OpenText™ Fortify on Demand

ユーザー ガイド

Version : 26.3

PDF Generated on : August 14, 2026

Table of Contents

1. ユーザー ガイド

このガイドでは、OpenText Fortify on Demand を使用してアプリケーション セキュリティ テストをクラウドで実行する方法について説明します。このガイドは、読者にアプリケーション セキュリティのエキスパートおよび開発チームを想定しています。

1.1. 序文

OpenText Fortify on Demand 顧客サポートへの問い合わせ

OpenText Fortify on Demand 顧客サポートへは以下の方法でご連絡ください。

- ライブチャットを開始するか、OpenText Fortify on Demand ポータルから OpenText Fortify on Demand ヘルプ センターにアクセスしてサポート チケットを作成する。
- 1.800.893.8141 または 650.800.3233 に電話で連絡する。

詳細情報

Application Security Testing 製品の詳細については、

Application Security"> Application Security を参照してください。

ドキュメント セットについて

ソフトウェアのドキュメント セットには、ソフトウェア製品およびコンポーネントすべてのインストール ガイド、ユーザー ガイド、および開発ガイドが含まれます。さらに、新機能、既知の問題、最終更新を記載したテクニカル ノートおよびリリース ノートも提供しています。以下の製品ドキュメントの Web サイトでこれらのドキュメントの最新バージョンを入手できます。

https://www.microfocus.com/support/documentation

1.2. 紹介

このセクションでは、次のトピックについて説明します。

- 製品名の変更
- OpenText Fortify on Demand (FoD) の概要
- セキュリティの評価システム
- サービス レベル目標

1.2.1. 製品名の変更

OpenText では、以下の製品名を変更中です。

以前の名前	新しい名前
OpenText™ Static Application Security Testing (OpenText SAST)	OpenText™ Fortify Static Application Security Testing (OpenText Fortify SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText FortifyDAST)
OpenText™ Core Application Security	OpenText™ Fortify on Demand
OpenText™ Core Software Composition Analysis (OpenText Core SCA)	OpenText™ Fortify Software Composition Analysis (OpenText Fortify SCA)
OpenText™ Application Security Aviator	OpenText™ Fortify Remediation Aviator
Fortify Applications and Tools	OpenText™ Application Security Tools

製品のスプラッシュ ページ、マストヘッド、ログイン ページ、および製品が表示されるその他の場所で製品名が変更されています。名前の変更は、製品の機能を明確にし、Fortify Software 製品を OpenText と合わせることを目的としています。ドキュメントのタイトルページなど、場合によっては、古い名前が括弧で囲んで示されることもあります。今後の製品リリースでは、さらに多くの変更が行われる見込みです。

1.2.2. OpenText Fortify on Demand (FoD) の概要

OpenText Fortify on Demand は Software-as-a-Service (SaaS) ソリューションです。組織はこのサービスを使用してソフトウェア セキュリティ保証プログラムを簡単にすばやく構築および拡張できます。OpenText Fortify on Demand のソフトウェア セキュリティ テストには、専門家レビュー、専用アカウント管理、年中無休のサポートによる高度で最新のアプリケーション テスト テクノロジが組み込まれています。

サービス

OpenText Fortify on Demand に送信されるアプリケーションは、ソフトウェア セキュリティのさまざまな脆弱性を分析するセキュリティ評価を受けます。OpenText Fortify on Demand は、静的、動的、モバイル、およびオープン ソースの評価を複数のサービス レベルで提供します。

- 静的評価では、アプリケーションのソース コード、バイトコード、またはバイナリ コードが分析されます。
- 動的評価では、実行している Web アプリケーションを分析します。
- モバイル評価は、モバイル アプリケーションのバイナリを分析します (ネットワークとバックエンド Web サーバーの分析も利用可能です)。
- オープン ソース ソフトウェア構成分析は、ペイロード内のオープン ソース コンポーネントを分析します。

テスト チームが、以下に示すように、セキュリティの脆弱性についてユーザーのアプリケーションを徹底的に分析します。

- アプリケーション スキャン: Fortify ソフトウェアを使用してアプリケーションがスキャンされます。
- 専門家によるレビュー: スキャン結果に対して自動監査を実行し、最大限の正確性を保証します。一部の評価タイプには、手動監査が含まれます。
- 修正検証: 評価には、見つかった問題が修正されていることを検証するための 1 つ以上の無料修正スキャンが含まれます。修正スキャンは、ベースライン評価で検出された脆弱性を修正するために変更を加えた後、同じアプリケーションで実行されます。

OpenText Fortify on Demand は、5 つ星評価システムを使用して評価されたアプリケーションを格付けします。評価結果は複数の方法で配信されます。UI のさまざまなビュー、カスタマイズ可能なレポート、詳細なデータ エクスポートが含まれます。

価格設定

OpenText Fortify on Demand サービスは、評価ユニットまたは評価スキャンの形式で権利を購入することにより利用できます。権利は注文期間の発効日から 12 か月間有効です。

任意の評価タイプの単一の評価またはサブスクリプション用の評価単位を精算できます。スキャン使用権は、特定の評価タイプの単一の評価またはサブスクリプションの数を表します。サブスクリプションでは、サブスクリプション期間中に選択したアプリケーションを無制限に評価できます。

特定の権利の詳細については、契約を参照してください。

サポート

OpenText Fortify on Demand では、セルフサービスのリソースと OpenText Fortify on Demand ヘルプ センターを通じて、専用サポート チームによるサポートを年中無休の 24 時間体制で提供しています。

1.2.3. セキュリティの評価システム

OpenText Fortify on Demand では、ユーザーのアプリケーションの脆弱性に関する有用な情報が提供されます。一貫性があり、わかりやすく、利用しやすい結果をユーザーに提供できるように、OpenText Fortify on Demand では、アプリケーションを評価する次のレポート規則が使用されます。

- 可能性と影響
- 優先順位
- 5 つ星評価

1.2.3.1. 可能性と影響

可能性と影響の評価は、検出された各脆弱性に対するリスクのレベルを定義します。

可能性

可能性とは、脆弱性が正確に特定され、悪用に成功する確率のことです。

影響

影響とは、攻撃者が脆弱性をうまく悪用することで資産に与える可能性のある、予想される損害のことです。このような損害としては、金銭的損失、コンプライアンス違反、ブランドの評判の喪失、否定的な評判などが考えられますが、これに限定されません。

1.2.3.2. 優先順位

OpenText Fortify on Demand は脆弱性 (「問題」とも呼ばれる) の重大度を分類する方法として、次の 6 つの優先度レベルを定義しています。

重大

重大な問題は、予想される影響が大きく、かつ発生する可能性が高くなります。重大な問題は、検出も悪用も容易で、資産の損害は大きいです。この問題は、アプリケーションにおける最も高いセキュリティ リスクを表します。そのため、重要な問題を直ちに修復します。

SQL インジェクションは重大な課題の例です。

高

優先度が高い問題は影響が大きいと予想されますが、発生の可能性は低い問題です。優先度の高い問題を検知して悪用することは多くの場合難しいですが、悪用されれば資産に対して大規模な損害をもたらします。この問題は、アプリケーションにおける大きなセキュリティ リスクを表します。優先度の高い問題は、予定されている次回のパッチ リリースで修復します。

優先度が高い問題の一例として、ハードコードされたパスワードが挙げられます。

中

優先度が中の問題は、影響が小さいものの、発生の可能性が高い問題です。優先度が中の問題を検知して悪用することは簡単ですが、悪用された場合の資産に対する損害は小規模です。これらの問題は、アプリケーションにとって中程度のセキュリティ リスクを示します。優先度が中の問題は次回予定されている製品更新プログラムで修復します。

パスの操作は優先度が中の問題の例です。

低

優先度が低い問題は影響が小さいと予想され、発生する可能性も低い問題です。優先度が低い問題は検出も悪用も難しい可能性があります。資産の損害は概して小さいです。この問題は、アプリケーションにおける小さなセキュリティ リスクを表します。優先度が低い問題も、時間の許す限り修復します。

デッド コードは優先度の低い問題の例です。

ベスト プラクティス

「ベスト プラクティス」は、アプリケーション内に重大な脆弱性がなく、お使いのアプリケーションのタイプに対して許容される範囲以下の小さな問題のみがあることを示しま

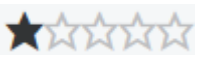
す。

情報

「情報」は最低の優先度レベルです。OpenText Fortify on Demand は脆弱性を示してはいないものの、一般的な関心を呼ぶことがあるアプリケーションに関する情報を提供します。

1.2.3.3. 5 つ星評価

OpenText Fortify on Demand の 5 つ星評価格付けでは、アプリケーション内に存在する脆弱性の可能性と影響に関する概要が提供されます。このシステムの最高の評価は 5 つ星です。これは脆弱性が何も見つからなかったことを示します。

 OpenText Fortify on Demand では、セキュリティのレビューを受けて重大な (高い可能性と大きな影響) 問題が見つかったアプリケーションには 1 つ星が与えられます。悪用するのが容易で、業務における影響や技術的な影響が大きい脆弱性は、業務上不可欠なソフトウェアには存在しないようにする必要があります。

 OpenText Fortify on Demand では、セキュリティのレビューを受けて重大な (高い可能性と大きな影響) 問題が見つからなかったアプリケーションには 2 つ星が与えられます。影響が大きい脆弱性は、悪用するのが容易でなくても、業務上不可欠なソフトウェアには存在しないようにする必要があります。

 OpenText Fortify on Demand では、セキュリティのレビューを受けて重大な (高い可能性と大きな影響) 問題が見つからず、2 つ星を受ける要件を満たしているアプリケーションには 3 つ星が与えられます。影響が小さいながら悪用が容易な脆弱性も十分配慮する必要があります。その理由は、攻撃者がこのような脆弱性の多くを一斉に悪用したり、影響が大きい攻撃を展開するための足掛かりとして影響が小さい脆弱性を利用したりした場合、このような脆弱性がより大きな脅威を生み出すことがあるためです。

 OpenText Fortify on Demand では、セキュリティのレビューを受けて中程度の (高い可能性と小さな影響) 問題が見つからず、3 つ星を受ける要件を満たしているアプリケーションには 4 つ星が与えられます。

 OpenText Fortify on Demand では、セキュリティのレビューを受けて問題が見つからなかったアプリケーションに最高の格付けである 5 つ星が与えられます。

1.2.4. サービス レベル目標

評価にはいずれも目標所要時間があります。これは、選択した評価タイプのサービス レベル目標 (SLO) によって表されます。SLO は、OpenText Fortify on Demand データ センターのタイム ゾーンに基づく営業日で指定されます。SLO は、静的評価の場合で 4 時間～ 2 営業日、動的評価の場合で 2 ～ 3 営業日、モバイル評価の場合で 1 ～ 4 営業日です。

Note

評価を設定しているときに、ポータルには、選択した評価タイプの SLO が表示されます。詳細については、「静的スキャンの設定の完了」、「動的スキャンの設定の完了」および「モバイル スキャンのセットアップの完了」を参照してください。

評価が通常のテスト要件を満たさない場合、テスト チームは顧客からの応答を待つ間、SLO タイマーを一時停止することがあります。テスト チームは速やかにタイマーを再開して、できるだけ早くテストを実施できるように尽力します。

SLO について、およびビジネス スケジュールと評価サービス レベルのバランスを取る方法についてさらに質問がある場合は、サポートに問い合わせてください。

Note

サービス レベル契約 (SLA) は、お客様との具体的な契約上の合意です。所要時間は、定義された SLO によって異なる場合があります。サービス レベル契約は、顧客作業指示書 (SOW) に定義されており、目標と義務 (目標を満たさない場合) が記載されています。

サービス レベル目標の開始日と終了日

SLO の開始日と終了日は次のように定義されます。

- **開始日**: アプリケーションの評価を開始するように依頼された日付です。
- **終了日**: 結果を入手できる日付です。

サービス レベル目標の例外

静的評価の SLO は、次の例外には適用されません。

- アプリケーションが、OpenText Fortify on Demand のベストプラクティス ガイドラインに沿って正しくパッケージされていない
- アプリケーションのペイロードが 1,000MB を超えている

動的またはモバイル評価の SLO は、次の例外には適用されません。

- テスト チームに、1 日 24 時間の連続アクセスおよび対象範囲のアプリケーションを評価するための完全に機能するテスト資格情報が提供されていない
- テスト チームが、15 以上の同時接続を使用して、HTTP/HTTPS リクエストへの平均応答時間 600 ミリ秒以内で連続して単一のアプリケーションを評価するようにセキュリティ テスト ツールを構成できない
- モバイル バイナリが難読化されているか、OpenText Fortify on Demand のベストプラクティス ガイドラインに沿って準備されていない

1.3. 使用の開始

このセクションでは、次のトピックについて説明します。

1.3.1. 開始する前に

OpenText Fortify on Demand にアクセスする前に、以下の準備が整っていることを確認してください。

- アクティブなインターネット接続
- ポータル資格情報

  > **Note**
  >
  > 資格情報の設定手順は、「Fortify on Demand へようこそ」の電子メールに記載されています。電子メールを受信していない場合は、迷惑メール フィルターを確認してください。

- 画面解像度 1280 x 720 以上のモニター (推奨 1920 x 1080)
- 以下のサポートされているブラウザーのいずれかがインストールされていること
  - Chrome 最新バージョン
  - Firefox Quantum 最新バージョン
  - Mac 上の Safari 最新バージョン (PC 上の Safari はサポートされていません)
  - Edge 最新バージョン

1.3.2. ポータルへのログインとログアウト

ポータル資格情報を受け取ると、ポータルにアクセスできるようになります。

ポータルへのログイン

ポータルにログインするには、次の手順を実行します。

1. ユーザー資格情報で指定されたポータルの URL をブラウザーのアドレス バーに入力します。

   [ログイン] ページが表示されます。

2. ユーザー名、パスワード、テナント コードを入力します。

Note

過去 30 日以内に SSO 経由でログインした場合は、SSO ログイン リンクを使用して再度ログインできます。

3. [**ログイン**] をクリックします。

ランディング ページが表示されます。チャレンジの質問とそれに対応する回答を設定していない場合は、アカウントの設定ページへリダイレクトされます。

> **Note**
>
> 組織で 2 要素認証を有効にしている場合は、SMS、電子メール、または TOTP で受け取るセキュリティ コードを入力するように求められます。

ポータルからのログアウト

ポータル ツールバー設定でポータルからログアウトします。20 分間アクティビティがない場合は、ポータルから自動的にログアウトされることに注意してください。

ポータルからログアウトするには、次の手順を実行します。

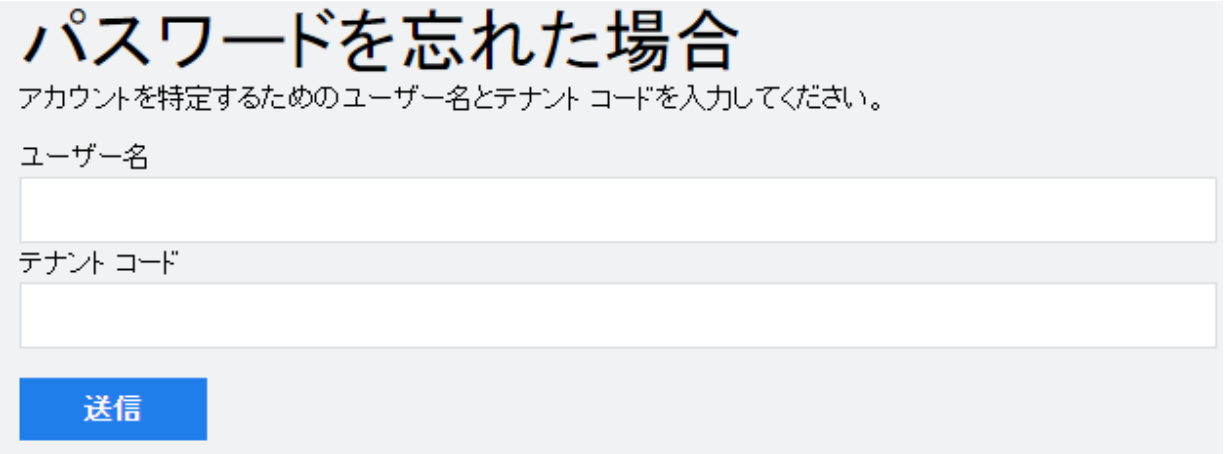
1. アカウント名をクリックし、[**ログアウト**] を選択します。

1.3.3. パスワードのリセット

忘れたパスワードをリセットするには、次の手順を実行します。

1. ログイン ページで、[**パスワードを忘れた場合**] をクリックします。

   [パスワードを忘れた場合] ページが表示されます。



2. ユーザー名とテナント コードを入力します。
3. [**送信**] をクリックします。

   ユーザー アカウントに関連付けられている電子メール アドレスに、パスワードのリセット用リンクを記載した電子メールが送信されます。

4. 電子メール内のリンクをクリックします。

   パスワードのリセット ページが表示されます。

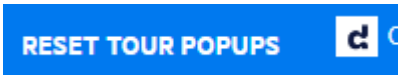
> **Note**
>
> パスワード リセット用リンクの有効期限が切れている場合は、電子メールに記載されている指示に従って新しいリンクをリクエストしてください。

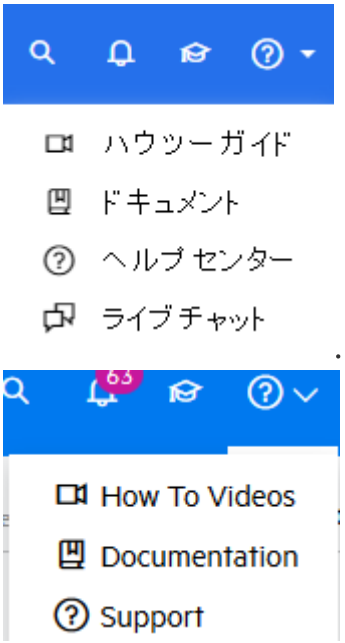
5. [**パスワード チャレンジの答え**] フィールドに、 パスワード チャレンジの質問に対する回答を入力します。パスワード チャレンジの質問と回答を設定していない場合、この手順は適用されません。
6. パスワードを入力し、確認のため再入力します。
7. [**OK**] をクリックします。

   パスワードがリセットされます。

1.3.4. ポータルの操作

ポータル ページ内のページレイアウトは共通です。次の表に、ポータルの一般的なナビゲーションを説明します。

タスク	アクション
親ビューに移動する	次のいずれかのビューを選択します。 
ユーザー ツアーを再生	ツールバーの [**ツアー ポップアップのリセット**] をクリックします。 
アカウントの設定と追加のリソースにアクセスする	ツールバーでアカウント名をクリックします。 
ポータルの検索にアクセスする	 をクリックします。詳細については、「ポータルの検索」を参照してください。
ポータルの通知にアクセスする	 をクリックします。詳細については、「通知の管理」を参照してください。

タスク	アクション
トレーニング コースにアクセスする	をクリックします。詳細については、「トレーニング コース」を参照してください。
ヘルプ リソースへのアクセス	[ヘルプ] メニューをクリックします。 
親ビュー内のページに移動する	サイドバーのアイコンをクリックします。
状況依存のヘルプにアクセスする	をクリックします。機能のヘルプ トピックを表示する新しいウィンドウが開きます。
ページで列を並べ替える	列のヘッダーをクリックします。ヘッダーの白い三角形は、並べ替えられるフィールドおよびデータの並べ替え順序を示します。順序を逆にするには、ヘッダーをもう一度クリックします。

タスク	アクション
ページ上に表示される項目数を変更する	[25]、[50]、または [100] をクリックします。  **Note** [アプリケーション] ページの [**検出**] タブには、ページごとに 250 個および 500 個のアイテムを表示できます。
リストの別のページを表示する	ページ番号または矢印をクリックします。 

1.3.5. ポータルの検索

OpenText Fortify on Demand には、ポータルのリソースを検索する方法がいくつか用意されています。ポータルのツールバーにある [**検索**] ボックスを使用すると、テナント レベルでアプリケーション、リリース、マイクロサービス、またはレポートを検索できます。

ポータル内のアプリケーション、リリース、マイクロサービス、またはレポートを検索するには、次の手順を実行します。

1. ポータル ツールバーの アイコンをクリックします。

   検索ボックスが表示されます。既定では、すべてのアイテム タイプが検索対象に含まれます。

   検索ボックス

2. 検索結果を絞り込むには、[**アプリケーション**]、[**リリース**]、[**レポート**]、および [**マイクロサービス**] の 1 つまたは複数のチェック ボックスの選択を解除します。
3. 検索ボックスには、検索するアイテムの名前の全体または一部を入力します。

   ドロップダウン リストに検索結果が表示されます。

   検索結果

4. リストから選択します。選択によりポータルが更新されます。

1.3.6. アカウント設定の管理

ポータルのツールバーからアカウント設定を表示および編集できます。

このセクションでは、次のトピックについて説明します。

- アカウント設定の編集
- アカウントのパスワードの変更

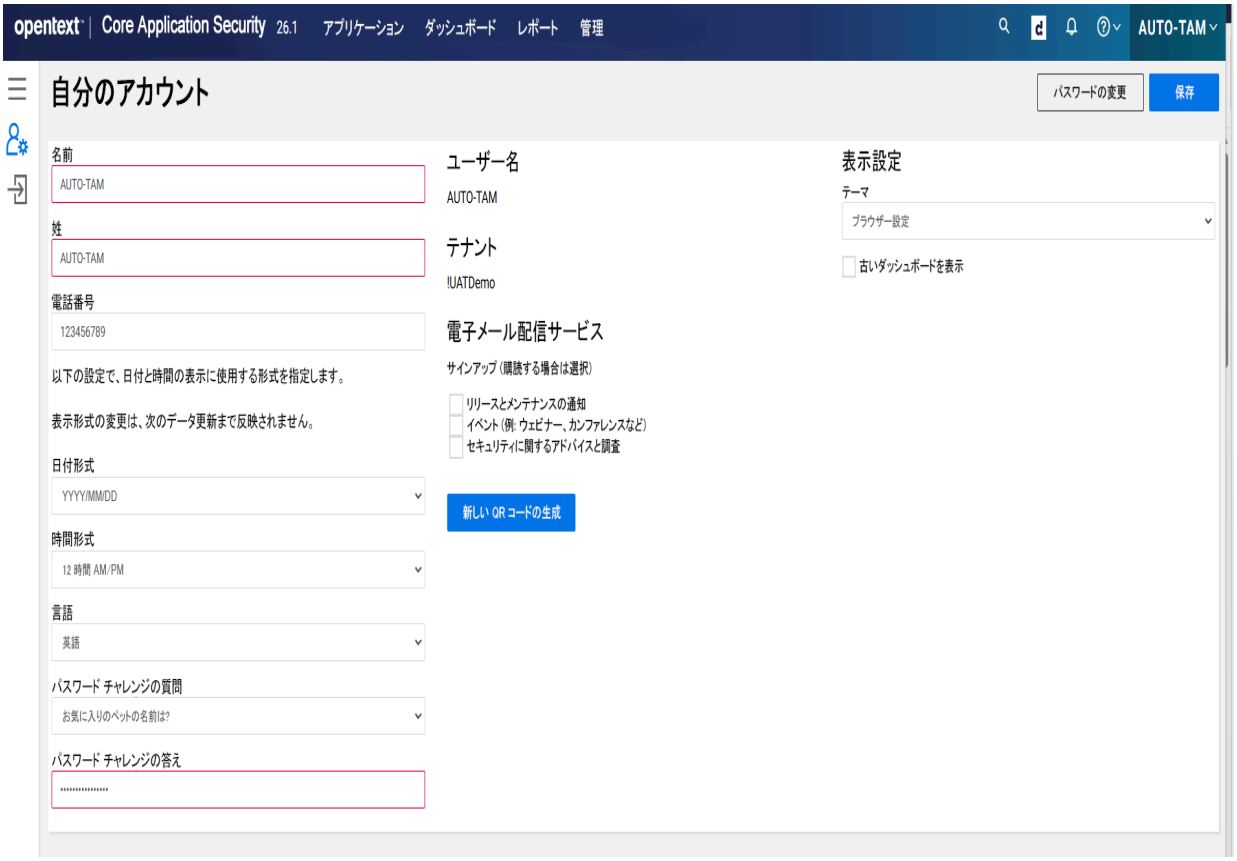
1.3.6.1. アカウント設定の編集

[自分のアカウント] ページでは、自分の連絡先情報、ポータル設定、パスワードのリセット用の質問と回答を更新できます。

アカウントの設定を編集するには、次の手順を実行します。

1. アカウント名をクリックし、[**アカウントの設定**] を選択します。

   [自分のアカウント] ページが表示されます。



2. 必要に応じてフィールドを更新します。赤色で囲まれたフィールドは入力が必須です。

フィールド	説明
名前	名前
姓	姓
電話番号	電話番号
日付形式	日付の表示形式: **MM/DD/YYYY**、**DD/MM/YYYY**、**YYYY/MM/DD**
時間形式	時間の表示形式: **12 時間 AM/PM**、**24 時間**
言語	表示言語: **English**、**Español**、**日本語** **Note** レポートは選択した言語で生成されます。
パスワード チャレンジの質問	パスワード チャレンジの質問のリスト
パスワード チャレンジの答え	選択したパスワード チャレンジの質問に対する大文字と小文字が区別されない回答 **Note** パスワード チャレンジの質問と回答を設定しておかないと、アカウントの変更を保存できなくなります。

3. [**電子メール配信サービス**] セクションでサブスクリプションを更新します。電子メール配信サービスにより、OpenText Fortify on Demand のイベントの最新情報が取得されます。登録すると、リリースおよびメンテナンス、セキュリティのアドバイス、関連するウェビナおよび会議の通知を受け取れます。

4. 新しい TOTP Authenticator を要求するには、[**新しい QR コードの生成**] をクリックします。[セキュリティ コード] 画面が表示されます。

   1. QR コードをスキャンします。
   2. TOTP 認証コードを入力します。
   3. [**送信**] をクリックしてコードを検証します。

5. [**保存**] をクリックします。

   変更が正常に保存されたことを知らせる確認メッセージが表示されます。

1.3.6.2. アカウントのパスワードの変更

[自分のアカウント] ページでアカウントのパスワードを変更できます。

Note

パスワードは 16 文字以上である必要があります。簡単で一般的な語句をパスワードに含めることはできません。また、少なくとも 1 個の大文字、1 個の小文字、1 個の数字、および 1 個の特殊文字を含める必要があります。

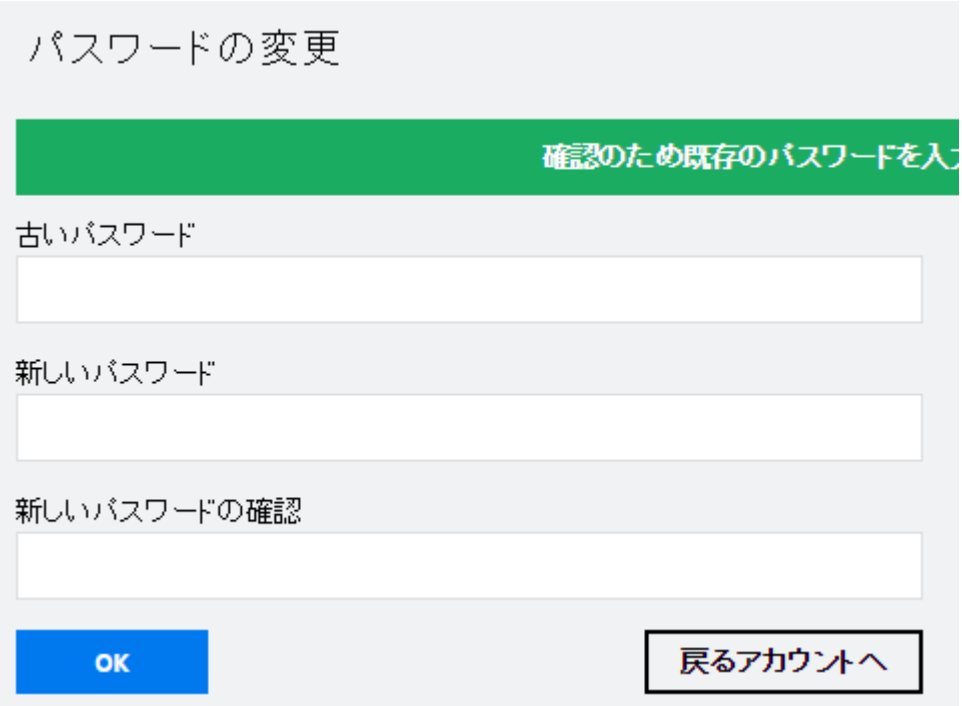
アカウントのパスワードを変更するには、次の手順を実行します。

1. アカウント名をクリックし、[**アカウントの設定**] を選択します。

   [自分のアカウント] ページが表示されます。

2. [**パスワードの変更**] をクリックします。

   [パスワードの変更] ページが表示されます。



3. [**古いパスワード**] フィールドに現在のパスワードを入力します。
4. [**新しいパスワード**] フィールドに新しいパスワードを入力します。
5. [**新しいパスワードの確認**] フィールドに新しいパスワードをもう一度入力します。
6. パスワードを変更するには [**OK**] ボタンを、ページを閉じるには [**アカウントに戻る**] をクリックします。

1.3.7. 通知の管理

OpenText Fortify on Demand は、ユーザーがポータルで重要なアクティビティをより適切に監視できるようにするための、堅固なインプロダクト通知エンジンを提供しています。これは特に大きなアプリケーションおよびユーザー ベースに重要です。最初に、ユーザーには、注意すべきイベント (たとえば、アプリケーションのビジネス クリティカリティが変更された場合、不合格になっているリリースが本番環境に昇格された場合、アプリケーションのスキャンが開始、一時停止、完了、またはキャンセルされた場合など) に対するシステム デフォルト グローバル サブスクリプションが割り当てられます。ユーザーは、自分がアクセスできるアプリケーションの通知にポータル ツールバーから簡単にアクセスできます。

ユーザーは、個別のサブスクリプションを作成して追加の通知を受け取ることができます。セキュリティ リーダーは、すべてのユーザー、特定のロール、または特定のグループに対しテナント レベルのグローバル サブスクリプションを作成することができます。次の通知トリガー タイプが使用できます。

- アプリケーションの作成、更新、削除
- リリースの作成、更新 (不合格になっているリリースの本番環境への昇格を含む)、削除
- スキャン ステータスの更新
- 問題の更新
- レポートの生成

このセクションでは、次のトピックについて説明します。

1.3.7.1. 通知の表示

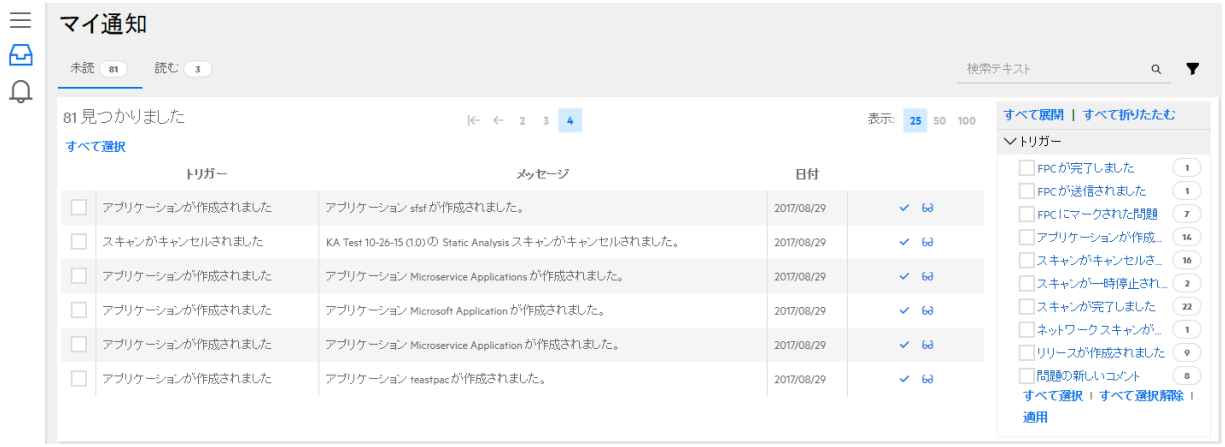
ポータルのすべてのページから通知を表示できます。登録されているトリガー イベントが発生した場合、ツールバーの [通知] アイコンの横にある数字が増えます。この数字は、既読としてマークされていない通知の集計です。

Note
既読と未読のすべての通知は 90 日後に削除されます。

通知を表示するには、次の手順を実行します。

1. ポータル ツールバーの 29 アイコンをクリックします。

   [通知] ページが表示され、未読の通知のリストが表示されます。



2. 通知の詳細を表示するには、通知のアクション列の アイコンをクリックします。関連アプリケーション、リリース、または個別の問題のページに移動します。

3. 通知を既読としてマーク付けするには、通知のアクション列の アイコンをクリックします。通知リストをフィルターし、[**既読としてマーク**] をクリックして通知を一括で編集することもできます。

   通知が [既読通知] に移動されて、集計から削除されます。

4. 前に既読としてマークした通知を表示するには、[**既読**] タブを選択します。

   既読通知のリストが表示されます。


マイ通知
未読 85
読む 3
検索テキスト
3 見つかりました
表示: 25 50 100
すべて選択
すべて展開 | すべて折りたたむ
トリガー
FPC が完了しました 1
FPC が送信されました 1
スキャンが完了しました 1
すべて選択 | すべて選択解除 | 適用
トリガー
メッセージ
日付
スキャンが完了しました
17.4 Dynamic Website Assessment (1) の Dynamic Website Assessment スキャンが完了しました。
2017/11/08
FPC が完了しました
17.4 Dynamic Website Assessment (1) の誤検知の再確認が完了しました。
2017/11/08
FPC が送信されました
17.4 Dynamic Website Assessment (1) の誤検知の再確認が送信されました。
2017/11/08

1.3.7.2. 独自サブスクリプションの作成

グローバル通知を受け取るだけでなく、独自のサブスクリプションを作成して、指定された条件によってトリガーされる通知を受け取ることができます。

独自のサブスクリプションを作成するには、次の手順を実行します。

1. ポータル ツールバーの 

アイコンをクリックします。

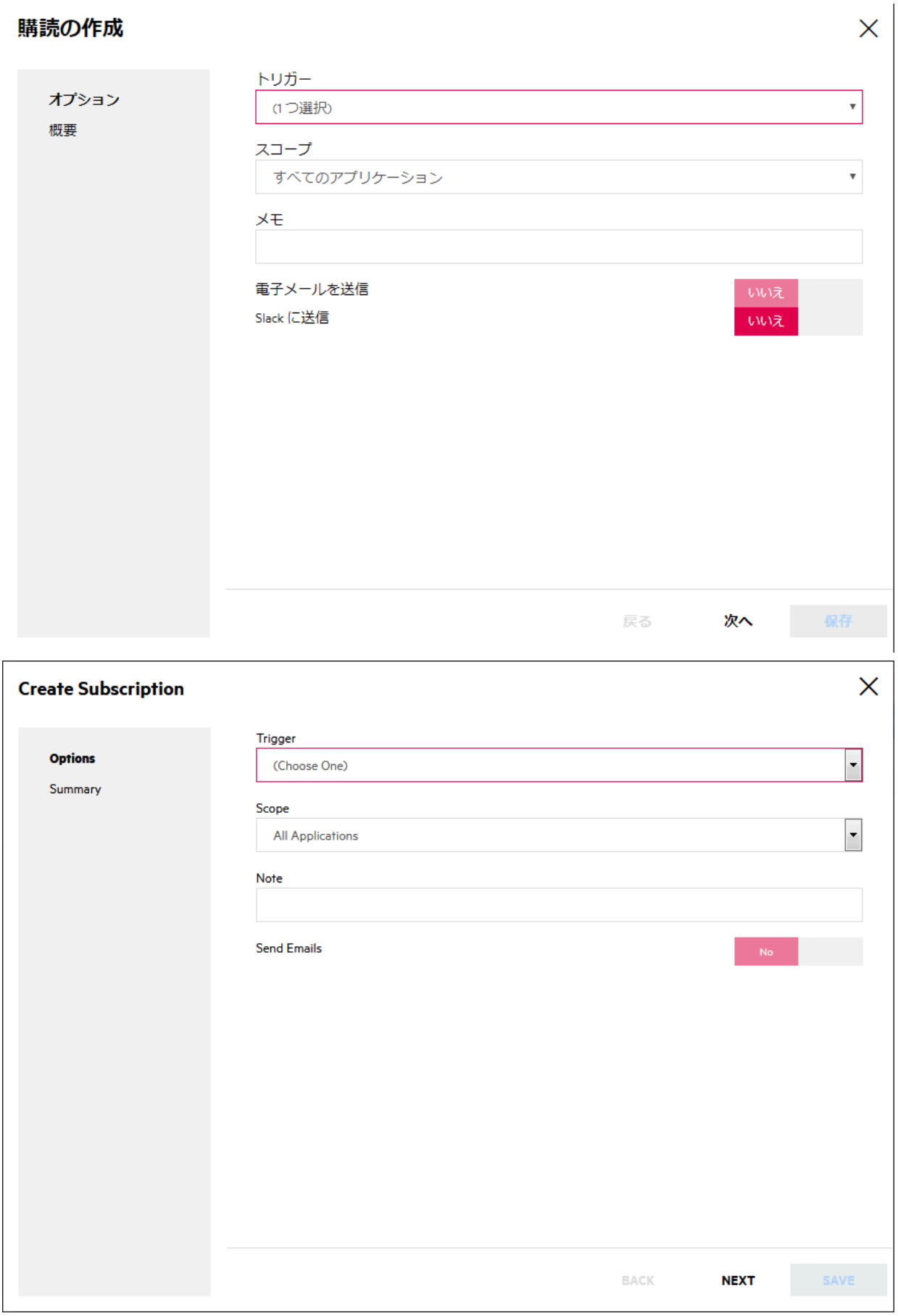
   [通知] ページが表示されます。

2. **[購読]** をクリックします。

   独自のサブスクリプションのリストが表示されます。

3. **[+ 新規サブスクリプション] をクリックします。**

   [サブスクリプションの作成] モーダル ウィンドウが開きます。



4. フィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
トリガー	リストからトリガー タイプを選択します。
スコープ	トリガーが適用されるスコープをリストの [**すべてのアプリケーション**] (既定)、[**アプリケーション**]、[**アプリケーションの種類**]、[**アプリケーション属性**]、[**ビジネス クリティカリティ**]、および [**所有するすべてのリリース**] から選択します。
	(オプション) サブスクリプションのメモを入力します。
電子メールを送信	(オプション) スライダーを [**いいえ**] から [**はい**] に移動して、電子メールの通知の送信を有効にします。このオプションは、[**ユーザーに割り当てられた問題**] トリガーと、問題以外のすべてのトリガーの場合に使用できます。
Slack に送信	(オプション) スライダーを [**いいえ**] から [**はい**] に移動して、通知を Slack に投稿します。このオプションは、Slack 統合が設定されている場合のみ使用可能で、セキュリティ リーダーに限定されます。

5. [**次へ**] をクリックします。

   [**すべてのアプリケーション**] 以外のスコープを選択した場合は、[スコープ] ページが表示されます。そうでない場合は、手順 7 に進みます。

6. スコープの値を選択して、[**次へ**] をクリックします。

7. 通知トリガー設定を確認し、[**保存**] をクリックします。

   新しいサブスクリプションが独自のサブスクリプションのリストに表示されます。

1.3.7.3. グローバル サブスクリプションの作成

セキュリティ リーダーは、すべてのユーザー、特定のロール、または特定のグループに対しテナント レベルのグローバル サブスクリプションを作成することができます。

グローバル サブスクリプションを作成するには、次の手順を実行します。

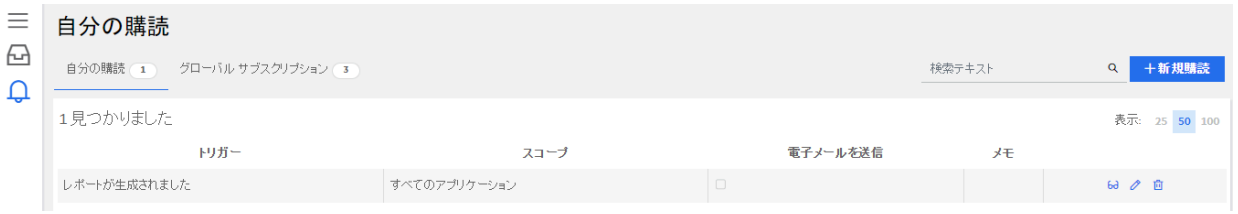
1. ポータル ツールバーの 

アイコンをクリックします。

   [通知] ページが表示されます。

2. [**購読**] をクリックします。

   独自のサブスクリプションのリストが表示されます。



3. [**グローバル サブスクリプション**] タブを選択します。

   システムデフォルト グローバル サブスクリプションを含むグローバル サブスクリプションのリストが表示されます。

4. **[+ 新規サブスクリプション] をクリックします。**

   [サブスクリプションの作成] モーダル ウィンドウが開きます。

5. フィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
トリガー	リストからトリガー タイプを選択します。
宛先	リストの [**すべてのユーザー**] (デフォルト)、[**グループ**]、および [**ロール**] からサブスクリプションのオーディエンスを選択します。[**グループ**] または [**ロール**] を選択した場合は、それぞれ特定のグループまたはロールを選択します。 **Note** 宛先は、通知で参照されるアプリケーションにアクセスできるユーザーに限定されます。
スコープ	トリガーが適用されるスコープをリストの [**すべてのアプリケーション**] (既定)、[**アプリケーション**]、[**アプリケーションの種類**]、[**アプリケーション属性**]、[**ビジネス クリティカリティ**]、および [**所有するすべてのリリース**] から選択します。
	(オプション) サブスクリプションのメモを入力します。

フィールド	説明
電子メールを送信	(オプション) スライダーを [**いいえ**] から [**はい**] に移動して、電子メールの通知の送信を有効にします。[**スキャンがキャンセルされました**] トリガーと [**スキャンが一時停止されました**] トリガーでは、[**電子メールを送信**] が常に有効になっています。このオプションは、[**ユーザーに割り当てられた問題**] トリガーと、問題以外のすべてのトリガーに使用できます。
Slack に送信	(オプション) スライダーを [**いいえ**] から [**はい**] に移動して、通知を Slack に投稿します。このオプションは、Slack 統合が設定されている場合に使用可能で、セキュリティ リーダーに限定されます。

6. [**次へ**] をクリックします。

   [**すべてのアプリケーション**] 以外のスコープを選択した場合は、[スコープ] ページが表示されます。そうでない場合は、手順 8 に進みます。

7. スコープの値を選択して、[**次へ**] をクリックします。

8. 通知トリガー設定を確認し、[**保存**] をクリックします。

   新しいサブスクリプションがグローバル サブスクリプションのリストに表示されます。

1.3.7.4. サブスクリプションの編集

カスタム サブスクリプションを編集できます。セキュリティ リーダーの場合、グローバル サブスクリプションを編集することもできます。

サブスクリプションを編集するには、次の手順を実行します。

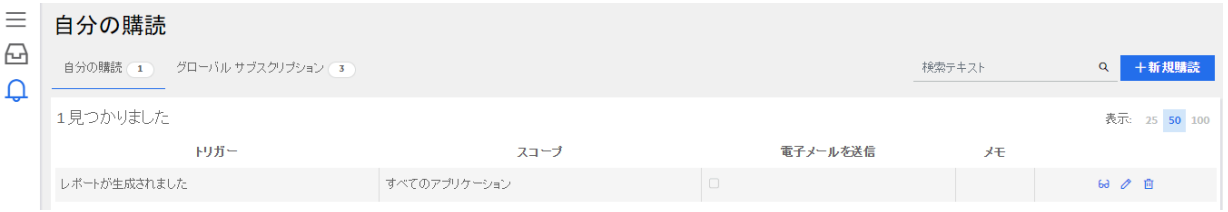
1. ポータル ツールバーの 

アイコンをクリックします。

   [通知] ページが表示されます。

2. [**購読**] をクリックします。

   カスタム サブスクリプションのリストが表示されます。



3. カスタム サブスクリプションを編集している場合、[**自分の購読**] タブからは移動しません。セキュリティ リーダーがグローバル サブスクリプションを削除する場合は、[**グローバル サブスクリプション**] タブを選択します。

4. 編集するサブスクリプションの横にある  アイコンをクリックします。

   [サブスクリプションの編集] ウィンドウが表示されます。

5. 必要に応じてフィールドを編集します。フィールドの詳細については、「独自サブスクリプションの作成」および「グローバル サブスクリプションの作成」を参照してください。

   サブスクリプションの変更が保存されます。

1.3.7.5. サブスクリプションの削除

作成した独自のサブスクリプションを削除することができます。セキュリティ リーダーはすべてのグローバル サブスクリプションおよびシステムデフォルト グローバル サブスクリプションを削除することができます。

サブスクリプションを削除するには、次の手順を実行します。

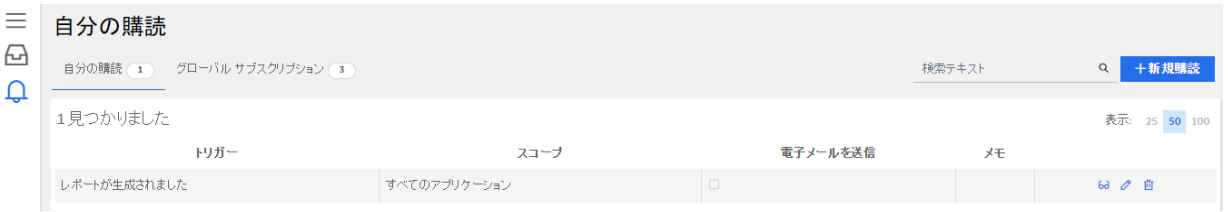
1. ポータル ツールバーの 

アイコンをクリックします。

   [通知] ページが表示されます。

2. [**購読**] をクリックします。

   独自のサブスクリプションのリストが表示されます。



3. 独自のサブスクリプションを削除する場合は、[**自分の購読**] タブからは移動しません。グローバル サブスクリプションを削除する場合は、[**グローバル サブスクリプション**] タブを選択します。

4. 削除するサブスクリプションの横にある アイコンをクリックします。

   確認メッセージが表示されます。

5. [**はい**] をクリックして、削除を確定します。

   サブスクリプションがサブスクリプションのリストから削除されます。

1.3.8. テナントの切り替え

TAM は、ポータル データセンターで管理するテナント アカウントを切り替えることができます。

> **Note**
> これは TAM のみの機能です。

テナントを切り替えるには、次の手順を実行します。

1. アカウント名をクリックし、[**テナントの切り替え**] を選択します。

   [テナントの切り替え] ページが表示されます。

2. 使用可能なテナントのリストから、切り替えるテナントを選択します。

   ポータルが更新され、選択したテナントのデータが表示されます。

1.4. アプリケーションおよびリリースの管理

セキュリティ評価基準は、OpenText Fortify on Demand のアプリケーションと、関連付けられているリリースに従って整理されています。ユーザーはポータルでアプリケーションとリリースを管理できます。

このセクションでは、次のトピックについて説明します。

- アプリケーションおよびリリースの構造化
- アプリケーションの管理
- リリースの管理
- テナントのアプリケーションの表示
- テナントのリリースの表示
- アプリケーションおよびリリースの検索
- ディープ リンクの作成

1.4.1. アプリケーションおよびリリースの構造化

OpenText Fortify on Demand では、セキュリティ評価のためにアプリケーションとリリースを定義します。

アプリケーション定義

アプリケーションはコードベースです。1 つ以上のリリースに対し最上位のコンテナとして機能します。

OpenText Fortify on Demand ではアプリケーションを次のコンテキストで定義します。

静的評価の場合、アプリケーションは、次のようなソースおよび/またはバイト コード命令ファイルのコレクションから成る展開可能なコード単位として定義されます。

- ビジネス アプリケーションの一部またはすべての機能を提供できる
- 同じテクノロジ ファミリで記述されている
- 単一のプラットフォームで構築される
- 疎結合コンポーネントを含まない
- アプリケーション サーバーで実行されるように構成できる (たとえば、Java アプリケーションの場合は Web アプリケーション アーカイブ [WAR] またはエンタープライズ アーカイブ [EAR] ファイル、あるいは .NET アプリケーションの場合は Team Foundation Server のソリューション)

独立した疎結合プロセスとして実行され、明確に定義された軽量のメカニズムを使用して通信し、ビジネス アプリケーションの単一機能を提供する、小さなモジュラー サービスとしてのマイクロサービス。マイクロサービス アーキテクチャを使用したアプリケーションの場合、静的サブスクリプションにより顧客はアプリケーションの一部またはすべてを形成する最大 10 個のマイクロサービスをテストする権利が付与されます。各マイクロサービスは 100 MB 以下の単一の ZIP ファイルとしてパッケージ化し、送信する必要があります。その他すべての静的評価サービスの場合、各マイクロサービスは個別のアプリケーションとみなされます。

次の条件がマイクロサービス アプリケーションに適用されます。

- サポート対象のテクノロジ スタックは、.NET、.NET Core、C/C++、Go、JAVA/J2EE、JS/TS/HTML、PHP、Python、Scala、および Ruby です。
- 複数のマイクロサービスに対して送信された静的スキャンはキューに入れられ、キューに入れられた順にスキャンされます。

- サード パーティ ライブラリは、マイクロサービスのスキャン時は常に除外されます。

動的評価の場合、アプリケーションは完全修飾ドメイン名 (FQDN) として定義されます。たとえば、www.microfocus.com の場合:

- www.microfocus.com は FQDN であり、アプリケーションです。
- www.microfocus.com/news/ は同じホスト名であるため、同じ FQDN であり、同じアプリケーションです。
- community.microfocus.com は別のサブドメインであるため、別の FQDN であり、別のアプリケーションです。
- www.microfocus.co.uk は別のドメイン名であるため、別の FQDN であり、別のアプリケーションです。

アプリケーションは、次の例外を除いて、単一の認証管理システムのみを持つことができます。

- フォーム認証と単一ネットワーク認証 (基本/ダイジェスト/NTLM) が許可されます。
- フォーム認証、単一ネットワーク認証、およびベアラ トークンなどのアプリケーションによって生成される認証が許可されます。

ユーザー ログインは「デイジー チェーン」でない場合があります。たとえば、2 つのフォーム認証メカニズムは許可されていません。

Web API アプリケーションの場合のみ、顧客は API エンドポイントの定義を提供する必要があります。

- 動的評価
  - REST API - すべてのパラメーターに有効な値とハードコードされた長期間有効な認証トークンを含む OpenAPI JSON 仕様または Postman コレクション
- Dynamic+ 評価
  - REST API - OpenAPI JSON 仕様または Postman コレクション
  - SOAP – 単一の SOAP WSDL ファイル

  すべてのパラメーターの有効な値を使用した実例を提供する必要があります。

モバイル評価の場合、アプリケーションは単一のハードウェア プラットフォーム向けの単一のインストール可能アプリケーションです。テスト用に送信されるモバイル アプリケー

ションは、コンパイル済みの IPA (iOS) または APK (Android) の形式である必要があります。

リリースの定義

リリースは、コードベースの特定の反復です。OpenText Fortify on Demand では、リリース バージョンの管理によってスキャン アクティビティの識別と追跡に役立つ方法が提供されます。リリースは、組織のレポートのニーズと開発プロセスに応じて構築することができます。

次の例に、リリースの構築方法を示します。

- 静的評価:
    - 継続的な統合ビルド サーバーからのビルドでの自動スキャンに対し、初回のベースライン リリースからコピーされた主要なリリースを 1 つ作成します。コードの主要展開 (状態のコピーを使用)、より詳細な分析 (サード パーティ ライブラリを含める/ベースラインに対する手動監査を選択する)、またはメトリックスに影響を与えずに 1 回のスキャンを行うためのサンドボックス リリースなどのシナリオに対し、定期的にブランチ リリースを作成します。
    - 主要な製品リリースごとに新しいリリースを作成し (状態のコピーを使用)、次のリリースに移動する前にリリース サイクル中にスキャンを実行します。
    - ビルドごとにリリースを作成します。傾向が見られず、オーバーヘッドが増加するため、このアプローチはお勧めしません。
- 動的評価:
    - スキャン中の環境 (開発、ステージング、UAT、または本番環境) に基づいて、すべてのスキャンに対し単一のリリースを作成します。リリースは通常、URL によって命名されます。
    - 主要な開発ごとに新しいリリースを作成します (状態のコピーを使用)。
- 静的評価および動的評価:
    - 上記の例を別個に、または組み合わせて実装します。たとえば、最初の静的評価例を主要なアプローチとして実装することも、メインの主要なリリース ブランチに対して動的評価を実行することも、静的スキャンから独立した個別のリリースに対し動的評価を実行することもできます。
- モバイル評価:
    - モバイル バイナリのみの評価の場合、静的評価例を実装します。
    - バックエンド Web サービスを含む評価の場合、動的評価例を実装します。

さらに、ソフトウェア開発ライフサイクル (SDLC) ステージをリリースに割り当て、その進捗を SDLC で追跡できます。OpenText Fortify on Demand は、以下の SDLC ステージ

を使用します。

- 開発
- QA/テスト
- 本番環境
- 廃棄

> **Note**
>
> 廃止されたリリースで新しいスキャンを開始できません。リリースが廃棄になり、スキャンが進行中の場合、スキャンは終了します。

1.4.2. アプリケーションの管理

アプリケーションをユーザー権限に応じて作成、表示、編集することができます。

このセクションでは、次のトピックについて説明します。

- アプリケーションの作成
- アプリケーションの詳細の表示
- アプリケーション設定の編集
- アプリケーションへのユーザー割り当ての管理
- アプリケーションのイベント ログの表示
- アプリケーションの削除

1.4.2.1. アプリケーションの作成

アプリケーションの初回セキュリティ評価を開始する前に、新しいアプリケーションを OpenText Fortify on Demand で作成する必要があります。

アプリケーションを作成するには、次の手順を実行します。

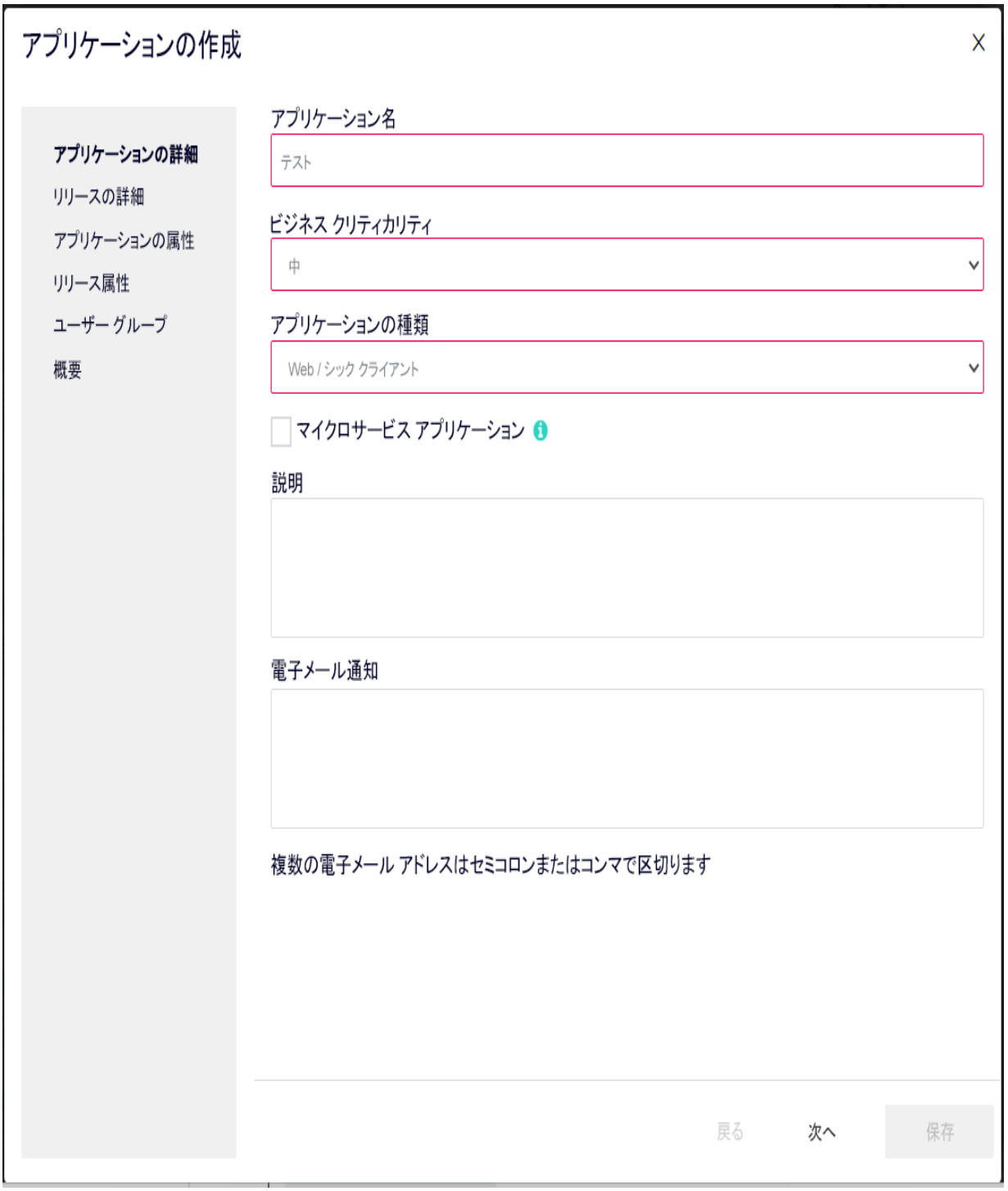
1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**+ 新しいアプリケーション**] をクリックします。

   [アプリケーションの作成] ウィザードが表示されます。

3. [**アプリケーションの詳細**] ページで、アプリケーションを定義します。他に指示がない限り、フィールドは必須です。


アプリケーションの作成
X
アプリケーションの詳細
リリースの詳細
アプリケーションの属性
リリース属性
ユーザー グループ
概要
アプリケーション名
テスト
ビジネス クリティカリティ
中
アプリケーションの種類
Web / シック クライアント
マイクロサービス アプリケーション
説明
電子メール通知
複数の電子メール アドレスはセミコロンまたはコンマで区切ります
戻る
次へ
保存

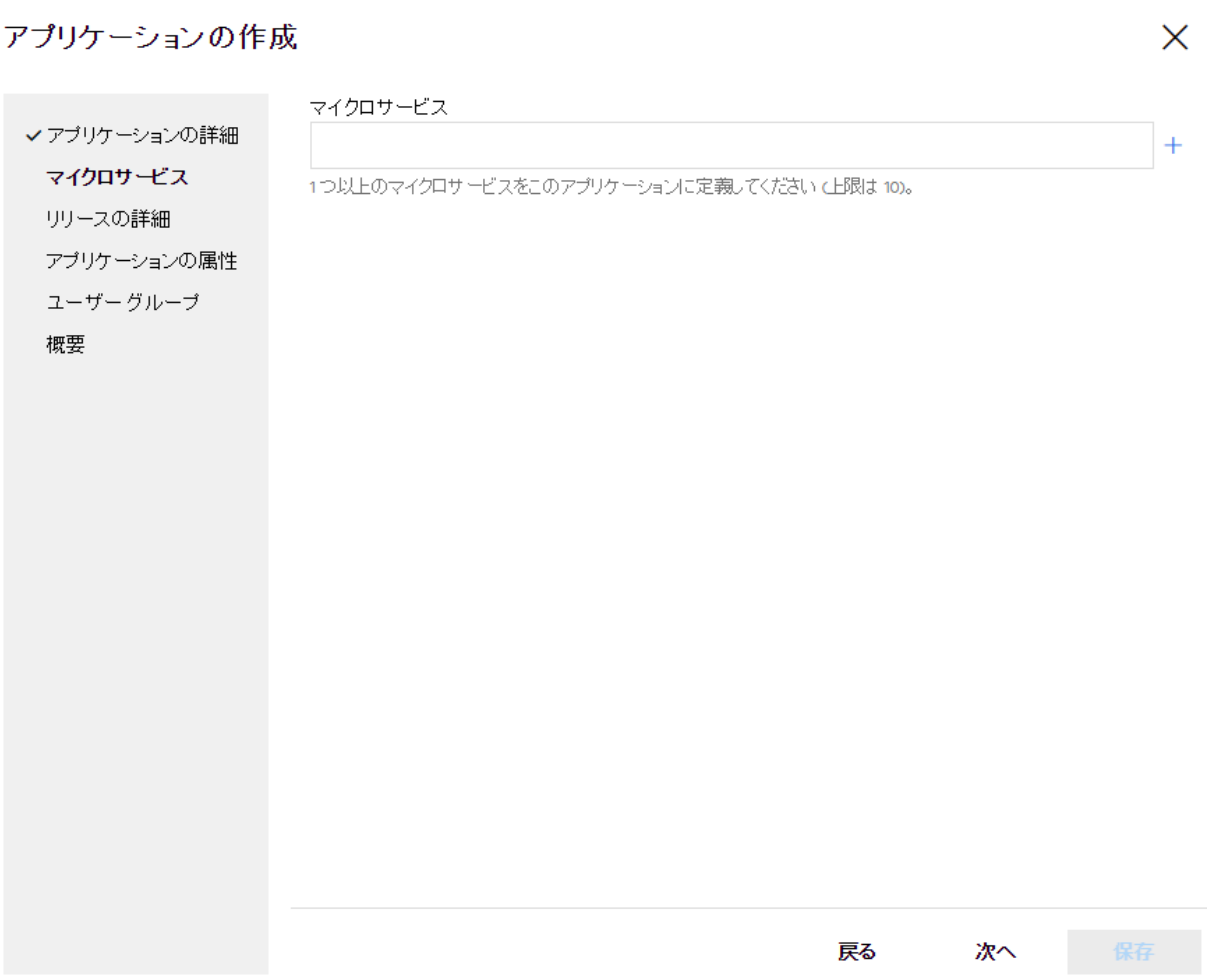
フィールド	説明
アプリケーション名	アプリケーション名を入力します。
ビジネス クリティカリティ	アプリケーションの重要度のレベルを選択します。 ◦ **高**: セキュリティの問題により、ビジネスに甚大な被害が生じる可能性があります。 ◦ **中**: セキュリティの問題により、ビジネスに大きな影響が生じる場合がありますが、ビジネスの存続に関わるほどの重大な被害ではありません。 ◦ **低**: 無視できる、または時間があるときに少しずつ解決してもよいセキュリティの問題です。
説明	(オプション) 複数のアプリケーションの管理に役立つアプリケーションの説明を入力します。
電子メール通知	(オプション) アプリケーションのスキャン ステータスの更新の電子メール通知を受信する電子メール アドレスのリストを表示します。複数の電子メール アドレスはセミコロンまたはコンマで区切ります。
アプリケーションの種類	アプリケーションの種類 [**Web/シック クライアント**] または [**モバイル**] を選択します。

フィールド	説明
マイクロサービス アプリケーション	機能を有効にするには、ヘルプ センター チケットを作成します。 ([**Web / シック クライアント**] アプリケーションのみ) アプリケーションをマイクロサービス アプリケーションとしてスキャンするには、チェックボックスをオンにします。 **Important** マイクロサービス アプリケーションの指定は永続的であり、アプリケーションの作成後に変更することはできません。

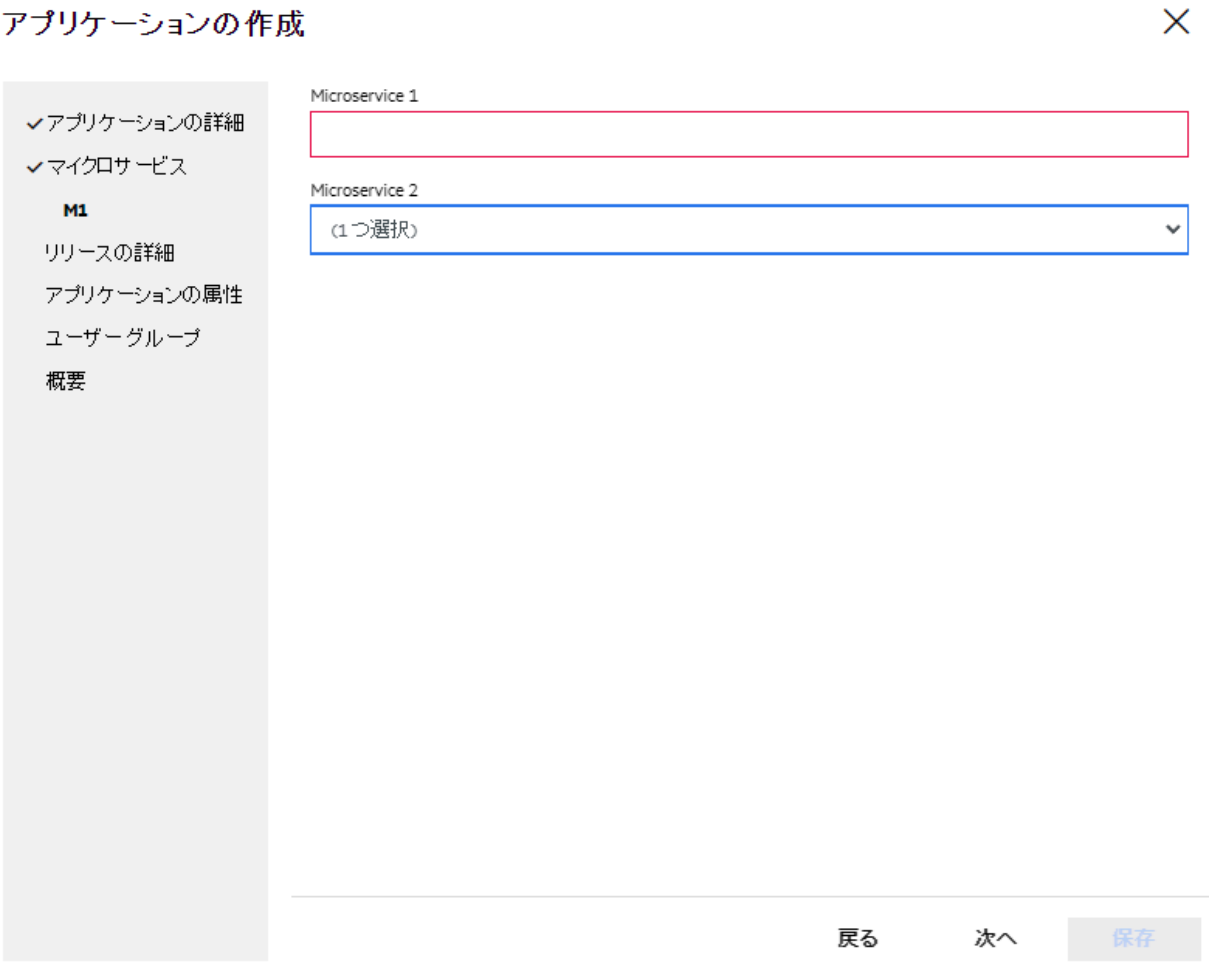
4. [**次へ**] をクリックします。
5. (マイクロサービス アプリケーションのみ) [**マイクロサービス**] ページで、マイクロサービス名をテキスト ボックスに入力し、＋をクリックします。

   マイクロサービスが下に追加されます。最大 10 個のマイクロサービスを追加できます。

   Note
   アプリケーションを作成した後にマイクロサービスを追加することもできます。



6. [**次へ**] をクリックします。
7. (マイクロサービス アプリケーションのみ) マイクロサービスの属性が構成されている場合は、マイクロサービスの属性を指定します。[**次へ**] をクリックして、前に追加したマイクロサービスごとにこれを行います。



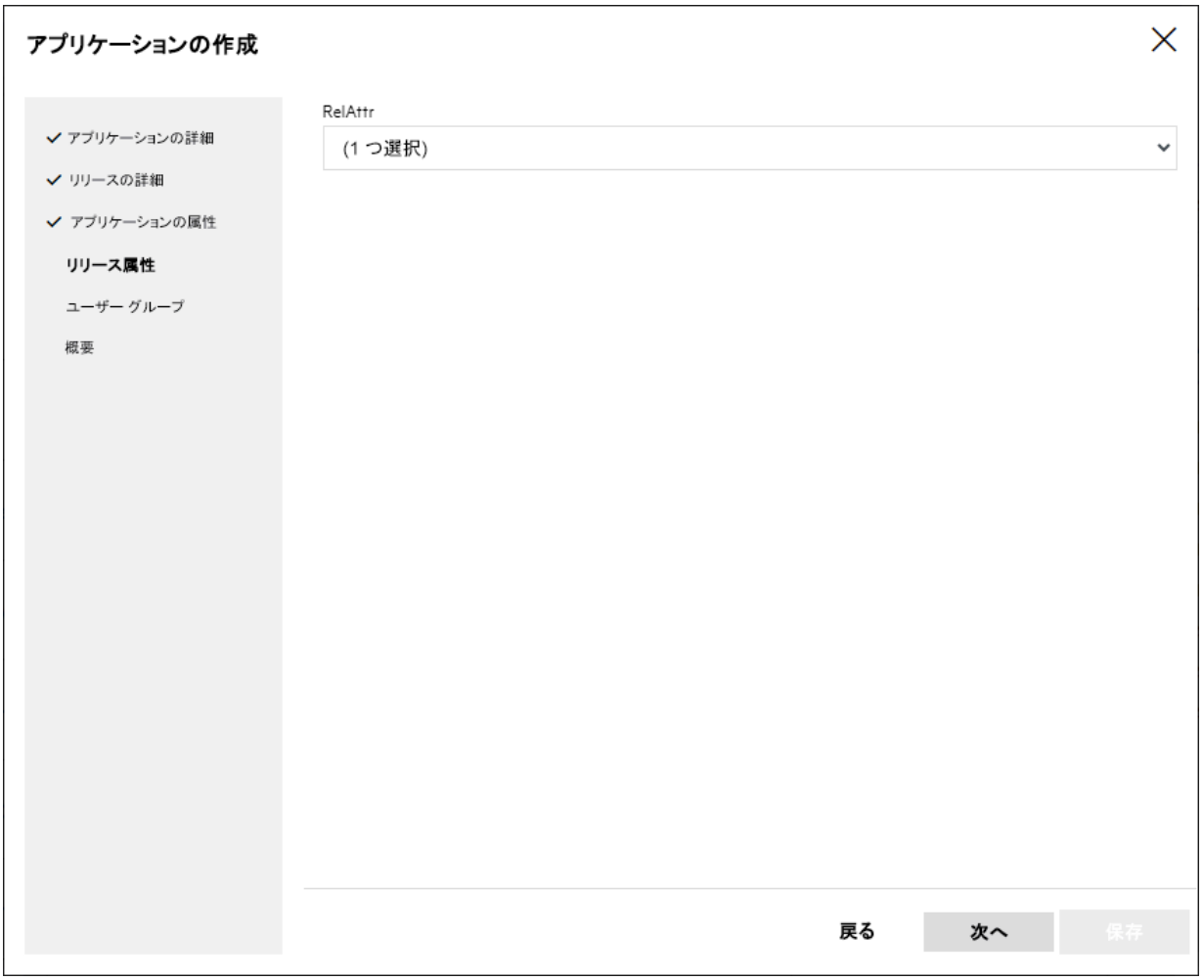
8. [**次へ**] をクリックします。
9. [**リリースの詳細**] ページで、アプリケーションのリリースを定義します。リリースは、テスト予定のアプリケーションの反復を表します。他に指示がない限り、フィールドは必須です。


アプリケーションの作成
✓ アプリケーションの詳細
✓ マイクロサービス
リリースの詳細
アプリケーションの属性
ユーザー グループ
概要
リリース名
SDLC ステータス
(1 つ選択)
マイクロサービス
(1 つ選択)
所有者
User, Test
説明
戻る
次へ
保存

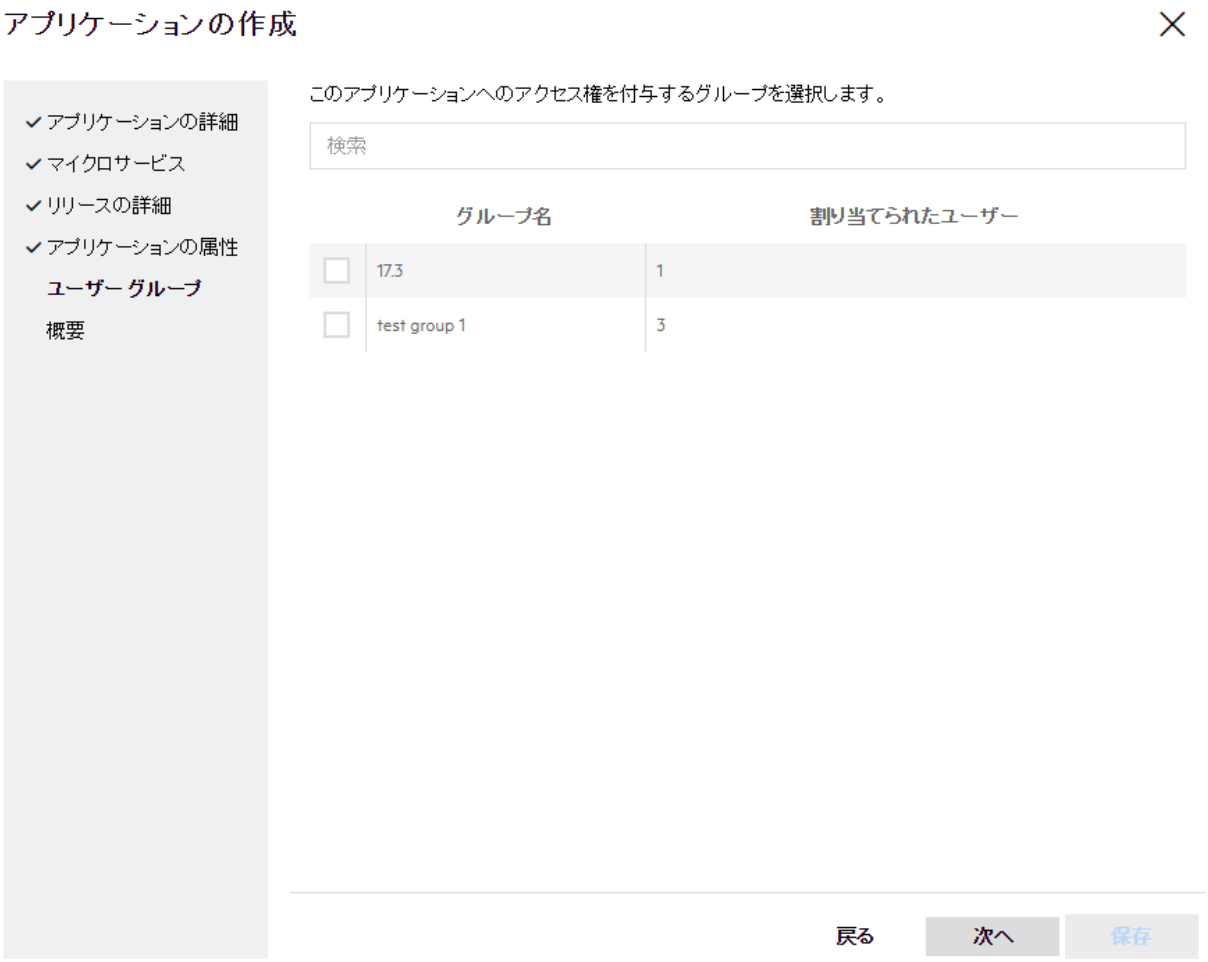
フィールド	説明
リリース名	リリース名を入力します。
SDLC ステータス	リストからソフトウェア開発ライフサイクルを選択します。[**廃棄**] オプションは利用できません。
マイクロサービス (マイクロサービスアプリケーションのみ)	リリースにリンクされるマイクロサービスをドロップ ダウン リストから選択します。リリースはマクロサービスにリンクする必要があります。
所有者	リリースから所有者を選択します。所有者には、リリースに対するスキャンステータス更新の電子メール通知が送信されます。
説明	(オプション) このリリースの説明に役立つ記述を入力します。

10. [**次へ**] をクリックします。
11. カスタム アプリケーションの属性がテナントに対して構成される場合、[**アプリケーションの属性**] ページで、アプリケーションの属性を指定します。

12. [**次へ**] をクリックします。
13. カスタム リリースの属性がテナントに対して構成される場合、[**リリースの属性**] ページで、リリースの属性を指定します。



14. テナントのユーザー グループが構成されている場合、[**ユーザー グループ**] ページで、アプリケーションにアクセスできるグループを選択します。検索ボックスを使用して、グループ名を検索できます。



15. [**次へ**] をクリックします。
16. [**概要**] ページで、アプリケーション設定を確認します。

17. [**アプリケーションの作成**] をクリックします。

    新しいアプリケーションのリリースの [概要] ページにリダイレクトされます。

1.4.2.2. アプリケーションの詳細の表示

[アプリケーションの概要] ページには、アプリケーションとそのリリースの概要が表示されます。アプリケーションのダッシュボードとして機能し、アプリケーションの本番環境セキュリティ リスクの迅速かつ包括的なスナップショットを提供します。このページでは、アプリケーションのリリースのフィルタリング、特定のリリースの検索、新しいリリースの作成、スキャンの開始を実行できます。

アプリケーションの詳細を表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 表示するアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。このページには、アプリケーションに関する詳細 (本番環境リスク、ポリシー準拠、セキュリティ ステータス、および関連するリリースのリスト (既定では完了済みの最新のスキャンから順に表示)) が表示されます。

1.4.2.2.1. [アプリケーションの概要] ページの操作

次の表に、[アプリケーションの概要] ページの操作方法を示します。

タスク	アクション
アプリケーションに適用されるセキュリティ ポリシーを表示する	[ポリシー準拠] ボックスの [**表示**] をクリックします。
アプリケーションの本番環境リリースの結合メトリックスを表示する	[**ポリシー準拠**] および [**本番環境の問題**] ボックスには、すべてのアプリケーションの本番環境リリースの星評価と問題の数が表示されます。[**重大**]、[**高**]、[**中**]、または [**低**] をクリックすると、優先度別に問題の詳細を表示できます。[アプリケーションの問題] ページでは、特定の [**インスタンス ID**] を基準にして問題を検索することもできます。
アプリケーションのセキュリティ ステータスを表示する	[**セキュリティ ステータス**] ボックスには、アプリケーションのセキュリティ ステータスが表示されます。
アプリケーションのリリースを検索する	テキスト ボックスに検索語を入力します。
リリースを作成する	[**+新規リリース**] をクリックします。
スキャンを開始する	リリースの横にある [**スキャンの開始**] をクリックし、スキャン タイプを選択します。SDLC ステータスが [**廃棄**] のリリースでは、このボタンは無効になっています。
リリースの詳細を表示する	リリース名をクリックします。
グラフを構成するデータを表示する	グラフの 1 セクションをクリックします。

タスク	アクション
リリースの最新のスキャン ステータスを表示する	該当するステータス アイコンにカーソルを合わせます。そのアイコンをクリックして、スキャン ステータスの詳細情報に直接アクセスします。  • スケジュールされたスキャンにスケジュールされた開始日が表示されます。 • 完了日は、「開始日 + 選択した評価タイプの SLO + 一時停止時間 + 週末」に基づいて計算されます。スキャンが SLO を過ぎている場合、予測される完了日には、「<release> でのスキャンに長い時間がかかります。詳しくは弊社までお問い合わせください。」と表示されます
フィルターを展開するか折りたたむ	すべて展開 | すべて折りたたむ またはフィルター名の横にある矢印をクリックします。
フィルター リストを非表示にするか表示する	をクリックします。
適用されたフィルターを削除する	[X] または [**フィルターをクリア**] をクリックします。

1.4.2.2.2. [アプリケーションの概要] ページのフィルタリング

既定では、[アプリケーションの概要] ページにはすべての結果が表示されます。表示されるデータは、フィルターを適用してカスタマイズできます。

> **Note**
>
> フィルターがフィルター リストに表示されるのは、結果にそのフィルターの複数の値が含まれている場合だけです。

[アプリケーションの概要] ページをフィルタリングするには、次の手順を実行します。

1. フィルター リストが現在表示されていない場合は、 をクリックして、フィルター リストを表示します。
2. 適用するフィルターを展開します。
3. フィルター値を選択します。次の表で、アプリケーション概要のフィルターについて説明します。

フィルター	説明	値
動的スキャンのステータス	動的スキャンのステータス	完了、キャンセル済み、進行中、未開始
モバイル スキャンのステータス	モバイル スキャンのステータス	完了、キャンセル済み、進行中、未開始
合格/不合格	ユーザー定義の合格/不合格の評価	不合格、合格
リリース作成日	リリース作成日	
スキャン タイプ	スキャンのタイプ	静的、動的、モバイル、ネットワーク、オープンソース
SDLC ステータス	リリースの SDLC ステータス	開発、QA/テスト、本番環境、廃棄
星評価	5 つ星評価システム	1、2、3、4、5
静的スキャンのステータス	静的スキャンのステータス	完了、キャンセル済み、進行中、未開始

フィルタリングの結果によりページが自動的に更新されます。適用されたフィルターは、ページの上部に表示されます。

1.4.2.3. アプリケーション設定の編集

アプリケーションが作成されたら、アプリケーション設定を編集できます。

アプリケーション設定を編集するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 編集するアプリケーションの名前をクリックします。

3. [**設定**] をクリックします。

   [設定] ページが表示されます。

4. 編集するアプリケーション設定に対応するタブを選択します。

フィールド	説明
アプリケーション名	アプリケーションの名前
ビジネス クリティカリティ	ビジネス クリティカリティ レベル
アプリケーションの種類	アプリケーションの種類 (マイクロサービス アプリケ-ションの場合は編集不可)
アプリケーションの説明	(オプション) 複数のアプリケーションの管理に役立つアプリケーションの説明
通知電子メール	(オプション) アプリケーションに関連するアクティビティの通知を受信する電子メール アドレス

- [**アプリケーションのサマリー**] タブには、アプリケーションの詳細が表示されます。
- (マイクロサービス アプリケーションのみ) [**マイクロサービス**] タブには、既存のマイクロサービスが表示されます。マイクロサービスを追加、編集、または削除したり、マイクロサービスの属性値を編集したりすることができます。

> **Note**
> リリースに関連付けられているマイクロサービスは削除できません。

- [**アプリケーションの属性**] タブには、システム属性およびカスタム属性が表示されます。

- [**バグ トラッカー**] タブには、バグ トラッカー統合の構成設定が表示されます。詳細については、「バグ トラッカーの統合」を参照してください。
- [**Application Defender**] タブには、Application Defender の統合の構成設定が表示されます。詳細については、「Fortify Application Defender の統合」を参照してください。
- [**ソース コントロール**] タブには、ソース コントロールの統合の構成設定が表示されます。詳細については、「ソース コントロールの統合」を参照してください。

5. 必要に応じて、アプリケーション設定を編集します。
6. [**保存**] をクリックします。

   アプリケーション設定が保存されます。

1.4.2.4. アプリケーションへのユーザー割り当ての管理

[**ユーザー管理**] 権限があるユーザーは、アプリケーション レベルで、アプリケーションへのユーザー アクセス権を管理できます。

> **Note**
>
> セキュリティ リーダーにはすべてのアプリケーションへのアクセス権があり、これらは削除できません。

アプリケーションへのユーザー アクセス権を管理するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. ユーザー アクセス権を編集するアプリケーションの名前をクリックします。

   [アプリケーション リリース] ページが表示されます。

3. [**アクセス**] をクリックします。

   [アプリケーションにアクセスできるユーザー] ページに、アプリケーションへのアクセス権を持つユーザーのリストが表示されます。

4. [**ユーザーの編集**] をクリックします。

   [ユーザーの割り当て] ウィンドウが表示されます。

5. 次のタスクを実行できます。

タスク	手順
アプリケーションへのユーザーの割り当て	1. [**ユーザーの編集**] をクリックします。 [ユーザーの割り当て] ウィンドウが表示されます。 2. [**使用可能**] タブを選択します。  アプリケーションに割り当てることができるセキュリティ リーダーでないユーザーの一覧が表示されます。 3. 次のアクションを実行してユーザーを選択します。 ▪ 個々のユーザーの横にあるチェック ボックスをオンにします。 ▪ [**割り当て**] チェック ボックスをオンにして、表示されているユーザーを選択します。 ▪ [**すべてのテナント ユーザーの割り当て**] チェック ボックスをオンにして、すべてのユーザーを選択します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。

タスク	手順
アプリケーションからのユーザーの削除	1. [**ユーザーの編集**] をクリックします。 [ユーザーの割り当て] ウィンドウが表示されます。 2. [**選択済み**] タブを選択します。  アプリケーションに割り当てられているセキュリティ リーダーでないユーザーの一覧が表示されます。 3. 次のアクションを実行してユーザーを削除します。 ▪ 個々のユーザーの横にあるチェック ボックスをオフにします。 ▪ [**割り当て**] チェック ボックスをオフにして、表示されているユーザーを削除します。 ▪ [**すべてのテナント ユーザーの割り当て解除**] チェック ボックスをオンにして、すべてのユーザーを削除します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。

6. [**保存**] をクリックします。

   アプリケーションに割り当てられたユーザーの変更が保存されます。

関連トピック:

ユーザー レベルでアプリケーションへのユーザー アクセス権を管理するには、「ユーザーのアプリケーション割り当ての管理」を参照してください。

1.4.2.5. アプリケーションのイベント ログの表示

[**アプリケーションの管理**] 権限があるユーザーは、アプリケーションのイベント ログを表示できます。アプリケーションのイベント ログには、アプリケーションに関連するすべてのイベントが記録されます。

- アプリケーションの作成、更新、削除
- リリースの作成、更新、削除
- アプリケーションへのユーザーおよびグループ アクセスの追加と削除
- スキャンの開始、更新、完了
- 使用権の消費
- レポートの作成、発行、ダウンロード、削除
- FPR のダウンロード
- データ エクスポート
- 高度な監査設定の作成、更新、削除

アプリケーションのイベント ログを表示するには、次の手順を実行します。

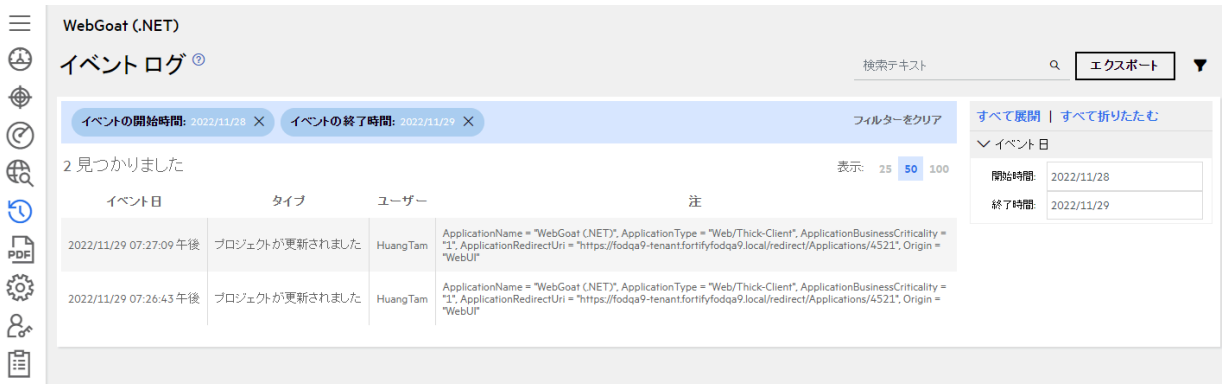
1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. イベント ログを表示するアプリケーションの名前をクリックします。

3. [**イベント ログ**] をクリックします。

   [イベント ログ] ページが表示されます。



4. 次のタスクを実行できます。

タスク	アクション
過去 13 か月のイベント ログをエクスポートする	[**エクスポート**] をクリックします。.csv ファイルがブラウザーの設定で指定したフォルダーにローカルに保存されます。
イベント ログを検索する	検索テキスト フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。
フィルター リストを非表示にするか表示する	をクリックします。
フィルターを展開するか折りたたむ	すべて展開 | すべて折りたたむ またはフィルター名の横にある矢印をクリックします。
適用されたフィルターを削除する	ページの上部にある [**X**] をクリックするか、[**フィルターをクリア**] をクリックします。既定では、フィルターは過去 24 時間に設定されています。

関連トピック

ポータルで発生したすべてのイベントの表示については、「管理イベント ログへのアクセス」を参照してください。

1.4.2.6. アプリケーションの削除

アプリケーションを削除すると、アプリケーションに関連付けられているすべてのデータが削除され、取り消すことはできません。アプリケーション データは、72 時間後に OpenText Fortify on Demand からパージされます。アプリケーションが誤って削除された場合は、アプリケーションが削除されてから 72 時間以内にサポートに連絡してください。

Note
削除されたアプリケーションの名前を再利用する必要がある場合は、アプリケーションが削除されてから 72 時間経過してから新しいアプリケーションを作成します。

アプリケーションを削除するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 削除するアプリケーションをクリックします。

3. [**設定**] をクリックします。
   [**アプリケーションのサマリー**] ページが表示されます。

4. [**X アプリケーションの削除**] をクリックします。

   確認メッセージが表示されます。

5. [**はい**] をクリックしてアプリケーションを削除します。

   [アプリケーション] ページに戻ります。

1.4.3. リリースの管理

リリースをユーザー権限に応じて作成、表示、編集することができます。

このセクションでは、次のトピックについて説明します。

- リリースの作成
- リリース詳細の表示
- リリースのセキュリティ ポリシーの上書き
- リリース設定の編集
- リリースの削除

1.4.3.1. リリースの作成

既存のアプリケーションの新しいリリースを作成できます。新しいリリースを作成する場合、まったく新しいリリースを開始するか、脆弱性およびその他の詳細を以前のリリースから受け継ぐことができます。

新しいリリースを作成するには、次の手順を実行します。

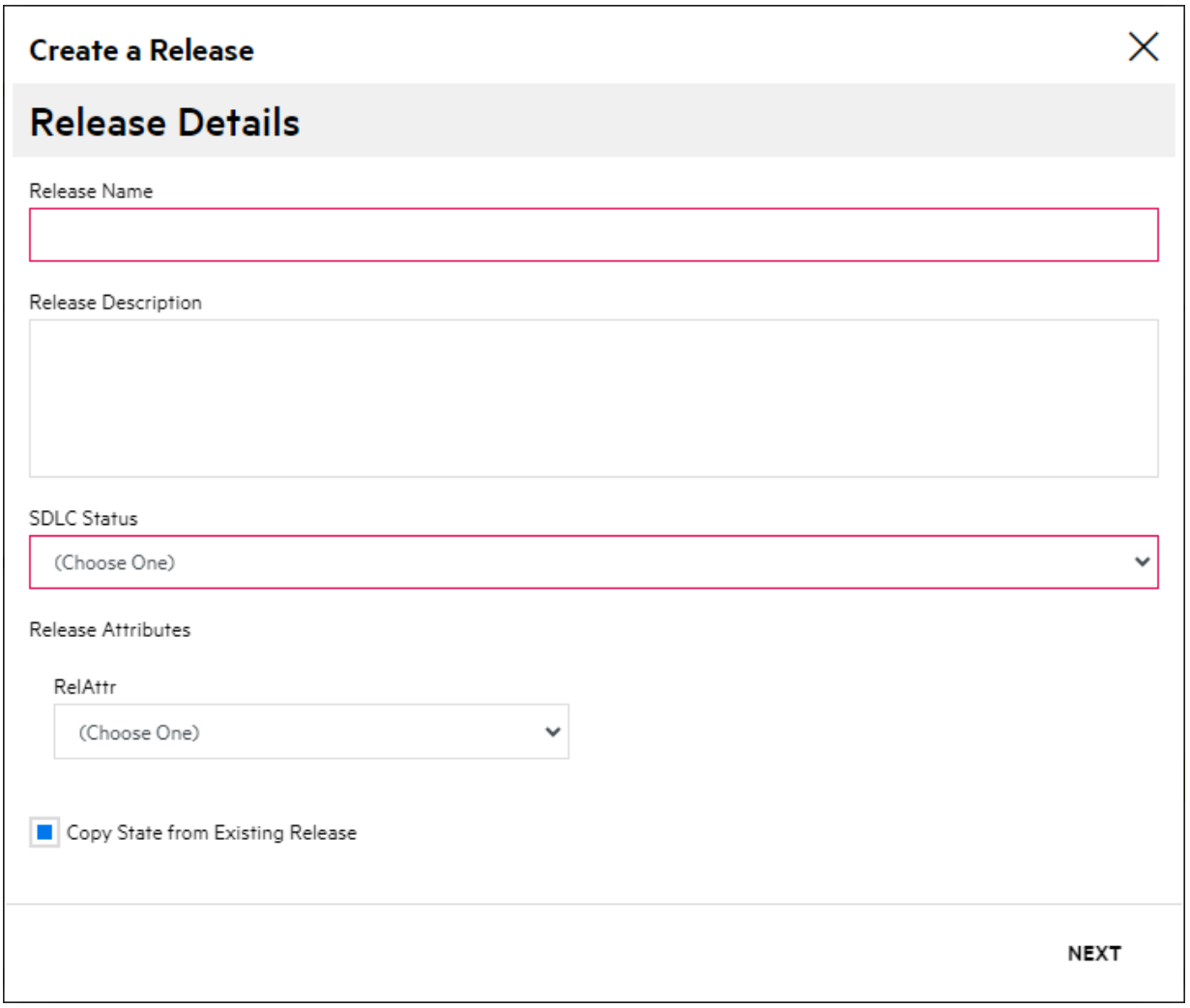
1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 新しいリリースを作成するアプリケーションをクリックします。

3. [**+ 新規リリース**] をクリックします。

   [リリースの作成] ウィザードが表示されます。



4. [**リリースの詳細**] ページで、必要に応じてフィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
リリース名	リリース名を入力します。
リリースの説明	(オプション) リリースの説明に役立つ記述を入力します。
SDLC ステータス	リリースのソフトウェア開発ライフサイクル ステージ [**開発**]、[**QA/テスト**]、[**本番環境**] を選択します。[**廃棄**] オプションは利用できません。
リリース属性	リリースの属性を指定します。
マイクロサービス (マイクロサービス アプリケーションのみ)	リリースにリンクされるマイクロサービスをドロップ ダウン リストから選択します。リリースはマイクロサービスにリンクする必要があります。マイクロサービスは複数のリリースにリンクすることができます。

フィールド	説明
既存のリリースから状態をコピー	(オプション、既定で選択されている) [**既存のリリースから状態をコピー**] を選択して、データを以前のリリースから新しいリリースに受け継ぎます。次のデータがコピーされます：リリース所有者、すべてのスキャン タイプのスキャン設定、星評価、問題数、および問題の詳細 (問題の履歴、バグ トラッカー リンク、添付されたスクリーンショットなど)。 **Note** 完了してインポートされたスキャンのデータがコピーされます。一時停止したスキャンと進行中のスキャンのデータ (スキャン設定を含む) はコピーされません。検証済みの修正の問題はコピーされません。

5. [**既存のリリースから状態をコピー**] を選択している場合は、[**次へ**] をクリックします。そうでない場合は、手順 7 に進みます。

6. [**既存のリリースから状態をコピー**] ページで、リストから脆弱性とその他の詳細を引き継ぐリリースを選択します。
7. [**保存**] をクリックします。

   新しいリリースの [概要] ページにリダイレクトされます。

> **Note**
> 以前のリリースからコピーすることを選択した場合、リリース データのコピー プロセスによって画面の更新が遅くなり、[概要] ページがすぐに表示されないことがあります。

1.4.3.2. リリース詳細の表示

[リリースの概要] ページには、リリースの概要がダッシュボード形式で表示され、リリースのセキュリティ リスクに関する、迅速かつ包括的なスナップショットが提供されます。わかりやすい視覚情報により、リリースに関する主要指標を確認できます。視覚的要素の多くはインタラクティブで、表示されるデータ セットにドリルダウンできます。

リリースの詳細を表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

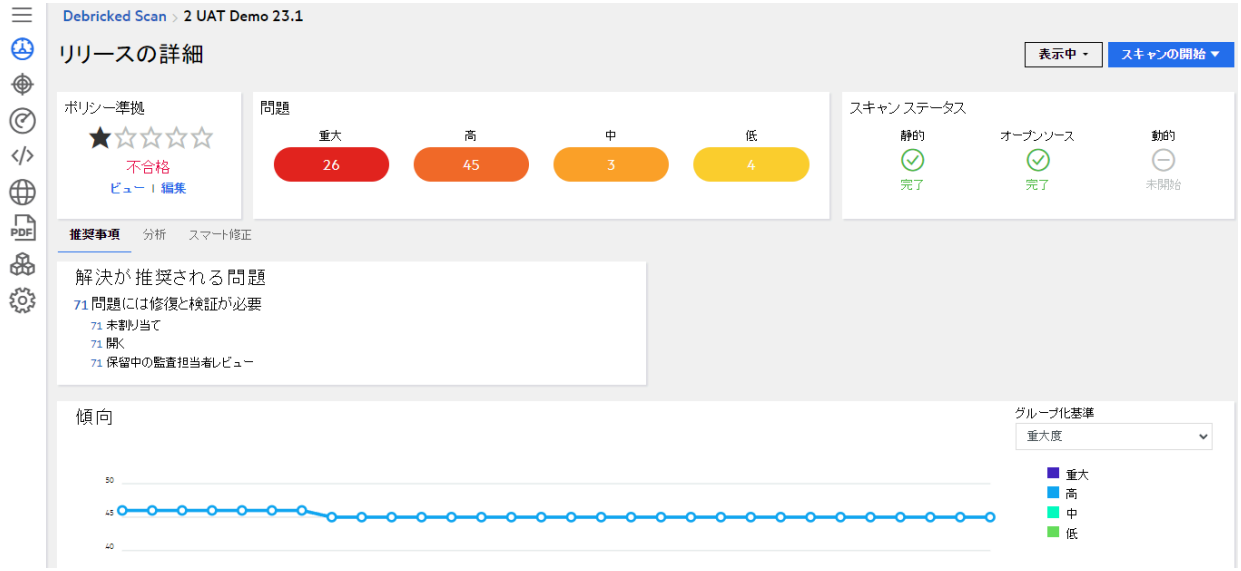
   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. 表示するリリースの名前をクリックします。

   [リリースの概要] ページが表示されます。

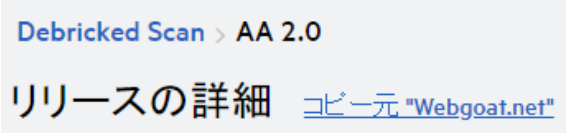


   [リリースの概要] ページの上部のセクションには、リリースのスキャン結果が要約されています。

   - [ポリシー準拠] ボックスには、星評価と合格/不合格のステータスが表示されます。
   - [問題] ボックスには、各重大度レベルの脆弱性の数が表示されます。[**重大**]、[**高**]、[**中**]、または [**低**] をクリックすると、優先度別に問題の詳細を表示できます。[リリースの問題] ページでは、特定の [**インスタンス ID**] を基準にして問題を検索することもできます。

