Micro Focus
Fortify Software Security Center

ソフトウェアバージョン: 21.2.0

ユーザガイド

ドキュメントリリース日 : 2021年 11月
ソフトウェアリリース日 : 2021年 11月

法的通知

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

保証

Micro Focusとその関連会社およびライセンサ(以下「Micro Focus」)の製品およびサービスに関する保証は、製品およびサービスに付属する保証規定に明示されている内容に限定されます。本書のいかなる記述も、追加の保証を構成するものではありません。Micro Focusは、本書の技術的内容や編集に関する誤りや欠落に関して責任を負いません。ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密性のあるコンピュータソフトウェアです。明確な指示がある場合を除き、保持、使用、またはコピーには、Micro Focusからの有効なライセンスが必要です。FAR 12.211および12.212に従って、商用コンピュータソフトウェア、コンピュータソフトウェアドキュメント、および商用品目の技術データは、米国政府に対して、ベンダーの標準商用ライセンスに基づいてライセンスされます。

著作権表示

商標表示

このドキュメントに記載されているすべての商標、サービスマーク、製品名、およびロゴは、該当する所有者に帰属します。

ドキュメントの更新情報

このドキュメントのタイトルページには、次の識別情報が記載されています。

- ソフトウェアバージョン番号
- ドキュメントリリース日。ドキュメントが更新されるたびに変更されます
- ソフトウェアリリース日。ソフトウェアのこのバージョンのリリース日付を示します

このドキュメントは7月 13, 2022に作成されました。最新の更新を確認する場合や、最新のドキュメントを使用しているかを確認する場合は、次のサイトをご覧ください。

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

目次

序文

Micro Focus Fortifyカスタマサポートへのお問い合わせ

サポートWebサイトにアクセスして、次の作業を実行できます。

- ライセンスとエンタイトルメントの管理
- 技術サポートリクエストの作成と管理
- ドキュメントやナレッジ記事の閲覧
- ソフトウェアのダウンロード
- コミュニティの探索

https://www.microfocus.com/support

詳細情報

Fortifyソフトウェア製品について詳しくは、次のリンクを参照してください。

https://www.microfocus.com/cyberres/application-security

ドキュメントセットについて

Fortifyソフトウェアのドキュメントセットには、すべてのFortifyソフトウェア製品およびコンポーネントのインストールガイド、ユーザガイド、および展開ガイドが含まれています。また、新機能、既知の問題、および最新の更新情報について説明するテクニカルノートとリリースノートもあります。これらのドキュメントの最新バージョンには、次のMicro Focus製品ドキュメントWebサイトからアクセスできます。

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

リリース間のドキュメント更新のお知らせを受け取るには、Micro Focusコミュニティの Fortify製品のお知らせを購読してください。

https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements

Fortify製品の機能紹介ビデオ

YouTubeのFortify Unpluggedチャネルで、Fortifyの製品と機能を紹介するビデオをご覧いただけます。

https://www.youtube.com/c/FortifyUnplugged

変更ログ

次の表に、このドキュメントへの変更を示します。

ドキュメントの改訂は、変更が製品の機能に影響を与える場合にのみ発行されます。

ソフトウェアリリース/ドキュメント改訂	変更点
21.2.0	**新しいトピック:** • "Micro Focus Fortify Software Security Center 21.2.0の新機能" ページ36 • "Fortify Software Security Centerとのコンポーネントの統合について" ページ46 • "Fortify Software Security Center をKubernetesクラスタへ展開する" ページ53 • "環境設定: システム全体とアプリケーションバージョン間" ページ198 • "LDAPエンティティの識別名の更新" ページ121 • "スキャンアーティファクトの詳細の表示" ページ290 • "問題のバッチの監査" ページ327 • "ScanCentral SAST Controllerを保守モードにする" ページ362 • "センサの安全なシャットダウン" ページ362 **変更されたトピック:** • "展開の概要" ページ45には、Fortify Software Security Center Dockerイメージへのアクセスを要求する方法に関する変更された情報が含まれています。 • "Fortify Software Security Centerインストール環境" ページ49に、Fortify Software Security Center環境のさまざまなコンポーネントの更新された図が追加されました。 • `fortify.home`のディレクトリ構造に関する情報が、"fortify.homeディレクトリについて" ページ57に追加されました。 • "BIRTレポート用のセキュリティの設定" ページ93の表とビューの表が変更されました。

ソフトウェアリリース/ドキュメント改訂	変更点
	• "Fortify Software Security Centerユーザ認証について" ページ105が変更され、SCIMに関する情報が含まれました。 • "LDAP認証の設定の準備" ページ105に、複数のLDAPサーバを使用するための要件に関する情報が追加されました。 • "LDAPサーバの設定" ページ108が変更され、［CREATE NEW LDAP CONFIGURATION］ダイアログボックスへの新しいフィールドの追加が反映されました。 • 保守的なジョブ実行戦略の説明が、"ジョブスケジューラの設定" ページ131で変更されました。 • "Fortify Software Security CenterでのKerberos認証の設定" ページ151で説明されている手順でステップが変更されました。 • 1ページの"バグトラッカーの統合について" ページ159にAzure DevOps Server関する重要な注意が追加されました。 • "Micro Focus Fortify更新サーバからのRulepackの更新" ページ176で説明されている手順が変更されました。 • "Rulepacksをエクスポートする" ページ177で、Rulepackのエクスポートで発生する処理が明確化されました。 • "ルールパックの削除" ページ178で、Rulepackの削除発生する内容が明確化されました。 • ［**ADD MISSING PERMISSIONS**］ボタンの追加を反映するために、"カスタム役割の作成" ページ208にステップが追加されました。 • "Webhookの作成" ページ270でハッシュベースのメッセージ認証コード(HMAC)の計算方法に関する情報が修正されました。 • "スキャンアーティファクトのアップロード" ページ288が更新され、［**3rd party results**］チェックボックスの削除が反映されました。 • ユーザインタフェースの変更を反映するように、"スキャンアーティファクトをダウンロードする" ページ292が変更されました。 • "監査する問題に関する情報の表示" ページ305に、問題テーブルの列とそれぞれの説明を一覧表示する表が含まれるようになりました。

ソフトウェアリリース/ドキュメント改訂	変更点
	• 「非表示の問題の表示」、「削除された問題の表示」、および「削除された問題の表示」は、すべて"問題の表示設定の設定" ページ325に移動されました。 • "検索修飾子" ページ313に、audience検索修飾子を使用しないことを推奨する注記が追加されました。 • "Fortify Scan結果の監査" ページ317は、ユーザ割り当ての変更を反映するように変更されました。 • "Fortify Software Security Centerの設定の自動化" ページ409には新しい詳細情報が含まれています。 **削除されたトピック:** • Micro Focus Fortify Software Security Center 21.1.1の新機能 • キーボードショートカットの無効化(ホットキー) - この情報は、"環境設定:システム全体とアプリケーションバージョン間" ページ198で利用できるようになりました。 • 電子メールアラートの受信の有効化と無効化 - この情報は、"環境設定:システム全体とアプリケーションバージョン間" ページ198で利用できるようになりました。 • [ADMINISTRATION]ビューでの設定へのアクセス • すべてのアプリケーションバージョンのデータをCSVファイルにエクスポートする
21.1.1	**新しいトピック:** • "SCIM 2.0プロトコルの実装" ページ123 • "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Azure ADへの接続の設定" ページ125 • "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" ページ128 • "外部管理されたユーザおよびグループを表示する" ページ216 • "ScanCentral SAST Controllerを保守モードにする" ページ362 **変更されたトピック:**

ソフトウェアリリース/ドキュメント改訂	変更点
	• "SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141」に、Azure ADとの統合に関するメモが追加されました。 • ユーザインタフェースの変更に基づいて、"ローカルユーザアカウントの作成" ページ210が変更されました。 • ユーザインタフェースの変更に基づいて、"ローカルユーザアカウントを編集する" ページ213が変更されました。 • "ジョブスケジューラの設定" ページ131に説明を追加しました。
21.1.0	**新しいトピック:** • Micro Focus Fortify Software Security Center 21.1.0の新機能 • "単一の問題のバグの送信" ページ247 • "複数の問題のバグの送信" ページ247 • "Sonatypeデータをエクスポートする" ページ346 **変更されたトピック:** • Oracleデータベースサポート用のJDBCドライバの取得に関する情報が、"JDBCドライバについて" ページ59から削除されました。 • "X.509証明書ベースのSSOを使用するためのFortify Software Security Centerの設定" ページ153に新しい最初のステップを追加しました。 • ユーザインタフェースの変更に基づいて、"ローカルユーザアカウントの作成" ページ210を変更しました。 • ユーザインタフェースの変更に基づいて、"ローカルユーザアカウントを編集する" ページ213を変更しました。 • 手順の変更に基づいて、"ローカルユーザアカウントのロック解除" ページ215を変更しました。 • "LDAPサーバの設定" ページ108で、 [**Cache: Max object lifetime**]詳細統合プロパティが [CREATE NEW LDAP CONFIGURATION]ダイアログボックスから削除されました。 [**Cache: Max thread pool size**]プロパティが追加されまし

ソフトウェアリリース/ドキュメント改訂	変更点
	た。その他の変更は、［SSL trust check］および［Hostname validation］チェックボックスの新たな配置を反映しています。 • "SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141」の「SAML SSO統合のトラブルシューティング」セクションから項目を削除しました。 • "Fortify Software Security CenterでのKerberos認証の設定" ページ151の「トラブルシューティング」セクションが削除されました。 • "スキャンアーティファクトのアップロード" ページ288で、長いHTTP応答の切り捨てに関する注意が追加されました。 • "アプリケーションバージョンの分析結果を承認する" ページ293に「承認処理を拒否する」というセクションが含まれるようになりました。 • ユーザインタフェースの変更を反映するように、"［OVERVIEW］および［AUDIT］ページに表示する問題をフィルタ処理する" ページ309が変更されました。 • 「抑止された問題の表示」および「削除された問題の表示」に小さな変更が行われました。 **削除されたトピック:** • Micro Focus Fortify Software Security Center 20.2.0の新機能 • (Oracleのみ)Fortify Software Security CenterへのJDBCドライバの追加 • 1つ以上の問題のバグの送信
20.2.0/リビジョン1 - 2020年12月4日	"バグトラッカーの統合について" ページ159に、Jira Cloudがサポートされているバグトラッカとして一覧表示されるようになりました。
20.2.0	**新しいトピック:** • 「Micro Focus Fortify Software Security Center 20.2.0の新機能」 • "Fortify Software Security Centerを使用したScanCentral DASTスキャンの実行と管理の有効化" ページ131

ソフトウェアリリース/ドキュメント改訂	変更点
	• "Sonatype結果の監査" ページ342 • "Webhookについて" ページ269 • "Webhookの許可" ページ269 • "Webhookの作成" ページ270 • "Webhookを編集する" ページ274 • "Webhookペイロードの表示" ページ275 • "Webhookの削除" ページ278 • "Webアプリケーションの被影響性分析について" ページ336 • "Sonatype結果の監査" ページ342 • "ScanCentral SASTの許可" ページ356 • "Fortify ScanCentral DASTの使用" ページ368 • "ScanCentral DASTの許可" ページ368 • "ScanCentral DASTへの動的スキャン要求の送信" ページ370 • "Webhookのペイロード" ページ412 **変更されたトピック:** • "展開の概要" ページ45に「KubernetesクラスタへのFortify Software Security Centerの展開」が含まれるようになりました。 • "Fortify Software Security Centerインストール環境" ページ49が、新しいScanCentral DASTおよびScanCentral DAST製品名に対応するために変更されました。 • 「(Oracleのみ) Fortify Software Security CenterへのJDBCドライバの追加」のMySQLへの参照が削除されました。これは、MySQLデータベースで使用するために、MariaDB JDBCドライバがSSC WARファイルに含まれるようになったためです。 • SQL ServerおよびMySQLサーバ用のJDBCドライバとFortify Software Security Centerソフトウェアのバンドルに関する情報が、"JDBCドライバについて" ページ59に追加されました。 • "Microsoft SQL Serverデータベースの使用" ページ61に、新しいセクション「Windowsドメイン認証」が含まれるようになり

ソフトウェアリリース/ドキュメント改訂	変更点
	ました。 • MySQL 8.0に対応するため、"MySQLデータベースの設定" ページ62が更新されました。 • "Fortify Software Security Centerの初回設定" ページ69のステップ12に注意が追加されました。 • ScanCentral DAST、ScanCentral SAST、およびWebhooks項目はが、" [ADMINISTRATION]ビューで使用可能な環境設定オプション" ページ81の設定オプションの表に追加されました。 • "Fortify Software Security CenterでのKerberos認証の設定" ページ151を使用したKerberos認証の設定に[**Troubleshooting**]セクションが含まれるようになりました。 • "SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141 • "Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164には、SourceAndLibScannerの入手方法に関する情報が含まれています。 • "Fortify Software Security Centerデータベースのアップグレードタスク" ページ181でタスク3が変更されました。 • 組織のバナーをカスタマイズするために必要なステップが、"Fortifyバナーの組織向けカスタマイズ" ページ156で変更されました。 • "Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164は、ユーザインタフェースの変更を反映するように変更されました。 • "Fortify Software Security Centerデータベースのアップグレードタスク" ページ181のデータベースアップグレードタスクの表にタスクが追加されました。 • "Fortify Software Security Centerの初回設定" ページ69、"アップグレード後のFortify Software Security Centerの設定" ページ184に、MySQLデータベースに接続するために使用するMariaDB JDBCドライバに関する注記が追加されました。 • "システムへの問題テンプレートの追加" ページ230に、「問題テンプレートの作成または変更」という新しいセクションが追

ソフトウェアリリース/ドキュメント改訂	変更点
	加されました。 • "新しいアプリケーションの最初のバージョンの作成" ページ231は、CREATE NEW APPLICATION VERSIONウィザードの変更を反映するように変更されました。 • "アプリケーションに新しいバージョンを追加する" ページ234は、CREATE NEW VERSIONウィザードへの変更を反映するように変更されました。 • "システムへの問題テンプレートの追加" ページ230に、「問題テンプレートの作成または変更」というセクションが追加されました。 • "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" ページ263および "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" ページ264が変更され、［APPLICATION PROFILE］ダイアログボックスの［**CUSTOM TAGS**］タブへの変更を反映するために修正されました。 • "スキャンアーティファクトのアップロード" ページ288が変更され、［**3rd party results**］チェックボックスの追加が反映されました。 • "Fortify Scan結果の監査" ページ317は、Static Code Analyzerによって明らかにされた問題の監査と、ScanCentral DASTおよびSonatypeを使用して明らかにされた問題を区別するために変更されました。 • "Sonatypeデータの表示" ページ338は、新しい［OPEN SOURCE］ページの追加を反映するように変更されました。 • "ScanCentral SASTスキャン要求の詳細の表示" ページ357は、製品名の変更を反映するように変更されました。 • "ScanCentral SASTスキャン要求のキャンセル" ページ359は、製品名の変更を反映するように変更されました。 • "ScanCentral SASTセンサプールについて" ページ363に、ScanCentral SASTセンサの有効期限に関する注記が追加されました。 • SSA Progress Reportの説明が、"BIRTレポート" ページ371から削除されました。 • "認証トークンを生成する" ページ380のトークン名オプションの表に、WIESystemTokenとWIEUserTokenトークンの説

ソフトウェアリリース/ドキュメント改訂	変更点
	明が含まれるようになりました。 • YaML形式の情報は、MySQLデータベースでのMariaDB JDBCドライバの使用に対応するために、"Fortify Software Security Centerの設定の自動化" ページ409」で変更されました。 **削除されたトピック:** • Micro Focus Fortify Software Security Center 20.1.0の新機能
20.2.0/リビジョン2: 2020年8月6日	**更新:** "MySQLデータベースの設定" ページ62 - サポートされていない設定(`query_cache_type`、`query_cache_size`、`innodb_file_format`、および`innodb_log_file_size`)は、ステップ5の環境設定の表から削除されました。`max-allowed-packet`設定がテーブルに追加されました。
20.2.0/リビジョン1: 2020年6月1日	**更新:** "Fortify Software Security Centerデータベースのアップグレードタスク" ページ181 - タスク2では、SQL ServerまたはMySQLデータベースを使用しているユーザに対して、Tomcatサーバから古いバージョンのJDBCドライバを削除し、JDBC JARファイルの場所がTomcatサーバのクラスパスに存在しなくなったことを通知するために、重要な注意が拡張されました。タスク3では、プラグインフレームワークフォルダへのパスが更新されました。
20.1.0	**一般:** • このリリースでは、Fortify CloudScanがFortify ScanCentralという名前に変更されたので、「CloudScan」がすべて「ScanCentral」に変更されました。 • アプリケーションバージョンが［Applications］ビューのアプリケーション名の下の展開可能なリストに表示されるようになったので、アプリケーションバージョンの選択方法に関する手順を含むすべてのトピックに小さな変更が加えられました。 **新しいトピック:** • Micro Focus Fortify Software Security Center 20.1.0の新

ソフトウェアリリース/ドキュメント改訂	変更点
	機能 • "Fortify Software Security CenterがX.509またはKerberos SSOソリューションを使用するように設定されている場合にユーザ名およびパスワードログインを有効にする" ページ154 • "Fortify Software Security Centerが保守モードでスタックしている場合" ページ175 • "属性と属性値の削除" ページ226 • "Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164 • "Sonatypeデータの表示" ページ338 **変更されたトピック:** • "JDBCドライバについて" ページ59 • 「(MySQLおよびOracleのみ) Fortify Software Security CenterへのJDBCドライバの追加」 • "Fortify Software Security Centerの初回設定" ページ69 • "BIRTレポート用のセキュリティの設定" ページ93 • "セッションログアウトについて" ページ76 • "電子メールアラート通知設定の設定" ページ99 • "シングルサインオンを使用するためのFortify Software Security Centerの設定" ページ139 • "Central Authorization Serverを使用するためのFortify Software Security Centerの設定" ページ140 • "Fortify Software Security CenterでのKerberos認証の設定" ページ151 • "SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141 • "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Fortify Software Security Centerの設定" ページ149 • "X.509証明書ベースのSSOを使用するためのFortify Software Security Centerの設定" ページ153 • "ローカルユーザアカウントの作成" ページ210

ソフトウェアリリース/ドキュメント改訂	変更点
	• "ローカルユーザアカウントを編集する" ページ213 • "ローカルユーザアカウントのロック解除" ページ215 • "属性と属性値の削除" ページ226 • "アプリケーションバージョンの新しいカスタム属性の指定" ページ228 • "新しいアプリケーションの最初のバージョンの作成" ページ231 • "アプリケーションに新しいバージョンを追加する" ページ234 • "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" ページ263 • "アプリケーションバージョンの分析結果を承認する" ページ293 • 「[Applications]ビューからの[AUDIT]ページへのアクセス」 • "ScanCentral SASTセンサプールの作成" ページ364 • "レポートを生成して表示する" ページ371 • "レポートテンプレートをダウンロードする" ページ376 • "認証トークンを生成する" ページ380 • "Fortify Software Security Center URLの指定について" ページ386 • "実装" ページ398 • "プラグインメソッドとメソッドコール" ページ400 • "Sonatype結果の監査" ページ342 **削除されたトピック** • [AUDIT]ページへのアクセス Fortify Software Security CenterがX.509証明書ベースのSSOを使用するように設定されている場合のローカルユーザ認証の有効化

第1章: はじめに

Fortify Software Security Center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。セキュリティチームと開発チームが協力して、Fortify Static Code Analyzer、Fortify WebInspect Enterprise、およびSonatypeで相互に関連するデータを共同のオンライン環境から使用できるようにすることで、セキュリティ上の欠陥を迅速で正確に解決できます。

対象ユーザ

このコンテンツは、Fortify Software Security Centerの展開および保守を担当するユーザ向けです。Fortify Software Security Centerの取得、インストール、および設定に必要なすべての情報を提供します。

ここで説明する情報は、エンタープライズアプリケーションの開発について少なくとも適度に知識を持ち、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ユーザを対象としています。対象は次のとおりです。

- システム管理者およびインスタンス管理者
- データベース管理者

Software Security Center APIドキュメントにアクセスする方法については、"Fortify Software Security Center APIドキュメントへのアクセス" ページ204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、主に2つの部分に分かれています。パート1("Fortify Software Security Centerの展開" ページ39)には、展開環境を説明し、Fortify Software Security Centerのインストールと設定の手順を説明する章が含まれています。パート2("Micro FocusFortify Software Security Centerの使用 " ページ191)には、Fortify Software Security Centerの使い方を説明する章が含まれています。

関連ドキュメント

このトピックでは、Micro Focus Fortifyソフトウェア製品に関する情報を提供するドキュメントについて説明します。

注: Micro Focus Fortifyの製品ドキュメントは、https://www.microfocus.com/support/documentationにあります。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製品およびFortify WebInspect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Micro Focus製品ドキュメントWebサイトで利用できます。

ドキュメント/ファイル名	説明
Micro Focus Fortify製品ソフトウェアのドキュメントについて About_Fortify_Docs_<*version*>.pdf	この文書では、Micro Focus Fortify製品マニュアルにアクセスする方法について説明します。 **注:** 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。
Micro Focus Fortify License and Infrastructure Managerインストールおよび使用ガイド LIM_Guide_<*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。
Micro Focus Fortifyソフトウェアシステム要件 Fortify_Sys_Reqs_<*version*>.pdf	このドキュメントでは、Fortifyソフトウェアのこの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ます。
Micro Focus Fortifyソフトウェアリリースノート FortifySW_RN_<*version*>.pdf	このドキュメントでは、Fortifyソフトウェア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。
Micro Focus Fortifyソフトウェア<*version*>の新機能 Fortify_Whats_New_<*version*>.pdf	このドキュメントでは、Fortifyソフトウェア製品の新機能について説明します。

Micro Focus Fortify ScanCentral DAST

以下のドキュメントには、Fortify 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Micro Focus製品ドキュメント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
Micro Focus Fortify ScanCentral DAST設定と使用ガイド SC_DAST_Guide_<*version*>.pdf	このドキュメントでは、Fortify ScanCentral DASTを設定および使用して、Webアプリケーションの動的スキャンを実行する方法について説明します。

Micro Focus Fortify ScanCentral SAST

以下のドキュメントには、Fortify ScanCentral SAST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Micro Focus製品マニュアルのWebサイト(https://www.microfocus.com/documentation/fortify-software-security-center)で利用できます。

ドキュメント/ファイル名	説明
Micro Focus Fortify ScanCentral SASTインストール、設定、使用ガイド SC_SAST_Guide_<*version*>.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ます。これは、リソースを大量に消費するFortify Static Code Analyzer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を対象にしています。

Micro Focus Fortify Software Security Center

以下のドキュメントには、Fortify Software Security Center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Micro Focus製品マニュアルのWebサイト(https://www.microfocus.com/documentation/fortify-software-security-center)で利用できます。

ドキュメント/ファイル名	説明
Micro Focus Fortify Software Security Centerユーザガイド SSC_Guide_<*version*>.pdf	このドキュメントでは、Software Security Centerのユーザ向けに、Software Security Centerを展開および使用する方法について詳しく説明します。Software Security Centerの取得、インストール、設定、使用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。Software Security Center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現在のステータスの概要を提供します。

Micro Focus Fortify Static Code Analyzer

以下のドキュメントには、Fortify Static Code Analyzer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Micro Focus製品マニュアルのWebサイト(https://www.microfocus.com/documentation/fortify-static-code)で利用できます。

ドキュメント/ファイル名	説明
Micro Focus Fortify Static Code Analyzerユーザガイド SCA_Guide_<*version*>.pdf	このドキュメントでは、Static Code Analyzerをインストールおよび使用して、多くの主要なプログラミングプラットフォームでコードをスキャン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。

ドキュメント/ファイル名	説明
Micro Focus Static Code Analyzerカスタムルールガイド SCA_Cust_Rules_Guide_<*version*>.zip	このドキュメントでは、Static Code Analyzer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。 **注:** 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。
Micro Focus Audit Workbenchユーザガイド AWB_Guide_<*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、バグトラッカーとの統合方法、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。
Micro Focus Fortify Eclipse用プラグインユーザガイド Eclipse_Plugins_Guide_<*version*>.pdf	このドキュメントでは、Fortify Eclipse用修復プラグインをインストールして使用する方法について説明します。
Micro Focus Fortify JetBrains IDEおよびAndroid Studio用プラグインユーザガイド JetBrains_AndStud_Plugins_Guide_<*version*>.pdf	このドキュメントでは、IntelliJ IDEAおよびAndroid Studio用のFortify分析プラグインと、IntelliJ IDEA、Android Studio、およびその他のJetBrains IDE用のFortify修復プラグインの両方をインストールして使用する方法について説明します。
Micro Focus Fortify Extension for Visual Studioユーザガイド VS_Ext_Guide_<*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。
Micro Focus Fortify Static Code Analyzerツールのプロパティリファレンスガイド SCA_Tools_Props_Ref_<*version*>.pdf	このドキュメントでは、Fortify Static Code Analyzerツールで使用されるプロパティについて説明します。

Micro Focus Fortify WebInspect

以下のドキュメントには、Fortify WebInspect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Micro Focus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
Micro Focus Fortify WebInspectインストールガイド WI_Install_<*version*>.pdf	このドキュメントでは、Fortify WebInspectの概要と、Fortify WebInspectをインストールして製品ライセンスを有効にする手順について説明します。
Micro Focus Fortify WebInspect Userユーザガイド WI_Guide_<*version*>.pdf	このドキュメントでは、Fortify WebInspectを設定および使用して、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方法について説明します。 **注:** このドキュメントは、Fortify WebInspect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。
Micro Focus Fortify WebInspect on Dockerユーザガイド WI_Docker_Guide_<*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Fortify WebInspectをダウンロード、設定、使用する方法について説明します。この製品のフルバージョンは、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)経由で設定されたヘッドレスセンサとして自動プロセスで使用することを目的としています。Fortify ScanCentral DASTのセンサとして実行し、Fortify Software Security Centerと組み合わせて使用することもできます。

ドキュメント/ファイル名	説明
Micro Focus Fortify WebInspect ツールガイド WI_Tools_Guide_<*version*>.pdf	このドキュメントでは、Fortify WebInspectおよびFortify WebInspect Enterpriseにパッケージ化されたFortify WebInspectの診断および侵入テストツールと設定ユーティリティの使用方法について説明します。
Micro Focus Fortify WebInspect Agentインストールガイド WI_Agent_Install_<*version*>.pdf	このドキュメントでは、サポート対象サーバまたはサービス上のサポート対象Java Runtime Environment (JRE)で実行されているアプリケーション、およびサポート対象バージョンのIIS上のサポート対象.NET Frameworkで実行されているアプリケーションのためにFortify WebInspect Agentをインストールする方法について説明します。
Micro Focus Fortify WebInspect Agentルールパックキットガイド WI_Agent_Rulepack_Guide_<*version*>.pdf	このドキュメントでは、Fortify WebInspect Agentルールパックキットの検出機能について説明します。Fortify WebInspect Agentルールパックキットは、Fortify WebInspect Agent上で実行され、実行中の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。Fortify WebInspect Agentルールパックキットは、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。

Micro Focus 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Micro Focus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
Micro Focus 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 Software Security CenterやFortify WebInspectとの統合、およびインストールのトラブルシューティングについて説明します。また、Fortify WebInspect Enterpriseシステムのコン

ドキュメント/ファイル名	説明
	ポーネントの設定方法についても説明します。これには、Fortify WebInspect Enterpriseのアプリケーション、データベース、センサ、およびユーザが含まれています。
Micro Focus 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Fortify WebInspect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ます。 **注:** 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。
Micro Focus Fortify WebInspectツールガイド WI_Tools_Guide_<*version*>.pdf	このドキュメントでは、Fortify WebInspectおよびFortify WebInspect Enterpriseにパッケージ化されたFortify WebInspectの診断および侵入テストツールと設定ユーティリティの使用方法について説明します。

Micro Focus Fortify Software Security Center 21.2.0の新機能

自動設定の変更

自動設定のパフォーマンス、安全性、および使い方は、チェックサムの計算と比較によって改善されました。詳細については、"Fortify Software Security Centerの設定の自動化" ページ409を参照してください。

システム環境の使用状況の変更

これまで、すべてのシステム環境変数値は、app.propertiesファイル内の変数に設定された値をオーバーライドしていました。このリリースの時点では、システム環境変数は一部のシステムプロパティのデフォルト値を提供し、*<app.context>*.autoconfigファイルの［appProperties］および［datasourceProperties］セクションの設定を上書きできます。

静的/動的な問題相関インジケータの導入

アプリケーションバージョンで静的スキャンと動的スキャンを実行し、その結果をFortify Software Security Centerにアップロードすると、［AUDIT］ページで特定の問題に対する静的および動的な結果が相関しているか(記号⇄でタグ付け)確認できます。相関の記号は、問題が静的スキャンと動的スキャンの両方によって明らかにされたかどうかを示します。詳細については、"監査する問題に関する情報の表示" ページ305を参照してください。

LDAPエンティティの識別名の更新

現在、Fortify Software Security Centerで使用するように設定されているLDAPサーバの識別名が変更された場合、関連付けられたLDAPエンティティの識別名の値を更新できます。詳細については、"LDAPエンティティの識別名の更新" ページ121を参照してください。

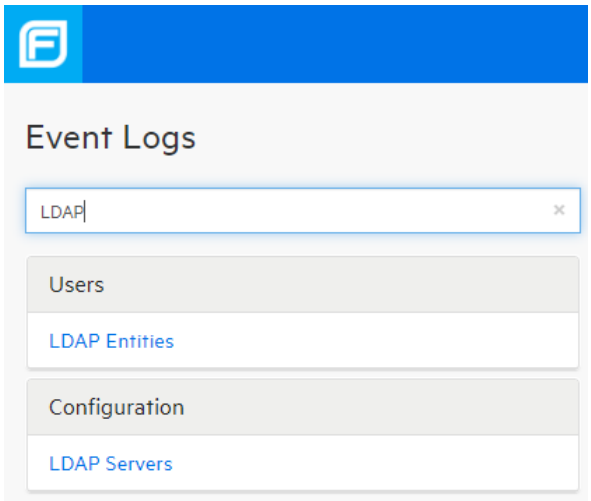
LDAPサーバからのユーザステータスマッピングのサポート

以前は、LDAPユーザが無効になっているか、LDAPサーバからロックアウトされている場合、LDAPに対する認証が失敗しました。トークン認証とSSO認証はLDAPサーバに対して直接認証できなかったので、ユーザステータスはデフォルトでisDisabled = false, isLocked=falseになっていました。したがって、コードはユーザステータスをチェックしますが、常に正常な認証が可能でした。このリリースでは、管理者はLDAPからFortify Software Security Centerのユーザオブジェクトにユーザステータス属性をマップできます。これにより、既存の認証チェックが正しく動作するようになりました。詳細は、"LDAPサーバの設定" ページ108を参照してください。

[ADMINISTRATION]ページの [Searchable Navigation]ペイン

必要なページに到達するために、 [ADMINISTRATION]ナビゲーションペインでノードを展開する必要がなくなりました。現在は、ナビゲーション画面の上にある新しい検索ボックスに文字列を入力して、開くページを見つけることができるようになりました。

たとえば、「LD」と入力すると、 [LDAP Entities]および [LDAP Servers]ページへのリンクが表示されます。



日付形式の変更

Fortify Software Security Centerユーザインタフェースに表示される日付の形式を変更できるようになりました。詳細については、"環境設定:システム全体とアプリケーションバージョン間" ページ198を参照してください。

ScanCentral SASTコントローラの保守モードへの移行とセンサのシャットダウン

ScanCentral SAST Controllerを新たに導入された保守モードに設定し、センサ上で実行されているスキャンのデータが失われるのを防ぐことができるようになりました。ScanCentral SAST Controllerセンサは、個別にシャットダウンするか、バッチでシャットダウンできます。詳細については、"ScanCentral SAST Controllerを保守モードにする" ページ362」および"センサの安全なシャットダウン" ページ362を参照してください。

新しい役割または編集された役割への依存許可の追加

以前は、依存関係(追加の許可)を新しい役割または編集された役割に手動で追加する必要がありました。役割に許可を追加すると、指定した許可に必要な追加の許可がFortify Software Security Centerによって一覧表示されるようになり、その許可の内容を正確に把握できるようになりました。また、新しい [ADD MISSING PERMISSIONS]ボタンを使用して、これらの依存関係を役割に追加できます。詳細については、"カスタム役割の作成" ページ208を参照してください 。

アーティファクトのRulepackの詳細

以前は、[ARTIFACTS]ページでスキャンのアーティファクトを調べると、スキャンの生成にどのバージョンのFortify Static Code Analyzerが使用されたかが確認できましたが、使用されているRulepackのバージョンは表示できませんでした。このリリースにより、スキャンの生成に使用されたRulepackのバージョンと、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バージョン別にグループ化して表示できます。詳細については、"スキャンアーティファクトの詳細の表示" ページ290を参照してください。

パートI: Fortify Software Security Centerの展開

次の章では、Fortify Software Security Centerの展開環境について説明し、Fortify Software Security Centerのインストールと設定の手順について説明します。

第2章: 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Fortify Software Security Center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、Fortify Software Security Centerファミリ製品が提供するセキュリティ脆弱性の集中的な要約により、さらに高レベルのセキュリティ保護された展開が必要になる可能性があります。

このセクションのトピックでは、Fortify Software Security Centerを安全に展開する方法の一部を要約しています。

施設へのアクセスのセキュリティ保護

Fortify Software Security Center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として保存および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さまざまな機会を提供します。このため、Fortifyでは、管理者がFortify Software Security Centerを安全な運用施設で展開することを推奨しています。また、基礎となるFortify Software Security Centerファイルシステムを保護し、Fortify Software Security Center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があります。

Tomcatサーバのセキュリティ保護

Fortify Software Security Center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証明書と共にHTTPSを使用するように、Tomcatサーバを設定します。また、運用環境で、Tomcatサーバを保護するために必要な追加の手順を実行します。

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、一部のクッキーの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。

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(フラグ)を追加することを推奨します。

- `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るのを防ぎます。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を通じてクッキー値にアクセスされるのを防ぎます。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、Fortifyではこの属性を有効にすることを推奨します。

`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。

HTTPSおよびSSL通信の使用について

すべての通信にHTTPSおよびセキュアソケットレイヤ(SSL)を使用するようにFortify Software Security CenterおよびFortifyクライアント製品(Audit Workbench、fortifyclient、Eclipse Completeプラグイン、Visual Studio拡張機能を含む)を設定することを強く推奨します。

HTTPSを使用してFortify Software Security Centerと通信するためのFortify Static Code Analyzerツールの設定

VeriSign、Entrust、Thawteなどの信頼されているルート認証局で購入および署名された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Fortify Software Security Centerと通信するためにクライアント側では何もする必要がありません。これらの証明書は信頼されています。これらのルートCA証明書がFortifyクライアント製品の使用するキーストア内にあるためです。

ただしデフォルトでは、Fortify Software Security Center、Audit Workbench、fortifyclient、Eclipse Completeプラグイン、およびVisual Studio拡張機能は、自己署名証明書または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Fortify Software Security Centerと通信するには、自己署名証明書またはローカル署名証明書を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。

重要 サードパーティの認証局を使用してローカル署名証明書を発行した場合は、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署名証明書をFortify Software Security CenterおよびFortify Static Code Analyzerツールが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実行します。

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 "<sca_install_dir>\jre\bin"
keytool -import -alias SSC -keystore ..\lib\security\cacerts -file
"YourCertFile.cer" -trustcacerts
```

ここで、`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Tomcatサーバで使用され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 -export -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。

詳細情報

java keytoolを使用して対話式に自己署名証明書を作成すると、姓名の入力を求めるプロンプトが表示されます。Fortify Software Security Center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。単に短いホスト名や「localhost」は使用しないでください。

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。

パスワードとユーザ役割のセキュリティ保護について

Fortify Software Security Centerを展開して初めてログインした後、直ちに新しいローカル管理者アカウントを1つ以上作成してから、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ます。Fortify Software Security Centerへのログイン方法については、"Fortify Software Security Centerへのログイン" ページ75を参照してください。

Fortify Software Security Centerの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した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

Fortify Software Security Centerアカウント管理の詳細については、"ユーザアカウントの管理" ページ207を参照してください。

LDAPを使用してFortify Software Security Center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。LDAP認証を使用するようにFortify Software Security Centerを設定する方法については、"LDAPユーザ認証" ページ105を参照してください。

コンピュータサービスとアカウントの管理

Fortify Software Security Center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、Fortify Software Security Centerではユーザアカウントからコンピュータの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

するために、Fortify Software Security Centerをホストするコンピュータに更 新 されたウイルス対 策 ソフトウェアを常 にインストールして実 行 します。

第3章: Fortify Software Security Centerの展開の準備

このセクションでは、初めてFortify Software Security Centerを展開するための準備をする方法について説明します。

大まかな展開タスク

次の表は、Fortify Software Security Centerの展開の準備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。また、これらのタスクを説明するトピックへのリンクも表示されています。

注: Fortify Software Security Centerをアップグレードする場合は、"Fortify Software Security Centerのアップグレード" ページ181を参照してください。

タスク	説明	情報と手順
1	Fortify Software Security Centerソフトウェアファイルと`fortify.license`ファイルをダウンロードします。	"Fortify Software Security Center ファイルをダウンロードする" ページ51
2	インストールバンドルを解凍して展開します。次に、TomcatサーバにFortify Software Security Centerを展開します。	"Fortify Software Security Centerソフトウェアの解凍と展開" ページ51
3	Fortify Software Security Centerデータベースに使用する予定のデータベースサーバ用のソフトウェアをインストールして設定します。	"Fortify Software Security Centerデータベースについて" ページ59
4	Fortify Software Security Centerにログインします。("Fortify Software Security Centerへのログイン" ページ75を参照してください)。	"Fortify Software Security Centerへのログイン" ページ75
5	Fortify Software Security Centerセットアップウィザードを使用して初期設定を実行します。(Fortifyライセンスを見つける、Fortify Software Security Centerデータベーステーブルを作成しデータベーススキーマを初期化する、データベースをシードするなど)。	"Fortify Software Security Centerの初回設定" ページ69
6	Fortify Software Security Centerサーバを再	

タスク	説明	情報と手順
	起動します。	
7	[ADMINISTRATION]ビューでFortify Software Security Centerの設定を完了します。(管理ビューで設定するオプションのリストについては、" [ADMINISTRATION]ビューで使用可能な環境設定オプション" ページ81を参照してください)。	"追加のFortify Software Security Center設定" ページ79
8	Eclipseプラグイン更新サイトの設定、バグトラッカ統合の設定、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" ページ159

Fortify Software Security Centerを削除する予定で、Fortify Software Security Centerデータベースが不要になった場合に完全に削除する方法については、"Fortify Software Security Centerデータベースの永久削除" ページ67を参照してください。

展開の概要

Fortify Software Security Center は、Fortify解析製品とツール(Fortify Static Code Analyzer、Fortify WebInspect Agent、Fortify ScanCentral、Audit Workbench)をSecure Development Lifecycle (SDL)全体で使用して収集および処理されたアプリケーションデータの一元的な管理と解析の機能を提供します。

Fortify Software Security Center 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、Fortify Software Security Center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 Fortify Software Security Center 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。

初期 Fortify Software Security Center 設定が完了したら、コアパラメータの設定を完了し、追加の設定をADMINISTRATIONビューから行います。手順については、"追加のFortify Software Security Center設定" ページ79を参照してください。

重要 1つの Fortify Software Security Center インスタンスの展開だけがサポートされています。さらに、そのインスタンスをロードバランサの背後に置いてはなりません。

システム要件については、ドキュメント『Micro Focus Fortifyソフトウェアシステム要件』を参照してください。

一元的管理を提供するために、Fortify Software Security Centerは次の外部コンポーネントと相互運用します。

- 必要なコンポーネント
  - Apache Tomcatサーバ
  - サードパーティデータベース
  - Fortify Security Contentサーバ
- オプションのコンポーネント
  - サードパーティのLDAP認証サーバ
  - 欠陥トラッキングシステム
  - パーサプラグイン
  - SMTP電子メールサーバ
  - 1つ以上のFortify解析エージェントおよびツール
  - Kubernetes

Fortify Software Security Centerとのコンポーネントの統合について

次のコンポーネントをFortify Software Security Centerと統合できます。

コンポーネント	統合手順
System for Cross-domain Identity Management (SCIM)	"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" ページ128 "SCIM/Azure AD統合のためのSSM 2.0シングルサインオンの設定" ページ145
Fortify Audit Assistant	"Audit Assistantの設定" ページ87
Java Message Service (JMS)	"Java Message Service設定の設定" ページ104
LDAPサーバ	"LDAPサーバの設定" ページ108
シングルサインオン(SSO)プロバイダ: • Central Authentication Server (CAS) • SPNEGO/Kerberos	"Central Authorization Serverを使用するためのFortify Software Security Centerの設定" ページ140 "Fortify Software Security CenterでのKerberos認証の設定" ページ151

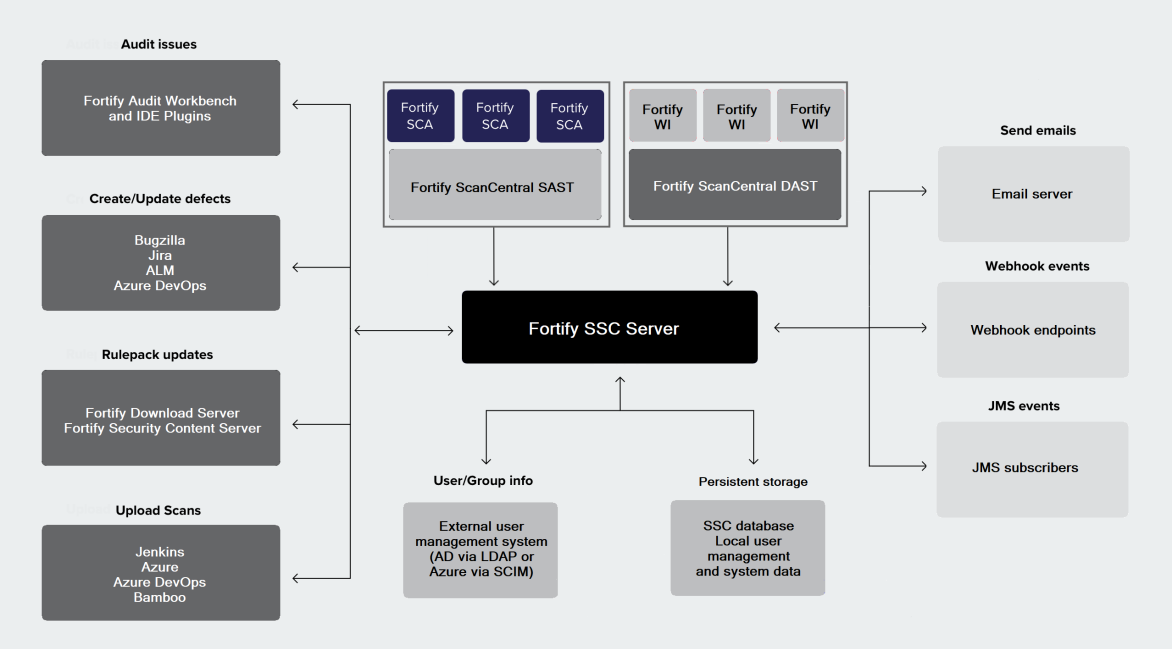
コンポーネント	統合手順
• SAML	"SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141
	"SCIM/Azure AD統合のためのSSM 2.0シングルサインオンの設定" ページ145
• HTTP	"HTTPヘッダを使用するシングルサインオンおよびシングルログアウトソリューションを使用するためのFortify Software Security Centerの設定" ページ149
• x509	"X.509証明書ベースのSSOを使用するためのFortify Software Security Centerの設定" ページ153
Fortify ScanCentral SAST	"Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設定" ページ130
Fortify ScanCentral DAST	"Fortify Software Security Centerを使用したScanCentral DASTスキャンの実行と管理の有効化" ページ131
Fortify Static Code Analyzerツール:	
• Fortify Audit Workbench	Micro Focus Fortify Audit Workbenchユーザガイド
• Fortify Jenkinsプラグイン	`https://www.microfocus.com/documentation/fortify-jenkins-plugin/`
• Eclipseプラグイン	Micro Focus Fortify Plugins for Eclipseユーザガイド
• Fortify Extension for Visual Studio	Micro Focus Fortify Extension for Visual Studioユーザガイド
• Fortify Extension for Visual Studio Code	`https://www.microfocus.com/documentation/fortify-visualstudio-code`
• Fortify Bambooプラグイン	`https://www.microfocus.com/documentation/fortify-plugin-for-bamboo/`
• Fortify Plugins for JetBrains IDEsおよび	Micro Focus Fortify Plugins for JetBrains IDEsおよびAndroid Studioユーザガイド

コンポーネント	統合手順
Android Studio	
• Fortify SourceAndLibScanner	Fortify Marketplace (`https://marketplace.microfocus.com/fortify`)からFortify SourceAndLibScannerをダウンロードしてください。このソフトウェアパッケージにドキュメントが付属しています。
Azure DevOps Extension	https://www.microfocus.com/documentation/fortify-azuredevops-extension
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" ページ 84

重要 他のFortify製品(ScanCentral DAST、Audit Workbenchなど)とFortify Software Security Centerを統合する場合は、通信するコンピュータ間のクロックスキューを最小限に抑えてください。NTP(Network Time Protocol)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、Fortify Software Security Centerに対する要求が失敗する可能性があります。

Fortify Software Security Centerインストール環境

次の図は、"展開の概要" ページ45に記載されている必須コンポーネントとオプションコンポーネントとFortify Software Security Centerとの関係を示しています。



次の表に、この図に示している必須およびオプションのFortify Software Security Centerインストールコンポーネントについて説明します。

コンポーネント	説明
1	Fortify Software Security Center Fortify Software Security Center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。
2	ユーザおよびアーティファクトデータを保存するためにFortify Software Security Centerで必要なサードパーティデータベース。Fortify Software Security Center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。
3	サードパーティのLDAP認証サーバ (オプション) LDAP認証を使用するようにFortify Software Security Centerを設定できます。

コンポーネント	説明
欠陥トラッキングサーバ	(オプション) Bugzilla、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できるようにFortify Software Security Centerを設定できます。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" ページ397を参照してください。
サードパーティの電子メールサーバ	(オプション)外部SMTP電子メールサーバを使用してアプリケーションの共同作業者にアラートを送信するようにFortify Software Security Centerを設定できます。
Fortify Static Code Analyzer分析エージェント	(オプション) Fortify Static Code Analyzerを使用してソースコードをスキャンし、問題を特定します。
Audit Workbenchソースコード監査ツール	Audit Workbenchは、SCAおよびアプリと一緒にインストールし、代替のソースコード監査ツールとして使用できます。
Fortify ScanCentral SAST	(オプション) Fortify Static Code Analyzerユーザは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コンピュータからこの目的のために提供されるコンピュータ(センサ)のグループにオフロードできます。
Fortify ScanCentral DAST	(オプション) Webアプリケーションの動的スキャンを設定し、Fortify Software Security Centerから実行するために使用できる動的なアプリケーションセキュリティテストツールです。
Fortify WebInspect Enterprise	(オプション) 潜在的で動的な問題を取得するために、Fortify WebInspectエージェントに接続する分析エージェント。
Fortifyダウンロードサーバ	インストールプログラムの取得に使用されます。
Fortify Security Content更新サーバ	Security Contentの取得および更新に使用されます。

重要 複数のFortify Software Security Centerサーバ間の負荷分散はサポートされていません。

Fortify Software Security Center ファイルをダウンロードする

Fortifyソフトウェアをダウンロードできるのは、Micro Focus Software Licenses and Downloads (SLD) ポータル(https://sld.microfocus.com)からだけです。そこで提供されているFortifyソフトウェアインストールパッケージの詳細については、ドキュメント『Micro Focus Fortifyソフトウェアシステム要件』を参照してください。

インストールファイルと`fortify.license`ファイルを、ドキュメント『Micro Focus Fortifyソフトウェアのシステム要件』の指示に従ってダウンロードします。役に立つハウツー動画(https://www.brainshark.com/mfLD/vu?pi=zFszsRA7ezW1H3z0&nodesktopflash=1)にもFortifyソフトウェアをダウンロードする方法の手順が説明されています。

次を参照

"Fortify Software Security Centerソフトウェアの解凍と展開" 下

Fortify Software Security Centerソフトウェアの解凍と展開

Fortify Software Security Centerインストールファイルを解凍して展開するには、次の手順に従います。

1. インストールファイルの内容を安全な場所の一時ディレクトリに抽出します。(インストールファイルは、"Fortify Software Security Center ファイルをダウンロードする" 上の手順に従ってダウンロードしたファイルです)。
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のディレクトリに抽出します。これにより、Fortify Software Security Center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`Fortify-Server-WAR`ディレクトリが作成されます。

   注: 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_install_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`フォルダから`<ssc_install_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。

   注: リソースファイルを`<ssc_install_dir>`ディレクトリにコピーする必要はありません。ただし、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行われます。

   次の表で、シードバンドルについて説明します。

ファイル名	説明
`Fortify_`	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

ファイル名	説明
`Process_Seed_Bundle-2021_Q4_0001.zip`	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-2021_Q4_0001.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Fortify Software Security Centerレポートセットが提供されます。
`Fortify_PCI_Basic_Seed_Bundle-2021_Q4_0001.zip`	(オプション)PCI Basic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。PCI DSSは、2021年6月から2022年10月の期間の既存開始評価と新規開始評価を引き続き受け入れます。2022年10月以降、新しいPCI Software Security Framework(SSF)が評価基準のセットになる予定です。これらの新しい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理解するために、PCI SSF Basicシードバンドル(`Fortify_PCI_SSF_Basic_Seed_Bundle-2021_Q4_0001.zip`)を使用してください。
`Fortify_PCI_SSF_Basic_Seed_Bundle-2021_Q4_0001.zip`	(オプション)PCI SSF Basic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に使用される一連の新しい標準として、2019年6月に導入されました。既存のPCI DSSは、2021年6月から2022年10月の期間の既存開始評価と新規開始評価を引き続き受け入れます。2022年10月以降、新しいPCI Software Security Framework(SSF)が評価基準のセットになる予定です。PCI DSSでの評価には、PCI Basicシードバンドル(`Fortify_PCI_Basic_Seed_Bundle-2021_Q4_0001.zip`)を使用してください。

Fortify Software Security Centerの展開には、プロセステンプレートシードバンドルとレポートシードバンドルが必要です。PCI Basicシードバンドルはオプションです。

4. `fortify.license` ファイルを `<ssc_install_dir>` ディレクトリにコピーします。(`fortify.license`ファイルの取得方法については、Micro Focus Fortifyソフトウェアシステム要件のドキュメントを参照してください)。

Fortify Software Security CenterをKubernetesクラスタへ展開する

次の手順では、Fortify Software Security CenterのKubernetes展開を準備して実行する方法について説明します。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、このリリースのドキュメント『Micro Focus Fortifyソフトウェアシステム要件』を参照してください。

注: Fortify Software Security Center設定の自動化については、"Fortify Software Security Centerの設定の自動化" ページ409を参照してください。Kubernetesクラスタへの展開の場合、すべての標準バンドルが含まれているので、それらを提供したり`<app_context>.autoconfig`ファイルに一覧する必要はありません。また、Fortify Software Security Center Dockerイメージ(`fortifydocker/sscwebapp`)は`SSC_AUTOCONFIG_SEARCHINDEX_LOCATION`システム環境変数を設定するため、Kubernetes展開では、グローバル検索が自動設定で使用する場合にデフォルトで有効になっています。

Fortify Software Security CenterのKubernetes展開を準備するには、次の手順を実行します。

1. kubectlをインストールして設定します。手順については、https://kubernetes.io/docs/tasks/tools/install-kubectlを参照してください。
2. Helmをインストールします。(ソフトウェアをダウンロードするには、https://github.com/helm/helm/releasesを参照してください。インストール手順については、https://helm.sh/docs/intro/installを参照してください。)
3. (エアギャップされたインストールのみ)Dockerをインストールします。インストール手順については、https://docs.docker.com/get-dockerを参照してください。
4. Fortify Software Security Center配布ZIPファイルのhelmディレクトリの内容を*<ssc_helm_dir>*ディレクトリに展開します。`<ssc_helm_dir>`ディレクトリに移動して、`ssc-values-example.yaml`ファイルを`ssc-values.yaml`にコピーします。

Fortify Software Security CenterのKubernetes展開

Fortify Software Security Center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、Fortify Software Security CenterDockerイメージ(fortifydocker/ssc-webapp)をDocker Hubレジストリから取得できます。アプリケーションをエアギャップされた環境に展開しなければならない場合は、プライベートレジストリを展開に使用して、そこにSSC Dockerイメージを転送する必要があります。

Fortify SSCをKubernetesクラスタに展開する

Fortify Software Security Centerをインターネットにアクセスできる環境に展開するために使用する手順は、エアギャップされた環境に展開する手順とほぼ同じです。唯一の違いは、エアギャップ展開では、Fortify SSCイメージを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プッシュする必要がある点です。

Fortify Software Security Center 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Fortifyカスタマサポート (https://www.microfocus.com/support)に伝えます。

   注: Fortifyカスタマサポートから、Docker Hub (fortifydocker組織)上のFortifyリポジトリへのアクセス権が与えられます。

2. Docker Hubレジストリに公開されているFortify Software Security Center 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 fortifydocker@microfocus.com へ送信します。
   - 名
   - 姓
   - 会社名
   - Docker ID
   - カスタマID
3. (エアギャップされたインストールの場合、またはプライベートレジストリを使用する場合。実行中のDockerサーバとDockerクライアントが想定されます。)Fortify SSCイメージをプライベートレジストリへ、次のようにして転送します。
   a. Docker Hubに `docker login` を使用してログインします。
   b. プライベートレジストリにログインする際に使用する `docker login <priv_reg_host_and_port>` 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。
   c. SSC Dockerイメージを、次のようにして転送します。
      i. `docker pull"fortifydocker/ssc-webapp:<tag>"`
      ii. *`docker tag"fortifydocker/ssc-webapp:<tag>""<priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"`*
      iii. `docker push "<priv_reg_host_and_port>/<priv_reg_path>/ssc-webapp:<tag>"`

      注: <Tag>に使用する値を調べるには、ディレクトリに移動して*tag*>に使用する値を調べるには、*<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 *<ssc_version>.<imageBuildNumber>* の形式で用意されています。

      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チャート値で指定する必要があります。

重要 イメージ名(`ssc-webapp`)とタグ(*<tag>*)の値は同じでなければなりません。

4. *<priv_reg_host_and_port>/<priv_reg_path>/* を *<ssc_helm_dir>*`/ssc-values.yaml` ファイルで `image.repositoryPrefix` パラメータの値として入力します。(`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。
5. 正確なイメージビルドタグを使用する場合は、*<imageBuildNumber>*値を `image.buildNumber` の値として入力します。それ以外の場合は、空のままにします。
6. 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` の場合、形式は次のようになります:

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

   注: `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。

7. 展開に必要なデータを含む別のKubernetesシークレットをプロビジョニングします。`secretRef.keys` ファイルを調べて受諾されたデータのリストを探します。最小限必要なセットは、`httpCertificateKeystoreFileEntry`、`httpCertificateKeystorePasswordEntry`、および `httpCertificateKeyPasswordEntry` です。

   シークレットを手動で作成する方法の例:

   a. *<ssc_secrets_dir>* ディレクトリを作成し、入力する `secretRef.keys` のキーごとに、*<ssc_secrets_dir>*で値を含むファイルを作成します。たとえば、`httpCertificateKeystoreFileEntry`の場合、必要なファイルはキーストアを含み、`httpCertificateKeystorePasswordEntry`の場合、必要なファイルはパスワードを含んでいます。

   b. `kubectl` コマンドを使用してシークレットを作成します。

      ```
      kubectl create secret generic "<ssc_secret_name>" --from-file
      "<ssc_secrets_dir>"
      ```

   c. *<ssc_helm_dir>*`/ssc-values.yaml` ファイルで *<ssc_secret_name>* を `secretRef.name` パラメータの値として入力します。

   d. *<ssc_secrets_dir>* で指定されたファイルごとに、ファイル名を *<ssc_helm_dir>*`/ssc-values.yaml` ファイル内の関連する `secretRef.keys.*Entry` パラメータの値として入力します。

注: シークレット内の変更は、展開によって自動的には適用されません。変更されたシークレットを既存の展開で使用するには、Fortify Software Security Centerポッドを手動で削除して自動再作成をトリガする必要があります。

8. 必要な他のパラメータを *<ssc_helm_dir>*/ssc-values.yaml ファイルに入力します。
   - urlHost は Fortify Software Security Center 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。Fortify Software Security Center インストールにアクセスするためのアドレスは <https://*<urlHost>*:*<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/)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 により参照された Fortify Software Security Center シークレットに変更を適用するには、ssc-webappポッドを手動で削除する必要があります(後で自動的に再作成されます)。

   注: : 必要に応じて、*<ssc_helm_dir>*/ssc-values.yamlファイルでパラメータに指定する値のほどんどを後で変更して、その後で Fortify Software Security Center 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。

展開

初めて Fortify Software Security Center 展開するには、次のコマンドを実行します。

```
helm install "<unique_deployment_name>" "<ssc_helm_dir>/ssc-<chart_version>+<ssc_version>.tgz" -f "<ssc_helm_dir>/ssc-values.yaml"
```

それ以降の展開では、次のコマンドを実行します。

```
helm upgrade "<unique_deployment_name>" "<ssc_helm_dir>/ssc-<chart_version>+<ssc_version>.tgz" -f "<ssc_helm_dir>/ssc-values.yaml"
```

次に、デフォルトの管理者アカウントを使用して Fortify Software Security Center にログインして、インストール後の設定を、標準インストールの後に行なうのと同じように実行します。詳細については、"Fortify Software Security Centerの初回設定" ページ69 を参照してください。

fortify.home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Fortify Software Security Centerリソースが存在する場所です。Fortify Software Security Centerの展開後は、次の場所にあります。

- Windowsシステムの場合は%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)

  注: %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システムの場合は$HOME/.fortify

注: これらはデフォルトディレクトリです。設定時にセットアップウィザードを使用して別のディレクトリを指定できます ("Fortify Software Security Centerの初回設定" ページ69を参照してください)。

ディレクトリ構造

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.xmlversion.propertiessecret.keylogs/ssc.log...init.token

              ...

plugin-framework/

fortify.license
```

ここで

log4j2.xml	オンザフライで変更できるログ設定です。
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表します。Fortify Software Security Centerを設定するユーザは、このトークンを使用して

	URL`<host>:<port>/init` のセットアップウィザードにアクセスします。
`app.properties`	お客様が設定(`ssc.properties`から抽出)できるアプリケーションプロパティを含むファイルです。
`datasource.properties`	データベース接続プロパティを含むファイルです。
`version.properties`	アプリケーションのアップグレードを目的として、Fortify Software Security Center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。
`secret.key`	Fortify Software Security Center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 (このファイルはFortify Software Security Centerによって上書きされません。ただし、`<fortify.home>/<app_context>/conf`ディレクトリで見つからない場合は生成されます)。 `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。Fortify Software Security Center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。
`plugin-framework`	プラグインフレームワーク設定と一時ストレージ(内部)です。
`fortify.license`	Fortify Software Security Centerのライセンスファイルです。

重要 `<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`
- `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は、Fortify Software Security Centerで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。

Fortify Software Security Centerデータベースについて

Fortify Software Security Center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。

重要 Fortify Software Security Center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。

重要 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、"Microsoft SQL Serverデータベースの使用" ページ61または"MySQLデータベースの設定" ページ62を参照してください。

その後、初めてFortify Software Security Centerに進んだ後、Fortify Software Security Centerセットアップウィザードを使用してデータベースへのコネクティビティを設定し、データベースをシード処理します ("Fortify Software Security Centerの初回設定" ページ69を参照してください)。

このセクションで説明するトピック:

JDBCドライバについて

SQL Server、MySQLサーバ、およびOracle用のJDBCドライバは、Fortify Software Security Center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への接続に使用されます。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。MariaDBは、Fortify Software Security Centerのバックエンドデータベースとしてサポートされていません。

Fortify Software Security Centerデータベース文字セットのサポートについて

Fortify Software Security Centerがサポートする各サードパーティのデータベースタイプでサポートされる文字セットのリストについては、ドキュメント『Micro Focusのソフトウェアシステム要件』を参照してください。

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、ドキュメント『Micro Focus Fortifyソフトウェアシステム要件』を参照してください。

データベースユーザアカウント権限

Fortify Software Security Center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、次の操作を行う権限が必要です。
  - 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

  重要 マイグレーションスクリプトの実行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。

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

  重要 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、次の操作を行う権限が必要です。
  - マイグレーションスクリプトを実行するユーザが権限を持つすべてのタスクを実行する。
  - 専用インスタンスにFortify Software Security Centerデータベースを作成する。
  - 既存のFortify Software Security Center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Fortify Software Security Centerユーザアカウントをバインドする。
  - Fortify Software Security Center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権限をFortify Software Security Center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、Fortify Software Security Center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レポートの拡張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" ページ93を参照)。

データベース固有の設定要件

次のトピックでは、Fortify Software Security Centerで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、Fortify Software Security Center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。

Microsoft SQL Serverデータベースの使用

Fortify Software Security CenterデータベースとしてSQL Serverデータベースを使用している場合は、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(https://docs.microsoft.com/en-us/sql/?view=sql-server-ver15)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*。

  注意 Fortify Software Security Center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。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ない*場合は、Fortify Software Security Centerが正常に動作しません。

  重要 Fortify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、Fortify Software Security Center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、https://docs.microsoft.com/en-us/sql/connect/jdbc/building-the-connection-url?view=sqlserver-ver15#Connectingintegratedを参照してください。
3. `JDK_JAVA_OPTIONS`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`mssql-jdbc_auth-<version>-<arch>.dll`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. 次に、次のいずれかを実行します。
   - `ssc.autoconfig`ファイルを使用して、Fortify Software Security Centerを設定します。
   - SQL認証を使用してFortify Software Security Centerを設定してから、`datasource.properties`ファイルから`db.username`および`db.password`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。

MySQLデータベースの設定

Fortify Software Security CenterデータベースとしてMySQLを使用している場合は、MySQLオプションファイルを設定する必要があります。

注意 Fortify Software Security Center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、Fortify Software Security Centerが正常に動作しません。

注: MySQLのサポートされているバージョンの詳細については、ドキュメント『Micro Focus Fortifyソフトウェアシステム要件』を参照してください。

ヒント: SSLを使用してFortify Software Security CenterをMySQL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オプションファイルを設定するには、次の手順を実行します。

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。

ヒント: オプションファイルと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。

  注: MySQL 8.0のデフォルトの場所は`c:\ProgramData\MySQL\MySQLServer 8.0`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、次の表の設定を設定します。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_lock_wait_timeout`	`300` (推奨)秒で表す
`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、おおよそ次のとおりです。 `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、コンピュータ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

設定	値
	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、そのサイズに大まかに比例します。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、10GBのバッファプールの初期化に約6秒かかります。MySQL 8.0のリファレンスマニュアル (https://dev.mysql.com/doc/refman/8.0/en)を参照してください。
sql_mode	TRADITIONAL
default_storage_engine	INNODB
max_allowed_packet	1G

6. ファイルを保存し、MySQLサーバを再起動します。

Oracleデータベースの設定

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。

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

OracleをFortify Software Security Center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。

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、データの管理性と可用性が向上します。(`partitioning.sql`スクリプトは、Oracleハッシュパーティションを使用して［SCAN_ISSUE、ISSUECACHE］および ［ISSUECACHE］テーブルをパーティショニングします)。

Oracleデータベースのパーティションの準備

`partitioning.sql`スクリプトを実行する前に、次の操作を行います。

1. データベースをバックアップします。
2. 補助テーブルスペースを作成します。(必要な補助テーブルスペースサイズを決定するには、`partitioning.sql`スクリプトを実行できます。
3. データに最も適合するパーティションの数を決定します。

   パーティショニングは、アプリケーションのバージョンIDに基づいて行います。レコードをハッシュパーティション間で均等に分散する必要があります。理想的には、アプリケーションバージョンと同じ数のパーティションを指定します。また、パーティションの数は、アプリケーションバージョンの数を増やすことを可能にする必要があります。

   1つのパーティションに数十万レコードを超えないレコードの分配の実現を試みてください。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推奨します。
4. データをパーティション化するのに十分なアプリケーションのダウンタイムをスケジュールします。その際には、次の場合に必要な時間を検討します。
   - データベースのパーティション

     重要 サポートされているパーティションの最大数は700です。これより多くを要求すると、Oracleパーティショニングスクリプトは失敗します。
   - データを補助テーブルスペースに移動する
   - データを元のテーブルスペースに戻す

データベースのパーティショニング

パーティショニングスクリプトを使用するには、次の手順に従います。

- `<ssc_distribution>/sql/oracle/extra`ディレクトリ内にあるOracleパーティショニングスクリプト(`partitioning.sql`)を実行するには、Oracle SQL*Plusクライアントを使用します。

注: スクリプトの実行時間は、データベースのサイズによって異なります。

スクリプトの実行中:

- 必要なパラメータは標準入力から取得されます。
- パーティション化されたテーブルは、補助テーブルスペース(*_PART名)で作成されます。
- データが元のテーブルスペースから補助テーブルスペースおよびパーティション化されたテーブルに移動されます。
- パーティション化されたテーブルに新しいパーティションインデックスが作成されます(*_PART名)。
- 元のテーブルとインデックスの名前が変更されます(*_NPART名)。
- パーティション化されたテーブルとインデックスの元の名前が復元されます(*_PART名が削除されます)。
- 元のテーブル(*_NPART)はドロップされます。
- パーティション化されたテーブルは元のテーブルスペースに戻されます。

ジョブ実行スレッド数の増加

データベースをパーティション分割した後、次のようにジョブ実行スレッドの数を増やしてください。

1. テキストエディタで`<fortify_home>/<context>/conf`に移動して`app.properties`ファイルを開きます。
2. `jobs.threadCount`プロパティの値を増やします。

   注: テストでは、`jobs.threadCount`の値を18に増やすとパフォーマンスが大幅に向上しました。
3. `app.properties`ファイルを保存して閉じます。

Fortify Software Security Centerデータベーステーブルおよびスキーマについて

Fortify Software Security Centerインストールディレクトリには、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スクリプトが含まれます。初期設定時("Fortify Software Security Centerの初回設定" ページ69を参照)、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、Fortify Software Security Centerのデータベーススキーマを初期化します。

Fortify Software Security Centerを初めて設定する前に、次のセクションに含まれ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権限" ページ60
- "データベース固有の設定要件" ページ61

Fortify Software Security Centerデータベースのシード処理について

初めてFortify Software Security Centerにログインする場合、Fortify Software Security Center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、Fortify Software Security Center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、Fortify Software Security Center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。

Fortify Software Security Centerには、ダウンロード済みシードバンドルが2つ必要です("Fortify Software Security Centerソフトウェアの解凍と展開" ページ51を参照してください)。

- 問題テンプレートシードバンドル(`Fortify_Process_Seed_Bundle-2021_Q4_0001.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-2021_Q4_0001.zip`)では、Fortify Software Security Center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 Basicバンドル`Fortify_PCI_Basic_Seed_Bundle-2021_Q4_0001.zip`および`Fortify_PCI_SSF_Basic_Seed_Bundle-2021_Q4_0001.zip`をインストールすることもできます。これらのPCI Basicバンドルでは、Payment Card Industryプロセステンプレートと関連付けレポートをFortify Software Security Center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Fortify Software Security Centerインストールパッケージに含まれています。初期Fortify Software Security Center展開後は、Fortify Support Portal (https://support.fortify.com)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)。

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Fortify Software Security Center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Fortify Software Security Center設定" ページ79を参照してください。

参照情報

"四半期ごとのセキュリティコンテンツ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" ページ189

Fortify Software Security Centerデータベースの永久削除

ある時点でFortify Software Security Centerを完全に削除する予定がある場合は、Fortify Software Security Centerデータベースを削除できます。Fortify Software Security Center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。

注意 `drop-tables.sql`スクリプトを実行すると、Fortify Software Security Center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、保存するデータをバックアップしてください。

Fortify Software Security Center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_install_dir>/sql`ディレクトリに移動し、Fortify Software Security Center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. Fortify Software Security Center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、Fortify Software Security Center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警告を確認します。
5. 次のスクリプトを実行して、Fortify Software Security Center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
   ```

第4章: Fortify Software Security Centerの初回設定

初めてFortify Software Security Centerを展開した後、ブラウザウィンドウにFortify Software Security CenterのURLを入力すると、Fortify Software Security Centerセットアップウィザード(セットアップウィザード)が開きます。ここでは、初回のサーバ設定のステップを完了できます。セットアップウィザードは、Fortify Software Security Centerの初めての展開、またはFortify Software Security Centerを保守モードにした後(1ページの "Fortify Software Security Centerの保守モードへの移行" ページ173を参照)にのみ、管理者だけが使用できます。

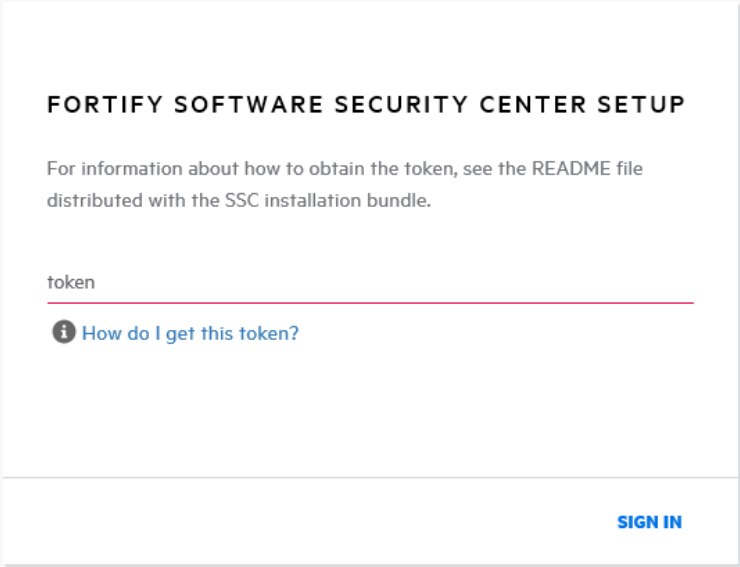
初めて Fortify Software Security Centerを設定するには、次の手順に従います。

1. Tomcatサーバに新しいバージョンのFortify Software Security Center WARファイルを展開した後、ブラウザウィンドウを開き、Fortify Software Security Centerサーバ のURLを入力します(`https://<host_IP>:<port>/<app_context>/`)。

   注: 通常の展開の場合、デフォルトのFortify Software Security Center URLは `<protocol>://<ssc_host>:<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>://<ssc_host>:<port>/`(末尾に`ssc`は付けません)です。

   `ssc.war`ファイルの名前を変更せずに配布されたWARファイルを使用してFortify Software Security Centerを展開する場合、`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ページの右上隅で、[ADMINISTRATORS]をクリックします。



3. <*fortify.home*><*app_context*>ディレクトリに移動し("fortify.homeディレクトリについて" ページ57を参照)、テキストエディタで`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. Webページで`init.token`ファイルからコピーした文字列をテキストボックスに貼り付け、 [**SIGN IN**]をクリックします。

   Fortify Software Security Centerセットアップウィザードが開きます。
6. セットアップウィザードの [**START**]ページの情報を読み、 [**NEXT**]をクリックします。
7. **CONFIGURATION**ステップの [**UPLOAD FORTIFY LICENSE**]で、次の操作を実行します。
   a. [**UPLOAD**]をクリックします。
   b. `fortify.license`ファイルを参照して選択し、 [**UPLOAD**]をクリックします。

   入力したライセンスが無効または期限切れである場合、Fortify Software Security Centerではその効果を示すメッセージが表示されます。

   右側のペインには、設定ファイル(`app.properties`、`datasource.properties`、および`version.properties`)が存在する設定ディレクトリのデフォルトパスが表示されます。
8. 構成ファイルディレクトリ内の機密情報に関する警告注意を読みます。設定プロパティファイルをデフォルト以外のディレクトリに保存する場合は、TomcatサーバでJVMシステムプロパティ`fortify.home`の別のパスを指定します。

   例: `-Dfortify.home=/home/fortify`
9. [**I have read and understood this warning**]チェックボックスをオンにし、 [**NEXT**]をクリックします。

10. CORE CONFIGURATION SETTINGSステップで、次の手順を実行します。
    a. [FORTIFY SOFTWARE SECURITY CENTER URL]ボックスに、Fortify Software Security CenterサーバのURLを入力します。
    b. 中央ペインで、[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Fortify Software Security Center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、ブラウザと直接のREST APIアクセスの両方に影響します。検証がオフの場合、あらゆるHTTP HostヘッダがFortify Software Security Centerにアクセスできます。
    c. Fortify Software Security Centerでグローバル検索を有効にするには、[GLOBAL SEARCH]ペインで[Enable global search]チェックボックスを選択します。
    d. 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)。

    注: 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。

    注: 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。

    e. [GLOBAL SEARCH]ペインで警告を読み、[I have read and understood this warning]チェックボックスを選択します。
11. [NEXT]をクリックします。
12. DATABASE SETUPステップで、次の手順を実行します。
    a. [DATABASE TYPE]ボックスで、Fortify Software Security Centerで使用するデータベースタイプを選択します。
    b. [DATABASE USERNAME]ボックスに、Fortify Software Security Center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権限" ページ60を参照してください。
    c. [DATABASE PASSWORD]ボックスに、Fortify Software Security Centerデータベースアカウントのパスワードを入力します。

    注: [DATABASE USERNAME]フィールドと[DATABASE PASSWORD]ボックス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の実行に必要な特権を持つユーザアカウント用に設定されている必要があります。これらの特権については、"データベースユーザアカウント権限" ページ60で説明されています。

d. [JDBC URL]ボックスに、Fortify Software Security CenterのURLを入力します。

注意 (MySQLデータベースタイプのみ)MariaDB JDBCドライバは、MySQLデータベースサーバへの接続に使用されます。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。正しい照合パラメータ構文の例:

```
jdbc:mysql://<host>:3306/<database_
name>?sessionVariables=collation_
connection=<collation>&rewriteBatchedStatements=true
```

MariaDBの構文の詳細については、(https://mariadb.com/kb/en)を参照してください。

重要 MySQLサーバデータベースを使用している場合は、URLの最後に次の項目を追加する必要があります。

- `rewriteBatchedStatements=true`
- `sessionVariables=collation_connection=COLLATION`

ここで、`COLLATION`はデータベースの照合タイプを表します。

例:

