OpenText™ Application Security

Application Security

Version : 26.2

Table of Contents

1. Application Security

ソフトウェアバージョン: 26.2.0

ドキュメントリリース日: 2026年9月

ソフトウェアリリース日: 2026年9月

1.1. 変更ログ

次の表に、このドキュメントに加えられた変更を一覧表示します。このドキュメントの改訂版は、変更が製品の機能に影響を与える場合にのみ、ソフトウェアリリース間で発行されます。

ソフトウェアリリース/ ドキュメント改訂	変更点
26.2.0	追加: • ダッシュボードビューの概要ページ • AI Assistantの設定 • Aviatorの設定 • Aviatorの自動修復結果の操作 • `sql-mode` のデフォルト値(MySQLデータベースの使用を参照) • Luceneのアップグレード 更新: • MySQLデータベースの使用 • `fortifyclient` が廃止されました(「fortifyclientユーティリティの使用」を参照) 削除: • ログイン画面、マストヘッド、Application Securityの概要画面からCEマークが削除されました。

ソフトウェアリリース/ ドキュメント改訂	変更点
25.4.0	追加: • IdPの公開鍵(X.509証明書)を使用してIdPメタデータ署名を検証するためのサポート(「SAML 2.0準拠のシングルサインオンの設定」を参照) • アプリケーションビューを保存する • Fortify CLI (fcli)ドキュメント • 事前に設定された役割におけるScanCentral DASTコントローラ役割 更新: • Oracleデータベースのパーティショニングによるパフォーマンスの改善の手順 • **アプリケーションビュー**の改善(「アプリケーションバージョンの表示」を参照) • **ご使用のバージョン**のための新しい**フィルタ**オプションの導入(「アプリケーションビューからアプリケーションとアプリケーションバージョンを検索する」を参照)

ソフトウェアリリース/ ドキュメント改訂	変更点
25.2.0	追加: • システム要件 • ルートコンテキストでの設定の自動化 更新: • 組み込まれた製品名の変更(「製品名の変更」を参照) • プラグインログファイルの場所が変更されました(「ディレクトリの内容」を参照)。 • 改善された最新の**アプリケーション**ビューの導入(「アプリケーションバージョンの表示」を参照) • ファイル数または行数が10%増加または減少した場合のアプリケーションバージョン処理ルール(「アプリケーションバージョンの分析結果処理ルールの設定」を参照) • ［**監査(AUDIT)**］ページの問題テーブルの［**分析のタイプ(Analysis Type)**］列と［**アーティファクト履歴(ARTIFACT HISTORY)**］テーブルには、製品の再ブランド化のためのSASTまたはDASTの分析タイプが表示されます(「監査する問題に関する情報の表示」および「スキャンアーティファクト詳細の表示」を参照) • Fortify ScanCentral SAST分析結果の表示とフィルタリングの改善(「Fortify ScanCentral SASTスキャン要求の詳細の表示」を参照) 削除:

ソフトウェアリリース/ ドキュメント改訂	変更点
	• Javaセキュリティマネージャの有効化に関するトピックは、サポートされなくなったため削除されました • Kerberos/SPNEGOおよびCASシングルサインオンソリューションのコンテンツ(それらがサポートされなくなったため) • ジョブスケジューラ設定からのジョブ実行戦略 • Magellan BIおよびレポーティングを使って実装されるダッシュボードテクノロジプレビューへの参照はすべて削除されました。この機能は非推奨であり、今後のリリースには予定されていません。
24.4.0/リビジョン1: 2024年11月	更新: • OpenText ScanCentral DASTと統合するために必要なサービスアカウントに関する情報を追加しました(「OpenText ScanCentral DASTスキャンの実行と管理の有効化」を参照)。

ソフトウェアリリース/ ドキュメント改訂	変更点
24.4.0	追加: • 管理者は、Magellan BIおよびレポーティングダッシュボードを実装して、包括的なアプリケーションセキュリティプログラムの概要を把握し、重要な脆弱性メトリックスのインサイトを得ることができます。この機能は技術プレビューとしてリリースされたため、機能の欠落、問題、ギャップがあれば報告してください。次のリリースの前に対応できます。 • 監査の問題履歴を確認する機能(「監査の問題履歴について」を参照) • 事前設定済みの役割およびユーザアカウントタイプにおけるFortify ScanCentral SASTコントローラ役割。 • ログ記録の設定 • キーストアファイルのマイグレーション 更新: • 連邦情報処理標準(FIPS)環境での実行 • `secret.key` パラメータの説明(「<fortify.home>ディレクトリの内容」を参照) 削除: • Fortify Software Security Centerのログレベルの変更、およびFortify Software Security Centerログのカスタマイズに関するトピックが削除さ

ソフトウェアリリース/ ドキュメント改訂	変更点
	れ、「ログ記録の設定」に置き換えられました • Webアプリケーションの感受性分析に関するトピックは、Fortify SourceAndLibScannerが非推奨になったので削除されました

ソフトウェアリリース/ ドキュメント改訂	変更点
24.2.0	追加: • アプリケーションバージョンのアーティファクトを保持する期間を定義するデータ保持ポリシーを管理者が有効にする機能(「データ保持について」を参照) • UIテーマの変更の手順(「システム全体とアプリケーションバージョン間の環境設定」を参照) • カスタマイズされたBIRTレポートをXLSX形式でダウンロードする方法(「XLSXでのカスタマイズされたBIRTレポートの生成とダウンロード」を参照) • 抑制された問題、優先度上書き、および分析タグに対する監査履歴の変更をOpenText ScanCentral DASTと同期させるよう、Kafkaを設定する機能(「Kafkaを使用した、OpenText ScanCentral DASTでの監査履歴変更の同期」および「Kafka StreamをOpenText ScanCentral DASTで使用するための設定」を参照) • `fortifyclient`に対する接続、読み取り、および書き込みのタイムアウトを設定する機能(「fortifyclient HTTPタイムアウト」を参照) 更新: • ディスクI/Oの監視に関する情報を追加しました • LDAP更新のデフォルトのスケジュール(「繰り返し実行されるクリーンア

ソフトウェアリリース/ ドキュメント改訂	変更点
	ップジョブ」を参照) • IdPメタデータの場所とキーストアの場所が変更されました(「SAML 2.0準拠のシングルサインオンを使用するためのApplication Securityの設定」を参照) • サポートされている演算子のリストを更新しました(「パフォーマンスインジケータの作成」を参照)。 • 問題の状態の説明を追加しました(「問題の状態の設定」を参照)。 • デフォルトのジョブ実行戦略が［柔軟(Flexible)］に変更されました(「ジョブスケジューラの設定」を参照) 削除: • BIRTレポート用のセキュリティの設定からの `activity`、`requirement`、および `requirementtemplate` テーブル名 • AuditTokenタイプの認証トークン • Bugzilla用のバグトラッカプラグインに関するすべての言及

1.2. はじめに

OpenText™ Application Securityは、ソフトウェア開発ライフサイクル全体にわたって、アプリケーションでセキュリティの脆弱性を自動的に検出する一連の機能を提供するブラウザベースの製品です。以下の製品から関連データを利用可能にすることで、セキュリティチームと開発チームは、迅速かつ正確にセキュリティの欠陥を解決するために協力できます。

- OpenText™ Static Application Security Testing (OpenText SAST)
- OpenText™ Fortify ScanCentral SAST
- OpenText™ ScanCentral DAST
- Fortify WebInspect Enterprise
- OpenText™ Core Software Composition Analysis (OpenText Core SCA)
- Sonatype

Application Securityが提供するもの:

- セキュリティチームは、アプリケーションの履歴と現在のステータスの大まかな概要を把握してリードします。セキュリティチームは、開発者と監査官の両方が効果的に共同して、アプリケーションの問題に最適な対応を提供できるようにします。
- 問題管理のための集中型施設を持つ監査官。マネージャがオフラインで作業する必要がある場合や、OpenText™ Fortify Audit Workbenchが提供する高度なツールを使用する必要がある場合は、現在のアプリケーションの状態と最新の監査情報をダウンロードできます。
- 企業のニーズを反映するために問題に優先順位を付ける能力を持つマネージャ。この優先順位付けを使用して、アプリケーション開発チームの活動を優先順位付けできます。
- 分析エージェントから受け取った特定の問題に関する情報を管理および送信する役割を担う開発者は、サポートされている統合開発環境(IDE)や、Fortify Audit Workbenchなどのスタンドアロンクライアントに送信します。その後、開発者はアプリケーションスナップショットを使用して、安全な開発ライフサイクルを通じて進行状況を測定できます。

このセクションでは、次のトピックについて説明します。

1.2.1. 製品名の変更

OpenTextでは、次の製品名を変更中です。

前の名前	新しい名前
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
Fortifyアプリケーションとツール	OpenText™ Application Security Tools

これらの製品名は、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、および製品が識別されるその他の場所で変更されました。名前の変更は、製品の機能を明確にし、Fortify Software製品とOpenTextとの整合性を高め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、古い名前が一時的に括弧に含まれる場合があります。今後の製品リリースで、さらに多くの変更を予定しています。

1.2.2. 対象読者

このガイドで提示されている情報は、(Application Securityの展開と保守を担当する)管理者、企業のセキュリティリード、監査担当者、開発チームマネージャ、および開発者を対象にしています。

Application Securityの展開、設定、および保守のコンテンツは、エンタープライズアプリケーションの開発に関して適度に知識を持ち、エンタープライズシステムおよびデータベース管理のスキルを持つ管理者向けです。Application Security APIドキュメントにアクセスする方法については、「APIドキュメントへのアクセス」を参照してください。

ドキュメント構造

このドキュメントは、2つの主要パートに分かれています。最初のパートは、セキュリティ保護された展開の提供から始まり、Application Securityを展開および設定する方法を説明するトピックがあります。第2のパートは、Application Securityの使用から始まり、Application Securityの使用法について説明します。

1.2.3. 関連ドキュメント

このトピックでは、OpenText Application Security Software製品に関する情報を提供しているドキュメントについて説明します。

Note

ほとんどのガイドは、PDF形式とHTML形式の両方で提供されています。製品ヘルプは、Fortify LIM (License and Infrastructure Manager)と、OpenText DAST製品内で利用できます。

すべての製品

以下のドキュメントには、すべての製品に関する一般情報が記載されています。特に明記されている場合を除き、これらのドキュメントは各製品の製品マニュアルのWebサイトで利用できます。

ドキュメント/ファイル名	説明(Description)
OpenText Application Security Softwareについて appsec-docs-n-*<version>*.pdf	このドキュメントでは、OpenText Application Security Softwareのドキュメントにアクセスする方法について説明しています。 **Note** このドキュメントは、製品のダウンロードにのみ含まれています。
OpenText™ Application Securityソフトウェアのシステム要件 appsec-sr-*<version>*.pdf	このドキュメントでは、OpenText Application Security Softwareの当該バージョンでサポートされている環境と製品について詳しく説明しています。
OpenText Application Security Software<version>の新機能 appsec-wn-*<version>*.pdf	このドキュメントでは、OpenText Application Security Software製品の新機能について説明しています。
OpenText Application Security Softwareリリースノート	このドキュメントでは、OpenText Application Security Softwareのこのリリースで行われた変更の概要と、他の製品ドキュメントには記載されていない重要な情報について説明します。

OpenText ScanCentral DAST

以下のドキュメントには、OpenText ScanCentral DASTに関する情報が記載されています。特に明記されている場合を除き、これらのドキュメントは製品マニュアルのWebサイト(https://www.microfocus.com/documentation/fortify-ScanCentral-DAST)で利用できます。

ドキュメント/ファイル名	説明(Description)
OpenText™ ScanCentral DASTの設定および使用ガイド sc-dast-ugd-<*version*>.pdf	このドキュメントでは、Webアプリケーションの動的スキャンを実行するためにOpenText ScanCentral DASTを設定し、使用する方法について説明しています。
OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド lim-ugd-<*version*>.pdf	このドキュメントでは、Fortify License and Infrastructure Manager (LIM)をインストール、設定、使用する方法について説明します。LIMは、ローカルWindowsサーバにインストールして、Dockerプラットフォーム上のコンテナイメージとして使用できます。
OpenText™ Dynamic Application Security TestingおよびOAST on Docker ユーザガイド dast-docker-ugd-<*version*>.pdf	このドキュメントでは、Dockerプラットフォーム上のコンテナイメージとして利用可能なOpenText DASTおよびFortifyOASTをダウンロード、設定、使用する方法について説明しています。OpenText DASTイメージは、コマンドラインインタフェース(CLI)またはアプリケーションプログラミングインタフェース(API)を介して設定されたヘッドレスセンサとして、自動化プロセスで使用されるように意図されています。OpenText ScanCentral DASTのセンサとして実行し、Application Securityと組み合わせて使用することもできます。FortifyOASTは、帯域外のアプリケーションセキュリティテスト(OAST)サーバで、OAST脆弱性の検出用のDNS、SMTP、およびHTTP/HTTPSサービスを提供します。

Fortify ScanCentral SAST

次のドキュメントでは、Fortify ScanCentral SASTの情報について説明します。このドキュメントは、製品ドキュメントのWebサイト

(https://www.microfocus.com/documentation/fortify-software-security-center)に用意されています。

ドキュメント/ファイル名	説明(Description)
OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド sc-sast-ugd-<バージョン>.pdf	このドキュメントでは、Fortify ScanCentral SASTをインストール、設定、使用して、静的コード分析のプロセスを合理化する方法について説明しています。このドキュメントの対象読者は、リソースを大量に消費するOpenText SASTプロセスの変換およびスキャンフェーズをオフロードするためにFortify ScanCentral SASTをインストール、設定、または使用するユーザです。

Application Security

以下のドキュメントには、Application Securityに関する情報が記載されています。このドキュメントは、製品ドキュメントのWebサイト(https://www.microfocus.com/documentation/fortify-software-security-center)に用意されています。

ドキュメント/ファイル名	説明(Description)
OpenText™ Application Securityユーザガイド ssc-ugd-<*version*>.pdf	このドキュメントでは、Application Securityのユーザ向けに、Application Securityをデプロイおよび使用する方法について詳しく説明しています。Application Securityをデプロイ、設定、使用するために必要なすべての情報を提供します。 これは、システムおよびインスタンス管理者、データベース管理者(DBA)、エンタープライズセキュリティリード、開発チームマネージャ、および開発者による使用を目的としています。Application Securityは、セキュリティチームのリードにプロジェクトの履歴とステータスの概要を提供します。

OpenText SAST

以下のドキュメントには、OpenText SAST (Fortify Static Code Analyzer)に関する情報が記載されています。別段の記載がある場合を除き、これらのドキュメントは製品ドキュメントWebサイト(https://www.microfocus.com/documentation/fortify-static-code)で入手できます。

ドキュメント/ファイル名	説明(Description)
OpenText™ Static Application Security Testingユーザガイド sast-ugd-<*version*>.pdf	このドキュメントでは、多くの主要なプログラミングプラットフォームにOpenText SASTをインストールし、コードをスキャンするために使用する方法について説明します。これは、セキュリティ監査とセキュアコーディングを担当するユーザを対象にしています。
OpenText™ Static Application Security Testingカスタムルールガイド sast-cr-ugd-<*version*>.zip	このドキュメントでは、OpenText SASTのカスタムルールを作成するために必要な情報について説明します。このガイドには、ルール作成の概念を実際のセキュリティ問題に適用する例が含まれています。 **Note** このドキュメントは、製品のダウンロードにのみ含まれています。
OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド lim-ugd-<*version*>.pdf	このドキュメントでは、Fortify License and Infrastructure Manager (LIM)をインストール、設定、使用する方法について説明します。LIMは、ローカルWindowsサーバにインストールして、Dockerプラットフォーム上のコンテナイメージとして使用できます。

OpenText Application Security Tools

次のドキュメントには、OpenText Application Security Toolsに関する情報が記載されています。これらのドキュメントは、製品ドキュメントのWebサイト (https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools) で入手できます。

ドキュメント/ファイル名	説明(Description)
OpenText™ Application Securityツールガイド sast-tgd-<*version*>.pdf	このドキュメントでは、Application Security Toolsのインストール方法について説明します。OpenText SASTを使用してコードのスキャン、分析結果の確認、分析結果ファイルの操作などを行うことのできるアプリケーションとコマンドラインツールの概要を提供します。
OpenText™ Fortify Audit Workbenchユーザガイド awb-ugd-<*version*>.pdf	このドキュメントでは、Fortify Audit Workbenchを使用して、ソフトウェアプロジェクトをスキャンして分析結果を監査する方法について説明します。このガイドには、バグトラッカとの統合方法、レポートの作成方法、共同監査の実行方法も記載されています。
OpenText™ Fortify Plugin for Eclipseユーザガイド ep-udg-<*version*>.pdf	このドキュメントでは、Fortify Plugin for Eclipseをインストールして、コードを分析および監査するために使用する方法について説明しています。
OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studioユーザガイド iap-udg-<*version*>.pdf	このドキュメントでは、Fortify Analysis Plugin for IntelliJ IDEA and Android Studioをインストールして、コードを分析し、必要に応じて分析結果をApplication Securityにアップロードするために使用する方法について説明しています。
OpenText™ Fortify Extension for Visual Studioユーザガイド vse-ugd-<*version*>.pdf	このドキュメントでは、Fortify Extension for Visual Studioをインストールおよび使用して、コードを分析、監査、修復し、ソリューションとプロジェクトのセキュリティに関する問題を解決する方法について説明します。

OpenText DAST

以下のドキュメントには、OpenText DAST (Fortify WebInspect)に関する情報が記載されています。これらのドキュメントは製品マニュアルのWebサイト (https://www.microfocus.com/documentation/fortify-webinspect)で利用できます。

ドキュメント/ファイル名	説明(Description)
OpenText™ Dynamic Application Security Testingインストールガイド dast-igd-<*version*>.pdf	このドキュメントでは、OpenText DASTの概要、インストール手順、製品ライセンスの有効化手順について説明しています。
OpenText™ Dynamic Application Security Testingユーザガイド dast-ugd-<*version*>.pdf	このドキュメントでは、WebアプリケーションやWebサービスをスキャンして分析するためにOpenText DASTを設定し、使用する方法について説明しています。 **Note** このドキュメントは、OpenText DASTヘルプのPDF版です。このPDFファイルは、ヘルプ情報から簡単に複数のトピックを印刷したり、ヘルプをPDF形式で閲覧したりできるようにするために用意されています。このコンテンツは、もともとWebブラウザで表示するヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。また、このPDF版では一部の対話型トピックやリンクされたコンテンツを表示できない場合があります。

ドキュメント/ファイル名	説明(Description)
OpenText™ Dynamic Application Security TestingおよびOAST on Docker ユーザガイド dast-docker-ugd-*<version>*.pdf	このドキュメントでは、Dockerプラットフォーム上のコンテナイメージとして利用可能なOpenText DASTおよびFortifyOASTをダウンロード、設定、使用する方法について説明しています。OpenText DASTイメージは、コマンドラインインタフェース(CLI)またはアプリケーションプログラミングインタフェース(API)を介して設定されたヘッドレスセンサとして、自動化プロセスで使用されるように意図されています。OpenText ScanCentral DASTのセンサとして実行し、Application Securityと組み合わせて使用することもできます。FortifyOASTは、帯域外のアプリケーションセキュリティテスト(OAST)サーバで、OAST脆弱性の検出用のDNS、SMTP、およびHTTP/HTTPSサービスを提供します。
OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド lim-ugd-*<version>*.pdf	このドキュメントでは、Fortify License and Infrastructure Manager (LIM)をインストール、設定、使用する方法について説明します。LIMは、ローカルWindowsサーバにインストールして、Dockerプラットフォーム上のコンテナイメージとして使用できます。
OpenText™ Dynamic Application Security Testingツールガイド dast-tgd-*<version>*.pdf	このドキュメントでは、OpenText DASTおよびFortify WebInspect Enterpriseにパッケージ化されているOpenText DASTの診断ツール、侵入テストツール、設定ユーティリティの使用方法について説明しています。

ドキュメント/ファイル名	説明(Description)
OpenText™ Dynamic Application Security Testing Agentインストールおよびルールパックガイド dast-agent-igd-<*version*>.pdf	このドキュメントでは、OpenText DAST Agentのインストール方法と、OpenText DAST AgentRulepackキットの検出機能について説明しています。OpenText DAST AgentRulepackキットはOpenText DAST Agent上で実行され、OpenText DAST Agentが実行中にコードのソフトウェアセキュリティ脆弱性を監視できるようにします。OpenText DAST AgentRulepackキットは、動的な結果を静的な結果と関連付けるのに役立つランタイムテクノロジを提供します。

Fortify WebInspect Enterprise

以下のドキュメントには、Fortify WebInspect Enterpriseに関する情報が記載されています。特に明記されている場合を除き、これらのドキュメントは製品マニュアルのWebサイト(https://www.microfocus.com/documentation/fortify-webinspect-enterprise)で利用できます。

ドキュメント/ファイル名	説明(Description)
OpenText™ Fortify WebInspect Enterpriseインストールおよび実装ガイド WIE_Install_<*version*>.pdf	このドキュメントでは、Fortify WebInspect Enterpriseの概要、Fortify WebInspect Enterpriseのインストール手順、Fortify Application SecurityやFortify DASTとの統合手順、およびインストールのトラブルシューティング手順について説明しています。また、Fortify WebInspect Enterpriseシステムのコンポーネント(WebInspect Enterpriseのアプリケーション、データベース、センサ、およびユーザなど)の設定方法についても説明しています。
OpenText™ Fortify WebInspect Enterpriseユーザガイド WIE_Guide_<*version*>.pdf	このドキュメントでは、Fortify WebInspect Enterpriseを使用してOpenText DASTセンサの分散ネットワークを管理し、WebアプリケーションとWebサービスをスキャンして分析する方法について説明しています。 **Note** このドキュメントは、Fortify WebInspect EnterpriseヘルプのPDF版です。このPDFファイルは、ヘルプ情報から簡単に複数のトピックを印刷したり、ヘルプをPDF形式で閲覧したりできるようにするために用意されています。このコンテンツは、もともとWebブラウザで表示するヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。また、このPDF版では一部の対話型トピックやリンクされたコンテンツを表示できない場合があります。

ドキュメント/ファイル名	説明(Description)
OpenText™ Dynamic Application Security Testingツールガイド dast-tgd-<*version*>.pdf	このドキュメントでは、OpenText DASTおよびFortify WebInspect Enterpriseにパッケージ化されているOpenText DASTの診断ツール、侵入テストツール、設定ユーティリティの使用方法について説明しています。

1.3. セキュリティ保護された展開の提供

分析されたソースコードにセキュリティ予防措置を適用するのと同様に、ソースコードにアクセスするOpenText Application Security Software分析製品へのアクセスもセキュリティ保護する必要があります。さらに、OpenText Application Security Software製品が提供する、セキュリティ脆弱性に的を絞った要約で、さらに高度なセキュリティで保護されたデプロイが要件とされる場合もあります。このセクションのトピックでは、Application Securityを安全にデプロイするいくつかの方法について説明しています。

このセクションでは、次のトピックについて説明します。

1.3.1. 施設へのアクセスのセキュリティ保護

Application Securityは、分析したアプリケーションのソースコードと、それらのアプリケーションで検出された問題をHTMLとして保存し、レンダリングします。プログラムソースコードおよび検出された脆弱性は、誤った処理や不正使用の機会を提供します。このため、OpenTextでは、管理者がApplication Securityをセキュリティ保護された運用施設にデプロイすることを推奨しています。また、基礎となるApplication Securityファイルシステムをセキュリティ保護するとともに、インストールディレクトリへのアクセスを制限する必要もあります。

1.3.2. Tomcatサーバのセキュリティ保護

Application Securityを実行するアプリケーションサーバの動作セキュリティを確認する必要があります。少なくとも、信頼された認証局によって発行されたSSL証明書とともにHTTPSを使用するように、Apache Tomcatサーバを設定します。また、運用環境で、Tomcatサーバをセキュリティ保護するために必要な追加の手順を実行します。

セキュアな暗号スイートの使用

OpenTextでは、TomcatでセキュアなSSL/TLS暗号スイートを使用することを推奨しています。

- APRベースのSSL接続

  SSLCipherSuiteディレクティブを使用します。詳細については、「SSL CipherSuite Directive」および「Cipher Suites and Enforcing Strong Security」を参照してください。

- JSSEベースのSSL接続

  `ciphers`属性と`honorCipherOrder`属性を使用します。詳細については、「Apache Tomcat 10 Configuration Reference - The HTTP Connector」を参照してください。

セキュリティの向上、相互運用性の向上、およびパフォーマンスの向上などの間にはトレードオフがあるため、暗号スイートの選択には正解がありません。ただし、Apacheでは「Apache Tomcat Ciphers」ドキュメントで、選択に役立つ情報を提供しています。

1.3.3. Tomcatサーバ属性を設定したクッキー内の機密データの保護

Tomcatサーバの設定によっては、一部のクッキーに含まれる機密情報が、不必要な開示に対して脆弱になる場合があります。

OpenTextでは、機密データを保護するために、Tomcatアプリケーションサーバでクッキー用に次の属性を追加することを推奨しています。

- `Secure` — `Secure` 属性は、SSLまたはTLSで保護されていない要求に対してクッキーが送信されないようにします。このオプションを使用して、セキュリティ保護されていないチャネル(HTTPなど)から情報を漏えいし、機密情報(セッション識別子など)を開示する可能性があるクッキーを防ぎます。
- `HttpOnly` — `HttpOnly` 属性は、クライアント側のスクリプトルーチンによるクッキー値へのアクセスを防ぎます。OpenTextでは、クライアント側のJavaScriptルーチンによってクッキーが読み込まれる場合を除き、この属性を有効にすることを推奨しています。

`Secure` および `HttpOnly` 属性の設定方法については、Apache Tomcat環境設定リファレンスのマニュアルを参照してください。

1.3.4. HTTPSおよびSSL通信の使用

OpenTextでは、すべての通信にHTTPSとSSL (Secure Sockets Layer)を使用するように、Application SecurityおよびOpenText Application Security Softwareクライアント製品(Audit Workbench、fortifyclient、Secure Code Pluginsなど)を設定することを強く推奨しています。

VeriSign、Entrust、Thawteなどの信頼されているルート認証局で購入した署名付きサードパーティ証明書を使用している場合は、HTTPSを使用してApplication Securityと通信するためにクライアント側で必要となる作業はありません。これらのルートCA証明書が信頼される理由は、OpenText Application Security Softwareクライアント製品が使用するキーストア内にあるためです。

一方、デフォルトでは、Application Security、OpenText Application Securityツール、およびfortifyclientユーティリティは、自己署名証明書や、内部またはローカルの署名機関によって署名された証明書を信頼しません。この場合、HTTPSを使用してApplication Securityと通信するには、自己署名証明書またはローカルで署名された証明書をJavaランタイム証明書ストアにインポートする必要があります。

Important

ローカルで署名された証明書を、サードパーティの認証局を使用して発行した場合は、証明書の発行に使用したCA証明書チェーンをインポートしてください。

自己署名証明書またはローカルで署名された証明書をApplication SecurityおよびOpenText Application Securityツールで使用するキーストアにインストールするには、これらの製品がインストールされている各コンピュータで次の操作を行います。

- コマンドプロンプトを開き、次のコマンドを実行します。

  ```
  cd "<tools_install_dir>/jre/bin"
  keytool -importcert -alias SSC -keystore
  ../lib/security/cacerts -file
  "YourCertFile.cer" -trustcacerts
  ```

  ここで

  - *<tools_install_dir>*は、OpenText Application Securityツールのインストールディレクトリです。

- `YourCertFile.cer`は、Tomcatサーバにインポートしたものと同じ証明書ファイルです。

何らかの理由でこの証明書ファイルが使用できない場合は、次のようにして、Tomcatサーバが使用するキーストアから証明書ファイルをエクスポートできます。

```
cd <java_home>/jre/bin
keytool -exportcert -alias SSC -keystore
<keystore_used_by_tomcat> -file YourCertFile.cer
```

エイリアスには任意の名前を使用できます。これらの例では、`SSC`を使用しています。

java keytoolを使用して対話形式で自己署名証明書を作成する際は、姓名の入力を求めるプロンプトが表示されます。Application Securityをホストするサーバの完全修飾ドメイン名(FQDN)を指定してください。単純に短いホスト名や`localhost`を使用することは避けてください。

HTTPS用に`server.xml`ファイルでコネクタを作成する場合は、キーストア内の証明書のエイリアス名を使用して属性`keyAlias`を含める必要があります。そうしない場合は、キーストアに複数の証明書が含まれている場合は、最初に見つかった証明書が使用されます。

1.3.5. パスワードとユーザ役割のセキュリティ保護について

OpenTextでは、Application Securityをデプロイして初めてサインインした後、直ちに新しいローカル管理者アカウントを1つ以上作成し、デフォルトの管理者アカウントを削除することを推奨しています。

アカウントセキュリティ機能には、次のものが含まれます。

- 一時的に非アクティブになっているアカウントを管理者が一時停止する機能
- 失敗したログオン試行に基づくアカウントの自動ロックアウト

LDAPを使用してApplication Securityユーザを認証する場合は、セキュリティ保護されたLDAP通信を使用するようにLDAPサーバを設定します。

参照情報

Application Securityへのサインイン

ユーザアカウントの管理

LDAPユーザ認証

1.3.6. コンピュータサービスとアカウントの管理

Application Securityのインストール時に、最小特権のユーザアカウントで実行されているサービスとして設定します。また、Application Securityではユーザアカウントからコンピュータのファイルシステムにアップロードされたファイルを一時的に保存することから、Application Securityをホストするコンピュータでは常に、更新されたウイルス対策ソフトウェアをインストールして実行してください。

1.4. Application Securityの展開

このコンテンツでは、初めてApplication Securityを準備して展開する方法について説明します。

このセクションでは、次のトピックについて説明します。

1.4.1. 展開の概要

Application Security は、Webアーカイブ(WAR)ファイルとしてパッケージされています。Tomcatサーバで動作し、サポートされているサードパーティデータベースが必要です。

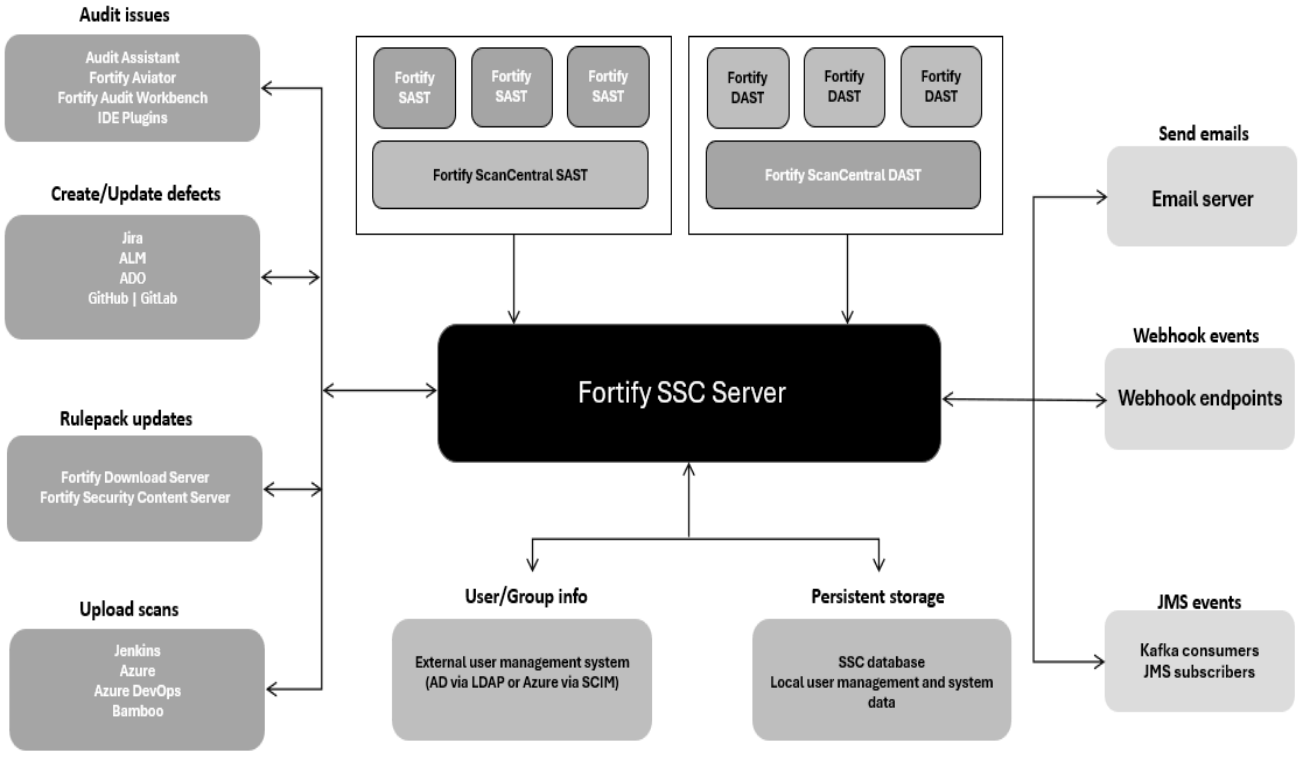
初期展開後に、Application Securityセットアップウィザードを使用して事前設定を完了します。これにより Application Security がサードパーティデータベースのような必須エンティティと連動できるようになります。

Tip

*上級ユーザのみ。*セットアップウィザードを使用する代わりに、Application Securityを展開する前に自動設定ファイルを設定して、設定を自動化することができます。その後は、サーバの起動時にセットアップウィザードで環境設定が取得され、設定が自動化されます。自動設定の設定方法については、「Application Securityの設定の自動化」を参照してください。

システム要件については、『*OpenText™ Application Securityソフトウェアシステム要件*』ドキュメントを参照してください。

次の図は、一元管理を実現する、必須コンポーネントおよびオプションコンポーネントとApplication Securityとの相互運用性を示しています。



次の表に図内のコンポーネントの説明を示します。

コンポーネント	説明(Description)
必要なコンポーネント	
Application Security	Application Securityは、Tomcatサーバによって実行されるWebアーカイブ(WAR)ファイルとして、またはKubernetes展開のHelmチャートとして配信されます。
Application Securityデータベース	ユーザおよびアーティファクトデータを保存するデータベースです。Application Securityを稼働状態にする前に、サポートされているサードパーティデータベースをインストールする必要があります。 **Important** 同じデータベーススキーマを共有する複数のApplication Securityインスタンスを展開することはできません。データの整合性を維持するために、各Application Securityインスタンスが専用のデータベーススキーマで動作するようにしてください。
Rulepack更新サーバ	OpenText SAST Application Securityコンテンツの取得および更新に使用されるサーバです。
Application Securityカスタマポータル	オフサイクルシードバンドルと、四半期ごとのOpenText SAST Application Securityコンテンツリリースの取得のために使用されるサーバです。
オプションのコンポーネント	

コンポーネント	説明(Description)
OpenText SAST (Fortify Static Code Analyzer)	OpenText SASTはソースコードをスキャンし、問題を特定します。
Fortify ScanCentral SAST	OpenText SASTユーザはFortify ScanCentral SASTを使用して、プロセッサ集約型のコード分析タスクをビルドマシンから、この目的のために提供されるマシン(センサ)のグループにオフロードできます。
OpenText DAST (Fortify WebInspect)	潜在的で動的な問題を取得するために、OpenText DASTエージェントに接続する分析エージェントです。
OpenText ScanCentral DAST	Application Securityから、OpenText DASTを使用してWebアプリケーションの動的スキャンを設定および実行できるツールです。
Fortify Audit WorkbenchおよびSecure Codeプラグイン	Application Securityに関する分析結果を共同で監査するツールです。これらのツールで、ソースコードをスキャンし、分析結果をアップロードすることもできます。
Jenkinsプラグイン Azure DevOps Extension	OpenText SASTでソースコードをスキャンし、分析結果をアップロードするプラグインです。

コンポーネント	説明(Description)
欠陥トラッキングサーバ	Jira、ALM、Azure DevOps Server、またはカスタマイズされたバグトラッキングシステムにバグを直接送信するための欠陥トラッキングサーバです。カスタマイズされたバグトラッキングシステムの作成方法については、バグトラッカプラグインの作成を参照してください。
パーサプラグイン	OpenText Core (Debricked)およびSonatypeからのオープンソースセキュリティデータの表示を可能にするプラグインです。サードパーティ製のパーサプラグインを接続することもできます。
電子メールサーバ	アプリケーションの共同作業者にアラートを送信するサードパーティのSMTP電子メールサーバです。
サードパーティのLDAP認証サーバ	LDAP認証を使用する外部ユーザ管理システムです。
Kubernetes	Application Securityの展開に対応したコンテナオーケストレーションプラットフォームです。

1.4.2. 大まかな展開タスク

次の表は、Application Securityの展開のために実行する必要がある大まかなタスクを一覧表示しています。

Note

Application Securityをアップグレードする場合は、Application Securityのアップグレードを参照してください。

タスク	説明(Description)	情報と手順
展開と初期設定の準備 展開と初期設定に必要な配布ファイル、ライセンスファイル、データベース資格情報、およびシードバンドルを収集します。		
1	インストールパッケージと `fortify.license` ファイルをダウンロードします。	Application Securityファイルのダウンロードと解凍
2	使用する予定のデータベースサーバソフトウェアをインストールして設定します。	Application Securityデータベースについて
3	(上級ユーザの場合のみオプション) Application Securityを展開する前に自動設定ファイルを設定して、展開と設定を自動化します。	Application Securityの設定の自動化
Tomcatサーバに展開する		
4	Tomcatサーバに Application Securityを展開します。	WARファイルを `<tomcat>/webapps/` ディレクトリにコピーし、Tomcatサーバを起動します。
初期設定の実行		

タスク	説明(Description)	情報と手順
5	初期設定を実行します(ライセンスファイルの提供、データベーステーブルの作成、データベーススキーマの初期化、コア設定の設定、データベースのシードなど)。	これを行うには、次の2つの方法があります。 • セットアップウィザードを使用して初期設定を実行する Application Securityの初回設定 • *上級ユーザのみ* 自動初期設定 Application Securityの設定の自動化
6	Application Securityに初めてサインインして、デフォルト以外の管理者アカウントを設定します。	Application Securityへのサインイン
7	シングルサインオンの設定、ユーザの管理、LDAPエンティティの登録、LDAPユーザ役割の管理、ユーザがアプリケーションに割り当て可能なカスタム属性の作成など、中核となる構成設定を完了します。	追加のApplication Security設定

タスク	説明(Description)	情報と手順
8	バグトラッキング統合の設定、パーサプラグインの管理、ユーザアカウント管理、セキュリティコンテンツの更新などの追加タスクを実行します。	追加のインストール関連タスク

1.4.3. Application Securityファイルのダウンロードと解凍

インストールパッケージと fortify.license ファイルを、ソフトウェアライセンスおよびダウンロード(SLD)ポータルから取得します。YouTube™にある役立つハウツービデオ「OpenText Software Fulfillment Trainingプレイリスト」では、OpenText Application Security Softwareのダウンロード方法も説明されています。

Application Securityインストールファイルを解凍するには、次の手順に従います。

1. インストールパッケージの内容を安全な場所にある一時ディレクトリに抽出します。
2. 配布ファイル(Fortify_*<version>*_Server_WAR_Tomcat.zip)を探し、すべての内容を安全な場所にあるディレクトリに抽出します。

   これには、Application Securityの設定や以前のバージョンからのアプリケーション移行などのタスクに必要なリソースとツールを含む ssc.war ファイルが含まれています。

   > **Note**
   >
   > 配布ファイルの内容を抽出するディレクトリは、すべてのトピックで*<ssc_distribution_dir>*ディレクトリと呼ばれます。

3. シードバンドルファイルを一時ディレクトリの srg_content ディレクトリから*<ssc_distribution_dir>*ディレクトリにコピーします。シードバンドルファイルを解凍しないでください。

   > **Note**
   >
   > リソースファイルを*<ssc_distribution_dir>*ディレクトリにコピーすることは求められていませんが、このドキュメントの手順は、ファイルをその場所に保存したという前提に基づいています。

   次の表で、シードバンドルについて説明します。

シードバンドルファイル名	説明
Fortify_Process_Seed_Bundle-2025_Q2_<*build*>.zip	データベーステーブルのシードに使用されるプロセステンプレートシードバンドル。デフォルトの管理者ユーザアカウントと問題テンプレートデータを提供します。
Fortify_Report_Seed_Bundle-2025_Q2_<*build*>.zip	データベーステーブルのシードに使用されるシードバンドルをレポートします。デフォルトのレポートセットを提供します。
Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<*build*>.zip	(オプション) PCI基本シードバンドルは、Payment Card Industry (PCI) Data Security Standard (DSS)プロセステンプレートと関連レポートを、デフォルトの問題テンプレートおよびレポートセットに追加します。2022年10月以降、PCI Software Security Framework(SSF)が評価の基準になりました。PCI SSF標準の下で、ソフトウェアセキュリティの問題が評価にどのような影響を与えるのかを学ぶために、PCI SSF基本シードバンドルを使用してください。

シードバンドルファイル名	説明
`Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<build>.zip`	(オプション) PCI SSF基本シードバンドルは、Payment Card Industry (PCI) Software Security Framework (SSF) プロセステンプレートと関連レポートを、デフォルトの問題テンプレートおよびレポートセットに追加します。PCI SSFは、支払いソフトウェアベンダが開発したシステムを評価するための一連の新しい標準として、2019年6月に導入されました。2022年10月以降、PCI Software Security Framework(SSF)が評価の基準になりました。PCI DSSでの評価には、PCI基本シードバンドルを使用してください。

4. `fortify.license` ファイルを*<ssc_distribution_dir>*ディレクトリにコピーします。

参照情報

大まかな展開タスク

1.4.4. Application Securityデータベースについて

Application Securityの新しいインスタンスを展開する場合は、まず、サードパーティのデータベースサーバソフトウェアをインストールして設定する必要があります。データベース要件については、『*Application Securityソフトウェアのシステム要件*』ドキュメントを参照してください。

Important

- Application Securityでは、すべてのデータベーススキーマ照合で大文字と小文字を区別する必要があります。
- SQL ServerまたはMySQLデータベースをインストールする場合、インストールには特別な注意が必要です。詳細については、「SQL Serverデータベースの使用」または「MySQLデータベースの設定」を参照してください。

その後、初めてApplication Securityを設定する際に、セットアップウィザードを使ってデータベースへのコネクティビティを設定し、それからデータベースをシード処理します(「Application Securityの初回設定」を参照)。

このセクションでは、次のトピックについて説明します。

1.4.4.1. JDBCドライバについて

SQL Server、MySQLサーバ、およびOracleデータベース用のJDBCドライバは、Application Securityソフトウェアにバンドルされています。

MariaDB JDBCドライバは、MySQLデータベースサーバに接続します。JDBC URLパラメータでは、MariaDBドライバ構文を使用する必要があります。なお、MariaDBは、Application Security用のデータベースとしてサポートされていません。

1.4.4.2. データベースサーバソフトウェアのインストールと設定

データベースソフトウェアのドキュメントの指示に従って、データベースサーバソフトウェアをインストールして設定します。サポートされているデータベースの詳細については、「*Application Securityソフトウェアのシステム要件*」ドキュメントを参照してください。

1.4.4.3. ディスクI/Oの監視

ディスクI/Oには、物理的なディスク上での入出力操作が含まれます。ディスク上のファイルからデータを読み取っている場合は、プロセッサは、ファイルが読み取られるのを待つ必要があります(ファイルにデータを書き込む場合も同様です)。Application SecurityはI/Oが多いデータベース操作を実行するので、パフォーマンスに影響が及びます。ディスクサブシステムの読み取り/書き込みが低レイテンシになるようにしてください。

アプリケーションのバージョン、アーティファクト、保存されたレポート、データエクスポート、イベントログなどのApplication Securityのオブジェクトクリーンアップアクションを実行しても、データベース管理者がデータベースを再最適化するまでは、データベースストレージの割り当てが実際に減少しない場合があります。Application Securityデータベースの定期的な監視と最適化をお勧めします。

1.4.4.4. データベースユーザアカウント許可

Application Securityデータベースで次のタスクを実行するユーザのアカウントを作成することを強く推奨します。

- ランタイムタスクの実行

  ランタイムタスクを実行するユーザには、次の操作を行う許可が必要です。

  - DML (Data Manipulation Language)操作を実行して、すべてのデータベーステーブルおよびビューでデータをSELECT、UPDATE、INSERT、およびDELETEする
  - ストアドプロシージャを実行する

- マイグレーションスクリプトの実行

  > **Important**
  >
  > マイグレーションスクリプトの実行用のユーザアカウントを別に作成することを強く推奨します。

  マイグレーションスクリプトを実行するユーザには、次の操作を行う許可が必要です。

  - DML (Data Manipulation Language)操作を実行して、すべてのデータベーステーブルおよびビューでデータをSELECT、UPDATE、INSERT、およびDELETEする
  - ストアドプロシージャを実行する
  - DDL (Data Definition Language)操作を実行して、データベーステーブル、ビュー、およびインデックスをCREATE、ALTER、およびDROPする
  - Oracleデータベースの場合、シーケンスを有効にする許可

- データベースの作成と管理

  > **Important**
  >
  > データベースの作成と管理に使用するユーザアカウントを別に作成することを強く推奨します。

  データベースを作成および管理するユーザには、次の操作を行う許可が必要です。

  - マイグレーションスクリプトを実行するユーザが許可を持つすべてのタスクを実行する
  - 専用インスタンスにApplication Securityデータベースを作成する
  - 既存のApplication Security専用データベースインスタンスをバックアップして更新する
  - 専用データベースインスタンスにApplication Securityユーザアカウントをバインドする

  - Application Securityデータベースの作成、初期化、および管理に必要な読み書き許可をApplication Securityユーザアカウントに割り当てる

    少なくとも、このユーザはWebアプリケーションがデータベースに接続できるデータベースアカウントを持っている必要があります。

- **レポートの作成と生成**

  レポーティングにさらなるセキュリティ対策を追加するには、Application Securityデータベースに対する読み込み専用アクセスを持つデータベースユーザアカウントを作成し、アカウント資格情報を使用して、BIRTレポートのセキュリティを設定します(「BIRTレポート用のセキュリティの設定」を参照)。

1.4.4.5. データベース固有の設定要件

次のトピックでは、サポートされるサードパーティデータベースの設定要件と、Application Securityで使用するようにデータベースを設定する方法について説明します。

1.4.4.5.1. SQL Serverデータベースの使用

Application SecurityデータベースとしてSQL Serverデータベースを使用するには、次のチェックを実行します。

- データベースの［Auto Update Stats Asynchronously］(`AUTO_UPDATE_STATISTICS_ASYNC`)オプションを有効にします。

  手順については、Microsoft SQLドキュメントのWebサイトを参照してください。

- SQL Serverデータベーススキーマの照合で*大文字と小文字が区別されている*ことを確認します。SQL Serverのデフォルトのインストールでは、*大文字と小文字が区別されません*。

  > **Important**
  >
  > OpenTextで提供されたSQLスクリプトを実行する前に、データベースへの接続が開いていないことを確認します。

- インストール時に使用されたデータベーススキーマで、スナップショットの分離が有効になっている(`ALLOW_SNAPSHOT_ISOLATION` と `READ_COMMITTED_SNAPSHOT` が `ON` に設定されている)ことを確認します。
- SQLスクリプトの実行中にクライアントツールをチェックして、［ANSI null default］オプションが `ON` に設定されていることを確認します。

  これを実行するには、 `SET` コマンド(`ANSI_NULL_DFLT_ON` を `ON` に設定)とクエリエディタのいずれかを使用します。

Windowsドメイン認証

Windowsドメイン認証の場合は、Application Securityを展開する前に、次の追加ステップを実行する必要があります。

1. `integratedSecurity=true` がJDBC URLに追加されていることを確認します。
2. `mssql-jdbc_auth-<version>-<arch>.dll` ファイルを取得します。

   詳細については、Windows Microsoftのドキュメントで「統合認証を使用して接続する」を参照してください。

3. `mssql-jdbc_auth-<version>-<arch>.dll` 環境変数の `-Djava.library.path` パラメータに指定されたディレクトリに `JDK_JAVA_OPTIONS` ファイルを配置します。

4. `PATH` 環境変数に含まれているディレクトリ(`C:\Windows\System32` など)に `mssql-jdbc_auth-<version>-<arch>.dll` ファイルを配置します。
5. 次のいずれかを実行します。
    - autoconfigファイルを使用してApplication Securityを設定します(「Application Securityの設定の自動化」を参照)。
    - SQL認証を使用してApplication Securityを設定してから、 `db.username` ファイルから `db.password` および `datasource.properties` パラメータを削除します。
6. データベースへの接続に使用するドメインアカウントでTomcatが実行されていることを確認します。

1.4.4.5.2. MySQLデータベースの使用

Important

MySQL 8.0は25.4リリースまでサポートされます。26.2リリース以降、サポート対象データベースバージョンはMySQL 8.4となります。移行手順については、「MySQL 8.0からMySQL 8.4への移行」をご覧ください。

Application SecurityデータベースとしてMySQLを使用するには、MySQLオプションファイルを設定する必要があります。サポートされているバージョンのMySQLの詳細については、「*Application Securityソフトウェアのシステム要件*」ドキュメントを参照してください。

Caution

Application Securityでは、すべてのデータベーススキーマ照合で*大文字と小文字を区別する*必要があります。インストールで*大文字と小文字が区別されていない*場合は、Application Securityが正常に動作しません。

Tip

SSLを使用してApplication SecuritvをMvSQLに接続する場合、`max_connections`システム変数(`my.cnf`ファイル内)の値を増やして、許可される同時クライアント接続数を増やすことを推奨します。これにより、`Too many connections`エラーが発生しなくなります。

MySQL 8.4オプションファイルを設定するには:

1. MySQLサーバを停止します。
2. MySQLサーバのインストールディレクトリに移動します。
3. MySQLオプションファイルをテキストエディタで開きます。

   Tip

   オプションファイルとそれらを読み取る順序を見つけるには、端末から次のコマンドを実行します: `mysql --help`。

   - Windowsシステムでは、デフォルトのオプションファイルは`my.ini`です。
   - Linuxシステムでは、デフォルトのオプションファイルは`my.cnf`です。
4. `[mysqld]`セクションと`[mysqldump]`セクションの両方で、`max_allowed_packet`を`1G`に設定します。

`[mysqldump]` セクションがない場合は、作成します。

5. `[mysqld]` セクションでは、次の表で説明されている設定を設定します。一覧表示された設定がファイルに含まれていない場合は、追加します。

設定	値
innodb_buffer_pool_size	512M (10GB以上を推奨) すべてのデータとインデックスが適合すると、最高のパフォーマンスが達成されます。 接続ごとのメモリと合計して、innodb_lock_wait_timeout値がサーバ上で使用可能なメモリの合計を超えないようにしてください。メモリ使用量の最大見積もりは、次のとおりです。 max_connections * max_allowed_packet + innodb_buffer_pool_size innodb_buffer_pool_sizeの値は、使用可能なメモリの60～80%が適切です。 innodb_buffer_pool_size値が大きいほど、テーブル内のデータにアクセスするために必要なディスクI/Oが少なくなります。専用データベースサーバでは、マシンの物理メモリサイズの最大80%に設定できます。ただし、次の場合は、この値を小さくすることを検討してください。 ◦ 物理メモリの競合により、オペレーティングシステムでページングが発生します。 ◦ InnoDBはバッファおよび制御構造用に追加のメモリを予約します。そのため、割り当てられるスペースの合計は、指定したサイズより約10%大きくなります。 ◦ アドレススペースは連続している必要があります。これは、特定の

設定	値
	アドレスにロードされるDLLを使用するWindowsシステムで問題を引き起こす可能性があります。 ◦ バッファプールの初期化にかかる時間は、そのサイズに比例します。大規模なインストールでは、この初期化時間が膨大になることがあります。たとえば、最新のLinuxx86_64サーバでは、10 GBのバッファプールの初期化に約6秒かかります。詳細については、『MySQL 8.4リファレンスマニュアル』を参照してください。
innodb_lock_wait_timeout	300 (推奨)、秒で表します
max_allowed_packet	1073741824
sql-mode	"TRADITIONAL"。これは STRICT_TRANS_TABLES、STRICT_ALL_TABLES、NO_ZERO_IN_DATE、NO_ZERO_DATE、ERROR_FOR_DIVISION_BY_ZERO、NO_ENGINE_SUBSTITUTION と同じです。
innodb_redo_log_capacity	1073741824 詳細については、『MySQL 8.4リファレンスマニュアル』を参照してください。
log_bin_trust_function_creators	1

Microsoft® Azure®に適用可能な追加設定

設定	値
sql_generate_invisible_primary_key	OFF
default_storage_engine	INNODB

Amazon Web Servicesに適用可能な追加設定

設定	値
default_storage_engine	INNODB

Google Cloud Platform™に適用可能な追加設定

設定	値
default_tmp_storage_engine	INNODB

6. ファイルを保存し、MySQLサーバを再起動します。

MySQL 8.0からMySQL 8.4への移行

以下のいずれかのオプションを使用して、MySQL 8.0データベースをMySQL 8.4に移行できます。

シナリオ1

MySQL 8.0を使用したApplication Securityからのアップグレード(バージョン24.4以降)

1. Tomcatサーバを停止します。
2. `<tomcat>/webapps/` ディレクトリからWARファイルを削除してから、新しいWARファイルを `<tomcat>/webapps/` ディレクトリにコピーします。

Note

- `<tomcat>` は、Tomcatインスタンスのルートディレクトリを表します。
- 現在のApplication SecurityバージョンではTomcat 10.1とJava 21が使用されています。古いバージョンのTomcatやJavaを使用している場合は、必要なバージョンにアップグレードしてください。

3. Tomcatサーバを起動します。
4. ブラウザを開き、アプリケーションセキュリティのWebアドレスを入力してセットアップウィザードを起動します。

5. セットアップウィザードを使用して、マイグレーションSQLスクリプトを生成します「アップグレード後のApplication Securityの設定」を参照してください。
6. MySQL 8.0を使用した26.2 Application Securityの設定が完了し、動作確認が取れたら、ログにエラーが記録されていないことを確認します。
7. Tomcatサーバを停止します。
8. `<fortify Home Directory>/ssc/conf` の下に `datasource.properties` ファイルのバックアップを作成してから `datasource.properties` を削除します。
9. MySQL 8.0データベースのSQLダンプを作成します (https://dev.mysql.com/doc/refman/8.0/en/mysqldump.htmlセクションを参照)。

   Note
   - すべての関数とプロシージャを含めるには、`mysqldump` 作成時に `--routines` オプションと `--triggers` オプションを含めます。
   - 必要に応じてデータを使用できるよう、MySQL 8.0ダンプのバックアップを必ず作成してください。

10. MySQL 8.4で、ダンプをインポートしてテーブルを作成します (https://dev.mysql.com/doc/refman/8.4/en/programs-client.htmlセクションを参照)。

    Note
    MySQL 8.4では、MySQL 8.0と同じユーザ名とデータベース名を使用することを推奨します。

11. Tomcatサーバを起動します。
12. ブラウザを開き、アプリケーションセキュリティのWebアドレスを入力してセットアップウィザードを起動します。
13. セットアップウィザードを使用して、マイグレーションSQLスクリプトを生成します「アップグレード後のApplication Securityの設定」を参照し、MySQL 8.4設定用にユーザ名、パスワード、JDBC URLを更新します。
14. データベースでマイグレーションスクリプトを実行します「データベースアップグレードスクリプトの実行準備」を参照してください。
    1TBを超えるデータを含むデータベースの移行には、5時間以上かかる場合があります。
15. セットアップウィザードを使用してデータベースを再シードします。

シナリオ2

MySQL8.0から MySQL8.4へのアップグレード(26.2 Application Security)

1. Tomcatサーバを停止します。

2. `<tomcat>/webapps/` ディレクトリからWARファイルを削除してから、新しいWARファイルを `<tomcat>/webapps/` ディレクトリにコピーします。

   Note
   `<tomcat>` は、Tomcatインスタンスのルートディレクトリを表します。

3. MySQL 8.0データベースのSQLダンプを作成します(https://dev.mysql.com/doc/refman/8.0/en/mysqldump.htmlセクションを参照)。

   Note
   - すべての関数とプロシージャを含めるには、 `mysqldump` 中に `--routines` オプションと `--triggers` オプションを含めます。
   - データを使用する場合に備えて、MySQL 8.0ダンプのバックアップを必ず作成してください。

4. MySQL 8.0をMySQL 8.4にアップグレードし、設定とサーバパラメータを更新し、MySQLサーバを再起動します。

5. Tomcatサーバを起動します。

6. ブラウザを開き、アプリケーションセキュリティのWebアドレスを入力してセットアップウィザードを起動します。

7. セットアップウィザードを使用して、マイグレーションSQLスクリプトを生成します

   「アップグレード後のApplication Securityの設定」を参照し、必要に応じてMySQL 8.4の設定データベースを更新します。

8. データベースでマイグレーションスクリプトを実行します(「データベースアップグレードスクリプトの実行準備」を参照)。

   1TBを超えるデータを含むデータベースの移行には、5時間以上かかる場合があります。

9. セットアップウィザードを使用してデータベースを再シードします。

1.4.4.5.3. Oracleデータベースの使用

このセクションでは、データベース関連のエラーを防ぐためにOracleデータベースを設定する方法について説明します。

1.4.4.5.3.1. 「No more data to read from socket」エラーの防止

OracleをApplication Securityデータベースとして使用する場合、「No more data to read from socket」というタイプの例外が表示される場合があります。

この例外に対して考えられる解決策の1つは、次を実行することです。

1. `$ORACLE_HOME/network/admin/` ディレクトリに移動します。
2. テキストエディタで `tnsnames.ora` ファイルを開きます。
3. `SERVER` の値を `DEDICATE` に設定します。
4. 変更を適用するには、データベースに関連付けられた有効なリスナを再起動します。

1.4.4.5.3.2. Oracleデータベースのパーティショニングによるパフォーマンスの改善

Oracleデータベース内の大量のデータに関連する大規模な入出力によって、データベースサーバが効果的にデータを操作できなくなる可能性があります。データベースパーティショニングにより、データベースサーバのパフォーマンスが向上し、データの管理と可用性が向上します。

ユーザは、自分の環境に最適なパーティション化を含むデータベースの最適化を特定して実装するために、DBAと一緒に作業する必要があります。OpenTextは、特定のデータベースの最適化や機能拡張に関するテクニカルサポートを検証または提供しているのではありません。

データベースパーティショニングや他のデータベースの最適化を実装する前に、次の操作を行うことを強く推奨します。

1. データベースをバックアップします。
2. 非運用環境で変更をテストして検証してから、実稼働データベースを変更します。

OpenTextでは、データベースのパーティショニング時に顧客データベースを最適化するためのガイダンスを提供していませんが、次の点を確認してください。

1. パーティションの数は、データの増加を許容するものである必要があります。
2. 1つのパーティションにつき100万レコード未満のレコードを分配することを検討してください。
3. データベースのパーティショニングには時間がかかる場合があります。データをパーティション分割するために十分なアプリケーションのダウンタイムを割り当てる必要があります。
4. パーティション化の後には、ジョブ実行スレッドの数を増やして最適化を検討します。
    1. ジョブ実行スレッドは、`<fortify.home>/<app_context>/conf/app.properties` ファイル内の `jobs.threadCount` プロパティによって設定されます。
5. パーティションを最適化すると、マイグレーションスクリプトと競合する可能性があります。 そのような場合、お客様のDBAは、製品のアップグレード時に適用される最適化を処理するために、マイグレーションスクリプトまたはパーティションスクリプト(あるいはその両方)を手動で調整する必要があります。

1.4.4.6. Application Securityデータベーステーブルおよびスキーマについて

Application Security配布ディレクトリ(*<ssc_distribution_dir>*)には、サポートされているサードパーティのデータベースタイプごとに初期化SQLスクリプトが含まれます。初期設定時(「Application Securityの初回設定」を参照)に、データベースタイプに対してこのスクリプトを実行してデータベーステーブルを作成し、Application Securityのデータベーススキーマを初期化します。

Application Securityを初めて設定する前に、以下のセクションで説明されている情報を確認してください。

- データベースユーザアカウント許可
- データベース固有の設定要件

1.4.4.7. Application Securityデータベースのシード処理について

初めてApplication Securityにサインインするときには、Application Securityでは最初のログインアカウント情報の処理と基本機能の提供のために、最小限のデータセットが必要です。シード処理によって、新しいデータベースの最小データセットが作成されます。

インストール後の一貫した設定を維持するには、Application Securityデータベースのシード処理が必要です。これには、デフォルトの管理者ユーザアカウントの作成や、問題テンプレート、レポート定義、Application Securityの運用に必要なその他のデフォルトデータなどの必須エンティティの作成が含まれます。

Application Securityには、ダウンロード済みシードバンドルが2つ必要です(「Application Securityファイルのダウンロードと解凍」を参照)。

- 問題テンプレートシードバンドル(`Fortify_Process_Seed_Bundle-2025_Q2_<build>.zip`)では、デフォルトの管理者ユーザアカウントと問題テンプレートデータを提供します。
- レポートシードバンドル(`Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip`)は、レポートのデフォルトセットを提供します。

オプションのPCI基本バンドル `Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_<build>.zip` および `Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<build>.zip` をインストールすることもできます。これらは、Payment Card Industryプロセステンプレートと関連レポートをテンプレートおよびレポートのデフォルトセットに追加します。

シードバンドルファイルはApplication Securityインストールパッケージに含まれています。初期展開後には、Application Securityカスタマポータル の［**PREMIUM CONTENT**］>［**FORTIFY EXCHANGE**］から、オフサイクルシードバンドルをダウンロードできます。四半期ごとのセキュリティコンテンツリリースには、更新されたシードバンドルが含まれることもあります。

Caution

Application Securityリリースに同梱されているバンドルのみを同じバージョンのApplication Securityインスタンス(新規インストールまたは現在のバージョンにアップグレードされた古いインスタンス)にロードします。

データベースのシード処理が終了したら、シードプロセスで作成されたユーザ設定可能なデータエンティティをApplication Securityユーザインタフェースから変更できます。詳細については、追加のApplication Security設定を参照してください。

参照情報

四半期ごとのOpenText SAST Application Security Contentリリースで提供されるレポートシードバンドルを使用したデータベースのシード処理

1.4.4.8. Application Securityデータベースの永久削除

ある時点でApplication Securityを完全に削除する予定がある場合は、Application Securityデータベースを削除できます。Application Securityデータベーススキーマとデータベース内のすべてのデータを完全に削除するには、`drop-tables.sql`スクリプトを実行します。

Caution

`drop-tables.sql`スクリプトを実行すると、Application Securityデータベーススキーマとデータベース内のすべてのデータが完全に削除されます。このスクリプトを実行する前に、保存するデータを必ずバックアップしてください。

Application Securityデータベーススキーマとデータベース内のすべてのデータを削除するには、次の手順を実行します。

1. `<ssc_distribution_dir>/sql/`ディレクトリに移動し、Application Securityで使用する予定のサードパーティデータベースのサブディレクトリを開きます。
   - `mysql`
   - `Oracle`
   - `sqlserver`
2. Application Securityデータベースタイプに一致するサブディレクトリから、`drop-tables.sql`スクリプトを実行するデータベースサーバまたは他の場所にコピーします。
3. データベースクライアントプログラムで、Application Securityで使用するために作成したデータベースアカウントにログインします。
4. このトピックの冒頭にある注意事項を確認します。
5. 次のスクリプトを実行して、Application Securityデータベーススキーマとデータベース内のすべてのデータを削除します。

```
drop-tables.sql
```

1.4.5. KubernetesでのApplication Securityの展開について

Kubernetesで完全なApplication Securityコンテナのオーケストレーションを行う場合は、`helm-ssc`のHelmチャートを設定して使用できます。このHelmチャートは、https://hub.docker.com/r/fortifydocker/helm-sscにあります。

> **Note**
>
> 製品のリリース直後には、Helmチャートを利用できない場合があります。現在のリリースのHelm chartチャートが使用可能な場合、そのドキュメントは、Application Security Documentation Webサイトで利用できます。

Application Security Kubernetes展開の準備および実行の手順については、「Kubernetesにおける SSCの展開」を参照してください。

必要なソフトウェアのサポートされているバージョンの詳細については、「*Application Securityソフトウェアのシステム要件*」(オプション)ドキュメントを参照してください。

Application SecurityをKubernetesクラスタへ展開する

Application Security をインターネットにアクセスできる環境、またはエアギャップされた環境に展開できます。アプリケーションをインターネットにアクセスできる環境に展開する予定の場合は、Application Security Dockerイメージ(fortifydocker/ssc-webapp)をDocker Hubレジストリから取得できます。エアギャップされた環境でアプリケーションを展開する必要がある場合は、プライベートレジストリを展開に使用し、そこにApplication Securityコンテナイメージを転送する必要があります。

エアギャップ展開では、Kubernetesクラスタからアクセス可能なプライベートレジストリにApplication Securityコンテナイメージをプッシュする必要があります。

Application SecurityをKubernetesクラスタに展開するには:

1. Docker Hubアカウントを作成して、アカウント名をカスタマサポートに伝えます。

   カスタマサポートから、Fortify Dockerリポジトリへのアクセスが付与されます。

   Fortify Dockerリポジトリに公開されているApplication Security Dockerイメージへのアクセス権を要請するには、次の情報を含む電子メールをmfi-fortifydocker@opentext.comへ送信します。

   - 名

- 姓
- 会社名
- Docker ID
- カスタマID

2. (エアギャップされたインストール、またはプライベートレジストリの場合。稼動中のDockerサーバとDockerクライアントが配置されているものとみなされます。)次のように、Application Securityコンテナイメージをプライベートレジストリに転送します。

    1. `docker login` を使用してDocker Hubにログインします。
    2. `docker login <priv_reg_host_and_port>` を使用してプライベートレジストリにログインします。ここで、 `<priv_reg_host_and_port>` は、プライベートレジストリのホストとポートを表します。
    3. 次のように、Application Securityコンテナイメージを転送します。

        1. ```
           docker pull "fortifydocker/ssc-webapp:<tag>"
           ```
        2. ```
           docker tag "fortifydocker/ssc-webapp:<tag>" "
           <priv_reg_host_and_port>/<priv_reg_path>/ssc-
           webapp:<tag>"
           ```
        3. ```
           docker push "
           <priv_reg_host_and_port>/<priv_reg_path>/ssc-
           webapp:<tag>"
           ```
           ```

Note

*<tag>*に使用する値を決定するには、`<ssc_helm_dir>` ディレクトリに移動して、`ssc-<chart_version>+<ssc_version>.tgz` ファイルを開きます。TGZファイル名の `<ssc_version>` 値(最新の公開イメージビルドのタグ)を使用します。

また、正確なイメージビルドのタグも次の形式で用意されています: `<ssc_version>.<imageBuildNumber>`

Docker Hubで使用可能なイメージタグを一覧表示できます。`<imageBuildNumber>` を使用する場合は、それを `image.buildNumber` Helmチャートの値で指定する必要があります。

Important

イメージ名(`ssc-webapp`)とタグ(`<tag>`)の値を変更してはなりません。

4. *<ssc_helm_dir>*/ssc-values.yaml ファイルで `image.repositoryPrefix` パラメータの値として「 *<priv_reg_host_and_port>*/*<priv_reg_path>*/ 」を入力します。

   `image.repositoryPrefix` パラメータに指定する値は、末尾にスラッシュ(/)を含める必要があります。

3. 正確なイメージビルドタグを使用する場合は、`<imageBuildNumber>` の値として `image.buildNumber` 値を入力します。それ以外の場合は、空のままにします。

4. レジストリ(Docker Hubまたはプライベートレジストリ)からイメージを取得するためのKubernetesシークレットをプロビジョニングします。手順については、`https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry` を参照し、*<ssc_helm_dir>*/ssc-values.yaml ファイルで `imagePullSecrets` パラメータの値としてシークレット名を入力します。シークレットが `regcred` である場合のフォーマットは次のとおりです。

   ```
   imagePullSecrets:
   - name: regcred
   ```

> **Note**
>
> `imagePullSecrets` 値は、Docker Hubレジストリへのアクセスに必要です。資格情報なしでアクセスできるプライベートレジストリがある場合は、 `imagePullSecrets` を指定する必要はありません。

5. (オプション)機密データを暗号化するための `secret.key` ファイルを準備します。
    1. 初めてApplication Securityを展開する場合は、標準配布の `bin` ディレクトリでパスワードツールを見つけ、次のコマンドを実行して新しいキーストアを生成する必要があります。

        `<ssc_distribution_dir>/bin pwtool secret.key`

        新しい `secret.key` ファイルが生成されます。

        Enterキーを押し、暗号化する文字列を入力します。
    2. コンテナ化されていないApplication SecurityをKubernetesクラスタに移行する場合は、次のディレクトリで既存のsecret.keyを見つける必要があります:

        `<fortify.home>/<app_context>/conf`

        secret.keyの場所の詳細については、「<fortify.homeディレクトリについて」を参照してください。
6. 必要な他のパラメータを `values.yaml` ファイルに入力します。
    - `urlHost` は Application Security へのアクセスを目的とした完全修飾DNS名を含んでいる必要があります。Application Security インストールにアクセスするためのアドレスは `<https://<hostname>:<service.httpsPort>/<sscPathPrefix>` です。たとえば、 `https://ssc.example.com:443/ssc` になります。ポートが443の場合は、URL(`https://ssc.example.com/ssc`)から省略できます。
    - 使いやすくするために、 `service.type` パラメータを `LoadBalancer` に設定することをお勧めします。
    - `secretRef.name` によって参照されるApplication Securityシークレットに変更を適用するには、ssc-webapp Podを手動で削除する必要があります(これは後ほど自動的に再作成されます)。

Note

必要に応じて、 values.yaml ファイルでパラメータに指定するほとんどの値を後で変更してから、Application Securityを再展開して変更を実装できます。Kubernetesクラスタによっては、例外は persistentVolumeClaim のパラメータとなる場合があります。

Tomcatアクセスログのカスタマイズ

ssc-webapp コンテナイメージでTomcatアクセスログのデフォルトフォーマットを変更するには、 HTTP_SERVER_ACCESS_LOG_PATTERN 環境変数をTomcat Access Log Valveのパターンに設定します。サポートされているパターンの詳細については、Apache Tomcat Configuration ReferenceのWebサイトを参照してください。

次の例に示すように、環境Helmチャート値を使用できます。

```
environment: - name: HTTP_SERVER_ACCESS_LOG_PATTERN value: '%h
%l %u %t "%r" %s %b'
```

Kubernetesクラスタへの展開のトラブルシューティング

このセクションでは、展開の試行中にエラーが発生した場合のトラブルシューティングのヒントを示します。

インストール段階でクラッシュした場合は、以下を実行します。

```
kubectl describe pod <pod_name>
```

インストール後にログを表示するには、以下を実行します。

```
kubectl logs <pod_name> -f
```

クラスタで実行中のPodのステータス(保留中、実行中、成功、失敗、または不明)を表示するには、以下を実行します。

```
kubectl get pods
```

Podが実行していない場合でも、インタラクティブ環境は前の状態を再ロードしています。数秒待って、もう一度 kubectl get pods を実行します。Podが実行しているのを確認した後、続行します。

すべてのサービス、割り当てられたIP (クラスタおよび外部)、およびポートのリストを表示するには、以下を実行します。

```
kubectl get services
```

それらの名前を一覧にするには、以下を実行します。

```
helm list
```

Helmによってインストールされた特定の展開の値/設定を取得するには、以下を実行します。

```
helm get values <installation_name>
```

マウントされているボリュームに関する情報を表示したり、イメージが正常に引き出されたかどうかを確認したりするには(たとえば、間違った資格情報が提供された場合)、以下を実行します。

```
kubectl describe --help
```

すべてが良好に見えても、Application Securityが想定どおりに動作せず、ログだけでは十分な情報が得られない場合は、以下を実行してコンテナファイルシステムを検査し、環境の状態をチェックし、詳細なデバッグタスクを実行します。

```
kubectl exec -it <pod_name> bash
```

これにより、コンテナのインタラクティブなブラウズと、他の内部ログ(TomcatまたはApplication Security自体)の出力と、他のコマンドの実行が可能になります。

展開のトラブルシューティングに関する視覚的なガイドについては、『Kubernetes展開のトラブルシューティングに関する視覚的なガイド』を参照してください。コンテナ化されたアプリケーションに関する一般的な問題のデバッグについては、「アプリケーションのトラブルシューティング」を参照してください。

1.4.6. ディレクトリについて

*<fortify.home>*ディレクトリは、設定ファイルおよび他のApplication Securityリソースが存在する場所です。

Application Securityの展開後、 `<fortify.home>` は次の場所にあります。

- Windowsシステムの場合: `%USERPROFILE%\.fortify`

  標準ユーザとWindowsサービスユーザの両方に適用されます。

  Note

  `%USERPROFILE%` は、Tomcatサービスを実行しているユーザを表します。Tomcatをインストールしたユーザとは限りません。

  ```
  Named Account = C:\Users\<username>
  LocalSystem [Default] = %WinDir%\System32\config\systemprofile
  LocalService = %WinDir%\ServiceProfiles\LocalService
  NetworkService = %WinDir%\ServiceProfiles\NetworkService
  ```

- Linuxシステムの場合: `$HOME/.fortify`

1.4.6.1. デフォルトの場所の変更

Tomcatサーバの起動に使用するJVM上で `fortify.home` システムプロパティを設定することにより、デフォルトの*<fortify.home>*ディレクトリの場所を上書きできます。たとえば、 `CATALINA_OPTS` 環境変数を使用してこのシステムプロパティを指定できます。または、WindowsシステムのTomcatサービス定義にある［Javaオプション(Java Options)］フィールドに `fortify.home` プロパティを追加することもできます。Javaシステムプロパティの設定の詳細については、Tomcatのマニュアルを参照してください。

例:

```
-Dfortify.home=/home/fortify
```

Note

Application Securityを設定(「Application Securityの初回設定」を参照)した後に、*<fortifv.home>*ディレクトリの場所を変更するには、更新後の `fortify.home` システムプロパティ値を使用してサーバを再起動する前に、既存の*<fortify.home>*ディレクトリの内容を新しい場所にコピーするか、移動してください。

1.4.6.2. ディレクトリの内容

<fortify.home> ディレクトリは次のように構成されています。

```
<fortify.home>   <app_context>/ conf/ app.properties
datasource.properties log4j2.xml secret.key version.properties
logs/ ssc.log ssc_plugins.log ... init.token plugin-framework/
fortify.license
```

ここで

- <app_context>

  Application Securityが展開されるアプリケーションサーバコンテキストです。詳細については、Application Securityの設定の自動化を参照してください。

- app.properties

  お客様が設定できるアプリケーションプロパティが含まれているファイルです。Application Securityの設定を自動化する場合、このファイルは起動ごとにautoconfigファイル内の appProperties キーに基づいて生成されます。詳細については、「Application Security設定の自動化」を参照してください。

- datasource.properties

  データベース接続プロパティが含まれているファイルです。Application Securityの設定を自動化する場合、このファイルは起動ごとにautoconfigファイル内の datasourceProperties キーに基づいて生成されます。詳細については、「Application Security設定の自動化」を参照してください。

- log4j2.xml

  デフォルトのログ設定が含まれているファイルです。この設定は手動で変更できますが、代わりにlog4j2設定上書き機能を使用することを強く推奨します(「ログ記録の設定」を参照してください)。

- secret.key

  Application Security内の重要な設定情報を暗号化および復号化するために使用される暗号化キーファイルです。このファイルがApplication Securityによって上書きされることはありません。ただし、このファイルが *<fortify.home>*/ *<app_context>*/conf/ ディレクトリにない場合は生成されます。

23.1.0より古いバージョンのApplication Securityを展開した場合は、`secret.key`を新しい形式に移行することをお勧めします。FIPS環境でApplication Securityを実行するには、`secret.key`を新しい形式に移行する必要があります。

詳細については、「secret.keyファイルの移行」を参照してください。

> **Note**
>
> `datasource.properties`ファイルおよび一部のデータベースフィールドには、`secret.key`ファイルに依存する暗号化されたエントリが含まれています。Application Securityインスタンスをコンピュータ間で移動する場合は、データベースファイルだけではなく`secret.key`ファイルも移動する必要があります。

- `version.properties`

  アプリケーションのアップグレードを目的として、Application Securityの現在および以前のバージョンに関する情報を格納するファイルです。

- `logs`

  Application Securityログファイルとプラグインログファイルを含むディレクトリです。

- `init.token`

  セットアップウィザードが読み込まれる(設定モードでサーバが起動する)たびに生成される新しいセキュリティトークンを含むファイルです。Application Securityを設定するユーザは、このトークンを使用してセットアップウィザードにアクセスします(「Application Securityの初回設定」を参照)。

- `plugin-framework`

  解凍されたプラグインを含むディレクトリであり、Application Securityによって完全に管理されます。

  > **Note**
  >
  > `plugin-framework`は、Application Securityによって自動的に管理され、バックアップを必要とする情報は含んでいません。

- `fortify.license`

  Application Securityライセンスファイルです。

Important

<fortify.home>/<app_context>/conf/ ディレクトリには、常に次のファイルが含まれている必要があります。

- app.properties
- datasource.properties
- log4j2.xml
- secret.key
- version.properties

これらのファイルのいずれかが見つからない場合、Application Securityは自動設定を実行するか、セットアップウィザードを起動して、不足しているファイルを再作成します。

1.4.6.3. secret.keyファイルのマイグレーション

Application Securityバージョン23.1.0以降では、FIPS環境で実行するために、secret.keyファイルの異なる形式を使用します。secret.keyはFIPS環境の外部で移行する必要があります。

`secret.key` のバージョンを確認し、secret.keyファイルを移行する必要があるかどうかを判断するために、 `secret.key` ファイルをテキストエディタで開きます。

更新された形式の `secret.key` には次のテキストが含まれていて、secret.keyを移行する必要がないことを示します。

`BEGIN FORTIFY SECRET KEY V1`

secret.keyファイルの取得

コンテナ化されていない展開では、 `secret.key` ファイルを `<fortify.home>/<app_context>/conf/` ディレクトリからコピーします。場所の詳細については、「<fortify.homeディレクトリについて」を参照してください。

コンテナ化された展開では、Kubernetesシークレットを使用して `secret.key` ファイルを作成した場合は、Kubernetesシークレットから `secret.key` を抽出します。それ以外の場合は、 `kubectl cp` コマンドを使用して、 `/fortify/ssc/conf/secret.key` ファイルを `container/fortify volume` からローカルファイルシステムにコピーします。

secret.keyファイルの移行

`<ssc_distribution_dir>/bin/` ディレクトリでマイグレーションツールを見つけて、次のコマンドを実行します。

```
<ssc_distribution_dir>/bin/pwmigtool <secret.key_file_to_migrate>
```

マイグレーションツールは、レガシーsecret.keyファイルの名前を `<secret.key_file_to_migrate>.pwtool-migration-backup` に変更します。

移行されたsecret.keyファイルの適用

コンテナ化されていない展開では、 `secret.key` ディレクトリにある `<fortify.home>/<app_context>/conf/` ファイルを置き換えて、Application Securityを再起動します。

コンテナ化された展開では、Kubernetesシークレットを使用して `secret.key` ファイルをプロビジョニングした場合は、シークレットを更新します。それ以外の場合は、 `kubectl cp` コマンドを使用して、 `/fortify/ssc/conf/secret.key` ファイルを `container/fortify volume` 内で置き換えます。

Application Securityの `webapp` ポッドを削除して再起動します。

1.5. Application Securityの初回設定

初めてApplication Securityをデプロイした後、ブラウザウィンドウにApplication SecurityのURLを入力すると、セットアップウィザードが開きます。セットアップウィザードを使用して、サーバの初期設定の手順を完了します。管理者にセットアップウィザードが使用可能になるのは、Application Securityを初めてデプロイした後、Application Securityをアップグレードした後、またはApplication Securityを保守モードにした後(「Application Securityの保守モードへの移行」を参照)に限られます。

初めて Application Securityを設定するには、次の手順に従います。

1. Tomcatサーバに新しいバージョンのApplication Security WARファイルをデプロイした後、ブラウザウィンドウを開き、Application SecurityサーバのURLを入力します(*<protocol>://<hostname>:<port>/<app_context>*)。

   > **Note**
   >
   > 標準的な展開の場合、デフォルトのApplication Security URLは *<protocol>://<hostname>:<port>*/ssc です。Kubernetesクラスタへの展開の場合、デフォルトのURLは *<protocol>://<hostname>:<port>* です(末尾に ssc を付けない)。
   >
   > 配布されたWARファイルを使用し、 ssc.war ファイルの名前を変更せずにApplication Securityをデプロイする場合、 <app_context> はTomcatサーバ設定で上書きされない限り、 ssc になります。

2. Webページの右上隅にある［**管理者(ADMINISTRATORS)**］をクリックします。
3. テキストエディタで *<fortify.home>/<app_context>*/init.token ファイルを開きます。

   TomcatがWindowsサービスとして実行されている場合、 init.token ファイルは %SystemRoot%\System32\config\systemprofile\.fortify\ssc\init.token にあります。

4. init.token ファイルの内容をクリップボードにコピーします。
5. セットアップウィザードのサインインで、 init.token ファイルからコピーした文字列を［**セキュリティトークン(Security Token)**］ボックスに貼り付けてから、［**サインイン(SIGN IN)**］をクリックします。
6. セットアップウィザードの［**開始(START)**］ページに記載されている情報を読んでから、［**次へ(NEXT)**］をクリックします。

7. ［**設定(CONFIGURATION)**］ページの［**FORTIFYライセンスのアップロード(UPLOAD FORTIFY LICENSE)**］で、次の操作を行います。

    1. ［**UPLOAD**］をクリックします。
    2. `fortify.license` ファイルを参照して選択し、［**UPLOAD**］をクリックします。

    セットアップウィザードに、環境設定ファイル(`app.properties` 、`datasource.properties` 、および `version.properties`)が格納される環境設定ディレクトリのデフォルトパスが表示されます。

8. 環境設定ファイルのディレクトリ内での機密情報に関する警告注意を読み、［**この警告を読んで理解しました(I have read and understood this warning)**］チェックボックスをオンにしてから、［**次へ(NEXT)**］をクリックします。

    このディレクトリの場所を変更する方法については、「<fortify.home>ディレクトリについて」を参照してください。

9. ［**コア環境設定(CORE CONFIGURATION SETTINGS)**］ページで、次の操作を行います。

    1. ［**FORTIFY SOFTWARE SECURITY CENTER URL**］で、Application SecurityサーバのURLを入力します。
    2. ［**HTTPホストヘッダ検証を有効にする(Enable HTTP host header validation)**］チェックボックスをオンにして、HTTP Hostヘッダ値がApplication SecurityのURL (`host.url` プロパティ)で設定された値と一致するようにします。

        ホストとポートの両方が一致している必要があります。これは、ブラウザにも、REST APIへの直接アクセスにも影響します。検証がオフの場合、あらゆるHTTP Hostヘッダが Application Securityにアクセスできます。

    3. グローバル検索を有効にするには、［**グローバル検索(GLOBAL SEARCH)**］ペインで次の操作を行います。

        1. ［**グローバル検索を有効にする(Enable global search)**］チェックボックスをオンにします。
        2. このチェックボックスの下にあるテキストボックスには、検索インデックスファイルのデフォルトの場所が表示されます。別の場所を使用する場合は、検索インデックスファイルの別のディレクトリパスを入力します。パスワードはインデックス付けされません。

            インデックス付けされたデータには機密情報(ユーザ名、電子メールアドレス、脆弱性カテゴリ、問題ファイル名など)が含まれる可

能性があるので、Tomcatサーバのユーザだけが読み込みおよび書き込みアクセス権を持つ安全な場所を選択してください。

> **Note**
>
> グローバル検索に必要なインデックス付けに最適なディスクサイズは、データの特性によって異なりますが、Luceneインデックスはデータベース内のデータよりはるかに小さくなります。たとえば、データベース問題ボリューム18GB(dbインデックス付き)に必要なインデックスサイズは約2GBです。

3. ［**グローバル検索(GLOBAL SEARCH)**］ペインに記載されている警告を読み、［**この警告を読んで理解しました(I have read and understood this warning)**］チェックボックスをオンにします。

10. ［**NEXT**］をクリックします。
11. ［**データソース(DATASOURCE)**］ページで、次の操作を行います。
    1. ［**データベースタイプ(DATABASE TYPE)**］リストから、Application Securityで使用するデータベースタイプを選択します。
    2. ［**データベースユーザ名(DATABASE USERNAME)**］ボックスに、データベースアカウントのユーザ名を入力します。

       詳細については、「データベースユーザアカウントの許可」を参照してください。
    3. ［**データベースパスワード(DATABASE PASSWORD)**］ボックスに、データベースアカウントのパスワードを入力します。

       ［**データベースユーザ名(DATABASE USERNAME)**］フィールドと［**データベースパスワード(DATABASE PASSWORD)**］フィールドで指定したデータベースユーザ資格情報が、マイグレーションスクリプトを実行するために必要な許可が与えられたユーザアカウントのものであることを確認します。これらの許可については、「データベースユーザアカウントの許可」で説明しています。
    4. ［**JDBC URL**］ボックスに、Application SecurityのURLを入力します。その際、次の点に注意してください。

       MySQLデータベースの場合:

- MySQLサーバが `sha256_password` または `caching_sha2_password` 認証プラグインを使用するように設定されている場合は、 `serverRsaPublicKeyFile` オプションを使用して、サーバRSA公開鍵をJDBCドライバに渡す必要があります。あるいは、セキュリティ保護の弱い `allowPublicKeyRetrieval` オプションを使用することもできます。詳細については、「MariaDB Connector/J」および「MySQL server」のドキュメントを参照してください。
- JDBC URLの末尾に、次の2つのステートメントを追加する必要があります。

  ```
  sessionVariables=collation_connection=<collation>
  rewriteBatchedStatements=true
  ```

  ここで、*<collation>*はデータベース照合タイプを表します。

  例:

  ```
  jdbc:mysql://<host>:3306/ssc?
  sessionVariables=collation_connection=utf8mb3_bin
  &rewriteBatchedStatements=true
  jdbc:mysql://<host>:3306/ssc?
  sessionVariables=collation_connection=latin1_gene
  ral_cs&rewriteBatchedStatements=true
  ```

  MariaDB JDBCドライバは、MySQLデータベースサーバに接続します。追加のJDBC URLパラメータでは、MariaDBドライバ構文を使用する必要があります。

SQL Serverデータベースの場合:

- JDBC URLの末尾に、次のプロパティ設定を追加する必要があります。 `sendStringParametersAsUnicode=false`

  例:

  ```
  jdbc:sqlserver://<host>:1433;database=
  <database_name>;
  sendStringParametersAsUnicode=false
  ```

> **Caution**
>
> Application Securityに組み込まれているSQL Server JDBCドライババージョンは、デフォルトで、暗号化された接続と信頼されたサーバ証明書を要件とします。証明書の検証結果として接続が失敗する場合は、Truststoreを設けることを推奨します。Truststoreを設けることができない場合は、信頼の検証を無効にすることができます。証明書は信頼されているが、証明書のDNS名がデータベースサーバのホスト名と一致しないという場合は、`hostNameInCertificate`接続プロパティを使用して正しいホスト名を指定します。
>
> 詳細については、記事「接続プロパティの設定」で`hostNameInCertificate`、`trustServerCertificate`、および`trustStore* JDBC URL`プロパティを参照してください。

5. ［**MAXIMUM IDLE CONNECTIONS**］ボックスに、プールに残すことのできるアイドル接続の最大数を入力します。

   デフォルト値は50です。

6. ［**MAXIMUM ACTIVE CONNECTIONS**］ボックスに、プールに残すことのできるアクティブ接続の最大数を入力します。

   デフォルト値は100です。

7. ［**MAXIMUM WAIT TIME (MS)**］ボックスに、システムが例外をスローするまでにプールが接続を待機する最大時間(接続がない場合)をミリ秒単位で入力します。

   デフォルト値は60000です。待機を無期限に延長するには、値をゼロ(0)に設定します。

8. 設定をテストするには、［**TEST CONNECTION**］をクリックします。

   接続テストに失敗した場合は、`ssc.log`ファイル(`<fortify.home>/<app_context>/logs`ディレクトリ内)をチェックして原因を特定します。

12. ［**スクリプトをダウンロード(DOWNLOAD SCRIPT)**］をクリックして`create-tables.sql`をダウンロードし、このスクリプトを実行します。

> **Note**
>
> Application Securityの設定を自動化する場合、*<app_context>*.autoconfig ファイル内でデータベースのマイグレーションをすでに有効にしてあるとしたら、create-tables.sql スクリプトを実行する必要はありません。Application Security設定を自動化する方法については、「Application Securityの設定の自動化」を参照してください。

13. データベースを初期化した後には、［**次へ(NEXT)**］をクリックします。
14. ［**データベースのシード処理(DATABASE SEEDING)**］ページで、次の操作を行います。
    1. ［**参照(BROWSE)**］をクリックし、Fortify_Process_Seed_Bundle-2025_Q2_*<build>*.zip ファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。
    2. ［**参照(BROWSE)**］をクリックし、Fortify_Report_Seed_Bundle-2025_Q2_*<build>*.zip ファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。
    3. (オプション)［**参照(BROWSE)**］をクリックし、Fortify_PCI_SSF_Basic_Seed_Bundle-2025_Q2_*<build>*.zip ファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。
    4. (オプション)［**参照(BROWSE)**］をクリックし、Fortify_PCI_Basic_Seed_Bundle-2025_Q2_*<build>*.zip ファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。

    使用可能なシードバンドルの詳細については、「Application Securityファイルのダウンロードと解凍」を参照してください。
15. ［**次へ(NEXT)**］、［**完了(Finished)**］の順にクリックします。
16. Linuxシステムの場合のみ、fontconfigライブラリ、DejaVu Sansフォント、およびDejaVu Serifフォントがサーバにインストールされていて、ユーザがBIRTレポートを生成できるようになっていることを確認します。
17. Tomcatサーバを再起動します。

Application Securityの初期設定が完了したら、コア属性の設定と追加の設定を完了できます。手順については、「追加のApplication Security設定」を参照してください。

後で環境設定を変更する必要が生じたら、Application Securityを保守モードにしてから必要な変更を加えます。Application Securityを保守モードにする方法については、1ページの「Application Securityの保守モードへの移行を参照してください。

参照情報

アップグレード後のApplication Securityの設定

Luceneのアップグレード

1.5.1. 初めてのApplication Securityへのサインイン

Application Securityデータベースを作成して初期化し、Tomcatサーバを設定し、TomcatでApplication Securityを展開した後、Application Securityにサインインできます。

Important

サインイン後に、デフォルト以外の管理者アカウントを少なくとも1つ作成してから、デフォルトの管理者アカウントを削除します。ユーザアカウントと役割の管理方法の詳細については、「Application Securityユーザ管理について」を参照してください。

Application Securityにサインインするには、次の手順に従います。

1. Webブラウザで、Application SecurityインスタンスのWebアドレスを入力します。

   Note

   標準的な展開の場合、デフォルトのApplication Security URLは `https://<hostname>:<port>/ssc` です。Kubernetesクラスタへの展開の場合、デフォルトのURLは `<hostname>:<port>` です(末尾に `ssc` を付けない)。

2. ユーザ名とパスワードを入力します。

   ［**ユーザ名(Username)**］と［**パスワード(Password)**］の両方にフィールドに**admin**と入力します。これらは、新規インストールのデフォルトの資格情報です。

3. ［**サインイン(SIGN IN)**］をクリックします。

4. プロンプトが表示されたら、パスワードを変更します。

   ユーザ名や一般的なフレーズ(名前、映画または楽曲のタイトル、日付、数字または文字シーケンス)が含まれない強力なパスワードを指定してください。パスワードが強力であると評価されると、そのパスワードを保存してサインインできるようになります。

次を参照

追加のApplication Security設定

Application Securityのサインインに必要なパスワード強度の設定

1.6. 追加のApplication Security設定

事前のApplication Security設定を完了し、`ssc.war`ファイルをデプロイしたら、Application Securityの［管理］ビューで設定を完了します。

このセクションでは、次のトピックについて説明します。

1.6.1. Application Securityとのコンポーネントの統合について

次の表は、Application Securityと統合できるコンポーネントを一覧表示しています。

コンポーネント	統合手順
セキュリティトレーニングベンダ	アプリケーションセキュリティトレーニングの設定
OpenText™ Fortify Audit Assistant	Fortify Audit Assistantの設定
Java Message Service (JMS)	Java Message Service設定の設定
LDAPサーバ	LDAPサーバの設定
System for Cross-domain Identity Management (SCIM)	SCIM 2.0プロトコルの実装
OpenText ScanCentral DAST	OpenText ScanCentral DASTスキャンの実行と管理の有効化
Fortify ScanCentral SAST	Fortify ScanCentral SASTとの統合を有効化
シングルサインオン(SSO)	シングルサインオンを使用するためのApplication Securityの設定について
バグトラッキングシステム	バグトラッキングシステムの統合について
ソフトウェア構成分析	• OpenText Core SCAの結果を表示するための準備 • Sonatypeの結果を表示するための準備
OpenText Application Security Tools	