- [スキャン ステータス] ボックスには、リリースの最新のスキャン ステータスが表示されます。
- タブには、問題へのドリルダウンのリンクを含む、スキャン結果が視覚表現で表示されます。

次の表に、[リリースの概要] ページの操作方法を示します。

タスク	アクション
ソースの状態のコピーを表示する (該当する場合)	リリース名の下にあるリンクをクリックします。 
修正済みの問題を表示または非表示にする	**[表示] > [修正済み]** を選択して、[検証済みの修正] の問題の表示と非表示を切り替えます。
抑制された問題を表示または非表示にする	**[表示] > [抑制済み]** を選択して、[誤検知を確認済み] と [抑制済み] の問題の表示と非表示を切り替えます。
スキャンを開始する	[**スキャンの開始**] をクリックして、リストからスキャン タイプを選択します。SDLC ステータスが [**廃棄**] のリリースでは、このボタンは無効になっています。
アプリケーションに適用されるセキュリティ ポリシーを表示する	[ポリシー準拠] ボックスの [**表示**] をクリックします。
ポリシー準拠を上書きする	[ポリシー準拠] ボックスの [**編集**] をクリックします。

タスク	アクション
リリースの最新のスキャン ステータスを表示する	該当するステータス アイコンにカーソルを合わせます。そのアイコンをクリックして、スキャン ステータスの詳細情報に直接アクセスします。  ◦ スケジュールされたスキャンにスケジュールされた開始日が表示されます。 ◦ 完了日は、「開始日 + 選択した評価タイプの SLO + 一時停止時間 + 週末」に基づいて計算されます。スキャンが SLO を過ぎている場合、予測される完了日には、「<release> でのスキャンに長い時間がかかります。詳しくは弊社までお問い合わせください。」と表示されます
問題の重大度またはスキャン タイプでフィルタリングされた問題をドリルダウンする	[問題] および [スキャン ステータス] ボックスの視覚的要素をクリックします。
スキャン結果の視覚表現を選択してさらに分析する	タブを選択します。詳細については、「[リリースの概要] のグラフ」を参照してください。

1.4.3.2.1. [リリースの概要] のグラフ

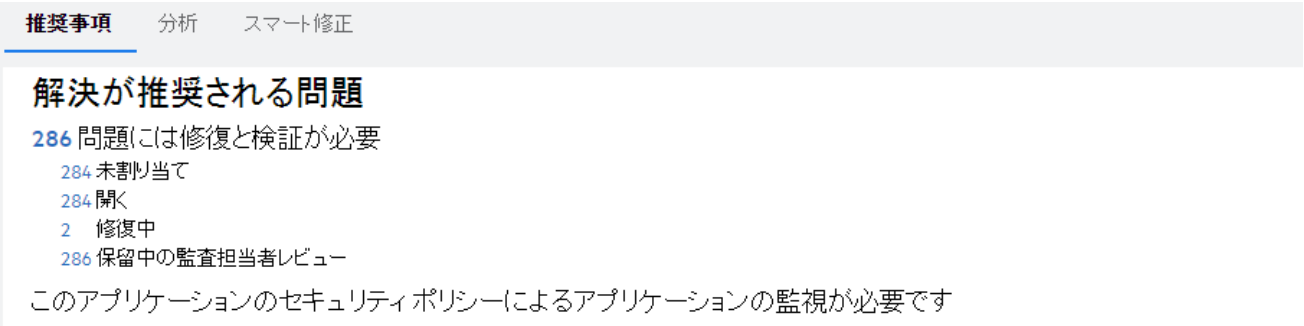
[リリースの概要] ページのタブでは、スキャン結果および問題へのドリルダウンのリンクが視覚的に表現されます。

- 推奨事項
- 分析
- スマート修正 (静的スキャン)
- アプリ情報 (モバイル スキャン)
- 評価 (モバイル スキャン)

> **Note**
>
> 修正済みの問題および抑制済みの問題を表示すると、脆弱性の数が増えます。更新された数は、脆弱性グラフにも表示されます。

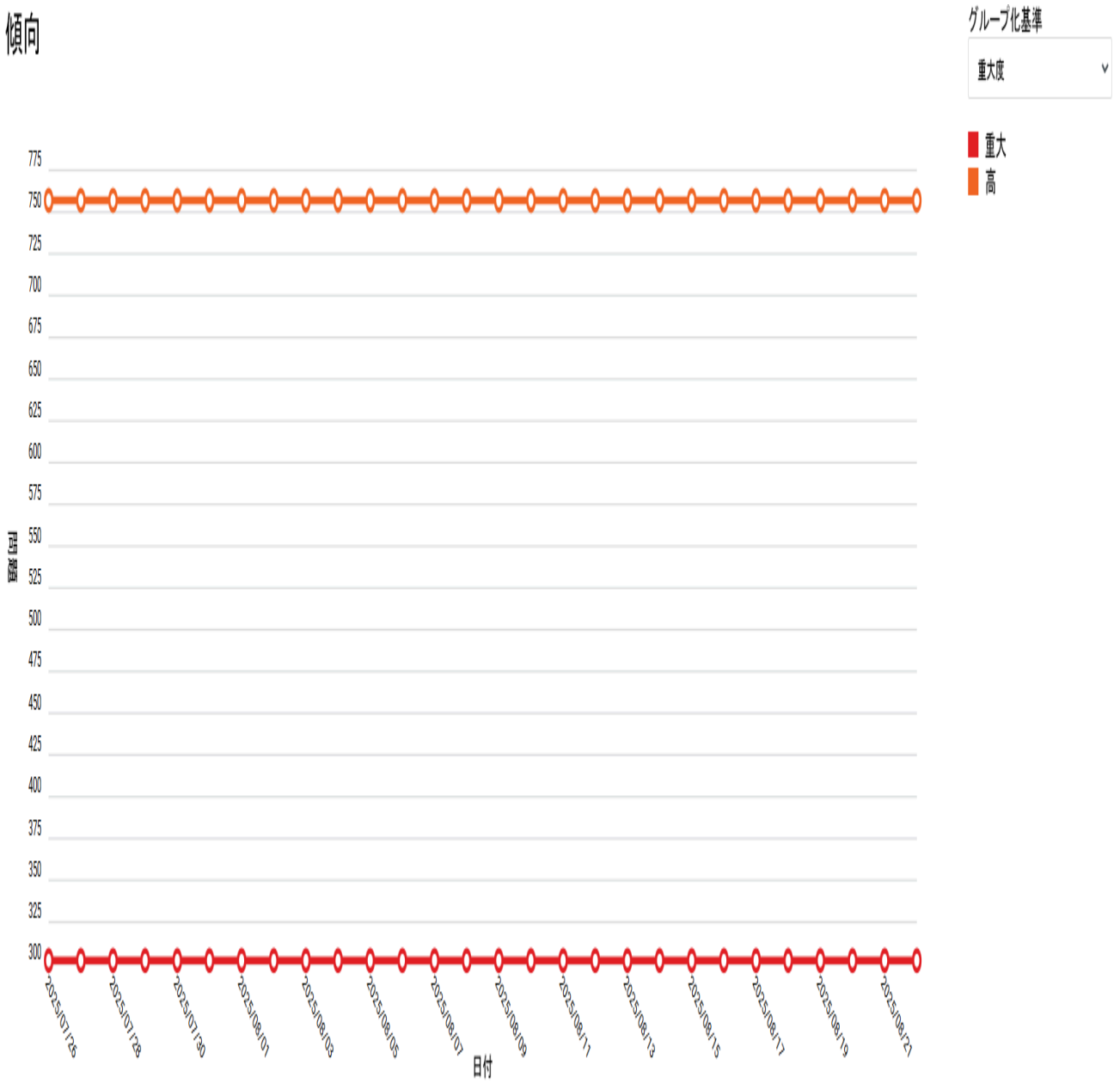
推奨事項

[解決が推奨される問題] セクションには、リリースがセキュリティ ポリシーに違反している理由がリストされます。特定の問題が原因でリリースが不合格になっている場合、それらの問題を直接表示できます。スキャン頻度を最小限に抑えることがポリシーで要求されている場合、その情報もここに表示されます。合格しているリリースやスキャン頻度の要件がないリリースの場合、このセクションは表示されません。



[傾向] セクションには、選択したファセットに関して測定されたリリースの脆弱性のトレンドが時間の経過とともに折れ線グラフで表示されます。数とタイプを表示するデータ ポイントにカーソルを置きます。データ セットの表示と非表示を切り替えるには、ラベルをクリックします。

傾向


グループ化基準
重大度
重大
高
775
750
725
700
675
650
625
600
575
550
525
500
475
450
425
400
375
350
325
300
問題
2025/07/26
2025/07/28
2025/07/30
2025/08/01
2025/08/03
2025/08/05
2025/08/07
2025/08/09
2025/08/11
2025/08/13
2025/08/15
2025/08/17
2025/08/19
2025/08/21
日付

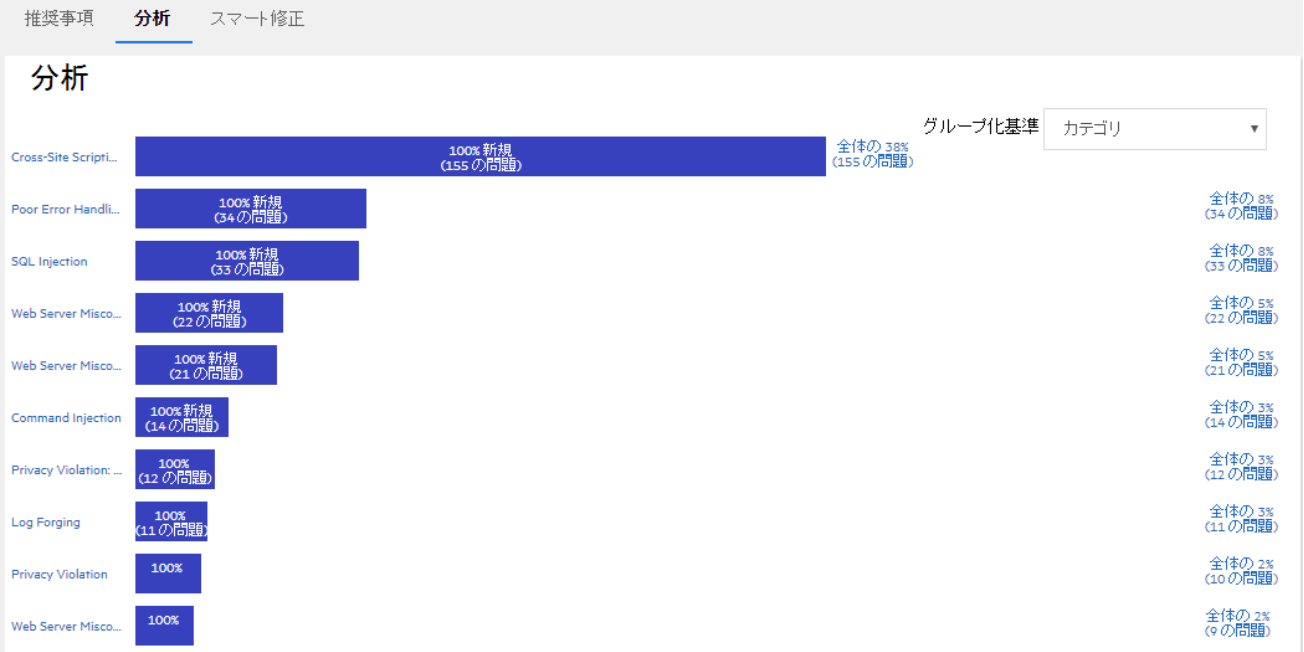
ファセット	説明
監査担当者ステータス	問題の監査担当者ステータス
CWE 上位 25 件 2023	CWE (Common Weakness Enumeration) 上位 25 件 2023 の分類
CWE 上位 25 件 2024	CWE (Common Weakness Enumeration) 上位 25 件 2024 の分類
CWE 上位 25 件 2025	CWE (Common Weakness Enumeration) 上位 25 件 2025 の分類
開発者ステータス	問題の開発者ステータス
FISMA (廃止予定)	FISMA の分類
GDPR	Fortify Software Security Research (SSR) からの GDPR の分類
割り当て済み	問題の割り当てステータス: [**誤**]、[**正**]
終了済み	問題の解決ステータス: [**誤**]、[**正**]
問題のステータス	問題のステータス: [**新規**]、[**既存**]、[**再発**]、[**修正済み**]
抑制済み	問題の抑制ステータス: [**誤**]、[**正**]
分野	Seven Pernicious Kingdoms の分類
NIST SP 800-53 Rev 5	National Institute of Standards and Technology Special Publication 800-53
OWASP ASVS 4.0	OWASP ASVS 4.0 の分類
OWASP ASVS 5.0	OWASP ASVS 5.0 の分類
OWASP 2017	OWASP 2017 の上位 10 件の分類

ファセット	説明
OWASP 2021	OWASP 2021 の上位 10 件の分類
OSWAP 2023	OWASP API Top 10 2023 の分類
OSWAP 2025	OWASP 2025 の上位 10 件の分類
OWASP LLM 2025	OWASP LLM 上位 10 件 2025 の分類
OWASP 2014 Mobile Top 10、OWASP 2024 Mobile Top 10	OWASP Mobile Top 10 の分類
PCI40	PCI 4.0 の分類
PCIDSS401	PCI 4.0.1 の分類
PCISSF12	PCI SSF バージョン 1.2
スキャン タイプ	問題のスキャン タイプ: **静的**、**動的**、**モバイル**
重大度	問題の重大度: [**重大**]、[**高**]、[**中**]、[**低**]
STIG52	DISA STIG 5.2 の分類
STIG53	DISA STIG 5.3 の分類
STIG61	DISA STIG 6.1 の分類
STIG62	DISA STIG 6.2 の分類
STIG63	DISA STIG 6.3 の分類
STIG64	DISA STIG 6.4 の分類

分析

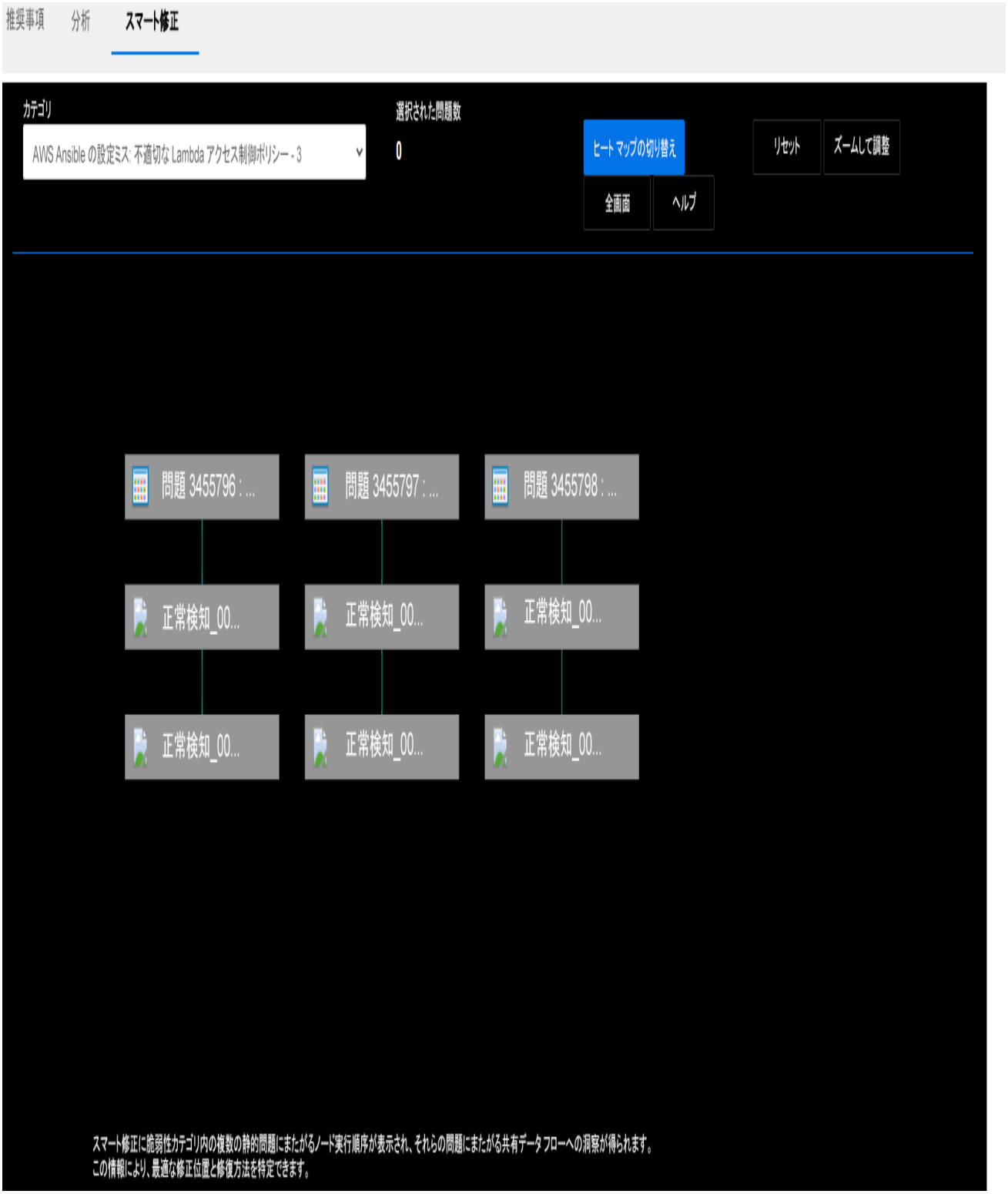
[分析] タブには、グループに分類されたリリースの脆弱性の棒グラフが表示されます。表示されるカテゴリは、選択した集計ファセット ([**割り当て**]、[**監査担当者ステータス**]、[**カテゴリ**]、[**開発者ステータス**]、[**スキャン タイプ**]、および [**OWASP 13**]) によって異なります。

グラフのいずれかの棒をクリックして、グループの詳細情報を表示します。たとえば、[**カテゴリ**] ファセットの [**プライバシーの侵害**] をクリックすると、プライバシー侵害の脆弱性を表示するフィルタリングされた [問題] ページにリダイレクトされます。



スマート修正 (静的スキャン)

[**スマート修正**] タブは、静的スキャンが実行されると使用できるようになります。このタブには、脆弱性カテゴリの静的問題におけるノード実行順序を視覚化する分析トレース図が表示され、問題の共有データ フローに関する洞察が得られます。この情報により、最適な修正位置と修復方法を特定できます。



[**カテゴリ**] リストで脆弱性カテゴリを選択して、分析トレース図を表示します。図は、以下の方法で操作できます。

- 上にスクロールして拡大するか、下にスクロールして縮小する。
- ノードをクリックして共有パスを強調表示する。
- 問題アイコンをクリックして、問題にドリルダウンする。
- ツールバーのコマンドを使用して図を操作する。

- **ヒート マップの切り替え**: データ フローの強調表示を有効/無効にします。
- **除去**: (ノードが選択されているときに使用可能): 問題フロー図を、選択した問題の統合データ フローに絞り込みます。
- **リセット**: 選択した問題カテゴリの既定のビューに図をリセットします。
- **ズームして調整**: リセットまたは除去することなく表示に合わせて図全体のサイズを変更します。
- **全画面**: 全画面モードで図を展開します。

アプリ情報 (モバイル スキャン)

[**アプリ情報**] タブには、プラットフォーム、アプリケーション名、識別子 (パッケージ名)、バージョン、ファイル サイズ、最小 OS 要件、デバイス要件など、モバイル アプリケーションのバイナリ ファイルに関する情報が表示されます。

評価 (モバイル スキャン)

OpenText Fortify on Demand のモバイル評価サービスでは、モバイル アプリケーションのテスト時に発見されたトラフィック エンドポイントの評価分析を実行します。[**評価**] タブには、分析結果が表示されます。識別されたすべてのホストと、それぞれが優良な状態であるかどうかの一覧が表示されます。モバイル スキャン結果には、優良な状態でないことが識別されたホスト専用の脆弱性も含まれます。

1.4.3.3. リリースのセキュリティ ポリシーの上書き

セキュリティ リーダーは、リリースを合格または不合格として設定することで、リリースのセキュリティ ポリシーを手動で上書きできます。この機能を使うと、人為的に問題を抑制しなくても、ポータルで実際の例外処理を反映できます。例外の理由は、アプリケーションのイベント ログに記録されます。リリースのステータスは、次回のスキャンで正式なセキュリティ ポリシーに自動的に戻ります。

リリースのセキュリティ ポリシーを上書きするには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

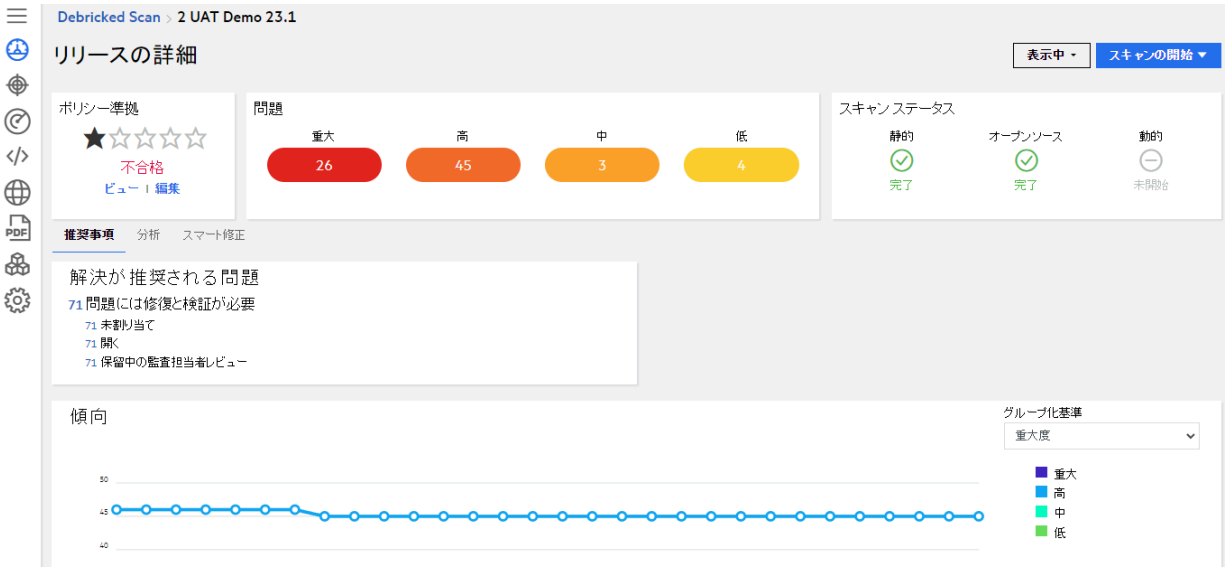
   [アプリケーション] ページが表示されます。

2. 編集するリリースを含むアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. セキュリティ ポリシーを上書きするリリースの名前をクリックします。

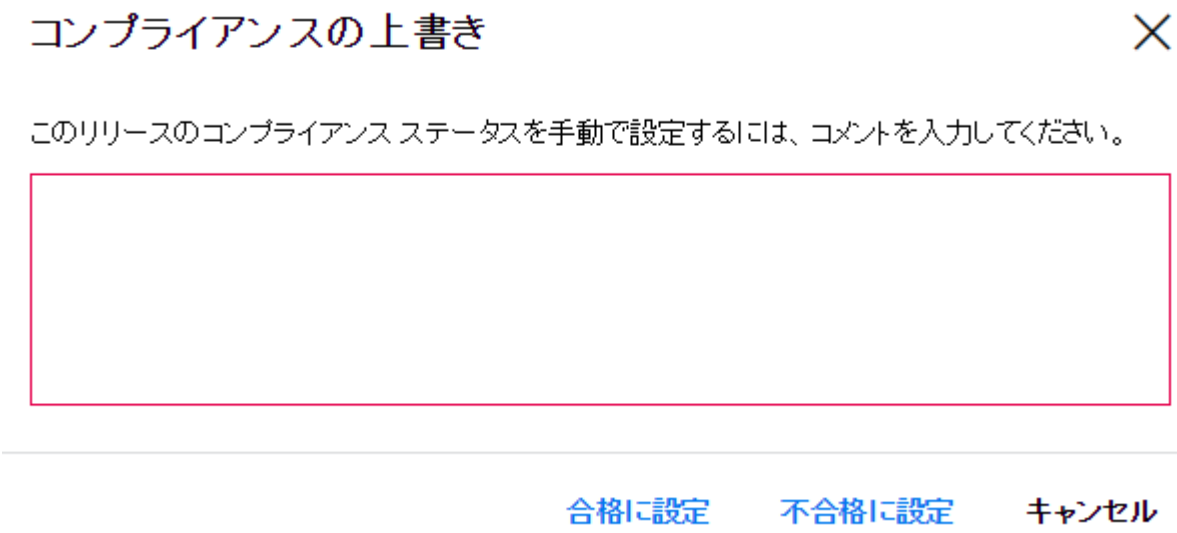
   [リリースの概要] ページが表示されます。



4. [ポリシー準拠] ボックスの [**編集**] をクリックします。

   [コンプライアンスの上書き] モーダル ウィンドウが表示されます。

5. フィールドにポリシー コンプライアンス結果を変更する正当な理由を入力します。



6. [**合格に設定**] または [**不合格に設定**] をクリックします。

   [リリースの概要] ページに戻ります。ポリシーの上書きが、[ポリシー準拠] ボックスに表示されます。

関連トピック:

- 星評価については、「5 つ星評価」を参照してください。
- セキュリティ ポリシーの管理については、「ポリシー管理」を参照してください。

1.4.3.4. リリース設定の編集

リリースが作成されたら、リリース設定を編集できます。

リリースの設定を編集するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

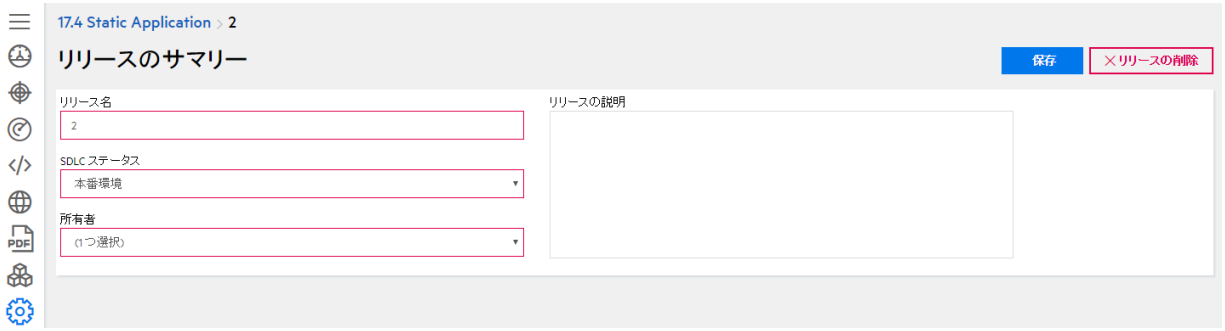
2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページに、使用しているリリースのリストが表示されます。

3. 編集するリリースを選択します。

4. [**設定**] をクリックします。

   [リリースの概要] ページが表示されます。



5. 必要に応じて [リリースのサマリー] ページを編集します。他に指示がない限り、フィールドは必須です。

フィールド	説明
リリース名	リリースの名前
マイクロサービス	(マイクロサービス アプリケーションのみ) リリースにリンクされているマイクロサービスの名前
SDLC ステータス	リリースのソフトウェア開発ライフサイクル ステージ
所有者	リリースに対するスキャン ステータス更新の電子メール通知を受信するリリースの所有者
Debricked のオープン ソースのスキャンを実行します	(Sonatype 使用権を持つテナントで利用可能) ソフトウェア構成分析ツールを Sonatype から OpenText Core SCA に切り替えるには、このチェックボックスをオンにします。一度設定を保存すると、元に戻すことはできません。切り替え後に OpenText Core SCA スキャンを正常に実行するには、テナントにアクティブな OpenText Core SCA 使用権が必要です。 **Note** テナントに非アクティブな Sonatype 使用権とアクティブな OpenText Core SCA 使用権がある場合、オープン ソース スキャンには OpenText Core SCA が利用されます。
リリースの説明	(オプション) リリースの内容を表す説明です。

6. [**保存**] をクリックして変更を保存します。

1.4.3.5. リリースの削除

[**アプリケーションの作成**] 権限を持つユーザーは、リリースを削除できます。リリースを削除すると、リリースに関連付けられているすべてのデータが削除され、取り消すことはできません。リリースのデータは、72 時間後に OpenText Fortify on Demand からパージされます。リリースが誤って削除された場合は、リリースが削除されてから 72 時間以内にサポートに連絡してください。

Note
削除されたリリースの名前を再利用する必要がある場合は、リリースが削除されてから 72 時間経過してから新しいリリースを作成します。

リリースを削除するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページに、使用しているリリースのリストが表示されます。

3. 削除するリリースをクリックします。

4. [**設定**] をクリックします。

5. [**x リリースの削除**] をクリックします。

6. **[はい]** をクリックします。

   [リリースの概要] ページに戻ります。

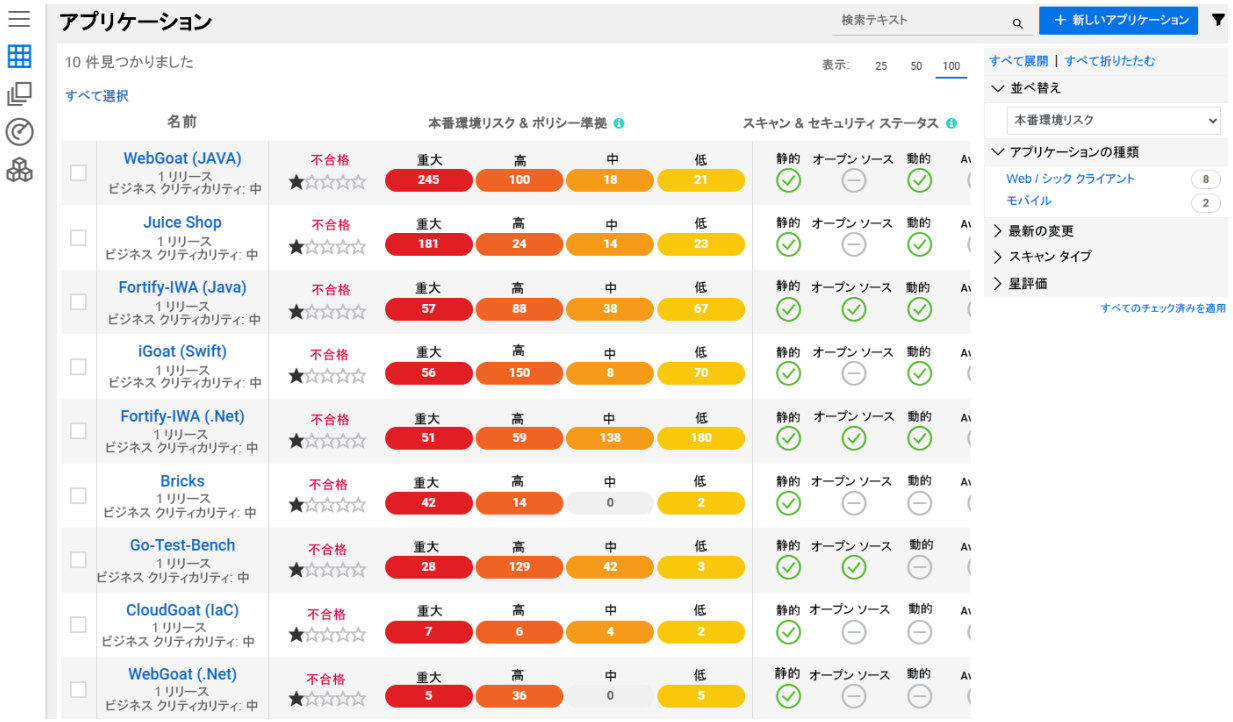
1.4.4. テナントのアプリケーションの表示

複数のアプリケーションのセキュリティ ステータスを同時に確認することができます。[アプリケーション] ページは、OpenText Fortify on Demand にログインした後のデフォルトのランディング ページです。本番リリースのリスクとポリシー準拠に重点を置いた、アプリケーションの概要が表示されます。

[アプリケーション] ページを表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

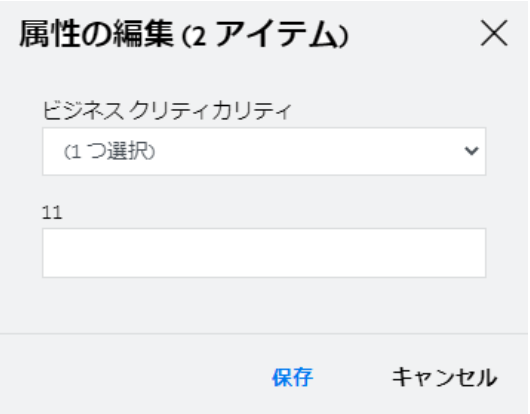
   [アプリケーション] ページが表示されます。グリッドには、各アプリケーションの詳細として、アプリケーション名、リリースの数、ビジネス クリティカリティ、すべての本番環境リリースの星評価と問題の数、すべてのリリースにまたがる最新スキャン ステータス、リスク関連の最新の変更が表示されます。

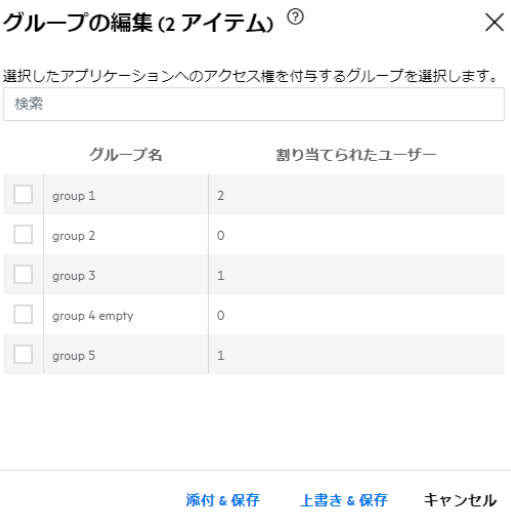


1.4.4.1. [アプリケーション] ページの操作

次の表に、[アプリケーション] ページの操作方法を示します。

タスク	アクション
アプリケーションを作成する	[**+ 新しいアプリケーション**] をクリックします。
アプリケーション リストを検索する	検索テキスト ボックスにキーワードまたは語句を入力して、**Enter** キーを押します。検索結果を削除するには、検索ボックスのテキストを削除して **Enter** キーを押すか、適用されたフィルターを削除します。 検索テキスト ボックスの使用については、「アプリケーションおよびリリースの検索」を参照してください。
フィルター リストを非表示にするか表示する	をクリックします。
フィルターを展開するか折りたたむ	[**すべて展開**]、[**すべて折りたたむ**] またはフィルター名の横にある矢印をクリックします。
フィルターの適用	フィルター名の下にある目的のフィルター値を選択します。フィルタリングの結果によりページが自動的に更新されます。一部のフィルターについては、[**適用**] をクリックしてページを更新します。
適用されたフィルターを削除する	適用された各フィルターの横にある [**X**] をクリックするか、[**フィルターをクリア**] をクリックします。
マイクロサービスの指定によりアプリケーションをフィルタリングする	目的のタブを選択します。 

タスク	アクション
複数のアプリケーションのアプリケーション属性を編集する	1. 個々のアプリケーションの横にあるチェック ボックスをオンにするか、[**すべて選択**] をクリックしてページ上のすべてのアプリケーションを選択します。 2. [**属性の編集**] をクリックします。 [属性の編集] ウィンドウが開きます。  3. 必要に応じてフィールドを更新します。 4. [**保存**] をクリックします。 アプリケーションの属性については、「アプリケーションの作成」を参照してください。

タスク	アクション
複数のアプリケーションのユーザー グループを編集する	1. 個々のアプリケーションの横にあるチェック ボックスをオンにするか、[**すべて選択**] をクリックしてページ上のすべてのアプリケーションを選択します。 2. [**グループの編集**] をクリックします。 [グループの編集] ウィンドウが開きます。  3. アプリケーションに割り当てるグループを選択します。 4. 選択したグループを既存の割り当て済みグループに追加するには、[**添付 & 保存**] をクリックします。既存の割り当て済みグループを選択したグループと置き換えるには、[**上書き & 保存**] をクリックします (ユーザー グループが選択されていない場合、既存の割り当て済みグループがすべて削除されます)。

タスク	アクション
	 **Note** [**上書き & 保存**] を使用するには、[**アプリケーションの管理**] 権限および [**すべてのアプリケーションのアクセス**] 権限の両方がユーザーに必要です。 グループの詳細については、「グループ」を参照してください。
アプリケーションの詳細を表示する	アプリケーション名をクリックします。
アプリケーションに適用されるセキュリティ ポリシーを表示する	星評価をクリックします。
アプリケーションの本番環境リリースの結合メトリックスを表示する	[**本番環境リスク & ポリシー準拠**] 列には、特定のアプリケーションの本番環境リリースの星評価と問題の数が表示されます。

タスク	アクション
アプリケーションのリリース全体の最新のスキャン ステータスを表示する	該当するステータス アイコンにカーソルを合わせます。そのアイコンをクリックして、スキャン ステータスの詳細情報に直接アクセスします。  • スケジュールされたスキャンにスケジュールされた開始日が表示されます。 • 予測される完了日は、「スキャン開始日 + 選択した評価タイプの SLO + 一時停止時間 + 週末」に基づいて計算されます。スキャンが SLO を過ぎている場合、予測される完了日には、「スキャンに長い時間がかかります。詳しくは弊社までお問い合わせください。」と表示されます
アプリケーションのリスク関連の最新の変更を表示する	[**最新の変更**] 列には、以下のリストからの最新の変更が表示されます。 • リスク プロファイルが更新されました • リリースが作成されました • リリースが本番環境に展開されました • 新しい動的脆弱性が検出されました • 新しい静的脆弱性が検出されました • 新しいモバイルの脆弱性が検出されました • ビジネス クリティカリティが更新されました • リリース合格セキュリティ ポリシー • リリース失敗セキュリティ ポリシー

1.4.4.2. [アプリケーション] ページのフィルタリング

既定では、[アプリケーション] ページには、すべてのアプリケーションが次の基準に基づいて上から順に並べられます。

- 降順に並べ替えられたアプリケーションが属するグループ:
  - 本番環境: 1 つ以上の本番環境リリースを持つアプリケーション (合格/不合格ステータスが不合格 > 未評価 > 合格の順に並べ替え)
  - 本番前: 1 つ以上の開発リリースまたは QA リリースを持つアプリケーション
  - 廃棄: 本番環境、開発、QA のいずれのリリースも持たないアプリケーション
- 各グループ (本番環境、本番前、廃棄) 内では、アプリケーションはビジネス クリティカリティ (高い順)、次に問題の数、重大度に基づいて並べられます

フィルターを適用すると、表示するアプリケーションを制限し、並べ替えの順序を変更できます。[アプリケーション] ページでは次のフィルターを使用できます。

Note

フィルターがフィルター リストに表示されるのは、結果にそのフィルターの複数の値が含まれている場合だけです。

フィルター	説明	値
アプリケーションの種類	アプリケーション作成時に選択されたアプリケーションの種類。	モバイル、Web / シック クライアント
ビジネス クリティカリティ	アプリケーションのビジネス クリティカリティ	高、中、低
マイクロサービスの有無	アプリケーションにマイクロサービスがあるかどうか	誤、正
動的スキャンのステータス	動的スキャンのステータス	スケジュール済み、進行中、完了、キャンセル済み、待機中
モバイル スキャンのステータス	モバイル スキャンのステータス	スケジュール済み、進行中、完了、キャンセル済み、待機中
最新の変更	アプリケーションで検出された最新の変更のカテゴリ	新しい監視の脆弱性が検出されました、リリース合格セキュリティ ポリシー、ビジネス クリティカリティが更新されました、リリースが作成されました、新しい動的脆弱性が検出されました、リリース失敗セキュリティ ポリシー
合格/不合格	ユーザー定義の合格/不合格の評価	不合格、合格、未評価
スキャン タイプ	スキャン タイプ	静的、動的、モバイル、オープン ソース

フィルター	説明	値
並べ替え	並べ替えの順序	[本番環境リスク] (既定)、[最新の変更]、[アプリケーション名 (A～Z)]、および [アプリケーション名 (Z～A)]
星評価	5 つ星評価システム	1、2、3、4、5
静的スキャンのステータス	静的スキャンのステータス	進行中、完了、キャンセル済み、待機中
<カスタム アプリケーションの属性>	選択リストになっているアプリケーションの属性	ユーザー定義
<カスタム マイクロサービスの属性>	選択リストになっているマイクロサービスの属性	ユーザー定義

1.4.5. テナントのリリースの表示

複数のアプリケーションを一度にレビューできるだけでなく、複数のアプリケーションの個々のリリースの詳細を同時に確認することもできます。[ご使用のリリース] ページには、OpenText Fortify on Demand のリリースの概要が表示されます。

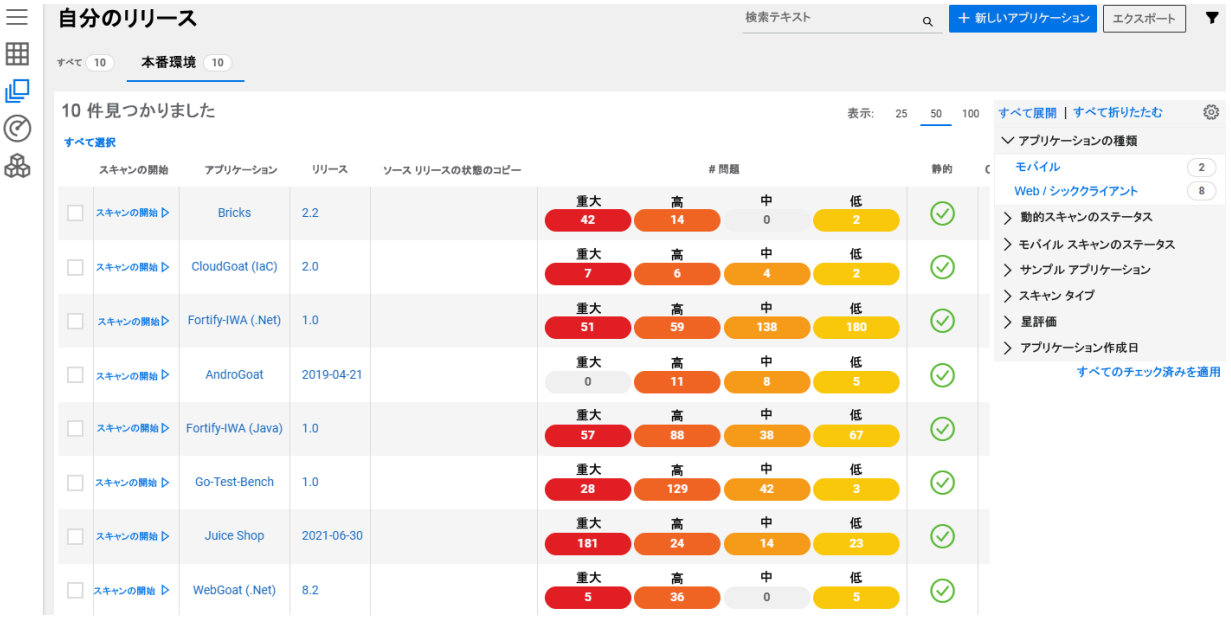
[ご使用のリリース] ページを表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。グリッドには、各リリースに関する詳細 (アプリケーション名、関連付けられたリリース名、リリースで見つかった問題の数、星評価、現在のスキャン ステータス) が表示されます。



3. タブを選択して、SDLC ステータスでリリースをフィルターします。既定の SDLC ステータスの [**すべて**] では、すべてのリリースが表示されます。既定の SDLC ステータスはアカウント設定で変更できます。

1.4.5.1. [ご使用のリリース] ページの操作

次の表に、[ご使用のリリース] ページの操作方法を示します。

タスク	アクション
アプリケーションを作成する	[**+ 新しいアプリケーション**] をクリックします。
リリース リストを検索する	検索テキスト ボックスにキーワードまたは語句を入力して、**Enter** キーを押します。検索結果を削除するには、検索ボックスのテキストを削除して **Enter** キーを押すか、適用されたフィルターを削除します。詳細については、「アプリケーションおよびリリースの検索」を参照してください。
.csv ファイルとしてデータをエクスポートする	[**エクスポート**] をクリックします。すべての脆弱性に関する詳細情報が含まれる .csv ファイルが、ブラウザーの設定で指定したフォルダーにローカルに保存されます。 **Note** [テナント ダッシュボード]、[ご使用のリリース]、および [リリースの問題] ページのエクスポート機能では同じ列フィールドが出力されます。現在適用されているフィルターはエクスポートにも適用されます。
グリッド列を変更する	1. をクリックします。 2. チェック ボックスを使用して選択を行います。 3. [**保存**] をクリックします。
フィルター リストを非表示にするか表示する	をクリックします。

タスク	アクション
フィルターを展開するか折りたたむ	すべて展開 | すべて折りたたむ  またはフィルター名の横にある矢印をクリックします。
フィルターの適用	フィルター名の下にある目的のフィルター値を選択します。フィルタリングの結果によりページが自動的に更新されます。一部のフィルターについては、[**適用**] をクリックしてページを更新します。
適用されたフィルターを削除する	ページの上部にある [**X**] をクリックするか、[**フィルターをクリア**] をクリックします。
SDLC ステータス別にリリースをフィルターする	SDLC ステータスに対応するタブを選択します。ビュー間で移動しても、選択されている SDLC ステータスは保持されます。 
列別にリリース リストを並べ替える	列のヘッダーをクリックします。ヘッダーの横にある矢印は、データの並べ替え順序を示します。順序を逆にするには、ヘッダーをもう一度クリックします。

タスク	アクション
複数のリリースのリリース属性を編集する	1. 個々のリリースの横にあるチェックボックスをオンにするか、[**すべて選択**] をクリックしてページ上のすべてのリリースを選択します。 2. [**属性の編集**] をクリックします。 [属性の編集] ウィンドウが開きます。  3. 必要に応じてフィールドを更新します。 4. [**保存**] をクリックします。 リリースの属性については、「リリースの作成」を参照してください。
スキャンを開始する	[**スキャンの開始**] をクリックして、スキャン タイプを選択します。
アプリケーションまたはリリースの詳細を表示する	アプリケーション名またはリリース名をクリックします。

タスク	アクション
リリースの最新のスキャン ステータスを表示する	ステータス アイコンにカーソルを置きます。そのアイコンをクリックして、スキャン ステータスの詳細情報に直接アクセスします。  • スケジュールされたスキャンにスケジュールされた開始日が表示されます。 • 完了日は、「開始日 + 選択した評価タイプの SLO + 一時停止時間 + 週末」に基づいて計算されます。スキャンが SLO を過ぎている場合、予測される完了日には、「<release> でのスキャンに長い時間がかかります。詳しくは弊社までお問い合わせください。」と表示されます
リリースの親アプリケーションに適用されるセキュリティ ポリシーを表示する	星評価をクリックします。

1.4.5.2. [ご使用のリリース] ページのフィルタリング

既定では、[自分のリリース] ページにはすべてのリリースが表示されます。表示するリリースは、フィルターを適用して制限できます。[自分のリリース] ページでは次のフィルターを使用できます。

Note

フィルターがフィルター リストに表示されるのは、リリースにそのフィルターの複数の値が含まれている場合だけです。

フィルター	定義	値
アプリケーション作成日	アプリケーションを作成した日	7 日未満、30 日未満、90 日未満、180 日未満
アプリケーションの種類	アプリケーション作成時に選択されたアプリケーションの種類。	モバイル、Web / シッククライアント
ビジネス クリティカリティ	アプリケーションのクリティカリティ	高、中、低
動的スキャンのステータス	動的スキャンのステータス	未開始、キャンセル済み、完了、進行中、待機中
MicroserviceName	マイクロサービスの名前	ユーザー定義
モバイル スキャンのステータス	モバイル スキャンのステータス	未開始、キャンセル済み、完了、進行中、待機中
合格/不合格	ユーザー定義の合格/不合格の評価	不合格、合格
スキャン タイプ	スキャン タイプ	静的、動的、モバイル
SDLC ステータス	リリースの SDLC ステータス	本番環境、QA/テスト、開発、廃棄
星評価	5 つ星評価システム	1、2、3、4、5
静的スキャンのステータス	静的スキャンのステータス	進行中、完了、キャンセル済み、待機中
<カスタム リリースの属性>	選択リストになっているリリースの属性	ユーザー定義

1.4.6. アプリケーションおよびリリースの検索

ポータル ツールバーに表示された最上位の検索ボックスに加え、各グリッドの [**検索テキスト**] ボックスを使用して、グリッドの表示コンテキスト内でアプリケーション名、リリース名、キーワード、URL を検索することができます。

検索テキスト

グリッド内のアプリケーションまたはリリースを検索するには、次の手順を実行します。

1. 検索する文字列を [**検索テキスト**] ボックスに入力します。

   このボックスに文字列全体を入力する必要はありません。たとえば、「Test App 1」という名前のアプリケーションを検索する場合は次のようになります。

   - ボックスに「**Test**」と入力した場合、検索結果に Test App 1 が**含まれます**。
   - ボックスに「**Tes**」と入力した場合、検索結果に Test App 1 は**含まれません**。
   - ボックスに「**Tes***」と入力した場合、検索結果に Test App 1 が**含まれます**。

2. **Enter** キーをクリックします。

   検索結果によりページが更新されます。

3. 目的のアプリケーションまたはリリースの名前をクリックします。ページが更新され、選択したアプリケーションまたはリリースのページが表示されて、検索ボックスがクリアされます。

検索結果の削除

適用した検索フィルターを削除するには、次の手順のいずれかを実行します。

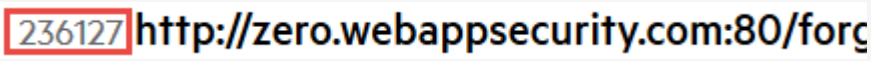
- 検索ボックスから検索文字列を削除します。
- ブラウザーの [**戻る**] 矢印をクリックします。

1.4.7. ディープ リンクの作成

OpenText Fortify on Demand では、アプリケーション、リリース、スキャン、および問題へのディープ リンクがサポートされます。

ディープ リンクを作成するには、次のパス形式を使用します。

- アプリケーション: https://*<fod_domain>*/redirect/Applications/*<application_id>*
- リリース: https://*<fod_domain>*/redirect/Releases/*<release_id>*
- スキャン: https://*<fod_domain>*/redirect/Scans/*<scan_id>*
- 問題: https://*<fod_domain>*.com/redirect/Issues/*<issue_id>*

> **Note**
>
> 問題の詳細パネルの上部には問題 ID が表示されます。
>
> 
>

ここで、*<fod_domain>* は、OpenText Fortify on Demand データ センターのドメインです。

- US: `ams.fortify.com`
- EMEA: `emea.fortify.com`
- APAC: `apac.fortify.com`
- FedRAMP: `fed.fortifygov.com`

1.5. 評価の実行

OpenText Fortify on Demand では、3 つの評価タイプ (静的、動的、モバイル) で包括的なセキュリティ テストが提供されています。

- 静的評価
- オープン ソース ソフトウェア構成分析
- 動的評価
- モバイル評価
- 使用権の消費
- スキャンの管理

1.5.1. 静的評価

静的評価では、アプリケーションのソース コード、バイトコード、またはバイナリの潜在的なセキュリティの脆弱性が分析されます。静的評価は OpenText SAST によって提供されます。OpenText SAST を使用した静的テストには以下が含まれます。

1. ソース コードの中間的な変換形式への変換
2. 変換されたコードの分析

このセクションでは、次のトピックについて説明します。

- OpenText SAST の要件
- 静的評価ファイルの準備
- 静的スキャンの構成
- 静的評価ペイロードのアップロード
- 静的評価のペイロード検証

1.5.1.1. OpenText SAST の要件

Note

OpenText Fortify on Demand での OpenText SAST の更新はメジャー リリースの間に行われることがあります。OpenText SAST の要件は、メジャー リリースのドキュメントで更新されます。OpenText SAST リリースの詳細については、OpenText Static Application Security Testing and Tools のドキュメントを参照してください。

このセクションでは、次のトピックについて説明します。

- サポート対象言語
- サポート対象コンパイラ
- サポートされているライブラリ、フレームワーク、テクノロジ

1.5.1.1.1. サポート対象言語

OpenText SAST は、次の表に記載されているプログラミング言語をサポートします。

言語/フレームワーク	バージョン
.NET (Core)	2.0 ～ 9.x
.NET Framework	2.0-4.8
ABAP/BSP	6.x、7.x
ActionScript	3.0
Apex	55-61
Bicep	0.12.X ～ 0.15.31
C#	5-13
C	C11、C17、C23 (「コンパイラ」を参照)
C++	C++11、C++14、C++17、C++20 (「コンパイラ」を参照)
Classic ASP (VBScript 付き)	2.0、3.0
COBOL	IBM Enterprise COBOL for z/OS 6.1 ～ 6.3 (CICS、IMS、DB2、および IBM MQ) Visual COBOL 6.0 ～ 8.0
ColdFusion	8-10
Dart	2.12-3.1
Docker (Dockerfiles)	すべて

言語/フレームワーク	バージョン
Flutter	2.0-3.13
Go	1.12-1.23
HCL	2.0 **Note** HCL 言語サポートは、Terraform およびサポートされているクラウド・プロバイダーの IaC (Infrastructure as Code) 構成に固有です。
HTML	5 以前
Java (Android を含む)	7-21
JavaScript	ECMAScript 2015–2023
JSON	ECMA-404
JSP	1.2-2.1
Kotlin	1.3-2.0
MXML (Flex)	4
Objective-C/C++	2.0 (「コンパイラ」を参照)
PHP	7.3-8.3

言語/フレームワーク	バージョン
PL/SQL	8-23
Python	2.6 ~ 2.7、3.0 ~ 3.12
Ruby	1.x
Scala	2.11 ~ 2.13、3.3 ~ 3.4
Solidity	0.4.12 ～ 0.8.21
Swift	5.0 ～ 5.10、6.0 (サポートされている swiftc のバージョンについては、「コンパイラ」を参照)
T-SQL	SQL Server 2005、2008、2012
TypeScript	3.6-5.4
VBScript	2.0、5.0
Visual Basic (VB.NET)	15.0-16.9
Visual Basic	6.0
XML	1.0
YAML	1.2

1.5.1.1.2. サポート対象コンパイラ

<<トピックは FoD と共有されます>>

OpenText SAST は、次の表に記載されているコンパイラをサポートします。

コンパイラ	バージョン	オペレーティング システム
gcc	GNU gcc 6.x ～ 10.4、11、12、13	Windows、Linux、macOS
	GNU gcc 4.9、5.x	Windows、Linux、macOS、AIX
g++	GNU g++ 6.x ～ 10.4、11、12、13	Windows、Linux、macOS
	GNU g++ 4.9、5.x	Windows、Linux、macOS、AIX
OpenJDK javac	9、10、11、12、13、14、17、21	Windows、Linux、macOS、AIX
Oracle javac	7、 8、 9	Windows、Linux、macOS
cl (MSVC)	2015、2017、2019、2022	Windows
Clang	14.0.3、15.0.0、16.0.0	macOS
Swiftc	5.8、5.8.1、5.9、5.9.2、5.10、6.0、6.0.2、6.0.3[1]	macOS

[1]OpenText SAST は、次の Xcode バージョンでビルドされたアプリケーションをサポートします: 16-16.4, 26.0-26.4。

1.5.1.1.3. サポートされているライブラリ、フレームワーク、テクノロジ

OpenText SAST は、専用の Fortify Secure Coding Rulepacks を使用し、コアのサポートされる言語を超えた脆弱性の適用範囲において、このセクションに記載されているライブラリ、フレームワーク、およびテクノロジをサポートします。

Java

- Adobe Flex Blaze DS
- Ajanta
- Amazon Web Services (AWS) SDK
- Android
- Android Jetpack
- Apache Axiom
- Apache Axis
- Apache Beam
- Apache Beehive NetUI
- Apache Catalina
- Apache Cocoon
- Apache Commons
- Apache ECS
- Apache Hadoop
- Apache HttpComponents
- Apache Jasper
- Apache Slide
- Apache Spring Security (Acegi)
- Apache Struts
- Apache Tapestry
- Apache Tomcat
- Apache Torque
- Apache Util
- Apache Velocity
- Apache Wicket
- Apache Xalan
- Apache Xerces
- ATG Dynamo
- Azure SDK
- Castor
- Display Tag
- Dom4j
- GDS AntiXSS
- Google Cloud
- Google Dataflow
- iBatis
- IBM MQ
- IBM WebSphere
- Jackson
- Jakarta Activation
- Jakarta EE (Java EE)
- Jasypt
- Java Annotations
- Java Excel API
- JavaMail
- JAX-RS
- JAXB
- Jaxen
- JBoss
- JDesktop
- JDOM
- Jetty
- JGroups
- json-simple
- JTidy Servlet
- JXTA
- JYaml
- Liferay Portal
- Mozilla Rhino
- MyBatis
- MyBatis-Plus
- Netscape LDAP API
- OkHttp
- OpenCSV
- Oracle Application Development Framework (ADF)
- Oracle BC4J
- Oracle JDBC
- Oracle OA Framework
- Oracle tcDataSet
- Oracle XML Developer Kit (XDK)
- OWASP Enterprise Security API (ESAPI)
- OWASP HTML Sanitizer
- OWASP Java Encoder
- Spring AI
- Spring MVC
- Spring Boot
- Spring Data Commons
- Spring Data JPA
- Spring Data MongoDB
- Spring Data Redis
- Spring HATEOAS
- Spring JMS
- Spring JMX
- Spring Messaging
- Spring Security
- Spring Webflow
- Spring WebSockets
- Spring WS
- Stripes
- Sun JavaServer Faces (JSF)
- Tungsten
- Weblogic

Apache Log4j Apache Lucene Apache MyFaces Apache OGNL Apache ORO Apache POI Apache SLF4J	Google Guava Google Web Toolkit gRPC Gson Hibernate	MongoDB	Plexus Archiver Realm Restlet SAP Web Dynpro Saxon SnakeYAML Spring	WebSocket XStream YamlBeans ZeroTurnaround ZIP Zip4J

Kotlin

Kotlin のサポートには、Java でカバーされるすべてのライブラリと次の Kotlin ライブラリが含まれます。

Kotlin の標準ライブラリ				

Scala

Scala のサポートには、Java でカバーされるすべてのライブラリと次の Scala ライブラリが含まれます。

Akka HTTP Scala Play	Scala Slick			

.NET

.NET Framework、.NET Core、および .NET Standard .NET WebSockets ADO.NET Entity Framework ADODB Amazon Web Services (AWS) SDK ASP.NET MVC ASP.NET SignalR ASP.NET Web API	Azure SDK Castle ActiveRecord CsvHelper Dapper DB2 .NET Provider DotNetZip Entity Framework Entity Framework Core fastJSON gRPC	Hot Chocolate IBM Informix .NET Provider Json.NET Log4Net Microsoft ApplicationBlocks Microsoft My Framework Microsoft Practices Enterprise Library Microsoft Web Protection Library	MongoDB MySQL Connector/NET NHibernate NLog Npgsql Open XML SDK Oracle Data Provider for .NET OWASP AntiSamy Saxon	SharePoint Services SharpCompress SharpZipLib SQLite .NET Provider SubSonic Sybase ASE ADO.NET Data Provider Xamarin Xamarin Forms YamlDotNet

C

ActiveDirectory LDAP Apple System Logging (ASL)	CURL Library GLib JNI	MySQL Netscape LDAP ODBC	OpenSSL POSIX Threads SQLite	Sun RPC WinAPI

C++

Boost Smart Pointers MFC	STL WMI			

SQL

Oracle ModPLSQL			

PHP

ADOdb Advanced PHP Debugging CakePHP PHP Debug	PHP DOM PHP Extension PHP Hash PHP JSON PHP Mcrypt	PHP Mhash PHP Mysql PHP OCI8 PHP OpenSSL PHP PostgreSQL	PHP Reflection PHP Simdjson PHP SimpleXML PHP Smarty PHP Sodium	PHP WordPress PHP XML PHP XMLReader PHP Zend PHP Zip

JavaScript/TypeScript/HTML5

Angular Anthropic Claude Apollo Server Bluebird child-process-promise エクスプレス	Gemini API GraphQL.js Handlebars Helmet iOS JavaScript Bridge jQuery	JS-YAML LangChain Mustache Node.js Azure Storage Node.js Core OpenAI	React React Native React Native Async Storage React Router SAPUI5/OpenUI5	Sequelize Underscore.js Vue

Python

aiopg Amazon Web Services (AWS) Lambda Amazon SageMaker Anthropic Claude Azure Functions Django Flask Google Cloud	Graphene gRPC httplib2 Jinja2 LangChain libxml2 lxml memcache-client	_mysql MySQL Connector/Python MySQLdb OpenAI oslo.config Paramiko psycopg2	pycrypto PyCryptodome pycurl pylibmc PyMongo PySpark PyYAML	requests simplejson six TensorFlow Twisted Mail urllib3 WebKit

Ruby

MySQL pg	Rack SQLite	Thor		

Objective-C

AFNetworking Apple AddressBook Apple AppKit Apple CFNetwork Apple ClockKit Apple CommonCrypto Apple CoreData	Apple CoreFoundation Apple CoreLocation Apple CoreServices Apple CoreTelephony Apple Foundation Apple HealthKit	Apple LocalAuthentication Apple MessageUI Apple Security Apple Social Apple UIKit	Apple WatchConnectivity Apple WatchKit Apple WebKit Hpple Objective-Zip Realm	SBJson SFHFKeychainUtils SSZipArchive ZipArchive ZipUtilities ZipZap

Swift

Alamofire Apple AddressBook Apple CFNetwork Apple ClockKit Apple CommonCrypto Apple CoreData	Apple CoreFoundation Apple CoreLocation Apple Foundation Apple HealthKit Apple LocalAuthentication	Apple MessageUI Apple Security Apple Social Apple SwiftUI Apple UIKit Apple WatchConnectivity	Apple WatchKit Apple WebKit Hpple Realm SQLite SSZipArchive	Zip ZipArchive ZIPFoundation ZipUtilities ZipZap

COBOL

Auditor CICS DLI	Micro Focus COBOL Run-time System MQ	POSIX SQL		

Go

GORM logrus gRPC				

Configuration

.NET 構成 Adobe Flex (ActionScript) Configuration Ajax Frameworks Amazon Web Service (AWS) Ansible AWS CloudFormation Azure Resource Manager (ARM) Build Management	Docker Configuration (Dockerfiles) GitHub Actions Google Android Configuration iOS Property List J2EE Configuration Java Apache Axis Java Apache Log4j Configuration Java Apache Spring Security (Acegi)	Java Apache Struts Java Apache Tomcat Configuration Java Blaze DS Java Hibernate Configuration Java iBatis Configuration Java IBM WebSphere Java MyBatis Configuration	Java OWASP AntiSamy Java Spring and Spring MVC Java Spring Boot Java Spring Mail Java Spring Security Java Spring WebSockets Java Weblogic Kubernetes Mule	OpenAPI 仕様 Oracle Application Development Framework (ADF) PHP Configuration PHP WordPress Silverlight 構成 Terraform (AWS、Azure、GCP) WS-SecurityPolicy XML Schema

Infrastructure as Code: Amazon Web Services

API Gateway AppSync Athena Aurora Backup Batch Certificate Manager CloudFormation CloudFront CloudTrail CloudWatch CodeStar Cognito Config	Database Migration Service (DMS) DocumentDB DynamoDB EC2 Elastic Block Store (EBS) Elastic Container Registry (ECR) Elastic Container Service (ECS) Elastic File System (EFS) Elastic Kubernetes Service (EKS) Elastic Load Balancing (ELB)	ElastiCache EMR FinSpace FSx Global Accelerator Glue GuardDuty Identity and Access Management (IAM) Image Builder Key Management Service (KMS) Kinesis Kinesis Video Streams	Lightsail Location Service Mainframe Modernization Managed Streaming for Apache Kafka (MSK) MemoryDB for Redis MQ Neptune OpenSearch Service Quantum Ledger Database (QLDB) RDS Redshift	Rekognition Route 53 SageMaker Secrets Manager Simple Notification Service (SNS) Simple Queue Service (SQS) Simple Storage Service (S3) Timestream Transfer Family VPC WorkSpaces Family

Infrastructure as Code: Microsoft Azure

App Service Automation Microsoft Entra Domain Services Azure Health Data Services Azure Kubernetes Service (AKS)	Batch Blob Storage Cache for Redis Cognitive Search Container Registry Cosmos DB Database for MariaDB	Database for MySQL Database for PostgreSQL Databricks Defender for Cloud Event Hubs Front Door IoT Central	IoT Hub Key Vault Logic Apps Media Services Monitor NetApp Files Policy ポータル	SignalR Service Site Recovery Spring Apps SQL Storage Accounts Virtual Machine Scale Sets Virtual Machines Web PubSub

Infrastructure as Code: Google Cloud

Apigee API Management App Engine BigQuery Cloud Bigtable	Cloud DNS Cloud Functions Cloud Key Management Cloud Load Balancing Cloud Logging	Cloud Spanner Cloud SQL Cloud Storage Compute Engine	Filestore Google Cloud Platform Google Kubernetes Engine (GKE)	Identity and Access Management (IAM) Media CDN Pub/Sub Secret Manager

シークレット

.netrc	Defined	HashiCorp (Terraform、Vault)	New Relic	Sendbird
1Password	DES	Heroku	npm	SendGrid
Actually Good Encryption (AGE)	DigitalOcean	HexChat	NuGet	Sentry
Adafruit	Docker	HubSpot	Okta	SHA1
Adobe	Doppler	Intercom	OpenVPN	SHA256
Airtable	Droneci	Java	コメント内のパスワード	SHA512
Algolia	Dropbox	JFrog (Artifactory)	接続文字列内のパスワード	Shippo
Alibaba (Aliyun)	Duffel	JSON Web Token	PowerShell スクリプト内のパスワード	Shopify
Amazon (AWS、MWS)	Dynatrace	KDE Wallet (Kwallet)	URI 内のパスワード	Sidekiq
Apple (macOS)	EasyPost	KeePass	PasswordSafe	Slack
Apache HTTP	Encryption key	Kraken	PayPal (Braintree)	SonarQube
Asana	Etsy	Kucoin	Pidgin	Square
Atlassian	Facebook	LaunchDarkly	Plaid	Squarespace
Authress	Fastly	Linear	Planetscale	StackHawk
基本アクセス認証	Finicity	LinkedIn	PostgreSQL	Stripe
bcrypt	Finnhub	Lob	Postman	Sumologic
Beamer	Flickr	Mailchimp	Prefect	Telegram
ベアラー トークン	Flutterwave	Mailgun	Pulumi	Travis
Bitbucket	Frame.io	Mapbox	PuTTY	Trello
Bittrex	Freshbooks	Mattermost	PyPI	Twilio
	Git	MD5	RapidAPI	Twitch
	GitHub	MessageBird		Twitter
	GitLab			Typeform
	Gitter			Yandex
	GNOME			Zendesk

Brevo (Sendinblue) Clojars Code Climate Codecov Coinbase Confluent Contentful Databricks Datadog	GNU (Bash) GoCardless Google (API、Google Cloud、OAuth) Grafana	Microsoft (Azure App Storage、Cosmos DB、Functions および Bitlocker、PowerShell、RDP、VBScript) Microsoft (Outlook) Mutt MySQL Netlify	Readme RSA Security Ruby (Ruby on Rails、RubyGems) Sauce Labs シークレットキー Secure Shell Protocol (SSH)	

1.5.1.2. 静的評価ファイルの準備

静的評価の最初の手順は、アプリケーションのソース コードまたはコンパイル済みファイルあるいはその両方を準備することです。静的評価が拒否されるのを防ぎ、包括的で正確なスキャン結果を取得するため、アプリケーションのプログラミング言語またはテクノロジ スタックの説明に従ってファイルを準備してください。

Note

オープン ソース ソフトウェア構成分析用のファイルの準備については、「オープン ソースの評価ファイルの準備」を参照してください。

このセクションでは、次のトピックについて説明します。

- 静的評価ファイルの要件
- Fortify ScanCentral SAST クライアントのインストールと使用
- .NET アプリケーション ファイルの準備
- Java アプリケーション ファイルの準備
- JavaScript テクノロジ/HTML/XML ファイルの準備
- Kotlin アプリケーション ファイルの準備
- ABAP (SAP) アプリケーション ファイルの準備
- C および C++ アプリケーション ファイルの準備
- Classic ASP、VBScript および Visual Basic アプリケーション ファイルの準備
- Dart および Flutter アプリケーション ファイルの準備
- ColdFusion Markup Language (CFML) アプリケーション ファイルの準備
- COBOL アプリケーション ファイルの準備
- Dockerfile と Infrastructure as Code (IaC) ファイルの準備
- Go アプリケーション ファイルの準備
- PHP アプリケーション ファイルの準備
- Python アプリケーション ファイルの準備
- Ruby アプリケーション ファイルの準備
- Solidity アプリケーション ファイルの準備
- Salesforce (Apex および Visualforce) アプリケーション ファイルの準備
- Scala アプリケーション ファイルの準備
- Android アプリケーション ファイルの準備 (ソース コード)
- iOS アプリケーション ファイルの準備 (ソース コード)

1.5.1.2.1. 静的評価ファイルの要件

静的評価のために送信されるアプリケーションは、次のファイル要件を満たしている必要があります。

- アプリケーション ファイルは、パスワードで保護されていない zip ファイルにパッケージ化する必要があります。tarball、rar、tar、7z など、その他のファイル拡張子はサポートされていません。
- 最大ペイロード サイズは、モノリシック アプリケーションの場合は 5 GB、マイクロサービス アプリケーションの場合は 100 MB です。試用版の最大ペイロード サイズは 150 MB に制限されています。
- ペイロードには、次のファイル タイプを少なくとも 1 つ含める必要があります。
    - バイナリ/コンパイル済みファイル: バイナリ/コンパイル済みファイルとは、アプリケーションのソース コード ファイルをコンパイルすることによって生成された、デバッグ コンパイル済みの実行可能ファイル、またはアプリケーションで使用されるサード パーティの依存関係によって生成された、実行可能ライブラリおよびリソース ファイルのことです。
    - ソース コード ファイル: ソース コード ファイルは、アプリケーション ファイルを生成するためにコンパイルされるテキスト ファイルです。
- アプリケーション ファイルは、アプリケーションが送信されるテクノロジ スタックの特定の要件を満たしている必要があります。アプリケーション ファイルは、そのテクノロジ スタックで指示されているとおりのものを準備します。
- 一般に、送信されるコードは完全に展開可能でなければなりません。つまり、たとえば、JAR ファイルには実行可能コードが含まれている必要があります。

1.5.1.2.2. Fortify ScanCentral SAST クライアントのインストールと使用

Fortify は、静的スキャンに必要なすべての依存関係とソース コード、および OpenText オープン ソース スキャンに必要なファイルを自動的にパッケージ化するためのスタンドアロン Fortify ScanCentral SAST クライアントを提供します。次の言語がサポートされています: .NET および .NET Core (MSBuild プロジェクト)、Apex、Classic ASP、ColdFusion、Dockerfiles、Go, Java (Gradle および Maven プロジェクト)、Javascript/Typescript、PHP、Python、Ruby。

Important

スタンドアロンの Fortify ScanCentral SAST クライアントは、オンプレミスの Fortify ScanCentral SAST ソフトウェアのコンポーネントであり、スキャンのためにコントローラに送信するコードをパッケージ化するために使用されます。OpenText Fortify on Demand は、Fortify ScanCentral SAST クライアントのパッケージ化機能のみを使用します。ソース コードのパッケージ化に関連する詳細が提供されています。

Fortify ScanCentral SAST クライアントの最新バージョンは、ポータルの [ツール] ページから入手できます。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

Fortify ScanCentral SAST クライアントの使用の詳細については、Fortify Software Security Center Documentationを参照してください。インストールされているバージョンに対応するドキュメントのバージョンを選択します。

- ソフトウェア要件: 『*OpenText™ Application Security Software System Requirements*』の「Fortify ScanCentral SAST Client Software Requirements」
- サポートされているビルド ツール: 『*OpenText™ Application Security Software System Requirements*』の「Fortify ScanCentral SAST Sensor Languages and Build Tools」
- コマンドライン オプション: 『*OpenText™ Fortify ScanCentral SAST インストール、構成、および使用ガイド*』の「パッケージ コマンド オプション」

1.5.1.2.3. .NET アプリケーション ファイルの準備

.NET 実装 (.NET、.NET Core、.NET Framework、および Android/iOS 対応の Xamarin アプリケーション) の場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST を使用したコードの自動パッケージ化 (推奨)
- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Important

ソース コードはデフォルトでスキャンされます。ソース コードはより正確で包括的なスキャン結果を生成するため、OpenTextMSP ポータルは、ソース コードを提供することを強くお勧めします。さらに、スキャン プロセスには誤検出の可能性があるため、監査者はソース コードを使用して手動で問題を確認できます。ソース コード スキャンがオプションでない場合は、サポート チームに連絡して、バイナリ/コンパイル コード スキャンを有効にしてください。

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>`。例: `scancentral package o mypayload.zip`。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

.NET の追加の `package` コマンドの例:

- Windows 上の dotnet プロジェクト: `scancentral package -bt dotnet -o mypayload.zip`
- csproj ファイルを使用した Windows 上の MSBuild プロジェクト: `scancentral package -bf my.csproj -o mypayload.zip`

IDE ツールを使用したコードのパッケージ化

IDE プラグインを使用すると、プロジェクト ファイルとパッケージ化に必要な依存関係を選択できます。IDE ツールの使用の詳細については、「IDE ツール」を参照してください。

コードの手動パッケージ化

コードの手動パッケージ化は次の作業で構成されます。

- ソース コード ファイルの準備
- コンパイル済みファイルの準備 (バイナリ/コンパイル コード用)
- ソース コードとコンパイル済みファイルを含む zip ファイルの作成

ソース コード ファイルの準備

ソース コードは、アプリケーションのすべてのプロジェクトで構成されます。完全なプロジェクトには、以下が含まれます。

- 必要なすべてのソース コード ファイル (C/C++、C#、または VB.NET)
- 必要なすべてのリファレンス ライブラリ

  これには関連するフレームワーク、NuGet パッケージ、およびサードパーティのライブラリからのアイテムが含まれます。
- C/C++ プロジェクトには、Visual Studio または MSBuild のインストールに属していない必要なすべてのヘッダー ファイルを含めます。
- ASP.NET プロジェクトと ASP.NET Core プロジェクトには、必要なすべての ASP.NET ページ ファイルを含めます。

サポート対象の ASP.NET ページのタイプは、ASPX、ASCX、ASAX、ASHX、ASMX、AXML、Master、CSHTML、VBHTML、BAML、および XAML です。

さらに、望ましくないスキャン結果を減らすために、次のタスクを必ず実行してください。

- 指定した .NET バージョンを対象とする依存関係のコピーを 1 つだけ含めます。
- ペイロード内のコードの重複を避けるため、`obj` および `bin/release` フォルダーは指定しないでください。

Note

Visual Studio 開発者コマンド プロンプトを使用している場合は、`dotnet restore` コマンドを実行して、プロジェクトに必要なすべてのリファレンス ライブラリを確実にダウンロードしてインストールしてください。このコマンドは、プロジェクトの最上位のフォルダーから実行する必要があります。

コンパイル済みファイルの準備 (バイナリ/コンパイル コード用)

- **フル** デバッグ モードでアプリケーションをクリーニングしてコンパイルします。対応する PDB ファイルが存在する場合、コンパイル済みファイルのスキャン結果にはファイル名と行番号のみが含まれます。対応するバイナリと PDB ファイルは、同じフォルダに存在する必要があります。対応する PDB ファイルがない場合は、バイナリが除外されます。

  Note

  サード パーティ ライブラリをスキャン結果に含める場合、対応する PDB ファイルが必要です。

- すべての依存関係を含むデバッグ ビルド ファイルを指定します。ペイロード内のコードの重複を避けるため、`obj` および `bin/release` フォルダーは指定しないでください。

Zip ファイルの作成

ソース コード ファイルとデバッグ ビルド ファイルを zip ファイルにパッケージ化します。ソース コード ファイルを別のルート ディレクトリに配置します。

アプリケーションに Javascript、HTML、XML のコンポーネントが含まれている場合、単に JavaScript、HTML、XML ファイルをペイロードに含めるだけでそれらをスキャンできます。

1.5.1.2.4. Java アプリケーション ファイルの準備

Java アプリケーションの場合は、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Important

ソース コードはデフォルトでスキャンされます。ソース コードはより正確で包括的なスキャン結果を生成するため、OpenTextMSP ポータルは、ソース コードを提供することを強くお勧めします。さらに、スキャン プロセスには誤検出の可能性があるため、監査者はソース コードを使用して手動で問題を確認できます。ソース コード スキャンがオプションでない場合は、サポート チームに連絡して、バイナリ コード スキャンを有効にしてください。

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

Java の追加の `package` コマンドの例:

- カスタム POM ファイルを含む Maven プロジェクト: `scancentral package -bf myCustomPom.xml -o mypayload.zip`
- カスタム ビルド パラメーターを含む Gradle プロジェクト: `scancentral package -bc clean build -o mypayload.zip`

IDE ツールを使用したコードのパッケージ化

IDE プラグインを使用すると、プロジェクト ファイルとパッケージ化に必要な依存関係を選択できます。IDE ツールの使用の詳細については、「IDE ツール」を参照してください。

コードの手動パッケージ化

コードの手動パッケージ化は次の作業で構成されます。

- ソース コード ファイルの準備
- コンパイル済みファイルの準備
- ソース コードとコンパイル済みファイルを含む zip ファイルの作成

ソース コード ファイルの準備

ソース コードと、Java アプリケーションが参照する関連 Kotlin ソース コードを提供します。

コンパイル済みファイルの準備

- アプリケーションをデバッグ モードでコンパイルします (たとえば、javac コンパイラを使用している場合は、`javac -g` を実行します)。デバッグ情報が提供されている場合、コンパイル済みファイルのスキャン結果にはファイル名と行番号のみが含まれます。
- JSP ファイルは WAR ファイルの一部である必要があります。JSP ファイルは事前コンパイルしないでください。
- アプリケーションを JAR、WAR、または EAR ファイルとしてパッケージ化します。
- ペイロード内のコードの重複を避けるため、共有ファイルのコピーを 1 つのみ指定します。
- ソース モード スキャンを使用する場合は、コンパイル済みファイルから依存関係のみを提供して、スキャン結果の重複の問題を最小限に抑えます。通常の場合、依存関係は `WEB-INF/lib` フォルダー (WAR) および `lib` または `APP-INF/lib` フォルダー (EAR) にあります。

- 混在モード スキャンを使用する場合は、依存関係を含むすべてのコンパイル済みファイルを提供します。

Zip ファイルの作成

ソース コード ファイルとコンパイル済みファイルを zip ファイルにパッケージ化します。zip ファイルには、複数の JAR、WAR、および EAR ファイルを含めることができます。ソース コードは JAR に含めないでください。ソース コード ファイルは別のルート ディレクトリに配置します。

アプリケーションに Javascript、HTML、XML のコンポーネントが含まれている場合、単に JavaScript、HTML、XML ファイルをペイロードに含めるだけでそれらをスキャンできます。

1.5.1.2.5. JavaScript テクノロジ/HTML/XML ファイルの準備

JavaScript、HTML、および XML ファイルは、**JS/TS/HTML** テクノロジ スタックのスタンドアロン ペイロードとして送信できます。**JS/TS/HTML** は、単純な Web アプリケーションと、JavaScript 関連のテクノロジを主に使用する Web アプリケーションに対する包括的なオプションです。React Native モバイル アプリケーションは、**React Native** テクノロジ スタックで送信されます。

さまざまな言語やテクノロジ スタックで構築され、JavaScript、HTML、または XML ファイルが含まれているアプリケーションの場合、言語またはテクノロジ スタックの手順に従ってアプリケーションをパッケージ化し、JavaScript、HTML、または XML ファイルをパッケージに含めます。

次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

コードの手動パッケージ化

JavaScript、TypeScript、HTML、または XML ファイルから成るアプリケーションの場合、ファイルを 1 つの zip ファイルにパッケージ化します。本番環境の依存関係をすべて含めます。たとえば、npm を使用している場合は、`npm install --only=prod` を実行します。

さらに、以下の作業を実行してください。

- `package.json` ファイルを含めます。
- トランスパイルされた TypeScript ではなく、TypeScript ソース コードのみを提供します。たとえば、Angular プロジェクトをビルドするときに生成される `dist` フォルダーは指定しないでください。
- 縮小されたコードはスキャン結果の品質を著しく低下させるため、縮小されたソースコードの JavaScript ファイルは含めないでください。

1.5.1.2.6. Kotlin アプリケーション ファイルの準備

Kotlin アプリケーションの場合は、Kotlin ソース コード ファイルと、Kotlin アプリケーションが参照する関連 Java ソース コードを zip ファイルにパッケージ化します。すべての依存関係を含めます。通常の場合、依存関係は `WEB-INF/lib` フォルダー (WAR) および `lib` または `APP-INF/lib` フォルダー (EAR) にあります。

Important

Kotlin ソース ファイルのスキャンはサポートされています。

1.5.1.2.7. ABAP (SAP) アプリケーション ファイルの準備

SAP データベースから ABAP コードを抽出し、スキャン用に準備する必要があります。Fortify ABAP エクストラクタ ツールは、ソース コード ファイルをプレゼンテーション サーバーにダウンロードするために提供されます。

トランスポート要求のインポート

Fortify ABAP エクストラクタは、ポータルの [ツール] ページから入手できます (「表示ツール」を参照)。Fortify ABAP エクストラクタの zip ファイルには次のファイルが含まれています。

- `K900XXX.S9S` (「XXX」はリリース番号)
- `R900XXX.S9S` (「XXX」はリリース番号)

これらのファイルは、ローカルのトランスポート ドメインの外部から SAP システムにインポートする必要がある SAP トランスポート要求を構成します。トランスポート要求は、SAP 管理者またはシステムにトランスポート要求をインストールする権限を持つ担当者がインポートする必要があります。

NSP ファイルには、プログラム、トランザクション (YSCA)、およびプログラムのユーザー インターフェイスが含まれています。それらをシステムにインポートした後、SAP データベースからコードを抽出することができます。

インストールの注意

Fortify ABAP エクストラクタのトランスポート要求は、SAP リリース 7.02、SP レベル 0006 を実行するシステムで作成されました。別の SAP バージョンを実行している場合は、「`Install release does not match the current version`」というトランスポート要求のインポート エラーが発生して、トランスポート要求のインストールに失敗します。

この問題を解決するには、次の手順を実行します。

1. トランスポート要求のインポートを再度実行します。

   [トランスポート要求のインポート] ダイアログ ボックスが開きます。

2. [**オプション**] タブをクリックします。
3. [**無効なコンポーネントのバージョンを無視する**] チェックボックスをオンにします。
4. インポートの手順を完了します。

これで問題が解決しない場合やシステムが異なるテーブル構造の SAP バージョンで実行されている場合は、OpenText では、OpenText Fortify on Demand で ABAP コードをスキ

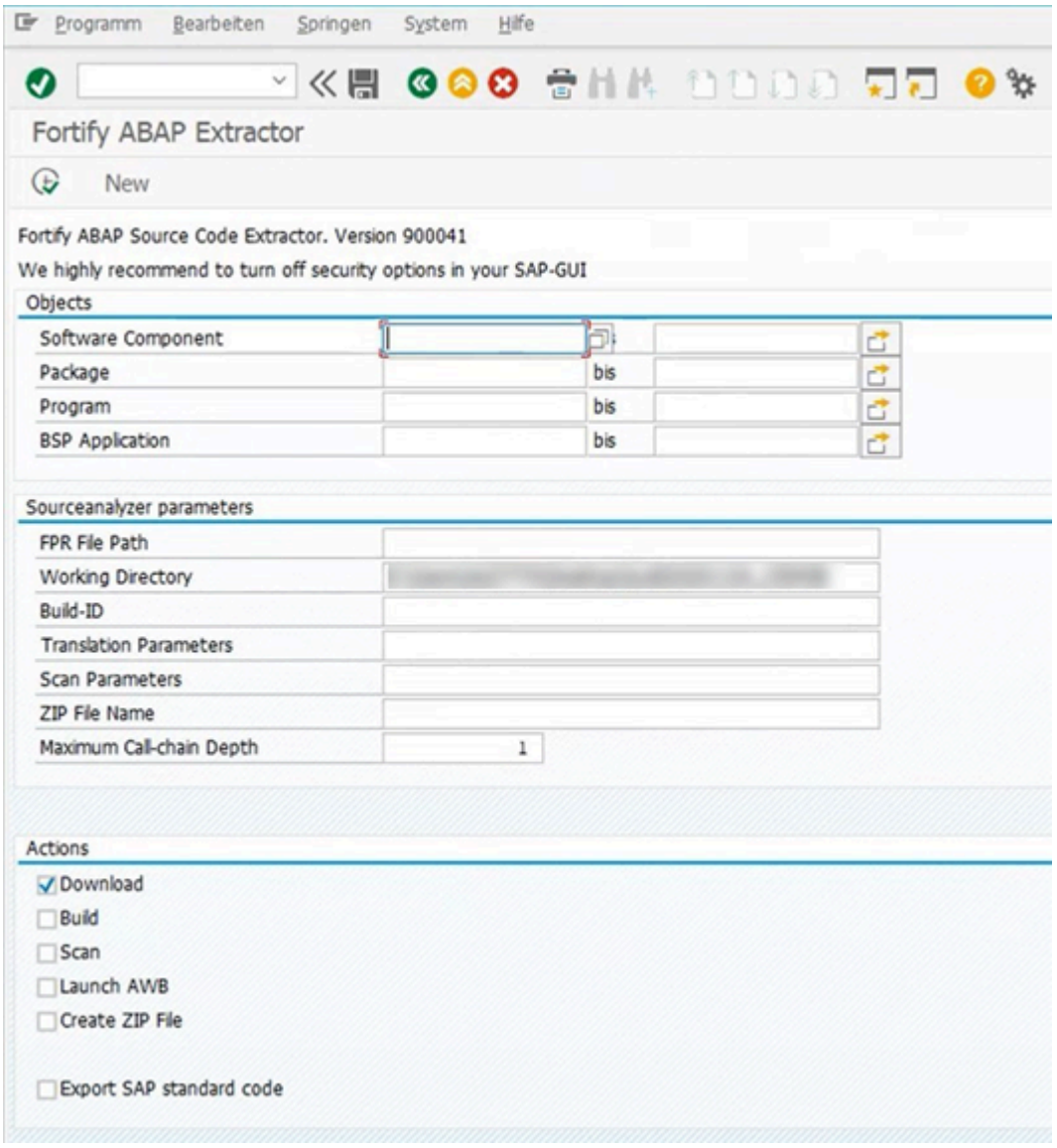
ャンできるように、独自のテクノロジを使用して ABAP ファイル構造をエクスポートすることをお勧めします。

Fortify ABAP エクストラクタの実行

ファイルをローカル システムにダウンロードしてオペレーティング システムのコマンドを実行する権限を持つアカウントを使用する必要があります。

Fortify ABAP エクストラクタを実行するには、次の手順を実行します。

1. トランザクション コードからプログラムを開始するか、エクストラクタ オブジェクトを手動で開始します。



2. スキャンするソフトウェア コンポーネント、パッケージ、プログラム、または BSP アプリケーションの範囲の開始名と終了名を入力します。

> **Note**
>
> 複数のオブジェクトまたは範囲を入力できます。

3. ソース コードを抽出するための基本設定を指定します。他に指示がない限り、フィールドは必須です。

> **Note**
>
> 一部のフィールドは、OpenText Fortify on Demand の使用には適用されません。使用可能なフィールドのみがリストされます。

フィールド	説明
作業ディレクトリ	抽出したソース コードを保存するディレクトリを入力または選択します。
ZIP ファイル名	(オプション) 圧縮パッケージに出力する場合は、ZIP ファイル名を入力します。
コールチェーンの最大深さ	グローバル SAP 関数 F は、F が明示的に選択されていない場合、または明示的に選択されたコードで始まり、長さがこの数値以下の関数呼び出しのチェーンを通じて F に到達できない場合、ダウンロードされません。サポート担当から指示がない限り、2 より大きい値は指定しないでください。

4. 実行するアクションを入力します。他に指示がない限り、フィールドは必須です。

Note

一部のフィールドは、OpenText Fortify on Demand の使用には適用されません。適用されるフィールドのみを以下にリストします。

フィールド	説明
ダウンロード	SAP データベースから抽出されたソース コードをダウンロードするには、このチェックボックスをオンにします。
ZIP ファイルを作成	(オプション) 出力を圧縮するには、このチェックボックスをオンにします。ソース コードが SAP データベースから抽出された後に手動で出力を圧縮することもできます。
SAP 標準コードをエクスポート	(オプション) カスタムコードとともに SAP 標準コードをエクスポートする場合は、このチェック ボックスをオンにします。

5. [**実行**] をクリックします。

Fortify ABAP エクストラクタの注意点

Fortify ABAP エクストラクタ プログラムはオンラインで実行されるため、抽出のために選択されたソース ファイルの量が許容されるプロセス実行時間を超える場合、「`max dialog work process time reached`」という例外が発生することがあります。この問題を回避するには、大規模なプロジェクトを一連の小さなエクストラクタ タスクとしてダウンロードします。たとえば、プロジェクトが 4 つの異なるパッケージで構成されている場合、各パッケージを同じプロジェクト ディレクトリに個別にダウンロードします。例外が頻繁に発生する場合は、SAP Basis の管理者に依頼して最大時間制限 (`rdisp/max_wprun_time`) の値を大きくします。

パッケージを ABAP から抽出するときに、Fortify ABAP エクストラクタは `TDEVC` フィールドがパッケージ名に一致するものすべてを `parentcl` から抽出します。次に、`TDEVC` からすでに抽出されたものと `parentcl` フィールドが等しいその他のすべてを

`TDEVC` から再帰的に抽出します。`TDEVC` から抽出されるフィールドは `devclass` です。

`devclass` の値はプログラム名のセットとして扱われ、ユーザーが指定可能なプログラム名と同じ方法で処理されます。

プログラムは、名前フィールドを次のいずれかと比較することによって `TRDIR` から抽出されます。

- 選択画面で指定したプログラム名
- パッケージを指定した場合は `TDEVC` から抽出された値のリスト

`TRDIR` の行は名前フィールドに指定されたプログラム名がある行で、行の抽出には式 `LIKE programname` が使用されます。

この最終的な名前のリストは、SAP システムからコードを取得するために `READ REPORT` とともに使用されます。このメソッドはクラスとメソッドを読み取り、またレコードに対して、単に `REPORTs` を読み取ります。

各 `READ REPORT` 呼び出しは、ローカル システムの一時フォルダーにファイルを生成します。

ソース コードがダウンロードされると、Fortify ABAP エクストラクタはソース内の `INCLUDE` 文を検出します。検出されると、ローカル システムにインクルード ターゲットをダウンロードします。

ABAP ソース コードのパッケージ化

Fortify ABAP エクストラクタで出力を圧縮しなかった場合は、ダウンロードしたソース コード ファイルを zip ファイルにパッケージ化します。

1.5.1.2.8. C および C++ アプリケーション ファイルの準備

OpenText Fortify on Demand では、C/C++ ソース コードまたはそのバイナリを直接スキャンできません。使用環境内で C/C++ コードを変換して、アーカイブにパッケージ化する必要があります。これにより、使用される環境変数とコンパイラで変換時の一貫性が確保されるため、テスト チームがビルド環境を再生成する必要性が減ります。C/C++ コードを変換してスキャン用にパッケージ化するための変換専用バージョンの OpenText SAST が提供されています。

OpenText SAST のインストール

OpenText SAST の最新バージョンは、ポータルの [ツール] ページから入手できます。Windows、macOS、および Linux オペレーティング システム用のインストーラをダウンロードできます。ソース コードを変換するには、有効なライセンス ファイルが必要です。ライセンスを発行するには、サポートに連絡してください。サポートは [ツール] ページから利用できます。

インストールと使用方法については、OpenText Static Application Security Testing and Tools のドキュメントのを参照してください。

コードの変換

1. コマンド ライン インターフェイスで、ディレクトリを通常のビルド ディレクトリに変更します。
2. 次のコマンドを実行します。

   `sourceanalyzer –debug –verbose –logfile translate.log -b <build-id> touchless <build_command>`

   ここで、 `<build_command>` はビルド スクリプトです。

   例:

   `sourceanalyzer –debug –verbose –logfile translate.log -b my_proj touchless make all`
3. コンソール出力でコマンドが完了したことを確認し、 `translate.log` にエラーのないことを確認して、プロジェクトが正常にビルドされるかどうかを検証します。

変換されたコードのパッケージ化

OpenText SAST モバイル ビルド セッション (MBS) では、プロジェクトの変換とプロジェクトのスキャンを別々のマシンで行うことができます。モバイル ビルド セッション ファイル (MBS ファイル) には、スキャンに必要なすべてのファイルが含まれています。

MBS ファイルを生成してパッケージ化するには、次の手順を実行します。

1. 変換を行ったマシンで、次のコマンドを実行し、モバイル ビルド セッションを生成します。

   `sourceanalyzer -b <build-id> -export-build-session <file.mbs>`

   `<file.mbs>` には、モバイル ビルド セッションに提供するファイル名を指定します。

2. MBS ファイルを zip ファイルのルートにパッケージ化します。他のファイル (追加の MBS ファイルを含む) またはディレクトリを含めないでください。含めると、スキャンがキャンセルされます。
3. **MBS/C/C++/Scala** テクノロジ スタック オプションで、zip ファイルを OpenText Fortify on Demand にアップロードします。

OpenText SAST の使用方法については、OpenText Static Application Security Testing and Tools のドキュメントのを参照してください。

1.5.1.2.9. Classic ASP、VBScript および Visual Basic アプリケーション ファイルの準備

Classic ASP、VBScript、および Visual Basic (VB6) アプリケーションの場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

コードの手動パッケージ化

ソース コード ファイルを単一の zip ファイルにパッケージ化します。

1.5.1.2.10. Dart および Flutter アプリケーション ファイルの準備

ソース コード ファイルを zip ファイルにパッケージ化します。すべての依存関係を含めます。

次のいずれかのコマンドを実行して、依存関係をダウンロードします。

- Flutter プロジェクトの場合は、`flutter pub get` を使用します。
- Dart のみのプロジェクトの場合は、`dart pub get` を使用します。

たとえば、プロジェクト ルート `myproject` を持つ Flutter プロジェクトの依存関係をダウンロードするには、次のコマンドを実行します。

```
cd myproject flutter pub get
```

Important

プロジェクトにネストされたパッケージが含まれており、それらの `pubspec.yaml` ファイルが異なる場合は、パッケージ ルートごとに `dart pub get` または `flutter pub get` を実行する必要があります。

Important

プロジェクト ディレクトリに以下が含まれていることを確認してください。

- 依存関係を指定する `pubspec.yaml` ファイル
- `pub` ツールによって自動的に生成された `package_config.json` ファイルを含む `.dart_tool` ディレクトリ

1.5.1.2.11. ColdFusion Markup Language (CFML) アプリケーション ファイルの準備

CFML アプリケーションの場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

コードの手動パッケージ化

ソース コード ファイルを単一の zip ファイルにパッケージ化します。

1.5.1.2.12. COBOL アプリケーション ファイルの準備

COBOL アプリケーションの場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package -targs "-copydirs <copybooks>" -targs "-dialect <cobol_dialect>" o <output_zip>` 。例: `scancentral package -targs "-copydirs copybooks" -targs "-dialect COBOL390" o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

コードの手動パッケージ化

COBOL ソース コード、COBOL ソース コードが使用するコピーブック ファイル、および COBOL ソース コードが参照する SQL INCLUDE ファイルを 1 つの zip ファイルにパッケージ化します。コピーブック ファイルと SQL INCLUDE ファイルは、COBOL ソース コードの `COPY` 文で使用されている名前を保持している必要があります。

コピーブック ファイルまたは SQL INCLUDE ファイルを、COBOL ソースが存在するディレクトリまたはサブディレクトリに含めないでください。COBOL のソース コードを `sources/` というフォルダーに、コピーブックを `copybooks/` というフォルダーに配置します。これらのフォルダーは zip ファイルのルートの同じレベルに配置します。

1.5.1.2.13. Dockerfile と Infrastructure as Code (IaC) ファイルの準備

Infrastructure as Code (IaC) 構成ファイルおよび Dockerfile は、**Infrastructure-As-Code/Dockerfile** テクノロジ スタックのスタンドアロンのペイロードとして送信できます。

コンテナ化されたアプリケーションの場合は、アプリケーションの言語やテクノロジ スタック向けの指示に従ってアプリケーションをパッケージ化し、Dockerfile をパッケージに含めます。

Note

OpenText SAST は、次のファイルを Dockerfile として変換します: `Dockerfile`、`dockerfile`、`*.Dockerfile`、および `*.dockerfile`。

OpenText SAST は、Dockerfile で次のエスケープ文字を受け入れます: バックスラッシュ (`\`) およびバッククォート (`` ` ``)。Dockerfile でエスケープ文字が設定されていない場合、OpenText SAST はバックスラッシュがエスケープ文字であると仮定します。

次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>`。例: `scancentral package o mypayload.zip`。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してく

ださい。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

コードの手動パッケージ化

ファイルを zip ファイルにパッケージ化し、**Infrastructure-As-Code/Dockerfile** テクノロジ スタックで送信します。

1.5.1.2.14. Go アプリケーション ファイルの準備

Go アプリケーションの場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

IDE ツールを使用したコードのパッケージ化

IDE プラグインを使用すると、プロジェクト ファイルとパッケージ化に必要な依存関係を選択できます。IDE ツールの使用の詳細については、「IDE ツール」を参照してください。

コードの手動パッケージ化

Go ソース コード ファイルを zip ファイルにパッケージ化します。標準の Go ライブラリに存在しない依存関係を含めます。これらの依存関係がベンダー フォルダーにあることを確認します。

Go に組み込まれている次の依存関係管理システムがサポートされています。

- Go モジュール (推奨)