```
jdbc:mysql://localhost:3306/ssc?sessionVariables=collation_
connection=utf8_bin&rewriteBatchedStatements=true
jdbc:mysql://localhost:3306/ssc?sessionVariables=collation_
connection=latin1_general_cs&rewriteBatchedStatements=true
```

MariaDB JDBCドライバは、MySQLデータベースサーバへの接続に使用されます。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。

重要 MSSQLサーバデータベースを使用している場合は、URLの最後に次のプロパティ設定を追加する必要があります。

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

e. [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。

f. [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。

g. [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。

h. 設定をテストするには、[TEST CONNECTION]をクリックします。Fortify Software Security Centerは、テストが成功したかどうかを示すメッセージを表示します。

注: 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)をチェックして原因を特定します。

13. DATABASE SEEDINGステップに進む前に、`create-tables.sql`スクリプトを実行します。手順については、"Fortify Software Security Centerデータベーステーブルおよびスキーマについて" ページ66を参照してください。
14. データベースを初期化した後、[NEXT]をクリックします。
15. (Linuxのみ)OpenJDKを使用している場合は、サーバにDejaVu sansフォントとDejaVu serifフォントをインストールしてください。これらのフォントは、https://github.com/dejavu-fonts/dejavu-fontsからダウンロードできます。これらのフォントを使用しないと、Fortify Software Security Centerはレポートを正常に生成できません。
16. DATABASE SEEDINGステップで、次の操作を実行します。
    a. 左ペインで、[BROWSE]を使用して`Fortify_Process_Seed_Bundle-2021_Q4_0001.zip`ファイルを見つけて選択し、[SEED DATABASE]をクリックします。
    b. [BROWSE]を使用して、`Fortify_Report_Seed_Bundle-2021_Q4_0001.zip`ファイルを見つけて選択し、[Seed Database]をクリックします。
    c. (オプション) [BROWSE]を使用して`Fortify_PCI_SSF_Basic_Seed_Bundle-2021_Q4_0001.zip`ファイルを見つけて選択し、[SEED DATABASE]をクリックします。

    注: これらの新しい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理解するために、PCI SSF Basicシードバンドルを使用してください。詳細については、"Fortify Software Security Centerソフトウェアの解凍と展開" ページ51を参照してください。

    d. (オプション) [BROWSE]を使用して`Fortify_PCI_SSF_Basic_Seed_Bundle-2021_Q4_0001.zip`ファイルを見つけて選択し、[SEED DATABASE]をクリックします。
    e. (オプション) [BROWSE]を使用して`Fortify_PCI_Basic_Seed_Bundle-2021_Q4_0001.zip`ファイルを見つけて選択し、[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、"Fortify Software Security Centerソフトウェアの解凍と展開" ページ51を参照してください。
17. [NEXT]をクリックします。
18. [FINISH]をクリックします。
19. Tomcatサーバを再起動します。

Fortify Software Security Centerの初期設定が完了したら、コアパラメータの設定を完了し、追加の設定を[ADMINISTRATION]ビューから行います。
([ADMINISTRATION]ビューの詳細については、"追加のFortify Software Security Center設定" ページ79を参照してください)。

注: 後で環境設定を変更する必要がある場合は、Fortify Software Security Centerを保守モードに入れ、必要な変更を加えます。Fortify Software Security Centerを保守モードにする方法については、1ページの「"Fortify Software Security Centerの保守モードへの移行" ページ173を参照してください。

参照情報

"アップグレード後のFortify Software Security Centerの設定" ページ184

第5章: Fortify Software Security Centerへのログイン

Fortify Software Security Center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Fortify Software Security Centerを展開した後、Fortify Software Security Centerにログインできます。

重要 ログイン後、デフォルト以外の管理者アカウントを少なくとも1つ作成してから、デフォルトの管理者アカウントを削除します。Fortify Software Security Centerユーザアカウントと役割の管理方法の詳細については、"Fortify Software Security Centerユーザ管理について" ページ167を参照してください。

Fortify Software Security Centerにログインするには、次の手順に従います。

1. Webブラウザで、Fortify Software Security CenterインスタンスのURLを入力します。

   注: 通常の展開の場合、デフォルトのFortify Software Security Center URLは`https://<ssc_host>:<port>/ssc`です。Kubernetesクラスタへの展開の場合、デフォルトのURLは`https://<ssc_host>:<port>/`(末尾に`ssc`は付けません)です。

2. ユーザ名とパスワードを入力します。

   Fortify Software Security Centerに初めてログオンする場合は、[**Username**]および[**Password**]フィールドの両方に「**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. [**LOGIN**]をクリックします。

   Fortify Software Security Centerに初めてログオンする場合は、パスワードの変更を要求するメッセージが表示されます。

4. Fortify Software Security Centerでパスワードの変更を求めるプロンプトが表示されたら、新しいパスワードを入力します。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)が含まれないパスワードを指定してください。「myredhorsedance」などの無関係な単語を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、パスワードを保存してからログインできます。

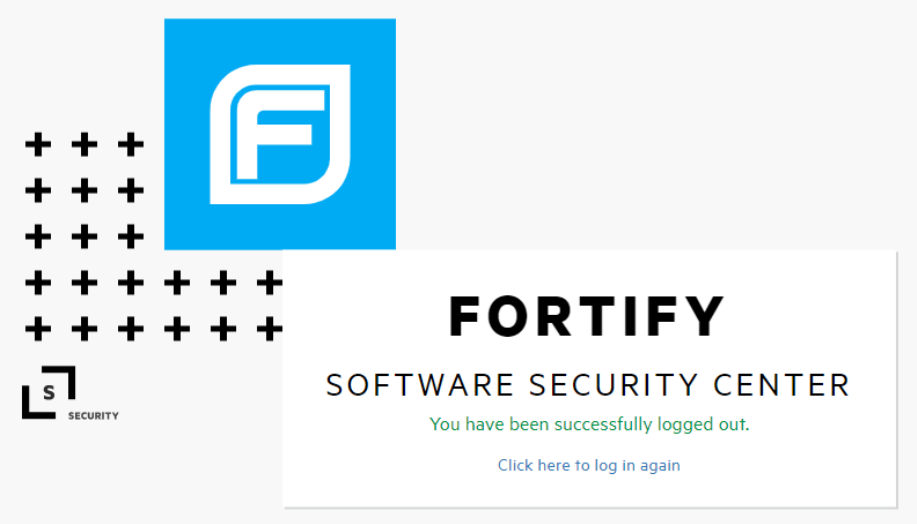
次を参照

"セッションログアウトについて" 次のページ

"追加のFortify Software Security Center設定" ページ79

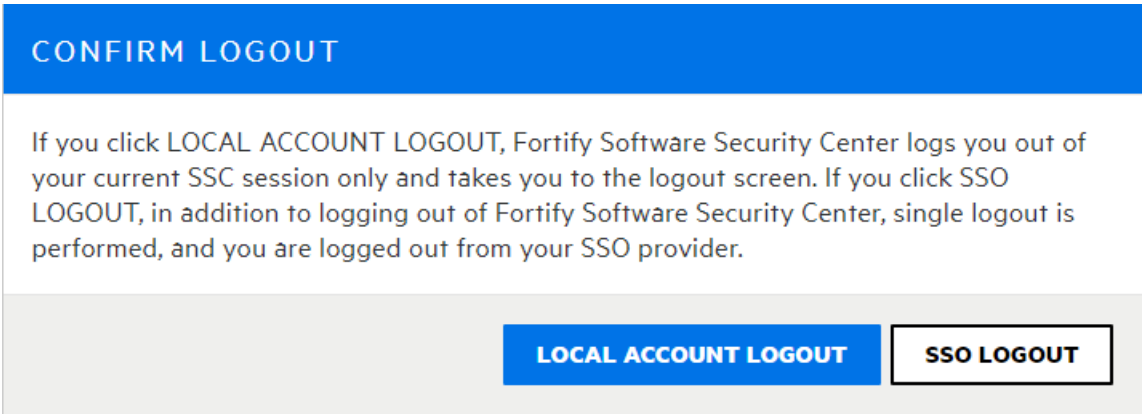
セッションログアウトについて

ローカルログインを使用してログ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Fortify Software Security Centerにログインし、その後ログアウトすると、Fortify Software Security Centerではここに表示される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ログインした場合、ログアウト時に、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できるセッションログアウト画面が表示されます。

注: Fortify Software Security Centerは、Central Authorization ServerおよびSAMLのシングルログアウトをサポートしています。



[LOCAL ACCOUNT LOGOUT]をクリックすると、Fortify Software Security Center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。

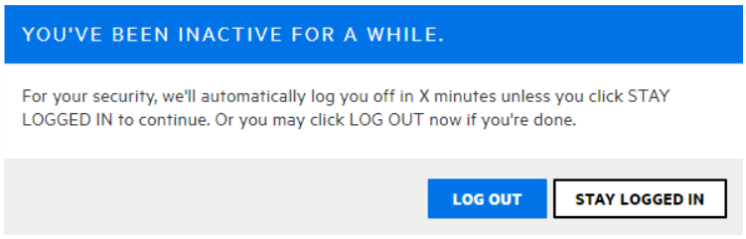
[SSO LOGOUT]をクリックすると、Fortify Software Security Centerからログアウトするほかに、シングルログアウトが実行され、SSOプロバイダからログアウトされます。

注: Fortify Software Security Centerから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

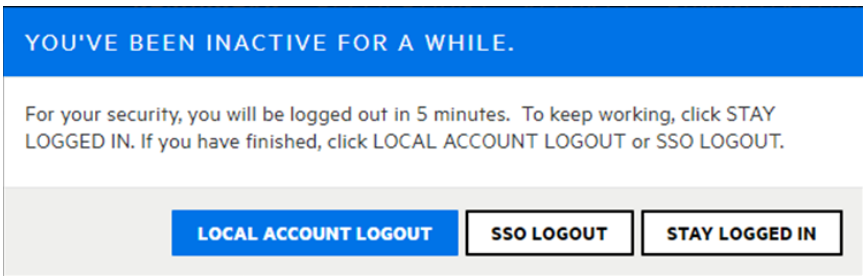
非アクティブによって、Fortify Software Security Centerセッションがタイムアウトに近付くと、Fortify Software Security Centerは次の2つのダイアログボックスのいずれかを表示します。

- ローカルログイン(ログ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)を使用してログインし、セッションがタイムアウトに近付いた場合は、ログアウトかログインの続行を可能にする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、Fortify Software Security Center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Fortify Software Security Center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。



[LOCAL ACCOUNT LOGOUT]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、Fortify Software Security CenterによってSSCセッションからのみログアウトされ、その後ログアウト画面が表示されます。

[SSO LOGOUT]をクリックすると、Fortify Software Security CenterによってSSCセッションからログアウトされ、その後SSOプロバイダからログアウトされます。

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" ページ95を参照してください。

注: Fortify Software Security Center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。

ログアウト画面

ローカルログインを使用してFortify Software Security Centerにログインした場合は、［**Click here to log in again**］リンクをクリックすると、ログイン画面が表示され、ここから再度ログインできます。

SSOプロバイダからFortify Software Security Centerにログインしている場合は、［**Click here to log in again**］リンクでSSOログインが開始されます。

第6章: 追加のFortify Software Security Center設定

事前のFortify Software Security Center設定を完了し、`ssc.war`ファイルを展開したら、Fortify Software Security Centerの［ADMINISTRATION］ビューから設定を完了します。

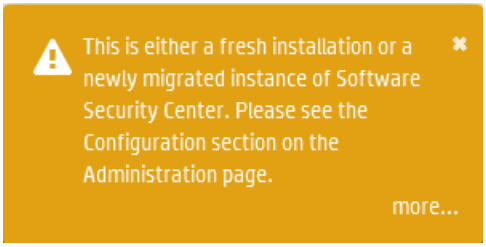
後から必要に応じて、［ADMINISTRATION］ビューで他の設定を設定および更新できます。

［ADMINISTRATION］ビューでの設定へのアクセス

［ADMINISTRATION］ビューの［**Configuration**］カテゴリからFortify Software Security Center設定を完了します。

［**Configuration**］カテゴリにアクセスするには、次の手順を実行します。

1. 管理者ユーザとしてFortify Software Security Centerにログインします。ログインの手順については、"Fortify Software Security Centerへのログイン" ページ75を参照してください。
2. 次のいずれかを実行します。
   - 初めてFortify Software Security Centerにアクセスする場合は、ページの上部に次のようなバナーが表示されます。［**Go**］をクリックして、［ADMINISTRATION］ビューの［**Configuration**］カテゴリを開きます。

     それ以外の場合は、次の手順を実行します。
     a. Fortifyのヘッダで、［**ADMINISTRATION**］をクリックします。
        ［ADMINISTRATION］ビューが開きます。左側のナビゲーションペインには、［ADMINISTRATION］ビューで使用可能なカテゴリへのリンクが表示されます。デフォルトでは、［Event Logs］ページが表示されます。
     b. 左側のペインで、［**Configuration**］を選択します。

このペインには、設定カテゴリオプションが表示されます。これらのオプションの詳細については、" ［ADMINISTRATION］ビューで使用可能な環境設定オプション" ページ81を参照してください。

問題統計しきい値の設定

［Issue Stats］ダッシュボードページには、Fortify Software Security Centerのアプリケーションバージョンの問題に関する概要情報が表示されます。この情報には、アプリケーションの確認と修復に必要な日数が含まれます。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、［Issue Stats］ページには［Average Days to Review］と［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、Fortify Software Security Centerは次のルールを適用します。

- Fortify Software Security Center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、Fortify Software Security Center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、Fortify Software Security Center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、Fortify Software Security Center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については、レビューする日は5 - 2 + 1、または4日です。

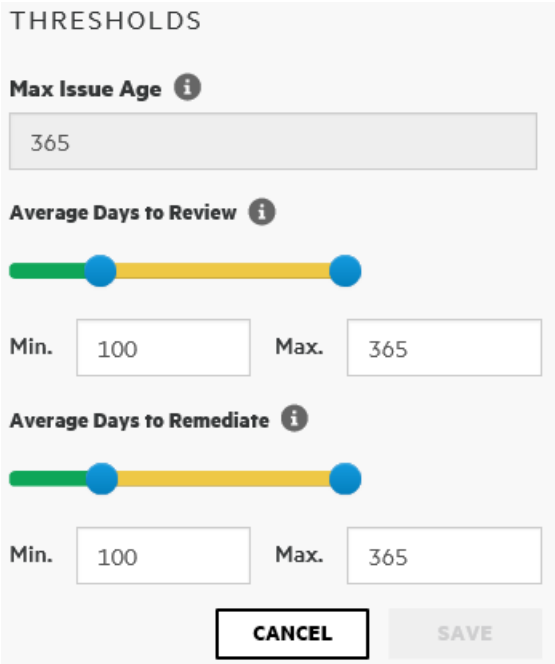
これらのルールのすべてが適用され、時間と日付の調整が行われます。その後、Fortify Software Security Centerは(auditTime - foundDate)と(removedDate - foundDate)の2つの値の平均値を計算して、監査して問題を修復する平均日数を取得します。

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。デフォルトでは、［Issue Stats］ページでは、100日(最小値)未満の値は緑のバー、365日(最大値)を超える値は赤、およびその間の値が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. Fortifyのヘッダで、[**ADMINISTRATION**]を選択します。
2. 左ペインの[**Metrics &Tracking**]で、[**Issue Age**]を選択します。
   [Issue Age]ページが開きます。**Average Days to Review**と**Average Days to Remediate**の最小値と最大値はそれぞれ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。
   - 次に表示される値を変更します。[**Min.**]と[**Max.**]コンボボックスです。
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。
   - 次に表示される値を変更します。[**Min.**]と[**Max.**]コンボボックスです。
5. [**SAVE**]をクリックします。

[Issue Stats]ダッシュボードページの色分けされた値に、変更が反映されます。

[ADMINISTRATION]ビューで使用可能な環境設定オプション

次の表は、[ADMINISTRATION]ビューで使用可能な環境設定オプションを一覧表示しています。(Fortifyのヘッダで、[**ADMINISTRATION**]を選択します。次に、左側の

ペインで、 [Configuration]を選択します。)

注: 一部の環境設定オプションの変更は、システムを再起動するまで有効にはなりません。

オプション	説明	手順
AppSec Training	アプリケーションセキュリティトレーニングを有効にして設定するために使用します。 [AUDIT]ページの問題の詳細セクションにある [GET TRAINING]ボタンが使用できるようになります。	"アプリケーションセキュリティトレーニングの設定" ページ84
Audit Assistant	Audit Assistantを有効にして設定する場合に使用します。Audit Assistantは、Fortify Scan Analyticsを使用して、Fortify Static Code Analyzerのスキャンを自動的に監査します。	"Audit Assistantの設定" ページ87
BIRT Reports	Fortify Software Security Centerのレポート機能に拡張セキュリティを適用する場合に使用します。	"BIRTレポート用のセキュリティの設定" ページ93
Core	タイムアウトやロックアウトの設定、セキュアコーディング用ルールパック更新のプロキシなど、コアFortify Software Security Center設定を設定するために使用します。	"コア設定の設定" ページ95
Email	電子メールアラートをユーザに送信するために使用するサーバ設定を設定する場合に使用します。	"電子メールアラート通知設定の設定" ページ99
Issue Audit	問題の監査の競合の問題を解決する方法を決定するための設定を選択する場合に使用します。	"問題監査の競合を解決するための戦略を設定する" ページ102
JMS	システムイベントをJava Message Service (JMS)に発行するようにFortify Software Security Centerを設定するために使用します。	"Java Message Service設定の設定" ページ104

オプション	説明	手順
LDAP Servers	1つ以上のLDAPサーバのLDAP認証およびLDAPサーバオプションを設定する場合に使用します。	1ページの「LDAPサーバの設定」
Maintenance Mode	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Fortify Software Security Center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。	"Fortify Software Security Centerの保守モードへの移行" ページ173
Proxy	ルールパック更新、Audit Assistantへの接続、およびバグトラッカプラグインのために単一のプロキシを設定する場合に使用します。	"Fortify Software Security Center統合のためのプロキシの設定" ページ128
ScanCentral DAST	Fortify Software Security Centerの[SCANCENTRAL]ビューから動的スキャンを管理および実行するようにFortify Software Security Centerを設定するために使用します。	"Fortify Software Security Centerを使用したScanCentral DASTスキャンの実行と管理の有効化" ページ131
ScanCentral SAST	ScanCentral SASTを監視したり、ScanCentral SASTの結果をFortify Software Security Centerの[SCANCENTRAL]ビューに表示したりするようにFortify Software Security Centerを設定するために使用します。	"Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設定" ページ130
Scheduler	Fortify Software Security Centerジョブスケジューラ設定を設定する場合に使用します。	"ジョブスケジューラの設定" ページ131
Security	Fortify Software Security Centerセキュリティ機能の設定に使用します。	"Fortify Software Security Centerのブラウザアクセスセキュリティの設定" ページ137
Seed Bundles	四半期ごとのセキュリティコンテンツリリースで配布されるシードバンドル	"四半期ごとのセキュリティコンテンツリリースで提供され

オプション	説明	手順
	をデータベースにシードするために使用します。	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" ページ189
SSO	次のいずれかのSSOソリューションを使用するようにFortify Software Security Centerを設定するために使用します。 • CAS SSO • SPNEGO/KERBEROS SSO • SAML SSO • HTTP SSO • X.509 SSO	"シングルサインオンを使用するためのFortify Software Security Centerの設定" ページ139
Web Services	Fortify Software Security Center Webサービスの設定に使用します。	"トークン認証が必要なWebサービスの設定" ページ155
Webhooks	Fortify Software Security Centerで発生するイベントに対してシステムを常に更新するWebhookを作成および管理するために使用します。	"Webhookの作成" ページ270

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Fortify Software Security Center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Fortify Software Security Center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. Fortifyのヘッダで、 [**ADMINISTRATION**]を選択します。
2. 左ペインで [**Configuration**]を選択し、 [**AppSec Training**]を選択します。
3. [AppSec Training]ページで、 [**Enable Training**]チェックボックスをオンにしたままにします。
4. オンライントレーニングベンダがFortify Software Security Centerと統合されているかどうかを確認して、対応するトレーニングURLを入手するには、Micro Focus Fortifyカスタマサポート(https://www.microfocus.com/support)にお問い合わせください。

5. [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. [SAVE]をクリックします。

[AUDIT]ページでは、問題の詳細セクションに[GET TRAINING]ボタンが表示されるようになりました。[GET TRAINING]をクリックすると、指定した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。

参照情報

"Fortify Scan結果の監査" ページ317

監査アシスタントについて

監査アシスタントはFortify Scan Analyticsと共に使用するオプションのツールです。Fortify Static Code Analyzerのスキャン結果から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。その判断を下すには、その監査のベースラインを確立するためのデータが監査アシスタントで必要になります。このデータは、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、ユーザが行った決定から構成されます。

Fortify共有データ(FortifyユーザとFortifyのセキュリティチームからプールされた匿名化データ)を使用するか、セキュリティチームが完了した監査データを使用することができます。監査アシスタントは、より多くのトレーニングデータを受け取ることで、問題が表す実際の脅威の評価がより正確になります。

トレーニングデータ(人間が監査した過去のスキャン結果から得られたメタデータ)は、何かを予測のために送信したことがなくても、送信することができます。

監査アシスタントは、トレーニングや予測データセットに含まれる補正を通じて学習することもできます。補正が登録されるのは、監査アシスタントが問題に割り当てた予測をユーザが確認し、同意できない場合は値を調整し、その問題をデータセットに含めて追加トレーニングさせた後です。

次のセクションでは、認証トークンをFortify Scan Analyticsから取得し、そのトークンを使用してFortify Scan Analyticsへの接続を設定する方法について説明します。この後のセクションでは、メタデータを送信するためにScan Analyticsを準備し、データを送信し、監査アシスタントの結果を確認し、修正した監査データを送信する方法について説明します。

参照情報

"Audit Assistantの設定" ページ87

"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" ページ238

"Audit Assistantの使用" ページ328

"予測ポリシーについて" ページ330

"予測ポリシーの定義" ページ330

"メタデータ共有の有効化" ページ331

"Audit Assistantへのトレーニングデータの送信" ページ332
"Audit Assistantの結果の確認" ページ332

Fortify Scan Analytics認証トークンの取得

Audit Assistantと統合するには、最初に、Fortify Scan Analytics認証トークンを取得する必要があります。

Fortify Scan Analytics認証トークンを取得するには、次の手順に従います。

1. Fortify Scan Analyticsにログオンします(https://analytics.fortify.com)。
2. Fortifyのヘッダで、 [**ADMINISTRATION**]をクリックし、 [**TOKENS**]を選択します。
3. [Tokens]ページで、 [**+ADD**]をクリックします。
4. [**Name**]ボックスに、生成するトークンの名前を入力します。
5. [**SAVE**]をクリックします。
   [Tokens]ページには、新しいトークンが一覧表示されます。
6. トークン名の右側にあるビューアイコン( )をクリックします。
   [Token]ウィンドウが開きます。
7. トークンテキストを選択してコピーし、 [**CLOSE**]をクリックします。

コピーしたトークンを使用して、Audit Assistantとの統合を設定します。("Audit Assistantの設定" 下を参照してください)。

Audit Assistantの設定

監査アシスタントはFortify Scan Analyticsと共に機能し、Fortify Static Code Analyzerのスキャン結果から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。

アプリケーションでAudit Assistantを使用するようにFortify Software Security Centerを設定するには、次の手順に従います。

1. 管理者としてFortify Software Security Centerにログインし、Fortifyのヘッダで [**ADMINISTRATION**]を選択します。
2. 左ペインで、 [**Configuration**]を選択してから、 [**Audit Assistant**]を選択します。
3. 次の表で説明するように、 [Audit Assistant]ページで設定をします。

フィールド* 必須	説明
Enable Audit Assistant	残りのフィールドを有効にするには、このチェックボックスをオンにします。
* Authentication token	Fortify Scan Analytics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については、 [**How do I get token**]を選択してください。または、"Fortify Scan Analytics認証トークンの取得" 上を参照してください。
* Fortify Scan	Fortify Scan AnalyticsサーバのURLを指定します。

フィールド* 必須	説明
Analytics server URL	
Use SSC proxy for Audit Assistant	すべてのFortify Software Security Center統合にプロキシを設定した場合("Fortify Software Security Center統合のためのプロキシの設定" ページ128を参照)、このチェックボックスを選択して、Audit Assistantのプロキシを使用できます。

4. Application Security Analyticsサーバへの接続をテストするには、 [TEST CONNECTION]をクリックします。
   接続が正常にテストされた後、先に進んで [Audit settings]セクションで設定を設定します。
5. [REFRESH POLICIES]をクリックして、 [Default prediction policy]リストに、新しいFortify Scan Analyticsサーバ上の現在のサーバポリシーを入力します。

   注: 個々のアプリケーションバージョンに設定されたAudit Assistant予測ポリシーは、使用可能なポリシーがFortify Scan Analyticsサーバで変更された場合、無効になる可能性があります。Fortify Software Security Centerは、ユーザが [REFRESH POLICIES]をクリックするたびに、Fortify Scan Analyticsから新しく受信したポリシーを検証します。Fortify Software Security Centerで1つ以上の無効なポリシーが検出されると、元のポリシーから変更された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。Fortify Software Security Center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。

6. [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 Scan Analyticsで定義されます)。
7. 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、 [Enable specific application version policies]を選択します。それ以外の場合、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。

   注: アプリケーションバージョンのポリシーは、 [APPLICATION PROFILE]ダイアログボックスから指定できます。手順については、"アプリケーションバージョンに対するAudit Assistantオプションの設定" ページ256を参照してください。

8. Audit Assistantがまだ評価されていない問題を自動的にFortify Scan Analyticsへ送信して評価させる場合は、 [Enable auto-predict]チェックボックスをオンにします。(自動予測機能の詳細については、"監査アシスタントの自動予測について" 次のページを参照してください)。

注: ここで自動予測を有効にする場合は、自動予測を使用する各アプリケーションバージョンに対して［APPLICATION PROFILE］ダイアログボックスを開き、そこでも有効にします。

9. Audit Assistantが問題を評価する分析値の適用をシステム全体のAnalysisカスタムタグ値に対して有効にするには、［**Enable auto-apply**］チェックボックスをオンにします。その後、［APPLICATION PROFILE］ウィンドウから、アプリケーションバージョンのプロジェクトベースごとにこの機能を有効にする必要があります。

注: ここで自動適用を有効にする場合は、自動適用を使用する各アプリケーションバージョンに対して［APPLICATION PROFILE］ダイアログボックスを開き、そこでも有効にします。

重要 自動適用機能を使用する前に、まずAudit Assistant分析タグの値をFortify Software Security Center Analysisタグ値にマップする必要があります。

10. ［**Enable auto-apply**］チェックボックスをオンにし、Audit Assistant分析タグの値をFortify Software Security Center Analysisタグ値に今すぐマップする場合は、［**here**］リンクをクリックして［Custom Tags］ページに移動し、"Fortify Software Security Centerカスタムタグ値へのAudit Assistant分析タグ値のマッピング" 次のページに記載されている手順に従います。
11. ［**SAVE**］をクリックします。

監査アシスタントの自動予測について

FPRが正常にアップロードおよび処理された後に、監査アシスタントの予測に関する問題を自動的に送信するようにFortify Software Security Center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、監査アシスタント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、評価のために監査アシスタントに自動的に送信されます。監査アシスタントが問題を評価した後、その問題は再検討されません。

自動予測の有効化

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、管理者が監査アシスタントの設定中にシステム全体で有効にします ("Audit Assistantの設定" ページ87)。この後、ユーザは［PROFILE］ウィンドウからアプリケーションバージョンごとに自動予測を有効にできます ("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" ページ238」を参照)。

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

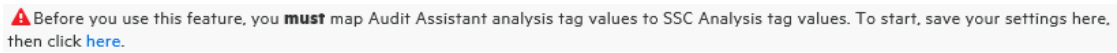
Audit Assistantを設定したときに("Audit Assistantの設定" ページ87)、監査アシスタントの自動適用を有効にした場合、次に1つ以上のリストタイプについてAudit Assistant分析タグの値をFortify Software Security Centerカスタムタグ値にマップする必要があります。その後、自動監査機能の使用を開始できます。

注: Audit Assistantの自動適用が機能には、アプリケーションバージョンの［APPLICATION PROFILE］ダイアログボックスで、マップされたカスタムタグをプライマリカスタムタグとして指定する必要があります。

Audit Assistant分析タグの値をFortify Software Security Centerリストタイプのカスタムタグ値にマップするには、次の手順に従います。

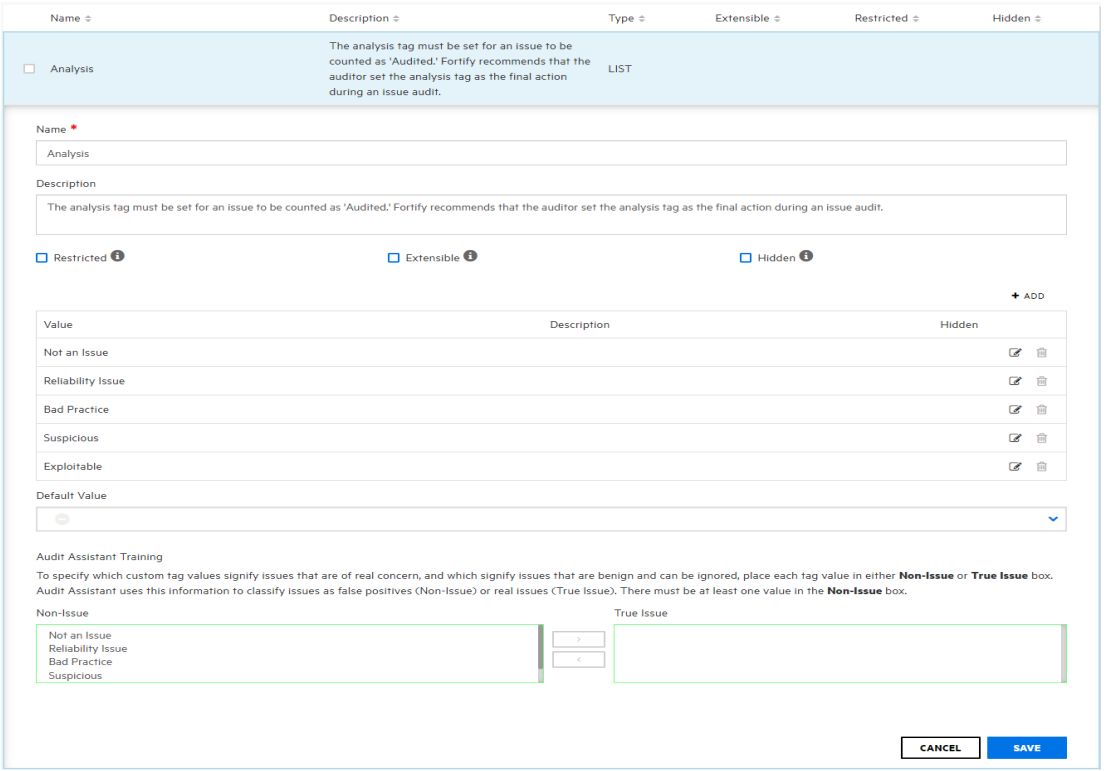
1. Audit Assistantを設定した(およびAudit Assistantの自動適用を有効にする)後、次のいずれかを実行します。
   - [ADMINISTRATION]ビューの左ペインから、[**Templates**]を選択して、[**Custom Tags**]を選択します。

   または

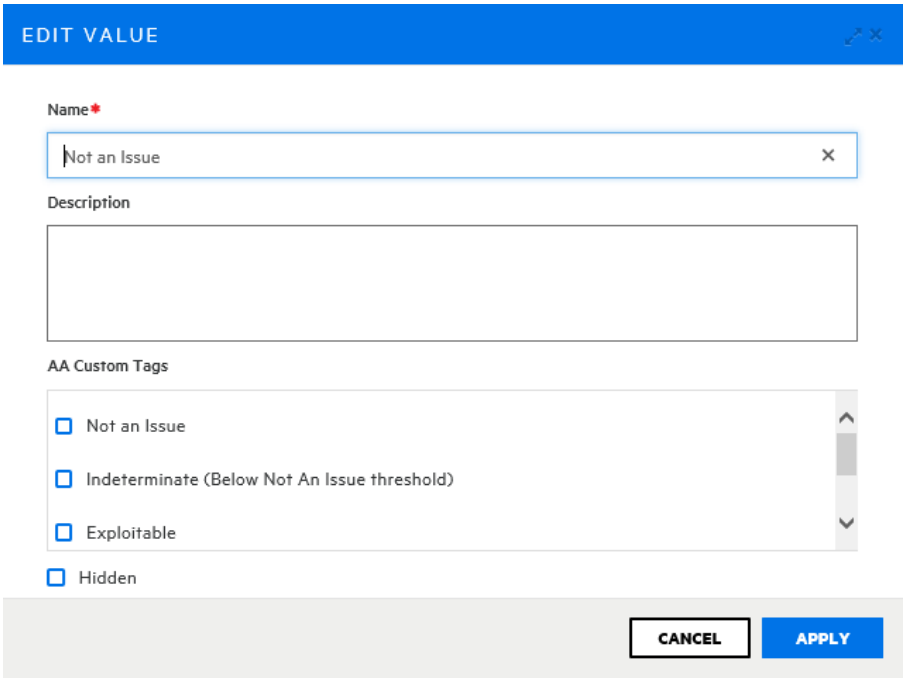
   - 自動適用を有効にしている場合は、[Audit Assistant]ページの下部にある**このリンクをクリック**します。

   [Custom Tags]ページが開きます。
2. 値をマップするリストタイプのカスタムタグ(Analysisなど)の行を展開します。
3. 展開したセクションの右下で、[**EDIT**]をクリックします。



テーブルに一覧表示されているカスタムタグ値が編集可能になり、[**Audit Assistant Training**]セクションが表示されます。

4. タグ値の表で、一覧表示されている値の[Edit value]アイコン( )を選択します。

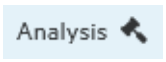


[EDIT VALUE]ダイアログボックスが開きます。

5. [AA Custom Tags]で、このカスタムタグ値を持つ問題の値のチェックボックスをオンにします。
6. [APPLY]をクリックします。

カスタムタグ値のリストに、Audit Assistant向けにマップした値が表示されます。

7. 自動監査向けにマップする値のすべてについて、手順4から6を実行します。
8. [SAVE]をクリックします。



マッピングを保存した後、Fortify Software Security Centerではカスタムタグ名の右側にガベルアイコンが表示されます。

注: [Audit Assistance Training]セクションは、データトレーニングの目的で使用されます。このセクションの設定方法については、ページ1の「システムへのカスタムタグの追加」を参照してください。

BIRTレポート用のセキュリティの設定

以下の一方または両方を実行して、BIRTレポーティングにセキュリティ対策を追加できます。

- Javaセキュリティマネージャを有効にする
- データベース内のテーブルおよびビューへのアクセスを制限する

Javaセキュリティマネージャの有効化

Javaセキュリティマネージャを有効にするには、次の手順に従います。

1. Fortify Software Security Centerに管理者としてログインします。
2. Fortifyのヘッダで、[ADMINISTRATION]をクリックします。
3. 左ペインで[Configuration]を選択し、[BIRT Reports]をクリックします。
4. [BIRT Reports]ページの[Enhanced security]、[Turn on security manager]チェックボックスを選択します。

   注: BIRTセキュリティマネージャが安全でないと見なす機能に依存するカスタムレポートを生成しようとすると、レポート生成が失敗する可能性があります。

5. [SAVE]をクリックします。

(OpenJDKのみのLinux)必要なフォントのインストール

LinuxシステムにFortify Software Security Centerがインストールされ、OpenJDKを実行している場合は、ユーザがレポートを正常に生成するために、サーバにfontconfigライブラリ、DejaVu Sansフォント、およびDejaVu serifフォントをインストールする必要があります。そうしないと、レポートの生成に失敗します。これらのフォントは、https://github.com/dejavu-fonts/dejavu-fontsからダウンロードできます。

レポーティング用のデータベースアカウントの作成

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、次のテーブルおよびビューへの読み込み(のみ)アクセスを有効にしてください。

テーブル		
activity	filterset	metavalue
attr	folder	projecttemplate
auditattachment	foldercountcache	reportexecblob
auditcomment	issuecache	requirement
catpackexternalcategory	measurement	requirementtemplate
catpackexternallist	measurementhistory	scan_rulepack
catpacklookup	metadef	sourcefile
datablob	metadef_t	snapshot
documentinfo	metaoption	userpreference
eventlogentry	metaoption_t	variable
		variablehistory
ビュー		
attrlookupview	defaultissueview	ruleview
auditvalueview	metadefview	view_standards
baseissueview	metaoptionview	

3. Fortify Software Security Centerに管理者としてログインします。
4. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
5. 左ペインで [Configuration]を選択し、 [BIRT Reports]をクリックします。
   Fortify Software Security Centerは、 [BIRT Reports]ページを表示します。
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. データベースへのデータベースユーザアカウントアクセスをテストするには、 [VALIDATE CONNECTION]をクリックします。
8. [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" 次のページ

"レポート生成タイムアウトの設定" 下

レポート生成用のメモリの割り当て

Fortify Software Security Center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、次の手順に従います。

1. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. 左ペインで [Configuration]を選択し、 [BIRT Reports]をクリックします。
3. [Set up BIRT execution]セクションの [Maximum heap size (MB)]ボックスでデフォルト値を選択し、新しい値を入力します。(Javaのヒープサイズの最小値と推奨値については、Micro Focus Fortifyソフトウェアシステム要件のドキュメントを参照してください)。
4. [SAVE]をクリックします。

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. 管理者としてFortify Software Security Centerにログインします。
2. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
3. 左ペインで [Configuration]を選択し、 [BIRT Reports]をクリックします。
4. [Set up BIRT execution]の [Execution timeout (minutes)]ボックスで既定値を選択し、新しい値を入力します。
5. [SAVE]をクリックします。

コア設定の設定

セットアップウィザードで実行した初期設定に加えて、管理ビューの [Configuration]セクションで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設定、ユーザ情報の表示、Fortify WebInspect Agentの問題の最大イベント数、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。Rulepacks更新プロキシの詳細については、"ルールパック更新のプロキシアップデートの設定について" ページ98を参照してください。

[ADMINISTRATION]ビューでFortify Software Security Centerのコア設定を設定するには、次の手順に従います。

1. 管理者としてFortify Software Security Centerにログインし、Fortifyのヘッダで [ADMINISTRATION]をクリックします。
2. [ADMINISTRATION]ビューの左ペインで、 [Configuration]を選択し、 [Core]を

選択します。

3. [Core]ページで、次の表で説明されている設定を設定します。

フィールド	説明
Absolute session timeout (minutes)	Fortify Software Security Centerがユーザを自動的にログオフする前に、ユーザを継続してアクティブにできる分数です。 デフォルト値は240です。
Days before password reset	ユーザがパスワードを変更する必要が生じるまでにFortify Software Security Centerパスワードが有効な日数です。 デフォルト値は30です。
Login attempts before lockout	Fortify Software Security Centerがユーザのアカウントをロックする前に、無効な資格情報を使用してユーザがFortify Software Security Centerにログインを試みることができる回数です。 Fortify Software Security Centerがユーザをロックアウトすると、そのユーザは**[Lockout time (minutes)]**ボックスで指定された分数の間、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" ページ215を参照してください。 デフォルト値は3です。
Lockout time (minutes)	ユーザが**Login Attempts before Lockout**で指定された回数Fortify Software Security Centerへのログインを試み、ログインできない場合、Fortify Software Security Centerは**[Lockout time (minutes)]**ボックスで指定された分数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。
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。

フィールド	説明
	• **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。
Maximum events per WebInspect Agent Issue	単一のFortify WebInspect Agentの問題内にログするイベントの最大数を決定します。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。
Inactive session timeout (minutes)	Fortify Software Security Centerがユーザを自動的にログオフするまでのユーザがアクティブでない時間(分)を入力します。 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) **注:** 英語は値を指定する必要はありません。
Rulepack	Fortify Rulepack更新サイトのURLです。

フィールド	説明
update URL	**重要** [Rulepack Update URL]フィールドのデフォルト値は、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。 デフォルト値`https://update.fortify.com`です。
Use SSC proxy for Rulepack update	Rulepackサーバがプロキシの背後にある場合にFortify Software Security Center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。 **注:** Fortify Software Security Centerプロキシを有効にし、正しく設定する必要があります。プロキシを設定する方法については、"Fortify Software Security Center統合のためのプロキシの設定" ページ128を参照してください。
User Administrator's email address (for user account requests)	電子メール通知が有効なときにシステム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を入力します。 新しいユーザアカウントの要求が次の場合にこの電子メールアドレスに送信されます。 [Can't access or need an account?]リンクがFortify Software Security Centerログインページで利用可能なときです。
Enable export to CSV from the Dashboard and AUDIT views	このチェックボックスを選択すると、ユーザはFortify Software Security Centerデータをカンマ区切りの値ファイルにエクスポートできます。 **注:** [Core]ページでこのプロパティだけを変更する場合、変更を実装するためにサーバを再起動する必要はありません。

4. [SAVE]をクリックします。
5. 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" ページ215

ルールパック更新のプロキシアップデートの設定について

デフォルトで、Fortify Software Security Centerでは、購読している現在のバージョンのFortify Secure Coding RulepacksをFortify Customer Portal

(https://update.fortify.com)からダウンロードします。

組織がプロキシを使用して外部リソースにアクセスする場合は、セキュリティ保護されたコーディングルールパックのアップデート(バグトラッキング、および使用する場合は監査アシスタント)用にプロキシを設定することを推奨します。すべてのHTTP(s)プロトコルベースのFortify Software Security Center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、"Fortify Software Security Center統合のためのプロキシの設定" ページ128を参照してください。

すべてのHTTP(s)プロトコルベースの統合で使用するために単一のプロキシを設定した後、そのプロキシをルールパックアップデートに対して有効にできます。手順については、"コア設定の設定" ページ95を参照してください。

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Fortify Software Security Centerを使用する予定の場合は、次の手順に従います。

1. Fortify Software Security Center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。

注: 電子メールアラートの受信を有効または無効に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" ページ101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。

重要 Fortify Software Security Centerにアクセスを要求するアカウントを持たないチームメンバーがいる場合は、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Fortify Software Security Centerにログインし、Fortifyのヘッダで[**ADMINISTRATION**]を選択します。
2. 左ペインで、[**Configuration**]を選択してから、[**Email**]を選択します。
   [Email]ページが開きます。
3. 次の表で説明されている電子メールサービス属性の設定をします。

フィールド	説明
Enable email	このチェックボックスを選択すると、Fortify Software Security Centerはすべてのタイプの電子メールメッセージを送信し、「Can't access or need an account?」リンクをログインダイアログボックスに追加できます。 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。

フィールド	説明
From email address	Fortify Software Security Centerから送信される電子メールを識別するためにFortify Software Security Center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です。
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です。
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。
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。
Trust the certificate	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。

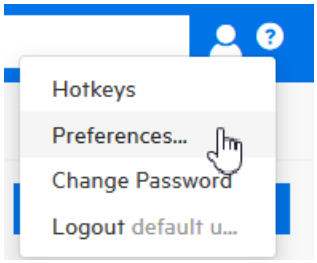
フィールド	説明
provided by the SMTP server	**注意** セキュリティ上の理由から、このチェックボックスをオフのままにすることを推奨します。

4. [SAVE]をクリックします。

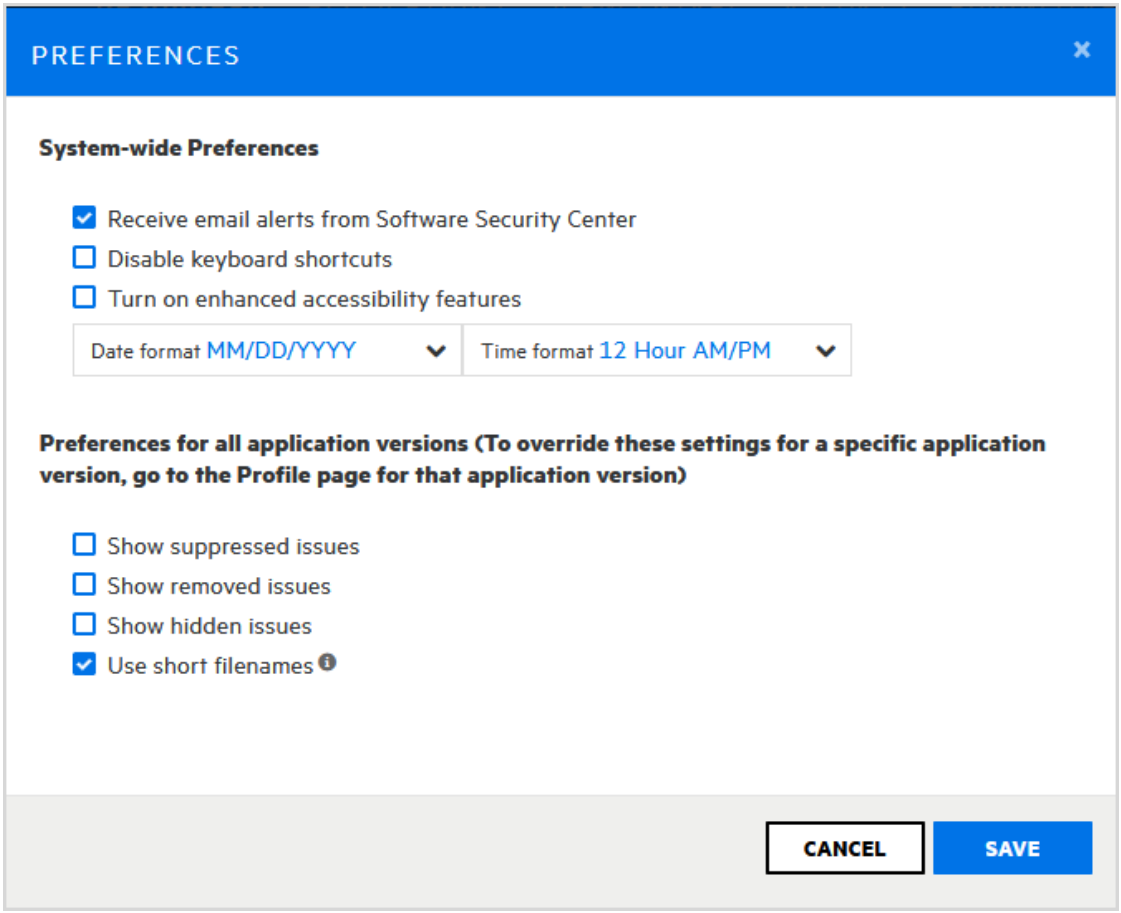
電子メールアラートの受信を有効化および無効化する

電子メールアラートの受信を有効化または無効化するには:

1. 管理者としてFortify Software Security Centerログインします。



2. Fortifyヘッダの右側にあるユーザプロファイルアイコンをクリックし、 [Preferences]を選択します。



[PREFERENCES]ダイアログボックスが開きます。

3. 次のいずれかを実行します。
   - 電子メールアラートの受信を無効にするには、[**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、[**Receive email alerts from Software Security Center**]チェックボックスをオンにします。
4. [**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" ページ99

"アラート定義" ページ282

"アラートの作成" ページ283

"アラートの削除" ページ286

問題監査の競合を解決するための戦略を設定する

複数の監査者が同じ問題に異なる製品(Fortify Software Security Center、Audit Workbench、またはIDEプラグイン)を使用して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、Fortify Software Security Center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、Fortify Software Security Center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。

注: 競合の解決が必要ないのは、これらの監査者が同じFortify Software Security Center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戦略の例:

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スキャン結果を監査しています。

ユーザAは、発見された問題にカスタムタグ値を設定し、結果をFortify Software Security Centerにアップロードします。

Fortify Software Security Center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、Fortify Software Security Center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。

別のAudit Workbenchインスタンス上で、ユーザBは、ユーザAが監査したのと同じ問題に対してカスタムタグ値を設定し、結果をFortify Software Security Centerにアップロードします。Fortify Software Security Center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: Fortify Software Security Center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。

Fortify Software Security Center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、Fortify Software Security Center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。

注: 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。

Fortify Software Security Center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. Fortify Software Security Centerに管理者としてログインします。
2. Fortifyのヘッダで、 [**ADMINISTRATION**]を選択します。
3. 左ペインで、 [**Configuration**]を選択してから、 [**Issue Audit**]を選択します。
   [SSUE AUDIT]ページが開きます。
4. [**Issue audit conflict resolving strategy**]リストから、次のいずれかを選択します。

- **Conflicts are resolved in favor of the SSC changes**
- **Conflicts are resolved in favor of the most recent changes**

5. [SAVE]をクリックします。

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" ページ304

Java Message Service設定の設定

システムイベントをJava Message Service (JMS)に発行する場合は、Fortify Software Security Centerの [ADMINISTRATION]ビューの [Configuration]カテゴリでJMS設定を設定します。

JMS設定を設定するには、次の手順を実行します。

1. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. [ADMINISTRATION]ビューの左ペインで、 [Configuration]を選択し、 [JMS]を選択します。
   [JMS]ページが開きます。
3. 次の表の説明に従って設定します。

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`などです。
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. [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。

Fortify Software Security Centerユーザ認証について

デフォルトでは、ユーザがFortify Software Security Centerにログオンするとき、またはFortifyクライアントを使用してFortifyプロジェクト結果ファイル(FPR)をアップロードするときに、Fortify Software Security Centerでデータベースを使用してユーザを認証してから、認証済みユーザをそのユーザに割り当てられたユーザ役割(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、Fortify Software Security Center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、Fortify Software Security Centerのデフォルトのデータベースのみ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" 下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" ページ123を参照してください。

LDAPユーザ認証

このセクションのトピックでは、Fortify Software Security Center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。

重要 Fortifyでは、LDAPサーバの設定前に、いつかLDAPサーバに問題が発生した場合に備え、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。

重要 Fortifyは複数のLDAPサーバの使用はサポートしますが、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ません。ただし、これらのサーバが同一である場合を除きます。

注: Fortify Software Security CenterのLDAPエンティティおよびユーザ役割を管理する方法については、"LDAPエンティティの登録" ページ119および"LDAPユーザ役割の管理について" ページ170を参照してください。

LDAP認証の設定の準備

LDAP認証を使用するようにFortify Software Security Center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。(http://www.jxplorer.org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. Fortify Software Security Centerで使用するLDAPアカウントを作成します。

   注: 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" ページ95を参照してください。

重要 Fortify Software Security Center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Fortify Software Security Center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Fortify Software Security Center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、Fortify Software Security Center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。

   注: Fortifyでは、Fortify Software Security Centerのユーザ名をLDAPサーバで複製しないことを勧めしています。

4. 必要な情報を収集して記録します。
5. Fortify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" 次のページおよび"LDAP referralサポートを無効化する" ページ108を参照してください。

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。**
  ユーザ名は、すべてのLDAP設定で一意にすることを強く推奨します。Fortify Software Security Center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サーバ間で一意ではない可能性があるデフォルトの`sAMAccountName`ではなく、`userPrincipalName`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、管理者が重複したユーザ名を避けにくい場合があります。Fortify Software Security Center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、一意でないユーザ名を持つユーザは、正常にFortify Software Security Centerにログインし、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、DAST統合などの一部の機能は、このようなユーザの場合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、Fortify Software Security Center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できるかもしれません。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、Fortify Software Security Centerに登録されている最初のLDAPサーバのLDAPオブジェクトが、`OU=org,DC=acme,DC=com`サブツリーを(直接または遷移的に)参照していないか、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、Fortify Software Security Center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、Fortify Software Security Center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。

参照情報

"LDAPサーバの設定" 次のページ

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するために使用されます。クライアントが要求した情報が別の場所(複数の場合あり)、場合によっては別のサーバまたは複数のサーバで検出される可能性を示すために、サーバから送信されます。

Fortify Software Security CenterでLDAPオブジェクトを要求し、このオブジェクトがreferralである場合、Fortify Software Security Centerでは別のサーバからこの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。そのアドレスはREFオブジェクト属性で返されます。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。

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ます。Fortify Software Security Centerサーバ側でこのオプションを無効にすると、Fortify Software Security Center-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" 次のページを参照してください。

注: referralの詳細については、http://docs.oracle.com/javase/jndi/tutorial/ldap/referral/overview.htmlを参照してください。

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. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左ペインで、 [Configuration]を選択してから、 [LDAP Servers]を選択します。
3. [LDAPサーバ]ページで、referralサポートを無効にするLDAPサーバ接続をクリックします。
   行が展開されて、LDAPサーバに関する詳細が表示されます。
4. [EDIT]をクリックします。
5. [ADVANCED INTEGRATION PROPERTIES]セクション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. [SAVE]をクリックします。

LDAPサーバの設定

次の手順では、Fortify Software Security Center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。

重要 [LDAP]ページでプロパティを設定する前に、"LDAPユーザ認証" ページ105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。

重要 ある時点で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ます。

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

1. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左のナビゲーションペインで、 [Configuration]を選択してから、 [LDAP Servers]を選択します。
3. [Integration with LDAP servers]ページで、 [NEW]をクリックします。
   [CREATE NEW LDAP CONFIGURATION]ダイアログボックスが開きます。
4. 次の表で説明されている属性を設定します。

フィールド	説明
BASIC SERVER PROPERTIES	
Enable this LDAP configuration	Fortify Software Security Center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

フィールド	説明
	ンにします。
Server name **重要** 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。	このサーバの固有の名前を入力します。

Server URL (ldap://<host>:<port>)	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、次の形式でURLを入力します。
	`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。

Base DN **重要** Fortify Software Security Center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。	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。 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、Fortify Software Security Center はDAPオブジェクトツリーの

フィールド	説明
	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。
Bind user DN	Fortify Software Security Center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。 アカウント指定子の一般形式は次の形式です。 `cn=<accountName>, ou=users,dc=<domainName>,dc=com` ここで、`<accountName>`はFortify Software Security Centerが排他的に使用するために作成した最小特権、読み込み専用認証サーバアカウントを表します。 **注意** 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。
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。ベースDNから検索することを推奨します。ただし、LDAPディレクトリのサイズが大きすぎてFortify Software Security Center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

フィールド	説明

	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Fortify Software Security Centerから隠すこともできます。
	たとえば、ベースDN companyName.comおよびそのベースDNのすべてのエントリ内を検索するには、次を指定して、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`

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。 このフラグを有効にして、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に制限しているのに、実際の結果が600件ある場合、このフラグを有効にすると、Fortify Software Security Centerから単に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、Fortify Software Security Centerと接続するLDAPサーバのタイプを選択します(**ACTIVE_DIRECTORY**または**OTHER**)。
ほとんどのユーザはMicrosoft Active Directoryを使用します。このページの残りのLDAP属性は、デフォルトのActive Directory設定で動作するように設定されています。ただし、LDAPサーバの設定が異なる場合は、これらの属性値を変更できます。	
SECURITY	
SSL trust check	このチェックボックスをオンにすると、LDAPサーバによって提示された証明書が信頼された認証

フィールド	説明
	局によって発行されたことを確認できます。
Hostname validation	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するようにするには、このチェックボックスをオンにします。
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、Fortify Software Security Center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。この情報は、トークンベースおよびSSOベースの認証スキーム中の拡張認証チェックに使用されます。
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、Fortify Software Security Center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。
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	Fortify Software Security Center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。

フィールド	説明
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。
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。
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

フィールド	説明
ADVANCED INTEGRATION PROPERTIES	
Cache LDAP user data **注:** LDAPユーザキャッシングを有効のままにすることを推奨します。LDAPサーバで直接行われたユーザ情報の変更は、Fortify Software Security Centerに最大1時間反映されない場合があります。ただし、Fortify Software Security CenterとLDAPサーバの接続が遅い場合や、検索が遅い大規模なLDAPディレクトリの場合、Fortify Software Security Centerのパフォーマンスが低下する可能性があります。LDAPサーバでは、ユーザデータが直接変更されることはめったにありません。	Fortify Software Security Center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、Fortify Software Security Centerの［ADMINISTRATION］ビューから手動でリフレッシュできます。手順については、"LDAPエンティティの手動更新" ページ121を参照してください。
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。この値は、複数のスレッドのLDAPキャッシュを同時に更新するタスク実行者のスレッドプールを設定するために使用されます。 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

フィールド	説明
	大数を入力します。デフォルト値は12です。
Enable paging in LDAP search queries **注:** 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。LDAPサーバでこの機能がサポートされるのを確認します。	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。
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 **注:** 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" ページ107を参照してください。	LDAPサーバが1つのみである場合は、［**Ignore**］を選択してLDAPの動作を高速化することを推奨します。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。
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、http://docs.spring.io/spring-security/site/docs/3.1.x/reference/ldap.htmlを

フィールド	説明
	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。Fortify Software Security Center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。
Enable nested LDAP groups **注:** 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、Fortify Software Security Center 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。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ます。	このチェックボックスを選択すると、Fortify Software Security Center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)。
Interval between LDAP server validation attempts (ms)	LDAPサーバが検証を試行した後、次に検証を試みる前に待機するミリ秒数。 デフォルト値は`5000`です。
Time to wait LDAP validation (ms)	キャッシュを更新する要求をLDAPサーバに送信した後にFortify Software Security Center

フィールド	説明
	が応答を待機する時間(ミリ秒単位)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ID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。

> **重要** 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と固有のベースDNを指定する必要があります。
>
> Fortifyは複数のLDAPサーバの使用はサポートしますが、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ません。ただし、これらのサーバが同一である場合を除きます。

参照情報

"LDAPサーバ設定のインポート" 次のページ
"LDAPサーバ設定を編集する" 次のページ
"LDAPエンティティの登録" ページ119
"LDAPユーザ認証" ページ105
"LDAPサーバ設定の削除" ページ122
"LDAPユーザ役割の管理について" ページ170

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. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左ペインで、 [Configuration]を選択してから、 [LDAP Servers]を選択します。
3. [Integration with 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. [EDIT]をクリックします。
5. "LDAPサーバの設定" ページ108で説明されている属性に必要なすべての変更をします。
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" 次のページ

"LDAPユーザ認証" ページ105

"LDAPユーザ役割の管理について" ページ170

LDAPサーバ設定のインポート

Fortify Software Security Center 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. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左ペインで [Configuration]を選択し、スクロールダウンして [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。
   [IMPORT LEGACY LDAP CONFIGURATION]ダイアログボックスが開きます。
4. 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て、テキストボックスに貼り付けます。
   コピーした内容に関する問題が Fortify Software Security Center で検出された場合は、エラーメッセージと、詳細を表示するリンクが表示されます。

   注: 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。これらを手動で入力する必要があります("LDAPサーバの設定" ページ108)を参照してください。
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サーバの設定" ページ108 の手順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" 下

"LDAPユーザ認証" ページ105

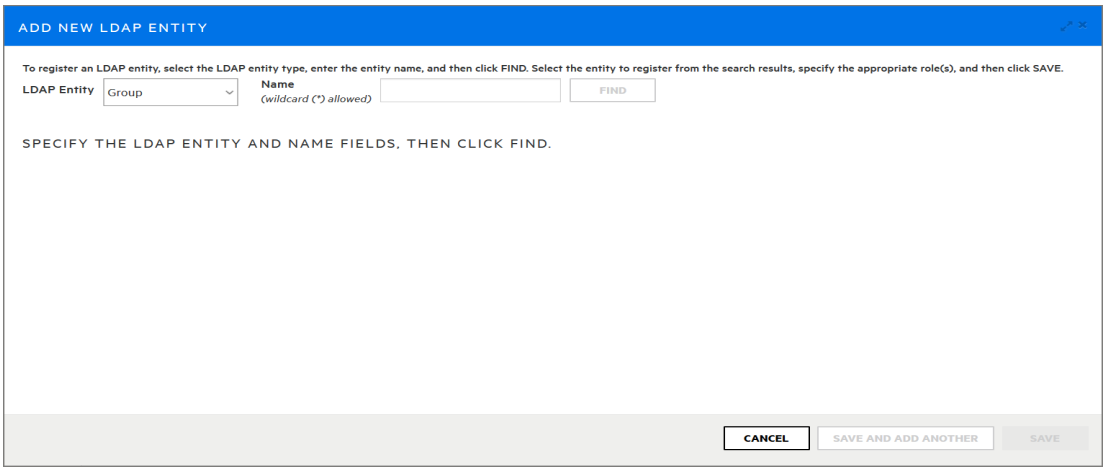
"LDAPユーザ役割の管理について" ページ170

LDAPエンティティの登録

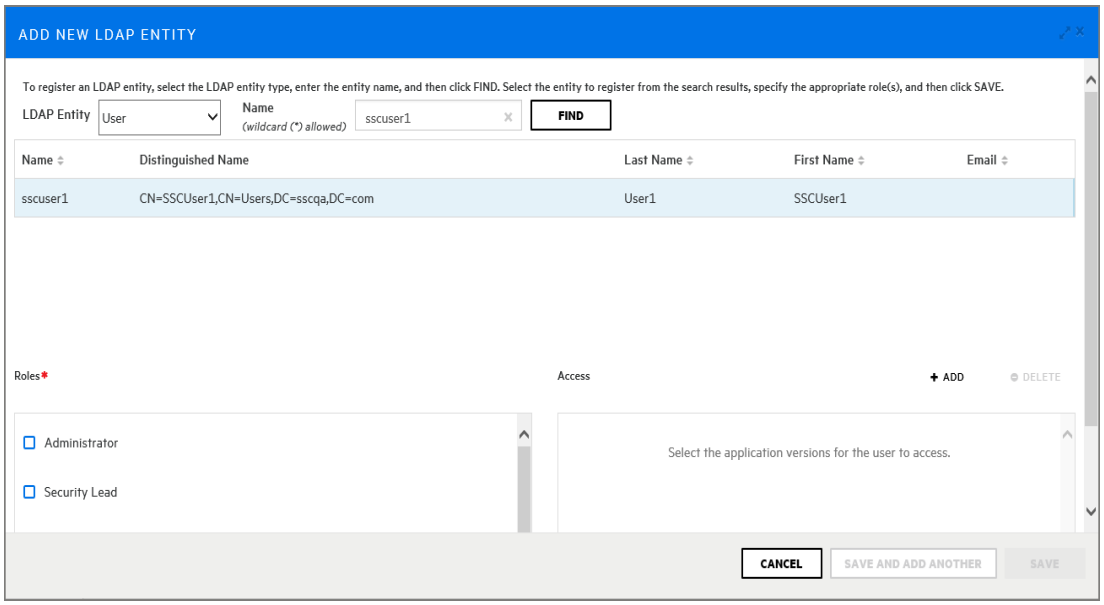
管理者レベルのアカウントを持つユーザは、LDAPグループ、部門、およびユーザをFortify Software Security Centerユーザのリストに追加できます。ユーザがグループに参加またはグループから離れると、Fortify Software Security Centerによってアクセス制御が自動的に更新されます。

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

1. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで [ADMINISTRATION]をクリックします。
2. 左ペインで、 [Users]をクリックし、 [LDAP Entities]を選択します。
3. [LDAP]ツールバーで、 [+ADD]をクリックします。
   [ADD NEW LDAP ENTITY]ウィンドウが開きます。



4. [LDAP Entity]リストから、登録するLDAPエンティティのタイプ(Group、User、またはOrganizational Unit)を選択します。
5. 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。



6. [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。
7. 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を提供するには、[Access]セクションで次の手順を実行します。

注: 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。

   a. [+ ADD]をクリックします。
      [SELECT APPLICATION VERSION]ダイアログボックスが開きます。
   b. [Application]リストから、LDAPエンティティがアクセスするアプリケーションの名前を選択します。
      Fortify Software Security Center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。
   c. 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。
   d. 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。
   e. [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。
8. 次のいずれかを実行します。
   - 変更を保存し、[Add New LDAP Entity]ダイアログボックスを閉じるには、[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。

   Fortify Software Security Centerがエンティティをユーザのリストに追加します。

Fortify Software Security Center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。

9. 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には、次の手順に従います。
   a. [LDAP]ページで、更新するLDAPエンティティのチェックボックスをオンにします。
   b. LDAPツールバーで、[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" ページ108を参照してください。

参照情報

"LDAPユーザ認証" ページ105

"LDAPユーザ役割の管理について" ページ170

LDAPエンティティの手動更新

Fortify Software Security Center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. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで[ADMINISTRATION]をクリックします。
2. 左ペインで、[Users]、[LDAP Entities]の順に選択します。
3. 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。
4. LDAPツールバーで、[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" ページ108を参照してください。

参照情報

"LDAPユーザ認証" ページ105

"LDAPエンティティの登録" ページ119

"LDAPユーザ役割の管理について" ページ170

LDAPエンティティの識別名の更新

何らかの理由で、Fortify Software Security Centerを使用するように設定されているLDAPサーバの識別名(DN)が変更された場合は、関連付けられたLDAPエンティティのDN値を更新する必要があります。

注: 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. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. 左ペインで、 [Users]、 [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)。

   [UPDATE DISTINGUISHED NAME]ダイアログボックスが開きます。
5. [Distinguished name]フィールドで現在無効な値を選択し、更新された識別名に置き換えます。
6. [SAVE]をクリックします。

参照情報

"LDAPサーバの設定" ページ108

LDAPサーバ設定の削除

Fortify Software Security Center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。デフォルトサーバは無効にしてください。

LDAPサーバ接続を削除するには、次の手順を実行します。

1. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左ペインで、 [Configuration]を選択してから、 [LDAP Servers]を選択します。
3. 次のいずれかを実行します。
   - [Integration with 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、 [LDAP Servers]ツールバーで [DELETE]をクリックします。

     または
   - [Integration with LDAP Servers]ページで、削除するLDAPサーバ接続をクリックし、展開されたサーバ詳細セクションの右下にある [DELETE]をクリックします。

   [DELETE LDAP CONFIGURATION]ダイアログボックスに、削除の続行を確認するメッセージが表示されます。
4. [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、Fortify Software Security Centerサーバを再起動します。

参照情報

"LDAPユーザ認証" ページ105

"LDAPエンティティの登録" ページ119

"LDAPユーザ役割の管理について" ページ170

SCIM 2.0プロトコルの実装

System for Cross-domain Identity Management (SCIM)をFortify Software Security Center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プロトコルを介してユーザおよびグループをFortify Software Security Centerにプッシュします。そのため、ユーザを追加するためにFortify Software Security Centerの [ADMINISTRATION]ビューを経由する必要がありません。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。

注: 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Fortify Software Security Centerとの相互運用性をテストする必要があります。現在のところ、公式にサポートされているのはAzure AD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。

- Fortify Software Security Center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を使用してのみログインできます。
- ローカルに作成されたユーザ名 ([ADMINISTRATION]> [Users]> [Local Users]) がすでにFortify Software Security Center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。 [ADMINISTRATION]ビューから作成されたユーザは、SCIMプロビジョニングにおいて読み込み専用です。

サポートされるSCIMリソース

Fortify Software Security Center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`)
  Fortify Software Security Centerでは、ユーザスキーマのすべての標準属性を受諾しますが、これらのサブセットのみを保存します("ユーザ属性マッピング" 次のページを参照)。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`)
  Fortify Software Security Centerでは、グループスキーマのすべての標準属性を受諾しますが、これらのサブセットのみを保存します("グループ属性マッピング" 次のページを参照)。

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Fortify Software Security Center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	SSC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Fortify Software Security Center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Fortify Software Security Center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	SSC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	必須
members	N/A	既存のユーザおよび/また

SCIMグループ属性	SSCグループ属性	コメント
		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Azure ADへの接続の設定" 下

"SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141

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Azure ADへの接続の設定

System for Cross-domain Identity Management (SCIM)プロトコルを使用して、Azure Active Directory (Azure AD)のユーザアカウントでFortify Software Security Center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
Fortify Software Security Center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" ページ128
Microsoft Azureで、Azure Active Directory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 Azureのドキュメント (https://docs.microsoft.com/en-us/azure/active-directory) **注:** 新しいアプリケーションでなにを行いたいかを示すプロンプトが表示されたら、 ⟦Integrate any other application you don't find in the gallery (Non-gallery)⟧オプションを選択します。
Azure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 Azureのドキュメント (https://docs.microsoft.com/en-us/azure/active-directory)
Azureから、アプリケーションをプロビジョニングします。	Microsoft Azureのドキュメント (https://docs.microsoft.com/en-us/azure/active-directory)

タスク	詳細
次の点に注意してください。 • 「Provisioning Mode」を「Automatic.」に設定します。 • 「Tenant URL」値のSSC URLを使用して、文字列 `/api/scim/v2?aadOptscim062020`を追加します。 **注:** `/api/scim/v2`は、SSC 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Azure ADのコンプライアンスが向上します。 • 「Secret Token」値については、SSCで作成したトークンを使用します(SCIMトークン - "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" ページ128を参照してください)。	
Azure ADから、Azure ADとFortify Software Security Center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 「Provisioning Status」のトグルを「On」に切り替える必要があります。	Microsoft Azureのドキュメント (https://docs.microsoft.com/en-us/azure/active-directory)

タスク	詳細
Azure AD SAMLメタデータが署名されています。Fortify Software Security Centerで署名を正常に検証するには、Azure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。 Azure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 Azure Active Directoryのドキュメント (https://docs.microsoft.com/en-us/azure/active-directory) • "SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141
Fortify Software Security Center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ソリューションを使用するためのFortify Software Security Centerの設定" ページ141
Fortify Software Security Center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、Fortify Software Security CenterでSAML SSOが有効であり、正常に初期化されている場合のみです。	`<ssc_hostname>:<port>/<context>/saml/metadata`
Azure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 Azureのドキュメント (https://docs.microsoft.com/en-us/azure/active-directory)
Fortify Software Security Center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" ページ216

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. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで[**ADMINISTRATION**]をクリックします。
2. [ADMINISTRATION]ビューの左ペインで、[**Configuration**]を選択し、[**SCIM**]までスクロールして選択します。
3. [**Enable SCIM**]チェックボックスをオンにします。
4. [**SCIM Token**]ボックスに、Fortify Software Security CenterSCIM 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、Fortify Software Security CenterとAzure ADの間の接続を設定する際に、Azure ADでシークレットトークンとして使用します)。

   重要 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Fortify Software Security Center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。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ます。

5. [**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ソリューションを使用するためのFortify Software Security Centerの設定" ページ141

"SCIM 2.0プロトコルの実装" ページ123

"外部管理されたユーザおよびグループを表示する" ページ216

Fortify Software Security Center統合のためのプロキシの設定

1つのプロキシを設定して、Fortify Software Security Center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ら、Audit Assistant("Audit Assistantの設定" ページ87)、Rulepack更新URL("コア設定の設定" ページ95)、およびバグトラッカプラグイン("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" ページ245)などのコンポーネントに対して、そのプロキシの使用を有効にできます([**Use SSC proxy for...**]チェックボックスを選択します)。

すべてのHTTPプロトコルベースのFortify Software Security Center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. Fortifyのヘッダで、[**ADMINISTRATION**]を選択します。
2. 左ペインで、[**Configuration**]を選択してから、[**Proxy**]を選択します。
   [Proxy]ページで、次の表に示す設定の値を指定します。

設定	説明
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	
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. [SAVE]をクリックします。

Fortify Software Security Centerで、プロキシ設定が成功したというメッセージが右上に表示されます。

参照情報

"Audit Assistantの設定" ページ87

"コア設定の設定" ページ95

"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" ページ245

Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設定

Fortify ScanCentral SASTを使用すると、プロセッサ集約型スキャンフェーズを専用のFortify Static Code Analyzerスキャンファームにオフロードすることで、Fortify Static Code Analyzerユーザはリソースを最大限に活用できます。ScanCentral SASTを監視し、その結果をFortify Software Security Centerに表示できます。ScanCentral SASTセンサプールを作成および管理できます。この機能を有効にするには、Fortify Software Security Centerで統合を設定する必要があります。

注: 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、『*Micro Focus 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。

Fortify Software Security CenterとScanCentral SASTの統合を設定するには、次の手順を実行します。

1. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで[**ADMINISTRATION**]をクリックします。
2. [ADMINISTRATION]ビューの左ペインで、[**Configuration**]を選択し、[**ScanCentral SAST**]を選択します。
   [ScanCentral SAST]ページが開きます。
3. [**Enable ScanCentral SAST**]チェックボックスをオンにします。
4. [**ScanCentral Controller URL**]ボックスに、ScanCentral SASTコントローラのURLを入力します。

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

5. [**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)を入力します。
6. [**SSC and ScanCentral controller shared secret**]ボックスに、コントローラのデータを要求するためにFortify Software Security Centerで使用する共有秘密鍵(非暗号化)を入力します(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`キー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。
7. [**SAVE**]をクリックします。
8. Fortify Software Security Centerサーバを再起動します。

参照情報

"ScanCentral SASTの許可" ページ356

"ScanCentral Controller情報の表示" ページ360

"ScanCentral SASTセンサプールについて" ページ363

"ScanCentral SASTセンサプールの作成" ページ364

Fortify Software Security Centerを使用したScanCentral DASTスキャンの実行と管理の有効化

Fortify 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、WebInspectセンササービス、およびFortify Software Security Center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。

ScanCentral DASTの動的スキャンの実行と管理を有効にするには、次の手順を実行します。

1. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで[ADMINISTRATION]をクリックします。
2. [ADMINISTRATION]ビューの左ペインで、[Configuration]を選択し、[ScanCentral DAST]を選択します。
3. [ScanCentral DAST]ページで、[Enable ScanCentral DAST]チェックボックスをオンにします。
4. [ScanCentral DAST server URL]ボックスに、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_Hostname>:<Port>/api/`

   `http://<DAST_API_IP_Address>:<Port>/api/`

   代わりにhttpsプロトコルを使用できます。

   重要 URLの末尾に/api/を含める必要があります。
5. [SAVE]をクリックします。

次のタスクを実行する方法については、『Micro Focus ScanCentral DAST設定および使用ガイド』を参照してください。

- ScanCentral DASTプールおよびセンサの管理
- 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

ジョブスケジューラの設定

Fortify Software Security Centerジョブスケジューラは、[ADMINISTRATION]ビューの[Configuration]セクションから設定します。

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. Fortifyのヘッダで、[ADMINISTRATION]を選択します。
2. 左ペインで、[Configuration]を選択してから、[Scheduler]を選択します。[Scheduler]ページが開きます。
3. 次の表の説明に従って設定します。

フィールド	説明
Number of days after which executed jobs will be removed	終了したジョブがFortify Software Security Centerから削除される日数。 デフォルト値は1(日)です。
Job execution strategy	使用するジョブ実行戦略を選択します。オプションは次のとおりです。 • **Conservative:** デフォルトの戦略は、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。このジョブ実行戦略は次のように機能します。 ◦ 削除ジョブなどの一部のジョブは、同時並行性が低い、または「排他的」なジョブと見なされます。このような排他的なジョブは1度に1つしか実行されません。(排他的なジョブを実行すると、実行中のジョブは設定された容量の60%まで減少します)。 ◦ `${job.numberOfConcurrentReports}`レポートジョブのみが同時に実行できます。 ◦ `${jobs.threadCount}`ジョブは同時に実行できる場合があります。`${job.numberOfDedicatedDataExports}`スレッドは、その数がカンマ区切り値(CSV)ファイルエクスポートジョブ用に予約されています。他のジョブは、それらのスレッドを使用できません。 • **Aggressive:** 高い同時並行性を可能にします。このオプションを使用すると、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。すべてのジョブは、すべての使用可能なワーカに対して等しく実行されます。 • **Exclusive jobs:** ジョブを1つずつ、順番に実行できるようにします。 デフォルト値は**Conservative**です。 **注:** 保守的な戦略と積極的な戦略の両方について、2つのワーカスレッドがカンマ区切り値(CSV)ジョブへのエクスポート専用です。("データをカンマ区切り値ファイルへエクスポートする" ページ202を参照してください)。

フィールド	説明
Token management - 夜間ジョブは、指定した日数前に期限切れになったトークンをクリアします。	
Warn days before expiry	ユーザに有効期限が近付いていることを通知する際の、トークンの有効期限が切れるまでの日数です。有効な値の範囲は3から30日です。 デフォルト値は7(日)です。 **注:** Fortify Software Security Centerサーバロケールでは、1日の開始は12 AMです。
Snapshot refresh - このセクション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に使用される変数とパフォーマンスインジケータの値が含まれます。	
Days of week	CRON式を入力して、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。値は、曜日の3文字の略語として入力するか(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」のように入力します。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。 **注:** 3文字の省略形は大文字で入力する必要があります。エントリ間のスペースはオプションです。 連続する日を入力するには、エントリをダッシュで分離します。たとえば、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。 スケジューラを毎日実行する場合は、「*****」と入力します(デフォルト)。
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1 A.M.に開始されます。 スケジューラを毎時間実行する場合は、「*****」と入力します。

フィールド	説明
	注: 「Days of Week」、「Hours」、および「Minutes」フィールドに入力した値が連結され、スケジューラが使用するCRON式が作成されます。 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、「Hours」ボックスに入力した時間より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示します)。
Index maintenance - このセクションのフィールドを使用して、Fortify Software Security Center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。このジョブは毎日実行することを推奨します。	
Days of 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か(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」のように入力します。 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。 **注:** 3文字の省略形は大文字で入力する必要があります。エントリ間のスペースはオプションです。 連続する日を入力するには、エントリをダッシュで分離します。たとえば、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。 スケジューラを毎日実行する場合は、「*****」と入力します。 デフォルト値は「*」です。
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1 A.M.に開始されます。 スケジューラを毎時間実行する場合は、「*****」と入力します。

フィールド	説明
	注: [Days of Week]、[Hours]、および [Minutes]フィールドに入力した値が連結され、スケジューラが使用するCRON式が作成されます。 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、[Hours]ボックスに入力した時間より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示します)。
Events maintenance	
Days to preserve	Micro Focus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。 Fortify Software Security Center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。新しいジョブが毎日11:30 p.mに作成されます。ブロックされていない場合は、直ちに作業を開始します。 デフォルト値は0です。(クリーンアップは行われません)。
Data export maintenance	
Days to preserve	Fortify Software Security Center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。 **注:** このジョブは毎日11:45 PM (23:45)に実行されます。

4. [SAVE]をクリックします。
5. 設定を実装するには、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" 次のページ

"スケジュールされたジョブのキャンセル" ページ137

ジョブ実行優先度の設定

Fortify Software Security Centerの新しいジョブはすべて優先度が「非常に低い」に設定されています。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。

Fortify Software Security Center管理者またはセキュリティリードである場合は、「PREPARED」状態のスケジュールされたジョブの優先度を変更できます。(ジョブの状態は、PREPARED、RUNNING、FINISHED、FAILED、またはCANCELEDが考えられます)。

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. Fortifyのヘッダで、 [**ADMINISTRATION**]を選択します。
2. [ADMINISTRATION]ビューの左のペインで、 [**Metrics & Tracking**]を選択し、[**Jobs**]をクリックします。
3. [**Jobs**]ツールバーの右側の [**Filter by**]リストから [**Prepared**]を選択します。
4. 一覧表示されているジョブをスクロールし、優先度を再設定するジョブの行を展開(クリック)します。
5. [**SET PRIORITY**]リストから、次のいずれかの優先度値を選択します。
   - Very Low
   - Low
   - Medium
   - High
   - Very High

   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、Fortify Software Security Centerではその可能性を示すメッセージがで表示され、変更を続行するかを確認するメッセージが表示されます。
6. 続行するには、 [**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" 次のページ

"ジョブスケジューラの設定" ページ131

スケジュールされたジョブのキャンセル

Fortify Software Security Center管理者またはセキュリティリードである場合は、準備済み状態のままのスケジュールされたジョブをキャンセルできます (ジョブの状態は、準備済み、実行中、完了、失敗、またはキャンセルです)。

ジョブをキャンセルするには、次の手順を実行します。

1. 管理者またはセキュリティリードとしてFortify Software Security Centerにログインしてから、Fortifyヘッダで [ADMINISTRATION]を選択します。
2. [ADMINISTRATION]ビューの左ペインにある [Metrics & Tracking]で、 [Jobs]を選択します。
3. [Jobs]ツールバーの右端にあるジョブ状態の [Filter by]リストから [Prepared]を選択します。
4. 一覧表示されているジョブをスクロールし、キャンセルするジョブの行をクリックします。
5. ジョブの行をクリックして展開し、詳細を表示します。
6. [CANCEL]をクリックします。
   Fortify Software Security Centerに、ジョブのキャンセルを確認するメッセージが表示されます。
7. ジョブのキャンセルを確認します。

参照情報

"ジョブスケジューラの設定" ページ131

Fortify Software Security Centerのブラウザアクセスセキュリティの設定

Fortify Software Security Center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. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. 左ペインで、 [Configuration]を選択してから、 [Security]を選択します。
   [Security]ページが開きます。
3. 次の表の説明に従って設定します。

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Fortify Software Security Center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。

フィールド	説明
	• `host.url`プロパティ(Fortify Software Security Center設定ウィザードを使用して設定)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、［**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Fortify Software Security Center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。Fortifyでは、Content-Security-Policyヘッダを無効にすることを推奨しますが、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。
Set value for Strict-Transport-Security header	Strict-Transport-Securityヘッダの値を入力します。このヘッダはブラウザに信号を送信し、HTTPの代わりにHTTPSを使用してFortify Software Security Centerと通信します。 **重要** この値を設定する場合は、注意が必要です。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のチートシートを参照してください(https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet)。 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。
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。 **重要** この値を設定する場合は、注意が必要です。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のチートシートを参照してください(https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet)。

フィールド	説明
	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. [SAVE]をクリックします。

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

次の表に、Fortify Software Security Centerでサポートするシングルサインオンソリューションのリストと、これらのSSOタイプを使用するためにFortify Software Security Centerを設定する方法に関する指示へのリンクを示します。

SSOソリューション	指示
Central Authorization Server (CAS)	"Central Authorization Serverを使用するためのFortify Software Security Centerの設定" 次のページ
SPNEGOベースのKerberos	"Fortify Software Security CenterでのKerberos認証の設定" ページ151
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ソリューションを使用するためのFortify Software Security Centerの設定" ページ141
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Fortify Software Security Centerの設定" ページ149
X.509証明書	"X.509証明書ベースのSSOを使用するためのFortify Software Security Centerの設定" ページ153

設定に関する制限

SSOソリューションを使用するためのFortify Software Security Center設定に関する制限は次のとおりです。

- ユーザにFortify Software Security Centerユーザインタフェースへのアクセス権を与えることをFortify Software Security CenterでサポートするSSOソリューションのみを使用できます。
- どの時点でも、Fortify Software Security Center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。

- Audit Workbench、fortifyclient、またはIDEプラグインにアクセスするユーザは、ログインにLDAPまたはローカルのFortify Software Security Centerユーザアカウントとパスワードを使用する必要があります。

SSOのデバッグログ記録を有効に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" ページ154を参照してください。

制限付きローカルログイン(SPNEGO/KerberosおよびX.509によるソリューションのみ)

重要 この制限は、Central Authorization Server (CAS)、SAML、またはHTTPヘッダによるSSOソリューションには適用されません。これらのSSOソリューションでは、ローカルログインがサポートされています。

アプリケーションのセキュリティを向上させるため、SSO認証が有効になっている場合、Fortify Software Security CenterではLDAPユーザとローカルユーザの両方がユーザ名とパスワードを使用してローカルにログインすることができません。ユーザはFortify Software Security Center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。SPNEGO/KerberosまたはX.509によるSSOソリューションを設定してローカルログインを有効にするには、管理者は`app.properties`ファイルにある`sso.localAuthenticationEnabled`プロパティを使用する必要があります。詳細については、ページ1の"Fortify Software Security Center がX.509またはKerberos SSOソリューションを使用するように設定されている場合にユーザ名およびパスワードログインを有効にする" ページ154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" ページ76

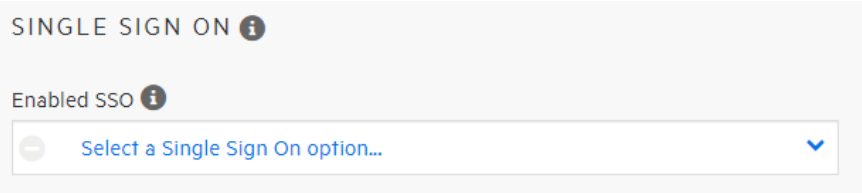
Central Authorization Serverを使用するためのFortify Software Security Centerの設定

注: CASのシングルログアウトは、Fortify Software Security Centerでサポートされています。

Central Authorization Server(CAS)を使用するようにFortify Software Security Centerを設定するには、次の手順を実行します。

1. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで[**ADMINISTRATION**]をクリックします。
2. [ADMINISTRATION]ビューの左ペインで、[**Configuration**]を選択し、[**SSO**]を選択します。
   [SINGLE SIGN ON]ページが開きます。

注: Fortify Software Security Centerに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. 使用可能なシングルサインオンソリューションのリストから、[**CAS**]を選択します。
4. [**Central Authentication Server URL**]ボックスに、CASサーバのURLを入力します。デフォルトは`http://localhost:8080/cas`です。
5. *<fortify.home>*/*<app_context>*/conf/app.propertiesの`host.url`プロパティでCAS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、Fortify Software Security Centerサービスパラメータのベースとして使用され、*<host.url>*/login/casに設定されています。
6. [**SAVE**]をクリックします。
7. 設定を実装するには、サーバを再起動します。

注: Fortify Software Security Centerの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" ページ154を参照してください。

SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定

注: SAMLのシングルログアウトは、Fortify Software Security Centerでサポートされています。

注意 SAMLを正常に統合するには、クライアントコンピュータとサーバコンピュータ(IdPとSP)のクロックを同期する必要があります。

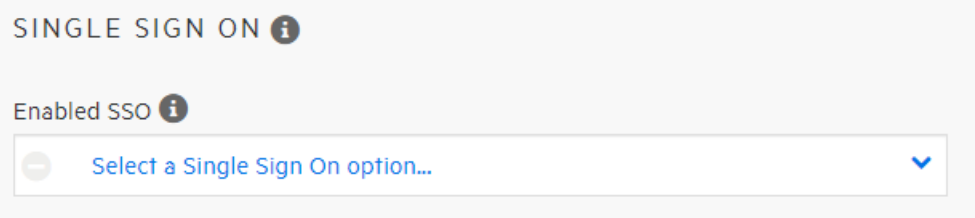
SAML 2.0を使用するSSOが動作するようFortify Software Security Centerを設定するには、次の手順に従います。

1. Fortify Software Security Center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Fortify Software Security Center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。(情報については、"LDAPユーザ認証" ページ105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Fortify Software Security Center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. IdPサーバからSAMLメタデータを取得し、それをFortify Software Security Centerファイルシステムに保存します。

4. 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。キーストアには、ルートCA証明書と署名の中間CA証明書が含まれる必要があります。
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)。デフォルトでは、メタデータ署名は必要ありません。
6. Fortify Software Security Centerにログインし、Fortifyのヘッダで [**ADMINISTRATION**]を選択します。
7. [ADMINISTRATION]ビューの左ペインで、 [**Configuration**]を選択し、 [**SSO**]を選択します。

   [SINGLE SIGN ON]ページが開きます。

   注: 1度に設定できるFortify Software Security Centerのシングルサインオンソリューションは1つのみです。

   SAML以外のシングルサインオンソリューションが現在設定されている場合、その名前がリストに表示されます。
8. 使用可能なシングルサインオンソリューションのリストから、 [**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の場所 (ステップ3で取得したメタデータ): `file:///location/of/idp-metadata.xml` **注:** Azure ADと統合している場合は、Azureの [**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 [**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	説明
	フィールドが表示されます)。 **注:** 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) **注:** SCIMプロトコルを使用して、Azure ADからのユーザデータでFortify Software Security Centerをプロビジョニングする場合は、Azureの［**Azure AD Identifier**］フィールドに表示されている値を使用します。(［**Set up <*application_name*>**］の［SAML-based Sign-on］ページにこのフィールドが表示されます)。
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。実行中のSSCインスタンスのURLを使用することを推奨します。 **重要** SAMLを正常に統合するには、クライアントコンピュータとサーバコンピュータ(IdPとSP)のクロックを同期する必要があります。
SP alias	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。
Keystore location	SAMLアサーションを暗号化および署名するためのJavaキーストアの場所

フィールド	説明
	注: 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。キーストアには、ルートCA証明書と署名の中間CA証明書が含まれる必要があります。
Keystore password	Javaキーストアファイルのパスワード
Signing & encryption key	署名/暗号化キー
Signing & encryption key password	署名/暗号化キーパスワード
SAML name identifier	ユーザ名属性(任意の文字列アサーション属性)

10. [SAVE]をクリックします。

重要 クライアントとサーバの時刻を同期させる必要があります。

11. *<fortify.home>*/*<app-context>*/conf/app.propertiesのhost.url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。URLは、Fortify Software Security Center SAMLメタデータのベースURLとして使用されます。
12. Fortify Software Security Centerを再起動します。
13. *<hostname>*:*<port>*/*<context>*/saml/metadataでFortify Software Security Center(SP)メタデータを生成します。
14. 前のステップで生成されたメタデータを開き、次の値が[SAML SSO]タブで指定した値と同じことを確認します。
    - エンティティIDの値は、"SP entity ID" 前のページで指定した値と一致します。
    - メタデータ内のSPエイリアスは、"SP alias" 前のページで指定したエイリアスです。
    - <AssertionConsumerService>バインディング内の場所URLは、IdPサーバからアクセスできます。
15. Fortify Software Security CenterメタデータをIDPサーバにアップロードします。
16. *<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Fortify Software Security Centerにリダイレクトされます。

注: Fortify Software Security Centerの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"

ページ154を参照してください。

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、Fortify Software Security Center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ユーザまたはローカルFortify Software Security Centerユーザとも一致しません(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。
  - Fortify Software Security Center 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。
  - Fortify Software Security Centerにユーザが存在します。
  - 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" ページ95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必要があります。IdPがプロキシサーバの背後にある場合、Fortify Software Security Center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Fortify Software Security Centerの設定" ページ149

SCIM/Azure AD統合のためのSSM 2.0シングルサインオンの設定

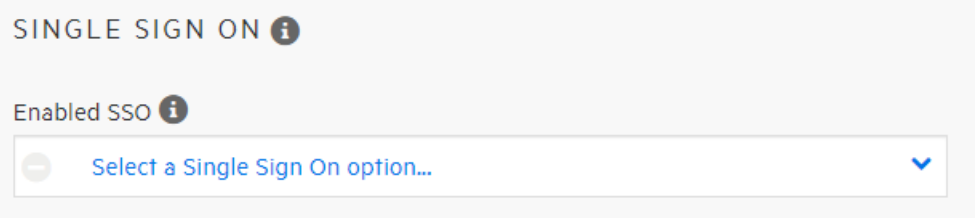
次の手順では、AZURE ADへの接続を設定するためにSCIM 2.0およびSM SAML 2.0を設定するために必要な手順について説明します。SAML 2.0準拠のシングルサインオンソリューションを使用するためにFortify Software Security Centerを設定する一般的な手順については、"SAML 2.0準拠のシングルサインオンソリューションを使用するためのFortify Software Security Centerの設定" ページ141」を参照してください。

注: SAMLのシングルログアウトは、Fortify Software Security Centerでサポートされています。

注意 SAMLを正常に統合するには、クライアントコンピュータとサーバコンピュータ(IdPとSP)のクロックを同期する必要があります。

Azure ADとSAML 2.0を使用するSSOが機能するようにFortify Software Security Centerを設定するには、次の手順に従います。

1. IdPサーバからSAMLメタデータを取得し、それをFortify Software Security Centerファイルシステムに保存します。
2. 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">)。
3. Fortify Software Security Centerにログインし、Fortifyのヘッダで[**ADMINISTRATION**]を選択します。
4. [ADMINISTRATION]ビューの左ペインで、[**Configuration**]を選択し、[**SSO**]を選択します。
   [SINGLE SIGN ON]ページが開きます。



   SAML以外のシングルサインオンソリューションが現在設定されている場合、その名前がリストに表示されます。
5. 使用可能なシングルサインオンソリューションのリストから、[**SAML**]を選択します。
6. 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の場所です。Azureの[**App Federation Metadata Url**]フィールドに値を入力します。(Azureの左側のペインの[**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)。 `file:///location/of/idp-metadata.xml` **注:** 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)。Azureの[**Azure AD Identifier**]フィールドに表示

フィールド	説明
	されている値を使用します。(「Set up <*application_name*>」の 「SAML-based Sign-on」ページの 「Azure AD Identifier」フィールドが表示されます)。
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。実行中のFortify Software Security CenterインスタンスのURLを使用することを推奨します。 **重要** SAMLを正常に統合するには、クライアントコンピュータとサーバコンピュータ(IdPとSP)のクロックを同期する必要があります。
SP alias	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。 **重要** SAMLを正常に統合するには、クライアントコンピュータとサーバコンピュータ(IdPとSP)のクロックを同期する必要があります。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。キーストアには、ルートCA証明書と署名の中間CA証明書が含まれる必要があります。
Keystore location	SAMLアサーションを暗号化および署名するためのJavaキーストアの場所
Keystore password	Javaキーストアファイルのパスワード
Signing & encryption key	署名/暗号化キー
Signing & encryption	署名/暗号化キーパスワード

フィールド	説明
key password	
SAML name identifier	ユーザ名属性(任意の文字列アサーション属性)

7. [SAVE]をクリックします。

重要 クライアントとサーバの時刻を同期させる必要があります。

8. <*fortify.home*>/<*app-context*>/conf/app.propertiesのhost.urlプロパティが、Azure ADがアクセスできるURLを指定していることを確認します。URLは、Fortify Software Security Center SAMLメタデータのベースURLとして使用されます。
9. Fortify Software Security Centerを再起動します。
10. <*hostname*>:<*port*>/<*context*>/saml/metadataでFortify Software Security Center(SP)メタデータを生成します。
11. 前のステップで生成されたメタデータを開き、次の値が[SAML SSO]タブで指定した値と同じことを確認します。
    - エンティティIDの値は、"SP entity ID" 前のページで指定した値と一致します。
    - メタデータ内のSPエイリアスは、"SP alias" 前のページで指定したエイリアスです。
    - <AssertionConsumerService>バインディング内の場所URLは、Azure ADからアクセスできます。
12. Azure ADにFortify Software Security Centerメタデータをアップロードします。
13. <*hostname*>:<*port*>/<*app_context*>へのアクセスを試みます。

Azure AD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、Azure AdからFortify Software Security Centerにリダイレクトされます。

注: Fortify Software Security Centerの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" ページ154を参照してください。

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、Fortify Software Security Center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ユーザまたはローカルFortify Software Security Centerユーザとも一致しません(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。

- Fortify Software Security Center 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。
- Fortify Software Security Centerにユーザが存在します。
- 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" ページ95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必要があります。IdPがプロキシサーバの背後にある場合、Fortify Software Security Center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Fortify Software Security Centerの設定" 下

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Fortify Software Security Centerの設定

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

1. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. 左ペインで、 [Configuration]を選択してから、 [SSO]を選択します。
   [SINGLE SIGN ON]ページが開きます。

   注: Fortify Software Security Centerに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. 使用可能なシングルサインオンソリューションのリストから、 [HTTP]を選択します。
4. [HTTP SSO Integration Attributes]で、次の設定をします。

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	Fortify Software Security Centerからログアウト後にリダイレクトするログアウトページアドレスを入力します。
SSO Logout	動的ディレクティブヘッダを入力します。

フィールド	説明
Response Header	
SSO Logout Response Code	このボックスに動的ディレクティブコードを入力します。
SSO Logout Response Text	このボックスに動的ディレクティブメッセージを入力します。

5. [SAVE]をクリックします。
6. LDAP認証を使用するようにFortify Software Security Centerを設定します。詳細については、"LDAPユーザ認証" ページ105を参照してください。
7. サーバを再起動します。

注: Fortify Software Security Centerの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" ページ154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Fortify Software Security Centerの設定" ページ139

Fortify Software Security CenterでのKerberos認証の設定

Fortify Software Security CenterでKerberos認証を設定するには、次の手順に従います。

注意 SPNEGO/Kerberos SSOでは、HTTPヘッダを介して大量のデータをFortify Software Security Centerに転送する必要があります。ヘッダサイズの制限が不十分な場合、「Bad Request」エラーが発生します。ヘッダサイズの制限を大きくするには、Tomcatサーバコネクタの`maxHttpHeaderSize`プロパティを設定します。

1. Active Directoryアカウントを作成し、次のようにアカウントのサービスプリンシパル名(SPN)を登録します。
   ```
   setspn -U -S HTTP/SSCServer.mydomain.lan SSCKerberos
   ```
2. keytabファイルを作成します。
   例:
   ```
   ktpass -out c:\SSCSERVER.keytab -princ HTTP/
   SSCServer.mydomain.lan@mydomain -mapUser mydomain\SSCKerberos -
   mapOp set -pType KRB5_NT_PRINCIPAL /crypto all /kvno 0 -pass
   3o(t&gSp&3hZ4#t9
   ```
3. (Linuxのみ)少なくとも、`krb5.conf`ファイルに次の情報が含まれていることを確認してください。
   ```
   [libdefaults]

