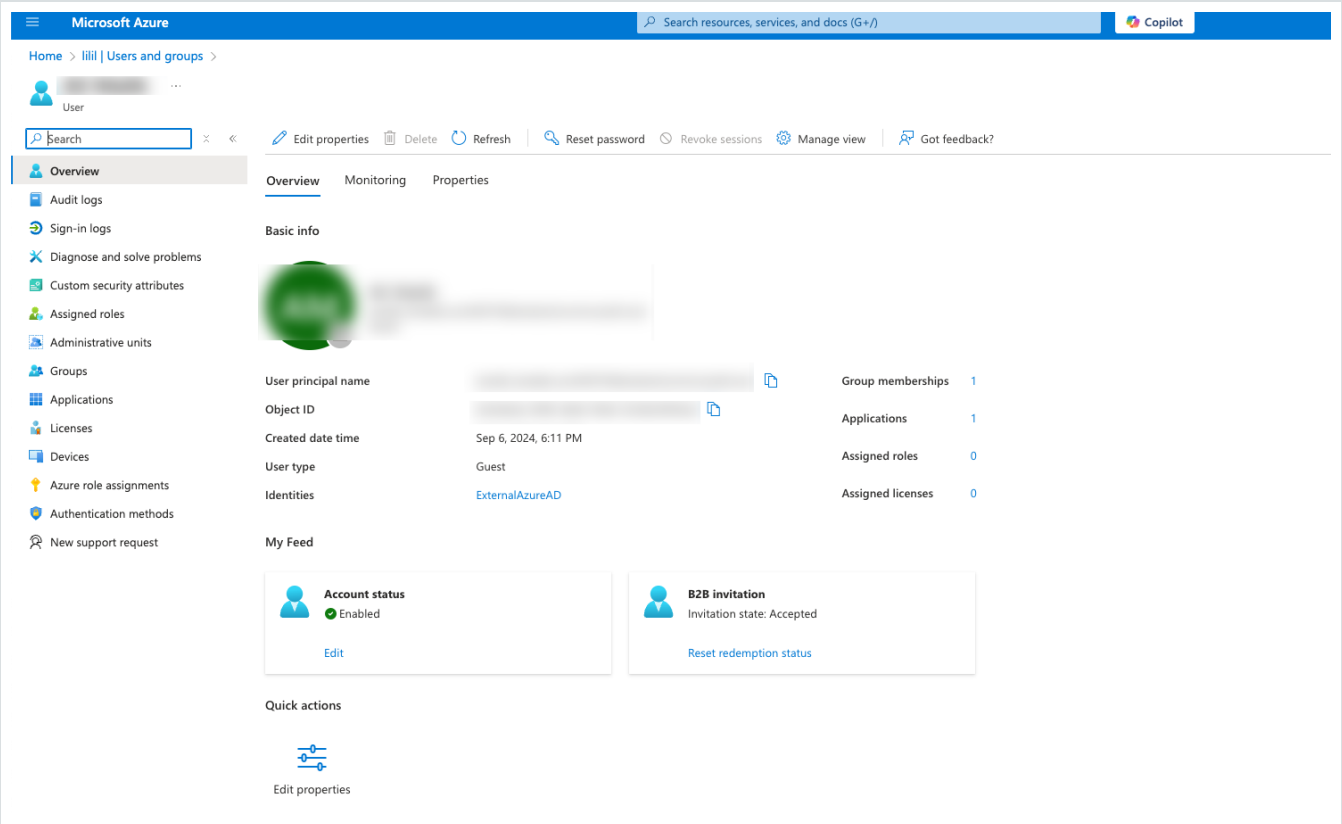
5. ユーザー (またはグループ) の [表示名] をクリックして、そのユーザー (またはグループ) のプロフィールを表示します。