  プロジェクトで Go モジュールを使用する場合は、プロジェクト ファイル (go.mod ファイルを含む) を zip ファイルのルートに配置する必要があります。プロジェクト ファイルをネストされたディレクトリに配置しないでください。

- GOPATH (Go 1.13 では廃止予定)

Note

次のエンティティはスキャンから除外されます。

- ベンダー フォルダー
- サブフォルダ内の `go.mod` ファイルによって定義されたすべてのプロジェクト
- `_test.go` サフィックスが付いているすべてのファイル (ユニット テスト)

1.5.1.2.15. PHP アプリケーション ファイルの準備

PHP アプリケーションの場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

IDE ツールを使用したコードのパッケージ化

IDE プラグインを使用すると、プロジェクト ファイルとパッケージ化に必要な依存関係を選択できます。IDE ツールの使用の詳細については、「IDE ツール」を参照してください。

コードの手動パッケージ化

ソース コード ファイルを単一の zip ファイルにパッケージ化します。パッケージに `php.ini` ファイルを含めます。このファイルに基づいて依存関係がどこに存在するかを特定することができます。

1.5.1.2.16. Python アプリケーション ファイルの準備

Python アプリケーションの場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

  Important

  Python マイクロサービスは、Fortify ScanCentral SAST クライアントを使用してパッケージ化する必要があります。

- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

IDE ツールを使用したコードのパッケージ化

IDE プラグインを使用すると、プロジェクト ファイルとパッケージ化に必要な依存関係を選択できます。IDE ツールの使用の詳細については、「IDE ツール」を参照してください。

コードの手動パッケージ化

OpenText SAST は PY ファイルを Python ソース コードとして処理します。PYC ファイル (コンパイル済み Python ファイル) はサポートされていません。OpenText SAST は、Django および Flask フレームワークの翻訳をサポートしています。

ソース コード ファイルを単一の zip ファイルにパッケージ化します。すべての標準モジュール、サードパーティ モジュール、およびパッケージを含めます。これらは、Python 仮想環境の `lib` フォルダー (少なくとも `site-packages` フォルダーを指定) にあります。

Note

アプリケーションがサポート対象言語に表示されていないバージョンの Python を使用している場合は、サポートに連絡して対応方法をご相談ください。

1.5.1.2.17. Ruby アプリケーション ファイルの準備

Ruby アプリケーションの場合、次のいずれかの方法を使用してアプリケーション ファイルを準備します。

- Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)
- IDE ツールを使用したコードのパッケージ化
- コードの手動パッケージ化

Fortify ScanCentral SAST クライアントを使用したコードの自動パッケージ化 (推奨)

Fortify ScanCentral SAST クライアントは、ソース コードと必要なすべての依存関係をプロジェクトに自動的にパッケージ化します。[ツール] ページから Fortify ScanCentral SAST クライアントをダウンロードして、ビルド マシンにインストールする必要があります。インストールの手順は、zip ファイルに保存されている README.txt ファイルに記載されています。

コマンド ライン インターフェイスで、プロジェクトの作業ディレクトリに移動し、`package` コマンドを実行します。基本的な構文は次のとおりです: `scancentral package o <output_zip>` 。例: `scancentral package o mypayload.zip` 。

Fortify ScanCentral SAST クライアントおよび追加のパッケージ化オプションの詳細については、「Fortify ScanCentral SAST クライアントのインストールと使用」を参照してください。

Note

Fortify ScanCentral SAST パッケージ化は、OpenText Fortify on Demand (FoD) IDE ツールと CICD ツールに組み込まれています。

コードの手動パッケージ化

展開する状態と同じようにアプリケーション全体とすべてのソース コード ファイルを 1 つの zip ファイルにパッケージ化します。

1.5.1.2.18. Solidity アプリケーション ファイルの準備

ソース コード ファイルを zip ファイルにパッケージ化します。すべての依存関係を含めます。

OpenText SAST は Solidity コンパイラ レジストリからコードの pragma 文で参照するコンパイラをダウンロードします。ファイルに pragma 文が含まれていない場合、デフォルトの ^0.8.0 が使用されます。

1.5.1.2.19. Salesforce (Apex および Visualforce) アプリケーション ファイルの準備

Salesforce (Apex および Visualforce) アプリケーションを準備するには、次の手順を実行します。

- Salesforce Web サイトで入手可能な Ant 移行ツールを使用して、アプリケーションを、それを開発して展開する Salesforce 組織 (org) からローカル コンピュータにダウンロードします。 `build.xml` ファイルで指定されたターゲットに対してプロジェクト マニフェスト ファイルが正しく設定されていることを確認してください。
- ダウンロードされたアプリケーションのバージョンには以下が含まれます。
  - `.cls` 拡張子を持つファイル内の Apex クラス
  - `.page` 拡張子を持つファイル内の Visualforce Web ページ
  - `.trigger` 拡張子を持つファイル内のデータベース「トリガー」関数と呼ばれる Apex コード ファイル
  - `.component` 拡張子を持つ Visualforce コンポーネント ファイル
  - `.object` 拡張子を持つオブジェクト
- Ant 移行ツールのドキュメントを使用して取得ターゲットを構成します。組織が AppExchange のアプリケーションを使用している場合は、それらがパッケージ化されたターゲットとしてダウンロードされていることを確認してください。
- ソース コード ファイルを単一の zip ファイルにパッケージ化します。

1.5.1.2.20. Scala アプリケーション ファイルの準備

使用環境内で Scala コードを変換して、アーカイブにパッケージ化する必要があります。Scala コードを変換してスキャン用にパッケージ化するために、Fortify Scala プラグインおよび変換専用バージョンの OpenText SAST が利用可能です。

OpenText SAST のインストール

OpenText SAST の最新バージョンは、ポータルの [ツール] ページから入手できます。Windows、macOS、および Linux オペレーティング システム用のインストーラをダウンロードできます。ソース コードを変換するには、有効なライセンス ファイルが必要です。ライセンスを発行するには、サポートに連絡してください。サポートは [ツール] ページから利用できます。

インストールと使用方法については、OpenText Static Application Security Testing and Tools のドキュメントのを参照してください。

コードの変換

Scala コードを変換するには、Lightbend から次の標準 Lightbend Enterprise Suite ライセンスおよび Fortify Scala プラグインを入手しておく必要があります。OpenText Fortify on Demand サポートに連絡して、ライセンス キーを取得してください。プラグインのダウンロード、および Scala コードの変換の手順については、https://developer.lightbend.com/guides/fortify/ にある Lightbend のドキュメントを参照してください。

Important

アプリケーションに Scala 以外の言語のソース コードが含まれている場合は、別の評価で他のソース コードを送信します。

変換されたコードのパッケージ化

OpenText SAST モバイル ビルド セッション (MBS) では、プロジェクトの変換とプロジェクトのスキャンを別々のマシンで行うことができます。モバイル ビルド セッション ファイル (MBS ファイル) には、スキャンに必要なすべてのファイルが含まれています。

MBS ファイルを生成してパッケージ化するには、次の手順を実行します。

1. 変換を行ったマシンで、次のコマンドを実行し、モバイル ビルド セッションを生成します。

`sourceanalyzer -b <build-id> -export-build-session <file.mbs>`

`<file.mbs>` には、モバイル ビルド セッションに提供するファイル名を指定します。

2. MBS ファイルを zip ファイルのルートにパッケージ化します。他のファイル (追加の MBS ファイルを含む) またはディレクトリを含めないでください。含めると、スキャンがキャンセルされます。
3. **MBS/C/C++/Scala** テクノロジ スタック オプションで、zip ファイルを OpenText Fortify on Demand にアップロードします。

OpenText SAST の使用方法については、OpenText Static Application Security Testing and Tools のドキュメントのを参照してください。

1.5.1.2.21. Android アプリケーション ファイルの準備 (ソース コード)

Android アプリケーションの場合は、Java または Kotlin のソース コード ファイルを単一の zip ファイルにパッケージ化します。Android コードをビルドするために必要なすべての依存関係をアプリケーション プロジェクトに含めます。

Note

OpenText SAST は Xamarin をサポートします。Xamarin アプリケーション ファイルの準備の方法については、「.NET アプリケーション ファイルの準備」を参照してください。Cordova、Ionic Framework、PhoneGap、Unity など、その他のサード パーティ製の開発ライブラリはサポートされていません。

関連トピック:

モバイル評価のための Android バイナリ ファイルの準備方法については、「Android アプリケーション ファイルの準備 (バイナリ)」を参照してください。

1.5.1.2.22. iOS アプリケーション ファイルの準備 (ソース コード)

iOS アプリケーションの場合は、次の手順に従ってソース コード ファイルを準備します。

- アプリケーションはコマンド ラインから xcodebuild を使用してビルドできる必要があります。
- プロジェクトのビルドに必要な依存関係がペイロードに存在し、パスワード保護された Github のような依存関係マネージャーによってアクセスされていないことを確認します。ペイロードは独立してビルド可能である必要があります。
- 開発者または環境固有の設定をアプリケーションから削除します。
- プロジェクトにバイナリ形式のプロパティ リスト ファイルが含まれている場合は、最初にそれらを XML 形式に変換する必要があります。これは、Xcode `plutil` コマンドによって実行できます。
- サード パーティ ライブラリのヘッダーが使用可能であることを確認します。
- Objective-C++ プロジェクトでは、non-fragile Objective-C ランタイム (ABI バージョン 2 または 3) を使用する必要があります。

ソース コード ファイルを単一の zip ファイルにパッケージ化します。

Note

OpenText SAST は Xamarin をサポートします。Xamarin アプリケーション ファイルの準備の方法については、「.NET アプリケーション ファイルの準備」を参照してください。Cordova、Ionic Framework、PhoneGap、Unity など、その他のサード パーティ製の開発ライブラリはサポートされていません。

関連トピック:

モバイル評価のための iOS バイナリ ファイルの準備方法については、「iOS アプリケーション ファイルの準備 (バイナリ)」を参照してください。

1.5.1.3. 静的スキャンの構成

静的スキャン用にアプリケーション ファイルを準備したら、静的スキャンの設定を構成する必要があります。設定は次のスキャンに引き継がれるため、静的スキャンの設定を構成するのはリリースごとに一度だけです。必要に応じて、以降の評価の設定を編集できます。

静的スキャンを構成するには、次の手順を実行します。

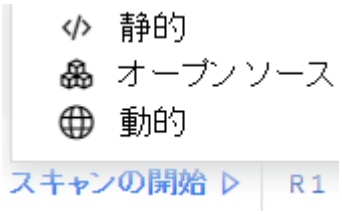
1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. アプリケーション名をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. 評価するリリースに対して [スキャンの開始] をクリックし、[静的] を選択します。



   [静的スキャンの設定] ページが表示されます。

4. 必要に応じてフィールドに入力します。

フィールド	必須	説明
評価タイプ	はい	評価タイプを選択します。組織のセキュリティポリシーで許可されている評価タイプのみが表示されます。 選択した評価タイプの SLO がフィールドの下に表示されます。

フィールド	必須	説明
使用権	はい	評価で使用する使用権を選択します。このフィールドには、購入可能な使用権を含む、選択した評価タイプに有効な使用権が表示されます。マイクロサービス アプリケーションは、サブスクリプションに制限されていることに注意してください。リリースにアクティブなサブスクリプションがある場合は、使用権を使用しないオプションのみが表示されます。

フィールド	必須	説明
		Note ◦ 動的プレミアムまたはモバイル プレミアム評価を介して提供される使用権を選択する場合、評価がアクティブ化され、使用権のすべてのコストが差し引かれます。 ◦ 開発者タイプの使用権がある場合、このフィールドにはその使用権タイプに関連付けられた ID のみが表示されます。

フィールド	必須	説明
監査の設定	はい	監査の基本設定を選択します。 ◦ **手動**: Fortify Audit Assistant によって高い信頼度で識別された誤検知が自動的に抑制されます。次に、セキュリティ エキスパートがスキャン結果を手動で確認します。 ◦ **自動**: Fortify Audit Assistant によって高い信頼度で識別された誤検出が自動的に抑制され、人による確認が行われることなく結果が発行されます。

フィールド	必須	説明
		Note Fortify Audit Assistant は、スキャンで見つかった新しい問題にのみ適用されます。自動監査を使用したスキャンで見つかった新しい問題には、誤検知の再確認は使用できません。 監査設定を選択する機能は、評価タイプによって異なります。 ◦ 静的単一スキャンでは、[自動] のみが許可されます。 ◦ 静的サブスクリプションでは、(リリースまたはマイクロサービスごとではなく) アプリケーションごとに 1 つの [手動] による監査が許可されます。 ◦ 静的+ 単一スキャンでは、[手動] のみが許可されます。

フィールド	必須	説明
		◦ 静的+ サブスクリプションでは、各評価に対して [自動] または [手動] による監査が許可されます。
Fortify Remediation Aviator	いいえ	自動監査を使用したスキャンの場合は、このチェック ボックスをオンにして Fortify Remediation Aviator の監査結果を保持し、拡充された修復支援が提供されるようにします。このオプションは、Fortify Remediation Aviator がセキュリティ ポリシーで許可されている場合は既定で選択されます。許可されていない場合、このオプションは無効になります。 このサービスは、追加の評価ユニットを 1 つ消費します。Fortify Remediation Aviator サービスが実行されない場合、使用権は差し引かれません。Fortify Remediation Aviator の詳細については、「Fortify Remediation Aviator の監査と修復」を参照してください。

フィールド	必須	説明
ソフトウェア構成分析	いいえ	オープン ソース ソフトウェア構成分析を含める場合は、チェック ボックスをオンにします。コードが OpenText Fortify on Demand 環境の外に出ることはありません。ソフトウェア構成分析を静的スキャンの一環として追加する方法の詳細については、「オープン ソース ソフトウェア構成分析」を参照してください。

フィールド	必須	説明
静的セキュリティ評価のためにサードパーティのライブラリをスキャンする	いいえ	**Note** サポート チームに連絡して、オプションを有効にします。 (オプション) チェックボックスを選択すると、サードパーティ ライブラリの脆弱性がスキャンされ、スキャン結果に含められます。これによって所要期間を大幅に短縮できます。このオプションはマイクロサービス アプリケーションでは利用できません。

フィールド	必須	説明
		Note このオプションを選択すると、組織がすべてのサード パーティ ベンダーからライブラリをスキャンする同意を得ていることを認めたことになります。

5. 必要な場合は、必須フィールドの下に表示されるセクションに追加のスキャン設定を構成できます。

   [**詳細設定**] をクリックして、必要に応じてフィールドに入力します。

フィールド	説明
スキャン ポリシー	スキャンに使用するスキャン ポリシーを選択します。使用可能なポリシーは次のとおりです。 ◦ セキュリティ **Note** バージョン 26.3 以降では、これはすべてのアプリケーションとリリースの最初のスキャンで既定の設定となります。 ◦ DevOps ◦ クラシック ◦ FoD (レガシー) **Note** アプリケーションまたはリリースに対して既にスキャンが存在する場合、既定のポリシーは FoD (レガシー) になります。
テクノロジ スタック	アプリケーションのテクノロジ スタックを選択します。選択可能な言語は、アプリケーション タイプ (Web/シック クライアントまたはモバイル) と、アプリケーションがマイクロサービス アプリケーションかどうかによって異なります。 自動検出機能が有効になっている場合は、[**自動検出**] を選択すると、OpenText Fortify on Demand がペイロードの内容に基づいてテクノロジ スタックを決定します。

フィールド	説明
言語レベル	適用可能な場合、リストからテクノロジ スタックの言語レベルを選択します。

[**レガシー設定**] をクリックして、必要に応じてフィールドに入力します。

フィールド	説明	廃止に関する注意事項
ビルド サーバーの統合	静的スキャンの設定 (評価タイプ、テクノロジスタック、言語レベル、監査の基本設定、ソフトウェア構成分析) が構成されると、[**ビルド サーバーの統合**] フィールドにトークンが自動的に入力されます。トークンは、外部ツールを使用して静的評価を送信するために使用できます。 **Note** BSI トークンは、リリースの評価全体で永続的です。	リリース ID は、BSI トークンを置き換えます。ビルド構成は、なるべく早くリリース ID に移行してください。

フィールド	説明	廃止に関する注意事項
ソース コントロール	ペイロードをアップロードする方法を選択します。 ◦ **手動アップロード** (既定): ペイロードをローカル システムから手動でアップロードします。 ◦ **ソース コントロール**: ペイロードをバージョン コントロール プラットフォームからアップロードします。このオプションは、ソース コントロールが設定されている場合に利用できます。詳細については、「ソース コントロールの統合」を参照してください。	この機能は廃止される予定です。なるべく早く、レガシー ソース管理統合を、該当するバージョン管理プラットフォーム上のパイプラインに移行する必要があります。詳細については、「CICD ツール」を参照してください。

フィールド	説明	廃止に関する注意事項
スキャン バイナリ	**Note** サポート チームに連絡して、オプションを有効にします。 (Java/J2EE/Kotlin、.NET、および .NET Core テクノロジ スタック) コンパイル済みファイルとソース コード ファイルをスキャンする場合は、チェック ボックスをオンにします。Fortify ScanCentral SAST でパッケージ化されたペイロードの場合、バイナリ ファイルのスキャンはサポートされていません。	

フィールド	説明	廃止に関する注意事項
	Note ソース コードを含める要求が有効で、このオプションがオンになっていない場合で、ペイロードにソース コードが含まれない場合、スキャンはキャンセルされます。	

6. [**DevOps と IDE の統合**] をクリックして、リリース ID を表示します。リリース ID は、CICD ツールを使用して静的スキャンを送信するために使用できます。リリース ID は、ポータルに保存されている最新のスキャン設定を取得するためのトークンになります。
7. [**保存**] をクリックします。

   静的スキャンの設定が保存されます。
8. 使用権の使用権限を保有し、使用権サブスクリプションを選択している場合は、[**購読の開始**] をクリックして、静的評価サブスクリプションを開始し、直ちに使用権を使用します。ユーザーが最初のスキャンを開始すると、権利から評価コストが差し引かれます。

Note

サポート チームに連絡して、オプションを有効にします。

1.5.1.4. 静的評価ペイロードのアップロード

アプリケーション ファイルをパッケージ化し、静的スキャンの設定を構成したら、スキャンのペイロードをアップロードします。最大ペイロード サイズの制限は 5 GB ですが、Web ブラウザーにも最大サイズに関する独自の制限があります (詳細については、お使いのブラウザーのドキュメントを参照してください)。大きなファイルをアップロードする際にポータルでタイムアウトが発生することがあるため、ファイル サイズが 500 MB 未満の場合にのみポータルを介してアップロードする必要があります。ポータルを介してアップロードできない場合は、「関連トピック」を参照して、ファイルをアップロードする別の方法をお試しください。またはサポート チームに連絡して、最適なアップロード オプションについてご相談ください。

進行中の状態にできるのは、リリースごとに 1 つの静的スキャンのみです。同じリリースのスキャンを含めて、アプリケーションの複数のスキャンを送信できます。その他のスキャンはキューに配置され、キューに配置された順にスキャンされます。各アプリケーションのキューには、スキャンを 30 個まで含めることができます。

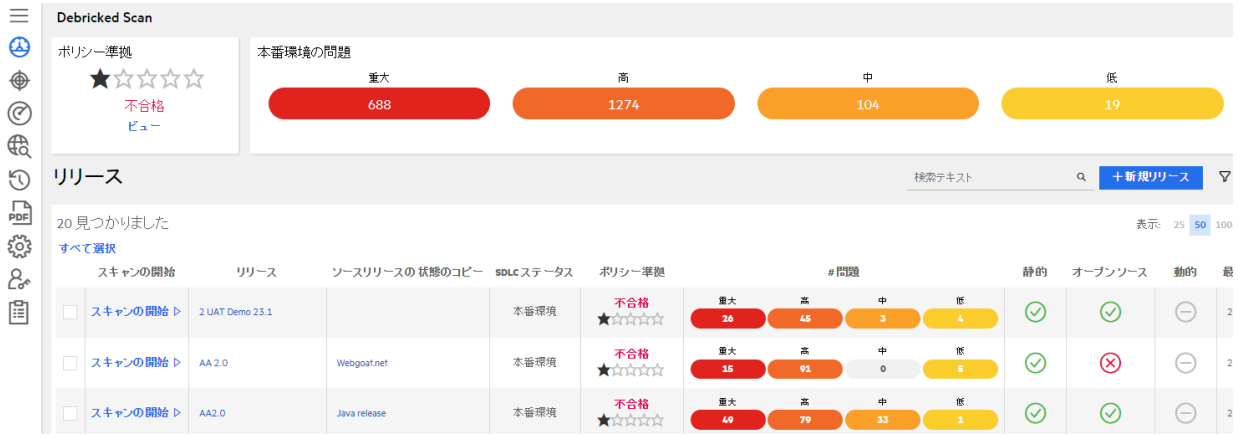
ポータルから静的評価ペイロードをアップロードするには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

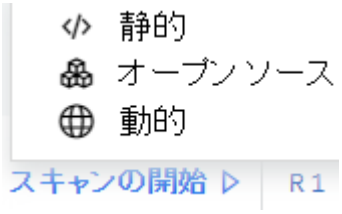
   [アプリケーション] ページが表示されます。

2. アプリケーション名をクリックします。

   [アプリケーションの概要] ページが表示されます。



3. 評価するリリースに対して [スキャンの開始] をクリックし、メニューから [静的] を選択します。



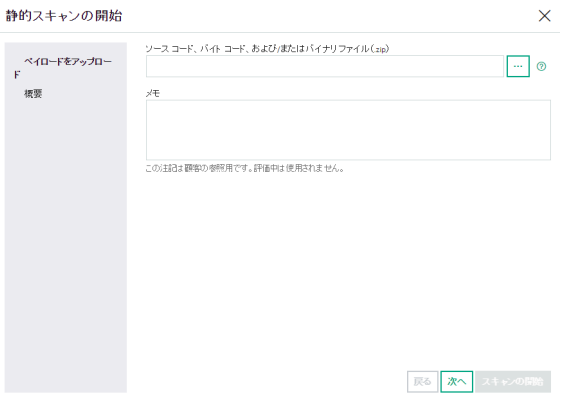
[静的スキャンの設定] ページが表示されます。

4. **[スキャンの開始]** をクリックします。

> **Note**
>
> アプリケーションで静的スキャンがアクティブになっている場合は、別のスキャンの開始がブロックされます。

[静的スキャンの開始] ウィンドウが開きます。

5. アップロードの方法に基づいて、関連するタスクを実行します。

アップロードの方法	手順
手動アップロード	 1. ... をクリックします。 2. zip ファイルに移動して選択します。

アップロードの方法	手順
ソース コントロール	 1. [**ソースの場所**] リストから [**ブランチ**] または [**リリース**] を選択します。 2. 特定のブランチまたはリリースを選択します。

6. フィールドに、アプリケーションの説明を入力します。

7. [**次へ**] をクリックします。

   静的スキャンの設定値の概要が表示されます。

8. 概要を確認します。必要に応じて、[**戻る**] をクリックし、修正を行います。値が正しい場合、[**スキャンの開始**] をクリックします。

   zip ファイルのアップロードが完了すると、[リリース スキャン] ページにリダイレクトされ、新しいスキャンのステータスが [**キューに配置**] になります。スキャンはキューの先頭に移動すると開始されます。

関連トピック

ポータルを使用するだけでなく、次の方法を使用して静的評価を送信することもできます。

- IDE プラグイン ツール: Visual Studio Extension、Eclipse Plugin、IntelliJ プラグイン、Fortify Extensions for Visual Studio Code。詳細については、「IDE ツール」を参照してください。
- ビルド サーバーの統合ツール: FoDUploader、Fortify Azure DevOps Extension、OpenText Fortify on Demand Jenkins Plugin。詳細については、「CICD ツール」を参照してください。
- OpenText Fortify on Demand API。詳細については、「OpenText Fortify on Demand API」を参照してください。

1.5.1.5. 静的評価のペイロード検証

ペイロードをアップロードした後、OpenText Fortify on Demand は次のペイロード検証チェックを実行し、静的テスト チームが静的評価を開始するために必要な条件が満たされていることを確認します。

- .zip ファイルが有効で破損していないこと
- ペイロードには、OpenText SAST でサポートされているファイル拡張子が含まれています。サポートされているファイル拡張子は次のとおりです: ABAP、abap、appxmanifest、as、asax、ascx、ashx、asmx、asp、aspx、baml、bas、bicep、BSP、bsp、cbl、cfc、cfm、cfml、class、cls、cob、conf、Config、config、cpx、cs、cscfg、csdef、cshtml、ctl、ctp、dart、dll、Dockerfile、dockerfile、erb、exe、frm、go、hcl、htm、html、inc、ini、jar、java、jmod、js、jsff、json、jsp、jspf、jspx、jsx、kt、kts、Master、master、mbs、mxml、page、php、phtml、pkb、pkh、pks、plist、properties、py、razor、rb、scala、settings、sol、sql、swift、tag、tagx、tf、tld、trigger、ts、tsx、vb、vbhtml、vbs、vbscript、wadcfg、wadcfgx、winmd、wsdd、wsdl、xaml、xcfg、xhtml、xmi、xml、xsd、yaml、yml。
- .NET アプリケーションの場合は、ペイロードに .dll または .exe ファイルが含まれていること
- Java および Kotlin アプリケーションの場合、ペイロードには .class、.java、.jar、.jsp、.kt、.ktm、または .kts ファイルが含まれます。
- Fortify ScanCentral SAST でパッケージ化したペイロードでは、[**スキャン バイナリ**] スキャン設定が有効になっていないこと
- Python マイクロサービス アプリケーションの場合、ペイロードは Fortify ScanCentral SAST クライアントを使用してパッケージ化されます。
- モバイル ビルド セッション (MBS) ファイルの送信が必要になるテクノロジ スタックでは、ペイロードに .mbs ファイルを 1 つだけ含めること
- ソース コードを含める要求が有効になっているテナントでは、ペイロードに次のファイル形式のファイルを含めます。

テクノロジ スタック	ソース ファイルの拡張子
.NET	.cs、.vb
ABAP	.abap
ASP	.asp
CFML	.cfm、.cfml、.cfc
COBOL	.cbl、.cob、.ccp、.cb2
Dockerfile/Infrastructure as Code	.dockerfile、.json、.xml、.tf、.yaml、dockerfile
Go	.go
JAVA/J2EE/Kotlin	.java、.kt、.ktm、.kts
JS/TS/HTML	.xsd、.xmi、.wsdd、.config、.cpx、.xcfg、.js、.ts
PHP	.php
PYTHON	.py
VB6	.vbs、.bas、.frm、.ctl、.cls
VBScript	.vbscript
Ruby	.rb

満たされていない条件があるとスキャンは自動的にキャンセルされ、キャンセルの理由を示す電子メールが送信されます。ファイルを受け取ると、コードが安全なサーバーに転送されて解析されます。

1.5.2. オープン ソース ソフトウェア構成分析

OpenText Fortify on Demand は、オープン ソース ソフトウェア構成分析を静的評価と組み合わせて、または独立した評価として提供します。アプリケーションは、次のソフトウェア構成分析ツールのいずれかを使用してスキャンされます。

- OpenText Core SCA (静的評価と組み合わせて、または独立した評価として提供)
- Sonatype (静的評価と組み合わせて提供、購入不可)

サポートされる言語は、C# (.NET)、Go、Java、JavaScript、Kotlin、Objective-C、PHP、Python、Ruby、および Swift です。

オープン ソース ソフトウェア構成分析を有効にするには、OpenText Core SCA の使用権を購入してください。使用権は、1 アプリケーションにつき 1 つの OpenText Core SCA サブスクリプションに使用されます。オープン ソース スキャンの送信時、ソフトウェア構成分析ツールは、オープン ソース コンポーネントがペイロードに含まれているかどうかを確認します。オープン ソース スキャン結果は、関連するセキュリティの問題とライセンスとともに、直接的および推移的な依存関係を特定します

アクティブな Sonatype 使用権を持たないテナントは、静的サブスクリプションごとに 5 つの補完的な Debricked スキャンを受け取ります。補完的なスキャンはサブスクリプション期間内に限ります。テナントがオープン ソース スキャンの権利を購入すると、補完的なスキャンは無効になります。

OpenText Core SCA の使用権に関心をお持ちの場合は、営業担当までお問い合わせください。

このセクションでは、次のトピックについて説明します。

1.5.2.1. オープン ソースの評価ファイルの準備

オープン ソース スキャンの場合、ペイロードに必要なファイルは、使用されているソフトウェア構成分析ツールによって異なります。

ロック ファイル分析の OpenText Core SCA ファイル要件

依存関係を確実に検出するために、OpenText Core SCA は、ビルド システムまたはパッケージ マネージャーに応じて、次のいずれかのアプローチを使用します。

- 一部のパッケージ マネージャーは、ロック ファイルを使用してプロジェクト内の依存関係を記述します (npm など)。通常、パッケージ マネージャーは自動的にロック ファイルを生成します。OpenText Core SCA は、ネイティブ ロック ファイルを使用した依存関係のスキャンをサポートしています。
- ビルド システム、パッケージ マネージャー、またはロック ファイルを使用しないビルド システム (Maven、Gradle など) の場合、OpenText Core SCA では、解決された依存関係ツリーを記述したファイルをビルド システムまたはパッケージ マネージャーの機能を使用して生成する必要があります。このファイルは OpenText Core SCA ロック ファイルと呼ばれます。

  次のいずれかの方法を使用して、ネイティブ ロック ファイルと OpenText Core SCA ロック ファイルの両方を生成できます。

  - (推奨) Fortify ScanCentral SAST クライアント (22.1.2 以降) を使用して、アプリケーション ファイルとともにロック ファイルを生成します。`package` コマンドに `-oss` オプションを追加して OpenText Core SCA CLI を呼び出し、ロック ファイルをパッケージに追加します。パッケージの生成は、ロック ファイルが正常にパッケージ化されるかどうかに依存しないことに注意してください。
  - (推奨) OpenText Core SCA CLI を実行して、アプリケーション ファイルとは別にロック ファイルを生成します。インストール手順および使用方法については、README.FoD.md を参照してください。
  - ロック ファイルを手動で生成します。CICD パイプラインに適切なコマンドを追加して、このプロセスを自動化できます。

次の表は、OpenText Fortify on Demand での OpenText Core SCA スキャンのファイル要件を示しています。

Important

必要なロック ファイルがペイロードに存在しない場合、OpenText Core SCA スキャンはキャンセルされます。

言語	パッケージ マネージャー	必要なファイル	メモ (Fortify ScanCentral SAST クライアントを使用しない場合)
C#	NuGet	`packages.lock.json`	ロック ファイルを生成するには、次のいずれかの方法を使用します。 • Debricked CLI から `debricked resolve` を実行します。詳細については、C# - Nuget, Paket を参照してください。 • .NET CLI から `dotnet restore --use-lock-file` を実行します。詳細については、ロック ファイルを使用した繰り返し可能なパッケージの復元の有効化に関する説明を参照してください。 • `.csproj` プロジェクト

言語	パッケージ マネージャー	必要なファイル	メモ (Fortify ScanCentral SAST クライアントを使用しない場合)
			ファイルで MSBuild プロパティ `RestorePackagesWithLockFile` を `true` に設定し、Nuget `restore` コマンドを実行します。詳細については、ロック ファイルを使用した繰り返し可能なパッケージの復元の有効化に関する説明を参照してください。
	Paket	`paket.lock`	`paket.lock` は Packet によって自動的に生成されます。

言語	パッケージ マネージャー	必要なファイル	メモ (Fortify ScanCentral SAST クライアントを使用しない場合)
Go	Go Dep	`gopkg.lock`	`gopkg.lock` は dep によって自動的に生成されます。 **Note** Go Dep は廃止予定であるため、Go Dep の更新は行われません。
	Go モジュール	`gomod.debricked.lock`	解決された依存関係ツリー ファイルを生成する手順については、「Go - Go モジュール、Go Dep、Bazel」を参照してください。

言語	パッケージ マネージャー	必要なファイル	メモ (Fortify ScanCentral SAST クライアントを使用しない場合)
Java/Kotlin	Bazel	WORKSPACE	WORKSPACE は Bazel によって自動的に生成されます。
		(推奨) `maven_install.json`	`rules_jvm_external` を使用して、すべての依存関係がそれぞれのバージョンに固定される `maven_install.json` を生成します。詳細については、推移的な Maven 依存関係を計算するためのリポジトリ ルールに関する説明を参照してください。
	Gradle	`gradle.debricked.lock`	解決された依存関係ツリー ファイルを生成する手順については、「Java と Kotlin - Gradle、Maven、Bazel」を参照してください。

言語	パッケージ マネージャー	必要なファイル	メモ (Fortify ScanCentral SAST クライアントを使用しない場合)
	Maven	`maven.debricked.lock`	解決された依存関係ツリー ファイルを生成する手順については、「Java と Kotlin - Gradle、Maven、Bazel」を参照してください。
JavaScript	Bower	`bower.debricked.lock`	解決された依存関係ツリー ファイルを生成する手順については、「JavaScript - NPM, Yarn, Bower」を参照してください。

言語	パッケージ マネージャー	必要なファイル	メモ (Fortify ScanCentral SAST クライアントを使用しない場合)
	npm	`package-lock.json`	`npm install` コマンドは、.npmrc ファイルで無効にされていない限り、自動的に `package-lock.json` を生成します。 `npm install --package-lock-only` コマンドは、 `package-lock.json` のチェックと依存関係のダウンロードを行わずに `node_modules` を生成します。
	Yarn	`yarn.lock`	`yarn.lock` は Yarn によって自動的に生成されます。
Objective-C	Cocoapods	`podfile.lock`	`podfile.lock` は、Cocoapods によって自動的に生成されます。

言語	パッケージ マネージャー	必要なファイル	メモ (Fortify ScanCentral SAST クライアントを使用しない場合)
PHP	Composer	`composer.lock`	`composer.lock` は、Composer によって自動的に生成されます。
Python	pip	`<file_name>.pip.debricked.lock`	解決された依存関係ツリー ファイルを生成する手順については、「Python - Pip, Pipenv」を参照してください。
	Pipenv	`Pipfile.lock`	`Pipfile.lock` は、プロジェクトの仮想環境に基づいて Pipenv によって自動的に生成されます。
Ruby	RubyGems	`Gemfile.lock`	`Gemfile.lock` は、RubyGems によって自動的に生成されます。
Swift	Cocoapods	`podfile.lock`	`podfile.lock` は、Cocoapods によって自動的に生成されます。

業界のベスト プラクティスに従って、ロック ファイルをソース コントロール リポジトリにコミットする必要があります。これにより、特に Fortify ScanCentral SAST クライアントを使用してペイロードをパッケージ化していない場合に、アプリケーション ファイルの準備プロセスが簡素化されます。

フィンガープリント分析の OpenText Core SCA ファイル要件

OpenText Core SCA は、アプリケーション ファイル (バイナリ ファイルを含む) のフィンガープリントを調べることで、マニフェスト ファイルで定義されていない管理対象外の依存関係のスキャンをサポートします (無関係なファイルの除外がいくつかあります)。`debricked.fingerprints.txt` ファイルが必要です。このファイルは、OpenText Core SCA スキャンを送信したときに OpenText Fortify on Demand によって自動的に生成されるファイルです。OpenText Core SCA スキャンには、フィンガープリント分析とロック ファイル分析の両方が含まれます。OpenText Core SCA ファイル フィンガープリント (現在サポートされている言語を含む) の詳細については、「ファイルのフィンガープリント」を参照してください。

場合によっては、ファイルのフィンガープリントから得られるパッケージやバージョンが、アプリケーションで使用される依存関係と異なる可能性があります。ユーザーは、特定のファイルまたはパスのフィンガープリントを除外することで、結果が正しいことを確認できます。これを行うには、マニフェスト ファイルに正しい依存関係を追加します。OpenText Core SCA CLI を使用した CycloneDX SBOM。または、`debricked-config.yaml` ファイルを生成して結果を上書きします。依存関係の除外の詳細については、「結果の管理または上書き」を参照してください。

Sonatype ファイルの要件

Sonatype スキャンのファイル要件については、
https://help.sonatype.com/iqserver/analysis を参照してください。

1.5.2.2. ポータルからのオープン ソース評価ペイロードのアップロード

オープン ソース ペイロードのアップロード方法は、オープン ソースの評価に静的評価が含まれているか、別に実行されるかどうかによって異なります。

- 静的スキャン評価にオープン ソース評価を含めるには、オープン ソース スキャンを含めるように静的スキャン設定を構成します。静的評価ペイロードには、必要なオープンソース ファイルを含めます。この方法は、OpenText Core SCA と Sonatype のどちらにも使用できます。詳細については、「静的スキャンの構成」を参照してください。
- オープン ソース評価を別途実行するには、ネイティブまたは OpenText Core SCA ロック ファイルをアップロードします。次の手順では、OpenText Core SCA のみのスキャンを送信する方法について説明します。

> **Note**
>
> サード パーティ ソフトウェアの部品表に対する OpenText Core SCA スキャンを送信できます。詳細については、「ソフトウェア部品表のインポート」を参照してください。

OpenText Core SCA のみのスキャンを送信するには、次の手順を実行します。

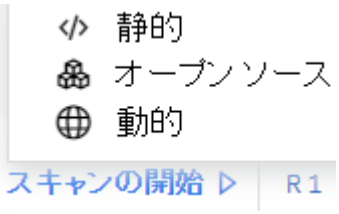
1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

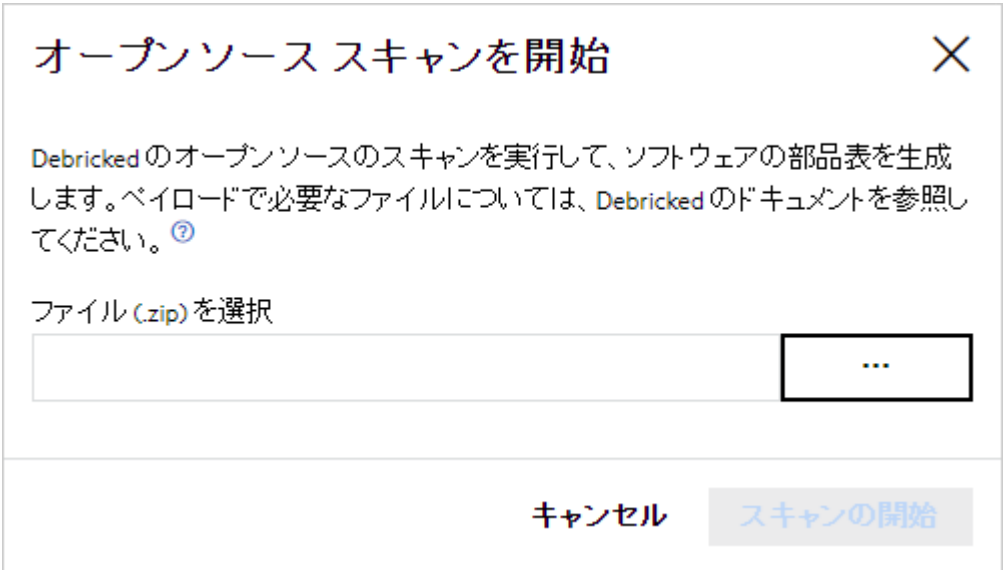
2. アプリケーション名をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. 評価するリリースに対して [スキャンの開始] をクリックし、[オープン ソース] を選択します。



[オープン ソース スキャン] ウィンドウが開きます。



4. **...** をクリックします。
5. ロック ファイルが含まれている zip ファイルに移動して選択します。zip ファイルには静的評価ペイロードか、またはロック ファイルのみのいずれかを含めることができます。
6. **[スキャンの開始]** をクリックします。

   zip ファイルのアップロードが完了すると、[リリース スキャン] ページにリダイレクトされ、新しいスキャンのステータスが [**キューに配置**] になります。スキャンはキューの先頭に移動すると開始されます。

1.5.2.3. リリース内のオープン ソース コンポーネントの表示

リリースの最新のスキャンにあるオープン ソース コンポーネントを表示できます。

リリースのオープン ソース コンポーネントを表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. [**オープン ソース コンポーネント**] をクリックします。

   [オープン ソース コンポーネント] ページが表示されます。

4. 複数のスキャン ツールの結果を使用できる場合は、結果を表示するソースをドロップダウン リストから選択します。

   ページが更新されて、選択したソースの結果が表示されます。

次の表に、[オープン ソース コンポーネント] ページの操作方法を示します。

タスク	アクション
オープン ソース コンポーネント リストをエクスポートする	[**エクスポート**] をクリックします。CSV ファイルをダウンロードするリンクがアカウント設定で指定された電子メール アドレスに送信されます。リンクは電子メールが送信されてから 7 日間有効です。
特定のスキャン ツールの結果を表示する	ドロップダウン リストから、表示するスキャン ツールを選択します。
オープン ソース コンポーネント リストを検索する	検索テキスト フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。
列の値によるフィルタリングと並べ替え	[**コンポーネント**]、[**ライセンス**]、[**スキャン ツール**]、[**スコープ**]、[**タイプ**] のいずれかの列見出しをクリックします。
パッケージ URL でフィルターされた問題を表示する	各コンポーネント行の問題数をクリックします。
コンポーネントのパッケージ URL と Open Source Select のリンクを表示する	[**詳細**] アイコンをクリックします。

1.5.2.4. テナント内のオープン ソース コンポーネントの表示

[**サードパーティのアプリを表示**] 権限を持つユーザーは、識別されたすべてのオープン ソース コンポーネントとこれらを使用しているアプリケーションについて、テナント規模の概要を表示できます。

テナント全体のオープン ソース コンポーネントを表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**オープン ソース コンポーネント**] をクリックします。

   [オープン ソース コンポーネント] ページが表示されます。

> **Note**
>
> 廃棄されたリリースからのオープン ソース スキャンの結果は除外されます。

次の表に、[オープン ソース コンポーネント] ページの操作方法を示します。

タスク	アクション
オープン ソース コンポーネント リストをエクスポートする	[**エクスポート**] をクリックします。CSV ファイルをダウンロードするリンクがアカウント設定で指定された電子メール アドレスに送信されます。リンクは電子メールが送信されてから 7 日間有効です。
特定のスキャン ツールの結果を表示する	ドロップダウン リストから、表示するスキャン ツールの結果を選択します。
オープン ソース コンポーネント リストを検索する	検索テキスト フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。
列の値によるフィルタリングと並べ替え	[**コンポーネント**]、[**ライセンス**]、[**スキャン ツール**]、[**スコープ**]、[**タイプ**] のいずれかの列見出しをクリックします。
アプリケーション、およびコンポーネントを使用する対応するリリースを表示します。	コンポーネントの行で [**リリースを表示**] をクリックします。
コンポーネントのパッケージ URL と Open Source Select のリンクを表示する	[**詳細**] アイコンをクリックします。

1.5.3. 動的評価

動的評価では、セキュリティの脆弱性調査のため、実行している Web アプリケーションを分析します。動的評価には、OpenText DAST を利用した自動テストおよび手動分析が含まれます。

OpenText DAST を使用した動的テストには、次のモードが含まれます。

- クロール (OpenText DAST がターゲット Web サイトの構造を識別するプロセス)
- 監査 (実際の脆弱性スキャン)

このセクションでは、次のトピックについて説明します。

- 動的テストに向けた Web サイトの準備
- Web API ファイルの準備
- OpenText Fortify on Demand Connect のセットアップ
- 動的スキャンの構成
- 動的スキャンのスケジュール
- 進行中のスキャンおよび完了したスキャンに対する動的スキャンの設定の編集

1.5.3.1. 動的テストに向けた Web サイトの準備

テスト プロセスを円滑に行うため、すべての動的評価で次の準備を行います。

- 評価を行う前に、Web アプリケーションが機能していること、およびユーザー資格情報が有効であることを確認します。Web アプリケーションがクライアント証明書認証を使用する場合は、サポートにお問い合わせください。
- テスト期間中は、すべての多要素認証コントロールを無効にします。これには、SMS メッセージ、電子メール検証、CAPTCHA、OATH トークン、物理トークンなどのセカンダリ認証メカニズムが含まれます。あるいは、非認証ユーザーが使用できるアプリケーション コンテンツのセキュリティを評価するために、評価を非認証で実行することもできます。
- すべての機能テストおよびパフォーマンス テストを評価前に完了し、テスト期間中にアプリケーションのコードを停止します。
- 一般的な注意事項として、OpenTextMSP ポータルでは、テスト プロセスを開始する前にすべてのデータをバックアップしておくことをお勧めします。テスト完了時には、問題のないことが分かっているデータをバックアップから復元し、データ破損が発生する可能性を排除します。

- OpenText Fortify on Demand の IP アドレスを、ファイアウォール、IPS、IDS、および WAF の許可リストに追加し、動的テスト チームがアプリケーションをスキャンできるようにします。IP アドレスはポータルの [動的スキャンの設定] ページから取得できます。状況によっては、ユーザーの許可を得てアドホック アドレスが使用される場合があります。

- OpenText Fortify on Demand の IP アドレスをセキュリティ運用チームとネットワーク運用チームに提供します。これにより、チームは、サイトに攻撃が送信されているのを確認しても、その攻撃が計画された反復セキュリティ スキャンの一環であることを把握でき、その IP アドレスをブロックしないようにします。
- Web サイトが http/https デフォルト ポート (80/443) を介してアクセス可能である限り、評価のために追加のポートを開く必要はありません。

- 内部サイトの場合は、OpenText Fortify on Demand Connect を使用してサイト間 VPN を設定します。詳細については、「Fortify on Demand 接続の設定」を参照してください。

スキャン プロセス中に自動化を利用する動的評価の場合は、次の準備を行ってください。

- ワークフロー マクロを作成して、スキャンをワークフロー駆動スキャンとして実行します。ワークフロー マクロは、Web Macro Recorder ツールを使用して Web サ

イトを操作したときの HTTP イベントの記録です。ポータルの [ツール] ページで利用できる OpenText DAST のイベントベースの Web Macro Recorder を使用して、ワークフロー マクロを作成できます。ワークフロー マクロの作成手順については、OpenText DAST ドキュメントの『*OpenText™ Dynamic Application Security Testing Tools ガイド*』を参照してください。

- 認証用のログイン マクロを作成します。ログイン マクロは、Web Macro Recorder ツールを使用して Web サイトにアクセスしてログインしたときに発生するイベントの記録です。ポータルの [ツール] ページで利用できる OpenText DAST のイベントベースの Web Macro Recorder を使用して、ログイン マクロを作成できます。ログイン マクロの作成手順については、OpenText DAST ドキュメントの『*OpenText™ Dynamic Application Security Testing Tools ガイド*』を参照してください。

Note

API を使用していて、動的評価タイプから DAST 自動評価タイプに切り替える場合は、スキャンを開始する前にポータルからログイン マクロをアップロードします。

1.5.3.2. Web API ファイルの準備

動的評価に Web API のテストが含まれる場合は、適切なセキュリティ テストのために、作業中のサンプル データを含むプロジェクト ファイルを提供する必要があります。次のガイドラインに従ってプロジェクト ファイルを準備します。

> **Note**
>
> 作業中のサンプル データを含むプロジェクト ファイルがない場合は、QA チームと開発チームに依頼して、これらのファイルを取得してください。通常は、Web API 機能をテストするために、これらの一連のファイルが用意されています。

REST

- OpenAPI ドキュメント ファイル、URL、Postman コレクション ファイル、URL などの API 定義を指定します。

  > **Note**
  >
  > Postman 環境ファイルはサポートされていません。

- リクエストには、ベースライン アプリケーションの動作を確立するための有効なパラメーター値を含める必要があります。
- API に認証が必要な場合は、テスト期間を通じて有効な資格情報を指定します。
  - Postman コレクションを提供している場合は、Postman コレクションで認証を構成します。

    > **Note**
    >
    > 動的認証はサポートされていません。

  - OpenAPI ドキュメントを提供している場合は、[動的スキャンの設定] ページに資格情報を指定します。

SOAP

- Web Service Definition Language (WSDL) のファイルまたは URL を指定します。
- テキストまたは XML 形式、あるいは SoapUI プロジェクトまたは Postman コレクション ファイルとしてリクエストと応答のペアを指定します。

- リクエストには、ベースライン アプリケーションの動作を確立するための有効なパラメーター値を含める必要があります。
- API に認証が必要な場合は、テスト期間を通じて有効な資格情報を指定します。
- SoapUI プロジェクトまたは Postman コレクション ファイルを送信する場合は、プロジェクト ファイル内で認証を構成します。[**追加メモ**] フィールドまたは [**追加資料**] フィールドに情報を指定することもできます。

gRPC

- proto ファイルを指定します。追加のインポートが必要な場合は、プライマリ proto ファイルと結合して「マスター」proto ファイルを作成する必要があります。gRPC proto ファイルは自己完結型である必要があります。インポートは、ユーザーが生成したファイルではなく、内部的に認識されたリソースに対して行う必要があります。OpenText DAST では、インポートされた proto ファイルからファイル パスを識別できません。

GraphQL

- GraphQL イントロスペクション ファイルまたは URL を指定します。スキャン用のスキーマ コンテンツをダウンロードするには、GraphQL API でイントロスペクションが有効になっている必要があります。

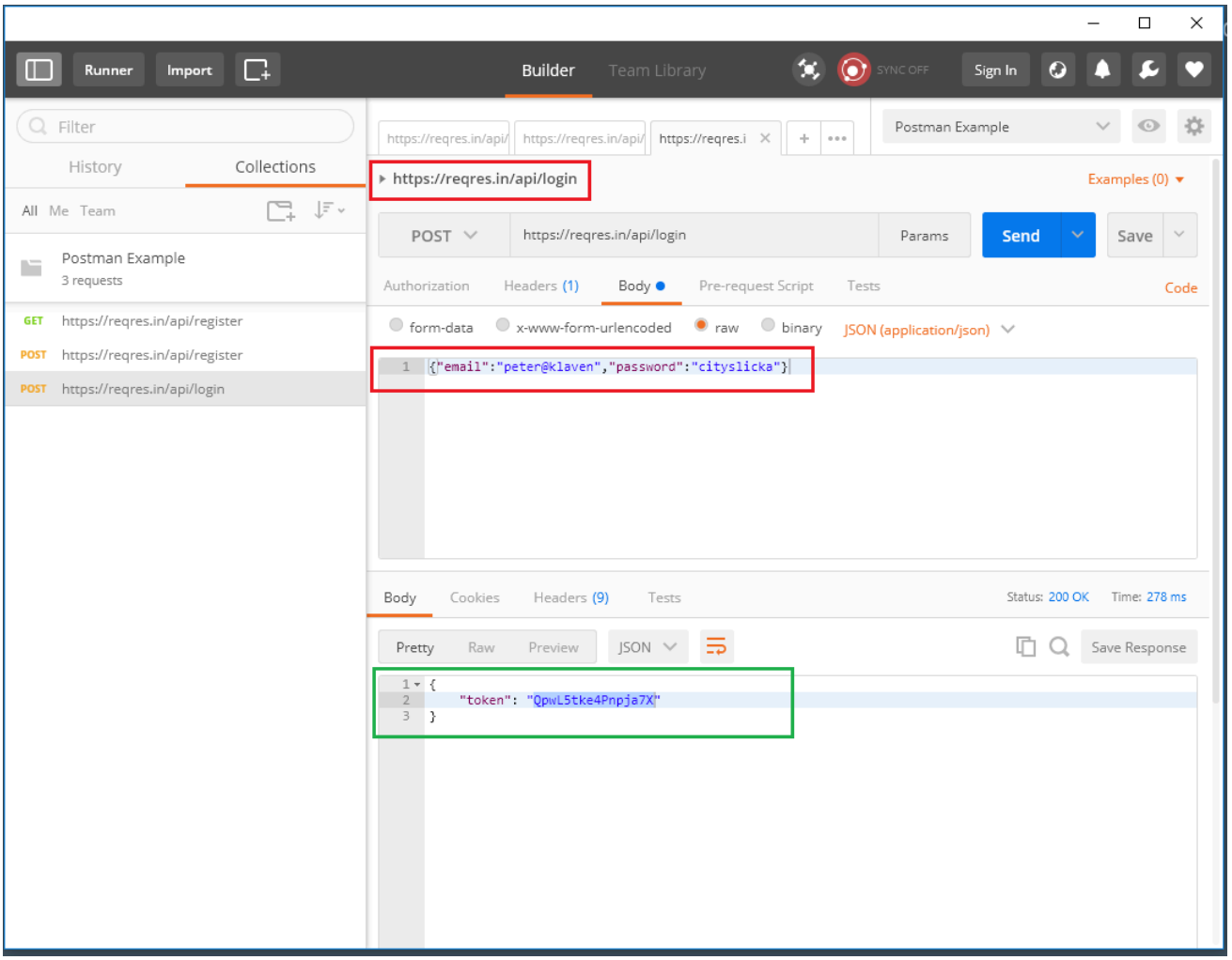
例

次に、作業中のサンプル データを含むプロジェクト ファイルの例を示します。

Note
指定する必要があるのは、入力パラメータ値のみです。応答は、ここでは単なる情報として示されています。

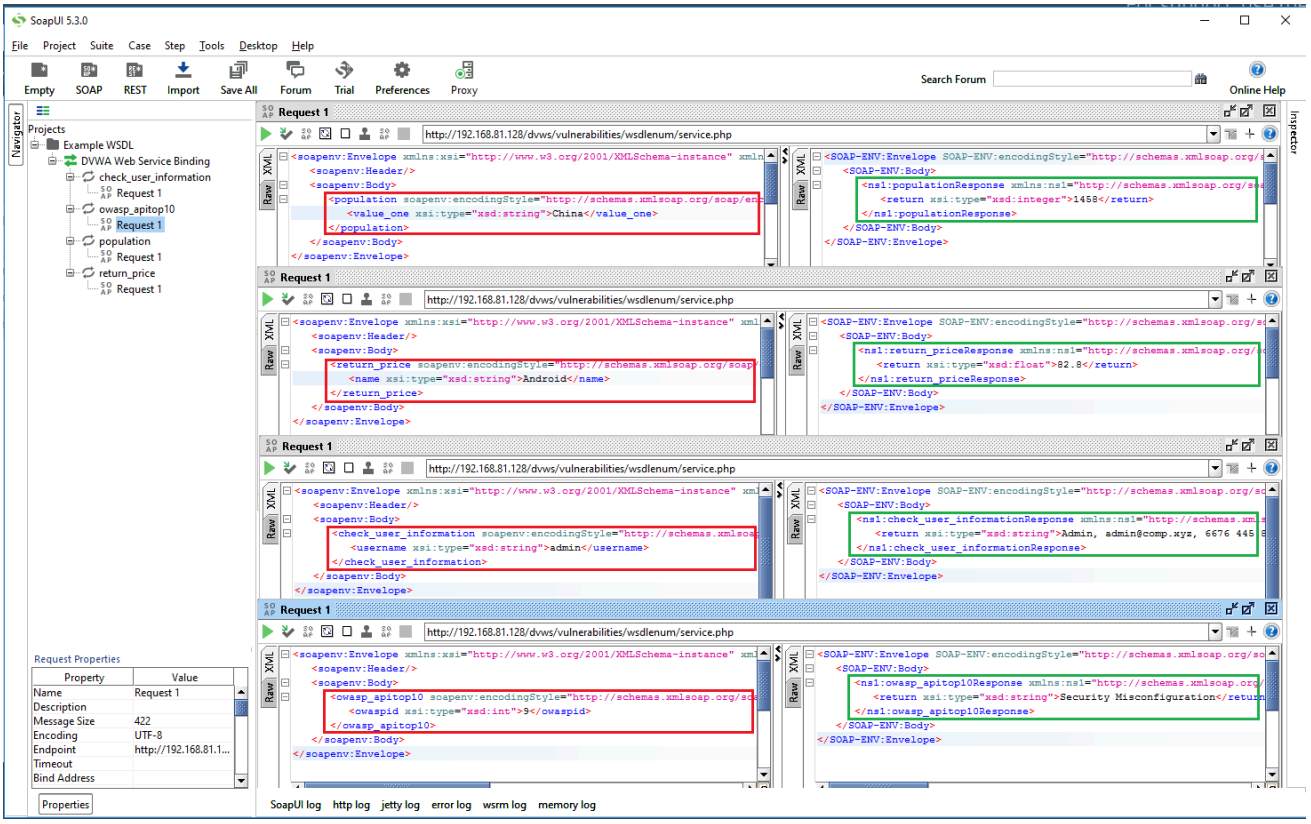
例 1 (REST)

次に、Postman UI でロードされた RESTful API エンドポイントの例を示します。このエンドポイントは、アプリケーションの認証を処理します。画面には、ユーザー名およびパスワードの入力値が正しい要求 (赤い枠)、およびアプリケーションからの応答 (緑の枠) が示されています。



例 2 (SOAP)

次に、SOAPUI UI にロードされ、作業中のパラメーター値を使用して更新された WSDL ファイルの例を示します。画面には、入力値が正しい 4 つの要求 (赤い枠)、および Web サービスからの対応する応答 (緑の枠) が示されています。


SoapUI 5.3.0
File Project Suite Case Step Tools Desktop Help
Empty SOAP REST Import Save All Forum Trial Preferences Proxy
Search Forum
Online Help
Navigator
Projects
Example WSDL
DVWA Web Service Binding
check_user_information
Request 1
owasp_apitop10
Request 1
population
Request 1
return_price
Request 1
Request 1
http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<soapenv:Header/>
<soapenv:Body>
<population soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/en
<value_one xsi:type="xsd:string">China</value_one>
</population>
</soapenv:Body>
</soapenv:Envelope>
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/
<SOAP-ENV:Body>
<ns1:populationResponse xmlns:ns1="http://schemas.xmlsoap.org/s
<return xsi:type="xsd:integer">1458</return>
</ns1:populationResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
Request 1
http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<soapenv:Header/>
<soapenv:Body>
<return_price soapenv:encodingStyle="http://schemas.xmlsoap.org/soap
<name xsi:type="xsd:string">Android</name>
</return_price>
</soapenv:Body>
</soapenv:Envelope>
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/s
<SOAP-ENV:Body>
<ns1:return_priceResponse xmlns:ns1="http://schemas.xmlsoap.org/
<return xsi:type="xsd:float">82.8</return>
</ns1:return_priceResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
Request 1
http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<soapenv:Header/>
<soapenv:Body>
<check_user_information soapenv:encodingStyle="http://schemas.xmlsoa
<username xsi:type="xsd:string">admin</username>
</check_user_information>
</soapenv:Body>
</soapenv:Envelope>
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/s
<SOAP-ENV:Body>
<ns1:check_user_informationResponse xmlns:ns1="http://schemas.xm
<return xsi:type="xsd:string">Admin, admin@comp.xyz, 6676 445
</ns1:check_user_informationResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
Request 1
http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<soapenv:Header/>
<soapenv:Body>
<owasp_apitop10 soapenv:encodingStyle="http://schemas.xmlsoap.org/s
<owaspid xsi:type="xsd:int">9</owaspid>
</owasp_apitop10>
</soapenv:Body>
</soapenv:Envelope>
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/s
<SOAP-ENV:Body>
<ns1:owasp_apitop10Response xmlns:ns1="http://schemas.xmlsoap.org
<return xsi:type="xsd:string">Security Misconfiguration</return
</ns1:owasp_apitop10Response>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
Request Properties
Property
Value
Name
Request 1
Description
Message Size
422
Encoding
UTF-8
Endpoint
http://192.168.81.1...
Timeout
Bind Address
Properties
Inspector
SoapUI log http log jetty log error log wsrm log memory log

1.5.3.3. OpenText Fortify on Demand Connect のセットアップ

OpenText Fortify on Demand Connect を使用して、サイト間 VPN を簡単にセットアップして、内部向け Web アプリケーションの動的評価を行うことができます。OpenText Fortify on Demand Connect は、OpenVPN サーバーとクライアント構成を実装して、安全なサイト間接続を作成します。Docker コンテナとして利用可能な OpenVPN クライアントをインストールする必要があります。

次の手順は、Docker のインストール、構成、および使用に精通していることを前提としています。

OpenText Fortify on Demand Connect をセットアップするには、次の手順を実行します。

1. Docker Hub で OpenText Fortify on Demand Connect Docker イメージをプルします。Fortify Docker リポジトリにアクセスするには資格情報が必要です。これは Docker ID を通じて付与されます。Fortify Docker リポジトリにアクセスするには、Docker ID を mfi-fortifydocker@opentext.com 宛てに電子メールで送信してください。
2. Linux x86_64 マシンに Docker コンテナをインストールします。マシンは次の要件を満たしている必要があります。
    - サポートされている Docker エンジンの最小バージョン: 20.10.17
    - 内部向けアプリケーションへのアクセス
3. (セキュリティ リーダー) OpenText Fortify on Demand Connect ネットワークを OpenText Fortify on Demand に追加します。「OpenText Fortify on Demand Connect ネットワークの追加」を参照してください。
4. (セキュリティ リーダー) ネットワークの docker コマンドをコピーし、動的スキャンがスケジュールされる前にマシン上で実行します。以下は docker コマンドの例です。

```
docker run --name fdc_client -d \ -e
"FDC_ADDRESS=35.155.176.67:443" \ -e
"FDC_UNAME=fodconnect_username" \ -e
"FDC_UPSWD=fodconnect_password" \ -e "FDC_PROXY=3128" \ --
privileged fortifydocker/fortify-
connect:23.1.0.5.alpine.3.17
```

docker コマンドが成功すると、コンテナ ID が返されます。

1.5.3.4. 動的スキャンの構成

動的評価のための Web アプリケーションを準備した後は、[動的スキャンの設定] ページに情報を入力する必要があります。動的スキャンの設定は次のスキャンに引き継がれるため、構成するのはリリースごとに一度だけです。必要に応じて、以降の評価の設定を編集できます。

Note

22.4 より前の動的スキャンの設定は、アプリケーション レベルで保存されていました。既存の動的スキャンの設定を保存または更新して、リリース レベルで保存されるようにしてください。

動的スキャンを構成するには、次の手順を実行します。

1. [アプリケーション] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. アプリケーション名をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. 評価するリリースに対して [スキャンの開始] をクリックし、[動的] を選択します。

   [動的スキャンの設定] ページが表示されます。

4. 必須フィールドに入力します。その他のすべてのフィールドはオプションであるか、既定値に設定されています。

フィールド	評価タイプ	説明
評価タイプ		評価タイプを選択します。組織のセキュリティポリシーで許可されている評価タイプのみが表示されます。 選択した評価タイプの SLO がフィールドの下に表示されます。 **Note** **[動的+ API]** 評価は、定義ファイルが使用できない場合に Web API をテストするために使用します。

フィールド	評価タイプ	説明
スキャン タイプ	DAST 自動	動的スキャン タイプを選択します。 ◦ Web サイト: このスキャンは動的 Web サイト スキャンに似ています。 ◦ ワークフロー駆動スキャン: このスキャンは、ワークフロー マクロを利用する動的 Web サイト スキャンに似ています。 ◦ API: このスキャンは動的 API スキャンに似ています。

フィールド	評価タイプ	説明
ワークフロー駆動スキャン	◦ Web サイト (オプション) ◦ DAST 自動: ワークフロー駆動スキャン	ワークフロー駆動スキャンは、監査のみのモード (クロールなし) を使用し、完全に自動化されています。OpenText DAST は、マクロに記録された URL のみを監査し、監査中に検出されたハイパーリンクはたどりません。 Web サイト評価の場合、スキャンをワークフロー駆動スキャンとして実行するには、チェックボックスをオンにする必要があります。ワークフロー マクロをアップロードします (「動的テストに向けた Web サイトの準備」を参照)。サポートされているマクロは、`.webmacro` ファイル、Burp Proxy キャプチャ、および `.har` ファイルです。

フィールド	評価タイプ	説明
		 **Note** スキャン対象のアプリケーションは、外部向けである必要があります。マクロに記録されたアクティビティは、他のスキャン設定を上書きします。

フィールド	評価タイプ	説明
使用権		評価で使用する使用権を選択します。このフィールドには、購入可能な使用権を含む、選択した評価タイプに有効な使用権が表示されます。リリースにアクティブなサブスクリプションがある場合は、使用権を使用しないオプションのみが表示されます。

フィールド	評価タイプ	説明
		Note ◦ 動的評価または動的 + 評価から DAST 自動評価に切り替える場合、評価ユニットは消費されません。ただし、DAST 自動評価から別の評価に切り替えると、新しい評価のコストを消費します。 ◦ このフィールドには、Fortify

フィールド	評価タイプ	説明
		使用権 ID のみが表示されます。開発者向け、Sonatype 向け、および Debricked 向けアプリケーションの場合、使用権 ID は表示されません。
タイム ゾーン		スキャンの開始時間をスケジュールするために使用されるユーザーが属するタイム ゾーンを選択します。
環境の向き		サイトが内部であるか外部であるかを選択します。

フィールド	評価タイプ	説明
誤検知の除去を要求 (オプション)	DAST 自動	アプリケーションごとに 1 回、テスト チームによる誤検知の除去を要求するには、チェック ボックスをオンにします。このオプションは、セキュリティ ポリシーで DAST 自動アドオンが許可されている場合は既定で選択されます。許可されていない場合、このオプションは無効になります。 **Important** ログイン マクロの生成と誤検知の除去は、アプリケーションごとに 1 回利用できるオプションのサービスとして提供されており、評価ユニットを追加で 1 つ消費します。

フィールド	評価タイプ	説明
		Important ログイン マクロの生成と誤検知の除去の両方を要求する場合、両方のオプションを一緒に選択する必要があります。片方のオプションだけ含まれたスキャンが完了すると、以降のスキャンでは両方のオプションが無効になります。

フィールド	評価タイプ	説明
Fortify on Demand 接続を使用する (オプション)		(オプション) サイトが内部の場合は、OpenText Fortify on Demand Connect を使用してサイト間 VPN をセットアップするためのチェックボックスをオンにし、サイト用に構成されている OpenText Fortify on Demand Connect ネットワークを選択します。詳細については、「Fortify on Demand 接続の設定」を参照してください。 **Important** スキャンをスケジュールする前に、VPN クライアントと VPN サーバー間の接続を初期化する必要があります。

必要な場合は、必須フィールドの下に表示されるセクションに追加のスキャン設定を構成できます。利用可能なセクションは、選択した評価タイプによって決まります。

スコープ (動的 Web サイト、動的+ Web サイト、動的+ API)

スキャンのスコープを編集するには、[**スコープ**] をクリックし、必要に応じてフィールドに入力します。

フィールド	説明
ホスト全体をスキャン (*<URL>*)	次のいずれかのオプションを選択します。 • **ホスト全体をスキャン (*<URL>*)** (既定): ホスト全体がスキャンされます。 **例**: https://foo.com/home の場合は、次の URL が含まれます。 ◦ https://foo.com/ ◦ https://foo.com/contact-us.html ◦ https://foo.com/folder/ ◦ https://foo.com/folder/folder2/page.aspx ◦ https://foo.com/home/folder/ ◦ https://foo.com/home/index.html • **スキャンを URL ディレクトリとサブディレクトリに制限する**: URL の最後のスラッシュが示すディレクトリとそのサブディレクトリのみがスキャンされます。**このオプションを選択した場合は、スキャン対象のディレクトリが最後のスラッシュによって示されていることを確認してください。** **例**: https://foo.com/home/ の場合は、次の URL が除外されます。 ◦ https://foo.com/ ◦ https://foo.com/folder/

フィールド	説明
URL ディレクトリとサブディレクトリにスキャンを制限	◦ https://foo.com/contact-us.html ◦ https://foo.com/folder/folder2/page.aspx

フィールド	説明
HTTP (:80) および HTTPS (:443) の使用を許可	HTTP および HTTPS のサイト スキャンを両方許可するには、このチェックボックスをオンにします (既定)。 **例**: https://foo.com/home の場合は、[**ホスト全体をスキャン**] オプションをオンにすると、http://foo.com/ およびそのサブディレクトリが含まれます。[**URL ディレクトリとサブディレクトリにスキャンを制限**] オプションが選択されている場合、http://foo.com/home とそのサブディレクトリのみが含まれます。 **Important** このフィールドは、[**動的**] および [**動的+ Web サイト評価**] の評価タイプには適用されません。

フィールド	説明
クロール中にフォームの送信を許可する	サイトのクロール中にフォームの送信を許可する場合は、このチェック ボックスをオンにします (既定)。これにより、アプリケーション対象領域がより明確になり、さらに徹底したスキャンを実行することができます。 このチェック ボックスをオフにしても、脆弱性チェック中にフォームの送信が妨げられることは**ありません**。SQL インジェクションやクロスサイト スクリプティングなどの重大な脆弱性を検出するには、フォームの送信が必要です。フォームの送信から特定の Web 機能を除外するには、[**以下を含む URL を除外**] フィールドで該当する URL を指定します。 **Important** [**動的**] および [**動的+ Web サイト評価**] 評価タイプの場合、このフィールドは**無効**になり、変更できません。
以下を含む URL を除外	(オプション) URL 全体またはその一部を指定し、 をクリックして、この文字列と一致する URL をスキャン対象から除外します。文字列ごとに新しいエントリを追加します。このフィールドは大文字と小文字が区別されません。 **例**: https://foo.com/login.html, login.html

フィールド	説明
URL を含める	(オプション、**動的+ Web サイト、動的 Web サイト**評価) 既定では、OpenText Fortify on Demand は指定した最上位のドメインの外側にある URL をスキャンしません。サブドメイン、API、オフサイトリソースなど、**動的サイト URL** ドメインにリンクされているリソースを監査するには、URL を入力して をクリックします。追加の URL ごとに新しいエントリを追加します。 **動的サイト URL** ドメイン、オフサイトドメイン、またはサードパーティ アプリケーションの下にある URL は含めないでください。 **例**: https://foo.com/home の場合、有効な URL は次のとおりです。 • www.foo.com (サブドメイン) • API.aws.com (API) • authfoo.com/login • api.foo.com • api.foo2.com

スコープ (ワークフロー駆動スキャンとしての動的 Web サイト)

スキャンのスコープを編集するには、[**スコープ**] をクリックします。ワークフロー マクロで定義されたホストのリストが表示されます。スキャンするホストを選択します。

スコープ (DAST 自動)

スキャンのスコープを編集するには、[**スコープ**] をクリックし、必要に応じてフィールドに入力します。

フィールド	スキャン タイプ	説明
ホスト全体をスキャン (*<URL>*)	Web サイト	次のいずれかのオプションを選択します。 • **ホスト全体をスキャン (*<URL>*)** (既定): ホスト全体がスキャンされます。 **例**: https://foo.com/home の場合は、次の URL が含まれます。 ◦ https://foo.com/ ◦ https://foo.com/contact-us.html ◦ https://foo.com/folder/ ◦ https://foo.com/folder/folder2/page.aspx ◦ https://foo.com/home/folder/ ◦ https://foo.com/home/index.html • **スキャンを URL ディレクトリとサブディレクトリに制限する**: URL の最後のスラッシュが示すディレク

フィールド	スキャン タイプ	説明
URL ディレクトリとサブディレクトリにスキャンを制限		トリとそのサブディレクトリのみがスキャンされます。**このオプションを選択した場合は、スキャン対象のディレクトリが最後のスラッシュによって示されていることを確認してください。** **例**: https://foo.com/home/ の場合は、次の URL が除外されます。 ◦ https://foo.com/ ◦ https://foo.com/folder/ ◦ https://foo.com/contact-us.html ◦ https://foo.com/folder/folder2/page.aspx

フィールド	スキャン タイプ	説明
以下を含む URL を除外	Web サイト	(オプション) URL 全体またはその一部を指定し、をクリックして、この文字列と一致する URL をスキャン対象から除外します。文字列ごとに新しいエントリを追加します。このフィールドは大文字と小文字が区別されません。 **例**: https://foo.com/login.html, login.html
重複ページ検出を有効にする	• Web サイト • ワークフロー駆動スキャン	チェック ボックスをオンにすると、ページ構造を比較して類似性のレベルを判断できるようになり、センサーが重複するリソースを識別して処理を除外できるようになります。 **Important** 重複ページの検出は、スキャンのクロール部分で機能します。監査によって重複するセッションが導入された場合、そのセッションはスキャンから除外されません。

フィールド	スキャン タイプ	説明
スキャン ポリシー	ポリシーはスキャン タイプによって異なります	ポリシー (センサーが Web アプリケーションに対して展開する脆弱性チェックと攻撃手法のコレクション) を選択します。 **標準**: 標準スキャンにはサーバーの自動クロールが含まれており、SQL インジェクションやクロスサイト スクリプティングなどの既知および未知の脆弱性のほか、Web サーバー、Web アプリケーション サーバー、Web アプリケーション層での不十分なエラー処理や弱い SSL 構成のチェックが実行されます。 **クリティカルとハイ**: クリティカルおよびハイポリシーを使用すると、本番サーバーを危険にさらすことなく、Web アプリケーションを迅速にスキャンして最も差し迫った脆弱性を見つけることができます。このポリシーは、SQL インジェクション、クロスサイト スクリプティング、およびその他のクリティカルで重大度の高い脆弱性をチェックします。データベースにデータを書き込んだり、サービス拒否状態を

フィールド	スキャン タイプ	説明
		引き起こしたりする可能性のあるチェックは含まれていないため、本番サーバーに対して安全に実行できます。 **パッシブ スキャン**: パッシブ スキャン ポリシーは、アプリケーションをスキャンして、積極的な悪用なしで検出可能な脆弱性を検出し、本番サーバーに対して安全に実行できるようにします。このポリシーによって検出される脆弱性には、パス開示、エラー メッセージ、および同様の性質の問題が含まれます。 **API**: API ポリシーには、API セキュリティ評価に関連するさまざまな問題を対象としたチェックが含まれています。これには、さまざまなインジェクション攻撃、トランスポート層セキュリティ、プライバシー侵害が含まれますが、クライアント側の問題を検出するためのチェックや、ディレクトリ列挙やバックアップ ファイル検索チェックなどの攻撃対象領域の検出は含まれません。このポリシーによって検出されたすべての脆弱性は、攻

フィールド	スキャン タイプ	説明
		撃者の直接の標的となる可能性があります。このポリシーは、Web API を消費するアプリケーションのスキャンを目的としたものではありません。
タイムボックス スキャンの期間 (時間)	• Web サイト • API	スキャンの最大継続時間を指定します。指定した期間が終了してもスキャンが完了しない場合、スキャンは終了し、部分的な結果が得られます。指定された期間内にスキャンが完了すると、完全な結果が得られます。インクリメンタル スキャンはサポートされていません。

認証 (動的 Web サイト、動的+ Web サイト、動的手動、動的+ API、動的+, DAST 手動)

認証設定を編集するには、[**認証**] をクリックし、必要に応じてフィールドに入力します。

Note

設定後、パスワード フィールドに保存された値は難読化されます。

認証

フィールド	説明

フィールド	説明
フォーム認証が必要	(オプション) フォーム認証が必要な場合は、チェック ボックスをオンにします。2 人以上のユーザーのユーザー名とパスワードを入力します。 **Note** **動的+ 評価**および**動的手動評価**中の認証では、3 つの追加のユーザー名、パスワード、およびロールを指定できます。追加のユーザー名、パスワード、およびロールを指定するには、フォームの下部にあるプラス記号をクリックします。[ロール] はオプションのフィールドで、最大 32 文字を入力できます。 **Important** パスワードの有効期限を長くするなど、スキャン期間中ユーザーの資格情報を有効に保つように準備を行ってください。サイト認証が失敗した場合、スキャンはキャンセルされます。 同時実行される複数のスキャンに同じ資格情報を指定すると、アカウントのロックアウト、パスワードの変更、またはその他のイベントにより、遅延や不正確な結果が発生する可能性があります。この問題を回避するには、同時にアクティブになるスキャンに異なる資格情報を指定してください。 自己登録が必要な場合は、[**一意の認証を生成してください**] チェックボックスをオンにします (利用可能な場合)。

フィールド	説明

フィールド	説明
2FA の有効化	2 段階認証を有効にするには、このチェックボックスを選択します。有効化したら、2FA モードを選択します。 • 電子メール: ◦ [**電子メール**] を選択すると、ユーザーごとに [**2FA 受信トレイ**] ドロップダウンが [**ロール**] テキスト ボックスの右側に表示されます。 ◦ ユーザーごとに異なる受信トレイを割り当てることができます。これにより、各ユーザーは、指定した受信トレイで 2 段階認証の確認メールを受け取ることができます。 • TOTP: [**TOTP**] が選択されている場合は、以下のオプションから 1 つを選択してください。 ◦ [**画像のアップロード**]: QR コードの画像ファイルをアップロードします。サポートされるファイル形式は JPEG と PNG です。 ◦ [**テキストの入力**]: TOTP のシークレット キーを入力します。

フィールド	説明
	Note 使用できる方法は1つだけです。シークレットキーを入力した場合はQR コードをアップロードできず、その逆も同様です。
ネットワークの認証が必要です	(オプション) ネットワーク認証が必要な場合は、チェック ボックスをオンにします。ユーザー名とパスワードを入力します。
追加の認証手順	(オプション) アカウント番号やテナントコードなどの追加認証が必要な場合は、チェック ボックスをオンにして、説明を入力します。 **Important** OpenText Fortify on Demand は多要素認証をサポートしません。例としては、SMS メッセージ、電子メール検証、CAPTCHA、OATH トークン、物理トークンなどが含まれます。

認証 (DAST 自動化)

認証設定を編集するには、[**認証**] をクリックし、必要に応じてフィールドに入力します。

Note

パスワード フィールドに保存された値は難読化されます。必要に応じて、パスワード フィールドをクリアして新しい値を指定できます。

フィールド	スキャン タイプ	説明
サイト認証を使用する	Web サイト	(オプション) サイト認証が必要な場合は、チェック ボックスをオンにします。ログイン マクロをアップロードします (「動的テストに向けた Web サイトの準備」を参照)。

フィールド	スキャン タイプ	説明
		Important パスワードの有効期限を長くするなど、スキャン期間中ユーザーの資格情報を有効に保つように準備を行ってください。サイト認証が失敗した場合、スキャンはキャンセルされます。 同時実行される複数のスキャンに同じ資格情報を指定すると、アカウントのロックアウト、パスワードの変更、またはその他のイベントにより、遅延や不正確な結果が発生する可能性があります。この問題を回避するには、同時にアクティブになるスキャンに異なる資格情報を指定してください。

フィールド	スキャン タイプ	説明
ログイン マクロの作成を要求	Web サイト	アプリケーションごとに 1 回、テスト チームによるログイン マクロの生成を要求するには、チェック ボックスをオンにします。スキャンが完了すると、[スキャン] ページでログイン マクロをダウンロードできるようになります。このオプションは、セキュリティ ポリシーで DAST 自動アドオンが許可されている場合は既定で選択されます。許可されていない場合、このオプションは無効になります。 **Important** ログイン マクロの生成と誤検知の除去は、アプリケーションごとに 1 回利用できるオプションのサービスとして提供されており、評価ユニットを追加で 1 つ消費します。

フィールド	スキャン タイプ	説明
		Important ログイン マクロの生成と誤検知の除去の両方を要求する場合、両方のオプションを一緒に選択する必要があります。どちらかのオプションを含むスキャンが完了すると、以降のスキャンでは両方のオプションが無効になります。
ネットワーク認証を使用する		(オプション) ネットワーク認証が必要な場合は、チェック ボックスをオンにします。認証タイプ、ユーザー名、パスワードを入力します。 **Note** ネットワーク認証が失敗した場合、スキャンはキャンセルされます。

API (DAST 自動化: API)

サイトで利用されている Web API のスキャンの手順を追加するには、[**API**] をクリックします。テストの自動化に適した Web API のプロジェクト ファイルの準備については、

「Web API ファイルの準備」を参照してください。

[**API タイプ**] フィールドで、API 定義タイプとして [**Postman コレクション**] または [**OpenAPI**] を選択します。

Note

OpenAPI Specification バージョン 2.0 と 3.0 がサポート対象です。

API 定義タイプに基づいて、関連するタスクを実行します。

API 定義タイプ	手順
Postman	[...] をクリックし、Postman コレクション ファイルを探して選択します。JSON ファイル形式が許可されます。ファイルがすでに存在する場合は、既存のファイルを使用するか、新しいファイルをアップロードします。

Postman コレクション (URL)	1. Postman コレクションの URL を指定します。
	2. URL にアクセスするために認証が必要な場合は、[**ヘッダー名**] フィールドにヘッダー名を指定し、[**ヘッダー値**] フィールドに資格情報を指定します。たとえば、[**ヘッダー名**] に `Authorization` と入力し、[**ヘッダー値**] に `Bearer <token>` と入力します。これは、リクエストを認証するために使用する資格情報とは別ではありません。
	例:
	`X-API-Key: <apikey>`
	`Authorization: <apikey>`
	`Authorization: Bearer <token>`
	Note
	資格情報をクエリ パラメータとして渡す場合は URL に含めます。

API 定義タイプ	手順
OpenAPI	[**ファイル**] または [**OpenAPI 仕様への URL**] を選択し、その選択に基づいて関連するタスクを実行します。
	ファイル • [...] をクリックし、OpenAPI ドキュメント ファイルを探して選択します。JSON ファイル形式が許可されます。ファイルがすでに存在する場合は、既存のファイルを使用するか、新しいファイルをアップロードします。 • API に認証が必要な場合は、[**API キー**] フィールドに API キー値を指定します。 **Note** サポートされているセキュリティ スキームは API キーです。リクエストに複数の API キーを指定することはできません。

API 定義タイプ	手順
	OpenAPI 仕様への URL • OpenAPI ドキュメントの URL を指定します。 • API に認証が必要な場合は、[**API キー**] フィールドに API キー値を指定します。 **Note** サポートされているセキュリティ スキームは API キーです。リクエストに複数の API キーを指定することはできません。

[**追加の手順**] フィールドに追加の手順を入力します。

API (動的 API、動的 API+、DAST 手動)

テストの自動化に適した Web API のプロジェクト ファイルの準備については、「Web API ファイルの準備」を参照してください。

サイトで利用されている Web API のスキャンの手順を追加するには、[**API**] をクリックします。

[**API タイプ**] フィールドで、API 定義タイプとして [**SOAP**]、[**REST**]、または [Postman] を選択します。

API 定義タイプに基づいて、関連するタスクを実行します。

API 定義タイプ	手順
SOAP	• 作業中のサンプル データを含む WSDL ファイルをアップロードします。JSON、WSDL、TXT、および XML の各ファイル形式が許可されます。 • (オプション) [**追加の手順**] フィールドに、必要なヘッダー、トークン、認証メカニズムなどの追加の手順を入力します。 • (オプション) ユーザー名とパスワード、または API キーとパスワードを入力します。
REST	• 作業中のサンプル データを含む API 定義ファイルをアップロードします。JSON、WSDL、TXT、および XML の各ファイル形式が許可されます。 • (オプション) [**追加の手順**] フィールドに、必要なヘッダー、トークン、認証メカニズムなどの追加の手順を入力します。 • (オプション) ユーザー名とパスワード、または API キーとパスワードを入力します。

API 定義タイプ	手順
Postman	• 作業中のサンプル データを含む API 定義ファイルをアップロードします。JSON、WSDL、TXT、および XML の各ファイル形式が許可されます。 • [**ファイル タイプを選択**] フィールドで、ファイル タイプとしてワークフロー、認証、環境、またはグローバルを選択します。ワークフロー ファイルは必須ですが、他のファイル タイプはオプションです。 • (オプション) [**追加の手順**] フィールドに、必要なヘッダー、トークン、認証メカニズムなどの追加の手順を入力します。 • (オプション) ユーザー名とパスワード、または API キーとパスワードを入力します。

スケジューリングおよび可用性 (動的 Web サイト、動的+ Web サイト、動的 API、動的+ API)

スキャン頻度およびサイトの可用性を編集するには、[**スケジューリングおよび可用性**] をクリックし、必要に応じてフィールドに入力します。

フィールド	説明
繰り返し頻度	スキャンの繰り返し頻度 [**繰り返さない**] (既定)、[**2 週間**]、[**1 か月**]、[**2 か月**]、[**3 か月**]、[**4 か月**]、[**6 か月**]、[**12 か月**] を選択します。単一スキャンを要求する場合、既定値のままにしてください。 スケジュールされた反復スキャンは自動化され、次の規定に従います。 • スキャンのスケジューリングは、前回のスキャンの開始日と繰り返し頻度によって決定される、計算されたスキャン日の 7 日前に行われます。たとえば、毎月スケジュールされるスキャンがその月の 5 日に開始された場合、次回のスキャンは翌月の 5 日にスケジュールされます。 • 使用権はスケジュールの時点で差し引かれます。 • スキャンがスケジュールされるのは、選択した評価タイプの有効な使用権がスケジュールの時点で存在している場合だけです。 • スキャンがキャンセルされると、その後のスキャンはスケジュールされません。 • 次回のスキャンをスケジュールするときにスキャンがまだ進行中の場合、OpenText Fortify on Demand は 1 日に 1 回、スキャン日が終了するまで次回のスキャンの再スケジュールを試みます。たとえば、月単位でスケジュールされていて毎月 5 日に開始されるスキャンが翌月の 5 日になっても進行中の場合、次回の再

フィールド	説明
	スケジュールは、その次の月の 5 日の 7 日前に行われます。
サイトの可用性	チェック ボックスを選択して、環境がテストに使用できる時間を示します。上記で指定したタイム ゾーンのローカル時間を使用します。スキャンに使用できる時間として、週に最低 4 時間を指定する必要があります。 **Note** サイトの可用性の制限により、所要時間に相当の影響が出る可能性があります。たとえば、テスト時間を 1 日の半分に制限すると、テスト期間が倍になる可能性があります。サイトの可用性の制約がある場合は、サポートに問い合わせて詳細情報を確認してください。

追加の詳細 (動的 Web サイト、動的+ Web サイト、動的+ API)

スキャンに関する詳細を追加するには、[**追加の詳細**] をクリックします。

フィールド	説明
同時要求のスレッド	スキャンに使用する同時要求の数を選択します。 • [**標準**] (既定): 5 個のクロール要求元スレッド、10 個の監査要求元スレッド、20 秒の要求タイムアウト • [**制限付き**]: 2 個のクロール要求元スレッド、3 個の監査要求元スレッド、5 秒の要求タイムアウト [**制限付き**] オプションを選択するとスキャンのロードが軽減されますが、スキャンには標準 SLO よりも時間がかかるようになります。
追加メモ	(オプション) 評価を開始する前にテストチームが知る必要のある情報を追加します。 **Note** 自由形式の除外ノートとホワイトリスト ノートがこのフィールドに移行されました。

フィールド	説明
追加資料	(オプション) アプリケーションのテストをスムーズに実施するのに役立つ資料 (30 MB 制限) をアップロードします。アップロードされたファイルは、下の [**アップロードされたファイル**] セクションに表示されます。動的評価のために以前に送信されたファイルをダウンロードすることもできます。 サポート対象のファイル タイプは、DOC、DOCX、PPT、TXT、PDF、PPTX、ZIP、XLS、XLSX、CSV です。
WAF 仮想パッチを生成する	**Note** サポート チームに連絡して、WAF の機能を有効にします。 (オプション) このチェックボックスを選択すると、Web アプリケーション ファイアウォール (WAF) に向けて脆弱性のエクスポートが生成されます。エクスポートは XML ファイルで、Imperva および F5 という WAF と互換性があります。評価が完了したら、[スキャン] ページでファイルをダウンロードできます。

フィールド	説明
前評価会議通話の要求	(オプション、動的プレミアム評価および動的+ 評価) 前評価会議通話を要求するには、このチェック ボックスをオンにします。評価が完了するとチェック ボックスがオフになります。 **Note** 72 時間以内にスケジュールされたスキャンに対しては前評価会議通話を要求することができません。 この機能はバージョン 25.4 で廃止され、バージョン 26.1 以降では利用できなくなります。

1. スキャン設定を構成したら、[**保存**] をクリックします。
    - フォームが完成したら、[**設定のステータス**] が [**有効**] としてマークされます。
    - フォームが不完全な場合は、[**設定のステータス**] が [**不完全**] としてマークされます。問題のリストがページの上部に表示されます。[**設定のステータス**] の隣の **x** アイコンにカーソルを置くと、リストを表示できます。

1.5.3.5. 動的スキャンのスケジュール

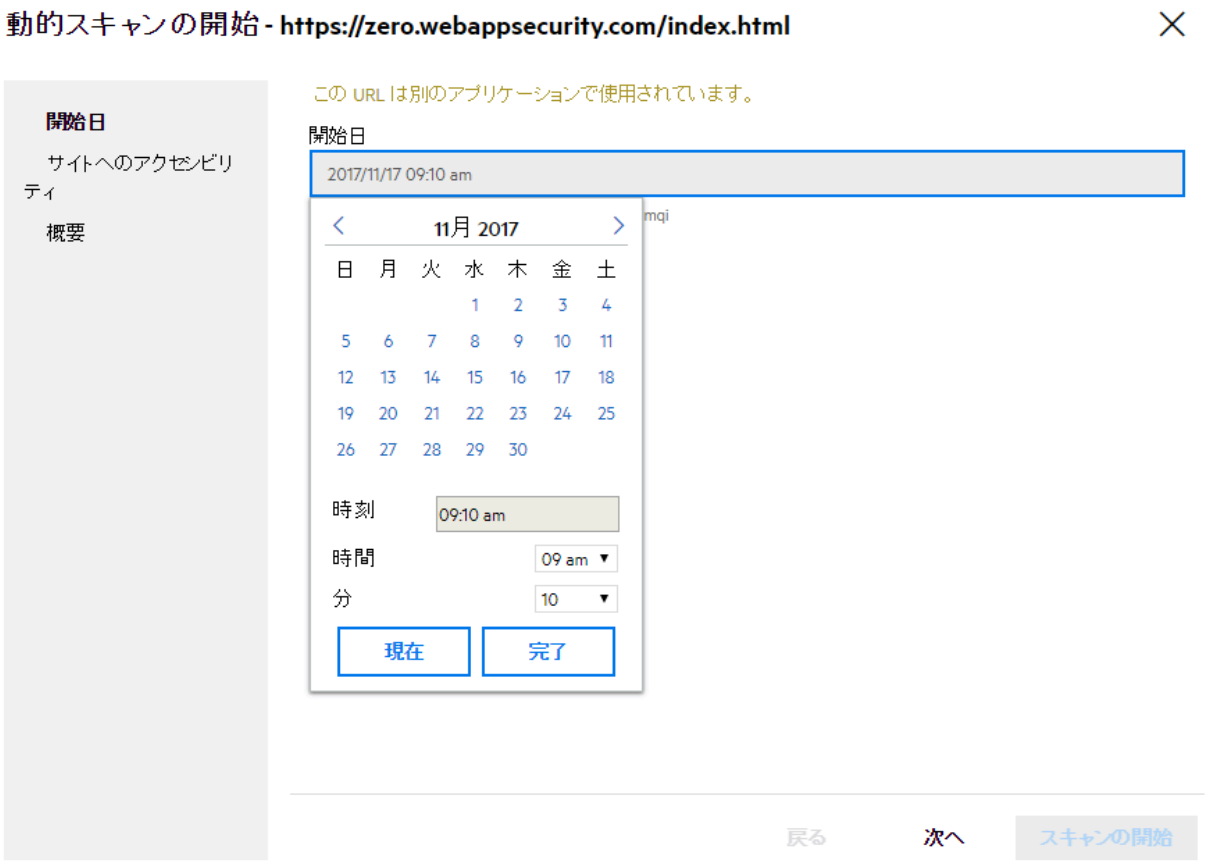
Web アプリケーションを準備し、動的スキャン設定を構成したら、動的スキャンをスケジュールできます。アプリケーションのすべてのリリースで、進行中の状態にできるのは 1 つの動的スキャンのみです。

動的スキャンをスケジュールするには、次の手順を実行します。

1. [スキャンの開始] をクリックします。

> **Note**
>
> アプリケーションで動的スキャンがアクティブになっている場合は、別のスキャンの開始がブロックされます。

現在の時刻とタイム ゾーンを示す [動的スキャンの開始] ウィンドウが開きます。



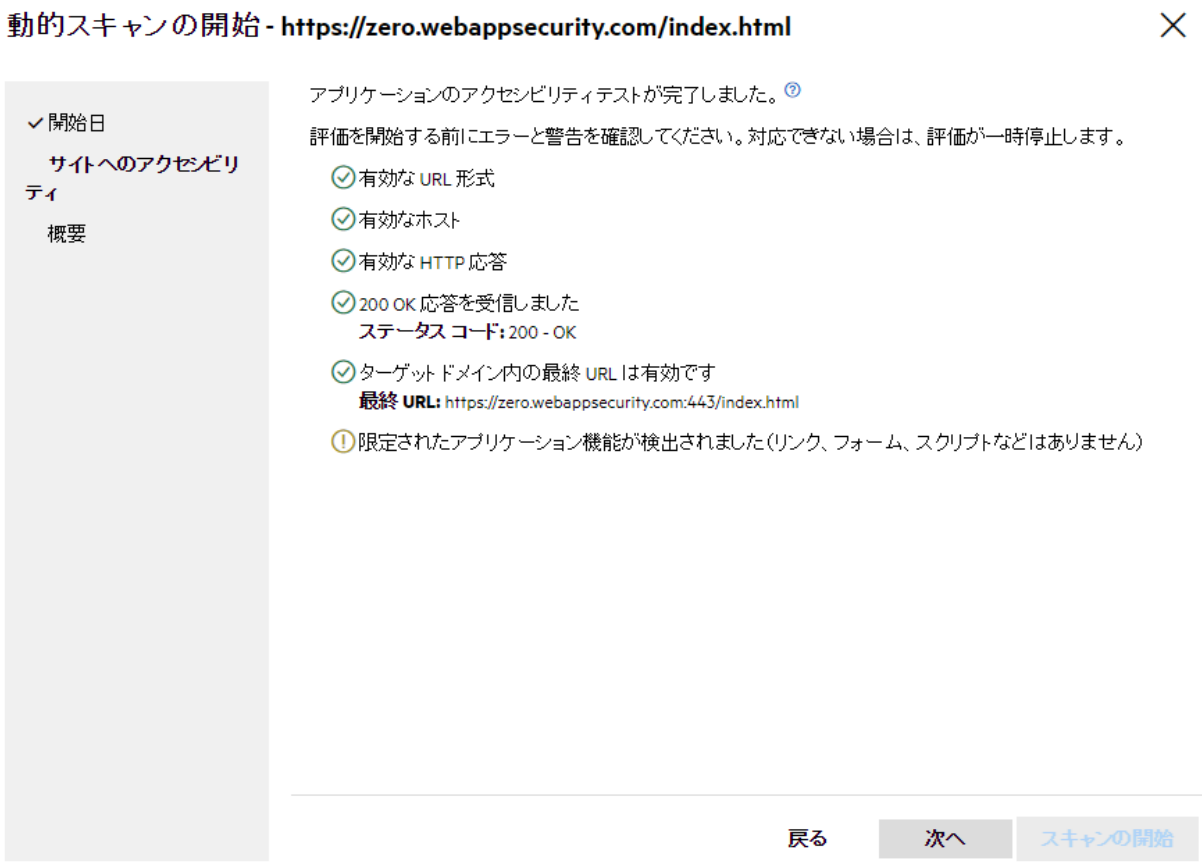
2. [**開始日**] フィールドをクリックします。

スキャンをすぐにスケジュールするには、[**今すぐ**] をクリックします。または、カレンダーを使用して開始日と開始時刻を選択し、[**完了**] をクリックします。

3. [**次へ**] をクリックします。

   サイト アクセシビリティ チェックの結果が表示されます。サイト アクセシビリティ チェックでは、次の基準が検索されます。

   - URL が切り替わります。
   - ホスト名の DNS が切り替わります。
   - OpenText Fortify on Demand は有効な HTTP 応答を受け取ります。
   - サーバーは有効な応答を返します (ステータス コードが一覧表示されます)。
   - リダイレクトがある場合、最終 URL はターゲット ドメイン内にあります (最終 URL が一覧表示されます)。
   - アプリケーションに限定された、または複雑なアプリケーション機能 (リンク、フォーム、スクリプトなど) があるかどうか。
   - 認証が要求された場合に更新済みの資格情報が入力されたかどうか。



   スキャンが一時停止されないように、スキャンを開始する前に問題を解決しておきます。

> **Note**
>
> サイト アクセシビリティ チェックは Web サイト スキャンで利用できます (VPN 経由でアクセスしたサイトは除く)。

4. [次へ] をクリックします。

   動的スキャンの設定値の概要が表示されます。

5. 概要を確認します。必要に応じて、[**戻る**] をクリックし、修正を行います。値が正しい場合、[**スキャンの開始**] をクリックします。

   [リリース スキャン] ページにリダイレクトされ、新しいスキャンのステータスが [**スケジュール済み**] になります。スケジュールした時刻にスキャンが開始します。反復スキャンをスケジュールすると、動的スキャンの設定を更新するまで、定義した間隔でリリースがスキャンされます。

関連トピック

ポータルを使用するだけでなく、次の方法を使用して動的評価を送信することもできます。

- ビルド サーバーの統合ツール: Fortify Azure DevOps Extension、OpenText Fortify on Demand Jenkins Plugin。詳細については、「CICD ツール」を参照してください。
- OpenText Fortify on Demand API。詳細については、「OpenText Fortify on Demand API」を参照してください。

1.5.3.6. 進行中のスキャンおよび完了したスキャンに対する動的スキャンの設定の編集

開始されていないスケジュール済みスキャンおよび一時停止されたスキャンに対する動的スキャン設定を編集できます。進行中のスキャンのスキャン設定を編集する必要がある場合は、ヘルプ センター チケットを作成してスキャンを一時停止します。テスト チームがチケットに応答します。

次のフィールドは、動的スキャンがスケジュールされた後は編集できません。

- **評価タイプ**。スキャンをキャンセルしてフィールドを編集します。
- **動的サイト URL**。リリースに完了したスキャンがない場合は、スキャンをキャンセルしてフィールドを編集します。それ以外の場合、フィールドはロックされます。

さらに、動的スキャンが正常に完了すると、次のフィールドが完了したスキャンの値に設定され、編集のためにロックされます。

- **動的サイト URL**
- **スキャン タイプ**
- [**スコープ**] セクションのすべてのフィールド (DAST 自動スキャンを除く)
- ワークフロー駆動スキャン フィールド
- [**認証**] セクションのすべてのフィールド (ユーザー名とパスワードのフィールドを除く)。
- [**API**] セクションのすべてのフィールド (ユーザー名とパスワードのフィールド、およびアップロードされたプロジェクト ファイルを除く)。