    default_realm = EXAMPLE.COM

   [realms]
   EXAMPLE.COM = {

   kdc = kerberos.example.com

   admin_server = kerberos.example.com

   }
   ```
4. 管理者としてFortify Software Security Centerにログインし、Fortifyのヘッダで[ADMINISTRATION]を選択します。
5. [ADMINISTRATION]ビューの左ペインで、[Configuration]を選択し、[SSO]を選択します。
   [SINGLE SIGN ON]ページが開きます。

   注: Fortify Software Security Centerに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。
6. [Enabled SSO]リストから[SPNEGO/KERBEROS]を選択します。
7. [SPNEGO/Kerberos Integration Attributes]で、次の表に示す情報を入力します。

フィールド	説明
Service principal name	Kerberosレルム内のFortify Software Security Centerのサービスプリンシパル名(SPN)です。指定する値には、Kerberos初期化ファイルで構成されたレルム名を含められます。

Keytab location	Fortify Software Security Centerプリンシパルキーを含むkeytabファイル(ステップ2で作成)の場所です。この場所では、ファイルURIスキームを使用してファイルへの絶対パスを指定する必要があります。
	Windowsの例:
	`file:///C:/Users/fortify/secrets/krb.keytab`
	Linuxの例:
	`file:///home/fortify/secrets/krb.keytab`

Krb5.conf location	オプションの`krb5.conf`ファイルの場所です。これにより、`java.security.krb5.conf`プロパティが設定されます。この場所では、ファイルURIスキームを使用してファイルへの絶対パスを指定する必要があります。例については、Keytab locationを参照してください。
Enable debug mode	デバッグモードを有効にするには、このチェックボックスを選択します。

8. [SAVE]をクリックします。
9. LDAPサーバのユーザ[User username attribute]の設定が正しいか確認します。("LDAPサーバの設定" ページ108を参照してください)。
10. サーバを再起動します。
11. LDAPユーザ名が正しく解決されていることを確認します。LDAPユーザ名の値を次のようにフォーマットします。

```
username@domain
```

12. 次のようにブラウザの設定を確認します。
    - Firefoxの場合は、サービスURLを`network.negotiate-auth.trusted-uris`(`about:config`)に追加します。たとえば、`service-machine.my.domain.lan`になります。
    - Internet ExplorerおよびChromeの場合は、イントラネットおよび信頼済みサイトにサービスURLを追加し、ローカルイントラネットゾーン設定に対してのみ自動ログオンを設定し、統合Windows認証を有効にします。

重要 Fortify Software Security Center LDAP設定のユーザ名マッピングがLDAPユーザエントリ属性と一致することを確認します。この属性には、Kerberosチケットで送信されたユーザ名が保持されます。Microsoft Active Directoryを使用する構成では、User Principal Name (UPN)属性はKerberosチケットで送信されたユーザ名を保持する必要があります。ただし、環境設定を変更する前にこれを確認してください。

注意 Fortify Software Security Centerで**SPNEGO/Kerberos** SSOソリューションを使用するように設定されている場合に、ユーザ(ローカルおよびLDAP)がユーザ名とパスワードを使用してログインできるようにする場合は、直接有効にする必要があります。手順については、"Fortify Software Security Center がX.509またはKerberos SSOソリューションを使用するように設定されている場合にユーザ名およびパスワードログインを有効にする" 次のページを参照してください。

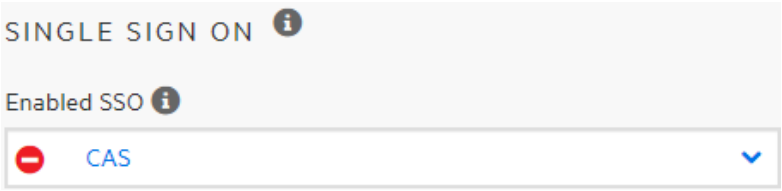
参照情報
"シングルサインオンを使用するためのFortify Software Security Centerの設定" ページ 139

X.509証明書ベースのSSOを使用するためのFortify Software Security Centerの設定

X.509証明書ベースのSSOを使用するようにFortify Software Security Center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。詳細については、https://tomcat.apache.org/tomcat-9.0-doc/config/http.html#SSL_Support_-_CertificateでcertificateVerificationおよび関連オプションを参照してください。
2. 管理者としてFortify Software Security Centerにログインし、[**ADMINISTRATION**]タブをクリックします。
3. [ADMINISTRATION]ビューの左ペインで、[**Configuration**]を選択し、[**SSO**]をクリックします。
   [SINGLE SIGN ON]ページが開きます。

   注: Fortify Software Security Centerに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。

4. 使用可能なシングルサインオンソリューションのリストから、[**X.509**]を選択します。
5. [**X.509 certificate username pattern**]ボックスに、X.509証明書からユーザ名を取得するためにFortify Software Security Centerで使用する正規表現を入力します。

注: 証明書のサブジェクトのCN属性と一致させるには、`CN=(.*?)`を指定できます。

6. [SAVE]をクリックします。
7. 設定を実装するには、Fortify Software Security Centerサーバを再起動します。

注意 X.509証明書ベースのSSOを使用するようにFortify Software Security Centerを設定する場合、ユーザ(ローカルおよびLDAP)がユーザ名とパスワードを使用してログインするには、ユーザ名とパスワードを直接有効にする必要があります。手順については、"Fortify Software Security CenterがX.509またはKerberos SSOソリューションを使用するように設定されている場合にユーザ名およびパスワードログインを有効にする" 下を参照してください。

Fortify Software Security CenterがX.509またはKerberos SSOソリューションを使用するように設定されている場合にユーザ名およびパスワードログインを有効にする

Fortify Software Security CenterがX.509またはKerberos SSOソリューションを使用するように設定されている場合、ローカルログインがデフォルトで無効になっています。ユーザ(ローカルおよびLDAP)が自分のユーザ名とパスワードを使用してログインできるようにするには、ローカル認証を次のように直接有効にする必要があります。

1. *<fortify.home>*/*<app_context>*/conf に移動して、app.propertiesファイルをテキストエディタで開きます。
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。

参照情報

"X.509証明書ベースのSSOを使用するためのFortify Software Security Centerの設定 " 前のページ

"Fortify Software Security CenterでのKerberos認証の設定 " ページ151

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

Fortify Software Security Center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。

Fortify Software Security Centerの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. *<fortify.home>*/*<app_context>*/conf ディレクトリに移動して、log4j2.xmlファイルをテキストエディタで開きます。
2. HTTPヘッダを使用するシングルサインオン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.FmHttpSsoAuthenticationFi
lter" level="debug"/>
```

3. SAML 2.0準拠のシングルサインオンソリューションの場合は、<!-- SSO SAML -->のマークが付いたセクションを見つけて、ロガーレベルを適切なデバッグ値に変更します。
4. CASシングルサインオンソリューションの場合は、<!-- SSO CAS -->のマークが付いたセクションを見つけて、ロガー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Fortify Software Security Centerの設定" ページ 139

トークン認証が必要なWebサービスの設定

Webサービスのトークン認証は、Fortify Software Security Centerの［ADMINISTRATION］ビューの［**Configuration**］セクションで有効または無効にします。

Fortify Software Security Centerでは、SOAP (Simple Object Access Protocol) Webサービスを使用する場合、次の2種類の認証をサポートします。

- ユーザ名とパスワードは、すべての要求で提供されます。
- 一時的なセキュリティトークンが生成され、認証用に渡されます。

トークン認証はデフォルトで有効になっています。トークン認証を使用しない場合は、［WEB SERVICE ATTRIBUTES］ページで無効にする必要があります。

認証トークンの詳細については、"fortifyclient認証トークン" ページ386を参照してください。

トークン認証を有効または無効にするには、次の手順を実行します。

1. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで［**ADMINISTRATION**］を選択します。
2. 左ペインで、［**Configuration**］を選択してから、［**Web Services**］を選択します。
   ［WEB SERVICE ATTRIBUTES］ページが開きます。
3. 次のいずれかを実行します。
   - トークン認証を有効にするには、［**Allow token authentication**］チェックボックスをオンにします。
   - トークン認証を無効にするには、［**Allow token authentication**］チェックボックスをオフにします。
4. ［**SAVE**］をクリックします。
5. サーバを再起動します。

Fortify Software Security Centerのログレベルの変更

Fortify Software Security Centerのログレベルの設定を変更するには、次の手順に従います。

1. *<fortify.home>*/*<app_context>*/confに移動し、テキストエディタでlog4j2.xmlファイルを開きます。
2. 98行目で、<Root level="warn">を<Root level="debug">に変更します。
3. ファイルを保存して閉じます。

設定の変更には約10秒かかります(設定内のmonitorInterval属性の値によって定義されます)。

注: 新しいロガーを追加し、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。

連邦情報処理標準を設定する(Fortify Software Security CenterをFortify WebInspect Enterpriseと統合する場合のみ)

Fortify Software Security CenterをFortify WebInspect Enterpriseと統合する場合は、連邦情報処理標準(FIPS)のコンプライアンスを有効にする必要があります。

OpenSSLがFIPSモードで動作することを要求するには、少なくともFIPSMode属性をonに設定する必要があります。OpenSSLが強制的にFIPSモードに入るようにするには、この属性をenterに設定します(OpenSSLがすでにFIPSモードの場合はエラーが発生します)。OpenSSLがすでにFIPSモードに入っている(OpenSSLがまだFIPSモードでない場合にエラーが発生する)ことを要求するには、この属性をrequireに設定します。

重要 FIPSモードで必要となるFIPS対応のOpenSSLライブラリは、自分で作成する必要があります。FIPSMode属性を上のいずれかの値に設定した場合は、SSLEngineも有効にする必要があります。

FIPS準拠暗号化を設定する方法については、ご使用のオペレーティングシステムのマニュアルを参照してください。

Fortifyバナーの組織向けカスタマイズ

Fortifyバナーをカスタマイズして、ユーザがログオンする場合やビュー(『DASHBOARD』、『APPLICATIONS』、『REPORTS』など)を切り替える場合に、組織のFortify Software Security Center Webサイトに関する情報を表示できます。

ユーザ用にカスタムのFortify Software Security Centerログオンエクスペリエンスを作成するには、次の手順を実行します。

1. <ssc.war>\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<!-- Add your custom banner here -->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、赤いテキストを含むバナーをWebページの最上部に追加します。ユーザがFortify Software Security Centerにログオンするたびにバナーが表示されます。

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

   My banner

   注意 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。行を追加すると、ユーザインタフェース表示に干渉します。

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. <*new_directory*>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ssc-htmlui-<*version*>.jarという名前で作成します。

   注: <*new_directory*>自体を新しいアーカイブに含めないでください。

8. Fortify Software Security Centerサーバを再起動します。

ユーザがFortify Software Security Center(『DASHBOARD』、『APPLICATIONS』、『REPORTS』など)でビューを切り替えるごとに表示するメッセージバナーを作成するには、次の手順を実行します。

1. <ssc.war>\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\app\ssc\views\partialsディレクトリに移動します。
4. テキストエディタでpageheader.htmlファイルを開きます。
5. テキスト<!-- Add your custom banner here -->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、赤いテキストを含むバナーをWebページの最上部に追加します。ユーザがビューを切り替えるたびにバナーが表示されます。

   ```
   <center><font color=red><message text></font></center>
   ```

   注意 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。行を追加すると、ユーザインタフェース表示に干渉します。

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. <*new_directory*>以下にあるすべてのファイルとディレクトリを含む新しいアーカイブをssc-htmlui-<*version*>.jarという名前で作成します。

   注: <*new_directory*>自体を新しいアーカイブに含めないでください。

8. Fortify Software Security Centerサーバを再起動します。

第7章: 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Fortify Software Security Center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。

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および［AUDIT］ビューに表示されるFortify Software Security Center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Fortify Software Security Center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. Fortify Software Security Centerに管理者としてログインし、Fortifyのヘッダで［**ADMINISTRATION**］をクリックします。
2. ［ADMINISTRATION］ビューの左ペインで、［**Configuration**］を選択し、［**Core**］を選択します。
   ［**Core**］ページが開きます。
3. ページの下部までスクロールし、［**Enable Export to CSV**］チェックボックスをオフにします。
4. ［**SAVE**］をクリックします。

参照情報

"コア設定の設定" ページ95

"データをカンマ区切り値ファイルへエクスポートする" ページ202

バグトラッカーの統合について

Fortify Software Security Centerを使用すると、チームは問題の監査中にFortify Software Security Centerからバグトラッキングシステムにバグを送信できます。Fortify Software Security Center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。

- Bugzilla

  注: BugzillaバグトラッカープラグインとBugzillaでXML-RPCを有効にする必要があります。手順については、https://www.bugzilla.org/docs/4.4/en/html/api/Bugzilla/WebService/Server/XMLRPC.htmlを参照してください

- Jira

- Jira Cloud

  注: Jira Cloudを使 用 する場 合 は、ログイン時 に 『Password』フィールドでJira認 証トークンを使 用 する必 要 があります。

- ALM
- Azure DevOps Server

  重 要 Azure DevOpsの 『Repro Steps』フィールド(Fortifyバグの説 明 を表 示)は、『Issue』作 業 アイテムのデフォルトでは非 表 示 になっています。Azure DevOps 2019.1以 降 を使 用 し、基 本 プロセスを使 用 する場 合 は、『Issue』作 業 アイテムをカスタマイズして 『Repro Steps』フィールドを表 示 する必 要 があります。

注: 組 織 で、Fortify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 " ページ397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、"バグトラッキングシステムを使 用 したセキュリティ脆 弱 性 の管 理 " ページ240を参 照 してください。

バグトラッカプラグインの管 理

次 のセクションでは、バグトラッカプラグインをシステムに追 加 したりシステムから削 除 したりする方 法 について説 明 します。

重 要 Bugzillaバグトラッカプラグインと正 常 に統 合 するには、BugzillaでXML-RPCを有 効 にする必 要 があります。手 順 については、https://www.bugzilla.org/docs/4.4/en/html/api/Bugzilla/WebService/Server/XMLRPC.htmlを参 照 してください。

バグトラッカプラグインの追 加

Fortify Software Security Center管 理 者 は、Fortify Software Security Center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。

重 要 認 証 ありのプロキシとhttpsのバグトラッカドメインを使 用 しても機 能 しません。接 続 を正 常 に行 う場 合 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. 管 理 者 としてFortify Software Security Centerにログインし、Fortifyのヘッダで、『ADMINISTRATION』を選 択 します。

2. [ADMINISTRATION]ビューの左 ペインで、 [**Plugins**]を選 択し、 [**Bug Tracking Plugins**]を選 択します。
   [Bug Tracking]ページが開きます。
3. ページヘッダで、 [**NEW**]をクリックします。
   Fortify Software Security Centerに、 [UPLOAD PLUGIN WARNING]ダイアログボックスが表 示されます。
4. 警 告を読み、プラグインのアップロードに伴う潜 在 的なリスクを受 け入 れる場 合 は、 [**OK**]をクリックします。
   [UPLOAD PLUGIN BUNDLE]ダイアログボックスが開きます。
5. [**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。
6. [**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

"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" ページ245

バグトラッカプラグインの削 除

Fortify Software Security Center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. 管 理 者 としてFortify Software Security Centerにログインし、Fortifyのヘッダで、 [**ADMINISTRATION**]を選 択します。
2. [ADMINISTRATION]ビューの左 ペインで、 [**Plugins**]を選 択し、 [**Bug Tracking Plugins**]を選 択します。
   [Bug Tracking]ページが開きます。
3. 削 除 するプラグインの行 を展 開します。
4. [**Disable**]をクリックし、プラグインが無 効 になった後 で [**REMOVE**]をクリックします。

参 照 情 報

"バグトラッカーの統 合 について" ページ159

"パーサプラグインの追 加 と管 理 " ページ164

"バグトラッカプラグインの作 成 " ページ397

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

Fortify Software Security Center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カにマップされます。

各 バグトラッカには、異 なるバグパラメータのセット が用 意 されています。また、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、Fortify Software Security Centerによって問 題 のバグIDが保 存 されます。

重 要 Fortify Software Security Center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 なバグトラッカ証 明 書 も、Fortify Software Security Centerが展 開 されているJava仮 想 マシンにインポートする必 要 があります。

バグトラッカパラメータ

バグトラッカを使 用 して送 信 されるバグでは、 [**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 を入 力 する必 要 があります。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。Fortify Software Security Center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 " ページ397を参 照 するか、または、Fortify Support (https://www.microfocus.com/support)に問 い合わせてください。

ALMパラメータ

ALM欠 陥トラッカの [Submit Bug]ダイアログボックスで、ALM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 Fortify Static Code Analyzerスキャンにはビルドラベルでタグ付 けされる必 要 があります。Fortify Software Security Centerではビルドラベルを使 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、ソースアナライザツールを実 行 してソースコードを分 析 モデルに変 換 するときに`-build-label <SVN_Revision_Number>`コ

マンドオプションを含めます。

- ALM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する必要があります。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にログインした後に[**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。

注: ALMのバグを表示するには、ALMブラウザプラグインをインストールし、ALM互換ブラウザを使用する必要があります。

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

Eclipseプラグイン更新サイトの設定

Eclipse更新サイトをホストするためにFortify Software Security Centerを使用できます。これにより、Fortify Plugin for Eclipseを中央の場所から配布でき、各開発者がプラグインをローカルにインストールする必要がなくなります。

Eclipse更新サイトを設定するには、次の手順を実行します。

1. `<ssc_install_dir>/WEB-INF/internal`に移動し、テキストエディタで`securityContext.xml`ファイルを開きます。

   注: `<ssc_install_dir>`は、Fortify Software Security Centerが展開されるディレクトリです。

2. 次のテキスト行を探します。

   ```
   <!--<security:intercept-url pattern="/update-site/**" access="PERM_
       ANONYMOUS"/>-->
   ```

3. テキスト行からコメントタグを削除して、次のようにします。

   ```
   <security:intercept-url pattern="/update-site/**" access="PERM_
       ANONYMOUS"/>
   ```

4. `securityContext.xml`ファイルを保存します。
5. Eclipse更新サイトのマッピングを有効にします。
6. `Fortify_SCA_and_Apps`インストーラを実行します。
7. `<sca_install_dir>/plugins/eclipse`のコンテンツ(`site.xml`ファイルと、featuresおよびpluginsディレクトリ内のjarファイルで構成されます)をWebサーバ上の`update-site`ディレクトリにコピーします。`<sca_install_dir>`は、Static Code Analyzerおよびアプリケーションインストーラによってファイルがインストールされた場所です。

開発者はEclipse IDEからURLを参照できます。クライアント側インストールの詳細については、『Micro Focus Fortify Plugins for Eclipseインストールおよび使用ガイド』を参照してください。

パーサプラグインの追加と管理

Fortify Software Security Center管理者は、Fortify Software Security Center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。

ヒント: Fortify Software Security Center用に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の「Sample parser plugin」ページを参照してください (https://github.com/fortify/sample-parser)。

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. 管理者としてFortify Software Security Centerにログインし、Fortifyのヘッダで、[ADMINISTRATION]を選択します。
2. 左ペインで、[Plugins]を選択し、[Parser Plugins]を選択します。
   [Parsers]ページが開きます。
3. [Parsers]ページヘッダで、[NEW]をクリックします。
   Fortify Software Security Centerに、サードパーティ製プラグインをアップロードするリスクについてアドバイスする[Upload Plugin Warning]が表示されます。
4. 警告を確認して続行するには、[OK]をクリックします。
   [Upload Plugin Bundle]ダイアログボックスが開きます。
5. [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. [START UPLOAD]をクリックします。
   [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。
   Fortify Software Security Centerに、テストしていないプラグインを有効にするリスクについてアドバイスする[Enable Plugin Warning]が表示されます。
9. [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" ページ160

Sonatype結果を表示するためのFortify Software Security Centerの準備

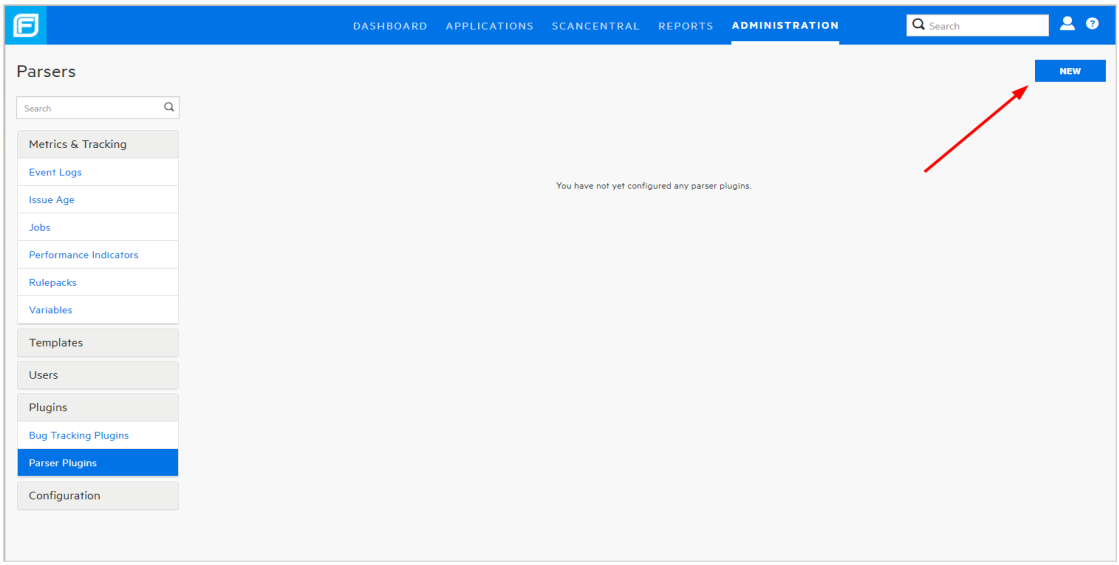
アプリケーションバージョンに関するSnatypeのNexus Lifecycleソリューションスキャン結果のオープンソースセキュリティデータは、Fortify Software Security Centerの[AUDIT]ページまたは[OPEN SOURCE]ページで表示できます。そうするには、まず必要なSnatype Parser Pluginをダウンロードしてインストールする必要があります。この操作を完了する

と、Fortify SourceAndLibScannerを使 用してFortify Software Security CenterにアップロードされたSonatypeスキャン結 果 が表 示 されます。

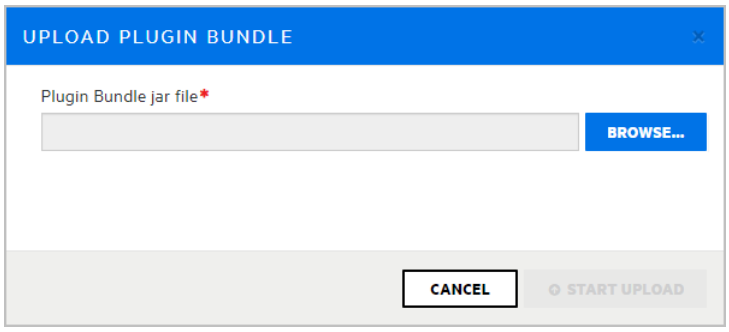
SourceAndLibScannerを取 得 するには、https://marketplace.microfocus.com/fortify/content/fortify-sourceandlibscannerに移動します。SourceAndLibScannerを使 用して、Sonatypeスキャン結 果 をFortify Software Security Centerにアップロードする方 法 については、『Micro Focus Fortify SourceAndLibScannerユーザガイド』を参 照してください。このガイドはFortify SourceAndLibScannerユーティリティにパッケージされています。

アップロードされたSonatypeデータを表 示 するためのFortify Software Security Centerの準 備 をするには、次 の手 順 に従 います。

1. ブラウザウィンドウを開き、Fortify Marketplace (https://marketplace.microfocus.com/fortify/content/sonatype-nexus-lifecycle-integration-with-ssc)に移 動します。
2. 「**Sonatype Lifecycle integration with SSC**」ページで、「**DOWNLOAD**」をクリックします。
3. `SonatypeFortifyBundle.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Fortify Software Security Centerにログオンします。
5. Fortifyのヘッダで、「**ADMINISTRATION**」を選 択します。
6. 左 ペインで、「**Plugins**」セクションを展 開 し、「**Parser Plugins**」を選 択します。

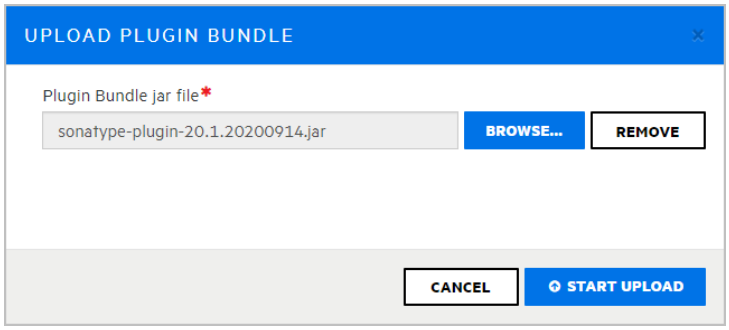


7. 「Parsers」ページで、「**NEW**」をクリックします。
8. 「UPLOAD PLUGIN WARNING」を閉じ、「**OK**」をクリックします。



[UPLOAD PLUGIN BUNDLE]ダイアログボックスが開きます。

9. [BROWSE]をクリックし、`sonatype-plugin-<version>.jar`に移 動して選 択します。



10. [UPLOAD PLUGIN BUNDLE]ダイアログボックスで、 [START UPLOAD]をクリックします。

    Fortify Software Security Centerは、アップロードが成 功したと知らせるメッセージを表 示します。 [Parsers]ページに、Sonatype Vulnerability Parserが一 覧 表 示されます。

11. Sonatype Vulnerability Parserの行を展 開し、 [ENABLE]をクリックします。
12. [ENABLE PLUGIN WARNING]を読み、 [OK]をクリックします。

参照情報

"Webアプリケーションの被 影 響 性 分 析 について" ページ336

"Sonatypeデータの表 示" ページ338

"Sonatype結 果 の監 査" ページ342

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 Fortify Software Security Center 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、Fortify Software Security Center 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 Fortify Software Security Center 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。

Fortify Software Security Center 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、 [AUDIT]ページから管 理 者 ユーザに問 題を割り当 てることができます。

参照情報

"Fortify Software Security Centerの役 割 に関 する許 可 情 報 の表 示" ページ169

Fortify Software Security Center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Fortify Software Security Center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:

Fortify Software Security Centerユーザアカウント

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、Fortify Software Security Center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 データに対 して読 み取り専 用 アクセス権 を持ちます。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、Software Security CenterからFortify WebInspect Enterpriseイン スタンスを登 録 および登 録 解 除 し、また、監 査 情 報 を取 得 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。

ユーザアカウント の詳 細 については、"ユーザアカウント とアクセス" ページ 194を参 照 してく ださい。

関 連 項 目

"ユーザアカウント の作 成 について" 下

"ローカルユーザアカウント のロック解 除 " ページ 215

ユーザアカウント の作 成 について

Fortify Software Security Centerのユーザモジュールには、ローカルユーザアカウント の編 集 、削 除 、またはー 時 停 止 に使 用 するツールが提 供 されています。

初 めてFortify Software Security Centerにログオンした後 、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 してから、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。

注 : Fortify Software Security Center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 またはー 時 停 止 できます。Fortify Software Security Centerでは、このようなアカウントに対 するー 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 の作 成 方 法 については、"ローカルユーザアカウント の作 成 " ページ 210を 参 照 してください。

Fortify Software Security Center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 " ページ 95を参 照 してください。ユーザアカウント 権 限 の 詳 細 については、"Fortify Software Security Centerのユーザアカウント 管 理 " ページ 207を参 照 してください。

参 照 情 報

"Fortify Software Security Centerの役 割 に関 する許 可 情 報 の表 示 " 次 のページ

"ローカルユーザアカウント のロック解 除 " ページ 215

Fortify Software Security Center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

注 意 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Fortify Software Security Center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Fortify Software Security Centerにアップロードされるのを防 ぐには、次 を確 認 します。

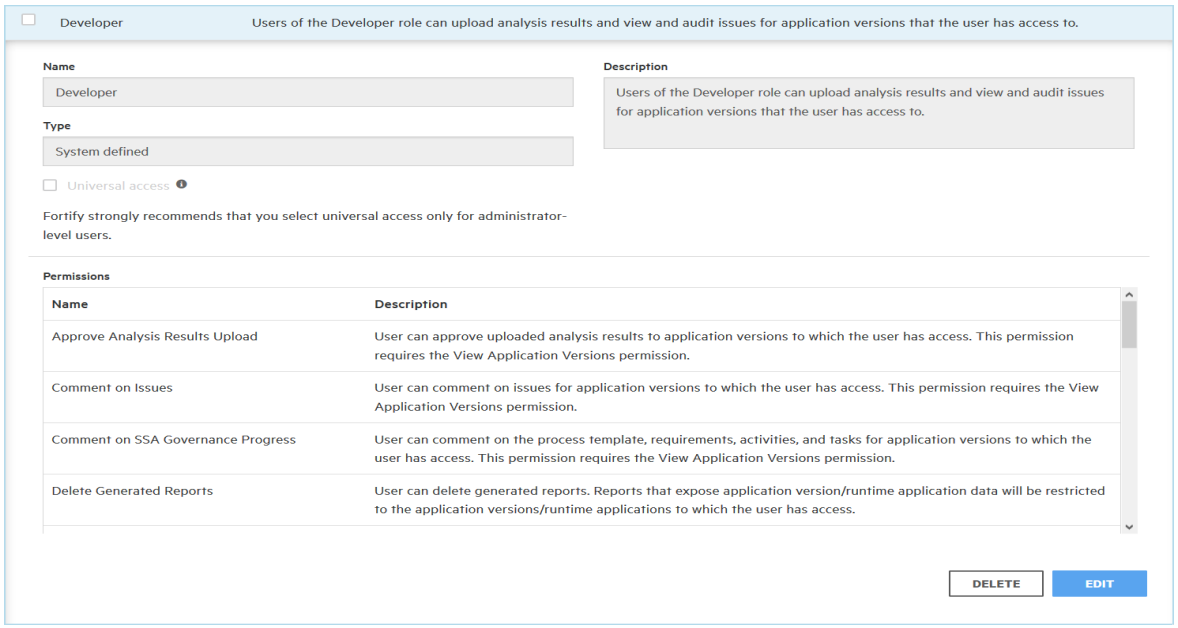
- 信 頼 されたユーザにのみアクセス許 可 を割 り当 てます。
- Fortify Software Security Centerにアップロード する前 に、すべてのカスタムテンプレートで任 意 のSQLクエリとコマンドをチェックしてください。

Fortify Software Security Centerの役 割 に関 する許 可 情 報 の表 示

さまざまなFortify Software Security Centerの役 割 が割 り当 てられたユーザが実 行 できるアクションに関 する詳 細 情 報 を表 示 するには、次 の手 順 に従 います。

1. Fortifyのヘッダで、 [ADMINISTRATION]を選 択 します。
2. 左 ペインで、 [Users]、 [Roles]の順 に選 択 します。
   [Roles]ページには、システム内 のすべての役 割 の名 前 と説 明 のリスト が表 示 されます。
3. 目 的 の役 割 の行 を選 択 します。

行 が展 開 され、役 割 の詳 細 (その役 割 に割 り当 てられたユーザに付 与 されているすべての許 可 のリスト が表 示 されるテーブルを含 む)が表 示 されます。



ユーザアカウントの詳 細については、"ユーザアカウントの管 理 " ページ207を参 照してください。

関 連 項 目

"ユーザアカウントの作 成 について" ページ168

"事 前 設 定 済 みの役 割 " ページ207

"ローカルユーザアカウントのロック解 除 " ページ215

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。

Fortify Software Security Centerのグループメンバーシップ

Fortify Software Security Center 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。ユーザがログオンすると、Fortify Software Security CenterがユーザをLDAPディレクトリ内 で調 べます。Fortify Software Security Center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 、Fortify Software Security Centerはそのユーザにすべての役 割 を割り当 てます。

Fortify Software Security Center 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 、Fortify Software Security Center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。

重 要 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、Fortify Software Security Center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。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 します。

参 照 情 報

"失 敗 したLDAPユーザログインの処 理" 下

失 敗 したLDAPユーザログインの処 理

Fortify Software Security Centerサーバにネストされたグループを設 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、不 正 な資 格 情 報 に関 するメッセージがログに記 録 されます。ただし、ログに「user is not authorized」というテキストが含 まれている場 合 、管 理 者 はユーザが正 しいLDAPグループに追 加 されていることを確 認 する必 要 があります。

ユーザがLDAP内 の正 しいグループに追 加 されていることを確 認 するには、次 の手 順 に従 います。

1. Fortifyのヘッダで、 [ADMINISTRATION]を選 択 します。
2. [ADMINISTRATION]ビューの左 ペインで、 [Users]を選 択 し、 [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、 [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、[ADMINISTRATION]ビューで、 [Event Logs]ページまたは [Jobs]ページのいずれかを確 認 します。

注 : データを更 新 すると、Fortify Software Security Centerへのアクセスがブロックされます。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

"Fortify Software Security Centerのグループメンバーシップ" 前 のページ

LDAPグループへのFortify Software Security Center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、Fortify Software Security Center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 なるアクセス権 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、Fortify Software Security Center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。異なるFortify Software Security Center役割に直接マップする新しいLDAPグループを作成することを推奨します。たとえばFORTIFY_ADMINSグループとFORTIFY_DEVELOPERSグループを作成できます。

Fortify Software Security Centerのグローバル検索機能

Fortify Software Security Center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きます。

グローバル検索は、初回ログ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。("Fortify Software Security Centerの初回設定" ページ69を参照してください)。

注: 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。なぜなら、アーティファクトアップロードジョブの最後に発生するようにスケジュールされている、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。

Fortify Software Security Centerサーバでグローバル検索を有効にするには、Tomcatサーバに検索インデックスディレクトリへの読み込みおよび書き込みアクセス権を提供する必要があります。

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

検索インデックスの問題のトラブルシューティング

グローバル検索機能について

Fortify Software Security Center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。グローバル検索は、初回ログ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。("Fortify Software Security Centerの初回設定" ページ69または"アップグレード後のFortify Software Security Centerの設定" ページ184を参照)。

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

"Fortify Software Security Centerのグローバル検 索 機 能 " 前 のページ

"検 索 インデックスの問 題 のトラブルシューティング" 下

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 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、Fortify Software Security Centerは起 動 時 ごとにインデックスを再 作 成 します。

Fortify Software Security Centerが最 初 のインデックスの作 成 に繰 り返 し失 敗 した場 合 は、インデックスディレクトリ全 体 を削 除 してからFortify Software Security Centerを再 起 動 します。

非 常 に大 きなデータベース(数 百 GB)で作 業 している場 合 、システムメモリが限 られているため、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、Fortify Software Security CenterのJavaのヒープサイズを増 やしてからFortify Software Security Center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、Micro Focus Fortify ソフトウェアシステム要 件 のドキュメントを参 照 してください)。

検 索 インデックスの保 守

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 [ADMINISTRATION]ビューから変 更 できます。Fortifyでは、このジョブを1日 1回 実 行 するスケジュールを設 定 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 " ページ131」を参 照 してください。

Fortify Software Security Centerの保 守 モードへの移 行

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Fortify Software Security Center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。

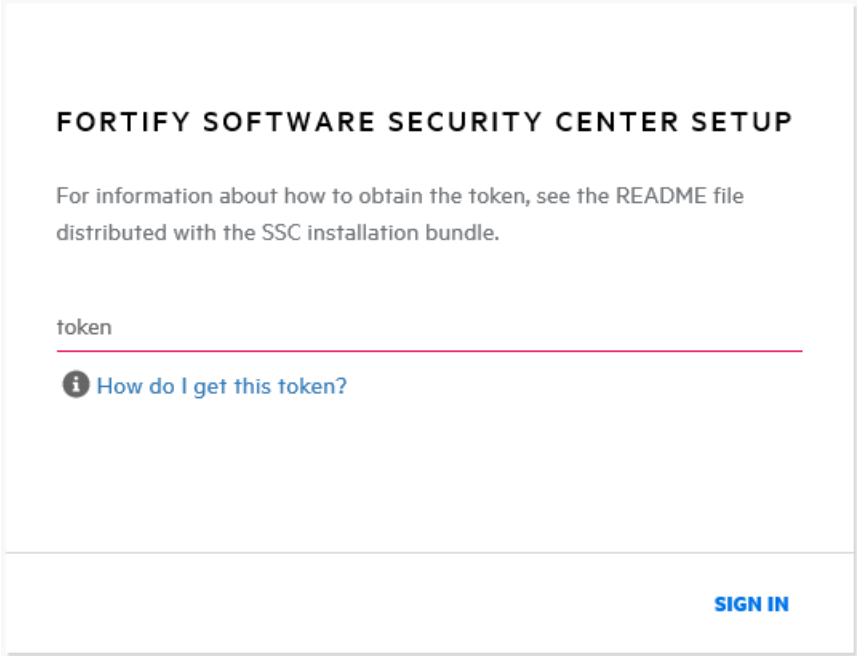
Fortify Software Security Centerを保 守 モードにするには、次 の手 順 に従 います。

1. Fortify Software Security Centerに管 理 者 としてログインし、Fortifyのヘッダで [**ADMINISTRATION**]を選 択 します。
2. 左 ペインで、 [**Configuration**]を選 択 してから、 [**Maintenance Mode**]を選 択 します。
   [Maintenance Mode]ページが開 きます。
3. [**Set to maintenance mode**]チェックボックスをオンにし、 [**SAVE**]をクリックします。

4. サーバを再 起 動します。
5. `<fortify.home>/<app_context>`ディレクトリに移 動し、`init.token`ファイルを開きます。
6. `init.token`ファイルの内 容 をクリップボードにコピーします。
7. Webブラウザウィンドウを開き、Fortify Software Security Centerインスタンスの URLを入 力します。

8. [Fortify Software Security Center Setup]画 面 の右 上 隅 の[ADMINISTRATORS]をクリックします。

9. `init.token`ファイルからコピーした文 字 列 をテキストボックスに貼 り付 け、[SIGN IN]をクリックします。

   Fortify Software Security Centerセットアップウィザードが開き、現 在 の環 境 設 定 すべてが表 示 されます。サーバ設 定 の情 報 については、"Fortify Software Security Centerの初 回 設 定" ページ69を参 照 してください。
10. サーバの設 定 が正 常 に完 了 したら、Tomcatを再 起 動します。

注: 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。

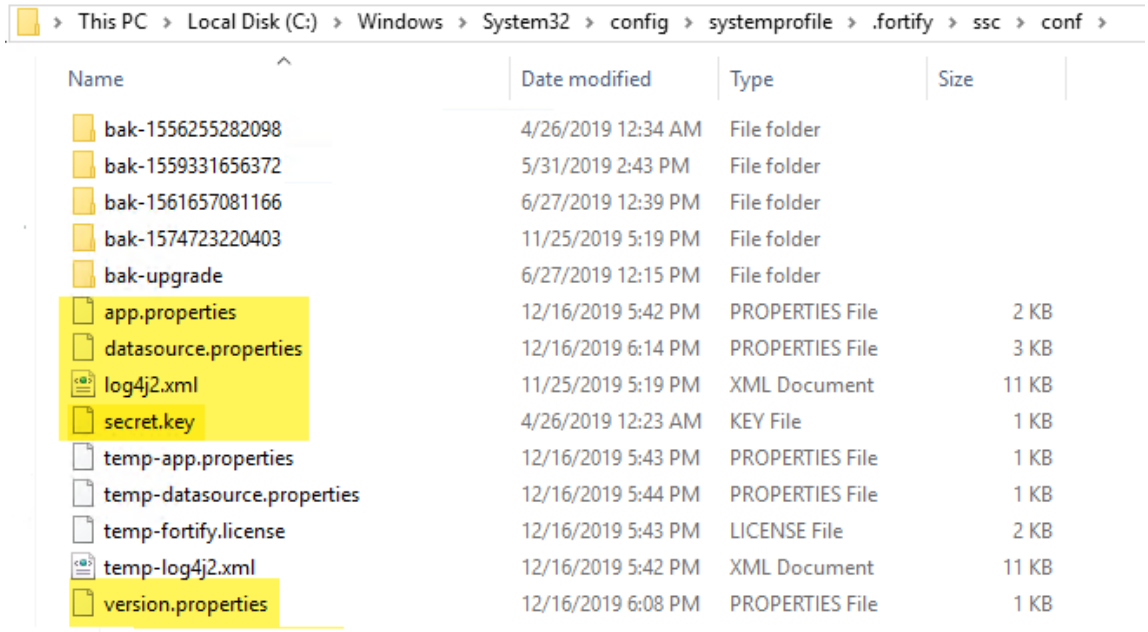
注: Fortify Software Security Centerインスタンスが保 守 モードでスタックしている場 合 は、"Fortify Software Security Centerが保 守 モードでスタックしている場 合 " 次 のページで説 明 されている解 決 策 のいずれかを試してください。

Fortify Software Security Centerが保 守 モード でスタックしている場 合

Fortify Software Security Centerは、 [ADMINISTRATION]ビューから保 守 モード に切り替 えられるか("Fortify Software Security Centerの保 守 モード への移 行 " ページ173を参 照)、`fortify.home\ssc\conf`ディレクトリで`version.properties`が見 つからなかった場 合 に保 守 モード に入 ります。

Fortify Software Security Center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。

- Fortify Software Security Center再 設 定します。指 示 については、"Fortify Software Security Centerの初 回 設 定 " ページ69を参 照してください。
- `fortify.home\ssc\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。
- 不 足しているファイルを`fortify.home\ssc\conf`ディレクトリから復 元します。



注 : `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、Fortify Software Security Center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。

Fortify Software Security Contentについて

Fortify製 品 では、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 が強 制 的 に適 用 されます。Fortify Software Security Contentは、

Fortify Secure Coding Rulepacks (ルールパック)および外 部 メタデータで構 成 されます。

- 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。

  Fortifyのアナライザやルールパックの機 能 に追 加 されるカスタムルールを作 成 できます。たとえば、場 合 によっては、専 有 セキュリティガイドラインを適 用 したり、すでにSecure Coding Rulepacksの対 象 ではないサードパーティのライブラリや事 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 したりする必 要 があります。

  ルールパックの管 理 方 法 については、次 を参 照 してください。

  - "Micro Focus Fortify更 新 サーバからのRulepackの更 新 " 下
  - "セキュリティコンテンツのインポート" ページ178
  - "ルールパックの削 除 " ページ178
  - "Rulepacksをエクスポートする" 次 のページ
  - "四 半 期 ごとのセキュリティコンテンツリリースで提 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" ページ189
- 外 部 メタデータには、Fortify脆 弱 性 カテゴリから代 替 カテゴリ(CWE、OWASP Top 10、PCIなど)へのマッピングが用 意 されています。

  外 部 `metadata.xml`ファイルは変 更 しないことを推 奨 します。そうしないと、ルールパックが四 半 期 ごとに更 新 されるたびに変 更 が上 書 きされます。("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" ページ189を参 照)。ただし、`customexternalmetadata.xml`ファイルを作 成 し、このファイル内 で新 しいマッピングを作 成 したり既 存 のマッピングを拡 張 したりできます。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。セキュリティコンテンツを更 新 するときに、このカスタムファイルは影 響 を受 けません。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、『Micro Focus Fortify Static Code Analyzerカスタムルールガイド』を参 照 してください。

  外 部 メタデータマッピングのスキーマは、`fortify.home\Core\config\schemas\externalmetadata.xsd`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" ページ179
  - "新 しいマッピングの作 成 " ページ180

注 : セキュリティコンテンツを定 期 的 に更 新 することが推 奨 されています。

Micro Focus Fortify更 新 サーバからのRulepackの更 新

最 新 のRulepackを使 用 することが重 要 です。最 新 のRulepackを確 実 に使 用 するには、FortifyサーバからRulepackをインポートします。

注: Fortify更 新 サーバがFortify Software Security Center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。Fortify Software Security Center用 に統 合 されたプロキシを設 定 する方 法 については、"Fortify Software Security Center統 合 のためのプロキシの設 定 " ページ128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. 管 理 者 またはセキュリティリードとしてFortify Software Security Centerにログインしてから、Fortifyヘッダで [**ADMINISTRATION**]を選 択 します。
2. [ADMINISTRATION]ビューの左 ペインにある [**Metrics &Tracking**]で、[**Rulepacks**]を選 択 します。
3. [Rulepacks]ページで、 [**UPDATE FROM SERVER**]をクリックします。
   Fortify Software Security Centerに、Rulepackの更 新 に関 する情 報 が表 示 され、続 行 するかどうかを示 すプロンプトが表 示 されます。
4. ダウンロードを続 行 するには、 [**OK**]をクリックします。
   更 新 が完 了 すると、Fortify Software Security Centerにインポートされたルールのリストが表 示 されます。
5. [**CLOSE**]をクリックします。

参 照 情 報

"ルールパックの削 除 " 次 のページ

"四 半 期 ごとのセキュリティコンテンツリリースで提 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" ページ189

"Rulepacksをエクスポートする" 下

"セキュリティコンテンツのインポート" 次 のページ

Rulepacksをエクスポートする

必 要 に応 じて、Rulepacksを一 方 のFortify Software Security Center インスタンスと別 のインスタンスとの間 で移 動 したり、あるいはFortify Software Security Center とAudit Workbenchとの間 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. Fortify Software Security Centerに管 理 者 またはセキュリティリードとしてログインします。
   Fortifyのヘッダで、 [**ADMINISTRATION**]をクリックします。
2. 左 ペインの [**Metrics &Tracking**]で、 [**Rulepacks**]を選 択 します。
3. [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、[**EXPORT**]をクリックします。

注: 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

"セキュリティコンテンツのインポート" 下

"ルールパックの削 除" 下

セキュリティコンテンツのインポート

セキュリティコンテンツ(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、Fortify Static Code Analyzer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. Fortify Software Security Centerに管 理 者 またはセキュリティリードとしてログインします。
   Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左 ペインの [Metrics &Tracking]で、 [Rulepacks]を選 択します。
3. [Rulepacks]ページで、 [IMPORT]を選 択します。
4. [IMPORT RULEPACK]ダイアログボックスで、 [+ADD FILES]をクリックします。
5. [File Upload]ダイアログボックスで、アップロードするファイルに移 動して選 択します。

注: 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 、Fortify Software Security Center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" 前 のページ

"ルールパックの削 除" 下

ルールパックの削 除

古 いルールパックは、Fortify Software Security Center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. Fortify Software Security Centerに管 理 者 またはセキュリティリードとしてログインします。
   Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左 ペインの [Metrics &Tracking]で、 [Rulepacks]を選 択します。

3. [Rulepacks]ページで、削 除 するルールパックのチェックボックスをオンにして、[DELETE]をクリックします。

   Fortify Software Security Centerに、選 択したルールパックの削 除 を確 認 するメッセージが表 示 され、システムに複 数 のバージョンのルールパックが含 まれている場 合 は、そのルールパックに含 まれるすべてのバージョンが削 除 されます。
4. [OK]をクリックします。

   Fortify Software Security Centerに、削 除 が成 功 したと知 らせるメッセージが表 示 されます。
5. 削 除 に失 敗 した場 合 は、[more]をクリックして [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" ページ177

"セキュリティコンテンツのインポート" 前 のページ

"Micro Focus Fortify更 新 サーバからのRulepackの更 新 " ページ176

現 在 のマッピングを拡 張 する

Fortify Software Security Center が外 部 メタデータで提 供 するマッピングを拡 張 したり、新 しいマッピングを作 成 したりできます。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>
        F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
        </ExternalListID>
        <ExternalCategoryDefinition>
                <Name>APP100 CAT I</Name>
                <Description>
                Description for APP100 CAT I.
                </Description>
                <OrderingInfo>1</OrderingInfo>
        </ExternalCategoryDefinition>
        <Mapping>
                <InternalCategory>
                Poor Style: Identifier Contains Dollar Symbol ($)
                </InternalCategory>
                <ExternalCategory>APP100 CAT I</ExternalCategory>
        </Mapping>
</ExternalListExtension>
```

重 要 マッピングファイルを拡 張 した後 に、Fortify Software Security Centerへ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" ページ178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 、Fortify Software Security Center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 " 下

"Fortify Software Security Contentについて" ページ175

新 しいマッピングの作 成

次 のように<ExternalList>を使 用 して、custom_metadata.xmlファイルを作 成 できます。

```
<ExternalList>
        <OrderingInfo>1</OrderingInfo>
        <ExternalListID>
        F2FA57EA-5BBB-4DDE-90A5-480BE65CE7E7
        </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>
</ExternalList>
```

重 要 カスタムマッピングファイルを作 成 した後 、それをFortify Software Security Center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" ページ178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 、Fortify Software Security Center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" 前 のページ

"Fortify Software Security Contentについて" ページ175

第8章: Fortify Software Security Centerのアップグレード

Fortify Software Security Center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インストールされている必要があります。たとえば、バージョン21.2.0にアップグレードするには、バージョン20.1.x、20.2.x、または21.1.xがインストールされている必要があります。バージョン19.2.x以前がインストールされている場合は、バージョン21.2.0に移行する前に、まず、バージョン20.1.x、20.2.x、または21.1.xにアップグレードする必要があります。

次の表は、Fortify Software Security Center 21.2.0にアップグレードするために必要なアップグレードパスを示しています。

現在のFortify Software Security Centerバージョンのアップグレードパス
20.1.x > 21.2.0 (直接)
20.2.x > 21.2.0 (直接)
21.1.x > 21.2.0 (直接)

現在のFortify Software Security Centerバージョンを最新バージョンに直接アップグレードできない場合は、バージョン固有のFortify Software Security Centerドキュメントで、以前のリリース(または直前のリリース)にアップグレードする方法を確認してください。

重要 Fortify Software Security CenterでFull ScanCentral SAST関連の機能を使用するには、ScanCentral Controllerおよびセンサが更新されている必要があります。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ScanCentralクライアントは、機能の制限なしで使用できます。

ScanCentralのセンサとクライアントをアップグレードする前、およびFortify Software Security Centerサーバをアップグレードする前に、ScanCentral Controllerをアップグレードする必要があります。ScanCentralコンポーネントをアップグレードする方法については、『*Micro Focus Fortify ScanCentralのインストール、設定、および使用ガイド*』を参照してください。

Fortify Software Security Centerデータベースのアップグレードタスク

次の表に記載されているタスクを表示順に実行して、Fortify Software Security Centerデータベースをアップグレードします。

タスク	説明
1	Tomcatサーバを停止します。
2	SSCフォルダとSSC WARファイルを<*tomcat*>/webappsディレクトリから削除します。 **重要** <*tomcat*>/webapps/<app>/libにJDBCドライバが存在する場合は、SSCフォルダを削除する前にJDBCドライバを<tomcat_server>/libにコピーします。
3	<*fortify.home*>\plugin-frameworkまたは<*fortify.home*>/plugin-frameworkフォルダから**プラグインフレームワーク**フォルダを削除します。 <*fortify.home*>ディレクトリの詳細については、"fortify.homeディレクトリについて" ページ57を参照してください。
4	新しいWARファイルを<*tomcat*>/webappsディレクトリにコピーします。
5	Tomcatサーバを起動します。
6	ブラウザを開き、Fortify Software Security CenterのURLを入力して、初期化モードでFortifyを起動します ("アップグレード後のFortify Software Security Centerの設定" ページ184を参照)。 バージョン17.20以降のインスタンスをマイグレーションする場合は、セットアップウィザードを使用して設定を検証します。
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Fortify Software Security Centerの設定" ページ184を参照)。
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" 次のページを参照)。 **注:** 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。
10	Tomcatサーバを再起動します。
11	バグトラッカプラグインは、ssc.warファイルの一部ではなくなりました。Fortify Software Security Centerをアップグレードして起動したら、古いバグトラッカプラグインを無効にして削除してから、現在の配布ファイ

タスク	説明
	ルから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、"バグトラッカーの統合について" ページ159を参照してください。

Fortify Software Security Centerデータベースのアップグレードの準備

Fortify Software Security Center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たFortify Software Security Center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、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Fortifyでは推奨しています。

注: アップグレードする前に、`c:\users\<username>\.fortify\plugin-framework`フォルダまたは`<fortify.home>/plugin-framework`フォルダからプラグインフレームワークフォルダを削除することを推奨します。

MySQLデータベースをアップグレードする場合は、"MySQL Server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" 下を参照してください。

MySQL Server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

Fortigy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ます。アップグレード後、前の設定に戻します。

Fortify Software Security Centerで使用するためにMySQLを設定する方法については、"MySQLデータベースの設定" ページ62を参照してください。

データベースアップグレードスクリプトの実行準備

Fortify Software Security Center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と同じデータベース権限が必要です。

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Fortify Software Security Centerデータベースをバックアップします。
- 既存のFortify Software Security Center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権限" ページ60を参照してください。

注 : 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。

WARファイルの更新と展開

SSC WARファイルを更新するには、次の手順に従います。

1. 現在展開されているSSC WARファイルの展開を解除します。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SSC WARファイルを展開します。

新しいWARファイルを展開したら、セットアップウィザードのステップと[ADMINISTRATION]ビューで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Fortify Software Security Centerの設定" 下および"追加のFortify Software Security Center設定" ページ79を参照してください。

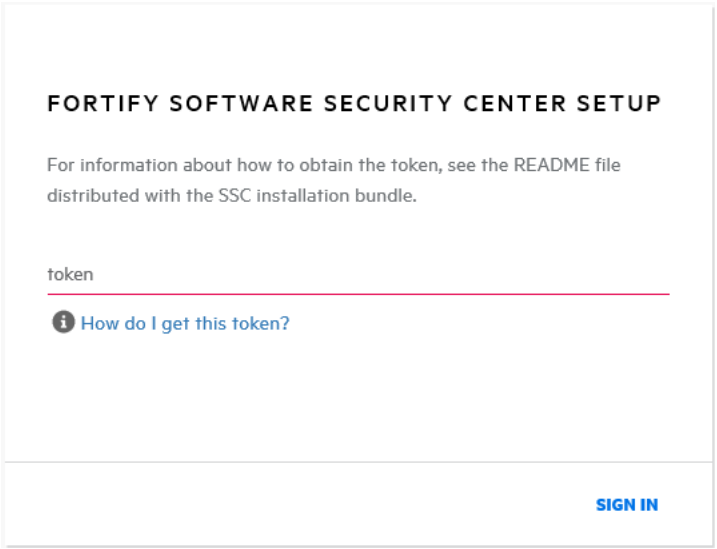
アップグレード後のFortify Software Security Centerの設定

Fortify Software Security Centerをアップグレードしてブラウザウィンドウでで Fortify Software Security CenterのURLに移動すると、セットアップウィザードが開きます。

注 : セットアップウィザードは、Fortify Software Security Centerの初めての展開、アップグレード後、またはサーバを保守モードにした後 (1ページの"Fortify Software Security Centerの保守モードへの移行" ページ173を参照)にのみ、管理者だけが使用できます。

1. Tomcatサーバに新しいバージョンのFortify Software Security Center WARファイルを展開した後、ブラウザウィンドウを開き、Fortify Software Security CenterサーバのURLを入力します。

2. *<fortify.home>*/*<app_context>*ディレクトリに移 動し、`init.token`ファイルを開きます。
3. `init.token`ファイルの内 容 をクリップボードにコピーします。
4. Fortify Software Security Center画 面 の右 上 隅 で、 [**ADMINISTRATORS**]をクリックします。



5. `init.token`ファイルからコピーした文 字 列 をテキストボックスに貼 り付 け、 [**SIGN IN**]をクリックします。

   Fortify Software Security Centerセットアップウィザードが開きます。
6. [**CONFIGURATION**]または [**CORE SETTINGS**]の手 順 で環 境 設 定 を変 更 する必 要 がある場 合 は、"Fortify Software Security Centerの初 回 設 定 " ページ69に記 載 されている手 順 に従 って変 更 できます。

7. DATABASE SETUPの手 順 に達 するまで［NEXT］をクリックします。
8. DATABASE SETUPステップで、次 の手 順 を実 行します。
   a. ［DATABASE TYPE］ボックスで、Fortify Software Security Centerデータベースタイプにー 致 するタイプを選 択します。
   b. ［DATABASE USERNAME］ボックスに、Fortify Software Security Center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権 限 " ページ60を参 照 してください。
   c. ［DATABASE PASSWORD］ボックスに、Fortify Software Security Centerデータベースのパスワードを入 力します。
   d. ［JDBC URL］ボックスに、Fortify Software Security CenterデータベースのURLを入 力します。

      注 意 ［JDBC URL］内 のデータベース名 (大 文 字 と小 文 字 を含 む)は、Fortify Software Security Centerデータベース名 と完 全 にー 致 している必 要 があります。

      注 : MariaDB JDBCドライバは、MySQLデータベースサーバへの接 続 に使 用されます。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>`で置 き換 えてください)。
   e. 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、`ssc.log`ファイル (`<fortify.home>/<appcontext>/logs`ディレクトリ)をチェックして原 因 を特 定 します。
   f. 接 続 が成 功 したとセットアップウィザードが示 した後 、右 側 のウィンドウで警 告 と指 示 を読 み、 ［DOWNLOAD SCRIPT］をクリックします。
   g. `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、"Fortify Software Security Centerデータベーステーブルおよびスキーマについて" ページ66を参 照 してください)。

      注 : 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の完 了 に数 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. DATABASE SEEDINGステップで 、次 の操 作 を実 行 します。
    a. 左 ペインで、 ［BROWSE］を使 用 してプロセスシードバンドルzipファイルを見 つけて選 択 し、 ［SEED DATABASE］をクリックします。

b. [BROWSE]を使用して、レポートシードバンドルzipファイルを見つけて選択し、[SEED DATABASE]をクリックします。
c. (オプション) [BROWSE]を使用してPCI基本シードバンドルzipファイルを見つけて選択し、[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。

ヒント: 後で環境設定を変更する必要がある場合は、Fortify Software Security Centerを保守モードに入れ、必要な変更を加えます。Fortify Software Security Centerを保守モードにする方法については、1ページの"Fortify Software Security Centerの保守モードへの移行" ページ173を参照してください。

参照情報
"Fortify Software Security Centerの初回設定" ページ69

Fortify Audit WorkbenchからのFortify Static Code Analyzerのアップグレード

Fortify Audit Workbenchのユーザは、Fortify Audit Workbenchユーザインタフェースから新しいFortify Static Code Analyzerおよび関連するツールバージョンの可用性をチェックできます。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Autoify Audit Workbenchのユーザ向けに有効にするには、最初にFortify Software Security Centerの管理者がFortify Software Security Center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。

Fortify Audit WorkbenchからFortify Static Code Analyzerおよび関連するツールをアップグレードする方法については、『*Micro Focus Fortify Audit Workbenchユーザガイド*』を参照してください。

参照情報

"Audit WorkbenchからFortify Static Code Analyzer Suiteのアップグレードを有効にする" 下

Audit WorkbenchからFortify Static Code Analyzer Suiteのアップグレードを有効にする

新しいFortify Static Code Analyzerインストーラを 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. Software Security Centerホストで、<*ssc_install_dir*> /WEB-INF/internal に移動して、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. <*ssc_install_dir*>/update-site/installersディレクトリに移動します。
5. readme.txt ファイルを開いて読み込みます。
6. readme.txt ファイルで、サンプルの update.xml ファイルの内容(<installerInformation> タグと </installerInformation> タグの間、両タグを含む)をコピーします。
7. 新しいテキストファイルを作成して、コピーしたテキストをそこに貼り付けます。
8. インストーラのバージョン情報を更新して、インストールを反映させます。例:

```
<filename>Fortify_SCA_and_Apps_<version>_windows_x64.exe</filename>
```

9. <downloadLocationList> タグの下で、URL情報を更新してSoftware Security Centerのインストールを反映させます。例:

```
<url>http://localhost:8080/ssc/update-site/installers/</url>
```

10. このファイルの名前を update.xml にして、<*ssc_install_dir*>/update-site/installersディレクトリに保存します。
11. Tomcatサーバを再起動します。
12. 新しいSCAおよびアプリインストーラファイル(Fortify_SCA_and_Apps_<*version*>_<*OS*>)を取得した後、次の操作をします。
    a. 新しいインストーラファイルを <*ssc_install_dir*>/update-site/installers ディレクトリにコピーします。
    b. テキストエディタでupdate.xmlファイルを開きます。
    c. versionId タグの間に、新しいインストーラのバージョンIDを記入します。(バージョンIDは、ピリオドのないバージョン番号です)。

       <*versionId*> タグ値がインストーラのFortify Static Code Analyzerのバージョンと一致することを確認します。
    d. 編集した update.xml ファイルを保存します。

Audit Workbenchのユーザが新しいバージョンのFortify Static Code Analyzerを確認してインストールできるようになりました。

注: 自動アップグレード機能に使用されるBitRock InstallBuilderツールは、1つのWindowsタグのみをサポートします。異なるバージョンのWindowsがある場合は、それらのバージョンに対応する設定ファイルが必要です。追加の設定ファイルを作成する方法については、<*ssc_install_dir*>/update-site/installersディレクトリに

ある `readme.txt` ファイルを参照してください。

期限切れライセンスの更新

Fortifyのライセンスファイルを取得する方法については、ドキュメント『*Micro Focus Fortifyソフトウェアシステム要件*』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、次の手順に従います。

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。

四半期ごとにリリースされるセキュリティコンテンツ

Micro Focus Fortifyは、新しいセキュリティコンテンツがダウンロード可能な場合お知らせします。これらの更新には、Rulepackと外部メタデータが含まれます。また、更新されたシードバンドルを含む場合もあります。

重要 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。

参照情報

"Fortify Software Security Centerデータベースのシード処理について" ページ67

"Fortify Software Security Contentについて" ページ175

"Micro Focus Fortify更新サーバからのRulepackの更新" ページ176

四半期ごとのセキュリティコンテンツ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

Micro Focus Fortifyは、新しいセキュリティコンテンツがダウンロード可能な場合お知らせします。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「**Micro Focus Security Fortify Premium Content**」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、"Fortify Software Security Centerデータベースのシード処理について" ページ67を参照してください。

注 : 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FPR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。
   a. Fortify Support Portal (https://www.microfocus.com/support)にログオンします。
   b. 左側の列で、 [PREMIUM CONTENT]を選択します。
   c. 右側で [FORTIFY EXCHANGE]を選択します。
   d. 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. 左ペインで [Configuration]を選択し、 [Seed Bundles]を選択します。
4. [Seed Bundles]ページで、 [BROWSE]をクリックし、`ReportBundle.zip`ファイルに移動して選択します。
5. [SEED BUNDLES]をクリックします。

Fortify Software Security Centerは、バンドルのアップロードが成功したと知らせるメッセージを表示します。

参照情報

"Fortify Software Security Centerデータベースのシード処理について" ページ67

パートII: Micro FocusFortify Software Security Centerの使 用

次 の章 では、Fortify Software Security Centerの使 い方 について説 明します 。

第9章: Fortify Software Security Centerの使用

Fortify Software Security Center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。セキュリティチームと開発チームが協力して、Fortify Static Code Analyzer、Fortify ScanCentral DAST、Fortify ScanCentral SAST、Fortify WebInspect、およびサードパーティのツールで相互に関連するデータを共同のオンライン環境から使用できるようにすることで、セキュリティ上の欠陥を迅速で正確に解決できます。

このセクションで説明するトピック:

Fortify Software Security Centerの中心的役割について

Fortify Software Security Centerでは、セキュリティ分析結果を収集、関連付け、およびエクスポートする場所を提供します。Fortify Software Security Centerサーバは中央の場所に配置され、静的分析、動的分析、リアルタイム分析など、さまざまなセキュリティアクティビティの結果を受け取ります。

Fortify Software Security Centerは、次の機能をサポートするように設計されています。

- 既存の脆弱性のベースラインを特定し、優先的とする
- 新しい脆弱性が導入されるのを防ぐ

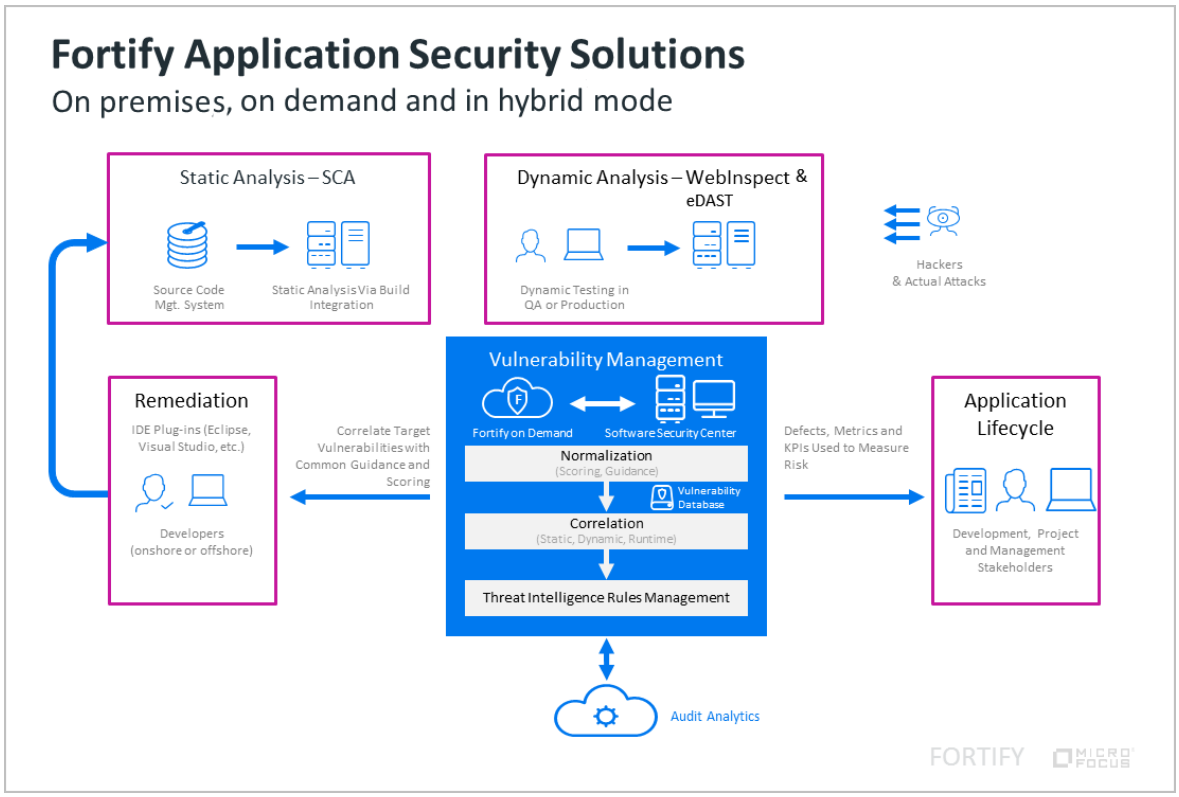
- 既 存 の脆 弱 性 を修 正 し、ベースラインを下 げる
- コード が内 部 および外 部 のセキュリティ指 令 を遵 守 するようにする

Fortify Software Security Centerは、組 織 内 で次 のような質 問 に答 えるために動 作 します。

- 優 れたアプリケーションセキュリティプラクティスの採 用 を促 進 するにはどうしたらよいか
- 開 発 チームにアクション可 能 な結 果 を得 るにはどうしたらよいか
- アプリケーションチームをチーム単 位 で測 定 するか、ユニットとして測 定 するか
- 長 期 的 な結 果 を追 跡 するにはどうしたらよいか

セキュリティ管 理 ワークフロー

次 の図 は、Fortify Software Security Center内 のセキュリティ管 理 プロセスの流 れを示 しています。



開 発 チームはスキャンを実 行 する際 に、継 続 的 な統 合 サーバから定 期 的 にスキャン結 果 をFortify Software Security Center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Fortify Software Security Centerに送 信 します。

Fortify Software Security Centerは時 間 をかけてスキャン結 果 と評 価 結 果 を相 互 に関 連 付 け、追 跡 し、Audit Workbench、またはFortify Plugin for Eclipse、Fortify

Extension for Visual StudioなどのIDEプラグインを通じて開発者が情報を利用できるようにします。

また、ALM、Jira、Azure DevOps Server、Bugzillaなどの欠陥トラッキングシステムに問題をプッシュすることもできます。

ユーザアカウントとアクセス

Fortify Software Security Centerでは、次の2つの認証方法がサポートされています。

- インタフェース内で作成されたローカルユーザアカウント
- 標準の企業認証に関連付けられたActive Directory/LDAPアカウント(Active Directory/LDAPの統合では、グループまたは部門によるユーザ割り当てがサポートされています)

このセクションで説明するトピック:

Active Directory/LDAPの統合

Active Directory/LDAPの統合により、Fortify Software Security Center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、Fortify Software Security Center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Fortify Software Security Center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。

Fortify Software Security Centerを展開するユーザは、インストール時に、Active Directory/LDAPの統合を設定する必要があります。詳細については、"LDAPサーバの設定" ページ108を参照してください。

参照情報

"LDAPエンティティの登録" ページ119

"Fortify Software Security Centerのユーザアカウント管理" ページ207

初めてのFortify Software Security Centerへのログイン

Fortify Software Security Centerにログインするには、Fortify Software Security Center管理者からインスタンスのURL、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Fortify Software Security Centerにログインするには、次の手順に従います。

1. Fortify Software Security Centerユーザインタフェースの最 新 バージョンに確 実 にアクセスするには、Webブラウザのキャッシュをクリアします。
2. Webブラウザで、次 のようにFortify Software Security Centerインスタンスの URLを入 力します。
   - セキュアHTTPプロトコルを使 用 するようにFortify Software Security Centerが設 定 されている場 合 は、次 のURLを入 力します。

     `https://<host_ip>:<port>/ssc/`

     ここで`<port>`は、Tomcatサーバが使 用 するポート番 号 を表します。
   - セキュリティ保 護 されていないHTTPプロトコルを使 用 するようにFortify Software Security Centerが設 定 されている場 合 は(推 奨しません)、次 のURLを入 力します。

     `http://<host_ip>:<port>/ssc/`

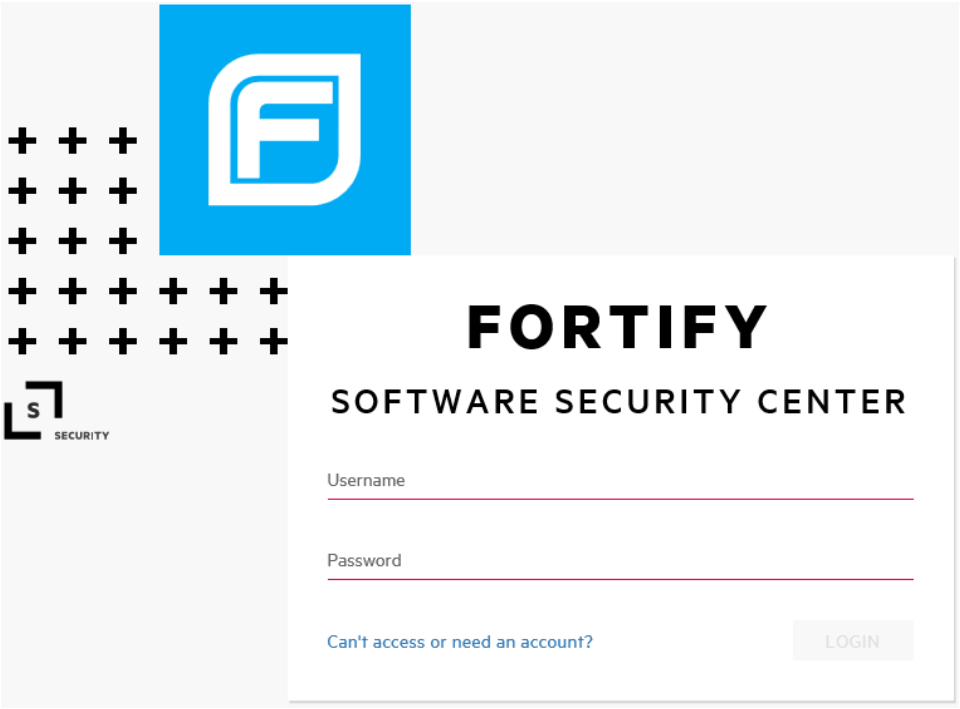
     ここで`<port>`は、Tomcatサーバが使 用 するポート番 号 を表します。
3. [**Username**]および [**Password**]ボックスに、管 理 者 から与 えられた資 格 情 報 を入 力します。
4. [**LOGIN**]をクリックします。
5. Fortify Software Security Centerでパスワードの変 更 を求 めるプロンプトが表 示 される場 合 は、パスワードを変 更します。手 順 については、"パスワードの変 更" ページ 197を参 照してください。

Fortify Software Security Centerへのアクセス権 の要 求

まだFortify Software Security Center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、ログインページからアシスタンスを要 求 できます。

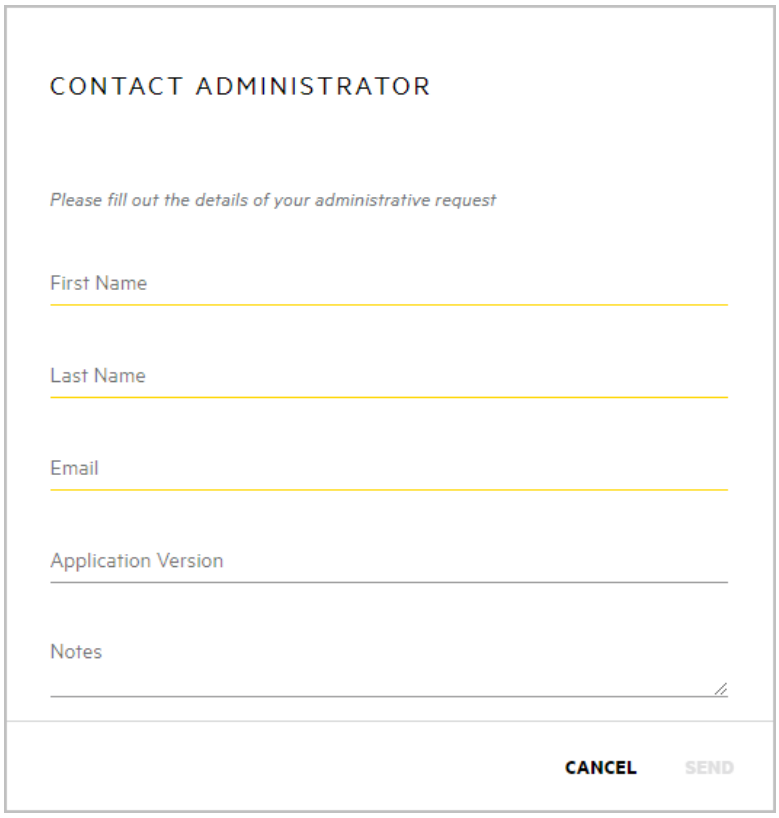
Fortify Software Security Centerへのアクセスを要 求 するには、次 の手 順 に従 います。

1. Webブラウザで、Fortify Software Security Centerインスタンスの URLを入 力します。



2. Fortify Software Security Center画 面 の下 部 にある [**Can't access or need an account?**]リンクをクリックします 。

注 : このリンクは、Fortify Software Security Center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。("電 子 メールアラート通 知 設 定 の設 定 " ページ99を参 照 してください)。



3. 必 要 な情 報 を入 力 し、 [SEND]をクリックします。

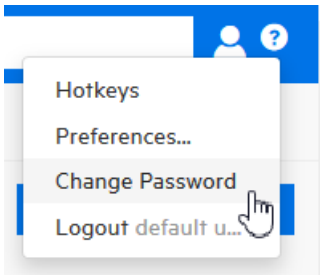
Fortify Software Security CenterからFortify Software Security Center管 理 者 に要 求 が送 信 されます。

パスワードの変 更

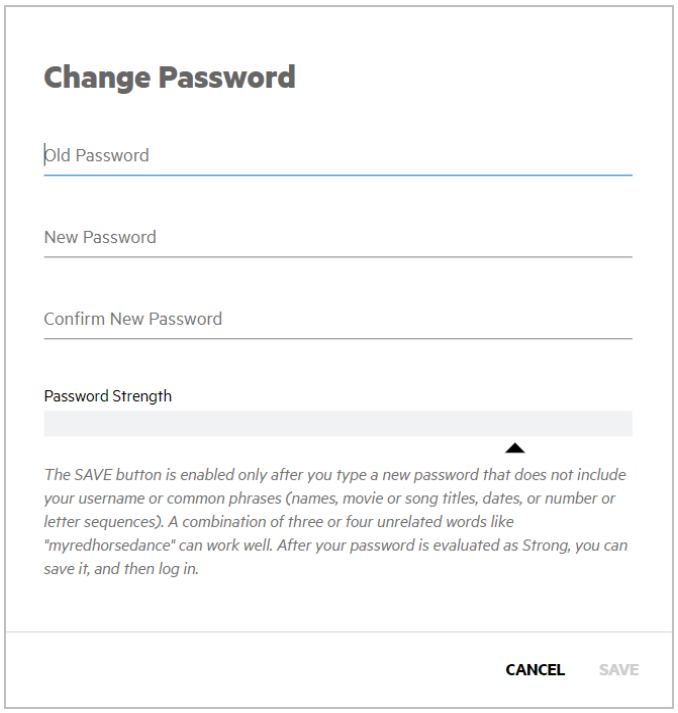
次 の手 順 では、パスワードを変 更 する方 法 について説 明 します。ローカルアカウントを使 用 してログオンしている場 合 のみ、パスワードを変 更 できます。

パスワードを変 更 するには、次 の手 順 を実 行 します。

1. Fortify Software Security Centerにログインします。



2. Fortifyヘッダの右 側 にあるユーザプロファイルアイコンをクリックし、 [Change Password]を選 択 します。



[Change Password]ダイアログボックスが開きます。

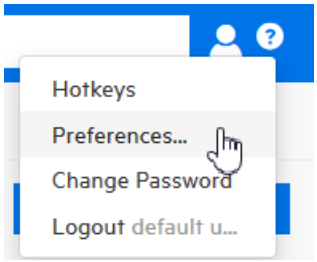
[Save]ボタンは、ユーザ名やー般的なフレーズ(名前、映画や楽曲のタイトル、日付、または数字や文字のシーケンス)を含まない強力な新しいパスワードを入力した後にのみ有効になります。「myredhorsedance」のように無関係な単語を3～4つ組み合わせて使用すると、うまく機能します。パスワードが強力であると評価されると、パスワードを保存してからログインできます。

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る場合は、[Save]をクリックします。

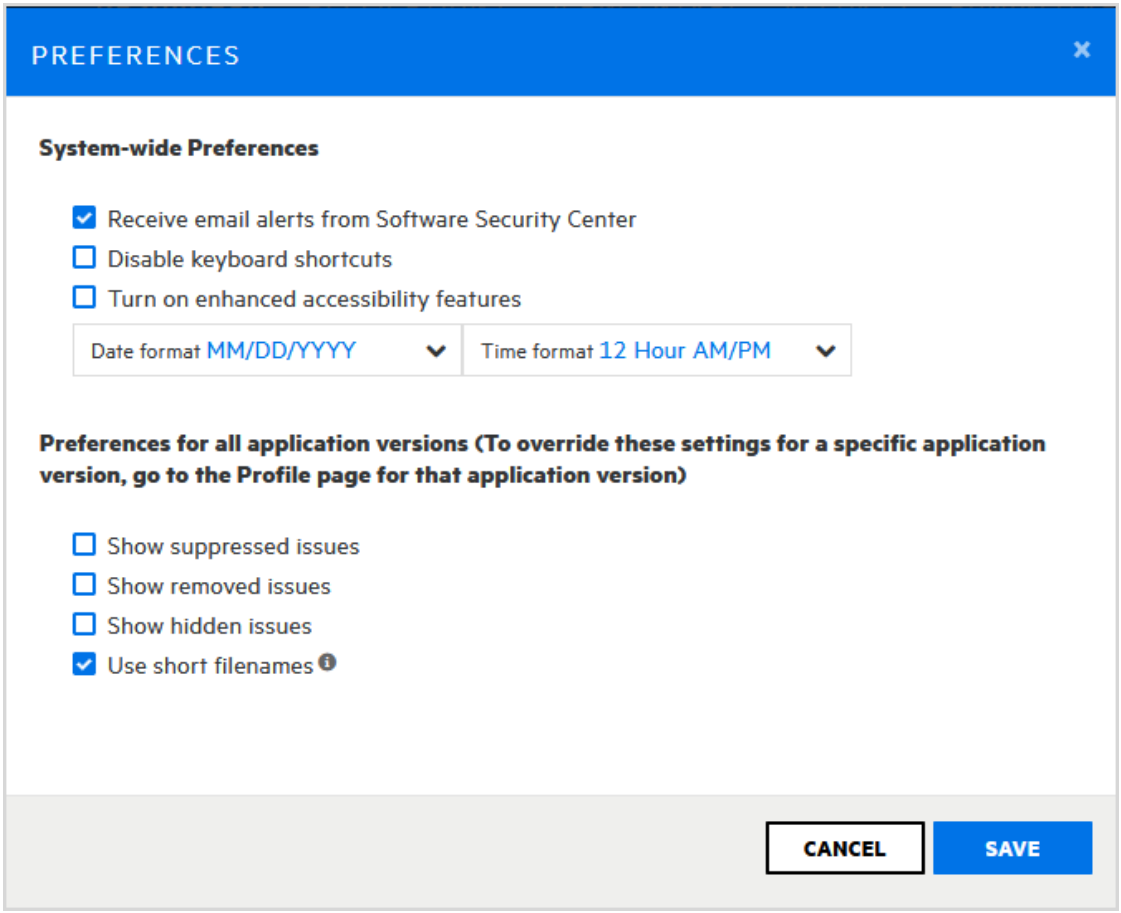
環境設定: システム全体とアプリケーションバージョン間

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. Fortifyヘッダの右側にあるユーザプロファイルアイコンをクリックし、[Preferences]を選択します。



[PREFERENCES]ダイアログボックスが開きます。

2. システム全 体に設 定を適 用するには、 [System-wide Preferences]で次 の操 作を実 行します。
   a. 有 効または無 効にする機 能のチェックボックスをオンにします。
   b. デフォルトのMM/DD/YYYYフォーマットではなく、日 付フォーマット, [Date format]リストから選 択します。
   c. デフォルトの12時 間(AM/PM)フォーマットではなく、フォーマットを適 用するには、[Time format]リストから選 択します。
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。

注意 ここで指 定する日 付と時 刻の設 定は、SCANCentral DASTページ(**SCANCENTRAL > DAST**)には適 用されません。DASTページの日 付と時 刻の設 定はそれぞれMM/DD/YYYYおよびh:mm:ssです。

注: 特 定のアプリケーションバージョンについてこれらの設 定を上 書きするには、そのアプリケーションバージョンの [APPLICATION PROFILE]ダイアログボックス

に移動します。

a. [AUDIT]ページの問題リストに抑止された問題を含めるには、 [Show suppressed issues]チェックボックスを選択します。
b. [AUDIT]ページに削除された問題を含めるには、 [Show removed issues]チェックボックスを選択します。
c. [AUDIT]ページに隠し問題を含めるには、 [Show hidden issues]チェックボックスを選択します。
d. [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、 [Use short file names]チェックボックスをオンにします。

4. [SAVE]をクリックします。

Fortify Software Security Centerダッシュボードについて

Fortify Software Security Centerにログインすると、アクセスできるアプリケーションバージョンのうち、組織にとって最大のビジネスリスクとなるもののデータがダッシュボードに表示されます。

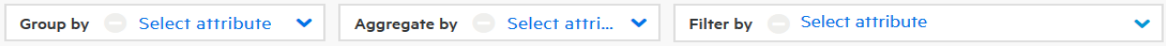
このセクションで説明するトピック:

[Issue Stats]ページ

Fortify Software Security Centerに最初にログインすると、ダッシュボードの [ISSUE STATS]ページが最初に表示されます。このページには、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概要情報が表示されます。この情報には、アプリケーションの確認と修復に必要な日数が含まれます。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、 [ISSUE STATS]ページには [Average Days to Review]と [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。

注: 管理者またはセキュリティリードの場合は、 [Issue Stats]ページの情報を確認するときにユーザ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" ページ80を参照してください。

テーブルのリストに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、Fortify Software Security Centerからアプリケーションバージョンの [AUDIT]ページに直接移動します。データにフィルタは適用されません。



ダッシュボードには、単独で使用したり、組み合わせて表示されるサマリデータを絞り込む3つの設定が提供されています。

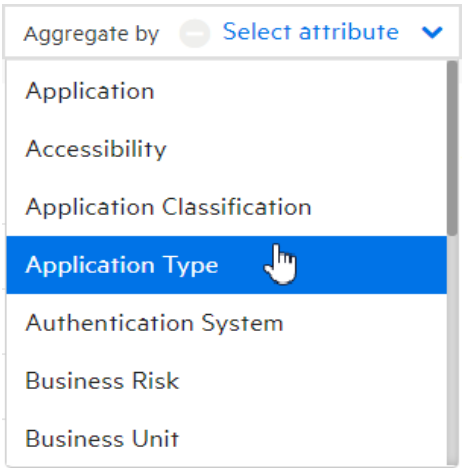
グループ化属性の選択

単一のアプリケーションバージョン属性に基づいてデータをグループ化するには、[Group by]リストから属性を選択します。(デフォルトのグループ化属性はアプリケーションバージョンです)。

選択したグループ化属性に加えて、結果のデータには、[Aggregate by]および[Filter by]リストから選択した属性が反映されます。

注: [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" ページ223を参照してください。

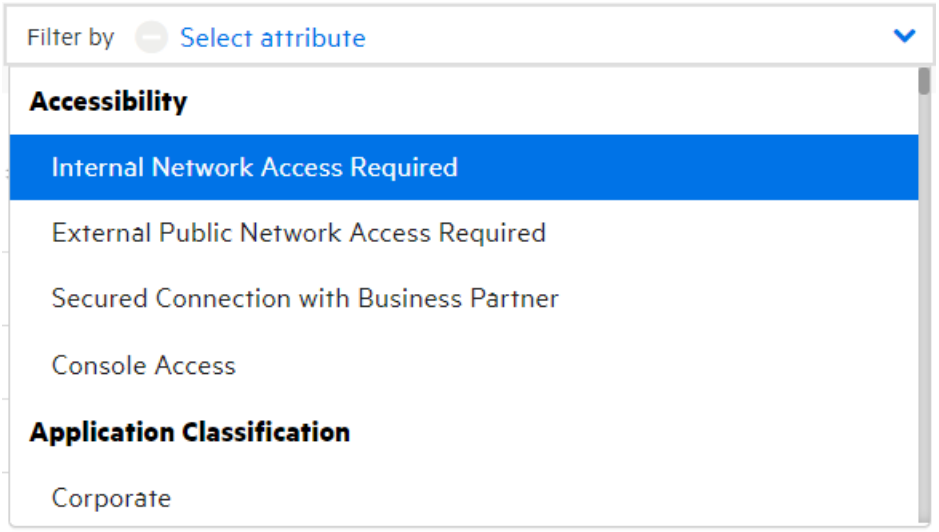
集計属性の選択



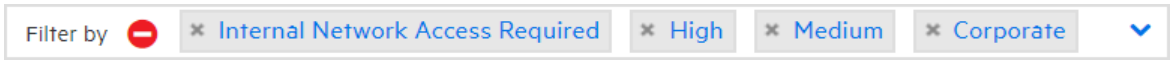
単一のアプリケーション属性に基づいてダッシュボードに表示されるデータを集約するには、[Aggregate by]リストから属性を選択します。ダッシュボードには、集計属性、および[Group by]と[Filter by]リストから選択した属性に基づいてデータが表示されます。

注: [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" ページ223を参照してください。

1つ以上のフィルタ属性の選択

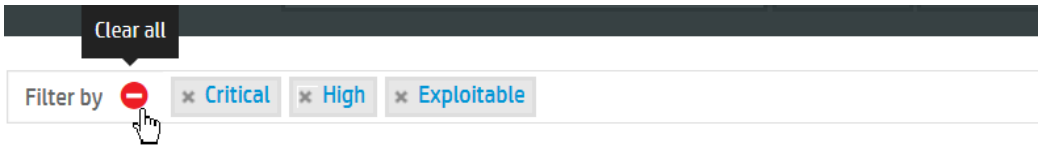


アプリケーション属性に基づいてデータを選択的に表示するには、[Filter by]リストから属性を選択します。複数の属性を選択できますが、1度に1つずつ選択する必要があります。



ダッシュボードには、選択したフィルタ属性、および[Group by]と[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。

カスタム属性リストから選択をクリアする



属性の選択をリストからクリアするには、[Clear all]アイコンをクリックします。

[ISSUE STATS]および[AUDIT]ページに表示されるFortify Software Security Center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、"データをカンマ区切り値ファイルへエクスポートする" 下を参照してください。

データをカンマ区切り値ファイルへエクスポートする

アプリケーションバージョンの選択したデータやすべてのFortify Software Security Center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。

ダッシュボード サマリテーブルをエクスポートする

ダッシュボードに表 示されるサマリテーブルをエクスポートするには:

1. Fortifyのヘッダで、 [DASHBOARD]をクリックします。
2. ツールバーで [EXPORT]をクリックします。

   注 : [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。

   [EXPORT CSV]ダイアログボックスが開きます。
3. [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) [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. [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:
   a. Fortifyのヘッダで、 [REPORTS]をクリックします。
   b. [レポート]ページで、 [DATA EXPORTS]をクリックします。
   c. ファイルを保 存するのか開くのかを指 定します。
   d. 結 果のテーブルで、エクスポートされたファイルの行にカーソルを移 動して、 [ダウンロード]アイコン をクリックします。

CSVファイルが削 除されるまで保 持される期 間を決 定するには、"ジョブスケジューラの設 定" ページ131に記 載されている手 順を参 照してください。

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

[Issue Stats]ページまたは [AUDIT]ページからCSVファイルにデータをエクスポートするには:

1. (オプション) [Issue Stats]ページからデータをエクスポートする場 合 は、集 約またはフィルタの適 用に使 用する属 性を選 択できます。 [AUDIT]ページで、フィルタの適 用に使 用する属 性を選 択できます。

   注 : [ISSUE STATS]ページまたは [AUDIT]ページで [Group by]に属 性を指 定すると、 [EXPORT]ボタンは削 除されます。

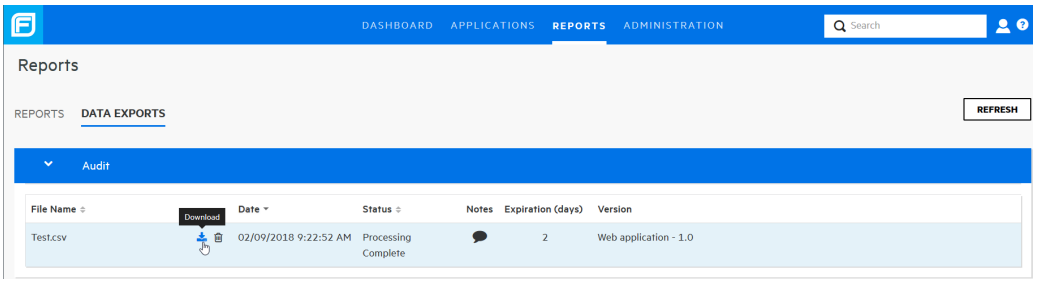
   

2. ツールバーで [EXPORT]をクリックします。

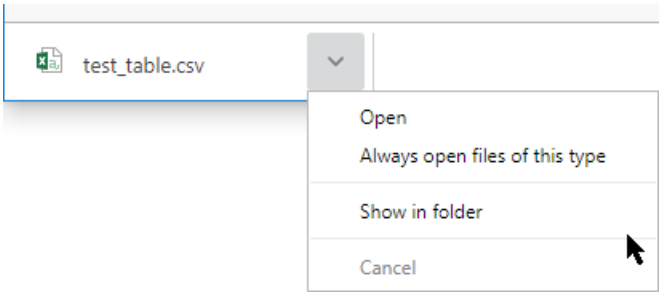
   注 : [EXPORT]ボタンが表 示されない場 合 は、管 理 者 がこの機 能を無 効にしています。

   [EXPORT CSV]ダイアログボックスが開きます。
3. [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) [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. [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:
   a. Fortifyのヘッダで、 [REPORTS]をクリックします。
   b. [レポート]ページで、 [DATA EXPORTS]をクリックします。



   c. 結 果 のテーブルで、エクスポートされたファイルの行 にカーソルを移 動して、 [ダウンロード]アイコン をクリックします。
   CSVファイルは [ダウンロード]フォルダに保 存 されます。



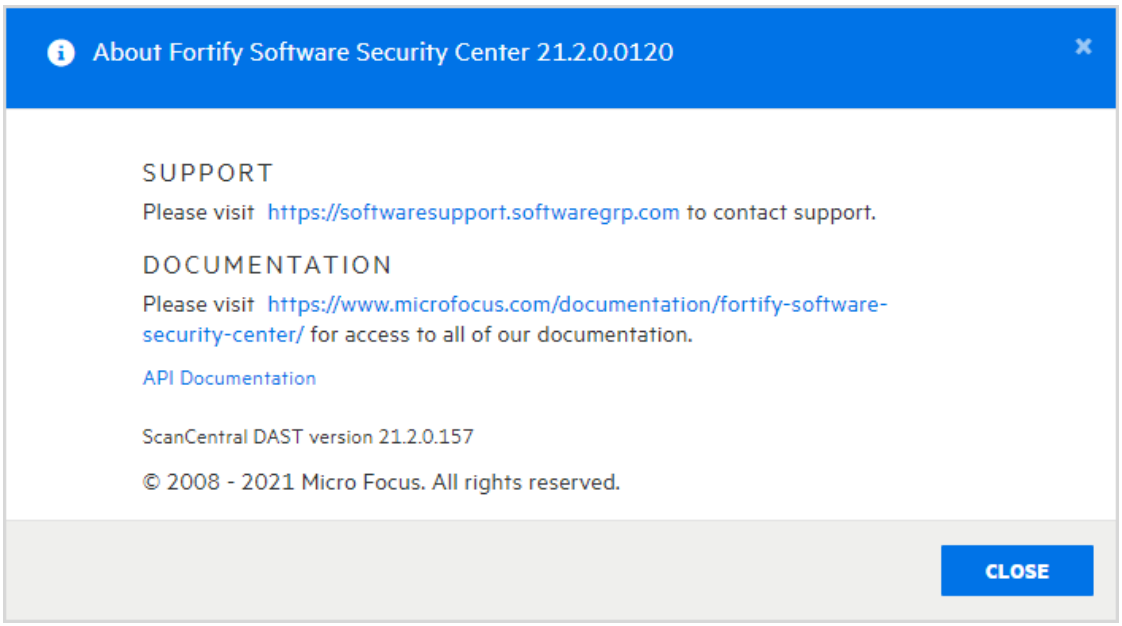
   d. ステータスバーで、CSVファイル名 の横 にある矢 印を選 択し、 [ダウンロード]フォルダでファイルを開くのか表 示 するのかを指 定します。

CSVファイルが削 除されるまで保 持される期 間を決 定するには、"ジョブスケジューラの設 定" ページ131に記 載されている手 順を参 照してください。

Fortify Software Security Center APIドキュメント へのアクセス

Fortify Software Security Center 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. Fortifyのヘッダで、ヘルプアイコン をクリックします。
   [About Fortify Software Security Center <*version*>]が開きます。



2. [**API Documentation**]をクリックします。

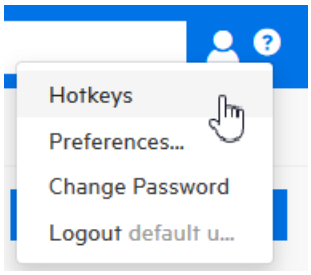
[FORTIFY SOFTWARE SECURITY CENTER API DOCUMENTATION VERSION <*version*>]Webページが開きます。

ヒント: また、Chrome DevToolsなどのプロキシを利 用してFortify Software Security Center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 するための適 切なエンドポイントコールを特 定することも非 常に役 立ちます。

Fortify Software Security Centerキーボードショートカットの表 示

Fortify Software Security Centerユーザインタフェースの移 動に使 用されるキーボードショートカットを表 示するには、次 の手 順に従います。

1. Fortify Software Security Centerにログインします。
2. 次 のいずれかを実 行します。
   - Fortifyヘッダの右 側にあるユーザプロファイルアイコンをクリックし、 [**Hotkeys**]を選択します。



   - キーボードの疑 問 符 (?)キーを押します。

参照情報

"環 境 設 定 : システム全 体 とアプリケーションバージョン間 " ページ198

第10章: ユーザアカウントの管理

この章のトピックでは、Fortify Software Security Centerユーザアカウントと取り扱い方法について説明します。

Fortify Software Security Centerのユーザアカウント管理

新しいFortify Software Security Center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、デフォルトの管理者アカウントを削除します。追加のFortify Software Security Centerユーザアカウントを作成するには、デフォルト以外のFortify Software Security Center管理者アカウントを使用します。

Fortify Software Security Centerでは、デフォルトのユーザ役割がいくつかサポートされています。次のセクションでは、これらの各役割について説明します。

このセクションでは、Fortify Software Security Centerの役割、ユーザアカウント管理、Fortify Software Security CenterにLDAPエンティティを登録する方法、およびMicrosoft Azure ADとの統合を設定する方法について説明します。

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および監視し、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ための情報にアクセスする必要があります。Fortify Software Security Center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。

役割について

役割により、ユーザがFortify Software Security Centerで実行できるアクションが決定されます。

Fortify Software Security Center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、Fortify Software Security Center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" 次のページを参照してください。

事前設定済みの役割

次の表は、Software Security Center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。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、"Fortify Software Security Centerの役 割に関 する許 可 情 報 の表 示 " ページ169を参 照してください。

役 割	説 明
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
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 します。 • 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 • スキャン結 果 のアップロード • 問 題 の監 査
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
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。
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
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
WebInspect Enterprise System	WebInspect EnterpriseインスタンスをFortify Software Security Center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。

参 照 情 報

"役 割 について" 前 のページ

"カスタム役 割 の作 成 " 下

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. Fortify Software Security Centerに管 理 者としてログインし、Fortifyのヘッダで［ADMINISTRATION］をクリックします。
2. ［ADMINISTRATION］ページの左 ペインで、［Users］を選 択し、［Roles］を選 択します。
3. ［Roles］ツールバーで、［NEW］をクリックします。
   ［CREATE NEW ROLE］ダイアログボックスが開きます。
4. 次の表で説 明する情 報を入 力します。

フィールド	説 明
Name	役 割 名
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。 **注 :** 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。

5. 許 可を追 加する(この役 割のユーザが使 用できる機 能 領 域を指 定)には、［+ADD PERMISSIONS］をクリックします。
   ［ADD PERMISSIONS］ダイアログボックスが開きます。
6. 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。
7. ［DONE］をクリックします。
   選 択した許 可に追 加の許 可が必 要な場 合は、警 告 記 号 ⚠の横に一 覧 表 示されます。
8. 一 覧 表 示された依 存 関 係を新しい役 割に追 加するには、［ADD MISSING PERMISSIONS］をクリックします。
   ［CREATE NEW ROLE］ダイアログボックスに、追 加の許 可 (依 存 関 係)が一 覧 表 示されます。
9. ［SAVE］をクリックします。

ヒント : また、［ADD MISSING PERMISSIONS］を使 用して、カスタム役 割を編 集するときに依 存 関 係を追 加できます。

Fortify Software Security Center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。

カスタム役 割 の削 除

［Roles］ページに一 覧 表 示 されているカスタム役 割 がユーザアカウントに割り当 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. Fortify Software Security Centerに管 理 者 またはセキュリティリードとしてログインし、［ADMINISTRATION］をクリックします。
2. ［ADMINISTRATION］ビューの左 ペインで、［Users］を選 択し、［Roles］を選 択します。
3. 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。
4. ［Roles］ツールバーで［DELETE］をクリックします。
   Fortify Software Security Centerに、役 割 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。

参 照 情 報

"カスタム役 割 の作 成 " ページ208

Fortify Software Security Center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Fortify Software Security Centerシステムを管 理 します。ローカルまたはLDAP Fortify Software Security Center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。

Fortify Software Security Center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、［AUDIT］ページから管 理 者 ユーザに問 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:

ローカルユーザアカウントの作 成

Fortify Software Security Center Administratorレベルのユーザは、新しいローカルユーザアカウントをFortify Software Security Centerユーザのリストに追 加 できます。

重 要 Fortify Software Security Center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。

Fortify Software Security Center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. Fortify Software Security Centerに管 理 者 としてログインし、Fortifyのヘッダで［**ADMINISTRATION**］をクリックします。
2. ［ADMINISTRATION］ビューの左 のペインで、［**Users**］を選 択 し、［**Local Users**］を選 択 します。
   ［**Local Users**］ページが開き、ローカルユーザが一 覧 表 示 されます。
3. ［**Local Users**］ツールバーで 、［**+ADD**］をクリックします。
   ［CREATE NEW USER］ダイアログボックスが開きます。
4. 次 の表 に表 示 されている情 報 を指 定 します。

フィールドまたはチェックボックス	説 明
Username	Fortify Software Security Centerへのログオン用 のユーザ名 。
First Name	(オプションですが、強 く推 奨)ユーザの名 。
Last Name	(オプションですが、強 く推 奨)ユーザの姓 。
Email	(オプション)ユーザの電 子 メールアドレス。 **注 意** 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。
Confirm Password	新 しいユーザのパスワード 。
User must change password at	Fortify Software Security Centerへの次 回 のログイン時 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。

フィールドまたはチェックボックス	説明
next login	
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	Fortify Software Security Centerへのユーザアクセスを一 時 停止 するには、このチェックボックスをオンにします。
Roles	(オプションですが、強く推 奨)ユーザに割り当 てるすべての役 割のチェックボックスをオンにします。 **注 意** 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、Fortify Software Security Centerにアクセスできません。
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。 **注 :** 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Fortify Software Security Center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 っています。 a. [SELECT APPLICATION VERSION]ダイアログを開くには、 [ADD]をクリックします。 b. [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。 c. 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。 右 側の [SELECTED VERSIONS]ウィンドウに 、選 択したバージョンが一 覧 表 示されます。

フィールドまたはチェックボックス	説 明
	d. 別 のアプリケーションバージョンまたはバージョンを追 加 するには、aからcのステップを繰り返します。 e. [DONE]をクリックします。

5. 次 のいずれかを実 行します。
   - 設 定 を保 存し、 [CREATE NEW USER]ダイアログボックスを終 了 するには、 [SAVE]をクリックします。
   - 設 定 を保 存して別 のユーザを作 成 するには、 [SAVE AND ADD ANOTHER] をクリックします。

Fortify Software Security Centerがローカルユーザのリストにユーザアカウントを追 加 します。

参照情報

"ローカルユーザアカウントを編 集 する" 下

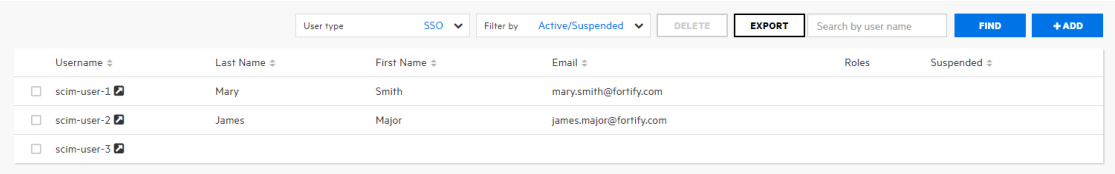
"ローカルユーザアカウントのロック解 除 " ページ215

ローカルユーザアカウントを編 集 する

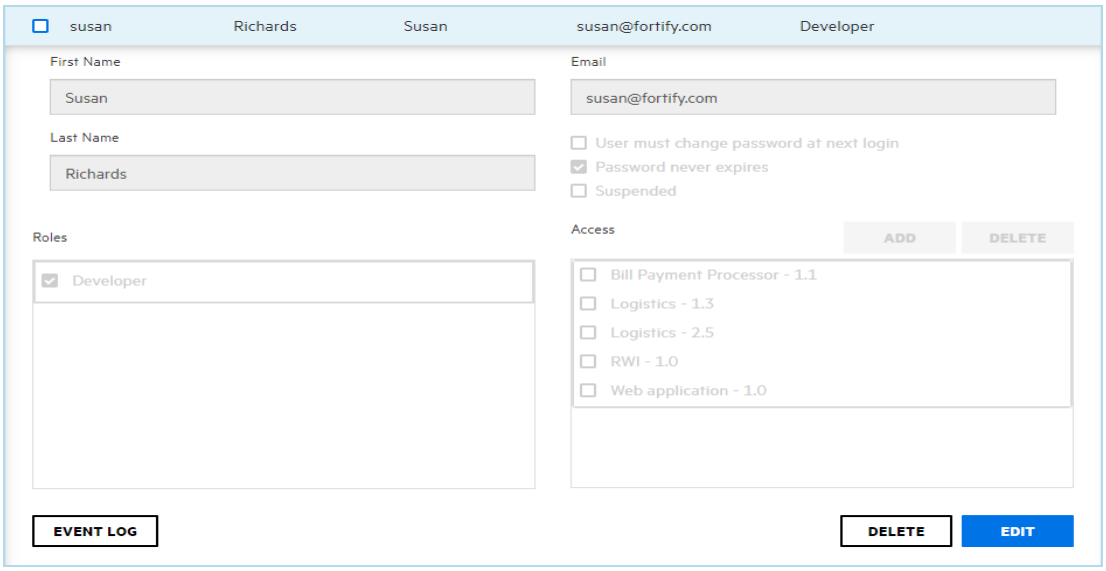
次 の手 順 では、Fortify Software Security Centerから作 成 されたローカルユーザアカウントと、SCIM APIを使 用してプロビジョニングされたユーザアカウントのアカウントを編 集 する方 法 について説 明します。

ローカルユーザアカウントを編 集 するには:

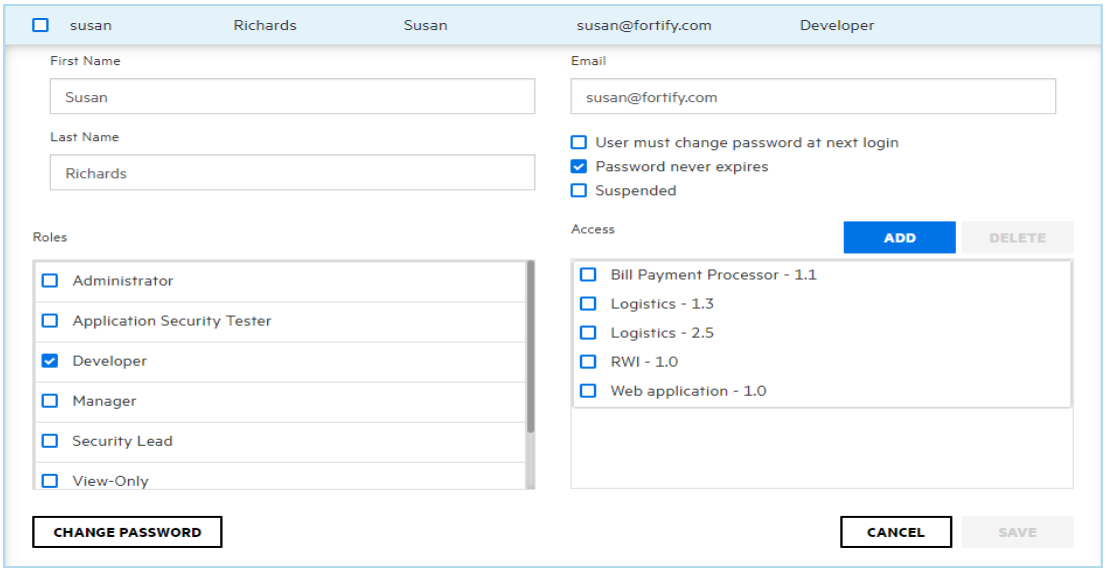
1. Fortifyのヘッダで、 [ADMINISTRATION]を選 択します。
2. [ADMINISTRATION]ビューの左 のペインで、 [Users]を選 択し、 [Local Users]をクリックします。
3. 外 部 で管 理 されている(SCIM APIを使 用してプロビジョニングされた)ユーザを選 択 的 に表 示 するには、 [User type]メニューから [SSO]を選 択します。



4. 編 集 するユーザアカウントを探して、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. 「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。

重 要 Fortify Software Security Center 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 およびアプリケーションバージョンの割 り当 てだけです。他 のすべての設 定 (および削 除)は、Azure ADから行 なう必 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、「Email」ボックスの下 のチェックボックスを必 要 に応 じて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 」セクションで、使 用 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. ユーザをアプリケーションバージョンから削 除 するには、 [**アクセス**]セクションで、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、 [**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、 [**ADD**]をクリックし、 [SELECT APPLICATION VERSION]ダイアログボックスを使 用して、ユーザが作業 するアプリケーションバージョンを指 定します。(詳 細については、"ローカルユーザアカウントの作 成" ページ210を参 照してください)。
10. ユーザのパスワードを変 更 するには、 [**CHANGE PASSWORD**]をクリックしてから、 [CHANGE PASSWORD]ダイアログボックスを使 用して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 、 [**CHANGE PASSWORD**]ボタンは使 用 できません)。
11. [**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" 下

"ローカルユーザアカウントの作 成" ページ210

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Fortify Software Security Centerへのログインに失 敗 すると、Fortify Software Security Centerはユーザがそれ以 上 のログインを試 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ており、Fortify Software Security Center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。

注 : 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. Fortifyのヘッダで、 [**ADMINISTRATION**]を選 択します。
2. [ADMINISTRATION]ビューの左 のペインで、 [**Users**]を選 択し、 [**Local Users**]をクリックします。
3. ロックされたユーザアカウントを表 示し、行 を展 開してアカウントの詳 細を表 示し、 [**UNLOCK USER**]をクリックします。
4. Fortify Software Security Centerからアカウントのロックを解 除 する確 認 を求 めるメッセージが表 示されます。
5. [**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" ページ210

"ローカルユーザアカウントを編 集 する" ページ213

外 部 管 理 されたユーザおよびグループを表 示 する

SCIMプロトコルを使 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. Fortify Software Security Center にローカル管 理 者 としてログインします。
2. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
3. 左 ペインで、 [Users]、 [Local Users]の順 に選 択 します。
4. [Local Users]ページの上 部 にある [User type]リストから、 [SSO]を選 択 します。
   Fortify Software Security Center に、SCIMプロトコルを使 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。 [Externally managed user]アイコン( )は、[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。

Azure ADから Fortify Software Security Center にプッシュされたグループを表 示 するには:

1. Fortify Software Security Center にローカル管 理 者 としてログインします。
2. Fortifyのヘッダで、 [ADMINISTRATION]を選 択 し、 [Users]、 [Local Groups]の順 に選 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

Azure AD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 てられていない場 合 や、 [Local Users]ページからユーザに個 別 に役 割 が割 り当 てられていない場 合 は、Fortify Software Security Center にアクセスできません。

注 : Fortify Software Security Center 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 およびアプリケーションバージョンの割 り当 てだけです。他 のすべての設 定 (および削 除)は、Azure ADから行 う必 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、 [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 " ページ123

"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 " ページ128

"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Azure ADへの接 続 の設 定 " ページ125

"SAML 2.0準 拠 のシングルサインオンソリューションを使 用 するためのFortify Software Security Centerの設 定 " ページ141

第11章: アプリケーションとアプリケーションバージョン

Fortify Software Security Centerで一貫した測定結果を得るために、単一コードベース用のアプリケーションを定義します。Fortify Software Security Center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Fortify Software Security Centerアプリケーションを作成します。Fortify Software Security Center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	+ 新規スキャン結果	= トレンド結果
Fortify Static Code Analyzer、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の問題と残っている問題を特定します。

Fortify Software Security Centerの分析処理ルールでは、新しいスキャンが以前のスキャンと同等か検証します。

このコンテンツでは、アプリケーションとアプリケーションバージョンに関する情報を提供します。アプリケーションの表示と作成、アプリケーション属性の設定、問題テンプレートの割り当てなど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:

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および監視し、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ための情報にアクセスする必要があります。Fortify Software Security Center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。

このセクションで説明するトピック:

アプリケーション作成プロセスについて

Fortify Software Security Centerにログインして新しいアプリケーションの追加を開始すると、[CREATE NEW APPLICATION VERSION]ウィザードに一連のステップが表示されます。これらの各ステップでは、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対して1つ以上の戦略的な選択肢が表示されます。チームが同意して選択を行った後、セキュリティリードは [FINISH]をクリックして作成プロセスを完了できます。

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。次のセクションでは、ウィザード画面に表示されるオプションについて説明します。

次に

"アプリケーションバージョン属性" ページ221

参照情報

"テンプレートの選択" ページ231

"新しいアプリケーションの最初のバージョンの作成" ページ231

"アプリケーションに新しいバージョンを追加する" ページ234

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として、展開されたアプリケーション内の脆弱性を追跡できるアプリケーションバージョンを作成する場合があります。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場合でも、ソフトウェアコンポーネント全体をまとめて追跡することは良い方法です。たとえば、テキスト操作ライブラリ自体は安全で、ファイルアクセスライブラリ自体は安全だとします。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の組み合わせは必ずしも安全ではありません。これは、処理されるテキストの出元がわからない場合があるからです。

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開発マネージャは、結果をアーカイブしてビューから削除するために、Software Security Centerで過去のバージョンを無効にできます。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" ページ266を参照してください。

  注: 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、(完全な書き換えに対して)単に発展したコードです。

継続的な展開のための戦略

継続的な展開を使用するアプリケーションの場合、`-build-label xxxx`フラグで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(`xxxx`はバージョン管理システムのIDを表す)識別できます。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。

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

Fortify Software Security Center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、Fortify Software Security Centerで提 供 される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。

Fortify Software Security Centerアプリケーションリスト の表 示

すべてのFortify Software Security Centerアプリケーションのリストを表 示 するには、次 の手 順 に従 います。

- Fortifyのヘッダで、 [APPLICATIONS]をクリックします。

参 照 情 報

" [Applications]ビューからのアプリケーションとアプリケーションバージョンの検 索 " ページ 239

アプリケーションバージョンの作 成 について

まったく新 しいアプリケーション用 に新 しいFortify Software Security Centerアプリケーションバージョンを作 成 することも、既 存 のアプリケーションバージョン用 にアプリケーションバージョンを作 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" ページ219

"新 しいアプリケーションの最 初 のバージョンの作 成 " ページ231

"アプリケーションに新 しいバージョンを追 加 する" ページ234

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、Fortify Software Security Center 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、 [CREATE NEW VERSION]ウィザードの指 示 に従 って、ビジネス、技 術 、および組 織 の必 須 およびオプションの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、アプリケーションバージョンは終 了 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

Fortify Software Security Center 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" 次のページを参照してください。

次の表は、Fortify Software Security Center 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、Fortify Software Security Center 管理者がシステムに追加したカスタム属性は含まれないので注意してください。アスタリスクが付いている属性は必須です。

技術属性	説明
*Development Phase	アプリケーションバージョンの現在の開発フェーズです。
*Development Strategy	アプリケーション開発に使用するスタッフの戦略
*Accessibility	アプリケーションを使用するために必要なアクセスのレベル
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	アプリケーションへ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	
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

組織属性	
Region	開発チームの地理的位置

ビジネスリスク属性	
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

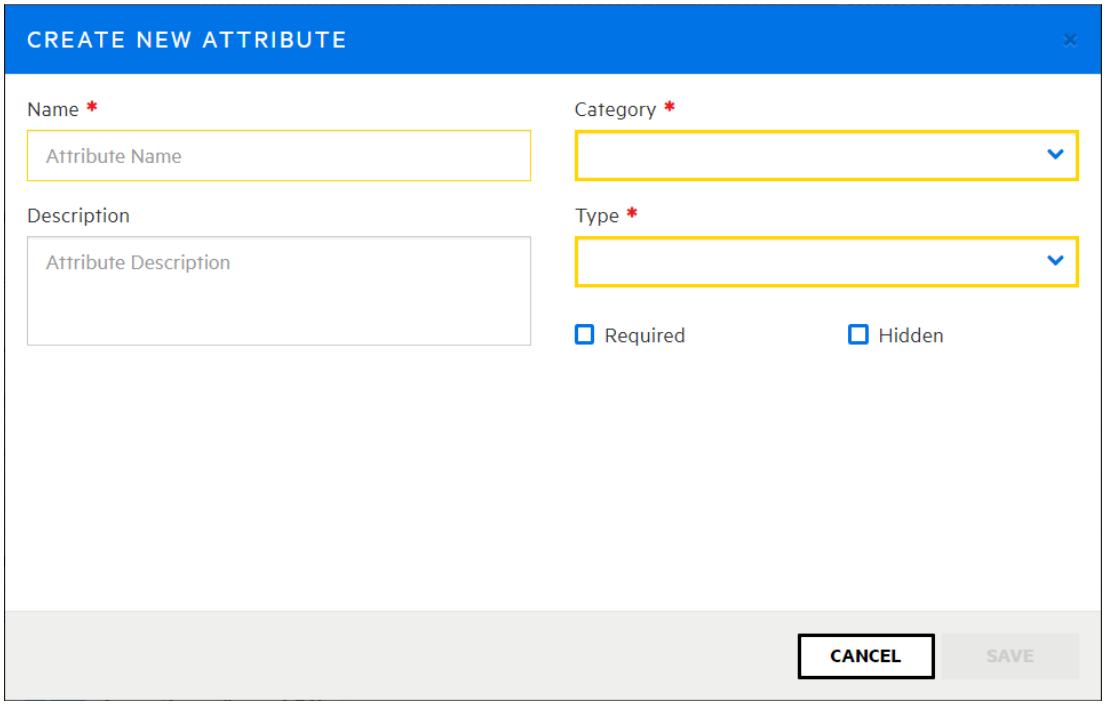
カスタム属性の作成

Fortify Software Security Center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。

注 : カスタム属性は、管理者またはセキュリティリードのユーザアカウントを持っている場合にのみ作成できます。

属性を作成するには、次の手順に従います。

1. Fortify Software Security Centerに管理者またはセキュリティリードとしてログインします。
2. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
3. 左ペインの [Templates]で、 [Attributes]をクリックします。
   [Attributes]ページの右側に属性が一覧表示されます。
4. [NEW]をクリックします。
   [CREATE NEW ATTRIBUTE]ダイアログボックスが開きます。



5. 次の表に示す情報を指定します。

フィールド	説明
Name	属性を説明する名前を入力します。 **重要** Fortify Software Security Centerが使用する設定済みの属性を削除し、その後同じ名前で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。
Description	簡単な説明を入力します。 説明は、CREATE NEW APPLICATION VERSIONウィザードの [attribute]フィールドの下に表示されます。
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、ここで定義する属性をユーザに設定する必要がある場合は、このチェックボックスをオンにします。
Hidden	新しい属性がCREATE NEW APPLICATION VERSIONウィザードに表示されるのを防ぐには、このチェックボックスをオンにします。 **注意** CREATE NEW APPLICATION VERSIONウィザード

フィールド	説明
	で属性が表示されるのを防ぐために [Hidden]を選択した場合は、 [Required]チェックボックスもクリアする必要があります。
Category	属性タイプを選択します。選択したカテゴリに応じて、CREATE NEW APPLICATION VERSIONウィザードのBusiness Attributes ステップ、Technical Attributesステップ、または Organization Attributesステップに属性が表示されます。
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。 **注 :** 単一選択タイプ属性を作成する場合、ユーザはダッシュボードの [Group by]リストおよび [Aggregate by]リストから属性を選択し、表示するデータをカスタマイズできます。 • 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。 **注 :** [List of Values]タイプのいずれかを選択すると、値とその説明を追加し、非表示にするかどうかを指定する追加フィールドが表示されます。 • 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。

フィールド	説明
	注 : このタイプは、Dynamic Scan Request属性では使用できません。 • ファイルアップロードフィールドを作成するには、[**ファイル**]を選択します。 • [Dynamic Scan Request]ダイアログボックスでファイルアップロードコントロールを作成するには、[**File**]を選択します。

6. [**SAVE**]をクリックします。

新しい属性は、ユーザが次にCREATE NEW APPLICATION VERSIONウィザードを使用するときに使用できます。

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の新しいカスタム属性の指定" ページ228を参照してください。

注 : デフォルトでは、Fortify Software Security Centerユーザインタフェースから作成した属性は削除可能です。Fortify Software Security Center 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、"Fortify Software Security Center APIドキュメントへのアクセス" ページ204を参照してください。

参照情報

"属性と属性値の削除" 下

"アプリケーションバージョン属性" ページ221

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、多くの場合はFortify Software Security Center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

Fortify Software Security Center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. Fortifyのヘッダで、[**ADMINISTRATION**]を選択します。
2. 左ペインで、[**Templates**]セクションを展開し、[**Attributes**]を選択します。

   属性を削除できる場合、名前の左側にあるチェックボックスが青色で表示されます。削除できない場合は、名前の左側にあるチェックボックスが灰色で表示されるため、選択して削除できません。

属性を削除できない理由の説明を表示するには、チェックボックスの上にカーソルを移動します (属性はシステム定義で削除不可か、ユーザ定義で変更済みなので削除できません)。

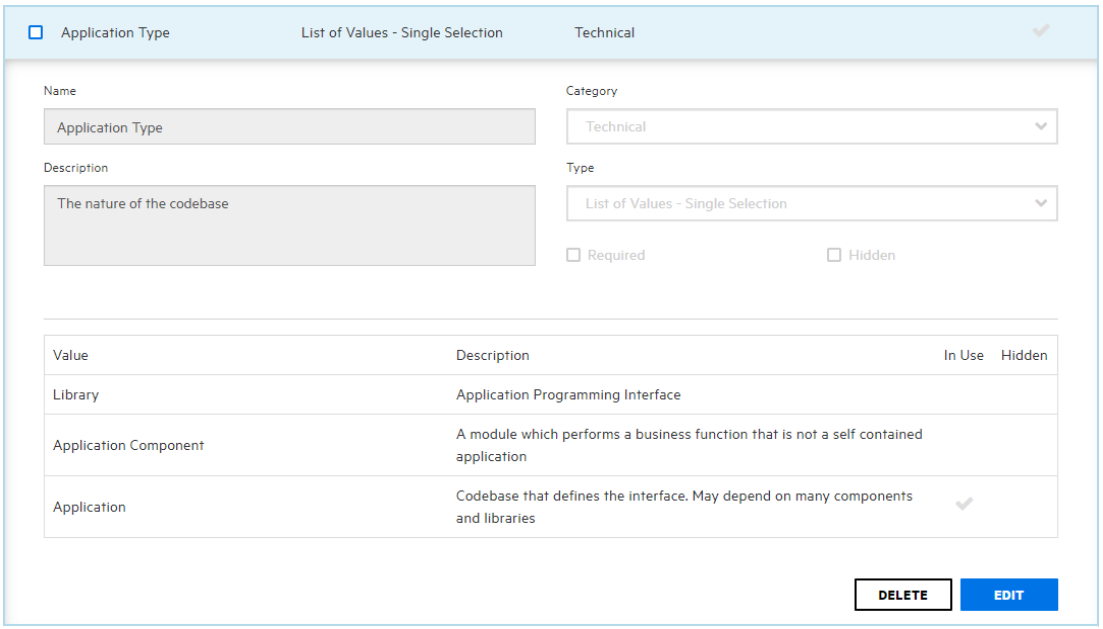
3. 削除する属性のチェックボックスをオンにして、 [DELETE]をクリックします。
   Fortify Software Security Centerに、選択した属性がシステムから完全に削除されるという事実のアラートが表示され、削除の続行を確認するメッセージが表示されます。
4. [OK]をクリックします。

注 : デフォルトでは、Fortify Software Security Centerユーザインタフェースから作成した属性は削除可能です。Fortify Software Security Center 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、"Fortify Software Security Center APIドキュメントへのアクセス" ページ204を参照してください。

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. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. 左ペインで、 [Templates]セクションを展開し、 [Attributes]を選択します。
3. 削除する1つ以上の値を持つ属性の行を展開します。

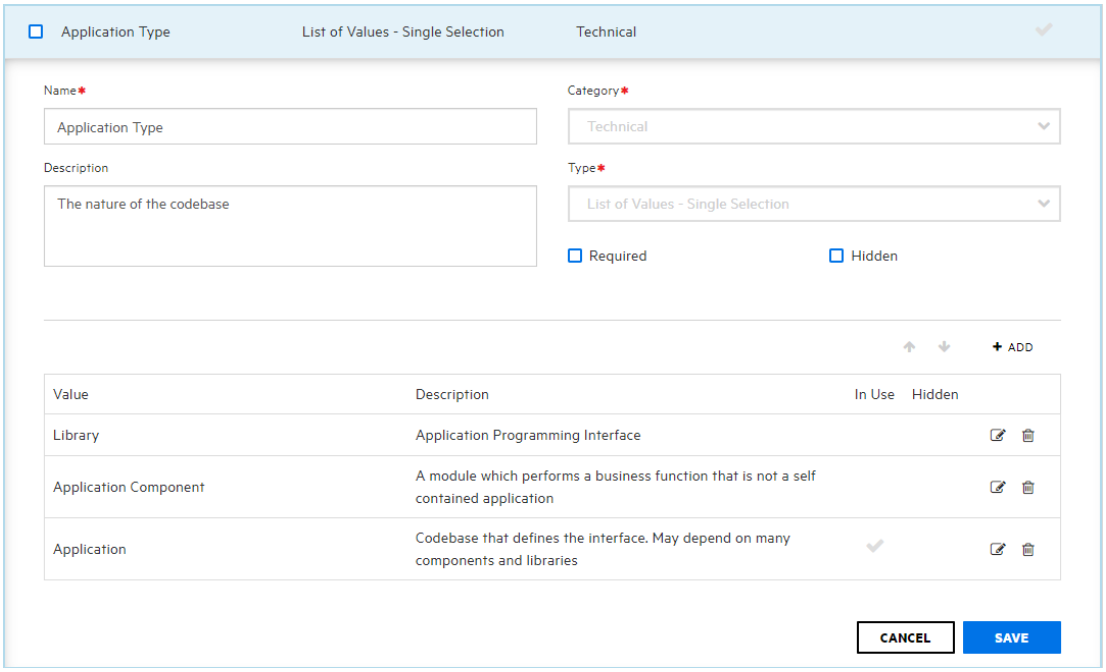


[In Use]列には、現在1つ以上のアプリケーションバージョンで使用されている値が表示されます。

4. [EDIT]をクリックします。

Fortify Software Security Centerに、加える変更により属性に基づく値を持つアプリケーションバージョンに影響を与える可能性があるという警告が表示され、属性の編集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。



6. 削除する値の右側にあるごみ箱アイコン(🗑)をクリックします。

注: 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

Fortify Software Security Center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、[CANCEL]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" ページ223

アプリケーションバージョンの新しいカスタム属性の指定

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. Fortifyのヘッダで、 [APPLICATIONS]を選択します。
2. [Applications]ビューで、アプリケーションの行を展開し、新しい属性を指定するバージョンを選択します。

   Fortify Software Security Centerに、そのバージョンの [AUDIT]ページが表示されます。
3. アプリケーションバージョンツールバーで、 [PROFILE]をクリックします。

   [APPLICATION PROFILE - <*application_name*> <*application_version*>]ウィンドウの [ADVANCED OPTIONS]セクションが開きます。
4. [APPLICATION SETTINGS]をクリックします。
5. [Version Settings]セクション で、編集アイコン🖉をクリックします。

   EDIT VERSIONウィザードの [Step 1. GENERAL]が開きます。
6. [NEXT]をクリックします。
7. [Step 2. DEFINE ATTRIBUTES AND RISK]で、属性カテゴリ([Technical Attributes]、 [Organization Attributes]、または [Business Risk Attributes])を選択し、カスタム属性の値(複数の場合あり)を選択します。
8. ウィザードのStep 4に移動し、 [FINISH]をクリックします。

参照情報

"カスタム属性の作成" ページ223

"アプリケーションバージョンの詳細を編集する" ページ239

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Fortify Software Security Center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

Fortify Software Security Centerには、事前に設計された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、アプリケーションのニーズに合わせてFortify Audit Workbenchから変更することもできます。

これらのすぐに使える問題テンプレートの説明を参照するには、次の手順に従います。

1. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. 左ペインで、 [Templates]を選択し、 [Issue]を選択します。

[Issue]ページには、問題テンプレートとその説明が一覧表示されます。

Fortify Software Security Center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、Fortify Software Security Center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。Fortify Audit Workbenchを使用して問題テンプレートを変更または作成する手順については、『Micro Focus Fortify Audit Workbenchユーザガイド』を参照してください。

システムへの問題テンプレートの追加

Fortify Audit Workbenchで作成または変更した問題テンプレートをFortify Software Security Centerに追加するには、次の手順を実行します。

1. 管理者としてFortify Software Security Centerにログインします。
2. Fortifyのヘッダで、 [**ADMINISTRATION**]をクリックします。
3. 左側のペインで、 [**Templates**]をクリックし、 [**Issue**]を選択します。
   Fortify Software Security Centerの右側のテーブル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。
   [CREATE NEW ISSUE TEMPLATE]ダイアログボックスが開きます。
5. [**Name**]ボックスにテンプレート名を入力します。
6. (オプション) [**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. [**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. [**SAVE**]をクリックします。

問題テンプレートの作成または変更

新しい問題テンプレートを作成したり既存のテンプレートを変更したりするためにFortify Audit Workbenchを使用する場合は、テンプレートに次のフィルタを含める必要があります。

```
<Filter>

  <actionParam>true</actionParam>

  <query>[category]:Insecure Dependency\: Vulnerable Component [analysis type]:SCA</query>