コンポーネント	統合手順
Fortify Audit Workbench	OpenText™ Fortify Audit Workbenchユーザガイド
OpenText™ Fortify Plugin for Eclipse	OpenText™ Fortify Plugin for Eclipseユーザガイド
OpenText™ Fortify Extension for Visual Studio	OpenText™ Fortify Extension for Visual Studioユーザガイド
OpenText™ Fortify Analysis Plugin for IntelliJ IDEAおよびAndroid Studio	OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studioユーザガイド
OpenText™ Fortify Jenkins Plugin	OpenText™ Fortify Jenkinsプラグインユーザガイド
OpenText™ Fortify Extensions for Visual Studio Code	OpenText™ Fortify Extensions for Visual Studio Code
OpenText™ Fortify Remediation Plugin for Eclipse	OpenText™ Fortify Remediation Plugin for Eclipseユーザガイド
OpenText™ Fortify Remediation Plugin for IntelliJ IDEAおよびAndroid Studio	OpenText™ Fortify Remediation Plugin for IntelliJ IDEAおよびAndroid Studioユーザガイド
OpenText™ Fortify Azure DevOps Extension	Fortify Azure DevOps Extensionユーザガイド

Important

Application Securityを他のコンポーネントと統合する場合は、通信するマシン間のクロックスキューを最小限に抑える必要があります。NTP(Network Time Protocol)などを使用してコンピュータのクロックタイムを同期することを推奨します。これができない場合、UTCベースで比較して5分未満のクロックスキューを維持することを提案します。そうしないと、Application Securityに対する通信要求が失敗する可能性があります。

1.6.2. 問題統計しきい値の設定

［**ダッシュボード(Dashboard)**］ビューの［**問題統計(Issue Stats)**ページには、アプリケーションバージョンの問題に関するサマリ情報が表示されます。この情報には、問題のレビューおよび修復にかかっている日数が含まれます。問題の処理の速さについて視覚的な手がかりを提供するために、［**問題統計(Issue Stats)**］ページには［**平均レビュー日数(Average Days to Review)**］と［**平均修復日数(Average Days to Remediate)**］の値の横に色付きバーが表示されます。緑色のバーは、問題が迅速に処理されている、赤いバーは問題処理が遅すぎる、オレンジ色のバーは問題処理がこれら2つの間のどこかにあることを示しています。

レビューする平均日数と修復する平均日数の計算方法

［**Average Days to Review**］と［**Average Days to Remediate**］を計算する前に、Application Securityは次のルールを適用します。

- Application Securityは、次の問題を計算から除外します。
  - 365日前以前に監査または削除された問題
  - すべての抑止された問題
  - 監査または削除されていない問題
- 監査された問題の経年変化を計算するため、Application Securityは問題が最初に監査された日時を使用します。
- 監査されていないが削除された問題については、 Application Securityは削除日を監査日として使用します。
- 問題の日付を計算するため、Application Securityは次の手順を実行して日付と時刻をクリーンアップします。
  - 検出された問題の日時を、問題が見つかった日付の12:00 AMに調整します。
  - 問題が監査された日と削除された日を翌日の12:00 amに調整します。

  これらの調整は、平均日数を正しく計算するために必要です。たとえば、これらの調整がない場合、同じ日付に検出および監査された問題の平均値はゼロになりますが、これは正しくありません。3月2日に検出され、3月5日に監査された問題の場合、レビュー日数は5 - 2 + 1、つまり4日間となります。

これらすべてのルールが適用されて、時間と日付の調整が行われた後、Application Securityは(auditTime - foundDate)と(removedDate - foundDate)の2つの平均値を計算し、監査して問題を修復するまでの平均日数を取得します。

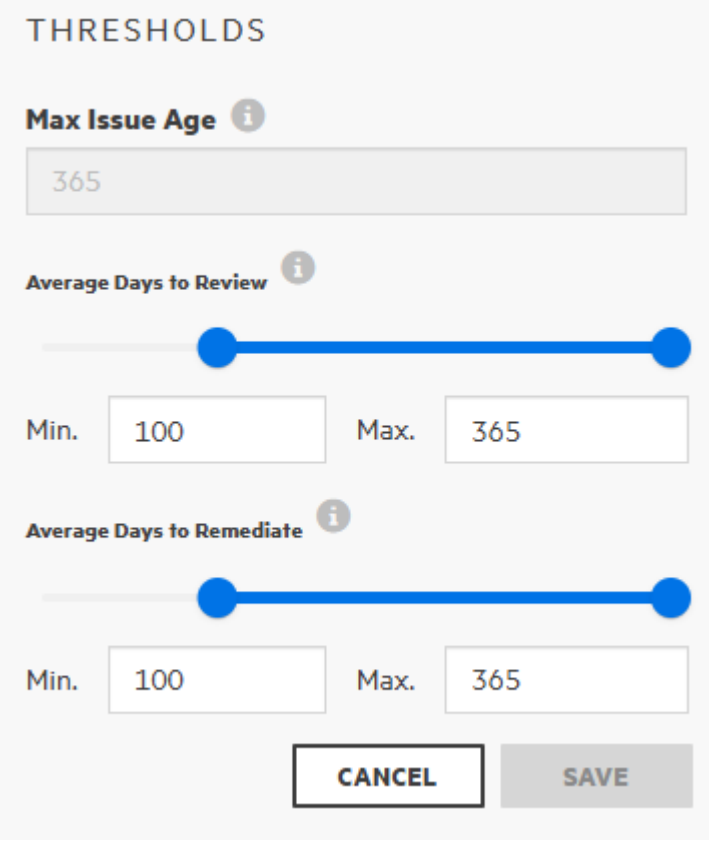
問題統計しきい値の設定

アクセス権を持つアプリケーションバージョンに関する概要情報を確認する際にユーザに表示される情報を決定するしきい値を設定します。デフォルトの［**問題統計(Issue Stats)**］ページでは、100日(最小値)未満の値は緑、365日(最大値)を超える値は赤、およびその間の値は黄色で表示されます。

Average Days to Reviewと**Average Days to Remediate**の色のしきい値を設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**問題の古さ(Issue Age)**］を選択します。

   ［**問題の古さ(Issue Age)**］ページが開きます。［**平均レビュー日数(Average Days to Review)**］と［**平均修復日数(Average Days to Remediate)**］の最小値と最大値は、デフォルトでそれぞれ100と365に設定されています。



3. 問題を確認する平均日数のしきい値をリセットするには、［**Average Days to Review**］の下で、次のいずれかを実行します。
   - スライダコントロールを調整します。
   - ［**最小(Min)**］ボックスと［**最大(Max)**］ボックスに示されている値を変更します。

4. 問題を修復する平均日数のしきい値をリセットするには、［**Average Days to Remediate**］の下で、次のいずれかを実行します。
    - スライダコントロールを調整します。
    - ［**最小(Min)**］ボックスと［**最大(Max)**］ボックスに示されている値を変更します。
5. ［**保存(SAVE)**］をクリックします。

1.6.3. アプリケーションセキュリティトレーニングの設定

組織がアプリケーションセキュリティトレーニングプラットフォームにアクセスできる場合は、そのトレーニングをApplication Securityに統合できます。その後、ユーザは監査時に、評価する問題とその最適な緩和策について、コンテキストに適したガイダンスにアクセスできます。

でApplication Securityアプリケーションセキュリティトレーニングを有効にするには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**アプリケーションセキュリティトレーニング(AppSec Training)**］を選択します。
3. ［**アプリケーションセキュリティトレーニング(AppSec Training)**］ページで、［**トレーニングを有効にする(Enable Training)**］チェックボックスをオンのままにします。
4. オンライントレーニングベンダがApplication Securityを統合しているかどうかを確認して、対応するトレーニングURLを取得するには、カスタマサポートにお問い合わせください。
5. ［**トレーニングURL(Training URL)**］ボックスに、アプリケーションセキュリティトレーニングURLを入力します。
6. ［**保存(SAVE)**］をクリックします。

［**監査(AUDIT)**］ページの問題の詳細セクションに、［**トレーニングを受ける(GET TRAINING)**］ボタンが表示されるようになります。ユーザは［**トレーニングを受ける(GET TRAINING)**］をクリックすることで、設定済みのアプリケーションセキュリティトレーニングWebサイトに移動できます。

次も参照

分析結果の監査

1.6.4. AI Assistantの設定

AI Assistantは、Application Security内で、サポートされているAIアシスタントを管理者が構成する単一の場所を提供します。このページには以下のタブが含まれています。

- Audit Assistant: Audit Assistant構成が含まれています。
- Aviator: Aviator構成が含まれています(環境で利用可能な場合)。

AI Assistantへのアクセス

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**AI Assistant**］を選択します。

AI Assistantタブの選択

一度に有効にできるのは、Audit AssistantとAviatorのいずれか一方のみです。別のAIアシスタントがすでに有効になっている状態で新たにAIアシスタントを有効にしようとすると、Application Securityには変更を行う前に警告メッセージが表示されます。

- アシスタントを切り替えるには［**Yes(はい)**］を選択します。Application Securityによって、現在有効なアシスタントが無効化され、選択したアシスタントが有効化されます。
- キャンセルするには［**No(いいえ)**］を選択します(または**Esc**を押す)。Application Securityによって変更は加えられず、以前の選択が復元されます。

参照情報

Fortify Audit Assistantの設定

Fortify Audit Assistantのベストプラクティス

Fortify Audit Assistantの使用

Aviatorの設定

1.6.4.1. Fortify Audit Assistantについて

Fortify Audit Assistantは、スキャンから返された問題が真の脆弱性であるか否かの判断を支援するオプションのツールです。Application SecurityはOpenText SAST分析結果で返された問題が真の脆弱性であるかどうかを判断するために、Fortify Audit Assistantと連携します。

その判断を下すには、Fortify Audit Assistantに予測のベースラインを確立するためのデータが必要です。このデータは、OpenText Core Application Security (Fortify on Demand)監査官がスキャン監査の際に、さまざまな問題をどのように特徴付けるかについて行った決定に基づいています。このデータは、プールされて匿名化され、監査官が行った決定に基づいてトレーニングデータと組み合わせて使用できます。Fortify Audit Assistantがより多くのトレーニングデータを受け取ることで、Fortify Audit Assistantは問題が表す実際の脅威をより正確に評価できるようになります。

参照情報

Fortify Audit Assistantの設定

Fortify Audit Assistantのベストプラクティス

Fortify Audit Assistantの使用

1.6.4.1.1. Fortify Audit Assistantの設定

Application SecurityはFortify Audit Assistantと共に機能し、Fortify Static Code Analyzerのスキャン結果で返された問題が真の脆弱性であるかどうかを判断するのに役立ちます。

Important

Fortify Audit Assistantで、1つ以上の第2世代(G2)予測ポリシーを作成します。G2予測モデルで機能する予測ポリシーを作成する必要があります。Fortify Audit Assistantで予測ポリシーを定義する方法の詳細については、「Fortify Audit Assistant Documentation」でFortify Audit Assistantヘルプを参照してください。

一度に有効にできるAIアシスタントは1つだけです。Aviatorが有効になっている状態でAudit Assistantを有効にしようとすると、Application Securityには変更を実行する前に警告メッセージが表示されます。詳細については、「AI Assistantの設定」を参照してください。

アプリケーションでFortify Audit Assistantを使用するようにApplication Securityを設定するには:

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**AI Assistant**］を選択します。
4. ［**Audit Assistant**］タブを選択します。
5. 次の表で説明するように、［**Audit Assistant**］ページで設定を行います。

フィールド	説明
［Audit Assistantを有効にする(Enable Audit Assistant)］チェックボックス	Fortify Audit Assistantを有効にするには、このチェックボックスをオンにします。
認証トークン(Authentication token)	(必須) Fortify Audit Assistantから取得した認証トークンをここに貼り付けます。トークンの取得方法を確認するには、［**トークンの取得方法(How do I get a token?)**］を選択します。
Fortify Audit AssistantサーバURL (Fortify Audit Assistant server URL)	(必須) Fortify Audit Assistantサーバの URLを指定します。
Audit Assistantにプロキシを使用(Use SSC proxy for Audit Assistant)	(オプション)すべてのApplication Security統合で使用するプロキシを設定済みの場合(「Application Security統合のプロキシの設定」を参照)、そのプロキシをFortify Audit Assistantで使用するには、このチェックボックスをオンにします。

6. 接続が正常にテストされたら、先に進んで、［**監査設定(Audit settings)**］セクションで次の設定をします。

   接続が正常にテストされたら、先に進んで、［**監査設定(Audit settings)**］セクションで次の設定をします。

7. ［**ポリシーの更新(REFRESH POLICIES)**］をクリックして、［**デフォルトの予測ポリシー(Default prediction policy)**］リストに、Fortify Audit Assistantサーバ上の現在のサーバポリシーを入力します。

Note

個々のアプリケーションバージョンに設定されたFortify Audit Assistant予測ポリシーは、使用可能なポリシーがFortify Audit Assistantサーバで変更されると、無効になる可能性があります。ユーザが［**ポリシーの更新(REFRESH POLICIES)**］をクリックするたびに、Application SecurityはFortify Audit Assistantから渡された新しいポリシーを検証します。Application Securityが1つ以上の無効なポリシーを検出した場合、元のポリシーから変更後のポリシーへのマッピングを示すテーブルが表示されます。その後、古い各ポリシーを識別し、その有効な置換をマップできます。Application Securityは、マッピングテーブルで送信した変更に基づいてポリシーを更新します。

8. ［**Default prediction policy**］リストから、すべてのアプリケーションバージョンに適用する予測ポリシーの名前を選択します。(ポリシーはFortify Audit Assistantで定義されます)。

9. 予測ポリシーをアプリケーションバージョンレベルで指定し、デフォルトのグローバル予測ポリシーを上書きする場合は、［**特定のアプリケーションバージョンのポリシーを有効にする(Enable specific application version policies)**］を選択します。

   それ以外の場合、Fortify Audit Assistantは前のステップで指定したデフォルトのグローバル予測ポリシーを使用します。アプリケーションバージョンのポリシーを指定するには、「アプリケーションバージョンに対してFortify Audit Assistantオプションを設定する」を参照してください。

10. 未監査の問題が評価対象としてApplication SecurityからFortify Audit Assistantに自動的に送信されるようにするには、［**自動予測を有効にする(Enable auto-prediction)**］チェックボックスをオンにします。

    その後、アプリケーションごとにこの機能を有効にする必要があります(「アプリケーションバージョンに対してFortify Audit Assistantオプションを設定する」を参照)。自動予測機能の詳細については、「Audit Assistantの自動予測について」を参照してください。

11. Fortify Audit Assistantが問題の有無を評価する分析値がシステム全体で［**分析(Analysis)**］カスタムタグ値に適用されるようにするには、［**自動適用を有効にする(Enable auto-apply)**］チェックボックスをオンにします。

    その後、アプリケーションごとにこの機能を有効にする必要があります(「アプリケーションバージョンに対してFortify Audit Assistantオプションを設定する」を参照)。

Important

自動適用機能を使用するには、その前に、Fortify Audit Assistant分析タグの値をApplication Security分析タグの値にマップする必要があります(「Application Securityカスタムタグ値へのFortify Audit Assistant分析タグ値のマッピング」を参照)。

12. ［**保存(SAVE)**］をクリックします。

参照情報

Application SecurityでのFortify Audit Assistantの使用

Fortify Audit Assistantワークフロー

Application Securityカスタムタグ値へのFortify Audit Assistant分析タグ値のマッピング

1.6.4.1.2. Fortify Audit Assistantの自動予測について

自動予測を［はい(yes)］に設定すると、FPRが正常にアップロードおよび処理された後に、Fortify Audit Assistantの予測に関する問題を自動送信するようにApplication Securityを設定できます。(予測用にFPRを手動で送信する場合は、自動予測を設定する必要はありません)。

アプリケーションバージョンに対して自動予測と自動適用の両方が有効になっている場合、予測が完了した後、Fortify Audit Assistantは新しい問題のカスタムタグに予測値を自動的に適用します。(監査アシスタントの予測結果は常にアプリケーションバージョンに適用されますが、自動適用が有効になっていない場合、情報は監査アシスタント固有のタグにのみ保存されます。自動適用が有効な場合、監査アシスタント固有の値も設定に基づいて他のタグにマップされます)。

FPR処理の最後に見つかった予測されていない(サポートされているアナライザによって明らかになった)問題だけが、評価のためにFortify Audit Assistantに自動的に送信されます。Fortify Audit Assistantが、一度評価した問題を再度検討することはありません。

アプリケーションバージョンの自動予測有効化は、2ステップのプロセスです。まず、管理者がFortify Audit Assistant設定で、Fortify Audit Assistantをシステム全体で有効にします(「Fortify Audit Assistantの設定」を参照)。その後、ユーザがアプリケーションバージョンごとに自動予測を有効にする必要があります(「アプリケーションバージョンの自動適用と自動予測を有効にする」を参照)。

1.6.4.2. Aviatorの設定

Aviatorは、Application Securityから有効化および管理可能なAIアシスタントです。Aviatorを有効にすると、OpenText™ Application Security Aviator for Vulnerability Remediationが生成したタグやコメントをApplication Security UIで確認し、以下のAPIを通じて修復を実施できます。

- `/projectVersions/{parentId}/remediations`
- `/projectVersions/{parentId}/remediations/{id}`

OpenText™ Application Security Aviator for Vulnerability Remediationに関する情報は、*OpenText™ Application Security Aviator for Vulnerability Remediationユーザガイド*をご覧ください。

> **Note**
> 問題に修復が含まれている場合は、`hasAviatorRemediation`キーを使用してIssues API経由で検証します。

Aviator設定へのアクセス

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**AI Assistant**］を選択します。
4. ［**Aviator**］タブを選択します。

Aviatorの有効化または無効化

1. ［**Aviator**］タブで［**Enable Aviator(Aviatorを有効化)**］チェックボックスをオンにして Aviatorを有効にします。
2. ［**保存(SAVE)**］をクリックします。

一度に有効にできるAIアシスタントは1つだけです。Audit Assistantが有効になっている状態でAviatorを有効にしようとすると、Application Securityには変更を実行する前に警告メッセージが表示されます。詳細については、「AI Assistantの設定」を参照してください。

次も参照

Aviatorの自動修復結果の操作

1.6.5. BIRTレポート用のセキュリティの設定

OpenTextでは、BIRTレポーティングを目的とした別個の読み取り専用データベースアカウントを作成することを推奨しています。

データベース内のテーブルおよびビューへの書き込みアクセスを制限するには、次の手順に従います。

1. BIRTレポート専用に使用するデータベースユーザアカウントを作成し、レポート生成に必要な最小限の許可を提供します。
2. 新しいユーザアカウントの場合、次の表に記載するデータベーステーブルおよびビューへの読み込み専用アクセスを有効にしてください。

テーブル		
attr	issuecache	reportexecblob
auditattachment	measurement	reportexecparam
auditcomment	measurementhistory	ruledescription
catpackexternalcategory	metadef	savedreport
catpackexternallist	metadef_t	scan
catpacklookup	metaoption	scan_rulepack
datablob	metaoption_t	seedhistory
documentinfo	metavalue	sourcefile
eventlogentry	metavalueselection	snapshot
f360global	project	userpreference
filterset	projecttemplate	variable
folder	projectversion	variablehistory
foldercountcache	projectversiondependency	
ビュー		
attrlookupview	defaultissueview	ruleview
auditvalueview	metadefview	view_standards
baseissueview	metaoptionview	

3. 管理者としてApplication Securityにサインインします。
4. ヘッダで、［**管理(Administration)**］を選択します。

5. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**BIRTレポート(BIRT Reports)**］をクリックします。
6. ［**DB Username**］と［**DB Password**］ボックスに、読み込み専用のデータベースアクセス権を持つデータベースアカウントの資格情報を入力します。
7. データベースユーザアカウントからデータベースにアクセスできるかどうかをテストするには、［**接続の検証(VALIDATE CONNECTION)**］をクリックします。
8. ［**保存(SAVE)**］をクリックします。

参照情報

レポート生成用のメモリの割り当て

レポート生成タイムアウトの設定

1.6.5.1. レポート生成用のメモリの割り当て

Application Securityレポートのセキュリティのためにメモリを割り当てるには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**BIRTレポート(BIRT Reports)**］をクリックします。
3. ［**BIRT実行の設定(Set up BIRT execution)**］で、［**最大ヒープサイズ(MB) (Maximum heap size (MB))**］ボックスに示されている値を選択し、新しい値を入力します。
4. ［**保存(SAVE)**］をクリックします。

1.6.5.2. レポート生成タイムアウトの設定

レポート生成タイムアウト値(その後、レポートの生成が停止され、「failed」に設定されます)を設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**BIRTレポート(BIRT Reports)**］をクリックします。
3. ［**BIRT実行の設定(Set up BIRT execution)**］で、［**実行タイムアウト(分数)(Execution timeout (minutes))**］ボックスに示されている値を選択し、新しい値を入力します。
4. ［**保存(SAVE)**］をクリックします。

1.6.6. コア設定の設定

セットアップウィザードで初期設定を行った後、いくつかのコア属性を設定する必要があります。これらの属性には、ユーザアカウントのタイムアウトとロックアウトの設定、ユーザ情報の表示、OpenText™ DAST Agentの問題ごとの最大イベント数、ランタイムイベント記述サーバのベースURL、およびユーザ管理者の電子メールアドレスが含まれます。このページでは、Rulepackの更新に使用するプロキシも設定します。Rulepack更新プロキシの詳細については、「Rulepack更新用のプロキシの設定について」を参照してください。

Application Securityのコア設定を構成するには:

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**コア(Core)**］を選択します。
4. ［**コア(Core)**］ページで、次の表で説明されている設定を構成します。

フィールド	説明
Absolute session timeout (minutes)	ユーザをアクティブな状態に維持できる期間(分数)。この期間が経過すると、ユーザは自動的にログアウトされます。 デフォルト値は `240` です。
Days before password reset	Application Securityパスワードが有効な期間(日数)。この期間が経過すると、ユーザはパスワードを変更するよう求められます。 デフォルト値は `30` です。

フィールド	説明
ユーザをロックアウトするまでのログイン試行回数(Login attempts allowed before a user is locked out)	ローカルユーザに許可される、無効な資格情報を使用したApplication Securityへのサインイン試行の回数。この回数に達すると、ユーザのアカウントがロックされます。 Application Securityによってロックアウトされたユーザは、［**ロックアウト時間(分)(Lockout time (minutes))**］ボックスに分単位で指定された期間、新しくログインを試みることができません。ユーザアカウントのロック解除方法については、「ローカルユーザアカウントのロック解除」を参照してください。デフォルト値は `3` です。 **Note** この設定はLDAPユーザには適用されません。グループポリシーエディタを使用してアカウントのロックアウトのしきい値が設定されていたなら、ログイン試行が連続して失敗した場合に、LDAPユーザアカウントはActive Directoryでロックアウトされることになります。

フィールド	説明
ロックアウト時間(分)(Lockout time (minutes))	ユーザのApplication Securityへのサインイン試行が［**ログアウトされるまでのログイン試行回数(Login Attempts before Lockout)**］で指定された回数失敗すると、Application Securityは［**ロックアウト時間(分数)(Lockout time (minutes))**］ボックスで指定された期間にわたってユーザアカウントをロックします。 デフォルト値は `30` です。

フィールド	説明
User lookup strategy	LDAPが有効な場合は、このリストから次のユーザルックアップ戦略のいずれかを選択します。 ◦ **Local users first, fallback to LDAP users (compatibility)** 最初にローカルユーザを検索し、次にLDAPユーザを検索します。認証エラーやユーザの混乱を避けるため、LDAPサーバとローカルストレージでユーザ名が重複しないようにしてください。 ◦ **LDAP users first, fallback to local users** 最初にLDAPユーザを検索し、次にローカルユーザを検索します。認証エラーやユーザの混乱を避けるため、LDAPサーバとローカルストレージでユーザ名が重複しないようにしてください。 ◦ **LDAP users exclusive, fallback to local administrator** (SSOの推奨戦略)LDAPユーザのみを検索し、ローカル管理者アクセスを許可します。
Display user first/last names and emails in user fields, along with login names	このチェックボックスをオンにすると、必要に応じ、ログイン名、姓と名、および電子メールアドレスのユーザ情報が表示されます。

フィールド	説明
Maximum events per WebInspect Agent Issue	ログに記録できる、OpenText DAST Agent問題1件あたりの最大イベント数。このしきい値に達すると、同じ問題に関連する新しいイベントは無視されます。 デフォルト値は `5` です。
非アクティブセッションのタイムアウト(分)(Inactive session timeout (minutes))	ユーザの非アクティブ状態が許容される期間(分数)。この期間が経過すると、ユーザはApplication Securityから自動的にログオフされます。 デフォルト値は `30` です。
Locale for Rulepacks	次のいずれかを入力します。 ◦ ja(日本語) ◦ zh_CN(簡体字中国語) ◦ zh_TW(繁体字中国語) ◦ es(スペイン語) ◦ pt_BR(ポルトガル語(ブラジル) **Note** 英語は値を指定する必要はありません。

フィールド	説明
Rulepack update URL	Rulepack更新サイトのURL。デフォルト値は `https://update.fortify.com` です。 **Important** ［**Rulepack更新URL(Rulepack Update URL)**］フィールドのデフォルト値は、カスタマサポート担当者から指示されない限り変更しないでください。
Use SSC proxy for Rulepack update	Rulepack更新サーバがApplication Securityプロキシの背後にある場合、そのプロキシを使用するには、このチェックボックスをオンにします。 **Note** Application Securityのプロキシを有効にして正しく設定する必要があります。詳細については、「Application Security統合のプロキシの設定」を参照してください。

フィールド	説明
ユーザ管理者の電子メールアドレス(ユーザアカウントの要求用) (User administrator's email address (for user account requests))	電子メール通知が有効にされている場合、システムによる電子メールアラートおよび通知を受信するユーザの電子メールアドレス。 サインインダイアログボックスで［**アカウントにアクセスできない場合、またはアカウントが必要な場合(Can't access or need an account?)**］リンクが使用可能な場合は、この電子メールアドレスに新しいユーザアカウントの要求が送信されます。
Enable export to CSV from the Dashboard and AUDIT views	デフォルトで、ユーザは［**ダッシュボード(Dashboard)**］ビューおよび［**監査(AUDIT)**］ページに表示されているApplication Securityデータをカンマ区切り値(CSV)ファイルにエクスポートできます。このチェックボックスをオフにすることで、この機能をブロックできます。 **Note** ［**コア(Core)**］ページでこの設定のみを変更する場合、その変更はサーバを再起動しなくても実装されます。

5. ［**保存(SAVE)**］をクリックします。
6. サーバを再起動します。

参照情報

ローカルユーザアカウントのロック解除

1.6.6.1. Rulepack更新用プロキシの設定について

デフォルトでは、Application SecurityはRulepack更新サーバから、ユーザが登録しているOpenText Secure Coding Rulepacksの最新バージョンをダウンロードします。

組織が外部リソースにアクセスするためにプロキシを使用している場合、OpenTextでは、Rulepack更新用(ならびにバグトラッキング用と、使用している場合はFortify Audit Assistant用)のプロキシを設定することを推奨しています。HTTP(S)プロトコルベースのすべてのApplication Security統合で使用するために単一のプロキシを設定する方法については、「Application Security統合のプロキシの設定」を参照してください。

HTTP(S)プロトコルベースのすべての統合で使用するために単一のプロキシを設定した後、そのプロキシをRulepack更新に対して有効にできます。

参照情報

コア設定の設定

1.6.7. CSVファイルへのデータエクスポートのブロック

デフォルトで、ユーザは［**ダッシュボード(Dashboard)**］ビューおよび［**監査(AUDIT)**］ページに表示されているApplication Securityデータをカンマ区切り値(CSV)ファイルにエクスポートできます。この機能はブロックできます。

ユーザがApplication SecurityデータをCSVファイルにエクスポートできないようにするには、次の手順に実行します。

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**コア(Core)**］を選択します。
4. ［**ダッシュボードおよび監査ビューからのCSVへのエクスポートを有効にする (Enable Export to CSV from the Dashboard and AUDIT views)**］チェックボックスをオフにします。
5. ［**保存(SAVE)**］をクリックします。

参照情報

コア設定の設定

ダッシュボードサマリテーブルをエクスポートする

データをカンマ区切り値ファイルへエクスポートする

1.6.8. ［バージョン情報(About)］ボックスのサポート連絡先リンクを変更する

デフォルトでは、［バージョン情報(About)］ボックスに、カスタマサポートポータルへのリンクが表示されます。そのリンクを自分の組織のサポートポータルへのリンクに置き換えることができます。

［バージョン情報(About)］ボックスに独自のサポートポータルを表示するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**カスタマイズ(Customization)**］を選択します。
4. ［**バージョン番号ボックスで組織のサポートURLの使用を有効にする(Enable using the support URL for your organization in the About box)**］チェックボックスをオンにします。
5. ［**組織のサポートURL (Support URL for your organization)**］ボックスに、組織のサポートポータルのWebアドレスを入力します。
6. ［**サポートURLに表示するテキスト(Text displayed for your support URL)**］ボックスに、組織のサポートポータルへのリンクに表示するテキストを入力します。
7. ［**保存(SAVE)**］をクリックします。

参照情報

バナーの組織向けカスタマイズ

ダッシュボードへのFortify Insightリンクの追加

1.6.9. ダッシュボードへのFortify Insightリンクの追加

Fortify Insightを購入した場合、ダッシュボードにFortify Insightのリンクを追加できます。

［**ダッシュボード(Dashboard)**］ビューにFortify Insightのリンクを追加するには:

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**カスタマイズ(Customization)**］を選択します。
4. ［**Fortify Insight URL**］の下で、［**ダッシュボードでFortify Insight URLの表示を有効にする(Enable display of the Fortify Insight URL on your Dashboard)**］チェックボックスをオンにします。
5. ［**Fortify Insight URL**］ボックスに、Fortify InsightページのURLを入力します。
6. ［**保存(SAVE)**］をクリックします。

参照情報

バナーの組織向けカスタマイズ

［バージョン情報(About)］ボックスのサポート連絡先リンクを変更する

システム全体のバナーを作成する

1.6.10. バナーの組織向けカスタマイズ

バナーをカスタマイズして、ユーザがサインインする際や、ビュー(［**ダッシュボード(Dashboard)**］、［**アプリケーション(Applications)**］、［**レポート**］など)を切り替える際に、組織のApplication Security Webサイトに関する情報を表示できます。

> **Caution**
>
> Application Securityインスタンスをアップグレードするたびに、バナーを再作成する必要があります。

ユーザのカスタムサインインエクスペリエンスを作成するには:

1. `<ssc_deploy_dir>/WEB-INF/lib/` ディレクトリに移動します。
2. `ssc-htmlui-<version>.jar` ファイルのコンテンツを新しいディレクトリ(残りの手順では `<new_directory>` とします)に抽出します。
3. `<new_directory>/META-INF/resources/html/login/` ディレクトリに移動します。
4. テキストエディタで `login.html` ファイルを開きます。
5. テキスト `<!--<center><font color="red">Add your custom banner here</font></center>-->` をコメント解除し、表示されるメッセージの外観、使用感、およびコンテンツを設定するHTML要素を指定します。

   スペースの制限により、メッセージテキストは1行に制限されます。複数行にすると、ユーザインタフェースに干渉します。次の例では、ログインした時点でApplication Security Webページの上部中央に表示される、赤いテキストのバナーを追加します。

   ```
   <center><font color=red size=10>Message_text</font></center>
   ```

6. `ssc-htmlui-<version>.jar` ファイルの名前を `ssc-htmlui-<version>.jar.orig` に変更します。
7. `ssc-htmlui-<version>.jar` 以下にあるすべてのファイルを含む新しいアーカイブを `<new_directory>` という名前で作成します。

   > **Important**
   >
   > 新しいアーカイブに `<new_directory>` をそのまま含めないでください。

8. Application Securityサーバを再起動します。

ユーザがビューを切り替えるたびに表示されるメッセージバナーを作成するには:

1. `<ssc_deploy_dir>/WEB-INF/lib/` ディレクトリに移動します。
2. `ssc-htmlui-<version>.jar` ファイルのコンテンツを新しいディレクトリ(残りの手順では `<new_directory>` とします)に抽出します。
3. `<new_directory>/META-INF/resources/html/ssc/` ディレクトリに移動します。
4. テキストエディタで `index.html` ファイルを開き、41行目に移動します。
5. テキスト `<div style="text-align: center;"><span style="color: red; ">Add your custom banner here</span></div>` をコメント解除し、表示されるメッセージの外観、使用感、およびコンテンツを設定するHTML要素を指定します。

   次の例では、Application Security Webページの上部中央に表示される、赤いテキストのバナーを追加します。

   ```
   <div style="text-align: center;"><span style="color: red; ">
   Message text x</span></div>
   ```

   Note

   スペースの制限により、メッセージテキストは1行に制限されます。複数行にすると、ユーザインタフェースに干渉します。

6. `ssc-htmlui-<version>.jar` ファイルの名前を `ssc-htmlui-<version>.jar.orig` に変更します。
7. `ssc-htmlui-<version>.jar` 以下のすべてのファイルとディレクトリを含む `<new_directory>` という名前の新しいアーカイブを作成します。

   Important

   新しいアーカイブに `<new_directory>` をそのまま含めないでください。

8. Application Securityサーバを再起動します。

参照情報

ダッシュボードへのFortify Insightリンクの追加

システム全体のバナーを作成する

1.6.11. システム全体のバナーを作成する

管理者は、アプリケーション内のすべてのページでヘッダの下に表示されるシステム全体のバナーを作成できます。バナーの長さは最大1,024文字です。バナーのコンテンツが2行を超える場合は、メッセージの残りの部分を表示する［**さらに表示(Show More)**］リンクが配置されます。

システム全体のバナーを作成するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**カスタマイズ(Customization)**］を選択します。
4. ［**カスタムバナー(Customized Banner)**］で、［**システム全体にカスタムバナーを表示(Display a custom banner system-wide)**］チェックボックスをオンにします。
5. ［**バナーに表示するテキストを入力(Enter the text to display in the banner)**］ボックスに、バナーに表示するテキストを入力します。
6. ［**保存(SAVE)**］をクリックします。

Note
バナーに表示されたハイパーリンクをクリックすると、次のメッセージが表示されます。
「Software Security Centerから移動しようとしています。続行しますか? (You is about the leave On the You about the Leave On You you leave Software Security Center.Do you want to continue?)」

確認すると、ハイパーリンクが新しいブラウザタブで開きます。

バナーの組織向けカスタマイズ

ダッシュボードへのFortify Insightリンクの追加

1.6.12. 電子メールアラート通知設定の設定

チームに電子メールアラート通知を送信するためにApplication Securityを使用するには:

1. Application Securityが使用するSMTP電子メールアカウントを作成します。
2. このトピックの説明に従って電子メール設定を設定します。

Note

電子メールアラートの受信を設定する方法については、「電子メールアラートの受信を有効化および無効化する」を参照してください。

電子メールアラート通知の送信に使用する設定を設定するには、次の手順に従います。

Important

アカウントを持っていないチームメンバーがApplication Securityへのアクセスを要求できるようにするには、電子メールサービス設定を有効にして設定する必要があります。

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**電子メール**］を選択します。
4. ［**電子メール**］ページで、次の表で説明されている電子メールサービス属性を設定します。

フィールド	説明
Enable email	このチェックボックスをオンにすると、Application Securityはすべてのタイプの電子メールメッセージを送信できるようになります。また、サインインダイアログボックスには、［アカウントにアクセスできない場合、またはアカウントが必要な場合(Can't access or need an account?)］リンクが追加されます。 このチェックボックスは、デフォルトではクリアされています。
From email address	Application Securityから送信される電子メールを識別するためにApplication Securityで使用する電子メールアドレスを入力します。たとえば、`fortifyserver@example.com`になります。
Default encoding of the email content	電子メールコンテンツに使用するエンコーディング方法を入力します。 デフォルト値はUTF-8です。
SMTP server	SMTPサーバの完全修飾ドメイン名を入力します。たとえば、`mail.example.com`になります。
SMTP server port	SMTPサーバのポート番号を入力します。 デフォルト値は25です。

フィールド	説明
SMTP username	SMTPサーバで認証が必要な場合は、SMTPユーザ名を入力します。
SMTP password	SMTPサーバで認証が必要な場合は、SMTPパスワードを入力します。
Secure email server connection	電子メールサーバ接続のセキュリティを設定する場合は、このチェックボックスをオンにします。
Enable SSL/TLS encryption	［**Secure email server connection**］チェックボックスをオンにした場合、このリストから次のいずれかを選択します。 ◦ (オプション)SMTPサーバがサポートしている場合は、［**STARTTLS**］を選択してTLS/SSLで暗号化されたSMTP接続にアップグレードします。 ◦ SMTPサーバに接続するときにSSL/TLS暗号化を有効にするには、［**SSL/TLS Encryption**］を選択します。 ◦ TLS/SSLで暗号化されたSMTP接続へのアップグレードが必要な場合は［**Force STARTTLS**］を選択します。SMTPサーバがサポートしていない場合、接続は失敗します。

フィールド	説明
Trust the certificate provided by the SMTP server	このチェックボックスを選択すると、証明書の検証をスキップしてSMTPサーバが提供する証明書を信頼します。 **Caution** セキュリティ上の理由から、OpenTextではこのチェックボックスをオフのままにすることを推奨しています。

5. ［**保存(SAVE)**］をクリックします。

1.6.12.1. 電子メールアラートを受信するかどうかを設定する

電子メールアラートを受信するかどうかを設定するには:

1. 管理者としてサインインします。
2. ヘッダの［**プロファイルメニュー(Profile menu)**］から［**初期設定(Preferences)**］を選択します。
3. ［**初期設定(PREFERENCES)**］ダイアログボックスで、次のいずれかの操作を行います。
    - 電子メールアラートを受信しないようにするには、［**Software Security Centerから電子メールアラートを受信する(Receive email alerts from Software Security Center)**］チェックボックスをオフにします。
    - 電子メールアラートの受信を有効にするには、［**Software Security Centerから電子メールアラートを受信する(Receive email alerts from Software Security Center)**］チェックボックスをオンにします。
4. ［**保存(SAVE)**］をクリックします。

参照情報

電子メールアラート通知設定の設定

アラートの作成

アラートの削除

1.6.13. 問題監査の競合を解決するための戦略を設定する

複数の監査者がそれぞれに異なる製品(Application Security、Audit Workbench、またはいずれかのSecure Code Plugins)を使用して同じ問題に取り組んでいる場合、特定のカスタムタグに異なる値を割り当てる可能性があります。以前は、Application Securityがこのような監査の競合を検出した場合、クライアント側の変更をすべて無視し、Application Security の既存のカスタムタグ値を優先して競合を解決していました。

Note

競合の解決が必要ないのは、これらの監査者が同じ Application Security インスタンス内で作業する場合です。

監査の競合を解決するためのデフォルトの戦略の例

Fortify Audit WorkbenchのユーザAとBは、どちらも同じアプリケーションバージョンの最新の分析結果を監査しています。

ユーザAが、明らかになった問題のカスタムタグ値を設定して、結果をApplication Securityにアップロードします。

Application Securityはアップロードを受け入れ、ユーザAが設定した値に基づいて、問題のカスタムタグ値を変更します。これで、ユーザAが設定したタグ値は、Application Securityでこれらの問題に対する現在のカスタムタグ値になります。

ユーザBが別のFortify Audit Workbenchインスタンスで、ユーザAによって監査された同じ問題に対してカスタムタグ値を設定し、結果をApplication Securityにアップロードします。Application Security は、Bが送信した1つ以上のカスタムタグ値が、同じ問題でユーザAが送信した値と競合していることを検出します。

結果: Application Securityは、ユーザBからの監査結果を無視し、ユーザAによって設定された値を保持します。

Application Security は、この戦略をすべてのアプリケーションバージョンに適用します。

この戦略を変更して、Application Security が最新の変更を優先して監査の競合を解決するようにできます。

Note

このタスクを実行するには、「問題の監査設定を管理する」許可を持っている必要があります。

Application Security が監査の競合を解決するために使用する戦略を設定するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**問題の監査(Issue Audit)**］を選択します。
4. ［**Issue audit conflict resolving strategy**］リストから、次のいずれかを選択します。
   - **SSCの変更に基づいて競合を解決する(Conflicts are resolved in favor of the SSC changes)** (デフォルト)
   - **最新の変更に基づいて競合を解決する(Conflicts are resolved in favor of the most recent changes)**
5. ［**保存(SAVE)**］をクリックします。
6. 変更を実装するには、Application Securityサーバを再起動します。

設定を変更すると、新しい戦略は新しいアップロードだけに適用されます。以前の競合の解決結果はすべて変更されません。

参照情報

現在の問題の状態について

1.6.14. Java Message Serviceの設定

システムイベントをJava Message Service (JMS)に発行する場合は、［管理］ビューでJMS統合属性を設定します。

JMS設定を設定するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**JMS**］を選択します。
3. ［**JMS**］ページで、次の表の説明に従って設定を行います。

フィールド	説明
Publish system events to JMS	システムイベントをJMSに発行するには、このチェックボックスをオンにします。
JMS server URL	JMSサーバのURLを入力します。たとえば、`tcp://123.0.1.2:12345`になります。
Include username in JMS body	JMSメッセージの本文にユーザ名を含めるには、このチェックボックスをオンにします。 このチェックボックスはデフォルトで選択されています。
JMS topic	JMSメッセージトピックを入力します。デフォルト値は`Fortify.Advisory.EventNotification`です。

4. ［**保存(SAVE)**］をクリックします。

5. 変更を実装するには、Tomcatサーバを再起動します。

1.6.15. Application Securityユーザ認証について

デフォルトでは、ユーザがApplication Securityにログオンする際、またはOpenText Application Securityのいずれかのツールを使用してFortifyプロジェクト結果(FPR)ファイルをアップロードする際に、Application Securityはデータベースを使用してユーザを認証し、その認証済みユーザを当該ユーザに割り当てられているユーザ役割(管理者、セキュリティリード、開発者など)にバインドします。

データベースのみ認証では、Application Securityユーザアカウントと役割を作成および管理するために別個の管理プロセスが必要になります。LDAPまたはSCIM 2.0 APIクライアントを使用して、Application Securityのデフォルトデータベース専用の認証を強化できます。LDAPユーザ認証の詳細については、「LDAPユーザ認証」を参照してください。
SCIM 2.0ユーザプロビジョニングについては、「SCIM 2.0プロトコルの実装」を参照してください。

1.6.16. LDAPユーザ認証

Active Directory/LDAPの統合により、Application Securityでは既存の企業資格情報に基づいてユーザを認証できます。また、グループ別または部門別の割り当てにより、Application Securityで既存のジョイナー/リーバープロセスを利用できます。グループに参加する新しいユーザは、自動的にApplication Securityにアクセスできます。グループを離れるユーザは、自動的にアクセスを失います。

このセクションのトピックでは、Application Securityのユーザ認証と、LDAP認証およびLDAPサーバオプションの設定について説明します。

Important

- OpenTextでは、LDAPサーバで問題が発生した場合に備え、LDAPサーバの設定前に少なくとも1つのローカル管理者アカウントを作成することを推奨しています。
- OpenTextでは複数のLDAPサーバの使用をサポートしていますが、ロードバランサの背後にある複数のLDAPサーバの使用はサポートしていません。ただし、同一のサーバを複数使用する場合はその限りではありません。

参照情報

LDAPエンティティの登録

LDAPユーザ役割の管理について

1.6.16.1. LDAP認証の設定の準備

LDAP認証を使用するようにApplication Securityを設定する前に、次のタスクを実行します。

1. LDAP管理アプリケーションをダウンロードします。

   LDAPサーバが使用するLDAPスキーマに精通していない場合は、*JXplorer*などのサードパーティのLDAP管理アプリケーションを使用して、LDAP認証ディレクトリを表示および変更できます。JXplorerから、標準のOSIスタイルのオープンソースライセンスでJXplorerを無料でダウンロードできます。

2. Application Securityで使用するLDAPアカウントを作成します。

   Note

   ユーザを参照するためにプライマリソースを設定する方法については、「コア設定の設定」を参照してください。

   Important

   Application SecurityにLDAPサーバへのアクセスを提供するためにユーザアカウント名を使用しないでください。

3. アカウント名の間の競合をチェックします。

   LDAPディレクトリにデフォルトのApplication Securityアカウント `admin` が含まれている場合、両方のアカウントを無効にする可能性がある競合が発生します。既存のApplication SecurityアカウントがLDAPサーバ向けに定義されたアカウントと同じ名前を持つ場合、Application Securityアカウント設定と属性はLDAPサーバに保存されているアカウント設定と属性よりも優先されます。

   Note

   OpenTextでは、Application Securityのユーザ名をLDAPサーバで複製しないことを推奨しています。

4. 必要な情報を収集して記録します。

5. OpenTextでは、referral機能を無効にすることを推奨しています。

「LDAPサーバreferral機能について」および「LDAP referralサポートを無効化する」を参照してください。

参照情報

LDAPサーバの設定

1.6.16.2. 複数のLDAPサーバの要件

複数のLDAPサーバを使用する場合は、次の要件が適用されます。

- **ユーザ名は、すべてのLDAPサーバで一意である必要があります。**

  OpenTextでは、すべてのLDAP設定でユーザ名を固有のものにすることを強く推奨しています。Application Securityは、所与のLDAPサーバ設定で指定されたusername属性に基づいてユーザを検索します。検索はすべてのサーバで実行されるので、検索で1つの結果だけが返されることが重要です。設定済みのすべてのLDAPサーバで一意の検索結果が生じるusername属性を必ず使用してください。たとえば、複数のActive Directoryを使用する場合、ADサーバ間で固有ではない可能性があるデフォルトの `userPrincipalName` ではなく、 `sAMAccountName` をusername属性として使用することが合理的な場合があります。

  この要件が満たされない場合...

  場合によっては、管理者がユーザ名の重複を回避するのが難しい場合があります。Application Securityで、ログイン時に特定のユーザ名が複数のLDAPサーバで発見された場合、そのユーザ名のすべてのパスワードを使用して解決しようとします。そして最初にパスワードが認証された事例を採用します。ほとんどの場合、固有でないユーザ名を持つユーザでも、正常にFortify Application Securityにサインインして、ほとんどのユーザインタフェース機能にアクセスできます。ただし、レポート生成、トークンベースの認証、OpenText ScanCentral DAST統合などの一部の機能は、このようなユーザに対してサポートされません。

- **個別のLDAPサーバ設定で完全に独立した名前空間(ツリー)を管理する必要がある**

  この要件により、Application SecurityによるLDAP識別名の一意の検索が確保されます。そのための最も簡単な(および推奨される)方法は、設定されたベース識別名が他のいずれのサフィックスになっていないことを確認することです。

  さらに複雑なケースでは、サブツリーを2つ目のLDAPサーバ設定で管理するように委任することが可能な場合もあります。ただし、その場合は、すべての送信識別名参照(グループメンバーDNなど)も、2つ目のLDAPサーバで管理する必要があります。たとえば、ベース識別名 `DC=acme,DC=com` を持つLDAPサーバ設定が1つあるのに対し、 `OU=org,DC=acme,DC=com` サブツリーが別のLDAPサーバで管理されている場合、 `OU=org,DC=acme,DC=com` LDAPサブツリーだけを管理する2つ目のLDAP設定を設定できます。ただし、Application Securityに登録されている1つ目のLDAPサーバのLDAPオブジェクトのいずれも、 `OU=org,DC=acme,DC=com` サブツリーを(直接または遷移的に)参照していないこと、そしてその逆も必ず確認する必要があります。

この要件が満たされない場合...

LDAPオブジェクトの識別名が複数のLDAPサーバのベース識別名と一致する場合、Application Securityはベース識別名が指定されたLDAPオブジェクト識別名と最も一致するLDAPサーバに対して検索を実行します。この場合、Application Securityで意図しないLDAPオブジェクトのデータが処理に使用され、予期しない動作を引き起こす可能性があります。

1.6.16.3. LDAPサーバreferral機能について

一部のLDAPサーバでは、「referral」と呼ばれる特別な機能を使用します。referralとは、他のオブジェクトの名前と場所を含むエンティティです。referralは、クライアント要求を別のサーバにリダイレクトします。サーバはreferralを送信して、クライアントから要求された情報が、おそらく別の1つ以上のサーバ上の1つ以上の場所で検出できることを示します。

Application SecurityがLDAPオブジェクトを要求し、そのオブジェクトがreferralである場合、Application Securityは、REFオブジェクト属性で返されたアドレスにある別のサーバに、そのLDAPオブジェクトに関する追加情報を要求する必要があります。これらの追加要求により、LDAP通信速度が低下する可能性があります。LDAPサーバがreferral機能を使用しない場合でも、referralをサポートする追加操作が実行されます。

OpenTextでは、referralがLDAPサーバで使用されていない場合は、LDAPライブラリのreferralサポートを無効にすることを推奨しています。Application Securityサーバ側でこのオプションを無効にすると、Application Security-LDAP間通信がはるかに高速になります。手順については、「LDAP referralサポートを無効化する」を参照してください。

Note

referralの詳細な説明については、Oracleドキュメントの「Referrals in the LDAP」を参照してください。

1.6.16.4. LDAP referralサポートを無効化する

referralサポートを無効にするには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**LDAPサーバ(LDAP Servers)**］を選択します。
3. referralサポートを無効にする対象のLDAPサーバ接続をクリックします。

   行が展開されて、LDAPサーバに関する詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. ［**高度な統合プロパティ(ADVANCED INTEGRATION PROPERTIES)**］エリアまで下にスクロールします。
6. 「**LDAP referral処理戦略**」リストから、［**無視**］を選択します。
7. ［**保存(SAVE)**］をクリックします。

1.6.16.5. LDAPサーバの設定

次の手順では、Application SecurityでLDAP認証サーバを使用するように設定する方法について説明します。

Important

［**LDAP**］ページでプロパティを設定する前に、「LDAPユーザ認証」の説明に従ってLDAP認証を準備する必要があります。そのセクションでは、複数のLDAPサーバを設定するための要件と推奨事項について説明しています。

Important

OpenTextでは、何らかの時点でLDAPサーバで問題が発生した場合に備え、いくつかのローカル管理者アカウントを管理することを推奨しています。

Application SecurityのLDAPサーバ接続を設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**LDAPサーバ(LDAP Servers)**］を選択します。
3. ［**LDAPサーバ(LDAP servers)**］ページで、［**新規(NEW)**］をクリックします。
4. ［**新しいLDAP設定の作成(CREATE NEW LDAP CONFIGURATION)**］ダイアログボックスで、次の表の説明に従って設定を行います。

フィールド	説明
BASIC SERVER PROPERTIES	
Enable this LDAP configuration	Application SecurityでこのLDAPサーバを使用するには、このチェックボックスをオンにします。
Server name	このサーバの固有の名前を入力します。 **Important** 複数のLDAPサーバを設定する場合は、それぞれに固有のサーバ名を指定してください。

フィールド	説明

サーバURL (Server URL)	LDAP認証サーバのURLを入力します。
	
	セキュリティ保護されていないLDAPを使用する場合は、URLを次の形式で入力します。
	
	`ldap://<hostname>:<port>`
	
	`ldap://` プロトコルを指定し、［**SSL trust check**］または［**Hostname validation**］チェックボックスが選択されている場合、StartTLSを使用してLDAPサーバに接続します。それ以外の場合は、暗号化されていない接続が使用されます。
	
	セキュリティ保護されたLDAPSを使用する場合は、URLを次の形式で入力します。
	
	`ldaps://<hostname>:<port>`
	
	LDAPSでは、暗号化されたユーザ資格情報だけが転送されます。

フィールド	説明
Base DN	LDAPディレクトリ構造検索のベース識別名(DN)を入力します。 **Important** Application Securityに複数のLDAPサーバを設定する場合は、それぞれに固有のベースDNを設定する必要があります。 たとえば、 `companyName.com` のベースDNは `dc=companyName,dc=com` です。 すべてのDN値では大文字と小文字が区別され、余分なスペースを含めることはできません。また、LDAPサーバエントリと完全に一致する必要があります。 値を指定しない場合は、 Application Security はDAPオブジェクトツリーのルートから検索します。複数のLDAPサーバを使用する場合、ベースDNはそれぞれに対して一意である必要があります。1つのサーバのベースDNが空の場合、別のLDAPサーバでは空にできません。

フィールド	説明
Bind user DN	Application Securityが認証サーバへの接続に使用するアカウントの完全識別名(DN)を入力します。バインドアカウントには専用のLDAPサービスアカウントを使用します。このアカウントを、Application Securityにログインするための標準的なユーザアカウントとして使用しないでください。 このアカウントは、Application Securityで排他的に使用するために作成した、最小限の特権が付与された読み込み専用の認証サーバアカウントでなければなりません。 **Important** セキュリティ上の理由から、実稼働環境では実際のユーザアカウント名は使用しないでください。 Active Directoryを使用する場合は、ドメイン名とユーザ名を次の形式で指定します。 `<domain_name>\<username>`
Bind user password	バインドユーザDNアカウントのパスワードを入力します。
Show password	入力したパスワードを表示するには、このチェックボックスをオンにします。

フィールド	説明

Relative search DNs (1 per line)	(オプション)相対識別名(RDN)を入力します。RDNは、LDAPディレクトリ検索でのベースDNからの開始点を定義します。OpenTextでは、ベースDNから検索することを推奨しています。ただし、LDAPディレクトリのサイズが大きすぎてApplication Securityユーザの検索に時間がかかる場合は、RDNを使用して検索するLDAPエントリの数を制限します。また、セキュリティ上の理由から、RDNを使用してLDAPツリーの一部をApplication Securityから隠すこともできます。
	
	たとえば、companyName.comというベースDNと、このベースDNに属するすべてのエントリの中から検索するには、次のように指定して、そのパス内のすべてのエントリを再帰的に検索します。
	
	`cn=users`
	
	または
	
	`cn=users,ou=divisionName`

フィールド	説明
Ignore partial result exception	検索結果にLDAPサーバが返すことができる数を超えるレコードが含まれる場合に検索が失敗しないようにするには、このチェックボックスをオンのままにします。 この設定を有効にして、LDAPサーバの設定ミスを非表示にすることもできます。たとえば、LDAPサーバがクエリ結果の数を500に制限している一方で、実際の結果が600件ある場合、この設定が有効にされていると、Application Securityから500件のレコードだけが返されます。
LDAP server type	このリストから、Application Securityと接続するLDAPサーバのタイプを選択します (［**ACTIVE_DIRECTORY**］または［**その他(OTHER)**］)。
SECURITY	
SSL trust check	ドメインコントローラでSSLが有効になっている場合は、このチェックボックスをオンのままにすると、LDAPサーバによって提示された証明書が信頼された認証局によって発行されたことを確認できます。ドメインコントローラがSSL用に設定されていない場合は、このチェックボックスをオフにします。

フィールド	説明
ホスト名検証(Hostname validation)	ドメインコントローラがSSLに対して有効になっている場合は、このチェックボックスをオンのままにすると、LDAPサーバのホスト名が、証明書の発行先のホスト名と一致します。ドメインコントローラがSSL用に設定されていない場合は、このチェックボックスをオフにします。
ユーザのステータスのマッピングを有効にする(Enable user status mapping)	(Microsoft Active Directoryのみ)このチェックボックスを選択すると、Application SecurityはこのLDAPサーバ上のユーザのステータス情報を取得できます。この情報により、トークンベースおよびSSOベースの認証スキームでの認証チェックが強化されます。
BASE SCHEMA	
Object class attribute	オブジェクトのクラスを入力します。たとえば、`objectClass`に設定すると、Application Securityは検索するエンティティタイプを決定する`objectClass`属性を検索します。デフォルト値は`objectClass`です。
Organizational unit class	LDAPオブジェクトを部門として定義するオブジェクトクラスを入力します。デフォルト値は`container`です。

フィールド	説明
User class	LDAPオブジェクトタイプをユーザとして識別するオブジェクトクラスを入力します。デフォルト値は `organizationalPerson` です。
Organizational unit name attribute	部門名を指定するグループ属性を入力します。デフォルト値は `cn` です。
Group class	LDAPオブジェクトタイプをグループとして識別するオブジェクトクラスを入力します。デフォルト値は `group` です。
Distinguished name (DN) attribute	Application Securityがエンティティの識別名を検索するために検索する属性を決定する値を入力します。デフォルト値は `distinguishedName` です。
USER LOOKUP SCHEMA	
User firstname attribute	ユーザの名を指定するユーザオブジェクト属性を入力します。デフォルト値は `givenName` です。
User lastname attribute	ユーザの姓を指定するユーザオブジェクト属性を入力します。デフォルト値は `sn` です。

フィールド	説明
Group name attribute	グループ名を指定するグループ属性を入力します。デフォルト値は `cn` です。
User username attribute	ユーザ名を指定するユーザオブジェクト属性を入力します。デフォルト値は `sAMAccountName` です。
User password attribute	ユーザのパスワードを指定するユーザオブジェクト属性を入力します。デフォルト値は `userPassword` です。
Group member attribute	グループのメンバーを定義するグループ属性を入力します。デフォルト値は `member` です。
User email attribute	ユーザの電子メールアドレスを指定するユーザオブジェクト属性を入力します。デフォルト値は `mail` です。
User memberOf attribute	LDAPユーザのLDAPグループ名を含むLDAP属性の名前を入力します。
USER PHOTO	
User photo enabled	LDAPサーバからユーザの写真を取得するには、このチェックボックスをオンにします。

フィールド	説明
User thumbnail photo attribute	Active Directoryのサムネイル写真属性
User thumbnail MIME default attribute	サムネイルMIMEのデフォルト属性
ADVANCED INTEGRATION PROPERTIES	
Cache LDAP user data	Application SecurityでLDAPユーザデータキャッシングを有効にするには、このチェックボックスをオンにします。 LDAPキャッシュは、Application Securityの［管理(Administration)］ビューから手動で更新できます。手順については、「LDAPエンティティの手動更新」を参照してください。 **Note** OpenTextでは、LDAPユーザキャッシングが有効にされた状態のままにすることを推奨しています。Application Securityによって、LDAPキャッシュが定期的に自動更新されます。

フィールド	説明
Cache: Max threads per cache	各更新プロセス(ユーザアクション)専用のスレッドの最大数を入力します。ユーザが［**Update**］をクリックすると、新しい更新プロセスが開始されます。デフォルト値は `4` です。
Cache: Initial thread pool size	使用可能なキャッシュ更新スレッドの初期数を入力します。この値により、複数のスレッドで同時にLDAPキャッシュを更新するタスク実行プログラムのスレッドプールが設定されます。デフォルト値は `4` です。
Cache: Max thread pool size	初期スレッドプールサイズが更新プロセスに対して不十分な場合に使用可能なスレッドの最大数を入力します。デフォルト値は `12` です。
Enable paging in LDAP search queries	LDAP検索クエリでページングを有効にするには、このチェックボックスをオンにします。 すべてのLDAPサーバがページングをサポートしているわけではありません。使用するLDAPサーバでこの機能がサポートされることを確認してください。

フィールド	説明
Page size of LDAP search request results	LDAPサーバが検索結果のサイズを特定の数のオブジェクトで制限し、［**Enable paging in LDAP search queries**］が選択されている場合は、LDAPサーバの制限値以下の値を入力します。デフォルト値は `999` です。
LDAP referrals processing strategy	OpenTextでは、使用するLDAPサーバが1つだけの場合、LDAPの動作を高速化するために［**無視(ignore)**］を選択することを推奨しています。マルチドメインLDAP設定を使用している場合にLDAP referralを使用する場合は、`follow` を選択します。デフォルト値は `ignore` です。 **Note** LDAPサーバでreferralが使用されていない場合は、「LDAPサーバreferral機能について」を参照してください。

フィールド	説明
LDAP authenticator type	このリストで、使用するLDAP認証タイプを次の中から1つ選択します。 ◦ **BIND_AUTHENTICATOR** - LDAPサーバへの直接認証(「バインド」認証)。 ◦ **PASSWORD_COMPARISON_AUTHENTICATOR** - ユーザが提供するパスワードは、リポジトリに格納されているパスワードと比較されます。 LDAP認証タイプの詳細については、https://spring.io/projects/spring-securityを参照してください。
LDAP password encoder type	LDAP認証方法がパスワード比較の場合にのみ、このリストから値を選択します。 LDAPサーバが使用するエンコーダタイプを選択する必要があります。Application Securityは、エンコードされたパスワードを比較します。たとえば、LDAPサーバがパスワードをエンコードするためにLDAP_SHA_PASSWORD_ENCODERを使用している場合に、［**MD4_PASSWORD_ENCODER**］を選択すると、パスワードの比較は失敗します。

フィールド	説明
Enable nested LDAP groups	このチェックボックスを選択すると、Application SecurityでのLDAPのネストされたグループのサポートが有効になります(特定のグループメンバー自体がグループである場合)。 **Note** ネストされたLDAPグループを使用するのは、どうしても必要な場合だけにしてください。ネストされたLDAPグループを有効にすると、Application Securityが認証中に余分なツリートラバーサルを実行しなければならなくなります。OpenTextでは、ネストされたグループを使用しない場合は、このチェックボックスをオフにすることを強く推奨しています。
Interval between LDAP server validation attempts (ms)	LDAPサーバが検証を試行した後、次に検証を試みるまで待機する時間(ミリ秒数)を入力します。デフォルト値は `5000` です。

フィールド	説明
Time to wait LDAP validation (ms)	Application Securityがキャッシュの更新要求をLDAPサーバに送信した後に応答を待機する時間(ミリ秒数)を入力します。指定した時間までに応答が受信されない場合、更新は実行されません。要求は、［LDAP server validation attempts］フィールドに設定された値によって決定される頻度で再送信されます。デフォルト値は `5000` です。
Base SID of Active Directory objects	(Microsoft Active Directoryのみ)LDAPディレクトリオブジェクトのベースセキュリティ識別子(SID)を指定します。
Object SID (objectSid) attribute	(Microsoft Active Directoryのみ)LDAPエンティティのオブジェクトID(Object Security Identifier)を含む属性の名前を入力します。 この属性は、オブジェクトセキュリティDに基づいてユーザを検索するために使用されます。Active Directoryおよび複数のLDAPサーバを使用する場合に必要です。

5. 設定の有効性を確認するには、［**VALIDATE CONNECTION**］をクリックします。
6. 設定の有効性を確認して保存するには、［**SAVE**］をクリックします。
7. 別のLDAPサーバを設定するには、手順3から6を繰り返します。

Important

複数のLDAPサーバを設定する場合は必ず、それぞれに固有のサーバ名と固有のベースDNを指定してください。

OpenTextでは複数のLDAPサーバの使用をサポートしていますが、ロードバランサの背後にある複数のLDAPサーバの使用はサポートしていません。ただし、同一のサーバを複数使用する場合はその限りではありません。

参照情報

LDAPサーバ設定を編集する

LDAPサーバ設定のインポート

LDAPユーザ認証

LDAPエンティティの登録

LDAPサーバ設定の削除

LDAPユーザ役割の管理について

1.6.16.5.1. LDAPサーバ設定を編集する

LDAPサーバ接続を編集するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**LDAPサーバ(LDAP Servers)**］を選択します。
3. ［**LDAPサーバ(LDAP Servers)**］ページで、編集するLDAPサーバ接続をクリックします。

   行が展開されて、LDAPサーバの詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. 「LDAPサーバを設定する」で説明されている属性に、必要なすべての変更を加えます。
6. 設定の有効性を確認するには、［**VALIDATE CONNECTION**］をクリックします。
7. 検証に成功した後に設定を保存するには、［**SAVE**］をクリックします。

参照情報

LDAPエンティティの登録

LDAPユーザ認証

LDAPユーザ役割の管理について

1.6.16.5.2. LDAPサーバ設定の削除

Application Securityインスタンスに対して複数のLDAPサーバが設定されている場合は、デフォルトサーバを除き、これらのサーバを削除できます。デフォルトサーバについては、無効にすることしかできません。

LDAPサーバ設定を削除するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**LDAPサーバ(LDAP Servers)**］を選択します。
3. 次のいずれかを実行します。
   - ［**LDAPサーバ(LDAP Servers)**］ページで、削除するLDAPサーバのチェックボックスをオンにしてから、［**LDAPサーバ(LDAP Servers)**］ツールバーで［**削除**］をクリックします。

     または

   - ［**LDAPサーバ(LDAP Servers)**］ページで、削除するLDAPサーバ接続をクリックし、［**削除**］をクリックします。
4. LDAP設定で操作を続行することを確認する場合は、［**OK**］をクリックします。
5. すべてのLDAPユーザに再認証を強制するには、Application Securityサーバを再起動します。

参照情報

LDAPユーザ認証

LDAPエンティティの登録

LDAPユーザ役割の管理について

1.6.16.5.3. LDAPサーバ設定のインポート

Application Securityインスタンスのアップグレードの一環として、既存のLDAP設定をインポートする必要があります。

レガシーLDAPサーバ設定をインポートするには、次の操作をします。

1. ヘッダで、［**管理**］をクリックします。
2. ナビゲーションペインで［**設定(Configuration)**］を選択し、下にスクロールして［**LDAPサーバ(LDAP Servers)**］を選択します。
3. LDAPサーバのヘッダで、［**IMPORT**］をクリックします。
4. ［**レガシーLDAP設定のインポート(IMPORT LEGACY LDAP CONFIGURATION)**］ダイアログボックスで、インポートするLDAP設定のレガシー `ldap.properties` ファイルの内容を手動でコピーし、テキストボックスに貼り付けます。

   Application Securityがコピーした内容に関する問題を検出した場合は、メッセージと、詳細を表示するリンクが表示されます。

   > **Note**
   >
   > エンコードされたバインドユーザDN (`ldap.user.dn`)およびバインドユーザパスワード(`ldap.user.password`)の値はインポートされません。これらの値は、手動で入力する必要があります(「LDAPサーバを設定する」を参照)。

5. 問題があればそれを修正して、［**NEXT**］をクリックします。
6. 「LDAPサーバを設定する」のステップ4の表で説明されている属性を設定します。
7. 設定の有効性を確認するには、［**VALIDATE CONNECTION**］をクリックします。
8. 設定の有効性を確認して保存するには、［**SAVE**］をクリックします。

参照情報

LDAPエンティティの登録

LDAPユーザ認証

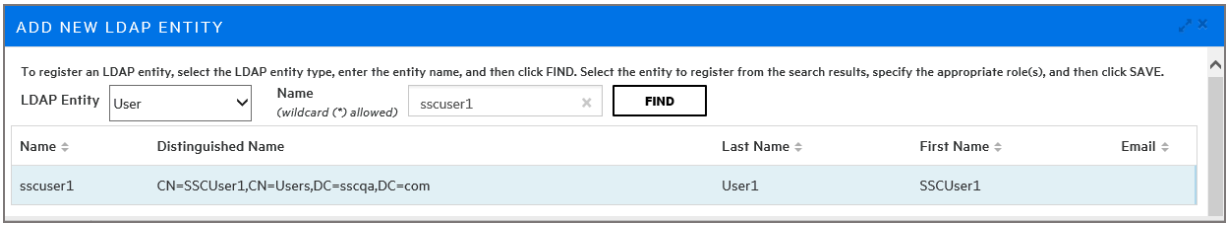
LDAPユーザ役割の管理について

1.6.16.5.4. LDAPエンティティの登録

管理者は、LDAPグループ、部門、およびユーザをApplication Securityユーザのリストに追加できます。ユーザがグループに参加またはグループから離れると、Application Securityによってアクセス制御が自動的に更新されます。

LDAP部門、グループ、またはユーザをApplication Securityに登録するには、次の手順に従います。

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**LDAPエンティティ(LDAP Entities)**］を選択します。
4. ［**LDAP**］ツールバーで 、［**+ADD**］をクリックします。
5. ［**LDAPエンティティ(LDAP Entity)**］リストから、登録するLDAPエンティティのタイプ(［**グループ(Group)**］、［**ユーザ(User)**］、または［**部門(Organizational Unit)**］)を選択します。
6. 返されたエンティティのリストで、登録するユーザ、グループ、または部門を選択します。



7. ［**Roles**］セクションで、選択したエンティティに割り当てる役割に対応するチェックボックスをオンにします。
8. LDAPエンティティにアプリケーションのバージョンへのアクセス権を付与するには、［**アクセス**］セクションで次の操作を行います。

> **Note**
>
> 複数のアプリケーションのバージョンを追加できますが、次の手順を使用して1度に1つ追加する必要があります。

   1. ［**+ ADD**］をクリックします。

2. ［**アプリケーションバージョンの選択(SELECT APPLICATION VERSION)**］ダイアログボックスの［**アプリケーション(Application)**］リストで、LDAPエンティティにアクセスさせるアプリケーションの名前を選択します。

   Application Securityは、アプリケーションのすべてのアクティブなバージョンを一覧表示します。

3. アプリケーションの非アクティブバージョンを表示するには、［**Show inactive versions**］チェックボックスを選択します。
4. エンティティがアクセスする全バージョンのチェックボックスを選択します。
5. ［**DONE**］をクリックします。

［**Access**］セクションには、選択したアプリケーションバージョンが一覧表示されます。

9. 次のいずれかを実行します。
   - 変更を保存して［**新しいLDAPエンティティの追加(Add New LDAP Entity)**］ダイアログボックスを閉じるには、［**保存(SAVE)**］をクリックします。
   - 変更を保存して別のLDAPエンティティを登録するには、［**SAVE AND ADD ANOTHER**］をクリックします。

Application Securityがエンティティをユーザのリストに追加し、以降は定期的にLDAPサーバキャッシュを自動更新します。

LDAPサーバの設定方法については、「LDAPサーバの設定」を参照してください。

参照情報

LDAPユーザ認証

LDAPユーザ役割の管理について

1.6.16.5.5. LDAPエンティティの手動更新

Application Securityによって、LDAPサーバキャッシュが自動的に定期的に更新されます。LDAPエンティティに変更を加える際、手動でLDAP更新プロセスを開始し、別の方法よりも変更を早く明らかにすることができます。

LDAP更新プロセスを手動で開始するには、次の手順に従います。

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**ユーザ**］、［**LDAPエンティティ(LDAP Entities)**］の順に選択します。
4. LDAPエンティティのリストで、更新するLDAPエンティティのチェックボックスを選択します。
5. ［**LDAP**］ツールバーで、［**更新(REFRESH)**］をクリックします。

LDAPサーバの設定方法については、「LDAPサーバの設定」を参照してください。

参照情報

LDAPユーザ認証

LDAPエンティティの登録

LDAPユーザ役割の管理について

1.6.16.5.6. 「無効」にマークされたLDAPエントリの処理

登録されたLDAPエンティティがLDAPサーバ内に存在しなくなったため、Application Security内にも必要なくなった場合は、そのエンティティをエンティティリストから削除します。または、LDAPエンティティの識別名が変更された場合は、それが反映されるようにApplication Security内のDN値を更新できます。

Note

次のステップは、LDAPグループ、部門、および個々のユーザに適用されます。

LDAPエンティティのDN値を更新するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**ユーザ**］、［**LDAPエンティティ(LDAP Entities)**］の順に選択します。
3. 変更する必要があるエンティティの行を選択し、［**EDIT**］をクリックします。
4. ［**UPDATE DISTINGUISHED NAME**］をクリックします

   このボタンは、現在のDNが無効な場合にのみ表示されます。
5. ［**識別名の更新(UPDATE DISTINGUISHED NAME)**］ダイアログボックスの［**識別名(Distinguished name)**］フィールドで現在無効な値を選択し、それを更新された識別名に置き換えます。
6. ［**保存(SAVE)**］をクリックします。

参照情報

LDAPサーバの設定

1.6.16.6. LDAPキャッシュの永続性の有効化

デフォルトでは、LDAPキャッシュはメモリ内に存在するに過ぎず、サーバのシャットダウン中に失われます。組織に大量のLDAPユーザがいる場合に、LDAPキャッシュが失われると、次回のサーバ起動が大幅に遅くなる可能性があります。

Note

組織に大量のLDAPユーザがいる場合は、次回のサーバ起動にかなりの時間がかかる可能性があります。これは、キャッシュを再構築する必要があるためです。

サーバのシャットダウン後もLDAPキャッシュを永続させるには:

1. Application Securityをシャットダウンします。
2. テキストエディタで `<fortify.home>/<app_context>/conf/app.properties` ファイルを開きます。
3. `ldap.cache.persistence.enabled` プロパティを `true` に設定します。
4. `app.properties` ファイルを保存して閉じます。
5. Application Securityを再起動します。

デフォルトのキャッシュ更新間隔の変更

デフォルトのキャッシュ更新間隔は1時間です。大きなLDAPグループがApplication Securityに登録されている場合、頻繁にキャッシュを更新するとApplication SecurityとLDAPサーバの負荷が増え、パフォーマンスに影響が出る可能性があります。

影響を減らすには、次のようにして間隔を長くします。

1. Application Securityをシャットダウンします。
2. テキストエディタで `<fortify.home>/<app_context>/conf/app.properties` ファイルを開きます。
3. 次の行を追加します:

```
ldap.cache.refresh.interval.hours=
<whole_number_between_1_and_12>
```

4. Application Securityを再起動します。

1.6.17. SCIM 2.0プロトコルの実装

System for Cross-domain Identity Management (SCIM)をApplication Securityで有効にした場合、SCIM 2.0 APIクライアントでは、識別情報データのプロビジョニングと管理のためにSCIM 2.0プロトコルを使用してユーザおよびグループをApplication Securityにプッシュします。つまり、ユーザを追加するためにApplication Securityの［管理］ビューで作業する必要がなくなります。代わりに、SCIM 2.0 APIクライアントからユーザとグループを設定します。

Note

任意のSCIM 2.0 APIクライアントと統合できます。ただし、その場合は、個別にApplication Securityとの相互運用性をテストする必要があります。公式にサポートされているのは、Microsoft Entra ID統合のみです。

SCIM APIを使用してプロビジョニングされるユーザは外部管理ユーザおよびシングルサインオンユーザのみであるため、次の条件が適用されます。

- Application Securityから外部管理ユーザに対しては、役割とアプリケーションバージョンを割り当てることのみが可能です。
- ユーザはSSOを使用してのみサインインできます。
- ローカルに作成されたユーザ名(［**管理(Administration)**］>［**ユーザ(Users)**］>［**ローカルユーザ(Local Users)**］)がすでにApplication Securityに存在する場合、同じユーザ名を持つユーザはSCIMを使用してプロビジョニングできません。［**管理**］ビューから作成されたユーザは、SCIMプロビジョニングでは読み込み専用となります。

サポートされるSCIMリソース

Application Securityでは、次のSCIMリソースをサポートしています。

- ユーザ(`urn:ietf:params:scim:schemas:core:2.0:User schema`)

  Application Securityでは、ユーザスキーマのすべての標準属性が許容されますが、保存されるのは、これらのサブセットのみです(「ユーザ属性マッピング」を参照)。Enterprise User拡張属性(`urn:ietf:params:scim:schemas:extension:enterprise:2.0:User schema`)も受諾しますが、保存しません。

- グループ(`urn:ietf:params:scim:schemas:core:2.0:Group schema`)

Application Securityでは、グループスキーマのすべての標準属性が許容されますが、保存されるのは、これらのサブセットのみです(「グループ属性マッピング」を参照)。

サポートされているオプション機能:

- リソースフィルタリング(RFC 7644 - 3.4.2.2 Filtering)
- PATCH操作(RFC 7644 - 3.5.2 - Modifying with PATCH)

ユーザ属性マッピング

次の表は、SCIMユーザ属性がApplication Securityユーザ属性にマップされる方法を示しています。

SCIMユーザ属性	Application Securityユーザ属性	コメント
meta.created	created	読み込み専用
meta.lastModified	lastModified	読み込み専用
id	N/A	読み込み専用、固有、不透過
userName	userName	固有、必須
active	suspended (not)	これに応じてApplication Securityの［Suspended］オプションが設定されます。
name.givenName	firstName	
name.familyName	lastName	
emails[type="work"].value	email	

グループ属性マッピング

次の表は、SCIMグループ属性がApplication Securityグループ属性にマップされる方法を示しています。

SCIMグループ属性	Application Securityグループ属性	コメント
meta.created	created	読み込み専用
meta.lastModified	lastModified	読み込み専用
id	N/A	読み込み専用、固有、不透過
displayName	name	Required
members	N/A	既存のユーザおよび/またはグループを参照する必要があります

参照情報

SCIM 2.0およびSAML 2.0を使用したユーザプロビジョニング用のMicrosoft Entra IDへの接続の設定

SAML 2.0準拠のシングルサインオンを使用するためのApplication Securityの設定

1.6.17.1. SCIM 2.0およびSAML 2.0を使用したユーザプロビジョニング用のMicrosoft Entra IDへの接続の設定

System for Cross-domain Identity Management (SCIM)プロトコルを使用して、Microsoft Entra IDのユーザアカウントでApplication Securityをプロビジョニングできます。次の表は、実行が必要な順序でこの機能を使用するためのタスクを一覧表示しています。

タスク	詳細
Application SecurityからSCIMを有効にする	SCIMによる外部管理されたユーザおよびグループのプロビジョニングの有効化
Microsoft Entraで、Microsoft Entra IDに移動し、エンタープライズアプリケーションを作成します。	Microsoft Entra IDのドキュメント **Note** Entra IDに新しいアプリケーションで実現したい機能を選択するプロンプトが表示されたら、［**ギャラリーにはない他のアプリケーションとの統合(ギャラリー以外) (Integrate any other application you don't find in the gallery (Non-gallery))**］オプションを選択します。
Entra IDから、新しいアプリケーションにユーザとグループを割り当てます。	Microsoft Entra IDのドキュメント

タスク	詳細
Entra IDから、アプリケーションをプロビジョニングします。 次の点に注意してください。 • ［**Provisioning Mode**］を［**Automatic.**］に設定します。 • Application SecurityのURLを［**テナントURL (Tenant URL)**］値として使用し、このURLに文字列 `/api/scim/v2?aadOptscim062020` を追加します。 **Note** `/api/scim/v2` は、Application Security SCIMエンドポイントのURLです。`aadOptscim062020` クエリパラメータにより、SCIM v2.0に対するEntra IDのコンプライアンスが向上します。 • ［**シークレットトークン(Secret Token)**］値には、Application Securityで作成したトークン(［**SCIMトークン(SCIM Token)**］)を使用します(「SCIMによる外部管理されたユーザおよびグループのプロビジョニングの有効化」を参照)。	Microsoft Entra IDのドキュメント

タスク	詳細
Entra IDから、Entra IDとApplication Securityの間のデータフロー用の属性マッピングを変更します。 ユーザの次の属性以外のすべての属性を削除します(グループの場合、属性マッピングは変更しません)。 • userName • active • emails[type eg "work"].value • name.givenName • name.familyName • externalID ［**プロビジョニングステータス(Provisioning Status)**］のトグルを［**オン(On)**］に切り替える必要があります。	Microsoft Entra IDのドキュメント
Entra ID SAMLメタデータが署名されています。Application Securityで署名を正常に検証するには、EntraからSAML署名証明書をダウンロードして、SSO SAML設定で使用するキーストア(SAMLキーストアの場所)にインポートする必要があります。 Entraで、作成したエンタープライズアプリケーションに移動します。SAMLベースのサインオンページで署名証明書をダウンロードし、キーストアにインポートします。	Microsoft Entra IDのドキュメント SAML 2.0準拠のシングルサインオンを使用するためのApplication Securityの設定

タスク	詳細
Application SecurityからSAMLシングルサインオンを設定します。	SAML 2.0準拠のシングルサインオンを使用するためのApplication Securityの設定
Application Securityからメタデータ XMLファイルを取得し、ローカルに保存します。このファイルにアクセスできるのは、Application SecurityでSAML SSOが有効にされ、正常に初期化されている場合のみです。	`<hostname>:<port>/<app_context>/saml/<metadata>`
Entraで、保存されたメタデータファイルをアップロードし、アップロードされたメタデータファイルのデータを使用してSAMLシングルサインオンのセットアップを完了します。	Microsoft Entra IDのドキュメント
Application Securityから、役割とアプリケーションのバージョンを外部管理ユーザおよびグループに割り当てます。	外部管理されたユーザおよびグループを表示する

1.6.17.2. SCIMによる外部管理されたユーザおよびグループのプロビジョニングの有効化

SCIMで外部管理されたユーザおよびグループのプロビジョニングを有効にするには、次の手順を実行します。

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**SCIM**］を選択します。
4. ［**SCIMを有効にする(Enable SCIM)**］チェックボックスをオンにします。
5. ［**SCIM Token**］ボックスに、Application SecuritySCIM APIで認証するためにベアラトークンとして使用するSCIMトークンを入力します。

   このトークンは、Application SecurityとEntra ID間の接続を設定する際に、Entra IDでシークレットトークンとして使用します。

   > **Important**
   >
   > トークンには、大文字と小文字、数字、ハイフン、およびアンダースコアを含めることができます。トークンには、32文字以上、512文字以下が含まれている必要があります。トークンによりApplication Securityでのユーザ管理へのアクセスが許可されるため、このトークンは保護する必要があります。OpenTextでは、セキュリティ保護されたランダム文字列ジェネレータを使用してトークンを生成することを推奨しています。

6. ［**保存(SAVE)**］をクリックします。

参照情報

SAML 2.0準拠のシングルサインオンを使用するためのApplication Securityの設定

SCIM 2.0プロトコルの実装

外部管理されたユーザおよびグループを表示する

1.6.18. 統合のプロキシの設定

1つのプロキシを設定して、Application SecurityのすべてのHTTP(s)プロトコルベースの統合で使用できます。プロキシを設定した後、Fortify Audit Assistant、Rulepack更新サーバURL、バグトラッキングプラグインなどのコンポーネントでの使用を有効化できます。

すべてのHTTPプロトコルベースのApplication Security統合で使用するために単一のプロキシを設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**プロキシ(Proxy)**］を選択します。

   ［**プロキシ(Proxy)**］ページで、次の表の説明に従って、設定の値を指定します。

フィールド	説明(Description)
Enable SSC proxy	このチェックボックスを選択すると、プロキシの使用が有効になります。
HTTP proxy host	HTTPプロキシホストの名前(プロトコル部分とポート番号なし)を入力します。たとえばsome.proxy.comです。
HTTP proxy port	HTTPプロキシポート番号を入力します。
HTTP proxy user	HTTP認証が必要な場合は、ユーザ名を入力します。
HTTP proxy password	HTTP認証が必要な場合は、パスワードを入力します。
HTTPS proxy	
Set up a different HTTPS proxy	HTTPS要求に対して別のセキュリティ保護されたプロキシを使用するには、このチェックボックスを選択します。
HTTPS proxy host	HTTPSプロキシホストの名前を入力します(プロトコル部分とポート番号なし)。たとえば、some.secureproxy.comです。
HTTPS proxy port	HTTPSプロキシポート番号を入力します。
HTTPS proxy user	HTTPS認証が必要な場合は、ユーザ名を入力します。
HTTPS proxy password	HTTPS認証が必要な場合は、パスワードを入力します。

3. ［**保存(SAVE)**］をクリックします。

参照情報

1.6.19. OpenText ScanCentral DASTスキャンの実行と管理の有効化

OpenText ScanCentral DASTは動的なアプリケーションセキュリティテストツールであり、OpenText DASTセンササービス、およびApplication Securityと組み合わせて使用できる他のサポート技術で構成されています。

OpenText ScanCentral DASTとの統合を有効にするには、Application Securityで次の手順を実行する必要があります。

1. OpenText ScanCentral DASTのサービスアカウントを作成して、Application Securityで認証します。OpenText ScanCentral DAST展開環境でこのサービスアカウントを使用する方法については、『*OpenText™ ScanCentral DAST設定と使用方法ガイド*』を参照してください。サービスアカウントは、次の要件を満たしている必要があります。
    - このアカウントは、管理者の役割を持つローカルユーザアカウントである必要があります。LDAPベースまたはSCIMベースのユーザアカウントなど、外部で管理されるアカウントは使用できません。
    - このアカウントは、OpenText ScanCentral DASTとApplication Securityを統合するためにのみ使用される専用アカウントである必要があります。このアカウントは、OpenText ScanCentral DASTユーザによるアクセスには使用できません。
2. 次の手順を実行して、Application SecurityでのOpenText ScanCentral DAST統合を有効にしてください。
    1. 管理者としてApplication Securityにサインインします。
    2. ヘッダで、［**管理(Administration)**］を選択します。
    3. ナビゲーションペインで、［**設定(Configuration)**］を開いてから、［**ScanCentral DAST**］を選択します。
    4. ［**ScanCentral DAST**］ページで、［**ScanCentral DASTを有効にする(Enable ScanCentral DAST)**］チェックボックスをオンにします。
    5. ［**ScanCentral DASTサーバURL(ScanCentral DAST server URL)**］ボックスに、OpenText ScanCentral DASTサーバのURLを入力します。

       ScanCentral DASTサーバのURLは、次のいずれかの形式である必要があります。

       `http://<DAST_API_Host>:<port>/api/`

`http://<DAST_API_IP>:<port>/api/`

代わりにhttpsプロトコルを使用できます。

> **Important**
>
> URLの末尾に `/api/` を含める必要があります。

6. ［**保存(SAVE)**］をクリックします。

次のタスクの実行方法については、『*OpenText™ ScanCentral DAST設定と使用方法ガイド*』を参照してください。

- OpenText ScanCentral DASTセンサおよびセンサプールの管理
- OpenText ScanCentral DASTスキャン、スケジュール、および設定の作成、実行、変更、および削除

1.6.20. OpenText ScanCentral DASTで使用するKafkaストリームの設定

オプションの設定として、Application Securityでの問題の監査の変更をOpenText ScanCentral DASTと同期するために、Apache® Kafka®サービスをデプロイできます。

監査履歴の変更をKafkaにストリーミングするようにApplication Securityを設定するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**Kafkaストリーム(Kafka Stream)**］を選択します。
3. ［**Kafka Stream**］ページで、次の表の説明に従って設定を行います。

フィールド	説明
Kafkaへの監査の更新のストリーミングを有効にする(Enable streaming audit updates to Kafka)	このチェックボックスをオンにすると、監査履歴の変更がApplication SecurityからKafkaに同期されます。
Kafkaブートストラップサーバのカンマ区切りリスト(A comma-separated list of Kafka bootstrap servers)	Kafkaインスタンスのブローカをカンマ区切りリストで指定します。 このリストに使用する構文: `<host1>:<port1>,<host2>:<port2>,...`
監査の更新が発行されるKafkaトピック(The Kafka topic to which audit updates are published)	監査イベントを検索するKafkaトピックを指定します。
Kafkaセキュリティ	
Kafkaストリーミングに対してTLS相互認証を有効にする(Enable TLS mutual auth for Kafka streaming)	このチェックボックスをオンにすると、Kafkaブローカとの通信に対して、双方向SSLプロトコルを使用した相互認証が有効になります。Application Securityは、TLSv1.2とTLSv1.3を使用して、双方向のSSLをサポートします。 このチェックボックスをオンにしない場合、Kafkaブローカとの通信のためのセキュリティプロトコルとして、PLAINTEXTが使用されます。

フィールド	説明
Truststoreファイルの場所(Truststore file location)	Truststore証明書を含む、JKSファイル形式のTruststoreファイルのパスを指定します。
Truststoreパスワード(Truststore password)	Truststoreファイルのパスワードを指定します。
キーストアの場所(Keystore location)	クライアントの公開鍵と秘密鍵を含む、JKSファイル形式のキーストアファイルのパスを指定します。
キーストアパスワード(Keystore password)	キーストアファイルのパスワードを指定します。
秘密鍵のパスワード(Private key password)	秘密鍵のパスワードを指定します。
Kafkaサーバのホスト名検証を有効にする(Enable hostname validation of Kafka server)	このチェックボックスをオンにすると、Kafkaサーバの完全修飾ドメイン名(FQDN)またはIPアドレスを、そのKafkaサーバの実際のホスト名またはIPアドレスに照らして検証します。これにより、正しいKafkaサーバに接続していることを確認できます。

4. ［**保存(SAVE)**］をクリックします。

有効な資格情報の生成とクライアントセキュリティの設定の詳細については、Apache Kafkaのドキュメントを参照してください。

1.6.21. Fortify ScanCentral SASTとの統合を有効化

OpenText SAST (Fortify Static Code Analyzer)のユーザは、リソースを最大限に活用するために、Fortify ScanCentral SASTを使用して、プロセッサ集約型のスキャンフェーズを専用のOpenText SASTスキャンファームにオフロードできます。Fortify ScanCentral SASTを監視し、その結果をApplication Securityに表示できます。また、センサプールを作成して管理することもできます。この機能を有効にするには、Application Securityで統合を設定する必要があります。

Note

Fortify ScanCentral SASTの設定方法と使用方法については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

統合を設定するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**ScanCentral SAST**］を選択します。
4. ［**ScanCentral SAST**］ページで、［**ScanCentral SASTを有効にする(Enable ScanCentral SAST)**］チェックボックスをオンにします。
5. ［**ScanCentral ControllerのURL (ScanCentral Controller URL)**］ボックスに、コントローラのURLを入力します。

   Important

   コントローラは、Application Securityと同じバージョン以上である必要があります。

6. ［**ScanCentralポーリング間隔(秒数) (ScanCentral poll period (seconds))**］ボックスに、ScanCentral SASTからのデータポーリングのセッション間隔(秒数)を入力します。
7. ［**SSCとScanCentral Controllerの共有シークレット(SSC and ScanCentral controller shared secret)**］ボックスに共有秘密鍵(非暗号化)を入力し、Application Securityがコントローラのデータを要求できるようにします。

平文を使用する場合、この文字列は、コントローラの `config.properties` ファイルに格納されている `ssc_scancentral_ctrl_secret` プロパティの値と一致する必要があります。

コントローラは、管理コンソールデータの要求時に共有秘密鍵を検証します。

8. ［**保存(SAVE)**］をクリックします。
9. Application Securityサーバを再起動します。

参照情報

Fortify ScanCentral SASTの許可

Fortify ScanCentral SAST Controller情報の表示

Fortify ScanCentral SASTセンサプールについて

Fortify ScanCentral SASTセンサプールの作成

1.6.22. ジョブスケジューラ属性の設定

Application Securityバックグラウンドジョブを処理するためのスケジュール属性を設定できます。

ジョブスケジューラ設定を設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**スケジューラ(Scheduler)**］を選択します。
3. ［**スケジューラ(Scheduler)**］ページで、次の表の説明に従って設定を行います。

フィールド	説明
実行済みジョブが削除されるまでの日数(Number of days after which executed jobs are removed)	完了したジョブを削除するまでの日数を入力します。デフォルト値は `1` (日)です。 キャンセルされたジョブの削除は毎日行われます。

フィールド	説明
ジョブ実行を一時停止する(Pause job execution)	このチェックボックス(［**スケジューラ(Scheduler)**］ページでは選択不可)は、サーバのシャットダウンまたはシステム保守の準備としてジョブ実行が(［**保守(Maintenance)**］ページで)一時停止されたかどうかを示します。 このチェックボックスをオンまたはオフにするために［**保守(Maintenance)**］ページに移動するには、［**こちら(here)**］リンクをクリックします。この設定の変更は、［**保守(Maintenance)**］ページで変更を保存した直後に有効になります。サーバを再起動する必要はありません。 ジョブの実行を一時停止すると、現在実行中のジョブ(アーティファクト処理、レポート生成、データエクスポート要求など)は完了まで続行します。新しく送信されたジョブは、処理対象としてキューに登録されます。［**ジョブ実行を一時停止する(Pause job execution)**］チェックボックスがオフにされると、通常のジョブの処理が再開されます。

フィールド	説明
	Important OpenTextでは、ジョブ実行を一時停止するのはサーバのシャットダウン直前にして、一時停止の期間をできる限り短くすることを強く推奨しています。これにより、大量のジョブがキューに登録されて後で処理されるという事態を回避できます。 **Caution** 保守後にサーバが再び起動しても、ジョブ実行は自動的には再開されません。ジョブ実行を再開するには、［**保守(Maintenance)**］ページに戻り、［**ジョブ実行を一時停止する(Pause job execution)**］チェックボックスをオフにする必要があります。
トークン管理(Token management)	

フィールド	説明
トークンの有効期限アラート(Token expiration alerts)	ユーザにトークン有効期限切れを予告する、トークン有効期限までの残り日数を入力します。有効な値の範囲は `3` ～ `30` 日です。 デフォルト値は `7` (日)です。 **Note** Application Securityサーバロケールでは、1日の開始は12 AMです。

スナップショット更新(Snapshot refresh) -このエリアのフィールドを使用して、スナップショットジョブをスケジュールします。

スナップショットとは、ある時点でキャプチャされたアプリケーションバージョン情報です。この情報には、スケジュールされた時刻にアプリケーションバージョンのトレンドを計算するための変数とパフォーマンスインジケータの値が含まれます。

Note

［**曜日(Days of the week)**］、［**時間(Hours)**］、および［**分(Minutes)**］フィールドに入力した値が連結されて、スケジューラが使用するCRON式が作成されます。

フィールド	説明
曜日(Days of the week)	CRON構文を入力して、履歴スナップショットジョブを実行する曜日を指定します。曜日の3文字の略語を使用することも(たとえば、木曜日の場合は「`THU`」と入力)、1桁の値として、日曜日の場合は`1`、月曜日の場合は`2`などと入力することもできます。複数の日にスケジューラを実行するには、エントリをカンマで区切ります。たとえば、`SUN,WED,FRI`または`1,4,6`と入力します。 **Note** 3文字の略語は大文字で入力します。エントリ間のスペースはオプションです。 連続する曜日を指定するには、エントリをダッシュで分離します。たとえば、平日にのみスケジューラを実行するには`MON-FRI`と入力します。 アスタリスク(`*`)を入力すると、スケジューラが毎日実行されます(デフォルト)。

