Tenable Web App Scanning ユーザーガイド

最終更新日: 2024 年 4 月 5 日

目次

Tenable Web App Scanning にようこそ 10

Tenable One サイバーエクスポージャー管理プラットフォーム 11

Tenable Vulnerability Management API 12

Tenable Web App Scanning のデプロイメントオプション 13

Tenable Web App Scanning を使い始める 15

Tenable Web App Scanning アプリケーショントポロジー 16

準備 18

インストール 25

スキャンの設定 27

追加の設定 29

Tenable Web App Scanning のライセンス 30

ライセンス制限の超過 33

Tenable Web App Scanning の要件 34

Tenable Web App Scanning へのログイン 35

Tenable Web App Scanning のナビゲーション 36

ブレッドクラムのナビゲーション 43

プレーンのナビゲーション 44

Tenable Web App Scanning の表 45

Tenable Web App Scanning ワークベンチの表 46

表のフィルタリング 49

Docker イメージとして Tenable Web App Scanning をデプロイする 52

Tenable Web App Scanning CI/CD アプリケーションスキャンの概要 55

Atlassian Bamboo 統合による Tenable Web App Scanning CI/CD スキャン 64

CircleCI 統合による Tenable Web App Scanning CI/CD スキャン 65
GitHub 統合による Tenable Web App Scanning CI/CD スキャン 67
GitLab 統合による Tenable Web App Scanning CI/CD スキャン 69
Jenkins 統合による Tenable Web App Scanning CI/CD スキャン 71
Tenable Web App Scanning をログアウトする 73
Tenable Web App Scanning ダッシュボード 74
スキャン済みアプリケーション 80
検出済みアプリケーション 83
アプリケーション資産のエクスポート 86
資産の削除 91
アプリケーションフィルター検索 93
アプリケーションの詳細の表示 98
Tenable Web App Scanning の検出結果 99
検出結果の詳細の表示 101
検出結果のエクスポート 104
Tenable Web App Scanning 検出結果からのレポートの生成 108
修正スキャンの起動 111
修正スキャンプラグインの考慮事項 113
検出結果の変更ルールと許容ルールの作成 118
脆弱性の深刻度インジケーター 121
脆弱性の状態 122
検出結果フィルター 124
検出結果のグループ化 128
Tenable Web App Scanning のスキャンワークフロー 131

スキャンの作成と起動 134
Tenable Web App Scanning のスキャンタイプ 137
スキャンのアクセス許可を設定する 138
スキャン設定を編集する 141
API スキャンの開始 143
Tenable Web App Scanning のスキャンテンプレートの設定 145
Tenable 提供の Tenable Web App Scanning テンプレートタイプ 147
ユーザー定義テンプレート 150
スキャンプラグインの表示 155
Tenable Web App Scanning スキャンの基本設定 160
Tenable Web App Scanning スキャンの詳細設定 165
Tenable Web App Scanning スキャンの範囲設定 172
Tenable Web App Scanning スキャンの評価設定 176
Tenable Web App Scanning スキャンのレポート設定 181
Tenable Web App Scanning スキャンのプラグイン設定 182
Tenable Web App Scanning スキャンの認証情報 185
Tenable Web App Scanning スキャンで認証情報を設定する 187
Selenium 認証情報の設定を自動的に設定する 189
Tenable Web App Scanning の Selenium コマンド 191
Tenable Web App Scanning スキャンでの HTTP サーバー認証設定 195
ウェブアプリケーション認証 196
クライアント証明書認証 201
スキャンの詳細の表示 202
スキャンステータス 206

スキャンの進行状況を表示する 208
深刻度の詳細のスキャンの注記 210
スキャンフィルター 212
スキャン設定のコピー 213
スキャン結果のエクスポート 214
Tenable Web App Scanning スキャンのインポート 217
スキャンフォルダーへのスキャンの移動 218
ゴミ箱フォルダーへのスキャンの移動 220
Tenable Web App Scanning 設定 222
全般設定 223
マイアカウント 232
アカウントの詳細の表示 234
アカウントを更新する 239
パスワードを変更する 242
二要素認証を設定する 244
API キーを生成する 249
自分のアカウントのロックを解除する 252
ライセンス情報 253
Tenable Web App Scanning のライセンス 258
ライセンス制限の超過 261
Tenable Web App Scanning のライセンスの種類 262
アクセス制御 263
ユーザー 264
ユーザーアカウントを作成する 266

ユーザーアカウントの編集 271
ユーザーリストの表示 274
Tenable Web App Scanning のパスワード要件 276
別のユーザーのパスワードの変更 277
各自のアカウントでユーザーをサポートする 278
別のユーザーの API キーの生成 280
ユーザーアカウントのロックの解除 282
ユーザーアカウントの無効化 283
ユーザーアカウントの有効化 285
ユーザーアクセス認証情報の管理 287
ユーザーアクティビティの監査 288
ユーザーをエクスポートする 290
ユーザーアカウントを削除する 294
ユーザーグループ 297
ユーザーグループを作成する 299
ユーザーグループを編集する 301
グループのエクスポート 303
グループを削除する 307
権限 309
アクセス許可設定の作成および追加 313
ユーザーまたはグループへのアクセス許可設定の追加 316
アクセス許可設定の編集 318
アクセス許可設定のエクスポート 320
ユーザーまたはユーザーグループからアクセス許可設定を削除する 324

アクセス許可設定の削除 327
ロール 328
Tenable 提供のロールと権限 331
カスタムロール 340
カスタムロールの作成 344
ロールを複製する 347
カスタムロールの編集 349
カスタムロールを削除する 350
ロールのエクスポート 351
アクセスグループ 355
アクセス許可設定への移行 357
アクセスグループをアクセス許可設定に変換する 359
アクセスグループの種類 361
[すべての資産]グループのユーザーを制限する 362
アクセスグループを作成する 364
アクセスグループのユーザーのアクセス許可を設定する 369
アクセスグループを編集する 373
アクセスグループに割り当てられていない資産を表示する 378
割り当てられたアクセスグループを表示する 379
アクセスグループを削除する 381
アクセスグループルールのフィルター 383
スキャンのアクセス許可の移行 387
アクティビティログ 389
アクティビティログのエクスポート 391

タグ 395
例: 資産のタグ付け 398
タグの形式と適用 402
手動タグまたは自動タグの作成 404
ルール付きのタグに関する考慮事項 407
タグルール 408
タグルールの作成 409
タグルールの編集 415
タグルールの削除 417
タグルールフィルター 419
資産フィルターを使用したタグの作成 428
タグまたはタグカテゴリの編集 430
資産フィルターを使用したタグの編集 432
タグの資産への追加 434
資産ビューを介して資産からタグを削除する 438
タグによる資産属性のオーバーライド 441
タグのエクスポート 442
タグカテゴリの削除 447
タグの削除 449
タグの表からタグで資産を検索する 452
クラウドセンサー 453
認証情報 458
管理された認証情報の作成 459
管理された認証情報を編集する 462

管理された認証情報のユーザーアクセス許可を設定する 464
認証情報のエクスポート 467
管理された認証情報を削除する 471
ファイルとプロセスの許可リスト 473

Tenable Web App Scanning にようこそ

Tenable Web App Scanning は、Tenable Nessus スキャナーが提供する既存の**ウェブアプリケーションテスト**ポリシーのテンプレートを大幅に改善します。今までのテンプレートでは、Javascript に依存した、HTML5 で構築されている最新のウェブアプリケーションに対応できず、お使いのウェブアプリケーションのセキュリティ態勢が充分に理解できない状態でした。

Tenable Web App Scanning は、最新のウェブアプリケーションに対応した、包括的な脆弱性スキャンを提供します。Tenable Web App Scanning の正確な脆弱性カバレッジによって誤検出や検出漏れが最小限に抑えられ、セキュリティチームはウェブアプリケーションの真のセキュリティリスクを把握できます。本製品は、HTML5 や AJAX のフレームワークを使用して構築されたウェブアプリケーションにも対応し、本番環境で中断したり遅延したりすることがないよう、安全で確実な外部スキャンを実行します。

Tenable Web App Scanning アーキテクチャとスキャンに関する詳細については、Tenable Web App Scanning を使い始めるを参照してください。

注意： Tenable Vulnerability Management は、単独で、または Tenable One パッケージの一部として購入できます。詳細については、Tenable One を参照してください。

ヒント： *Tenable Web App Scanning ユーザーガイド*は、英語と日本語で提供されています。Tenable Web App Scanning ユーザーインターフェースは、英語、日本語、フランス語で提供されています。ユーザーインターフェースの言語を切り替えるには、全般設定 を参照してください。

Tenable One サイバーエクスポージャー管理プラットフォーム

Tenable One は、サイバーエクスポージャー管理プラットフォームです。DX 時代のアタックサーフェス全体の可視化、起こり得る攻撃を防ぐための取り組みへのフォーカス、サイバーリスクの正確な伝達を支援することで、最大限のビジネスパフォーマンスを発揮できるようにします。

このプラットフォームは、Tenable Research による高速で広範な脆弱性カバレッジを基盤として構築されており、IT 資産、クラウドリソース、コンテナ、ウェブアプリケーション、ID システムを含む、業界で最大の網羅性を誇る脆弱性カバレッジを提供します。また、包括的な分析機能が作業の優先順位付けを可能にし、サイバーリスクを伝達します。Tenable One を利用する組織は、以下のことが行えます。

- DX 時代のアタックサーフェス全体を包括的に可視化
- 起こり得る脅威に先駆けた攻撃防止対策の優先順位付け
- より適切な判断を可能にするサイバーリスクの伝達

ヒント: Tenable One 製品の使用開始の詳細については、Tenable One デプロイメントガイドを参照してください。

Tenable Vulnerability Management API

API を参照してください

Tenable Vulnerability Management API を利用すると、スキャン、ポリシー作成、ユーザー管理など、Tenable Vulnerability Management プラットフォームのさまざまな機能を使用して、独自のアプリケーションを開発できます。

Tenable Web App Scanning のデプロイメントオプション

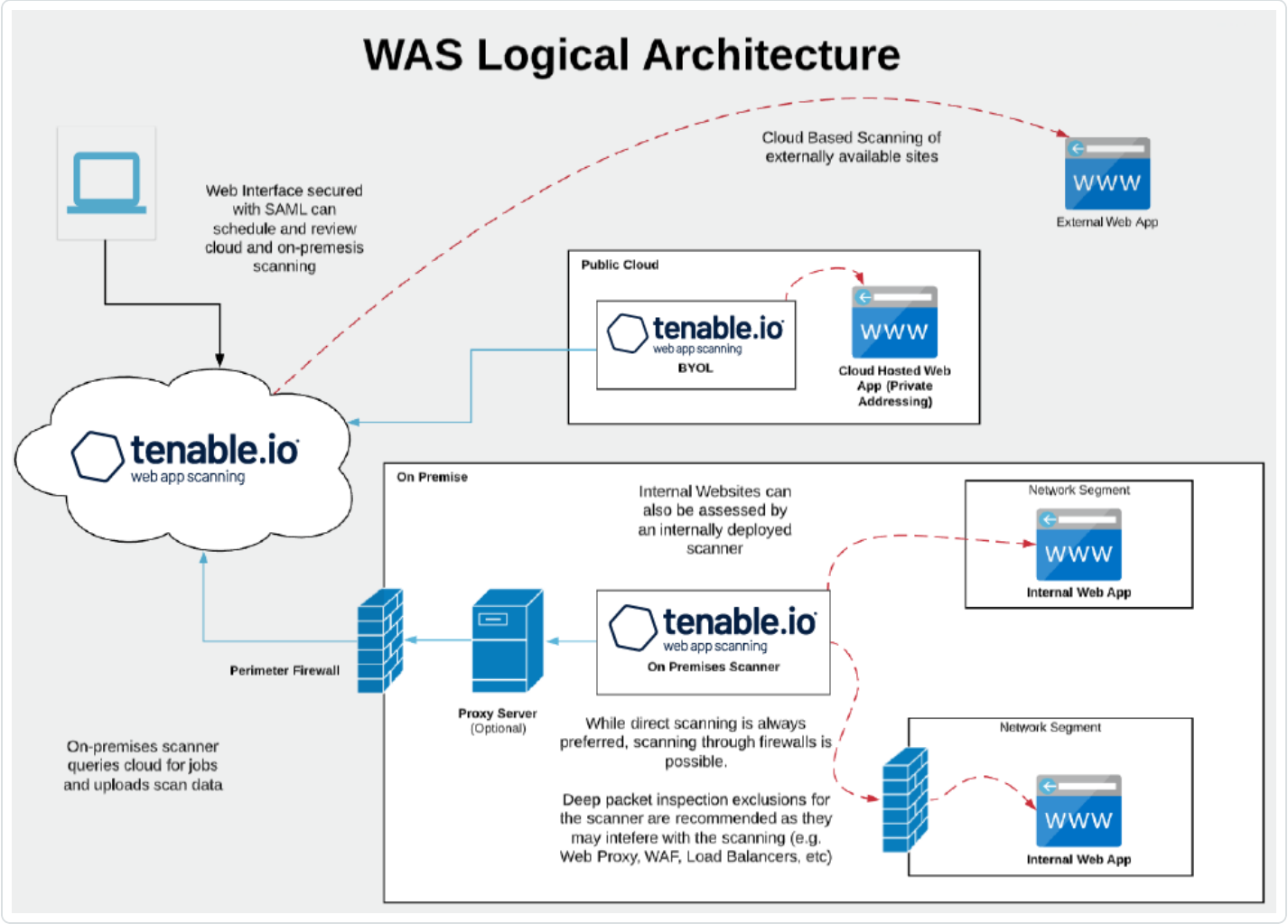
Tenable は、Tenable Web App Scanning のデプロイメントオプションを数多く用意しています。詳細については、以下に挙げる製品ページを参照してください。

- Tenable Core + Web App Scanning - Tenable Core オペレーティングシステムを使用して、お使いの環境の Tenable Web App Scanning のインスタンスを実行できます。Tenable Core + Tenable Web App Scanning をデプロイすると、安全な Tenable Core プラットフォームを通して Tenable Web App Scanning プロセスを監視および管理することができます。
- Tenable Nessus Expert の Tenable Web App Scanning - Tenable Nessus Expert の Tenable Web App Scanningでは、従来の Tenable Nessus スキャナー、Tenable Nessus Agents、Tenable Nessus Network Monitor がスキャンできなかったウェブアプリケーションの脆弱性をスキャンして、対処することができます。
- Tenable Web App Scanning Docker イメージ - Tenable Web App Scanning を Docker イメージとしてデプロイして、コンテナで実行することができます。基本となっているイメージは Tenable Web App Scanning の Oracle Linux 8 インスタンスです。環境変数を使って Tenable Web App Scanning インスタンスをセットアップすることで、Docker イメージを設定で自動的にデプロイできます。Docker イメージがデプロイされると、イメージを更新したりスキャナーログを収集したりすることもできます。
- Tenable Web App Scanning CI/CD アプリケーションスキャン - Tenable Web App Scanning Docker イメージを継続的インテグレーションおよび継続的デリバリ/継続的デプロイメント (CI/CD) ツールとしてデプロイし、マージ前にソフトウェア上で Tenable Web App Scanning スキャンを実行することができます。アプリケーションのライフサイクルの任意の時点で CI/CD のアプリケーションとサービスをスキャンすることで、脆弱性をできるだけ早く発見し、セキュリティスタンスを大幅に改善できます。

Tenable Web App Scanning を使い始める

ウェブアプリケーションの脆弱性のスキャンと、Tenable Nessus、Tenable Nessus Agents または Tenable Nessus Network Monitor の従来の脆弱性のスキャンの間には、大きな違いがあります。その結果、Tenable Web App Scanning (Tenable Web App Scanning) では、脆弱性の評価と管理に対して異なるアプローチが必要です。

Tenable Web App Scanning アプリケーショントポロジー



Tenable Web App Scanning は、従来の Tenable Nessus ベースのウェブアプリケーションスキャンポリシーよりも大幅に改善されています。

- Tenable Nessus のレガシースキャンテンプレートは、Javascript、HTML 5、AJAX、シングルページアプリケーション (SPA) などの最新のウェブアプリケーションフレームワークと互換性がないので、ウェブアプリケーションのセキュリティ状況を完全には理解できない可能性があります。
- Tenable Web App Scanning は、最新のウェブアプリケーションに対応した、包括的な脆弱性スキャンを提供します。その正確な脆弱性カバレッジによって誤検出や検出漏れが最小限に抑えられ、セキュリティチームはウェブアプリケーションの真のセキュリティリスクを把握できます。本番環境のウェブアプリケーションで中断や遅延が発生しないように、安全な外部スキャンを提供します。

- Tenable Web App Scanning は、リージョン固有のクラウドスキャナーを使用します。ウェブアプリケーションの分析範囲に公開されている資産のみが含まれている場合は、それ以上のスキャナーは必要はありません。ウェブアプリケーションが公開されていない場合、インストール計画は、ウェブアプリケーションを実行する場所や自社のデータストレージのニーズによって異なります。

次の開始手順に従って、Tenable Web App Scanning のデプロイメントを設定、管理します。

1. 準備
2. インストール
3. スキャンの設定
4. 追加の設定

準備

開始する前に、Tenable Web App Scanning の基本をよく理解し、実装と設定のデプロイメント計画と分析ワークフローを作成します。

Tenable Web App Scanning プログラムのタイプ

動的アプリケーションセキュリティテスト (DAST) 技術に基づいて、ウェブアプリケーションスキャンプログラムを操作する実行可能な方法がいくつかあります。ほとんどのプログラムは、各アプローチをいくつか組み合わせて使用し、各サイトの異なるニーズに対応しています。次のリストは、Tenable がサポートするスキャンテンプレートを示しています。

- **スキャン:** 利用可能なチェックの完全なセット。これには、API スキャンを除く、事前に構築された他のすべてのテンプレートが含まれます。
- **概要:** 影響を低減しスキャンを高速化するためにいくつかのアクティブなテストを省いた、「スキャン」テンプレートの簡易バージョン。
- **PCI:** Tenable がクレジットカード業界 (PCI) セキュリティ標準用に提供する、認証提供の一部として使用される特別なテンプレート。認証への提出のみに PCI ライセンスを使用します。それ以外の場合、このテンプレートは「スキャン」テンプレートの簡易バージョンです。
- **SSL/TLS:** ウェブサーバーの暗号化設定の現在の状態と証明書の状態 (証明書の残り時間など) に焦点を当てた正常性チェックスキャン。
- **設定監査:** セキュリティプログラムの状態を評価するために外部監査プロバイダーが通常レビューする、外部から閲覧可能なウェブサーバー設定を検出するコンプライアンス監査。
- **API スキャン:** スキャナーが関連する脆弱性を正常に検出できるように、アプリケーションプログラミングインターフェース (API) を説明するための追加の設定を必要とする特別なテンプレート。これには、「スキャン」テンプレートにあるいくつかの類似したテストが含まれますが、その他の API エンドポイントに固有のテストも追加されます。

表面レベルのクイックチェック

「SSL_TLS」または「設定監査」スキャンテンプレートは、通常、詳細なスキャンではなく、数分程度で完了する迅速なテストを定期的に実行する際に使用します。これにより、ベストプラクティスではない特定のサイトまたは一般に公開されている設定パラメーターの証明書タイプおよび暗号化タイプの問題など、表面レベルの概要を確認できます。

- **未調整の詳細スキャン:** このアプローチは、調整や微調整を必要とせずに、「スキャン」テンプレートを使用してほとんどの脆弱性の検出を最適化し、サイトが一般的に経験するドライブバイスタイルの攻撃をシミュレートします。これらのスキャンは迅速にデプロイされ、基本的な検証を使用して明らかなスキャンエラーを回避しながら、スキャンターゲットから貴重な増分可視性を返します。ただし、このアプローチではタイムアウト (Tenable Vulnerability Management のデフォルトの 8 時間など) が発生したり、正しいスキャンのために認証や微調整を必要とするサイトのより複雑なセクションを見逃したりする可能性があります。これらの欠陥は、フォーラム、ブログ、大量の製品、複数の言語、または多数のページがあるサイトに共通して発生します。

- **認証済みの詳細スキャン:** 未調整の詳細スキャンと同様ですが、このアプローチは認証を使用します。これは、スキャン設定ページまたは Tenable の Chrome 拡張で行うことができます。未調整スキャンの利点に加えて、認証スキャンはユーザーとしてログオンし、潜在的な問題をテストします。Tenable は、特に本番環境では、管理ユーザーとしてログオンしないことを推奨しています (「重要な考慮事項」セクションを参照)。認証では、テストユーザーアカウントを作成して管理し、一意のサイト設定を更新する必要があります。

- **調整済みの詳細スキャン:** 認証に加えて、速度を求めたり複雑さに対応したりするためにスキャンを最適化する他の方法を使用できます (「重要な考慮事項」を参照)。これらの改良には、デプロイ前の初期段階に費やした時間が含まれており、サイトの更新頻度によっては準定期的な調整が必要になる場合があります。

本番環境前のスキャン

本番環境サイトへのスキャナーの影響を制限し 100% の稼働時間を維持するには、Tenable Vulnerability Management API を使用してスキャンを統合し、週次または月次のビルドに基づいてスキャンをトリガーするか、定期的なスケジュールで本番環境前でスキャンを検討できます。これにより、内部ビルドとは異なる可能性がある、より露出された本番環境のサイトを保護できます。このスキャンのアプローチは、ほとんどの成熟した企業でそれぞれ異なるレベルで機能しますが、多くの場合、オンサイトの重要度とリソースの可用性に依存します。

API スキャン

企業は、ウェブアプリケーション、B2B トランザクション、モバイルアプリケーション、自動化シナリオを強化するために、API をますます採用しています。Tenable Web App Scanning 内の API スキャンテンプレートを使用してこれらの潜在的な危険性を評価することで、より多くの重大なサイバーリスクを可視化できます。一般に、リスクが高く露出が多い場合、成熟したプログラムや企業は API をより頻繁にスキャンすることになります。最終的に、セキュリティプログラムが開発されると、多くの企業がすべての脆弱な場所を事

前に特定し、それらを完全にカバーできるようになります。このタイプのスキャンでは、スキャナーが API 自体と通信するためのエンドポイント定義を提供するために、開発スタッフからのより多くの入力を必要とし、OpenAPI ファイルに依存する可能性があります。

使用する Tenable Web App Scanning プログラムを決定する

ほとんどのプログラムは、「SSL_TLS」または「設定監査」テンプレートに基づいたいくつかのスキャンから始まります。それにより、脆弱性マネージャーはスキャンを確立し結果をレビューする方法を学ぶことができます。その後、Tenable Web App Scanning スキャンテンプレートを使用して未調整のスキャンを実行します。

タイムアウトは、プログラムを最初に構築するときに一般的に発生するものです。Tenable Vulnerability Management のデフォルトのスキャン完了タイムアウトは 8 時間で、これを延長してもスキャンが「完了」しない可能性があります。スキャンの完了は、速度を上げるための調整でのみ実現可能です。

未調整のスキャンに基づいてプログラムを実行し、タイムアウトを受け入れることも可能です。多くのウェブアプリケーションの脆弱性は、同じ脆弱性が複数のページにまたがって存在しているため、数時間かかる最初のスキャンでかなりの割合の脆弱性を自動的に検出できることがあります。Tenable の独自の監視でこれを確認できます。通常、スキャンを調整してもスキャンの効率性と精度はほんのわずかしか改善せず、スキャン設定の調整にはより多くの時間を要します。

ほとんどの成熟した企業は、最も重要なサイトでスキャンを調整しています。これには、サイトごとの 10～20 分の作業が含まれますが、オペレーターに経験があると短縮できます。企業の知識レベルと利用できるリソースにより、詳細な調整を行えるサイトのパーセンテージが決定されます。特に多くのウェブサイトを持つ企業では、すべてのサイトが調整されていることは稀です。ウェブサイトの動的な性質が、この理由の一部になっています。ウェブサイトは数年ごとに大幅に拡張または変更されることが多く、テストサイトの開発ペースに合わせてスキャン設定を見直す必要があります。

- **最初にプロセスに焦点を当てる:** まず、Tenable Web App Scanning「スキャン」(完全な検査のセット)または「概要」スキャン(検査は少ないが影響も少ない)テンプレートで開始します。スキャナーの出力をよく理解し、チームと協力して検出結果をワークフローに組み込み、緩和および解決プログラムを開発します。
- **重要な領域について詳しく調べる:** 基本となる手順をいくつか確立し、スキャナーからの出力を企業内の適切な人物に決定したら、より高度に調整されたスキャンに時間をかけ、最も重要なサイトの可視性を向上させます。

- **アクションを実行する:** スキャンは、企業のアクションを促すために大量のデータを返します。データの潜在的な消費者を考慮してください。開発者は、必要な修正を特定し、時間とともに改善するための詳細な情報を求めています。経営者は、どのサイトがビジネスに最大のリスクを与えるかを把握し、それに従ってリソースを割り当てる必要があります。セキュリティリーダーが特定の脆弱性分類に焦点を当てるには、すべてのサイトの OWASP 脆弱性カテゴリなどの一般的なカテゴリ情報が必要です。

注意: Tenable Professional Services は、Tenable Web App Scanning スキャンの新規ユーザーに強く推奨されるクイックスタートプログラムを提供し、新しいプログラムを開発するメカニズムの確立を支援します。また、ProServe チームは、より広範な脆弱性管理プログラムを開発する内部プロセスと初期目標を確立するためのワークショップを実施します。これらのサービスは、企業が効果的なサイバーセキュリティプログラムの確かな基礎と理解を得て、製品に慣れるのに役立ちます。詳しくは、Tenable の営業担当者 (sales@tenable.com) にお尋ねください。

スキャン結果を最適化するための重要な考慮事項

1. **ウェブアプリケーションの場所を特定します。**

    - **公開ウェブサイト**

      インターネットベースの Tenable Web App Scanning またはオンプレミススキャナーを使用して、Tenable Vulnerability Management から外部ウェブサイトをスキャンできます。

    - **プライベートウェブサイト**
      オンプレミス Tenable Web App Scanning スキャナーを使用して、Tenable Vulnerability Management から内部またはイントラネットのウェブアプリケーションをスキャンできます。

2. **スキャナーにターゲットへのネットワークルートがあることを確認します。**

    スキャナーがウェブアプリケーションに到達できない場合や、入力の提供や結果の取得ができない場合、スキャンは失敗します。遅延などのネットワークの制約は、スキャンやネットワークコントロールに影響を与える可能性があります (たとえば、ホストベースのファイヤーウォール、ネットワークファイヤーウォール、ネットワーク分離など)。内部ウェブアプリケーションスキャナーを「許可」リストに常に含めます。

3. **スキャナーの場所が遅延またはサーバーの応答時間に影響を与える可能性があります。**

    スキャン中にタイムアウトが多すぎると、セッションが終了します。ターゲットにできる限り近いスキャナーを選択してください。サイトマッププラグインの添付ファイルを確認し、ページ読み込み時間が長くなっていたりタイムアウトしたりしていないかチェックします。これは、低速のサーバーでの同時テストが多すぎるか、ウェブアプリケーションに十分接近していないスキャナー (US スキャナーからのオースト

ラリアのスキャンなど)、または読み込み時間が長くなるサイト設定で発生する可能性があります。スキャナーの場所を変更することで、スキャナーの速度を低下させる詳細設定の再調整をせずに済むようになります。一見矛盾するように見えますが、スキャン速度の設定を遅くすることで、クエリのレートが低下し返されるクエリの変動が少なくなり、応答が遅いサイトで結果が高速化することがあります。

4. **スキャナーは1人のユーザーとして動作します。**

   スキャナーは、リンクをたどり、ボタンを押し、アクセスできるものに基づいてユーザーのアクションをシミュレートできます。サイト検出フェーズの結果として、サイト上で望ましくないやり取りが発生する可能性があります。たとえば、ユーザーがメールを送信できる場合、スキャナーがフォームに入力し、[メール送信]ボタンを2回以上押す可能性があります。スキャナーに特定のボタンアクションの文脈はないものの、ページ全体またはページ要素のいずれかを教えたり除外したりしない限り、意図せずボタンが押されることはありません(詳細については、スコープ設定に関するドキュメントを参照してください)。このようなアクションを防ぐためにページ要素を除外するとスキャンの精度が低下します。そのため、本番稼働前にこのようなサイトを定期的にスキャンする計画を立てるようにしてください。

5. **スキャナーは複数のユーザーとして動作します。**

   デフォルト設定では、スキャナーは同時にウェブサイトをナビゲートする複数のユーザーとして動作します。処理能力の高いサーバーでは、通常このアクティビティによる影響は最小限に抑えられます。ただし、サーバーの状態が不明な場合は、(少なくとも最初のテストでは)スキャンの速度をデチューンして、同時セッションによるサイトへの潜在的な影響に注意することができます。このようなテストの設定の詳細については、詳細設定を参照してください。

6. **各サイトのチューニングをカスタマイズします。これは手間がかかる作業ですが、オプションです。**

   ウェブアプリケーションはそれぞれ異なるため、通常、ほとんどのウェブサイトで調整はカスタマイズされて適用されます。それぞれのウェブサイトでは、独自の構造、サイトマップ、サードパーティのライブラリ、コンポーネント、カスタムコードが連動しています。調整済みスキャンへどれだけ投資するかは、リソースの可用性、サイトの重要度、ビジネスへの影響によって異なります。

7. **認証を調整するとき、本番環境で Tenable Web App Scanning スキャンをウェブサイト管理者として実行しないでください。テスト環境または本番前の環境でのみ実行します。**

   管理者の認証情報でウェブアプリケーションスキャンを実行すると、ユーザーが作成されたり削除されたり、その他の望ましくない管理機能が実行される可能性があります。

8. **速度を調整する場合、サイトの基本部分だけを把握するようにすることで、DAST スキャンを高速化できます。**

    a. サイトマッププラグインおよび関連する添付ファイルを確認します。

    b. 設定を変更します。ページタイムアウトが大量に発生する場合は、「ネットワークタイムアウト」を増やすか、「最大同時リクエスト」および「1 秒あたりのリクエスト」を減らします。または、サイトマップ添付ファイルで 5 秒を超える平均ページ応答時間を見つけます。

    c. 1 秒未満の応答が得られウェブサーバーへの影響が最小限になるよう、スキャン設定の高速化を検討してください。

    d. サイトコンテンツの重複を排除します。スキャナーはサイトテキスト、画像、動画コンテンツをテストせず、入力フィールドとインタラクションのみをテストします複数の言語を使用するものの根底にあるコードが同じサイトなどの冗長ページがある場合は、サイトの 1 つの言語バージョンをテストするだけで済みます。

    e. バイナリ除外をさらに追加します。Tenable Web App Scanning は、テキスト、画像、動画を「テスト」せず、除外するファイル拡張子を決定します。スキャン範囲 セクションでは、特定のサイトに適応できるデフォルトセットを説明します。

    f. 重要な URL に優先順位を付けます。機密データを返す可能性があるフォームなど、アプリケーションの重要な部分を特定します。スキャン範囲 セクションの「包める」または手動のクロールスクリプトを使用して、これらの URL をテストの範囲に追加します。また、これらのサイトで本番前のテストが必要かどうかを検討することもできます。

9. **複雑さを調整する際は、セッション記録を使用してスキャナーをトレーニングします。**

    これを行うには、Tenable Chrome 拡張機能または Selenium IDE を使用し、スキャン設定のスキャン範囲内で追加します。このプロセスでは、手動クロールを実行して、スキャナーがサイト内の非常に複雑な場所をテストできるようにすることができます。たとえば、サイトでは、他の方法では利用できないページに到達するために、特定の一連のボタンを押し、特定の正しい値のセットを入力することが必要な場合があります。スキャナーが再度テストできるように、この手順を記録できます。

10. **スキャナーとターゲットの間にウェブアプリケーションファイヤーウォール (WAF)、ウェブプロキシ、またはロードバランサーがあるかどうかを確認します。**

    一部のネットワークデバイスでは、スキャンが妨害されたり結果が完全に無効になったりする可能性があります。ファイヤーウォールでフィルター処理された結果の「リモート」ビューのみを受信すれば十分だと考えるかもしれません。しかし、WAF のビルトイン保護は、欠陥を実行する 1 つまたは 2 つの

方法しか防止しない可能性があります。リスクベースの決定を行うには、サイトの真の状態の全体像を把握することが必須です。バイパス機能をサポートするようにWAFを設定し、特定のIPまたはIPとエージェントヘッダー文字列の組み合わせで着信スキャンを証明および承認できるようにします。Tenableスキャナー IP範囲のリストは、ここから入手できます。

11. **一部のサイトでは、特定のブラウザIDが必要な場合があります。**

    アプリケーションがデフォルトのユーザーエージェント(デフォルトでは「WAS/%v」として設定)と互換性があるかどうかを確認します。互換性がない場合は、Mozilla/5.0などの標準ブラウザからの特定のヘッダーまたは一般に利用可能なヘッダーが必要な場合があります。一部のサーバー側の保護またはウェブアプリケーションのファイヤーウォールでは、特定の結果セットが必要になる場合があります。この場合、サイトに正常にアクセスできる既知のブラウザからユーザーエージェント文字列をコピーできます。

12. **重要なサイトを最初に注意深くターゲットにします。**

    ターゲットサイトは本番環境に接続していますか、それ以外の点で重要なサイトですか。ウェブアプリケーションスキャナーがサービスの中断を引き起こす場合、ビジネスにどのような影響がありますか。サイトの最初のスキャンは常に、スタッフの手元にある環境または本番前の環境で制御された方法で実行します。サイトの性質を理解したら、完全な自動化を開始できます。

詳細およびガイド付き製品ウォークスルーについては、弊社のTenable製品教育のYouTubeチャネルを参照してください。これらの短い説明ビデオでは、脆弱なウェブアプリケーションを保護するための上記の認証手順および調整手順を含む、Tenable Web App Scanningを最大限に活用する方法を説明しています。

インストール

1. **デプロイメントの準備**

    a. **Tenable Vulnerability Management プラットフォームおよび Tenable Web App Scanning アプリケーションへの必要なアクセス権を確認します。**結果をスキャンおよび表示するための Tenable Web App Scanning への適切なアクセス権を持つユーザーを作成します。ロールベースアクセスコントロール(RBAC)を設定すると、ユーザーアクセスを許可できるようになります。設定には管理者の認証情報が必要です。

    b. **ローカルスキャナーが必要かどうかを判断します。**ローカルまたはクラウドベースのスキャナーをデプロイすると、それらを Tenable Vulnerability Management に接続できます。これらのスキャナーは、インターネットに接続するウェブアプリケーション、開発環境、または本番前の環境で使用できます(適切なファイヤーウォールルールが適用される場合)。

    Tenable Core + Tenable Web App Scanning スキャナーは、VMware (.ova)、Hyper-V (.zip)、または物理マシン(.ISO)へのインストールをサポートしています。これをローカルのオンプレミスまたはクラウドベースの開発環境にデプロイして、インターネットに直接接続されていないウェブアプリケーションをスキャンできます。

    ローカルスキャナーはここからダウンロードできます。次のアクセスが揃っていることを確認してください。

    - Tenable Vulnerability Management と通信するためのポート 443 経由の https://cloud.tenable.com への送信アクセス
    - 管理インターフェースへのブラウザアクセス用のポート 8000 での HTTPS 経由の着信アクセス

2. **特定と計画**

    a. **セキュリティ目標を定義します。**なぜスキャンしているのか、何を達成したいのか、何をもって成功とするかを定義します。

    b. **スキャンの優先度を決定します。**クイックスキャンの範囲内にあるより詳細なスキャンが必要なターゲットウェブアプリケーションを特定します。

c. **完全なカバレッジを確保します。**スキャンする必要がある他の(特定されていない可能性がある)ウェブサーバー、サービス、アプリケーションがあるかどうかと、それらを見つける方法を決定します。

3. ドキュメンテーション

a. **すべてのデータを記録します。**デプロイメント要件の完全な詳細、デプロイされたスキャナーリソース(該当する場合)、スキャン用に特定されたウェブアプリケーション、スキャンに適用した調整と関連する根拠をキャプチャするドキュメントを作成および管理します。

b. **検出結果を伝達します**。受信者、詳細レベル、レポート配布の頻度を特定するためのレポート要件を確立します。チケットシステムが脆弱性の詳細を必要とする一方で、開発者はPDFを必要とする場合があります。経営者は、全体的なエクスポージャーとリスク低減のより高いレベルのサマリーを好むことがよくあります。

スキャンの設定

分析ワークフローを準備し、ウェブアプリケーション資産の範囲を決定した後で、それらの資産のスキャンを設定して実行することができます。

Tenable では、より詳細なスキャン用の設定を判断できるように、最初に大まかな概要スキャンを実行することを推奨しています。

1. 次のいずれかを行います。

    - 概要スキャンを設定して実行する方法

        1. 次のいずれかを行います。

            - 概要スキャンを実行して、どのウェブアプリケーションを Tenable Web App Scanning がデフォルトでスキャンすべきか判断するには、**[概要]** スキャンテンプレートを使用してスキャンを作成します。
            - 概要スキャンを実行してウェブアプリケーションが一般的なセキュリティの業界標準と互換性があるかどうかを判断するには、**[設定監査]** スキャンテンプレートを使用してスキャンを作成します。

            > **注意:** Tenable が提供する概要スキャンのスキャンテンプレートでは認証は必要ありません。ただし、これらのスキャンから得られたプラグイン結果は、より詳細なスキャンを実行する際にウェブアプリケーションで必要になる認証情報のタイプを特定するのに役立ちます。

        2. スキャン結果とスキャン戦略を確認し、標準のウェブアプリケーションスキャンで使うときに調整が必要な設定を判断します。

    - 標準スキャンを設定して実行する方法

        1. 評価のニーズに最も適したテンプレートを使用してスキャンを作成します。

            - 包括的な脆弱性スキャンを実行するには、**[スキャン]** テンプレートを選択します。
            - スキャンを実行して、ウェブアプリケーションが SSL/TLS 公開鍵暗号化を適切に実装しているかどうかを判断するには、**[SSL TLS]** テンプレートを選択します。

2. (オプション) ユーザーアクセス許可とプラグインの設定を含むスキャン設定をします。

   注意: 標準スキャンに認証情報オプションを設定することもできます。ただし、認証情報が必要になるのは、ウェブアプリケーションの認証で必要とされる場合のみです。

3. スキャンのステータスを監視します。

2. スキャンを起動します。
3. スキャン結果を表示して分析します。
   - 検出結果を分析します。
   - 詳細なスキャン、調整と最適化、ページタイムアウトの確認、ページにアクセスする時間の長さ、エラー、または反復的なコンテンツを削除する機会への入力として、クロールされたサイトマップを使用します。
   - より高い優先度の問題がないか「スキャンノート」を確認します。これにより、スキャン改善の提案が提供される可能性があります。
4. ビジネスニーズに基づいてスキャンをさらに調整します。
   a. **詳細設定を試します。** 前の手順で収集したデータに基づいて、いくつかの場所でスキャン調整を実行します。これで、対象のウェブアプリケーション用にスキャンを更新してデプロイできます。詳細は、を参照してください。
      - 範囲設定
      - 評価設定
      - 詳細設定

注意: Tenable Web App Scanning 試用版ライセンスでは、クラウドスキャナーを使用して最大 5 つのスキャンを同時に実行することができます。オンプレミススキャナーを使用すると、任意の数のスキャンを同時に実行することができます。

追加の設定

必要に応じて他の機能を設定し、既存の設定を調整します。

1. スキャンに認証情報を追加します。

    - サーバーの HTTP プロトコルに必要な方法を使用してスキャンでウェブアプリケーションに認証する必要がある場合は、HTTP サーバーベースの認証を追加します。
    - ウェブアプリケーションに必要な方法を使用してスキャンでウェブアプリケーションに認証する必要がある場合は、ウェブアプリケーションの認証を追加します。

2. Google Chrome 拡張機能 Tenable Web App Scanning をダウンロードして、Selenium 認証情報を自動で設定します。

3. スキャン設定、ユーザーアクセス許可、プラグイン設定などのカスタム調整をさらに検討します。

    ヒント: 各アプリケーションは固有なものです。スキャンを実行し結果を分析すると、スキャンを最も効率的に実行し、アプリケーションのすべての領域をカバーするのに役立つ手法が明らかになります。ウェブアプリケーションのサイズまたは複雑さによっては、スキャンが完了しても、結果を分析してさらに最適化することができます。Tenable では、スキャンが完了した後の「スキャンノート」とサイトマッププラグインへの添付ファイルを定期的に確認することを強く推奨しています。

Tenable Web App Scanning のライセンス

このトピックでは、スタンドアロン製品の Tenable Web App Scanning 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を説明し、購入できるアドオンコンポーネントをリストし、ライセンスの超過または期限切れになるとどうなるかを説明します。Tenable Web App Scanning の使用方法については、Tenable Web App Scanning ユーザーガイドを参照してください。

Tenable Web App Scanning のライセンシング

Tenable Web App Scanning には、クラウドバージョンとオンプレミスバージョンの 2 つのバージョンがあります。クラウドバージョン向けに、Tenable はサブスクリプションモデルを提供しています。オンプレミスバージョン向けに、Tenable はサブスクリプションモデルのほか、永久ライセンスとメンテナンスライセンスを提供しています。

> **注意**: Tenable Web App Scanning オンプレミスバージョンには Tenable Security Center ライセンスが必要です。

Tenable Web App Scanning を使用する際は、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 Web App Scanning は、それらのライセンスを環境内の*資産* (一意の完全修飾ドメイン名 (FQDN)) に割り当てます。

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

> **ヒント**: 現在のライセンス数と利用可能な資産を表示するには、Tenable の上部ナビゲーションバーで  、**[ライセンス情報]** の順にクリックします。詳細については、ライセンス情報ページを参照してください。

資産のカウント方法

Tenable Web App Scanning は、環境内のリソースをスキャンして FQDN を特定することで、ライセンスのある資産数を判断します。過去 90 日間に脆弱性の有無がスキャンされた FQDN は、ライセンスにカウントされます。

FQDN は、RFC-3986 インターネット標準に従って、完全な URL で一覧表示されます。この標準に従って、各 FQDN には次のコンポーネントと形式が含まれています。

```
hostname.parent-domain.top-level-domain
```

スキャンでウェブアプリケーションターゲットを指定した場合、FQDN のいずれかのコンポーネントが別のスキャンされたターゲットまたは以前にスキャンされた資産のコンポーネントと異なる場合、Tenable Web App Scanning はそのターゲットを別の資産としてカウントします。FQDN のすべてのコンポーネントが一致する限り、異なるパスを持つ複数のターゲットは 1 つの資産として FQDN カウントに追加されます。

たとえば、次のターゲットは 1 つの資産としてカウントされます。

```
hostname.parent-domain.top-level-domain/path1
hostname.parent-domain.top-level-domain/path2
hostname.parent-domain.top-level-domain/path2/path3
```

次の表は、すべての FQDN コンポーネントが一致するかどうかに基づいて、スキャンターゲットが同じ資産と見なされる場合と別々の資産と見なされる場合を示しています。

同じ資産	別の資産
• https://example.com • https://example.com/welcome • https://example.com/welcome/get-started • https://example.com/welcome/get-started/create-new-user • http://example.com	• *https://en.example.com (異なるホスト名)* • *https://www.ex-ample.com (異なる親ドメイン名)* • *https://www.example.org (異なる最上位レベルドメイン)*

Tenable Tenable Web App Scanning のコンポーネント

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 Web App Scanning 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
• 外部スキャン機能 • OWASP Top 10 の問題	追加のクラウドスキャンの併用 **ヒント**: 併用は、ライセンスのある資産に基づいており、同時に実

• HTML5 のクローリング • Tenable Vulnerability Management との統合（所有している場合） • API の使用	行できる Tenable 管理のクラウドスキャナーの数を決定します。

ライセンスの流用

資産を購入しても、追加の資産を購入しない限り、資産の総数は契約期間中ずっと静的です。ただし Tenable Web App Scanning は削除した資産のライセンスを 24 時間以内に流用します。さらに、90 日間または指定した期間スキャンされなかった資産のライセンスを流用します。

ライセンス制限の超過

環境の急激な拡大、または予期しない脅威による使用率の急増に対応できるよう、Tenable Web App Scanning ライセンスには 10% の柔軟性があります。ただし、ライセンスされている以上の資産をスキャンすると、Tenable はその超過について明確に伝達し、その後 3 段階で機能を削減します。

シナリオ	結果
3 日間連続して、ライセンスされている以上の資産をスキャンした。	Tenable Web App Scanning にメッセージが表示されます。
15 日間以上、ライセンスされている以上の資産をスキャンした。	Tenable Web App Scanning には、機能の制限に関するメッセージと警告が表示されます。
45 日間以上、ライセンスされている以上の資産をスキャンした。	Tenable Web App Scanning にメッセージが表示されます。エクスポート機能が無効になります。

ヒント: 不適切なスキャンや製品の設定ミスにより、スキャンが過剰になり、資産数が増加する可能性があります。詳細については、スキャンのベストプラクティスを参照してください。

期限切れのライセンス

購入した Tenable Web App Scanning 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 プラットフォームにサインインできなくなります。

Tenable Web App Scanning の要件

ハードウェア要件

シナリオ	推奨ハードウェア
Tenable Web App Scanning で最大 4 個のウェブアプリケーションを同時に実行	**CPU**: 2 GHz コア x 4 **コア RAM:** 16 GB RAM **ハードドライブ:** 100 GB

アプリケーション要件

Tenable Web App Scanning は特定のプラグインの実行に Google Chrome ブラウザを使用するため、スキャン対象となるすべてのアプリケーションに Google Chrome との互換性が必要です。

Tenable Web App Scanning へのログイン

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

始める前に

- 自分のユーザーアカウントの認証情報を取得します。

  注意: 管理者として Tenable Web App Scanning インスタンスに初めてログインする場合には、Tenable がセットアップ中に初回認証情報を提供します。新しいパスワードは初回ログイン後に設定できます。初回セットアップの後に Tenable Vulnerability Management にログインする場合には、Tenable Web App Scanning アカウントの登録に使用したメールアドレスがユーザー名になります。

- *一般要件ユーザーガイド*のシステム要件をレビューして、ご利用のコンピューターとブラウザが要件を満たしていることを確認します。

Tenable Web App Scanning にログインする方法

1. サポートされているブラウザで、https://cloud.tenable.com に移動します。

   ログインページが表示されます。

2. [ユーザー名] ボックスで、Tenable Web App Scanning のユーザー名を入力します。

3. [パスワード] ボックスで、登録時に作成した Tenable Web App Scanning のパスワードを入力します。

4. (オプション) 後のセッションのためにユーザー名を保存するには、**[ログイン情報を記憶しますか?]** チェックボックスを選択します。

5. **[サインイン]** をクリックします。

   ランディングページが表示されます。

   注意: 一定の時間 (通常 30 分) 使用しない場合、Tenable Web App Scanning からログアウトします。

Tenable Web App Scanning のナビゲーション

Tenable Web App Scanning には、重要な情報を強調し、ユーザーインターフェースをより効率的に操作するのに役立つ、便利なショートカットやツールが含まれています。

クイックアクションメニュー

クイックアクションメニューは、最もよく利用されるアクションをリスト表示します。

クイックアクションメニューにアクセスする方法

1. 右上にある ☆ **クイックアクション** ボタンをクリックします。

   クイックアクションメニューが表示されます。

2. リンクをクリックして、一覧にあるいずれかのアクションを開始します。

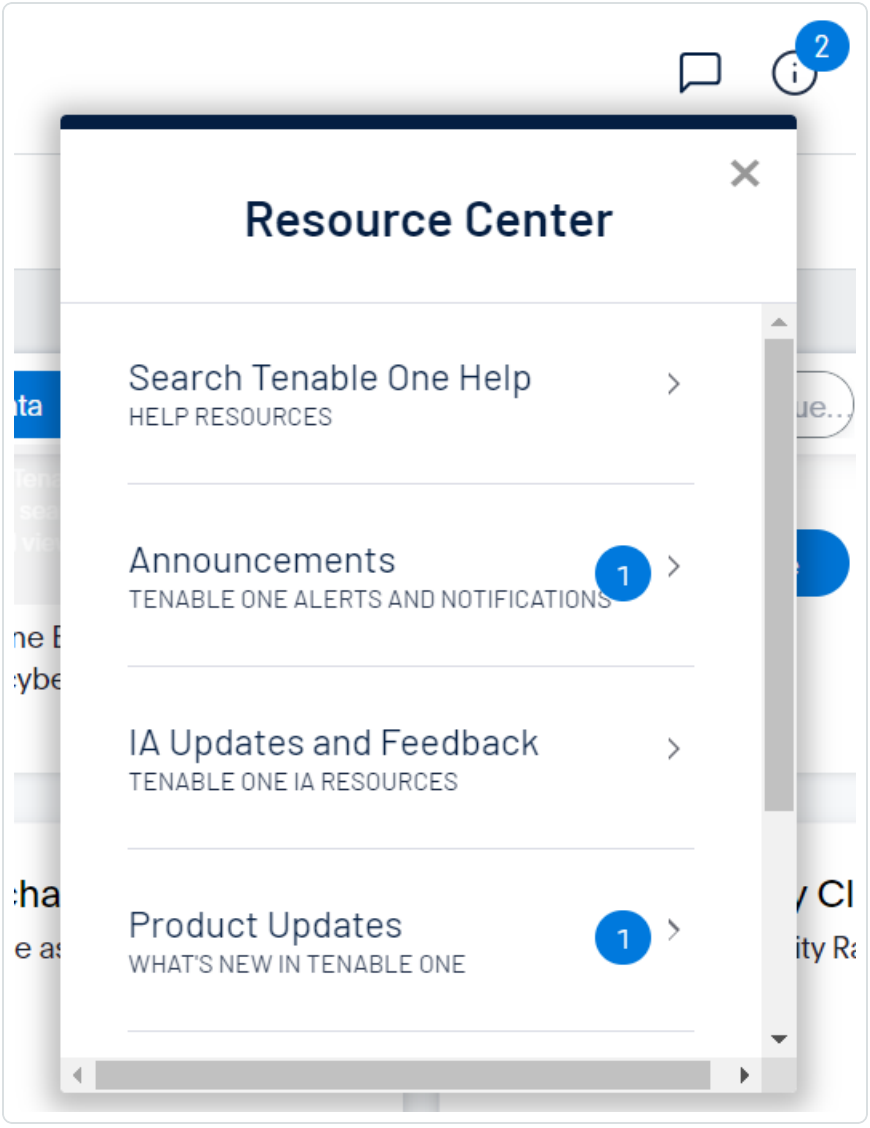
リソースセンター

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

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。

通知

Tenable Web App Scanning の **[通知]** パネルにはシステム通知のリストが表示されます。🔔 ボタンは、現時点で確認されていない通知の数を示しています。**[通知]** パネルを開くと、これらの通知は Tenable Web App Scanning によって確認済みとしてマーキングされます。通知を確認したら、消去して **[通知]** パネルから削除できます。

> **注意:** Tenable Web App Scanning は類似の通知をグループ化してまとめます。

通知を表示するには:

- 右上の 🔔 ボタンをクリックします。

  [通知] パネルが表示され、システムの通知のリストが表示されます。

  [通知] パネルでは、以下の操作を実行できます。

  - 1つの通知を消去するには、通知の隣の ✕ ボタンをクリックします。
  - 通知のグループを展開するには、グループ化された通知の下部にある **[追加の通知]** をクリックします。
  - 展開された通知のグループを折りたたむには、展開された通知の上部にある **[表示数を減らす]** をクリックします。
  - 展開された通知のグループを消去するには、展開された通知の上部にある **[グループのクリア]** をクリックします。
  - すべての通知を消去するには、パネルの下部にある **[すべてクリア]** をクリックします。

設定アイコン

ワークスペース

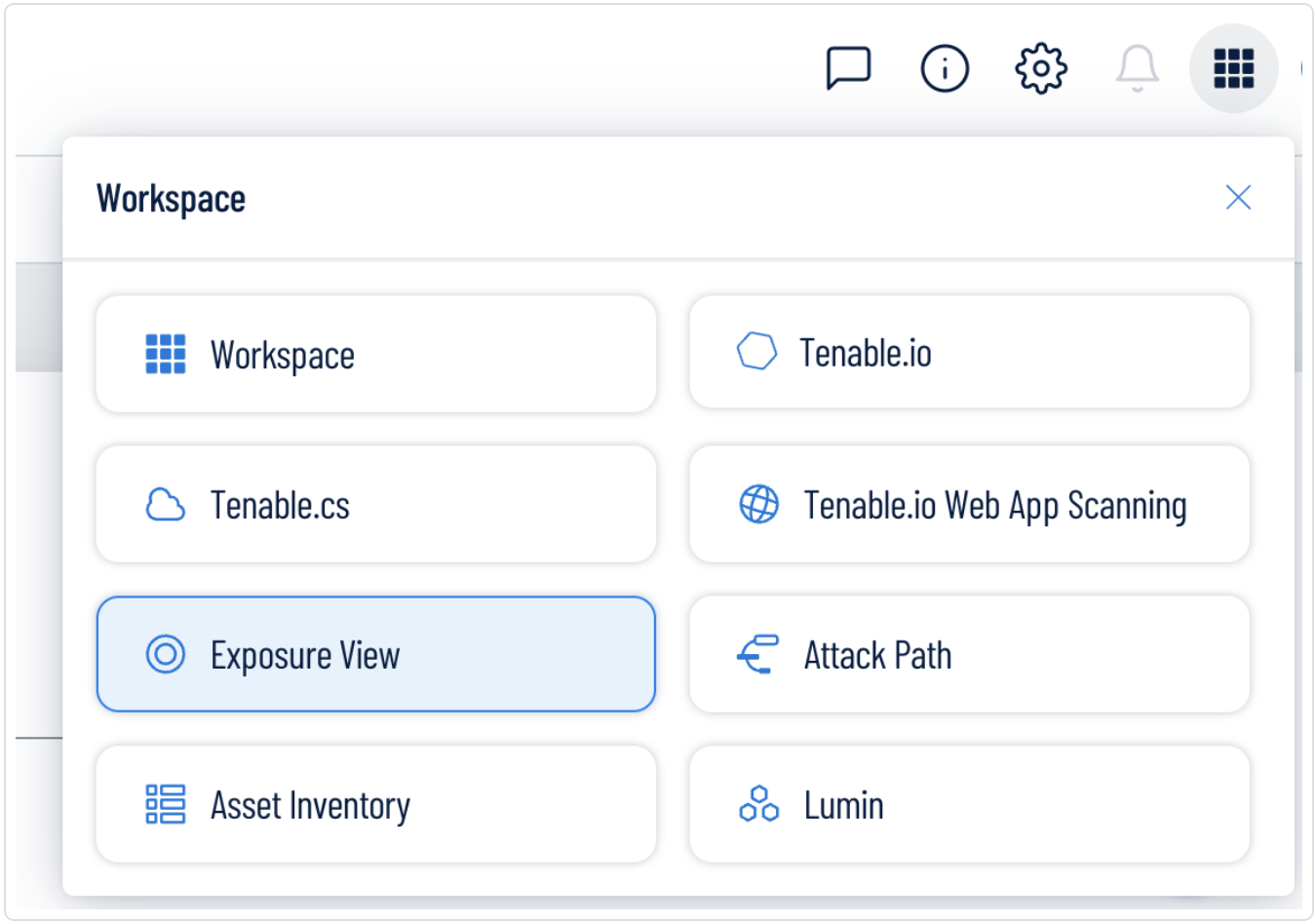
Tenable にログインすると、デフォルトで **[ワークスペース]** ページが表示されます。**[ワークスペース]** ページで、Tenable アプリケーションを切り替えたり、デフォルトのアプリケーションを設定して今後 **[ワークスペース]** ページをスキップするようにしたりできます。上部のナビゲーションバーに表示される **[ワークスペース]** メニューから、アプリケーションを切り替えることもできます。

ワークスペースメニューを開く

[ワークスペース] メニューを開く方法

1. いずれかの Tenable アプリケーションの右上隅にある ボタンをクリックします。

   [ワークスペース] メニューが表示されます。



2. アプリケーションタイルをクリックして開きます。

ワークスペースページを表示する

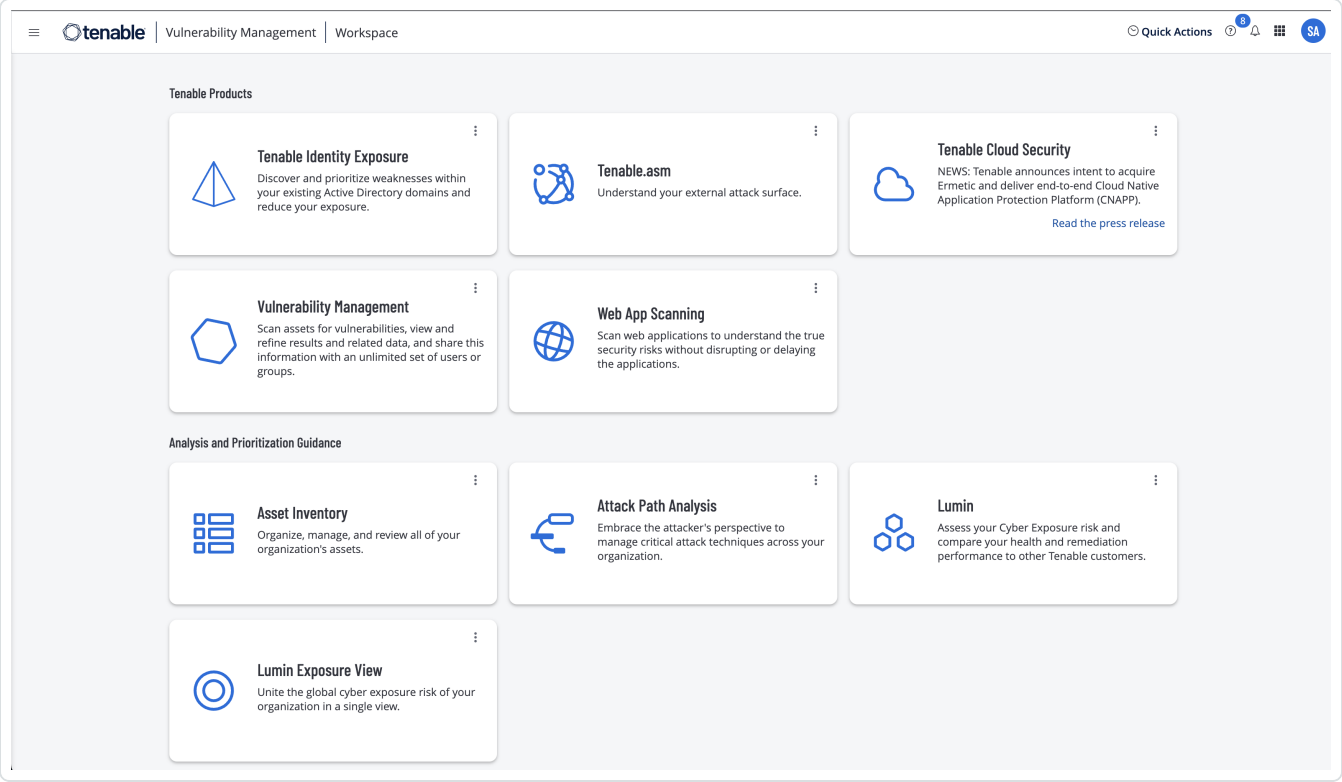
[ワークスペース] ページを表示する方法

1. いずれかの Tenable アプリケーションの右上隅にある ボタンをクリックします。

   [ワークスペース] メニューが表示されます。

2. **[ワークスペース]** メニューの **[ワークスペース]** をクリックします。

[ワークスペース] ページが表示されます。



デフォルトのアプリケーションを設定する

Tenable にログインすると、デフォルトで **[ワークスペース]** ページが表示されます。ただし、今後 **[ワークスペース]** ページをスキップするように、デフォルトアプリケーションを設定することもできます。

> デフォルトでは、**管理者**、**スキャンマネージャー**、**スキャンオペレーター**、**標準**、**基本**のロールを持つユーザーは、デフォルトのアプリケーションを設定できます。別のロールをお持ちの場合は、管理者に連絡して、**[マイアカウント]** から **[管理]** アクセス許可をリクエストしてください。詳細については、カスタムロールを参照してください。

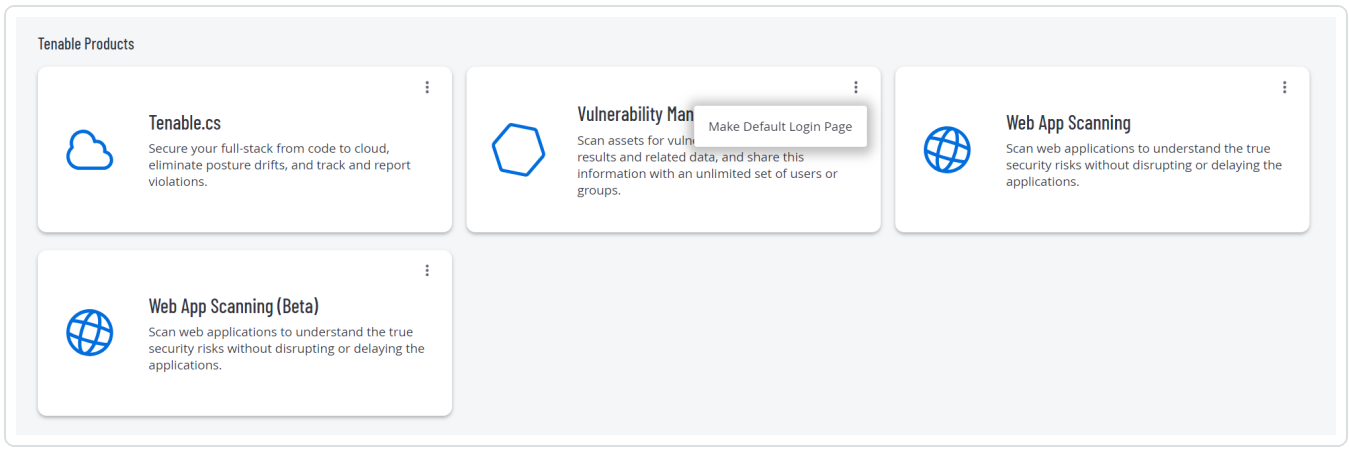
デフォルトのログインアプリケーションを設定する方法

1. Tenable にログインします。

   [ワークスペース] ページが表示されます。

2. 選択するアプリケーションの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。



3. メニューで、**[デフォルトログインページの作成]** をクリックします。

   ログインするとこのアプリケーションが表示されるようになります。

デフォルトのアプリケーションを削除する

デフォルトのアプリケーションを削除する方法

1. Tenable にログインします。

   [ワークスペース] ページが表示されます。

2. 削除するアプリケーションの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。

3. **[デフォルトログインページの削除]** をクリックします。

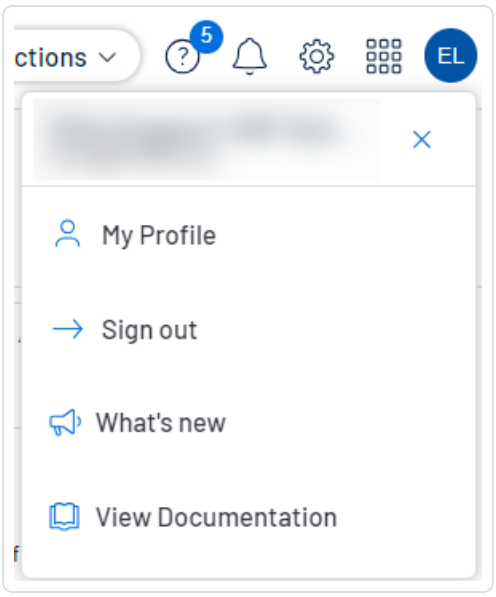
   ログインすると **[ワークスペース]** ページが表示されるようになります。

ユーザーアカウントメニュー

ユーザーアカウントメニューには、ユーザーアカウントのいくつかのクイックアクションがあります。

1. 右上の青いユーザー円をクリックします。

   ユーザーアカウントメニューが表示されます。



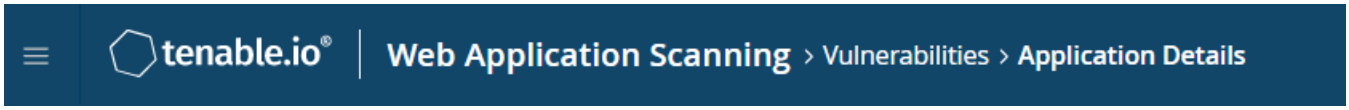
2. 次のいずれかを行います。

   - **[マイプロファイル]** をクリックして、自身のユーザーアカウントを設定します。**[マイアカウント]** 設定ページに直接移動します。
   - Tenable Web App Scanning からサインアウトするには、**[サインアウト]** をクリックします。
   - **[新機能]** をクリックして、Tenable Web App Scanning リリースノートに直接移動します。
   - **[ドキュメントの表示]** をクリックし、Tenable Web App Scanning ユーザーガイドのドキュメントに直接移動します。

Tenable Web App Scanning インターフェースのナビゲーション方法の詳細については、次のトピックを参照してください。

ブレッドクラムのナビゲーション

Tenable Web App Scanning インターフェースでは、特定のページの上部のナビゲーションバーにブレッドクラムが表示されます。ブレッドクラムには、現在のページに到達するまでにアクセスしたページの経路が左から右に向かって表示されます。



ブレッドクラムのナビゲーション方法

- 上部のナビゲーションバーで、ブレッドクラムのリンクをクリックし、前のページに戻ります。

プレーンのナビゲーション

Tenable Web App Scanning では、固定されたページとオーバーラップするプレーンが組み合わされています。

新しいインターフェースのプレーンのナビゲーション方法

1. 次のいずれかの方法を使用してプレーンにアクセスします。

   - ダッシュボード上のウィジェットをクリックします。
   - 左側のナビゲーションプレーンを次のように使用します。

     a. 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     b. 左側のナビゲーションプレーンで、メニューオプションをクリックします。

   左側のナビゲーションプレーンを除き、プレーンは画面の右側から開きます。

2. プレーンの左端にある次のボタンを使用してプレーンを操作します。

ボタン	短縮名	アクション
⤡	展開	プレーンを展開します。一部のプレーンは全画面に展開できます。
⤢	戻す	展開したプレーンをデフォルトのサイズに戻します。
×	閉じる	プレーンを閉じます。
←	プレビューを展開する	プレビュープレーンを展開します。
→	プレビューを元に戻す	展開したプレーンをプレビュープレーンに戻します。

3. 前のプレーンをクリックして、前のプレーンまたはページに戻ります (新しいプレーンは閉じます)。

Tenable Web App Scanning の表

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

Tenable Web App Scanning ワークベンチの表

Tenable Vulnerability Management ワークベンチの表とは、Tenable Vulnerability Management のインターフェースで **[調査]** セクション外にあるすべての表です。これらの表には検索機能とナビゲーション機能があります。列をドラッグアンドドロップして任意の順番に配置できる機能や、列幅の変更、複数列のデータを一度に並べ替える機能も備えています。詳細は、Tenable Web App Scanning ワークベンチの表を参照してください。

調査の表

調査 の表とは、Tenable Vulnerability Management のユーザーインターフェースの **[調査]** セクションにあるすべての表です。これらの表には Tenable Vulnerability Management ワークベンチの表にある多くの機能が含まれていますが、追加のカスタマイズ機能とフィルタリング機能も含まれています。詳細は、Explore Tables を参照してください。

Tenable Web App Scanning ワークベンチの表

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

注意: カスタマイズ可能な表では、表の行を右クリックすることでアクションボタンにアクセスすることもできます。ブラウザメニューにアクセスするには、Ctrl キーを押しながら右クリックします。

Tenable Web App Scanning ワークベンチの表とは、Tenable Web App Scanning のインターフェースで **[調査]** セクション外にあるすべての表です。

Tenable Web App Scanning ワークベンチの表を操作する方法

1. ワークベンチの表を表示します。
2. 次のいずれかを行います。

    - 表内を移動する場合

        - ソート順を調整するには、列のタイトルをクリックします。

          選択した列のデータを基準に、Tenable Web App Scanning は表のすべてのページをソートします。

        - Tenable Web App Scanning で、各ページに表示される行数を増減するには、**[ページ当たりの件数]** をクリックして、数字を選択します。

          Tenable Web App Scanning によって表が更新されます。

        - 表の行で利用可能なすべてのアクションボタンを表示するには、⋮ ボタンをクリックします。

          このボタンは、行に対して 5 つ以上のアクションが可能な場合に、個別のアクションボタンの代わりに表示されます。

        - 表の別のページに移動するには、矢印をクリックします。

ボタン	アクション
|<	表の最初のページに移動します。

< >	表の前のページまたは次のページに移動します。
>|	表の最後のページに移動します。

注意: 制限により、検出結果の合計数が 1000 の制限を超えていることがわからないことがあります。この場合、表のインターフェースが変わったり、ページ割のラベリングが変わったり、最終ページへのナビゲーションボタンが無効になったりする可能性があります。

- 表内を検索する場合

  新しいインターフェースでは、さまざまなページやプレーンの各表の上に検索ボックスが表示されます。いくつかのケースでは、検索ボックスは **[フィルター]** ボックスの横に表示されます。

  a. **[検索]** ボックスに検索条件を入力します。

     検索条件は、検索する表内のデータの種類によって異なります。

  b. 🔎 ボタンをクリックします。

     Tenable Web App Scanning は検索条件に従って表にフィルターを適用します。

- 列順を変更するには、列のヘッダーをドラッグアンドドロップして表内の別の場所に移動させます。

- 列を削除または追加する場合

  a. 任意の列にカーソルを合わせます。

     ヘッダーに ☰ ボタンが表示されます。

  b. ☰ ボタンをクリックします。

     列の選択ボックスが表示されます。

  c. 表で表示または非表示にする列のチェックボックスを、それぞれ選択または選択解除します。

     ヒント: 検索ボックスを使用すると列名を素早く見つけることができます。

     選択された内容に応じて表が更新されます。

- 列幅を調整する場合

  a. サイズ調整カーソルが表示されるまで、2 つの列の間のヘッダーにカーソルを合わせます。

     列幅をクリックしたままドラッグして、好みの幅に調整します。

     > **ヒント:** 内容に合わせて列幅を自動調整するには、列のヘッダーの右側をダブルクリックします。

- 表のデータをソートするには、列のヘッダーをクリックします。

  選択した列のデータを基準に、Tenable Web App Scanning は表のすべてのページをソートします。

- 複数の列を使用して表のデータをソートするには、**Shift** を押しながら 1 つ以上の列のヘッダーをクリックします。

  > **注意:** すべての表や列で複数の列によるソートができるわけではありません。

  Tenable Web App Scanning は、列を選択した順序で表のすべてのページをソートします。

表のフィルタリング

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

Tenable Web App Scanning では、さまざまなページやプレーンの各表の上に**[フィルター]**ボックスが表示されます。

表をフィルタリングする方法

1. **[フィルター]**の横にある ⌄ ボタンをクリックします。

   フィルター設定が表示されます。

2. (オプション) Tenable Vulnerability Management でフィルターを素早く選択するには、☆**[フィルターの選択]**をクリックします。

   ドロップダウンリストが表示されます。

   a. ドロップダウンリストで、適用するフィルターを検索します。

      検索条件に基づいて、リストが更新されます。

   b. 適用するフィルターの横にあるチェックボックスを選択します。

      選択したフィルターがフィルターセクションに表示されます。

3. **[カテゴリの選択]**ドロップダウンボックスで、属性を選択します。

   たとえば、検出結果をフィルタリングする場合には**[深刻度]**を、資産をフィルタリングする場合には**[資産 ID]**を選択できます。

4. **[演算子の選択]**ドロップダウンボックスで、演算子を選択します。

   注意: **[次の値を含む]**または**[次の値を含まない]**演算子を使用するには、次のベストプラクティスに従ってください。

   - 最も正確で完全な検索結果を生成するには、検索値に単語全体を入力します。
   - 検索値には終止符を含めません。

- 資産をフィルタリングする際は、検索値は大文字と小文字が区別されます。
- 可能であれば、Tenable は**[次の値に等しい]**または**[次の値に等しくない]**演算子の代わりに**[次の値を含む]**または**[次の値を含まない]**演算子を使用することを推奨しています。

5. **[値を選択する]**ボックスで、次のいずれかを行います。

値の種類	アクション
テキスト	フィルタリングしたい値を入力します。 入力を開始するまで、ボックスには予測入力の例が表示されます。入力内容が属性として無効な場合は、テキストボックスの周囲に赤い枠線が表示されます。
単一の有効な値	属性にデフォルトの値が関連付けられている場合、Tenable Web App Scanning は自動的にそのデフォルトの値を選択します。 デフォルトの値を変更する、またはデフォルトの値が関連付けられていない場合は、次を行います。 a. ボックスをクリックしてドロップダウンリストを表示します。 b. リストから値を探して、選択します。
複数の有効な値	1つ以上の値を選択するには、次を行います。 a. ボックスをクリックしてドロップダウンリストを表示します。 b. 値を探して、選択します。 選択した値がボックスに表示されます。 c. すべての該当する値が選択されるまで、繰り返します。

	d. ドロップダウンリストの外側をクリックして、リストを閉じます。 値を選択解除するには、次を行います。 a. 削除する値にカーソルを合わせます。 値の上に ✕ ボタンが表示されます。 b. ✕ ボタンをクリックします。 値がボックスから消えます。

6. (オプション) フィルターセクションの左下で、次を行います。
   - 別のフィルターを追加するには、**[追加]** ボタンをクリックします。
   - すべてのフィルターを消去するには、**[フィルターのリセット]** ボタンをクリックします。
7. **[適用]** をクリックします。

   Tenable Web App Scanning が 1 つまたは複数のフィルターを表に適用します。
8. (オプション) 1 つまたは複数のフィルターを後で使用するために保存します。
9. (オプション) 適用したフィルターを消去します。
   a. 表のヘッダーで、**[すべてのフィルターのクリア]** をクリックします。

      Tenable Web App Scanningにより、保存された検索条件を含むすべてのフィルターが表から消去されます。

      > **注意:** フィルターを消去しても、ページの右上で選択された日付範囲は変更されません。詳細は、Tenable Web App Scanning の表 を参照してください。

Docker イメージとして Tenable Web App Scanning をデプロイする

Tenable Web App Scanning を Docker イメージとしてデプロイして、コンテナで実行できます。基本となっているイメージは Tenable Web App Scanning の Oracle Linux 8 インスタンスです。環境変数を使って Tenable Web App Scanning インスタンスをセットアップすることで、設定で Docker イメージを自動的にデプロイできます。Docker イメージがデプロイされると、イメージを更新したりスキャナーログを収集したりすることもできます。

注意: Tenable Web App Scanning にはコマンドラインインターフェースまたは設定ウィザードがないため、環境変数を使用して Tenable Web App Scanning を設定する必要があります。

注意: Tenable Web App Scanning docker イメージは AMD 64 ビットシステムでのみ機能します。ARM または Windows システムはサポートしていません。