これらのフィールドを編集するには、状態のコピー機能を使用して別のリリースを作成し、スキャン設定を再構成します。

Note

動的評価タイプから DAST 自動評価タイプに切り替える場合は、動的スキャン設定を編集できます。DAST 自動スキャン設定は、動的評価スキャン設定と一致する必要があります。たとえば、リリースの元の評価タイプが動的 Web サイトだった場合、新しい評価タイプは DAST 自動 Web サイトである必要があります。

API 定義タイプが GraphQL URL の場合、動的 API から DAST 自動への切り替えは、ポータル経由でのみサポートされます。

1.5.4. モバイル評価

モバイル評価では、モバイル アプリケーションをテストします。クライアント、ネットワーク、およびバックエンド サーバーにわたるセキュリティ テストが提供されます。OpenText Fortify on Demand は Android および iOS のプラットフォームをサポートしています。

このセクションでは、次のトピックについて説明します。

- サポートされるプラットフォームとオペレーティング システム
- モバイル評価ファイルの準備
- モバイル テストに向けたバックエンドの準備
- モバイル スキャンの構成
- モバイル スキャンのスケジュール
- 進行中のスキャンに対するモバイル スキャンの設定の編集

1.5.4.1. サポートされるプラットフォームとオペレーティング システム

ハードウェア プラットフォーム

OpenText Fortify on Demand は次のハードウェア プラットフォームをサポートします。

	モバイル	Mobile+
電話 (小型のフォーマット)	該当なし	はい
タブレット (大型のフォーマット)	該当なし	はい
SIM/セルラー サービス	該当なし	はい
ハードウェア タイプ (Apple Watch、Samsung Galaxy)	該当なし	いいえ

オペレーティング システムとアーキテクチャ

OpenText Fortify on Demand は、次のオペレーティング システムとネイティブ アーキテクチャをサポートしています。

	モバイル	Mobile+
iOS の最小バージョン (`MinimumOSVersion`)	該当なし	18.5 まで
ネイティブの iOS アーキテクチャ	ARMv7、ARM64	ARMv7、ARM64
Android の最小バージョン (`android:minSdkVersion`)	該当なし	33 (Android 13) まで
ネイティブの Android アーキテクチャ	ARMv7、ARM64	ARMv7、ARM64

1.5.4.2. モバイル評価ファイルの準備

モバイル評価の最初の手順は、OpenText Fortify on Demand へのアップロードに向けてモバイル アプリケーションのバイナリ ファイルを準備することです。モバイル アプリケーションの効果的な解析を実現するため、モバイル アプリケーションのフレームワークの説明に従ってファイルを準備してください。

このセクションでは、次のトピックについて説明します。

- Android アプリケーション ファイルの準備 (バイナリ)
- iOS アプリケーション ファイルの準備 (バイナリ)

1.5.4.2.1. Android アプリケーション ファイルの準備 (バイナリ)

Note
デバイス レベルで言語設定や地域設定を行う必要があるアプリケーションはサポートされていませんが、言語や地域固有のコンテンツを含むアプリケーション、またはユーザーがアプリケーション内でこれらの設定を構成できるアプリケーションはサポートされています。

Android アプリケーションの場合、以下の手順に従ってアプリケーションのバイナリ (.aab または .apk) ファイルを準備します。

- アプリケーションが MDM 機能を必要としないことを確認します。
- バイナリ ファイル全体を提供します。送信されたファイルのみがテストされるため、アプリケーションの更新を必要とする機能はサポートされません。
- オンデバイス テストを含む評価 (モバイル+) では、送信済みアプリケーションを物理デバイスにインストールして動作可能であることを確認します。
- モバイル+ 評価のテストを円滑に行うには、ルート検出、アプリケーションの改変、または証明書のピン止めのメカニズムを無効にします。これらの機能をそのままにしておくと、テストが制限されてスキャンの範囲に影響します。
- AAB ファイルのモバイル+ 評価では、マニフェストで `<dist:fusing dist:include="true" />` が指定されている動的機能モジュールがサポートされています。

Important
アプリケーションの後続のスキャンを修正スキャンまたは新しいスキャンとして送信する場合、OpenText MSP ポータルは、スキャン間の問題追跡の整合性を保つためアプリケーション ID (パッケージ名) の一貫性を維持することをお勧めします。アプリケーション ID は、一意の問題を追跡する問題 ID を計算するために使用されます。スキャン間でアプリケーション ID を変更すると、多くの既存の問題が、スキャン結果に「既存」ではなく「新規」として表示されます。

関連トピック:

静的評価のための Android ファイルのアップロード方法については、「Android アプリケーション ファイルの準備 (ソース コード)」を参照してください。

1.5.4.2.2. iOS アプリケーション ファイルの準備 (バイナリ)

> **Note**
> デバイス レベルで言語設定や地域設定を行う必要があるアプリケーションはサポートされていませんが、言語や地域固有のコンテンツを含むアプリケーション、またはユーザーがアプリケーション内でこれらの設定を構成できるアプリケーションはサポートされています。

iOS アプリケーションの場合、以下の手順に従ってアプリケーションのバイナリ (.ipa) ファイルを準備します。

- オンデバイス テストを含む評価 (モバイル+) では、送信済みアプリケーションを物理デバイスにインストールして動作可能であることを確認します。
- モバイル+ 評価のテストを円滑に行うには、アプリケーションの改変または証明書のピン止めのメカニズムを無効にします。これらの機能をそのままにしておくと、テストが制限されてスキャンの範囲に影響します。
- アプリケーションが MDM 機能を必要としないことを確認します。
- サポートされている次の配布タイプを使用して、送信するアプリケーションをエクスポートします。
    - App Store への送信 (IPA には実行可能コードを含める必要があるため、アプリケーションをエクスポートする際には、[**ビットコードを含める**] チェックボックスをオフにします)
    - アド ホック
    - エンタープライズ
    - 開発

> **Important**
> 次の配布タイプは、サポートされていません。
>
> - App Store からの IPA のダウンロード。IPA は、ダウンロードしたユーザーに対して暗号化されます。
> - [ビットコードを含める] の設定がある App Store への送信。IPA には、実行可能コードは含まれません。

送信されたファイルのみがテストされるため、アプリケーションの更新を必要とする機能はサポートされません。

Note

- アプリケーションの後続のスキャンを修正スキャンまたは新しいバージョンのスキャンとして送信する場合、OpenTextMSP ポータルは、スキャン間の問題追跡の整合性を保つためアプリケーション ID (バンドル識別子) の一貫性を維持することをお勧めします。アプリケーション ID は、一意の問題を追跡する問題 ID を計算するために使用されます。スキャン間でアプリケーション ID を変更すると、多くの既存の問題が、スキャン結果に「既存」ではなく「新規」として表示されます。
- IPA は、デバイスにインストールされる前に、セキュリティ評価に必要な使用権を追加して IPA をテスト デバイスにインストールできるようにするために再署名されます。この再署名プロセスにより、特定のアプリケーション機能に必要な使用権が削除されたり、アプリケーションの整合性に関連するセキュリティ メカニズムがトリガーされる可能性があります。MAST チームは、再署名によって発生する問題を軽減するためのさまざまな手法を維持し、進化させています。重要なアプリケーション機能への影響が解消されない場合、MAST チームがソリューションまたは回避策を調査して推奨するまで、スキャンが一時停止されることがあります。

関連トピック:

アップロードする iOS ソース コード ファイルの準備方法については、「iOS アプリケーション ファイルの準備 (ソース コード)」を参照してください。

1.5.4.3. モバイル テストに向けたバックエンドの準備

バックエンドの Web アプリケーション テストを含むモバイル評価の場合、テスト プロセスを円滑にするために次の準備を行います。

- 評価を行う前に、Web アプリケーションが機能していること/ユーザー資格情報が有効であることを確認します。
- すべての機能テストおよびパフォーマンス テストを評価前に完了し、セキュリティ テスト期間中にアプリケーションのコードを停止します。
- 一般的な注意事項として、OpenText はテスト プロセスを開始する前にすべてのデータをバックアップしておくことをお勧めします。テスト完了時には、問題のないことが分かっているデータをバックアップから復元し、データ破損が発生する可能性を排除します。
- Web アプリケーションは公的にアクセス可能でなければなりません。OpenText Fortify on Demand は VPN を介したスキャンをサポートしません。
- OpenText Fortify on Demand の IP アドレスを、ファイアウォール、IPS、IDS、および WAF の許可リストに追加し、モバイル テスト チームがアプリケーションをスキャンできるようにします。IP アドレスはポータルの [モバイル スキャンの設定] ページから取得できます。状況によっては、ユーザーの許可を得てアドホック アドレスが使用される場合があります。
- OpenText Fortify on Demand の IP アドレスをセキュリティ運用チームとネットワーク運用チームに提供します。これにより、チームは、サイトに攻撃が送信されているのを確認しても、その攻撃が計画された反復セキュリティ スキャンの一環であることを把握でき、その IP アドレスをブロックしないようにします。

Note

Web サイトが http/https デフォルト ポート (80/443) を介してアクセス可能である限り、評価のために追加のポートを開く必要はありません。

1.5.4.4. モバイル スキャンの構成

今回初めてリリースのモバイル評価を送信する場合は、[モバイル スキャンのセットアップ] ページに情報を入力する必要があります。設定は次のスキャンに引き継がれるため、このページに入力するのはリリースごとに一度だけです。必要に応じて、以降の評価の設定を編集できます。

モバイル スキャンをセットアップするには、次の手順を実行します。

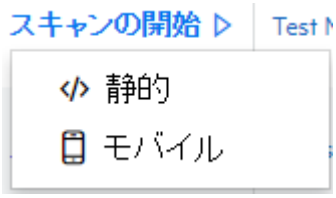
1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. アプリケーション名をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. 評価するリリースに対して [スキャンの開始] をクリックし、メニューから [モバイル] を選択します。



   [モバイル スキャンのセットアップ] ページが表示されます。

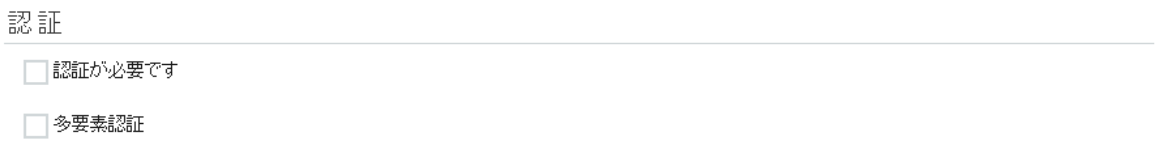
4. 必要に応じてフィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
評価タイプ	評価タイプを選択します。組織のセキュリティ ポリシーで許可されている評価タイプのみが表示されます。 選択した評価タイプの SLO がフィールドの下に表示されます。
使用権	評価で使用する使用権を選択します。このフィールドには、購入可能な使用権を含む、選択した評価タイプに有効な使用権が表示されます。リリースにアクティブなサブスクリプションがある場合は、使用権を使用しないオプションのみが表示されます。
フレームワーク タイプ	モバイル OS [**iOS**]、[**Android**]、[**Windows**] (プレミアム評価のみ) を選択します
タイム ゾーン	スキャンの開始時間をスケジュールするために使用されるユーザーが属するタイム ゾーンを選択します。
監査の設定	監査の基本設定を選択します。この値は、モバイル標準評価、モバイル プレミアム評価、およびモバイル+ 評価で**手動**に固定されています。 **自動的に結果を公開** - スキャン結果は、スキャン完了時に自動的に公開されます。 **手動** – スキャン結果は、監査者がレビューしてから公開されます。

5. 必要な場合は、必須フィールドの下に表示されるセクションに追加のスキャン設定を構成できます。利用可能なセクションは、選択した評価タイプによって決まります。

   認証 (モバイル標準、モバイル プレミアム、モバイル+)

   認証設定を編集するには、[**認証**] セクションで必要に応じてフィールドに入力します。



フィールド	説明
認証	(オプション) 認証が必要な場合は、チェック ボックスをオンにして、2 人以上のユーザーのユーザー名とパスワードを入力します。資格情報を追加するには、[+] を選択します。ユーザー名とパスワードは最大6つまで登録できます。 **Important** 同時実行される複数のスキャンに同じ資格情報を指定すると、アカウントのロックアウト、パスワードの変更、またはその他のイベントにより、遅延や不正確な結果が発生する可能性があります。たとえば、アプリの Android バージョンと iOS バージョンのスキャンを同時に行うようにスケジュールする場合などです。この問題を回避するには、同時にアクティブになるスキャンに異なる資格情報を指定してください。
多要素認証	(オプション) 多要素認証が必要な場合は、チェック ボックスをオンにして、多要素認証の詳細を指定します。

API (モバイル標準、モバイル プレミアム、モバイル+)

Web API の詳細を追加するには、[**API**] セクションで必要に応じてフィールドに入力します。

Web サービス

Web サービスへのアクセス

除外

URL の例: mail.google.com、メモの例: ショッピング カートのチェックアウト機能は本番サーバーに接続します。テストしないでください。

Web サービスのスキャンは契約者本人が管理するサイトに限定されています。サードパーティのエンドポイント (Salesforce や Google アナリティクスなど) は、エンドポイントの所有者からの書面による承認なしにはテストされません。
Fortify on Demand の評価が行われる IP 範囲とネットワーク: 15.0.0.0/8, 16.0.0.0/8, 174.137.32.22/32, 62.73.140.103/32, 62.73.140.104/32

環境の可用性

日	終日	深夜～午前 4 時	午前 4 時～午前 8 時	午前 8 時～午後 12 時	午後 12 時～午後 4 時	午後 4 時～午後 8 時	午後 8
日	■	□□□□	□□□□	□□□□	□□□□	□□□□	□
月	■	□□□□	□□□□	□□□□	□□□□	□□□□	□
火	■	□□□□	□□□□	□□□□	□□□□	□□□□	□
水	■	□□□□	□□□□	□□□□	□□□□	□□□□	□
木	■	□□□□	□□□□	□□□□	□□□□	□□□□	□
金	■	□□□□	□□□□	□□□□	□□□□	□□□□	□
土	■	□□□□	□□□□	□□□□	□□□□	□□□□	□

Fortify on Demand はサイトの可用性の制限に対応できますが、スキャン ウィンドウを小さくすると、スキャンに要する時間が一般的な SLA より長くなります。

フィールド	説明
API へのアクセス	(オプション) チェック ボックスをオンにして、アプリケーションで利用されている Web API を OpenText Fortify on Demand がスキャンできるようにします。
除外	(オプション) アプリケーションが HTTP/HTTPS 経由で通信する Web サイト、バックエンド Web サービス、Web API、内部サービスのリストを作成します。これらはスキャン中に除外されます。これにより、テスト チームが正しいコンテキストと範囲でスキャンを実行できるようになります。検出されたドメインの中で除外されていないものは、脆弱性として分類される場合があります。

フィールド	説明
環境の可用性	チェック ボックスを選択して、環境がテストに使用できる時間を示します。上記で指定したタイム ゾーンのローカル時間を使用します。 テストの一時停止と再開のために、スキャンに要する時間が一般的なスキャンの標準の SLA より長くなります。サイトの可用性の制約がある場合は、サポート チームに問い合わせて詳細情報を確認してください。 **Note** ブラックアウト時間にアプリケーションが変更されると結果が不確かになります。

追加資料 (モバイル標準、モバイル プレミアム、モバイル+)

スキャンに関する詳細を追加するには、[**追加資料**] セクションで必要に応じてフィールドに入力します。


追加資料
追加資料/情報(30MB制限)をアップロード
Upload
アプリケーションと評価の追加メモの追加
このアプリケーションをテストするための特別な要件をリストします。たとえば、SIM カードが必要、有効な電話番号が必要、場所の制限、証明書のピンニングの詳細、
ルート化/ジェイルブレイクの実行などです。
前評価会議通話の要求
この機能はリリース 26.1 以降では提供されなくなります
アップロードされたファイル
名前
作成済み
表示できる項目はありません。
保存
スキャンの開始

フィールド	説明
追加資料/情報 (30 MB 制限) をアップロード	(オプション) アプリケーションのテストをスムーズに実施するのに役立つ資料 (30 MB 制限) をアップロードします。アップロードされたファイルは、下の [**アップロードされたファイル**] セクションに表示されます。 サポート対象のファイル タイプは、DOC、DOCX、PPT、TXT、PDF、PPTX、ZIP、XLS、XLSX、CSV です。
アプリケーションと評価の追加メモの追加	(オプション) アプリケーションを正常に構築するためにテスト チームが知る必要のある情報を追加します。
前評価会議通話の要求	(オプション。プレミアム評価およびモバイル+ 評価のみ) チェック ボックスをオンにして、前評価会議通話を要求します。評価が完了するとチェック ボックスがオフになります。 **Note** 72 時間以内にスケジュールされたスキャンに対しては前評価会議通話を要求することができません。 この機能はバージョン 25.4 で廃止され、バージョン 26.1 以降では利用できなくなります。

6. [モバイル スキャンのセットアップ] ページに情報を入力したら、[**保存**] をクリックします。
    - フォームが完成したら、[**設定のステータス**] が [**有効**] としてマークされます。
    - フォームが不完全な場合は、[**設定のステータス**] が [**不完全**] としてマークされます。問題のリストがページの上部に表示されます。または、[**設定のステータ**

ス] の隣の **x** アイコンにカーソルを置いてリストを表示することもできます。

次の手順:

モバイル スキャンのスケジュール

1.5.4.5. モバイル スキャンのスケジュール

モバイル アプリケーションを準備し、モバイル スキャン設定を構成したら、ペイロードをアップロードしてモバイル スキャンをスケジュールできます。アプリケーションのすべてのリリースで、進行中の状態にできるのは 1 つのモバイル スキャンのみです。

モバイル スキャンをスケジュールするには、次の手順を実行します。

1. [スキャンの開始] をクリックします。

> **Note**
>
> アプリケーションでモバイル スキャンがアクティブになっている場合は、別のスキャンの開始がブロックされます。

[モバイル スキャンの開始] ウィンドウが開きます。

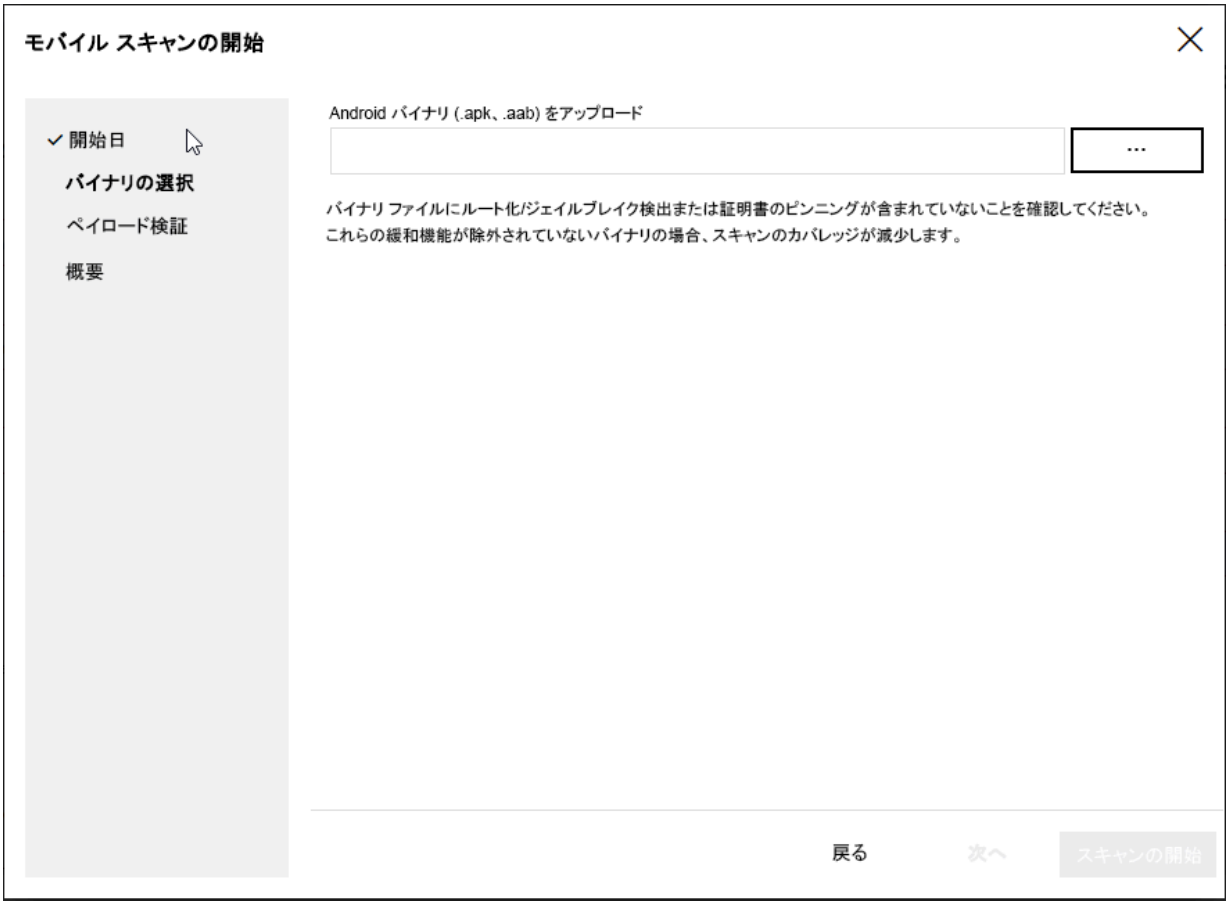
2. [**開始日**] フィールドをクリックします。

   スキャンをすぐにスケジュールするには、[**今すぐ**] をクリックします。または、カレンダーを使用して開始日と開始時刻を選択し、[**完了**] をクリックします。

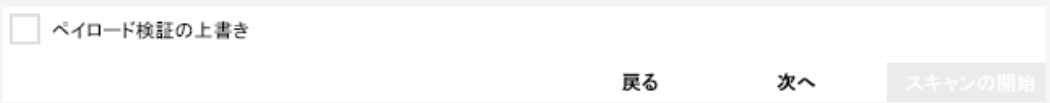
> **Note**
>
> この手順は、バックエンド テストを含むモバイル スキャンにのみ適用されます。

3. [**次へ**] をクリックします。

   [バイナリの選択] ページが表示されます。



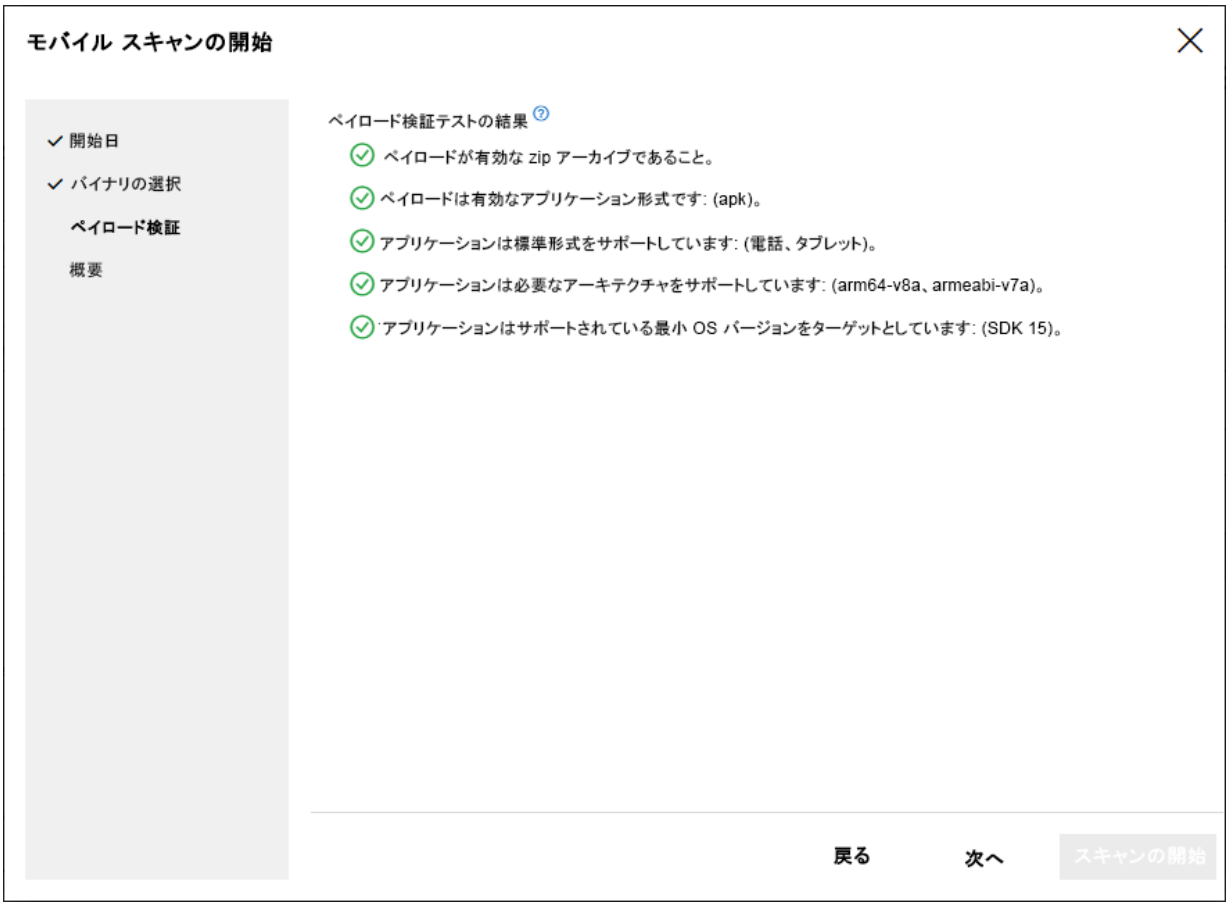
4. [**...**] をクリックし、バイナリ ファイルに移動して選択します。

> **Note**
>
> 500 MB を超えるペイロードの場合は [**ペイロード検証の上書き**] チェック ボックスが表示されます。モバイル ペイロードの検証をスキップするには、[**ペイロード検証の上書き**] チェック ボックスをオンにします。
>
> 
>

5. [**次へ**] をクリックします。

ペイロード検証結果が表示されます。ペイロード検証では、次の基準が検索されます。

- ペイロードが有効な zip アーカイブであること。(モバイル、モバイル+)
- ペイロードが有効なアプリケーション形式であること。(モバイル、モバイル+)
- アプリケーションが標準のデバイス形式をサポートしていること。(モバイル+)
- アプリケーションが必要なアーキテクチャをサポートしていること。(モバイル+)
- アプリケーションが、サポートされているオペレーティング システムの最小バージョンをターゲットにしていること。(モバイル+)
- iOS アプリケーションのバンドル実行可能ファイルに実行可能コードが含まれていること。(モバイル+)
- iOS アプリケーションのバンドル実行可能ファイルが暗号化されていないこと。(モバイル+)
- iOS アプリケーションのバンドル実行可能ファイルが物理デバイスで実行されること。(モバイル+)



OpenText MSP ポータルでは、スキャンがキャンセルされないように、スキャンを開始する前に問題を解決しておくことをお勧めします。場合によっては、検証が失敗してもテストチームがスキャンを続行する可能性があります。[**検証の失敗を上書き**] を選択して、次の手順に進みます。検証の失敗の上書きの詳細については、サポートにお問い合わせください。

6. [**次へ**] をクリックします。

   [概要] ページが表示されます。

7. 概要を確認します。必要に応じて、[**戻る**] をクリックし、修正を行います。値が正しい場合、[**スキャンの開始**] をクリックします。

   [リリース スキャン] ページにリダイレクトされ、新しいスキャンのステータスが [**スケジュール済み**] になります。スケジュールした時刻にスキャンが開始します。

> **Note**
>
> プレミアム モバイルの権利を使用した場合、「<モバイル プレミアム名> (ソース)」という関連する静的な権利を静的スキャンの開始時に利用できるようになりました。

関連トピック

ポータルを使用するだけでなく、次の方法を使用してモバイル評価を送信することもできます。

- OpenText Fortify on Demand API。詳細については、「OpenText Fortify on Demand API」を参照してください。

1.5.4.6. 進行中のスキャンに対するモバイル スキャンの設定の編集

一時停止されたスキャンおよび開始前のスケジュール済みスキャンに対するモバイル スキャンの設定を編集できます。[**評価タイプ**]、[**フレームワーク タイプ**]、および [**監査の基本設定**] フィールドは編集できません。これらのフィールドを編集する必要がある場合は、スキャンをキャンセルしてモバイル評価を再送信してください。

進行中のスキャンを一時停止してスキャンの設定を編集する必要がある場合は、ヘルプ センター チケットを作成してください。テスト チームがチケットに対して更新情報を直接返信します。ヘルプ センター チケットの作成方法については、「ヘルプ センター チケットの送信」を参照してください。

1.5.5. 使用権の消費

ポータルは使用権の消費を管理します。使用可能な使用権の数は、[スキャンの設定] ページに表示されます。スキャンを購入した場合、使用可能な評価の数が表示されます。評価単位を購入した場合、各評価の単位コストと、すべての使用権で使用可能な単位の合計数が表示されます。

スキャンを開始またはスケジュールすると、コストは権利の割り当てから自動的に差し引かれます。1回スキャンを実行するたびに単一スキャンが差し引かれ、サブスクリプションが一度差し引かれて、サブスクリプションの終了日までアプリケーションに対して有効になります。使用権コストがサブスクリプション終了日に置き換えられているため、サブスクリプション契約されているアプリケーションを識別できます。

追加の使用権情報は、次のソースで参照できます。

- 使用権の消費およびアクティブな使用権ダッシュボード タイル。詳細については、「ダッシュボードのグラフ タイプ」を参照してください。
- 使用権の消費データ エクスポート。詳細については、「データ エクスポート テンプレートの作成」を参照してください。
- [管理] ビューの [使用権] ページ。詳細については、「使用権の表示」を参照してください。

1.5.6. スキャンの管理

スキャン アクティビティをテナント、アプリケーション、リリースの各レベルで管理できます。[スキャン] ページにはテナント全体のスキャンが表示されます。ユーザーはアプリケーションをドリルダウンすることができ、[アプリケーション スキャン] ページにはアプリケーションに対して実行されたスキャン、[リリース スキャン] ページにはリリースに対して実行されたスキャンが表示されます。類似するレイアウトおよび機能を共有するスキャン ページは、ユーザーがスキャンの詳細を確認し、進行状況を追跡するための単一のビューを提供します。

このセクションでは、次のトピックについて説明します。

- すべてのスキャンの表示
- アプリケーションのスキャンの表示
- リリース スキャンの表示
- [スキャン] ページの操作
- [自分のスキャン] ページのフィルタリング
- スキャン ステータスの確認
- スキャンのキャンセル
- 一時停止したスキャンの再開
- スキャンにリンクされたヘルプ センター チケットの表示

1.5.6.1. すべてのスキャンの表示

すべてのアプリケーションのスキャンをテナント レベルで表示できます。

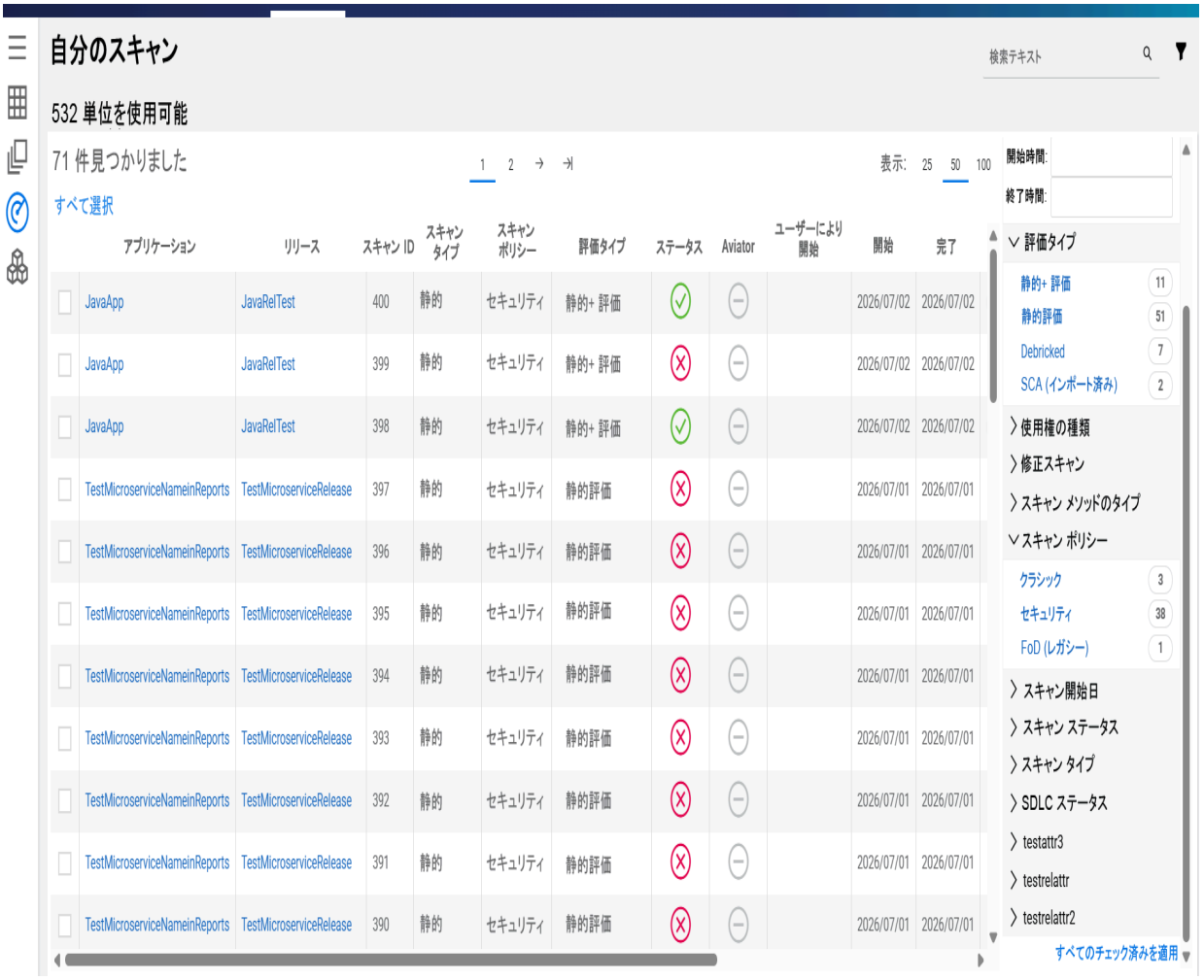
スキャンをテナント レベルで表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**自分のスキャン**] をクリックします。

   [スキャン] ページが表示されます。使用可能な権利の数が一番上に表示されます。



次の表に、[スキャン] ページの操作方法を示します。

タスク	アクション
スキャン リストを検索する	検索テキスト ボックスにキーワードまたは語句を入力して、**Enter** キーを押します。検索結果を削除するには、検索ボックスのテキストを削除して **Enter** キーを押します。詳細については、「アプリケーションおよびリリースの検索」を参照してください。
フィルター リストを非表示にするか表示する	をクリックします。
フィルターを展開するか折りたたむ	すべて展開 | すべて折りたたむ またはフィルター名の横にある矢印をクリックします。
スキャンに関連付けられたヘルプ センター チケットの表示	をクリックします。
進行中のスキャンのキャンセル要求	▪▪▪ をクリックして [**スキャンをキャンセル**] を選択します。「進行中のスキャンのキャンセル」を参照してください。
スキャンの概要の表示	▪▪▪ をクリックして [**スキャンの概要**] を選択します。スキャンの概要には、スキャン ID および以前のスキャンとの比較が含まれます。
静的なスキャン メモの表示	▪▪▪ をクリックして [**メモをスキャン**] を選択します。

タスク	アクション
スキャン結果のダウンロード	静的、動的、モバイル: ▪▪▪ をクリックし、[**結果のダウンロード**] を選択します。 オープン ソース: ▪▪▪ をクリックし、[**SBOM をダウンロード**] を選択します。CycloneDX をダウンロードするには、[**CycloneDX**] を選択します。SPDX をダウンロードするには、[**SPDX**] を選択します。
静的スキャン ペイロードのマニフェストのダウンロード	▪▪▪ をクリックして [**マニフェストのダウンロード**] を選択します。マニフェストにはアップロードされたファイルがリストされ、画像、メディア ファイル、CSS ファイルは除外されます。
静的スキャン ペイロードのダウンロード	ソース コードのダウンロード機能を有効にするには、サポートに問い合わせてください。 をクリックし、完了したスキャンに対して [**ソース コードのダウンロード**] を選択します。

タスク	アクション
属性の編集	リストから 1 つ以上のスキャンを選択して [**属性の編集**] をクリックするか、または ▪▪▪ をクリックして [**属性の編集**] を選択します。 **Note** [スキャン] リスト ビューから 1 つ以上のスキャンを選択し、カスタム属性値を追加できます。[**属性の編集**] ウィンドウにスキャン タイプの属性が表示されます。このウィンドウで、必要に応じて値を入力または更新できます。
動的スキャンのサイト ツリーのダウンロード	▪▪▪ をクリックして [**サイト ツリーのダウンロード**] を選択します。 **動的スキャンとモバイル + 評価スキャン**は、サイト ツリーのダウンロードをサポートします。 • 動的 + Web サイト評価: 手動のサイト ツリーがアップロードされた場合、[**自動**] と [**手動**] のスキャン モード オプションが表示されます。 • 動的な手動による評価: [**手動**] のみが表示されます。 • モバイル + 評価: [**手動**] のみが表示されます。 選択したスキャン モードが [自動] の場合は、ファイル タイプとして CSV または JSON を選択します。 選択したスキャン モードが [手動] の場合、ファイル タイプは .txt になります。

タスク	アクション
動的スキャンで検出されたホストを表示	▪▪▪ をクリックして [**検出されたホスト**] を選択します。検出されたホストは、アプリケーションが参照するホストですが、許可されたホストとして指定されていないホストです。
SBOM に対する Debricked スキャンの送信	をクリックし、[**Debricked に送信**] を選択します。SBOM がダウンロードできる状態になっている必要があります。
インポート済みスキャンの削除	▪▪▪ および [**インポート済みスキャンをキャンセル**] をクリックします。「インポート済みスキャンの削除」を参照してください。
WAF エクスポート ファイルを作成する	サポート チームに連絡して、WAF の機能を有効にします。 をクリックし、[**WAF/IPS に送信**] を選択します。エクスポートされるのは、XML ファイルです。

1.5.6.2. アプリケーションのスキャンの表示

アプリケーションをドリル ダウンして、そのアプリケーションのみのスキャンを表示できます。

スキャンをアプリケーション レベルで表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. スキャンを表示するアプリケーションの名前をクリックします。

3. [**スキャン**] をクリックします。

   [アプリケーション スキャン] ページが開き、アプリケーションに対して実行されたスキャンが表示されます。

   アプリケーション スキャン ビュー

次の表に、[アプリケーション スキャン] ページの操作方法を示します。

タスク	アクション
スキャンに関連付けられたヘルプ センター チケットの表示	をクリックします。
進行中のスキャンのキャンセル要求	をクリックして [**スキャンをキャンセル**] を選択します。「進行中のスキャンのキャンセル」を参照してください。
スキャンの概要の表示	をクリックして [**スキャンの概要**] を選択します。スキャンの概要には、スキャン ID および以前のスキャンとの比較が含まれます。
静的なスキャン メモの表示	をクリックして [**メモをスキャン**] を選択します。
スキャン結果のダウンロード	静的、動的、モバイル: をクリックし、[**結果のダウンロード**] を選択します。 オープン ソース: をクリックし、[**SBOM をダウンロード**] を選択します。CycloneDX をダウンロードするには、[**CycloneDX**] を選択します。SPDX をダウンロードするには、[**SPDX**] を選択します。
静的スキャン ペイロードのマニフェストのダウンロード	をクリックして [**マニフェストのダウンロード**] を選択します。マニフェストにはアップロードされたファイルがリストされ、画像、メディア ファイル、CSS ファイルは除外されます。

タスク	アクション
属性の編集	リストから 1 つ以上のスキャンを選択して [**属性の編集**] をクリックするか、または をクリックして [**属性の編集**] を選択します。 **Note** [スキャン] リスト ビューから 1 つ以上のスキャンを選択し、カスタム属性値を追加できます。[**属性の編集**] ウィンドウにスキャン タイプの属性が表示されます。このウィンドウで、必要に応じて値を入力または更新できます。

タスク	アクション
動的スキャンのサイト ツリーのダウンロード	をクリックして [**サイト ツリーのダウンロード**] を選択します。 **動的スキャンとモバイル + 評価スキャン**は、サイト ツリーのダウンロードをサポートします。 • 動的 + Web サイト評価: 手動のサイト ツリーがアップロードされた場合、[**自動**] と [**手動**] のスキャン モード オプションが表示されます。 • 動的な手動による評価: [**手動**] のみが表示されます。 • モバイル + 評価: [**手動**] のみが表示されます。 選択したスキャン モードが [自動] の場合は、ファイル タイプとして CSV または JSON を選択します。 選択したスキャン モードが [手動] の場合、ファイル タイプは .txt になります。
動的スキャンで検出されたホストを表示	をクリックして [**検出されたホスト**] を選択します。検出されたホストは、アプリケーションが参照するホストですが、許可されたホストとして指定されていないホストです。
SBOM に対する Debricked スキャンの送信	をクリックし、[**Debricked に送信**] を選択します。SBOM がダウンロードできる状態になっている必要があります。

タスク	アクション
インポート済みスキャンの削除	をクリックして [**インポート済みスキャンをキャンセル**] を選択します。「インポート済みスキャンの削除」を参照してください。
WAF エクスポート ファイルを作成する	サポート チームに連絡して、WAF の機能を有効にします。 をクリックし、[**WAF/IPS に送信**] を選択します。エクスポートされるのは、XML ファイルです。

1.5.6.3. リリース スキャンの表示

リリースをドリル ダウンして、そのリリースのみのスキャンを表示できます。

スキャンをリリース レベルで表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. 実行されたスキャンを表示するリリースの名前をクリックします。

4. [**スキャン**] をクリックします。

   [リリース スキャン] ページが開き、リリースに対して実行されたスキャンが表示されます。

次の表に、[リリース スキャン] ページの操作方法を示します。

タスク	アクション
スキャンのインポート	[**スキャンのインポート**] をクリックして、スキャン タイプを選択します。OpenText Fortify on Demand は、オンプレミスのスキャン結果 (オンプレミス スキャンのインポート) およびオープンソースのスキャン結果 (ソフトウェア部品表のインポート) をサポートします。
スキャンに関連付けられたヘルプ センター チケットを表示する	をクリックします。
進行中のスキャンのキャンセル要求	をクリックして [**スキャンをキャンセル**] を選択します。「進行中のスキャンのキャンセル」を参照してください。
スキャンの概要の表示	をクリックして [**スキャンの概要**] を選択します。スキャンの概要には、スキャン ID および以前のスキャンとの比較が含まれます。
静的なスキャン メモの表示	をクリックして [**メモをスキャン**] を選択します。

タスク	アクション
スキャン結果のダウンロード	• 静的、動的、モバイル: をクリックし、[**結果のダウンロード**] を選択します。 • オープン ソース: をクリックし、[**SBOM をダウンロード**] を選択します。CycloneDX をダウンロードするには、[**CycloneDX**] を選択します。SPDX をダウンロードするには、[**SPDX**] を選択します。
静的スキャン ペイロードのマニフェストのダウンロード	をクリックして [**マニフェストのダウンロード**] を選択します。マニフェストにはアップロードされたファイルがリストされ、画像、メディア ファイル、CSS ファイルは除外されます。
静的スキャン ペイロードのダウンロード	ソース コードのダウンロード機能を有効にするには、サポートに問い合わせてください。 をクリックし、完了したスキャンに対して [**ソース コードのダウンロード**] を選択します。

タスク	アクション
属性の編集	リストから 1 つ以上のスキャンを選択して [**属性の編集**] をクリックするか、または をクリックして [**属性の編集**] を選択します。 **Note** [スキャン] リスト ビューから 1 つ以上のスキャンを選択し、カスタム属性値を追加できます。[**属性の編集**] ウィンドウにスキャン タイプの属性が表示されます。このウィンドウで、必要に応じて値を入力または更新できます。

タスク	アクション
動的スキャンのサイト ツリーのダウンロード	をクリックして [**サイト ツリーのダウンロード**] を選択します。 **動的スキャンとモバイル + 評価スキャン**は、サイト ツリーのダウンロードをサポートします。 • 動的 + Web サイト評価: 手動のサイト ツリーがアップロードされた場合、[**自動**] と [**手動**] のスキャン モード オプションが表示されます。 • 動的な手動による評価: [**手動**] のみが表示されます。 • モバイル + 評価: [**手動**] のみが表示されます。 選択したスキャン モードが [自動] の場合は、ファイル タイプとして CSV または JSON を選択します。 選択したスキャン モードが [手動] の場合、ファイル タイプは .txt になります。
動的スキャンで検出されたホストを表示	をクリックして [**検出されたホスト**] を選択します。検出されたホストは、アプリケーションが参照するホストですが、許可されたホストとして指定されていないホストです。
ログイン マクロをダウンロード	をクリックして [ログイン マクロをダウンロード] を選択します。

タスク	アクション
DAST 自動スキャンに失敗したログ ファイルのダウンロード	
SBOM に対する Debricked スキャンの送信	をクリックし、[**Debricked に送信**] を選択します。SBOM がダウンロードできる状態になっている必要があります。
インポート済みスキャンの削除	をクリックして [**インポート済みスキャンをキャンセル**] を選択します。「インポート済みスキャンの削除」を参照してください。
WAF エクスポート ファイルを作成する	サポート チームに連絡して、WAF の機能を有効にします。 をクリックし、[**WAF/IPS に送信**] を選択します。エクスポートされるのは、XML ファイルです。

1.5.6.4. [スキャン] ページの操作

次の表に、[自分のスキャン] ページ、[アプリケーション スキャン] ページ、[リリース スキャン] ページの操作方法を示します。[スキャン] ページは、注記がある場合を除き、同じ機能を共有しています。

タスク	アクション	注
スキャン リストを検索する	検索テキスト ボックスにキーワードまたは語句を入力して、**Enter** キーを押します。検索結果を削除するには、検索ボックスのテキストを削除して **Enter** キーを押します。詳細については、「アプリケーションおよびリリースの検索」を参照してください。	テキスト検索は [自分のスキャン] ページでのみ利用できます。
フィルター リストを非表示にするか表示する	 をクリックします。	フィルタリングは [自分のスキャン] ページで利用できます。他のスキャン ページでは利用できません。詳細については、「[自分のスキャン] ページのフィルター オプション」を参照してください。
フィルターを展開するか折りたたむ	 またはフィルター名の横にある矢印をクリックします。	
スキャンに関連付けられたヘルプ センター チケットの表示	をクリックします。	
進行中のスキャンのキャンセル要求	▪▪▪ をクリックして [**スキャンをキャンセル**] を選択します。「進行中のスキャンのキャンセル」を参照してください。	

タスク	アクション	注
スキャンの概要の表示	▪▪▪ をクリックして [**スキャンの概要**] を選択します。スキャンの概要には、スキャン ID および以前のスキャンとの比較が含まれます。	
静的なスキャン メモの表示	▪▪▪ をクリックして [**メモをスキャン**] を選択します。	
スキャン結果のダウンロード	静的、動的、モバイル: ▪▪▪ をクリックし、[**結果のダウンロード**] を選択します。 オープン ソース: ▪▪▪ をクリックし、[**SBOM をダウンロード**] を選択します。CycloneDX をダウンロードするには、[**CycloneDX**] を選択します。SPDX をダウンロードするには、[**SPDX**] を選択します。	
静的スキャン ペイロードのマニフェストのダウンロード	▪▪▪ をクリックして [**マニフェストのダウンロード**] を選択します。マニフェストにはアップロードされたファイルがリストされ、画像、メディア ファイル、CSS ファイルは除外されます。	

タスク	アクション	注
静的スキャン ペイロードのダウンロード	ソース コードのダウンロード機能を有効にするには、サポートに問い合わせてください。 をクリックし、完了したスキャンに対して [**ソースコードのダウンロード**] を選択します。	静的スキャン ペイロードのダウンロードは [自分のスキャン] ページと [リリース] ページでのみ利用できます。
属性の編集	リストから 1 つ以上のスキャンを選択して [**属性の編集**] をクリックするか、または ▪▪▪ をクリックして [**属性の編集**] を選択します。 **Note** [スキャン] リスト ビューから 1 つ以上のスキャンを選択し、カスタム属性値を追加できます。[**属性の編集**] ウィンドウにスキャン タイプの属性が表示されます。このウィンドウで、必要に応じて値を入力または更新できます。	

タスク	アクション	注
動的スキャンのサイト ツリーのダウンロード	▪▪▪ をクリックして [**サイト ツリーのダウンロード**] を選択します。 **動的スキャンとモバイル + 評価スキャン**は、サイト ツリーのダウンロードをサポートします。 • 動的 + Web サイト評価: 手動のサイト ツリーがアップロードされた場合、[**自動**] と [**手動**] のスキャン モード オプションが表示されます。 • 動的な手動による評価: [**手動**] のみが表示されます。 • モバイル + 評価: [**手動**] のみが表示されます。 選択したスキャン モードが [自動] の場合は、ファイル タイプとして CSV または JSON を選択します。 選択したスキャン モードが [手動] の場合、ファイル タイプは .txt になります。	

タスク	アクション	注
動的スキャンで検出されたホストを表示	▪▪▪ をクリックして [**検出されたホスト**] を選択します。検出されたホストは、アプリケーションが参照するホストですが、許可されたホストとして指定されていないホストです。	
動的スキャンで使用するログイン マクロをダウンロード	▪▪▪ をクリックして [**ログイン マクロをダウンロード**] を選択します。	ログイン マクロは、次のスキャン タイプで使用できます: DAST 自動 Web サイト、動的、動的+
失敗した動的スキャンのスキャン ログのダウンロード	▪▪▪ をクリックして [**スキャン ログをダウンロード**] を選択します。	スキャン ログは DAST 自動スキャンで使用できます。
SBOM に対する OpenText Core SCA スキャンの送信	をクリックし、[**Debricked に送信**] を選択します。SBOM がダウンロードできる状態になっている必要があります。	
インポート済みスキャンの削除	▪▪▪ をクリックして [**インポート済みスキャンをキャンセル**] を選択します。「インポート済みスキャンの削除」を参照してください。	

タスク	アクション	注
WAF エクスポート ファイルを作成する	サポート チームに連絡して、WAF の機能を有効にします。 をクリックし、[**WAF/IPS に送信**] を選択します。エクスポートされるのは、XML ファイルです。	

Note

ダウンロード可能な期間は、データ保持ポリシーによって設定されます。

1.5.6.5. [自分のスキャン] ページのフィルタリング

フィルターを適用することで、[自分のスキャン] ページに表示されるスキャンを制限できます。[自分のスキャン] ページでは、次のフィルター オプションとグループ化オプションが用意されています。

Note

フィルターがフィルター リストに表示されるようにするには、結果にそのフィルターの複数の値が含まれている必要があります。

フィルター	説明	値
開始日	スキャンが開始された日付範囲	
完了日	スキャンが完了した日付範囲	
評価タイプ	スキャンの評価タイプ	
使用権の種類	スキャンの使用権の種類	単一スキャン、N/A、サブスクリプション、修正
修正	スキャンが修復スキャンかどうかを指定	誤、正
リリース	スキャンに関連付けられたリリース	
スキャン ステータス	静的、動的、モバイル、およびネットワーク スキャンのステータス	進行中、完了、キャンセル済み、待機中
スキャン ポリシー	スキャンに使用されるスキャン ポリシーの種類	セキュリティ、DevOps、クラシック、FoD (レガシー)
スキャン タイプ	スキャン タイプ	静的、動的、モバイル、ネットワーク、オープンソース

1.5.6.6. スキャン ステータスの確認

ポータルでスキャン ステータスを確認できます。アプリケーションの通知リストのリリース所有者、スキャン送信者、およびユーザーは、スキャン ステータスの更新 (スキャンの開始、スキャンの完了、スキャンのキャンセル、スキャンの一時停止、誤検知の再確認の送信、誤検知の再確認の完了) に関する電子メール通知も受信します。

Note

利用可能なスキャン ステータスは評価タイプによって異なります。進行中のスキャンはテナントごとに 25 件までという制限があります。

- 静的: アプリケーションで進行中の状態にできるのは、リリースごとに 1 つの静的スキャンのみです (アプリケーションごとに進行中を最大 2 つ)。その他のスキャンはキューに配置され、キューに配置された順にスキャンされます。各アプリケーションのキューには、スキャンを 30 個まで含めることができます。
- オープン ソース: アプリケーションで進行中の状態にできるのは、リリースごとに 1 つの OpenText Core SCA スキャンのみです (アプリケーションごとに進行中を最大 2 つ)。その他のスキャンはキューに配置され、キューに配置された順にスキャンされます。
- 動的: アプリケーションで進行中の状態にできるのは、一度に 1 つの動的スキャンのみです。スキャンをキューに配置することはできません。
- モバイル: アプリケーションで進行中の状態にできるのは、一度に 1 つのモバイル スキャンのみです。スキャンをキューに配置することはできません。

アプリケーションのスキャン ステータスを確認するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. スキャン ステータスを確認するアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. スキャン ステータスのアイコンにカーソルを置き、リリース全体の最新のスキャンに関する追加情報を示すツールチップを表示します。

4. 次のステータス アイコンをクリックすると、スキャン ステータスの詳細情報に直接アクセスできます。

   - 未開始: 関連する [スキャンの設定] ページにリダイレクトされます。
   - スケジュール済み: 関連する [スキャンの設定] ページにリダイレクトされます。
   - 進行中: マイクロサービス アプリケーションのキューに静的スキャンが入っている場合は、[リリース スキャン] ページまたは [アプリケーション スキャン] ページにリダイレクトされます。
   - キューに登録済み: 関連する [スキャンの設定] ページにリダイレクトされます。
   - 一時停止: [リリース スキャン] ページの [ヘルプ センター チケット] ウィンドウにリダイレクトされます。
   - キャンセル済み: 関連する [スキャンの設定] ページにリダイレクトされます。

   - 完了: 関連するスキャン タイプでフィルターされた [リリースの問題] ページ (静的、動的、およびモバイル スキャン) または [アプリケーションの問題] ページにリダイレクトされます。

> **Note**
>
> DAST 自動スキャンと OpenText Core SCA スキャンでは部分的な結果が得られることがあります。部分的な結果で完了したスキャンのスキャン ステータス アイコンは、オレンジ色で強調表示されます。

1.5.6.7. スキャンのキャンセル

まだ開始されていないか、開始されているがまだ完了していないスキャンのキャンセルが必要になる場合があります。ポータルはキャンセル要求の処理を自動化します。使用権コストの返還が適切であると判断されれば、返還されます。

スキャンをキャンセルするには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. スキャンをキャンセルするアプリケーションの名前をクリックします。

   [リリース] ページが表示されます。

3. [**スキャン**] をクリックします。

   [アプリケーション スキャン] ページが表示されます。

4. スキャンの行の ▪▪▪ をクリックし、[**スキャンをキャンセル**] を選択します。

   確認メッセージが表示されます。

5. [**はい**] をクリックして、スキャンのキャンセルを確定します。

   - ステータスが [**キューに配置**] または [**スケジュール済み**] のスキャンの場合、スキャンは自動的にキャンセルされます。
   - ステータスが [**進行中**] のスキャンの場合:
     - 監査されていない静的スキャンの場合、そのスキャンは自動的にキャンセルされます。
     - 動的スキャン、モバイル スキャン、または監査中の静的なスキャンの場合、ヘルプ センター チケット (キャンセル要求とスキャン詳細を含む) が生成されます。テスト チームに電子メールが送信され、テスト チームはスキャンを手動でキャンセルします。

- ステータスが [**待機中**] のスキャンの場合、スキャンは自動的にキャンセルされます。電子メールがテスト チームに送信されます。

スキャンがキャンセルされると、そのスキャンに関連付けられているヘルプ センター チケットは解決済みとマークされます。

1.5.6.8. 一時停止したスキャンの再開

追加情報が必要な場合、テスト チームはスキャンを一時停止します。スキャンを再開できるように、関連付けられているヘルプ センター チケットに返信してください。テストの一時停止と再開のために、スキャンに要する時間が標準の SLO より長くなることに注意してください。

> **Note**
>
> 保留期間が連続 21 日を超えるスキャンは、自動的にキャンセルされます。スキャンに関連付けられたヘルプ センター チケットは、解決済みとしてマークされます。

一時停止したスキャンを再開するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. アプリケーションの [**スキャン & セキュリティ ステータス**] 列にある一時停止ステータスのアイコンをクリックします。

   [ヘルプ センター チケット] ウィンドウが表示されます。

3. [**保留中のチケット**] セクションをクリックします。

   スキャン対象の保留中のチケットが表示されます。

4. チケットをクリックして、コメントを表示します。

5. [**公開コメントを追加**] をクリックします。

   以下のテキスト ボックスが表示されます。

6. チケットに追加するコメントを入力します。

7. [**公開コメントを追加**] をクリックします。

   コメントがポータルとヘルプ センター両方のチケット詳細に追加されます。評価のステータスが [進行中] に戻ります。

   > **Note**
   >
   > チケットに添付を追加する必要がある場合は、ヘルプ センターで追加する必要があります。

1. アカウント名をクリックします。
2. [ヘルプ センター] を選択します。

[ヘルプ センター] が別のウィンドウで開きます。

3. [チケットを表示] をクリックします。

送信されるチケット一覧が表示された新しい画面が表示されます。各チケットには、ステータスの一覧が左側の列に表示されています。ステータスは、[**新規**]、[**未解決**]、[**保留中**]、[**解決済み**] のいずれかです。

4. [保留中を表示] をクリックします。

一覧には、ユーザーの組織からのアクションが必要なチケットのみが表示されています。

> **Note**
> [保留中] のチケットの総数は、ページ上部の [ヘルプ センター] リンクの上に赤色の数字で表示されます。

5. [応答] をクリックして、質問に対する応答を入力します。

応答を送信するとすぐに、評価のステータスが [進行中] に変わります。

1.5.6.9. スキャンにリンクされたヘルプ センター チケットの表示

アクティブなスキャンにリンクされたヘルプ センター チケットを、[スキャン] ページ、[アプリケーション スキャン] ページおよび [リリース スキャン] ページに直接表示できます。

Note
スキャンが一時停止された場合は、ステータス バーにある [**ヘルプ センター チケット**] ボタンをクリックして、任意のリリースレベルのページから関連するヘルプ センター チケットにアクセスできます。

アクティブ スキャンにリンクされたヘルプ センター チケットを表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

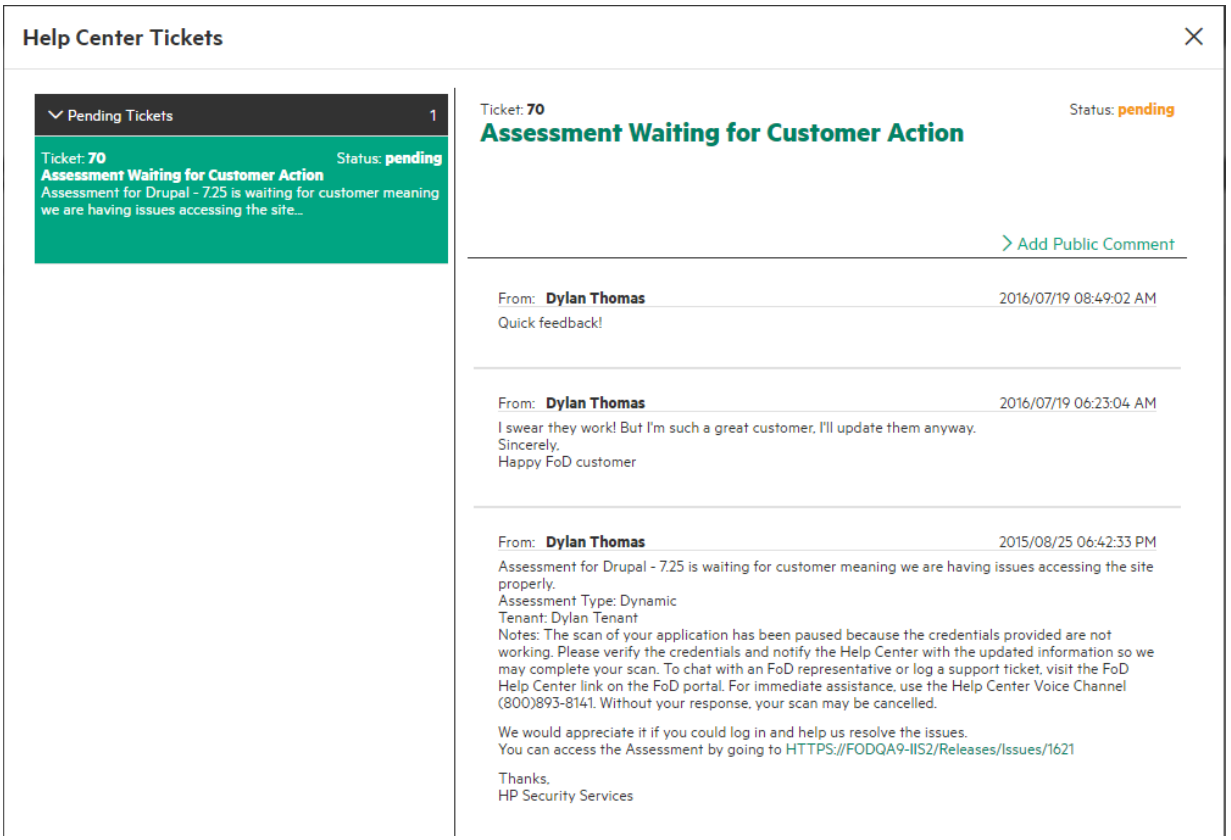
2. アプリケーション名をクリックします。

3. [**スキャン**] をクリックします。

   アプリケーションまたはリリースに対して実行されたすべてのスキャンのリストが表示されます。

4. アイコンをクリックします。

   [ヘルプ センター] モーダル ウィンドウが開き、スキャンと関連付けられている保留中のチケット、未解決のチケット、解決済みのチケットがすべて表示されます。



5. [保留中のチケット] セクションで、コメントを表示するチケットをクリックします。
6. [**公開コメントを追加**] をクリックします。

   以下のテキスト ボックスが表示されます。
7. チケットに追加するコメントを入力します。
8. [**公開コメントを追加**] をクリックします。

   コメントがポータルとヘルプ センター両方のチケット詳細に追加されます。

1.6. 脆弱性の修復

テスト チームは、スキャンの完了後にスキャン結果をポータルに発行します。OpenText Fortify on Demand にログインして、スキャン結果を表示し、アプリケーションで検出された脆弱性を修復します。

このセクションでは、次のトピックについて説明します。

- 問題のレビュー
- 問題点の詳細
- 問題の更新
- 問題修復の監査
- Fortify Remediation Aviator の監査と修復
- 監査テンプレート
- データフロー クレンズ ルール
- 修復スキャンの要求

1.6.1. 問題のレビュー

アプリケーション レベルおよびリリース レベルの両方のスキャンで見つかった問題に関する詳細情報を表示できます。[アプリケーションの問題] ページには、アプリケーションのすべてのリリース (廃棄されたリリースを除く) で見つかった問題が表示されます。[リリースの問題] ページには、リリースのすべてのスキャンで見つかった問題が表示されます。

似たレイアウトおよび機能を共有する [アプリケーションの問題] ページと [リリースの問題] ページには、問題データの単一の統合されたビューが提供されます。ページは 3 つのパネルに分割されます。

- ナビゲーション パネルには問題のリストが表示されます。問題は重大度に応じて編成され、重大度レベルごとのタブと、すべての問題を示すタブが表示されます。
- 問題の詳細のパネルには、ナビゲーション パネルで選択した問題の詳細が表示されます。詳細は、いくつかのタブで整理されています。使用可能なタブは、問題が検出されたスキャン タイプによって異なります。
- 監査パネルは折りたたむことができます。ここには、ナビゲーション パネルで選択した問題のユーザー修正フィールドのほか、問題のステータス、問題が発生した日付、および問題が見つかった直近の日付が表示されます。

問題には、次のいずれかのステータスがあります。

ステータス	説明
新規	最新のスキャンで初めて発生した脆弱性。
既存	最新のスキャンで発生し、なおかつ前回またはそれ以前のスキャンでも発生していた脆弱性。
再発	最新のスキャンで発生し、以前のスキャンでも発生していたものの、前回のスキャンでは発生しなかった脆弱性。言い換えると、問題が発生した後、1 回または複数回のスキャンでは出現しなかったため、修正されたと見なされていたものの、その後に再び発生したということです。
修正済み/検証済みの修正	以前に少なくとも 1 回は発生したものの、最新のスキャンでは識別されなかった脆弱性。[**修理済み**] の脆弱性は、既定では非表示です。[**修正済み**] の脆弱性を表示するには、[**固定を表示**] を [リリースの概要] および [問題] ページで選択します。

このセクションでは、次のトピックについて説明します。

- アプリケーションの問題の表示
- リリースの問題の表示
- [問題] ページの操作
- [問題] ページのフィルタリングとグループ化
- 問題フィルターとグループ化のカスタマイズ
- 問題に対する属性の割り当て

1.6.1.1. アプリケーションの問題の表示

アプリケーションのすべてのリリース (廃止になったリリースを除く) の問題を表示できます。

問題をアプリケーション レベルで表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

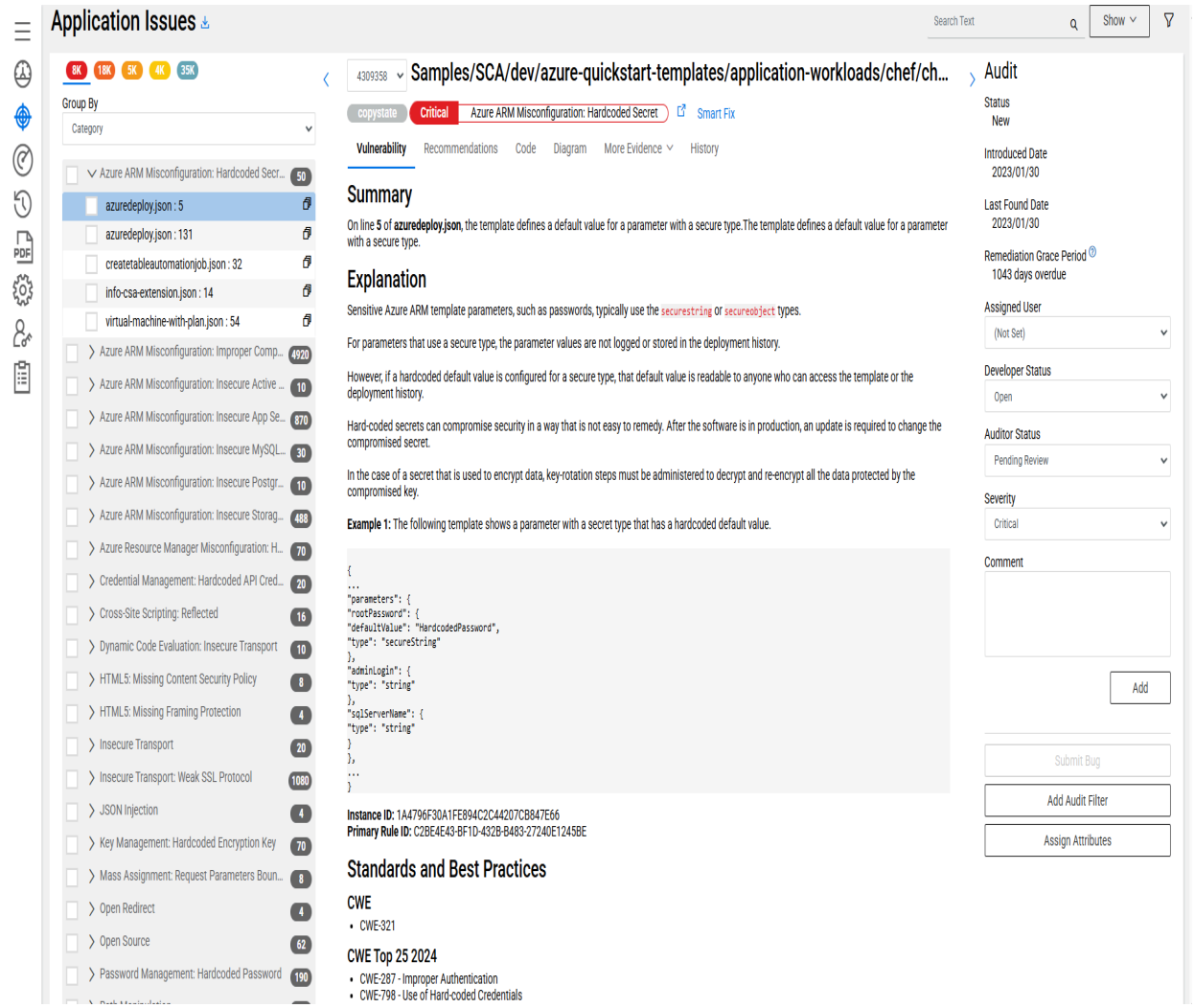
   [アプリケーション] ページが表示されます。

2. 表示するアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [**問題**] をクリックします。

   [アプリケーションの問題] ページが表示されます。グループ内では、問題はファイル名、次に行番号の順に並べ替えられます。複数のリリースにわたる同じインスタンス ID の問題は、単一のビューにまとめられます。グループを選択するときに、個々の問題を選択解除できます。


Application Issues
Search Text
Show
8K 18K 5K 4K 35K
Group By
Category
Azure ARM Misconfiguration: Hardcoded Secr... 50
azuredeploy.json : 5
azuredeploy.json : 131
createtableautomationjob.json : 32
info-csa-extension.json : 14
virtual-machine-with-plan.json : 54
Azure ARM Misconfiguration: Improper Comp... 4920
Azure ARM Misconfiguration: Insecure Active ... 10
Azure ARM Misconfiguration: Insecure App Se... 870
Azure ARM Misconfiguration: Insecure MySQL... 30
Azure ARM Misconfiguration: Insecure Postgr... 10
Azure ARM Misconfiguration: Insecure Storag... 488
Azure Resource Manager Misconfiguration: H... 70
Credential Management: Hardcoded API Cred... 20
Cross-Site Scripting: Reflected 16
Dynamic Code Evaluation: Insecure Transport 10
HTML5: Missing Content Security Policy 8
HTML5: Missing Framing Protection 4
Insecure Transport 20
Insecure Transport: Weak SSL Protocol 1080
JSON Injection 4
Key Management: Hardcoded Encryption Key 70
Mass Assignment: Request Parameters Boun... 8
Open Redirect 4
Open Source 62
Password Management: Hardcoded Password 190
4309358 Samples/SCA/dev/azure-quickstart-templates/application-workloads/chef/ch...
copystate Critical Azure ARM Misconfiguration: Hardcoded Secret Smart Fix
Vulnerability Recommendations Code Diagram More Evidence History
Summary
On line 5 of azuredeploy.json, the template defines a default value for a parameter with a secure type.The template defines a default value for a parameter with a secure type.
Explanation
Sensitive Azure ARM template parameters, such as passwords, typically use the securestring or secureobject types.
For parameters that use a secure type, the parameter values are not logged or stored in the deployment history.
However, if a hardcoded default value is configured for a secure type, that default value is readable to anyone who can access the template or the deployment history.
Hard-coded secrets can compromise security in a way that is not easy to remedy. After the software is in production, an update is required to change the compromised secret.
In the case of a secret that is used to encrypt data, key-rotation steps must be administered to decrypt and re-encrypt all the data protected by the compromised key.
Example 1: The following template shows a parameter with a secret type that has a hardcoded default value.
{
...
"parameters": {
"rootPassword": {
"defaultValue": "HardcodedPassword",
"type": "secureString"
},
"adminLogin": {
"type": "string"
},
"sqlServerName": {
"type": "string"
}
},
...
}
Instance ID: 1A4796F30A1FE894C2C44207CB847E66
Primary Rule ID: C2BE4E43-BF1D-432B-B483-27240E1245BE
Standards and Best Practices
CWE
CWE-321
CWE Top 25 2024
CWE-287 - Improper Authentication
CWE-798 - Use of Hard-coded Credentials
Audit
Status
New
Introduced Date
2023/01/30
Last Found Date
2023/01/30
Remediation Grace Period
1043 days overdue
Assigned User
(Not Set)
Developer Status
Open
Auditor Status
Pending Review
Severity
Critical
Comment
Add
Submit Bug
Add Audit Filter
Assign Attributes

1.6.1.2. リリースの問題の表示

オープン ソース スキャンの問題やオンプレミス スキャンの問題など、アプリケーションのリリースの問題を表示できます。

問題をリリース レベルで表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

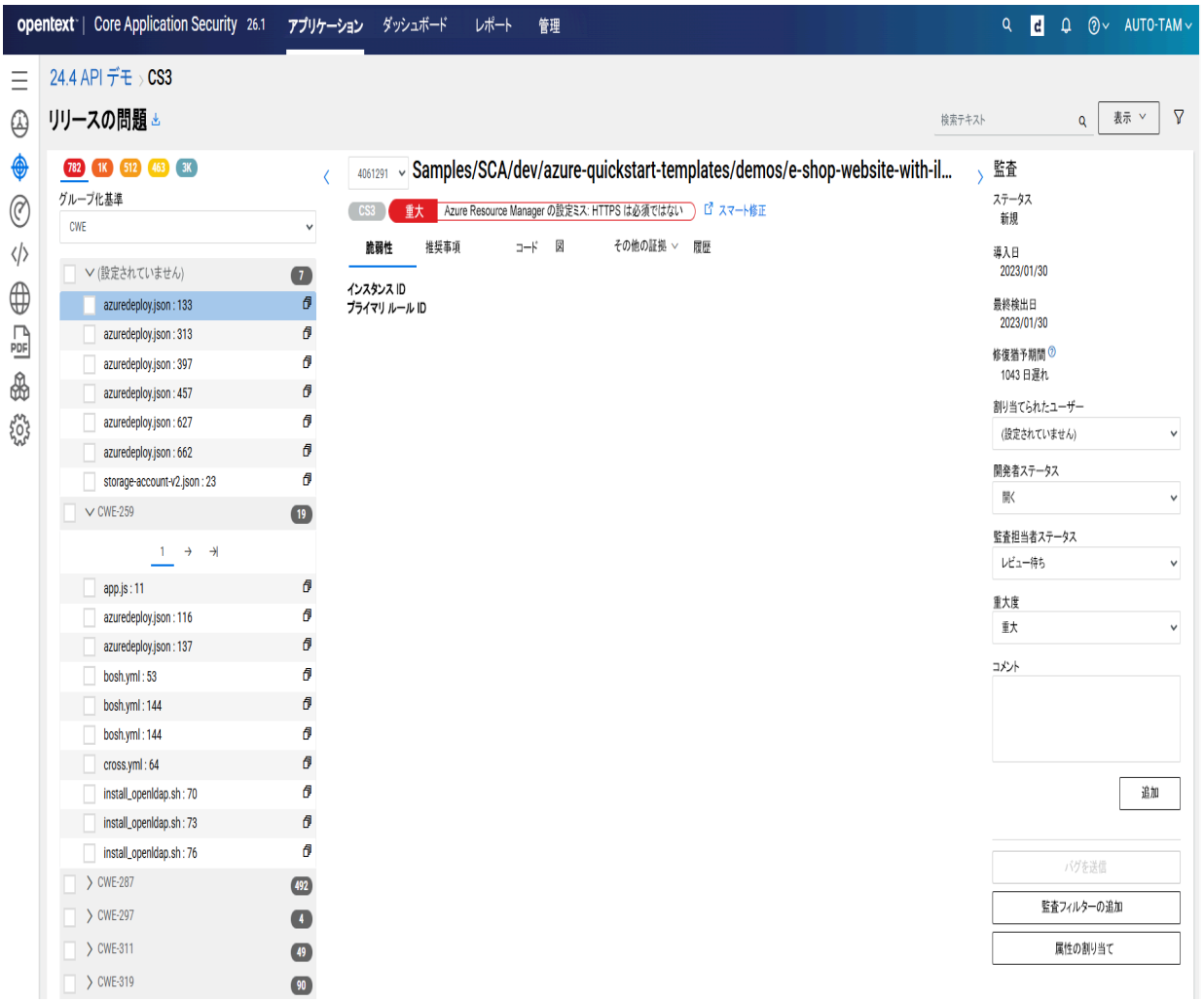
2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. リストからリリースを選択します。

4. [**問題**] をクリックします。

   [リリースの問題] ページが表示されます。グループ内では、問題はファイル名、次に行番号の順に並べ替えられます。グループを選択するときに、個々の問題を選択解除できます。


opentext | Core Application Security 26.1
アプリケーション
ダッシュボード
レポート
管理
AUTO-TAM
24.4 API デモ › CS3
リリースの問題
検索テキスト
表示
782
1K
512
463
3K
グループ化基準
CWE
(設定されていません) 7
azuredeploy.json : 133
azuredeploy.json : 313
azuredeploy.json : 397
azuredeploy.json : 457
azuredeploy.json : 627
azuredeploy.json : 662
storage-account-v2.json : 23
CWE-259 19
app.js : 11
azuredeploy.json : 116
azuredeploy.json : 137
bosh.yml : 53
bosh.yml : 144
bosh.yml : 144
cross.yml : 64
install_openldap.sh : 70
install_openldap.sh : 73
install_openldap.sh : 76
CWE-287 492
CWE-297 4
CWE-311 49
CWE-319 90
4061291
Samples/SCA/dev/azure-quickstart-templates/demos/e-shop-website-with-il...
CS3
重大
Azure Resource Manager の設定ミス: HTTPS は必須ではない
スマート修正
脆弱性
推奨事項
コード
図
その他の証拠
履歴
インスタンス ID
プライマリ ルール ID
監査
ステータス
新規
導入日
2023/01/30
最終検出日
2023/01/30
修復猶予期間
1043 日遅れ
割り当てられたユーザー
(設定されていません)
開発者ステータス
開く
監査担当者ステータス
レビュー待ち
重大度
重大
コメント
追加
バグを送信
監査フィルターの追加
属性の割り当て

1.6.1.3. [問題] ページの操作

次の表に、[アプリケーションの問題] ページと [リリースの問題] ページの操作方法を説明します。

一般的なナビゲーション

タスク	アクション
誤検知の再確認を送信する	[**再確認を送信**] をクリックします。[**誤検知の再確認を送信**] 権限が必要です。
問題のデータのエクスポート	をクリックします。CSV ファイルをダウンロードするリンクがアカウント設定で指定された電子メール アドレスに送信されます。リンクは電子メールが送信されてから 7 日間有効で、送信されたユーザーのみがアクセスできます。 **Note** [テナント ダッシュボード]、[自分のリリース]、[アプリケーションの問題]、および [リリースの問題] ページのエクスポート機能では同じ列フィールドが出力されます。現在適用されているフィルターはエクスポートにも適用されます。
問題を検索する	検索テキスト フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。
修正済みの問題を表示または非表示にする	[**抑制済みを表示**] をクリックして、[検証済みの修正] の問題の表示と非表示を切り替えます。
抑制された問題を表示または非表示にする	[**抑制済みを表示**] をクリックして、[誤検知を確認済み] と [抑制済み] の問題の表示と非表示を切り替えます。
フィルター リストを非表示にするか表示する	をクリックします。

タスク	アクション
フィルター オプションとグループ化オプションをカスタマイズする	⚙ をクリックします。選択内容に応じて、[問題] ページに表示されるオプションが決まります。詳細については、「問題フィルターとグループ化のカスタマイズ」を参照してください。
フィルターを展開するか折りたたむ	[**すべて展開**]、[**すべて折りたたむ**] またはフィルター名の横にある矢印をクリックします。
フィルターを適用する	フィルター名の下にある目的のフィルター値を選択します。フィルタリングの結果によりページが自動的に更新されます。一部のフィルターについては、[**適用**] をクリックしてページを更新します。詳細については、「[問題] ページのフィルター オプションとグループ化オプション」を参照してください。
適用されたフィルターをクエリとして保存する	[**クエリを保存**] をクリックします。[カスタム クエリに名前を付ける] ウィンドウが表示されます。クエリの名前を入力し、[**保存**] をクリックします。保存されたクエリが [**準備されたクエリ**] フィルターに表示されます。
適用されたフィルターを削除する	[**X**] または [**フィルターをクリア**] をクリックします。

ナビゲーション パネル

タスク	アクション
パネルを展開または折りたたむ	› または ‹ をクリックします。
重大度レベルを基準にして問題を表示する	[**重大**]、[**高**]、[**中**]、[**低**]、[**すべて**] のいずれかのタブを選択します。
表示された問題を属性別にグループ化する	[**グループ化基準**] リストから値を選択します。グループ内では、問題はファイル名、次に行番号の順に並べ替えられます。詳細については、「[問題] ページのフィルター オプションとグループ化オプション」を参照してください。
問題に関する他の詳細情報を表示する	問題の説明をクリックします。
複数の問題を選択する	問題の横にあるチェック ボックスを選択します。
グループ内の問題を順番に表示	右側と左側の矢印をクリックします ←→。

問題の詳細パネル

タスク	アクション
複数のリリースで見つかった問題の特定のインスタンスを表示する	リリース固有の問題 ID をドロップダウンリストから選択します。[リリースの問題] ページの問題の詳細パネルには、デフォルトでそのリリースに固有の問題が表示されます。 
問題の分析トレース図を同じカテゴリのものとともに表示する	[**スマート修正**] リンクをクリックします。[スマート修正] の全画面ビューが表示されます。ここには選択した問題のカテゴリのすべての問題が表示され、選択した問題のデータ フローが強調表示されます。
問題に関する具体的な詳細情報を表示する	タブを選択します。詳細については、「問題の詳細の表示」を参照してください。

監査パネル

タスク	アクション
パネルを展開または折りたたむ	› または ‹ をクリックします。
問題を編集する	使用可能なフィールドを編集します。詳細については、「問題の更新」を参照してください。
問題をバグ トラッカーに送信する	[**バグを送信**] をクリックします。詳細については、「バグ トラッカーへの問題の送信」を参照してください。
問題の監査フィルターを追加する	[**監査フィルターの追加**] をクリックします。詳細については、「問題に対するアプリケーション監査テンプレート フィルターの作成」を参照してください。
問題に属性を割り当てる	[**属性の割り当て**] をクリックします。詳細については、「問題に属性を割り当てる」を参照してください。

1.6.1.4. [問題] ページのフィルタリングとグループ化

[問題] ページでは次のフィルター オプションとグループ化オプションを使用できます。

Note

フィルターをフィルター リストに表示するには、フィルターを有効にする必要があり (「問題フィルターとグループ化のカスタマイズ」を参照)、結果にはそのフィルターに対応する複数の値が含まれている必要があります。

フィルターとグループ化	説明	値
App Defender のステータス	問題のカテゴリが Application Defender でサポートされているかどうか	資格あり、資格なし
割り当てられたユーザー	ユーザーが定義	設定されていません、ユーザーが定義
監査済みタイムスタンプ	[**監査担当者ステータス**] の最終更新日 (フィルターのみ)	

フィルターとグループ化	説明	値
監査担当者ステータス	監査担当者の問題修復ステータス。	• 未抑制のシステム値: [レビュー待ち]、[修復が必要]、[修復が遅延]、[リスクを緩和済み]、[疑わしい]、[提案済み「問題ではありません」] **Note** [疑わしい] および [提案済み「問題ではありません」] は Fortify Remediation Aviator によって設定されます。 • 抑制済みのシステム値: [リスクを受け入れ済み]、[問題ではありません]、[Aviator 監査担当者ステータス抑制済み] • ユーザー定義

フィルターとグループ化	説明	値
不具合が送信されました	問題がバグとしてバグ トラッカーに送信されました	誤、正
カテゴリ	問題のカテゴリ	
準備されたクエリ	既定のクエリ (フィルターのみのオプション)	自分の未解決の問題
カスタム クエリ	保存されたカスタム クエリ (フィルターのみのオプション)	ユーザー定義
CWE	Common Weakness Enumeration の分類	
CWE Top 25 2023	CWE (Common Weakness Enumeration) 上位 25 件 2023 の分類	
CWE Top 25 2024	CWE (Common Weakness Enumeration) 上位 25 件 2024 の分類	
CWE Top 25 2025	CWE (Common Weakness Enumeration) 上位 25 件 2025 の分類	
開発者ステータス	開発者の問題修復ステータス	• システム値: [再確認済み]、[未解決]、[修復中]、[修復済み]、[修正しない]、[サード パーティ コンポーネント] • ユーザー定義

フィルターとグループ化	説明	値
DISA STIG 6.1	DISA Application Security and Development STIG 6.1	
DISA STIG 6.2	DISA Application Security and Development STIG 6.2	
DISA STIG 6.3	DISA Application Security and Development STIG 6.3	
DISA STIG 6.4	DISA Application Security and Development STIG 6.4	
誤検知の再確認		設定されていません、再確認済み、問題を確認済み
FISMA	FISMA の分類 (廃止予定)	
Fortify Remediation Aviator	Fortify Remediation Aviator により監査	誤、正
添付あり		誤、正
コメントあり		誤、正
メモがあります		誤、正
導入日	元々の問題作成日 (フィルターのみ)	

フィルターとグループ化	説明	値
修復猶予期間	残り日数または期限超過日数。このフィールドは、開発者ステータス カテゴリが [未解決] である問題にのみ適用されます。	
抑制済み	問題が抑制済み (フィルターのみ)	誤、正
問題のエージ	アプリケーションで問題が発生してから経過した日数 (フィルターのみ)。これらのカテゴリは累計です。たとえば、30 日を超える問題は 10 日を超える問題としてもカウントされます。	>/< 5 日、>/< 10 日、>/< 30 日、>/< 60 日、>/< 45 日、>/< 90 日
マイクロサービス		
NIST SP 800-53 Rev. 5	National Institute of Standards and Technology Special Publication 800-53	
OWASP 2014 Mobile	OWASP モバイル上位 10 件 2014 の分類	
OWASP 2017	OWASP 2017 の上位 10 件の分類	
OWASP 2021	OWASP 2021 の上位 10 件の分類	

フィルターとグループ化	説明	値
OWASP 2025	OWASP 2025 の上位 10 件の分類	
OWASP LLM 上位 10 件 2025	OWASP LLM 上位 10 件 2025 の分類	
OWASP API 上位 10 件 2023	OWASP API Top 10 2023 の分類	
OWASP ASVS 4.0	OWASP ASVS 4.0 の分類	
OWASP ASVS 5.0	OWASP ASVS 5.0 の分類	
OWASP モバイル上位 10 件 2024	OWASP モバイル上位 10 件 2024 の分類	
パッケージ	パッケージまたは名前空間	
PCI 4.0	PCI 4.0 の分類	
PCI DSS 4.0.1	PCI 4.0.1 の分類	
PCI SSF1.2	PCI SSF 1.2 の分類	
リリース	問題が特定されたリリース (フィルターのみ) **Note** [**リリース**] フィルターは、[アプリケーションの問題] ページにのみ表示されます。	

フィルターとグループ化	説明	値
スキャン ツール	問題の検出に使用したスキャン ツール	DAST、DAST (手動)、SAST、MAST、Debricked、Sonatype
スキャン タイプ	問題が属するスキャン タイプ	動的、静的、モバイル、オープン ソース
スコープ	本番環境または非本番環境の依存関係 (OpenText Core SCA スキャン)	
重大度	問題の重大度 (フィルターのみ)	重大、高、中、低、ベスト プラクティス、情報
シンク	静的スキャンの問題に適用可能なデータフロー シンク機能	
ソース	静的スキャンの問題に適用可能なデータフロー ソース機能	
ステータス	問題のステータス	新規、既存、再発、修正済み/検証済みの修正
<カスタム属性>	カスタム属性	ユーザー定義

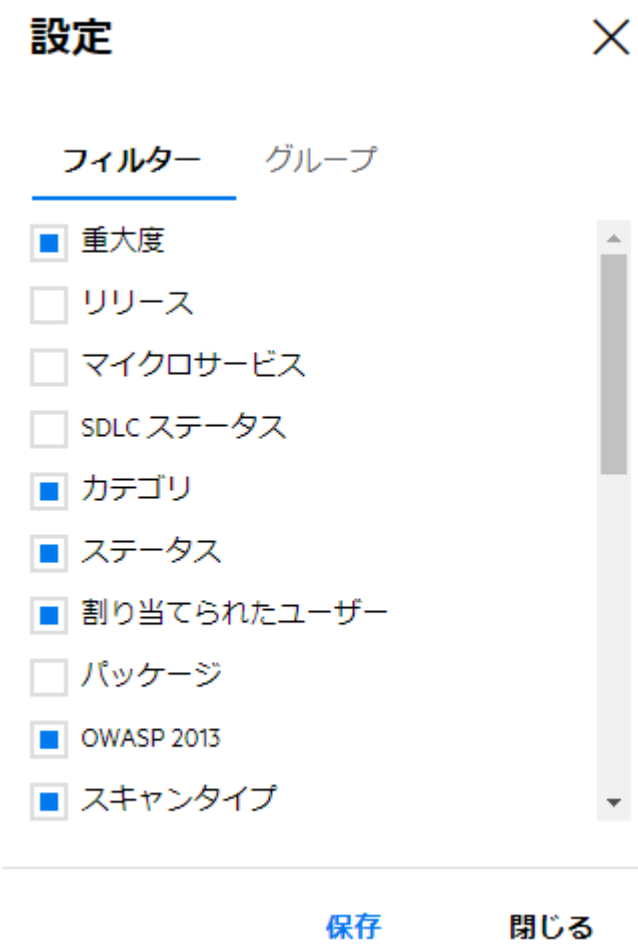
1.6.1.5. 問題フィルターとグループ化のカスタマイズ

[アプリケーションの問題] ページまたは [リリースの問題] ページに表示される問題フィルターとグループ化をカスタマイズできます。

問題フィルターとグループ化をカスタマイズするには、次の手順を実行します。

1. 監査パネルで をクリックします。

   [設定] ウィンドウが表示されます。



2. 関連するタスクを実行します。

タスク	手順
問題フィルターのカスタマイズ	1. [**フィルター**] タブを選択します。 2. 追加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。 3. 削除するフィルターの横にあるチェック ボックスを選択解除します。 4. [**保存**] をクリックします。 [問題] ページがフィルター リストの新しいフィルターで更新されます。 **Note** フィルターがフィルター リストに表示されるのは、結果にそのフィルターの複数の値が含まれている場合だけです。
問題グループ化のカスタマイズ (ナビゲーション パネルの [**グループ化基準**] オプション)	1. [**グループ**] を選択します。 2. [**グループ化基準**] リストに追加する値の横にあるチェック ボックスを選択します。 3. [**グループ化基準**] リストから削除する値の横にあるチェック ボックスをオフにします。 4. [**保存**] をクリックします。 [問題] ページが新しいグループ値で更新されます。

1.6.1.6. 問題に対する属性の割り当て

属性は情報提供のみを目的としたものであり、評価プロセスには影響しません。必要な権限を持つユーザーは、[問題] ページから問題に属性を割り当てることができます。

問題に属性を割り当てるには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 属性を割り当てるアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [アプリケーションの問題] ページまたは [リリースの問題] ページに移動します。

   アプリケーションの問題

4. 監査パネルで [**属性の割り当て**] をクリックします。

   [属性の割り当て] ウィンドウが表示されます。

5. 関連するタスクを実行します。

   属性の割り当て

   1. [**グループ**] を選択します。
   2. 問題の属性を入力します。
   3. [**保存**] をクリックします。属性が保存されます。

1.6.2. 問題点の詳細

[アプリケーションの問題] ページまたは [リリースの問題] ページの問題の詳細パネルには、アプリケーションで検出された脆弱性の分析に役立つ包括的な問題の詳細が表示されます。詳細は、いくつかのタブに分かれています。使用可能なタブは、問題が検出されたスキャン タイプによって異なります。

このセクションでは、次のトピックについて説明します。

- 静的スキャンの問題の詳細
- オープン ソース スキャンの問題の詳細
- 動的スキャンの問題の詳細
- モバイル スキャンの問題の詳細

1.6.2.1. 静的スキャンの問題の詳細

静的スキャンの問題に関する問題詳細パネルには、問題 ID、問題の場所、問題の重大度、および問題のカテゴリが上部に表示されます。その下にあるいくつかのタブには、問題に関する追加情報 (技術情報、コード行 (ソース コードが送信されている場合)、分析トレース図など) が表示されます。

脆弱性

[**脆弱性**] タブには、問題に関する次の技術情報 (問題の概要、問題の実行と意味の説明、問題のインスタンス ID とルール ID、Fortify Software Security Research が提供する基準やベスト プラクティスの情報) が表示されます。

推奨事項

[推奨事項] タブには、問題を修復するための推奨事項と、詳細に調べるためのヒントやリファレンスが表示されます。利用可能な場合は、[**インタラクティブ トレーニング**] セクションに、問題カテゴリに関するインタラクティブ トレーニング、問題カテゴリに関するビデオ、その他の教育リソースへのリンクが含まれています。[**インタラクティブ トレーニング**] セクションは Secure Code Warrior によって提供されています。Secure Code Warrior の詳細については、「Secure Code Warrior の統合」を参照してください。

コード

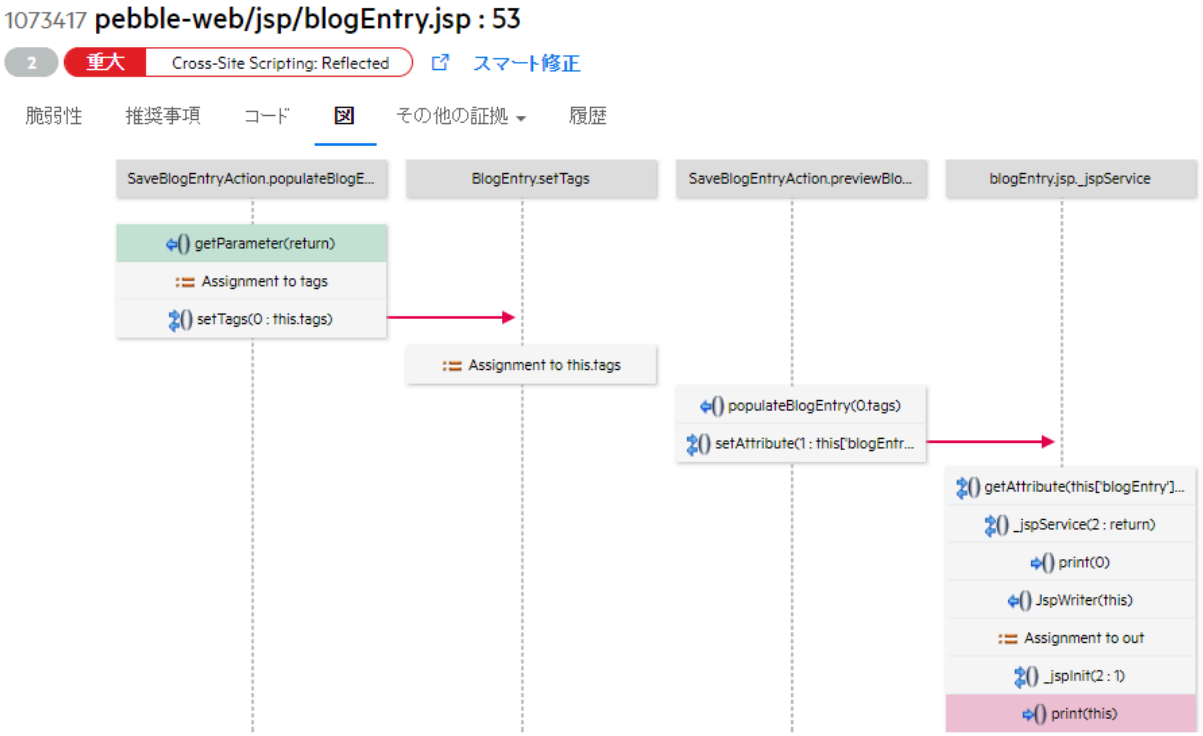
[コード] タブには、問題が検出された特定のコードが表示されます。ユーザーは次の操作を実行して、コードのレビューを簡単に行うことができます。

- ワード ラップを有効または無効にする
- 複数の分析トレースを必要に応じて切り替える
- コードを重ねて表示するのか、それともコードとともに分析トレースをツリー ビューで表示するのかを切り替える
- ツリー ビュー内で分析トレース ノードを選択した場合、コードの行にジャンプする
- インライン分析トレースの表示を有効または無効にする

Note
選択した問題のカテゴリのすべての問題を表示するには、[**スマート修正**] リンクをクリックします。

図

[図] タブには、問題の分析トレース図が表示されます。



その他の証拠

[**その他の証拠**] タブにはメモとスクリーンショットが表示されます。これはドロップダウン メニューから別個にアクセスできます。

- [**注**] セクションには、問題に関するテスト チームからのメモが表示されます。
- [**スクリーンショット**] セクションでは、問題に関するコンテキスト情報を提供するスクリーンショットをアップロードできます。詳細については、「スクリーンショットのアップロード」を参照してください。

履歴

[**履歴**] タブには次の問題イベントのログ (監査の変更、コメント、システム イベント (ステータスの変更、状態のコピー操作、および誤検知の再確認の結果)) が表示されます。ログはイベント タイプ (監査、バグ トラッカー、コメント、またはシステム イベント) を基準にしてフィルタリングできます。


3889610 EternalStorage/EternalStorage.sol : 4
Solidity
重大
Solidity の設定ミス: 既知の脆弱性を持つコンパイラ
スマート修正
脆弱性
推奨事項
コード
図
その他の証拠
履歴
監査
コメント
システム イベント
OpenText™ Core Application Security 2024/04/02 11:32:52 AM
リリース Solidity のスキャン 58934 で問題が見つかりました。
コメントを追加
追加

1.6.2.2. オープン ソース スキャンの問題の詳細

オープン ソース スキャンの問題に関する問題詳細パネルには、問題 ID、問題の場所、問題の重大度、およびルール IDが上部に表示されます。その下にある複数のタブには、問題に関する追加情報が表示されます。

Note

前回の Sonatype スキャンでオープン ソースの問題がアクティブな脆弱性ではないと判明した場合、問題詳細パネルにはメッセージ「This vulnerability is no longer listed as an active vulnerability. (この脆弱性はアクティブな脆弱性としてリストされなくなりました。)」が表示されます。また、問題のステータスは [**検証済みの修正**] とマークされます。これは、削除済みのオープン ソース コンポーネントに関連する問題には適用されません。

脆弱性

[**脆弱性**] タブには、問題に関する次の技術情報 (使用したスキャン ツールからの脆弱性データ、インスタンス ID とルール ID、ファイルの場所、Fortify Software Security Research が提供する標準とベスト プラクティスの情報) が表示されます。

スキャン ツールからの脆弱性データの詳細については、次のリンクを参照してください。

- Sonatype: https://guides.sonatype.com/iqserver/technical-guides/sonatype-vuln-data/
- OpenText Core SCA: https://debricked.com/docs/security/security-about#data-refinement

Note

脆弱性 API エンドポイントでは、Debricked の問題は、[**CheckId**] フィールドに入力 **Malware CVE** が返されます。

脆弱性

推奨事項

[推奨事項] タブには、修復情報および詳細な調査のためのリファレンスが表示されます。[**すべての問題を表示**] をクリックすると、リリース内のパッケージ URL でフィルターされたすべての問題が表示されます。

さらに、OpenText Core SCA の問題については、Open Source Select の健全性メトリックがグラフィカルに表示されます。Open Source Select は、GitHub 上のすべてのオープン ソース プロジェクトのデータベースです。

推奨事項

依存関係 (OpenText Core SCA、CycloneDX)

[**依存関係**] タブには、脆弱なコンポーネントの視覚化された依存関係ツリーが表示されます。依存関係ツリーは、脆弱なコンポーネントを含むルート ノード (直接的な依存関係) ごとに表示されます。

Note

依存関係の詳細と `debricked.fingerprints.txt` ファイルがない SBOM では依存関係ツリーは利用できません。

OpenTextMSP ポータルでは、依存関係ツリーを確認し、ルート修正の解決策を使用して問題を解決することをお勧めします。ルート修正には、影響を受ける依存関係の脆弱なバージョンを含まない直接的な依存関係の次のバージョンが含まれます。簡単に言うと、ルート修正は、依存関係ツリーのルートから始まる依存関係の脆弱性に対する解決策です。ルート修正の使用の詳細については、「ルート修正の解決策を使用して脆弱性を手動で解決するにはどうすればよいですか?」を参照してください。

- さまざまなロック ファイルで見つかった問題については、ドロップダウン リストからロック ファイルを選択すると、選択したロック ファイルの完全パスが表示されます。
- 依存関係ツリーは展開したり折りたたんだりできます。
- 脆弱なノードは赤色でマークされます。
- 表示される依存関係ツリーの数は、既知の安全なバージョンを持つルート ノード、またはロックファイルのみの修正であるルート ノードの数です。ロックファイルのみ修正とは、リポジトリ内でロックファイルを再生成でき、脆弱性が解決されることを意味します。直接的な依存関係を更新する必要はありません。代わりに、同じバージョンを再インストールします (たとえば、yarn update を実行し、新しい `yarn.lock` ファイルを生成します)。

依存関係

その他の証拠

[**その他の証拠**] タブにはメモとスクリーンショットが表示されます。これはドロップダウン メニューから別個にアクセスできます。

- [**注**] セクションには、問題に関するテスト チームからのメモが表示されます。
- [**スクリーンショット**] セクションでは、問題に関するコンテキスト情報を提供するスクリーンショットをアップロードできます。詳細については、「スクリーンショットのアップロード」を参照してください。

  その他の証拠

履歴

[**履歴**] タブには問題に関連する次のイベントのログ (監査の変更、コメント、システム イベント (ステータスの変更、状態のコピー操作、および誤検知の再確認の結果)) が表示されます。ログはイベント タイプ (監査、バグ トラッカー、コメント、またはシステム イベント) を基準にしてフィルタリングできます。

履歴

1.6.2.3. 動的スキャンの問題の詳細

動的スキャンの問題に関する問題詳細パネルには、問題 ID、問題の場所、問題の重大度、および問題のカテゴリが上部に表示されます。その下にある複数のタブには、脆弱性に関する追加情報 (技術情報、要求、応答など) が表示されます。

脆弱性

[**脆弱性**] タブには、問題に関する次の技術情報 (問題の概要 (問題のインスタンス ID とルール ID を含む)、問題の実行と意味の説明、Fortify Software Security Research が提供する基準やベスト プラクティスの情報) が表示されます。

脆弱性ビュー

推奨事項

[推奨事項] タブには、問題を修復するための推奨事項と、詳細に調べるためのヒントやリファレンスが表示されます。利用できる場合、[**インタラクティブ トレーニング**] セクションには、Secure Code Warrior により提供される、問題カテゴリのインタラクティブ トレーニングへのリンクが含まれています。Secure Code Warrior の詳細については、「Secure Code Warrior の統合">Secure Code Warrior の統合」を参照してください。

推奨事項ビュー

.