  <action>hide</action>

</Filter>
```

問題テンプレートを作成または変更してFortify Software Security Centerにアップロードする方法については、『Fortify Audit Workbenchユーザガイド』を参照してください。

テンプレートの選択

Fortify Software Security Centerの発行テンプレートは、Fortifyクライアント製品とサーバ製品にアプリケーションデータの分類、要約、レポーティングの最適な方法を提供します。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。

新しいアプリケーションの最初のバージョンの作成

Fortify Software Security Center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。次の手順では、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方法について説明します。

新しいアプリケーションを作成するには、次の手順に従います。

1. Fortify Software Security Centerに管理者またはセキュリティリードとしてログインします。
2. ツールバーで、 [+ NEW APPLICATION VERSION]をクリックします。
   [CREATE NEW APPLICATION VERSION]ウィザードの [GENERAL]タブが開きます。
3. [Application Setup]で、次の操作を行います。
   a. [Application name]ボックスに、新しいアプリケーションの名前を入力します。
   b. (オプション) [Application Description]ボックスに、説明を入力します。
4. [Version Setup]セクションで、次の表で説明する情報を指定します。

フィールド	説明
Version name	(必須)バージョンの名前を入力します。
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。
Use existing application version	a. 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ます。それ以外の場合は、ステップ5に進みます。 b. [SELECT APPLICATION VERSION]ダイアログボックスを開くには、 [BROWSE]をクリックします。 c. [APPLICATION]で、検索ボックスに文字列を入力し、[FIND]をクリックしてアプリケーションのリストを絞り込み、新しいアプリケーションに使用する設定を含むアプリケーションを

フィールド	説明
	選択します。 右側の［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。 d. アプリケーションの非アクティブバージョンを含めるには、［Show inactive］チェックボックスを選択します。 e. 必要なバージョンのチェックボックスをオンにして、［DONE］をクリックします。 デフォルトでは、Fortify Software Security Center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。 f. 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。 g. 選択したアプリケーションバージョンに関連する問題をすべてコピーするには、［Application state］チェックボックスをオンにします。

5. ［NEXT］をクリックして、［ATTRIBUTES］設定に進みます。
6. ［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
Development Phase	［New］を選択したままにしてください。
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。

フィールド	説明
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。

7. (オプション) 「ORGANIZATION ATTRIBUTES」タブをクリックし、次の選択をします。
   - 「Business Unit」リストから、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」リストから、このアプリケーション開発の対象業界を選択します。
   - 「Region」から、アプリケーションに関連付ける領域を選択します。
8. (オプション) 「BUSINESS RISK ATTRIBUTES」タブをクリックし、次の操作を実行します。
   a. 「Business Risk」リストから、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。
   b. 「Known Compliance Obligations」セクションで、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。
   c. 「Data Classification」セクションで、このアプリケーションが保存するデータ分類すべてのチェックボックスをオンにします。
   d. 「Application Classification」セクションで、このアプリケーションを開発しているすべてのコンシューマタイプのチェックボックスをオンにします。
9. 「TEMPLATE」設定に進むには、「NEXT」をクリックします。
10. 「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。右側のペインの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。
11. 「ACCESS」タブに進むには、「NEXT」をクリックします。
12. a. Fortify Software Security Centerデータベースからユーザを割り当てるには、「LOCAL」を選択したままにしてください。
    b. 割り当てるチームメンバーのチェックボックスをオンにします。

    注 : 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。

    または

    a. LDAPディレクトリからユーザを割り当てるには(Fortify Software Security CenterサーバにLDAP認証が設定されている場合)、「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。
    b. 割り当てるチームメンバーのチェックボックスをオンにします。

注 : 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 力して、 [**FIND**]をクリックします。

13. [**SAVE**]をクリックします。
    Fortify Software Security Centerは、アプリケーションが正 常 に作 成 されたことを示します。新 しいアプリケーションバージョンが [APPLICATIONS]ビューに表 示 されます。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、 [DASHBOARD]ビューにも表 示 されます。
14. [**CLOSE**]をクリックします。

参照情報

"アプリケーションに新しいバージョンを追 加 する" 下

アプリケーションに新 しいバージョンを追 加 する

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。次 の手 順 では、既 存 のアプリケーションの新 しいバージョンを作 成 する方 法 について説 明します。

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. Fortify Software Security Center に管 理 者 またはセキュリティリードとしてログインします。
2. ダッシュボードから、 [**+ NEW APPLICATION VERSION**]をクリックします。
   [CREATE NEW APPLICATION VERSION]ウィザードの [**GENERAL**]タブが開きます。
3. [**Application Setup**]で、次 の操 作 を行います。
   a. [**Add to existing application**]チェックボックスをオンにします。
   b. [**BROWSE**]をクリックし、 [SELECT APPLICATION]ダイアログボックスで、新しいバージョンを作 成 するアプリケーションを見 つけて選 択します。
   c. [**DONE**]をクリックします。

   [**Application name**]フィールドと [**Application description**]フィールドに、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。
4. [**Version Setup**]セクションで、次 の表 で説 明 する情 報 を指 定します。

フィールド	説 明
Version name	バージョンの名 前 を入 力 するか、バージョン名 を一 覧 から選 択します。
Version description	(オプション)アプリケーションのこのバージョンに関 する説 明 を入 力します。

フィールド	説明
Use existing application version	a. 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ます。それ以外の場合は、［NEXT］をクリックして［ATTRIBUTES］タブに進みます。 b. ［SELECT APPLICATION VERSION］ダイアログボックスを開くには、［BROWSE］をクリックします。 c. 新しいバージョンに使用する設定を持つアプリケーションを見つけて選択します。 右側の［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。(非アクティブバージョンを表示するには、［Show inactive］チェックボックスを選択します)。 d. ［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、［DONE］をクリックします。 デフォルトでは、Fortify Software Security Center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。 e. 一部の設定を除外するには、次のチェックボックスの1つ以上をオフにします。 ◦ Version attributes ◦ Custom tags ◦ Analysis processing rules ◦ User access settings ◦ Bug tracker integration settings f. 選択したアプリケーションバージョンに関連する問題をすべてコピーするには、［Application state］チェックボックスをオンにします。

5. ［ATTRIBUTES］設定に進むには、［NEXT］をクリックします。
6. ［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
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	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

フィールド	説明
Strategy	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。

7. (オプション) [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
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。

8. (オプション) [BUSINESS RISK ATTRIBUTES]タブを選択します。
9. [Business Risk]リストから、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。
10. 次の表に示す情報を指定します。

フィールド	説明
Known Compliance	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

フィールド	説明
Obligations	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。

11. テンプレート設定に進むには、 [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。

    注 : 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. [ACCESS]タブに進むには、 [NEXT]をクリックします。
14. [ASSIGN TEAM]で、次のいずれかを実行します。

    注 : 管理者役割のユーザは、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。ユーザをチームに所属させるには、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。

    - ユーザを Fortify Software Security Center データベースから割り当てるには、 [LOCAL]を選択してから、割り当てるチームメンバーのチェックボックスをオンにします。

    注 : 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。

    - あるいは、LDAP認証が Fortify Software Security Center サーバに設定されている場合は:

    a. [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。
    b. 割り当てるチームメンバーのチェックボックスをオンにします。

    注 : 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て、 [FIND]をクリックします。

15. [SAVE]をクリックします。

Fortify Software Security Center にバージョンが正 常 に作 成 されたことが示 され て、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リストに追 加 されま す。

16. [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" ページ231

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 が監 査 アシスタントを設 定し、自 動 適 用をシステム全 体 で有 効にし、ADMINISTRATIONビューの [カスタムタグ]セクションで適 切 なプライマリタグフィールドをマップした場 合 、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 、監 査 アシスタントを使 用して静 的 解 析 の問 題 に関 する予 測 を要 求 すると、Fortify Software Security Centerがこれらの予 測 をカスタムタグ値 に適 用します。

監 査 アシスタントが自 動 的にカスタムタグ値 を問 題 に適 用すると、問 題 に保 存 されたメタデータはそれが監 査 アシスタントによって監 査 されたことを示します。カスタムタグ名 の横 にグレーの小 槌 が表 示 されて、ユーザは監 査 アシスタントが問 題 を予 測 したことを確 認 できます。

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:

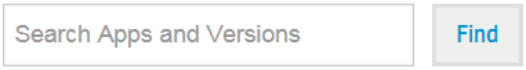
1. Fortifyダッシュボードから、自 動 適 用を有 効にするアプリケーションバージョンのリンクを選 択します。
   [AUDIT]ページには、アプリケーションバージョンに関 連 する問 題 が一 覧 表 示 されます。
2. ページヘッダで、 [PROFILE]をクリックします。
3. [AUDIT ASSISTANT OPTIONS]を選 択します。
4. 監 査 アシスタントが監 査 されていない問 題 を自 動 的にAudify Scan Analyticsへ送 信して評 価 させる場 合 は、 [Enable auto-predict]チェックボックスをオンにします。(自 動 予 測 の詳 細 については、"監 査 アシスタントの自 動 予 測 について" ページ89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 が監 査 アシスタントにマップされていない場 合 、Fortify Software Security Centerがその結 果 に対 する警 告 を表 示 して、管 理 者 に問 い合 わせるよう勧 めます。
6. [APPLY]をクリックします。
7. Fortify Software Security Center で、設 定 を保 存 するかどうかを確 認 するようメッセージが表 示 されます。
8. [OK]をクリックします。
9. [CLOSE]をクリックします。

参照情報

"Audit Assistantの設定" ページ87

[Applications]ビューからのアプリケーションとアプリケーションバージョンの検索

[Applications]ビューから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次の手順に従います。



1. [Applications]テーブルの上にある [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。
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

"Fortify Software Security Centerでのグローバル検索" ページ334

アプリケーション概要ページの更新

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 [Overview]ページの見出しに「詳細情報」アイコン(🔄)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。

- アイコンをクリックし、 [Refresh application metrics]ダイアログで [Refresh now]をクリックします。

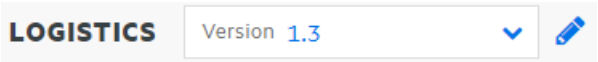
現在のシステムアクティビティによっては、メトリックの更新に時間がかかる場合があります。更新が完了すると、 [概要]ページにアプリケーションの最新データが表示されます。

注: システムスケジュールに従って、メトリックも自動的に更新されます。

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. Fortifyのヘッダで、 [APPLICATIONS]をクリックします。
2. [アプリケーション]テーブルで、編集するアプリケーションバージョンを選択します。



3. [AUDIT]ページのアプリケーション名の右側で、編集アイコン をクリックします。
   [EDIT VERSION: <*version*>]ウィンドウが開きます。
4. "アプリケーションに新しいバージョンを追加する" ページ234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. 変更を行った後、 [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" ページ249

バグトラッキングシステムを使用したセキュリティ脆弱性の管理

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、Software Security Center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、Software Security Center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Software Security Centerに戻るリンク

このセクションで説明するトピック:

バグトラッカの設 定

チームがFortify Software Security Center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Fortify Software Security Centerを設 定 する必 要 があります。その後 、開 発 者 またはセキュリティリード はバグを送 信 して、重 要 なセキュリティ問 題 に対 処できます。

セキュリティリード または開 発 マネージャは、次 のように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" 下

"バグトラッカプラグインの管 理 " ページ160

"バグトラッカプラグインの作 成 " ページ397

バグ報 告 用 Velocityテンプレート

Fortify Software Security Center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。

Fortify Software Security Centerには、Fortify Software Security Center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 " 下

"バグトラッカープラグインの速 度 テンプレートを編 集 する" ページ243

"Velocityテンプレート の削 除 " ページ244

バグトラッカプラグインへのVelocityテンプレート の追 加

Fortify Software Security Centerには、Fortify Software Security Center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。

重要 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前に、テンプレート内の変数を正しく参照する方法を理解するために、事前に定義されたテンプレートを注意深く確認してください。

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、テンプレート内の変数はレンダリング前に検証することを強く推奨します (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. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. 左ペインで、 [Templates]を選択し、 [Bug Filing]を選択します。
   [Bug Filing]ページには、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. [EDIT]をクリックします。
5. [+ ADD FIELD]をクリックします。
   [ADD TEMPLATE]ダイアログボックスが開きます。
6. [Mapped field]ボックスに、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る、マップするフィールドの名前を入力します (テキストベースのフィールドのみマップできます)。
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、 [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サイトに移動します。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。

   注: 一部の問題では、すべての変数を使用できないことがあります。特に、「ATTRIBUTE_COMMENTS」、「ISSUE_DETAIL」、「ISSUE_RECOMMENDATION」などの詳細コンテンツは、単一の問題によるバグを報告している場合にのみ利用できます。
8. [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. [SAVE]をクリックします。

[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した。

参照情報

"バグ報告用Velocityテンプレート" ページ241

"バグトラッカープラグインの速度テンプレートを編集する" 下

"バグトラッカの設定" ページ241

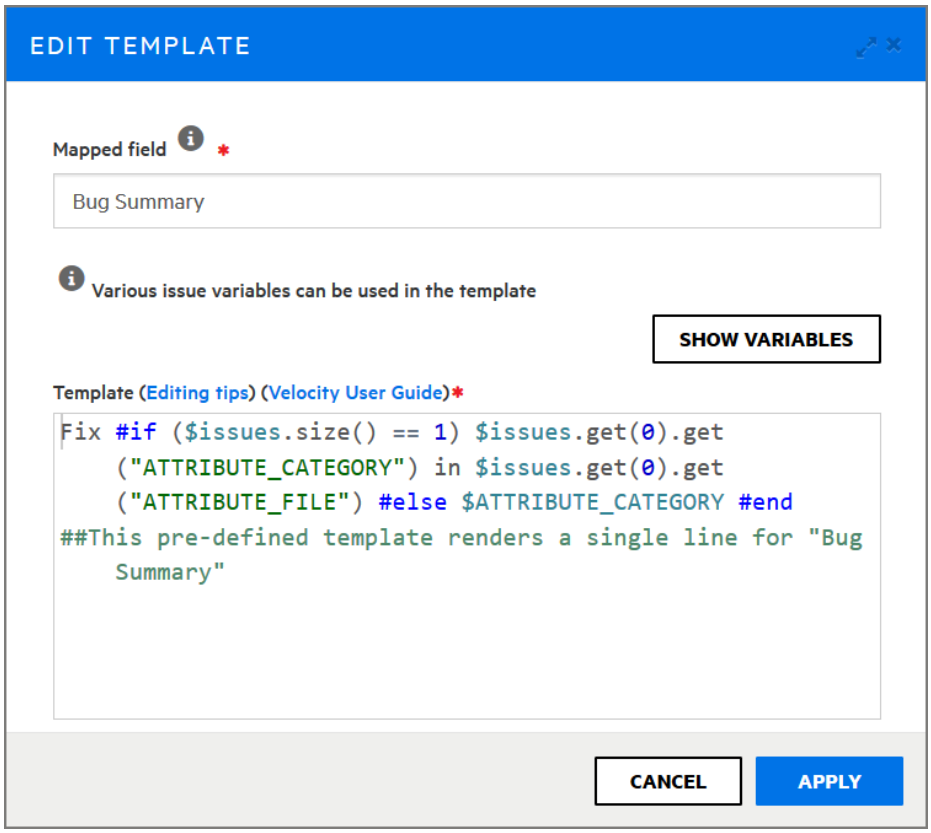
"Velocityテンプレートの削除" 次のページ

バグトラッカープラグインの速度テンプレートを編集する

バグトラッカープラグインの速度テンプレートを編集するには:

1. Fortifyのヘッダで、 [**ADMINISTRATION**]を選択します。
2. [ADMINISTRATION]ページの左ペインで、 [**テンプレート**]を選択し、 [**Bug Filing Templates**]を選択します。
3. 右側のテーブルで、使用するバグトラッカー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. [**EDIT**]をクリックします。

5. 変更するマップされたフィールドの右側にある [**Edit field**]アイコンをクリックします。
   [EDIT TEMPLATE]ダイアログボックスが開きます。



6. テンプレートの編集方法に関するヒントを見るには、 [**Editing tips**]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サイトに移動します。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. [**Mapped field**]ボックスと [**テンプレート**]ボックスの内容に必要な変更を加えます。
8. [**APPLY**]をクリックします。
9. [**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" 下

"バグ報告用Velocityテンプレート" ページ241

"バグトラッカプラグインへのVelocityテンプレートの追加" ページ241

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. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. [Bug Filing]ページの左ペインで、 [Templates]を選択し、 [Bug Filing]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。
   Fortify Software Security Centerからテンプレートグループを削除する確認を求めるメッセージが表示されます。

   注意 事前定義のテンプレートグループは削除しないことを強く推奨します。

5. 削除を続行するには、 [OK]をクリックします。

[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" ページ241

"バグトラッカプラグインへのVelocityテンプレートの追加" ページ241

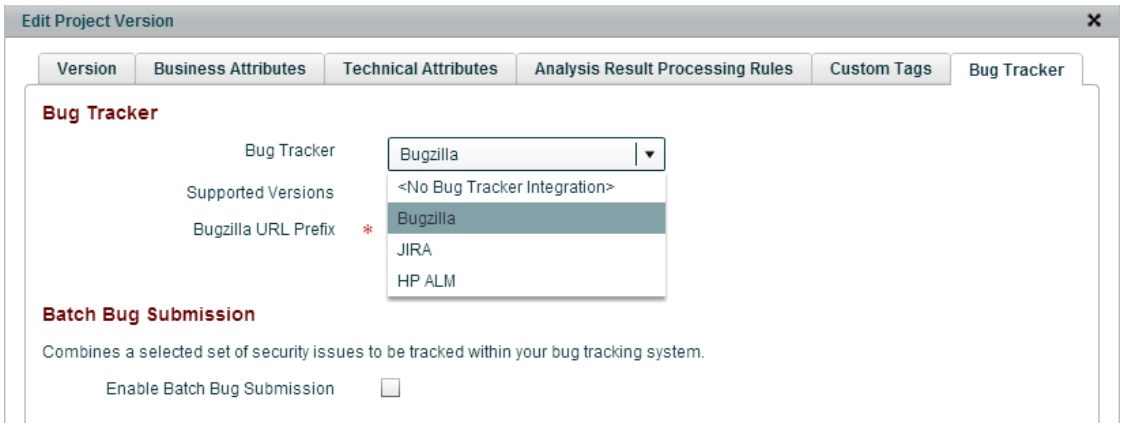
"バグトラッカープラグインの速度テンプレートを編集する" ページ243

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。Fortify Software Security Centerにバグトラッカを追加する方法については、"バグトラッカプラグインの管理" ページ160を参照してください。

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. Fortifyのヘッダで、 [APPLICATIONS]をクリックします。
2. [Applications]テーブルで、バグトラッカを割り当てるアプリケーションバージョンをクリックします。
   選択したアプリケーションバージョンの [AUDIT]ページには、そのバージョンに関する問題が一覧表示されます。
3. 右上で、 [PROFILE]をクリックします。
   [APPLICATION PROFILE - <*Application_Name*><*Application_Version*>]ダイアログボックスが開きます。
4. [BUG TRACKER]タブをクリックします。



5. [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。
   [TEST BUG TRACKER PLUGIN CONFIGURATION]ダイアログボックスが開きます。
7. バグトラッカ認証資格情報を入力し、[TEST]をクリックします。
   Fortify Software Security Center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、Fortify Software Security Center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。
    [SUCCESS]ダイアログボックスには、バグ設定が成功したというメッセージが表示されます。
11. [OK]をクリックします。
12. [CLOSE]をクリックします。

参照情報

"バグトラッカーの統合について" ページ159

"バグトラッカプラグインの管理" ページ160

"複数の問題のバグの送信" 次のページ

"バグトラッカプラグインの作成" ページ397

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" ページ245)、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 [AUDIT] ページで、バグを送信する問題の行を展開します。
2. [FILE BUG] をクリックします。

   注 : [FILE BUG] ボタンが使用できない場合、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可能性があります。(この問題に対処するには、"バグトラッカプラグインの管理" ページ160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" ページ245を参照してください)。

   この問題に対してすでにバグが送信されている場合は、新しいバグを送信できないことに注意してください。

   [FILE ISSUES (1)] ダイアログボックスが開きます。
3. [Login] 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、 [LOGIN] をクリックします。

   Fortify Software Security Center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。
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" 下

"問題に対して送信されたバグの表示" ページ326

複数の問題のバグの送信

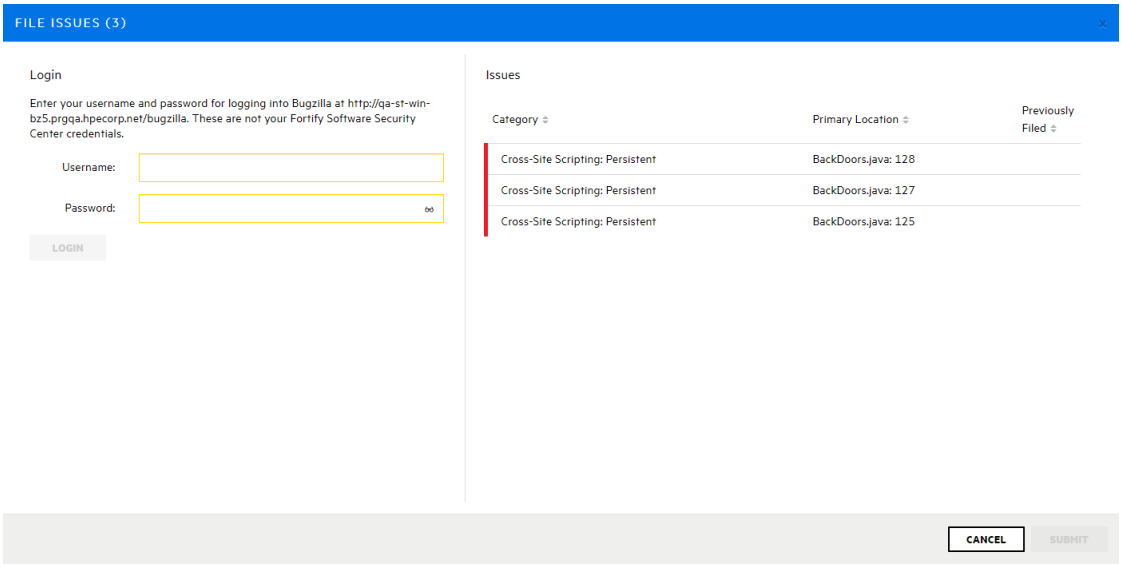
アプリケーションバージョンに対してバグトラッキングプラグインが指定されている場合 ("アプリケーションバージョンへのバグトラッキングシステムの割り当て" ページ245)、1つ以上の問題を対象にするバグを送信できます。(1つの問題に対してバグを報告する方法については、"単一の問題のバグの送信" 上を参照してください)。

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 [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、 [Issues] テーブルの上にある [File Bug] アイコンをクリックします。

[FILE ISSUES]ダイアログボックスが開きます。

注 : チェックボックスをオンにした後で、 [**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" ページ245を参照してください)。



注 : 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。 [FILE ISSUES]ダイアログボックスには、「Some selected issues have already been filed and will be ignored」というメッセージが表示され、 [**Previously Filed**]カラムに問題のバグアイコンが表示されます。

2. [**Login**]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、 [**LOGIN**]をクリックします。

   Fortify Software Security Center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。

参照情報

"単一の問題のバグの送信" 前のページ

"問題に対して送信されたバグの表示" ページ326

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、Fortify Software Security Centerでバグに対して特定の更新を加えることができます。Fortify Software Security Center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。

スキャンの結果、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いずれかが解決しない(および選択基準に一致する)場合、Fortify Software Security Centerではバグトラッキングシステムをチェックして、バグが有効な未解決状態にあるかどうかを確認し、必要に応じてバグを再び開きます。

バグに関連付けられているすべての問題が削除された場合 (問題が修正されたか選択基準に一致しなくなったため)、Fortify Software Security Centerではバグを更新して、利害関係者がチケットを解決または終了できる可能性があることを示します。監査と追跡可能性を有効にするために、Fortify Software Security Center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" ページ245を参照してください。

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。

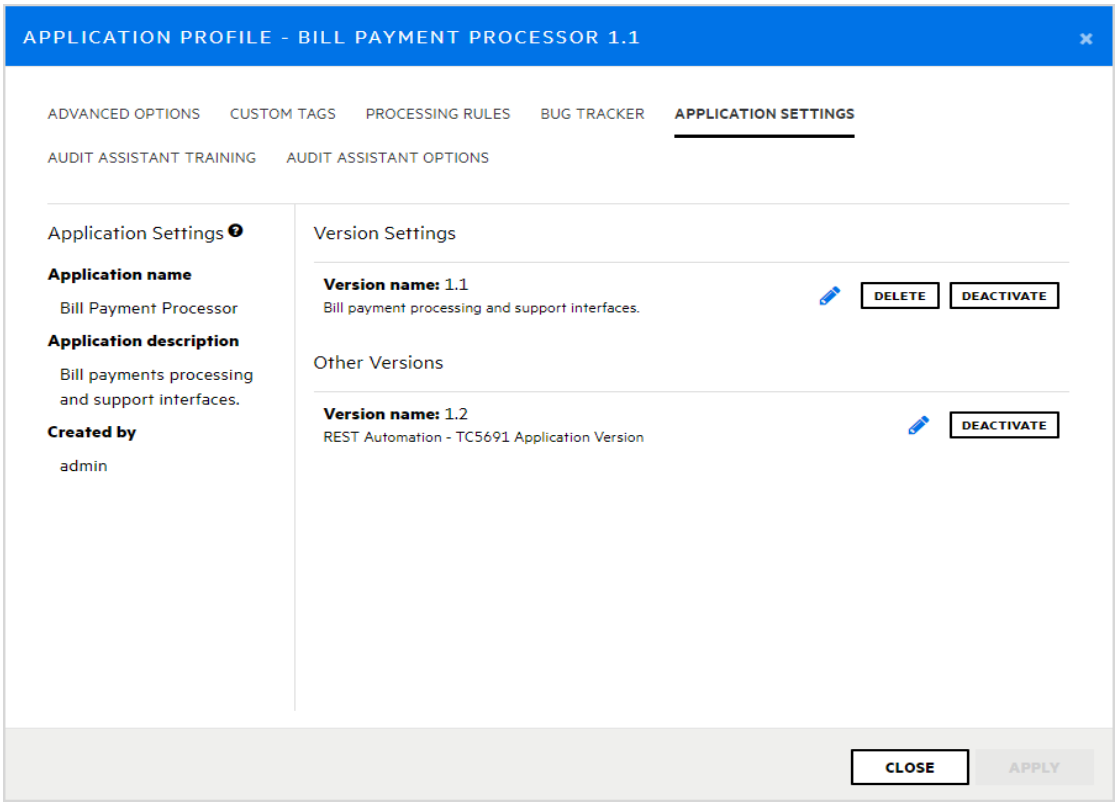
注意 Fortifyでは、アプリケーションバージョンに関連付けられているテンプレートは、そのアプリケーションバージョンに対してまだ結果が処理されていない場合にのみ変更することを推奨します。すでに結果が処理されているアプリケーションバージョンの問題テンプレートを変更した場合、Fortify Software Security Centerは、問題メトリックは再計算されず、以前に割り当てられたテンプレートに基づいて生成されたメトリックは利用できず、削除することはできません。

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. Fortify Software Security Center に管理者またはセキュリティリードとしてログインします。
2. ダッシュボードの [ISSUE STATS]ページで、変更するアプリケーションバージョンの名前をクリックします。
   選択したバージョンの [AUDIT]ページが開きます。
3. アプリケーションバージョンツールバーで、 [PROFILE]をクリックします。

[APPLICATION PROFILE <*application_version*>]ダイアログボックスが開きます。

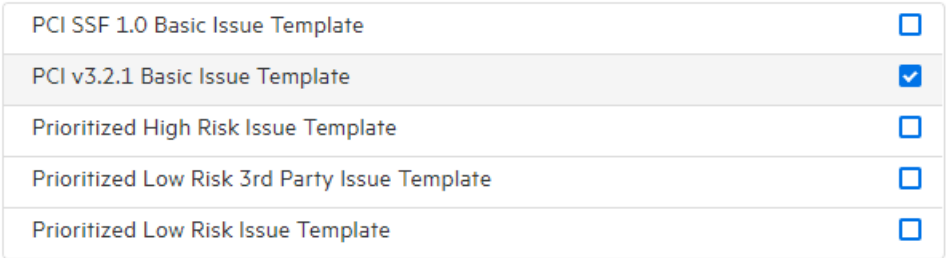
4. [**APPLICATION SETTINGS**]をクリックします。



5. [**Version Settings**]で、編集アイコンをクリックします。
[EDIT VERSION]ダイアログボックスが開きます。

注意 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。既存のメトリックスは再計算されません。

6. [**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。

7. 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。

8. [SAVE]をクリックします。

テンプレートを変更した後、Fortify Software Security Centerは、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(別のユーザによるものなど)を無効にし、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エラーメッセージを表示します。

注 : 影響を受けるアプリケーションバージョンを監査する、Fortify Audit Workbenchユーザには、この情報は表示されません。

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

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が処理される際に従うルールを設定できます。

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、次の手順に従います。

1. 管理者としてFortify Software Security Centerにログインし、ダッシュボードで、分析結果の処理ルールを設定するアプリケーションバージョンのリンクをクリックします。
   アプリケーションバージョンの [AUDIT]ページが開きます。
2. アプリケーションバージョンツールバーで、 [PROFILE]をクリックします。
   [APPLICATION PROFILE - <*Application_Version*>]ダイアログボックスが開きます。
3. [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。
4. 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。次の表で、処理ルールについて説明します。

ルール	説明
Require approval if the Build Project is different between scans	Fortify Software Security Center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、Fortify Software Security Centerによってファイルの外部メタデータバージョンとFortify Software Security Centerサーバ上の外部メタデータバー

ルール	説明
	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後(上位)である場合、Fortify Software Security Centerではファイルのアップロードに対する承認が必要です。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前(低い)、または同じ場合は、Fortify Software Security CenterはFPRファイルのアップロードを許可します。
Require approval if file count differs by more than 10%	Fortify Software Security Center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。カウントが10%を超えて異なる場合は、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。
Perform Force Instance ID migration on upload	新しいバージョンのFortify Static Code AnalyzerまたはRulepackは、古いバージョンのFortify Static Code Analyzer(またはRulepack)によって過去のスキャンで作成されたものからインスタンスIDを変更できます。実際には、両方のインスタンスが同じ問題を識別します。このルールを有効にすると、Fortify Static Code Analyzer(またはRulepack)のバージョンのバージョンが同じ場合でも、古いインスタンスIDが対応する新しいインスタンスIDに移行されます。("Automatically perform Instance ID migration on upload" 次のページも参照してください)。
Require approval if result has Fortify Java Annotations	Fortify Software Security Centerが結果をチェックして、Fortify Javaの注釈を含めるかどうかを判断します。Fortify Software Security Centerが注釈を見

ルール	説明
	つけた場合は、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。
Require approval if line count differs by more than 10%	Fortify Software Security Centerは、スキャンと前のスキャンの行数を比較します。カウントが10%を超えて異なる場合は、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。
Automatically perform Instance ID migration on upload	新しいバージョンのFortify Static Code AnalyzerまたはRulepackは、古いバージョンのFortify Static Code AnalyzerまたはRulepackによって過去のスキャンで作成されたインスタンスIDからインスタンスIDを変更できます。実際には、両方のインスタンスが同じ問題を識別します。このルールを有効にすると、古いインスタンスのIDが対応する新しいインスタンスのDに自動的に移行され、問題の履歴が保持されます。このルールは、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無効にした方が便利な場合があります。("Perform Force Instance ID migration on upload" 前のページも参照してください)。
Require approval if the engine version of a scan is newer than the engine version of the previous scan	Fortify Software Security Centerは、スキャンエンジン(Fortify Static Code Analyzer、Fortify WebInspect、Fortify WebInspect Agent)のバージョンが、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確認します。新しいバージョンが検出された場合は、アップロードに管理者承認のフラグを設定します。
Ignore SCA scans performed in Quick Scan mode	Quick Scan Modeで実行される、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

ルール	説明
	は、高信頼性と高重大度の問題が検索されます。
Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan	Fortify Software Security Center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確認します。Rulepackが追加、削除、または更新された場合は、アップロードに管理者承認のフラグを設定します。
Require approval if Fortify SCA or Fortify WebInspect Agent scan does not have valid certification	Fortify Software Security Centerは、Fortify Static Code AnalyzerまたはWebInspect Agentスキャンに有効な証明書があるかを確認します。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、ルールには管理者承認が必要です。
Require approval if result has analysis warnings	Fortify Software Security Centerは、Fortify Static Code AnalyzerまたはFortify WebInspect 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、ルールには管理者承認が必要です。 **注 :** このルールは、指定された結果ファイルの最初のアップロードにのみ適用され、その後のファイルのアップロードには適用されません。たとえば、分析警告を含む以前にアップロードされたFPRファイルに監査情報を追加する場合、Fortify Software Security Centerでは変更されたファイルが再びアップロード

ルール	説明
	される際に管理者承認は必要とされません。
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、ルールには管理者承認が必要です。
Require the issue audit permission to upload audited analysis files	ユーザが監査された分析ファイルをアップロードしようとしたが、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解凍)を持ってない場合、このルールは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	分析結果に承認が必要な場合、このルールは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FPRを承認すると、以前のすべてのFPRが自動的に承認されます。

Fortify Software Security Centerで、分析結果処理ルールの設定を保存する確認メッセージが表示されます。

5. [APPLY]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" ページ288

"アプリケーションバージョンの分析結果を承認する" ページ293

アプリケーションバージョンに対するAudit Assistantオプションの設定

アプリケーションバージョンのAudit Assistantオプションを設定するには、次の手順に従います。

1. アプリケーションでAudit Assistantを使用するようにFortify Software Security Centerが設定されていることを確認します。("Audit Assistantの設定" ページ87を参照してください)。
2. ダッシュボードから、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を選択します。
3. [AUDIT]ページで、 [**PROFILE**]をクリックします。

   [APPLICATION PROFILE - <*application_name*> <*application_version*>]ウィンドウの [**ADVANCED OPTIONS**]セクションが開きます。
4. [**AUDIT ASSISTANT OPTIONS**]をクリックします。
5. [**Application version prediction policy**]リストから、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。

   注: [**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。("Audit Assistantの設定" ページ87を参照してください)。それ以外の場合、Audit Assistantはデフォルトの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予測ポリシーを指定しない場合、Audit Assistantはデフォルトの予測ポリシーを使用します。
6. Audit Assistantが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 Scan Analyticsサーバに自動的に送信するようにするには [**Enable auto-prediction**]をオンにします。

   注: [**Enable auto-prediction**]および [**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。("Audit Assistantの設定" ページ87を参照してください)。
7. Audit Assistantが、Scan Analyticsサーバからマップされたカスタムタグ値に予測値を自動的に割り当てるようにするには、 [**Enable auto-apply**]チェックボックスを選択します。
8. [**APPLY**]をクリックします。

参照情報

"Audit Assistantの設定" ページ87

カスタムタグ

Fortify Software Security Center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。

Fortify Software Security Centerには「Analysis」という名前の単一デフォルトタグが用意されているため、すぐにアプリケーションの監査を有効にできます。Analysisタグの有効な値は、Exploitable、Not an Issue、Suspicious、Reliability Issue、およびBad Practiceです。Analysisタグ属性を変更したり、タグ値を変更したり、監査ニーズに基づいて新しいタグ値を追加したりすることができます。

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。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。開発者が自身の問題を監査した後、セキュリティエキスパートが同じ問題をレビューし、それぞれを「承認済み」または「承認しない」とマークできます。

注 : 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Fortify Software Security Centerで定義されていない場合、Audit WorkbenchユーザがFPRファイルをFortify Software Security Centerにアップロードした後に新しいカスタムタグは失われます。

このセクションで説明するトピック:

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. [ADMINISTRATION]ページの左ペインから、[**Templates**]をクリックして、[**Custom Tags**]をクリックします。
2. [**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。

3. [EDIT]をクリックします。
4. タグ属性を変更し、変更を保存します。

> **注意** カスタムタグに指定する名前がデータベース予約語で指定されていないことを確認します。

参照情報

"カスタムタグ値の追加" 次のページ

ページ1の「システムへのカスタムタグの追加」

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. ADMINISTRATIONビューの左ペインから、[**テンプレート**]をクリックして、[**Custom Tags**]を選択します。
   [カスタムタグ]ページには、既存のすべてのカスタムタグが一覧表示されます。
2. 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。
3. [EDIT]をクリックします。
4. [Hidden]チェックボックスを選択します。
5. [SAVE]をクリックします。

カスタムタグは [AUDIT]ページやFortify Audit Workbenchに表示されなくなりました。

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。

> **注:** 次の場合は、カスタムタグを削除できません。
>
> - タグが現在プライマリタグとして設定されている。
> - タグが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。
> - カスタムタグを使用して問題が監査されている。
>
> [Analysis]タグは削除できます。

カスタムタグを削除するには、次の手順を実行します。

1. [ADMINISTRATION]ページの左ペインから、[**Templates**]を選択して、[**Custom Tags**]を選択します。
   [Custom Tags]ページが開きます。既存のカスタムタグが右側に表示されます。
2. 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。

3. [Custom Tags]ツールバーで [DELETE]をクリックします。
4. タグ(複数の場合あり)を削除するメッセージが表示されたら、 [OK]をクリックします。

参照情報

"カスタムタグ" ページ256

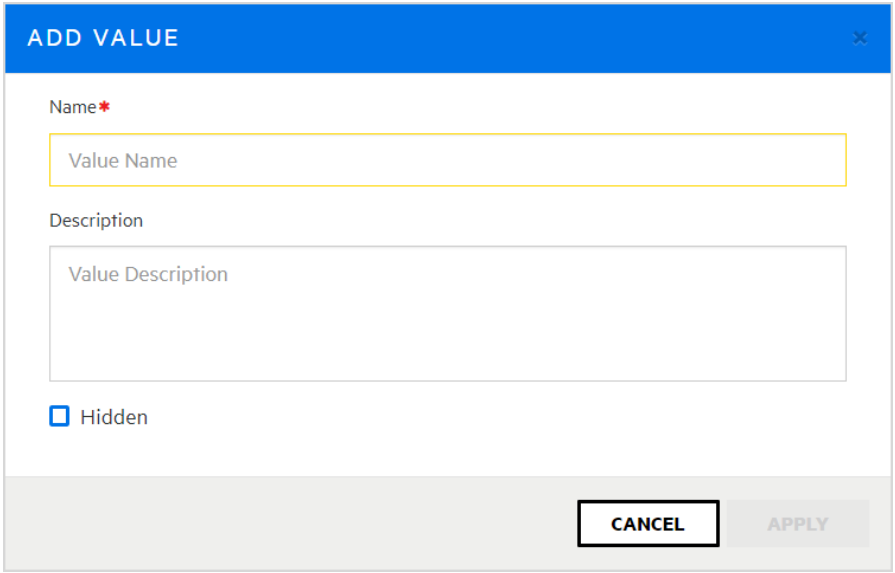
カスタムタグ値の追加

Fortify Software Security Center管理者は、システムでリストタイプのカスタムタグに値を追加できます。

注: 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。

リストタイプのカスタムタグに値を追加するには、次の手順を実行します。

1. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左ペインで、 [Templates]をクリックし、 [Custom Tags]をクリックします。
   [Custom Tags]ページには、システム内のカスタムタグが一覧表示されます。
3. 値を追加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. 値の表の下で、 [EDIT]をクリックします。
5. 値の表の上で、 [+ ADD]をクリックします。



6. [ADD VALUE]ダイアログボックスで、名前と、必要に応じて新しい値の説明を入力します。
   Audit Assistantを使用するようにFortify Software Security Centerが設定されていて、自動適用が有効な場合は、Audit Assistantタグを新しいタグ値にマップする必要があります。

7. Audit Assistantタグを新しいタグ値にマップするには、 [**AA Custom Tags**]で、新しいタグ値に対応するAudit Assistantタグのチェックボックスをオンにします。(必要に応じて、後でマッピングを変更できます)。
8. [Assign]ダイアログボックスまたは [Audit Workbench]でタグが表示されるのを防ぐには、 [**Hidden**]チェックボックスをオンにします。
9. [**APPLY**]をクリックします。
10. [Custom Tags]ページの [**Audit Assistant Training**]の下で、新しい値が [**Non-Issue**]リストに一覧表示されます。実際の問題ではない場合は、そのままにしてください。実際にこの値が実際の問題に適用される場合は、値を選択して [**True Issue**]リストに移動します。

注: [**Non-Issue**]リストと [**True Issue**]リストの両方には、それぞれ少なくとも1つの値が含まれている必要があります。

11. [**SAVE**]をクリックします。

参照情報

"カスタムタグを編集する" 下

"カスタムタグ値の削除" 次のページ

1ページの「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" ページ263

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. ADMINISTRATIONビューの左ペインから、 [**テンプレート**]をクリックして、 [**Custom Tags**]を選択します。
   [Custom Tags]ページには、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。
2. 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。
3. 値の表の下で、 [**EDIT**]をクリックします。
4. 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。
   表示されるフィールドの詳細については、ページ1の「システムへのカスタムタグの追加」を参照してください。

参照情報

"カスタムタグ値の削除" 次のページ

"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" ページ263

カスタムタグ値 の削 除

管 理 者 またはセキュリティリード は、カスタムタグ値 を削 除 できます。

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。

注 : 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 、またはその値 を使 用 して問 題 が監 査 されている場 合 は、カスタムタグ値 を削 除 できません。

1. [ADMINISTRATION]ビューの左 ペインから、 [**Templates**]を選 択 して、 [**Custom Tags**]を選 択 します。
   [Custom Tags]ページには、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。
2. 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。
3. 値 の表 の下 で、 [**EDIT**]をクリックします。
4. 値 の表 で、削 除 する値 の行 にある [**Remove value**]アイコン をクリックします。
5. [**SAVE**]をクリックします。

参 照 情 報

"カスタムタグを編 集 する" 前 のページ

ページ1の「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 " ページ259

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。

注 : 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. Fortifyのヘッダで、 [**ADMINISTRATION**]をクリックします。
2. 左 ペインで、 [**Templates**]を選 択 し、 [**Issue**]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. [EDIT]をクリックします。
5. [CUSTOM TAGS]セクションで、 [+ADD CUSTOM TAG]をクリックします。
   [ADD CUSTOM TAG]ダイアログボックスが開きます。
6. 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、 [+ADD]をクリックします。
   [CUSTOM TAGS]テーブルに、追加したタグが一覧表示されます。
7. [SAVE]をクリックします。

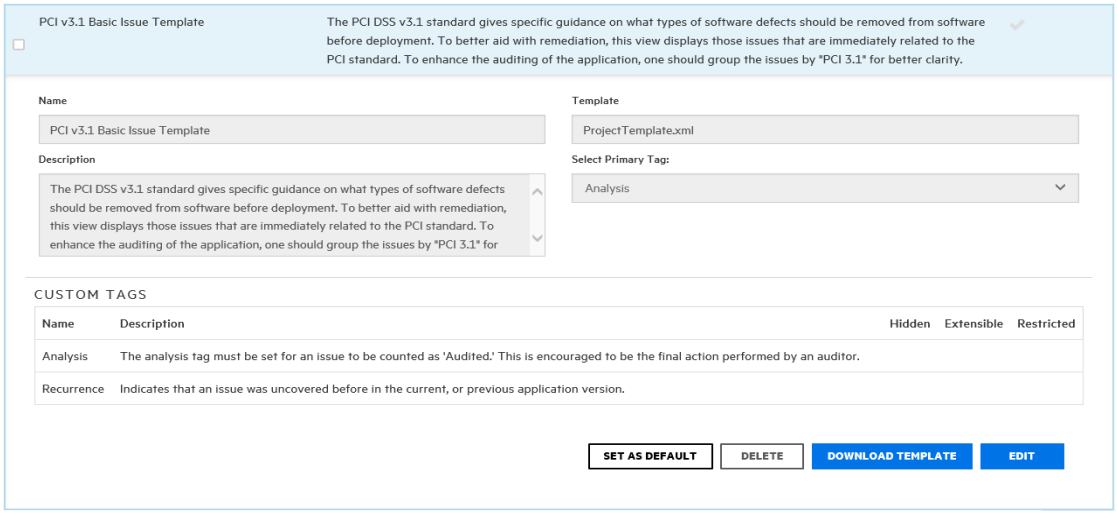
参照情報

"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" ページ264

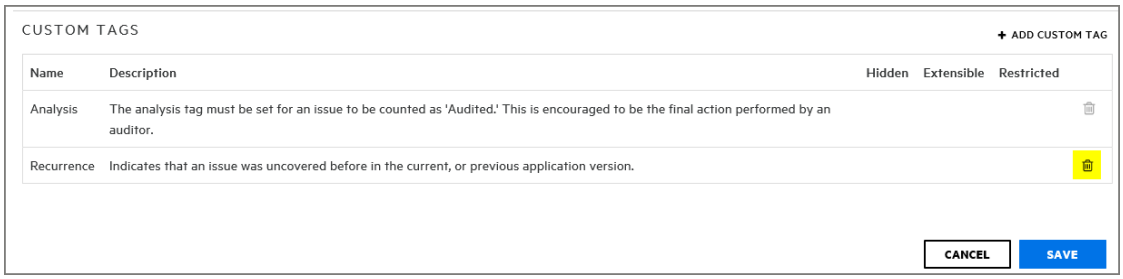
問題テンプレートからのカスタムタグの削除

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. [ADMINISTRATION]ページの左のペインから [Templates]を選択し、 [Issue]を選択します。
   右側の表には、システム内のすべての問題テンプレートが一覧表示されます。
2. 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。 [CUSTOM TAGS]セクションには、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。



3. 展開した行の下部にある [EDIT]をクリックします。



4. 最後の列で、テンプレートから削除するカスタムタグの削除アイコンをクリックします。
5. [SAVE]をクリックします。

参照情報

"カスタムタグ" ページ256

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. [Applications]ビューで、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。

   選択したバージョンの [AUDIT]ページが開きます。
2. アプリケーションバージョンツールバーで、 [PROFILE]をクリックします。
3. [APPLICATION PROFILE]ダイアログボックスで、 [CUSTOM TAGS]タブを選択します。
4. [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。
5. 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。

   Fortify Software Security Center 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、Analysisタグはプライマリタグです。

   監査時に、プライマリタグは最初に一覧表示されます。Analysis以外のlist-typeカスタムタグが Fortify Software Security Center 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、これらのタグの1つをAnalysisの代わりにプライマリタグとして選択できます。
6. (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:

注 : 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。

a. [SELECT PRIMARY]をクリックします。
[SELECT PRIMARY TAG]ダイアログボックスが開きます。
b. [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。

注 : 監 査アシスタントを使 用する場 合で、監 査アシスタントのガイダンス情 報を提 供していない場 合は、タグを編 集してその情 報を含 める必 要 があります。監 査アシスタントのガイダンスを提 供する方 法については、1ページの「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" ページ260を参 照してください。

c. [DONE]をクリックします。
7. [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

1ページの「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 " ページ259

"カスタムタグを編 集する" ページ260

"Fortify Scan結 果の監 査 " ページ317

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. Fortifyのヘッダで、 [APPLICATIONS]をクリックします。
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名 をクリックします。
[AUDIT]ページが開きます。
3. アプリケーションバージョンツールバーで、 [PROFILE]をクリックします。
[APPLICATION PROFILE]ウィンドウが開きます。
4. [CUSTOM TAGS]タブをクリックします。
5. [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. [CLOSE]をクリックします。

参照情報

ページ1の「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" ページ263

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。Fortify Software Security Center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、Fortify Software Security Center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. Fortifyのヘッダで、 [ADMINISTRATION]を選択します。
2. [ADMINISTRATION]ページの左ペインから、 [Templates]を選択して、 [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。

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。Fortify Software Security Center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。

アプリケーションバージョンの削除について

Fortify Software Security Centerでアプリケーションを直接削除することはできません。Fortify Software Security Center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。

Fortify Software Security Center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、 [DASHBOARD]ページおよび [Applications]ページの表示から取り除く場合は、バージョンを無効にできます。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" 次のページ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の削 除 " 次 のページ

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 [Applications]ビューで非 表 示 にされます。アプリケーションのすべてのバージョンを削 除 すると、アプリケーションは完 全 に削 除 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. [Applications]ビューで、アプリケーションの行 を展 開 し、無 効 にするバージョンを選 択 します。
   選 択 したバージョンの [AUDIT]ページが開きます。
2. [**PROFILE**]をクリックします。
3. [APPLICATION PROFILE]ダイアログボックスで、 [**APPLICATION SETTINGS**]をクリックします。
4. [**Version Settings**]ペインで、 [**DEACTIVATE**]をクリックします。
   Fortify Software Security Centerに、バージョンの無 効 化 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。
   [**DEACTIVATE**]ボタンが [**ACTIVATE**]ボタンになります。必 要 に応 じて、後 でバージョンを再 度 有 効 にできます。
6. [APPLICATION PROFILE]ダイアログボックスを閉 じます。

参 照 情 報

"アプリケーションバージョンの削 除 " 次 のページ

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 化 され、 [DASHBOARD]ビューまたは [Applications]ビューに一 覧 表 示 されていない場 合 は、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 化 されたアプリケーションバージョンが、アプリケーションの唯 一 存 在 するバージョンだった場 合 は、次 の操 作 を実 行 して、アプリケーションにアクセスして再 度 有 効 にできます。

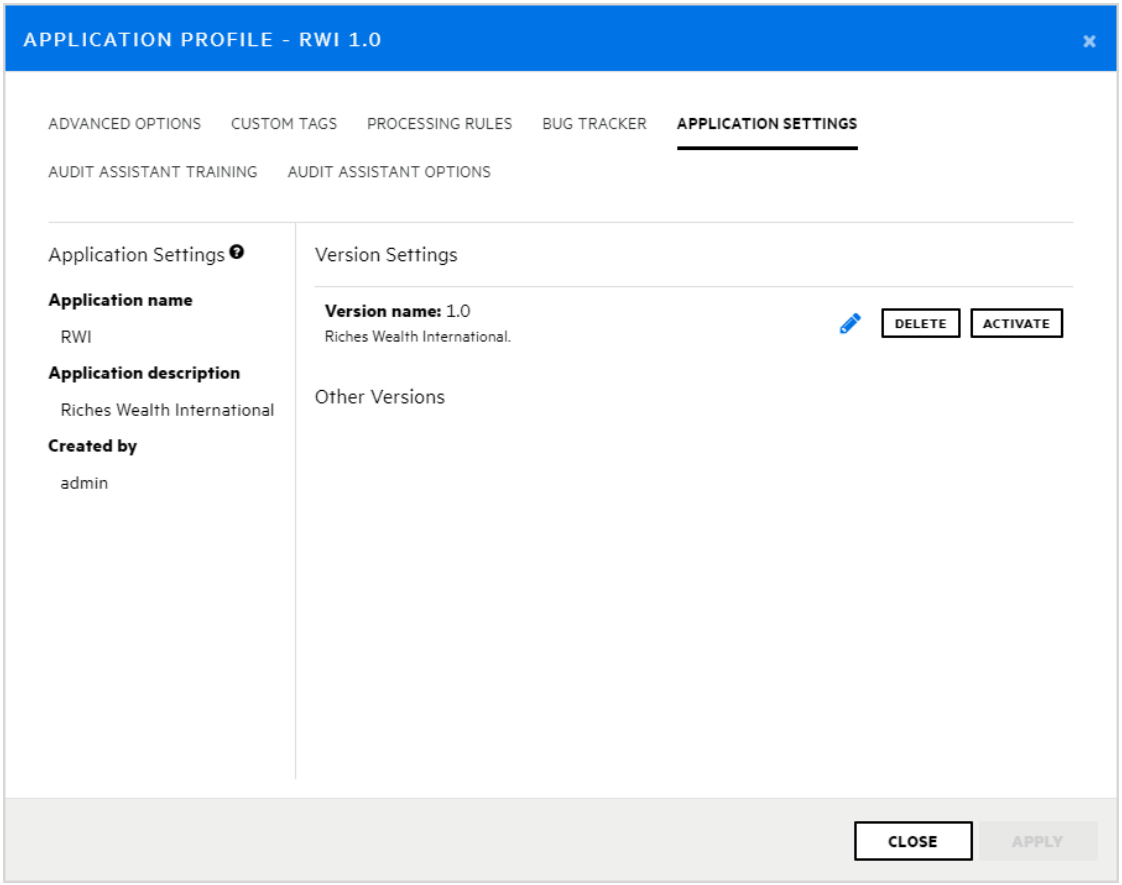
- 無 効 化 されたアプリケーションの新 しいバージョンを作 成 し、次 に説 明 する手 順 に従 います。

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. Fortifyのヘッダで、 [**APPLICATIONS**]をクリックします。
2. [Applications]ビューで、 [**Show inactive versions**]チェックボックスを選 択 します。
3. 表 で、無 効 化 されたアプリケーションバージョン番 号 をクリックします。

選 択したアプリケーションバージョンの [AUDIT]ページが開きます。

4. アプリケーションバージョンツールバーで、 [**PROFILE**]をクリックします。
   [APPLICATION PROFILE - *<application_version>*]ダイアログボックスが開きます。
5. [**APPLICATION SETTINGS**]タブを選 択します。



6. [**ACTIVATE**]をクリックします。
   Fortify Software Security Centerでアクティベーションを確 認 するメッセージが表 示 されます。
7. [**OK**]をクリックします。
8. [**CLOSE**]をクリックします。

アプリケーションバージョンが、Fortify Software Security Centerの [Dashboard]および [Applications]ビューに再 び表 示 されます。

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、Fortify Software Security Centerの [Dashboard]ビューおよび [Applications]ビューの表 示 から取り除く場 合 は、"アプリケーションバージョンの無 効 化 " 前 のページを参 照してください。

重要 アプリケーションのすべてのバージョンを削除すると、Fortify Software Security Centerによってアプリケーションが自動的に削除されます。

Fortify Software Security Centerアプリケーションバージョンを削除するには、次の手順を実行します。

1. [Applications]ビューから、削除するアプリケーションバージョンの名前を選択します。

   Fortify Software Security Centerで、選択したバージョンの [OVERVIEW]ページが開きます。
2. アプリケーションバージョンツールバーで、 [**PROFILE**]をクリックします。
3. [APPLICATION PROFILE]ダイアログボックスで、 [**APPLICATION SETTINGS**]をクリックします。
4. [**Version Settings**]ペインで、 [**Delete**]をクリックします。

   Fortify Software Security Center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。

Fortify Software Security Centerによって、データベースからバージョンが削除されます。

第12章: Webhookについて

Webhookを作成して、Fortify Software Security Center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。

このセクションで説明するトピック:

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Fortify Software Security Center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、任意の種類の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。 • [**Send me everything!**]オプションが選択された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

Fortify Software Security Centerの各役割が実行できるアクションをすべて表示するには、次の手順に従います。

1. Fortifyのヘッダで、 [ADMINISTRATION]を選 択します。
2. 左 ペインで、 [Users]、 [Roles]の順 に選 択します。
   [Roles]テーブルに、ユーザに割り当 てることができるすべての役 割 のリストが表 示 されます。
3. 特 定 の役 割 でユーザが実 行 できるアクションをすべて表 示 するには、その役 割 の行 をクリックします。

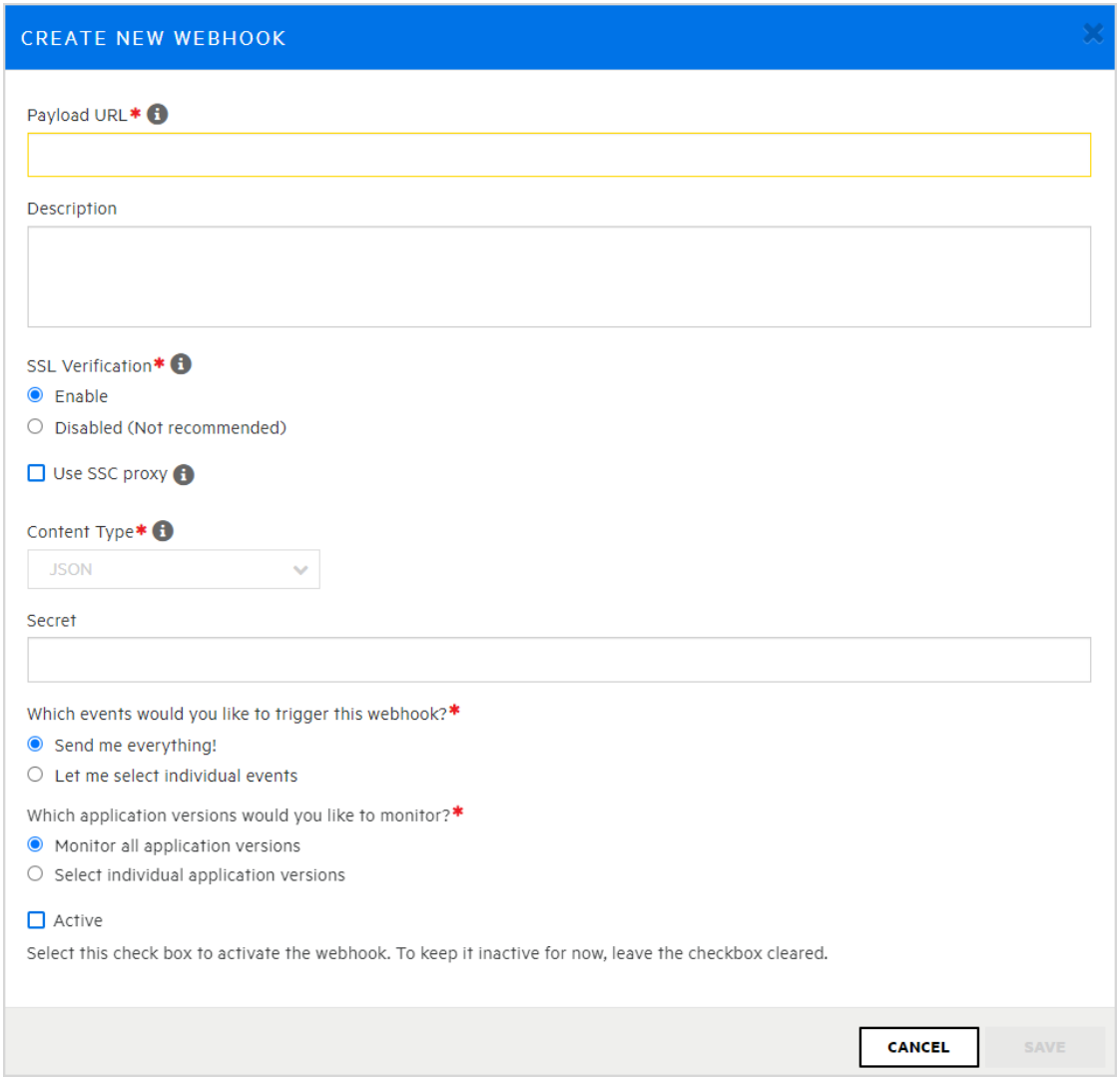
Webhookの作 成

管 理 者 はWebhookを作 成 して、グローバルかアプリケーションバージョン固 有 かに関 係 なくあらゆる種 類 のイベントを監 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。

注 : Webhookを操 作 する許 可 を持 つ役 割 の詳 細 については、"Webhookの許 可 " 前 のページを参 照 してください。

新しいWebhookを作 成 するには、次 の手 順 を実 行 します。

1. Fortify Software Security Center に管 理 者 またはセキュリティリードとしてログイン し、Fortifyヘッダで [ADMINISTRATION]をクリックします。
2. [ADMINISTRATION]ページの左 ペインで、 [Configuration]を選 択 してから、 [Webhooks]を選 択 します。
   [Webhooks]ページには、すでに設 定 されているWebhookが一 覧 表 示 されます。
3. [Webhooks]ページで、 [NEW]をクリックします。



4. [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
Payload URL	このボックスで、要求されたペイロードの送信先URLを指定します。
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。

フィールド	説 明
Use SSC proxy	(オプション) Fortify Software Security Center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Webhookに使 用 できます。Fortify Software Security Center統 合 用 にプロキシを設 定 する方 法 については、"Fortify Software Security Center統 合 のためのプロキシの設 定 " ページ128を参 照 してください。
Content Type	配 信 されるペイロードに使 用 される形 式 を表 示 します。 **注 :** このリリースでサポートされているコンテンツタイプはJSONのみです。
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、プレフィックス`sha256=`を持 つ16進 数 としてエンコードされます。
Which events would you like to trigger this webhook?	次 のいずれかを実 行 します。 • ペイロードに次 のイベントを含 めるには、 [**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)。 ◦ グローバルイベント: • USER_CREATED • USER_DELETED • USER_UPDATED • LOCAL_USER_ACCOUNT_LOCKED • APP_VERSION_CREATED • APP_VERSION_DELETED • REPORT_GENERATION_COMPLETE

フィールド	説明
	• REPORT_GENERATION_REQUESTED ◦ アプリケーションバージョンイベント: • ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS • ANALYSIS_RESULT_UPLOAD_FAILURE • ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL • ANALYSIS_RESULT_INDEXING_COMPLETED • ANALYSIS_RESULT_UPLOAD_APPROVED • APP_VERSION_UPDATED • イベントの注目しているサブセットをペイロードに含めるには、 [Let me select individual events]を選択し、 [Global Events]リストや [Application version events]リスト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。
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、次の手順を実行します。 i. [Select Individual Application Versions]オプションを選択します。 ii. [ADD]をクリックします。 iii. [SELECT APPLICATION VERSION]ダイアログボックスの [APPLICATION]リストから、監視するアプリケーションを選択します。 iv. 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

フィールド	説明
	す。 v. [DONE]をクリックします。 vi. 別のアプリケーションバージョン(複数の場合あり)を追加するには、これらの手順を繰り返します。
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。

5. Webhookの設定が完了したら、[SAVE]をクリックします。

参照情報

"Webhookペイロードの表示" 次のページ

"Webhookの削除" ページ278

Webhookを編集する

Webhookを編集するには:

1. Fortify Software Security Centerに管理者またはセキュリティリードとしてログインし、Fortifyヘッダで[ADMINISTRATION]をクリックします。

   注: 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。

2. [ADMINISTRATION]ページの左ペインで、[Configuration]を選択してから、[Webhooks]を選択します。
   [Webhooks]ページには、すでに設定されているWebhookが一覧表示されます。
3. 行を選択すると、編集するWebhookの詳細が表示されます。
4. "Webhookの作成" ページ270で説明されているフィールドの値を変更します。
5. (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。
6. [SAVE]をクリックします。

参照情報

"Webhookペイロードの表示" 次のページ

"Webhookの作成" ページ270

Webhookペイロードの表示

管理者の場合は、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. Fortify Software Security Center に管理者またはセキュリティリードとしてログインし、Fortifyヘッダで [ADMINISTRATION]をクリックします。
2. [ADMINISTRATION]ページの左ペインで、 [Configuration]を選択してから、 [Webhooks]を選択します。

   Webhookテーブルには、次のように既存のすべてのWebhookのリストと、それぞれのステータスが表示されます。

   ✓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。

   注 : リストに表示されたWebhookの [Status]フィールド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、 [Recent deliveries]テーブルの上にある [Active]チェックボックスが選択されていることを確認します。

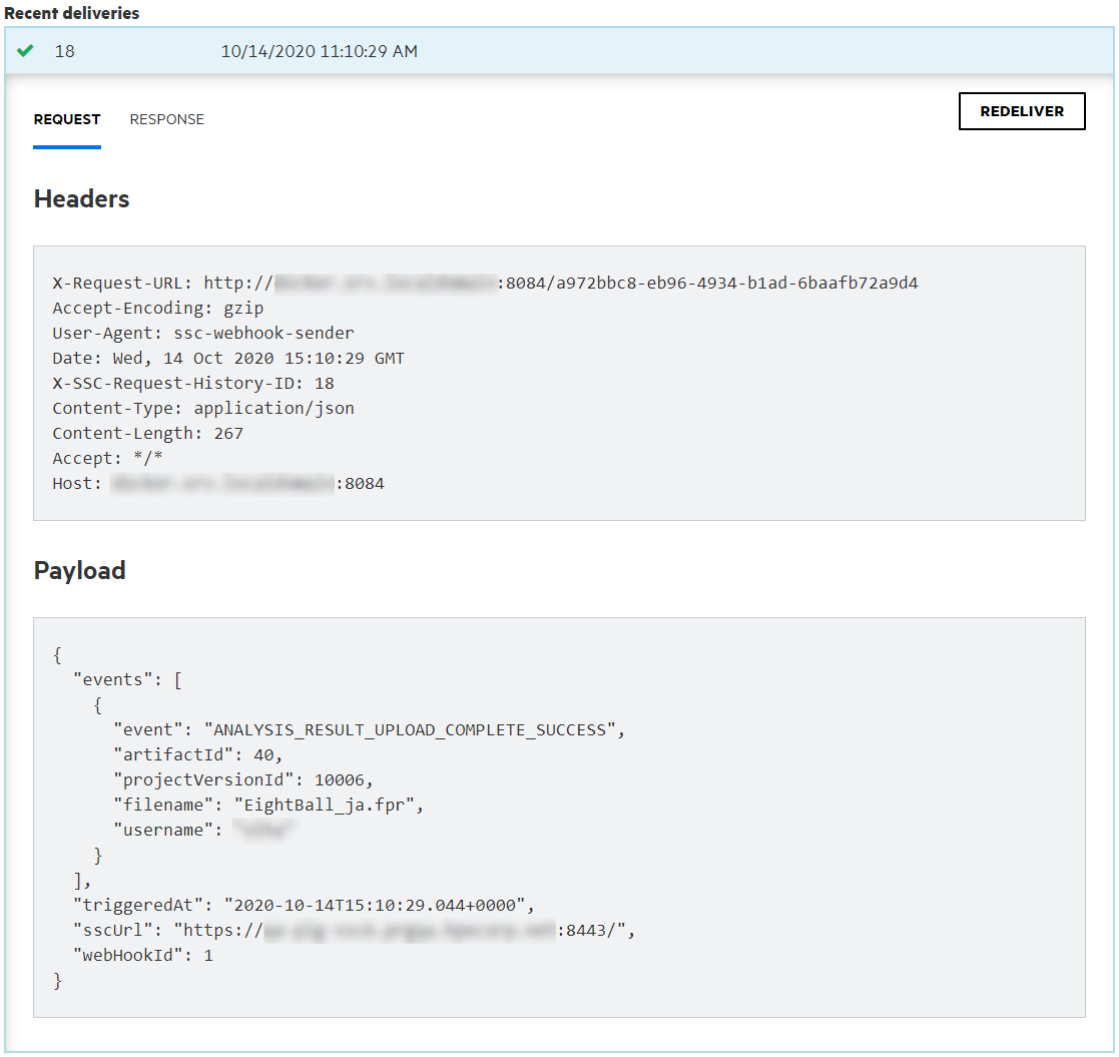
3. Webhookテーブルで、Webhookを選択してその詳細を展開し、最近配信されたペイロード(最大10個)を調査します(可能な場合)。

   Recent deliveries

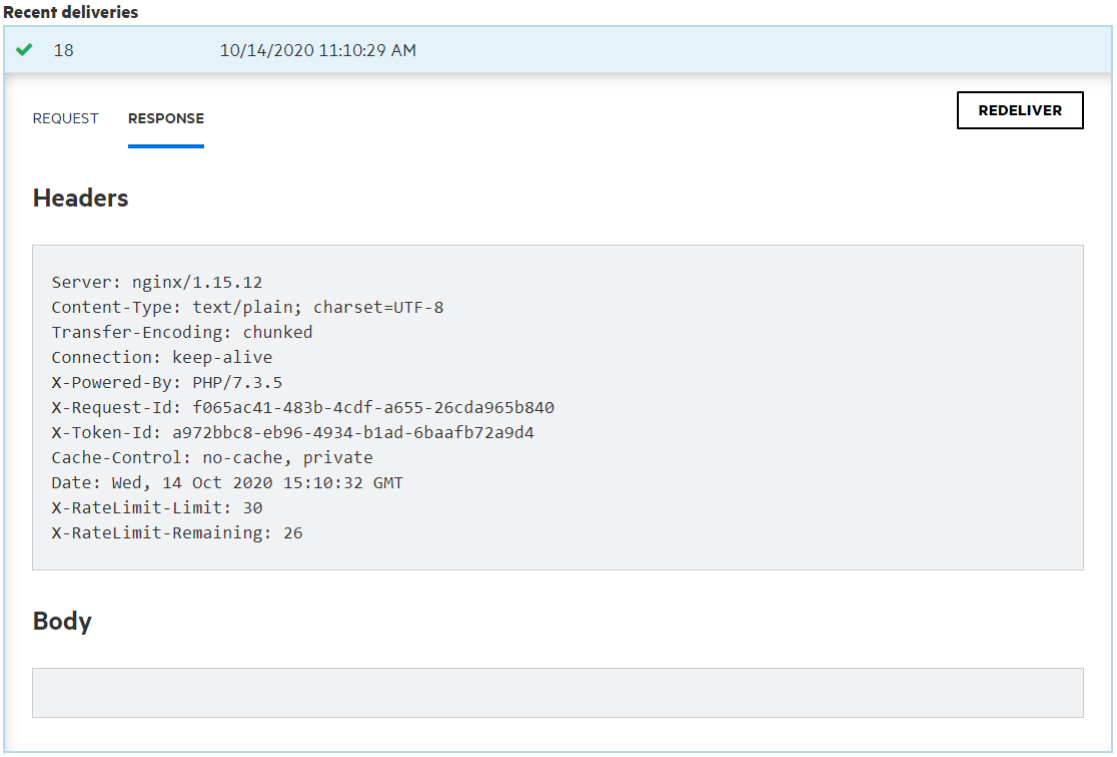
✔ 22	10/14/2020 11:29:20 AM
✔ 21	10/14/2020 11:23:47 AM
✔ 20	10/14/2020 11:23:00 AM
✔ 19	10/14/2020 11:10:29 AM
✔ 17	10/14/2020 11:09:59 AM
✔ 15	10/14/2020 11:08:40 AM
✔ 14	10/14/2020 11:08:20 AM
✔ 13	10/14/2020 10:43:17 AM
✔ 12	10/14/2020 10:18:14 AM
✔ 8	10/14/2020 10:00:39 AM

   [Recent deliveries]には、最近配信されたペイロード(最大10個)のリストが表示されます。

4. 調 査 するペイロード の行 をクリックします。



5. 応 答 の本 文 またはヘッダの詳 細 を表 示 するには、 [RESPONSE]タブを選 択 します。



配信されたペイロードのコンテンツの詳細については、ページ1の「"Webhookのペイロード" ページ412を参照してください。

参照情報

"Webhookの削除" 次のページ

"Webhookの作成" ページ270

"Webhookを編集する" ページ274

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. Fortify Software Security Center に管理者またはセキュリティリードとしてログインし、Fortifyヘッダで [**ADMINISTRATION**]をクリックします。

   注 : 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。

2. [ADMINISTRATION]ページの左ペインで、 [**Configuration**]を選択してから、[**Webhooks**]を選択します。

［Webhooks］ページには、設定されているすべてのWebhookが一覧表示されます。

3. ペイロードを再配信するWebhookの行を選択します。
4. ［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" ページ270

"Webhookを編集する" ページ274

"Webhookペイロードの表示" ページ275

Webhookの削除

Webhookを削除するには、次の手順を実行します。

1. Fortify Software Security Center に管理者またはセキュリティリードとしてログインし、Fortifyヘッダで［ADMINISTRATION］をクリックします。
2. 左ペインで、［Configuration］を選択してから、［Webhook］を選択します。
   ［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。
3. 表で、削除するWebhookのチェックボックスをオンにして、［DELETE］をクリックします。

参照情報

"Webhookの作成" ページ270

"Webhookを編集する" ページ274

第13章: 変数、パフォーマンスインジケータ、およびアラート

Fortify Software Security Center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。Fortify Software Security Center変数は、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です。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。Fortify Software Security Center変数とパフォーマンスインジケータでは、カスタマイズされたメトリックを作成するために使用できる構成ブロックが提供されます。これらの構成ブロックは、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。

変数の値を使用してアラートをトリガできます。これにより、Fortify Software Security Centerでは、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できます。Fortify Software Security Center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。

このセクションで説明するトピック:

変数の使用

セキュリティリードまたは管理者の場合は、アプリケーションの変数を定義できます。次のトピックでは、Fortify Software Security Center変数の構文と検索文字列に関する情報を示し、変数を作成する方法について説明します。

変 数 の作 成

Fortify Software Security Center変 数 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 としてログインし、 [ADMINISTRATION]をクリックします。

   注 : 開 発 者 アカウントを持 つユーザはFortify Software Security Center変 数 を作 成 できません。

2. 左 側 のペインの [Metrics & Tracking]で、 [Variables]を選 択 します。
3. [Variables]ツールバーで [NEW]をクリックします。
   [CREATE NEW VARIABLE]ダイアログボックスが開きます。
4. 次 の表 で説 明 する情 報 を入 力 します。

フィールド	説 明
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。
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Fortify Software Security Center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、 [Search String]ボックスの下 にある [Syntax Guide]リンクを選 択 するか、"変 数 の構 文 " 下 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。 [Folder]リストには、使 用 可 能 なすべての問 題 テンプレートに関 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. Fortify Software Security Center変 数 を検 証 した後 、 [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。

変 数 の構 文

Fortify Software Security Center変 数 の形 式 は`modifier:searchstring`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、Fortify Software Security Center関 係 演 算 子 を示 します。

関係演算子	説明	例
数値範囲	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 に隣 接 する数 値 を含 めて指 定 するには、左 括 弧 または右 括 弧 ("[ ]")を使 用 します。 範 囲 から隣 接 する数 値 を除 外 (より大 きいまたは小 さい)に指 定 するには、開 き括 弧 と閉 じ括 弧 ("( )")を使 用 します。	`(2,4]` 2より大 きく、4以 下 の範 囲 を示 します。
! (等しくない)	感 嘆 符 (!)が付 いた修 飾 子 を削 除 します。	`!file:Main.java` `Main.java`.に存 在 しないすべての問 題 を返 します。

パフォーマンスインジケータ

Fortify Software Security Center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。このセクションでは、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。

Fortify Software Security Centerパフォーマンスインジケータの式 の一 般 的 な形 式 は次 のとおりです。