始める前に

- ご使用のオペレーティングシステム用の Docker をダウンロードして、インストールします。
- https://hub.docker.com/r/tenable/was-scanner から Tenable Web App Scanning Docker イメージにアクセスします。

Docker イメージのデプロイまたは削除

Docker イメージとして Tenable Web App Scanning をデプロイメントする方法

1. 演算子の説明に従って、デプロイメントに適切なオプションを指定して演算子を使用します。
2. 環境変数の説明に従って、-e 演算子を使用して環境変数を設定します。

Docker イメージとしての Tenable Web App Scanning を停止および削除する方法

注意: Docker コンテナとして実行中の Tenable Web App Scanning を削除すると、そのコンテナデータは失われます。

1. ターミナルで、`docker stop` コマンドを使用して、実行中のコンテナを停止します。

```
$ docker stop <container name>
```

2. docker rm コマンドを使用して、コンテナを削除します。

```
$ docker rm <container name>
```

演算子

演算子	説明
--name	Docker でコンテナの名前を設定します。
-d	コンテナをデタッチモードで起動します。
-e	環境変数に前置されます。 Tenable Web App Scanning インスタンスの設定の変更を行うために設定できる環境変数の説明については、環境変数を参照してください。

環境変数

Tenable Vulnerability Management にリンクされている Tenable Web App Scanning イメージのデプロイです。

変数	必須	説明
WAS_SCANNER_NAME	○	Tenable Vulnerability Management に表示される Tenable Web App Scanning スキャナーの名前。
WAS_LINKING_KEY	○	Tenable Vulnerability Management からのリンクキー。
WAS_SCANNER_GROUPS	×	スキャナーを追加する必要があるスキャナーグループ(例:「scanner-group-1、sec-scanner-group」)。
WAS_AUTO_UNLINK_ON_EXIT	×	スキャナー停止時にスキャナーのリンクを自動的に解除します。
WAS_PLATFORM_URL	×	デフォルトは https://cloud.tenable.com です。

WAS_PROXY_URL	×	プラットフォームへのプロキシに使用する URL。

Docker イメージの更新

Docker イメージを更新する方法

- docker pull tenable/was-scanner を実行します。

  これにより、Docker から最新バージョンのスキャナーがプルされます。

スキャナーログの収集

スキャナーログを収集するには、次のいずれかのオプションを使用します。

- WAS_LOG_TO_STDOUT を実行します。

  これにより、ログが stdout に出力され、docker logs <コンテナ ID> でそれらを収集できるようになります。

- WAS_SCANNER_LOG_FILE を、ホストにマウントした特定の場所に設定します。

  たとえば、docker run -e WAS_SCANNER_LOG_FILE=/scanner/scanner.log -v $PWD:/scanner となります。

  注意: このオプションでは、コンテナの停止後もログファイルが PWD に残ります。

Tenable Web App Scanning CI/CD アプリケーションスキャンの概要

Tenable Web App Scanning Docker イメージを継続的インテグレーションおよび継続的デリバリ/継続的デプロイメント (CI/CD) ツールとしてデプロイし、マージ前にソフトウェア上で Tenable Web App Scanning スキャンを実行することができます。アプリケーションのライフサイクルの任意の時点で CI/CD のアプリケーションとサービスをスキャンすることで、脆弱性をできるだけ早く発見し、セキュリティスタンスを大幅に改善できます。

始める前に

- CI/CD ビルドシステムが Docker コンテナの使用をサポートしていることを確認してください。

注意: CI/CD ビルドのスキャンは、一度に 1 つのスキャンに制限されています。

Tenable Web App Scanning の Docker イメージによる CI/CD ビルドのスキャン

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

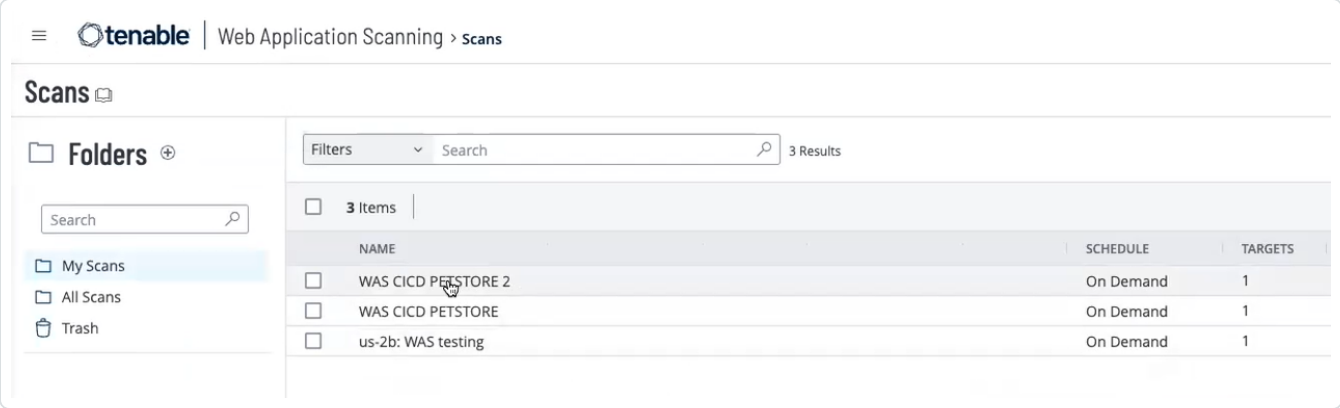
2. 左側のナビゲーションプレーンで、**[統合]** をクリックします。

   [統合] ページが表示されます。

3. 左側のナビゲーションプレーンで、統合のタイプを選択します。

   - Atlassian Bamboo
   - CircleCI
   - GitHub
   - GitLab
   - Jenkins

4. Tenable Web App Scanning ユーザーインターフェースでスキャンを見つけます。



注意: **[スキャナータイプ]** および **[スキャナー]** フィールドは CI/CD スキャンには適用されないため、デフォルト設定のままにしておく必要があります。

注意: CI/CD パイプラインに統合するためにスキャンを設定する場合、Tenable では、ランタイムが比較的短いスキャンテンプレートを選択して、ビルドプロセスの潜在的な遅延を回避することを推奨しています。詳細については、[スキャンテンプレート] セクションを参照してください。

注意: ターゲットのホスト名が本番アプリケーションとは異なるものであることを確認してください。そうすることで、ビルド中に見つかった脆弱性と、本番アプリケーションの脆弱性との混在を防ぐことができます。

5. 選択したスキャンのスキャン設定をスキャンパイプラインステージにエクスポートします。

   [スキャン] ページで、選択したスキャンの ⋮ ボタンをクリックし、**[CI/CD 用にエクスポート]** を選択します。

6. スキャン設定ファイルを Git リポジトリにアップロードします。

7. (オプション) 設定ファイルで 認証スキャンの編集 を作成します。

8. API キーを生成します。

   注意: API キーがない場合は、**[アカウント]** ページで生成できます。詳細は、API キーを生成する を参照してください。

9. 生成した API キーを優先シークレットストレージプロバイダーにコピーします。

   警告: Tenable では、スキャナーを Tenable にリンクするために使用される API キーや、スキャン対象のウェブアプリに認証するためにスキャナーが使用するユーザー名 / パスワードの組み合わせなどの、機密情報を

非表示にするという対策を常に講じることを推奨しています。これらはソースコントロールには含めず、リポジトリまたは使用中の継続的インテグレーションツールが提供する安全なストレージに保管してください。

10. 次の手順を実行してスキャンを実行します。

```
docker pull tenable/was-scanner:latest
docker run -e WAS_MODE=cicd -e ACCESS_KEY=${TENABLE_IO_ACCESS_KEY}
SECRET_KEY=${TENABLE_IO_SECRET_KEY} -v ./:/scanner tenable/was-
scanner:latest
```

11. vulnerability_threshold フィールドパラメーターを **[重大]**、**[高]**、**[中]**、または **[低]** に設定します。

注意: このフィールドに設定したしきい値によって、ビルドがしきい値を満たすかどうかに応じて、ビルドの合格または不合格が決まります。スキャンエラーまたは設定が不完全なために、ビルドが失敗することもあります。

12. (オプション) 以下の CI/CD パイプラインワークフローファイル セクションで説明されているように、CI/CD 統合に必要なパイプラインワークフローファイルの特定のアウトラインに従います。

13. **[スキャン]** ページで選択したスキャンに移動して、結果を確認します。

14. (オプション) ログを取得します。後述のレポートとログセクションを参照してください。

注意: スキャナー Docker イメージは、ホストと Docker コンテナ間のシームレスなファイル交換のために /scanner ディレクトリを使用します。リポジトリにある tenable_was.conf ファイルをマウントするには、docker run コマンドで -v $PWD:/scanner を使用します。設定ファイルがリポジトリのトップレベルにある場合、スキャン後にこのディレクトリから tenable_was_scan.html および scanner.log ファイルを取得できます。

認証スキャンの編集

スキャン設定を作成しそのスキャンに認証情報を追加するときに、エクスポートした CI/CD ファイルの認証情報を編集することもできます。エクスポートされた tenable_was.conf ファイルでは、これらの認証情報 (パスワード、認証トークンなど) に関連する機密情報の代わりに、プレースホルダーテキストが含まれる場合があります。たとえば、${?USER_PASS_PASSWORD} と ${?USER_PASS_USERNAME} は、次のサンプルファイルのプレースホルダーです。

注意: ログインフォーム、Cookie 認証、API キーの認証方法では、認証スキャンを編集する必要があります。

```
scan {
  credentials {
    "user_pass" {
    "auth_type"=auto
    password=${?USER_PASS_PASSWORD}
    username=${?USER_PASS_USERNAME}
  }
}
```

Docker イメージを実行する場合、これらのプレースホルダーは、スキャナーが実際の値を取得する環境変数を表します。そのため、これらの環境変数が存在することを確認してください。前の例では、次の例に示すように、これらの値を入力するために必要な環境変数を使用して docker イメージを実行します。

```
`docker run -e WAS_MODE=cicd -e USER_PASS_USERNAME=<the username here> -e
USER_PASS_PASSWORD=<the password here> ..etc, etc`
```

値がキーおよび値の両方として機能する場合は、対応するキーと値のペアを含む JSON オブジェクトとして値を提供する必要があります。たとえば、ウェブアプリケーションでログインフォーム認証を使用し、「ユーザー名」や「パスワード」などのフィールド名と値の両方が必要な場合は、次のように設定する必要があります。

```
scan {
  credentials {
    "login_form" {
    "auth_headers"=${?LOGIN_FORM_AUTH_HEADERS}
    "login_check"=Welcome
    "login_check_pattern"=Welcome
    "login_check_url"="http://app:3000/home.html"
    "login_parameters"=${?LOGIN_FORM_LOGIN_PARAMETERS};
  }
}
```

次の入力例を使用できます。

```
`docker run -e WAS_MODE=cicd -e LOGIN_FORM_LOGIN_PARAMETERS='{"username":
"my_username", "password":"my_password"}'-e LOGIN_FORM_AUTH_HEADERS='{}'
…etc, etc`
```

注意: 値が空の場合でも、すべてのプレースホルダー値に値が存在することを確認してください。

CI/CD パイプラインワークフローファイル

原理を理解すると、パイプラインワークフローファイルの設定を利用可能な多くのツールに適用できます。以下は、Jenkins のパイプラインワークフローファイルの例です。

```
pipeline {
  agent any
  stages {
    stage('build-run-scan') {
      environment {
        ACCESS_KEY = credentials('ACCESS_KEY')
        SECRET_KEY = credentials('SECRET_KEY')
      }
      steps {
        sh '''
        docker pull swaggerapi/petstore
        docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
        docker pull tenable/was-scanner:latest
        docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest
        '''
      }
    }
  }
  post {
    always {
```

```
      sh '''
      docker rm $(docker stop $(docker ps -a -q --filter
ancestor="tenable/was-scanner:latest" --format="{{.ID}}")) || true
      docker rm $(docker stop $(docker ps -a -q --filter
ancestor="swaggerapi/petstore" --format="{{.ID}}")) || true
      docker system prune -f --volumes
      '''
      archiveArtifacts 'scanner.log'
      publishHTML([allowMissing: false, alwaysLinkToLastBuild: false,
keepAll: true, reportDir: '', reportFiles: 'tenable_was_scan.html',
reportName: 'WAS Report'])
      cleanWs()
    }
  }
}
```

レポートとログ

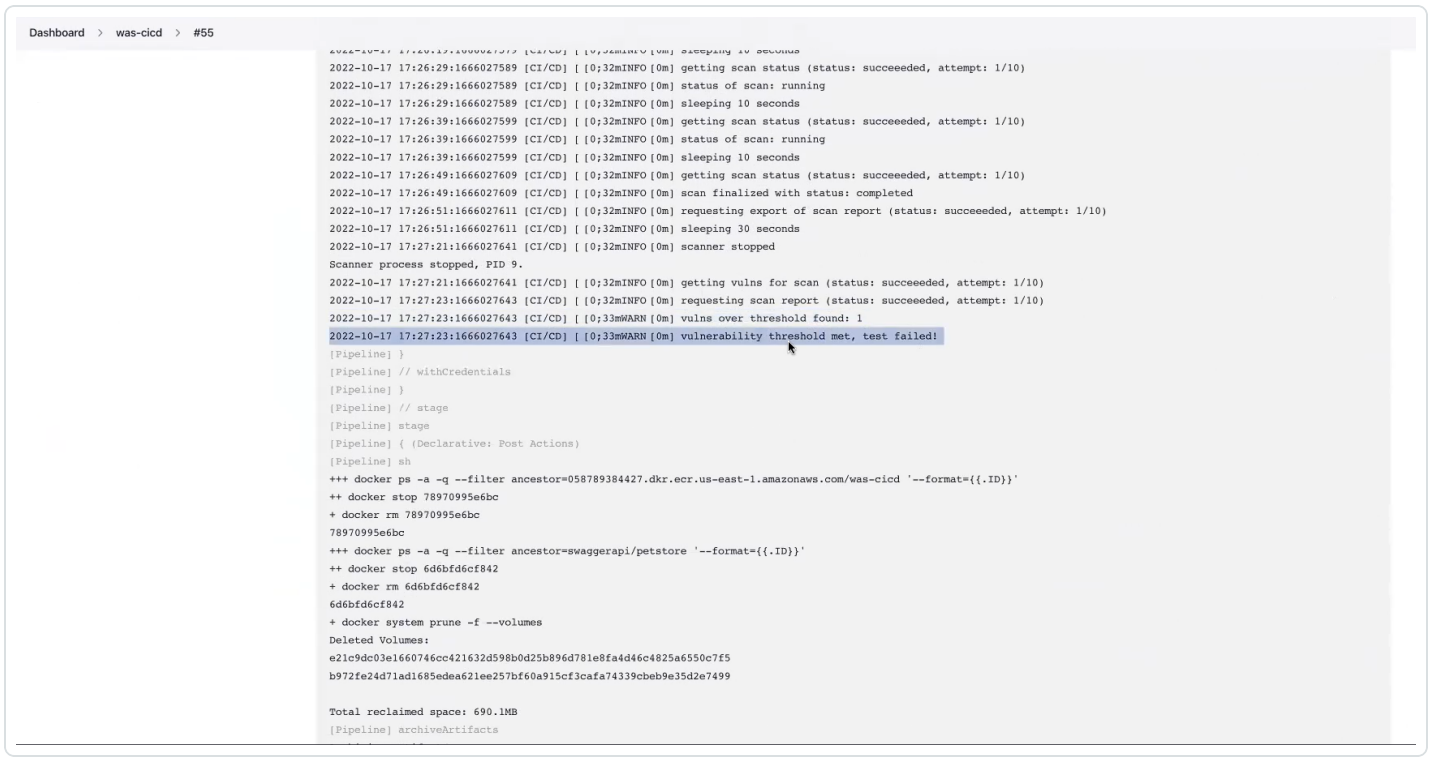
各ビルドの後に、コンソール出力、HTML レポート (tenable_was_scan.html)、およびスキャナーログファイル(scanner.log)を生成できます。コマンドラインを使用して、HTML レポートとスキャナーログをアーカイブします。これらは各 CI/CD ツールに固有です。ビルド完了後のコンソール出力は、ビルドの合否、および考えられる原因を示します。HTML レポートは、tenable-was.conf ファイルに入力した vulnerability_threshold に基づいて詳細なスキャン結果を示します。

> **注意:** Tenable では、スキャナーログがデバッグに役立つ可能性があるため、スキャナーログを保持することを推奨しています。

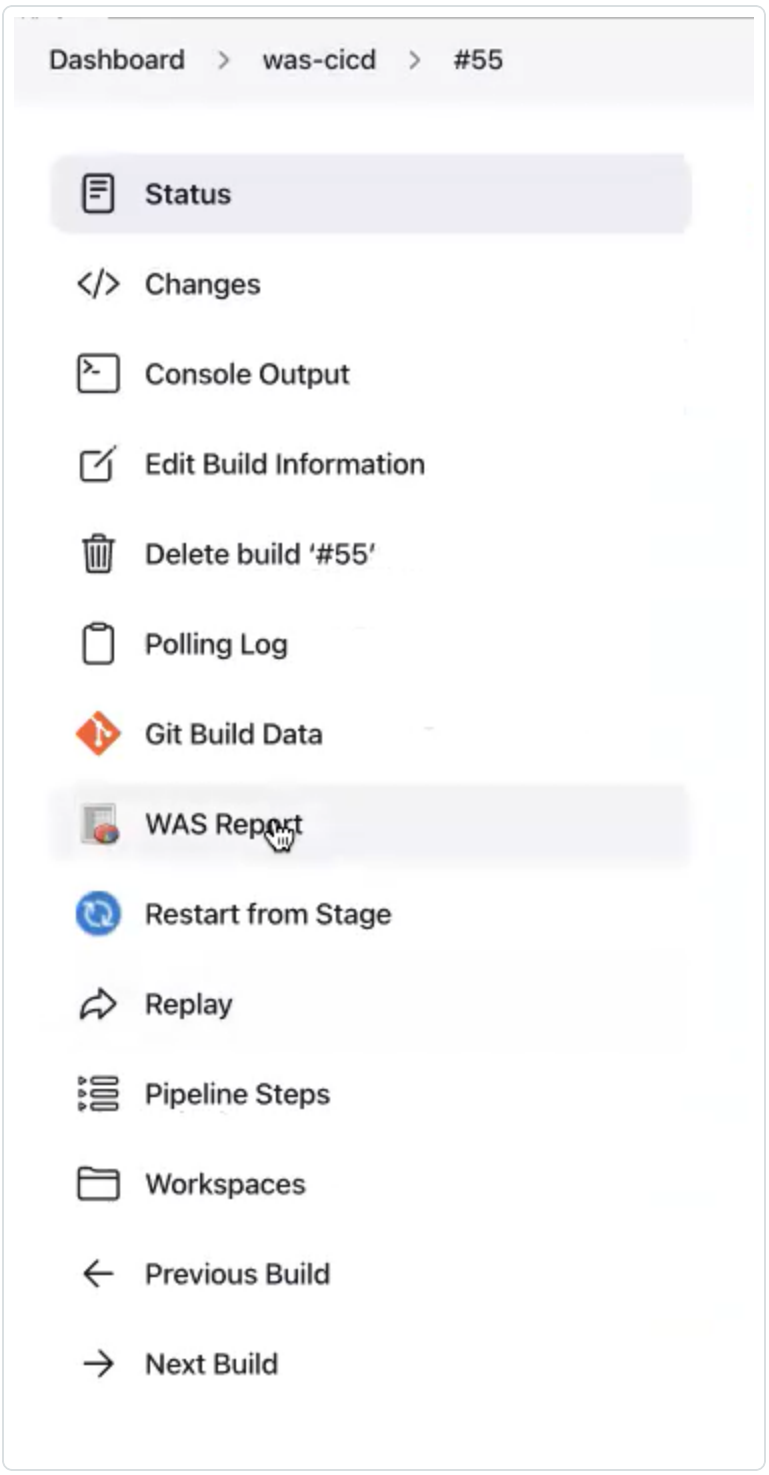
Jenkins パイプラインワークフローファイルのアーカイブコマンドラインの例

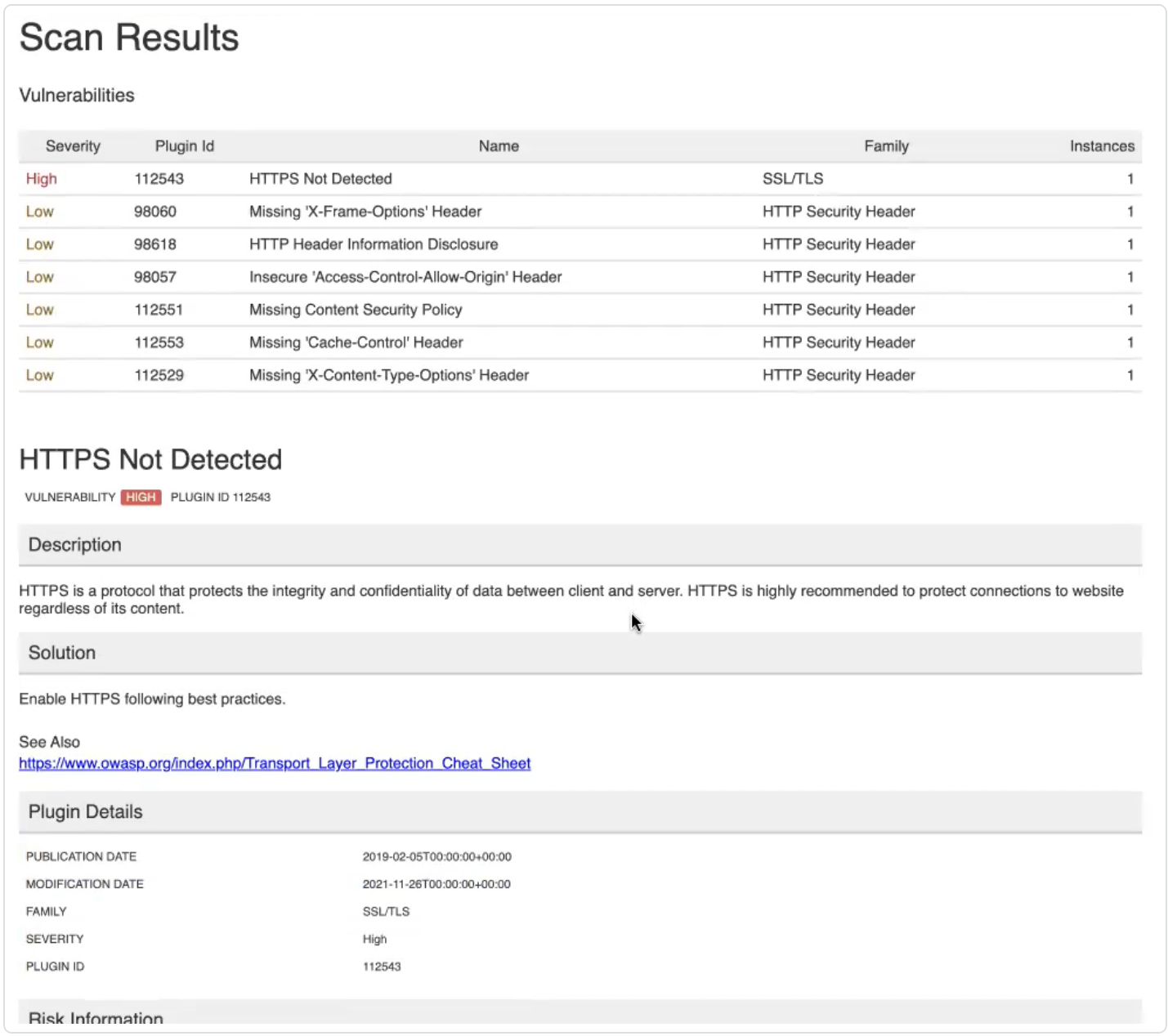
```
archiveArtifacts 'scanner.log' publishHTML([allowMissing: false,
alwaysLinkToLastBuild: false, keepAll: true, reportDir: '', reportFiles:
'tenable_was_scan.html', reportName: 'WAS Report']
```

コンソール出力の例


Dashboard > was-cicd > #55
2022-10-17 17:26:29:1666027589 [CI/CD] [[0;32mINFO [0m] getting scan status (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:29:1666027589 [CI/CD] [[0;32mINFO [0m] status of scan: running
2022-10-17 17:26:29:1666027589 [CI/CD] [[0;32mINFO [0m] sleeping 10 seconds
2022-10-17 17:26:39:1666027599 [CI/CD] [[0;32mINFO [0m] getting scan status (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:39:1666027599 [CI/CD] [[0;32mINFO [0m] status of scan: running
2022-10-17 17:26:39:1666027599 [CI/CD] [[0;32mINFO [0m] sleeping 10 seconds
2022-10-17 17:26:49:1666027609 [CI/CD] [[0;32mINFO [0m] getting scan status (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:49:1666027609 [CI/CD] [[0;32mINFO [0m] scan finalized with status: completed
2022-10-17 17:26:51:1666027611 [CI/CD] [[0;32mINFO [0m] requesting export of scan report (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:51:1666027611 [CI/CD] [[0;32mINFO [0m] sleeping 30 seconds
2022-10-17 17:27:21:1666027641 [CI/CD] [[0;32mINFO [0m] scanner stopped
Scanner process stopped, PID 9.
2022-10-17 17:27:21:1666027641 [CI/CD] [[0;32mINFO [0m] getting vulns for scan (status: succeeeded, attempt: 1/10)
2022-10-17 17:27:23:1666027643 [CI/CD] [[0;32mINFO [0m] requesting scan report (status: succeeeded, attempt: 1/10)
2022-10-17 17:27:23:1666027643 [CI/CD] [[0;33mWARN [0m] vulns over threshold found: 1
2022-10-17 17:27:23:1666027643 [CI/CD] [[0;33mWARN [0m] vulnerability threshold met, test failed!
[Pipeline] }
[Pipeline] // withCredentials
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Declarative: Post Actions)
[Pipeline] sh
+++ docker ps -a -q --filter ancestor=058789384427.dkr.ecr.us-east-1.amazonaws.com/was-cicd '--format={{.ID}}'
++ docker stop 78970995e6bc
+ docker rm 78970995e6bc
78970995e6bc
+++ docker ps -a -q --filter ancestor=swaggerapi/petstore '--format={{.ID}}'
++ docker stop 6d6bfd6cf842
+ docker rm 6d6bfd6cf842
6d6bfd6cf842
+ docker system prune -f --volumes
Deleted Volumes:
e21c9dc03e1660746cc421632d598b0d25b896d781e8fa4d46c4825a6550c7f5
b972fe24d71ad1685edea621ee257bf60a915cf3cafa74339cbeb9e35d2e7499
Total reclaimed space: 690.1MB
[Pipeline] archiveArtifacts

HTML レポートの例


Dashboard > was-cicd > #55
Status
Changes
Console Output
Edit Build Information
Delete build '#55'
Polling Log
Git Build Data
WAS Report
Restart from Stage
Replay
Pipeline Steps
Workspaces
Previous Build
Next Build



Scan Results

Vulnerabilities

Severity	Plugin Id	Name	Family	Instances
High	112543	HTTPS Not Detected	SSL/TLS	1
Low	98060	Missing 'X-Frame-Options' Header	HTTP Security Header	1
Low	98618	HTTP Header Information Disclosure	HTTP Security Header	1
Low	98057	Insecure 'Access-Control-Allow-Origin' Header	HTTP Security Header	1
Low	112551	Missing Content Security Policy	HTTP Security Header	1
Low	112553	Missing 'Cache-Control' Header	HTTP Security Header	1
Low	112529	Missing 'X-Content-Type-Options' Header	HTTP Security Header	1

HTTPS Not Detected

VULNERABILITY HIGH PLUGIN ID 112543

Description

HTTPS is a protocol that protects the integrity and confidentiality of data between client and server. HTTPS is highly recommended to protect connections to website regardless of its content.

Solution

Enable HTTPS following best practices.

See Also
https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Plugin Details

PUBLICATION DATE	2019-02-05T00:00:00+00:00
MODIFICATION DATE	2021-11-26T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	High
PLUGIN ID	112543

Risk Information

CI/CD ツールの統合の例

- Atlassian Bamboo
- CircleCI
- GitHub
- GitLab
- Jenkins

Atlassian Bamboo 統合による Tenable Web App Scanning CI/CD スキャン

Atlassian Bamboo のアプリケーションに対して、継続的インテグレーションおよび継続的デリバリ/継続的デプロイメント CI/CD で Tenable Web App Scanning Docker イメージをデプロイすることができます。この統合の詳細については、Atlassian Bamboo のドキュメントを参照してください。

始める前に

- Bamboo ビルドエージェントが利用できる統合環境にアプリをデプロイできるようにするか、テストのためにビルドエージェントで直接実行できるようにします。
- CI/CD アプリケーションスキャンの概要で概要情報を確認してください。

Atlassian Bamboo のパイプラインワークフローファイルの例

```
#!/usr/bin/env bash

# start your application
docker pull swaggerapi/petstore
docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_PATH=/v2 -
-name petstore swaggerapi/petstore

# run the scanner
docker pull tenable/was-scanner:latest
docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_KEY=${bamboo_
ACCESS_KEY} -e SECRET_KEY=${bamboo_SECRET_KEY} --link petstore tenable/was-
scanner:latest
```

CI/CD ツールの統合の例

- CircleCI
- GitHub
- GitLab
- Jenkins

CircleCI 統合による Tenable Web App Scanning CI/CD スキャン

CircleCI のアプリケーションに対して、継続的インテグレーションおよび継続的デリバリ/継続的デプロイメント CI/CD で Tenable Web App Scanning Docker イメージをデプロイすることができます。この統合の詳細については、CircleCI のドキュメントを参照してください。

始める前に

- GitLab ビルドエージェントが利用できる統合環境にアプリをデプロイできるようにするか、テストのためにビルドエージェントで直接実行できるようにします。
- CI/CD アプリケーションスキャンの概要で概要情報を確認してください。

CircleCI のパイプラインワークフローファイルの例

```
version: 2.1

jobs:
  build-run-scan:
    machine:
      image: ubuntu-2204:2022.04.2
    steps:
      - checkout
      - run: |
          docker pull swaggerapi/petstore
          docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
          docker pull tenable/was-scanner:latest
          docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest
workflows:
  was-workflow:
    jobs:
      - build-run-scan
```

CI/CD ツールの統合の例

- Atlassian Bamboo
- GitHub
- GitLab
- Jenkins

GitHub 統合による Tenable Web App Scanning CI/CD スキャン

GitHub のアプリケーションに対して、継続的インテグレーションおよび継続的デリバリ/継続的デプロイメント CI/CD で Tenable Web App Scanning Docker イメージをデプロイすることができます。この統合の詳細については、GitHub のドキュメントを参照してください。

始める前に

- GitHub ビルドエージェントが利用できる統合環境にアプリをデプロイできるようにするか、テストのためにビルドエージェントで直接実行できるようにします。
- CI/CD アプリケーションスキャンの概要で概要情報を確認してください。

GitHub のパイプラインワークフローファイルの例

```
name: CI WAS Scan
on:
  push:
    branches:
      - main
  pull_request:
jobs:
  tenablescan:
    name: was-cicd
    runs-on: ubuntu-latest
    steps:
      - name: Clone repo
        uses: actions/checkout@v2
      - name: Build + Run PetStore
        run: |
          docker pull swaggerapi/petstore
          docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
      - name: Run WAS
        run: |
          docker pull tenable/was-scanner:latest
```

```
          docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest || true
          ls $(pwd)
        env:
          ACCESS_KEY: ${{ secrets.ACCESS_KEY }}
          SECRET_KEY: ${{ secrets.SECRET_KEY }}
```

CI/CD ツールの統合の例

- Atlassian Bamboo
- CircleCI
- GitHub
- GitLab
- Jenkins

GitLab 統合による Tenable Web App Scanning CI/CD スキャン

GitLab のアプリケーションに対して、継続的インテグレーションおよび継続的デリバリ/継続的デプロイメント CI/CD で Tenable Web App Scanning Docker イメージをデプロイすることができます。この統合の詳細については、GitLab のドキュメントを参照してください。

始める前に

- GitLab ビルドエージェントが利用できる統合環境にアプリをデプロイできるようにするか、テストのためにビルドエージェントで直接実行できるようにします。
- CI/CD アプリケーションスキャンの概要で概要情報を確認してください。

GitLab のパイプラインワークフローファイルの例

```
stages:
       - build
build-run-scan:
       stage: build
       image: docker
       services:
       - docker:dind
       script:
       - docker pull swaggerapi/petstore
       - docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
       - docker pull tenable/was-scanner:latest
       - docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_KEY=${ACCESS_
KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-scanner:latest
```

CI/CD ツールの統合の例

- Atlassian Bamboo
- CircleCI

- GitHub
- Jenkins

Jenkins 統合による Tenable Web App Scanning CI/CD スキャン

Jenkins のアプリケーションに対して、継続的インテグレーションおよび継続的デリバリ/継続的デプロイメント CI/CD で Tenable Web App Scanning Docker イメージをデプロイすることができます。この統合の詳細については、Jenkins のドキュメントを参照してください。

始める前に

- Jenkins ビルドエージェントが利用できる統合環境にアプリをデプロイできるようにするか、テストのためにビルドエージェントで直接実行できるようにします。
- CI/CD アプリケーションスキャンの概要で概要情報を確認してください。

Jenkins のパイプラインワークフローファイルの例

```
pipeline {
  agent any
  stages {
    stage('build-run-scan') {
      environment {
        ACCESS_KEY = credentials('ACCESS_KEY')
        SECRET_KEY = credentials('SECRET_KEY')
      }
      steps {
        sh '''
        docker pull swaggerapi/petstore
        docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
        docker pull tenable/was-scanner:latest
        docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest
        '''
      }
    }
  }
```

```
  post {
    always {
      sh '''
        docker rm $(docker stop $(docker ps -a -q --filter
ancestor="tenable/was-scanner:latest" --format="{{.ID}}")) || true
        docker rm $(docker stop $(docker ps -a -q --filter
ancestor="swaggerapi/petstore" --format="{{.ID}}")) || true
        docker system prune -f --volumes
        '''
        archiveArtifacts 'scanner.log'
        publishHTML([allowMissing: false, alwaysLinkToLastBuild: false,
keepAll: true, reportDir: '', reportFiles: 'tenable_was_scan.html',
reportName: 'WAS Report'])
        cleanWs()
    }
  }
}
```

CI/CD ツールの統合の例

- Atlassian Bamboo
- CircleCI
- GitHub
- GitLab

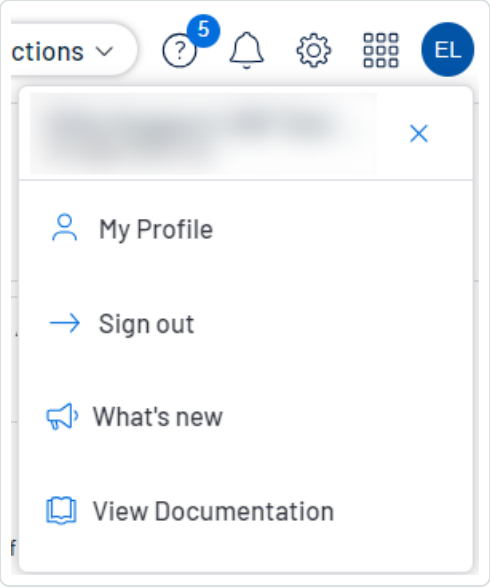
Tenable Web App Scanning をログアウトする

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

Tenable Web App Scanning をログアウトする方法

1. 右上の青いユーザー円をクリックします。

   ユーザーアカウントメニューが表示されます。



2. **[サインアウト]** をクリックします。

Tenable Web App Scanning ダッシュボード

デフォルトの **Web Application Scanning** ダッシュボードには Tenable Web App Scanning が収集したデータが表示されます。

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

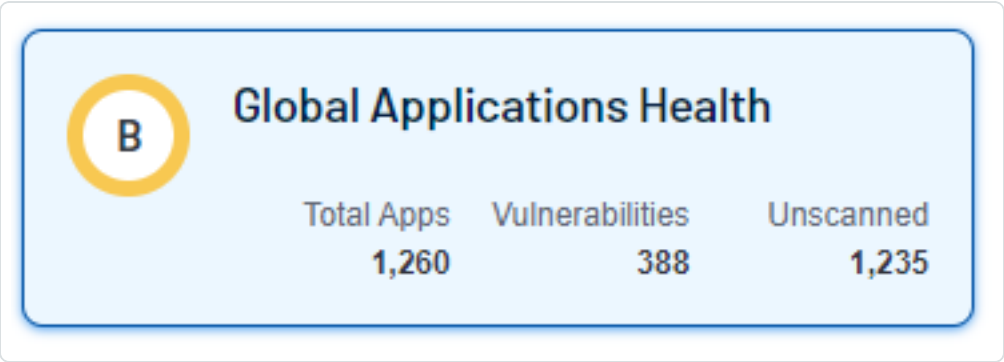
知っていましたか?ウェブアプリケーションサイバーエクスポージャー: WAS 利用者のすべてのアプリケーションのサイバーエクスポージャー平均スコアは 460 です。

Tenable Web App Scanning では、リスクの評価に役立つ複数のメトリクスを使用します。

- 総合スコア
- 資産のエクスポージャースコア (AES)
- 上位の要因
- 修正
- 防止

Tenable Web App Scanning グローバルアプリケーションの健全性

次の表では、**Web Application Scanning** ダッシュボードの **[グローバルアプリケーションの健全性]** セクションに表示されるセクションとウィジェットについて説明します。ウィジェットをクリックすると、データに関する詳細をウィジェットに表示できます。左側のパネルの **[グローバルアプリケーションの健全性]** ウィジェットには、**アプリの合計**、**脆弱性**、**未スキャン**のアプリケーションの情報が表示されます。



総合スコア

ダッシュボードのリングチャートの外周の円は、4 つのスキャン対象アプリケーションと、残りのアプリケーションが含まれる小さな **[その他]** のセグメントの資産のエクスポージャースコア (AES) を追跡します。このセグメントをクリックすると、次の 4 つのアプリケーションとそれらに関連する詳細を表示できます。各セグメントの色は、現在の AES スコアに合わせて変化します。ダッシュボードのリングチャートの中央には、全体的な Cyber Exposure Score (CES) のスコアが表示され、色が現在の CES グレードとともに変化します。アプリケーションの詳細については、検出結果を参照してください。

ヒント: ダッシュボードのリングチャートの内側の円はすべてのアプリケーションにわたる総合スコア (CES) を表し、外側の円は個別のアプリケーションスコア (AES) を表します。内側の円では健全であることが示されても、外側の円には健全でないアプリケーションが表示される場合があります。

ウィジェット	説明
総合スコア	Tenable Web App Scanning が検出した検出結果の数。Tenable Web App Scanning は、検出結果を深刻度 (**重大**と**高**) 別に分類します。 Tenable でリスク分析に使用する脆弱性の格付けと深刻度のメトリクスについては、*Tenable Vulnerability Management ユーザーガイド*の深刻度と VPR を参照してください。
スキャンされたウェブアプリ	経時的にスキャンされたアプリケーションの数

ウィジェット	説明
ケーション	
不完全なスキャン	過去 90 日間の不完全なスキャンの数。
非認証スキャン	過去 90 日間の認証されていないスキャンの数。

資産のエクスポージャースコア (AES)

Tenable Web App Scanning は、ネットワーク上の各アプリケーションの動的な AES を計算します。これは、アプリケーションの相対的なサイバーエクスポージャーを 0 ~ 1000 の整数で表したものです。AES が高くなるほど、高いサイバーエクスポージャーを示しています。

Tenable Web App Scanning は、現在の ACR(Tenable が提供する、またはカスタム) と、アプリケーションに関連付けられている VPR に基づいて AES を計算します。

AES カテゴリ	AES 範囲
高	650 ~ 1000
中	350 ~ 649
低	0 ~ 349

注意: 資産のエクスポージャースコア (AES) は、有効な Lumin ライセンスを持つお客様だけが、Tenable Web App Scanning で参照できます。

上位の要因

ユーザーインターフェースの右側にある上位の要因のリストは、お使いの Tenable Web App Scanning インスタンスに存在するスキャンされたアプリケーションの深刻度分類を示しています。これらの項目が総合スコアを高める要因になっています。次のことを調べて対処すると、スコアを下げることができます。

- **% のアプリケーションに、重大、高、中、低のいずれかのリスクがあります**
- **% のアプリケーションに、重大、高、中、低のいずれかのリスクがあります**

- **(xyz 個) のアプリケーションの脆弱性があります**
- **アプリケーションあたり、平均で (xyz 個) の脆弱性があります**

注意: Tenable Web App Scanning はこのリストに 4 つの項目だけを表示します。最初の 2 つの項目は常に、存在するリスクの深刻度が最も高いアプリケーション 2 つを表示します。最後の 2 つの要因項目は、必ずダッシュボードにあるものです。

アプリケーションサイバーエクスポージャーの管理

修正

修正メトリクスは、すべてのウェブアプリケーションで、重大な脆弱性と未認証のスキャンに対処し、解決するのに役立ちます。

ウィジェット	説明
重大な脆弱性を修正する	Tenable Web App Scanning が検出した検出結果の数。Tenable Web App Scanning は、検出結果を深刻度 (**重大**と**高**) 別に分類します。 Tenable でリスク分析に使用する脆弱性の格付けと深刻度のメトリクスについては、*Tenable Vulnerability Management ユーザーガイド*の深刻度と VPR を参照してください。
不完全なスキャンに対処する	過去 90 日間の認証されていないスキャンの数。 **注意:** 不完全なスキャンとは、ステータスが「中止」、「キャンセル」、「部分的なエラー」のいずれかのスキャンです。
認証されていないスキャンに対処する	過去 90 日間の認証されていないスキャンの数。
OWASP Top 10 の脆弱性を修正する	過去 90 日間の認証されていないスキャンの数。

防止

防止メトリクスは、未スキャンのアプリケーションとスキャン済みのアプリケーションでのすべての検出結果の中から潜在的な脆弱性を早期に特定し、緩和するのに役立ちます。

ウィジェット	説明
未スキャンのウェブアプリケーションをスキャンする	過去 90 日間の不完全なスキャンの数。
検出結果をすべて調べる	経時的にスキャンされたアプリケーションの数

Tenable Web App Scanning 統計

次の表では、**Web Application Scanning** ダッシュボードの[統計]セクションに表示されるウィジェットについて説明します。ウィジェットをクリックすると、データに関する詳細をウィジェットに表示できます。

ウィジェット	説明
検出結果	Tenable Web App Scanning が検出した検出結果の数。Tenable Web App Scanning は、検出結果を深刻度(**重大**と**高**)別に分類します。 Tenable でリスク分析に使用する脆弱性の格付けと深刻度のメトリクスについては、*Tenable Vulnerability Management ユーザーガイド*の深刻度と VPR を参照してください。
スキャンされたウェブ資産	経時的にスキャンされた資産の数。
不完全なスキャン	過去 90 日間の不完全なスキャンの数。
認証されていないスキャン	過去 90 日間の認証されていないスキャンの数。

OWASP Top 10

このチャートには、最新の OWASP (Open Web Application Security Project) の Top 10 Most Critical Web Application Security Risks (上位 10 個の最も重大なウェブアプリケーションセキュリティリスク) ドキュメントに記載されているものの中で、Tenable Web App Scanning が検出した脆弱性が表示されます。

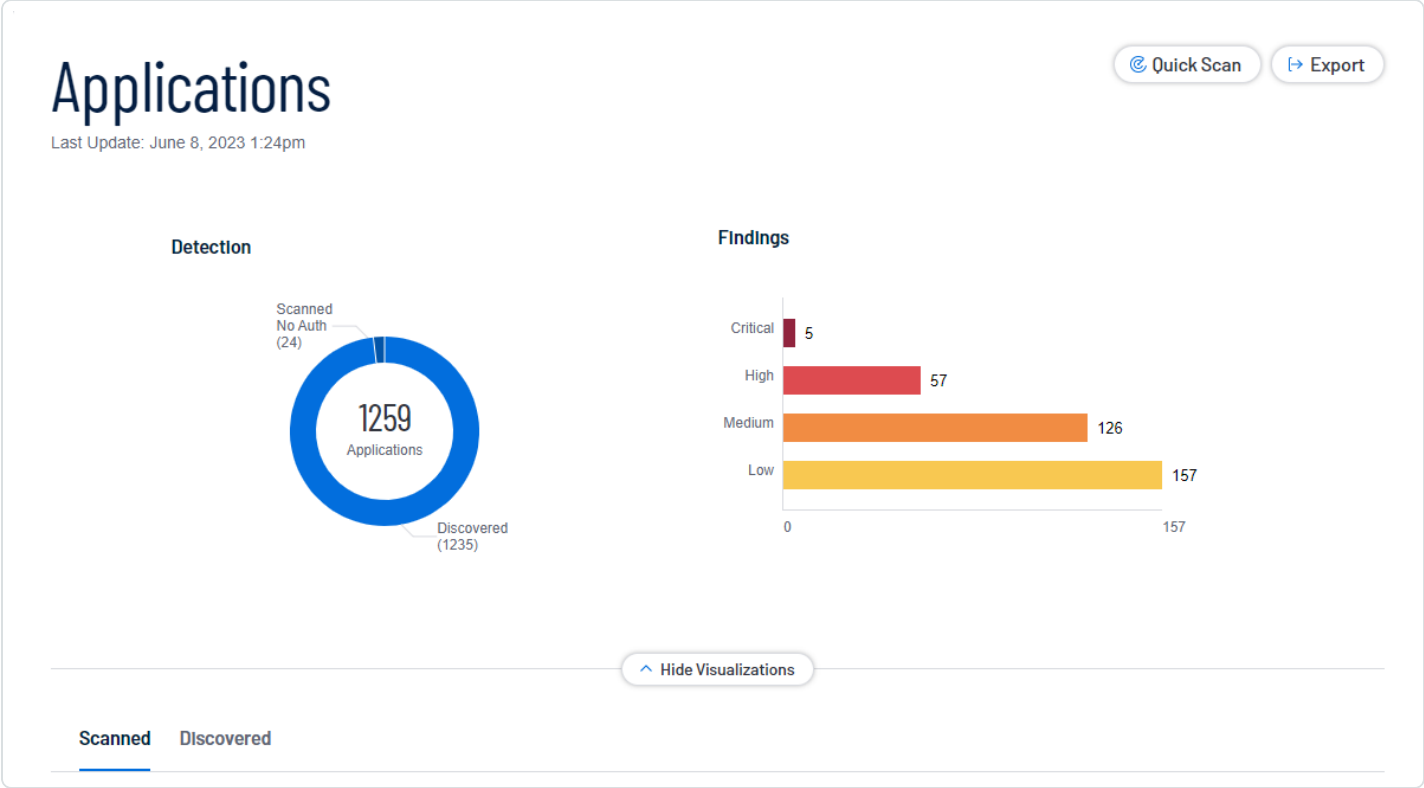
次のステップ

特定のアプリケーションのスコアと詳細を表示するには、以下のページを参照してください。

- スキャン済みアプリケーション
- 検出済みアプリケーション

スキャン済みアプリケーション

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか



[アプリケーション] ページでドリルダウンして、**スキャン済み**のアプリケーションだけを表示できます。また、**[スキャン済み]** アプリケーションタブでは、スキャン済みアプリケーション資産をエクスポートすることができます。詳細については、アプリケーションのエクスポートを参照してください。

スキャン済みアプリケーションを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[アプリケーション]** をクリックします。

   [アプリケーション] ページが表示されます。デフォルトでは、**[スキャン済み]** タブが表示され、アプリケーションがビジュアル化されて表示されます。

3. スキャン済みアプリケーションの表で ⋮ ボタンをクリックすると、次のアクションのいずれかまたはすべてを実行できます。

    - 資産をエクスポートする
    - 資産にタグを追加する
    - 資産からタグを削除する
    - リストから資産を削除する

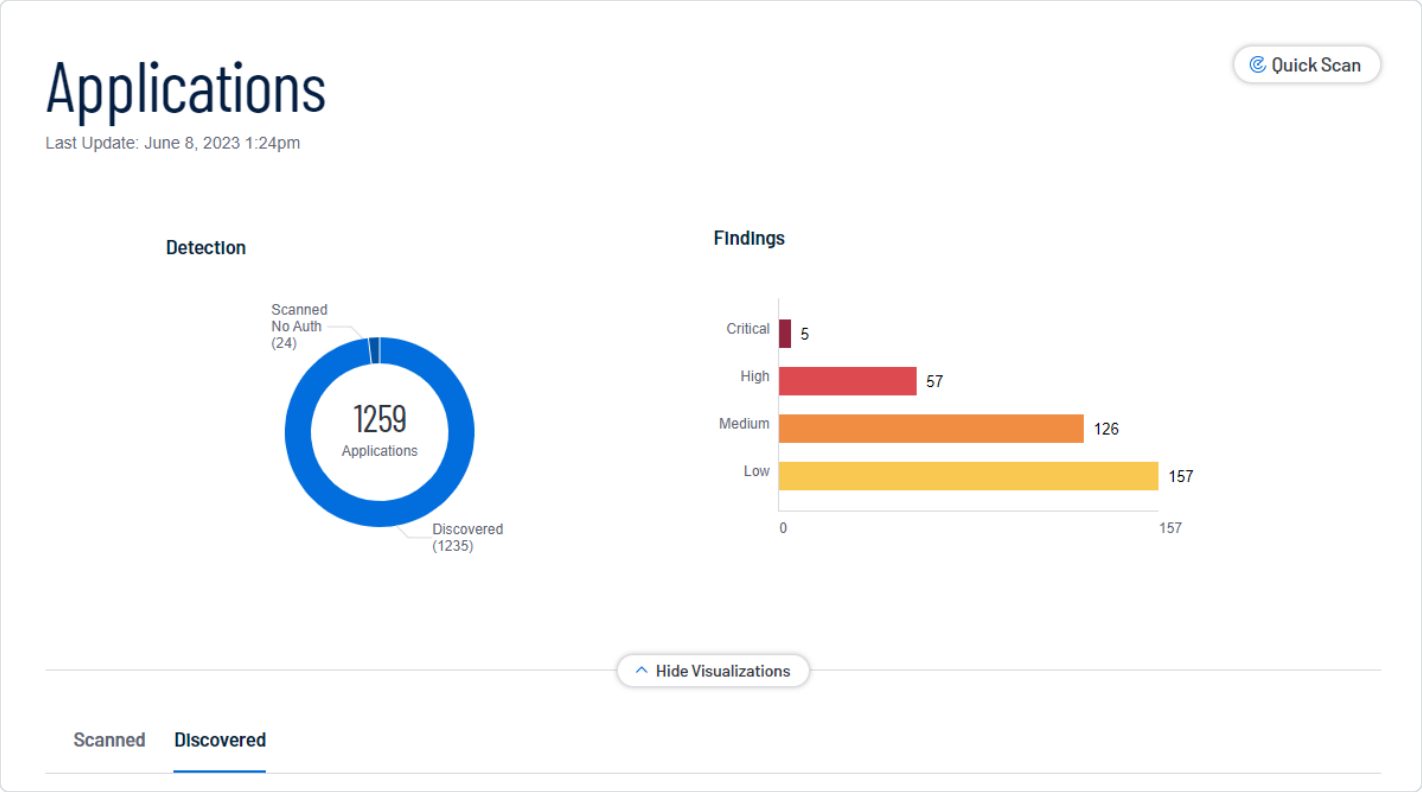
次の表では、スキャン済みアプリケーションに関する基本情報を確認できます。

フィルター	説明
ACR	(Tenable Lumin のライセンスが必要) 資産の ACR。
AES	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES の AES カテゴリ。
資産 ID	資産の UUID。
最終認証スキャン日	資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。
最終ライセンススキャン日	資産にライセンスがあると識別された直近のスキャン日時。ライセンスのある資産に関する詳細は、ライセンス情報 を参照してください。
最終スキャン日	スキャンの際に資産が最後に確認された日時。
ライセンス済み	資産が Tenable Web App Scanning インスタンスの資産カウントに含まれるかどうかを規定します。
名前	特定の資産属性の存在に基づいて Tenable Web App Scanning によって次の順序で割り当てられる資産識別子です。 1. エージェント名 (エージェントスキャンの場合) 2. NetBIOS 名 3. FQDN

	4. IPv6 アドレス 5. IPv4 アドレス たとえばスキャンによって、ある資産に対して NetBIOS 名と IPv4 アドレスが特定された場合、NetBIOS 名が資産名として表示されます。
オペレーティングシステム	スキャンにより資産にインストールされていると特定されたオペレーティングシステム。
SSL/TLS	資産がホストされているアプリケーションが SSL/TLS 公開鍵暗号化を使用するかどうかを指定します。
タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。

検出済みアプリケーション

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか



[アプリケーション] ページでドリルダウンすると、**検出済み**のアプリケーションだけを表示できます。

検出済みアプリケーションを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[アプリケーション]** をクリックします。

   [アプリケーション] ページが表示されます。デフォルトでは、**[スキャン済み]** タブが表示され、アプリケーションがビジュアル化されて表示されます。

3. 左下の**[検出済み]** をクリックします。

   検出済みのアプリケーションのリストが表示されます。

4. 検出済みアプリケーション資産の表で ⋮ ボタンをクリックすると、次のアクションのいずれかまたはすべてを実行できます。

   - スキャンを作成する
   - 検出結果にタグを追加する
   - 検出結果からタグを削除する
   - リストから検出結果を削除する

次の表では、検出済みアプリケーションに関する基本情報を確認できます。

列	説明
資産 ID	スキャンで脆弱性が検出された資産の UUID。この値は Tenable Web App Scanning に対して一意です。
名前	資産名。Tenable Web App Scanning はこの識別子に、特定の資産属性が存在するかに応じて、次の優先順位に基づいて資産属性を割り当てます。 1. エージェント名 (エージェントスキャンの場合) 2. NetBIOS 名 3. FQDN 4. IPv6 アドレス 5. IPv4 アドレス たとえばスキャンによって、ある資産に対して NetBIOS 名と IPv4 アドレスが特定された場合、NetBIOS 名が資産名として表示されます。 この列はデフォルトで表に表示されます。
ホスト名	資産のホスト名。
レコードタイプ	資産のタイプ。
レコード値	資産の値。
ドメイン	資産のドメイン名。

DNS (FQDN)	資産ホストの完全修飾ドメイン名。
IP アドレス	資産の IP アドレス(存在する場合)。
ホスティングプロバイダー	資産のホスティングプロバイダー。
ASN	資産の自律システム番号 (ASN)。
ライセンス済み	資産が Tenable Web App Scanning の資産カウントに含まれるかどうかを規定します。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
更新日	ユーザーが資産を最後に更新した日時。
ポート	資産に関連付けられているポート。
アクション	資産で実行できるアクション。

アプリケーション資産のエクスポート

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[アプリケーション] ページで、資産を.csv または .json 形式でエクスポートできます。作成する資産エクスポートをカスタマイズできます。エクスポートをスケジュールし、特定のメールアドレスに送信し、期限切れを設定できます。

注意: ドメインインベントリ資産はエクスポートできません。

アプリケーションページからアプリケーション資産をエクスポートする

[アプリケーション] ページから資産をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[アプリケーション]** をクリックします。

   [アプリケーション] ページが表示されます。

3. 左側で、エクスポートする資産の横にあるチェックボックスを選択します。最大 200 個の資産を選択できます。200 個を超える資産をエクスポートする必要がある場合は、すべての資産を選択してください。

   表の上部にアクションバーが表示されます。

4. アクションバーで、[→ **[エクスポート]** をクリックします。

   [エクスポート] ウィンドウが表示されます。

5. (オプション) 検出結果の行の ⋮ ボタンをクリックします。

   [エクスポート] ウィンドウが表示されます。

6. **[エクスポート]** ウィンドウで次の設定を行います。

a. (オプション) **[名前]** ボックスにエクスポートの名前を入力します。

b. **[フォーマット]** セクションで、使用するエクスポート形式をクリックします。

形式	説明
.csv	資産のリストを含む .csv ファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
.json	ネストされた資産のリストを含む .json ファイル。Tenable Web App Scanning は .json ファイルに空のフィールドを含めません。

c. (オプション) **[設定]** セクションで、含めるフィールドの横のチェックボックスを選択します。選択されたフィールドのみを表示するには、**[選択したフィールドを表示]** をクリックします。

注意: これらのフィールド選択を変更すると、Tenable Web App Scanning は次回 **[資産]** ページからエクスポートするときに、変更したフィールドをデフォルトとして保持します。

d. (オプション) **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

7. (オプション) **[スケジュール]** トグルをオンにして、エクスポートのスケジュールを設定します。

a. **[開始日時]** セクションで、エクスポートスケジュールの開始日時を選択します。

注意: 特定の日付を指定しないフィルターを使用してエクスポートをスケジュールした場合、それらのフィルターは時間の経過とともにエクスポートを更新します。たとえば、**[最終確認日]** が 2023 年 3 月 15 日 **よりも後**である資産のエクスポートをスケジュールすると、Tenable Web App Scanning では、さらに資産が検出されるたびにエクスポートカウントが増加します。

b. **[タイムゾーン]** ドロップダウンボックスで、タイムゾーンを選択します。

c. **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。

d. **[繰り返し終了]** ドロップダウンボックスで、スケジュールを終了する日付を選択します。**[なし]** を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

8. (オプション) エクスポートの完了時にメール通知を送信するには、**[E メール通知]** トグルをオンにします。

   a. **[受信者の追加]** ボックスに、通知を送信するメールアドレスを入力します。

   b. **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有します。

9. **[エクスポート]** をクリックします。

   エクスポートのサイズによっては、Tenable Web App Scanning によるエクスポートの処理が完了するまでに数分かかる場合があります。処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。

   > ダウンロードが完了する前に **[エクスポート]** ウィンドウを閉じた場合は、**[設定]** > **[エクスポート]** でファイルにアクセスできます。

アプリケーションの詳細ページから資産をエクスポートする

[アプリケーションの詳細] ページから資産をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションウィンドウで、**[アプリケーション]** をクリックします。

   [アプリケーション] ページが表示されます。

3. エクスポートするアプリケーション資産をクリックします。

4. 右上にある **[エクスポート]** をクリックします。

   [エクスポート] ウィンドウが表示されます。

5. **[エクスポート]** ウィンドウで次の情報を追加します。

   a. (オプション) **[名前]** ボックスにエクスポートの名前を入力します。

   b. **[フォーマット]** セクションで、使用するエクスポート形式をクリックします。

形式	説明
.csv	資産のリストを含む .csv ファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
.json	ネストされた資産のリストを含む .json ファイル。Tenable Web App Scanning は .json ファイルに空のフィールドを含めません。

c. (オプション) **[設定]** セクションで、含めるフィールドの横のチェックボックスを選択します。選択されたフィールドのみを表示するには、**[選択したフィールドを表示]** をクリックします。

注意: これらのフィールド選択を変更すると、Tenable Web App Scanning は次回 **[資産]** ページからエクスポートするときに、変更したフィールドをデフォルトとして保持します。

d. (オプション) **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

6. (オプション) **[スケジュール]** トグルをオンにして、エクスポートのスケジュールを設定します。

a. **[開始日時]** セクションで、エクスポートスケジュールの開始日時を選択します。

注意: 特定の日付を指定しないフィルターを使用してエクスポートをスケジュールした場合、それらのフィルターは時間の経過とともにエクスポートを更新します。たとえば、**[最終確認日]** が 2023 年 3 月 15 日**よりも後**である資産のエクスポートをスケジュールすると、Tenable Web App Scanning では、さらに資産が検出されるたびにエクスポートカウントが増加します。

b. **[タイムゾーン]** ドロップダウンボックスで、タイムゾーンを選択します。

c. **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。

d. **[繰り返し終了]** ドロップダウンボックスで、スケジュールを終了する日付を選択します。**[なし]** を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

7. (オプション) エクスポートの完了時にメール通知を送信するには、**[E メール通知]** トグルをオンにします。

a. **[受信者の追加]** ボックスに、通知を送信するメールアドレスを入力します。

b. **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有します。

8. **[エクスポート]** をクリックします。

Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ダウンロードが完了する前に **[エクスポート]** ウィンドウを閉じた場合は、**[設定]** > **[エクスポート]** でファイルにアクセスできます。

> **注意:** **[詳細]** ページの **[検出結果]** タブから、資産に関するすべての検出結果をエクスポートできます。詳細は、検出結果のエクスポートを参照してください。

資産の削除

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

資産を削除すると、Tenable Web App Scanning は資産の表のデフォルトビューから資産を削除し、資産に関連付けられた脆弱性データを削除し、スキャン結果と資産の照合を停止します。

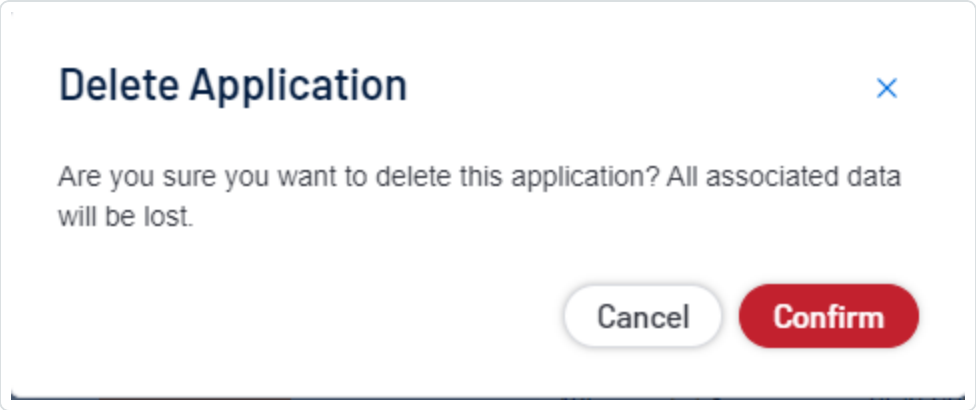
1 つの資産を削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 次のいずれかを行います。

場所	アクション
[資産] ページ	a. 資産の表を表示します。 b. 資産表の削除する資産の行で、⋮ ボタンをクリックします。 メニューが表示されます。 c. 🗑 **[削除]** をクリックします。 確認ウィンドウが表示されます。
[資産の詳細] ページ	a. 資産の詳細を表示します。 b. 右上で🗑 **[削除]** をクリックします。 確認ウィンドウが表示されます。



3. 確認ウィンドウで、**[削除]**をクリックします。

   Tenable Web App Scanning により資産が削除されます。

複数の資産を削除する方法

注意: Tenable Web App Scanningでは、**アプリケーション**の表で一度に削除できるアプリケーションのレコード数は 1,000 に制限されています。(個別に選択してまたは**[すべてのアプリケーションを選択する]**機能を使って) 上限の 1,000 を超えるレコードを選択した場合は、アクションボタンが表のツールバーに表示されます。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 次のいずれかを行います。

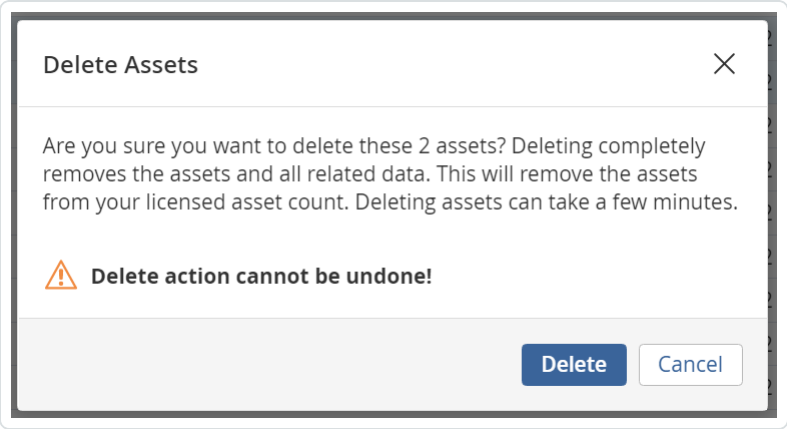
   - スキャン済みアプリケーションを表示します。
   - 検出済みアプリケーションを表示します。

3. 資産の表で、削除する各アプリケーションの横にあるチェックボックスをクリックします。

   ページの下部またはテーブルの上部に、アクションバーが表示されます。

4. アクションバーで、🗑 **[削除]**ボタンをクリックします。

   確認ウィンドウが表示されます。]



5. 確認ウィンドウで、**[削除]**をクリックします。

   Tenable Web App Scanning により、選択された資産が削除されます。

アプリケーションフィルター検索

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[アプリケーション]セクションの**[スキャン済み]**と**[検出済み]**ページで、所属組織のアプリケーションと検出結果をフィルタリングすることができます。使用できるフィルターの一覧については、Discovered ApplicationsまたはScanned Applicationsを参照してください。

パフォーマンスを最適化するために、Tenable では、適用できる検出結果フィルターの数を 18 に、適用できる資産フィルターの数を 35 に制限しています。

[アプリケーション]セクションで表をフィルタリングする方法

1. 左上にある ☰ ボタンをクリックします。

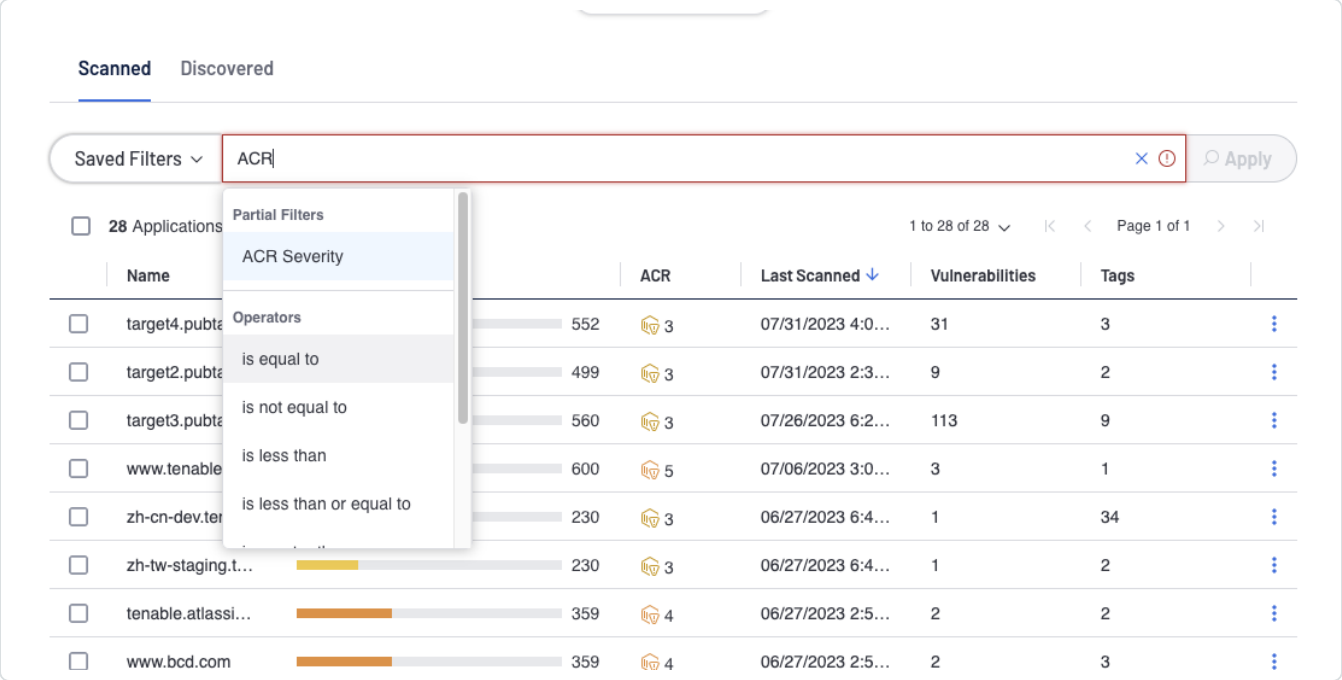
   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[アプリケーション]**をクリックします。

   [アプリケーション]ページが表示されます。デフォルトでは、**[スキャン済み]**タブが表示され、アプリケーションのビジュアライゼーションが表示されます。

3. アプリケーションリストの上にある検索ボックスを**クリック**します。

次の画像に示すように、現在のフィルターを示すドロップダウンボックスが表示されます。



ヒント: 矢印キーを使用してフィルタードロップダウンボックス内を移動し、**Enter** キーを押してオプションを選択できます。

4. ドロップダウンボックスで、**AND** または **OR** 条件を選択するか、またはテキストボックスに条件を入力します。
5. ドロップダウンボックスで、フィルターを選択するか、またはテキストボックスにフィルター名を入力します。
6. ドロップダウンボックスで、次に示す演算子のいずれかを選択するか、またはテキストボックスに演算子を入力します。

注意: (') または (") で始まる値や (*) または (,) を含む値でフィルタリングする場合は、値を引用符 (") で囲む必要があります。

注意: フィルターは、最大で 2 つのネストレベルを持つことができます。

演算子	説明
存在す	選択されたフィルターが存在するアイテムを表示します。

演算子	説明
る	
存在しない	選択されたフィルターが存在しないアイテムを表示します。
次の値に等しい	フィルター値に一致するアイテムを表示します。
次の値に等しくない	フィルター値を含まないアイテムを表示します。
次の値より大きい **次の値以上**	指定されたフィルター値より大きい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以上]** 演算子を使用します。
次の値より小さい **次の値以下**	指定されたフィルター値より小さい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以下]** 演算子を使用します。
直近	今日より前の数時間、数日、数か月、または数年以内の日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
後	指定されたフィルター値より後の日付のアイテムを表示します。
前	指定されたフィルター値より前の日付のアイテムを表示します。
経過	今日より前の数時間、数日、数か月、または数年が経過した日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
日付	指定された日付のアイテムを表示します。

演算子	説明
期間	指定された 2 つの日付間のアイテムを表示します。
次の値を含む:	指定されたフィルター値を含むアイテムを表示します。
次の値を含まない:	指定されたフィルター値を含まないアイテムを表示します。
ワイルドカード	次のように、ワイルドカード (*) でアイテムを絞り込みます。 • **次で始まるまたは終わる** - 指定したテキストで始まるまたは終わる値を表示します。たとえば、「1」で始まるすべての値を見つけるには、*1** と入力します。「1」で終わるすべての値を見つけるには、**1* と入力します。 • **次の値を含む** - 指定したテキストを含む値を表示します。たとえば、最初と最後の文字の間のどこかに「1」があるすべての値を見つける場合は、**1** と入力します。 • **大文字と小文字の区別をオフにする** – 大文字と小文字を区別せずに値を表示します。たとえば、**プラグイン名** が「TLS バージョン 1.2 プロトコル検出」または「tls バージョン 1.2 プロトコル検出」である検出結果を検索するには、**tls バージョン 1.2 プロトコル検出* と入力します。

7. ドロップダウンボックスで、フィルター値を選択するか、またはテキストボックスにフィルター値を入力します。

> **ヒント:** 一部のテキストフィルターは、フィルター値内のテキストのセクションを表すワイルドカードとして文字 (*) をサポートしています。たとえば、フィルターして 1 で終わるすべての値を表示する場合は、**1* と入力します。フィルターして 1 で始まるすべての値を表示する場合は、*1* と入力します。
>
> このワイルドカード演算子を使用して、特定のテキストを含む値を表示するようにフィルタリングできます。たとえば、最初と最後の文字の間のどこかに 1 があるすべての値を表示するようにフィルターを掛ける場合は、**1** と入力します。

8. (オプション) フィルターを追加または削除するには、次のいずれかを実行します。

- 複数のフィルターを追加するには、**Space** キーを押してから、別の条件、演算子、フィルター、値を選択します。
- 1 つのフィルターを削除するには、フィルターの右側にある ✕ ボタンをクリックします。
- すべてのフィルターを削除するには、テキストボックスの右隅にある ✕ ボタンをクリックします。

9. **[適用]** をクリックします。

   Tenable Web App Scanning がデータをフィルタリングします。

10. (オプション) フィルターを保存して、後でアクセスしたり、チームの他のメンバーと共有したりします。

> **ヒント**: Tenable Web App Scanning では検出結果の検索がバックグラウンドで実行されるので、ユーザーは **[検出結果]** ページから他のページに移動し、複雑な検索の完了後にページに戻ってくることができます。検索を**キャンセル**することもできます。さらに、Tenable Web App Scanning は、直近検索の 30 分間のキャッシュ、トップツールバーへの日時表記、次回のアクセス用に **[検出結果]** ページの状態保存も行います。

アプリケーションの詳細の表示

必要な追加ライセンス: Tenable Web App Scanning

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

特定の資産の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[アプリケーション]** をクリックします。

   [資産] ページが表示されます。デフォルトでは、**[スキャン済み]** タブが表示されます。

3. (オプション) 表データを選別します。

4. アプリケーションの表で、詳細を表示するアプリケーションの行をクリックします。

   [アプリケーションの詳細] ページが表示されます。

Tenable Web App Scanning の検出結果

必要な追加ライセンス: Tenable Web App Scanning

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[検出結果] ページには、企業の脆弱性に関する検出結果と、Tenable Web App Scanning が検出結果を特定したアプリケーションに関するインサイトが表示されます。検出結果は、アプリケーション上に表示される脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。

[検出結果] ページには、識別されたウェブアプリケーションの検出結果が検出結果のタイプ別に整理されたリストビューが含まれています。ドリルダウンして、次のいずれかの検出結果タイプの検出結果を表示できます。**[検出結果]** ページでドリルダウンすると、ウェブアプリケーションの脆弱性に対する脆弱性検出結果のみを表示できます。

注意: Tenable は、15 か月間のみ検出結果データを保持します。

ウェブアプリケーションの脆弱性検出結果を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[検出結果]** をクリックします。

   [検出結果] ページが表示され、検出結果を示す表が表示されます。

3. 検出結果の表では、⋮ ボタンをクリックすることで次のアクションのいずれかまたはすべてを実行できます。

   - 検出結果を承認する
   - 検出結果をエクスポートする
   - 選択したタイプのすべての検出結果を表示する

次の表では、ウェブアプリケーションの脆弱性検出結果に関する基本情報を確認できます。

列	説明

アプリケーション名	スキャナーで脆弱性が検出されたアプリケーションの名前です。この値は Tenable Web App Scanning に対して一意です。 このフィルターは、デフォルトでフィルタープレーンに表示されます。
深刻度	CVSS に基づく脆弱性の深刻度。詳細は、CVSS vs. VPR を参照してください。 この列はデフォルトで表に表示されます。
名前	検出結果で検出された脆弱性を特定したプラグインの名前です。 この列はデフォルトで表に表示されます。
プラグイン ID	検出結果で検出された脆弱性を特定したプラグインの ID。 この列はデフォルトで表に表示されます。
ファミリー	脆弱性を特定したプラグインのファミリー。 この列はデフォルトで表に表示されます。
状態	脆弱性の状態です。 この列はデフォルトで表に表示されます。
最終更新日	スキャンがアプリケーション上で脆弱性を検出した直近の日付 この列はデフォルトで表に表示されます。
ID	スキャンで脆弱性が検出されたアプリケーションの UUID。この値は Tenable Web App Scanning に対して一意です。
初回確認日	スキャンがアプリケーション上で脆弱性を検出した最初の日付。