フィールド	説明
Hours	24時間表記を使用して、反復スケジューラジョブの実行を開始する時間を入力します。たとえば、`1`と入力すると、ジョブは午前1時に開始されます。 アスタリスク(`*`)を入力すると、スケジューラは1時間ごとに実行されます デフォルト値は`0` (午前0時)です。
Minutes	繰り返し発生するスケジューラジョブの実行を開始する分を入力します。たとえば、［**時間(Hours)**］ボックスに入力した時間の24分後にジョブを開始するには、`24`と入力します。 デフォルト値は`0`です(ジョブが最初の1分で実行を開始することを意味します)。

インデックス保守(Index maintenance) -このエリアのフィールドを使用して、Application Securityフルテキスト検索インデックスの保守をスケジュールします。OpenTextでは、このジョブは毎日実行することを推奨しています。

Note

［**曜日(Days of the week)**］、［**時間(Hours)**］、および［**分(Minutes)**］フィールドに入力した値が連結されて、スケジューラが使用するCRON式が作成されます。

フィールド	説明
曜日(Days of the week)	CRON式を入力して、インデックス保守ジョブを実行する曜日を指定します。値は、曜日の3文字の略語として入力することも(たとえば、木曜日の場合は `THU` を使用)、1桁の値として、日曜日の場合は `1`、月曜日の場合は `2` などと入力することもできます。 複数の日にスケジューラを実行するには、エントリをカンマで区切ります。たとえば、 `SUN,WED,FRI` または `1,4,6` と入力します。 **Note** 3文字の略語は大文字で入力します。エントリ間のスペースはオプションです。 連続する曜日を指定するには、エントリをダッシュで分離します。たとえば、平日にのみスケジューラを実行するには `MON-FRI` と入力します。 アスタリスク(`*`)を入力すると、スケジューラが毎日実行されます(デフォルト)。

フィールド	説明
Hours	24時間表記を使用して、反復インデックス保守ジョブの実行を開始する時間を入力します。たとえば、`1`と入力すると、ジョブは午前1時に開始されます。 アスタリスク(`*`)を入力すると、スケジューラは1時間ごとに実行されます デフォルト値は`0` (午前0時)です。
Minutes	繰り返し発生するインデックス保守ジョブの実行を開始する分を入力します。たとえば、［**時間(Hours)**］ボックスに入力した時間の24分後にジョブを開始するには、`24`と入力します。 デフォルト値は`0`です(ジョブが最初の1分で実行を開始することを意味します)。
Events maintenance	

フィールド	説明
保持日数(Days to preserve)	Application Securityが過去のイベントを削除するまでの日数を入力します。イベントの削除を指定しない場合は、`0`と入力します。 Application Securityは、専用のクリーンアップジョブの次回実行時に新しい値を使用します。新しいジョブは毎日午後11時30分に作成され、ブロックされていない場合は直ちに処理が開始されます。 デフォルト値は`0`です。これは、クリーンアップが実行されないことを意味します。
レポートの保守(Reports maintenance)	
保持日数(Days to preserve)	生成されたレポートがApplication Securityで保持される日数を入力します。デフォルト値は`0`です。これは、クリーンアップが実行されないことを意味します。 クリーンアップジョブに要する時間やリソースが過大にならないよう、毎晩の実行で最大2000件の古いレポート（および関連エンティティ）が消去されます。残りのレポートは、その後の数日間でApplication Securityによって徐々にクリーンアップされます。
データエクスポートの保守(Data export maintenance)	

フィールド	説明
保持日数(Days to preserve)	Application Securityがエクスポートされた監査レポートを保持する日数を入力します。 デフォルト値は `2` です。 **Note** このジョブは毎日11:45 PM (23:45)に実行されます。

4. ［**保存(SAVE)**］をクリックします。
5. 設定を適用するには、サーバを再起動します。

参照情報

ジョブ実行優先度の設定

バックグラウンドジョブ実行戦略の設定

スケジュールされたジョブのキャンセル

繰り返し実行されるクリーンアップジョブ

1.6.22.1. ジョブ実行優先度の設定

Application Securityの新しいジョブの優先度は、いずれも［**非常に低い(Very Low)**］に設定されます。優先度が同じ複数のジョブは、ジョブキューに追加された順序で処理されます。つまり、キューに最初に追加されたジョブが最初に処理されます。優先度の高い値が設定されたジョブは、優先度の低いジョブよりも前に処理されます。

Application Security管理者またはセキュリティリードは、スケジュールされて［**準備済み(Prepared)**］状態になっているジョブの優先度を変更できます。ジョブ状態の有効な値は、［準備済み(Prepared)］、［実行中(Running)］、［完了(Finished)］、［失敗(Failed)］、および［キャンセル(Canceled)］です。

スケジュールされたジョブの優先度を設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**メトリックとトラッキング(Metrics & Tracking)**］を選択し、［**ジョブ(Jobs)**］を選択します。
3. ［**ジョブ(Jobs)**］ツールバーの［**状態によるフィルタ処理(Filter by state)**］リストから［**準備済み(Prepared)**］を選択します。
4. 優先度を変更するジョブの行をクリックして展開します。
5. ［**優先度の設定(SET PRIORITY)**］リストから、優先度を選択します。

   ジョブの優先度を変更すると、キュー内の他のジョブに影響する場合があります。ジョブに設定した優先度が他のジョブに影響を与える可能性がある場合、その可能性を示すメッセージが表示され、変更を続行するかどうかを確認するよう求められます。
6. 優先度の変更を適用するには、［**OK**］をクリックします。

変更された優先度設定がジョブテーブルに反映されます。

参照情報

スケジュールされたジョブのキャンセル

ジョブスケジューラの設定

1.6.22.2. スケジュールされたジョブのキャンセル

管理者またはセキュリティリードは、準備済み状態になっているままのスケジュール済みジョブをキャンセルできます。ジョブ状態の有効な値は、［準備済み(Prepared)］、［実行中(Running)］、［完了(Finished)］、［失敗(Failed)］、および［キャンセル(Canceled)］です。

ジョブをキャンセルするには、次の手順を実行します。

1. Application Securityに管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**ジョブ(Jobs)**］を選択します。
4. ［**ジョブ(Jobs)**］ツールバーの［**状態によるフィルタ処理(Filter by State)**］リストから［**準備済み(Prepared)**］を選択します。
5. キャンセルするジョブの行をクリックします。
6. ［**CANCEL**］をクリックします。
7. ジョブのキャンセルを確認するには、［**OK**］をクリックします。

参照情報

ジョブスケジューラ属性の設定

1.6.23. 繰り返し実行されるクリーンアップジョブ

Application Securityでは、いくつかのクリーンアップジョブを繰り返し実行します。次の表で説明します。

ジョブ名	説明(Description)	影響を受けるテーブル	デフォルトのスケジュール
データエクスポートのクリーンアップ(Data Export Cleanup)	指定されている日数を経過したエクスポート済みデータ(CSVファイルなど)を削除します(「ジョブスケジューラの設定」を参照)。	dataexport documentinfo datablob	毎日(23:45) このジョブをスケジュールする方法については、「ジョブスケジューラの設定」を参照してください。
イベントログのクリーンアップ(Event Log Cleanup)	［**スケジューラ(Scheduler)**］ページで指定されている日数を経過したイベントレコードを削除します。	eventlogentry	毎日(23:30) このジョブをスケジュールする方法については、「ジョブスケジューラの設定」を参照してください。
期限切れトークンのクリーンアップ(Expired Tokens Cleanup)	有効期限が過ぎた期限切れトークンを削除します。	agentcredential	毎日、6時間おき、00:00から開始
IDテーブルのクリーンアップ(ID Table Cleanup)	ユーザ許可の操作やレポートの生成でフィルタ処理に使用されたIDを削除します。	id_table pv_id_table	毎日(23:00) このジョブをスケジュールする方法については、「ジョブスケジューラの設定」を参照してください。

ジョブ名	説明(Description)	影響を受けるテーブル	デフォルトのスケジュール
ジョブのクリーンアップ(Job Cleanup)	完了したジョブを削除します。失敗したジョブは、そのジョブの開始時刻から数えて、設定された日数が経過した時点で削除されます。キャンセルされたジョブは、開始時刻に関係なくクリーンアップされます。	jobqueue	毎日(23:00)
孤立したデータのクリーンアップ(Orphaned Data Cleanup)	不要になった添付ファイルに関連付けられているメタデータを削除します。	documentinfo	毎週日曜日(23:30)
孤立したソースファイルのクリーンアップ(Orphaned Source Files Cleanup)	既存の問題から参照されなくなったソースファイルを削除します。	sourcefile	毎日(0:00) job.sourceFileCleanup.cronを使用して設定します。
レポートのクリーンアップ(Report Cleanup)	［**スケジューラ(Scheduler)**］ページの［**保持日数(Days to preserve)**］で指定されている日数を経過している生成済みレポートを削除します。	savedreport documentinfo datablob	クリーンアップのスケジュールなし このジョブをスケジュールする方法については、「ジョブスケジューラの設定」を参照してください。

ジョブ名	説明(Description)	影響を受けるテーブル	デフォルトのスケジュール
Webhook履歴のクリーンアップ(Webhook History Cleanup)	古いwebhookイベントエントリを削除します。	webhookhistory	毎日(3:30)
インデックス保守(Index Maintenance)	グローバル検索(フルテキスト)インデックスと既存のデータベースエントリとの間の不整合を解決します。たとえば、不完全なサーバシャットダウンやインデックス付けジョブの失敗を原因とする不整合を解決します。	N/A	毎日(0:00) このジョブをスケジュールする方法については、「ジョブスケジューラの設定」を参照してください。
LDAPの更新(LDAP Refresh)	LDAPエンティティに関連付けられたキャッシュを更新します。	N/A	6時間おき
履歴スナップショット(Historical Snapshot)	古いスナップショットを再作成します。	N/A	毎日(0:00) このジョブをスケジュールする方法については、「ジョブスケジューラの設定」を参照してください。

ジョブ名	説明(Description)	影響を受けるテーブル	デフォルトのスケジュール
アラートリマインダ(Alert Reminder)	リマインダアラートを送信します。	N/A	毎日(3:00)
トークンの期限切れアラート(Token Expiry Alerts)	間もなく期限切れになるトークンについてユーザに通知します。	N/A	毎日(3:00)

1.6.24. データ保持について

管理者はデータ保持を有効にして、アーティファクトがApplication Securityで保持される期間を定義するデフォルトのデータ保持ポリシーを設定することができます。アプリケーションバージョンごとに、アーティファクトの保持期間と、保持するアーティファクトの数を定義できます。

定義された保持期間に達すると、アーティファクトはApplication Securityからのパージ対象となります。データ保持を有効にする際に、Application Securityからアーティファクトをパージするデータクリーンアップサービスをスケジュールできます。

Caution

アーティファクトがパージされると、そのアーティファクトはApplication Securityから完全に削除され、復元できなくなります。

データ保持を有効にすると、Application Securityはすべてのアプリケーションにデフォルトのデータ保持ポリシーを適用します。また、デフォルトのデータ保持ポリシーからオプトアウトする個々のアプリケーションのバージョンを設定することもできます。

このセクションでは、次のトピックについて説明します。

1.6.24.1. データ保持の有効化

Fortify Application Securityのデータ保持ポリシーを有効化するには:

1. 管理者としてサインインし、［**管理**］をクリックします。
2. ナビゲーションペインで、［**ポリシー(Policies)**］を展開し、［**データ保持ポリシー(Data Retention Policy)**］を選択します。

   ［**データ保持(Data Retention)**］ページに、デフォルトのデータ保持ポリシーと、データ保持ポリシーが適用されていないアプリケーションバージョンが一覧表示されます。
3. 次の表で説明するように、［**データ保持(Data Retention)**］ページで設定を行います。

フィールド	説明
データ保持ポリシーを有効にする (Enable Data Retention Policy)	このチェックボックスをオンにすると、データ保持機能が有効になります。
アプリケーションバージョンに、デフォルトポリシーのオプトアウトを許可する(Allow application versions to opt-out of the default policy)	このチェックボックスをオンにすると、個々のアプリケーションバージョンでデフォルトポリシーをオプトアウトできます。

フィールド	説明
曜日(Days of the week)	(必須)データクリーンアップサービスを実行する曜日を1つ以上指定します。 `1`から`7`までの値を使用して曜日(日曜日から土曜日)を指定します。ここで、`1`は日曜日を表し、`7`は土曜日を表します。 cron構文を使用して、次の例で説明するように曜日を1つ以上指定します。 ◦ 1つの曜日—週に1回だけデータクリーンアップサービスを実行するには、1桁の数字を入力します。 たとえば、`3`と入力すると、火曜日にのみ、［**時間(Hours)**］ボックスで指定された時刻にデータクリーンアップサービスが実行されます。 ◦ 複数の曜日—週に数回データクリーンアップサービスを実行するには、エントリをカンマで区切ります。 たとえば、`1,4,6`と入力すると、日曜日、水曜日、金曜日に、［**時間(Hours)**］ボックスで指定された時刻にデータクリーンアップサービスが実行されます。 ◦ 曜日の範囲—連続する曜日を入力するには、エントリをダッシュで分離します。たとえば、`2-6`と入力すると、月曜日から金曜日に、［**時間(Hours)**］ボックスで指定された時刻にデータクリーンアップサービスが実行されます。

フィールド	説明
	◦ 毎日—アスタリスク(*)を入力すると、毎日、［**時間(Hours)**］ボックスで指定された時刻にデータクリーンアップサービスがスケジュールされます。 **Note** OpenTextでは、システム応答性への影響を最小限に抑えるために、システムがアイドル状態の場合にのみデータクリーンアップサービスを有効にすることを強く推奨しています。

フィールド	説明
Hours	(必須)データクリーンアップサービスを実行する時刻を入力します。 `0` から `23` までの値を使用して、24時間表記で時刻を指定します。ここで、`0` は午前0時を表し、`23` は午後11時を表します。 cron構文を使用して、次の例で説明するように時刻を1つ以上指定します。 ◦ 1つの時刻—特定の時刻に1回だけデータクリーンアップサービスを実行するには、1桁の数字を入力します。 たとえば、`3` と入力すると、［**曜日(Days of the week)**］ボックスで指定された曜日の午前3時から午前3時59分までの間にデータクリーンアップサービスが実行されます。 ◦ 複数の時刻—1日に数回データクリーンアップサービスを実行するには、各時刻をカンマで区切ります。 たとえば、`4,18` と入力すると、［**曜日(Days of the week)**］ボックスで指定された曜日の午前4時から午前4時59分までの間と、午後6時から午後6時59分までの間にデータクリーンアップサービスが実行されます。 ◦ 時間帯—1日の特定の時間帯にデータクリーンアップサービスを実行するには、エントリをダッシュで分離します。

フィールド	説明
	たとえば、`3-6`と入力すると(`3,4,5,6`と同等)、［**曜日(Days of the week)**］ボックスで指定された曜日の午前3時から午前6:59までの間にデータクリーンアップサービスが実行されます。 ◦ 1日の複数の時間帯にデータクリーンアップサービスを実行するには、複数の範囲または値をカンマで区切ります。 たとえば、`3-5,17-19`と入力すると、［**曜日(Days of the week)**］ボックスで指定された曜日の午前3時から午前5時59分までの間と、午後5自から午後7時59分までの間にデータクリーンアップサービスが実行されます。 ◦ 毎時: アスタリスク(`*`)を入力すると、［**曜日(Days of the week)**］フィールドで定義された指定日の1時間おきに、データクリーンアップサービスがスケジュールされます。

フィールド	説明
	Note OpenTextでは、システム応答性への影響を最小限に抑えるために、システムがアイドル状態の場合にのみデータクリーンアップサービスを有効にすることを強く推奨しています。また、サービスを午後10時から午前3時(cron構文では値 `22`、`23`、`0`、`1`、および `2` に対応)にスケジュールすることは避けてください。これは、夜間に実行されるApplication Securityの他の保守ジョブは、デフォルトでこの時間帯に設定されるためです。

4. ［**保存(SAVE)**］をクリックします。

参照情報

デフォルトのデータ保持ポリシーの編集

1.6.24.2. デフォルトのデータ保持ポリシーの編集

OpenTextでは、初めてデータ保持ポリシーを有効にする際は、ポリシーのプロパティを最大許容値のままにすることを推奨しています。これは、ポリシーがアーティファクトの削除を指示し始める前に、個々のアプリケーションバージョンでポリシーをオプトアウトできるよう、時間の余裕を設けるためです。独自の要件に基づいて、デフォルトのデータ保持ポリシーを編集できます。

デフォルトのデータ保持ポリシーでのアーティファクトのパージは、次の2つのルールに依存します。

- ルール1—アーティファクトの数>未パージのアーティファクトの最大数、かつ、アーティファクトの存続期間>アーティファクトの最小存続期間
- ルール2—存続期間>最大存続期間、かつ、アーティファクトの数>未パージのアーティファクトの最小数

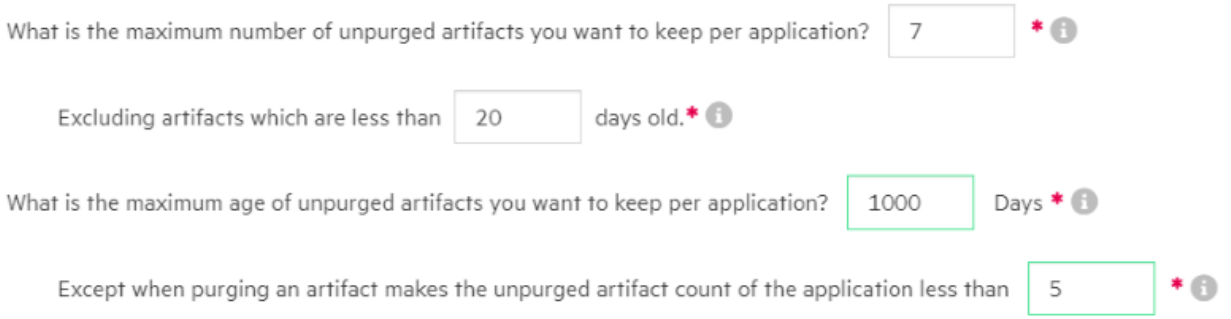
データ保持ポリシーのガイドラインは分析タイプごとに評価され、アーティファクトがパージの対象となるには、少なくともルールのうち1つを満たす必要があります。どちらのルールも満たされない場合、指定したアーティファクトの最大数や最大存続期間に関係なく、アーティファクトは保持されます。

デフォルトのデータ保持ポリシーを編集するには:

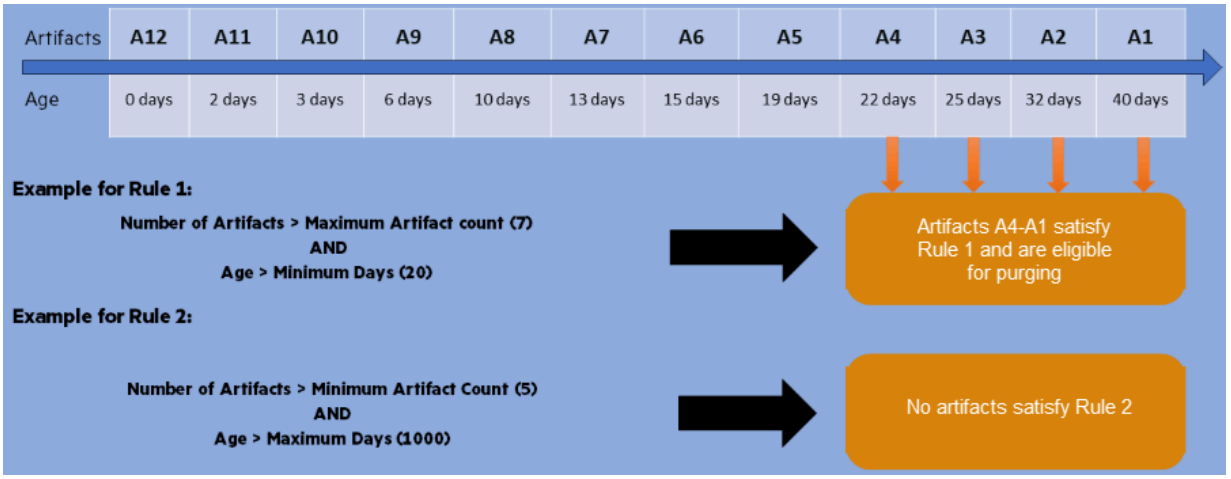
1. 管理者としてサインインし、［**管理**］をクリックします。
2. ナビゲーションペインで、［**ポリシー(Policies)**］を展開し、［**データ保持ポリシー(Data Retention Policy)**］を選択します。
3. ［**データ保持(Data Retention)**］ページで、［**デフォルトのデータ保持ポリシー(Default data retention policy)**］の横にある［**ポリシーの編集(Edit Policy)**］ボタン🖊をクリックします。
4. ［**ポリシーの編集(Edit Policy)**］ダイアログボックスで、要件に基づいて次の設定を行います。

   シナリオの例:

   12のアーティファクトを含むアプリケーションバージョンでデータ保持ポリシーが有効であり、デフォルトのデータ保持ポリシーに次の値が設定されています。



次の図は、このシナリオで、デフォルトのデータ保持ポリシーによってアーティファクトがどのようにパージ対象となるかを示しています。



Application Securityは、少なくとも1つのルールを満たすアーティファクトをパージします。Application SecurityはA1からA4のアーティファクトをパージします。

5. ［**保存(SAVE)**］をクリックします。

1.6.25. 安全なブラウザアクセスの設定

Application Securityドメインにアクセスするブラウザのセキュリティを設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**セキュリティ(Security)**］を選択します。
3. ［**セキュリティ(Security)**］ページで、次の表の説明に従って設定を行います。

フィールド	説明
Content-Security-Policy	使用するCSPのレベル(必要な場合)を指定します。HTTP Content-Security-Policyヘッダを使用して、ブラウザがロードできるリソース、およびApplication Securityからロードされたページで実行できるアクションを制御します。これは、クロスサイトスクリプティング(XSS)攻撃から保護するのに役立ちます。 次のいずれかのオプションを選択します。 ◦ `host.url` プロパティで(セットアップウィザードを使用して)設定されたベースURLにのみアクセスを制限するには、［**厳密(Strict)**］を選択します。 ◦ 厳密なCSPよりも制限の厳しいポリシーを有効にするには、［**Relaxed**］を選択します。これはデフォルト設定です。任意のホスト:ポートからApplication Securityドメインにアクセスできます。 ◦ Content-Security-Policyヘッダを無効にするには、［**Disabled**］を選択します。OpenTextでは、Content-Security-Policyヘッダを無効にすることを推奨していますが、CSPが予期しない問題を引き起こす場合は、このオプションを使用できます。

フィールド	説明
Set value for Strict-Transport-Security header	Strict-Transport-Securityヘッダの値を入力します。このヘッダは、HTTPの代わりにHTTPSを使用してApplication Securityと通信するよう、ブラウザに指示します。 **Important** この値は、慎重に設定してください。ユーザに重大な影響を与える可能性があります。詳細については、「HTTP Strict Transport Security Cheat Sheet」を参照してください。 Strict-Transport-Securityヘッダは、Tomcatサーバによって決定される安全なチャネルを介してのみ送信されます。

フィールド	説明
Set value for Public-Key-Pins header	Public-Key-Pinsヘッダの値を入力します。これにより、中間者(MITM)攻撃のリスクが減少します。 **Important** この値は、慎重に設定してください。ユーザに重大な影響を与える可能性があります。詳細については、「HTTP Strict Transport Security Cheat Sheet」を参照してください。 Public-Key-Pinsヘッダは、Tomcatサーバによって決定された安全なチャネルを介してのみ送信されます。

4. ［**保存(SAVE)**］をクリックします。

1.6.26. シングルサインオンを使用するためのApplication Securityの設定について

次の表に、サポート対象のシングルサインオンソリューションと、これらのシングルサインオンソリューションと連携するようにApplication Securityを設定する手順へのリンクを記載します。

SSOソリューション	手順
SAML 2.0準拠のシングルサインオン	SAML 2.0準拠のシングルサインオンを使用するためのApplication Securityの設定
HTTPヘッダ	HTTPヘッダを使用するシングルサインオンおよびシングルログアウトソリューションを使用するためのApplication Securityの設定
X.509証明書	X.509証明書ベースのSSOを使用するためのApplication Securityの設定

環境設定に関する制限事項

SSOソリューションと連携するようにApplication Securityを設定する際には、次の制限が適用されます。

- ユーザがSSOでユーザインタフェースにアクセスできるようにするには、Application Securityがサポートしているソリューションのみを使用できます。
- どの時点でも、Application Securityで使用するSSOソリューションを1つしか設定できません。
- Fortify Audit Workbench、fortifyclient、またはいずれかのSecure Code Pluginsにアクセスするユーザは、LDAPまたはローカルのApplication Securityユーザアカウントとパスワードを使用してサインインする必要があります。
- (X.509 SSOソリューションのみ)ローカルまたはLDAPのユーザが各自のユーザ名とパスワードを使用してサインインできるようにするには、こうしたサインインを直接有効にする必要があります。

アプリケーションのセキュリティを向上させるために、X.509 SSO認証が有効になっている場合、Application SecurityはLDAPユーザとローカルユーザの両方に対し、ユーザ名とパスワードを使用したローカルでのログインを許可しません。ユーザはApplication Securityにアクセスするために、設定されたSSO方式またはAPIトークンのみを使用できます。X.509 SSOソリューションを設定したローカルログインを有効にするには、管理者が `sso.localAuthenticationEnabled` プロパティ(`app.properties` ファイル内)を使用する必要があります。詳細については、「X.509証明書ベースのSSOを使用するためのApplication Securityの設定」を参照してください。

参照情報

セッションログアウトについて

1.6.26.1. SAML 2.0準拠のシングルサインオンの設定

Application SecurityをSAML 2.0シングルサインオンで動作するように設定する前に、次の点に注意してください。

- Application Securityは、インバウンドおよびアウトバウンドのSAMLメッセージに対するHTTP REDIRECTおよびHTTP POSTバインディングをサポートしています。
- Application SecurityではSAMLのシングルログアウトがサポートされています。IdPによって送信されるログアウト応答およびログアウト要求は、必ず署名されている必要があります。
- SAMLを正常に統合するには、クライアントマシンとサーバマシン(IdPとSP)のクロックを同期する必要があります。

Note
アイデンティティプロバイダー(例: Okta)を削除または置換する前に、まずApplication Securityからユーザを削除してください。

SAML 2.0を使用するSSOが動作するようApplication Securityを設定するには、次の手順に従います。

1. Application SecurityのユーザおよびIdPにLDAPディレクトリを使用している場合は、LDAP認証を使用するようにApplication Securityを設定します。それ以外の場合、IdPユーザはローカルユーザと一致する必要があります。詳細については、「LDAPユーザ認証」を参照してください。
2. IDPをSSL(https)で実行する場合は、SSLを使って実行するようにApplication Securityを設定します。そうしないと、IdPに対する認証中のプロトコル切り替えが認証に干渉する可能性があります。
3. SAMLメッセージのデジタル署名とSAMLアサーションの暗号化に使用する公開鍵/秘密鍵のペアを用意します。IdPが特定の認証局によって署名された鍵を必要としない場合は、OpenSSLやJavaのkeytoolなどを使用して、独自の自己署名鍵を生成できます。次のコマンド例では、特定のエイリアスの下に自己署名鍵を格納するキーストアを生成します。

```
keytool -genkeypair -alias <key_alias> -keyalg <RSA_or_EC
algorithm> -keystore <keystore_filename> -storepass
<password_to_protect_keystore> -keypass
<password_to_protect_key> -validity
<number_of_days_the_key_is_valid>
```

エイリアスと両方のパスワードの値をメモしておきます。後で、Application Securityの［管理］ビューでこれらの値を指定する必要があります。

4. IdPサーバからSAMLメタデータを取得し、それをApplication Securityファイルシステムに保存します。
5. メタデータファイルを開き、IdP EntityDescriptorのエンティティIDをメモします(<EntityDescriptor entityID="THE_VALUE_YOU_ARE_LOOKING_FOR">)。

   メタデータが署名されているかどうかを確認します(［Signature］セクションが存在します)。メタデータが署名されている場合、署名はPKIX検証アルゴリズムで検証され、キーストアに存在する公開鍵はすべてトラストアンカーとして使用されます。

   キーストアに、署名のルートCA証明書と中間CA証明書が含まれていることを確認します。
6. Application Securityにサインインし、ヘッダで［**管理(Administration)**］を選択します。
7. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**SSO**］を選択します。

   1度に設定できるシングルサインオンソリューションは1つのみです。
8. ［**有効なSSO(Enabled SSO)**］リストから、［**SAML**］を選択します。
9. 次の表に示す情報を指定します。

フィールド	説明

IdP metadata location	識別情報プロバイダメタデータ(ステップ4で取得したメタデータ)の場所。
	例
	◦ Windowsシステムの場合:
	`file:///C:/fortify/federation-metadata.xml`
	◦ Linuxシステムの場合:
	`file:///home/fortify/federation-metadata.xml`
	Note
	Entra IDと統合している場合は、Azureの［**アプリのフェデレーションメタデータURL (App Federation Metadata Url)**］フィールドに表示される値を入力します。(Azureの左側のペインの［**管理(Manage)**］で、［**Single Sign-on**］を選択し、［**SAML**］を選択します。
	［**SAML Signing Certificate**］の［**App Federation Metadata Url**］フィールドが表示されます)。

フィールド	説明
	Note IdPがプロキシサーバの背後にある場合は、IdPメタデータをローカルのシステムにダウンロードし、ローカルで参照する必要があります。現在のSAML実装では、httpプロキシを使用したメタデータの取得はサポートされていません。
Default IdP	IdP EntityDescriptorのエンティティID(IdPメタデータから) **Note** SCIMプロトコルを使用して、Entra IDからのユーザデータでApplication Securityをプロビジョニングする場合は、Entra IDの［**Azure AD識別子(Azure AD Identifier)**］フィールドに示されている値を使用します(このフィールドは、SAMLベースのサインオンページの［**<アプリケーション名>の設定(Set up *<application_name>*)**］で確認できます)。

フィールド	説明
SP entity ID	サービスプロバイダエンティティIDの値は、1024文字を超えないURLで、フェデレーション全体でグローバルに一意である必要があります。OpenTextでは、実行中のApplication Securityインスタンスの URLを使用することを推奨しています。
SP エイリアス	サービスプロバイダのエイリアスには、英数字、コロン、ダッシュ、およびアンダースコアのみを含める必要があります。スラッシュ、ハッシュマーク、セミコロン、または疑問符は使用できません。 このフィールド値は重要な役割を果たさないので、一般的な値を指定できます。たとえば、`fortify_ssc`を使用できます。

フィールド	説明
キーストアの場所(Keystore location)	SAMLメッセージの署名とSAMLアサーションの暗号化に使用される鍵のペアを格納しているキーストアの場所。 例: ◦ Windowsの場合: `file:///C:/fortify/keystore.jks` ◦ Linuxの場合: `file:///home/fortify/keystore.jks` **Note** IdPメタデータが署名されている場合、署名はPKIX検証アルゴリズムで検証され、キーストアに存在する公開鍵はすべてトラストアンカーとして使用されます。キーストアに、署名のルートCA証明書と中間CA証明書が含まれていることを確認します。
キーストアパスワード(Keystore password)	キーストアファイルのパスワード
署名および暗号化キー(Signing & encryption key)	キーストアファイル内の署名/暗号化キーのエイリアス
署名および暗号化キーのパスワード(Signing & encryption key password)	署名/暗号化キーパスワード

フィールド	説明
SAML name identifier	IdPによって送信されるSAMLアサーションに含まれる、認証済みユーザのユーザ名を保持する要素の名前。Application Securityユーザのユーザ名に一致します。ユーザ名が*<NameID>*要素内でリリースされている場合は、NameID値を使用します。ユーザ名がいずれかの*<Attribute>*要素内でリリースされている場合は、その属性の名前の値を指定します。この情報は、使用しているIdPサーバで使用可能または設定可能である必要があります。

10. ［**保存(SAVE)**］をクリックします。

> **Note**
> メタデータを生成した後(つまり、ステップ15の後)、［**IdPメタデータ署名の検証を有効にする(Enable IdP metadata signature verification)**］チェックボックスをオンにします。

11. `host.url` の `<fortify.home>/<app_context>/conf/app.properties` プロパティでIdPサーバがアクセスできるURLを指定していることを確認します。

    このURLは、Application Security SAMLメタデータで*<AssertionConsumerService>*および*<SingleLogoutService>*の場所を構成するためのベースURLとして使用されます。

12. IdPから送信されるSAMLアサーションが暗号化されている場合は、認証応答メッセージが署名されている必要があります。

> **Important**
>
> Active Directoryフェデレーションサービス(AD FS)と統合する場合は、IdPパラメータ `SamlResponseSignature` の値を `MessageAndAssertion` (推奨)または `MessageOnly` に設定します。

13. 最近のGoogle Chrome™またはChromiumベースのブラウザでは、クッキーポリシーがデフォルトで `SameSite=Lax` に設定されています。つまり、クッキーはサードパーティサイトへのサブリクエストでは送信されません。つまり、クッキーはサードパーティサイトへのサブリクエストでは送信されません。

    > **Note**
    >
    > Application Securityから開始されたシングルログアウトは、クッキーポリシー設定に関係なく正しく動作します。

    ChromeまたはChromiumベースのブラウザでシングルログアウトを機能させるには、セッションクッキーの `SameSite` ポリシーを `None` に変更する必要があります。

    > **Important**
    >
    > これはデフォルトよりもセキュリティ保護の弱いポリシーであることを意味します。したがって、そのように変更することが組織にとって最適なアプローチかどうかを判断する必要があります。コンテナのデプロイポリシーを変更するには、 `HTTP_SERVER_SAME_SITE_COOKIES` 環境変数を使用します。コンテナ以外の展開の場合は、Tomcat設定のcontextセクションに `<CookieProcessor sameSiteCookies="none"/>` を追加します。詳細については、『Apache Tomcat 10 Configuration Reference』ドキュメントを参照してください。

14. Application Securityを再起動します。
15. `<hostname>:<port>/<app_context>/saml/metadata/<SP_alias>` でApplication Security(SP)メタデータを生成します 。
16. IdPメタデータが署名されている場合(<Signature>セクションが存在する場合)に限り(手順5を参照)、次の手順に従います。それ以外の場合はステップ17に進みます。
    1. Application Securityで［**SSO**］設定ページに移動し、IdP提供の公開鍵(X.509証明書)を使用してIdPメタデータ署名を検証するために、［**IdPメタデータ署名の検証を有効にする(Enable IdP metadata signature verification)**］チェックボックスをオンにします。
    2. ［**保存(SAVE)**］をクリックします。
    3. Application Securityを再起動します。
17. 前のステップ(ステップ15)で生成されたメタデータを開き、`<AssertionConsumerService>` および `<SingleLogoutService>` に含まれるロケー

ションのURLにIdPサーバからアクセス可能であることを確認します。

18. Application SecurityメタデータをIDPサーバにアップロードします。
19. `<hostname>:<port>/<app_context>` へのアクセスを試みます。

IdPサーバにリダイレクトされ、資格情報を入力できます。認証に成功すると、IdPサーバからApplication Securityにリダイレクトされます。

Note

SSO認証に関連するログ記録情報を取得する方法については、「シングルサインオン認証のデバッグログ記録を有効にする」を参照してください。

1.6.26.1.1. SAML SSO統合のトラブルシューティング

問題: *<hostname>*:*<port>*/*<app-context>*/login.jsp ページにアクセスした後、ユーザがIdPにリダイレクトされません。

- ログインページはSSOから除外され、ローカル管理者がアプリケーションにアクセスし、SAML SSO設定を修正できます。

問題: ユーザはIdPで認証されますが、 Application Securityで認証されません。

- IdPからSAMLアサーションで受信したユーザ名は、どのLDAPユーザアカウントまたはローカルのApplication Securityユーザアカウントとも一致しません(ユーザルックアップ戦略に基づく)。次の情報を確認します。
  - Application Security SAML設定の「SAML name identifier」は、ユーザ名を含むS SAMLアサーション内の属性に設定されます。
  - ユーザがApplication Security内に存在し、役割が割り当てられています。
  - ユーザルックアップ戦略が正しく設定されています(「コア設定の設定」を参照)。

問題: IdPメタデータをローカルで参照するのではなく、IdPメタデータの場所をHTTP URLとして設定したい。

- 設定ではHTTPの場所を受け入れますが、IdPをプロキシサーバの背後に置くことはできません。IdPがプロキシサーバの背後にある場合、Application Securityがメタデータにアクセスできないので、データはローカルで参照する必要があります。

参照情報

HTTPヘッダを使用するシングルサインオンおよびシングルログアウトソリューションを使用するためのApplication Securityの設定

1.6.26.2. HTTPヘッダを使用するシングルサインオンおよびシングルログアウトソリューションの設定

ヘッダを使用するSSOを使用するためにApplication Securityを設定するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**SSO**］を選択します。

   1度に設定できるシングルサインオンソリューションは1つのみです。
3. ［**有効なSSO(Enabled SSO)**］リストから、［**HTTP**］を選択します。
4. 次の表に示す情報を指定します。

フィールド	説明
HTTP header for username	SSOログオンに使用するHTTPヘッダを入力します。 デフォルト値は*username*です。
IdP login page	識別情報プロバイダのログインページのURLを入力します。
SSO Logout page	Application Securityからログアウトしたユーザのリダイレクト先とするログアウトページのアドレスを入力します。
SSO Logout Response Header	動的ディレクティブヘッダを入力します。
SSO Logout Response Code	動的ディレクティブコードを入力します。
SSOログアウト応答テキスト (SSO Logout Response Text)	動的ディレクティブメッセージを入力します。

5. ［**保存(SAVE)**］をクリックします。
6. LDAP認証を使用するようにApplication Securityを設定します。

   詳細については、「LDAPユーザ認証」を参照してください。
7. サーバを再起動します。

Note

SSO認証に関連するログ記録情報を取得する方法については、「シングルサインオン認証のデバッグログ記録を有効にする」を参照してください。

参照情報

シングルサインオンを使用するためのApplication Securityの設定

1.6.26.3. X.509証明書ベースのシングルサインオンの設定

X.509証明書ベースのSSOを使用するようにApplication Securityを設定するには、次の手順を実行します。

1. TomcatでX.509クライアント証明書を設定します。

   certificateVerificationおよび関連オプションの詳細については、Apache Tomcatのドキュメントを参照してください。

2. 管理者としてApplication Securityにサインインします。
3. ヘッダで、［**管理(Administration)**］を選択します。
4. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**SSO**］をクリックします。

   1度に設定できるシングルサインオンソリューションは1つのみです。

5. ［**有効なSSO(Enabled SSO)**］リストから、［**X.509**］を選択します。
6. ［**X.509認定ユーザ名パターン(X.509 certificate username pattern)**］ボックスに、Application Securityでクライアント証明書からユーザ名を取得する方法を指定するための正規表現を入力してから、次のいずれかの操作を行います。

   - X.509認定の［サブジェクト(Subject)］フィールドからユーザ名を取得するには、キャプチャグループを含む正規表現を使用します。そのあとで、この正規表現を［サブジェクト(Subject)］フィールド値のユーザ名と一致させるために使用します。

     例:証明書の［サブジェクト(Subject)］フィールドのCN属性と一致させるには、`CN=(.*?)`パターンを指定します。

   - X.509認定のサブジェクト代替名(SAN)拡張の［その他の名前(Other Name)］からユーザ名を取得するには、`$0!OID$regex`パターンを使用します。ここで、

     - `OID`は、ユーザ名を取得するその他の名前の識別子を表します。文字列値を含むその他の名前だけがサポートされます。
     - `regex`は、その他の名前の値からユーザ名を取得するために使用するキャプチャグループを含む正規表現を表します。

     例: 広く使用されているSANのその他の名前の1つは、ユーザプリンシパル名(UPN)です (`OID1.3.6.1.4.1.311.20.2.3`)。その値は、`username@domain`とい

う形式になります。

UPNに含まれる `username@domain` 全体と一致させるには、次のパターンを入力します。

```
$0!1.3.6.1.4.1.311.20.2.3$(\S+@\S+)
```

UPNに含まれる `@` 記号の前のユーザ名のみ(ドメイン名は除外)と一致させるには、次のパターンを入力します。

```
$0!1.3.6.1.4.1.311.20.2.3$(.+?(?=@))
```

7. ［**保存(SAVE)**］をクリックします。
8. 設定を実装するには、Application Securityサーバを再起動します。

Important

X.509証明書ベースのSSOを使用するように設定した場合、ローカルおよびLDAPのユーザがユーザ名とパスワードを使用してサインインできるようにするには、こうしたサインインを直接有効にする必要があります。

X.509 SSOを設定した場合にユーザ名とパスワードによるログインを有効にするには:

1. テキストエディタで `<fortify.home>/<app_context>/conf/app.properties` ファイルを開きます。
2. `sso.localAuthenticationEnabled` プロパティを `true` に設定します。
3. `app.properties` ファイルを保存して閉じます。
4. サーバを再起動します。

1.6.26.4. シングルサインオン認証のデバッグログ記録を有効にする

Application Security のシングルサインオン(SSO)認証に関連する追加のログ記録情報を取得したい場合は、ログ記録設定を更新します。

SSO認証に関連する追加のログ記録情報を取得するには:

1. テキストエディタで *<fortify.home>*/*<app_context>*/conf/log4j2.xml ファイルを開きます。
2. HTTPヘッダを使用するSSOソリューションの場合は、次のロガー定義を log4j2.xml ファイルに追加します。

```
 <Logger
name="com.fortify.manager.web.security.auth.FmHttpSsoAuthent
icationFilter" level="debug"/>
```

3. SAML 2.0準拠のSSOソリューションの場合は、 <!-- SSO SAML --> でマークされたセクションを見つけて、そのセクションで各ロガーのレベルを適切なデバッグ値に変更します。

参照情報

シングルサインオンを使用するためのApplication Securityの設定

1.6.27. ログ記録の設定

Application Securityのログ記録サービスには、Apache Log4j™ 2が使用されます。ログ記録の設定は、 *<fortify.home>/<app_context>*/conf/log4j2.xml ファイル内にあります。

Important

log4j2.xml ファイルはApplication Securityによって管理されるため、Application Securityの再起動またはアップグレード時に上書きされる可能性があります。設定を永続的に変更する場合は、このファイルを使用しないでください。

Application Securityの実行中に、この環境設定ファイルに加えられた変更は、約10秒(設定に含まれる monitorInterval 属性の値によって定義された時間)以内に適用されます。環境設定ファイルに新しいロガーを追加して、そのレベルを設定することはできません。既存のロガーに対する変更だけが動的に選び出されます。

永続的なログ記録の設定変更を実装するには、カスタムのLog4j2環境設定上書きファイルを設定します。環境設定上書きファイルを変更した後、Application Securityを再起動しない場合も、前述のメインの環境設定ファイルと同じルールが適用されます。付属の log4j2.xml ファイルに含まれる設定と、カスタムのLog4j2環境設定上書きファイルがマージされます。競合が発生した場合は、環境設定上書きファイルが優先されます。

カスタムのログ4j2環境設定上書きファイルを作成するには:

1. メインの log4j2.xml ファイルをコピーして、環境設定上書きファイルを作成します。
2. 環境設定上書きファイルに変更を加えます。

   環境設定上書きファイルに新しいアペンダまたはロガーを追加し、既存のものを変更できます。

   カスタムの環境設定上書きファイルは、メインの環境設定ファイルと同じファイル形式を使用します。
3. COM_FORTIFY_SSC_LOG4J2_OVERRIDEシステム環境変数または com.fortify.ssc.log4j2.override JVMシステムプロパティを、カスタムLog4j2環境設定ファイルの絶対パスに設定します。

1.6.28. 連邦情報処理標準(FIPS)環境での実行

FIPSは、米国政府などの組織で使用される暗号化モジュールおよびアルゴリズムに関する一連の標準およびガイドラインです。FIPSに準拠するとは、FIPSのドキュメントで定義されている最小限のセキュリティ要件を満たすことを意味します。Application Securityは、Red Hat Enterprise Linux 9 (RHEL 9)上で実行されているFIPS準拠環境で実行できます。Application SecurityをFIPS環境で実行するために必要な設定はありませんが、LDAPサーバ、SMTPサーバ、およびWebhookがセキュリティ保護された接続として設定されていることを確認する必要があります。セキュリティ保護された接続として設定されていない場合、Application Securityでエラーが発生します。

FIPSに準拠した暗号化の設定方法については、RHEL 9のドキュメントを参照してください。

Application SecurityをFIPS環境で実行する前に、次の点を確認してください。

- Application Securityバージョン24.4.0以降を使用していること。そうでない場合は、重要なデータを暗号化するために、`secret.key`ファイルが格納されているApplication Securityキーストアを移行する必要があります。

  詳細については、「<fortify.home>ディレクトリについて」を参照してください。

- LDAPサーバ、SMTPサーバ、およびWebhookがセキュリティ保護された接続として設定されていること。

Note

Application Securityコンテナは、Javaに対するFIPSモードの有効化をサポートしていません。

1.6.29. Application Securityのサインインに必要なパスワード強度の設定

password.strength.min.score プロパティ (*<fortify.home>*/*<app_context>*/conf/app.properties にある)を使用して、必要なパスワード強度を調整できます。次の表に、有効なプロパティ値とそれぞれの値が表す強度を記載します。

値	パスワード強度
0	非常に弱い
1	弱い
2	Medium
3	強い
4	非常に強い

パスワードの強度は、専用のパスワード強度ライブラリに基づいて計算されます。このライブラリでは、パスワードを破るまでの時間の見積もり、予測可能な文字シーケンスやユーザ名がパスワードに含まれていないかどうかの判定、一般的なパスワード辞書の照合などの方法を適用します。

参照情報

セッションログアウトについて

追加のApplication Security設定

1.6.30. 監査の問題履歴について

監査対象として新しいスキャンをアップロードする際に、問題の属性の変更を確認できます。問題履歴には、属性値に加えられたすべての変更と、それぞれの変更が行われた日時が一覧表示されます。

問題履歴には、Application Securityがアップロードされたスキャンから抽出したすべての属性が含まれます。問題履歴には、［**監査(AUDIT)**］ページでの検索またはフィルタ処理に使用できる属性のみが含まれます。

監査の問題履歴を有効にするには、「監査の問題履歴を有効にする」を参照してください。

［**問題履歴(Issue History)**］タブは、次の問題属性に関する情報を提供します。

問題屬性		
analyzer	issueInstanceId	remediation_effort
accuracy	kingdom	rule
audience	likelihood	severity
category	line	sink
class	manual	source
codesnippet	mapped_category	sourcefile
confidence	min_virtual_call_confidence	sourceline
engine_priority	package	source_context
file	primary_context	taint
impact	probability	url

Note

- 監査の問題履歴を有効にすると、Application Securityが、新しくアップロードされたFPRで値が変更された属性と、その以前の値および新しい値のリストを保存するようになります。
- アプリケーションバージョンで最新のアップロードスキャンよりも古いスキャンをアップロードした場合、問題履歴に保存される新しい変更エントリが生成されることはありません。
- アプリケーションバージョンからFPRを削除すると、そのFPRのアップロードによって作成された問題履歴エントリが削除されます。
- アプリケーションバージョンをコピーしても、そのコピーには既存の問題履歴は含まれません。

参照情報

スキャン結果の監査

1.6.30.1. 監査の問題履歴を有効にする

監査の問題履歴を有効にするには:

1. テキストエディタで *<fortify.home>*/*<app_context>*/conf/app.properties ファイルを開きます。
2. issue.attrChangelog.enabled プロパティの値を true に設定します。
3. app.properties ファイルを保存して閉じます。
4. Application Securityサーバを再起動します。

Note

Application Securitvの自動設定で監査の問題履歴を有効にすることもできます。自動設定は、 app.properties ファイルに対して行った変更を上書きします。手順については、「Application Securityの設定の自動化」を参照してください。

参照情報

監査の問題履歴

1.7. 追加のインストール関連タスク

このセクションでは、新しいApplication Securityのインストールに関連する追加タスクについて説明します。

このセクションでは、次のトピックについて説明します。

1.7.1. バグトラッキングシステムの統合について

チームは問題の監査中にバグトラッキングシステムにバグを送信できます。Application Securityでは、次のバグトラッキングシステムとの統合をサポートしています。

- OpenText™ ALM Quality Center
- Azure DevOps Server

  Important

  - Azure DevOpsの［**再現手順(Repro Steps)**］フィールドにはバグの説明が表示されますが、デフォルトで、このフィールドは問題の作業項目で非表示になっています。Azure DevOps 2019.1以降のバージョンを使用し、かつ基本プロセスを使用する場合は、問題の作業項目をカスタマイズして［**再現手順(Repro Steps)**］フィールドを表示する必要があります。
  - ログイン時に［**パスワード(Password)**］ボックスで、Azure DevOpsが生成した個人用アクセストークンを使用する必要があります。個人用アクセストークンの詳細については、Microsoft Azure DevOps Servicesのドキュメントを参照してください。

- Jira Software Server
- Jira Software Cloud

  ログイン時に［**パスワード(Password)**］ボックスでJira認証トークンを使用する必要があります。

組織で、OpenTextが提供する以外のバグトラッキングシステムを使用している場合は、そのシステム用の新しいプラグインを作成できます。手順については、バグトラッカプラグインの作成を参照してください。

バグトラッキングシステムを設定して使用して、アプリケーションバージョンのセキュリティ脆弱性を管理する方法については、「セキュリティ脆弱性の管理にバグトラッキングシステムを利用する」を参照してください。

1.7.1.1. バグトラッカプラグインの追加

管理者は、Application Securityをサードパーティ製のバグトラッカプラグインに接続できます。

Important

認証およびHTTPSバグトラッカドメインを持つプロキシは使用できません。接続を正常に行うには、次のいずれかを使用します。

- 認証ありのプロキシとhttp://bugtracker.domain.com
- 認証なしのプロキシとhttps://bugtracker.domain.com
- 認証なしのプロキシとhttp://bugtracker.domain.com

バグトラッカプラグインをシステムに追加するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**プラグイン(Plugins)**］を展開し、［**バグトラッカプラグイン(Bug Tracking Plugins)**］を選択します。
3. ［**バグトラッキング(Bug Tracking)**］ページで、［**新規(New)**］をクリックします。
4. プラグインをアップロードするリスクを受け入れるには、［**OK**］をクリックします。
5. ［**プラグインバンドルのアップロード(UPLOAD PLUGIN BUNDLE)**］ダイアログボックスで、［**参照(BROWSE)**］をクリックし、プラグインのJARファイルを見つけて選択します。

   Application Securityが提供するJARファイル、または自分で作成したバグトラッカプラグイン用のJARファイルのいずれかを使用できます。

   バグトラッカ用に用意されているJARファイルは、次の場所に保存されています。

バグトラッカプラグイン	JARファイル
ALM用バグトラッカプラグイン	`<ssc_distribution_dir>/plugins/BugTrackerPluginAlm/com.fortify.BugTrackerPluginAlm-<version>.jar`
Azure DevOps用バグトラッカプラグイン	`<ssc_distribution_dir>/plugins/BugTrackerPluginAzure/com.fortify.BugTrackerPluginAzure-<version>.jar`
Jira用バグトラッカプラグイン	`<ssc_distribution_dir>/plugins/BugTrackerPluginJira/com.fortify.BugTrackerPluginJira-<version>.jar`

6. ［**アップロードの開始(START UPLOAD)**］をクリックします。

   アップロードが完了すると、［Bug Tracking］テーブルに新しいプラグインが一覧表示されます。

7. バグトラッカプラグインを有効にするには、［**ENABLE**］をクリックします。

プラグインの［**Plugin State**］フィールドに値［**ENABLED**］が表示されます。

参照情報

バグトラッカプラグインの作成

アプリケーションバージョンへのバグトラッキングシステムの割り当て

1.7.1.2. バグトラッカプラグインの削除

管理者は、サードパーティ製のバグトラッカプラグインをシステムから削除できます。

システムからバグトラッカプラグインを削除するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**プラグイン(Plugins)**］を展開し、［**バグトラッカプラグイン(Bug Tracking Plugins)**］を選択します。
3. ［**バグトラッキング(Bug Tracking)**］ページで、削除するプラグインの行を展開します。
4. ［**無効にする(Disable)**］をクリックし、プラグインが無効になった後で［**削除(REMOVE)**］をクリックします。

次も参照

バグトラッキングシステムの統合について

パーサプラグインの追加と管理

バグトラッカプラグインの作成

1.7.1.3. バグトラッキングシステムのログオン資格情報のセキュリティ保護

Application Securityのバグを報告する場合は、バグトラッキングシステムのユーザ名とパスワードを入力します。ユーザ名とパスワードのペアはHTTPセッションに保存され、各アプリケーションのバグトラッキングシステムにマップされます。

各バグトラッキングシステムには、異なるバグパラメータのセットがあり、異なるユーザ入力も必要です。これらのパラメータは動的であり、バグトラッキングシステム自体からフェッチできます。一部のパラメータにはデフォルト値を指定できます。

バグ設定を完了して保存すると、バグトラッキングシステムにバグが作成され、Application Securityによって問題のバグIDが保存されます。

Important

Application SecurityがSSLを介して通信するように設定されている場合は、必要なバグトラッキングシステム証明書を、Application Securityが展開されているJava仮想マシン(JVM)にインポートする必要もあります。

1.7.1.4. バグトラッカパラメータ

バグトラッキングアプリケーションを使用して送信されるバグでは、［**バグの送信 (Submit Bug)**］ダイアログボックスに標準的なサマリとバグの説明の入力が必要です。優先度レベル、修復の締切日、および割り当て先ユーザの値を追加することもできます。Application Securityでは、選択したアプリケーションに基づいて、バグトラッキングシステムから［**Issue Type**］フィールドと［**Affects version**］フィールドの値を動的にフェッチします。

アプリケーションに追加のフィールドが必要な場合は、使用前にプラグインの変更が必要になる場合があります。手順については、「バグトラッカプラグインの作成」を参照するか、カスタマサポートにお問い合わせください。

1.7.1.4.1. ALM Quality Centerパラメータ

ALM Quality Centerバグトラッキングシステムの［**バグの送信(Submit Bug)**］ダイアログボックスで、ALM Quality Centerのインストールを反映するパラメータを選択します。

- バグサマリ
- バグの説明
- ALMドメイン
- ALMプロジェクト
- 重大度

ALM Quality Centerプロジェクトが ALI (詳細は後述)と統合されている場合は、欠陥の説明に、問題が発生した可能性のある候補変更セットが含まれています。

ALM Quality Center統合にはいくつかの重要なポイントがあります。変更セット検出が機能するには、次の条件を満たしている必要があります。

- 各OpenText SASTスキャンをビルドラベルでタグ付けします。Application Security はそれを使用して、スキャンをソース管理リビジョン番号にマップします。これを行うには、OpenText SASTの実行時に `-build-label <SVN_Revision_Number>` コマンドオプションを含め、ソースコードを翻訳します。
- ALM Quality Center内の個々のプロジェクトに対してALI拡張を有効にし、適切なソース管理リポジトリを設定してください。個々のプロジェクトに対してALI拡張が正常に有効になっている場合は、ALM Quality Centerにログインした後に［**コード変更(Code Changes)**］タブが表示されます。
- 変更セットの検出要件が満たされているかどうかに関係なく、ALM Quality Center のバグがログに記録されます。前提条件が満たされていない場合、変更セット検出メッセージはスキップされます。
- 現在、Subversionは、変更セット検出でサポートされている唯一のソース管理リポジトリです。

> **Note**
>
> ALM Quality Centerのバグを表示するには、ALM Quality Centerブラウザプラグインをインストールし、ALM Quality Centerと互換性のあるブラウザを使用する必要があります。

ALIおよびALM Quality Centerの詳細については、それらの製品のドキュメントを参照してください。

1.7.2. パーサプラグインの追加と管理

管理者は、Application Securityをサードパーティ製のパーサプラグインに接続できます。

Tip

独自のパーサプラグインを作成できます。手順については、GitHubで「サンプルのパーサプラグイン」ページを参照してください。

パーサプラグインをシステムに追加するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**プラグイン(Plugins)**］を展開し、［**パーサプラグイン(Parser Plugins)**］を選択します。
3. ［**パーサ(Parsers)**］ページで、［**新規(New)**］をクリックします。
4. サードパーティプラグインをアップロードするリスクに関する警告を確認して続行するには、［**OK**］をクリックします。
5. ［**プラグインバンドルのアップロード(Upload Plugin Bundle)**］ダイアログボックスで［**参照(BROWSE)**］をクリックし、プラグインのバンドルファイル(JARファイル)を見つけて選択します。
6. ［**アップロードの開始(START UPLOAD)**］をクリックします。

   ［**パーサ(Parsers)**］ページに、アップロードしたプラグインが一覧表示されます。
7. パーサ名が表示されている行を展開するには、その行をクリックします。
8. パーサプラグインを有効にするには、［**ENABLE**］をクリックします。
9. テストされていないプラグインを有効にするリスクに関する警告を確認して続行するには、［**OK**］をクリックします。

参照情報

バグトラッカプラグインの管理

1.7.2.1. OpenText Core SCA (Debricked)の結果を表示する準備

OpenText Core SCAからのオープンソースセキュリティデータは、Application Securityの［**監査(AUDIT)**］ページまたは［**オープンソース(OPEN SOURCE)**］ページで表示できます。そのためには、まず、必要なパーサプラグインをダウンロードしてインストールする必要があります。その後、アップロードされたオープンソース分析結果が表示されます。

OpenText Core SCAデータを表示するためにApplication Securityを準備するには:

1. ブラウザで、https://github.com/fortify/fortify-ssc-parser-debricked-cyclonedx/releasesに移動します。
2. ［**資産(Assets)**］をクリックし、最新バージョンのパーサを選択してダウンロードします。

   本ドキュメントの執筆時点の最新バージョンは `fortify-ssc-23.2+-parser-debricked-cyclonedx-1.2.0.zip` です。
3. ダウンロードしたZIPファイルの内容をローカルディレクトリに抽出します。
4. 管理者としてApplication Securityにサインインします。
5. ヘッダで、［**管理(Administration)**］を選択します。
6. ナビゲーションペインで［**プラグイン(Plugins)**］を展開し、［**パーサプラグイン(Parser Plugins)**］を選択します。
7. ［**パーサ(Parsers)**］ページで、［**新規(New)**］をクリックします。
8. プラグインをアップロードするリスクを受け入れるには、［**OK**］をクリックします。
9. ［**プラグインバンドルのアップロード(UPLOAD PLUGIN BUNDLE)**］ダイアログボックスで、［**参照(BROWSE)**］をクリックしてから、展開したJARファイルを選択します。
10. ［**プラグインバンドルのアップロード(UPLOAD PLUGIN BUNDLE)**］ダイアログボックスで、［**アップロードを開始(START UPLOAD)**］をクリックします。

    ［**パーサ(Parsers)**］ページに、OpenText Core SCAパーサプラグインが一覧表示されます。
11. アップロードが完了したら、OpenText Core SCAパーサプラグインの行を展開し、［**有効にする(ENABLE)**］をクリックします。

12. プラグインの有効化警告メッセージを受け入れるには、［**OK**］をクリックします。

参照情報

スキャンアーティファクトのアップロード

オープンソースデータの表示

1.7.2.2. Sonatypeの結果を表示するための準備

アプリケーションバージョンに関するSonatypeのNexus Lifecycleソリューション分析結果のオープンソースセキュリティデータは、Application Securityの［**監査(AUDIT)**］ページまたは［**オープンソース(OPEN SOURCE)**］ページから表示できます。そうするには、まず必要なSonatype Parser Pluginをダウンロードしてインストールする必要があります。その後、アップロードされたSonatype分析結果が表示されます。

アップロードされたSonatypeデータを表示するためのApplication Securityの準備をするには、次の手順に従います。

1. Webブラウザで、https://marketplace.opentext.com/cybersecurity/content/sonatype-for-fortify-sscに移動します。
2. ［**Sonatype for Fortify SSC**］ページで、［**最新バージョンの取得(GET NEWEST)**］をクリックします。
3. `SonatypeFortifyBundle-<version>.zip` ファイルの内容をローカルディレクトリに解凍します。
4. 管理者としてApplication Securityにサインインします。
5. ヘッダで、［**管理(Administration)**］を選択します。
6. ナビゲーションペインで、［**プラグイン(Plugins)**］セクションを開き、［**パーサプラグイン(Parser Plugins)**］を選択します。
7. ［**パーサ(Parsers)**］ページで、［**新規(New)**］をクリックします。
8. プラグインをアップロードするリスクを受け入れるには、［**OK**］をクリックします。
9. ［**プラグインバンドルのアップロード(UPLOAD PLUGIN BUNDLE)**］ダイアログボックスで、［**参照(BROWSE)**］をクリックしてから、`sonatype-plugin-<version>.jar` ファイルを選択します。
10. ［**アップロードの開始(START UPLOAD)**］をクリックします。
11. アップロードが完了したら、Sonatype Vulnerability Parserの行を展開し、［**有効にする(ENABLE)**］をクリックします。
12. プラグインを有効にするリスクを受け入れるには、［**OK**］をクリックします。

参照情報

スキャンアーティファクトのアップロード

1.7.3. Application Securityユーザ管理について

このセクションでは、さまざまなタイプのApplication Securityユーザアカウントについて、およびユーザ用にこれらのアカウントを作成する方法について説明します。

このセクションで説明するトピック:

1.7.3.1. 管理者アカウント

管理者アカウントを持つユーザは、すべてのApplication Securityユーザおよびアプリケーションバージョンデータへの完全なアクセス権を持ち、Application Securityシステム全体を管理できます。管理者アカウントを持つユーザだけが、他のユーザアカウントを作成、編集、削除できます。ローカルユーザアカウントを変更するには、ローカル管理者でなければなりません。

ローカルまたはLDAP Application Securityユーザアカウントの作成と編集に必要な管理者レベルアカウントのみを作成することを推奨します。セキュリティリードおよびそれ以下のアカウントは、他のすべてのアプリケーション関連アクティビティを実行できます。

Application Securityでは、管理者レベルアカウントをアプリケーションバージョンに明示的に追加できます。これにより、［**監査(AUDIT)**］ページから管理者に問題を割り当てることができます。

参照情報

Application Securityの役割に関する許可情報の表示

1.7.3.2. ユーザアカウントタイプ

ユーザアカウントの管理に使用される管理者レベルのアカウントに加えて、Application Securityは権限レベルの順で、次のユーザアカウントタイプをサポートします。

- **管理者**—管理者は、すべてのアプリケーションバージョンにアクセスし、システム内のすべてのアクションを実行できます。
- **セキュリティリード**—セキュリティリードは、ユーザアカウントの作成と編集を除くすべての管理操作にアクセスできます。セキュリティリードは、アプリケーションバージョンを作成し、作成したバージョンまたは割り当てられたバージョンのすべての側面を編集できます。
- **マネージャ**—マネージャはほとんどの管理データに読み取り専用でアクセスできます。マネージャは、割り当てられたアプリケーションバージョンのすべてのデータを作成および編集できます。
- **開発者**—開発者は、一部の管理データに読み取り専用でアクセスできます。開発者は、割り当てられたアプリケーションバージョンのデータのサブセットを作成および編集できます。

- **表示のみ**—表示のみのユーザは、アクセス権を持つアプリケーションバージョンの一般情報および問題を表示できます。表示のみのユーザは、分析結果または監査の問題をアップロードできません。

- **アプリケーションセキュリティテスタ**—アプリケーションセキュリティテスタは、動的スキャン要求の実行に関連する操作を実行できます。アプリケーションセキュリティテスタは、アプリケーションのバージョンの表示、レポートの表示と生成、動的スキャンの処理、結果および監査の問題のアップロードができます。

- **WebInspect Enterprise System**—WebInspect Enterprise Systemの役割を割り当てられたユーザは、Application SecurityからOpenText™ Fortify WebInspect Enterpriseインスタンスを登録および登録解除できます。また、問題の監査情報を取得することもできます。この役割は、Fortify WebInspect Enterpriseの使用のみを目的にしています。

- **ScanCentral SAST Controller**—ScanCentral SAST Controllerの役割を割り当てられたユーザは、スキャンの実行が許可されているものの「分析結果のアップロード」は許可されていないユーザの代わりに、Fortify ScanCentral SASTを使用してApplication Securityにスキャンをアップロードできます。この役割は、Fortify ScanCentral SAST Controllerを設定する際に限って使用されるよう意図されています。Fortify ScanCentral SAST設定でこの役割を使用する方法については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

参照情報

ユーザアカウントの作成について

ローカルユーザアカウントのロック解除

1.7.3.3. ユーザアカウントの作成について

管理者は、ローカルユーザアカウントを編集、削除、または一時停止できます。OpenTextでは、初めてApplication Securityにサインインした後、デフォルト以外の管理者アカウントを少なくとも1つ作成し、デフォルトの管理者アカウントを削除することを推奨しています。

デフォルト以外の管理者アカウントを作成した後、新しいアカウントを使用してユーザアカウントを作成します。

Note

管理者は、残っている最後の管理者レベルのアカウントを除くすべてのユーザアカウントを削除または一時停止できます。Application Securityでは、このようなアカウントに対する一時停止機能と削除機能が自動的に無効になります。

ユーザアカウントのタイムアウトとロックアウトの設定方法については、「コア設定の設定」を参照してください。ユーザアカウントの許可の詳細については、「アカウント管理」を参照してください。

参照情報

ローカルユーザアカウントの作成

Application Securityの役割に関する許可情報の表示

ローカルユーザアカウントのロック解除

1.7.3.4. Application Securityへの破壊的ライブラリおよびテンプレートのアップロードの防止

Caution

悪意のあるユーザがレポートライブラリまたはテンプレートを変更して、任意の破壊的な結果をもたらす可能性があるSQLクエリおよびコマンドを含める可能性があります。信頼されたユーザによって作成され、悪意のあるクエリやコマンドがないか確認されたライブラリとテンプレートのみをアップロードします。

レポート定義およびライブラリを管理する権限を持つユーザだけが、カスタムレポートライブラリおよびテンプレートをApplication Securityにアップロードできます。任意の破壊的なコマンドを実行するテンプレートがApplication Securityにアップロードされないようにするには、次のようにします。

- 信頼されたユーザにのみアクセス許可を割り当てます。
- Application Securityにアップロードする前に、すべてのカスタムテンプレートで任意のSQLクエリとコマンドをチェックしてください。

1.7.3.5. Application Securityの役割に与えられている許可を表示する

割り当てられているApplication Securityの役割によって、ユーザが実行できるアクションに関する詳細情報を表示するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**役割(Roles)**］を選択します。

   ［**役割(Roles)**］ページに、システム内のすべての役割の名前と説明が一覧表示されます。
3. 対象の役割の行をクリックして、その役割に関する詳細を表示します。

   ［**許可(Permissions)**］テーブルに、その役割が割り当てられたユーザに与えられるすべての許可が一覧表示されます。

参照情報

ユーザアカウントの管理

ユーザアカウントの作成について

事前設定済みの役割

ローカルユーザアカウントのロック解除

1.7.3.6. LDAPユーザ役割の管理について

相対識別名(RDN)は、ベース識別名(DN)をさらに修飾します。たとえば、特定のLDAPディレクトリのベースDNが `dc=domainName, dc=com,` 、フルDNが `cn=group1,ou=users,dc=domainName,dc=com,` である場合、RDNは `cn=group1,ou=users.` になります。

このセクションのトピックでは、LDAP RDNを使用してユーザの役割を決定する方法について説明します。

1.7.3.6.1. Application Securityのグループメンバーシップ

Application Security がユーザを特定のグループのメンバーとして認識するためには、ユーザアカウントはLDAPディレクトリ内のグループオブジェクトを参照する必要があります。ユーザがサインインする際に、Application Securityはそのユーザをディレクトリ内で検索します。Application Securityがユーザのグループを、グループメンバーシップ属性で指定された共通名(CN)によって確かめます。ユーザが複数のグループに属し、それらのグループが異なる役割にマップされている場合、Application Securityはそのユーザにすべての役割を割り当てます。

Application Security は、ネストされたグループをサポートします。たとえば、あるユーザがグループAのメンバーであり、グループAがグループBのメンバーである場合、Application Securityはそのユーザを両方のグループのメンバーであると認識します。

Important

ネストされたLDAPグループを使用するのは、どうしても必要な場合だけにしてください。ネストされたLDAPグループを有効にすると、Application Securityが認証中に余分なツリートラバーサルを実行しなければならなくなります。OpenTextでは、ネストされたグループを使用しない場合は、このチェックボックスをオフにすることを強く推奨しています。

参照情報

失敗したLDAPユーザログインの処理

1.7.3.6.2. 失敗したLDAPユーザログインの処理

Application Securityサーバを対象に、ネストされたLDAPグループを設定している場合、誤った資格情報が原因でログイン試行中にLDAP認証が失敗すると、サインインで不正な資格情報に関するメッセージが表示されます。ただし、ログに「user is not authorized (ユーザは認証されていません)」というテキストが含まれている場合は、次の点を確認してください。

- ユーザがApplication Securityに登録され、役割が割り当てられているか。LDAP管理者に問い合わせて、ユーザが属すると想定されるグループの実際のメンバーであるかどうかを確認します。
- ユーザがLDAPグループに属している場合は、そのグループがApplication Securityに登録され、役割が割り当てられているかどうかを確認します。
- 特別なケース: ユーザがApplication Securityに登録されたLDAPグループに属しているが、そのグループに追加されたのがたった数時間前である場合は、LDAPキャッシュを手動で更新するか、自動更新を数時間待ちます。

LDAPキャッシュの更新を手動で要求するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**LDAPエンティティ(LDAP Entities)**］を選択します。
3. LDAPサーバのチェックボックスをオンにします。
4. ［**LDAP**］ページヘッダで、［**更新(REFRESH)**］をクリックします。
5. LDAPキャッシュの更新が完了したかどうかを判断するには、［管理］ビューで、［**イベントログ(Event Logs)**］ページまたは［**ジョブ(Jobs)**］ページのいずれかを確認します。

Note

LDAPキャッシュの更新が完了するには長い時間がかかる場合があります。

参照情報

Application Securityのグループメンバーシップ

1.7.3.6.3. LDAPグループへのApplication Security役割のマッピングについて

ほとんどの環境では、LDAPディレクトリには、Application Securityにアクセスする必要のないユーザが含まれます。また、ユーザのグループによっては、異なるアクセス許可が必要になる場合があります。

LDAPユーザ権限付与を設定する前に、Application Security役割(管理者、マネージャ、開発者、および監査官)に関連付けるLDAPグループを決定する必要があります。OpenTextでは、新しいLDAPグループを作成して、それぞれ異なるApplication Security役割に直接マップすることを推奨しています。たとえばFORTIFY_ADMINSグループとFORTIFY_DEVELOPERSグループを作成できます。

1.7.4. Application Securityのグローバル検索機能

Application Securityには、アプリケーションバージョン、問題、レポート、コメント、およびユーザの全体に検索用語を適用するグローバルなカテゴリベースの検索機能があります。新しく追加されたドキュメント(アーティファクト、アプリケーションバージョン、ユーザ)には、自動的にすぐにインデックスが付けられます。

Note

アップロードされたFPRファイルのインデックス付けはすぐには行われません。それは、アーティファクトアップロードジョブの最後に行われるようにスケジュールされる、別の新しい問題のインデックス付けジョブとして実行されるためです。

1日1回実行されるインデックス保守ジョブは、インデックスの正常な状態を維持します。この実行時間は［**管理(Administration)**］ビューから変更できます。このジョブを1日1回実行するようにスケジュールすることを推奨します。実行されたジョブを再スケジュールする方法については、「ジョブスケジューラの設定」を参照してください。

Application Securityサーバでグローバル検索を有効にするには、検索インデックスディレクトリへの読み取りおよび書き込みアクセス権をTomcatサーバに提供する必要があります。グローバル検索は、初回サインイン時またはアップグレード後の設定時に有効にできます。

推奨ディスクサイズ

グローバル検索に必要なインデックス付けに最適なディスクサイズは、データの特性によって異なりますが、Luceneインデックスはデータベース内のデータよりはるかに小さくなります。たとえば、データベース問題ボリューム18GB(dbインデックス付き)に必要なインデックスサイズは約2GBです。

参照情報

Application Securityの初回設定

アップグレード後のApplication Securityの設定

Luceneのアップグレード

検索インデックスの問題のトラブルシューティング

1.7.4.1. 検索インデックスの問題のトラブルシューティング

検索インデックスの正常性を示すインジケータとして、検索インデックスディレクトリ(設定ウィザードまたは自動設定で指定)にマーカーファイル `healthy.index` が含まれます。このファイルが検索インデックスディレクトリに存在しない場合は、Application Securityは起動時ごとにインデックスを再作成します。

初期インデックスの作成が繰り返し失敗する場合には、インデックスディレクトリ全体を削除してから、Application Securityを再起動します。

大きなデータベース(数百GB)で作業している場合には、システムメモリが限られているためにFull Reindexジョブが失敗する可能性があります。この問題が発生した場合は、Application SecurityのJavaのヒープサイズを増やしてからApplication Securityを再起動します。Javaのヒープサイズの最小値と推奨値については、「*Application Securityソフトウェアのシステム要件*」ドキュメントを参照してください。

1.7.5. Application Securityを保守モードに入れる

サーバの環境設定を変更する必要がある場合は、いつでもApplication Securityを保守モードに移行し、必要な変更を加えることができます。

Application Securityを保守モードにするには、次の手順に従います。

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**保守(Maintenance)**］を選択します。
4. ［**保守(Maintenance)**］ページで［**保守モードに設定する(Set to maintenance mode)**］チェックボックスをオンにし、［**保存(SAVE)**］をクリックします。
5. サーバを再起動します。

   > **Note**
   >
   > この `autoconfig` ファイルはKubernetesシークレット内にあり、削除できません。

6. テキストエディタで *<fortify.home>/<app_context>/init.token* ファイルを開きます。
7. `init.token` ファイルの内容をクリップボードにコピーします。
8. Webブラウザウィンドウを開き、Application Securityインスタンスのwebアドレスを入力します。
9. ［**管理者(ADMINISTRATORS)**］をクリックします。
10. `init.token` ファイルからコピーした文字列を［**セキュリティトークン(Security Token)**］フィールドに貼り付け、［**サインイン(SIGN IN)**］をクリックします。

    Application Securityセットアップウィザードには、現在の設定がすべて表示されます。サーバ設定に関する情報については、Application Securityの初回設定を参照してください。
11. サーバの設定が正常に完了したら、Tomcatを再起動します。

Note

または、 `-Dcom.fortify.ssc.forceInit` のJavaオプションを設定して、セットアップの完了後にセットアップウィザードを再初期化することもできます。

Note

Application Securityインスタンスが保守モードでスタックしている場合は、Application Securityが保守モードでスタックしている場合で説明されている解決策のいずれかを試してください。

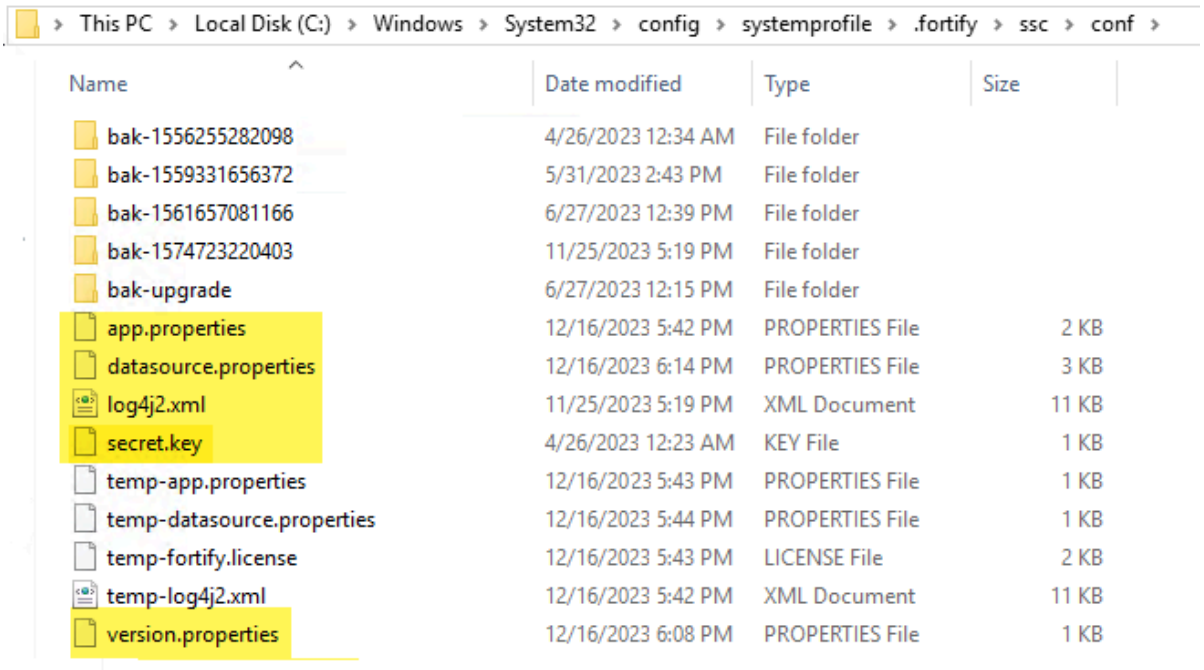
サーバの保守を容易にするため、ジョブの実行を一時停止できます。これにより、実行中のジョブは終了しますが、新しいジョブは実行されません。詳細については、「ジョブ実行の一時停止と再開」を参照してください。

1.7.5.1. Application Securityが保守モードでスタックしている場合

Application Securityは、管理者によって保守モードに切り替えられたとき(「Application Securityを保守モードに入れる」を参照)、または *<fortify.home>/<app_context>*/conf/ ディレクトリで version.properties を突き止められないときに、保守モードに入ります。

Application Securityインスタンスが保守モードでスタックしている場合は、次のいずれかを試してください。

- Application Security再設定します。指示については、Application Securityの初回設定を参照してください。
- *<fortify.home>/<app_context>*/conf/ ディレクトリに移動し、 version.properties ファイル内で maintenance.mode を false に設定します。
- 見つからないファイルを元のインストールファイルから <fortify.home> / <app_context>/conf/ ディレクトリに復元します。



Note

datasource.properties ファイルおよび一部のデータベースフィールドには、 secret.key ファイルに依存する暗号化されたエントリが含まれています。したがって、Application Securityインスタンスをコンピュータ間で移動する場合は、データベースファイルだけではなく secret.key ファイルも移動する必要があります。

1.7.6. ジョブ実行の一時停止と再開

何らかの理由でサーバをシャットダウンする必要がある場合は、ユーザアクティビティを一時停止して、システム内のすべてのユーザに対して新しいジョブの実行を停止できる一方、Application Securityで進行中のジョブは完了できます。これは、サーバのシャットダウン時にデータの破損や消失を防ぐのに役立ちます。

サーバ上でジョブ実行を一時停止するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**保守(Maintenance)**］を選択します。
4. ［**保守(Maintenance)**］ページで、［**ジョブ実行を一時停止する(Pause job execution)**］チェックボックスをオンにしてから、［**保存(SAVE)**］をクリックします。

   設定を保存した直後に、以下のようになります。

   > **Important**
   >
   > 大量のジョブがキューに登録されるのを防ぐために、この設定を長時間にわたって有効にしないようにお勧めします。ジョブ実行を一時停止した後、キューに登録されているジョブを完全に処理するために必要な時間を確保してから、サーバをシャットダウンしてください。

   - 進行中のすべてのジョブを完了できます。
   - それ以降にユーザが送信する新しいジョブはすべてキューに登録され、後で［**ジョブ実行を一時停止する(Pause jobs execution)**］チェックボックスをオフにすると実行されます。
   - ジョブ実行が一時停止されたことをユーザに通知するためのバナーがApplication Securityに表示されます。
5. 次回サーバを起動するときに、［**保守(Maintenance)**］ページに戻り、［**ジョブ実行を一時停止する(Pause job execution)**］チェックボックスをオフにしてから、［**保存(SAVE)**］をクリックします。

参照情報

Application Securityの保守モードへの移行

1.7.7. OpenText SAST Application Security Contentについて

OpenText Application Security Software製品は、ルールのナレッジベースを使用して、分析用のコードベースにセキュアなコーディング標準を強制的に適用します。OpenText SAST Application Security Contentは、OpenText Secure Coding Rulepacksと外部メタデータで構成されています。

- ルールパックは、よく知られた言語や公開APIのための一般的なセキュアコーディングのイディオムを記述しています。

  ユーザはカスタムルールを記述して、OpenText SASTとOpenText Secure Coding Rulepacksの機能に追加できます。たとえば、専有セキュリティガイドラインを適用しなければならない場合や、OpenText Secure Coding Rulepacksではまだ対応していないサードパーティライブラリや事前コンパイルされたその他のバイナリを使用するアプリケーションを分析しなければならない場合があります。カスタムルールの作成方法については、『OpenText™ Static Application Security Testingカスタムルールガイド』を参照してください。

  OpenText Secure Coding Rulepacksの管理方法については、次を参照してください。

  - Rulepack更新サーバによるRulepacksの更新
  - OpenText SAST Application Security Contentのインポート
  - ルールパックの削除
  - Rulepacksをエクスポートする
  - 四半期ごとのOpenText SAST Application Security Contentリリースで提供されるレポートシードバンドルを使用したデータベースのシード処理

- 外部メタデータは、OpenText Application Security Software脆弱性カテゴリを代替カテゴリ(CWE、OWASP Top 10、PCIなど)にマップします。

  OpenTextでは、外部ファイルを変更しないことを推奨しています。変更しても、四半期ごとのリリースでRulepacksを更新するたびに、その変更が上書きされます。ただし、カスタムの外部メタデータXMLファイルを作成し、そこで新しいマッピングを作成して既存のマッピングを拡張することはできます。さまざまな分類体系(内部アプリケーションのセキュリティ基準や追加のコンプライアンス義務など)に変更の問題をマップすることもできます。OpenText SAST Application Security Contentを更新する際に、このカスタムファイルが影響を受けることはありません。独自のカスタムルールまたはカスタムの外部メタデータを作成する方法については、『*OpenText™ Static Application Security Testingカスタムルールガイド*』を参照してください。

付属の外部メタデータマッピングファイルは、`<ssc_deploy_dir>/WEB-INF/Core/config/ExternalMetadata/` ディレクトリ内にあります。

外部メタデータの管理方法については、次を参照してください。

- 現在のマッピングを拡張する
- 新しいマッピングの作成

利用可能な最新のOpenText Secure Coding Rulepacksを使用することが重要です。OpenTextでは、定期的にOpenText SAST Application Security Contentを更新することを推奨しています。

1.7.7.1. Rulepack更新サーバによるRulepacksの更新

利用可能な最新のRulepackを使用することが重要です。最新のRulepackを使用していることを確実にするために、Rulepack更新サーバからRulepackをインポートできます。

Note

Rulepack更新サーバがApplication Securityプロキシの背後にある場合は、そのプロキシを使用してRulepackを更新できます。Application Securityで使用する統合プロキシを設定する方法については、「Application Security統合のプロキシの設定」を参照してください。

最新のRulepackをインポートするには、次の手順に従います。

1. Application Securityに管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**Rulepacks**］を選択します。
4. ［**Rulepacks**］ページで、［**サーバから更新(UPDATE FROM SERVER)**］をクリックします。

   Application Securityに、Rulepackの更新内容に関する情報が表示されます。
5. 更新を続行するには、［**OK**］をクリックします。

   更新が完了すると、Application Securityにインポートされたルールが一覧表示されます。
6. ［**閉じる(CLOSE)**］をクリックします。

参照情報

ルールパックの削除

四半期ごとのOpenText SAST Application Security Contentリリースで提供されるレポートシードバンドルを使用したデータベースのシード処理

Rulepacksをエクスポートする

OpenText SAST Application Security Contentのインポート

1.7.7.2. Rulepacksをエクスポートする

必要に応じて、RulepacksをあるApplication Securityインスタンスから別のインスタンスに移動したり、Application SecurityとAudit Workbench間で移動したりできます。

Rulepacksを、それらをインポートするために使用するのと同じファイル名で、ファイル拡張子(`.bin` または `.xml`)も含めてエクスポートします。

Rulepackをエクスポートするには:

1. 管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**Rulepacks**］を選択します。
4. ［**Rulepacks**］ページで、エクスポートするRulepackのチェックボックスをオンにしてから、［**エクスポート(EXPORT)**］をクリックします。

> **Note**
>
> 選択したRulepackに複数のバージョンがある場合は、最新バージョンだけがエクスポートされます。

参照情報

OpenText SAST Application Security Contentのインポート

ルールパックの削除

1.7.7.3. OpenText SAST Application Security Contentのインポート

セキュリティコンテンツ(OpenText™ Fortify Custom Rules Editorを使用して作成されたカスタムRulepack、拡張マッピングファイル、カスタムマッピングファイルなど)をインポートして、OpenText SASTおよびFortify Audit Workbenchで使用できます。

セキュリティコンテンツをインポートするには、次の手順に従います。

1. 管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**Rulepacks**］を選択します。
4. ［**Rulepacks**］ページで、［**インポート(IMPORT)**］を選択します。
5. ［**Rulepackのインポート(IMPORT RULEPACK)**］ダイアログボックスで、［**+ファイルを追加(+ADD FILES)**］をクリックします。
6. アップロードするファイルを検索して選択します。
7. ［**アップロードの開始(START UPLOAD)**］をクリックします。
8. ［**閉じる(CLOSE)**］をクリックします。

Note

拡張したマッピングを含むFPRファイルをアップロードし、そのマッピングがサーバに存在しない場合、Application Securityに処理の警告が表示されます。

参照情報

Rulepacksをエクスポートする

ルールパックの削除

1.7.7.4. ルールパックの削除

古いルールパックは、Application Securityから削除できます。

ルールパックを削除するには、次の手順を実行します。

1. 管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**Rulepacks**］を選択します。
4. ［**Rulepacks**］ページで、削除するRulepackのチェックボックスをオンにしてから、［**削除**］をクリックします。
5. 選択したRulepackの削除を確認するには、［**OK**］をクリックします。
6. 削除に失敗した場合は、［**詳細**］をクリックして［**詳細(DETAILS)**］ウィンドウを開き、失敗の原因を確認します。

参照情報

Rulepacksをエクスポートする

OpenText SAST Application Security Contentのインポート

Rulepack更新サーバによるRulepacksの更新

1.7.7.5. 既存のマッピングを拡張する

<ExternalListExtension> 要素を使用して、既存のマッピングを拡張することができます。それをする場合は、次のことを念頭に置いてください。

- 新しいマッピングの追加だけができます。
- 既存のマッピングを上書きすることはできません。

現在のマッピングを拡張するには、次の形式を使用します。

```
 <ExternalListExtension> <ExternalListID>EEE3F9E7-28D6-4456-
8761-3DB99436F4EE</ExternalListID> <ExternalCategoryDefinition>
<Name>APP100 CAT 1</Name> <Description> Description for App100
CAT 1. </Description> OrderingInfo>1</OrderingInfo>
</ExternalCategoryDefinition> <Mapping> <InternalCategory> Poor
Style: Indentifier Contains Dollar Symbol ($)
</InternalCategory> <ExternalCategory>App100 CAT
1</ExternalCategory> </Mapping> </ExternalListExtension>
```

Important

マッピングファイルを拡張した後に、Application Securityへアップロードする必要があります。手順については、「OpenText SAST Application Security Contentのインポート」を参照してください。

拡張したマッピングを含むFPRファイルをアップロードし、そのマッピングがサーバに存在しない場合、Application Securityに処理の警告が表示されます。

参照情報

新しいマッピングの作成

OpenText SAST Application Security Contentについて

1.7.7.6. 新しいマッピングの作成

<ExternalList> 要素を使用して、カスタムの外部メタデータファイルを次の形式で作成できます。

```
 <ExternalList> <ExternalListID>3C6ECB67-BBD9-4259-A8DB-
B49328927248</ExternalListID> <Name>My Custom Mapping</Name>
<Shortcut>MCM</Shortcut> <Description>My custom mapping
description</Description> <Group>MCM</Group>
<ExternalCategoryDefinition> <Name>Custom Mapping CAT 1</Name>
<Description> Description for Custom Mapping CAT 1.
</Description> OrderingInfo>1</OrderingInfo>
</ExternalCategoryDefinition> <Mapping> <InternalCategory>SQL
Injection</InternalCategory> <ExternalCategory>Custom Mapping
CAT 1</ExternalCategory> </Mapping>
<OrderingInfo>1</OrderingInfo> </ExternalList>
```

Important

カスタムマッピングファイルを作成した後、それをApplication Securityにアップロードする必要があります。手順については、「セキュリティコンテンツのインポート」を参照してください。

カスタムマッピングを含むFPRファイルをアップロードし、そのマッピングがサーバに存在しない場合、Application Securityには処理の警告が表示されます。

参照情報

現在のマッピングを拡張する

OpenText Application Security Softwareセキュリティコンテンツについて

1.7.8. Fortify Audit WorkbenchからのOpenText SASTおよびOpenText Application Securityツールのアップグレードを可能にする

Fortify Audit Workbenchを使用しているすべてのお客様は、新しいバージョンのOpenText SASTおよびOpenText Application Security ToolsがFortify Audit Workbenchから利用可能かどうかを確認できます。インストールされているバージョンより新しいバージョンが使用可能な場合は、ユーザがそのバージョンをダウンロードし、ローカルインスタンスをアップグレードできます。また、Fortify Audit Workbenchのユーザは、起動時に新しいバージョンが自動的にチェック、ダウンロード、およびインストールされるようにFortify Audit Workbenchを設定することもできます。

この機能をFortify Audit Workbenchのユーザ向けに有効にするには、最初に管理者がApplication Securityホストコンピュータで自動アップグレード機能を設定する必要があります。

新しいOpenText SASTおよびOpenText Application Security Toolsのインストーラを Fortify Audit Workbenchユーザがアップグレードで使用できるようにするには:

1. Application Securityホストで、 `<ssc_deploy_dir>` / `WEB-INF/internal/securityContext.xml` ファイルをテキストエディタで開きます。
2. 次の行を見つけて、コメント解除します。

   ```
   <!-- <security:intercept-url pattern="/update-site/**" access="PERM_ANONYMOUS"/> -->
   ```

3. `securityContext.xml` ファイルを保存して閉じます。
4. OpenText_SAST_*<version>*または OpenText_Application_Security_Tools_*<version>*インストーラファイルを `<ssc_deploy_dir>/update-site/installers/` ディレクトリにコピーします。
5. `<ssc_deploy_dir>/update-site/installers/` ディレクトリで、更新する製品ごとに更新XMLファイルを作成します。
   1. OpenText SASTの更新を有効にするには、次の例を使用して更新XMLファイル(`update-sast.xml` など)を作成します。

```
<installerInformation> <versionId>2620</versionId> <!--
The version of the installer file with periods removed-
-> <version>26.2.0</version> <!--The version of the
installer file--> <platformFileList> <platformFile>
<filename>OpenText_SAST_windows-
x64_26.2.0.exe</filename> <platform>windows-
x64</platform> </platformFile> <platformFile>
<filename>OpenText_SAST_linux-x64_26.2.0.run</filename>
<platform>linux-x64</platform> </platformFile>
<platformFile> <filename>OpenText_SAST_osx-
x64_26.2.0.app.zip</filename> <platform>osx</platform>
</platformFile> </platformFileList>
<downloadLocationList> <downloadLocation>
<url>http://localhost:8080/update-
site/installers/</url> </downloadLocation>
</downloadLocationList> </installerInformation>
```

2. OpenText Application Security Toolsの更新を有効にするには、次の例を使用して更新XMLファイル(`update-tools.xml` など)を作成します。

```
<installerInformation> <versionId>2620</versionId> <!--
The version of the installer file with periods removed-
-> <version>26.2.0</version> <!--The version of the
installer file--> <platformFileList> <platformFile>
<filename>OpenText_Application_Security_Tools_windows-
x64_26.2.0.exe</filename> <platform>windows-
x64</platform> </platformFile> <platformFile>
<filename>OpenText_Application_Security_Tools_linux-
x64_26.2.0.run</filename> <platform>linux-
x64</platform> </platformFile> <platformFile>
<filename>OpenText_Application_Security_Tools_osx-
x64_26.2.0.app.zip</filename> <platform>osx</platform>
</platformFile> </platformFileList>
<downloadLocationList> <downloadLocation>
<url>http://localhost:8080/update-
site/installers/</url> </downloadLocation>
</downloadLocationList> </installerInformation>
```

6. Tomcatサーバを再起動します。

Note

アップグレード機能に使用されるAutoUpdateツールの詳細については、『Install Builderユーザガイド』を参照してください。

これで、Fortify Audit Workbenchのユーザは、新しいバージョンのOpenText SASTまたはOpenText Application Security Toolsを確認してインストールできるようになりました。Fortify Audit Workbenchからアップグレードを実行する方法については、『*OpenText™ Fortify Audit Workbenchユーザガイド*』を参照してください。