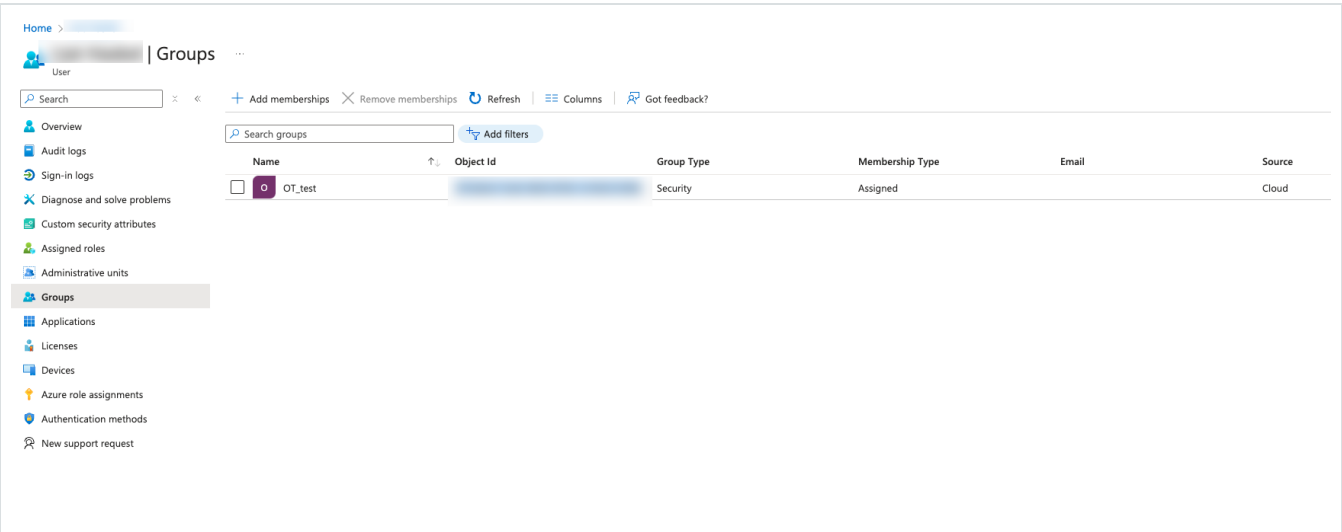
[プロファイル] ページが表 示されます。

6. 左 側 のナビゲーションバーで、[グループ] を選 択します。

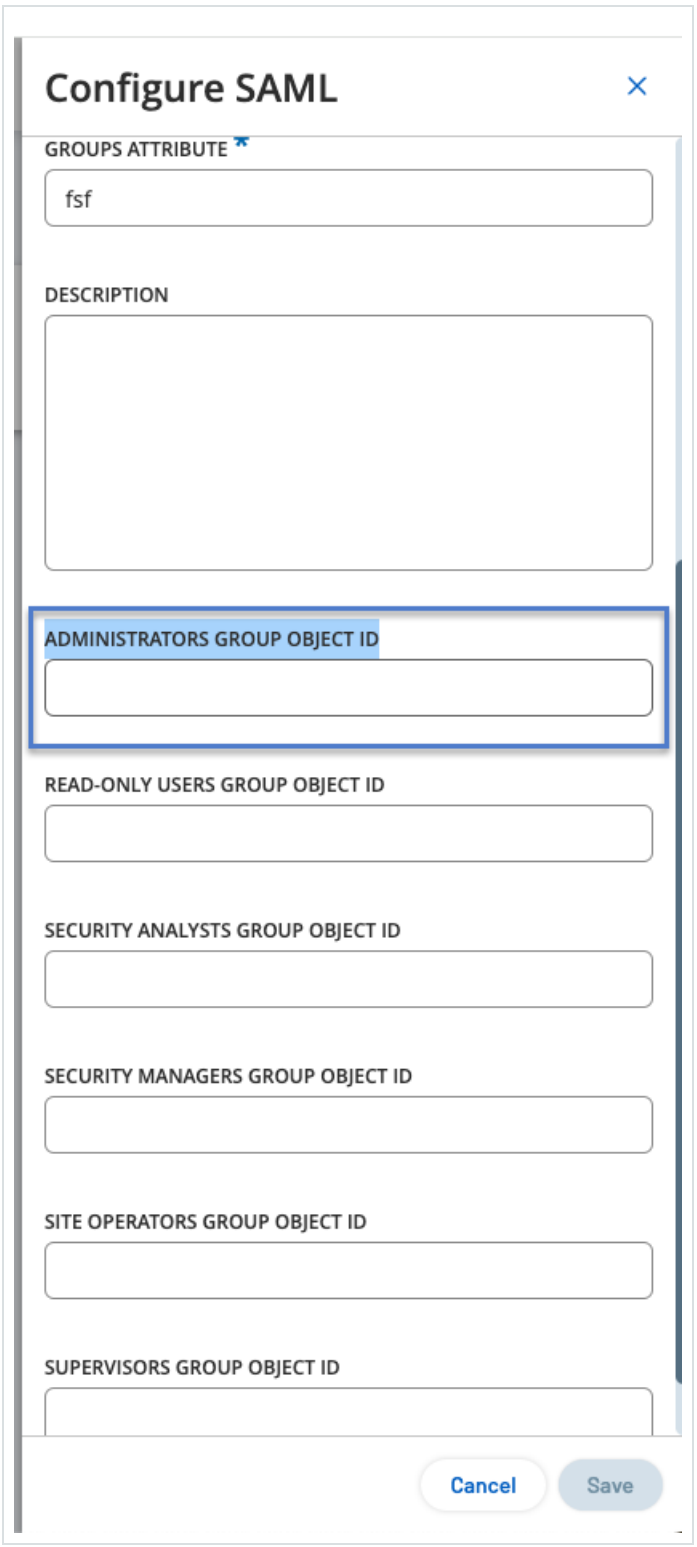
   [グループ] ページが表 示されます。