検出結果の詳細の表示

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[検出結果] ページで Tenable Web App Scanning の脆弱性検出結果をクリックすると、その検出結果に関する基本的な詳細がプレビューパネルに表示されます。

特定の検出結果の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[検出結果]** をクリックします。

   [検出結果] ページが表示され、検出結果を示す表が表示されます。

3. 検出結果の表で、詳細を表示する検出結果の行をクリックします。

   [検出結果の詳細] ページが表示されます。

4. (オプション) 右上の **[深刻度が情報を含む]** をオンにして、情報レベルの深刻度の結果を一覧表示します。このオプションはデフォルトでオフになっています。深刻度レベルの詳細については、脆弱性の深刻度インジケーターを参照してください。

次の表は、各オプションに表示される情報を示しています。

セクション	説明
説明	検出結果で検出された脆弱性を特定した Tenable プラグインの説明です。
ソリューション	検出結果で検出された脆弱性を修正する方法に関する概要です。公式のソリューションが使用可能な場合にのみ表示されます。
その他の関連項目	検出結果で検出された脆弱性についての役立つ情報を含む外部ウェブサイトへのリンクです。
脆弱性プロパティ	プラグインが特定した脆弱性に関する情報です。次のものが含まれます。 • **深刻度** - 脆弱性の深刻度。 • **悪用される可能性** - 脆弱性の潜在的な悪用可能性において考慮される、脆

	弱性の特性 • **悪用される** - 脆弱性が悪用される可能性のある特に一般的な方法。 • **脆弱性の公開日** - 脆弱性の定義が最初に公開された日付 (たとえば、CVE が公開された日付)。 • **パッチ公開日** - ベンダーがその脆弱性に対してのパッチを公開した日付。
検出	Tenable Web App Scanning が脆弱性を最初に検出した時に関する情報。次の情報が含まれます。 • **初回確認日** - スキャンがアプリケーション上で脆弱性を検出した最初の日付 • **最終確認日** - スキャンがアプリケーション上で脆弱性を検出した直近の日付 • **経過日数** - ネットワーク内のアプリケーション上で、スキャンによって脆弱性が最初に検出されてから経過した日数
プラグインの詳細	検出結果で検出された脆弱性を検出したプラグインに関する情報で、次のものが含まれます。 • **プラグイン ID** - 検出結果で検出された脆弱性を特定したプラグインの ID。 • **公開日** - 脆弱性を特定したプラグインが公開された日付 • **変更日** - プラグインが変更された直近の日付。 • **ファミリー** - 脆弱性を特定したプラグインのファミリー • **深刻度** - 脆弱性を特定したプラグインの深刻度
リスク情報	影響を受けている資産に脆弱性が与える相対リスクに関する情報で、次のものが含まれます。 • **リスクファクター** - プラグインに関連する CVSS に基づくリスク要因 • **修正されたリスク** - プラグインのリスクを修正するために適用されたアクション [許容] または [変更] を示します • **CVSS3 基本スコア** - CVSSv3 基本スコア (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性) • **CVSS3 攻撃元区分** - 脆弱性に関する追加の CVSSv3 メトリクス

	• **CVSS2 基本スコア** - CVSSv2 基本スコア(時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性) • **CVSS2 攻撃元区分** - 脆弱性に関する追加の CVSSv2 メトリクス
参照情報	プラグインに関連する脆弱性、エクスプロイト、または更新情報に関するサードパーティ情報への参照の一覧です。

検出結果のエクスポート

[検出結果] ページでは、検出結果を .csv または json 形式でエクスポートできます。作成するエクスポートをカスタマイズできます。エクスポートをスケジュールし、特定のメールアドレスに送信し、期限切れを設定できます。

[検出結果] ページから検出結果をエクスポートする

[検出結果] ページから検出結果をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[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。

3. 左側で、エクスポートする検出結果の横にあるチェックボックスを選択します。最大 200 件の検出結果を選択できます。200 件を超える結果をエクスポートする必要がある場合は、すべての結果を選択してください。

   オプションのドロップダウンボックスが表示されます。

4. ドロップダウンボックスで [→ **[エクスポート]** をクリックします。

   [エクスポート] プレーンが表示されます。

5. **[エクスポート]** プレーンで次の設定を指定します。

   a. (オプション) **[名前]** ボックスにエクスポートの名前を入力します。

   b. **[フォーマット]** セクションで、使用するエクスポート形式をクリックします。

形式	説明
.csv	検出結果のリストを含む .csv ファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してく

	ださい。
.json	ネストされた検出結果のリストを含む .json ファイル。Tenable Vulnerability Management は .json ファイルに空のフィールドを含めません。

c. (オプション) **[設定]** セクションで、エクスポートに含めるフィールドの横のチェックボックスを選択します。選択されたフィールドのみを表示するには、**[選択したフィールドを表示]** をクリックします。

注意: これらのフィールド選択を変更すると、Tenable Web App Scanning は選択内容をデフォルトとして保持し、次回に **[検出結果]** ページからエクスポートするときに適用します。

d. (オプション) **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

6. (オプション) **[スケジュール]** トグルをオンにして、エクスポートのスケジュールを設定します。

a. **[開始日時]** セクションで、エクスポートスケジュールの開始日時を選択します。

b. **[タイムゾーン]** ドロップダウンボックスで、タイムゾーンを選択します。

c. **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。

d. **[繰り返し終了]** ドロップダウンボックスで、スケジュールを終了する日付を選択します。**[なし]** を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

7. (オプション) エクスポートの完了時にメール通知を送信するには、**[E メール通知]** トグルをオンにします。

a. **[受信者の追加]** ボックスに、通知を送信するメールアドレスを入力します。

b. **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有します。

8. **[エクスポート]** をクリックします。

エクスポートのサイズによっては、Tenable Web App Scanning によるエクスポートの処理が完了するまでに数分かかる場合があります。処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。

ダウンロードが完了する前に**[エクスポート]**プレーンを閉じた場合は、**[設定]** > **[エクスポート]**でエクスポートファイルにアクセスできます。

[検出結果の詳細]ページから検出結果をエクスポートする

[検出結果の詳細]ページから検出結果をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで**[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。

3. 行にある[検出結果]をクリックします。

   [検出結果の詳細]ページが表示されます。

4. 一番上の行で [→ **[エクスポート]**をクリックします。

   [エクスポート]プレーンが表示されます。

5. **[エクスポート]**プレーンで次の情報を追加します。

   a. (オプション)**[名前]**ボックスにエクスポートの名前を入力します。

   b. **[フォーマット]**セクションで、使用するエクスポート形式をクリックします。

形式	説明
.csv	検出結果のリストを含む.csvファイル。 **注意:** .csvエクスポートファイルに=、+、-、@のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Managementはセルの先頭に単一引用符(')を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
.json	ネストされた検出結果のリストを含む.jsonファイル。Tenable Web App Scanningは.jsonファイルに空のフィールドを含めません。

c. (オプション) **[設定]** セクションで、含めるフィールドの横のチェックボックスを選択します。選択されたフィールドのみを表示するには、**[選択したフィールドを表示]** をクリックします。

> **注意:** これらのフィールド選択を変更すると、次回に **[検出結果]** ページからエクスポートするとき、Tenable Web App Scanning はその選択内容をデフォルトとして保持します。

d. (オプション) **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

6. (オプション) **[スケジュール]** トグルをオンにして、エクスポートのスケジュールを設定します。

a. **[開始日時]** セクションで、エクスポートスケジュールの開始日時を選択します。

b. **[タイムゾーン]** ドロップダウンボックスで、タイムゾーンを選択します。

c. **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。

d. **[繰り返し終了]** ドロップダウンボックスで、スケジュールを終了する日付を選択します。**[なし]** を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

7. (オプション) エクスポートの完了時にメール通知を送信するには、**[E メール通知]** トグルをオンにします。

a. **[受信者の追加]** ボックスに、通知を送信するメールアドレスを入力します。

b. **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有します。

8. **[エクスポート]** をクリックします。

Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ダウンロードが完了する前に **[エクスポート]** プレーンを閉じた場合は、**[設定]** > **[エクスポート]** でエクスポートファイルにアクセスできます。

Tenable Web App Scanning 検出結果からのレポートの生成

[検出結果] ページから、1 つ以上の脆弱性に関するレポートを生成することができます。

[検出結果] ページからレポートを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[検出結果]** をクリックします。

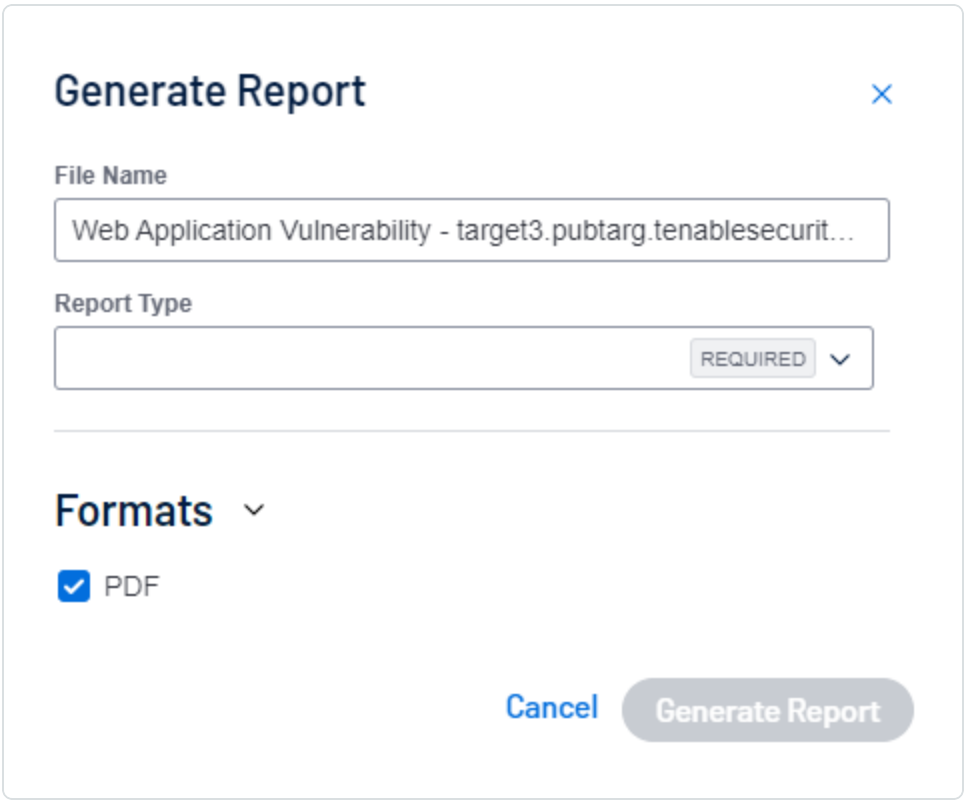
   [検出結果] ページが表示されます。

3. 行にある ⋮ ボタ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。

4. ドロップダウンボックスで [→ **[レポートを生成]** をクリックします。

   [レポートを生成] プレーンが表示されます。



5. レポートを作成する検出結果を選択します。

範囲	アクション
1 つの脆弱性のレポートを作成する	次のいずれかを行います。 • **[アクション]** 列で、レポートを作成する脆弱性の行にある ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。
複数の脆弱性のレポートを作成する	次のいずれかを行います。 • レポートを作成する脆弱性を複数選択します。すべての脆弱性を選択するには、リストの一番上にあるチェックボックスを選択します。 Tenable Web App Scanning のアクションバーが有効になります。

6. **[レポートを生成]** をクリックします。

   [レポートを生成] ポップアップが表示されます。

7. (オプション) **[名前]** ボックスに、レポートの新しい名前を入力します。

8. **[レポートタイプ]** ドロップダウンボックスから、レポートを選択します。

レポートタイプ
Web App Scanning エグゼクティブ検出結果レポート
Web App Scanning 脆弱性検出の資産別詳細レポート
Web App Scanning 脆弱性検出のプラグイン別詳細レポート

9. (オプション) **[スケジュール]** トグルをクリックして、レポートのスケジュール設定を有効にします。

   レポートをスケジュールするためのフィールドが表示されます。

   - レポートをスケジュールするには、次の設定を変更します。
     - **[開始日時]** ボックスで、レポートをスケジュールするタイミングを選択します。デフォルトは現在の日付と時刻です。

- **[タイムゾーン]** ボックスで、必要なタイムゾーンを選択するか、デフォルトのタイムゾーンをそのまま使用します。
- **[繰り返し]** ドロップダウンボックスで、レポート生成の頻度を **[毎日]**、**[毎週]**、**[毎月]**、**[カスタム]**、または **[繰り返さない]** から選択します。デフォルトは **[毎日]** です。
- **[繰り返し終了]** ドロップダウンボックスで、スケジュールを終了する日付 (**[日付を指定]** または **[なし]**) を選択します。**[日付を指定]** を選択した場合は、レポートスケジュールを終了する日付を **[終了日]** ボックスに指定します。
- **[受信者の追加]** ボックスに、レポートの送信先の受信者のメールアドレスを入力します。

- **[レポートをスケジュール]** をクリックします。

  Tenable Web App Scanning がレポートをスケジュールし、確認メッセージを表示します。

10. **[レポートを生成]** をクリックします。

    Tenable Web App Scanning がレポートを生成します。通知メッセージの **[レポート結果]** リンクをクリックすると、**[レポート結果]** ページで新しいレポートが表示されます。新しいレポートは強調表示されています。

修正スキャンの起動

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[検出結果] ページまたは **[検出結果の詳細]** ページで、既存のスキャン結果に対するフォローアップスキャンを実行する修正スキャンを作成することができます。修正スキャンを使用して、スキャンターゲット上の脆弱性の修正アクションが成功したかどうかを検証することができます。以前に脆弱性が特定されたターゲット上の脆弱性を修正スキャンで特定できない場合、システムはその脆弱性のステータスを **[修正済み]** に変更します。

Tenable Web App Scanning インターフェースで修正スキャンを起動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[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。

3. 行にある ⋮ ボタ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。

4. ドロップダウンボックスで、 **[修正スキャンの起動]** をクリックします。

   [修正スキャンの作成] 設定ページが表示されます。

   (オプション) 選択した検出結果の **[検出結果の詳細]** にある **[修正スキャンの起動]** ボタンを使用することもできます。

   注意: 元のスキャン設定がマルチターゲットスキャン用であった場合、Tenable は修正対象の正しいターゲットを見極めようとしますが、Tenable では、ユーザーがターゲットをダブルチェックし、確定することを推奨しています。

   注意: 設定ページには、次の 3 つの事項を除き、元のスキャンの作成に使用したのと同じスキャンテンプレート設定が表示されます。**[クロールスクリプト]** の下にファイルが作成され、修正スキャンプロセスに使用されます。**[評価]** の **[監査する要素]** セクションには、プラグインの修正対象の要素が表示されます。プラグインと関連する依存関係のみが有効になるため、設定さ

れるプラグインも異なります。

5. (オプション) スキャン情報を入力します。
6. **[保存]** をクリックしてスキャン設定を保存するか、**[保存して実行]** をクリックしてスキャンを起動します。

   注意:「修正の対象となる脆弱性のページを複製できませんでした」という注記が付いたエラーが表示される場合があります。このスキャンの注記は、スキャナーが脆弱性データに表示されたページを複製できなかったことを示しています。この脆弱性を修正するには、元のスキャンを再実行してみてください。

   Tenable Web App Scanning がスキャンを起動します。

次の手順

- **[スキャン]** ページの **[修正スキャン]** フォルダーで次のいずれかを実行します。
  - スキャン設定を編集する。
  - スキャンを起動する。
- スキャンが完了したら次の操作を実行します
  a. **[スキャン]** ページの **[修正スキャン]** フォルダーで次の操作を実行します。
     - 完了した修正スキャンに検出結果が表示されていないことを確認するために、クリックして検出結果のリストを確認します。

  b. **[検出結果]** ページで次の操作を実行します。
     - 修正スキャンのターゲットとなった資産上で選択した脆弱性のステータスが **[修正済み]** になったことを確認します。

修正スキャンプラグインの考慮事項

修正スキャンでサポートされていないプラグインのタイプや、フルスキャン修正のみのプラグインタイプがあります。次の表にそれらを一覧表示しています。

修正で使用できないプラグインのリスト

これらのプラグインは、修正スキャンをしても意味がないか、現在サポートされていません。

プラグイン名	プラグイン番号
OpenAPI インポートに成功しました	112569
OpenAPI インポートに失敗しました	112570
許可されている HTTP バージョン	112613
API が検出されました	112616
セッション Cookie が検出されました	112798
API キー認証に成功しました	113010
API キー認証に失敗しました	113011
OpenAPI インポートに失敗しました	112570
許可されている HTTP バージョン	112613
API が検出されました	112616
セッション Cookie が検出されました	112798
API キー認証に成功しました	113010
API キー認証に失敗しました	113011
OpenAPI インポートに失敗しました	112570
許可されている HTTP バージョン	112613
API が検出されました	112616

セッション Cookie が検出されました	112798
API キー認証に成功しました	113010
ベアラートークンの認証に成功しました	113012
ベアラートークンの認証に失敗しました	113013
Basic 認証が検出されました	113063
Kerberos 認証に成功しました	113224
Kerberos 認証に失敗しました	113225
クライアント証明書認証に成功しました	113329
クライアント証明書認証に失敗しました	113330
パフォーマンステレメトリ	113393
SOAP API が検出されました	114166
gRPC が検出されました	114167
Amazon Web Service が検出されました	114199
Google Cloud Platform が検出されました	114200
Microsoft Azure が検出されました	114201
Microsoft Entra ID が検出されました	114202
GraphQL のバッチ処理	114211
HTTP/2 平文アップグレードサポートが検出されました	114219
シリアル化されたデータが検出されました	114224
スキャンの情報	98000
除外ルールにより URI がブロックされました	98007
ウェブアプリケーションファイヤーウォールが検出されました	98008
ウェブアプリケーションサイトマップ	98009

ネットワークタイムアウトが発生しました	98019
HTTP サーバー認証が検出されました	98024
HTTP サーバー認証に成功しました	98025
HTTP サーバー認証に失敗しました	98026
ログインフォーム認証に失敗しました	98034
ログインフォーム認証に成功しました	98035
スキャンが断続的にログアウトしています	98043
ログアウト後にスキャンが中止されました	98044
許可された HTTP メソッド	98047
興味深い応答	98050
検出されたテクノロジー	98059
Cookie が収集されました	98061
DOM 要素が除外されました	98111
ターゲット情報	98136
タイムアウト回数が多すぎてスキャンが中止されました	98137
スクリーンショット	98138
Cookie 認証に成功しました	98139
Cookie 認証に失敗しました	98140
Selenium 認証に成功しました	98141
Selenium 認証に失敗しました	98142
Selenium クロールに成功しました	98143
Selenium クロールに失敗しました	98145
外部 URL	98154

エラーメッセージ	98611
HTTPS を使用しない Basic 認証	98615
Fetch/XHR が検出されました	98772

フルスキャン修正プラグイン

特定の脆弱性ページは複製されず、これらのプラグインに対してアプリケーションのフルクロールが実行されます。この形式の修正スキャンの実行は、より長い時間がかかる場合があります。

プラグイン番号	プラグイン名
HTTP から HTTPS へのリダイレクトが有効になっていません	112544
フルパス開示	112550
JSON ウェブトークンの弱いシークレット	112697
API バージョンが検出されました	112714
Microsoft FrontPage の安全でない拡張機能の設定	112772
GraphQL が検出されました	112809
GraphQL Introspection が有効化されました	112894
GraphQL フィールド提案が検出されました	112895
Power Apps OData フィードが検出されました	112949
Magento 管理パネルのログインフォームがブルートフォース攻撃を受けました	113117
Magento 接続マネージャーがブルートフォース攻撃を受けました	113118
Joomla 管理パネルのログインフォームがブルートフォース攻撃を受けました	113133
Wordpress 管理パネルのログインフォームがブルートフォース攻撃を受けました	113136
Drupal 管理パネルのログインフォームがブルートフォース攻撃を受	113137

けました	
Weblogic コンソールのログインフォームがブルートフォース攻撃を受けました	113138
OpenAPI の暗号化されていないトラフィックが許可されています	113143
Google クラウドサービスアカウントの秘密鍵の開示	113150
AWS 認証情報の開示	113164
Apache mod_negotiation の代替ファイル名の開示	113165
蓄積型クロスサイトスクリプティング (XSS)	113250
ログインフォームのクロスサイトリクエストフォージェリ	113332
ウェブキャッシュのポイズニング	113338
ASP.NET ViewState のリモートコードの実行	113340
Amazon Cognito のユーザー列挙	113371
Amazon Cognito の安全でないアクセス許可	113374
SQL ステートメントの開示	113555
外部バックエンド API が検出されました	114128
ベアラートークンの認証が検出されました	114136
NTLM 認証が検出されました	114137
Digest 認証が検出されました	114138
プライベート IP アドレスの開示	98077
メールアドレスの開示	98078
サブリソースの整合性の欠如	98647
無効なサブリソースの整合性	98649
ソースコードの受動的開示	98779

検出結果の変更ルールと許容ルールの作成

Tenable Web App Scanning では、脆弱性の検出結果に影響するルールを作成できます。変更ルールはホスト脆弱性またはウェブアプリケーションの検出結果の深刻度を変更し、許容ルールは、深刻度を変更せずに検出結果のリスクを許容します。このトピックでは、[検出結果] ページでルールを作成する方法について説明します。

注意: ルールが IP アドレスによって指定される場合、各ネットワーク上で見つかった指定の IP に対してそのルールが適用されます。詳細については、*Tenable Vulnerability Management ユーザーガイド*のネットワークを参照してください。

検出結果で変更ルールを作成する

変更ルールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[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。

3. ルールを作成する検出結果の行で ⋮ ボタ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。

4. **[変更]** をクリックします。

   [変更] プレーンが表示されます。

5. 次のオプションを指定します。

   a. **新しい深刻度** - 脆弱性に関する適切な深刻度レベルを選択します。

   b. **ターゲット** - **[すべて]** を選択してすべての資産をターゲットにするか、**[カスタム]** を選択してルールを実行するターゲットを指定します。

      注意: **[ターゲット]** ドロップダウンを **[すべて]** に設定した場合、このオプションにより既存のルールがオーバーライドされる可能性があることを知らせる警告が表示されます。

c. **ターゲットとなるホスト** - 必要に応じて、ルールの 1 つ以上のカスタムターゲットを入力します。IP アドレス、IP 範囲、CIDR、ホスト名の任意の組み合わせを含むコンマ区切りリストを入力できます。

> **注意**: 指定できるコンマ区切りカスタムエントリは 1000 個までとなっています。これよりも多くのカスタムエントリをターゲットにする場合は、複数のルールを作成してください。

d. (オプション) **有効期限日** - ルールが期限切れになる日付を選択します。

e. (オプション) **コメント** - ルールの説明を入力します。このオプションは、ルールが変更された場合にのみ表示されます。

6. **[保存]** をクリックします。

   Tenable Web App Scanning が既存の検出結果にルールを適用し始めます。システムの負荷と一致する検出結果の数によっては、このプロセスに時間がかかる場合があります。Tenable Web App Scanning はダッシュボードを更新し、影響を受けている検出結果のインスタンスがいくつ変更されたかを示すラベルが表示されます。

   > **注意:** 変更ルールによって、スキャンの履歴結果に影響が出ることはありません。

検出結果で許容ルールを作成する

[検出結果] ワークベンチから許容ルールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[検出結果]** をクリックします。

3. ルールを作成する検出結果の行で ⋮ ボタ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。

4. **[許容]** をクリックします。

   [リスクの許容] ウィンドウが表示されます。

5. 次のオプションを指定します。

a. **ターゲット** - **[すべて]** を選択してすべての資産をターゲットにするか、**[カスタム]** を選択してルールを実行するターゲットを指定します。

b. **ターゲットとなるホスト** - 必要に応じて、ルールの 1 つ以上のカスタムターゲットを入力します。IP アドレス、IP 範囲、CIDR、ホスト名の任意の組み合わせを含むコンマ区切りリストを入力できます。

> **注意**: 指定できるコンマ区切りカスタムエントリは 1000 個までとなっています。これよりも多くのカスタムエントリをターゲットにする場合は、複数のルールを作成してください。

c. (オプション) **有効期限日** - ルールが期限切れになる日付を選択します。

d. (オプション) **コメント** - ルールの説明を入力します。このオプションは、ルールが変更された場合にのみ表示されます。

6. (オプション) 脆弱性を誤検出として報告する方法

a. **[誤検出として報告する]** トグルを有効にします。

[Tenable へのメッセージ] ボックスが表示されます。

b. **[Tenable へのメッセージ]** ボックスに、誤検出の説明を入力します。

7. **[保存]** をクリックします。

Tenable Web App Scanning が既存の検出結果にルールを適用し始めます。システムの負荷と一致する検出結果の数によっては、このプロセスに時間がかかる場合があります。

脆弱性の深刻度インジケーター

Tenable は、すべての脆弱性に、CVSSv2 または の静的なスコア

Tenable Web App Scanning インターフェースでは、深刻度カテゴリ、許容済みステータス、変更済みステータスごとに異なるアイコンを使用します。変更の詳細については、検出結果の変更ルールの作成を参照してください。

アイコン	カテゴリ	詳細
	緊急	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[重大]** に変更しました。
	高	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[高]** に変更しました。
	中	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[中]** に変更しました。
	低	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[低]** に変更しました。
	情報	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[Info]** に変更しました。

脆弱性の状態

Tenable は、ネットワークで検出されたすべての脆弱性に対して、脆弱性の状態を割り当てます。脆弱性の状態別に追跡、フィルタリングすることで、脆弱性の検出、解決、再発の推移を確認できます。

脆弱性の状態追跡が利用可能になりました。2024 年 1 月より、既存の脆弱性がある資産に対して新規または追加のスキャンを実行すると、脆弱性が修正される場合があります。この変化は、Tenable Web App Scanning、および Tenable Vulnerability Management 調査ワークベンチで確認することができます。必要な対応はありませんが、Tenable ではこれらのアップデートを確認するために 1 つ以上のスキャンを実行することを推奨しています。

注意: この機能は現在、Tenable Web App Scanning FedRAMP Moderate では利用できません。

注意: **[アクティブ]** 状態を使用して脆弱性をフィルタリングした場合、Tenable Web App Scanning は **[新規]** 状態の脆弱性も返します。フィルタリングでは、**[新規]** は **[アクティブ]** のサブカテゴリです。

脆弱性の状態	表示の有無	説明
新規	ダッシュボードに表示	[調査] ページの **[新規]** は Tenable Web App Scanning が脆弱性を 1 回検出したことを示します。 [脆弱性資産] と [検出結果] タブの **[新規]** は、Tenable Web App Scanning が脆弱性を 1 回、または最初の検出から最長 14 日後までに複数回検出したことを示します。
アクティブ	ダッシュボードに表示	[調査] ページの **[アクティブ]** は Tenable Web App Scanning が脆弱性を複数回検出したことを示します。 [脆弱性資産] と [検出結果] タブの **[アクティブ]** は Tenable Web App Scanning が脆弱性を複数回検出し、最初の検出が 14 日以上前に行われたことを示します。
修正済み	ダッシュボードでは非表示だが、フィルターにより表示可能	過去にホストにあったが、現在は存在しない脆弱性。

脆弱性の状態	表示の有無	説明
再表面化	ダッシュボードに表示	以前にホストで修正済みとしてマークされたが、Tenable Web App Scanning により再び検出された脆弱性。 脆弱性が**[再表面化]**となった場合、次が起こるまではこの状態が維持されます。 • 後のスキャンでこの脆弱性が修正済みと判定される。この時点で脆弱性は**[修正済み]**状態に戻ります。

検出結果フィルター

[検出結果] ページで分析を表示することができます。

ウェブアプリケーションの検出結果フィルター

オプション	説明
資産 ID	スキャンで脆弱性が検出された資産の UUID。
資産名	スキャナーで脆弱性が検出された資産の名前。 このフィルターは、デフォルトでフィルタープレーンに表示されます。
Bugtraq ID	脆弱性を特定したプラグインの Bugtraq ID。
CPE	プラグインが特定する脆弱性の共通プラットフォーム一覧 (CPE) 番号。
CVE	プラグインが特定する脆弱性の共通脆弱性識別子 (CVE) ID。
CVSSv2 基本値	CVSSv2 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。
CVSSv2 攻撃元区分	脆弱性に対する、加工していない CVSSv2 メトリクス。詳細は、CVSSv2 のドキュメントを参照してください。
CVSSv3 基本値	CVSSv3 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。
CVSSv3 攻撃元区分	脆弱性に関する、その他の CVSSv3 メトリクス。
CWE	脆弱性の共通脆弱性タイプ一覧 (CWE)。
初回確認日	スキャンが資産上で初めて脆弱性を検出した日付。
入力名	脆弱性によって悪用される特定のウェブアプリケーションコンポーネントの名前。
入力タイプ	脆弱性によって悪用されるウェブアプリケーションコンポーネントのタイプ (フォーム、Cookie、ヘッダーなど)。
最終観察	スキャンで最後に検出結果が観察された日付。

日	
元の深刻度	スキャンが検出結果を最初に検出した際の脆弱性の CVSS ベースの深刻度。詳細は、CVSS vs. VPR を参照してください。
OWASP 2010	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2010 年のカテゴリ。
OWASP 2013	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2013 年のカテゴリ。
OWASP 2017	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2017 年のカテゴリ。
OWASP 2021	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2021 年のカテゴリ。
OWASP API 2019	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2019 年のカテゴリ。可能なオプションは次のとおりです。 • **API1:2019 破られたオブジェクトレベルの承認** • **API2:2019 破られたユーザー認証** • **API3:2019 過剰なデータ漏洩** • **API4:2019 リソースとレート制限の不足** • **API5:2019 破られた関数レベルの承認** • **API6:2019 一括割り当て** • **API7:2019 セキュリティの不適切な設定** • **API8:2019 インジェクション** • **API9:2019 不適切な資産管理** • **API10:2019 不十分なロギングとモニタリング**
プラグインの説明	検出結果で検出された脆弱性を特定した Tenable プラグインの説明。
プラグイン	脆弱性を特定したプラグインのファミリー。

ファミリー	
プラグイン ID	検出結果で検出された脆弱性を特定したプラグインの ID。 このフィルターは、デフォルトでフィルタープレーンに表示されます。
プラグイン変更日	プラグインが最後に変更された日付。
プラグイン名	この監査検出結果を識別したプラグインの名前。 このフィルターは、デフォルトでフィルタープレーンに表示されます。
公開されたプラグイン	脆弱性を特定したプラグインが公開された日付です。
修正されたリスク	脆弱性の深刻度に適用されるリスクの変更。可能なオプションは次のとおりです。 • **変更** • **許容済み** • **なし** 詳細は、変更ルールと許容ルールを参照してください。
深刻度	CVSS スコアベースの深刻度詳細については、Tenable Vulnerability Management ユーザーガイドの CVSS スコアと VPR を参照してください。 このフィルターは、デフォルトで **[重大]**、**[高]**、**[中]**、**[低]** が選択された状態でフィルタープレーンに表示されます。
ソリューション	検出結果で検出された脆弱性を修正する方法に関する概要。
状態	検出結果で検出された脆弱性の状態。詳細は、脆弱性の状態を参照してください。 このフィルターは、デフォルトで **[アクティブ]** と **[再表面化]** が選択された状態でフィルタープレーンに表示されます。
Url	スキャナーで脆弱性が検出された完全な URL。 このフィルターは、デフォルトでフィルタープレーンに表示されます。

WASC	プラグインが対象とする脆弱性に関連付けられている Web Application Security Consortium (WASC) のカテゴリ。

検出結果のグループ化

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

Findings ページで、脆弱性の検出結果を特定の属性でグループ化できます。

注意: **[次でグループ化]** 機能を使用する場合、一度にエクスポートできるのは最大 5 つの検出結果のみです。

脆弱性の検出結果をグループ化する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[検出結果]** をクリックします。

   [検出結果] ページが表示され、検出結果を示す表が表示されます。デフォルトでは **[グループ化なし]** がアクティブになっています。

3. (オプション) ウェブアプリケーションの脆弱性の検出結果を分析するには、**[ウェブアプリケーションの検出]** タブをクリックします。

4. 次のいずれかを行います。

ウェブアプリケーションの検出結果をグループ化する方法

注意: パフォーマンスを最適化するために、Tenable では、**[調査]** > **[検出結果]** ビューまたは **[資産]** ビュー (**[次でグループ化]** 表を含む) に適用できるフィルターの数を 7 つに制限しています。

a. **[ウェブアプリケーションの検出結果]** 表の上部の **[次でグループ化]** の横にある、検出結果をグループ化する際の基準となる、次のいずれかの属性をクリックします。

注意: デフォルトでは、グループ化**なし**の設定がアクティブであるため、検出結果はグループ化されずに表示されます。

- **資産** - 影響を受けている資産に関連付けられているウェブアプリケーションの一意の名前。

- **プラグイン** - ウェブアプリケーションリソースタイプの ID (リソースグループや仮想マシンなど)。

ウェブアプリケーションの検出結果の表が表示され、選択した属性でグループ化された検出結果が表示されます。

b. (オプション) グループ化された検出結果に関する次の詳細を表示します。

注意: 表に表示される詳細は、検出結果をグループ化するために選択した属性によって異なります。

列	説明
資産	
資産名	スキャンで脆弱性が検出された資産の名前。この値は Tenable Vulnerability Management に対して一意です。
脆弱性	グループ化された検出結果の各セットについて、脆弱性の CVSS ベースの深刻度別の割合を示す説明画像。詳細は、CVSS vs. VPR を参照してください。
緊急	グループ化された検出結果の各セットにおいて、CVSS ベースの深刻度評価で緊急とされた脆弱性の数。詳細については、CVSS vs. VPR を参照してください。
重要	グループ化された検出結果の各セットにおいて、CVSS ベースの深刻度評価で重要とされた脆弱性の数。詳細は、CVSS vs. VPR を参照してください。
脆弱性カウント	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した脆弱性の数。
最終確認日	スキャンが資産上でこの脆弱性を検出した直近の日時。
アクション	グループ化された検出結果の各セットで実行できるアクション。

プラグイン	
深刻度	グループ化された検出結果の各セットで特定された CVSS ベースの深刻度スコア詳細は、CVSS vs. VPR を参照してください。
名前	脆弱性を特定したプラグインの名前。
ファミリー	脆弱性を特定したプラグインのファミリー。
CVSSv2 基本値	CVSSv2 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。 **注意:** 深刻度メトリクス設定に基づいて、このパラメーターは CVSSv3 ベーススコアを表示する可能性があります。詳細は、全般設定 を参照してください。
プラグイン ID	脆弱性を特定したプラグインの ID。
資産数	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した資産の数。
脆弱性カウント	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した脆弱性の数。
アクション	グループ化された検出結果の各セットで実行できるアクション。

5. (オプション) 表のデータを選別します。詳細は、Tenable Web App Scanning の表 を参照してください。
6. (オプション) 別の属性でグループ化するには、**[次でグループ化]** の横にある別の属性をクリックします。

   表には、新しい属性でグループ化された検出結果が表示されます。
7. (オプション) グループ化を削除するには、**[次でグループ化]** の横の **[なし]** をクリックします。

   表にグループ化していない検出結果が表示されます。

Tenable Web App Scanning のスキャンワークフロー

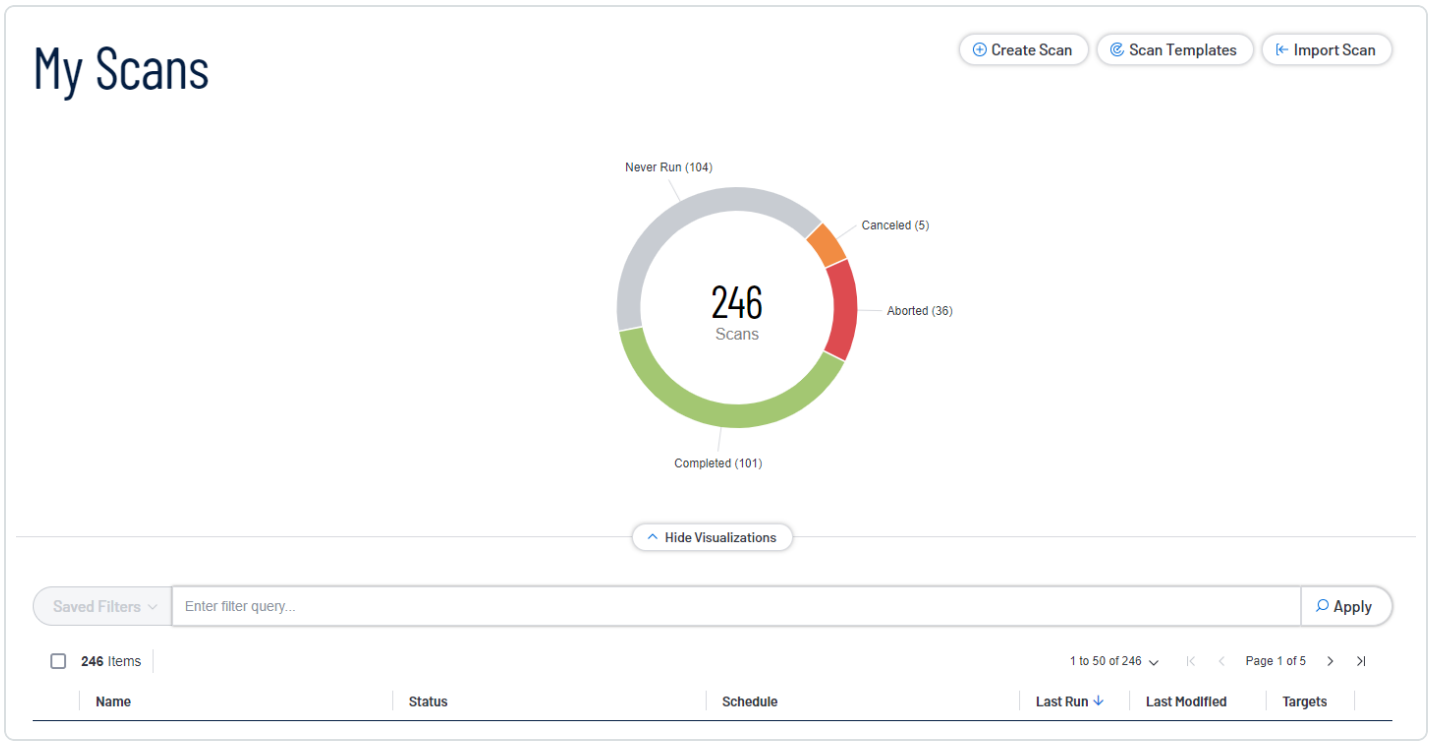
使用しているウェブアプリケーションに関するデータを収集するようにウェブアプリケーションスキャンを設定し、分析することができます。この概要では、Tenable Web App Scanning のスキャンを作成、設定、起動、管理するのに必要な主な手順について説明します。一人ですべてのステップを行うか、複数の人でステップをシェアして行うことができます。

脆弱性の状態追跡が利用可能になりました。2023 年 8 月より、既存の脆弱性がある資産に対して新規または追加のスキャンを実行すると、脆弱性が修正される場合があります。この変更は、Tenable Web App Scanning、および Tenable Vulnerability Management の調査ワークベンチで確認することができます。必要な対応はありませんが、Tenable ではこれらのアップデートを確認するために 1 つ以上のスキャンを実行することを推奨しています。

知っていましたか? WAS **スキャン**利用者の 65% が、クイックスキャンを好んでいます。

マイスキャン

[マイスキャン] ページには、スキャンの合計数、およびスキャンステータスのいくつかのカテゴリ(**実行しない**、**キャンセル**、**中止**、**完了**)がわかるビジュアル化されたウィジェットが表示されます。これらのビジュアライゼーションは、**[ビジュアライゼーションの非表示]** または **[ビジュアライゼーションの表示]** ボタンをクリックすることで、非表示にしたり再表示したりすることができます。詳細は、スキャンのステータスを参照してください。



ヒント：[マイスキャン] のリングチャート のセグメントを**クリック**すると、そのステータスでフィルタリングすることができます。セグメントの選択を解除するには、選択したセグメントをもう一度**クリック**します。

[マイスキャン] ページを表示する

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. **[マイスキャン]** ページで ⋮ ボタンをクリックすると、次のアクションのいずれかまたはすべてを実行できます。

   - 編集
   - 開始
   - 移動

- コピー
- ゴミ箱

> **注意：** すべてのスキャンアクションが、リスト内のすべてのスキャンに使用できるわけではありません。たとえば、**インポート済み**としてタグ付けされているスキャンには、**[移動]**と**[ゴミ箱]**のアクションしか使用できません。

次のステップ

- スキャンの作成と起動
- アプリケーションダッシュボードの表示
- 検出結果の表示
- 設定の表示

スキャンの作成と起動

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

脆弱性の状態追跡が利用可能になりました。2023 年 8 月より、既存の脆弱性がある資産に対して新規または追加のスキャンを実行すると、脆弱性が修正される場合があります。この変更は、Tenable Web App Scanning、および Tenable Vulnerability Management の調査ワークベンチで確認することができます。必要な対応はありませんが、Tenable ではこれらのアップデートを確認するために 1 つ以上のスキャンを実行することを推奨しています。

Tenable Web App Scanning インターフェースでスキャンを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. 次のいずれかを行います。

   - 1 つのスキャンを起動する方法:

     a. スキャンの表で、起動するスキャンの横にある ⋮ ボタンをクリックします。

     b. 行の右側にある ▷ **[起動]** ボタンをクリックします。

        スキャンが起動し、**[ステータス]** 列が更新され、スキャンのステータスが反映されます。

   - 複数のスキャンを起動する方法:

     a. スキャンの表で、起動するスキャンの横にある 1 つ以上のチェックボックスを選択します。

        ページの上部にアクションバーが表示されます。

b. アクションバーで、▷**[起動]** ボタンをクリックします。

スキャンが起動し、それぞれの **[ステータス]** 列が更新され、スキャンのステータスが反映されます。

- スキャンテンプレートを使用せずに新しいスキャンを作成して起動する方法:

a. ページの右上にある ⊕ **[スキャンの作成]** ボタンをクリックします。

[スキャンの作成] ページが表示されます。デフォルトでは、**[スキャン]** タブがアクティブになっています。

b. スキャン情報を入力してから **[保存]** をクリックしてスキャンセットアップを保存するか、**[保存して実行]** をクリックしてスキャンを起動します。

- **Tenable テンプレート**を使用して新しいスキャンを作成して起動する方法

a. ページの右上にある ⊕ **[スキャンの作成]** ボタンをクリックします。

[スキャンの作成] ページが表示されます。デフォルトでは、**[スキャン]** タブがアクティブになっています。

b. **[Tenable テンプレート]** を選択します。

c. リストからテンプレートを選択します。詳細は、Tenable 提供の Tenable Web App Scanning テンプレートを参照してください。

d. スキャンテンプレートの設定が完了したら、**[保存して実行]** をクリックします。

- 以前に作成した**ユーザーテンプレート**を使用して新しいスキャンを作成して起動する方法

a. ページの右上にある ⊕ **[スキャンの作成]** ボタンをクリックします。

[スキャンの作成] ページが表示されます。デフォルトでは、**[スキャン]** タブがアクティブになっています。

b. **[ユーザーテンプレート]** を選択します。

c. リストからテンプレートを選択します。詳細は、Tenable 提供の Tenable Web App Scanning テンプレートを参照してください。

d. スキャンテンプレートの設定が完了したら、**[保存して実行]**をクリックします。

> **注意:** 新しいユーザーテンプレートを作成するには、ユーザーテンプレートを参照してください。

4. スキャン情報を入力してから**[保存]**をクリックしてスキャンセットアップを保存するか、**[保存して実行]**をクリックしてスキャンを起動します。

   Tenable Web App Scanning がスキャンを起動します。

> **注意:** システムにかかる負荷によっては、スキャンを起動すると、そのスキャンが完了するまでに時間を要することがあります。スキャン時間が長引くことを避けるには、過剰な数のスキャンを同時に行わないようにしてください。同時スキャンの数が多すぎると、システムのスキャン能力が枯渇してしまうことがあります。Tenable Web App Scanning は必要に応じて自動的にそれらのタイミングをずらし、一貫したパフォーマンスでスキャンを行えるようにします。

> **注意:** Tenable Web App Scanning は、4 時間以上 **保留**ステータスになったままのスキャンを中止します。Tenable Web App Scanning によってスキャンが中止された場合は、重複するスキャンの数が減るようにスキャンのスケジュールを変更します。問題が解決しない場合は、Tenable サポート にお問い合わせください。

Tenable Web App Scanning のスキャンタイプ

Tenable Web App Scanning スキャンのスキャンタイプを利用すると、適切なレベルのオプションでスキャンをすぐに開始できます。

知っていましたか? WAS **スキャン**利用者の 65% が、クイックスキャンを好んでいます。

スキャンタイプ

タイプ	説明	スキャン時間
クイックスキャン	最大 70% の脆弱性をすばやく検出する概要スキャン。このスキャンでは、SSL/TLS および HTTP セキュリティヘッダーに関連する設定の問題を重点的に調べます。このスキャンタイプは、Tenable Web App Scanning ユーザーインターフェースのほとんどのページにあるボタンから起動できます。	3 分以内
基本スキャン	アプリケーション全体をクロールし、最大 85% の脆弱性を検出する標準スキャン。このスキャンでは、設定ミスとコンポーネントの脆弱性を重点的に調べます。	1 時間未満
フルスキャン	アプリケーション全体をクロールし、すべての既知の脆弱性を検出する包括的スキャン。このスキャンでは、設定ミス、コンポーネントの脆弱性、よく発生する一般的な脆弱性を重点的に調べます。	数時間
カスタムスキャン	すべての設定を管理し、実行するプラグインを選択します。	変動

注意: 各スキャンタイプ (およびスキャンテンプレート) は、プラグインのファミリーと個々のプラグインをサポートしています。詳細については、スキャンプラグインの表示を参照してください。

スキャンのアクセス許可を設定する

必要な追加ライセンス: Tenable Web App Scanning

必要なユーザーロール: 管理者

既存のスキャンで、新しいユーザーまたはグループのアクセス許可を追加するか、既存のアクセス許可を更新することができます。

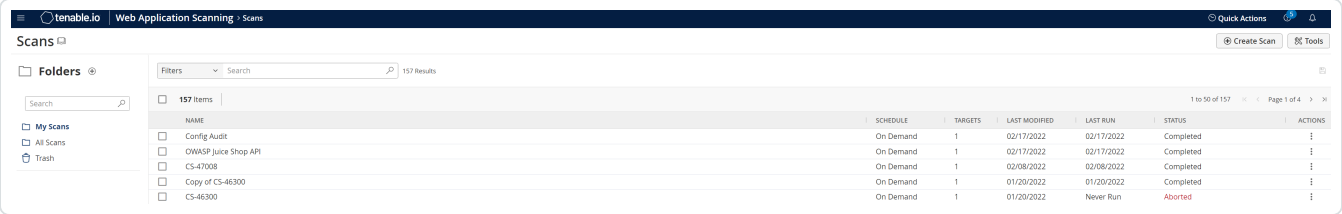
アクセス許可を追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[ウェブアプリスキャン]** セクションで、**[スキャン]** をクリックします。

   Tenable Web App Scanning の **[スキャン]** ページが表示されます。



   注意: Tenable Web App Scanning ライセンスが期限切れになった場合、ウェブアプリケーションスキャンはスキャンの表に表示されなくなります。

3. スキャンの表で、アクセス許可を設定するスキャンの行にカーソルを合わせます。
4. 行の右側にある ✎ ボタンをクリックします。

   [スキャンの更新] ページが表示されます。

5. **[ユーザーアクセス許可]** セクションで、⊕ ボタンをクリックします。

   [ユーザーアクセス許可の追加] プレーンが表示されます。

6. **[ユーザーまたはグループを追加する]** ドロップダウンボックスで、スキャンを共有するユーザー名またはグループを選択します。

   ユーザー名またはグループが、ドロップダウンボックスの下のユーザーのリストに表示されます。

ヒント：ユーザーまたはグループの名前をドロップダウンボックスに入力している場合、Tenable Web App Scanning によってテキストに一致するオプションのリストが表示されます。

7. ユーザーまたはグループの名前の横のドロップダウンボックスで、ユーザーまたはグループに適用するアクセス許可を選択します。
8. **[追加]** をクリックします。

   [ユーザーアクセス許可の追加] プレーンが表示されなくなります。

   ユーザーまたはグループは、選択したアクセス許可と共に、**[ユーザーアクセス許可]** セクションに表示されます。
9. **[保存]** をクリックします。

   Tenable Web App Scanning はスキャンのアクセス許可を更新します。

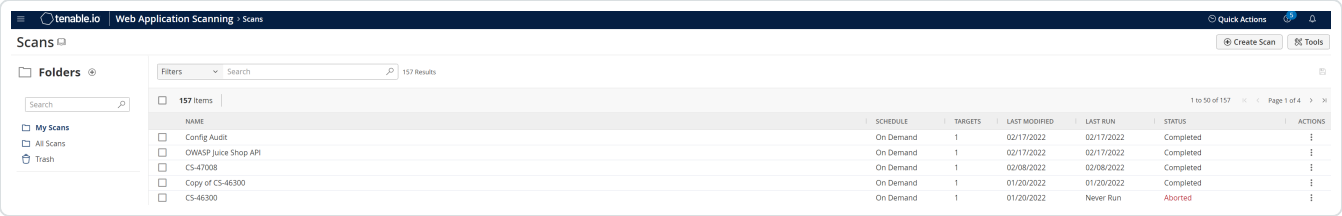
既存のアクセス許可を更新する方法

注意： スキャンを所有しているユーザーのアクセス許可を更新することはできません。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。
2. 左側のナビゲーションプレーンの **[ウェブアプリスキャン]** セクションで、**[スキャン]** をクリックします。

   Tenable Web App Scanning の **[スキャン]** ページが表示されます。



注意： Tenable Web App Scanning ライセンスが期限切れになった場合、ウェブアプリケーションスキャンはスキャンの表に表示されなくなります。

3. スキャンの表で、アクセス許可を設定するスキャンに対応する行にカーソルを合わせます。
4. 行の右側にある ✎ ボタンをクリックします。

   [スキャンの更新] ページが表示されます。

5. **[ユーザーアクセス許可]** セクションで、次の操作を実行できます。

アクション	手順
ユーザーまたはグループのアクセス許可を更新する	ユーザーまたはグループの名前の横のドロップダウンボックスで、適用するアクセス許可を選択します。
ユーザーまたはグループからすべてのアクセス許可を削除する	• ユーザーまたはグループの名前にカーソルを合わせます。 ドロップダウンボックスの横に ⊗ ボタンが表示されます。 • ⊗ ボタンをクリックします。 ユーザーまたはグループの名前がリストから削除されます。

6. **[保存]** をクリックします。

Tenable Web App Scanning がアクセス許可を更新します。

スキャン設定を編集する

必要な Tenable Web App Scanning ユーザーロール: スキャンマネージャーまたは管理者

必要なスキャンのアクセス許可: 設定可

Tenable Web App Scanning スキャンまたはユーザー定義スキャンテンプレートで可能な設定は、Tenable 提供のスキャンテンプレートのタイプによって異なります。詳細は、Tenable Web App Scanning のスキャンテンプレートの設定 を参照してください。

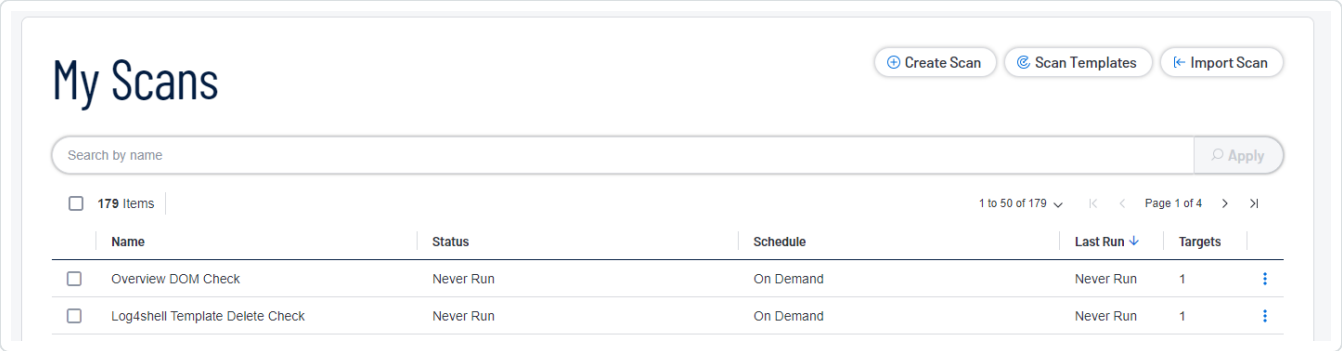
新しいインターフェースでスキャンを設定する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   Tenable Web App Scanning で **[マイスキャン]** ページが表示されます。



3. リストで、編集するスキャンの ⋮ ボタンをクリックします。

4. ✎ ボタンをクリックします。

   [スキャンの更新] ページが表示されます。

5. スキャン設定を変更します。

6. (オプション) **[詳細設定]** セクションで **[セッションの設定]** を追加します。

注意: このトークンを指定すると、スキャナーでトークン検証をスキップできるようになり、スキャンにかかる時間が短縮されます。既存のスキャンの編集中にのみ利用可能です。詳しくは、詳細設定を参照してください。

7. **[保存]** をクリックします。

   Tenable Web App Scanning によりスキャン設定が保存されます。

API スキャンの開始

必要な追加ライセンス: Tenable Web App Scanning

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

必要なスキャンのアクセス許可: 制御可

注意: システムにかかる負荷によっては、スキャンを起動すると、そのスキャンが完了するまでに時間を要することがあります。スキャン時間が長引くことを避けるには、過剰な数のスキャンを同時に行わないようにしてください。同時スキャンの数が多すぎると、システムのスキャン能力が枯渇してしまうことがあります。Tenable Web App Scanning は必要に応じて自動的にそれらのタイミングをずらし、一貫したパフォーマンスでスキャンを行えるようにします。

Tenable Web App Scanning では、スキャンテンプレートを使用して検出スキャン、評価スキャン、API スキャンを作成できます。テンプレートと設定に関する一般的な情報については、スキャンテンプレートと設定を参照してください。

注意: コンテナで 25 を超えるスキャンを同時に実行することはできません。

始める前に

- 使用できる API の説明に用いる swagger ファイルを参照用に用意します。

Tenable Web App Scanning API スキャンを起動する方法

1. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   Tenable Web App Scanning の **[スキャン]** ページが表示されます。

   注意: Tenable Web App Scanning ライセンスが期限切れになった場合、スキャンの表に Tenable Web App Scanning スキャンが表示されなくなります。

2. トップナビゲーションで、**[ウェブアプリケーションスキャン]** を選択します。

3. ページの右上にある **[スキャンの作成]** ボタンをクリックします。

   [スキャンテンプレート] ページが表示されます。

4. **API** スキャンテンプレートを選択します。

5. [スキャンの作成 - API スキャン] ページの **[設定]** セクションで、次の最低限必要な設定を入力します。

   注意: 必須ではありませんが、Tenable ではすべてのスキャンをスケジュールして繰り返し実行することを推奨しています。Tenable Web App Scanning スキャンのスケジュールの詳細については、スケジュールを参照してください。

   - 名前
   - スキャナー
   - ターゲット

6. **[範囲]** セクションで、スキャンする API の OpenAPI (Swagger) ファイルを追加します。

   注意: 1 MB より大きい OpenAPI (Swagger) ファイルを API スキャンに添付すると、エラーメッセージが表示されます。この制限の詳細については、ナレッジの記事を参照してください。Swagger 仕様ファイルの詳細については、OpenAPI (Swagger) 仕様を参照してください。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management は、設定済み Tenable Web App Scanning スキャンのリストを返します。

8. スキャンを開始するには、実行する必要のあるスキャンの **[アクション]** 列の ⋮ ボタンをクリックし、**[起動]** を選択します。

9. スキャンが完了したら、スキャンをクリックして結果を表示します。

注意: Tenable Web App Scanning は、4 時間以上 **保留** ステータスになったままのスキャンを中止します。Tenable Web App Scanning によってスキャンが中止された場合は、重複するスキャンの数が減るようにスキャンのスケジュールを変更します。問題が解決しない場合は、Tenable サポート にお問い合わせください。

Tenable Web App Scanning のスキャンテンプレートの設定

スキャンの設定により、スキャンのパラメーターを独自のネットワークセキュリティのニーズに合うように改良できます。設定可能なスキャン設定は、スキャンやユーザー定義テンプレートのベースになっている Tenable 提供のテンプレートによって変わります。

これらの設定は、個別のスキャンで、または個別のスキャンの作成に使用するユーザー定義テンプレートで設定できます。

ユーザー定義テンプレートでの設定

ユーザー定義テンプレートを設定する際は、次のことに注意してください。

- ユーザー定義テンプレートを設定すると、その設定はそのユーザー定義テンプレートに基づいて作成されたすべてのスキャンに適用されます。
- ユーザー定義テンプレートは、Tenable 提供のテンプレートをベースにして作成します。ほとんどの設定は、同じ Tenable 提供のテンプレートを使用する個別のスキャンで設定できるものと同じです。

  ただし、一部の **[基本]** 設定はユーザー定義テンプレートの作成にだけ使用でき、個別のスキャンの設定時には表示されません。詳細については、ユーザー定義テンプレートを参照してください。
- ユーザー定義テンプレートで設定できても、ユーザー定義テンプレートに基づく個別のスキャンで変更することができない設定があります。こうした設定を個別のスキャンで変更したい場合は、代わりに Tenable 提供のテンプレートに基づいて個別のスキャンを作成してください。

  Tenable Web App Scanning のスキャン設定は、次のカテゴリに分類されます。

  - ユーザー定義テンプレートの基本設定
  - Tenable Web App Scanning スキャンの基本設定
  - Tenable Web App Scanning スキャンの範囲設定
  - Tenable Web App Scanning スキャンのレポート設定
  - Tenable Web App Scanning スキャンの評価設定
  - Tenable Web App Scanning スキャンの詳細設定
  - Tenable Web App Scanning スキャンの認証情報

    - Tenable Web App Scanning スキャンのプラグイン設定

- ユーザー定義テンプレートで**認証情報**を設定した場合、他のユーザーがテンプレートに基づくスキャンに、スキャン固有の認証情報または管理された認証情報を追加することにより、それらの認証情報をオーバーライドできます。

Tenable 提供の Tenable Web App Scanning テンプレートタイプ

Tenable Web App Scanning は、特定のスキャン目的のために使用するスキャナーテンプレートを提供しています。

> **注意:** 各スキャンタイプ (およびテンプレート) は、プラグインのファミリーと個々のプラグインをサポートしています。詳細については、スキャンプラグインの表示を参照してください。

Tenable Web App Scanning には次のスキャナーテンプレートが用意されています。

テンプレート	説明
API	API 内で脆弱性の有無をチェックするスキャン。このスキャンは、OpenAPI (Swagger) 仕様ファイルで記述された RESTful API を分析します。添付ファイルのサイズは 1 MB に制限されています。 **ヒント:** API のスキャンに認証用のキーやトークンが必要な場合、**[HTTP 設定]** セクションの [詳細] 設定で必要になるカスタムヘッダーを追加することができます。 **注意:** API スキャンテンプレートは、パブリックベータ版として提供されています。この機能は、ベータ期間中の継続的な改善に伴い、変更される可能性があります。 **注意:** API スキャンは一度に 1 つのターゲットのみをサポートします。 **注意**: 1 MB より大きい OpenAPI (Swagger) ファイルを API スキャンに添付すると、エラーメッセージが表示されます。この制限の詳細については、ナレッジの記事を参照してください。Swagger 仕様ファイルの詳細については、OpenAPI (Swagger) 仕様を参照してください。
設定監査	ウェブアプリケーションの HTTP セキュリティヘッダーおよび他の外部向けの設定を分析し、アプリケーションが一般的なセキュリティ業界標準に準拠しているかどうかを確認する高レベルのスキャン。 **[設定監査]** スキャンテンプレートを使用してスキャンを作成する場合、Tenable Web App Scanning はセキュリティ業界標準のコンプライアンスに関連するプラグインについてのみウェブアプリケーションを分析します。
Log4Shell	Apache Log4j の Log4Shell 脆弱性 (CVE-2021-44228) をローカルチェックで検出します。

概要	ウェブアプリケーション内のどの URL をデフォルトで Tenable Web App Scanning がスキャンするかを決定する高レベルの予備的なスキャン。 **[概要]** スキャンテンプレートは、ウェブアプリケーション内のアクティブな脆弱性を分析するものではありません。そのため、このスキャンテンプレートは **[スキャン]** テンプレートほど多くのプラグインファミリーオプションを提供していません。 **注意:** このスキャンテンプレートは、従来の Tenable Web App Scanning インターフェースの **[ウェブアプリケーションの概要]** テンプレートに相当します。
PCI	Tenable PCI ASV 用にウェブアプリケーションのクレジットカード業界データセキュリティ標準 (PCI DSS) のコンプライアンスを分析するスキャン(このスキャンでは、**リクエストのリダイレクト制限**を表示および編集することもできます。この制限のデフォルト値は 3 です)。
クイックスキャン	ウェブアプリケーションの HTTP セキュリティヘッダーおよび他の外部向けの設定を分析し、アプリケーションが一般的なセキュリティ業界標準に準拠しているかどうかを確認する**設定監査**スキャンに似た高レベルのスキャン。スケジュール設定はありません。 **[クイックスキャン]** スキャンテンプレートを使用してスキャンを作成する場合、Tenable Web App Scanning はセキュリティ業界標準のコンプライアンスに関連するプラグインについてのみウェブアプリケーションを分析します。
スキャン	ウェブアプリケーションの広範囲の脆弱性を評価する包括的なスキャン。 **[スキャン]** テンプレートは、すべてのアクティブなウェブアプリケーションプラグイン用のプラグインファミリーオプションを提供します。 **[スキャン]** テンプレートを使用してスキャンを作成すると、Tenable Web App Scanning は、**[設定監査]**、**[概要]**、**[SSL TLS]** テンプレートを使用して作成されたスキャンがチェックするすべてのプラグイン、および特定の脆弱性検出のための追加のプラグインについてウェブアプリケーションを分析します。 このスキャンテンプレートを使用してスキャンを実行すると、ウェブアプリケーションのより詳細な評価が提供されますが、他の Tenable Web App Scanning スキャンよりも時間がかかります。 **注意:** このスキャンテンプレートは、従来の Tenable Web App Scanning インターフェース

	の **[ウェブアプリケーションスキャン]** テンプレートに相当します。
SSL TLS	ウェブアプリケーションが SSL/TLS 公開鍵暗号化を使用しているかどうかを確認し、使用している場合には、暗号化がどのように設定されているかを確認するためのスキャン。 **[SSL TLS]** テンプレートを使用してスキャンを作成する場合、Tenable Web App Scanning は、SSL/TLS の実装に関連するプラグインについてのみウェブアプリケーションを分析します。スキャナーは、URL をクロールしたり、個別のページの脆弱性を評価したりしません。

スキャンまたはユーザー定義スキャンテンプレートで可能な設定は、スキャンの作成に使用する Tenable 提供のスキャンテンプレートタイプによって異なります。

ユーザー定義テンプレート

必要なテンプレートのアクセス許可: 所有者

Tenable は、特定のスキャン目的のために使用できるさまざまなスキャンテンプレートを用意しています。Tenable 提供のスキャンテンプレートをカスタマイズして他のユーザーと共有したい場合は、ユーザー定義スキャンテンプレートを作成できます。

[スキャン] ページから、ユーザー定義の Tenable Web App Scanning テンプレートを作成、編集、コピー、エクスポート、削除できます。Tenable Web App Scanning スキャンテンプレートをエクスポートすることもできます。

テンプレートをクリックしてその設定とパラメーターを表示または編集するか、次の手順に従ってユーザー定義テンプレートを管理します。

ユーザー定義テンプレートの作成

ユーザー定義スキャンテンプレートを作成することで、カスタムスキャン設定を保存して、他の Tenable Web App Scanning ユーザーと共有できます。

スキャンテンプレートを定義すると、Tenable Web App Scanning は定義した人物にそのスキャンテンプレートに対する所有者のアクセス許可を割り当てます。他のユーザーにテンプレートのアクセス許可を割り当てることでスキャンテンプレートを共有できますが、テンプレートを削除できるのは所有者だけです。

ユーザー定義スキャンテンプレートを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. ページの右上にある **[スキャンテンプレート]** をクリックします。

   [スキャンテンプレート] ページが表示されます。

4. ページの右上にある ⊕ **[テンプレートの作成]** ボタンをクリックします。

   [テンプレートの選択] ページが表示されます。

5. ユーザー定義スキャンテンプレートのベースとして使用するテンプレートのタイルをクリックします。

   [テンプレートの作成] ページが表示されます。

6. スキャンを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定をします。詳細は、Tenable Web App Scanning スキャンの基本設定 を参照してください。
範囲	スキャンに含めるまたはスキャンから除外する URL とファイルタイプを指定します。詳細は、Tenable Web App Scanning スキャンの範囲設定 を参照してください。
資産	スキャンによる脆弱性の識別方法と、識別対象の脆弱性を指定します。これには、マルウェアの識別、総当たり攻撃に対するシステムの脆弱性の評価、ウェブアプリケーションの感染性が含まれます。詳細は、Tenable Web App Scanning スキャンの評価設定 を参照してください。
詳細	スキャン効率を高めるための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

   選択された内容に応じてスキャンテンプレート表が更新されます。

ユーザー定義テンプレートの編集

必要なテンプレートのアクセス許可: 設定可

ユーザー定義スキャンテンプレートを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. ページの右上にある **[スキャンテンプレート]** をクリックします。

   [スキャンテンプレート] ページが表示されます。

4. スキャンテンプレートの表で、編集するスキャンの行にある ⋮ ボタンをクリックします。

5. [編集] を選択します。

6. スキャンテンプレートのオプションを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定をします。詳細は、Tenable Web App Scanning スキャンの基本設定 を参照してください。
範囲	スキャンに含めるまたはスキャンから除外する URL とファイルタイプを指定します。詳細は、Tenable Web App Scanning スキャンの範囲設定 を参照してください。
資産	スキャンによる脆弱性の識別方法と、識別対象の脆弱性を指定します。これには、マルウェアの識別、総当たり攻撃に対するシステムの脆弱性の評価、ウェブアプリケーションの感染性が含まれます。詳細は、Tenable Web App Scanning スキャンの評価設定 を参照してください。
詳細	スキャン効率を高めるための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

7. **[保存]** をクリックします。

   Tenable Web App Scanning はユーザー定義スキャンテンプレートを保存し、それを **[スキャンテンプレート]** ページのテンプレートリストに追加します。

ユーザー定義テンプレートのコピー

ユーザー定義スキャンテンプレートをコピーすると、Tenable Web App Scanning はコピーの作成者にそのコピーに対する所有者アクセス許可を割り当てます。他のユーザーにテンプレートのアクセス許可を割り当てることでコピーを共有できますが、コピーされたテンプレートを削除できるのは所有者だけです。

ユーザー定義スキャンテンプレートをコピーする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. ページの右上にある **[スキャンテンプレート]** をクリックします。

   [スキャンテンプレート] ページが表示されます。

4. スキャンテンプレートの表で、編集するスキャンの行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

5. メニューにある ボタンをクリックします。

   [テンプレートをコピーしました] というメッセージが表示されます。Tenable Web App Scanning は、スキャンテンプレートのコピーを作成し、その名前の末尾に*「- コピー」*を付けます。そして、そのコピーの作成者に所有者のアクセス許可を与えます。コピーがスキャンテンプレートの表に表示されます。

ユーザー定義テンプレートの削除

ユーザー定義スキャンテンプレートを削除すると、Tenable Vulnerability Management によりすべてのユーザーアカウントから削除されます。

始める前に

- 削除するテンプレートを使用している、すべてのスキャンを削除します。スキャンによって現在使用中のスキャンテンプレートは削除できません。

1 つまたは複数のユーザー定義スキャンテンプレートを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. ページの右上にある **[スキャンテンプレート]** をクリックします。

   [スキャンテンプレート] ページが表示されます。

4. 1つまたは複数の削除するユーザー定義スキャンテンプレートを選択します。

   - 1つのスキャンテンプレートを選択する場合:

     a. スキャンの表で、起動するスキャンにカーソルを合わせます。

     b. 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。

     c. メニューにある 🗑 ボタンをクリックします。

        確認ウィンドウが表示されます。

   - 複数のスキャンテンプレートを選択する場合:

     a. スキャンテンプレートの表で、削除する各スキャンテンプレートのチェックボックスを選択します。

        ページの下部またはテーブルの上部に、アクションバーが表示されます。

     b. アクションバーで、🗑 ボタンをクリックします。

        確認ウィンドウが表示されます。

5. 確認ウィンドウで、**[削除]** をクリックします。

   Tenable Web App Scanning により、選択した1つまたは複数のユーザー定義スキャンテンプレートが削除されます。

スキャンプラグインの表示

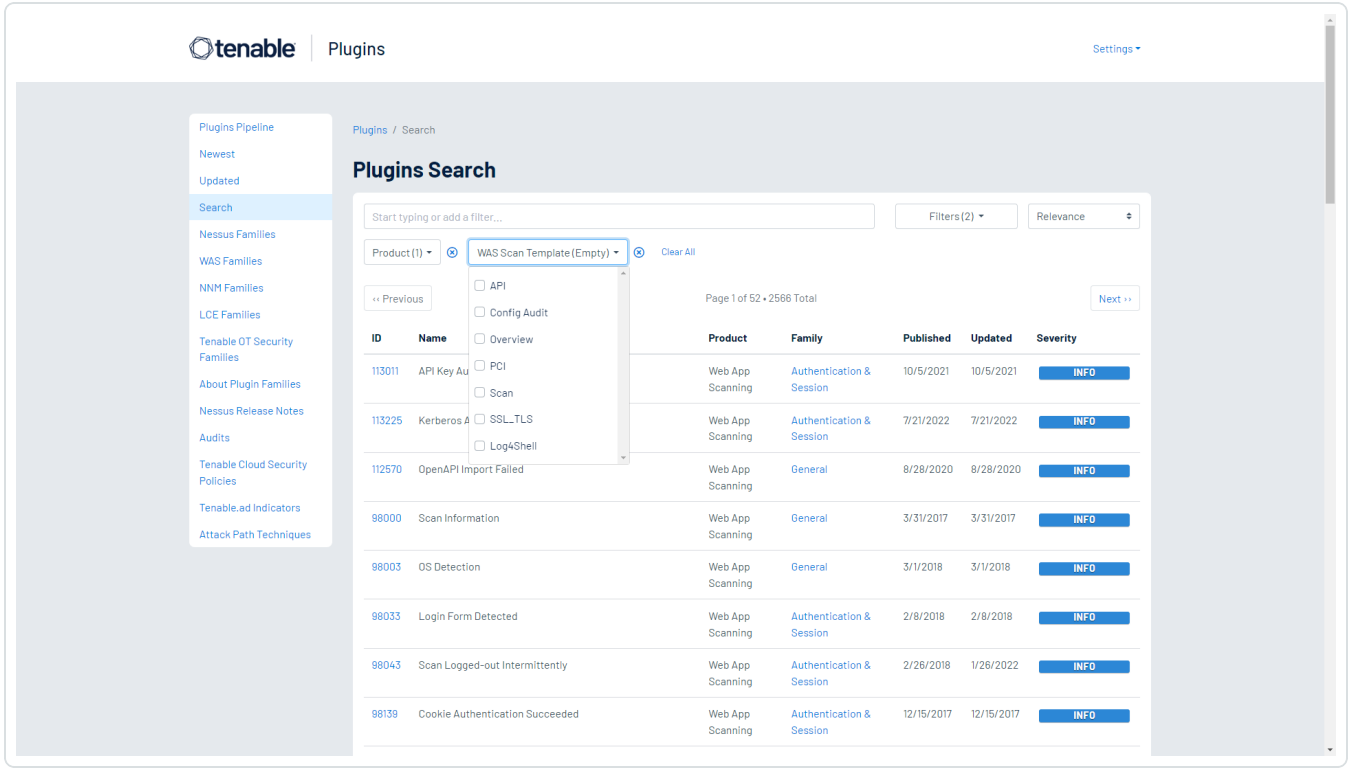
Tenable プラグインパイプラインで Web App Scanning プラグインファミリーページを表示すると、スキャンテンプレートとスキャンタイプが使用している Tenable Web App Scanning プラグインとプラグインファミリーを表示できます。

現在のスキャンプラグインを表示するには、次の 2 つの方法のいずれかを使用します。

検索ボックスを使用する

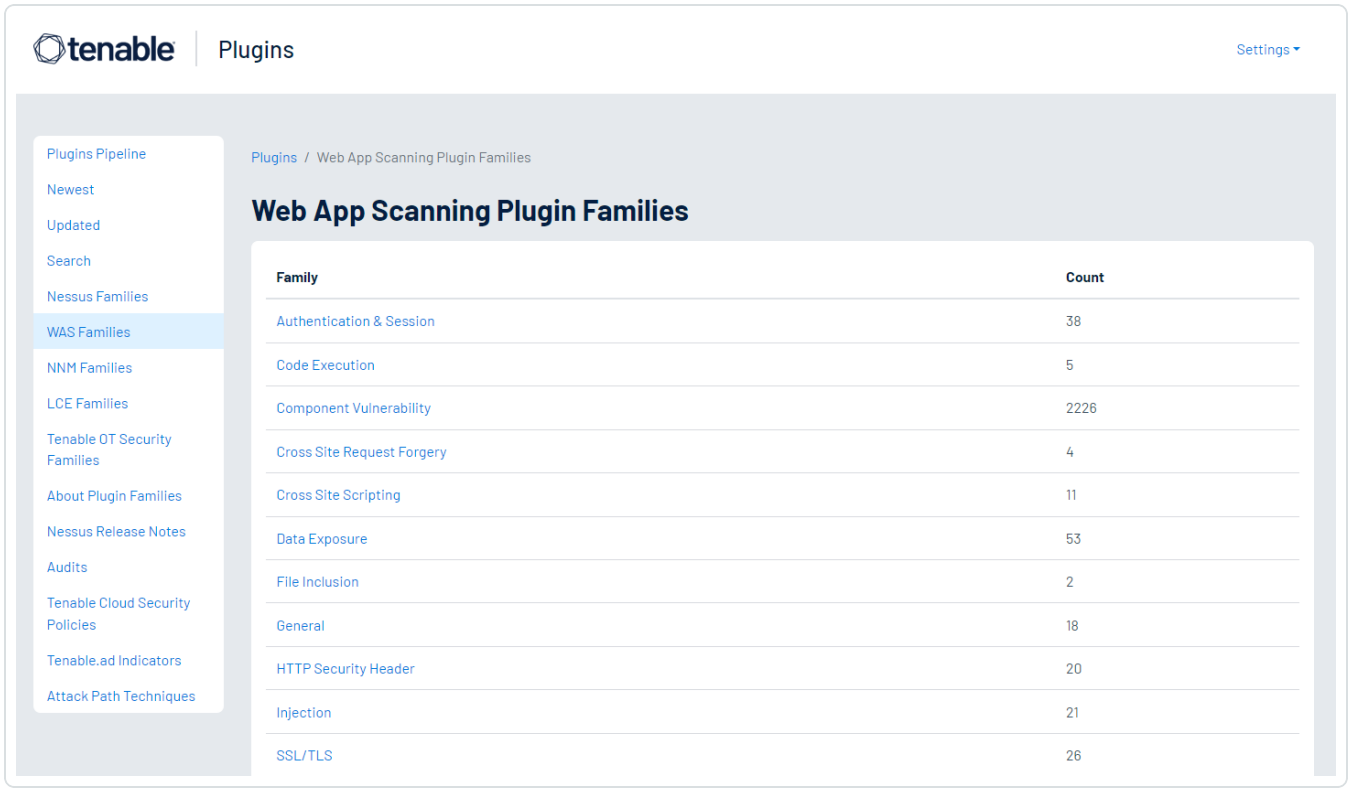
1. [Web App Scanning プラグインファミリー] ページに移動します。
2. 左側のナビゲーションで、**[検索]** をクリックします。

