opentext™

OpenText™ Fortify Software Security Center

ソフトウェアバージョン: 24.2.0

ユーザガイド

ドキュメントリリース日 : 2024年5月
ソフトウェアリリース日 : 2024年5月

法的通知

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

著作権表示

商標表示

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、OpenText™ Fortify Software Security CenterCE 24.2を対象として6月 28, 2024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 16
カスタマサポートへのお問い合わせ 16
詳細情報 16
ドキュメントセットについて 16
Fortify製品の機能紹介ビデオ 17

変更ログ 18

第1章: はじめに 26
対象ユーザ 26
ドキュメント構造 26
関連ドキュメント 26
すべての製品 27
Fortify ScanCentral DAST 28
Fortify ScanCentral SAST 28
Fortify Static Code Analyzer 29
Fortify WebInspect 30
Fortify WebInspect Enterprise 32

Part I: Fortify Software Security Centerの展開 34
第2章: セキュリティ保護された展開の提供 35
施設へのアクセスのセキュリティ保護 35
Tomcatサーバのセキュリティ保護 35
より安全な暗号スイートの使用 35
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 36
HTTPSおよびSSL通信の使用について 36
HTTPSを使用してFortify Software Security Centerと通信するように Fortify Static Code Analyzerアプリケーションを設定する 36
パスワードとユーザ役割のセキュリティ保護について 37
コンピュータサービスとアカウントの管理 38
第3章: Fortify Software Security Centerの展開の準備 39
大まかな展開タスク 39
展開の概要 40

Fortify Software Security Centerとのコンポーネントの統合について 41
Fortify Software Security Centerインストール環境 45
Fortify Software Security Center ファイルをダウンロードする 47
Fortify Software Security Centerソフトウェアの解凍と展開 47
Fortify Software Security CenterをKubernetesクラスタへ展開する 49
Fortify Software Security CenterのKubernetes展開 50
KubernetesクラスタへのFortify Software Security Center展開のトラブルシューティング 53
<fortify.home>ディレクトリについて 56
デフォルトディレクトリ位置 56
デフォルトの場所を変更する 56
ディレクトリの内容 57
Fortify Software Security Centerデータベースについて 59
JDBCドライバについて 59
Fortify Software Security Centerデータベース文字セットのサポートについて 60
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 60
ディスクI/Oの監視 60
データベースユーザアカウント権限 60
データベース固有の設定要件 61
Microsoft SQL Serverデータベースの使用 61
Windowsドメイン認証 62
MySQLデータベースの設定 63
Oracleデータベースの設定 65
「No more data to read from socket」エラーの防止 65
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 65
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 67
Fortify Software Security Centerデータベースのシード処理について 67
Fortify Software Security Centerデータベースの永久削除 68
第4章: Fortify Software Security Centerの初回設定 70
第5章: Fortify Software Security Centerへのログイン 76
セッションログアウトについて 77
非アクティブセッションのタイムアウト 78
ログアウト画面 79
第6章: 追加のFortify Software Security Center設定 80
管理(Administration)]ビューでの環境設定へのアクセス 80
問題統計しきい値の設定 81
レビューする平均日数と修復する平均日数の計算方法 81

問題統計しきい値の設定 81
管理(Administration)]ビューで使用可能な環境設定オプション 82
アプリケーションセキュリティトレーニングの設定 85
監査アシスタントについて 86
Fortify Audit Assistant認証トークンの取得 87
Audit Assistantの設定 87
監査アシスタントの自動予測について 90
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 90
BIRTレポート用のセキュリティの設定 93
Javaセキュリティマネージャの有効化 93
(OpenJDKのみのLinux)必要なフォントのインストール 94
レポーティング用のデータベースアカウントの作成 94
レポート生成用のメモリの割り当て 95
レポート生成タイムアウトの設定 95
コア設定の設定 96
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 99
電子メールアラート通知設定の設定 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 102
問題監査の競合を解決するための戦略を設定する 104
Java Message Service設定の設定 105
Kafkaの設定 106
Fortify Software Security Centerユーザ認証について 108
LDAPユーザ認証 108
LDAP認証の設定の準備 108
複数のLDAPサーバの要件 109
LDAPサーバreferral機能について 110
LDAP referralサポートを無効化する 111
LDAPサーバの設定 111
LDAPサーバ設定を編集する 120
LDAPサーバ設定の削除 121
LDAPサーバ設定のインポート 121
LDAPエンティティの登録 122
LDAPエンティティの手動更新 124
「無効」にマークされたLDAPエントリの処理 125
LDAPキャッシュの永続性の有効化 125
SCIM 2.0プロトコルの実装 127
SCIM 2.0およびSAML 2.0を使用したユーザプロビジョニング用のMicrosoft Entra IDへの接続の設定 129

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 132
Fortify Software Security Center統合のプロキシの設定 132
Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設定 134
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 135
ジョブスケジューラの設定 135
ジョブ実行優先度の設定 141
スケジュールされたジョブのキャンセル 143
繰り返し実行されるクリーンアップジョブ 143
Fortify Software Security Centerのブラウザアクセスセキュリティの設定 146
シングルサインオンを使用するためのFortify Software Security Centerの設定 148
設定に関する制限 149
Central Authenticationサービスを使用するためのFortify Software Security Centerの設定 149
SAML 2.0準拠のシングルサインオンを使用するためのFortify Software Security Centerの設定 150
SAML SSO統合のトラブルシューティング 155
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 156
Fortify Software Security CenterでのKerberos認証の設定 158
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 160
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 161
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 162
トークン認証が必要なWebサービスの設定 162
Fortify Software Security Centerのログレベルの変更 163
連邦情報処理標準(FIPS)環境でのFortify Software Security Centerの実行 164
Fortifyバナーの組織向けカスタマイズ 164
システム全体のバナーを作成する 166
ダッシュボードへのFortify Insightリンクの追加 167
[Fortify Software Security Centerについて(About Fortify Software Security Center)]ボックスのサポート連絡先リンクを変更する 168
Fortify Software Security Centerログ記録のカスタマイズ 170

Fortify Software Security Centerのログインに必要なパスワード強度の設定 171
第7章: 追加のインストール関連タスク 172
CSVファイルへのデータエクスポートのブロック 172
バグトラッカーの統合について 172
バグトラッカプラグインの管理 174
バグトラッカプラグインの追加 174
バグトラッカプラグインの削除 176
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 176
バグトラッカパラメータ 176
ALMパラメータ 177
パーサプラグインの追加と管理 177
Sonatype結果を表示するためのFortify Software Security Centerの準備 178
Debricked結果を表示するためのFortify Software Security Centerの準備 180
管理者アカウント 182
Fortify Software Security Centerユーザ管理について 182
Fortify Software Security Centerユーザアカウント 182
ユーザアカウントの作成について 183
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 184
Fortify Software Security Centerの役割に関する許可情報の表示 184
LDAPユーザ役割の管理について 185
Fortify Software Security Centerのグループメンバーシップ 185
失敗したLDAPユーザログインの処理 186
LDAPグループへのFortify Software Security Center役割のマッピングについて 187
Fortify Software Security Centerのグローバル検索機能 187
グローバル検索機能について 187
検索インデックスの問題のトラブルシューティング 188
Fortify Software Security Centerの保守モードへの移行 188
Fortify Software Security Centerが保守モードでスタックしている場合 190
ジョブ実行の一時停止と再開 191
Fortify Software Security Contentについて 192
Fortify更新サーバからのルールパックの更新 193
Rulepacksをエクスポートする 194
セキュリティコンテンツのインポート 194
ルールパックの削除 195

現在のマッピングを拡張する 196
新しいマッピングの作成 196
第8章: Fortify Software Security Centerのアップグレード 198
Fortify Software Security Centerデータベースのアップグレードタスク 199
Fortify Software Security Centerデータベースのアップグレードの準備 200
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 200
データベースアップグレードスクリプトの実行準備 201
WARファイルの更新と展開 201
アップグレード後のFortify Software Security Centerの設定 201
Fortify Audit WorkbenchからのFortify Static Code Analyzerのアップグレード 205
Fortify Static Code AnalyzerおよびFortifyのアプリとツールのAudit Workbenchからのアップグレードを有効化する 205
Fortify Audit Assistantの設定の更新 206
期限切れライセンスの更新 207
四半期ごとにリリースされるセキュリティコンテンツ 207
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 208

Part II: Fortify Software Security Centerの使用 210
第9章: Fortify Software Security Centerの使用 211
Fortify Software Security Centerの中心的役割について 211
セキュリティ管理ワークフロー 212
ユーザアカウントとアクセス 213
Active Directory/LDAPの統合 213
初めてのFortify Software Security Centerへのログイン 213
Fortify Software Security Centerへのアクセス権の要求 214
パスワードの変更 216
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 218
Fortify Software Security Centerダッシュボードについて 219
[ssue Stats] ページ 219
データをカンマ区切り値ファイルへエクスポートする 222
ダッシュボードサマリテーブルをエクスポートする 222
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 223
Fortify Software Security Center APIドキュメントへのアクセス 225
Fortify Software Security Centerのキーボードホットキーの表示 226
第10章: ユーザアカウントの管理 227

Fortify Software Security Centerのユーザアカウント管理 227
チームのトラッキングについて 227
役割について 227
事前設定済みの役割 227
カスタム役割の作成 228
カスタム役割の削除 230
Fortify Software Security Centerアカウント管理 230
ローカルユーザアカウントの作成 230
ローカルユーザアカウントを編集する 233
ローカルユーザアカウントのロック解除 235
外部管理されたユーザおよびグループを表示する 236
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 236
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 238
開発チームのトラッキングについて 240
アプリケーション作成プロセスについて 240
アプリケーションバージョンを作成するための戦略 241
パッケージソフトウェアの戦略 241
継続的な展開のための戦略 242
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 242
Fortify Software Security Centerアプリケーションリストの表示 242
アプリケーションバージョンの作成について 242
アプリケーションバージョン属性 242
カスタム属性の作成 244
属性と属性値の削除 247
属性の削除 247
属性値の削除 248
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 250
問題テンプレートについて 251
システムへの問題テンプレートの追加 252
問題テンプレートの作成または変更 252
テンプレートの選択 252
新しいアプリケーションの最初のバージョンの作成 253
アプリケーションに新しいバージョンを追加する 256
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 260
[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 263
アプリケーション概要ページの更新 263
アプリケーションバージョンの詳細を編集する 263
アプリケーションバージョンをデフォルトのデータ保持ポリシーからオプトアウ264

トするための設定
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 264
バグトラッカの設定 265
バグ報告用Velocityテンプレート 266
バグトラッカプラグインへのVelocityテンプレートの追加 266
バグトラッカプラグインのVelocityテンプレートのカスタマイズ 267
Velocityテンプレートの削除 269
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 269
単一の問題のバグの送信 271
複数の問題のバグの送信 272
バグ状態管理 273
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 273
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 275
インスタンスIDマイグレーションに影響する処理ルールについて 280
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 281
カスタムタグ 282
システムへのカスタムタグの追加 283
カスタムタグ属性の変更 286
カスタムタグをグローバルで非表示にする 286
カスタムタグの削除 286
カスタムタグ値の追加 287
カスタムタグ値を追加する 287
カスタムタグ値を追加する(Fortify Audit Assistantが設定済みの場合) 288
問題の状態を設定する 291
カスタムタグを編集する 293
カスタムタグ値の削除 293
カスタムタグと問題テンプレートを関連付ける 294
問題テンプレートからのカスタムタグの削除 294
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 295
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 297
問題テンプレートによるカスタムタグの管理 297
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 298
データ保持について 298
データ保持の有効化 298
デフォルトのデータ保持ポリシーの編集 302
アプリケーションバージョンの削除について 303
アプリケーションバージョンの無効化 303
アプリケーションバージョンの再有効化 304
アプリケーションバージョンの削除 305

第12章: Webhookについて 307
Webhookの許可 307
Webhookの作成 308
Webhookを編集する 313
Webhookペイロードの表示 313
Webhookペイロードの再配信 316
Webhookの削除 317
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 318
変数の使用 318
変数の作成 319
変数の構文 319
パフォーマンスインジケータ 320
パフォーマンスインジケータの作成 320
アラート定義 321
アラートの作成 322
アラートを編集する 325
アラートの削除 325
アラートの表示とマーク 325
第14章: スキャンアーティファクトの操作について 327
スキャンアーティファクトのアップロード 327
ファイル処理エラーの表示 329
スキャンアーティファクトの詳細の表示 330
スキャンアーティファクトをダウンロードする 331
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 331
個々のスキャン結果をダウンロードする 332
アプリケーションバージョンの分析結果を承認する 332
承認処理を拒否する 333
高レベルサマリ結果の表示 334
[Issue Stats] ページにサマリメトリックを表示する 334
[CHART] ページにサマリメトリックを表示する 335
[Overview] ページにサマリメトリックを表示する 336
問題メタデータの表示 337
外部リストへのスキャン結果のマッピング 338
スキャンアーティファクトのパージ 339
アーティファクトの削除 341
第15章: 協同監査 343
現在の問題の状態について 345
監査する問題に関する情報の表示 345
フォルダに基づく問題の表示 347

ユーザに割り当てられた問題の表示 349
[OVERVIEW]および[AUDIT]ページに表示する問題をフィルタ処理する 349
問題の検索 352
検索修飾子 354
検索クエリの例 357
スキャン結果の監査 358
相関する問題の監査 366
抑止、削除、および非表示の問題について 367
問題の表示設定の設定 368
抑止された問題の表示 368
削除された問題の表示 369
非表示の問題の表示 369
フィルタセットを使用して表示問題を変更する 370
割り当てられた問題の優先度の上書き 371
Fortify Software Security Center上で優先度の上書き機能を有効または無効にする 372
監査中に優先度値を上書きする 373
問題に対して送信されたバグの表示 376
問題のバッチの監査 376
Audit Assistantの使用 377
Audit Assistantワークフロー 377
監査アシスタントについて 379
Fortify Audit Assistantのベストプラクティス 379
タグの一貫した使用 380
予測しきい値の管理 380
監査官が行った決定を使用してモデルをトレーニングする 381
予測ポリシーについて 381
予測ポリシーの定義 382
Fortify Audit Assistantの設定の更新 383
Audit Assistantの使用 384
Audit Assistantワークフロー 384
Audit Assistantの設定 385
Fortify Audit Assistant認証トークンの取得 389
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 389
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 391
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 392
Audit Assistantの結果の確認 396
Audit Assistantのトレーニングについて 397
Audit Assistantトレーニングタグの選択 398

Audit Assistantへのトレーニングデータの送信 399
Fortify Software Security Centerでのグローバル検索 400
Webアプリケーションの被影響性分析について 402
被影響性分析の要件 402
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 403
オープンソースデータのエクスポート 404
Fortify Software Security CenterとFortify WebInspect Enterpriseの統合 405
Fortify Software Security CenterでのFortify WebInspectスキャン結果の表示 406
WebInspectの監査データ 408
誤検出 408
動的スキャン要求をFortify WebInspect Enterpriseに送信する 409
Fortify WebInspect Enterpriseの動的スキャン要求の処理 411
動的スキャン要求を編集およびキャンセルする 412
動的スキャン要求状態 412
動的スキャン要求を編集する 412
動的スキャン要求をキャンセルする 412
オープンソースデータの表示 413
[監査(AUDIT)]ページからのオープンソースデータの表示 413
[オープンソース(OPEN SOURCE)]ページからのオープンソースデータの表示 413
Debricked SBOMのダウンロード 415
第16章: Fortify ScanCentral SASTの使用 417
ScanCentral SASTの許可 418
ScanCentral SASTスキャン要求の詳細の表示 419
ScanCentral SASTスキャン要求の優先順位付け 421
ScanCentral SASTスキャン要求のキャンセル 422
ScanCentral SASTセンサ情報の表示 422
ScanCentral Controller情報の表示 424
コントローラの停止 424
ScanCentral SAST Controllerを保守モードにする 425
センサの安全なシャットダウン 426
ScanCentral SASTコントローラを保守モードから削除する 426
ScanCentral SASTセンサプールについて 427
定義済みのセンサプール 427
ScanCentral SASTセンサプールの作成 428
ScanCentral SASTセンサのプール間での移動 430
ScanCentralプールの削除 431
第17章: Fortify ScanCentral DASTの使用 432

ScanCentral DASTの許可 432
ScanCentral DASTへの動的スキャン要求の送信 434
Kafkaを使用したFortify ScanCentral DASTの監査履歴変更の同期 434
第18章: BIRTレポート 435
BIRTライブラリ 435
レポートライブラリのインポート 436
レポートを生成して表示する 436
BIRTレポートのカスタマイズ 439
BIRT Report Designerの取得 440
レポートテンプレートをダウンロードする 440
カスタマイズされたBIRTレポートのXLSX形式による生成とダウンロード 442
レポート定義のインポート 443
第19章: 認証トークン 445
認証トークンを生成する 445
管理(Administration)]ビューからのトークンの生成 445
コマンドラインからトークンを生成する 447
認証トークンを編集する 449
認証トークンの削除 449

付録A: fortifyclientユーティリティの使用 450
fortifyclientの要件 450
Fortify Software Security Center URLの指定について 451
fortifyclient認証トークン 451
fortifyclient HTTPタイムアウト 451
fortifyclientクライアントオプションとパラメータの一覧 452
アップロード認証トークンについて 452
fortifyclientを使用したアップロード認証トークンの取得 452
fortifyclient認証トークンでのDaysToLiveの指定 453
fortifyclient認証トークンの一覧 454
トークンの無効化 454
アプリケーションバージョンの一覧表示 455
アプリケーションバージョンのパージ 456
FPRのアップロードについて 456
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 457
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 457
FPRのダウンロードについて 458

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 459
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 459
コンテンツバンドルのインポート 460
監査添付ファイルをダウンロードする 461

付録B: バグトラッカプラグインの作成 462
使用例 462
コンポーネントのセットアップ 463
実装 463
プラグインメソッドとメソッドコール 465
Plugin Helper 470
エラー処理 471
ほぼステートレス 471
バグトラッカプラグインのデバッグ 471
カスタマイズしたバグトラッカープラグインの展開 472

付録C: Fortify Software Security Centerの設定の自動化 474

付録D: Webhookのペイロード 477
イベントペイロード 478
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 479
プロジェクトバージョンペイロード 479
プロジェクトバージョンで更新されたペイロード 480
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 481
レポート生成ペイロード 482
ユーザペイロード 483

ドキュメントのフィードバックを送信する 485

序文

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、FortifyコミュニティのOpenText Fortify製品のお知らせを購読してください。

https://community.microfocus.com/cyberres/fortify/w/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、IDおよびこのドキュメントに加えられた変更を一覧表示します。

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
24.2.0	**追加** • 管理者はデータ保持を有効にして、アプリケーションバージョンのアーティファクトを保持する期間を定義できます。詳細については、「"データ保持について" ページ298」を参照してください。 • UIテーマを変更できます。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218」を参照してください。 • 「"カスタマイズされたBIRTレポートのXLSX形式による生成とダウンロード" ページ442」では、カスタマイズしたBIRTレポートをXLSX形式でダウンロードする方法が説明されています。 • Kafkaを設定して、抑止された問題、優先度の上書き、および分析タグに関する監査履歴の変更を、FortifyScanCentral DASTと同期することができます。詳細については、「"Kafkaを使用したFortify ScanCentral DASTの監査履歴変更の同期" ページ434」と「"Kafkaの設定" ページ106」を参照してください。 • `fortifyclient`の接続、読み取り、および書き込みのタイムアウトを設定できます。詳細については、「"fortifyclient HTTPタイムアウト" ページ451」を参照してください。 **更新** • 「"ディスクI/Oの監視" ページ60」に情報メモが追加されました。 • 「"繰り返し実行されるクリーンアップジョブ" ページ143」のLDAP更新のデフォルトのスケジュールが変更されました。 • 「"SAML 2.0準拠のシングルサインオンを使用するためのFortify Software Security Centerの設定" ページ150」のIdPメタデータの場所とキーストアの場所が変更されました。 • 「"パフォーマンスインジケータ" ページ320」および「"パフォーマンスインジケータの作成" ページ320」にあるサポートされている演算子のリス

ソフトウェアリリース/ドキュメント改訂	変更点
	トを更新しました。 • 「"カスタムタグ値の追加" ページ287」の「問題の状態を設定する」セクションに問題の状態に関する説明が追加されました。 • 「"ジョブスケジューラの設定" ページ135」で、デフォルトのジョブ実行戦略が [柔軟(Flexible)] に変更されました。 **削除** • 「"BIRTレポート用のセキュリティの設定" ページ93」のテーブル名 `activity`、`requirement`、`requirementtemplate`。 • 「"認証トークンを生成する" ページ445」の「コマンドラインからトークンを生成する」セクションのAuditToken。 • 「"バグトラッカプラグインの管理" ページ174」の「バグトラッカプラグインの追加」セクションの、Bugzilla用バグトラッカプラグイン。
23.2.0	**追加** • "Fortify Audit Assistantのベストプラクティス" ページ379では、新しいGen 2エンジンが搭載された最新バージョンのOpenText Fortify Audit Assistantにアップグレードする際の、Fortify Audit Assistantのベストプラクティスが説明されています。 • Fortify Audit Assistantがバージョン23.2.0にアップグレードされ、その変更に対応するためにFortify Audit Assistantに関するトピックが更新されました。 • "Fortify Audit Assistantの設定の更新" ページ383では、Audit Assistantの新しいG2予測エンジンを使用できるようにFortify Audit Assistantを設定する方法が説明されています。 • "連邦情報処理標準(FIPS)環境でのFortify Software Security Centerの実行" ページ164 • MySQLおよびMS SQLデータベースユーザ向けの`scan_issue(ID)`が、INTからBIGINTに変更されました。詳細については、"Fortify Software Security Centerデータベースのアップグレードの準備" ページ200を参照してください。 • Fortify ScanCentral DASTで、ベースURLアプリケーションバージョン属性の設定がサポートされるようになりました。ベースURLは、"新し

ソフトウェアリリース/ドキュメント改訂	変更点
	いアプリケーションの最初のバージョンの作成" ページ253または"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256で設定できます。 • AutomationTokenは、REST APIのほとんどへのアクセスを提供する新しいAPIトークンです。詳細については、"認証トークンを生成する" ページ445を参照してください。 • Debricked Software Bill of Materials (SBOM)のダウンロードのサポート。詳細については、"Debricked SBOMのダウンロード" ページ415を参照してください。 • 新しいシステム全体のバナーを使用することにより、管理者は削除されるまで残るメッセージをSSCに追加できます。詳細については、"システム全体のバナーを作成する" ページ166を参照してください。 **更新** • Microsoft Azure ADおよびAzure Active Directoryへの参照はすべて、それぞれMicrosoft Entra IDおよびMicrosoft Entraに変更されました。 • UIおよびドキュメント全体を通して、Micro FocusがOpenTextに置き換えられました。 • 以前は、監査中にユーザが一旦割り当てられると、問題からユーザを削除する方法がありませんでした。このリリースでは、問題に割り当てられたユーザの削除または変更を [監査(Audit)] ページで行えます。詳細については、"スキャン結果の監査" ページ358のステップ13にあるメモを参照してください。 • "カスタムタグ値の追加" ページ287の「問題の状態を設定する」セクションに、問題の状態の設定に関する手順を追加しました。 • 以前は、新しいアプリケーションバージョンを作成し、既存のアプリケーションバージョンに基づくようにそのバージョンを設定し、アプリケーションの状態を保存することを選択した場合、 [検出日(Detected on date)] は保持されませんでした。検出日は、問題のコピー元となったアプリケーションバージョンの最新スキャンの日付に変更されました。このリリースでは、 [検出日(Detected on date)] が永続化され、新しいアプリケーションバージョンで使用でき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
	削除 • PackageFinderおよびProjectProvisioningのサンプルは、Samplesフォルダ(*<ssc_install_dir>/Samples/*)から削除され、サポートされなくなりました。 • Fortify Audit Assistant G2モデルでは異なるトレーニングメソッドが使用されるため、「メタデータ共有を有効にする」のトピックが削除されました。 • 次のレポートが非推奨になりました。SANS 2009および2010、STIG 4.10、4.9、およびそれ以前、OWASP 2013およびそれ以前、CWE Top 25 2019および2020、WASC 24 +2。 • SOAP APIはデフォルトで無効になっており、すべてのSOAP API要求は「410 Gone」応答で拒否されます。SOAP API (/fm-ws/*)エンドポイントの代わりに、REST API (/api/v1/*、/download/*、および/transfer/*)エンドポイントを使用してください。詳細については、Fortify Softwareバージョン23.2.0リリースノートを参照してください。 • REST APIベースのfortifyclientが、プライマリfortifyclientユーティリティです。これは、Tools/fortifyclientフォルダにあります。詳細については、Fortify Softwareバージョン23.2.0リリースノートを参照してください。
23.1.0	企業所有権の変更を反映して、Micro Focusへの参照のほとんどが削除されました。 **追加:** • "ダッシュボードへのFortify Insightリンクの追加" ページ167 • "Fortify Software Security Centerのログインに必要なパスワード強度の設定" ページ171 **更新:** • "Tomcatサーバのセキュリティ保護" ページ35に、セキュア暗号スイートの使用に関する情報が追加されました。 • "Fortify Software Security Center ファイルをダウンロードする" ページ47で、ハウツー動画のURLが変更されました。 • "Fortify Software Security Centerデータベースのシード処理につい

ソフトウェアリリース/ドキュメント改訂	変更点
	て" ページ67に注意メモが追加されました。 • "Fortify Software Security Centerの初回設定" ページ70に情報メモが追加されました。 • "LDAPサーバの設定" ページ111で、キャッシュされたLDAPユーザデータに関する注記が変更されました。 • "ジョブスケジューラの設定" ページ135で、新たに導入された柔軟なジョブ実行戦略の説明が追加されました。 • IdPによって送信されるログアウト応答およびログアウト要求に署名する必要があるという注記と、1つの新しいステップが、"SAML 2.0準拠の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150に追加されました。 • サブジェクト代替名(SAN)拡張を検索する機能に関する情報が、"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160に追加されました。 • " [Fortify Software Security Centerについて(About Fortify Software Security Center)]ボックスのサポート連絡先リンクを変更する" ページ168で、 [バージョン情報(About)]ボックスのサポート連絡先リンクを変更する手順が変更されました。 • 失敗したLDAPユーザログインを処理するためのトラブルシューティング情報が、"失敗したLDAPユーザログインの処理" ページ186に追加されました。 • "Fortify Static Code AnalyzerおよびFortifyのアプリとツールのAudit Workbenchからのアップグレードを有効化する" ページ205で、Fortify Static Code AnalyzerおよびFortifyのアプリとツールのFortify Software Security Centerからのアップグレードを有効化する手順が変更され、このリリースでのインストールファイルの分離が反映されました。 • "Webhookの作成" ページ308に、グローバルイベントとアプリケーションバージョンイベントの説明が追加されました。 • "検索クエリの例" ページ357から古い検索クエリの例が削除されました。 • "割り当てられた問題の優先度の上書き" ページ371に、新しいセクション「問題レポートでの優先度の上書き情報の表示」を追加し、

ソフトウェアリリース/ドキュメント改訂	変更点
	優先度の上書きがレポートでどのように表現されるようになったのかを説明しました。「制限事項」セクションが、このトピックから削除されました。 **削除:** Micro Focus Fortify Software Security Center 22.2.0の新機能 Eclipseプラグイン更新サイトの設定
22.2.0	**追加:** • Micro Focus Fortify Software Security Center 22.2.0の新機能 • "Fortify Software Security Centerのログインに必要なパスワード強度の設定" ページ171 • "Fortify Software Security CenterをKubernetesクラスタへ展開する" ページ49に、"Apache Tomcatアクセスログのカスタマイズ" ページ53という新しいセクションが追加されました。展開手順も変更されました。 • "LDAPキャッシュの永続性の有効化" ページ125 • "[Fortify Software Security Centerについて(About Fortify Software Security Center)]ボックスのサポート連絡先リンクを変更する" ページ168 • "Fortify Software Security Centerログ記録のカスタマイズ" ページ170 • "Debricked結果を表示するためのFortify Software Security Centerの準備" ページ180 • "割り当てられた問題の優先度の上書き" ページ371 • "オープンソースデータの表示" ページ413 • "ScanCentral SASTスキャン要求の優先順位付け" ページ421 • "ScanCentral SASTセンサのプール間での移動" ページ430 **更新:** • "Fortify Software Security Centerとのコンポーネントの統合について" ページ41のファイルダウンロード用URL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.home>ディレクトリについて" ページ56で、*<fortify.home>*ディレクトリ内容の説明の一部が変更されました。 • "BIRTレポート用のセキュリティの設定" ページ93に、非GUIのLinux OSに関する重要な注意が追加されました。 • 「LDAPエンティティの識別名の更新」というトピックタイトルが、"「無効」にマークされたLDAPエントリの処理" ページ125に変更されました。 • "SAML 2.0準拠のシングルサインオンを使用するためのFortify Software Security Centerの設定" ページ150で、SAML 2.0を使用するSSOを使用するためのFortify Software Security Centerの設定手順が大幅に改訂されました。 • "バグトラッカーの統合について" ページ172に、Azure DevOpsに必要なパーソナルアクセストークンに関する重要な注意が追加されました。 • "Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ178の手順が編集され、ファイルダウンロード用URLが変更されました。 • "Fortify Software Security Centerのアップグレード" ページ198で、アップグレードのバージョン番号が更新されました。 • "Fortify Software Security Centerデータベースのアップグレードタスク" ページ199に、Microsoft SQLデータベースに関する重要な注意が追加されました。 • "Fortify Software Security Center APIドキュメントへのアクセス" ページ225が改訂され、 [Fortify Software Security Center <version>について(About Fortify Software Security Center *<version>*)]ボックスの変更が反映されました。 • 「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」という見出しが、"バグトラッカプラグインのVelocityテンプレートのカスタマイズ" ページ267に変更されました。 • "監査する問題に関する情報の表示" ページ345に列ソートに関する注意が追加されました。 • "問題の検索" ページ352に日付タイプのカスタムタグの問題を検索

ソフトウェアリリース/ドキュメント改訂	変更点
	する方法に関する情報が追加されました。 • "検索修飾子" ページ354で、[fortify priority order]修飾子の説明が変更され、修飾子の表に[engine priority]修飾子が追加されました。 • 「Fortify Scan結果の監査」という見出しが、"スキャン結果の監査" ページ358に変更されました。 • "Webアプリケーションの被影響性分析について" ページ402のファイルダウンロード用URLが変更されました。 • 「Sonatypeデータをエクスポートする」というトピックが、"オープンソースデータのエクスポート" ページ404に変更されました。 • "BIRTライブラリ" ページ435と"レポートライブラリのインポート" ページ436に、非GUIのLinux OSからレポートを生成する際の重要な注意が追加されました。 • "BIRT Report Designerの取得" ページ440で、Eclipseダウンロードページのが修正され、Eclipse BIRT Report Designerのインストール方法に関する説明が記載されたURLが含められました。 • "認証トークンを生成する" ページ445で、トークンの有効期限の延長に関する誤った表現が修正されました。 **削除:** • Micro Focus Fortify Software Security Center 22.1.0の新機能 • SCIM/Entra ID統合のためのSAML 2.0シングルサインオンの設定

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 ScanCentral SAST、ScanCentral DAST、およびSonatypeの相関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かつ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225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I ("Fortify Software Security Centerの展開" ページ34)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II ("Fortify Software Security Centerの使用" ページ210の使用)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、Fortifyソフトウェア製品に関する情報を提供しているドキュメントについて説明します。

注: 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。別段の記載がある場合を除き、これらのドキュメントは製品ドキュメントWebサイトで入手できます。

ドキュメント/ファイル名	説明
Fortifyソフトウェアドキュメントについて About_Fortify_Docs_<*version*>.pdf	この文書では、Fortify製品のドキュメント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。
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。
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。
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。
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。

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。別段の記載がある場合を除き、このドキュメントは製品ドキュメントWebサイト(https://www.microfocus.com/documentation/fortify-ScanCentral-DAST)で入手できます。

ドキュメント/ファイル名	説明
Fortify ScanCentral DASTの設定および使用ガイド 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。

Fortify ScanCentral SAST

次のドキュメントでは、Fortify ScanCentral SASTの情報について説明します。別段の記載がある場合を除き、このドキュメントは製品ドキュメントWebサイト(https://www.microfocus.com/documentation/fortify-software-security-center)で入手できます。

ドキュメント/ファイル名	説明
Fortify ScanCentral SASTインストール、設定、および使用ガイド 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。

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。別段の記載がある場合を除き、これらのドキュメントは製品ドキュメントWebサイト(https://www.microfocus.com/documentation/fortify-static-code)で入手できます。

ドキュメント/ファイル名	説明
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。
Fortify Static Code Analyzerアプリケーションおよびツールガイド SCA_Apps_Tools_<*version*>.pdf	このドキュメントでは、Fortify Static Code Analyzerのアプリケーションとツールのインストール方法について説明します。Fortify Static Code Analyzerを使用してコードのスキャン、分析結果の確認、分析結果ファイルの操作などを行うことのできるアプリケーションとコマンドラインツールの概要を提供します。
Fortify 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。
Fortify 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。
Fortify Plugin for Eclipseユーザガイド Eclipse_Plugin_Guide_<*version*>.pdf	このドキュメントでは、Fortify Complete Plugin for Eclipseをインストールして使用する方法について説明します。

ドキュメント/ファイル名	説明
Fortify Analysis Plugin for IntelliJ IDEAおよびAndroid Studioユーザガイド IntelliJ_AnalysisPlugin_Guide_<*version*>.pdf	このドキュメントでは、Fortify Analysis Plugin for IntelliJ IDEA and Android Studioをインストールして使用する方法について説明します。
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。

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。別段の記載がある場合を除き、これらのドキュメントは製品ドキュメントWebサイト(https://www.microfocus.com/documentation/fortify-webinspect)で入手できます。

ドキュメント/ファイル名	説明
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。
Fortify WebInspect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、

ドキュメント/ファイル名	説明
	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。
Fortify WebInspectおよびOAST 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およびFortify OASTをダウンロード、設定、使用する方法について説明します。Fortify WebInspectイメージの目的は、コマンドラインインタフェース(CLI)またはアプリケーションプログラミングインタフェース(API)を経由して設定されたヘッドレスセンサとして自動化プロセスで使用することです。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。Fortify OASTは、帯域外のアプリケーションセキュリティテスト(OAST)サーバで、OAST脆弱性の検出用のDNSサービスを提供します。
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。
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。
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

ドキュメント/ファイル名	説明
	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。

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。別段の記載がある場合を除き、これらのドキュメントは製品ドキュメントWebサイト(https://www.microfocus.com/documentation/fortify-webinspect-enterprise)で入手できます。

ドキュメント/ファイル名	説明
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、FortifyWebInspect Enterpriseシステムのコンポーネントの設定方法についても説明します。これには、FortifyWebInspect 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。
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。

ドキュメント/ファイル名	説明
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。

Part 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。

より安全な暗号スイートの使用

Fortifyでは、Tomcatで弱いSSL/TLS暗号スイートを無効にして、より安全なスイートを利用することをお勧めします。

APRベースのSSL接続

APRベースのSSL接続を使用する場合は、SSLCipherSuiteディレクティブを使用します。詳細については、https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslciphersuiteおよび「Cipher Suites and Enforcing Strong Security」(https://httpd.apache.org/docs/current/ssl/ssl_howto.html)を参照してください。

JSSEベースのSSL接続

JSSEベースのSSL接続を使用する場合は、`ciphers`および`honorCipherOrder`属性を使用します。詳細については、「Apache Tomcat 9 Configuration Reference - The

HTTP Connector」を参照してください。

セキュリティの向上、相互運用性の向上、およびパフォーマンスの向上などの間にはトレードオフがあるため、暗号スイートの選択には正解がありません。ただし、Apacheは、選択に役立つ情報を提供しています(https://cwiki.apache.org/confluence/display/TOMCAT/Ciphersを参照)。

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と通信するようにFortify Static Code Analyzerアプリケーションを設定する