```
Variable[operator]Variable
```

ここで`operator`は、標 準 的 な数 学 的 演 算 子 (+、 -、 */)です。

パフォーマンスインジケータの作 成 方 法 については、"パフォーマンスインジケータの作 成 " 下 を参 照 してください。

パフォーマンスインジケータの作 成

Fortify Software Security Center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 としてFortify Software Security Centerにログインし、[ADMINISTRATION]タブをクリックします。

注 : 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、Fortify Software Security Centerパフォーマンスインジケータを作 成 できません。

2. 左 側 のペインの 『Metrics & Tracking』で、 『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。
   『CREATE NEW PERFORMANCE INDICATOR』ダイアログボックスが開きます。
4. 次 の表 で説 明 する情 報 を入 力 します。

フィールド	説 明
Name	パフォーマンスインジケータの名 前 を入 力 します。
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Fortify Software Security Center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式 の形 式 は次 のとおりです。 `Variable[operator]Variable` ここで、オペレータは標 準 的 な数 学 オペレータ(+、 -、 *、 /)です。
Return Type	このリストから、返 す値 の種 類 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 して正 常 に検 証 したら、 『SAVE』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。

アラート定 義

アラート定 義 には、ダッシュボードの 『Todo List』ウィンドウでFortify Software Security Center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。

注 : この機 能 は、Fortify Software Security Center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。

次 に

"アラートの作 成" 次 のページ

参 照 情 報

"電 子 メールアラート通 知 設 定 の設 定 " ページ99
"電 子 メールアラートの受 信 を有 効 化 および無 効 化 する" ページ101
"アラートの削 除 " ページ286

アラートの作 成

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。

Fortify Software Security Centerアラートを作 成 するには、次 の手 順 を実 行 します。

1. Fortifyのヘッダで、 [ADMINISTRATION]をクリックします。
2. 左 側 のペインで、 [Templates]をクリックし、 [Alerts]を選 択 します。
   [Alerts]ページには、現 在 までに定 義 されているアラートが表 示 されます。
3. [Alerts]ツールバーで [NEW]をクリックします。
   [CREATE NEW ALERT]ダイアログボックスが開きます。
4. [Name]ボックスに、アラートの名 前 を入 力 します。
5. (オプション) [Description]ボックスに、アラートの内 容 を説 明 するテキストを入 力 します。
6. アラートを有 効 にせずに作 成 するには、 [Enable Alert]チェックボックスをオフにします。このアラートを有 効 にするには、チェックボックスをオンのままにします。
7. [Type]の横 で、作 成 するアラートのタイプを選 択 します。

   注 : 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。

8. [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、 [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、 [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Fortify Software Security Centerユーザに送 信 するには、 [All system users]を選 択 します。

   注 : 選 択 したオプションに関 係 なく、通 知 を受 信 します。

9. 次 のいずれかの表 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。

パフォーマンスインジケータ
a. [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。 b. オペレータのリストからオペレータを選 択 します。 c. 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 [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、後続のスキャンで多くの新しい重大な問題が発見された場合でも1回だけトリガされます。

d. 新しいアーティファクトのアップロードごとにFortify Software Security Centerでアラートをリセットするには、 [Reset after triggering]チェックボックスをオンにします。

変数

a. [Alert when]リストから、変数を選択します。
b. オペレータのリストから、適切なオペレータを選択します。
c. 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、後続のスキャンで新しい問題が発見された場合でも1回だけトリガされます。

d. 新しいアーティファクトのアップロードごとにFortify Software Security Centerでアラートをリセットするには、 [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

- [Alert when]リストから、アラートをトリガするFortify Software Security Centerシステムイベントを選択します。

スケジュールされたアラート(管理者のみ)

[Alert when]の下で、次の手順を実行します。

a. カレンダコントロールを使用して、Fortify Software Security Centerからアラートを送信する日付を指定します。
b. 右側の2つのボックスに、アラートを送信する時間と分(hh:mm)を入力します。
c. [AM]と [PM]を切り替え、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。
d. 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。

e. 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。

10. パフォーマンスインジケータアラートまたは変 数 アラートを作 成 する場 合 は、次 の手 順 を実 行 して、アラートを使 用 するアプリケーションバージョンを指 定 します。
    a. [ADD]をクリックします。
       [SELECT APPLICATION VERSION]ダイアログボックスが開きます。
    b. [APPLICATION]リストで、アラートを使 用 するアプリケーションを選 択 します。
       [VERSIONS]ペイン(中 央)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。
    c. [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。
    d. 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。それ以 外 の場 合 は、[VERSIONS]リストで、アラートを使 用 するバージョンのチェックボックスをオンにします。
       右 側 のペインには、新 しいアラートを受 信 するために選 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。
    e. 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。
    f. [DONE]をクリックします。
11. [Message]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。

    注 : 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。

12. [SAVE]をクリックします。
    [Version assignees]を受 信 者 として選 択 した場 合 、Fortify Software Security Centerに次 のアラートが表 示 されます。
    「Are you sure you want to notify all application versions users? This could potentially notify a large amount of users every time the alert triggers.」
13. 続 行 するには、[OK]をクリックします。それ以 外 の場 合 は、[CANCEL]をクリックし、受 信 者 として[Me Only]を選 択 します。

Fortify Software Security Centerに、新 しいアラートの詳 細 が表 示 されます。

参 照 情 報

"アラートの削 除 " 次 のページ

"電 子 メールアラート通 知 設 定 の設 定 " ページ99

"電 子 メールアラートの受 信 を有 効 化 および無 効 化 する" ページ101

"アラート定 義 " ページ282

アラートを編 集 する

Fortify Software Security Center アラートを編 集 するには:

1. Fortify Software Security Centerに管 理 者 としてログインし、Fortifyのヘッダで [ADMINISTRATION]をクリックします。
2. 左 側 のペインで、 [Templates]をクリックし、 [Alerts]を選 択します。
   [Alerts]ページには、定 義したアラートすべてが表 示されます。
3. [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。
4. アラート設 定 の右 下 で、 [EDIT]をクリックします。
5. 必 要 な変 更 を行い、 [SAVE]をクリックします。

アラートの削 除

Fortify Software Security Centerアラートを削 除 するには、次 の手 順 を実 行します。

1. 管 理 者 としてFortify Software Security Centerにログインし、 [ADMINISTRATION]タブをクリックします。
2. 左 側 のペインで、 [Templates]を選 択し、 [Alerts]を選 択します。
   [Alerts]ページには、定 義したアラートすべてが表 示されます。
3. [Alerts]テーブルで、削 除 するアラートの左 側 にあるチェックボックスをオンにします。
4. [Alerts]ツールバーで [DELETE]をクリックします。
   Fortify Software Security Centerに、削 除 の続 行を確 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。

参 照 情 報

"電 子 メールアラート通 知 設 定 の設 定" ページ99

"アラート定 義" ページ282

"アラートの作 成" ページ283

アラートの表 示とマーク

Fortify Software Security Centerでは、ユーザまたは別 のユーザが受 信 するように設 定 した未 読 アラートにフラグが設 定 されます。これらのフラグは、ダッシュボードの右 側 と、各 ビューのFortifyヘッダの右 側 にある折 りたたみ可 能 なペインに表 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。

- Fortifyヘッダの右端で、未読アラートの数を示す赤い円をクリックします。
- ダッシュボードの折りたたみ可能なペインの [Todo List]セクションで、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。

- [ALERTS]ウィンドウでアラート名の左側にあるチェックボックスを選択し、[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。

- [ALERTS]ウィンドウでアラート名の左側にあるチェックボックスを選択し、[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が付けられている場合は、既読アラートのフラグが表示されなくなります。これらのアラートを表示するには、ダッシュボードに移動し、折りたたみ可能なペインの [Todo List]セクションで [Show all alert notifications]をクリックします。

第 14章 : スキャンアーティファクト の操 作 について

次 のセクションでは、スキャンアーティファクト の操 作 に関 するさまざまな側 面 について説 明します。

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Fortify Software Security Center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 " ページ332を参 照 してください。

注 : Fortify Software Security Centerがデータベースにデータを挿 入 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、Fortify Software Security Centerの [AUDIT]ページに表 示 されるデータにのみ影 響 します。

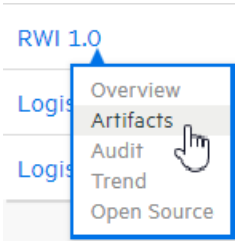
重 要 Fortify Software Security Centerにアップロード するファイルは2GBを超 えない ようにしてください。

重 要 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 " ページ164を 参 照 してください。

サード パーティのデータを含 む生 のスキャンファイルは、`scan.info`メタデータファイルと ー 緒 にZIPファイルにパックする必 要 があります。`scan.info`プロパティファイルには、 結 果 を生 成 したスキャンエンジンを識 別 する`engineType`プロパティの値 を指 定 する 必 要 があります。このエンジンタイプは、設 定 されたパーサプラグインによって登 録 さ れたエンジンタイプと一 致 する必 要 があります。また`scan.info`ファイルも、ISO-8601 形 式 の`scanDate`プロパティ値 を指 定 できます。https://github.com/fortify/sample-parserから`scan.info`コンテンツを取 得 できます。

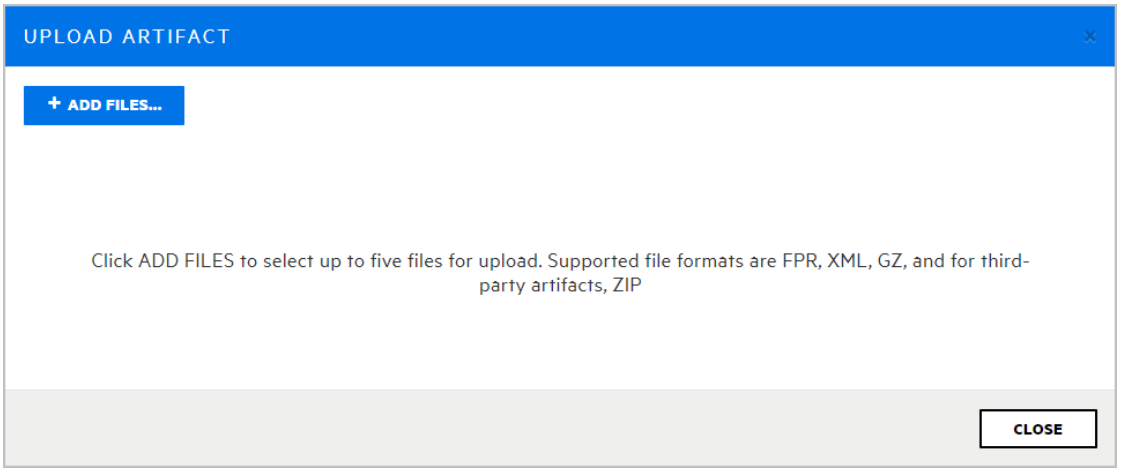
スキャンアーティファクト をFortify Software Security Centerデータベースにアップロード する には、次 の手 順 に従 います。

1. [Dashboard]または [Applications]ビューで、アーティファクト をアップロード するアプリ ケーションバージョンにカーソルを移 動 し、ショートカット メニューから [**Artifacts**]を選 択 します。



2. [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。

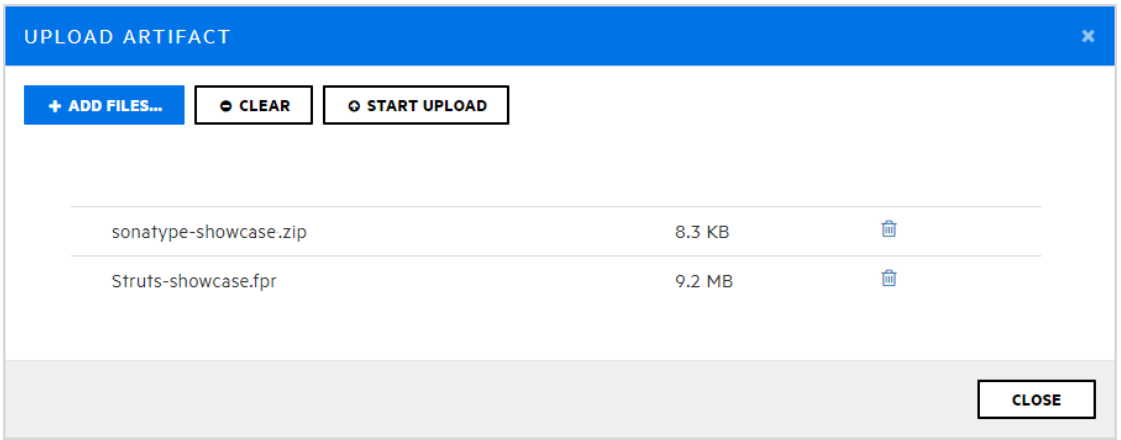
3. [ARTIFACT]をクリックします。



[UPLOAD ARTIFACT]ダイアログが開きます。

4. [+ 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に移 動して選 択します。

アーティファクト のアップロード でサポートされているフォーマット は、FPR、XML、GZ、およびZIP(サード パーティのアーティファクト 用)です。



[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。パーサプラグインが設定されている場合は、[Select type]リストが表示されます。

重要 [Select type]リストは使用されなくなりました。このリストからタイプを選択しないでください。

6. リストからファイルを削除するには、そのファイルのごみ箱アイコ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。

注 : 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、そのルールを承認してからFortify Software Security Centerで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" ページ293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。

[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" ページ292

"Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164

"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" ページ251

"アプリケーション識別子を使用したFPRファイルのアップロード" ページ391

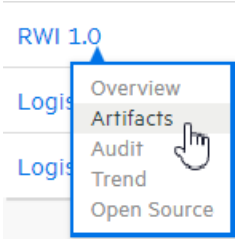
"アプリケーション名とバージョンを使用したFPRファイルのアップロード" ページ392

スキャンアーティファクトの詳細の表示

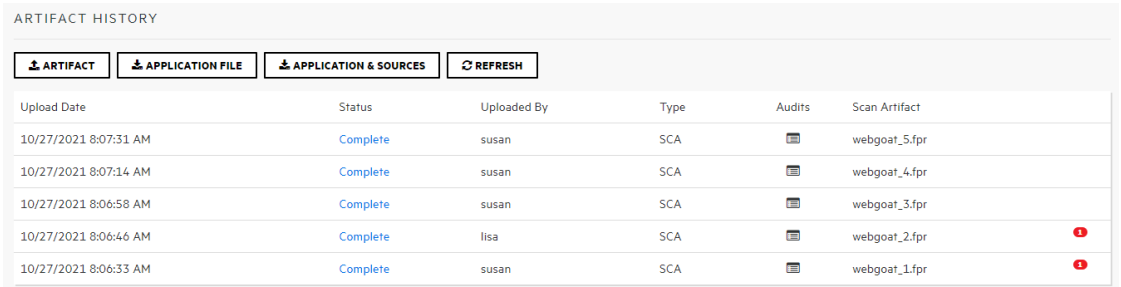
次の手順では、アップロードされたスキャンアーティファクトについて利用可能な詳細について説明します。(スキャンアーティファクトのアップロード方法については、"スキャンアーティファクトのアップロード" ページ288を参照してください)。

スキャンアーティファクトをFortify Software Security Center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。

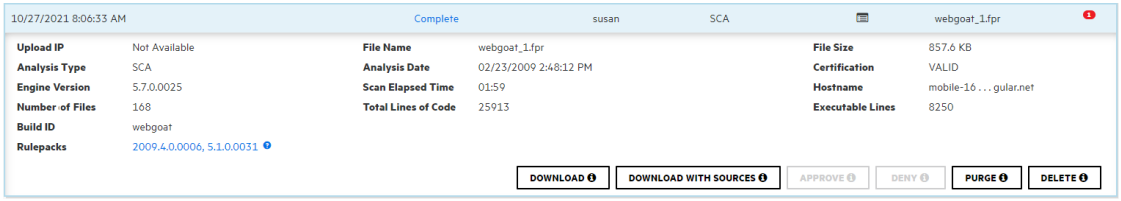
1. [Dashboard]または [Applications]ビューで、アーティファクトの詳細を表示するするアプリケーションバージョンにカーソルを移動し、ショートカットメニューから [**Artifacts**]を選択します。



[**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。



2. 表示されているアーティファクトの1つの詳細を表示するには、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。

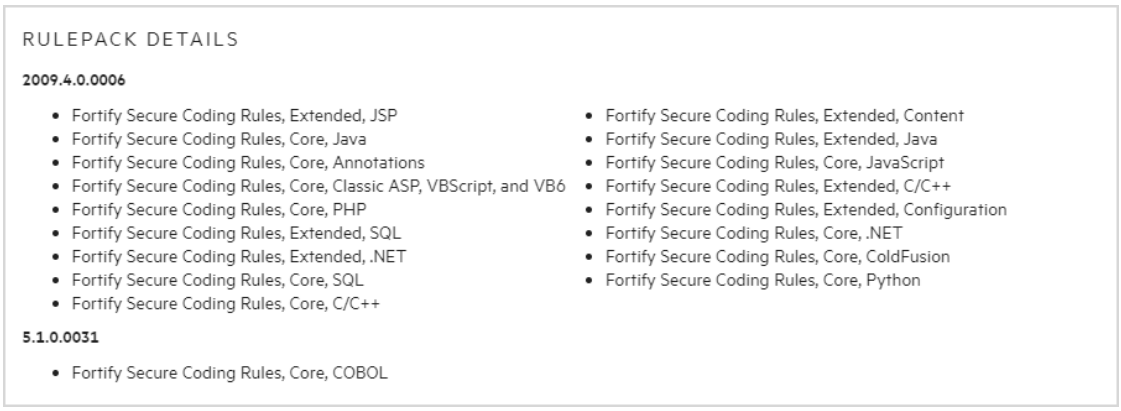
3. スキャンの処理エラーに関連するコードの行を表示するには、円の付いた番号 (1) をクリックします。

[SCAN WARNING]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。

このフィールドには、スキャンの生成に使用されるRulepackのバージョンが表示されます。

4. スキャン中に適用されるコーディングルールの、Rulepackのバージョン別にグループ

化されたリストを表 示するには、 [Rulepacks]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

注 : 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、そのルールを承 認してからFortify Software Security Centerで処 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" 次のページを参 照してください。

参照情報

"スキャンアーティファクトをダウンロードする" 下

"スキャンアーティファクトのパージ" ページ300

"Sonatype結 果を表 示するためのFortify Software Security Centerの準 備" ページ164

"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" ページ251

"アプリケーション識 別子を使 用したFPRファイルのアップロード" ページ391

"アプリケーション名 とバージョンを使 用したFPRファイルのアップロード" ページ392

スキャンアーティファクトをダウンロードする

[ARTIFACT HISTORY]ページから、アプリケーションバージョンのマージされた最 新のFPRファイルをダウンロードしたり、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できます。

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後 の最 新のスキャン結 果をFPR形 式でダウンロードするには:

1. Fortifyのヘッダで、 [APPLICATIONS]をクリックします。
2. [アプリケーション]ビューで、アプリケーションの行を展 開し、目 的のバージョンを選 択します。
3. アプリケーションバージョンツールバーで、 [ARTIFACTS]をクリックします。

[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。
   - アプリケーションバージョンのマージされた最新のスキャン結果をダウンロードするには、[ARTIFACT HISTORY]テーブルの上部で[APPLICATION FILE]をクリックします。
     

   - マージされた現在のアプリケーションスキャン結果をFPR形式でソースと共にダウンロードするには、[ARTIFACT HISTORY]テーブルの上部で[APPLICATION & SOURCES]をクリックします。
     

5. スキャン結果をFortify Audit Workbenchで開くには、[Downloads]フォルダで、ダウンロードしたFPRファイルをダブルクリックします。

個々のスキャン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. Fortifyのヘッダで、[APPLICATIONS]をクリックします。
2. [アプリケーション]ビューで、アプリケーションの行を展開し、目的のバージョンを選択します。
3. アプリケーションバージョンツールバーで、[ARTIFACTS]をクリックします。
   [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。

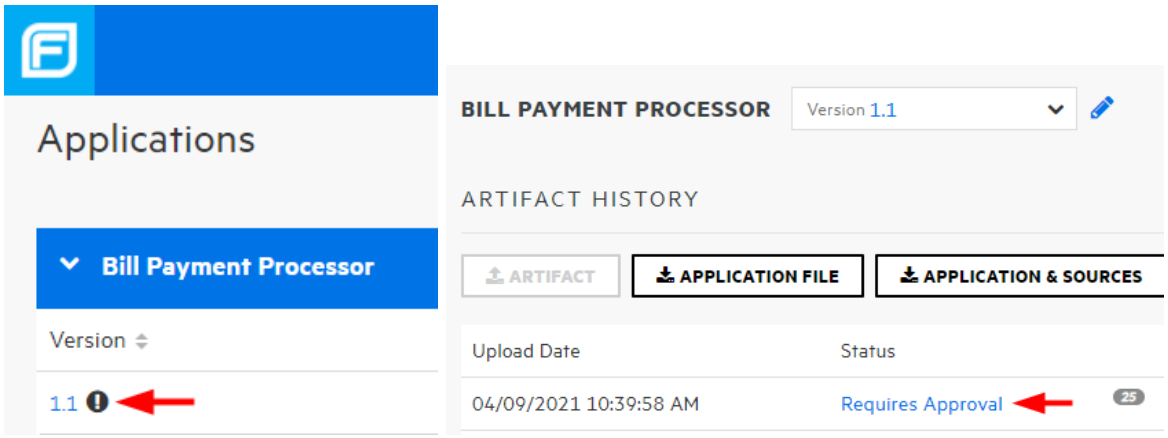
参照情報

"スキャンアーティファクトのアップロード" ページ288

"アーティファクトの削除" ページ301

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用に設定された処理ルールと、スキャンの処理で使用した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な場合があります。("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" ページ251を参照してください)。分析結果に承認が必要な場合は、[アプリケーション]ビューのバージョン名の横にあるアラートアイコン()と、[ARTIFACT HISTORY]テーブルの[ステータス]列の[Requires Approval]の値で示されます。



注 : 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 Fortify Software Security Center で処理したくない場合は、"承認処理を拒否する" 下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 Fortify Software Security Center がアーティファクトを処理できるようにするには:

1. [アプリケーション]ビューで、アプリケーション行を展開し、カーソルをバージョン番号に移動して、ショートカットメニューから [**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。
2. [**ステータス**]列の値が [**Requires Approval**]の行を展開します。
3. 展開したセクションの下で、 [**APPROVE**]をクリックします。
   [APPROVE UPLOAD OF ANALYSIS RESULTS]ダイアログボックスが開きます。 [**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。
4. [**Approval 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。
5. [**APPROVE**]をクリックします。

Fortify Software Security Center 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

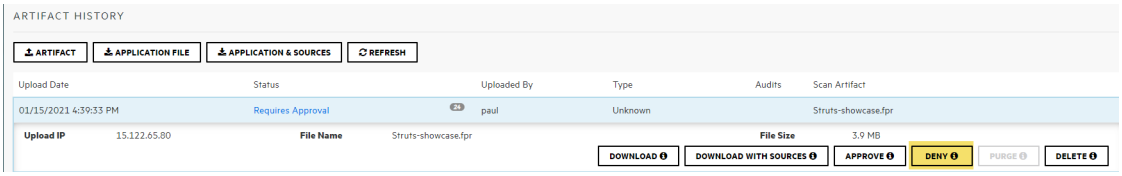
アーティファクトが誤ってアップロードされた場合、または何らかの理由でアーティファクトを Fortify Software Security Center で処理したくない場合は、そのアーティファクトを削除するか、あるいはアーティファクトアップロードの記録を保持したい場合は、承認を拒否できます。

アーティファクトの承認を拒否するには:

1. [アプリケーション]ビューで、アプリケーション行を展開し、カーソルをバージョン番号に移動して、ショートカットメニューから [**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。

2. 承 認 が必 要 で、Fortify Software Security Center で処 理したくないアーティファクトの行 を展 開します。



3. 展 開された詳 細 セクションの下 部 で、 [DENY]をクリックします。

[DENY UPLOAD OF ANALYSIS RESULTS]ダイアログボックスが開きます。 [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 に一 覧 表 示 されます。

4. [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。
5. [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。

高レベルサマリ結 果 の表 示

Fortify Software Security Centerには、Fortify Software Security Centerダッシュボードまたは [Overview]ページから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 するための方 法 がいくつか用 意 されています。

[Issue Stats]ページにサマリメトリックを表 示 する

[Issue Stats]ページから(個 別 にまたはまとめて)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、次 の手 順 に従 います。

- Fortifyのヘッダで、 [DASHBOARD]を選 択します。

[Issue Stats]ページ(Fortify Software Security Centerのデフォルトの [Dashboard]ビュー)の次 の3つのポートレットには、アクセス権 を持 つ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。

- [Issues Remediated]ポートレットには、現 在 までに修 正 された問 題 の合 計 数 、確 認 にかかった平 均 日 数 、および修 正 に必 要 な平 均 日 数 が表 示 されます。
- [Issues Pending Review]ポートレットには、開 いている問 題 の合 計 数 と確 認 された問 題 の数 が表 示 されます。
- [Application Versions]ポートレットには、スキャンされたファイルの数 に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コードの行 数 が表 示 されます。

[Issue Stats]ページのテーブルには、アクセス権 を持 っている各 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。テーブルのリストに表 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、Fortify Software Security Centerからアプリケーションバージョンの［AUDIT］ページに直 接 移 動します。

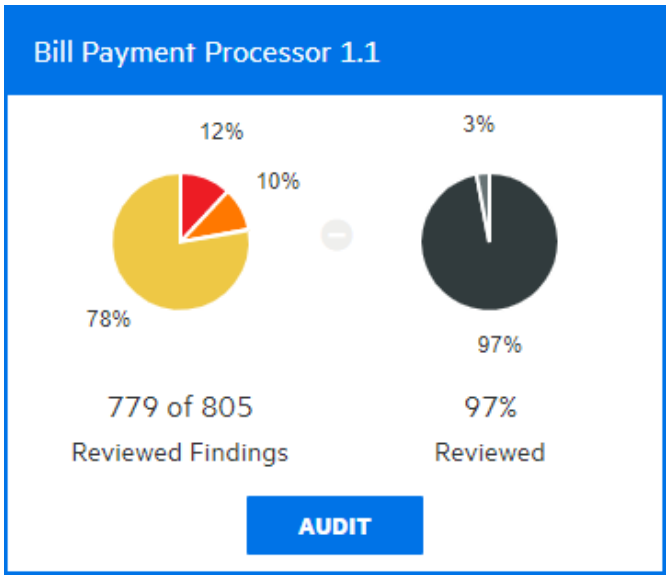
ポートレットとテーブルを同 時 に使 用 すると、どのくらい迅 速 に問 題 が確 認 および修 正 されるのかを確 認 できます。

［CHART］ページにサマリメトリックを表 示 する

［CHART］ページから、個 々 のアプリケーションバージョンのサマリメトリックをグラフィカルに表 示 できます。

［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、次 の手 順 に従 います。

1. ダッシュボードのツールバーで、［**CHART**］をクリックします。
   Fortify Software Security Center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、カーソルをアプリケーションバージョンの色 付 きバーに移 動します。

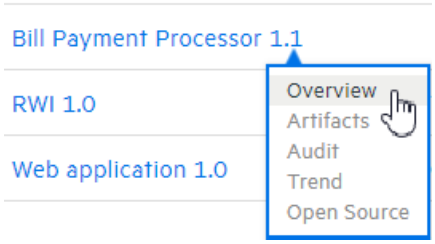


Fortify Software Security Centerに、バージョンのサマリ結 果 が表 示 されます。この例 では、左 側 の円 グラフに、このアプリケーションバージョンについて現 在 までに監 査 された結 果 の97%(779/805)のセキュリティ評 価 が表 示 されています。右 側 のグラフには、監 査 された結 果 の割 合 (97)と、まだ監 査 されていない結 果 の割 合 (3)が表 示 されています。

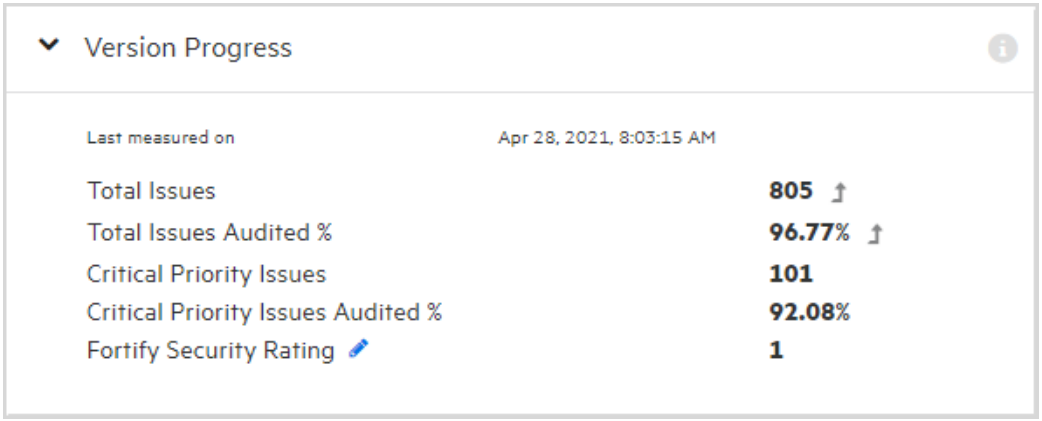
注 : アプリケーションバージョンの［AUDIT］ページに移 動 するには、［**AUDIT**］をクリックします。

[Overview]ページにサマリメトリックを表示する

[Overview]ページから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は、次の手順に従います。



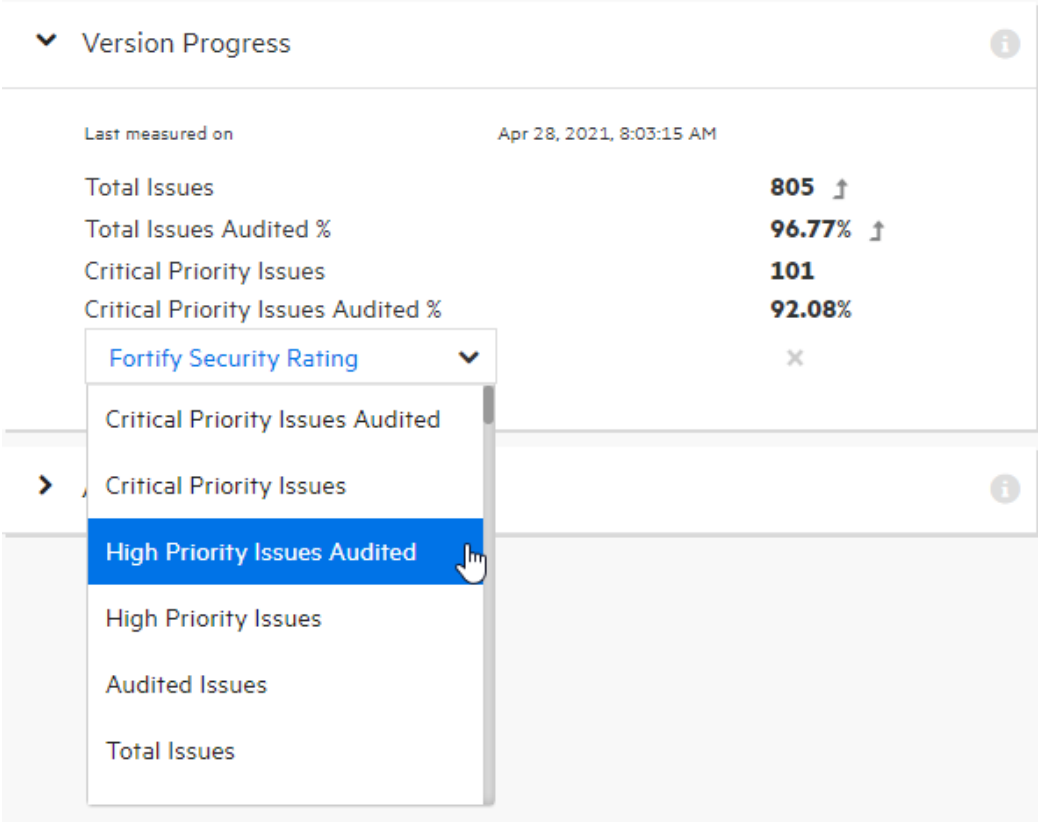
1. Fortifyのダッシュボードで、目的のバージョンのリンク上にカーソルを合わせ、ショートカットメニューから [**Overview**]を選択します。
2. [**Overview**]ページで、右側のペインが折りたたまれている場合は拡大します。



[**Version Progress**]セクションには、傾向矢印を使用したサマリ情報が表示されます。

3. Fortify Security Rating以外のメトリックを表示するには、編集アイコン( )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。



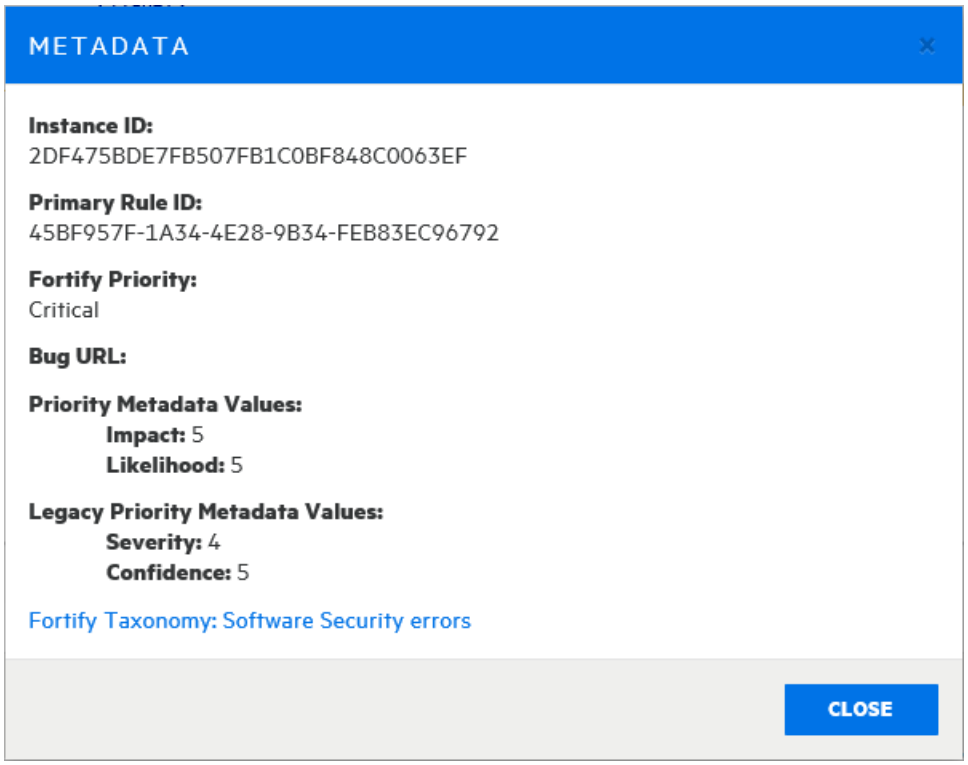
参照情報

"Fortify Scan結 果の監 査" ページ317

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 [AUDIT]ページに移 動します。
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. 問 題の詳 細セクションの左 下で、 [METADATA]をクリックします。



［METADATA］ボックスには、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)、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表示されます。

注 : 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Fortify Software Security Center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**］リンクを選択します。

外部リストへのスキャン結果のマッピング

Fortifyは、外部メタデータドキュメントをRulepackと一緒に配布します。このドキュメントには、Fortifyカテゴリから代替カテゴリ(OWASP 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。

注 : カスタムマッピングの作成方法の詳細については、『Micro Focus Fortify Static Code Analyzerの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Fortify Software Security Center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Fortify Software Security Centerにインポートするには、次の手順に従います。

1. 管理者としてログインし、Fortifyヘッダの [ADMINISTRATION]タブをクリックします。
2. 左ペインの [Metrics &Tracking]で、 [Rulepacks]を選択します。
3. [Rulepacks]ページの右上隅で、 [IMPORT]をクリックします。
   「IMPORT RULEPACK]ダイアログボックスが開きます。
4. [+ ADD FILES]をクリックします。
5. ドキュメントに移動して選択し、 [START UPLOAD]をクリックします。

Fortify Software Security Centerと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Fortify Software Security Centerにインポートし、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。

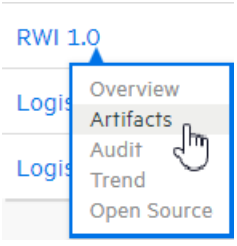
スキャンアーティファクトのパージ

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、Fortify Software Security Center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Fortifyのカスタマサポート (https://www.microfocus.com/support)に相談して、アーティファクトパージが影響を受けるかどうかを判断してください。

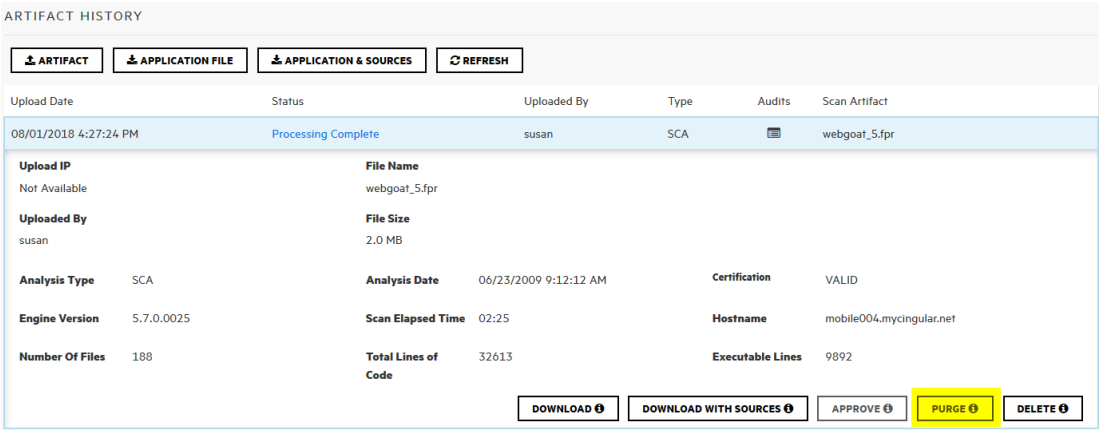
Fortify Software Security Centerデータベースからスキャンアーティファクトをパージするには、次の手順に従います。



1. [DASHBOARD]から、パージするアーティファクトのあるアプリケーションバージョンにカーソルを移動し、ショートカットメニューから [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。

2. 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、選択したアーティファクトの詳細が表示されます。



3. アーティファクトの詳細の下で、 [PURGE]をクリックします。
   Fortify Software Security Centerで、アーティファクトをパージする意向を確認するメッセージが表示されます。
4. [OK]をクリックします。

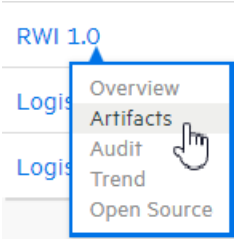
参照情報

"アーティファクトの削除" 下

アーティファクトの削除

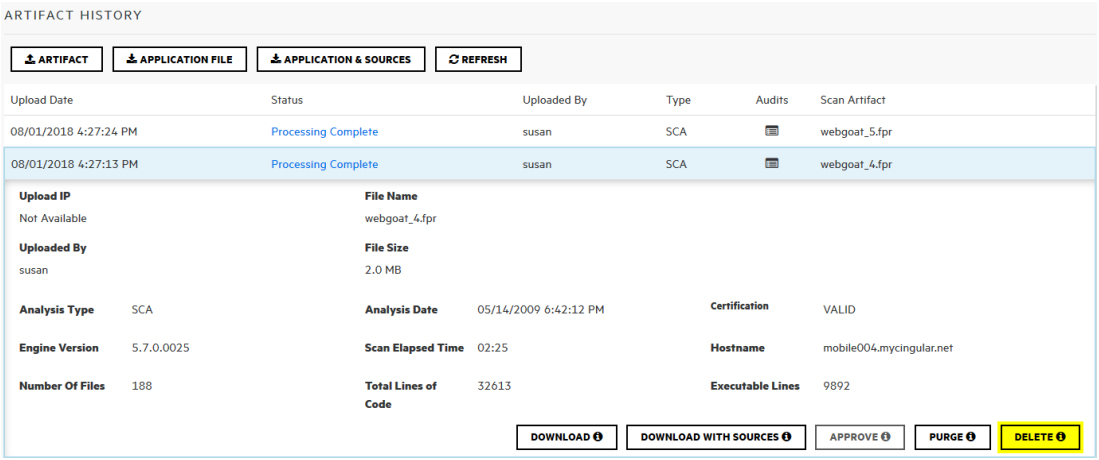
アーティファクトを削除すると、アーティファクトのすべてのトレースが削除されます。誤ってアーティファクトをアップロードした場合は、このオプションを使用します。

Fortify Software Security Center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、次の手順を実行します。



1. [DASHBOARD]から、削除するアーティファクトのあるアプリケーションバージョンにカーソルを移動し、ショートカットメニューから [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。
2. 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、選 択したアーティファクトの詳 細が表 示されます。



3. アーティファクトの詳 細の下 で、 [DELETE]をクリックします。
   Fortify Software Security Centerに、アーティファクトの削 除を確 認するメッセージが表 示されます。
4. [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パージ" ページ300

第15章: 協同監査

分析エンジン(Fortify Static Code Analyzer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べきかどうかを完全に判断する技術はありません。

Fortify Software Security Center内で実行するか、Audit Workbench内で実行するか、監査アシスタント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項目が達成されます。

- 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

Fortify Software Security Center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。

Fortify Software Security Centerでは、Fortify Software Security Centerアプリケーションに関連する問題を監査するWebベースの協同環境を提供します。次のセクションでは、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。

これらのトピックの情報は、Fortify Software Security Center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知っているという前提に基づいて説明されます (Fortify Software Security Centerの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" ページ217を参照してください)。

このセクションで説明するトピック:

現在の問題の状態について

Fortify Software Security Centerでは、どの分析エンジン(アナライザ)があるアプリケーションバージョンの個々の問題を明らかにしたかを追跡し、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かまたは[AUDIT]ページに入力された後、Fortify Software Security Centerで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、Fortify Software Security Center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。

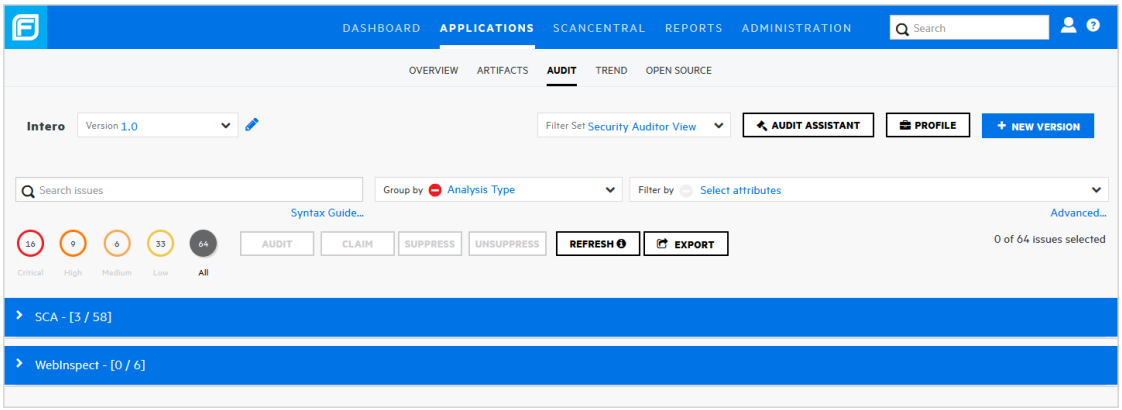
新しいスキャン結果がアップロードされるたびに、Fortify Software Security Centerではすべての問題をチェックして、以前のスキャンで明らかにされたかどうかを判断します。

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、次の手順に従います。

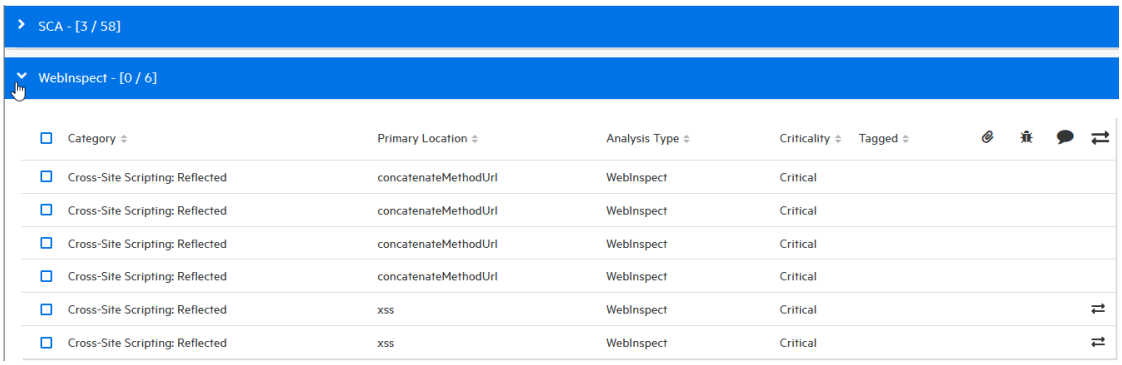
1. 監査するアプリケーションバージョンのスキャン結果をアップロードします。説明については、"スキャンアーティファクトのアップロード" ページ288を参照してください。

2. アプリケーションバージョンの [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。("[OVERVIEW] および [AUDIT] ページに表示する問題をフィルタ処理する" ページ309および"Fortifyの優先度に基づく問題の表示" ページ307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。



次の表は、問題テーブルの列とそれぞれの説明を示しています。

列	説明
Category	発見された問題のカテゴリを表示します。
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行を表示します
Analysis Type	スキャンで使用される分析エンジンを表示します
Criticality	問題が示す相対的脅威を示します
Tagged	問題に適用されたカスタムタグ値がある場合は、その値を表示します。
Attachments	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
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
Comments	問題にコメントが追加されたかどうかを示します
Correlation	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。

参照情報

"Fortify Scan結果の監査" ページ317

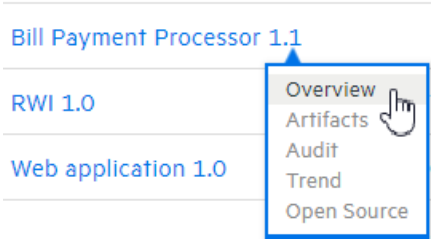
"Sonatype結果の監査" ページ342

Fortifyの優先度に基づく問題の表示

[OVERVIEW]および [AUDIT]ページには、 [Critical]リンク、 [High]リンク、 [Medium]リンク、 [Low]リンク、および [All]リンクが含まれています。これらのリンクを使用して、Fortifyの優先度順(および企業に与える可能性のあるリスク)に基づいて問題を表示できます。

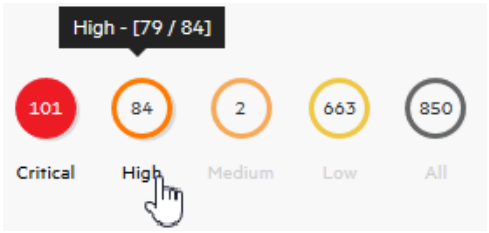
Fortifyの優先度の変更に基づいて [OVERVIEW]ページから問題を表示するには、次の手順に従います。

1. ダッシュボードで目的のアプリケーションのバージョン番号にカーソルを合わせ、 [Overview]を選択します。



アプリケーションバージョンの [OVERVIEW]ページが開きます。 [Group by]リストと [Filter by]リストの左側にある [Critical]リンク、 [High]リンク、 [Medium]リンク、 [Low]リンク、および [All]リンクには、それぞれのFortifyの優先度カテゴリ内の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。

2. 確認された優先度カテゴリ内の問題の数を確認するには、カーソルをリスクカテゴリに移動します。

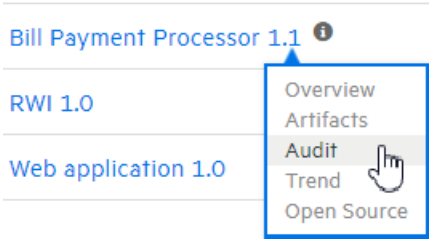


確認された問題の数が左側に表示され、問題の合計数が右側に表示されます。この例では、優先度が高い問題の合計数の79/84を確認できます。

3. 指定したFortifyの優先度に基づいて [OVERVIEW]ページに問題チャートを表示するには、リンクを選択します。

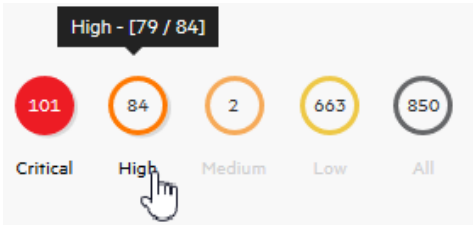
Fortifyの優先度の変更に基づいて [AUDIT]ページから問題を表示するには、次の手順に従います。

1. ダッシュボードで目的のアプリケーションのバージョン番号にカーソルを合わせ、 [Audit]を選択します。



アプリケーションバージョンの [OVERVIEW]ページが開きます。検索フィールドの下にある [Critical]リンク、 [High]リンク、 [Medium]リンク、 [Low]、および [All]リンクには、それぞれのFortifyの優先度カテゴリ内の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。

2. 確認された優先度カテゴリ内の問題の数を確認するには、カーソルをリスクカテゴリに移動します。



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。この例では、優先度が高い問題の合計数の79/84が確認されました。

3. 指定したFortifyの優先度に基づいて [AUDIT]ページに問題のリストを表示するには、優先度リンクを選択します。

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" 次のページ

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. Fortifyのヘッダで、 [APPLICATIONS]をクリックします。
2. [Applications]ビューで、 [My assigned issues]チェックボックスを選択します。
   [Applications]ビューには、アプリケーションバージョンのリストと、ユーザに割り当てられているそれぞれの問題の数が表示されます。Fortify Software Security Centerでユーザに割り当てられた問題が見つからない場合は、ユーザに知らせるメッセージが表示されます。

参照情報

"問題の表示設定の設定" ページ325

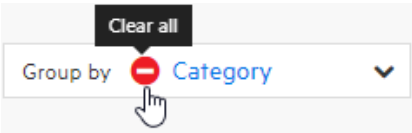
[OVERVIEW]および [AUDIT]ページに表示する問題をフィルタ処理する

[OVERVIEW]ページまたは [AUDIT]ページから、アプリケーションバージョンの表示に関する問題をフィルタ処理するには、次の手順に従います。

注 : また、フィルタセットを選択して、 [OVERVIEW]ページおよび [AUDIT]ページに表示され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" ページ326を参照してください。

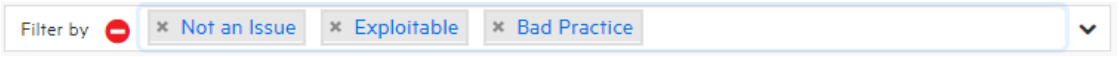
[OVERVIEW]ページまたは [AUDIT]ページに表示される問題をフィルタ処理するには:

1. [**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。



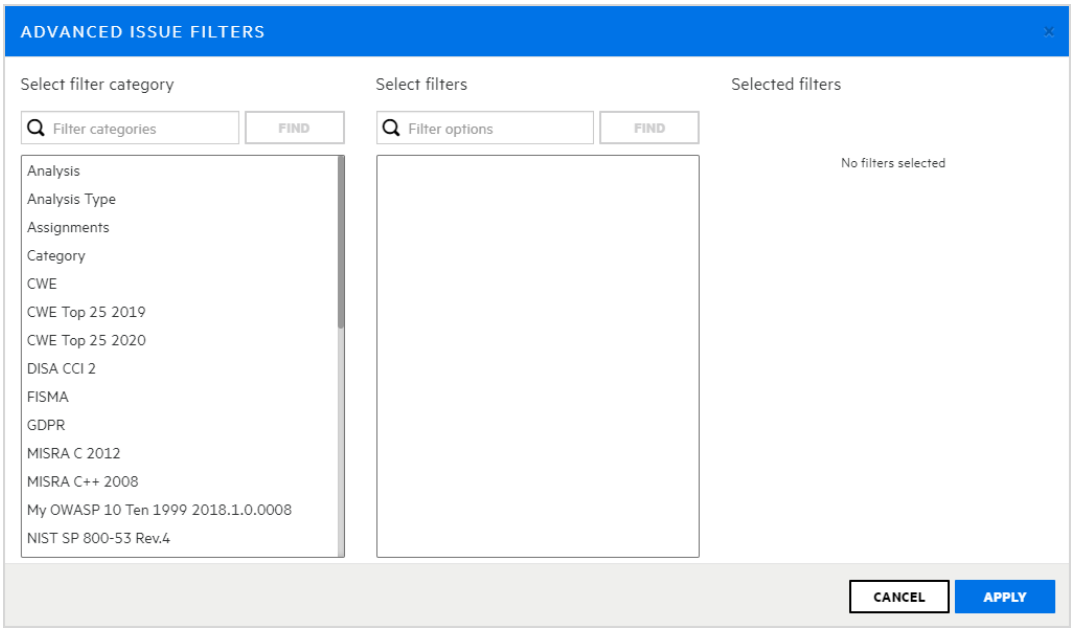
(選択した属性を削除するには、 [**Clear all**]アイコンをクリックします)。

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。ただし、1度に1つを選択する必要があります。



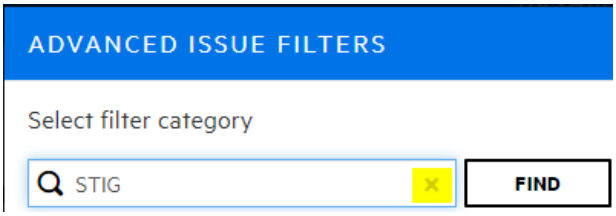
(選択した属性を削除するには、その名前の横にある **x** アイコンをクリックします。選択したすべての属性を削除するには、 [**Clear all**]アイコンをクリックします)。

3. 解 析 以 外 のカスタムタグの値 に基 づいて、またはOWASP、WASC、または他 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 をフィルタするには:
   a. [**Filter by**]リストの下 にある [**詳 細**]リンクをクリックします。



   [ADVANCED ISSUE FILTERS]ウィンド ウが開きます。

   b. [**Select filter category**]リスト から、カテゴリを選 択します。(リストされたカテゴリを絞 り込 むには、 [**Filter categories**]ボックスにテキスト 文 字 列 を入 力して、 [**FIND**]をクリックします。)

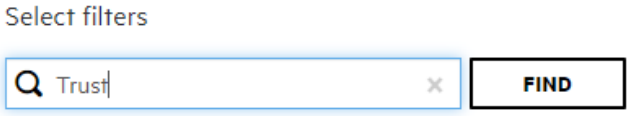


   フィルタカテゴリの完 全 なリストを再 び表 示 するには、 [**Filter categories**]ボックスの**x**をクリックします。

   [**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。

   c. リストをさらに絞 り込 むには、 [**Select filters**]の下 の [**Filter options**]ボックスにテキスト 文 字 列 を入 力して、 [**FIND**]をクリックします。

   [**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。

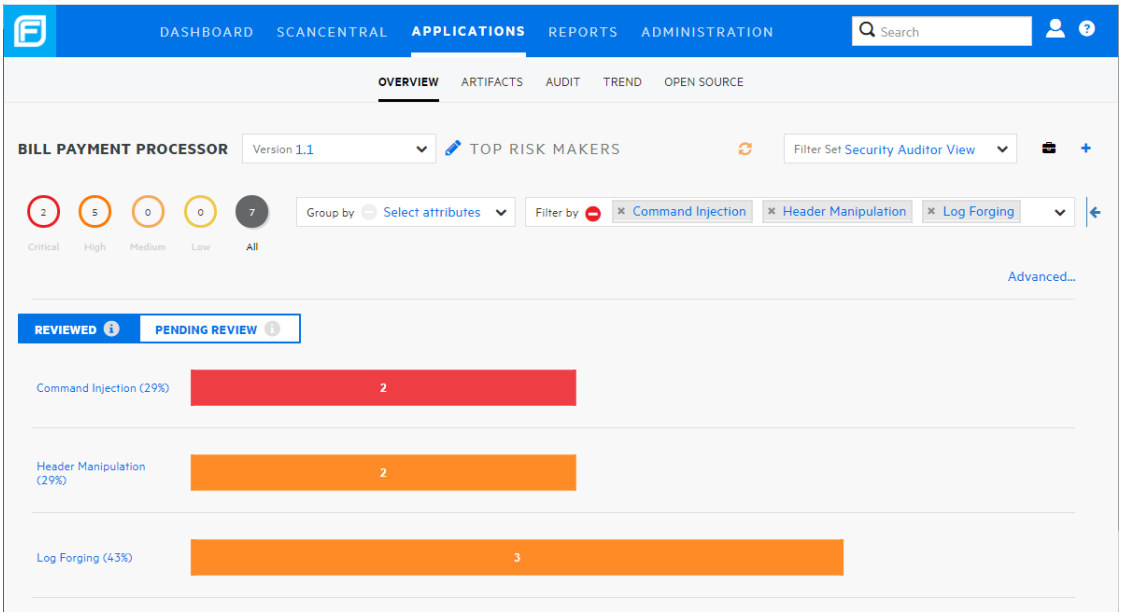


フィルタの完全なリストを再び表示するには、[Filter categories]ボックスのxをクリックします。

d. [Select filters]リストで、右側の[Selected filters]リストに追加する各フィルタをクリックします。

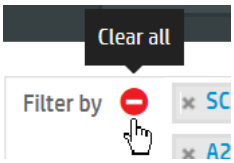
e. 別のフィルタカテゴリのフィルタを追加するには、これらの手順を繰り返します。

f. [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. フィルタの1つを削除するには、左側の閉じる記号をクリックします。



5. 選択したすべてのフィルタをクリアするには、[Clear all]アイコンをクリックします。

参照情報

"問題の検索" 下

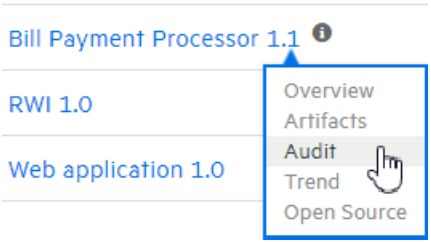
"Fortifyの優先度に基づく問題の表示" ページ307

"Fortify Software Security Centerでのグローバル検索" ページ334

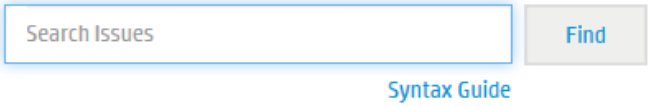
問題の検索

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. ダッシュボードのアプリケーションバージョンサマリテーブルで、カーソルを目的のアプリケーションバージョンに移動し、 [**Audit**]を選択します。



2. [**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
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	排他的範囲は「(」および「)」、包括的範囲は「[」および「]」というように、標準的な数学構文を使用します。たとえば(2,4]は、2より大きく、4以下を意味します
not equal	文字列の前に感嘆符(!)を付け、文字列で指定された問題を除外します。例: `file:!Main.java`は、`Main.java`内にないすべての問題を返します

注: 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。

検索用語をさらに修飾子で修飾するには、構文`modifier:<search_term>`を使用します。("検索修飾子" 次のページを参照してください)。

注: アプリケーションバージョンに日付タイプのカスタムタグが割り当てられている場合に、問題に割り当てられた日付に基づいて問題を検索する場合は、日付を`<DateCustomTag>: yyyy-mm-dd`形式で指定する必要があります。

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、Fortify Software Security Center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。

   Fortify Software Security Centerは、検索文字列に一致する問題を一覧表示します。

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

"[OVERVIEW]および[AUDIT]ページに表示する問題をフィルタ処理する" ページ309

"検索クエリの例" ページ316

"Fortify Software Security Centerでのグローバル検索" ページ334

検索修飾子

検索修飾子を使用して、検索用語を適用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、名前にスペースを含む修飾子を使用するには、修飾子を角括弧で区切る必要があります。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。

修飾子を使用して条件付けしない検索は、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に基づいて検索文字列とマッチします。

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、指定した文字列を含む結果が返されます。

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。この場合、アナライザが`control flow`であるすべての結果を返します。

次の表に、検索修飾子を示します。これらの中には、括弧で囲まれた短縮名があるものがあります。どちらかの修飾子文字列を使用できます。

修飾子	説明
`[issue age]`	`new`、`updated`、`reintroduced`、または`removed`という

修飾子	説明
	問題の新しさを検索します。
<*custom_tagname*>	指定したカスタムタグを検索します。空白を含むタグ名は角括弧で区切る必要があります。 例: `[my tag]:value`
`analysis`	指定した監査分析値(たとえば`exploitable`、`not an issue`など)を持つ問題を検索します。
`analyzer`	指定したアナライザの問題を検索します
`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。 **注:** 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。Fortifyではこの検索修飾子は使用しないことをお勧めしています。
`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。
`comments` `(comment, com)`	この問題について送信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。Static Code Analyzerを使用すると、コード分析で行われた想定の数に基づいて信頼値が計算されます。想定が多い場合は、信頼性の値が低くなります。
`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。

修飾子	説明
[fortify priority order]	Static Code Analyzerによって決定された指定優先度に一致する優先度レベルを持つ問題を検索します。有効な値は、critical、high、medium、およびlowで、予想される影響と悪用の可能性に基づいています。 影響値は、問題の悪用が成功した場合に発生する可能性のある損害を示します。likelihood値は、信頼性、ルールの精度、および問題が悪用される可能性の組み合わせです。
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。
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 10 2013]、[SANS Top 25 2011]、および [PCI <*version*>]などが含まれます。空白を含むフィールド名は角括弧で区切ります。
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。

修飾子	説明
	[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。
[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" 下を参照してください。

参照情報

"問題の検索" ページ311

検索クエリの例

検索修飾子を使用する検索クエリの例を次に示します。

- getSSN()をソースとしてjspが含まれるファイル名のプライバシー侵害を検索するには、次のように入力します。

  ```
  category:"privacy violation" source:getssn file:jsp
  ```

- com/fortify/sscが含まれるすべてのファイル名を検索するには、次のように入力します。

  ```
  file:com/fortify/ssc
  ```

- mydbcode.sqlcleanseを名前の一部とするトレースを含むすべてのパスを検索するには、次のように入力します。

  ```
  trace:mydbcode.sqlcleanse
  ```

- `cleanse`を名前の一部とするトレースを含むすべてのパスを検索するには、次のように入力します。

  ```
  trace:cleanse
  ```

- 修飾子の一部として`cleanse`が含まれるすべての問題を検索するには、次のように入力します。

  ```
  cleanse
  ```

- `[my tag]`が割り当て済みで`P1`に設定されている監査済みのすべての問題を検索するには、次のようにを入力します。

  ```
  [my tag]:P1
  ```

- コメント内に`asdf`を含む、すべての抑止された脆弱性を検索するには、次のように入力します。

  ```
  suppressed:true comments:asdf
  ```

- SQLインジェクション以外のすべてのカテゴリを検索するには、次のように入力します。

  ```
  category:!SQL Injection
  ```

- `java`または`jsp`のどちらかがファイル名に含まれる問題を検索するには、次のように入力します。

  ```
  filename:java OR filename:jsp
  ```

- `java` を含み、12行目で発生する問題を検索するには、次のコマンドを入力します。