   [プラグイン検索] ページが表示されます。
3. **[フィルターの追加]** ボックスで **[製品]** を選択し、**[Web App Scanning]** を選択します。
4. **[フィルターの追加]** ボックスで **[WAS スキャンテンプレート]** を選択し、必要なテンプレートを選択します。
5. 選択したテンプレートを持つすべてのプラグインが表示されます。

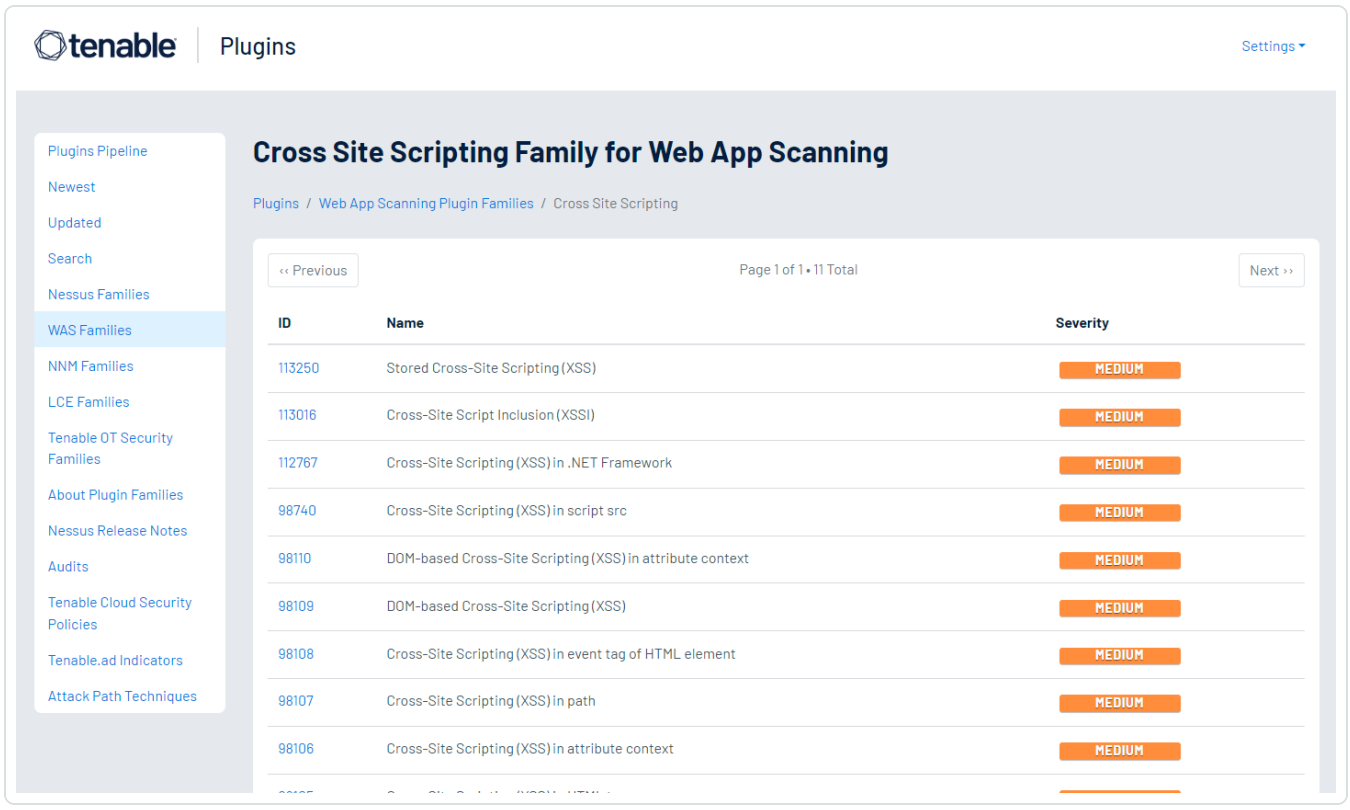


プラグインとプラグインファミリーを操作する

1. [Web App Scanning プラグインファミリー] ページに移動します。



2. 1 つのファミリーを選択すると、そのプラグインのリストが表示されます。



3. 特定の**プラグイン ID** を選択すると、レポートに表示されるとおりにプラグイン出力が表示されます。

4. プラグイン情報の右上で、**[プラグインの詳細]**と、**[スキャンテンプレート]**の横にリストされているスキャンのタイプとテンプレートを表示します。

注意: スキャンまたはユーザー定義スキャンテンプレートを作成し、**[API]**、**[概要]**、**[(基本)スキャン]**、**[標準スキャン]**、**[カスタム]** テンプレート、またはスキャンタイプを選択するときに、**[プラグイン]** の項目を設定できます。詳細については、Tenable Web App Scanning スキャンのプラグイン設定を参照してください。

Tenable Web App Scanning スキャンの基本設定

設定によって、スキャン設定における組織的およびセキュリティ関連の基本要素を指定します。これには、スキャンの名前、ターゲット、スキャンがスケジュールされているかどうか、スキャンにアクセスできるユーザーの指定が含まれます。

スキャンまたはユーザー定義スキャンテンプレートを作成したときに**設定**できます。任意のスキャンタイプを選択できます。詳細は、Scan Templates を参照してください。

> **ヒント:** 設定を保存して他のスキャンに適用したい場合は、ユーザー定義スキャンテンプレートを作成して設定できます。

[基本] 設定には、次のセクションが含まれます。

- 一般
- スケジュール
- 通知
- ユーザーアクセス許可
- データ共有

一般

スキャンの一般的な設定

設定	デフォルト値	説明	必須
名前	なし	スキャンまたはテンプレートの名前を指定します。	○
説明	なし	スキャンまたはテンプレートの説明を指定します。	×
ターゲット	なし	Tenable Web App Scanning ライセンスに表示されるスキャンするターゲットの URL を指定します。正規表現やワイルドカードは使用できません。 **警告**: Tenable Web App Scanning スキャンからターゲットを削除する場合 (たとえば、2 つ以上のターゲットから 1 つのターゲットに減らす場合)、スキャンを再起動しなければエクスポートを配信できません。	○

設定	デフォルト値	説明	必須
		注意: **[ターゲット]** ボックスに入力した URL の FQDN ホストが、ライセンスに表示されているホストとは異なっていて、スキャンが正常に実行された場合、入力した新しい URL はライセンスに追加される資産としてカウントされます。 **注意:** ユーザー定義スキャンテンプレートを作成する場合、ターゲットの設定はテンプレートに保存されません。新しいスキャンを作成するたびにターゲットを入力します。	
フォルダー	マイスキャン	保存後にスキャンが表示されるフォルダーを指定します。	○
スキャナータイプ	内部スキャナー	ローカルの内部スキャナーとクラウド管理対象スキャナーのどちらがスキャンを実行するかを指定し、**[スキャナー]** フィールドの選択肢として、ローカルスキャナーとクラウド管理対象スキャナーのどちらをリストするかを決めます。	○
スキャナー	不定	スキャンを実行するスキャナーを指定します。	○

スケジュール

スキャンのスケジュール設定

注意: ユーザー定義スキャンテンプレートを作成する場合、スケジュールの設定はスキャンテンプレートに保存されません。新しいスキャンを作成するたびにスケジュールを設定してください。

設定	Default (デフォルト)	説明
スケジュール	off	スキャンが指定されているかどうかを指定するトグルデフォルトでは、スキャンはスケジュールされていません。 **[スケジュール]** トグルが無効になっている場合、他のスケジュール設定は非表示のままになります。

設定	Default (デフォルト)	説明
		トグルをクリックする等、スケジュールが有効になり、残りの **[スケジュール]** 設定が表示されます。

頻度	一度	スキャンを開始する頻度を指定します。
		
		注意 : ターゲットをスキャンできる頻度は、いくつかの要因 (ウェブアプリケーションの更新頻度、ウェブアプリケーションに含まれるコンテンツなど) によって異なります。ほとんどのウェブアプリケーションについて、Tenable では少なくとも 1 か月に 1 回スキャンを実行することを推奨しています。
		
		• **一度**: 特定の時間にスキャンをスケジュールします。
		• **日単位**: 特定の時間、または最大 20 日で、日単位でスキャンの実行をスケジュールします。
		• **週単位**: 時間と曜日ごとに、最大 20 週間、継続的にスキャンの実行をスケジュールします。
		• **月単位**: 1~ 20 か月単位でスキャンの実行をスケジュールします。
		  • **Day of Month**: 月の特定の曜日で選択した時間にスキャンが繰り返されます。
		  • **Week of Month**: スキャンを開始する週にスキャンが毎月繰り返されます。たとえば、開始日を 10 月 3 日と選択し、それが月の第 1 週に当たる場合、スキャンは翌月以降、毎月第 1 週の選択した時刻に繰り返します。
		
		注意: 毎月、同じ日時でスキャンするようスケジュールする場合、Tenable では、開始日を 28 日以前に設定することを推奨します。いくつかの月に存在しない日付 (例: 29 日) を開始日に選択した場合、Tenable Vulnerability Management は、それらの日にはスキャンを実行できません。
		
		• **毎年**: 時間と曜日ごとに、最大 20 年間、年単位でスキャンの実行をスケジュールします。

設定	Default (デフォルト)	説明
開始	不定	スキャンを開始する正確な日時を指定します。 **注意:** 過剰な数のスキャンを同時に実行されるようにスケジュールした場合、Tenable Web App Scanning のスキャン能力が枯渇する場合があります。必要な場合は、一貫したスキャンのパフォーマンスを確保するために、Tenable Web App Scanning が同時スキャンをシフトします。 デフォルトでは、開始日はスキャンを作成する日付になっています。開始時間は 1 時間刻みで、24 時間形式で表示されます。たとえば、2019 年 10 月 31 日の午後 9 時 12 分にスキャンを作成する場合、デフォルトの開始日時は *10/31/2019* および *22:00* になります。
タイムゾーン	不定	**[開始]** に設定した値のタイムゾーン

通知

スキャンの通知設定

設定	デフォルト値	説明
E メールの受信者	なし	スキャンが完了して結果が利用可能になったときに通知される、0 個または複数のメールアドレスをコンマ、スペース、または改行で区切って指定します。

ユーザーアクセス許可

ユーザーにアクセス許可を設定して、他のユーザーにスキャンまたはユーザー定義スキャンテンプレートを共有します。ユーザーのアクセス許可の追加または編集についての詳細は、スキャンのアクセス許可を設定する を参照してください。

アクセス許可	説明
アクセスなし	(既定) このアクセス許可を設定されたユーザーは、スキャンに関与することはできません。

表示可	このアクセス許可を設定されたユーザーは、スキャンの結果を表示することができます。
Can Control	このアクセス許可を持つユーザーは、**[表示可]** で許可されているタスクに加えて、スキャンの起動および停止が可能です。スキャンの設定を表示または編集したり、スキャンを削除したりすることはできません。
設定可	このアクセス許可を持つユーザーは、**[制御可]** で許可されているタスクに加えて、スキャンの設定の表示と、スキャンの所有権以外のスキャンの設定の変更が可能です。スキャンを削除することも可能です。

データ共有

設定	デフォルト値	説明
スキャン結果	ダッシュボードに表示	スキャン結果を非公開にするか **[ダッシュボード]** ページと **[検出結果]** ページに表示するかを指定します。**[プライベート表示]** に設定されている場合、スキャン結果の **[最終確認日]** の日付は更新されず、結果を表示するにはスキャンに直接アクセスする必要があります。

Tenable Web App Scanning スキャンの詳細設定

詳細設定では、ウェブアプリケーションスキャンで実装する必要がある追加のコントロールを指定します。

詳細設定は、Tenable 提供のスキャンテンプレートを使用してスキャンまたはユーザー定義スキャンテンプレートを作成するときに設定できます。ただし、**[概要]**と**[スキャン]**テンプレートタイプでは、**[設定監査]**や**[SSL TLS]**テンプレートタイプよりも多くの**詳細**設定が可能です。詳細は、Scan Templates を参照してください。

[詳細設定]オプションを使用して、スキャンの効率とパフォーマンスを制御することができます 。

- 一般
- HTTP 設定
- 画面設定
- 制限
- Selenium の設定
- パフォーマンス設定
- セッションの設定

一般

[一般]オプションは、**[概要]**および**[スキャン]**テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明
Target Scan Max Time (HH:MM:SS)(対象資産スキャン最大時間 (HH:MM:SS))	08:00:00	スキャンジョブが停止するまでの実行最長時間を指定します。時間、分、秒で表示されます。 **注意:** 設定できる最大期間は 99:59:59 (時間:分:秒) です。
最大キュー時間 (HH:MM:SS)	08:00:00	スキャンが Queued 状態を続ける最大期間を指定します。時間、分、秒で表示されます。

		注意: 設定できる最大期間は 48:00:00 (時間:分:秒) です。
このスキャンのデバッグログを有効にする	無効	プラグインから利用可能なデバッグログを、スキャナーがこのスキャンの脆弱性出力に添付するかどうかを指定します。
Debug Flags (デバッグフラグ)	無効	(**[このスキャンのデバッグログを有効にします]** を有効にしたときのみ表示) デバッグ用に、サポートから提供されるキーと値のペアを指定できます。

HTTP 設定

これらの設定では、スキャナーで識別するユーザーエージェント、およびスキャナーでウェブアプリケーションに対するリクエストに含める必要がある HTTP レスポンスヘッダーを指定します。

Tenable 提供のスキャンテンプレートをベースにしたスキャンおよびユーザー定義スキャンテンプレートで **[クロールの設定]** オプションを設定することができます。

設定	Default (デフォルト)	説明
Use a different User Agent to identify scanner (異なるユーザーエージェントを使用してスキャナを特定する)	無効	スキャナーで HTTP リクエストを送信するときに Chrome 以外のユーザーエージェントヘッダーを使用するかどうかを指定します。
User Agent (ユーザーエージェント)	Chrome's user-agent (Chrome のユーザーエージェント)	スキャナーが HTTP リクエストを送信するときに使用するユーザーエージェントヘッダーの名前を指定します。 このオプションは、**[異なるユーザーエージェントを使用してスキャナーを特定する]** チェックボックスを選択した後にのみ設定できます。 デフォルトでは、Tenable Web App Scanning は、使用中の

		マシンのオペレーティングシステムとプラットフォームに対応するオペレーティングシステムとプラットフォーム用の Chrome が使用するユーザーエージェントを使用します。Chrome のユーザーエージェントの詳細については、*Google Chrome* のドキュメントを参照してください。 **注意:** 現在の Tenable Web App Scanning ユーザーエージェントヘッダーは次のとおりです。 `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36` **注意:** スキャナーからのすべてのリクエストが、ユーザーエージェントによって送信されるわけではありません。
スキャン ID HTTP ヘッダーの追加	無効	スキャナーがターゲットに送信するすべての HTTP リクエストにもう 1 つ `X-Tenable-Was-Scan-Id` ヘッダー (スキャン ID で設定されている) を追加するかどうかを指定します。これにより、ウェブサーバーのログでスキャンジョブを特定し、スキャン設定を変更してサイトを保護することができます。
Custom Headers (カスタムヘッダー)	なし	リクエストおよびレスポンスの形式の各 HTTP リクエストに挿入するカスタムヘッダーを指定します。 ⊕ ボタンをクリックし、各追加のヘッダーの値を入力することで、カスタムヘッダーを追加することができます。 **注意:** ユーザーエージェントのカスタムヘッダーを入力した場合、その値は **[ユーザーエージェント]** 設定ボックスに入力された値をオーバーライドします。

画面設定

[画面設定] オプションは、**[概要]** および **[スキャン]** テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明

Screen Width (画面の幅)	1600	スキャナーに埋め込まれたブラウザの画面の幅 (ピクセル単位) を指定します。
Screen Height (画面の高さ)	1200	スキャナーに埋め込まれたブラウザの画面の高さ (ピクセル単位) を指定します。
Ignore Images (画像を無視する)	無効	埋め込まれたブラウザがターゲットのウェブページ上の画像をクロールするか無視するかを指定します。

制限

[制限] オプションは、**[概要]** および **[スキャン]** テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明
Number of URLS to Crawl and Browse (クロールおよびブラウズする URL の数)	10000	スキャナーでクロールを試行する URL の最大数を指定します。
Path Directory Depth (パスディレクトリの深さ)	10	スキャナーでクロールするサブディレクトリの最大数を指定します。 たとえば、ターゲットが `www.example.com` で、スキャナーで `www.example.com/users/myname` をクロールしたい場合、テキストボックスに「2」と入力します。
Path Directory Depth (ページ DOM 要素の深さ)	5	スキャナーでクロールする HTML にネストされた要素のレベルの最大数を指定します。
Max Response Size (最大レスポンスサイズ)	500000	スキャナーで分析するページの最大読み込みサイズ (バイト単位) を指定します。 スキャナーで URL をクロールし、応答がこの上限を超えた場合、スキャナーはそのページの脆弱

		性を分析しません。
リダイレクト制限のリクエスト	3	スキャナーでページのクロールの試行を停止するまでに、スキャナーが従うリダイレクトの数を指定します。

Selenium の設定

この設定では、記録されている Selenium 認証情報を使用してウェブアプリケーションに対する認証を試行するときのスキャナーの動作を指定します。

これらのオプションは、Selenium 認証情報を使用してウェブアプリケーションに認証されるようにスキャンを設定している場合に設定します。詳細は、Tenable Web App Scanning スキャンの認証情報 を参照してください。

[Selenium の設定] オプションは、**[概要]** および **[スキャン]** テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明
Page Rendering Delay (ページレンダリング遅延)	30000	スキャナーがページの表示を待機する時間 (ミリ秒単位) を指定します。
Command Execution Delay (コマンド実行遅延)	500	スキャナーがコマンドを処理してから次のコマンドを実行する前に待機する時間 (ミリ秒単位) を指定します。
Script Completion Delay (スクリプト完了遅延)	5000	スキャナーがすべてのコマンドが新しいコンテンツを表示して処理を終了するのを待機する時間 (ミリ秒単位) を指定します。

パフォーマンス設定

設定	Default (デフォルト)	説明
Max Number of Concurrent HTTP	10	単一ホストに許可される確立された HTTP

Connections (同時 HTTP 接続の最大数)		セッションの最大数を指定します。
Max Number of HTTP Requests Per Second (1 秒当たりの最大 HTTP リクエスト数)	25	スキャンの期間中に単一ホストに許可される HTTP リクエストの最大数を指定します。
Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)	無効	ネットワークの混雑が発生した場合にスキャナーでスキャンを調整するかどうかを指定します。
Network Timeout (In Seconds) (ネットワークタイムアウト (秒))	5	スキャナーがスキャンを中止する前にホストからの応答を待機する時間 (秒単位) を指定します。プラグイン内で特に指定されていない場合に有効になります。 インターネット接続の速度が遅い場合、Tenable は長い待機時間を指定することを推奨します。
Browser Timeout (In Seconds) (ブラウザータイムアウト (秒))	30	スキャナーがスキャンを中止する前にブラウザからの応答を待機する時間 (秒単位) を指定します。プラグイン内で特に指定されていない場合に有効になります。 インターネット接続の速度が遅い場合、Tenable では長い待機時間を指定することを推奨します。
Timeout Threshold (タイムアウトしきい値)	100	スキャナーがスキャンを中止するまでに許可される連続タイムアウト数を指定します。

セッションの設定

これらのトークンを指定すると、スキャナーでトークン検証をスキップできるようになり、スキャンにかかる時間が短縮されます。セッション設定は、既存のスキャンを編集している場合にのみ使用できます。

トークンタイプ	デフォルト	説明
クッキー	なし	スキャナーが使用するアプリケーションの認証クッキーの名前。
ヘッダー	なし	スキャナーが使用するアプリケーションの認証ヘッダーの名前。

Tenable Web App Scanning スキャンの範囲設定

[範囲] を設定し、スキャンに含めるまた除外する URL およびファイルタイプを指定します。

スキャンまたはユーザー定義スキャンテンプレートを作成し、**[概要]** または **[スキャン]** テンプレートタイプを選択したときに、**[範囲]** の項目を設定できます。詳細は、Scan Templates を参照してください。

ヒント: 設定を保存して他のスキャンに適用したい場合は、ユーザー定義スキャンテンプレートを作成して設定できます。

[範囲] 設定には、次のセクションが含まれます。

- クロールスクリプト
- OpenAPI (Swagger) 仕様
- スキャンの包含
- スキャンの除外

クロールスクリプト

複雑なアクセスロジックを使用するページをスキャナーが分析できるようにするためにスキャンに追加する必要がある Selenium スクリプト。

設定	説明
ファイルの追加	1 つ以上の記録されている Selenium スクリプトファイルをスキャンに追加できるようにするハイパーリンク。 スクリプトは `.side` ファイルとして追加される必要があります。

OpenAPI (Swagger) 仕様

スキャンしたい RESTful API の仕様ファイルです。ファイルは OpenAPI 仕様 (v2 または v3) に準拠し、JSON または YAML 形式が使われています。

設定	説明
ファイルの追	1 つまたは複数の OpenAPI (v2 または v3) 仕様ファイルを追加するためのハイパーリンクです。仕様ファイルには、JSON または YAML のいずれかの形式が使われています。

加	

スキャンの包含

スキャナーで含めるURLおよびスキャナーでそれらのURLをクロールする方法。

設定	Default (デフォルト)	説明
URLの一覧	なし	[基本]設定で指定したターゲットURL以外の、スキャンで確実に分析したいURL。 各URLを絶対URLとして入力します。 各URLを別々の行に入力します。 **注意:** すべてのURLは同じドメインでなければならず、ワイルドカードは使用できません。
アプリケーションのクロール中に見つかったURLをスキャナーが処理する方法を指定します。	Crawl all URLs detected (検出されたすべてのURLをクロール)	スキャナーがURLをクロールするときに従う制限を指定します。 次のいずれかを選択します。 • **Crawl all URLs detected** (検出されたすべてのURLをクロール) - スキャナーはターゲットURLのドメインホスト上で検出したすべてのURLと子パスをクロールします。 • **Limit crawling to specified URLs and child paths** (指定されたURLと子パスにクロールを制限) - スキャナーはターゲットURLと子パスのみをクロールします。 • **Limit crawling to specified URLs** (指定されたURLにクロールを制限) - スキャナーはターゲットURLのみをクロールします。ターゲットURLの子パスはクロールしません。

スキャンの除外

スキャナーでスキャンから除外する URL の属性。

設定	デフォルト値	説明
Regex for Excluded URLs	logout	スキャナーが URL で検索できるスキャンから除外する正規表現パターンを指定できるテキストボックスオプション。改行することで、複数の正規表現を指定できます。 **注意:** 除外する正規表現値は、URL に含まれる値である必要があります。たとえば、`http://www.example.com/blog/today.htm` という URL では、有効な正規表現値は `blog` または `today` となります (URL 全体ではありません)。また、正規表現の値には大文字と小文字の区別があります。
File Extensions to Exclude	js、css、png、jpeg、gif、pdf、csv、svn-base、svg、jpg、ico、woff、woff2、exe、msi、zip	スキャナーでスキャンから除外するファイルタイプを指定できるテキストボックスオプション 各ファイルタイプはコンマで区切ります。 **注意**: 特定のファイル拡張子を除外すると役立つ場合があります。スキャナーはスキャン対象がウェブページではなくてもそれを認識せず、ウェブページであるかのようにスキャンを試みることがあるためです。これは時間の無駄になり、スキャン速度を低下させます。使用することがわかっており、スキャンする必要がないことが確実な場合は、追加のファイル拡張子を追加できます。たとえば、Tenable にはデフォルトで .png や .jpeg などのさまざまな画像拡張子が含まれています。
パスの分解	未選択	このチェックボックスオプションを使用して、スキャン中に識別された各 URL を、ディレクトリパスレベルを基にして追加の URL にブレークダウンするかどうかを指定できます。 たとえば、ターゲットとして *www.example.com/dir1/dir2/dir3* を指定し、**[パスの分解]** を選択した場合、スキャナーは、以下のそれぞれをターゲットの個別の URL として分析します。 • www.example.com/dir1/dir2/dir3 • www.example.com/dir1/dir2 • www.example.com/dir1

設定	デフォルト値	説明
		ウェブアプリケーションスキャンの対象範囲を拡大するには、このオプションを選択します。 **注意:** パスの分解を含むスキャンは、パスの分解のないスキャンよりも完了に時間がかかることがあります。
バイナリを除外	選択済み	スキャナーで応答の URL をバイナリ形式で監査するかどうかを指定できるチェックボックスオプション。 ウェブアプリケーションスキャンの対象範囲を拡大するには、このオプションを選択します。 **注意:** バイナリを含むスキャンは、スキャナーがバイナリ応答を読み取ることができないので、完了するまでに時間がかかる場合があります。

その他

設定	説明
類似したページを重複除外	類似ページが既に監査されているページをスキャナーに無視させるかどうかを指定できるチェックボックスオプション。

Tenable Web App Scanning スキャンの評価設定

[評価] 設定では、スキャナーが URL をクロールするときにどのウェブアプリケーション要素を監査するかを指定します。**評価** 設定は、スキャンやユーザー定義スキャンテンプレートを作成する際に設定できます。詳細は、Scan Templates を参照してください。

評価 設定には、次のセクションが含まれます。

- スキャンタイプ
- 共通ページとバックアップページ
- 認証情報ブルートフォース攻撃
- 監査する要素
- オプション
- DOM 要素の除外

スキャンタイプ

これらの設定では、スキャナーで実行する評価の強度を指定します。

設定	デフォルト値	説明	必須
評価	推奨	以下のオプションから選択してスキャナーで実行するスキャンタイプを指定できるドロップダウンボックス。 • **推奨** - Tenable の推奨に基づくスキャナーの監査要素。 • **なし** - スキャナーはどの要素も監査しません。 • **高速** - スキャナーはリストに表示されている最も一般的な要素を監査します。 • **広範囲** - スキャナーはリストに表示されているすべての要素を監査します。 • **カスタム** - スキャナーは選択した要素だけを監査します。 **注意:** **[推奨]**、**[高速]**、または **[広範囲]** を選択してからこのセクション	○

設定	デフォルト値	説明	必須
		の設定を変更すると、**[スキャンタイプ]** 設定が自動的に**[カスタム]**に変更されます。	

共通ページとバックアップページ

設定	デフォルト値	説明
Detection Level (検出レベル)	最も検出されたページ	以下のオプションから選択してスキャナーでクロールするページを指定できるドロップダウンボックスです。 • **最も検出されたページ** - スキャナーは最も多く検出されたページのみをクロールします。 • **拡張辞書** - スキャナーは、非表示のページを検出するためにより多くのパスバリエーションをテストします。全体的なスキャン時間は長くなります。 **注意:** **[検出レベル]**ドロップダウンボックスは、**[スキャンタイプ]** 設定で**[カスタム]**を選択した場合にのみ使用できます。

認証情報ブルートフォース攻撃

[認証情報ブルートフォース攻撃] 設定は**[スキャン]**テンプレートでのみ使用できます。

設定	Default (デフォルト)	説明
認証情報ブルートフォース攻撃	無効	有効の場合、**[プラグイン]** 設定に含まれるブルートフォース攻撃を実行するプラグインが実行されます。 無効の場合、**[プラグイン]** 設定に含まれている場合でもブルートフォース攻撃プラグインは実行されません。

設定	Default (デフォルト)	説明
		注意: [認証情報ブルートフォース] の設定は、**[スキャンタイプ]** 設定で **[カスタム]** を選択した場合にのみ使用できます。

監査する要素

この設定では、スキャナーで脆弱性を分析するウェブアプリケーション内の要素を指定します。

設定	スキャナーのアクション
Cookies	Cookie ベースの脆弱性をチェックします。
ヘッダー	ヘッダーの脆弱性と安全ではない設定 (X-Frame-Options の消失など) をチェックします。
フォーム	フォームベースの脆弱性をチェックします。
リンクおよびクエリ文字列パラメーター	リンクおよびそれらのパラメーターの脆弱性をチェックします。
パラメーター名	パラメーター名の広範囲のファジングを実行します。
パラメーター値	パラメーター値の広範囲のファジングを実行します。
パスパラメーター	パスのパラメーターを評価します。パスパラメーターは、URL リライトにおいて、URL 内のアクションのオブジェクトを特定するために使用されます。たとえば、**scanId** は次の URL のパスパラメーターで、結果を表示するスキャンを特定するために使用されます。 `http://example.com/scan/scanId/results`
JSON 要素 / リクエスト本文	JSON リクエストデータを監査します。

設定	スキャナーのアクション
(JSON)	
XML 要素 / リクエスト本文 (XML)	XML リクエストデータを監査します。
UI フォーム	JavaScript コードに関連付けられている入力およびボタングループをチェックします。 **注意**: UI フォームでは、Tenable Web App Scanning はページとボタンで入力を受け取り、フォームのような要素 (UI フォーム) を作成します。Tenable Web App Scanning は各ボタンに、ページ上のすべての入力を含む `UIForm` 要素を作成します。
UI 入力	関連付けられたドキュメントオブジェクトモデル (DOM) イベントに対して孤立している入力要素をチェックします。 **注意**: UI 入力は、イベントに応答する入力がある場合です。たとえば、検索バーに入力した後、検索バーは「onEnter」イベントに応答して次のページを読み込みます。そのため、Tenable Web App Scanning はこのベクトルも監査するために `UIInput` 要素を作成します。

オプション

設定	Default (デフォルト)	説明
リモートファイルインクルード用の URL	None (なし)	Tenable Web App Scanning がリモートファイルインクルージョン (RFI) の脆弱性をテストするために使用できるリモートホスト上のファイルを指定します。 スキャナーがインターネットに到達できない場合は、スキャナーはこの内部でホストされているファイルを使用して、より正確な RFI テストを実行します。 **注意:** ファイルを指定しない場合、Tenable Web App Scanning は安全な Tenable でホストされたファイルを使用して RFI テストを実行します。

DOM 要素の除外

DOM 要素の除外は、スキャンが特定のページ要素やその子を対象にして動作しないようにします。この設定は、スキャン、概要、および PCI スキャンテンプレートで使用できます。

注意: スキャナーが属性値に基づいて要素を除外するかどうかを決定する際に、等価性チェックが実行されます。したがって、css `class foo` のある要素を除外する場合、スキャナーは `class="foo"` の要素を除外しますが、`class="foo bar"` の要素は除外しません。

⊕ ボタンをクリックして、**[テキストコンテンツ]** または **[CSS 属性]** を選択すると、除外項目を追加できます。

設定	Default (デフォルト)	説明
Text Contents	なし	テキストの内容に基づいて要素を除外します。 たとえば、スキャナーが Log Out という名前のログアウトボタンをクリックすることを防ぎたい場合は、`Log Out` というテキストをマッチさせます。
CSS Attribute	なし	CSS 属性のキーと値のペアに基づいて、要素を除外します。 たとえば、CSS 属性のキーと値のペア `id="logout"` を含むフォームとスキャナーが連動しないようにするには、キーに `id`、値に `logout` と入力します。

Tenable Web App Scanning スキャンのレポート設定

レポート設定では、スキャンレポートに含める追加の項目を指定します。たとえば Tenable PCI ASV スキャンに関するスキャンレポートでは、該当する場合、ロードバランサーの使用の詳細が必要です。

Tenable が提供するスキャンテンプレート **[PCI]** を使用してスキャンまたはユーザー定義スキャンテンプレートを作成するときに、**レポート**設定を行えます。詳細は、Scan Templates を参照してください。

レポート設定には、次のセクションが含まれます。

- (Tenable PCI ASV 6.1) ロードバランサーの使用

(Tenable PCI ASV 6.1) ロードバランサーの使用

この設定では、スキャンレポートに含めるロードバランサーの使用状況を指定します。

設定	デフォルト値	説明	必須
(Tenable PCI ASV 6.1) ロードバランサーの使用	なし	テキストボックスを使用して、Tenable PCI ASV に必要なロードバランサーとそれらの設定のリストを入力できます(該当する場合)。	×

Tenable Web App Scanning スキャンのプラグイン設定

必要な Tenable Web App Scanning ユーザーロール: スキャンマネージャーまたは管理者

[プラグイン] を設定して、スキャナーでウェブアプリケーションをスキャンするときに使用するプラグインおよびプラグインファミリーを指定します。

スキャンが作成され起動されると、Tenable Web App Scanning はさまざまなプラグインファミリーのプラグインを使用します。それぞれが特定のタイプの検出結果または脆弱性を特定して、ウェブアプリケーションを分析するように設計されています。Tenable Web App Scanning では、98000 ~ 98999 と 112290 ~ 117290 のプラグイン ID 範囲をスキャンに使用します。Tenable Web App Scanning プラグインファミリーの詳細については、Tenable Web App ScanningTenable Web App Scanning プラグインファミリーサイトを参照してください。

注意：Tenable Web App Scanning には、スキャンごとに各プラグインの最初に検出された 25 のインスタンスのみがスキャン結果に表示されます。スキャン結果に 1 つのプラグインの 25 のインスタンスが表示された場合は、修正ステップを実行して対応する脆弱性を解決してから、ターゲットを再スキャンすることをお勧めします。

スキャンまたはユーザー定義スキャンテンプレートを作成し、**[API]**、**[概要]**、**[(基本) スキャン]**、**[標準スキャン]**、**[カスタム]** のテンプレートまたはスキャンタイプを選択するときに、**[プラグイン]** の項目を設定できます。詳細については、スキャンプラグインの表示を参照してください。

ヒント: 設定を保存して他のスキャンに適用したい場合は、ユーザー定義スキャンテンプレートを作成して設定できます。

プラグインの設定には次のセクションがあります。

- すべて有効
- プラグインの表

すべて有効

クリックしてすべてのプラグインの有効または無効を同時に切り替えます。

プラグインの表

列	説明	アクション
名前	グループ化されたプラグインが属するプラグインファミリーを指定します。	• 各プラグインファミリーの名前を表示します。 • 列を選択して、表をアルファベット順またはファミリー名ごとにソートします。
合計	プラグインファミリーのプラグインの数を指定します。	• ファミリー内のプラグインの数を表示します。 • 列を選択して、各ファミリーのプラグインの数で表をソートします。
ステータス	ターゲット分析するためにプラグインファミリーのプラグインをスキャナーで使用するかどうかを指定するトグルです。	• **[ステータス]**トグルをクリックし、プラグインファミリーのプラグインを無効にします。 • (オプション) 無効になったプラグインファミリーを有効にするには、**[ステータス]**トグルをクリックします。

プラグインの表で、個別のプラグインの詳細を表示したり無効にしたりすることができます。

個別のプラグインに関する詳細を表示する方法

1. 表で、表示するプラグインが含まれているファミリーの行をクリックします。

   プラグインファミリーの詳細ペインが表示され、ファミリー内の各プラグインの名前、ID、およびステータスがページ分割されたリストが表示されます。

2. (オプション) 特定のプラグインを見つけるには、**[検索]**ボックスに名前または ID を入力します。
3. 詳細を表示するプラグインをクリックします。

個別のプラグインを無効にする方法

1. 表で、無効にするプラグインが含まれているファミリーの行をクリックします。

   プラグインファミリーの詳細ペインが表示され、ファミリー内の各プラグインの名前、ID、およびステータスがページ分割されたリストが表示されます。

2. (オプション) 特定のプラグインを見つけるには、**[検索]** ボックスに名前または ID を入力します。

3. **[ステータス]** 列で、無効にするプラグインの横にあるチェックボックスを選択します。

4. (オプション) 無効になったプラグインを有効にするには、このチェックボックスを選択します。

5. **[保存]** をクリックします。

   詳細プレーンが消去されます。

   Tenable Web App Scanning によってプラグインの選択が更新されます。

Tenable Web App Scanning スキャンの認証情報

注意: このセクションのトピックでは、新しいインターフェースでの認証情報についてのみ説明します。新しいインターフェースをアクティブにした場合、従来のインターフェースで設定した過去の認証情報のスナップショットを表示できますが、それらの認証情報を変更することはできません。

Tenable Web App Scanning スキャンでは、Tenable Web App Scanning でウェブアプリケーションの認証スキャンを実行できるように認証情報を設定することができます。認証されたスキャンを設定することで、認証されていないスキャンよりも広範なチェックを実行できるようになり、スキャン結果がより正確になります。

Tenable Web App Scanning のスキャンは管理された認証情報を使用します。管理された認証情報によって、認証情報の設定を認証マネージャーで一元的に保存できます。その後、これらの認証情報設定を、スキャンごとに認証情報を設定する代わりに、複数のスキャン設定に追加できます。

Tenable Web App Scanning スキャンでは、次の認証タイプの認証情報がサポートされています。

- HTTP サーバー認証
- ウェブアプリケーション認証
- クライアント証明書認証

ヒント: API スキャンテンプレートを使用して API をスキャンするときに、API 認証にキーまたはトークンが必要な場合は、**[HTTP設定]** セクションの [詳細] 設定で、必要になるカスタムヘッダーを追加することができます。

次の方法を使用して Tenable Web App Scanning スキャンで認証情報を設定することができます。

認証情報のカテゴリ	認証タイプ	設定方法
HTTP サーバー認証	–	Tenable Web App Scanning のユーザーインターフェースを使用して、スキャンの認証情報を手動で設定します。
ウェブアプリケーション認証	ログインフォーム	
	Cookie 認証	
	Selenium 認	次のいずれかを行います。

	証	◦ Chrome の Selenium IDE (Integrated Development Environment) 拡張機能を使用して、認証情報を記録し、Tenable Web App Scanning ユーザーインターフェースを使用して認証情報をスキャンに手動で追加します。 **注意:** Chrome の Selenium IDE 拡張機能の詳細については、Google Chrome のドキュメントを参照してください。 ◦ Tenable Web App Scanning Chrome 拡張機能 を使用して認証情報を記録し、スキャン設定に認証情報を自動的に追加します。 **ヒント:** Tenable Web App Scanning で使用する Selenium スクリプトの詳細については、Tenable Web App Scanning の Selenium コマンドを参照してください。
	API キー ベアラー認証	Tenable Web App Scanning のユーザーインターフェースを使用して、スキャンの認証情報を手動で設定します。
クライアント証明書認証	-	Tenable Web App Scanning のユーザーインターフェースを使用して、スキャンの認証情報を手動で設定します。

Tenable Web App Scanning スキャンで認証情報を設定する

必要な Tenable Web App Scanning ユーザーロール: スキャンマネージャーまたは管理者

始める前に

- (Cookie 認証) スキャンするウェブアプリケーションの Cookie 認証の認証情報を特定します。
- (Selenium 認証) Chrome ウェブストアで Selenium IDE 拡張機能をダウンロードし、次のいずれかを実行します。
  - Selenium IDE 拡張機能を使用して認証情報を設定するには、Selenium IDE 拡張機能をダウンロードします。
  - Tenable Web App Scanning Chrome 拡張機能 を使用して認証情報を設定するには、Tenable Web App Scanning Chrome 拡張機能 をダウンロードします。

Tenable Web App Scanning スキャンで認証情報を設定する方法

1. スキャンを作成または編集します。
2. **[認証情報]** をクリックします。

   認証情報の詳細が表示されます。
3. **[認証情報の追加]** の横にある ⊕ ボタンをクリックします。

   [認証情報タイプの選択] プレーンが表示されます。
4. 次のいずれかを行います。
   - 既存の認証情報を追加する

     [認証情報タイプの選択] の **[管理された認証情報]** プレーンには、**[使用可能]** または **[編集可能]** のアクセス許可を持つ認証情報が含まれています。

     a. (オプション) リストで管理された認証情報を検索するには、テキストボックスに検索条件を入力し、🔍 ボタンをクリックします。

b. **[管理された認証情報]** セクションで、追加する管理された各認証情報をクリックします。

[認証情報タイプの選択] プレーンは開いたままになります。

c. **[認証情報タイプの選択]** プレーンを閉じるには、プレーンの右上にある ✕ ボタンをクリックします。

- 新しい認証情報を作成する

a. **[ウェブアプリケーション認証]** セクションで、作成する認証情報タイプをクリックします。

- **HTTP Server Application**
- **ウェブアプリケーション認証**

該当する認証情報のタイプの設定プレーンが表示されます。

b. 1つ目のテキストボックスに、認証情報の名前を入力します。

c. (オプション) 2番目のテキストボックスに、認証情報の説明を入力します。

d. 認証情報タイプの設定を設定します。

- **HTTP Server Application**
- **ウェブアプリケーション認証**

5. ユーザーアクセス許可を追加します。
6. **[保存]** をクリックして、認証情報の変更を保存します。

Tenable Web App Scanning により設定プレーンが閉じられ、認証情報がスキャンの認証情報の表に追加されます。

新しい認証情報を作成した場合は、Tenable Web App Scanning によってその認証情報が認証マネージャーに追加されます。

7. **[保存]** をクリックして、スキャンの変更を保存します。

Selenium 認証情報の設定を自動的に設定する

必要な追加ライセンス: Tenable Web App Scanning

Tenable Web App Scanning Chrome 拡張機能 を使用して、Selenium 認証情報を記録し、それらの認証情報を新しいスキャンまたは既存のスキャンに自動的に追加することができます。

注意: Tenable Web App Scanning Chrome 拡張機能 は、ウェブアプリケーションスキャンの Selenium 認証情報の設定のみを更新します。その他のスキャンオプションは、Tenable Web App Scanning Chrome 拡張機能 インターフェースを使用して設定する必要があります。

始める前に

- Chrome ウェブストアから Tenable Web App Scanning Chrome 拡張機能 をダウンロードします。
- Log in to Tenable Vulnerability Management の説明に従って、Tenable Vulnerability Management にログインします。

Tenable Web App Scanning Chrome 拡張機能 を使用して Selenium 認証情報を記録する方法

1. ブラウザの右上の Tenable Vulnerability Management ロゴをクリックします。

   Tenable Web App Scanning Chrome 拡張機能の **[スキャンを作成する]** ウィンドウが表示されます。

2. 次のいずれかを行います。

タスク	アクション
Selenium 認証情報を既存のスキャンに記録および追加する	• **[既存のスキャンに追加する]** をクリックします。 **[既存のスキャンに追加する]** ウィンドウが表示され、既存のスキャンのリストが表示されます。 • 検索ボックスに、Selenium 認証情報を追加するスキャンの名前を入力します。 • 🔎ボタンをクリックします。

	Tenable Web App Scanning Chrome 拡張機能 によって、入力した名前でリストがフィルタリングされます。 • Selenium 認証情報を追加するスキャンをクリックします。
Selenium 認証情報を新しいスキャンに記録および追加する	• **[新規のスキャンを作成する]** をクリックします。 **[新規スキャン]** ウィンドウが表示されます。 • **[名前]** ボックスにスキャンの名前を入力します。 • **[URL]** ボックスに、スキャンするウェブアプリケーションのターゲットを URL 形式で入力します。

3. **[次へ]** をクリックします。

   スキャンターゲットとして指定したリンクが拡張機能によって開かれます。

4. **[記録]** をクリックします。

   Tenable Web App Scanning Chrome 拡張機能 によってセッションの記録が開始されます。

   記録が開始されたことを示すメッセージが表示されます。

5. ウェブアプリケーションを認証するために使用するログイン手順を実行します。

6. システムに正常に認証した後で、正常に認証されたときにのみ表示されるウェブページ上のテキスト (たとえば [**Welcome,** [ユーザー名]**!**]) をハイライトします。

7. 右下の **[完了]** をクリックします。

8. (オプション) 記録したログイン手順を再生するには、**[再生]** をクリックします。

9. 認証ログイン手順を正常に記録した後で、**[保存]** をクリックします。

   Tenable Web App Scanning Chrome 拡張機能 が認証を保存してスキャンにインポートします。

次の手順

- Tenable Web App Scanning Chrome 拡張機能 を使用して新しいスキャンを作成した場合は、Tenable Web App Scanning Chrome 拡張機能 インターフェースで他のオプションを設定する必要があります。

Tenable Web App Scanning の Selenium コマンド

Tenable Web App Scanning の Selenium コマンドは、認証およびクロールのスクリプトを記録するために使用されます。これにより、ユーザーは特定のシナリオで何を実行するかをスキャナーに正確に指示できるようになります。これらのコマンドは、Selenium IDE 拡張機能と Tenable Web App Scanning Chrome 拡張機能 の両方で実行できます。どちらも Chrome ウェブストアでダウンロードできます。

Tenable Web App Scanning の Selenium コマンドのサポートについては、以下に詳述します。

サポートされているコマンド	サポートされていないコマンド
• addSelection • answerOnNextPrompt • assert • assertAlert • assertChecked • assertConfirmation • assertEditable • assertElementNotPresent • assertElementPresent • assertNotChecked • assertNotEditable • assertNotSelectedValue • assertNotText • assertPrompt • assertSelectedLabel • assertSelectedValue • assertText • assertTitle	• close • debugger • do • else • else if • end • execute async script • execute script • for each • if • repeat if • run • select window • store • store attribute • store json • store text • store title

- assertValue
- check
- chooseCancelOnNextConfirmation
- chooseCancelOnNextPrompt
- chooseOkOnNextConfirmation
- click
- clickAt
- doubleClick
- doubleClickAt
- echo
- editContent
- mouseDown
- mouseDownAt
- mouseMoveAt
- mouseOut
- mouseOver
- mouseUp
- mouseUpAt
- open
- pause
- removeSelection
- runScript
- select
- selectFrame

- store value
- store window handle
- store xpath count
- times
- while

- sendKeys

  > **注意：** sendKeys コマンドは、任意のテキストに加えて以下のエスケープシーケンスのみをサポートします。
  >
  > - `${KEY_ENTER}`
  > - `${KEY_DELETE}`
  > - `${KEY_BACKSPACE}`

- setSpeed
- setWindowSize
- submit
- type
- uncheck
- verify
- verifyChecked
- verifyEditable
- verifyElementNotPresent
- verifyElementPresent
- verifyNotChecked
- verifyNotEditable
- verifyNotSelectedValue
- verifyNotText
- verifySelectedLabel
- verifySelectedValue
- verifyText
- verifyTitle

• verifyValue • waitForElementEditable • waitForElementNotEditable • waitForElementNotPresent • waitForElementNotVisible • waitForElementPresent • waitForElementVisible • webdriverAnswerOnNextPrompt • webdriverAnswerOnVisiblePrompt • webdriverChooseCancelOnNextConfirmation • webdriverChooseCancelOnNextPrompt • webdriverChooseCancelOnVisibleConfirmation • webdriverChooseCancelOnVisiblePrompt • webdriverChooseOkOnNextConfirmation • webdriverChooseOkOnVisibleConfirmation	

Tenable Web App Scanning スキャンでの HTTP サーバー認証設定

Tenable Web App Scanning スキャンでは、HTTP サーバーベースの認証の認証情報に関する次の項目を設定できます。

オプション	アクション
ユーザー名	Tenable Web App Scanning で HTTP ベースのサーバーを認証するために使用するユーザー名を入力します。
パスワード	Tenable Web App Scanning で HTTP ベースのサーバーを認証するために使用するパスワードを入力します。
認証タイプ	ドロップダウンリストで、次の認証タイプのいずれかを選択します。 • **Basic/Digest** • **NTLM** • **Kerberos**
Kerberos ドメイン	(Kerberos 認証タイプを有効にする場合に必要) Kerberos ターゲット認証が属する領域 (該当する場合)。
キー配布センター (KDC)	(Kerberos 認証タイプを有効にする場合に必要) このホストが、ユーザーのセッションチケットを提供します。

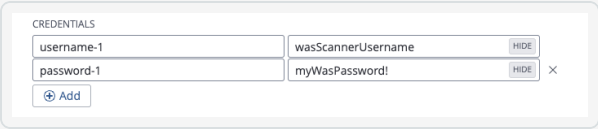
注意: Tenable Web App Scanning は、単一のターゲットに対する複数の HTTP 認証タイプをサポートしていません。

ウェブアプリケーション認証

Tenable Web App Scanning スキャンで、次のいずれかのタイプの**ウェブアプリケーション認証**の認証情報を設定できます。

- ログインフォーム認証
- Cookie 認証
- Selenium 認証
- API キー認証
- ベアラー認証

ログインフォーム認証

オプション	アクション
Authentication Method (認証方法)	ドロップダウンボックスで、**[ログインフォーム]** を選択します。
ログインページ	スキャンするウェブアプリケーションのログインページの URL を入力します。
認証情報	ターゲットのログインフォームの各フィールド (ユーザー名、パスワード、ドメインなど) について、次のように認証情報エントリに入力します。 a. 左側のテキストボックスに、ログインフィールドの名前または ID HTML DOM 属性の値を入力します。 b. 行の右側のテキストボックスに、ログイン時にそのテキストフィールドに挿入するリテラル値を入力します。 典型的な設定の例 

	ヒント: テキストフィールドの名前または ID HTML DOM 属性を表示するには、テキストフィールドを右クリックし、Firefox または Chrome ブラウザで [検査] を選択します。 **ヒント:** 認証情報なしの **[概要]** スキャンを実行する場合、プラグイン 98033 (**[ログインフォームが検出されました]**) が、必要なログインボックスを自動的に検出してプラグインの出力にそれを表示することがあります。
正常な認証を検証するためのパターン	認証が成功した場合にのみウェブサイトに表示される単語、語句、または正規表現を入力します (たとえば、**ようこそ**、*[ユーザー名]* さん!)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。
アクティブなセッションを確認するためのページ	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します (たとえば、**こんにちは**、*[ユーザー名]* さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

Cookie 認証

オプション	アクション
Authentication Method (認証方法)	ドロップダウンボックスで、**[Cookie 認証]** を選択します。
セッション Cookie	次を実行します。 a. 最初のテキストボックスで、Cookie 認証の認証情報の名前を入力します。 b. 2 番目のテキストボックスに、Cookie 認証の認証情報の値を入力します。
アクティブなセッションを確認するため	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。

のページ	
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します(たとえば、**こんにちは**、*[ユーザー名]*さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に `.*` は必要ありません。

Selenium 認証

オプション	アクション
Authentication Method(認証方法)	**[Selenium 認証]**を選択します。
Selenium Script (.side)	次を実行します。 a. Selenium IDE 拡張機能で、認証の認証情報を Selenium IDE 拡張機能に記録します。 b. **[ファイルの追加]**をクリックします。 お使いのオペレーティングシステムのファイルマネージャーが表示されます。 c. Selenium 認証情報 `.side` ファイルに移動して選択します。 Tenable Web App Scanning によって認証情報ファイルがインポートされます。
アクティブなセッションを確認するためのページ	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します(たとえば、**こんにちは**、*[ユーザー名]*さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に `.*` は必要ありません。

API キー認証

オプション	アクション
認証方法	**API キー**を選択します。
ヘッダー	次を実行します。 a. 最初のテキストボックスに、HTTP ヘッダーの名前を入力します。 b. 2 番目のテキストボックスに、HTTP ヘッダーの値を入力します。 c. (オプション) ⊕ ボタンをクリックしてヘッダーを追加します。
アクティブなセッションを確認するためのページ	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します (たとえば、**こんにちは**、*[ユーザー名]* さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

ベアラー認証

オプション	アクション
認証方法	**[ベアラー認証]** を選択します。
ベアラートークン	ベアラートークンの値を入力します。 **注意**: ベアラートークンは OAuth の一部です。Tenable Web App Scanning が OAuth をサポートするのは、OAuth が OpenIDConnect に含まれ、selenium スクリプトを介して記録可能な場合です。OpenIDConnect に含まれない OAuth の実装は、トークンが動的であるか、または認証目的で特別な静的 (非動的) トークンを作成した場合にのみサポートされます。
アクティブなセッションを確認するため	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。

のページ	
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します（たとえば、**こんにちは**、*[ユーザー名]*さんなど）。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

クライアント証明書認証

Tenable Web App Scanning スキャンで、**クライアント証明書認証**の認証情報を設定できるようになりました。

オプション	アクション
クライアント証明書	ホストとの通信に使用される PEM 形式の証明書を含むファイル。
クライアント証明書のプライベートキー	クライアント証明書の PEM 形式のプライベートキーを含むファイル。
クライアント証明書のプライベートキーのパスフレーズ	プライベートキーのパスフレーズ(必要な場合)。
正常な認証を検証するためのページ	Tenable Web App Scanning が認証されたセッションを検証するためにアクセスできる URL を入力します。
正常な認証を検証するためのパターン	認証が成功した場合にのみウェブサイトに表示される単語、語句、または正規表現を入力します(たとえば、ようこそ、[ユーザー名]さん!)。先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

スキャンの詳細の表示

必要なスキャンのアクセス許可: 表示可

所有しているウェブアプリケーションのスキャン、または所有者により共有されているスキャンのスキャン結果を表示することができます。

個別のウェブアプリケーションのスキャンの詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. スキャンの表で、詳細を表示するスキャンをクリックします。

   [スキャンの詳細] ページが表示されます。デフォルトでは、このページには最後に実行されたスキャンの詳細が表示されます。

4. 次のいずれかを行います。

セクション	アクション
表ヘッダー	• スキャン設定を編集します。 • スキャンを [ゴミ箱] フォルダーに移動します。
深刻度の概要	現在表示されてるスキャンジョブについて、**[重大]**、**[高]**、**[中]**、または **[低]** の脆弱性重大度の脆弱性の数を表示します。
[スキャンの詳細] セクション	現在表示されているスキャンジョブについて、次の詳細を表示します。 • **ステータス** - スキャンのステータス • **開始時刻** - スキャンの開始日時 • **テンプレート** - スキャンを設定および実行するために使用したスキャンテンプレート

	• **終了時刻** - スキャンの終了日時 • **スキャナー** - スキャンを実行したスキャナー • **ターゲット** - スキャンが評価するターゲット

[プラグイン別の脆弱性] タブ	現在表示されているスキャンジョブについて、プラグイン別に整理された脆弱性データを表示します。
	
	このタブでは、次のことを実行できます。
	• 各脆弱性に関する情報を表示します。
	  • 深刻度アイコン - 脆弱性の深刻度
	  • **名前** - 共通脆弱性識別子 (CVE) システムで定義された脆弱性の名前
	  • **ファミリー** - プラグインファミリー
	  • **脆弱性** - 脆弱性インスタンスの数
	  ヒント: 脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、脆弱性 URL および脆弱性を識別するために入力された情報によって一意的に識別されます。
	• 並べ替え、ページ当たりの行数の増減、または表の別のページに移動します。Tenable Web App Scanning の表を参照してください。
	• 脆弱性の詳細を表示するには、その脆弱性の行をクリックします。
	  [脆弱性の詳細] ページが表示されます。
	  [脆弱性の詳細] ページで、プラグインの添付ファイルを表示して、各プラグインに関する詳細を表示できます。

[注記] タブ	現在表示されているスキャンジョブについて、Tenable Web App Scanning がスキャンの成功および効率に関する文脈を提供するために生成したスキャンの注記を表示します。 より効果的な結果が得られるようなスキャン設定をスキャナーがスキャン中に識別した場合のみ、**[注記]** タブが表示され、スキャンの注記が表示されます。

	このタブでは、次のことを実行できます。 • スキャンの注記に関する情報を表示します。 • **深刻度** - スキャンのパフォーマンスに対する検出結果の深刻度を数量化するために使用されるメトリクス。**[重大]**、**[高]**、**[中]**、**[低]**、または **[情報]** として表示されます。スキャンの注記の脆弱性メトリクスの詳細については、深刻度の詳細のスキャンの注記 を参照してください。 • **スキャンの注記** - スキャンの注記のわかりやすいタイトル。 • **説明** - スキャンの検出結果に関する詳細情報、トラブルシューティングのアドバイス、および全体的なスキャンの品質を向上させるための提案。
[履歴] タブ	スキャンの履歴を表示します。 このタブには、スキャンの実行履歴が表で表示されます。現在 **[スキャンの詳細]** ページに表示されているスキャンの実行に対して、Tenable Web App Scanning により **[最新]** というラベルが追加されます。デフォルトで、最も最近実行されたスキャンに **[最新]** ラベルが追加されます。 **注意:** [履歴] タブの履歴表示は、インポートされたスキャンや設定済みでもまだ実行されていないスキャンは対象になりません。 このタブでは、次のことが実行できます。 • 実行されたスキャンの各回についての概要情報を表示します。 • **作成日** - スキャンの作成が開始された日時 • **開始時刻** - スキャナーによってスキャンが開始された日時 • **終了時刻** - スキャンが完了した日時 • **所要時間** - スキャンの所要時間 **注意: [継続期間]** の時間には、Tenable Web App Scanning でスキャンを実行して結果を処理するためにかかった時間、およびス

	キャンが **[保留中]** ステータスだった時間が含まれます。 結果として、**[継続期間]** の時間は、[詳細設定] で指定した **[スキャン全体の最大時間]** とは異なります。こちらはスキャンの実行時間にのみ適用されます。 • **ステータス** - スキャンのステータス • 表に表示されるデータをフィルタリングします。 • 表をソートするか表の別のページに移動します。詳細は、Tenable Web App Scanning の表 を参照してください。 • 表のスキャンジョブの行をクリックすると、過去のスキャンの詳細が表示されます。 Tenable Web App Scanning は選択されたスキャンジョブに **[最新]** とマーキングし、**[スキャンの詳細]** セクションを更新して選択されたジョブのデータを表示します。

スキャンステータス

Tenable Web App Scanning では、スキャンはその状態に応じて、次のステータスの値を持つことができます。

注意: Tenable Web App Scanning スキャン進捗インジケーターのパーセンテージは、スキャンの完了したタスクのパーセンテージを表します。1 つのタスクしかないスキャンでは、スキャンが完了するまで進捗状況が 0% と表示されます。

ヒント: Tenable Web App Scanning スキャンでは、スキャンステータスにカーソルを合わせるとポップアップウィンドウが表示され、スキャンされたターゲットの数や経過時間または最終スキャン時間など、より多くのステータス情報が示されます。ウィンドウには、スキャンの現在のステータスに基づいて異なる情報が表示されます。

ステータス	説明
Tenable Web App Scanning スキャン	
中止	スキャナーがスキャンの直近のスキャンジョブを完了しませんでした。ジョブが 4 時間以上実行されずにキューに入れられていたために Tenable Web App Scanning がスキャンジョブを中止したか、Tenable Web App Scanning またはスキャナーで他の問題が発生したためにスキャンを中止した可能性があります。 Tenable Web App Scanning がスキャンを中止した理由の詳細については、スキャンの注記を表示するを参照してください。
キャンセル	ユーザーのリクエストにより、Tenable Web App Scanning が最後のスキャンジョブを正常に停止しました。
完了	スキャナーがスキャンの直近のスキャンジョブを完了しました。
Never Run	スキャンが、空であるか(新規もしくは実行前)、保留中 (Tenable Web App Scanning がスキャンの実行リクエストを処理中) のどちらかです。
Pending	Tenable Web App Scanning がスキャンを開始キューに入れました。 **注意:** Tenable Web App Scanning は、4 時間以上 **保留中** ステータスになったままのスキャンを中止します。Tenable Web App Scanning によってスキャンが中止された場合は、重複するスキャンの数が減るようにスキャンのスケジュールを変更してください。問題が解決しない場合は、Tenable サポート にお問い合わせください。

ステータス	説明
処理	スキャンが完了しましたが、結果はまだ処理中になっています。スキャナーは、脆弱性の検出結果、添付ファイル、メモ、およびその他のメタデータを処理しています。
Running	スキャナーが現在スキャンを実行中です。
Stopping	スキャナーは停止リクエストを受け、停止しています。

スキャンの進行状況を表示する

必要な追加ライセンス: Tenable Web App Scanning

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

必要なスキャンのアクセス許可: 制御可

Tenable Web App Scanning スキャンを起動するときに、実行されるスキャンの進行状況を表示できます。スキャンの進行状況情報は履歴データを基にしているので、Tenable Web App Scanning スキャンの進行状況データは履歴スキャンに対してのみ表示されます。

Tenable Web App Scanning スキャンのスキャン進行状況を表示する方法

1. 既存のスキャンを起動します。

   スキャンのステータスが **[ステータス]** 列に表示されます。

2. ステータスが **[保留中]** から **[実行中]** に変わった後に、スキャンステータスの横に、次のスキャン進行状況インジケーターが表示されます。

進行状況インジケーター	説明
割合	スキャナーが完了したスキャンジョブの状況が、予想される全体のスキャン時間の割合として表示されます。
推定時間	スキャナーがスキャンを完了するまでの残りの予測時間が分単位で表示されます。
超過時間	以前のスキャンジョブと比較して、スキャンジョブにかかっている余分な時間。このインジケーターは、当該スキャンが以前のスキャンより時間がかかっている場合にのみ表示されます。
進行状況バー	スキャナーがスキャンを完了するまでの残り時間の視覚的なインジケーター。スキャンが完了するか他の理由で停止した場合 (たとえば、Tenable Vulnerability

	Management がスキャンを停止した場合)、進行状況バーは非表示になります。

実行中でない Tenable Web App Scanning スキャンのスキャン進行状況を表示するには、スキャンステータスをご覧ください。

深刻度の詳細のスキャンの注記

Tenable Web App Scanning は、次の表で説明されている深刻度のレベルを使用して、スキャン結果に表示されるスキャンの注記を分類します。

レベル	説明	例
緊急	スキャンがウェブアプリケーションの可用性または正常な動作に影響を与えた可能性があることを説明する情報。 スキャンの注記のタイトルは赤で表示されます。	**サービスがが応答しなくなりました** - 非常に多くの連続するリクエストタイムアウトの発生後、スキャナーがスキャンを中止しました。スキャン結果が不完全な可能性があります。ターゲットが破損または使用不可能になっていないことを確認する必要があります。 Tenable では、繰り返しのタイムアウトを調べて、スキャナーが送信したリクエストをターゲットがサポートできない理由を特定することを推奨します。場合によってはスキャンテンプレートでパフォーマンス設定を緩和する必要があります。
高	スキャナーがウェブアプリケーションターゲットの分析を完了する前にスキャンが予期せず停止したことを説明する情報。結果として、スキャンはウェブアプリケーションの脆弱性を十分に分析しなかったため、ユーザーはトラブルシューティングを行ってスキャンを再試行する必要があります。 スキャンの注記のタイトルは黄色で表示されます。	**スキャンのクラッシュ** - 予期しない理由でスキャンがクラッシュしました。結果として、スキャン結果がないか未完了です。
中	スキャン結果が欠落また未完了である理由を説明する情報。情報は通常、設定ミスのために開始できなかったスキャンに関したものです。ウェブアプリケーションは影響を受けません。	**範囲外の URL** - ターゲット URL が、スキャンテンプレートの設定で指定されたいずれかの範囲除外条件と一致しているために、スキャナーがターゲット URL をスキャンしませんでした。

	スキャンの注記のタイトルは白黒で表示されます。	
低	スキャン実行時間中のバリエーションを説明する情報。検出結果は、ウェブアプリケーションまたはスキャン結果に影響しません。 スキャンの注記のタイトルは緑で表示されます。	**ターゲットの応答が切り捨てられました** - ターゲットのスキャン結果が、スキャン設定で指定されている **[最大応答サイズ]** を超えています。結果として、コンテンツが切り捨てられ、そのためにデータ収集および評価エラーが発生しました。
情報	スキャン結果に影響しないが、より効率的にスキャン設定をするために役立つ可能性がある情報。 スキャンの注記のタイトルは青で表示されます。	**認証が検出されました** - スキャナーが、HTTP サーバーの認証またはログインフォームを検出しました。スキャナーがより多くのページにアクセスできるようにするための認証情報を設定できます。

スキャンフィルター

[スキャン] ページでは、Tenable 提供のフィルターを使って Tenable Web App Scanning スキャンをフィルタリングできます。

フィルター	説明
作成日	スキャン設定が作成された日付です。
説明	スキャン設定の説明です。
完了日	スキャンが最後に完了した日付です。
最終変更日	スキャン設定が最後に変更された日付です。
最終スキャン日	スキャンが最後に実行された日付です。
名前	スキャン設定の名前です。
スケジュール	スキャンスケジュールが有効かオンデマンドかでフィルタリングします。
ステータス	スキャンのステータスです。スキャンステータスに関する詳細は、Scan Status を参照してください。
ターゲット	スキャンの起動に使用されるターゲット URL です。
テンプレート	スキャン設定のベースとなった Tenable 提供のスキャンテンプレートです。
ユーザーテンプレート	スキャン設定のベースとなったユーザー定義スキャンテンプレートです。

スキャン設定のコピー

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

スキャンの設定をコピーすると、Tenable Web App Scanning はコピーの作成者にそのコピーに対する所有者のアクセス許可を割り当て、元のスキャンからのコピーのスキャンのアクセス許可を割り当てます。

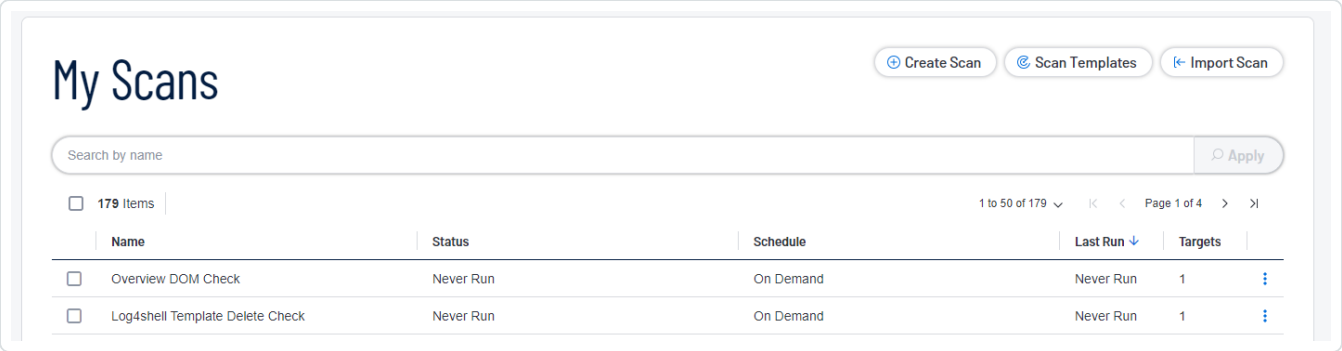
スキャン設定をコピーする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   Tenable Web App Scanning で **[マイスキャン]** ページが表示されます。



3. 行にある ⋮ ボタンをクリックします。

   オプションのドロップダウンボックスが表示されます。

4. **[コピー]** をクリックします。

   [フォルダへのコピー] プレーンが表示されます。ここにはスキャンフォルダーのリストが含まれます。

5. コピーを保存するフォルダーをクリックします。

6. **[コピー]** をクリックします。

   [スキャンは正常にコピーされました] メッセージが表示され、Tenable Web App Scanning は、スキャンのコピーを作成し、その名前の末尾に「*- コピー*」を付けます。そして、そのコピーの作成者に所有者のアクセス許可を与えます。選択したフォルダーのコピーがスキャンの表に表示されます。

スキャン結果のエクスポート

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

必要なスキャンのアクセス許可: 表示可

インポートされたスキャン結果、および Tenable Web App Scanning がスキャナーから直接集めた結果の両方をエクスポートすることができます。

Tenable Web App Scanning は、個別のスキャン結果を 15 か月が経過するまで保持します。

注意: フィルターは Tenable Web App Scanning のエクスポートには適用できません。すべての結果がエクスポートされます。

注意: アーカイブされたスキャン結果 (すなわち、35 日よりも前の結果) では、エクスポート形式は `.nessus` および `.csv` ファイルに限定されます。

注意: スキャンがアクティブに実行中の場合、Tenable Vulnerability Management インターフェースに **[エクスポート]** ボタンは表示されません。スキャンが完了するのを待ってから、スキャン結果をエクスポートしてください。

新しいインターフェースで個別のスキャン結果をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

3. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

4. 次のいずれかを行います。

場所	エクスポートの範囲
スキャンの表	a. スキャンの表で、エクスポートするスキャンにカーソルを合わせます。 b. ⋮ ボタンをクリックします。 メニューが表示されます。 c. ↦**[エクスポート]** をクリックします。 **[エクスポート]** プレーンが表示されます。
スキャンの詳細	a. スキャンの表で、エクスポートするスキャンをクリックします。 b. スキャン名の横にある ↦**[エクスポート]** をクリックします。 **[エクスポート]** プレーンが表示されます。

5. エクスポート形式を選択します。

形式	説明	アーカイブされたスキャン結果に対応
Tenable Web App Scanning		
HTML	ターゲット、スキャン結果、スキャンの注記のリストを含むウェブベースの `.html` ファイル。	該当なし
PDF	ターゲット、スキャン結果、スキャンの注記のリストを含む Adobe `.pdf` ファイル。 **注意:** Tenable Vulnerability Management では、40 万件を超える個別のスキャン結果を含む PDF ファイルはエクスポートできません。	該当なし
Nessus	XML フォーマットの `.nessus` ファイル。ターゲットのリスト、ユーザーが定義したスキャンの設定、およびスキャン結果が含まれます。パ	該当なし

	スワード認証情報は、XML にプレーンテキストとしてエクスポートされないように削除されます。 **注意:** .nessus ファイル形式については、Nessus File Format (Nessus ファイル形式) を参照してください。	
CSV	スキャン結果のみを含む .csv テキストファイル。	該当なし
JSON	ターゲットのリスト、ユーザーが定義したスキャンの設定、スキャン結果が含まれる、.json ファイル。パスワード認証情報は、.json ファイルにプレーンテキストとしてエクスポートされないように削除されます。	該当なし
ZIP	指定された Tenable Web App Scanning スキャンのデバッグ情報を含む .zip ファイルを返します。ZIP ファイルには、ブラウザコンソールのログ、HTTP リクエストと応答、および該当する場合は Selenium の情報が含まれています。	○

6. Tenable Vulnerability Management スキャンでは、**[PDF - カスタム]** または **[HTML - カスタム]** 形式を選択した場合、

   - 既定の **[データ]** 設定を維持します (**[脆弱性]** が選択されています)。
   - エクスポートファイルでスキャン結果をグループ化する方法に応じて、**[グループ化]** リストから **[資産]** または **[プラグイン]** のいずれかを選択します。

7. **[エクスポート]** をクリックします。

   Tenable Vulnerability Management によりエクスポートファイルが作成されます。ブラウザの設定によっては、ブラウザがエクスポートファイルを自動的にコンピューターにダウンロードするか、続行する前にダウンロードの確認を促すメッセージを表示されます。

Tenable Web App Scanning スキャンのインポート

必要な Tenable Web App Scanning ユーザーロール: スキャンマネージャーまたは管理者

新しいインターフェースで Tenable Web App Scanning スキャンをインポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   [マイスキャン] ページが表示されます。

3. ページの右上にある **[スキャンをインポートする]** をクリックします。

   ファイルディレクトリが表示されます。

   注意: Tenable Web App Scanning スキャンのインポートでは `.json` ファイルタイプのみがサポートされています。

4. インポートするスキャンファイルを参照して選択します。

5. **[開く]** をクリックします。

   注意: **[キャンセル]** をクリックすると、インポートをキャンセルします。

   [スキャン] ページが表示され、インポートしたスキャンが表に表示されます。

   注意: スキャンの表で **[最終更新日]** 行をクリックすると、インポートしたスキャンがスキャンリストの一番上に表示されます。

   Tenable Web App Scanningは、インポートされたスキャン結果の処理を開始します。処理が完了すると、インポートされたデータは個別のスキャン詳細および集計されたデータビュー(ダッシュボードなど)に表示されます。インポートされたファイルのサイズによっては、このプロセスに最大 30 分かかる可能性があります。

   ヒント: 十分と思われる処理時間が経過しても、インポートされたデータが個別のスキャン結果や集計されたデータビューに表示されない場合は、アクセスグループ内でインポートされたターゲットに対する適切なアクセス許可が割り当てられていることを確認してください。

スキャンフォルダーへのスキャンの移動

必要なスキャンのアクセス許可: 表示可

スキャンをデフォルトフォルダーから**[マイスキャン]**デフォルトフォルダー、またはカスタムスキャンフォルダーに移動できます。またスキャンを、カスタムフォルダーから**[マイスキャン]**デフォルトフォルダーに、または別のカスタムフォルダーに移動することもできます。

スキャンを**[すべてのスキャン]**デフォルトフォルダーから移動すると、そのスキャンは選択したフォルダーと**[すべてのスキャン]**フォルダーの両方に表示されます。

スキャンを**[マイスキャン]**デフォルトフォルダーから移動すると、そのスキャンはカスタムフォルダーにのみ表示されます。

スキャンをゴミ箱に移動する方法に関する詳細は、Move a Scan to the Trash Folderを参照してください。

スキャンをスキャンフォルダーに移動する方法

1. 左上にある☰ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]**をクリックします。

   [マイスキャン]ページが表示されます。

3. **[フォルダー]**セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

4. スキャンの表で、移動するスキャンにカーソルを合わせます。

5. 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。

6. メニューで**[移動]**をクリックします。

   [フォルダーに移動]プレーンが表示されます。このプレーンにはスキャンフォルダーのリストが含まれます。

7. フォルダーを検索します。

    a. 検索ボックスにフォルダー名を入力します。

    b. 🔎 ボタンをクリックします。

        Tenable Web App Scanning がリストを制限して、検索に合致するフォルダーのみを表示します。

8. フォルダーのリストで、スキャンを移動するフォルダーをクリックします。

9. **[移動]** をクリックします。

    Tenable Web App Scanning は選択したフォルダーにスキャンを移動します。

ゴミ箱フォルダーへのスキャンの移動

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

必要なスキャンのアクセス許可: 表示可

あるユーザーが共有されたスキャンを **[ゴミ箱]** フォルダーに移動すると、Tenable Web App Scanning はそのユーザーのアカウントのスキャンのみを移動します。そのスキャンへの **[表示可]** またはそれ以上のアクセス許可を持つ他のすべてのユーザーに対しては、スキャンは元のフォルダーに残ります。