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 -importcert -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 -exportcert -alias SSC -keystore <keystore_used_by_tomcat> -
file
YourCertFile.cer
```

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

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76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227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108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198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47
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47
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	Tomcatサーバを起動してから、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76を参照してください)。	"Fortify Software Security Centerへのログイン" ページ76
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70

タスク	説明	情報と手順
	ヒント: 上級ユーザ専用: Fortify Software Security Centerを展開する前に設定を自動化できます。その後は、サーバの起動時にセットアップウィザードで環境設定が取得され、インストール全体が自動化されます。詳細については、"Fortify Software Security Centerの設定の自動化" ページ474を参照してください。	
6	Fortify Software Security Centerサーバを再起動します。	
7	管理(Administration)]ビューでFortify Software Security Centerの設定を完了します。(管理(Administration)]ビューで設定するオプションのリストについては、" 管理(Administration)]ビューで使用可能な環境設定オプション" ページ82を参照してください)。	"追加のFortify Software Security Center設定" ページ80
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172

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68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。

ヒント: 上級ユーザ専用。Fortify Software Security Centerを展開する前に設定を自動化できます。

Fortify Software Security Centerの初期設定が終了したら、コアパラメータの設定を完了し、 管理(Administration)]ビューから追加の設定を行います。手順については、"追加のFortify Software Security Center設定" ページ80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、『OpenText™ 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-	"SCIMによる外部管理されたユーザおよびグループのプロ

コンポーネント	統合手順
domain Identity Management (SCIM)	ビジョニングの有効化" ページ132 "SAML 2.0準拠の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150
Fortify Audit Assistant	"Audit Assistantの設定" ページ385
Java Message Service (JMS)	"Java Message Service設定の設定" ページ105
LDAPサーバ	"LDAPサーバの設定" ページ111
シングルサインオン(SSO)プロバイダ:	
• Central Authenticationサービス(CAS)	"Central Authenticationサービスを使用するためのFortify Software Security Centerの設定" ページ149
• SPNEGO/Kerberos	"Fortify Software Security CenterでのKerberos認証の設定" ページ158
• SAML	"SAML 2.0準拠の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150
• 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156
• 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160
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134
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135
Fortify Static Code Analyzerアプリケーションとツール:	
• Fortify Audit Workbench	*Fortify Audit Workbenchユーザガイド* https://www.microfocus.com/ja-

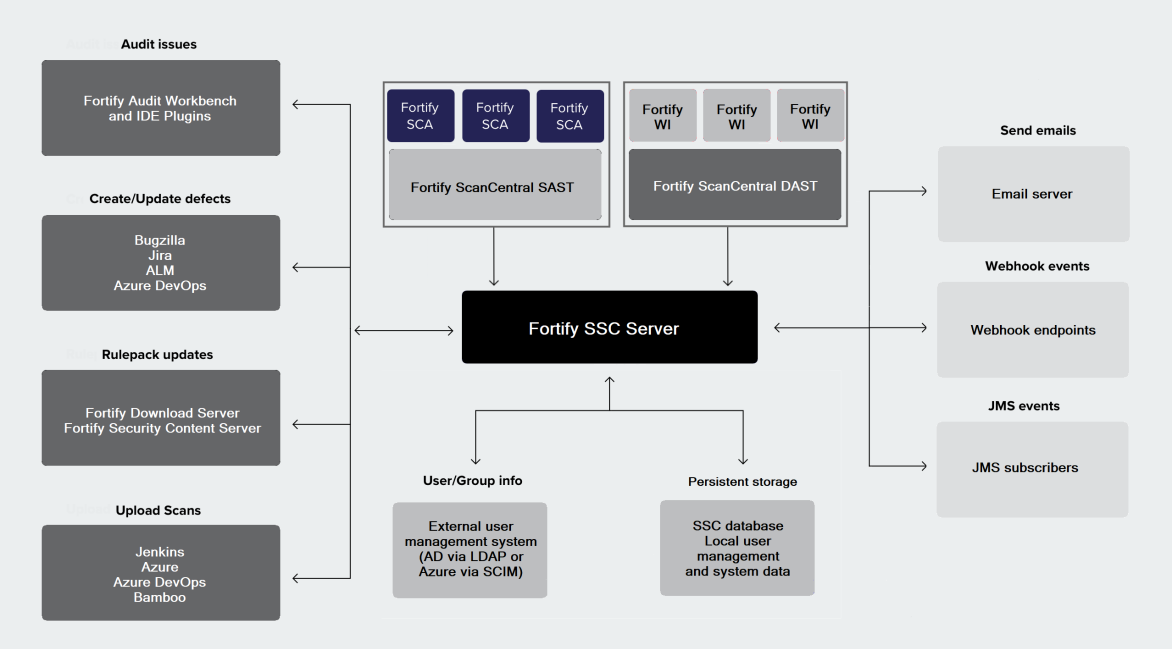
コンポーネント	統合手順
	jp/documentation/fortify-static-code-analyzer-and-tools
• Fortify Jenkinsプラグイン	*Fortify Jenkinsプラグインユーザガイド* https://www.microfocus.com/ja-jp/documentation/fortify-jenkins-plugin
• Fortify Eclipseプラグイン	*Fortify Plugin for Eclipseユーザガイド* https://www.microfocus.com/ja-jp/documentation/fortify-static-code-analyzer-and-tools
• Fortify Extension for Visual Studio	*Fortify Extension for Visual Studioユーザガイド* https://www.microfocus.com/ja-jp/documentation/fortify-visual-studio-code
• Fortify Extension for Visual Studio Code	Fortify Visual Studio Codeドキュメント https://www.microfocus.com/ja-jp/documentation/fortify-visual-studio-code
• Fortify Plugin for Bamboo	Fortify Plugin for Bambooユーザガイド https://www.microfocus.com/ja-jp/documentation/fortify-plugin-for-bamboo
• Fortify Analysis Plugin for IntelliJ IDEAおよびAndroid Studio	*Fortify Analysis Plugin for IntelliJ IDEAおよびAndroid Studioユーザガイド* https://www.microfocus.com/ja-jp/documentation/fortify-static-code-analyzer-and-tools
• Fortify Remediation Plugin for Eclipse	*Fortify Remediation Plugin for Eclipseユーザガイド*
• Fortify Remediation Plugin for IntelliJ IDEAおよびAndroid Studio	*Fortify Remediation Plugin for IntelliJ IDEAおよびAndroid Studioユーザガイド*
• Fortify SourceAndLibScanner	Fortify Marketplace (https://marketplace.microfocus.com/cyberres/category/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

コンポーネント	統合手順
	しています。
Fortify Azure DevOps Extension	https://www.microfocus.com/ja-jp/documentation/fortify-azure-devops-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85

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40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
Fortify SSC サーバ	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。
SSCデータベース	ユーザおよびアーティファクトデータを保存するために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。
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。
欠陥トラッキン	(オプション) Bugzilla、Jira、ALM、Azure DevOps Server、または

コンポーネント	説明
グサーバ	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462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およびIDEプラグイン	Audit WorkbenchおよびFortify IDEプラグインは、代替のソースコード監査ツールとして使用できます。
Jenkins Azure DevOps Bamboo	これらのプラグインを使用して、ソースコードをスキャンし(Fortify Static Code Analyzerを使用して)、スキャン結果をアップロードします。
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	(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 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、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、『*Fortifyソフトウェアシステム要件*』ドキュメントを参照してください。

ドキュメント『Fortifyソフトウェアシステム要件』にある指示に従ってインストールファイルと`fortify.license`ファイルをダウンロードします。役に立つハウツー動画(https://www.youtube.com/playlist?list=PL8yfmcqTN8GE9XCGVgxMQDFFZy9_-R-e3)でも、Fortifyソフトウェアをダウンロードする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-2024_Q2_<build>.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-2024_Q2_<build>.zip`	データベーステーブルのシードに使用されるシードバンドルをレポートします。デフォルトのFortify Software Security Centerレポートセットが提供されます。
`Fortify_PCI_Basic_Seed_Bundle-2024_Q2_<build>.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-2024_Q2_<build>.zip`)を使用してください。
`Fortify_PCI_SSF_Basic_Seed_Bundle-2024_Q2_<build>.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-2024_Q2_<build>.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、ドキュメント『Fortifyソフトウェアシステム要件』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『OpenText™ Fortifyソフトウェアシステム要件』を参照してください。

KubernetesおよびHelmのスペースでは、次のものが必要です。

- 永続ボリューム: 設定ファイルおよびログファイル用。Kubernetes永続ボリュームは、PodSecurityContext `fsGroup`フィールドをサポートしている必要があります。Fortify Software Security CenterのHelmチャートの展開では、「user」Helmチャート値(「user.uid」、「user.gid」)を使用したデフォルトのUIDおよびGIDの変更がサポートされています。`fsGroup`がサポートされている場合、Fortify Software Security Centerの機能に影響を与えることなく、UIDとGIDの両方を変更できます。

  Fortify Software Security Centerが`fsGroup`サポートのない永続ボリュームを持つKubernetesで実行される場合、またはFortify Software Security Centerコンテナイメージが Kubernetesの外部で使用される場合、Fortify Software Security Centerは、デフォルト以外のGIDで実行すると開始できません。この場合は、Fortify Software Security Centerボリュームのディレクトリとファイルに対するパーミッションを手動で設定してから開始する必要があります。
- シークレットファイル - ユーザ名やパスワードなど、ライセンスやデータベースへの接続に関するあらゆる情報が保存されます。KubernetesではFortify Software Security CenterがHTTPS上でのみ動作するため、これはSSLまたはHTTPSに関して重要です。そのため、TLSまたはSSL接続が必要です。この情報(トラスト、キーストア、ライセンスファイル)はすべてシークレットファイルに保存されます。ライセンスとキーストアを用意しておく必要があります。

- `ssc-values.yaml`ファイル - Helmチャートのためのすべてのパラメータを保存または設定するために使用します。Helmチャートには、SSCを設定するためのデータが必要です。

結果をSSCに保存する必要があり、そのためにはSSCデータベースを使用します。また、Kubernetesスペース内のデータベースのバージョンは、ssc dbに使用されるバージョンと同じである必要があります。

ユーザにsscへのアクセス権を付与する必要もあります。それには、Kubernetesのコンポーネントである何らかのサービス(ロードバランサ、クラスタIP、またはノードポート)が必要です。

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。アップグレード手順については、https://helm.sh/docs/helm/helm_upgrade/#helm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ファイルから*<ssc_helm_dir>*ディレクトリにHelmディレクトリの内容をコピーします。*<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。エアギャップされた環境でアプリケーションを展開する必要がある場合は、プライベートレジストリを展開に使用し、そこにFortify Software Security Centerコンテナ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、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Fortify Software Security Centerコンテナイメージを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、アカウント名をカスタマサポート(https://www.microfocus.com/support)に伝えます。

   注: 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クライアントが配置されていると見なされます。)次のようにして、Fortify Software Security Centerコンテナイメージをプライベートレジストリに転送します。
   a. `docker login`を使用してDocker Hubにログインします。
   b. `docker login <priv_reg_host_and_port>`を使用してプライベートレジストリにログインします。*<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. 次のように、Fortify Software Security Centerコンテナイメージを転送します。
      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>に使用する値を決定するには、*<ssc_helm_dir>*ディレクトリに移動して、`ssc-<chart_version>+<ssc_version>.tgz`ファイルを開きます。TGZファイル名の*<ssc_version>*値(最新の公開イメージビルドのタグ)を使用します。

      また、正確なイメージビルドのタグも *<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チャートの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>*)の値を変更してはなりません。

   d. *<ssc_helm_dir>*`/ssc-values.yaml`ファイルで`image.repositoryPrefix`パラメータの値として「*<priv_reg_host_and_port>*/*<priv_reg_path>*/」を入力します。(`image.repositoryPrefix` パラメータに指定する値は、末尾にスラッシュ(/)を含める必要があります。
4. 正確なイメージビルドタグを使用する場合は、`image.buildNumber`の値として*<imageBuildNumber>*値を入力します。それ以外の場合は、空のままにします。
5. レジストリ(Docker Hubまたはプライベートレジストリ)からイメージを取得するためのKubernetesシークレットをプロビジョニングします。手順については、`https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry`を参照し、*<ssc_helm_dir>*`/ssc-values.yaml`ファイルで `imagePullSecrets` パラメータの値としてシークレット名を入力します。シークレットが`regcred`である場合のフォーマットは次のとおりです。

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

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。

6. 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。受諾されたデータのリストをsecretRef.keysファイルで調べます。最小限必要のセットには、httpCertificateKeystoreFileEntry、httpCertificateKeystorePasswordEntry、およびhttpCertificateKeyPasswordEntryが含まれます。

   次の例は、シークレットを手動で作成する方法を示すものです。

   a. *<ssc_secrets_dir>*ディレクトリを作成します。
   b. secretRef.keysの必須項目ごとにファイルを作成します。ディレクトリには少なくとも3つのファイルが必要です。HTTPS証明書とその秘密鍵を含むJavaキーストアファイル、キーストアのパスワードを含むファイル、およびHTTPS証明書の秘密鍵のパスワードを含むファイルです。
   c. 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>"
      ```

   d. *<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。
   e. *<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 Pod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。

7. 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によって参照されるFortify Software Security Centerシークレットに変更を適用するには、ssc-webapp Podを手動で削除する必要があります(これは後ほど自動的に再作成されます)。

   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ほとんどの値を後で変更してから、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70を参照してください。

Apache Tomcatアクセスログのカスタマイズ

ssc-webappコンテナイメージでTomcatアクセスログのデフォルトフォーマットを変更するには、`HTTP_SERVER_ACCESS_LOG_PATTERN`環境変数をTomcat Access Log Valveのパターンに設定します。サポートされているパターンの詳細については、Apache Tomcat 9 Configuration ReferenceのWebサイト(`https://tomcat.apache.org/tomcat-9.0-doc/config/valve.html#Access_Log_Valve`)を参照してください。

次の例に示すように、環境Helmチャート値を使用できます。

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

KubernetesクラスタへのFortify Software Security Center展開のトラブルシューティング

このセクションでは、展開を試みているときに発生する可能性があるエラーメッセージについて説明します。

インストール段階でクラッシュした場合は、以下を実行します。

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

インストール後にログを表示するには、以下を実行します。

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

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

```
kubectl get pods
```

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

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

```
kubectl get services
```

それらの名前を一覧にするには、以下を実行します。

```
helm list
```

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

```
helm get values <installation name>
```

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

```
 kubectl describe --help
```

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

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

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

その他のトラブルシューティング資料

展開のトラブルシューティングに関する視覚的なガイドについては、『A visual guide on troubleshooting Kubernetes deployments』(https://learnk8s.io/troubleshooting-deployments)を参照してください。コンテナ化されたアプリケーションの一般的な問題の

デバッグについては、『アプリケーションのトラブルシューティング』
(https://kubernetes.io/docs/tasks/debug/debug-application)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。

デフォルトディレクトリ位置

Fortify Software Security Centerの展開後、*<fortify.home>*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

デフォルトの場所を変更する

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

例: -Dfortify.home=/home/fortify

注: Fortify Software Security Centerを設定("Fortify Software Security Centerの初回設定" ページ70を参照)した後に、<fortify.home>ディレクトリの場所を変更する場合は、更新後のfortify.homeシステムプロパティ値を使用してサーバを再起動する前に、既存の<fortify.home>ディレクトリの内容を新しい場所にコピーするか、移動してください。

ディレクトリの内容

*<fortify.home>*ディレクトリは次のように構成されています。

```
<fortify.home>/<app_
context
>/
conf/
app.properties
datasource.propertieslog4j2.xmlversion.propertiessecret.keylogs/ssc.log...init.token

                ...

plugin-framework/

/logs

fortify.license
```

ここで

<app_context>	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。詳細については、"Fortify Software Security Centerの設定の自動化" ページ474を参照してください。
log4j2.xml	デフォルトのログ設定です。この設定は手動で変更できますが、代わりにlog4j2設定上書き機能を使用することを強く推奨します("Fortify Software Security Centerログ記録のカスタマイズ" ページ170を参照してください)。
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	お客様が設定できるアプリケーションプロパティが含まれているファイルです。
datasource.properties	データベース接続プロパティが含まれているファイルです。
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 (このファイルがFortify Software Security Centerによって上書きされることはありません。ただし、このファイルが*<fortify.home>/<app_context>*/confディレクトリにない場合は生成されます)。 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。 **注:** プラグインで問題が発生した場合は、通常、メインのFortify Software Security Centerログよりも詳しい情報をplugin-framework/logsで参照できます。
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63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70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 59
Fortify Software Security Centerデータベース文字セットのサポートについて 60
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 60
ディスクI/Oの監視 60
データベースユーザアカウント権限 60
データベース固有の設定要件 61
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 67
Fortify Software Security Centerデータベースのシード処理について 67
Fortify Software Security Centerデータベースの永久削除 68

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

ディスクI/Oの監視

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

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

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

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 8.0オプションファイルを設定するには:

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

   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
`default_storage_engine`	INNODB
`innodb_buffer_`	`512M` (`10GB`以上を推奨)

設定	値
pool_size	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、10 GB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。
innodb_lock_wait_timeout	300 (推奨)。秒で表す。
innodb_	512M

設定	値
log_file_size	
max_allowed_packet	1G
sql-mode	"TRADITIONAL"

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 [SSUECACHE] 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70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47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-2024_Q2_<*build*>.zip)では、デフォルトの管理者ユーザアカウントと問題テンプレートデータを提供します。

- レポートシードバンドル(Fortify_Report_Seed_Bundle-2024_Q2_<build>.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-2024_Q2_<build>.zipおよびFortify_PCI_SSF_Basic_Seed_Bundle-2024_Q2_<build>.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)。

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

データベースのシード処理が終了したら、シードプロセスで作成されたユーザ設定可能なデータエンティティを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80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208

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188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。

   配布されたWARファイルを使用し、`ssc.war`ファイルの名前を変更せずに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、 **管理者(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56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。
6. Fortify Software Security Centerセットアップウィザードの **[スタート(START)]**ページの情報を読み、 **[次へ(NEXT)]**をクリックします。
7. **[設定(CONFIGURATION)]**ステップの **[FORTIFYライセンスのアップロード(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。このディレクトリの場所を変更する方法については、"<fortify.home>ディレクトリについて" ページ56を参照してください。
9. **[この警告を読んで理解しました(I have read and understood this warning)]** チェックボックスをオンにして、 **[次へ(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. 左ペインの **[FORTIFY SOFTWARE SECURITY CENTER URL]** に、Fortify Software Security CenterサーバのURLを入力します。
    b. 中央ペインで、 **[HTTPホストヘッダ検証を有効にする(Enable HTTP host header validation)]** チェックボックスをオンにして、HTTP Hostヘッダ値が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. **[データソース(DATASOURCE)]** ステップで、次の操作を実行します。
    a. **[データベースタイプ(DATABASE TYPE)]** リストから、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. **[データベースユーザ名(DATABASE USERNAME)]** 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. **[データベースパスワード(DATABASE PASSWORD)]** 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: **データベースユーザ名(DATABASE USERNAME)**]フィールドと **データベースパスワード(DATABASE PASSWORD)**]フィールドで指定したデータベースユーザ資格情報が、マイグレーションスクリプトの実行に必要な権限を持つユーザアカウント用に設定されていることを確認します。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**]にFortify Software Security CenterのURLを入力するときは、次の点に注意が必要です。

MySQLデータベースの場合 -

- MySQLサーバが`sha256_password`または`caching_sha2_password`認証プラグインを使用するように設定されている場合は、serverRsaPublicKeyFileオプションでJDBCドライバにサーバRSA公開鍵を提供する必要があります。あるいは、セキュリティ保護の弱いallowPublicKeyRetrievalオプションを使用することもできます。詳細については、MariaDB Connector/JおよびMySQLサーバの文書(`https://mariadb.com/kb/en/mariadb-connector-j`および`https://dev.mysql.com/doc`)を参照してください。
- MySQLサーバデータベースを使用している場合は、URLの末尾に次のもの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

Examples:

```
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。

MSSQLサーバデータベースの場合 -

- 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
```

- **注意** Fortify Software Security Centerには、暗号化された接続と信頼されるサーバ証明書をデフォルトで必要とするMSSQL JDBCドライバのバージョンが同梱されています。証明書の検証の結果として接続が失敗

する場合は、Truststoreを設けることをお勧めします。Truststoreを設けることができない場合は、信頼の検証を無効にすることができます。証明書は信頼されているが、証明書のDNS名がデータベースサーバのホスト名と一致しないという場合は、`hostNameInCertificate`接続プロパティを使用して正しいホスト名を指定します。

詳細については、https://learn.microsoft.com/ja-jp/sql/connect/jdbc/setting-the-connection-propertiesにある「接続プロパティの設定」という記事の`hostNameInCertificate`、`trustServerCertificate`、および `trustStore* JDBC URL`プロパティを参照してください。

e. **[最大アイドル接続数(MAXIMUM IDLE CONNECTIONS)]**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. **[最大アクティブ接続数(MAXIMUM ACTIVE CONNECTIONS)]**に、プールに残すことのできるアクティブな接続の最大数を入力します。デフォルト値は100です。

g. **[最大待機時間(ミリ秒) (MAXIMUM WAIT TIME (MS))]**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. **[データベースのシード(DATABASE SEEDING)]**ステップに進む前に、**[**をクリックして`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67を参照してください。

注: Fortify Software Security Centerの設定を自動化する場合に、`<app_context>.autoconfig`ファイル内でデータベースのマイグレーションを有効にしてある場合は、`create-tables.sql`スクリプトを実行する必要がありません。Fortify Software Security Center設定を自動化する方法については、"Fortify Software Security Centerの設定の自動化" ページ474を参照してください。

14. データベースを初期化した後には、**[次へ(NEXT)]**をクリックします。

15. (Linuxのみ)Linuxシステムでは、fontconfigライブラリ、DejaVu sansフォント、およびDejaVu serifフォントがサーバにインストールされていることを確認します。

16. **[データベースのシード(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-2024_Q2_<build>.zip`ファイルを見つけて選択し、**[SEED DATABASE]**をクリックします。
    b. **[参照(BROWSE)]**を使用して`Fortify_Report_Seed_Bundle-2024_Q2_<build>.zip`ファイルを見つけて選択し、**[SEEDデータベース(SEED DATABASE)]**をクリックします。
    c. (オプション) **[参照(BROWSE)]**を使用して`Fortify_PCI_SSF_Basic_Seed_Bundle-2024_Q2_<build>.zip`ファイルを見つけて選択し、**[SEEDデータベース(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47を参照してください。

    d. (オプション) **[BROWSE]**を使用して`Fortify_PCI_Basic_Seed_Bundle-2024_Q2_<build>.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47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 [管理(Administration)]ビューから行います。([管理(Administration)]ビューの詳細については、"追加のFortify Software Security Center設定" ページ80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188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201

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182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

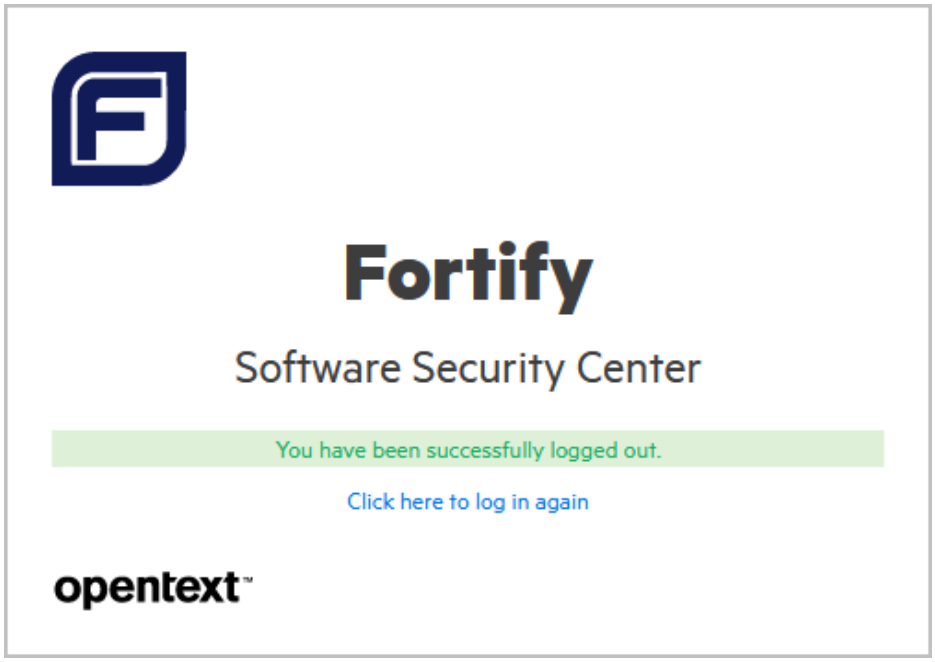
"セッションログアウトについて" 次のページ

"追加のFortify Software Security Center設定" ページ80

"Fortify Software Security Centerのログインに必要なパスワード強度の設定" ページ171

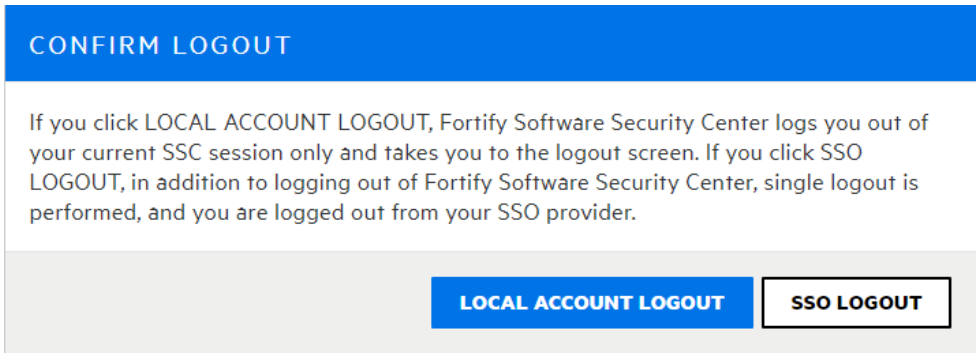
セッションログアウトについて

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では、Central AuthenticationサービスおよびSAMLのシングルログアウトをサポートしています。



[ローカルアカウントログアウト(LOCAL ACCOUNT LOGOUT)]をクリックすると、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。

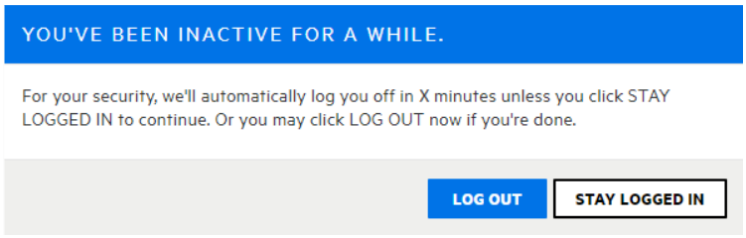
[SSO LOGOUT]をクリックすると、Fortify Software Security Centerからログアウトするほかに、シングルログアウトが実行され、SSOプロバイダからログアウトされます。

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

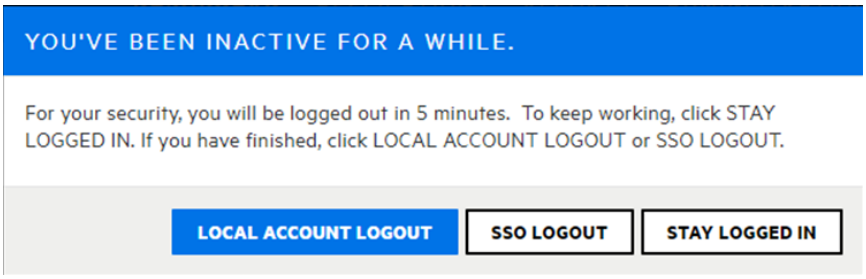
非アクティブによって、Fortify Software Security Centerセッションがタイムアウトに近付くと、Fortify Software Security Centerは次の2つのダイアログボックスのいずれかを表示します。

- 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96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ファイルをデプロイしたら、Fortify Software Security Centerの [管理(Administration)]ビューから設定を完了します。

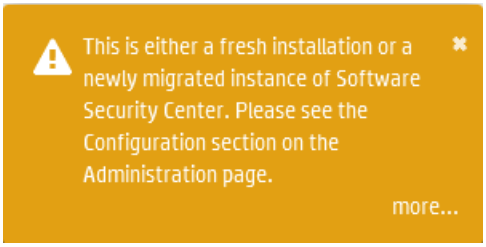
後から必要に応じて、 [管理(Administration)]ビューで他の設定を設定および更新できます。

[管理(Administration)]ビューでの環境設定へのアクセス

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

[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76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。 **[移動(Go)]**をクリックして、 [管理(Administration)]ビューの **[設定(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. OpenTextのヘッダで、 **[管理(Administration)]**をクリックします。
        左側のナビゲーションペインに、 [管理(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、 [イベントログ(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、" [管理(Administration)]ビューで使用可能な環境設定オプション" ページ82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。

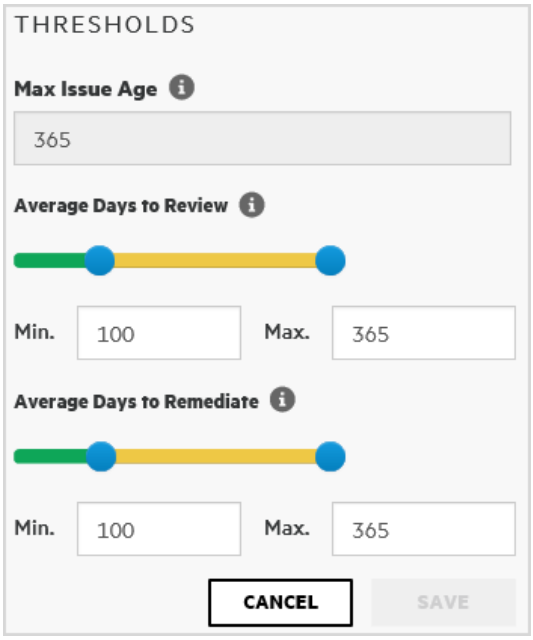
これらのルールのすべてが適用され、時間と日付の調整が行われます。その後、Fortify Software Security Centerは(auditTime - foundDate)と(removedDate - foundDate)の2つの値の平均値を計算して、監査して問題を修復する平均日数を取得します。

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. OpenTextのヘッダで、 管理(Administration)]を選択します。
2. 左ペインの メトリックとトラッキング(Metrics & Tracking)]で、 問題の古さ(Issue Age)]を選択します。
   [ssue 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。

[ssue 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。

管理(Administration)]ビューで使用可能な環境設定オプション

次の表は、 管理(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。(OpenTextのヘッダで、 管理(Administration)]を選択します。次に、左

側のペインで、 **設定(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85
Audit Assistant	Fortify Static Code Analyzerのスキャンを自動的に監査するために使用します。	"Audit Assistantの設定" ページ385
BIRTレポート	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96
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104
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105
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。	"LDAPサーバの設定" ページ111

オプション	説明	手順
保守	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。サーバのシャットダウンの準備として、ここからジョブの実行を一時停止することもできます。	"Fortify Software Security Centerの保守モードへの移行" ページ188
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統合のプロキシの設定" ページ132
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135
SCIM	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ために使用します。	"SCIMによる外部管理されたユーザおよびグループのプロビジョニングの有効化" ページ132
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148
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	"Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設定" ページ134

オプション	説明	手順
	たりするようにFortify Software Security Centerを設定するために使用します。	
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135
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146
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をデータベースにシードするために使用します。	"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208
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162
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308

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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで **設定(Configuration)**]を選択し、 **アプリケーションセキュリティトレーニング(AppSec Training)**]を選択します。
3. 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、対応するトレーニングURLを取得するには、カスタマサポート(https://www.microfocus.com/support)にお問い合わせください。
5. [トレーニングURL(Training URL)]ボックスに、アプリケーションセキュリティトレーニングURLを入力します。
6. [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

"スキャン結果の監査" ページ358

監査アシスタントについて

Audit Assistantは、スキャンから返された問題が真の脆弱性であるかどうかを判断するのに役立つオプションのツールです。Audit Assistantがその判断を下すには、予測のベースラインを確立するためのデータが必要です。このデータは、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、Fortify on Demand監査官が行った決定に基づいています。このデータは、プールされて匿名化され、監査官が行った決定に基づいてトレーニングデータと組み合わせて使用できます。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。

次のセクションでは、認証トークンをOpenText Fortify Audit Assistantから取得し、そのトークンを使用してOpenText Fortify Software Security Centerへの接続を設定する方法について説明します。このセクションでは、新しいG2エンジンを搭載した最新バージョンのOpenText Fortify Audit Assistantにアップグレードする際の、Fortify Audit Assistantのベストプラクティスについても説明します。詳細については、「"Fortify Audit Assistantのベストプラクティス" ページ379」を参照してください。

以降のセクションでは、Audit Assistantのトレーニングの設定方法、データの送信方法、およびAudit Assistantの結果の確認方法について説明します。

参照情報

"Audit Assistantの設定" ページ385

"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391

"Audit Assistantの使用" ページ384

"予測ポリシーについて" ページ381

"予測ポリシーの定義" ページ382

"Audit Assistantへのトレーニングデータの送信" ページ399

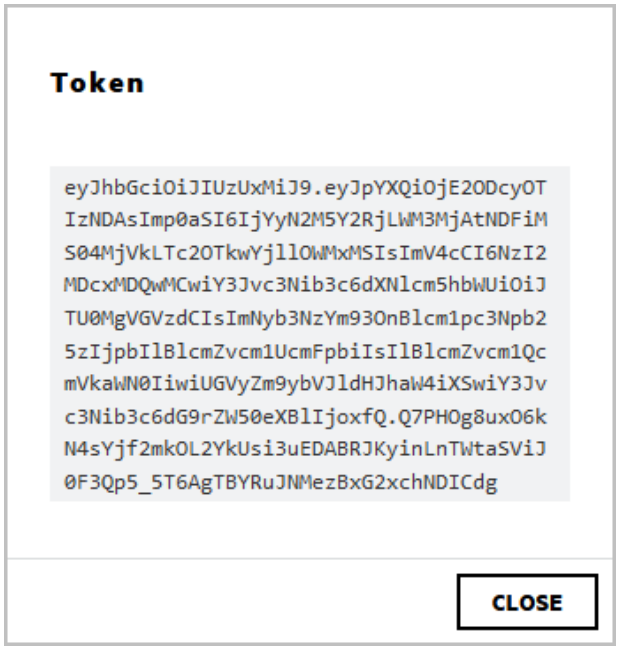
"Audit Assistantの結果の確認" ページ396

Fortify Audit Assistant認証トークンの取得

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

Fortify Audit Assistant認証トークンを取得するには:

1. Fortify Audit Assistantにログオンします。
2. OpenTextのヘッダで、 **管理(ADMINISTRATION)**]をクリックし、 **トークン(TOKENS)**]を選択します。
3. トークン(Tokens)]ページで、 **追加(+ADD)**]をクリックします。
4. **名前(Name)**]フィールドに、生成するトークンの名前を入力します。
5. **保存(SAVE)**]をクリックします。
   トークン(Tokens)]ページに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。



7. トークン(Tokens)]ウィンドウで、トークンテキストを選択してコピーし、 **閉じる(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" ページ385を参照してください)。

Audit Assistantの設定

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

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

1. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(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
Audit Assistantを有効にする(Enable Audit Assistant)]チェックボックス	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 Audit Assistantから取得した認証トークンをここに貼り付けます。トークンの取得手順については、 **トークンの取得方法(How do I get a token?)**]を選択します。または、"Fortify Audit Assistant認証トークンの取得" ページ389を参照してください。
* Fortify Audit AssistantサーバURL	Fortify Audit AssistantサーバのURLを指定します。
Audit Assistantにプロキシを使用(Use SSC proxy for Audit Assistant)	すべてのFortify Software Security Center統合にプロキシを設定してある場合("Fortify Software Security Center統合のプロキシの設定" ページ132を参照)、このチェックボックスを選択すると、Fortify Audit Assistantに対してそのプロキシを使用できます。

4. Fortify Audit Assistantサーバへの接続をテストするには、 **接続のテスト(TEST CONNECTION)**]をクリックします。
   接続が正常にテストされたら、先に進んで、 **監査設定(Audit settings)**]セクションで次の設定をします。
5. **ポリシーの更新(REFRESH POLICIES)**]をクリックして、 **デフォルトの予測ポリシー(Default prediction policy)**]リストに、Fortify Audit Assistantサーバ上の現在のサーバポリシーを入力します。

   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 Audit Assistant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 **ポリシーの更新(REFRESH POLICIES)**]をクリックするたびに、Fortify Audit Assistantから受け取る新しい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。

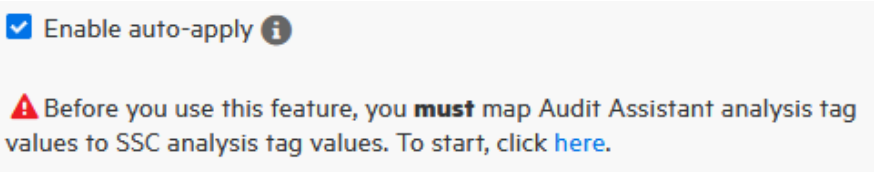
6. **Default prediction policy**]リストから、すべてのアプリケーションバージョンに適用する予測ポリシーの名前を選択します。(ポリシーはFortify Audit Assistantで定義されます)。
7. 予測ポリシーをアプリケーションバージョンレベルで指定し、デフォルトのグローバル予測ポリシーを上書きする場合は、 **特定のアプリケーションバージョンのポリシーを有効にする(Enable specific application version policies)**]を選択します。それ以外の場合、Fortify Audit Assistantは前のステップで指定したデフォルトのグローバル予測ポリシーを使用します。

注: アプリケーションバージョンのポリシーは、 [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスから指定できます。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389を参照してください。

8. 未監査の問題をFortify Software Security Centerで自動的にFortify Audit Assistantに送信して評価が行われるようにするには、 **自動予測を有効にする(Enable auto-prediction)**]チェックボックスをオンにします。その後、 [アプリケーションプロファイル(APPLICATION PROFILE)]ウィンドウから、アプリケーションバージョンごとにこの機能を有効にする必要があります。(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の [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスを開き、そこでも自動予測を有効にします。

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、 **自動適用を有効にする(Enable auto-apply)**]チェックボックスをオンにします。その後、 [アプリケーションプロファイル(APPLICATION PROFILE)]ウィンドウから、アプリケーションバージョン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の [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスを開き、そこでも自動適用を有効にします。

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. **自動適用を有効にする(Enable auto-apply)**]チェックボックスがオンにしてあり、Audit Assistant分析タグの値をFortify Software Security Center Analysisタグ値にすぐにマップしたい場合は、**こちら(here)**]リンクをクリックして**カスタムタグ(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" ページ392に記載されている手順に従います。
11. **保存(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

自動予測を[はい(yes)]に設定すると、FPRが正常にアップロードおよび処理された後に、Fortify Audit Assistantの予測に関する問題を自動送信するように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、Fortify Audit Assistantは新しい問題のカスタムタグに予測値を自動的に適用します。(監査アシスタントの予測結果は常にアプリケーションバージョンに適用されますが、自動適用が有効になっていない場合、情報は監査アシスタント固有のタグにのみ保存されます。自動適用が有効な場合、監査アシスタント固有の値も設定に基づいて他のタグにマップされます)。

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

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Fortify Audit Assistantの設定時にシステム全体に対して自動予測を有効にします。("Audit Assistantの設定" ページ385)。その後、ユーザは**プロファイル(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する必要があります。("アプリケーションバージョンの自動適用と自動予測を有効にする" ページ391」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

Fortify Audit AssistantをFortify Software Security Centerと一緒に使用するには、Fortify Audit Assistant分析タグ値をリストタイプのFortify Software Security Centerカスタムタグ値にマップする必要があります。Fortify Audit Assistant分析タグ値は、Fortify Software Security Centerと一緒にインストールされ、脆弱性を監査済みとして識別するために必要な**分析(Analysis)**]カスタムタグにマップすることもできますが、その目的のために別のリストタイプのカスタムタグを選択することもできます。

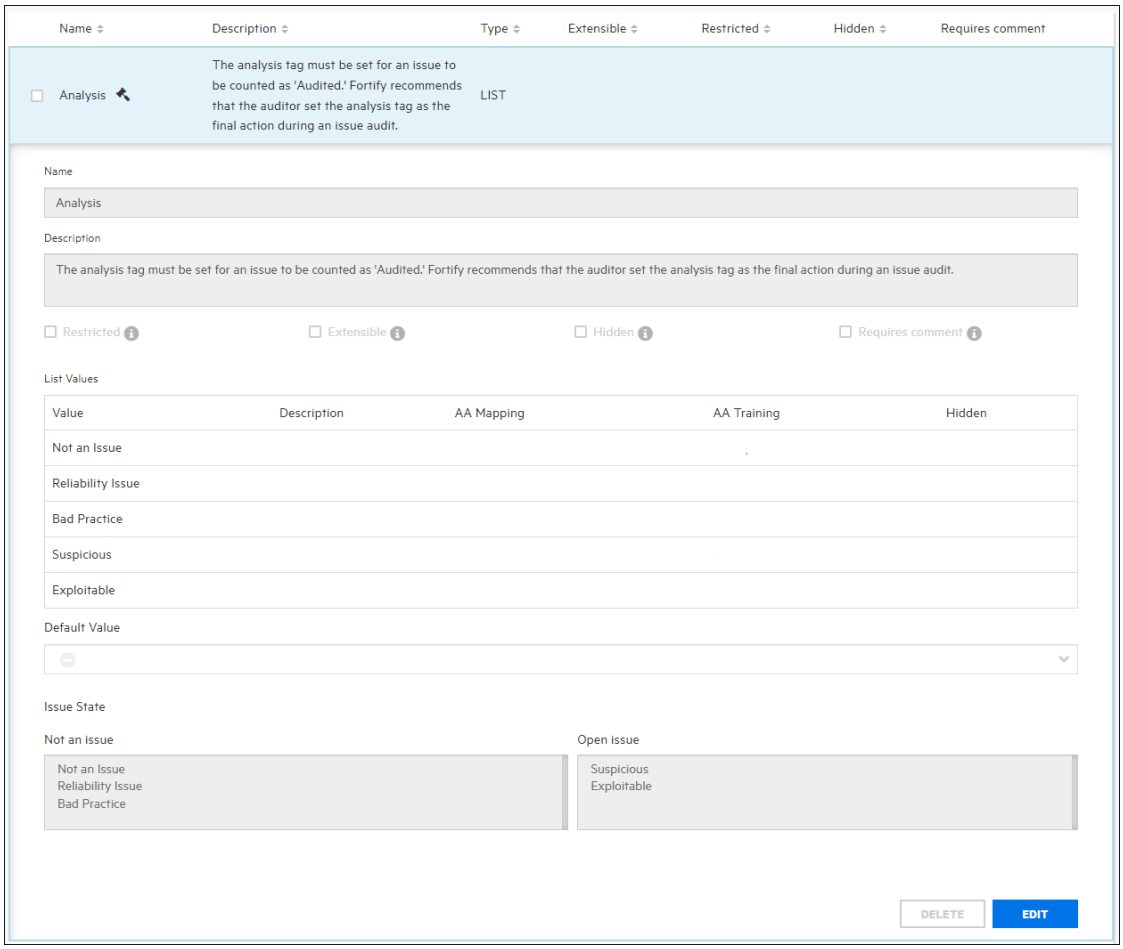
Fortify Audit Assistantの設定時に**自動適用を有効にする(Enable auto-apply)**]チェックボックスをオンにした場合、どのFortify Audit Assistant分析タグ値をリストタイプの

カスタムタグ値に自動的に適用するのかを、AAに通知することもできます。

メモ: カスタムタグ値をまだ作成していない場合は、値を作成してFortify Audit Assistantにマップする方法について、"カスタムタグ値の追加" ページ287を参照してしてください。デフォルトの [分析(Analysis)] カスタムタグか自分で作成したカスタムタグを使用している場合は、このセクションの手順に従います。

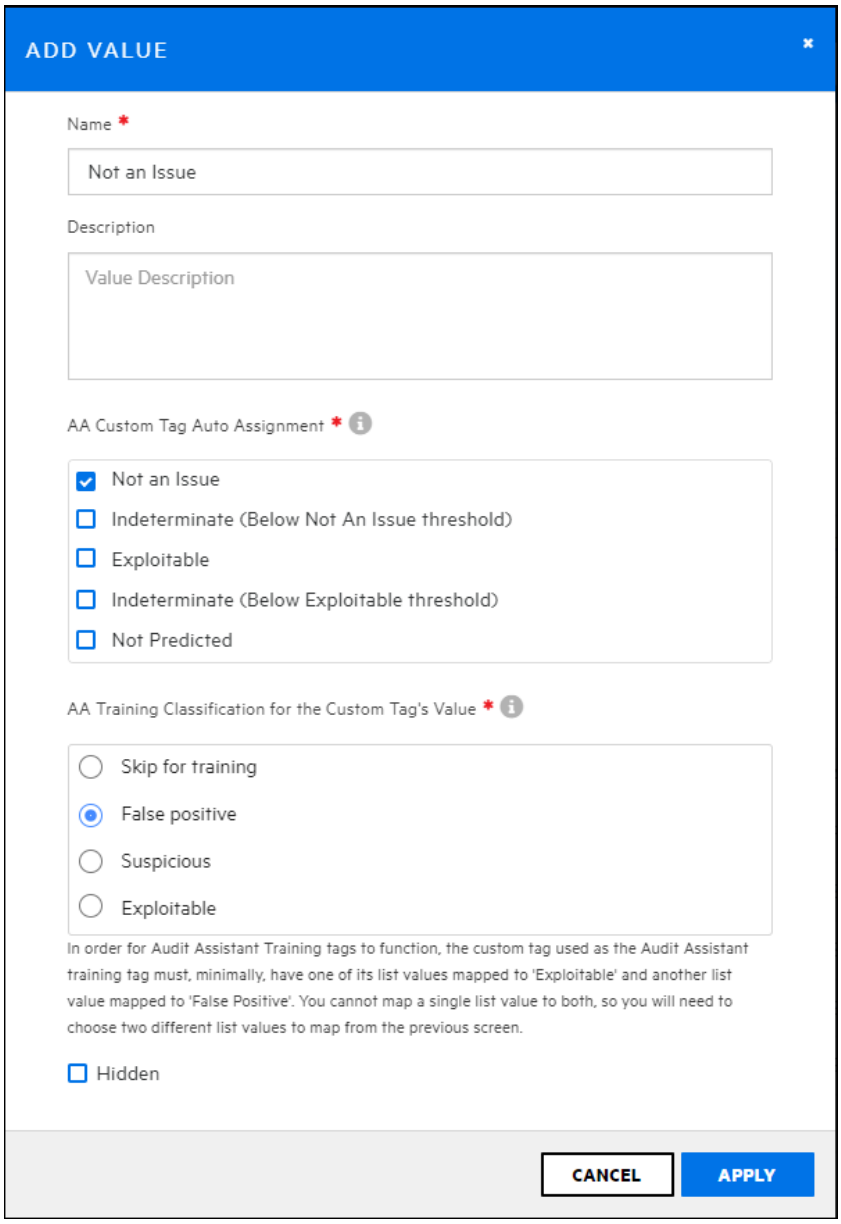
Fortify Audit Assistant分析タグ値をリストタイプのFortify Software Security Centerカスタムタグ値にマップするには:

1. OpenTextのメニューバーで、 **[管理(Administration)]** をクリックします。
2. 左ペインで、 **[テンプレート(Templates)]** をクリックし、 **[カスタムタグ(Custom Tags)]** をクリックします。
   [カスタムタグ(Custom Tags)] ページにカスタムタグが一覧表示されます。
3. 値を編集するタグの行をクリックします。
   行が展開されて、タグの詳細が表示されます。



4. 画面の右下隅で、 **[編集(EDIT)]** をクリックします。
   行の最後に、テーブル内の値の [編集(EDIT)] アイコン(✎)が表示されます。
5. 値の [編集(EDIT)] アイコン(✎)をクリックします。

[値の追加(ADD VALUE)]ダイアログボックスが表示されます。



6. Fortify Audit Assistantを使用するようにFortify Software Security Centerが設定され、自動適用が有効になっている場合、 [値の追加(ADD VALUE)]ダイアログには [AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)]セクションと、 [カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)]セクションが表示されます。
7. 新しい値が [AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)]セクションのAudit Assistantの予測値と一致する場合は、そのチェックボックスをオンにすると、選択したAudit Assistantの予測値にそのリスト値が自動的にマップされます。これにより、アプリケーションバージョンの **[プロファイル]**の **[Audit Assistantオプション(Audit Assistant Options)]**セクションで **自動適用を有効にする(Enable**

auto-apply)]を選択しているすべてのアプリケーションバージョンに対して、自動監査が有効になります。

8. Fortify Audit Assistantモデルのトレーニング時に新しい値を使用する場合は、[カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)]セクションでラジオボタンを選択します。Fortify Audit Assistantトレーニングタグが機能するには、少なくとも2つのリスト値をAudit Assistantトレーニングタグにマップする必要があります。1つは[誤検出(False Positive)]Fortify Audit Assistantトレーニングタグにマップされ、もう1つのリスト値は[悪用可能(Exploitable)]Fortify Audit Assistantトレーニングタグにマップされる必要があります。
9. 追加のリスト値をマップするには、ステップ6 ~ 9を繰り返します。
10. Fortify Audit Assistantトレーニングタグにマップする必要があるすべてのリスト値を編集し終えたら、[**適用(APPLY)**]をクリックして、[**保存(SAVE)**]をクリックします。

参照情報

"Audit Assistantの設定" ページ385

"カスタムタグ値の追加" ページ287

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. OpenTextのヘッダで、[**管理(Administration)**]をクリックします。
3. 左ペインで[**設定(Configuration)**]を選択し、[**BIRTレポート(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、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		
attr	issuecache	reportexecblob
auditattachment	measurement	reportexecparam
auditcomment	measurementhistory	ruledescription
catpackexternalcategory	metadef	savedreport
catpackexternallist	metadef_t	scan
catpacklookup	metaoption	scan_rulepack
datablob	metaoption_t	seedhistory
documentinfo	metavalue	sourcefile
eventlogentry	metavalueselection	snapshot
f360global	project	userpreference
filterset	projecttemplate	variable
folder	projectversion	variablehistory
foldercountcache	projectversiondependency	
ビュー		

attrlookupview	defaultissueview	ruleview
auditvalueview	metadefview	view_standards
baseissueview	metaoptionview	

3. Fortify Software Security Centerに管理者としてログインします。
4. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
5. 左ペインで **設定(Configuration)**]を選択し、 **BIRTレポート(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" 下

"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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで **設定(Configuration)**]を選択し、 **BIRTレポート(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。
4. **保存(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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
3. 左ペインで **設定(Configuration)**]を選択し、 **BIRTレポート(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(Administration)]ビューの[設定(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99を参照してください。

[管理(Administration)]ビューでFortify Software Security Centerのコア設定を設定するには:

1. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで[管理(Administration)]をクリックします。
2. 左ペインで、[設定(Configuration)]を選択して、[コア(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。
ユーザをロックアウトするまでのログイン試行回数 (Login attempts allowed before a user is locked out)	無効な資格情報を使用するローカルユーザがFortify Software Security Centerによってアカウントをロックされずに Fortify Software Security Centerへのログインを試みることのできる回数。 Fortify Software Security Centerによってロックアウトされたユーザは、[ロックアウト時間(分)(Lockout time (minutes))]ボックスに分単位で指定された期間、新しくログインを試みることができません。(ユーザアカウントのロック解除方法については、"ローカルユーザアカウントのロック解除" ページ235を参照してください。デフォルト値は3です。

フィールド	説明
	注: この設定はLDAPユーザには適用されません。グループポリシーエディタを使用してアカウントのロックアウトのしきい値が設定されていたなら、ログイン試行が連続して失敗した場合に、LDAPユーザアカウントはActive Directoryでロックアウトされることになります。
ロックアウト時間(分)(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。 • **LDAP users first, fallback to local users** 最初にLDAPユーザを検索し、次にローカルユーザを検索します。認証エラーやユーザの混乱を避けるため、LDAPサーバとローカルストレージでユーザ名が重複しないようにしてください。 • **LDAP users exclusive, fallback to local administrator** (SSOの推奨戦略)LDAPユーザのみを検索し、ローカル管理者アクセスを許可します。
Display user first/last names and emails in user fields, along with login names	このチェックボックスをオンにすると、必要に応じ、ログイン名、姓と名、および電子メールアドレスのユーザ情報が表示されます。

フィールド	説明
Maximum events per WebInspect Agent Issue	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。
非アクティブセッションのタイムアウト(分)(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 update URL	Fortify Rulepack更新サイトのURLです。 **重要** [Rulepack更新URL(Rulepack Update URL)]フィールドのデフォルト値は、カスタマサポート担当者から指示されない限り変更しないでください。 デフォルト値は、`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統合のプロキシの設定" ページ132を参照してください。
User	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

フィールド	説明
Administrator's email address (for user account requests)	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235

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統合のプロキシの設定" ページ132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96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102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、OpenTextのヘッダで **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **電子メール(Email)**]を選択します。
3. 電子メール(Email)]ページで、次の表で説明されている電子メールサービス属性設定を設定します。

フィールド	説明
Enable email	このチェックボックスを選択すると、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。
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。

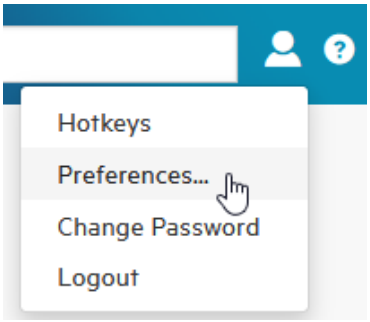
フィールド	説明
SMTP username	SMTPサーバで認証が必要な場合は、SMTPユーザ名を入力します。
SMTP password	SMTPサーバで認証が必要な場合は、SMTPパスワードを入力します。
Secure email server connection	電子メールサーバ接続のセキュリティを設定する場合は、このチェックボックスをオンにします。
Enable SSL/TLS encryption	[Secure email server connection]チェックボックスをオンにした場合、このリストから次のいずれかを選択します。 • (オプション)SMTPサーバがサポートし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

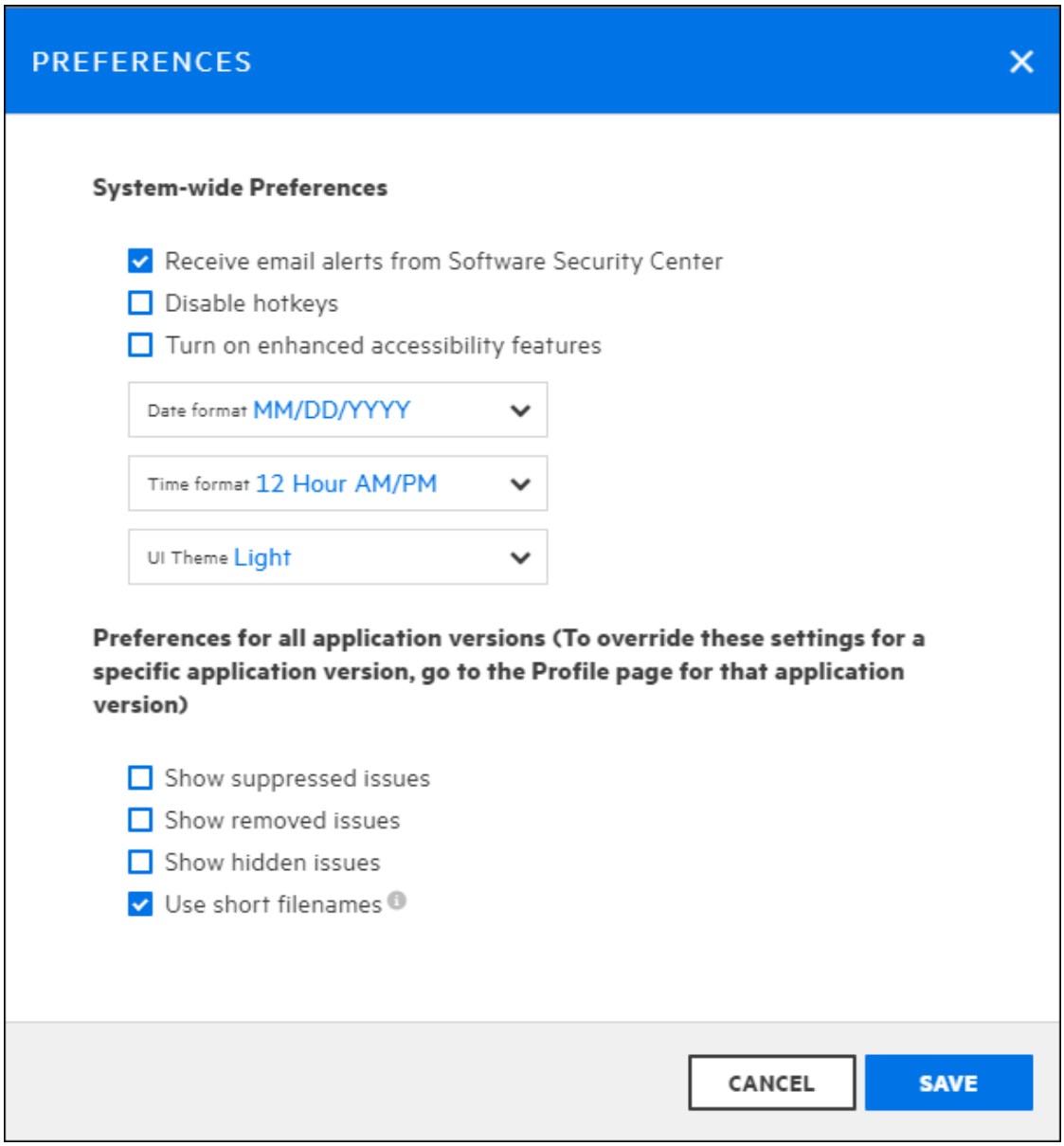
電子メールアラートの受信を有効化および無効化する

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. OpenText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、 **環境設定(Preferences)**]を選択します。



3. [環境設定(PREFERENCES)]ダイアログボックスで、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化するには、 [**Software Security Centerから電子メールアラートを受信する(Receive email alerts from Software Security Center)**]チェックボックスをオフにします。
   - 電子メールアラートの受信を有効にするには、 [**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321

"アラートの作成" ページ322

"アラートの削除" ページ325

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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
3. 左ペインで、 **設定(Configuration)**]を選択してから、 **問題の監査(Issue Audit)**]を選択します。
   [SSUE AUDIT]ページが開きます。
4. **[ssue audit conflict resolving strategy**]リストから、次のいずれかを選択します。
   - **SSCの変更に基づいて競合を解決する(Conflicts are resolved in favor of the SSC changes)]** (デフォルト)
   - **最新の変更に基づいて競合を解決する(Conflicts are resolved in favor of the most recent changes)**
5. **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345

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 管理(Administration)]ビューの 設定(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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **JMS**]を選択します。
3. JMS]ページで、次の表の説明に従って設定を行います。

フィールド	説明
Publish system events to JMS	システムイベントをJMSに発行するには、このチェックボックスをオンにします。
JMS server URL	JMSサーバのURLを入力します。 たとえば、`tcp://123.0.1.2:12345`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。

フィールド	説明
	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。

Kafkaの設定

オプションの設定として、Fortify Software Security Centerと共にKafkaサービスを展開し、Fortify Software Security Centerの問題の監査の変更を、Fortify ScanCentral DASTと同期することができます。

監査履歴の変更をKafkaにストリーミングするためにFortify Software Security Centerを設定するには:

1. OpenTextのヘッダで、 [管理(Administration)]を選択します。
2. 左ペインで、 [設定(Configuration)]を選択してから、 [Kafka Stream]を選択します。
3. [Kafka Stream]ページで、次の表の説明に従って設定を行います。

フィールド	説明
Kafkaへの監査の更新のストリーミングを有効にする(Enable streaming audit updates to Kafka)	このチェックボックスをオンにすると、監査履歴の変更がFortify Software Security CenterからKafkaに同期されます。
Kafkaブートストラップサーバのカンマ区切りリスト(A comma-separated list of Kafka bootstrap servers)	Kafkaインスタンスのブローカをカンマ区切りリストで指定します。 このリストに使用する構文: `<host1>:<port1>,<host2>:<port2>,...`
監査の更新が発行されるKafkaトピック(The Kafka topic to which audit updates are published)	監査イベントを検索するKafkaトピックを指定します。
Kafkaセキュリティ	
Kafkaストリーミングに対してTLS相互認証を有効にする(Enable TLS	このチェックボックスをオンにすると、Kafkaブローカとの通信に対して、双方向SSLプロト

フィールド	説明
mutual auth for Kafka streaming)	コルを使用した相互認証が有効になります。 このチェックボックスをオンにしない場合、Kafkaブローカとの通信のためのセキュリティプロトコルとして、PLAINTEXTが使用されます。 **注:** Fortify Software Security Centerは、TLSv1.2とTLSv1.3を使用する双方向のSSLをサポートしています。
Truststoreファイルの場所 (Truststore file location)	Truststore証明書が入った、`.jks`ファイル形式のTruststoreファイルへのパスを指定します。
Truststoreパスワード(Truststore password)	Truststoreファイルのパスワードを指定します。
キーストアの場所(Keystore location)	クライアントの公開鍵と秘密鍵が入った、`.jks`ファイル形式のキーストアファイルのパスを指定します。
キーストアパスワード(Keystore password)	キーストアファイルのパスワードを指定します。
秘密鍵のパスワード(Private key password)	秘密鍵のパスワードを指定します。
Kafkaサーバのホスト名検証を有効にする(Enable hostname validation of Kafka server)	このチェックボックスをオンにすると、Kafkaサーバの完全修飾ドメイン名(FQDN)またはIPアドレスを、そのKafkaサーバの実際のホスト名またはIPアドレスに照らして検証します。これにより、正しいKafkaサーバに接続していることを確認できます。

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

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127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122および"LDAPユーザ役割の管理について" ページ185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96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111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. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **[LDAPサーバ(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108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. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
2. 左のナビゲーションペインで、 **設定(Configuration)**]を選択してから、 **[LDAPサーバ(LDAP Servers)**]を選択します。
3. **[**ntegration with LDAP servers]ページで、 **[NEW**]をクリックします。
4. 新しいLDAP設定の作成(CREATE NEW LDAP CONFIGURATION)]ダイアログボックスで、次の表に示す属性を設定します。

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エント

フィールド	説明

	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。
	例: 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**)。
SECURITY	
SSL trust check	ドメインコントローラでSSLが有効になっている場合は、このチェックボックスをオンのままにすると、LDAPサーバによって提示された証明書が信頼された認証局によって発行されたことを確認できます。ドメインコントローラがSSL用に設定されていない場合は、このチェックボックスをオフにします。

フィールド	説明
ホスト名検証(Hostname validation)	ドメインコントローラがSSLに対して有効になっている場合は、このチェックボックスをオンのままにすると、LDAPサーバのホスト名が、証明書の発行先のホスト名と一致します。ドメインコントローラがSSL用に設定されていない場合は、このチェックボックスをオフにします。
ユーザのステータスのマッピングを有効にする(Enable user status mapping)	(Microsoft Active Directoryのみ)このチェックボックスを選択すると、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

フィールド	説明
	distinguishedNameです。
USER LOOKUP SCHEMA	
User firstname attribute	ユーザの名を指定するユーザオブジェクト属性を入力します。 デフォルト値はgivenNameです。
User lastname attribute	ユーザの姓を指定するユーザオブジェクト属性を入力します。 デフォルト値はsnです。
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

フィールド	説明
User thumbnail MIME default attribute	サムネイルMIMEのデフォルト属性
ADVANCED INTEGRATION PROPERTIES	
Cache LDAP user data **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。Fortify Software Security Centerによって、LDAPキャッシュが定期的に自動更新されます。	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 [管理(Administration)]ビューから手動で更新できます。手順については、"LDAPエンティティの手動更新" ページ124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。

フィールド	説明
Page size of LDAP search request results	LDAPサーバが検索結果のサイズを特定の数のオブジェクトで制限し、 [**Enable paging in LDAP search queries**] が選択されている場合は、LDAPサーバの制限値以下の値を入力します。デフォルト値は999です。
LDAP referrals processing strategy **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110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

フィールド	説明
	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。

フィールド	説明
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サーバ設定を編集する" 下

"LDAPサーバ設定のインポート" 次のページ

"LDAPユーザ認証" ページ108

"LDAPエンティティの登録" ページ122

"LDAPサーバ設定の削除" 次のページ

"LDAPユーザ役割の管理について" ページ185

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. OpenTextのヘッダで、 [管理(Administration)]をクリックします。
2. 左ペインで、 [設定(Configuration)]を選択してから、 [LDAPサーバ(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111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108

"LDAPユーザ役割の管理について" ページ185

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. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 [**LDAPサーバ(LDAP Servers)**]を選択します。
3. 次のいずれかを実行します。
   - [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108

"LDAPエンティティの登録" 次のページ

"LDAPユーザ役割の管理について" ページ185

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

   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111)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111 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108

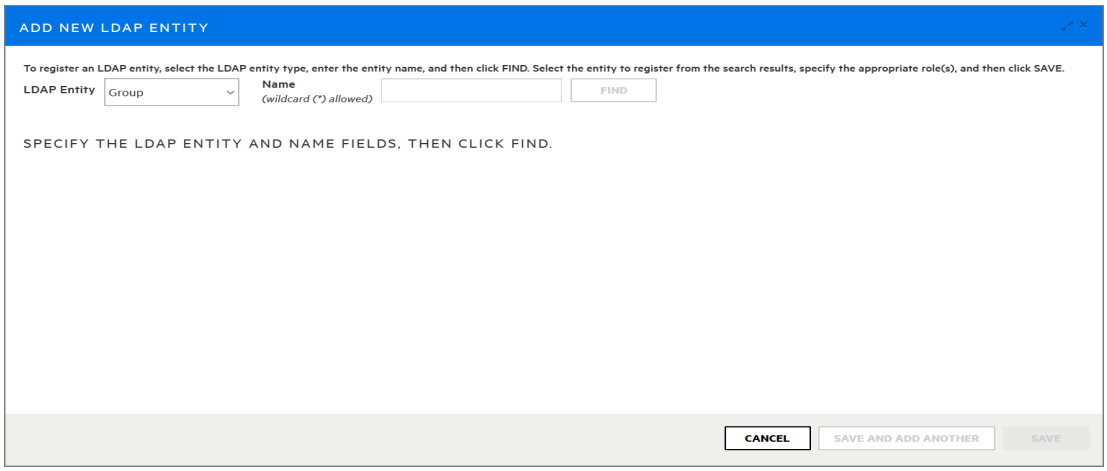
"LDAPユーザ役割の管理について" ページ185

LDAPエンティティの登録

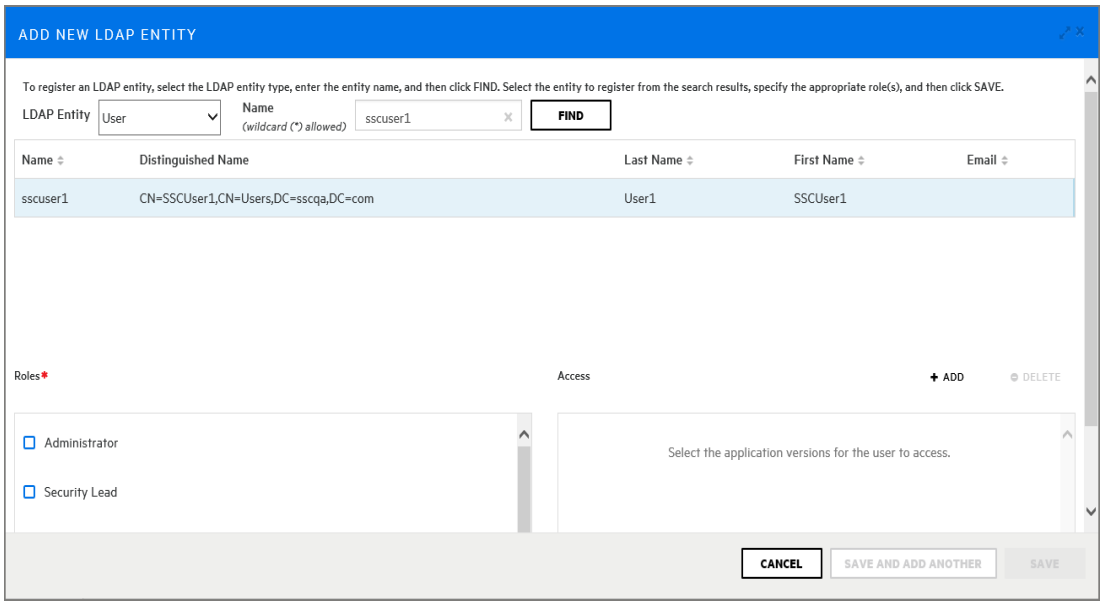
管理者レベルのアカウントを持つユーザは、LDAPグループ、部門、およびユーザをFortify Software Security Centerユーザのリストに追加できます。ユーザがグループに参加またはグループから離れると、Fortify Software Security Centerによってアクセス制御が自動的に更新されます。

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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**]をクリックします。
2. 左ペインで、 **[ユーザ(Users)**]をクリックし、 **[LDAPエンティティ(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。



4. 新しいLDAPエンティティの追加(ADD NEW LDAP ENTITY)]ウィンドウの **[LDAPエンティティ(LDAP Entity)]**リストから、登録するLDAPエンティティのタイプ(**グループ(Group)]**、 **ユーザ(User)]**、または **部門(Organizational Unit)]**)を選択します。
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。
b. [アプリケーションバージョンの選択(SELECT APPLICATION VERSION)]ダイアログボックスの[アプリケーション(Application)]リストで、LDAPエンティティから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。

LDAPサーバの設定方法については、"LDAPサーバの設定" ページ111を参照してください。

参照情報

"LDAPユーザ認証" ページ108

"LDAPユーザ役割の管理について" ページ185

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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで[管理(Administration)]をクリックします。
2. 左ペインで、[ユーザ(Users)]、[LDAPエンティティ(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111を参照してください。

参照情報

"LDAPユーザ認証" ページ108

"LDAPエンティティの登録" ページ122

"LDAPユーザ役割の管理について" ページ185

「無効」にマークされたLDAPエントリの処理

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

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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **ユーザ(Users)**]、 **LDAPエンティティ(LDAP Entities)**]の順に選択します。
3. 変更する必要があるエンティティの行を選択し、 **EDIT**]をクリックします。
4. **UPDATE DISTINGUISHED NAME**]をクリックします (このボタンは、現在のDNが無効な場合にのみ表示されます)。
5. 識別名の更新(UPDATE DISTINGUISHED NAME)]ダイアログボックスの **識別名(Distinguished name)**]フィールドで現在無効な値を選択し、それを更新された識別名に置き換えます。
6. **保存(SAVE)**]をクリックします。

参照情報

"LDAPサーバの設定" ページ111

LDAPキャッシュの永続性の有効化

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

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

サーバのシャットダウン後もLDAPキャッシュを永続させるには:

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

デフォルトのキャッシュ更新間隔の変更

デフォルトのキャッシュ更新間隔は1時間です。大きなLDAPグループがFortify Software Security Centerに登録されている場合、頻繁にキャッシュを更新するとFortify Software Security CenterとLDAPサーバの負荷が増え、パフォーマンスに影響が出る可能性があります。影響を減らすには、次のようにして間隔を長くします。

1. Fortify Software Security Centerをシャットダウンします。
2. *<fortify.home>*/*<app_context>*/confディレクトリに移動し、テキストエディタで app.propertiesファイルを開きます。
3. 次の行を追加します:

   ldap.cache.refresh.interval.hours=*<whole number value between 1 and 12>*
4. Fortify Software Security Centerを再起動します。

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プロトコルを使用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。つまり、ユーザを追加するためにFortify Software Security Centerの [管理(Administration)]ビューを経由する必要はありません。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Microsoft Entra ID統合のみです。

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

- 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(**[管理(Administration)] > [ユーザ(Users)] > [ローカルユーザ(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。 [管理(Administration)]ビューから作成されたユーザは、SCIMプロビジョニングでは読み込み専用です。

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Microsoft Entra IDへの接続の設定" 下

"SAML 2.0準拠の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150

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

System for Cross-domain Identity Management (SCIM)プロトコルを使用して、Microsoft Entra IDのユーザアカウントで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132
Microsoft Entraで、Microsoft Entra IDに移動し、エンタープライズアプリケーションを作成します。	Microsoft Entra IDのドキュメント (https://learn.microsoft.com/en-us/entra) **注:** Entra IDに新しいアプリケーションで実現したい機能を選択するプロンプトが表示されたら、[ギャラリーにはない他のアプリケーションとの統合 (ギャラリー以外) (Integrate any other application you don't find in the gallery (Non-gallery))] オプションを選択します。
Entraから、新しいアプリケーションにユーザとグループを割り当てます。	Microsoft Entra IDのドキュメント (https://learn.microsoft.com/en-

タスク	詳細
	us/entra)
Entraから、アプリケーションをプロビジョニングします。 次の点に注意してください。 • [Provisioning Mode]を[Automatic.]に設定します。 • [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Entra IDのコンプライアンスが向上します。 • [シークレットトークン(Secret Token)]値については、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132を参照してください)。	Microsoft Entra IDのドキュメント (https://learn.microsoft.com/en-us/entra)
Entra IDから、Entra ID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	Microsoft Entra IDのドキュメント (https://learn.microsoft.com/en-us/entra)

タスク	詳細
• externalID [Provisioning Status] のトグルを [On] に切り替える必要があります。	
Entra ID 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、EntraからSAML署名証明書をダウンロードして、SSO SAML設定で使用するキーストア(SAMLキーストアの場所)にインポートする必要があります。 Entraで、作成したエンタープライズアプリケーションに移動します。SAMLベースのサインオンページで署名証明書をダウンロードし、キーストアにインポートします。	• Microsoft Entra IDのドキュメント (https://learn.microsoft.com/en-us/entra) • "SAML 2.0準拠の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150
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を使用するためのFortify Software Security Centerの設定" ページ150
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>
Entraで、保存されたメタデータファイルをアップロードし、アップロードされたメタデータファイルのデータを使用してSAMLシングルサインオンのセットアップを完了します。	Microsoft Entra IDのドキュメント (https://learn.microsoft.com/en-us/entra)
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236

SCIMによる外部管理されたユーザおよびグループのプロビジョニングの有効化

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

1. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで [**管理(Administration)**] をクリックします。
2. 左ペインで、 [**設定(Configuration)**] を選択してから、スクロールして、 [**SCIM**] を選択します。
3. [**SCIMを有効にする(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Entra IDの間の接続を設定する際に、Entra IDでシークレットトークンとして使用します)。

   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を使用するためのFortify Software Security Centerの設定" ページ150

"SCIM 2.0プロトコルの実装" ページ127

"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236

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

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385)、Rulepack更新URL("コア設定の設定" ページ96)、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269)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. OpenTextのヘッダで、 [**管理(Administration)**] を選択します。
2. 左ペインで、 [**設定(Configuration)**] を選択してから、 [**プロキシ(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385

"コア設定の設定" ページ96

"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269

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、『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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**]をクリックします。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **ScanCentral SAST**]を選択します。
3. ScanCentral SAST]ページで、 **ScanCentral SASTを有効にする(Enable ScanCentral SAST)**]チェックボックスをオンにします。
4. **ScanCentral ControllerのURL (ScanCentral Controller URL)**]ボックスに、ScanCentral SAST Controller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418

"ScanCentral Controller情報の表示" ページ424

"ScanCentral SASTセンサプールについて" ページ427

"ScanCentral SASTセンサプールの作成" ページ428

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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**]をクリックします。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **ScanCentral DAST**]を選択します。
3. ScanCentral DAST]ページで、 **ScanCentral DASTを有効にする(Enable ScanCentral SAST)**]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。

以下のタスクを実行する方法については、『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、 管理(Administration)]ビューの **設定(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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(Configuration)**] > **スケジューラ(Scheduler)**]の順に選択しま

す。

3. [スケジューラ(Scheduler)]ページで、次の表の説明に従って設定を行います。

フィールド	説明
実行済みジョブが削除されるまでの日数 (Number of days after which executed jobs are removed)	終了したジョブがFortify Software Security Centerから削除されるまでの日数。 デフォルト値は1(日)です。 キャンセルされたジョブの削除は毎日行われます。
ジョブ実行戦略 (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)。 ◦ 最大で、`${job.numberOfConcurrentReports}`個までのレポートジョブを同時に実行できます。 ◦ 最大で、`${numberOfConcurrentExclusiveJobs}`個までの排他的なジョブを同時に実行できます (デフォルト値は1です)。 ◦ 最大で、`${jobs.threadCount}`個までのジョブを同時に実行できます。`${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。 • **柔軟(Flexible):** この戦略のオプションは[保守的(Conservative)]戦略と同じですが、ジョブキューワーカの使用が改善されます。

フィールド	説明
	• **積極的(Aggressive):** 同時並行性が向上します。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 [**柔軟(Flexible)**] 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222を参照してください)。
ジョブ実行を一時停止する(Pause job execution)	このチェックボックス([スケジューラ(Scheduler)] ページでは選択できません)は、サーバのシャットダウンまたはシステム保守の準備としてジョブ実行が([保守(Maintenance)] ページから)一時停止されたかどうかを示します。 このチェックボックスをオンまたはオフにするために [保守(Maintenance)] ページに移動するには、 [こちら(here)] リンクをクリックします。この設定の変更は、 [保守(Maintenance)] ページから変更を保存した直後に有効になります。サーバを再起動する必要はありません。 ジョブの実行を一時停止すると、現在実行中のジョブ(アーティファクト処理、レポート生成、データエクスポート要求など)は完了まで続行します。新しいジョブが送信されるとキューに登録され、 [**ジョブ実行を一時停止する(Pause job execution)**] チェックボックスがオフにされて通常の処理が再開されたら、処理されます。 **重要** サーバのシャットダウン直前にジョブ実行を一時停止して、一時停止の期間をできる限り短くすることを強く推奨します。そうすれば大量のジョブをキューに登録して後で処理することを避けられます。 **注意** 保守後にサーバが再び起動しても、ジョブ実行は自動的には再開されません。ジョブ実行を再開するには、 [保守(Maintenance)] ページに戻り、 [**ジョブ実行を一時**

フィールド	説明
	停止する(Pause job execution)] チェックボックスをオフにする必要があります。
トークン管理(Token management)	
トークンの有効期限アラート(Token expiration alerts)	トークンの有効期限が残り何日になったら、ユーザに有効期限切れを予告するか。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。

フィールド	説明
	スケジューラを毎時間実行する場合は、「*」と入力します。 **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。

フィールド	説明
	スケジューラを毎時間実行する場合は、「*」と入力します。 **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	OpenText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)。
レポートの保守(Reports maintenance)	
保持日数(Days to preserve)	生成されたレポートがFortify Software Security Centerで保持される日数を入力します。デフォルト値は0です (クリーンアップは行われません)。 クリーンアップジョブに要する時間やリソースが過大にならないよう、毎晩の実行で最大2000件の古いレポート(および関連エンティティ) が消去されます。残りのレポートは、その後の数日間でFortify SSCによって徐々にクリーンアップされます。
データエクスポートの保守(Data export maintenance)	
保持日数(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。

フィールド	説明
	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" 下

"スケジュールされたジョブのキャンセル" ページ143

"繰り返し実行されるクリーンアップジョブ" ページ143

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. OpenTextのヘッダで、 [管理(Administration)]を選択します。
2. 左ペインで、 [メトリックとトラッキング(Metrics & Tracking)]を選択し、 [ジョブ(Jobs)]を選択します。
3. [ジョブ(Jobs)]ツールバーの右端の [フィルタ条件(Filter by)]リストから [準備済み(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135

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、OpenTextのヘッダで [**管理(Administration)**] を選択します。
2. 左ペインの [**メトリックとトラッキング(Metrics & Tracking)**] で、 [**ジョブ(Jobs)**] を選択します。
3. [**ジョブ(Jobs)**] ツールバーの右端にあるジョブ状態の [**フィルター条件(Filter by)**] リストから [**準備済み(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135

繰り返し実行されるクリーンアップジョブ

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

ジョブ名と 説明	影響を受けるテーブル	デフォルトのスケジュール
データエクスポートのクリーンアップ(Data Export Cleanup) 指定した日数より古いエクスポート済みデータ(CSVファイルなど)を削除します ("ジョブスケジューラの設定" ページ135)。	dataexport、documentinfo、およびdatablob	毎日 (23:45) Fortify Software Security Centerユーザインタフェースからこのジョブをスケジュールする方法については、"ジョブスケジューラの設定" ページ135を参照してください。
イベントログのクリーンアップ(Event Log Cleanup)	eventlogentry	毎日 (23:30)

ジョブ名と 説明	影響を受けるテーブル	デフォルトのスケジュール
[スケジューラ(Scheduler)]ページに指定した日数より古いイベントレコードを削除します。		Fortify Software Security Centerユーザインタフェースからこのジョブをスケジュールする方法については、"ジョブスケジューラの設定" ページ135を参照してください。
期限切れトークンのクリーンアップ(Expired Tokens Cleanup) 有効期限が過ぎた期限切れトークンを削除します。	agentcredential	毎日、6時間おき、00:00から開始
IDテーブルのクリーンアップ(ID Table Cleanup) ユーザ許可の操作やレポートの生成でフィルタ処理に使用されたIDを削除します。	id_table pv_id_table	毎日(23:00) Fortify Software Security Centerユーザインタフェースからこのジョブをスケジュールする方法については、"ジョブスケジューラの設定" ページ135を参照してください。
ジョブのクリーンアップ(Job Cleanup) 完了したジョブを削除します。(失敗したジョブは、そのジョブの開始時刻から数えて、設定された日数が経過した後で削除されます。キャンセルされたジョブは、開始時刻に関係なくクリーンアップされます)。	jobqueue	毎日(23:00)
孤立したデータのクリーンアップ(Orphaned Data Cleanup)	documentinfo	毎週日曜日(23:30)

ジョブ名と 説明	影響を受けるテーブル	デフォルトのスケジュール
不要になった添付ファイルに関連付けられているメタデータを削除します。		
孤立したソースファイルのクリーンアップ(Orphaned Source Files Cleanup) 既存の問題から参照されなくなったソースファイルを削除します。	sourcefile	毎日(0:00) job.sourceFileCleanup.cronを使用して設定します。
レポートのクリーンアップ(Report Cleanup) [スケジューラ(Scheduler)]ページの**保持日数(Days to preserve)**]に指定した日数より古い生成済みレポートを削除します。	savedreport documentinfo datablob	クリーンアップのスケジュールなし Fortify Software Security Centerユーザインタフェースからこのジョブをスケジュールする方法については、"ジョブスケジューラの設定" ページ135を参照してください。
Webhook履歴のクリーンアップ(Webhook History Cleanup) 古いwebhookイベントエントリを削除します。	webhookhistory	毎日(3:30)
インデックス保守(Index Maintenance) グローバル検索(フルテキスト)インデックスと既存のデータベースエントリとの間の不整合(不完全なサーバシャットダウンやインデックス付けジョブの失敗によるものなど)を解決します。	N/A	毎日(0:00) Fortify Software Security Centerユーザインタフェースからこのジョブをスケジュールする方法については、"ジョブスケジューラの設定" ページ135を参照してください。

ジョブ名と 説明	影響を受けるテーブル	デフォルトのスケジュール
LDAPの更新(LDAP Refresh) LDAPエンティティに関連付けられたキャッシュを更新します。	N/A	6時間おき
履歴スナップショット(Historical Snapshot) 古いスナップショットを再作成します。	N/A	毎日(0:00) Fortify Software Security Centerユーザインタフェースからこのジョブをスケジュールする方法については、"ジョブスケジューラの設定" ページ135を参照してください。"ジョブスケジューラの設定" ページ135
アラートリマインダ(Alert Reminder) リマインダアラートを送信します。	N/A	毎日(3:00)
トークンの期限切れアラート(Token Expiry Alerts) 間もなく期限切れになるトークンについてユーザに通知します。	N/A	毎日(3:00)

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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **セキュリティ(Security)**]を選択します。
3. セキュリティ(Security)]ページで、次の表の説明に従って設定を行います。

フィールド	説明
Content-Security-Policy	使用するCSPのレベル(必要な場合)を指定します。HTTP Content-Security-Policyヘッダを使用して、ブラウザがロードできるリソース、および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。 • `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-	Public-Key-Pinsヘッダの値を入力します。これにより、中

フィールド	説明
Key-Pins header	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)。 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
CAS (Central Authenticationサービス)	"Central Authenticationサービスを使用するためのFortify Software Security Centerの設定" 次のページ
SPNEGO/ KERBEROS	"Fortify Software Security CenterでのKerberos認証の設定" ページ158
SAML 2.0準拠のシングルサインオン	"SAML 2.0準拠のシングルサインオンを使用するためのFortify Software Security Centerの設定" ページ150
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156
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160

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162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 Authenticationサービス(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161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77

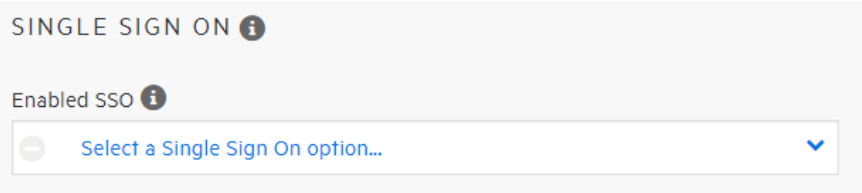
Central Authenticationサービスを使用するためのFortify Software Security Centerの設定

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 Authenticationサービス(CAS)を使用するようにFortify Software Security Centerを設定するには:

1. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで[**管理(Administration)**]をクリックします。
2. 左ペインで、[**設定(Configuration)**]を選択してから、[**SSO**]を選択します。

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. [**シングルサインオン(SINGLE SIGN ON)**]ページの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サービスのURL (Central Authentication Service URL)**]ボックスに、CAS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162を参照してください。

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

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

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

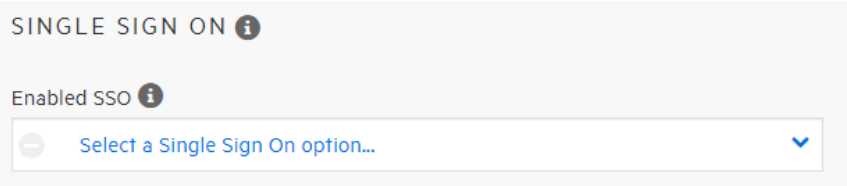
SAML 2.0を使用するSSOが動作するようFortify Software Security Centerを設定するには、次の手順に従います。

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108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. SAMLメッセージのデジタル署名とSAMLアサーションの暗号化に使用する公開鍵/秘密鍵のペアを用意します。IdPが特定の認証局によって署名された鍵を必要としない場合は、OpenSSLやJavaのkeytoolなどを使用して、独自の自己署名鍵を生成できます。次のコマンド例では、特定のエイリアスの下に自己署名鍵を格納するキーストアを生成します。

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

   エイリアスと両方のパスワードの値をメモしておきます。これらの値を、後で [Fortify Software Security Centerの管理(Fortify Software Security Center Administration)] セクション(**管理(Administration)**] > **設定(Configuration)**] > **SSO**] > **SAML**])で指定する必要があります。
4. IdPサーバからSAMLメタデータを取得し、それをFortify Software Security Centerファイルシステムに保存します。
5. メタデータファイルを開き、IdP EntityDescriptorのエンティティIDをメモします(<EntityDescriptor entityID="THE_VALUE_YOU_ARE_LOOKING_FOR">)。メタデータが署名されているかどうかを確認します([Signature] セクションが存在します)。メタデータが署名されている場合、署名はPKIX検証アルゴリズムで検証され、キーストアに存在する公開鍵はすべてトラストアンカーとして使用されます。キーストアには、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。
6. Fortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**] を選択します。
7. 左ペインで、 **設定(Configuration)**] を選択してから、 **SSO**] を選択します。

   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、[シングルサインオン(SINGLE SIGN ON)]ページのリストにその名前が表示されます。

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(ステップ3で取得したメタデータ)の場所。
	例
	• Windowsの場合:
	`file:///C:/fortify/federation-metadata.xml`
	• Linuxの場合:
	`file:///home/fortify/federation-metadata.xml`
	注: Entra IDと統合している場合は、Azureの[アプリのフェデレーションメタデータURL (App Federation Metadata Url)]フィールドに表示される値を入力します。(Azureの左側のペインの[管理(Manage)]で、[Single Sign-on]を選択し、[SAML]を選択します。[SAML Signing Certificate]の[App Federation Metadata Url]フィールドが表示されます)。
	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)。

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

Keystore location	SAMLメッセージの署名とSAMLアサーションの暗号化に使用される鍵のペアを格納するキーストアの場所。
	例
	• Windowsの場合:
	`file:///C:/fortify/keystore.jks`
	• Linuxの場合:
	`file:///home/fortify/keystore.jks`
	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	キーストアファイルのパスワード
署名および暗号化キー(Signing & encryption key)	キーストアファイル内の署名/暗号化キーのエイリアス
署名および暗号化キーのパスワード (Signing & encryption key	署名/暗号化キーパスワード

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

10. **[保存(SAVE)]**をクリックします。
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。このURLは、Fortify Software Security Center SAMLメタデータ内に*<AssertionConsumerService>*および*<SingleLogoutService>*の場所を構築するためのベースURLとして使用されます。
12. IdPから送信されるSAMLアサーションが暗号化されている場合は、認証応答メッセージが署名されている必要があります。

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

13. 最近のChromeまたはChromiumベースのブラウザは、デフォルトでSameSite=Laxクッキーポリシーに設定されています。つまり、クッキーはサードパーティサイトへのサブリクエストでは送信されません。このため、Fortify Software Security Centerから開始されていないシングルログアウトは正しく動作しません。

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

    ChromeまたはChromiumベースのブラウザでシングルログアウトを機能させるには、セッションクッキーのSameSiteポリシーをNoneに変更する必要があります。これはデフォルトよりもセキュリティ保護の弱いポリシーであるため、そのように変更することが組織にとって最適なアプローチかどうかを判断する必要があります。コンテナ展開用のポリシーを変更するには、 HTTP_SERVER_SAME_SITE_COOKIES環境変数を使用します。コンテナ以外の展開の場合は、Tomcat設定のcontextセクションに<CookieProcessor sameSiteCookies="none"/>を追加します。詳細については、https://tomcat.apache.org/tomcat-9.0-doc/config/context.html#Nested_Componentsを参照してください。

14. Fortify Software Security Centerを再起動します。
15. `<hostname>:<port>/<context>/saml/metadata/<SP_alias>`でFortify Software Security Center(SP)メタデータを生成します。
16. 前のステップで生成されたメタデータを開き、`<AssertionConsumerService>`および`<SingleLogoutService>`内の場所URLにIdPサーバからアクセス可能であることを確認します。
17. Fortify Software Security CenterメタデータをIDPサーバにアップロードします。
18. `<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162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。
  - ユーザがFortify Software Security Center内に存在し、役割が割り当てられています。
  - ユーザルックアップ戦略が正しく設定されています(「"コア設定の設定" ページ96」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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **SSO**]を選択します。

   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. **シングルサインオン(SINGLE SIGN ON)**]ページの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統合属性(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 Response Header	動的ディレクティブヘッダを入力します。
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108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162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148

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、OpenTextのヘッダで **管理(Administration)**]を選択します。
5. 左ペインで、 **設定(Configuration)**]を選択してから、 **SSO**]を選択します。

   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. **シングルサインオン(SINGLE SIGN ON)**]ページの **有効なSSO(Enabled SSO)**]リストから、 **SPNEGO/KERBEROS**]を選択します。
7. **SPNEGO/Kerberos統合属性(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111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。
    - Chromeの場合は、イントラネットのサイトと信頼できるサイトにサービス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。

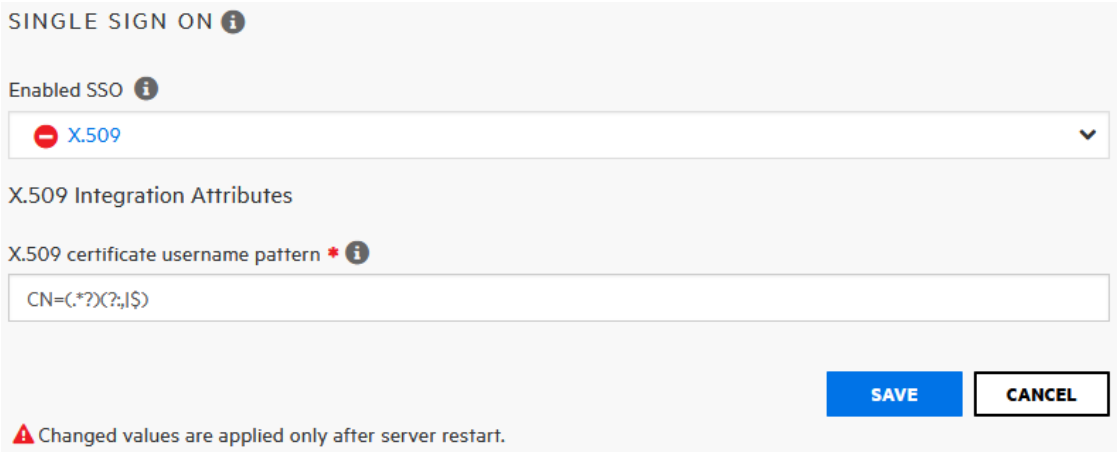
参照情報
"シングルサインオンを使用するためのFortify Software Security Centerの設定" ページ 148

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certificate Verification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、OpenTextのヘッダで**管理(Administration)**]を選択します。
3. 左ペインで、**設定(Configuration)**]を選択してから、**SSO**]をクリックします。

注: Fortify Software Security Centerに対して一度に設定できるサインオンソリューションは1つのみです。



4. [Single Sign-on(SINGLE SIGN ON)]ページの [有効なSSO (Enabled SSO)]リストから [X.509]を選択します。
5. [X.509認定ユーザ名パターン(X.509 certificate username pattern)]ボックスに、Fortify Software Security Centerでクライアント証明書からユーザ名を取得する方法を指定する正規表現を入力します。
   - X.509認定の [サブジェクト(Subject)]フィールドからユーザ名を取得するには、キャプチャグループを含む正規表現を使用します。そのあとで、この正規表現を [サブジェクト(Subject)]フィールド値のユーザ名と一致させるために使用します。

     例: 証明書の [サブジェクト(Subject)]フィールドのCN属性と一致させるには、`CN=(.*?)`パターンを指定します。
   - X.509認定のサブジェクト代替名(SAN)拡張の [その他の名前(Other Name)]からユーザ名を取得するには、`$0!OID$regex`パターンを使用します。ここで、
     - `OID`は、ユーザ名を取得するその他の名前の識別子を表します。文字列値を含むその他の名前だけがサポートされます。
     - `regex`は、その他の名前の値からユーザ名を取得するために使用するキャプチャグループを含む正規表現を表します。

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

     UPNの下で`username@domain`全体と一致させるには、次のパターンを指定します。

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

     UPNの下で、ドメインを含めずに、`@`記号の前のユーザ名だけと一致させるには、次のパターンを指定します。

     ```
     $0!1.3.6.1.4.1.311.20.2.3$(.+?(?=@))
     ```
6. [保存(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" ページ160

"Fortify Software Security CenterでのKerberos認証の設定" ページ158

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.FmHttpSsoAuthenticationFil
   ter" 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、そのセクションで各ロガーのレベルを適切なデバッグ値に変更します。
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、そのセクションで各ロガーのレベルを適切なデバッグ値に変更します。

参照情報

"シングルサインオンを使用するためのFortify Software Security Centerの設定" ページ148

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 [管理(Administration)] ビューの **[設定(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451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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで[**管理(Administration)**]を選択します。
2. 左ペインで、[**設定(Configuration)**]を選択してから、[**Webサービス(Web Services)**]を選択します。
3. [Webサービス属性(WEB SERVICE ATTRIBUTES)]ページで、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、[**トークン認証を許可する(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(FIPS)環境でのFortify Software Security Centerの実行

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

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

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(「ダッシュボード(Dashboard)」、 「アプリケーション(Applications)」、 「レポート(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。

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

ユーザのためにカスタムFortify Software Security Centerログオンエクスペリエンスを作成するには:

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`<!--<center><font color="red">Add your custom banner here</font></center>-->`をコメント解除し、表示されるメッセージの外観、使用感、およびコンテンツを設定するHTML要素を指定します。

   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>
   ```