HTTP

[**HTTP**] タブには、要求と応答の内容、ヘッダー、パラメーターが表示され、ドロップダウン メニューから別個にアクセスできます。

[**証拠**] セクションには、問題が見つかった完全なセッション トラフィックが一覧表示されます。

HTTP

その他の証拠

[**その他の証拠**] タブにはメモとスクリーンショットが表示されます。これはドロップダウン メニューから別個にアクセスできます。

- [**注**] セクションには、問題に関するテスト チームからのメモが表示されます。

- [**スクリーンショット**] セクションでは、問題に関するコンテキスト情報を提供するスクリーンショットをアップロードできます。詳細については、「スクリーンショットのアップロード」を参照してください。

  その他の証拠

履歴

[**履歴**] タブには次の問題イベントのログ (監査の変更、コメント、システム イベント (ステータスの変更、状態のコピー操作、および誤検知の再確認の結果)) が表示されます。ログはイベント タイプ (監査、バグ トラッカー、コメント、またはシステム イベント) を基準にしてフィルタリングできます。

履歴

1.6.2.4. モバイル スキャンの問題の詳細

モバイル スキャンの問題に関する問題詳細パネルには、問題 ID、問題の場所、問題の重大度、および問題のカテゴリが上部に表示されます。その下にある複数のタブには、問題に関する追加情報が表示されます。

脆弱性

[**脆弱性**] タブには、問題に関する次の技術情報 (問題の概要、問題のインスタンス ID とルール ID、問題の実行と意味の説明) が表示されます。

推奨事項

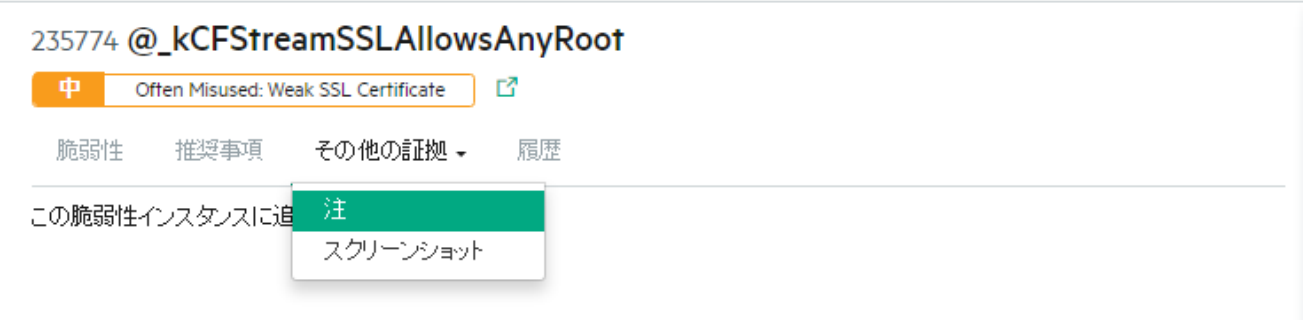
[推奨事項] タブには、問題を修復するための推奨事項と、詳細に調べるためのヒントやリファレンスが表示されます。利用できる場合、[**インタラクティブ トレーニング**] セクションには、Secure Code Warrior により提供される、問題カテゴリのインタラクティブ トレ

ーニングへのリンクが含まれています。Secure Code Warrior の詳細については、「Secure Code Warrior の統合」を参照してください。

その他の証拠

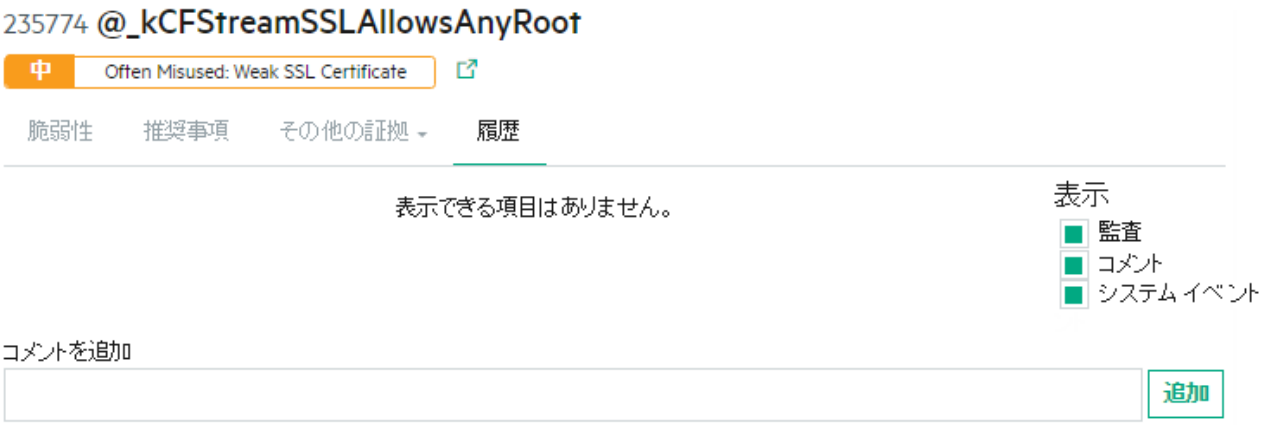
[**その他の証拠**] タブにはメモとスクリーンショットが表示されます。これはドロップダウン メニューから別個にアクセスできます。

- [**注**] セクションには、問題に関するテスト チームからのメモが表示されます。
- [**スクリーンショット**] セクションでは、問題に関するコンテキスト情報を提供するスクリーンショットをアップロードできます。詳細については、「スクリーンショットのアップロード」を参照してください。



履歴

[**履歴**] タブには次の問題イベントのログ (監査の変更、コメント、システム イベント (ステータスの変更、状態のコピー操作、および誤検知の再確認の結果)) が表示されます。ログはイベント タイプ (監査、バグ トラッカー、コメント、またはシステム イベント) を基準にしてフィルタリングできます。


235774 @_kCFStreamSSLAllowsAnyRoot
中
Often Misused: Weak SSL Certificate
脆弱性
推奨事項
その他の証拠
履歴
表示できる項目はありません。
表示
監査
コメント
システム イベント
コメントを追加
追加

1.6.3. 問題の更新

スキャン結果に提供される情報を使用して、見つかった脆弱性を修復します。修復作業を追跡するために、問題をアプリケーションとリリースの両方のレベルで更新できます。

このセクションでは、次のトピックについて説明します。

- 問題の編集
- 複数の問題の編集
- スクリーンショットのアップロード

1.6.3.1. 問題の編集

[アプリケーションの問題] ページと [リリースの問題] ページの両方で問題を編集できます。問題の編集の権限を持つユーザーは、問題の開発者ステータスと、割り当てられたユーザーを編集できます。監査権限があるユーザーは、問題の監査者ステータスおよび重大度を編集することもできます。

問題を編集するには、次の手順を実行します。

Note

[アプリケーションの問題] ページで問題を編集する方法は以下のとおりです。問題の選択と更新は、[リリースの問題] ページでも同じように機能します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 編集する問題のあるアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [**問題**] をクリックします。

   [アプリケーションの問題] ページが表示されます。

4. ナビゲーション パネルで、編集する問題を選択します。問題が複数のリリースで見つかった場合、特定のインスタンスを選択するには、問題の詳細パネルのドロップダウン リストからリリース固有の問題 ID を選択します。

5. 監査パネルで、必要に応じてフィールドを編集します。

フィールド	説明
割り当てられたユーザー	問題を割り当てるユーザーを選択します
開発者ステータス	問題の開発ステータスを選択します。既定値は [**未解決**] です。ステータスの状態は、[未解決] または [終了済み] になります。 ◦ 問題をレビューする場合、[**修復中**] を選択します。 ◦ 問題が妥当であるという確信がない場合は、[**誤検知の再確認**] を選択します。誤検知の再確認プロセスの詳細については、「誤検知の再確認の送信」を参照してください。 ◦ 問題を修復した場合、[**修復済み**] を選択します。 ◦ 問題を修復しない場合、[**修正しない**] を選択します。 ◦ 問題がサードパーティ コードにある場合は、[**サード パーティ コンポーネント**] を選択します。
監査担当者ステータス	問題の監査ステータスを選択します。既定の状態は [**レビュー待ち**] です。ステータスの状態は、[未抑制] または [抑制済み] になります。 ◦ 未抑制: **修復が必要、修復が遅延、リスクを緩和済み** ◦ 抑制済み: **リスクを受け入れ済み、問題ではありません**
重大度	デフォルトの問題の重大度を変更するには、別の重大度を選択します。

フィールド	説明
コメント	[**コメント**] フィールドに補足コメントを入力し、[**追加**] をクリックします。

6. [問題] ページを更新して問題の変更内容を確認します。

> **Note**
>
> 抑制された問題は、[問題] ページに表示されず、[**抑制を表示**] が選択された場合にのみ表示されます。

関連トピック

バグ トラッカーへの問題の送信

1.6.3.2. 複数の問題の編集

[アプリケーションの問題] ページと [リリースの問題] ページの両方で複数の問題を一括編集できます。

複数の問題を編集するには、次の手順を実行します。

> **Note**
>
> [アプリケーションの問題] ページで複数の問題を編集する方法は以下のとおりです。問題の選択と更新は、[リリースの問題] ページでも同じように機能します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 編集する問題のあるアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [**問題**] をクリックします。

   [アプリケーションの問題] ページが表示されます。

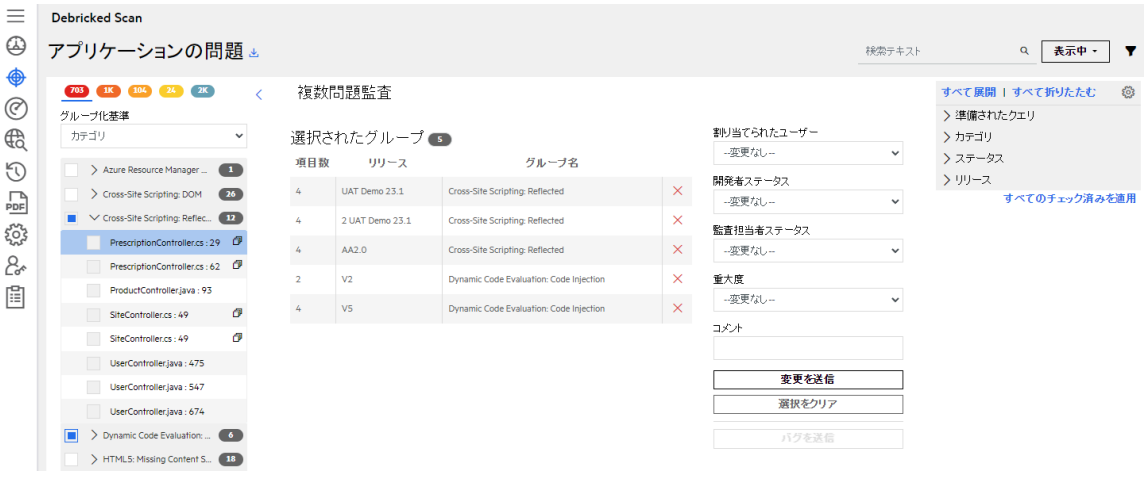
4. 次のアクションを実行して複数の問題を選択します。

   - ナビゲーション パネルで、問題の横にあるチェック ボックスを選択します。

   > **Note**
   >
   > [リリースの問題] ページで、[**他のリリースの問題を含める**] チェック ボックスをオンにして、リリースで見つかった問題のすべてのインスタンスを選択します。問題は個別に削除できます。
   >
   > 
   >

- ナビゲーション パネルで、グループ名の横にあるチェック ボックスを選択してグループ内のすべての問題を選択することもできます。

> **Note**
>
> [リリースの問題] ページで、[**他のリリースの問題を含める**] チェック ボックスをオンにして、同じリリースで見つかった問題を別のグループとして選択できます。リリース グループは個別に削除できます。
>
> 
>



5. 監査フィールドを編集するには、次のタスクを実行します。

タスク	説明
監査フィールドを手動で編集する	監査パネルで、必要に応じてフィールドを編集します。編集可能なフィールドは、[**割り当てられたユーザー**]、[**開発者ステータス**]、[**監査担当者ステータス**]、[**重大度**]、[**コメント**] です。

タスク	説明
監査の詳細をある問題から別の問題にコピーする	1. 問題パネルで、コピーする問題の行の [**監査の詳細を表示**] をクリックします。 [問題 ID] ウィンドウが表示されます。  2. コピーする監査エントリとコメント エントリを選択します。 3. すべての添付ファイルをコピーするには、[**添付ファイルを含める**] チェック ボックスをオンにします。 4. [**監査の詳細をコピー**] をクリックします。 [問題] ページにリダイレクトされます。監査値が、選択した監査エントリ、コメント、および添付ファイルとともに、選択した他の問題に適用されます。

タスク	説明
	Important 選択した問題のインスタンス ID が一致する必要があります。一致しない場合は、監査の詳細のコピーを続行できません。

6. [**変更を送信**] をクリックします。

   [問題] ページが更新されて、問題の変更内容が表示されます。

関連トピック

バグ トラッカーへの問題の送信

1.6.3.3. スクリーンショットのアップロード

問題のスクリーンショットを [アプリケーションの問題] ページまたは [リリースの問題] ページでアップロードできます。

- サポートされるファイル タイプは .jpg、.gif、および .png です。
- ファイルの大きさは 3MB 以下にする必要があります。

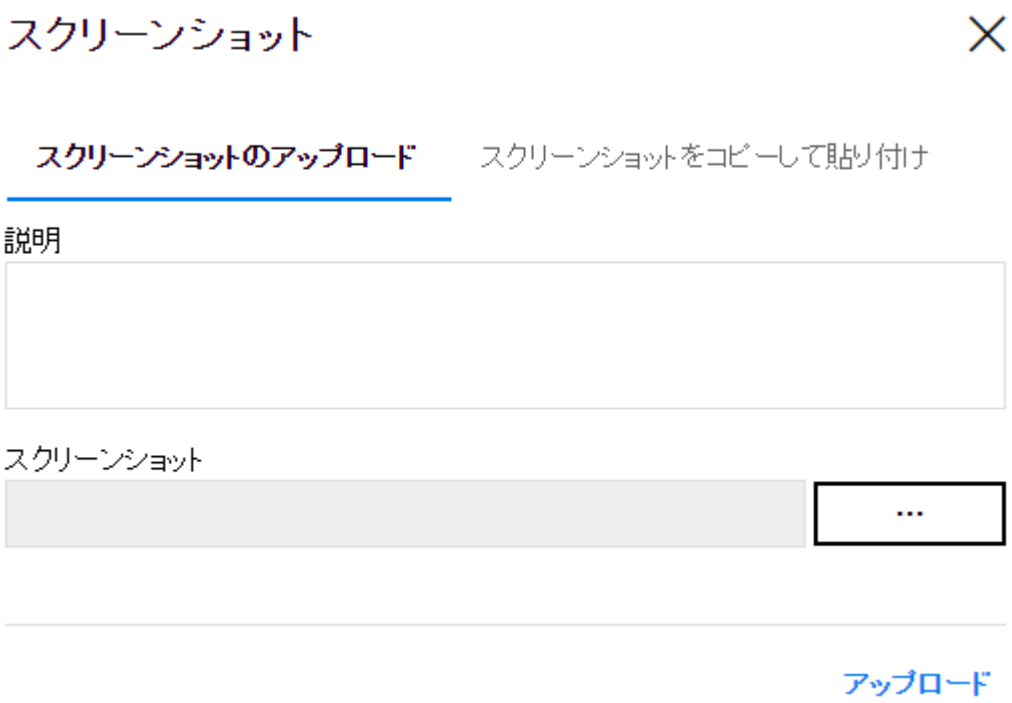
スクリーンショットをアップロードするには、保存されたファイルをアップロードする方法と、イメージをコピーしてモーダル ウィンドウに貼り付ける方法があります。

問題のスクリーンショットをアップロードするには、次の手順を実行します。

1. 問題の詳細パネルで、**[その他の証拠]** タブ > **[スクリーンショット]** の順に選択します。

2. [+ スクリーンショットを追加] をクリックします。

   [スクリーンショット] モーダル ウィンドウが表示されます。



3. 次のいずれかの方法を選択して、スクリーンショットをアップロードします。

   - ファイルをアップロードする

     1. **[スクリーンショットのアップロード]** タブを選択します。
     2. (オプション) ファイルの説明を入力します。
     3. **...** をクリックし、スクリーンショットを参照して選択します。
     4. **[アップロード]** をクリックします。

   - スクリーンショットをコピーして貼り付ける

     1. **[スクリーンショットをコピーして貼り付け]** タブを選択します。
     2. (オプション) ファイルの説明を入力します。
     3. 画像をクリップボードにコピーします。
     4. ボックスを選択し、 **Ctrl キーを押しながら V キー** を押してクリップボードから画像を貼り付けます。
     5. **[アップロード]** をクリックします。

     タブには、アップロードされたスクリーンショットの詳細およびスクリーンショットを表示、保存、削除するためのアイコンが表示されます。

アイコン	説明
	ブラウザでスクリーンショットを表示します。
	スクリーンショットを開くか、ローカル システムに保存します。
	スクリーンショットを削除します。

1.6.4. 問題修復の監査

OpenText Fortify on Demand を使用すると、組織の開発チームやセキュリティ チームは問題修復を監査できます。ここでは、問題修復ワークフローにさまざまなユーザー ロールが関与します。**問題の編集**権限があるユーザー (通常、開発チーム) は問題を受け取り、問題を修復するかどうかを決定します。**問題の監査**権限があるユーザー (通常、セキュリティ チーム) は、開発チームの完了後に問題を検証し、問題を抑制するかどうかを決定します。**問題の表示**の権限を持つユーザーは、問題を表示することはできますが、変更を行うことはできません。

このセクションでは、次のトピックについて説明します。

- 監査担当者の監査ワークフロー
- 開発者の監査ワークフロー

1.6.4.1. 監査担当者の監査ワークフロー

次の手順は、新しい問題を割り当てたり、終了済みの問題をレビューしたりする場合にセキュリティ チームが実行する一般的なワークフローを示しています。

セキュリティ チームの監査担当者には、[**監査担当者ステータス**] および [**重大度**] フィールドを編集できる問題の監査権限が必要です。

新しい問題の割り当て

次の既定値が設定された新しい問題がキューに登録されます。

- **開発者ステータス**: **未解決**
- **ユーザー**: **(設定されていません)**
- **監査担当者ステータス**: **レビュー待ち**
- **重大度**: OpenText Fortify on Demand ランクの既定

セキュリティ チームは、問題をレビューし、修復のために開発者に割り当てます。

新しい問題を、修正のために開発者に割り当てるには、次の手順を実行します。

1. [**開発者ステータス**] が [**開いた状態**] に設定されている問題をレビューします。
2. 必要に応じて、[**重大度**] リストから異なる問題の重大度を選択します。問題の重大度の詳細ついては、「優先順位」を参照してください。
3. [**ユーザー**] リストから、問題に割り当てる開発者を選択します。

終了済みの問題のレビュー

問題に対する作業が完了したら、開発者は [**開発者ステータス**] を終了済みの状態 ([**修復済み**]、[**修正しない**]、[**サード パーティ コンポーネント**]) に変更します。その後、問題は監査のためにセキュリティ チームの問題キューに戻されます。

終了済みの問題をレビューするには、次の手順を実行します。

1. 終了済みの問題に対する変更内容を監査します。
2. 変更内容の評価に基づいて、問題を抑制するかどうかを決定し、[**監査担当者ステータス**] リストから対応する理由を選択します。
    - 未抑制: **修復が必要**、**修復が遅延**、**リスクを緩和済み**
    - 抑制済み: **リスクを受け入れ済み**、**問題ではありません**
3. [**修復が必要**] を選択した場合、問題を開発者に再度割り当てます。
4. 補足コメントを追加します。

1.6.4.2. 開発者の監査ワークフロー

次の手順は、問題を修復したり、問題を終了したりする場合に開発チームが実行する一般的なワークフローを示しています。

開発チームの開発者には、[**開発者ステータス**] および [**ユーザー**] フィールドを編集できる問題の編集権限が必要です。

問題の修復

セキュリティ チームは、修復のために未解決の問題を開発者に割り当てます。

問題を修復するには、次の手順を実行します。

1. [**開発者ステータス**] を [**修復中**] に設定します。
2. 問題をレビューし、次のいずれかの操作を実行します。
    - 問題が妥当であるという確信がない場合は、問題に誤検知のフラグを付ける。誤検知の再確認プロセスの詳細については、「誤検知の再確認の送信」を参照してください。
    - 問題を修復する。
    - 問題を修復しない。

問題の終了

問題を終了するには、次の手順を実行します。

1. 問題に対する作業が終了したら、[**開発者ステータス**] を [**修復済み**]、[**修正しない**]、または [**サード パーティ コンポーネント**] に設定します。

    この問題は、この時点で終了します。

2. 補足コメントを追加します。
3. [**ユーザー**] リストから、問題をレビューする監査担当者を選択します。

1.6.5. Fortify Remediation Aviator の監査と修復

Fortify Remediation Aviator サービスは、Claude 3.5 Sonnet 大規模言語モデル (LLM) を備えた生成人工知能 (GAI) を活用して結果を監査し、強化された修復ガイダンスを提供します。修復ガイダンスは、スキャン結果に追加されたコメントで構成されており、コードスニペットが含まれます。

Fortify Remediation Aviator は、Fortify Audit Assistant 初回監査後のスキャン結果に適用されます。Fortify Remediation Aviator コンテンツがスキャン結果に追加され、OpenText Fortify on Demand にインポートされます。コンテンツはポータルと API で利用できます。

可用性と対象範囲

- Fortify Remediation Aviator は、自動監査を使用した静的評価に利用できます。
- サポートされているテクノロジ スタック、カテゴリ、およびファイル タイプの詳細については、「Fortify Static Code Analyzer and Tools」を参照してください。
- スキャン結果が非常に大きい場合や、1 つのカテゴリに非常に多くの問題が含まれるスキャン結果の場合、Fortify Remediation Aviator は各カテゴリで、問題のサブセットに制限される可能性があります。

監査と修復ガイダンス

Fortify Remediation Aviator は、[**監査担当者ステータス**] が [**レビュー待ち**] の問題を確認します。Fortify Remediation Aviator は、[**監査担当者ステータス**] を更新してメモを追加します。これらのアクションは、[問題] ページの [問題の詳細] パネルにある [**履歴**] タブに記録されます。監査アクションは [**監査**] として記録され、修復ガイダンスは [**コメント**] として記録されます。

- 誤検知は [**問題ではありません**] とマークされ、自動的に抑制されます。

  問題ではありません

- 一時的な誤検知は [**提案済み「問題ではありません」**] とマークされ、抑制されません。

  提案済み「問題ではありません」

- 正常検知は [**修復が必要**] とマークされます。修復支援は、追加のコメントで構成されており、コード スニペットが含まれます。

修復が必要

- 一時的な正常検知は [**疑わしい**] とマークされ、抑制されません。

  疑わしい

- サポートされていないフレームワーク、言語、カテゴリの問題は [**レビュー待ち**] として残ります。

  レビュー待ち

問題のフィルタリングとグループ化の詳細については、「[問題] ページの操作」を参照してください。

1.6.6. 監査テンプレート

監査テンプレートにより、一貫性のある監査の判断基準を静的、動的、モバイル、オープン ソース スキャンに適用できます。監査テンプレートは、指定されたタイプのすべてのスキャンで問題の抑制または問題の重大度の変更を行うカスタム フィルターで構成されています。

監査テンプレートは、グローバルおよびアプリケーション レベルでスキャン タイプごとに作成できます。セキュリティ リーダーは、グローバル監査テンプレートを管理できます。「**問題の監査**」権限を持つユーザーは、自分がアクセス権を持つアプリケーションの監査テンプレートを管理できます。

Important

監査テンプレートは高度な機能であり、脆弱性のメトリックスとレポートが大幅に変更される場合があります。監査テンプレートを使用する前にドキュメントを確認する必要があります。他に疑問がある場合は、サポート チームに問い合わせてください。

このセクションでは、次のトピックについて説明します。

- グローバル監査テンプレートの作成
- アプリケーション監査テンプレートの作成
- 問題に対するアプリケーション監査テンプレートの作成
- 監査テンプレートの使用法と例

1.6.6.1. グローバル監査テンプレートの作成

セキュリティ リーダーは、グローバル監査テンプレートを管理できます。グローバル監査テンプレートは、テナント内で指定されたタイプのスキャンすべてに適用されます。

監査テンプレートは次の条件に従います。

- 監査テンプレート フィルターは大文字と小文字を区別しない。
- 新規作成または変更された監査テンプレート フィルターは、以降に公開されたスキャンに適用される。

グローバル監査テンプレートを作成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**監査ツール**] をクリックします。

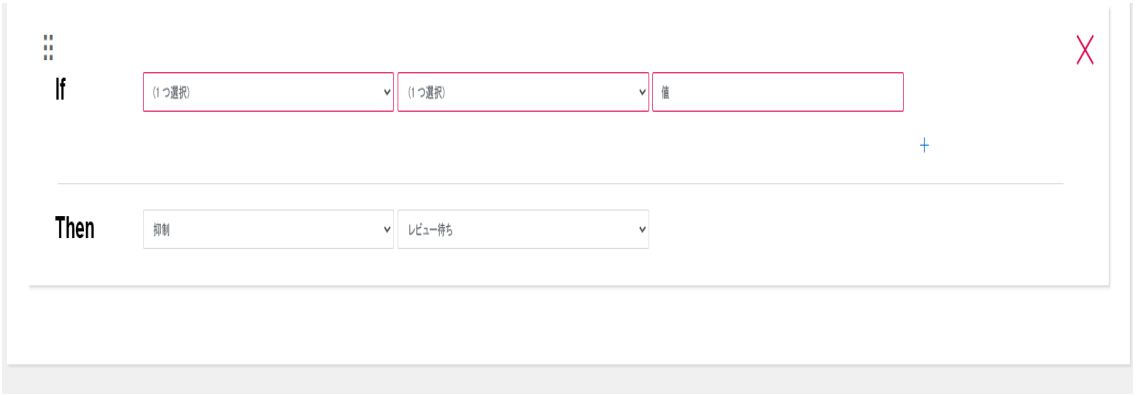
   [高度な監査ツール] ページが表示されます。

3. [**グローバル監査テンプレート**] タブで、[**スキャン タイプ**] リストから、グローバル監査テンプレートを適用するスキャン タイプを選択します。

4. フィルターを追加するには、次の手順を実行します。複数のフィルターを追加できます。

   1. [**フィルターの追加**] をクリックします。

      空のフィルターが表示されます。



2. フィルター条件を指定します。
    1. **IF** 行で、フィルターを適用する問題属性またはカスタム属性を選択します。

> **Note**
>
> 静的、動的、およびモバイル問題属性は、Fortify Software Security Content によって設定されます。オープン ソース問題属性は、Sonatype によって設定されます。

フィールド	スキャン タイプ	説明
重大度	静的、動的、モバイル、オープン ソース	問題の重大度
ルール ID	静的、動的、モバイル、オープン ソース	問題を特定したルールの一意の IDルール ID は、問題の詳細パネルの [**脆弱性**] タブにあります。
分野	静的、動的、モバイル	Seven Pernicious Kingdoms の分類
カテゴリ	静的、動的、モバイル	1 つ以上のルール ID を含む脆弱性カテゴリ。カテゴリに基づくフィルターがそのカテゴリに属するすべてのルール ID に適用されます。
<カスタム アプリケーションの属性>	静的、動的、モバイル	テナント内のカスタム属性 (選択リスト、テキスト、およびブール値)
URL	動的、モバイル	問題の URL
本文	動的、モバイル	HTTP メッセージの本文
ヘッダー	動的、モバイル	HTTP 要求ヘッダー

フィールド	スキャン タイプ	説明
パラメーター	動的、モバイル	HTTP クエリ パラメーター
コンポーネント名	オープン ソース	コンポーネント名
コンポーネントのバージョン	オープン ソース	コンポーネントのバージョン
ファイルの場所	オープン ソース	ファイルの場所

2. 次のいずれかの演算子を選択します。

演算子	説明
次を含む	指定された値を含む結果を検索します
次を含まない	指定された値を含まない結果を検索します
次と等しい	指定された値に完全一致するものを検索します
次と等しくない	指定された値に一致しない結果を検索します

3. 問題属性の値を入力します。ワイルドカードは使用できません。

> **Note**
>
> 以前にカスタム選択リストまたはブール属性と [**次と等しい**] 演算子を選択した場合、値は事前に入力されています。

4. 必要に応じて、[**+**] をクリックして追加のフィルター条件を作成します。

5. 複数のフィルター条件を組み合わせるには、**および** あるいは**または** を選択します。

3. **THEN** 行で、一致する結果に適用する監査アクションとして次のいずれかを選択します。

演算子	説明
抑制	一致する結果を抑制します。抑制が自動的に発生するときに適用する監査担当者ステータスを次の中から選択できます。 ▪ レビュー待ち ▪ リスクを受け入れ済み ▪ 問題 ▪ Aviator 監査担当者ステータス抑制済み
重大度の設定	一致する結果の問題の重大度を指定された値に設定します。

5. フィルターの配置を変更するには、⠿ をクリックし、フィルターを目的のスロットにドラッグします。
6. フィルターの追加と配置が完了したら、[**保存**] をクリックします。

   グローバル監査テンプレートが保存されます。

関連トピック:

アプリケーション監査テンプレートの作成方法については、「アプリケーション監査テンプレートの作成」を参照してください。

1.6.6.2. アプリケーション監査テンプレートの作成

「**問題の監査**」権限を持つユーザーは、自分がアクセス権を持つアプリケーションの監査テンプレートを管理できます。アプリケーション監査テンプレートは、アプリケーションに対して指定されたタイプのスキャンすべてに適用されます。

監査テンプレートは次の条件に従います。

- 監査テンプレート フィルターは大文字と小文字を区別しない。
- 新規作成または変更された監査テンプレート フィルターは、以降に公開されたスキャンに適用される。

アプリケーション監査テンプレートを作成するには、次の手順を実行します。

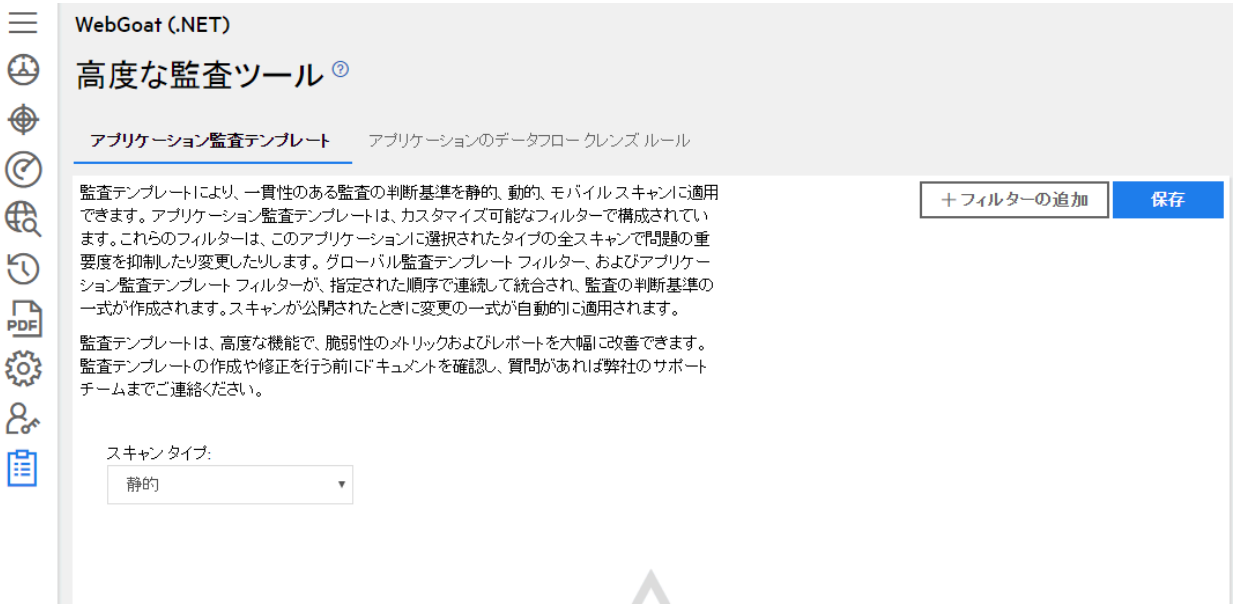
1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. アプリケーション監査テンプレートを作成するアプリケーションの名前をクリックします。

3. [**監査ツール**] をクリックします。

   [高度な監査ツール] ページが表示されます。

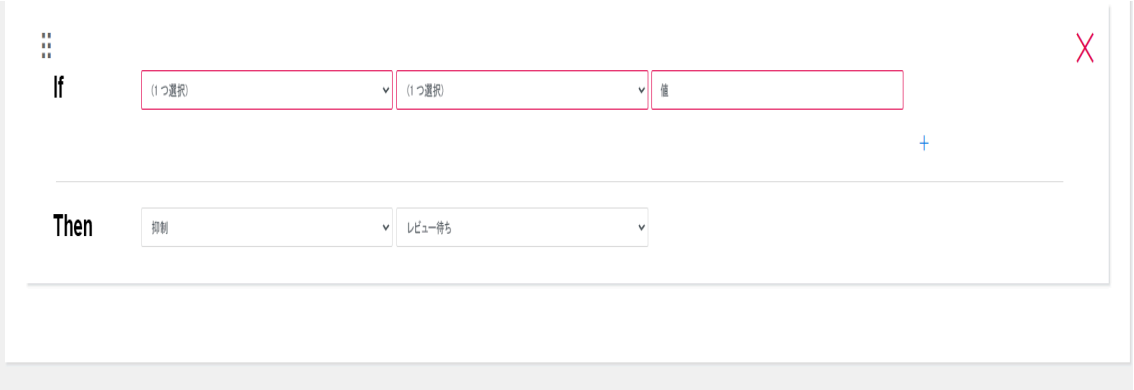


4. [**アプリケーション監査テンプレート**] タブで、[**スキャン タイプ**] リストから、アプリケーション監査テンプレートを適用するスキャン タイプを選択します。

5. フィルターを追加するには、次の手順を実行します。複数のフィルターを追加できます。

1. [**フィルターの追加**] をクリックします。

   空のフィルターが表示されます。



2. フィルター条件を指定します。

   1. **IF** 行で、フィルターを適用する次の問題属性のいずれかを選択します。

      Note

      静的、動的、およびモバイル問題属性は、Fortify Software Security Content によって設定されます。オープン ソース問題属性は、Sonatype によって設定されます。

フィールド	スキャン タイプ	説明
重大度	静的、動的、モバイル、オープン ソース	問題の重大度。
ルール ID	静的、動的、モバイル、オープン ソース	問題を特定したルールの一意の IDルール ID は、問題の詳細を表示するときに [**脆弱性**] タブに表示されます。
分野	静的、動的、モバイル	Seven Pernicious Kingdoms の分類。
カテゴリ	静的、動的、モバイル	1 つ以上のルール ID を含む脆弱性カテゴリ。カテゴリに基づくフィルターがそのカテゴリに属するすべてのルール ID に適用されます。
ファイル	静的	ファイルのフル パス
パッケージ	静的	パッケージまたは名前空間
ソース	静的	データフローのソース機能
シンク	静的	データフローのシンク機能

フィールド	スキャン タイプ	説明
URL	動的、モバイル	問題の URL
本文	動的、モバイル	HTTP メッセージの本文
ヘッダー	動的、モバイル	HTTP 要求ヘッダー
パラメーター	動的、モバイル	HTTP クエリ パラメーター
コンポーネント名	オープン ソース	コンポーネント名
コンポーネントのバージョン	オープン ソース	コンポーネントのバージョン
ファイルの場所	オープン ソース	ファイルの場所

2. 次のいずれかの演算子を選択します。

演算子	説明
次を含む	指定された値を含む結果を検索します
次を含まない	指定された値を含まない結果を検索します
次と等しい	指定された値に完全一致するものを検索します
次と等しくない	指定された値に一致しない結果を検索します

3. 問題属性の値を入力します。ワイルドカードは使用できません。

4. 必要に応じて、[**+**] をクリックして追加のフィルター条件を作成します。
5. 複数のフィルター条件を組み合わせるには、[**および**] あるいは [**または**] を選択します。

3. **THEN** 行で、一致する結果に適用する監査アクションとして次のいずれかを選択します。

演算子	説明
抑制	一致する結果を抑制します。抑制が自動的に発生するときに適用する監査担当者ステータスを次の中から選択できます。 ▪ レビュー待ち ▪ リスクを受け入れ済み ▪ 問題 ▪ Aviator 監査担当者ステータス抑制済み
重大度の設定	一致する結果の問題の重大度を指定された値に設定します。

6. フィルターの配置を変更するには、  をクリックし、フィルターを目的のスロットにドラッグします。
7. フィルターの追加と配置が完了したら、[**保存**] をクリックします。

   アプリケーション監査テンプレートが保存されます。

関連トピック:

グローバル監査テンプレートの作成方法については、「グローバル監査テンプレートの作成」を参照してください。

1.6.6.3. 問題に対するアプリケーション監査テンプレートの作成

[**問題の監査**] 権限を持つユーザーは、アプリケーション監査テンプレートを新規作成できることに加えて、[問題] ページから問題に対するアプリケーション監査テンプレート フィルターを作成できます。これにより、監査者は問題をレビューしながら監査の判断基準を簡単に適用できます。

問題に対するアプリケーション監査テンプレートを作成するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 監査するアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [アプリケーションの問題] ページまたは [リリースの問題] ページに移動します。

   アプリケーションの問題

4. 監査パネルで [**監査フィルターの追加**] をクリックします。

   [監査テンプレート] ウィンドウが表示されます。

5. 関連するタスクを実行します。

   - 選択した問題に既存のフィルターが適用されている場合、そのフィルターが表示されます。フィルターは編集できます。

     > **Note**
     >
     > 複数のフィルターが適用され、その中の 1 つが抑制の場合は、そのフィルターのみが表示されます。

     監査テンプレート

     1. [**フィルターの編集**] をクリックします。

        [アプリケーション監査テンプレート] ページにリダイレクトされます。

     2. 必要に応じて既存のフィルターを編集します。

- 選択した問題に適用されるフィルターがない場合、問題に適用される事前に定義された条件のリストから新しいフィルターを作成できます。

  監査テンプレート

  1. フィルター条件を選択します。複数の条件は AND 演算子で結合されます。
  2. 監査アクションを選択します。[**抑制**] の場合、使用可能なオプションは、[レビュー待ち]、[リスクを受け入れ済み]、[問題ではありません]、および [Aviator 監査担当者ステータス抑制済み] です。[**重大度の設定**] の場合、使用可能なオプションは、[重大]、[高]、[中]、[低] です。
  3. [**フィルターの作成**] をクリックします。アプリケーション監査テンプレートが保存されます。

1.6.6.4. 監査テンプレートの使用法と例

監査テンプレート フィルターは、表示される順番に集計されます。最初にグローバル監査テンプレート フィルター、次にアプリケーション監査テンプレート フィルターが集計され、監査の判断基準の一式が作成されます。これらの判断基準は、スキャンが公開されたときに自動的に適用されます。監査テンプレートの結果としての問題の変更は、[**監査**] タイプのイベントとして、[問題の詳細] パネルの [**履歴**] タブに表示されます。グローバル監査の変更とアプリケーション監査の変更は個別に記録されます。

一般に、ルールベースのフィルターよりもカテゴリベースのフィルターを使用しますが、例外としてルールベースのフィルターの方が適しているシナリオもあります。たとえば、ルール ID ベースのフィルターを使用して、動的スキャンでの SSL/TLS チェックに関するさまざまな修復ポリシーを扱うことができます。

セキュリティ コンテンツの更新ごとにカテゴリとルールは変更されます。セキュリティ コンテンツの更新後はフィルターを確認し、必要に応じて更新することが重要です。

- 新しいカテゴリが追加されている場合があります。
- カテゴリ名が変更されている可能性があります。カテゴリベースのフィルターを更新して変更された名前を反映する必要があります。
- 新しいルールがカテゴリに追加されている場合があります。既存のカテゴリ フィルターは、新しいルールにも適用されます。新しいルールは、カテゴリ内の既存のルールとは明らかに異なる新しい重大な脆弱性をカバーする場合があることに注意してください。
- 既存のルールは、新しいガイダンスと業界標準を反映するように更新されている可能性があります。たとえば、脆弱性に関する新しい情報によって脆弱性に対する重大度が高くなる可能性があります。

カテゴリおよびルールの変更の詳細については、Fortify Software Security Research (SSR) による Fortify Software Security Content の四半期ごとの更新情報を参照してください。この情報にはヘルプ センターからアクセスできます。

次の例は、いくつかのフィルターの組み合わせとその適用方法を示します。

例 1:

監査テンプレート フィルター:

1. [**重大度**] が [**重大**] に [**等しい**] 場合、[**重大度の設定**] を [**高**] に設定
2. [**重大度**] が **[重大] に [等しい]** 場合、[**重大度の設定**] を [**中**] に設定

結果: 選択したスキャン タイプの重大な問題は [中] に設定されます。

例 2:

監査テンプレート フィルター:

1. [**重大度**] が [**重大**] に [**等しい**] 場合、[**重大度の設定**] を [**高**] に設定
2. [**重大度**] が [**高**] に [**等しい**] 場合、[**重大度の設定**] を [**中**] に設定

結果: 選択したスキャン タイプの重大な問題は [高] に設定され、[高] の問題は [中] 設定されます。

例 3:

監査テンプレート フィルター: [**ルール ID**] が [**11516 に等しい**] 場合、[**抑制**] に設定

結果: 選択したスキャン タイプのルール ID 1156 の問題は抑制されます。

例 4:

グローバル監査テンプレート フィルター: [**重大度**] が [**重大**] に [**等しい**] 場合、[**重大度の設定**] を [**高**] に設定

アプリケーション監査テンプレート フィルター: [**重大度**] が [**重大**] に [**等しい**] 場合、[**重大度の設定**] を [**中**] に設定

結果: 選択したタイプのすべてのスキャンの重要な問題は [高] に設定されますが、上のアプリケーションでの選択されたタイプのスキャンの重大な問題は [中] に設定されます。

1.6.7. データフロー クレンズ ルール

データフロー クレンズ ルールには、問題のあるデータ (ユーザー制御入力) をレンダリングする検証ロジックおよびその他のアクションを記述します。OpenText SAST は、静的スキャンに組み込まれているデータフロー クレンズ ルールにより、クレンジング機能を認識できます。その結果、データフロー クレンズ ルールは、データフローの問題に関する誤検出を防ぐのに役立ちます。

データフロー クレンズ ルールは、グローバルおよびアプリケーション レベルで作成できます。セキュリティ リーダーは、グローバル データフロー クレンズ ルールを管理できます。「**問題の監査**」権限を持つユーザーは、自分がアクセス権を持つアプリケーションのデータフロー クレンズ ルールを管理できます。

> **Important**
>
> データフロー クレンズ ルールは高度な機能であり、スキャンで検出された脆弱性が大幅に変更される場合があります。OpenTextMSP ポータルは、データフロー クレンズ ルールを使用する前にドキュメントを確認することを強くお勧めします。他に疑問がある場合は、サポートに問い合わせてください。

このセクションでは、次のトピックについて説明します。

- グローバル データフロー クレンズ ルールの作成
- アプリケーションのデータフロー クレンズ ルールの作成
- データフロー クレンズ ルールの使用法と例

1.6.7.1. グローバル データフロー クレンズ ルールの作成

セキュリティ リーダーは、グローバル データフロー クレンズ ルールを管理できます。グローバル データフロー クレンズ ルールは、テナントのすべての静的スキャンに適用されます。

データフロー クレンズ ルールは次の条件に従います。

- データフロー クレンズ ルールは大文字と小文字を区別し、英数字に制限されます。
- データフロー クレンズ ルールは、今後開始されるスキャンに適用されます。

グローバル データフロー クレンズ ルールを作成するには、次の手順を実行します。

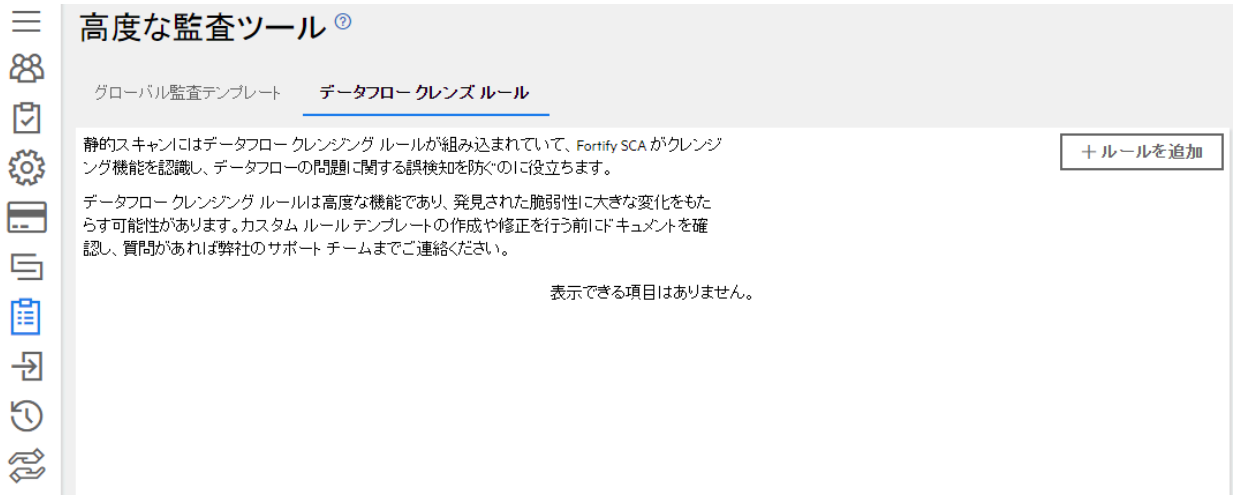
1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**監査ツール**] をクリックします。

   [高度な監査ツール] ページが表示されます。

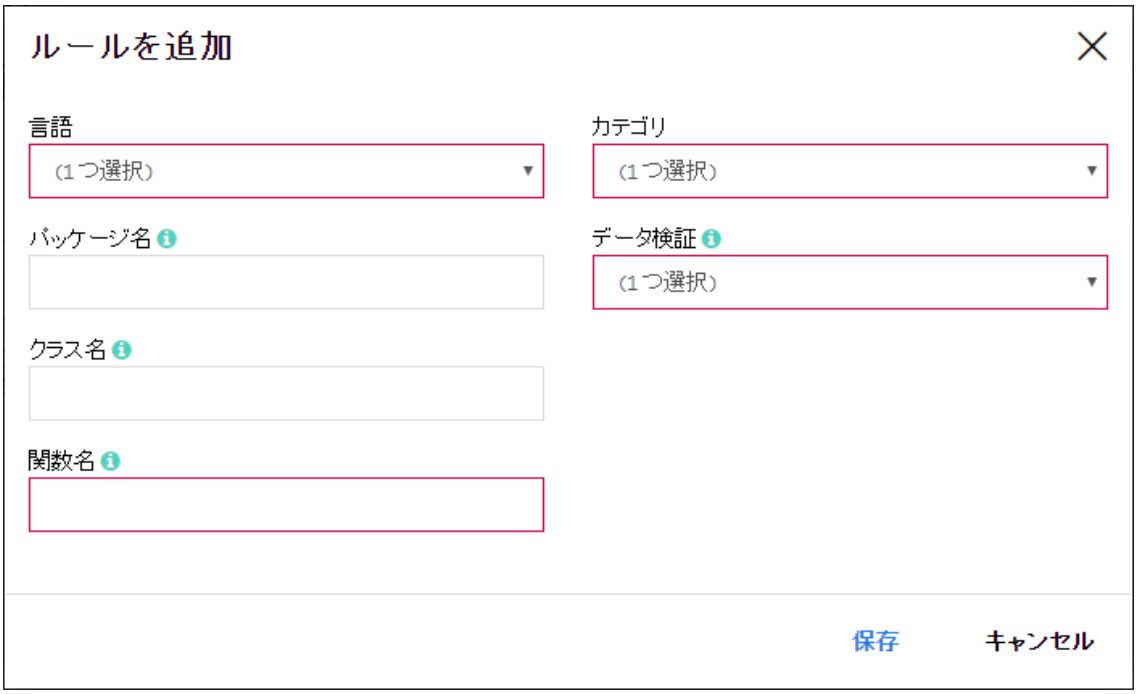
3. [**データフロー クレンズ ルール**] タブを選択します。



4. ルールを追加するには、次の手順を実行します。複数のルールを追加できます。

    1. [**ルールを追加**] をクリックします。

       [ルールを追加] ウィンドウが開きます。



2. 必要に応じてフィールドに入力します。他に指示がない限り、フィールドは必須です。

> **Note**
>
> ルールは、インターフェイスまたはスーパークラスには適用されません。

フィールド	説明
言語	テクノロジ スタックを選択します。
パッケージ名	(オプション) 検証関数を含むパッケージまたは名前空間の名前を入力します。パッケージ名を指定しない場合、ルールはパッケージ内にない関数のみに一致します。
クラス名	(オプション) 検証関数を含むクラスの名前を入力します。クラス名を指定しない場合、ルールはクラス内にない関数のみに一致します。ネストされたクラスを指定するには、ドット表記を使用します (たとえば、`OuterClass.NestedClass`)。 **Note** .NET 言語の場合、汎用クラスのクラス名の規則として、クラス名に続けて @ とタイプ パラメーターの数を追加します。たとえば、`System.Func<T, TResult>` の場合、クラス名は `Func@2` となります。
関数名	検証関数の名前を入力します。

フィールド	説明
カテゴリ	検証関数によって修復される脆弱性カテゴリを選択します。

フィールド	説明
データ検証	関数によって検証されたデータを選択します。 ▪ [**戻り値**]: `value = web.getWebInput(foo, bar)` の `value` を参照する場合に使用します ▪ [**オブジェクト関数**]: `value = web.getWebInput(foo, bar)` の `web` または `object = new MyObject()` の `object` を参照する場合に使用します ▪ [**引数**]: 関数の引数を参照する場合に使用します。引数には 0 で始まるインデックスが付けられます。たとえば、`bar` の `value = web.getWebInput(foo, bar)` を参照するには 1 を指定します。 例: `string filename = UploadedFile.FileName(); if (Validators.IsValidFileName(filename)) { System.IO.File.Delete(filename); }` **データフロー クレンズ ルールの使用法と例:** グローバルおよびアプリケーションのデータフロー クレンズ ルールは、スキャン中に適用される単一ルールのセットに集約されます。ルールに基づいて削除された問題は、FPR には表示されません。

フィールド	説明
	次の例は、いくつかのデータフロー クレンズ ルールとその適用方法を示しています: 例 1: 言語: **Java** パッケージ名: **com.fortify.appsec** クラス名: **Validation** 関数名: **validateAlphaNumeric** Category: **SQL インジェクション** データ検証: **戻り値** 結果: メソッドの戻り値はクレンジング済みと見なされ、SQL インジェクションの問題のフラグは付けられません。 例 2: 言語: **Java** パッケージ名: **java.util** クラス名: **Map** 関数名: **clear** Category: **SQL インジェクション** データ検証: **オブジェクト関数** 結果: データは、Map.clear() メソッドの呼び出し後にクレンジング済みと見なされ、SQL インジェクションの問題のフラグは付けられません。

5. ルールの追加が完了したら、[**保存**] をクリックします。

   グローバル データフロー クレンズ ルールが保存されます。

1.6.7.2. アプリケーションのデータフロー クレンズ ルールの作成

「**問題の監査**」権限を持つユーザーは、自分がアクセス権を持つアプリケーションのデータフロー クレンズ ルールを管理できます。アプリケーションのデータフロー クレンズ ルールは、アプリケーションのすべての静的スキャンに適用されます。

データフロー クレンズ ルールは次の条件に従います。

- データフロー クレンズ ルールは大文字と小文字を区別し、英数字に制限されます。
- データフロー クレンズ ルールは、今後開始されるスキャンに適用されます。

アプリケーションのデータフロー クレンズ ルールを作成するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

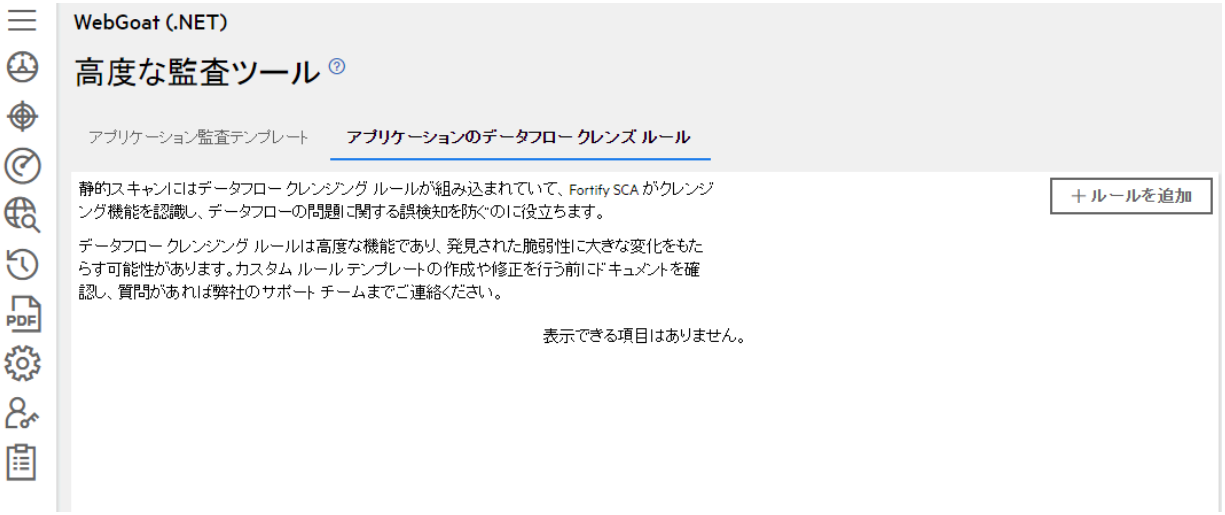
   [アプリケーション] ページが表示されます。

2. アプリケーション監査テンプレートを作成するアプリケーションの名前をクリックします。

3. [**監査ツール**] をクリックします。

   [高度な監査ツール] ページが表示されます。

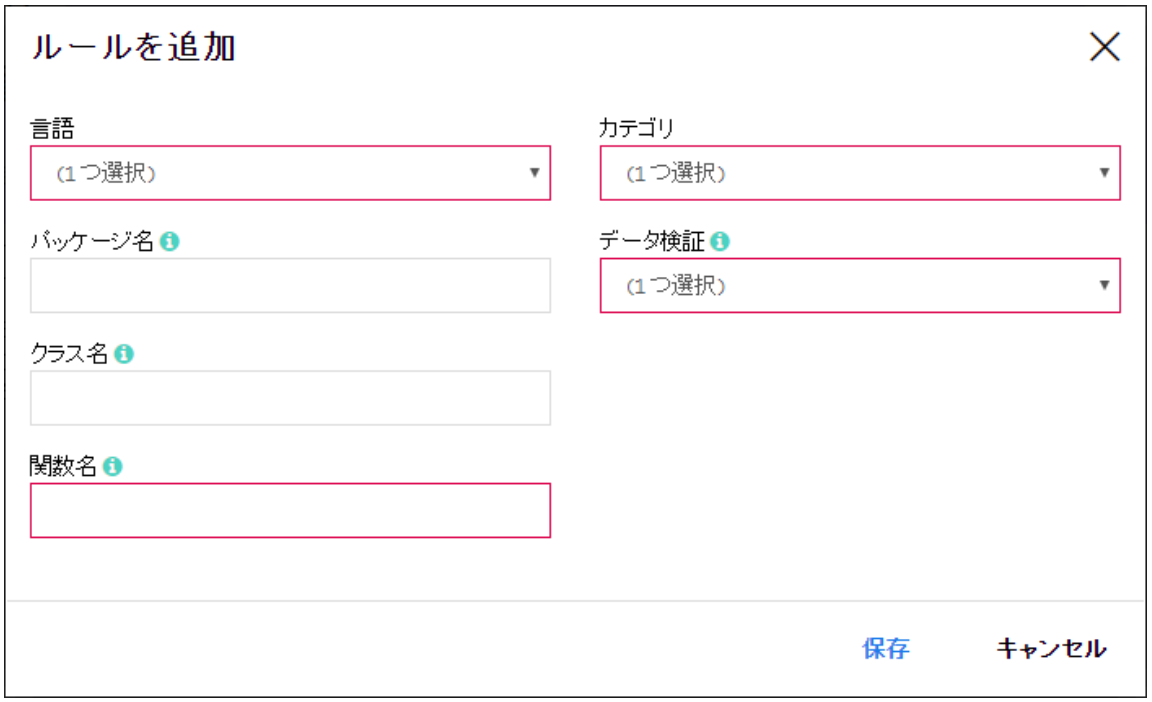
4. [**データフロー クレンズ ルール**] タブを選択します。



5. ルールを追加するには、次の手順を実行します。複数のルールを追加できます。

   1. [**ルールを追加**] をクリックします。

      [ルールを追加] ウィンドウが開きます。



2. 必要に応じてフィールドに入力します。他に指示がない限り、フィールドは必須です。

> **Note**
>
> ルールは、インターフェイスまたはスーパークラスには適用されません。

フィールド	説明
言語	テクノロジ スタックを選択します。
パッケージ名	(オプション) 検証関数を含むパッケージまたは名前空間の名前を入力します。パッケージ名を指定しない場合、ルールはパッケージ内にない関数のみに一致します。
クラス名	(オプション) 検証関数を含むクラスの名前を入力します。クラス名を指定しない場合、ルールはクラス内にない関数のみに一致します。ネストされたクラスを指定するには、ドット表記を使用します (たとえば、`OuterClass.NestedClass`)。 **Note** .NET 言語の場合、汎用クラスのクラス名の規則として、クラス名に続けて @ とタイプ パラメーターの数を追加します。たとえば、`System.Func<T, TResult>` の場合、クラス名は `Func@2` となります。
関数名	検証関数の名前を入力します。
カテゴリ	検証関数によって修復される脆弱性カテゴリを選択します。

フィールド	説明
データ検証	関数によって検証されたデータを選択します。 ▪ [**戻り値**]: `value = web.getWebInput(foo, bar)` の `value` を参照する場合に使用します ▪ [**オブジェクト関数**]: `value = web.getWebInput(foo, bar)` の `web` または `object = new MyObject()` の `object` を参照する場合に使用します ▪ [**引数**]: 関数の引数を参照する場合に使用します。引数には 0 で始まるインデックスが付けられます。たとえば、`bar` の `value = web.getWebInput(foo, bar)` を参照するには 1 を指定します。

6. ルールの追加が完了したら、[**保存**] をクリックします。

   アプリケーションのデータフロー クレンズ ルールが保存されます。

1.6.7.3. データフロー クレンズ ルールの使用法と例

グローバルおよびアプリケーションのデータフロー クレンズ ルールは、スキャン中に適用される単一ルールのセットに集約されます。ルールに基づいて削除された問題は、FPR には表示されません。

次の例は、いくつかのデータフロー クレンズ ルールとその適用方法を示しています。

例 1:

言語: **Java**

パッケージ名: `com.fortify.appsec`

クラス名: `Validation`

関数名: `validateAlphaNumeric`

Category: **SQL インジェクション**

データ検証: **戻り値**

結果: メソッドの戻り値はクレンジング済みと見なされ、SQL インジェクションの問題のフラグは付けられません。

例 2:

言語: **Java**

パッケージ名: `java.util`

クラス名: `Map`

関数名: `clear`

Category: **SQL インジェクション**

データ検証: **オブジェクト関数**

結果: データは、`Map.clear()` メソッドの呼び出し後にクレンジング済みと見なされ、SQL インジェクションの問題のフラグは付けられません。

1.6.8. 修復スキャンの要求

初回スキャンで特定された問題を修正した後で、修正スキャンを要求して、問題が修正されたかどうかを検証することができます。評価には、1 つ以上の修正スキャンが含まれます。

- 単一評価には、1 つの修正スキャンが含まれています。
- サブスクリプションの場合、修正スキャン期間中の修正スキャンの回数に制限はありません。
- 修復スキャン期間は、初回スキャンから 30 日間です。例外事項は契約書に記載されています。

[スキャンの設定] ページで [**<assessment_type> - 修正**] を選択して、修正スキャンを要求します。修正スキャンは、初回スキャンと同じアプリケーションで実行する必要があります。たとえば、初回スキャンが本番前サイトで実行された場合は、修正スキャンも本番前サイトで実行する必要があります。修正スキャンは、完全な初回スキャンよりも短時間で完了します。

Note

一部の動的スキャン フィールドは編集用にロックされています。詳細については、「進行中のスキャンおよび完了したスキャンに対する動的スキャンの設定の編集」を参照してください。

1.7. ダッシュボードとレポート

OpenText Fortify on Demand は、評価結果をデータの表示および分析のためのさまざまな形式で提供します。

ダッシュボードは主要指標を視覚的に表示します。ユーザーは複数のダッシュボードを構成して、自分のニーズに関連するデータを表示できます。ダッシュボードは一般的な概要に役立ちますが、ユーザーはレポートを通じて評価結果の詳細ビューを取得できます。OpenText Fortify on Demand では、包括的かつカスタマイズ可能な一連のレポートが提供されます。

このセクションでは、次のトピックについて説明します。

- ダッシュボード
- レポート

1.7.1. ダッシュボード

OpenText Fortify on Demand は、ユーザーがアプリケーションのセキュリティ データを表示および分析するのに役立つダッシュボードを提供します。これらのダッシュボードは、組織のアプリケーション セキュリティ プログラムの包括的な概要を提供し、主要な脆弱性メトリックに関する洞察を提供するとともに、OpenText Fortify on Demand 製品スイート全体で一貫したダッシュボード エクスペリエンスを実現します。

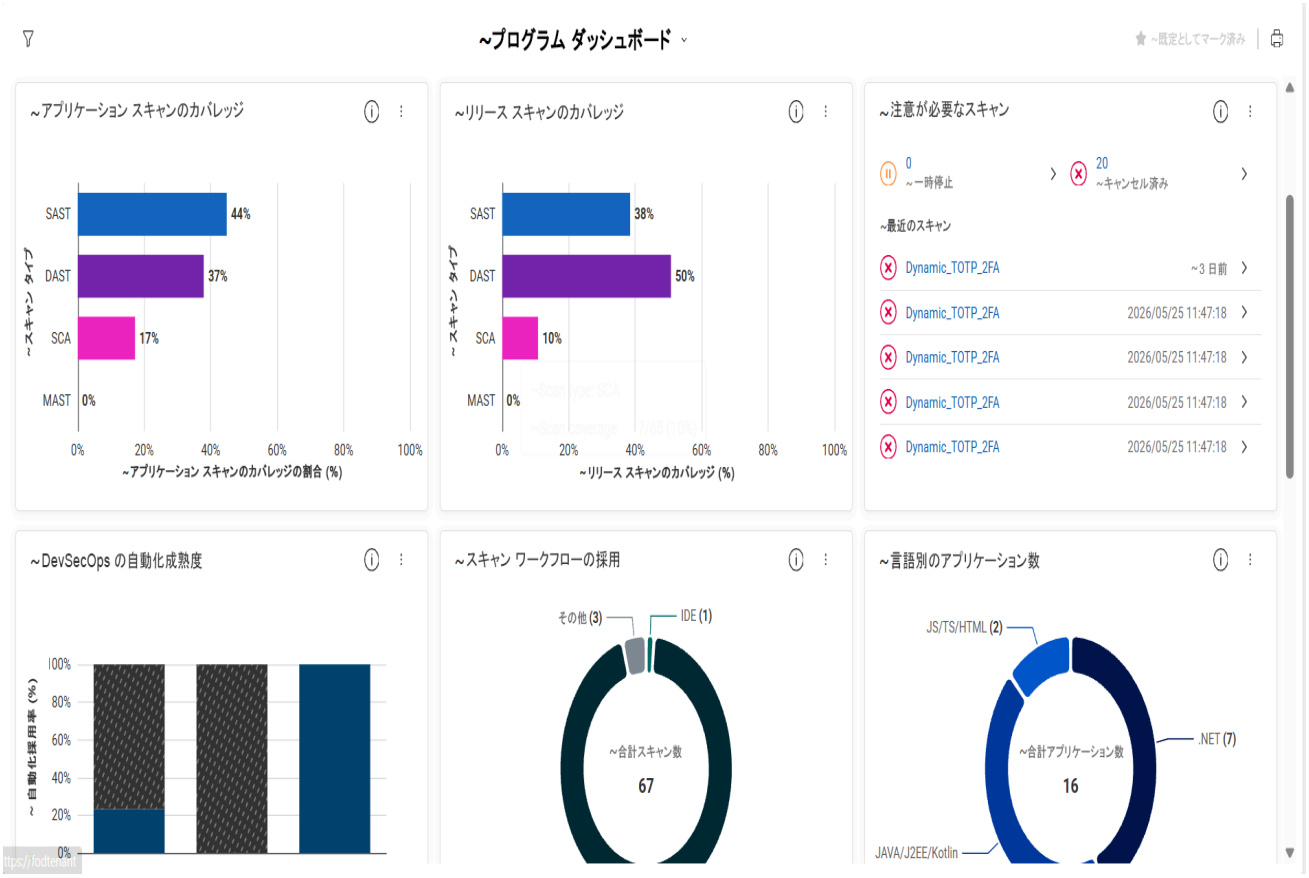
次のダッシュボード タイプを利用できます。

- **プログラム ダッシュボード**
- **修復ダッシュボード**
- **リスク エクスポージャー ダッシュボード**

ダッシュボード ビューを開くと、既定で [**プログラム ダッシュボード**] が表示されます。このダッシュボードは、プログラムの概要を分かりやすく表示します。

既定のビューに加えて、ダッシュボード選択リストを使用して他のダッシュボードに切り替えることができます。

- [**修復ダッシュボード**] は、修正アクティビティをハイライトし、リスク解決に向けた進捗状況を追跡します。
- [**リスク エクスポージャー ダッシュボード**] は、プログラム全体のリスク レベルを特定し評価することに重点を置いています。



次の表に、[**プログラム ダッシュボード**] ページの操作方法を示します。

タスク	アクション
ダッシュボードのタスク	
現在のダッシュボードを既定に設定する	[**既定としてマーク**] をクリックします。
ダッシュボード内のすべてのグラフをフィルタリングする	以下のアプリケーションおよびリリースフィルターから、1 つ以上のフィルター値を選択します。 • アプリケーションの種類 • ビジネス クリティカリティ • マイクロサービス • 合格/不合格 • 星評価 • SDLC ステータス
ダッシュボードの印刷	ツールバーの [**印刷**] アイコンをクリックします。ブラウザーの印刷ビューでダッシュボードが表示され、そこで印刷または保存できます。
タイルのタスク	
タイルのサイズを調整する	タイルの境界線にカーソルを置き、ハンドルをクリックしてドラッグします。
グラフのタスク	
グラフのデータ セットをドリルダウンする	視覚要素をポイントし、ポインターが手の形に変わったらクリックします。

ダッシュボードは以下の要素で構成されています。

- 主要なメトリックスの単一データ ポイント。
- テナント データの特定のファセットを視覚化する個別のグラフ。
- 細かいレベルでカスタマイズ可能なタイル。

ダッシュボードの制限

新しいダッシュボードの現在の実装には、次の制限があります。

- 新しいダッシュボードの作成や既存のダッシュボードのカスタマイズはサポートされていません。
- グラフ内の問題の数は、一意かどうかを考慮したものではありません。
- ほとんどのグラフ タイプで CSV エクスポートがサポートされています。エクスポート機能は、すべてのグラフで利用できるわけではありません。

グラフに表示されているデータは、可能な場合は、フィルタリングしてダウンロードできます。

このセクションでは、次のトピックについて説明します。

- ダッシュボードのタイプ

1.7.1.1. ダッシュボードのタイプ

次のダッシュボード タイプを利用できます。

- 修復ダッシュボード

  ダッシュボードには以下のグラフが含まれます。

  > **Note**
  >
  > インタラクティブなグラフには、データ セットにドリルダウンするためのリンクが含まれています。

  - 重大度別のレビュー範囲
  - スキャン タイプ別のレビュー範囲 (DAST、SAST、MAST、SCA が対象)
  - 平均修復時間
  - 重大度別の修復範囲
  - スキャン タイプ別の修復範囲 (DAST、SAST、MAST、SCA が対象)
  - 重大度別の平均修復時間
  - 問題修復の傾向
  - 問題再発率
  - 頻繁に再発している問題
  - SAST Aviator の採用
  - SAST Aviator の投資利益率 (ROI)

- リスク エクスポージャー ダッシュボード

  ダッシュボードには以下のグラフが含まれます。

  > **Note**
  >
  > インタラクティブなグラフには、データ セットにドリルダウンするためのリンクが含まれています。

  - コンプライアンス ポリシー別のリリース (廃止されたリリースは除く、インタラクティブ)

  - 重大度別の未解決の問題
  - 星評価別のリリース (廃止されたリリースを除く、インタラクティブ)
  - スキャン タイプ別の使用状況概要 (静的、動的、オープンソース、モバイルが対象、インタラクティブ)
  - オープン ソースのセキュリティ リスク
  - 問題密度
  - 最も流行している問題
- プログラム ダッシュボード

  ダッシュボードには以下のグラフが含まれます。

  > **Note**
  >
  > インタラクティブなグラフには、データ セットにドリルダウンするためのリンクが含まれています。

  - プログラムの概要
  - アプリケーション スキャンのカバレッジ
  - リリース スキャンのカバレッジ
  - 注意が必要なスキャン
  - DevSecOps の自動化成熟度
  - スキャン ワークフローの採用
  - 言語別のアプリケーション数
  - スキャン アクティビティの傾向
  - 使用権

    > **Note**
    >
    > 十分なデータが利用可能になるまで、傾向チャートはレンダリングされません。

1.7.2. レポート

OpenText Fortify on Demand では、評価結果の詳細なレポートを生成する機能が提供されています。次のタイプのレポートを生成できます。

- 事前定義されたシステム レポート
- カスタム レポート
- アプリケーション、リリース、スキャン、問題、または使用権の消費のデータ エクスポート
- ベンダー管理機能を使用している場合のベンダー レポート

Note

オープン ソース コンポーネント レポートは、OpenText Fortify on Demand レポート機能を介して使用できます。レポートは、オープン ソース コンポーネント システム テンプレートを使用して生成できます。テンプレートには以下のモジュールが含まれます。

- オープン ソースの部品表: アプリケーションで検出されたコンポーネントの完全なリスト。
- 脆弱性のあるオープン ソース コンポーネント: セキュリティに関する既知の問題が含まれるコンポーネントのリスト

このセクションでは、次のトピックについて説明します。

- レポートの表示
- レポートの生成
- 自動生成レポートのスケジュール
- テンプレート
- データ エクスポート

1.7.2.1. レポートの表示

ポータルでレポートを表示するには、2 つの方法があります。1 つ目の方法は、[レポート] ビューにアクセスして、テナントのすべてのアプリケーションとリリースに対して生成されたすべてのレポートを表示する方法です。もう 1 つの方法は、[**アプリケーション**] ビューにアクセスして、各アプリケーションの詳細情報から、特定のアプリケーションまたはリリースに関連するレポートを表示する方法です。

このセクションでは、次のトピックについて説明します。

- すべてのレポートの表示
- [自分のレポート] ページのフィルター
- アプリケーション レポートの表示
- リリース レポートの表示

1.7.2.1.1. すべてのレポートの表示

[レポート] ページは、レポート ビューの既定のランディング ページであり、すべてのアプリケーションのレポートをテナント レベルで表示できます。

レポートをテナント レベルで表示するには、次の手順を実行します。

1. [レポート] ビューを選択します。

   [レポート] ページが表示されます。このページには、レポートの対象となるアプリケーションとリリース、レポートの作成日時、レポート タイプ、レポート生成のステータス、およびレポートを生成したユーザーが表示されます。

次の表に、[レポート] ページの操作方法を示します。

タスク	アクション
レポート リストを検索する	[**検索テキスト**] フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。検索結果を削除するには、[X] をクリックします。 [**検索テキスト**] ボックスの使用については、「アプリケーションの検索について」を参照してください。
カスタム レポートをインポートする	[**インポート**] をクリックします。
レポートを作成する	[**+ 新規レポート**] をクリックします。
フィルター リストを非表示にするか表示する	をクリックします。
フィルターを展開するか折りたたむ	[**すべて展開**]、[**すべて折りたたむ**] またはフィルター名の横にある矢印をクリックします。
フィルターの適用	フィルター名の下にある目的のフィルター値を選択します。フィルタリングの結果によりページが自動的に更新されます。一部のフィルターについては、[**適用**] をクリックしてページを更新します。フィルター値の詳細については、「[自分のレポート] ページのフィルター」を参照してください。
適用されたフィルターを削除する	適用された各フィルターの横にある [**X**] をクリックするか、[**フィルターをクリア**] をクリックします。
レポートをダウンロードする	をクリックします。レポートがブラウザーの設定で指定したローカルのフォルダーにダウンロードされます。

タスク	アクション
レポートを削除する	をクリックします。
レポートをテナントと共有する	をクリックします。レポートの共有は、別のテナントとの関係を確立している場合に可能です。「ベンダー管理」を参照してください。 **Note** 現在、複数のリリースを含むレポートを共有することはできません。

1.7.2.1.2. [自分のレポート] ページのフィルター

既定では、[自分のレポート] ページには過去 7 日間に作成されたすべてのレポートが表示されます。表示するレポートは、フィルターを適用して制限できます。[自分のレポート] ページでは次のフィルターを使用できます。

Note

フィルターがフィルター リストに表示されるのは、結果にそのフィルターの複数の値が含まれている場合だけです。

フィルター	説明	値
アプリケーション	レポートの適用	ユーザー定義
作成日の範囲	レポートを生成した日	
作成者	レポートを生成したユーザー	ユーザー定義
リリース	リリース	
レポート テンプレート	レポート テンプレートのタイプ	システム定義、ユーザー定義
ステータス	レポート作成ステータス	キューに配置、開始済み、完了

1.7.2.1.3. アプリケーション レポートの表示

選択したアプリケーションのレポートを表示できます。

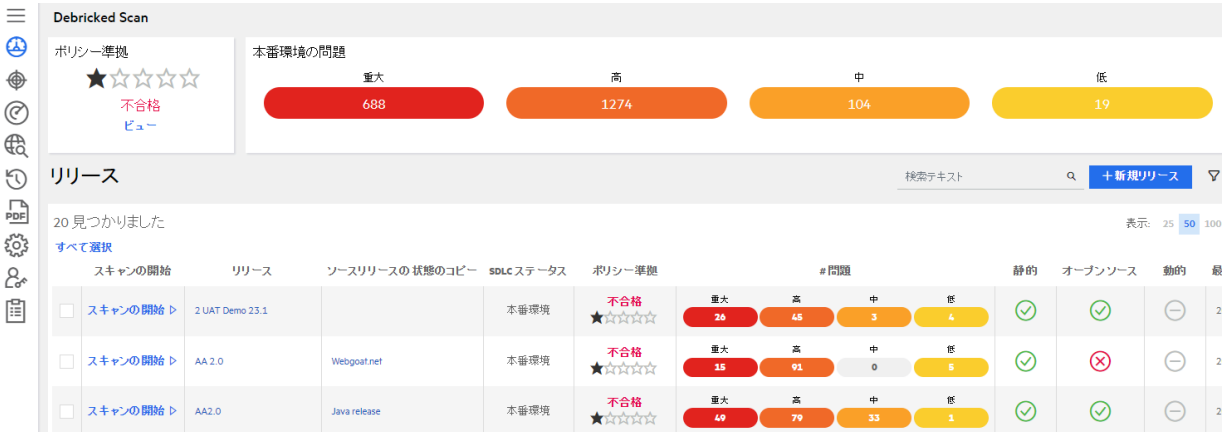
アプリケーションのレポートを表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. レポートを表示するアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。



3. [レポート] をクリックします。

   [レポート] ページに、アプリケーションのすべてのレポートが表示されます。

4. 一覧からレポートを選択します。

1.7.2.1.4. リリース レポートの表示

アプリケーションをドリル ダウンして、選択したリリースのレポートを表示できます。

リリースのレポートを表示するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

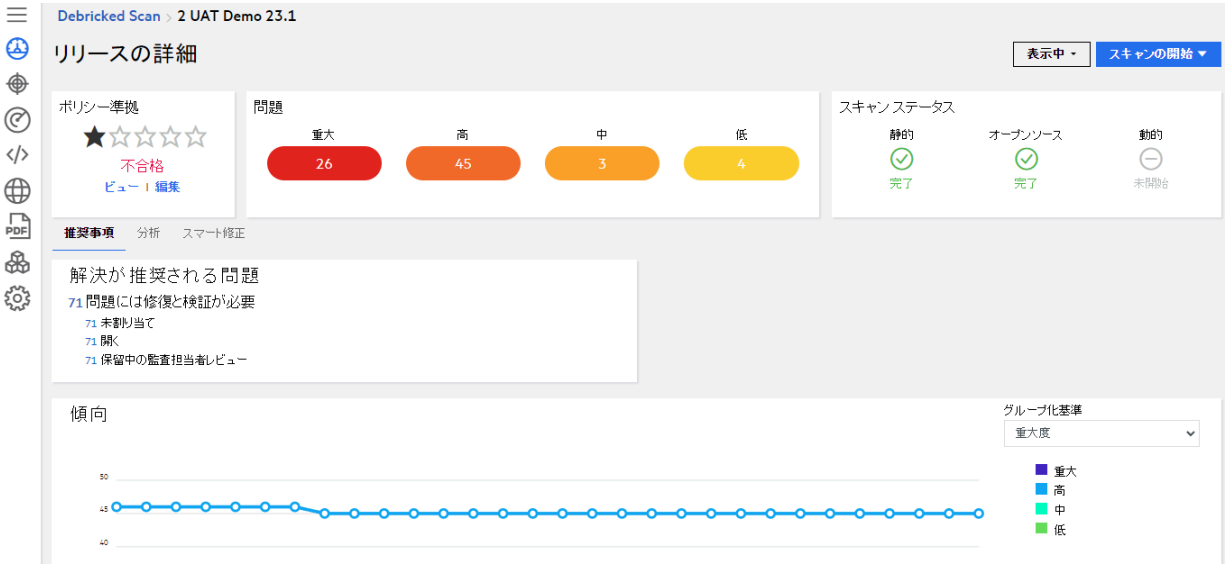
   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. レポートを表示するリリースの名前をクリックします。

   [リリースの概要] ページが表示されます。



4. [レポート] をクリックします。

   [レポート] ページに、選択したリリースのすべてのレポートが表示されます。

5. 一覧からレポートを選択します。

1.7.2.2. レポートの生成

事前定義されたレポート テンプレートまたはカスタムのレポート テンプレートを使用して、リリースのレポートを生成します。レポートは PDF および HTML 形式で使用できます。PDF レポートの生成が失敗する場合は、PDF バージョンの代わりに HTML バージョンが自動的に生成されます。

極端にサイズの大きい PDF レポートを生成する際のエラーを防ぐ目的で、**分析トレース**、**要求/応答**、**問題の詳細**テンプレート モジュールを含み、問題の数が 5000 を超える PDF レポートは生成できません。HTML レポートを生成するか、モジュールを削除した代替レポート テンプレートや問題の数を削減する追加のフィルターを含む代替レポート テンプレートを使用します。

Note

特定の言語でレポートを生成するには、アカウントの設定で言語を選択する必要があります。詳細については、「自分のアカウント情報の編集」を参照してください。

レポートを生成するには、次の手順を実行します。

Note

次の手順では、[レポート] ページでレポートを生成する方法について説明します。アプリケーションのレポート ページとリリースのレポート ページでレポートを生成することもできます。

1. [**レポート**] ビューを選択します。

   [レポート] ページが表示されます。

2. [+ 新規レポート] をクリックします。

   [レポートの作成] ウィザードが表示されます。

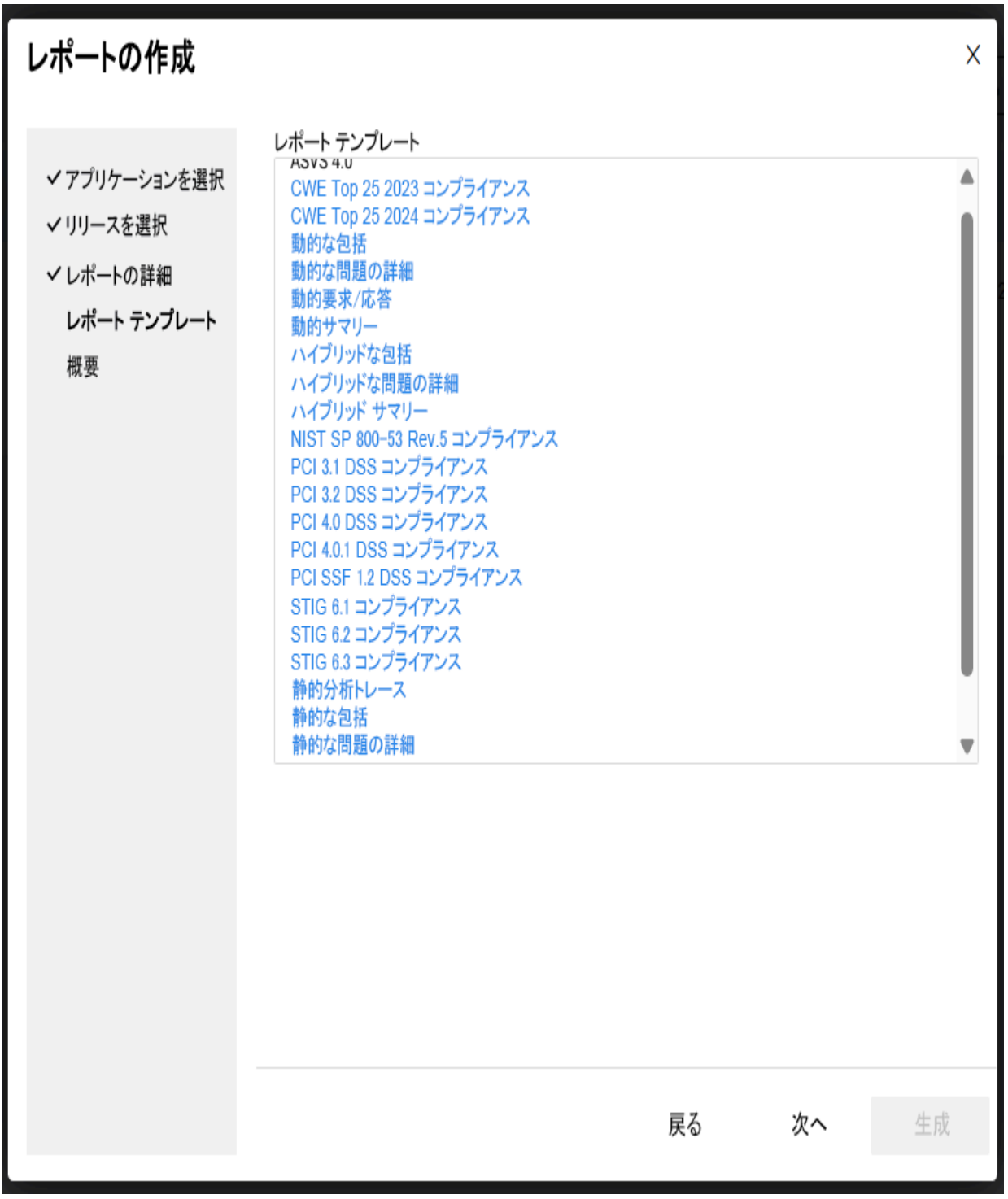
3. **アプリケーションを選択**: アプリケーションを選択し、[**次へ**] をクリックします。

4. **リリースを選択**: リリースを選択し、[**次へ**] をクリックします。複数のリリースを選択した場合、レポートはリリースごとに生成され、zip ファイルにパッケージ化されます。

5. **レポートの詳細**: フィールドをすべて入力して、[**次へ**] をクリックします。他に指示がない限り、フィールドは必須です。

フィールド	説明
レポート名	レポート名を入力します。
注	レポートのメモを入力します。
ファイル タイプ	レポートのファイル タイプとして [**PDF**] または [**HTML**] を選択します。

6. **レポート テンプレート**: レポート テンプレート タイプを選択し、[**次へ**] をクリックします。
    - システム レポート テンプレートは青色で表示され、カスタム レポート テンプレートは黒色で表示されます。
    - リリースに静的な問題データだけが含まれている場合、静的レポート テンプレートのみが使用可能です。
    - リリースに動的な問題データだけが含まれている場合、動的レポート テンプレートのみが使用可能です。



7. **概要**: レポートの概要を確認し、[**生成**] をクリックします。

[レポート] ページにリダイレクトされます。レポートは、「完了」ステータスが表示されると使用できるようになります。

> **Note**
>
> をクリックすると、生成中のレポートを削除できます。

8. 生成されたら、レポートの行で をクリックします。
9. (ファイル タイプに応じて) PDF または zip ファイルが、ブラウザーの設定で指定したフォルダーに保存されます。

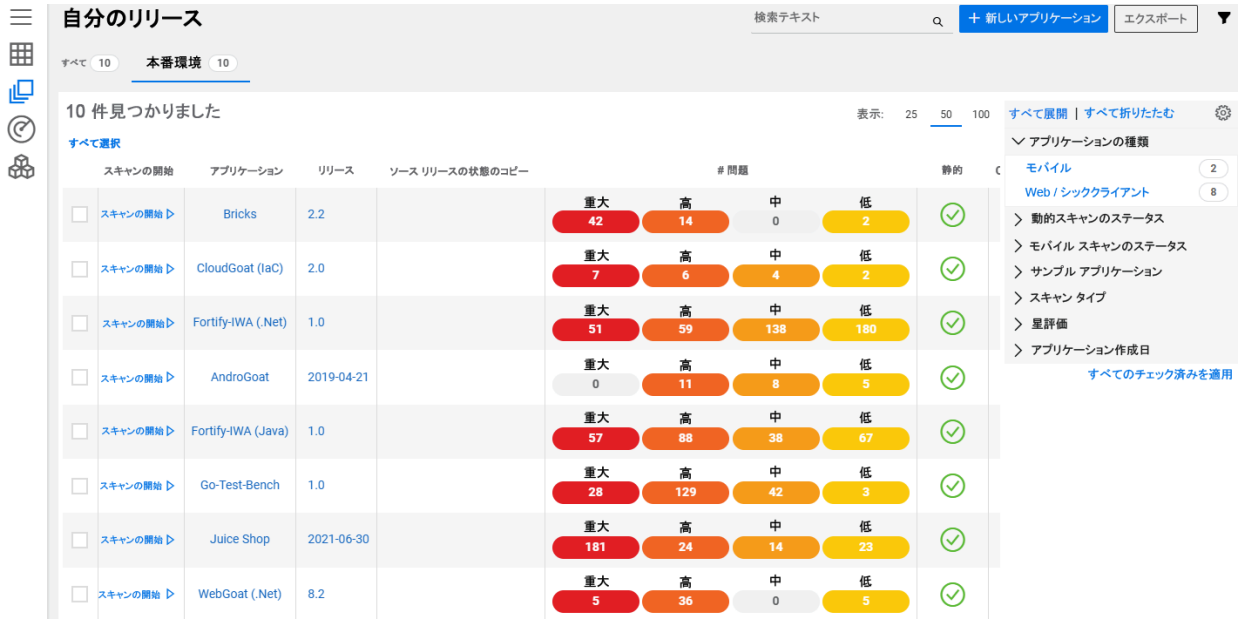
1.7.2.3. 自動生成レポートのスケジュール

同一アプリケーションで複数の評価を実行する計画があり、毎回同じレポートを生成したい場合には、自動生成レポート機能を使用すると時間を節約できます。

レポートの自動生成をスケジュールするには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [**ご使用のリリース**] グリッドに、使用しているリリースのリストが表示されます。

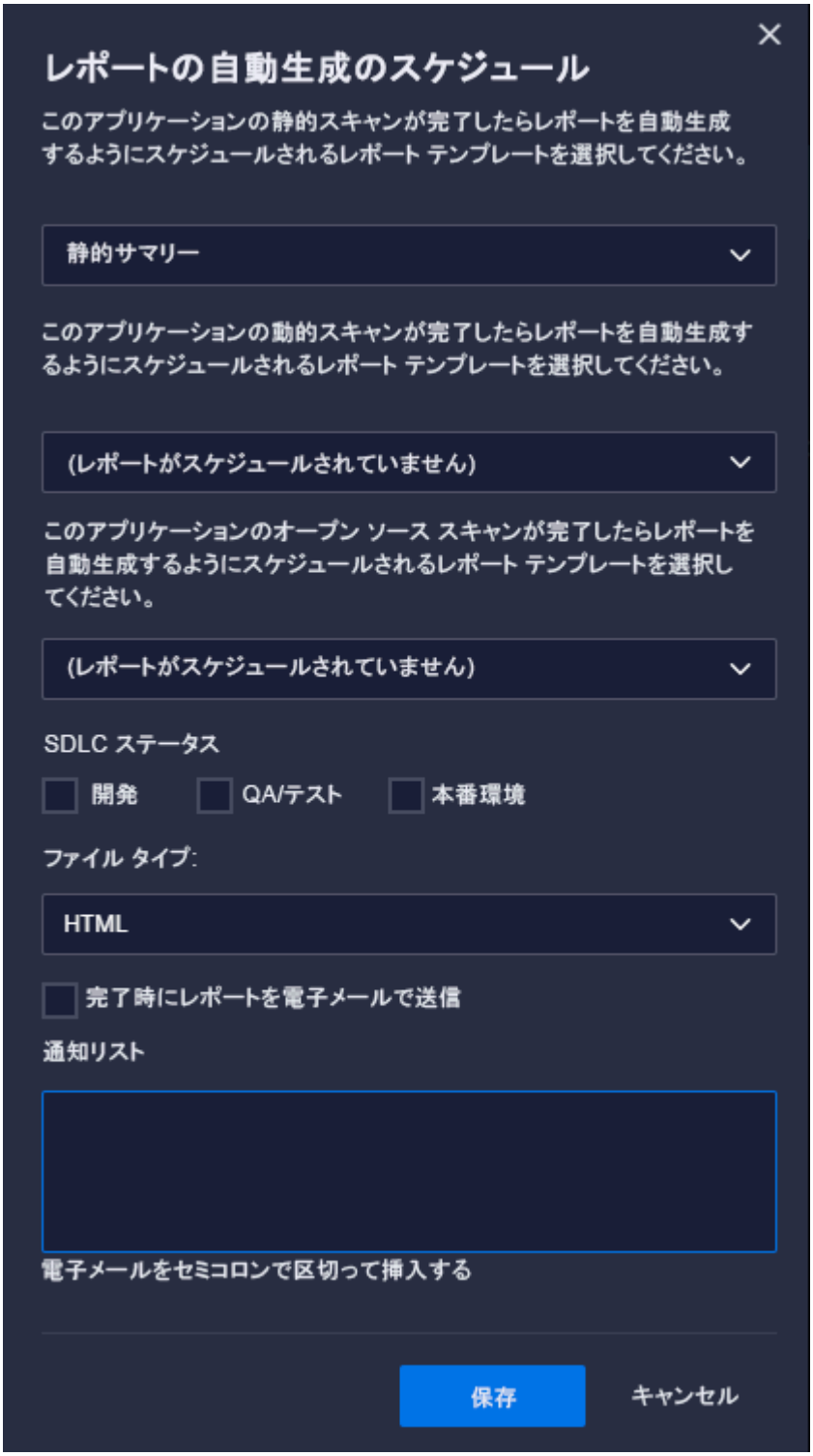


2. 自動生成レポートをスケジュールするアプリケーションの名前をクリックします。
3. [レポート] をクリックします。

   [レポート] ページが表示されます。

4. **[自動レポートのスケジュール]** をクリックします。

[レポートの自動生成のスケジュール] モーダル ウィンドウが表示されます。



5. 静的スキャンの完了時にレポートを生成するために使用するレポート テンプレートを選択します。
6. 動的またはモバイル スキャンの完了時にレポートを生成するために使用するレポート テンプレートを選択します。
7. オープン ソース スキャンの完了時にレポートを生成するために使用するテンプレートを選択します。これは、Debricked スキャンと Sonatype スキャンの両方に適用されます。

8. レポートの生成をトリガーする SDLC ステータスのチェックボックスを選択します。
9. [**ファイル タイプ**] リストからレポートのファイル タイプを選択します。
10. レポートを特定の宛先に自動的に配信するには、[**完了時にレポートを電子メールで送信**] を選択し、[**通知リスト**] フィールドに、レポートの送信先の電子メールアドレスを入力します。
11. [**保存**] をクリックします。

    自動生成レポートの設定が保存されます。

1.7.2.4. テンプレート

テンプレートを表示、作成、編集、削除できるのは、レポートの作成権限を持つユーザーです。

[テンプレート] ページには、既存のレポート テンプレートのリストが、テンプレートを表示、コピー/編集、および削除するためのリンクと共に表示されます。システムとカスタムの 2 種類のレポートテンプレートがあります。

システム レポート テンプレートには、動的、ハイブリッド、モバイルの各レポート用と、PCI、STIG、および FISMA コンプライアンス レポート用のテンプレートがあります。システム テンプレートはコピーおよび抑制できますが、編集または削除することはできません。

OpenText Fortify on Demand では、[**テンプレート ウィザード**] を使用してカスタム レポート テンプレートを作成できます。テンプレートに含めるレポート モジュールやフィルターを構成し、このテンプレートを使用して、組織にとって最も有用な情報を提供するレポートを生成することができます。カスタム レポート テンプレートは編集および削除することができます。

Note

使用例: 高レベルの管理レビュー用に作成されたレポートの場合、そのレポートを読む人がセキュリティ評価の全詳細の確認を必要としないときには、[**静的サマリー**] テンプレートを選択できます。このレポート テンプレートには、分析タイプおよび OWASP の上位 10 件に基づくタイトル ページ、エグゼクティブ サマリー、問題のブレークダウン、問題の一覧が含まれています。PCI レポート、問題の詳細に関するコメント、分析トレース レポートは (追加しない限り) 含まれません。