[ゴミ箱] フォルダーに移動されたスキャンは、**[ゴミ箱]** のラベルが付いた状態で **[すべてのスキャン]** フォルダーにも表示されます。

注意: スキャンを **[ゴミ箱]** フォルダーに移動した後、**[設定可]** アクセス許可を持つユーザーがスキャンを完全に削除するまで、スキャンは **[ゴミ箱]** フォルダーに残ります。

注意: スケジュールされたスキャンは、スキャン所有者の **[ゴミ箱]** フォルダーにある場合には実行されません。

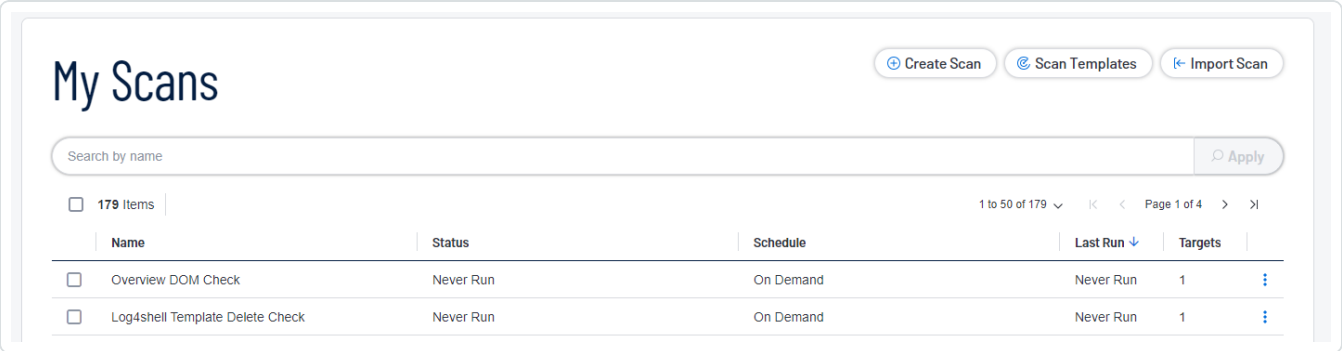
1 つまたは複数のスキャンを [ゴミ箱] フォルダーに移動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[スキャン]** をクリックします。

   Tenable Web App Scanning で **[マイスキャン]** ページが表示されます。



3. 行にある ⋮ ボタンをクリックします。

オプションのドロップダウンボックスが表示されます。

4. 次のいずれかを行います。

   - 1つのスキャンを選択する場合

     a. スキャンの表で、移動するスキャンにカーソルを合わせます。

        アクションボタンが行に表示されます。

     b. ⋮ボタンをクリックします。

        メニューが表示されます。

     c. **[ゴミ箱]**をクリックします。

   - 複数のスキャンを選択する場合

     a. スキャンの表で、移動する各スキャンの横にあるチェックボックスを選択します。

        ページの下部またはテーブルの上部に、アクションバーが表示されます。

     b. アクションバーで、**[ゴミ箱]**をクリックします。

   Tenable Web App Scanningが1つまたは複数の選択したスキャンを**[ゴミ箱]**フォルダーに移動します。

Tenable Web App Scanning 設定

[設定] ページでは、すべての Tenable Web App Scanning の設定の表示と管理ができます。

[設定] ページにアクセスする方法

1. 右上の ⚙ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. **[設定]** をクリックします。

   [設定] ページが表示されます。

注意: すべての**設定**オプションは Tenable Vulnerability Management 内で直接管理されます。[設定] セクションにアクセスすると、Tenable Vulnerability Management ユーザーインターフェースとドキュメントに自動的にリダイレクトされます。

全般設定

必要なユーザーロール: 管理者

[一般] ページで、Tenable Web App Scanning インスタンスの全般設定を設定できます。

全般設定にアクセスする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

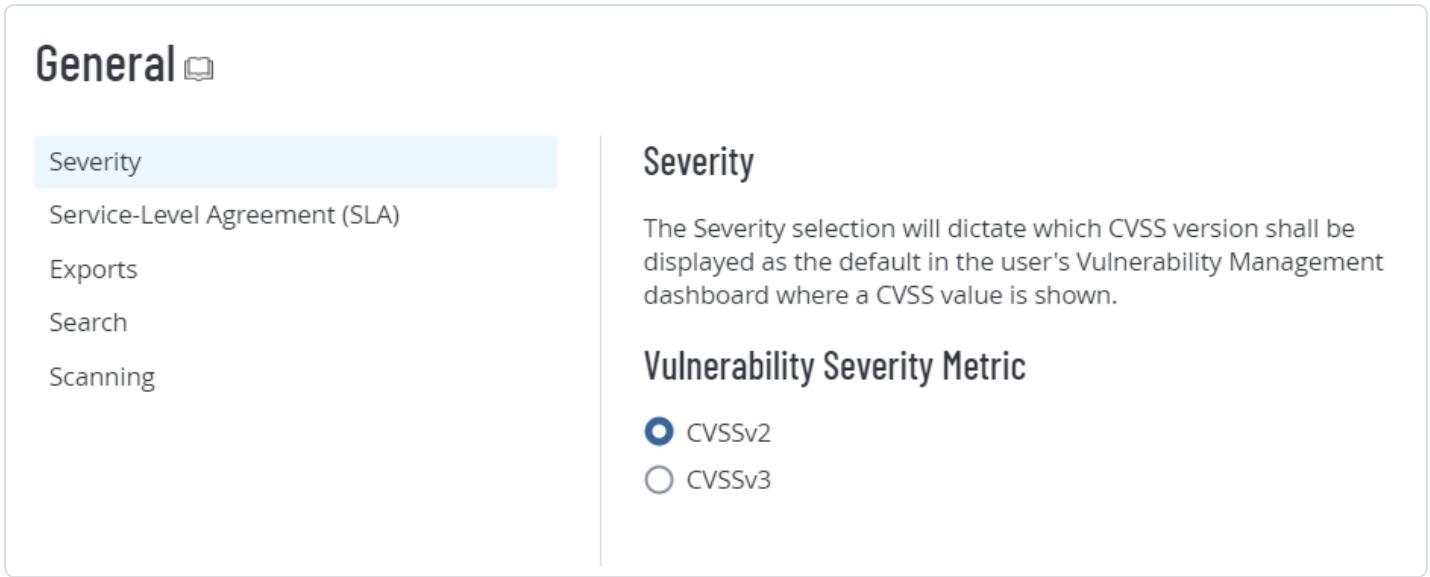
3. **[一般]** タイルをクリックします。

   [一般] ページが表示されます。デフォルトでは、**[深刻度]** タブがアクティブになっています。

ここでは、以下のオプションを設定できます。

深刻度

Tenable Web App Scanning はデフォルトで個別の脆弱性インスタンスの深刻度の計算に CVSSv2 スコアを使用します。Tenable Web App Scanning での脆弱性の深刻度の計算に CVSSv3 スコア(利用できる場合)を使用する場合は、深刻度メトリクス設定で設定できます。



ヒント：脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。

CVSSv2 と CVSSv3 の深刻度や範囲の詳細は、CVSS Scores vs. VPRを参照してください。

注意：この設定は、以下には影響しません。

- Tenable Web App Scanning 脆弱性。
- Tenable Container Security脆弱性
- **[SLA の進捗：脆弱性の経過日数]** ウィジェットに表示される計算。SLA の深刻度を変更するには、**[一般]** ページの **[サービスレベルアグリーメント (SLA)]** タブに移動します。

注意：CVSS 深刻度メトリクス設定を変更した場合、新しい設定は、システムに入ってくる新しい検出結果にのみ反映されます。既存の検出結果は、以前の深刻度設定のみを反映します (別の方法で変更しない限り)。変更ルールの詳細については、変更/許容ルールを参照してください。

深刻度設定を行う方法

1. **[深刻度]** タブで、Tenable Web App Scanning での深刻度の計算に使用するメトリクスを選択します。
   - **CVSSv2** - すべての深刻度の計算に CVSSv2 スコアを使用します。
   - **CVSSv3** - すべての深刻度の計算に CVSSv3 スコアを使用します。CVSSv3 スコアを利用できない場合に限り CVSSv2 スコアを使用します。
2. **[保存]** をクリックします。
3. システムで変更が保存され、選択された内容に基づき深刻度が計算されるようになります。

   変更前に検出された脆弱性は、すべて検出された時点での深刻度が維持されます。変更後は、スキャンで検出された脆弱性の深刻度は、すべて新たに選択された内容に基づいて設定されます。そのため、1 つの脆弱性について異なる CVSS スコアや深刻度が表示される場合があります。

   ヒント：脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。

サービスレベルアグリーメント (SLA)

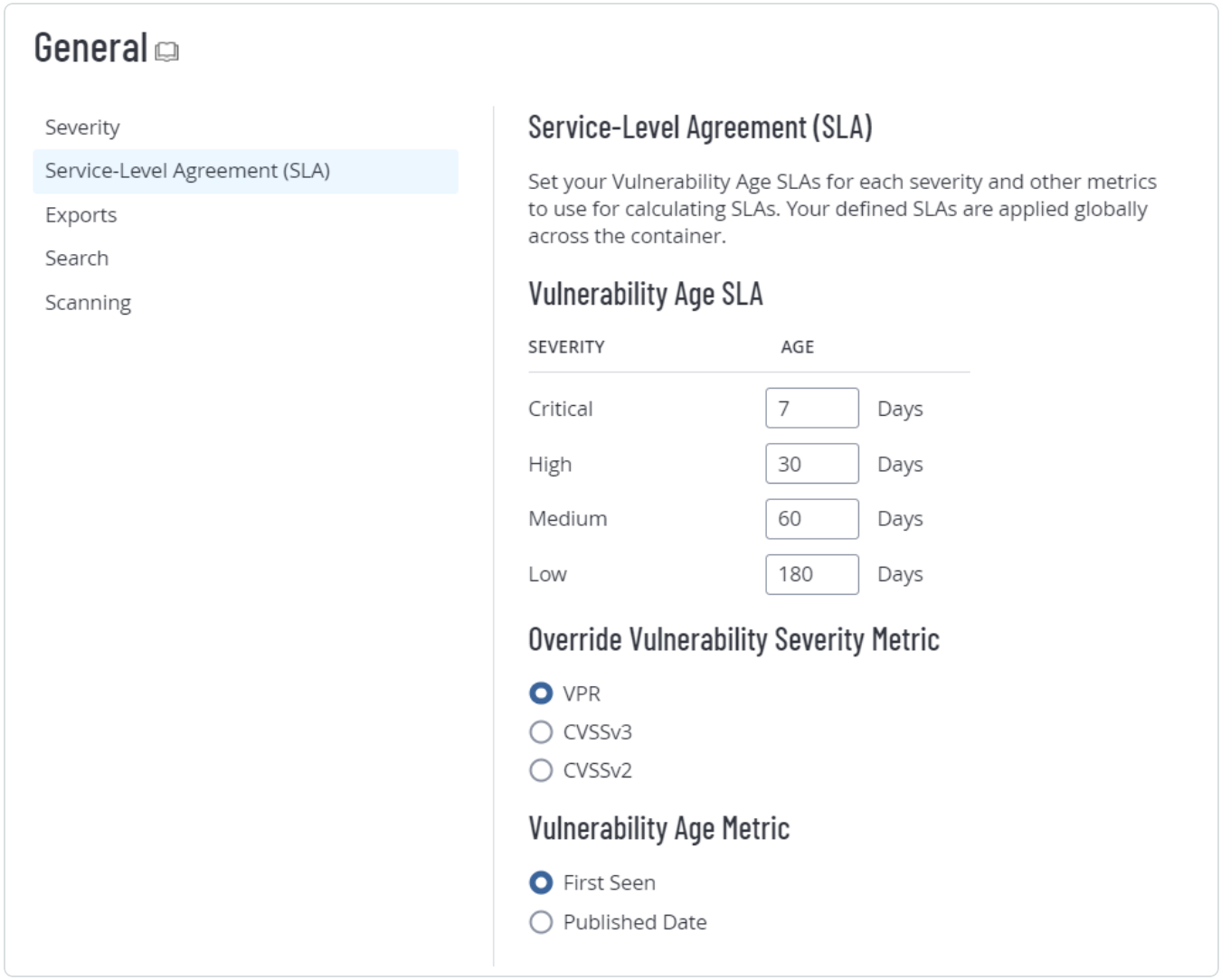
サービスレベルアグリーメント (SLA) 設定を行うと、Tenable による SLA データの計算方法を変更できます。

このデータは **[脆弱性管理の概要]** ダッシュボードの **[SLA 進捗状況: 脆弱性の経過日数]** ウィジェットで表示できます。詳細は、Vulnerability Management Overview を参照してください。

SLA 設定を行う方法

1. **[サービスレベルアグリーメント (SLA)]** タブをクリックします。

   SLA オプションが表示されます。



2. 次のオプションを設定します。

オプション	デフォルト	説明/アクション
Vulnerability Age SLA	• **Critical** 7 日 • **High** 30 日 • **Medium** 60 日 • **Low** 180 日	各深刻度に含まれている日数を変更するには、**[重大]**、**[高]**、**[中]**、または**[低]**の横にあるボックスに整数を入力します。
Override Vulnerability Severity Metric	VPR	Tenable が SLA データの計算に VPR 深刻度、CVSSv2 深刻度、または CVSSv3 深刻度のいずれを使用するかを指定します。 これらのメトリクスについては、CVSS vs. VPRを参照してください。 **注意:** このオプションは、**[SLA の進捗: 脆弱性の経過日数]** ウィジェットに表示される計算にのみ反映されます。製品の他のすべての領域に対し、深刻度メトリクスの変更を反映させるには、**[一般]** ページの **[深刻度]** タブに移動します。
脆弱性の経過日数メトリクス	初回確認日	Tenable が SLA データの計算に **First Seen** または **Published Date** のいずれを使用するかを指定します。

3. **[保存]** をクリックします。

   Tenable Web App Scanning によって SLA 設定が保存されます。

言語

[一般] ページで、Tenable Web App Scanning コンテナ内のプラグイン言語を、英語、日本語、簡体字中国語、繁体字中国語に変更できます。この設定は、コンテナ内のすべてのユーザーに影響します。

プラグイン言語を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[一般]** タイルをクリックします。

   [一般] タイルが表示されます。デフォルトでは、**[深刻度]** タブがアクティブになっています。

4. **[言語]** タブをクリックします。

   [言語] タブが表示されます。

5. **[言語]** で、新しい言語を選択します。

   Tenable Web App Scanning によって、コンテナのプラグイン言語が更新されます。

エクスポート

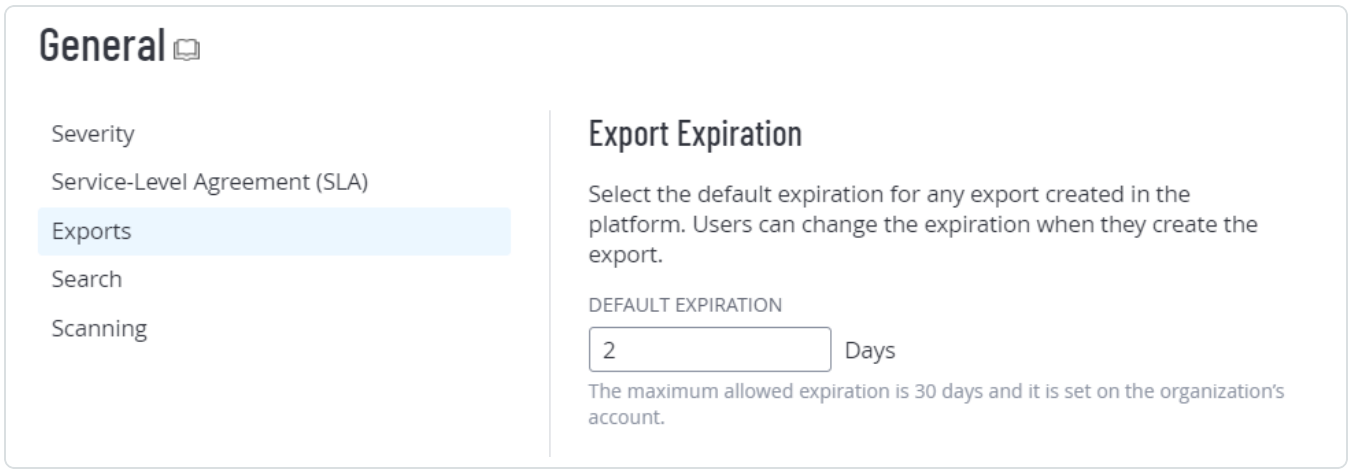
デフォルトのエクスポート有効期限を設定する方法

エクスポートを作成する場合、エクスポートファイルの有効期限を最大 30 暦日 (Tenable Web App Scanning が許可する最大日数) まで設定できます。

デフォルトでは、Tenable Web App Scanning で作成するエクスポートの有効期限は 30 日です。Tenable Web App Scanning が許可するエクスポートファイルの有効期限の日数を減らしたい場合は、デフォルトのエクスポート有効期限日数を設定できます。

1. **[エクスポート]** タブをクリックします。

   [エクスポートの有効期限] オプションが表示されます。



2. **[デフォルトの有効期限]** ボックスに、Tenable Web App Scanning が許可するエクスポート有効期限までの日数を入力します。

   注意: Tenable Web App Scanning では、エクスポート有効期限に最大 30 暦日を設定できます。

   注意: 日数は 1 から 30 の整数で入力する必要があります。

3. **[保存]** をクリックします。

   Tenable Web App Scanning によって設定が保存され、エクスポートの有効期限が切れるまでの許容日数が更新されます。

検索

プラグイン出力データ保持を有効にすると、スキャンを起動するたびに Tenable Web App Scanning でプラグイン出力データを保存できるようになります。その後、プラグイン出力で脆弱性の検出結果をフィルターできます。詳細は、Findings Filtersを参照してください。

注意: この設定が 35 日間使用されないと、Tenable がこの設定を自動的に無効にします。その後のすべてのスキャンでプラグイン出力の検索を実行するには、この設定を再度有効にします。この設定は、**Explore** ユーザーインターフェース内で通常の検索を実行する必要がある場合にのみ使用します。

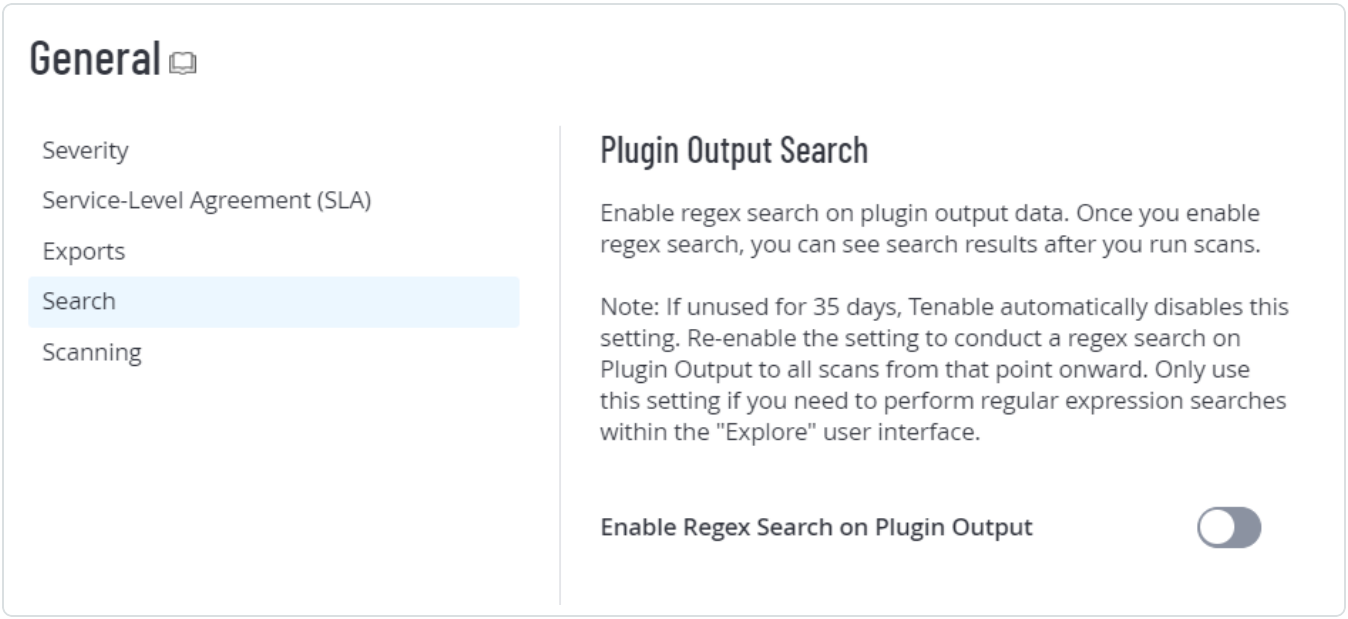
プラグイン出力データ保持を有効にしたら、スキャンを起動して、Tenable Web App Scanning がプラグイン出力データを識別して保存できるようにする必要があります。

注意: 有効にしたプラグイン出力データ保持を無効にすることはできません。

プラグイン出力データ保持を有効にする方法

1. 左側のナビゲーションプレーンで、**[検索]** タブをクリックします。

   検索オプションが表示されます。



2. **[プラグイン出力で正規表現検索を有効にします]** トグルをクリックします。
3. **[保存]** をクリックします。

   Tenable Web App Scanning で、ご使用のアカウントのプラグイン出力データ保持が有効になります。

次の手順

- ホスト資産のスキャンを起動します。

スキャン中

[スキャン] セクションでは、2 つの設定を使用して Tenable Web App Scanning が情報レベルのプラグインを処理する方法を変更できます。

警告: Tenable は今後数週間のうちにすべてのお客様のこれらの設定を削除します。詳細については、Tenable の担当者までお問い合わせください。

高容量トラフィック情報のプラグインの処理

この設定を無効にすると、Tenable Web App Scanning がスキャンされたすべてのホストのすべてのオープンポートに関して個別の検出結果を生成しなくなります。この設定を無効にすると、スキャン時間とスキャン結果のエクスポート時間が短縮され、有効にすると時間が非常に長くなる場合があります。詳細については、Platform Performance Improvement FAQ - Info Plugins (プラットフォームパフォーマンスの向上に関する FAQ - 情報プラグイン) を参照してください。

影響を受けるプラグイン ID

- 34220 - Netstat Portscanner (WMI)
- 34252 - Microsoft Windows リモートリスナーの列挙 (WMI)
- 11219 - Nessus SYN スキャナー
- 14272 - Netstat Portscanner (SSH)
- 25221 - リモートリスナーの列挙 (Linux / AIX)
- 10736 - DCE サービスの列挙
- 99265 - macOS リモートリスナーの列挙
- 10335 - Nessus TCP スキャナー
- 14274 - Nessus SNMP スキャナー
- 34277 - Nessus UDP スキャナー

ヒント: これらのプラグインの詳細については、Tenable プラグインサイトを参照してください。

開いているポートの検出結果を再配置する

開いているポートの検出結果を **[検出結果]** ワークベンチではなく **[資産の詳細]** ページに表示して、Tenable Web App Scanning が検出結果を処理する方法を変更するには、この設定を有効にします。この変更が所属組織に与える可能性のある影響については、Tenable Vulnerability Management New Data Format: Relocate Open Port Findings (Tenable Vulnerability Management の新しいデータ形式: 開いているポートの検索結果を再配置する) を参照してください。

注意: **[開いているポートの検出結果を再配置する]** を有効にすると、開いているポートが個別の検出結果として保存されなくなるため、サードパーティ統合で開いているポートの検出結果データを受け取ることができなります。

この設定では、以下を実行できます。

- 開いているポートの検出結果を**[検出結果]**ワークベンチから**[資産の詳細]**ページに*移動*します。**[資産の詳細]**ページは、**[資産]**ワークベンチでホスト資産をクリックすると表示されます。

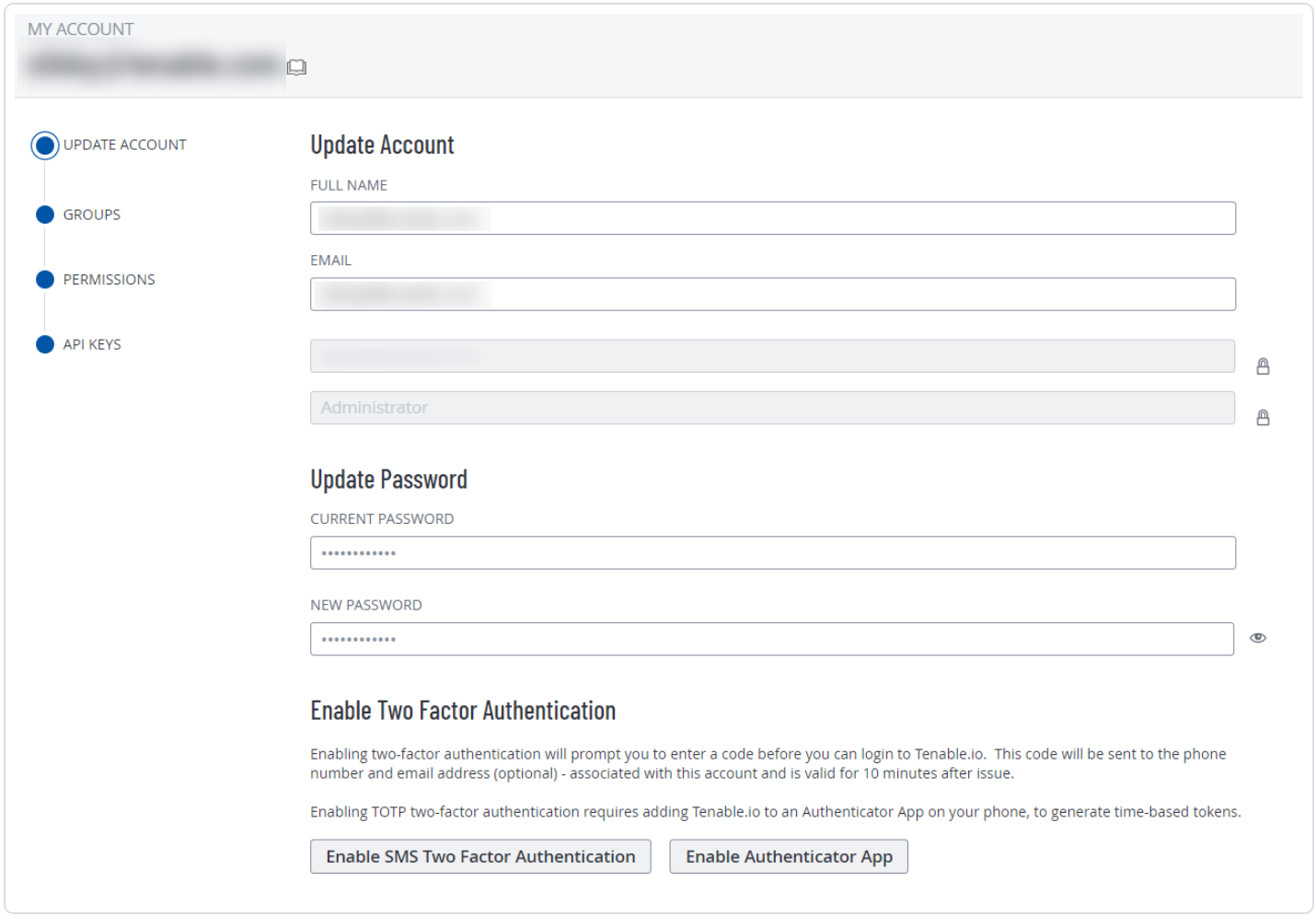
  次の高トラフィックプラグインの開いているポートの検出結果が[資産の詳細]ページに移動

  - 34220 - Netstat Portscanner (WMI)
  - 34252 - Microsoft Windows リモートリスナーの列挙 (WMI)
  - 11219 - Nessus SYN スキャナー
  - 14272 - Netstat Portscanner (SSH)
  - 25221 - リモートリスナーの列挙 (Linux / AIX)
  - 10736 - DCE サービスの列挙
  - 99265 - macOS リモートリスナーの列挙
  - 10335 - Nessus TCP スキャナー
  - 14274 - Nessus SNMP スキャナー
  - 34277 - Nessus UDP スキャナー

- **[資産の詳細]**ページの**[オープンポート]**タブを有効にします。このタブに、開いているポートの検出結果が表示されるようになります。
- **[資産]**ワークベンチで**[オープンポート]**フィルターを有効にし、ホスト資産の開いているポートを検索できます。
- **[タグ]**ページで**[オープンポート]**ルールを有効にし、開いているポートにタグを付けることができます。
- **[資産]**ワークベンチに[オープンポート]フィールドを追加し、開いているポートのデータをエクスポートできるようにします。
- (オプション) 開いているポートの検出結果を一括資産エクスポート API に追加します。詳細については、*Tenable 開発者ポータル*の API 変更ログを参照してください。この機能をリクエストするには、Tenable の Customer Success Manager までご連絡ください。

マイアカウント

[**My Account**] ページから、独自のユーザーアカウントを変更できます。



次のいずれかの方法で マイアカウント ページに移動できます。

- **[設定]** ページから **[マイアカウント]** ページにアクセスする方法

  a. 左上にある ☰ ボタンをクリックします。

  左側にナビゲーションプレーンが表示されます。

  b. 左のナビゲーションプレーンで **[設定]** をクリックします。

  [設定] ページが表示されます。

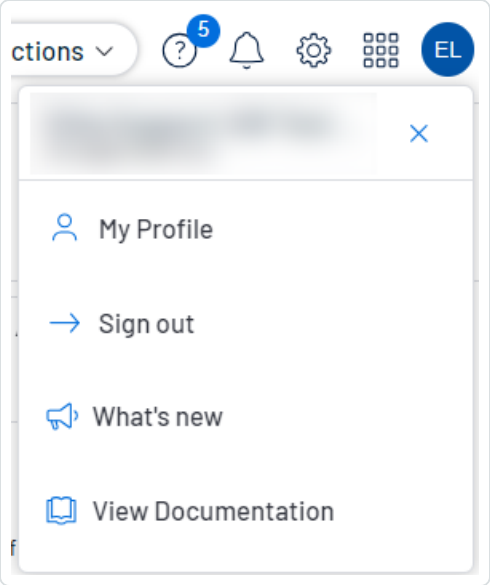
c. **[マイアカウント]** タイルをクリックします。

[マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

- 任意のページの上部ナビゲーションメニューから **[マイアカウント]** ページにアクセスする方法

a. 右上の青いユーザー円をクリックします。

ユーザーアカウントメニューが表示されます。



b. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

アカウントの詳細の表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[マイアカウント] ページでは、ログインの詳細、ユーザーロール、割り当てられているグループとアクセス許可など、アカウントに関する詳細を表示できます。

アカウントの詳細を表示する方法

1. 次のいずれかを行います。

   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

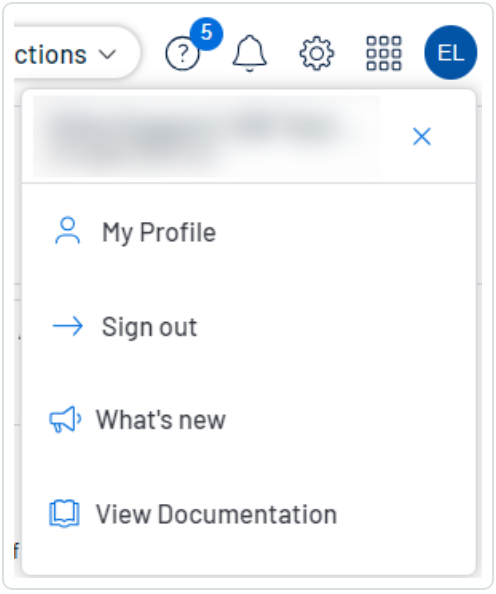
        [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

        [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

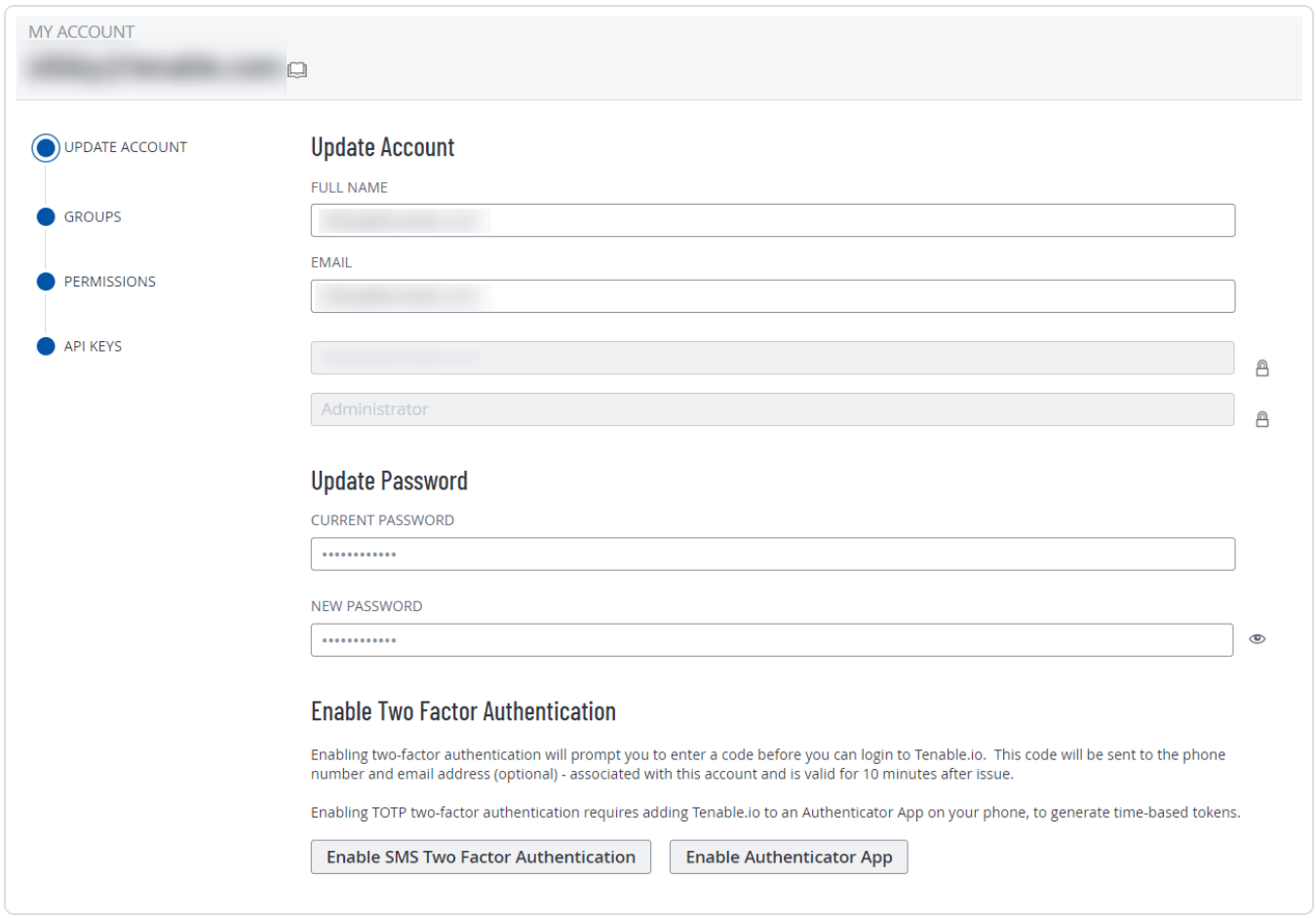
   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。



2. ページの左側で、以下の選択肢から選択します。

オプション	アクション
アカウントの更新	• **[アカウントのアップデート]** をクリックします。 **[アカウントのアップデート]** セクションが表示され、アカウントに関する以下の項目の詳細が表示されます。 ◦ **氏名** ◦ **Eメール** ◦ **ユーザー名** ◦ **ロール**

	• (オプション) 基本的なアカウント情報 (名前やメールアドレスなど) を更新します。 **注意:** ユーザー名やロールを変更することはできません。 • (オプション) パスワードを変更します。 • (オプション) アカウントで二要素認証を設定または無効にします。 • (オプション) アカウントでベータ版機能の探索機能を有効または無効にします。
グループ	• **[グループ]** をクリックします。 **注意:** **[マイアカウント]** ページでグループ設定を変更することはできません。詳細は、ユーザーグループを参照してください。 • **[グループ]** 表には以下の内容が表示されます。 ◦ 割り当てられているユーザーグループ ◦ 各ユーザーグループのメンバー数
アクセス許可	• **[アクセス許可]** をクリックします。 **注意:** アクセス許可をユーザーに適用すると、指定された資産タグ (つまり、オブジェクト)、およびそれらのオブジェクトに該当する資産に対して特定のアクションが実行できるようになります。アクセス許可は、個別のユーザーまたはユーザーグループのすべてのメンバーに適用できます。詳細は、権限を参照してください。 **注意:** **[マイアカウント]** ページでアクセス許可設定を変更することはできません。 • **[アクセス許可]** 表には以下の内容が表示されます。 ◦ アカウントに割り当てられているアクセス許可の名前 ◦ それらのアクセス許可によって実行できるアクション ◦ 各アクセス許可が適用されるオブジェクト
API	• **[API キー]** をクリックします。

キー	• API キーの説明が表示されます。 • API キーを生成する. **警告:** **[生成]** ボタンをクリックすると、既存の API キーはすべて置き換えられます。以前の API キーを使用していたアプリケーションを更新する必要があります。 **警告**: **[API キー]** タブを閉じる前に、アクセスキーと秘密鍵を必ずコピーしてください。このタブを閉じてしまうと、Tenable Web App Scanning からキーを取得することはできなくなります。

注意: ユーザーアカウントの有効期限は、そのアカウントが属する Tenable Web App Scanning コンテナの作成日に基づいて設定されます。Tenable は、この設定を直接制御します。詳細については、Tenable サポート にお問い合わせください。

アカウントを更新する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

始める前に

- (オプション) アカウントの詳細を表示します。

アカウントを更新する方法

1. 次のいずれかを行います。
    - 左上にある ☰ ボタンをクリックします。

      左側にナビゲーションプレーンが表示されます。

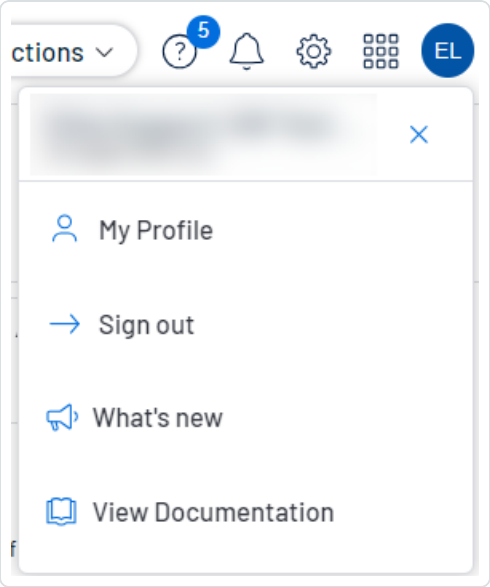
      a. 左のナビゲーションプレーンで **[設定]** をクリックします。

      [設定] ページが表示されます。

      b. **[マイアカウント]** タイルをクリックします。

      [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。
    - 右上の青いユーザー円をクリックします。

      ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. (オプション) **[名前]** を編集します。
3. (オプション) **[E メール]** を編集します。

有効なメールアドレスは、

name@domein

の形式である必要があります。ここで、*domain* はお使いの Tenable Web App Scanning インスタンス用に承認されたドメインに対応します。

このメールアドレスは、**[ユーザー名]** として設定されたメールアドレスをオーバーライドします。このオプションを空のままにすると、Tenable Web App Scanning は **[ユーザー名]** の値をメールアドレスとして使用します。

> **注意:** 初期設定の間に、Tenable は Tenable Web App Scanning インスタンス用に承認されたドメインを設定します。お使いのインスタンスにドメインを追加する方法については、Tenable サポート にお問い合わせください。

4. **[保存]** をクリックします。

Tenable Web App Scanning はアカウントへの変更を保存します。

5. (オプション) パスワードを変更します。

6. (オプション) 二要素認証を設定します。
7. (オプション) API キーを生成します。

パスワードを変更する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

いずれの種類のユーザーアカウントのパスワードも変更できます。パスワードを変更する方法は、ユーザーアカウントに割り当てられたロールによって若干異なります。

別のユーザーのパスワードを変更するには、別のユーザーのパスワードの変更を参照してください。

パスワードを変更するには

1. 次のいずれかを行います。
   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

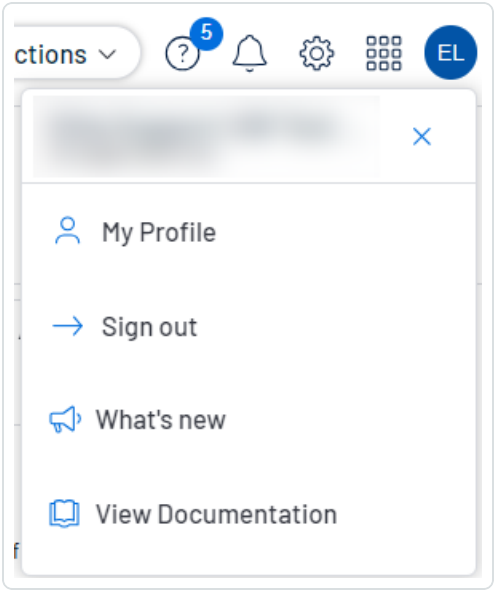
     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

     [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

     [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。
   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. **[現在のパスワード]** ボックスに現在のパスワードを入力します。
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。詳細は、Tenable Web App Scanning のパスワード要件を参照してください。
4. **[保存]** ボタンをクリックします。

Tenable Web App Scanning により新しいパスワードが保存され、お使いのアカウントで現在アクティブなセッションが終了します。Tenable Web App Scanning によりその後、再認証を求めるメッセージが表示されます。

5. 新しいパスワードを使用して、Tenable Web App Scanning にログインします。

二要素認証を設定する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[マイアカウント] ページで、自分のアカウントに二要素認証を設定できます。

ヒント: 管理者は、ユーザーアカウントを作成または編集するときに、他のアカウントに対して二要素認証を強制することもできます。

注意: 二要素認証を設定する前に、International Phone Availability リストを確認して、Tenable Web App Scanning からテキストメッセージを受信できることを確認してください。

二要素認証を追加または変更する方法

1. 次のいずれかを行います。

   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

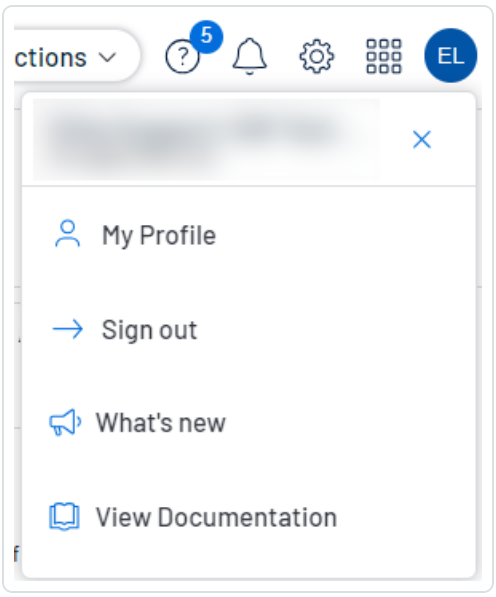
        [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

        [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. **[二要素認証を有効にする]** セクションで、以下のいずれかを行います。

- SMS の二要素認証を有効にします。

a. **[SMS 二要素認証を有効にする]** をクリックします。

[二要素認証] プレーンが表示されます。

b. **[現在のパスワード]** ボックスに現在の Tenable Web App Scanning のパスワードを入力します。

c. **[電話番号]** ボックスに自分の携帯電話番号を入力します。

> **注意:** Tenable Web App Scanning はデフォルトで携帯電話の番号を米国内の番号として扱い、国コードの +1 を前に付けるよう設定されています。お使いの携帯電話が米国内の番号でない場合、適切な国コードを前に付けてください。

d. **[次へ]** をクリックします。

[検証コード] プレーンが表示され、Tenable Web App Scanning より検証コードが記載されたテキストメッセージが電話番号宛てに送信されます。

e. **[検証コード]** ボックスに、受け取った検証コードを入力します。

f. **[次へ]**をクリックします。

[二要素認証が正常にセットアップされました]メッセージが表示され、Tenable Web App Scanningによって設定がTenable Web App Scanningアカウントに適用されます。

g. (オプション) Tenable Web App Scanningが、ユーザーアカウントに関連付けられたメールアドレス宛てに検証コードを送信するかどうかを設定する方法

a. **[バックアップのEメールを送信する]**チェックボックスを選択するかクリアします。

b. **[更新]**をクリックします。

Tenable Web App Scanningはバックアップメールの設定を更新します。

注意: この設定の電話番号を保存すると、電話番号の編集や変更はできなくなります。使用する追加の電話番号がある場合は、新しい認証セットアップを設定する必要があります。

- 次のように、認証アプリケーションベースの認証を有効にします。

a. **[Authenticatorアプリを有効にする]**をクリックします。

[二要素認証]プレーンが表示されます。

b. **[現在のパスワード]**ボックスに現在のTenable Web App Scanningのパスワードを入力します。

c. **[次へ]**をクリックします。

[時間ベースのワンタイムパスワード]プレーンが表示されます。

d. お好みの認証アプリケーションで、QRコードをスキャンします。

認証アプリケーションにTenable Web App Scanningの検証コードが表示されます。

e. **[検証コード]**ボックスに、認証アプリケーションに表示されたコードを入力します。

注意: 正しい検証コードが入力されない場合、Tenable Web App ScanningによってQRコードがロックされます。認証アプリケーションからの設定を削除して、新しいQRをスキャンしてください。

f. **[次へ]**をクリックします。

[二要素認証が正常にセットアップされました] メッセージが表示され、Tenable Web App Scanning によって設定が Tenable Web App Scanning アカウントに適用されます。

新しいインターフェースで二要素認証を無効にする方法

1. 次のいずれかを行います。

   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

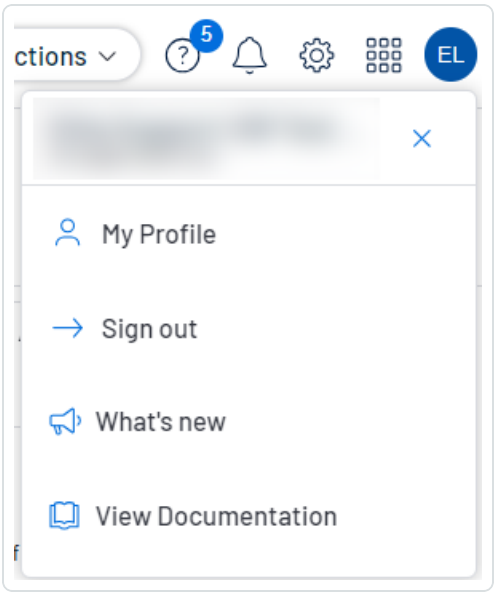
     [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

     [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



     a. **[マイプロファイル]** をクリックします。

     [マイアカウント] ページが表示されます。

2. **[パスワードの変更]** セクションの **[現在のパスワード]** ボックスに、現在のパスワードを入力します。

3. **[二要素認証を有効にする]** セクションで、**[無効化]** をクリックします。

   [二要素認証を無効化する] の確認メッセージが表示されます。

4. 警告メッセージを読み、**[続行]** をクリックします。

   Tenable Web App Scanning でお使いのアカウントの二要素認証が無効化されます。

API キーを生成する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

お使いのユーザーアカウントに関連付けられた API キーにより、お客様の企業にライセンスされた、すべての Tenable Web App Scanning 製品の API にアクセスすることが可能になります。

注意: **Tenable Web App Scanning API を認証するには** Tenable Web App Scanning API のアクセスキーと秘密鍵が必要です。

注意: お使いのユーザーアカウントに関連付けられた API キーを使って、お客様の会社にライセンス付与されているすべての Tenable Vulnerability Management 製品の API にアクセスすることができます。個別の製品に別々のキーを設定することはできません。たとえば、Tenable Vulnerability Management で API キーを生成した場合、この操作により Tenable Web App Scanning および Tenable Container Security の API キーも変更されます。

注意: アプリケーションごとに、同一の API キーを使用してください。以下は例ですが、これらに限定されません。

- Tenable Web App Scanning の統合
- サードパーティの統合
- その他のカスタムアプリケーション (Tenable Professional Services からのものを含む)

API キーを生成する方法は、ユーザーアカウントに割り当てられたロールによって異なります。管理者は、任意のアカウントの API キーを生成できます。詳細は、別のユーザーの API キーの生成 を参照してください。他のロールは自分のアカウントの API キーを生成できます。

自分のアカウントの API キーを生成する方法

1. 次のいずれかを行います。
    - 左上にある ☰ ボタンをクリックします。

      左側にナビゲーションプレーンが表示されます。

a. 左のナビゲーションプレーンで **[設定]** をクリックします。

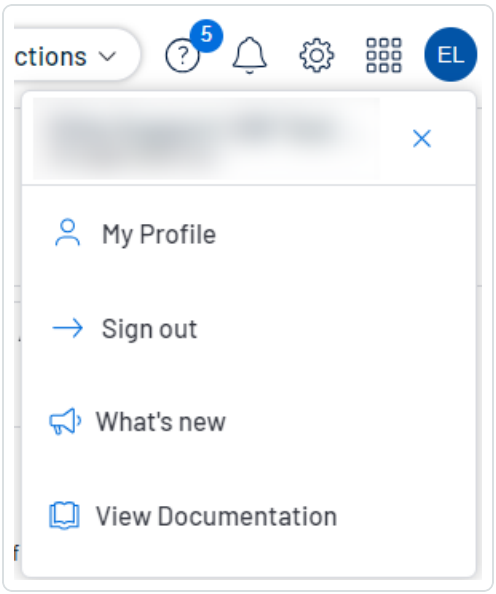
[設定] ページが表示されます。

b. **[マイアカウント]** タイルをクリックします。

[マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

- 右上の青いユーザー円をクリックします。

ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. **[API キー]** タブをクリックします。

[API キー] セクションが表示されます。

3. **[生成]** をクリックします。

[API キーを生成する] ウィンドウが警告とともに表示されます。

> **警告:** **[生成]** ボタンをクリックすると、既存の API キーはすべて置き換えられます。以前の API キーを使用していたアプリケーションを更新する必要があります。

4. 警告を確認し、**[生成]** をクリックします。

Tenable Web App Scanning により新しいアクセスキーと秘密鍵が生成され、ページの **[カスタム API キー]** セクションに新しいキーが表示されます。

> **ヒント:** **[生成]** ボタンが無効になっている場合は、管理者に連絡して、アカウントの API アクセスが有効になっていることを確認してください。詳細は、ユーザーアカウントの編集を参照してください。

5. 新しいアクセスキーと秘密鍵を安全な場所にコピーします。

> **警告:** **[API キー]** タブを閉じる前に、アクセスキーと秘密鍵を必ずコピーしてください。このタブを閉じてしまうと、Tenable Web App Scanning からキーを取得することはできなくなります。

自分のアカウントのロックを解除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

Tenable Web App Scanning でログインを試みて 5 回連続して失敗すると、アカウントがロックされます。

注意: アカウントで指定されたメールアドレスにアクセスできない場合、Tenable Web App Scanning インスタンスの管理者が代わりにパスワードをリセットできます。

注意: ユーザーは、ユーザーインターフェースからロックアウトされる可能性がありますが、適切な認証 (api_permit) が割り当てられている場合は API リクエストを送信できます。詳細は、Tenable 開発者ポータルを参照してください。

自分のアカウントのロックを解除する方法

1. Tenable Web App Scanning ログインページで、**[パスワードをお忘れですか?]** をクリックします。リンクをクリックします。

   パスワードリセットのページが表示されます。

2. **[ユーザー名]** ボックスに、Tenable Web App Scanning のユーザー名を入力します。

3. CAPTCHA ボックスに、質問に対する自分の答えを入力します。

4. **[送信]** をクリックします。

   Tenable Web App Scanning により、ユーザーアカウントで指定されたメールアドレス宛てにパスワード復旧の手順が送信されます。

5. メールに記載された手順に従い、パスワードをリセットします。詳細については、パスワード要件を参照してください。

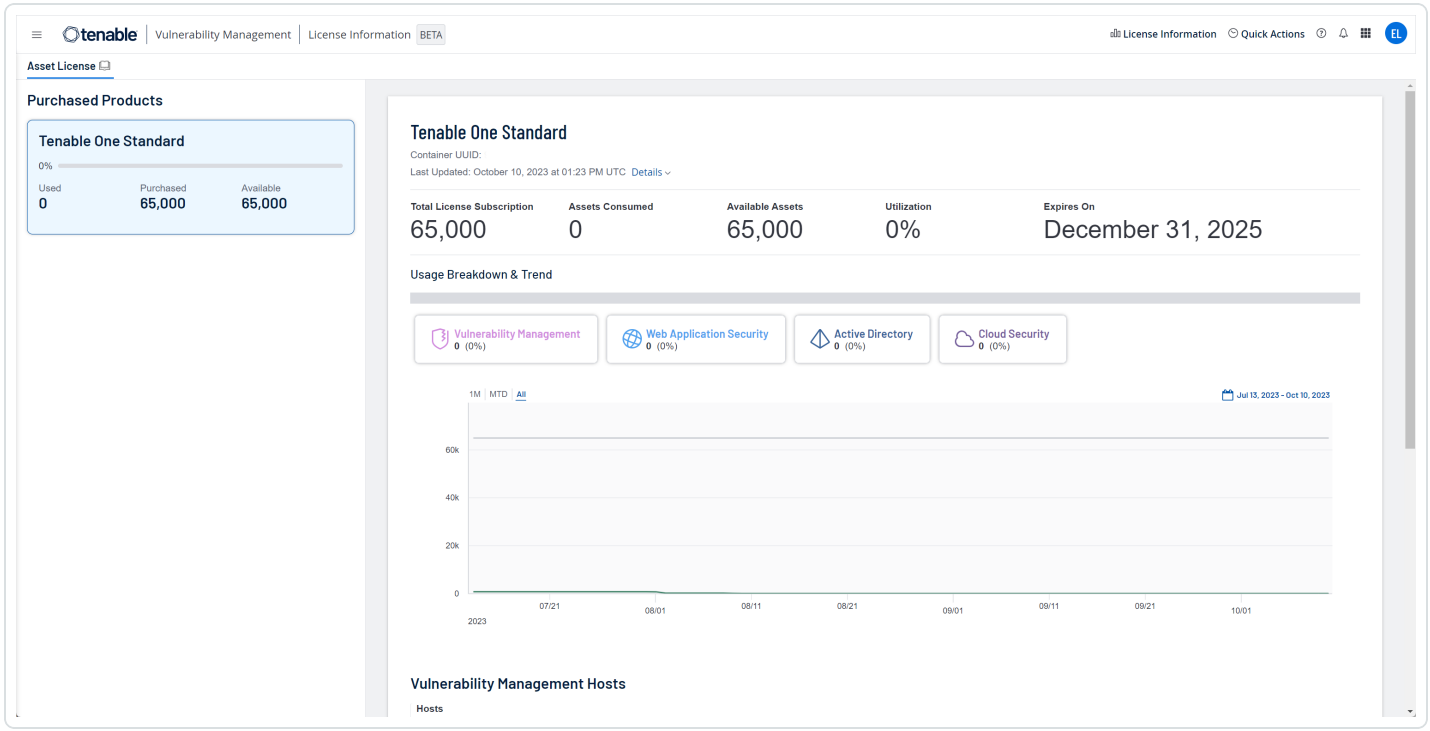
ライセンス情報

[ライセンス情報] ページでは、Tenable 製品とそのライセンスの使用状況の内訳を確認することができます。この情報は、製品別または期間別にビジュアル化された概要など、複数の方法で表示することができます。これにより、一時的な使用量の急増や製品の設定ミスなどの傾向を特定することができます。

ヒント: **[ライセンス情報]** ページに表示される各製品の Tenable ライセンスの仕組みについては、Tenable 製品のライセンスを参照してください。ライセンス超過についての詳細は、Tenable Cloud Overage Process (Tenable クラウドライセンス超過プロセス) を参照してください。

[ライセンス情報] ページの表示

[ライセンス情報] ページを表示するには、上部のナビゲーションバーから **[ライセンス情報]** をクリックします。



[ライセンス情報] ページには、現在の Tenable コンテナにある全製品のライセンス使用状況が表示され、次のセクションがあります。

セクション	説明
購入済みの製	左側で、製品タイルをクリックして詳細を表示します。製品が評価中または期

品	限切れの場合は、ラベルが表示されます。 • **使用中** - 製品サブスクリプションで使用または評価されたライセンスの総数。 • **購入済み** - その製品で購入したライセンスの数。 • **使用可能** - サブスクリプションで利用可能な、まだ評価されていない残りのライセンスの数。
製品のサマリー	ページの上部に、選択した製品のサマリーを表示します。 • **製品名** - 製品の名前。 • **コンテナ UUID** - コンテナの一意の ID。 • **最終更新日** - 製品が最後に更新された日時。 • **サイト名** - Tenable のクラウドにインストールされている製品を含むクラスター。 • **リージョン** - クラスターが配置されている地域。 • **プラグインセット** - 製品の Nessus プラグインセットのバージョン。 • **プラグインの更新** - Nessus プラグインセットが最後に更新された日時。 • **合計ライセンスサブスクリプション** - 製品サブスクリプションの一部として購入したライセンスの総数。 • **消費された資産** - 製品サブスクリプションで使用または評価されたライセンスの総数。 • **利用可能な資産** - サブスクリプションで利用可能な、まだ評価されていない残りのライセンスの数。 • **使用率** - 使用済みのライセンスの割合。この値は、消費されたライセンス数を合計ライセンスサブスクリプション数で割って計算されます。 • **有効期限日** - Tenable サブスクリプションが期限切れとなる日付。
使用率の内訳と傾向	資産の使用率の内訳を視覚的に表示します。 • **棒グラフ** - (Tenable One のみ) Tenable One コンポーネント別の合計ライ

	センス使用量を棒グラフで表示します。 **注意**: Tenable Cloud Security の新しいバージョンがある場合、ライセンスのある資産の数は、**計算**、**サーバーレス**、**コンテナリポジトリ**の資産に比率を乗算し、**コンテナイメージ** (Tenable Container Security がある場合) を加算して算出されます。所属組織に比率がある場合は、**[クラウドセキュリティ]** セクションの **[ライセンス比率]** フィールドに表示されます。ご利用のクラウドリソースに Tenable が適用する場合がある比率については、Tenable の担当者にお問い合わせください。 • **使用量の推移** - ライセンスの使用量の推移を折れ線グラフで表示します。X 軸は期間、Y 軸は使用された資産の数です。グラフの上部にあるフィルターを使用して、左側で期間を切り替えるか、右側でカスタムの日付範囲を指定します。 **ヒント**: (Tenable One のみ) グラフの上のタイルをクリックして、製品を選択または選択解除できます。
脆弱性管理ホスト	ライセンスとしてカウントされる Tenable Vulnerability Management 資産の数を表示します。 • **ホスト** - ライセンスとしてカウントされるホストの数。
クラウドセキュリティリソース	Tenable Cloud Security によって特定された環境内のクラウドリソースの数を表示します。 **注意**: Tenable Cloud Security には 2 つのバージョンがあります。最新バージョンの場合、ライセンスのあるクラウド資産の数は、**[計算]**、**[サーバーレス]**、**[コンテナリポジトリ]** の各フィールドに表示され、Tenable Container Security の場合には **[コンテナイメージ]** フィールドにも表示されます。ライセンスのあるクラウド資産の*合計*を表示するには、**使用率の内訳と傾向** セクションを参照してください。 • **ライセンス比率** – (新規バージョンのみ) **コンピューティング**、**サーバーレス**、および**コンテナリポジトリ**のリソースに適用される任意の比率。たとえば、企業の比率が 3 である場合、10 コンピューティングリソースは 30 の *ライセンス取得済みの* Tenable 資産に等しくなります。クラウドリソースに適用される比率 Tenable に関する詳細については、Tenable の担当者にお問い合わせください。

	• **コンピューティング** – (新規バージョンのみ) AWS EC2 インスタンスや Azure 仮想マシンなどのクラウドコンピューティングリソース。このフィールドにカーソルを合わせると、*請求可能な*リソース、または比率が適用される前のリソースの合計数が表示されます。 • **サーバーレス** – (新規バージョンのみ) AWS Lambda や Azure Functions などのクラウドサーバーレスリソース。このフィールドにカーソルを合わせると、*請求可能な*リソース、または比率が適用される前のリソースの合計数が表示されます。 • **コンテナリポジトリ** – (新規バージョンのみ) Tenable Cloud Security によってスキャンされたクラウドコンテナリポジトリ。このフィールドにカーソルを合わせると、*請求可能な*リソース、または比率が適用される前のリソースの合計数が表示されます。 • **コンテナイメージ (レガシーのコンテナセキュリティ)** – ライセンスとしてカウントされるパッケージ化されたアプリケーションの数。Tenable Container Security をお持ちの場合にのみ使用されます。 • **請求可能** - (レガシーのみ) ライセンスがあると見なされるクラウド資産のサブセット。通常は過去 90 日間にスキャンされたクラウドコンピューティング、ストレージ、ネットワークリソースです。 **ヒント:** Tenable Cloud Security の新しいバージョンを使用している場合、これらの資産はライセンスに対してカウントされません。 • **請求不可能** - (レガシーのみ) リポジトリまたはパイプライン内でローカルにスキャンされた、インフラのコード化 (IaC) 資産。これらは、ライセンスがあるとは見なされません。
Web App Scanning FQDN	ライセンスとしてカウントされる Tenable Web App Scanning リソースの数を表示します。 • **FQDN** - ライセンスとしてカウントされる完全修飾ドメイン名の数。 **注意**: Tenable Web App Scanning は、ユーザーアカウントでスキャンされる*完全修飾ドメイン名* (FQDN) の数によって資産カウントを決定します。脆弱性のスキャンが正常に終わるまで、資産はライセンスの制限数に対してカウントされません。

Attack Surface Management 資産	Tenable Attack Surface Management リソースを表示します。 • **観察可能オブジェクト** - Tenable Attack Surface Management で検出され、インベントリに追加された資産の数。 **注意**: Tenable One Standard のお客様の場合、これらのリソースは資産ライセンスとしてカウントされません。
Active Directory ユーザー	ライセンスとしてカウントされる Tenable Identity Exposure リソースの数を表示します。 • **ユーザー** - 有効なアクティブユーザーの数。

Tenable Web App Scanning のライセンス

このトピックでは、スタンドアロン製品の Tenable Web App Scanning 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を説明し、購入できるアドオンコンポーネントをリストし、ライセンスの超過または期限切れになるとどうなるかを説明します。Tenable Web App Scanning の使用方法については、Tenable Web App Scanning ユーザーガイドを参照してください。

Tenable Web App Scanning のライセンシング

Tenable Web App Scanning には、クラウドバージョンとオンプレミスバージョンの 2 つのバージョンがあります。クラウドバージョン向けに、Tenable はサブスクリプションモデルを提供しています。オンプレミスバージョン向けに、Tenable はサブスクリプションモデルのほか、永久ライセンスとメンテナンスライセンスを提供しています。

> **注意**: Tenable Web App Scanning オンプレミスバージョンには Tenable Security Center ライセンスが必要です。

Tenable Web App Scanning を使用する際は、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 Web App Scanning は、それらのライセンスを環境内の*資産* (一意の完全修飾ドメイン名 (FQDN)) に割り当てます。

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

> **ヒント**: 現在のライセンス数と利用可能な資産を表示するには、Tenable の上部ナビゲーションバーで  、**[ライセンス情報]** の順にクリックします。詳細については、ライセンス情報ページを参照してください。

資産のカウント方法

Tenable Web App Scanning は、環境内のリソースをスキャンして FQDN を特定することで、ライセンスのある資産数を判断します。過去 90 日間に脆弱性の有無がスキャンされた FQDN は、ライセンスにカウントされます。

FQDN は、RFC-3986 インターネット標準に従って、完全な URL で一覧表示されます。この標準に従って、各 FQDN には次のコンポーネントと形式が含まれています。

```
hostname.parent-domain.top-level-domain
```

スキャンでウェブアプリケーションターゲットを指定した場合、FQDN のいずれかのコンポーネントが別のスキャンされたターゲットまたは以前にスキャンされた資産のコンポーネントと異なる場合、Tenable Web App Scanning はそのターゲットを別の資産としてカウントします。FQDN のすべてのコンポーネントが一致する限り、異なるパスを持つ複数のターゲットは 1 つの資産として FQDN カウントに追加されます。

たとえば、次のターゲットは 1 つの資産としてカウントされます。

```
hostname.parent-domain.top-level-domain/path1
hostname.parent-domain.top-level-domain/path2
hostname.parent-domain.top-level-domain/path2/path3
```

次の表は、すべての FQDN コンポーネントが一致するかどうかに基づいて、スキャンターゲットが同じ資産と見なされる場合と別々の資産と見なされる場合を示しています。

同じ資産	別の資産
• https://example.com • https://example.com/welcome • https://example.com/welcome/get-started • https://example.com/welcome/get-started/create-new-user • http://example.com	• *https://en.example.com (異なるホスト名)* • *https://www.ex-ample.com (異なる親ドメイン名)* • *https://www.example.org (異なる最上位レベルドメイン)*

Tenable Tenable Web App Scanning のコンポーネント

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 Web App Scanning 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
• 外部スキャン機能 • OWASP Top 10 の問題 • HTML5 のクローリング	追加のクラウドスキャンの併用 **ヒント**: 併用は、ライセンスのある資産に基づいており、同時に実行できる Tenable 管理のクラウドスキャナーの数を決定します。

• Tenable Vulnerability Management との統合（所有している場合） • API の使用	

ライセンスの流用

資産を購入しても、追加の資産を購入しない限り、資産の総数は契約期間中ずっと静的です。ただし Tenable Web App Scanning は削除した資産のライセンスを 24 時間以内に流用します。さらに、90 日間または指定した期間スキャンされなかった資産のライセンスを流用します。

ライセンス制限の超過

環境の急激な拡大、または予期しない脅威による使用率の急増に対応できるよう、Tenable Web App Scanning ライセンスには 10% の柔軟性があります。ただし、ライセンスされている以上の資産をスキャンすると、Tenable はその超過について明確に伝達し、その後 3 段階で機能を削減します。

シナリオ	結果
3 日間連続して、ライセンスされている以上の資産をスキャンした。	Tenable Web App Scanning にメッセージが表示されます。
15 日間以上、ライセンスされている以上の資産をスキャンした。	Tenable Web App Scanning には、機能の制限に関するメッセージと警告が表示されます。
45 日間以上、ライセンスされている以上の資産をスキャンした。	Tenable Web App Scanning にメッセージが表示されます。エクスポート機能が無効になります。

ヒント: 不適切なスキャンや製品の設定ミスにより、スキャンが過剰になり、資産数が増加する可能性があります。詳細については、スキャンのベストプラクティスを参照してください。

期限切れのライセンス

購入した Tenable Web App Scanning 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 プラットフォームにサインインできなくなります。

Tenable Web App Scanning のライセンスの種類

Tenable Web App Scanning のライセンスの種類は、サポートされている機能セットによって異なる場合があります。最も注目すべき点は、Lumin Exposure View 機能によって、動的計算とサイバーエクスポージャーリスクスコアが Tenable ユーザーインターフェースに追加されたことです。Lumin Exposure View メトリクスの詳細については、アプリケーションダッシュボードを参照してください。

次の表で、各種の Tenable Web App Scanning ライセンスがサポートする機能を確認してください。

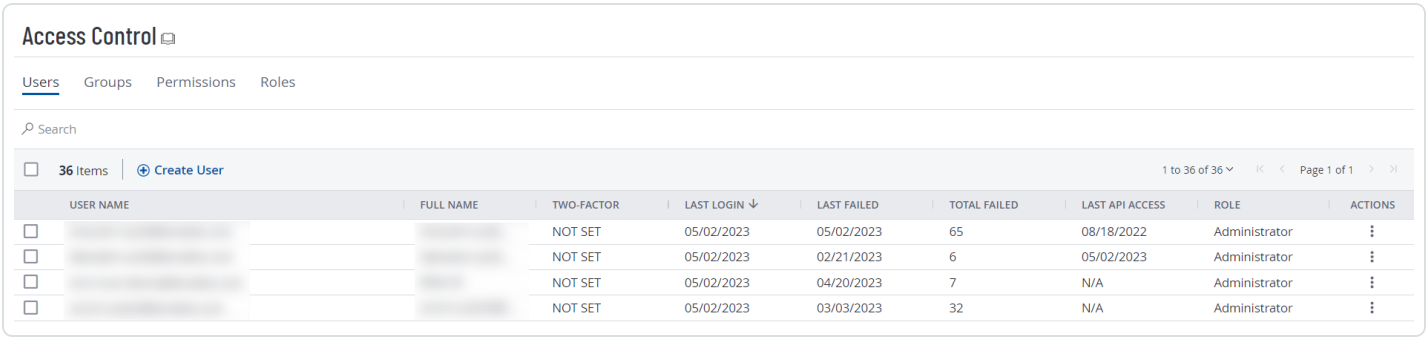
ライセンスマトリクス

ライセンス	AES/CES/ACR スコアをサポート
WAS のみ	×
WAS + Lumin のみ	○
EP ライセンス (WAS + Lumin を含む)	○
Tenable One ライセンス (Standard および Enterprise)	○

アクセス制御

必要なユーザーロール: 管理者

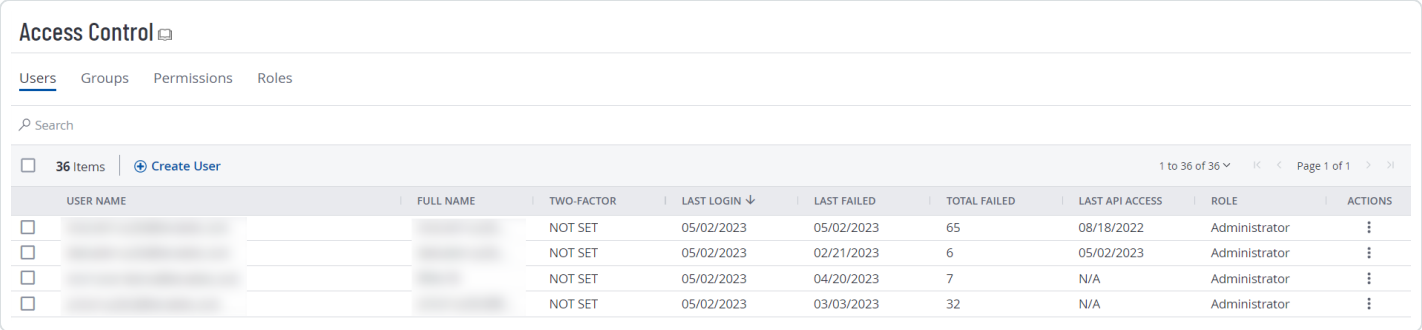
[アクセス制御] ページから、アカウントのユーザーとグループのリスト、およびそれらに割り当てられたアクセス許可を表示および設定できます。



ユーザー

このセクション内のトピックは、Tenable Vulnerability Management の主な機能強化の機能更新を反映するように変更されています。詳細は、Tenable Vulnerability Management Key Enhancements を参照してください。

アクセス制御 ページの **[ユーザー]** タブで、管理者ユーザーは Tenable Web App Scanning の組織のリソース用のユーザーアカウントを作成して管理できます。



ユーザーの表

列	説明
名前	アカウントのユーザー名
氏名	ユーザーのフルネーム
前回のログイン	ユーザーが最後に Tenable Web App Scanning インターフェースに正常にログインした日付
Last Failed	ユーザーが最後に Tenable Web App Scanning インターフェースへのログインに失敗した日付
Total Failed	ユーザーがログイン試行に失敗した合計回数 この数字は、管理者またはユーザーがユーザーアカウントのパスワードをリセットしたときにリセットされます。
Last API Access	ユーザーが最後に API キーを生成した日付
ロール	ユーザーに割り当てられたロール詳細は、ロールを参照してください。

アクション	管理者ユーザーがユーザーに対して実行できるアクション(ユーザーのエクスポートなど)

[ユーザー] ページでは、次のアクションを実行できます。

- ユーザーアカウントの作成
- ユーザーリストの表示
- ユーザーアカウントの編集
- 別のユーザーのパスワードの変更
- 各自のアカウントでユーザーをサポートする
- 別のユーザーの API キーを生成する
- ユーザーアカウントのロックの解除
- ユーザーアカウントの無効化
- ユーザーアカウントの有効化
- ユーザーアクセス認証情報の管理
- ユーザーアクティビティの監査
- ユーザーをエクスポートする
- Delete a User Account

ユーザーアカウントを作成する

必要なユーザーロール: 管理者

[ユーザー] ページで、新しいユーザーのアカウントを作成できます。

ヒント: SAML IdP によるアカウントの作成については、SAML のドキュメントを参照してください。

注意: ユーザーアカウントの有効期限は、そのアカウントが属する Tenable Web App Scanning コンテナの作成日に基づいて設定されます。Tenable は、この設定を直接制御します。詳細については、Tenable サポート にお問い合わせください。

ユーザーアカウントを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

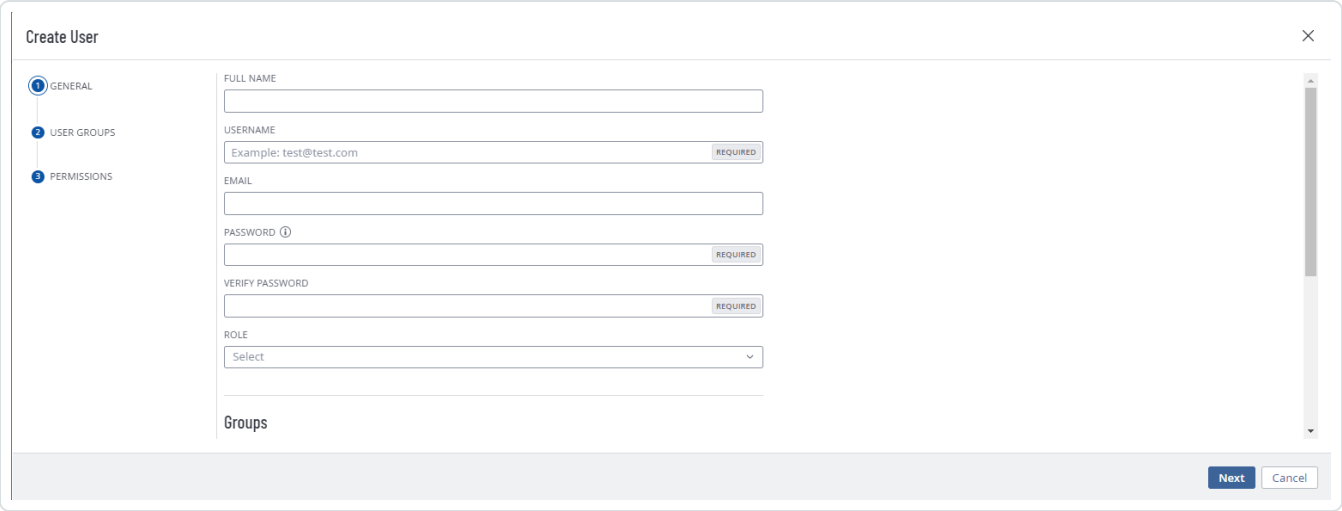
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ⊕ **[ユーザーの作成]** ボタンをクリックします。