7. [オブジェクト ID] 列で、Tenable にマッピングするグループの値を選択してコピーします。



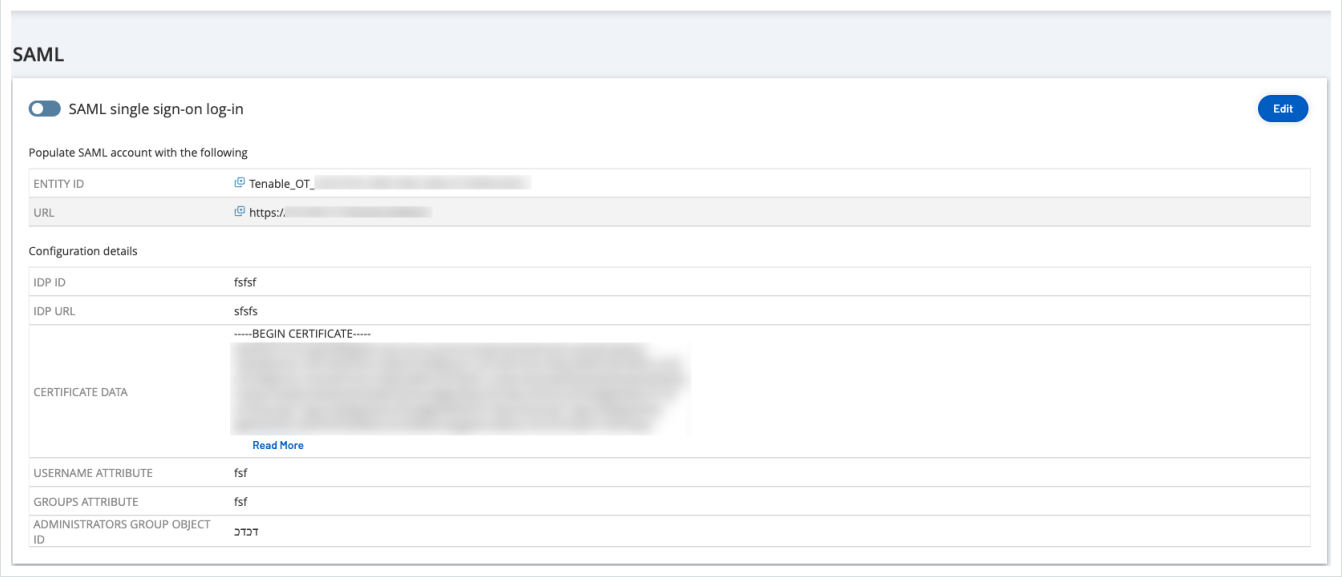
8. OT Security コンソールに戻り、コピーした値を必要な [グループオブジェクト ID] ボックスに貼り付けます。たとえば、[Administrators Group Object ID](管理者グループオブジェクト ID) です。