このセクションでは、次のトピックについて説明します。

- カスタム レポート テンプレートの作成
- カスタム レポート テンプレートの編集
- カスタム レポート テンプレートの削除
- システム レポート テンプレートの抑制

1.7.2.4.1. カスタム レポート テンプレートの作成

カスタム レポート テンプレートを作成するには、レポート テンプレートを新規作成するか、いずれかのシステム テンプレートを基に必要な変更を加えます。

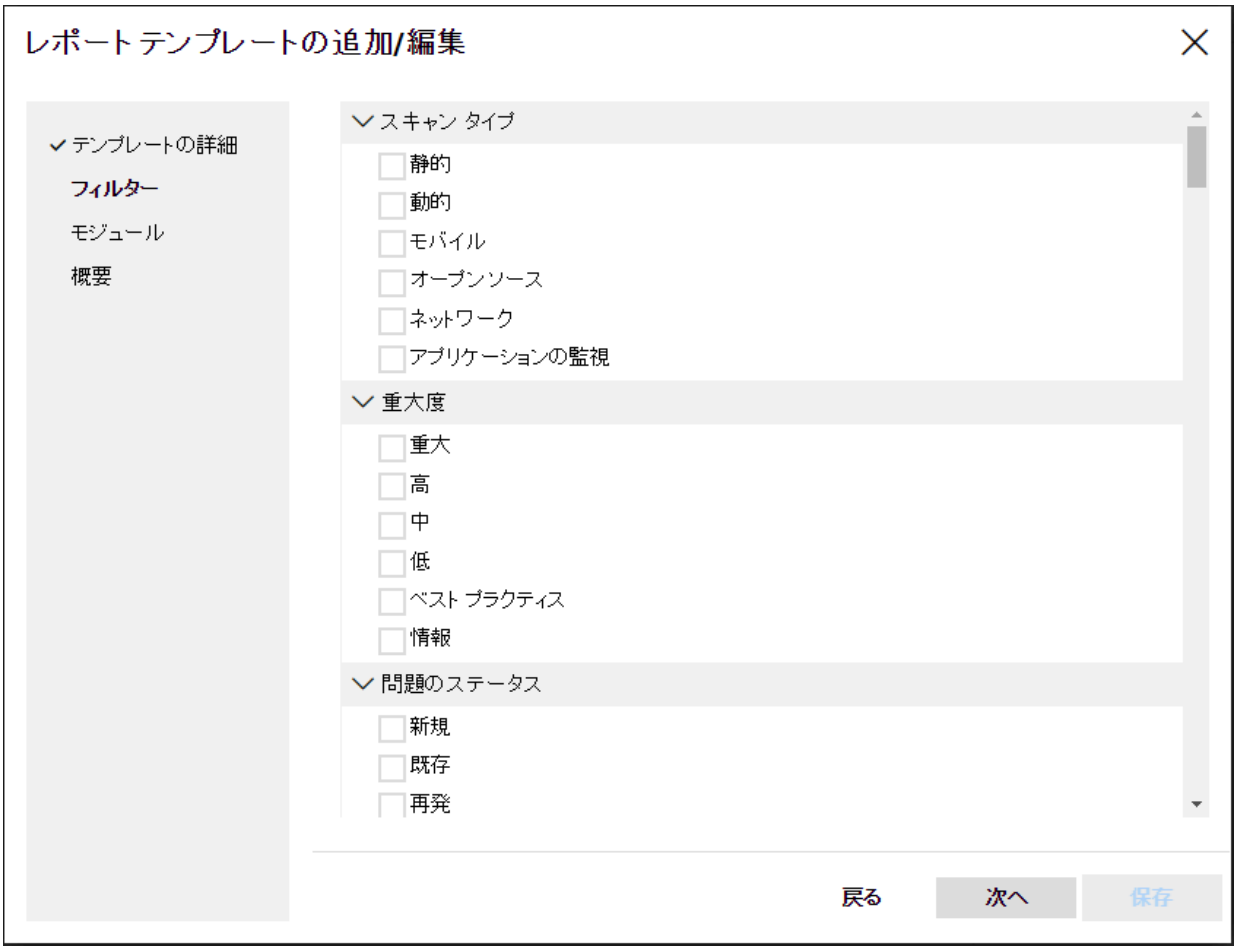
カスタム レポート テンプレートを作成するには、次の手順を実行します。

1. [レポート] ビューを選択します。
2. [テンプレート] アイコンをクリックします。

   [テンプレート] ページが表示されます。
3. 次のいずれかの操作を実行します。
   - [**+新規テンプレート**] をクリックしてテンプレートを新規作成します。
   - 希望のシステム テンプレートの列で アイコンをクリックして、テンプレートのクローンを作成します。

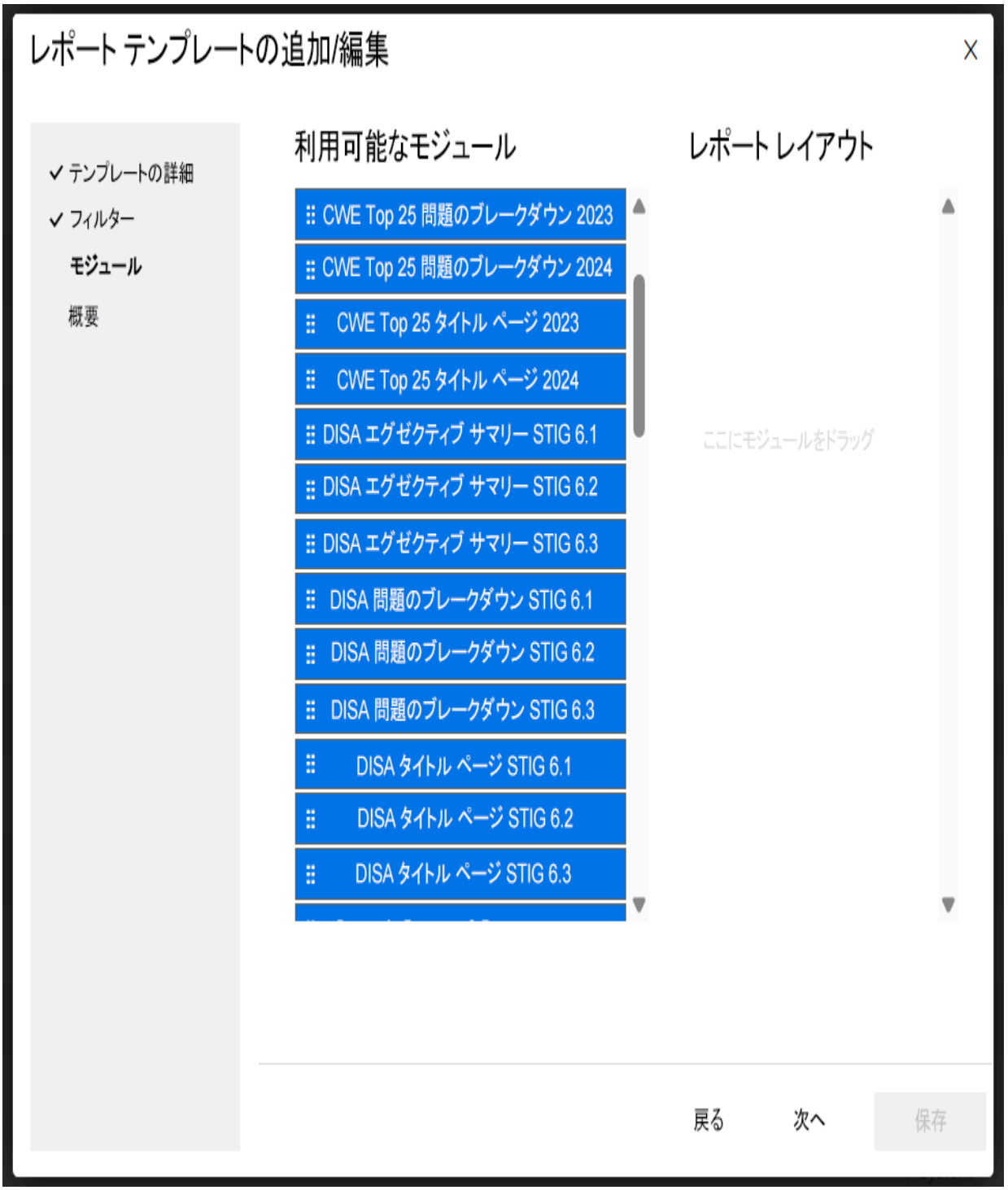
   [レポート テンプレートの追加/編集] ウイザードが表示されます。
4. **テンプレートの詳細**: [**テンプレート名**] フィールドに、新しいテンプレートの名前を入力し、[**次へ**] をクリックします。

5. **フィルター**: 目的のフィルターを選択し、[**次へ**] をクリックします。他に指示がない限り、フィールドは必須です。

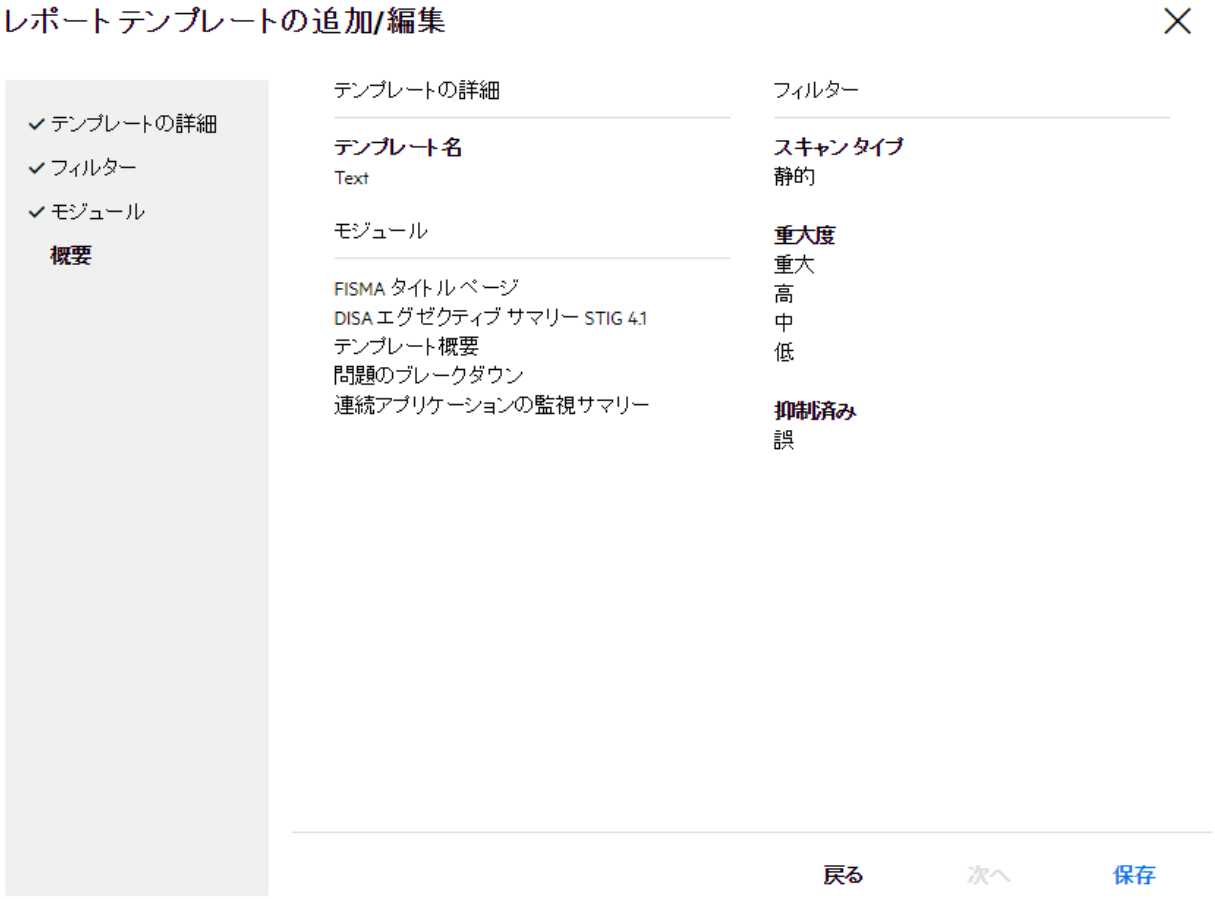

レポート テンプレートの追加/編集
テンプレートの詳細
フィルター
モジュール
概要
スキャン タイプ
静的
動的
モバイル
オープンソース
ネットワーク
アプリケーションの監視
重大度
重大
高
中
低
ベスト プラクティス
情報
問題のステータス
新規
既存
再発
戻る
次へ
保存

フィールド	説明
スキャン タイプ	スキャン タイプ
重大度	(オプション) 問題の重大度
問題のステータス	(オプション) 問題のステータス ([**新規**]、[**既存**]、[**再発**])
開発者ステータス	(オプション) 問題の開発者ステータス
監査担当者ステータス	(オプション) 問題の監査担当者ステータス
問題のエージ	(オプション) 問題が最初に導入された時点からの日数
カテゴリ	(オプション) 問題の脆弱性カテゴリ
抑制済み	(オプション) 問題の抑制ステータス (既定値は [**誤**])
誤検知の再確認	(オプション) 問題の誤検知の再確認ステータス

6. **モジュール**: テンプレートに含めるレポート モジュールを選択し、[**次へ**] をクリックします。
    - 含めるモジュールを [**利用可能なモジュール**] 列から [**レポートのレイアウト**] 列にドラッグします。利用可能なモジュールは、選択したスキャン タイプによって決まります。
    - [**レポートのレイアウト**] 列にアイテムをドラッグ アンド ドロップして、生成されたレポートのモジュールの順序を変更します。



7. **概要**: テンプレートの概要を確認し、[**保存**] をクリックします。



作成したカスタム レポート テンプレートがテンプレートのリストに表示されます。必要に応じて、テンプレートの名前で検索します。

1.7.2.4.2. カスタム レポート テンプレートの編集

[レポート テンプレートの追加/編集] ウィザードを使用して、既存のカスタム レポート テンプレートを編集できます。

カスタム レポート テンプレートを編集するには、次の手順を実行します。

1. [レポート] ビューを選択します。
2. [テンプレート] をクリックします。

   [テンプレート] ページが表示されます。
3. 編集するテンプレートの行の アイコンをクリックします。

   [レポート テンプレートの追加/編集] ウイザードが表示されます。
4. ウィザードの各手順で、必要に応じてフィールドを編集します。詳細については、「カスタム レポート テンプレートの作成」を参照してください。

   Note

   廃止予定のモジュールの削除は永続的で、テンプレートを保存した後に元に戻すことはできません。
5. [**保存**] をクリックします。

   テンプレートの変更が保存されます。

1.7.2.4.3. カスタム レポート テンプレートの削除

テナント内のカスタム レポート テンプレートを削除することができます。

カスタム レポート テンプレートを削除するには、次の手順を実行します。

1. [**レポート**] ビューを選択します。
2. [テンプレート] をクリックします。

   [テンプレート] ページが表示されます。
3. テンプレートのリストから、削除するカスタム テンプレートを見つけます。
4. テンプレートの行の ✕ アイコンをクリックします。

   確認メッセージが表示されます。
5. [**はい**] をクリックしてテンプレートを削除します。

1.7.2.4.4. システム レポート テンプレートの抑制

セキュリティ リーダーはシステム テンプレートを抑制して、レポート生成中にポータルのユーザーがシステム レポート テンプレートを表示または使用できないよう禁止することができます。

1. [レポート] ビューを選択します。
2. [テンプレート] をクリックします。

   [テンプレート] ページが表示されます。
3. 抑制するシステム テンプレートの横にある アイコンをクリックします。

   確認メッセージが表示されます。
4. [**はい**] をクリックして、システム レポート テンプレートの抑制を確認します。

   システム レポート テンプレートが抑制されていると表示されます。 アイコンをクリックして、ポータル内のユーザーに対してシステム レポート テンプレートを復元することができます。

1.7.2.5. データ エクスポート

データ エクスポートは、テナント全体の特定のカテゴリ (アプリケーション、リリース、スキャン、問題、または使用権の消費) に対する関連データの完全なリストです。データ エクスポート権限を持つユーザーは、データ エクスポートを生成できます。データ エクスポートは CSV ファイルとして提供されます。

このセクションでは、次のトピックについて説明します。

- データ エクスポートの表示
- データ エクスポート テンプレートの作成
- データ エクスポートの生成

1.7.2.5.1. データ エクスポートの表示

データ エクスポートを表示するには、次の手順を実行します。

1. [レポート] ビューをクリックします。

   [レポート] ページが表示されます。

2. **[データ エクスポート]** をクリックします。

   [データ エクスポート] ページが表示されます。

次の表に、[データ エクスポート] ページの操作方法を示します。

タスク	アクション
データ エクスポート テンプレートの作成	[**+新規データのエクスポート**] をクリックします。詳細については、「データ エクスポート テンプレートの作成」を参照してください。
既存のテンプレートを使用して、データ エクスポートを生成します。	テンプレートの行で ▷ をクリックします。詳細については、「データ エクスポートの生成」を参照してください。
データ エクスポート テンプレートの編集	テンプレートの行で ✎ をクリックします。
データ エクスポート テンプレートの削除	テンプレートの行で ✕ をクリックします。既存のデータ エクスポートを持つテンプレートは削除できません。
テンプレートに対する生成済みのデータ エクスポートの表示	テンプレートの行にある › をクリックし、テンプレートに対して過去 3 か月に生成されたファイルを表示します。 
データ エクスポートの削除	データ エクスポートの行で ✕ をクリックします。データ エクスポートがまだ実行中の場合は、キャンセルされます。
データ エクスポート ファイルをダウンロードする	データ エクスポートの行で ⤓ をクリックします。

1.7.2.5.2. データ エクスポート テンプレートの作成

データ エクスポートを生成するための基礎としてデータ エクスポート テンプレートが使用されます。フィルターの適用、および反復データ エクスポートのスケジュールが可能です。

データ エクスポート テンプレートを作成するには、次の手順を実行します。

1. [レポート] ビューをクリックします。

   [レポート] ページが表示されます。

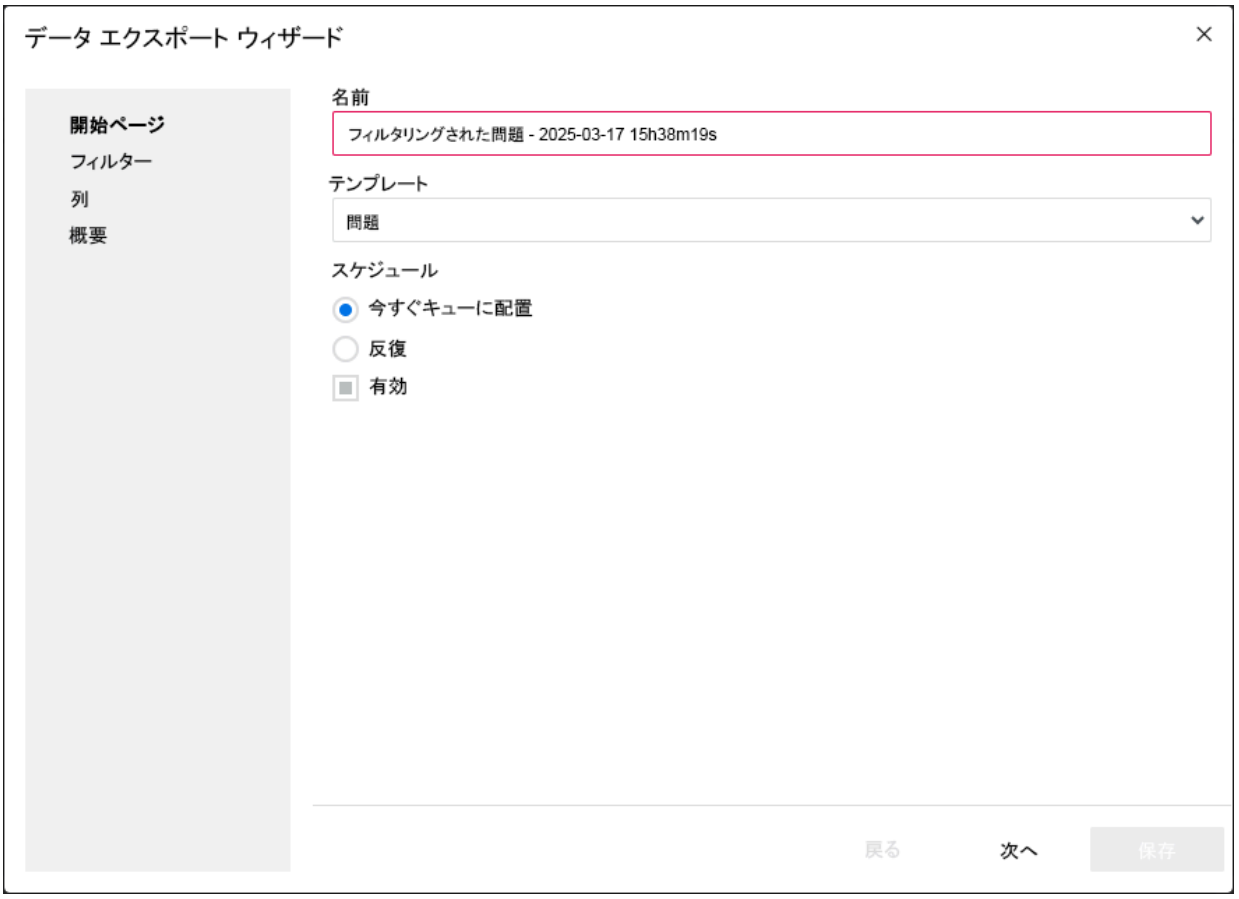
2. **[データ エクスポート]** をクリックします。

   [データ エクスポート] ページが表示されます。

3. **[+新規データのエクスポート]** をクリックします。

   [データ エクスポート ウィザード] が表示されます。

4. **開始ページ**: フィールドをすべて入力して、**[次へ]** をクリックします。

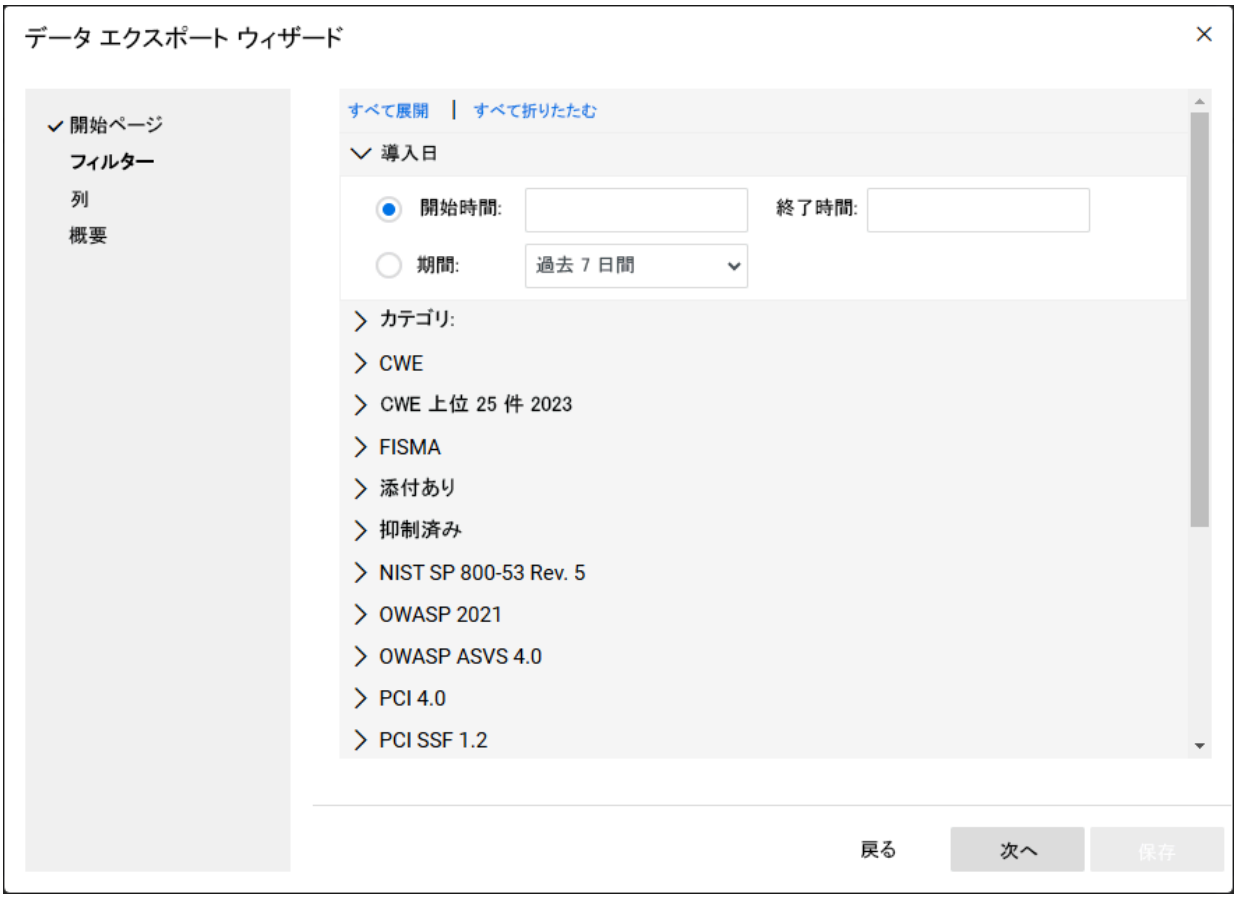

データ エクスポート ウィザード
開始ページ
フィルター
列
概要
名前
フィルタリングされた問題 - 2025-03-17 15h38m19s
テンプレート
問題
スケジュール
今すぐキューに配置
反復
有効
戻る
次へ
保存

フィールド	説明
名前	データ エクスポート テンプレートの名前を入力します。
テンプレート	次の中からデータ エクスポートのテンプレート タイプを選択します。 ◦ **アプリケーション** - アプリケーションのリスト ◦ **アプリケーション リリース** - リリースのリスト ◦ **スキャン** - スキャンのリスト ◦ **問題** - 問題のリスト ◦ **使用権の消費** - 削除済み、キャンセル済み、および進行中のスキャンを含む、使用権が消費されたスキャンのリスト

フィールド	説明
スケジュール	データ エクスポートをスケジュールするためのオプションを次の中から 1 つ選択します。 ◦ **今すぐキューに配置** - データ エクスポートをただちにキューに入れます ◦ **反復** - ウィザードで指定したスケジュールに従ってデータ エクスポートを生成します このオプションが選択されている場合は、[**有効**] チェックボックスを使用できます。スケジュールに従ってデータ エクスポートを自動的に生成するには、このチェックボックスをオンにします (既定)。そうでない場合は、データ エクスポートを手動で生成する必要があります。

5. **フィルター**: 目的のフィルターを選択して、[**次へ**] をクリックします。利用可能なフィルターは、選択したテンプレート タイプによって決まります。


データ エクスポート ウィザード
開始ページ
フィルター
列
概要
すべて展開 | すべて折りたたむ
スキャン開始日
開始時間:
終了時間:
期間:
過去 7 日間
評価タイプ
使用権の種類
修正スキャン
スキャン メソッドのタイプ
スキャン ポリシー
セキュリティ
クラシック
FoD (レガシー)
すべて選択 | すべて選択解除
スキャン ステータス
スキャン タイプ
戻る
次へ
保存



Note

スキャン データ エクスポートには、[**スキャン開始日**] フィルターが必要です。問題データ エクスポートには、[**導入日**] フィルターが必要です。

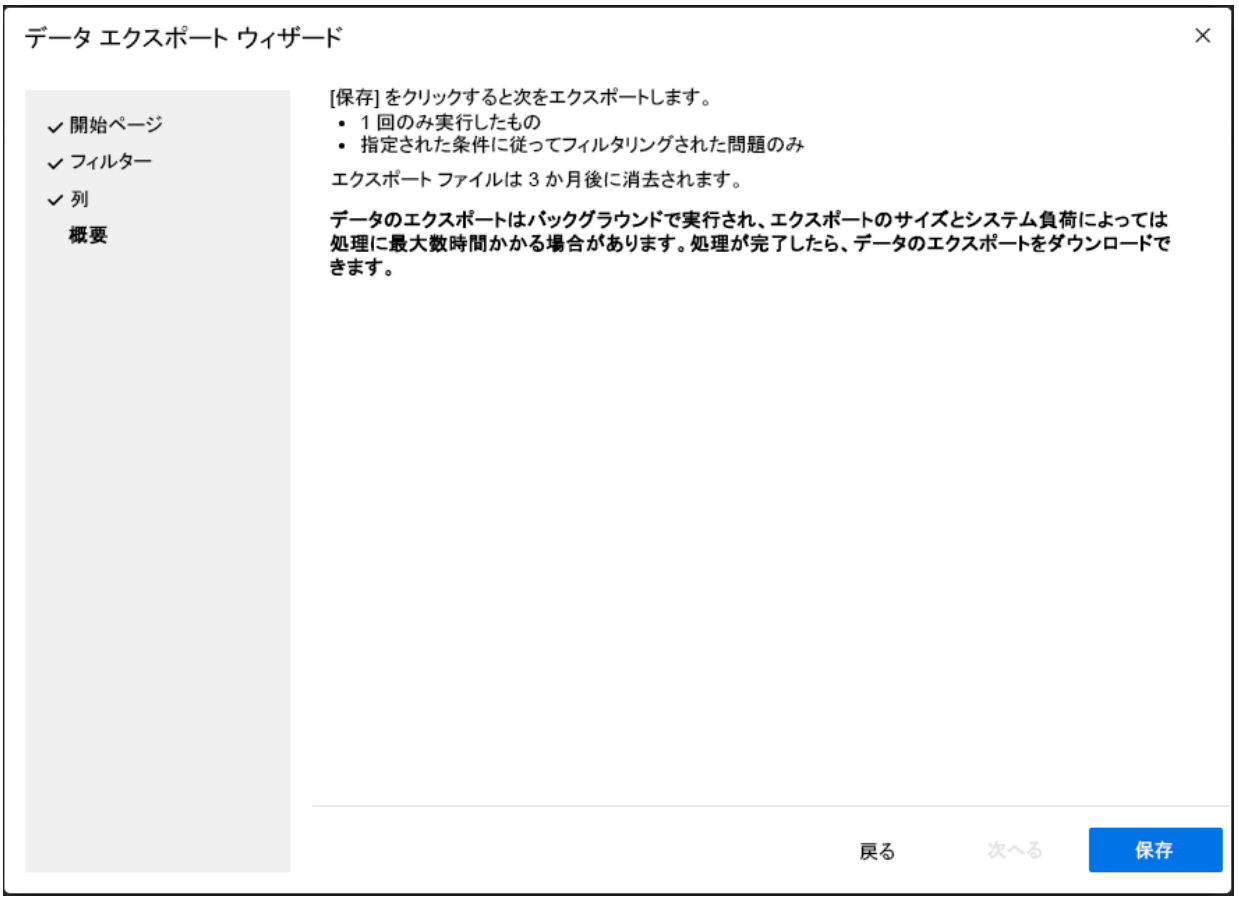
[**開始日**] は、使用権の消費データのエクスポートに必須です。

6. **列** (スキャンと問題データのエクスポートで使用可能): データ エクスポートに含める列を選択し、[**次へ**] をクリックします。

7. **スケジュール** (反復データ エクスポートで使用可能): 繰り返し頻度を選択し、データ エクスポートを生成する曜日または日付を選択します。[**次へ**] をクリックします。

> **Note**
>
> データのエクスポートは、サーバーの時刻が 24:00 のときに実行されます。

8. **概要**: データ エクスポートの概要を確認し、[**保存**] をクリックします。



データ エクスポート テンプレートがデータ エクスポート リストに表示されます。

1.7.2.5.3. データ エクスポートの生成

データ エクスポートを生成するには、既存のデータ エクスポート テンプレートを使用します。

> **Note**
>
> データ エクスポートに含まれるのは、データ エクスポートが生成された時点で完了している評価の結果のみですが、使用権の消費データ エクスポートは例外です。

データ エクスポートを生成するには、次の手順を実行します。

1. [レポート] ビューをクリックします。

   [レポート] ページが表示されます。

2. **[データ エクスポート]** をクリックします。

   [データ エクスポート] ページが表示されます。

3. データ エクスポート テンプレートの行で ▷ をクリックします。

   データ エクスポートがキューに入れられて生成されます。

4. テンプレートの横の ＞ をクリックして、生成されたデータ エクスポートを表示します。

   データ エクスポートが利用可能になるまで「処理中」ステータスが表示されます。

> **Note**
>
> ✕ をクリックして、実行時間の長いデータ エクスポートをキャンセルします。

5. 生成されたら、データ エクスポートの行で ⬇ をクリックします。

   CSV ファイルがブラウザーの設定で指定したフォルダーに保存されます。

1.8. 管理

テナントの管理はポータルから実行されます。アクセス権および権限はユーザー ロールによって決まります。

このセクションでは、次のトピックについて説明します。

- ポータル管理
- ユーザー管理
- ポリシー管理
- シングル サインオン (SSO)
- ベンダー管理

1.8.1. ポータル管理

セキュリティ リーダーは、ポータル設定の構成、セキュリティの構成、管理イベント ログの確認などの、ポータル管理を実行できます。

このセクションでは、次のトピックについて説明します。

- ユーザー セキュリティの構成
- API キーの管理
- 属性の管理
- OpenText Fortify on Demand Connect ネットワークの管理
- 使用権の表示
- 管理イベント ログの表示
- SASTの構成

1.8.1.1. ユーザー セキュリティの構成

セキュリティ リーダーは、次のユーザー セキュリティ設定を構成することができます。

- パスワードのリセット頻度
- パーソナル アクセス トークンの最大有効日数
- 2 要素認証
- IP 制限

> **Note**
>
> IP 制限機能は 24.3 では無効になっています

ユーザー セキュリティ設定を構成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー設定] ページが表示されます。

2. [**設定**] をクリックします。

   [設定] ページが表示されます。

3. [**セキュリティ**] タブを選択します。

4. 必要に応じてフィールドを編集します。

セクション	手順
パスワードの有効期限頻度	新しいパスワードについて、パスワードをリセットする頻度を指定するには、次の手順を実行します。 [**パスワードのリセット頻度**] フィールドで、パスワードのリセットの頻度を指定します。新しい値によって、180 日の既定値が上書きされます。
パーソナル アクセス トークンの最大有効日数	新しい PAT のパーソナル アクセス トークンの最大有効日数を指定するには、次の手順を実行します。 [**パーソナル アクセス トークンの最大有効日数**] フィールドで、パーソナル アクセス トークンの最大有効日数を指定します。新しい値によって、180 日の既定値が上書きされます。

セクション	手順
2 要素認証	2 要素認証を構成して、ユーザー アカウントを保護します。構成が完了した後は、すべてのユーザーは 2 要素認証を使用してログインする必要があります。 2 要素認証を構成するには、次の手順を実行します。 1. [**2 要素認証を有効化**] フィールドで、スライダーを [**いいえ**] から [**はい**] に移動して 2 要素認証を有効にします。 2. ユーザーがログイン コードを受信する方法を、電子メール、SMS、TOTP またはそのすべてから選択します。セキュリティ リーダーによって TOTP が有効にされた後に初めてログインしようとすると、QR コードを含む新しい [Fortify on Demand] ページが表示されます。 3. ユーザーが 2 要素認証コードの入力を求められる頻度を、[**頻度**] リストの [**ログインごと**]、[**4 時間**]、[**8 時間**]、[**12 時間**]、[**24 時間**] から選択します。

セクション	手順
IP 制限	特定の IP アドレスからログインしているユーザーにアクセスを制限することによって、テナントへのアクセスを制限します。 特定の IP アドレスにアクセスを制限するには、次の手順を実行します。 1. [**ログイン制限の有効化**] フィールドで、スライダーを [**いいえ**] から [**はい**] に移動して IP 制限を有効にします。 2. [**任意の IP アドレスからのテクニカル アカウント マネージャー (TAM) のアクセスを許可する**] フィールドで、スライダーを [**いいえ**] から [**はい**] に移動して、TAM による任意の IP アドレスからテナントへのアクセスを許可します。 3. テナントにアクセスできる IP アドレスを管理するには、次のタスクを実行します。

タスク	手順
IP アドレスを許可されたリストに追加する	[**+追加**] をクリックして、IP アドレスの名前 (特殊文字は許可されません) と IP アドレスを入力します。有効な IP アドレス形式は 127.0.0.1、127.0.0.*、および 127.0.0.[0-255] です。

セクション	手順
既存の IP アドレスを許可されたリストから削除する	[**許可された IP アドレス**] リストの IP アドレスの横にある [**x**] をクリックします。

5. [**保存**] をクリックします。

   ユーザー セキュリティ設定が保存されます。

1.8.1.2. API キーの管理

API キーは OpenText Fortify on Demand API への認証に使用されます。セキュリティ リーダーは、API キーを管理できます。

Note

このセクションでは、API キーの管理について説明します。OpenText Fortify on Demand API の使用方法については、「アプリケーション プログラミング インターフェイス (API)」を参照してください。

このセクションでは、次のトピックについて説明します。

- API キーの作成
- API キー ロール
- API キーの編集または削除

1.8.1.2.1. API キーの作成

セキュリティ リーダーは、API キーを作成できます。

API キーを作成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

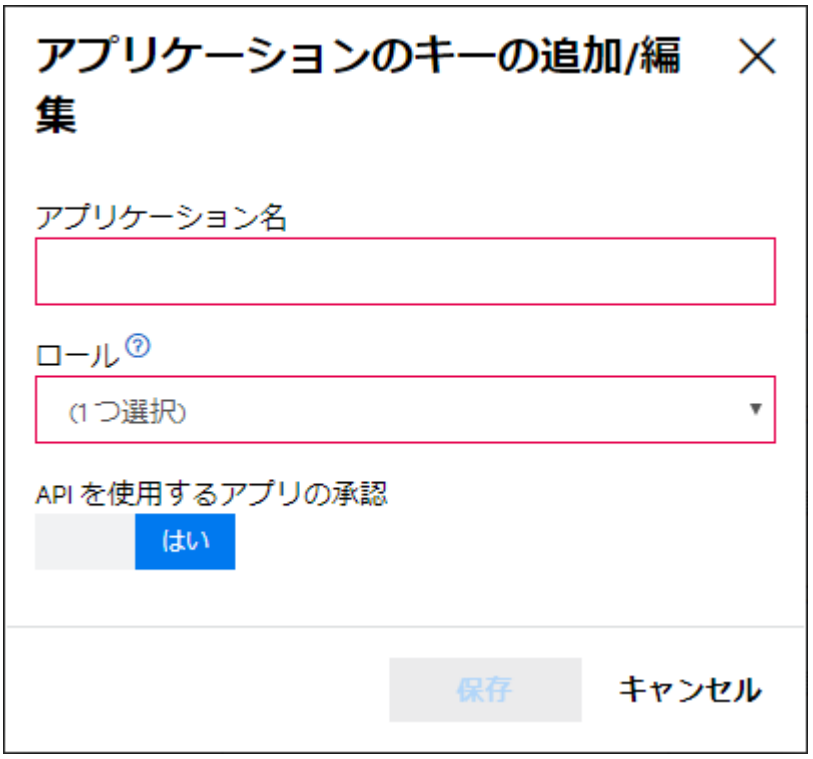
2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. [**API**] タブを選択します。

4. [**+キーの追加**] をクリックします。

   [**アプリケーションのキーの追加/編集**] ウィンドウが開きます。



5. フィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
アプリケーション名	アプリケーションの名前。
ロール	適切な API キー権限を持つロールを選択します。「API キー ロール」を参照してください。
API を使用するアプリの承認	キーを有効にする場合は [**はい**] を選択します。キーが使用されていない場合は、[**いいえ**] を選択してキーを無効にします。

6. [**保存**] をクリックします。

   [シークレット キー] ウィンドウが開きます。

7. Base64 でエンコードされたシークレット コードをコピーします。シークレット コードは 1 回だけ表示されます。

8. [**閉じる**] をクリックします。

   API キー リストに新しい API キーが表示されます。

Note

デフォルトでは、API キーはすべてのアプリケーションにアクセスできます。API キーへのアプリケーションの割り当てについては、「API キーの編集または削除」を参照してください。

1.8.1.2.2. API キー ロール

専用の API キーは、事前設定済みの変更できない権限セットが含まれるロールに関連付けられています。API キーは、テナント内のすべてのアプリケーションへのアクセス権があります。アプリケーションを API キーに割り当てて、アプリケーション アクセスを更新できます。

次の表に、各 API キー ロールに対して設定された権限の一覧を示します。

ロール	権限	使用例
セキュリティ リーダー	すべての権限	すべての AppSec プログラム機能と関連するインフラストラクチャへのフル アクセス権
アプリケーションの管理	サードパーティのアプリを表示、アプリケーションの管理、問題の監査、レポートの作成、静的スキャン/動的スキャン/モバイル スキャンの開始	ユーザー管理機能を除く、フル機能を備えたカスタムまたは内部システムとの統合
スキャンの開始	サードパーティのアプリを表示、アプリケーションの表示、問題の表示、レポートの表示、静的スキャン/動的スキャン/モバイル スキャンの開始	継続的な統合とサーバー構築
読み取り専用	サードパーティのアプリを表示、アプリケーションの表示、問題の表示、レポートの表示	脆弱性管理システムまたは Governance, Risk Management, and Compliance (GRC) システムへのデータ インポート
ユーザー管理	ユーザー ID の表示、ユーザー グループの表示、ユーザー ID の管理、ユーザー グループの管理	ユーザー管理機能を備えた、フル機能を備えたカスタムまたは内部システムとの統合

1.8.1.2.3. API キーの編集または削除

セキュリティ リーダーは、API キーに対して次のタスクを実行できます。

- 新しいシークレットの生成
- API キー設定の編集
- アプリケーションの割り当ておよび割り当て解除

> **Note**
>
> セキュリティ リーダー ロールを持つ API キーには、すべてのアプリケーションへのアクセス権があります。これは変更できません。

- API キーの削除

API キーを変更するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. [**API**] タブを選択します。

4. 次のタスクを実行できます。

タスク	手順
新しいシークレットの生成	1. [**新しいシークレット**] をクリックします。 確認メッセージが表示されます。 2. **[はい]** をクリックします。これによって現在のシークレットは無効になります。
API キー設定の編集	1. [**編集**] をクリックします。 [アプリケーションのキーの追加/編集] ウィンドウが開きます。 2. 必要に応じてフィールドを編集します。
API キーの削除	1. [**削除**] をクリックします。 確認メッセージが表示されます。 2. **[はい]** をクリックします。

タスク	手順
API キーへのアプリケーションの割り当て	1. [**アプリケーションの割り当て**] をクリックします。 2. [**使用可能**] タブを選択します。  3. 次のアクションを実行してアプリケーションを選択します。 ▪ 個々のアプリケーションの横にあるチェック ボックスをオンにします。 ▪ [**割り当て**] チェック ボックスをオンにして、表示されているアプリケーションを選択します。 ▪ [**すべてのテナント アプリケーションの割り当て**] チェック ボックスをオンにして、すべてのアプリケーションを選択します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。 4. [**保存**] をクリックします。

タスク	手順
API キーからのアプリケーションの割り当て解除	1. [**アプリケーションの割り当て**] をクリックします。 2. [**選択済み**] タブを選択します。  3. 次のアクションを実行してアプリケーションを削除します。 ■ 個々のアプリケーションの横にあるチェック ボックスをオフにします。 ■ [**割り当て**] チェック ボックスをオフにして、表示されているアプリケーションを削除します。 ■ [**すべてのテナント アプリケーションの割り当て解除**] チェック ボックスをオンにして、すべてのアプリケーションを削除します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。 4. [**保存**] をクリックします。

1.8.1.3. 属性の管理

属性はアプリケーションに関する追加情報を提供し、これらは、アプリケーション、リリース、マイクロサービス、問題、およびスキャンを追跡するためのフィルターとして使用されます。属性は情報提供目的で使用され、評価プロセスにはまったく影響しません。

セキュリティ リーダーは、属性を追加、編集、および削除することができます。システムレベルの属性は事前に定義されており、削除できません。一部のシステム属性は編集可能です。

次のタイプの属性を使用できます。

- アプリケーションの属性。アプリケーションの属性は、システム属性であり、カスタム属性でもあります。
- マイクロサービスの属性。マイクロサービスの属性はカスタム属性です。
- リリースの属性。リリースの属性はシステム属性です。
- 問題の属性。問題の属性はシステム属性です。次の問題の属性は編集できます: [**監査担当者ステータス (開いた状態)**]、[**監査担当者ステータス (終了済み)**]、[**開発者ステータス (オープン)**]、および [**開発者ステータス (終了済み)**]
- スキャン属性: スキャン属性はカスタム属性です。

このセクションでは、次のトピックについて説明します。

- 属性の追加
- 属性の編集
- 属性の削除

1.8.1.3.1. 属性の追加

セキュリティ リーダーは、マイクロサービスの属性とアプリケーションの属性を追加できます。

属性を追加するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー設定] ページが表示されます。

2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. [**+属性を追加**] をクリックします。

   [属性定義] ウィンドウが表示されます。

4. 次のフィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
名前	新しい属性の名前を指定します。
属性タイプ	属性タイプを選択します。使用可能なオプションは次のとおりです。 ◦ アプリケーション ◦ マイクロサービス ◦ リリース ◦ 問題 ◦ スキャン
データ タイプ	データ タイプを選択します。 ◦ **選択リスト**: この属性タイプでは、リストから値を選択できます。属性の有効な値を定義する必要があります。この値は、その属性のドロップダウン リストとして表示されます。 ◦ **テキスト**: この属性タイプでは、自由形式のテキストを使用できます。これは、チケット番号や各新リリースに固有の他の識別子を割り当てる場合に使用する最適なタイプです。 ◦ **ブーリアン**: この属性タイプでは、バイナリ値 (**正/誤**) を選択できます。 ◦ **日付**: この属性タイプでは、カレンダーから日付を選択できます。 ◦ **ユーザー**: この属性タイプでは、テナントのアクティブなすべてのユーザーのリストからユーザーを選択できます。

フィールド	説明
必須 (オプション)	属性を必須として指定する場合は、このチェック ボックスをオンにします。このフィールドは問題とスキャンの属性には使用できません。
セキュリティ リーダーのみが編集可能 (オプション)	セキュリティ リーダーのみが使用できるようにする場合は、このチェック ボックスをオンにします。このオプションは、[**アプリケーションの管理**] 権限よりも優先されます。 **Note** このオプションを選択すると、属性を必須にすることができなくなります。セキュリティ リーダー以外に対する [**アプリケーションの作成**] 権限が機能しなくなるからです。
Note 以下のフィールドは、[**必須**] と [**セキュリティ リーダーのみが編集可能**] の両方のフィールドが有効になっている場合にのみ適用されます。	
既定値を指定します	選択したデータ型に基づいて既定値を入力します。[**データ タイプ**] が [選択リスト] の場合は、リストから既定値を選択できます。

5. [**保存**] をクリックします。

   新しい属性が属性リストに表示されます。

1.8.1.3.2. 属性の編集

セキュリティ リーダーは、既存の属性の選択リストの値と特定の設定を編集できます。属性名または属性タイプを変更することはできません。

> **Note**
>
> 問題の属性の値は編集できます。[**開発者ステータス (オープン)**] 属性の既定値である [**開いた状態**] および [**修復中**] は編集できません。

属性を編集するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

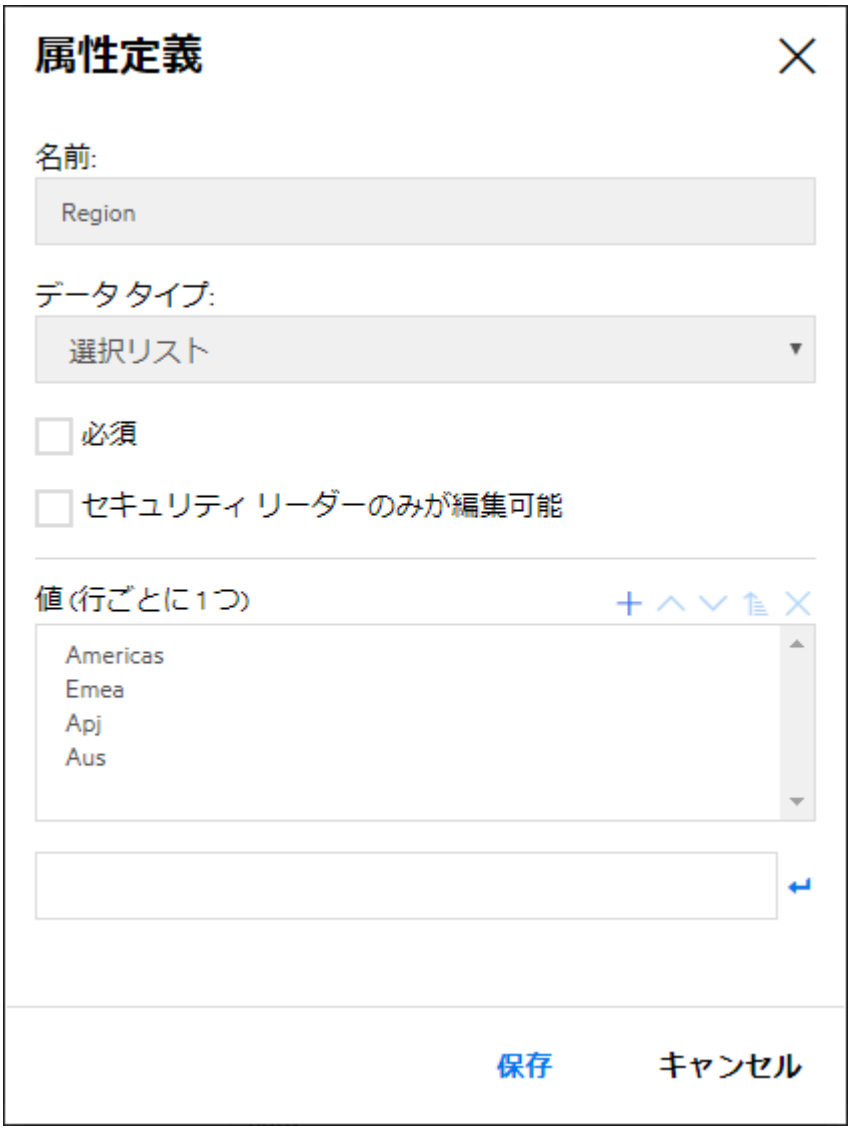
   [ユーザー設定] ページが表示されます。

2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. 編集する属性の行の [**編集**] をクリックします。

   [属性定義] ページが表示されます。



4. 必要に応じてフィールドを編集します。フィールドはデータ タイプによって異なります。

データ タイプ	使用可能なアクション
選択リスト	◦ 新しい値を追加するには ＋ をクリックします。 ◦ リストされた値を並べ替えるには ∧ ∨ を使用します。 ◦ 値をアルファベット順に並べ替えるには をクリックします。 ◦ リストから値を削除するには ✕ をクリックします。
選択リスト、テキスト、ブール値、日付、ユーザー	次のチェック ボックスを選択または選択解除します。 ◦ **必須**: 属性を必要に応じて必須に指定します。 ◦ **セキュリティ リーダーのみが編集可能**: セキュリティ リーダーのみが使用できるようにします。このオプションは、[**アプリケーションの管理**] 権限よりも優先されます。 **Note** このオプションを選択すると、属性を必須にすることができなくなります。セキュリティ リーダー以外に対する [**アプリケーションの作成**] 権限が機能しなくなるからです。

5. [**保存**] をクリックします。

   属性の変更が保存されます。

1.8.1.3.3. 属性の削除

カスタムの属性は削除することができます。システムレベルの属性は削除できません。

属性を削除するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー設定] ページが表示されます。

2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. 編集する属性の行の [**削除**] をクリックします。

   確認メッセージが表示されます。

4. **[はい]** をクリックします。

   属性および関連するすべての値が削除されます。

1.8.1.4. OpenText Fortify on Demand Connect ネットワークの管理

OpenText Fortify on Demand Connect を使用して、動的評価のためのサイト間 VPN を確立します。セキュリティ リーダーは、VPN クライアントを VPN サーバーに登録するために使用される OpenText Fortify on Demand Connect ネットワークを管理できます。

1.8.1.4.1. OpenText Fortify on Demand Connect ネットワークの追加

セキュリティ リーダーは OpenText Fortify on Demand Connect ネットワークを追加できます。このネットワークは、サイト間 VPN 構成で参照されます。

Note

個別の評価用に OpenText Fortify on Demand Connect をセットアップする方法については、「OpenText Fortify on Demand Connect のセットアップ」を参照してください。

OpenText Fortify on Demand Connect ネットワークを追加するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー設定] ページが表示されます。

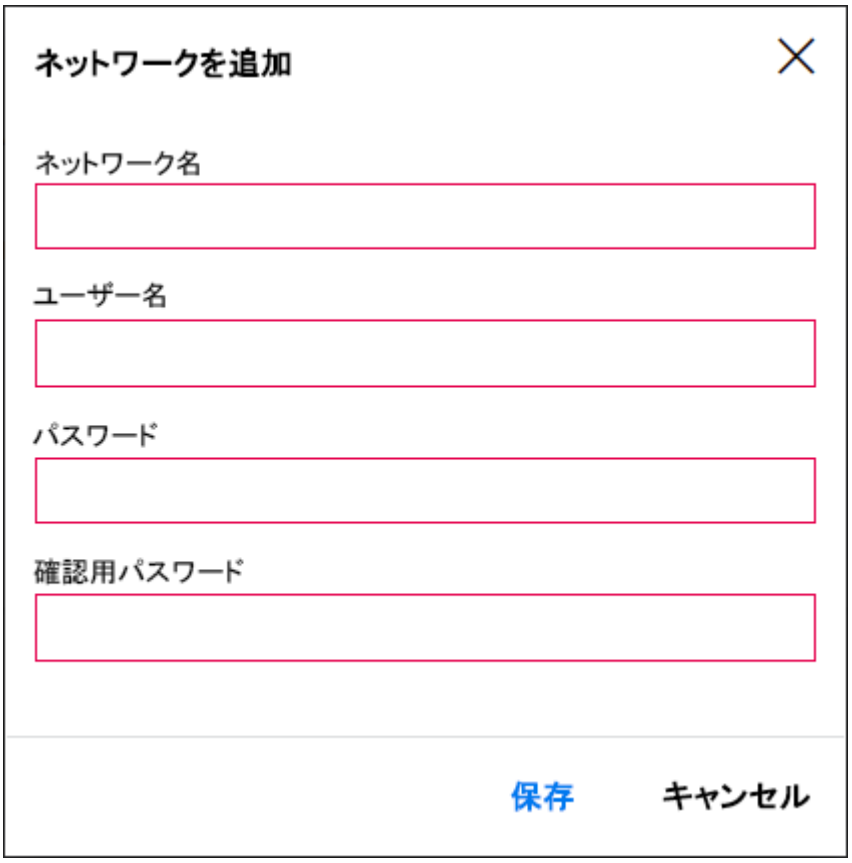
2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. [**OpenText Fortify on Demand Connect**] タブを選択します。

4. [**+ ネットワークを追加**] をクリックします。

   [ネットワークを追加] ウィンドウが表示されます。



5. 次のフィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
ネットワーク名	ネットワーク名を指定します。
ユーザー名	OpenText Fortify on Demand Connect ネットワークのユーザー名を指定します。
パスワード	OpenText Fortify on Demand Connect ネットワークのパスワードを指定します。使用できる文字は、大文字と小文字、および数字です。$ (ドル記号)、` (バッククォート)、\ (バックスラッシュ) を除く特殊文字をエスケープするには、パスワードを二重引用符で囲みます。
確認用パスワード	パスワードをもう一度指定してください。

6. [**保存**] をクリックします。

   ネットワーク リストに新しいネットワークが表示されます。[**Docker コマンドの表示**] リンクを使用できます。ここには、VPN クライアントを実行して VPN クライアントと VPN サーバー間の接続を初期化する Docker コマンドのコードが含まれています。

1.8.1.4.2. OpenText Fortify on Demand Connect ネットワークの削除

セキュリティ リーダーは OpenText Fortify on Demand Connect ネットワークを削除できます。

> **Note**
>
> OpenText Fortify on Demand Connect ネットワークは編集できません。既存のネットワークを更新する必要がある場合は、ネットワークを削除して新しいネットワークを追加する必要があります。

OpenText Fortify on Demand Connect ネットワークを削除するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー設定] ページが表示されます。

2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. [**OpenText Fortify on Demand Connect**] タブを選択します。

4. 削除するネットワークの行の [**削除**] をクリックします。

   確認メッセージが表示されます。

5. **[はい]** をクリックします。

   ネットワークが削除されます。

1.8.1.5. 使用権の表示

セキュリティ リーダーは、テナントの期限切れの使用権とアクティブな使用権のリストを表示できます。

テナントの使用権を表示するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**使用権**] をクリックします。

   [使用権] ページが表示されます。このページには、「使用権 ID」、「使用権の種類」、「分析タイプ」、「購入数量」、「開発者数」、「使用数量」、「開始日」、「終了日」、「リマインダー日」、「説明」、「アクション」などの詳細情報が表示されます。

3. 次のタスクを実行できます。

タスク	手順
使用権の説明の追加または編集	使用権の行の [**編集**] をクリックして、説明を入力します。説明の長さの上限は 50 文字です。
有効期限が切れる使用権に関する電子メール リマインダーの追加または編集	[**リマインダーを編集**] をクリックします。次のフィールドに入力します。 ◦ **1 回目のリマインダー (日数)**: 使用権の有効期限が切れる何日前にリマインダーを送信するかを選択します。 ◦ **2 回目のリマインダー (日数)**: 別のリマインダーを追加する場合は、チェック ボックスをオンにして、使用権の有効期限が切れる何日前にリマインダーを送信するかを選択します。 ◦ **送信先電子メール**: 電子メール アドレスをカンマで区切って指定します。 一度設定すると、リマインダーはテナント内のすべての使用権に適用されます。

1.8.1.6. 管理イベント ログの表示

セキュリティ リーダーは、管理イベント ログを表示できます。管理イベント ログには、アプリケーション関連のすべてのイベントと、次の管理関連のイベントが記録されます。

- ユーザー ログインの成功または失敗、およびユーザー ログアウト
- ユーザーの作成、更新、削除
- グループの作成、更新、削除
- ロールの作成、更新、削除
- ダッシュボードおよびイベント ログのエクスポート
- API キーおよびパーソナル アクセス トークンの作成、更新、削除、新しいシークレットの生成
- API 認証の成功または失敗
- 管理設定および SSO 設定に対する変更

管理イベント ログを表示するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**イベント ログ**] をクリックします。

   [イベント ログ] ページが表示されます。

3. 次のタスクを実行できます。

タスク	アクション
過去 13 か月のイベント ログをエクスポートする	[**エクスポート**] をクリックします。.csv ファイルがブラウザーの設定で指定したフォルダーにローカルに保存されます。
イベント ログを検索する	検索テキスト フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。
フィルター リストを非表示にするか表示する	をクリックします。
フィルターを展開するか折りたたむ	すべて展開 | すべて折りたたむ またはフィルター名の横にある矢印をクリックします。
適用されたフィルターを削除する	ページの上部にある [**X**] をクリックするか、[**フィルターをクリア**] をクリックします。既定では、フィルターは過去 24 時間に設定されています。

関連トピック:

特定のアプリケーションに関連するイベントの表示の詳細については、「アプリケーションのイベント ログの表示」を参照してください。

1.8.1.7. SASTの構成

セキュリティ リーダーは、監査担当者ステータスを構成できるため、顧客が自分で管理できるようにすることができます。

Fortify Remediation Aviator の監査担当者ステータスを構成するには、次の手順を実行します。

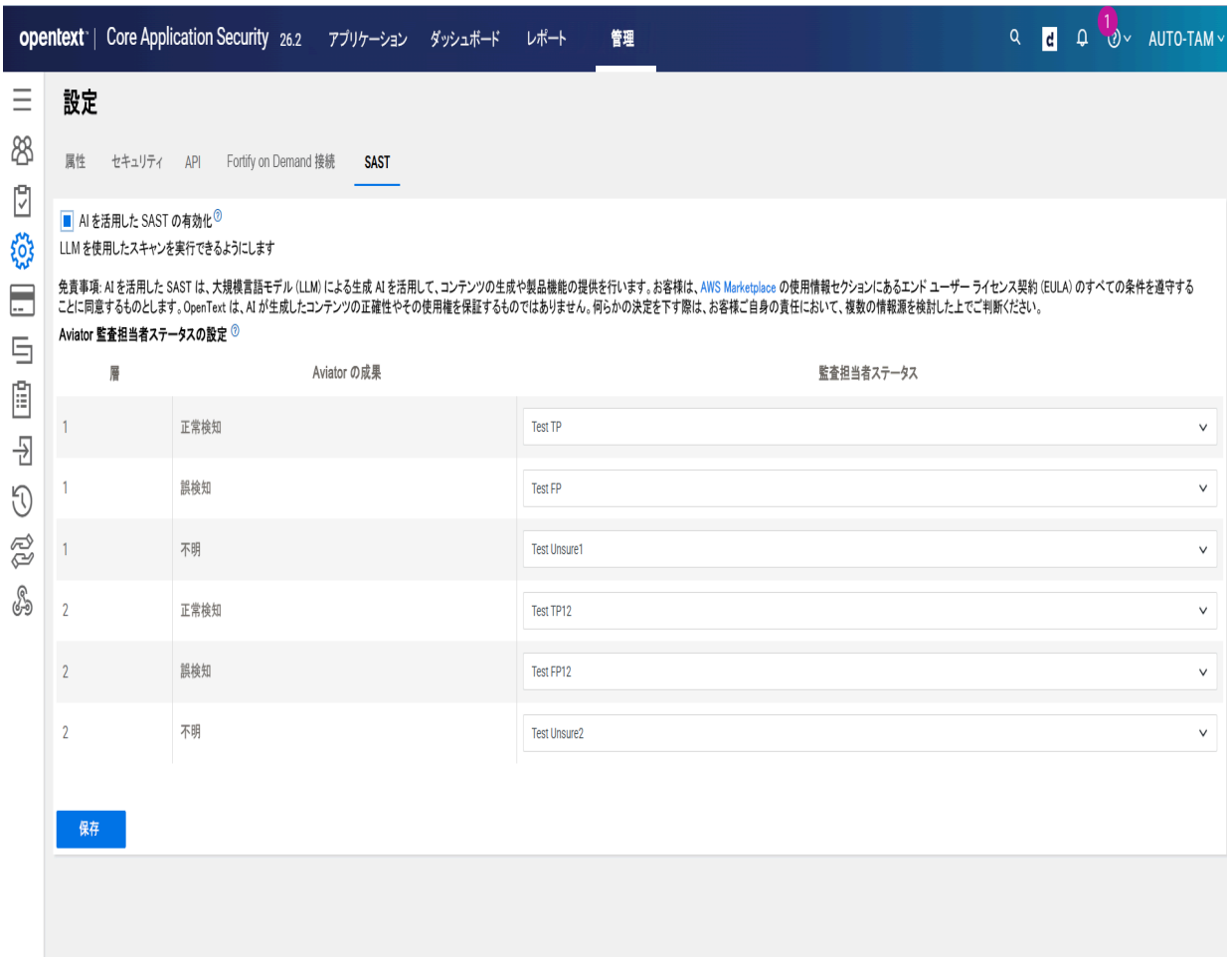
1. [**管理**] ビューを選択します。

   [ユーザー設定] ページが表示されます。

2. [**設定**] をクリックします。

   [設定] ページの [**属性**] タブが表示されます。

3. [**SAST**] タブを選択します。



4. 各フィールドに値を指定します。他に指示がない限り、すべてのフィールドは必須です。

フィールド	説明
AI を活用した SAST の有効化	AI を活用した SAST を有効にするには、このチェックボックスを選択して契約内容に同意します。 SAST は、以下の 12 種類のプログラミング言語向けに、AI を活用したスキャン機能を導入しました。  この機能は、次世代 SAST アーキテクチャに基づいて構築されており、将来のリリースで追加言語をより迅速にオンボーディングすることが可能になります。この機能強化に合わせて、OpenText Fortify on Demand は、新しいアーキテクチャを使用してこれらの言語をスキャンする機能を追加しました。 **Note** 契約内容に同意すると、チェックボックスが選択され、設定がテナントレベルで保存されます。契約内容に同意しない場合、チェックボックスは選択解除されたままになります。

フィールド	説明
Aviator 監査担当者ステータスの設定	
層	Aviator 層を示します。 ◦ 層 1 - Java や .Net などの言語 ◦ 層 2 - その他の言語
Aviator の成果	Aviator の成果を示します。
監査担当者ステータス	Aviator ステータスを選択します。選択されたステータスに基づいて、Aviator は監査担当者ステータスを構成します。

5. [**保存**] をクリックして構成のマッピングを保存します。ポータルで利用可能な任意の監査担当者ステータスに対するマッピングを構成できます。

1.8.2. ユーザー管理

セキュリティ リーダーとユーザー管理権限を持つユーザーは、OpenText Fortify on Demand のユーザーを管理できます。セキュリティ リーダーは、すべてのユーザー管理タスクを実行できます。ユーザー管理権限を持つユーザーは、ユーザー アカウントとグループを管理できますが、ロールを管理することはできません。

このセクションでは、次のトピックについて説明します。

- ロールと権限
- ユーザー
- グループ
- SCIM (System for Cross-domain Identity Management) の構成

1.8.2.1. ロールと権限

OpenText Fortify on Demand のユーザー アクションは、ロールによって制御されます。ロールは、実行可能なアクションを指定する権限のコレクションです。各ユーザーは特定のロールに割り当てられます。セキュリティ リーダーは、ユーザーのロールへの割り当て、ロールの作成、編集、削除など、ロールの管理を実行できます。

6 つの既定のロールを利用できます。組織は、ニーズへの対応を向上させるためにカスタム ロールを定義することもできます。カスタム ロールを使用して、ユーザー ロールを組織内の既存のロールに合わせたり、ユーザーの責任を拡張または制限することができます。小規模組織ではロールの権限を増やし、大規模組織や高度な構造の組織ではロールの権限を制限すると便利です。

このセクションでは、次のトピックについて説明します。

1.8.2.1.1. 権限

ユーザーが実行できるアクションは権限で指定します。OpenText Fortify on Demand権限は、テナント レベルの権限およびアプリケーション レベルの権限という 2 つのタイプに分類されます。

- **テナント レベルの権限**は、ユーザー管理、データのエクスポート、ツールのダウンロードなど、テナント レベルで適用される権限です。テナント レベルの権限の詳細なリストについては、「テナント レベルの権限」を参照してください。
- **アプリケーション レベルの権限**は、アプリケーションの作成、スキャンの開始、問題の編集、レポートの管理など、アプリケーションに適用される権限です。アプリケーション レベルの権限の詳細なリストについては、「アプリケーション レベルの権限」を参照してください。

テナント レベルの権限

次の表に、ロールに対して使用可能なテナント レベルの権限を示します。セキュリティ リーダー ロールに関連付けられている管理を除くテナント レベルの権限は、カスタム ロールに割り当てることができます。

カテゴリ	権限	許可されるアクション
管理	該当なし (セキュリティ リーダーに限定)	• セキュリティ ポリシーの管理 • 属性の管理 • ユーザー セキュリティの構成 • API キーの管理 • Application Defender の構成 • SSO の構成 • 管理イベント ログの表示 • ロールの管理 • グローバル監査テンプレートの管理 • すべてのアプリケーションの静的スキャン ペイロードをダウンロード

カテゴリ	権限	許可されるアクション
アプリケーション アクセス	• **手動** - 既定では、アプリケーションは割り当てられません。アプリケーションは、ユーザーまたはグループに割り当てる必要があります。 [**手動**] が選択されている場合は、[**ユーザー管理**]、[**データのエクスポート**]、[**ベンダー管理**] が [**拒否**] に設定されます。 • **すべて** - すべてのアプリケーションにアクセスできます。テナント レベルの権限に関する制限はありません。	ロールに割り当てられたアプリケーション レベルの権限によって決定されます。
ユーザー管理	**拒否、許可** ([**アプリケーションへのアクセス**] を [**すべて**] に設定する必要があります)	• ユーザーの追加、編集、および削除 (他のセキュリティ リーダーを編集できるのはセキュリティ リーダーのみです) • ユーザー データのエクスポート • グループの管理 • ユーザーへのトレーニング コースの割り当て • トレーニング レポートの表示

カテゴリ	権限	許可されるアクション
データ エクスポート	**拒否**、**許可** ([**アプリケーションへのアクセス**] を [**すべて**] に設定する必要があります)	• [データ エクスポート] タブの表示 • データ エクスポートの作成 • データ エクスポート テンプレートの編集 • データ エクスポート テンプレートの削除 • データ エクスポートの生成 • データ エクスポートのダウンロード • データ エクスポート ファイルの削除
ベンダー管理	**拒否**、**許可** ([**アプリケーションへのアクセス**] を [**すべて**] に設定する必要があります)	• ベンダーの確認および承認 • ベンダーになるための要求 • ベンダーへのレポートの発行
ツールのダウンロード	[**拒否**]、[**許可**]	[ツール] ページの表示
トレーニングへのアクセス	[**拒否**]、[**許可**]	トレーニング コースの受講
サード パーティのアプリの表示	[**拒否**]、[**許可**]	すべてのアプリケーションで使用中のオープン ソース コンポーネントの表示

カテゴリ	権限	許可されるアクション
Web フックの構成	**拒否、許可** ([**アプリケーションへのアクセス**] を [**すべて**] に設定する必要があります)	Web フックの管理
ダッシュボード	**表示、** **作成**	新しいダッシュボードの表示 新しいダッシュボードの管理 (近日公開)

アプリケーション レベルの権限

次の表に、ロールに対して使用可能なアプリケーション レベルの権限を示します。任意のアプリケーション レベルの権限をカスタム ロールに割り当てることができます。

カテゴリ	権限	許可されるアクション
アプリケーション	**表示、管理、作成**	ビュー • 問題、スキャン、およびレポートの表示 • スキャン結果のダウンロード (FPR および SBOM) 管理 • すべての [**表示**] 権限アクション • アプリケーション設定の編集 (アプリケーション名を除く) • アプリケーションに割り当てられたユーザーの表示 • リリースの作成 • リリース設定の編集 • リリースの削除 • アプリケーション イベント ログの表示とエクスポート • スキャン結果のインポート (FPR および SBOM) 作成 • すべての [**管理**] 権限アクション • 新規アプリケーションを作成 • アプリケーション名の編集 • アプリケーションの削除

カテゴリ	権限	許可されるアクション
問題	**表示、編集、監査**	ビュー • スクリーンショットの追加と削除 • 問題のリストのエクスポート 編集 • すべての [**表示**] アクション • [**割り当てられたユーザー**] および [**開発者ステータス**] フィールドの編集、コメントの追加 • バグを送信 監査 • すべての [**編集**] アクション • [**重大度**] および [**監査担当者ステータス**] フィールドの編集 • アプリケーション監査テンプレートの作成と編集

カテゴリ	権限	許可されるアクション
レポート	**表示、作成**	ビュー • メイン レポートの表示 • メイン レポートのダウンロード • ベンダー レポートの表示 • ベンダー レポートのダウンロード • テナント ダッシュボードのエクスポート • リリース ページのエクスポート 作成 • レポートの作成 • レポートの削除 • レポート テンプレートの表示 • レポート テンプレートの作成 • レポート テンプレートの編集
動的スキャンの開始	**[拒否]**、**[構成]**、**[許可]**	構成 • [動的スキャンの設定] ページの編集 許可 • 動的スキャンをスケジュール • 動的スキャンのキャンセル

カテゴリ	権限	許可されるアクション
静的スキャンの開始	[**拒否**]、[**構成**]、[**許可**]	構成 • [静的スキャンの設定] ページの編集 許可 • 静的スキャン ペイロードのアップロード • 静的スキャンのキャンセル • 割り当てられたアプリケーションの静的スキャン ペイロードをダウンロード
モバイル スキャンの開始	[**拒否**]、[**構成**]、[**許可**]	構成 • [モバイル スキャンの設定] ページの編集 許可 • モバイル スキャンのスケジュール • モバイル スキャンのキャンセル
誤検知の再確認の送信	[**拒否**]、[**許可**]	誤検知の再確認を送信する
使用権の使用	[**拒否**]、[**許可**]	スキャンを開始するときの使用権の使用

1.8.2.1.2. 既定のロール

OpenText Fortify on Demand は、6 つの既定のロールで構成されます。既定のロールは、セキュリティ リーダーと開発者のロール以外は編集または削除できます。

- **セキュリティ リーダー** - フル アクセス権。セキュリティ リーダーはすべてのアプリケーションにアクセスでき、アプリケーションおよびリリースの作成、データの処理、問題の監査、レポートの管理など、あらゆるタスクを実行できます。セキュリティ リーダーは管理権限を持つ唯一のロールであり、ロール、セキュリティ ポリシー、およびその他の管理設定を管理できます。
- **開発者** - 制限付きアクセス権。開発者は、ユーザーに割り当てられたアプリケーションにアクセスできます。開発者は、問題データの処理およびレポートの管理を行うことができます。開発者は新規ユーザーの既定のロールです。
- **開発者リーダー** - 中レベルのアクセス権。開発者リーダーは新しいアプリケーションを作成できますが、ユーザーに割り当てられたアプリケーションにしかアクセスできません。開発者リーダーは、問題データの処理、スキャンの開始、およびレポートの管理を行うことができます。
- **アプリケーション リーダー** - 中レベルのアクセス権。アプリケーション リーダーは開発者リーダーと同じアクセス権を持っていますが、それに加え、問題を監査することができます。
- **エグゼクティブ** - 読み取り専用アクセス権。エグゼクティブは、ユーザーに割り当てられたアプリケーションに対する読み取り専用アクセス権を持っています。
- **レビューア** - 読み取り専用アクセス権。レビューアは、すべてのアプリケーションに対する読み取り専用アクセス権を持っています。

次の表に、既定の各ロールに対して設定された権限の一覧を示します。

権限	セキュリティ リーダー	開発者	開発者リーダー (編集可能)	アプリケーションリーダー (編集可能)	エグゼクティブ (編集可能)	レビューア (編集可能)
テナント レベルの権限						
管理	X					
アプリケーションアクセス	すべて	手動	手動	手動	手動	すべて
ユーザー管理	X					
データエクスポート	X					
ベンダー管理	X					
ツールのダウンロード	X	X	X	X		
教育へのアクセス	X	X	X	X	X	X
サードパーティのアプリの表示	X					
Web フックの構成	X					

権限	セキュリティ リーダー	開発者	開発者リーダー (編集可能)	アプリケーション リーダー (編集可能)	エグゼクティブ (編集可能)	レビューア (編集可能)
アプリケーション レベルの権限						
アプリケーション	作成	ビュー	作成	作成	ビュー	ビュー
問題	監査	編集	編集	監査	ビュー	ビュー
レポート	作成	作成	作成	作成	ビュー	ビュー
動的スキャンの開始	開始	拒否	開始	開始	拒否	拒否
静的スキャンの開始	開始	拒否	開始	開始	拒否	拒否
モバイル スキャンの開始	開始	拒否	開始	開始	拒否	拒否
ビルド サーバーの構成	X					
誤検知の再確認の送信	X					
使用権の使用	X	X	X	X	X	X

1.8.2.1.3. ロールの表示

テナントのロールを表示するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**ロール**] タブを選択します。

次の表に、[**ロール**] タブの操作方法を示します。

タスク	アクション
ロール リストを検索する	検索フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。検索結果を削除するには、検索フィールドのテキストを削除して **Enter** キーを押します。
ロールを作成する	[**ロールの追加**] をクリックします。詳細については、「ロールの作成」を参照してください。
ロールに割り当てられたユーザーを表示する	アクション列の [**ユーザーの表示**] をクリックします。
ロールを編集する	アクション列の [**編集**] をクリックします。詳細については、「ロールの編集」を参照してください。
ロールを削除する	アクション列の [**削除**] をクリックします。詳細については、「ロールの削除」を参照してください。

1.8.2.1.4. ロールの作成

ロールを作成するには、次の手順を実行します。

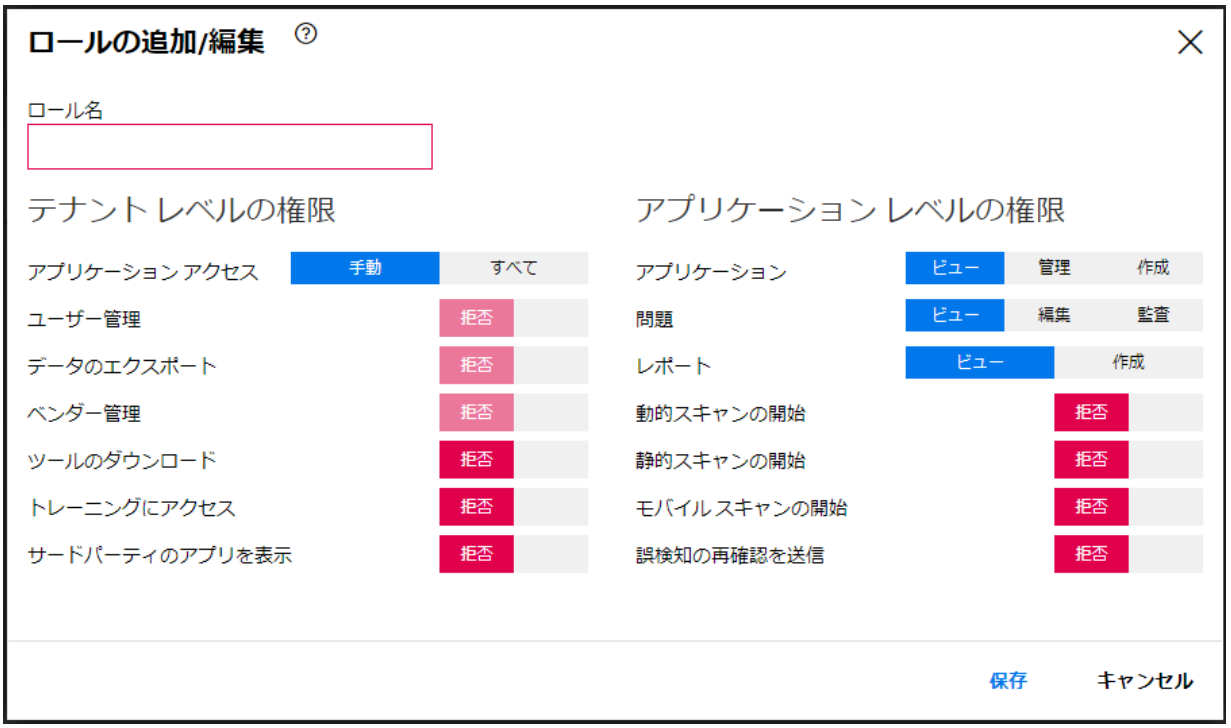
1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**ロール**] タブを選択します。

3. [**+ ロールの追加**] をクリックします。

   [ロールの追加/編集] ウィンドウが表示されます。



4. [**ロール名**] フィールドで、新しいロールの名前を入力します。

5. ロールに対するテナントおよびアプリケーション レベルの権限を選択します。特定の権限の詳細については、「権限」を参照してください。
6. [**保存**] をクリックします。

   新しいロールがロール リストに表示されます。

1.8.2.1.5. ロールの編集

ロールを編集するには、次の手順を実行します。

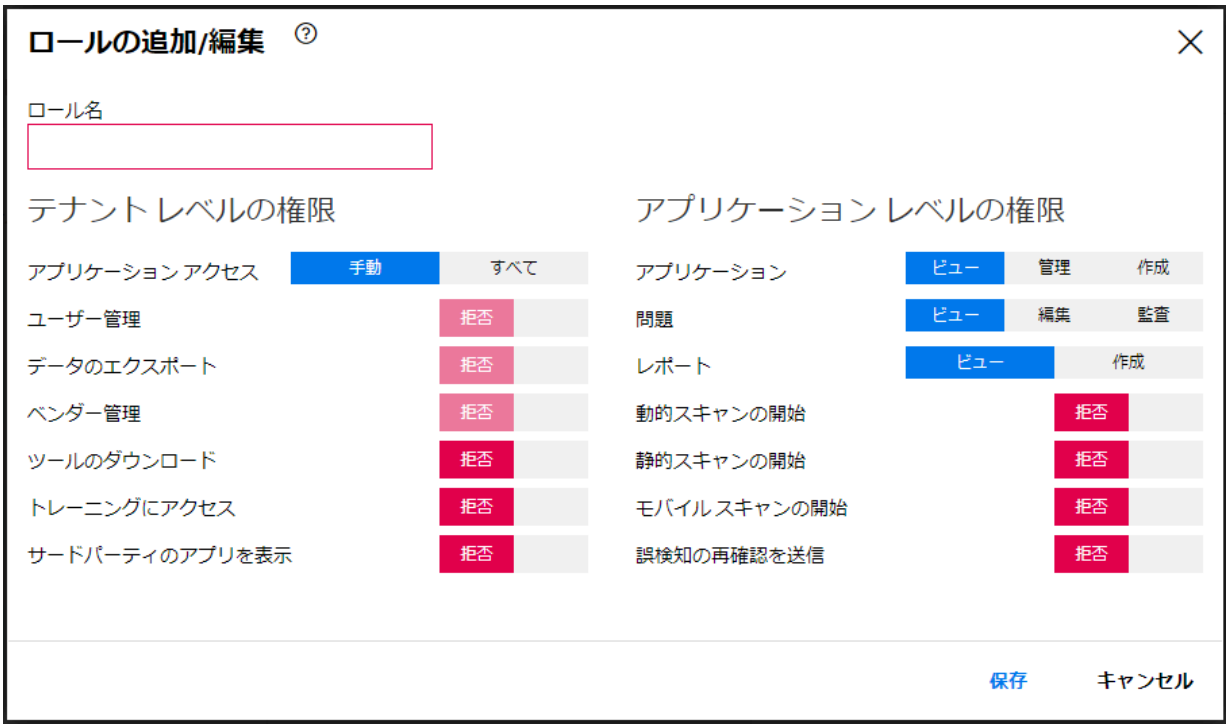
1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**ロール**] タブを選択します。

3. 編集するロールの行の [**編集**] をクリックします。

   [ロールの追加/編集] モーダル ウィンドウが表示されます。



> **Note**
>
> セキュリティ リーダーと開発者ロールの権限セットは編集できません。

4. 必要に応じてフィールドを編集します。
5. [**保存**] をクリックします。

   ロールの変更が保存されます。

1.8.2.1.6. ロールの削除

セキュリティ リーダーおよび開発者のロールと、ユーザーが割り当てられているロールは削除できません。

ロールを削除するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**ロール**] タブを選択します。

3. 削除するロールの行の [**削除**] をクリックします。

   確認メッセージが表示されます。

4. **[はい]** をクリックします。

   ロールが削除されます。

1.8.2.2. ユーザー

ユーザー管理権限を持つユーザーは、ユーザーとグループを管理できます。

このセクションでは、次のトピックについて説明します。

- ユーザーの表示
- ユーザーの作成
- ユーザー アカウントの編集
- ユーザーへのアプリケーション割り当ての管理
- ユーザー アカウントの削除

1.8.2.2.1. ユーザーの表示

テナントのユーザーを表示するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページの [**ユーザー**] タブが表示されます。このタブにはユーザー リストが表示されます。

次の表に、[**ユーザー**] タブの操作方法を示します。

タスク	アクション
[ユーザー] リストを検索する	検索フィールドに単語または語句を入力して、**Enter** キーを押します。検索結果を削除するには、検索フィールドのテキストを削除して **Enter** キーを押します。
ユーザー リストをエクスポートする	[**エクスポート**] をクリックします。すべてのユーザーに関する詳細が含まれる CSV ファイルが、ブラウザーの設定で指定したフォルダーにローカルに保存されます。
ユーザーを追加する	[**ユーザーを追加**] をクリックします。詳細については、「ユーザー アカウントの追加」を参照してください。
ユーザーに割り当てられたアプリケーションを管理する	アクション列の [**アプリケーションの割り当て**] をクリックします。詳細については、「ユーザーのアプリケーション割り当ての管理」を参照してください。
ユーザーに割り当てられたアプリケーションを表示する	アクション列の [**アプリケーションの表示**] をクリックします。
ユーザーを編集する	アクション列の [**編集**] をクリックします。詳細については、「ユーザー アカウントの編集」を参照してください。
ユーザーを削除する	アクション列の [**削除**] をクリックします。詳細については、「ユーザー アカウントの削除」を参照してください。

1.8.2.2.2. ユーザーの作成

ユーザーを作成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページの [**ユーザー**] タブが表示されます。

2. [**+ ユーザーを追加**] をクリックします。

   [ユーザーの追加/編集] ウィンドウが表示されます。

3. 必要に応じてフィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
ユーザー名	一意のユーザー名を入力します。ユーザーの作成後にユーザー名を変更することはできません。
電子メール	ユーザーの電子メール アドレスを入力します。
名前	ユーザーの名を入力します。
姓	ユーザーの姓を入力します。
電話番号	(オプション) ユーザーの電話番号を入力します。ハイフンなどの区切り文字は使用できません。
ロール	ユーザー ロールを選択します (既定のロールは**開発者**)。ユーザー ロールの詳細については、「Role」を参照してください。
パスワードは無期限です	(オプション) パスワードを永続的にするには、チェックボックスをオンにします。
非アクティブ	(オプション) ユーザーを非アクティブとしてマークする場合は、チェックボックスをオンにします。ゆーザーは OpenText Fortify on Demand にログインできなくなります。

4. (オプション) ユーザーを割り当てるグループを選択します。検索ボックスを使用してグループ リストをフィルターすることができます。
5. [**保存**] をクリックします。

   ユーザー リストに新しいユーザーが表示されます。

1.8.2.2.3. ユーザー アカウントの編集

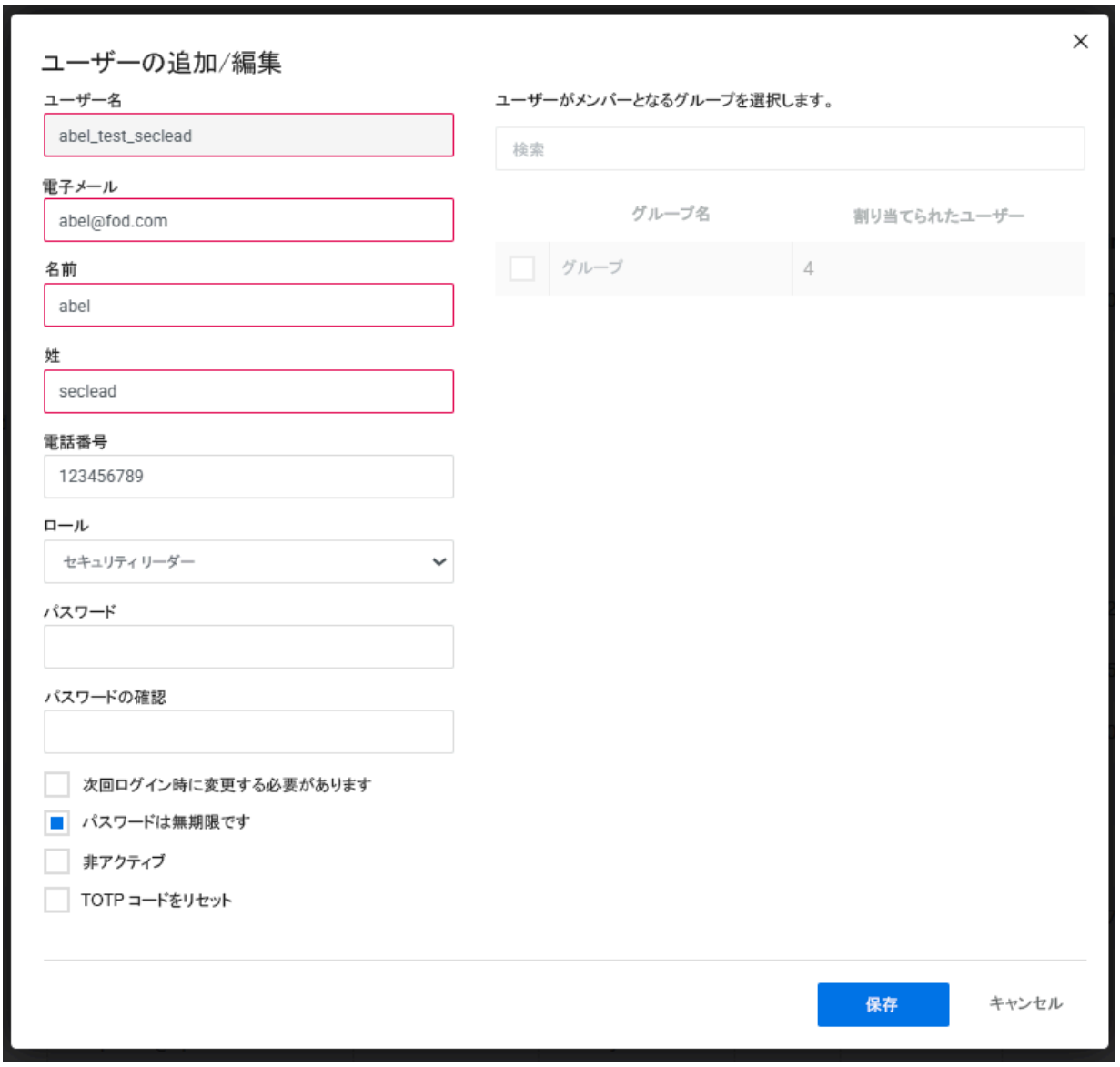
ユーザーパスワードのリセットなど、既存のユーザー アカウントを編集することができます。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページの [**ユーザー**] タブが表示されます。

2. 編集するユーザーの行の [**編集**] をクリックします。

   [ユーザーの追加/編集] ウィンドウが開きます。



3. 必要に応じてフィールドを編集します。次のフィールドはユーザーのパスワードのリセットに使用されます。

4.