   [ユーザーの作成] ページが表示されます。



5. 次のオプションを設定します。

注意: 各セクションのオプションを表示して設定するには、左側のメニューでセクションを選択する必要があります。

オプション	アクション
[一般] セクション	
氏名	ユーザーの氏名を入力します。
ユーザー名	有効なユーザー名を入力します。 有効なユーザー名は、次の形式である必要があります。 *name@domain* ここで、*domain* はお使いの Tenable Web App Scanning インスタンス用に承認されたドメインに対応します。 **注意:** 初期設定の間に、Tenable は Tenable Web App Scanning インスタンス用に承認されたドメインを設定します。インスタンスにドメインを追加する方法については、Tenable の担当者にお問い合わせください。 **注意:** Tenable Vulnerability Management のユーザー名に次の文字を含めることはできません:

	'、！ 、# 、$、% 、^、& 、*、(、)、/、\、|、{、}、[、]、"、:、;、 ~ 、`、<、>、,
メール	有効なメールアドレスを *name@domein* の形式で入力します。この *domain* は、お使いの Tenable Web App Scanning インスタンスで承認されたドメインになります。 このメールアドレスは、**[ユーザー名]** ボックスに設定されたメールアドレスをオーバーライドします。このオプションを空のままにすると、Tenable Web App Scanning は **[ユーザー名]** の値を、ユーザーのメールアドレスとして使用します。 **注意:** 管理者は、承認されていないドメインのメールアドレスで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作成後は、メールアドレスを別の承認されたドメインにのみ変更できます。
パスワード	有効なパスワードを入力します。詳細については、パスワード要件を参照してください。 Tenable Web App Scanning では、パスワードは最低 12 文字の長さで、次のものを含む必要があります。 • 大文字 • 小文字 • 数字 • 特殊文字
パスワードの確認	パスワードをもう一度入力します。
ロール	ドロップダウンボックスで、ユーザーに割り当てるロールを選択します。 **注意:** 管理者ユーザーには、Tenable Web App Scanning

	アカウントのすべてのリソースに対する完全なアクセス権があります。
認証	利用可能なセキュリティ設定オプションを選択または選択解除します。選択する場合、以下の設定があります。 **注意:** カスタムロールのあるユーザーに対して**パスワードアクセス**または**SAML**オプションを有効にすると、そのユーザーは自動的にダッシュボードおよびウィジェットへの基本的なアクセス権を持ちます。 • **API キー** - ユーザーがAPIキーを生成することを許可します。 **ヒント:** この設定だけを選択して、APIのみのユーザーアカウントを作成できます。 • **SAML** - ユーザーがSAMLシングルサインオン(SSO)を使用してアカウントにログインできるようにします。詳細は、SAMLを参照してください。 • **ユーザー名 / パスワード** - ユーザーがパスワードを使用してアカウントにログインできるようにします。 **注意:** このオプションの選択を解除すると、MFAオプションを選択できません。 • **二要素が必要です** - ユーザーが自分のアカウントにログインするには二要素認証の入力が必要です。 **ヒント:** マイアカウントページで、自分のアカウントに二要素認証を設定できます。
[ユーザーグループ] セクション	
ユーザーグループ	ユーザーの割当先となる1つまたは複数のユーザーグルー

	プを選択します。 デフォルトでは、新しいユーザーはシステム生成の**[すべてのユーザー]**ユーザーグループに属し、これによって**[基本]**ロールが割り当てられます。 次の手順でユーザーグループを追加します。 • **[ユーザーグループ]**ボックスの任意の場所をクリックします。 検索ボックスとロールのドロップダウンリストが表示されます。 • (オプション)**[検索]**ボックスに、ユーザーグループ名を入力します。 入力すると、検索条件に一致するユーザーグループのリストが表示されます。 • 追加するユーザーグループをクリックします。 **[ユーザーグループ]**ボックスに、Tenable Web App Scanningによってユーザーグループを表すラベルが追加されます。 • これらの手順を繰り返して、別のユーザーグループにユーザーを追加します。
[アクセス許可]セクション	
アクセス許可	**[アクセス許可]**の表で、ユーザーに割り当てるアクセス許可設定を選択します。

6. **[保存]**をクリックします。

> **注意:** ユーザーにアクセス許可を割り当てると、ボタンは**[追加して保存]**と表示されます。

Tenable Web App Scanningによって新しいユーザーアカウントが一覧表示されます。

ユーザーアカウントの編集

必要なユーザーロール: 管理者

ユーザーアカウントを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、編集するユーザーの名前をクリックします。

   [ユーザーの編集] ページが表示されます。

5. 次のオプションを設定します。

オプション	アクション
アカウント設定	
Full Name	ユーザーの氏名を編集します。
ユーザー名	このオプションは編集できません。
メール	有効なメールアドレスを *name@domein* の形式で入力します。この *domain* は、お使いの Tenable Web App Scanning インスタンスで承認されたドメインになります。 このメールアドレスは、**[ユーザー名]** ボックスに設定されたメールアドレスをオーバーライドします。このオプションを空のままにすると、Tenable Web App Scanning は **[ユーザー名]** の値を、ユーザーのメールアドレスとして使用します。

	注意: 管理者は、承認されていないドメインのメールアドレスで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作成後は、メールアドレスを別の承認されたドメインにのみ変更できます。
新しいパスワード	有効なパスワードを入力します。詳細については、パスワード要件を参照してください。 Tenable Web App Scanning では、パスワードは最低 12 文字の長さで、次のものを含む必要があります。 • 大文字 • 小文字 • 数字 • 特殊文字
ロール	ドロップダウンボックスから、ユーザーに割り当てるロールを選択します。
グループ	
User Groups	ユーザーを割り当てる 1 つまたは複数のユーザーグループを選択します。ユーザーは、そのユーザーグループに関連付けられているロールとアクセス許可を継承します。
セキュリティ設定	利用可能なセキュリティ設定オプションを選択または選択解除します。選択する場合、以下の設定があります。 • **API** - ユーザーが API キーを生成することを許可します。 **ヒント:** この設定だけを選択して、API のみのユーザーアカウントを作成できます。 • **SAML** - ユーザーが SAML シングルサインオン (SSO) を使用してアカウントにログインできるようにします。詳細は、SAML を参照してください。 • **Password Access** - ユーザーがパスワードを使用してアカウントにログインできるようにします。

	注意： このオプションの選択を解除すると、MFA オプションを選択できません。 • **MFA** - ユーザーが自分のアカウントにログインするためには二要素認証の入力が必要です。 **ヒント：** My Accountページで、自分のアカウントに二要素認証を設定できます。

6. (オプション) ユーザーの API キーを生成します
7. **[保存]** をクリックします。

   Tenable Web App Scanning はアカウントへの変更を保存します。

ユーザーリストの表示

必要なユーザーロール: 管理者

アクセス制御ページの**[ユーザー]**タブで、Tenable Web App Scanning インスタンス上のすべてのユーザーのリストを表示できます。

Tenable Web App Scanning インスタンスのユーザーとユーザーデータを表示する方法

1. 左のナビゲーションプレーンで**[設定]**をクリックします。

   [設定]ページが表示されます。

2. **[アクセス制御I]**タイルをクリックします。

   [アクセス制御]ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

3. **[ユーザー]**タブをクリックします。

   [ユーザー]タブが開き、Tenable Web App Scanning インスタンス上のすべての Tenable Web App Scanning ユーザーアカウントの表が表示されます。このドキュメントでは、この表をユーザー表と呼びます。

ユーザー表

ユーザー表で、Tenable Web App Scanning インスタンス上のユーザーに関する以下の情報を表示できます。

列	説明
名前	アカウントのユーザー名
前回のログイン	ユーザーが最後に Tenable Web App Scanning インターフェースに正常にログインした日付
Last Failed	ユーザーが最後に Tenable Web App Scanning インターフェースへのログインに失敗した日付
Total Failed	ユーザーがログイン試行に失敗した合計回数 この数字は、管理者またはユーザーがユーザーアカウントのパスワードをリセットした

	ときにリセットされます。
Last API Access	ユーザーが最後に API キーを生成した日付
ロール	ユーザーに割り当てられたロール詳細は、ロールを参照してください。
アクション	管理者ユーザーがユーザーに関して実行できるアクション (ユーザーのエクスポートなど)

Tenable Web App Scanning のパスワード要件

Tenable Web App Scanning はすべてのアカウントに対し、次のパスワード要件を適用します。

パスワード基準

パスワードは最低 12 文字の長さで、次のものを含む必要があります。

- 大文字
- 小文字
- 数字
- 特殊文字

パスワードの有効期限

Tenable Web App Scanning のパスワードに有効期限はありません。

アカウントのロックアウト

デフォルトでは、ログイン試行が 5 回失敗すると、Tenable Web App Scanning はユーザーをアカウントからロックアウトします。ユーザーが自分のアカウントからロックアウトされた場合、ユーザー自身が自分のアカウントのロックを解除するか、管理者がパスワードをリセットします。

パスワード履歴

現在のパスワードや以前のパスワードを再利用することはできません。

別のユーザーのパスワードの変更

必要なユーザーロール: 管理者

別のユーザーアカウントのパスワードを変更するには、管理者の権限が必要です。自分自身のパスワードを変更するには、パスワードを変更するを参照してください。

別のユーザーのパスワードを変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、編集するユーザーの名前をクリックします。

   [ユーザーの編集] ページが表示されます。

5. **[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。詳細については、「パスワード要件」を参照してください。

6. **[保存]** をクリックします。

   Tenable Web App Scanning は、ユーザーアカウントの新しいパスワードを保存します。

各自のアカウントでユーザーをサポートする

必要なユーザーロール: 管理者

管理者として、ユーザーサポート機能を使用し、別のアカウントとしてログインをシミュレートできます。ユーザーアカウントをサポートする間、そのユーザーのパスワードを取得したり、管理者アカウントからログアウトしたりすることなく、そのユーザーとして Tenable Vulnerability Management で操作できます。

注意: **ユーザーアシスト**は、次の認証設定のいずれかまたは両方が有効になっているユーザーアカウントでのみ使用できます。

- **ユーザー名 / パスワード**
- **SAML**

これらのセキュリティ設定を有効にするには、ユーザーアカウントの編集を参照してください。

各自のアカウントでユーザーをサポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、サポートするユーザーアカウントのチェックボックスをクリックします。

   表の上部にアクションバーが表示されます。

   注意: 一度に選択できるユーザーは 1 人だけです。

5. アクションバーで、👤 ボタンをクリックします。

   により、サポートしているユーザー用のデフォルトのダッシュボードが更新されて表示されます。ユーザーをサポートしている間、の各ページの上部にはサポートしているユーザーのロールを記載したオーバーレイが表示されます。

各自のアカウントでユーザーのサポートを停止する方法

- 任意のページの上部にある、サポート中のユーザーのロールが表示されているオーバーレイで ✕ ボタンをクリックします。

別のユーザーの API キーの生成

必要なユーザーロール: 管理者

お使いのユーザーアカウントに関連付けられた API キーにより、お客様の企業にライセンスされた、すべての Tenable Vulnerability Management 製品の API にアクセスすることが可能になります。これらのキーは、Tenable Vulnerability Management REST API での認証に使用する必要があります。

管理者は、任意のアカウントの API キーを生成できます。他のロールは、自分自身のアカウントの API キーを生成できます。詳細は、Generate API Keysを参照してください。

注意: お使いのユーザーアカウントに関連付けられた API キーを使って、お客様の会社にライセンス付与されているすべての Tenable Vulnerability Management 製品の API にアクセスすることができます。個別の製品に別々のキーを設定することはできません。たとえば、Tenable Vulnerability Management で API キーを生成した場合、この操作により Tenable Web App Scanning および Tenable Container Security の API キーも変更されます。

別のユーザーの API キーを生成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、編集するユーザーの名前をクリックします。

   [ユーザーの編集] ページが表示されます。

5. **[API キー]** セクションで、**[API キーの生成]** をクリックします。

   警告: 新しい API キーを生成すると、既存の API キーはすべて置き換えられます。以前の API キーを使用していたアプリケーションを更新する必要があります。

   警告メッセージが表示されます。

6. 警告を確認し、**[置き換えと生成]**をクリックします。

   [API キーの生成]テキストボックスが表示されます。

   アカウントの新しいアクセスキーと秘密鍵がテキストボックスに表示されます。

7. (オプション)**[API キーの再生成]**をクリックします。

8. 新しいアクセスキーと秘密鍵を安全な場所にコピーします。

   警告:[ユーザーの編集]ページから移動する前に、アクセスキーと秘密鍵を必ずコピーしてください。このページを閉じてしまうと、Tenable Web App Scanning からキーを取得することはできなくなります。

ユーザーアカウントのロックの解除

Tenable Web App Scanning でログインを試みて 5 回連続して失敗すると、アカウントがロックされます。

> **注意:** ユーザーは、ユーザーインターフェースからロックアウトされる可能性がありますが、適切な認証 (api_permit) が割り当てられている場合は API リクエストを送信できます。詳細は、Tenable 開発者ポータルを参照してください。

次のいずれかの方法で、ユーザーアカウントのロックを解除できます。

- ユーザーがユーザーアカウントで指定されたメールアドレスにアクセスできる場合、ユーザーは自分のアカウントのロックを解除できます。
- ユーザーが上記メールアドレスにアクセスできない場合、管理者権限を持つ別のユーザーがそのユーザーのパスワードをリセットできます。

ユーザーアカウントの無効化

必要なユーザーロール: 管理者

ユーザーアカウントを無効にすると、ユーザーがログインできなくなり、そのユーザーのスキャンが実行されなくなります。無効のユーザーアカウントを有効にする方法については、ユーザーアカウントの有効化を参照してください。

重要: ユーザーアカウントを無効にしても、そのユーザーに対してスケジュールされたレポートは無効になりません。さらに、無効なユーザーが他のユーザーとレポートを共有した場合、これらの他のユーザーはそのレポートを生成できます。詳細は、Reportsを参照してください。

ユーザーアカウントを無効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. 無効にする1人または複数人のユーザーを選択します。

   - 1人のユーザーを選択する場合

     a. で、無効にするユーザーアカウントの行にある ⋮ ボタンをクリックします。

        アクションボタンが行に表示されます。

     b. 行にある ⊘ ボタンをクリックします。

        確認ウィンドウが表示されます。

   - 複数のユーザーを選択する場合

a. で、無効にする各ユーザーのチェックボックスをクリックします。

ページの下部またはテーブルの上部に、アクションバーが表示されます。

b. アクションバーで、⊘ ボタンをクリックします。

確認ウィンドウが表示されます。

5. 確認ウィンドウで、**[無効化]** をクリックします。

成功したことを示すメッセージが表示され、

Tenable Web App Scanning により、選択した 1 人または複数のユーザーが無効になります。で、無効になったユーザーは薄いグレーで表示されます。

> **注意:** 無効にされたユーザーに進行中のセッションがある場合は、引き続き制限付きのアクセス権が付与される場合があります。ただし、ログアウト後は再度ログインできません。

ユーザーアカウントの有効化

必要なユーザーロール: 管理者

ユーザーアカウントを無効にした場合は、アカウントを再度有効にしてユーザーのアクセスを復元できます。

ユーザーアカウントを有効にするには:

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. 有効にする 1 人または複数のユーザーを選択します。

   ### 1 人のユーザーを選択します。

   a. で、有効にするユーザーアカウントの行にある ⋮ ボタンをクリックします。

      アクションボタンが行に表示されます。

      > **注意:** ユーザーが無効になっている場合はグレー表示されます。

   b. 行にある ✓ ボタンをクリックします。

      確認ウィンドウが表示されます。

   ### 複数のユーザーを選択します。

   a. で、有効にする各ユーザーのチェックボックスをクリックします。

      ページの下部またはテーブルの上部に、アクションバーが表示されます。

b. アクションバーで、✓ ボタンをクリックします。

確認ウィンドウが表示されます。

5. 確認ウィンドウで、**[有効]** をクリックします。

成功したことを示すメッセージが表示され、

Tenable Web App Scanning により、選択した 1 人または複数のユーザーが有効になります。ユーザーテーブルで、有効になったユーザーは黒で表示されます。

ユーザーアクセス認証情報の管理

ユーザーは、次の方法を使用して Tenable Web App Scanningにアクセスできます。

- ユーザー名とパスワードログイン
- シングルサインオン(SSO)詳細は、SAML を参照してください。
- Tenable Web App Scanning REST API(API キー使用)詳細は、別のユーザーの API キーの生成 を参照してください。

新規ユーザーを作成すると、すべてのアクセス権がデフォルトで認証されます。企業のセキュリティポリシーに応じて、SSO を強化するためにユーザ名およびパスワードログインを無効化するなど、特定のアクセス方法を無効化できます。

Tenable Web App Scanning Platform API を使用して、ユーザーのアクセス認証の表示、付与、失効ができます。詳細については、Tenable 開発者ポータルのユーザー認証を取得するおよびユーザー認証を更新するを参照してください。

ユーザーアクティビティの監査

必要なユーザーロール: 管理者

Tenable Web App Scanning では、監査ログによって企業の Tenable Web App Scanning アカウントで実行されるユーザーイベントが記録されます。各イベントで、ログには次に関する情報が含まれます。

- 実行されたアクション
- アクションが実施された時期
- ユーザー ID
- ターゲットのエンティティ ID

監査ログは、企業内のユーザーが Tenable Web App Scanning で行ったアクションに対する可視性をもたらし、セキュリティ上の課題や他の潜在的な問題を特定するのに役立ちます。

企業の Tenable Web App Scanning アカウントの監査ログを表示する方法

- Tenable 開発者ポータルでの記載内容に従い、**[監査ログ]** エンドポイントを使用します。

ログに記録されるイベント

監査ログイベントには以下が含まれます。

アクション	説明
audit.log.view	システムが監査ログリクエストを受け取り、処理しました。
session.create	システムが、ユーザーに対するセッションを作成しました。このイベントは、ユーザーのログインによってトリガーされます。
session.delete	セッションが期限切れとなったか、またはユーザーがセッションを終了しました。
session.impersonation.end	管理者が、別のユーザーになりすますセッションを終了しました。
session.impersonation.start	管理者が、別のユーザーになりすますセッションを開始しました。

user.authenticate.mfa	二要素認証が成功し、ログインが許可されました。
user.authenticate.password	ユーザーがパスワードを使用してセッションの開始を認証しました。
user.create	管理者が新しいユーザーアカウントを作成しました。
user.delete	管理者がユーザーアカウントを削除しました。
user.impersonation.end	管理者が、他のユーザーへのなりすましを停止しました。
user.impersonation.start	管理者が、他のユーザーへのなりすましを開始しました。
user.logout	ユーザーがセッションからログアウトしました。
user.update	管理者またはユーザーのどちらかが、ユーザーアカウントを更新しました。

ユーザーをエクスポートする

必要なユーザーロール: 管理者

[ユーザー] ページでは、1 人以上のユーザーを CSV または JSON 形式でエクスポートできます。

ユーザーをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ユーザー]** タブをクリックします。

   [ユーザー] ページが表示されます。このページの表には、Tenable Web App Scanning インスタンスのすべてのユーザーが一覧表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Web App Scanning ワークベンチの表 を参照してください。

6. エクスポートするユーザーを選択します。

エクスポート範囲	アクション
選択したユーザー	選択したユーザーをエクスポートする方法 a. で、エクスポートする各ユーザーのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。

	注意： [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。 200 人以上のユーザーをエクスポートする場合は、リスト内のすべてのユーザーを選択して、[→ **[エクスポート]** をクリックします。
1 人のユーザー	1 人のユーザーをエクスポートする方法 a. で、エクスポートするユーザーの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- ユーザーの表の **[アクション]** 列で、エクスポートするユーザーの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意： デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	ユーザーのリストを含む CSV テキストファイル

	注意: .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたユーザーのリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Web App Scanning では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Web App Scanning がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Web App Scanning がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Web App Scanning によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

ユーザーアカウントを削除する

必要なユーザーロール: 管理者

ユーザーアカウントを削除する前に、ユーザーアカウントを無効にする必要があります。

警告: ユーザーアカウントを削除すると、アカウントを復元することも、操作を元に戻すこともできません。

警告: Tenable Web App Scanning はオブジェクトの移行をサポートしていません。Tenable Web App Scanning ユーザーを削除すると、アプリケーションは削除されたユーザーに属するオブジェクトを再割り当てしません。所有者が削除された場合、Tenable Web App Scanning スキャンを新しい所有者に再割り当てすることはできません。

警告: ユーザーアカウントを削除する前に、関連する修正プロジェクトを割り当て直してください。これらは自動的には再割り当てされません。

次の表に、ユーザーを削除したときにどのオブジェクトが移行、保持、または完全に削除されるかを示します。

オブジェクトタイプ	削除	注記
スキャンの監査ファイル	○	完全に削除
スキャンのスケジュール	×	新しいオブジェクト所有者に移行 **注意:** 移行されたスキャンスケジュールは、完全に削除された他のオブジェクト (監査ファイル、ターゲットグループ、管理されていない認証情報など) に依存している場合は無効になることがあります。
過去のスキャン結果	×	新しいオブジェクト所有者に移行
スキャンテンプレート	×	新しいオブジェクト所有者に移行
スキャンの管理されていな	○	完全に削除

オブジェクトタイプ	削除	注記
い認証情報		
カスタムダッシュボード/ウィジェット	○	完全に削除
認証情報の管理	×	保持 (**[作成者]** 値に **[null]** が表示)
タグ	×	保持 (**[作成者]** 値に **[null]** が表示)
変更/許容ルール	×	保持 (**[所有者]** 値に **[不明なユーザー]** が表示)
除外	×	保持
システムターゲットグループ	×	保持
User Target Groups	×	新しいオブジェクト所有者に移行
保存された検索条件	○	完全に削除
コネクタ	×	保持
センサー	×	保持

ユーザーアカウントの削除手順

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

[アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、削除するユーザーアカウントの行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

5. メニューにある 🗑 ボタンをクリックします。

   注意: ユーザーが無効になっていない場合は、🗑 ボタンは表示されません。ユーザーを削除する前にユーザーを無効にします。

   注意: デフォルトの管理者アカウントを削除することはできません。デフォルトの管理者アカウントを削除する場合は、Tenable サポート に連絡する必要があります。

   ユーザー画面が表示されます。

6. **[新しいオブジェクト所有者の選択]** ドロップダウンリストボックスから、ユーザーのオブジェクト (スキャン結果、ユーザー定義スキャンテンプレートなど) の転送先のユーザーを選択します。

7. 🗑 **[削除]** をクリックします。

   確認のメッセージが表示されます。

8. **[削除]** をクリックします。

   Tenable Web App Scanningユーザーを削除し、ユーザーオブジェクトを指定されたユーザーに転送します。

ユーザーグループ

このセクション内のトピックは、Tenable Vulnerability Management の主な機能強化の機能更新を反映するように変更されています。詳細は、Tenable Vulnerability Management Key Enhancements を参照してください。

ユーザーグループを使用して、Tenable Web App Scanning のさまざまなリソースのユーザーのアクセス許可を管理することができます。ユーザーをグループに割り当てると、ユーザーはグループに割り当てられたアクセス許可を継承します。企業では、グループを使用して、ユーザーのロールや企業のセキュリティ方針に基づいてユーザーにアクセス許可を割り当てることができます。

注意: ユーザーグループがユーザーアカウントおよびアクセスグループとやり取りする方法の例については、例: アクセスグループを参照してください。

ユーザーグループを表示するには、次の手順を使用します。

1. 左のナビゲーションプレーンで **[設定]** をクリックします。

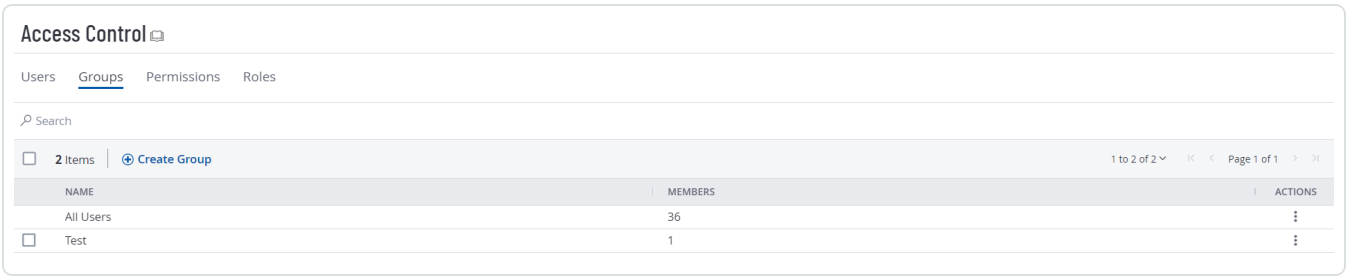
   [設定] ページが表示されます。

2. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

3. **[グループ]** タブをクリックします。

   [グループ] ページが表示されます。



[ユーザーグループ] ページに、Tenable Web App Scanning インスタンス内のすべてのユーザーグループの表が表示されます。このドキュメントでは、この表を*ユーザーグループの表*と呼びます。

ユーザーグループの表には次の列が含まれています。

列	説明
名前	グループ名。Tenable によって提供されている **[すべてのユーザー]** グループと **[管理者]** グループを除くすべてのユーザーグループにこの名前を定義することができます。
Members	ユーザーグループに割り当てられているユーザーの数
アクション	グループで実行できるアクション

[グループ] タブでは、次のアクションを実行できます。

- グループを作成する
- グループを編集する
- グループのエクスポート
- グループを削除する

ユーザーグループを作成する

必要なユーザーロール: 管理者

ユーザーグループを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

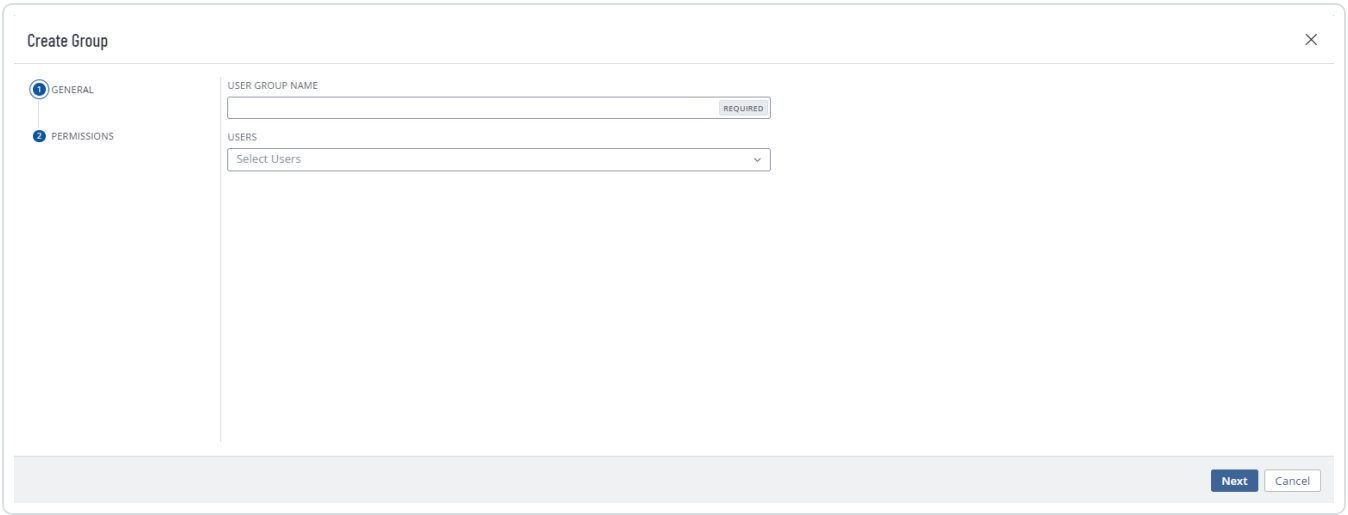
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ユーザーグループの表の上部にある ⊕ **[ユーザーグループの作成]** ボタンをクリックします。

   [グループの作成] ページが表示されます。



5. **[ユーザーグループ名]** ボックスで、新規グループの名前を入力します。

6. ユーザーをグループに追加します。

a. 追加するユーザーごとに、[ユーザー]ドロップダウンボックスをクリックして、ユーザー名の入力を始めます。

入力に伴い、Tenable Web App Scanning は検索に一致するよう、ドロップダウンボックスのユーザーリストを絞り込みます。

b. ドロップダウンボックスでユーザーを選択します。

Tenable Web App Scanning は、ユーザーグループに追加するユーザーのリストにそのユーザーを追加します。

> **ヒント:** 追加するユーザーリストからユーザーを削除するには、そのユーザーにカーソルを合わせて ✕ ボタンをクリックします。

7. **[保存]**をクリックします。

Tenable Web App Scanning はユーザーグループを作成し、リスト化されたユーザーをメンバーとして追加します。

[**Groups**] ページが表示され、ユーザーグループの表にリストされている新しいグループを確認できます。

ユーザーグループを編集する

必要なユーザーロール: 管理者

グループを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ユーザーグループの表で、編集するユーザーグループをクリックします。

   [ユーザーグループの編集] ページが表示されます。

5. 次のいずれかを行います。

   - **[ユーザーグループ名]** ボックスに新しいグループ名を入力します。
   - ユーザーをグループに追加する場合

     a. 追加するユーザーごとに、**[ユーザー]** ドロップダウンボックスをクリックして、ユーザー名の入力を始めます。

     入力に伴い、Tenable Web App Scanning は検索に一致するよう、ドロップダウンボックスのユーザーリストを絞り込みます。

     b. ドロップダウンボックスでユーザーを選択します。

     Tenable Web App Scanning は、ユーザーグループに追加するユーザーのリストにそのユーザーを追加します。

   - ユーザーをグループから削除する場合

a. **[ユーザー]** リストで、削除するユーザーアカウントの横にある × ボタンをクリックします。

Tenable Vulnerability Management により、そのユーザーが **[ユーザー]** リストから削除されます。

- グループのアクセス許可を追加または削除します。

6. **[保存]** をクリックします。

Tenable Web App Scanning により、変更したユーザーグループが保存されます。

[**Groups**] ページが表示され、ユーザーグループの表にリストされている新しいグループを確認できます。

グループのエクスポート

必要なユーザーロール: 管理者

アクセス制御ページの**[グループ]**タブでは、1つ以上のユーザーグループをCSVまたはJSON形式でエクスポートできます。

ユーザーグループをエクスポートする方法

1. 左上にあるボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで**[設定]**をクリックします。

   [設定]ページが表示されます。

3. **[アクセス制御I]**タイルをクリックします。

   [アクセス制御]ページが表示されます。このページで、Tenable Web App Scanningアカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[グループ]**タブをクリックします。

   [グループ]タブが開き、Tenable Web App Scanningインスタンス内のすべてのユーザーグループを一覧にした表が表示されます。

5. (オプション)表データを選別します。詳細は、Tenable Web App Scanning ワークベンチの表を参照してください。

6. 次のいずれかを行います。

1つのグループをエクスポートする場合

a. グループの表で、エクスポートするグループの行を右クリックします。

   アクションオプションがカーソルの横に表示されます。

   -または-

   グループの表の**[アクション]**列で、エクスポートするグループの行にあるボタンをクリックします。

アクションボタンが行に表示されます。

b. **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス

複数のグループをエクスポートする場合

a. グループの表で、エクスポートする各グループのチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで、[→ **[エクスポート]** をクリックします。

> **注意:** 個別に選択してエクスポートできるグループは最大 200 個です。200 個以上のグループをエクスポートする場合は、グループの表の上部にあるチェックボックスを選択して、Tenable Web App Scanning インスタンス上のすべてのグループを選択してから、[→ **[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  > **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	グループのリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたグループのリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    > **注意**: Tenable Web App Scanning では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。
    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。

- **[タイムゾーン]**ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
- **[繰り返し]**ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
- **[繰り返し終了]**ドロップダウンで、スケジュールが終了する日付を選択します。

  注意: [無し]を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]**トグルをクリックします。

      [メール通知]セクションが表示されます。
    - **[受信者の追加]**ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須)**[パスワード]**ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      注意: Tenable Web App Scanning がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]**をクリックします。

    Tenable Web App Scanning がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Web App Scanning によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]**でエクスポートファイルにアクセスできます。

グループを削除する

必要なユーザーロール: 管理者

注意: Tenable 提供の**[管理者]**または**[すべてのユーザー]**のユーザーグループを削除することはできません。

始める前に

- すべてのユーザーをユーザーグループから削除します。ユーザーが含まれているユーザーグループを削除することはできません。

1 つ以上のユーザーグループを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで**[設定]**をクリックします。

   [設定]ページが表示されます。

3. **[アクセス制御I]**タイルをクリックします。

   [アクセス制御]ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[グループ]**タブをクリックします。

   [グループ]ページが表示されます。このページの表に、Tenable Web App Scanning アカウントのすべてのユーザーグループがリストされます。

5. 次のいずれかを行います。

   - 1 つのユーザーグループを削除する方法

     a. ユーザーグループの表で、削除するユーザーグループの ⋮ ボタンをクリックします。

     メニューが表示されます。

     b. 🗑 **[削除]**ボタンをクリックします。

     確認ウィンドウが表示されます。

- 複数のユーザーグループを削除する方法

  a. ユーザーグループの表で、削除す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。

     表の上部にアクションバーが表示されます。

  b. アクションバーで、**[削除]** ボタンをクリックします。

     確認ウィンドウが表示されます。

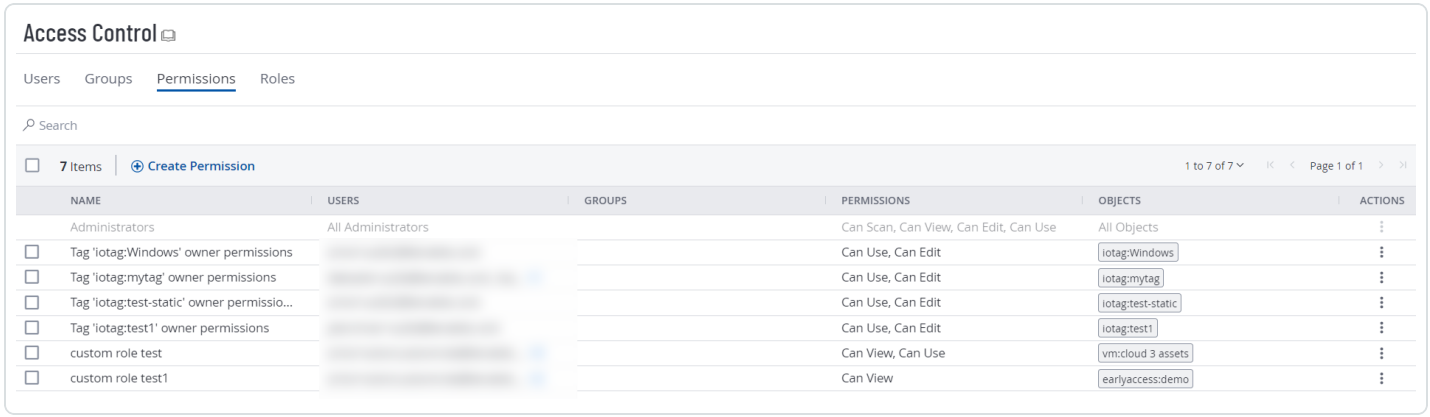
6. 確認ウィンドウで、**[削除]** をクリックします。

   Tenable Web App Scanningにより、選択した1つまたは複数のユーザーグループが削除されます。削除されたグループは、ユーザーグループの表に表示されなくなります。

権限

Tenable Web App Scanning では、企業のアカウントで企業のリソースとデータに対して特定のアクションを実行できるユーザーを決定する設定を作成および管理できます。このドキュメントでは、これらの設定を***アクセス許可設定***[1]と呼びます。

[マイアカウント] ページで、各ユーザーは自分に割り当てられたアクセス許可設定を表示できます。ただし、他のユーザーのアクセス許可設定を表示または管理できるのは、管理者ユーザーのみです。詳細は、Tenable 提供のロールと権限 を参照してください。



ユーザーまたはユーザーグループを作成する場合、過去に作成したタグで指定された条件を満たす資産に対して、既存のアクセス許可設定をそれらに割り当てることができます。Tenable Web App Scanning では、これらの資産とそれらを定義するタグを***オブジェクト***[2]と言います。

ロールとアクセス許可の違いは何ですか?

- ロール - ロールにより、Tenable Web App Scanning の主要機能の権限を管理し、ユーザーがアクセスできる Tenable Web App Scanning モジュールや機能を制御できます。
- アクセス許可 - アクセス許可により、タグ、資産、その検出結果など、自分のデータへのアクセスを管理できます。

アクセス許可設定を作成する場合は、以下にある定義済みのアクセス許可を 1 つ以上選択する必要があります。これらのアクセス許可は、アクセス許可設定で定義された 1 つまたは複数のオブジェクトに対してユーザーが実行できるアクションを決定します。

---

[1]特定のユーザーおよびグループが特定のリソースセットで実行できるアクションを決定するために、管理者が作成できる設定です。
[2]アクセス許可設定において、アクセス許可を定義する資産とタグのことです。

アクセス許可	説明
閲覧可	ユーザーまたはグループがオブジェクトによって定義された資産を表示できるようにします。 **注意**: Tenable Lumin ライセンスをお持ちの場合、資産の詳細を表示するには、その資産に対する **[閲覧可]** アクセス許可が必要です。ただし、アカウントにライセンスが付与されている資産の合計数は、アクセス許可に関わらず表示することができます。CES (Cyber Exposure Score) と AES (資産のエクスポージャースコア) の値も表示できます。これらは、アカウントにライセンスが付与されているすべての資産のリスクの合計に基づきます。詳細は、Tenable Lumin Metrics を参照してください。
スキャン可	ユーザーまたはグループがオブジェクトによって定義された資産をスキャンできるようにします。 **注意:** 手動で入力されたターゲットが有効と見なされるには、次の基準を満たす必要があります。 • ユーザーが管理者である、 または • ユーザーに少なくともスキャンオペレーターロール権限があり、かつ • ターゲットが Tenable Web App Scanning システム内に存在しない場合、ユーザーは IPv4、IPV6 または FQDN を介してターゲットを明示的に参照するオブジェクトに対する**スキャン可能**アクセス許可を持っている必要があります。オブジェクトに複数のルールがある場合、それらのルールは「いずれかに一致」フィルターで結合される必要があります。または • ターゲットが Tenable Web App Scanning システム内に既に存在する場合、ユーザーが**スキャン可能**アクセス許可を持つオブジェクトによってターゲットがタグ付けされる必要があります。
編集可	ユーザーまたはグループがオブジェクトを定義するタグを編集できるようにします。
使用可	ユーザーまたはグループがオブジェクトを定義するタグを使用できるようにします。

Tenable Web App Scanning でアクセス許可設定を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

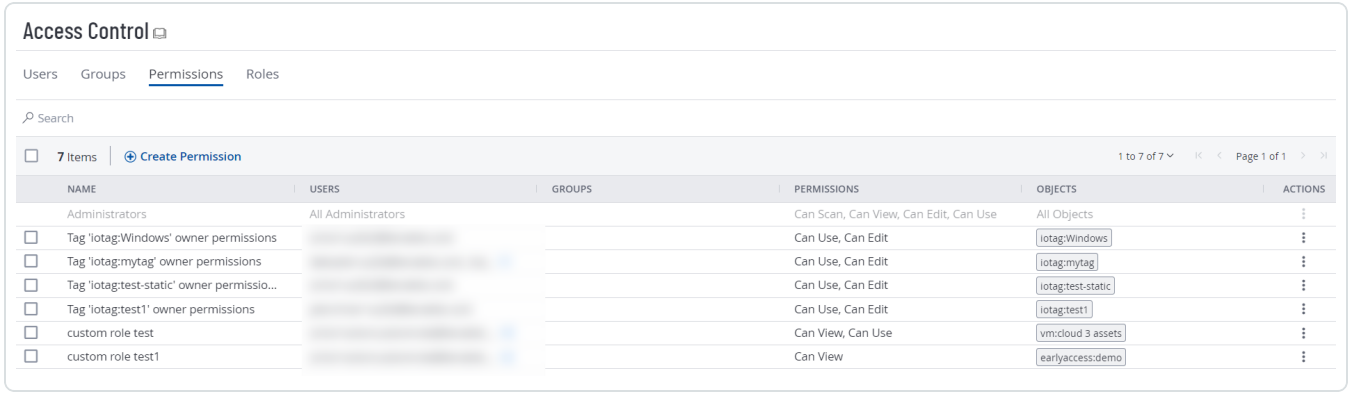
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Web App Scanning インスタンスのすべてのアクセス許可設定が一覧表示されます。



> **注意:** アクセス許可の表の最初の行には、管理者の読み取り専用エントリが含まれています。このエントリは、管理者がアカウントのすべてのリソースに対するすべてのアクセス許可を持っていることを示すために存在します。詳細は、ロールを参照してください。

[アクセス許可] タブでは、次のアクションを実行できます。

- アクセス許可設定の作成および追加
- ユーザーまたはグループへのアクセス許可設定の追加
- アクセス許可設定の編集
- アクセス許可設定のエクスポート

- ユーザーまたはユーザーグループからアクセス許可設定を削除する
- アクセス許可設定の削除

アクセス許可設定の作成および追加

必要なユーザーロール: 管理者

Tenable Web App Scanning でアクセス許可設定を作成すると、その設定を 1 人以上のユーザーまたはグループに適用できます。

始める前に

- Tenable Web App Scanning アカウントのユーザーまたはグループを作成します。
- アクセス許可を作成するオブジェクトのタグを作成します。

ユーザーまたはグループにアクセス許可設定を作成および追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

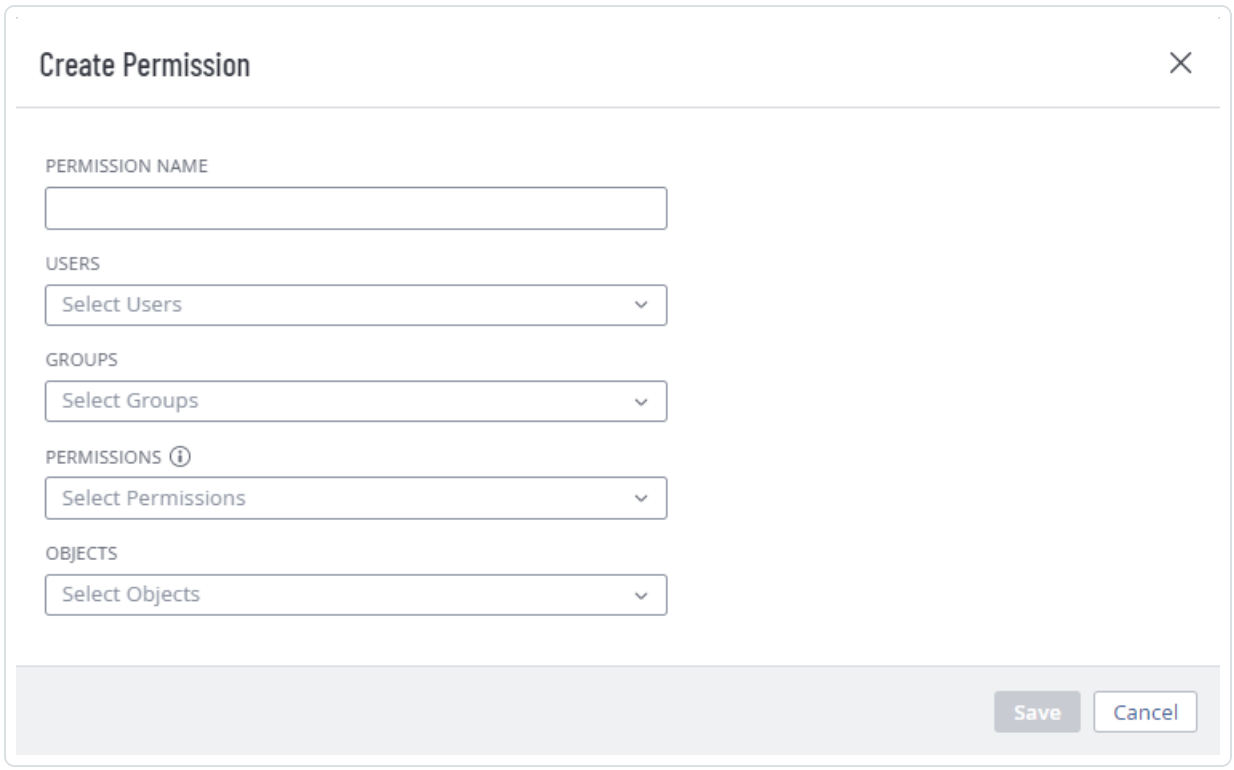
   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Web App Scanning インスタンスのすべてのアクセス許可設定が一覧表示されます。

5. 表の上部にある **[アクセス許可を作成]** をクリックします。

   [アクセス許可を作成] ウィンドウが表示されます。



6. **[アクセス許可名]**ボックスに、アクセス許可設定の名前を入力します。
7. (オプション)**[ユーザー]**ドロップダウンボックスで、1人以上のユーザーを選択します。

   注意:[ユーザー]ボックスはオプションですが、少なくとも1人のユーザーまたはユーザーグループが選択されていない限り、アクセス許可設定を保存することはできません。

8. (オプション)**[グループ]**ドロップダウンボックスで、1つ以上のユーザーグループを選択します。

   注意:[グループ]ボックスはオプションですが、少なくとも1人のユーザーまたはユーザーグループが選択されていない限り、アクセス許可設定を保存することはできません。

   注意:[グループ]ドロップダウンボックスで**[すべてのユーザー]**を選択して、Tenable Web App Scanningインスタンス上のすべてのユーザーにアクセス許可設定を割り当てることができます。ただし、アクセス許可設定をすべてのユーザーに割り当てることはセキュリティのベストプラクティスに反するため、Tenableは慎重に行うことを推奨しています。

9. **[アクセス許可]**ドロップダウンボックスで、1つ以上のアクセス許可を選択します。

注意: **[編集可]** アクセス許可を **[表示可]** または **[スキャン可]** アクセス許可とともにアクセス許可設定に追加すると、割り当てられたユーザーは、表示およびスキャンできる資産の範囲を変更することができるようになります。Tenable は、**[編集可]** アクセス許可に **[表示可]** または **[スキャン可]** を組み合わせるのは、管理者ユーザーにのみ行うことを推奨しています。

注意: **[編集可]** アクセス許可を選択すると、Tenable Web App Scanning によって **[使用可]** アクセス許可が自動的に追加されます。

10. **[オブジェクト]** ドロップダウンボックスで、アクセス許可設定を適用するオブジェクトを 1 つ以上選択します。

    注意: ドロップダウンボックス内のオブジェクトは、資産を識別および定義する前に作成されたタグです。詳細については、アクセス許可を参照してください。

    ヒント: **[すべての資産]** を選択すると、資産が既存のオブジェクトに一致するかどうかに関係なく、ユーザーとグループがインスタンス上のすべての資産を表示またはスキャンできるようになります。また、**[すべてのタグ]** を選択すると、ユーザーとグループがインスタンス上のすべてのオブジェクトを編集または使用できるようにもなります。オブジェクトの詳細については、アクセス許可を参照してください。

11. **[保存]** をクリックします。

    確認のメッセージが表示されます。

    Tenable Web App Scanning により変更が保存されます。アクセス許可設定が [**Permissions**] タブに表示されます。

ユーザーまたはグループへのアクセス許可設定の追加

必要なユーザーロール: 管理者

始める前に

- Tenable Web App Scanning アカウントのユーザーまたはグループを作成します。
- アクセス許可設定を作成します。

ユーザーまたはグループにアクセス許可設定を追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. 次のいずれかを行います。

   - ユーザーにアクセス許可設定を追加する場合

     a. **[ユーザー]** タブをクリックします。

     [ユーザー] タブが表示されます。このタブには、Tenable Web App Scanning インスタンスのすべてのユーザーのリストが含まれています。

     b. ユーザーの表で、アクセス許可設定を追加するユーザーをクリックします。

     [ユーザーの編集] ページが表示されます。

     c. 表の上部にある **[アクセス許可]** セクションで、**[アクセス許可の追加]** をクリックします。

     [アクセス許可の追加] ウィンドウが表示されます。

     d. 1つ以上のアクセス許可設定の横にあるチェックボックスを選択します。

e. **[追加]** をクリックします。

アクセス許可設定は、**[ユーザーの編集]** ページの **[アクセス許可]** 表に表示されます。

- ユーザーグループにアクセス許可設定を追加する場合

a. **[グループ]** タブをクリックします。

[グループ] タブが表示されます。このタブには、Tenable Web App Scanning インスタンスのすべてのユーザーグループのリストが含まれています。

b. グループの表で、アクセス許可設定を追加するグループをクリックします。

[ユーザーグループの編集] ページが表示されます。

c. 表の上部にある **[アクセス許可]** セクションで、**[アクセス許可の追加]** をクリックします。

[アクセス許可の追加] ウィンドウが表示されます。

d. 1つ以上のアクセス許可設定の横にあるチェックボックスを選択します。

e. **[追加]** をクリックします。

アクセス許可設定は、**[ユーザーグループの編集]** ページの **[アクセス許可]** 表に表示されます。

5. **[保存]** をクリックします。

Tenable Web App Scanning によって変更が保存され、ユーザーまたはグループにアクセス許可設定が追加されます。

アクセス許可設定の編集

必要なユーザーロール: 管理者

アクセス許可設定を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブには、Tenable Web App Scanning インスタンスのすべてのアクセス許可設定のリストが含まれています。

5. 表で、編集するアクセス許可設定をクリックします。

   [アクセス許可の詳細] ページが表示されます。

6. (オプション) **[アクセス許可名]** ボックスに、アクセス許可設定の新しい名前を入力します。

7. (オプション) ユーザーまたはユーザーグループを追加または削除します。

8. (オプション) アクセス許可を追加または削除します。

   注意: *[編集可]* アクセス許可を *[表示可]* または *[スキャン可]* アクセス許可とともにアクセス許可設定に追加すると、そのアクセス許可設定で選択されたユーザーは、表示およびスキャンできる資産の範囲を変更できます。Tenable は、*[編集可]* アクセス許可に *[閲覧可]* または *[スキャン可]* を組み合わせるのは、管理者ユーザーにのみ行うことを推奨しています。

   注意: **[編集可]** アクセス許可を選択すると、Tenable Web App Scanning によって **[使用可]** アクセス許可が自動的に追加されます。

注意: 別のアクセス許可設定を使用して割り当てられたアクセス許可と重複する特定のオブジェクトのユーザーまたはグループにアクセス許可を割り当てることはできません。たとえば、オブジェクトに*[編集可]*アクセス許可を選択したものの、**[ユーザー]**にリストされているユーザーが既存のアクセス許可設定に基づいてそのオブジェクトを編集することが既にできる場合、Tenable Web App Scanningによってエラーメッセージが生成され、選択を変更して冗長性を削除するまで現在のアクセス許可設定が保存できなくなります。

a. アクセス許可を追加するには、**[アクセス許可]**ドロップダウンボックスで、1つ以上のアクセス許可を選択します。

b. アクセス許可を削除するには、**[アクセス許可]**ドロップダウンボックスで、削除する各アクセス許可の横にある ✕ ボタンをクリックします。

9. (オプション) オブジェクトを追加または削除します。

a. オブジェクトを追加するには、**[オブジェクト]**ドロップダウンボックスからオブジェクトを1つ以上選択します。

b. オブジェクトを削除するには、**[オブジェクト]**ドロップダウンボックスで、削除する各オブジェクトの横にある ✕ ボタンをクリックします。

10. **[保存]**をクリックします。

Tenable Web App Scanningにより変更が保存されます。更新されたアクセス許可設定が[**Permissions**]タブに表示されます。

アクセス許可設定のエクスポート

必要なユーザーロール: 管理者

[アクセス許可] ページでは、1 つ以上のアクセス許可を CSV または JSON 形式でエクスポートできます。

アクセス許可設定をエクスポートする場合

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Web App Scanning インスタンスのすべてのアクセス許可設定が一覧表示されます。

   注意: アクセス許可の表の最初の行には、管理者の読み取り専用エントリが含まれています。このエントリは、管理者がアカウントのすべてのリソースに対するすべてのアクセス許可を持っていることを示すために存在します。詳細は、ロールを参照してください。

5. (オプション) 表データを選別します。詳細は、Tenable Web App Scanning ワークベンチの表 を参照してください。

6. 次のいずれかを行います。

   ### 1 つのアクセス許可設定をエクスポートする場合

   a. アクセス許可設定の表で、エクスポートするアクセス許可設定の行を右クリックします。

      アクションオプションがカーソルの横に表示されます。

      -または-

アクセス許可設定の表の **[アクション]** 列で、エクスポートするアクセス許可設定の行にある ⋮ ボタンをクリックします。

アクションボタンが行に表示されます。

b. **[エクスポート]** をクリックします。

複数のアクセス許可設定をエクスポートする場合

a. アクセス許可設定の表で、エクスポートする各アクセス許可設定のチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで ⋮ **[その他]** をクリックします。

メニューが表示されます。

c. [→ **[エクスポート]** をクリックします。

> **注意:** 個別に選択してエクスポートできるアクセス許可設定は最大 200 個です。200 個以上のアクセス許可設定をエクスポートする場合は、アクセス許可設定の表の上部にあるチェックボックスを選択して、Tenable Web App Scanning インスタンス上のすべてのアクセス許可設定を選択してから、[→ **[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。このプレーンには以下が含まれています。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	アクセス許可設定のリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたアクセス許可設定のリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Web App Scanning では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Web App Scanning がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Web App Scanning がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Web App Scanning によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

ユーザーまたはユーザーグループからアクセス許可設定を削除する

必要なユーザーロール: 管理者

注意: Tenable 提供の **[管理者]** または **[すべてのユーザー]** のユーザーグループからアクセス許可設定を削除することはできません。

ユーザーまたはユーザーグループからアクセス許可設定を削除するには、次の手順に従います。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ユーザーからアクセス許可設定を削除する方法

   - 次のいずれかを行います。

     - **[ユーザー]** タブからアクセス許可設定を削除する場合

       a. **[ユーザー]** タブをクリックします。

       [ユーザー] タブが表示されます。このタブには、Tenable Web App Scanning インスタンスのすべてのユーザーのリストが含まれています。

       b. で、アクセス許可設定を削除するユーザーをクリックします。

       [ユーザーの編集] ページが表示されます。

       c. **[アクセス許可]** 表の **[アクション]** 列で、削除するアクセス許可設定の横にある ⋮ ボタンをクリックします。

       d. **[削除]** 🗑 ボタンをクリックします。

Tenable Web App Scanning によってユーザーのアクセス許可設定が削除されます。

e. (オプション) アクセス許可設定を削除するユーザーごとにこの手順を繰り返します。

- **[アクセス許可]** タブからアクセス許可を削除する場合

a. **[アクセス許可]** タブをクリックします。

[アクセス許可] タブが表示されます。このタブの表には、Tenable Web App Scanning インスタンスのすべてのアクセス許可設定が一覧表示されます。

b. 表で、削除するアクセス許可設定をクリックします。

[アクセス許可の詳細] ページが表示されます。

c. **[ユーザー]** で、アクセス許可設定を削除する各ユーザーの横にある ✕ ボタンをクリックします。

Tenable Vulnerability Management によって、**[ユーザー]** リストからアクセス許可設定が削除されます。

5. ユーザーグループからアクセス許可設定を削除する方法

- 次のいずれかを行います。

- **[グループ]** タブからアクセス許可設定を削除する場合

a. **[グループ]** タブをクリックします。

[グループ] タブが表示されます。このタブには、Tenable Vulnerability Management インスタンスのすべてのユーザーグループのリストが含まれています。

b. ユーザーグループの表で、アクセス許可設定を削除するグループをクリックします。

[ユーザーグループの編集] ページが表示されます。

c. **[アクセス許可]** 表の **[アクション]** 列で、削除するアクセス許可設定の横にある ⋮ ボタンをクリックします。

d. **[削除]** 🗑 ボタンをクリックします。

Tenable Vulnerability Management によってユーザーグループからアクセス許可設定が削除されます。

e. (オプション) アクセス許可設定を削除するユーザーグループごとにこの手順を繰り返します。

- **[アクセス許可]** タブからアクセス許可設定を削除する場合

a. **[アクセス許可]** タブをクリックします。

[アクセス許可] タブが表示されます。このタブの表には、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定が一覧表示されます。

b. 表で、削除するアクセス許可をクリックします。

[アクセス許可の詳細] ページが表示されます。

c. **[グループ]** で、アクセス許可設定を削除する各ユーザーグループの横にある ✕ ボタンをクリックします。

Tenable Vulnerability Management によって、**[グループ]** リストからアクセス許可設定が削除されます。

6. **[保存]** をクリックします。

Tenable Vulnerability Management によって変更が保存され、ユーザーまたはグループからアクセス許可が削除されます。

アクセス許可設定の削除

必要なユーザーロール: 管理者

注意: デフォルトのアクセス許可設定を削除することはできません。

ユーザーまたはユーザーグループからアクセス許可設定を削除するには、次の手順に従います。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Web App Scanning インスタンスのすべてのアクセス許可設定が一覧表示されます。

5. 表の **[アクション]** 列で、削除するアクセス許可設定の横にある ⋮ ボタンをクリックします。

6. **[削除]** 🗑 ボタンをクリックします。

   Tenable Web App Scanning がアクセス許可設定を削除します。

ロール

ロールにより、Tenable Web App Scanning の主要機能の権限を管理し、Tenable Web App Scanning でユーザーがアクセスできる Tenable Web App Scanning リソースを制御できます。

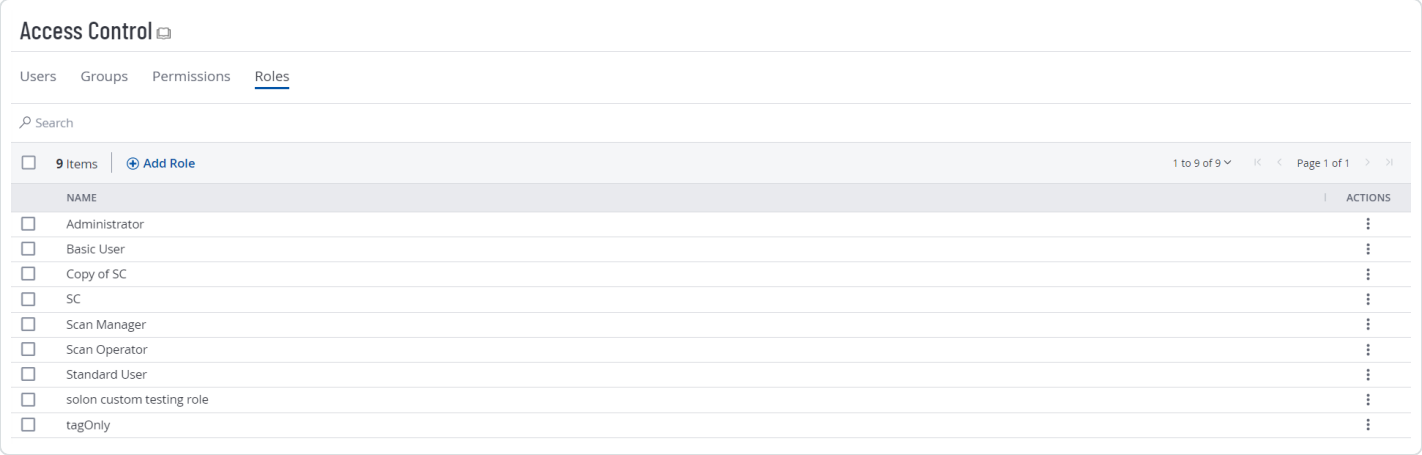
ユーザーを作成するときには、そのユーザーが実行できる操作にだいたい該当するロールを選択する必要があります。

注意: 個別のユーザーまたはグループにアクセス許可を割り当てることにより、特定のリソースへのユーザーアクセスをさらに絞り込むことができます。詳細は、権限を参照してください。

ロールとアクセス許可の違いは何ですか?

- ロール - ロールにより、Tenable Web App Scanning の主要機能の権限を管理し、ユーザーがアクセスできる Tenable Web App Scanning モジュールや機能を制御できます。
- アクセス許可 - アクセス許可により、タグ、資産、その検出結果など、自分のデータへのアクセスを管理できます。

[ロール] ページでは、Tenable 提供のすべてのロールと、Tenable Web App Scanning インスタンスで作成されたカスタムロールを表示できます。



以下のロールのいずれか種類をユーザーに割り当てることができます。

ロールの種類	説明
Tenable 提供のロール	アカウントのライセンスで指定された Tenable Web App Scanning 製品によって断定される、事前定義された一連の権限が含まれています。各ロールには下位ロールの

と権限	権限が含まれ、新しい権限が追加されます。管理者が最も多くの権限を持っています。ただのユーザーには最小限のアクセス許可があります。
カスタムロール	Tenable Web App Scanning インスタンス上のユーザー権限とリソースへのアクセス権を調整できる、権限のカスタムセットが含まれています。

ユーザーロールを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

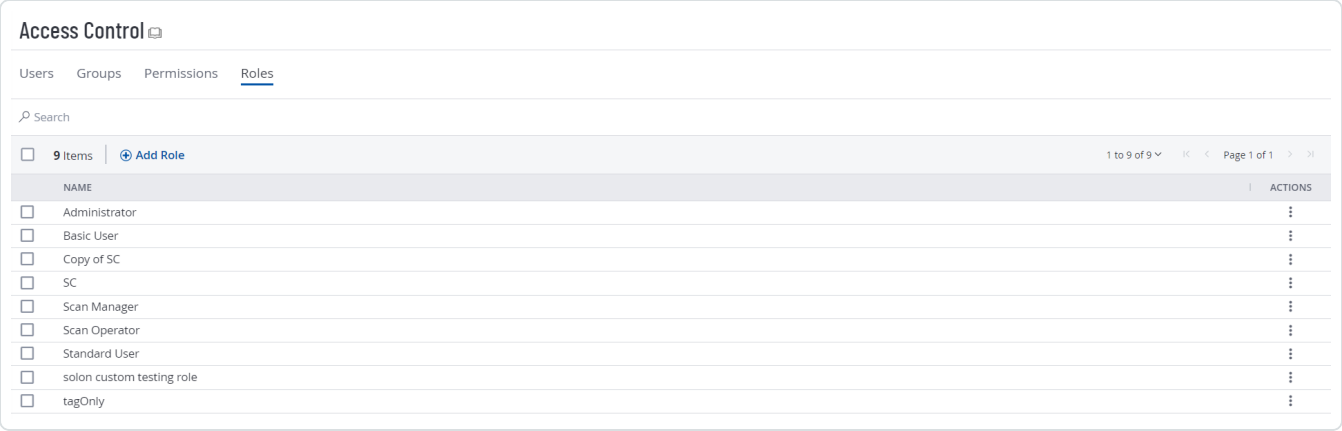
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Web App Scanning インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。



[**Roles**] ページでは、次のアクションを実行できます。

- カスタムロールの作成
- ロールを複製する

- カスタムロールの編集
- ロールのエクスポート
- カスタムロールを削除する

Tenable 提供のロールと権限

以下の表は、Tenable 提供の各ユーザーロールに関連付けられた権限を各製品の機能別にまとめたものです。

注意: 個別のユーザーまたはグループにアクセス許可を割り当てることにより、特定のリソースへのユーザーアクセスをさらに絞り込むことができます。詳細は、権限を参照してください。

領域	Tenable Web App Scanning で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
Activity Logs	表示、エクスポート	-	-	-	-
API キー	表示、修正	表示、修正	表示、修正	表示、修正	表示、修正
アカウント設定	表示、修正	表示、修正	表示、修正	表示、修正	表示、修正
エージェント	表示、削除	表示、削除	-	-	-
エージェントフリーズ期間	表示、作成、修正、削除	表示、作成、修正、削除	-	-	-
エージェントグループ	表示、作成、修正、削除	表示、作成、修正、削除	-	-	-
エージェント設定	表示、修正	表示、修正	-	-	-
資産	表示、修正、エクスポート、削除	表示、修正、エクスポート、削除	表示、修正、エクスポート、削除	表示、修正、エクスポート、削除	表示、エクスポート
コネクタ	表示、作成、修正、	-	-	-	-

領域	Tenable Web App Scanning で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	削除				
ダッシュボード	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除
除外	表示、インポート、エクスポート、削除	表示、インポート、エクスポート、削除	-	-	-
Exports	表示、修正、エクスポート、削除	-	-	-	-
全般設定	表示、修正	-	-	-	-
正常性とステータス	表示	-	-	-	-
認証情報の管理	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除
PCI 管理	表示、インポート、エクスポート、修正、削除	-	-	-	-
変更ルール	表示、作成、修正、削除	-	-	-	-
レポート	表示、実	表示、実	表示、実	表示、実	表示

領域	Tenable Web App Scanning で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	行、作成、修正、削除	行、作成、修正、削除	行、作成、修正、削除	行、作成、修正、削除	
レポート結果	表示、削除	表示、削除	表示、削除	表示、削除	表示
スキャン[1]	表示、インポート、実行、作成、修正、削除	表示、インポート、実行、作成、修正、削除	表示、インポート、実行、作成、修正、削除	表示、インポート、実行、作成[2]、修正、削除	表示[3]、インポート
スキャン結果	表示、エクスポート、削除	表示、エクスポート、削除	表示、エクスポート、削除	表示、エクスポート、削除	表示、エクスポート、削除
センサー	表示、追加、修正、削除	表示、追加、修正、削除	-	-	-
スキャナーグループ	表示、作成、修正、削除	表示、作成、修正、削除	-	-	-
タグ[4]	表示、タグカテゴリの作成、タグ値の	表示、タグ値の作成、削除、割り当	表示、削除、割り当て、割り当て	表示、削除、割り当て、割り当て	表示、割り当て、割り当て解除

[1]ユーザーができることはユーザーロールによって決まりますが、特定のスキャンに対してユーザーが持つアクセス許可はスキャンアクセス許可によって決まります。
[2]ユーザーが共有する既存のユーザー定義ポリシーを使用してスキャンを作成できます。
[3]スキャンの一覧を表示できますが、スキャンの詳細設定は表示できません。
[4]タグの割り当ておよび割り当て解除は、[資産の詳細]ページから実行できます。

領域	Tenable Web App Scanning で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	作成、削除、エクスポート、割り当て、割り当て解除	て、割り当て解除	解除[1]	解除	
ユーザーグループ	表示、作成、修正、削除、エクスポート	-	-	-	-
ユーザー定義のスキャンテンプレート	表示、インポート、エクスポート、修正、削除	表示、インポート、エクスポート、修正、削除	表示、インポート、エクスポート、修正、削除	-	-
ユーザー	表示、作成、修正、削除	-	-	-	-
脆弱性	表示、エクスポート	表示、エクスポート	表示、エクスポート	表示、エクスポート	表示、エクスポート

領域	Tenable Web App Scanning で提供されるロールと権限					
	管理者	スキャンマネージャー	標準	スキャンオペレーター	WAS Reader	基本
ダッシュボード	表示、作成、	表示、作成、修正、	表示、作成、	表示、作成、	表示	表示

[1]標準ユーザーがタグを表示、削除、割り当て、割り当て解除するには、**[使用可]** アクセス許可が必要です。

領域	Tenable Web App Scanning で提供されるロールと権限					
	管理者	スキャンマネージャー	標準	スキャンオペレーター	WAS Reader	基本
	修正、削除	削除	修正、削除	修正、削除		
Tenable 提供スキャンテンプレート	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示	-	-
User-Defined Templates	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	-	-
スキャン (スキャンアクセス許可も必要です)	表示、インポート、作成、修正、実行、削除	表示、インポート、作成、修正、実行、削除	表示、作成、修正、実行、削除	表示、作成[1]、修正、実行、削除、ゴミ箱に移動	表示	表示
認証情報の管理	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除

[1]ユーザーが共有する既存のユーザー定義ポリシーを使用してスキャンを作成できます。

領域	Tenable Web App Scanning で提供されるロールと権限					
	管理者	スキャンマネージャー	標準	スキャンオペレーター	WAS Reader	基本
スキャンアクセス許可	表示、作成、修正、削除[1]	表示、作成、修正、削除[2]	表示、作成、修正、削除[3]	表示、作成、修正、削除[4]	-	-
スキャン結果 (スキャンアクセス許可も必要です)	表示、削除	表示、削除	表示、削除	表示、削除	表示、削除	表示、削除

領域	Lumin Exposure View で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
設定	管理、読み取り	読み取り	読み取り	読み取り	読み取り
アクセスできる資産タイプ	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、

[1]管理者は、アカウントの任意のユーザーが所有するスキャンのアクセス許可を作成、変更、削除することができます。
[2]スキャンマネージャーユーザーは、自分が所有するスキャンのアクセス許可のみを作成、変更、削除することができます。
[3]Standard ユーザーは、自分が所有するスキャンのアクセス許可のみを作成、変更、削除することができます。
[4]Scan Operator ユーザーは、自分が所有するスキャンのアクセス許可のみを作成、変更、削除することができます。

領域	Lumin Exposure View で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	ウェブアプリケーション、ID	ウェブアプリケーション、ID	ウェブアプリケーション、ID	ウェブアプリケーション、ID	ウェブアプリケーション、ID
エクスポート	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理
エクスポージャーカード	作成、共有、読み取り	作成、共有、読み取り	作成、共有、読み取り	共有、読み取り	読み取り

領域	Asset Inventory で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
アクセスできる資産タイプ	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID
エクスポート	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理
タグ	作成、編集	作成、編集	-	-	-

領域	Attack Path Analysis で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
エクスポート	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理

領域	Attack Path Analysis で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
検出結果	管理、読み取り	管理、読み取り	読み取り	読み取り	読み取り
クエリ	検索、保存	検索、保存	検索、保存	検索	検索

領域	Tenable Attack Surface Management で提供されるロールと権限		
	ビジネス管理者	アクティブユーザー	閲覧専用ユーザー
インベントリ	管理、追加、修正、削除	追加、修正、放置	閲覧
提案	管理、追加、修正、削除	管理、追加、修正、削除	閲覧
サブスクリプション	管理、追加、修正、削除	管理、追加、修正、削除	閲覧
レポート	管理、追加、修正、削除	管理、追加、修正、削除	閲覧
テキストレコード	管理、修正、削除	管理、修正、削除	閲覧
ユーザーアカウント	管理、修正、削除	-	-
ビジネス	管理、修正	-	-

注意: デフォルトでは、Tenable One 内で作成された Tenable Attack Surface Management ユーザーには**アクティブユーザー**の役割が付与されます。

領域	Tenable Container Security で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
ダッシュ	表示	表示	表示	表示	表示

ボード					
データ使用量	表示[1]	表示	表示	表示	表示
イメージ	表示、Tenable Vulnerability Management にプッシュ、削除[2]	表示、Tenable Vulnerability Management にプッシュ、削除	表示、Tenable Vulnerability Management にプッシュ、削除	表示、Tenable Vulnerability Management にプッシュ、削除	-
イメージリポジトリ	表示、検索、削除	表示、検索、削除	表示、検索、削除	表示、検索、削除	表示、検索
コンテナ	表示	表示	表示	表示	表示
ポリシー	作成、表示、編集、アクセス許可の設定、削除	作成、表示、編集、アクセス許可の設定、削除	表示	表示	表示
コネクタ	作成、設定、表示、削除	-	-	-	-
CS スキャナー	ダウンロード、表示、設定、実行	ダウンロード、表示、設定、実行	ダウンロード、表示、設定、実行	ダウンロード、表示、設定、実行	ダウンロード
スキャン結果	表示、検索	表示、検索	表示、検索	表示、検索	表示、検索

[1]管理者ロールを持つユーザーは、その他のロールでは表示できないライセンス情報を表示できます。
[2]管理者ロールを持つユーザー以外のユーザーは、自分がインポートしたイメージのみを削除できます。管理者ユーザーは、アカウント上のすべてのユーザーのイメージを削除できます。

カスタムロール

Tenable Web App Scanning インスタンスでユーザーのカスタムロールを作成して、自社のニーズに固有の権限をそれらのユーザーに付与できます。

カスタムロールを作成する場合は、以下の権限の一部またはすべてを追加できます。カスタムロールを編集して権限を削除することもできます。ロールに追加またはロールから削除できる権限は、各権限が適用される Tenable Web App Scanning の領域によって異なります。

> **注意:** アカウント上のリソースへのユーザーのアクセスは、ユーザーのロールに関係なく、ユーザーのアクセス許可によって制限される場合があります。

- **作成** - ユーザーはエクスポージャーカードまたはタグを作成できます。この権限は、それぞれ Lumin Exposure View および Asset Inventory に固有のものです。
- **管理** - 権限が適用される領域でユーザーが作成、変更、削除を行えるようにします。

  > **注意:** **管理**権限をカスタムロールに追加すると、Tenable Web App Scanning は自動的に**読み取り**権限も追加します。最初に**管理**権限を無効にしない限り、**読み取り**権限は無効にできません。

- **すべて管理** - ユーザーは、他のユーザーが作成したエクスポートを含め、エクスポートを表示、変更、削除できます。
- **自分のもののみ管理** - ユーザーは、自分が作成したエクスポートのみを表示、変更、削除できます。
- **共有** - ユーザーは、他のユーザーまたはグループとオブジェクトを共有できます。

  > **注意**: カスタムロールで **[読み取り]** アクセス許可も有効になっていない場合、そのカスタムロールは、オブジェクトの共有相手となる他のユーザーのリストにアクセスできません。

- **読み取り** - ユーザーは、権限が適用される領域のアイテムを閲覧できます。
- **使用** - ユーザーは、Tenable Web App Scanning スキャンの作成中に Tenable 提供のスキャンテンプレートを使用できます。
- **PCI の提出** - ユーザーは、PCI 検証のためにスキャンを送信できるようになります。詳細については、*Tenable PCI ASV ユーザーガイド*を参照してください。
- **検索** - ユーザーは、権限が適用される範囲でクエリを検索できます。この権限は、Attack Path Analysis に固有です。

- **保存** - ユーザーは、権限が適用されるクエリを保存できます。この権限は、Attack Path Analysis に固有です。
- **クラウドリソース** - ユーザーは、**クラウドリソース**データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。
- **コンピューティングリソース** - ユーザーは、**コンピューティングリソース**データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。
- **ID** - ユーザーは、**ID** データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。
- **ウェブアプリケーション** - ユーザーは、**ウェブアプリケーション**データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。