Configure SAML
GROUPS ATTRIBUTE *
fsf
DESCRIPTION
ADMINISTRATORS GROUP OBJECT ID
READ-ONLY USERS GROUP OBJECT ID
SECURITY ANALYSTS GROUP OBJECT ID
SECURITY MANAGERS GROUP OBJECT ID
SITE OPERATORS GROUP OBJECT ID
SUPERVISORS GROUP OBJECT ID
Cancel
Save

9. OT Security の異なるユーザーグループにマッピングする各グループに対して、ステップ 1～7 を繰り返します。

10. [保存] をクリックして保存し、サイドパネルを閉じます。

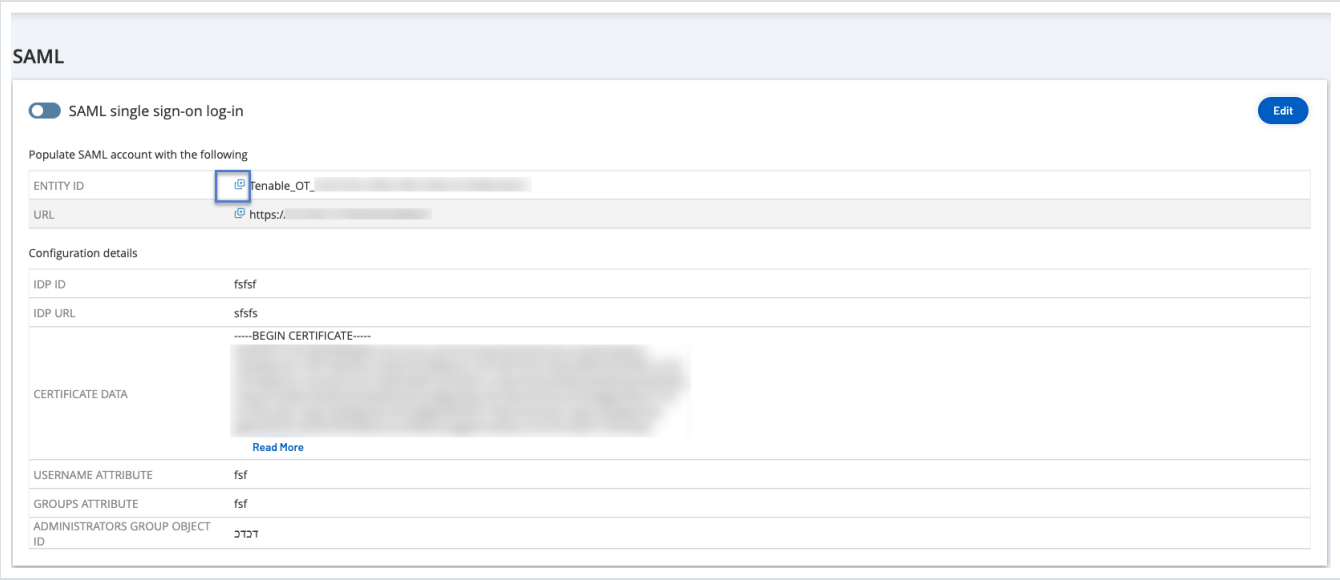
    OT Security コンソールに [SAML] ページが表示され、そこに設定された情報が表示されます。