1.8. Application Securityのアップグレード

Application Securityの最新バージョンに直接アップグレードするには、最新の3つのバージョンのいずれかがすでにインストールされている必要があります。古いバージョンをお使いの場合は、まず以下のいずれかのバージョンにアップグレードする必要があります。以下のバージョンは直接アップグレードに対応しています。

- 25.4.x
- 25.2.x
- 24.4.x

このセクションでは、次のトピックについて説明します。

1.8.1. アップグレードの前提条件

アップグレードに必要な次の前提条件を満たしてください。

- 24.2.xより前のバージョンからアップグレードする場合は、アップグレードする前に、Javaバージョン17がインストールされていることを確認します。
- Application SecurityでFull Fortify ScanCentral SAST関連の機能を使用するには、更新されたコントローラおよびセンサが必要です。センサメトリックが必要ない場合は、既存のセンサを使用できます。既存のFortify ScanCentral SASTクライアントは、機能の制限なしで使用できます。

Important

センサとクライアントをアップグレードする前、およびApplication Securityサーバをアップグレードする前に、コントローラをアップグレードする必要があります。アップグレードする方法については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

次も参照

データベースのアップグレードの準備

1.8.2. データベースのアップグレードの準備

Application Securityデータベースのマイグレーションプロセスでは、通常の使用時に作成されたトランザクションよりも大きいトランザクションが作成されます。実稼働環境で正常に実行されているデータベースの場合、データベースのマイグレーションでは通常、データベースの設定やリソースを変更する必要はありません。大規模なデータベースの場合、OpenTextでは、マイグレーションプロセスに対応するために必要なデータベースリソースと設定を確認し、必要に応じて増やすことを推奨しています。

バージョン23.1.0以前からバージョン23.2.0以降にアップグレードする場合、MySQLおよびSQLデータベースが最大32bの整数上限に達しないように、マイグレーション中に `scan_issue` テーブル内のID列のデータ型がINTからBIGINTに変更されることに注意してください。

SQL Serverが `scan_issue` テーブルでID値を負の数値にリセットする問題 `DBCC CHECKIDENT (scan_issue, reseed, -2147483648)` に対して推奨される回避策をすでに適用している場合は、追加の手動マイグレーションステップを行う必要があります。マイグレーションが完了したら、ID値を正の数にリセットします。リセットするには、 `DBCC CHECKIDENT (scan_issue, RESEED)` クエリを実行します。クエリを実行するユーザは、テーブルを含むスキーマの所有者か、sysadmin、db_owner、またはdb_ddladmin固定データベースロールを持っている必要があります。

MySQLデータベースをアップグレードする場合は、「MySQLデータベースのアップグレード時のInnodbバッファプールサイズの設定」を参照してください。

1.8.2.1. MySQLデータベースのアップグレード時のInnodbバッファプールサイズの設定

OpenTextでは、MySQLデータベースをアップグレードする場合は、`innodb_buffer_pool_size`変数を少なくとも2.5GBに設定することを推奨しています。アップグレード後、前の設定に戻します。

参照情報

MySQLデータベースの使用

1.8.2.2. データベースアップグレードスクリプトの実行準備

Application Securityデータベースアップグレードスクリプトには、データベース作成スクリプトに必要なものと同じ、データベースに対する許可が必要です。

データベースアップグレードスクリプトを実行する前に、次のタスクを実行します。

- データベースクライアントツールを使用して、既存のApplication Securityデータベースをバックアップします。
- 既存のApplication Securityデータベースの作成に使用されたデータベースアカウント情報を取得します。「データベースユーザアカウントの許可」を参照してください。

Note

1TBを超えるデータを含むデータベースの移行には、5時間以上かかる場合があります。

1.8.3. アップグレードタスク

Application Securityを新しいバージョンにアップグレードするには、次の表で説明するタスクを記載順に実行します。

タスク	説明(Description)
1	Tomcatサーバを停止します。
2	*<tomcat>*/webapps/ ディレクトリからWARファイルを削除してから、新しいWARファイルを *<tomcat>*/webapps/ ディレクトリにコピーします(「WARファイルの更新と展開」を参照)。 **Note** *<tomcat>*は、Tomcatインスタンスのルートディレクトリを表します。
3	Tomcatサーバを起動します。
4	ブラウザを開き、アプリケーションセキュリティのWebアドレスを入力してセットアップウィザードを起動します。
5	セットアップウィザードを使用して、マイグレーションSQLスクリプトを生成します(「アップグレード後のApplication Securityの設定」を参照)。

タスク	説明(Description)
6	データベースでマイグレーションスクリプトを実行します(「データベースアップグレードスクリプトの実行準備」を参照)。 1TBを超えるデータを含むデータベースの移行には、5時間以上かかる場合があります。 **Important** (SQL Serverデータベースのみ) Application Securityを新しいSQL Serverデータベースバージョンに移行して、データベースのバックアップと復元を行った後、Application Securityデータベースを現在ホストしているSQLエンジンが反映されるように(SQL Server Management Studioで)互換性レベルを変更する必要があります。
7	セットアップウィザードを使用してデータベースを再シードします。
8	Tomcatサーバを再起動します。
9	バグトラッカプラグインは`ssc.war`ファイルに含まれていません。Application Securityをアップグレードして起動した後、古いバグトラッカプラグインを削除し、最新のインストールパッケージに含まれる新しいプラグインをインストールしてください。詳細については、「バグトラッカの統合について」を参照してください。

1.8.4. Luceneのアップグレード

Application Security 26.2バージョンにはLuceneの更新バージョンが含まれています。Luceneのインデックス形式はメジャーアップグレードまたはマイナーアップグレードで変更される可能性があるため、以前のApplication Securityバージョンで作成されたフルテキスト(グローバル検索)インデックスは、26.2 Application Securityに移行した後は機能しません。推奨される方法は、既存のフルテキスト検索インデックスコンテンツを削除し、Application Security 26.2にそれらを再作成/再インデックスさせることです。

- Application Security 26.2の新規インストール: フルテキスト検索を有効にすると、インデックスが作成され、正常に機能します。
- Application Security 26.2への移行: 以前のフルテキスト検索インデックスは機能しません。フルテキストインデックスフォルダの内容を削除してApplication Securityを再起動すると、新しいインデックスが作成されます。

25.2から26.2への移行

1. 以前のバージョンのApplication Securityで、プロパティファイル `<fortify.home>/<app_context>/conf/app.properties` を編集してフルテキスト検索を無効にします。
2. フルテキスト検索インデックスフォルダの内容を削除します。
3. Application Security(以前のバージョン)を再起動します。
4. インデックスフォルダが作成されていないことを確認します。
5. Application Securityを26.2にアップグレードし、(プロパティファイルで)フルテキスト検索を再度有効化します。
6. Application Security 26.2を再起動します。
7. 新しいインデックスが作成されており、フルテキスト検索が正常に動作していることを確認します。

Note
膨大なデータの再インデックス化には時間がかかることがあります。ビッグデータのテスト中は以下を記録します。

- テストに使用されたデータベースのサイズ。
- インデックスの作成と再起動後の機能復旧に要した時間。

検証(アップグレード後)

Application Security UI内で、およびREST APIを使用して、以前使用したのと同じフルテキスト検索を実行し、結果が以前の動作や範囲と一致していることを確認します。

1.8.5. WARファイルの更新と展開

Application Security WARファイルを更新するには:

1. 現在デプロイされているApplication Security WARファイルをデプロイ解除します。

   手順については、Tomcatサーバのドキュメントを参照してください。

2. 新しいApplication Security WARファイルをデプロイします。

新しいWARファイルをデプロイした後、セットアップウィザードのステップと［**管理**］ビューでの設定タスクを完了します。詳細と手順については、アップグレード後のApplication Securityの設定および追加のApplication Security設定を参照してください。

1.8.6. アップグレード後のApplication Securityの設定

Application Securityをアップグレードした後、ブラウザウィンドウでApplication SecurityのWebアドレスを入力すると、セットアップウィザードが開きます。セットアップウィザードを使用して、データベースのデータマイグレーションを実行し、データベースに再度シードします。

Note

管理者にセットアップウィザードが使用可能になるのは、Application Securityを初めてデプロイした後、Application Securityをアップグレードした後、またはApplication Securityサーバを保守モードにした後(「Application Securityの保守モードへの移行」を参照)に限られます。

1. テキストエディタで *<fortify.home>*/*<app_context>*/init.token ファイルを開きます。
2. init.token ファイルの内容をクリップボードにコピーします。
3. Webブラウザを開き、Application SecurityサーバのURLを入力します。
4. ［**管理者(ADMINISTRATORS)**］をクリックします。
5. セットアップウィザードのサインインで、 init.token ファイルからコピーした文字列を［**セキュリティトークン(Security Token)**］フィールドに貼り付けてから、［**サインイン(SIGN IN)**］をクリックします。
6. ［**設定(CONFIGURATION)**］または［**コア環境設定(CORE CONFIGURATION SETTINGS)**］ページで環境設定に変更を加える必要がある場合は、「Application Securityの初回設定」に記載されている手順に従って変更できます。
7. ［**データベースセットアップ(DATABASE SETUP)**］ページに達するまで［**次へ(NEXT)**］をクリックします。
8. ［**データベースセットアップ(DATABASE SETUP)**］ページで、次の操作を行います。
    1. ［**DATABASE TYPE**］ボックスで、Application Securityデータベースタイプに一致するタイプを選択します。
    2. ［**DATABASE USERNAME**］ボックスに、Application Securityデータベースのユーザ名を入力します。

詳細については、「データベースユーザアカウントの許可」を参照してください。

3. ［**DATABASE PASSWORD**］ボックスに、Application Securityデータベースのパスワードを入力します。
4. ［**JDBC URL**］ボックスに、Application SecurityデータベースのURLを入力します。

> **Caution**
>
> JDBC URLに含まれるデータベース名(大文字と小文字を含む)は、Application Securityデータベース名と完全に一致している必要があります。

MariaDB JDBCドライバは、MySQLデータベースサーバに接続します。すべてのJDBC URLパラメータでは、MariaDBドライバ構文を使用する必要があります。正しい照合パラメータ構文の例:

```
jdbc:mysql://<host>:3306/<database_name>?
sessionVariables=collation_connection=<collation_name>
```

パラメータ `connectionCollation=<collation_name>` を `sessionVariables=collation_connection=<collation_name>` に置き換えます。

5. データベースへの接続をテストするには、［**TEST CONNECTION**］をクリックします。

   接続テストに失敗した場合は、`<fortify.home>/<app_context>/logs/ssc.log` ファイルをチェックして原因を突き止めます。

6. セットアップウィザードに正常に接続されたことが示されたら、警告と指示を読んでから、［**スクリプトをダウンロード(DOWNLOAD SCRIPT)**］をクリックします。
7. `ssc-migration.sql` スクリプトを保存して実行します。

   手順については、Application Securityデータベーステーブルおよびスキーマについてを参照してください。

> **Note**
>
> ソースデータベースのサイズによっては、データマイグレーションが完了するまで数時間かかる場合があります。

9. ssc-migration.sql スクリプトを実行した後、［**NEXT**］をクリックします。
10. ［**データベースのシード処理(DATABASE SEEDING)**］ページで、次の操作を行います。
    1. ［**参照(BROWSE)**］をクリックし、プロセスシードバンドルzipファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。
    2. ［**参照(BROWSE)**］をクリックし、レポートシードバンドルzipファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。
    3. (オプション)［**参照(BROWSE)**］をクリックし、PCI SSFシードバンドルzipファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。
    4. (オプション)［**参照(BROWSE)**］をクリックし、PCI基本シードバンドルzipファイルを見つけて選択してから、［**データベースにシード(SEED DATABASE)**］をクリックします。
11. ［**NEXT**］をクリックします。
12. ［**FINISH**］をクリックします。
13. Tomcatサーバを再起動します。

> **Tip**
>
> 後で環境設定を変更する必要がある場合は、Application Securityを保守モードに入れ、必要な変更を加えます。Application Securityを保守モードにする方法については、1ページの「Application Securityの保守モードへの移行を参照してください。

1.8.7. 期限切れライセンスの更新

Fortifyライセンスファイルを取得する方法については、「Application Securityファイルのダウンロードと解凍」を参照してください。

期限切れになった年間ライセンスを更新するには:

1. Tomcatサーバを停止します。
2. ダウンロードした `fortify.license` ファイルを*<fortify.home>*ディレクトリに配置します。
3. Tomcatサーバを再起動します。

1.8.8. 四半期ごとのOpenText SAST Application Security Contentで提供されるレポートシードバンドルを使用したデータベースのシード処理

OpenTextは、新しいセキュリティコンテンツをダウンロードできるようになった時点でユーザに通知します。この更新されたコンテンツに新しいシードバンドルが含まれるかどうかを確認するには、通知ドキュメントの見出し「**OpenText™ Security Fortify Premium Content**」の下を確認します。このセクションには、新しいシードバンドルの存在に関する情報が含まれています。新しいシードバンドルが含まれている場合は、それを使用してデータベースを再シードできます。シードバンドルとデータベースのシード処理の詳細については、Application Securityデータベースのシード処理についてを参照してください。

Important

更新された外部メタデータファイルには、レポーティングが依存するマッピングへの変更が含まれる場合があります。更新されたセキュリティコンテンツに新しいレポートシードバンドルが含まれる場合は、レポートを実行する前に、ルールとマッピングを更新してください。

Note

データベースをシード処理すると、新しいアプリケーションバージョンの作成と、レポートジョブおよび分析結果処理ジョブの実行がブロックされます。

四半期ごとのセキュリティコンテンツリリースから、データベースにレポートシードバンドルをシードするには、次の手順に従います。

1. 次のように、更新されたセキュリティコンテンツをダウンロードします。
    1. Application Securityカスタマポータルにログインします。
    2. ナビゲーションペインで［**プレミアムコンテンツ(PREMIUM CONTENT)**］を選択します。
    3. ［**EXCHANGE**］リンクをクリックします。
    4. 最新のレポートシードバンドルを選択してダウンロードします。
2. シードバンドルZIPファイルの内容を抽出します。
3. 管理者としてApplication Securityにサインインします。

4. ヘッダで、［**管理(Administration)**］を選択します。
5. ナビゲーションペインで、［**設定(Configuration)**］を展開し、［**シードバンドル(Seed Bundles)**］を選択します。
6. ［**シードバンドル(Seed Bundles)**］ページで、［**参照(BROWSE)**］をクリックし、`ReportBundle.zip` ファイルを見つけて選択します。
7. ［**SEED BUNDLES**］をクリックします。

参照情報

Application Securityデータベースのシード処理について

OpenText Application Security Softwareセキュリティコンテンツについて

Rulepack更新サーバによるRulepacksの更新

1.9. Application Securityの使用

開発チームはスキャンを実行する際に、定期的な分析結果をApplication Securityに送信します。セキュリティチームは、動的評価の定期的な結果をApplication Securityに送信します。

Application Securityは一定の期間にわたる分析結果と評価結果を相互に関連付けて追跡し、Audit Workbenchや、Fortify Plugin for Eclipse、Fortify Extension for Visual StudioなどのSecure Code Pluginsを通じて開発者が情報を入手できるようにします。

また、バグトラッキングシステムに問題を送信して、分析レポートを生成することもできます。

このセクションでは、次のトピックについて説明します。

1.9.1. Application Securityへのサインイン

Application Securityにサインインするには、Application Security管理者からインスタンスのWebアドレス、ユーザ名、およびパスワードを入手する必要があります。

初めてApplication Securityにサインインするには:

1. Webブラウザで、Application Securityインスタンスの次のWebアドレスを入力します。

   `<protocol>://<hostname>:<port>/<app_context>`

   ここで、 `<port>` はTomcatサーバが使用するポート番号を表します。

2. ユーザ名とパスワードを入力します。
3. ［**サインイン(SIGN IN)**］をクリックします。
4. Application Securityでパスワードの変更を求めるプロンプトが表示される場合は、パスワードを変更します。

1.9.1.1. セッションログアウトについて

ローカルログインを使用してサインインダイアログボックスからLDAPまたはローカルアカウントのユーザ名とパスワードでApplication Securityにサインインした場合、ログアウトする際に、Application Securityにはログアウト画面が表示されます。

シングルログアウトがサポートされているSSOアカウントを使用してサインインした場合は、ログアウトする際に、ローカルアカウントまたはSSOアカウントのいずれかからログアウトするためのセッションログアウト画面が表示されます。

Note

Application Securityは、SAMLのシングルログアウトをサポートしています。シングルサインオンおよびシングルログアウトの詳細については、「HTTPヘッダを使用するシングルサインオンおよびシングルログアウトソリューションの設定」を参照してください。

［**ローカルアカウントログアウト(LOCAL ACCOUNT LOGOUT)**］をクリックすると、Application Securityによって現在のセッションからログアウトされ、ログアウト画面が表示されます。

［**SSO LOGOUT**］をクリックすると、Application Securityからログアウトするほかに、シングルログアウトが実行され、SSOプロバイダからログアウトされます。

Note

Application Securityから完全にログアウトするには、すべてのブラウザウィンドウを閉じます。

非アクティブセッションのタイムアウト

非アクティブによって、セッションがタイムアウトに近付くと、Application Securityは次の2つのダイアログボックスのいずれかを表示します。

- ローカルログインを使用してログインダイアログボックスからユーザ名とパスワードでLDAPまたローカルアカウントにログインした場合、セッションがタイムアウトに近付くと、ログアウトするか、ログインされた状態を維持するかを選択するためのダイアログボックスが表示されます。

  ［**LOG OUT**］をクリックするか、非アクティブ状態が続いてセッションがタイムアウトすると、Application Securityによってセッションからログアウトされ、ログアウト画面が表示されます。

- シングルログアウトがサポートされているSSOプロバイダを通じてApplication Securityにログオンしている場合は、ローカルユーザアカウントからのログアウト、SSOログアウトの実行、ログインの続行のためのダイアログボックスが表示されます。

  ［**ローカルアカウントからのログアウト(LOCAL ACCOUNT LOGOUT)**］をクリックした場合、または非アクティブ状態が続いてセッションがタイムアウトになった場合は、Application Securityはユーザをセッションからのみログアウトしたうえで、ログアウト画面を表示します。

  ［**SSOログアウト(SSO LOGOUT)**］をクリックすると、Application Securityはユーザをセッションからログアウトした後、SSOプロバイダからログアウトします。

  セッションタイムアウトの設定方法については、コア設定の設定を参照してください。

Note

Application Securityから完全にログアウトするには、ブラウザ(すべてのタブ)を閉じます。

1.9.2. Application Securityへのアクセス権の要求

まだユーザアカウントを持っていない場合、またはユーザ名またはパスワードを忘れた場合は、サインインページから支援を求めることができます。

Application Securityへのアクセスを要求するには、次の手順に従います。

1. Webブラウザで、Application SecurityインスタンスのWebアドレスを入力します。
2. ［**アカウントにアクセスできない場合、またはアカウントが必要な場合(Can't access or need an account?)**］をクリックします。

   このボタンは、Application Security管理者が電子メール通知を有効にしている場合にのみ使用可能になります(「電子メールアラート通知設定の設定」を参照)。
   電子メールアラート通知設定の設定に加えて、［**ユーザ管理者の電子メールアドレス(ユーザアカウントの要求用) (User administrator's email address (for user account requests))**］を設定する必要があります(「コア設定の設定」を参照)。
3. 必要な情報を入力し、［**送信(SEND)**］をクリックします。

1.9.3. パスワードの変更

次の手順では、パスワードを変更する方法について説明します。ローカルアカウントを使用してログオンしている場合のみ、パスワードを変更できます。

パスワードを変更するには、次の手順を実行します。

1. Application Securityにサインインします。
2. ヘッダの［**プロファイルメニュー(Profile menu)**］から［**パスワード変更**］を選択します。

   ［**パスワード変更**］ダイアログボックスの［**保存(SAVE)**］ボタンは、ユーザ名や一般的なフレーズ(名前、映画や楽曲のタイトル、日付、数字、または文字のシーケンス)を含まない強力な新しいパスワードを入力してからでないと有効になりません。「myredhorsedance」のように無関係な単語を3から4つ組み合わせて使用すると、うまく機能します。パスワードが強力であると評価されると、そのパスワードを保存してサインインできるようになります。
3. 古いパスワードを入力し、新しいパスワードを入力して、新しいパスワードを確認します。
4. パスワードの強度が許容されたら、［**保存(SAVE)**］をクリックします。

1.9.4. システム全体およびアプリケーションバージョンのすべてにわたる初期設定の設定

システム全体の動作、およびアプリケーションバージョン間の環境設定ができます。

システム全体の設定をするには、次の手順に従います。

1. ヘッダの［**プロファイルメニュー(Profile menu)**］から［**初期設定(Preferences)**］を選択します。
2. システム全体に適用する環境設定を行うには、［**初期設定(PREFERENCES)**］ダイアログボックスの［**システム全体の初期設定(System-wide Preferences)**］で、次の操作を行います。
    1. 有効にする機能のチェックボックスをオンにして、無効にする機能のチェックボックスをオフにします。
    2. デフォルトのMM/DD/YYYY日付フォーマットではなくYYYY/MMDD日付フォーマットを適用するには、それを［**日付フォーマット(Date format)**］リストから選択します。
    3. デフォルトの12時間AM/PMフォーマットではなく24時間フォーマットを適用するには、［**時刻フォーマット(Time format)**］リストから選択します。
    4. テーマを変更するには、［**UIテーマ(UI Theme)**］一覧から、［ライト(Light)］、［ダーク(Dark)］、［自動(Automatic)］のいずれかを選択します。

    > **Note**
    >
    > ［自動(Automatic)］テーマを適用する場合、テーマはオペレーティングシステムまたはブラウザテーマに基づいて設定されます。

3. すべてのアプリケーションバージョンの環境設定を設定するには、次の手順に従います。

> **Note**
>
> 特定のアプリケーションバージョンを対象に、上記の設定を上書きするには、［**アプリケーションプロファイル(Application Profile)**］の［**詳細オプション(Advanced Options)**］に変更を加えます。

1. ［**監査(AUDIT)**］ページの問題リストに抑止された問題を含めるには、［**抑止された問題を表示(Show suppressed issues)**］チェックボックスをオンにします。
2. ［**監査(AUDIT)**］ページに削除された問題を含めるには、［**削除された問題を表示(Show removed issues)**］チェックボックスをオンにします。
3. ［**監査(AUDIT)**］ページに非表示にされた問題を含めるには、［**非表示にされた問題を表示(Show hidden issues)**］チェックボックスをオンにします。
4. ［**監査(AUDIT)**］ページの問題リストに短いファイル名を表示するには、［**短縮ファイル名を使用(Use short file names)**］チェックボックスをオンにします。

4. ［**保存(SAVE)**］をクリックします。

1.9.5. キーボードホットキーの表示

Application Securityユーザインタフェースの操作に使用するキーボードホットキーを表示するには:

1. Application Securityにサインインします。
2. 次のいずれかを実行します。
    - ヘッダの［**プロファイルメニュー(Profile menu)**］から［**ホットキー(Hotkeys)**］を選択します。
    - キーボードで「**?**」を押します。

参照情報

システム全体およびアプリケーションバージョンのすべてにわたる初期設定の設定

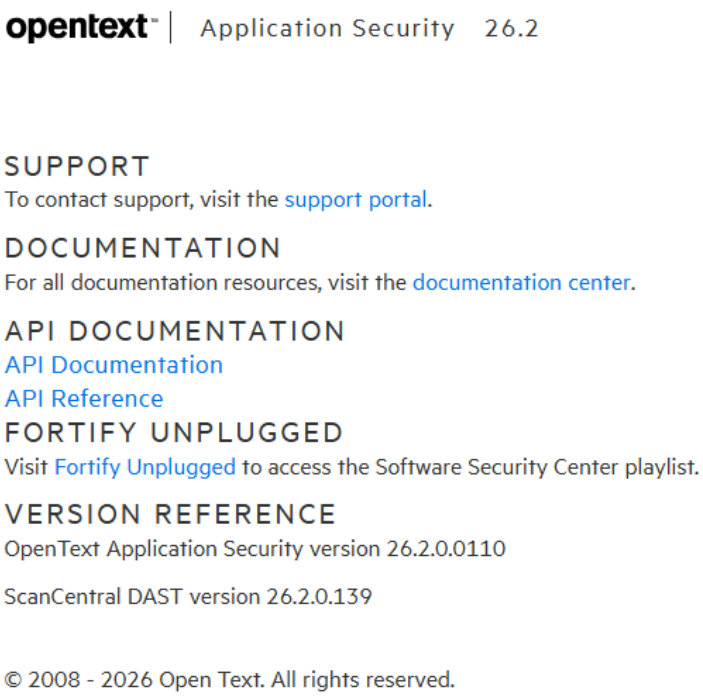
1.9.6. APIドキュメントにアクセスする

Important

外部アプリケーションからApplication Security APIを呼び出すと、Application Securityインスタンスに悪影響を及ぼす可能性があります。OpenTextでは、外部アプリケーションのサポートを提供していません。外部呼び出しによってインスタンスのパフォーマンスが低下している場合、OpenTextでは、直接的な外部呼び出しを中止し、間接的にApplication Securityと統合する別の方法を実装することを推奨しています。そのための支援として、スペシャリストサービスを利用できます。

Application Security APIドキュメントにアクセスするには、次の手順を実行します。

1. ヘッダで［**ヘルプ**］ボタンをクリックします。



2. ［**APIドキュメント(API Documentation)**］リンクをクリックします。

Application Security APIドキュメントWebページがブラウザに開きます。

Tip

Chrome DevToolsなどのプロキシを利用してApplication Securityトラフィックを傍受し、ユーザインタフェースのアクションを実行するのに適切なエンドポイント呼び出しを特定すると役立ちます。

1.9.7. Application Securityダッシュボードについて

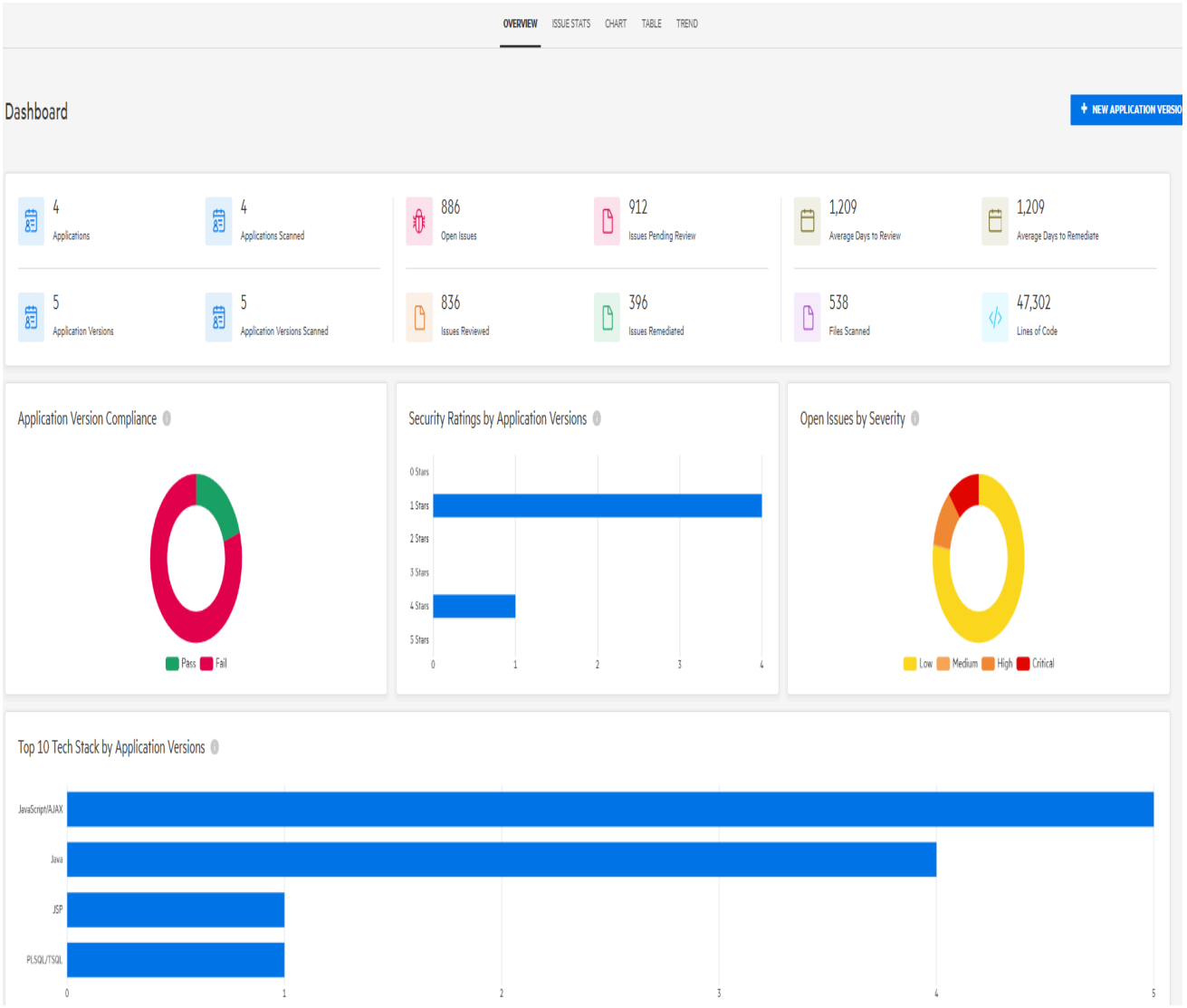
Application Securityにサインインすると、［**ダッシュボード(Dashboard)**］ビューに、ユーザがアクセスできるアプリケーションバージョンのうち、組織に最大のビジネスリスクをもたらす可能性のあるバージョンのデータが表示されます。

このセクションで説明するトピック:

1.9.7.1. 概要

OpenText™ Application Securityに初めてサインインすると、［**ダッシュボード**］ビューに［**概要**］ページが表示されます。このページでは主要な指標が視覚的に表示されるため、アプリケーションセキュリティプログラムの全体像を把握できます。

［**概要**］ページには、アクセス可能なすべてのアプリケーションバージョンに関するアプリケーションバージョン、コード分析、問題管理の概要が表示されます。最大500個のアプリケーションバージョンを含む標準データセットでは、ナビゲーション後数秒以内にすべての指標とグラフがレンダリングされます。ブラウザを手動で更新することで、重複やレンダリングの問題が発生することなく最新のデータが表示されるようになります。



［**概要**］ページには、アクセス可能なすべてのアプリケーションバージョンに関する以下の指標が表示されます。

指標	説明(Description)
アプリケーション	バージョン付きアプリケーションの総数
アプリケーションバージョン	アプリケーションバージョンの総数
スキャンされたアプリケーション	スキャンされたバージョンを含むアプリケーションの総数
スキャンされたアプリケーションバージョン	スキャンされたアプリケーションバージョンの総数
未解決の問題*	全アプリケーションバージョンにおける未解決問題の総数
レビュー待ちの問題*	レビュー待ちの問題の総数
レビューされた問題*	レビューされた問題の総数
修正された問題*	修正された問題の総数
レビューにかかる平均日数	問題のレビューにかかる平均日数。この値には、小数点以下1桁までの数字が含まれる場合があります。
スキャンされたファイル	全アプリケーションバージョンにおけるスキャンされたファイルの総数
修正にかかる平均時間	問題の修正にかかる平均日数。この値には、小数点以下1桁までの数字が含まれる場合があります。
コードの行数	分析されるコード行の総数

* 集計において同じ問題が複数回カウントされることを避けるため、問題の件数は一意のインスタンスIDに基づいてカウントされます。

グラフィカル表現

［**概要**］ページには以下のグラフィカル表現が含まれています。

アプリケーションバージョンのコンプライアンス

［**Application Version Compliance(アプリケーションバージョンのコンプライアンス)**］ドーナツグラフには、セキュリティ評価に基づいて全アプリケーションバージョンのコンプライアンスステータスが表示されます。

- 合格：セキュリティ評価が3つ星、4つ星、または5つ星のアプリケーションバージョン
- 不合格：セキュリティ評価が0つ星、1つ星、または2つ星のアプリケーションバージョン

各セグメントにカーソルを合わせると、セグメントラベル(合格または不合格)とアプリケーションバージョンのカウントが表示されます。

アプリケーションバージョンごとのセキュリティ評価

［**Security Ratings by Application Versions(アプリケーションバージョンごとのセキュリティ評価)**］横棒グラフには、セキュリティ評価(0～5つ星)ごとにグループ化されたアプリケーションバージョンのカウントが表示されます。各バーにカーソルを合わせると、セキュリティ評価とアプリケーションバージョンのカウントが表示されます。

重大度ごとの未解決の問題

［**Open Issues by Severity(重大度ごとの未解決の問題)**］ドーナツグラフには 、以下の重大度ごとに未解決の問題が表示されます。

- 重大
- High
- Medium
- Low

各セグメントにカーソルを合わせると、問題の重大度とカウントが表示されます。

アプリケーションバージョンごとのテクノロジースタックトップ10

［**Top 10 Tech Stacks by Application Versions(アプリケーションバージョンごとのテクノロジースタックトップ10)**］横棒グラフには、アプリケーションバージョン数が最も多いテクノロジースタックトップ10(メインのプログラミング言語またはフレームワーク)が表示されます。存在するテクノロジースタックが10個未満の場合、グラフには空のフィラーバーなしで利用可能なスタックのみが表示されます。バーは、アプリケーションバージョン数を基準に降順で並べられます。各バーにカーソルを合わせると、テクノロジースタック名とアプリケーションバージョンのカウントが表示されます。

次も参照

新しいアプリケーションの最初のバージョンの作成

アラートの表示とマーク

1.9.7.2. 問題統計

［**ダッシュボード(Dashboard)**］ビューの［**問題統計(ISSUE STATS)**ページには、ユーザがアクセスできるアプリケーションバージョンの問題に関するサマリ情報として、問題を確認して修復するまでにかかる平均日数などが表示されます。問題の処理の速さについて視覚的な手がかりを提供するために、［**問題統計(ISSUE STATS)**］ページには［**平均レビュー日数(Average Days to Review)**］と［**平均修復日数(Average Days to Remediate)**］の値の横に色付きバーが表示されます。カラーバーは問題管理の期間を示しています。

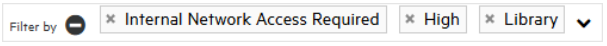
Note

管理者またはセキュリティリードは、ユーザが［**問題統計(ISSUE STATS)**］ページで情報を確認するときに表示される情報を決定するしきい値を設定できます。詳細については、「問題統計しきい値の設定」を参照してください。

テーブルに一覧表示されているアプリケーションバージョンをクリックすると、Application Securityで、そのアプリケーションバージョンの［**監査(AUDIT)**］ページに直接移動できます。データにフィルタは適用されません。

［**ダッシュボード(Dashboard)**］ビューには、表示されるサマリデータを絞り込むための3つの設定が用意されています。これらの設定は、単独で使用することも、組み合わせて使用することもできます。

表示設定	説明(Description)
アプリケーション属性によるグループ化 (Group by an application attribute)	［**グループ化条件(Group by)**］リストから属性を選択します。デフォルトでグループ化に使用される属性は、アプリケーションバージョンです。 ［**ダッシュボード(Dashboard)**］ビューには、選択したグループ化属性に加えて、［**集計条件(Aggregate by)**］リストおよび［**フィルタ条件(Filter by)**］リストから選択した属性を反映するデータが表示されます。 **Note** ［**Group by**］リストに(単一選択タイプの)カスタム属性が含まれる場合は、表示されるデータを細かく制御できます。カスタム属性の作成方法については、カスタム属性の作成を参照してください。

表示設定	説明(Description)
アプリケーション属性による集計 (Aggregate by an application attribute)	［**集計条件(Aggregate by)**］リストから属性を選択します。［**ダッシュボード(Dashboard)**］ビューに、集計属性と、［**グループ化条件(Group by)**］リストおよび［**フィルタ条件(Filter by)**］リストから選択した属性に基づいてデータが表示されます。 **Note** ［**Aggregate by**］リストに(単一選択タイプの)カスタム属性が含まれる場合は、表示されるデータを細かく制御できます。カスタム属性の作成方法については、カスタム属性の作成を参照してください。
1つ以上のアプリケーション属性によるフィルタ処理(Filter by one or more application attributes)	［**フィルタ条件(Filter by)**］リストから属性を選択します。複数の属性を条件にフィルタ処理を行うことができますが、1度に1つずつ選択する必要があります。  ［**ダッシュボード(Dashboard)**］ビューに、フィルタ属性と、［**グループ化条件(Group by)**］リストおよび［**集計条件(Aggregate by)**］リストから選択した属性に基づいてデータが表示されます。

リストから選択した属性をクリアするには、［**すべてクリア(Clear all)**］ボタンをクリックします。

［**問題統計(ISSUE STATS)**］ページおよび［**監査(AUDIT)**］ページに表示されるApplication Securityデータをカンマ区切り値(CSV)ファイルにエクスポートできます。詳細については、「データのカンマ区切り値ファイルへのエクスポート」を参照してください。

1.9.7.3. アプリケーションバージョンの高レベルのサマリメトリックを表示する

アプリケーションバージョンのサマリメトリックスを(個別に、またはまとめて)表示するには:

- ヘッダで、［**ダッシュボード(Dashboard)**］を選択します。

［**問題統計(Issue Stats)**］ページの次の3つのタイルに、ユーザがアクセスできるすべてのアプリケーションの統合メトリックが表示されます。

- ［**修復された問題(Issues Remediated)**］タイルには、現在までに修正された問題の合計数、レビューにかかった平均日数、および修正の平均所要日数が表示されます。
- ［**レビューが保留中の問題(Issues Pending Review)**］タイルには、未解決の問題の合計数と、確認済みの問題の数が表示されます。
- ［**アプリケーション(Application versions)**］タイルには、ユーザがアクセスできるアプリケーションバージョンの合計数と、それらのアプリケーションバージョンでスキャンされたファイルの数およびスキャンされたコードの行数が表示されます。

［**問題統計(Issue Stats)**］ページのテーブルには、ユーザがアクセスできる各アプリケーションバージョンのサマリメトリックが表示されます。テーブルに一覧表示されているアプリケーションバージョンをクリックすると、そのアプリケーションバージョンの［**監査(AUDIT)**］ページに直接移動します。

参照情報

アプリケーションバージョンのサマリメトリック(グラフ形式)を表示する

スキャン結果の監査

特定のアプリケーションバージョンの高レベルのサマリメトリックを表示する

1.9.7.4. アプリケーションバージョンの高レベルのサマリメトリック(グラフ形式)を表示する

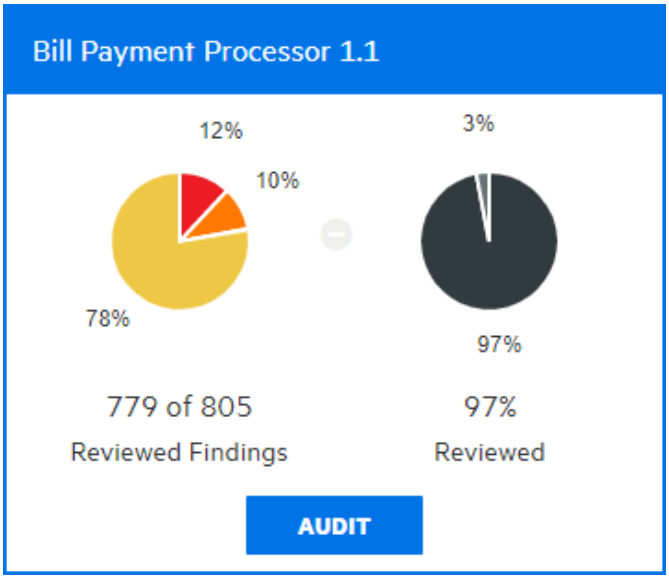
［**チャート(CHART)**］ページから、個々のアプリケーションバージョンの高レベルのサマリメトリックをグラフ形式で表示できます。

［**チャート(CHART)**］ページからアプリケーションバージョンのサマリメトリックを表示するには:

1. ［**ダッシュボード(Dashboard)**］ビューで、［**チャート(CHART)**］をクリックします。

   Application Securityで、［**REVIEWED**］タブが開きます。

2. アプリケーションバージョンのリストで、アプリケーションバージョンの色付きバーをポイントすると、そのバージョンのサマリ結果が表示されます。



   この例では、左側の円グラフに、このアプリケーションバージョンについて現在までに監査された結果の97% (805件のうちの779件)のセキュリティ評価が表示されています。右側のグラフには、監査された結果の割合(97)と、まだ監査されていない結果の割合(3)が表示されています。

3. アプリケーションバージョンの［**監査(AUDIT)**］ページに移動するには、［**監査(AUDIT)**］をクリックします。

参照情報

アプリケーションバージョンのサマリメトリックを表示する

スキャン結果の監査

特定のアプリケーションバージョンのサマリメトリックを表示する

1.9.7.5. ダッシュボードサマリテーブルをエクスポートする

すべてのアプリケーションバージョンのデータをカンマ区切り値(CSV)ファイルにエクスポートできます。システムがCSVファイルを保持する期間を確認するには、「ジョブスケジューラの設定」を参照してください。

［**ダッシュボード(Dashboard)**］ビューに表示されるサマリテーブルをエクスポートするには:

1. ヘッダで［**ダッシュボード(Dashboard)**］、［**問題統計(ISSUE STATS)**］の順に選択します。
2. ［**ダッシュボード(Dashboard)**］のツールバーで、［**エクスポート(EXPORT)**］をクリックします。

   > **Note**
   >
   > ［**エクスポート(EXPORT)**］ボタンが無効になっている場合、これは管理者によってこの機能が無効にされていることを意味します。

3. ［**ファイル名(File name)**］ボックスに、ファイルの名前を入力します。
4. (オプション)［**ノート(Notes)**］ボックスに、エクスポートするデータに関する情報を入力します。
5. ［**保存(SAVE)**］をクリックします。
6. エクスポートされた結果を表示するには:
   1. ヘッダで、［**レポート**］をクリックします。
   2. ［**データエクスポート(DATA EXPORTS)**］をクリックします。
   3. ［**問題統計(Issue Stats)**］テーブルで、エクスポートされたファイルの行をポイントして［**ダウンロード(Download)**］ボタンをクリックします。

参照情報

アプリケーションバージョンの選択したデータをCSVファイルにエクスポートする

1.10. ユーザアカウントの管理

新しいApplication Securityインストールのプライマリシステム管理者は、セキュアな展開ガイドライン(「セキュリティ保護された展開の提供」を参照)の説明に従って、デフォルト以外の管理者レベルのアカウントを作成してから、デフォルトの管理者アカウントを削除します。追加のApplication Securityユーザアカウントを作成するには、デフォルト以外のApplication Security管理者アカウントを使用します。

このセクションでは、Application Securityの役割、ユーザアカウント管理、Application SecurityにLDAPエンティティを登録する方法、およびMicrosoft Entra IDとの統合を設定する方法について説明します。

このセクションでは、次のトピックについて説明します。

1.10.1. チームのトラッキングについて

管理者またはセキュリティリードは、チームの進捗状況をトラックして監視するための情報にアクセスして、優れたアプリケーションセキュリティプラクティスが実施および順守されていることを確認する必要があります。Application Securityは、優れたセキュリティプラクティスの採用を促進するための中心的な役割を果たします。情報がどのようにトラックおよびレポートされるのかを理解することにより、アプリケーションセキュリティ規格に基づいて開発チームの進捗状況を正確に測定できます。

1.10.2. 役割について

役割により、ユーザがApplication Securityで実行できるアクションが決定されます。

Application Security機能へのユーザアクセスを細かく制御するには、カスタム役割を作成し、Application Securityインタフェースから許可を割り当てることができます。役割の作成方法については、「カスタム役割の作成」を参照してください。

1.10.2.1. 事前設定済みの役割

次の表は、Application Securityでユーザに割り当て可能な事前設定済みの役割を一覧表示しています。役割は権限レベルの降順で一覧表示されています。事前設定済みの各役割に関連付けられている許可を表示する方法については、「Application Securityの役割に関する許可情報の表示」を参照してください。

役割	説明(Description)
管理者	システムおよびすべての結果へのフルアクセス権を保持
セキュリティリード	アプリケーションのバージョンとユーザを作成できるセキュリティチームメンバー
マネージャ	開発者による結果の処理を指導する責任 マネージャはアプリケーションを作成できませんが、チームメンバーへのアクセス権を付与または取り消しできます。
開発者	セキュリティの結果を生成し、セキュリティの問題を選別または修正するアクションを取る責任を負う開発者
表示のみ	結果を表示できますが、問題の選別や修正プロセスに干渉することはできません。 ユーザの例: システム自動化アカウントまたは一時監査官
アプリケーションセキュリティテスタ	次を含む動的スキャン要求の実行に必要なタスクを実行できます。 • アプリケーションバージョンの表示 • レポートの表示と生成 • 動的スキャンの処理 • 分析結果のアップロード • 問題の監査

役割	説明(Description)
WebInspect Enterprise System	Fortify WebInspect EnterpriseインスタンスをApplication Securityに接続し、問題の監査情報を取得できます。 この役割は、WebInspect Enterpriseインスタンスによる使用のみを意図しています。
ScanCentral SASTコントローラ	スキャンを実行する許可を持っているものの、「分析結果のアップロード」許可を持っていないユーザの代わりに、スキャンをFortify ScanCentral SASTからApplication Securityにアップロードできます。この役割は、ScanCentral SASTコントローラを設定する場合にのみ使用します。詳細については、『*OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド*』を参照してください。
ScanCentral DASTコントローラ	この役割は、ScanCentral DASTコントローラを設定する場合にのみ使用します。詳細については、『*OpenText ScanCentral™ DAST設定および使用ガイド*』を参照してください。

参照情報

役割について

カスタム役割の作成

1.10.2.2. カスタム役割の作成

独自の役割を定義し、許可を割り当てることができます。

新しい役割の許可を定義および設定するには、次の手順を実行します。

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**役割(Roles)**］を選択します。
4. ［**役割(Roles)**］ページで、［**新規(NEW)**］をクリックします。
5. ［ **新しい役割の作成(CREATE NEW ROLE)**］ダイアログボックスで、次の表に示す情報を入力します。

Important

［**名前(Name)**］フィールドと［**説明(Description)**］フィールドの改行を除き、値は、文字 `=` 、 `-` 、 `+` 、または `@` で始めることはできません。また、制御文字を含めることはできません。制限されている範囲に含まれるUnicode文字の完全なリストについては、「ASCIIおよびUnicodeでの制御文字」を参照してください。

フィールド	説明(Description)
名前(Name)	役割名
説明(Description)	(オプションだが、推奨)役割の説明
Universal access	すべてのアプリケーションバージョンに新しい役割アクセスを割り当てるには、このチェックボックスをオンにします。 **Note** 管理者レベルのユーザにのみユニバーサルアクセスを選択することを強く推奨します。

6. 許可を追加するには、［**+許可の追加(+ADD PERMISSIONS)**］をクリックします。

   許可は、この役割のユーザが使用できる機能領域を指定します。

7. ［**許可の追加(ADD PERMISSIONS)**］ダイアログボックスで、テーブルをスクロールし、新しい役割に付与する許可に対応するチェックボックスをオンにします。

8. ［**DONE**］をクリックします。

   選択したいずれかの許可に追加の許可が必要な場合は、警告記号⚠付きで一覧表示されます。

9. 必要な依存関係を新しい役割に追加するには、［**欠けている許可の追加(ADD MISSING PERMISSIONS)**］をクリックします。

   ［**新しい役割の作成(CREATE NEW ROLE)**］ダイアログボックスに、依存関係のある追加の許可が一覧表示されます。

10. ［**保存(SAVE)**］をクリックします。

Tip

また、カスタム役割を編集するときに、欠けている許可を追加できます。

Application Securityでは、互換性のないことが判明している状態に対して保護する許可をチェックします。選択した役割と許可が競合しない場合は、［**Roles**］ページに戻り、新しい役割に関する詳細情報が表示されます。

1.10.2.3. カスタム役割の削除

［**役割(Roles)**］ページに一覧表示されているカスタム役割がどのユーザアカウントにも割り当てられていない場合は、その役割を削除できます。

役割を削除するには、次の手順を実行します。

1. Application Securityに管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**役割(Roles)**］を選択します。
4. テーブルで、削除するカスタムロールの左側にあるチェックボックスをオンにします。
5. ［**Roles**］ツールバーで［**DELETE**］をクリックします。
6. ［**OK**］をクリックして、カスタム役割の削除を確認します。

参照情報

カスタム役割の作成

1.10.3. アカウント管理

管理者アカウントを持つユーザだけが、新しいユーザアカウントを作成したり、既存のアカウントの情報を編集したりできます。管理者アカウントを使用してApplication Securityシステムを管理します。ローカルまたはLDAP Application Securityユーザアカウントの作成と編集に必要な管理者レベルアカウントのみを作成することを推奨します。セキュリティリードおよびそれ以下のアカウントは、他のすべてのアプリケーション関連アクティビティを実行できます。

Application Securityでは、管理者レベルアカウントをアプリケーションバージョンに明示的に追加できます。これにより、［**監査(AUDIT)**］ページから管理者に問題を割り当てることができます。

このセクションで説明するトピック:

1.10.3.1. ローカルユーザアカウントの作成

管理者は、新しいローカルユーザアカウントをApplication Securityに追加できます。

> **Important**
>
> Application Securityから外部管理ユーザは作成できません。これらは、SCIM APIを使用してのみプロビジョニングできます。

Application Securityユーザアカウントを作成するには、次の手順に従います。

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**ローカルユーザ(Local Users)**］を選択します。
4. ［**ローカルユーザ(Local Users)**］ツールバーで、［**+追加(+ADD)**］をクリックします。
5. ［**新しいユーザの作成(CREATE NEW USER)**］ダイアログボックスで、次の表に示す情報を入力します。

   > **Important**
   >
   > 次の表でアスタリスク(*)で示されているフィールドの値は、文字 `=`、`-`、`+`、または `@` で始めることはできません。また、制御文字を含めることはできません。

フィールド	説明(Description)
*ユーザ名(Username)	アカウントのユーザ名。
*名(First Name)	(オプションですが、強く推奨)ユーザの名。
*姓(Last Name)	(オプションですが、強く推奨)ユーザの姓。
*電子メール(Email)	(オプション)ユーザの電子メールアドレス。 **Note** 電子メールアドレスは必要ありませんが、ユーザが電子メールアラートおよび通知を受信するには、電子メールアドレスを指定する必要があります。
Password	新しいユーザアカウントのパスワード。 ［**Password Strength**］インジケータは、入力したパスワードの相対強度を表示します。ユーザアカウント情報を保存できるのは、パスワードが強力または非常に強力と評価された場合のみです。

フィールド	説明(Description)
Confirm Password	新しいユーザアカウントのパスワード。
User must change password at next login	Application Securityへの次回のサインイン時にユーザにパスワードの変更を要求する場合は、このチェックボックスをオンのままにします。
Password never expires	このチェックボックスを選択すると、ユーザが変更するまで最初に割り当てられたパスワードを使用できます。 ユーザに30日ごとにパスワードの変更を要求するには、このチェックボックスをオフのままにします。
Suspended	このユーザアカウントからApplication Securityへのアクセスを一時停止するには、このチェックボックスをオンにします。

フィールド	説明(Description)
役割	(オプションですが、強く推奨)ユーザアカウントに割り当てるすべての役割のチェックボックスをオンにします。 **Caution** これはオプションですが、役割が割り当てられていないユーザは、そのユーザが役割を割り当てられたローカルグループに属していない限り、Application Securityにアクセスできません。

フィールド	説明(Description)
Access	新しいユーザがアクセスできるアプリケーションを指定するには、次の手順に従います。 **Note** **管理者**または**WebInspect Enterprise System**の役割をユーザに割り当てた場合、そのユーザはすべてのApplication Securityアプリケーションに対するユニバーサルアクセス権を持ちます。 1. ［**ADD**］をクリックします。 2. ［**Application**］リストから、ユーザがアクセスできるアプリケーションを選択します。 中央ペインの［**VERSIONS**］リストには、選択したアプリケーションのアクティブなバージョンすべてが表示されます。 3. ユーザがアクセスできるすべてのバージョンのチェックボックスをオンにします。 すべてのバージョンを選択するには、［**Select all**］チェックボックスをオンにします。 ［**選択済みバージョン (SELECTED VERSIONS)**］ペインには、選択したバージョンが一覧表示されます。

フィールド	説明(Description)
	4. 別のアプリケーションバージョン(複数可)を追加するには、bとcのステップを繰り返します。 5. ［**DONE**］をクリックします。

6. 次のいずれかを実行します。
   - 設定を保存して別のユーザを作成するには、［**保存して別のものを追加(SAVE AND ADD ANOTHER)**］をクリックします。
   - 設定を保存し、［**新しいユーザの作成(CREATE NEW USER)**］ダイアログボックスを閉じるには、［**保存(SAVE)**］をクリックします。

参照情報

ローカルユーザアカウントを編集する

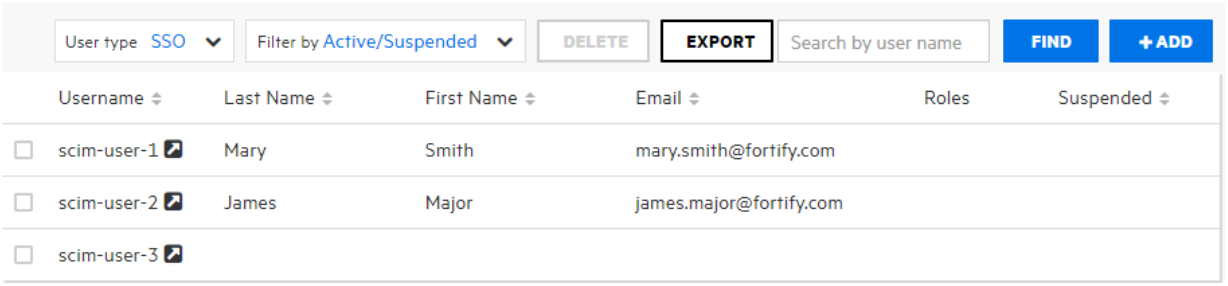
ローカルユーザアカウントのロック解除

1.10.3.2. ローカルユーザアカウントを編集する

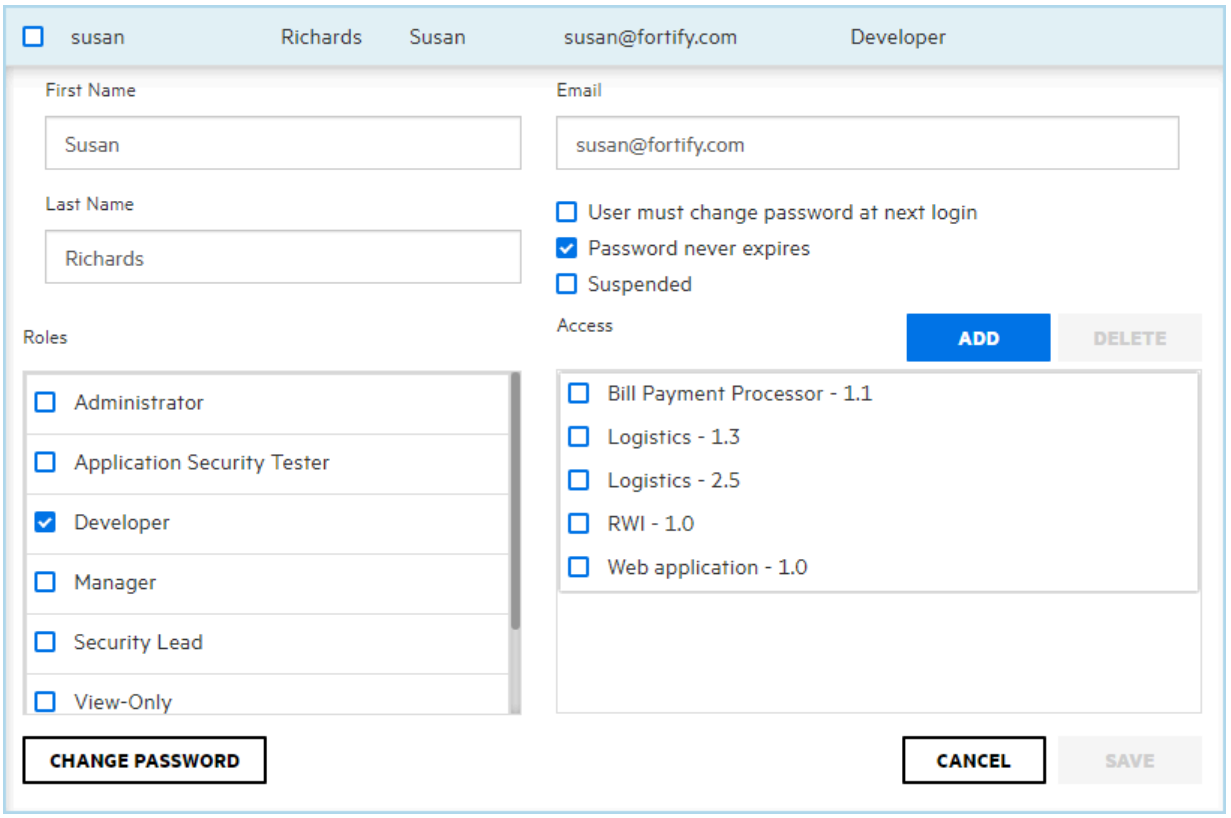
次の手順では、Application Securityから作成されたローカルユーザアカウントと、SCIM APIを使用してプロビジョニングされたユーザアカウントのアカウントを編集する方法について説明します。

ローカルユーザアカウントを編集するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**ローカルユーザ(Local Users)**］をクリックします。
3. 外部で管理されている(SCIM APIを使用してプロビジョニングされた)ユーザを選択的に表示するには、［**ユーザタイプ(User type)**］リストから［**SSO**］を選択します。



4. 編集するユーザアカウントを探し、行をクリックして展開し、アカウントの詳細を表示します。
5. ［**編集(EDIT)**］をクリックします。



6. ［**First Name**］、［**Last Name**］、および［**Email**］の各ボックスの値に必要な変更を加えます。

> **Important**
>
> ［**名(First Name)**］、［**姓(Last Name)**］、および［**電子メール(Email)**］フィールドの値は、文字 `=`、`-`、`+`、または `@` で始めることはできません。また、制御文字を含めることはできません。これらの範囲に含まれるUnicode文字の完全なリストについては、「Control characters in ASCII and Unicode」を参照してください。

> **Important**
>
> Application Securityから、外部で管理されるユーザおよびグループアカウントに対して行える変更は、役割とアプリケーションバージョンの割り当てのみです。Entra IDから他のすべての設定(および削除)を実行する必要があります。

7. 電子メールアドレスのパスワード有効期限ポリシーを変更するには、［**電子メール(Email)**］ボックスの下のチェックボックスをオンまたはオフにします。
8. ユーザに割り当てられた役割を変更するには、［**役割(Roles)**］エリアで、選択可能な役割のチェックボックスをオンまたはオフにします。

9. アプリケーションバージョンからユーザを削除するには、［**アクセス(Access)**］エリアで、アプリケーションバージョンのチェックボックスをオンにして、［**削除(DELETE)**］をクリックします。ユーザを別のアプリケーションバージョンに割り当てるには、［**追加(ADD)**］をクリックし、ユーザがアクセスできるアプリケーションバージョンを指定します。
10. ユーザのパスワードを変更するには、［**パスワード変更(CHANGE PASSWORD)**］をクリックしてから、新しいパスワードを指定します。

    外部で管理されているユーザの場合、［**パスワード変更(CHANGE PASSWORD)**］ボタンは使用できません。
11. ［**保存(SAVE)**］をクリックします。

参照情報

ローカルユーザアカウントのロック解除

ローカルユーザアカウントの作成

1.10.3.3. ローカルユーザアカウントのロック解除

ローカルユーザが3回連続してサインインに失敗すると、Application Securityはユーザがそれ以上のサインインを試みるのを防ぎます。電子メール通知が有効な場合、ユーザがロックアウトされており、Application Security管理者に通知する必要があることを助言する電子メールをユーザは受け取ります。管理者は、ユーザのアカウントのロックを解除できます。

Note

ユーザアカウントのロックとロック解除は、SCIM APIによってプロビジョニングされたユーザには適用されません。

ユーザが自分のアカウントからロックアウトされたという通知を受け取った後、次のようにアカウントのロックを解除します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**ローカルユーザ(Local Users)**］をクリックします。
3. ロックを解除するユーザアカウントを探して、行をクリックして展開します。
4. ［**ユーザのロックを解除する(UNLOCK USER)**］をクリックします。
5. ユーザアカウントのロック解除を確認するには、［**OK**］をクリックします。

参照情報

ローカルユーザアカウントの作成

ローカルユーザアカウントを編集する

1.10.3.4. 外部管理されたユーザおよびグループを表示する

SCIM APIを使用してプロビジョニングされた外部管理ユーザを表示するには:

1. ローカル管理者としてログインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**ローカルユーザ(Local Users)**］を選択します。
4. ［**ローカルユーザ(Local Users)**］ページの上部にある［**ユーザタイプ(User type)**］リストから、［**SSO**］を選択します。

   Application Securityに、SCIM APIを使用してプロビジョニングされたユーザが一覧表示されます。［**外部管理されたユーザ(Externally managed user)**］シンボル( )が、［**ローカルユーザ(Local Users)**］テーブルに一覧表示されている各ユーザ名の横に表示されます。

Entra IDからプッシュされたグループを表示するには:

1. Application Securityにローカル管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**ローカルグループ(Local Groups)**］を選択します。

外部管理されたユーザおよびグループに役割を割り当てる

Entra IDなどのアイデンティティ管理サービスからプロビジョニングされたローカルグループのユーザまたはメンバーは、そのグループに1つ以上の役割が割り当てられているか、［**ローカルユーザ(Local Users)**］ページからユーザに個別に役割が割り当てられているのでない限り、Application Securityにアクセスできません。

Important

Application Securityから、外部で管理されるユーザおよびグループアカウントに対して行える変更は、役割とアプリケーションバージョンの割り当てのみです。Entra IDから他のすべての設定(および削除)を実行する必要があります。

外部管理されたユーザおよびグループへの役割の割り当ては、［**管理(Administration)**］ビューで作成したローカルユーザへ割り当てるのと同じように行います。

参照情報

SCIM 2.0プロトコルの実装

SCIMによる外部管理されたユーザおよびグループのプロビジョニングの有効化

SCIM 2.0およびSAML 2.0を使用したユーザプロビジョニング用のMicrosoft Entra IDへの接続の設定

SAML 2.0準拠のシングルサインオンを使用するためのApplication Securityの設定

1.11. アプリケーションとアプリケーションバージョン

一貫した測定結果を得るために、単一のコードベースを対象にアプリケーションを定義します。Application Securityでは、コードベースの反復的な開発と修正を「アプリケーション」と「アプリケーションバージョン」に編成します。

- アプリケーションは、1つ以上のアプリケーションバージョンのコンテナとして機能するコードベースです。新しいコードベースを使用する場合は、新しいApplication Securityアプリケーションを作成します。Application Securityでは、そのアプリケーションの最初のバージョンを自動的に作成します。
- アプリケーションバージョンは、最終的に展開されるアプリケーションまたはコードベースのインスタンスです。アプリケーションコードベースの特定バージョンのデータ、監査、および属性が含まれています。既存のコードベースを使用している場合は、新しいアプリケーションではなく新しいアプリケーションバージョンを作成します。

アプリケーションバージョンは、チームトラッキングの基本ユニットです。開発者の目の前で情報を取得したりレポートやパフォーマンスインジケータを生成したりする際に役立つ、セキュリティ結果の保存先になります。アプリケーションバージョンのコード分析結果は、次の表に示すようにトラッキングされます。

既存の分析結果	+新規分析結果	=トレンド結果
OpenText SAST (Fortify Static Code Analyzer)、OpenText DAST (Fortify WebInspect)、または他のアナライザから得られた以前のセキュリティ分析の結果	このスキャンを実行するために使用したものと同じアナライザからの既存の結果とマージする 解決済み問題をマークする 新しい問題を特定する 変更されていない問題を保持する	修復されたセキュリティ問題と未解決の問題を特定する

分析処理ルールにより、新しいスキャンが以前のスキャンに匹敵するものであることが検証されます。

このセクションでは、次のトピックについて説明します。

1.11.1. 開発チームのトラッキングについて

管理者またはセキュリティリードは、チームの進捗状況をトラックして監視するための情報にアクセスして、優れたアプリケーションセキュリティプラクティスが実施および順守されていることを確認する必要があります。Application Securityは、優れたセキュリティプラクティスの採用を促進するための中心的な役割を果たします。アプリケーションとアプリケーションバージョンを通じて情報がどのようにトラックおよびレポートされるのかを理解することにより、アプリケーションセキュリティ規格に基づいて開発チームの進捗状況を正確に評価できます。

このセクションでは、次のトピックについて説明します。

1.11.1.1. アプリケーション作成プロセスについて

Application Securityにサインインして、新しいアプリケーションを追加するプロセスを開始すると、ウィザードに一連のステップが表示されます。これらのステップのそれぞれで、アプリケーションバージョンの作成を担当するチームメンバーに戦略の選択肢が提示されます。セキュリティリードが作成プロセスを完了するには、チームが合意のうえで戦略を選択する必要があります。

通常、セキュリティチームは、アプリケーションバージョンの作成を実際に開始する前に、すべてのオプションを評価して決定します。以下のセクションでは、ウィザードページに表示されるオプションについて説明しています。

参照情報

アプリケーションバージョン属性

テンプレートの選択

新しいアプリケーションの最初のバージョンの作成

アプリケーションに新しいバージョンを追加する

1.11.1.2. アプリケーションバージョンを作成するための戦略

セキュリティリードは、ユーザがデプロイされたアプリケーション内の脆弱性を追跡することを可能にするアプリケーションバージョンを作成できます。セキュリティの脆弱性は、多くの場合、異なるコンポーネントが一緒に存在するコードの領域で発生します。チームがそれぞれ異なるコンポーネントで作業するとしても、ソフトウェアコンポーネント全体を1つのソフトウェアとして追跡することが有効な手法です。たとえば、テキスト操作ライブラリは単独では安全であり、ファイルアクセスライブラリも単独では安全だとします。これらのテキスト操作ライブラリとファイルアクセスライブラリを組み合わせて使用する場合は、必ずしも安全であるとは言えません。これは、処理されるテキストの出所がわからない場合があるためです。

1.11.1.2.1. パッケージソフトウェアの戦略

具体的なバージョンとして出荷または展開されるソフトウェアの場合は、次の方法を使用できます。

- 新しいアプリケーションを作成する場合は、新しいアプリケーションバージョンを開始します。
- リリースごとにアプリケーションバージョンを1つ作成します。たとえば、セキュリティリードまたはマネージャは、過去のを無効にして結果をアーカイブしてから、それらのアプリケーションバージョンをビューから削除できます。アプリケーションバージョンを無効にする方法については、アプリケーションバージョンの無効化を参照してください。

  > **Note**
  >
  > 無効化されたアプリケーションバージョンは表示されませんが、データベースにはまだ存在します。アプリケーションのすべてのバージョンを削除すると、データベースからアプリケーションが削除されます。

- 発展するコードベースを備えた既存のアプリケーションを使用している場合は、既存のバージョンに基づいてアプリケーションバージョンを作成します。たとえば、アプリケーションAには複数のバージョンがあります。各新しいバージョンは、前のバージョンの結果に基づいて開始されます。後続の各バージョンは、(完全な書き換えではなく)コードが進化したものです。

1.11.1.2.2. 継続的な展開のための戦略

継続的デプロイを使用するアプリケーションの場合、`-build-label xxxx`オプションを使用してスキャンを実行すると、どのソースコントロールチェックアウトがスキャンされたのかを識別できます(`xxxx`はバージョン管理システムのIDを表します)。ソース制御チェックアウトにスキャンを関連付けると、個々の問題がいつ導入および修正されたのか判断する機能が向上します。

1.11.1.3. レポーティング用のアプリケーションバージョンの注釈付けについて

Application Securityには、個々のアプリケーションバージョンに適用できる一連のアプリケーション属性があります。これらの属性を使用して、レポーティング用にアプリケーションバージョンをグループ化したり、アプリケーションバージョンを外部システムに関連付けしたりできます。

管理者は、アプリケーション属性の基本セットをカスタマイズできます。サンプルのカスタマイズにより、組織では、アプリケーションID、業務部門、事業部、またはコンプライアンス義務別にオンボーディングの進行状況を追跡できます。

1.11.2. アプリケーションバージョンの作成について

Application Securityアプリケーションバージョンをまったく新しいアプリケーションとして作成することも、既存のアプリケーションバージョンの新しいアプリケーションとして作成することもできます。次のトピックでは、各方法の手順について説明します。

アプリケーション作成プロセスについて

新しいアプリケーションの最初のバージョンの作成

アプリケーションに新しいバージョンを追加する

1.11.2.1. アプリケーションバージョン属性

アプリケーションバージョンには、ビジネス属性、技術属性、組織属性があります。これらの属性は、Application Security がアプリケーション間の比較およびレポート作成を行うために使用するメタデータです。

新しいアプリケーションバージョンを作成するときは、［**新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)**］ウィザードの指示に従って、必須およびオプションの技術属性、組織属性、ビジネス属性、OpenText ScanCentral DASTアプリケーション属性を選択できます。必要なすべての属性の値を選択するまでは、アプリケーションバージョンを作成できません。たとえば、アプリケーションバージョンを作成するには、次の属性の値を指定する必要があります。

- Development phase
- Development strategy
- Accessibility

Application Securityが提供するデフォルト属性に加えて、管理者およびセキュリティリードはカスタム属性を作成してアプリケーションバージョンに割り当てることができます。カスタム属性は、特定のデータのサブセットに焦点を当てる必要があるとき非常に便利です。カスタム属性の作成方法については、カスタム属性の作成を参照してください。

次の表は、Application Security アプリケーションのデフォルトの属性のセットを示しています。このリストには、管理者がシステムに追加する可能性のあるカスタム属性は記載されていません。

技術属性	説明(Description)
Development Phase	(必須)アプリケーションバージョンの現在の開発フェーズ
Development Strategy	(必須)アプリケーション開発に使用する人員配属戦略
Accessibility	(必須)アプリケーションを使用するために必要なアクセス権のレベル
Application Type	コードベースの性質(ライブラリ、アプリケーション、またはアプリケーションコンポーネント)
Target Deployment Platform	アプリケーションの展開プラットフォーム
Interfaces	アプリケーションへのアクセスに使用するインタフェース
Development Languages	アプリケーションの開発に使用する言語
Authentication System	アプリケーションにアクセスしようとするユーザを認証するために使用するシステム

組織属性	説明(Description)
Business Unit	開発するアプリケーションの対象となる事業部、またはアプリケーションを開発する事業部
Industry	開発するアプリケーションの対象となる業界
Region	開発チームの地理的位置

ビジネスリスク属性	説明(Description)
Business Risk	アプリケーションが組織のビジネス目標に与える相対的なリスク(高、中、低)。
Known Compliance Obligations	アプリケーションが満たさなければならないすべての既知のコンプライアンス義務
Data Classification	このアプリケーションによって保存されるデータを入力します。
Application Classification	アプリケーションの直接のコンシューマ

OpenText ScanCentral DAST属性	説明(Description)
ベースURL(Base URL)	相対パスを確立するのに役立つ、アプリケーションのすべてのページの先頭に付加されるURLプレフィックス

1.11.2.1.1. カスタム属性の作成

Application Securityには、管理者とセキュリティリードが、アプリケーションとアプリケーションのバージョンを分類するための技術、組織、およびビジネス属性が含まれています。管理者またはセキュリティリードとして、アプリケーションバージョンに設定できる独自のカスタム属性を作成できます。

カスタム属性を作成するには:

1. 管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**属性(Attributes)**］を選択します。
4. ［**NEW**］をクリックします。
5. ［**新しい属性の作成(CREATE NEW ATTRIBUTE)**］ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明
名前(Name)	属性を説明する名前を入力します。 **Important** Application Securityがデフォルトで使用する属性を削除した場合、後で同じ名前を付けた新しい属性を作成すると、データベースのマイグレーションが失敗する可能性があります。
説明(Description)	簡単な説明を入力します。 入力した説明は、［**新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)**］ウィザードの属性フィールドの下に表示されます。
Category	属性タイプを選択します。 選択したカテゴリに応じて、属性は［**新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)**］ウィザードの対応する属性タブに表示されます。

フィールド	説明
Type	次のいずれかのコントロールタイプを選択します。 ◦ ユーザが1行のテキストを入力できるテキストフィールドを作成するには、［**Text - Single Line**］を選択します。 ◦ ユーザが属性に対して1つの値のみを選択できるリストを作成するには、［**List of Values - Single Selection**］を選択します。 **Note** 単一選択タイプの属性を作成すると、ユーザがその属性を［**Dashboard(ダッシュボード)**］ビューの［**グループ化条件(Group By)**］リストと［**集計条件(Aggregate by)**］リストから選択し、表示されるデータをカスタマイズできるようになります。 ◦ ユーザが属性に対して複数の値を選択できるリストを作成するには、［**List of Values - Multiple Selection**］を選択します。 ◦ ユーザが複数行のテキストを入力できるテキストフィールドを作成するには、［**Text - Multiple Lines**］を選択します。

フィールド	説明
	Note ［値のリスト(List of Values)］タイプのいずれかを選択すると、追加のフィールドが表示されます。これらのフィールドで、値とその説明を追加し、非表示にするかどうかを指定します。 ◦ 属性のチェックボックスを作成するには、［Boolean］を選択 します。 ◦ 整数値を受け入れるフィールドを作成するには、［Integer］を選択 します。 ◦ 属性のカレンダ選択コントロールを作成するには、［Date］を選択 します。 Note このタイプは、Dynamic Scan Request属性では使用できません。

フィールド	説明
Required	ユーザがアプリケーションテンプレートを作成するときに、この属性の設定を必須にするには、このチェックボックスをオンにします。
Hidden	作成する新しい属性が［**新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)**］ウィザードで表示されないようにするには、このチェックボックスをオンにします。 **Important** 作成する新しい属性が［**新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)**］ウィザードで表示されないようにするために［**非表示(Hidden)**］を選択する場合は、［**必須(Required)**］チェックボックスをクリアする必要があります。

6. ［**保存(SAVE)**］をクリックします。

新しい属性は、ユーザが次に新しいアプリケーションバージョンを作成するときに使用可能になります。

既存のアプリケーションバージョンでカスタム属性を指定する方法については、「アプリケーションバージョンに新しいカスタム属性を適用する」を参照してください。

Note

デフォルトでは、ユーザインタフェースを使用して作成したカスタム属性は削除することができます。Application Security APIを使用して、削除不可属性を定義できます。このAPIにアクセスする方法については、「APIドキュメントにアクセスする」を参照してください。

参照情報

属性と属性値の削除

アプリケーションバージョン属性

1.11.2.1.2. 属性と属性値の削除

属性または属性値が使用されなくなった場合、1つ以上のアプリケーションバージョンに現在関連付けられている場合であっても、通常はその属性または属性値をApplication Securityデータベースから削除できます。これにより、システムから属性または属性値のすべてのトレースが削除されます。

属性の削除

Application Securityデータベースから属性を削除するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**属性(Attributes)**］を選択します。

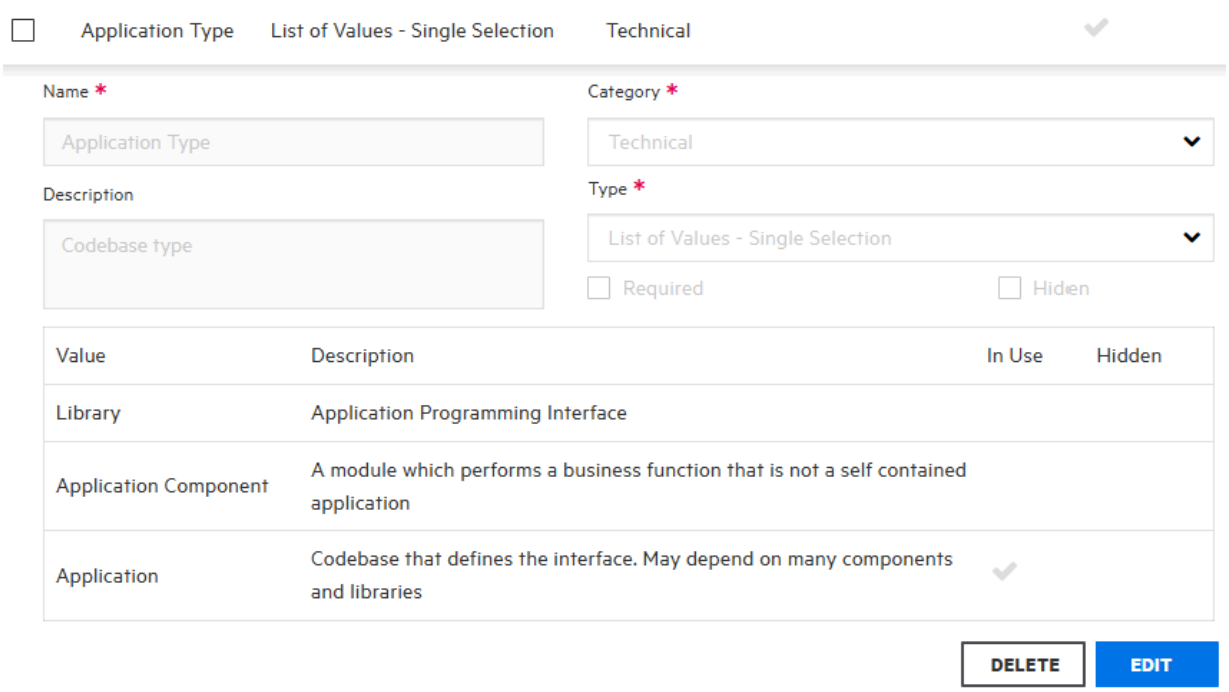
   削除できない属性のチェックボックスは淡色表示され、その属性を削除対象として選択することはできません。

   属性を削除できない理由の説明を表示するには、チェックボックスをポイントします。削除できない属性は、システム定義の属性、またはユーザ定義で削除不可として指定された属性です。
3. 削除する属性のチェックボックスをオンにして、［**DELETE**］をクリックします。
4. システムから属性を完全に除去することを確認するには、［**OK**］をクリックします。

属性値の削除

属性値を削除するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**属性(Attributes)**］を選択します。
3. 1つ以上の値を削除する対象の属性の行をクリックして展開します。



［**使用中(In Use)**］列には、現在1つ以上のアプリケーションバージョンで使用されている値が示されます。

4. ［**編集(EDIT)**］をクリックします。
5. 属性を編集することを確認するには、［**OK**］をクリックします。
6. 削除する値の［**削除**］ボタンをクリックします。

> **Note**
>
> 一部の属性値は、1つ以上のアプリケーションバージョンで現在使用されている場合でも削除できます。ただし、次の値は削除できません。
>
> - 使用されているシステム定義のリストタイプ属性の値
> - リストタイプ以外のシステム定義属性の値
> - 使用されていて、動的スキャンタイプ属性に属する値
> - 使用されていて削除不可として指定されているユーザ定義属性の値

Application Securityでは、確認を求めることなく値が削除されます。値を削除しない場合は、［**キャンセル**］をクリックして値を復元します。

参照情報

カスタム属性の作成

1.11.2.1.3. アプリケーションバージョンに新しいカスタム属性を適用する

新しいカスタム属性をアプリケーションバージョンに適用するには、次の手順を実行します。

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. 新しい属性を指定する対象のアプリケーションバージョンを選択します。

   Application Securityに、そのバージョンの［**監査(AUDIT)**］ページが表示されます。
3. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
4. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**アプリケーション設定(APPLICATION SETTINGS)**］をクリックします。
5. ［**バージョン設定(Version Settings)**］エリアで、［**編集(Edit)**］ボタン🖊をクリックします。
6. ［**属性(ATTRIBUTES)**］を選択します。
7. 属性カテゴリを選択してから、新しいカスタム属性の値(複数可)を選択します。
8. ［**保存(SAVE)**］をクリックします。

参照情報

カスタム属性の作成

アプリケーションバージョンの詳細を編集する

1.11.2.2. 問題テンプレートについて

アプリケーションは問題テンプレートによって定義されます。*問題テンプレート*では、アプリケーションソースコード内で明らかにされた問題をApplication Securityで設定し優先度を付ける方法を決定します。

問題テンプレートには次の設定が含まれます。

- フォルダフィルタ - 問題をフォルダにソートする方法を制御します
- 表示フィルタ - 表示/非表示を切り替える問題を制御します
- フォルダプロパティ -名前、色、およびアクティブなフィルタセット
- カスタムタグ - 表示する監査フィールドと各監査フィールドの値を指定します

Application Securityには、複数の問題テンプレートが付属しています。これらのテンプレートは、そのまま使用することも、Fortify Audit Workbenchで、アプリケーションのニーズに合わせて変更を加えることもできます。

これらの問題テンプレートの説明を表示するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**問題テンプレート(Issue Templates)**］を選択します。

［**問題(Issue)**］ページに、問題テンプレートとそれぞれの説明が一覧表示されます。

Application Security問題テンプレートをFortify Audit Workbenchにインポートして変更し、新しい名前で保存してから、Application Securityにインポートすることができます。Fortify Audit Workbenchで新しい問題テンプレートを一から作成することもできます。

Note

Fortify Audit Workbenchでフィルタセットやフォルダを編集または作成する際には、Fortify Audit WorkbenchとApplication Securityのそれぞれで使用される検索修飾子によって、異なる結果になる場合があることにご注意ください。検索式に基づくすべての検索、フィルタ、またはフォルダが同じ結果を生成するとは限りません。たとえば、OWASPやCWEなどの外部メタデータカテゴリを含む検索式は、Application SecurityとFortify Audit Workbenchでは異なる場合があるため、同じ結果にならない可能性があります。一致する外部カテゴリが複数ある場合、Application Securityではそれらのいずれかと一致しますが、Fortify Audit Workbenchではすべての外部カテゴリとの完全一致を期待します。Application Securityで使用する問題テンプレートを編集または作成する際にこの問題が発生した場合は、カスタマサポートにお問い合わせください。

Fortify Audit Workbenchで問題テンプレートを変更または作成する方法については、『OpenText™ Fortify Audit Workbenchユーザガイド』を参照してください。

1.11.2.2.1. システムへの問題テンプレートの追加

問題テンプレートをFortify Audit WorkbenchからApplication Securityに追加するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**問題テンプレート(Issue Templates)**］を選択します。

   Application Securityに、システム問題テンプレートが一覧表示されます。
4. ［**NEW**］をクリックします。
5. ［**名前**］ボックスに、テンプレート名を入力します。
6. (オプション)［**説明(Description)**］ボックスに、テンプレートの使用方法をユーザに知らせる説明を入力します。
7. ［**テンプレート(Template)**］の横にある［**参照(BROWSE)**］をクリックし、新しいテンプレートまたは変更されたテンプレートを見つけて選択します。
8. ［**保存(SAVE)**］をクリックします。

1.11.2.2.2. テンプレートの選択

Application Securityの問題テンプレートは、アプリケーションデータの分類、要約、レポーティングに最適な手段となります。また、発行テンプレートを使用すると、アプリケーションレベルではなく、エンタープライズレベルでカスタマイズされたアプリケーション設定を使用できます。

アプリケーションの作成完了後にアプリケーションの発行テンプレートを変更することもできますが、アプリケーション作成プロセスを完了する前に、セキュリティチームがテンプレートの選択を慎重に検討する必要があります。

1.11.2.3. 新しいアプリケーションの最初のバージョンの作成

アプリケーションバージョンは、アプリケーションコードベースの特定のバリアントのデータと属性で構成されます。

新しいアプリケーションの最初のバージョンを作成するには:

1. 管理者またはセキュリティリードとしてサインインします。
2. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューで、［**+新しいアプリケーションバージョン(+ NEW APPLICATION VERSION)**］をクリックします。

   ［**新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)**］ウィザードが開きます。
3. ［**全般(GENERAL)**］タブで、次の表に示す情報を入力します。

フィールド	説明(Description)
アプリケーションのセットアップ(Application Setup)	
アプリケーション名(Application name)	(必須)アプリケーション名を入力します。 **Important** アプリケーション名を `=`、`-`、`+`、または `@` 文字で始めることはできません。また、制御文字を含めることもできません。これらの範囲に含まれるUnicode文字の完全なリストについては、「Control characters in ASCII and Unicode」を参照してください。
アプリケーションの説明(Application description)	(オプション)新しいアプリケーションの説明を入力します。
バージョンのセットアップ(Version Setup)	

フィールド	説明(Description)
Version name	(必須)バージョンの名前を入力します。 **Important** バージョン名を `=`、`-`、`+`、または `@` 文字で始めることはできません。また、制御文字を含めることもできません。これらの範囲に含まれるUnicode文字の完全なリストについては、「Control characters in ASCII and Unicode」を参照してください。
バージョンの説明(Version description)	(オプション)このアプリケーションの最初のバージョンに関する情報を入力します。

フィールド	説明(Description)
Use existing application version	既存のアプリケーションバージョンの設定を使用するには、このチェックボックスをオンにして、次の操作を行います。 1. ［**参照(BROWSE)**］をクリックします。 2. 新しいアプリケーションに適用する設定が使われているアプリケーションを見つけて選択します。 アプリケーションのリストを絞り込むには、検索ボックスに文字列を入力して［**検索(FIND)**］をクリックします。 ［**バージョン(VERSIONS)**］ペインには、選択したアプリケーションのアクティブなバージョンが一覧表示されます。非アクティブなバージョンを表示するには、［**非アクティブなバージョンを表示(Show inactive)**］チェックボックスをオンにします。 3. ［**バージョン(VERSIONS)**］リストで、目的のバージョンのチェックボックスをオンにし、［**完了(DONE)**］をクリックします。 デフォルトでは、Application Securityに選択したアプリケーションバージョンのすべての設定が含まれます。 4. 1つ以上の設定を除外するには、該当する設定のチェックボックスをクリアします。

フィールド	説明(Description)
	5. 選択したアプリケーションバージョンに関連する問題と監査をすべてコピーするには、［**アプリケーションの状態(Application state)**］チェックボックスをオンにします。 最新のアプリケーションバージョンのメトリックが更新されるまでの監査のみがコピーされます。アプリケーションの状態をコピーする前にアプリケーションのメトリックを更新するには、「アプリケーションメトリックを再計算する」を参照してください。

4. ［**属性(ATTRIBUTES)**］設定に進むには、［**次へ(NEXT)**］をクリックします。
5. ［**TECHNICAL ATTRIBUTES**］タブで、次の表に示す情報を入力します。

フィールド	説明(Description)
Development Phase	［**新規(New)**］を選択します。
Development Strategy	アプリケーションバージョンの開発に使用する戦略を選択します。
Accessibility	アプリケーションへのアクセス方法を指定する値を選択します。
Application Type	アプリケーションタイプを選択します。
Target Deployment Platform	ターゲット展開プラットフォームを選択します。
Interfaces	アプリケーションにアクセスするために使用できるインタフェースのチェックボックスをオンにします。
Development Languages	アプリケーションバージョンの開発に使用する言語のチェックボックスをオンにします。
Authentication System	アプリケーションにアクセスするために使用する認証システムのチェックボックスをオンにします。

このタブには、組織によって定義された技術属性も表示されることがあります。

6. (オプション)［**組織属性(ORGANIZATION ATTRIBUTES)**］タブを選択し、次の表で説明する情報を入力します。

フィールド	説明(Description)
Business Unit	新しいアプリケーションを関連付ける事業部を選択します。
Industry	このアプリケーション開発の対象とする業界を選択します。
Region	アプリケーションに関連付ける地域を選択します。

このタブには、組織によって定義された組織属性も表示されることがあります。

7. (オプション)［**ビジネスリスク属性(BUSINESS RISK ATTRIBUTES)**］タブをクリックし、次の表で説明する情報を入力します。

フィールド	説明(Description)
Business Risk	この新しいアプリケーションが組織のビジネス目標に与える相対的なリスクを最も適切に表す値を選択します。
Known Compliance Obligations	新しいアプリケーションに適用されるすべての既知のコンプライアンス義務のチェックボックスをオンにします。
Data Classification	このアプリケーションが保存するデータ分類のチェックボックスをすべてオンにします。
Application Classification	このアプリケーション開発の対象コンシューマタイプのチェックボックスをすべてオンにします。

このタブには、組織によって定義されたビジネスリスク属性も表示されることがあります。

8. OpenText ScanCentral DASTを使用している場合は、［**ScanCentral DAST属性(SCANCENTRAL DAST ATTRIBUTES)**］タブを選択し、次の手順を実行します。
   - ［**ベースURL (Base URL)**］を入力して、アプリケーション内のすべてのページのプレフィックスを設定します。
9. ［**ポリシー(POLICIES)**］設定に進むには、［**次へ(NEXT)**］をクリックします。

   アプリケーションバージョンのオプトアウトを許可するようにデータ保持ポリシーが設定されている場合、このアプリケーションバージョンをデータ保持ポリシーからオプトアウトすることもできます。デフォルトでは、すべてのアプリケーションバージョンがデフォルトのデータ保持ポリシーの対象となります。データ保持ポリシーの詳細については、「データ保持について」を参照してください。
10. このアプリケーションバージョンをデータ保持ポリシーからオプトアウトするには、［**適用するデータ保持ポリシー(Data Retention Policy to Follow)**］リストで、［**なし(デフォルトからのオプトアウト) (None (Opt-out of Default))**］を選択します。
11. ［**テンプレート(TEMPLATE)**］設定に進むには、［**次へ(NEXT)**］をクリックします。
12. ［**問題テンプレート(Issue Template)**］で、問題検出の最小しきい値を設定するテンプレートのチェックボックスをオンにします。

    右側のペインに表示されるテンプレートの説明を表示するには、そのチェックボックスをオンにします。デフォルトのテンプレートは、優先的な高リスク問題テンプレートです。
13. ［**アクセス(ACCESS)**］設定に進むには、［**次へ(NEXT)**］をクリックします。
14. このアプリケーションバージョンのチームにユーザを追加するには、次のいずれかを実行します。
    - Application Securityデータベースからユーザを割り当てるには:
      1. ［**ローカル(LOCAL)**］を選択します。
      2. 割り当てるチームメンバー(複数可)のチェックボックスをオンにします。

         特定のユーザを検索するには、［**Search by user name**］ボックスにユーザ名を入力し、［**FIND**］をクリックします。
    - LDAPディレクトリからユーザを割り当てるには:

1. ［**LDAP**］をクリックし、［**View By**］リストから、LDAPエンティティの表示に使用する属性を選択します。
2. 割り当てるチームメンバー(複数可)のチェックボックスをオンにします。

   特定のユーザを検索するには、［**Search by user name**］ボックスにユーザ名を入力し、［**FIND**］をクリックします。

15. ［**保存(SAVE)**］をクリックします。

    新しいアプリケーションバージョンが［**アプリケーション(Applications)**］ビューに表示されます。そのアプリケーションバージョンのデータがアップロードされると、［**ダッシュボード(Dashboard)**］ビューにも表示されるようになります。

16. ［**閉じる(CLOSE)**］をクリックします。

参照情報

スキャンアーティファクトのアップロード

アプリケーションに新しいバージョンを追加する

1.11.2.4. アプリケーションに新しいバージョンを追加する

Important
既存バージョンをコピーまたは使用して新しいアプリケーションバージョンを作成する前に、Application Securityが現在の状態の再計算を完了するまで待つ必要があります。

既存のアプリケーションの新しいバージョンを作成するには:

1. 管理者またはセキュリティリードとしてサインインします。
2. ［**アプリケーション(Applications)**］ビューで、アプリケーションバージョンを選択してから、［**+新しいバージョン(+ NEW VERSION)**］をクリックします。

   ［**アプリケーション名(Application name)**］ボックスと［**アプリケーションの説明(Application description)**］ボックスに、選択したアプリケーションの名前と説明が入力されます。
3. ［**全般(GENERAL)**］タブの［**バージョンのセットアップ(Version Setup)**］で、次の表で説明する情報を指定します。

フィールド	説明(Description)
バージョン名(Version name)	バージョンの名前を入力します。 **Important** バージョン名を `=`、`-`、`+`、または `@` 文字で始めることはできません。また、制御文字を含めることもできません。これらの範囲に含まれるUnicode文字の完全なリストについては、「Control characters in ASCII and Unicode」を参照してください。
バージョンの説明(Version description)	(オプション)アプリケーションのこのバージョンについての説明を入力します。

フィールド	説明(Description)
Use existing application version	既存のアプリケーションバージョンの設定を使用するには、このチェックボックスをオンにして、次の操作を行います。 1. ［**参照(BROWSE)**］をクリックします。 2. 新しいアプリケーションに適用する設定が使われているアプリケーションを見つけて選択します。 アプリケーションのリストを絞り込むには、検索ボックスに文字列を入力して［**検索(FIND)**］をクリックします。 ［**バージョン(VERSIONS)**］ペインには、選択したアプリケーションのアクティブなバージョンが一覧表示されます。非アクティブなバージョンを表示するには、［**非アクティブなバージョンを表示(Show inactive)**］チェックボックスをオンにします。 3. ［**バージョン(VERSIONS)**］リストで、目的のバージョンのチェックボックスをオンにし、［**完了(DONE)**］をクリックします。 デフォルトでは、Application Securityに選択したアプリケーションバージョンのすべての設定が含まれます。 4. 1つ以上の設定を除外するには、該当する設定のチェックボックスをクリアします。