   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。

Fortify Software Security Centerでユーザがビュー([ダッシュボード(Dashboard)]、 [アプリケーション(Applications)]、 [レポート(Reports)]など)を切り替えるたびに表示するメッセージバナーを作成するには:

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ディレクトリに移動します。
4. テキストエディタでindex.htmlファイルを開き、41行目に移動します。
5. テキスト 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、雰囲気、および内容を設定する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。

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

   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*>以下のすべてのファイルとディレクトリを含むssc-htmlui-<*version*>.jarという名前の新しいアーカイブを作成します。
8. Fortify Software Security Centerサーバを再起動します。

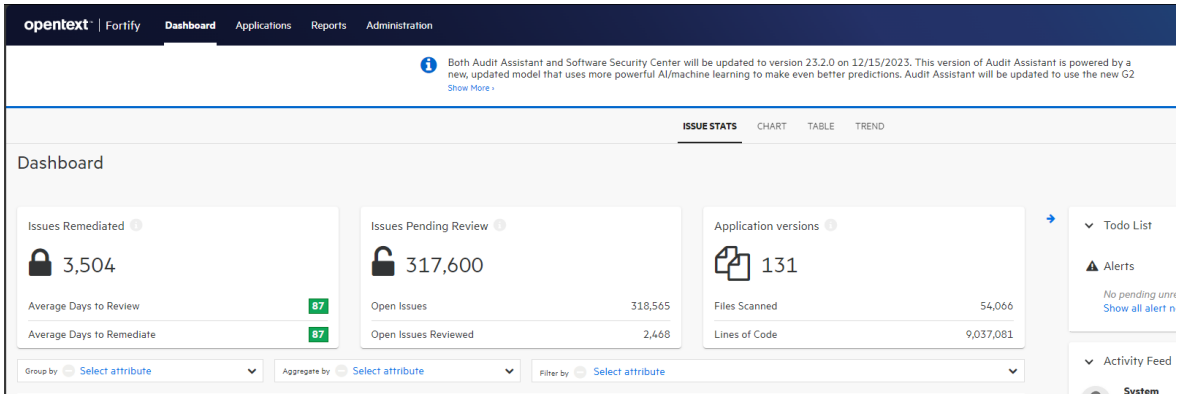
参照情報

"ダッシュボードへのFortify Insightリンクの追加" ページ167

"システム全体のバナーを作成する" 次のページ

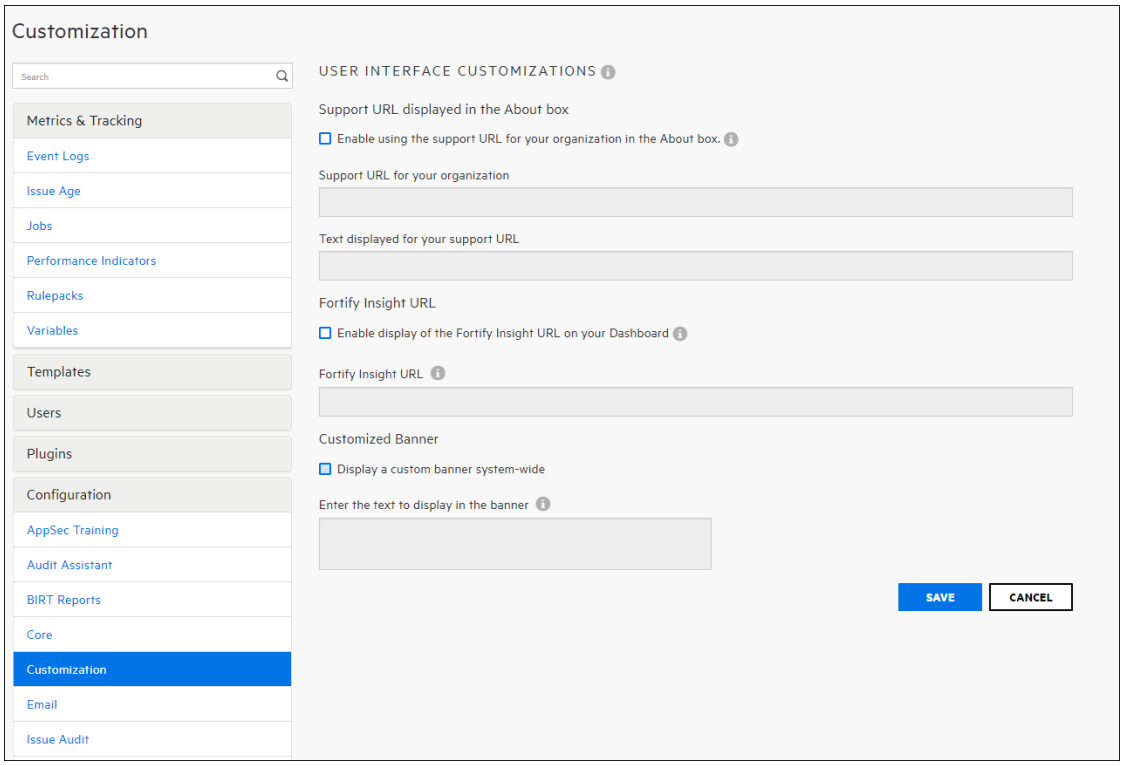
システム全体のバナーを作成する

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



システム全体のバナーを作成するには:

1. 管理者としてFortify Software Security Centerにログインします。
2. OpenTextのヘッダで、 **[管理(Administration)]** をクリックします。
3. 左側のペインで **[設定(Configuration)]** を展開し、 **[カスタマイズ(Customization)]** を選択します。



4. **[システム全体にカスタムバナーを表示(Display a custom banner system-wide)]** チェックボックスをオンにします。
5. テキストボックスにバナーのテキストを入力します。
6. **[保存(SAVE)]** をクリックします。

参照情報

"Fortifyバナーの組織向けカスタマイズ" ページ164

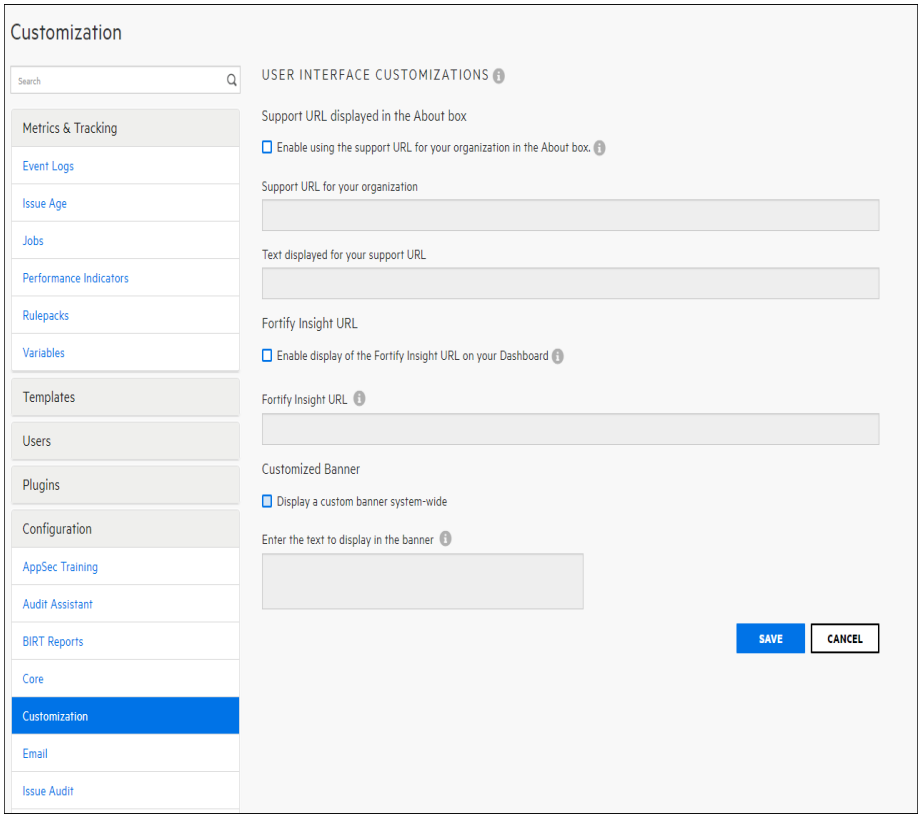
"ダッシュボードへのFortify Insightリンクの追加" 下

ダッシュボードへのFortify Insightリンクの追加

Fortify Insightを購入した場合は、Fortify Software Security Centerダッシュボードに Fortify Insightリンクを追加することで、Fortify Software Security CenterをFortify Insightダッシュボードにリンクできます。

Fortify Software Security Centerダッシュボードに Fortify Insightリンクを追加するには:

1. 管理者ユーザとしてFortify Software Security Centerにログインします。
2. OpenTextのヘッダで、 **[管理(Administration)]** をクリックします。
3. 左側のペインで **[設定(Configuration)]** を展開し、 **[カスタマイズ(Customization)]** を選択します。



4. **[Fortify Insight URL]**の下で、**ダッシュボードでFortify Insight URLの表示を有効にする(Enable display of the Fortify Insight URL on your Dashboard)**]チェックボックスをオンにします。
5. **[Fortify Insight URL]**ボックスに、Fortify InsightページのURLを入力します。
6. **保存(SAVE)**]をクリックします。

参照情報

"Fortifyバナーの組織向けカスタマイズ" ページ164

" [Fortify Software Security Centerについて(About Fortify Software Security Center)]ボックスのサポート連絡先リンクを変更する" 下

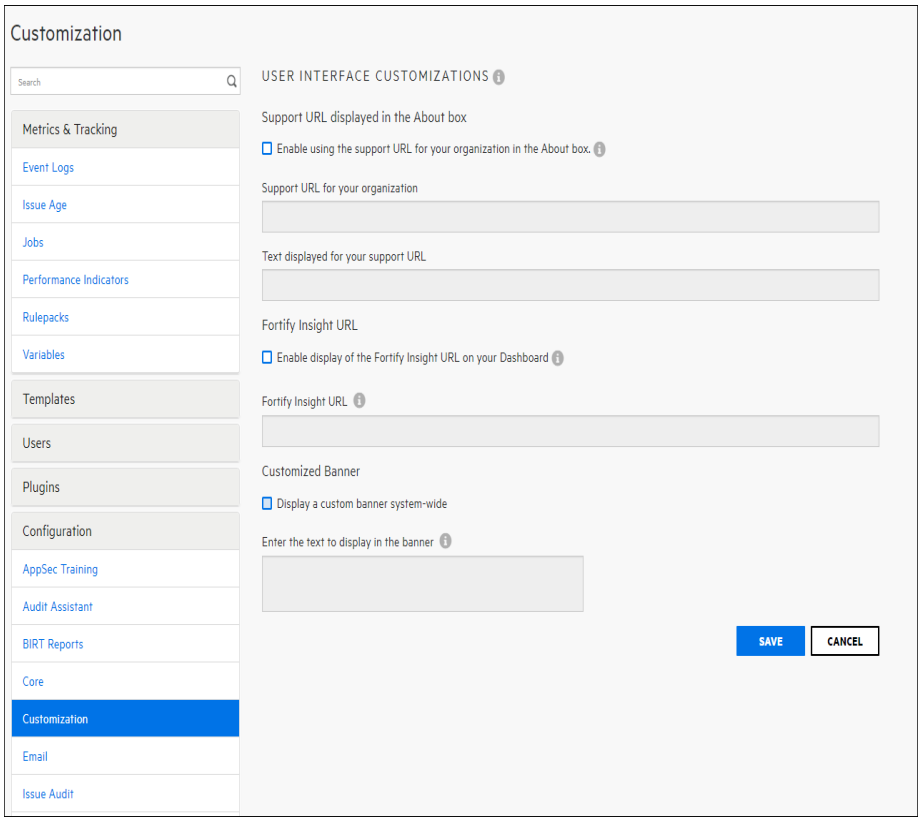
"システム全体のバナーを作成する" ページ166

[Fortify Software Security Centerについて(About Fortify Software Security Center)]ボックスのサポート連絡先リンクを変更する

デフォルトでは、[Fortify Software Security Center <version>について(About Fortify Software Security Center <version>)]ボックスには、サポートポータルへのリンクが表示されます。そのリンクを自分の組織のサポートポータルへのリンクに置き換えることができます。

独自のサポートポータルを [Fortify Software Security Centerについて(About Fortify Software Security Center)] ボックスに表示するには:

1. 管理者ユーザとしてFortify Software Security Centerにログインします。
2. OpenTextのヘッダで、 **管理(Administration)**] をクリックします。
3. 左側のペインで **設定(Configuration)**] を展開し、 **カスタマイズ(Customization)**] を選択します。



4. **[バージョン番号ボックスで組織のサポートURLの使用を有効にする(Enable using the support URL for your organization in the About box)]** チェックボックスをオンにします。
5. **[組織のサポートURL (Support URL for your organization)]** ボックスに、組織のサポートポータルのURLを入力します。
6. **[サポートURLに表示するテキスト(Text displayed for your support URL)]** ボックスに、サポートへの新しいリンクに表示するテキストを入力します。
7. **[保存(SAVE)]** をクリックします。

参照情報

"Fortifyバナーの組織向けカスタマイズ" ページ164

"ダッシュボードへのFortify Insightリンクの追加" ページ167

Fortify Software Security Centerログ記録のカスタマイズ

Fortify Software Security Centerインスタンスのログ記録をカスタマイズするには、カスタムlog4j2設定ファイルをプロビジョニングして、*<fortify.home>/<app_context>*/conf内の標準のlog4j2設定ファイルを上書きしたり、これに追加したりすることができます。

カスタムLog4j2設定上書きファイルをプロビジョニングするには、COM_FORTIFY_SSC_LOG4j2_OVERRIDEシステム環境変数またはcom.fortify.ssc.log4j2.overrideJVMシステムプロパティをカスタムLog4j2XML設定ファイルの絶対パスに設定します。

<fortify.home>/*<app_context>*/conf/log4j2.xmlファイルを直接変更するよりも、これらの方法のいずれかを用いたほうが管理が容易になるので、これらの方法を用いることを強く推奨します。

Fortify Software Security Centerのログインに必要なパスワード強度の設定

password.strength.min.scoreプロパティ(*<fortify.home>*/*<app_context>*/conf/app.propertiesにある)を使用して、必要なパスワード強度を調整できます。次の表に、有効な値とそれぞれの値が表す強度を一覧にして示します。

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

パスワード強度は、1つの大文字や1つの特殊文字などの要件に基づいて決定されません。その代わりに、専用のパスワード強度ライブラリに基づいて計算されます。そこで使用されるのは、パスワードを破るまでの時間の見積もり、予測可能な文字シーケンスやユーザ名がパスワードに含まれていないかどうかの判定、一般的なパスワード辞書の照合などの方法です。

次を参照

"セッションログアウトについて" ページ77

"追加のFortify Software Security Center設定" ページ80

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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**] をクリックします。
2. 左ペインで、 **設定(Configuration)**] を選択して、 **コア(Core)**] を選択します。
3. コア(Core)] ページの下部までスクロールし、 **CSVへのエクスポートを有効にする(Enable Export to CSV)**] チェックボックスをオフにします。
4. **保存(SAVE)**] をクリックします。

参照情報

"コア設定の設定" ページ96

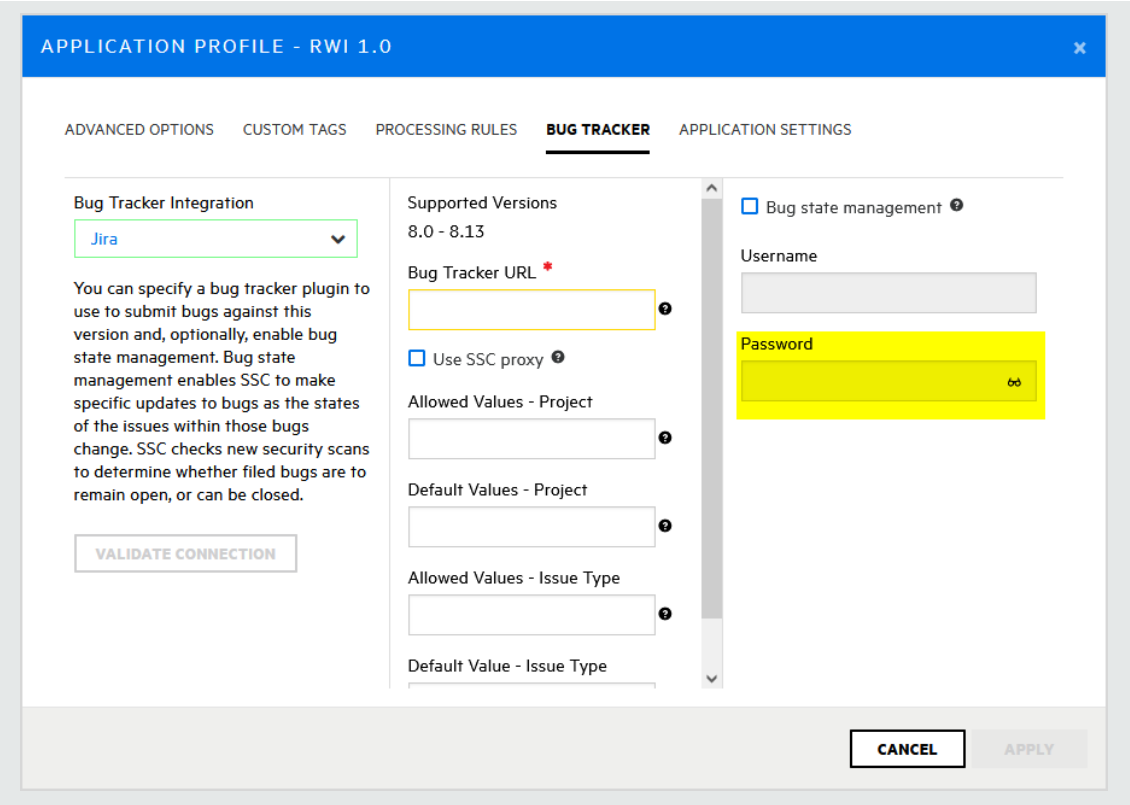
"データをカンマ区切り値ファイルへエクスポートする" ページ222

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。

- Jira
- Jira Cloud

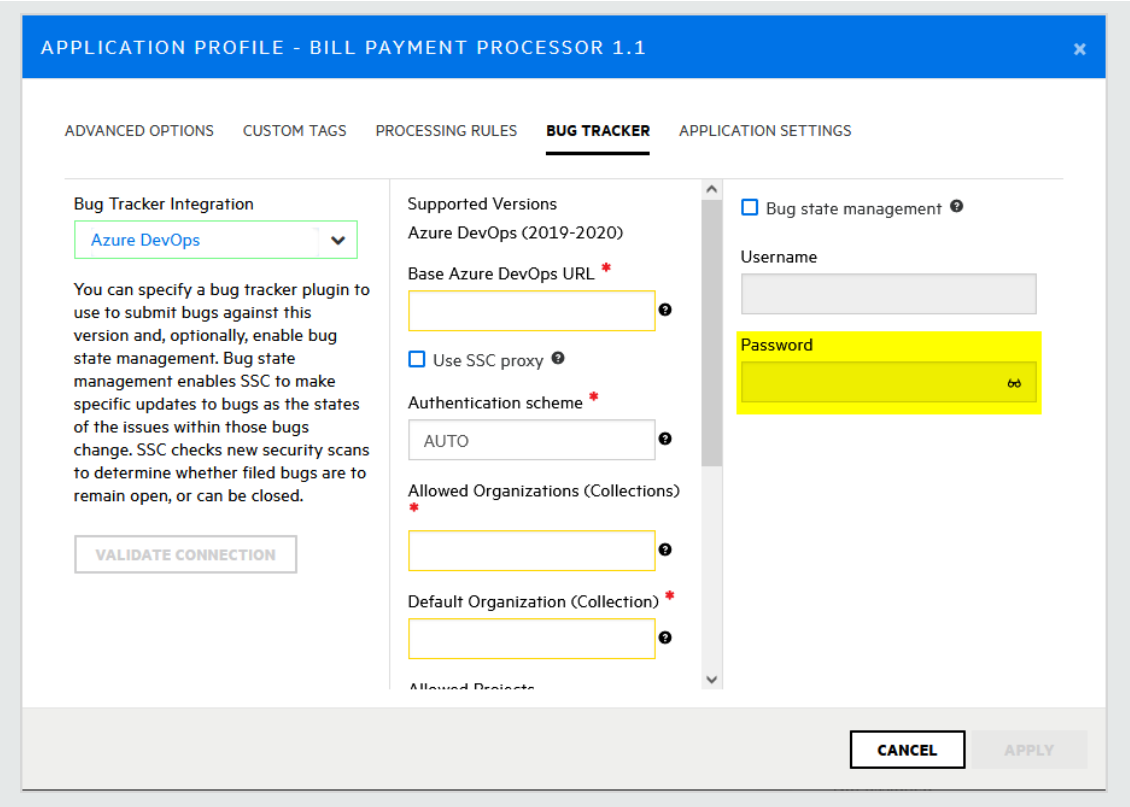
> **注:** Jira Cloudを使用する場合は、ログイン時に [Password] フィールドでJira認証トークンを使用する必要があります。



- ALM
- Azure DevOps Server

重要 Azure DevOpsの [再現手順(Repro Steps)]フィールドにはFortifyのバグの説明が表示されますが、デフォルトで、このフィールドは問題の作業項目で非表示になっています。Azure DevOps 2019.1以降のバージョンを使用し、かつ基本プロセスを使用する場合は、問題の作業項目をカスタマイズして [再現手順(Repro Steps)]フィールドを表示する必要があります。

重要 Azure DevOpsを使用している場合は、ログイン時の [パスワード(Password)]フィールドで、Azure DevOpsが生成した個人用アクセストークンを使用する必要があります。Azure DevOpsの個人用アクセストークンの詳細については、https://learn.microsoft.com/ja-jp/azure/devops/organizations/accounts/use-personal-access-tokens-to-authenticate?view=azure-devops&tabs=Windowsを参照してください。



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462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264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。

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、OpenTextのヘッダで、[**管理(Administration)**]を選択します。
2. 左ペインで、[**プラグイン(Plugins)**]を選択し、[**バグトラッキングプラグイン(Bug Tracking Plugins)**]を選択します。
3. [バグトラッキング(Bug Tracking)]ページのヘッダで、[**新規(New)**]をクリックします。
   Fortify Software Security Centerに、[プラグインのアップロードの警告(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。
5. [プラグインバンドルのアップロード(UPLOAD PLUGIN BUNDLE)]ダイアログボックスで、[参照(BROWSE)]をクリックし、プラグインのJARファイルを見つけて選択します。Fortify Software Security Centerが提供するJARファイルまたは自分で作成したバグトラッカプラグイン用のJARファイルを使用できます("バグトラッカプラグインの作成" ページ462を参照してください)。
   Fortify Software Security Centerが提供するバグトラッカのJARファイルは、次の場所にあります。

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

6. [**アップロードの開始(START UPLOAD)**]をクリックします。
   アップロードが完了すると、[Bug Tracking]テーブルに新しいプラグインが一覧表示されます。
7. バグトラッカプラグインを有効にするには、[**ENABLE**]をクリックします。

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

参照情報

"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269

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

参照情報

"バグトラッカーの統合について" ページ172

"パーサプラグインの追加と管理" 次のページ

"バグトラッカプラグインの作成" ページ462

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462を参照するか、カスタマサポート(https://www.microfocus.com/support)にお問い合わせください。

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。

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、OpenTextのヘッダで、[管理(Administration)]を選択します。
2. 左ペインで、[プラグイン(Plugins)]を選択し、[パーサプラグイン(Parser Plugins)]を選択します。
3. [パーサ(Parsers)]ページヘッダで、[NEW(新規)]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。
5. [プラグインバンドルのアップロード(Upload Plugin Bundle)]ダイアログボックスで、[参照(BROWSE)]をクリックし、プラグインのバンドルファイル(JARファイル)を見つけて選択します。
6. [アップロードの開始(START UPLOAD)]をクリックします。
   [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174

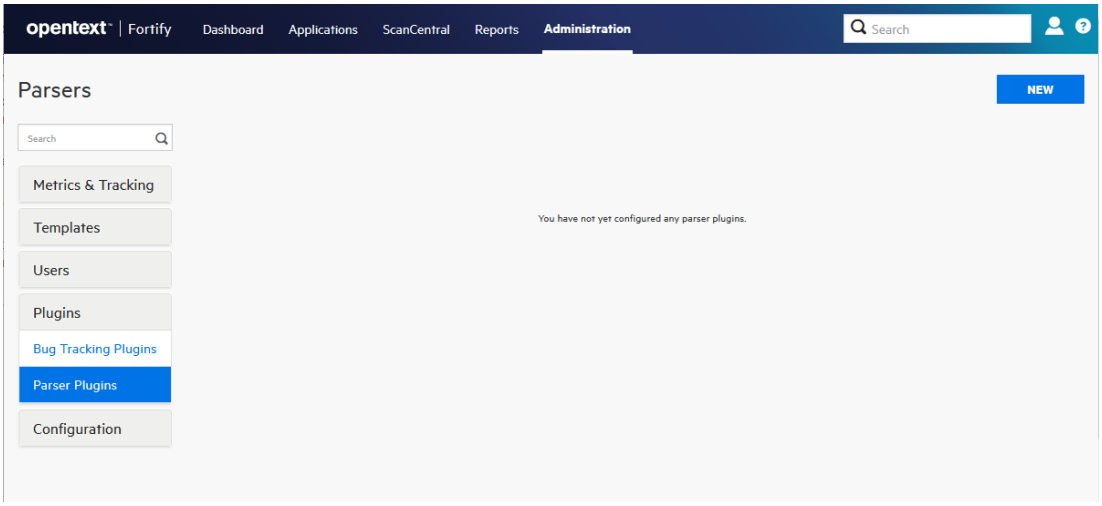
Sonatype結果を表示するためのFortify Software Security Centerの準備

アプリケーションバージョンに関するSonatype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[監査(AUDIT)]ページまたは[オープンソース(OPEN SOURCE)]ページで表示できます。そうするには、まず必要なSonatype Parser Pluginをダウンロードしてインストールする必要があります。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スキャン結果が表示されます。

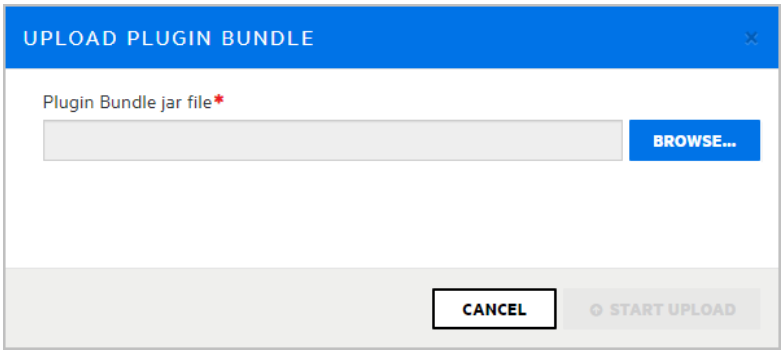
Fortify SourceAndLibScannerを取得するには、https://marketplace.microfocus.com/cyberres/content/fortify-sourceandlibscannerにアクセスします。SourceAndLibScannerを使用して、オープンなSonatypeスキャン結果をFortify Software Security Centerにアップロードする方法については、『OpenText™ Fortify SourceAndLibScannerユーザガイド』を参照してください。このガイドは、Fortify SourceAndLibScannerユーティリティに付属しています。

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。

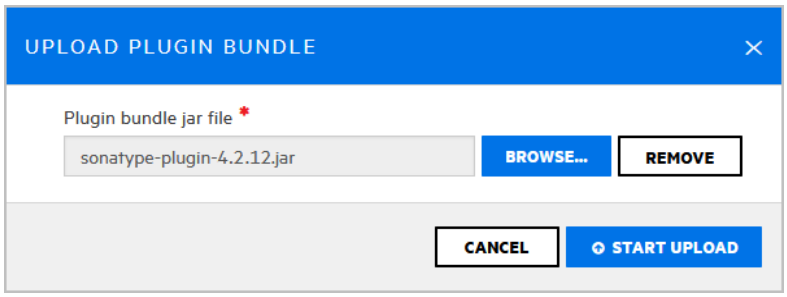
1. ブラウザウィンドウを開いて、Fortify Marketplace (https://marketplace.microfocus.com/cyberres/content/sonatype-nexus-lifecycle-integration-with-ssc)に移動します。
2. [**Sonatype Nexus LifecycleとSSCの統合(Sonatype Nexus Lifecycle integration with SSC)**]ページで、**最新バージョンの取得(GET NEWEST)**]をクリックします。
3. `SonatypeFortifyBundle-<version>.zip`ファイルの内容をローカルディレクトリに解凍します。
4. 管理者としてFortify Software Security Centerにログオンします。
5. OpenTextのヘッダで、**管理(Administration)**]を選択します。
6. 左ペインで、**プラグイン(Plugins)**]セクションを展開し、**パーサプラグイン(Parser Plugins)**]を選択します。



7. [**パーサ(Parsers)**]ページで、**新規(New)**]をクリックします。
8. [**UPLOAD PLUGIN WARNING**]を閉じ、**OK**]をクリックします。



9. [**プラグインバンドルのアップロード(UPLOAD PLUGIN BUNDLE)**]ダイアログボックスで、**参照(BROWSE)**]をクリックしてから、`sonatype-plugin-<version>.jar`ファイルに移動して選択します。



10. [プラグインバンドルのアップロード(UPLOAD PLUGIN BUNDLE)]ダイアログボックスで、 [**アップロードを開始(START UPLOAD)**]をクリックします。
    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

"スキャンアーティファクトのアップロード" ページ327

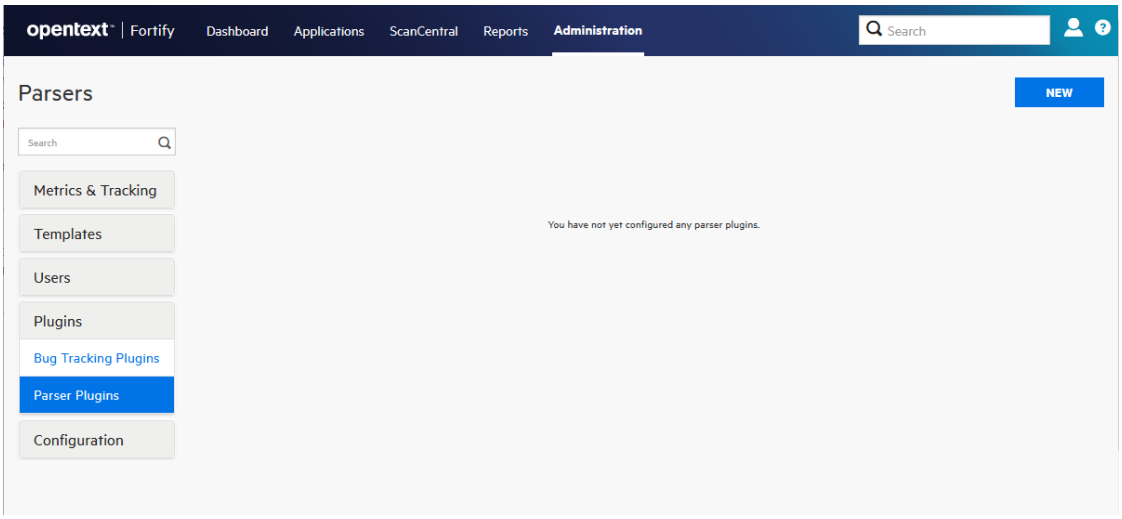
"Webアプリケーションの被影響性分析について" ページ402

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

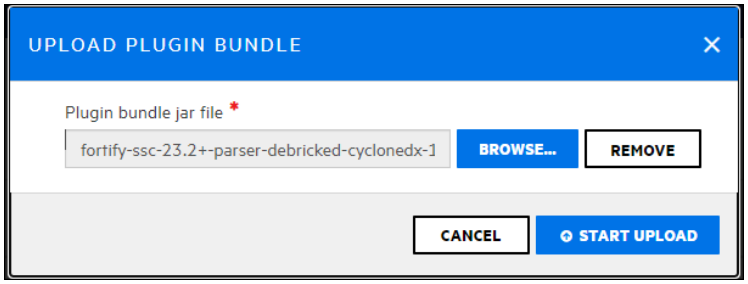
Debrickedからのオープンソースのセキュリティデータは、Fortify Software Security Centerの [監査(AUDIT)]ページまたは [オープンソース(OPEN SOURCE)]ページで表示できます。そのためには、まず、必要なパーサプラグインをダウンロードしてインストールする必要があります。この操作を完了すると、Fortify Software Security Centerにアップロードされたオープンソーススキャン結果が表示されます。

Debrickedのデータを表示するためのFortify Software Security Centerの準備をするには:

1. ブラウザウィンドウを開き、https://github.com/fortify/fortify-ssc-parser-debricked-cyclonedx/releasesに移動します。
2. [**資産(Assets)**]をクリック(展開)して、最新バージョンのパーサを選択します。本ドキュメントの執筆時点の最新バージョンは`fortify-ssc-23.2+-parser-debricked-cyclonedx-1.10.zip`です。
3. [**ダウンロード(Downloads)**]フォルダに移動して、ダウンロードしたZIPファイルの内容をローカルディレクトリに抽出します。
4. 管理者としてFortify Software Security Centerにログオンします。
5. OpenTextのヘッダで、 [**管理(Administration)**]を選択します。
6. 左ペインで、 [**プラグイン(Plugins)**]セクションを展開し、 [**パーサプラグイン(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。
9. [プラグインバンドルのアップロード (UPLOAD PLUGIN BUNDLE)] ダイアログボックスで、 **参照 (BROWSE)** をクリックしてから、展開したJARファイルに移動して選択します。



10. [プラグインバンドルのアップロード (UPLOAD PLUGIN BUNDLE)] ダイアログボックスで、 **アップロードを開始 (START UPLOAD)** をクリックします。

    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。 [パーサ (Parsers)] ページに、Fortify Software Security Center用のDebrickedパーサプラグインが一覧表示されます。
11. Debrickedパーサプラグインの行を展開してから、 **有効にする (ENABLE)** をクリックします。
12. [プラグインの有効化の警告 (ENABLE PLUGIN WARNING)] を読み、 [OK] をクリックします。

参照情報

"スキャンアーティファクトのアップロード" ページ327

"オープンソースデータの表示" ページ413

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184

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 182
ユーザアカウントの作成について 183
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 184
Fortify Software Security Centerの役割に関する許可情報の表示 184
LDAPユーザ役割の管理について 185

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213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235

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、または一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一時停止できます。Fortify Software Security Centerでは、このようなアカウントに対する一時停止機能と削除機能が自動的に無効になります。

ユーザアカウントの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230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96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227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" 下

"ローカルユーザアカウントのロック解除" ページ235

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。

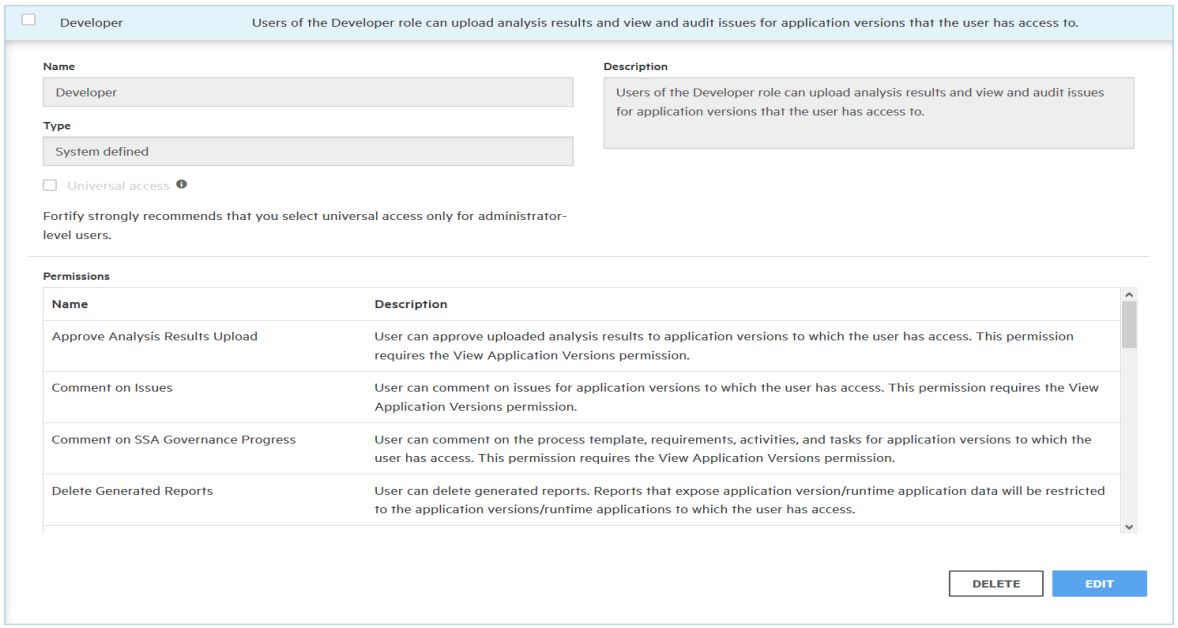
- 信頼されたユーザにのみアクセス許可を割り当てます。
- Fortify Software Security Centerにアップロードする前に、すべてのカスタムテンプレートで任意のSQLクエリとコマンドをチェックしてください。