次の表に、Tenable Web App Scanning の各セクションでカスタムロールに使用できる権限オプションを示します。

注意: カスタムロールを作成するときは、**[一般設定]**、**[ライセンス]**、および **[マイアカウント]** セクションの**読み取り**権限を含める必要があります。これらのセクションの**読み取り**権限を含めないと、ロールに割り当てられたユーザーは Tenable Web App Scanning にログインできません。

セクション	権限オプション
Asset Inventory	
アクセスできる資産タイプ	**クラウドリソース、コンピューティングリソース、ID、ウェブアプリケーション**
インベントリ	**読み取り**
エクスポート	**自分のもののみ管理**
タグ	**作成、編集**
Attack Path Analysis	
エクスポート	**自分のもののみ管理**
検出結果	**読み取り、管理**
クエリ	**保存、検索**

Lumin Exposure View	
アクセスできる資産タイプ	**クラウドリソース、コンピューティングリソース、ID、ウェブアプリケーション**
エクスポート	**自分のもののみ管理**
エクスポージャーカード	**読み取り、作成、共有**
設定	**読み取り、管理**
プラットフォーム設定	
資産	**読み取り**
検出結果	**読み取り**
マイアカウント	**読み取り、管理**
アクセス制御	**読み取り、管理** **注意:** アクセス制御 で**管理**権限を追加すると、そのカスタムロールを持つユーザーはだれでも、管理者ユーザーを作成し、そのユーザーとしてログインし、そのユーザー自身のインスタンスを含め、Tenable Vulnerability Management インスタンスの任意のユーザーの権限やアクセス許可を変更することができます。アクセス制御 設定を管理できるユーザーアカウントを作成する場合、Tenable はそのユーザーに管理者ロールを割り当てることを推奨します。詳細は、Tenable 提供のロールと権限を参照してください。
Activity Log	**読み取り**
全般設定	**読み取り、管理**
ライセンス情報	**読み取り**
ワークスペース	
資産	**読み取り**
検出結果	**読み取り**
Vulnerability Management	

Dashboard	**管理、共有** **注意:** Dashboards セクションのカスタムロール権限には、ダッシュボードをエクスポートする機能が含まれていません。ユーザーがダッシュボードをエクスポートできるようにするには、Tenable が提供するロールをユーザーに割り当てます。 **注意:**すべてのユーザーは、自分に割り当てられた権限に関係なく、自分が作成したダッシュボード、または他のユーザーが共有してくれたダッシュボードを表示できます。
エクスポート	**すべて管理、自身を管理**
変更/許容ルール	**読み取り、管理**
スキャン	
Nessus/Nessus Agent スキャン	**読み取り、管理、PCI の提出**
スキャンの除外	**読み取り、管理**
Tenable 提供のスキャンテンプレート	**使用**
ユーザー定義スキャンテンプレート	**読み取り、管理**
管理された認証情報	**読み取り、管理**
ターゲットグループ	**読み取り、管理**

カスタムロールの作成

必要なユーザーロール: 管理者

注意: Tenable アプリケーションは現在、カスタムロールによるスキャンとセンサーの管理をサポートしていません。

カスタムロールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

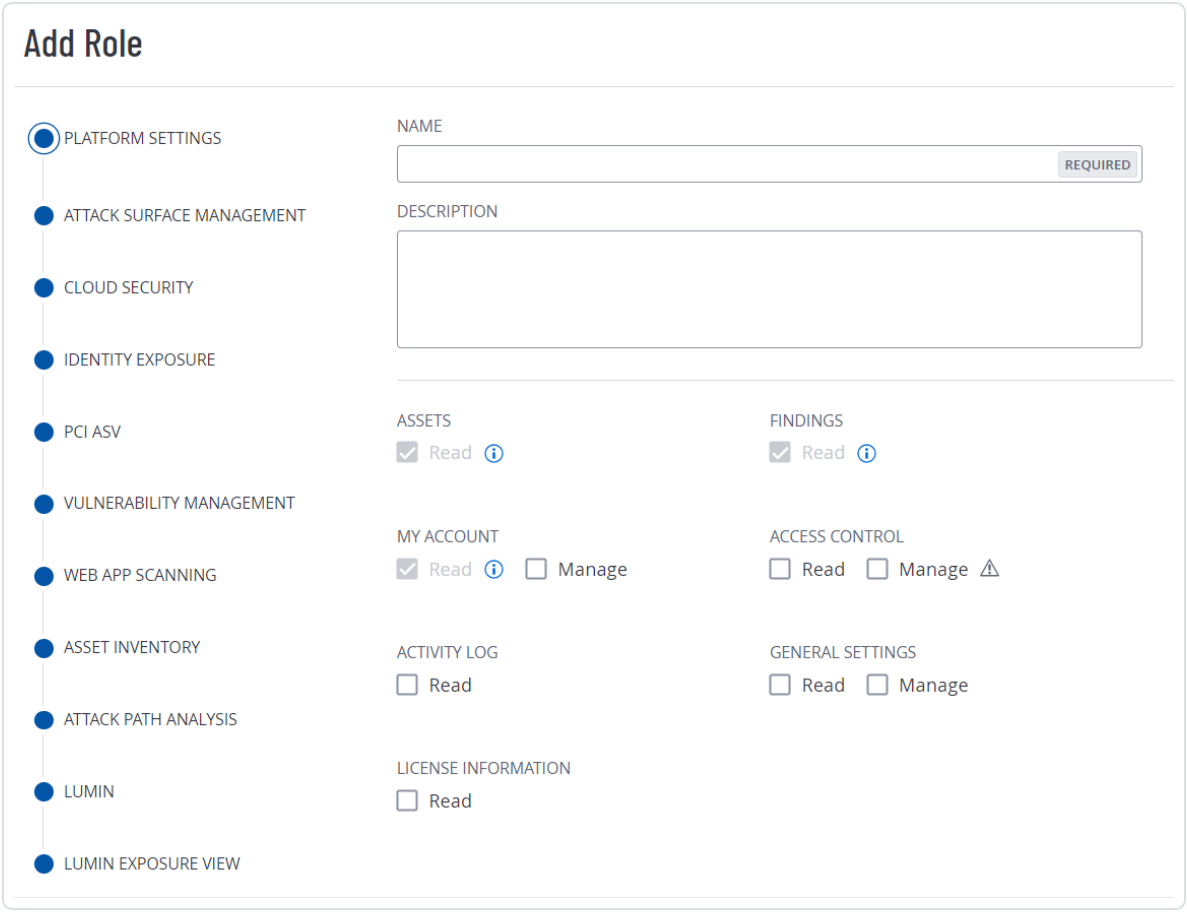
   [ロール] ページが表示されます。このページの表に、Tenable Web App Scanning インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. 次のいずれかを行います。

   - 既存のロールを複製して変更します。
   - 新しいロールを追加する

     a. 表の上部にある **[ロールの追加]** をクリックします。

        [ロールの追加] ページが表示されます。



b. **[名前]**ボックスにカスタムロールの名前を入力します。

c. (オプション)**[説明]**ボックスに、カスタムロールの説明を入力します。

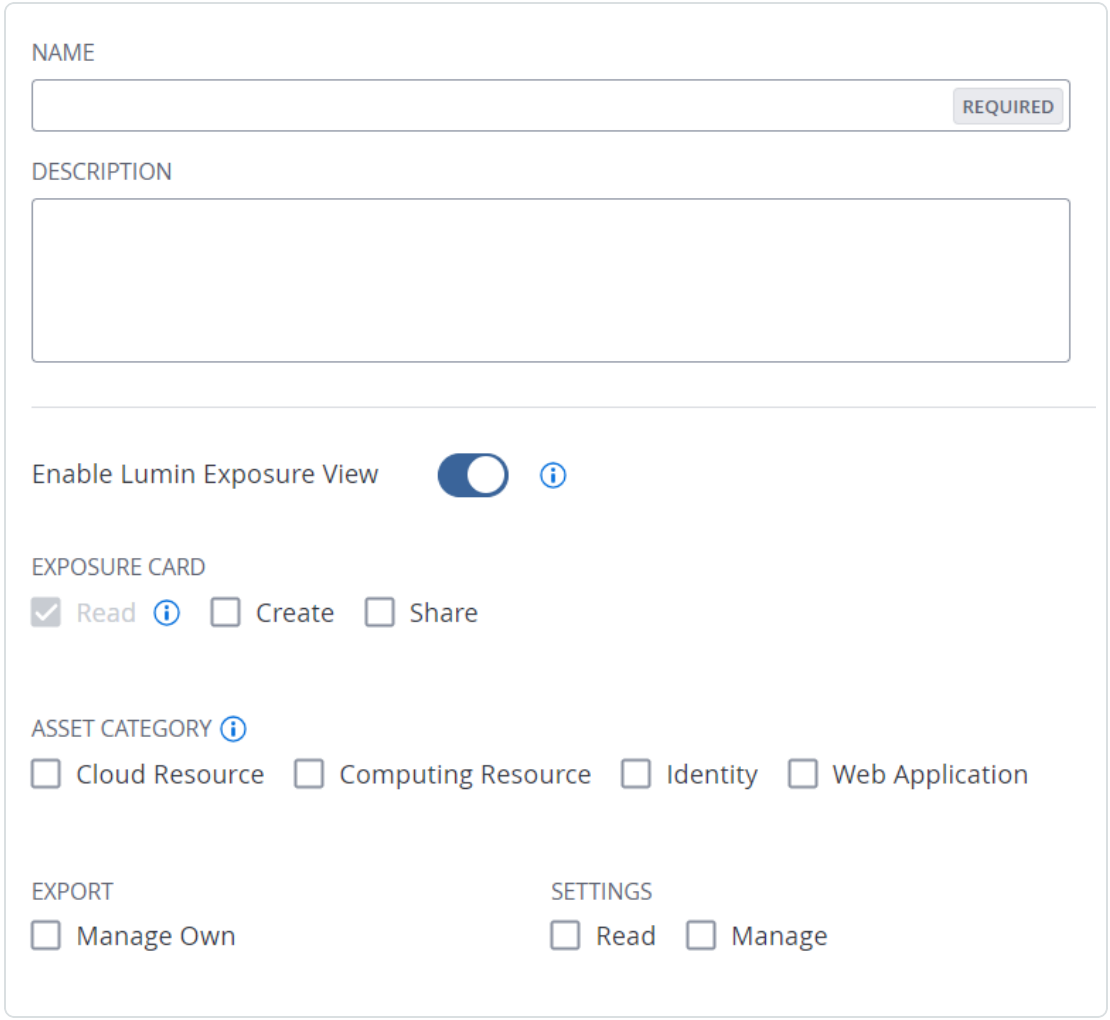
d. カスタムロールがアクセスできるアプリケーションを決定します。

   i. 左側のパネルで、[アプリケーション名]をクリックします。

      [有効化]トグルが表示されます。

   ii. **[有効化]**トグルをクリックして、作成しているカスタムロールについて、このアプリケーションへのアクセスを有効または無効にします。

      一部のアプリケーションでは、アプリケーションに関連付けられた権限が表示されます。



iii. カスタムロールに追加する各権限のチェックボックスを選択します。

e. **[保存]**をクリックします。

Tenable Web App Scanning によってロールが保存され、ロールの表に追加されます。

ロールを複製する

必要なユーザーロール: 管理者

カスタムロールを作成するには、既存のカスタムロールを複製し、必要に応じて新しいロールの設定を変更します。

注意: Tenable 提供のロールは複製できません。

複製を使用してカスタムロールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Web App Scanning インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. ロールの表で、複製するロールの横にあるチェックボックスを選択します。

   表の上部にアクションバーが表示されます。

6. アクションバーで ⋮ **[その他]** をクリックします。

   メニューが表示されます。

7. **[複製]** をクリックします。

   ロールのコピーが表に表示され、「[ロール名] のコピー」がプレフィックスとして付きます。

8. 複製されたロールをクリックします。

[ロールの詳細] ページが表示されます。複製するロールの名前、説明、および選択した権限は、元のロールからコピーされます。

9. 次の設定から1つ以上を更新します。

    - 名前 - **[名前]** ボックスにロールの新しい名前を入力します。
    - 説明 - **[説明]** ボックスに、ロールの説明を入力します。
    - Privileges - Tenable Web App Scanning の各領域で、ロールに追加またはロールから削除する各権限の横にあるチェックボックスを選択または選択解除します。

10. **[保存]** をクリックします。

    Tenable Web App Scanning によって変更が複製ロールに保存されます。

カスタムロールの編集

必要なユーザーロール: 管理者

注意: Tenable アプリケーションは現在、カスタムロールによるスキャンとセンサーの管理をサポートしていません。

カスタムロールを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Web App Scanning インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. ロールの表で、編集するロールをクリックします。

   [ロールの詳細] ページが表示されます。

6. 次の設定から 1 つ以上を更新します。

   - 名前 - **[名前]** ボックスにロールの新しい名前を入力します。
   - 説明 - **[説明]** ボックスに、ロールの説明を入力します。
   - Privileges - Tenable Web App Scanning の各領域で、ロールに追加またはロールから削除する各権限の横にあるチェックボックスを選択または選択解除します。

7. **[保存]** をクリックします。

   Tenable Web App Scanning により変更が保存されます。

カスタムロールを削除する

必要なユーザーロール: 管理者

注意: 削除できるのはカスタムロールのみです。Tenable 提供のロールと権限は削除できません。

カスタムロールを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Web App Scanning インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. 表の **[アクション]** 列で、削除するロールの横にある ⋮ ボタンをクリックします。

6. **[削除]** 🗑 ボタンをクリックします。

   Tenable Web App Scanning によってロールが削除され、ロールの表からそのロールが削除されます。

ロールのエクスポート

必要なユーザーロール: 管理者

[ロール] ページでは、1 つ以上のユーザーグループを CSV または JSON 形式でエクスポートできます。

ユーザーロールをエクスポートする場合

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表には、Tenable Web App Scanning インスタンス上のすべての Tenable 提供ロールとカスタムロールが一覧表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Web App Scanning ワークベンチの表 を参照してください。

6. 次のいずれかを行います。

1 つのロールをエクスポートする場合

a. ロールの表で、エクスポートするロールの行を右クリックします。

   アクションオプションがカーソルの横に表示されます。

   -または-

   ロールの表の **[アクション]** 列で、エクスポートするロールの行にある ⋮ ボタンをクリックします。

   アクションボタンが行に表示されます。

b. **[エクスポート]** をクリックします。

複数のロールをエクスポートする場合

a. ロールの表で、エクスポートする各ロールのチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで、[→ **[エクスポート]** をクリックします。

> **注意:** 個別に選択してエクスポートできるロールは最大 200 個です。200 個以上のロールをエクスポートする場合は、ロールの表の上部にあるチェックボックスを選択して、Tenable Web App Scanning インスタンス上のすべてのロールを選択してから、[→**[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	ロールのリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたロールのリストを含む JSON ファイル

	空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Web App Scanning では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

    - **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      注意: Tenable Web App Scanning がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Web App Scanning がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Web App Scanning によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

アクセスグループ

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

注意: スキャン結果の表示、および特定のターゲットのスキャンを制御していたシステムターゲットグループのアクセス許可は、アクセスグループに移行しました。詳細は、スキャンのアクセス許可の移行 を参照してください。

アクセスグループを使用することで、次を実行できる組織のユーザーまたはグループを制御できます。

- 特定の資産および関連する脆弱性を、集約されたスキャン結果のビュー(新しいインターフェースのダッシュボード、および従来のインターフェースのワークベンチ)で表示する。
- 特定のターゲットに対してスキャンを実行し、ターゲットの個別のスキャン結果を表示する。

アクセスグループに含まれる資産またはターゲットは、設定したルールにより規定されます。アクセスグループのルールでは、資産またはターゲットをグループに関連付けるために Tenable Vulnerability Management が使用する、固有の属性を指定します。(たとえば、AWS Account ID、FQDN、IP アドレスなど)アクセスグループでユーザーまたはユーザーグループにアクセス許可を割り当てることで、そのアクセスグループに関連付けられた資産またはターゲットに対する、表示またはスキャンのアクセス許可をユーザーグループに属するユーザーに付与できます。

注意: アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのにある程度の時間を要する場合があります。

[アクセスグループ] ページにあるアクセスグループの表の **[ステータス]** 列で、この割り当てプロセスのステータスを確認できます。

アクセスグループを表示、作成、編集できるのは管理者のみです。他のロールを割り当てられているユーザーは、自分が所属するアクセスグループおよびそれに関連するルールを表示できますが、アクセスグループのその他のユーザーを表示することはできません。

注意: **アクセスグループ**タイルは、1 つ以上のアクセスグループが割り当てられている場合や、自分が管理者であり、Tenable Vulnerability Management のユーザーがアクセスグループに割り当てられている場合にのみ表示されます。すべてのアクセスグループを権限設定に変換すると、**アクセスグループ**タイルはアカウントに表示されなくなります。

デフォルトでは、すべてのユーザーがTenable Vulnerability Managementインスタンスのすべての資産に**アクセスできない**ようになっています。したがって、資産にアクセス権を割り当てる場合は、アクセスグループを作成し、そのグループのユーザー権限を設定する必要があります。

> **注意:** Tenable Vulnerability Management はアクセスグループの範囲にかかわらず、動的タグをあらゆる資産に適用します。結果として、自分が作成したタグが、自分の所属するアクセスグループ外にある資産に適用される場合があります。

企業当たり5,000個までアクセスグループが作成できます。

アクセス許可設定への移行

必要なユーザーロール: 管理者

Tenable は、すべてのアクセスグループを、アクセス許可設定に変換しています。この変換の実行中に、既存のアクセスグループが変更中であることに気づく場合があります。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

Tenable Vulnerability Management は、ユーザーとグループの管理を統合して**アクセス制御**ページに移動し、アクセス管理をより直感的で効率的なものにしました。

その一環として、Tenable Vulnerability Management はアクセスグループを権限に置き換えます。この機能により、アクセス許可設定を作成できます。これらのアクセス許可設定では、タグを使用して、Tenable Vulnerability Management インスタンス上のどのユーザーとグループが、組織のリソースを使用して特定のタスクを実行できるかを決定します。

以前は、アクセスグループを作成して、インスタンス上のユーザーのアクセス設定をカスタマイズする必要がありました。アクセス許可設定を作成すると、ユーザーとグループを管理する **[アクセス制御]** ページで、ユーザーとグループのアクセス設定を表示して管理できます。

Tenable Vulnerability Management では、既存のすべてのアクセスグループがアクセス許可設定に変換され次第、アクセスグループを廃止する予定です。Tenable Vulnerability Management では、アクセス許可設定を使用して、リソースへのユーザーアクセスを管理することを推奨しています。

新しい設定方法について

Tenable Vulnerability Management はアクセスグループデータをアクセス許可設定に変換しますが、それに伴って以下の変更が生じていますのでご注意ください。

- Tenable Vulnerability Management は、複数のアクセスグループタイプがあるアクセスグループを分割して、タイプ別のグループとして再編成します。アクセスグループタイプの詳細については、アクセスグループの種類を参照してください。
- Tenable Vulnerability Management は、すべての **[ターゲットのスキャン]** タイプのアクセスグループを、**[資産の管理]** タイプのアクセスグループに変換します。

- Tenable Vulnerability Management は、タグルールのフィルターと演算子に一致するようにアクセスグループルールフィルターをアップデートします。
- タグではなくルールに基づく、お使いのインスタンス上のアクセスグループについては、Tenable Vulnerability Management は、アクセスグループルールに基づいてタグを作成し、新しいタグを参照するように各グループをアップデートしています。タグルールの詳細については、タグルールを参照してください。
- インストール環境のアクセスグループごとに、Tenable Vulnerability Management は、そのアクセスグループで定義されたルールとユーザーアクセス許可に基づいてアクセス許可設定を作成しています。

同等タスク

次の表に、**[アクセスグループ]** ページで実行可能な一般的なタスクと、**[アクセス許可]** ページ上の同等のタスクを示します。

アクセスグループ	アクセス許可
アクセスグループを作成する	アクセス許可設定の作成および追加
割り当てられたアクセスグループを表示する	アカウントの詳細の表示
アクセスグループを編集する	アクセス許可設定の編集
アクセスグループのユーザーのアクセス許可を設定する	• ユーザーまたはグループへのアクセス許可設定の追加 • ユーザーまたはユーザーグループからアクセス許可設定を削除する
アクセスグループを削除する	アクセス許可設定の削除

アクセスグループをアクセス許可設定に変換する

必要なユーザーロール: 管理者

Tenable は、すべてのアクセスグループを、アクセス許可設定に変換しています。この変換の実行中に、既存のアクセスグループが変更中であることに気づく場合があります。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

[アクセスグループ] ページで、既存のアクセスグループをアクセス許可設定に変換できます。

注意: アクセスグループをアクセス許可設定に変換した場合、変換したアクセス許可設定をアクセスグループに戻すことはできません。

注意: **アクセスグループ**タイルは、1 つ以上のアクセスグループが割り当てられている場合や、自分が管理者であり、Tenable Vulnerability Management のユーザーがアクセスグループに割り当てられている場合にのみ表示されます。すべてのアクセスグループをアクセス許可設定に変換すると、**アクセスグループ**タイルはアカウントに表示されなくなります。

アクセスグループをアクセス許可設定に変換する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルタブをクリックします。

   [アクセスグループ] ページタブが表示されます。このページタブには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. アクセスグループの表で、変換するアクセスグループのチェックボックスを選択します。

   表の上部にアクションバーが表示されます。

5. **[権限へ移行]** をクリックします。

   確認のメッセージが表示されます。

6. 確認ウィンドウで、[→ **[権限へ移行]** をクリックします。

   Tenable Vulnerability Management は、アクセスグループのアクセス許可設定への変換を開始します。

   Tenable Vulnerability Management は、アクセスグループの **[ステータス]** 列を更新して、現在の移行ステータスを表示します。

アクセスグループの種類

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

次の種類のアクセスグループを作成できます。スキャンするターゲットの識別子に基づいて、アクセスグループの種類を選択してください。

タイプ	説明
資産の管理	ユーザーは、以前のスキャン時に作成された資産レコードを表示して、それらの資産に関連するターゲットをスキャンできます。 表示またはスキャンしたいターゲットを過去にスキャンしたことがあり、資産の属性 (たとえばオペレーティングシステムや AWS Account ID など) に基づいたタグによってターゲットを最もよく識別できる場合に、この種類のアクセスグループを使用します。
ターゲットのスキャン	ユーザーは、このアクセスグループに関連付けられたターゲットをスキャンし、そのスキャン結果を表示できます。 表示またはスキャンしたいターゲットを過去にスキャンしたことがなく、特定の資産識別子 (特に FQDN、IPv4 アドレス、または IPv6 アドレス) を使用することでのみターゲットの識別が可能な場合に、この種類のアクセスグループを使用します。

注意: アクセスグループの種類名は、指定されたターゲットに対してユーザーが取ることのできる、各グループが管理するアクションの制限を示すものではありません。**[資産の管理]** と **[ターゲットのスキャン]** グループの両方で、指定されたターゲットの分析結果をダッシュボードに表示するため、または指定されたターゲットをスキャンするため、あるいはその両方を行うためのアクセス許可をユーザーに付与することができます。ユーザーのアクセス許可についての詳細は、アクセスグループのユーザーのアクセス許可を設定するを参照してください。ユーザーのアクセス許可についての詳細は、ユーザーグループを編集するを参照してください。

ヒント: ユーザーに両タイプのスキャンターゲットのスキャンを許可するには、そのユーザーを両方のアクセスグループタイプに追加します。

[すべての資産]グループのユーザーを制限する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行を参照してください。

必要なユーザーロール: 管理者

[すべての資産]グループは、システムによって生成されるデフォルトのアクセスグループで、すべての資産が属します。

デフォルトでは、次の条件が真となります。

- **[すべての資産]**グループには、企業内のすべてのユーザーを含む**[すべてのユーザー]**ユーザーグループが割り当てられます。
- **[すべてのユーザー]**グループのアクセス許可として、**[閲覧可]**および**[スキャン可]**が設定されます。

すべてのユーザーがすべての資産をスキャンしたり、個別および集約された結果を表示したりできないようにしたい場合は、**[すべてのユーザー]**グループのアクセス許可を**[アクセスなし]**にする必要があります。その後で特定のユーザーまたはユーザーグループを任意で追加して、すべての資産へのアクセス権を個別に付与することができます。

注意: アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのにある程度の時間を要する場合があります。

[アクセスグループ]ページにあるアクセスグループの表の**[ステータス]**列で、この割り当てプロセスのステータスを確認できます。

[すべての資産]グループのユーザーのアクセス許可を制限する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで**[設定]**をクリックします。

   [設定]ページが表示されます。

3. **[アクセスグループ]** タイルタブをクリックします。

   [アクセスグループ] ページタブが表示されます。このページタブには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. アクセスグループの表で、**[すべての資産]** グループをクリックします。

   [すべての資産アクセスグループを編集] ページが表示されます。

5. **[ユーザーとグループ]** セクションで、**[すべてのユーザー]** グループが表示されている箇所を見つけます。

6. **[すべてのユーザー]** グループの表示から、**[編集可]** と **[スキャン可]** の両方のラベルを削除します。

   a. ラベルにカーソルを合わせます。

      ラベル上に ✕ ボタンが表示されます。

   b. ✕ ボタンをクリックします。

      Tenable Vulnerability Management によりラベルが削除されます。

   注意：[すべてのユーザー] ユーザーグループを設定する際、Tenable では以下に留意するよう推奨しています。

   - **[すべての資産]** のアクセス許可を **[閲覧可]** のままにした場合、すべてのユーザーが企業のすべての資産またはターゲットに対するスキャン結果を表示できます。
   - **[すべての資産]** のアクセス許可を **[スキャン可]** に設定した場合、すべてのユーザーが企業のすべての資産またはターゲットをスキャンし、関連するスキャン結果を表示することができます。

7. (オプション) **[すべての資産]** グループに追加するユーザーまたはグループのそれぞれに対して、ユーザーアクセス許可を設定します。

8. **[保存]** をクリックします。

   [アクセスグループ] ページが表示されます。**[すべての資産]** グループへのアクセスは、追加したユーザーまたはグループに制限されます。

   [ユーザーグループ] タブが表示されます。企業の資産にはどのユーザーもアクセスできません。

9. (オプション) **[すべての資産]** グループにアクセスできるようにするユーザーグループで、**[すべての資産]** アクセスグループに対するアクセス許可を設定します。

アクセスグループを作成する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

AWS アカウント ID、FQDN、IP アドレス、およびその他の固有の属性を使用し、ルールに基づいてグループ資産へのアクセスグループを作成できます。その後ユーザーまたはユーザーグループにアクセス許可を割り当て、そのアクセスグループで資産を表示またはスキャンすることができます。

アクセスグループを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセスグループ]** タイルタブをクリックします。

   [アクセスグループ] ページタブが表示されます。このページタブには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

5. ページの右上にある ⊕ **[アクセスグループの作成]** ボタンをクリックします。

   [アクセスグループの作成] ページが表示されます。

6. **[一般]** セクションの **[名前]** ボックスで、アクセスグループの名前を入力します。

   注意: 名前は企業内で一意である必要があります。

7. **[種類]** セクションで、スキャンするターゲットの種類に基づいて、適切なアクセスグループの種類を選択します。

   ある種類のアクセスグループを作成した後で、設定の最中にその種類を変更すると、Tenable Vulnerability Management は操作の確認を促すメッセージを表示します。確認すると、Tenable Vulnerability Management はそれまでに追加されたルールのフィルター基準を消去します。

8. **[ルール]** セクションで、アクセスグループにルールを追加します。

   アクセスグループのルールでは、資産またはターゲットをアクセスグループに含めるかどうかを判断する際に Tenable Vulnerability Management が評価する条件を規定します。

   > **注意:** 1 つのアクセスグループにつき最大 1,000 個のルールを追加できます。

   a. **[カテゴリ]** ドロップダウンボックスで、資産またはターゲットを絞り込むために属性を選択します。

   b. **[演算子]** ドロップダウンボックスで、演算子を選択します。

      たとえば次の演算子があります。

      • **is equal to**: Tenable Vulnerability Management は、指定された語句との完全一致に基づいてルールを資産またはターゲットと照合します。

      > **注意:** Tenable Vulnerability Management では、1 つの IPv4 アドレスを指定するルールに対してはこの演算子を「等しい」と解釈しますが、IPv4 範囲または CIDR 範囲を指定するルールに対しては演算子を「含む」と解釈します。

      • **contains**: Tenable Vulnerability Management は、指定された語句との部分一致に基づいてルールを資産またはターゲットと照合します。

      • **starts with**: Tenable Vulnerability Management は、ルールを指定された語句で始まる資産またはターゲットと照合します。

      • **ends with**: Tenable Vulnerability Management は、ルールを指定された語句で終了する資産またはターゲットと照合します。

   c. テキストボックスで、選択したカテゴリに有効な値を入力します。

ヒント: 複数の値をコンマで区切って入力できます。**IPV4 アドレス**の場合は、CIDR 表記 (例: 192.168.0.0/24)、範囲 (例: 192.168.0.1-192.168.0.255)、**コンマ区切りリスト** (例: 192.168.0.0, 192.168.0.1) を使用できます。

d. (オプション) 別のルールを追加するには、⊕ **[追加]** ボタンをクリックします。

注意: アクセスグループに複数のルールを設定した場合、アクセスグループにはいずれかのルールに適合する資産またはターゲットが含まれます。たとえば、**[ネットワーク名]** 属性に適合するルールと、**[IPv4 アドレス]** に適合するルールの 2 つを設定した場合、アクセスグループには指定されたネットワーク内のすべての資産に加えて、指定されたネットワークに属するかどうかに関わらず、指定された IPv4 アドレスを持つすべての資産が含まれます。

9. **[基準]** セクションで、Tenable Vulnerability Management で資産またはターゲットのアクセスグループとの照合に使用する基準を指定します。

オプション	アクション
タグ	(資産の管理グループのみ) アクセスグループのタグ基準を指定する方法 a. **[タグ]** オプションをクリックします。 **[検索]** ボックスが表示されます。 b. **[検索]** ボックスで、任意の場所をクリックします。 所属企業のタグのリストが表示されます。 c. タグをクリックします。 Tenable Vulnerability Management によってタグを表すラベルが **[検索]** ボックスに追加されます。 d. 次のいずれかを実行します。 • 別のタグを追加するには、これらの手順を繰り返します。 • タグを削除するには、ボックス内のタグにカーソルを合わせ、ラベルの横にある ✕ ボタンをクリックします。 **注意:** タグのみを基準として、資産をアクセスグループに一致させる場合は、このオプ

	ションを使用します。タグと追加の資産属性で資産を一致させるには、**[ルール]** オプションを使用してから、他のルールに加えて 1 つ以上のタグをルールとして指定します。
ルール	アクセスグループのルールでは、資産またはターゲットをアクセスグループに含めるかどうかを判断する際に Tenable Vulnerability Management が評価する条件を規定します。 **注意:** 1 つのアクセスグループにつき最大 1,000 個のルールを追加できます。 アクセスグループのルール基準を指定する方法 a. **[ルール]** オプションをクリックします。 b. **[カテゴリ]** ドロップダウンボックスで、資産またはターゲットを絞り込むために属性を選択します。 **注意:** 既存のタグに基づいてルールを作成できます。詳細は、タグを参照してください。 c. **[演算子]** ドロップダウンボックスで、演算子を選択します。 たとえば次の演算子があります。 • **is equal to**: Tenable Vulnerability Management は、指定された語句との完全一致に基づいてルールを資産またはターゲットと照合します。 **注意:** Tenable Vulnerability Management では、1 つの IPv4 アドレスを指定するルールに対してはこの演算子を「等しい」と解釈しますが、IPv4 範囲または CIDR 範囲を指定するルールに対しては演算子を「含む」と解釈します。 • **contains**: Tenable Vulnerability Management は、指定された語句との部分一致に基づいてルールを資産またはターゲットと照合します。 • **starts with**: Tenable Vulnerability Management は、ルールを指定された語句で始まる資産またはターゲットと照合します。 • **ends with**: Tenable Vulnerability Management は、ルールを指定された語句で終了する資産またはターゲットと照合します。

d. テキストボックスで、選択したカテゴリに有効な値を入力します。

ヒント: 複数の値をコンマで区切って入力できます。**IPV4 アドレス**の場合は、CIDR 表記 (例: 192.168.0.0/24)、範囲 (例: 192.168.0.1-192.168.0.255)、コンマ区切りリスト (例: 192.168.0.0, 192.168.0.1) を使用できます。

e. (オプション) 別のルールを追加するには、**[追加]** ボタンをクリックします。

注意: アクセスグループに複数のルールを設定した場合、アクセスグループには*いずれか*のルールに適合する資産またはターゲットが含まれます。たとえば、**[ネットワーク名]** 属性に適合するルールと、**[IPv4 アドレス]** に適合するルールの 2 つを設定した場合、アクセスグループには指定されたネットワーク内のすべての資産に加えて、指定されたネットワークに属するかどうかに関わらず、指定された IPv4 アドレスを持つすべての資産が含まれます。

注意: **[ユーザーとグループ]** セクションで、アクセスグループのユーザーグループに割り当てられているアクセス許可を表示できます。新規アクセスグループに対し、Tenable Vulnerability Management はデフォルトで、**[すべてのユーザー]** グループに **[アクセスなし]** アクセス許可を割り当てます。**[すべてのユーザー]** グループでこれらのアクセス許可を変更することもできますし、デフォルトのアクセス許可を保持したまま、追加のユーザーグループでアクセスグループに対してより高いレベルのアクセス許可を割り当てることもできます。詳細は、ユーザーグループを編集するを参照してください。

10. **[ユーザーとグループ]** セクションで、アクセスグループのユーザーのアクセス許可を設定します。
11. **[保存]** をクリックします。

    Tenable Vulnerability Management によりアクセスグループが作成されます。[**アクセスグループ**] ページが表示されます。

注意: アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのにある程度の時間を要する場合があります。

[アクセスグループ] ページにあるアクセスグループの表の **[ステータス]** 列で、この割り当てプロセスのステータスを確認できます。

次の手順

- ユーザーグループで、このアクセスグループにアクセス許可を割り当てます。

アクセスグループのユーザーのアクセス許可を設定する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

個別のユーザーまたはユーザーグループに対して、アクセスグループのアクセス許可を設定できます。グループに対してアクセスグループのアクセス許可を設定する場合、グループ内のすべてのユーザーに同じアクセス許可を割り当てます。詳細は、ユーザーグループ を参照してください。

ユーザーまたはユーザーグループに対して、次のアクセスグループのアクセス許可を割り当てることができます。

- **アクセスなし** - (**[すべてのユーザー]** ユーザーグループのみ) (特別にアクセス許可を割り当てたユーザーやグループを除く) すべてのユーザーは、アクセスグループで指定された資産またはターゲットをスキャンできません。またすべてのユーザーは、指定された資産やターゲットに関連する、個別の、または集約されたスキャン結果を表示することもできません。
- **閲覧可** - ユーザーが表示できる、集約されたスキャン結果のビュー (ワークベンチ/ダッシュボード) には、このアクセスグループで指定された資産やターゲットのスキャンデータが含まれます。このアクセス許可をアクセスグループの **[すべてのユーザー]** グループに割り当てた場合、このアクセスグループの資産やターゲットに対する集約されたスキャン結果を、すべてのユーザーが表示できます。
- **スキャン可** - ユーザーは、アクセスグループで指定された資産やターゲットをスキャンしたり、資産やターゲットの個別のスキャン結果を表示したりできます。このアクセス許可がない場合、Tenable Vulnerability Management がこのアクセスグループで指定された資産やターゲットを使用するスキャンの設定を妨げることはありませんが、スキャナーはその資産やターゲットをスキャンしません。このアクセス許可をアクセスグループの **[すべてのユーザー]** グループに割り当てた場合、すべてのユーザーはアクセスグループの資産やターゲットをスキャンしたり、関連する個別のスキャン結果を表示したりできます。

アクセスグループにおけるユーザーのアクセス許可は、階層的ではなく累積的です。ユーザーに対して資産またはターゲットのスキャンを許可し、かつその資産またはターゲットに対する集約された結果の表示も許可するには、アクセスグループでそのユーザーのアクセス許可を、**[閲覧可]** と **[スキャン可]** の両方に設定する必要があります。

ヒント: クラウドインフラを監査するスキャンを実行するには、127.0.0.1 をターゲットとして含む **[ターゲットのスキャン]** アクセスグループを設定し、ユーザーのアクセス許可を **[スキャン可]** に設定します。

アクセスグループのユーザーのアクセス許可を設定する方法

1. アクセスグループを作成または編集します。
2. **[ユーザーとグループ]** セクションで、次のいずれかを行います。

   - **[すべてのユーザー]** ユーザーグループのアクセス許可を編集する。

     [すべてのユーザー] ユーザーグループのデフォルトの値は、アクセスグループに依存します。

     - **[すべてのユーザー]** アクセスグループの場合、Tenable Vulnerability Management は **[すべてのユーザー]** グループに対してデフォルトでは **[閲覧可]** および **[スキャン可]** アクセス許可を割り当てます。Tenable では、初期設定時にこれらのアクセス許可を制限することをお勧めします。
     - 他のすべてのアクセスグループの場合、Tenable Vulnerability Management は **[すべてのユーザー]** グループに対してデフォルトでは **[アクセスなし]** アクセス許可を割り当てます。これらのアクセスグループに対しては、次のように **[すべてのユーザー]** グループのアクセス許可を設定します。

       a. **[すべてのユーザー]** グループのアクセス許可ドロップダウンの横にある ⌄ ボタンをクリックします。

       b. **[閲覧可]** をクリックします。

       c. アクセス許可ドロップダウンの横にある ⌄ ボタンをもう一度クリックします。

       d. **[スキャン可]** をクリックします。

       e. **[保存]** をクリックします。

       Tenable Vulnerability Management がすべてのユーザーに対して、グループ内の資産やターゲットの表示やスキャンを許可します。

   - ユーザーをアクセスグループに追加する

     a. 検索ボックスで、ユーザーまたはグループの名前を入力します。

     入力すると、ユーザーとグループのフィルタリングされたリストが表示されます。

b. 検索結果からユーザーまたはグループを選択します。

Tenable Vulnerability Managementにより、デフォルトでは**[閲覧可]**アクセス許可が付与された状態でユーザーがアクセスグループに追加され、関連するラベルが表示されているユーザーに追加されます。

c. (オプション) ユーザーに**[スキャン可]**アクセス許可を追加します。

i. ユーザーまたはグループのアクセス許可ドロップダウンの横にある ⌄ ボタンをクリックします。

ii. **[スキャン可]**をクリックします。

Tenable Vulnerability Management により、表示されているユーザーに**[スキャン可]**ラベルが追加されます。

d. **[保存]**をクリックします。

Tenable Vulnerability Management によりユーザーがアクセスグループに追加されます。

- 既存のユーザーにアクセス許可を追加する。

a. 編集するユーザーまたはグループを見つけます。

b. ユーザーまたはグループのアクセス許可ドロップダウンの横にある ⌄ ボタンをクリックします。

c. **[閲覧可]**または**[スキャン可]**を適宜クリックします。

Tenable Vulnerability Management により、表示されているユーザーに新しいアクセス許可を示すラベルが追加されます。

d. **[保存]**をクリックします。

Tenable Vulnerability Management により変更内容がアクセスグループに保存されます。

- 既存のユーザーからアクセス許可を削除する。

a. 編集するユーザーまたはグループを見つけます。

b. 削除する権限を示すラベルの✕ボタン

Tenable Vulnerability Managementをクリックします。により、表示されているユーザーからアクセス許可ラベルが削除されます。

[すべてのユーザー] グループから最後のアクセス許可を削除した場合、Tenable Vulnerability Management はそのグループのアクセス許可を **[アクセスなし]** に設定します。

個別のユーザーまたはグループから最後のアクセス許可を削除した場合、Tenable Vulnerability Management によりそのユーザーをアクセスグループから削除する旨の確認メッセージが表示されます。

- ユーザーをアクセスグループから削除する。

a. 削除するユーザーまたはユーザーグループの横にある ✕ ボタンをクリックします。

ユーザーまたはグループが **[ユーザーとグループ]** リストから消えます。

b. **[保存]** をクリックします。

Tenable Vulnerability Management により変更内容がアクセスグループに保存されます。

アクセスグループを編集する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行を参照してください。

必要なユーザーロール: 管理者

既存のアクセスグループのルールを編集したり、アクセスグループに割り当てられているユーザーとユーザーグループを追加または削除したりできます。

注意: システムによって生成された **[すべての資産]** アクセスグループの名前またはルール基準を編集することはできません。

ユーザー定義のアクセスグループの名前と基準は編集できます。システムによって生成された **[すべての資産]** アクセスグループの名前と基準は編集できません。

注意: **[ユーザーとグループ]** セクションで、アクセスグループのアクセス許可を設定したユーザーグループを表示することはできますが、編集はできません。これらのアクセス許可を変更するには、各ユーザーグループを編集してください。

アクセスグループを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Web App Scanning アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセスグループ]** タイルタブをクリックします。

[アクセスグループ] ページタブが表示されます。このページタブには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

5. アクセスグループの表で、編集するアクセスグループをクリックします。

   [アクセスグループの編集] ページが表示されます。

6. **[一般]** セクションの **[名前]** ボックスで、アクセスグループの新しい名前を入力します。

7. **[種類]** セクションで、アクセスグループの種類を編集します。

   a. 変更後のアクセスグループの種類を選択します。

      Tenable Vulnerability Managementにより操作の確認を促すメッセージが表示されます。

   b. **[確認]** をクリックします。

      Tenable Vulnerability Management により、それまでに追加されたルールのフィルター基準が消去されます。

8. **[ルール]** セクションで、アクセスグループのルールを編集します。

   アクセスグループのルールでは、資産またはターゲットをアクセスグループに含めるかどうかを判断する際に Tenable Vulnerability Management が評価する条件を規定します。

   - 既存のルールを編集するには、必要に応じてカテゴリ、演算子、値を変更します。
   - 既存のルールを削除するには、ルールの横にある ✕ ボタンをクリックします。
   - 新しいルールを追加するには、⊕ **[追加]** をクリックして新しいルールを作成します。

9. **[基準]** セクションで、Tenable Vulnerability Management で資産またはターゲットをアクセスグループと照合する際に使用する基準を指定します。

オプション	アクション
タグ	(資産の管理グループのみ) アクセスグループのタグ基準を指定する方法 a. **[タグ]** オプションをクリックします。 **[検索]** ボックスが表示されます。

	b. **[検索]** ボックスで、任意の場所をクリックします。 所属企業のタグのリストが表示されます。 c. タグをクリックします。 Tenable Vulnerability Management によってタグを表すラベルが **[検索]** ボックスに追加されます。 d. 次のいずれかを実行します。 • 別のタグを追加するには、これらの手順を繰り返します。 • タグを削除するには、ボックス内のタグにカーソルを合わせ、ラベルの横にある ✕ ボタンをクリックします。 **注意:** タグのみを基準として、資産をアクセスグループに一致させる場合は、このオプションを使用します。タグと追加の資産属性で資産を一致させるには、**[ルール]** オプションを使用してから、他のルールに加えて 1 つ以上のタグをルールとして指定します。
ルール	アクセスグループのルールでは、資産またはターゲットをアクセスグループに含めるかどうかを判断する際に Tenable Vulnerability Management が評価する条件を規定します。 **注意:** 1 つのアクセスグループにつき最大 1,000 個のルールを追加できます。 アクセスグループのルール基準を指定する方法 a. **[ルール]** オプションをクリックします。 b. **[カテゴリ]** ドロップダウンボックスで、資産またはターゲットを絞り込むために属性を選択します。 **注意:** 既存のタグに基づいてルールを作成できます。詳細は、タグを参照してください。 c. **[演算子]** ドロップダウンボックスで、演算子を選択します。 たとえば次の演算子があります。

• **is equal to**: Tenable Vulnerability Management は、指定された語句との完全一致に基づいてルールを資産またはターゲットと照合します。

> **注意:** Tenable Vulnerability Management では、1 つの IPv4 アドレスを指定するルールに対してはこの演算子を「等しい」と解釈しますが、IPv4 範囲または CIDR 範囲を指定するルールに対しては演算子を「含む」と解釈します。

• **contains**: Tenable Vulnerability Management は、指定された語句との部分一致に基づいてルールを資産またはターゲットと照合します。

• **starts with**: Tenable Vulnerability Management は、ルールを指定された語句で始まる資産またはターゲットと照合します。

• **ends with**: Tenable Vulnerability Management は、ルールを指定された語句で終了する資産またはターゲットと照合します。

d. テキストボックスで、選択したカテゴリに有効な値を入力します。

> **ヒント:** 複数の値をコンマで区切って入力できます。**IPV4 アドレス**の場合は、CIDR 表記 (例: 192.168.0.0/24)、範囲 (例: 192.168.0.1-192.168.0.255)、コンマ区切りリスト (例: 192.168.0.0, 192.168.0.1) を使用できます。

e. (オプション) 別のルールを追加するには、**[追加]** ボタンをクリックします。

> **注意:** アクセスグループに複数のルールを設定した場合、アクセスグループにはいずれかのルールに適合する資産またはターゲットが含まれます。たとえば、**[ネットワーク名]** 属性に適合するルールと、**[IPv4 アドレス]** に適合するルールの 2 つを設定した場合、アクセスグループには指定されたネットワーク内のすべての資産に加えて、指定されたネットワークに属するかどうかに関わらず、指定された IPv4 アドレスを持つすべての資産が含まれます。

10. **[ユーザーとグループ]** セクションで、アクセスグループのユーザーのアクセス許可を設定します。
11. **[保存]** をクリックします。

Tenable Vulnerability Management が変更内容をアクセスグループに反映します。**[アクセスグループ]** ページが表示されます。

> **注意:** アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのに

ある程度の時間を要する場合があります。

[アクセスグループ] ページにあるアクセスグループの表の **[ステータス]** 列で、この割り当てプロセスのステータスを確認できます。

次の手順

- (オプション) ユーザーグループでアクセスグループのアクセス許可を変更します。

アクセスグループに割り当てられていない資産を表示する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

資産がどのアクセスグループのルール基準とも一致しない場合、Tenable Vulnerability Management はその資産をどのアクセスグループにも割り当てません。これらの割り当てられていない資産は、**[すべての資産]** グループのユーザーアクセス許可が割り当てられているユーザーグループにのみ表示されます。所属する企業で **[すべての資産]** グループのメンバーシップを制限している場合、**[すべての資産]** グループのメンバーではないユーザーアクセス許可を持たないユーザーグループのユーザーは、これらの割り当てられていない資産を閲覧できません。またユーザーは、このように閲覧が制限されていることをすぐに理解するとは限りません。**[すべての資産]** グループのアクセス許可を持つユーザーグループのメンバーであるユーザーは、フィルターを使用してこれらの割り当てられていない資産を特定できます。

アクセスグループに割り当てられていない資産を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[資産ビュー]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。

3. 以下の手順でフィルターを作成します。

   - カテゴリ: **アクセスグループに属する**
   - 演算子: **is equal to**
   - 値: **false**

4. **[適用]** をクリックします。

   資産テーブルが更新され、アクセスグループに割り当てられていないすべての資産が表示されます。

割り当てられたアクセスグループを表示する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

管理者は、すべてのアクセスグループについて、ルールおよびアクセスグループに割り当てられたユーザーとユーザーグループを表示できます。アクセスグループのパラメーターを編集することもできます。

他のすべてのロールのユーザーは、自分に割り当てられたアクセスグループしか表示できません。表示には、各アクセスグループに関連付けられたルールが含まれますが、アクセスグループに割り当てられた他のユーザーまたはユーザーグループは除外されます。アクセスグループの設定を編集することはできません。

注意: アクセスグループタイルは、1 つ以上のアクセスグループが割り当てられている場合や、自分が管理者であり、Tenable Vulnerability Management のユーザーがアクセスグループに割り当てられている場合にのみ表示されます。すべてのアクセスグループを権限設定に変換すると、**アクセスグループ**タイルはアカウントに表示されなくなります。

ユーザーが自分に割り当てられたアクセスグループを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルタブをクリックします。

   [アクセスグループ] ページタブが表示されます。このページタブには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. **[アクセスグループ]** ページには、以下の情報を含む表が含まれています。

- **名前** - アクセスグループ名
- **所有者** - アクセスグループの所有者
- **権限タイプ** - アクセスグループのタイプ
- **最終変更日** - 組織のユーザーがアクセスグループ設定を最後に変更した日付
- **最終変更者** - アクセスグループ設定を最後に変更した組織のユーザー
- **ステータス** - 資産をアクセスグループに一致させる Tenable Vulnerability Management プロセスのステータス可能な値は**進行中**または**完了**です。進行中のプロセスの完了率を表示するには、[進行中] ステータスにカーソルを合わせます。

5. (オプション) 詳細を表示するには、アクセスグループをクリックします。

   [アクセスグループの編集] ページが表示されます。

   管理者の場合、このページにはルールおよび割り当てられたユーザーとユーザーグループが含まれ、すべてのアクセスグループのパラメーターを編集できます。

   他のロールに割り当てられたユーザーの場合、このページにはルールのみが含まれ、ルールの編集はできません。

アクセスグループを削除する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行を参照してください。

必要なユーザーロール: 管理者

注意: システム生成の **[すべての資産]** グループは削除できません。

1 つ以上のアクセスグループを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルタブをクリックします。

   [アクセスグループ] ページタブが表示されます。このページタブには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. 削除するアクセスグループを選択します。

   - 1 つのアクセスグループを選択します。

     a. アクセスグループの表で、削除するアクセスグループにカーソルを合わせます。

        アクションボタンが行に表示されます。

     b. 🗑 ボタンをクリックします。

        確認ウィンドウが表示されます。

   - 複数のアクセスグループを選択します。

a. アクセスグループの表で、削除するアクセスグループの横にあるチェックボックスを選択します。

   ページの下部またはテーブルの上部に、アクションバーが表示されます。

b. アクションバーで、 ボタンをクリックします。

   確認ウィンドウが表示されます。

5. 確認ウィンドウで、**[削除]** ボタンをクリックします。

   Tenable Vulnerability Management により選択されたアクセスグループが削除され、アクセスグループ表が更新されます。

アクセスグループルールのフィルター

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行を参照してください。

アクセスグループのルールを作成するために、次のセクションで説明されているフィルターを使用できます。詳細については、次を参照してください。

- Tenable が提供するフィルター
- Tenable が提供するフィルターのガイドライン
- タグフィルター

Tenable が提供するフィルター

次の表の右端の 2 列は、**[資産の管理]** または **[ターゲットのスキャン]** のグループタイプにフィルターを使用できるかどうかを示します。

フィルター	説明	資産の管理	ターゲットのスキャン
AWS Account ID	資産に関連付けられた Amazon Web Services (AWS) アカウントの正規ユーザー識別子です。詳細は、AWS ドキュメントの「AWS アカウントの識別子」を参照してください。	○	×
AWS 可用性ゾーン	AWS が仮想マシンインスタンスをホストしているアベイラビリティゾーンの名前。詳細は、AWS ドキュメントの「リージョンとアベイラビリティゾーン」を参照してください。	○	×
AWS EC2 AMI ID	Amazon Elastic Compute Cloud (Amazon EC2) での、Linux AMI イメージの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。	○	×

AWS EC2 インスタンス ID	Amazon EC2 での Linux インスタンスの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。	○	×
AWS EC2 名	Amazon EC2 での仮想マシンインスタンスの名前。	○	×
AWS EC2 製品コード	Amazon EC2 での仮想マシンインスタンスの立ち上げに使用された AMI に関連付けられた製品コード。	○	×
AWS リージョン	たとえば 'us-east-1' などの、AWS が仮想マシンインスタンスをホストするリージョン。詳細は、AWS ドキュメントの「リージョンとアベイラビリティゾーン」を参照してください。	○	×
AWS セキュリティグループ	Amazon EC2 で、仮想マシンインスタンスを割り当てたセキュリティグループ。詳細は、Amazon Virtual Private Cloud ユーザーガイドの「セキュリティグループ」を参照してください。	○	×
AWS サブネット ID	スキャン時に仮想マシンインスタンスが動作していた、AWS サブネットの固有識別子。	○	×
AWS VPC ID	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、「Amazon Virtual Private Cloud ユーザーガイド」を参照してください。	○	×
Azure リソース ID	Azure Resource Manager での、リソースの固有識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。	○	×
Azure VM ID	Microsoft Azure 仮想マシンインスタンスの固有識別子。詳細は、Microsoft Azure ドキュメントの「Azure VM Unique ID のアクセスと使用」を参照してください。	○	×
FQDN/Hostname	次のうちのいずれかです。 • 資産の完全修飾ドメイン名 • 資産のホスト名。	○	○

Google Cloud インスタンス ID	Google Cloud Platform (GCP) での、仮想マシンインスタンスの固有識別子。	○	×
Google Cloud プロジェクト ID	GCP で、仮想マシンインスタンスが所属するプロジェクトのカスタマイズされた名前。詳細は、GCP ドキュメントの「プロジェクトの作成と管理」を参照してください。	○	×
Google Cloud ゾーン	GCP で、仮想マシンインスタンスが動作しているゾーン。詳細は、GCP ドキュメントの「リージョンとゾーン」を参照してください。	○	×
IPv4 アドレス	資産の IPv4 アドレス。このフィルターでは、CIDR 表記 (例: 192.168.0.0/24)、範囲 (例: 192.168.0.1-192.168.0.255)、コンマ区切りのリスト (例: 192.168.0.0, 192.168.0.1) を使用できます。	○	○
IPv6 アドレス	資産の IPv6 アドレス。	×	○
MAC アドレス	資産の MAC アドレスです。	○	×
NetBIOS 名	資産の NetBIOS 名。	○	×
ネットワーク名	資産が所属するネットワークの名前です。	○	×
オペレーティングシステム	資産にインストールされているオペレーティングシステム。	○	×
Qualys 資産 ID	Qualys の資産の資産 ID。詳細は、Qualys のドキュメントを参照してください。	○	×
Qualys ホスト ID	Qualys での資産のホスト ID。詳細は、Qualys のドキュメントを参照してください。	○	×
ServiceNow Sys ID	ServiceNow での、資産の固有レコード識別子です。詳細は、ServiceNow のドキュメントを参照してください。	○	×

Tenable が提供するフィルターのガイドライン

- **[ターゲットのスキャン]** アクセスグループのルールを設定する際、資産の属性タイプは、関連するスキャンに使用されるターゲットの形式と一致する必要があります。たとえば、**[ターゲットのスキャン]** アクセスグループのルールが **[FQDN/ホスト名]** 属性でフィルタリングする場合、スキャンターゲットが FQDN またはホスト名の形式で指定されている場合には関連するスキャンは成功しますが、スキャンターゲットが IPv4 形式で指定されている場合には失敗します。

タグフィルター

Tenable Vulnerability Management では、タグにより資産に説明メタデータを追加することで、資産を事業の文脈別にグループに分けることができます。詳細は、タグを参照してください。

作成したタグを使用して、資産を **[資産の管理]** アクセスグループに割り当てることができます。

ルールにタグフィルターを追加する方法

1. **[カテゴリ]** ドロップダウンボックスで、**[タグ]** を選択します。
2. **[演算子]** ドロップダウンボックスで、**[含む]** を選択します。
3. テキストボックスで、検索するタグカテゴリと値を次の形式で入力します。

   ```
   Category Name:Value Name
   ```

4. ルールの作成を続行するか、アクセスグループを作成するの説明に従って、アクセスグループを保存します。

注意: 関連付けられている値が 100,000 以上あるタグカテゴリは、ルールとしてアクセスグループに追加できません。

スキャンのアクセス許可の移行

ユーザーが特定のターゲットをスキャンできるかどうかを制御していた、システムターゲットグループのアクセス許可は、アクセスグループに移行しました。

注意: Tenable は、近い将来にアクセスグループを非推奨にする予定です。現在はまだ、アクセスグループを作成および管理できます。ただし、Tenable では、代わりにアクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することを推奨しています。

この移行により、次に示す既存の Tenable Vulnerability Management の設定が影響を受けます。

要素	アクション
既存のアクセスグループ	Tenable Vulnerability Management: • 既存のアクセスグループはすべて、**[資産の管理]** の種類のアクセスグループへと更新されます。 • **[すべてのユーザー]** トグルは、デフォルトの **[すべてのユーザー]** グループで置き換えられます。 • 現在表示のアクセス権を持つ既存のユーザーまたはユーザーグループには、**[閲覧可]** アクセス許可が割り当てられます。
既存のシステムターゲットグループ	既存の各システムターゲットグループに対して、Tenable Vulnerability Management は次を実行します。 • 新たに **[ターゲットのスキャン]** の種類のアクセスグループを作成します。このアクセスグループは、既存のシステムターゲットグループと同じスキャンターゲットを指定します。Tenable Vulnerability Management は移行されたアクセスグループの所有者として、[移行] を表示します。 • システムターゲットグループで **[スキャン可]** アクセス許可を持つすべてのユーザーを新しいアクセスグループに移動し、そのユーザーにそのアクセスグループでの **[スキャン可]** アクセス許可を割り当てます。そのターゲットでの結果をユーザーが表示できるようにするには、そのアクセスグループでユーザーに **[閲覧可]** アクセス許可を設定してください。 **注意:** この移行では、既存のシステムターゲットグループは削除されません。移行により、システムターゲットグループから **[スキャン可]** アクセス許可のみが削除されます。

	注意：移行時に既存のターゲットグループにスキャンのアクセス許可が含まれている場合、新しい Tenable Vulnerability Management ユーザーインターフェースでターゲットグループの表の **[アクセス許可]** 列のグループに **[スキャン]** ラベルが表示される場合があります。このラベルは、過去のスキャンのアクセス許可のみを表します。現在のスキャンのアクセス許可は、アクセスグループで指定されます。
既存のスキャン設定、ダッシュボードフィルター、および保存した検索	既存のスキャン設定は、システムターゲットグループのターゲット設定として維持されます。既存のダッシュボードフィルターおよび保存した検索は、システムターゲットグループのフィルター設定として維持されます。システムターゲットグループの **[アクセス許可]** がある場合、スキャン設定でターゲットグループを指定するために、あるいはダッシュボードおよび検索のフィルターで、そのシステムターゲットグループを使用し続けることができます。ただし、そのターゲットでのスキャン結果を表示できるユーザーを指定するには、適切なアクセスグループで **[Can View]** アクセス許可を設定してください。

アクティビティログ

必要なユーザーロール: 管理者

[アクティビティログ] ページでは、企業の Tenable Web App Scanning アカウント内のすべてのユーザーに対するイベントのリストを表示できます。各アクティビティが行われたタイミング、アクション、アクター、その他アクティビティに関連する情報を確認できます。

重要: Tenable では現在アクティビティログデータは 3 年保持され、その後 Tenable のデータベースから削除されます。

アクティビティログを表示する方法

1. 左上にある ☰ ボタンをクリックします。

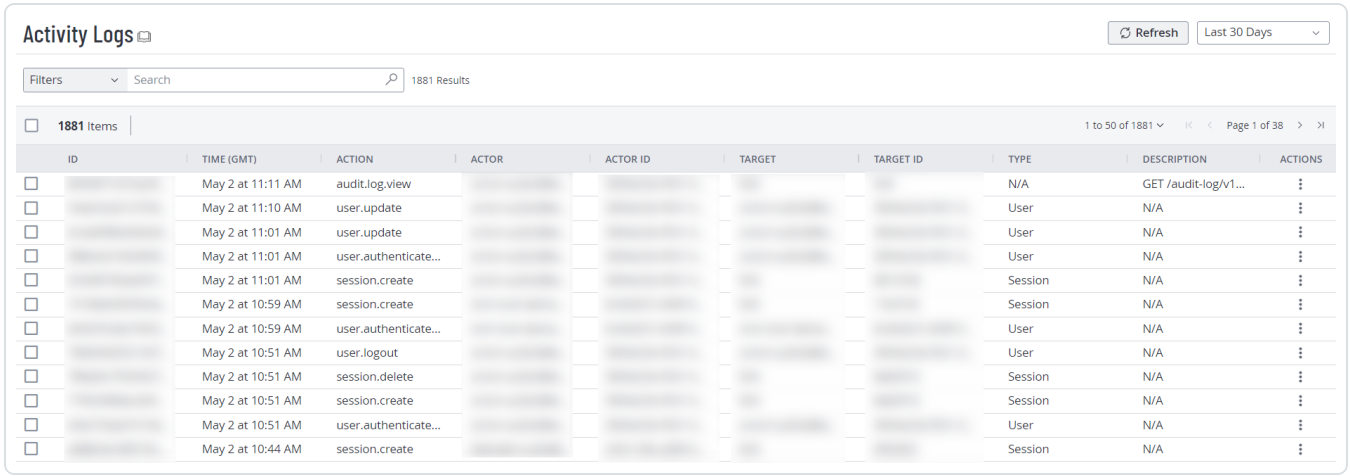
   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクティビティログ]** タイルをクリックします。

   [アクティビティログ] ページが表示されます。このページには、企業の Tenable Web App Scanning アカウントに関連するアクティビティのリストが表示されます。



4. (オプション) 表データを選別します。詳細は、Tenable Web App Scanning の表 を参照してください。

5. (オプション) 表にフィルターを適用します。

フィルター	説明
アクター ID	アクションを実行したアカウントの ID
ターゲット ID	アクションの影響を受けたアカウントの ID (存在する場合)
アクション	アクションの種類
日付	アクションが実行された日付

6. (オプション) アクティビティログの表を更新するには、右上にある **[更新]** ボタンをクリックします。
7. (オプション) 表を特定の期間でフィルタリングします。
    - **過去 7 日間**
    - **過去 14 日間**
    - **過去 30 日間**
    - **過去 90 日間**
    - **すべて**

次の手順

- (オプション) 1 つ以上のアクティビティログをエクスポートします。

アクティビティログのエクスポート

必要なユーザーロール: 管理者

[アクティビティログ] ページでは、1 つ以上のアクティビティログを CSV または JSON 形式でエクスポートできます。

アクティビティログをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクティビティログ]** タイルをクリックします。

   [アクティビティログ] ページが表示されます。このページには、企業の Tenable Web App Scanning アカウントに関連するアクティビティのリストが表示されます。

4. (オプション) 表データを選別します。詳細は、表のフィルタリング を参照してください。

5. エクスポートするアクティビティログを選択します。

エクスポート範囲	アクション
選択したアクティビティログ	選択したアクティビティログをエクスポートする方法 a. アクティビティログの表で、エクスポートする各アクティビティログのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→**[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のアクティビティログをエクスポートする場合は、リスト内のすべてのア

	クティビティログを選択してから、[→**[エクスポート]**をクリックします。
1つのアクティビティログ	1つのアクティビティログをエクスポートする方法 a. アクティビティログの表で、エクスポートするアクティビティログの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- アクティビティログの表の**[アクション]**列で、エクスポートするアクティビティログの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. [→ **[エクスポート]**をクリックします。

[エクスポート]プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス。
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]**ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	アクティビティログのリストを含むCSVテキストファイル。

	注意: .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたアクティビティログのリストを含む JSON ファイル。 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Web App Scanning では、エクスポート有効期限に最大 30 暦日を設定できます。
10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。
    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。
11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。
    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Web App Scanning がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Web App Scanning がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Web App Scanning によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポートプレーンを閉じた場合は、Exportsページからエクスポートファイルにアクセスできます。

タグ

Tenable Web App Scanning で記述メタデータを資産にタグ付けすることで、資産に独自の事業の文脈を追加できます。資産タグは、主に *カテゴリ:値* のペアで設定されます。たとえば、資産を場所ごとにグループ化する場合は、*[場所]* というカテゴリを作成し、その値を *Headquarters* にできます。その後、個々の資産に手動でタグを適用するか、ルールをタグに追加して Tenable Web App Scanning が一致する資産に自動的にタグを適用するようにできます。

タグ構造の詳細については、タグの形式と適用を参照してください。

> **注意:** 個別のカテゴリを使用せずにタグを作成する場合、Tenable では、すべてのタグに使用できる汎用カテゴリの *[カテゴリ]* を追加することを推奨しています。

タグを利用して資産に独自の事業の文脈を付加することで、分析ビューをタグでフィルタリングすることが可能になります。

タグを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

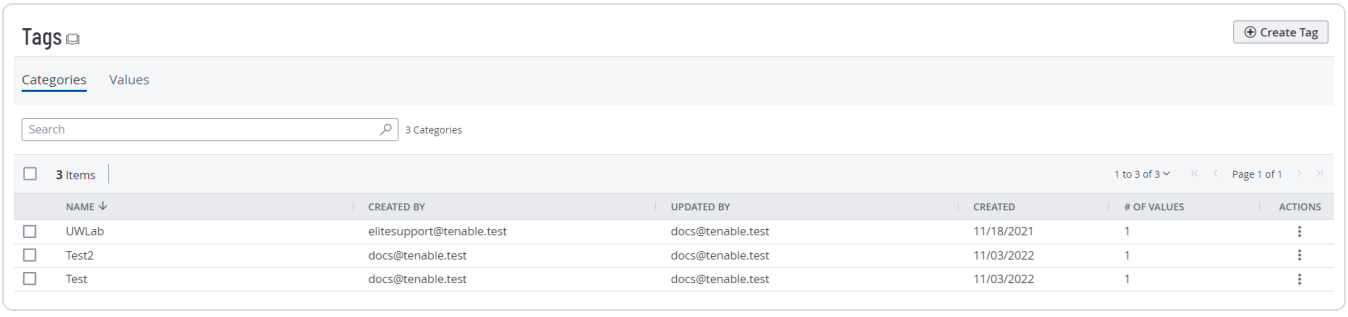
2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。



4. 次のいずれかを行います。

Tenable Web App Scanning インスタンス上のすべてのタグに割り当てられたカテゴリを表示する方法

a. **[カテゴリ]** 表で、タグカテゴリとそれに関連するデータを確認できます。

列	説明
名前	タグの名前
作成者	タグを作成したユーザーのユーザー名
最終使用者	タグの値またはカテゴリを最後に作成または編集したユーザーのユーザー名
作成日	タグが作成された日付
値の数	当該タグカテゴリに関連付けられているタグ値の数
アクション	タグで実行できるアクション

Tenable Web App Scanning インスタンス上のすべてのタグを表示する方法

a. **[値]** タブをクリックします。

[値] ページが開き、Tenable Web App Scanning インスタンス上のすべてのタグの表が表示されます。

b. **[値]** 表で、タグとそれらに関連するデータを確認できます。

列	説明
名前	タグの名前
作成者	タグを作成したユーザーのユーザー名
更新者	タグのカテゴリまたは値を最後に更新したユーザーのユーザー名
作成日	タグが作成された日付
適用方法	タグの適用が**手動**または**自動**で行われるかを示します

最終処理日時	Tenable Web App Scanning によって最後にスキャン処理が行われ、関連するすべての資産に適用した日時
評価	Tenable Vulnerability Management が特定を終了し、一致するすべての資産にタグを適用したかどうかを示します
アクション	タグで実行できるアクション

例: 資産のタグ付け

一般的なユースケースとして、次の資産のタグ付けの設定例を確認してください。タグについての一般的な情報は、タグを参照してください。

- 例: インストール済みソフトウェア別に自動でタグ付けする
- 例: 優先度によって手動でタグ付けする
- 例: タグ付けされた資産の ACR 値の更新

例: インストール済みソフトウェア別に自動でタグ付けする

あなたの会社では、Oracle と Wireshark の、2 種類のソフトウェア上で動作する資産を管理しています。会社はソフトウェアの種類に基づいて、資産の所有者のアクセス許可を従業員に割り当てます。従業員は、自身が管理するソフトウェアの種類の資産上に認められた、脆弱性を解決する義務があります。

管理者ユーザーであるあなたは、両方のソフトウェアの種類に対する動的タグを作成できます。そうすることで、従業員は **[インストール済みのソフトウェア]** タグを使用して資産を検索し、自身が管理するソフトウェアの種類によって Tenable Web App Scanning 資産をフィルタリングできます。

> **注意:** より厳密な結果を得るためには、タグの値を該当する NVD 共通プラットフォーム一覧 (CPE) に合わせて設定します。例: `cpe:/a:microsoft:office`

インストール済みソフトウェア別に自動で資産にタグ付けする方法

1. 次の設定を使用して、Oracle 資産のタグを作成して自動的に適用します。

オプション	値
カテゴリ	*インストール済みのソフトウェア*
値	*Oracle*
ルール	以下のルールを指定して有効にします。 • **すべてに一致** • **カテゴリ**: *インストール済みのソフトウェア* • **演算子**: *次の値に等しい*: • **値**: *Oracle*

2. 次の設定を使用して、Wireshark 資産のタグを作成して自動的に適用します。

オプション	値
カテゴリ	*インストール済みのソフトウェア*
値	*Wireshark*
ルール	以下のルールを指定して有効にします。 • **すべてに一致** • **カテゴリ**: *インストール済みのソフトウェア* • **演算子**: *次の値に等しい*: • **値**: *Wireshark*

3. 従業員に、新しいタグを使用して資産の表で資産をフィルタリングするか、タグの表から資産を検索するように指示します。

例: 優先度によって手動でタグ付けする

あなたの会社には機密性の高い資産があり、従業員にはそれらの資産の脆弱性を、資産の他の属性(たとえば資産の VPR)に関わらず最優先で対処してほしいとします。

従業員がそれらの機密性の高い資産を最初に表示し、対応することを確実にするため、**[高優先度]**タグを作成して、従業員に優先してほしい資産に手動で追加できます。そうすることで、従業員は**[高優先度]**タグを使用して、自身が管理する最優先の資産でフィルタリングし、資産を検索できます。

優先度によって資産に手動でタグ付けする方法

1. 次の設定を使用して、最優先の資産のタグを作成します。

オプション	値
カテゴリ	*優先度*
値	*高優先度*
値の説明	このタグを持つ資産の脆弱性修復の緊急度に関するカスタムの説明です。

2. 最優先の資産に、タグを手動で適用します。
3. 従業員に、新しいタグを使用して資産の表で資産をフィルタリングするか、タグの表から資産を検索するように指示します。

例: タグ付けされた資産の ACR 値の更新

あなたの会社では Tenable Lumin を使用して Cyber Exposure を評価しています。共通のエクスポージャーを持つ資産のグループがありますが、Tenable によって割り当てられる ACR の値は資産のグループ内で異なります。

資産の ACR 値をカスタマイズするには、任意のタグ内で属性設定を使用して、そのタグが付いた資産の ACR 値を自動的に更新できます。

タグが付いたすべての資産の ACR 値を更新する方法

1. タグを作成して、手動でまたは自動的に適用します。
2. タグが付いた資産に対して属性オーバーライドを設定します。
    a. **[属性オーバーライド]**トグルをクリックして、このタグを持つ資産への属性の自動適用を有効にします。

    基準ボックスが表示されます。

b. 最初のボックスで、属性を選択します(例: **ACR(資産重大度の格付け)(ACR)**)。

c. 2番目のボックスで、値を選択します(例: **9(重大)**)。

3. **[保存]**をクリックします。

タグが付いたすべての資産の属性がTenable Vulnerability Managementによって更新されます。

注意: タグを介して資産属性をオーバーライドする場合、システムの負荷や資産の数によっては、Tenable Vulnerability Managementがタグが付いた資産の属性を更新するのに時間を要する場合があります。

ヒント: タグ更新済みのACR値に対してTenable Vulnerability Managementが優先度を付ける方法についての詳細は、ACR(資産重大度の格付け)(ACR)を参照してください。

4. 資産表で更新されたACR値を確認するように、従業員に指示します。

タグの形式と適用

資産タグは、主に *カテゴリ:値* のペアで設定されます。たとえば、資産を場所ごとにグループ化する場合は、*[場所]* というカテゴリを作成し、その値を *Headquarters* にできます。

注意: 個別のカテゴリを使用せずにタグを作成する場合、Tenable では、すべてのタグに使用できる汎用カテゴリの *[カテゴリ]* を追加することを推奨しています。

次の場合に、タグメンバーシップが再評価されます。

- タグを更新または作成する場合
- Tenable Web App Scanning がデータをインポートする場合
- 12 時間ごと

手動タグと自動タグ

タグを作成すると、Tenable Web App Scanning により、タグルールに一致するインスタンス上の資産に、そのタグが自動的に適用されます。これらの自動的に適用されるタグは、*動的タグ*と呼ばれることもあります。自動タグを作成すると、Tenable Web App Scanning が、現在のすべての資産と、企業のアカウントに新しく追加された資産にそのタグを適用します。Tenable Web App Scanning はまた、資産の属性に変更がないか定期的に確認し、その結果に応じて自動タグを追加または削除します。

注意: 自動タグを作成または編集する場合、システムの負荷や対象資産の数によっては、Tenable Web App Scanning がタグを既存の資産に適用するのに時間を要する場合があります。

ルールなしでタグを作成し、個別の資産に手動で適用することもできます。または、自動タグを、そのタグのルール基準を満たさない可能性のある他の資産に手動で適用することもできます。これらの手動で適用されるタグは、*静的タグ*と呼ばれることもあります。

手動タグは アイコンで表示され、自動タグは アイコンで表示されます。

説明については、以下の例を参照してください。

シナリオ	タグのタイプ	タグアイコン
カテゴリ:値 ペアに *Location:Headquarters* を指定してタグを作成しますが、タグルールは追加しません。後で、そのタグを本社 (headquraters) にある資産に追	手動	

加します。		
カテゴリ: *値* ペアを *Location*: *Headquarters* にしてタグを作成し、タグルールで IP アドレス範囲を指定します。これにより Tenable Web App Scanning によって、その IP アドレス範囲内にあるすべての既存の資産または新規の資産に、このタグが自動的に適用されます。	自動	

手動タグまたは自動タグの作成

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

注意: **[タグ付け]** ページでタグを作成する場合は、汎用資産フィルターのリストから選択してタグルールを作成できます。特定の資産タイプに固有のフィルターに基づいてタグを作成する場合、Tenable は、**[資産]** ページでタグを作成することを推奨しています。[資産] ページでは、各資産タイプに固有の追加のフィルターを選択できます。

タグを適用できない場合、タグルールから返される資産が多過ぎて Tenable Web App Scanning で処理できない可能性があります。たとえば、ワイルドカードを含む完全修飾ドメイン名 (FQDN) の長いリストには、多数の資産が含まれます。この状況が発生した場合、Tenable では、より厳密なタグルールを使用して資産の数を減らすことを推奨しています。必要に応じて、追加のタグを使用して各リストを結合できます。

[タグを作成] ページで、手動タグを作成して資産に個別に適用できます。Tenable Web App Scanning が一致する資産を識別してタグ付けする際に使用するタグルールを作成することで、自動タグを作成することもできます。