フィールド	説明
パスワード	ユーザーの新しいパスワードを入力します。パスワードは複雑さの要件を満たす必要があります。
確認用パスワード	同じパスワードをもう一度入力します。
次回ログイン時に変更する必要があります	ユーザーが次回ログインするときにアカウント パスワードを変更するようにする場合は、チェックボックスをオンにします。
パスワードは無期限です	ユーザー アカウントのパスワードを期限切れにならないようにする場合は、チェックボックスをオンにします。
非アクティブ	ユーザーを非アクティブにする場合は、チェックボックスをオンにします。
TOTP コードのリセット	特定のユーザーの TOTP コードをリセットする場合は、チェックボックスをオンにします。

5. [**保存**] をクリックします。

   ユーザーの変更が保存されます。

1.8.2.2.4. ユーザーへのアプリケーション割り当ての管理

[**ユーザー管理**] 権限を持つユーザーは、[管理] ビューからユーザーへのアプリケーションアクセス権を管理できます。

ユーザーへのアプリケーション アクセス権を管理するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページの [**ユーザー**] タブが表示されます。

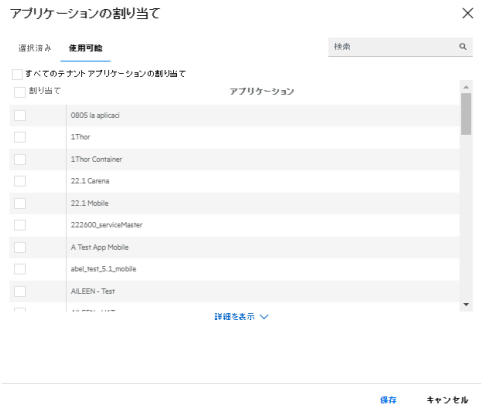
   

2. アプリケーション アクセス権を編集するユーザーの行の [**アプリケーションの割り当て**] をクリックします。

   [アプリケーションの割り当て] ウィンドウが表示されます。

   > **Note**
   >
   > 「**すべてのアプリケーションへのアクセス**」権限を持つロールにユーザーが割り当てられている場合、リンクは使用できません。

3. 次のタスクを実行できます。

タスク	手順
ユーザーへのアプリケーションの割り当て	1. [**使用可能**] タブを選択します。  2. 次のアクションを実行してアプリケーションを選択します。 ▪ 個々のアプリケーションの横にあるチェック ボックスをオンにします。 ▪ [割り当て] チェック ボックスをオンにして、表示されているアプリケーションを選択します。 ▪ [**すべてのテナント アプリケーションの割り当て**] チェック ボックスをオンにして、すべてのアプリケーションを選択します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。

タスク	手順
ユーザーからのアプリケーションの削除	1. [**アプリケーションの割り当て**] をクリックします。 2. [**選択済み**] タブを選択します。  3. 次のアクションを実行してアプリケーションを削除します。 ▪ 個々のアプリケーションの横にあるチェック ボックスをオフにします。 ▪ [**割り当て**] チェック ボックスをオフにして、表示されているアプリケーションを削除します。 ▪ [**すべてのテナント アプリケーションの割り当て解除**] チェック ボックスをオンにして、すべてのアプリケーションを削除します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。

4. [**保存**] をクリックします。

ユーザーに割り当てられたアプリケーションの変更が保存されます。

関連トピック

アプリケーション レベルでアプリケーションへのユーザー アクセス権を管理するには、「アプリケーションのユーザー割り当ての管理」を参照してください。

1.8.2.2.5. ユーザー アカウントの削除

ユーザー アカウントを削除するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページの [**ユーザー**] タブが表示されます。

2. 削除するユーザーの行の [**削除**] をクリックします。

   確認メッセージが表示されます。

3. **[はい]** をクリックします。

   ユーザーが削除されます。

> **Note**
>
> ユーザーが削除されると、参照整合性のために必要な場合を除き、出現するユーザー名、氏名、電子メール、および電話番号は削除され、一意のユーザー ID に置き換えられます。

1.8.2.3. グループ

ユーザーは、アプリケーションを割り当てることができるグループに並べ替えることができます。これにより、アプリケーションの割り当てを効率化することができます。グループは、ビジネス グループ、地域、または他の組織構造について設計することができます。

このセクションでは、次のトピックについて説明します。

- グループの表示
- グループの作成
- グループの編集
- グループのアプリケーション割り当ての管理
- グループの削除

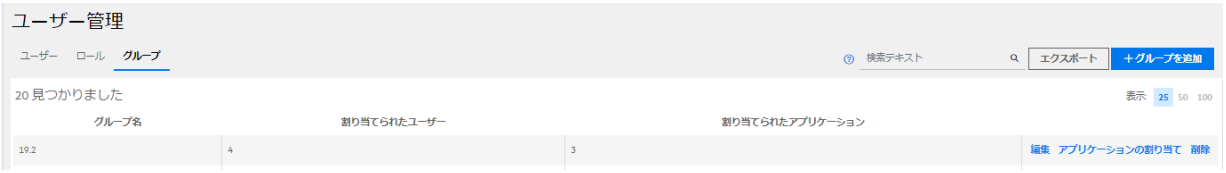
1.8.2.3.1. グループの表示

テナントのグループを表示するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**グループ**] タブを選択します。



次の表に、[**グループ**] タブの操作方法を示します。

タスク	アクション
グループ リストを検索する	検索フィールドにキーワードまたは語句を入力して、**Enter** キーを押します。検索結果を削除するには、検索フィールドのテキストを削除して **Enter** キーを押します。
.csv ファイルとしてデータをエクスポートする	[**エクスポート**] をクリックします。ユーザー グループの詳細が含まれる CSV ファイルが、ブラウザーの設定で指定したフォルダーにローカルに保存されます。
グループを追加する	[**グループを追加**] をクリックします。詳細については、「グループの作成」を参照してください。
グループ名と割り当てられたユーザーを編集する	アクション列の [**編集**] をクリックします。詳細については、「グループの編集」を参照してください。
アプリケーションの割り当ておよび割り当て解除	アクション列の [**アプリケーションの割り当て**] をクリックします。詳細については、「グループのアプリケーション割り当ての管理」を参照してください。
グループを削除する	アクション列の [**削除**] をクリックします。詳細については、「グループの削除」を参照してください。

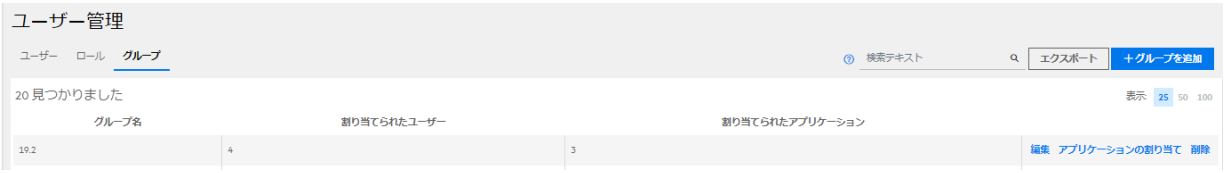
1.8.2.3.2. グループの作成

グループを作成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**グループ**] タブを選択します。



3. [**+ グループを追加**] をクリックします。

   [グループの追加/編集] ウィンドウが表示されます。

4. [**グループ名**] フィールドで、グループの名前を指定します。
5. (オプション) [**グループの説明**] フィールドで、グループの説明を指定します。
6. 次のアクションを実行してアプリケーションを選択できます。
   - 個々のユーザーの横にあるチェック ボックスをオンにします。
   - [**割り当て**] チェック ボックスをオンにして、表示されているユーザーを選択します。

- [**すべてのテナント アプリケーションの割り当て**] チェック ボックスをオンにして、すべてのユーザーを選択します。

7. [**保存**] をクリックします。

   新しいグループがグループ リストに表示されます。

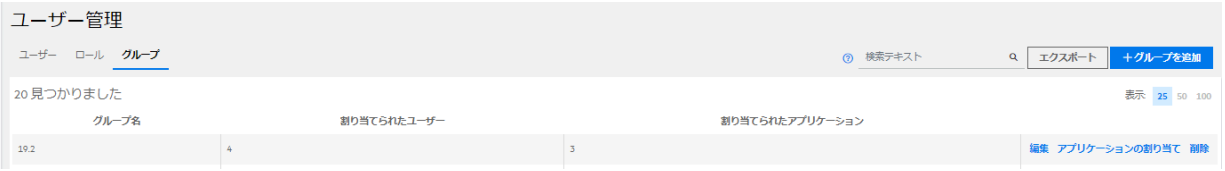
1.8.2.3.3. グループの編集

グループ名を編集したり、グループのユーザー割り当てを管理したりするには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

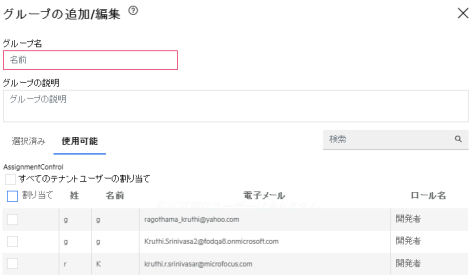
2. [**グループ**] タブを選択します。



3. 編集するグループの行の [**編集**] をクリックします。

   [グループの追加/編集] ウィンドウが表示されます。

4. 次のタスクを実行できます。

タスク	手順
グループ名を編集する	[**グループ名**] フィールドで、グループの新しい名前を入力します。
グループにユーザーを割り当てる	1. [**使用可能**] タブを選択します。  2. 次のアクションを実行してアプリケーションを選択します。 ▪ 個々のユーザーの横にあるチェック ボックスをオンにします。 ▪ [**割り当て**] チェック ボックスをオンにして、表示されているユーザーを選択します。 ▪ [**すべてのテナント ユーザーの割り当て**] チェック ボックスをオンにして、すべてのユーザーを選択します。 検索フィールドを使用して、ユーザーの一覧をフィルターできます。

タスク	手順
グループからユーザーの割り当てを解除する	1. [**選択済み**] タブを選択します。  2. 次のアクションを実行してユーザーを削除します。 ▪ 個々のユーザーの横にあるチェック ボックスをオフにします。 ▪ [**割り当て**] チェック ボックスをオフにして、表示されているユーザーを削除します。 ▪ [**すべてのテナント ユーザーの割り当て解除**] チェック ボックスをオンにして、すべてのユーザーを削除します。 検索フィールドを使用して、ユーザーの一覧をフィルターできます。

5. [**保存**] をクリックします。

   グループの変更が保存されます。

1.8.2.3.4. グループのアプリケーション割り当ての管理

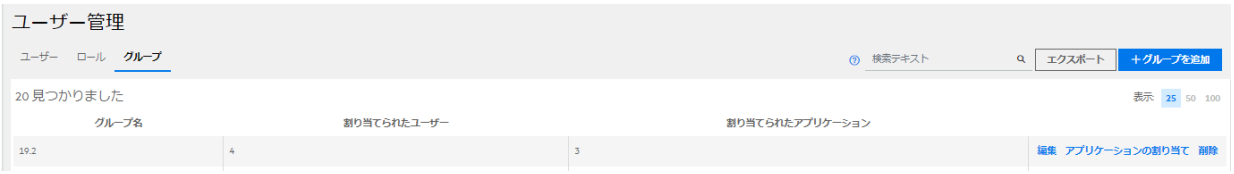
ユーザー管理権限を持つユーザーは、[管理] ビューからグループのアプリケーション割り当てを管理できます。

グループのアプリケーション割り当てを管理するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**グループ**] タブを選択します。



3. アプリケーションを割り当てるグループの行の [**アプリケーションの割り当て**] をクリックします。

   [アプリケーションの割り当て] ウィンドウが表示されます。

4. 次のタスクを実行できます。

タスク	手順
グループにアプリケーションを割り当てる	1. [**アプリケーションの割り当て**] をクリックします。 2. [**使用可能**] タブを選択します。 3. 次のアクションを実行してアプリケーションを選択します。 ▪ 個々のアプリケーションの横にあるチェック ボックスをオンにします。 ▪ [**割り当て**] チェック ボックスをオンにして、表示されているアプリケーションを選択します。 ▪ [**すべてのテナント アプリケーションの割り当て**] チェック ボックスをオンにして、すべてのアプリケーションを選択します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。 4. [**保存**] をクリックします。

タスク	手順
グループからアプリケーションの割り当てを解除する	1. [**アプリケーションの割り当て**] をクリックします。 2. [**選択済み**] タブを選択します。  3. 次のアクションを実行してアプリケーションを削除します。 ▪ 個々のアプリケーションの横にあるチェック ボックスをオフにします。 ▪ [**割り当て**] チェック ボックスをオフにして、表示されているアプリケーションを削除します。 ▪ [**すべてのテナント アプリケーションの割り当て解除**] チェック ボックスをオンにして、すべてのアプリケーションを削除します。 検索フィールドを使用して、アプリケーションの一覧をフィルターできます。 4. [**保存**] をクリックします。

5. [**保存**] をクリックします。

グループに割り当てられたアプリケーションの変更が保存されます。

関連トピック:

同時に複数のグループを割り当てる方法については、「[アプリケーション] ページからのグループのマルチ編集」を参照してください。

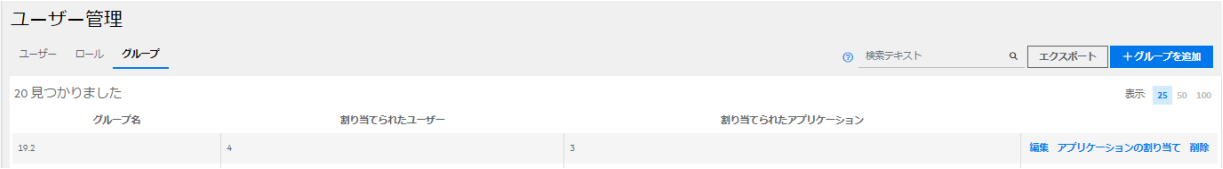
1.8.2.3.5. グループの削除

グループを削除するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**グループ**] タブを選択します。



3. 削除するグループの行の [**削除**] をクリックします。

   確認メッセージが表示されます。

4. **[はい]** をクリックします。

   グループが削除されます。

1.8.2.4. SCIM (System for Cross-domain Identity Management) の構成

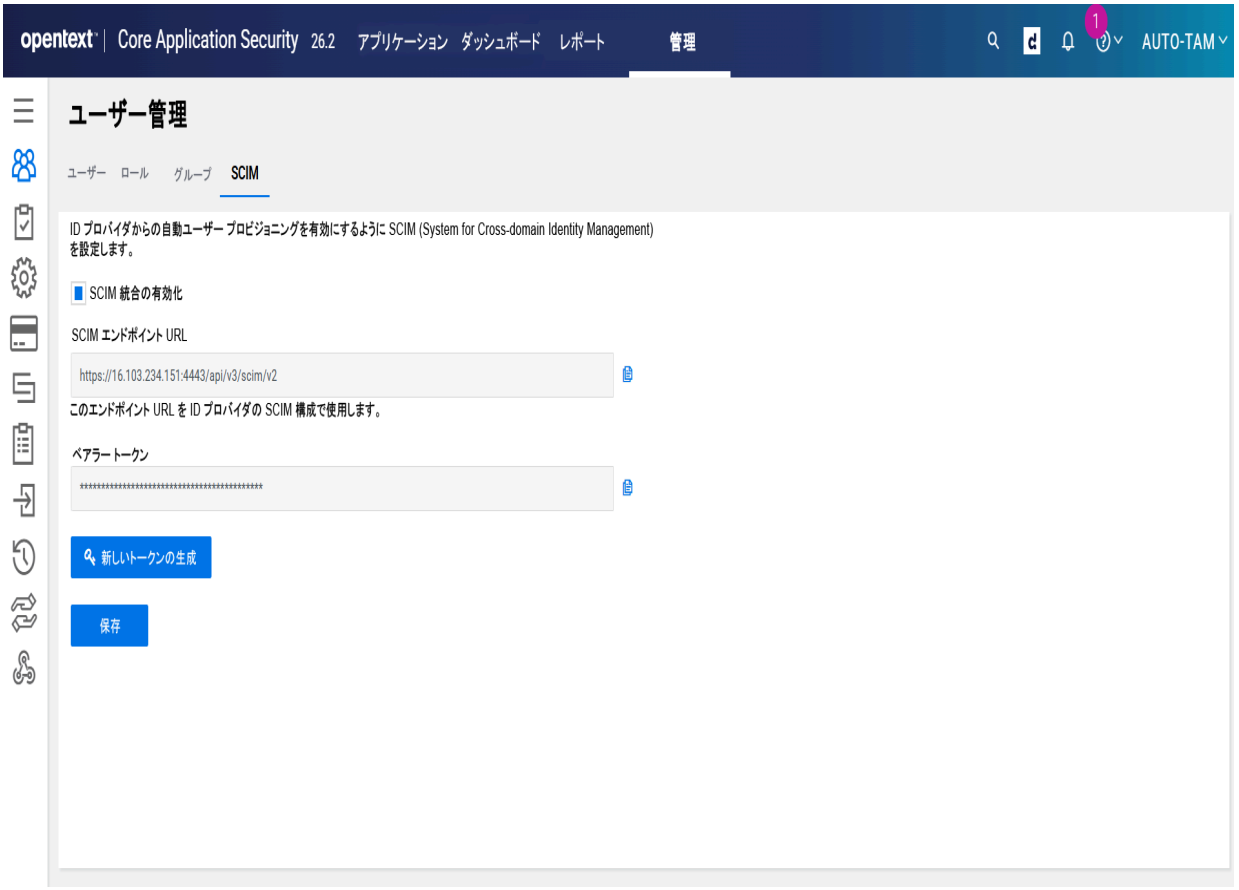
SCIM (System for Cross-domain Identity Management) を構成すると、SCIM 2.0 標準に準拠した、ID プロバイダからのユーザーのプロビジョニングの自動化が可能になります。

SCIM を構成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**SCIM 統合**] タブを選択します。



各フィールドに値を指定します。他に指示がない限り、すべてのフィールドは必須です。

タスク	アクション
SCIM 統合の有効化	初めてトークンを生成する場合は、このチェックボックスを選択します。
SCIM エンドポイント URL	ID プロバイダの SCIM 構成のエンドポイント URL。これは自動的に生成され、編集できません。URL をコピーするには、コピー アイコンをクリックします。
新しいトークンを生成する	トークンを生成するには、[**新しいトークンを生成する**] をクリックします。
ベアラー トークン	生成されたベアラー トークンは暗号化された形式です。このトークンをコピーするには、コピー アイコンをクリックします。
保存	[**保存**] をクリックして設定を保存します。

1.8.3. ポリシー管理

セキュリティ リーダーは、テナント内のアプリケーションにセキュリティ ポリシーが適用される方法を設定できます。また、カスタム セキュリティ ポリシーを作成して管理できます。

このセクションでは、次のトピックについて説明します。

- セキュリティ ポリシーの作成
- セキュリティ ポリシーの設定
- セキュリティ ポリシーの削除

1.8.3.1. セキュリティ ポリシーの作成

カスタム セキュリティ ポリシーを作成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**ポリシー管理**] をクリックします。

   [ポリシー管理] ページの [**スコープ**] タブが表示されます。

3. [**ポリシー**] タブを選択します。

4. [**+ポリシーの追加**] をクリックします。

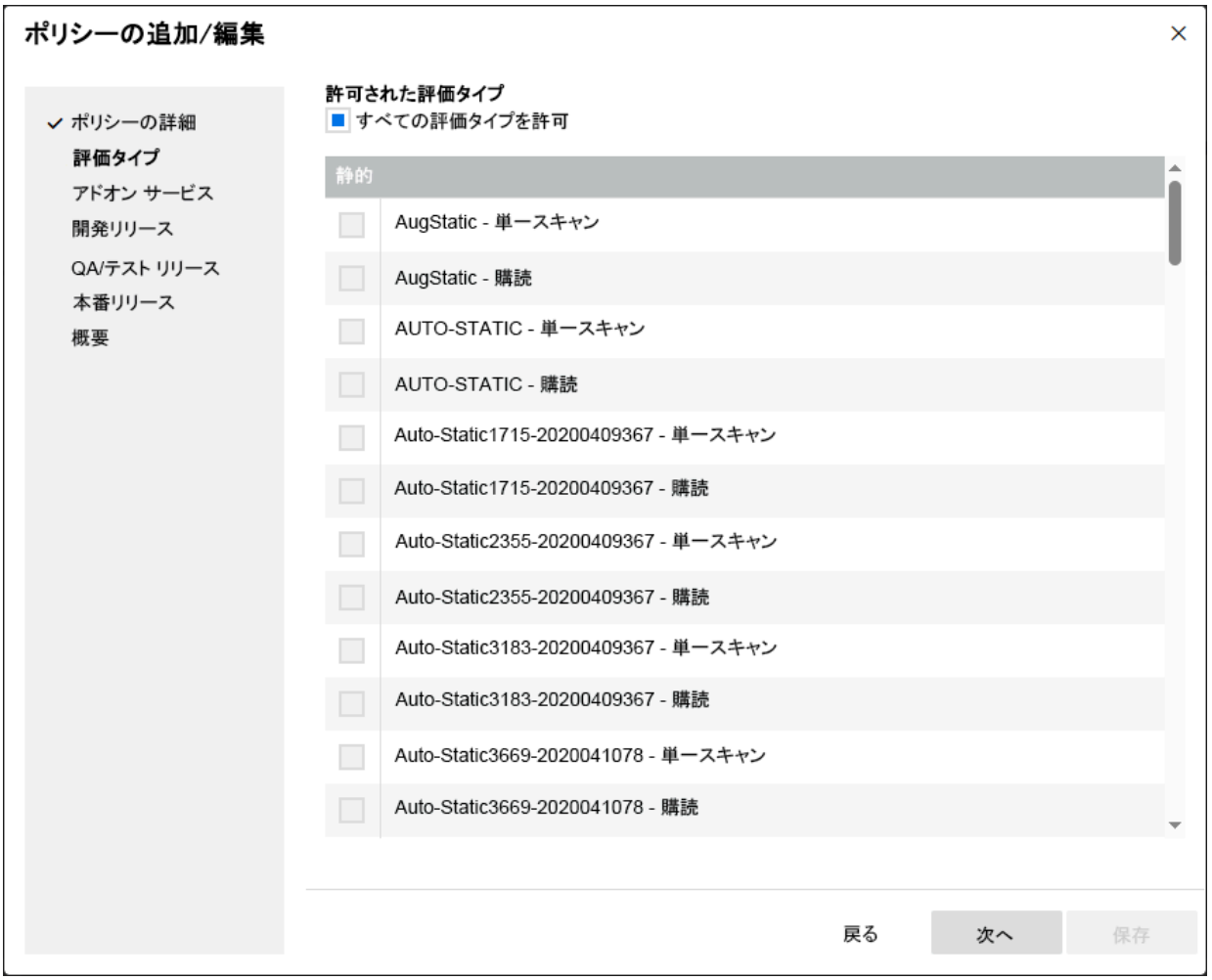
   [**ポリシーの追加/編集**] ウィザードが表示されます。

5. [ポリシーの詳細] ページで、フィールドをすべて入力して [**次へ**] をクリックします。


ポリシーの追加/編集
X
ポリシーの詳細
評価タイプ
アドオン サービス
開発リリース
QA/テスト リリース
本番リリース
概要
ポリシー名
新しいポリシー
星評価
3 つ星以上
コンプライアンス要件
すべての脆弱性カテゴリ
戻る
次へ
保存

フィールド	説明
ポリシー名	ポリシーの名前を入力します。
星評価	合格と判別されるためにアプリケーションが得る必要のある最小の星評価を選択します。星評価については、「5つ星評価」を参照してください。
コンプライアンス要件	アプリケーションの合格/不合格ステータスを決定する際に採用する脆弱性を選択します。すべての脆弱性の既定値を維持するか、OWASP 2021、OWASP 2025、PCI 3.2 などの特別なコンプライアンス要件がタグ付けされている問題のみを含めることができます。 **Note** 合格/不合格ステータスには、オープン ソースの問題が含まれています。

6. [評価タイプ] ページで、ポリシーが適用されているアプリケーションに使用できる評価タイプを選択します。[**すべての評価タイプを許可**] は既定で選択されています。ポリシー作成後に追加されたものを含むすべての評価タイプをセキュリティ ポリシーで許可するには、既定設定のままにしておきます。評価タイプを個別に選択するには、[**すべての評価タイプを許可**] を選択解除します。[**次へ**] をクリックします。



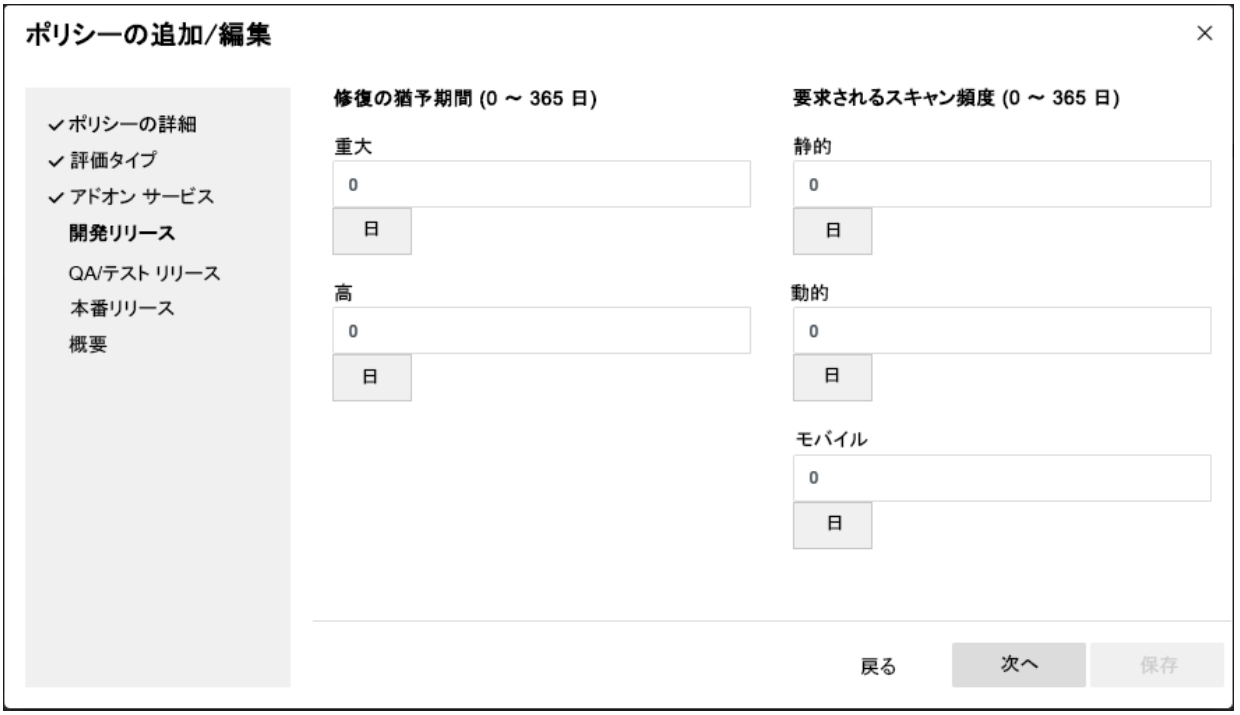
Note

ポリシーの更新が行われたアプリケーションに、現在のポリシーによって許可されていない評価タイプに対応するアクティブなサブスクリプションまたは利用可能な修復がある場合、そのサブスクリプションまたは修復は、有効期限が切れるか使用されるまでは引き続き利用可能です。

7. [アドオン サービス] ページで、ポリシーが適用されているアプリケーションに使用できるアドオン サービスを選択します。ポリシーが適用される前にアドオン サービスが有効になっているアプリケーションには制限は適用されません。

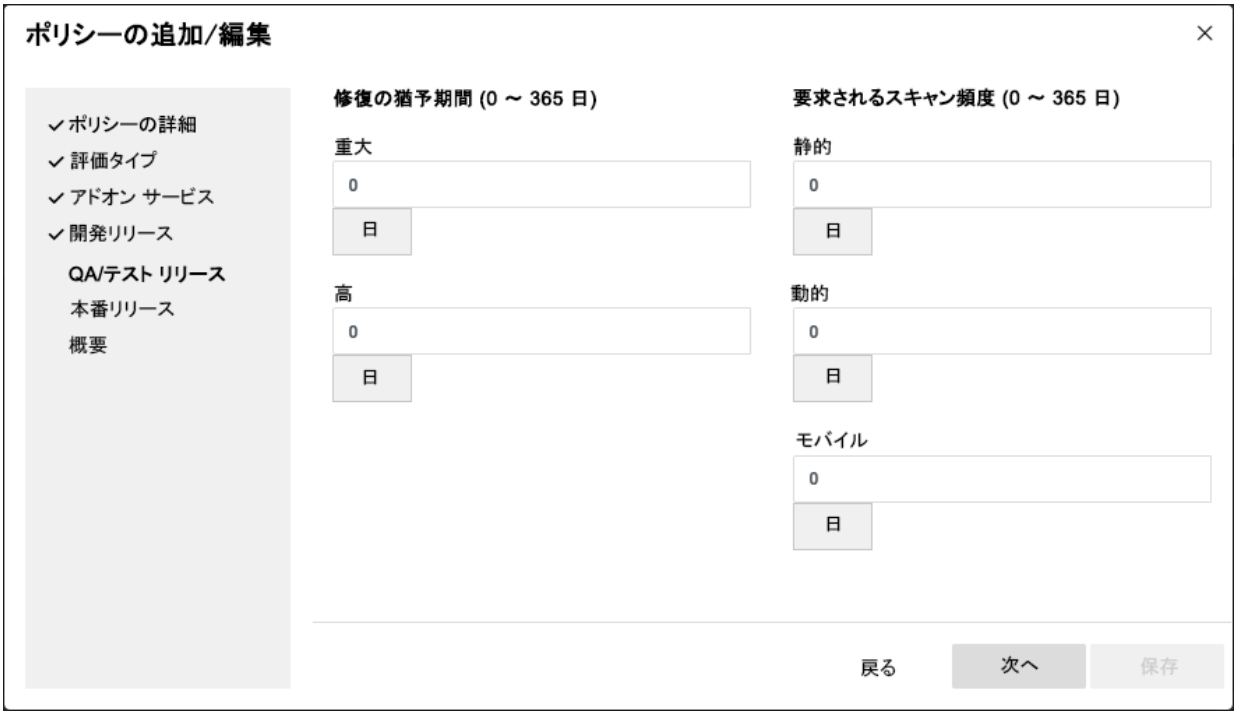
フィールド	説明
Fortify Remediation Aviator を許可	スキャン設定での Fortify Remediation Aviator の選択を許可します。このオプションは、Fortify Remediation Aviator がテナントに対して有効になっている場合は既定で選択されます。有効になっていない場合、このオプションは無効になります。 **Note** ポリシー制限が適用される前に Fortify Remediation Aviator がスキャンで実行された場合、アプリケーションのスキャン設定では、Fortify Remediation Aviator を引き続き選択できます。
DAST 自動アドオンを許可	スキャン設定での DAST 自動アドオンの選択を許可します。このオプションは、DAST 自動評価がテナントに対して有効になっている場合は既定で選択されます。有効になっていない場合、このオプションは無効になります。

8. [開発リリース] ページで、開発ステータス リリースに適用されるフィールドに入力します。[**次へ**] をクリックします。



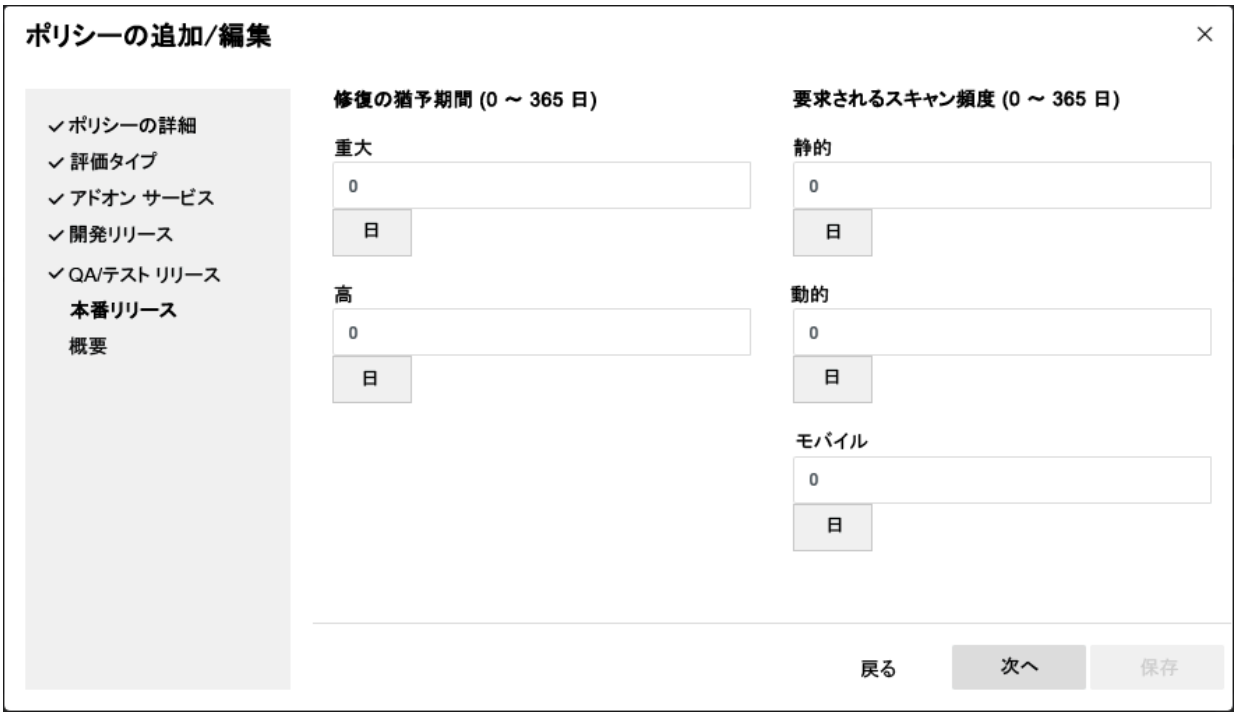
フィールド	説明
修復の猶予期間 (0 ～ 365 日)	問題の重大度レベルごとに、問題の修復猶予期間を指定します。開発リリースで見つかった問題がその猶予期間の範囲内であれば、リリースの合格/不合格ステータスには影響しません。 **Note** 上記で指定した星評価により、表示される問題の重大度レベルが決定されます。
要求されるスキャン頻度 (0 ～ 365 日)	スキャン タイプごとに必要なスキャン頻度を指定します。開発リリースは、スキャン タイプの指定の期間内にスキャンを完了しないと失敗します。値 0 はスキャンが不要であることを意味します。

9. [QA/テスト リリース] ページで、QA/テスト ステータス リリースに適用されるフィールドに入力します。[**次へ**] をクリックします。



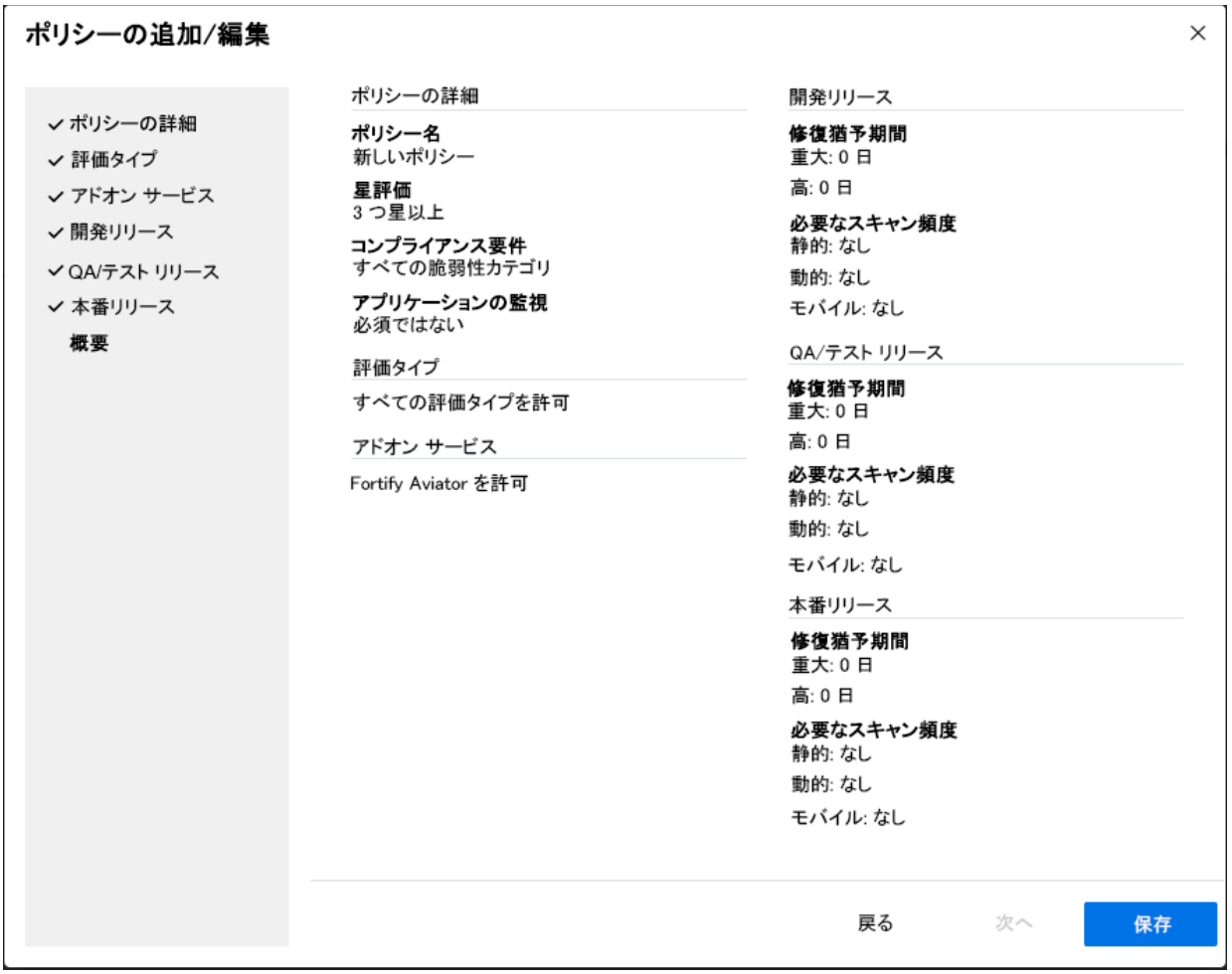
フィールド	説明
修復の猶予期間 (0 ～ 365 日)	問題の重大度レベルごとに、問題の修復猶予期間を指定します。QA/テスト リリースで見つかった問題がその猶予期間の範囲内であれば、リリースの合格/不合格ステータスには影響しません。 **Note** 上記で指定した星評価により、表示される問題の重大度レベルが決定されます。
要求されるスキャン頻度 (0 ～ 365 日)	スキャン タイプごとに必要なスキャン頻度を指定します。QA/テスト リリースは、スキャン タイプの指定の期間内にスキャンを完了しないと失敗します。値 0 はスキャンが不要であることを意味します。

10. [本番リリース] ページで、本番環境ステータス リリースに適用されるフィールドに入力します。[**次へ**] をクリックします。



フィールド	説明
修復の猶予期間 (0 ～ 365 日)	問題の重大度レベルごとに、問題の修復猶予期間を指定します。本番環境リリースで見つかった問題がその猶予期間の範囲内であれば、リリースの合格/不合格ステータスには影響しません。 **Note** 上記で指定した星評価により、表示される問題の重大度レベルが決定されます。
要求されるスキャン頻度 (0 ～ 365 日)	スキャン タイプごとに必要なスキャン頻度を指定します。本番環境リリースは、スキャン タイプの指定の期間内にスキャンを完了しないと失敗します。値 0 はスキャンが不要であることを意味します。

11. [概要] ページで、ポリシーの設定を確認します。[**保存**] をクリックします。



新しいポリシーが [**ポリシー**] タブに表示されます。

関連トピック:

- 合格/不合格設定の手動での上書きについては、「リリースのセキュリティ ポリシーの上書き」を参照してください。

1.8.3.2. セキュリティ ポリシーの設定

テナントのセキュリティ ポリシーを設定するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**ポリシー管理**] をクリックします。

   [**ポリシー管理**] ページの [**ポリシー割り当て**] タブが表示されます。

3. [**編集**] をクリックします。

   [**割り当てスコープの編集**] モーダル ウィンドウが開きます。

4. [**スコープ**] リストからスコープを選択し、ポリシーの適用方法を決定します。テナントごとに 1 つのスコープのみを適用できます。使用可能な値は次のとおりです。

- **ビジネス クリティカリティ**: 割り当てられたビジネス クリティカリティ レベルに従ってアプリケーションをグループ化します。ビジネス クリティカリティ レベルの詳細については、「アプリケーションの作成」を参照してください。
- **アプリケーションの種類**: Web / シック クライアントまたはモバイルとしてアプリケーションをグループ化します。
- **アプリケーションの属性**: [**属性**] リストから選択したアプリケーション属性の値に基づいてアプリケーションをグループ化します。テナントにアプリケーションの属性が作成されていない場合、この値は無効です。

  Note
  選択は値が 10 未満の選択リスト タイプ属性に限定されます。

5. [**保存**] をクリックします。

   [**スコープ**] タブに戻ります。

6. 選択したスコープの各値に割り当てるポリシーを選択します。

7. [**保存**] をクリックします。

   セキュリティ ポリシー設定が保存されます。

1.8.3.3. セキュリティ ポリシーの削除

現在使用されていないカスタム セキュリティ ポリシーを削除できます。OpenText Fortify on Demand のデフォルト ポリシーは編集できますが、削除はできません。

カスタム セキュリティ ポリシーを削除するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**ポリシー管理**] をクリックします。

   [ポリシー管理] ページの [**スコープ**] タブが表示されます。

3. [**ポリシー**] タブを選択します。

4. 削除するポリシーの行の [**削除**] をクリックします。

   確認メッセージが表示されます。

5. **[はい]** をクリックします。

   ポリシーは削除されています。

1.8.4. シングル サインオン (SSO)

シングル サインオン (SSO) を使用すると、OpenText Fortify on Demand の個別の資格情報を管理する必要がなくなり、管理者はユーザー アクセスおよびプロビジョニングをシームレスに管理できます。OpenText Fortify on Demand では、ID フェデレーションのための SAML 2.0 標準を使用して SSO を既存の ID プロバイダーに統合することができます。

OpenText Fortify on Demand は以下の SAML 2.0 バインディングをサポートしています。

- OpenText Fortify on Demand から ID プロバイダーへの SAML 認証要求の POST およびリダイレクト バインディング
- ID プロバイダーから OpenText Fortify on Demand への SAML アサーション応答の POST バインディング

セキュリティ リーダーは、テナントの SSO を構成することができます。SSO の構成は次のタスクから成ります。

- OpenText Fortify on Demand での SSO の構成。方法については、「OpenText Fortify on Demand での SSO の構成」を参照してください。
- OpenText Fortify on Demand への ID プロバイダー メタデータの追加。方法については、「ID プロバイダのメタデータの追加」を参照してください。
- OpenText Fortify on Demand での暗号化の構成。方法については、「暗号化の構成」を参照してください。
- OpenText Fortify on Demand メタデータのダウンロード方法については、「OpenText Fortify on Demand メタデータのダウンロード」を参照してください。
- ID プロバイダでの SSO の構成。方法については、「ID プロバイダでの SSO の構成」を参照してください。

Important
テナントの SSO 設定が変更されるたびに、システムはセキュリティ リーダーに自動的に電子メール通知を送信します。

1.8.4.1. OpenText Fortify on Demand での SSO の構成

OpenText Fortify on Demand SSO 設定を構成し、OpenText Fortify on Demand 属性名を ID プロバイダーの属性名にマッピングします。

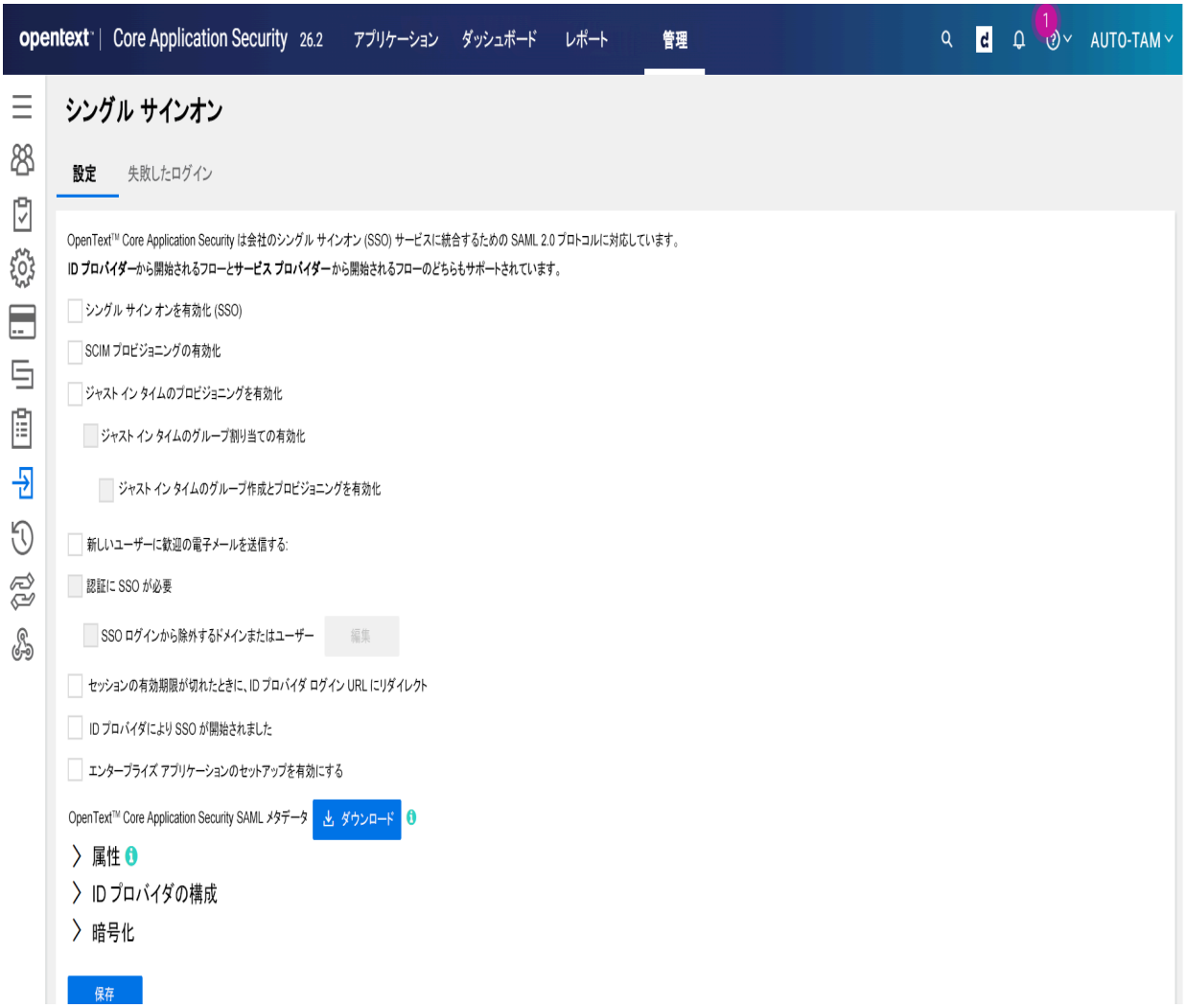
OpenText Fortify on Demand SSO 設定を構成するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**シングル サインオン**] をクリックします。

   [シングル サインオン] ページが表示されます。



3. 必要なオプションのチェックボックスをオンにします。

フィールド	説明	
シングル サイン オンを有効化 (SSO)	このオプションは SSO を有効にします。	
SCIM プロビジョニングの有効化	このオプションを使用すると、SCIM を介してユーザーおよびグループのプロビジョニングを行うことができます。このオプションを選択した場合、SCIMが設定されていないとSSO構成を保存できません。 **Note** **[SCIM プロビジョニングの有効化]** と **[ジャスト イン タイムのプロビジョニングを有効化]** はどちらもオプションですが、互いに排他的です。一度に有効にできるのは 1 つのみです。	
ジャスト イン タイムのプロビジョニングを有効化	ID プロバイダで認証するユーザーの OpenText Fortify on Demand ユーザー アカウントを自動作成または更新します。	

フィールド	説明	
ジャスト イン タイムのグループ割り当てを有効化	[**ジャスト イン タイムのプロビジョニングを有効化**] を選択する必要があります。このオプションにより、ID プロバイを介して OpenText Fortify on Demand ユーザー グループの割り当てを自動更新できます。	
ジャスト イン タイムのグループ作成とプロビジョニングを有効化	[**ジャスト イン タイムのプロビジョニングを有効化**] および [**ジャスト イン タイムのグループ割り当てを有効化**] を選択する必要があります。このオプションにより、既存の ID プロバイダを介して OpenText Fortify on Demand ユーザー グループの割り当てを自動作成できます。	
新しいユーザーに歓迎の電子メールを送信する:	ポータルを介して作成された新しいユーザーには、歓迎の電子メールが送信されます。ただし、歓迎の電子メールには、SSO を通して認証されるユーザーには適用されないパスワード設定手順が含まれます。このオプションが選択されていない場合、新しいユーザーに歓迎の電子メールは送信されません。	

フィールド	説明	
認証に SSO が必要	このオプションでは、すべてのユーザーが SSO を使用する必要があります。このオプションが選択されていない場合、ユーザーは標準のログインページで SSO 認証のユーザー名とパスワードを使用して OpenText Fortify on Demand にログインできます。	

フィールド	説明	
	Note このオプションを有効にすると、OpenText Fortify on Demand Web API を使用する特定のクライアントおよび統合の利用が回避されます。Web API では SAML 認証トークンのサポートが限定されているからです。たとえば、iOS クライアントで OpenText Fortify on Demand に接続するには、SSO 以外の資格情報が必要になります。 . この場合の推奨アプロ—チは、SSO 以外の認証用の	

フィールド	説明	
	「パーソナル アクセス トークン (personal access token)」として使用できる強力なランダム パスワード (32 文字以上) を生成することです。 ◦ **SSOログインから除外するドメインまたはユーザー**: このオプションを使用すると、SSO ログインから除外するドメインまたはユーザーのリストを追加できます。[**編集**] をクリックして SSO ログインから除外するドメイン名または電子メール ID を指定します。ドメイン名または電子メール ID を追加したら、[**保存**] をクリックして変更を保存します。	

フィールド	説明	
	Note **[認証に SSO が必要]** が選択されていない場合、このオプションは無効になります。	
セッションの有効期限が切れたときに、ID プロバイダ ログイン URL にリダイレクト	このオプションは、セッションが期限切れになった後またはユーザーがログアウトしたときに、ユーザーを ID プロバイダのログイン ページにリダイレクトします。この機能を使用するには、ブラウザーおよび直近 30 日以内のユーザー ログイン セッションに対して Cookie が有効になっている必要があります。	

フィールド	説明	
ID プロバイダにより SSO が開始されました	サービス プロバイダーが開始する SAML 認証フローと、ID プロバイダーが開始する SAML 認証フローの両方がサポートされています。 ◦ (推奨) このオプションが選択されていない場合は、サービス プロバイダー フローが使用されます。ユーザーは、このページで提供される SSO ログイン URL を使用して OpenText Fortify on Demand にログインします。OpenText Fortify on Demand は次にサービス プロバイダーから開始される ID プロバイダーへのユーザー認証要求を行います。 ◦ このオプションが選択されている場合、ID プロバイダーから開始されるフローが使用されます。ユーザーは ID プロバイダーに直接接続してログインし、認証成功後に OpenText Fortify on Demand にリダイレクトされます。	

フィールド	説明	

フィールド	説明	
エンタープライズ アプリケーションのセットアップを有効にする	組織に複数のテナントがある場合、このオプションにより、単一の ID プロバイダを介した認証が有効になります。	

フィールド	説明	
	Note このオプションを選択し、既存の SSO 構成がある場合は、更新された OpenText Fortify on Demand メタデータをダウンロードして ID プロバイダにインポートし、ID プロバイダのメタデータを OpenText Fortify on Demand に再インポートする必要があります。または、`?t=<sso_login_url_guid>` を、OpenText Fortify on Demand SSO 設定の **ID プロバイダ名**と ID プロバイダ設	

フィールド	説明	
	定のサービス プロバイダ名の両方に追加することもできます。`<sso_login_url_guid>` は SSO ログイン URL 内にある一意の識別子です。	

4. [**属性**] セクションで、OpenText Fortify on Demand によって予期される属性名を、ID プロバイダーで構成された属性名にマッピングします。ここで定義される各属性名は、ID プロバイダーで使用される属性の正確な「**Name**」値と一致していなければなりません。この属性名は、完全スキーム URL として定義されることがよくあります。属性のより短い「**FriendlyName**」値を送信する ID プロバイダーもあり、この値も属性マッピングで使用できます。各属性の説明については、「ID プロバイダの構成」を参照してください。

5. [**カスタム セキュリティ リーダー マッピングの有効化**] を選択して、カスタム値 (既定の「Security Lead」の値ではなく) を SAML アサーションのセキュリティ リーダー ロールにマッピングします。その値を [**カスタム マッピング**] フィールドに入力します。これにより、マッピングに使用される既定の「Security Lead」の値が無効になります。
6. [**保存**] をクリックします。

   SSO 設定が保存されます。テナントの SSO 設定が変更されるたびに、システムはセキュリティ リーダーにも自動的に電子メール通知を送信します。

1.8.4.2. ID プロバイダのメタデータの追加

ID プロバイダーのメタデータを OpenText Fortify on Demand にインポートするか、手動で構成して追加します。

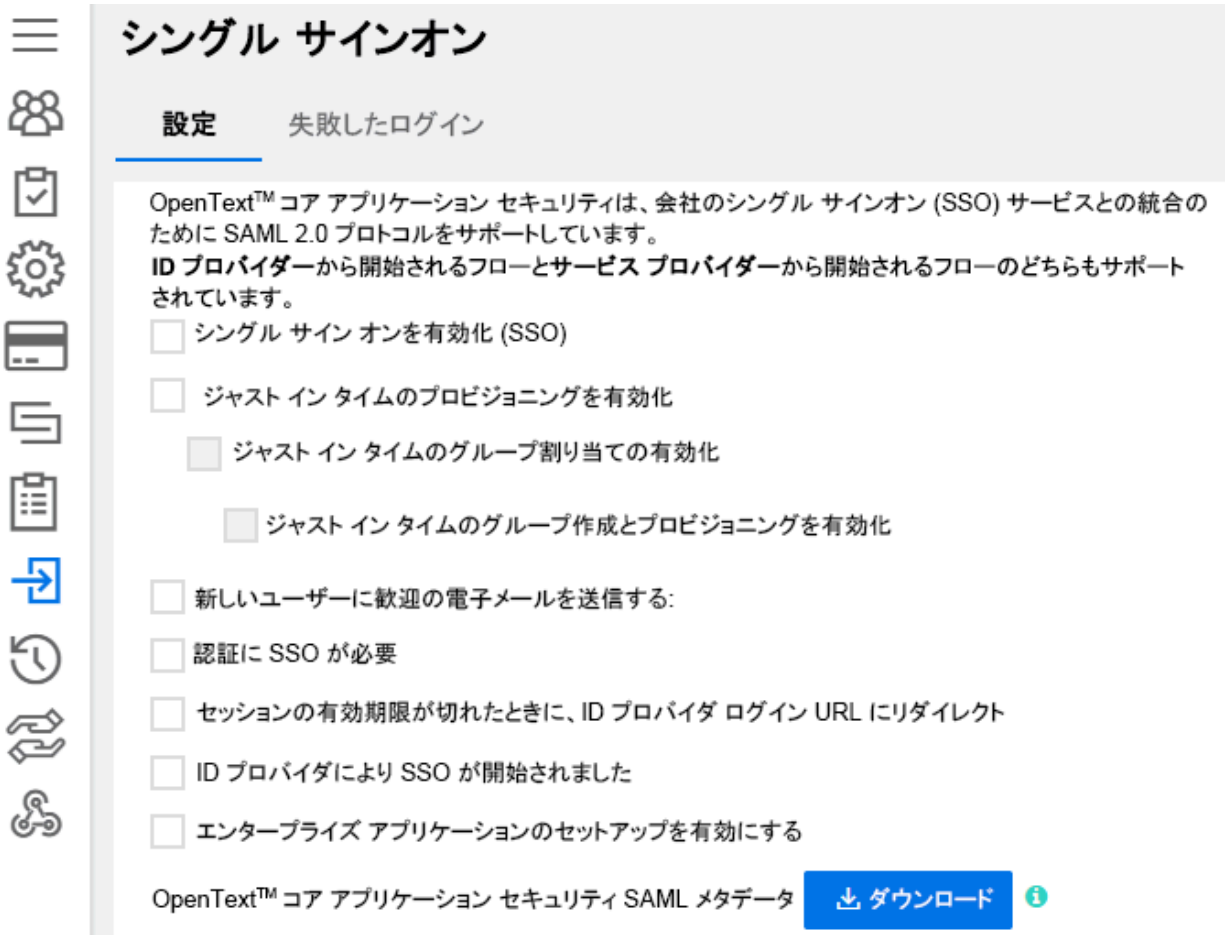
ID プロバイダーのメタデータを追加するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**シングル サインオン**] をクリックします。

   [シングル サインオン] ページが表示されます。



3. [**ID プロバイダの構成**] セクションで、ID プロバイダのメタデータを追加する方法を選択します。

- **ID プロバイダのメタデータのインポート**
- **手動編集**

4. 選択した方法の手順に従います。

> **Note**
>
> SSO が構成されると、ユーザーは [**SSO ログイン URL**] ボックスのリンクを使用して、OpenText Fortify on Demand にログインする必要があります。

- ID プロバイダーのメタデータをインポートする:

  1. [参照] ボタンをクリックします。
  2. .xml ファイルに移動して選択します。

3. [**インポート**] をクリックします。

- ID プロバイダーのメタデータを手動で構成する:

1. ID プロバイダーの情報をフィールドに入力する:

- **ID プロバイダ名**
- **ID プロバイダ ログイン URL**
- **認証リクエストのバインディング** (ID プロバイダーでサポートされているバインディングを使用するには、[**ID プロバイダが対応する値に制限**] を選択します)
- **SAML 要求署名アルゴリズム**
- **ID プロバイダの証明書**

5. [**保存**] をクリックします。

ID プロバイダー メタデータが OpenText Fortify on Demand に追加されます。

1.8.4.3. 暗号化の構成

OpenText Fortify on Demand SSO の暗号化を設定します。

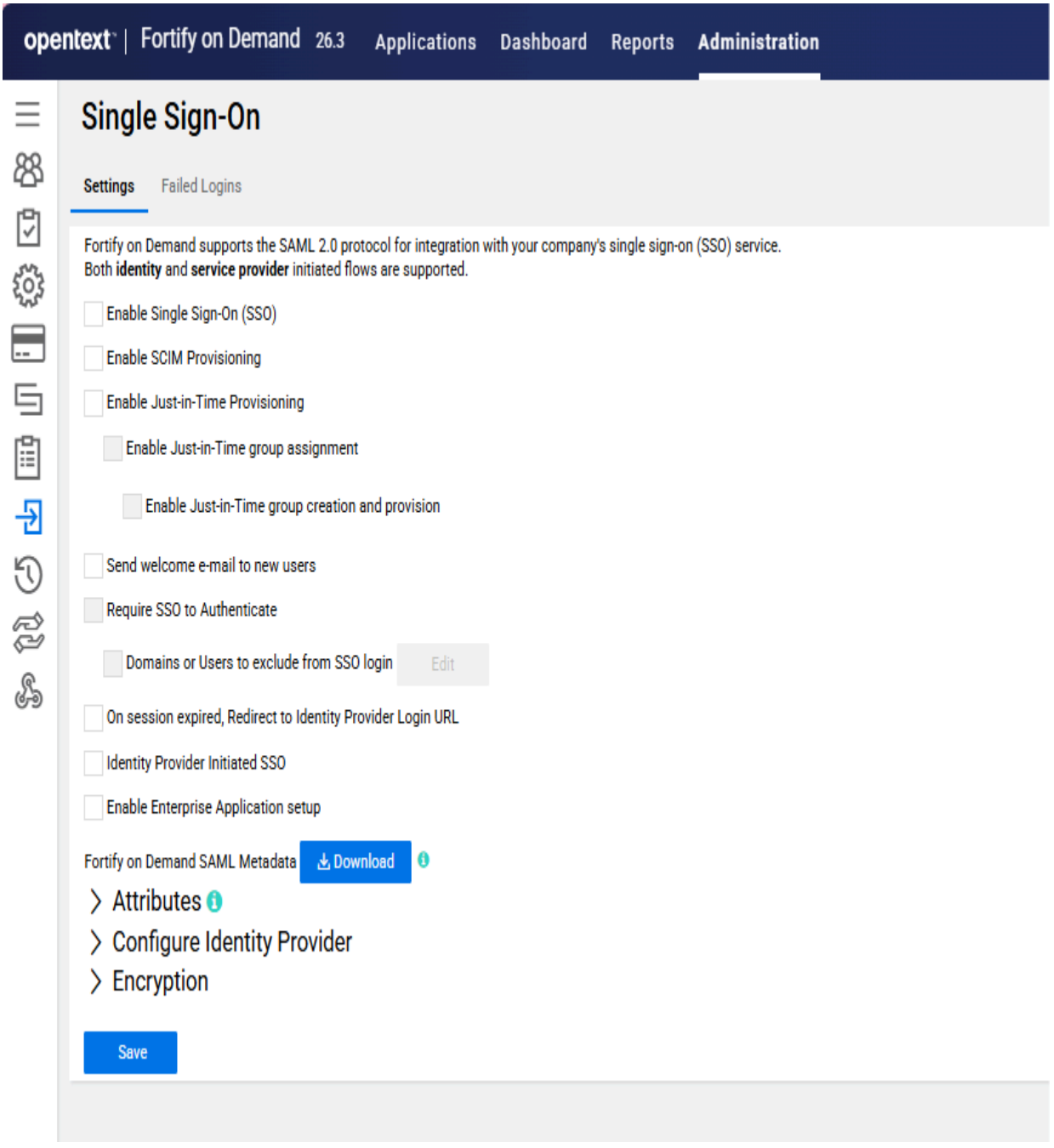
暗号化を設定するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

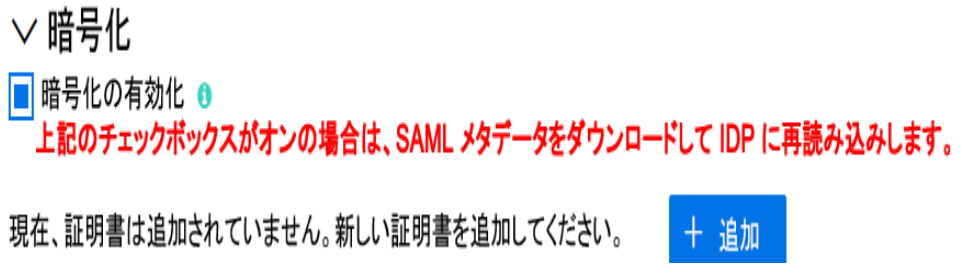
   [ユーザー管理] ページが表示されます。

2. [**シングル サインオン**] をクリックします。

   [シングル サインオン] ページが表示されます。



3. [**暗号化**] セクションで、[**暗号化の有効化**] チェックボックスをオンにして新しい暗号化証明書を追加します。



4. 新しい証明書を追加するには、**[追加] をクリックします。**証明書は次の詳細を使用して作成されます:
   - 証明書名
   - 証明書開始日
   - 証明書終了日

Note

- 初めて暗号化を設定する場合、有効期間が 1 年間のデフォルトの証明書が表示されます。必要に応じて、その証明書を削除して新しい証明書を生成することができます。
- 暗号化が有効になっていて、証明書を作成せずに SAML 構成を保存しようとすると、エラー メッセージが表示されます。
- Fortify on Demand 内に同じ ID プロバイダを共有する複数のテナントがある場合、各テナントが異なる暗号化証明書を作成することがあります。ただし、ID プロバイダ (IDP) にアップロードされるのは、これらの暗号化証明書のうち 1 つだけです。
- 1 つのテナントに対して暗号化を有効にすると、同じ ID プロバイダ (IDP) を共有する他のすべてのテナントにも影響します。したがって、それらすべてのテナントに対しても暗号化を有効にする必要があります。ただし、任意のテナントから IDP に証明書をアップロードすると、Fortify on Demand 内の他のすべてのテナントに対して自動的に復号化が行われます。

1. 有効な証明書を .crt ファイルとしてダウンロードできます。証明書をダウンロードするには、[**ダウンロード**] をクリックします。有効期限が切れた証明書や、まもなく期限が切れる証明書をダウンロードすることはできません。 このようなシナリオでは、新しい証明書を追加することもできます。

2. 証明書を削除するには、[**削除**] をクリックします。

5. [**保存**] をクリックします。

   暗号化の詳細が OpenText Fortify on Demand に追加されます。

> **Note**
> SAML 暗号化証明書を作成すると、SAML メタデータの一部になります。署名証明書に加えて、Core Application Security SAML メタデータをダウンロードすると、暗号化証明書にアクセスできます。

6. セキュリティの観点から、SAML 暗号化証明書は定期的に更新し、アクティブな証明書の有効期限が切れる前に代わりの証明書を作成することをお勧めします。
   暗号化を初めて設定するときは、有効期間が 1 年の既定の証明書が表示されます。必要に応じて、その証明書を削除して新しい証明書を生成することができます。

7. 暗号化が有効になっていて、アクティブな証明書がない状態で SAML 構成を保存しようとすると、エラー メッセージが表示されます。

8. 同じ ID プロバイダを共有する複数のテナントがある場合、各テナントが異なる暗号化証明書を作成することがあります。ただし、ID プロバイダ (IdP) にアップロードされるのは、これらの暗号化証明書のうち 1 つだけです。

   1 つのテナントに対して暗号化を有効にすると、同じ ID プロバイダを共有する他のすべてのテナントにも影響します。したがって、それらすべてのテナントに対しても暗号化を有効にする必要があります。ただし、任意のテナントから IdP に証明書をアップロードすると、他のすべてのテナントに対して自動的に復号化が行われます。

1.8.4.4. OpenText Fortify on Demand メタデータのダウンロード

OpenText Fortify on Demand からの認証要求に応答するように ID プロバイダーを構成するために役立つ OpenText Fortify on Demand メタデータをダウンロードします。メタデータ ファイルには、アサーション コンシューマー サービス URL、OpenText Fortify on Demand 証明書、およびエンティティ ID (サービス プロバイダー名とも呼ばれる) が含まれます。

OpenText Fortify on Demand メタデータ ファイルをダウンロードするには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**シングル サインオン**] をクリックします。

   [シングル サインオン] ページが表示されます。

3. [**ダウンロード**] をクリックします。

   メタデータ ファイルが、ブラウザーの設定で指定したローカルのフォルダーに保存されます。

> **Note**
>
> メタデータは、メタデータの自動取得をサポートする ID プロバイダーの構成をサポートするために URL としても利用できます。このメタデータ ファイルには、ポータル サイトで絶対パス「/SAML」 (例: https://ams.fortify.com/SAML) を使用してアクセスします。メタデータの URL には認証が不要であるため、ID プロバイダーは OpenText Fortify on Demand 資格情報を提供しなくてもアクセスできます。

1.8.4.5. ID プロバイダでの SSO の構成

OpenText Fortify on Demand は、ブラウザーベースの認証フローの SAML 2.0 仕様に適合するあらゆる ID プロバイダーをサポートしています。ID プロバイダーを OpenText Fortify on Demand と共に使用するように構成するためのガイドラインとして、以下の手順を使用します。

OpenText Fortify on Demand サービス プロバイダについて必要なほとんどの情報は、SAML メタデータから取得できます。多くの ID プロバイダは、すべての設定を手動で構成するのではなく、メタデータをインポートすることを許可しています。

ID プロバイダで SSO を構成するには、次の手順を実行します。

1. OpenText Fortify on Demand からの認証要求を受け入れます。

   ID プロバイダは、OpenText Fortify on Demand サービス プロバイダ名から送信される認証要求を受け入れる必要があります。このサービス プロバイダ名は「https://*<tenant_host>*/SAML」で、*<tenant_host>* はご利用のデータセンター (たとえば、「https://ams.fortify.com/SAML」) になります。サービス プロバイダ名は、OpenText Fortify on Demand SAML メタデータから取得できます。

   OpenText Fortify on Demand はすべての認証要求に署名するため、OpenText Fortify on Demand SAML メタデータで提供される SAML 証明書で署名を検証することも選択できます。

   > **Note**
   >
   > バージョン 5.2 以前は、OpenText Fortify on Demand は一部の ID プロバイダーと互換性のないサービスプロバイダー名を使用していました。バージョン 5.2 以前で SSO 認証を設定した場合、「urn:fortify:FodServiceProvider」サービス プロバイダ名を既存の ID プロバイダ構成との後方互換性のために保持できます。できるだけ早く、新しいサービスプロバイダー名に移行することをお勧めします。

2. すべての SAML アサーションに署名します。

   OpenText Fortify on Demand に送信されるすべての SAML アサーションは、OpenText Fortify on Demand SSO 設定で指定された ID プロバイダの証明書を使用して、署名する必要があります。OpenText Fortify on Demand は、SAML 応答全体または応答に含まれるアサーションのみの署名を受け入れます。

> **Note**
>
> OpenText Fortify on Demand は暗号化されたアサーションをサポートしません。

3. ID プロバイダーのシステムクロックが、できれば NIST などの中央時間提供サービスから適切に設定されていることを確認してください。

   たいていの SAML アサーションには、ID プロバイダーによって指定された有効な時間が含まれます。OpenText Fortify on Demand はアサーションを受け取ると、システムクロックと照合して、時間を確認します。OpenText Fortify on Demand はクロック設定の誤差を考慮して、最大 3 分のクロック スキューを許容します。アサーションで指定された時間が切れてから 3 分以上後にアサーションを受け取ると、アサーションは拒否されます。

4. ユーザーが認証された後に ID プロバイダーが SAML アサーション応答を送信する URL を設定します。

   この URL はアサーション コンシューマー サービス URL と呼ばれます。ID プロバイダーによっては、「応答 URL」などと呼ぶ場合もあります。この URL は OpenText Fortify on Demand SAML メタデータから取得できます。

5. SAML アサーションに含める ID クレーム属性を定義します。OpenText Fortify on Demand は SAML アサーションのこのクレーム属性を使用して、認証されたユーザーに関する情報を取得します。

   すべてのアサーションは、OpenText Fortify on Demand に照らしてユーザーを識別する `User Name` 属性を含む必要があります。この値は、OpenText Fortify on Demand 全体で一意でなければならないため、電子メール アドレスなどの組織で一意の ID を使用する必要があります。

   > **Note**
   >
   > システムによっては、SAML アサーションの Subject 要素に **NameID** 値を使用して、ユーザー ID を渡します。OpenText Fortify on Demand では、**NameID** の使用がサポートされていないため、`User Name` の属性も割り当てる必要があります。

   以下の属性は、ジャストインタイム (JIT) プロビジョニングに使用されます。属性は新しい OpenText Fortify on Demand ユーザーを作成するときに必要です。既存の OpenText Fortify on Demand ユーザーを更新する場合、属性はすべてオプションで、既存の値は指定されていない属性用に保持されています。

属性	必須	説明
Email	はい	ユーザーの電子メールアドレス。値は、User Name の値と同じにすることができますが、必須ではありません。User Name と Email の両方を OpenText Fortify on Demand SSO 設定の同じ属性に割り当てることもできます。
First Name	はい	ユーザーの名前。
Last Name	はい	ユーザーの姓。
Mobile Number	いいえ	ユーザーの携帯電話番号。
Role	いいえ	ユーザー ロール。値は、OpenText Fortify on Demand のロール名 (大文字と小文字は区別されない) に一致するプレーン テキスト文字列である必要があります。値を指定しない場合、新規ユーザーには「**Developer**」ロールが設定されます。値がロール名と一致しない場合は、エラーが返されます。

属性	必須	説明
Group	いいえ	ユーザー グループ。値はプレーン テキスト文字列である必要があります (最大 50 文字で、大文字と小文字は区別されない)。値が OpenText Fortify on Demand の既存のユーザー グループと一致しない場合、ポータル SSO オプション [**ジャスト イン タイムのグループ作成とプロビジョニングを有効化**] が選択されていると、ユーザー グループが作成されます。 **Note** ユーザーが SSO を使用してログインし、SAML アサーションで Groups 属性が空の場合、既存のユーザー グループの割り当てはすべて削除されます。

属性	必須	説明
provision_user	はい	ユーザーが見つからない場合に、OpenText Fortify on Demand でユーザーを自動的に作成するかどうかを指定します。値を TRUE に設定すると、新しいユーザーが作成されます。値を FALSE に設定するか、指定しない場合、ユーザーは作成されず、OpenText Fortify on Demand に既存のユーザーがいない場合はログイン要求が失敗します。. **Note** ポータルで値を指定せずに JIT プロビジョニングを有効にした場合、provision_user は既定で TRUE に設定されます。

属性	必須	説明
update_user	いいえ	既存のユーザーの詳細が OpenText Fortify on Demand で SAML アサーションの属性値から自動的に更新されるかどうかを指定します。値が TRUE に設定されている場合、ユーザーの詳細は自動的に更新されます。値が FALSE に設定されている場合、ユーザーの詳細は更新されません。 値を指定しない場合、provision_user 属性の値が使用されます。作成と更新を個別に制御する場合は、両方を指定できます。たとえば、ポータルでユーザーを手動で作成し、ユーザーの詳細はアサーション値から更新することを望む場合などです。

属性	必須	説明
`mtt`	いいえ	ポータル SSO オプション [**エンタープライズ アプリケーションのセットアップを有効にする**] が選択されている場合、この属性は必須です。 SSO ログイン URL 内にある一意の識別子 (引用符で囲む)。たとえば、URL が https://ams.fortify.com/SSO/Login/c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc の場合、識別子は `c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc` です。

Important

OpenText Fortify on Demand の構成を、ID プロバイダが使用する属性を認識するように設定する必要もあります。「SSO 設定の構成」を参照してください。

1.8.4.6. 失敗したログインのトラブルシューティング

失敗した SSO 認証要求のトラブルシューティングは、SAML アサーションに渡された実際の値がユーザーからは見えないために、難しい作業になる場合があります。トラブルシューティングを支援するために、ポータルは失敗した SAML アサーションのログを提供しています。失敗したアサーションは 30 日後に削除されます。

失敗した SAML アサーションのログを表示するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**シングル サインオン**] をクリックします。

   [シングル サインオン] ページが表示されます。

3. [**失敗したログイン**] タブを選択します。

   失敗した SAML アサーションのログが表示されます。

   グリッドには以下の列が含まれます。

   - 受信時刻 - SAML アサーションを受信した時刻。
   - IP アドレス – 認証を要求したクライアントの IP アドレス。
   - ユーザー名 – アサーションで指定されたユーザー名 (ユーザー名がある場合)。
   - 理由 – SAML アサーションが拒否された理由の簡単な説明。

4. 失敗したログインの [**ロー アサーション**] リンクをクリックして、デコードされた SAML アサーションの XML ビューを開きます。

   このページには、ID プロバイダーによってアサーションが発行された時刻、提供された属性と値、有効な期間とオーディエンス、アサーションの署名に使用される証明書など、アサーションの詳細が表示されます。

1.8.5. ベンダー管理

会社が取引しているベンダーや会社の別の部門と評価結果を共有する場合は、各エンティティに OpenText Fortify on Demand を備えた独自のテナントがある場合に限り、ポータルを使用して共有できます。テナント間の関係は 1 つのテナントが開始し、もう 1 つのテナントが確認する必要があります。相手の許可なく、テナントとの接続を確立することはできません。

また各リンクは一方向のみで行われます。つまり、レポートを共有する場合は、もう 1 つのテナントに対してリンクを開始する必要があります。そのテナントがレポートを共有する場合は、そのテナントもリンクを開始する必要があります。[ベンダー レポート] リンクは、正常な共有リレーションシップが設定され、レポートが共有された後でのみ表示されます。

共有するのは評価結果のみで、コードは共有されません。

このコンテキストでは、「ベンダー」はレポートの送信元のテナントを意味し、「顧客」はレポートの送信先のテナントを意味します。

このセクションでは、次のトピックについて説明します。

- 他のテナントとの関係の開始
- 別のテナントによって開始された関係の受け入れ
- ベンダー管理レポートの公開
- 公開済みレポートの表示

1.8.5.1. 他のテナントとの関係の開始

テナントを「ベンダー」 (他のテナントにレポートを送信できるテナント) に設定するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

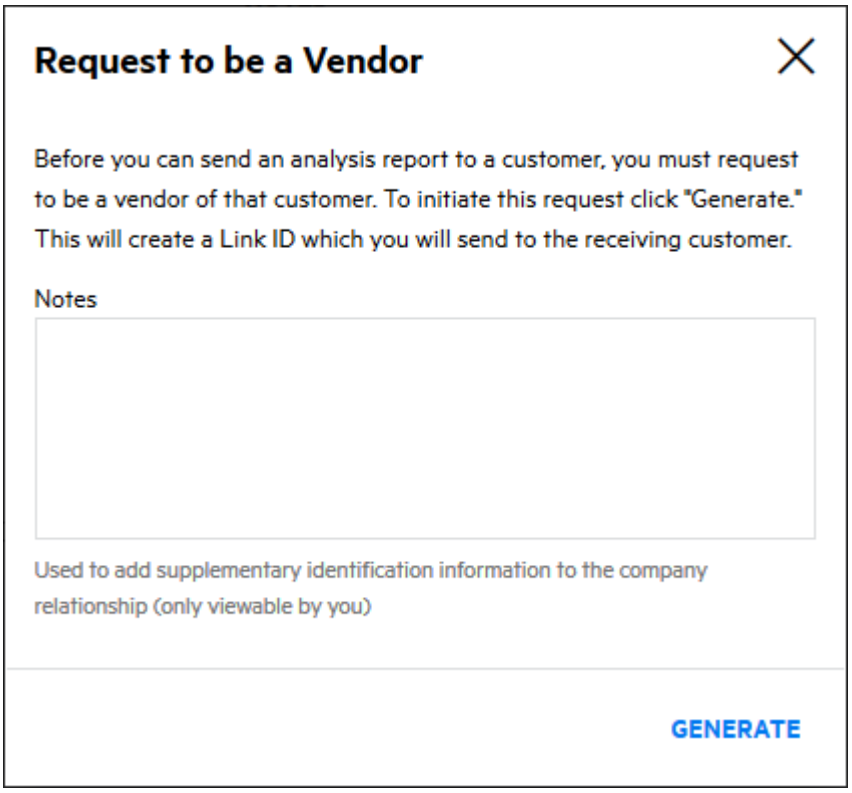
   [**ユーザー管理**] ページが表示されます。

2. [**ベンダー**] をクリックします。
3. [**顧客**] タブを選択します。

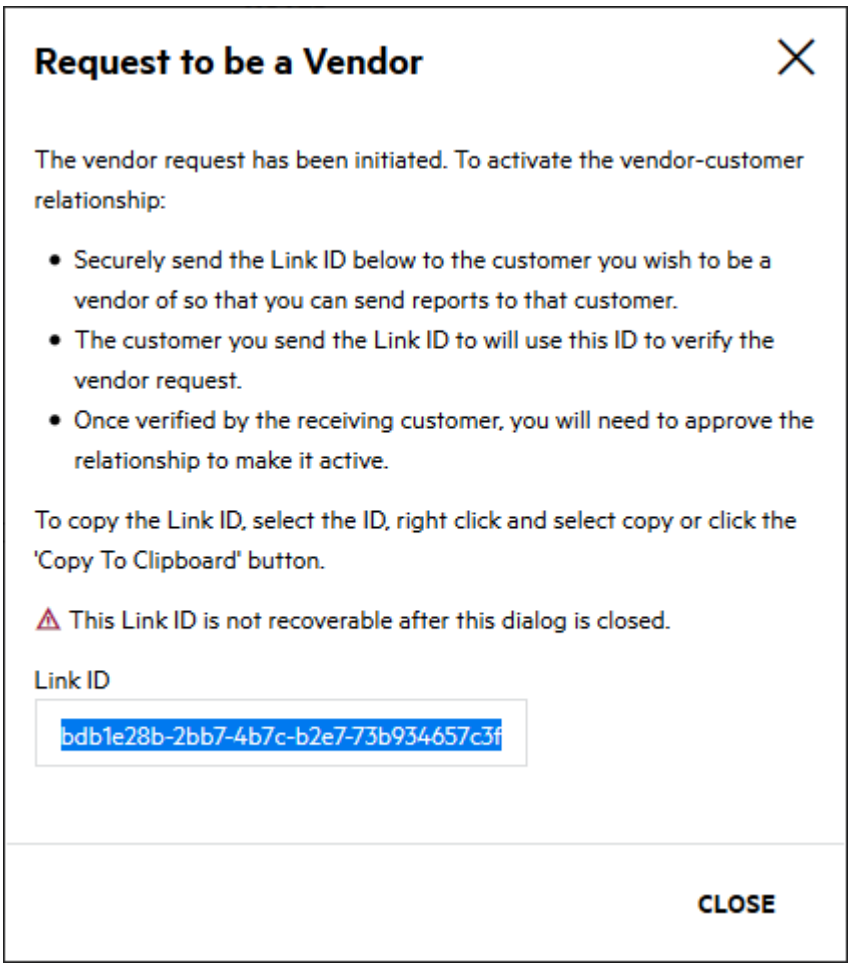
> **Note**
>
> 「自分のベンダー」はレポートの送信元のテナントを意味し、「顧客」はレポートの送信先のテナントを意味します。

4. [**ベンダーになるための要求**] をクリックします。

   ベンダーと顧客の関係に関する情報を追加するには、オプションの [**メモ**] ボックスを使用します。



5. [**生成**] をクリックして、[**リンク ID 番号**] を表示します。



6. [**リンク ID 番号**] をコピーします。

7. このリンクを電子メールまたはその他の安全な送信手段を使用して、接続する会社またはテナントの適切な連絡先に送信します。
8. [**閉じる**] をクリックします。

1.8.5.2. 別のテナントによって開始された関係の受け入れ

別のテナントによって開始された関係の受け入れは、2 ステップのプロセスです。

- リレーションシップの確認
- テナントを顧客として設定

リレーションシップの確認

要求を送信した別のテナントとのリレーションシップを確認するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

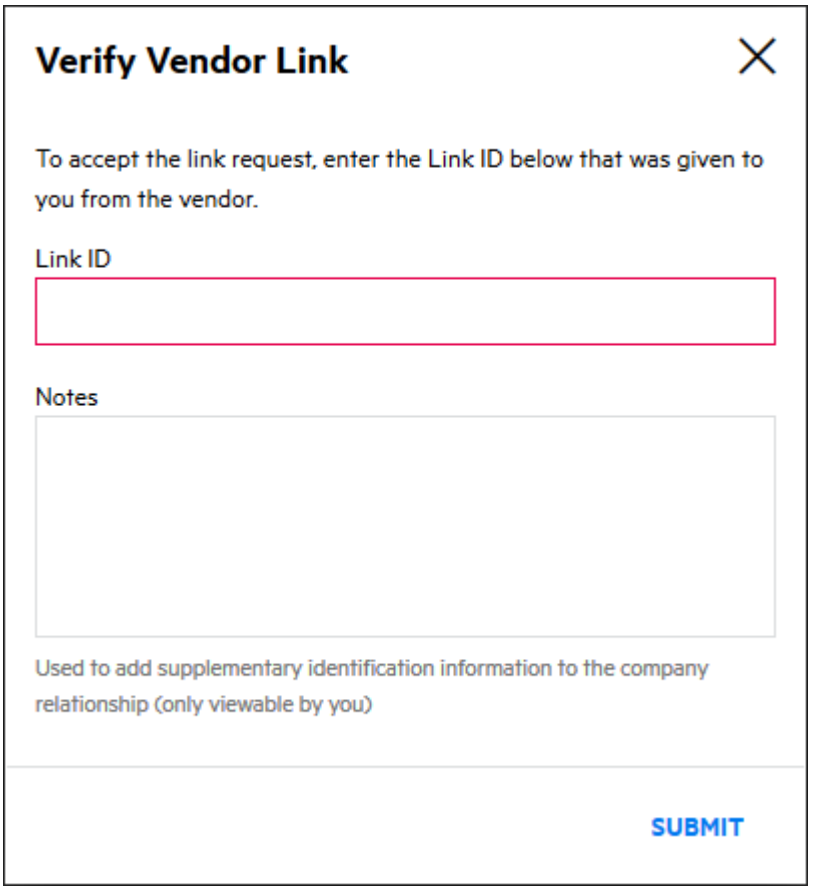
2. [**ベンダー**] をクリックします。

[ベンダー管理] ページが開き、[自分のベンダー] および [顧客] タブが表示されます。このコンテキストでは、「ベンダー」はレポートの送信元のテナントを意味し、「顧客」はレポートの送信先のテナントを意味します。

テナントを顧客として設定

「顧客」 (つまり別のテナントからレポートを受け取ることができるユーザー) としてテナントを設定するには、次の手順を実行します。

1. [**自分のベンダー**] をクリックします。
2. [**ベンダーのリンクを確認**] をクリックします。



3. 別のテナントから受信した [**リンク ID**] を貼り付けます。
4. (オプション) 会社の関係に関する補足情報を追加します (子会社、AUS 部門など)。この情報は自分に対してのみ表示されます。
5. [**送信**] をクリックします。

1.8.5.3. ベンダー管理レポートの公開

OpenText Fortify on Demand 内の他のテナントとの関係を確立した後、自分のレポートを「公開」してそのテナントで確認できるようにします。

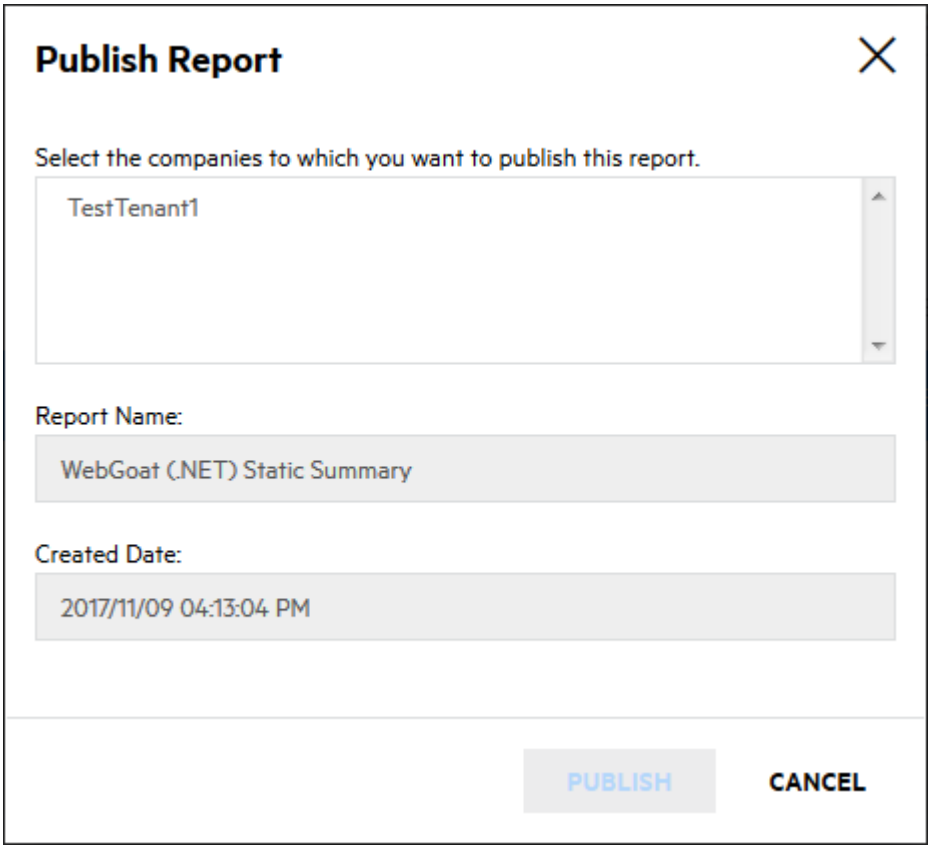
レポートを承認済みベンダーと共有するには、次の手順を実行します。

1. [レポート] ページを選択します。

   テナントのためにこれまでに生成されたレポートがすべて示された新しい画面が表示されます。

2. 共有するレポートの名前をクリックします。ページが更新され、レポート リストの下に [**レポートの詳細**] が表示されます。

3. [**レポートの発行**] ウィンドウが表示されます。他のテナントと関係を確立している場合、それらのテナント名が白いボックス内に表示されます。



4. レポートを送信するテナント名を選択し、[公開] をクリックします。

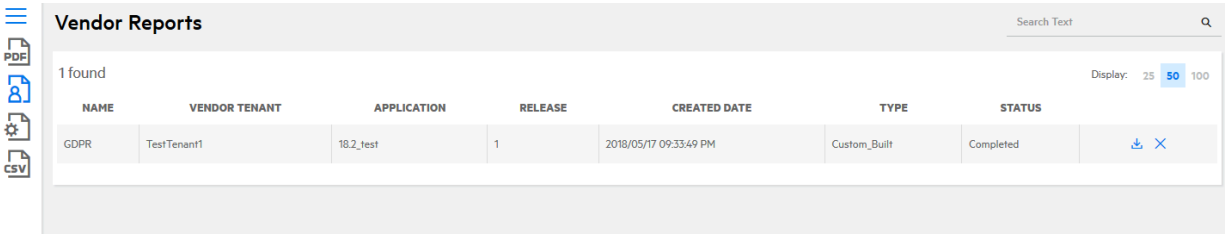
   公開に向けてレポートがキューに入れられたことと、その他のテナントに送信されるということを知らせるメッセージが表示されます。

1.8.5.4. 公開済みレポートの表示

他のテナントがユーザーにレポートを「公開」したら (つまり、テナントとのレポートの「共有」)、次の手順に従ってそのレポートを表示することができます。

1. [レポート] ページを選択します。
2. [ベンダー レポート] をクリックします。

   他のテナントと共有しているレポートを示す [レポート リスト] が表示されます。



3. リストからレポートを強調表示し、[**アクション**] 列で [**結果のダウンロード**] をクリックします。

   システムの [ダッシュボード] フォルダーでレポートを PDF 形式で入手できることを示すメッセージが表示されます。

Note

注: レポート タイプ リストの画面に [**ベンダー レポート**] が表示されない場合、他のテナントとまだレポートを共有していないことを示します。ユーザーと他のテナントの両方が必要なすべての手順を完了して、正常な共有リレーションシップを作成していること、および特定のレポートがユーザーに「公開」されていることを確認します。

1.9. OpenText Fortify on Demand API

OpenText Fortify on Demand が提供する RESTful アプリケーション プログラミング インターフェイス (API) を使用して、さまざまなタスクを実行し、アプリケーションやリリースのデータにアクセスできます。API の最新バージョンはバージョン 3 です。API Root URL は、テナントのデータ センターによって決まります。

データ センター	API Root URL
AMS	https://api.ams.fortify.com
EMEA	https://api.emea.fortify.com
APAC	https://api.apac.fortify.com
SGP	https://api.sgp.fortify.com
FedRAMP	https://api.fed.fortifygov.com
試用版	https://api.trial.fortify.com

Note
OpenText Fortify on Demand API は Cross-Origin Resource Sharing (CORS) をサポートしません。

このセクションでは、次のトピックについて説明します。

- API エクスプローラを使用した API ドキュメントの表示
- API エクスプローラを使用した API エンドポイントのテスト
- API 認証
- API スコープ
- API レート リミット
- パーソナル アクセス トークン

1.9.1. API エクスプローラを使用した API ドキュメントの表示

OpenText Fortify on Demand API ドキュメントは、API エクスプローラの形式で提供されます。API エクスプローラは Swagger (OpenAPI) フレームワーク上に構築されていて、ポータルから直接使用できます。これを使用すると、API を自己説明的で双方向的なものにすることができます。ユーザーは API に対する最新の更新情報を即座に表示して呼び出しをテストしたり、JSON で記述された API を使用して、Swagger Editor や Swagger Codegen などのオープン ソース ツールを通してさまざまなプログラミング言語でスタブや SDK を生成したりできます。

API エクスプローラを表示するには:

1. ツールバーのアカウント名をクリックし、[**API エクスプローラ**] を選択します。

   リソースの一覧を示す API エクスプローラのページが新しいウィンドウで表示されます。

2. 次の操作を使用してリソースの詳細を確認できます。

   - API エクスプローラ ページの上部にある [**GET JSON**] をクリックします。ブラウザーに JSON で記述された API が表示されます。


```
{"swagger":"2.0","info":{"version":"v3","title":"Fortify on Demand Web API Explorer"},"host":"16.103.234.237","schemes":["http"],"paths":{"/api/v3/applications/{applicationId}":
{"get":{"tags":["Applications"],"summary":"Retrieves an individual application by id","operationId":"ApplicationsV3_GetApplication","consumes":[],"produces":
["application/json","text/json","application/xml","text/xml"],"parameters":[{"name":"applicationId","in":"path","description":"The application
id","required":true,"type":"integer","format":"int32"}],"responses":{"200":{"description":"Ok","schema":{"$ref":"#/definitions/Application"}},"401":
{"description":"Unauthorized"},"404":{"description":"NotFound"},"500":{"description":"InternalServerError"}},"deprecated":false},"put":{"tags":["Applications"],"summary":"Update an
application","operationId":"ApplicationsV3_PutApplication","consumes":["application/json","text/json","application/xml","text/xml","application/x-www-form-
urlencoded","multipart/form-data"],"produces":["application/json","text/json","application/xml","text/xml"],"parameters":[{"name":"applicationId","in":"path","description":"The
application id","required":true,"type":"integer","format":"int32"},{"name":"requestModel","in":"body","description":"The application data","required":true,"schema":
{"$ref":"#/definitions/PutApplicationRequest"}}],"responses":{"200":{"description":"Ok","schema":{"$ref":"#/definitions/PutApplicationResponse"}},"400":
{"description":"BadRequest","schema":{"$ref":"#/definitions/PutApplicationResponse"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":
{"description":"NotFound"},"422":{"description":"UnprocessableEntity","schema":{"$ref":"#/definitions/PutApplicationResponse"}},"500":
{"description":"InternalServerError"}},"deprecated":false},"delete":{"tags":["Applications"],"summary":"Deletes an application","operationId":"ApplicationsV3_Delete","consumes":
[],"produces":["application/json","text/json","application/xml","text/xml"],"parameters":[{"name":"applicationId","in":"path","description":"The application
id","required":true,"type":"integer","format":"int32"}],"responses":{"200":{"description":"Ok","schema":{"$ref":"#/definitions/DeleteApplicationResponse"}},"400":
{"description":"BadRequest","schema":{"$ref":"#/definitions/DeleteApplicationResponse"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":
{"description":"NotFound"},"500":{"description":"InternalServerError"}},"deprecated":false}},"/api/v3/applications":{"get":{"tags":["Applications"],"summary":"Retrieve a collection
of applications","operationId":"ApplicationsV3_GetApplications","consumes":[],"produces":["application/json","text/json","application/xml","text/xml"],"parameters":
[{"name":"filters","in":"query","description":"<p>A delimited list of field filters.</p>\r\n<p>Field name and value should be separated by a colon (:).</p>\r\n<p>Multiple fields
should be separated by a plus (+). Example, fieldname1:value+fieldname2:value</p>","required":false,"type":"string"},{"name":"orderBy","in":"query","description":"The field name to
order the results by.","required":false,"type":"string"},{"name":"fields","in":"query","description":"Comma separated list of fields to return.","required":false,"type":"string"},
{"name":"offset","in":"query","description":"Offset of the starting record. 0 indicates the first record.","required":false,"type":"integer","format":"int32"},
{"name":"limit","in":"query","description":"Maximum records to return. The maximum value allowed is 50.","required":false,"type":"integer","format":"int32"}],"responses":{"200":
{"description":"Ok","schema":{"$ref":"#/definitions/ApplicationListResponse"}},"400":{"description":"BadRequest","schema":{"$ref":"#/definitions/ErrorResponse"}},"401":
{"description":"Unauthorized"},"500":{"description":"InternalServerError"}},"deprecated":false},"post":{"tags":["Applications"],"summary":"Create a new application and
release","operationId":"ApplicationsV3_PostApplication","consumes":["application/json","text/json","application/xml","text/xml","application/x-www-form-urlencoded","multipart/form-
data"],"produces":[],"parameters":[{"name":"requestModel","in":"body","description":"The application data","required":true,"schema":
{"$ref":"#/definitions/PostApplicationRequest"}}],"responses":{"204":{"description":"No Content"},"201":{"description":"Created","schema":
{"$ref":"#/definitions/PostApplicationResponse"}},"400":{"description":"BadRequest","schema":{"$ref":"#/definitions/ErrorResponse"}},"401":{"description":"Unauthorized"},"422":
{"description":"UnprocessableEntity","schema":{"$ref":"#/definitions/ErrorResponse"}},"500":
```


     Swagger Editor や Swagger Codegen など Swagger をサポートするコード ジェネレータ ツールに JSON ファイルを貼り付けるか、インポートして、クライアント スタブまたは SDK を生成することができます。

- [**Show/Hide**] をクリックすると、エンドポイントの表示と非表示が切り替わります。
- [**List Operations**] をクリックすると、リソースのエンドポイントが表示されます。
- [**Expand Operations**] をクリックすると、すべてのリソースのエンドポイントの説明が表示されます。
- エンドポイントをクリックして、説明を表示します。

1.9.2. API エクスプローラを使用した API エンドポイントのテスト

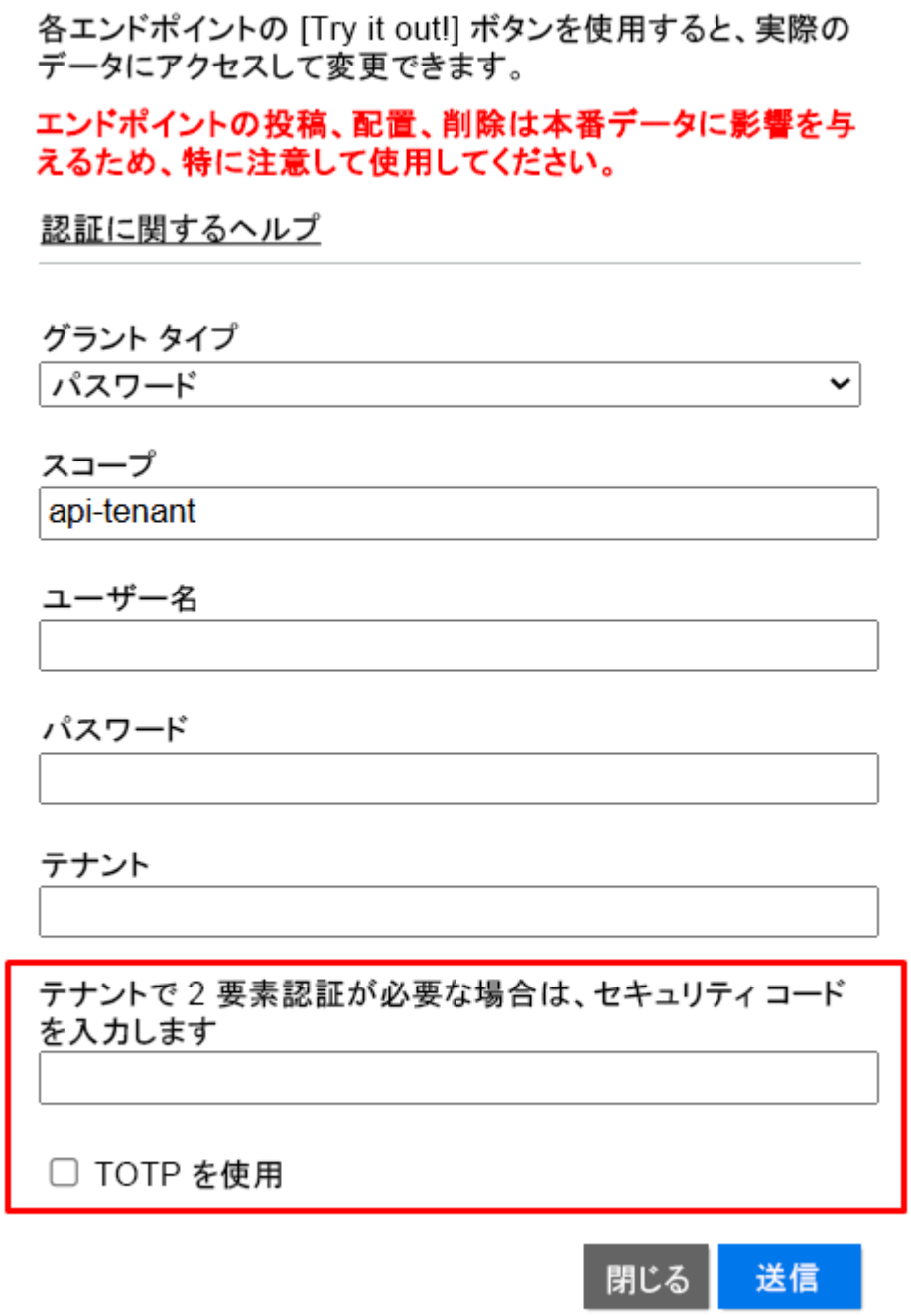
API エクスプローラでバージョン 3 API エンドポイントをテストできます。

Important

API エクスプローラの POST、PUT、および DELETE メソッドは、ポータル内のテナント データを変更します。

1. API エクスプローラ ページの上部にある [**Authenticate**] をクリックします。

モーダル ウィンドウが開き、認証資格情報を入力します。



2. [**グラント タイプ**] リストで認証方法を選択します。
    - **password**: ポータル内のユーザー アカウント資格情報
    - **client_credentials**: ポータル内で生成された API キー
3. [**スコープ**] フィールドにアクセス トークンに付与されるスコープを入力します。複数のスコープ値はスペースで区切ります。スコープのリストについては、「API スコープ」を参照してください。
4. 認証資格情報を入力します。

認証の方法	手順
client_credentials	1. [**クライアント ID**] フィールドに API キーを入力します。API キーの作成については、「API キーの作成」を参照してください。 2. [**クライアント シークレット**] フィールドに API シークレットを入力します。

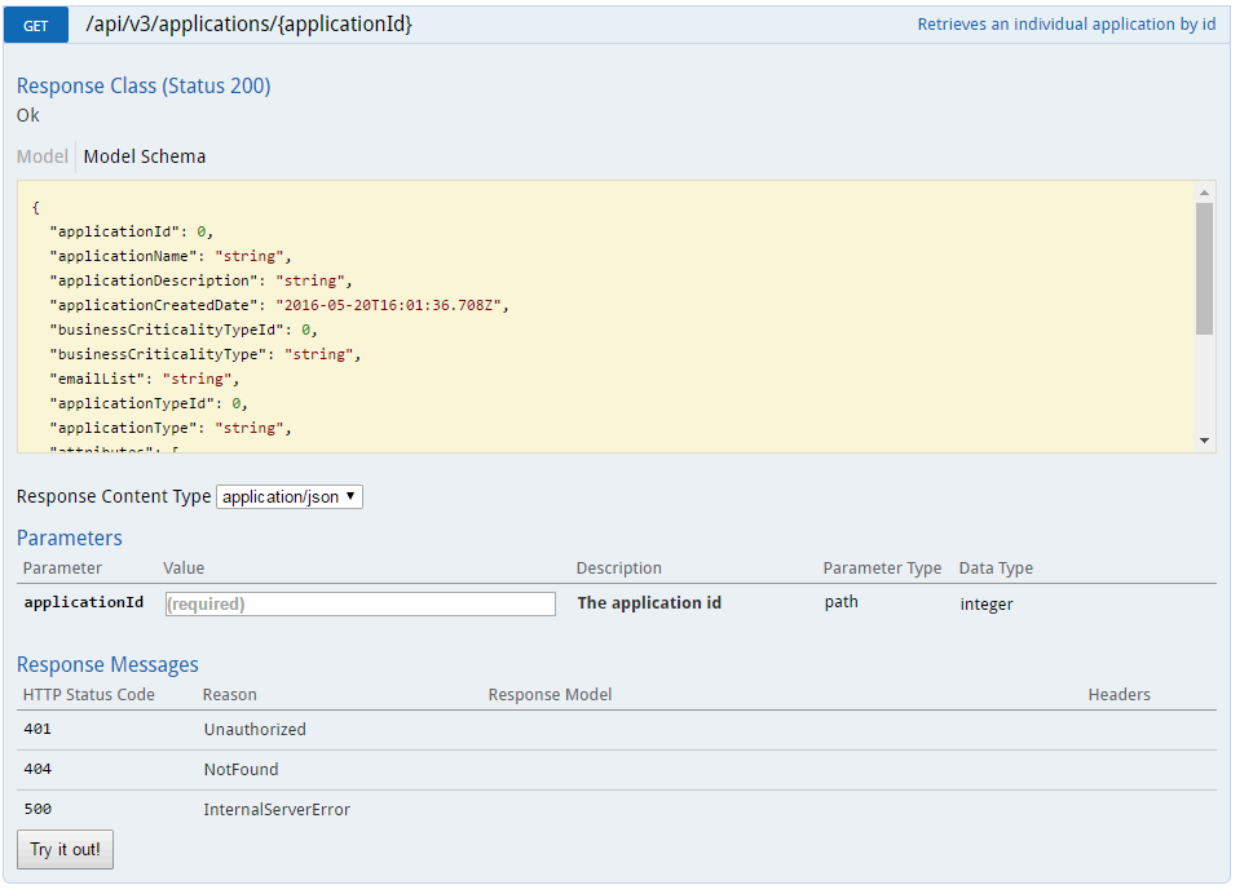
認証の方法	手順
password	 **Note** アカウントの設定からテナント コードとユーザー名を取得できます。 1. [**ユーザー名**] フィールドにアカウントのユーザー名を入力します。 2. [**パスワード**] フィールドにアカウントのパスワードまたはパーソナル アクセス トークンを入力します。  **Note** パーソナル アクセス トークンが使用され、指定されたスコープがパーソナル アクセス トークンの許可されたスコープのサブセットではない場合、認証は失敗します。 3. [**テナント**] フィールドにテナント コードを入力します。 4. (2 要素認証が有効の場合に必要) [**セキュリティ コード**] フィールドに、2 要素認証の一部として受信したセキュリティ コードを入力します。 5. 検証コードが時間ベースのワンタイム パスワード (TOTP) 認証アプリケーションによって生成された

認証の方法	手順
	場合は、[**TOTP を使用**] を選択してください。

5. [**送信**] をクリックします。

   セッションのアクセス トークンが生成されます。

6. エンドポイントを展開し、表示されたフィールドにパラメーターを入力します。



7. [**Try it out!**] をクリックします。

   応答が下に追加されます。

Try it out! Hide Response

Curl

```
curl -X GET --header 'Accept: application/json' --header 'Authorization: Bearer gAAAAH21jER2935DMsX8qvA2q6qyhpPh8cOVeDfNo_9KeqnWz
```