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. OpenTextのヘッダで、 **管理(Administration)**] を選択します。
2. 左ペインで、 **ユーザ(Users)**] 、 **役割(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227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183

"事前設定済みの役割" ページ227

"ローカルユーザアカウントのロック解除" ページ235

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 (ユーザは認証されていません)」というテキストが含まれている場合は、次の点を確認してください。

- ユーザがFortify Software Security Centerに登録され、役割が割り当てられているか。LDAP管理者に問い合わせて、ユーザが属すると想定されるグループの実際のメンバーであるかどうかを確認します。
- ユーザがそのLDAPグループに属している場合は、そのグループがFortify Software Security Centerに登録され、役割が割り当てられているかどうかを確認します。
- 特別なケース: ユーザがFortify Software Security Centerに登録されたLDAPグループに属しているが、そのグループに追加されたのがたった数時間前である場合は、LDAPキャッシュを手動で更新するか、自動更新を数時間待ちます。

LDAPキャッシュの更新を手動で要求するには:

1. OpenTextのヘッダで、 **管理(Administration)**] を選択します。
2. 左ペインで、 **ユーザ(Users)**] 、 **LDAPエンティティ(LDAP Entities)**] の順に選択します。
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、 管理(Administration)] ビューで、 **イベントログ(Event Logs)**] ページまたは **ジョブ(Jobs)**] ページのいずれかを確認します。

注: 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70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70または"アップグレード後のFortify Software Security Centerの設定" ページ201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、OpenText 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 管理(Administration)]ビューから変更できます。このジョブを1日1回実行するようにスケジュールすることを推奨します。実行されたジョブを再スケジュールする方法については、「"ジョブスケジューラの設定" ページ135」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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**]を選択します。

2. 左ペインで、 **設定(Configuration)**]を選択してから、 **保守(Maintenance)**]を選択します。
3. 保守(Maintenance)]ページで **保守モードに設定する(Set to maintenance mode)**]チェックボックスをオンにし、 **保存(SAVE)**]をクリックします。
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には、現在の設定がすべて表示されます。サーバ設定に関する情報については、"Fortify Software Security Centerの初回設定" ページ70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" 下で説明されている解決策のいずれかを試してください。

サーバの保守を容易にするため、ジョブの実行を一時停止できます。これにより、実行中のジョブは終了しますが、新しいジョブは実行されません。詳細については、"ジョブ実行の一時停止と再開" 次のページを参照してください。

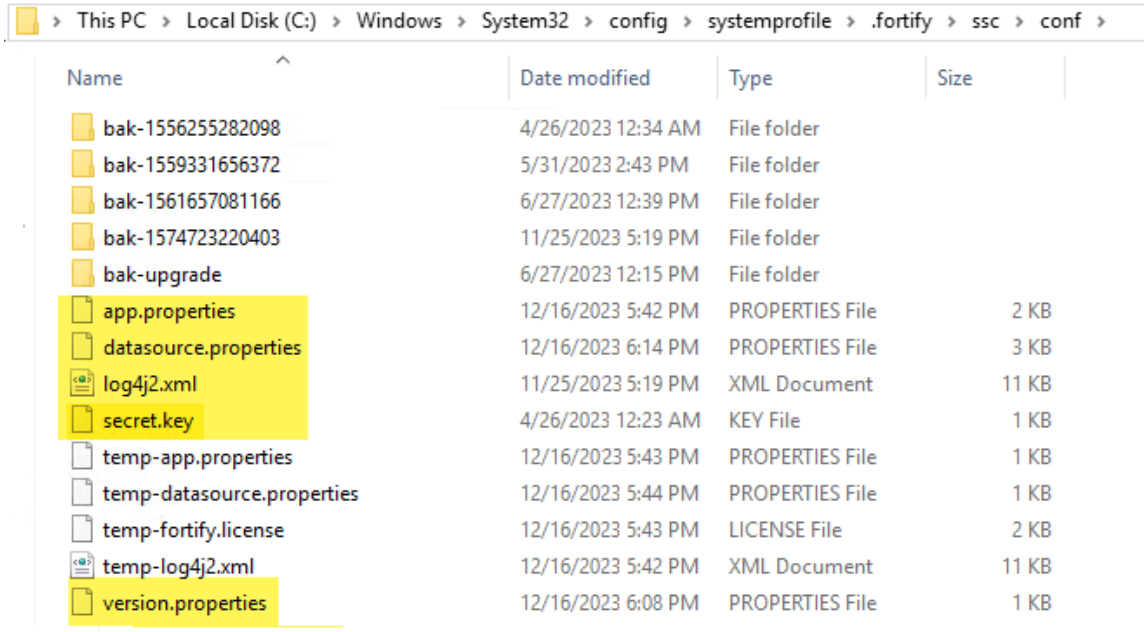
Fortify Software Security Centerが保守モードでスタックしている場合

Fortify Software Security Centerは、 管理(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188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70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。

ジョブ実行の一時停止と再開

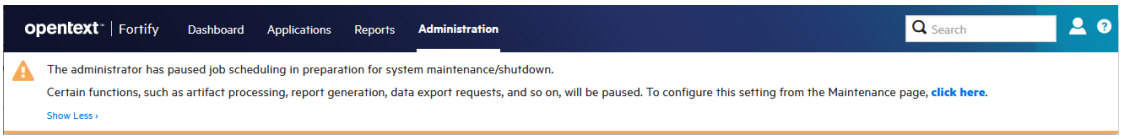
何らかの理由でサーバをシャットダウンする必要がある場合は、ユーザアクティビティを一時停止して、システム内のすべてのユーザに対して新しいジョブの実行を無効にできますが、Fortify Software Security Centerで進行中のジョブは完了できます。これは、サーバのシャットダウン時にデータの破損や消失を防ぐのに役立ちます。

サーバ上でジョブ実行を一時停止するには:

1. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(Configuration)**]を選択してから、 **保守(Maintenance)**]を選択します。
3. 保守(Maintenance)]ページで、 **ジョブ実行を一時停止する(Pause job execution)**]チェックボックスをオンにしてから、 **保存(SAVE)**]をクリックします。
   設定を保存した直後に、以下のようになります。

重要 大量のジョブがキューに登録されるのを防ぐために、この設定を長時間有効にしないようにお勧めします。ジョブ実行を一時停止した後、キューに登録されているジョブを完全に処理するために必要な時間を確保してから、サーバをシャットダウンしてください。

- 進行中のすべてのジョブを完了できます。
- それ以降にユーザが送信する新しいジョブはすべてキューに登録され、後で **[ジョブ実行を一時停止する(Pause jobs execution)]** チェックボックスをオフにすると実行されます。
- ジョブ実行が一時停止されたことをユーザに通知するためのバナーがFortify Software Security Centerに表示されます。



4. 次回サーバを起動したら、 **[保守(Maintenance)]** ページに戻って、 **[ジョブ実行を一時停止する(Pause job execution)]** チェックボックスをオフにしてから、 **[保存(SAVE)]** をクリックします。

参照情報

"Fortify Software Security Centerの保守モードへの移行" ページ188

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。カスタムルールを作成する方法については、『Fortify Static Code Analyzerカスタムルールガイド』を参照してください(Fortify Static Code Analyzer製品のダウンロードにのみ含まれています)。

  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。

  - "Fortify更新サーバからのルールパックの更新" 次のページ
  - "セキュリティコンテンツのインポート" ページ194
  - "ルールパックの削除" ページ195
  - "Rulepacksをエクスポートする" ページ194

- "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208

- 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208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外部メタデータを作成する方法については、『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196
  - "新しいマッピングの作成" ページ196

注: 最新のルールパックを使用することが重要です。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。

Fortify更新サーバからのルールパックの更新

最新のルールパックを使用することが重要です。最新のRulepackが確実にインストールされていることを確認したい場合は、それをFortifyサーバからインポートします。

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統合のプロキシの設定" ページ132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、OpenTextのヘッダで **管理(Administration)**]を選択します。
2. 左ペインの **[メトリックとトラッキング(Metrics & Tracking)**]で、 **[ルールパック(Rulepacks)**]を選択します。
3. **[ルールパック(Rulepacks)**]ページで、 **[サーバから更新(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208

"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" 下

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。
   OpenTextのヘッダで、 [**管理(Administration)**]をクリックします。
2. 左ペインの [**メトリックとトラッキング(Metrics & Tracking)**]で、 [**ルールパック(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" 次のページ

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。
   OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
2. 左ペインの **メトリックとトラッキング(Metrics & Tracking)**]で、 **ルールパック(Rulepacks)**]を選択します。
3. Rulepacks]ページで、 **MPORT**]を選択します。
4. MPORT 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。
   OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
2. 左ペインの **メトリックとトラッキング(Metrics & Tracking)**]で、 **ルールパック(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" 前のページ

"セキュリティコンテンツのインポート" ページ194

"Fortify更新サーバからのルールパックの更新" ページ193

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194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192

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194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192

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24.2.xにアップグレードするには、バージョン22.2.x、23.1.x、または23.2.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22.1.x以前がインストールされている場合は、まずバージョン22.2.x、23.1.x、または23.2.xにアップグレードしてから、バージョン24.2.xに移行することができます。

次の表は、Fortify Software Security Center 24.2.0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。

アップグレードパス Fortify Software Security Centerのバージョン
22.1.x (またはそれ以前) > 22.2.x > 23.1.x > 24.2.x
22.2.x > 24.2.x (直接)
23.1.x > 24.2.x (直接)
23.2.x > 24.2.x (直接)

注: Fortify Software Security Center バージョン24.2.xではJava 17が必要です。以前のバージョンでJava 11を使用している場合は、Fortify Software Security Center バージョン24.2.xにアップグレードする前にJavaバージョン17にアップグレードする必要があります。

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、『*OpenText™ 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。
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 Software Security Center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201を参照してください)。
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201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" ページ201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。 **重要** (Microsoft SQLデータベースのみ)Fortify Software Security Centerを新しいSQLデータベースバージョンに移行し、データベースのバックアップと復元が済んだら、現在Fortify Software Security Centerデータベースをホストしているエンジンを反映するよう、(SQL Server Management Studioから)互換性レベルを変更してください。
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`ファイルに含まれていません。Fortify

タスク	説明
	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172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。

Fortify Software Security Centerバージョン23.2.0以降にアップグレードする場合、マイグレーション中に、MySQLおよびSQL Serverデータベースのid列の`scan_issue`テーブルタイプがINTからBIGINTに変更される点に注意して、最大32bの整数制限に達しないようにする必要があります。

SQL Serverが`scan_issue`テーブルのID値を`DBCC CHECKIDENT`で負の数にリセットするための推奨回避策(`scan_issue, reseed, -2147483648`)をすでに適用している場合は、追加の手動マイグレーションステップを実行する必要があります。23.2.0へのマイグレーション後、ID値を正の数にリセットします。リセットは、`DBCC CHECKIDENT (scan_issue、RESEED)`というクエリを実行することで行えます。クエリを実行するユーザは、テーブルを含むスキーマの所有者か、sysadmin、db_owner、またはdb_ddladmin固定データベースロールを持っている必要があります。

MySQLデータベースをアップグレードする場合は、"MySQL 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63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。

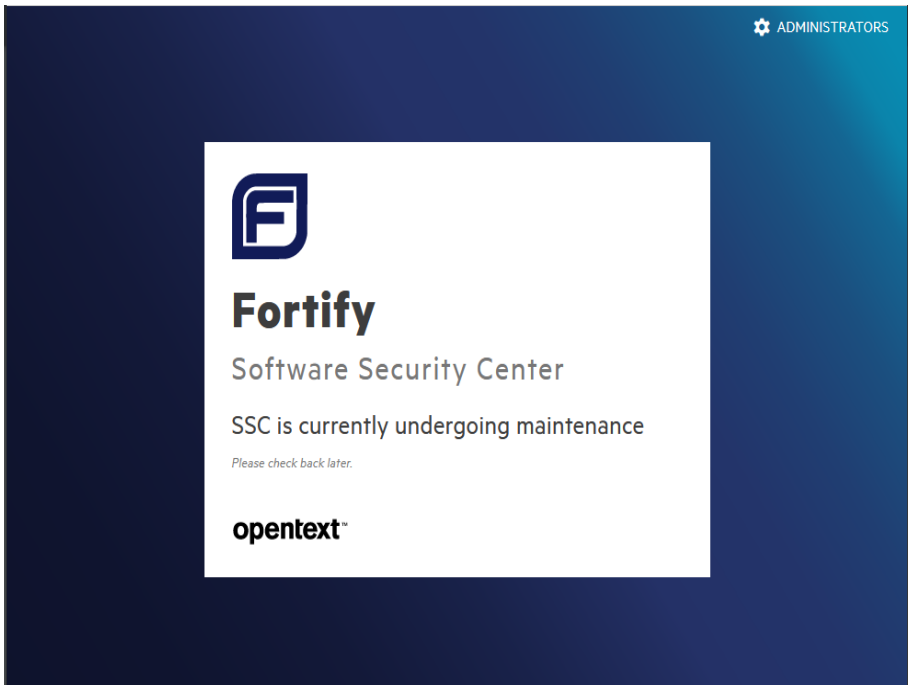
新しいWARファイルをデプロイしたら、セットアップウィザードのステップと 管理(Administration)]ビューでの設定タスクを完了します。詳細と手順については、"アップグレード後のFortify Software Security Centerの設定" 下および"追加のFortify Software Security Center設定" ページ80を参照してください。

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188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 **[トークン(TOKEN)]** フィールドに貼り付け、 **[サインイン(SIGN IN)]** をクリックします。
6. Fortify Software Security Centerセットアップウィザードの **[設定(CONFIGURATION)]** または **[コア設定(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70に記載されている手順に従って変更できます。
7. **[データベースセットアップ(DATABASE SETUP)]** ステップに達するまで **[次へ(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一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一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67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188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70

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バージョンのFortify Static Code AnalyzerおよびFortifyアプリとツールの使用可能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、『*OpenText™ Fortify Audit Workbenchユーザガイド*』を参照してください。

参照情報

"Fortify Static Code AnalyzerおよびFortifyのアプリとツールのAudit Workbenchからのアップグレードを有効化する" 下

Fortify Static Code AnalyzerおよびFortifyのアプリとツールのAudit Workbenchからのアップグレードを有効化する

新しいFortify Static Code AnalyzerおよびFortifyのアプリとツールのインストーラを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. Fortify Software Security Centerホストで、`<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。
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. Fortify_SCAまたはFortify_Apps_and_Toolsインストーラファイルを`<ssc_install_dir>/webapps/ssc/update-site/installers`ディレクトリにコピーします。
5. 次のようにして、`<ssc_install_dir>/webapps/ssc/update-site/installers`ディレクトリに、更新する製品の`update.xml file`を作成します。
   a. Static Code Analyzerの更新を有効にするには、次のXMLコードを使用します。

```
<installerInformation> <versionId>####</versionId> <version>##.##</version>
<platformFileList> <platformFile> <filename>Fortify_SCA_<version>_windows_
x64.exe</filename> <platform>windows-x64</platform> </platformFile>
```

```
<platformFile> <filename>Fortify_SCA_<version>_linux_x64.run</filename>
<platform>linux-x64</platform> </platformFile> <platformFile>
<filename>Fortify_SCA_<version>_osx_x64.app.zip</filename>
<platform>osx</platform> </platformFile> </platformFileList>
<downloadLocationList> <downloadLocation> <url>http://localhost:8080/update-
site/installers/</url> </downloadLocation> </downloadLocationList>
</installerInformation>
```

b. Fortifyアプリケーションとツールの更新を有効にするには、次のXMLコードを使用してupdate.xmlファイルを作成します。

```
<installerInformation> <versionId>####</versionId> <version>##.##</version>
<platformFileList> <platformFile> <filename>Fortify_Apps_Tools_<version>_
windows_x64.exe</filename> <platform>windows-x64</platform> </platformFile>
<platformFile> <filename>Fortify_Apps_Tools_<version>_linux_
x64.run</filename> <platform>linux-x64</platform> </platformFile>
<platformFile> <filename>Fortify_Apps_Tools_<version>_osx_
x64.app.zip</filename> <platform>osx</platform> </platformFile>
</platformFileList> <downloadLocationList> <downloadLocation>
<url>http://localhost:8080/update-site/installers/</url> </downloadLocation>
</downloadLocationList> </installerInformation>
```

6. Tomcatサーバを再起動します。

これで、Audit Workbenchのユーザは、新しいバージョンのFortify Static Code Analyzerおよびアプリケーションとツール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。

Fortify Audit Assistantの設定の更新

Fortify Software Security Centerをバージョン23.2.0以降にアップグレードしたら、Fortify Audit Assistant 23.2.0以降と連携できるように設定を行う必要があります。Fortify Audit Assistantでは第2世代の(G2)予測エンジンが追加されており、Fortify Software Security Center 23.2.0以降ではこれを使用する必要があります。

Fortify Audit AssistantへのFortify Software Security Center接続を更新するには:

1. G2予測ポリシーを1つ以上作成します。詳細については、"予測ポリシーの定義" ページ382を参照してください。

   注: Fortify Audit Assistant 23.2.0より前のバージョンで作成された予測ポリシーは使用できません。Fortify Software Security Centerをバージョン23.2.0以降にアップグレードすると、第1世代(G1)のポリシーは使用できなくなります。それら

はアップグレード中に削除されます。G2エンジンで動作する新しい予測ポリシーを作成する必要があります。

2. OpenTextのヘッダで、 **管理(Administration)]** をクリックします。
3. 左ペインで、 **設定(Configuration)**] をクリックして、 **[Audit Assistant**] をクリックします。

   [Audit Assistant] ページが表示されます。
4. **[Audit Assistantを有効にする(Enable Audit Assistant)**] チェックボックスをオンにします。
5. **[ポリシーの更新(Refresh Policies)]** ボタンをクリックし、設定を保存します。

   Audit Assistantが正しく設定されると、 [Audit Assistantのポリシーの更新(AUDIT ASSISTANT REFRESH POLICIES)] ウィンドウが表示され、「更新に成功しました(Refresh was successful)」というメッセージが表示されます。これで、SSCのすべての予測ポリシーが一貫します。 **[OK**] をクリックします。
6. [デフォルトの予測ポリシー(Default prediction policy)] ボックスで、デフォルトとして使用するポリシーを選択します。予測ポリシーをアプリケーションバージョンに割り当てない場合、ここで選択したデフォルトが使用されます。 **[保存(SAVE)**] をクリックします。
7. (オプション)アプリケーションバージョンレベルで予測ポリシーを設定できるようにするには、 **[特定のアプリケーションバージョンのポリシーを有効にする(Enable specific application version policies)**] チェックボックスをオンにします。
8. (オプション)プロジェクト内の未監査の問題にFortify Audit Assistantで予測を自動的に適用するには、 **[自動予測を有効にする(Enable auto-prediction)**] チェックボックスをオンにします。
9. (オプション)Fortify Audit Assistantで予測値をカスタムタグに自動的に適用するには、 **[自動適用を有効にする(Enable auto-apply)**] チェックボックスをオンにします。

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、「*Fortifyソフトウェアシステム要件*」ドキュメントを参照してください。

期限切れになった年間ライセンスを更新するには:

1. Tomcatサーバを停止します。
2. ダウンロードした`fortify.license`ファイルを<*fortify.home*>ディレクトリに配置します。
3. Tomcatサーバを再起動します。

四半期ごとにリリースされるセキュリティコンテンツ

OpenText Fortifyでは、新しいセキュリティコンテンツをダウンロードできるようになると、ユーザに通知します。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192

"Fortify更新サーバからのルールパックの更新" ページ193

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

OpenText Fortifyでは、新しいセキュリティコンテンツをダウンロードできるようになると、ユーザに通知します。この更新されたコンテンツに新しいシードバンドルが含まれるかどうかを確認するには、通知ドキュメントの見出し「**OpenText™ Security Fortify Premium Content**」の下を確認します。このセクションには、新しいシードバンドルの存在に関する情報が含まれています。新しいシードバンドルが含まれている場合は、それを使用してデータベースを再シードできます。シードバンドルとデータベースのシード処理の詳細については、"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. カスタマサポートポータル(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

Part II: Fortify 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 211
セキュリティ管理ワークフロー 212
ユーザアカウントとアクセス 213
Active Directory/LDAPの統合 213
初めてのFortify Software Security Centerへのログイン 213
Fortify Software Security Centerへのアクセス権の要求 214
パスワードの変更 216
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 218
Fortify Software Security Centerダッシュボードについて 219
[Issue Stats] ページ 219
データをカンマ区切り値ファイルへエクスポートする 222
Fortify Software Security Center APIドキュメントへのアクセス 225
Fortify Software Security Centerのキーボードホットキーの表示 226

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、監査、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

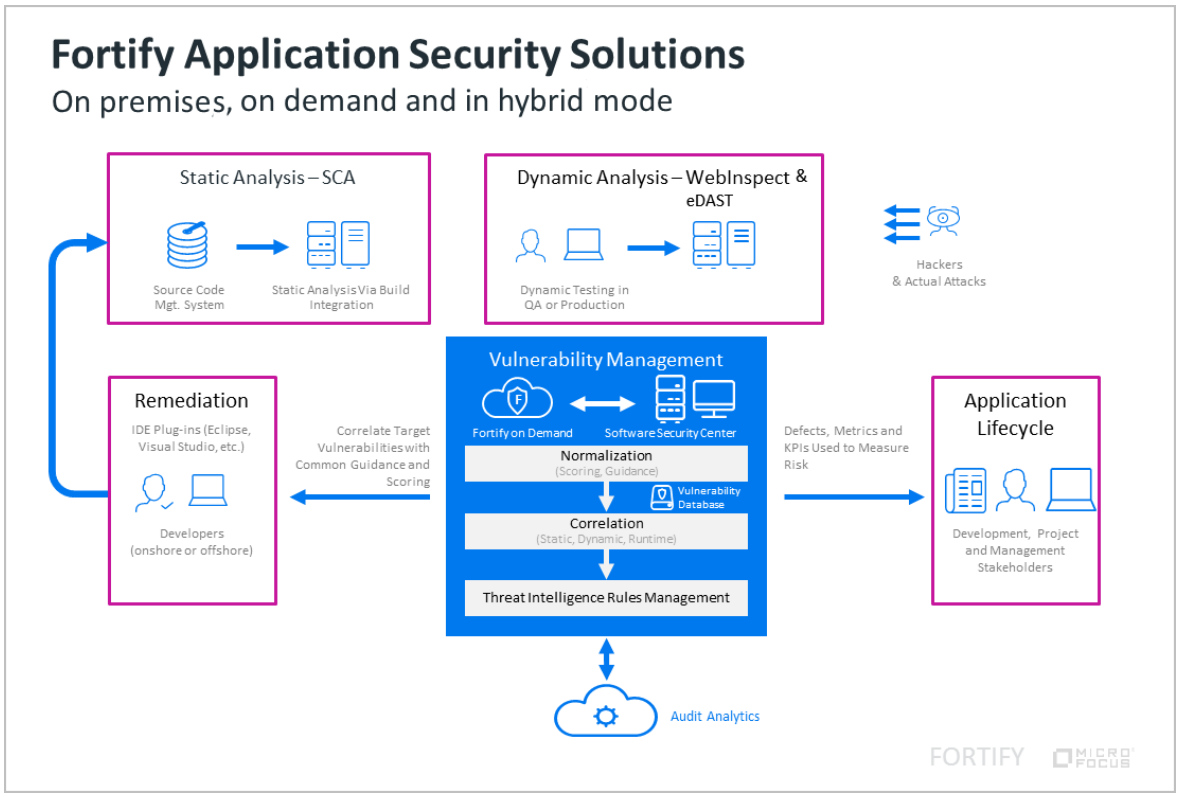
- 既存の脆弱性を修正し、ベースラインを下げる
- コードが内部および外部のセキュリティ指令を遵守するようにする

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 213
初めてのFortify Software Security Centerへのログイン 213
Fortify Software Security Centerへのアクセス権の要求 214
パスワードの変更 216
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 218

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111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122

"Fortify Software Security Centerのユーザアカウント管理" ページ227

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:

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/`

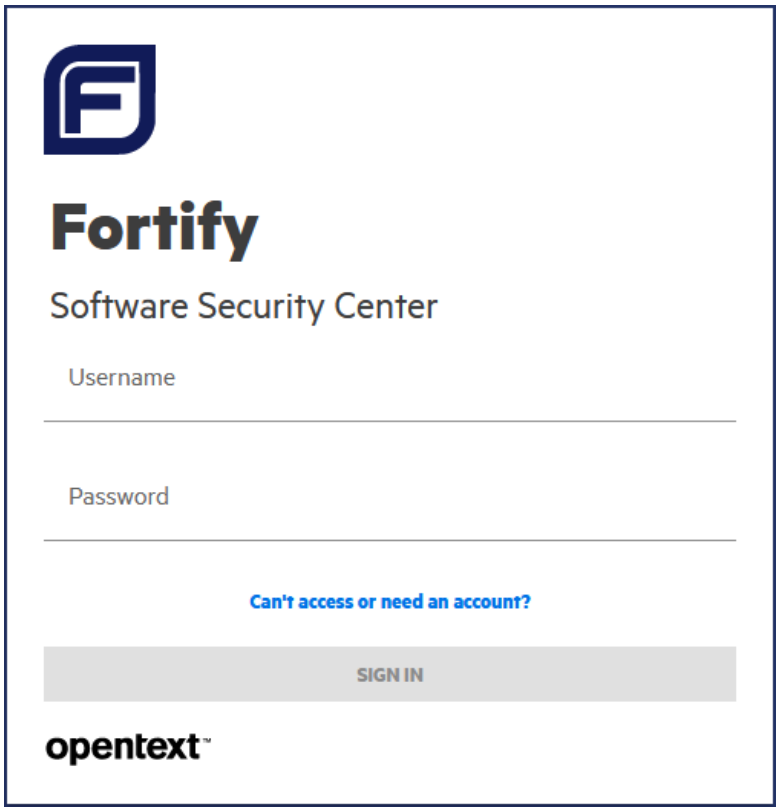
     ここで`<port>`は、Tomcatサーバが使用するポート番号を表します。
3. [**Username**]および[**Password**]ボックスに、管理者から与えられた資格情報を入力します。
4. [**LOGIN**]をクリックします。
5. Fortify Software Security Centerでパスワードの変更を求めるプロンプトが表示される場合は、パスワードを変更します。手順については、"パスワードの変更" ページ 216を参照してください。

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。

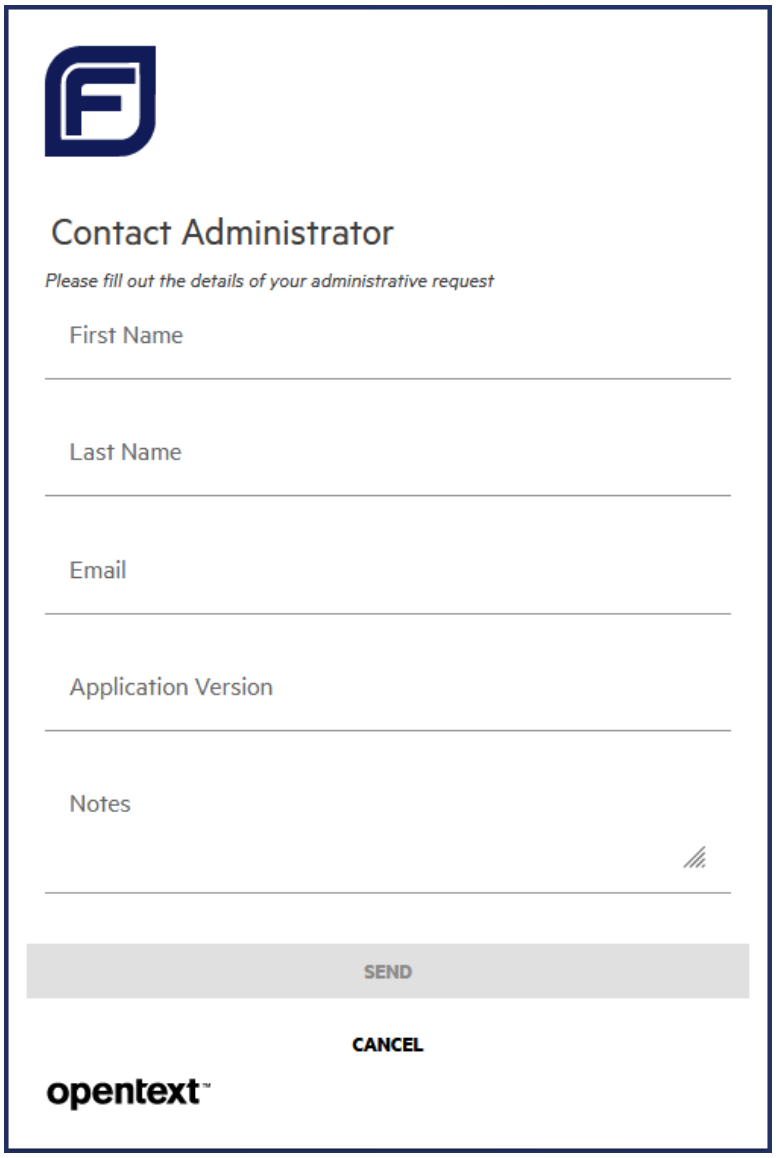
Fortify Software Security Centerへのアクセスを要求するには、次の手順に従います。

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 **[アクセスできないか、アカウントが必要ですか? (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、 **送 信 (SEND)**] をクリックします。

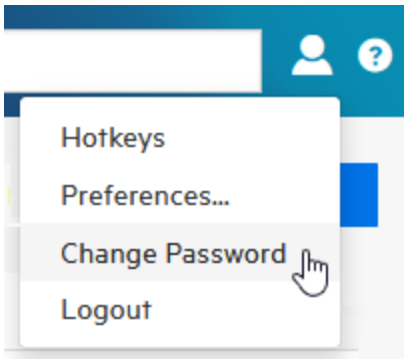
Fortify Software Security CenterからFortify Software Security Center管 理 者 に要 求 が送 信 されます。

パスワードの変 更

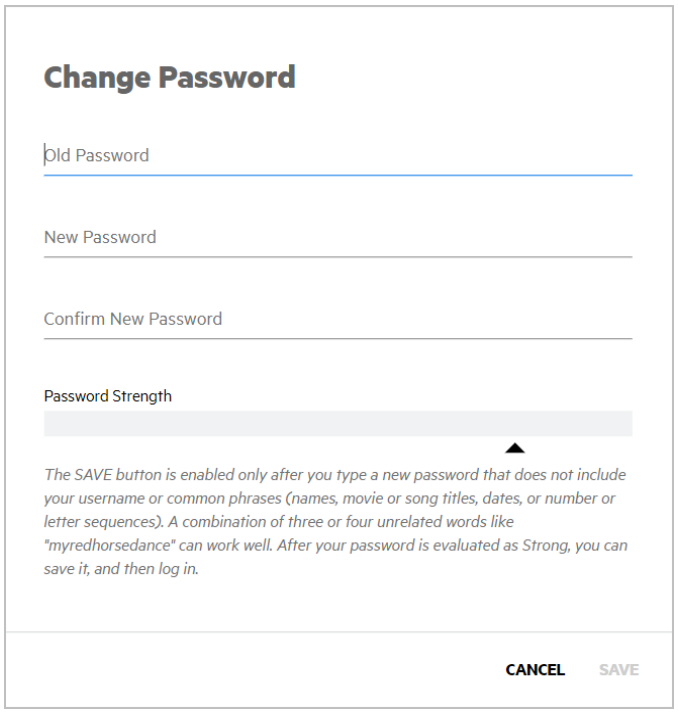
次 の手 順 では、パスワードを変 更 する方 法 について説 明 します。ローカルアカウントを使 用 してログオンしている場 合 のみ、パスワードを変 更 できます。

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. OpenText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、[**パスワード変更**]を選択します。



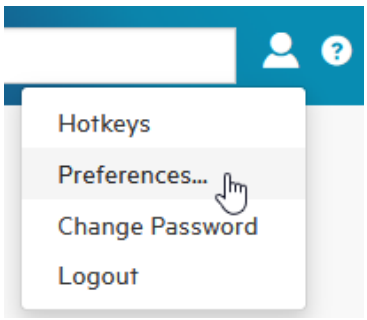
[パスワード変更(Change Password)]ダイアログボックスの[**保存(Save)**]ボタンは、ユーザ名や一般的なフレーズ(名前、映画や楽曲のタイトル、日付、または数字や文字のシーケンス)を含まない強力な新しいパスワードを入力した後にのみ有効になります。「myredhorsedance」のように無関係な単語を3から4つ組み合わせて使用すると、うまく機能します。パスワードが強力であると評価されると、パスワードを保存してからログインできます。

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。

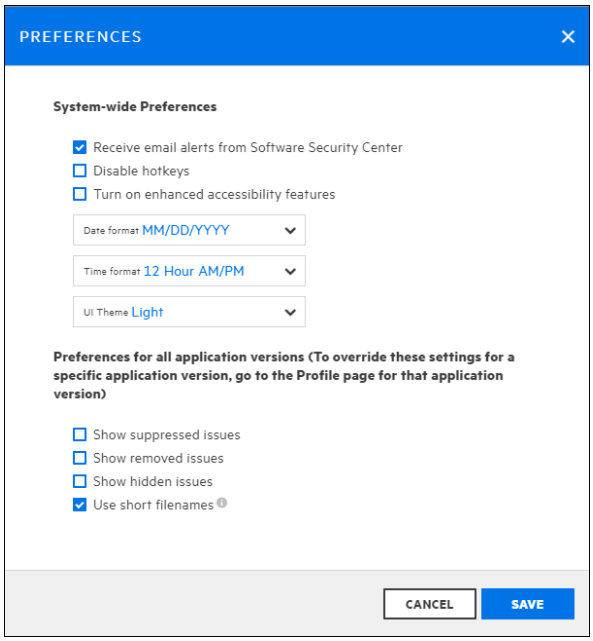
環境設定: システム全体とアプリケーションバージョン間

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. OpenText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てから、 **環境設定(Preferences)**]を選択します。



2. システム全体に適用する環境設定を行うには、 **[環境設定(PREFERENCES)]**ダイアログボックスの **[システム全体の環境設定(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日付フォーマットではなくYYYY/MMDD日付フォーマットを適用するには、それを **[日付フォーマット(Date format)]**リストから選択します。
   c. デフォルトの12時間AM/PMフォーマットではなく24時間フォーマットを適用するには、それを **[時刻フォーマット(Time format)]**リストから選択します。

d. テーマを変更するには、 [UIテーマ(UI Theme)] 一覧から、 [ライト(Light)] 、 [ダーク(Dark)] 、 [自動(Automatic)] のいずれかを選択します。

注: [自動(Automatic)] テーマを適用する場合、UIテーマはオペレーティングシステムまたはブラウザテーマに基づいて設定されます。

3. すべてのアプリケーションバージョンの環境設定を設定するには、次の手順に従います。

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 [アプリケーションプロファイル(APPLICATION PROFILE)] ダイアログボックスに移動します。

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:

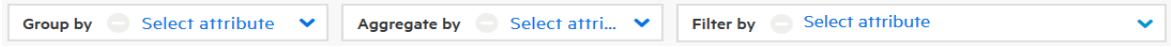
[Issue Stats] ページ 219
データをカンマ区切り値ファイルへエクスポートする 222
Fortify Software Security Center APIドキュメントへのアクセス 225
Fortify Software Security Centerのキーボードホットキーの表示 226

[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。

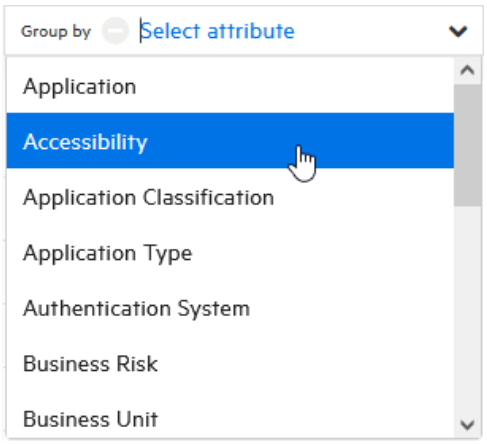
注: 管理者またはセキュリティリードの場合は、[Issue Stats] ページの情報を確認するときにユーザに表示される情報を決定するしきい値を設定できます。詳細については、"問題統計しきい値の設定" ページ81を参照してください。

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

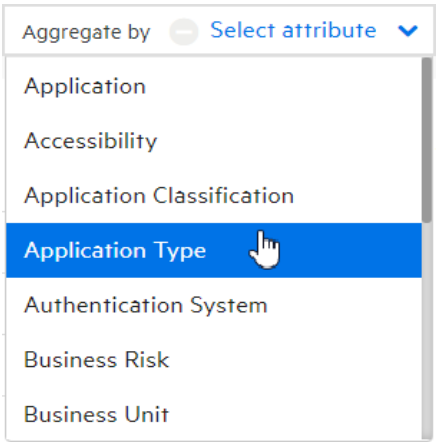


単一のアプリケーションバージョン属性に基づいてデータをグループ化するには、[Group by] リストから属性を選択します。(デフォルトのグループ化属性はアプリケーションバージョンです)。

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244を参照してください。

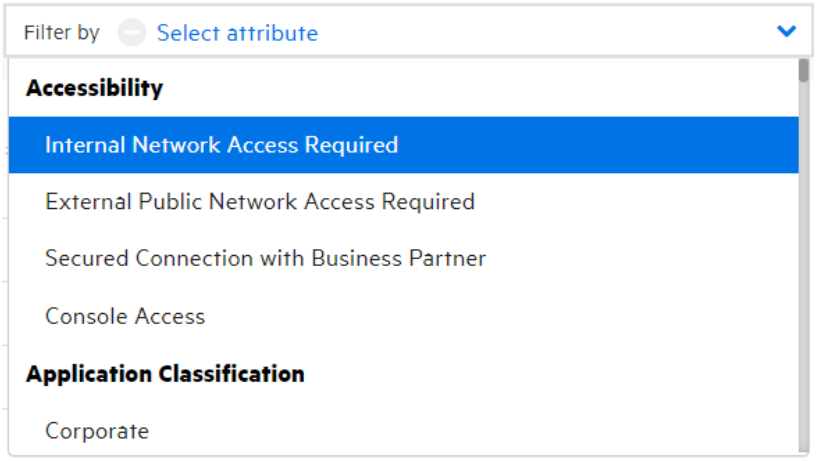
集計属性の選択



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244を参照してください。

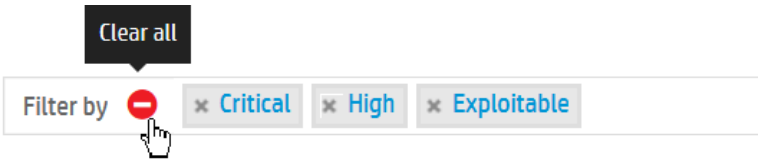
1つ以上のフィルタ属性の選択



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. OpenTextのヘッダで、 **[ダッシュボード(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。

3. **[CSVのエクスポート(EXPORT CSV)]**ダイアログボックスの **[ファイル名(File Name)]**ボックスに、ファイルの名 前を入 力します。
4. (オプション) **[ノート(Notes)]**ボックスに、エクスポートするデータに関する情 報を入 力します。
5. **[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. OpenTextのヘッダで、 **[レポート(Reports)]**をクリックします。
   b. **[データエクスポート(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。

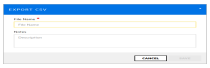
CSVファイルが削 除されるまで保 持される期 間を決 定するには、"ジョブスケジューラの設 定" ページ135に記 載されている手 順を参 照してください。

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

[ダッシュボード(Dashboard)]の[問題統計(ISSUE STATS)]タブまたは[監査(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:

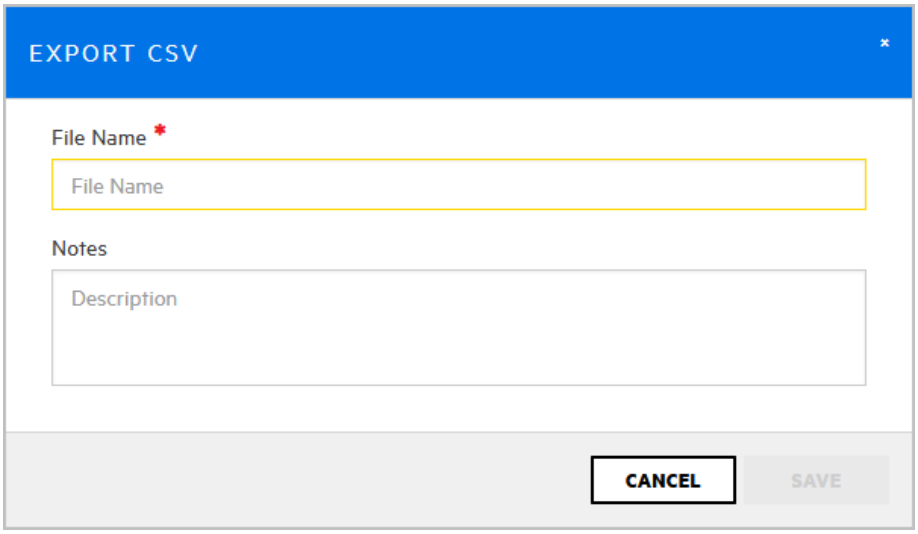
1. (オプション)[問題統計(Issue Stats)]ページからデータをエクスポートする場合は、集約またはフィルタに使用する属性を選択できます。[AUDIT]ページで、フィルタの適用に使用する属性を選択できます。

   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。

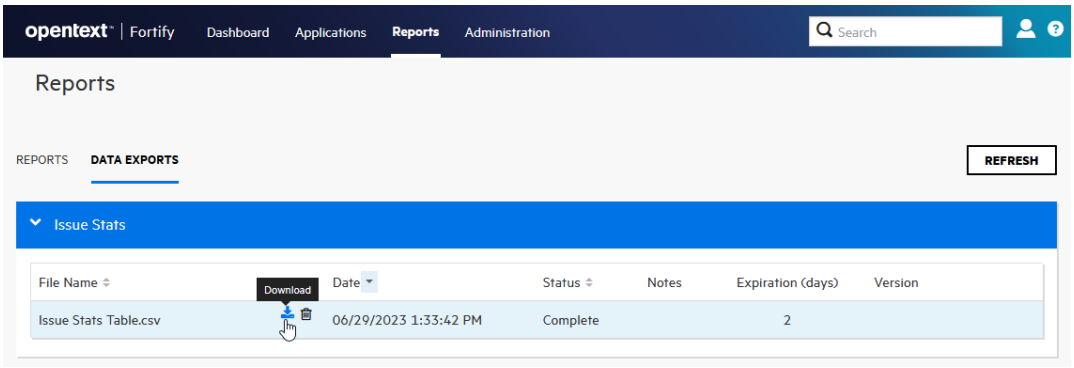
   

2. ツールバーで[EXPORT]をクリックします。

   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。

3. [CSVのエクスポート(EXPORT CSV)]ダイアログボックスの[ファイル名(File Name)]ボックスに、ファイルの名前を入力します。
4. (オプション)[ノート(Notes)]ボックスに、エクスポートするデータに関する情報を入力します。
5. [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. [レポート(Reports)]をクリックします。
   b. [データエクスポート(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。