  ```
  filename:java AND line:12
  ```

参照情報

"問題の検索" ページ311

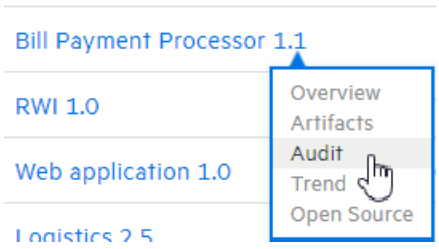
"検索修飾子" ページ313

Fortify Scan結果の監査

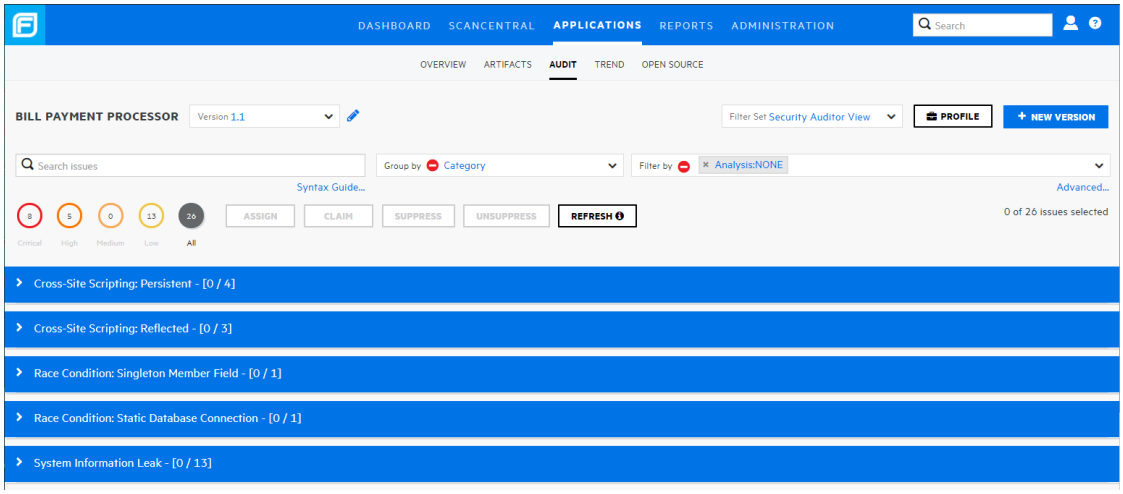
Sonatypeの問題を監査する方法については、"Sonatype結果の監査" ページ342を参照してください。

監査する問題を表示するには、次の手順に従います。

1. 監査するアプリケーションバージョンのスキャン結果をアップロードします。説明については、"スキャンアーティファクトのアップロード" ページ288を参照してください。



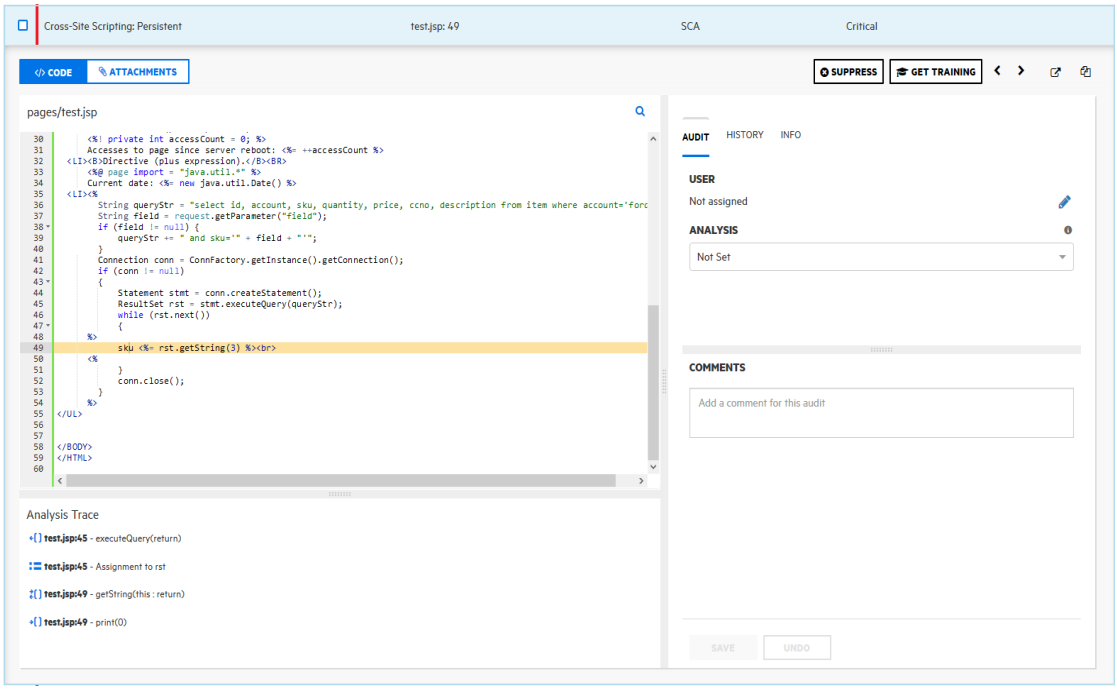
2. アプリケーションバージョンの [AUDIT]ページを開きます。
3. 監査する問題を選択的に表示するには、問題リストにフィルタを適用します。("[OVERVIEW]および [AUDIT]ページに表示する問題をフィルタ処理する" ページ309および"Fortifyの優先度に基づく問題の表示" ページ307を参照してください)。
4. 問題テーブルで、グループを選択した場合は、グループを展開して、グループに含まれている問題を表示します。



問題を監査するには、次の手順に従います。

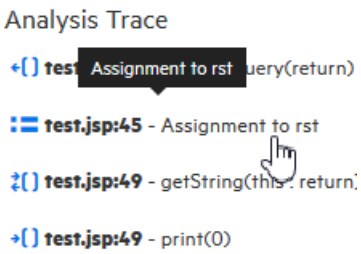
1. 問題を展開して詳細を表示するには、テーブル内の該当する行をクリックします。

   次の画面キャプチャは、Fortify Static Code Analyzerのスキャン中に明らかにされた問題の詳細を示しています。WebInspectの検索結果の表示については、"Fortify Software Security CenterでのFortify WebInspectスキャン結果の表示" ページ347を参照してください。Sonatypeの結果の表示の「Sonatypeデータの表示」詳細については、"Sonatypeデータの表示" ページ338を参照してください。



ヒント: 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、[**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、[**Copy issue link to clipboard**]ボタン()をクリックします。

[**CODE**]タブには、問題に関連するソースの領域が表示されます。

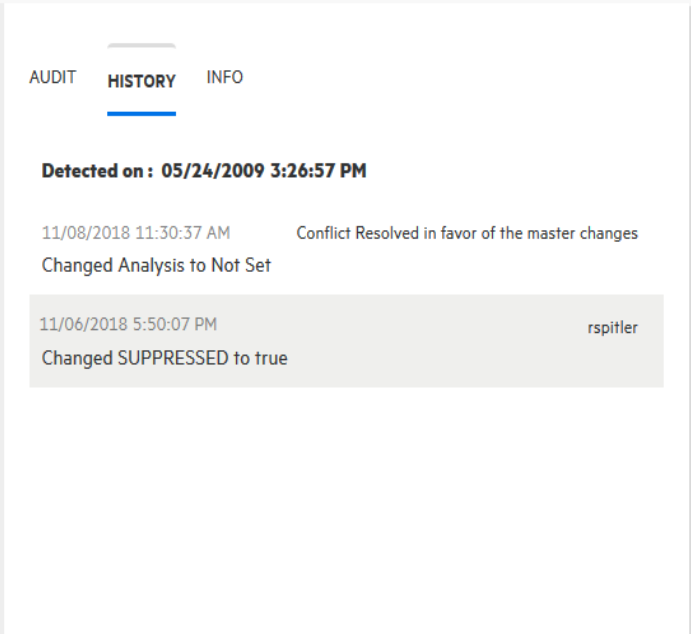


2. 汚染されたデータの経緯のステップに関するサマリの詳細を表示するには、[**Analysis Trace**]の下で、そのステップにカーソルを移動します。
3. ステップに関連付けられているコードを表示するには、[**Analysis Trace**]の下のステップをクリックします。

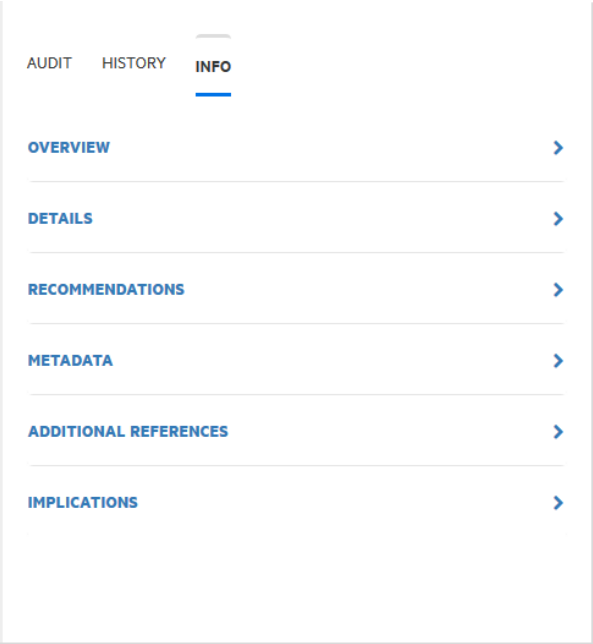
   対応するコード行が[**CODE**]タブで強調表示されます。
4. 問題に関連するコード内の特定の文字列を検索するには、次の手順に従います。

   a. 検索アイコンをクリックします。

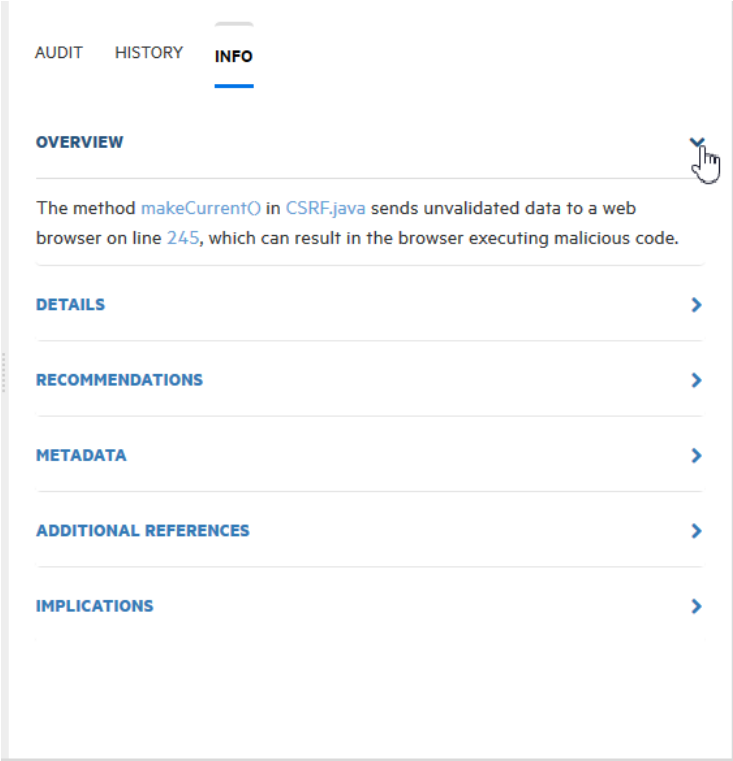
b. 表示されたテキストボックスに、文字列を入力します。次へのアイコン と前へのアイコン を使用して、検索結果を移動します。



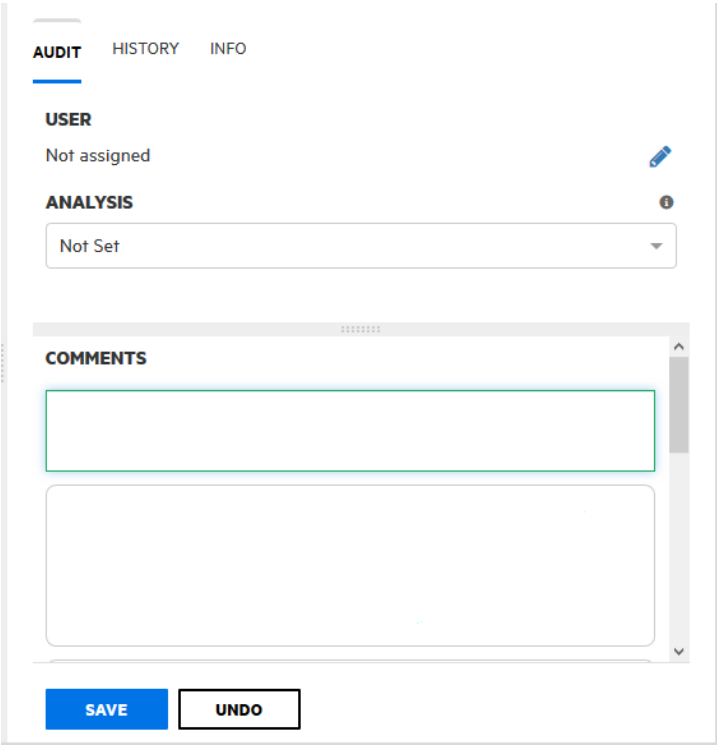
5. 問題の履歴を表示するには、右側のペインで [HISTORY]タブを選択します。



6. 問題の概要、結果に関する詳細、改善に関する推奨事項、問題のメタデータ、追加リソースへの参照、およびアプリケーションバージョンに対する影響を表示するには、右側のペインで [INFO]タブを選択します。



7. 行を展開して情報クラスを表示するには、対応する矢印記号(›)を選択します。



8. 監査を開始するのに十分な情報がある場合は、右側のペインで [AUDIT]タブを選択します。

9. (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、 [SUPPRESS]をクリックします。
10. (オプション)管理者がFortify Software Security Centerでアプリケーションセキュリティトレーニングを設定している場合 ("アプリケーションセキュリティトレーニングの設定" ページ84を参照)、選択した問題を処理する方法に関する状況に応じた適切なガイダンスを得るには、 [GET TRAINING]をクリックします。Fortify Software Security Centerから移動するというメッセージが表示されます。 [OK]をクリックします。

    Fortify Software Security Centerがアプリケーションセキュリティトレーニングウェブサイトを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、および言語に基づいてトレーニングコンテンツを表示します。

    注 : 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。

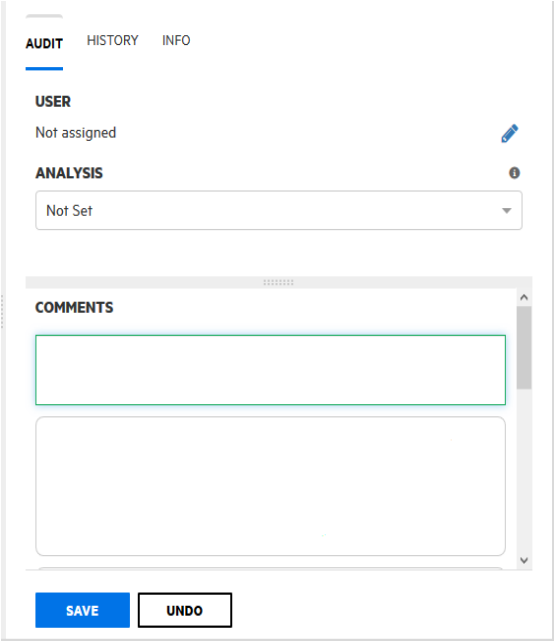
11. ファイルを問題に添付するには、次の手順に従います。
    a. [ATTACHMENTS]をクリックします。
    b. [CLICK HERE TO ADD]をクリックします。
    c. [UPLOAD ATTACHMENT]ダイアログボックスで、 [BROWSE]をクリックし、アップロードするファイルに移動して選択します。

    サポートされているファイル形式は、TXT、LOG、DOC、DOCX、PDF、PPTX、JPG、JPEG、BMP、PNG、TIFF、GIF、ZIP、GZIP、TAR、および7ZIPです。(XML形式のドキュメントはサポートされていません)。

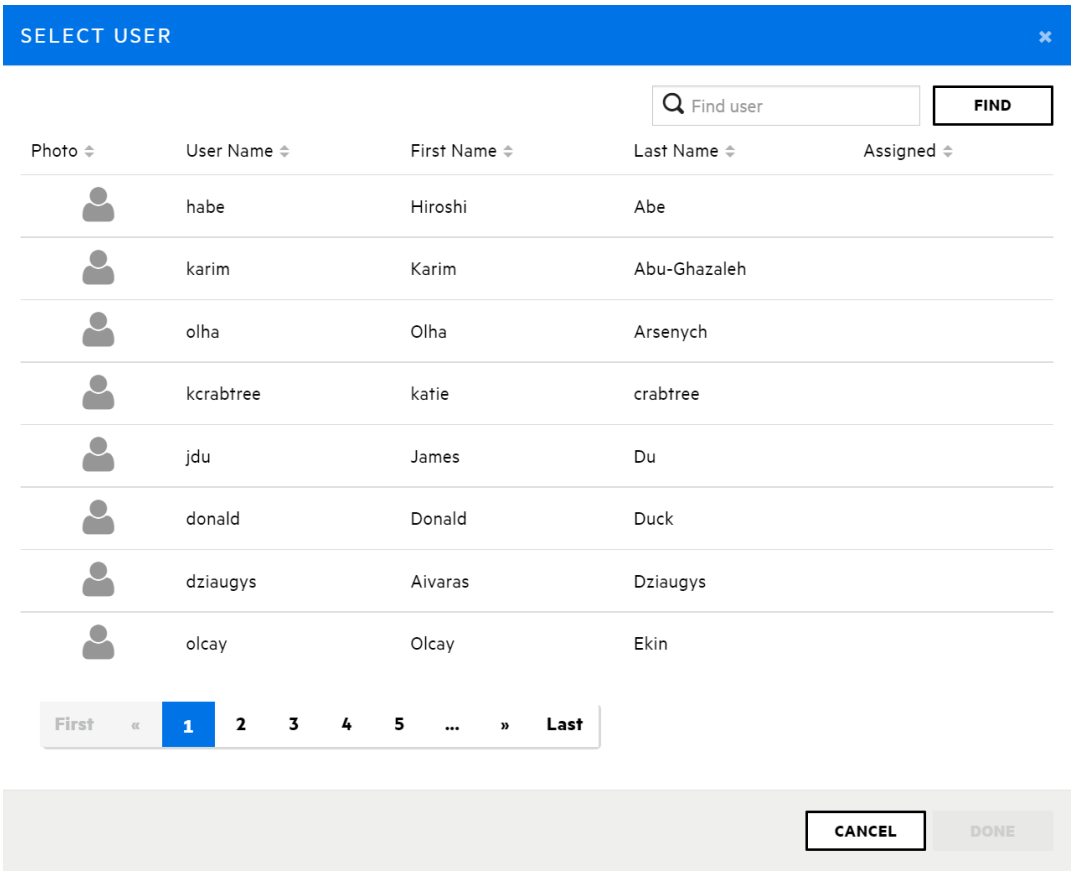
    注 : ファイルサイズは3MBを超えられません。

    d. (オプション) [Description]ボックスに、ファイルの説明を入力します。
    e. [SAVE]をクリックします。

    イメージファイルを添付した場合、Fortify Software Security Center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。
12. [CODE]をクリックし、右画面で [AUDIT]タブを選択します。



13. ユーザを問題に割り当てるには、次の手順に従います。
    a. [USER]で、[Edit assigned user]アイコンをクリックします。



[SELECT USER]ダイアログボックスが開きます。

b. 問題に割り当てるユーザを見つけるには、 [Find user]ボックスにユーザ名の一部またはすべてを入力し、 [FIND]をクリックします。

c. 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。

d. [DONE]をクリックします。

[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)。

14. [<*Primary_Tag_Name*>]リストで、この問題の評価を反映する値を選択します。

15. 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、これらのタグの値を指定します。

注 : アプリケーションバージョンの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してください。そうしないと、Fortify Software Security Centerでこの問題は未監査として扱われます。

注 : Audit Assistantが問題を評価した場合は、右側のペインに他のフィールド(**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、"Audit Assistantの結果の確認" ページ 332を参照してください。

16. (オプション) [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。(監査設定を保存した後、 [COMMENTS]セクションにはコメント、および以前に保存した他のコメントが一覧表示されます)。

17. [AUDIT]タブの下部にある [SAVE]をクリックします。

参照情報

"問題のバッチの監査" ページ327

"監査アシスタントについて" ページ85

抑止、削除、および非表示の問題について

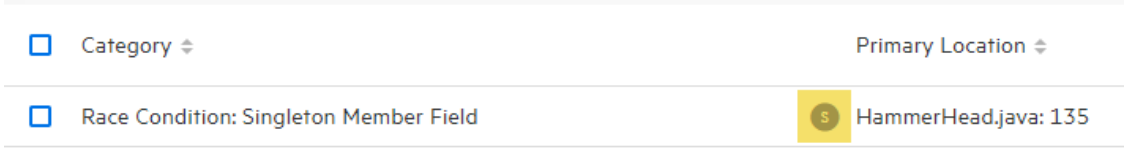
問題ペインに、抑止、削除、および非表示の問題を一覧表示するかどうかを制御できます。

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。

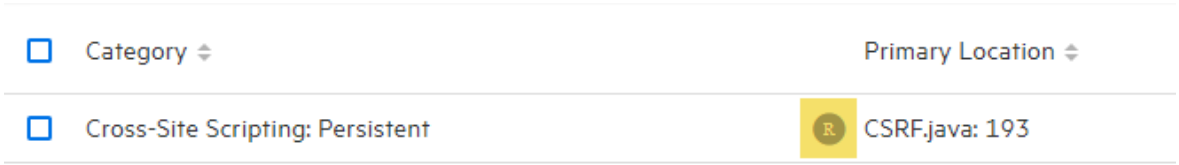
抑止された問題は、 [OVERVIEW]ページの展開可能なペインの [Version Progress]セクションに表示される [Total Issues]の値には含まれません。抑止された

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、"Fortify Scan結果の監査" ページ317を参照してください。抑止された問題の表示方法については、"問題の表示設定の設定" 下を参照してください。



削除された問題

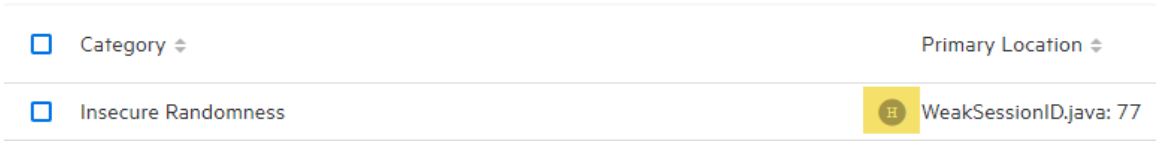
アプリケーションでスキャンが複数回実行されるうちに、問題が修正されたり古くなることがよくあります。Fortify Software Security Centerでスキャン結果がマージされると、以前のスキャンで見つかったが、最新の分析結果で明らかでなくなった問題が削除としてマークされます。



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。削除された問題の表示方法については、"問題の表示設定の設定" 下を参照してください。

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。

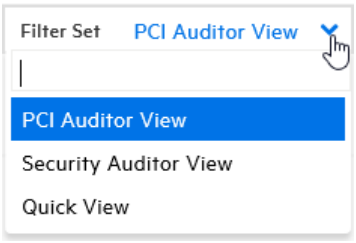


非表示の問題の表示方法については、"問題の表示設定の設定" 下を参照してください。

問題の表示設定の設定

[Application Profile]ダイアログボックスから、個々のアプリケーションバージョンに対して特定の表示設定ができます。

フィルタセットを使用して表示問題を変更する



注: 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た発行テンプレートによって異なります。ここに示す3つのフィルタセットは、Fortifyが提供する問題テンプレートに含まれています。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。

Fortify Software Security Center では、 [OVERVIEW]ページと [AUDIT]ページでのアプリケーションバージョン問題の表示を変更する次のフィルタセットを提供しています。

- 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。

問題に対して送信されたバグの表示

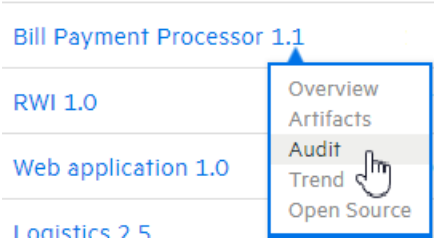
[AUDIT]ページの問題テーブルには、リストに表示された問題に対してバグが送信されたかどうかを示す [**Bug submitted**]列(🐞)列が含まれています。

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。

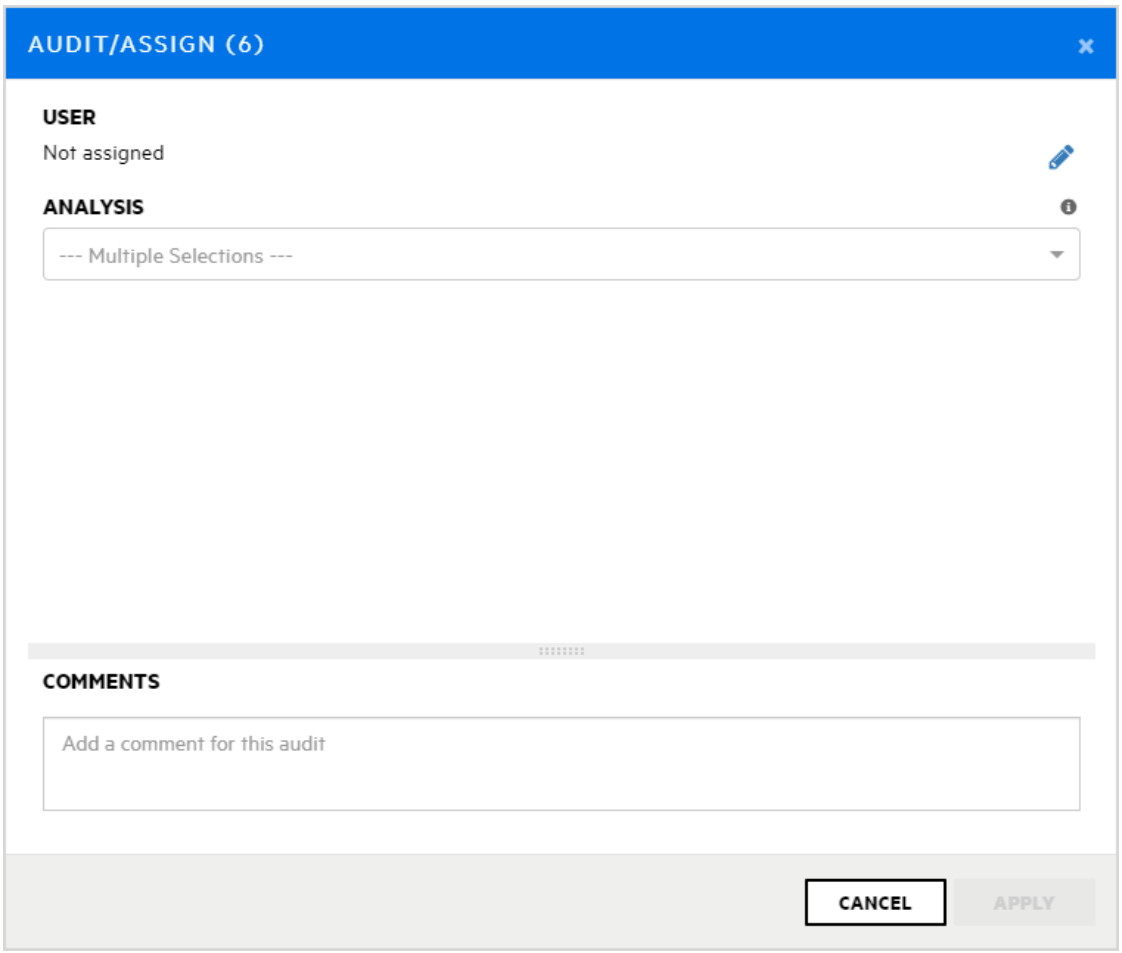
ヒント: バグを表示するには、バグトラッカーアプリケーションでサポートされているブラウザを使用する必要があります。

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. アプリケーションバージョンの [AUDIT] ビューを開きます。
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. [AUDIT] をクリックします。



[AUDIT/ASSIGN] ダイアログボックスが開きます。

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。

a. [Edit assigned user]アイコン🖉を選 択します。
[SELECT USER]ダイアログボックスが開きます。
b. これらの問 題 に割り当 てるユーザを見 つけるには、 [Find user]ボックスにユーザ名 の一 部 またはすべてを入 力し、 [FIND]をクリックします。
c. 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。
d. [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. [ANALYSIS]リストで、この問 題 のバッチの評 価 を反 映 する値 を選 択します。
6. (オプション)下 部 の [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。
7. [APPLY]をクリックします。

参 照 情 報

"Fortify Scan結 果 の監 査 " ページ317

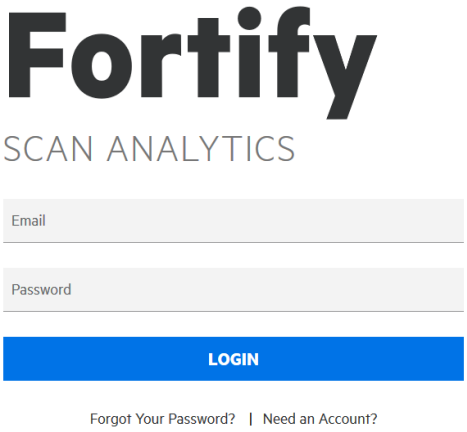
Audit Assistantの使 用

次 のセクションでは、Audit Assistantワークフロー、予 測 ポリシーおよびその使 用 方 法 、メタデータ共 有 を有 効 にする方 法 、Audit Assistantにデータを送 信 する方 法 、および監 査 アシスタントの結 果 を確 認 する方 法 について説 明します。

Audit Assistantワークフロー

Audit Assistantを使 用 するワークフローは次 のとおりです。

1. 次 の方 法 で、Fortify Scan Analyticsアカウントを取 得します。
   a. https://analytics.fortify.comに移 動します。



   b. 次 をクリックします [Need an Account?]

c. [Request a Fortify Scan Analytics Tenant]フォームのフィールドに入力し、[**Request Now**]をクリックします。

Fortify Scan Analyticsに接続する方法に関する情報が記載された電子メールがFortifyから送信されます。

2. Fortify Scan Analyticsを使用して、1つ以上のポリシーを作成します。
3. (オプション)匿名メタデータの共有を選択します。
4. Fortify Scan Analyticsトークンを取得します。
5. Fortify Software Security Centerから:
   - Fortify Scan Analyticsを設定してテストし、[Audit Assistant Configuration]ページで[**REFRESH POLICIES**]をクリックして[**Default prediction policy**]リストに入力します("Audit Assistantの設定" ページ87を参照)。
   - デフォルトの予測ポリシーを指定します。
   - (オプション)Audit Assistantを有効にして、監査されていない問題を自動的にFortify Scan Analyticsに送信して予測を実施します。
   - (オプション)Audit Assistantを有効にして、カスタムタグに予測値を自動的に適用します。
6. Fortify Software Security Centerから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Audit Assistantに送信します。このステップを「トレーニング」と呼びます。
7. Fortify Software Security Centerからアプリケーションバージョンを開き、Fortify Static Code Analyzerスキャン結果をAudit Assistantに送信します。
8. Audit Assistantが評価を完了したら、その結果を確認し、必要に応じて調整します。
9. 修正された結果をAudit Assistantに送信します。

次のセクションでは、認証トークンをFortify Scan Analyticsから取得し、そのトークンを使用してFortify Scan Analyticsへの接続を設定する方法について説明します。この後のセクションでは、メタデータを送信するためにScan Analyticsを準備し、データを送信し、監査アシスタントの結果を確認し、修正した監査データを送信する方法について説明します。

参照情報

"予測ポリシーについて" 次のページ

"予測ポリシーの定義" 次のページ

"Audit Assistantの設定" ページ87

"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" ページ238

"メタデータ共有の有効化" ページ331

"Audit Assistantへのトレーニングデータの送信" ページ332

"Audit Assistantの結果の確認" ページ332

予測ポリシーについて

監査アシスタントを使用してスキャン結果を処理するには、最初に、少なくとも1つの予測ポリシーを、Fortify Scan Analyticsで定義する必要があります。予測ポリシーでは、監査アシスタントおよびFortify Scan Analyticsが不定として扱う問題、つまり真の問題でもなく問題以外でもないと判断するために使用する信頼しきい値を決定します。

注: 監査アシスタントの設定時に、管理者は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、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ない場合に、Scan Analyticsによってそのアプリケーションバージョンに対して使用されます。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、Scan Analyticsはそのポリシーを使用して問題を評価します。

参照情報

"予測ポリシーの定義" 下

"アプリケーションバージョンに対するAudit Assistantオプションの設定" ページ256"Audit Assistantの設定" ページ87

"Audit Assistantの設定" ページ87

"監査アシスタントの自動予測について" ページ89

予測ポリシーの定義

監査アシスタントを使用するには、監査アシスタントが不定(真の問題でも問題以外でもない)として扱う問題を判断するために使用できる予測ポリシーを少なくとも1つ定義する必要があります。詳細については、"予測ポリシーについて" 上を参照してください。

予測ポリシーを定義するには、次の方法を使用します。

1. Fortify Scan Analyticsにログインします(https://analytics.fortify.com)。
2. Fortifyのヘッダで、 [**PREDICTION POLICIES**]を選択します。
3. [Prediction Policies]ページで、 [**+ADD**]をクリックします。
   [Prediction Policies > Add]ページが開きます。
4. [**Policy Name**]ボックスに、ポリシーの名前を入力します。
   [Prediction Policies | Add]ページには、2つの信頼しきい値設定が含まれています。これらを使用して、監査アシスタントが不定(真の問題でも問題以外でもない)として扱う問題を設定します。
   監査アシスタントの結果は次のとおりです。
   - [**AA_Prediction**]値の場合、監査アシスタントによる悪用可能性評価に基づいて問題をグループ分けします。指定可能な値は、 [**Exploitable**]、 [**Below Threshold - Exploitable**]、 [**Not an issue**]、 [**Below Threshold - Not an issue**]、および [**Not Predicted**]です。

注: 監査アシスタントは、データフローおよび制御フローの静的分析の問題のみを予測します。

- [AA_Confidence]値(0.00～1.00の範囲のパーセンテージ値)は、[AA_Prediction]値による監査アシスタントの信頼レベルを表します。

[AA_Confidence]値が予測ポリシーに対してここで設定した信頼しきい値のいずれかを下回る場合、監査アシスタントは問題を不定として扱い、[AA_Prediction]値に[Not Predicted]を割り当てします。

5. [Confidence Threshold - Not an Issue]および[Confidence Threshold - Exploitable]スライダを、Fortify Software Security Centerにおけるアプリケーションの許容可能レベルに設定します。

注: しきい値を高く設定するほど、監査アシスタントの結果に偽陰性が含まれる可能性が低くなります(デフォルトの80%のしきい値を使用したテストでは、偽陰性の発生率は1%未満になります)。

6. (オプション)[Description]ボックスに、ポリシーの説明を入力します。
7. [SAVE]をクリックします。

参照情報

"予測ポリシーについて" 前のページ

"Audit Assistantの設定" ページ87

"アプリケーションバージョンに対するAudit Assistantオプションの設定" ページ256

メタデータ共有の有効化

監査メタデータを、Fortify Community Intelligenceデータセット(Fortifyユーザからの匿名監査メタデータのプール)に提供できます。そうした場合、Fortify Community Intelligenceデータプールを活用して、自分のデータを評価できます。それ以外の場合、Audit Assistantは、送信するトレーニングメタデータに限り、問題を評価するために使用するメタデータを制限します。

注: トレーニングデータを送信せず、さらにメタデータの共有を有効にしていない場合、Fortify Scan Analyticsは問題を評価しません。

データ共有を有効にするには、次の手順に従います。

1. Fortify Scan Analyticsにログインします(https://analytics.fortify.com)。
2. 左ペインで、[Settings]選択します。
3. [Share anonymous issue metrics]チェックボックスを選択します。
4. [Save]をクリックします。

参照情報

"Audit Assistantの設定" ページ87

"予測ポリシーについて" 前のページ

Audit Assistantへのトレーニングデータの送信

次の手順では、評価のためにトレーニングデータをAudit Assistantに送信する方法について説明します。Fortify Software Security Center環境から転送されるデータはすべて匿名化され、機密情報が含まれないことに注意してください。また、トレーニング用にAudit Assistantに送信されるデータには、アプリケーションバージョンのプライマリカスタムタグだけが含まれるので注意してください。

Audit Assistantにトレーニングデータを送信するには、次の手順に従います。

1. ダッシュボードから、必要なアプリケーションバージョンの［OVERVIEW］、［ARTIFACTS］、［AUDIT］、または［TREND］ページを開きます。
2. アプリケーションバージョンツールバーで、［**PROFILE**］をクリックします。
3. ［APPLICATION PROFILE］ダイアログボックスで、［**AUDIT ASSISTANT TRAINING**］タブをクリックします。

   注 : ［**AUDIT ASSISTANT TRAINING**］タブは、管理者がAudit AssistantとFortify Software Security Centerの統合を設定した場合にのみ表示されます。Audit Assistantの設定の詳細については、"Audit Assistantの設定" ページ 87を参照してください。

   ［**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。

   ［**Data last sent for training**］フィールドに［**Sending**］ステータスが表示されます。
5. ［**Data last sent for training**］フィールドが更新された日付と時刻で更新された後、［APPLICATION PROFILE］ダイアログボックスを閉じます。
6. アプリケーションバージョンツールバーで［**ARTIFACTS**］をクリックし、アップロードの［**Status**］フィールドが［**Processing Complete**］かどうかを確認します。

処理が完了したら、［AUDIT］ページで結果を表示できます。手順については、"Audit Assistantの結果の確認" 下を参照してください。

参照情報

"監査アシスタントについて" ページ85

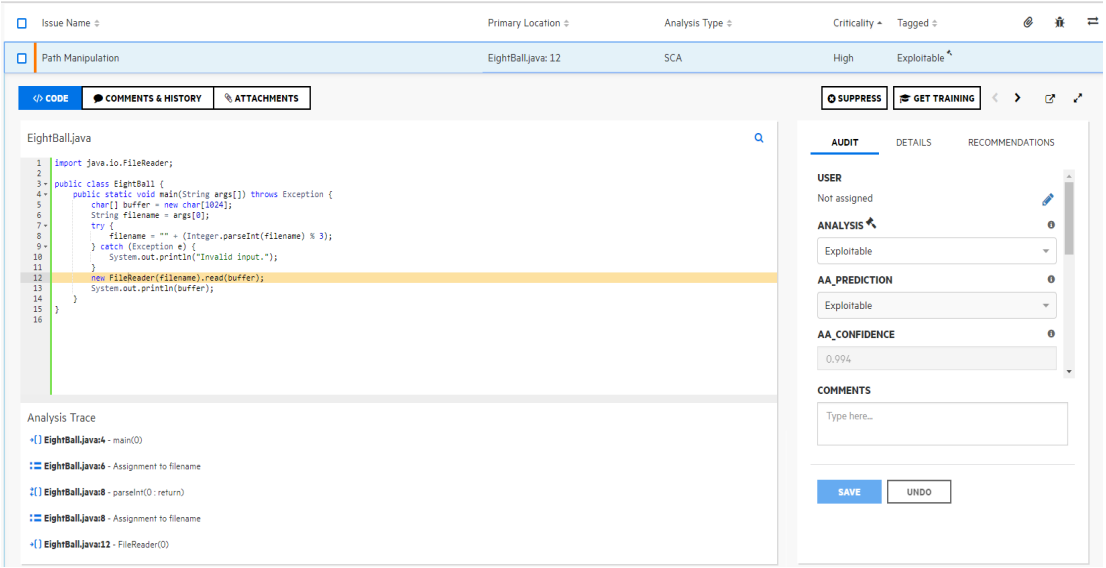
"アプリケーションバージョンの自動適用と自動予測を有効にする" ページ238

Audit Assistantの結果の確認

Audit Assistantにスキャン結果を送信し、Audit Assistantが問題の評価が完了したら、その結果を確認できます。

Audit Assistantの結果を表示するには、次の手順に従います。

1. アプリケーションバージョンの [AUDIT]ページに移動します。
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。("Fortifyの優先度に基づく問題の表示" ページ307および" [OVERVIEW]および [AUDIT]ページに表示する問題をフィルタ処理する" ページ309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. 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のカスタムタグに加えて、右ペインには次のものが表示されます。
   - **AA_PREDICTION** - Audit Assistantが問題に割り当てた悪用可能性レベル。
   - **AA_CONFIDENCE** - 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0.982は、98.2%の信頼レベルを示します。
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、AA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. [**SAVE**]をクリックします。

参照情報

"監査アシスタントについて" ページ85

"Fortify Scan結果の監査" ページ317

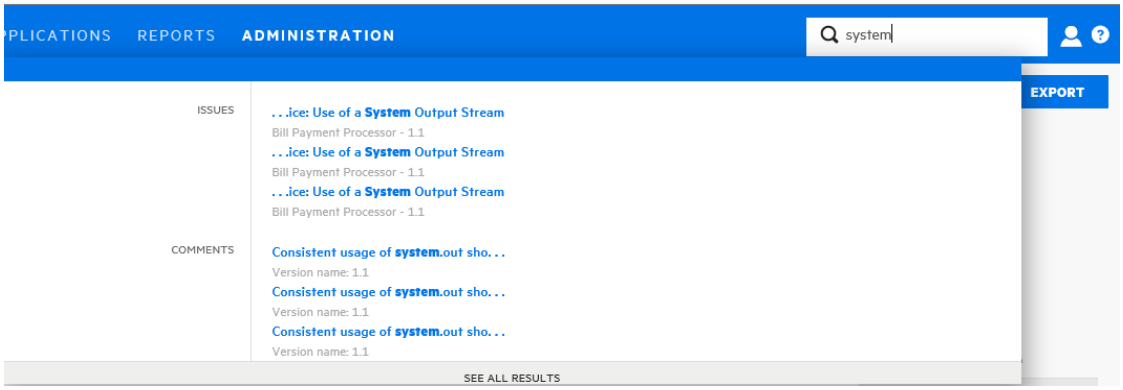
Fortify Software Security Centerでのグローバル検索

Fortify Software Security Centerユーザインタフェースの場所に関係なく、ヘッダのグローバル [**Search**]フィールド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。

注: 検索ボックスは、Fortify Software Security Center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、"Fortify Software Security Centerの初回設定" ページ69を参照してください。

グローバル [**Search**]フィールドを使用するには、次の手順に従います。

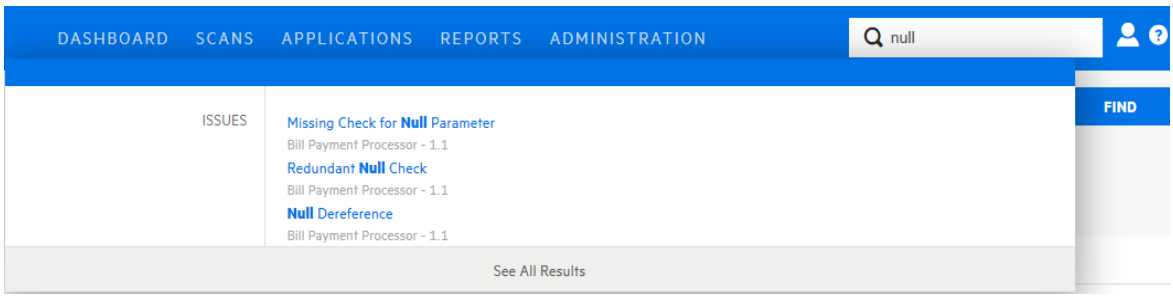
1. どのビューからでもよいので、 [**Search**]ボックスに検索文字列を入力します。



   Fortify Software Security Center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。

   Fortify Software Security Centerは、項目を表示したり作業したりできるユーザインタフェースを開きます。
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

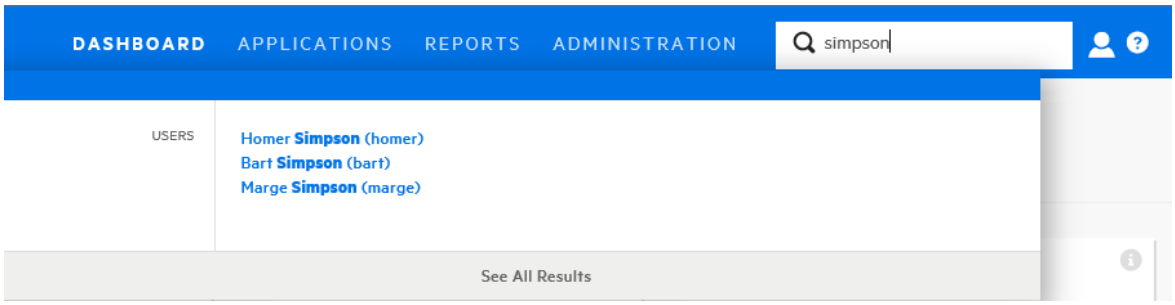


表示された結果から問題を選択すると、Fortify Software Security Centerで対応するバージョンページが表示され、問題のフルビューが展開されます。

[See All Results]を選択すると、Fortify Software Security Centerで [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、 [next]および [previous]ボタンを使用して、すべての結果をページに表示できます。

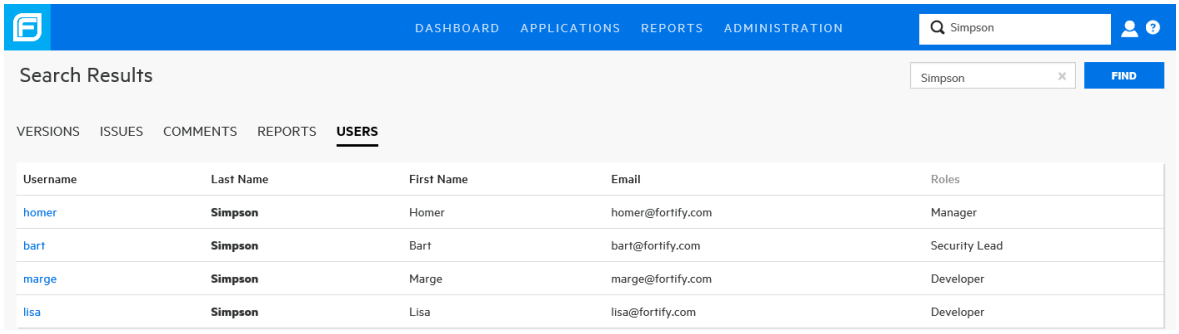
注: 問題の検索結果には、削除、非表示、または抑止された問題が含まれます。選択した項目が [AUDIT]ページに表示されない場合は、アプリケーションバージョンの表示設定をチェックして、 [ADVANCED OPTIONS]タブで適切なフラグが有効になっているか確認し、削除、非表示、および抑止された問題を表示します。手順については、"問題の表示設定の設定" ページ325を参照してください。

例: ユーザの検索



表示された結果から1人のユーザを選択した後、必要な許可を持っている場合、Fortify Software Security Centerの [ADMINISTRATION]ビューでユーザアカウントの詳細が表示されます。

[See All Results]を選択すると、Fortify Software Security Centerで [Search Results]ページが表示されます。



参照情報

" [Applications]ビューからのアプリケーションとアプリケーションバージョンの検索" ページ239

Webアプリケーションの被影響性分析について

被影響性分析は、FortifyとSonatypeが共同開発した機能です。SonatypeによってWebアプリケーションに関して明らかにされる、アプリケーションのクラスパスの一部である既知の脆弱性が考慮に入れられます。これは、実際に関数またはメソッドを呼び出したのか、ユーザが制御する入力が関数またはメソッドに到達することを許可したのかを判断します。これは、公開された問題に対してコードに真に脆弱性があるかどうかを示します。被影響性分析は、記述された脆弱性に実際に影響を受けやすいかどうかを判断します。単にアプリケーションのライブラリのコレクションにその依存性があることを判断するだけではありません。

Sonatypeでは、脆弱性のあるコンポーネントに、アップグレード可能で脆弱性のないバージョンがあるか確認します。ある場合は、関数またはメソッドの署名を書き込みます。Fortify Software Security Centerでは、この署名を受け取り、この関数が呼び出されたのか、またはユーザが制御する入力がこの関数に達したかどうかを確認します。関数が呼び出された場合、Fortify Software Security Centerでは「呼び出し済み」とラベル付けします。ユーザが制御する入力がこの関数に達した場合、Fortify Software Security Centerでは「制御可能」とラベル付けします。Sonatypeデータを監査した後で、アプリケーションに存在することが証明された脆弱性を持つオープンソースコンポーネントを、悪用可能性の証拠がないコンポーネントよりも優先的にアップグレードできます。Webアプリケーションコードに対する被影響性分析スキャンを実行すると、Fortify Software Security Centerに表示される結果が著しく向上します。

被影響性分析の要件

Webアプリケーションで被影響性分析を実施するには、Fortify Software Security Centerの他に次のものが必要です。

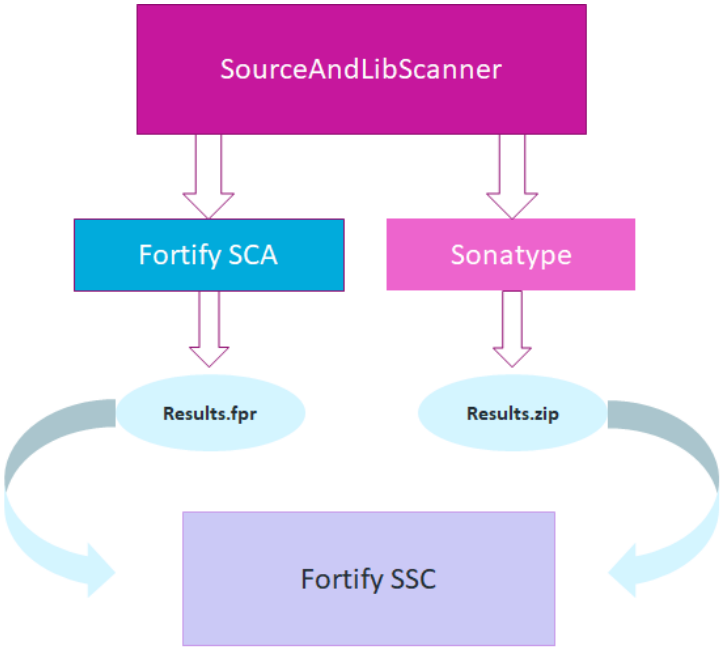
- Fortify Static Code Analyzer
- Fortify Software Security Center用Sonatypeプラグイン

  プラグインをダウンロードして設定する方法については、"Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164を参照してください)。
- Fortify SourceAndLibScanner

  SourceAndLibScannerを取得するには、https://marketplace.microfocus.com/fortify/content/fortify-sourceandlibscannerに移動します。

  SourceAndLibScannerのソフトウェア要件、およびこのツールのインストールと使用の方法については、SourceAndLibScannerユーティリティにパッケージされている『Micro Focus Fortify SourceAndLibScannerユーザガイド』を参照してください。

アプリケーションの結果を最適化する一般的なワークフロー



アプリケーションに最適なスキャン結果を得るステップは次のとおりです。

1. Sonatypeプラグインをダウンロードしてインストールします。("Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164を参照してください)。
2. ([OPEN SOURCE]ページでのみ)被影響性分析の検出結果が含まれる結果を取得するには、SourceAndLibScannerを使用してアプリケーションのオープンソースコンポーネントの脆弱性を明らかにするSonatypeスキャンを実行し、Webアプリケーションバージョンのスキャンを実行し、Fortify Software Security Centerで結果のFPRファイルをアプリケーションバージョンにアップロードします。詳細については、"Webアプリケーションの被影響性分析について" 前のページを参照してください。

   > SourceAndLibScannerを使用してFortify Static Code Analyzerスキャンや Sonatypeライブラリスキャンを実行し、その結果をFortify Software Security Centerにアップロードする方法については、『Micro Focus Fortify SourceAndLibScannerユーザガイド』を参照してください。

3. Fortify Software Security Centerで結果のZIPファイルをアプリケーションバージョンにアップロードします。
4. Fortify Software Security Centerで結果のFPRファイルを指定されたアプリケーションバージョンにアップロードします。

   SourceAndLibScannerおよびFortify Statics Code Analyzerでは、オープンソースコンポーネントの脆弱性に対応する被影響性分析を提供します。

注: SourceAndLibScannerを使用して開始されたFortify Static Code Analyzerスキャンによって明らかにされた問題は、Sonatypeの検出結果のコンテキストでのみ重大です。この結果、 [AUDIT]ページでデフォルトでは非表示になります。

5. [OPEN SOURCE]ページから結果を監査します("Sonatype結果の監査" ページ342を参照)。Sonatypeの問題は [AUDIT]ページから監査できます。ただし、被影響性分析の結果は [OPEN SOURCE]ページでのみ表示され、 [**Invoked**]、[**Controllable**]、および [**Evidence**]フィールドで表されます。

Sonatypeデータの表示

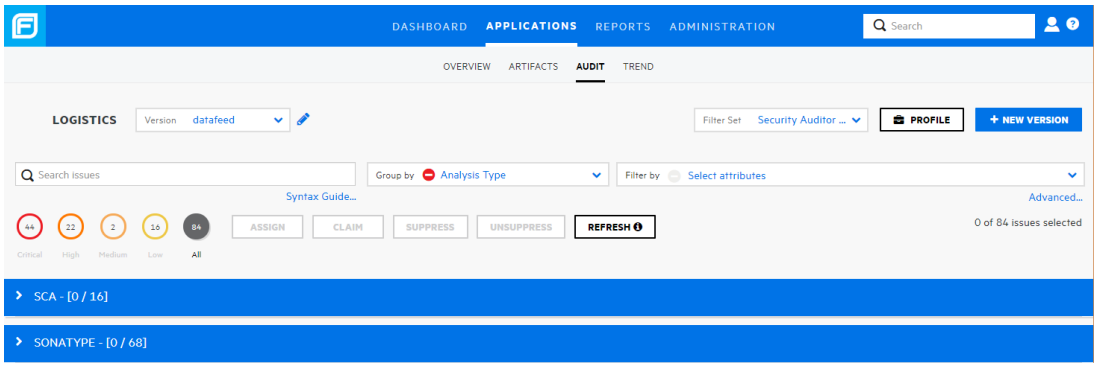
Fortify Software Security Center用のSonatypeパーサプラグインをダウンロード、インストール、および有効化した後(1ページの"Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164を参照)、アプリケーションバージョン用にFortify Software Security CenterにアップロードされたSonatype脆弱性データを表示できます。

アプリケーションバージョンにアップロードされたSonatype結果は、 [AUDIT]ページまたは [OPEN SOURCE]ページから表示できます。

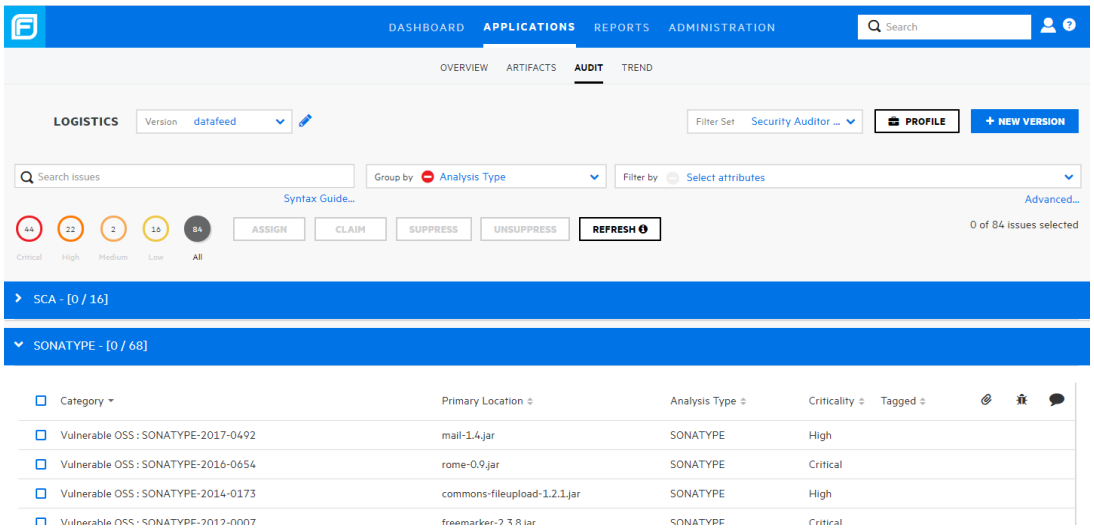
[AUDIT]ページでのSonatypeデータの表示

Sonatype脆弱性の結果を [AUDIT]ページから表示するには、次の手順に従います。

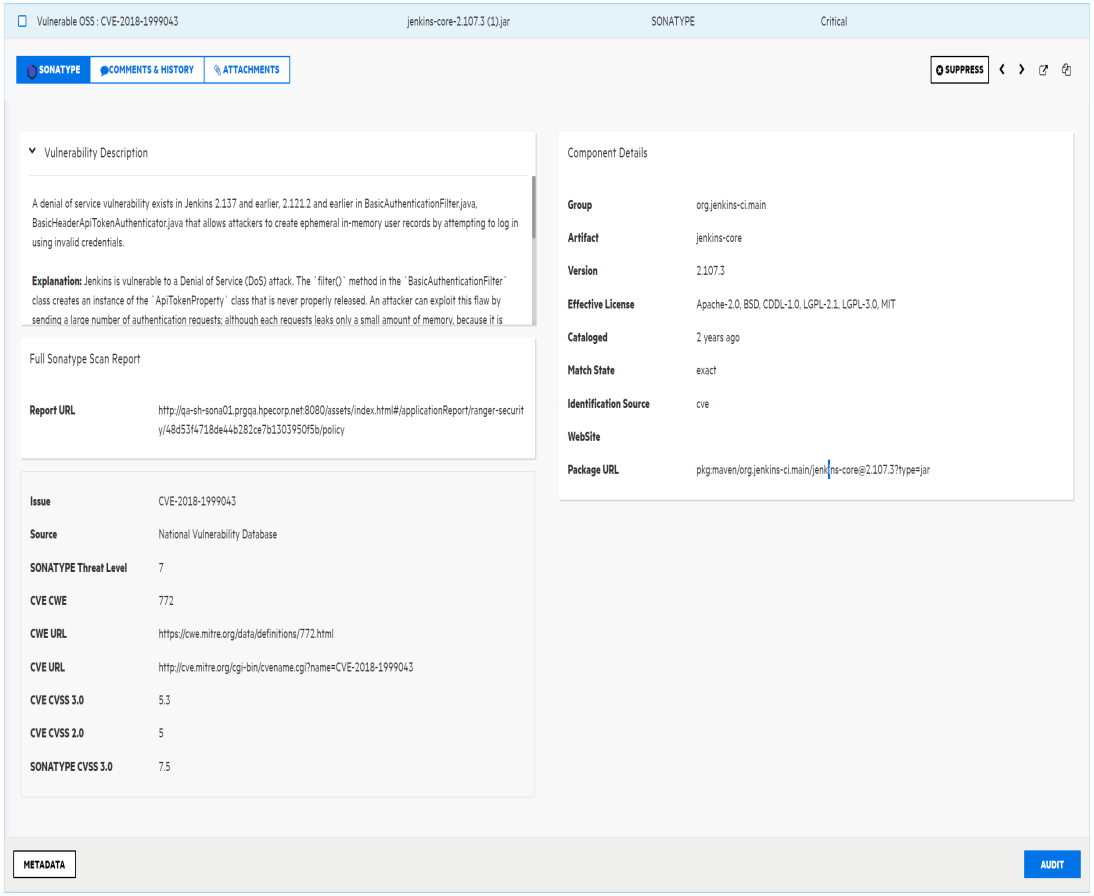
1. Fortifyのヘッダで、 [**APPLICATIONS**]をクリックします。
2. [Applications]ビューで、目的のアプリケーションの行を展開し、Sonatype結果がアップロードされているバージョンを選択します。
   [AUDIT]ページが開きます。
3. [**Group by**]リストから [**Analysis Type**]を選択します。



4. [**SONATYPE**]ヘッダを展開します。



5. 結果を調べる行を展開します。



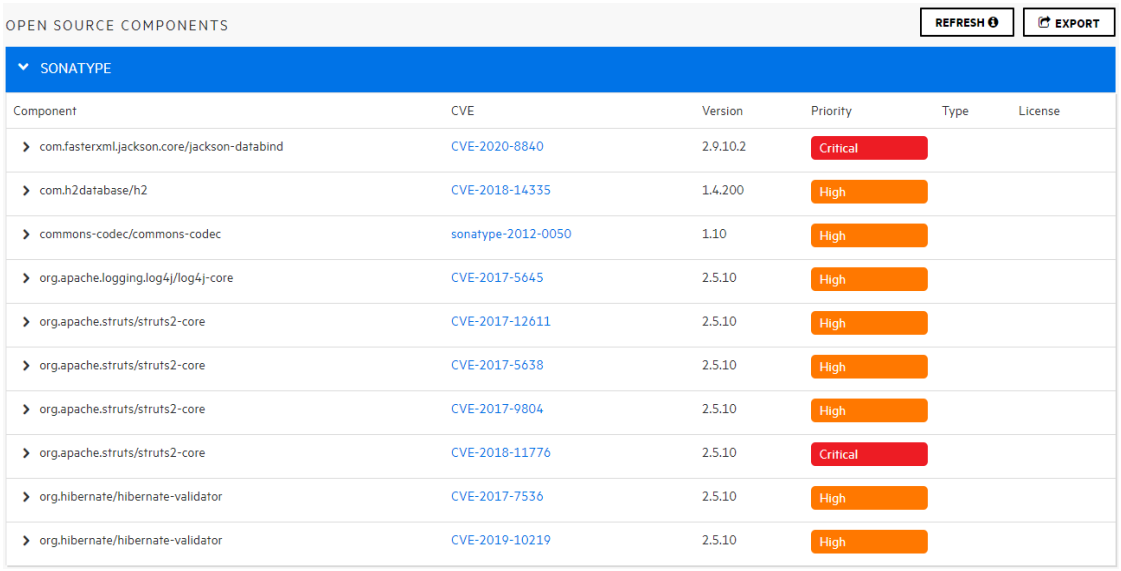
表示されるSonatype脆弱性データを解釈する方法については、Sonatypeのドキュメントを参照してください。

Sonatypeデータを監査する方法については、1ページの"Sonatype結果の監査" ページ342を参照してください。

[OPEN SOURCE]ページでのSonatypeデータの表示

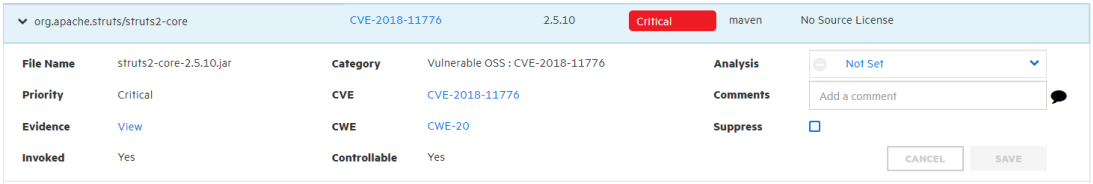
Sonatype結果を[OPEN SOURCE]ページから表示するには、次の手順に従います。

1. Fortifyのヘッダで、[APPLICATIONS]をクリックします。
2. [Applications]ページで、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。
   [AUDIT]ページが開きます。
3. ページヘッダで、[OPEN SOURCE]をクリックします。



注: [OPEN SOURCE]ページは、選択したアプリケーションバージョンに対して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
File Name	問題が検出されたコンポーネントファイルの名前。

フィールド	説明
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)	[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	[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	SourceAndLibScannerを使用して、Fortify Static Code AnalyzerスキャンとコードのSonatype OSSスキャンを実行し、結果のアーティファクトをFortify Software Security Centerにアップロードした場合、このフィールドが表示されます。 Sonatype脆弱性が呼び出された、制御可能、またはその両方の場合は、[**View**]リンクをこのフィールドで使用できます。リンクをクリックすると、[AUDIT]ページの被影響性分析に対応するソースコードが表示されます。
CWE	Common Weakness Enumeration。このリンクをクリックすると、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。
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" ページ324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。値が「Yes」の場合、

フィールド	説明
	[Evidence]フィールドに [View]リンクが表示されます。
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。値が「Yes」の場合、 [Evidence]フィールドに [View]リンクが表示されます。

Sonatypeデータフィールドの詳細については、Sonatypeのドキュメント(https://help.sonatype.com/docs)を参照してください。

参照情報

"Sonatype結果の監査" 下

"Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ164

"Webアプリケーションの被影響性分析について" ページ336

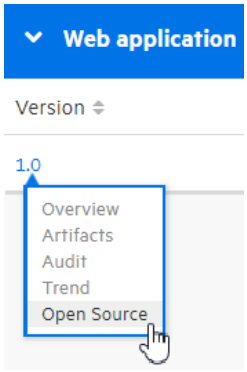
Sonatype結果の監査

Sonatypeの結果を監査するには、プライマリカスタムタグの値を設定し、必要に応じてコメントを追加します。Sonatype脆弱性は、 [OPEN AUDIT]ページ、または [OPENSOURCE]ページから監査できます。

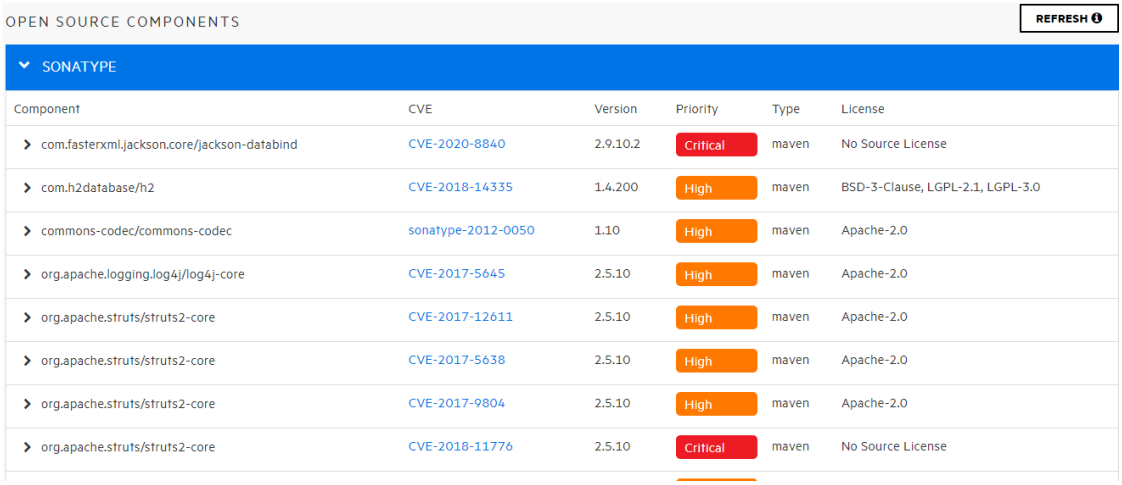
注: プライマリタグ値に加えた変更と、 [AUDIT]ページから追加したコメントは、自動的に [OPEN SOURCE]ページに反映されます。同様に、プライマリタグ値に加えた変更と、 [OPEN SOURCE]ページから追加したコメントは、 [AUDIT]ページに自動的に反映されます。

[OPEN SOURCE]ページでのSonatype問題の監査

[AUDIT]ページからアップロードされたSonatype結果を監査するには、次の手順に従います。



1. [DASHBOARD]または [APPLICATIONS]ビューから、Sonatype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の [OPEN SOURCE]ページを開きます。



2. 監査する脆弱性の行をクリックします。

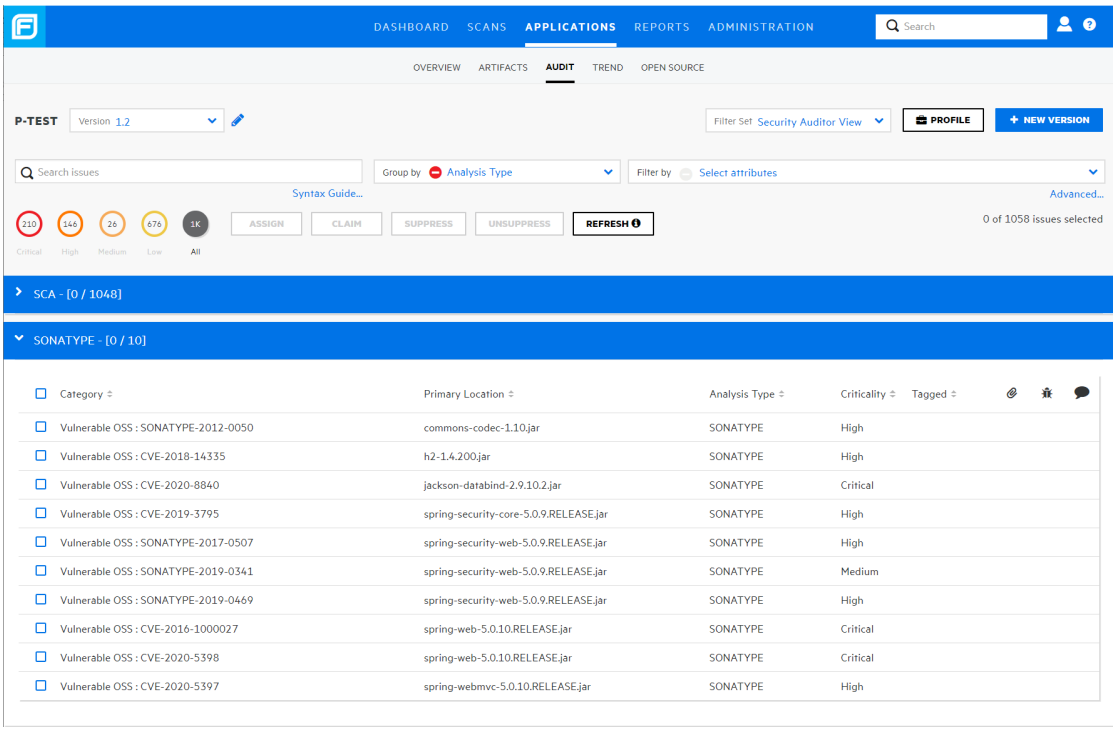
3. [Analysis](またはプライマリタグとして設定された他のタグ)リストから、問題のプライマリタグ値を選択します。
4. (オプション) [Comments]ボックスに、監査用に保存するコメントを入力します。
5. (オプション)問題に懸念がないと思う場合は、このチェックボックスをオンにします。問題の抑止の詳細については、"抑止、削除、および非表示の問題について" ページ 324を参照してください。
6. [SAVE]をクリックします。

変更は、[AUDIT]ページでも同じ問題に反映されます。

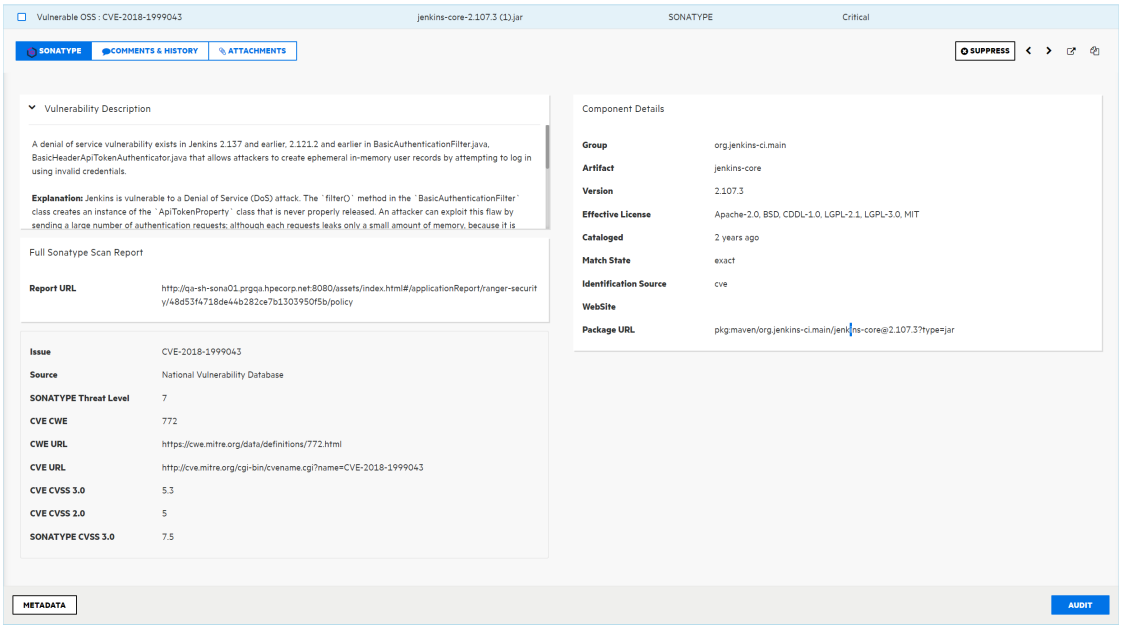
[AUDIT]ページでのSonatype問題の監査

[AUDIT]ページからアップロードされたSonatype結果を監査するには、次の手順に従います。

1. アプリケーションバージョンの [AUDIT]ページを開き、監査するSonatypeデータを表示します。(手順については、"Sonatypeデータの表示" ページ338を参照してください。)

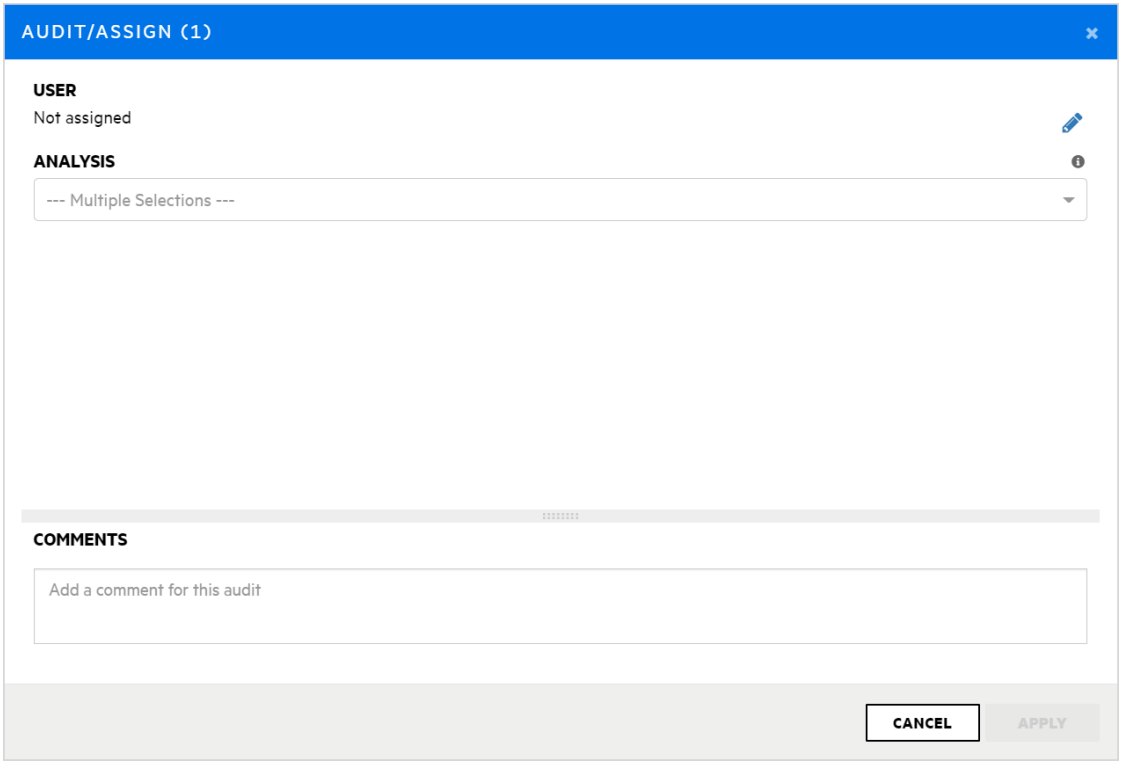


2. 脆弱性を展開して詳細を表示するには、テーブル内の該当する行をクリックします。



ヒント: 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、[**Open in a new tab**]アイコン( )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、[**Copy issue link to clipboard**]アイコン( )をクリックします。

3. (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、 [SUPPRESS]をクリックします。
4. [SONATYPE]タブで、 [AUDIT]をクリックします。



5. 修 正 を問 題 に割 り当 てるには、次 の手 順 に従 います。
   a. [USER]で、 [Assign user]アイコンを選 択 します。
      [SELECT USER]ダイアログボックスが開 きます。
   b. 問 題 に割 り当 てるユーザを見 つけるには、 [Find user]ボックスにユーザ名 の一 部 またはすべてを入 力 し、 [FIND]をクリックします。または、システム内 のすべてのユーザを一 覧 表 示 するには、 [Find all users]チェックボックスをクリックします。
   c. 問 題 に割 り当 てるユーザを見 つけるには、 [Find user]ボックスにユーザ名 の一 部 またはすべてを入 力 し、 [FIND]をクリックします。
   d. 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、 [DONE]をクリックします。
      [Assigned]セクションに、修 復 者 として割 り当 てたユーザの名 前 が一 覧 表 示 されます。
6. [ANALYSIS]リストで、この問 題 の評 価 を反 映 する値 を選 択 します。
7. (オプション)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、これらのタグの値 を指 定 します。

アプリケーションバージョンの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してください。そうしないと、Fortify Software Security Centerでこの問題は未監査として扱われます。

8. (オプション)脆弱性に関するコメントを追加するには、右ペインの下部にあるテキストボックスにコメントを入力します。(監査設定を保存した後、[COMMENTS]セクションにはコメント、および以前に保存した他のコメントが一覧表示されます)。
9. [APPLY]をクリックします。

監査設定が保存されます。

参照情報

"Webアプリケーションの被影響性分析について" ページ336

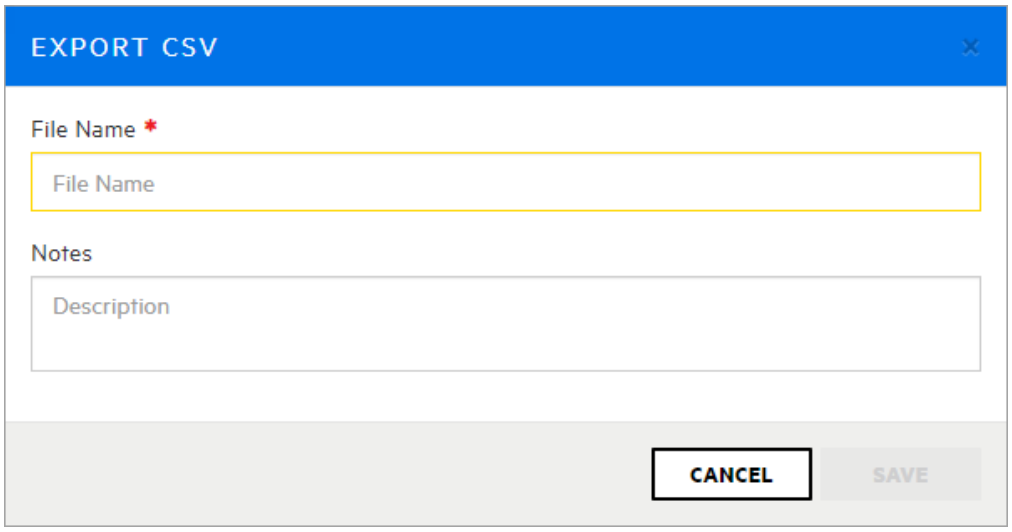
"Sonatypeデータの表示" ページ338

Sonatypeデータをエクスポートする

[OPEN SOURCE COMPONENTS]ページに表示されているSnatypeデータをエクスポートするには:

1. Fortify Software Security Center のアプリケーションバージョンのSnatypeデータをアップロードした後、アプリケーションバージョンの [OPEN SOURCE COMPONENTS] ページに移動します。

2. [OPEN SOURCE COMPONENTS]テーブルの上で、 [EXPORT]をクリックします。



3. [EXPORT CSV]ダイアログボックスが開きます。
4. [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。
5. (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。
6. [SAVE]をクリックします。

7. エクスポートされた結 果 を表 示 するには:
   a. Fortifyのヘッダで、 [REPORTS]をクリックします。
   b. [レポート]ページで、 [DATA EXPORTS]タブをクリックします。
   c. 結 果 のテーブルで、エクスポートされたファイルの行 にカーソルを移 動して、 [ダウンロード]アイコン 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 を決 定 するには、"ジョブスケジューラの設 定 " ページ131に記 載 されている手 順 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。

Fortify Software Security CenterとFortify WebInspect Enterpriseの統 合

Fortify Software Security Center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WebInspect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、Fortify Software Security CenterWebInspectの結 果 をFortify Software Security Center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Fortify Software Security Centerのユーザに示します。

Fortify Software Security CenterでのFortify WebInspectスキャン結 果 の表 示

Fortify WebInspect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Fortify Software Security Center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 " ページ288)。Fortify WebInspectの問 題 の詳 細 は、その他 のアナライザ(Fortify Static Code Analyzerなど)で見 つかった問 題 に表 示 される問 題 とは多 少 異 なります。

重 要 Fortify WebInspectをFortify Software Security Centerと正 常 に統 合 するには、Fortify Software Security CenterサーバとWebInspect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

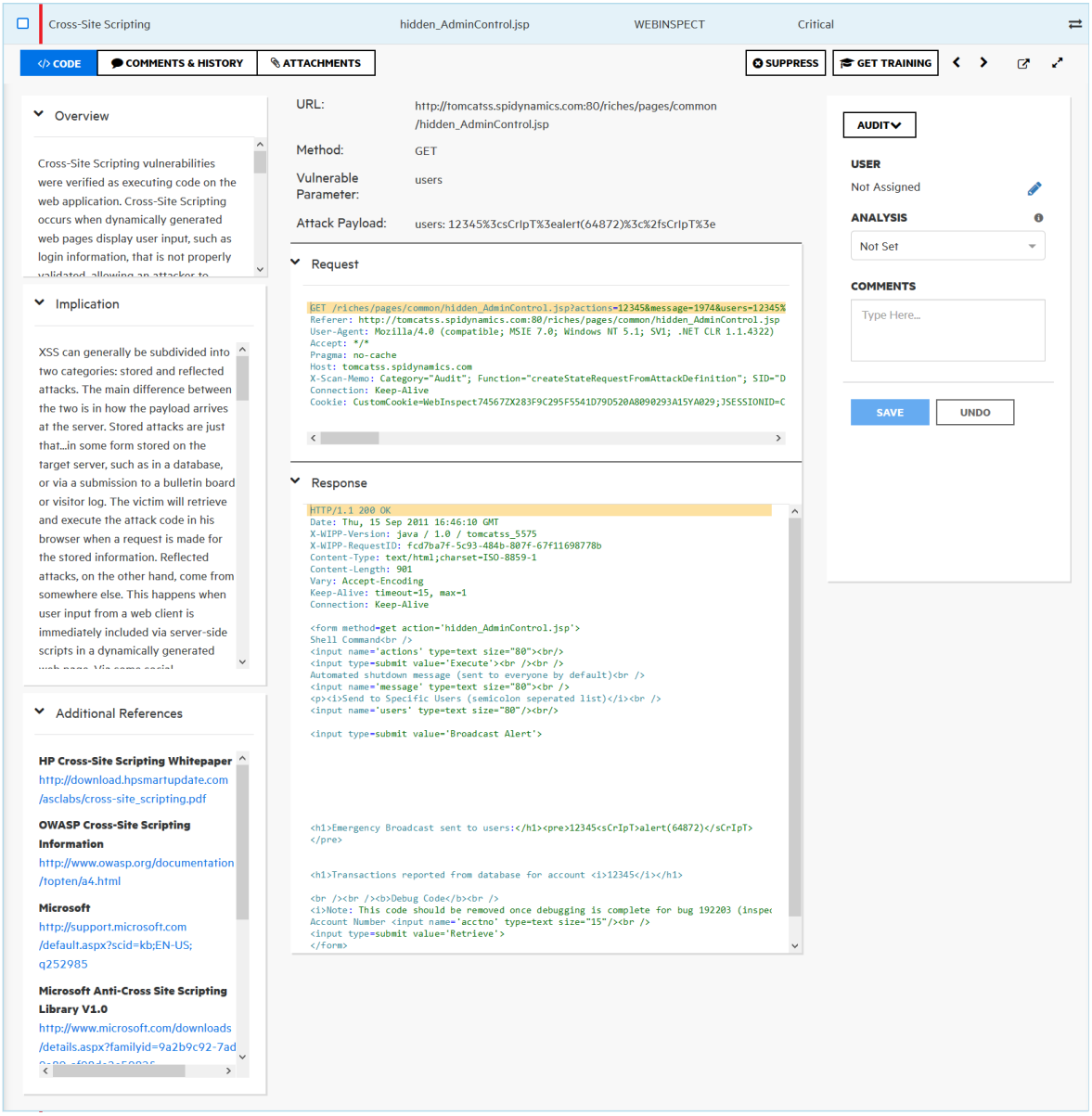
Method: 攻 撃 に使 用 されるHTTPメソッド (GET、PUT、POSTなど)

Vulnerable Parameter: 脆 弱 なパラメータの名 前

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。

注 : 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。



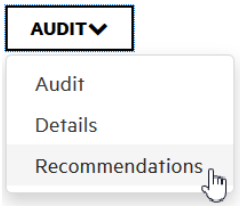
[Steps]タブは、ステップがWebInspectの結果ファイルに含まれている場合にのみ使用できます。

追加の詳細と推奨事項の表示

問題に関する追加の詳細と推奨事項を表示するには、問題ツールバーで次のいずれかをクリックします。

- **Open in new tab**
- **Expand to full screen**

右側の [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、 [DETAILS]リストから [Recommendations]を選択します。

右側にあるペインを使用して問題を監査する方法については、"Fortify Scan結果の監査" ページ317を参照してください。

WebInspectの監査データ

スクリーンショットに加えて、次の種類の監査データがWebInspectからFortify Software Security Centerに転送されます。

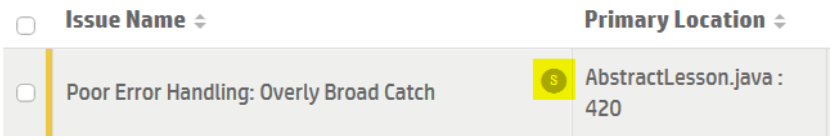
- **脆弱性メモ**。WebInspectの脆弱性メモは、問題コメントとしてFortify Software Security Centerに転送されます。
- **無視された脆弱性**。WebInspectで [Ignored]マークが付けられた脆弱性は、Fortify Software Security Centerへの転送時に [Suppressed]マークが付けられます。
- **誤検出**。

誤検出

Fortify Software Security Center には、Fortify WebInspect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。Fortify WebInspect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 Fortify Software Security Center 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。Fortify Software Security Center でFortify WebInspectの誤検出に [Analysis]値「問題でない」が割り当てられます。Fortify

WebInspect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**」としてマークされます。



注 : 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

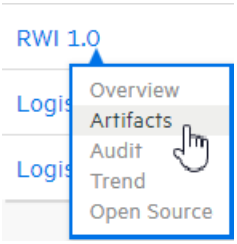
"問題の表示設定の設定" ページ325

動的スキャン要求をFortify WebInspect Enterpriseに送信する

WebInspect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は、WebInspectスキャンをFortify Software Security Center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. [Dashboard] で、スキャンするアプリケーションバージョンにカーソルを移動し、ショートカットメニューから [**Artifacts**] を選択します。
2. [ARTIFACT HISTORY] ページで、 [**DYNAMIC SCAN**] をクリックします。
   [DYNAMIC SCAN - <*APPLICATION VERSION*>] ダイアログボックスが開きます。
3. 次の表で説明する情報を入力します。

   注 : 次の表に、ユーザまたは別のFortify Software Security Center管理者がシステムに追加したカスタムダイナミックスキャン属性は含まれまていません。

ダイナミックスキャン属性 * (必須フィールド)	説明
*URL	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。手順については、"Fortify WebInspect Enterpriseの動的スキャン要求の処理" 次のページを参照してください。
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。

注: WebInspect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。

Fortify Software Security Center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WebInspectテスタは、指定した時間にスキャンを実行し、Fortify Software Security Centerに結果をアップロードします。

5. Fortify Software Security Center管理者またはアプリケーションセキュリティテスタの場合は、WebInspect Enterpriseから要求された動的スキャンを直ちに実行できます。手順については、"Fortify WebInspect Enterpriseの動的スキャン要求の処理" 下を参照してください。

参照情報

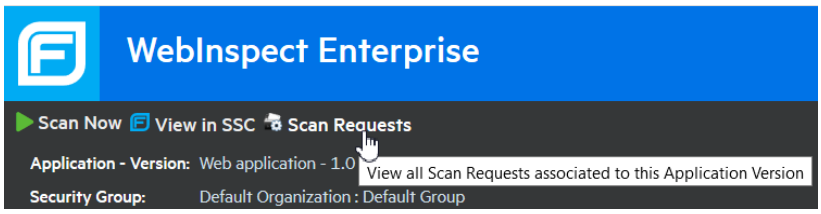
"Fortify Software Security CenterでのFortify WebInspectスキャン結果の表示" ページ 347

Fortify WebInspect Enterpriseの動的スキャン要求の処理

管理者またはアプリケーションセキュリティテスタの役割を持っている場合は、Fortify WebInspect Enterpriseを起動して、Fortify Software Security Center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。

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。

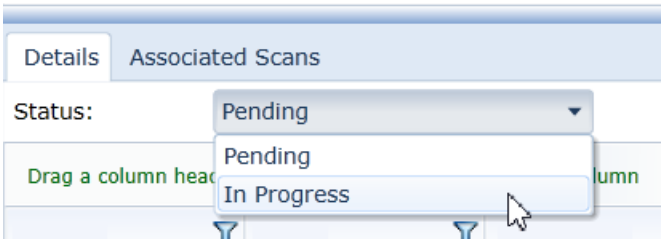
1. Fortify WebInspect EnterpriseでFortify Software Security Centerを初期化してから、WebInspect Enterprise Consoleを使用してFortify Software Security Centerアプリケーションバージョンを WebInspectプロジェクトと同期します。(手順については、『Micro Focus Fortify WebInspect Enterpriseユーザガイド』を参照してください)。
2. Fortify Software Security Centerの［Dashboard］で、動的スキャンが要求されているアプリケーションバージョンにカーソルを移動し、ショートカットメニューから［**Artifacts**］を選択します。
3. ［ARTIFACTS］ページで、［**LAUNCH WIE**］をクリックします。



4. Fortify WebInspect Enterpriseのヘッダで、［**Scan Requests**］をクリックします。

［SCAN REQUESTS］ビューには、Fortify Software Security Center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、Fortify Software Security Center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、Fortify Software Security Centerに結果をアップロードします。詳細な手順については『Micro Focus Fortify WebInspect Enterpriseユーザガイド』を参照してください。

参照情報

"動的スキャン要求をFortify WebInspect Enterpriseに送信する" ページ350

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現在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。

Fortify Software Security Center 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" ページ350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。

動的スキャン要求の保留中は、その要求を編集またはキャンセルできます。ただし、スキャンが開始されるとすぐに、編集またはキャンセルできなくなります。

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:

注: 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。
   [Dynamic Scan Request]ダイアログボックスが開きます。
3. 動的スキャン属性の値を編集してから、 [送信する]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。

注 : 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。
   Fortify Software Security Center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。

第16章: Fortify ScanCentral SASTの使用

Fortify Software Security Center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、[Scan Requests]ページ、[Sensors]ページ、[Controller]ページ、および[Sensor Pools]ページが表示されます。次のセクションでは、これらのページと機能について説明します。Fortify Software Security CenterとScanCentral SAST間の接続を設定する方法については、"Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設定" ページ130を参照してください。

このセクションで説明するトピック:

ScanCentral SASTの許可

次の表は、ScanCentral SAST関連タスクを実行する権限を持つFortify Software Security Centerの役割を示しています。

注: 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、『Micro Focus 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	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、ScanCentral SAST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バージョンのスキャン要求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バージョンのセンサプール割り当てだけを表示できます
管理者 セキュリティリード マネージャ	「Scan Requests」、「Sensors」、および「Sensor Pools」ページの情報の表示 センサプールの変更を伴うすべてのタスクの実行 スキャン要求のキャンセル センサプールへのセンサとアプリケーションバージョンの割り当て。 **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。
管理者	ScanCentral SASTデータの表示、ダウンロード、および管理
セキュリティリード	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、ScanCentral SASTデータの表示、ダウンロード、および管理 **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。
マネージャ	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、ScanCentral SASTデータの表 示 、ダウンロード 、および管 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。
開 発 者	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、ScanCentral SASTデータを表 示します。

各 Fortify Software Security Centerの役 割 が実 行 できるアクションを確 認 するには、次の手 順 に従 います。

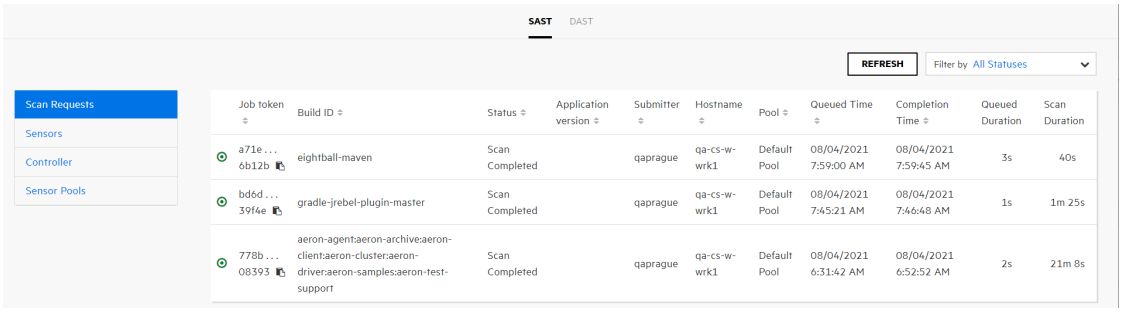
1. Fortifyのヘッダで、 [ADMINISTRATION]を選 択します。
2. 左 ペインで、 [Users]、 [Roles]の順 に選 択します。
   [Roles]テーブルに、ユーザに割り当 てることができるすべての役 割 のリストが表 示されます。
3. 特 定 の役 割 でユーザが実 行 できるアクションをすべて表 示 するには、その役 割 の行をクリックします。

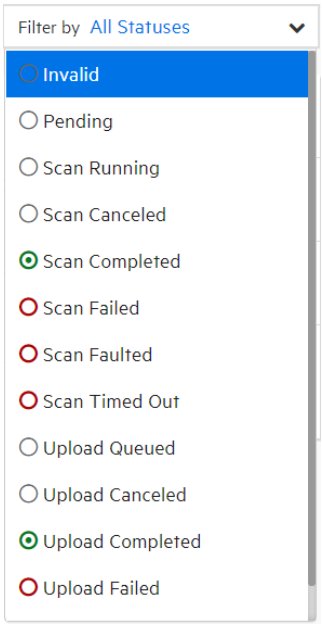
ScanCentral SASTスキャン要 求 の詳 細 の表 示

ScanCentral SASTスキャン要 求 の詳 細 を表 示します。

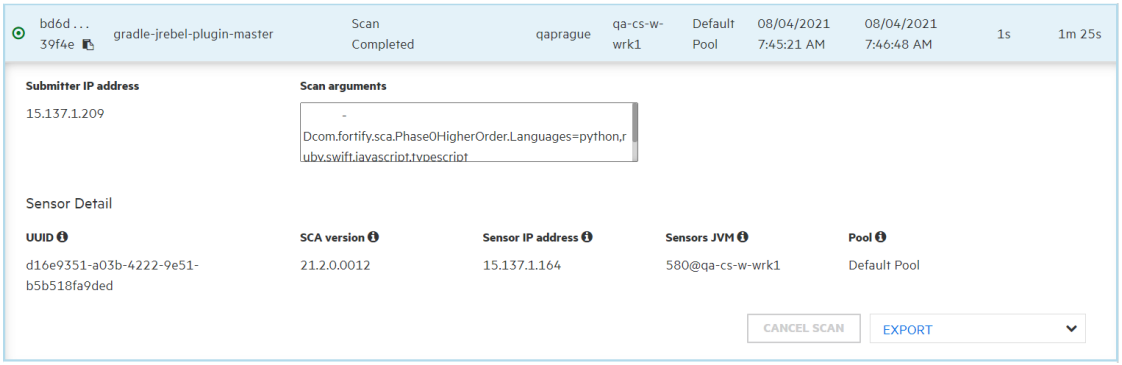
注 : 静 的コード分 析 プロセスを合 理 化 するために、Fortify ScanCentral SASTをインストール、設 定 、および使 用 する方 法 については、『*Micro Focus Fortify ScanCentral SASTインストール、設 定 、および使 用 ガイド*を参 照 してください。

1. Fortifyのヘッダで、 [SCANCENTRAL]をクリックし、 [SAST]タブを選 択します。
   [Scan Requests]ページに、すべてのスキャン要 求 とそれぞれの詳 細 のリストが表 示されます。





2. (オプション)現 在 の状 態 に基 づいて表 示 された要 求 をフィルタ処 理 するには、 [**Filter by**]リストから状 態 を選 択 します。
3. 行 を展 開 し、特 定 のスキャンに関 する詳 細 を表 示 するには、その行 をクリックしま す。



4. スキャン要 求 の詳 細 をエクスポートするには、次 の手 順 に従 います。
   a. [**EXPORT**]リストから、[**FPR**]を選 択 してスキャンで見 つかった脆 弱 性 のある FPRファイルをエクスポートするか、[**Log**]を選 択 してスキャンからログファイルをエク

スポートします。

b. エクスポートされたファイルの場 所を指 定します。

5. 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

"ScanCentral SASTスキャン要 求のキャンセル" 下

"ScanCentral SASTセンサ情 報の表 示" 下

"ScanCentral Controller情 報の表 示" 次のページ

ScanCentral SASTスキャン要 求のキャンセル

注 : 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、『*Micro Focus 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。

保 留 中 のScanCentralスキャン要 求をキャンセルするには、次 の手 順を実 行します。

1. Fortifyのヘッダで、 [SCANCENTRAL]をクリックします。
   [SAST]ページが開き、 [Scan Requests]タブにすべてのスキャン要 求 が一 覧 表 示されます。
2. 現 在 の状 態 に基 づいて表 示された要 求をフィルタ処 理するには、 [Filter by]リストから [Pending]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. 右 下の [CANCEL SCAN]をクリックします。
   Fortify Software Security Centerに、要 求のキャンセルを確 認するメッセージが表 示されます。
5. キャンセルを確 認します。
6. [Scan Requests]テーブルに表 示されるデータを更 新するには、 [REFRESH]をクリックします。

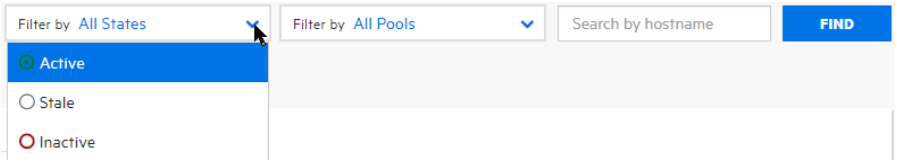
ScanCentral SASTセンサ情 報の表 示

ScanCentral SAST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 示します。

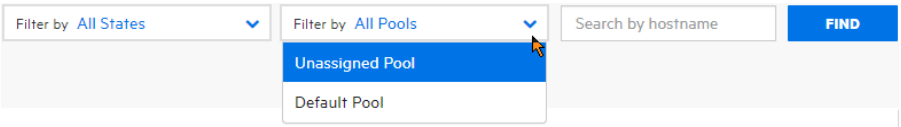
注 : 静 的コード分 析プロセスを合 理 化 するために、Fortify ScanCentral SASTをインストール、設 定 、および使 用する方 法については、『*Micro Focus Fortify ScanCentral SASTインストール、設 定 、および使 用ガイド*を参 照してください。

1. Fortifyのヘッダで、 [SCANCENTRAL]をクリックします。
2. [SAST]タブを選 択します。
3. 左 側 のペインで、 [Sensors]を選 択します。

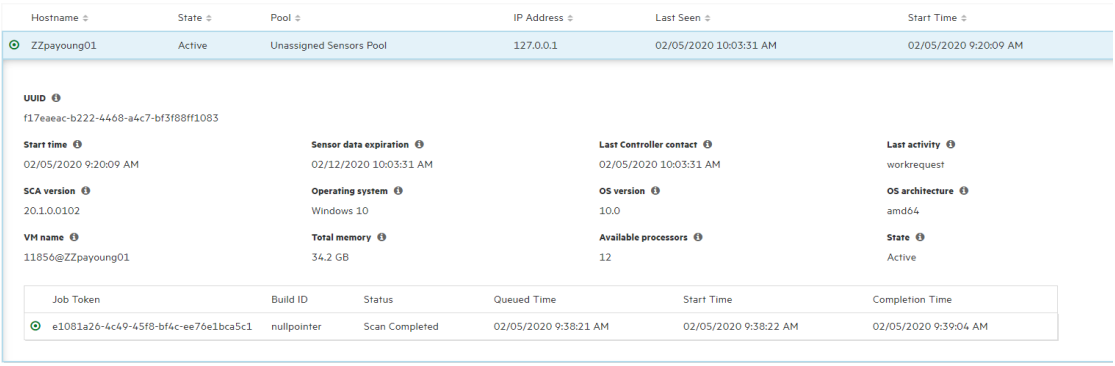
センサの状 態は [active]、 [inactive]、または [stale]です。



4. 現 在 の状 態 ([Active]、 [Inactive]、または [Stale])に基 づいて表 示 されるセンサをフィルタ処 理 するには、1番 目 の [Filter by]リストから状 態 を選 択 します ([All States]がデフォルトです)。



5. それぞれ割 り当 てられたプールに基 づいて表 示 されたセンサをフィルタ処 理 するには、2番 目 の [Filter by]リストから [Unassigned Pool]、名 前 付 きプール、または [All Pools](デフォルト)を選 択 します。
6. 行 を展 開 し、センサに関 する詳 細 を表 示 するには、その行 をクリックします。



参照情報

"ScanCentral SASTスキャン要 求 のキャンセル" 前 のページ

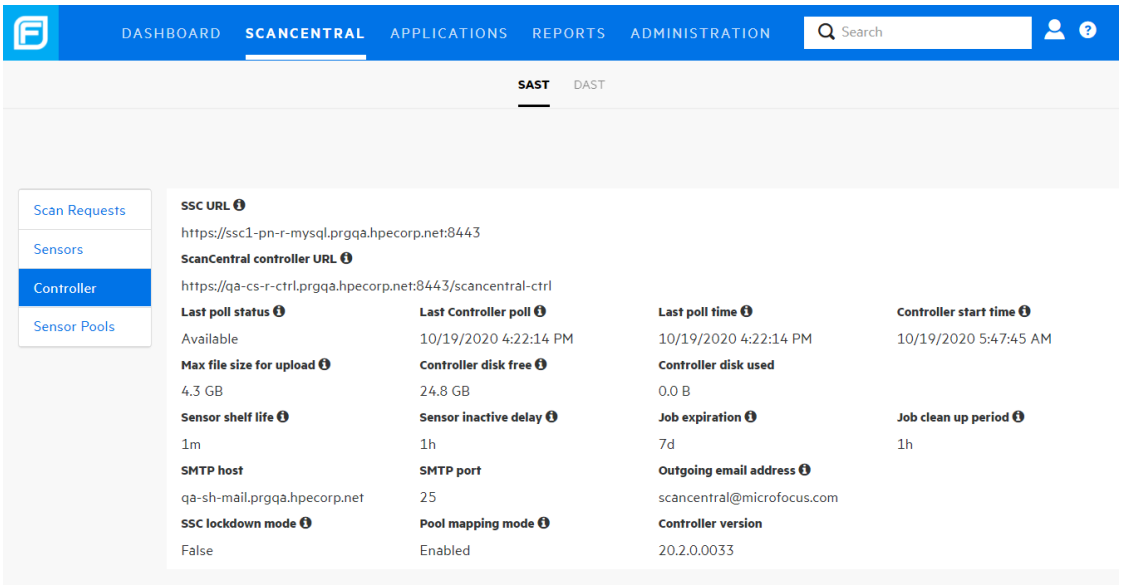
"ScanCentral SASTスキャン要 求 の詳 細 の表 示 " ページ357

ScanCentral Controller情 報 の表 示

ScanCentral Controllerの情 報 を表 示 します。

注 : 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、『*Micro Focus 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。

1. Fortifyのヘッダで、 [SCANCENTRAL]をクリックします。
2. 左 側 のペインで、 [Controller]を選 択 します。



3. 表 示される各 値 については、情 報 アイコン(ℹ)をクリックします。

参 照 情 報

"ScanCentral SASTスキャン要 求 の詳 細 の表 示" ページ357

"ScanCentral SASTスキャン要 求 のキャンセル" ページ359

"ScanCentral SASTセンサ情 報 の表 示" ページ359

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、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Fortifyでは強 く推 奨 します。("ScanCentral SAST Controllerを保 守 モード にする" 次 のページを参 照 してください)。

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、Tomcatのbinディレクト リに移 動 します。

   Windowsシステムの場 合 :

   ```
   cd <controller_dir>\tomcat\bin
   ```

   Linuxシステムの場 合 :

   ```
   cd <controller_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