手順 4 - Azure で設定を完成させる

Azure で設定を完成させる手順

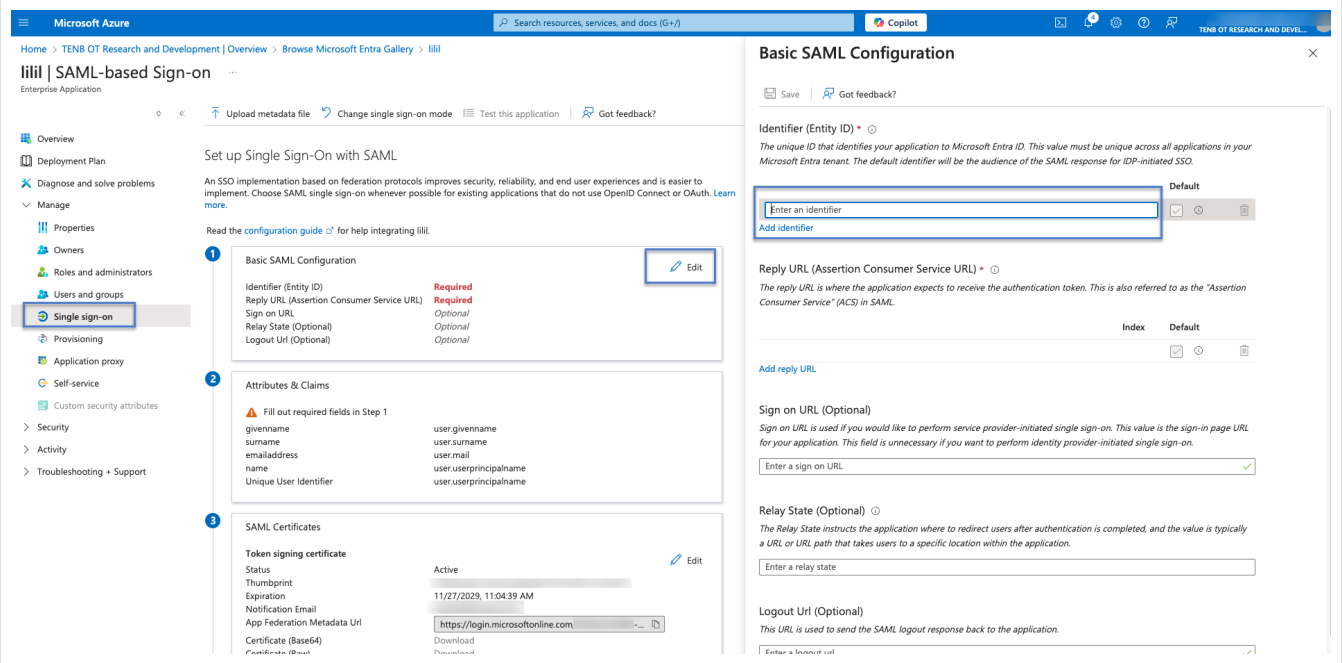
1. OT Security [SAML] ページで、 ボタンをクリックして [エンティティ ID] をコピーします。



2. Azure コンソールで、左側のナビゲーションメニューの [Single sign-on](シングルサインオン) をクリックします。

   [SAML-based Sign-on](SAML ベースのサインオン) ページが表示されます。

3. セクション 1 [基本 SAML 設定] の [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)] ボックスに貼り付けて、以前に入力した一時的な値を置き換えます。



4. OT Security に切り替え、[SAML] ページで、 ボタンをクリックして [URL] をコピーします。

5. Azure コンソールに切り替え、[基本 SAML 設定] セクションの [応答 URL (アサーションコンシューマサービス URL)] に、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 applications](Azure Enterprise アプリケーション) ページに表示されます。

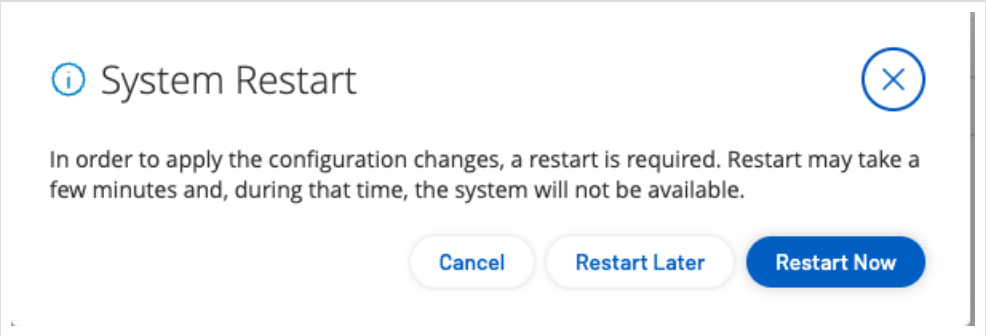
手順 5 - 統合をアクティブ化する

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。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。