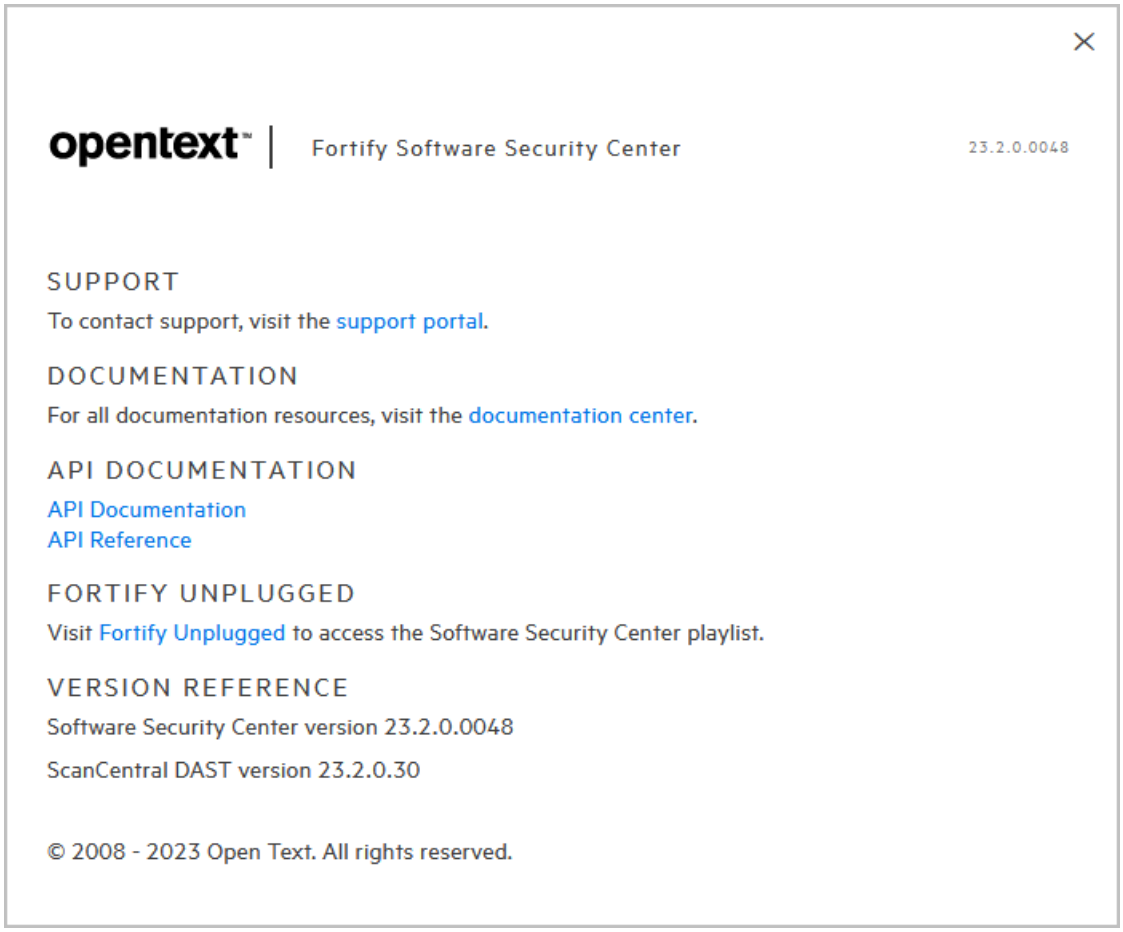
CSVファイルは **ダウンロード**] フォルダに保 存されます。

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135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. OpenTextのヘッダで、ヘルプアイコンをクリックします。



2. **[Fortify Software Security Center <version>について(About Fortify Software Security Center <*version*>)]ボックスで、 [APIドキュメント(API Documentation)]リンクをクリックします。**

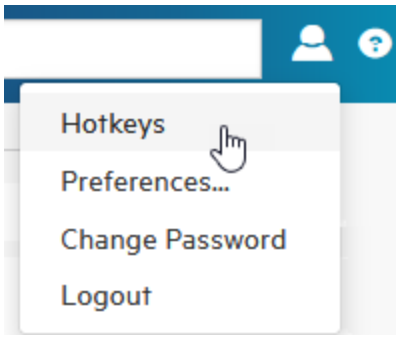
[FORTIFY SOFTWARE SECURITY CENTER APIドキュメント <version> (FORTIFY SOFTWARE SECURITY CENTER API DOCUMENTATION VERSION <*version*>)]Webページが開きます。

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のキーボード ホット キーの表 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 ホット キーを表 示 するには:

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。
   - OpenText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、 **ホット キー (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218

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 Entra ID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184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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで[管理(Administration)]をクリックします。
2. 左ペインで、[ユーザ(Users)]、[役割(Roles)]の順に選択します。
3. [役割(Roles)]ツールバーで、[新規(NEW)]をクリックします。
4. [新しい役割の作成(CREATE NEW ROLE)]ダイアログボックスで、次の表に示す情報を入力します。

重要 [名前(Name)]フィールドと[説明(Description)]フィールドの値は、文字=、-、+、または@で始めることはできません。また、制御文字を含めることはできません([説明(Description)]フィールドの改行を除きます)。制限されている範囲に含まれているUnicode文字の完全なリストについては、https://www.aivosto.com/articles/control-characters.htmlを参照してください。

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。
6. [許可の追加(ADD PERMISSIONS)]ダイアログボックスで、テーブルをスクロールし、新しい役割に付与する許可に対応するチェックボックスをオンにします。
7. [終了(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. 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、 [管 理(Administration)] をクリックします。
2. 左 ペインで、 [ユーザ(Users)] 、 [役 割(Roles)] の順に選 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228

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 230
ローカルユーザアカウントを編 集する 233
ローカルユーザアカウントのロック解 除 235
外 部 管 理されたユーザおよびグループを表 示する 236

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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで[**管理(Administration)**]をクリックします。
2. 左ペインで、[**ユーザ(Users)**]、[**ローカルユーザ(Local Users)**]の順に選択します。
   [**ローカルユーザ(Local Users)**]ページには、ローカルユーザが一覧表示されます。
3. [**ローカルユーザ(Local Users)**]ツールバーで、[**+追加(+ADD)**]をクリックします。
4. [新しいユーザの作成(CREATE NEW USER)]ダイアログボックスで、次の表に示す情報を入力します。

重要 次の表でアスタリスク(*)で示されているフィールドの値は、文字=、-、+、または@で始めることはできません。また、制御文字を含めることはできません。

フィールドまたはチェックボックス	説明
*ユーザ名(Username)	Fortify Software Security Centerログオン用のユーザ名。
*名(First Name)	(オプションですが、強く推奨)ユーザの名。
*姓(Last Name)	(オプションですが、強く推奨)ユーザの姓。
*電子メール(Email)	(オプション)ユーザの電子メールアドレス。 **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。

フィールドまたはチェックボックス	説明
User must change password at next login	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。
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

フィールドまたはチェックボックス	説明
	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。 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

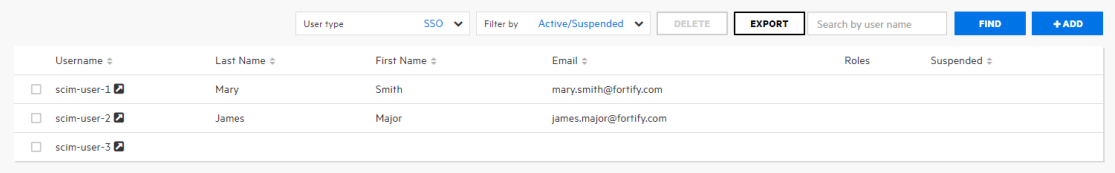
"ローカルユーザアカウントのロック解 除" ページ235

ローカルユーザアカウントを編 集 する

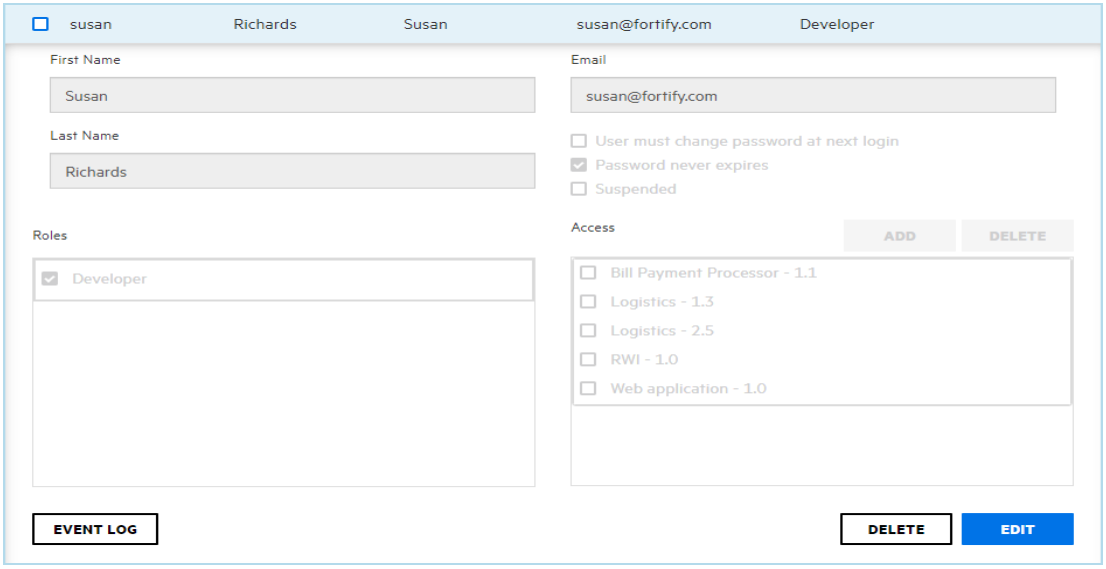
次 の手 順 では、Fortify Software Security Centerから作 成されたローカルユーザアカウントと、SCIM APIを使 用してプロビジョニングされたユーザアカウントのアカウントを編 集 する方 法について説 明します。

ローカルユーザアカウントを編 集 するには:

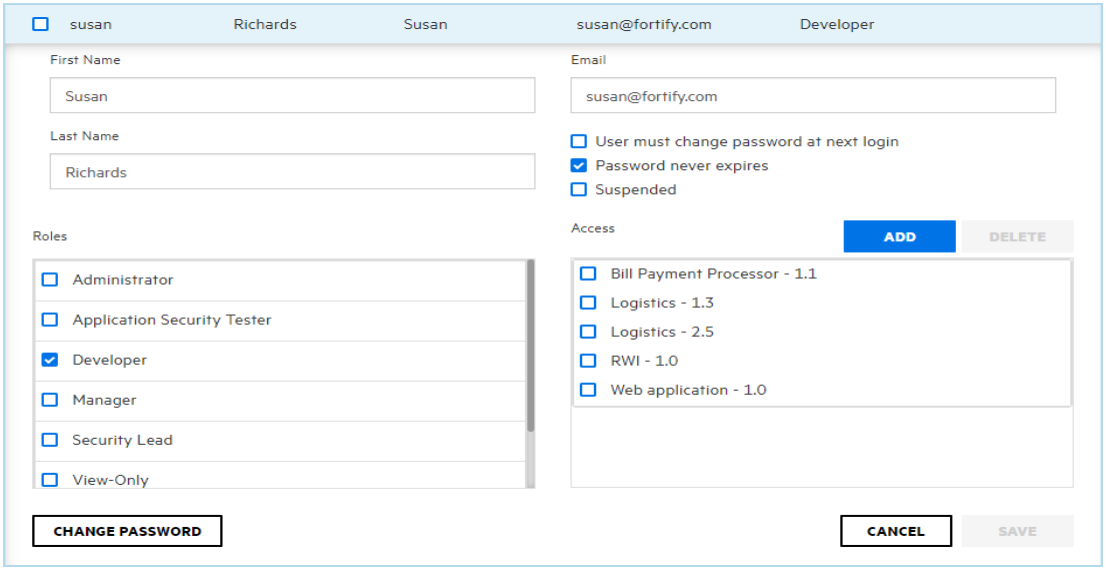
1. OpenTextのヘッダで、 [管 理(Administration)] を選 択します。
2. 左 ペインで、 [ユーザ(Users)] を選 択してから、 [ローカルユーザ(Local Users)] をクリックします。
3. 外 部で管 理されている(SCIM APIを使 用してプロビジョニングされた)ユーザを選 択的に表 示するには、 [ユーザタイプ(User type)] メニューから [SSO] を選 択します。



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　名 (First Name)】、 姓 (Last Name)】、および 電 子メール(Email)】フィールドの値 は、文 字 =、-、+、または@で始 めることはできません。また、制 御文 字を含 めることはできません。制 限されているこれらの範 囲に含 まれているUnicode文 字の完 全なリストについては、https://www.aivosto.com/articles/control-characters.htmlを参 照してください。

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、役割とアプリケーションバージョンの割り当てのみです。他のすべての設定(および削除)は、Entra IDから行う必要があります。

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、 **電子メール(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(Roles)**] セクションで、選択可能な役割のチェックボックスをオンまたはオフにします。
9. アプリケーションバージョンからユーザを削除するには、 **アクセス(Access)**] 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、 **削除(DELETE)**] をクリックします。ユーザを別のアプリケーションバージョンに割り当てるには、 **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230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230

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. OpenTextのヘッダで、 **管理(Administration)**] を選択します。
2. 左ペインで、 **ユーザ(Users)**] を選択してから、 **ローカルユーザ(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たら、 **ユーザのロック解除(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230

"ローカルユーザアカウントを編 集する" ページ233

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. OpenTextのヘッダで、 [管 理(Administration)]をクリックします。
3. 左 ペインで、 [ユーザ(Users)]、 [ローカルユーザ(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。

Entra ID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. OpenTextのヘッダで、 [管 理(Administration)]を選 択し、 [ユーザ(Users)]、 [ローカルグループ(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

Entra IDなどのアイデンティティ管 理サービスからプロビジョニングされたローカルグループのユーザまたはメンバーは、そのグループに1つ以 上の役 割が割り当 てられていない場 合や、 [ローカルユーザ(Local Users)]ページからユーザに個 別に役 割が割り当 てられていない場 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 割とアプリケーションバージョンの割り当 てのみです。他 のすべての設 定(および削 除)は、Entra ID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、 [管 理(Administration)]ビューで作 成したローカルユーザへ割り当 てるのと同じように行います。

参照情報

"SCIM 2.0プロトコルの実 装" ページ127

"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132

"SCIM 2.0およびSAML 2.0を使 用したユーザプロビジョニング用 のMicrosoft Entra IDへの接 続 の設 定 " ページ129

"SAML 2.0準 拠 の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150

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 240
アプリケーション作成プロセスについて 240
アプリケーションバージョンを作成するための戦略 241
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 242
Fortify Software Security Centerアプリケーションリストの表示 242
アプリケーションバージョンの作成について 242
アプリケーションバージョン属性 242
問題テンプレートについて 251
新しいアプリケーションの最初のバージョンの作成 253
アプリケーションに新しいバージョンを追加する 256
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 260
[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 263
アプリケーション概要ページの更新 263
アプリケーションバージョンの詳細を編集する 263
アプリケーションバージョンをデフォルトのデータ保持ポリシーからオプトアウトするための設定 264
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 264
バグトラッカの設定 265
バグ報告用Velocityテンプレート 266
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 269
単一の問題のバグの送信 271
複数の問題のバグの送信 272
バグ状態管理 273
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 273
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 275
インスタンスIDマイグレーションに影響する処理ルールについて 280
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 281
カスタムタグ 282
システムへのカスタムタグの追加 283
カスタムタグ属性の変更 286
カスタムタグをグローバルで非表示にする 286
カスタムタグの削除 286
カスタムタグ値の追加 287
カスタムタグを編集する 293

カスタムタグ値の削除 293
カスタムタグと問題テンプレートを関連付ける 294
問題テンプレートからのカスタムタグの削除 294
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 295
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 297
問題テンプレートによるカスタムタグの管理 297
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 298
データ保持について 298
データ保持の有効化 298
デフォルトのデータ保持ポリシーの編集 302
アプリケーションバージョンの削除について 303
アプリケーションバージョンの無効化 303
アプリケーションバージョンの再有効化 304
アプリケーションバージョンの削除 305

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 240
アプリケーションバージョンを作成するための戦略 241
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 242
Fortify Software Security Centerアプリケーションリストの表示 242

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" 次のページ

参照情報

"テンプレートの選択" ページ252

"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253

"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256

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303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。

- OpenTextのヘッダで、 **[アプリケーション(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 263

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240

"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253

"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256

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、 新しいバージョンの作成(CREATE NEW VERSION)] ウィザードの指示に従って、技術、組織、ビジネス、および Scancentral DAST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
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

ScanCentral DAST属性	
ベースURL(Base URL)	アプリケーションのすべてのページの先頭に付くURLプレフィックス。相対パスを確立するのに役立ちます。

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。

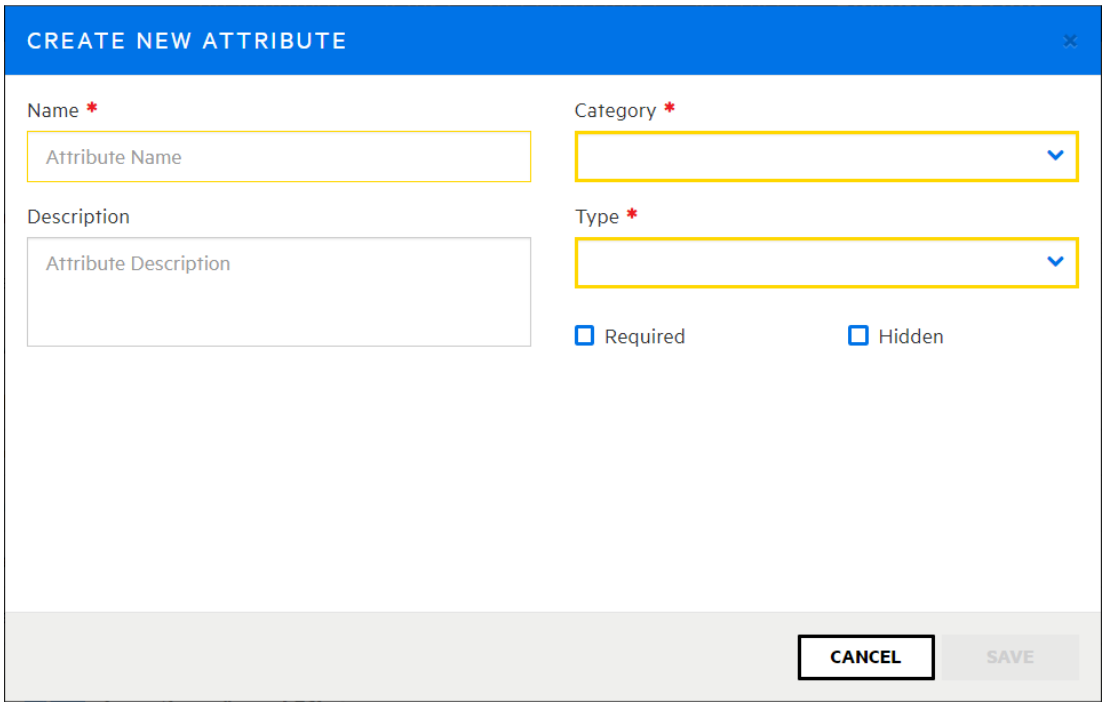
注: カスタム属性は、管理者またはセキュリティリードのユーザアカウントを持っている場合にのみ作成できます。

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. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
3. 左ペインの **テンプレート(Templates)**]で、 **属性(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。



5. [新しい属性の作成 (CREATE NEW ATTRIBUTE)] ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明
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

フィールド	説明
	す。 **注意** CREATE NEW APPLICATION VERSIONウィザード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

フィールド	説明
	選択します。 **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250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225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242

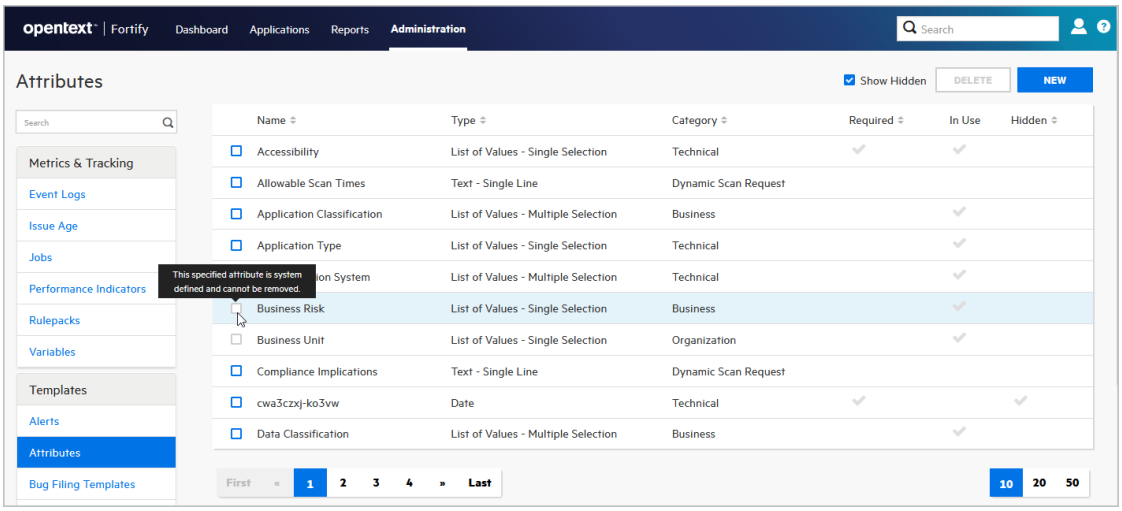
属性と属性値の削除

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。

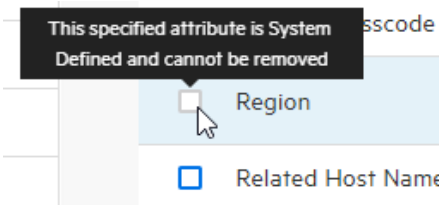
属性の削除

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. OpenTextのヘッダで、 [**管理(Administration)**] を選択します。
2. 左ペインで、 [**テンプレート(Templates)**] セクションを展開し、 [**属性(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。

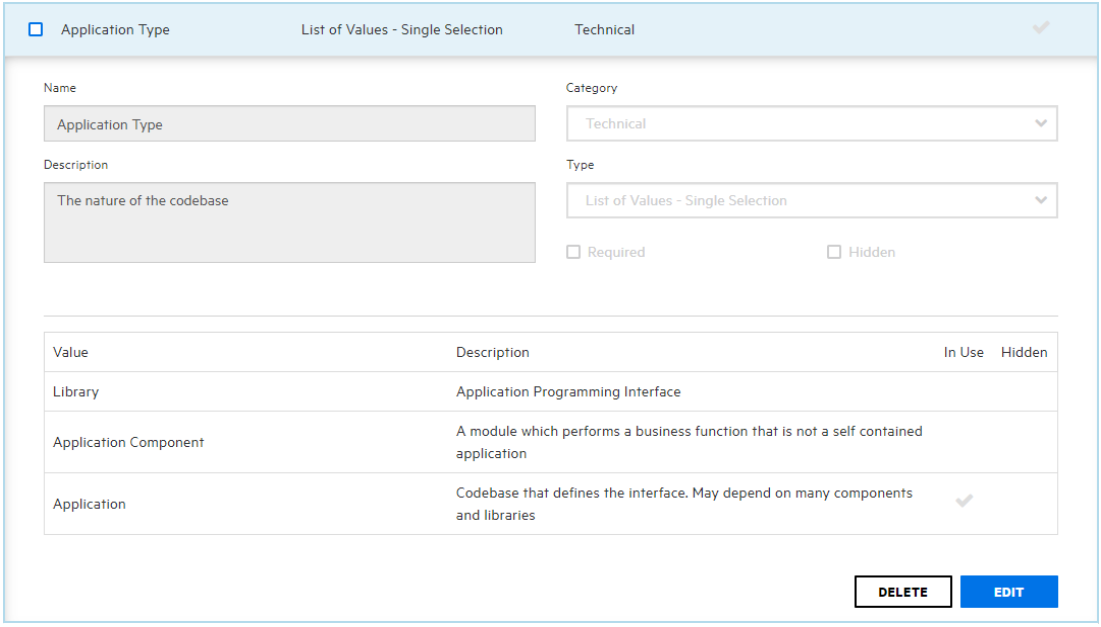
注 : デフォルトでは、Fortify Software Security Centerユーザインタフェースから作成した属性は削除可能です。Fortify Software Security Center APIを使用して、削除不可属性を定義できます。このAPIにアクセスする方法については、"Fortify Software Security Center APIドキュメントへのアクセス" ページ225を参照してください。

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. OpenTextのヘッダで、 **[管理 (Administration)]** を選択します。
2. 左ペインで、 **[テンプレート (Templates)]** セクションを展開し、 **[属性 (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。

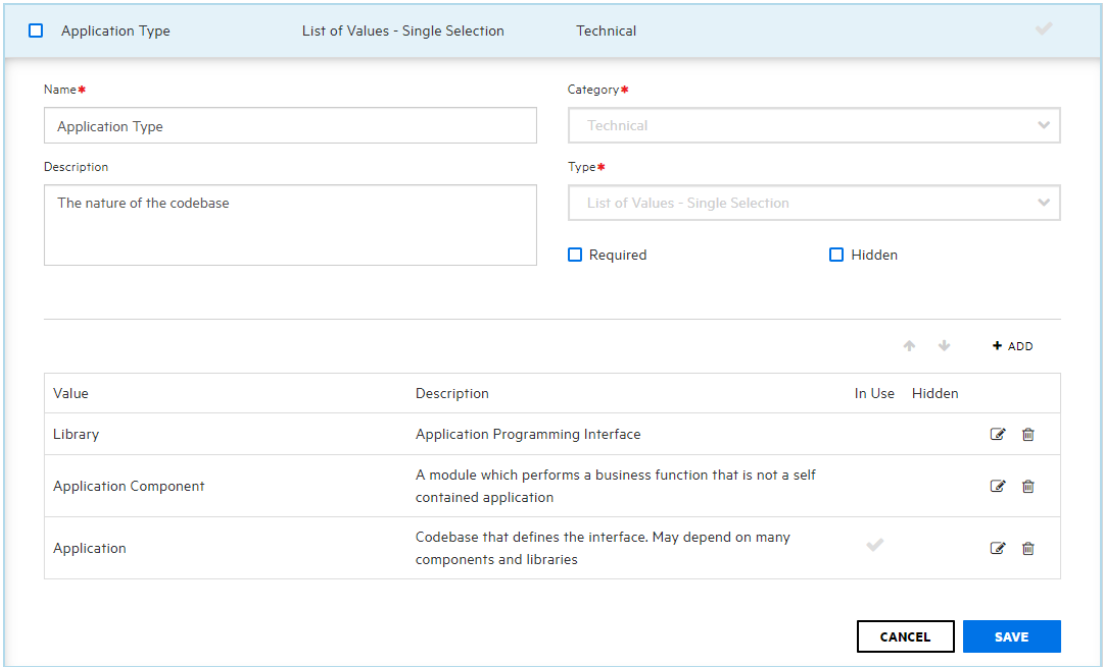


[In Use] 列には、現在1つ以上のアプリケーションバージョンで使用されている値が表示されます。

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244

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. OpenTextのヘッダで、 [アプリケーション(Applications)]を選択します。
2. [アプリケーション(Applications)]ビューで、アプリケーションの行を展開し、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。
6. [ステップ1. 一般(Step 1. GENERAL)]([バージョンの編集(EDIT VERSION)]ウィザード内)で、 [次へ(NEXT)]をクリックします。
7. [ステップ2. 属性とリスクの定義(Step 2. DEFINE ATTRIBUTES AND RISK)]で、属性カテゴリ([技術属性(Technical Attributes)]、 [組織属性(Organization Attributes)]、または [ビジネスリスク属性(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. ウィザードのステップ4に移動し、 [完了(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244

"アプリケーションバージョンの詳細を編集する" ページ263

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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **テンプレート(Templates)**]を選択して、 **問題(Issue)**]を選択します。

[ssue]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。

メモ: Fortify Audit Workbenchでフィルタセットやフォルダを編集または作成する場合、Fortify Audit WorkbenchとFortify Software Security Centerによって使用される検索修飾子で、生成される結果が異なる場合があります。検索式に基づくすべての検索、フィルタ、またはフォルダが同じ結果を生成するとは限りません。たとえば、検索式にOWASPやCWEなどの外部メタデータカテゴリが含まれている場合、Fortify Software Security CenterとFortify Audit Workbenchでは式が異なる場合があるため、結果が一致しないことがあります。一致する外部カテゴリが複数ある場合、Fortify Software Security Centerではそれらのいずれかと一致しますが、Fortify Audit Workbenchではすべての外部カテゴリとの完全一致を期待します。Fortify Software Security Centerで使用する問題テンプレートを編集または作成する際にこの問題が発生した場合は、カスタマサポートにお問い合わせください。

Fortify Audit Workbenchで問題テンプレートを変更または作成する方法については、*『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. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
3. 左側のペインで、 **テンプレート(Templates)**]を選択してから、 **問題(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。
5. 新しい問題テンプレートの作成(CREATE NEW ISSUE TEMPLATE)]ダイアログボックスの **名前(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) **説明(Description)**]ボックスに、テンプレートの使用方法をユーザに知らせる説明を入力します。
7. **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\: Vulerable 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。
3. [新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)] ウィザードの [一般(GENERAL)] タブで、次の表に示す情報を入力します。

重要 次の表でアスタリスク(*)で示されているフィールドの値は、文字=、-、+、または@で始めることはできません。また、制御文字を含めることはできません。制限されているこれらの範囲に含まれているUnicode文字の完全なリストについては、https://www.aivosto.com/articles/control-characters.htmlを参照してください。

フィールド	説明
アプリケーションのセットアップ(Application Setup)	
*アプリケーション名 (Application name)	(必須)アプリケーション名を入力します。
アプリケーションの説明 (Application description)	(オプション)新しいアプリケーションの説明を入力します。
バージョンのセットアップ(Version Setup)	
*バージョン名 (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	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

フィールド	説明
application version	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4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。

4. [NEXT] をクリックして、 [ATTRIBUTES] 設定に進みます。
5. [TECHNICAL ATTRIBUTES] タブで、次の表に示す情報を入力します。

フィールド	説明
Development Phase	[新規 (New)] を選択します。
Development Strategy	アプリケーションバージョンの開発に使用する戦略を選択します。
Accessibility	アプリケーションへのアクセス方法を指定する値を選択します。
Application Type	アプリケーションタイプを選択します。

フィールド	説明
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。

6. (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。
7. (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。
8. (オプション)Fortify ScanCentral DASTを使用している場合は、 [SCANCENTRAL DASTの属性(SCANCENTRAL DAST ATTRIBUTES)] タブをクリックして、次の操作を行います。
   a. [ベースURL] を入力して、アプリケーション内のすべてのページのプレフィックスを設定します。

   [テンプレート(TEMPLATE)] 設定に進むには、 [次へ(NEXT)] をクリックします。
9. [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。
10. [ACCESS] タブに進むには、 [NEXT] をクリックします。

11. 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。

12. [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[アプリケーション(Applications)]ビューに表示されます。そのアプリケーションバージョンのデータがアップロードされると、[ダッシュボード(Dashboard)]ビューにも表示されます。
13. [閉じる(CLOSE)]をクリックします。

注 : 新しいアプリケーションは、その分析結果(アーティファクト)をアップロードするまでダッシュボードに表示されません。ただし、[アプリケーション(Applications)]ビューには表示されます。アプリケーションバージョンのアーティファクトをアップロードする方法については、"スキャンアーティファクトのアップロード" ページ327を参照してください。

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。
3. [新しいアプリケーションバージョンの作成(CREATE NEW APPLICATION VERSION)]ウィザードの[一般(GENERAL)]タブにある[アプリケーションセットアップ(Application Setup)]で、次の操作を実行します。

a. [既存のアプリケーションに追加する(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。 **重要** 次の表でアスタリスク(*)で示されているフィールドの値は、文字=、-、+、または@で始めることはできません。また、制御文字を含めることはできません。制限されているこれらの範囲に含まれているUnicode文字の完全なリストについては、https://www.aivosto.com/articles/control-characters.htmlを参照してください。
バージョンの説明(Version description)	(オプション)アプリケーションのこのバージョンに関する説明を入力します。
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、[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。

フィールド	説明
	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 Strategy	新しいアプリケーションバージョンの開発に使用する戦略を選択します。
Accessibility	アプリケーションへのアクセス方法を指定する値を選択します。
Application Type	アプリケーションタイプを選択します。
Target Deployment Platform	ターゲット展開プラットフォームを選択します。
Interfaces	アプリケーションにアクセスするために使用できるインタフェースのチェックボックスをオンにします。
Development Languages	アプリケーションバージョンの開発に使用する言語のチェックボックスをオンにします。
Authentication System	アプリケーションにアクセスするために使用する認証システムのチェックボックスをオンにします。

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 Obligations	アプリケーションバージョンが満たさなければならないすべての既知のコンプライアンス義務のチェックボックスをオンにします。
Data Classification	アプリケーションバージョンに適用されるすべてのデータ分類のチェックボックスをオンにします。
Application Classification	このアプリケーションバージョンに適用されるすべてのアプリケーション分類のチェックボックスをオンにします。

11. (オプション)Fortify ScanCentral DASTを使用している場合は、 [SCANCENTRAL DASTの属性(SCANCENTRAL DAST ATTRIBUTES)] タブをクリックして、次の操作を行います。
    a. [ベースURL] を入力して、アプリケーション内のすべてのページのプレフィックスを設定します。
12. テンプレート設定に進むには、 [次へ(NEXT)] をクリックします。
13. [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。

14. [ACCESS]タブに進むには、 [NEXT]をクリックします。
15. [チーム(TEAM)]で、次のいずれかを実行します。

注: 管理者の役割のユーザは、すべてのアプリケーションに対するフルアクセス権をすでに持っています。ユーザをチームに割り当てるには、そのユーザに別の役割も割り当てられていなければなりません。これは、管理者がローカルユーザでもLDAPユーザでも同じです。

- 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。

16. [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。

17. [閉じる(CLOSE)]をクリックします。

参照情報

"新しいアプリケーションの最初のバージョンの作成" ページ253

アプリケーションバージョンの自動適用と自動予測を有効にする

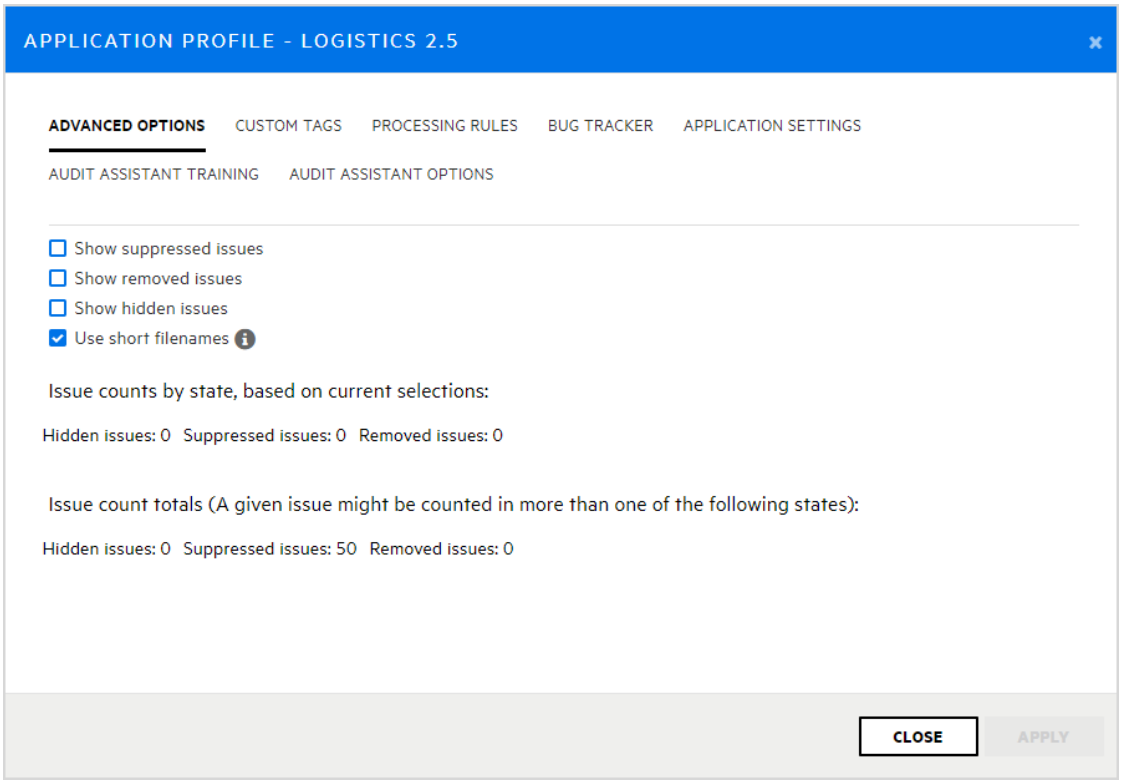
管理者がFortify Audit Assistantを設定し、自動適用をシステム全体で有効にし、 [管理(Administration)]ビューの [カスタムタグ(Custom Tags)]セクションで適切なプライマリタグフィールドをマップしてある場合、ユーザは特定のアプリケーションバージョンに対して自動適用を有効にできます。

自動適用をアプリケーションバージョンで有効にした場合、Fortify Audit Assistantを使用して静的分析の問題に関する予測を要求すると、Fortify Software Security Centerがそれらの予測をカスタムタグ値に適用します。

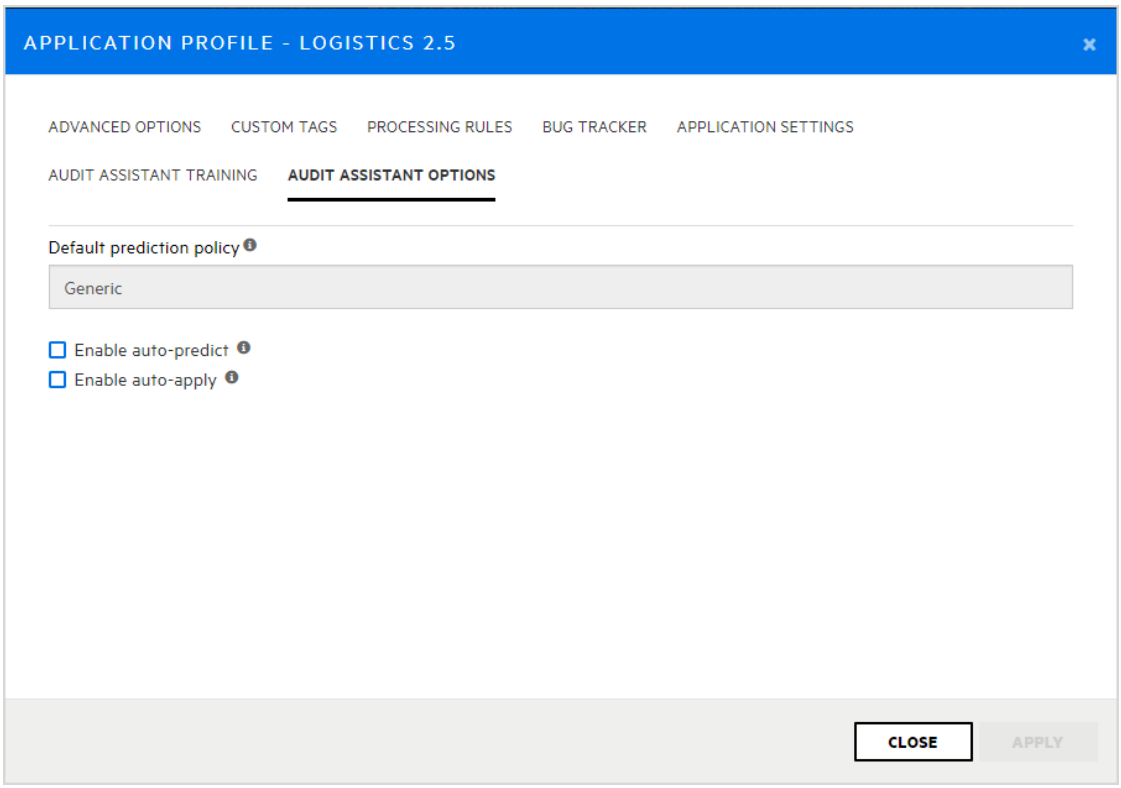
Fortify Audit Assistantが自動的にカスタムタグ値を問題に適用すると、その問題のために保存されたメタデータは、それがFortify Audit Assistantによって監査されたことを示します。カスタムタグ名の横にグレーの小槌が表示されて、ユーザはFortify Audit Assistantがその問題を予測したことを確認できます。

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。



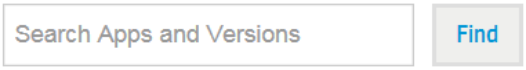
4. 未監査の問題をFortify Audit Assistantで自動的に評価するには、**自動予測を有効にする(Enable auto-predict)**]チェックボックスをオンにします。(自動予測の詳細については、"監査アシスタントの自動予測について" ページ90を参照してください)。
5. **Enable auto-apply**]チェックボックスをオンにします。
   プライマリタグの値が監査アシスタントにマップされていない場合、Fortify Software Security Centerがその結果に対する警告を表示して、管理者に問い合わせるよう勧めます。
6. **APPLY**]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385

[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400

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。

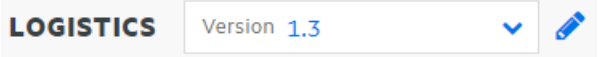
現在のシステムアクティビティによっては、メトリックの更新に時間がかかる場合があります。更新が完了すると、 [概要]ページにアプリケーションの最新データが表示されます。