Request URL

```
http://16.103.234.237/api/v3/applications/4191
```

Response Body


```
{
  "applicationId": 4191,
  "applicationName": "Test Application",
  "applicationDescription": null,
  "applicationCreatedDate": "2016-01-26T10:23:22.717",
  "businessCriticalityTypeId": 3,
  "businessCriticalityType": "Low",
  "emailList": null,
  "applicationTypeId": 1,
  "applicationType": "Web_Thick_Client",
  "attributes": null
}
```


Response Code

```
200
```

Response Headers


```
{
  "pragma": "no-cache",
  "date": "Thu, 19 May 2016 14:14:34 GMT",
  "server": "Microsoft-IIS/8.5",
  "x-powered-by": "ASP.NET",
  "content-type": "application/json; charset=utf-8",
  "expires": "-1",
  "cache-control": "no-cache",
  "content-length": "296",
  "x-ua-compatible": "IE=Edge"
}
```

1.9.3. API 認証

OpenText Fortify on Demand API 要求の認証は、ベアラ トークンを介して行われます。トークン エンドポイントに要求を送信して、ベアラ トークンを取得します。

OpenText Fortify on Demand API コールを認証するには、次の手順を実行します。

1. 次の本文パラメーターを指定して、トークンのエンドポイント `<datacenter_root_URL>/oauth/token` に POST 要求を送信します。

> **Note**
>
> データ センターの API Root URL のリストについては、「アプリケーション プログラミング インターフェイス (API)」を参照してください。

本文パラメーター	説明
`scope`	アクセス トークンに付与されるスコープ (小文字)。複数のスコープ値はスペースで区切ります。スコープのリストについては、「API スコープ」を参照してください。
`grant_type`	グラント タイプ (小文字): ◦ `password` : ユーザーの資格情報 (リソース所有者のパスワード認証情報) ◦ `client_credentials` : API キーとシークレット
`username`	アカウント ユーザー名は `<tenant_code>\<username>` です。テナント コードとユーザー名は、アカウントの設定に表示されます。ユーザー名を引用符で囲み、特殊文字をエスケープします。

本文パラメーター	説明
password	アカウントのパスワードまたはパーソナル アクセス トークン。パスワードを引用符で囲み、特殊文字をエスケープします。 **Note** SSO ユーザーは、パーソナル アクセス トークンを使用するように制限されます。 **Note** パーソナル アクセス トークンがパスワードとして使用され、指定されたスコープがパーソナル アクセス トークンの許可されたスコープのサブセットを構成しない場合、認証は失敗します。パーソナル アクセス トークンの詳細については、「パーソナル アクセス トークンの作成」を参照してください。
client_id	API キー
client_secret	API シークレット

"access_token" という名前で JSON 応答でトークンが返されます。

2. このトークンを認証ヘッダーでベアラ トークンとして使用します。

   `Authorization: Bearer {token}`

以下は、ユーザー資格情報を使用してベアラ トークンを取得する要求の例です。

```
 curl --request POST 'https://api.ams.fortify.com/oauth/token' \
--form 'scope="api-tenant"' \ --form 'grant_type="password"' \ -
-form 'username="myTenantCode\\myUsername"' \ --form
'password="myPassword"'
```

以下は、API キーとシークレットを使用してベアラ トークンを取得する要求の例です。

```
 curl --request POST 'https://api.ams.fortify.com/oauth/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \ --
data-urlencode 'scope=api-tenant' \ --data-urlencode
'grant_type=client_credentials' \ --data-urlencode
'client_id=myApiKey' \ --data-urlencode
'client_secret=myApiSecret'
```

1.9.4. API スコープ

スコープは、アクセス トークンに付与されるアクセス権限を制限します。スコープは、現在ユーザーが持っている以上の権限を付与しません。API エクスプローラにエンドポイントの詳細を表示し、許可されたスコープを確認できます。

次の表に、使用可能なスコープを示します。

スコープ	説明
api-tenant	すべてのエンドポイントへのアクセスを許可する
start-scans	静的、動的、およびモバイル スキャンを構成し開始する。静的および動的スキャンをインポートする
manage-apps	アプリケーションを管理する
view-apps	アプリケーションを表示する
manage-issues	問題を管理する
view-issues	問題を表示する
manage-reports	レポートを管理する
view-reports	レポートを表示する
manage-users	ユーザーを管理する
view-users	ユーザーを表示する
manage-notifications	通知を管理する
view-tenant-data	テナント レベルのデータを表示する

1.9.5. API レート リミット

OpenText Fortify on Demand では、エンドポイントごと、およびユーザーごと、またはキー ベースごとの API レート リミットが実装されます。

次のエンドポイントは制限されません。

- PUT/api/v3/releases/{releaseId}/dynamic-scans/import-scan
- POST /api/v3/releases/{releaseId}/mobile-scans/start-scan
- PUT /api/v3/releases/{releaseId}/mobile-scans/import-scan
- POST /api/v3/releases/{releaseId}/static-scans/start-scan
- PUT /api/v3/releases/{releaseId}/static-scans/import-scan

次の表に、制限されるエンドポイントのレート リミットを示します。

エンドポイント	最大要求	秒
POST /api/v3/applications	6	30
PUT /api/v3/applications/{applicationId:int}	1	30
GET /api/v3/eventlogs/download	1	300
POST /api/v3/releases	6	30
PUT /api/v3/releases/{releaseId:int}	1	30
POST /api/v3/releases/{releaseId:int}/dynamic-scans/start-scan	1	30
GET /api/v3/releases/{releaseId:int}/fpr **Note** レート リミットはスキャンのタイプごとに設定されます。	1	30
GET /api/v3/releases/{releaseId:int}/vulnerabilities/{vulnId}/all-data	1	1

エンドポイント	最大要求	秒
POST /api/v3/releases/{releaseId:int}/vulnerabilities/bug-link	1	5
POST /api/v3/releases/{releaseId:int}/vulnerabilities/bulk-edit	1	5
その他のエンドポイント	10	1

トラッキング レート リミット

API エンドポイントを呼び出すときに、応答 HTTP ヘッダーにレート リミットおよびレート リミットに近付く速度が示されます。

- X-Rate-Limit-Limit: 要求の最大数
- X-Rate-Limit-Remaining: 要求の残りの数
- X-Rate-Limit-Reset: レート リミットがリセットされるまでの秒数

API エンドポイントのレート リミットに達すると、API は HTTP 429 「Too Many Requests (要求が多すぎる)」 応答ステータスを次のような応答メッセージと一緒に返します。

```
{ "errors": [ { "errorCode": null, "message": "Rate limit of 1 request(s) every 15 second(s) has been exceeded" } ] }
```

レート リミットを回避するためのベスト プラクティス

API を呼び出すときにレート リミットを回避するには、次のベスト プラクティスを使用して、API 要求の数を減らして、制御します。

- よく使用するデータをキャッシュします。

  よく使用する API エンドポイントの場合、API 応答をキャッシュして、データを要求するときにキャッシュされた応答をロードします。

- 不必要な API 呼び出しをなくします。

利用されていないデータの取得要求および OpenText Fortify on Demand への変更のないデータの送信要求を調べます。

- 要求レートの制御

  定期的にレート リミットに達する場合は、要求のレートを制御して、指定されたレート リミット内に収まるようにするプロセスを含めることを検討してください。固定要求レートを設定して、要求レートを静的に制御するか、要求をトラッキングし、レート リミットに近付くと制御することによって動的に制御することができます。

1.9.6. パーソナル アクセス トークン

パーソナル アクセス トークンは、生成したユーザーに関連付けられた一意のキーです。これらは API への認証に使用される代替パスワードとして機能します。ユーザーの権限を持ち、スコープでさらに制限することができます。パーソナル アクセス トークンを使用すると、ポータルで設定されている 2 要素認証および SSO 要件がバイパスされます。

Note

パーソナル アクセス トークンを使用してポータルにログインすることはできません。

パーソナル アクセス トークンは、OpenText Fortify on Demand と統合するための柔軟で安全な認証方法を提供します。ユーザーは、特定のニーズに合わせてスコープの異なる複数のトークンを使用したり、トークンの有効期限を指定したりできます。また、いつでもトークンを無効にできます。

OpenText Fortify on Demand は、パーソナル アクセス トークンの有効期限が切れる 14 日前に電子メール通知とポータル通知を送信します。新しいシークレットが生成されない限り、有効期限切れのパーソナル アクセス トークンは使用できません。

このセクションでは、次のトピックについて説明します。

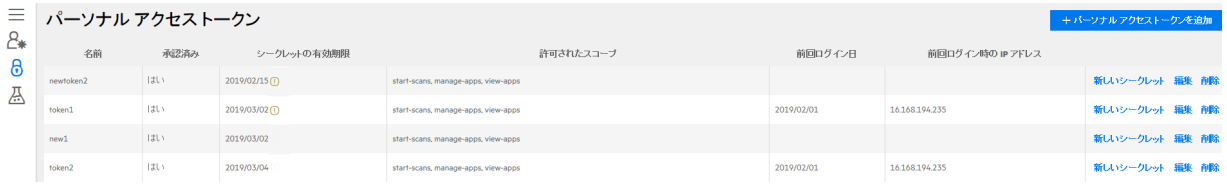
- パーソナル アクセス トークンの作成
- パーソナル アクセス トークンの編集または削除

1.9.6.1. パーソナル アクセス トークンの作成

パーソナル アクセス トークンを作成するには:

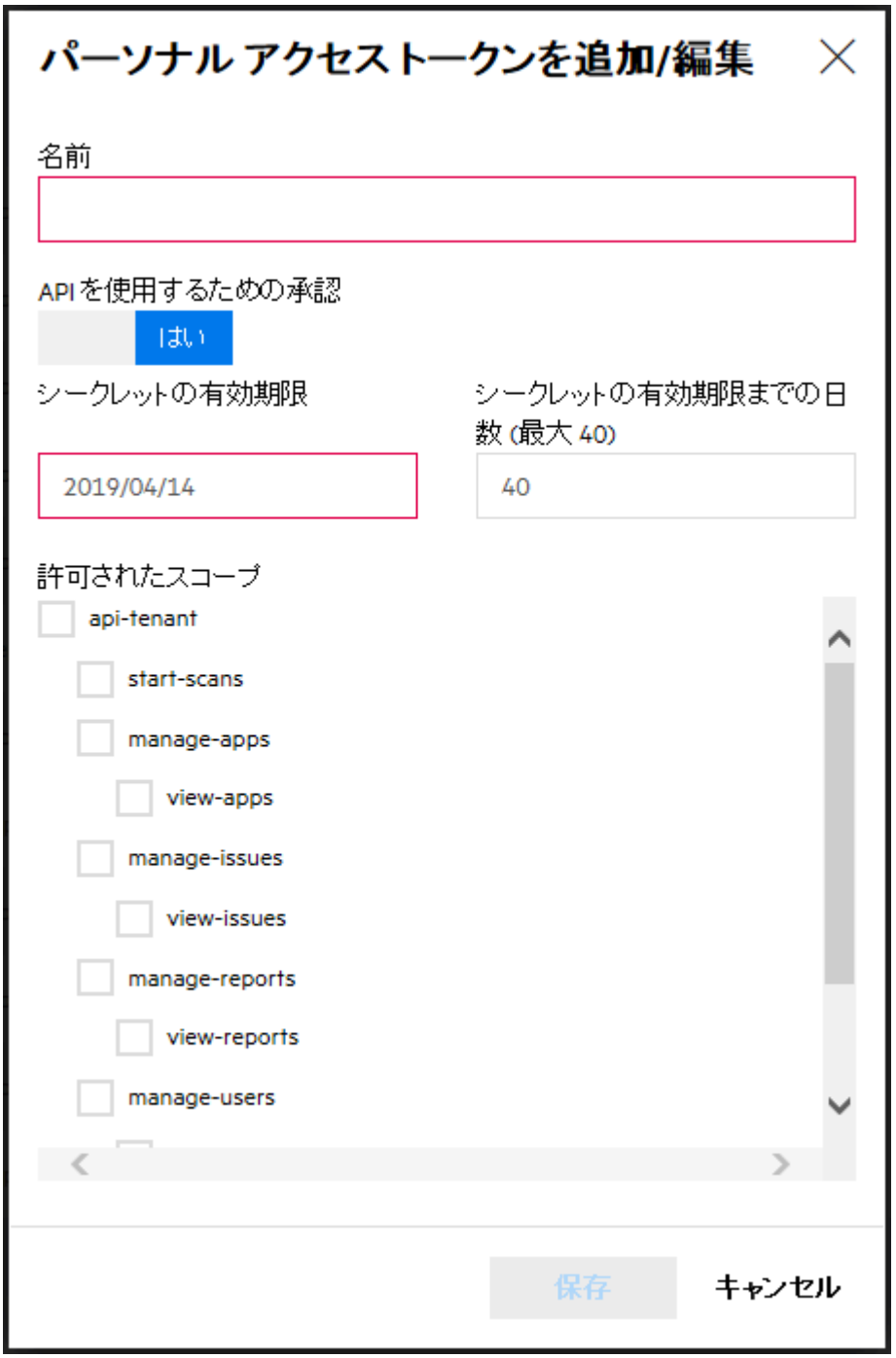
1. アカウント名をクリックし、[**パーソナル アクセス トークン**] を選択します。

   [パーソナル アクセス トークン] ページが表示されます。



2. [**+ パーソナル アクセス トークンの追加**] をクリックします。

   [パーソナル アクセス トークンの追加/編集] ウィンドウが開きます。



3. フィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
名前	トークンの名前を入力します。
API を使用するための承認	トークンは、既定では有効になっています。トークンを無効にするには、スライダーを [**いいえ**] に移動します。
シークレットの有効期限、シークレットの有効期限までの日数	カレンダーを使用して有効期限を選択するか、シークレットの有効期限までの日数を入力します。トークンは、設定した日付の 午前 0 時 (太平洋時間) に期限切れになります。有効期限は、ポータルで設定されている最大有効期間を超えることはできません。
許可されたスコープ	トークンに許可されたスコープを選択します。スコープの詳細については、「API スコープ」を参照してください。

4. [**保存**] をクリックします。

   [シークレット キー] ウィンドウが開きます。

5. Base64 でエンコードされたシークレットをコピーします。シークレットは 1 回だけ表示されます。

6. [**閉じる**] をクリックします。

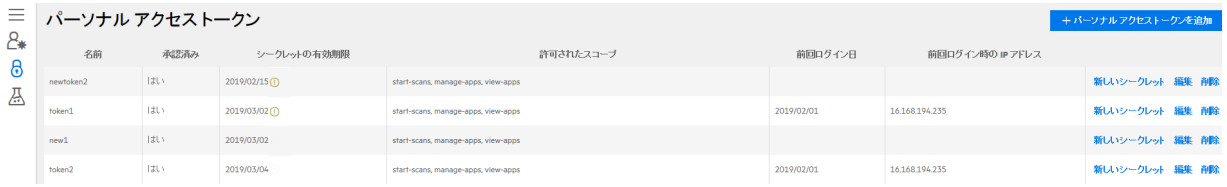
   パーソナル アクセス トークンのリストに新しいトークンが表示されます。

1.9.6.2. パーソナル アクセス トークンの編集または削除

パーソナル アクセス トークンを編集または削除するには:

1. アカウント名をクリックし、[**パーソナル アクセス トークン**] を選択します。

   [パーソナル アクセス トークン] ページが表示されます。



2. 次のタスクを実行できます。

タスク	手順
新しいシークレットの生成	• [**新しいシークレット**] をクリックします。 [新しいシークレット] ウィンドウが開きます。 • カレンダーを使用して有効期限を選択するか、シークレットの有効期限までの日数を入力します。トークンは、設定した日付の 午前 0 時 (太平洋時間) に期限切れになります。有効期限は、ポータルで設定されている最大有効期間を超えることはできません。 • [**作成**] をクリックします。これによって現在のシークレットは無効になります。
トークンの編集	• [**編集**] をクリックします。 [パーソナル アクセス トークンの追加/編集] ウィンドウが開きます。 • 必要に応じてフィールドを編集します。現在のシークレットの有効期限は編集できません。
トークンの削除	• [**削除**] をクリックします。 確認メッセージが表示されます。 • **[はい]** をクリックします。

1.10. 統合とツール

OpenText Fortify on Demand は、組織がアプリケーション セキュリティ テストを DevOps プロセスに統合するのに役立つ各種統合とツールを提供します。

- CICD ツール
- IDE ツール
- スキャン準備および追跡ツール
- ツールの表示およびダウンロード
- ポータルの統合
- トレーニング コース

1.10.1. CICD ツール

次の継続的統合および継続的配信 (CICD) 統合ツールにより、静的テストと動的テストを既存のビルド自動化に統合できます。

CICD ツール	説明	詳細情報
OpenText Fortify on Demand アップローダー	静的スキャンのためにコードをビルド サーバーから OpenText Fortify on Demand にアップロードするスタンドアロン ユーティリティ	GitHub
Fortify Azure DevOps Extension	以下のための Azure DevOps 拡張機能: • OpenText Fortify on Demand にコードをアップロードし、静的スキャンをビルド タスクとリリース タスクとして送信する • 動的スキャンをビルド タスクとリリース タスクとして送信する	• Visual Studio Marketplace • ドキュメント
Fortify on Demand Jenkins Plugin	コードを OpenText Fortify on Demand にアップロードして、静的スキャンをビルドタスクとして送信するための Jenkins プラグイン	• Jenkins • ドキュメント
Fortify CLI	さまざまな Fortify 製品とやり取りするためのコマンドライン ユーティリティ	GitHub リポジトリ

CICD ツール	説明	詳細情報
Fortify Bitbucket Pipelines	次に対する Bitbucket パイプラインのコレクション: • OpenText Fortify on Demand へのコードのアップロードと静的スキャンの送信	• Bitbucket • ドキュメント
Fortify GitHub Actions	次に対する GitHub アクションのコレクション: • OpenText Fortify on Demand へのコードのアップロードと静的スキャンの送信	• GitHub マーケットプレイス • ドキュメント
Fortify GitLab CI Templates	次に対する GitLab テンプレートのコレクション: • OpenText Fortify on Demand へのコードのアップロードと静的スキャンの送信	GitLab
Fortify CI Tools	構成可能なランナーを使用して CICD ワークフローを実行する DevSecOps パイプライン用の Fortify の静的アプリケーションセキュリティ テストの統合を簡素化するための Docker コンテナ	Docker Hub

1.10.2. IDE ツール

次の統合開発環境 (IDE) ツールにより、開発者は静的テストのために IDE から OpenText Fortify on Demand にコードをアップロードできます。

Note

各 IDE ツールのドキュメントはスタンドアロン ガイドとして利用できるようになりました。

IDE ツール	説明	詳細情報
Fortify on Demand Plugin for Eclipse	静的スキャンのためにコードを OpenText Fortify on Demand にアップロードし、スキャン結果を開いて修復する Eclipse プラグイン	Fortify on Demand Plugin for Eclipse
Core Application Security Plugin for IntelliJ IDEA	静的スキャンのためにコードを OpenText Fortify on Demand にアップロードし、スキャン結果を開いて修復する IntelliJ IDEA プラグイン	Core Application Security Plugin for IntelliJ IDEA
Fortify on Demand Extension for Visual Studio	静的スキャンのためにコードを OpenText Fortify on Demand にアップロードし、スキャン結果を開いて修復する Visual Studio 拡張機能	Fortify on Demand Extension for Visual Studio
Core Application Security Remediation Extension for Visual Studio Code	OpenText Fortify on Demand のアプリケーション リリースから直接問題を表示および監査する Visual Studio Code 拡張機能	Core Application Security Remediation Extension for Visual Studio Code
Fortify Extensions for Visual Studio Code Analysis	静的スキャンののためにコードをアップロードする Visual Studio Code 拡張機能	Fortify Visual Studio Code 拡張機能のドキュメント

IDE ツール	説明	詳細情報
Fortify Security Assistant Plugin for Eclipse	コードの記述時に Java ファイルの潜在的なセキュリティの問題にアラートを表示する Eclipse プラグイン。[1] これには意味解析とクラス内データフローのアナライザーが含まれており、以下を検出します。 • 危険性が疑われる関数および API の使用 • 悪影響を与えるデータが、クラス内レベルの脆弱な関数および API に到達することで発生した問題。	Eclipse 用の Fortify セキュリティ アシスタント プラグインのドキュメント
Fortify Security Assistant Plugin for IntelliJ	コードの記述時に Java ファイルの潜在的なセキュリティの問題にアラートを表示する IntelliJ IDEA プラグイン。[1] これには構造および構成のアナライザーが含まれており、以下を検出します。 • 危険性が疑われる関数および API の使用 • プロパティおよび XML ファイルの安全でないアプリケーション構成	IntelliJ 用の Fortify セキュリティ アシスタント プラグインのドキュメント

IDE ツール	説明	詳細情報
Fortify Security Assistant Extension for Visual Studio	C# (.cs)、Razor (.cshtml)、WebForms (.aspx)、.config、.xml、および .ini ファイルにおける潜在的なセキュリティの問題にアラートを表示する Visual Studio 拡張機能。[1] これには構造および構成のアナライザーが含まれており、以下を検出します。 • 危険性が疑われる関数および API の使用 • 安全でないアプリケーション構成	Visual Studio 用の Fortify セキュリティ アシスタント拡張機能のドキュメント

[1] Fortify セキュリティ アシスタントには、問題をスキャンし、Fortify セキュリティ コンテンツをインストールまたは更新するための有効なライセンス ファイルが必要です。ライセンスは、すべての Fortify セキュリティ アシスタント バージョンで有効です。

1.10.3. スキャン準備および追跡ツール

静的スキャン用のアプリケーション ソース コードを準備するには、次のツールを使用します。

静的スキャン ツール	説明	詳細情報
OpenText SAST	C/C++ および Scala コードを変換してスキャン用にパッケージ化するための変換専用バージョンの OpenText SAST **Note** OpenText SAST には、ソース コードを変換するための有効なライセンス ファイルが必要です。	OpenText Static Application Security Testing and Tools のドキュメント
Fortify ABAP Extractor	ソース コード ファイルをプレゼンテーション サーバーにダウンロードするための SAP トランスポート要求	ABAP (SAP) アプリケーション ファイルの準備
Fortify ScanCentral SAST クライアント	ソース コードをパッケージ化するためのスタンドアロンの Fortify ScanCentral SAST クライアント	Fortify ScanCentral SAST
Fortify Audit Workbench	FPR ファイルを表示および監査するためのツール	OpenText Static Application Security Testing and Tools のドキュメント

動的スキャン用の Web アプリケーションを準備するには、次のツールを使用します。

動的スキャン ツール	説明	詳細情報
ワークフロー マクロ レコーダー	ワークフロー マクロを作成するためのスタンドアロン ユーティリティ	OpenText Dynamic Application Security Testing のドキュメント
ログイン マクロ レコーダー	ログイン マクロを作成するためのスタンドアロン ユーティリティ	OpenText Dynamic Application Security Testing のドキュメント

追跡ツール:

ツール	説明	詳細情報
Software Security Sync Utility	OpenText Fortify on Demand のアプリケーション、リリース、およびスキャンと Fortify Software Security Center (SSC) との間で自動化された同期およびスケジュールされた同期を実行するためのスタンドアロン ユーティリティ	GitHub
OpenText Fortify on Demand バグ トラッカー	OpenText Fortify on Demand の問題をバグ トラッカーに送信するためのスタンドアロン ユーティリティ	GitHub

1.10.4. ツールの表示およびダウンロード

OpenText Fortify on Demand により、利用可能なツールを表示およびダウンロードできます。

使用可能なツールを表示するには、次の手順を実行します。

1. アカウント名をクリックし、リストから [**ツール**] を選択します。

   [ツール] ページが表示されます。

2. インストーラー、ライセンス、および使用方法については、リンクをクリックしてください。

Note

ほとんどのツールの使用にはライセンスは必要ありません。次の条件に該当する場合は、サポートに連絡してライセンスを要求してください。

- OpenText SAST: C、C++、および Scala コードをスキャンする場合
- Fortify Audit Workbench: FPR ファイルを表示する場合
- Fortify セキュリティ アシスタント: アクティブな静的サブスクリプションがある場合

1.10.5. ポータルの統合

OpenText Fortify on Demand は、ポータルを通じて管理するさまざまな統合を提供しています。

このセクションでは、次のトピックについて説明します。

- バグ トラッカーの統合
- 外部スキャンの統合
- Secure Code Warrior の統合
- 通知のための Slack 統合
- ソース コントロールの統合
- 構成された統合の追跡
- Web フック

1.10.5.1. バグ トラッカーの統合

脆弱性の結果をバグ追跡ツールにリンクするテナントのために、OpenText Fortify on Demand では、次に示す最新バージョンのバグ トラッカーを統合できるようになっています。

- OpenText Application Quality Management (以前の ALM)
- OpenText Software Delivery Management Octane (以前の ALM Octane)
- Jira
- Bugzilla
- Azure DevOps/Azure DevOps Server

ユーザーはサポートされているバグ トラッカーに問題をバグとして送信し、ポータルからバグを直接管理することができます。サポートされていないバグ トラッカーの場合、ユーザーは手動でバグ トラッカー リンクを問題に追加できます。

このセクションでは、次のトピックについて説明します。

- バグ トラッカー統合の構成
- バグ トラッカーへの問題の送信
- 問題の手動リンク

1.10.5.1.1. バグ トラッカー統合の構成

バグ トラッカー統合はアプリケーション レベルで構成されます。OpenText Fortify on Demand とバグ トラッカー サーバーとの間の接続を確立する必要があります (VPN は接続を確立するためのオプションではありません)。サーバーには、バグを追加および終了するための専用ユーザー アカウントが必要です。

アプリケーションのバグ トラッカー統合を構成するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

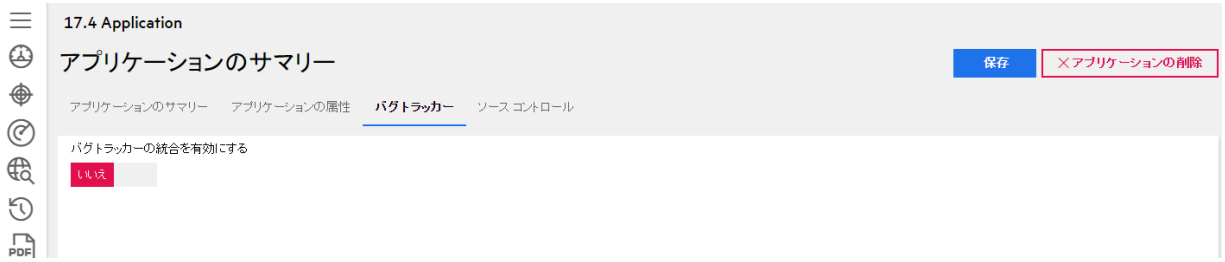
2. バグ トラッカー統合を構成するアプリケーションをクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [**設定**] をクリックします。

   [設定] ページが表示されます。

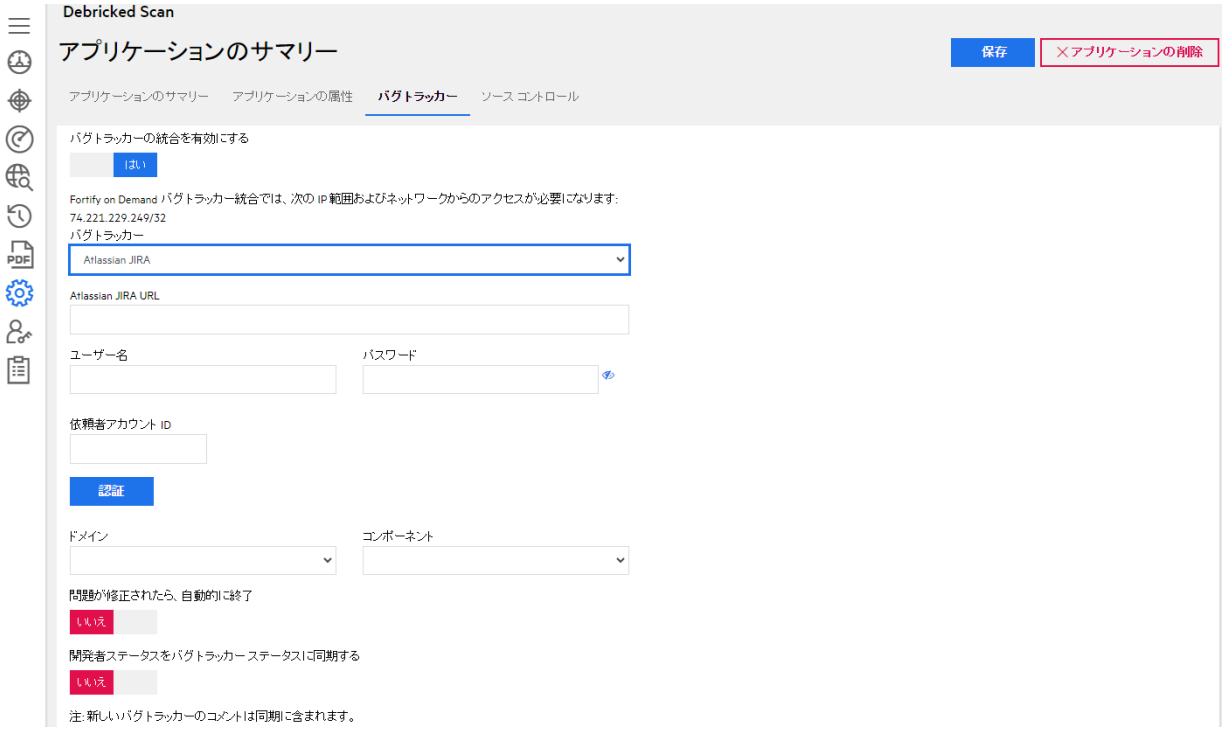
4. [**バグ トラッカー**] タブを選択します。



5. [**バグ トラッカーの統合を有効にする**] スライダーを [**いいえ**] から [**はい**] に移動してバグ トラッカー統合を有効にします。

6. [**バグ トラッカー**] リストからバグ トラッカーを選択します。

サポートされているバグ トラッカーを選択すると、追加のフィールドが下に表示されます。フィールド名は、選択されたバグ トラッカーに基づきます。



7. [**URL**] フィールドに、バグ トラッカー サイトの URL を入力します。
8. [**ユーザー名**] および [**パスワード**] フィールドに、バグ トラッカー サイトにログインするためのログイン資格情報を入力します。

   [レポーター] フィールドが必要なクラウド JIRA インスタンスがある場合は、提供された [**ユーザー名**] に関連付けられているユーザー ID を [**依頼者アカウント ID**] フィールドに入力します。

   Important

   Atlassian は、REST API のパスワードによる基本認証と Cookie ベースの認証について、サポートを終了しました。

   Microsoft は、REST API のパスワードによる基本認証について、サポートを終了しました。

9. [**認証**] をクリックします。

   認証が成功すると、「認証済み」メッセージが表示されます。バグ トラッカー サイトのカテゴリのリストも入力されます。

Tip

バグ トラッカーを認証できない場合、次のトラブルシューティングのヒントを参照してください。

- バグ トラッカー インスタンスが公的にアクセス可能であることを確認します。たとえば、Jira インスタンスのアクセシビリティは、コマンド `curl -D- -u <Jira_userid>:<Jira_password> http://<host>.atlassian.net/rest` を使用してテストできます。
- 適用可能な場合は、バグ トラッカー API を有効にします。
- バグ トラッカーへのログインに使用されるアカウントにバグ トラッカー API にアクセスするための権限があることを確認します。
- ファイアウォール、IPS、IDS、および WAF の許可リストに OpenText Fortify on Demand の IP アドレスを追加します。IP アドレスは [バグ トラッカー] タブに表示されます。

10. アプリケーションの問題を送信する既定のカテゴリを選択します。フィールドは、選択したバグ トラッカーに固有です。

    ValueEdge/ALM Octane: **プロジェクト**と**ワークスペース**

    ALM.Net: **ドメイン**と**プロジェクト**

    Jira: **プロジェクト**、**コンポーネント**

    Bugzilla: **製品**、**コンポーネント**

    Azure DevOps/Azure DevOps Server: **プロジェクト**

11. [**問題が修正されたら、自動的に終了**] スライダーを [**はい**] に移動して、バグの状態管理を有効にします。バグの状態管理を有効にすると、リンクされた問題が [**検証済みの修正**] または [**抑制済み**] としてマークされている場合、OpenText Fortify on Demand はバグを次の表に示されているステータスに自動的に設定します。複数の問題にリンクされているバグは、すべての問題が [**検証済みの修正**] または [**抑制済み**] にならない限り、終了しません。

バグ トラッカー	終了済みステータス
ALM Octane	修正済み (phase.defect.fixed)
ALM	固定
Jira	完了
Azure DevOps/Azure DevOps Server	解決済み
ALM.Net	修正済み (phase.defect.fixed)
Bugzilla	ステータス: 解決済み、解決: 修正済み

Note

OpenText Fortify on Demand は、再発した問題にリンクしているバグを再オープンしません。

12. (Azure DevOps および JIRA で利用可能) [バグの状態管理] が有効になっている場合は、[**開発者ステータスをバグ トラッカー ステータスに同期する**] スライダーを [**はい**] に移動して、OpenText Fortify on Demand の [**開発者ステータス**] の値をバグ トラッカー ステータスの値と同期します。バグ トラッカー ステータスの値を [**開発者ステータス**] の値にマッピングします。

Note

[**開発者ステータス**] はバグ トラッカー ステータスの値と自動的に同期されるため、送信された問題の [**開発者ステータス**] フィールドは OpenText Fortify on Demand で編集できなくなります。新しいバグ トラッカーのコメントが同期に含まれます。

13. (Azure DevOps で利用可能) バグを送信するときにカスタム フィールドの既定値を指定します。該当する場合は、Azure DevOps からの既定値が設定されます。赤色でマークされたカスタム フィールドは入力が必須です。

    フィールド値を Azure DevOps の既定値にリセットするには、フィールドをクリアします。

14. [**保存**] をクリックします。

    バグ トラッカー設定が保存されます。

1.10.5.1.2. バグ トラッカーへの問題の送信

アプリケーションのバグ トラッカー統合が構成されると、アプリケーション アクセスおよび問題の編集権限を持つユーザーは、OpenText Fortify on Demand 問題をバグとしてバグ トラッカーに送信することができます。このポータルでは、同じ問題は複数回送信されません。

問題をバグ トラッカーに送信するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. バグ トラッカーに送信する問題があるアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [アプリケーションの問題] ページまたは [リリースの問題] ページに移動します。

   - [アプリケーションの問題] ページに移動するには、次の手順を実行します。

     1. [**問題**] をクリックします。

        [アプリケーションの問題] ページが表示されます。

   - [リリースの問題] ページに移動するには、次の手順を実行します。

     1. リリース名をクリックします。
     2. [**問題**] をクリックします。

[リリースの問題] ページが表示されます。

4. ナビゲーション パネルで、送信する問題を 1 つ以上選択します。問題を一括送信するには、編集する問題の横にあるチェック ボックスを選択します。

> **Note**
> [アプリケーションの問題] ページで、複数のリリースで見つかった問題の横にあるチェック ボックスを選択すると、問題のすべてのインスタンスが選択されます。

5. 監査パネルで [**バグを送信**] をクリックします。

   [バグを <bug_tracker> に送信] ウィンドウが開きます。フィールドには、問題の概要を含む既定値が入力されています。必要に応じて、既定値を編集します。

6. OpenText Fortify on Demand は、ALM、Jira、および Azure DevOps のカスタム フィールドをサポートします。バグ トラッカーにカスタム フィールドが含まれている場合、それらのフィールドは [**カスタム値 (必須)**] セクションに表示されます。フィールドに入力します。

7. [**送信**] をクリックします。

   [問題] ページに戻ります。問題の送信が保留中の場合、監査パネルに [**バグ保留中**] ステータスが表示されます。問題の送信が完了すると、監査パネルに、問題のバグ トラッカー URL にリンクする [**バグを参照**] ボタンが表示されます。

Note

リリースがコピーされると、バグ トラッカー内の問題が更新されます。新しくコピーされた問題へのリンクが、バグ トラッカー内の問題の説明に追加されます。

1.10.5.1.3. 問題の手動リンク

ポータルで問題へのバグ トラッカー リンクを手動で追加できます。これにより、他のバグ トラッカーを使用するテナントが OpenText Fortify on Demand の問題に関連付けられている外部のバグを追跡できるようになります。

OpenText Fortify on Demand 問題をサポートされていないバグ トラッカーとリンクするには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. バグ トラッカーに送信する問題があるアプリケーションの名前をクリックします。

   [アプリケーションの概要] ページが表示されます。

3. [アプリケーションの問題] ページまたは [リリースの問題] ページに移動します。

   - [アプリケーションの問題] ページに移動するには、次の手順を実行します。

     1. [**問題**] をクリックします。

        [アプリケーションの問題] ページが表示されます。

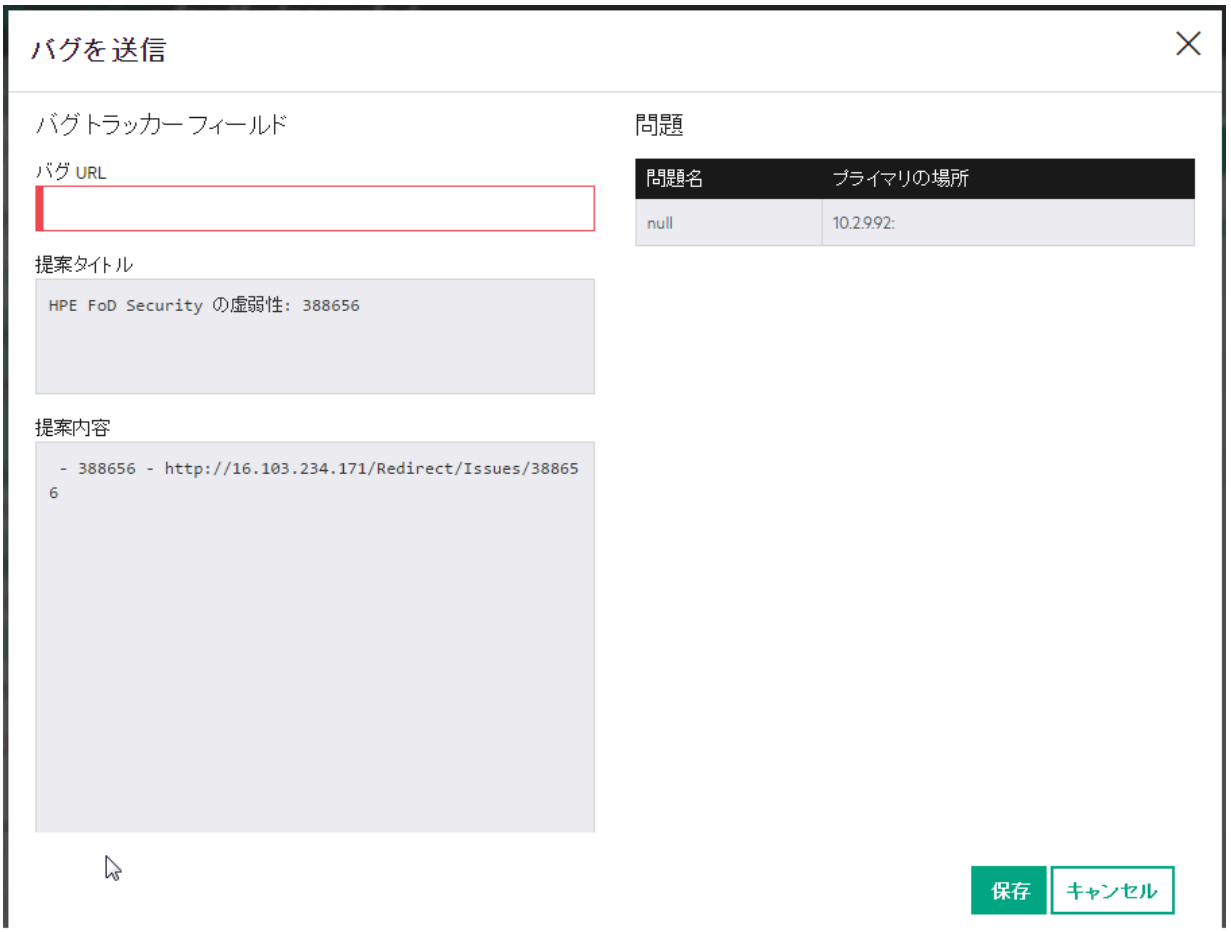
   - [リリースの問題] ページに移動するには、次の手順を実行します。

     1. リリース名をクリックします。
     2. [**問題**] をクリックします。

[リリースの問題] ページが表示されます。

4. ナビゲーション パネルで、送信する問題を 1 つ以上選択します。問題を一括送信するには、編集する問題の横にあるチェック ボックスを選択します。
5. [**バグを送信**] をクリックします。

   [バグを送信] モーダル ウィンドウが表示されます。



6. [**バグ URL**] フィールドで、問題に追加するバグ トラッカー リンクを入力します。
7. [**保存**] をクリックします。

   問題の送信が完了すると、監査パネルに、問題のバグ トラッカー URL にリンクする [**バグを参照**] ボタンが表示されます。

1.10.5.2. 外部スキャンの統合

外部ソースからのスキャン結果を OpenText Fortify on Demand にインポートして、複数ソースからのスキャン結果を 1 つのビューで管理できます。OpenText Fortify on Demand は次のスキャン タイプのインポートをサポートします。

- オンプレミスの OpenText SAST と OpenText DAST のスキャン結果
- CycloneDX 1.4、1.5、1.6、および 1.7 標準に準拠したオープン ソース スキャン結果

このセクションでは、次のトピックについて説明します。

- オンプレミス スキャンのインポート
- ソフトウェア部品表のインポート
- インポート済みスキャンの削除

1.10.5.2.1. オンプレミス スキャンのインポート

オンプレミスの OpenText SAST と OpenText DAST のスキャン結果を OpenText Fortify on Demand にインポートできます。FPR または SARIF のインポート時:

- スキャンの開始と完了の時間には、FPR または SARIF のスキャン日付が使用されます。
- グローバル監査テンプレートおよびアプリケーション監査テンプレートが適用されます。
- OpenText SAST または OpenText DAST によって提供されるインスタンス ID を使用して、インポートされた FPR または SARIF 全体の問題を追跡します。OpenText Fortify on Demand は重複する FPR または SARIF をチェックしません。

  たとえば、FPR または SARIF を空のリリースにインポートすると、インポートされたすべての問題のステータスは [**新規**] になります。同じ FPR または SARIF を再度インポートすると、すべての問題のステータスは [**新規**] から [**既存**] に変わります。別の FPR または SARIF をインポートすると、問題のステータスは次のように変わります。

  - リリースと最新の FPR または SARIF の両方に存在する問題のステータスは、[**既存**] になります。
  - 最新の FPR または SARIF にのみ存在する問題のステータスは、[**新規**] になります。
  - リリースに存在し、最新の FPR または SARIF に存在しない問題のステータスは [**固定**] になります。
- リリースに存在しない FPR または SARIF の抑制済みの問題はインポートされ抑制されます。リリースに存在する FPR または SARIF の問題については、抑制ステータスは無視されます。

Note

最後に完了した同じタイプのスキャンよりも日付が古いスキャンの FPR または SARIF は受け入れられません。

静的 FPR、動的 FPR、または静的 SARIF をインポートするには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. FPR または SARIF をインポートするリリースをクリックします。

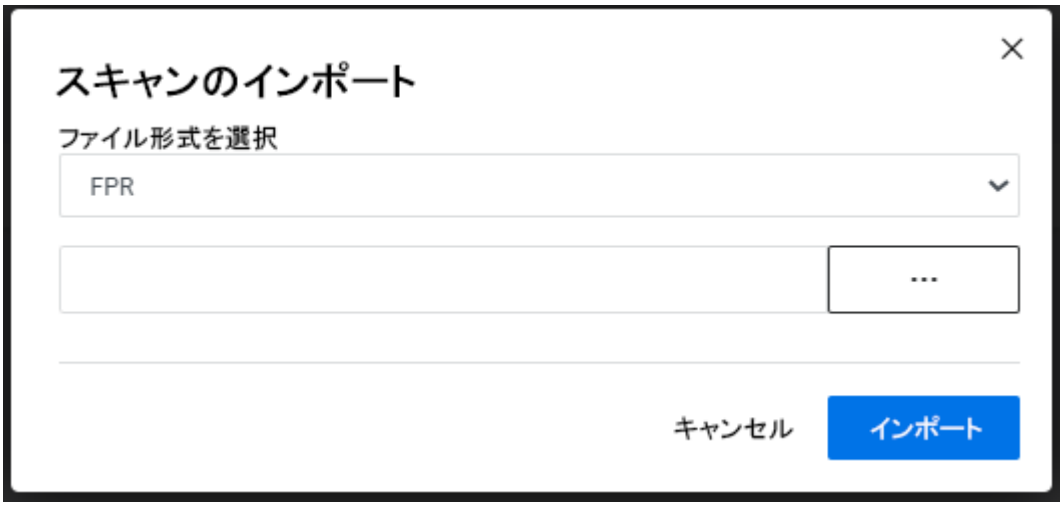
   [リリースの概要] ページが表示されます。

4. [**スキャン**] をクリックします。

   [**リリース スキャン**] ページが表示されます。

5. **[スキャンのインポート] > [動的 | 静的]** を選択します。

   [スキャンのインポート] ウィンドウが開きます。



6. ファイル形式として FPR または SARIF を選択します。

> **Note**
> SARIF ファイルのサポートは、静的スキャン タイプでのみ利用できます。

7. [...] をクリックし、FPR ファイルまたは SARIF ファイルに移動して選択します。

8. [**次へ**] をクリックします。

   インポートが完了すると、結果が [問題] ページに表示されます。スキャンが [リリース スキャン] ページに表示され、ステータスは [完了] になり、評価タイプは [WebInspect (インポート済み)] (OpenText SAST の場合) または [SCA (インポート済み)] (OpenText SAST の場合) になります。

1.10.5.2.2. ソフトウェア部品表のインポート

[**アプリケーションの管理**] 権限を持つユーザーは、サード パーティからのオープン ソース スキャン結果 (ソフトウェア部品表 (SBOM) と呼ばれる) をインポートできます。SBOM をインポートするには、次の要件を満たしている必要があります。

- SBOM が CycloneDX 1.4、1.5、1.6、および 1.7 標準に準拠する JSON ファイルである。
- SBOM で `metadata` オブジェクトの下に単一の `tools` エントリが含まれている。
- SBOM のバージョンが、最近インポートされた SBOM のバージョンよりも新しい。

ソフトウェア部品表をインポートするには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. オープン ソース スキャンをインポートするリリースをクリックします。

   [リリースの概要] ページが表示されます。

4. [**スキャン**] をクリックします。

   [リリース スキャン] ページが表示されます。

5. **[スキャンのインポート] > [オープン ソース]** を選択します。

   [オープン ソース スキャンをインポート] ウィンドウが開きます。

6. [...] をクリックし、SBOM に移動して選択します。
7. SBOM に対するオープン ソース スキャンを送信する場合、[**Debricked スキャンを実行して、脆弱性とライセンス情報を追加します**] を選択します。SBOM をインポートすると、1 つの OpenText Core SCA の使用権が、1 つの OpenText Core SCA サブスクリプションに使用されます。このサブスクリプションは、アプリケーションの配下にインポートされた SBOM のスキャンに有効です。

   Note

   必要な場合は、オープン ソース スキャンを後で送信することもできます。[スキャン] ページで、インポートした SBOM を探し、[**Debricked に送信**] を選択します。

8. [**次へ**] をクリックします。

   インポートが完了すると、結果が [問題] ページに表示されます。スキャンが [リリース スキャン] ページに表示され、ステータスは [完了] になり、評価タイプは [<toolName> (インポート済み)] になります。

1.10.5.2.3. インポート済みスキャンの削除

アプリケーションの管理権限があるユーザーは、インポート済みのスキャン結果ファイルを削除できます。同じタイプの後続のスキャンがインポートされている場合は、スキャンを削除できません。

インポート済みスキャンを削除するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. 前回インポートされたスキャンを削除するアプリケーションの名前をクリックします。

   [アプリケーション リリース] ページが表示されます。

3. [**スキャン**] をクリックします。

   [アプリケーション スキャン] ページが開き、アプリケーションに対して実行されたスキャンが表示されます。

> **Note**
> リリースに対して実行されたスキャンのみが表示されるようにスキャンリストをフィルタリングするには、[アプリケーション リリース] ページからリリースの名前をクリックします。

4. インポート済みスキャンのアクション列で [**インポート済みスキャンをキャンセル**] をクリックします。

   確認メッセージが表示されます。

5. [**はい**] をクリックして、スキャンのキャンセルを確定します。

   スキャンとスキャンに関連付けられたすべての問題が削除されます。

1.10.5.3. Secure Code Warrior の統合

OpenText Fortify on Demand は Secure Code Warrior と連携して、サポート対象の脆弱性カテゴリについて無料のインタラクティブ トレーニングを OpenText Fortify on Demand 顧客に提供しています。問題を表示すると、ユーザーは [問題の詳細] パネルの [**推奨事項**] タブの [**ローンチ トレーニング**] リンクからトレーニング モジュールを開始できます。

モジュールは短い実践的な課題から構成されています。ここでユーザーはソフトウェア設計やコードの脆弱性を分析し、脆弱性を修復または緩和します。Secure Code Warrior でサポートされるすべての脆弱性カテゴリのサンプル モジュールが用意されています。モジュールは、カテゴリ、サブカテゴリ、および言語の階層で編成されています。

OpenText Fortify on Demand では、ユーザーおよび組織情報は Secure Code Warrior と共有されません。追加のトレーニングは Secure Code Warrior から購入できます。詳細については、https://www.securecodewarrior.com/ を参照してください。

1.10.5.3.1. Secure Code Warrior トレーニングの開始

Secure Code Warrior トレーニングを開始するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

   [アプリケーション] ページが表示されます。

2. [**ご使用のリリース**] をクリックします。

   [ご使用のリリース] ページが表示されます。

3. リストからリリースを選択します。

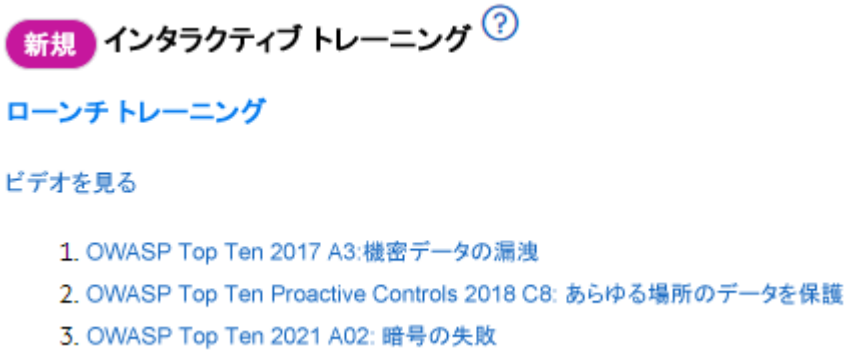
4. [**問題**] をクリックします。

   [リリースの問題] ページが表示されます。

5. ナビゲーション パネルで、Secure Code Warrior のトレーニングを使用できる問題カテゴリの中から問題を選択します。

6. [**推奨事項**] タブを選択します。

7. [**インタラクティブ トレーニング**] セクションでは、次のタスクを実行できます。
    - トレーニング モジュールを開始するには、[**ローンチ トレーニング**] をクリックします。
    - 問題カテゴリに関するビデオを閲覧するには、[**ビデオを見る**] をクリックします。
    - 問題カテゴリの詳細については、外部の教育リソースへのリンクをクリックしてください。



Note

問題がサポートされている脆弱性カテゴリに属していない場合は、Secure Code Warrior のホーム ページにリダイレクトされます。

1.10.5.4. 通知のための Slack 統合

OpenText Fortify on Demand は、Slack に通知を投稿するための Slack 統合を提供します。セキュリティ リーダーは、テナント用に 1 つ以上の Web フックを設定することができます。Web フックが設定されると、セキュリティ リーダーは通知サブスクリプションを作成するときに Slack に通知を投稿することができます。

このセクションでは、次のトピックについて説明します。

- Slack 統合の構成
- Slack 統合の削除

1.10.5.4.1. Slack 統合の構成

テナント用に 1 つ以上の Web フックを設定することにより、Slack 統合を構成できます。

Web フックを設定するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**統合**] をクリックします。

   [**統合**] ページが表示されます。

3. [**Slack**] セクションを展開します。

4. [**統合の追加**] をクリックします。

   - 現在ワークスペースにサインインしていない場合は、Slack ワークスペースのサインイン ページにリダイレクトされます。

- 現在 1 つ以上のワークスペースにサインインしている場合は、認証ページにリダイレクトされます。

> **Note**
>
> ワークスペースのアプリと統合を管理する権限が必要です。

5. 接続するワークスペースにサインインしていない場合は、サインインのプロセスを完了します。サインインしている場合は、次の手順に進みます。
6. まだワークスペースを選択していない場合は、認証ページの右上にあるリストから選択します。

7. 通知が投稿されるチャンネルまたはユーザーのダイレクト メッセージを選択します。使用可能な値は、アクセス権のあるチャンネルとユーザー アカウントです。
8. [**承認**] をクリックして OpenText Fortify on Demand が Slack アカウントにアクセスすることを承認します。

   OpenText Fortify on Demand にリダイレクトされます。「Slack 統合に成功しました (Integration Successful)」というメッセージが表示されます。これで、チャンネルに通知を投稿できるようになりました。Slack への通知の投稿の有効化の詳細については、「独自サブスクリプションの作成」および「グローバル サブスクリプションの作成」を参照してください。

1.10.5.4.2. Slack 統合の削除

OpenText Fortify on Demand の Slack 統合は次の方法で削除できます。

- Slack ワークスペースの所有者およびアプリを管理する権限を持つユーザーは、特定の認証を削除したり、Slack ワークスペースから OpenText Fortify on Demand アプリケーションを削除したりすることができます。それによって Slack への投稿が失敗します。
- セキュリティ リーダーは、OpenText Fortify on Demand の Web フックを削除することができます。

Slack 統合を削除するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**統合**] をクリックします。

   [**統合**] ページが表示されます。

3. [**Slack**] セクションを展開します。

4. 基本設定とユーザー権限に応じて、次のタスクを実行します。
   - Slack の認証を削除するには、次の手順を実行します。
     1. Web フックの行で をクリックします。

        ワークスペース アプリのディレクトリの「OpenText Fortify on Demand」ページにリダイレクトされます。

        > **Note**
        >
        > このページには Slack ワークスペースからもアクセスすることができます。

     2. 特定の認証を削除するか、アプリケーションを削除してすべての認証を削除します。Slack からのアプリケーションの削除の詳細については、Slack ドキュメントの「Remove apps and custom integrations from your workspace」を参照してください。
   - OpenText Fortify on Demand で Web フックを削除するには、次の手順を実行します。
     1. Web フックの行で をクリックします。

        Web フックが削除されます。

1.10.5.5. ソース コントロールの統合

> **Important**
>
> ポータルを介したソース コントロールの統合は、レガシー統合です。この機能は廃止される予定です。既存のユーザーは、なるべく早く、ソース コントロールの統合を、該当するバージョン コントロール プラットフォーム上のパイプラインに移行する必要があります。Fortify では、Bitbucket、GitHub、GitLab など、さまざまなバージョン コントロール プラットフォーム用のパイプライン テンプレートが提供されています。詳細については、「CICD ツール」を参照してください。

OpenText Fortify on Demand では、GitHub および Bitbucket 用のポータルを介したソース コントロールの統合を提供しています。これにより、OpenText Fortify on Demand は、これらのプラットフォームのリポジトリからソース コードを取得して静的評価を行うことができます。

サポートされる言語は、Java、JavaScript、.NET、PHP、Python です。OpenText Fortify on Demand にアップロードするコードを準備するための要件は、「静的評価ファイルの準備」で説明されている要件と同じです。.NET および Java の場合は、ファイルを事前コンパイルしてリリースにアップロードし、ペイロードの受け入れを確認する必要があります。

ソース コントロール統合はアプリケーション レベルで構成されます。構成が完了したら、ユーザーは静的評価の開始時に、アップロードするブランチまたはリリースを選択できます。

このセクションでは、次のトピックについて説明します。

- Bitbucket とのソース コントロールの統合の構成
- GitHub とのソース コントロールの統合の構成

1.10.5.5.1. Bitbucket とのソース コントロールの統合の構成

Important

ポータルを介したソース コントロールの統合は、レガシー統合です。この機能は廃止される予定です。既存のユーザーは、なるべく早く、ソース コントロールの統合を、該当するバージョン コントロール プラットフォーム上のパイプラインに移行する必要があります。Fortify では、Bitbucket、GitHub、GitLab など、さまざまなバージョン コントロール プラットフォーム用のパイプライン テンプレートが提供されています。詳細については、「CICD ツール」を参照してください。

Bitbucket 統合では、Bitbucket の OAuth コンシューマーを追加する必要があります。

Bitbucket とのソース コントロールの統合を構成するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

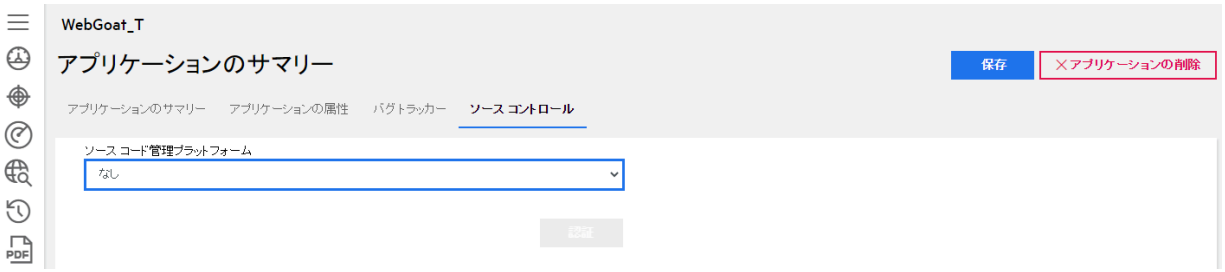
   [アプリケーション] ページが表示されます。

2. 編集するアプリケーションの名前をクリックします。

3. [**設定**] をクリックします。

   [アプリケーションのサマリー] ページが表示されます。

4. [**ソース コントロール**] タブを選択します。



5. [**ソース コード管理プラットフォーム**] リストから [**Bitbucket**] を選択します。

6. [**クライアント キー**] フィールドと [**クライアント シークレット**] フィールドに、Bitbucket で生成された OAuth コンシューマーのキーとシークレットを入力します。

   キーとシークレットを生成するには、Bitbucket の OAuth コンシューマーを追加します。コンシューマーを構成するとき、以下の作業を実行してください。

- コールバック URL を `https://<fod_domain>/Redirect/OAuth/` に設定します。ここで、`<fod_domain>` は OpenText Fortify on Demand のドメインおよびスキーマです。
  - US: `ams.fortify.com`
  - EMEA: `emea.fortify.com`
  - APAC: `apac.fortify.com`
  - FedRAMP: `fed.fortifygov.com`
- アカウント、ワークスペース メンバーシップ、プロジェクト、およびリポジトリに読み取り権限を割り当てます。

Bitbucket の OAuth コンシューマーの追加の詳細については、Bitbucket ドキュメントの「Integrate another application through OAuth」セクションを参照してください。

> **Tip**
>
> ワークスペースの OAuth コンシューマー設定で [**これはプライベート コンシューマーです**] チェック ボックスがオンになっていることを確認してください。

7. [**認証**] をクリックします。

   認証に成功すると、Bitbucket サイトにリダイレクトされます。

8. 自分のアカウントに OpenText Fortify on Demand アプリケーションがアクセスすることを承認します。

   [**チーム**] フィールドと [**リポジトリ**] フィールドにデータが入力されています。[**チーム**] フィールドには、自分のユーザー アカウントと、アクセス先のリポジトリのすべてのチームが表示されます。

9. アプリケーションにリンクするリポジトリを所有するチームを [**チーム**] リストから選択します。
10. リポジトリを [**リポジトリ**] リストから選択します。
11. [**保存**] をクリックします。

    ソース コントロールの統合の設定が保存されます。

1.10.5.5.2. GitHub とのソース コントロールの統合の構成

Important

ポータルを介したソース コントロールの統合は、レガシー統合です。この機能は廃止される予定です。既存のユーザーは、なるべく早く、ソース コントロールの統合を、該当するバージョン コントロール プラットフォーム上のパイプラインに移行する必要があります。Fortify では、Bitbucket、GitHub、GitLab など、さまざまなバージョン コントロール プラットフォーム用のパイプライン テンプレートが提供されています。詳細については、「CICD ツール」を参照してください。

GitHub 統合では、各データ センターに固有の OpenText Fortify on Demand Github マーケットプレース アプリケーションを使用します。GitHub Enterprise とのソース コントロールの統合は利用できません。

GitHub とのソース コントロールの統合を構成するには、次の手順を実行します。

1. [**アプリケーション**] ビューを選択します。

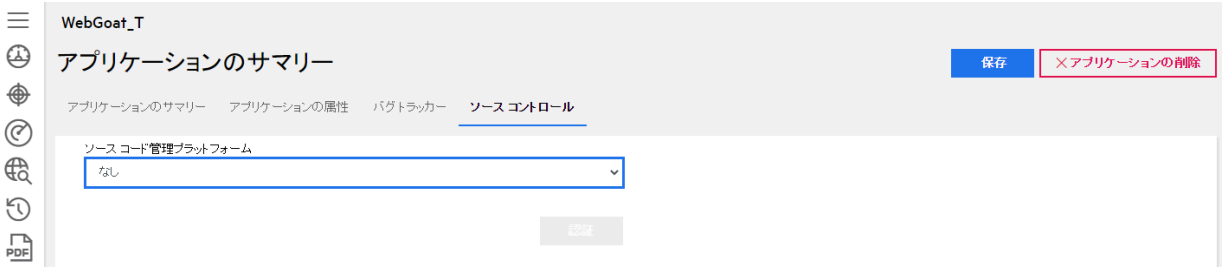
   [アプリケーション] ページが表示されます。

2. 編集するアプリケーションの名前をクリックします。

3. [**設定**] をクリックします。

   [アプリケーションのサマリー] ページが表示されます。

4. [**ソース コントロール**] タブを選択します。



5. [**ソース コード管理プラットフォーム**] リストから [**Github**] を選択します。

6. [**認証**] をクリックします。

   認証に成功したら、GitHub サイトにリダイレクトされます。

7. 自分のアカウントに OpenText Fortify on Demand アプリケーションがアクセスすることを承認します。

[**組織**] フィールドと [**リポジトリ**] フィールドにデータが入力されています。[**組織**] フィールドには、自分のユーザー アカウントと、アクセス先のリポジトリのすべての組織が表示されます。

8. アプリケーションにリンクするリポジトリを所有する組織を [**組織**] リストから選択します。
9. リポジトリを [**リポジトリ**] リストから選択します。
10. [**保存**] をクリックします。

    ソース コントロールの統合の設定が保存されます。

1.10.5.6. 構成された統合の追跡

セキュリティ リーダーは、外部ツールを使用して OpenText Fortify on Demand 内のすべてのアプリケーションでユーザーが構成した統合を追跡できます。現在、追跡可能な統合はバグ トラッカー、ソース コントロール、および Slack です。

テナント全体でユーザーが構成した統合を追跡するには、次の手順を実行します。

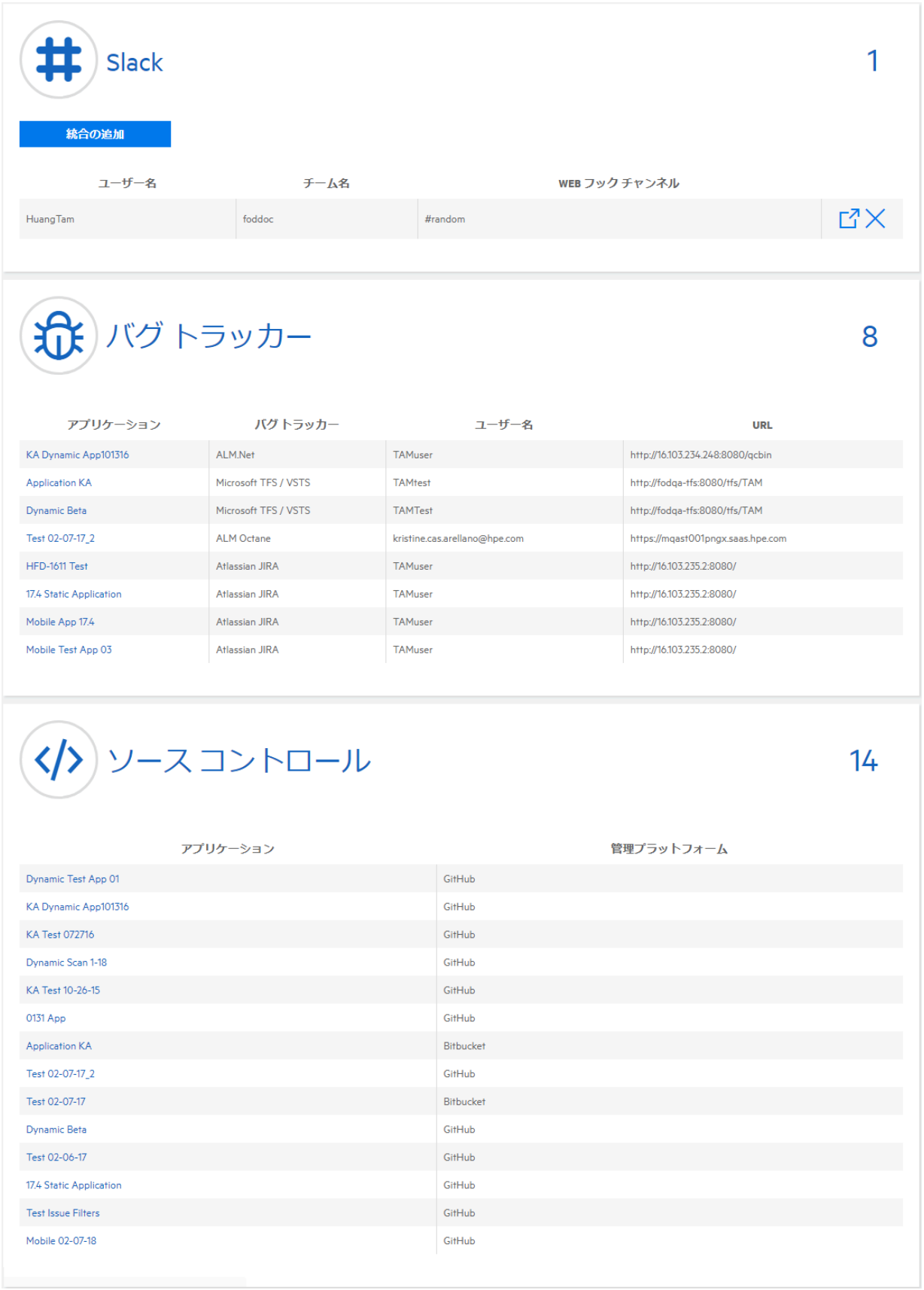
1. [**管理**] ビューを選択します。

   [**ユーザー管理**] ページが表示されます。

2. [**統合**] をクリックします。

   [**統合**] ページが表示されます。

3. 表示するセクションを展開します。



4. 次の操作を実行できます。

   - Slack: Web フックの行にあるリンクをクリックして特定の認証を削除するか、Web フックを削除します。詳細については、「Slack 統合の削除」を参照して

ください。

- バグ トラッカー: アプリケーション行のリンクをクリックすると、アプリケーションのバグ トラッカー設定にリダイレクトされます。詳細については、「バグ トラッカー統合の構成」を参照してください。
- ソース コントロール: アプリケーション行のリンクをクリックすると、アプリケーションのソース コントロール設定にリダイレクトされます。詳細については、「ソース コントロールの統合」を参照してください。

1.10.5.7. Web フック

Web フックを使用すると、スキャン イベントが発生したときに、外部 Web サーバーに通知を送信できます。[**Web フックの構成**] 権限を保有するユーザーは、登録しているイベントが発生したときに、Web フックをトリガーするように構成できます。スキャンの開始、スキャンの一時停止、スキャンの再開、スキャンのキャンセル、スキャンの完了の各イベントを利用できます。Web フックが登録されているイベントが発生すると、OpenText Fortify on Demand は Web フックに構成されている URL に HTTP POST ペイロードを送信します。Web フックは、スキャンを組み込む CICD パイプラインのポーリングの代わりに使用できます。

このセクションでは、次のトピックについて説明します。

- Web フックの構成
- Web フックの要求と応答
- Web フックの配信の表示

1.10.5.7.1. Web フックの構成

[**Web フックの構成**] 権限を保有するユーザーは、テナントに Web フックを構成できます。Web フックは、少なくとも 1 つのリリースに割り当てる必要があります。

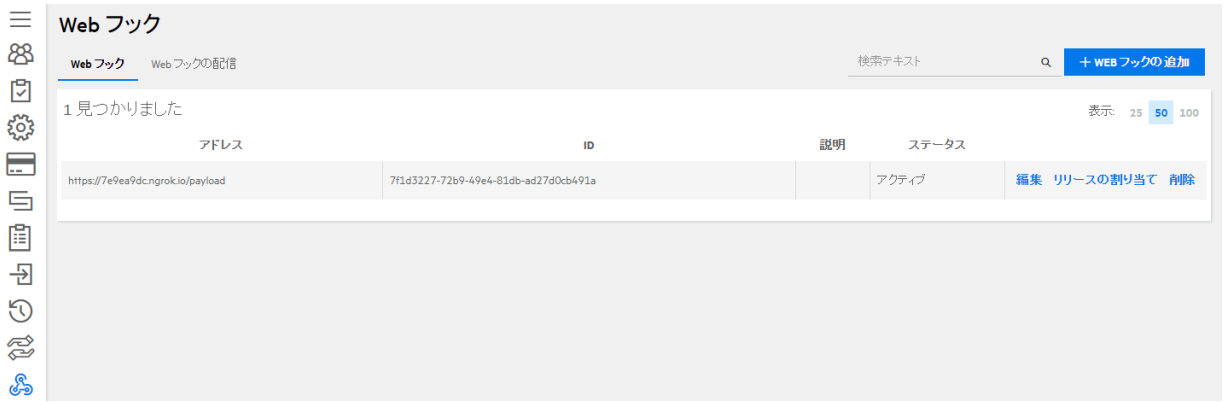
Web フックを設定するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**Web フック**] をクリックします。

   [Web フック] ページが表示されます。



3. [**Web フックを追加**] をクリックします。

   [Web フックの追加/編集] ウィンドウが表示されます。

4. 必要に応じてフィールドに入力します。他に指示がない限り、フィールドは必須です。

フィールド	説明
ペイロード URL	Web フックの POST 要求を受信するサーバーの URL を入力します。たとえば `https://7e9ea9dc.ngrok.io/payload` です。
説明	(オプション) Web フックを説明する語句を入力します。
シークレット	(オプション) ペイロード URL に送信された Web フックの要求が OpenText Fortify on Demand からのものであることを検証するために使用できるシークレットを入力します。HMAC-SHA256 アルゴリズムは、ペイロード本文のハッシュを計算するためにシークレットと組み合わせて使用されます。出力は HMAC で、要求のヘッダーに `X-FOD-Signature` として含まれます。 **Tip** Web フック要求を検証するには、シークレットと組み合わせて HMAC-SHA256 アルゴリズムを使用して生ペイロード本文をハッシュし、そのハッシュを 16 進数エンコードでエンコードすることによって HMAC を計算します。出力が `X-FOD-Signature` の値と一致することを確認します。

フィールド	説明
すべてのアプリケーション リリースの監視	◦ [**はい**] に設定すると、すべてのアプリケーション リリースを監視します。 ◦ [**いいえ**] に設定すると、個々のリリースを監視します (既定)。監視するリリースは、Web フックを構成した後に指定できます。
アクティブ	◦ [**はい**] に設定すると、Web フックの要求の送信が有効になります (既定)。 ◦ [**いいえ**] に設定すると、Web フックの要求の送信が無効になります。

5. Web フックをトリガーするスキャン イベントを選択します。
6. [**Web フックのテスト**] をクリックして、ペイロード URL を ping します。

   Web フックが正しく構成されている場合は、「ping イベントが正常に送信されました」というメッセージが表示されます。
7. [**保存**] をクリックします。

   新しい Web フックが Web フックのリストに表示されます。

   Note

   Web フックは、アドレス、説明、およびフル ID で検索できます。部分文字列の一致は、アドレスと説明でサポートされています。
8. 個々のリリースの監視を選択した場合は、Web フックの行で [**編集**] をクリックします。

   [リリースの割り当て] ウィンドウが表示されます。

9. Web フックが監視するリリースを選択して、[**保存**] をクリックします。

   これで、選択したリリースに Web フックが割り当てられます。

1.10.5.7.2. Web フックの要求と応答

OpenText Fortify on Demand は、JSON ペイロードを要求の本文とする HTTP POST 要求として Web フックのイベントに関する情報を送信します。

Note

SSL 検証は、デフォルトで有効になっています。ペイロードの URL が HTTPS の場合、OpenText Fortify on Demand は Web フック要求を送信する際に SSL 証明書を確認します。

要求の例

次に、ヘッダーにハッシュ署名 (`X-FOD-Signature`) と JSON ペイロードを含む要求の例を示します。

ヘッダー:

```
connection: close expect: 100-continue content-length: 324 host:
webhook.site content-type: application/json; charset=utf-8 x-
fod-signature:
4F837B0AE04303E975BBCF9FFBBC09E0016013835757BD611C20F7930711980F
x-fod-deliveryid: f8d97b5e-4cae-414b-aa84-8de766f8116f
```

ペイロード:

```
{ "deliveryId": "f8d97b5e-4cae-414b-aa84-8de766f8116f",
"eventName": "scan_started", "payload": { "scanId": 31278,
"tenantId": 1126, "applicationId": 14155, "applicationName":
"Zero", "releaseId": 16149, "releaseName": "v1", "scanType":
"dynamic" }, "webhookId": "a798dc91-3242-4dc6-8188-
2fd3e4aae86e", "triggeredAt": "2021-07-02T16:08:28.5496187Z" }
```

応答の例:

次に、OpenText Fortify on Demand が受信する応答の例を示します。

```
Transfer-Encoding = chunked Vary = Accept-Encoding X-Request-Id
= e9cbce0c-108f-46e9-b2cc-89f6f0104dca X-Token-Id = 89be42d3-
a8dd-4414-9e31-6b09a5590ee5 Cache-Control = no-cache, private
Date = Fri, 02 Jul 2021 16:08:29 GMT Set-Cookie =
laravel_session=CRuQJLoiFx9ay1UV88ufH83vCOjq1PL0JNOwY59v;
expires=Fri, 02-Jul-2021 18:08:29 GMT; Max-Age=7200; path=/;
httponly Server = nginx/1.14.2
```

1.10.5.7.3. Web フックの配信の表示

[**Web フックの構成**] 権限を保有するユーザーは、HTTP 要求 (ペイロードを含む) およびその応答などの Web フックの配信の詳細を表示できます。

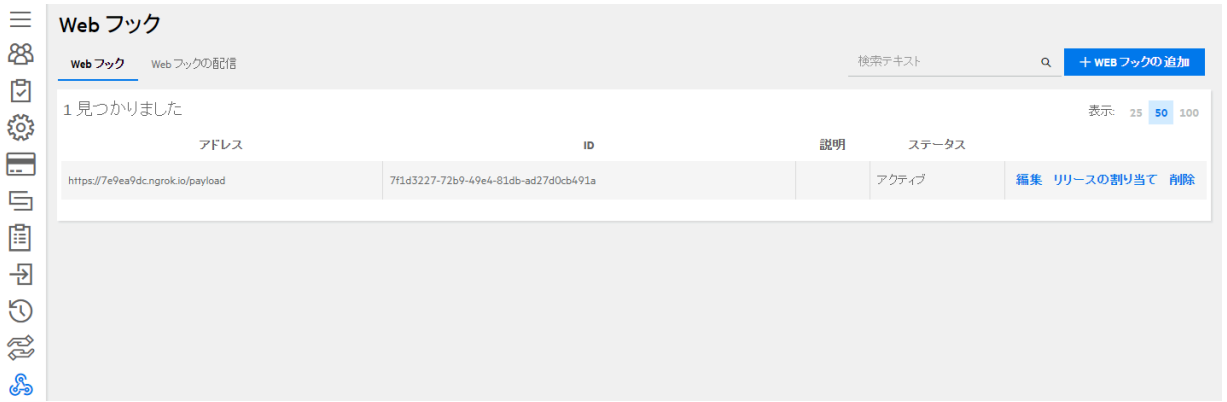
Web フックの配信のリストを表示するには、次の手順を実行します。

1. [**管理**] ビューを選択します。

   [ユーザー管理] ページが表示されます。

2. [**Web フック**] をクリックします。

   [Web フック] ページが表示されます。



3. [**Web フック配信**] タブを選択します。

   Web フック配信のリストが表示されます。

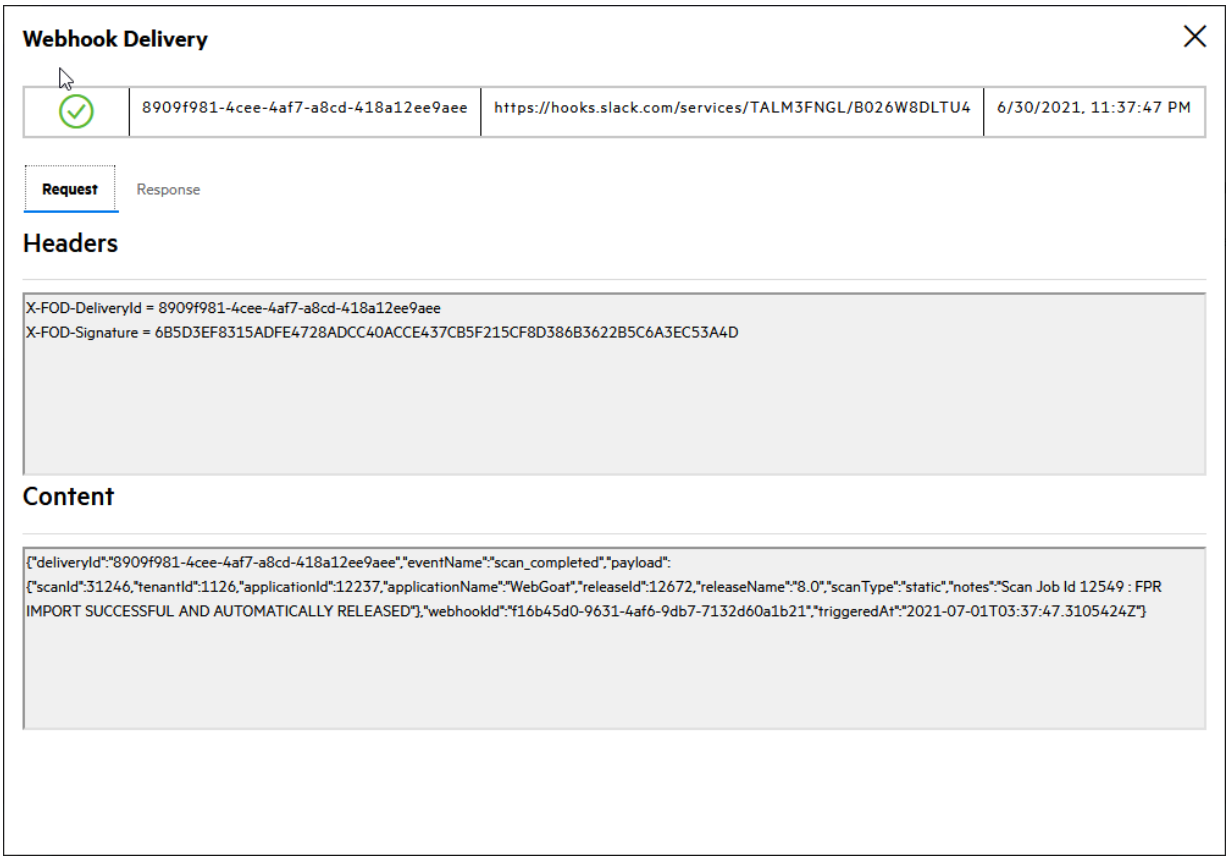
Note

Web フックの配信は、アドレス (部分文字列一致がサポートされます) とフル ID によって検索できます。

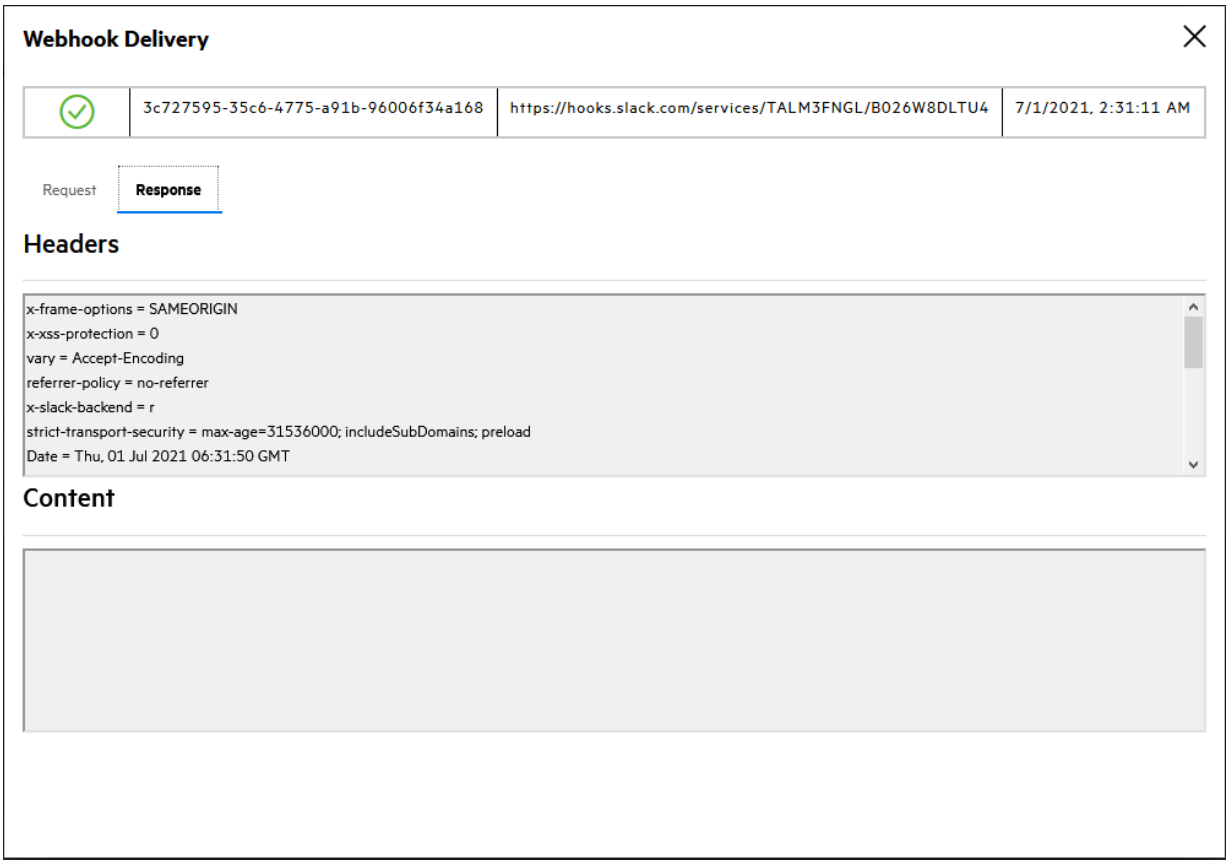
4. Web フックの行で [**詳細**] をクリックします。

   HTTP 要求およびその応答を含む [Web フック配信] ウィンドウが表示されます。

   要求:



   応答:


Webhook Delivery
3c727595-35c6-4775-a91b-96006f34a168
https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4
7/1/2021, 2:31:11 AM
Request
Response
Headers
x-frame-options = SAMEORIGIN
x-xss-protection = 0
vary = Accept-Encoding
referrer-policy = no-referrer
x-slack-backend = r
strict-transport-security = max-age=31536000; includeSubDomains; preload
Date = Thu, 01 Jul 2021 06:31:50 GMT
Content

1.10.6. トレーニング コース

OpenText Fortify on Demand は Security Innovations と連携して、安全な開発トレーニング コースを提供しています。これらが含まれているかどうか、契約を確認してください。コースの追加に関心をお持ちの場合は、営業担当までお問い合わせください。

この機能を使用するには、ポータルに対しポップアップとクッキーを有効にしておく必要があります。

1.10.6.1. トレーニング コースの表示

割り当てられたトレーニング コースを表示するには、次の手順を実行します。

1. ポータル ツールバーの  アイコンをクリックします。

   [トレーニング] ページが表示されます。[コース] タブに、割り当てられたコースと、コース名、親カリキュラム、モジュール ID、コース完了ステータス、前回試行日、過ぎた日付、およびコースのリンクのリストが表示されます。

2. 次のいずれかの操作を実行します。

   - コースの行にある [**コースを開始**] リンクをクリックして、コースを開始します。

     > **Note**
     > コースの開始により完了ステータスがリセットされます。過ぎた日付はリセットされません。結果が正しく記録されたことを確認したら、コースウィンドウを閉じます。

   - コースの行にある [**コースを再開**] リンクをクリックして、前回の終了した時点からコースを続行します。
   - コースの行にある [**コースを参照**] リンクをクリックして、完了ステータスや過ぎた日付に影響を与えずに内容を確認することができます。

   確認メッセージが表示されます。

3. **[はい]** をクリックします。

   新しいウィンドウにコースが表示されます。

1.10.6.2. トレーニング コースの割り当て

テナントが使用できるトレーニング コースを自分に割り当てることができます。また、**ユーザー管理**権限を持つユーザーは、テナント内のすべてのアクティブなユーザーにトレーニング コースを割り当てることができます。コースはさまざまなタイプのカリキュラムにグループ化されていて、カリキュラムとして割り当てられます。

自分または別のユーザーにトレーニング コースを割り当てるには、次の手順を実行します。

1. ポータル ツールバーの アイコンをクリックします。

   [トレーニング] ページが表示されます。

2. [**割り当て**] タブを選択します。

   ロールに**ユーザー管理**権限が設定されている場合は、テナント内のアクティブなユーザーおよびこれらのユーザーに割り当てられたカリキュラムのリストが表示されます。それ以外の場合は、ユーザー アカウントおよび自分に割り当てられたカリキュラムのみが表示されます。

3. ユーザーの横にある をクリックします。

   [コースのカリキュラム] モーダル ウィンドウが表示されます。

4. ユーザーに割り当てるカリキュラムの横にあるチェックボックスをオンにします。

   [**保存**] をクリックします。

   [**割り当て**] タブに、保存した変更内容が表示されます。

1.10.6.3. トレーニング レポートの表示

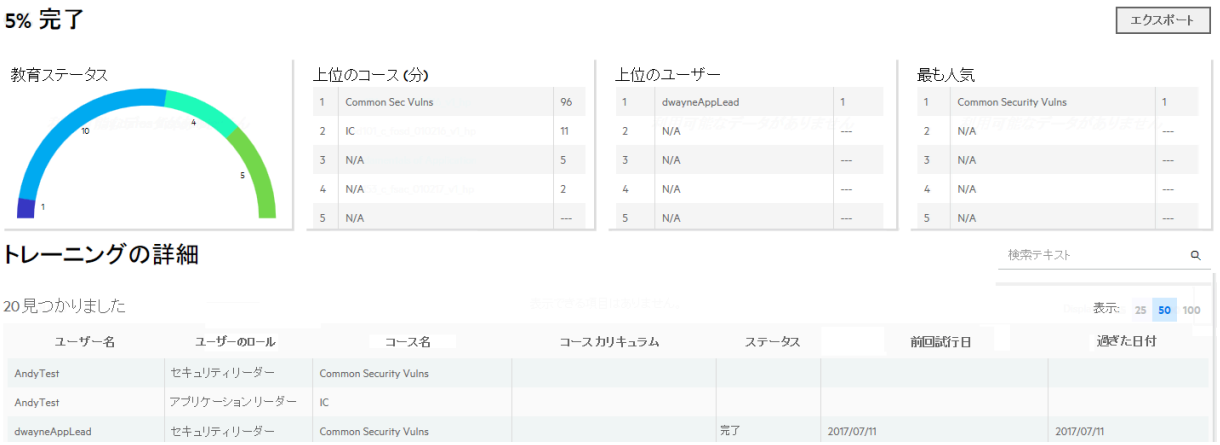
ユーザー管理権限を持つユーザーは、トレーニング進行状況レポートを表示することにより、テナント内で割り当てられたトレーニング コースのユーザー進行状況を追跡することができます。このレポートには、ユーザー アクティビティのテナントレベルの概要や、ユーザーごとのコース完了ステータスのリストが表示されます。

トレーニング レポートを表示するには、次の手順を実行します。

1. ポータル ツールバーの アイコンをクリックします。

   [トレーニング] ページが表示されます。

2. [**レポート**] タブを選択します。



   このタブには、次の情報が表示されます。

   - 割り当てられたコースの中で、完了したコースが占める割合
   - ユーザーの進行状況および傾向の概要を示すグラフ:
     - **教育ステータス**: 完了済み、進行中、開始前のコースの数
     - **上位のコース**: 利用された分数に基づく、最もアクティブなコース
     - **上位のユーザー**: 利用したコース数に基づく、最もアクティブなユーザー
     - **最も人気**: 最もよく利用されているコース
   - [**トレーニングの詳細**] グリッドの各行には、テナント ユーザー、割り当てられたコース、コースの進行状況のステータス、コースへの最後のアクセス日、最後のコース完了日が表示されます。

3. [**エクスポート**] をクリックして、[**トレーニングの詳細**] グリッドを CSV ファイルとしてエクスポートします。検索結果がエクスポートに適用されます。

1.11. ポリシーとサポート

ポータルの管理と保守に関する詳細については、OpenText Fortify on Demand のポリシーをご覧ください。他にご質問がある場合は、サポート担当に問い合わせてください。

- メンテナンス スケジュールとソフトウェア更新
- データ保持ポリシー
- サポートの取得

1.11.1. メンテナンス スケジュールとソフトウェア更新

OpenText Fortify on Demand は、メンテナンス スケジュールとソフトウェア更新に関する以下の情報を提供します。

メンテナンス スケジュール

OpenText Fortify on Demand では、スケジュールされたメンテナンスを計画する顧客のために、必要に応じて使用される事前定義の時間枠が予約されています。すなわち、週 2 時間 (木曜日 00:00 ～ 02:00) および月 48 時間 (土曜日 00:00 ～ 日曜日 00:00) の時間枠です。これらのメンテナンス時間枠は必要に応じて使用され、ほとんどの場合、ユーザーによる OpenText Fortify on Demand の機能へのアクセスや利用には影響しません。

各データ センターのメンテナンス時間枠は次のタイム ゾーンを使用して設定されます。

データ センター	メンテナンスのタイム ゾーン
AMS	米国東部時間
EMEA	グリニッジ標準時
APAC	オーストラリア東部時間

他の環境でのスケジュールされたメンテナンスの詳細については、サポートに問い合わせてください。

ソフトウェア更新

OpenText Fortify on Demand は、ソフトウェア アップグレードの開発、リリース、および OpenText Fortify on Demand プラットフォームおよびサポート コンポーネントへの適用を行うかどうか、およびいつ行うかを決定します。メジャー リリースは通常四半期ごとに提供され、マイナー リリースとパッチは必要に応じて提供されます。OpenText Fortify on Demand がソフトウェアのアップグレードによるサービスの中断を予定していない限り、OpenText Fortify on Demand は顧客に通知することなくいつでも SaaS アップグレードを実施できます。OpenText Fortify on Demand は、毎月スケジュールされているメンテナンス時間枠を使用して主要なソフトウェア更新を適用することを目的としています。

脆弱性を識別する OpenText Fortify on Demand の能力を拡張および改善するためのセキュリティ コンテンツの更新は、OpenText Fortify on Demand サービスの重要な要素で

す。セキュリティ コンテンツの更新は、Fortify Software Security Research (SSR) のチームによって開発され、一般に暦四半期の終わりにリリースされます。OpenText Fortify on Demand は、通常、更新されたセキュリティ コンテンツを公開から数週間以内に展開します。重要な新しい脅威やゼロデイの脆弱性に対しては、セキュリティ コンテンツの更新が四半期ごとの更新とは別に展開されることがあります。OpenText では、ユーザーに、サイバーセキュリティのブログを読み、セキュリティについて常に最新の情報を手に入れることをお勧めします。

1.11.2. データ保持ポリシー

OpenText Fortify on Demand では、v18.4 リリース時点での顧客を対象に以下のデータ保持ポリシーが採用されています。OpenText では、保持しておく必要があるデータ保持期間外のファイルを確認のうえダウンロードしておくことをお勧めします。

データ保持ポリシー

製品リソース	ファイル タイプ	保持期間
データのエクスポート ([アプリケーション] および [リリースの問題] ページ)	.csv	7 日間
ソース コード	.zip	15 日間
モバイル アプリケーション バイナリ	.ipa、.apk	30 日間
通知	適用外	3 か月
データ エクスポート (グローバルの [レポート] ページ)	.csv	3 か月
イベント ログ	.csv	13 か月
ユーザー生成レポート	.pdf、.html	2 年
Fortify のスキャン結果ファイル	.fpr	2 年
ソフトウェア部品表 (SBOM)	.json	2 年

製品リソース	ファイル タイプ	保持期間
サイト ツリー	.csv	2 年
アプリケーション データ	適用外	顧客により管理*
リリース データ	適用外	顧客により管理*
問題のデータ	適用外	顧客により管理*
ユーザー データ	適用外	顧客により管理*

*顧客は OpenText Fortify on Demand でアクティブなステータスを維持している限り、指定されたデータの作成および削除に対して責任を負います。顧客はいつでもアプリケーション、リリース、またはユーザーを削除できます。アプリケーションまたはリリースに関連する問題のデータも削除されます。OpenText Fortify on Demand サービスの終了時、終了データの取得期間は 30 日間になります。

詳細については、サポートまでお問い合わせください。

1.11.3. サポートの取得

OpenText Fortify on Demand では、セルフサービスのリソースとヘルプ センターを通じて、専用サポート チームによるサポートを年中無休の 24 時間体制で提供しています。セルフサービス リソースには、デモ用のビデオ、ナレッジベース、および製品ドキュメントが含まれます。解決できない問題がある場合は、サポートとのライブ チャットを開始するか、ヘルプ センターでサポート チケットを送信して、専用の FEDRamp サポート電子メールにリクエストを送信してください。インターネット アクセスを利用できない場合は、サポートに電話で問い合わせることができます (800.893.8141 または 650.800.3233)。

- サポート リソースへのアクセス
- ヘルプ センター チケットの送信
- ヘルプ センター チケットの追跡

1.11.3.1. サポート リソースへのアクセス

サポート リソースは、ポータルから入手できます。ポータルには、紹介ビデオ、HTML ユーザー ガイド、ライブ チャット、およびヘルプ センターへの直接リンクが含まれています。ヘルプ センターは OpenText Fortify on Demand のサポート チケット システムです。これは、ナレッジベースと PDF 形式のユーザー ガイドも提供しています。

Note

ヘルプ センターには、OpenText Fortify on Demand の資格情報を使用して関連する URL から直接ログインすることができます。

- AMS: https://helpcenter.ams.fortify.com
- EMEA: https://helpcenter.emea.fortify.com
- APAC: https://helpcenter.apac.fortify.com
- SGP: https://fodsgp.zendesk.com/

サポート リソースにアクセスするには、次の手順を実行します。

[ヘルプ] メニューをクリックし、次のいずれかを選択します。

- **ハウツー ガイド** - Fortify Digital Learning に含まれるハウツー ビデオ ガイドを開きます。
- **ドキュメント** - ユーザー ガイドを開きます
- **ヘルプ センター** - ヘルプ センターを開きます
- **ライブ チャット** - 年中無休対応のサポートとのチャットを行うためのライブ チャットを開きます

1.11.3.2. ヘルプ センター チケットの送信

ヘルプ センターでサポート チケットを送信します。

ヘルプ センター チケットを送信するには、次の手順を実行します。

1. [ヘルプ] メニューをクリックし、[**ヘルプ センター**] を選択します。
2. **[チケットを送信]** をクリックします。

   [**依頼を送信**] フォームが表示されます。
3. ドロップダウン リストからチケットのタイプを選択します。
   - [**チケットを作成**] - 一般的な製品に関する質問またはテナント固有の問題に関するヘルプを表示する
   - [**FoD 不具合送信**] - バグまたは問題を報告する
   - [**FoD 拡張機能送信**] - 拡張機能を要求する
4. 選択したチケット タイプに表示されるフィールドに入力します。できるだけ多くの詳細を提供します。
5. [**送信**] をクリックします。

   ページ上部のメッセージは、ヘルプ センターのチケットが送信されたことを示します。

1.11.3.3. ヘルプ センター チケットの追跡

テナントに対して送信されたサポート チケットをヘルプ センターで追跡できます。自分が送信したチケット、自分に割り当てられているチケット、コピーが送られたチケット (アプリケーションの通知リストに含まれているユーザーは、アプリケーションにリンクされたチケットに自動的に追加されます) のみを表示できます。

ヘルプ センター チケットを追跡するには、次の手順を実行します。

1. [ヘルプ] メニューをクリックし、[**ヘルプ センター**] を選択します。
2. **[チケットを表示]** をクリックします。

   チケットが表示されます。チケットには、次のいずれかのステータスがあります。

   - **オープン** - 要求は受信されてサポートに割り当てられ、サポートが解決に着手しています。
   - **ユーザーの応答待ち** - 割り当てられたサポートからのフォローアップ質問があります。保留中のチケットは、通常は、ユーザーが回答し、問題の解決を続行するためにサポートが必要とする情報を提供するまで、そのままの状態でとどまります。
   - **解決済み** - サポートは問題を解決しました。解決済みのチケットは、[解決済み] となってから 7 日後に自動的に閉じます。チケットは、クローズされるまでは再オープンできます。
   - **クローズ** - チケットは完了しており、再度開くことはできません。元のチケットに追加サポートが必要な場合は、フォローアップ要求を作成します。
3. 表示するチケットの数を制限するには、[**ステータス**] フィルターでリストを絞り込みます。
   - **任意** - すべてのチケットを表示します。
   - **未解決** - サポート チームがまだ対応中のチケットを表示します。
   - **ユーザーの応答待ち** - ユーザーの組織からのアクションが必要なチケットを表示します。
   - **解決済み** - 解決済みのチケットを表示します。

For more info, visit https://docs.microfocus.com