フィールド	説明(Description)
	5. 選択したアプリケーションバージョンに関連する問題と監査をすべてコピーするには、［**アプリケーションの状態(Application state)**］チェックボックスをオンにします。 最新のアプリケーションバージョンのメトリックが更新されるまでの監査のみがコピーされます。アプリケーションの状態をコピーする前にアプリケーションのメトリックを更新するには、「アプリケーションメトリックを再計算する」を参照してください。

4. ［**属性(ATTRIBUTES)**］設定に進むには、［**次へ(NEXT)**］をクリックします。
5. ［**TECHNICAL ATTRIBUTES**］タブで、次の表に示す情報を入力します。

フィールド	説明(Description)
Development Phase	この一覧から、新しいバージョンの現在の開発フェーズを選択します。
Development Strategy	新しいアプリケーションバージョンの開発に使用する戦略を選択します。
Accessibility	アプリケーションへのアクセス方法を指定する値を選択します。
Application Type	アプリケーションタイプを選択します。
Target Deployment Platform	ターゲット展開プラットフォームを選択します。
Interfaces	アプリケーションにアクセスするために使用できるインタフェースのチェックボックスをオンにします。
Development Languages	アプリケーションバージョンの開発に使用する言語のチェックボックスをオンにします。
Authentication System	アプリケーションにアクセスするために使用する認証システムのチェックボックスをオンにします。

このタブには、組織によって定義された技術属性も表示されることがあります。

6. (オプション)［**組織属性(ORGANIZATION ATTRIBUTES)**］タブを選択し、次の表で説明する情報を入力します。

フィールド	説明(Description)
Business Unit	開発しているアプリケーションバージョンの事業部を選択します。
Industry	アプリケーションバージョンが適用される業界セクタを選択します。
Region	開発しているアプリケーションバージョンの地域を選択します。

このタブには、組織によって定義された組織属性も表示されることがあります。

7. (オプション)［**ビジネスリスク属性(BUSINESS RISK ATTRIBUTES)**］タブを選択し、次の表で説明する情報を入力します。

フィールド	説明(Description)
Business Risk	このアプリケーションバージョンが組織に与えるリスクを最も適切に表す値を選択します。
Known Compliance Obligations	アプリケーションバージョンが満たさなければならないすべての既知のコンプライアンス義務のチェックボックスをオンにします。
Data Classification	アプリケーションバージョンに適用されるすべてのデータ分類のチェックボックスをオンにします。
Application Classification	このアプリケーションバージョンに適用されるすべてのアプリケーション分類のチェックボックスをオンにします。

このタブには、組織によって定義されたビジネスリスク属性も表示されることがあります。

8. OpenText ScanCentral DASTを使用している場合は、［**ScanCentral DAST属性(SCANCENTRAL DAST ATTRIBUTES)**］タブを選択し、次の手順を実行します。
    - ［**ベースURL (Base URL)**］を入力して、アプリケーション内のすべてのページのプレフィックスを設定します。

    このタブには、組織によって定義されたOpenText ScanCentral DAST属性も表示されることがあります。

9. ［**ポリシー(POLICIES)**］設定に進むには、［**次へ(NEXT)**］をクリックします。

    アプリケーションバージョンのオプトアウトを許可するようにデータ保持ポリシーが設定されている場合、このアプリケーションバージョンをデータ保持ポリシーからオプトアウトすることもできます。デフォルトでは、すべてのアプリケーションバージョンがデフォルトのデータ保持ポリシーの対象となります。データ保持ポリシーの詳細については、「データ保持について」を参照してください。

10. このアプリケーションバージョンをデータ保持ポリシーからオプトアウトするには、［**適用するデータ保持ポリシー(Data Retention Policy to Follow)**］リストで、［**なし(デフォルトからのオプトアウト) (None (Opt-out of Default))**］を選択します。
11. ［**テンプレート(TEMPLATE)**］設定に進むには、［**次へ(NEXT)**］をクリックします。
12. ［**Issue Template**］で、問題検出の最小しきい値を設定するテンプレートのチェックボックスをオンにします。

    右側のペインに表示されるテンプレートの説明を表示するには、そのチェックボックスをオンにします。デフォルトのテンプレートは、優先的な高リスク問題テンプレートです。
13. ［**アクセス(ACCESS)**］設定に進むには、［**次へ(NEXT)**］をクリックします。
14. このアプリケーションバージョンのチームにユーザを追加するには、次のいずれかを実行します。

    Note

    管理者の役割のユーザは、すべてのアプリケーションに対するフルアクセス権をすでに持っています。管理者ユーザをチームに割り当てるには、そのユーザに別の役割も割り当てられていなければなりません。これは、管理者がローカルユーザでもLDAPユーザでも同じです。

    - Application Securityデータベースからユーザを割り当てるには:
        1. ［**ローカル(LOCAL)**］を選択します。
        2. 割り当てるチームメンバー(複数可)のチェックボックスをオンにします。

           特定のユーザを検索するには、［**Search by user name**］ボックスにユーザ名を入力し、［**FIND**］をクリックします。
    - LDAPディレクトリからユーザを割り当てるには:
        1. ［**LDAP**］をクリックし、［**View By**］リストから、LDAPエンティティの表示に使用する属性を選択します。
        2. 割り当てるチームメンバー(複数可)のチェックボックスをオンにします。

           特定のユーザを検索するには、［**Search by user name**］ボックスにユーザ名を入力し、［**FIND**］をクリックします。

15. ［**保存(SAVE)**］をクリックします。

    新しいアプリケーションバージョンが、アプリケーションバージョンのリストに表示されます。

16. ［**閉じる(CLOSE)**］をクリックします。

参照情報

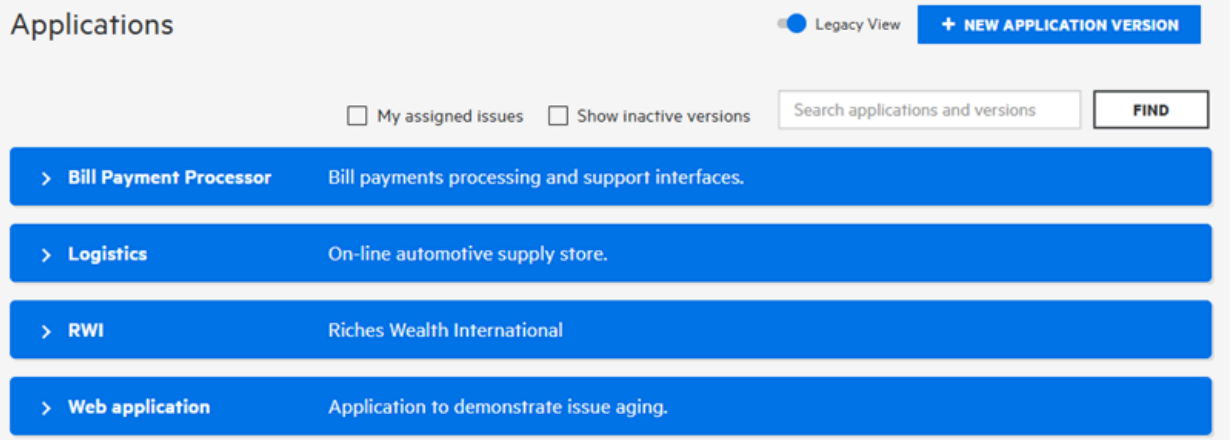
新しいアプリケーションの最初のバージョンの作成

1.11.3. アプリケーションのバージョンを表示する

アプリケーションのバージョンを表示するには:

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。

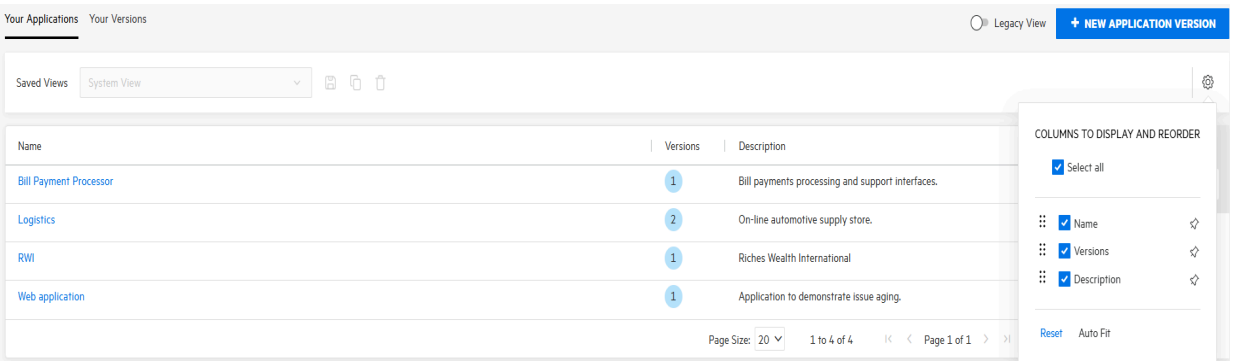
   初めて［**アプリケーション(Applications)**］ビューにアクセスする際は、［**レガシービュー(Legacy View)**］にアプリケーションが表示されます。



   ［**レガシービュー(Legacy View)**］でアプリケーションのバージョンを表示するには、アプリケーションの行をクリックします。

2. 最新の［**アプリケーション(Applications)**］ビューでアプリケーションを表示するには、［**レガシービュー(Legacy View)**］スイッチをオフにします。

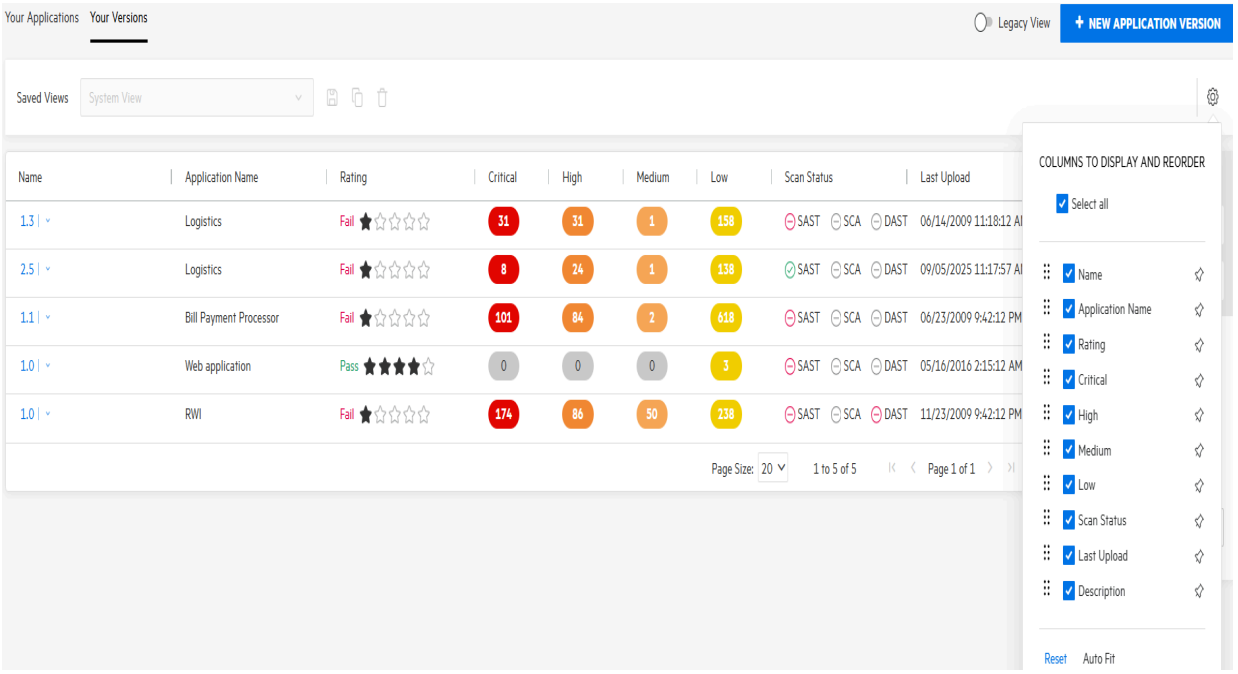
   ［**自分のアプリケーション(Your Applications)**］ページには、アプリケーションの名前、バージョンの数、アプリケーションの説明が表示されます。



   アプリケーションのバージョンを表示するには、アプリケーション名をクリックします。

   ［**自分のバージョン(Your Versions)**］ページには、アプリケーションバージョン

名、バージョンの説明、アプリケーション名、評価(Fortify Security Ratingパフォーマンスインジケータのビジュアル)、スキャンタイプとステータス、および前回のスキャン日時が表示されます。



Note

［**表示する列と並べ替える列(Columns to Display and Reorder)**］で［**Scan Status(スキャンステータス)**］を選択すると以下のようになります。

スキャンタイプがSTATIC/SAST (SCA)の場合:
- **SAST**が表示されます。
- 過去30日間に存在していた場合、緑色のチェックマークが表示されます。
- 過去に存在し、30日以上経過している場合は、赤いハイフンが表示されます。
- 存在しない場合は、グレーのハイフンが表示されます。

スキャンタイプがDYNAMIC/DAST (WebInspect)の場合:
- **DAST**が表示されます。
- 過去30日間に存在していた場合、緑色のチェックマークが表示されます。
- 過去に存在し、30日以上経過している場合は、赤いハイフンが表示されます。
- 存在しない場合は、グレーのハイフンが表示されます。

スキャンタイプがOPEN SOURCE (Sonatype, Debricked)の場合:
- **SCA**が表示されます。
- 過去30日間に存在していた場合、緑色のチェックマークが表示されます。
- 過去に存在し、30日以上経過している場合は、赤いハイフンが表示されます。
- 存在しない場合は、グレーのハイフンが表示されます。

アイコンにカーソルを合わせると、 最後のスキャン日を確認できます。

［**自分のアプリケーション(Your Applications)**］ページまたは［**自分のバージョン(Your Versions)**］ページに表示されるすべての列を確認するには、［**表示する列と並べ替える列(Columns to Display and Reorder)**］をクリックします。デフォルトでは、［**すべて選択**］チェックボックスがオンになっています。

［**すべて選択**］チェックボックスをオフにして、表示する必要がある列を選択することも、表示する必要がない列の名前の横にあるチェックボックスをオフにすることもできます。［**自分のアプリケーション(Your Applications)**］ページまたは［**自分のバージョン(Your Versions)**］ページから列を削除するには、削除する列をテーブルの外にドラッグします。
すべての列をドラッグした場合は、［**表示する列と並べ替える列(Columns to Display and Reorder)**］をクリックし、表示する必要がある列を選択します。
列の幅を調整するには、［**リセット(Reset)**］または［**自動調整(Auto Fit)**］をクリックします。
列名をドラッグアンドドロップすることで、要件に応じて列を配置できます。

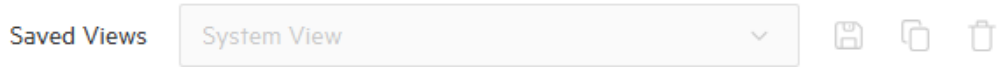
参照情報

アプリケーションビューからアプリケーションとアプリケーションバージョンを検索する

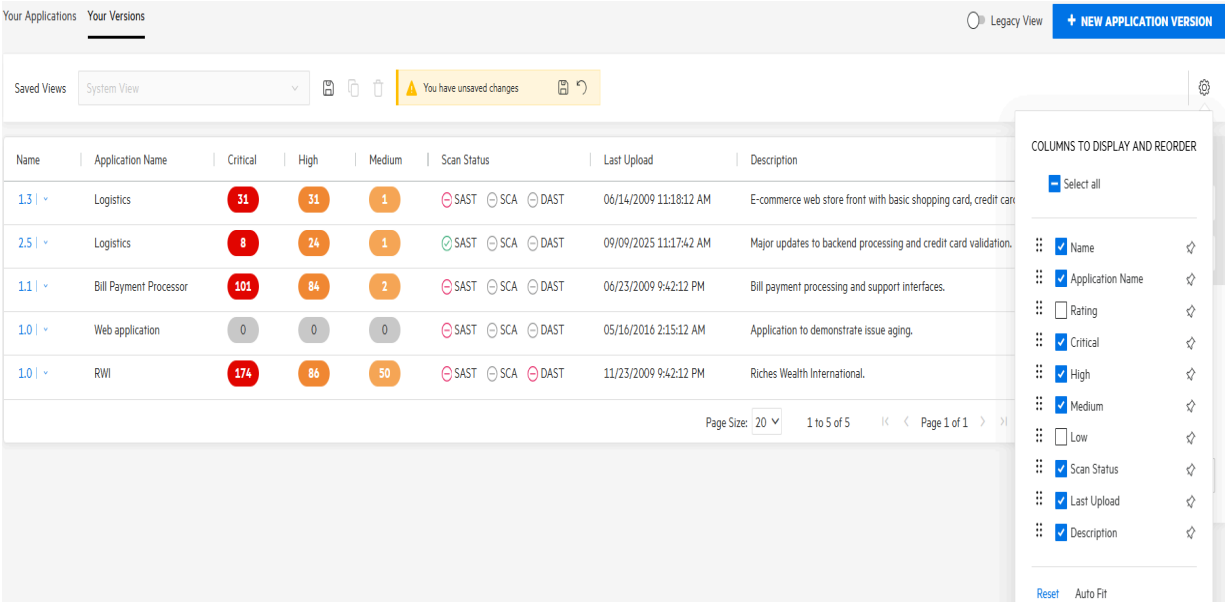
1.11.4. アプリケーションビューを保存する

アプリケーションビューを保存するには:

1. ［**アプリケーション(Applications)**］ビューにアクセスすると、［**ご使用のアプリケーション(Your Applications)**］ページまたは［**ご使用のバージョン(Your versions)**］ページのデフォルトビューが表示されます。［**保存されたビュー(Saved Views)**］のリストは空です。



2. ページを変更するときに、［**表示または並べ替えするカラム(Columns to Display or Reorder)**］、［**フィルタ(Filters)**］、［**一般(General)**］、または［**属性(Attributes)**］オプションを使用して、［**ビューの保存/更新(Save/Update view)**］アイコンを有効にします。



3. 変更を保存するには、［**ビューの保存/更新(Save/Update view)**］をクリックします。
   変更を破棄するには、［**元に戻す(Undo)**］をクリックします。
4. ビューの名前を入力します。必要に応じて、［**デフォルトビューとしてマーク(Mark as default view)**］を選択します。
5. ［**保存(SAVE)**］をクリックします。保存されたビューの名前がリストに表示されます。

新しいビューを作成および保存できます。保存済みのビューを変更し、［**フィルタ/ビューの名前変更(Rename fiter/view)**］をクリックして必要に応じて保存できます。

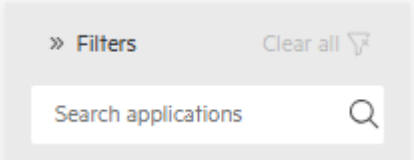
保存したビューを削除するには、ビューを選択して［**削除(Delete)**］をクリックします。

1.11.5. アプリケーションビューからアプリケーションとアプリケーションバージョンを検索する

特定のアプリケーションを検索する

特定のアプリケーションを検索するには:

1. ［**自分のアプリケーション(Your Applications)**］ページを選択します。
2. ［**フィルタ(Filters)**］の［**アプリケーションの検索(Search applications)**］ボックスに、検索するアプリケーション名の少なくとも一部を入力します。



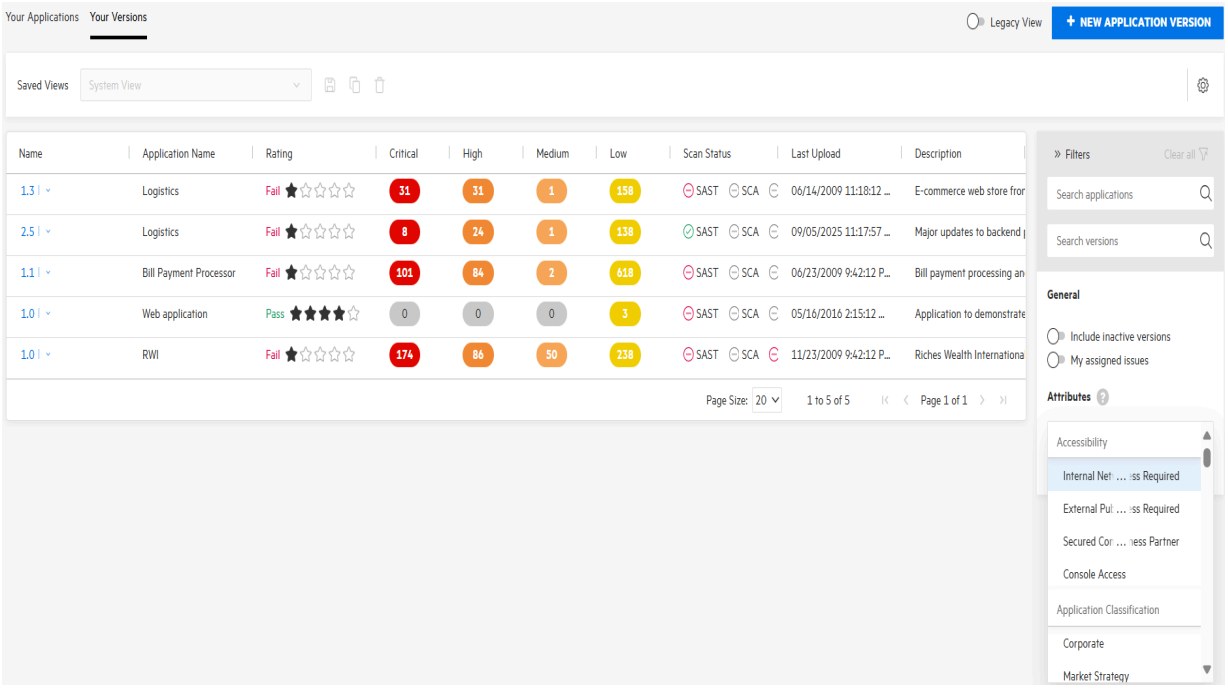
3. 完全な［**アプリケーション(Applications)**］テーブルに戻るには、検索ボックスのテキストをクリアします。

アプリケーションバージョンを検索する

アプリケーションバージョンを検索するには:

1. ［**自分のバージョン(Your Versions)**］ページを選択します。

2. ［**フィルタ(Filters)**］で、次の操作を任意に組み合わせて実行します。



   - ［**アプリケーションの検索(Search applications)**］ボックスに、検索するアプリケーション名の少なくとも一部を入力します。
   - ［**バージョンの検索(Search versions)**］ボックスに、検索するアプリケーションバージョン名の少なくとも一部を入力します。

> **Note**
> ワイルドカードアスタリスク(*)および疑問符(?)は、どちらの検索ボックスでもサポートされていません。

   - ［**属性(Attributes)**］リストで、検索する属性ごとに1つのオプションを選択します。最大3つのオプションを選択できます。
     選択した属性を削除するには、その名前の横にある［**x**］をクリックします。選択したすべての属性を削除するには、［**すべてクリア(Clear all)**］をクリックします。

   ［**自分のバージョン(Your Versions)**］ページに、検索条件に一致するすべてのアプリケーションバージョンが一覧表示されます。

3. 完全な［**自分のバージョン(Your Versions)**］ページに戻るには、［**すべてクリア(Clear all)**］をクリックします。

(**レガシービュー**)特定のアプリケーションまたはアプリケーションバージョンを検索するには:

1. ［**アプリケーションとバージョンの検索(Search Apps and Versions)**］ボックスに、検索するアプリケーションまたはバージョンのアプリケーション名またはバージ

ョン名の少なくとも一部を入力します。

ワイルドカードアスタリスク(*)および疑問符(?)はサポートされていません。

2. ［**Find**］をクリックします。

［**Applications**］テーブルには、検索文字列に一致するアプリケーションのすべてのバージョンが一覧表示されます。

3. 完全な［**Applications**］テーブルに戻る場合は、検索ボックスのテキストをクリアします。

参照情報

グローバル検索

1.11.6. アプリケーションメトリックを再計算する

アプリケーションバージョンに保留中の監査情報がある場合は、そのバージョンの［**概要(OVERVIEW)**］ページに［保留中の変更(Pending Changes)］ボタンが表示されます。

アプリケーションのメトリックを再計算するには、次の手順に従います。

- ［**保留中の変更(Pending Changes)**］ボタンをクリックし、［**アプリケーションメトリックの更新(REFRESH APPLICATION METRICS)**］ダイアログボックスで［**今すぐ更新(REFRESH NOW)**］をクリックします。

アプリケーションメトリックスを更新すると、アプリケーションの状態(マージされた分析結果)も更新されます。現在のシステムアクティビティによっては、メトリックの更新に時間がかかる場合があります。更新が完了すると、［**概要(OVERVIEW)**］ページにアプリケーションの最新データが表示されます。

参照情報

スキャンアーティファクトをダウンロードする

1.11.7. アプリケーションバージョンの詳細を編集する

アプリケーションバージョンの詳細を編集するには:

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. 編集するアプリケーションバージョンを選択します。
3. ［**監査(Audit)**］ページで、［**編集(Edit)**］ボタンをクリックします。

4. ［**バージョンの編集(EDIT VERSION)**］ダイアログボックスで、「アプリケーションに新しいバージョンを追加する」で説明されているいずれかのフィールドの値を編集するタブをクリックします。
5. ［**保存(SAVE)**］をクリックします。

参照情報

アプリケーションバージョンに関連付けられているテンプレートを変更する

1.11.8. アプリケーションバージョンの選択したデータをCSVファイルにエクスポートする

アプリケーションバージョンの選択したデータをカンマ区切り値(CSV)ファイルにエクスポートできます。システムがCSVファイルを保持する期間を確認するには、「ジョブスケジューラの設定」を参照してください。

アプリケーションバージョンのデータをエクスポートするには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アプリケーションバージョンを選択します。
3. (オプション)［**監査(AUDIT)**］ページで、フィルタ条件とする属性を選択できます。
4. ［**エクスポート(EXPORT)**］をクリックします。

> **Note**
>
> ［**EXPORT**］ボタンが表示されない場合は、管理者がこの機能を無効にしています。

5. ［**ファイル名(File name)**］ボックスに、ファイルの名前を入力します。
6. (オプション)［**ノート(Notes)**］ボックスに、エクスポートするデータに関する情報を入力します。
7. ［**保存(SAVE)**］をクリックします。
8. エクスポートされた結果を表示するには:
    1. ヘッダで、［**レポート**］をクリックします。
    2. ［**データエクスポート(DATA EXPORTS)**］をクリックします。
    3. ［**監査(Audit)**］テーブルで、エクスポートされたファイルの行をポイントして［**ダウンロード(Download)**］ボタンをクリックします。

参照情報

ダッシュボードサマリテーブルをエクスポートする

1.11.9. セキュリティ脆弱性の管理にバグトラッキングシステムを利用する

ソフトウェアの欠陥を修正する開発者は、バグトラッキングシステムを使用してワークロードを管理する場合が多いです。セキュリティの脆弱性はバグの一種であり、脆弱性情報をバグトラッキングシステムに取り込むと、開発者がその他の開発アクティビテイに従って、適切な修正手段を講じるのに役立ちます。その結果、セキュリティへの意識が向上し、セキュリティ問題の修正が迅速になります。

開発チームがすでに使用されているバグトラッキングシステムにバグを提出できるように、Application Securityから複数のバグトラッキングシステムのいずれかにマップできます。

開発者がバグを提出すると、Application Securityで次の基本的な脆弱性情報がバグチケットに入力されます。

- 検出された問題の種類について説明する詳細
- 修正のガイダンス(実行するアクションに関する指示付き)
- 問題の完全な詳細を参照するためにApplication Securityに戻るリンク

このセクションでは、次のトピックについて説明します。

1.11.9.1. バグトラッカの設定

チームがApplication Securityからバグトラッキングシステムにアクセスして使用できるようにするには、セキュリティリードまたは開発マネージャがバグトラッカインスタンスに接続するようApplication Securityを設定する必要があります。これにより、開発者またはセキュリティリードがバグを送信して、重要なセキュリティ問題に対処できるようになります。

セキュリティリードまたはマネージャは、次の手順に従って、バグトラッキングシステムにチームがアクセスできるようにします。

1. アプリケーションバージョンの詳細を編集します。
2. バグトラッカを設定します。

参照情報

バグ報告用Velocityテンプレート

バグトラッカプラグインの追加

バグトラッカプラグインの作成

1.11.9.2. バグ報告用Velocityテンプレート

Application Securityでバグを報告するためのテキストベースのフィールドは、問題データを参照するApache Velocityテンプレートに関連付けできます。1つ以上の問題のバグを送信すると、対応するテンプレートと問題のデータを使用して、マップされたフィールドのコンテンツが生成されます。

Application Securityには、Application Securityに付属するサポートされているバグトラッカプラグインに関するサマリフィールドおよび説明フィールド用に定義済みテンプレートが用意されています。これらの定義済みテンプレートを編集したり、プラグインが提供する他のテキストベースのフィールドをマップするテンプレートを追加したりできます。

このセクションでは、次のトピックについて説明します。

バグトラッカプラグインへのVelocityテンプレートの追加

バグトラッカプラグインのVelocityテンプレートのカスタマイズ

Velocityテンプレートの削除

1.11.9.2.1. バグトラッカプラグインへのVelocityテンプレートの追加

Application Securityには、Application Securityに付属するサポートされているバグトラッカプラグインに関するサマリフィールドおよび説明フィールド用に定義済みテンプレートが用意されています。これらのテンプレートを編集したり、プラグインが提供する他のテキストベースのフィールドをマップするテンプレートを追加したりできます。

Important

新しいテンプレートを追加したり既存のテンプレートを編集したりする場合は、その前に事前に定義されたテンプレートを注意深く確認して、テンプレート内の変数を正しく参照する方法を理解してください。

テンプレートを作成(または編集)する場合は、次の点に注意が必要です。

- ランタイムエラーを回避するために、OpenTextでは、テンプレート内の変数をレンダリング前に検証することを強く推奨しています。(マクロの使い方の例については、定義済みのテンプレートを参照してください)。
- (複数の問題を含むバグではなく)単一の問題によるバグに対してコンテンツを異なる方法でレンダリングする場合は、条件を使用します。

Velocityテンプレートをバグトラッカプラグインに追加するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**バグ報告テンプレート(Bug Filing Templates)**］を選択します。

   ［**バグ報告(Bug Filing)**］ページに、サポートされているバグトラッカのテンプレートグループが一覧表示されます。
3. テーブルで、バグトラッカプラグインのテンプレートグループを表示する行をクリックします。

   行が展開され、プラグインの説明およびサマリフィールドにマップされた事前定義済みテンプレートの詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. ［**+ ADD FIELD**］をクリックします。

6. ［**マップ済みフィールド(Mapped field)**］ボックスに、マップするフィールドの名前を、バグトラッカプラグインのダイアログボックスに表示されているとおりに入力します。

   テキストベースのフィールドでなければマップできないことにご注意ください。

7. ［**Template**］ボックスに、マッピングのVelocity Template Language (VTL)ステートメントを入力します。

   VTLステートメントの形式については、［**編集に関するヒント(Editing tips)**］リンクをクリックしてください。テンプレートの記述方法の詳細な手順にアクセスするには、［**Velocity User Guide**］リンクをクリックします。これにより、Apache Velocity ProjectのWebサイトに移動されます。使用可能なすべての変数のリストを表示するには、［**変数を表示(SHOW VARIABLES)**］をクリックします。

8. ［**適用(APPLY)**］をクリックします。

9. 別のテンプレートを追加するには、手順5～8を繰り返します。

10. ［**保存(SAVE)**］をクリックします。

［**バグ報告(Bug Filing)**］ページで、バグトラッキングプラグインの詳細に新しいテンプレートが含まれるようになります。

参照情報

バグ報告用Velocityテンプレート

バグトラッカプラグインのVelocityテンプレートのカスタマイズ

バグトラッカの設定

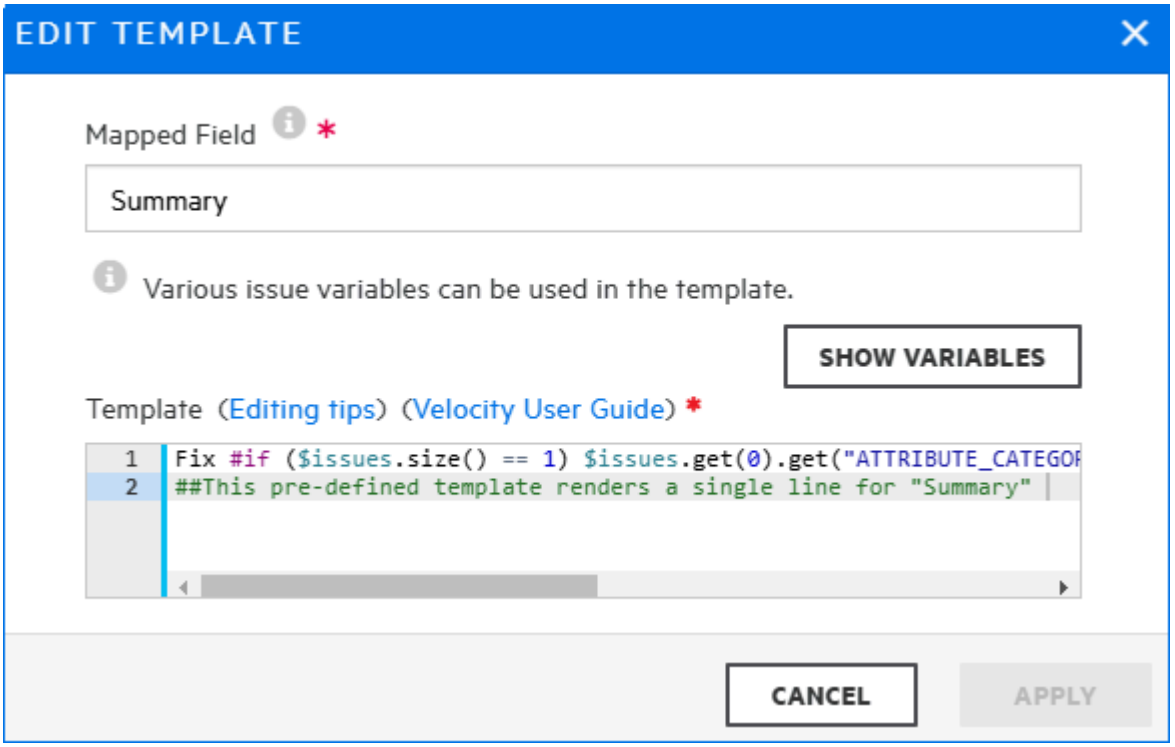
Velocityテンプレートの削除

1.11.9.2.2. バグトラッカプラグインのVelocityテンプレートのカスタマイズ

バグトラッカプラグインのVelocityテンプレートをカスタマイズするには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**バグ報告テンプレート(Bug Filing Templates)**］を選択します。
3. テーブルで、使用するバグトラッカプラグインのテンプレートグループをクリックします。

   行が展開され、プラグインで提供される説明およびサマリフィールドにマップされた事前設定済み速度テンプレートの詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. 編集するマップされたフィールドの［**フィールドを編集(Edit field)**］ボタンをクリックします。



6. テンプレートの編集に役立つヒントを確認するには、［**編集に関するヒント(Editing tips)**］リンクをクリックします。

   テンプレートの変更方法の詳細な手順にアクセスするには、［**Velocity User Guide**］リンクをクリックします。これにより、Apache Velocity ProjectのWebサ

イトに移動されます。使用可能なすべての変数のリストを表示するには、［**SHOW VARIABLES**］をクリックします。

7. ［**マップされたフィールド(Mapped field)**］ボックスと［**テンプレート(Template)**］ボックスの内容に必要な変更を加えます。
8. ［**適用(APPLY)**］をクリックします。
9. ［**保存(SAVE)**］をクリックします。

バグトラッカープラグインに表示される詳細に、変更内容が含まれるようになりました。

参照情報

Velocityテンプレートの削除

バグ報告用Velocityテンプレート

バグトラッカプラグインへのVelocityテンプレートの追加

1.11.9.2.3. Velocityテンプレートの削除

バグトラッカプラグインがアプリケーションバージョンに関連付けされていない場合は、関連付けられたテンプレートグループを削除できます。

バグトラッカプラグインに関連付けられたテンプレートグループを削除するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**バグ報告テンプレート(Bug Filing Templates)**］を選択します。
3. テンプレートグループのリストで、バグトラッカプラグインの名前をクリックします。

   行が展開され、プラグインで提供される説明およびサマリフィールドにマップされた事前設定済みテンプレートの詳細が表示されます。
4. ［**DELETE**］をクリックします。

   > **Caution**
   >
   > OpenTextでは、事前定義済みのテンプレートグループを削除しないことを強く推奨しています。

5. 削除を続行するには、［**OK**］をクリックします。

［**バグ報告(Bug Filing)**］ページに、バグトラッカプラグインのVelocityテンプレートが一覧表示されなくなります。

参照情報

バグ報告用Velocityテンプレート

バグトラッカプラグインへのVelocityテンプレートの追加

バグトラッカプラグインのVelocityテンプレートのカスタマイズ

1.11.9.3. アプリケーションバージョンへのバグトラッキングシステムの割り当て

バグトラッキングシステムをアプリケーションバージョンに割り当てるには、次の手順に従います。これを実行する前に、バグトラッカプラグインがすでにシステムに存在している必要があります。

バグトラッキングシステムと統合するには、次の手順に従います。

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. バグトラッカの割り当て先とするアプリケーションバージョンを選択します。

   選択したアプリケーションバージョンの［**監査(AUDIT)**］ページに、そのバージョンの問題が一覧表示されます。
3. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
4. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**バグトラッカ(BUG TRACKER)**］タブをクリックします。
5. ［**バグトラッカの統合(Bug Tracker Integration)**］リストから、このアプリケーションバージョンのバグを追跡するために使用するアプリケーションを選択します。
6. 必要なフィールドに入力し、［**VALIDATE CONNECTION**］をクリックします。
7. ［**バグトラッカプラグイン設定のテスト(TEST BUG TRACKER PLUGIN CONFIGURATION)**］ダイアログボックスで、バグトラッカ認証資格情報を入力し、［**テスト(TEST)**］をクリックします。

   Application Securityでバグトラッカへの接続が確認されると、テストが成功したというメッセージが表示されます。
8. ［**OK**］をクリックします。

   アプリケーションバージョンのバグ状態管理を有効にできます。バグ状態管理を有効にすると、Application Securityはバグ内の問題の状態が変化するのに応じ、バグを更新できます。
9. (オプション)バグ状態管理を有効にするには、［**Bug state management**］チェックボックスをオンにします。
10. ［**Username**］および［**Password**］ボックスにバグトラッカの資格情報を入力し、［**APPLY**］をクリックします。
11. ［**OK**］をクリックします。

12. ［**閉じる(CLOSE)**］をクリックします。

参照情報

バグトラッキングシステムの統合について

バグトラッカプラグインの追加

複数の問題のバグの送信

バグトラッカプラグインの作成

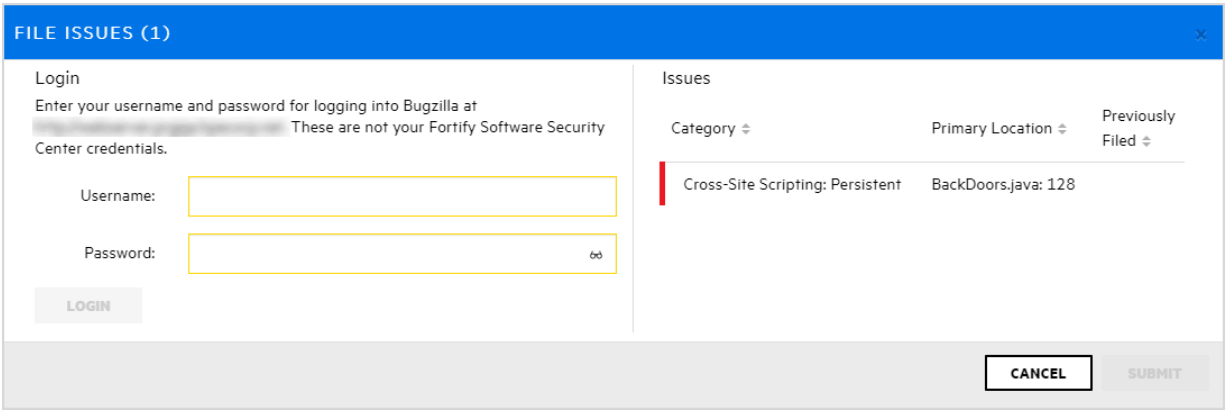
1.11.9.4. 単一の問題のバグの送信

アプリケーションバージョンにバグトラッキングプラグインが指定されている場合(アプリケーションバージョンへのバグトラッキングシステムの割り当て)、そのバグトラッカを使用して、1つ以上の問題を対象にするバグを送信できます。

単一の問題のバグを送信するには、次の手順に従います。

1. アプリケーションバージョンの［**監査(AUDIT)**］ページで、バグを送信する対象の問題の行を展開します。
2. ［**FILE BUG**］をクリックします。

   ［**バグを報告(FILE BUG)**］ボタンが有効になっていない場合、これは、バグトラッカがアプリケーションバージョンに割り当てられていないことを意味します。これに対処するには、「バグトラッカプラグインの追加」および「アプリケーションバージョンへのバグトラッキングシステムの割り当て」を参照してください。また、問題に関するバグがすでに送信されている場合、その問題に対して新しいバグを送信することはできません。



3. ［**ログイン**］エリアで、このアプリケーションバージョンに関連付けられたバグトラッカのユーザ名とパスワードを入力し、［**ログイン**］をクリックします。

   Application Securityは、作業セッション中は資格情報を保持します。そのため、そのセッション中に追加のバグを報告する必要はありません。

   ［**ログイン**］エリアには、当該アプリケーションバージョンを対象に指定されたバグトラッカのフィールドが表示されます。
4. バグトラッカに必要なすべてのフィールドに入力し、［**SUBMIT**］をクリックします。

送信が成功すると、問題のバグアイコンが問題テーブルの［**Bug submitted**］列に表示されます。

参照情報

複数の問題のバグの送信

問題に対して送信されたバグの表示

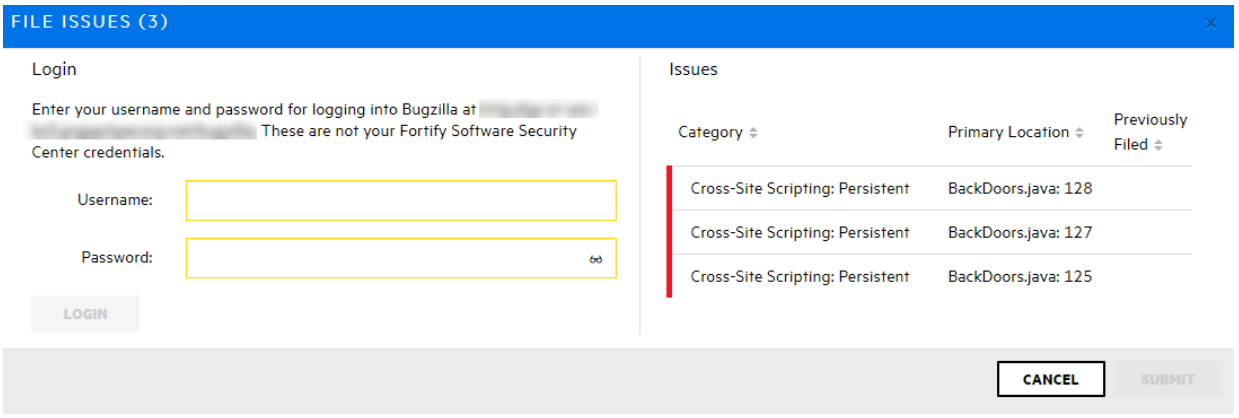
1.11.9.5. 複数の問題のバグの送信

アプリケーションバージョンに対してバグトラッキングプラグインが指定されている場合(アプリケーションバージョンへのバグトラッキングシステムの割り当て)、1つ以上の問題を対象にするバグを送信できます。1つの問題だけを対象にバグを報告する方法については、「単一の問題のバグの送信」を参照してください。

複数の問題を対象にする単一のバグを送信するには、次の手順に従います。

1. アプリケーションバージョンの［**監査(AUDIT)**］ページで、バグに含めるすべての問題のチェックボックスをオンにしてから、問題テーブルの上にある［**バグを報告(File Bug)**］ボタンをクリックします。

   チェックボックスをオンにした後で、［**バグの報告(File Bug)**］アイコンが表示されない場合は、まずアプリケーションバージョンのバグトラッカを設定する必要があります。「アプリケーションバージョンへのバグトラッキングシステムの割り当て」を参照してください。



> **Note**
>
> 選択した問題に対してバグが以前に送信されていた場合、その問題に対して新しいバグを送信することはできません。［**問題の報告(FILE ISSUES)**］ダイアログボックスには、「選択された問題の中に、報告済みの問題があります。これらの問題は無視されます(Some selected issues have already been filed and will be ignored)」というメッセージが表示され、［**報告済み(Previously Filed)**］列で、該当する問題にバグアイコンが示されます。

2. ［**ログイン**］エリアで、このアプリケーションバージョンに関連付けられたバグトラッカのユーザ名とパスワードを入力し、［**ログイン**］をクリックします。

Application Securityは、作業セッション中は資格情報を保持します。そのため、そのセッション中に追加のバグを報告する必要はありません。

［**ログイン**］セクションには、アプリケーションバージョン向けに指定されたバグトラッカのフィールドが表示されます。

3. すべての必須フィールドに入力し、［**SUBMIT**］をクリックします。

送信が成功すると、選択した問題のバグアイコンが問題テーブルの［**Bug submitted**］列に表示されます。

次も参照

単一の問題のバグの送信

問題に対して送信されたバグの表示

1.11.9.6. バグ状態管理

バグ状態管理では、バグ内の問題の状態が変化するのに合わせて、Application Securityでバグに対して特定の更新を加えることができます。Application Securityでは、新しいセキュリティスキャンをチェックして、報告されたバグが未解決のままなのか、終了できるのかを判断します。

分析結果に、以前に送信されたバグに関連するセキュリティ上の問題の中に、まだ解決されていないものが1つ以上あることが示されている場合(および、それらの問題が選択基準に一致する場合)、Application Securityはバグトラッキングシステムをチェックして、バグの状態が未解決の問題として有効であるかどうかを確認し、必要に応じてバグを再び未解決の問題にします。

バグに関連付けられているすべての問題が(修正されたか選択基準に一致しなくなったため)削除された場合、Application Securityはバグを更新して、利害関係者がチケットを解決または終了できることを示します。監査と追跡可能性を有効にするために、Application Securityではバグを自動的に解決または終了しません。

アプリケーションバージョンのバグの状態管理を有効にする方法については、「アプリケーションバージョンへのバグトラッキングシステムの割り当て」を参照してください。

1.11.10. アプリケーションバージョンに関連付けられているテンプレートを変更する

問題テンプレートを含め、既存のアプリケーションバージョンの多くの設定を変更できます。ただし、アプリケーションバージョンに別の問題テンプレートを割り当てるか、サーバ上の問題テンプレートを更新すると、データベースキャッシュと既存の監査セッション間の同期が失われるので、注意してください。

Caution

OpenTextでは、アプリケーションバージョンに関連付けられているテンプレートは、そのアプリケーションバージョンでの結果の処理が完了していない限り、変更しないことを推奨しています。すでに結果が処理されているアプリケーションバージョンの問題テンプレートを変更した場合、Application Securityは、問題メトリックは再計算されず、以前に割り当てられたテンプレートに基づいて生成されたメトリックは利用できず、削除することはできません。

アプリケーションバージョンに関連付けられているテンプレートを変更するには、次の手順に従います。

1. 管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**アプリケーション(Applications)**］を選択します。
3. 変更するアプリケーションバージョンを選択します。
4. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
5. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**アプリケーション設定(APPLICATION SETTINGS)**］をクリックします。
6. ［**バージョン設定(Version Settings)**］エリアで、編集ボタン🖊をクリックします。

   Caution

   テンプレートを変更すると、アプリケーションバージョンに対して計算されるメトリックスが変更される可能性があります。既存のメトリックは再計算されません。

7. ［**バージョンの編集(EDIT VERSION)**］ダイアログボックスで、［**テンプレート(TEMPLATE)**］タブをクリックします。

テンプレートのリストでは、現在割り当てられているテンプレートが選択済みとしてマークされます。

8. アプリケーションバージョンに使用するテンプレートのチェックボックスをオンにします。
9. ［**保存(SAVE)**］をクリックします。

テンプレートを変更すると、Application Securityにより、影響を受けるアプリケーションバージョンの監査セッション(別のユーザによるセッションなど)が無効にされて、アプリケーションバージョン監査セッションを再起動する必要があるというメッセージが表示されます。

Note

Fortify Audit Workbenchを使用して影響を受けるアプリケーションバージョンを監査するユーザには、この情報は表示されません。

1.11.11. アプリケーションバージョンの分析結果処理ルールを設定する

分析結果処理ルールにより、コードスキャンの管理者の承認と監視が可能になります。スキャンアーティファクトのアップロード時にアプリケーションバージョンの分析結果の処理に対して適用するルールを指定できます。

アプリケーションバージョンの分析結果処理ルールを設定するには:

1. 管理者としてサインインします。
2. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
3. 分析結果の処理ルールを設定する対象のアプリケーションバージョンを選択します。
4. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
5. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで［**処理ルール(PROCESSING RULES)**］タブを選択し、一覧表示されている処理ルールを確認します。
6. アプリケーションバージョンに適用する処理ルールのチェックボックスをオンまたはオフにします。

   次の表に、これらのルールの説明を記載します。

処理ルール	説明
Require approval if the Build Project is different between scans	Application Securityは、Build Projectのスキャンと、その前のスキャンを比較します。Build Projectが異なる場合は、スキャンをアップロードする前に管理者の承認が必要です。
Check external metadata file versions in scan against versions on server	ユーザがFPRファイルをアップロードしようとすると、Application Securityによってファイルの外部メタデータバージョンと Application Securityサーバ上の外部メタデータバージョンが比較されます。FPRファイルの外部メタデータバージョンがサーバ上の外部メタデータファイルバージョンよりも新しい場合、Application Securityはファイルのアップロードに対し、承認を要件とします。FPRファイルの外部メタデータバージョンがサーバ上の外部メタデータファイルのバージョンよりも古いか同じである場合、Application Securityは、FPRファイルのアップロードを許可します。
Require approval if file count decreases by more than 10% (ファイル数が10%を超えて減っている場合は承認を必要とする)	Application Securityは、スキャンのファイル数と直前のスキャンを比較します。ファイル数が10%を超えて減っている場合は、管理者が承認してからでないと、スキャンをアップロードできません。

処理ルール	説明
Require approval if file count increases by more than 10% (ファイル数が10%を超えて増えている場合は承認を必要とする)	Application Securityは、スキャンのファイル数と直前のスキャンを比較します。ファイル数が10%を超えて増えている場合は、管理者が承認してからでないと、スキャンをアップロードできません。
Require approval if result has Fortify Java Annotations (結果にFortify Java Annotationがある場合は承認を必要とする)	Application Securityは、スキャン結果にFortify Java注釈が含まれているかどうかをチェックします。注釈が1つでも検出された場合は、管理者が承認してからでないと、スキャンをアップロードできません。
Require approval if line count decreases by more than 10% (行数が10%を超えて減っている場合は承認を必要とする)	Application Securityは、スキャンと前のスキャンの行数を比較します。行数が10%を超えて減っている場合は、管理者が承認してからでないと、スキャンをアップロードできません。
Require approval if line count increases by more than 10% (行数が10%を超えて増えている場合は承認を要件とする)	Application Securityは、スキャンと前のスキャンの行数を比較します。行数が10%を超えて増えている場合は、管理者が承認してからでないと、スキャンをアップロードできません。

処理ルール	説明
Require approval if the engine version of a scan is newer than the engine version of the previous scan (スキャンのエンジンバージョンが前のスキャンのエンジンバージョンよりも新しい場合は承認を必要とする)	Application Securityは、スキャンエンジンバージョンがアプリケーションですでに使用されているバージョンよりも新しいかどうかをチェックします。新しいバージョンが検出された場合は、管理者が承認してからでないと、スキャンをアップロードできません。

処理ルール	説明
Ignore SCA quick scan results and SCA speed dial results performed with a setting of less than four (4未満の設定で実行されるSCAクイックスキャンの結果とSCAスピードダイヤルの結果を無視する)	クイックスキャンモードで実行されるOpenText SAST (Fortify Static Code Analyzer)スキャンの処理をブロックします。このスキャンでは、信頼レベルと重大度の高い問題が検索されます。このルールを使用すると、4未満のレベルで実行されたスピードダイヤル分析結果もアップロードされなくなります。 スピードダイヤル分析結果とクイックスキャン分析結果のアップロードを有効にするには、このチェックボックスをオフにします。 **Caution** OpenTextでは、フルスキャン分析結果のアップロードとスピードダイヤル分析結果のアップロードのどちらかを選択した後は、アプリケーションバージョン用にアップロードする以降の分析結果を同じタイプにするように推奨しています。

処理ルール	説明
Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan (スキャンで使用するRulepackが前のスキャンで使用したRulepackと一致しない場合は承認を必要とする)	Application Securityは、Rulepackを追加または削除したかどうか、およびRulepackのバージョンが変更されているかどうかをチェックします。Rulepackが追加、削除、または更新されていることが検出された場合は、管理者が承認してからでないと、スキャンをアップロードできません。
Require approval if SCA or WebInspect Agent scan does not have valid certification (SCAまたはWebInspect Agentスキャンに有効な証明書がない場合は承認を必要とする)	Application Securityは、OpenText SASTまたはOpenText DAST Agentスキャンに有効な証明書があるかどうかをチェックします。証明書が有効でない場合、誰かがアップロードの結果を改ざんした可能性があります。証明書が見つからない場合は、改ざんを検出できません。証明書が存在しないか有効でない場合、スキャンアップロードには管理者の承認が必要です。

処理ルール	説明
Require approval if result has analysis warnings	Application Securityは、OpenText SASTまたはOpenText DAST Agentスキャンに分析警告が含まれているかどうかをチェックします。分析警告が検出された場合、スキャンアップロードには管理者の承認が必要です。 **Note** この処理ルールは、所定の結果ファイルの最初のアップロードにのみ適用され、以降のアーティファクトのアップロードには適用されません。たとえば、以前にアップロードされた、分析警告を含むFPRファイルに監査情報が追加された場合、Application Securityでは、管理者の承認がなくても変更後のアーティファクトを再びアップロードできます。

処理ルール	説明
Perform Force Instance ID migration on upload	新しいバージョンのOpenText SAST (Fortify Static Code Analyzer)またはRulepackにより、それよりも前のバージョンのOpenText SASTまたはRulepackによるスキャンで作成されたインスタンスIDを変更できます。どちらのインスタンスIDも同じ問題を特定します。この処理ルールを有効にすると、OpenText SASTまたはRulepackのバージョンが同じ場合でも、古いインスタンスIDは対応する新しいインスタンスIDに強制的に移行されます。このルールの動作の詳細については、インスタンスIDマイグレーションに影響する処理ルールについてを参照してください。

処理ルール	説明
Automatically perform Instance ID migration on upload	新しいバージョンのOpenText SAST (Fortify Static Code Analyzer)またはRulepackにより、それよりも前のバージョンのOpenText SASTまたはRulepackによるスキャンで作成されたインスタンスIDを変更できます。どちらのインスタンスIDも同じ問題を特定します。このルールを有効にすると、問題の履歴を保持するために、古いインスタンスIDは対応する新しいインスタンスIDに自動的に移行されます。カスタマサポートのトラブルシューティング手段としては、このルールを無効にしたほうが役立つ場合があります。 このルールの動作の詳細については、インスタンスIDマイグレーションに影響する処理ルールについてを参照してください。
Warn if audit information includes unknown custom tag	監査情報に不明なカスタムタグが含まれる場合、処理ルールは管理者の承認を要件とします。
Require the issue audit permission to upload audited analysis files	監査された分析ファイルをアップロードしようとするユーザに、監査の問題に必要な許可(問題に対するカスタムタグ値の編集、問題へのコメントの追加、および問題の抑制と抑制解除)が与えられていない場合、この処理ルールにより、アップロードがブロックされます。

処理ルール	説明
Disallow upload of analysis results that change values of hidden tags (非表示にされたタグの値を変更する分析結果のアップロードを禁止する)	分析結果に、非表示にされたタグの値に対する変更が含まれる場合、Application Securityは分析結果のアップロードをブロックします。
Disallow upload of analysis results if there is one pending approval	分析結果に必要な承認がすべて行われていない場合、Application Securityは分析結果のアップロードをブロックします。
Disallow approval for processing if an earlier artifact requires approval	以前のスキャンアーティファクトが承認を必要とし、承認されていない場合、このルールはユーザによる現在のスキャンアーティファクトの承認をブロックします。 この処理ルールが選択されていない場合、ユーザが現在のアーティファクトを承認すると、それ以前のすべてのアーティファクトが自動的に承認されます。

7. ［**適用(APPLY)**］をクリックします。
8. 分析結果処理ルールの設定を保存することを確認するには、［**OK**］をクリックします。

インスタンスIDマイグレーションに影響する処理ルールについて

次の2つの処理ルールがインスタンスIDマイグレーションに影響します。「Perform Force Instance ID migration on upload (アップロード時にインスタンスIDの強制マイグレーションを実行する)」と「Automatically perform Instance ID migration on upload (アップロード時にインスタンスIDマイグレーションを自動的に実行する)」です。問題インスタンスIDは、次のいずれかの理由で変更される可能性があります。

- 新しいOpenText SASTバージョンでのIID生成アルゴリズムの変更
- 新しいRulepackバージョンの使用
- スキャン設定の変更

  たとえば、スキャンに対して追加のルールの使用が指定された場合。
- 脆弱なコードの複製

  たとえば、1つのアプリケーションバージョンで同じ脆弱なコードが複数回コピーされ、貼り付けられた場合。この場合、OpenText SASTにより最初の複製フラグメントに固有のインスタンスIDが生成されて、残りすべての複製フラグメントでは、生成されたそのインスタンスIDがインクリメントされて使用されます。したがって、別個の2回のスキャンのそれぞれで、所定のコードフラグメントが検出される順序によっては、同一のコードフラグメントに対して別々のインスタンスIDが作成される可能性があります。

「**Automatically perform Instance ID migration on upload (アップロード時にインスタンスIDマイグレーションを自動的に実行する)**」ルールは、新しいOpenText SASTバージョンによるIID生成アルゴリズムの変更またはRulepackバージョンでの変更が原因で発生する問題インスタンスIDの変更に対処するものです。たとえば、Application Securityが、最新のスキャンで使用されたOpenText SASTバージョンは以前のスキャンで使用されたバージョンよりも新しいことを検出したとします。この場合、「**Automatically perform Instance ID migration on upload (アップロード時にインスタンスIDマイグレーションを自動的に実行する)**」が選択されていれば、Application Securityがマイグレーションを実行します。Application Securityが、使用されているOpenText SASTバージョンでの変更を検出しなかった場合、マイグレーションは実行されません(「**Automatically perform Instance ID migration on upload (アップロード時にインスタンスIDマイグレーションを自動的に実行する)**」が選択されているとしても、マイグレーションは実行されません)。

「**Perform Force Instance ID migration on upload (アップロード時にインスタンスIDの強制マイグレーションを実行する)**」ルールでは、スキャン設定の変更または脆弱なコード複製が原因で発生するインスタンスIDの変更が解決されます。Application Securityは、OpenText SASTのバージョンまたはRulepackのバージョンが変更されたかどうかを簡単に判断できます。Application Securityは、このような変更を検出すると、マイグレーションを自動的に実行します。ただし、他のケース(コードの複製、スキャン設定)でApplication Securityがこの判断を行うことはできません。このような場合は、この処理ルールを使用して、Application Securityに強制的にマイグレーションを実行させることができます。

スキャン設定の変更または脆弱なコードの複製の結果として問題インスタンスIDが変更される可能性がある場合、OpenTextでは、「**Perform Force Instance ID migration on**

upload (アップロード時にインスタンスIDの強制マイグレーションを実行する)」処理ルールを選択することを推奨しています。

> **Note**
>
> インスタンスIDマイグレーションには時間がかかることが、この2つのルールが存在する理由です。IIDマイグレーションを毎回実行することが望ましくない場合もあるため、これらのルールでは、スキャンをアップロードするたびにインスタンスIDマイグレーションを実行するかどうかを決定できるようになっています。

参照情報

スキャンアーティファクトのアップロード

アプリケーションバージョンの分析結果を承認する

1.11.12. アプリケーションバージョンに対してFortify Audit Assistantオプションを設定する

Fortify Audit Assistantを設定する際に、デフォルトのFortify Audit Assistantオプションを上書きする機能を設定した場合は、特定のアプリケーションバージョンを対象に、これらのデフォルトオプションを上書きできます(「Fortify Audit Assistantの設定」を参照)。そうでない場合、すべてのアプリケーションバージョンにデフォルトの設定が使用されます。

アプリケーションバージョンに対してFortify Audit Assistantオプションを設定するには:

1. アプリケーションでFortify Audit Assistantを使用するようにApplication Securityが設定されていることを確認します。
2. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
3. Fortify Audit Assistantオプションを設定する対象のアプリケーションバージョンを選択します。
4. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
5. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**AUDIT ASSISTANTオプション(AUDIT ASSISTANT OPTIONS)**］タブを選択します。
6. ［**アプリケーションバージョンの予測ポリシー(Application version prediction policy)**］リストから、Fortify Audit Assistantでこのアプリケーションバージョンに適用する予測ポリシーを選択します。

   Note

   ［**Enable specific application version policies**］オプションがシステム全体で有効になっている場合にのみ、アプリケーションバージョン予測ポリシーを指定できます。そうでない場合、Fortify Audit Assistantはデフォルトの予測ポリシーを使用します。

7. このアプリケーションバージョンの監査されていない問題を評価のためにFortify Audit Assistantサーバに送信するには［**自動予測を有効にする(Enable auto-prediction)**］をオンにします。

Note

［**自動予測を有効にする(Enable auto-prediction)**］および［**自動適用を有効にする(Enable auto-apply)**］チェックボックスは、これらの監査設定がシステム全体で有効になっている場合にのみ使用できます。

8. マップされたカスタムタグ値に予測値がFortify Audit Assistantによって自動的に適用されるようにするには、［**自動適用を有効にする(Enable auto-apply)**］チェックボックスをオンにします。
9. ［**適用(APPLY)**］をクリックします。
10. 変更を確認するには、［**OK**］をクリックします。
11. ［**閉じる(CLOSE)**］をクリックします。

参照情報

Fortify Audit Assistantの設定

1.11.13. アプリケーションバージョンの自動適用と自動予測を有効にする

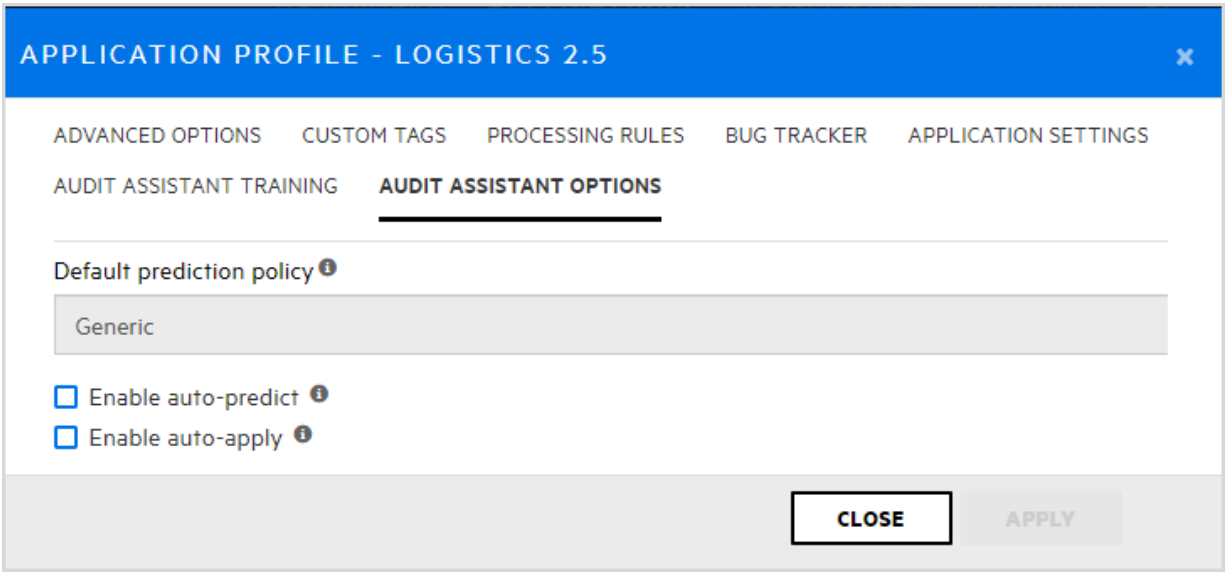
管理者がFortify Audit Assistantを設定済みで、自動適用をシステム全体で有効にして適切なプライマリタグフィールドをマップしてある場合、ユーザは特定のアプリケーションバージョンに対して自動適用を有効にできます。

自動適用をアプリケーションバージョンで有効にした場合、Fortify Audit Assistantを使用して静的分析の問題に関する予測を要求すると、Application Securityがそれらの予測をカスタムタグ値に適用します。

Fortify Audit Assistantが自動的にカスタムタグ値を問題に適用すると、その問題のために保存されたメタデータは、それがFortify Audit Assistantによって監査されたことを示します。カスタムタグ名の横に、ユーザにFortify Audit Assistantがその問題を予測したことを示すグレーの小槌が表示されます。

アプリケーションバージョンの自動適用を有効にするには:

1. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］で、自動適用を有効にするアプリケーションバージョンを選択します。
2. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
3. ［**AUDIT ASSISTANT OPTIONS**］を選択します。



4. 未監査の問題をFortify Audit Assistantで自動的に評価するには、［**自動予測を有効にする(Enable auto-predict)**］チェックボックスをオンにします。

   自動予測の詳細については、「Audit Assistantの自動予測について」を参照してください。

5. ［**Enable auto-apply**］チェックボックスをオンにします。

   プライマリタグの値がAudit Assistantにマップされていない場合、Application Securityがその影響に関する警告を表示し、管理者に問い合わせるようアドバイスします。

6. ［**適用(APPLY)**］をクリックします。
7. 設定を保存するには、［**OK**］をクリックします。
8. ［**閉じる(CLOSE)**］をクリックします。

参照情報

Fortify Audit Assistantの設定

1.11.14. カスタムタグについて

Application Securityでコードを監査するために、セキュリティチームは分析結果を調べ、アプリケーションの問題に関連する「タグ」に値を割り当てます。開発チームは、これらのタグ値を使用して、対処する問題と順序を決定できます。

デフォルトで、Application Securityに用意されているタグは、問題の評価に使用する［**分析(Analysis)**］という名前のデフォルトタグのみです。［**分析(Analysis)**］タグの有効な値は、［**悪用可能(Exploitable)**］、［**問題でない(Not an Issue)**］、［**疑わしい(Suspicious)**］、［**信頼性の問題(Reliability Issue)**］、および［**不適切な手法(Bad Practice)**］です。［**分析(Analysis)**］タグでは、属性の変更、タグ値の変更、監査ニーズをサポートする新しいタグ値の追加を行うことができます。

監査プロセスを絞り込むために、独自のカスタムタグを定義できます。［**分析(Analysis)**］タグと同様に、カスタムタグ定義は、アプリケーションバージョンに関連付けることができる問題テンプレートに保存されます。たとえば、問題のサインオフプロセスを追跡するために使用するカスタムタグを作成できます。開発者が自分に割り当てられた問題を監査した後、セキュリティの専門家がそれらの問題を確認して、それぞれの問題を「承認済み」または「不承認」としてマークできます。

Note

Fortify Audit Workbenchのユーザは、監査時にカスタムタグをプロジェクトに追加できます。ただし、対応するアプリケーションバージョンに関連付けられている問題テンプレートに対してこれらのカスタムタグがApplication Securityで定義されていない場合、Fortify Audit WorkbenchユーザがFPRファイルをApplication Securityにアップロードすると、新しいカスタムタグは失われます。

このセクションでは、次のトピックについて説明します。

1.11.14.1. システムへのカスタムタグの追加

管理者は、システムにカスタムタグを追加できます。

> **Note**
>
> 作成してアプリケーションバージョンに割り当てるカスタムタグの値に基づいて、問題をフィルタできます。詳細については、「概要ページと監査ページに表示する問題をフィルタ処理する」を参照してください。

カスタムタグを追加するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］を選択します。
3. ［**カスタムタグ(Custom Tags)**］ページで、［**新規(NEW)**］をクリックします。
4. ［**名前(Name)**］ボックスに新しいタグの名前を入力します。

   > **Important**
   >
   > カスタムタグに指定する名前がデータベース予約語でないことを確認します。

5. (オプション)［**Description**］ボックスに、カスタムタグの使い方を説明するコンテンツを入力します。
6. ［**タイプ(Type)**］リストから、次の表に一覧表示されているタグタイプの1つを選択します。

Type	受諾可能な値
Date	システム全体の初期設定で指定されている形式のカレンダの日付(「システム全体およびアプリケーションバージョンのすべてにわたる初期設定の設定」を参照)。
Decimal	最高18桁の精度を持つ数値(小数点以下9桁まで)
List	タグに指定する値のリストから選択
Text	最大500文字の文字列(HTML/XMLタグおよび新規改行は使用できない)

7. (オプション)次のオプションのタグ機能の一部またはすべてを選択します。
    - **制限(Restricted)**—特定の許可を持つユーザ(マネージャ、セキュリティリード、管理者)にのみタグの変更を許可するには、このチェックボックスをオンにします。
    - **拡張可能(Extensible)**—(リストタイプのみ)リストタイプのカスタムタグを拡張可能にします。つまり、監査官は問題を監査するときに値を追加できます。監査時にユーザがリストタグに新しい値を追加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。
    - **非表示(Hidden)**—［**割り当て(ASSIGN)**］ダイアログボックスやFortify Audit Workbenchでタグが表示されないようにするには、このチェックボックスをオンにします。
    - **コメントが必要(Requires comment)**—ユーザがこのカスタムタグの値を変更する際に常にコメントを残すことを要件とする場合は、このチェックボックスをオンにします。コメントを必要とするカスタムタグが変更されると、システムは自動的にコメントを追加して、タグに変更が加えられたことを示します。

> **Note**
>
> コメントを必要とする新しいカスタムタグが日付タイプタグの場合、監査中にユーザがタグに対して選択する日付は、常に［**初期設定(PREFERENCES)**］ダイアログボックスで指定されている形式になります。

8. 新しいカスタムタグが日付タグ、10進数タグ、またはテキストタイプのタグの場合は、［**保存(Save)**］をクリックします。新しいカスタムタグがリストタイプタグの場合は、値を追加する必要があります。リストタイプのカスタムタグの値を作成する方法については、「カスタムタグ値の追加」を参照してください。

次も参照

Application Securityカスタムタグ値へのFortify Audit Assistant分析タグ値のマッピング

カスタムタグをグローバルで非表示にする

カスタムタグの削除

Custom tags

カスタムタグを編集する

カスタムタグと問題テンプレートを関連付ける

問題テンプレートによるカスタムタグの管理

FPRファイル内の問題テンプレートを使用したカスタムタグの管理

1.11.14.2. カスタムタグ属性の変更

カスタムタグの属性を変更するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］をクリックします。
3. ［**カスタムタグ(Custom Tags)**］ページで、変更するタグを表示する行をクリックします。

   行が展開され、詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. タグ属性を変更し、変更を保存します。

> **Caution**
>
> カスタムタグに指定する名前がデータベース予約語でないことを確認します。

参照情報

カスタムタグ値の追加

システムへのカスタムタグの追加

1.11.14.3. カスタムタグをグローバルで非表示にする

カスタムタグをグローバルで非表示にするには、次の操作をします。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］をクリックします。
3. 非表示にするタグの行をクリックします。

   行が展開されて、タグの詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. ［**Hidden**］チェックボックスを選択します。
6. ［**保存(SAVE)**］をクリックします。

非表示にしたカスタムタグは、［**監査(AUDIT)**］ページやFortify Audit Workbenchで表示されなくなります。

1.11.14.4. カスタムタグの削除

管理者またはセキュリティリードは、カスタムタグを削除できます。

Note

次の場合は、カスタムタグを削除できません。

- プライマリタグとして設定されている。
- 問題の監査で使用されている。
- 現在、アプリケーションバージョンまたは問題テンプレートに関連付けられている。アプリケーションバージョンからカスタムタグを削除する方法については、「カスタムタグをアプリケーションバージョンから関連付け解除する」を参照してください。問題テンプレートからカスタムタグを削除する方法については、「問題テンプレートからのカスタムタグの削除」を参照してください。

［**分析(Analysis)**］タグを削除することはできません。

カスタムタグを削除するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］をクリックします。
3. 削除するカスタムタグのチェックボックスをオンにします。
4. ［**カスタムタグ(Custom Tags)**］ツールバーで［**削除(DELETE)**］をクリックします。
5. 選択したタグの削除を確認するには、［**OK**］をクリックします。

参照情報

Custom tags

1.11.14.5. カスタムタグ値の追加

管理者は、リストタイプのカスタムタグに値を追加できます。

Note

カスタムタグに拡張可能属性が割り当てられている場合は、問題の監査時に値を追加できます。

Fortify Audit Assistantが設定されている場合は、「カスタムタグ値を追加する([%=FortifyProducts_Vars.AuditAssistant%]が設定されている場合)」を参照してください。

リストタイプのカスタムタグに値を追加するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］をクリックします。
3. 値を編集する対象のタグの行をクリックします。
4. ［**編集(EDIT)**］をクリックします。
5. ［**+ ADD**］をクリックします。

   ［**値の追加(ADD VALUE)**］ダイアログボックスが開きます。
6. 名前を入力し、必要に応じて新しい値の説明を入力します。
7. (オプション)［割り当て(Assign)］ダイアログボックスやFortify Audit Workbenchでタグが表示されないようにするには、［**非表示(Hidden)**］チェックボックスをオンにします。
8. ［**適用(APPLY)**］、［**保存(SAVE)**］の順にクリックします。
9. (オプション)問題の状態を設定します。
10. さらに値を追加するには、ステップ5～9を繰り返します。

次も参照

カスタムタグ値を追加する([%=FortifyProducts_Vars.AuditAssistant%]が設定されている場合)

カスタムタグをアプリケーションバージョンに割り当てる

1.11.14.5.1. カスタムタグ値を追加する (Fortify Audit Assistantが設定済みの場合)

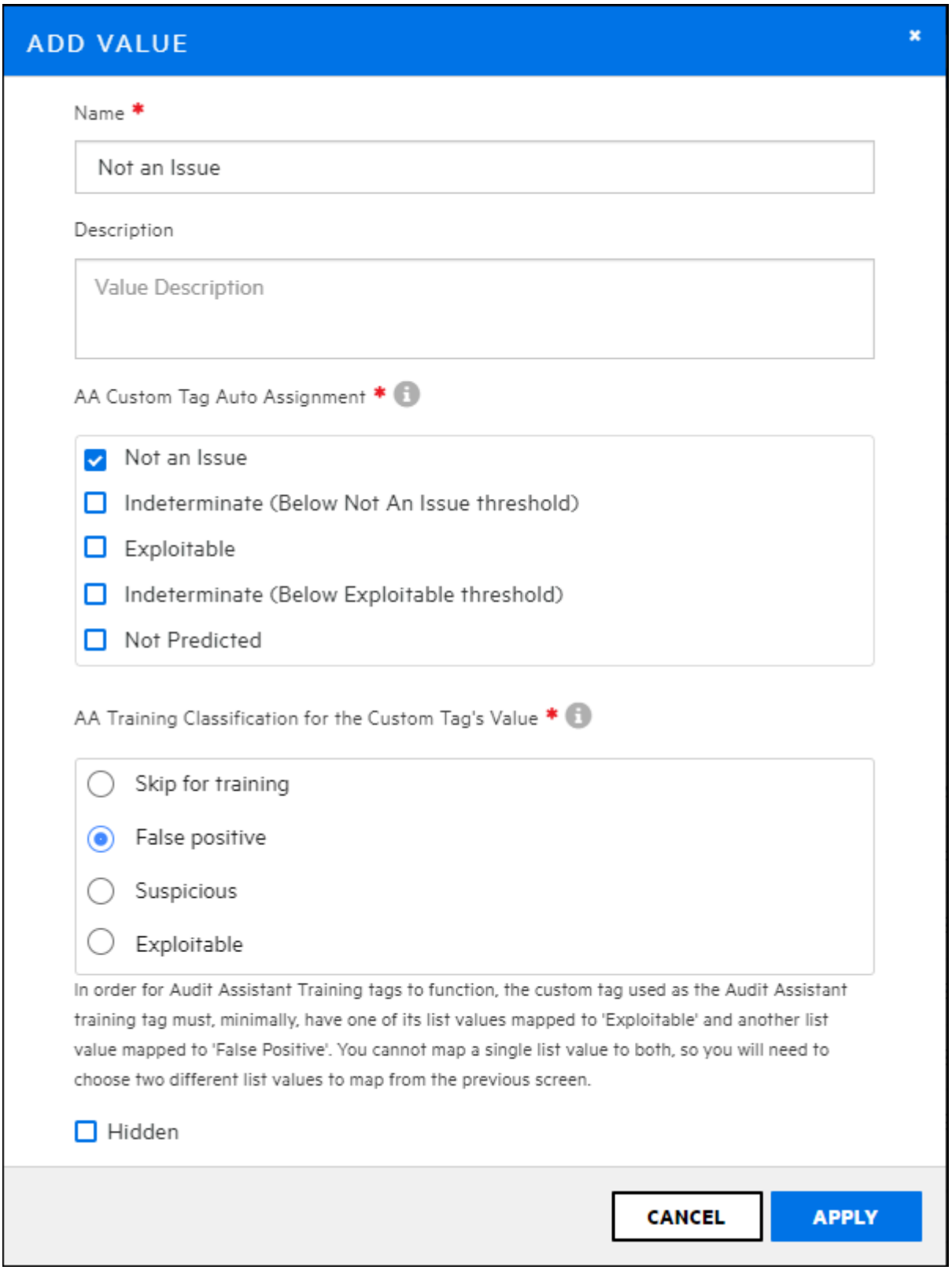
カスタムタグ値を追加または編集する際は、次の操作を行います。

- 新しい値の名前を指定する
- (オプション)新しい値の説明を入力する
- カスタム値をFortify Audit Assistantの値にマップし、Fortify Audit Assistantモデルのトレーニングでその値を使用するかどうかを決定する
- 値を問題の状態に割り当てる

Fortify Audit Assistantが設定済みの場合にリストタイプのカスタムタグに値を追加するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］をクリックします。
3. 値を編集する対象のタグの行をクリックします。
4. ［**編集(EDIT)**］をクリックします。
5. ［**+ ADD**］をクリックします。

   Fortify Audit Assistantの自動適用機能が有効になっている場合、［**値の追加(ADD VALUE)**］ダイアログボックスには［**AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)**］エリアと［**カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)**］エリアが表示されます。



6. 新しい値が［**AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)**］エリアのFortify Audit Assistantの予測値と一致する場合、そのチェックボックスをオンにすると、選択したAudit Assistantの予測値にそのリスト値が自動的にマップされます。

   これにより、自動適用機能を有効にしているすべてのアプリケーションバージョンで、値の自動マッピングが可能になります。

7. Fortify Audit Assistantをトレーニングするには、このカスタムタグ値がFortify Audit Assistantに対して持つ意味を選択します。Fortify Audit Assistantのトレーニングで使用するリスト値ごとに、このステップを繰り返します。

   問題にこのタグ値を設定すると、Fortify Audit Assistantは、ユーザによる問題分類に基づいて、ユーザが問題をどのように捉えているかを学習します。トレーニングですべてのリスト値を使用する必要はありませんが、トレーニングを行うには、少なくとも2つ割り当てる必要があります。［**悪用可能(Exploitable)**］と［**誤検出(False Positive)**］のそれぞれに、1つの値を割り当てる必要があります。

8. (オプション)問題の監査時や、Fortify Audit Workbenchでタグが表示されないようにするには、［**非表示(Hidden)**］チェックボックスをオンにします。

9. (オプション)問題の状態を設定します(「問題の状態を設定する」を参照)。
10. ［**適用(APPLY)**］、［**保存(SAVE)**］の順にクリックします。

Note

新しいカスタムタグを使用してアプリケーションバージョンの問題を監査するには、まずタグをアプリケーションバージョンに割り当てる必要があります。手順については、「アプリケーションバージョンへのカスタムタグの割り当て」を参照してください。

1.11.14.5.2. 問題の状態を設定する

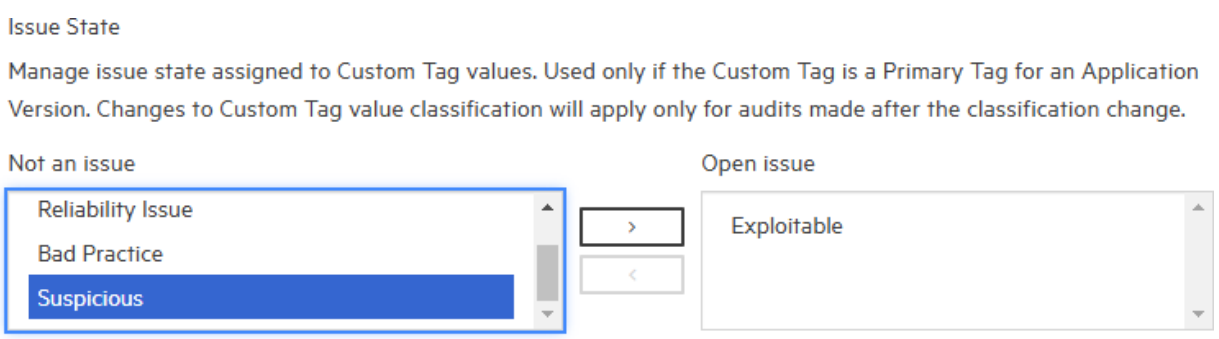
カスタムタグに値を追加する際に、Fortify Audit Assistantが有効になっている場合は、その問題の状態を設定できます。問題の状態を使用して、［問題でない(Not an Issue)］か［未解決の問題(Open Issue)］のいずれかのカテゴリに問題を割り当てることができます。結果を監査する際に、［**グループ化条件(Group By)**］メニューから［**問題の状態(Issue State)**］を選択すると、解決を要する問題とその数をすばやく評価できます。問題を監査し、［**分析(Analysis)**］カスタムタグに値を割り当てると、選択した値に基づいて［問題の状態(Issue State)］フォルダが更新されます。

カスタムグループは、プライマリタグに設定された分析のレベルに基づき、監査された問題が［未解決の問題(Open Issue)］と［問題でない(Not an Issue)］のどちらであるかを定義します。［疑わしい(Suspicious)］および［悪用可能(Exploitable)］に等しい値は、分析タグで［未解決の問題(Open Issue)］と見なされます。

追加されたリストタイプのすべてのカスタムタグ値は、初期状態では［**問題の状態(Issue State)**］エリアの［**問題でない(Not an issue)**］リストに表示されます。

カスタムタグ値の［問題の状態(Issue State)］を設定する

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］をクリックします。
3. 値を編集するタグの行をクリックします。
4. ［**編集(EDIT)**］をクリックします。
5. ［**問題の状態(Issue State)**］エリアで、未解決の問題とみなす値を選択します。
6. ［**選択した値を移動(Move selected)**］ボタン›を使用して、選択した値を［**問題でない(Not an issue)**］リストから［**未解決の問題(Open issue)**］リストに移動します。



7. すべての値が適切な問題の状態リストに表示されるまで、ステップ5～6を繰り返します。
8. ［**保存(SAVE)**］をクリックします。

次も参照

カスタムタグを編集する

カスタムタグ値の削除

システムへのカスタムタグの追加

カスタムタグをアプリケーションバージョンに割り当てる

1.11.14.6. カスタムタグを編集する

管理者レベルのユーザの場合は、カスタムタグを本システムで変更できます。

カスタムタグを編集するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］を選択します。
3. 編集するタグの行をクリックして展開し、詳細を表示します。
4. ［**編集(EDIT)**］をクリックします。
5. 表示されたフィールドの値を編集して、［**SAVE**］をクリックします。

参照情報

システムへのカスタムタグの追加

カスタムタグ値の削除

カスタムタグをアプリケーションバージョンに割り当てる

1.11.14.7. カスタムタグ値の削除

管理者やセキュリティリードは、カスタムタグ値を削除できます。

> **Note**
>
> カスタムタグ値がアプリケーションバージョンや問題テンプレートに現在関連付けられている場合や、問題の監査で使用されている場合、そのカスタムタグ値を削除することはできません。

カスタムタグの値を削除するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］を選択します。
3. 値を削除するタグの行をクリックします。

   行が展開されて、タグの詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. 値のテーブルで、削除する値の行にある［**値を削除(Remove value)**］ボタンをクリックします。
6. ［**保存(SAVE)**］をクリックします。

参照情報

カスタムタグを編集する

システムへのカスタムタグの追加

カスタムタグ値の追加

1.11.14.8. カスタムタグと問題テンプレートを関連付ける

最初に問題テンプレートを作成して問題テンプレートファイルをアップロードした後、その問題テンプレートファイルで定義されているカスタムタグは、最初に問題テンプレートに関連付けられているカスタムタグです。既存のカスタムタグの更新が無視される理由は、タグが前のセクションで説明した手順を使用して更新されるように設計されているけれども、その問題テンプレートファイルで新しく定義されたカスタムタグがシステムに追加され、問題テンプレートに関連付けられているためです。

> **Note**
>
> 問題テンプレートに関連付けられているカスタムタグは、その問題テンプレートを使用して最初に作成されるときにアプリケーションバージョンに割り当てられるデフォルトのタグセットです。

カスタムタグを問題テンプレートに関連付けるには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を選択し、［**問題テンプレート(Issue Templates)**］を選択します。
3. カスタムタグに関連付ける問題テンプレートが表示された行をクリックします。

   行は展開されて、テンプレートの詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. ［**カスタムタグ(CUSTOM TAGS)**］エリアで、［**+カスタムタグを追加(+ADD CUSTOM TAG)**］をクリックします。
6. ［**カスタムタグの追加(ADD CUSTOM TAG)**］ダイアログボックスで、問題テンプレートに関連付けるカスタムタグのチェックボックスをオンにして、［**+追加(+ADD)**］をクリックします。
7. ［**保存(SAVE)**］をクリックします。

参照情報

カスタムタグをアプリケーションバージョンから関連付け解除する

1.11.14.9. 問題テンプレートからのカスタムタグの削除

問題テンプレートからカスタムタグを削除するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**問題テンプレート(Issue Templates)**］を選択します。
3. 削除するカスタムタグに関連付けられた問題テンプレートを表示する行をクリックします。

   行が展開され、問題テンプレートの詳細が表示されます。［**カスタムタグ(CUSTOM TAGS)**］エリアには、テンプレートに現在関連付けられているカスタムタグが一覧表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. 最後の列で、テンプレートから削除するカスタムタグの［**カスタムタグを削除(Remove custom tag)**］ボタンをクリックします。

   > **Note**
   >
   > 問題テンプレートから指定したプライマリタグを削除することはできません。
6. ［**保存(SAVE)**］をクリックします。

参照情報

Custom tags

1.11.14.10. カスタムタグをアプリケーションバージョンに割り当てる

新しいカスタムタグを使用してアプリケーションバージョンの問題を監査するには、まずタグをアプリケーションバージョンに割り当てる必要があります。

カスタムタグをアプリケーションバージョンに割り当てるには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. 編集するアプリケーションバージョンを選択します。または、アプリケーションの行を展開し、監査するバージョンの名前を選択します。
3. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
4. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**カスタムタグ(CUSTOM TAGS)**］タブを選択します。
5. ［**ASSIGN/REMOVE**］をクリックします。

   ［**CUSTOM TAGS**］タブには、監査の問題で使用可能なすべてのタグが一覧表示されます。
6. アプリケーションバージョンに割り当てるカスタムタグのチェックボックスをオンにして(複数のタグを選択できます)、［**DONE**］をクリックします。

   選択したタグは、割り当てられたタグとして一覧表示されています。

   Application Security で問題の監査を正常に完了するには、「プライマリタグ」として指定されているカスタムタグの値を指定する必要があります。デフォルトでは、［**分析(Analysis)**］タグがプライマリタグになります。

   監査時に、プライマリタグは最初に一覧表示されます。［**分析(Analysis)**］以外のリストタイプのカスタムタグがApplication Securityインスタンスに存在し、アプリケーションバージョンに割り当てられている場合は、それらのタグのいずれかを(［**分析(Analysis)**］タグの代わりに)プライマリタグとして選択できます。
7. (オプション)現在のプライマリタグ以外のタグをプライマリとして割り当てるには:

Note

list-typeカスタムタグを割り当てることができるのは、プライマリタグとする場合だけです。

1. ［**SELECT PRIMARY**］をクリックします。
2. ［**プライマリタグの選択(Select Primary Tag)**］リストから、プライマリカスタムタグとして設定するタグを選択します。

   Note

   Fortify Audit Assistantを使用する場合、Fortify Audit Assistantのガイダンス情報をまだ提供していなければ、タグを編集してその情報を含める必要があります。Fortify Audit Assistantのガイダンスを提供する方法については、「システムへのカスタムタグの追加」を参照してください。カスタムタグを編集する方法については、「カスタムタグを編集する」を参照してください。

3. ［**DONE**］をクリックします。

8. ［**閉じる(CLOSE)**］をクリックします。

割り当てられたカスタムタグは、次にチームメンバーがアプリケーションバージョンに関する問題を監査するときに使用可能になります。

参照情報

カスタムタグをアプリケーションバージョンから関連付け解除する

1.11.14.11. カスタムタグをアプリケーションバージョンから関連付け解除する

カスタムタグをアプリケーションバージョンから関連付け解除できるのは、そのアプリケーションバージョンの監査で使用していない場合です。

カスタムタグをアプリケーションバージョンから関連付け解除するには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. カスタムタグが割り当てられているアプリケーションバージョンを選択します。
3. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
4. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**カスタムタグ(CUSTOM TAGS)**］タブを選択します。
5. ［**割り当て/削除(ASSIGN/REMOVE)**］をクリックします。

   ［**CUSTOM TAGS**］タブには、システム内のすべてのカスタムタグが一覧表示されます。アプリケーションバージョンに関連付けられているタグのチェックボックスが選択されています。
6. 削除するカスタムタグのチェックボックスをオフにして、［**DONE**］をクリックします。
7. ［**閉じる(CLOSE)**］をクリックします。

このアプリケーションバージョンの［**監査(AUDIT)**］ページの［**監査(AUDIT)**］タブでは、削除したカスタムタグが問題詳細に一覧表示されなくなります。

すべてのアプリケーションバージョンとこれが割り当てられている問題テンプレートからカスタムタグを削除した後には、そのタグを削除できます。

参照情報

問題テンプレートからのカスタムタグの削除

システムへのカスタムタグの追加

カスタムタグをアプリケーションバージョンに割り当てる

1.11.14.12. 問題テンプレートによるカスタムタグの管理

問題テンプレートファイルで定義されたカスタムタグは、その特定の問題テンプレートに割り当てられます。直接問題テンプレートをアップロードして既存のカスタムタグを更新することはできません。Application Securityで更新されたカスタムタグが検出されると、警告が表示され、続行を確認するメッセージが表示されます。

次のように、Application Securityのカスタムタグ管理セクションを使用して既存のカスタムタグを更新する必要があります。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］を選択します。
3. 更新を完了します。

問題テンプレートのアップロードを通じて新しいカスタムタグを追加できます。これにより、たとえばソフトウェア監査に参加していないセキュリティチームのメンバーが、問題テンプレートおよび問題テンプレートのカスタムタグを定義できます。

1.11.14.13. FPRファイル内の問題テンプレートを使用したカスタムタグの管理

通常、FPRファイルには問題のテンプレートが含まれています。Application Securityにアップロードされ たFPRファイルに、編集可能として設定されたカスタムタグを含む問題テンプレートが含まれている場合は、タグに値を追加できます。

1.11.15. アプリケーションバージョンの削除について

Application Securityでアプリケーションを直接削除することはできません。Application Securityでは、すべてのバージョンが削除された後にアプリケーションを自動的に削除します。

Application Securityで管理者の役割が割り当てられている場合 は、任意のアプリケーションバージョンを削除できます。セキュリティリードまたはマネージャの役割を持っている場合は、割り当てられているアプリケーションバージョンを削除できます。

バージョンを削除するのではなく、［**ダッシュボード(Dashboard)**］ビューおよび［**アプリケーション(Applications)**］ビューに表示されないようにしたい場合は、バージョンを無効化できます。

このセクションでは、次のトピックについて説明します。

1.11.15.1. アプリケーションバージョンの無効化

アプリケーションバージョンを無効にすると、そのバージョンが［**アプリケーション(Applications)**］ビューで非表示にされます。

アプリケーションバージョンを無効にするには、次の手順を実行します。

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. 無効にするアプリケーションバージョンを選択します。
3. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
4. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**アプリケーション設定(APPLICATION SETTINGS)**］タブをクリックします。
5. ［**Version Settings**］ペインで、［**DEACTIVATE**］をクリックします。
6. ［**OK**］をクリックして、アプリケーションバージョンの無効化を確認します。