"ScanCentral SAST Controllerを保 守 モードにする" 下

ScanCentral SAST Controllerを保 守 モードにする

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。

次 の手 順 では、Controllerを保 守 モードにする方 法について説 明します。

重 要 Controllerを保 守 モードにする場 合 、Controllerはバージョン21.2.0以 降 である必 要 があります。

Controllerを保 守 モードにする

1. Fortify Software Security Centerに管 理 者 としてログオンし、Fortifyのヘッダで［**SCANCENTRAL**］をクリックします。
2. SASTページの左 ペインで、［**Controller**］を選 択します。
3. ［**START MAINTENANCE MODE**］をクリックします。

ControllerはFortify Software Security Centerから保 守 要 求を受 け取り、センサがスキャンを実 行している場 合 は、ControllerのモードがACTIVEからWAITING_FOR_JOB_COMPLETEDに変 わります。ジョブが処 理されていない場 合 、モードは直 接 ACTIVEから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。

センサの安 全 なシャットダウン

このセクションでは、ScanCentral SASTセンサをシャットダウンに移 行 する方 法 、またはスケジュールされたモードをFortify Software Security Centerからシャットダウンする方 法について説 明します。

重 要 コントローラが保 守 モードの場 合 (ページ1の「ScanCentral SAST Controllerを保 守 モードにする」"ScanCentral SAST Controllerを保 守 モードにする" 上 を参照)、Fortify Software Security Center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。また、Fortify Software Security Center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には、センサのバージョンが21.2.0以 降 である必 要 があります。

センサのシャットダウン

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. Fortify Software Security Centerに管 理 者 としてログオンし、Fortifyのヘッダで［SCANCENTRAL］をクリックします。
2. ［SAST］タブの左 ペインで、［センサ］を選 択します。
3. センサテーブルで、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。

注 : ［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。

- センサバージョンが21.2.0より前
- 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。

ScanCentral SAST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. Fortify Software Security Centerに管 理 者 としてログオンし、Fortifyのヘッダで［SCANCENTRAL］をクリックします。
2. SASTページの左 ペインで、［CONTROLLER］を選 択します。
3. ［END MAINTENANCE MODE］をクリックします。

参 照 情 報

"ScanCentral SAST Controllerを保 守 モードにする" 前 のページ

"コントローラの停 止 " ページ361

ScanCentral SASTセンサプールについて

Fortify Software Security Center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。これらのグループは、スキャン要 求 のターゲットに設 定 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詳細に制御できます。センサプールの使用例を次に示します。

- センサのコンピューティング能力(物理メモリのサイズ)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。
- 組織のチームまたは事業部に基づいてプールを作成し、リソースが分散されることで、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いようにします。

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る場合、コントローラは使用可能なセンサプールをFortify Software Security Center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、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。

注: 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、『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

Fortify Software Security Center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。[Use unassigned sensors]チェックボックスが選択されている場合、デフォルトセンサプールでは未割り当てセンサプールのセンサを使用します。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

"ScanCentral SASTセンサプールの作成" 下

"ScanCentral SASTの許可" ページ356

"ScanCentralプールの削除" ページ367

ScanCentral SASTセンサプールの作成

Fortify Software Security CenterサーバがScanCentral SASTと統合されている場合は、センサプールを作成して、スキャン要求をターゲットにできます。

注: 静的コード分析プロセスを合理化するために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、『Micro Focus 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. Fortifyのヘッダで、[SCANCENTRAL]を選択します。
2. [SAST]タブを選択します。
3. 左側のペインで、[Sensor Pools]を選択します。

［Sensor Pools］ページには、デフォルトプールとシステム上 に作 成されたその他 のセンサプールが一 覧 表 示されます。

注 : 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。

4. ［+ NEW POOL］をクリックします。

注 :

［+ NEW POOL］ボタンが無 効 な場 合 は、Fortify Software Security Center がコントローラに接 続されていない状 態 を示します。このボタンが無 効になっている場 合 は、［SCANCENTRAL SAST CONFIGURATION］設 定 を確 認します ("Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設 定 " ページ130を参 照)。

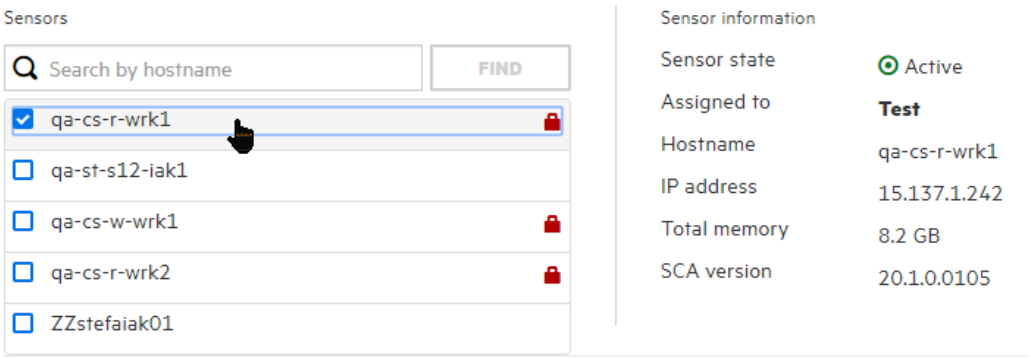
［CREATE NEW POOL］ダイアログボックスが開きます。

5. ［Name］ボックスに、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、または 0～9)。
6. (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。
7. 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。

注 : ［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。その代 わり、プールでは割り当 てられていない使 用 可 能 なセンサを利 用 できます。センサは割り当 てられていないままです。

注 : 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 のアイコンは、センサが既 存 のプールに割り当 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、その行 を選 択します。右 側 の［Sensor information］セクションには、現 在 割り当 てられているプールを含 む、センサに関 する基 本 情 報 が一 覧 表 示されます。



8. 特 定 のセンサを検 索 するには、テーブルの上 部 にある検 索 ボックスにホスト名 を入 力し、 [FIND]をクリックします。
9. 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。
10. 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、次 の手 順 を実 行します。

    a. [Versions]で [ADD]をクリックします。

    [SELECT APPLICATION VERSION]ダイアログボックスが開きます。

    b. [APPLICATION]ペイン(左)で、このプールに割 り当 てるバージョンのアプリケーションを選 択します。

    [VERSIONS]ペイン(中 央)には、選 択したアプリケーションのアクティブなすべてのバージョンが一 覧 表 示 されます。

    c. 選 択したアプリケーションの任 意 の非 アクティブバージョンを一 覧 表 示 するには、[Show inactive versions]チェックボックスをオンにします。

    d. 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、[Select All]チェックボックスをオンにします。そうではなく、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、バージョン名 の横 のチェックボックスをオンにします。

    [SELECTED VERSIONS]ペイン(右)に選 択 内 容 が一 覧 表 示 されます。

e. 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。

f. [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 にあるごみ箱 アイコン( )をクリックします。

g. [DONE]をクリックします。

[CREATE NEW POOL]ダイアログボックスで、 [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。表 の [Pool]列 には、含まれるセンサの新 しいプール名 も一 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" 下

"ScanCentral SASTセンサ情 報 の表 示" ページ359

ScanCentralプールの削 除

ScanCentralプールを削 除 するには、次 の手 順 を実 行します。

1. Fortifyのヘッダで、 [SCANCENTRAL]を選 択します。
   [Scan Requests]ビューが開き、ScanCentralの [Scan Requests]ページが開きます。
2. 左 側 のペインで、 [Sensor Pools]を選 択します。
   [Sensor Pools]ページが開き、 [Sensor Pools]タブに既 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 [Delete Pool]アイコンが表 示 されます。アイコンが青 色 の である場 合 は、プールを削 除 できます。アイコンが灰 色 の である場 合 は、プールを削 除 できません。
3. 削 除 するプールに対 応 する [Delete Pool]アイコン をクリックします。

Fortify Software Security Center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

"ScanCentral SASTセンサ情 報 の表 示" ページ359

"ScanCentral SASTセンサプールの作 成" ページ364

第17章: Fortify ScanCentral DASTの使用

動的スキャンを要求および管理するために、Fortify Software Security CenterがFortify 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[Scans]ページ、[Sensors]ページ、[Sensor Pools]ページ、[Settings List]ページ、および[Schedules]ページが表示されます。Fortify Software Security CenterとScanCentral間の接続を設定する方法については、"Fortify Software Security Centerを使用したScanCentral DASTスキャンの実行と管理の有効化" ページ131を参照してください。

このセクションで説明するトピック:

ScanCentral DASTの許可

次の表は、ScanCentral DAST関連タスクを実行する権限を持つFortify Software Security Center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、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
管理者、セキュリティリード、およびマネージャ	• [Scan Requests]、[Sensors]、および[Sensor Pools]ページの情報の表示 • センサプールの変更を伴うすべてのタスクの実行 • スキャン要求のキャンセル • センサプールへのセンサとアプリケーションバージョンの割り当て。 **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	• DASTデータの表示 • 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 • DASTプールとセンサの管理 • DASTアーティファクトのダウンロード
マネージャ	• アプリケーションに割り当てられていないジョブを除き、ScanCentral SASTデータの表示、ダウンロード、および管理 • DASTデータの表示 • DAST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	• DASTデータの表示 • 既存の設定テンプレートを参照したDASTスキャンの実行 • DAST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	• DASTデータの表示 • 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 • DASTアーティファクトのダウンロード

各Fortify Software Security Centerの役割が実行できるアクションを確認するには、次の手順に従います。

1. Fortifyのヘッダで、［ADMINISTRATION］を選択します。
2. 左ペインで、［Users］、［Roles］の順に選択します。
   ［Roles］テーブルに、ユーザに割り当てることができるすべての役割のリストが表示されます。

3. 特 定 の役 割 でユーザが実 行 できるアクションをすべて表 示 するには、その役 割 の行 をクリックします。

ScanCentral DASTへの動 的スキャン要 求 の送 信

Fortify Software Security CenterがFortify 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、Fortify Software Security CenterからScanCentral DASTの動 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

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、『Micro Focus Fortify 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

"Fortify Software Security Centerを使 用 したScanCentral DASTスキャンの実 行 と管 理 の有 効 化 " ページ131

"ScanCentral DASTの許 可 " ページ368

第18章: BIRTレポート

Fortify Software Security Center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、EclipseのWebサイトで次のページを参照してください。

http://www.eclipse.org/birt/phoenix/intro

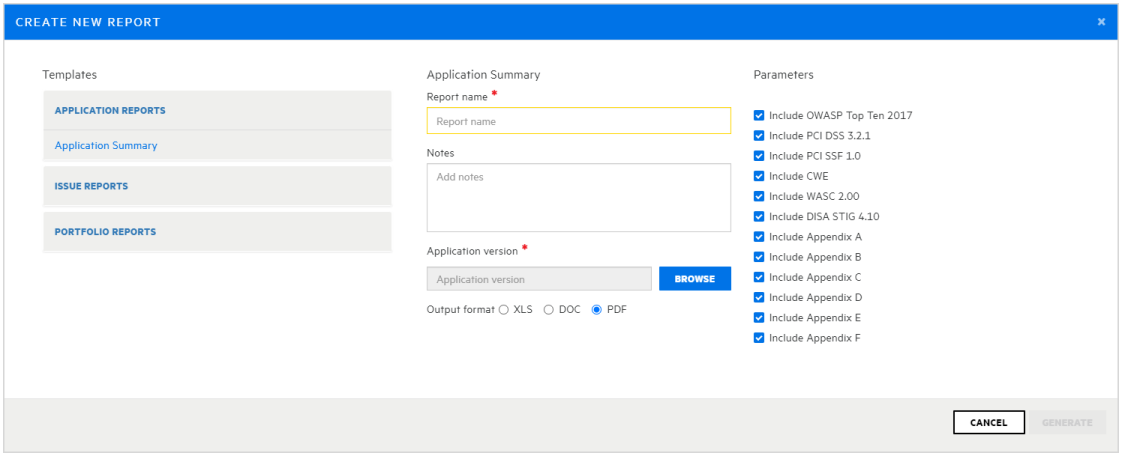
Fortify Software Security Centerでは、次のレポートカテゴリのテンプレートが提供されます。

- アプリケーションレポート:
  アプリケーションの単一バージョンの概要を表示するには、Application Summaryレポートを使用します。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、単一のFortify Software Security Centerアプリケーションバージョンに特定の脆弱性カテゴリが存在する場合の概要を示します。
- 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は、複数のFortify Software Security Centerアプリケーションバージョンの問題の傾向と指標を比較できるレポートが含まれています。

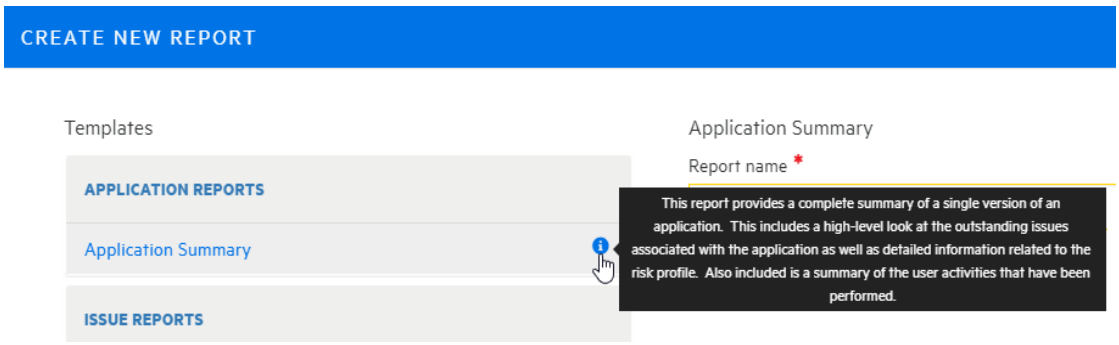
レポートを生成して表示する

Fortify Software Security Centerレポートを生成して表示するには:

1. Fortifyのヘッダで、[**REPORTS**]をクリックします。
   [**レポート**]ページが開きます。
2. [**レポート**]ページツールバーで、[**+ NEW REPORT**]をクリックします。

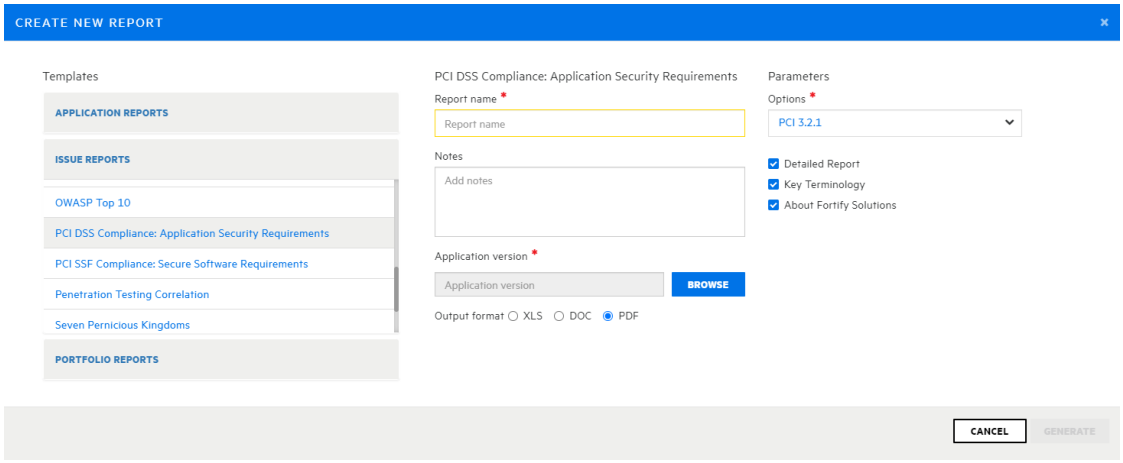


[CREATE NEW REPORT]ダイアログボックスが開きます。



一覧表示されたテンプレートから得られたレポートの説明を見るには、カーソルをレポートリストに移動して、情報アイコン ⓘ に移動します。

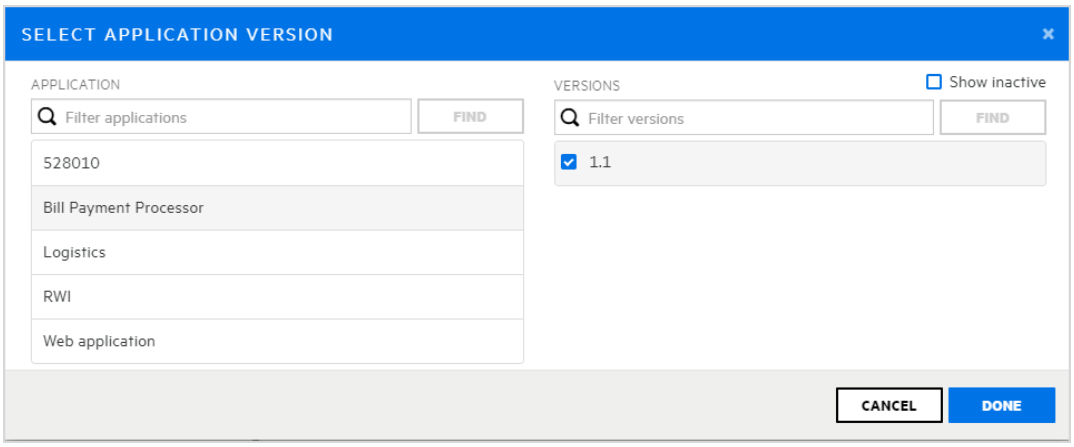
3. 使用するレポートテンプレートに移動して選択します。



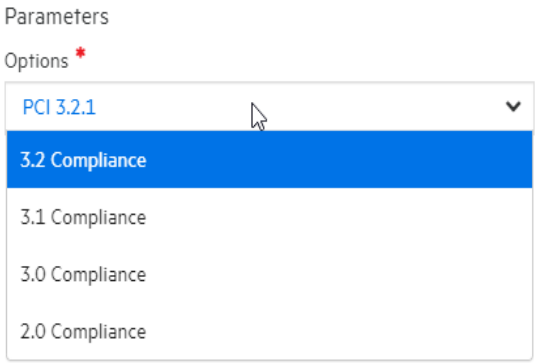
右側のペインには、選択したテンプレートの設定フィールドが表示されます。

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。

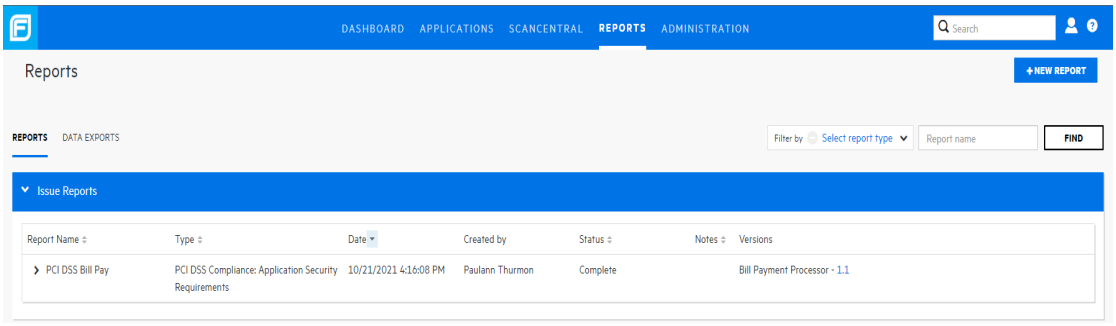
5. report に含めるアプリケーションバージョンを指定するには:
   a. [Application version]で、 [BROWSE]をクリックします。
      [SELECT APPLICATION VERSION]ダイアログボックスが開きます。
   b. [APPLICATION]ペイン(左)で、アプリケーション名を選択します。
      [VERSIONS]ペイン(右)には、選択したアプリケーションのアクティブなバージョンが一覧表示されます。
   c. レポートに含めるバージョンのチェックボックスをオンにします。(1つだけ選択できます。)



   d. [DONE]をクリックします。

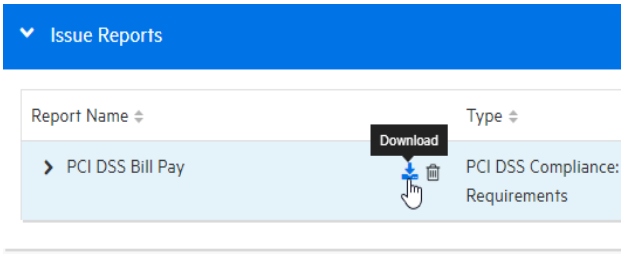


6. レポートテンプレートの複数のエディションがある場合(たとえば、CWE/SANSの上位25の問題レポートの場合)、 [Options]リストから、生成するエディションを選択します。レポートタイプによっては、追加の設定が必要な場合や使用可能な場合があります。
7. 生成するレポートの形式を選択するには、 [Output format]の横で、 [XLS]、 [DOC]、または [PDF]を選択します。
8. [CREATE NEW REPORT]ダイアログボックスで、 [GENERATE]をクリックします。



Fortify Software Security Center でレポートが追加される [**レポート**]テーブルには、すべてのレポートがカテゴリに基づい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**」の値が表示されます。

> **注 :** レポートの設定時に [**Notes**]ボックスに内容を入力した場合、[**Notes**]列にはレポートのメモアイコンが表示されます。



9. レポートを表示するには、カーソルをレポート名に移動して、 [**ダウンロード**]アイコン をクリックします。
10. レポートを保存するか開きます。

参照情報

"レポートテンプレートをダウンロードする" ページ376

"レポート定義のインポート" ページ378

BIRTライブラリ

BIRTライブラリを使用すると、一般的に必要な機能とレポート項目をカプセル化できます。これらのライブラリは、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、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1人で作成する必要がないため、レポート開発タスクの細分化が可能になります。

> **注 :** BIRTレポートライブラリを使用する前に、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" ページ376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を多 数 のレポートデザインで使 用している場 合 、ロゴを変 更 するにはライブラリに変 更 を加 えれば済 みます。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。

レポートライブラリのインポート

管 理 者 レベルのユーザの場 合 は、Fortify Software Security Center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. [ADMINISTRATION]ビューの左 ペインから、 [**Templates**]を選 択 して、 [**Report Libraries**]を選 択 します。
   [**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。
2. [**IMPORT**]をクリックします。
   [MPORT NEW LIBRARY TEMPLATE]ダイアログボックスが開 きます。
3. (オプション) [**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。
4. [**BROWSE**]をクリックし、レポートライブラリリソースに移 動 して選 択 します。
5. [**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

"Fortify Software Security Center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 " ページ169

"レポートを生 成 して表 示 する" ページ371

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。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。

Fortify Software Security CenterBIRT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。
   Fortify Software Security Centerレポートでサポートされ ているBIRT Report Designerバージョンの詳 細 については、ドキュメント『Micro Focus Fortifyソフトウェアシステム要 件 』を参 照 してください。
   Eclipse BIRT Report Designerのダウンロードについては、「"BIRT Report Designerの取 得 " 次 のページ」を参 照 してください。

2. Fortify Software Security Center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Fortify Software Security Center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。Fortify Software Security Center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" 下を参照してください。
3. Fortify Software Security Center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Fortify Software Security Center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. Fortify Software Security Center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Fortify Software Security Centerにインポートします。

レポート定義をFortify Software Security Center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" ページ378を参照してください。

BIRT Report Designerの取得

Fortify Software Security Center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、ドキュメント『Micro Focus Fortifyソフトウェアシステム要件』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ブラウザウィンドウを開き、次のダウンロードページに移動します。
   http://download.eclipse.org/birt/downloads/build_list.php
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、`https://www.eclipse.org/birt/documentation/install.php`を参照してください。

レポートテンプレートをダウンロードする

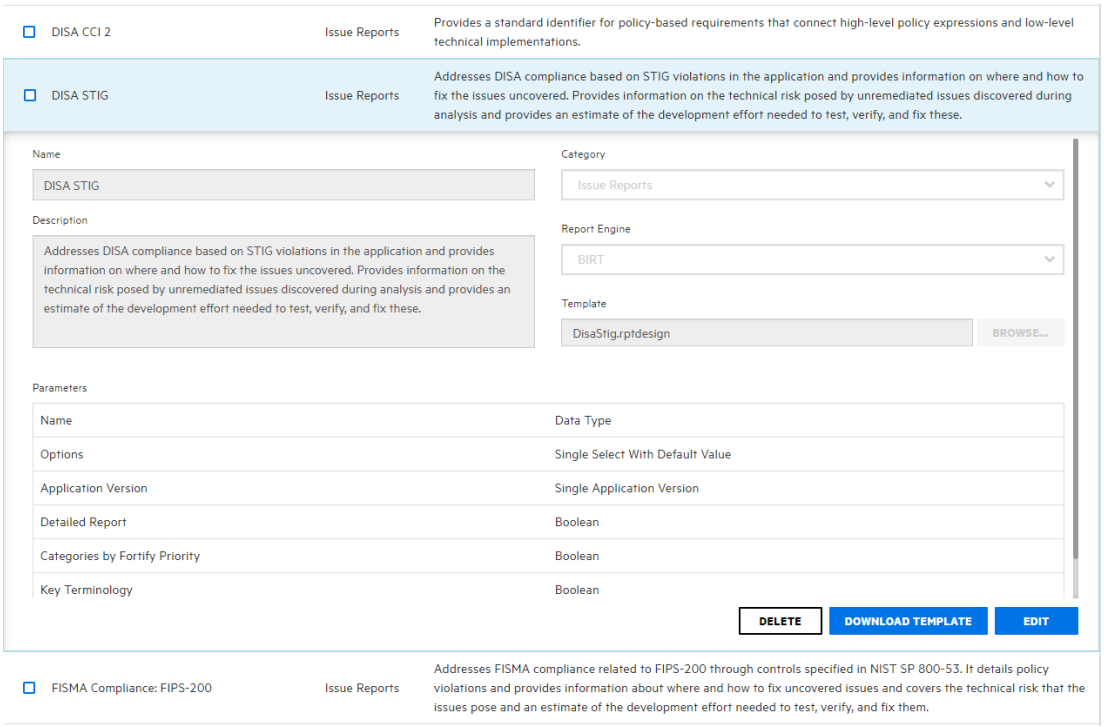
Fortify Software Security Centerレポートテンプレートを変更のためにダウンロードできます。

注意 Fortify Software Security Centerレポートテンプレートのダウンロード、変更、および再インポートは可能ですが、カスタマイズされたレポートテンプレートはサポートされていないのでご注意ください。

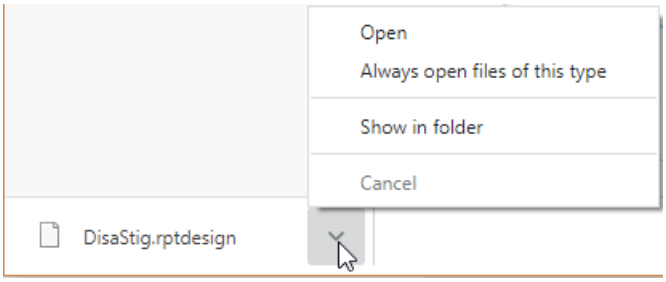
注 : 「Options」という名 前 のパラメータをBIRTレポート で変 更 することはできません。

Fortify Software Security Center レポートテンプレートをダウンロード するには:

1. Fortifyのヘッダで、 [**ADMINISTRATION**]をクリックします。
2. 左 側 のペインで、 [**テンプレート**]を展 開して、 [**レポート**]を選 択します。
   右 側 のテーブルには、システム内 の各 レポート の名 前 、タイプ、および説 明 が表 示 されます。
3. 目 的 のレポート の行 をクリックします。



4. レポート 詳 細 セクションの右 下 で、 [**DOWNLOAD TEMPLATE**]をクリックします。



5. 画 面 の左 下 で、ダウンロードしたレポートテンプレートファイル名 (`*.rptdesign`)の横 にある矢 印 をクリックし、 [**Show in folder**]を選 択します。

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 Fortify Software Security Center に再 インポート することができます。そうする場 合 は、変 更 したレポートファイルの名 前 を変 更して、インポート時 に元 のテンプレートが置 き換 わら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 Fortify Software Security Center 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" 下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" ページ371

レポート定義のインポート

Fortify Software Security Centerレポートは、オープンソースのBusiness Intelligence and Reporting Tools (BIRT)システムに基づいて作成されます。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Fortify Software Security Center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、インポートレポート定義ファイルをFortify Software Security Centerに追加することができます。そうするには、Fortify Software Security CenterBIRT定義(`rptdesign`ファイル名拡張子)が必要です。

注意 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Fortify Software Security Centerに展開する前に、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. Fortifyのヘッダで、 [**ADMINISTRATION**]をクリックします。
2. 左ペインで、 [**Templates**]を選択し、 [**Report Templates**]を選択します。
   [**Reports**]テーブルには、既存のレポートテンプレートと、レポートテンプレートのタイプと説明が一覧表示されます。
3. [**IMPORT**]をクリックします。
   [IMPORT NEW REPORT TEMPLATE]ダイアログボックスが開きます。
4. 次の表で説明する情報を入力します。

フィールド	説明
Name	テンプレートの名前を入力します。
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	このリストから、テンプレートが属するカテゴリを選択します。
Report Engine	このリストでは、 [**BIRT**]を選択したままにします。
Template	ファイル名の拡張子 `rptdesign`

フィールド	説明
	を持つFortify Software Security Center BIRT定義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。
   a. [ADD PARAMETER]をクリックします。
   b. [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
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。
Description	(オプション)パラメータの説明を入力します。
Identifier	パラメータの固有の識別子を入力します。
Data Type	このリストから、このパラメータのデータ型を選択します。

6. [APPLY]をクリックします。
7. 新しいレポート定義を定義のリストに追加するには、[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" ページ371

第19章: 認証トークン

認証トークンは、ユーザがパスワードを使用せずにFortify Software Security Center内でアクションを自動化できる固有のキーです。ユーザはトークンを要求し、Fortify Software Security Centerサーバに対して認証を受け、時間制限のあるアクションの小規模セットに関して実行許可を示す文字列を受け取ります。たとえば、`AnalysisUploadToken`トークンでは、ユーザがインタフェースにログインしたり結果を表示したりすることは許可されません。一般的なアクションには、スキャン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。

認証トークンを生成する

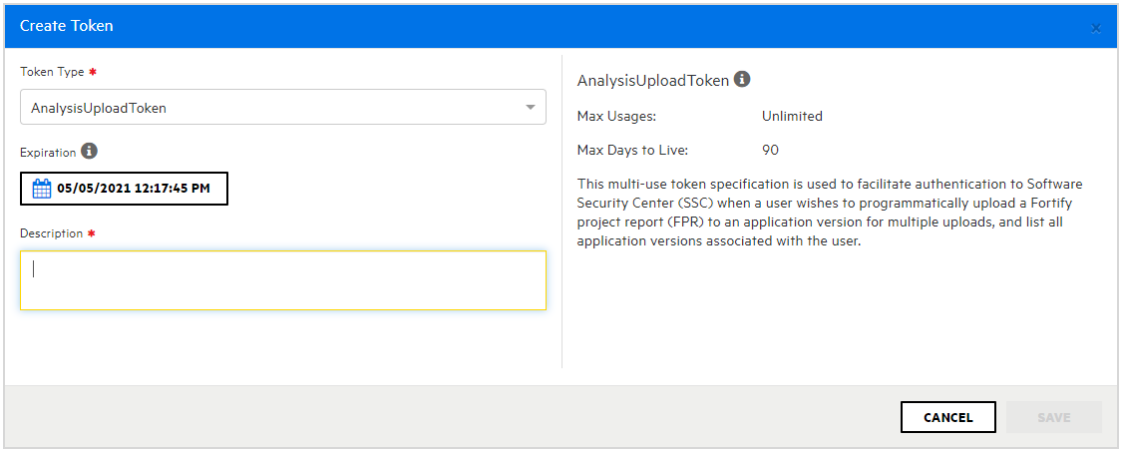
認証トークンの生成は、Fortify Software Security CenterのADMINISTRATIONビューから、あるいはコマンドラインインタフェースからできます。自分のトークンの詳細を見ることができるのは、自分だけです。Fortify Software Security Center 管理者は、作成されたトークンの期限を延長することはできますが、トークンに関する詳細情報を見ることはできません。

> **注:** あらゆるタイプのトークンを作成できますが、トークンが実行するように設計されたアクションを実行するために必要な許可を持っていない方は、トークンを使用することができません。

ADMINISTRATIONビューからトークンを生成する

認証トークンを Fortify Software Security Center ユーザインタフェースから生成するには:

1. Fortifyページヘッダで、 [**ADMINISTRATION**]を選択します。
2. [ADMINISTRATION]ビューの左ペインで、 [**Users**]セクションを展開し、 [**Token Management**]を選択します。
3. [**Token Management**]ツールバーで、 [**NEW**]をクリックします。
   [Create Token]ダイアログボックスが開きます。
4. [**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を表示するには、"コマンドラインからトークンを生成する" ページ382の表を参照してください。

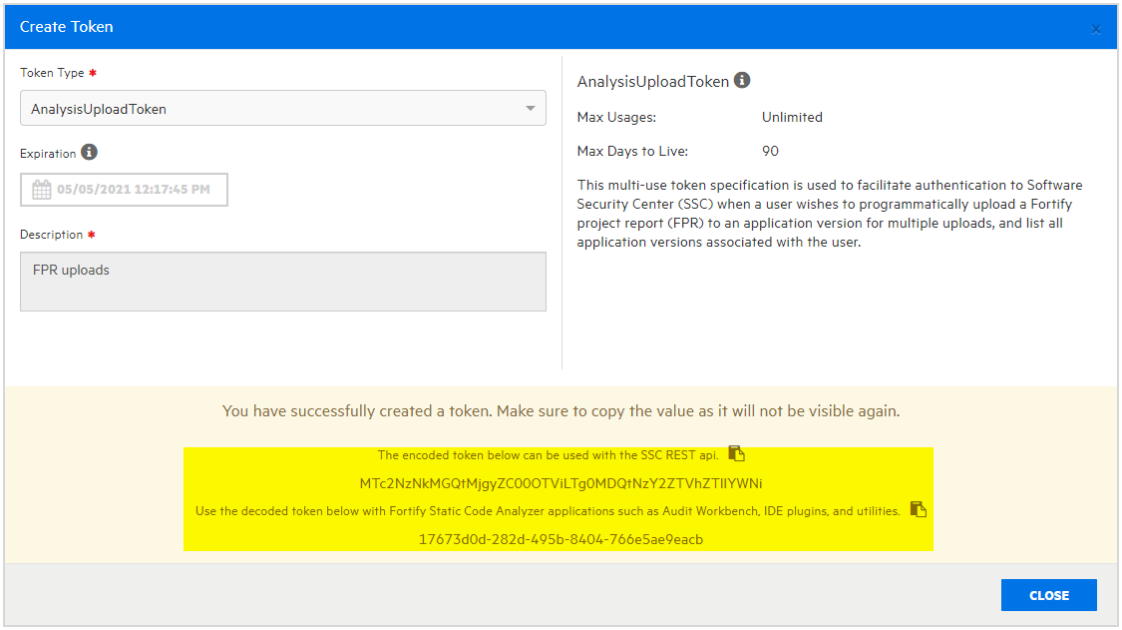


[Create Token]ダイアログボックスには、選 択したトークンタイプの説 明 が右 側 のペインに表 示されます。

5. [**有 効 期 限**]カレンダコントロールを使 用して、トークンの期 限 が切 れる日 を指 定します。(有 効 期 限 は、指 定した日 付 の現 在 の時 刻 に設 定されます。)

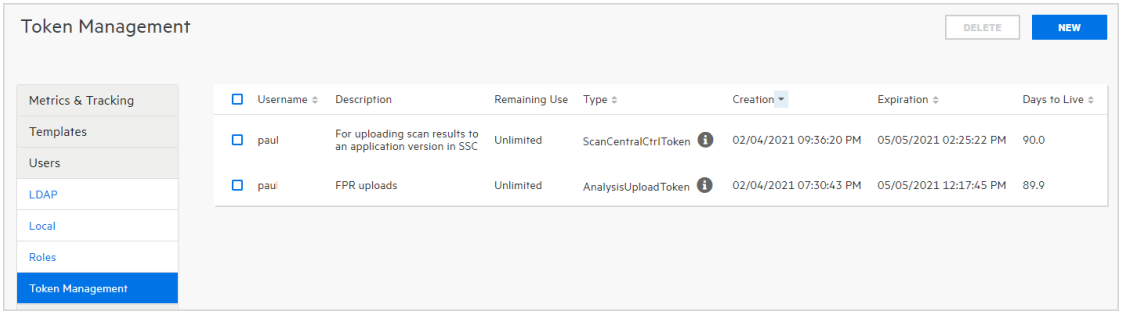
> **注 :** デフォルトでは、有 効 期 限 の値 は、選 択したトークンタイプに対して有 効 な最 大 日 数 に設 定されます。これをそれより前 の日 付 に設 定すると、トークンの有 効 期 限 は短 くなります。.

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. [**SAVE**]をクリックします。



[Create Token]ダイアログボックスには、トークンが正 常 に作 成されたことを知 らせるメッセージが表 示されます。

8. メッセージの下 部 で、エンコードまたはデコードされたトークン文 字 列 をコピーして保 存します。(Software Security Centerにはこれらの情 報 は再 表 示されません)。



[Token Management]ページには新しいトークンが一 覧 表 示 されます。

コマンドラインからトークンを生 成 する

コマンドラインからトークンを生 成 するには、次 のコマンドを実 行します。

```
fortifyclient token -gettoken <token_name> -url <ssc_url> -user
<username> -password <password>
```

次 の表 に、選 択 可 能 な *<token_name>* オプションを示します。

オプション	説 明
AnalysisDownloadToken	マージされた結 果 ファイルをダウンロードする
AnalysisUploadToken	スキャン結 果 を Fortify Software Security Center にアップロードしてアプリケーションを一 覧 表 示 する
AuditToken	現 在 のセキュリティ問 題 に関 する詳 細 をロードして、解 析 タグを適 用 する
CIToken	Software Security Centerと継 続 的 な統 合 プラグインとの統 合 を可 能 にする
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 Fortify Software Security Center からパージできるようにする
ReportFileTransferToken	一 般 には自 動 化 スクリプトにより、既 存 のレポートの認 証 されたセッション内 でのダウンロードをサポートする/fileTokensエンドポイントを使 用 して、プログラム的 に作 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

オプション	説 明
	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 CLIツールを使 用した ScanCentral通 信 のため
ToolsConnectToken	このトークンを、Fortify Software Security Centerと接 続したFortify Static Code Analyzerアプリケーション(Audit Workbench、IDEプラグイン、ユーティリティ)で使 用して、スキャン結 果 の共 同 的な監 査 、修 正 、アップロードをします。
UnifiedLoginToken	ほとんどのREST APIへのアクセスが可 能 になります。1日 未 満 の短 い実 行 自 動 化 が対 象 です。

認 証トークンは、ランタイム時 に `WEB-INF/internal/serviceContext.xml` で定 義 されます。

参 照 情 報

"fortifyclient認 証トークンでのDaysToLiveの指 定 " ページ388.

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 に複 数 使 用トークンの有 効 期 限 を変 更 してもらうこともできますが、トークンに関 する他 の情 報 を管 理 者 が見 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. Fortifyページヘッダで、 [**ADMINISTRATION**]を選 択 します。
2. [ADMINISTRATION]ビューの左 ペインで、 [**Users**]セクションを展 開 し、 [**Token Management**]を選 択 します。
   [Token Management]ページには、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. [EDIT]をクリックします。
5. 有 効 期 限 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**]で、カレンダコントロールをクリックして、別 の有 効 期 限 を指 定 します。

   注 : 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. [SAVE]をクリックします。

参 照 情 報

"認 証 トークンを生 成 する" ページ380

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. Fortifyページヘッダで、 [**ADMINISTRATION**]を選 択 します。
2. [ADMINISTRATION]ビューの左 ペインで、 [**Users**]セクションを展 開 し、 [**Token Management**]を選 択 します。

   [Token Management]ページには、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。

   Fortify Software Security Centerで、トークンの削 除 を確 認 するメッセージが表 示 されます。
4. [OK]をクリックします。

参 照 情 報

"認 証 トークンを生 成 する" ページ380

付 録 A: fortifyclientユーティリティの使 用

このセクションのトピックでは、Fortify Software Security Center間 でオブジェクトをセキュアに転 送 するために使 用 できるFortify Software Security Centerの`fortifyclient`コマンドラインユーティリティ(Windowsシステムの場 合 は`fortifyclient.bat`)について説 明します。

注 : このセクション全 体 で、`<ssc_install_dir>`は`Fortify_<version>_Server_WAR_Tomcat.zip`ファイルを抽 出 したディレクトリを表 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。

fortifyclientの要 件

`fortifyclient` を使 用してスキャン結 果 (FPRファイル)をアップロードするには、自 分 のFortify Software Security Center インスタンスのURLを知 っていて、次 のいずれかを持 っていなければなりません。

- `fortifyclient` コマンドラインユーティリティで指 定 された操 作 を実 行 できるだけの権 限 を持 つ、Fortify Software Security Centerサーバ上 のユーザアカウント
- `fortifyclient` 認 証トークン

このセクションで説 明 するトピック:

Fortify Software Security Center URLの指 定について

ほとんどのfortifyclientコマンドにはFortify Software Security Center URLが含 まれます。fortifyclientに渡されるFortify Software Security Center URLには、ポート番号 とコンテキストパス/ssc/の両 方を含 める必 要 があります。Fortify Software Security Center URLの正 しい形 式 は次 のとおりです。

```
http://<hostname>:<port>/ssc/
```

例 :

- 非 ルートアプリケーションの場 合 : http://www.company.com/ssc
- ルートアプリケーションの場 合 : http://ssc.company.com

注 : このガイドのコード例 で、<ssc_url>はこのトピックで説 明されている正 しい形 式 のFortify Software Security Center URLを表 します。

fortifyclient認 証トークン

fortifyclient 認 証トークンを使 用すると、スクリプトされたプロセスが Fortify Software Security Center のユーザ名 とパスワードを明らかにすることなく操 作を実 行できるようになります。既 存 の Fortify Software Security Center 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、トークンを作 成する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、Fortify Software Security Center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。

fortifyclientクライアントオプションとパラメータの一 覧

fortifyclientコマンドとパラメータを一 覧 表 示 するには、次 の手 順 に従 います。

1. コマンドラインから、<ssc_install_dir>/Tools/fortifyclient/binディレクトリに移 動します。
2. コマンドプロンプトで「fortifyclient」と入 力します。(Windowsシステムの場 合 は、「fortifyclient.bat」と入 力 します)。

Fortify Software Security Centerでは、コマンド名 とオプション名 の大 文 字 と小 文 字 が区 別されます。

アップロード認証トークンについて

fortifyclientのアップロード認証トークンにより、FPRがFortify Software Security Centerにアップロードされるときにアカウントおよびパスワード情報を隠すことができます。

このセクションで説明するトピック:

fortifyclientを使用したアップロード認証トークンの取得

アップロード認証トークンは、Fortify Software Security CenterのADMINISTRATIONビューから取得するか、あるいは fortifyclient を使用して取得できます。次の手順では、fortifyクライアントを使用してアップロード認証トークンを取得する方法について説明します。ADMINISTRATIONビューからトークンを生成する方法については、"認証トークンを生成する" ページ380を参照してください。

fortifyclient を使用して解析アップロードトークンを取得するには、次のものが必要です。

- Fortify Software Security Center のURL("Fortify Software Security Center URLの指定について" 前のページを参照)
- fortifyclient アクセストークンを使用する権限がある Fortify Software Security Center ユーザアカウント

fortifyclient を使用して解析アップロードトークンを取得するには:

1. <*ssc_install_dir*>/Tools/fortifyclient/bin ディレクトリに移動して、次のコマンドを実行します:

   ```
   fortifyclient -url <ssc_url> token -gettoken AnalysisUploadToken
        -user <account_name>
   ```

   ここで AnalysisUpLoadToken は、大文字と小文字を区別する fortifyclient アップロードトークン指定子です。

   パスワードの入力を求められます。
2. <*account_name*> のパスワードを入力します。

   fortifyclient で一般的な形式のトークンが表示されます。

   ```
   cb79c492-0a78-44e3-b26c-65c14df52e86
   ```
3. 返されたトークンをテキストファイルにコピーします。

fortifyclient でトークンを使用して Fortify Software Security Center の情報を読み書きできるかどうかは、-userパラメータにより指定されたユーザアカウントの権限に応じて異なります。

fortifyclient認証トークンでのDaysToLiveの指定

"アップロード認証トークンについて" 前のページで説明したように、fortifyclientでは、管理でユーザアカウント情報を隠すことができるトークンがサポートされています。

-daysToLiveパラメータを使用して、指定した日数が経過した後にfortifyclientトークンが期限切れになるように設定できます。次のコマンドの例では、-daysToLiveパラメータを使用して、2日後に期限切れになるトークンを取得する方法を示しています。

```
fortifyclient -url <ssc_url> token -gettoken AnalysisUploadToken
    -user admin -daysToLive 2
```

ここで<ssc_url>は、Fortify Software Security CenterインスタンスのURLを表します("Fortify Software Security Center URLの指定について" ページ386を参照)。

daysToLiveパラメータは大文字と小文字を区別するため、上記の例のように正確に入力する必要があります。

fortifyclient認証トークンの一覧

Fortify Software Security Center管理者は、fortifyclientを使用してすべてのFortify Software Security Centerユーザアカウントのすべての既存のアクセストークンを一覧表示できます。fortifyclientユーティリティでは、Fortify Software Security Center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のリストのフィルタリングはサポートされていません。

すべてのアクセストークンを一覧表示するには、次の手順に従います。

1. <ssc_install_dir>/Tools/fortifyclient/bin ディレクトリに移動して、次を実行します:

   ```
   fortifyclient -url <ssc_url> listtokens -user <admin_account_name>
   ```

   ここで<ssc_url>は、Fortify Software Security CenterインスタンスのURLを表し("Fortify Software Security Center URLの指定について" ページ386を参照)、<admin_account_name>はFortify Software Security Center管理者レベルのユーザアカウントの名前です。
2. プロンプトが表示されたら、管理者レベルのユーザアカウントのパスワードを入力します。

   すべてのfortifyclient認証トークンのID、所有者、作成日、有効期限、および作成IPアドレスを示すリストが返されます。

トークンの無効化

作成したトークンは、Fortify Software Security Centerユーザインタフェースから削除するか、`invalidatetoken`コマンドを実行して無効にできます。

Fortify Software Security Centerユーザインタフェースからトークンを削除するには、次の手順に従います。

1. Fortifyページヘッダで、 [**ADMINISTRATION**]を選択します。
2. [ADMINISTRATION]ビューの左ペインで、 [**Users**]セクションを展開し、 [**Token Management**]を選択します。
3. [**Token Management**]ページで、削除するトークンを表示する行をクリックします。
   行が展開され、トークンの詳細が表示されます。
4. [**DELETE**]をクリックします。
   Fortify Software Security Centerで、トーク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。

コマンドラインから既存の認証トークンを無効にするには、次の手順に従います。

注: 管理者も代わりにこの操作を実行できます。

1. *<ssc_install_dir>*`/Tools/fortifyclient/bin`ディレクトリに移動します。
2. 次のコマンドを実行します。

```
fortifyclient -url <ssc_url> invalidatetoken [ -invalidateByID
   <token_ID> | -invalidateForUser <owner> | -invalidate <token> ]
```

ここで

<ssc_url>	Fortify Software Security CenterインスタンスのURLを表します ("Fortify Software Security Center URLの指定について" ページ386を参照)
<token_ID>	無効にするトークンのIDを表します。
<owner>	トークンが無効になるユーザを表します。
<token>	無効にするトークンの名前を表します。

参照情報

"認証トークンを生成する" ページ380

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 のアクセストークンを作 成Fortify Software Security Centerするために使 用したアカウントがアクセスできるアプリケーションバージョンを一 覧 表 示 できます。

注: 管 理 者 レベルのユーザは、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 のユーザは、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 を付 与 された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 アカウントのユーザは、アクセスが許 可 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。("アップロード認 証トークンについて" ページ387を参 照)。

アプリケーション識 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のリストを取 得 するには、次 の手 順 に従 います。

1. <*ssc_install_dir*>/Tools/fortifyclient/binディレクトリに移 動 します。
2. 次 のコマンドを実 行 します。

```
fortifyclient -url <ssc_url> -authtoken <token> listApplicationVersions
```

ここで<*ssc_url*>は、Fortify Software Security Centerインスタンスの URLを表 し("Fortify Software Security Center URLの指 定 について" ページ386を参 照)、<*token*>は、有 効 なfortifyclient認 証トークンです。また、-userパラメータと-passwordパラメータを使 用して、ユーザアカウントの資 格 情 報 を指 定 することもできます。

トークンを作 成したユーザアカウントがアクセスできるすべてのアプリケーションバージョンについて、fortifyclientユーティリティにはアプリケーションバージョンID、名 前 、および番 号 が一 覧 表 示 されます。

アプリケーションバージョンのパージ

特 定 の日 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のすべての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. <*ssc_install_dir*>/Tools/fortifyclient/binディレクトリに移 動 します。
2. 次 のコマンドを実 行 します。

```
fortifyclient -url <ssc_url> purgeApplicationVersion <app_identifier>
    -scanDate <MMDDYYYY>
```

ここで<*ssc_url*>は、Fortify Software Security Centerインスタンスの URLを表 し("Fortify Software Security Center URLの指 定 について" ページ386を参 照)、<*app_identifier*>は、-application <*app_name*>、

`-applicationVersion<version_name>`、または`-applicationVersionID <id>`を表します。

FPRのアップロードについて

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Fortify Software Security Centerにアップロードします。これを行うには、認証トークンまたはユーザ名とパスワードを使用できます。このセクションのトピックでは、認証トークンを使用してFPRをアップロードする方法について説明します。ユーザ名とパスワードの使用例については、"FPRのダウンロードについて" ページ393を参照してください。
`Fortifyclient`のアップロードアクセストークンでは、スクリプトを使用してFPRをFortify Software Security Centerにアップロードする際に、`AccessUploadToken`トークンを使用してユーザ資格情報を隠します。セキュリティを強化するために、アクセストークンの`DaysToLive`パラメータを使用することもできます。

注: このセクションで説明する手順を実行するには、まず認証トークンを取得する必要があります ("アップロード認証トークンについて" ページ387を参照)。

次のトピックで説明されている方法のいずれかを使用してFPRファイルをアップロードできます。

アプリケーション識別子を使用したFPRファイルのアップロード

アプリケーション識別子を使用してFPRをFortify Software Security Centerにアップロードするには、次の手順に従います。

1. `<ssc_install_dir>/Tools/fortifyclient/bin`ディレクトリに移動します。
2. 次のコマンドを実行します。

```
fortifyclient -url <ssc_url> -authtoken <token> uploadFPR -file
<fpr_name> -applicationVersionID <id>
```

ここで

<ssc_url>	Fortify Software Security CenterインスタンスのURLを表します ("Fortify Software Security Center URLの指定について" ページ386を参照)

<token>	有効なfortifyclientアプリケーショントークンを表します
<fpr_name>	FPRファイルのフルパスと名前とその拡張子を表します
<id>	Fortify Software Security Centerアプリケーションバージョン識別子を表します

Fortify Software Security Centerアプリケーション識別子を取得する方法については、"アプリケーションバージョンの一覧表示" ページ390を参照してください。

アプリケーション名とバージョンを使用したFPRファイルのアップロード

アプリケーション名とバージョンを使用してFPRをFortify Software Security Centerアプリケーションバージョンにアップロードするには、次の手順に従います。

1. *ssc_install_dir*>/Tools/fortifyclient/binディレクトリに移動します。
2. 次のコマンドを実行します。

   fortifyclient -url *<ssc_url>* -authtoken *<token>* uploadFPR -file *<fpr_name>* -application *<app_name>*, -applicationVersion *<version_name>*.

   ここで

<ssc_url>	Fortify Software Security Centerインスタンスの URLを表します ("Fortify Software Security Center URLの指定について" ページ386を参照)
<token>	有効なfortifyclientアプリケーショントークンを表します
<fpr_name>	FPRファイルのフルパスと名前とその拡張子を表します
<app_name>	Fortify Software Security Centerアプリケーション名を表します
<version_name>	指定したアプリケーション名に対応するFortify Software Security Centerアプリケーションバージョンを表します

参照情報

"アプリケーション識別子を使用したFPRファイルのアップロード" 前のページ

FPRのダウンロードについて

fortifyclientを使用し、Fortify Software Security Center識別子またはアプリケーションバージョンを指定して、FPRをダウンロードできます。このセクションでは、両方の方法を使用してFPRをダウンロードする手順について説明します。

認証トークンまたはユーザ名とパスワードを使用してFPRをダウンロードできます。このセクションのトピックでは、ユーザ名とパスワードを使用して、FPRをダウンロードする方法について説明します。認証トークンの使用例については、"FPRのアップロードについて" ページ391を参照してください。

このセクションで説明するトピック:

アプリケーション識別子を使用してFPRをダウンロードする

fortifyclient を使用してFPRファイルを Fortify Software Security Center へ、アプリケーション識別子を使用してダウンロードするには:

1. <*ssc_install_dir*>/Tools/fortifyclient/binディレクトリに移動します。
2. 次のコマンドを実行します。

```
fortifyclient -url <ssc_url> -user <Username> -password <password>
downloadFPR -file <FPRname> -applicationVersionID <id>
```

ここで

<*ssc_url*>	Fortify Software Security Centerインスタンスの URLを表します ("Fortify Software Security Center URLの指定について" ページ386を参照)
<*Username*>	FPRファイルを含むアプリケーションバージョンにアクセスできる開発者以上のレベルのSoftware Security Centerアカウントのユーザ名を表します。
<*password*>	FPRファイルを含むアプリケーションバージョンにアクセスできる開発者以上のレベルのSoftware Security Centerアカウントのパスワードを表します。
<*FPRname*>	FPRファイルのフルパスと名前とその拡張子を表します
<*id*>	Fortify Software Security Centerアプリケーションバージョン識別子を表します

Fortify Software Security Centerアプリケーション識別子を取得する方法については、"アプリケーションバージョンの一覧表示" ページ390を参照してください。

アプリケーション名とバージョンを使用してFPRをダウンロードする

FPRを Fortify Software Security Center アプリケーションバージョンに、アプリケーション名とバージョンを使用してダウンロードするには:

1. *<ssc_install_dir>*/Tools/fortifyclient/binディレクトリに移動します。
2. 次のコマンドを実行します。

```
fortifyclient -url <ssc_url> -user <username> -password <password>
   downloadFPR -file <fpr_name> -project <app_name> -version <app_
   version>
```

ここで

<ssc_url>	Fortify Software Security CenterインスタンスのURLを表します ("Fortify Software Security Center URLの指定について" ページ386を参照)
<username>	FPRファイルを含むアプリケーションバージョンにアクセスできる開発者以上のレベルの Fortify Software Security Center アカウントのユーザ名を表します。
<password>	FPRファイルを含むアプリケーションバージョンにアクセスできる開発者以上のレベルの Fortify Software Security Center アカウントのパスワードを表します。
<fpr_name>	FPRファイルのフルパスと名前とその拡張子を表します
<app_name>	Fortify Software Security Centerアプリケーション名を表します
<app_version>	指名したアプリケーションに対応する Fortify Software Security Center アプリケーションバージョンを表します

コンテンツバンドルのインポート

Fortify Software Security Center の継続的サポートの一環として、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(.zip ファイル名拡張

子)が定期的に提供されます。

注: Fortify Software Security Center では、コンテンツバンドルをインポートするための認証トークンの使用をサポートしていません。

コンテンツバンドルを Fortify Software Security Center にインポートするには、次の操作をします。

1. `<ssc_install_dir>/Tools/fortifyclient/bin`ディレクトリに移動します。
2. 次のコマンドを実行します。

```
fortifyclient -url <ssc_url> -user <username> -password <password>
   import -bundle <bundle_name>
```

where

<ssc_url>	Fortify Software Security CenterインスタンスのURLを表します ("Fortify Software Security Center URLの指定について" ページ386を参照)
<username>	fprファイルを含むアプリケーションバージョンにアクセスできるマネージャ以上のレベルの Fortify Software Security Center アカウントのユーザ名を表します。
<password>	fprファイルを含むアプリケーションバージョンにアクセスできるマネージャ以上のレベルの Fortify Software Security Center アカウントのパスワードを表します。
<bundle_name>	コンテンツバンドル(`.zip` ファイル名拡張子)へのフルパス名を表します。

監査添付ファイルをダウンロードする

監査添付ファイルをダウンロードするには:

1. *<ssc_install_dir>*/Tools/fortifyclient/binディレクトリに移動します。
2. 次のコマンドを実行します。

```
fortifyclient -url <ssc_url> downloadAttachment -file
   <destination_file> -attachmentId <Attachment_Id>
```

ここで

<ssc_url>	Fortify Software Security Centerインスタンスの URLを表します ("Fortify Software Security Center URLの指定について" ページ386を参照)
<destination_file>	ダウンロードされたFPRファイルのフルパスを表します
<Attachment_Id>	ダウンロードする添付ファイルのIDを表します

付録B: バグトラッカプラグインの作成

Fortify Software Security Centerでは、外部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。この統合により、Fortify Software Security CenterユーザはFortify Software Security Centerの問題を監査する時点でバグをログに記録できます。提供時点では、システムはJira、Bugzilla、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、ドキュメント『Micro Focus Fortifyソフトウェアシステム要件』を参照してください)。会社で別のバグトラッカシステムを使用している場合は、そのシステム用に新しいプラグインを作成できます。このセクションでは、新しい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。

注: このガイドおよびFortify Software Security Center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。

重要 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_install_dir>/Samples/<BugTrackerPlugin_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。

使用例

Fortify Software Security Centerの管理者として、"バグトラッカーの統合について" ページ159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。Fortify Software Security Center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移動できます。

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。

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を使用して記述できる、独立したコンポーネントです。

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。

注: 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JRE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。

実装

プラグインフレームワークを使用するFortify Software Security Center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);
}
```

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。おそらく資格情報ストア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、ほぼ常に`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。
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

メソッドまたはコール	説明
	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するために使用されます。
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。コールは、実行される操作を使用してプラグインの設定を設定します。
testConfiguration (call)	プラグインフレームワークは、`setConfiguration`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`testConfiguration`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。
getShortDisplayName	`getShortDisplayName`メソッドは、プラグインの短い表示名を返す場合に使用されます。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するために使用されます。 **重要** Fortify Software Security Center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。(整合性を保つには、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。
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を含む値を返す場合に使用されます。このメソッドは、たとえ

メソッドまたはコール	説明
	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。 **注意** Fortify Software Security Center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。(整合性を保つには、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。
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。Fortify Software Security Center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さまざまな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" ページ405を参照してください)。
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

メソッドまたはコール	説明

	`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表示され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。

onParameterChange	プラグインフレームワークは、`hasDependentParams`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`onParameterChange`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。

メソッドまたはコール	説明

	• 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か確認します。
	• 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。

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.getIssueDetail()オブジェクトからではなく、bug.getParams()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、BugSubmission.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: • Fortify Software Security Center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、`MultiIssueBugSubmission.getIssueDetails()`の`getLastBuildWithoutIssue()`、`getDetectedInBuild()`、および`getFileName()`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するために使用されます。
getBugDeepLink	このメソッドは、バグへのディープリンクを作成するために使用されます。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。

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。

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 むエラーメッセージはユーザに送 り返 されるため、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。

ほぼステートレス

Fortify Software Security Center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。Software Security Center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。

バグトラッカプラグインのデバッグ

Apache Commonsのログ記 録 はプラグインでサポートされています。結 果 のログは、`<fortify.home>/<appcontext>/plugin-framework//logs`ディレクトリ内 のファイル `plugin-framework.log`に追 加 されます。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。

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 をビルドします。

次 に示 すのは、バグトラッカープラグインをGradleでビルド するために使 用 するスクリプト の例 です。

```
apply plugin: 'java'

sourceCompatibility = '1.8'

targetCompatibility = '1.8'

dependencies {

compile fileTree(dir: 'lib', include: '*.jar')

}

jar.enabled = false // デフォルト の非osgi jarをビルド時 に生 成 する必 要 はありません。

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)
```

重要 Fortify Software Security Center 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。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。(整合性を保つには、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_install_dir>*/Samples/*<bugtracker>*/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" ページ397

付録C: Fortify Software Security Centerの設定の自動化

<*app_context*>.autoconfigファイルを使用して、展開前にFortify Software Security Centerの設定を自動化できます。このファイルには、Fortify Software Security Center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。自動設定ファイルは、Fortify Software Security Center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。<*app_context*>.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。

注: 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、Fortify Software Security Center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。

Fortify Software Security Centerの設定を自動化するには、次の手順に従います。

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、Fortify Software Security Center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。ファイル名は、ROOTコンテキスト(_default_.autoconfig)を除き、アプリケーションコンテキスト名(Fortify Software Security Center、<*app_context*>.autoconfig)と一致している必要があります。
2. 次の項目を<*app_context*>.autoconfigファイルに、YAML形式で追加します。

```
 appProperties:
   # <fortify.home>/<app_context >/conf/app.propertiesのプロパティをすべて含めます。# 例は次のとおりです。host.url:
   'http://ssc.example.org:8888/ssc' # searchIndex.location:
   '/home/ssc/search_index' # host.validation: false

datasourceProperties:
   # <fortify.home>/<app_context>/conf/datasource.propertiesのプロパティをすべて含めます。# 例: # 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=false'

 # MySQL database # jdbc.url: 'jdbc:mysql://mysql-host:3306/ssc_
   db? sessionVariables=collation_connection=latin1_general_
   cs&rewriteBatchedStatements=true'

 # Oracle database # jdbc.url: 'jdbc:oracle:thin:oracle-
   host:1521:ssc_db'

 dbMigrationProperties:
   #自動データベースマイグレーションマイグレーションを有効にします。
   migration.enabled: true # オプションで代替マイグレーション資格情報を指定します # migration.username: ssc_db_admin_username #
   migration.password: ssc_db_admin_password

seeds:
   #環境に適した場所へのパスを変更します- '/home/ssc/bundles/Fortify_
   Process_Seed_Bundle-2021_Q4_0001.zip' -
   '/home/ssc/bundles/Fortify_PCI_Basic_Seed_Bundle-2021_Q4_
   0001.zip' - '/home/ssc/bundles/Fortify_PCI_SSF_Basic_Seed_
   Bundle-2021_Q4_0001.zip' - '/home/ssc/bundles/Fortify_Report_
   Seed_Bundle-2021_Q4_0001.zip'
```

3. ファイルを<*fortify.home*>(Windowsシステムの場合%USERPROFILE%\.fortify)に保存します。
4. フォルダ <*fortify.home*>内にfortify.licenseファイルのコピーを配置します。
5. Tomcatサーバを起動します。
6. *.autoconfigファイルを保存して、Fortify Software Security Centerを再起動します。

自動設定の最後に、Fortify Software Security Centerは有効な設定チェックサムを計算し、autoconfig.checksumプロパティの値としてversion.propertiesファイルに保存します。

Fortify Software Security Center起動したときに`<app.context>.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、Fortify Software Security Center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、Fortify Software Security Centerは保守モード(`version.properties`ファイルの`(maintenance.mode=true)`に設定され、次回のサーバ起動時に完全自動設定が強制実行されるかセットアップウィザードが表示されます。

チェックサムには次の内容が含まれます。

- autoconfig appPropertiesからの有効なプロパティ
- autoconfig datasourcePropertiesからの有効なプロパティ
- 有効なautoconfig seedsからのファイル名
- `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。

Fortify Software Security Centerは、完全に設定されていない場合にのみ、完全自動設定を実行します。Fortify Software Security Centerは、チェックサムが一致しないが、それ以外は設定済みの場合にのみ軽量自動設定を実行します。

軽量自動設定では、 `ssc.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はスキップされます。autoconfigによって提供されるバンドルのシード処理は引き続き実行されます。

付録D: 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”:1,
      “projectVersionId”:1,
      “filename”:”file.fpr”,
      “username”:”testUser1”
    }
  ],
  “triggeredAt”:”2020-08-21T12:19:24.502+0000”,
  “sscUrl”:” http://localhost:8180/ssc”,
  “webhookId”: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 [event]フィールドがあります。

注: 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。

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
  入力可能な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”:1,
  “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”
}
```

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
  入力可能なイベントタイプ:
  - APP_VERSION_CREATED
  - APP_VERSION_UPDATED
  - APP_VERSION_DELETED

例:

```
{
   “event”:”APP_VERSION_CREATED”,
   “projectId”:1,
   “projectName”:”Test application”,
   “projectVersionId”:1,
   “projectVersionName”:”v1”
}
```

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のID

- previousProjectVersionName - (親)アプリケーションバージョンの名前
- 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”
}
```

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”
}
```

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 - Fortify Software Security Center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 - Fortify Software Security Center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 - Fortify Software Security Center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”
}
```

ドキュメントのフィードバックを送信する

このドキュメントに関するご意見は、電子メールでドキュメントチームまでお寄せください。

注: 弊社製品に関する技術的な問題が発生した場合は、ドキュメントチームに電子メールを送信しないでください。代わりに、Micro Focus Fortifyカスタマサポート (https://www.microfocus.com/support)にご連絡いただくと、サポートを受けることができます。

このコンピュータに電子メールクライアントが設定されている場合は、前のドキュメントチームに連絡するためのリンクをクリックすると、表題の行に以下の情報が付いた状態で電子メールウィンドウが開きます。

ユーザガイド(Fortify Software Security Center 21.2.0)に関するフィードバック

電子メールにフィードバックを追加して、［送信］をクリックします。

電子メールクライアントが使用できない場合は、前の情報をWebメールクライアントの新しいメッセージにコピーして、FortifyDocTeam@microfocus.comにフィードバックを送信してください。

皆様のご意見をお待ちしております。