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. OpenTextのヘッダで、 [アプリケーション(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。

4. [バージョンの編集 : <version> (EDIT VERSION: <*version*>)] ウィンドウで、"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256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. 変更を行った後には、 **[保存(SAVE)]** をクリックします。

参照情報

"アプリケーションバージョンに関連付けられているテンプレートを変更する" ページ273

"アプリケーションバージョンをデフォルトのデータ保持ポリシーからオプトアウトするための設定" 下

アプリケーションバージョンをデフォルトのデータ保持ポリシーからオプトアウトするための設定

すべてのアプリケーションバージョンに対してデータ保持ポリシーを有効にして、 **[アプリケーションバージョンに、デフォルトポリシーのオプトアウトを許可する(Allow application versions to opt-out of the default policy)]** オプションを選択した場合、個々のアプリケーションバージョンを、デフォルトのデータ保持ポリシーからオプトアウトするように設定できます。

デフォルトのデータ保持ポリシーをオプトアウトするには:

1. Fortify Software Security Centerにログインして、 **[アプリケーション(Applications)]** タブをクリックします。
2. **[アプリケーション(Applications)]** テーブルで、デフォルトのデータ保持ポリシーをオプトアウトするアプリケーションバージョンを選択します。
3. **[監査(AUDIT)]** ページ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。
4. **[バージョンの編集(EDIT VERSION)]** ウィンドウで、 **[ポリシー(Policies)]** タブをクリックします。
5. **[データ保持ポリシー(DATA RETENTION POLICY)]** で **[適用するデータ保持ポリシー(Data Retention Policy to Follow)]** の値を **[なし(デフォルトのオプトアウト)(None (Opt-out of Default))]** に変更します。
6. **[保存(SAVE)]** をクリックします。

参照情報

"データ保持について" ページ298

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 265
バグ報告用Velocityテンプレート 266
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 269
単一の問題のバグの送信 271
複数の問題のバグの送信 272
バグ状態管理 273

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" 次のページ
"バグトラッカプラグインの管理" ページ174
"バグトラッカプラグインの作成" ページ462

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

"バグトラッカプラグインのVelocityテンプレートのカスタマイズ" 次のページ

"Velocityテンプレートの削除" ページ269

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. OpenTextのヘッダで、 **管理(Administration)]**を選択します。
2. 左ペインで、 **テンプレート(Templates)**]を選択してから、 **[バグ報告テンプレート(Bug Filing Templates)**]を選択します。
   [バグ報告(Bug Filing)]ページには、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。
6. [テンプレートの追加(ADD TEMPLATE)]ダイアログボックスの **[マップ済みフィールド(Mapped field)]**ボックスに、マップするフィールドの名前を、 [バグトラッカプラグイン(bug tracker plugin)]ダイアログボックスに表示されるとおりに入力します。(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」、および「ISSUE_RECOMMENDATION」などの詳細な内容は、単一の問題のバグを報告している場合にのみ得られます。
8. [適用(APPLY)]をクリックします。
9. 別のテンプレートを追加するには、手順5 ~ 8を繰り返します。
10. [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" 前のページ

"バグトラッカプラグインのVelocityテンプレートのカスタマイズ" 下

"バグトラッカの設定" ページ265

"Velocityテンプレートの削除" ページ269

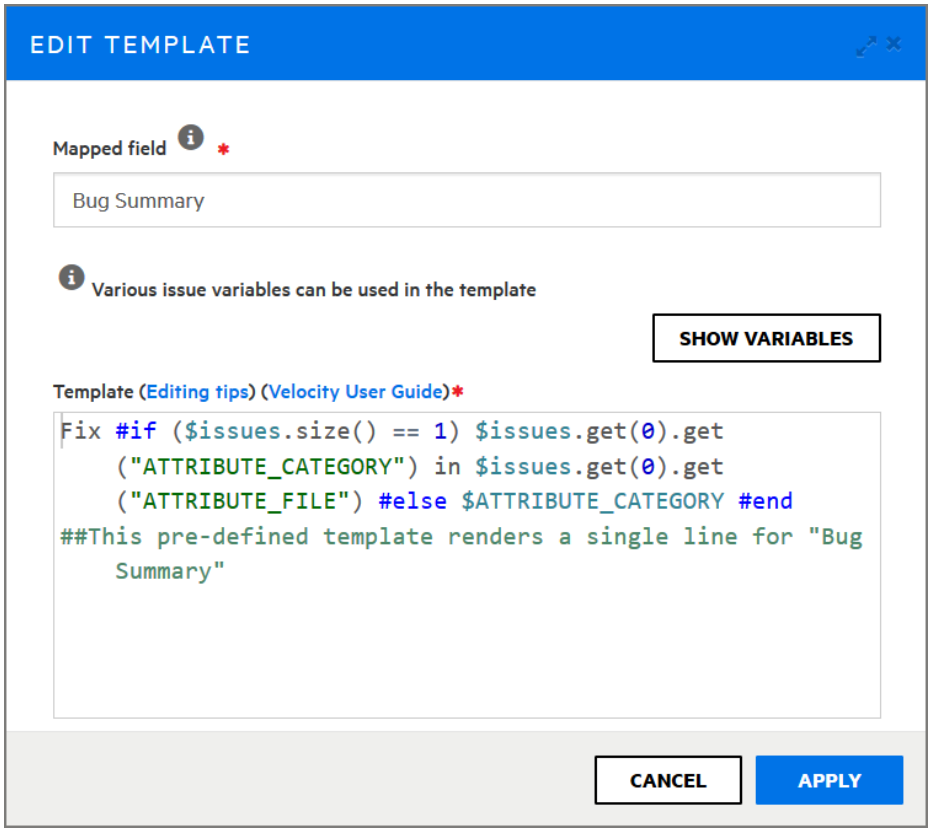
バグトラッカプラグインのVelocityテンプレートのカスタマイズ

バグトラッカプラグインのVelocityテンプレートをカスタマイズするには:

1. OpenTextのヘッダで、 [管理(Administration)]を選択します。
2. 左ペインで、 [テンプレート(Templates)]を選択してから、 [バグ報告テンプレート(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。



6. テンプレートの編集に役立つヒントを見るには、 [編集に関するヒント(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" 次のページ

"バグ報告用Velocityテンプレート" ページ266

"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266

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、 **管理(Administration)**]を選択します。
2. 左ペインで、 **テンプレート(Templates)**]を選択してから、 **バグ報告テンプレート(Bug Filing Templates)**]を選択します。
3. テンプレートグループのリストで、バグトラッカプラグインの名前をクリックします。
   行が展開され、プラグインで提供される説明およびサマリフィールドにマップされた事前設定済みテンプレートの詳細が表示されます。
4. **DELETE**]をクリックします。
   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266

"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266

"バグトラッカプラグインのVelocityテンプレートのカスタマイズ" ページ267

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

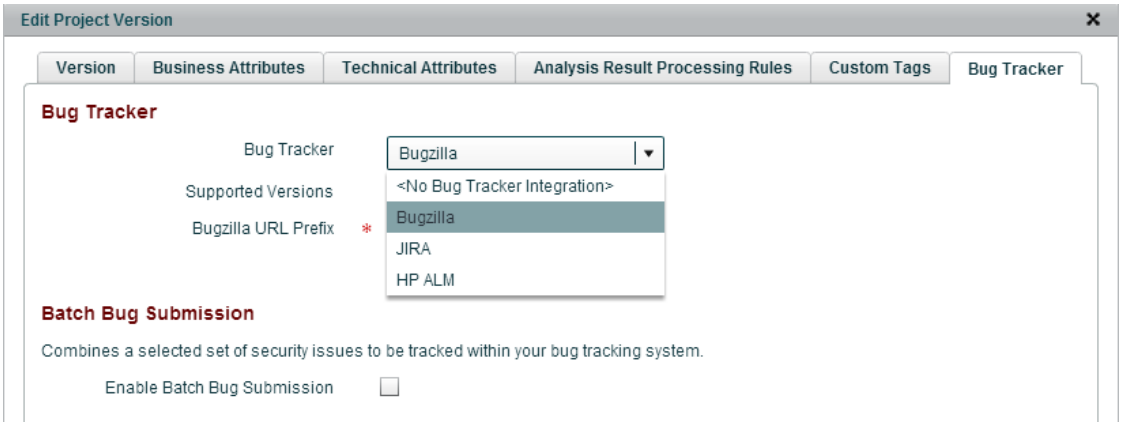
バグトラッキングシステムをアプリケーションバージョンに割り当てるには、次の手順に従います。これを実行する前に、バグトラッカプラグインがすでにシステムに存在している必要があります。Fortify Software Security Centerにバグトラッカを追加する方法については、"バグトラッカプラグインの管理" ページ174を参照してください。

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. OpenTextのヘッダで、 **アプリケーション(Applications)**]をクリックします。
2. **アプリケーション(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。
4. [アプリケーションプロファイル - <Application_Name><Application_Version> (APPLICATION PROFILE - <*Application_Name*><*Application_Version*>)] ダイアログボックスで、 [バグトラッカ (BUG TRACKER)] タブをクリックします。



5. [バグトラッカの統合 (Bug Tracker Integration)] リストから、このアプリケーションバージョンのバグを追跡するために使用するアプリケーションを選択します。
6. 必要なフィールドに入力し、 [VALIDATE CONNECTION] をクリックします。
7. [バグトラッカプラグイン設定のテスト (TEST BUG TRACKER PLUGIN CONFIGURATION)] ダイアログボックスで、バグトラッカ認証資格情報を入力し、 [テスト (TEST)] をクリックします。

   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172

"バグトラッカプラグインの管理" ページ174

"複数の問題のバグの送信" ページ272

"バグトラッカプラグインの作成" ページ462

単一の問題のバグの送信

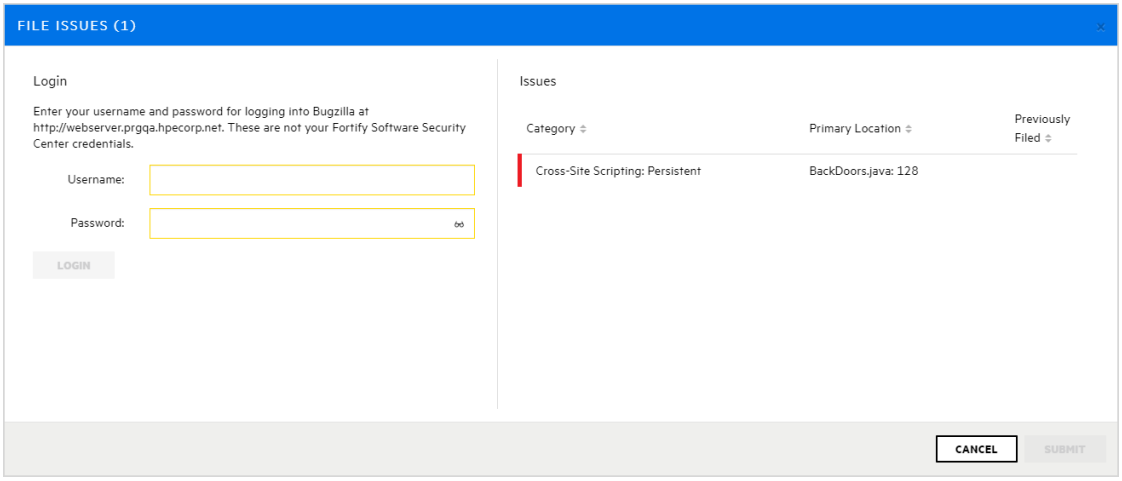
アプリケーションバージョンにバグトラッキングプラグインが指定されている場合 ("アプリケーションバージョンへのバグトラッキングシステムの割り当て" ページ269)、そのバグトラッカを使用して、1つ以上の問題を対象にするバグを送信できます。

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174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269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。



3. [ファイルの問題 (1)(FILE ISSUES (1))] ダイアログボックスの [**ログイン(Login)**] に、このアプリケーションバージョンに関連付けられたバグトラッカのユーザ名とパスワードを入力し、 [**ログイン(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376

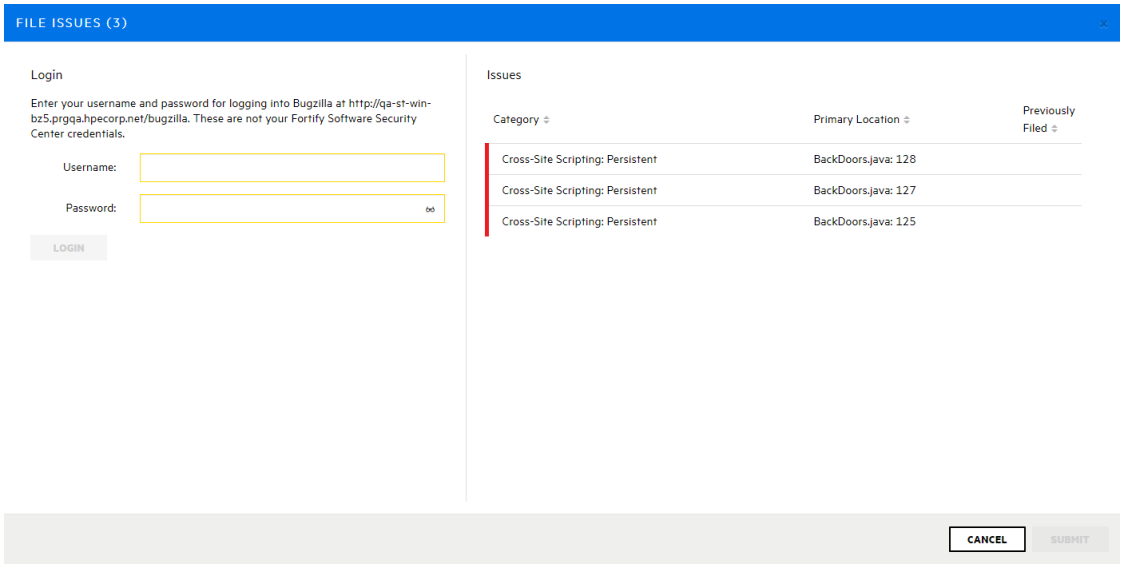
複数の問題のバグの送信

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269)、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" 前のページ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。

   注 : チェックボックスをオンにした後で、 [**バグの報告 (File Bug)**] アイコンが表示されない場合は、まずアプリケーションバージョンのバグトラッカを設定する必要があります。("アプリケーションバージョンへのバグトラッキングシステムの割り当て" ページ269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. [ファイルの問題 (FILE ISSUES)] ダイアログボックスの [**ログイン (Login)**] に、このアプリケーションバージョンに関連付けられたバグトラッカのユーザ名とパスワードを入力し、 [**ログイン (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" ページ271

"問題に対して送信されたバグの表示" ページ376

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269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

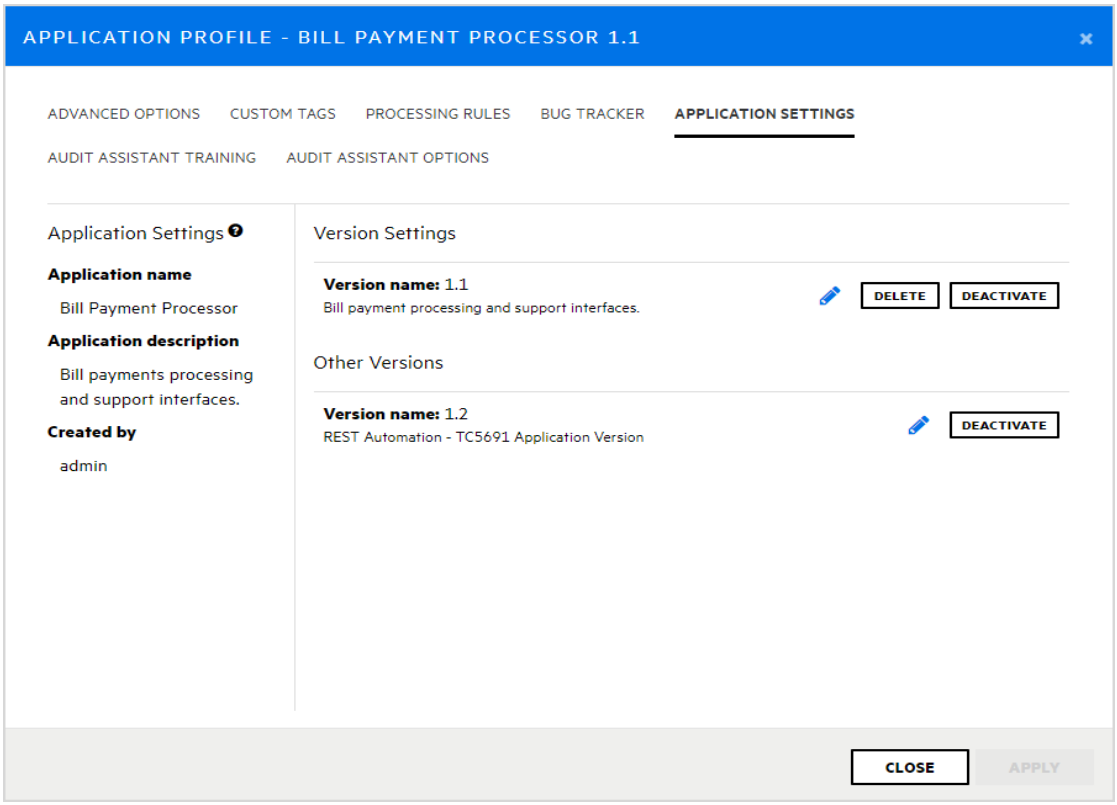
問題テンプレートを含め、既存のアプリケーションバージョンの多くの設定を変更できます。ただし、アプリケーションバージョンに別の問題テンプレートを割り当てるか、サーバ上の問題テンプレートを更新すると、データベースキャッシュと既存の監査セッション間の同期が失われるので、注意してください。

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。

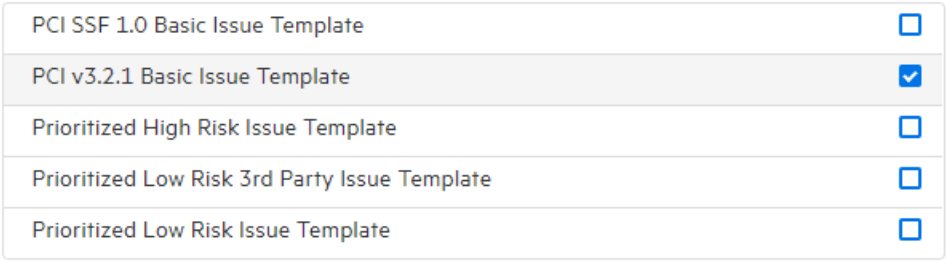
1. Fortify Software Security Center に管理者またはセキュリティリードとしてログインします。
2. ダッシュボードの [SSUE STATS] ページで、変更するアプリケーションバージョンの名前をクリックします。
3. [監査 (AUDIT)] ページのアプリケーションバージョンツールバーで、 **[プロファイル (PROFILE)]** をクリックします。
4. [アプリケーションプロファイル<application_version> (APPLICATION PROFILE <*application_version*>)] ダイアログボックスで、 **[アプリケーション設定 (APPLICATION SETTINGS)]** をクリックします。



5. **[バージョン設定 (Version Settings)]** で、編集アイコンをクリックします。

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. [バージョンの編集 (EDIT VERSION)] ダイアログボックスで、 **[テンプレート (TEMPLATE)]** タブをクリックします。



テンプレートのリストでは、現在割り当てられているテンプレートが選択済みとしてマークされます。

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指定できます。

アプリケーションバージョンの分析結果処理ルールを設定するには:

1. 管理者として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。
2. [**監査(AUDIT)**]ページのアプリケーションバージョンツールバーで、 [**プロファイル(PROFILE)**]をクリックします。
3. [アプリケーションプロファイル(APPLICATION PROFILE) - <Application_Version> (APPLICATION PROFILE - <*Application_Version*>)]ダイアログボックスで、 [**処理ルール(PROCESSING RULES)**]タブを選択し、一覧表示されている処理ルールを確認します。
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、これらの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

ルール	説明
	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インスタンスIDを変更できます。どちらのインスタンスIDも同じ問題を特定します。このルールを有効にすると、Fortify Static Code Analyzer (またはRulepack)のバージョンが同じ場合でも、古いインスタンスIDは対応する

ルール	説明
	新しいインスタンスIDに移行します。このルールの動作の詳細については、"インスタンスIDマイグレーションに影響する処理ルールについて" ページ280を参照してください。
Require approval if result has Fortify Java Annotations (結果にFortify Java Annotationがある場合は承認を必要とする)	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を変更できます。どちらのインスタンスIDも同じ問題を特定します。このルールを有効にすると、古いインスタンスIDは対応する新しいインスタンスIDに自動的に移行され、問題の履歴は保持されます。(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ほうが便利な場合があります)。 このルールの動作の詳細については、"インスタンスIDマイグレーションに影響する処理ルールについて" ページ280を参照してください。
Require approval if the engine	Fortify Software Security Centerは、

ルール	説明
version of a scan is newer than the engine version of the previous scan (スキャンのエンジンバージョンが前のスキャンのエンジンバージョンよりも新しい場合は承認を必要とする)	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 quick scan results and SCA speed dial results performed with a setting of less than four (4未満の設定で実行されるSCAクイックスキャンの結果とSCAスピードダイヤルの結果を無視する)	クイックスキャンモードで実行されるFortify Static Code Analyzerスキャンの処理をブロックします。このスキャンでは、高信頼性と高重大度の問題が検索されます。このルールを使用すると、4未満のレベルで実行されたスピードダイヤル分析結果もアップロードされなくなります。 スピードダイヤル分析結果のアップロードを有効にするには、このチェックボックスをオフにします。 **注意** フルスキャン結果のアップロードとスピードダイヤル分析結果のアップロードの間で二者択一を行った後は、アプリケーションバージョン用にアップロードする将来のスキャン結果を同じタイプにするようお勧めします。
Require approval if the Rulepacks used in the scan do not match the Rulepacks used in the previous scan (スキャンで使用するRulepackが前のスキャンで使用したRulepackと一致しない場合は承認を必要とする)	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	Fortify Software Security Centerは、

ルール	説明
not have valid certification	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

ルール	説明
	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。

インスタンスIDマイグレーションに影響する処理ルールについて

次の2つの処理ルールがインスタンスIDマイグレーションに影響します。「Perform Force Instance ID migration on upload」と「Automatically perform Instance ID migration on upload」です。これらの使い方を理解しておくと便利です。

問題インスタンスIDは、次のいずれかの理由で変更される可能性があります。

- 新しいFortify Static Code AnalyzerバージョンでのIID生成アルゴリズムの変更
- 新しいRulepackバージョンの使用
- スキャン設定の変更(たとえば、スキャンに対して追加のルールの使用が指定された場合)。
- 脆弱なコードの複製(たとえば、1つのアプリケーションバージョンで同じ脆弱なコードが複数回コピーされ、貼り付けられた場合。この場合は、Fortify Static Code Analyzerにより最初の複製フラグメントの固有のインスタンスIDが生成され、次いでこの生成されたインスタンスIDが残りのすべての複製フラグメントのためにインクリメントされます。したがって、別個の2回のスキャンによって、同一のコードフラグメントに対して別々のインスタンスIDが作成される可能性があり、これはこれらの2回のスキャンによってそれらが明らかにされる順序に依存します)。

「**Automatically perform Instance ID migration on upload (アップロード時にインスタンスIDマイグレーションを自動的に実行する)**」ルールでは、新しいFortify Static Code AnalyzerバージョンによるIID生成アルゴリズムの変更またはRulepackバージョンの変更が原因で発生する問題インスタンスIDの変更が解決されます。たとえば、最新のスキャ

ンで使用されたFortify Static Code Analyzerバージョンが以前のスキャンで使用されたバージョンより新しいことがFortify Software Security Centerによって検出された場合です。「Automatically perform Instance ID migration on upload (アップロード時にインスタンスIDマイグレーションを自動的に実行する)」が選択された場合は、Fortify Software Security Centerによってマイグレーションが実行されます。使用されているFortify Static Code Analyzerバージョンの変更がFortify Software Security Centerによって検出されなかった場合、マイグレーションは実行されません(「Automatically perform Instance ID migration on upload (アップロード時にインスタンスIDマイグレーションを自動的に実行する)」が選択されている場合でも)。

「**Perform Force Instance ID migration on upload (アップロード時にインスタンスIDの強制マイグレーションを実行する)**」ルールでは、スキャン設定の変更または脆弱なコード複製が原因で発生するインスタンスIDの変更が解決されます。Fortify Software Security Centerは、Static Code Analyzerのバージョンまたは Rulepackのバージョンが変更されたかどうかを簡単に判断できます。Fortify Software Security Centerは、このような変更を検出すると、マイグレーションを自動的に実行します。ただし、他のケース(コードの複製、スキャン設定)でFortify Software Security Centerがこの判断を行うことはできません。このような場合は、この処理ルールを使用して、Fortify Software Security Centerに強制的にマイグレーションを実行させることができます。

スキャン設定の変更または脆弱なコードの複製の結果として問題インスタンスIDが変更される可能性がある場合は、「**Perform Force Instance ID migration on upload (アップロード時にインスタンスIDの強制マイグレーションを実行する)**」処理ルールを選択することをお勧めします。

注: インスタンスIDマイグレーションには時間がかかることが、この2つのルールが存在する理由です。実際には、IIDマイグレーションを毎回実行するわけではないため、これらのルールによって、スキャンをアップロードするたびにインスタンスIDマイグレーションを実行するかどうかを決定できます。

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327

"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332

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

Fortify Audit Assistantを設定する際に **特定のアプリケーションバージョンのポリシーを有効にする(Enable specific application version policies)**]を選択した場合は、アプリケーションバージョンのデフォルト設定を上書きすることができます。これを選択しなかった場合は、すべてのアプリケーションバージョンでデフォルト設定が使用されます。アプリケーションバージョンレベルでデフォルト設定を上書きする機能を使用したい場合は、"Audit Assistantの設定" ページ385を参照してください。

アプリケーションバージョンに対してFortify Audit Assistantオプションを設定するには:

1. アプリケーションで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385を参照してください)。
2. ダッシュボードから、Fortify Audit Assistantオプションを設定するアプリケーションバージョンを選択します。
3. [監査(AUDIT)]ページで、 **[プロファイル(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385を参照してください)。それ以外の場合、Fortify 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、Fortify Audit Assistantはデフォルトの予測ポリシーを使用します。
6. このアプリケーションバージョンの監査されていない問題を評価のためにFortify Audit Assistantサーバに送信するには **[自動予測を有効にする(Enable auto-prediction)]**をオンにします。

   注: **[自動予測を有効にする(Enable auto-prediction)]**および **[自動適用を有効にする(Enable auto-apply)]**チェックボックスは、これらの監査設定がシステム全体で有効になっている場合にのみ使用できます。("Audit Assistantの設定" ページ385を参照してください)。
7. マップされたカスタムタグ値に予測値がFortify Audit Assistantによって自動的に適用されるようにするには、 **[自動適用を有効にする(Enable auto-apply)]**チェックボックスをオンにします。
8. **[適用(APPLY)]**をクリックします。
9. Fortify Software Security Centerにより、これらのオプションの保存を確認するメッセージが表示されます。 **[OK]**をクリックします。
10. **[CLOSE]**をクリックします。

参照情報

"Audit Assistantの設定" ページ385

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。開発者が自分に割り当てられた問題を監査した後には、セキュリティの専門家がそれらの問題を確認して、それぞれに「承認済み」か「不承認」のマークを付けることができます。

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:

システムへのカスタムタグの追加 283
カスタムタグ属性の変更 286
カスタムタグをグローバルで非表示にする 286
カスタムタグの削除 286
カスタムタグ値の追加 287
カスタムタグを編集する 293
カスタムタグ値の削除 293
カスタムタグと問題テンプレートを関連付ける 294
問題テンプレートからのカスタムタグの削除 294
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 295
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 297
問題テンプレートによるカスタムタグの管理 297
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 298

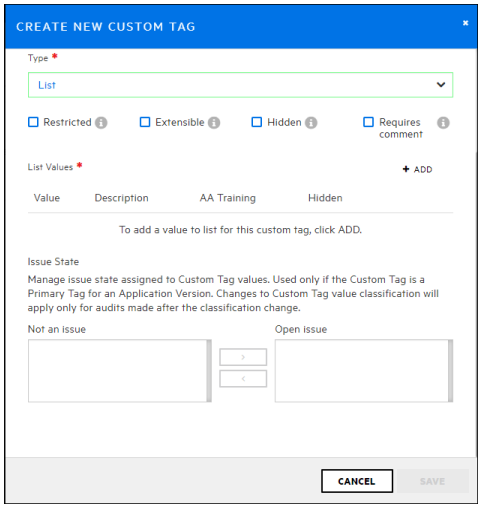
システムへのカスタムタグの追加

Fortify Software Security Center管理者の場合は、システムにカスタムタグを追加できます。次のトピックでは、サポートされている各カスタムタグタイプをFortify Software Security Centerに追加する方法について説明します。

注 : 作成してアプリケーションバージョンに割り当てるカスタムタグの値に基づいて、問題をフィルタできます。詳細については、" [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349を参照してください。

カスタムタグを追加するには、次の手順を実行します。

1. OpenTextのヘッダで、 **[管理 (Administration)]** をクリックします。
2. 左ペインで、 **[テンプレート (Templates)]** を選択し、 **[カスタムタグ (Custom Tags)]** を選択します。
3. [Custom Tags] ページヘッダで、 **[新規 (NEW)]** をクリックします。
   [新しいカスタムタグの作成 (CREATE NEW CUSTOM TAG)] 画面が表示されます。



4. [新しいカスタムタグの作成 (CREATE NEW CUSTOM TAG)] ダイアログボックスで、 **[名前 (Name)]** ボックスに新しいタグの名前を入力します。

   重要 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。

5. (オプション) [Description] ボックスに、カスタムタグの使い方を説明するコンテンツを入力します。
6. **[タイプ (Type)]** リストから、次の表に一覧表示されているタグタイプの1つを選択します。

タイプ	受諾可能な値
Date	[環境設定 (PREFERENCES)] ダイアログボックスで指定されたフォーマットのカレンダの日付 ("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218」を参照してください)。
Decimal	最高18桁の精度を持つ数値 (小数点以下9桁まで)

タイプ	受諾可能な値
List	タグに指定する値のリストから選択
Text	最大500文字の文字列(HTML/XMLタグおよび新規改行は使用できない)

7. (オプション)次のオプションのタグ機能の一部または全部を選択します。
   - **制限(Restricted):** 特定の許可を持つユーザ(マネージャ、セキュリティリード、管理者)にのみタグの変更を許可するには、このチェックボックスをオンにします。
   - **拡張可能(Extensible):** (リストタイプのみ)リストタイプのカスタムタグは拡張可能です。つまり、監査官は問題を監査するときに値を追加できます。監査時にユーザがリストタグに新しい値を追加できるようにする場合は、このチェックボックスをオンにします。
   - **非表示(Hidden):** 割り当て(ASSIGN)]ダイアログボックスまたは 監査ワークベンチ(Audit Workbench)]でタグが表示されないようにするには、このチェックボックスをオンにします。
   - **コメントが必要(Requires comment):** このカスタムタグの値を変更する際にユーザに常にコメントを残すことを求める場合は、このチェックボックスをオンにします。コメントを必要とするカスタムタグが変更されると、システムは自動的にコメントを追加して、タグに変更が加えられたことを示します。

     注: コメントを必要とする新しいカスタムタグが日付タイプタグの場合、監査中にユーザがタグに対して選択する日付は、常に 環境設定(PREFERENCES)]ダイアログボックスで指定されたフォーマットになります。
8. 新しいカスタムタグが日付タグ、10進数タグ、またはテキストタイプのタグの場合は、 **保存(Save)**]をクリックします。新しいカスタムタグがリストタイプタグの場合は、値を追加する必要があります。リストタイプのカスタムタグの値を作成する方法については、"カスタムタグ値の追加" ページ287を参照してください。

参照情報

"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" ページ392

"カスタムタグをグローバルで非表示にする" 次のページ

"カスタムタグの削除" 次のページ

"カスタムタグ" ページ282

"カスタムタグを編集する" ページ293

"カスタムタグと問題テンプレートを関連付ける" ページ294

"問題テンプレートによるカスタムタグの管理" ページ297

"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" ページ298

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. [管理(Administration)]ページの左ペインから、**[テンプレート(Templates)]**をクリックして、**[カスタムタグ(Custom Tags)]**をクリックします。
2. **[カスタムタグ(Custom Tags)]**ページで、変更するタグを表示する行をクリックします。
   行が展開され、詳細が表示されます。
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

"システムへのカスタムタグの追加" ページ283

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. **[管理(Administration)]ビューの左ペインから、[テンプレート(Templates)]**をクリックして、**[カスタムタグ(Custom Tags)]**を選択します。
   [カスタムタグ(Custom Tags)]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。

- プライマリタグとして設定されている。
- 問題の監査で使用されている。
- 現在、アプリケーションバージョンまたは問題テンプレートに関連付けられている。アプリケーションバージョンからカスタムタグを削除する方法については、"カスタムタグをアプリケーションバージョンから関連付け解除する" ページ297を参照してください。問題テンプレートからカスタムタグを削除する方法については、"問題テンプレートからのカスタムタグの削除" ページ294を参照してください。

分析タグは削除できません。

カスタムタグを削除するには、次の手順を実行します。

1. **[管理(Administration)]**ビューの左ペインから、**[テンプレート(Templates)]**を選択して、**[カスタムタグ(Custom Tags)]**を選択します。
   [カスタムタグ(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282

カスタムタグ値の追加

Fortify Software Security Center管理者は、リストタイプのカスタムタグに値を追加できます。

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。

カスタム値を追加または編集する場合は、次の操作を行います。

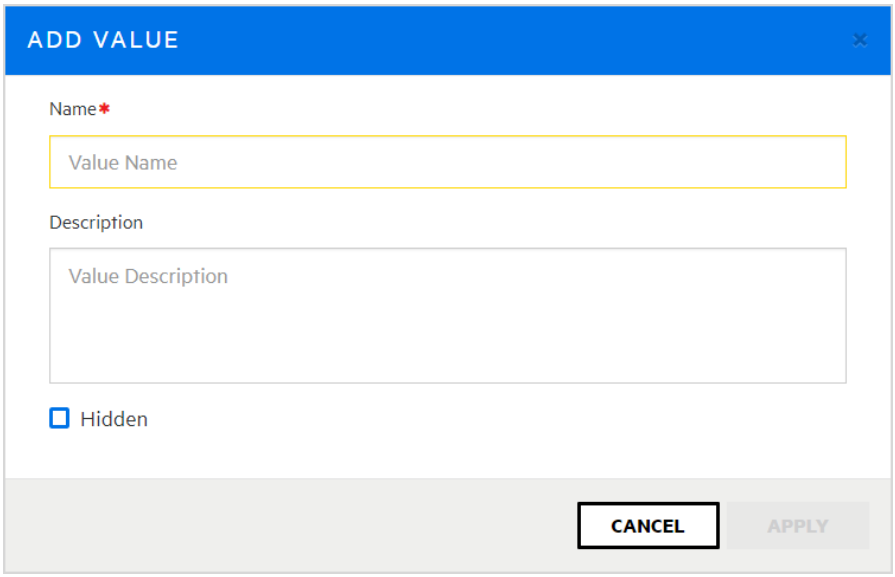
- 新しい値の名前を作成する
- (オプション)新しい値の説明を作成する
- (オプション)Fortify Audit Assistantが設定されている場合は、カスタム値をFortify Audit Assistant値にマップし、Fortify Audit Assistantモデルのトレーニングでその値を使用するかどうかを決定する
- 値を問題の状態に割り当てる(Fortify Audit Assistantを有効にする必要があります)

カスタムタグ値を追加する

メモ: Fortify Audit Assistantが設定されている場合は、"カスタムタグ値を追加する(Fortify Audit Assistantが設定済みの場合)" 次のページを参照してください。

リストタイプのカスタムタグに値を追加するには:

1. OpenTextのメニューバーで、 **管理(Administration)**] をクリックします。
2. 左ペインで、 **テンプレート(Templates)**] をクリックし、 **カスタムタグ(Custom Tags)**] をクリックします。
   カスタムタグ(Custom Tags)] ページにカスタムタグが一覧表示されます。
3. カスタム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. 画面の右下隅で、 **編集(EDIT)**] をクリックします。
5. 値の表の上で、 **+追加(+ ADD)**] をクリックします。
   値の追加(Add Value)] ダイアログボックスが表示されます。



6. 値の追加(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。
7. (オプション) 割り当て(Assign)] ダイアログボックスや 監査ワークベンチ(Audit Workbench)] にタグが表示されないようにするには、 **非表示(Hidden)**] チェックボックスをオンにします。
8. **適用(APPLY)**] 、 **保存(SAVE)**] の順にクリックします。
9. (オプション)各値に問題の状態を設定します。
10. 追加する必要がある追加値に対して、手順5 ~ 9を繰り返します。

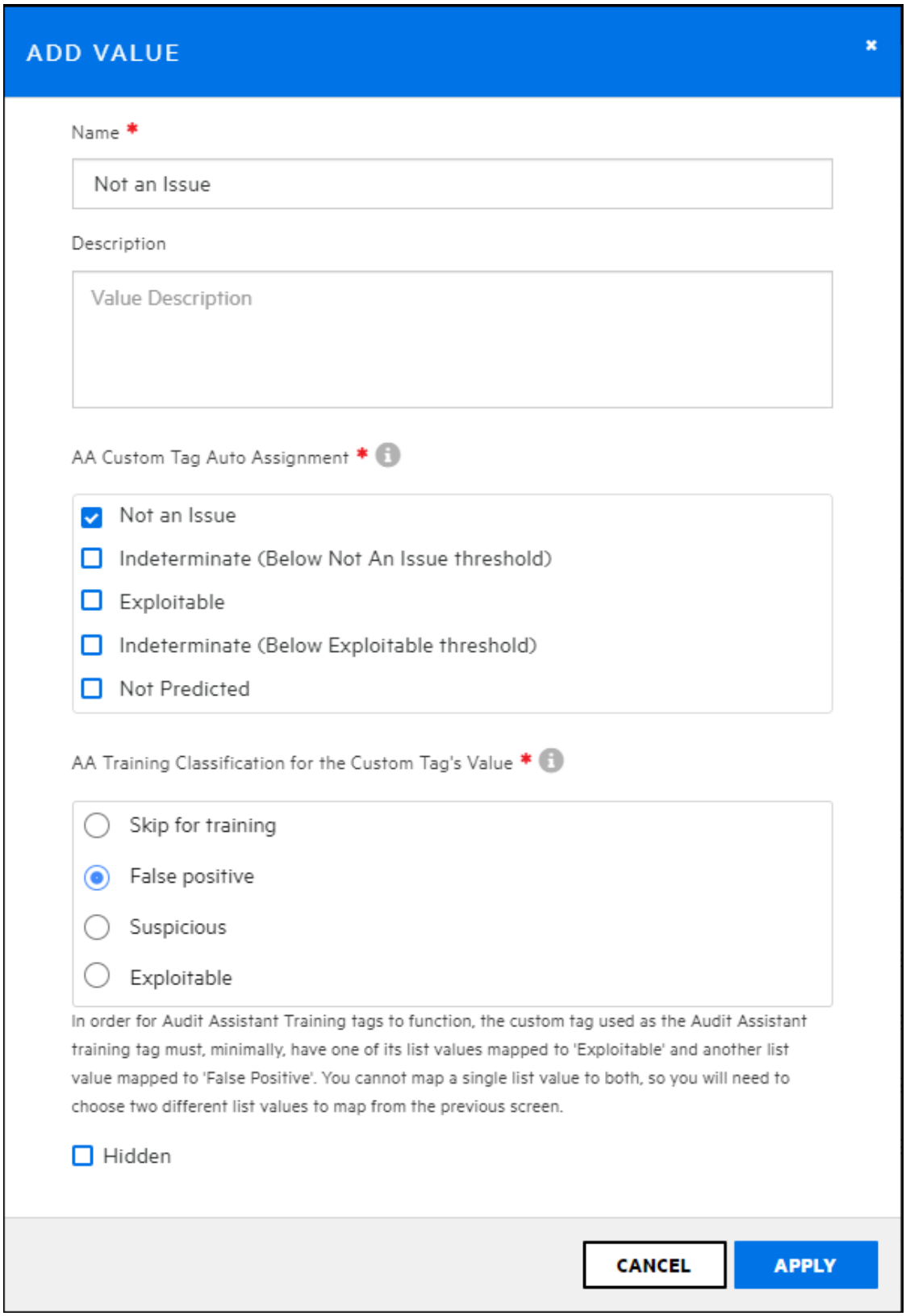
カスタムタグ値を追加する(Fortify Audit Assistantが設定済みの場合)

Audit Assistantが設定済みの場合にリストタイプのカスタムタグに値を追加するには:

1. OpenTextのメニューバーで、 **管理(Administration)]** をクリックします。
2. 左ペインで、 **テンプレート(Templates)**] をクリックし、 **カスタムタグ(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. Fortify Audit Assistantを使用するようにFortify Software Security Centerが設定され、自動適用が有効になっている場合、 [値の追加(ADD VALUE)] ダイアログボックスには **[AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)]** セクションと、 **[カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)]** セクションが表示されます。


ADD VALUE
Name *
Not an Issue
Description
Value Description
AA Custom Tag Auto Assignment *
Not an Issue
Indeterminate (Below Not An Issue threshold)
Exploitable
Indeterminate (Below Exploitable threshold)
Not Predicted
AA Training Classification for the Custom Tag's Value *
Skip for training
False positive
Suspicious
Exploitable
In order for Audit Assistant Training tags to function, the custom tag used as the Audit Assistant training tag must, minimally, have one of its list values mapped to 'Exploitable' and another list value mapped to 'False Positive'. You cannot map a single list value to both, so you will need to choose two different list values to map from the previous screen.
Hidden
CANCEL
APPLY

新しい値が [AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)] セクションのAudit Assistantの予測値と一致する場合は、そのチェックボックスをオンにすると、選択したAudit Assistantの予測値にそのリスト値が自動的にマップされます。これにより、アプリケーションバージョンの **[プロファイル]** の **[Audit Assistantオプション(AUDIT ASSISTANT OPTIONS)]** セクションで **[自動適用を有効にする(Enable auto-apply)]** を選択しているすべてのアプリケーションバージョンに対して、値の自動マッピングが有効になります。