   必要に応じて、後でバージョンを再度有効にできます。
7. ［**閉じる(CLOSE)**］をクリックします。

参照情報

アプリケーションバージョンの再有効化

アプリケーションバージョンの削除

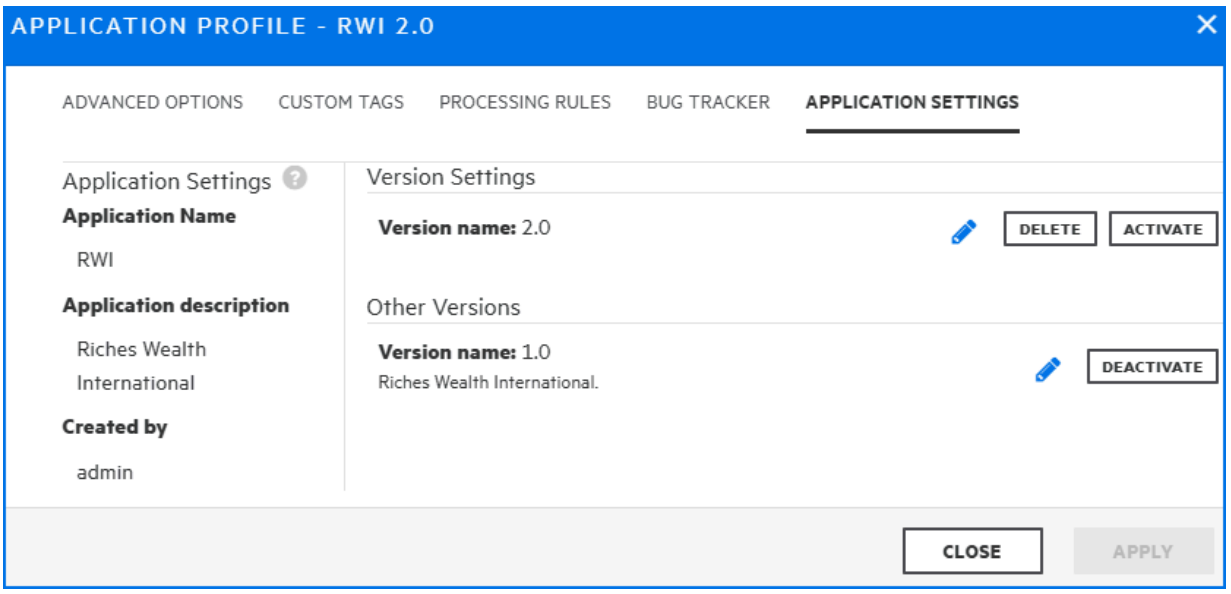
1.11.15.2. アプリケーションバージョンの再有効化

特定のアプリケーションバージョンが無効にされていて、［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューに一覧表示されていない場合、そのバージョンを再度有効化して再び表示することができます。

無効にされたアプリケーションバージョンが、そのアプリケーションの唯一のバージョンである場合は、まず、無効にされたアプリケーションの新しいバージョンを作成してから、次の手順に従ってアプリケーションを再度有効にする必要があります。

アプリケーションの別のバージョンが存在する場合にアプリケーションバージョンを再度有効化するには、次の手順に従います。

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. ［フィルタ(Filters)］で、［**非アクティブなバージョンを含める(Include inactive versions)**］スイッチをオンにします(または、［**レガシービュー(Legacy View)**］で［**非アクティブなバージョンの表示(Show inactive versions)**］チェックボックスをオンにします)。
3. 非アクティブなアプリケーションバージョンを選択します。
4. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
5. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**アプリケーション設定(APPLICATION SETTINGS)**］タブを選択します。



6. ［**有効化(ACTIVATE)**］をクリックします。

7. 有効化を確認するには、［**OK**］をクリックします。

8. ［**閉じる(CLOSE)**］をクリックします。

アプリケーションバージョンが、［**ダッシュボード(Dashboard)**］ビューおよび［**アプリケーション(Applications)**］ビューに再び表示されます。

1.11.15.3. アプリケーションバージョンの削除

アプリケーションバージョンを削除するのではなく、Application Securityの［**ダッシュボード(Dashboard)**］ビューおよび［**アプリケーション(Applications)**］ビューで表示されないようにする場合は、「アプリケーションバージョンの無効化」を参照してください。

> **Important**
>
> アプリケーションのすべてのバージョンを削除すると、Application Securityにより、そのアプリケーションが自動的に削除されます。

Application Securityアプリケーションバージョンを削除するには:

1. ［**アプリケーション(Applications)**］ビューで、削除するアプリケーションバージョンを選択します。
2. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
3. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**アプリケーション設定(APPLICATION SETTINGS)**］タブを選択します。
4. ［**Version Settings**］ペインで、［**Delete**］をクリックします。

   Application Securityに、バージョンの削除を確認するメッセージが表示されます。
5. ［**OK**］をクリックします。

Application Securityにより、当該バージョンがデータベースから削除されます。

1.12. Webhookについて

Null

Webhookを作成して、Application Securityで発生するイベントに関して外部システムを更新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。

1.12.1. Webhookの許可

次の表は、Webhookに関連するタスクを実行する許可を持つApplication Securityの役割を示しています。

役割	許可
管理者	ユーザはWebhookを作成、表示、および管理して、イベントを監視できます。
セキュリティリード	• ユーザはWebhookを表示できます。Webhookで監視されるアプリケーションバージョンには、ユーザが明示的な表示許可を持っているアプリケーションのみが含まれるようにフィルタが適用されます。 • ユーザは、明示的な表示許可を持っているエンティティでのみWebhook監視イベントを作成および管理できます。 セキュリティリードは、次の情報を作成または管理できません。 • ［**全部送ってください(Send me everything!)**］オプションが選択されているWebhook • ［**All Application Versions**］オプションが選択されたWebhook • ユニバーサルアクセスが必要なイベントを監視するために設定されたWebhook

参照情報

Application Securityの役割に与えられている許可を表示する

1.12.2. Webhookの作成

Null

管理者はWebhookを作成して、グローバルのイベントとアプリケーションバージョン固有のイベントのいずれかを監視できます。セキュリティリードは、表示する許可を持つエンティティのイベントを監視するWebhookを作成できます。

新しいWebhookを作成するには、次の手順を実行します。

1. Application Securityに管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**Webhook (Webhooks)**］を選択します。
4. ［**Webhook (Webhooks)**］ページで、［**新規(NEW)**］をクリックします。
5. ［**新しいWebhookの作成(CREATE NEW WEBHOOK)**］ダイアログボックスで、次の表で説明する情報を入力します。

フィールド	説明(Description)
Payload URL	要求されたペイロードの送信先のURLを指定します。
説明(Description)	(オプション)Webhookとそのペイロードの説明を指定します。
SSL Verification	指定したURLに基づいてWebhookを呼び出すのにSSL証明書の検証が必要かどうかを指定します。
Use SSC proxy	(オプション) Application Security統合用にプロキシを設定している場合は、このチェックボックスをオンにすると、それをWebhookに使用できます。Application Security統合用にプロキシを設定する方法については、「Application Security統合用のプロキシの設定」を参照してください。
Content Type	配信されるペイロードに使用されるフォーマットを指定します。 **Note** JSONは現在サポートされている唯一のコンテンツタイプです。

フィールド	説明(Description)
Secret	(オプション) POST要求のデータ整合性および真正性を検証するために使用されるWebhookシークレットを入力します。シークレットはハッシュベースメッセージ認証コード(HMAC)を計算するために使用されます。HMACは「X-SSC-Signature」ヘッダを介してペイロードの宛先に伝達されます。このコードはHMAC-SHA256アルゴリズムを使用して計算されます。シークレットはキーとして使用され、ペイロード本文(HTTPの「Date」ヘッダ値が追加された状態)がメッセージとして使用されます。HMAC値は、`sha256=`プレフィックスを持つ16進数としてエンコードされます。

フィールド	説明(Description)
Which events would you like to trigger this webhook?	次のいずれかを実行します。 ◦ ペイロードに以下のイベントを含めるには、［**全部送ってください(Send me everything!)**］を選択します。これは、現在および将来のすべてのイベントに適用されます。 ◦ 注目しているイベントのサブセットをペイロードに含めるには、［**個別イベントを選択する(Let me select individual events)**］を選択し、［**グローバルイベント(Global Events)**］リストと［**アプリケーションバージョンイベント(Application version events)**］リスト(下記参照)で、ペイロードに含めるイベントのチェックボックスをオンにします。

フィールド	説明(Description)
	グローバルイベント(システム全体): **USER_CREATED**: 新しいローカルユーザ、ローカルグループ、またはLDAPエンティティがApplication Securityに追加されました。 **USER_DELETED**: ローカルユーザ、ローカルグループ、またはLDAPエンティティがApplication Securityから削除されました。 **USER_UPDATED**: ローカルユーザ、ローカルグループ、またはLDAPエンティティが更新されました。 **LOCAL_USER_ACCOUNT_LOCKED**: 無効な資格情報によるサインイン試行が多すぎるため、Application Securityからローカルユーザがロックアウトされました。 **APP_VERSION_CREATED**: Application Securityで新しいアプリケーションバージョンが作成されました。 **APP_VERSION_DELETED**: Application Securityからアプリケーションバージョンが削除されました。 **REPORT_GENERATION_COMPLETE**: 要求された新しいレポートを表示およびダウンロードできます。 **REPORT_GENERATION_REQUESTED**: 新しいレポートが要求されました。

フィールド	説明(Description)
	アプリケーションバージョンイベント(アプリケーションバージョン固有): **ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS:** アップロードされたアーティファクトの処理が正常に行われ、そのデータが使用可能です。 **ANALYSIS_RESULT_UPLOAD_FAILURE:** アップロードされたアーティファクトは正常に処理されませんでした。 **ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL:** アップロードされたスキャンアーティファクトを処理するには承認が必要です。 **ANALYSIS_RESULT_INDEXING_COMPLETED:** アップロードされたアーティファクトの処理をApplication Securityが終了した後に、グローバル検索のためのデータのインデックス付けが完了しました。 **ANALYSIS_RESULT_UPLOAD_APPROVE:** アーティファクトのアップロードが承認されました。 **APP_VERSION_UPDATED:** アプリケーションのバージョンが更新されました。

フィールド	説明(Description)
監視対象のアプリケーションバージョン (Which application versions would you like to monitor?)	次のいずれかを実行します。 ◦ すべてのアプリケーションバージョン(既存のアプリケーションバージョンと今後作成されるアプリケーションバージョン)を監視するには、［**Monitor All Application Versions**］オプションを選択します。 ◦ アプリケーションバージョンのサブセットのみを監視するには、［**個別のアプリケーションバージョンを選択(Select individual application versions)**］オプションを選択して、以下の操作を実行します。 1. ［**ADD**］をクリックします。 2. ［**アプリケーション(APPLICATION)**］リストから、監視するアプリケーションを選択します。 3. すべてのバージョンを選択するには、［**Select all**］チェックボックスをオンにします。それ以外の場合は、バージョンのチェックボックスをオンにします。 4. さらにアプリケーションバージョンを追加するには、手順ii~iiiを繰り返します。 5. ［**DONE**］をクリックします。

フィールド	説明(Description)
Active	Webhookをアクティブにする場合は、このチェックボックスをオンにします。Webhookを非アクティブのままにするには、チェックボックスをオフのままにします。

6. ［**保存(SAVE)**］をクリックします。

参照情報

Webhookペイロードの表示

Webhookの削除

1.12.3. Webhookを編集する

Webhookを編集するには:

1. Application Securityに管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。

   > **Note**
   >
   > セキュリティリードの方は、明示的な表示許可があるエンティティを監視するWebhookだけを編集できます。

3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**Webhook (Webhooks)**］を選択します。

   ［**Webhook (Webhooks)**］ページには、既存のすべてのWebhookが一覧表示されます。

4. 行を選択すると、編集するWebhookの詳細が表示されます。
5. ［**編集(EDIT)**］をクリックします。
6. 「Webhookの作成」で説明されている任意のフィールドの値を変更します。
7. (オプション)変更を行った後にペイロードの再配信を要求するには、［**Recent deliverie**］で、再配信するペイロードの行を選択して、［**REDELIVER**］をクリックします。
8. ［**保存(SAVE)**］をクリックします。

参照情報

Webhookペイロードの表示

Webhookの作成

1.12.4. Webhookペイロードの表示

管理者はすべてのWebhookペイロードを表示できます。セキュリティリードの場合は、表示する明示的な許可を持っているアプリケーションバージョンのWebhookペイロードのみを表示できます。

Webhookペイロードを表示するには、次の手順に従います。

1. Application Securityに管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**Webhook (Webhooks)**］を選択します。

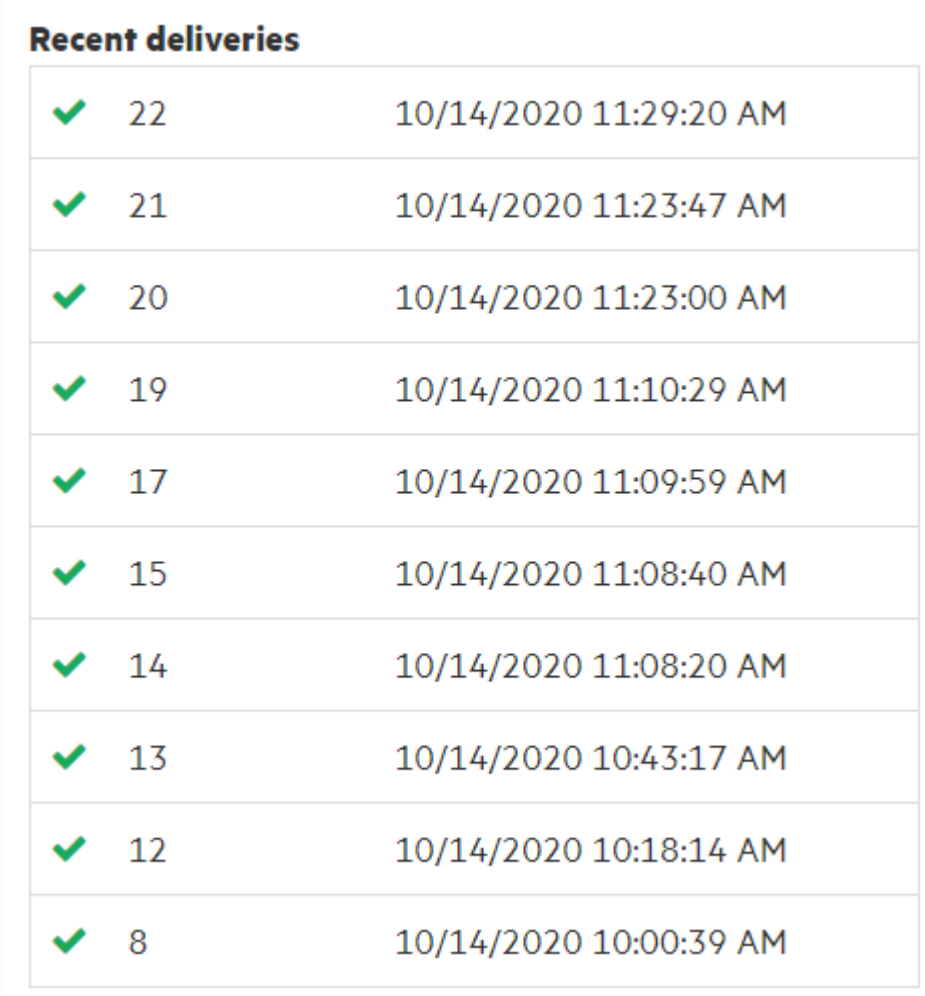
   ［**Webhook (Webhooks)**］ページに、既存のすべてのWebhookとその現在のステータスが一覧表示されます。

   ✔緑色のチェックマークは、最後のペイロード要求に成功したことを示します。

   ✘赤いxは、Webhookはアクティブであるが、要求された最後のペイロードを配信できなかったことを示します。

   > **Note**
   >
   > リストに表示されたWebhookの［**ステータス(Status)**］列にアイコンが表示されない場合は、Webhookテーブルでその行を展開し、［**アクティブ(Active)**］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。

4. Webhookテーブルで、Webhookを選択してその詳細を展開し、最近配信されたペイロード(最大10個)を調査します。



5. 調査するペイロードの行をクリックします。
6. 応答のヘッダまたは本文の詳細を表示するには、［**応答(RESPONSE)**］タブを選択します。

参照情報

Webhookのペイロード

Webhookの削除

Webhookの作成

Webhookを編集する

1.12.5. Webhookペイロードの再配信

WebhookのペイロードURLに配信されるペイロードに影響する変更が行われた場合、ペイロードの再配信を要求できます。

Webhookペイロードの再配達を要求するには、次の手順に従います。

1. 管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。

   > **Note**
   >
   > セキュリティリードの方は、明示的な表示許可があるエンティティを監視するWebhookだけを編集できます。

3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**Webhook (Webhooks)**］を選択します。
4. ペイロードを再配信するWebhookの行を選択します。
5. ［**Recent deliveries**］で、再配信するペイロードの行を選択し、［**REDELIVER**］をクリックします。

参照情報

Webhookの作成

Webhookを編集する

Webhookペイロードの表示

1.12.6. Webhookの削除

Webhookを削除するには、次の手順を実行します。

1. 管理者またはセキュリティリードとしてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで［**設定(Configuration)**］を展開し、［**Webhook (Webhooks)**］を選択します。
4. 削除するトークンのチェックボックスをオンにして、［**削除(DELETE)**］をクリックします。

参照情報

Webhookの作成

Webhookを編集する

1.13. 変数、パフォーマンスインジケータ、およびアラート

Application Securityでは、アプリケーションバージョンで測定された値とイベント条件を変数として保存できます。変数とは、アプリケーションバージョンごとに定期的に評価されるメトリックの定義を指します。変数では、数値データの問題、条件、その他のカテゴリがカウントされます。

パフォーマンスインジケータでは、アプリケーションバージョンの境界を越えて正規化され、貨幣原価などの複雑なより高レベルの抽象化を表すことができるメトリックに変数が組み合わされます。変数とパフォーマンスインジケータを、カスタマイズされたメトリックを作成するための構成ブロックとして使用して、カスタマイズされたアラート定義に組み込むことができます。

変数の値は、アラート定義で受信者として指定されたユーザのダッシュボードに表示するアラートをトリガするために使用できます。Application Securityでは、アプリケーションバージョンチームのメンバーにアラート通知を電子メールで送信することもできます。

このセクションでは、次のトピックについて説明します。

1.13.1. 変数の作成

管理者またはセキュリティリードは、アプリケーションで使用する変数を定義できます。

Application Security変数を作成するには、次の手順を実行します。

1. 管理者またはセキュリティリードとしてサインインし、［**管理**］をクリックします。

   Note

   開発者アカウントで変数を作成することはできません。

2. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**変数(Variables)**］を選択します。
3. ［**変数(Variables)**］ツールバーで［**新規(NEW)**］をクリックします。
4. ［**新しい変数の作成(CREATE NEW VARIABLE)**］ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明
名前(Name)	文字(a～z、A～Z)で始まり、文字、数字(0～9)、およびアンダースコア文字(_)のみを含む変数名を入力します。
説明(Description)	(オプション)他のユーザが変数の使い方を理解できるよう、説明を入力します。
Search String	有効なApplication Security変数検索文字列を入力します。検索文字列の作成方法については、［**構文ガイド(Syntax Guide)**］リンクを選択するか、「Variable syntax」を参照してください。
Folder	このリストから、変数に関連付けるデフォルトのフィルタセットのフォルダを選択します。 ［**フォルダ(Folder)**］リストには、使用可能なすべての問題テンプレートのそれぞれに関連付けられた固有のフォルダ名が表示されます。変数値は、フォルダ名がアプリケーションバージョンの問題テンプレートに関連付けられている場合に計算されます。

5. ［**保存(SAVE)**］をクリックします。

［**Variables**］テーブルに新しいプールが一覧表示されます。

1.13.1.1. 変数の構文

Application Security変数の形式は `<modifier>:<search_string>` です。例:

```
[Fortify Priority Order]:critical audited:false
```

文字列の完全一致を検索するには、文字列を引用符で囲みます。条件なしで文字列を検索するには、引用符を使用せずに文字列を入力します。

次の表に、関係演算子を記載します。

関係演算子	説明	例
number range	数値の範囲の開始と終了を指定するために使用されるカンマ区切りの番号のペアです。 範囲の開始値または終了値を含めた範囲を指定するには、角括弧を使用します。 範囲の開始値または終了値を除外した範囲(その数値より大きい、またはより小さい数値の範囲)を指定するには、丸括弧を使用します。	`(2,4]` 2より大きく、4以下の範囲を意味します。
`!` (等しくない)	感嘆符(`!`)が付いた検索文字列以外の文字列を検索します。	`file:!Main.java` `Main.java.` には含まれていないすべての問題を返します。

1.13.2. パフォーマンスインジケータの作成

Application Securityパフォーマンスインジケータでは、アプリケーションバージョンの境界を越えて正規化され、貨幣原価などの複雑、高レベルの抽象化を表すことができるメトリックに変数を組み合わせることができます。このトピックでは、パフォーマンスインジケータの構文とパフォーマンスインジケータの作成方法について説明します。

Application Securityパフォーマンスインジケータを作成するには、次の手順を実行します。

1. セキュリティリードまたは管理者としてApplication Securityにサインインし、［**管理**］タブをクリックします。

   > **Note**
   >
   > マネージャまたは開発者の役割が割り当てられているユーザは、Application Securityパフォーマンスインジケータを作成できません。

2. ナビゲーションペインで［**メトリックとトラッキング(Metrics & Tracking)**］を展開し、［**パフォーマンスインジケータ(Performance Indicators)**］を選択します。

   右側のテーブルには、既存のパフォーマンスインジケータが一覧表示されます。

3. ［**NEW**］をクリックします。

4. ［**新しいパフォーマンスインジケータの作成(CREATE NEW PERFORMANCE INDICATOR)**］ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明
名前(Name)	パフォーマンスインジケータの名前を入力します。
説明(Description)	(オプション)このパフォーマンスインジケータの説明を入力します。
Equation	有効なパフォーマンスインジケータ式を入力します。 パフォーマンスインジケータの形式は次のとおりです。 `<variable><operator><variable>` ここで、*<operator>*は標準的な数学演算子(`+` , `-` 、 `*` 、 `/`)、比較演算子(`==` , `>` , `<`)、または参考演算子(`?`)です。*<variable>*はApplication Securityの既存の変数です。
Return Type	戻り値の型を選択します。

5. 新しいパフォーマンスインジケータを設定して検証したら、［**SAVE(保存)**］をクリックします。

［**Performance Indicators**］テーブルに新しいインジケータが一覧表示されます。

1.13.3. アラートの作成

Null

アラート定義には、ダッシュボードの［**Todo List**］ウィンドウでApplication Securityによりアラート通知を生成するタイミングを決定するために、変数またはパフォーマンスインジケータを含めることができます。

> **Note**
>
> この機能は、Application Security管理者が電子メール通知を有効にしている場合にのみ使用できます。

特定のアプリケーションバージョンに割り当てられたユーザに1つ以上のアラート通知に関する電子メールメッセージを送信するアラート通知を設定できます。

アクセスが付与されているアプリケーションバージョンに関するアラートを定義できます。

Application Securityアラートを作成するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**アラート**］を選択します。

   ［**アラート**］ページには、定義されているすべてのアラートが表示されます。
4. ［**アラート**］ツールバーで［**新規(NEW)**］をクリックします。
5. ［**名前**］ボックスに、アラートの名前を入力します。
6. (オプション)［**説明**］ボックスに、アラートの説明を入力します。
7. アラートを有効にせずに作成するには、［**アラートを有効にする(Enable Alert)**］チェックボックスをオフにします。
8. ［**タイプ(Type)**］の横で、作成するアラートのタイプを選択します。

   > **Note**
   >
   > スケジュールされたアラートを作成できるのは管理者のみです。
9. ［**受信者(Recipients)**］の横で、次のいずれかを実行します。

- アラートを自分にのみ送信するには、［**自分のみ(Me only)**］オプションを選択したままにします。
- アプリケーションバージョンの割り当て先ユーザに割り当てられたユーザにアラートを送信するには、［**バージョンの割り当て先ユーザ(Version assignees)**］オプションを選択します。
- (スケジュールされたアラートの場合のみ)アラートをすべてのApplication Securityユーザに送信するには、［**すべてのシステムユーザ(All system users)**］を選択します。

選択したオプションに関係なく、通知を受信します。

10. 次の表に示すように、選択したアラートタイプの情報を入力します。

アラートタイプ	手順
パフォーマンスインジケータ	1. ［**いつアラートを送信するか(Alert when)**］リストから、パフォーマンスインジケータを選択します。 2. オペレータのリストからオペレータを選択します。 3. 数値を入力します。選択したパフォーマンスインジケータのタイプによって、値が整数かパーセンテージかが決まります。 デフォルトでは、パフォーマンスインジケータの値が［**いつアラートを送信するか(Alert when)**］に設定された条件を満たすと、パフォーマンスインジケータアラートが1回だけトリガされます。たとえば、トリガ条件が［Critical Exposure Issues < 50］に設定されたアラートは1回だけトリガされ、後続のスキャンで新しい重大な問題が発見されたとしても再度トリガされることはありません。 4. 新しいアーティファクトのアップロードごとにアラートをリセットするには、［**トリガの後にリセット(Reset after triggering)**］チェックボックスをオンにします。

アラートタイプ	手順
変数	1. ［**Alert when**］リストから、変数を選択します。 2. オペレータのリストからオペレータを選択します。 3. 数値を入力します。選択した変数のタイプによって、値が整数かパーセンテージかが決まります。 デフォルトでは、変数の値が［**Alert when**］に設定された条件を満たすと、変数アラートが1回だけトリガされます。たとえば、トリガ条件が［`NEWIssues = 0`］に設定されたアラートは1回だけトリガされ、後続のスキャンで新しい問題が発見されたとしても再度トリガされることはありません。 4. 新しいアーティファクトのアップロードごとにアラートをリセットするには、［**トリガの後にリセット(Reset after triggering)**］チェックボックスをオンにします。
システムイベント	◦ ［**いつアラートを送信するか(Alert when)**］リストから、アラートをトリガするシステムイベントを選択します。

アラートタイプ	手順
スケジュールされたアラート(管理者のみ)	1. ［**いつアラートを送信するか(Alert when)**］ダイアログボックスでカレンダをクリックして開き、Application Securityでアラートを送信する日付を指定します。 2. アラートを送信する時間と分(hh:mm)を入力します。 3. ［**AM**］と［**PM**］をクリックして切り替えて、アラートが午前に送信されるのか、午後に送信されるのかを決定します。 4. 国および地域のリストから、日時設定を適用する国または地域を選択します。 5. タイムゾーンのリストから、日時設定を適用するタイムゾーンを選択します。

11. パフォーマンスインジケータまたは変数アラートについては、次の手順に従って、アラートを使用する対象のアプリケーションバージョンを指定します。
    1. ［**ADD**］をクリックします。
    2. ［**アプリケーションバージョンの選択(SELECT APPLICATION VERSION)**］ダイアログボックスの［**アプリケーション(APPLICATION)**］リストから、アラートを使用する対象のアプリケーションバージョンを指定します。

       ［**バージョン(VERSIONS)**］ペインには、選択したアプリケーションのアクティブなバージョンが一覧表示されます。
    3. ［**VERSIONS**］リストにアプリケーションの非アクティブなバージョンを含めるには、［**Show inactive**］チェックボックスをオンにします。
    4. すべてのアプリケーションバージョンに対してアラートを使用するには、［**Select all**］チェックボックスをオンにします。そうでなければ、［**バージョン(VERSIONS)**］リストで、アラートを使用する対象バージョンのチェックボックスをオンにします。

5. 別のアプリケーションのバージョンを選択するには、ステップb～dを繰り返します。
6. ［**DONE**］をクリックします。

12. ［**Message(メッセージ)**］ボックスに、アラートを受信した理由を受信者に伝えるメッセージを入力します。

    スケジュールされたアラートを作成する場合は、メッセージテキストが必要です。

13. ［**保存(SAVE)**］をクリックします。

参照情報

アラートの削除

電子メールアラート通知設定の設定

電子メールアラートの受信を有効化および無効化する

1.13.3.1. アラートを編集する

Application Securityアラートを編集するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. 左側のペインで、［**テンプレート(Templates)**］をクリックしてから、［**アラート(Alerts)**］を選択します。

   ［**アラート**］ページには、定義したすべてのアラートが表示されます。
4. ［**アラート**］テーブルで、編集するアラートの行を見つけて選択します。

   行が展開されて、アラート設定が表示されます。
5. ［**編集(EDIT)**］をクリックします。
6. 必要な変更を行い、［**SAVE**］をクリックします。

1.13.3.2. アラートの削除

Application Securityアラートを削除するには:

1. 管理者としてApplication Securityにサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**アラート**］を選択します。

   ［**アラート**］ページには、定義したすべてのアラートが表示されます。
4. ［**アラート**］テーブルで、削除するアラートのチェックボックスをオンにします。
5. ［**Alerts**］ツールバーで［**DELETE**］をクリックします。
6. 削除を確認するには、［**OK**］をクリックします。

1.13.4. アラートの表示とマーク

Application Securityでは、ユーザまたは別のユーザが受信するように設定されたアラートが未読になっている場合、そのアラートにフラグが設定されます。これらのアラート通知は、［**ダッシュボード(Dashboard)**］ビューの［**Todoリスト(Todo List)**］と、すべてのビューのヘッダに表示されます。

未読アラートを表示するには、次のいずれかを実行します。

- ヘッダで、未読アラートの数を示す赤い円をクリックします。
- ［**ダッシュボード(Dashboard)**］ビューの［**Todoリスト(Todo List)**］エリアで、未読アラートの数を示す赤い円をクリックします。

［ALERTS］ウィンドウが開き、未読アラートのリストが表示されます。

アラートに既読マークを付けるには、次の手順に従います。

- ［アラート(ALERTS)］ウィンドウで、アラート名のチェックボックスをオンにしてから、［**既読としてマーク(MARK AS READ)**］をクリックします。

アラートに未読マークを付けるには、次の手順に従います。

- ［アラート(ALERTS)］ウィンドウで、アラート名のチェックボックスをオンにしてから、［**未読としてマーク(MARK AS UNREAD)**］をクリックします。

既読アラートを表示するには、次の手順に従います。

- ［**View**］リストから［**Read**］を選択します。

未読アラートを表示するには、次の手順に従います。

- ［**View**］リストから［**Unread**］を選択します。

すべてのアラート(既読と未読)を表示するには、次の手順に従います。

- ［**View**］リストから［**All**］を選択します。

すべてのアラートに既読マークを付けると、赤いアラート通知が表示されなくなります。非表示になっているアラートを表示するには、［**ダッシュボード(Dashboard)**］ビューに移動して、［**Todoリスト(Todo List)**］エリアで［**すべてのアラート通知を表示(Show all alert notifications)**］リンクをクリックします。

1.14. スキャンアーティファクトの操作

以下のセクションでは、スキャンアーティファクト操作のいくつかの側面について説明します。

1.14.1. スキャンアーティファクトのアップロード

次の手順では、スキャンアーティファクトをApplication Securityデータベースにアップロードする方法について説明します。トレーニングメタデータをFortify Audit Assistantに送信する方法については、「Audit Assistantへのトレーニングデータの送信」を参照してください。

Note

Application Securityがデータベースにデータを追加すると、100,000文字を超えるHTTP応答が切り捨てられます。このような応答は、最後が切れているか、応答の他の場所に `\n\n...\n\n` が含まれるかのいずれかです。これは、ダウンロードされたスキャンには影響を及ぼしません。これは、Application Securityの［**監査(AUDIT)**］ページに表示されるデータにのみ影響します。

Important

Application Securityにアップロードするファイルは2GBを超えないようにしてください。

Important

サードパーティのアーティファクトをアップロードするには、適切なパーサを設定する必要があります。詳細については、 パーサプラグインの追加と管理を参照してください。

スキャンアーティファクトをApplication Securityデータベースにアップロードするには、次の手順に従います。

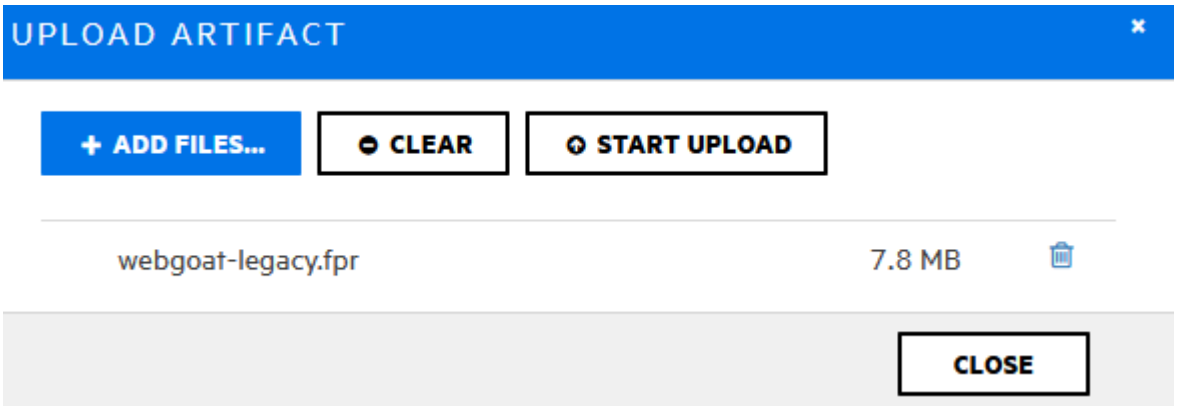
1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アーティファクトをアップロードする対象のアプリケーションバージョンを選択し、［**アーティファクト(Artifacts)**］ページを選択します。

   ［**アーティファクト履歴(ARTIFACT HISTORY)**］テーブルには、アプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧にされます。
3. ［**ARTIFACT**］をクリックします。

4. ［**アーティファクトのアップロード(UPLOAD ARTIFACT)**］ダイアログボックスで、［**+ファイルの追加(+ADD FILES)**］をクリックします。
5. アップロードする1つ以上(最大5つ)のアーティファクトファイルを選択します。

   OpenText Core SCAまたはSonatypeのサードパーティパーサが有効になっている場合は、リストからそのアーティファクトタイプを選択できます。

   ［**アーティファクトのアップロード(UPLOAD ARTIFACT)**］ダイアログボックスに、選択したファイルが一覧表示されます。



6. リストからファイルを削除するには、そのファイルの［**削除**］ボタンをクリックします。

   一覧表示されているファイルを削除するには、［**CLEAR**］をクリックします。
7. ［**START UPLOAD**］をクリックします。

   各ファイルがアップロードされると、ダイアログボックスに進行状況バーが表示されます。
8. ファイルが正常にアップロードされた後、［**CLOSE**］をクリックします。

> **Note**
>
> スキャンアーティファクトが分析結果処理ルールに基づく承認を必要とする場合は、アーティファクトを承認してから処理する必要があります。詳細については、アプリケーションバージョンの分析結果を承認するを参照してください。

ファイル処理エラーの表示

アップロードされたアーティファクトの処理でエラーが発生した場合、［**ARTIFACT HISTORY**］テーブルの［**Status**］列には［**Error Processing**］と表示され、違反した処理ルールの数を示す円で囲った数字が表示されます。

違反した処理ルールに関する情報を表示するには、次の手順に従います。

- 円で囲まれた数字をクリックします。

［**アーティファクトの処理に関するメッセージ(Artifact Processing Messages)**］ボックスが開き、アップロード中に発生した問題の詳細が表示されます。

参照情報

スキャンアーティファクトをダウンロードする

アプリケーションバージョンの分析結果処理ルールの設定

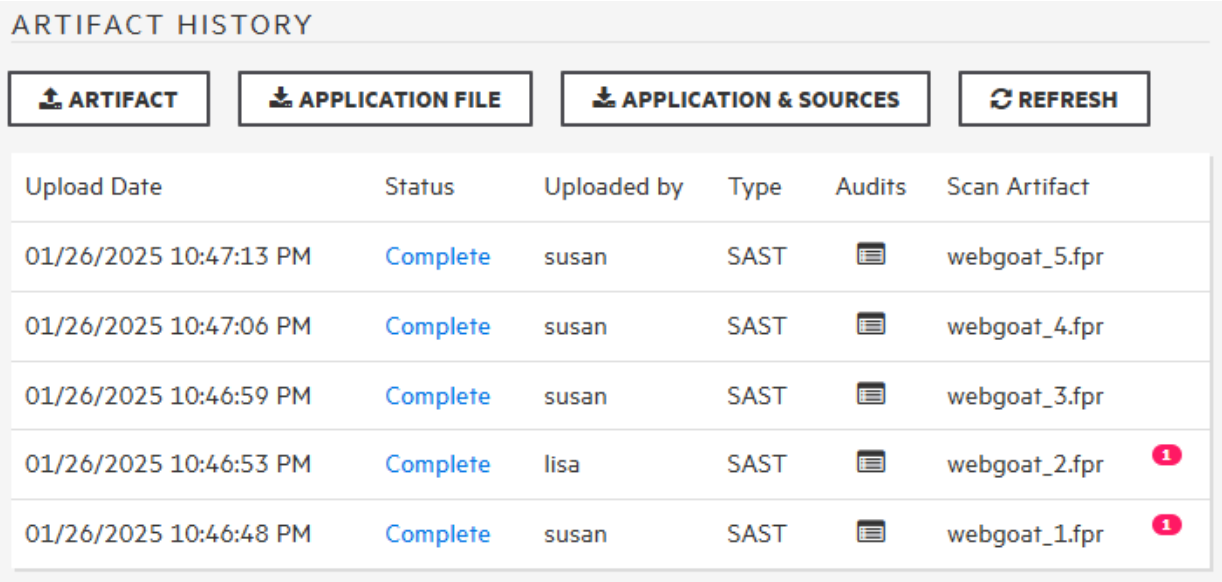
FPRファイルのアップロード

1.14.2. スキャンアーティファクトの詳細の表示

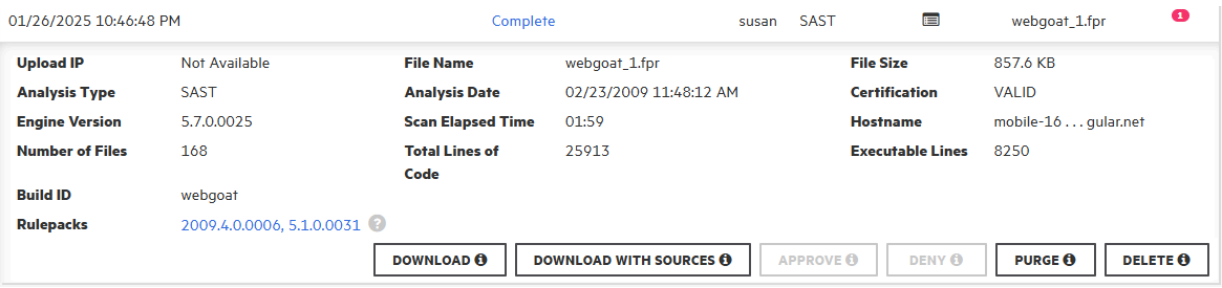
アップロードされたスキャンアーティファクトに関する詳細を表示するには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アーティファクトの詳細を表示する対象のアプリケーションバージョンを選択してから、［**アーティファクト(Artifacts)**］ページを選択します。

   [**ARTIFACT HISTORY**]テーブルには、アプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧表示されます。



3. アーティファクトに関する詳細を表示するには、そのアーティファクトに対応する行をクリックします。



   表示される詳細情報は、分析エンジンのバージョン、スキャンされたファイル数とコード行数、分析日などです。

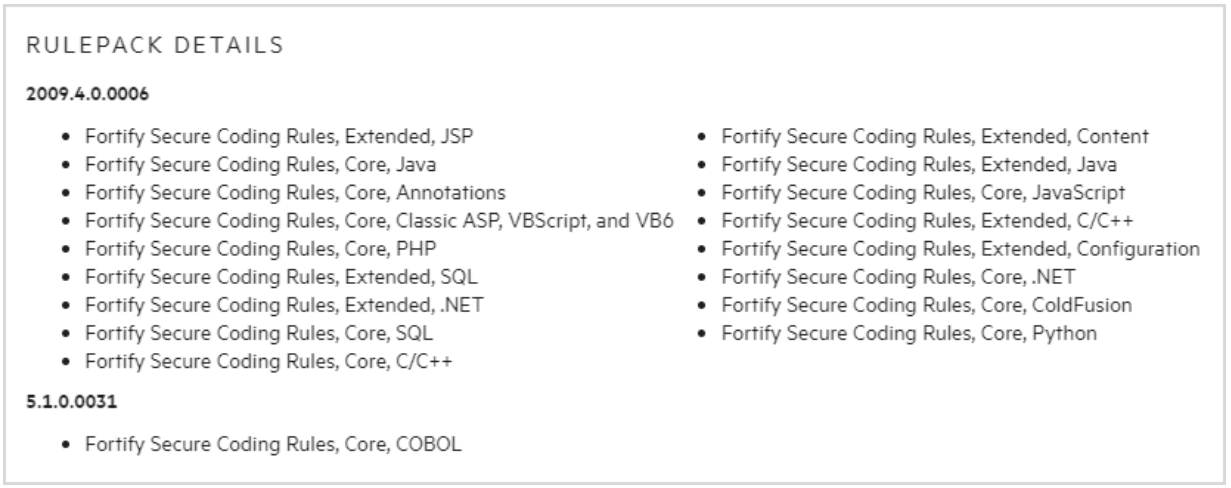
   アップロードされたアーティファクトの処理中にエラーが発生した場合は、［**ARTIFACT HISTORY**］テーブルの［**Status**］列に［**Error Processing**］と表示さ

れます。右側の数字は、違反した処理ルールの数を示します。

4. スキャンの処理エラーに関連するコードの行を表示するには、円で囲まれた数字(1)をクリックします。

   ［**スキャンに関する警告(SCAN WARNINGS)**］ボックスには、処理ルール違反が発生したコード行と違反の説明が表示されます。

5. Rulepackのバージョン別にグループ化された、スキャン中に適用されるコーディングルールのリストを表示するには、［**Rulepacks**］バージョンのリンクをクリックします。


RULEPACK DETAILS

2009.4.0.0006

- Fortify Secure Coding Rules, Extended, JSP
- Fortify Secure Coding Rules, Core, Java
- Fortify Secure Coding Rules, Core, Annotations
- Fortify Secure Coding Rules, Core, Classic ASP, VBScript, and VB6
- Fortify Secure Coding Rules, Core, PHP
- Fortify Secure Coding Rules, Extended, SQL
- Fortify Secure Coding Rules, Extended, .NET
- Fortify Secure Coding Rules, Core, SQL
- Fortify Secure Coding Rules, Core, C/C++
- Fortify Secure Coding Rules, Extended, Content
- Fortify Secure Coding Rules, Extended, Java
- Fortify Secure Coding Rules, Core, JavaScript
- Fortify Secure Coding Rules, Extended, C/C++
- Fortify Secure Coding Rules, Extended, Configuration
- Fortify Secure Coding Rules, Core, .NET
- Fortify Secure Coding Rules, Core, ColdFusion
- Fortify Secure Coding Rules, Core, Python

5.1.0.0031

- Fortify Secure Coding Rules, Core, COBOL

スキャンアーティファクトが分析結果処理ルールに基づく承認を必要とする場合は、アーティファクトを承認してから処理する必要があります。詳細については、アプリケーションバージョンの分析結果を承認するを参照してください。

参照情報

スキャンアーティファクトのアップロード

スキャンアーティファクトをダウンロードする

スキャンアーティファクトのパージ

アプリケーションバージョンの分析結果処理ルールの設定

FPRファイルのアップロード

1.14.3. 分析結果のダウンロード

アプリケーションバージョンの分析結果がマージされた最新のFPRファイルをダウンロードすることも、個々のスキャンの結果として得られたFPRファイルをダウンロードすることもできます。分析結果をFortify Audit Workbenchで開くには、ダウンロードされたFPRファイルをダブルクリックします。

アプリケーションバージョンのマージされたFPRファイルをダウンロードする

アプリケーションバージョンのマージされた最新の分析結果をFPR形式でダウンロードするには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アプリケーションバージョンを選択するか、アプリケーションの行をクリックして展開し、バージョンを選択します。
3. ［**アーティファクト(ARTIFACTS)**］を選択します。

   [**ARTIFACT HISTORY**]テーブルには、アプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧表示されます。
4. 次のいずれかを実行します。
   - マージされた最新のアプリケーションバージョン分析結果をダウンロードするには、［**アーティファクト履歴(ARTIFACT HISTORY)**］テーブルの上部にある［**アプリケーションファイル(APPLICATION FILE)**］をクリックします。
   - マージされた最新のアプリケーション分析結果をソースと併せてダウンロードするには、［**アーティファクト履歴(ARTIFACT HISTORY)**］テーブルの上部にある［**アプリケーションとソース(APPLICATION & SOURCES)**］をクリックします。

個々の分析結果をダウンロードする

特定の処理されたスキャンの結果をダウンロードするには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アプリケーションバージョンを選択するか、アプリケーションの行をクリックして展開し、バージョンを選択します。

3. ［**アーティファクト(ARTIFACTS)**］を選択します。

   [**ARTIFACT HISTORY**]テーブルには、アプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧表示されます。

4. ダウンロードするアーティファクトの行をクリックして展開し、アーティファクトの詳細を表示します。

5. アーティファクトをダウンロードするには、［**DOWNLOAD**］をクリックします。

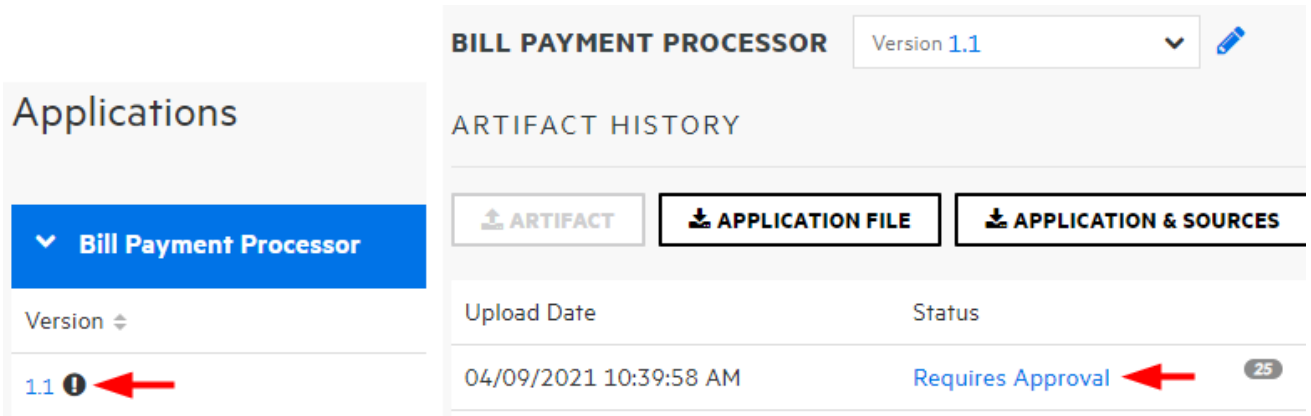
参照情報

スキャンアーティファクトのアップロード

アーティファクトの削除

1.14.4. アプリケーションバージョンの分析結果を承認する

アプリケーションバージョンに対して設定された処理ルールと、スキャンを処理するために使用したRulepackが期限切れ(サーバのRulepackより古い)かどうかによって、分析結果に承認が必要になる場合があります(「アプリケーションバージョンの分析結果処理ルールの設定」を参照)。分析結果に承認が必要な場合は、［**アプリケーション(Applications)**］ビューでバージョン名の横にアラートアイコン(❗)が表示され、［**アーティファクト履歴(ARTIFACT HISTORY)**］テーブルの［**ステータス**］列の値が［**承認が必要(Requires Approval)**］となります。



Note

アーティファクトが誤ってアップロードされた場合、またはApplication Securityがアーティファクトを処理しないようにする必要がある場合は、「承認処理を拒否する」で説明されている手順に従ってください。

アプリケーションバージョンの分析結果を承認して Application Security がアーティファクトを処理できるようにするには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アプリケーションバージョンを選択してから、［**アーティファクト(Artifacts)**］を選択します。

   ［**ARTIFACT HISTORY**］テーブルには、選択したアプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧表示されます。
3. ［**ステータス**］列の値が［**承認が必要(Requires Approval)**］となっている行を展開します。

4. ［**APPROVE**］をクリックします。

   ［**Processing Messages**］セクションには、承認要件をトリガした内容の説明が、具体的に表示されます。

5. ［**承認に関するコメント(Approval Comment)**］ボックスに、これらの分析結果を承認する理由を説明するコメントを入力します。

6. ［**APPROVE**］をクリックします。

Application Security でアーティファクトの処理が続行されます。

承認処理を拒否する

アーティファクトが誤ってアップロードされた場合、または何らかの理由でアーティファクトを Application Security で処理したくない場合は、そのアーティファクトを削除するか、あるいはアーティファクトアップロードの記録を保持したい場合は、承認を拒否できます。

アーティファクトの承認を拒否するには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。

2. アプリケーションバージョンを選択してから、［**アーティファクト(Artifacts)**］を選択します。

   ［**ARTIFACT HISTORY**］テーブルには、選択したアプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧表示されます。

3. 承認が必要で、Application Security で処理したくないアーティファクトの行を展開します。

4. ［**DENY**］をクリックします。

   ［**処理に関するメッセージ(Processing Messages)**］エリアに、具体的に何が原因で承認が必要になったのかに関する説明が一覧表示されます。

5. ［**Comment**］ボックスに、これらの結果を承認する理由を示すコメントを入力します。

6. ［**DENY**］をクリックします。

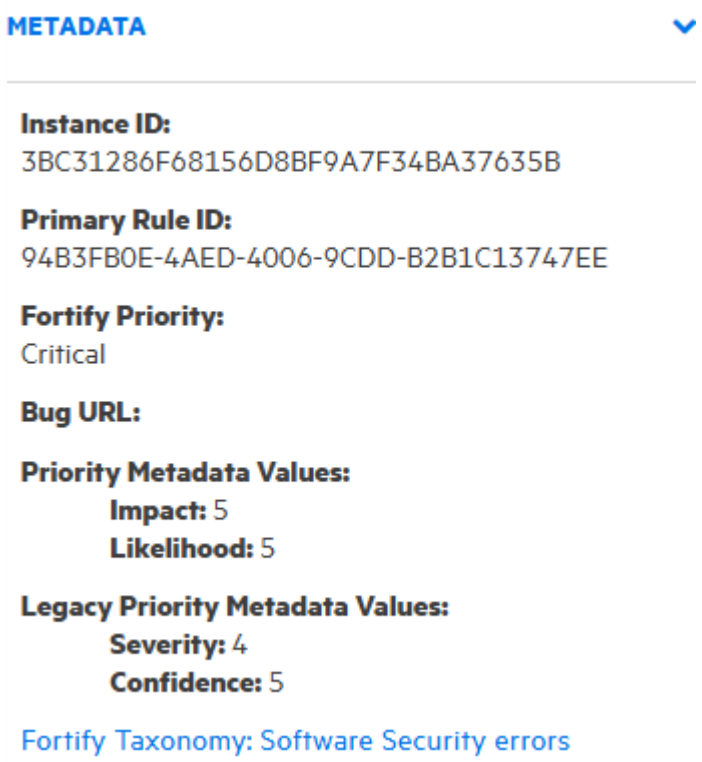
アーティファクトの［**ステータス**］値は［**Approval Denied**］に変わります。

1.14.5. 問題メタデータの表示

問題のメタデータを表示するには、次の手順に従います。

1. 目的のアプリケーションバージョンの［**監査(AUDIT)**］ページを開きます。
2. グループ化を選択した場合は、問題テーブルでグループを展開して、そのグループに含まれる問題を表示します。
3. 問題名が表示されている行をクリックします。

   ［**Code**］タブには、問題の概要、［**Analysis**］の値(設定されている場合)、スタックトレース、および問題が見つかったコードのセクションが表示されます。
4. ［**INFO**］タブをクリックし、クリックして［**メタデータ(METADATA)**］を展開します。



   メタデータ情報には、固有の問題識別子(インスタンスID)、問題が生成されたルールの固有の識別子(プライマリルールID)、バグURL (該当する場合)、優先度メタデータの値、および古い優先度メタデータの値が含まれます。

Note

表示されるインスタンスIDは、特定のアプリケーションバージョンに固有であり、その他のアプリケーションバージョンには関連付けられません。

5. ソフトウェアのセキュリティエラーに関する詳細情報を提供するWebサイトに移動するには、［**Fortify Taxonomy: Software Security errors**］リンクをクリックします。

1.14.6. 外部リストへの分析結果のマッピング

OpenTextは、Rulepackで外部メタデータドキュメントを配布します。このドキュメントには、Fortifyカテゴリから代替カテゴリ(OWASP Top Ten 2010、PCI、CWEなど)へのマッピングが含まれています。セキュリティリードは独自のファイルを作成して、さまざまな分類体系(内部アプリケーションのセキュリティ基準や追加のコンプライアンス義務など)に変更問題をマップすることもできます。カスタムマッピングの作成方法の詳細については、『OpenText™ Static Application Security Testingカスタムルールガイド』を参照してください。

変更された、または新しい外部メタデータドキュメントをすべてのアプリケーションに適用するには、最初にApplication Securityにインポートする必要があります。

新しいまたは変更された外部メタデータドキュメントをApplication Securityにインポートするには、次の手順に従います。

1. 管理者としてサインインします。
2. ヘッダで、［**管理(Administration)**］を選択します。
3. ナビゲーションペインの［**メトリックとトラッキング(Metrics & Tracking)**］で、［**Rulepacks**］を選択します。
4. ［**Rulepacks**］ページで、［**インポート(IMPORT)**］をクリックします。
5. ［**Rulepackのインポート(IMPORT RULEPACK)**］ダイアログボックスで、［**+ファイルを追加(+ADD FILES)**］をクリックします。
6. ドキュメントを見つけて選択し、［**アップロード開始(START UPLOAD)**］をクリックします。

Application SecurityとFortify Audit Workbenchとの間で共同監査する場合は、変更したマッピングドキュメントをApplication Securityにインポートし、Fortify Audit WorkbenchでFPRファイルを開いて、スキャン結果でのマッピングの動作を確認できます。

1.14.7. スキャンアーティファクトのパージ

アーティファクトをパージすると、アップロードされたアーティファクト、アーティファクト処理の一時的な結果、およびソースファイルの相互参照情報を削除することによって、Application Securityデータベースで領域が回復します。

アプリケーションバージョンのアーティファクトをパージする前に、次の点を考慮してください。

- パージ後は、パージされたアーティファクトを削除したり、パージされていない最も古いアーティファクトを削除したりすることはできません。
- パージは、システム内の問題ベースメトリクスには影響を与えません。
- カスタムレポートがある場合は、まずカスタマサポートに相談して、アーティファクトのパージがそれらに影響を及ぼすかどうかを確認してください。
- パージすると、分析日が同じか、それより前のアーティファクトがすべて削除されます。

次のすべての条件を満たすアーティファクトをパージできます。

- まだパージされていない。
- 特定の分析エンジンタイプから生成されたスキャンが1つだけ入っているのではない。たとえば、アプリケーションバージョンに対してOpenText SASTが生成したアーティファクトが1つしか存在しない場合、そのアーティファクトをパージすることはできません。同じ分析エンジンからの2つのアーティファクトがアプリケーションバージョン用にアップロードされた場合は、その2つのアーティファクトのうちの古い方だけをパージできます。
- ステータスが次のいずれかである。
  - PROCESS_COMPLETE
  - ERROR_PURGING
  - ERROR_DELETING

次の場合は、アーティファクトをパージできません。

- 処理中の場合
- 処理中にエラーが発生した場合
- 分析エンジンタイプの最新のスキャンが含まれている。

Application Securityデータベースからスキャンアーティファクトをパージするには、次の手順に従います。

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アーティファクトをパージする対象のアプリケーションバージョンを選択してから、［**アーティファクト(Artifacts)**］を選択します。

   [**ARTIFACT HISTORY**]テーブルには、アプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧表示されます。
3. データベースからパージするアーティファクトを表示する行をクリックします。

   テーブルが展開されて、選択したアーティファクトの詳細が表示されます。
4. ［**パージ(PURGE)**］をクリックします。
5. アーティファクトのパージを確認するには、［**OK**］をクリックします。

参照情報

アーティファクトの削除

1.14.8. アーティファクトの削除

アーティファクトを削除すると、アーティファクトのすべてのトレースが削除されます。

> **Note**
>
> 処理中のアーティファクトやパージ済みのアーティファクトは削除できません。

Application Securityデータベースからスキャンアーティファクトを削除するには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. アーティファクトを削除する対象のアプリケーションバージョンを選択してから、［**アーティファクト(Artifacts)**］を選択します。

   [**ARTIFACT HISTORY**]テーブルには、アプリケーションバージョン用にアップロードされたスキャンアーティファクトすべてが一覧表示されます。
3. 削除するスキャンアーティファクトを表示する行をクリックします。

   テーブルが展開されて、選択したアーティファクトの詳細が表示されます。
4. ［**DELETE**］をクリックします。
5. アーティファクトの削除を確認するには、［**OK**］をクリックします。

参照情報

スキャンアーティファクトのページ

1.15. Aviatorの自動修復結果の操作

OpenText™ Application Security Aviator for Vulnerability Remediationを使用することで、静的スキャン中に検出された脆弱性に対して、AIが支援したコード修正を用いてコードを自動的に修復できます。

OpenText™ Application Security Aviator for Vulnerability Remediationでは、大規模言語モデル(LLM)を活用することで、静的スキャン結果を監査して脆弱性を特定し、自動修復の提案を行います。OpenText™ Application Security Aviator for Vulnerability Remediationで得られた結果は、Application Security内に監査情報として保存されます。

このセクションでは、アップロードされたFPRファイルに含まれるOpenText™ Application Security Aviator for Vulnerability Remediationの自動修復結果をApplication Securityがどのように受信、保存、提供するかについて説明します。AIが支援した自動修復結果はApplication Security監査で確認でき、VS Code、Visual Studio、IntelliJ、EclipseなどのIDEプラグインで取得可能です。そのため、ユーザは自動修復結果を使用し、手動での作業を最小限に抑えながら、ソースコードを迅速かつ正確に修正できます。

Application Securityから直接リポジトリにコード修正を適用またはプッシュすることはできません。

自動修復データの受信

OpenText™ Application Security Aviator for Vulnerability Remediationがアップロードされたファイル内の脆弱性を分析した後、自動修復データが生成されます。自動修復 データ `remediations.xml` はFPRファイルに含まれています。

次の場合に `remediations.xml` ファイルが含まれます。

- Application Securityで既知のスキャンに対してOpenText™ Application Security Aviator for Vulnerability Remediationが実行された
- 自動修復結果を含むFPRが(FCLI、IDE、または手動アップロードを通じて)直接Application Securityにアップロードされた

このリリースバージョンでは、自動修復結果を含むFPRをApplication Securityにアップロードすることがサポートされています。FPRのアップロードについては、「スキャンアーティファクトのアップロード」を参照してください。

Application Securityでは、FPR利用時に `remediations.xml` を自動的に検出して処理を行います。

Application Securityにおける自動修復データの表示

Application Securityで問題を確認する際、自動修復データが表示されます。設定によってはデータが以下として表示されます。

- 専用の自動修復フィールド
- 問題の詳細内のコメントまたは推奨事項セクション

これにより、ユーザはApplication Securityを離れることなく、AIが支援した推奨事項を確認できます。

REST APIを使用した自動修復データの取得

IDEプラグインでは、以下のREST APIエンドポイントを使用して、特定の課題に関する自動修復データを取得できます。

- `/projectVersions/{parentId}/remediations`
- `/projectVersions/{parentId}/remediations/{id}`

このエンドポイントは、Application Securityによって保存された修復の詳細を返します。返されたデータは、Application SecurityがFPRファイルから受け取った修正情報と同じものです。

次も参照

Aviatorの設定

スキャンアーティファクトのアップロード

分析結果のダウンロード

1.16. 協同監査

分析エンジン(OpenText SASTなどのアナライザ)でソースコードをスキャンすると、そのすべての検出項目は実際の脆弱性ではなく「潜在的な」脆弱性として表示されます。それぞれのアプリケーションは固有のものであり、すべての機能は開発チームが最も理解している特定のコンテキスト内で実行されるため、開発者に直接確認することなく、疑わしい振る舞いを脆弱性とみなすかどうかを完全に判断できるテクノロジというものはありません。

Application Security内で実行するか、Fortify Audit Workbenc内で実行するか、Fortify Audit Assistantによって実行されるかに関係なく、問題の監査によって次の目的が達成されます。

- アプリケーション情報を集約および集中させる
- セキュリティチームが、実際の脆弱性を表す問題を協同で判断できる
- セキュリティチームが、脆弱性に基づいて問題の優先度を協同で決定できる

Application Securityでは、問題を分類および表示するために問題テンプレートを使用します。
このセクションでは、監査プロセスの概要と、監査インタフェースを表示および使用する方法について説明します。ここで記載する情報は、読者がアプリケーションバージョンを作成および設定する方法を把握していることを前提としています。アプリケーションとアプリケーションバージョンについては、「アプリケーションとアプリケーションバージョン」を参照してください。

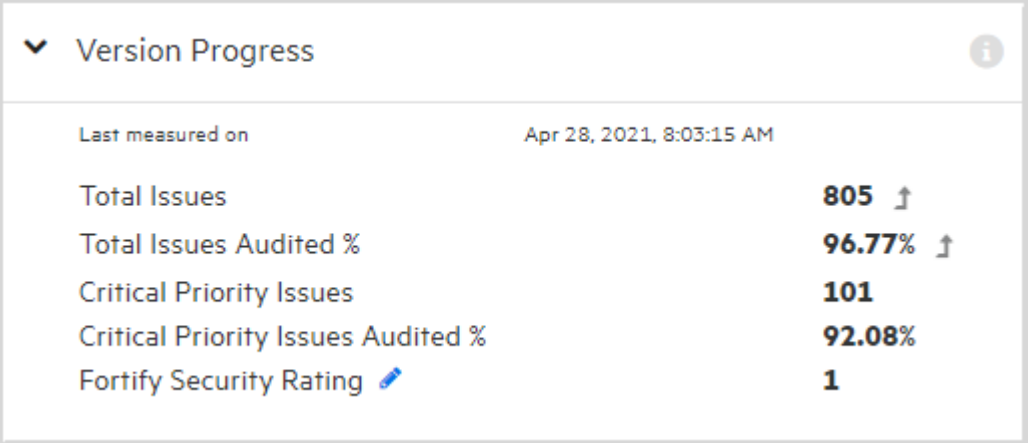
このセクションでは、次のトピックについて説明します。

1.16.1. 特定のアプリケーションバージョンの高レベルのサマリメトリックを表示する

アプリケーションバージョンの高レベルのサマリ結果を表示するには:

1. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
2. 対象のアプリケーションバージョンを選択してから、［**概要(Overview)**］を選択します。
3. ［**概要(OVERVIEW)**］ページで、右側のペインが折りたたまれている場合は展開します。

   ［**バージョン進捗状況(Version Progress)**］エリアに、傾向矢印を使用したサマリ情報が表示されます。



4. ［**Fortify Security Rating**］以外のメトリックを表示するには、［**編集(Edit)**］ボタン をクリックし、リストから、表示する別のメトリックを選択します。

参照情報

アプリケーションバージョンのサマリメトリックを表示する

1.16.2. 現在の問題の状態について

Application Securityでは、アプリケーションバージョンで各問題を明らかにした分析エンジンを追跡し、新しい情報をアプリケーションバージョンの既存の結果本体にマージします。新しい監査情報がサーバにアップロードされた後、または［**監査(AUDIT)**］ページに入力された後、Application Securityはその情報を特定の問題の既存の監査情報にマージします。また、Application Securityでは分析エンジンが問題を発見しなくなった後に「削除済み」として問題をマークします。

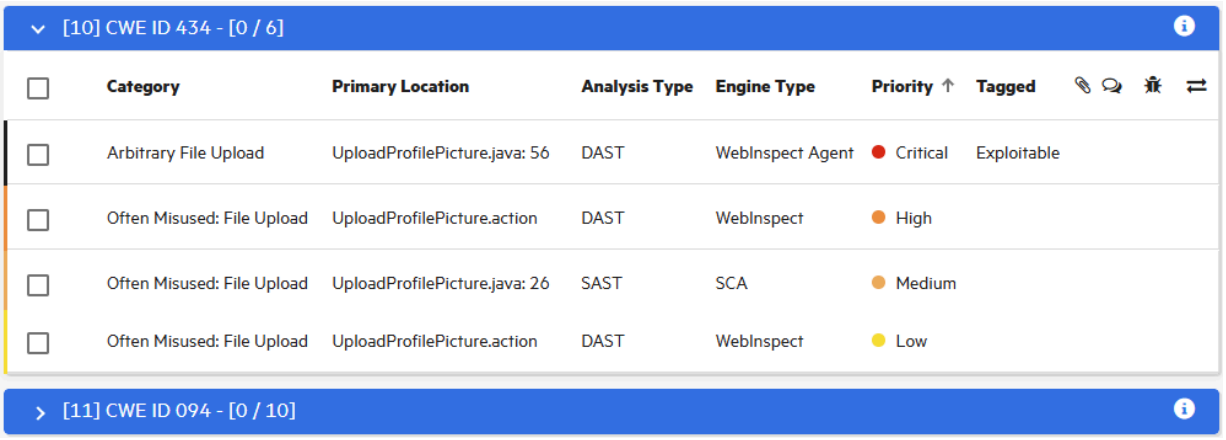
新しい分析結果がアップロードされるたびに、Application Securityはすべての問題をチェックして、それぞれの問題が以前のスキャンで明らかにされたものであるかどうかを判断します。

1.16.3. 監査する問題に関する情報の表示

監査する問題を表示するには:

1. 監査するアプリケーションバージョンの分析結果をアップロードします(「スキャンアーティファクトのアップロード」を参照)。
2. アプリケーションバージョンの［**監査(AUDIT)**］ページを開きます。
3. 監査する問題を選択的に表示するには、問題リストにフィルタを適用します。

   詳細については、「表示する問題をフィルタ処理する」および「フォルダに基づく問題の表示」を参照してください。
4. 問題テーブルで、グループを選択した場合は、グループを展開して、グループに含まれている問題を表示します。



次の表で、問題テーブルの列について説明します。一覧表示されている問題をソートするには、列ヘッダをクリックします(ただし、［**添付ファイルあり(Contains attachment)**］列(📎)、［**コメントあり(Contains comments)**］列(💬)、または［**バグ送信済み(Bug submitted)**］列(🐞)でソートすることはできません)。

列	説明(Description)
Category	明らかになった問題のカテゴリを表示します(ソートは英数字順です)。
主な場所(Primary Location)	スキャンされたファイルと、問題が検出されたコードの行を表示します(ソートは英数字順です)。
分析のタイプ(Analysis Type)	コードに対して実行された分析のタイプを表示します。
エンジンタイプ	スキャンを実行するために使用された分析エンジンを表示します。
Priority	問題が表す相対的脅威を示します(ソートは高優先度から低優先度の順または低優先度から高優先度の順です)。
タグ付き(Tagged)	問題に適用されたプライマリカスタムタグ値がある場合は、その値を表示します。
 添付ファイルあり(Contains attachment)	添付ファイルが問題に関連付けられているかどうかを示します
 コメントあり(Contains comments)	問題にコメントが追加されたかどうかを示します
 送信されたバグ(Bug submitted)	問題に対して不具合が送信されたかどうかを示します

列	説明(Description)
⇄ 相関する問題あり(Has correlated issues)	問題の静的および動的な結果が相関しているかどうかを示します。問題がある場合は、表に2回(分析タイプごとに1回)表示されます。 それ以降の静的スキャンまたは動的スキャンで問題が修正済みである場合は、相関アイコンが削除されます。 (ソートでは、相関する問題が最初または最後に表示されます。)

参照情報

分析結果の監査

1.16.3.1. フォルダに基づく問題の表示

［**概要(OVERVIEW)**］ページと［**監査(AUDIT)**］ページには、［**重大(Critical)**］リンク、［**高(High)**］リンク、［**中(Medium)**］リンク、［**低(Low)**］リンク、および［**すべて(All)**］リンクが含まれています。これらのリンクは、Fortifyフォルダへの割り当てに基づいて問題を表示するために使用できます。デフォルトで、フォルダはFortify優先度値(および企業にもたらす潜在的リスク)に対応していますが、表示されるフォルダには、Fortify Audit Workbenchで作成されてフィルタセット(および問題テンプレート)に追加されたカスタムフォルダを含めることができます(『OpenText™ Fortify Audit Workbenchユーザガイド』を参照してください)。

Note

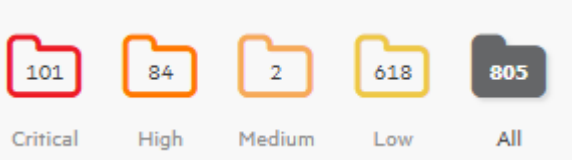
Fortify Audit Workbenchでフィルタセットやフォルダを編集または作成する際は、Fortify Audit WorkbenchとApplication Securityで使用される検索修飾子が一致しない場合があることにご注意ください。検索式に基づくすべての検索、フィルタ、またはフォルダが同じ結果を生成するとは限りません。また、OWASPやCWEなどの外部メタデータカテゴリを含む検索式は、Application SecurityとFortify Audit Workbenchでは異なる場合があるため、同じ結果にならない可能性があります。一致する外部カテゴリが複数ある場合、Application Securityではそれらのいずれかと一致しますが、Fortify Audit Workbenchではすべての外部カテゴリとの完全一致を期待します。Application Securityで使用する問題テンプレートを編集または作成する際にこの問題が発生した場合は、カスタマサポートにお問い合わせください。

Fortifyフォルダ割り当てに基づいて［**概要(OVERVIEW)**］ページから問題を表示するには:

1. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューで、対象のアプリケーションバージョンを選択してから、［**概要(Overview)**］を選択します。

   アプリケーションバージョンの［**概要(OVERVIEW)**］ページが開きます。［**グループ化条件(Group by)**］リストと［**フィルタ条件(Filter by)**］リストの左側に、それぞれのフォルダに含まれる問題の合計数が表示されます。デフォルトでは、すべての問題が表示されます。フィルタ条件として使用する属性を選択すると、それに応じてフォルダに表示される数字も変わります。

2. フォルダに含まれる確認済みの問題の数を表示するには、フォルダをポイントします。



確認済みの問題の数の後に続いて、問題の合計数が表示されます。たとえば、「**High - [79 / 84]**」は、優先度の高い合計84件の問題のうち、79件が確認済みであることを意味します。

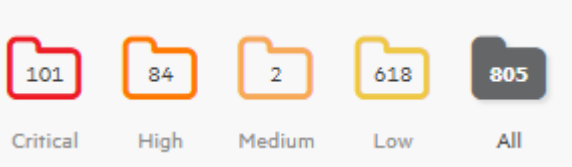
3. 割り当てられたフォルダに基づいて［**概要(OVERVIEW)**］ページに問題チャートを表示するには、フォルダを選択します。

Fortifyフォルダ割り当てに基づいて［**監査(AUDIT)**］ページから問題を表示するには:

1. ［**ダッシュボード(Dashboard)**］で、対象のアプリケーションバージョンをポイントして［**監査(Audit)**］を選択します。

   アプリケーションバージョンの［**監査(Audit)**］ページが開きます。検索ボックスの下に、それぞれのフォルダに含まれる問題の合計数が表示されます。デフォルトでは、すべての問題が表示されます。フィルタ条件として使用する属性を選択すると、それに応じてフォルダに表示される数字も変わります。

2. 特定のフォルダに割り当てられている確認済みの問題の数を表示するには、フォルダをポイントします。



   確認された問題の数が左側に表示され、問題の合計数が右側に表示されます。たとえば、「**High - [79 / 84]**」は、優先度の高い合計84件の問題のうち、79件が確認済みであることを意味します。

3. フォルダ割り当てに基づいて［**監査(AUDIT)**］ページに問題のリストを表示するには、フォルダを選択します。

参照情報

［OVERVIEW］および［AUDIT］ページに表示する問題をフィルタ処理する

1.16.3.2. ユーザに割り当てられた問題の表示

ユーザに割り当てられている問題をすべて表示するには、次の手順に従います。

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. ［**フィルタ(Filters)**］で、［**自分に割り当てられている問題(My assigned issues)**］スイッチをオンにします(または、［**レガシービュー(Legacy View)**］で［**自分に割り当てられている問題(My assigned issues)**］チェックボックスをオンにします)。

   ［**アプリケーション(Applications)**］ビューに、自分に割り当てられている問題を伴うアプリケーションバージョンが一覧表示されます。

参照情報

問題の表示設定の設定

1.16.4. 表示する問題をフィルタ処理する

以下の手順では、［**概要(OVERVIEW)**］ページまたは［**監査(AUDIT)**］ページに表示する、アプリケーションバージョンの問題をフィルタ処理する方法を説明しています。

> **Note**
>
> また、フィルタセットを選択して、［**概要(OVERVIEW)**］ページおよび［**監査(AUDIT)**］ページに表示する問題を変更することもできます。詳細と手順については、「フィルタセットを使用して表示問題を変更する」を参照してください。

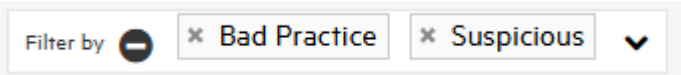
［**概要(OVERVIEW)**］ページまたは［**監査(AUDIT)**］ページに表示される問題をフィルタ処理するには:

1. ［**グループ化条件(Group By)**］リストから、問題テーブルの問題をグループ化するために使用する属性を選択します。

   選択した属性を削除するには、［**すべてクリア(Clear all)**］ボタンをクリックします。

2. ［**Filter by**］リストから、問題テーブルに表示する問題をフィルタするために使用する属性を選択します。

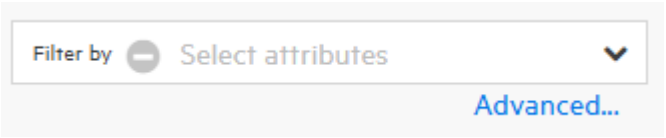
   このリストから複数の属性を選択できます。属性は一度に1つずつ選択する必要があります。

   選択した属性を削除するには、その名前の横にある［**x**］をクリックします。選択したすべての属性を削除するには、［**すべてクリア(Clear all)**］ボタンをクリックします。

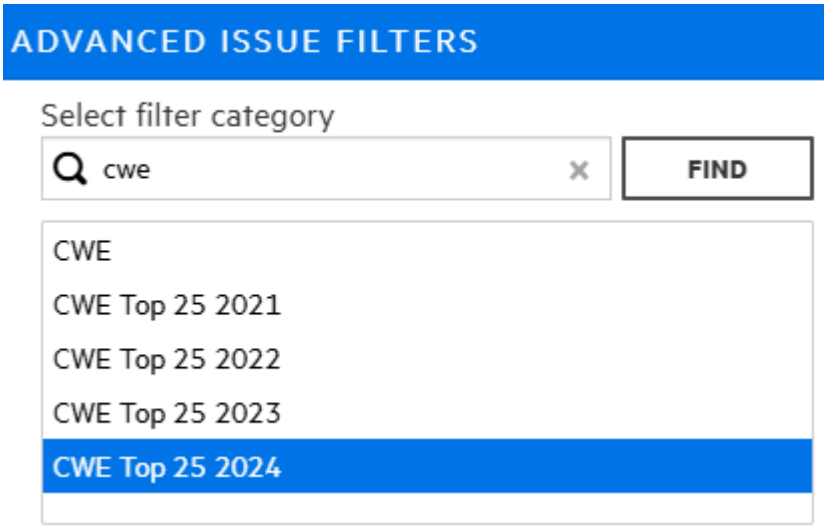
3. ［**分析(Analysis)**］以外のカスタムタグの値に基づいて、またはOWASP、CWE、あるいは他のセキュリティ脅威分類に関連するリスクに基づいて問題をフィルタ処理するには:

   1. ［**詳細(Advanced)**］リンクをクリックします。

2. ［**高度な問題フィルタ(ADVANCED ISSUE FILTERS)**］ダイアログボックスの［**フィルタカテゴリの選択(Select filter category)**］リストから、カテゴリを選択します。

   一覧にされるカテゴリを絞り込むには、［**カテゴリのフィルタ処理(Filter categories)**］ボックスにテキスト文字列を入力して、［**検索(FIND)**］をクリックします。



   ［**フィルタの選択(Select filters)**］リストには、選択したカテゴリで使用可能なフィルタが入っています。

3. ［**フィルタの選択(Select filters)**］リストをさらに絞り込むには、［**フィルタオプション(Filter options)**］ボックスにテキスト文字列を入力して、［**検索(FIND)**］をクリックします。

   ［**フィルタの選択(Select filters)**］リストには、一致するテキストを含むフィルタが表示されます。

   フィルタの完全なリストを再び表示するには、［**カテゴリのフィルタ処理(Filter categories)**］ボックスの［**x**］をクリックします。

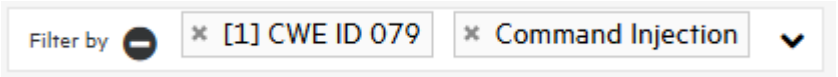
4. ［**フィルタの選択(Select filters)**］リストで、フィルタ条件とする各フィルタをクリックします。

   選択した各フィルタが［**選択済みのフィルタ(Selected filters)**］リストに追加されます。

5. 別のフィルタカテゴリのフィルタを追加するには、これらのステップbからdを繰り返します。

6. ［**適用(APPLY)**］をクリックします。

   ［**Filter by**］ボックスには、選択したフィルタがすべて表示されています。



4. フィルタを削除するには、フィルタの［**x**］をクリックします。
5. ［**グループ化条件(Group by)**］と［**フィルタ条件(Filter by)**］と高度なフィルタの選択をすべてクリアするには、［**すべてクリア(Clear all)**］ボタンをクリックします。

参照情報

相関する問題の監査

問題の検索

フォルダに基づく問題の表示

グローバル検索

1.16.5. 問題の検索

検索クエリを作成して、アプリケーションバージョンに関して表示された問題のリストを絞り込むことができます。

問題を検索するクエリを作成するには、次の手順に従います。

1. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューで、対象のアプリケーションバージョンを選択します。

   選択したアプリケーションバージョンの［**監査(Audit)**］ページが表示されます。

2. ［**問題の検索(Search Issues)**］ボックスに、次の構文を使用して検索クエリを入力します。実行する比較の種類を指定するには、検索用語を区切り記号で囲みます。

比較	説明(Description)
contains	特別な修飾区切り記号を使用せずに用語を検索します
equals	用語が引用符(`""`)で囲まれている場合は完全一致を検索します
number range	丸括弧または角括弧で範囲の開始値あるいは終了値を範囲から除外するか範囲に含めるかを示す、標準的な数学表記を使用して、数値範囲を検索します。 例: `(2,4]` は、2より大きく、4以下の範囲を示します。
not equal	文字列の先頭に感嘆符(`!`)を付加すると、その文字列で指定された問題が除外されます。 例: `file:!Main.java` は、 `Main.java` に含まれていないすべての問題を返します。

> **Note**
>
> 検索文字列の例を表示するには、［**Syntax Guide**］リンクをクリックします。

修飾子を使用して、検索用語にさらに条件を付けることができます。修飾子を使用する場合の構文は、 *<modifier>:<search_term>* です。

検索文字列には、複数の修飾子と検索用語を含められます。複数の修飾子を指定した場合は、Application Securityは変更された検索用語のすべてと一致する問題だけを返します。たとえば、 file:ApplicationContext.java category:SQL Injection は ApplicationContext.java で見つかったSQLインジェクションに関する問題のみを返します。

検索文字列で同じ修飾子を2回以上使用する場合、それらの修飾子で修飾された検索用語は、OR比較として扱います。たとえば、 file:ApplicationContext.java category:SQL Injection category:Cross-Site Scripting は ApplicationContext.java で見つかったSQLインジェクションの問題とサイト間スクリプティングに関する問題を返します。

複雑な検索の場合は、検索クエリ間に AND または OR キーワードを挿入できます。検索では、 AND と OR 操作の優先度が同じであることに注意してください。

3. ［**Find**］をクリックします。
4. 問題リストに戻る場合は、検索ボックスのテキストをクリアします。

参照情報

検索修飾子

［OVERVIEW］および［AUDIT］ページに表示する問題をフィルタ処理する

検索クエリの例

グローバル検索

1.16.5.1. 検索修飾子

検索修飾子を使用して、検索用語の適用対象とする、問題の属性を指定できます。カスタムタグの名前など、名前にスペースが含まれる修飾子を使用するには、修飾子を角括弧で囲む必要があります。たとえば、新しい問題を検索するには、「`[issue age]:new`」と入力します。

修飾子で条件が付けられていない検索は、属性kingdom、primary rule id、analyzer、filename、severity、class name、function name、instance id、package、confidence、type、subtype、taint flags、category、sink、およびsourceに基づく検索クエリに一致します。

次の例で、検索修飾子を適用する検索と、適用しない検索を使用する方法について説明します。

- すべての修飾子に検索を適用するには、「`control flow`」のような文字列を入力します。これにより、すべての修飾子が検索され、「control flow」文字列を含むすべての結果が返されます。
- 特定の修飾子に検索を適用するには、修飾子名と文字列を「`analyzer:control flow`」のように入力します。これにより、Control Flow Analyzerによって検出されたすべての結果が返されます。

次の表に、検索修飾子の説明を記載します。いくつかの検索修飾子には、括弧で囲まれた短縮名があります。どちらかの修飾子文字列を使用できます。

修飾子	説明
analysis	指定した監査分析値(exploitable 、 not an issue など)が設定された問題を検索します。
[analysis type]	アナライザ製品に基づいて問題を検索します。
analyzer	指定したアナライザ(control flow 、 data flow 、 structural など)で検出された問題を検索します。
audience	対象のオーディエンス別に問題を検索します。有効な値は、 targeted 、 medium および broad です。 **Note** このメタデータは、使用されなくなったレガシ情報であり、今後のリリースで削除される予定です。OpenTextでは、この検索修飾子を使用しないことを推奨しています。
audited	問題を検索して、プライマリカスタムタグが設定されている true か、プライマリカスタムタグが設定されていない false かを確認します。デフォルトのプライマリタグはAnalysisタグです。
category (cat)	指定したカテゴリまたはカテゴリの部分文字列を検索します。

修飾子	説明
`comments` (`comment`, `com`)	追加されたコメントに検索用語が含まれている問題を検索します。
`commentuser`	指定したユーザからのコメントを持つ問題を検索します。
`confidence` (`con`)	指定した信頼値を持つ問題を検索します。OpenText SASTでは、コード分析で使用される想定の数に基づいて信頼性の値を計算します。想定が多い場合は、信頼性の値が低くなります。
`<custom_tagname>`	指定したカスタムタグ値に基づいて問題を検索します。 日付タイプのカスタムタグで特定の日付を検索するには、yyyy-mm-dd形式で日付を指定します。 カスタムタグに値が設定されていない問題を検索するには、検索用語として `<none>` を使用します。たとえば、「Target Date」というラベルが付いた日付タイプのカスタムタグに値が設定されていないすべての問題を検索するには、次のように入力します。 `[Target Date]:<none>`
`[engine priority]`	問題を特定したエンジンによって決定された元の優先度値に基づいて問題を検索します。

修飾子	説明
`file`	指定したファイルで、プライマリロケーションまたはシンクノード機能呼び出しが発生する問題を検索します。
`[fortify priority order]`	指定された優先度に一致する優先度レベルの問題を検索します。有効な値は、`critical`、`high`、`medium`、および`low`です。
`historyuser`	指定したユーザによって監査データが変更された問題を検索します。
`[issue age]`	`new`、`updated`、`reintroduced`、または`removed`という問題の新しさを検索します。
`kingdom`	指定した分野のすべての問題を検索します。
`maxconf`	検索用語として指定した数以下の信頼値を持つすべての問題を検索します。
<metadata_listname>	指定したメタデータ外部リストを検索します。メタデータ外部リストには、`[OWASP top ten <year>]`、`[CWE top 25 <version>]`、`[stig <version>]`、`[pci ssf <version>]`などがあります。

修飾子	説明
`minconf`	検索用語として指定した数以上の信頼値を持つすべての問題を検索します。
`package`	指定したパッケージまたは名前空間でプライマリロケーションが発生する問題を検索します。データフローの問題では、主なロケーションはシンク機能です。
`[primary context]`	指定したコードコンテキストで、プライマリロケーションまたはシンクノード関数呼び出しが発生する問題を検索します。また、sinkと[source context]も参照してください。
`primaryrule` (`rule`)	指定したシンクルールに関連する問題を検索します。
`sink`	指定したシンク機能名を持つ問題を検索します。[primary context]も参照してください。
`source`	指定したソース関数名を持つデータフローの問題を検索します。[source context]も参照してください。

修飾子	説明
[source context]	指定したコードコンテキストにソース関数呼び出しが含まれるデータフローの問題を検索します。 sourceと[primary context]も参照してください。
sourcefile	指定したファイルに含まれるソース関数呼び出しに関するデータフローの問題を検索します。 fileも参照してください。
status	ステータスがレビューされた、レビューされていない、またはレビュー中の問題を検索します。
suppressed	抑止されている問題を検索します。
taint	指定したtaintフラグを持つ問題を検索します。

修飾子を使用する検索クエリの例については、検索クエリの例を参照してください。

参照情報

問題の検索

1.16.5.2. 検索クエリの例

次の表に、検索クエリの例を記載します。

検索ターゲット	クエリ(Query)
名前に `jsp` が含まれ、 `getSSN()` をソースとするファイル内のすべてのプライバシー侵害	`category:"privacy violation" source:getssn file:jsp`
`com/test/123` が含まれるすべてのファイル名	`file:com/test/123`
修飾子の一部として `cleanse` が含まれるすべての問題	`cleanse`
`[my tag]` が割り当てられて、 `P1` に設定された、監査済みのすべての問題	`[my tag]:P1`
コメントに `asdf` が含まれる、抑制されたすべての脆弱性	`suppressed:true comments:asdf`
SQLインジェクションを除くすべてのカテゴリ	`category:!SQL Injection`
名前に `java` または `jsp` が含まれるファイル内のすべての問題	`file:java OR file:jsp`
名前に `java` が含まれるファイルで、12行目で発生したすべての問題	`file:java AND line:12`
`version` ラベル付きのカスタムタグに値が指定されているすべての問題	`version:!<none>`

参照情報

1.16.6. グローバル検索

どのビューを開いているかに関係なく、ヘッダでグローバル［**検索(Search)**］ボックスにアクセスできます。ここで入力する検索文字列は、すべてのアプリケーションバージョン、問題、レポート、コメント、およびユーザに適用されます。

Note

検索ボックスは、Application Securityのセットアップ時に［**Enable global search**］が選択されている場合にのみ表示されます。詳細情報については、Application Securityの初回設定を参照してください。

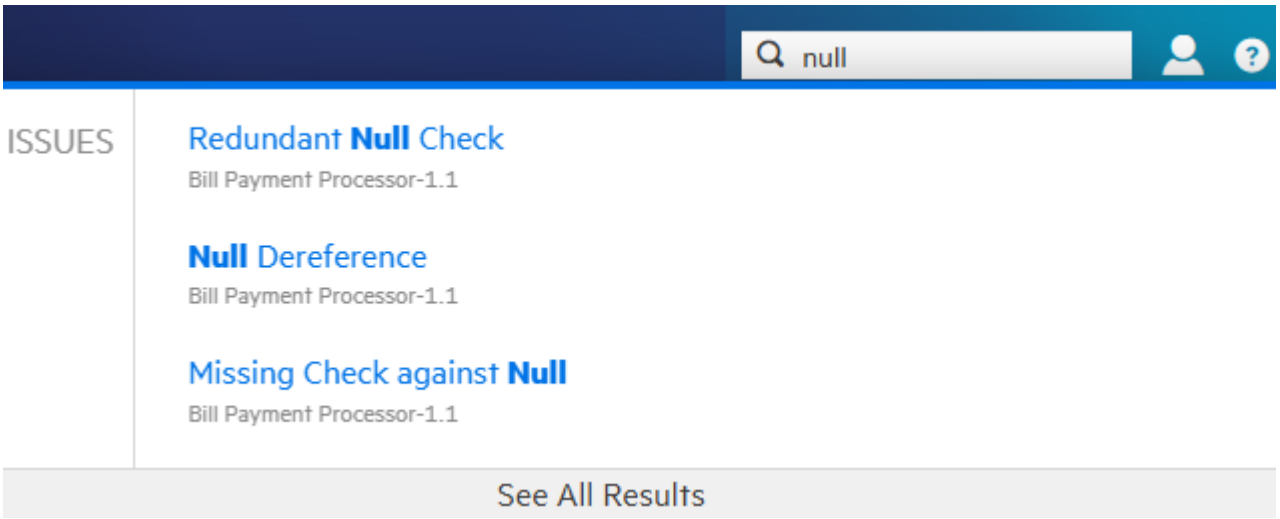
グローバル［**検索(Search)**］フィールドを使用するには:

1. どのビューからでもよいので、［**Search**］ボックスに検索文字列を入力します。

   Application Securityは、検索文字列に一致する最初のいくつかの項目をカテゴリ別に表示します。アプリケーションのバージョンも表示されます。

2. リストされている特定の項目に移動するには、項目をクリックします。
3. すべての検索結果のリストを表示するには、一覧表示されている項目の下にある［**See All Results**］をクリックします。

例: 問題の検索



検索結果のリストから問題を選択すると、Application Securityで対応するバージョンページが表示され、問題のフルビューが展開されます。

［**すべての結果を表示(See All Results)**］を選択すると、Application Securityに［**検索結果(Search Results)**］ページが表示されます。ここから、問題の最初の一致結果をフルビ

ューに展開して開くことができます。そこから、次へボタンと前へボタンを使用して、すべての結果に移動できます。

Note

問題の検索結果には、削除された問題、非表示にされた問題、または抑止された問題が含まれる場合があります。選択した項目が［**監査(AUDIT)**］ページに表示されない場合は、アプリケーションバージョンに設定されている表示初期設定をチェックして、削除された問題、非表示にされた問題、および抑止された問題が表示されるように適切に設定されていることを確認します。手順については、問題の表示設定の設定を参照してください。

参照情報

アプリケーションビューからアプリケーションとアプリケーションバージョンを検索する

1.16.7. 分析結果の監査

次の手順は、［**監査(AUDIT)**］タブでスキャン結果を監査する方法について説明しています。オープンソースの結果を処理する場合は、［**監査(AUDIT)**］ページまたは［**オープンソース(OPEN SOURCE)**］ページで分析結果を監査できます。

監査する問題を表示するには:

1. 監査するアプリケーションバージョンの分析結果をアップロードします。

   手順については、「スキャンアーティファクトのアップロード」を参照してください。

2. アプリケーションバージョンの［**監査(AUDIT)**］ページを開きます。

   ［**監査(AUDIT)**］ページのテーブルに、割り当てられたフォルダに基づいて問題が一覧表示されます(デフォルトでは重大から低の順)。

3. 監査する問題を選択的に表示するには、問題リストにフィルタを適用します。

   詳細については、「表示する問題をフィルタ処理する」および「フォルダに基づく問題の表示」を参照してください。

4. 問題テーブルでグループ化の条件となる属性を選択した場合は、グループを展開して、そこに含まれている問題を表示します。

問題を監査するには:

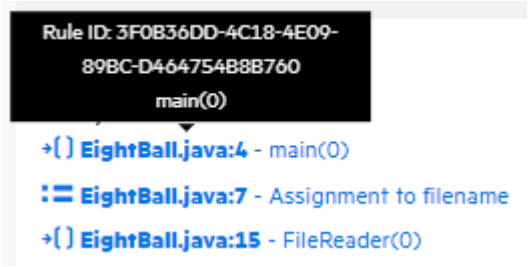
1. 問題を展開して詳細を表示するには、テーブル内の該当する行をクリックします。

   OpenText DASTの結果を表示する方法については、「Application SecurityでのOpenText DASTスキャン結果の表示」を参照してください。

   > **Tip**
   >
   > 問題の詳細を新しいブラウザウィンドウで表示するには、［**新しいタブで開く(Open in a new tab)**］ボタンをクリックします。問題のリンクをコピーして後で簡単にアクセスするには、［**問題のリンクをクリップボードにコピーする(Copy issue link to clipboard)**］ボタンをクリックします。

   ［**コード(CODE)**］タブには、問題に関連するソースコードの中で、汚染されたデータがたどってきた経路が表示されます。

2. 汚染されたデータがたどってきた経路に沿ったステップに関するサマリの詳細を表示するには、［**分析トレース(Analysis Trace)**］で、そのステップをポイントします。