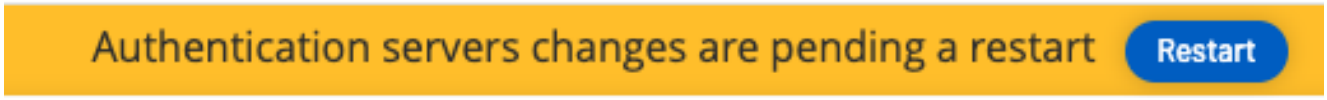
統合をアクティブ化する方法

1. OT Security コンソールの [SAML] ページで、[SAML single sign on login](SAML シングルサインオンログイン) トグルをクリックして SAML を有効にします。

   [System Restart](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、[Restart Later](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。

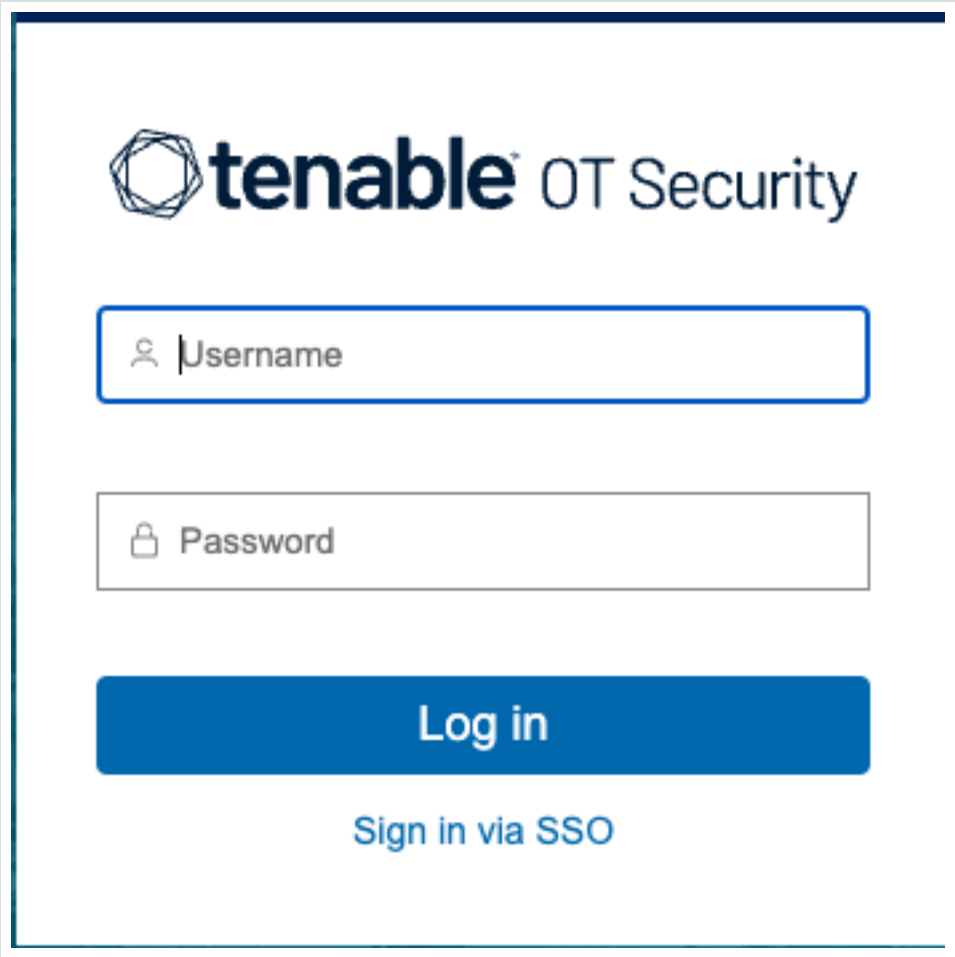


SSO を使用したサインイン

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 でサインイン] 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 ログインウィンドウで、[SSO でサインイン] 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っている場合、OT Security は Microsoft の [Pick an account] (アカウントの選択) ページにリダイレクトし、そこでログインに必要なアカウントを選択できます。