注意: 最大 100 個のタグカテゴリを作成でき、各カテゴリには最大 100,000 個のタグを含めることができます。

[タグ] ページで自動タグを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

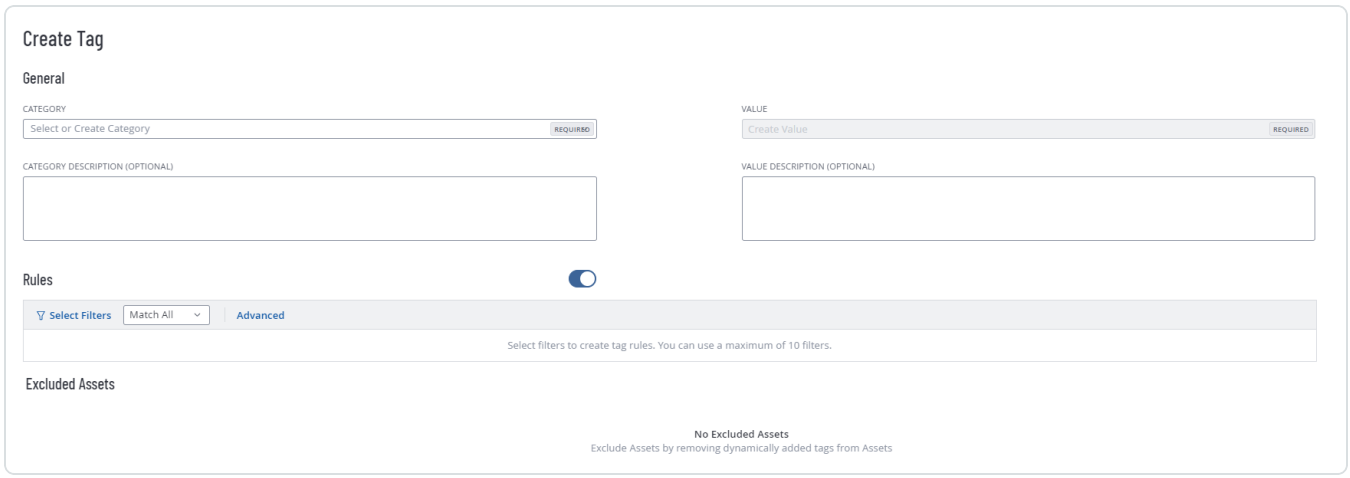
3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. ページの右上にある ⊕ **[タグの作成]** ボタンをクリックします。

   [タグの作成] ページが表示されます。



5. **[カテゴリ]** ドロップダウンボックスをクリックします。
6. **[新しいカテゴリの追加]** ボックスにカテゴリを入力します。

   入力に伴って、リストでは一致が絞り込まれます。
7. ドロップダウンボックスから既存のカテゴリを選択するか、新しいカテゴリの場合は **["*カテゴリ名*"の作成]** をクリックします。

   注意: Tenable Web App Scanning インスタンスでは最大 100 個のカテゴリを作成できます。
8. (オプション) **[カテゴリの説明]** ボックスに、タグカテゴリの説明を入力します。
9. **[値]** ボックスに、タグの名前を入力します。

   注意: タグ名は、コンマを含めず 50 文字以内にしてください。

   ヒント: Tenable では、タグカテゴリに直接対応するタグ名を指定することを推奨しています。たとえば、カテゴリが *[場所]* の場合は、「*Headquarters*」が適切な値になります。
10. (オプション) **[値の説明]** ボックスに、新しいタグの説明を入力します。
11. 次のいずれかを行います。

    ### タグを手動タグとして保存する方法

    a. **[保存]** をクリックします。

       Tenable Web App Scanning によって、タグがタグの表に保存されます。

    b. (オプション) 1 つ以上の資産に手動でタグを追加します。

タグを保存して自動的に適用する方法

a. タグルールを作成します。

b. **[保存]**をクリックします。

Tenable Web App Scanning は、タグを作成して、既存の資産を評価し、タグルールに一致する資産にタグを自動的に適用します。

> **注意:** 自動タグを作成する場合、システムの負荷や資産の数によっては、Tenable Web App Scanning がタグを適用し、除外された資産を更新するのに数分かかる場合があります。

ルール付きのタグに関する考慮事項

自動での適用

Tenable Web App Scanning は次の状況のとき、タグルールに照らして資産を評価します。

- 新しい資産が(スキャン経由、コネクタによるインポート、または Tenable Web App Scanning API を活用して)追加されると、Tenable Web App Scanning は資産をタグルールに照らして評価します。
- タグルールが作成または更新されると、Tenable Web App Scanning はそのタグルールに照らして資産を評価します。

  > **注意:** タグルールを作成または編集すると、システムの負荷や対象資産の数によっては、Tenable Web App Scanning がタグを既存の資産に適用するのに時間を要する場合があります。

- 既存の資産が更新されると、Tenable Web App Scanning は資産を再評価し、資産の属性がタグルールに一致していない場合は、そのタグを削除します。

手動による適用

ルール付きで設定されたタグを手動で適用すると、Tenable Web App Scanning は以後、そのルールに基づく評価からその資産を除外します。

タグルール

タグルールを使用すると、Tenable Web App Scanning は作成されたタグを、タグルールに一致するインスタンス上の資産に自動的に適用します。これらの自動的に適用されるタグは、*動的タグ*または*自動タグ*と呼ばれています。

タグルールは、資産属性に基づく1つ以上のフィルターと値のペアで設定されます。ルールを作成してタグに追加すると、Tenable Web App Scanning が、タグルールに一致するインスタンス上のすべての資産にそのタグを適用します。

> **注意:** Tenable Web App Scanning は、タグごとに最大 1,000 のルールをサポートします。この制限は、1 つのタグ値に対して最大 1,000 個の **and** または **or** 条件を指定できることを意味します。さらに、Tenable Web App Scanning は、個別のタグルールごとに最大 1,024 個の値をサポートします。

自動タグに関する詳細は、タグの形式と適用を参照してください。

[タグ] セクションで、タグルールを使用して次のタスクを実行できます。

- タグルールの作成
- タグルールの編集
- タグルールの削除

タグルールの作成

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

タグを作成または編集して自動的に適用する場合は、ルールを作成し、タグルールフィルターを通してタグに適用する必要があります。タグルールは、**[基本]** モードまたは **[詳細]** モードのいずれかで作成できます。

注意: タグルールを **[基本]** モードで作成してから **[詳細]** モードに切り替えると、作成したルールは **[詳細]** モードの形式で表示されます。ただし、**[詳細]** モードから **[基本]** モードに切り替えた場合は、Tenable Web App Scanning によりルールセクションからすべてのルールが削除されます。

注意: **[タグ付け]** ページでタグを作成する場合は、汎用資産フィルターのリストから選択してタグルールを作成できます。特定の資産タイプに固有のフィルターに基づいてタグを作成する場合、Tenable は、**[資産]** ページでタグを作成することを推奨しています。[資産] ページでは、各資産タイプに固有の追加のフィルターを選択できます。

タグの自動適用に関する詳細は、ルール付きのタグに関する考慮事項を参照してください。

始める前に

- タグを作成または編集します。

ルールを作成してタグに追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[値]** タブをクリックします。

[値] ページが開き、Tenable Web App Scanning インスタンス上のすべてのタグの表が表示されます。

5. ルールの設定を有効にするには、**[ルール]** トグルをクリックします。

   [ルール] セクションが表示されます。

6. 作成するタグルールごとに、次のいずれかを実行します。

   注意: デフォルトでは **[基本]** モードがアクティブになっています。

   ### [基本] モードでタグルールを作成する方法

   a. **[ルール]** セクションで、▽ **[フィルターの選択]** をクリックします。

      ドロップダウンボックスが開き、タグルールフィルターオプションが一覧表示されます。

      注意: タグルールフィルターによって、1 つのフィルターに適用可能な値の数の上限が異なります。これらの制限の詳細については、タグルールフィルターを参照してください。

   b. フィルターを選択します。

      選択したフィルターが **[ルール]** セクションに表示されます。

   c. ドロップダウンボックスの外側をクリックします。

      ドロップダウンボックスが閉じられます。

   d. フィルターで、∨ ボタンをクリックします。

      フィルターが展開されます。

   e. 1 つ目のドロップダウンボックスで、フィルターに適用する演算子を選択します。

   f. 2 つ目のドロップダウンボックスで、フィルターの値を 1 つ以上選択または入力します。

   g. (オプション) 別のルールを作成するには、**[基本]** モードでタグを作成する手順を繰り返します。

   h. (オプション) 別のルールを作成する方法

i. **[基本]** モードでタグルールを作成する手順を繰り返します。

ii. **[ルール]** セクションの **[いずれかに一致]** ドロップダウンボックスで、次のいずれかを実行します。

- いずれかのルールに一致する資産にタグを適用するには、**[いずれかに一致]** を選択します。

  OR 演算子が各ルールの間に表示され、Tenable Web App Scanning はそのタグに指定されたルールのいずれかを満たす資産にタグを適用します。

- すべてのルールに一致する資産のみにタグを適用するには、**[すべてに一致]** を選択します。

  各ルールの間に **AND** 演算子が表示されます。

  Tenable Web App Scanning は、そのタグに指定されたすべてのルールを満たす資産にのみタグを適用します。

[詳細] モードでタグルールを作成する方法

a. **[ルール]** セクションで、**[詳細]** をクリックします。

テキストボックスが表示されます。

b. テキストボックス内にカーソルを置きます。

ドロップダウンボックスが開き、タグルールフィルターオプションが一覧表示されます。

> **注意:** タグルールフィルターによって、1 つのフィルターに適用可能な値の数の上限が異なります。これらの制限の詳細については、タグルールフィルターを参照してください。

> **注意:** タグルールに誤字が含まれていた場合は、問題の説明を含むエラーが **[ルール]** ボックスに表示されます。

c. 適用するフィルターを選択または入力します。

> **ヒント:** 矢印キーを使用してフィルタードロップダウンボックス内を移動し、**Enter** キーを押してオプションを選択できます。

フィルターがテキストボックスに表示されます。

フィルターの右側に演算子のドロップダウンボックスが表示されます。

d. 次の演算子のいずれかを選択します。選択できる演算子は、選択したフィルターに応じて異なります。

> **注意:** (') または (") で始まる値や (*) または (,) を含む値でフィルタリングする場合は、値を引用符 (") で囲む必要があります。

演算子	説明
存在する	選択されたフィルターが存在するアイテムを表示します。
存在しない	選択されたフィルターが存在しないアイテムを表示します。
次の値に等しい	フィルター値に一致するアイテムを表示します。
次の値に等しくない	フィルター値を含まないアイテムを表示します。
次の値より大きい **次の値以上**	指定されたフィルター値より大きい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以上]** 演算子を使用します。
次の値より小さい **次の値以下**	指定されたフィルター値より小さい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以下]** 演算子を使用します。

演算子	説明
直近	今日より前の数時間、数日、数か月、または数年以内の日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
後	指定されたフィルター値より後の日付のアイテムを表示します。
前	指定されたフィルター値より前の日付のアイテムを表示します。
経過	今日より前の数時間、数日、数か月、または数年が経過した日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
日付	指定された日付のアイテムを表示します。
期間	指定された 2 つの日付間のアイテムを表示します。
次の値を含む:	指定されたフィルター値を含むアイテムを表示します。
次の値を含まない:	指定されたフィルター値を含まないアイテムを表示します。
ワイルドカード	次のように、ワイルドカード (*) でアイテムを絞り込みます。 • **次で始まるまたは終わる** - 指定したテキストで始まるまたは終わる値を表示します。たとえば、「1」で始まるすべての値を見つけるには、*1** と入力します。「1」で終わるすべての値を見つけるには、**1* と入力します。 • **次の値を含む** - 指定したテキストを含む値を表示します。たとえば、最初と最後の文字の間のどこかに「1」があるすべての値を見つける場合は、**1** と入力します。 • **大文字と小文字の区別をオフにする** - 大文字と小文字を区別せずに値を表示します。たとえば、**プラグイン名** が「TLS バージョン 1.2 プロトコル検出」*または*「tls バージョン 1.2 プロトコル検出」である検出結果を検索するには、**tls バージョン 1.2 プロトコル検出* と入力します。

演算子の右側にフィルターの値を選択または入力します。

> **ヒント:** 一部のテキストフィルターは、フィルター値内のテキストのセクションを表すワイルドカードとして文字 (*) をサポートしています。たとえば、フィルターして 1 で終わるすべての値を表示する場合は、*1 と入力します。フィルターして 1 で始まるすべての値を表示する場合は、1* と入力します。
>
> ワイルドカード演算子を使用して、特定のテキストを含む値を表示することができます。たとえば、最初と最後の文字の間のどこかに 1 があるすべての値を表示するようにフィルターを掛ける場合は、*1* と入力します。

e. (オプション) 複数のタグのルールを作成する方法

i. **Space** キーを押します。

修飾子ドロップダウンボックスが開き、**AND And** と **OR Or** がオプションとして表示されます。

ii. 修飾子を選択します。

iii. **Space** キーを押します。

ドロップダウンボックスが開き、タグルールフィルターオプションが一覧表示されます。

iv. **[詳細]** モードでタグルールを作成する手順を繰り返します。

7. **[保存]** をクリックします。

Tenable Web App Scanning が、ルールを作成してタグに適用します。

タグルールの編集

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

自動タグを作成した後、**[値の編集]** ページでタグに適用するルールを編集できます。

注意: [タグ付け] ページでルールを編集する場合は、汎用資産フィルターのリストから選択してタグルールを作成できます。ただし、特定の資産タイプ (ウェブアプリケーション資産など) に固有のフィルターを追加する場合、Tenable では、**[資産]** ページでタグを編集することを推奨しています。[資産] ページでは、各資産タイプに固有のフィルターを選択できます。

始める前に

- 自動タグを作成します。

タグルールを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[値]** タブをクリックします。

   [値] ページが開き、Tenable Web App Scanning インスタンス上のすべてのタグの表が表示されます。

5. タグの表で、タグルールを編集するタグをクリックします。

   [値の編集] ページが表示されます。

ヒント: [値] 表で確認するタグをクリックすれば、[カテゴリの編集] ページから [値の編集] ページに移動することもできます。

6. ルールの設定を有効にするには、**[ルール]** トグルをクリックします。

   [ルール] セクションが表示されます。

7. **[ルール]** セクションで、編集するルールフィルターにある ⌄ ボタンをクリックします。

   ドロップダウンボックスが表示され、そのフィルターに対して以前に選択したルール値の一覧が表示されます。

   注意: 1 つのタグルールに適用できるフィルターは最大 10 個です。

8. (オプション) 1 つ目のドロップダウンボックスで、新しい演算子を選択します。

9. (オプション) 2 つ目のボックスで、ルール値を追加または削除します。

   注意: ルールフィルターに選択可能なオプション (日付範囲など) がある場合は、それらのオプションがフィルターの下に表示されます。そうでない場合は、値を入力する必要があります。

10. ルールドロップダウンボックスの外側をクリックします。

    ドロップダウンボックスが閉じられます。

11. **[保存]** をクリックします。

    Tenable Web App Scanning が、変更内容を保存して、既存の資産を評価し、更新されたタグルールに一致する資産にタグを自動的に適用します。

    注意: システムの負荷や資産の数によっては、Tenable Web App Scanning が資産にタグを適用し、資産属性を更新するのに時間を要する場合があります。

タグルールの削除

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

自動タグから 1 つのルールが削除されると、Tenable Web App Scanning はそのタグルールに一致するすべての資産からそのタグを削除します。自動タグからすべてのルールを削除すると、そのタグは手動タグになります。

タグルールを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[タグ]** ページで、**[値]** タブをクリックします。

   [値] ページが開き、Tenable Web App Scanning インスタンス上のすべてのタグを含む表が表示されます。

5. タグの表で、タグルールを削除するタグをクリックします。

   [値の編集] ページが表示されます。

   > **ヒント:** **[値]** 表で確認するタグをクリックすれば、**[カテゴリの編集]** ページから **[値の編集]** ページに移動することもできます。

6. **[ルール]** セクションで、削除するルールの ✕ ボタンをクリックします。

   ルールが **[ルール]** セクションに表示されなくなります。

7. **[保存]**をクリックします。

   Tenable Web App Scanning が変更を保存して適用します。

タグルールフィルター

注意: タグルールに誤字が含まれていた場合は、問題について説明したエラーが **[ルール]** ボックスに表示されます。

注意: Tenable Web App Scanning は、タグごとに最大 1,000 のルールをサポートします。この制限は、1 つのタグ値に対して最大 1,000 個の **and** または **or** 条件を指定できることを意味します。さらに、Tenable Web App Scanning は、個別のタグルールごとに最大 1,024 個の値をサポートします。

[タグ] ページで、以下のフィルターから選択して自動タグのルールを作成できます。

フィルター	説明
アカウント ID	資産をホストするクラウドサービスの資産リソースに割り当てられた一意の識別子。
ACR	(Tenable Lumin ライセンスが必要) 資産の ACR (資産重大度の格付け) です。
ACR 深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された ACR の ACR カテゴリ。
AES	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES (資産のエクスポージャースコア)。
AES の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES の AES カテゴリ。
エージェント名	資産をスキャンして特定した、Tenable Nessus エージェントの名前。
ARN	資産の Amazon リソース名 (ARN)。
ASN	資産の自律システム番号 (ASN)。
[評価済み] と [検出済み]	Tenable Web App Scanning が資産の脆弱性をスキャンしたかどうか、または Tenable Web App Scanning が検出スキャンで資産を検出しただけかどうかを指定します。可能な値は次のとおりです。 • **評価済み** • **検出済みのみ**

資産 ID	資産の UUID。
AWS 可用性ゾーン	AWS が仮想マシンインスタンスをホストしているアベイラビリティゾーンの名前。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS EC2 AMI ID	Amazon Elastic Compute Cloud (Amazon EC2) での、Linux AMI イメージの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 インスタンス ID	Amazon EC2 での Linux インスタンスの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 名	Amazon EC2 での仮想マシンインスタンスの名前。
AWS EC2 製品コード	Amazon EC2 での仮想マシンインスタンスの立ち上げに使用された AMI に関連付けられた製品コード。
AWS インスタンスの状態	AWS での仮想マシンインスタンスのスキャン時の状態。可能な値については、Amazon Elastic Compute Cloud ドキュメントの API インスタンスの状態を参照してください。
AWS インスタンスタイプ	Amazon EC2 での仮想マシンインスタンスのタイプ。Amazon EC2 のインスタンスタイプは、インスタンスの仕様を決定します (たとえば、どのくらいの RAM を持つか)。可能な値の一覧は、AWS ドキュメントの Amazon EC2 インスタンスタイプを参照してください。
AWS 所有者 ID	仮想マシンインスタンスを作成した Amazon AWS アカウントの UUID。詳細は、AWS ドキュメントの AWS アカウント ID を参照してください。 この属性は、Amazon EC2 インスタンスのみに対して値を持ちます。他の資産タイプに対しては、この属性は空となります。
AWS リージョン	たとえば `us-east-1` などの、AWS が仮想マシンインスタンスをホストするリージョン。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS セキュリティグループ	Amazon EC2 インスタンスに関連付けられた AWS セキュリティグループ (SG)。

AWS サブネット ID	スキャン時に仮想マシンインスタンスが動作していた、AWS サブネットの固有識別子。
AWS VPC ID	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、Amazon Virtual Private Cloud ユーザーガイドを参照してください。
Azure リソースグループ	Azure Resource Manager でのリソースグループの名前。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソース ID	Azure Resource Manager での、リソースの固有識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソースタイプ	Azure Resource Manager でのリソースのリソースタイプ。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure サブスクリプション ID	Azure Resource Manager でのリソースの固有サブスクリプション識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure VM ID	Microsoft Azure 仮想マシンインスタンスの固有識別子。詳細は、Microsoft Azure ドキュメントの Azure VM Unique ID のアクセスと使用を参照してください。
BIOS ID	資産の NetBIOS 名。
クラウドプロバイダー	資産をホストするクラウドプロバイダーの名前。
作成日	Tenable Web App Scanning が資産レコードを作成した日時。
カスタム属性	カテゴリと値のペアを使用してカスタム属性を検索するフィルター。カスタム属性の詳細については、Tenable 開発者ポータルを参照してください。
削除	資産が削除済みかどうかを指定します。
Deleted Date	ユーザーが資産レコードを削除した日付、またはユーザーが資産を削除してからの日数。ユーザーが資産レコードを削除した場合、Tenable Web App Scanning は資産のライセンスカウントが期限切れとなるまで、そのレコードを保持します。
DNS (FQDN)	資産ホストの完全修飾ドメイン名。 **注意:** これは、**[名前]** フィルターを使用する必要があるウェブアプリケーション資

	産には適用されません。
ドメイン	ソースとして追加されたドメイン、またはアタックサーフェス管理によってユーザーに属するものとして検出されたドメイン。
初回確認日	スキャンが最初に資産を特定した日時。
Google Cloud インスタンス ID	Google Cloud Platform (GCP) での、仮想マシンインスタンスの固有識別子。
Google Cloud プロジェクト ID	GCP で、仮想マシンインスタンスが所属するプロジェクトのカスタマイズされた名前。詳細は、GCP ドキュメントのプロジェクトの作成と管理を参照してください。
Google Cloud ゾーン	GCP で、仮想マシンインスタンスが動作しているゾーン。詳細は、GCP ドキュメントのリージョンとゾーンを参照してください。
プラグインの結果有り	資産が関連付けられたプラグイン結果を持つかどうかを指定します。
ホスト名 (ドメインインベントリ)	アタックサーフェス管理スキャン中に検出された資産のホスト名。ドメインインベントリ資産でのみ使用されます。
ホスティングプロバイダー	資産のホスティングプロバイダー。
IaC リソースタイプ	資産のインフラのコード化 (IAC) リソースタイプ。
インストール済みのソフトウェア	スキャンにより資産上に存在が確認されたソフトウェアアプリケーションを表す、共通プラットフォーム一覧 (CPE) の値。このフィールドは CPE 2.2 形式に対応します。詳細は、CPE 仕様書バージョン 2.2 の Component Syntax セクションを参照してください。Tenable スキャンで特定された資産に関して、このフィールドは、Tenable Nessus プラグイン ID 45590 を使用するスキャンが資産を評価した場合にのみ値を持ちます。 **注意:** アプリケーションが検出された最初のスキャンから 30 日の間に、そのアプリケーションを検出するスキャンがなかった場合、Tenable Web App Scanning はそのアプリケーションの検出を期限切れとみなします。その結果、次にその資産をスキャンで評価する際、Tenable Web App Scanning は期限切れとなったアプリケーションを **[インストール済みソフトウェア]** 属性から削除します。このアクティビティは、削除の種類の属性変更として資産アクティビティログに記録されま

	す。
IPv4 アドレス	資産レコードに関連付けられた IPv4 アドレスです。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します (例: hostname_example, example.com, 192.168.0.0)。IP アドレスには、個別のアドレス、CIDR 表記 (例: 192.168.0.0/24)、または範囲 (例: 192.168.0.1-192.168.0.255) を指定できます。 **注意:** CIDR マスクの /0 はすべての IP アドレスに適合するため、このパラメーターではサポートされていません。このパラメーターに値 /0 を指定すると、Tenable Web App Scanning は 400 Bad Request エラーメッセージを返します。 **注意:** タグフィルターの値が終止符 (.) で終わらないようにしてください。
IPv6 アドレス	スキャンにより資産レコードと関連付けられた IPv6 アドレス。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します。IPV6 アドレスは完全に一致する必要があります (例: 0:0:0:0:0:ffff:c0a8:0)。 **注意:** タグフィルターの値が終止符 (.) で終わらないようにしてください。
属性	資産が属性であるかどうかを指定します。
自動スケール	資産を自動的にスケーリングするかどうかを指定します。
サポートなし	Tenable Web App Scanning で資産がサポートされていないかどうかを指定します。
最終監査日	資産が最後に監査された日時。
最終認証スキャン日	資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。
最終ライセンススキャン日	資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証ス

	キャンでは、**[最終ライセンススキャン日]**フィールドは更新されますが、**[最終認証スキャン日]**フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management Licensesを参照してください。
最終確認日	資産を特定した直近のスキャンの日時。
ライセンス済み	資産がTenable Web App Scanningインスタンスの資産カウントに含まれるかどうかを規定します。
MACアドレス	スキャンにより資産レコードと関連付けられたMACアドレス。
最後に検出された緩和策	資産の軽減ソフトウェアを識別した直近のスキャン日時。
名前	特定の資産属性の存在に基づいてTenable Web App Scanningによって次の順序で割り当てられる資産識別子です。 1. エージェント名(エージェントスキャンの場合) 2. NetBIOS名 3. FQDN 4. IPv6アドレス 5. IPv4アドレス たとえばスキャンによって、ある資産に対してNetBIOS名とIPv4アドレスが特定された場合、NetBIOS名が資産名として表示されます。
NetBIOS名	資産のNetBIOS名。
ネットワーク	資産を特定したスキャナーに関連付けられているネットワークオブジェクトの名前。デフォルトの名前は**Default**です。詳細は、Networksを参照してください。
開いているポート	資産のポートを開きます。
オペレーティングシステム	スキャンにより資産にインストールされていると特定されたオペレーティングシステム。
ポート	資産に関連付けられているポート。

パブリック	資産がパブリックネットワークで使用可能かどうかを指定します。
レコードタイプ	資産タイプ。
リージョン	資産が実行されるクラウドリージョン。
リポジトリ	資産に関連付けられているコードリポジトリ。
リソースカテゴリ	クラウドリソースタイプが属するカテゴリの名前 (オブジェクトストレージや仮想ネットワークなど)。
リソースタグ (キー別)	Amazon Web Services (AWS) などのクラウドソースから同期された、タグキー (Name など) と一致するタグ。
リソースタグ (値別)	Amazon Web Services (AWS) などのクラウドソースから同期された、タグ値と一致するタグ。
リソースタイプ	資産のクラウドリソースタイプ (ネットワーク、仮想マシンなど)。
ServiceNow Sys ID	該当する場合、ServiceNow での資産の固有レコード識別子。詳細は、ServiceNow のドキュメントを参照してください。
ソース	資産を特定したスキャンのソース。可能なフィルター値は次のとおりです。 • AWS • AWS FA • Azure • AZURE FA • Cloud Connector • Cloud IAC • クラウドランタイム • GCP • Nessus Agent • Nessus Scan • NNM

	• ServiceNow • WAS
SSL/TLS	資産がホストされているアプリケーションが SSL/TLS 公開鍵暗号化を使用するかどうかを指定します。
システムの種類	プラグイン ID 54615 によりレポートされたシステムの種類。詳細は、Tenable プラグインを参照してください。
タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。
ターゲットグループ	資産が所属するターゲットグループ。資産がターゲットグループに所属していない場合、この属性は空になります。詳細は、ターゲットグループを参照してください。
Tenable ID	資産に存在するエージェントの UUID。
終了	資産が終了しているかどうかを指定します。
タイプ	資産が管理されているシステムのタイプ。可能なフィルター値は次のとおりです。 • **クラウドリソース** • **コンテナ** • **ホスト** • **クラウド**
更新日	ユーザーが資産を最後に更新した日時。

VPC	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、Amazon Virtual Private Cloud ユーザーガイドを参照してください。

資産フィルターを使用したタグの作成

必要なユーザーロール: 管理者

資産をフィルタリングする時に、フィルターをタグルールとして使用して、新しい自動タグを作成できます。

タグを作成すると、Tenable Web App Scanning はそれらのフィルターで特定された資産にタグを自動的に適用します。

[タグ付け] ページから資産の手動タグまたは自動タグを作成することもできます。

資産フィルターを使用してタグを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

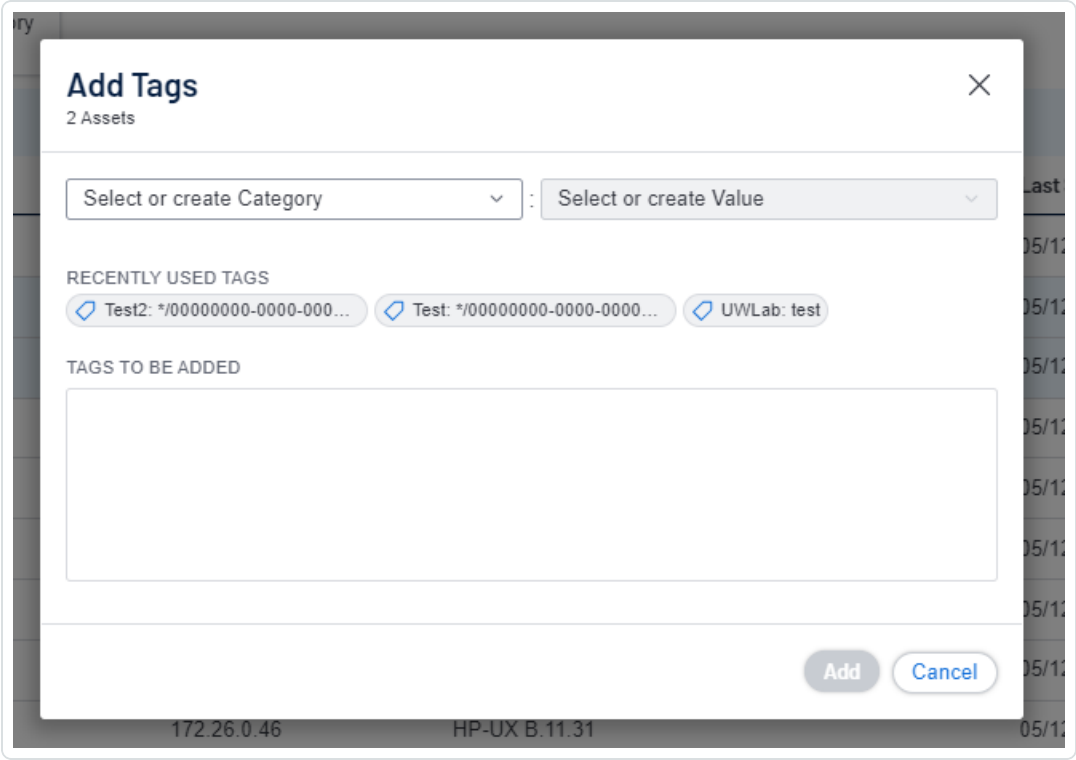
   [資産] ページが表示されます。

3. 表をフィルタリングします。この時、タグに追加またはタグから削除するルールに応じて、フィルターを選択および選択解除します。

   選択したフィルターは、フィルター画面の上にあるヘッダーに表示されます。

4. ヘッダーで、最初のフィルターの左側にある 🏷 **[タグの追加]** ボタンをクリックします。

   [タグの追加] ウィンドウが表示されます。



5. **[タグの作成 / 選択]** の最初のドロップダウンボックスにカテゴリを入力します。

   入力に伴って、リストでは一致が絞り込まれます。

6. ドロップダウンボックスから既存のカテゴリを選択するか、カテゴリを新規作成する場合は [***"カテゴリ"*** **の作成**] をクリックします。

   ヒント: 汎用タグカテゴリを作成してさまざまなタグ値に適用すると、タグをグループ化できます。たとえば、*[場所]* カテゴリを作成し、*Headquarters* や *Offshore* などの複数の値に適用すると、場所タグのグループを作成できます。

7. **[タグの作成 / 選択]** の 2 番目のドロップダウンボックスに新しいタグの値を入力します。

8. ドロップダウンボックスで、**[*"値"* の作成]** をクリックします。

9. **[保存]** をクリックします。

   Tenable Web App Scanning によってタグが保存され、アカウントの該当する資産に適用されます。

   注意: Tenable Web App Scanning が対象の資産にタグを適用するには最大で数分かかる場合があります。

タグまたはタグカテゴリの編集

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

[タグ付け] セクションで、タグの 1 つ以上の設定要素を編集できます。これには、タグが属しているカテゴリ、タグの名前と説明、およびタグに適用されているルールが含まれます。

タグまたはタグカテゴリを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. 個別のタグを編集する方法

   a. **[タグ]** ページで、**[値]** タブをクリックします。

      [値] ページが開き、Tenable Web App Scanning インスタンス上のすべてのタグを含む表が表示されます。

   b. **[値]** 表で、編集するタグをクリックします。

      [値の編集] ページが表示されます。

      > **ヒント:** **[値]** 表で確認するタグをクリックすれば、**[カテゴリの編集]** ページから **[値の編集]** ページに移動することもできます。

   c. (オプション) **[値]** ボックスで、タグ名を編集します。

   d. (オプション) **[値の説明 (オプション)]** ボックスで、タグの説明を編集します。

e. (オプション) タグルールを設定します。

5. タグカテゴリを編集する方法

注意: タグカテゴリを編集すると、Tenable Web App Scanning はそのタグカテゴリ内のすべてのタグのカテゴリを変更します。

a. タグカテゴリの表で、編集するカテゴリをクリックします。

[カテゴリの編集] ページが表示されます。

b. タグカテゴリの表で、編集するカテゴリをクリックします。

[カテゴリの編集] ページが表示されます。

c. (オプション) 名前を編集するには、**[カテゴリ]** ボックスに新しい名前を入力します。

d. (オプション) 説明を編集するには、**[カテゴリの説明]** ボックスに新しい説明を入力します。

6. **[保存]** をクリックします。

Tenable Web App Scanning が変更を保存して適用します。

資産フィルターを使用したタグの編集

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

[資産] ページでは、資産フィルターを使用してタグのルール、カテゴリ、値を編集できます。

資産フィルターを使用してタグを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

3. 表をフィルタリングします。この時、タグに追加またはタグから削除するルールに応じて、フィルターを選択および選択解除します。

   適用したフィルターは、フィルター画面の上にあるヘッダーに表示されます。

4. ヘッダーで、最初のフィルターの左側にある ◇ ボタンをクリックします。

   [資産と一致するタグ] ウィンドウが表示されます。

5. 次のいずれかを行います。

   - 最後に使用したタグを編集する場合

     a. **[最近使用したタグ]** で、編集するタグをクリックします。

     タグカテゴリが **[カテゴリを選択または作成する]** ドロップダウンボックスに表示されます。

     タグの値が **[値を選択または作成する]** ドロップダウンボックスに表示されます。

   - 他のタグを編集する場合

a. **[カテゴリを選択または作成する]**ドロップダウンボックスにカテゴリ名を入力します。

入力に伴って、リストでは一致が絞り込まれます。

b. 編集するタグのカテゴリを選択します。

c. **[値を選択または作成する]**ドロップダウンボックスに値名を入力します。

入力に伴って、リストでは一致が絞り込まれます。

d. ドロップダウンボックスから編集するタグの値を選択します。

6. (オプション) タグカテゴリを編集する方法

a. **[カテゴリを選択または作成する]**ドロップダウンボックスにカテゴリの新しい名前を入力します。ドロップダウンボックスに

["*カテゴリ*" の作成] が表示されます。

b. ドロップダウンボックスから **["*カテゴリ*" の作成]** を選択します。

ドロップダウンボックスに新しいカテゴリ名が選択された状態で表示されます。

7. (オプション) タグの値を編集する方法

a. **[値を選択または作成する]**ドロップダウンボックスにタグの新しい値を入力します。ドロップダウンボックスに

["*値*" の作成] が表示されます。

b. ドロップダウンボックスから **["*値*" の作成]** を選択します。

ドロップダウンボックスに新しい値名が選択された状態で表示されます。

8. (オプション) **[タグ用の選択した検索フィルター]** ボックスで、タグから削除するフィルター内にある ✕ をクリックします。

9. **[保存]** をクリックします。

Tenable Web App Scanning で編集が保存されます。

タグの資産への追加

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する使用可アクセス許可

タグを作成すると、Tenable Web App Scanning インスタンスの 1 つ以上の資産に手動で適用できます。

タグを資産に追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

3. 資産リストを表示します。

4. (オプション) 表データを選別します。詳細は、Tenable Web App Scanning ワークベンチの表 を参照してください。

5. 次のいずれかを行います。

   ### 1 つの資産にタグを追加する方法

a. タグを追加するページを選択します。

場所	アクション
[資産] ページ	**[資産]** ページからタグを追加する方法 a. 資産の表で、タグを追加する資産の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 資産の表の **[アクション]** 列で、タグを追加する資産の ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[タグの追加]** をクリックします。
[資産の詳細] ページプレビュー画面	**[資産の詳細]** ページからタグを追加する方法 a. 資産の表で、タグを追加する資産の行をクリックします。 資産の **[資産の詳細]** ページのプレビュー画面が表示されます。 b. プレビュー画面の左側の **[タグ]** の横にある ⊕ ボタンをクリックします。
[資産の詳細] ページ	**[資産の詳細]** ページからタグを追加する方法 a. タグを削除する資産の **[資産の詳細]** ページを表示します。 **[資産の詳細]** ページが表示されます。 b. 右上の **[アクション]** ボタンをクリックします。

	アクションメニューが表示されます。 c. アクションメニューで、[**タグの追加**] をクリックします。 -または- ページの左側の **[タグ]** の横にある ⊕ ボタンをクリックします。

[タグの追加] ウィンドウが表示されます。

b. **[追加]** をクリックします。

資産の表が表示されます。確認のメッセージが表示されます。Tenable Web App Scanning は、資産に **[追加予定のタグ]** で指定されたタグを追加します。

複数の資産にタグを追加する場合

a. 資産の表で、タグを追加する各資産のチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. **[タグの追加]** をクリックします。

資産の表が表示されます。確認のメッセージが表示されます。Tenable Web App Scanning は、資産に **[追加予定のタグ]** で指定されたタグを追加します。

6. 次のいずれかを行います。

最後に使用したタグを追加する場合

- **[最近使用したタグ]** で、追加するタグを選択します。

タグが **[追加予定のタグ]** ボックスに表示されます。

> **ヒント: [追加予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせて ✕ ボタンをクリックします。

新しいタグまたは既存のタグを追加する場合

a. **[カテゴリ]** ボックスに、カテゴリを入力します。

入力に伴って、リストでは一致が絞り込まれます。

b. ドロップダウンボックスから既存のカテゴリを選択するか、新しいカテゴリの場合は **["*カテゴリ名*" の作成]** をクリックします。

> **ヒント:** 汎用タグカテゴリを作成してさまざまなタグ値に適用すると、タグをグループ化できます。たとえば、*[場所]* カテゴリを作成し、*Headquarters* や *Offshore* などの複数の値に適用すると、場所タグのグループを作成できます。

c. **[値]** ボックスに値を入力します。

入力に伴って、リストでは一致が絞り込まれます。

d. ドロップダウンボックスから既存の値を選択するか、値を新規作成する場合は **["*値*" の作成]** をクリックします。

> **注意:** この方法で新しいタグを作成した場合、その新しいタグは資産に追加するまで保存されません。

タグが **[追加予定のタグ]** ボックスに表示されます。

> **ヒント:** **[追加予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせて ✕ ボタンをクリックします。

7. **[追加]** をクリックします。

資産の表が表示されます。確認のメッセージが表示されます。Tenable Web App Scanning は、資産に **[追加予定のタグ]** で指定されたタグを追加します。

資産ビューを介して資産からタグを削除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要なアクセスグループのアクセス許可: 表示可、編集可

この手順では、**[資産]** ページの資産からタグを削除する方法を説明します。**[資産別の脆弱性]** ページから資産タグを削除することもできます。

資産が動的タグのルールに一致してもタグを適用したくない場合は、資産からタグを手動で削除できます。後でタグを資産に再適用する場合は、タグルールの編集の説明に従って、除外資産リストから資産を削除できます。

1 つの資産からタグを削除する場合

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[資産ビュー]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。

3. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

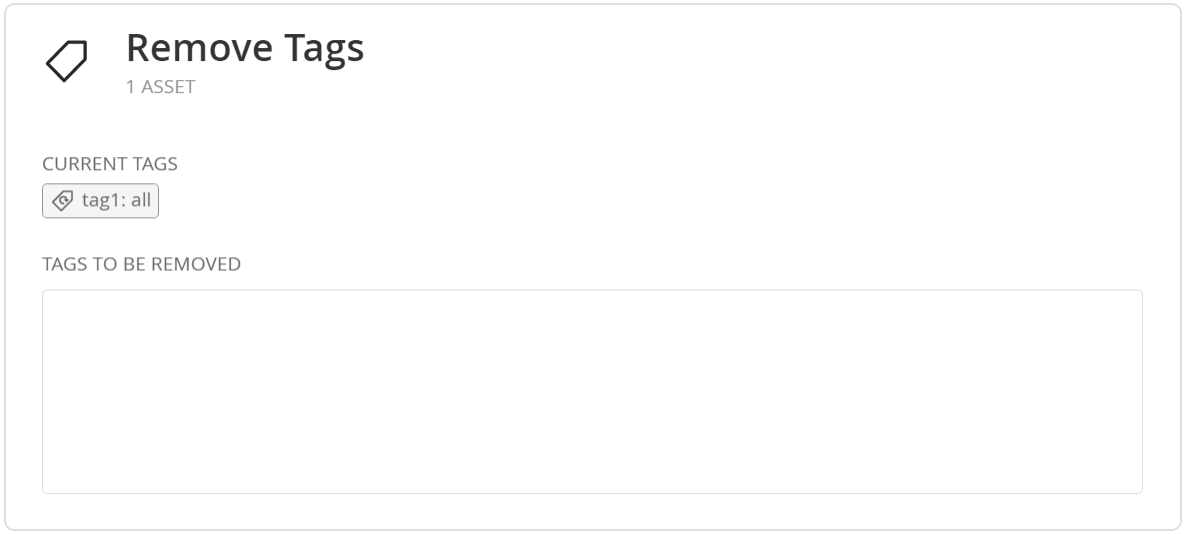
   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

4. 次のいずれかを行います。

場所	アクション
[資産] ページ	a. 資産の表のタグを削除する資産の行で、⋮ ボタンをクリックします。 メニューが表示されます。 b. **[タグの削除]** をクリックします。
[資産] ページ	a. 資産の表で、タグを削除する各資産のチェックボックスを選択します。 ページの下部またはテーブルの上部に、アクションバーが表示され

	ます。 b. アクションバーで、 **[タグの削除]** をクリックします。
[資産の詳細] ページ	a. 資産の表で、タグを削除する資産をクリックします。 **[資産の詳細]** ページが表示されます。 b. 右側のパネルの **[タグ]** セクションで、資産から削除するタグの名前をクリックします。 メニューが表示されます。 c. **[タグの削除]** をクリックします。

[タグの削除] プレーンが表示されます。



5. **[現在のタグ]** で、削除する各タグをクリックします。

   タグが **[削除予定のタグ]** ボックスに表示されます。

   ヒント: [削除予定のタグ] からタグを削除するには、そのタグにカーソルを合わせ、× ボタンをクリックします。

6. **[削除]** をクリックします。

   Tenable Vulnerability Management により、資産から **[削除予定のタグ]** で指定されたタグが削除されます。

複数の資産からタグを削除する場合

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[資産ビュー]** セクションで、**[資産]** をクリックします。

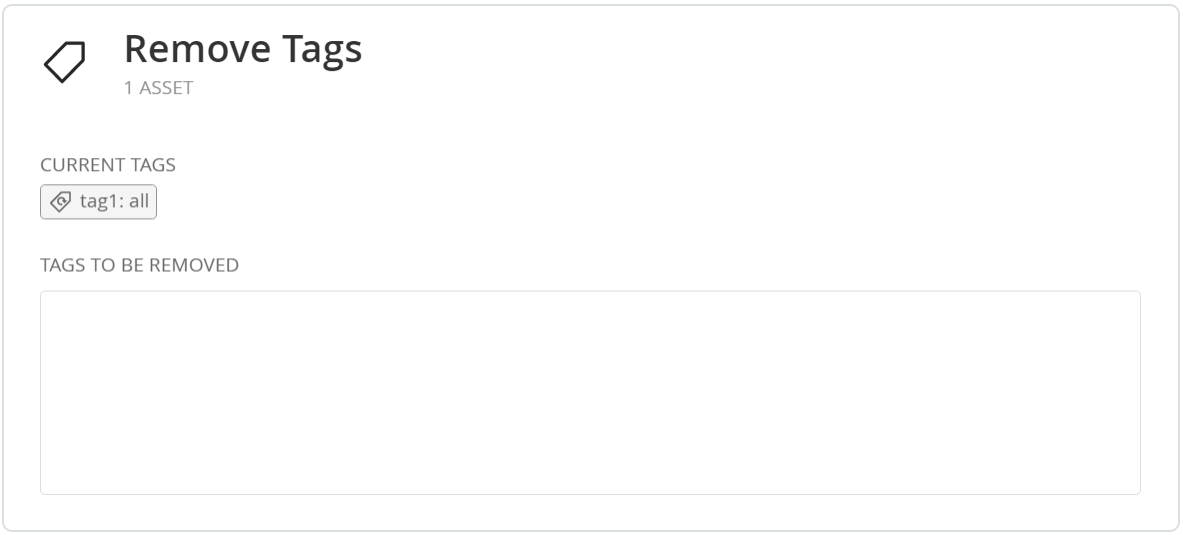
   [資産] ページが表示されます。

3. 資産の表で、タグを削除する各資産の横にあるチェックボックスをクリックします。

   ページの下部またはテーブルの上部に、アクションバーが表示されます。

4. アクションバーで、**[タグの削除]** をクリックします。

   [タグの削除] プレーンが表示されます。



5. **[現在のタグ]** で、削除する各タグをクリックします。

   タグが **[削除予定のタグ]** ボックスに表示されます。

   > **ヒント: [削除予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせ、✕ ボタンをクリックします。

6. **[削除]** をクリックします。

   Tenable Web App Scanning により、選択した資産から **[削除予定のタグ]** で指定されたタグが削除されます。

タグによる資産属性のオーバーライド

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

手動または自動で適用されるようにタグを編集する場合、そのタグが付いたすべての資産に対して Tenable Vulnerability Management が上書きする資産属性を指定することができます。

たとえば、ACR 属性を選択して、タグが付いたすべての資産の特定の ACR 値を一括変更できます。

ヒント: ACR の優先順位付けについては、タグによる資産属性のオーバーライドを参照してください。

新しいインターフェースでタグを使用して資産属性をオーバーライドする方法

1. タグの作成を開始します。
2. このタグが付いたすべての資産の属性を自動的にオーバーライドするには、属性を編集します。
    a. **[属性オーバーライド]** トグルをクリックして、このタグを持つ資産への属性の自動適用を有効にします。

    基準ボックスが表示されます。

    b. 最初のボックスで、属性を選択します (例: **ACR (資産重大度の格付け) (ACR)**)。

    c. 2 番目のボックスで、値を選択します (例: **9 (重大)**)。
3. **[保存]** をクリックします。

    タグが付いたすべての資産の属性が Tenable Vulnerability Management によって更新されます。

    注意: タグを介して資産属性をオーバーライドする場合、システムの負荷や資産の数によっては、Tenable Vulnerability Management がタグが付いた資産の属性を更新するのに時間を要する場合があります。

    ヒント: タグ更新済みの ACR 値に対して Tenable Vulnerability Management が優先度を付ける方法についての詳細は、ACR (資産重大度の格付け) (ACR)を参照してください。

タグのエクスポート

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

[タグ] ページでは、タグのカテゴリと値を CSV または JSON 形式でエクスポートできます。

タグのカテゴリや値をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. (オプション) 表データを選別します。詳細は、Tenable Web App Scanning ワークベンチの表 を参照してください。

   注意: **[タグ]** ページの表をフィルタリングすることはできません。

5. 次のいずれかを行います。

   タグカテゴリをエクスポートする場合

a. エクスポートするタグカテゴリを選択します。

エクスポート範囲	アクション
選択したタグカテゴリ	選択したタグカテゴリをエクスポートする方法 a. カテゴリの表で、エクスポートする各タグカテゴリのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のタグカテゴリをエクスポートする場合は、リストにあるすべてのタグカテゴリを選択して、[→ **[エクスポート]** をクリックします。
1 つのタグカテゴリ	1 つのタグカテゴリをエクスポートする方法 a. カテゴリの表で、エクスポートするタグカテゴリの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- カテゴリの表の **[アクション]** 列で、エクスポートするタグカテゴリの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[エクスポート]** をクリックします。

タグ値をエクスポートする場合

a. **[値]** タブをクリックします。

[値] タブが表示されます。このタブは、すべてのタグ値を含む表があります。

b. エクスポートするタグ値を選択します。

エクスポート範囲	アクション
選択したタグ値	選択したタグ値をエクスポートする方法 a. 値の表で、エクスポートする各タグ値のチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のタグ値をエクスポートする場合は、リストにあるすべてのタグ値を選択して、[→ **[エクスポート]** をクリックします。
1 つのタグ値	1 つのタグ値をエクスポートする方法 a. カテゴリの表で、エクスポートするタグ値の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 値の表の **[アクション]** 列で、エクスポートするタグ値の行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

注意: デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	タグのカテゴリまたは値のリストを含む CSV テキストファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	タグのカテゴリまたは値がネストされたリストを含む JSON ファイル。 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

> **注意**: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。
    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。

- **[繰り返し終了]**ドロップダウンで、スケジュールが終了する日付を選択します。

  注意: [無し]を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]**トグルをクリックします。

      [メール通知]セクションが表示されます。

    - **[受信者の追加]**ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須)**[パスワード]**ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      注意: Tenable Web App Scanning がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]**をクリックします。

    Tenable Web App Scanning がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Web App Scanning によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]**でエクスポートファイルにアクセスできます。

タグカテゴリの削除

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

タグカテゴリを削除すると、Tenable Web App Scanning によりそのカテゴリ下に作成されたタグがすべて削除され、それらのタグが適用されたすべての資産からもそれらのタグが削除されます。

注意: タグカテゴリを削除すると、関連するすべての値と割り当ても削除されます。特定のタグを削除する場合は、タグの削除を参照してください。

タグカテゴリを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[カテゴリ]** タブをクリックします。

   タグカテゴリの表が表示されます。

5. 1 つのタグカテゴリを削除する場合

   a. タグの表の **[アクション]** 列で、⋮ ボタンをクリックします。

      メニューが表示されます。

b. **[削除]** ボタンをクリックします。

確認ウィンドウが開き、カテゴリと関連するすべてのタグと割り当てを削除するかどうかを確認するメッセージが表示されます。

複数のタグカテゴリを削除する場合

a. タグカテゴリの表で、削除する各カテゴリのチェックボックスを選択します。

ページの下部またはテーブルの上部に、アクションバーが表示されます。

b. アクションバーで、**[削除]** ボタンをクリックします。

確認ウィンドウが開き、カテゴリと関連するすべてのタグと割り当てを削除するかどうかを確認するメッセージが表示されます。

6. **[削除]** をクリックします。

Tenable Web App Scanning によりタグカテゴリとそれに関連するすべてのタグが削除され、それらのタグを適用したすべての資産からも削除されます。

タグの削除

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

タグを削除すると、Tenable Web App Scanning はそのタグを適用したすべての資産から、その特定のタグを削除します。

1 つ以上のタグを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. 1 つ以上のタグを削除します。

削除の範囲	アクション
1 つのタグ	1 つのタグを削除する場合 a. **[値]** タブをクリックします。 **[値]** タブが開き、Tenable Web App Scanning インスタンスのすべてのタグを含む表が、*カテゴリ: 値* の形式で表示されます。 b. タグの表で、削除するタグの行を右クリックします。 アクションオプションがカーソルの横に表示されます。

	-または- タグの表の **[アクション]** 列で、削除するタグの ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 c. 🗑 **[削除]** をクリックします。
複数のタグ	複数のタグを削除する場合 a. **[値]** タブをクリックします。 **[値]** タブが開き、Tenable Web App Scanning インスタンスのすべてのタグを含む表が、*カテゴリ: 値* の形式で表示されます。 b. タグの表で、削除する各タグのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 c. アクションバーで、🗑 **[削除]** をクリックします。 -または- タグカテゴリを削除して、カテゴリ内にあるすべてのタグを削除します。

5. **[値]** タブをクリックします。
6. 1つのタグを削除する場合
   a. タグの表で、削除するタグにカーソルを合わせます。
   アクションボタンが行に表示されます。
   b. 🗑 **[削除]** ボタンをクリックします。
   確認ウィンドウが表示されます。

複数のタグを削除する場合

a. タグの表で、削除する各タグのチェックボックスを選択します。
ページの下部またはテーブルの上部に、アクションバーが表示されます。
b. アクションバーで、🗑 **[削除]** ボタンをクリックします。

確認ウィンドウが表示されます。

7. **[確認]**をクリックします。

   Tenable Web App Scanning はそのタグを削除し、そのタグを適用したすべての資産からもそのタグを削除します。

タグの表からタグで資産を検索する

必要な Tenable Vulnerability Management ユーザーロール: VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

タグで資産を検索すると、特定のタグが適用されている資産を確認できます。

タグの表からタグで資産を検索する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[値]** タブをクリックします。

5. 表にある ⋮ ボタンをクリックします。

   アクションメニューが表示されます。

6. 🔎**[タグ別に検索]** をクリックします。

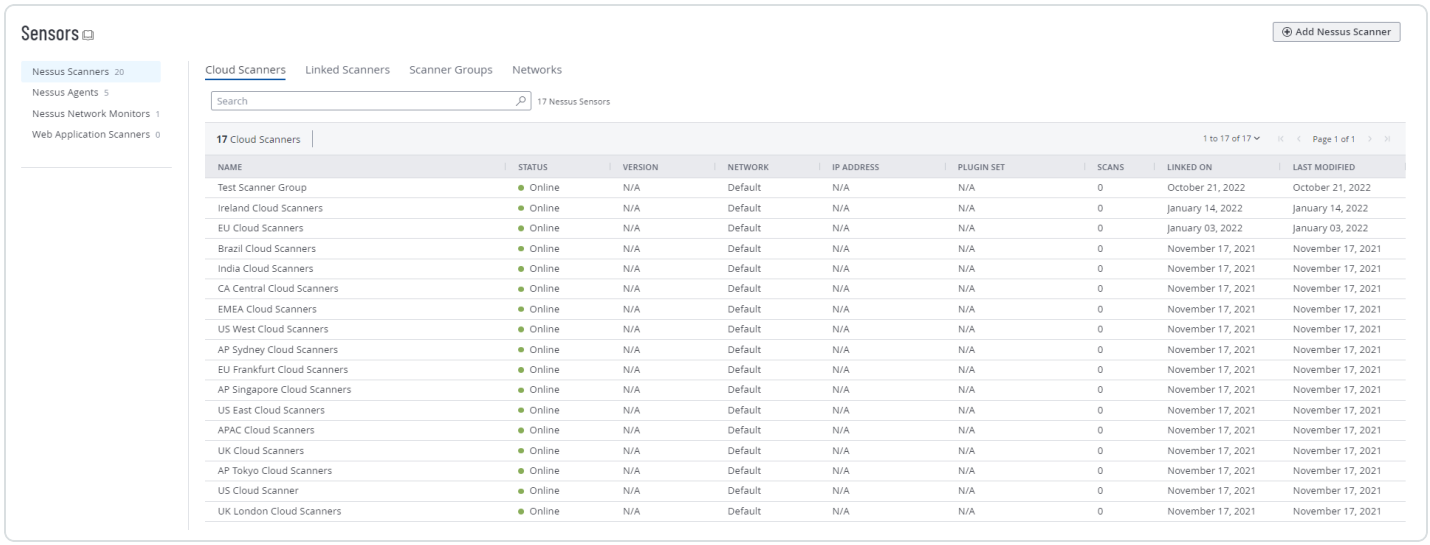
   [**Assets**] ページが表示され、選択したタグでフィルタリングされた資産の表が表示されます。

クラウドセンサー

デフォルトで、Tenable は Tenable Web App Scanning で使用する地域のクラウドセンサーを提供しています。スキャンを作成して起動するときに、これらのセンサーを選択できます。

次の表は、各地域のクラウドセンサーとその IP アドレス範囲 (許可リスト登録用) を示しています。これらの IP アドレス範囲は Tenable専用です。

Tenable Web App Scanning



注意: クラウドコネクタを使用する場合、Tenable はサイトが拠点を置く地域の IP アドレスを許可リストに登録することをお勧めします。

注意: これらの IP アドレスは送信リクエスト用ですが、着信 cloud.tenable.com リクエストにも使用されます。

ヒント: データをプログラムで解析するユーザーのために、下の表のクラウドセンサーと IP アドレスの情報は JSON 形式でも提供されます。

Tenable Attack Surface Management に関連付けられたクラウド IP については、*Tenable Attack Surface Management ユーザーガイド*の Cloud Sensors を参照してください。

センサー地域	IPv4 範囲	IPv6 範囲
ap-northeast-1	13.115.104.128/25 35.73.219.128/25	2406:da14:e76:5b00::/56
ap-southeast-1	13.213.79.0/24	2406:da18:844:7100::/56

センサー地域	IPv4 範囲	IPv6 範囲
	18.139.204.0/25 54.255.254.0/26	
ap-southeast-2	13.210.1.64/26 3.106.118.128/25 3.26.100.0/24	2406:da1c:20f:2f00::/56
ap-south-1	3.108.37.0/24	2406:da1a:5b2:8500::/56
ca-central-1	3.98.92.0/25 35.182.14.64/26	2600:1f11:622:3000::/56
eu-west-1	3.251.224.0/24	2a05:d018:f53:4100::/56
eu-west-2	18.168.180.128/25 18.168.224.128/25 3.9.159.128/25 35.177.219.0/26	2a05:d01c:da5:e800::/56
eu-central-1	18.194.95.64/26 3.124.123.128/25 3.67.7.128/25 54.93.254.128/26	2a05:d014:532:b00::/56
me-central-1	51.112.93.0/24	2406:da17:524:dd00::/56
us-east-1	34.201.223.128/25 44.192.244.0/24 54.175.125.192/26	2600:1f18:614c:8000::/56
us-east-2	13.59.252.0/25 18.116.198.0/24 3.132.217.0/25	2600:1f16:8ca:e900::/56
us-west-1	13.56.21.128/25 3.101.175.0/25 54.219.188.128/26	2600:1f1c:13e:9e00::/56

センサー地域	IPv4 範囲	IPv6 範囲
us-west-2	34.223.64.0/25 35.82.51.128/25 35.86.126.0/24 44.242.181.128/25 35.93.174.0/24	2600:1f14:141:7b00::/56
sa-east-1	15.228.125.0/24	2600:1f1e:9a:ba00::/56
静的	162.159.129.83/32 162.159.130.83/32	2606:4700:7::a29f:8153 2606:4700:7::a29f:8253

ヒント: 内部スキャナーまたはエージェント通信には、以下を追加します。

- 162.159.129.83/32
- 162.159.130.83/32
- 162.159.140.26/32
- 172.66.0.26/32
- 2606:4700:7::1a
- 2a06:98c1:58::1a
- 2606:4700:7::a29f:8153
- 2606:4700:7::a29f:8253
- ワイルドカード文字 (*) 付きの *.cloud.tenable.com として、cloud.tenable.com およびすべてのサブドメイン (sensor.cloud.tenable.com など) を許可してください。

注意: Tenable サポート による Tenable Web App Scanning に関する問題のトラブルシューティングを行う場合、次の IP 範囲を許可リストに追加するよう求められる場合があります。

- 13.59.250.76/32

地域のクラウドセンサーが以下のグループに分かれて表示されます。

- **US East Cloud Scanners**: us-east-1 (バージニア州) または us-east-2 (オハイオ州) 範囲のスキャナーグループ

- **US West Cloud Scanners**: us-west-1 (カリフォルニア州) または us-west-2 (オレゴン州) 範囲のスキャナーグループ
- **AP Singapore Cloud Scanners**: ap-southeast-1 (シンガポール) 範囲のスキャナーグループ
- **AP Sydney Cloud Scanners**: ap-southeast-2 (シドニー) 範囲のスキャナーグループ
- **AP Tokyo Cloud Scanners**: ap-northeast-1 (東京) 範囲のスキャナーグループ
- **CA Central Cloud Scanners**: ca-central-1 (カナダ) 範囲のスキャナーグループ
- **EU Frankfurt Cloud Scanners**: eu-central-1 (フランクフルト) 範囲のスキャナーグループ
- **UK Cloud Scanners**: eu-west-2 (ロンドン) 範囲のスキャナーグループ
- **Brazil Cloud Scanners**: sa-east-1 (サンパウロ) 範囲のスキャナーグループ
- **India Cloud Scanners**: ap-south-1 (ムンバイ) 範囲のスキャナーグループ
- **Amazon GOV-CLOUD**: Federal Risk and Authorization Management Program (FedRAMP) 環境で利用可能なスキャナーグループ
- **US Cloud Scanner**: 次の AWS 範囲のスキャナーグループ
    - us-east-1 (バージニア州)
    - us-east-2 (オハイオ州)
    - us-west-1 (カリフォルニア州)
    - us-west-2 (オレゴン州)
- **APAC Cloud Scanners**: 次の AWS 範囲のスキャナーグループ
    - ap-northeast-1 (東京)
    - ap-southeast-1 (シンガポール)
    - ap-southeast-2 (シドニー)
    - ap-south-1 (ムンバイ)
- **EMEA Cloud Scanners**: 次の AWS 範囲のスキャナーグループ

- eu-west-1 (アイルランド)
- eu-west-2 (ロンドン)
- eu-central-1 (フランクフルト)

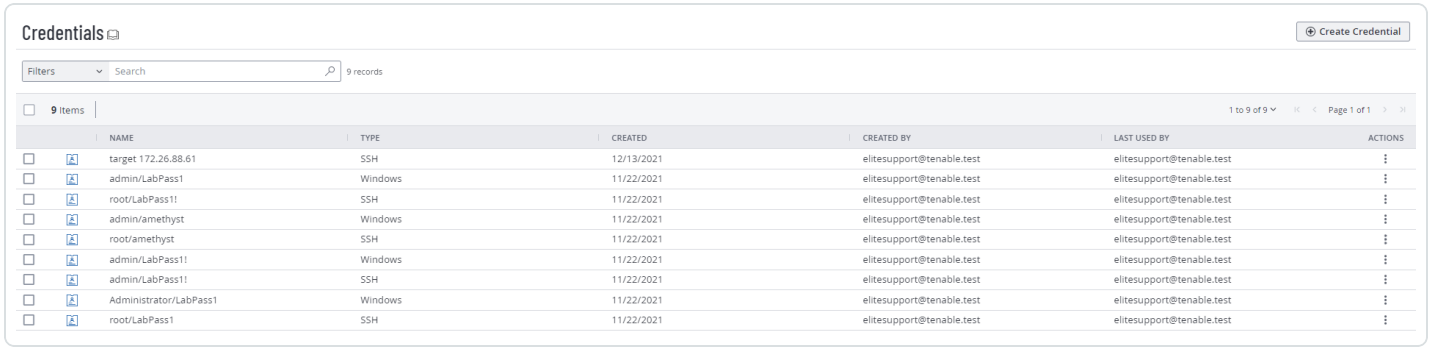
注意： 中国本土にある Tenable Nessus スキャナー、Tenable Nessus Agents、Tenable Web App Scanning スキャナー、または Tenable Nessus Network Monitor (NNM) を介して Tenable Vulnerability Management に接続している場合は、sensor.cloud.tenable.com ではなく sensor.cloud.tenablecloud.cn で接続する必要があります。

認証情報

注意: このセクションでは、管理された認証情報を作成し維持する方法を説明します。スキャン固有またはポリシー固有の認証情報の詳細は、Credentials in Tenable Vulnerability Management Scans またはTenable Web App Scanning スキャンの認証情報を参照してください。

管理された認証情報によって、認証情報の設定を認証マネージャーで一元的に保存できます。その後、これらの認証情報設定を、スキャンごとに認証情報を設定する代わりに、複数のスキャン設定に追加できます。

アクセス許可が付与されたユーザーは、管理された認証情報をスキャンで使用できます。認証情報のユーザーアクセス許可によって、どのユーザーが管理された認証情報を使用し編集できるかが管理されます。



管理された認証情報の作成

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

このトピックでは、管理された認証情報を Tenable Web App Scanning認証マネージャーで作成する方法を説明します。

スキャン固有の認証情報を管理された認証情報に変換するだけでなく、管理された認証情報をスキャン設定中に作成することもできます。詳細については、Add a Credential to a Scan (Tenable Vulnerability Management)または Tenable Web App Scanning で認証情報を設定するを参照してください。

管理された認証情報を作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

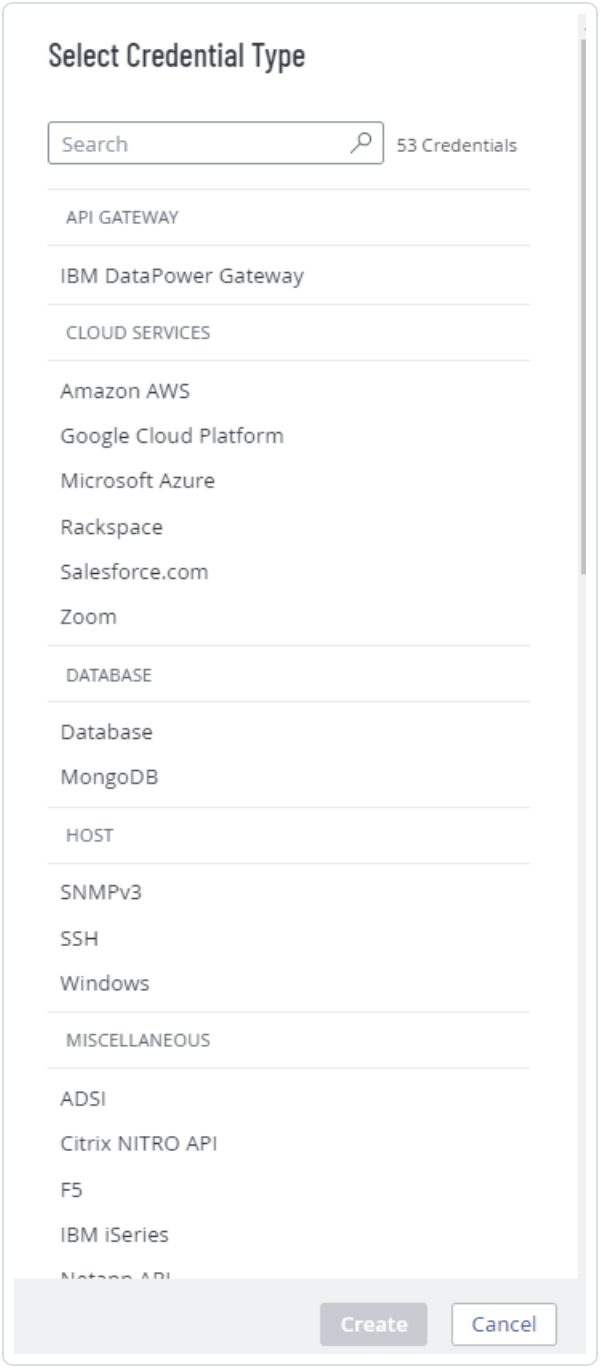
   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. ページの右上にある ⊕ **[認証情報の作成]** ボタンをクリックします。

   [認証情報タイプの選択] プレーンが表示されます。



5. 次のいずれかを行います。

   - 使用できる認証情報タイプのうちいずれかを選択します。
   - カテゴリセクションで認証情報タイプをクリックします。

   認証情報が表示されます。

6. **[タイトル]** ボックスに、認証情報の名前を入力します。

7. (オプション) **[説明]** ボックスに、認証情報の説明を入力します。
8. 選択した認証情報タイプを設定します。

   認証情報設定の詳細については、認証情報 (Tenable Vulnerability Management) または認証情報 (Tenable Web App Scanning) を参照してください。
9. ユーザーアクセス許可を追加します。
10. **[保存]** をクリックします。

    Tenable Web App Scanning は [**Credentials**] ページの認証情報の表に認証情報を追加します。

管理された認証情報を編集する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

このトピックでは、認証情報を Tenable Vulnerability Management認証マネージャーで編集する方法を説明します。

スキャン設定中に管理された認証情報を編集することもできます。詳細については、Tenable Vulnerability Management の場合は認証情報をスキャンに追加する、Tenable Web App Scanning の場合は Tenable Web App Scanning スキャンで認証情報を設定するを参照してください。

編集可 アクセス許可を持つ認証情報を編集できます。

管理された認証情報を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. 編集したい認証情報について、認証情報の表をフィルタリングまたは検索します。詳細は、Tenable Web App Scanning の表 を参照してください。

5. 認証情報の表で、編集する認証情報の名前をクリックします。

   [認証情報設定] プレーンが表示されます。

6. 次のいずれかを行います。

   - 認証情報の名前または説明を編集します。

     a. 名前または説明ボックスの上にカーソルを合わせます。

     b. ボックスの横に表示される ✎ ボタンをクリックします。

     c. 変更を行います。

     d. ボックスの右下にある ✓ ボタンをクリックして、変更内容を保存します。

   - 認証情報タイプの設定を編集します。これらの設定の詳細については、認証情報 (Tenable Vulnerability Management) または認証情報 (Tenable Web App Scanning) を参照してください。

   - 認証情報のユーザーアクセス許可を設定します。

7. **[保存]** をクリックします。

管理された認証情報のユーザーアクセス許可を設定する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

認証情報を使用するスキャンのために設定するアクセス許可とは別に、管理された認証情報のユーザーアクセス許可を設定します。

個別のユーザーまたはユーザーグループに対して認証情報のアクセス許可を設定できます。グループに対して認証情報のアクセス許可を設定する場合、グループ内のすべてのユーザーに同じアクセス許可を割り当てます。認証情報を管理するユーザーのグループを作成することで、認証情報のマネージャーロールと同等のアクセス許可を作成することもできます。詳細は、ユーザーグループを参照してください。

管理された認証情報を作成する場合、Tenable Web App Scanning は自動的に**[編集可]**アクセス許可を割り当てます。

管理された認証情報のユーザーアクセス許可を設定する方法

1. 管理された認証情報を作成または編集します。

場所	アクション
認証マネージャー内	作成または編集
スキャン設定内	作成または編集

2. 次のいずれかを行います。

- ユーザーまたはユーザーグループのアクセス許可を追加する

ヒント: 個別のユーザーは企業を離れたり企業に加わったりすることがあるので、Tenable では、個別のユーザーではなくユーザーグループにアクセス許可を割り当てることを推奨します。

a. [認証情報設定]プレーンで、**[ユーザーのアクセス許可]**タイトルの横にある ⊕ ボタンをクリックします。

[ユーザーアクセス許可の追加]設定が表示されます。

b. 検索ボックスで、ユーザーまたはグループの名前を入力します。

入力すると、ユーザーとグループのフィルタリングされたリストが表示されます。

c. 検索結果からユーザーまたはグループを選択します。

d. ユーザーまたはグループのアクセス許可ドロップダウンの横にある ⌄ ボタンをクリックします。

e. アクセス許可レベルを選択します。

- **使用可** - ユーザーは、管理された認証情報の表の認証情報の表示と、スキャンでの認証情報の使用が可能です。
- **編集可** - ユーザーは、認証情報設定の表示と編集、認証情報の削除、スキャンでの認証情報の使用が可能です。

f. **[追加]**をクリックします。

g. **[保存]**をクリックします。

- ユーザーまたはユーザーグループのアクセス許可を編集する

a. [認証情報設定]プレーンの**[ユーザーのアクセス許可]**セクションで、ユーザーまたはグループのアクセス許可ドロップダウンの横にある ⌄ ボタンをクリックします。

b. アクセス許可レベルを選択します。

- **使用可** - ユーザーは、管理された認証情報の表の認証情報の表示と、スキャンでの認証情報の使用が可能です。
- **編集可** - ユーザーは、認証情報設定の表示と編集、認証情報の削除、スキャンでの認証情報の使用が可能です。

c. **[保存]** をクリックします。

- ユーザーグループのアクセス許可を削除する

a. [認証情報設定] プレーンの **[ユーザーのアクセス許可]** セクションで、削除するユーザーまたはグループにカーソルを合わせます。

b. そのユーザーまたはユーザーグループの横にある ✕ ボタンをクリックします。

そのユーザーまたはグループは、**[ユーザーのアクセス許可]** リストから削除されます。

c. **[保存]** をクリックします。

認証情報のエクスポート

必要なユーザーロール: 管理者

[認証情報] ページでは、1 つ以上の管理されている認証情報データをエクスポートできます。

注意: 認証情報データをエクスポートしても、ユーザー名、パスワード、キーなどの認証の詳細はエクスポートに含まれません。

認証情報データをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. (オプション) 表データを選別します。詳細は、Tenable Web App Scanning ワークベンチの表 を参照してください。

5. エクスポートする認証情報を選択します。

エクスポート範囲	アクション
選択した認証情報	選択した認証情報をエクスポートする方法 a. 認証情報の表で、エクスポートする各認証情報のチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。

	注意: [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。 200 個以上の認証情報をエクスポートする場合は、リスト内のすべての認証情報を選択してから、[→ **[エクスポート]** をクリックします。
1 つの認証情報	1 つの認証情報をエクスポートする方法 a. 認証情報の表で、エクスポートする認証情報の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 認証情報の表の **[アクション]** 列で、エクスポートする認証情報の行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. [→ **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	認証情報のリストを含む CSV テキストファイル

	注意: .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Web App Scanning はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされた認証情報のリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Web App Scanning では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Web App Scanning がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Web App Scanning がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Web App Scanning によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Web App Scanning はコンピューターにエクスポートファイルをダウンロードします。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポートプレーンを閉じた場合は、Exportsページからエクスポートファイルにアクセスできます。

管理された認証情報を削除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、VM スキャンオペレーター、VM 標準、VM スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

編集可 アクセス許可を持つ認証情報を削除できます。

管理された認証情報を削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. 削除したい認証情報について、認証情報の表をフィルタリングまたは検索します。詳細は、Tenable Web App Scanning の表 を参照してください。

5. 表で、削除する認証情報にカーソルを合わせます。

   アクションボタンが行に表示されます。

6. 🗑 ボタンをクリックします。

   [Confirm Deletion] ウィンドウが表示されます。

7. 次のいずれかを行います。

   - スキャンで認証情報を使用しない場合は、**[削除]** をクリックします。
   - スキャンで認証情報を使用する場合には

a. **[スキャンの表示]** をクリックします。

[スキャン] プレーンが表示されます。

b. 認証情報を使用するスキャンをフィルタリングまたは検索します。

c. 次のいずれかを行います。

- **[キャンセル]** をクリックして、削除をキャンセルします。
- **[削除]** をクリックして、削除を確定します。

ファイルとプロセスの許可リスト

Tenable では、アンチウィルスプログラムやホストベースの侵入防止システムを含む、ファーストパーティとサードパーティの両方のエンドポイントセキュリティソフトウェアにおいて、以下の Tenable Web App Scanning (WAS) ファイルとプロセスの使用を許可することを提案しています。

許可リスト
ファイル
/opt/ruby/lib/ruby/*/bundler/templates/newgem/bin/*.tt
/opt/ruby/lib/ruby/gems/*/gems/bundler-*/lib/bundler/templates/newgem/bin/*.tt
プロセス
/opt/nessus-was-scanner-*/bin/*
/opt/nessus-was-scanner-*/bundle/ruby/*/bin/*
/opt/nessus-was-scanner-*/bundle/ruby/*/gems/*/bin/*
/opt/openssl/bin/*
/opt/ruby/bin/*
/opt/ruby/lib/ruby/*/bundler/templates/newgem/bin/*
/opt/ruby/lib/ruby/gems/*/gems/*/bin/*