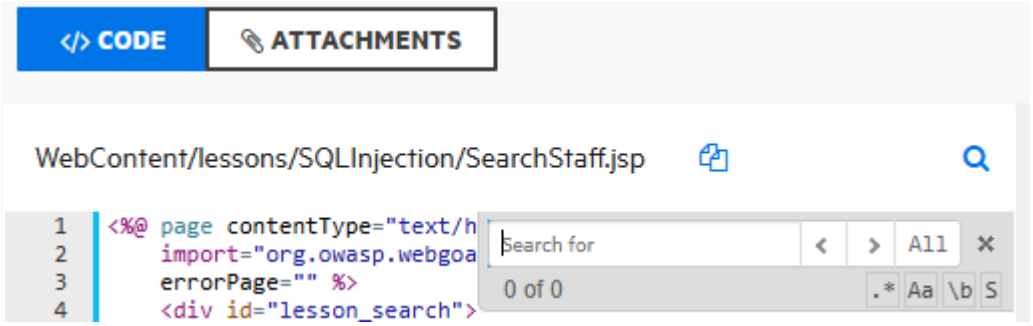


3. ステップに関連付けられているコードを表示するには、［**Analysis Trace**］の下のステップをクリックします。

   対応するコード行が［**CODE**］タブで強調表示されます。

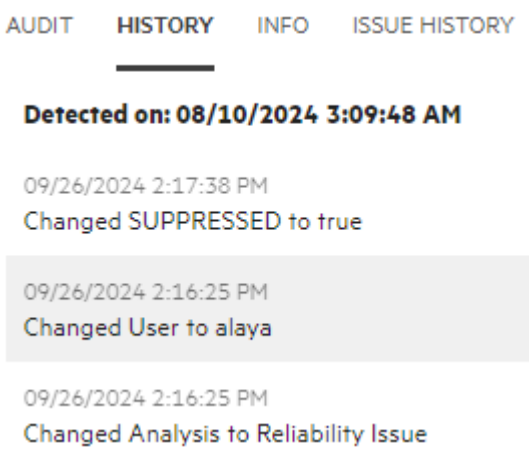
4. 問題に関連するコード内の特定の文字列を検索するには、次の手順に従います。

   1. ［**コード(CODE)**］タブで、検索ボタンをクリックします。
   2. ［**検索対象(Search for)**］ボックスに、検索文字列を入力します。

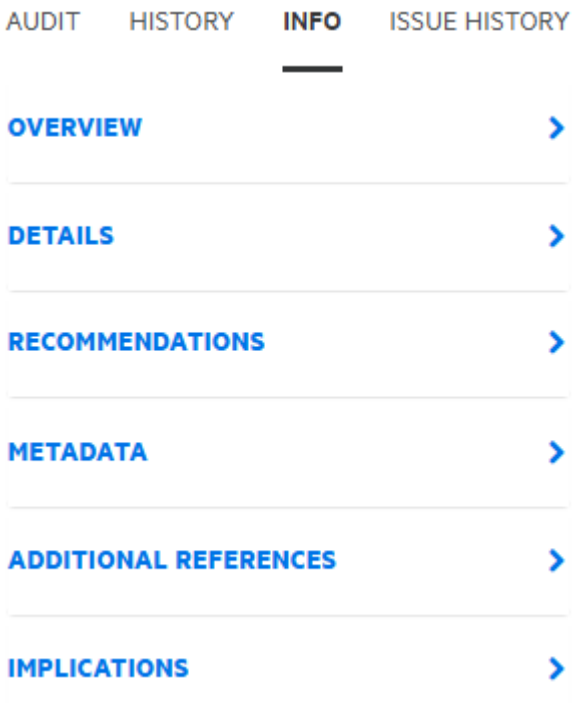


   ［**次へ(Next)**］ボタン `›` と［**前へ(Previous)**］ボタン `‹` を使用して、検索結果を移動します。

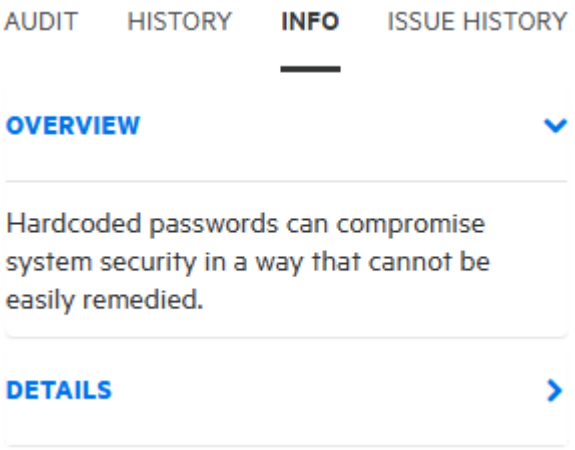
5. 問題について得られる監査履歴を表示するには、右側のペインの［**履歴(HISTORY)**］タブを選択します。



6. 問題の概要、結果に関する詳細、改善に向けた推奨事項、問題のメタデータ、その他のリソースへの参照、およびアプリケーションバージョンに対する影響を確認するには、右側のペインで［**情報(INFO)**］タブを選択します。

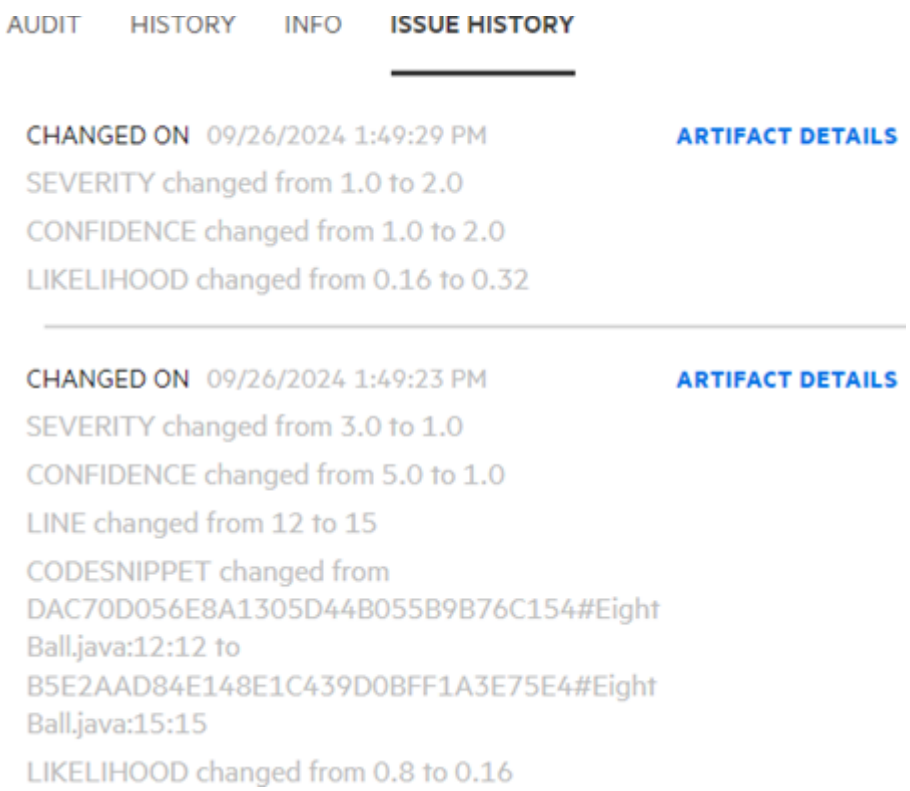


7. 行を展開して情報のカテゴリを表示するには、対応する矢印(›)を選択します。

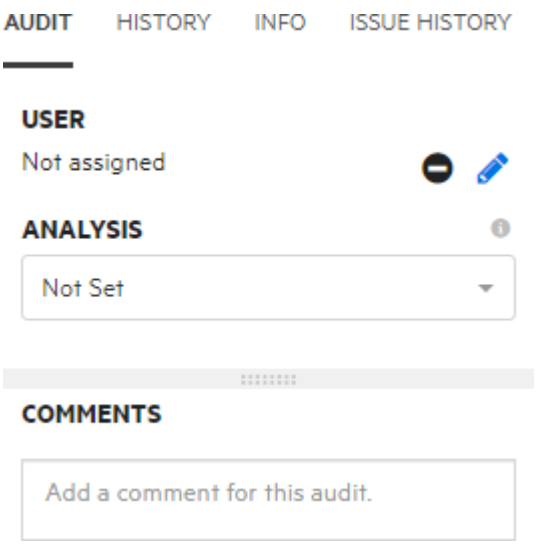


8. 問題の属性の変更を確認するには、［**問題履歴(ISSUE HISTORY)**］タブを選択します。

［**アーティファクトの詳細(ARTIFACT DETAILS)**］をクリックすると、スキャン履歴からのアーティファクトのリストが表示されます。詳細については、「監査の問題履歴」を参照してください。



9. 監査を開始するのに十分な情報を入手したら、［**監査(AUDIT)**］タブを選択します。



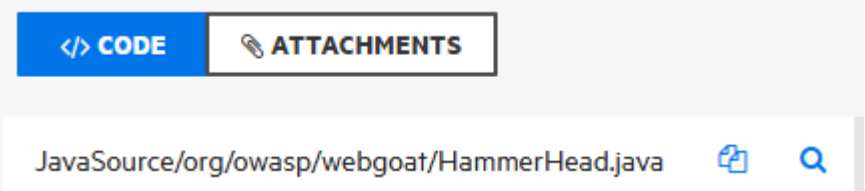
10. (オプション)問題が修正済みか、すぐには影響しないために表示から除外するには、［**抑止(SUPPRESS)**］をクリックします。

11. (オプション)管理者によってアプリケーションセキュリティトレーニングが設定されている場合、選択した問題を処理する方法について、状況に応じた適切なガイダンスを得るには、［**トレーニングを受ける(GET TRAINING)**］をクリックします。

    アプリケーションセキュリティトレーニングWebサイトが新しいブラウザタブで開き、選択した問題のカテゴリ、サブカテゴリ、および言語に基づくトレーニングコンテンツが表示されます。

12. ファイルを問題に添付するには、次の手順に従います。

1. ［**添付ファイル(ATTACHMENTS)**］をクリックします。



2. ［**ここをクリックして追加(CLICK HERE TO ADD)**］をクリックします。
3. ［**添付ファイルのアップロード(UPLOAD ATTACHMENT)**］ダイアログボックスで［**参照(BROWSE)**］をクリックし、アップロードするファイルを選択します。

> **Note**
>
> ファイルサイズは3MBを超えないようにしてください。

4. (オプション)［**説明(Description)**］ボックスに、ファイルの説明を入力します。
5. ［**保存(SAVE)**］をクリックします。

   イメージファイルを添付した場合、Application Securityでは右側の［**Image Preview**］にイメージのプレビューが表示されます。

> **Note**
>
> ファイルが問題に添付された後は、その説明のみを変更できます。

13. ［**コード(CODE)**］をクリックし、［**監査(AUDIT)**］タブを選択します。
14. ユーザを問題に割り当てるには、次の手順に従います。
    1. ［**ユーザ(USER)**］で、［**割り当てられたユーザを編集(Edit assigned user)**］ボタン🖊をクリックします。
    2. ［**ユーザの選択(SELECT USER)**］ダイアログボックスから問題に割り当てるユーザを見つけるには、［**ユーザの検索(Find user)**］ボックスにユーザ名の一部またはすべてを入力し、［**検索(FIND)**］をクリックします。
    3. 返された名前のリストで、問題に割り当てるユーザの名前をクリックします。
    4. ［**DONE**］をクリックします。

> **Note**
>
> 割り当てられたユーザを削除するには、［**ユーザの割り当て解除(Unassign User)**］ボタンをクリックします。 または、割り当てられたユーザを別のユーザに変更するには、［**割り当てられたユーザの編集(Edit assigned user)**］ボタンを選択し、優先するユーザを選択します。

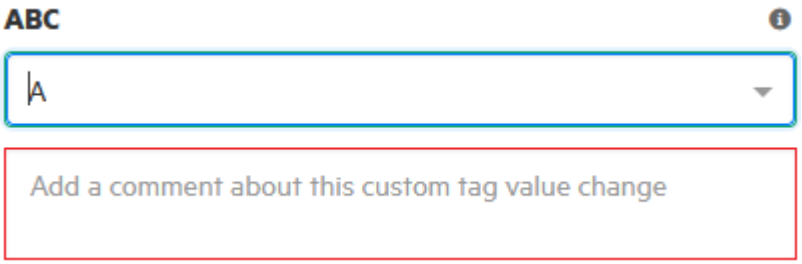
［**監査(AUDIT)**］タブに、選択したユーザ名とアバターが表示されます(使用可能な場合)。

15. ［**分析(Analysis)**］リスト(またはプライマリタグとして定義されている他のタグ)から、この問題についての評価を示す値を選択します。

    値を指定しない場合、Application Securityは問題を未監査として扱います。

16. 追加のカスタムタグがアプリケーションバージョンに関連付けられている場合は、それらのタグの値を指定します。

    管理者が、割り当てるカスタムタグに関するコメントの入力を必須として指定している場合は、カスタムタグ値ボックスの下に表示される赤枠のボックスにコメントを入力する必要があります。



> **Note**
>
> Fortify Audit Assistantが問題を評価した場合は、追加のタグとして［**AA_Prediction**］、［**AA_Confidence**］、および［**AA_Training**］が表示されます。これらのフィールドの使い方については、「Fortify Audit Assistantの結果の確認」を参照してください。

17. ［**コメント(COMMENTS)**］ボックスに、この問題の監査に関するコメントを入力します。
18. ［**保存(SAVE)**］をクリックします。

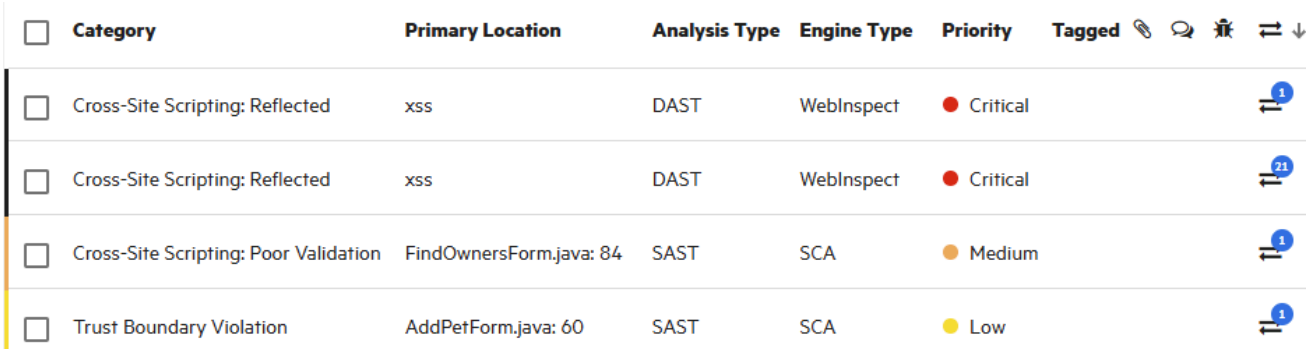
参照情報

1.16.7.1. 相関する問題の監査

アプリケーションバージョン用にアップロードされたアーティファクトに、静的(OpenText SAST)分析と動的(OpenText DAST)分析の両方の結果が含まれる場合、複数の問題が相互に関連し合っている可能性があります。

ある問題が別の分析タイプを使用して明らかになった他の1つ以上の問題と関連している場合、［**相関する問題あり(Has correlated issues)**］ボタンと、相関する問題の数が表示されます。これには、選択した問題をターゲットとするものと、それに由来するものの両方が含まれます。

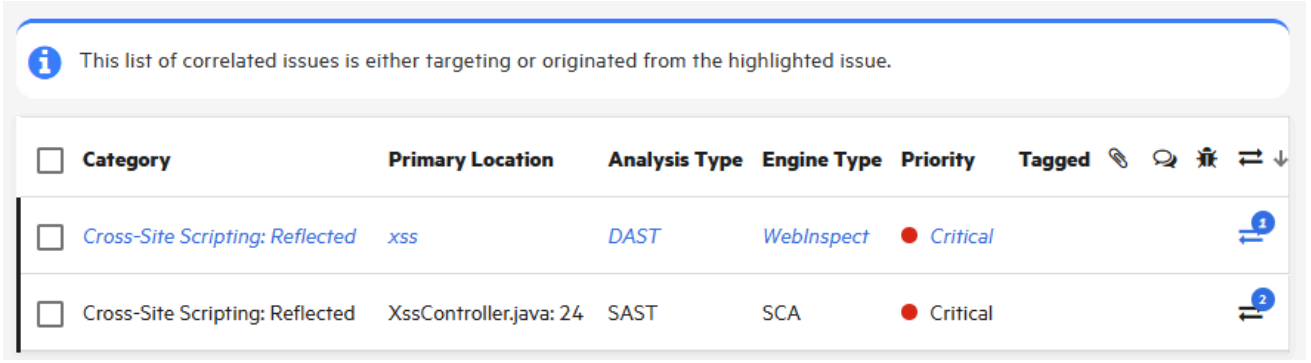
他の問題と相関する問題を一覧表示するには、［**相関する問題あり(Has correlated issues)**］列ヘッダ⇄をクリックします。



青い円に表示される数字は、ある問題と相関する問題の数を示します。

相関する問題を一覧にするには:

- 円または［**相関する問題あり(Has correlated issues)**］ボタン⇄をクリックします。



「分析結果の監査」の説明に従って、一覧表示されている問題を監査できます。

Note

監査の後、1つの問題に存在することが明らかになった根本的な問題が開発者によって修正されると、相関関係にある残りの問題も修正されることがあります。

すべての問題のテーブルに戻るには、［**フィルタ条件(Filter by)**］リストの右側にある［**すべてクリア(CLEAR ALL)**］をクリックします。

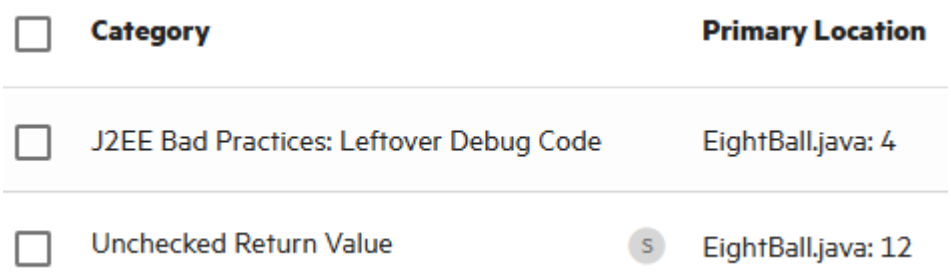
1.16.7.2. 抑止、削除、および非表示の問題について

問題ペインに、抑止、削除、および非表示の問題を一覧表示するかどうかを制御できます。

抑止された問題

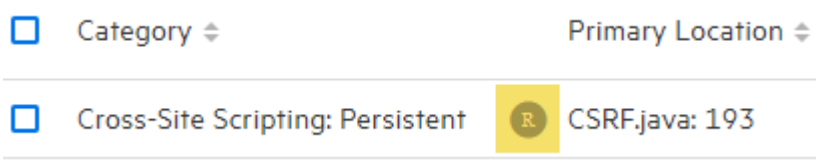
アプリケーションバージョンの連続したスキャンを評価する際に、一部の公開された問題を完全に抑止したい場合があります。特定の脆弱性が現在懸念される問題ではなく、決してそうならないと確信できる場合は、問題に抑止のマークを付けると便利です。また、高優先度ではない、またはすぐに問題になる可能性がない特定のタイプの問題に対して警告を表示しないこともできます。たとえば、修正済みの問題や修正予定のない問題を抑止できます。

抑止された問題は、［**概要(OVERVIEW)**］ページの展開可能なペインで［**Version Progress**］セクションに表示される［**問題の合計数(Total Issues)**］の値には含まれません。抑止された問題は、アプリケーションバージョンメトリックの計算にも含まれません。問題を抑止する方法については、「スキャン結果の監査」を参照してください。



削除された問題

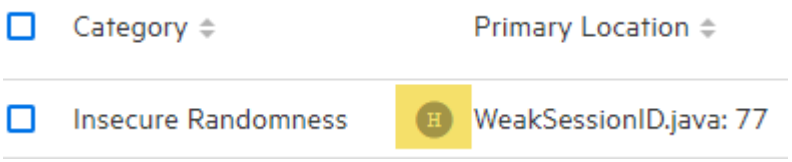
アプリケーションでスキャンが複数回実行されるうちに、問題が修正されたり古くなることがよくあります。Application Securityで分析結果がマージされると、以前のスキャンで検出されたものの、最新の分析結果では明らかでなくなった問題が［削除済み(Removed)］としてマークされます。



削除された問題は、［OVERVIEW］ページの展開可能なペインの［**Version Progress**］セクションに表示される［**Total Issues**］の値には含まれません。

非表示の問題

Fortify Audit Workbenchでは、通常、ユーザは他の問題に集中できるよう、一時的に問題のグループを非表示にします。たとえば、自分に割り当てられている問題を除くすべての問題を非表示にできます。



参照情報

問題の表示設定の設定

1.16.7.2.1. 問題の表示設定の設定

個々のアプリケーションバージョンを対象に、特定の表示初期設定を設定できます。

抑止された問題の表示

アプリケーションバージョンに関連する抑止された問題を表示するには、次の手順に従います。

1. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューで、対象のアプリケーションバージョンを選択します。

   Application Securityに、選択したバージョンの［**監査(AUDIT)**］ページが開きます。

2. ツールバーで［**プロファイル(PROFILE)**］をクリックします。

   ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログが［**詳細オプション(ADVANCED OPTIONS)**］タブに開きます。

   チェックボックスの下にある［**Issue counts by state, based on current selections**］に、選択したアプリケーションバージョンに関連付けられているデータベース内の非表示、抑止、および削除された問題の数が表示されます。

   > **Note**
   >
   > 選択したフィルタセットは、表示される抑止された問題の数には影響を与えません。たとえば、抑止された問題が選択したフィルタセットで非表示になっている場合でも、抑止された問題の数に含まれます。

3. ［**Show suppressed issues**］チェックボックスを選択します。
4. ［**適用(APPLY)**］、［**閉じる(CLOSE)**］の順にクリックします。

   ［**監査(AUDIT)**］ページに、削除されたすべての問題が表示されます。［**プライマリロケーション(Primary Location)**］列では、抑止された各問題に［**S**］タグが示されます。

削除された問題の表示

Application Securityがアップロードされた分析結果をマージする際は、以前のスキャンで検出されたものの、最新の分析結果では明らかでなくなった問題を削除します。

アプリケーションバージョンで削除された問題を表示するには、次の手順に従います。

1. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューで、対象のアプリケーションバージョンのバージョン名を選択します。
   Application Securityに、選択したバージョンの［**監査(AUDIT)**］ページが開きます。
2. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
   ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスが［**詳細オプション(ADVANCED OPTIONS)**］タブに開きます。
   チェックボックスの下にある［**Issue counts by state, based on current selections**］に、選択したアプリケーションバージョンに関連付けられているデータベース内の非表示、抑止、および削除された問題の数が表示されます。

   > **Note**
   > 選択したフィルタセットによって、削除された問題の表示数は影響を受けません。たとえば、抑止された問題が選択したフィルタセットで非表示になっている場合でも、削除された問題の数に含まれます。

3. ［**Show removed issues**］チェックボックスを選択します。
4. ［**APPLY**］、［**CLOSE**］の順にクリックします。

［**監査(AUDIT)**］ページに、削除されたすべての問題が表示されます。［**プライマリロケーション(Primary Location)**］列では、削除された各問題に［**R**］タグが示されます。

非表示にされた問題の表示

非表示にされた問題とは、Application Securityで、フィルタセットルールが現在有効であるために表示されない問題を指します。アプリケーションバージョンに関連する、非表示にされた問題を表示するには:

アプリケーションバージョンに関連する非表示の問題を明らかにするには、次の手順に従います。

1. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューで、対象のアプリケーションバージョンを選択します。

   Application Securityに、選択したバージョンの［**監査(AUDIT)**］ページが開きます。

2. ツールバーで［**プロファイル(PROFILE)**］をクリックします。

   ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスが［**詳細オプション(ADVANCED OPTIONS)**］タブに開きます。

   チェックボックスの下にある［**Issue counts by state, based on current selections**］に、選択したアプリケーションバージョンに関連付けられているデータベース内の非表示、抑止、および削除された問題の数が表示されます。

3. ［**Show hidden issues**］チェックボックスを選択します。

4. ［**APPLY**］、［**CLOSE**］の順にクリックします。

   ［**監査(AUDIT)**］ページに、非表示にされた問題がすべて表示されるようになります。［**プライマリロケーション(Primary Location)**］列では、非表示された各問題に［**H**］タグが示されます。

1.16.7.3. フィルタセットを使用して表示問題を変更する

フィルタセットを使用することで、［**概要(OVERVIEW)**］ページ、［**監査(AUDIT)**］ページ、および［**オープンソース(OPEN SOURCE)**］ページでのアプリケーションバージョンの問題の表示を変更できます。一覧表示されるフィルタセットは、アプリケーションバージョンに割り当てられている問題テンプレートによって異なります。OpenTextが提供する問題テンプレートには、3つのフィルタセットが含まれています。ただし、異なるフィルタセット名とフィルタ条件を持つ他の問題テンプレートを使用することができます。

Application Securityには、次のフィルタセットが用意されています。

- クイックビュー

  クイックビューフィルタセットを使用すると、［重大］フォルダの問題(影響が大きくなる可能性と発生する可能性が高い)と［高］フォルダの問題(影響が大きくなる可能性が高く発生する可能性が低い)を表示できます。このフィルタセットは、最初に結果に注目することで最も差し迫った問題にすばやく対処できる便利なものです。

- セキュリティ監査人ビュー

  このビューには、監査すべき幅広いセキュリティ上の問題が示されます。セキュリティ監査人ビューフィルタには表示フィルタが含まれないので、すべての問題が表示されます。

- PCI監査人ビュー

  このビューは、アプリケーションをPayment Card Industry Security Standards(支払いカード業界のセキュリティ標準)の順守に関して監査する責任を担う個人のために定義されています。

1.16.7.4. 割り当てられた問題の優先度の上書き

分析結果が解析されて、Application Securityにロードされると、サポートされている各エンジンタイプのスキャンパーサが各問題に優先度値を割り当てます。ただし、この優先度値には、影響を受けるコードまたはアプリケーションのフルコンテキストが反映されていません。影響を受けるコードの使用に関連する他の要因によっては、別の優先度を割り当てることが妥当な場合があります。たとえば、対象のコードのセクションがアプリケーション内で呼び出されることがない場合や、アプリケーションが小規模な部門による使用のみを目的としており、他のアプリケーションやシステムに接続されないため、特定された脆弱性の悪用の危険性が低い場合は、「重大」優先度値が割り当てられた脆弱性を「中」または「低」の優先度に分類したほうが妥当である可能性があります。このような使用例を可能にするために、Application Securityでは、問題に最初に割り当てられた優先度を信頼できるユーザが変更できるようになっています。このような優先度の変更は、生成されたレポートに反映されます。

Caution

この機能を使用した変更は、システム内のデータによっては生成されるレポートや計算されるメトリックなどに影響が及ぶという点で、長期的な変更と見なす必要があります。使用する前に、計画している変更についてセキュリティリードと話し合ってください。

優先度の上書き機能を有効にする

優先度の上書きは、システムを新しくデプロイする際にそのシステムに対して有効にすることも、既存のApplication Securityインスタンスに対して有効にすることもできます。

優先度の上書き機能を有効にするには:

1. ［**管理(Administration)**］ビューのナビゲーションペインで、［**設定(Configuration)**］を展開し、［**問題の監査(Issue Audit)**］を選択します。
2. ［**優先度の上書きを有効にする(Enable Priority Override)**］チェックボックスをオンにします。
3. ［**保存(SAVE)**］をクリックします。
4. サーバを再起動します。

サーバの再起動後、この機能は有効になり、すべてのアプリケーションバージョンに適用されます。［**監査(AUDIT)**］ページで、問題の詳細(［**監査(AUDIT)**］タブ)に［**優先度の上書き(PRIORITY OVERRIDE)**］リストタグが表示されるようになります。

ユーザがこの機能を使用できるようにするには、それらのユーザのために「制限付きカスタムタグ値の編集」許可を含む新しいユーザ役割を作成します。これらの役割は、問題の優先度を正確に評価する知識と注意力を持つ信頼できるユーザにのみ付与します。ユーザ役割の作成方法については、「カスタム役割の作成」を参照してください。

> **Note**
>
> 制限付きカスタムタグ値を編集する許可を持っているユーザ役割は、問題の優先度を上書きできますシステム定義のセキュリティリード役割は、制限付きカスタムタグを編集できます。

優先度の上書き機能を無効にするには:

1. ［**管理(Administration)**］ビューのナビゲーションペインで、［**設定(Configuration)**］を展開し、［**問題の監査(Issue Audit)**］を選択します。
2. ［**優先度の上書きを有効にする(Enable priority override)**］チェックボックスをオフにします。
3. ［**保存(SAVE)**］をクリックします。
4. サーバを再起動します。

サーバの再起動後に、この機能がシステム全体で無効になり、［**優先度の上書き(PRIORITY OVERRIDE)**］リストタグが問題の詳細に表示されなくなります。

監査中に優先度値を上書きする

監査中に問題の優先度値を上書きするには:

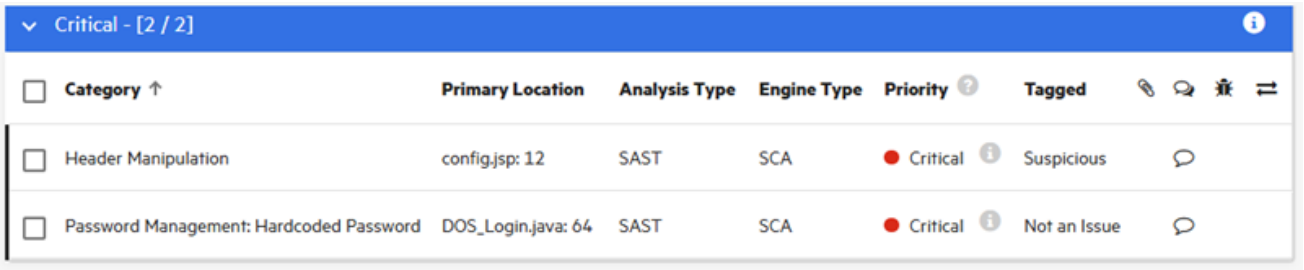
1. ［**監査(AUDIT)**］ページで、問題を含む行を展開します。
2. 右側のペインの［**監査(AUDIT)**］タブの［**優先度の上書き(PRIORITY OVERRIDE)**］リストから、必要な優先度値を選択します。
3. (必須)リストの下の赤枠のボックスに、値を変更した理由を説明するコメントを入力します。

   > **Note**
   >
   > 監査を保存する前に上書きを元に戻す場合は、［**元に戻す(UNDO)**］をクリックします。

4. 新しい優先度値および関連付けられたコメントを保存するには、［**保存(SAVE)**］をクリックします。

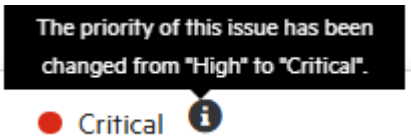
優先度値が変更された問題を表示する

自分および他のユーザが手動で割り当てた優先度値を持つ問題を表示するには、［**グループ化条件(Group By)**］リストから［**優先度の上書き(Priority Override)**］を選択します。



問題テーブルに、優先度が上書きされた問題が、優先度上書きタグの値ごとにグループ化されて一覧表示されます。優先度値が変更されていない問題は、［**未設定(Not Set)**］の下に分類されます。

［**優先度(Priority)**］値がどのように変更されたのかを確認するには、情報アイコンをポイントします。



問題レポートでの優先度の上書き情報の表示

アプリケーションバージョンの監査で優先度上書きタグが使用された場合は、生成する問題レポートにその情報を含めることができます。

優先度の上書き情報を新しい問題レポートに含めるには、レポートのパラメータを指定するときに、［**詳細なレポート(Detailed Report)**］および［**Fortifyの優先度別のカテゴリ(Categories by Fortify Priority)**］チェックボックスをオンのままにします。

問題レポートに優先度値を上書きした問題が含まれている場合(かつ、［**詳細なレポート(Detailed Report)**］および［**Fortifyの優先度別のカテゴリ(Categories by Fortify Priority)**］オプションが選択されている場合)は、次に示すように、その効果のメモがカバーページに表示されます。

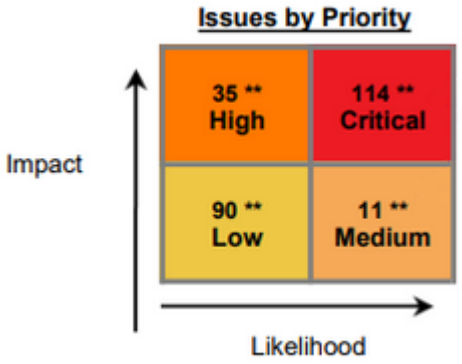
Fortify Software Security Center

OWASP Top 10 2021

RWI - 1.0

Note: This report calculates counts based on issue priority. Issue priority is initially set based on the raw scan information. However, reviewers are able to modify the original issue priority based on additional contextual information. If the issue details section is included in the report, it will indicate the issues where the original value has been changed.

優先度の上書き機能が使用され、［**詳細なレポート(Detailed Report)**］および［**Fortifyの優先度別のカテゴリ(Categories by Fortify Priority)**］パラメータが(手動またはデフォルトで)選択されている場合は、［**エグゼクティブサマリ(Executive Summary)**］の［**優先度別の問題(Issues by Priority)**］キューブで、優先度値が変更されている問題に2つのアスタリスクが表示されます。



これらのレポートの［**問題の詳細(Issue Details)**］セクションには、現在の優先度値と元の優先度値が表示されます。

Path Manipulation ***Remediation Effort(Hrs): 0.5***		**Low** **Original: Critical**
Package: com.order.splc		
Location	**Analysis Info**	**Analyzer**
WEB-INF/src/java/com/order/splc/ConnFactory.java:20 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnFactory.ConnFactory() **In** WEB-INF/src/java/com/order/splc/ConnFactory.java:16	SCA
WEB-INF/src/java/com/order/splc/ConnectionFactory.java:30 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnectionFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnectionFactory.ConnectionFactory() **In** WEB-INF/src/java/com/order/splc/ConnectionFactory.java:26	SCA

元の優先度値に戻す

問題の元の優先度値を上書きして保存した後、その優先度値を元の値に戻すには:

1. ［**監査(AUDIT)**］ページで、問題を含む行を展開します。
2. ［**優先度の上書き(PRIORITY OVERRIDE)**］リストタグの右側で、元に戻すボタンをクリックします。
3. (必須)リストの下の赤枠のボックスに、値を変更した理由を説明するコメントを入力します。
4. 新しい優先度値および関連付けられたコメントを保存するには、［**保存(SAVE)**］をクリックします。

レポートには、エンジンによって設定された元の優先度(変更されていない場合)か、上書きされた値かに関係なく、現在有効な優先度値が反映されます。ユーザが優先度値を変更した場合は、これらのレポートには変更された値が表示されます。そうでない場合は、レポートに元の優先度が表示されます。

1.16.7.5. 問題に対して送信されたバグの表示

［**監査(AUDIT)**］ページの問題テーブルには、リストに表示された問題に対してバグが送信されたかどうかを示す［**バグ送信済み(Bug submitted)**］列列が含まれています。

バグを表示するには、［**VIEW BUG**］アイコン()をクリックし、割り当てられたバグトラッキングアプリケーションにログインします。

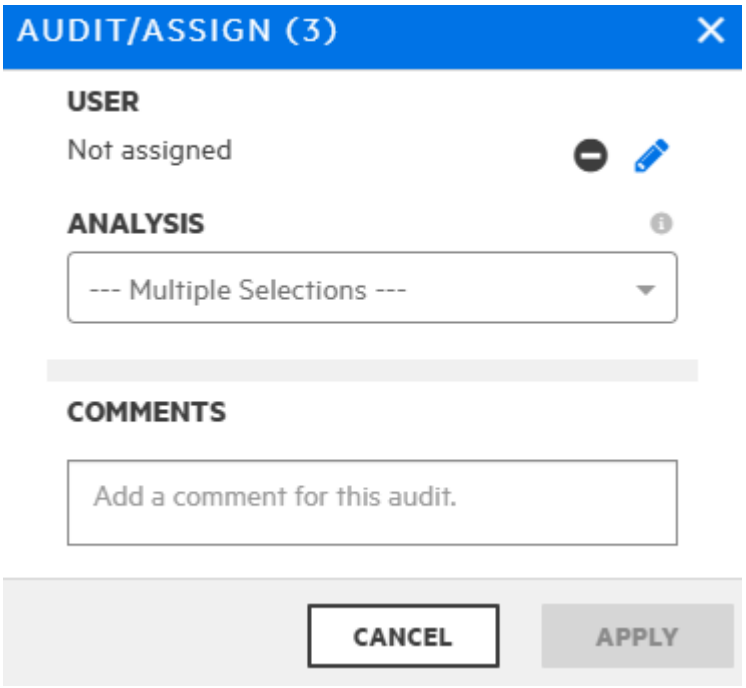
Tip

バグを表示するには、バグトラッカーアプリケーションでサポートされているブラウザを使用する必要があります。

1.16.7.6. 問題のバッチの監査

アプリケーションバージョンの複数の問題を同時に監査するには、次の手順に従います。

1. ［**アプリケーション(Applications)**］で、アプリケーションバージョンの［**監査(AUDIT)**］ページを開きます。
2. 問題リストで、バッチ監査に含める問題のすべてのチェックボックスをオンにします。
3. ［**監査(AUDIT)**］をクリックします。



4. 選択した問題にユーザを割り当てるには、次の手順に従います。
    1. ［**割り当てられたユーザの編集(Edit assigned user)**］ボタン🖉を選択します。
    2. ユーザアカウントを見つけるには、［**ユーザの検索(Find user)**］ボックスにユーザ名の一部またはすべてを入力し、［**検索(FIND)**］をクリックします。
    3. 返される名前のリストで、割り当てるユーザの名前をクリックします。
    4. ［**DONE**］をクリックします。

        ［**USER**］セクションに、選択したユーザ名とアバターが表示されます(使用可能な場合)。
5. ［**分析(ANALYSIS)**］リスト(またはプライマリタグとして定義されている他のタグ)から、この問題のバッチの評価を示す値を選択します。

6. 追加のカスタムタグがアプリケーションバージョンに関連付けられている場合は、それらのタグの値を指定します。

> **Note**
>
> Fortify Audit Assistantが問題を評価した場合は、追加のタグとして［**AA_Prediction**］、［**AA_Confidence**］、および［**AA_Training**］が表示されます。これらのフィールドの使い方については、「Fortify Audit Assistantの結果の確認」を参照してください。

7. (オプション)［**コメント(COMMENTS)**］ボックスに、この問題の監査に関するコメントを入力します。
8. ［**適用(APPLY)**］をクリックします。

参照情報

スキャン結果の監査

1.16.8. Application SecurityでのFortify Audit Assistantの使用

Fortify Audit Assistantバージョン23.2.0のリリースで、OpenTextは新しいFortify Audit Assistantエンジンを導入しました。この第2世代(G2)エンジンは、大幅に改善された予測エンジンを備えており、脆弱性評価でチームが下す決定により提供されるトレーニングデータといっそう調和がとれたものとなります。返される結果はより正確で、環境内のアプリケーションとの関連性が高いものになります。

このセクションでは、Fortify Audit Assistant G2エンジンの能力と精度を最大限に活用する方法を説明します。

Note

Application Securityをバージョン23.2.0以降に更新していない場合は、以前のFortify Audit Assistantエンジン(G1)を引き続き利用できます。アップグレードすると、Fortify Audit AssistantのG1バージョンはサポートされなくなります。オフクラウドバージョンのFortify Audit Assistantをインストールしているユーザも、Application Securityバージョン23.2.0以降と併用する場合は、G2バージョンにアップグレードする必要があります。

1.16.8.1. タグの一貫した使用

Fortify Audit Assistantは、予測を行う際に［誤検出(FALSE POSITIVE)］と［悪用可能(EXPLOITABLE)］という2つのタグを使用します。

Fortify Audit Assistantを最大限に活用するには:

- タグをFortify Audit Assistantタグにマップする

  悪用可能な脆弱性を特定するために使用するタグをFortify Audit Assistantの［悪用可能(EXPLOITABLE)］タグにマップし、問題でない脆弱性にラベルを付けるために使用するタグをFortify Audit Assistantの［誤検出(FALSE POSITIVE)］タグにマップします。このようにしなければ、Fortify Audit AssistはOpenText Core Application Security監査官による決定に基づくグローバルモデルを使用します。使用するタグがFortify Audit Assistantタグにマップされている場合、自社の監査官による決定がグローバルモデルと併せて使用されます。これにより、ご利用のソフトウェア環境および意思決定プロセスに適した決定が考慮されるため、結果を改善できます。

- 脆弱性に一貫してタグ付けする

  Fortify Audit Assistantを最大限に活用するには、監査官がFortify Audit Assistantにマップされたタグを一貫して使用する必要があります。

詳細については、「Application Securityカスタムタグ値へのFortify Audit Assistant分析タグ値のマッピング」を参照してください。

1.16.8.2. Application Securityカスタムタグ値へのFortify Audit Assistant分析タグ値のマッピング

Application SecurityでFortify Audit Assistantを使用するには、Fortify Audit Assistant分析タグ値をリストタイプのApplication Securityカスタムタグ値にマップする必要があります。Fortify Audit Assistant分析タグ値は、Application Securityと一緒にインストールされる、脆弱性を監査済みとして識別するために必要な［**分析(Analysis)**］カスタムタグにマップできます。あるいは、この目的で、別のリストタイプのカスタムタグを選択することもできます。

Fortify Audit Assistantを設定する際に［**自動適用を有効にする(Enable auto-apply)**］チェックボックスをオンにした場合、Fortify Audit Assistantに対し、リストタイプのカスタムタグ値に自動的に適用するFortify Audit Assistant分析タグ値を指示することもできます。

Note

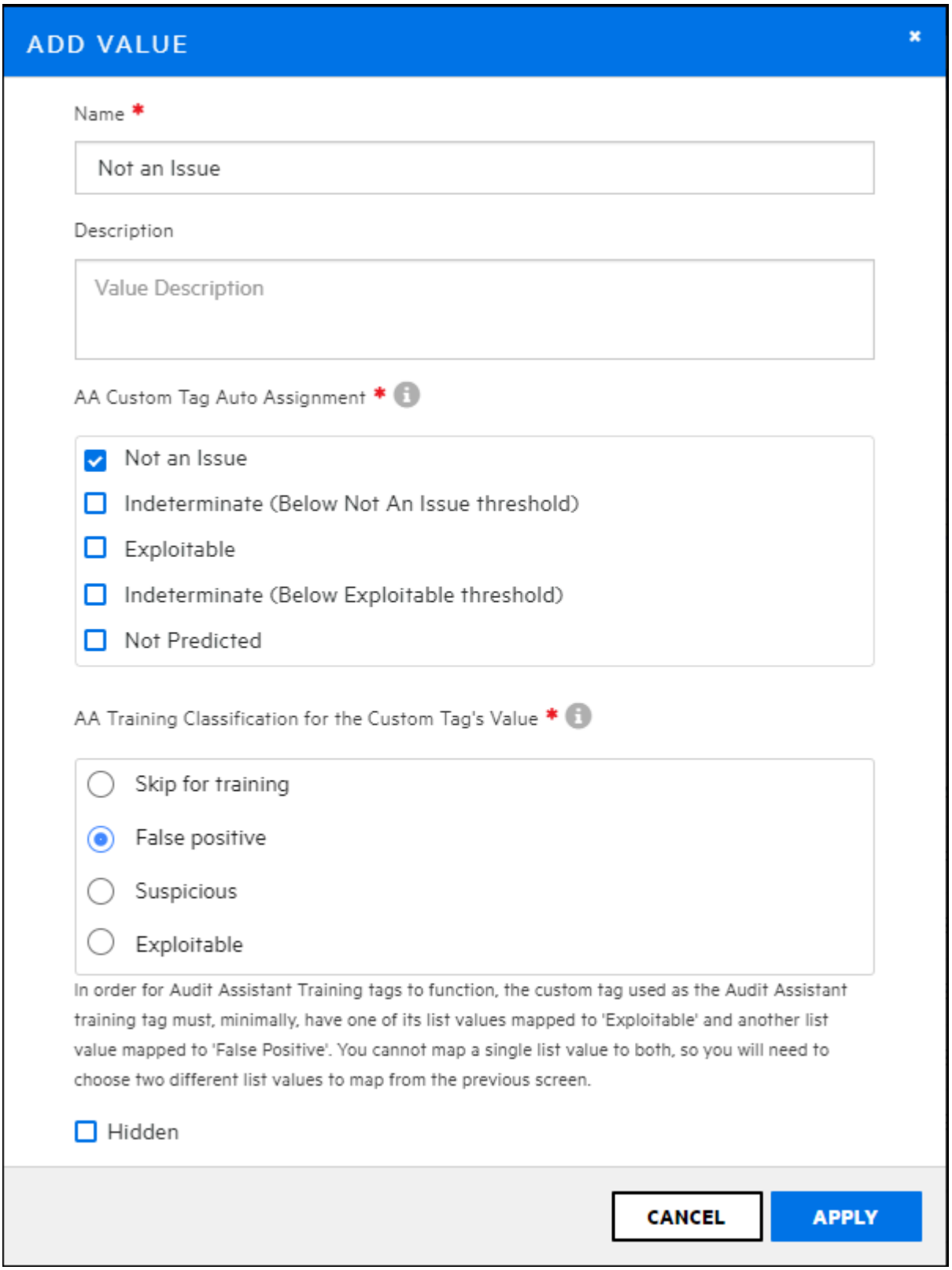
カスタムタグ値をまだ作成していない場合、値を作成してFortify Audit Assistantにマップする方法については、「カスタムタグ値の追加」を参照してしてください。デフォルトの［**分析(Analysis)**］カスタムタグ、または自分で作成したカスタムタグを使用する場合は、以下の手順に従います。まず、タグを作成するか、［**分析(Analysis)**］カスタムタグを使用します。

Fortify Audit Assistant分析タグ値をリストタイプのApplication Securityカスタムタグ値にマップするには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**カスタムタグ(Custom Tags)**］をクリックします。
3. 編集するタグの行をクリックします。

   行が展開されて、タグの詳細が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. ［**リスト値(List Values)**］テーブルで、編集する値の［**値を編集(EDIT value)**］ボタンをクリックします。

   ［**値の追加(ADD VALUE)**］ダイアログボックスが開きます。



Fortify Audit Assistantを使用するようにApplication Securityが設定されていて、自動適用が有効になっている場合、［値の追加(ADD VALUE)］ダイアログボックスには**［AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)］**エリアと、**［カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)］**エリアが表示されます。

6. 新しい値が［**AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)**］エリアのFortify Audit Assistantの予測値と一致する場合、そのチェックボックスをオンにすると、選択したAudit Assistantの予測値にそのリスト値が自動的にマップされます。

   これにより、自動監査が有効にされているすべてのアプリケーションバージョンを自動的に監査できるようになります。

7. ［**カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)**］エリアで、Fortify Audit Assistantモデルをトレーニングする際に使用するオプションを選択します。

   Fortify Audit Assistantトレーニングタグが機能するには、少なくとも2つのリスト値をAudit Assistantトレーニングタグにマップする必要があります。1つは［誤検出(False Positive)］Fortify Audit Assistantトレーニングタグにマップされ、もう1つのリスト値は［悪用可能(Exploitable)］Fortify Audit Assistantトレーニングタグにマップされる必要があります。

8. さらに他のリスト値もマップするには、ステップ5～7を繰り返します。
9. ［**適用(APPLY)**］、［**保存(SAVE)**］の順にクリックします。

参照情報

Fortify Audit Assistantの設定

カスタムタグ値の追加

1.16.8.3. 予測ポリシーの設定について

Fortify Audit Assistantを使用して分析結果に関する予測を行うには、まず、少なくとも1つの予測ポリシーを定義する必要があります。予測ポリシーで、予測に対する信頼しきい値を確立します。次の2種類の信頼しきい値を設定できます。

- 誤検出(False Positive)
- 悪用可能(Exploitable)

デフォルトの信頼しきい値は80%に設定されていますが、0～100%の間で10%単位で設定できます。信頼しきい値を上げると結果の信頼性が向上し、設定されたしきい値以上の結果のみに絞り込まれます。しきい値を調整することで、ソフトウェア環境に合わせて予測ポリシーを微調整できます。

これらの値を調整することはできますが、OpenTextでは、調整する前にデフォルト設定をしばらく使用することを推奨しています。Fortify Audit Assistantを使用するにつれて、提供するトレーニングデータが結果にプラスの影響を与え、最初のスキャンの結果が劇的に向上する可能性があります。

最小信頼しきい値に達していなければ、予測は行われません。信頼しきい値を下回る信頼レベルは正確ではありません。したがって、Fortify Audit Assistantでは、設定された信頼レベルに基づく評価を行うことができません。

Note

管理者はFortify Audit Assistantを設定する際に、デフォルトのグローバル予測ポリシーを選択します。このポリシーは、対象となるアプリケーションバージョンに対して予測ポリシーが指定されていない場合に使用されます。アプリケーションバージョンに予測ポリシーが指定されている場合、Fortify Audit Assistantはそのポリシーを使用して問題を評価します。

トレーニングが結果に与える影響を評価して、ノイズが多すぎることがわかったら、しきい値を調整できます。しきい値を高く設定するほど、Fortify Audit Assistantの予測に対する信頼レベルが高くなります。この場合、信頼しきい値を満たすか超える脆弱性だけが、誤検出または悪用可能と特定されるようになるため、ヒット数が少なくなります。

Fortify Audit Assistantで予測ポリシーを定義する方法の詳細については、「Fortify Audit Assistant Documentation」でFortify Audit Assistantヘルプを参照してください。

参照情報

アプリケーションバージョンに対してFortify Audit Assistantオプションを設定する

Fortify Audit Assistantの設定

Fortify Audit Assistantの自動予測について

1.16.8.4. Fortify Audit Assistantワークフロー

Fortify Audit Assistantを使用する際のワークフローは次のとおりです。

1. バージョン23.2.0以降にアップグレードした後に、Fortify Audit Assistantの設定を更新します。詳細については、「Fortify Audit Assistantの設定」を参照してください。
2. Fortify Audit Assistantアカウントを取得します。
    1. https://analytics.fortify.comに移動します。
    2. ［**アカウントが必要ですか? (Need an Account?)**］リンクをクリックします。

       ［**Fortify Audit Assistantテナントの要求(Request a Fortify Audit Assistant Tenant)**］ウィンドウが開きます。
    3. 会社情報を入力し、［**購読(Subscribe)**］をクリックします。

       入力した情報が確認されると、ようこそ電子メールが届きます。
3. Fortify Audit Assistantにログインして、1つ以上の予測ポリシーを作成します。

   Fortify Audit Assistantで予測ポリシーを定義する方法の詳細については、「Fortify Audit Assistant Documentation」でFortify Audit Assistantヘルプを参照してください。
4. Fortify Audit Assistantトークンを取得します。

   詳細については、「Fortify Audit Assistant Documentation」でFortify Audit Assistantヘルプを参照してください。
5. ［**Audit Assistant**］ページで、次の手順を実行します。
    - Fortify Audit Assistantへの接続を設定してテストし、［**ポリシーの更新(REFRESH POLICIES)**］をクリックして、［**デフォルトの予測ポリシー(Default prediction policy)**］リストに値を自動入力します。
    - デフォルトの予測ポリシーを指定します。
    - (オプション) Application Securityで、未監査の問題を予測対象としてFortify Audit Assistantに自動的に送信できるようにします。
    - (オプション) Fortify Audit Assistantで、カスタムタグに予測値を自動的に適用できるようにします。
      詳細については、「Fortify Audit Assistantの設定」を参照してください。

6. Application Securityでアプリケーションバージョンを開き、最新の完全監査スキャンをFortify Audit Assistantに送信します。

   このステップは「トレーニング」と呼ばれます。詳細については、「Audit Assistantへのトレーニングデータの送信」を参照してください。

7. Application Securitydeアプリケーションバージョンを開き、OpenText SAST分析結果をFortify Audit Assistantに送信します。
8. Fortify Audit Assistantが評価を完了したら、結果を確認し、必要に応じて調整します。
9. 修正された結果をFortify Audit Assistantに送信します。

次も参照

予測ポリシーについて

Fortify Audit Assistantの設定

アプリケーションバージョンに対してFortify Audit Assistantオプションを設定する

アプリケーションバージョンの自動適用と自動予測を有効にする

Fortify Audit Assistantへのトレーニングデータの送信

Fortify Audit Assistantの結果の確認

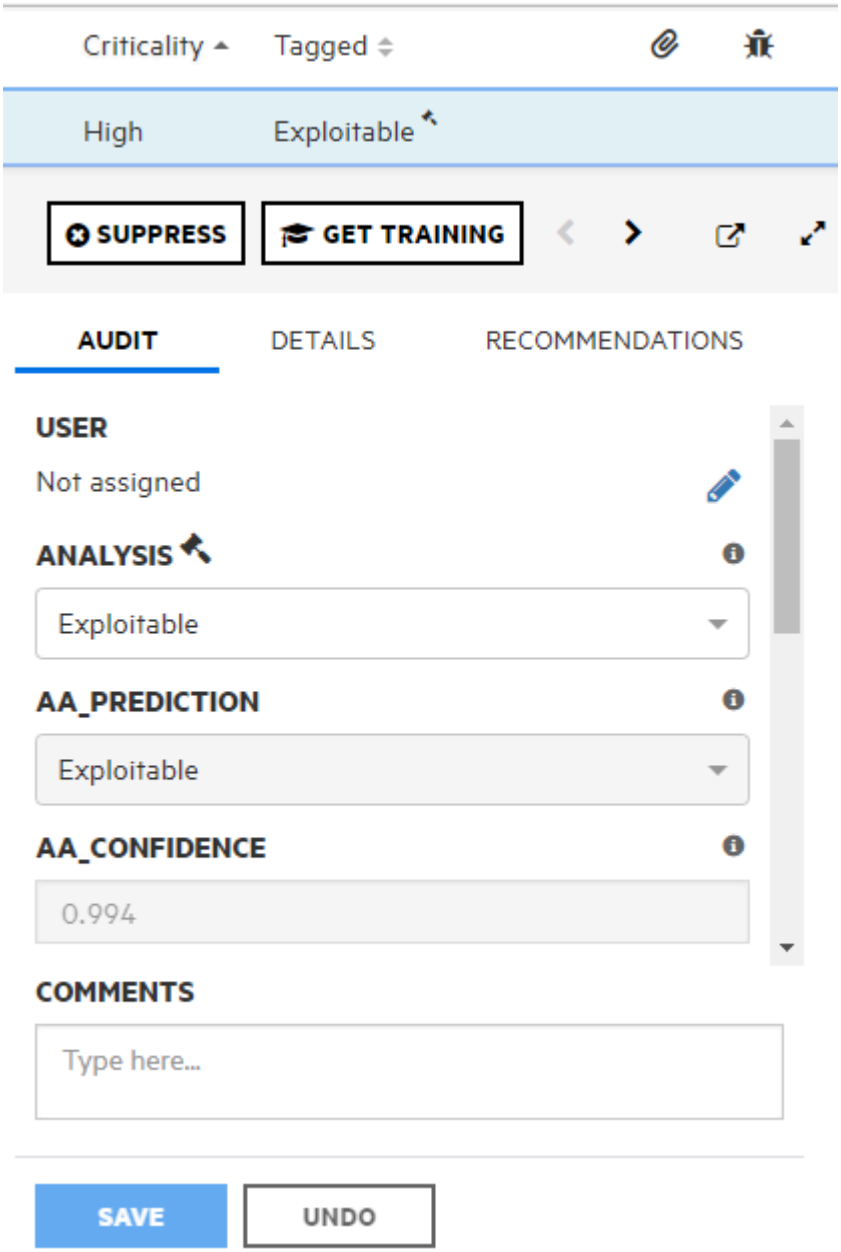
1.16.8.5. Fortify Audit Assistantの結果の確認

分析結果をFortify Audit Assistantに送信して、問題の評価が完了したら、結果を確認できます。

Fortify Audit Assistantの結果を表示するには:

1. アプリケーションバージョンの［**監査(AUDIT)**］ページを開きます。
2. 監査する問題を表示するには、［Fortify Priority］リスクリンク、［**Group by**］リスト、および［**Filter by**］リストを使用します。

   「フォルダに基づく問題の表示」と「概要ページと監査ページに表示する問題をフィルタ処理する」を参照してください。
3. 問題テーブルで、グループを選択した場合は、グループを展開して、グループに含まれている問題を表示します。
4. 問題を展開して詳細を表示するには、テーブル内の該当する行をクリックします。



5. ［**分析(Analysis)**］タグおよびアプリケーションバージョンに関連付けられているその他すべてのカスタムタグに加えて、［**監査(Audit)**］タブには次のものが表示されます。

   - **AA_PREDICTION**—Fortify Audit Assistantが問題に割り当てた悪用可能性レベル。
   - **AA_CONFIDENCE**—Fortify Audit Assistantの［**AA_PREDICTION**］値の正確性に対する信頼性。

     これは、0.000から1.000の範囲の値で表されるパーセンテージです。たとえば、値0.994は、99.4%の信頼レベルを意味します。

6. 悪用可能性評価が表示された［**AA_Prediction**］値と一致する場合は、カスタムタグ値のリストから、Fortify Audit Assistant評価に対応する値を選択できます。それ以

外の場合は、別のカスタムタグ値を選択します。

7. ［**保存(SAVE)**］をクリックします。

参照情報

Fortify Audit Assistantについて

スキャン結果の監査

1.16.8.6. Fortify Audit Assistantのトレーニングについて

ユーザは、スキャン結果の監査時に監査官が行った決定を使用してFortify Audit Assistantをトレーニングできます。ユーザが提供するトレーニングデータを使用することにより、Fortify Audit Assistantは、ユーザの環境内で実行されているアプリケーションに対してより正確で関連性の高い予測を行えます。送信するデータは、監査済みの分析結果に基づいて生成および計算された、機密でないメタデータです。

デフォルトでは、［Audit Assistantトレーニングタグ(Audit Assistant Training Tag)］として他のカスタムタグが選択されていない場合、［Audit Assistantトレーニングタグ(Audit Assistant Training Tag)］がプライマリカスタムタグとして設定されます。

トレーニングデータをFortify Audit Assistantに提供するようにApplication Securityを設定するには:

- ［Audit Assistantトレーニングタグ(Audit Assistant Training Tag)］として使用するカスタムタグを選択します。デフォルトの［**分析(Analysis)**］カスタムタグを使用することも、自分で作成したタグを選択することもできます。カスタムタグを選択しない場合、Fortify Audit Assistantではプライマリタグが使用されます。
- カスタムタグ値をFortify Audit Assistantのトレーニングタグ値にマップします。
- トレーニングデータをFortify Audit Assistantに送信します。

参照情報

Fortify Audit Assistantトレーニングタグの選択

Application Securityカスタムタグ値へのFortify Audit Assistant分析タグ値のマッピング

Fortify Audit Assistantへのトレーニングデータの送信

1.16.8.6.1. 監査官が行った決定を使用してモデルをトレーニングする

使用するタグをAudit Assistantタグにマップして、監査済み分析結果を送信すると、監査官が下した決定が考慮に入れられて、Fortify Audit Assistantの予測が組織の予測にさらに沿ったものとなります。

トレーニングデータを最大限に活用するには、［悪用可能(EXPLOITABLE)］と［誤検出(FALSE POSITIVE)］の両方の評価を監査に含める必要があります。言語ごとに1,500以上の問題を送信すると、Fortify Audit Assistantの予測が大幅に改善されるはずです。

Note

1言語あたり1,500の問題に、相当する数の［悪用可能(EXPLOITABLE)］と［誤検出(FALSE POSITIVE)］の結果が含まれている必要があります。ただし、すべての言語が同時にこのしきい値に達するとは限りません。

詳細については、「Audit Assistantのトレーニングについて」を参照してください。

1.16.8.6.2. Fortify Audit Assistantトレーニングタグの選択

Fortify Audit Assistantトレーニングを設定するには、Fortify Audit Assistantをトレーニングするために使用するカスタムタグを選択する必要があります。カスタムタグを選択しない場合は、プライマリタグが使用されます。

Fortify Audit Assistantタグを選択するには:

1. 管理者としてサインインします。
2. ヘッダで、［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］を選択します。
3. アプリケーションバージョンを選択してから、［**監査(Audit)**］を選択します。
4. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
5. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**カスタムタグ(CUSTOM TAGS)**］を選択します。
6. ［Audit Assistantトレーニングタグ(Audit Assistant Training Tag)］として使用するカスタムタグを選択します。
7. ［**AAトレーニングタグの選択(SELECT AA TRAINING TAG)**］をクリックします。

   ［**Audit Assistantトレーニングタグの選択(SELECT AUDIT ASSISTANT TRAINING TAG)**］ダイアログが開きます。選択したカスタムタグがトレーニング用にまだ設定されていない場合、［**AAトレーニングタグの選択(SELECT AA TRAINING TAG)**］ボックスには［**未設定(Not Set)**］と表示されます。
8. ［**AAトレーニングタグの選択(SELECT AA TRAINING TAG)**］リストから、Fortify Audit Assistantトレーニングタグとして使用するカスタムタグを選択します。

1.16.8.6.3. Fortify Audit Assistantへのトレーニングデータの送信

アプリケーションバージョンがセキュリティ監査官によって監査された後、トレーニングデータをFortify Audit Assistantに送信できます。送信するデータは、監査済みの分析結果に基づいて生成および計算された、機密でないメタデータです。

デフォルトでは、Fortify Audit Assistantトレーニングタグとしてプライマリカスタムタグが使用されます。

トレーニングデータをFortify Audit Assistantに送信するには:

1. ［**ダッシュボード(Dashboard)**］ビューまたは［**アプリケーション(Applications)**］ビューで、対象のアプリケーションバージョンを選択してから、［**監査(Audit)**］を選択します。
2. ツールバーで［**プロファイル(PROFILE)**］をクリックします。
3. ［**アプリケーションプロファイル(APPLICATION PROFILE)**］ダイアログボックスで、［**Audit Assistantトレーニング(AUDIT ASSISTANT TRAINING)**］タブをクリックします。

   ［**Data last sent for training**］フィールドには、アプリケーションバージョンのトレーニングデータが最後に送信された日付と時刻が表示されます。
4. 新しいトレーニングデータを送信するには、［**SEND FOR TRAINING**］をクリックします。
5. ［**閉じる(CLOSE)**］をクリックします。
6. ［**アーティファクト(ARTIFACTS)**］を選択し、アップロードの［**ステータス**］フィールドに［**完了(Complete)**］と表示されているかどうかを確認します。

処理が完了していれば、［**監査(AUDIT)**］ページで結果を表示できます。

参照情報

Fortify Audit Assistantの結果の確認

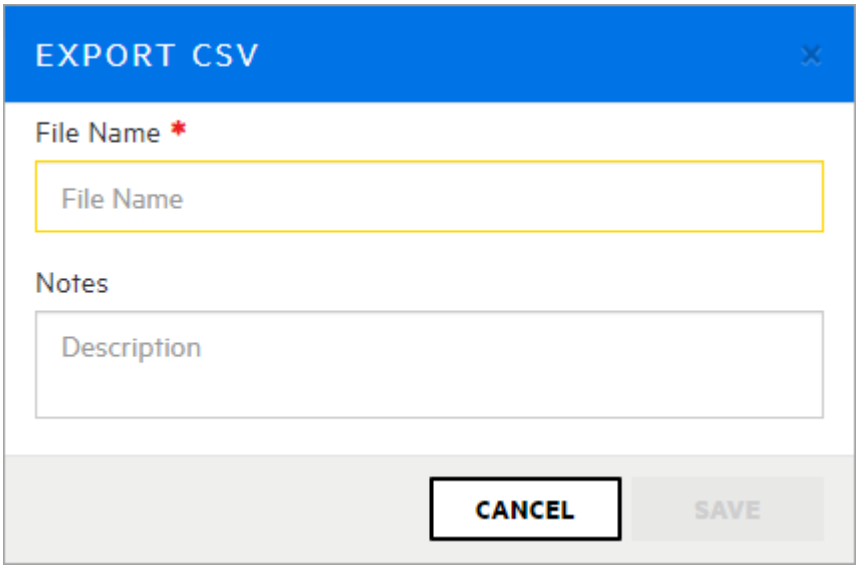
Fortify Audit Assistantについて

アプリケーションバージョンの自動適用と自動予測を有効にする

1.16.9. オープンソースデータのエクスポート

［**オープンソースコンポーネント(OPEN SOURCE COMPONENTS)**］ページに表示されるオープンソースデータをエクスポートするには:

1. アプリケーションバージョンのオープンソースデータをアップロードした後、そのアプリケーションバージョンの［**オープンソース(OPEN SOURCE)**］ページを選択します。
2. ［**エクスポート(EXPORT)**］をクリックします。



3. ［**ファイル名(File Name)**］ボックスに、生成するCSVファイルの名前を入力します。
4. (オプション)［**Notes**］ボックスに、生成されたファイルに関連付けるメモを入力します。
5. ［**保存(SAVE)**］をクリックします。
6. エクスポートされた結果を表示するには:
    1. ヘッダで、［**レポート**］をクリックします。
    2. ［**データエクスポート(DATA EXPORTS)**］タブをクリックします。
    3. 結果のテーブルで、エクスポートされたファイルの行をポイントして［**ダウンロード(Download)**］ボタンをクリックします。

結果のCSVファイルに、オープンソースフィールドが `<engine_type>.<field_name>` として表示されます。たとえば、`SONATYPE.cweurl` が［Sonatype **CWE URL**］フィールドに対応しています。

CSVファイルが削除されるまで保持される期間を確認するには、「ジョブスケジューラ属性の設定」を参照してください。これらのレポートのデフォルトの有効期限は2日です。

1.16.10. Application SecurityとFortify WebInspect Enterpriseの統合

Application SecurityとFortify WebInspect Enterpriseは緊密に統合され、スキャン結果を共有できます。管理者は、ユーザインタフェースから動的スキャンの要求を送信することもできます。このセクションでは、OpenText DASTの結果をApplication Securityに表示する方法について説明し、動的スキャンを要求する手順をApplication Securityのユーザに示します。

1.16.10.1. Application SecurityでのOpenText DAST分析結果の表示

OpenText DASTでは、スキャン結果(結果データと監査データ)がFPR形式で保存され、ユーザはそれをApplication Securityにアップロードできます。「スキャンアーティファクトのアップロード」を参照してください。OpenText DASTの問題の詳細は、OpenText SASTなど、他のアナライザで明らかにされた問題に関して表示される問題とは異なります。

Important

OpenText DASTをApplication Securityと正常に統合するには、Application SecurityサーバとOpenText DASTサーバの両方に、Javaランタイム環境で信頼されるCA証明書をインストールする必要があります。

［**CODE**］タブの左ペインにある［**Overview**］セクションには、結果に関するサマリ情報と［**Implications**］セクションが表示されます。［**Additional References**］セクションには、使用可能な関連する参照のリストが表示されます。

中央のペインには、次の情報が表示されます。

URL—脆弱性が検出されたWebサイトページ

メソッド(Method)—攻撃に使用されるHTTPメソッド(GET、PUT、POSTなど)

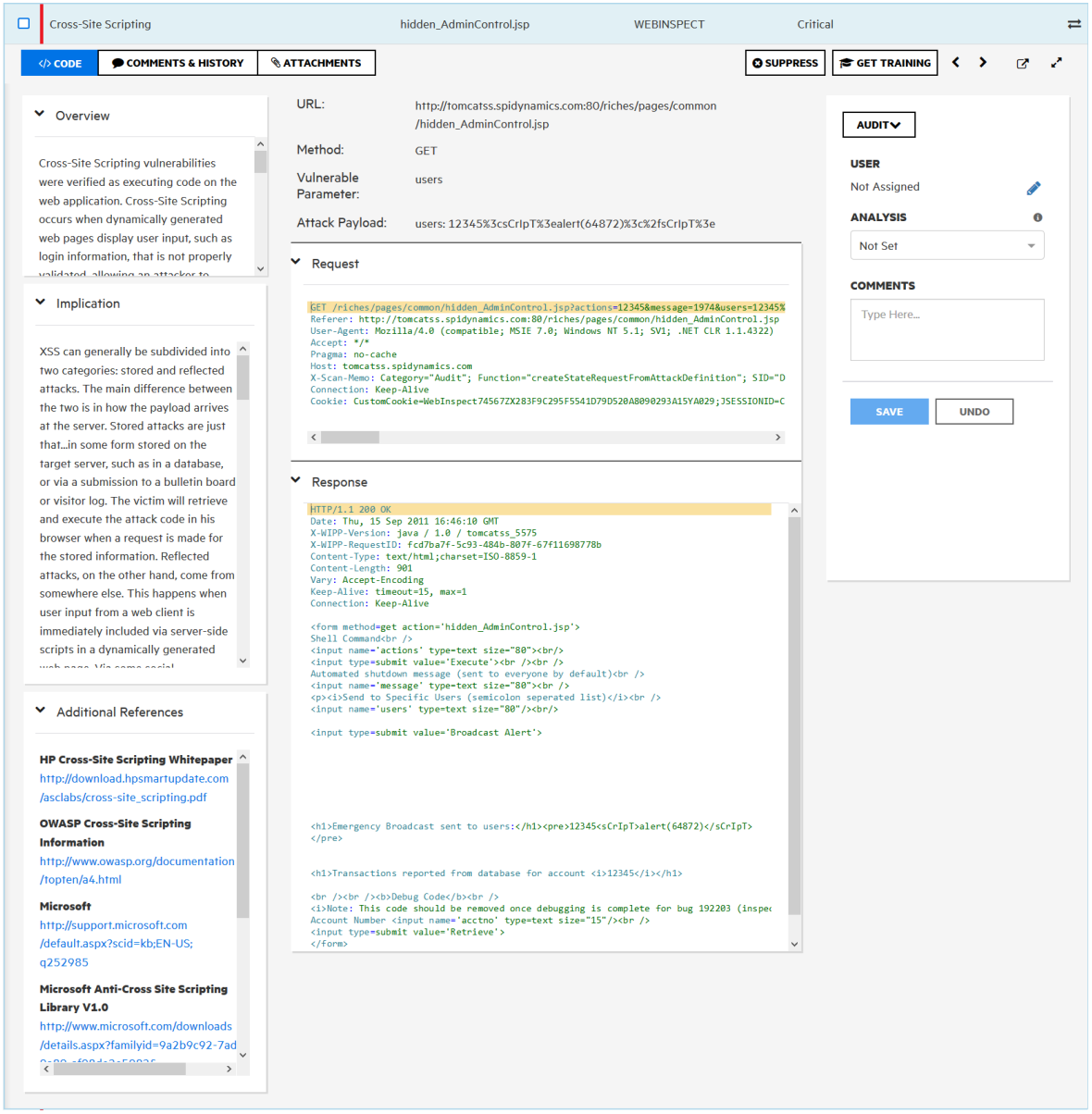
脆弱なパラメータ(Vulnerable Parameter)—脆弱なパラメータの名前

攻撃ペイロード(Attack Payload)—脆弱性を悪用するためにペイロードとして使用されるシェルコード

この情報の下にある［**Request**］セクションには行われた要求が表示され、攻撃が強調表示されます。［**Response**］セクションには要求への応答が表示され、トリガが強調表示されます。

Note

応答にバイナリデータまたは大量の(50 KBを超える)データが含まれている場合は、［**Response**］セクションの下部に［**Download Response**］ボタンが表示されます。これらの応答をテキストファイルでダウンロードするには、［**Download Response**］をクリックします。



［**ステップ(Steps)**］タブは、OpenText DASTの結果ファイルにステップが含まれている場合にのみ使用できます。

追加の詳細と推奨事項の表示

問題の追加の詳細と推奨事項を表示するには、問題ツールバーで、［**新しいタブで開く(Open in new tab)**］ボタン、または［**全画面に拡大(Expand to full screen)**］ボタンをクリックします。

［**詳細(Details)**］には、この問題で調べる内容に関する提案が表示されます。

問題に対処する方法に関する推奨事項とヒントを表示するには、［**監査(AUDIT)**］リストから［**推奨事項(Recommendations)**］を選択します。

問題を監査する方法については、「スキャン結果の監査」を参照してください。

1.16.10.2. OpenText DAST監査データ

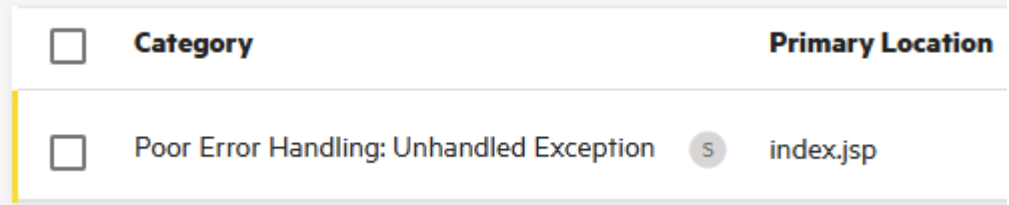
スクリーンショットに加えて、次の種類の監査データがOpenText DASTからApplication Securityに転送されます。

- **脆弱性メモ(Vulnerability Notes)**—OpenText DASTの脆弱性メモは、問題コメントとしてApplication Securityに転送されます。
- **無視された脆弱性(Ignored Vulnerabilities)**—OpenText DASTで［無視(Ignored)］マークが付けられた脆弱性は、Application Securityへの転送後に［抑止(Suppressed)］マークが付けられます。
- **誤検出**

1.16.10.3. 誤検出

Application Securityには、OpenText DASTの「誤検出」ステータスに直接相当するステータスはありません。OpenText DASTユーザが脆弱性を誤検出としてマークした場合、脆弱性は脆弱性リストから非表示にされて、脆弱性カウントから除外されます。

誤検出ステータスを Application Security でエミュレートするには、デフォルトの**解析**カスタムタグを使用できます。Application SecurityでOpenText DASTの誤検出に［**分析(Analysis)**］値「問題でない」が割り当てられます。OpenText DASTの問題をリストとカウントから隠す動作をエミュレートするために、問題は「**抑止(Suppressed)**」としてマークされます。



Note

選択した**解析**の値が「問題でない」から変更されたり欠けている場合、あるいは［**解析**］リストがアプリケーションバージョンから除去されている場合、誤検出ステータスの問題は失われます。この問題は「抑止」とマークされています。

参照情報

問題の表示設定の設定

1.16.10.4. 動的スキャン要求をFortify WebInspect Enterpriseに送信する

OpenText DASTが環境にインストールされ、次のいずれかの役割が割り当てられている場合には、スキャンをApplication Securityから要求できます。

- 管理者
- セキュリティリード
- マネージャ
- 開発者

アプリケーションバージョンのスキャン要求を作成するには、次の手順に従います。

1. ［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］ビューから、スキャンするアプリケーションバージョンを選択し、［**アーティファクト(Artifacts)**］を選択します。
2. ［**アーティファクト履歴(ARTIFACT HISTORY)**］ページで、［**動的スキャン(DYNAMIC SCAN)**］をクリックします。
3. 次の表に示す情報を指定します。

   次の表には、ユーザまたは別のApplication Security管理者がシステムに追加したカスタム動的スキャン属性は含まれていません。

動的スキャン属性	説明(Description)
URL	(必須)スキャンするサイトのURL
Site Login	スキャンするサイトにログオンするために必要なユーザ名
Site Passcode	サイトへのアクセスに使用するパスワード
Network Login	ネットワーク認証に必要なユーザ名
Network Passcode	ネットワーク認証に必要なパスワード
Related Host Name(s)	アプリケーションがスキャンできるホスト
Web Services Used	スキャンするアプリケーションが使用するWebサービスのカンマ区切りのリスト
Technologies Used	スキャンするサイトで使用されるテクノロジのカンマ区切りのリスト
Compliance Implications	コンプライアンスに関する潜在的な影響に関する情報
Allowable Scan Times	テスタがスキャンを実行できる日時 例: 2018年9月3日から2018年11月30日まで、月曜日から金曜日、17:00から06:00 スケジュールを設定して後で実行する代わりに、すぐにスキャンを実行できます。
WSDL	Webサービス記述言語ファイル(*.wsdl、*.webmacro、または*.xml)を参照して選択します。

Note

OpenText DASTでスキャン要求を処理する動的テスタは、ビジネスリスクやコンプライアンスへの影響など、他のアプリケーションバージョンの属性に興味を持つ場合があります。テスタは、既存のWebサービスメソッドを使用して、アプリケーションバージョンの属性を取得できます。

4. ［**SUBMIT**］をクリックします。

   Application Securityは、要求の送信が成功したことを確認するメッセージを表示します。

   次に、スキャン要求を監視して応答するOpenText DASTテスタは、指定した時間にスキャンを実行し、Application Securityに結果をアップロードします。

5. Application Security管理者またはApplication Securityテスタであれば、要求された動的スキャンをFortify WebInspect Enterpriseから直ちに実行できます。

参照情報

Application SecurityでのOpenText DAST分析結果の表示

Fortify WebInspect Enterpriseの動的スキャン要求の処理

1.16.10.5. Fortify WebInspect Enterpriseの動的スキャン要求の処理

管理者またはApplication Securityテスタの役割を持っている場合には、Fortify WebInspect Enterpriseを起動して、Application Securityユーザが送信した動的スキャン要求を表示および処理できます。

Fortify WebInspect Enterpriseで動的スキャン要求を処理するには、次の手順に従います。

1. Fortify WebInspect EnterpriseでApplication Securityを初期化してから、WebInspect Enterprise Consoleを使用してApplication Securityアプリケーションバージョンを WebInspectプロジェクトと同期します(*OpenText™ Fortify WebInspect Enterpriseユーザガイド*を参照)
2. Application Securityの［**ダッシュボード(Dashboard)**］または［**アプリケーション(Applications)**］ビューから、動的スキャンが要求されたアプリケーションバージョンを選択し、［**アーティファクト(Artifacts)**］を選択します。
3. ［**アーティファクト(ARTIFACTS)**］ページで、［**WIEを起動する(LAUNCH WIE)**］をクリックします。
4. ヘッダの下で、［**スキャン要求(Scan Requests)**］をクリックします。

   ［**スキャン要求(SCAN REQUESTS)**］ビューには、Application SecurityからFortify WebInspect Enterpriseに送信された動的スキャン要求すべてが一覧表示されます。
5. 保留中の要求を選択します。
6. 下のペインの［**Details**］タブの［**Status**］リストから［**In Progress**］を選択し、［**Change Status**］をクリックします。アプリケーションバージョンに割り当てられているユーザは、Application Securityでスキャン要求が保留中でなくなったのを確認できるようになります。
7. ビューの上部で［**Create a Web Site Scan**］をクリックし、スキャンウィザードの手順を完了してスキャンを実行し、Application Securityに結果をアップロードします。詳細な手順については『OpenText™ Fortify WebInspect Enterpriseユーザガイド』を参照してください。

次も参照

動的スキャン要求をFortify WebInspect Enterpriseに送信する

1.16.10.6. 動的スキャン要求を編集およびキャンセルする

アプリケーションバージョンに対して最後に送信された動的スキャン要求のステータスを表示するには:

1. スキャン要求を送信したアプリケーションバージョンの詳細ページの［問題］タブに移動します。
2. ［**Dynamic Scan Request**］リストから、［**Last Scan Status**］を選択します。

Application Security に、スキャン要求が送信された日付と時刻、および要求ステータスの情報が表示されます。

動的スキャン要求状態

動的スキャン要求を送信した後で(動的スキャン要求をFortify WebInspect Enterpriseに送信するを参照)、要求はPENDING状態になります。テスタがWebInspectからスキャンを開始すると、要求状態はIN_PROGRESSになります。WebInspectテスタがスキャンを完了すると、スキャン要求はCOMPLETED状態になります。

動的スキャン要求が保留中の場合には、その要求を編集またはキャンセルできます。ただし、スキャンが始まるとすぐに、編集もキャンセルもできなくなります。

動的スキャン要求を編集する

動的スキャン要求を編集するには:

> **Note**
>
> 編集できるのは、送信したスキャン要求だけです。

1. 動的スキャンを要求したアプリケーションバージョンの詳細ページの［Issues］タブに移動します。
2. ［**Dynamic Scan Request**］リストから［**Edit**］を選択します。
3. ［**動的スキャン要求(Dynamic Scan Request)**］ダイアログボックスで、動的スキャン属性の値を編集してから、［**送信(Submit)**］をクリックします。

動的スキャン要求をキャンセルする

保留中の動的スキャン要求をキャンセルするには、次の手順に従います。

Note

キャンセルできるのは、送信したスキャン要求だけです。

1. 動的スキャンを要求したプロジェクトバージョンの詳細ページの［Issues］タブに移動します。
2. ［**Dynamic Scan Request**］リストから［**Cancel**］を選択します。

   Application Securityでは、最後の動的スキャン要求をキャンセルすることを確認するように求めるプロンプトが表示されます。
3. ［**Yes**］をクリックします。

1.16.11. オープンソースデータの表示

Application Security対応のOpenText Core SCAまたはSonatypeパーサプラグインをダウンロードしてインストールして有効化すると、所定のアプリケーションバージョンに関してアップロードされたオープンソース脆弱性データを表示できるようになります。アプリケーションバージョンに関してアップロードされた結果は、［**監査(AUDIT)**］ページまたは［**オープンソース(OPEN SOURCE)**］ページから表示できます。

［監査(AUDIT)］ページからのオープンソースデータの表示

［**監査(AUDIT)**］ページからオープンソース脆弱性結果を表示するには:

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. オープンソースの結果がアップロードされているアプリケーションバージョンを選択します。
3. ［**監査(AUDIT)**］ページの［**グループ化条件(Group By)**］リストから、［**分析タイプ(Analysis Type)**］を選択します。
4. ［**DEBRICKED**］ヘッダまたは［**SONATYPE**］ヘッダを展開してから、結果を調べる行を展開します。

表示されるOpenText Core SCA脆弱性データを解釈する方法については、Debrickedのドキュメントを参照してください。表示されるSonatype脆弱性データを解釈する方法については、Sonatypeのドキュメントを参照してください。

オープンソース結果を監査する方法については、「分析結果の監査」を参照してください。

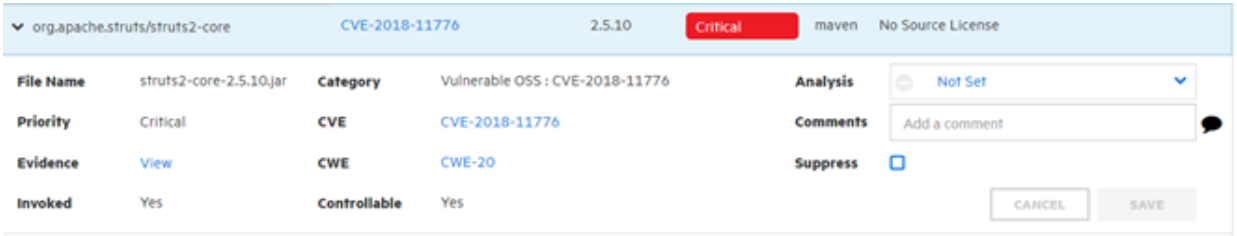
［オープンソース(OPEN SOURCE)］ページからのオープンソースデータの表示

［**オープンソース(OPEN SOURCE)**］ページからオープンソース結果を表示するには:

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. オープンソースの結果がアップロードされているアプリケーションバージョンを選択します。
3. ［**オープンソース(OPEN SOURCE)**］をクリックします。

［**オープンソース(OPEN SOURCE)**］ページは、選択したアプリケーションバージョンに関するオープンソースの結果がアップロードされている場合にのみ表示されます。

4. ［**OPEN SOURCE COMPONENTS**］テーブルで、調べる問題の行をクリックします。



次の表に、詳細の説明を示します。

フィールド	説明(Description)
File Name	問題が検出されたコンポーネントファイルの名前。
Category	OSSインデックスカテゴリ: Common Vulnerabilities and Exposures ID
Analysis(または割り当てられた他のプライマリタグ)	［**オープンソース(OPEN SOURCE)**］ページから問題を監査する場合は、このリストから割り当てるプライマリタグ値を選択できます。
Priority	Fortifyの優先度評価
CVE	脆弱性に割り当てられたCVE (Common Vulnerabilities and Exposures)ID番号。リンクをクリックすると、CVEサイト上の脆弱性の詳細な説明に直接移動します。
Comments	［**オープンソース(OPEN SOURCE)**］ページから問題を監査する場合は、ここにコメントを追加できます。
Evidence	脆弱性が呼び出された場合や制御可能な場合の証拠へのリンク。
CWE	Common Weakness Enumeration。このリンク(もしあれば)をクリックすると、Common Weakness EnumerationのWebサイトが開き、発見されたソフトウェアの弱点タイプの詳細が表示されます。

フィールド	説明(Description)
抑止する(Suppress)	問題に懸念がないと思う場合は、このチェックボックスをオンにします。問題の抑止の詳細については、抑止、削除、および非表示の問題についてを参照してください。
Invoked	このフィールドには、コード内で問題が呼び出されたかどうかが表示されます。
制御可能(Controllable)	このフィールドには、ユーザが制御する入力がメソッドまたは関数に到達したかどうかが表示されます。

表示されるOpenText Core SCA脆弱性データを解釈する方法については、Debrickedのドキュメントを参照してください。表示されるSonatype脆弱性データを解釈する方法については、Sonatypeのドキュメントを参照してください。

参照情報

Debrickedの結果を表示するための準備

Sonatypeの結果を表示するための準備

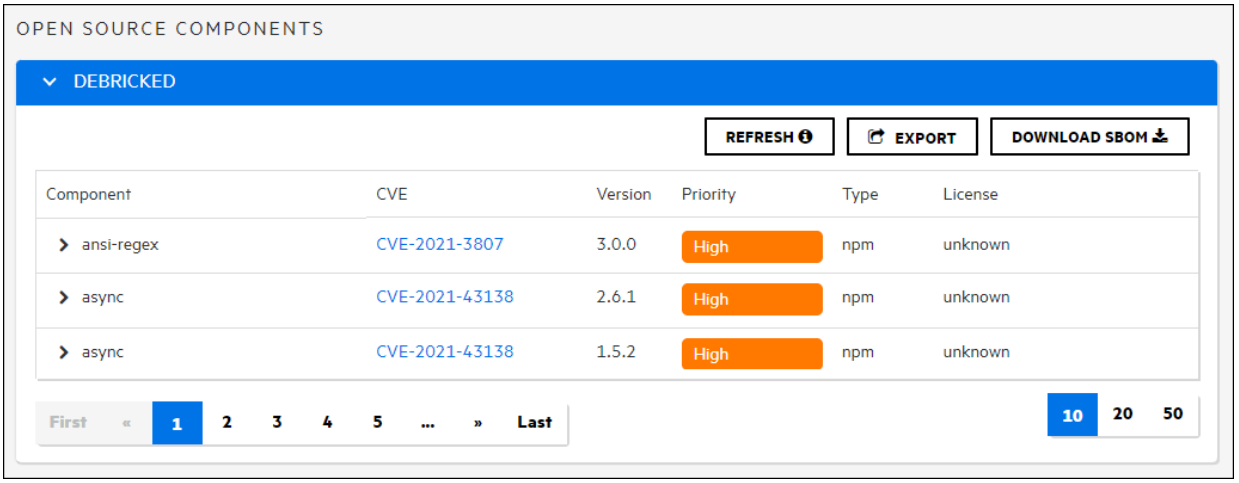
1.16.12. OpenText Core SCA (Debricked) SBOM (Software Bill of Materials)のダウンロード

Software Bill of Materials (SBOM)は、ソフトウェアアプリケーションに含まれるソフトウェアの依存関係のリストです。これには、直接的な依存関係に加えて、直接的な依存関係で使用される依存関係(間接的または遷移的な依存関係とも呼ばれる)も含まれます。SBOMでは、ソフトウェアの構築時に使用されるサプライチェーン関係が説明されます。SBOMは、CycloneDX形式です。

SBOMをJSONファイルとしてダウンロードして、使用しているオープンソースコンポーネントを評価できます。SBOMで提供される情報を基に、使用しているバージョンがプロジェクトに対して安全か、それとも別のバージョンやオープンソースパッケージに変更する必要があるかどうかを決定することができます。

SBOMをダウンロードするには:

1. ヘッダで、［**アプリケーション(Applications)**］を選択します。
2. オープンソースの結果がアップロードされているアプリケーションバージョンを選択します。
3. ［**オープンソース(OPEN SOURCE)**］をクリックします。
4. ［**Debricked**］グループを展開します。



5. ［**SBOMをダウンロード(Download SBOM)**］をクリックします。
6. ダウンロードされたJSONファイルをテキストエディタで開き、SBOMを表示します。

1.17. OpenText ScanCentral DASTの使用

動的スキャンを要求および管理するために、Application SecurityがOpenText ScanCentral DASTと通信するように設定されている場合は、［**ScanCentral**］ビューの［**DAST**］タブに［**スキャン(Scans)**］、［**センサ(Sensors)**］、［**センサプール(Sensor Pools)**］、［**設定リスト(Settings List)**］、および［**スキャンスケジュール(Scan Schedules)**］の各ページが表示されます。Application SecurityとOpenText ScanCentral DAST間の接続を設定する方法については、「OpenText ScanCentral DASTスキャンの実行と管理の有効化」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。

1.17.1. OpenText ScanCentral DASTの許可

次の表は、OpenText ScanCentral DAST関連タスクを実行する権限を持つApplication Securityの役割を示しています。

役割	許可
表示のみ	• アプリケーションバージョンに割り当てられていないジョブを除き、OpenText ScanCentral DASTデータを表示します。 **制限:** • ユーザは、割り当てられているアプリケーションのスキャンだけを表示できます • ユーザは、割り当てられたアプリケーションのセンサプール割り当てだけを表示できます

役割	許可
セキュリティリード	• OpenText ScanCentral DASTデータの表示 • スキャン、スケジュール、および設定の作成、実行、変更、および削除 • プールとセンサの管理 • アーティファクトのダウンロード • 既存のテンプレートと基本設定からのスキャンの実行 • 拒否間隔、アプリケーションの優先度レベル、および保持ポリシーの管理 • グローバル制限、制限付きスキャン設定、およびプライベートデータ設定の管理 • 鍵ストアおよびアーティファクトのリポジトリの管理 **制限:** • ユーザは、割り当てられたアプリケーションバージョンのスキャン要求のみをキャンセルできます。 • ユーザは、センサプールに割り当てられているアプリケーションバージョンのみを割り当てることができます。

役割	許可
マネージャ	• OpenText ScanCentral DASTデータの表示 • プールとセンサの管理 **制限:** • ユーザはスキャン関連データを更新できません • ユーザは、割り当てられたアプリケーションバージョンのスキャン要求のみをキャンセルできます。 • ユーザは、センサプールに割り当てられているアプリケーションバージョンのみを割り当てることができます。
開発者	• OpenText ScanCentral DASTデータの表示 • 既存のテンプレートと基本設定からのスキャンの実行 • アーティファクトのダウンロード
アプリケーションセキュリティテスタ	• OpenText ScanCentral DASTデータの表示 • スキャン、スケジュール、および設定の作成、実行、変更、および削除 • 既存のテンプレートと基本設定からのスキャンの実行 • アーティファクトのダウンロード

参照情報

Application Securityの役割に関する許可情報の表示

1.17.2. OpenText ScanCentral DASTへの動的スキャン要求の送信

Application SecurityがOpenText ScanCentral DASTと統合されており、次のいずれかの役割がユーザに割り当てられている場合は、Application Securityから動的スキャンを要求できます。

- 管理者
- アプリケーションセキュリティテスタ
- セキュリティリード
- 開発者

OpenText ScanCentral DASTスキャンを設定し、スキャン、センサ、センサプール、設定、およびスキャンスケジュールを使用する方法については、『*OpenText™ ScanCentral DASTの設定および使用ガイド*』を参照してください。

参照情報

OpenText ScanCentral DASTスキャンの実行と管理の有効化

OpenText ScanCentral DASTの許可

1.17.3. KafkaをOpenText ScanCentral DASTで使用した監査履歴変更の同期

Application Securityにおいて、［**監査(AUDIT)**］ページで管理され、OpenText ScanCentral DASTに発行される問題のことを、検出結果と呼びます。

Application SecurityでKafkaを設定すると、抑止された問題、優先度の上書き、分析タグの設定に関する監査履歴の変更を、OpenText ScanCentral DASTに同期できます。Application SecurityでKafkaを設定する方法については、「Kafka Streamの設定」を参照してください。

Application Securityで問題を監査するとき、バックグラウンドプロセスは、監査をKafkaトピックに発行するよう要求します。OpenText ScanCentral DASTは監査を処理し、抑止された問題、優先度の上書き、分析タグの設定を［スキャン(Scans)］ビューとスキャンの視覚化に反映します。

1.18. Fortify ScanCentral SASTの使用

Application SecurityがFortify ScanCentral SASTと通信するように設定されている場合は、［**ScanCentral**］ビューで［**SAST**］タブが有効になっています。［**SAST**］タブには、［**スキャン要求(Scan Requests)**］、［**センサ(Sensors)**］、［**コントローラ(Controller)**］、および［**センサプール(Sensor Pools)**］ページが表示されます。Application SecurityとScanCentral SAST間の接続を設定する方法については、「Fortify ScanCentral SASTとの統合を有効化」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。

1.18.1. Fortify ScanCentral SASTの許可

次の表に、Fortify ScanCentral SAST関連タスクの実行が許可されるApplication Securityの役割を記載します。

Note

静的コード分析プロセスを合理化するためにFortify ScanCentral SASTをインストール、設定、および使用する方法については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

役割	許可
表示のみ	• どのアプリケーションバージョンにも割り当てられていないジョブを除き、Fortify ScanCentral SASTデータを表示できます。 **制限:** • ユーザに表示されるスキャン要求は、そのユーザに割り当てられているアプリケーションバージョンのスキャン要求に限られます。 • ユーザに表示されるセンサプール割り当ては、そのユーザに割り当てられたアプリケーションバージョンのセンサプール割り当てに限られます。

役割	許可
管理者	• Fortify ScanCentral SASTデータを表示、ダウンロード、および管理できます。 • センサプールの変更を伴うすべてのタスクを実行できます。 • スキャン要求のキャンセル • センサプールにセンサとアプリケーションバージョンを割り当てることができます。 **制限:** • ユーザは、割り当てられたアプリケーションバージョンのスキャン要求のみをキャンセルできます。 • ユーザは、センサプールに割り当てられているアプリケーションバージョンのみを割り当てることができます。
セキュリティリード、マネージャ	• どのアプリケーションバージョンにも割り当てられていないジョブを除き、Fortify ScanCentral SASTデータを表示、ダウンロード、および管理できます。 **制限:** • ユーザは、割り当てられたアプリケーションバージョンのスキャン要求のみをキャンセルできます。 • ユーザは、センサプールに割り当てられているアプリケーションバージョンのみを割り当てることができます。

役割	許可
開発者	• どのアプリケーションバージョンにも割り当てられていないジョブを除き、Fortify ScanCentral SASTデータを表示できます。

参照情報

Application Securityの役割に関する許可情報の表示

1.18.2. Fortify ScanCentral SASTスキャン要求の詳細の表示

静的コード分析プロセスを合理化するためにFortify ScanCentral SASTをインストール、設定、および使用する方法については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

スキャン要求の詳細を表示するには:

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。

   ［**スキャン要求(Scan Requests)**］ページに、すべてのスキャン要求と各スキャンの詳細が一覧表示されます。

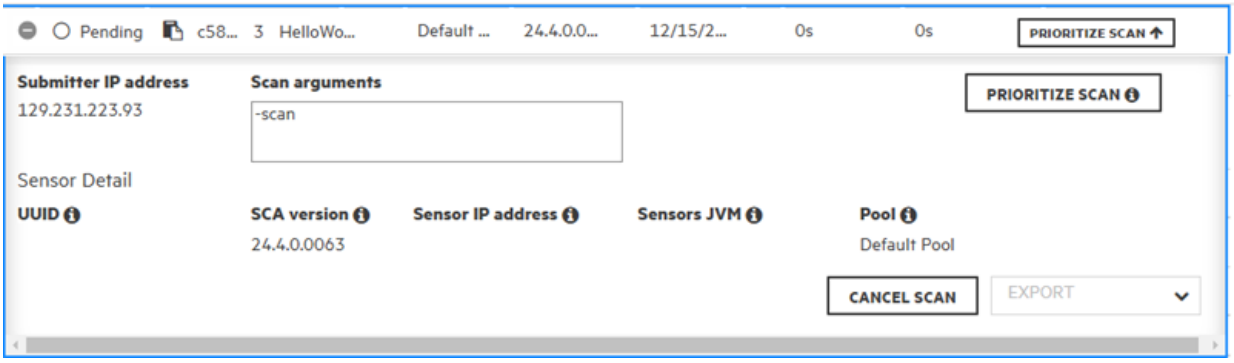
2. (オプション)表示されるスキャン要求をフィルタ処理するには、列見出しをクリックしてリストからフィルタ条件を選択するか、日付と時刻を選択するか、または選択した列タイプに応じて検索文字列を入力します。

   たとえば、結果をアプリケーション名でフィルタ処理するには、［**アプリケーション(Application)**］列見出しをクリックし、名前の最初の数文字を入力します。ジョブステータスでフィルタ処理するには、［**ステータス**］列見出しをクリックし、リストからステータスを選択します。

   適用されているフィルタをすべてクリアするには、［**リセット(RESET)**］をクリックします。

3. (オプション)表示を変更するには(ソートをクリアする、表示する列を選択するなど)、［**表示オプション(Display options)**］ボタンをクリックします。

4. 行を展開してスキャンの詳細を表示するには、［**スキャンの詳細を表示(Show scan details)**］ボタンをクリックします。



5. スキャン要求の詳細をエクスポートするには、［**エクスポート(EXPORT)**］リストから、［**FPR**］を選択してスキャンで検出されなかった脆弱性を含むFPRファイルをエ

クスポートするか、［**ログ(Log)**］を選択してスキャンのログファイルをエクスポートします。

6. 表示されたデータを更新するには、［**REFRESH**］をクリックします。

参照情報

Fortify ScanCentral SASTスキャン要求の優先順位付け

Fortify ScanCentral SASTスキャン要求のキャンセル

Fortify ScanCentral SASTセンサ情報の表示

Fortify ScanCentral SAST Controller情報の表示

1.18.3. Fortify ScanCentral SASTスキャン要求の優先順位付け

特定のセンサプールに複数のスキャン要求が割り当てられており、そのうちの1つを他のすべての要求より先に実行したい場合は、その要求を優先して、そのプールのジョブキューの先頭に移動します。

スキャン要求に優先順位を付けるには:

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。
2. ［**ステータス**］リストから［**保留中**］を選択します。

   ［**優先度(Priority)**］列内の数字は、スキャンジョブが実行される順序を示します。この数字が小さいほど、プール内でスキャンが早く実行されます。たとえば、優先度が-10のスキャン要求は、同じプール内の優先度が-2のスキャン要求より前に実行されます。
3. 最初に実行するスキャンの行で、［**優先スキャン(PRIORITIZE SCAN)**］をクリックします。

1.18.4. Fortify ScanCentral SASTスキャン要求のキャンセル

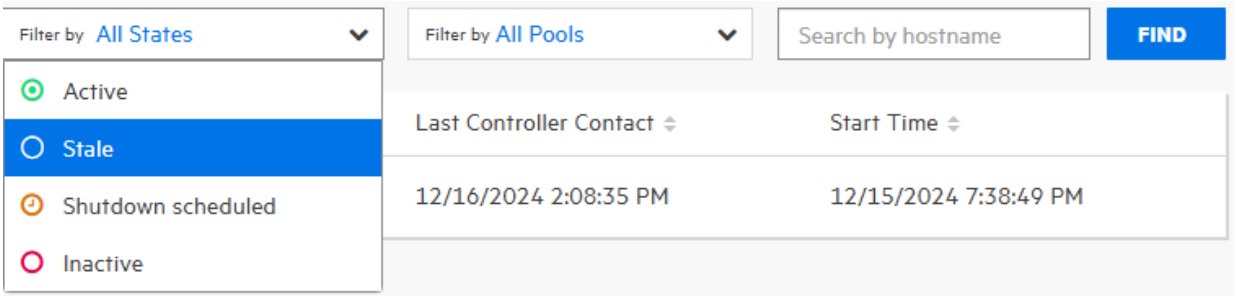
保留中のスキャン要求をキャンセルするには:

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。
2. ［ステータス］リストから［**保留中**］を選択します。
3. キャンセルする保留中のスキャン要求の行を展開します。
4. ［**スキャンをキャンセル(CANCEL SCAN)**］をクリックします。
5. スキャン要求のキャンセルを確認します。
6. ［**スキャン要求(Scan Requests)**］ページに表示されるデータを更新するには、［**更新(REFRESH)**］をクリックします。

1.18.5. Fortify ScanCentral SASTセンサ情報の表示

センサの状態とアクティビティに関する現在の情報を表示するには:

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。
2. ナビゲーションペインで、［**センサ(Sensors)**］を選択します。
3. 表示されるセンサを現在のセンサの状態に基づいてフィルタ処理するには、［**フィルタ条件(Filter by)**］状態リストから、［**アクティブ(Active)**］、［**非アクティブ(Inactive)**］、［**古い(Stale)**］、または［**シャットダウン予定(Shutdown scheduled)**］を選択します。



   デフォルトでは、あらゆる状態のすべてのセンサが表示されます。
4. 表示されるセンサをプールに基づいてフィルタ処理するには、［**フィルタ条件(Filter by)**］プールリストから、［**未割り当てのプール(Unassigned Pool)**］または名前付きプールのいずれかを選択します。

   デフォルトでは、あらゆるプールのすべてのセンサが表示されます。
5. センサの詳細を表示するには、そのセンサの行をクリックします。

参照情報

Fortify ScanCentral SASTスキャン要求のキャンセル

Fortify ScanCentral SASTスキャン要求の詳細の表示

1.18.6. Fortify ScanCentral SAST Controller情報の表示

コントローラの情報を表示するには:

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。
2. ナビゲーションペインで、［**コントローラ(Controller)**］を選択します。
3. 表示される各値の説明については、情報ボタンをクリックします。

参照情報

Fortify ScanCentral SASTスキャン要求の詳細の表示

Fortify ScanCentral SASTスキャン要求のキャンセル

Fortify ScanCentral SASTセンサ情報の表示

1.18.6.1. コントローラの停止

次の手順を使用して、コントローラをただちに停止できます。ただし、OpenTextでは、実行中のスキャンを保持するために、まずコントローラを保守モードにすることを強く推奨しています。

コントローラを停止するには、次の手順に従います。

1. コントローラがインストールされているコンピュータで、次のコマンドを入力します。

   ```
   cd <controller_install_dir>/tomcat/bin
   ```

2. 次のいずれかのコマンドを入力します。

   Windowsシステムの場合: `shutdown.bat`

   Linuxシステムの場合: `./shutdown.sh`

参照情報

コントローラを保守モードにする

1.18.6.2. コントローラを保守モードにする

Fortify ScanCentral SAST Controllerを突然シャットダウンすると、センサですでに開始されているスキャンが失われる可能性があります。このような問題を回避するには、Controllerを保守モードにします。その後、Controllerはクライアントからの新しいジョブ要求を受け付けず、キューに入っているジョブをセンサに割り当てません。

Controllerが保守モードに設定された後、センサは現在実行中のスキャンを完了しますが、新しいスキャンは受け付けません。Controllerを再度起動し実行すると、センサが再度使用可能になります。

Controllerを保守モードにする

1. 管理者としてサインインします。
2. ヘッダで［**ScanCentral**］を選択し、［**SAST**］ページを選択します。
3. ナビゲーションペインで、［**コントローラ(Controller)**］を選択します。
4. ［**START MAINTENANCE MODE**］をクリックします。

コントローラがApplication Securityからの保守要求を受信し、スキャンを実行しているセンサが1つでもある場合は、コントローラモードが［**ACTIVE**］から［**WAITING_FOR_JOB_COMPLETED**］に変わります。処理されているジョブがない場合、モードは［**ACTIVE**］から直接［**MAINTENANCE**］に変わります。この時点で、Controllerを安全にシャットダウンできます。

1.18.6.3. Fortify ScanCentral SASTセンサを安全にシャットダウンする

このトピックでは、センサをシャットダウン状態またはシャットダウン予定モードに移行する方法について説明します。

> **Important**
>
> コントローラが保守モードの場合(「コントローラを保守モードにする」を参照)、Application Securityユーザインタフェースからセンサをシャットダウンすることはできません。

アクティブなセンサをシャットダウンするには次の手順に従います。

1. 管理者としてサインインします。
2. ヘッダで［**ScanCentral**］を選択し、［**SAST**］ページを選択します。
3. ナビゲーションペインで、［**センサ(Sensors)**］を選択します。
4. 次のいずれかを実行します。
    - シャットダウンするセンサの行を展開し、［**SHUT DOWN**］をクリックします。
    - シャットダウンする1つ以上のセンサのチェックボックスをオンにして、［**SHUT DOWN**］をクリックします。

    > **Note**
    >
    > ［**SHUT DOWN**］ボタンが有効になっていない場合は、次の意味を持つ可能性があります。
    >
    > - センサはすでにシャットダウンされている
    > - コントローラが保守モード
    > - センサが非アクティブまたは無効

シャットダウンしたセンサがスキャンを実行している場合、そのセンサの［**State**］の値が［**Active**］から［**Shutdown scheduled**］に変わります。スキャンが完了すると、状態が［**Inactive**］に変わります。

1.18.6.4. コントローラを保守モードから削除する

コントローラを保守モードから削除するには:

1. 管理者としてサインインします。
2. ヘッダで［**ScanCentral**］を選択し、［**SAST**］ページを選択します。
3. ナビゲーションペインで、［**コントローラ(CONTROLLER)**］を選択します。
4. ［**END MAINTENANCE MODE**］をクリックします。

参照情報

コントローラを保守モードにする

コントローラの停止

1.18.7. Fortify ScanCentral SASTセンサプールについて

Application SecurityサーバがFortify ScanCentral SASTと統合されている場合、管理者、マネージャ、またはセキュリティリードは、任意の基準に基づいて「センサプール」と呼ばれるセンサのグループを作成できます。

センサプールを使用すると、スキャン要求に対して使用するセンサをきめ細かく制御できます。センサプールの使用例としては、以下が挙げられます。

- センサのコンピューティング能力(物理的なメモリサイズ)に基づいてプールを作成し、多くのメモリを必要とするスキャン要求をそれらのプールに割り当てます。
- 組織内のチームや事業部に基づいてプールを作成します。これにより、リソースが分散され、あるチームがすべてのセンサを消費したり、他のチームから送信されたスキャン要求をブロックしたりすることがなくなります。

スキャン要求がアプリケーションバージョンに関連付けられている場合、コントローラは使用可能なセンサプールをApplication Securityに照会します。スキャン要求がアプリケーションバージョンに関連付けられていない場合、Fortify ScanCentral SASTクライアントではスキャン要求に対して特定のセンサプールを要求できます。

Note

デフォルトでは、センサは非アクティブになってから168時間(7日)後に削除されます。このデフォルト値を変更する方法の詳細については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

定義済みのセンサプール

Application Securityには、未割り当てセンサプールとデフォルトプールという2つの定義済みセンサプールが用意されています。新しく登録されたセンサすべてが含まれる未割り当てセンサプールは、他のプールの共有センサプールとして機能します。センサプールを作成する際に［**未割り当てのセンサを使用(Use unassigned sensors)**］チェックボックスをオンにすると、デフォルトのセンサプールが未割り当てのセンサプールに含まれるセンサを使用するようになります。このセンサプールには、特定のセンサプールに割り当てられていないスキャン要求が含まれています。

参照情報

Fortify ScanCentral SASTセンサプールの作成

1.18.7.1. Fortify ScanCentral SASTセンサプールの作成

Application SecurityサーバがFortify ScanCentral SASTと統合されている場合は、センサプールを作成して、スキャン要求のターゲットにできます。

> **Note**
>
> 静的コード分析プロセスを合理化するためにFortify ScanCentral SASTをインストール、設定、および使用する方法については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

新しいセンサプールを作成するには、次の手順を実行します。

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。
2. ナビゲーションペインで、［**センサプール(Sensor Pools)**］を選択します。

   ［**センサプール(Sensor Pools)**］ページに、デフォルトプールとシステム上に作成されているその他すべてのセンサプールが一覧表示されます。

   > **Note**
   >
   > デフォルトプールには、センサプールに割り当てられていないすべてのアプリケーションバージョンが含まれます。

3. ［**+新しいプール(+ NEW POOL)**］をクリックします。

   ［**+新しいプール(+ NEW POOL)**］ボタンが無効になっている場合、これはApplication Securityがコントローラに接続されていないことを意味します。Fortify ScanCentral SASTの設定を確認してください(「Fortify ScanCentral SASTとの統合を有効化」を参照)。

4. ［**名前(Name)**］ボックスに、新しいプールの名前を入力します。

   プール名の最初の文字はUnicode英数字である必要があります(小文字または大文字のa～z、あるいは0～9)。

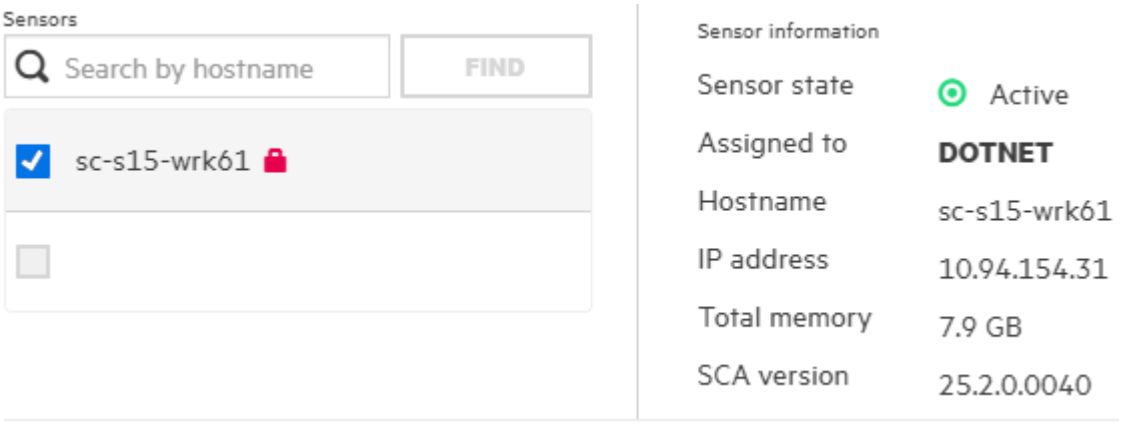
5. (オプション)［**Description**］ボックスに、新しいプールの説明(プロパティまたは目的)を入力します。

6. 割り当てられていないセンサを新しいプールで使用するには、［**Use unassigned sensors**］チェックボックスをオンにします。

> **Note**
>
> ［**Use unassigned sensors**］チェックボックスをオンにしても、これらのセンサは新しいプールに割り当てされません。代わりに、プールで、使用可能な未割り当てのセンサを利用できるようになります。センサは割り当てられていないままです。

> **Note**
>
> 1つのプールで最大10個のセンサを使用できます。

［**Sensors**］テーブルには、他のプールに割り当てられているセンサも含め、システム内のすべてのセンサのホスト名が一覧表示されますホスト名の横にある南京錠の記号は、センサがプールに割り当てられていることを示します。センサに関する情報を表示するには、そのセンサの行を選択します。［**センサ情報(Sensor information)**］エリアに、センサに関する基本情報(センサが現在割り当てられているプールなど)が一覧表示されます。



7. 特定のセンサを検索するには、［**ユーザ名で検索(Search by user name)**］ボックスにそのセンサのホスト名を入力し、［**検索(FIND)**］をクリックします。

8. 新しいプールに割り当てる各センサのチェックボックスをオンにします。

   すでに割り当てられているセンサのチェックボックスをオンにすると、そのセンサは現在割り当てられているプールから移動されます。

9. アプリケーションバージョンをプールに割り当てるには:

   1. ［**バージョン(Versions)**］で、［**追加(ADD)**］をクリックします。

2. ［**アプリケーション(APPLICATION)**］ペインで、このプールに割り当てるアプリケーションを選択します。

   ［**バージョン(VERSIONS)**］ペインに、選択したアプリケーションのすべてのアクティブなバージョンが一覧表示されます。

3. 選択したアプリケーションの非アクティブバージョンのすべてを一覧表示するには、［**非アクティブなバージョンの表示(Show inactive versions)**］チェックボックスをオンにします。

4. 一覧表示されているすべてのバージョンを新しいプールに割り当てるには、［**すべて選択**］チェックボックスをオンにします。または、アプリケーションバージョンのサブセットのみを割り当てるには、割り当てるバージョン名の横にあるチェックボックスをオンにします。

   ［**選択済みのバージョン(SELECTED VERSIONS)**］ペインに、選択したバージョンが一覧表示されます。

5. 別のアプリケーションのバージョンをこのプールに割り当てるには、ステップb～dを繰り返します。
6. ［**選択済みのバージョン(SELECTED VERSIONS)**］リストからアプリケーションバージョンを削除するには、アプリケーション名の横にある［**削除**］ボタン🗑をクリックします。
7. ［**DONE**］をクリックします。

10. ［**新しいプールの作成(CREATE NEW POOL)**］ダイアログボックスで、［**保存(SAVE)**］をクリックします。

［**Sensor Pools**］テーブルに新しいプールが一覧表示されます。

プールは、いつでも編集または削除できます。

参照情報

ScanCentralプールの削除

Fortify ScanCentral SASTセンサ情報の表示

1.18.7.2. プール間でのセンサの移動

Fortify ScanCentral SASTセンサをプール間で移動させるには:

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。
2. ナビゲーションペインで、［**センサプール(Sensor Pools)**］を選択します。
3. ［**センサプール(SENSOR POOLS)**］ページで、別のプールに割り当てるセンサを含むセンサプールを選択します。
4. ［**プールの編集(EDIT POOL)**］をクリックします。
5. ［**センサ(Sensors)**］で、別のプールに割り当てるセンサのチェックボックスをオフにします。
6. ［**保存(SAVE)**］をクリックします。
7. ［**センサプール(SENSOR POOLS)**］ページで、現在割り当てられていないセンサの割り当て先とするセンサプールを選択してから、「Fortify ScanCentral SASTセンサプールの作成」に記載されている手順に従って、現在割り当てられていないセンサを割り当てます。

参照情報

Fortify ScanCentral SASTセンサプールについて

1.18.7.3. Fortify ScanCentral SASTセンサプールの削除

センサプールを削除するには:

1. ヘッダで［**ScanCentral**］、［**SAST**］の順に選択します。
2. ナビゲーションペインで、［**センサプール(Sensor Pools)**］を選択します。

   ［**センサプール(Sensor Pools)**］に、既存のすべてのプールが一覧表示されます。テーブルの最後の列には、各プールの［**プールを削除(Delete Pool)**］ボタン🗑が表示されます。
3. 削除するプールに対応する［**プールを削除(Delete Pool)**］ボタン🗑をクリックします。

Application Securityによってリストからプールが削除され、削除されたプールに割り当てられているすべてのセンサが［**Unassigned Sensors**］タブに追加されます。

参照情報

Fortify ScanCentral SASTセンサ情報の表示

Fortify ScanCentral SASTセンサプールの作成

1.19. BIRTレポート

Application Securityレポートは、Business Intelligence and Reporting Technology(BIRT)システムに基づいて作成されます。BIRTは、Eclipseをベースにしたオープンソースのレポーティングシステムです。BIRTの詳細については、BIRTのWebサイトを参照してください。

次のレポートカテゴリのテンプレートを利用できます。

- アプリケーションレポート

  1つのアプリケーションバージョンについて要約するアプリケーション概要レポート。このレポートには、アプリケーションバージョンに関連する未解決の問題と、そのリスクプロファイルに関連する詳細情報が含まれています。また、ユーザアクティビティの概要も含まれます。

- 問題レポート

  問題レポートグループは、1つのアプリケーションバージョンにおける、脆弱性カテゴリそれぞれの有無を要約します。

- ポートフォリオレポート

  ポートフォリオレポートグループに含まれるレポートでは、複数のアプリケーションバージョンの問題のトレンドと指標を比較できます。

このセクションでは、次のトピックについて説明します。

1.19.1. BIRTライブラリ

BIRTライブラリを使用して、一般的に必要となる機能とレポート項目をカプセル化できます。その後、これらのライブラリを任意の数のBIRTレポートにインポートして再利用できます。また、ライブラリという概念により、レポート開発タスクを分割できるため、1人のレポート開発者がレポートごとにすべてのコンポーネントを作成する必要がなくなります。

BIRTレポートライブラリを使用するには、その前に、BIRT Report Designerを取得する必要があります。手順については、「BIRT Report Designerの取得」を参照してください。

ライブラリを参照するレポートは、レポートの実行中に自動的に更新されます。これは、この機能がないとビジネスや技術的な変更でレポートの再作業が必要になってしまう場合に便利です。たとえば、企業ロゴなどのライブラリコンポーネントが多数のレポート設計で使用されている場合、ライブラリに変更を加えるだけで、ロゴを変更できます。参照元のすべてのレポートには、変更が自動的に反映されます。

1.19.2. レポートライブラリのインポート

管理者は、Application Securityサーバにレポートライブラリを追加できます。

レポートライブラリを追加するには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**レポートライブラリ(Report Libraries)**］を選択します。

   ［**レポートライブラリ(Report Libraries)**］ページには、システム内のすべてのレポートライブラリが一覧表示されます。
3. ［**IMPORT**］をクリックします。
4. (オプション)［**説明(Description)**］ボックスに、インポートするライブラリの説明を入力します。
5. ［**参照(BROWSE)**］をクリックし、レポートライブラリリソースを見つけて選択します。
6. ［**保存(SAVE)**］をクリックします。

［**Report Libraries**］テーブルに追加されたライブラリが含まれます。

参照情報

Application Securityへの破壊的ライブラリおよびテンプレートのアップロードの防止

レポートを生成して表示する

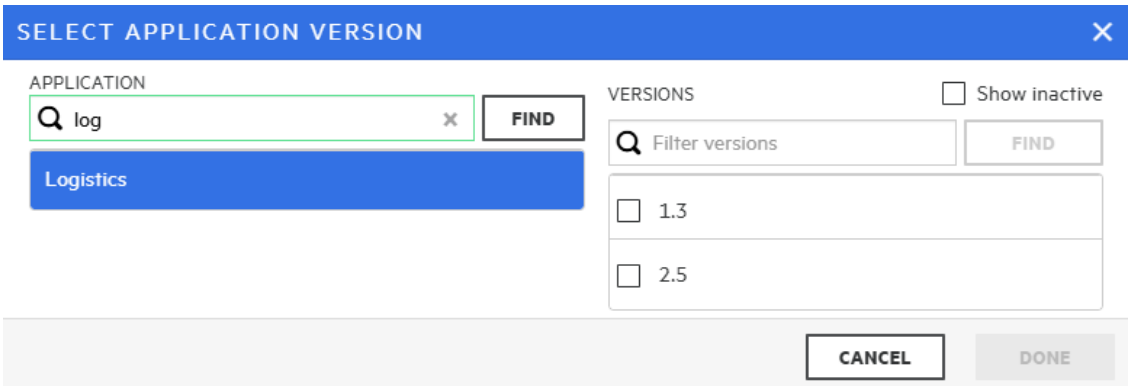
1.19.3. レポートを生成してダウンロードする

レポートを生成してダウンロードするには:

1. ヘッダで、［**レポート**］をクリックします。
2. ［**レポート**］ツールバーで、［**+新規レポート(+ NEW REPORT)**］をクリックします。
3. 使用するレポートテンプレートを選択します。

   ［**パラメータ(Parameters)**］ペインに、選択したテンプレートの設定フィールドが表示されます。
4. 必要なレポート設定(レポート名や出力形式など)を指定します。
5. レポートに含めるアプリケーションバージョンを指定するには:

   1. ［**アプリケーションバージョン(Application version)**］で、［**参照(BROWSE)**］をクリックします。
   2. ［**アプリケーションバージョンの選択(SELECT APPLICATION VERSION)**］ダイアログボックスの［**アプリケーション(APPLICATION)**］で、一覧表示されているアプリケーションのいずれか1つを選択します。または、［**アプリケーションのフィルタ処理(Filter applications)**］ボックスにアプリケーション名の一部またはすべてを入力して「**Enter**」キーを押し、フィルタ条件に一致したアプリケーション名を選択します。

      選択したアプリケーションのアクティブなバージョンが［**バージョン(VERSIONS)**］の下に表示されます。
   3. レポートに含めるバージョンのチェックボックスをオンにします。(1つだけ選択できます。)

      ポートフォリオレポートの場合、レポートに含める複数のアプリケーションバージョンを選択できます。

4. ［**DONE**］をクリックします。

6. ［**パラメータ(Parameters)**］ペインで、次の操作を行います。
   - レポートテンプレートの複数のエディションがある場合、［**オプション(Options)**］リストから、生成するエディションを選択します。
   - レポートタイプによっては、追加の設定が必要な場合や使用可能な場合があります。

7. ［**生成(GENERATE)**］をクリックします。

   Application Securityの［**レポート**］テーブルに、生成されたレポートが追加されます。このテーブルには、すべてのレポートがレポートテンプレートごとにグループ化されて一覧表示されます。レポートの生成が完了すると、［**ステータス**］フィールドに［**完了(Complete)**］の値が表示されます。

   > **Note**
   >
   > レポートの設定時に［**メモ**］ボックスに内容を入力した場合、［**メモ**］列にメモアイコンが表示されます。

8. レポートをダウンロードするには、レポート名をポイントして［**ダウンロード(Download)**］ボタン  をクリックします。

レポートをシステムから自動的に削除するまで保持する日数を指定する方法については、「ジョブスケジューラの設定」を参照してください。

参照情報

カスタマイズされたBIRTレポートのXLSX形式による生成とダウンロード

レポートテンプレートをダウンロードする

レポート定義のインポート

1.19.4. カスタマイズされたBIRTレポートのXLSX形式による生成とダウンロード

カスタマイズされたBIRTレポートをXLSX形式でダウンロードするには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**レポートテンプレート(Report Templates)**］を選択します。

   ［**レポート**］ページに、システム内の各レポートの名前、タイプ、および説明が一覧表示されます。
3. カスタマイズされた、目的のレポートテンプレートの行をクリックします。
4. ［**編集(EDIT)**］をクリックします。
5. ［**+パラメータの追加(+ ADD PARAMETER)**］をクリックします。
6. ［**新規パラメータの追加(ADD NEW PARAMETER)**］ダイアログボックスで、次の表で説明する情報を入力します。

フィールド	説明(Description)
名前(Name)	カスタマイズされたレポートテンプレートのパラメータに対応するパラメータの名前を入力します。
説明(Description)	(オプション)パラメータの説明を入力します。
識別子(Identifier)	`enableXlsxGeneration` と入力すると、カスタマイズされたレポートテンプレートにXLSX出力形式が追加されます。
データ型(Data Type)	［**ブール値(Boolean)**］を選択します。

7. ［**適用(APPLY)**］をクリックします。
8. ［**保存(SAVE)**］をクリックして変更を適用します。

9. ヘッダで、［**レポート**］をクリックします。
10. ［**+新規レポート(+ NEW REPORT)**］をクリックします。
11. ［**テンプレート(Templates)**］ペインで、すでに設定した、カスタマイズ済みのレポートテンプレートを選択します。
12. ［**レポート名(Report name)**］ボックスに、カスタマイズされたBIRTレポートの名前を入力します。
13. ［**出力形式(Output format)**］として［**XLSX**］を選択します。
14. ［**生成(GENERATE)**］をクリックします。

    Application Securityの［**レポート**］テーブルに、カスタマイズされたBIRTレポートが追加されます。レポートの生成が完了すると、［**ステータス**］フィールドに［**完了(Complete)**］と表示されます。
15. レポートをダウンロードするには、レポート名をポイントして［**ダウンロード(Download)**］ボタン  をクリックします。

1.19.5. BIRTレポートのカスタマイズ

BIRTレポートのカスタマイズは初心者レベルのアクティビティではありません。Eclipse BIRT Report Designerでのデータベースの操作と設計、SQLの構文、およびレポートの設計について理解している必要があります。OpenTextでは、レポートのカスタマイズを支援する、スペシャリストサービスを利用することを推奨しています。

Application SecurityBIRTレポートをカスタマイズするには、次の手順を実行します。

1. サポートされているバージョンのEclipse BIRT Report Designer (*Report Designer*) を取得します。

   Eclipse BIRT Report Designerのダウンロードについては、「BIRT Report Designerの取得」を参照してください。

2. Application Securityレポート定義をReport Designerにロードします。

   通常は、まずレポート定義をApplication Securityエクスポートし、そのレポート定義をReport Designerにアップロードします。Application Securityレポート定義をエクスポートする方法については、レポートテンプレートをダウンロードするを参照してください。

3. Application Securityデータベースの実行中のインスタンスにReport Designerを接続します。

   Report DesignerをApplication Securityデータベースに接続すると、BIRTレポートに追加したデータベースクエリをロードおよび検証できます。

4. Report Designerを使用して、レポート定義にレポート設計要素を追加し、それらの設計要素にデータベースクエリを追加します。

5. Application Securityのローカルインスタンスを使用して、カスタマイズされたBIRTレポートの操作をテストします。

6. カスタマイズされたレポート定義をApplication Securityにインポートします。

参照情報

レポート定義のインポート

1.19.6. BIRT Report Designerの取得

レポートをカスタマイズするには、サポートされているバージョンのEclipse BIRT Report Designer (Report Designer)を使用する必要があります。サポートされているバージョンの詳細については、『Application Securityソフトウェアのシステム要件』ドキュメントを参照してください。

Eclipse BIRT Report Designerをダウンロードするには、次の手順を実行します。

1. Webブラウザで、「Eclipse Downloads」ページに移動します。
2. ご使用のオペレーティングシステム用のReport DesignerフルEclipseインストールをダウンロードします。
3. Designerをインストールします。

   手順については、BIRTのWebページを参照してください。

1.19.7. レポートテンプレートをダウンロードする

Application Security レポートテンプレートを変更のためにダウンロードできます。

Caution

レポートテンプレートをダウンロード、変更、および再インポートすることは可能ですが、OpenTextではカスタマイズされたレポートテンプレートをサポートしていないことにご注意ください。

Note

「Options」という名前のパラメータをBIRTレポートで変更することはできません。

Application Security レポートテンプレートをダウンロードするには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**レポートテンプレート(Report Templates)**］を選択します。

   ［**レポート**］ページに、システム内の各レポートの名前、タイプ、および説明が一覧表示されます。
3. 目的のレポートの行をクリックします。
4. ［**テンプレートをダウンロード(DOWNLOAD TEMPLATE)**］をクリックします。

BIRT Report Designerを使用してダウンロードしたレポートを変更して、そのファイルをApplication Security に再インポートすることができます。それには、変更したレポートファイルの名前を変更してからインポートして、元のテンプレートが置き換えられないようにしてください。

カスタマイズされたBIRTレポートをApplication Securityにインポートする方法については、「レポート定義のインポート」を参照してください。

参照情報

レポートを生成して表示する

1.19.8. レポート定義のインポート

BIRTレポート定義は、レポートを生成するために必要な情報をApplication Securityレポートエンジンに提供します。これには、レポート名、レポートパラメータ、およびレポートテンプレートファイルの名前などの情報が含まれます。

BIRTを使用すると、レポート定義ファイルをApplication Securityにインポートできます。それには、Application Security BIRT定義ファイル(`.rptdesign` 拡張子が付いたファイル)が必要です。

> **Caution**
>
> BIRTレポートを開発するとき、指定したデータベース資格情報はレポート設計ファイルに安全に保存されていません。レポートをApplication Securityにデプロイする前に、レポートから資格情報を削除してください。

レポート定義をインポートするには、次の手順に従います。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで、［**テンプレート(Templates)**］を展開し、［**レポートテンプレート(Report Templates)**］を選択します。

   ［**レポート**］ページに、システム内の各レポートの名前、タイプ、および説明が一覧表示されます。
3. ［**IMPORT**］をクリックします。
4. ［**新しいレポートテンプレートのインポート(IMPORT NEW REPORT TEMPLATE)**］ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明(Description)
名前(Name)	テンプレートの名前を入力します。
説明(Description)	(オプション)テンプレートとその目的の説明を入力します。
Category	テンプレートのカテゴリを選択します。
Report Engine	［**BIRT**］が選択されたままにします。
Template	Application Security BIRT定義ファイル(`.rptdesign` 拡張子が付いたファイル)を参照して選択します。

5. (オプション)次のように、1つ以上のパラメータをレポート定義に追加します。
    1. ［**ADD PARAMETER**］をクリックします。
    2. ［**新規パラメータの追加(ADD NEW PARAMETER)**］ダイアログボックスで、次の表で説明する情報を入力します。

フィールド	説明(Description)
名前(Name)	インポートするテンプレート内のパラメータに対応するパラメータの名前を入力します。
説明(Description)	(オプション)パラメータの説明を入力します。
識別子(Identifier)	パラメータの固有の識別子を入力します。
データ型(Data Type)	このパラメータのデータ型を選択します。

6. ［**適用(APPLY)**］をクリックします。
7. ［**保存(SAVE)**］をクリックします。

参照情報

レポートを生成して表示する

1.20. 認証トークン

認証トークンは、ユーザ名とパスワードを明らかにせずに、ユーザがApplication Securityでのアクションを自動化し、スクリプト化されたプロセスを使用して操作を実行できるようにするための固有のキーです。

認証トークンは、そのトークンを作成したユーザのアカウントタイプ(管理者、セキュリティリード、マネージャ、開発者)の特権を継承します。`fortifyclient` が認証トークンを使用して操作を実行するとき、Application Securityが操作を、トークンを作成するために使用したアカウント名の下にログします。

このセクションでは、次のトピックについて説明します。

1.20.1. 認証トークンのタイプ

使用できるトークンタイプは複数あり、それぞれに、通常は時間制限がある少数のアクションのセットを対象とした異なる機能が備わっています。たとえば、AnalysisUploadTokenトークンは、ユーザにインタフェースへのサインインや結果の表示を許可しません。一般的なアクションには、分析結果のアップロードやレポートのダウンロードがあります。

次の表に、使用可能なトークンタイプの説明を記載します。

トークンタイプ	説明
AnalysisDownloadToken	マージされた結果ファイルのダウンロードを可能にします。
AnalysisUploadToken	Application Securityへの分析結果のアップロードと、アプリケーションの一覧表示を可能にします。
AutomationToken	発行元ユーザに許可されているREST APIエンドポイントの大半へのアクセスを可能にします。長期的な自動化での使用に適しています。 最大使用量: 無制限 最大有効期限: 365日 **Caution** このトークンが提供するアクセスと許容される最大有効期限を考えると、APIの誤用や意図しない使用のリスクを減らすため、特別な注意を払ってトークンのセキュリティを確保する必要があります。OpenTextでは、このトークンの計画的な使用を評価して、環境のリスクに対する許容度に基づき、その有効期限を制限することを強く推奨しています。
CIToken	Application Securityと継続的インテグレーションプラグインとの統合を可能にします。

トークンタイプ	説明
PurgeProjectVersionToken	すべてのアプリケーションバージョンのリストをプログラムで要求し、アプリケーションバージョンをパージすることを可能にします。
ReportFileTransferToken	通常は、認証されたセッション内での既存のレポートのダウンロードを可能にするために、/fileTokensエンドポイントを使用した自動化スクリプトでプログラムによって作成されます。
ReportToken	ユーザが次のことをできるようになる: • 保存されたレポートのリストを要求する • レポートIDに基づいて保存されたレポートを要求する • 保存されたレポートを削除する • 特定のアプリケーションバージョンに関連付けられた保存済みレポートのリストを返す • 新しいレポートを生成する
ScanCentralCtrlToken	Fortify ScanCentral SASTクライアントとの通信に使用されます。
ToolsConnectToken	OpenText Application Securityのツール(Fortify Audit WorkbenchおよびSecure Code Plugins)が、共同作業による分析結果の監査、修正、アップロードを目的としてApplication Securityに接続するために使用します。

トークンタイプ	説明
UnifiedLoginToken	REST APIの大半へのアクセスを可能にします。1日未満の短い実行自動化が対象です。

1.20.2. 認証トークンを生成する

認証トークンを生成するには、Application Securityの［**管理**］ビューを使用するか、コマンドラインからfortifyclientユーティリティを使用します。自分のトークンの詳細を見ることができるのは、自分だけです。Application Security管理者は、作成するトークンの有効期限を延長できますが、そのトークンの最大有効日数を超えることはできません。

Note

あらゆるタイプのトークンを作成できますが、所定のトークンに意図されたアクションを実行するために必要な許可が与えられていないユーザが、そのトークンを使用することはできません。

認証トークンを生成するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**トークン管理(Token Management)**］を選択します。
3. ［**新規(NEW)**］をクリックして、［**トークンの作成(Create Token)**］ダイアログボックスを開きます。
4. ［**トークンタイプ(Token Type)**］リストから、作成するトークンのタイプを選択します。

   使用可能なトークンタイプのリストについては、「認証トークンのタイプ」に記載されている表を参照してください。

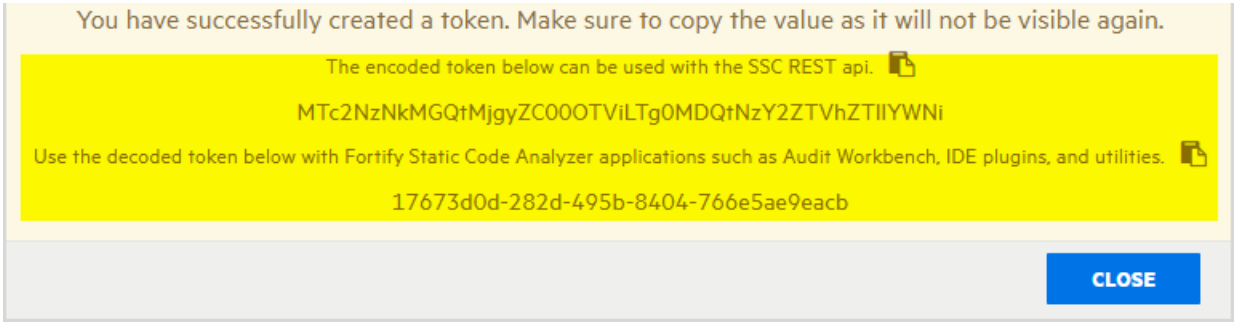
   ［**トークンの作成(Create Token)**］ダイアログボックスに、選択したトークンタイプの説明が表示されます。
5. ［**有効期限(Expiration)**］カレンダを使用して、トークンを期限切れにする日付を指定します。

   有効期限が、指定した日付の現在の時刻に設定されます。デフォルトでは、有効期限の値は、選択したトークンタイプに対して有効な最大日数に設定されます。これをそれより前の日付に設定すると、トークンの有効期限は短くなります。
6. ［**Description**］ボックスに、新しいトークンの使用目的の説明を入力します。
7. ［**保存(SAVE)**］をクリックします。

   ［**トークンの作成(Create Token)**］ダイアログボックスに、トークンが正常に作成されたことを通知するメッセージが表示されます。

8. エンコードまたはデコードされたトークン文字列をコピーし、保存します。

   これらのトークン値が再度表示されることはありません。



9. ［**閉じる(CLOSE)**］をクリックします。

［**トークン管理(Token Management)**］ページに、新しいトークンが一覧表示されます。

認証トークンは、ランタイム時に `<ssc_deploy_dir>/WEB-INF/internal/serviceContext.xml` で定義されます。

参照情報

コマンドラインから認証トークンを生成する

fortifyclient認証トークンでのDaysToLiveの指定

1.20.3. 認証トークンを編集する

あらゆるトークンの説明、およびマルチ使用トークンの有効期限を変更できます。管理者はマルチ使用トークンの有効期限も変更できますが、管理者がこのトークンに関する他の情報を確認することはできません。

認証トークンの説明を変更し、マルチ使用トークンの有効期限を変更するには:

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**トークン管理(Token Management)**］を選択します。

   ［**トークン管理(Token Management)**］ページには、ユーザが生成したすべてのトークンが一覧表示されます。
3. 編集するトークンを表示する行をクリックします。

   行は展開されて、トークンに関する詳細情報が表示されます。
4. ［**編集(EDIT)**］をクリックします。
5. 存続日数が1日を超えるトークンの有効期限を変更するには、［**有効期限(Expiration)**］カレンダをクリックし、別の有効期限を指定します。

   デフォルトでは、有効期限の値は、選択したトークンタイプに対して有効な最大日数に設定されます。これをそれより前の日付に設定すると、トークンの有効期限は短くなります。
6. ［**保存(SAVE)**］をクリックします。

参照情報

認証トークンを生成する

1.20.4. 認証トークンの削除

不要になった認証トークン、または使用できなくなった認証トークンを削除するには、次の手順を実行します。

1. ヘッダで、［**管理(Administration)**］を選択します。
2. ナビゲーションペインで［**ユーザ(Users)**］を展開し、［**トークン管理(Token Management)**］を選択します。

   ［**トークン管理(Token Management)**］ページには、ユーザが生成したすべてのトークンが一覧表示されます。
3. 削除するトークンのチェックボックスをオンにして、［**DELETE**］をクリックします。
4. ［**OK**］をクリックして、トークンを削除することを確認します。

参照情報

認証トークンを生成する

1.21. Fortify CLI (fcli)ドキュメント

Fortify CLI (fcli)は、統合されたコマンドラインインタフェースツールで、OpenText™ Application Security、OpenText SAST、OpenText DASTなど、さまざまなLiify製品と一貫したやり取りを行います。fcliは、各Liify製品に対して個別のツールやAPIを使用する代わりに、アプリケーションやバージョンの管理、スキャン結果のアップロード、レポートの生成、セキュリティワークフローの自動化などの一般的なタスクを実行するための単一の合理化されたインタフェースを提供します。

OpenText™ Application Securityユーザのために、fcliは、アプリケーションバージョンの作成と設定、アーティファクトとスキャンの管理、脆弱性のクエリ、およびCI/CDパイプラインへのFortifyの統合など、操作を簡素化します。Webインタフェースを手動で使用せずにスクリプトを使用して、OpenText™ Application Security機能と対話する必要がある自動化シナリオ、スクリプト作成、およびDevSecOpsワークフローに役立ちます。このツールはJSON出力をサポートし、他のシステムとの解析や統合を容易に行えるので、アプリケーションセキュリティテストおよび管理プロセスの拡張を考えるユーザにとって重要なユーティリティです。

fcliドキュメントへの参照を次に示します。

- リポジトリ: https://github.com/fortify/fcli
- リリース: https://github.com/fortify/fcli/releases
- 最新リリース: https://github.com/fortify/fcli/releases/tag/latest
- ドキュメントのホームページ: https://fortify.github.io/fcli/
- 最新のインストールと使用方法ガイド: https://fortify.github.io/fcli/latest/

1.22. fortifyclientユーティリティの使用

Important

`fortifyclient` 機能はバージョン26.2で非推奨となり、バージョン26.4で削除されます。

fortifyclientユーティリティを使用して、コマンドラインから認証トークンの生成、Application Securityとの間での安全なオブジェクトの転送、アプリケーションバージョンのアーティファクトのパージを行うことができます。

このセクションでは、次のトピックについて説明します。

1.22.1. fortifyclientを使用するための準備

fortifyclientユーティリティは、`<ssc_distribution_dir>/Tools/fortifyclient/bin/` にあります。

fortifyclientを使用するには、次の情報が必要です。

- すべてのコマンドには、Application SecurityのURLが必要です。「アプリケーションの設定オプション」で「host.url」を参照してください。
- トークンを生成するコマンドと、既存のトークンを一覧表示するコマンドには、Application Securityユーザアカウントの資格情報が必要です。
- トークンを無効にするコマンドには、ユーザアカウント資格情報または認証トークンのいずれかを使用する必要があります。
- その他すべてのコマンドには、認証トークンが必要です。

  fortifyclientが認証トークンを使用して操作を実行すると、Application Securityはその操作を、トークンを作成するために使用したアカウント名でログに記録します。

参照情報

Application Securityファイルのダウンロードと解凍

1.22.1.1. fortifyclient HTTPタイムアウト

fortifyclientに対して、接続、読み取り、および書き込みのHTTPタイムアウトを設定できます。どのタイムアウトについても、有効な範囲は `1` から `2147483` 秒です。次の表に、HTTPタイムアウトを変更するために使用できる環境変数を示します。

環境変数	説明(Description)
`FORTIFYCLIENT_CONNECT_TIMEOUT_SEC`	クライアントが接続を確立するためのHTTP接続タイムアウトを秒単位で指定します。 デフォルト値は `10` 秒です。
`FORTIFYCLIENT_READ_TIMEOUT_SEC`	クライアントが応答を受信するためのHTTP読み込みタイムアウトを秒単位で指定します。 デフォルト値は `600` 秒です。
`FORTIFYCLIENT_WRITE_TIMEOUT_SEC`	クライアントが要求本文を配信するためのHTTP書き込みタイムアウトを秒単位で指定します。 デフォルト値は `60` 秒です。

1.22.2. fortifyclientのコマンドとオプションを一覧表示する

fortifyclientのコマンドとオプションを一覧表示するには:

1. コマンドプロンプトで、次のコマンドを入力します。

   `cd <ssc_distribution_dir>/Tools/fortifyclient/bin/` .

2. 使用可能なすべてのコマンドを一覧表示するには、 `fortifyclient -h` と入力します。
3. 特定のコマンドのすべてのオプションを一覧表示するには、 `fortifyclient -h <command>` と入力します。

fortifyclientユーティリティのコマンド名とオプション名では、大文字と小文字が区別されます。

1.22.3. コマンドラインから認証トークンを生成する

コマンドラインから認証トークンを生成するには、fortifyclientユーティリティを使用します。既存の Application Security ユーザアカウントの資格情報を使用して、認証トークンを作成できます。認証トークンは、そのトークンを作成したユーザのアカウントタイプ(管理者、セキュリティリード、マネージャ、開発者)に与えられた許可を継承します。

次の例では、分析結果をApplication Securityにアップロードするための認証トークンを生成します。

```
fortifyclient token -url <host.url> -gettoken
AnalysisUploadToken -user Developer1 -password <password>
```

参照情報

認証トークンのタイプ

認証トークンを生成する

1.22.3.1. トークンの有効期限切れになるまでの日数を指定する

認証トークンを作成する際は、 `-daysToLive` オプションを使用して、有効期限切れになるまでの日数を指定できます。

次のコマンド例では、2日後に期限切れになる分析アップロードトークンを生成します。

```
fortifyclient token -url <host.url> -gettoken
AnalysisUploadToken -user Developer1 -password <password> -
daysToLive 2
```

`daysToLive` パラメータは大文字と小文字を区別するため、上記の例に示すとおりに入力する必要があります。

参照情報

コマンドラインから認証トークンを生成する

1.22.4. 認証トークンを一覧表示する

Application Security管理者はfortifyclientを使用して、すべてのApplication Securityユーザアカウントの既存のすべての認証トークンを一覧表示できます。fortifyclientユーティリティでは、Application Securityアカウント名またはアカウント特権レベルによるトークンリストのフィルタ処理をサポートしていません。

次のコマンド例は、すべてのユーザアカウントの既存の認証トークンを一覧表示します。

```
fortifyclient listtokens -url <host.url> -user Admin1 -password
<password>
```

fortifyclientユーティリティは、すべての認証トークンのトークンID、所有者、作成日、有効期限を含むリストを返します。

Note

このユーティリティでは、セッショントークンは一覧表示されません。セッショントークンとは、Application Securityが自動的に作成して、セッションに関連付けるトークンを指します。

1.22.5. トークンの無効化

既存のトークンを無効化するには、Application Securityユーザインタフェースでトークンを削除するか、`invalidatetoken`コマンドを実行します。特定のユーザアカウントのすべてのトークンを無効化することも、トークンIDまたはトークン値を指定して単一のトークンを無効化することもできます。

次のコマンド例では、特定のユーザアカウントのすべての認証トークンを削除します。

```
fortifyclient invalidatetoken -url <host.url> -invalidateForUser
-user Developer1 -password <password>
```

次のコマンド例では、トークンIDを指定して、特定のユーザアカウントの既存の認証トークンを削除します。

```
fortifyclient invalidatetoken -url <host.url> -invalidateByID
<token_ID> -user Developer2 -password <password>
```

次のコマンド例では、トークン値を指定して、既存の認証トークンを無効化します。

```
fortifyclient invalidatetoken -url <host.url> -invalidate
<token>
```

参照情報

認証トークンを一覧表示する

認証トークンの削除

1.22.6. アプリケーションバージョンの一覧表示

fortifyclientを使用して、特定の認証トークンを作成するために使用されたアカウントがアクセス可能なアプリケーションバージョンを一覧表示できます。

> **Note**
>
> 管理者は、すべてのアプリケーションバージョンを表示できます。セキュリティリードは、自分が作成したアプリケーションバージョン、またはアクセス権が付与されているアプリケーションバージョンを表示できます。マネージャおよび開発者は、アクセス権が付与されているアプリケーションバージョンを表示できます。

このセクションのコマンドを実行するには、まずアップロード認証トークンを取得する必要があります。「コマンドラインから認証トークンを生成する」を参照してください。

次のコマンド例は、特定のユーザアカウントのアプリケーションバージョン識別子、アプリケーション名、およびアプリケーションバージョンを一覧表示します。

```
fortifyclient listApplicationVersions -url <host.url> -authtoken
<token>
```

fortifyclientユーティリティは、トークンを作成したユーザアカウントがアクセス可能なすべてのアプリケーションバージョンのアプリケーションバージョンID、アプリケーション名、およびバージョンを一覧表示します。

次も参照

コマンドラインから認証トークンを生成する

1.22.7. Uploading FPR files

ユーザは、FPR形式のアプリケーション分析結果ファイルを定期的にApplication Securityにアップロードします。コマンドラインからこれを行うには、認証トークンが必要です。FPRファイルをアップロードするには、アプリケーションバージョン識別子、またはアプリケーションバージョン名とバージョンを指定します。

Note

When naming an FPR, only a limited set of characters is supported. Ensure to use supported characters and avoid unsupported characters in file names.

Supported characters

- Uppercase and lowercase letters (`A–Z` , `a–z`)
- Numbers (`0–9`)
- Periods (`.`)
- Dashes (`-`)
- Underscores (`_`)

Unsupported characters

- Special character `#`

If a special character is used, it is automatically replaced with an underscore (`_`). This replacement does not change the meaning or integrity of the FPR.

Examples

Upload an FPR file to Application Security using an application version identifier:

```
fortifyclient uploadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -applicationVersionID <id>
```

Upload an FPR file to Application Security using an application name and version:

```
fortifyclient uploadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -application MyApp -applicationVersion 1.0
```

See Also

Generating an authentication token from the command line

Listing application versions

1.22.8. FPRファイルのダウンロード

fortifyclientを使用してFPRファイルをダウンロードするには、アプリケーションバージョン識別子、またはアプリケーションバージョン名とバージョンを指定します。

例

アプリケーションバージョン識別子を使用して、Application SecurityからFPRファイルをダウンロードします。

```
fortifyclient downloadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -applicationVersionID <id>
```

アプリケーション名とバージョンを使用して、Application SecurityからFPRファイルをダウンロードします。

```
fortifyclient downloadFPR -url <host.url> -authtoken <token> -file MyScan.fpr -application MyApp -applicationVersion 1.0
```

参照情報

コマンドラインから認証トークンを生成する

アプリケーションバージョンの一覧表示

1.22.9. アプリケーションバージョンのアーティファクトのパージ

指定した日付より前にスキャンされたアプリケーションバージョンに関連付けられているすべてのアーティファクトをパージできます。

次のコマンド例では、MMMM dd, yyyyより前にスキャンされたアプリケーションバージョンからすべてのアーティファクトをパージします。

```
fortifyclient purgeApplicationVersion -url <host.url> -authtoken <token> -application MyApp -applicationVersion 1.0 -scanDate MMddyyyy
```

アプリケーションバージョン識別子を使用してアプリケーションバージョンを指定することもできます。

参照情報

コマンドラインから認証トークンを生成する

アプリケーションバージョンの一覧表示

1.22.10. コンテンツバンドルのインポート

OpenTextは、1つ以上の問題テンプレートまたはレポート定義を含むセキュリティコンテンツバンドルを(ZIPファイルとして)定期的に提供します。

次のコマンド例では、セキュリティコンテンツバンドルをApplication Securityにインポートします。

```
fortifyclient import -url <host.url> -authtoken <token> -bundle
bundle.zip
```

1.22.11. 監査添付ファイルをダウンロードする

次のコマンド例では、Application Securityから監査添付ファイルをダウンロードします。

```
fortifyclient downloadAttachment -url <host.url> -authtoken
<token> -file xyz.png -attachmentId <attachment_id>
```

1.23. バグトラッカプラグインの作成

Application Securityは、外部バグトラッキングアプリケーションとの統合をサポートしています。これにより、ユーザは問題を監査する時にバグをログに記録できます。提供時点では、システムはJira、ALM、およびAzure DevOps Serverと統合できます。サポートされている特定のバージョンについては、「*Application Security Softwareのシステム要件*」のドキュメントを参照してください。貴社が別のバグトラッキングシステムを使用している場合は、それを対象とする新しいプラグインを作成できます。このセクションでは、カスタムのバグトラッカプラグインを作成および展開する方法について説明します。

Note

このヘルプおよびApplication Securityユーザインタフェースでは、「バグ」と「欠陥」という用語は同じ意味で使用されます。

Important

独自のプラグインを作成する前に、提供されているプラグインサンプルを調査することを強く推奨します。サンプルは次のディレクトリにあります。

<ssc_distribution_dir>/Samples/*<bugtracker_plugin_name>*/

このセクションでは、次のトピックについて説明します。

1.23.1. 使用例

Application Securityの管理者として、「バグトラッカーの統合について」の説明に従って、特定のアプリケーションバージョンで使用する外部バグトラッキングシステムを設定できます。Application Securityでは、選択したバグトラッカーに必要な環境設定パラメータフィールドが表示され、これらの値をアプリケーションバージョンごとに1回だけ設定します。バグトラッカー環境設定パラメータの値の有効性をテストしたら(オプション)、ユーザがアプリケーションバージョンの欠陥をログに記録するたびに、その値を使用するデータベースに保存します。

アプリケーションバージョンに対するバグを送信するユーザは、バグトラッカーにログオンし、バグトラッカーでバグパラメータに提供される必須のフィールドに値を入力します。必須のパラメータ情報には、サマリ、説明、重大度レベル、コンポーネントなどの項目を含めることができます。

プラグインフレームワークでは、バグトラッキングパラメータの動的な側面がサポートされています。ユーザがパラメータ値を変更すると、プラグインで変更が検出され、新しいリスト選択で更新されたバグパラメータのリストが使用可能になります。

バグが提出されると、問題に対するバグIDがデータベースに保存されます。その後、ユーザはプラグインで提供される外部バグリンクを使用してバグにアクセスできます。

バグを報告するユーザから受諾された資格情報はサーバセッションに保存され、同じセッション中に後で送信されたプリケーションに対するバグで再利用されます。

1.23.2. コンポーネントのセットアップ

バグトラッカプラグインは、希望するIDEを使用して記述する、独立したコンポーネントにすることができます。

次の依存関係でバグトラッカプラグインを設定します。

- プラグインは、`fortify-public-<version>.jar` で定義および配布されるパブリックAPIを実装する必要があります(必須)。
- Apache Commons Logging (オプション)
- Apache Commons Lang (オプション)

希望するビルドシステムを使用して、配布可能コンポーネントをビルドできます。

Note

プラグインにJavaEEパッケージへの依存関係がある場合、プラグイン開発者は、必要なJavaEE JARファイルをプラグイン独自のライブラリパスにバンドルする必要があります。また、これらのパッケージがJava™ Runtime Environmentから利用できる状況に依存しないでください。javaEEモジュールはJava 9では非推奨となりました。このようなパッケージには、JAXB APIおよび実装、javax.activation、javax.annotation、javax.transaction、javax.xml.ws、およびCORBA関連のパッケージが含まれます。

1.23.3. 実装

プラグインフレームワークを使用するApplication Securityバージョンでは、すべてのプラグインが `com.fortify.pub.bugtracker.plugin.BatchBugTrackerPlugin` インタフェースを実装している必要があります。今後のリリースで利用可能になる後方互換性サポートを利用できるよう、実装クラスで `com.fortify.pub.bugtracker.plugin.AbstractBatchBugTrackerPlugin` を拡張することを強く推奨します。

以下に示すBatchBugTrackerPluginインタフェースは、BatchBugTrackerPluginの拡張機能です。

```
 public interface BatchBugTrackerPlugin extends BugTrackerPlugin
{ public void addCommentToBug (Bug bug, java.lang.String
comment, UserAuthenticationStore credentials); public Bug
fileMultiIssueBug (MultiIssueBugSubmission bug,
UserAuthenticationStore credentials); public
java.util.List<BugParam> getBatchBugParameters
(UserAuthenticationStore credentials); public boolean
isBugClosed (Bug bug, UserAuthenticationStore credentials);
public boolean isBugClosedAndCanReOpen (Bug bug,
UserAuthenticationStore credentials); public boolean isBugOpen
(Bug bug, UserAuthenticationStore credentials); public
java.util.List<BugParam> onBatchBugParameterChange
(java.lang.String changedParamIdentifier,
java.util.List<BugParam> currentValues, UserAuthenticationStore
credentials); public void reOpenBug (Bug bug, java.lang.String
comment, UserAuthenticationStore credentials); }
```

以下に示すBugTrackerPluginインタフェースは、BatchBugTrackerPluginのベースインタフェースです(後方互換性を確保するために別個に管理)。

```
 public interface BugTrackerPlugin { public boolean
requiresAuthentication(); public List<BugTrackerConfig>
getConfiguration(); public void setConfiguration(Map<String,
String> configuration); public void
testConfiguration(UserAuthenticationStore credentials); public
String getShortDisplayName(); public String
getLongDisplayName(); public List<BugParam>
getBugParameters(IssueDetail issueDetail,
UserAuthenticationStore credentials); public List<BugParam>
onParameterChange(IssueDetail issueDetail, String
changedParamIdentifier, List<BugParam> currentValues,
UserAuthenticationStore credentials); public Bug
fileBug(BugSubmission bug, UserAuthenticationStore credentials);
public void validateCredentials(UserAuthenticationStore
credentials); public Bug fetchBugDetails(String bugId,
UserAuthenticationStorecredentials); public String
getBugDeepLink(String bugId); }
```

1.23.4. プラグインメソッドとメソッドコール

次の表は、プラグインで使用するメソッドとコールを一覧表示しています。

メソッドまたはコール	説明
requiresAuthentication	このメソッドでは、バグトラッキング操作のためにフレームワークがユーザに資格情報を要求する必要がある場合に `true` が返されます。 資格情報ストアなどからプラグインが別のメカニズムを使用して資格情報を取得する場合や、プラグインがリアルタイムではなく非同期でバグトラッキングシステムと対話する場合を除き、 `true` が返されます。メソッドが `false` を返した場合、システムはプラグインメソッドのすべての `UserAuthenticationStore` パラメータについてnullを渡します。
getBatchBugParameters	プラグインフレームワークによって、プラグインがバッチバグを送信するために必要なバグパラメータのリストを取得するために使用されます。デフォルト値またはnull値を指定します。このメソッドが呼び出される前に、プラグインインスタンスで `BugTrackerPlugin.setConfiguration(java.util.Map)` メソッドが呼び出されます。パラメータ選択リストとデフォルトは、実装がバグトラッキングシステムで有効な選択肢のリストを決定することで、動的に行えます。

メソッドまたはコール	説明
getConfiguration	プラグインフレームワークは、このメソッドを使用して、プラグイン設定中にユーザに提示される質問に関するメタデータを取得します。戻り値は、設定項目に関する必要な情報を提供するBugTrackerConfigオブジェクトのリストです。各項目は、ユーザインタフェースのテキストボックスに対応しています。各項目の値フィールドは、テキストボックスのデフォルト値を指定します。
setConfiguration (call)	アプリケーションバージョンのバグトラッキングシステムを選択し、設定をデータベースに保存した後、すべてのプラグインとの今後のやり取りの前に `setConfiguration` コールが行われます。
testConfiguration (call)	プラグインフレームワークは、`testConfiguration` コールを使用して以前に設定された設定をテストするために `setConfiguration` コールを使用します。このメソッドは、設定された設定詳細を使用してバグトラッキングシステムをヒットし、可能な限り検証します。このプラグインが認証を必要と宣言した場合、ユーザ資格情報はユーザからフェッチされます。

メソッドまたはコール	説明
getShortDisplayName	`getShortDisplayName` メソッドは、プラグインの短い表示名を返します。この文字列は、利用可能なバグトラッカプラグインのリストに入力されます。 **Important** Application Securityが提供するサンプルバグトラッカーコードをカスタマイズしても、同じプラグインクラス名を使用する場合は、プラグインの短い表示名を変更しないでください。(整合性を保つため、長い表示名も変更しないようにしてください。)メイン実装クラスの名前を変更する場合は、プラグインの表示名も変更する必要があります。

メソッドまたはコール	説明
getLongDisplayName	`getLongDisplayName` メソッドは、設定から取得したバグトラッキングシステムの追加IDを含む値を返します。このメソッドは、たとえば、ユーザにバグトラッキングシステムの資格情報を入力するように求めるメッセージが表示される場合に使用されます。 **Important** Application Securityが提供するサンプルバグトラッカーコードをカスタマイズしても、同じプラグインクラス名を使用する場合は、プラグインの短い表示名を変更しないでください。(整合性を保つため、長い表示名も変更しないようにしてください。)メイン実装クラスの名前を変更する場合は、プラグインの表示名も変更する必要があります。

メソッドまたはコール	説明
getBugParameters	`getBugParameters` メソッドは、ユーザに提示するバグパラメータに関するメタデータを返します。Application Securityは、次の3つのバグパラメータタイプをサポートしています。 • BugParamTextはテキストボックスに変換されます。 • BugParamTextAreaは複数行のテキストボックスに変換され、通常はバグの説明に使用されます。 • BugParamChoiceはリストに変換されます。 • `issueDetail` オブジェクトには、ユーザがバグをログに記録しようとしている問題の詳細が含まれます。デフォルトでは、説明や概要など、このオブジェクトから抽出可能ないくつかのバグパラメータが設定されます。pluginHelperで保護されたメンバーには、提案されたデフォルトのバグ説明を作成するヘルパーメソッドがあります。(「Plugin Helper」を参照してください)。

メソッドまたはコール	説明

onBatchBugParameterChange	ユーザがユーザインタフェースでパラメータの値を変更した場合、このメソッドは更新された選択リストを取得して、他のバッチバグパラメータを探します。このメソッドが呼び出される前に、プラグインインスタンスで `BugTrackerPlugin.setConfiguration(Map)` メソッドが呼び出されます。プラグインバグパラメータの `BugParamChoice.getHasDependentParams()` 属性が `true` に設定されている場合、ユーザインタフェース層でパラメータ値が変更されるたびにこのメソッドが呼び出されます。
	
	推奨事項:
	
	• 依存パラメータを持つ各バグパラメータに対して実行します。
	• パラメータ値がnullに変わる場合(選択なし)は、忘れずに処理してください。
	• 選択が変わる場合は、戻りリストのパラメータ値をnullに設定することを忘れないでください。
	• 新しいパラメータを追加する前に、パラメータがすでに戻りリストに存在していないか確認してください。
	• 変更がない場合はnullを返します
	
	• 次のいずれかの方法を使用します。
	  ◦ `currentValues` パラメータを変更して返します。
	  ◦ 保持されている生のパラメータから戻り値を構築します。返す前に、値と選択リストを設定します。

メソッドまたはコール	説明

onParameterChange	プラグインフレームワークは、`onParameterChange`とマークされたバグパラメータの値(BugParamChoiceクラスjavadocを参照)が変更されるたびに`hasDependentParams`メソッドを呼び出します。このメソッドはアクションを実行し、表示するバグパラメータの新しいリストを返します。
	
	次のガイドラインに注意してください。
	
	• 依存パラメータを持つ各バグパラメータに対して実行します。
	• パラメータ値がnullに変わるとき(選択なし)は、忘れずに処理してください。
	• 選択が変わる場合は、戻りリストのパラメータ値をnullに設定することを忘れないでください。
	• 新しいパラメータを追加する前に、戻りリストをチェックして、そのパラメータがすでに含まれていないことを確認してください。
	• 変更がない場合はnullを返します。
	• 次のいずれかの方法を使用します。
	  ◦ `currentValues`パラメータを変更して返します。
	  ◦ 保持されている生のパラメータから戻り値を構築します。返す前に、値と選択リストを設定します。

メソッドまたはコール	説明
fileBug	このメソッドは、外部バグトラッキングシステムにバグを報告します。渡された `BugSubmission` オブジェクトは、すべてのバグ詳細を包含します。 `bug.getIssueDetail()` オブジェクトと `bug.getParams()` オブジェクトを正しく区別してください。`bug.getIssueDetail()` オブジェクトは問題の詳細を返し、 `bug.getParams()` オブジェクトはユーザが提供するバグパラメータ値を返します。 ユーザが編集可能なバグパラメータとしてBug Descriptionを追加した場合は、`bug.getParams()` オブジェクトからではなく、 `bug.getIssueDetail()` オブジェクトからバグ説明をフェッチします。fileBugオブジェクトの戻り値はbugIdである必要があります。bugIdを使用すると、 `fetchBug` メソッドでバグをフェッチし、 `getBugDeepLink` メソッドでディープリンクを作成できます。 リポジトリにアクセスできる場合、B `ugSubmission.getIssueDetail()` 、つまり `getLastBuildWithoutIssue()` 、`getDetectedInBuild()` 、および `getFileName()` は、変更セットの検出を実行します。

メソッドまたはコール	説明
fileMultiIssueBug	バグトラッキングシステムに関する複数の問題を含むバグをファイルします。このメソッドが呼び出される前に、プラグインインスタンスで `BugTrackerPlugin.setConfiguration(Map)` メソッドが呼び出されます。 推奨事項: • Application Securityは、`MultiIssueBugSubmission.getIssueDetails()` を使用して取得した概要と説明を提供します。ユーザは、これらの値を指定しません。概要と説明をバグパラメータとして追加した場合は、ユーザが指定した値を取得するために `bug.getParams()` を使用します。 • リポジトリにアクセスできる場合は、`getLastBuildWithoutIssue()` の `getDetectedInBuild()` 、`getFileName()` 、および `MultiIssueBugSubmission.getIssueDetails()` フィールドを使用して変更セットの検出を実行します。
fetchBug	このメソッドは、現在のバグステータスをフェッチします。
getBugDeepLink	このメソッドは、バグへのディープリンクを作成します。バグトラッカがディープリンクをサポートしていない場合は、nullを返します。

各パラメータおよび他のサポートクラスの詳細については、パブリックAPI javadocを参照してください。

1.23.5. Plugin Helper

指定されたクラス**AbstractBatchBugTrackerPlugin**から拡張されたバグトラッカプラグインクラスの場合は、保護されたメンバー**BugTrackerPluginHelper**が利用可能です。このヘルパーオブジェクトを使用して、パラメータの検索、デフォルト値のロードなど、頻繁に使用するプラグイン操作を実行できます。詳細については、javadocを参照してください。プラグインサンプルでの使用状況も確認します。

1.23.6. エラー処理

エラー処理とレポーティングを適正に行うには、すべてのプラグインメソッドで次の方法を使用して例外をスローします。

- ユーザが対処できるエラーには `com.fortify.pub.bugtracker.support.BugTrackerException` をスローします。たとえば無効な設定、バグトラッキングシステムから生じるエラー、バグトラッキングシステムの障害などです。この例外を含むメッセージはユーザに送られるため、ユーザに分かりやすいことが求められます。
- バグトラッキングシステムに渡された資格情報が正しくない場合に限り、`com.fortify.pub.bugtracker.support.BugTrackerAuthenticationException` をスローします。この例外の結果として、キャッシュされたバグトラッカー資格情報がクリアされます。
- 内部例外の場合は `RuntimeException` またはそのサブクラスをスローします。

1.23.7. ほぼステートレス

Application Securityからプラグインフレームワークのバグトラッカに送信する(およびバグトラッカプロバイダと通信する必要がある)すべてのトップレベル要求で、`setConfiguration`が呼び出されます。プラグイン内に保存する必要がある状態は、このメソッドが提供する設定値のみです。設定値は、バグトラッカプラグインの内部処理中に使用できます。この時点から、すべてのプラグイン呼び出しはステートレスであることが求められます。

プラグインインスタンスでは、状態を維持したり、接続を開いたままにしたり、前の呼び出しで開いた接続を使用したりすることはできません。Application Securityでは、プラグイン操作全体でプラグインインスタンスをキャッシュしたり再利用したりしません。呼び出しごとに新しい状態を開き、メソッドが終了する前にクリーンアップする必要があります。

1.23.8. バグトラッカプラグインのデバッグ

プラグインはApache Commonsのログ記録をサポートしています。結果のログは、`ssc_plugins.log` ファイルに追加されます。このファイルは `<fortify.home>/<app_context>/logs/` ディレクトリにあります。すべての例外は自動的にログに記録されます。IDE内のプラグインプロジェクトからTomcatサーバに接続して、プラグインのリモートデバッグを実行することもできます。

1.23.9. カスタマイズしたバグトラッカープラグインの展開

カスタマイズしたバグトラッカープラグインを展開するには、プラグインクラスとその依存クラスすべてを含むJARファイルをビルドします。

次のスクリプト例は、バグトラッカープラグインをGradleでビルドするものです。

```
apply plugin: 'java'sourceCompatibility = '1.8'
targetCompatibility = '1.8' dependencies { compile fileTree(dir:
'lib', include: '*.jar') } jar.enabled = false // There is no
need to generate a default non-osgi jar during build. clean {
delete "${projectDir}/dist" } task pluginJar(type: Jar) {
baseName "com.fortify.BugTrackerPluginAlm" from
sourceSets.main.output destinationDir =
file("${projectDir}/dist") manifest { from "${projectDir}/META-
INF/MANIFEST.MF" } from(projectDir) { include
"plugin.properties" include "plugin.xml" } into("lib") { from
"${projectDir}/lib" include "*.jar" exclude "fortify-
public*.jar" } } build.dependsOn(pluginJar)
```

Important

Application Securityに付属しているサンプルバグトラッカーコードをカスタマイズしても、同じプラグインクラス名を使用する場合は、プラグインの短い表示名を変更しないでください。これは、バグフィールドテンプレートグループの名前に使用されます。(整合性を保つため、長い表示名も変更しないようにしてください。)メイン実装クラスの名前を変更する場合は、プラグインの表示名も変更する必要があります。

すべてのバグトラッカープラグインの依存関係を含むライブラリをビルドする方法については、`<ssc_distribution_dir>/Samples/<bugtracker_plugin_name>/README` ファイルを参照してください。

参照情報

バグトラッカプラグインの作成

1.24. 高度な設定

このセクションでは、管理者向けの高度な設定のトピックについて説明します。

このセクションでは、次のトピックについて説明します。

1.24.1. Application Securityの設定の自動化

autoconfigファイルを使用して、展開前にApplication Securityの設定を自動化できます。このファイルには、Application Securityの設定可能な各側面に関するセクションが含まれています。autoconfigファイルは、Application Securityのサイレントアップデートおよびインストール用の設定とシードバンドルを提供することで、自動展開を可能にします。autoconfigファイルを使用すると、セットアップウィザードのすべてのタスクを自動化できます。セットアップウィザードは、サーバの起動時にこのファイルを選択し、インストール全体を自動化します。

Note

`datasource.properties`ファイルおよび一部のデータベースフィールドには、`secret.key`ファイルに依存する暗号化されたエントリが含まれています。したがって、Application Securityインスタンスをコンピュータ間で移動する場合は、プロパティファイルだけではなく`secret.key`ファイルも移動する必要があります。

Application Securityの設定を自動化するには、次の手順に従います。

Important

ルートコンテキストで設定を自動化するには、「ルートコンテキストでの設定の自動化」を参照してください。

1. テキストエディタを開き、`<app_context>.autoconfig`という名前のファイルを作成します。ここで、*<app_context>*は、Application Securityがデプロイされているアプリケーションサーバのコンテキストです(`<fortify.home>`に作成されるディレクトリの名前)。
2. 以下に示すYAML形式の項目を`<app_context>.autoconfig`ファイルに追加します。

   Note

   使用するデータベースエンジンのデータベースプロパティのみをコピーします。各プロパティの前にあるハッシュ記号(#)は、必ず削除してください。

```
appProperties: # Include any property found in
<fortify.home>/<app_context>/conf/app.properties # For
example, host.url: 'https://ssc.example.com/ssc/' #
searchIndex.location: '/home/<app_context>/search_index' #
host.validation: false datasourceProperties: # Include any
property found in
<fortify.home>/<app_context>/conf/datasource.properties #
For example: # db.username: ssc_db_admin_username #
db.password: ssc_db_admin_password  # SQL Server database #
jdbc.url: 'jdbc:sqlserver://mssql-
host:1433;database=ssc_db;sendStringParametersAsUnicode=fals
e' # SQL Server database # jdbc.url: 'jdbc:mysql://mysql-
host:3306/ssc_db?
sessionVariables=collation_connection=latin1_general_cs&rewr
iteBatchedStatements=true' # Oracle database # jdbc.url:
'jdbc:oracle:thin:oracle-host:1521:ssc_db'
dbMigrationProperties: # Enable automatic database migration
migration.enabled: true # Optionally specify alternative
migration credentials # migration.username:
ssc_db_admin_username # migration.password:
ssc_db_admin_password seeds: # Modify the path to the
appropriate location for your environment  -
'/home/ssc/bundles/ Fortify_Process_Seed_Bundle-
2025_Q2_<build>.zip ' - '/home/ssc/bundles/
Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<build>.zip ' -
'/home/ssc/bundles/ Fortify_PCI_SSF_Basic_Seed_Bundle-
2025_Q2_<build>.zip ' - '/home/ssc/bundles/
Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip '
```

3. *<app_context>*.autoconfig ファイルを *<fortify.home>/* ディレクトリに保存します。
4. fortify.license ファイルのコピーを <fortify.home>/ ディレクトリに配置します。
5. WARファイル名の形式が *<app_context>*.war であることを確認します。
6. Tomcatサーバを起動します。

自動設定が完了すると、Application Securityは有効な設定チェックサムを計算し、version.properties プロパティの値として autoconfig.checksum ファイルに保存します。

Application Security起動したときに`autoconfig`ファイルが存在していた場合、有効な設定チェックサムが計算され、`version.properties`ファイルに保存されているチェックサムと比較されます。チェックサムが一致しない場合、Application Securityは軽量自動設定を実行し、`autoconfig.checksum`値を更新します。

何らかの理由で自動設定が失敗すると、Application Securityは保守モードにされます(`version.properties`ファイル内で`maintenance.mode=true`と設定されます。このプロパティは、次回のサーバ起動時に完全自動設定を適用するか、セットアップウィザードを表示するかを指定するものです)。

チェックサムには次の内容が含まれます。

- autoconfig `appProperties`キーに含まれる有効なプロパティ
- autoconfig `datasourceProperties`キーに含まれる有効なプロパティ
- 有効なautoconfig `seeds`キーに含まれるファイル名
- `conf/app.properties`ファイル内のすべてのプロパティ
- `conf/datasource.properties`ファイル内のすべてのプロパティ

`dbMigrationProperties`のプロパティはチェックサムに含まれません。

Application Securityが完全自動設定を実行するのは、設定が完全に完了していない場合のみです。チェックサムは一致しないものの、それを抜かせば設定が完了している場合は、軽量の自動設定のみを実行します。

軽量の自動設定では、`autoconfig`ファイルの設定に関係なくデータベースのマイグレーションがスキップされ、最初の内部バンドルシード処理もスキップされます。ただし、autoconfig `seeds`キーで指定されたバンドルのシード処理は実行されます。

1.24.1.1. ルートコンテキストでの設定の自動化

ルートコンテキストでApplication Securityの設定を自動化するには:

1. テキストエディタを開き、 `_default_.autoconfig` という名前のファイルを作成します。
2. 以下に示すYAML形式の項目を `_default_.autoconfig` ファイルに追加します。

Note

使用するデータベースエンジンのデータベースプロパティのみをコピーします。各プロパティの前にあるハッシュ記号(#)は、必ず削除してください。

```
appProperties: # Include any property found in
<fortify.home>/_default_/conf/app.properties. # For example,
host.url: 'https://ssc.example.com/' # searchIndex.location:
'<fortify.home>/_default_/index' # host.validation: false
datasourceProperties: # Include any property found in
<fortify.home>/_default_/conf/datasource.properties. # For
example: # db.username: ssc_db_admin_username # db.password:
ssc_db_admin_password # MSSQL database # jdbc.url:
'jdbc:sqlserver://mssql-
host:1433;database=ssc_db;sendStringParametersAsUnicode=fals
e' # MySQL database # jdbc.url: 'jdbc:mysql://mysql-
host:3306/ssc_db?
sessionVariables=collation_connection=latin1_general_cs&rewr
iteBatchedStatements=true' # Oracle database # jdbc.url:
'jdbc:oracle:thin:oracle-host:1521:ssc_db'
dbMigrationProperties: # Enable automatic database migration
migration.enabled: true # Optionally specify alternative
migration credentials # migration.username:
ssc_db_admin_username  # migration.password:
ssc_db_admin_password seeds: # Modify the path to the
appropriate location for your environment  -
'/home/ssc/bundles/ Fortify_Process_Seed_Bundle-
2025_Q2_<build>.zip ' - '/home/ssc/bundles/
Fortify_PCI_Basic_Seed_Bundle-2025_Q2_<build>.zip ' -
'/home/ssc/bundles/ Fortify_PCI_SSF_Basic_Seed_Bundle-
2025_Q2_<build>.zip ' - '/home/ssc/bundles/
Fortify_Report_Seed_Bundle-2025_Q2_<build>.zip '
```

3. _default_.autoconfig ファイルを *<fortify.home>* ディレクトリに保存します。
4. fortify.license ファイルのコピーを <fortify.home> フォルダに配置します。
5. ssc.war ファイルの名前を ROOT.war に変更します。
6. Tomcatサーバを起動します。

参照情報

Application Securityの設定の自動化

1.24.2. アプリケーションの設定オプション

管理者がApplication Security環境設定を更新するには、`<fortify.home>/<app_context>/conf/app.properties` ファイルを使用するか、Application Securityの設定を自動化するために使用されているautoconfigファイルの `appProperties` セクションを使用します。

プロパティ名	説明(Description)
Application SecurityのURL	
host.url	Application Securityにアクセスするためのアドレスを指定します(Application Securityの設定の自動化)
host.validation	`true`に設定すると、`host.url`の値に対するHTTPホスト検証が有効になります(Application Securityの設定の自動化)。デフォルトは`false`です。
グローバル検索	
searchIndex.location	ローカルファイルシステム上でのフルテキストインデックスディレクトリの絶対パスを指定します(Application Securityの設定の自動化)。
バックグラウンドジョブの実行	
jobs.threadCount	ジョブ処理スレッドプールのサイズを指定します(Oracleデータベースのパーティショニングによるパフォーマンスの改善)。デフォルト値は`10`です。
job.exclusiveJobOverheadPercentage	排他的なジョブ(アーティファクトのパージ、アーティファクトの削除、アプリケーションバージョンの削除など)の実行中に`jobs.threadCount`値に適用する縮小率を指定します。デフォルト値は`20`です。有効な値は、`0`から`100`までの範囲です。

プロパティ名	説明(Description)
job.numberOfDedicatedDataExports	データエクスポート用に予約するジョブ処理スレッドの数を指定します。デフォルト値は `2` です。
job.numberOfConcurrentReports	同時に実行できるレポートジョブの最大数を指定します。デフォルト値は `2` です。
job.numberOfConcurrentExclusiveJobs	同時に実行できる排他的ジョブの最大数を指定します。デフォルト値は `1` です。
パスワード	
password.strength.min.score	新しく保存するパスワードの強度の最小許容スコアを指定します(Application Securityのサインインに必要なパスワード強度の設定)。デフォルト値は3です。
sso.localAuthenticationEnabled	`true` に設定すると、X.509 SSOでローカルパスワード認証を使用できます(シングルサインオンを使用するためのApplication Securityの設定について)。デフォルトはfalseです。
LDAPキャッシュ	
ldap.cache.persistence.enabled	`true` に設定すると、Application Securityは起動時間を短くするためにLDAPキャッシュをデータベースに保存します(LDAPキャッシュの永続性の有効化)。デフォルトは `true` です。

プロパティ名	説明(Description)
ldap.cache.refresh.interval.hours	キャッシュ更新間隔(時間数)を指定します(LDAPキャッシュの永続性の有効化)。デフォルトは1時間です。有効な値は、`1`から`12`までの範囲です。
監査の問題履歴	
issue.attrChangelog.enabled	`true`に設定すると、監査の問題履歴機能が有効になります(監査の問題履歴を有効にする)。デフォルトは`false`です。

1.24.2.1. バックグラウンドジョブ実行戦略の設定

次の表で、Application Securityバージョン25.2.0より前に存在していたバックグラウンドジョブ実行戦略を再現する方法について説明します。

レガシージョブ実行戦略	説明(Description)	設定手順
保守的	ジョブの同時並行性、スループット、およびジョブの安定性のバランスをとります。	必要な変更はありません。

レガシージョブ実行戦略	説明(Description)	設定手順
積極的	同時並行性が向上します。この戦略を使用すると、ジョブスケジューラはジョブの実行方法に制限を適用しません。すべてのジョブが均等に、使用可能なすべてのワーカで実行されます。 OpenTextでは、このジョブ実行戦略の使用を推奨していません。	• `job.exclusiveJobOverheadPercentage` を `0` に設定します。 • `job.numberOfConcurrentReports` を `jobs.threadCount` と同じ値に設定します。 OpenTextでは、スキャン処理のスループットを向上させるとともに、レポート生成によって消費されるピークメモリを減らすために、`jobs.threadCount` 値またはデフォルト値の `2` よりも小さい値を使用することを推奨しています。 • `job.numberOfConcurrentExclusiveJobs` を `jobs.threadCount` と同じ値に設定します。 OpenTextでは、スキャン処理のスループットを向上させるとともに、データベース内でのロック競合を回避するために、デフォルト値の

レガシージョブ実行戦略	説明(Description)	設定手順
		`1` を使用することを推奨しています。
排他的ジョブ	ジョブを1つずつ、順番に実行できるようにします。 OpenTextでは、このジョブ実行戦略の使用を推奨していません。	• `jobs.threadCount` を `1` に設定します。 • `job.numberOfDedicatedDataExports` を `0` に設定します。

1.25. Webhookのペイロード

各Webhookペイロードには次のフィールドが含まれています。

- events—Webhookイベントリスト(トリガされたイベントに関する情報)
- sscUrl—サーバのURLアドレス
- webhookId—関連付けられたWebhook ID
- triggeredAt—ペイロードが作成された(作成され、データベースに保存された)日付

例:

```
{ "events":[ {
"event":"ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS",
"artifactId":l, "projectVersionId":l, "filename":"file.fpr",
"username":"testUser1" } ], "triggeredAt":"2020-08-
21T12:19:24.502+0000", "sscUrl":"http://localhost:8180/ssc",
"webhookId":1 }
```

このセクションでは、次のトピックについて説明します。

1.25.1. イベントペイロード

［events］アレイには、次に説明する実際のイベントペイロードが入力されます。各イベントには、イベントタイプについて説明する［イベント(event)］フィールドがあります。

Note

現在、1つのアレイに1つのイベントのみがあります。イベントの集約はサポートされていません。

1.25.2. アーティファクトアップロードペイロード

アーティファクトイベント用に生成されたペイロードには、次のフィールドが含まれています。

- artifactId—アップロードされたアーティファクトのID
- projectVersionId—アーティファクトがアップロードされたアプリケーションバージョンのID
- filename—アーティファクトファイル名
- username—イベントをアップロードしたユーザのユーザ名
- event—アーティファクトアップロードイベントのタイプ

  アップロードイベントタイプ:

  - ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS
  - ANALYSIS_RESULT_UPLOAD_FAILURE
  - ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL
  - ANALYSIS_RESULT_INDEXING_COMPLETED

例:

```
 { "event":"ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS",
"artifactId":1, "projectVersionId":l, "filename":"file.fpr",
"username":"testUser1" }
```

アーティファクトアップロードで承認されたペイロード

これは、アーティファクトアップロードペイロードの拡張機能であり、承認するユーザと承認コメントを識別するための追加フィールドが含まれています。

フィールド:

- artifactId—アップロードされたアーティファクトのID
- projectVersionId—アーティファクトがアップロードされたアプリケーションバージョンのID
- filename—アーティファクトファイル名
- username—アップロードするユーザのユーザ名
- approvalUsername—承認するユーザのユーザ名
- approvalComment—承認時に送信されるコメント

例:

```
 { "event":"ANALYSIS_RESULT_UPLOAD_APPROVED", "artifactId":1,
"projectVersionId":1, "filename":"file.fpr",
"username":"testUser1", "approvalUsername":"testUser2",
"approvalComment":"upload has been approved" }
```

1.25.3. プロジェクトバージョンペイロード

アプリケーションバージョンイベント用に生成されたペイロードには、次のフィールドが含まれています。

- projectId—アプリケーションID
- projectName—アプリケーション名
- projectVersionId—アプリケーションバージョンID
- projectVersionName—アプリケーションバージョン名
- event—アプリケーションバージョンイベントのタイプ

  イベントタイプ:

  - APP_VERSION_CREATED
  - APP_VERSION_UPDATED
  - APP_VERSION_DELETED

例:

```
 { "event":"APP_VERSION_CREATED", "projectId":1,
"projectName":"Test application", "projectVersionId":1,
"projectVersionName":"vl" }
```

プロジェクトバージョンで更新されたペイロード

これはプロジェクトバージョンペイロードの拡張機能であり、行われた変更を識別するための追加フィールドがあります。

フィールド:

- projectId—アプリケーションID
- projectName—アプリケーション名
- projectVersionId—アプリケーションバージョンID
- projectVersionName—アプリケーションバージョン名
- event—APP_VERSION_UPDATED
- changes—アプリケーションバージョンで変更された内容を定義する値リスト

  入力可能な値:

  - ACTIVE—アプリケーションバージョンの［active］ステータスが変更された場合

- COMMITTED—アプリケーションバージョンがコミットされたか、またはコミット解除された場合
- PROJECT_VERSION_NAME—アプリケーションバージョン名が変更された場合
- PROJECT_TEMPLATE—問題テンプレートが変更された場合
- ATTRIBUTES—ビジネス/技術属性が変更された場合
- USER_ACCESS_ADDED—1人以上のユーザがアプリケーションバージョンに追加された場合
- USER_ACCESS_REMOVED—1人以上のユーザがアプリケーションバージョンから削除された場合
- CUSTOM_TAG—アプリケーションバージョンにカスタム属性が追加または削除された場合
- PRIMARY_TAG—アプリケーションバージョンのプライマリタグが変更された場合

例:

```
 { "event" APP_VERSION_UPDATED", "projectId":1,
"projectName":"Test application", "projectVersionId":1,
"projectVersionName":"v1", "changes":["ACTIVE","COMMITTED"] }
```

以前のペイロードから作成されたプロジェクトバージョン

これは、プロジェクトバージョンで更新されたペイロードの拡張機能です。この場合は、既存のアプリケーションバージョンの環境設定値が新しいアプリケーションバージョンにコピーされます。このペイロードには、新しいアプリケーションバージョンの基礎になるアプリケーションバージョンに関する追加情報が含まれています。

フィールド:

- projectId—親アプリケーションのID
- projectName—親アプリケーションの名前
- projectVersionId—(子)アプリケーションバージョンID
- projectVersionName—アプリケーションバージョン名
- previousProjectId—(親)アプリケーションのID
- previousProjectName—(親)アプリケーションの名前
- previousProjectVersionId—(親)アプリケーションバージョンID
- previousProjectVersionName—(親)アプリケーションバージョン名
- event—APP_VERSION_CREATED

例:

```
 { "event":"APP_VERSION_CREATED", "projectId":1,
"projectName":"Test application", "projectVersionId":2,
"projectVersionName":"v2", "previousProjectId":1,
"previousProjectName":"Test application",
"previousProjectVersionId":1, "previousProjectVersionName":"v1"
}
```

1.25.4. レポート生成ペイロード

レポートイベント用に生成されたペイロードです。

フィールド:

- reportId—要求されたレポートのID
- reportName—レポート生成用に指定された名前
- renderingEngine—レポートレンダリングエンジン
- reportType—レポートタイプ
- event—レポート生成イベントのタイプ

  入力可能な値:

  - REPORT_GENERATION_COMPLETE
  - REPORT_GENERATION_REQUESTED

例:

```
 { "event":"REPORT_GENERATION_COMPLETE", "reportId":1,
"reportName":Test report", "renderingEngine":"BIRT",
"reportType":"PROJECT" }
```

1.25.5. ユーザペイロード

ユーザライフサイクルイベント用に生成されたペイロードです。

フィールド:

- id—ユーザID
- username—ユーザのユーザ名
- event—ユーザイベント
    - USER_CREATED - Application Securityで認証エンティティ(LOCAL_USER、LOCAL_GROUP、LDAP_USER、LDAP_GROUP、またはLDAP_ORGANIZATIONAL_UNIT)が作成されました。
    - USER_DELETED - Application Securityから認証エンティティ(LOCAL_USER、LOCAL_GROUP、LDAP_USER、LDAP_GROUP、またはLDAP_ORGANIZATIONAL_UNIT)が削除されました。
    - USER_UPDATED - Application Securityで認証エンティティ(LOCAL_USER、LOCAL_GROUP、LDAP_USER、LDAP_GROUP、またはLDAP_ORGANIZATIONAL_UNIT)が更新されました。
    - LOCAL_USER_ACCOUNT_LOCKED
- userType—ユーザのタイプ

  入力可能なタイプ:

    - LOCAL_USER
    - LOCAL_GROUP
    - LDAP_USER
    - LDAP_GROUP
    - LDAP_ORGANIZATIONAL_UNIT

例:

```
 { "id":1, "username":"testUser", "event":"USER_CREATED",
"userType":"LOCAL_USER" }
```