7. Fortify Audit Assistantをトレーニングするには、このカスタムタグ値がFortify Audit Assistantに対して持つ意味を選択します。問題にこのタグ値を設定すると、Fortify Audit Assistantは、ユーザによるここでの問題分類に基づいて、ユーザが問題をどのように見ているかを学習します。トレーニングですべてのリスト値を使用する必要はありませんが、トレーニングを行うには、少なくとも2つを割り当てる必要があります。1つは [悪用可能(Exploitable)] に割り当て、もう1つは [誤検出(False Positive)] に割り当てる必要があります。Fortify Audit Assistantのトレーニングで使用するリスト値ごとに、この手順を繰り返します。
8. **[適用(APPLY)]**、**[保存(SAVE)]** の順にクリックします。
9. (オプション)各値に問題の状態を設定します。

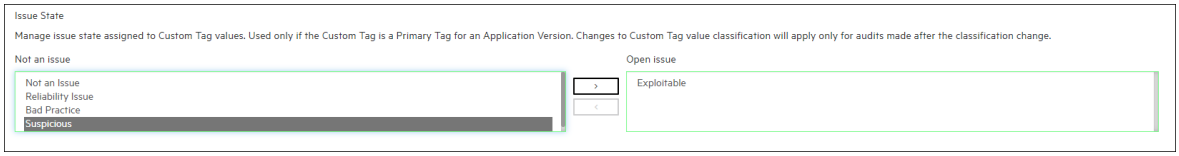
メモ: 新しいカスタムタグを使用してアプリケーションバージョンの問題を監査するには、まずタグをアプリケーションバージョンに割り当てる必要があります。手順については、"カスタムタグをアプリケーションバージョンに割り当てる" ページ295を参照してください。

問題の状態を設定する

プライマリタグに設定された分析のレベルに基づいて、問題が「未解決の問題(Open Issue)」と「問題でない(Not an Issue)」のどちらであるか、問題の監査がカスタムグループにより行われました。[疑わしい(Suspicious)] および [悪用可能(Exploitable)] に等しい値は、分析タグで [未解決の問題(Open Issue)] と見なされます。

カスタムタグに値を追加する際に、Fortify Audit Assistantが有効になっている場合は、その問題の状態を設定できます。[問題の状態(Issue State)] では、[問題でない(Not an Issue)] か [未解決の問題(Open Issue)] のいずれかのカテゴリに問題を割り当てることができます。結果を監査する際に、**[グループ化条件(Group By)]** メニューから **[問題の状態(Issue State)]** を選択すると、解決を要する問題とその数をすばやく評価できます。問題を監査し、[分析(Analysis)] カスタムタグ値に値を割り当てると、[問題の状態(Issue State)] フォルダは選択した値に基づいて更新されます。

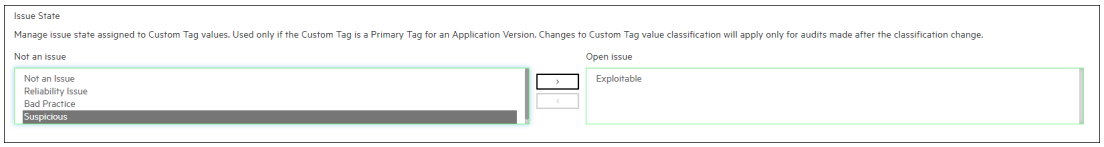
リストタイプのカスタムタグ値を追加すると、[問題の状態(Issue State)] セクションの [問題でない(Not an issue)] 側にその値が表示されます。



カスタムタグ値の [問題の状態(Issue State)] を設定する

メモ: すでに [カスタムタグ] ページを開き、編集モードにある場合は、手順5から開始します。

1. OpenTextのメニューバーで、 **[管理(Administration)]** をクリックします。
2. 左ペインで、 **[テンプレート(Templates)]** をクリックし、 **[カスタムタグ(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. 値を編集するタグの行をクリックします。
   行が展開されて、タグの詳細が表示されます。
4. 値の表の下で、 **[EDIT]** をクリックします。
5. [問題の状態(Issue State)] セクションで、未解決の問題とみなす値を選択します。
6. 矢印ボタンを使用して、選択した値を [問題でない(Not an issue)] ボックスから [未解決の問題(Open issue)] ボックスに移動します。



   間違えたり、変更したい場合は、 [未解決の問題(Open issue)] ボックスで値を選択し、戻る矢印ボタンを使用して [問題でない(Not an issue)] ボックスに戻します。
7. すべての値が適切な [問題の状態(Issue State)] ボックスに表示されるまで、手順5 ~ 6を続行します。
8. **[保存(SAVE)]** ボタンをクリックします。

参照情報

"カスタムタグを編集する" 次のページ

"カスタムタグ値の削除" 次のページ

"システムへのカスタムタグの追加" ページ283

"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295

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. [管理(Administration)]ビューの左ペインから、**[テンプレート(Templates)]**をクリックして、**[カスタムタグ(Custom Tags)]**を選択します。
   [カスタムタグ(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、"システムへのカスタムタグの追加" ページ 283を参照してください。

参照情報

"カスタムタグ値の削除" 下

"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295

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. [管理(Administration)]ビューの左ペインから、**[テンプレート(Templates)]**を選択して、**[カスタムタグ(Custom Tags)]**を選択します。
   [カスタムタグ(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" 上

"システムへのカスタムタグの追加" ページ283

"カスタムタグ値の追加" ページ287

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. OpenTextのヘッダで、 **管理(Administration)**] をクリックします。
2. 左ペインで、 **テンプレート(Templates)**] を選択して、 **問題(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。
6. カスタムタグの追加(ADD CUSTOM TAG)] ダイアログボックスで、問題テンプレートに関連付けるカスタムタグのチェックボックスをオンにして、 **+追加(+ADD)**] をクリックします。
   カスタムタグ(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。

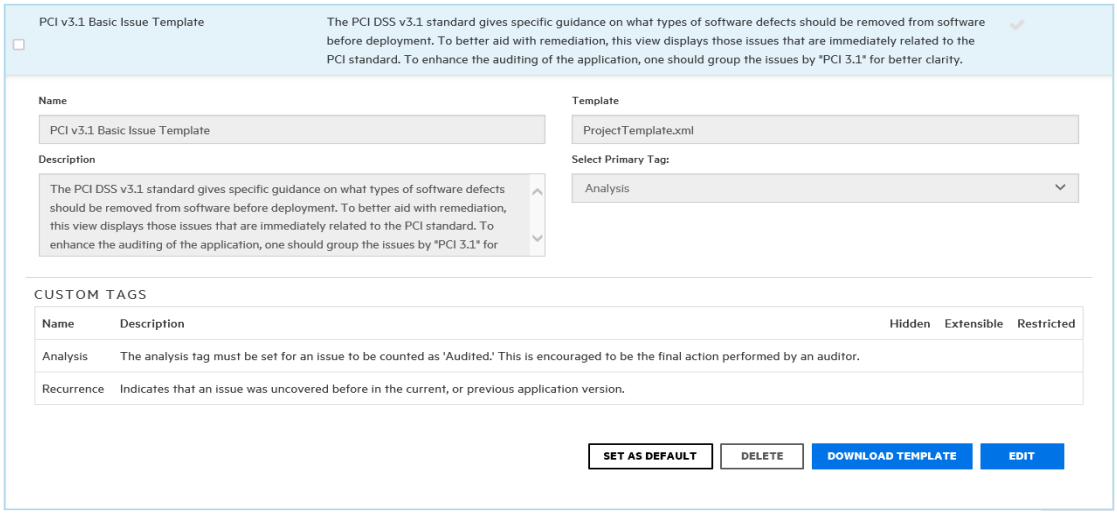
参照情報

"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297

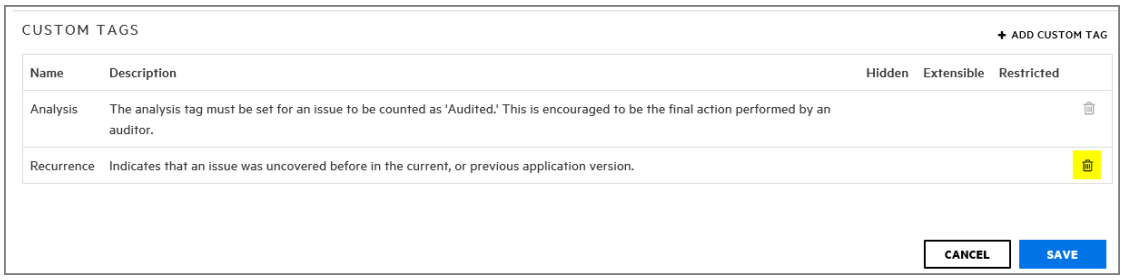
問題テンプレートからのカスタムタグの削除

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. 管理(Administration)] ページの左ペインから、 **テンプレート(Templates)**] を選択して、 **問題(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。

注: 問題テンプレートから指定したプライマリタグを削除することはできません。

5. [**保存(SAVE)**] をクリックします。

参照情報

"カスタムタグ" ページ282

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。
2. [監査(AUDIT)] ページのアプリケーションバージョンツールバーで、 [**プロファイル(PROFILE)**] をクリックします。
3. [アプリケーションプロファイル(APPLICATION PROFILE)] ダイアログボックスで、 [**カスタムタグ(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。
   b. [プライマリタグの選択(SELECT PRIMARY TAG)]ダイアログボックスの **[プライマリタグの選択(Select Primary Tag)]**リストから、プライマリカスタムタグとして設定するタグを選択します。

      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、"システムへのカスタムタグの追加" ページ283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293を参照してください。

   c. [DONE]をクリックします。
7. [閉じる(CLOSE)]をクリックします。

割り当てられたカスタムタグは、次にチームメンバーがアプリケーションバージョンに関する問題を監査するときに使用可能になります。

参照情報

"カスタムタグをアプリケーションバージョンから関連付け解除する" 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. OpenTextのヘッダで、 **[アプリケーション(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。
3. **[監査(AUDIT)]** ページのアプリケーションバージョンツールバーで、 **[プロファイル(PROFILE)]** をクリックします。
4. **[アプリケーションプロファイル(APPLICATION PROFILE)]** ウィンドウで、 **[カスタムタグ(CUSTOM TAGS)]** タブを選択します。
5. **[割り当て/削除(ASSIGN/REMOVE)]** をクリックします。
   [CUSTOM TAGS] タブには、システム内のすべてのカスタムタグが一覧表示されます。アプリケーションバージョンに関連付けられているタグのチェックボックスが選択されています。
6. 削除するカスタムタグのチェックボックスをオフにして、 **[DONE]** をクリックします。
7. **[CLOSE]** をクリックします。

このアプリケーションバージョンの **[監査(AUDIT)]** ページ上に表示されている問題の詳細内の **[監査(AUDIT)]** タブでは、カスタムタグが一覧にされなくなりました。

すべてのアプリケーションバージョンとこれが割り当てられている問題テンプレートからカスタムタグを削除した後には、そのタグを削除できます。

参照情報

"問題テンプレートからのカスタムタグの削除" ページ294

"システムへのカスタムタグの追加" ページ283

"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295

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. OpenTextのヘッダで、 **[管理(Administration)]** を選択します。
2. 左ペインで、 **[テンプレート(Templates)]** を選択し、 **[カスタムタグ(Custom Tags)]** を選択します。
3. 更新を完了します。

問題テンプレートのアップロードを通じて新しいカスタムタグを追加できます。これにより、たとえばソフトウェア監査に参加していないセキュリティチームのメンバーが、問題テンプレートおよび問題テンプレートのカスタムタグを定義できます。

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。

データ保持について

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

定義された保持時間の期間に達すると、アーティファクトはFortify Software Security Centerからのパージ対象となります。クリーンアップサービスをスケジュールして、Fortify Software Security Centerからアーティファクトをパージすることができます。

注意 アーティファクトがパージされると、そのアーティファクトはFortify Software Security Centerから永久に削除され、回復できません。

データ保持を有効にした場合、Fortify Software Security Centerはすべてのアプリケーションにデフォルトのデータ保持ポリシーを適用します。

また、デフォルトのデータ保持ポリシーからオプトアウトする個々のアプリケーションのバージョンを設定することもできます。

このセクションで説明するトピック:

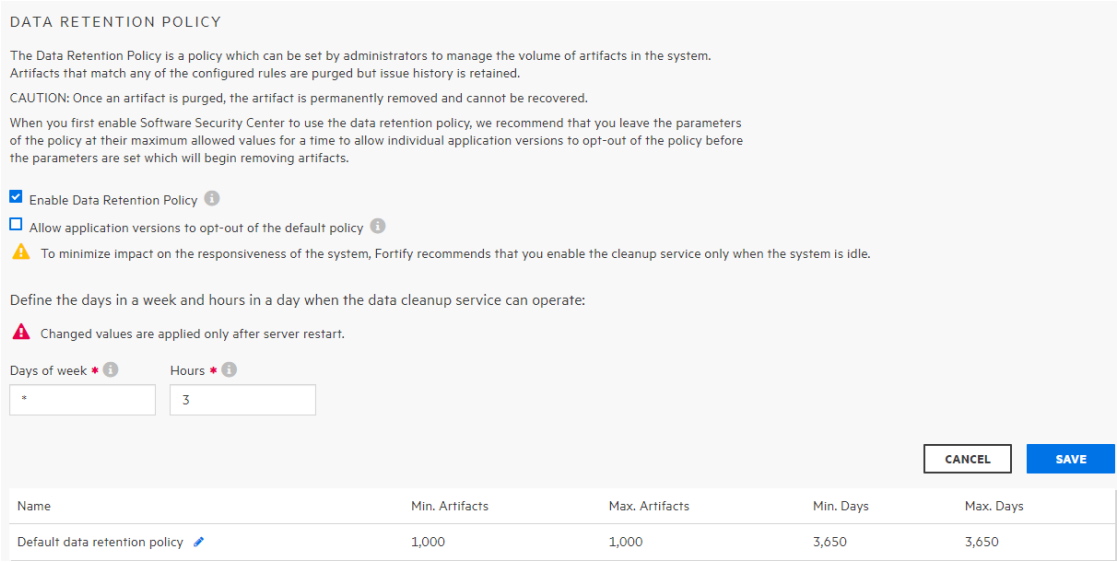
データ保持の有効化 298
デフォルトのデータ保持ポリシーの編集 302

データ保持の有効化

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

1. Fortify Software Security Centerに管理者としてログインして、 **管理者(Administration)**] タブをクリックします。
2. 左ペインの **ポリシー(Policies)**] で、 **データ保持ポリシー(Data Retention Policy)**] を選択します。

   データ保持ポリシー(Data Retention Policy)] ページには、デフォルトのデータ保持ポリシーと、データ保持ポリシーが適用されていないアプリケーションバージョンが一覧表示されます。



3. 次の表で説明するように、 [データ保持ポリシー(Data Retention Policy)] ページで設定を行います。

フィールド *必須	説明
データ保持ポリシーを有効にする(Enable Data Retention Policy)	このチェックボックスをオンにすると、データ保持機能が有効になります。
アプリケーションバージョンに、デフォルトポリシーのオプトアウトを許可する(Allow application versions to opt-out of the default policy)	このチェックボックスをオンにすると、個々のアプリケーションバージョンでデフォルトポリシーをオプトアウトできます。 詳細については、「"アプリケーションバージョンをデフォルトのデータ保持ポリシーからオプトアウトするための設定" ページ 264」を参照してください。
*曜日 (Days of week)	データクリーンアップサービスをスケジュールする曜日を1つ以上指定します。 次のように、1から7の値を使用して曜日を指定します。 1=日曜日、2=月曜日、3=火曜日、4=水曜日、5=木曜日、

フィールド *必須	説明
	6=金曜日、7=土曜日 次のいずれかのcron構文を使用して、1つ以上の曜日を指定します。 • 単一値: 週の1日のみデータクリーンアップを実行するには、1桁の数字を入力します。 たとえば、「3」と入力すると、火曜日にのみ [時間(Hours)] フィールドで定義された指定時間にデータクリーンアップが実行されます。 • 複数値: 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、「1,4,6」と入力すると、日曜日、水曜日、金曜日の [時間(Hours)] フィールドで定義された指定時間にクリーンアップサービスが実行されます。 • 値の範囲: 連続する曜日を入力するには、エントリをダッシュで分離します。たとえば、2-6と入力すると、月曜日から金曜日の [時間(Hours)] フィールドで定義された指定時間にクリーンアップサービスが実行されます。 • 毎日: 「*」アスタリスク([*)を入力すると、毎日、 [時間(Hours)] フィールドで定義された指定時間にクリーンアップサービスがスケジュールされます。 **注:** Fortifyでは、システム応答性への影響を最小限に抑えるために、システムがアイドル状態の場合にのみクリーンアップサービスを有効にすることを強くお勧めします。
*時間(Hours)	データクリーンアップサービスを実行する時間を選択できます。 0から23の値を使用して時刻を指定します。24時間表記を使用し、0は午前0時、23は午後11時を表します。 次のいずれかのcron構文を使用して、1日のうち1時間またはそれ以上を指定します。 • 単一値: 特定の時間にのみデータクリーンアップを実行するには、1桁の数字を入力します。 たとえば、「3」と入力すると、 [曜日(Days of week)] フィー

フィールド *必須	説明
	ルドで定義された指定日の午前3時にのみデータクリーンアップが実行されます。 • 複数値: 複数の時間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、2,4,6,18,20,22と入力すると、[曜日(Days of week)]フィールドで定義された指定日の午後6時から午前6時までの偶数時にデータクリーンアップサービスが実行されます。 • 値の範囲: 1日の連続した時間帯にスケジューラを実行するには、エントリをダッシュで分離します。 たとえば、0-6と入力すると、[曜日(Days of week)]フィールドで定義された指定日の午前0時から午後6時まで、1時間ごとにデータクリーンアップサービスが実行されます。 • 複数の範囲/値: 1日のうちの複数の連続した時間帯、または1日のうちの連続する時間帯と特定の時間にスケジューラを実行するには、複数の範囲または値をカンマで区切ります。 たとえば、0-5,17-23と入力すると、[曜日(Days of week)]フィールドで定義された指定日の午後5時から午前5時まで、1時間ごとに、データクリーンアップサービスが実行されます。 たとえば、0-5,12,18-20,23と入力すると、[曜日(Days of week)]フィールドで定義された指定日の午後11時から午前5時の1時間おきと、午後0時、および午後6時から午後8時の1時間おきにデータクリーンアップサービスが実行されます。 • 毎時: アスタリスク(*)を入力すると、[曜日(Days of week)]フィールドで定義された指定日の1時間おきに、データクリーンアップサービスがスケジュールされます。 **注:** Fortifyでは、システム応答性への影響を最小限に抑えるために、システムがアイドル状態の場合にのみクリーンアップサービスを有効にすることを強くお勧めします。

4. [保存(SAVE)]をクリックします。

デフォルトのデータ保持ポリシーの編集

Software Security Centerで初めてデータ保持ポリシーの使用を有効にする場合、Fortifyでは、ポリシーのプロパティで、ポリシーがアーティファクトの削除を開始するよう指示するまで個々のアプリケーションバージョンがポリシーをオプトアウトできる時間の設定を、許容されている最大値のままにしておくようお勧めします。

独自の要件に基づいて、デフォルトのデータ保持ポリシーを編集できます。

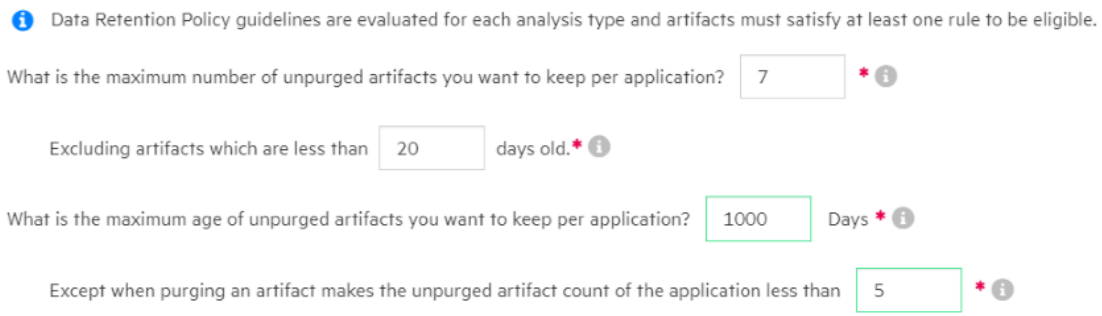
デフォルトのデータ保持ポリシーを編集するには:

1. **[データ保持ポリシー(Data Retention Policy)]**ページで、**[デフォルトのデータ保持ポリシー(Default Data Retention Policy)]**をクリックして展開し、**[ポリシーの編集(Edit Policy)]**をクリックします。
2. **[ポリシーの編集(Edit Policy)]**ダイアログボックスで、要件に基づいて次の設定を行います。

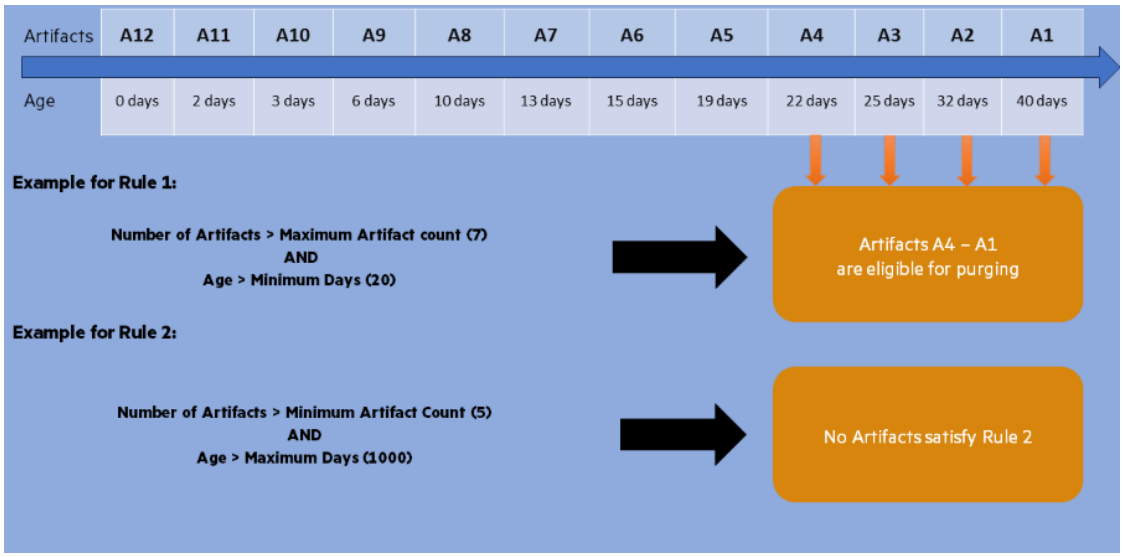
> **注:** デフォルトのデータ保持ポリシー下でのアーティファクトのパージは、次の2つのルールの効果に依存します。デフォルトのデータ保持ポリシー下でのアーティファクトのパージは、次の2つのルールの効果に依存します。
>
> - ルール1: アーティファクトの数>未パージのアーティファクトの最大数かつアーティファクトの保存時間>アーティファクトの最小保存時間
> - ルール2: 保存時間>最長保存期間かつアーティファクトの数>未パージのアーティファクトの最小数
>
> データ保持ポリシーのガイドラインは分析タイプごとに評価され、アーティファクトがパージの対象となるには、少なくともルールのうち1つを満たす必要があります。どちらのルールも満たされていない場合、アーティファクトの数や保存期間に関して指定した最大値に関係なく、アーティファクトは保持されます。

シナリオの例:

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



次の図は、デフォルトのデータ保持ポリシー下でアーティファクトがどのようにパージ対象となるかを例示しています。



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

3. **[保存(SAVE)]**をクリックします。

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、[ダッシュボード(Dashboard)]ページおよび[アプリケーション(Applications)]ページに表示されないようにしたい場合、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" 下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" ページ305

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。
2. 選択したバージョンの [監査(AUDIT)]ページで、 **[プロファイル(PROFILE)]**をクリックします。
3. [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスで、 **[アプリケーション設定(APPLICATION SETTINGS)]**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. [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスを閉じます。

参照情報

"アプリケーションバージョンの再有効化" 下

"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、 [ダッシュボード(Dashboard)]または [アプリケーション(Applications)]ビューに一覧表示されていない場合は、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。

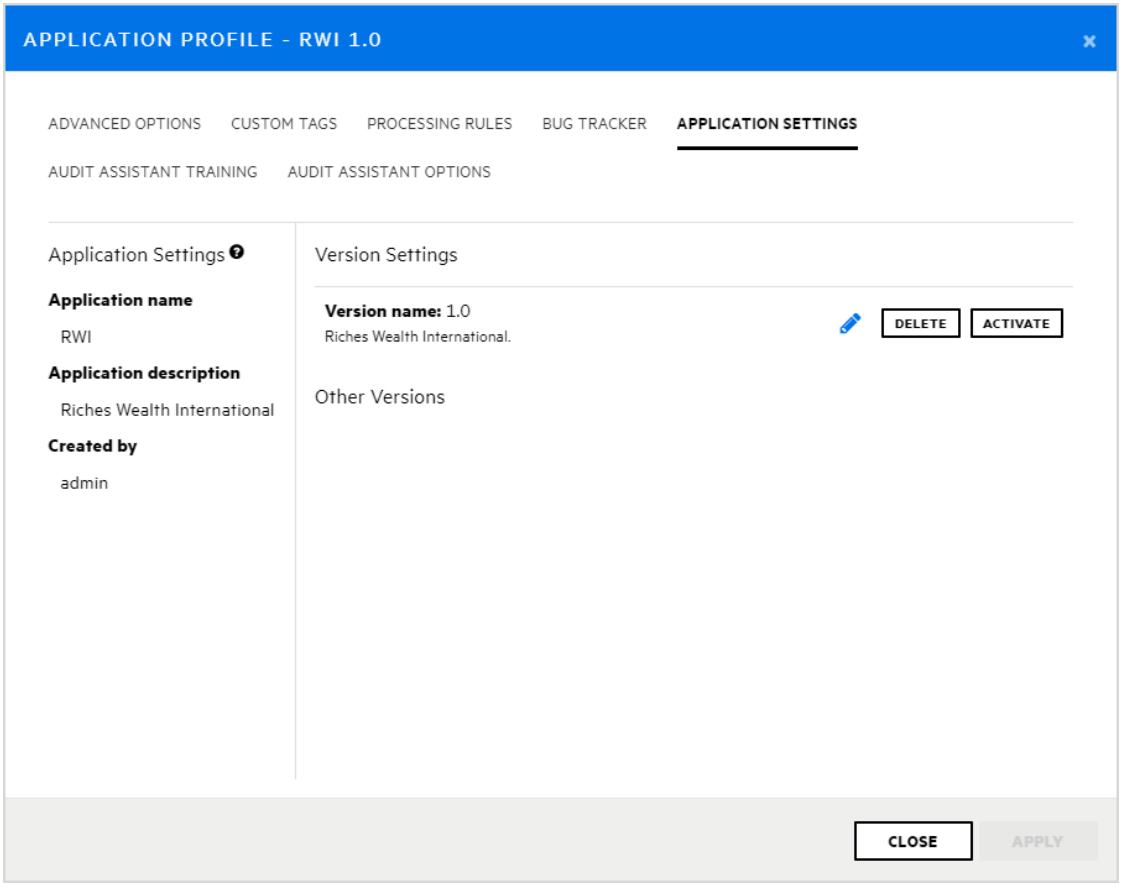
無効化されたアプリケーションバージョンが、アプリケーションの唯一存在するバージョンだった場合は、次の操作を実行して、アプリケーションにアクセスして再度有効にできます。

- 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. OpenTextのヘッダで、 **[アプリケーション(Applications)]**をクリックします。
2. **[非アクティブなバージョンの表示(Show inactive versions)]**チェックボックスをオンにします。
3. 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。
4. [監査(AUDIT)]ページのアプリケーションバージョンツールバーで、 **[プロファイル(PROFILE)]**をクリックします。

5. [アプリケーションプロファイル - <application_version> (APPLICATION PROFILE - *<application_version>*)] ダイアログボックスで、 **[アプリケーション設定 (APPLICATION SETTINGS)]** タブを選択します。



6. **[有効化 (ACTIVATE)]** をクリックします。
   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" ページ303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 307
Webhookの作成 308
Webhookを編集する 313
Webhookペイロードの表示 313
Webhookペイロードの再配信 316
Webhookの削除 317

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. OpenTextのヘッダで、 **管 理 (Administration)**] を選 択します。
2. 左 ペインで、 **ユーザ(Users)**] 、 **役 割 (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

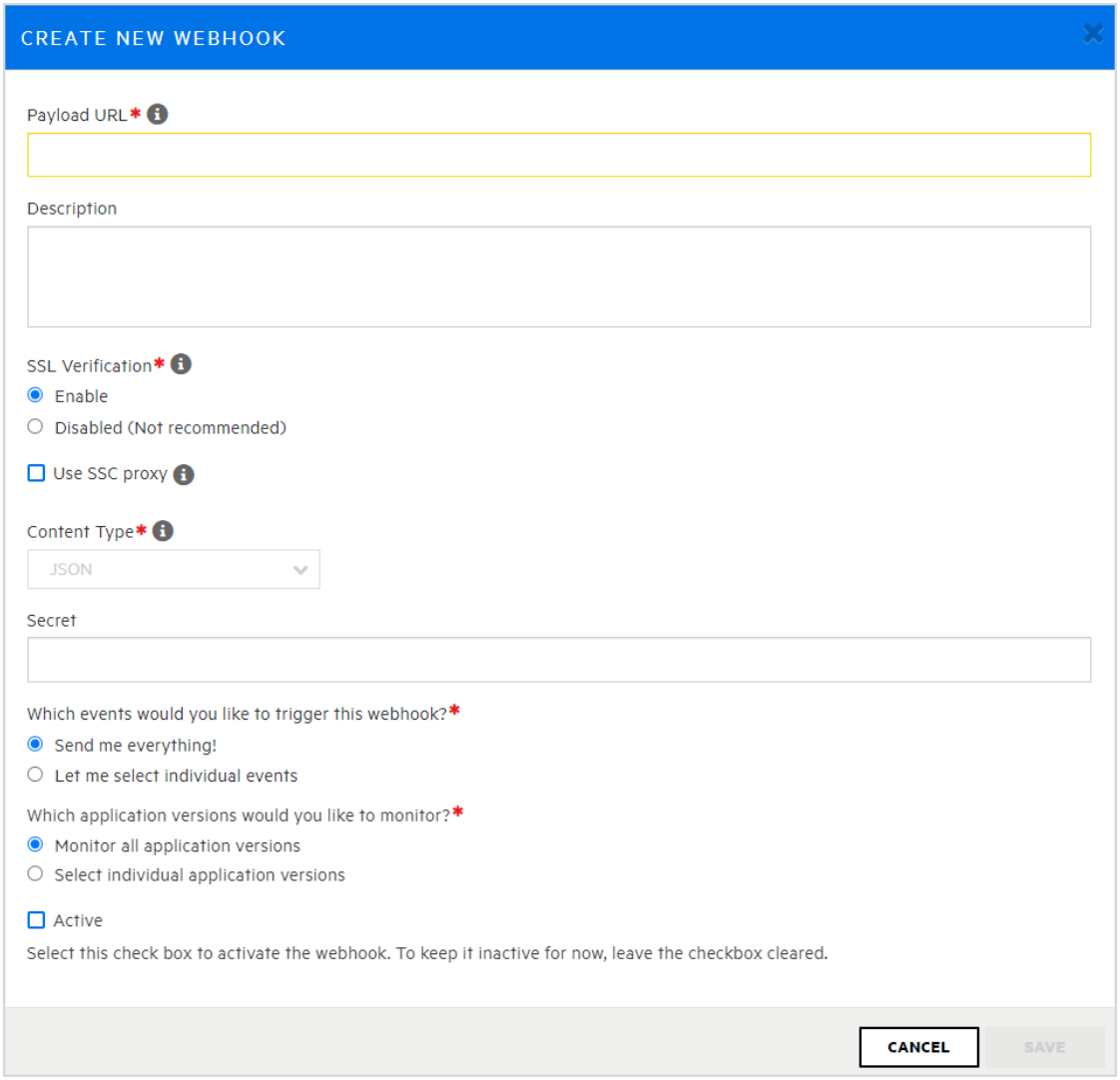
管 理 者 はWebhookを作 成 して、グローバルかアプリケーションバージョン固 有 かに関 係 なくあらゆる種 類 のイベントを監 視 できます。セキュリティリードは、表 示 する許 可 を持 つエンティティのイベントを監 視 するWebhookを作 成 できます。

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. 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、OpenTextのヘッダで **管 理 (Administration)**] をクリックします。
2. 左 ペインで、 **設 定 (Configuration)**] を選 択 してから、 **Webhook (Webhooks)**] を選 択 します。

   Webhook (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統合のプロキシの設定" ページ132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)。 • 注目しているイベントのサブセットをペイロードに含めるには、 **[個別イベントを選択する(Let me select individual events)]**を選択し、 **[グローバルイベント(Global Events)]**リストと **[アプリケーションバージョンイベント(Application version events)]**リスト(下記参照)で、ペイロードに含めるイベントのチェックボックスをオンにします。

フィールド	説明
グローバルイベント(システム全体) USER_CREATED: 新しいローカルユーザ、ローカルグループ、またはLDAPエンティティがFortify Software Security Centerに追加されました。 USER_DELETED: ローカルユーザ、ローカルグループ、またはLDAPエンティティがFortify Software Security Centerから削除されました。 USER_UPDATED: ローカルユーザ、ローカルグループ、またはLDAPエンティティが更新されました。 LOCAL_USER_ACCOUNT_LOCKED: 無効な資格情報によるログイン試行が多すぎるため、Fortify Software Security Centerからローカルユーザがロックアウトされました。 APP_VERSION_CREATED: SSCで新しいアプリケーションバージョンが作成されました。 APP_VERSION_DELETED: Fortify Software Security Centerからアプリケーションバージョンが削除されました。 REPORT_GENERATION_COMPLETE: 要求された新しいレポートを表示およびダウンロードできます。 REPORT_GENERATION_REQUESTED: 新しいレポートが要求されました。 **アプリケーションバージョンイベント(アプリケーションバージョン固有)** ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS: アップロードされたアーティファクトの処理がFortify Software Security Centerに対して正常に行われ、そのデータが使用可能です。 ANALYSIS_RESULT_UPLOAD_FAILURE: アップロードされたアーティファクトは正常に処理されませんでした。 ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL: アップロードされたスキャンアーティファクトを処理するには承認が必要です。 ANALYSIS_RESULT_INDEXING_COMPLETED: Fortify Software Security Centerがアップロードされたの処理を終了した後に、グローバル検索のためのデータのインデックス付けが完了しました。 ANALYSIS_RESULT_UPLOAD_APPROVE: アーティファクトのアップロードが承認されました。 APP_VERSION_UPDATED: [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスからアプリケーションバージョンが更新されました。	
アプリケーションバージョンイベント	

フィールド	説明
ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS: 分析結果が正常にアップロードされました。 ANALYSIS_RESULT_UPLOAD_FAILURE: 分析結果のアップロードに失敗しました。 ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL: 分析のアップロードには承認が必要です。 ANALYSIS_RESULT_INDEXING_COMPLETED: 分析結果のインデックス付けが完了しました。 ANALYSIS_RESULT_UPLOAD_APPROVED: 分析のアップロード結果が承認されました。 APP_VERSION_UPDATED: アプリケーションのバージョンが更新されました。	
監視対象のアプリケーションバージョン (Which application versions would you like to monitor?)	次のいずれかを実行します。 • すべてのアプリケーションバージョン(既存のアプリケーションバージョンと今後作成されるアプリケーションバージョン)を監視するには、 [Monitor All Application Versions] オプションを選択します。 • アプリケーションバージョンのサブセットのみを監視するには、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

フィールド	説明
	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" 下

"Webhookの削除" ページ317

Webhookを編集する

Webhookを編集するには:

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、OpenTextのヘッダで [管理(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. 左ペインで、 [設定(Configuration)]を選択してから、 [Webhook (Webhooks)]を選択します。

   [Webhook (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308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" 下

"Webhookの作成" ページ308

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. 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、OpenTextのヘッダで [管理(Administration)]をクリックします。
2. 左ペインで、 [設定(Configuration)]を選択してから、 [Webhook (Webhooks)]を選択します。

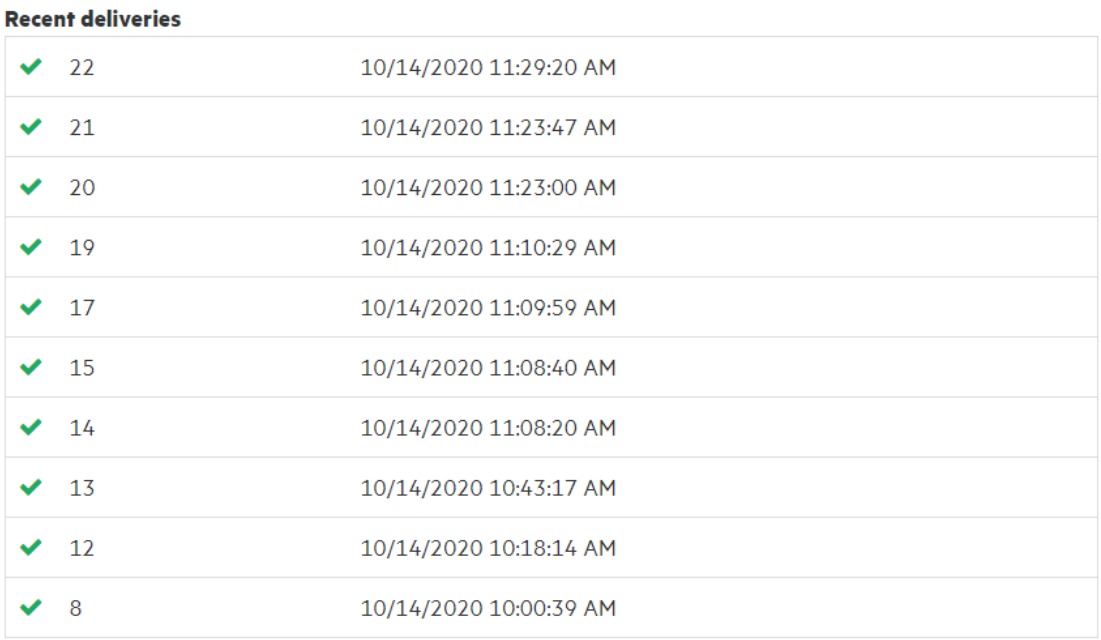
   Webhookテーブルには、次のように既存のすべてのWebhookのリストと、それぞれのステータスが表示されます。

   ✓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。

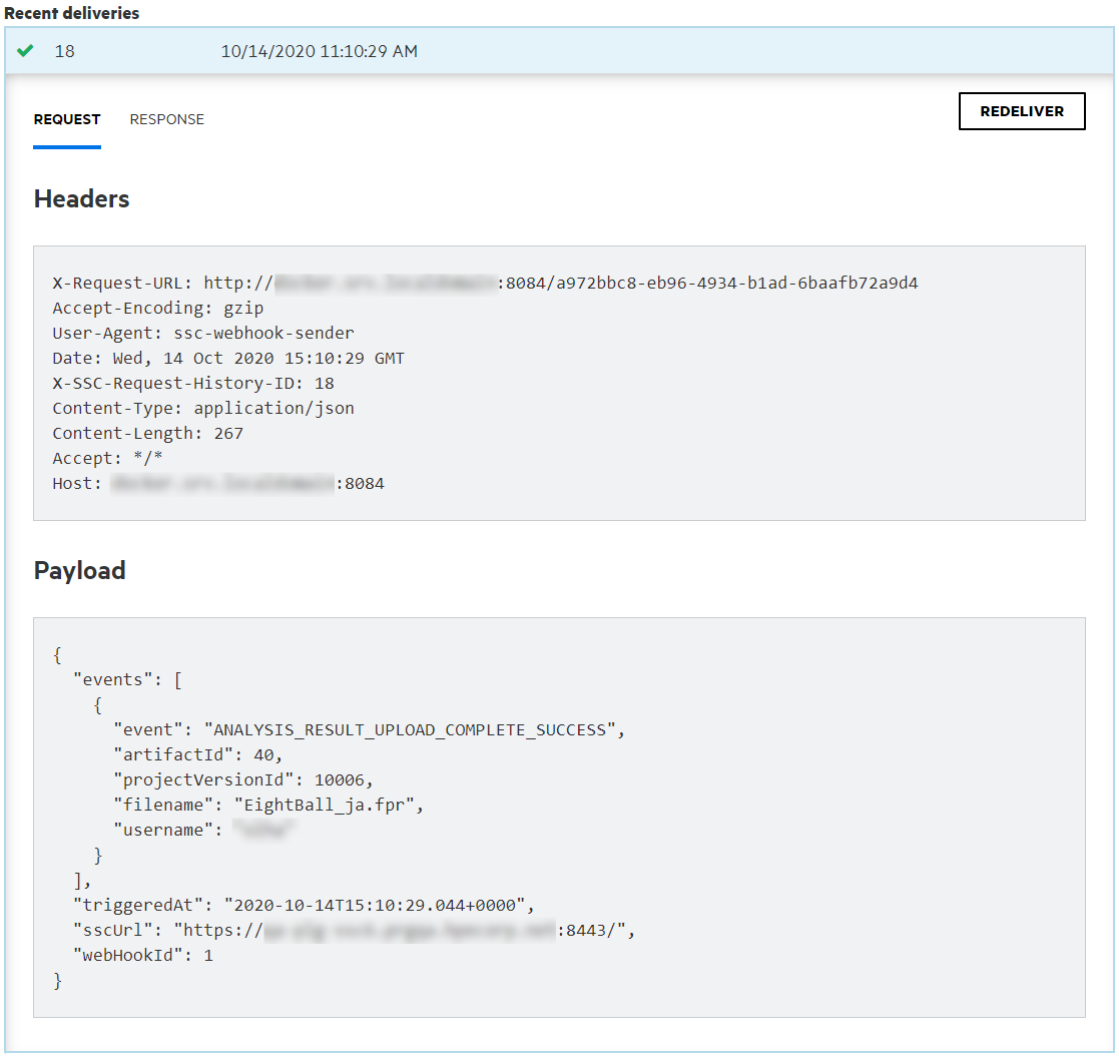
   注: リストに表示されたWebhookの [Status]フィールドにアイコンが表示されない場合は、Webhookテーブルでその行を展開し、 [Recent deliveries]テーブルの上にある [Active]チェックボックスが選択されていることを確認します。

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)。

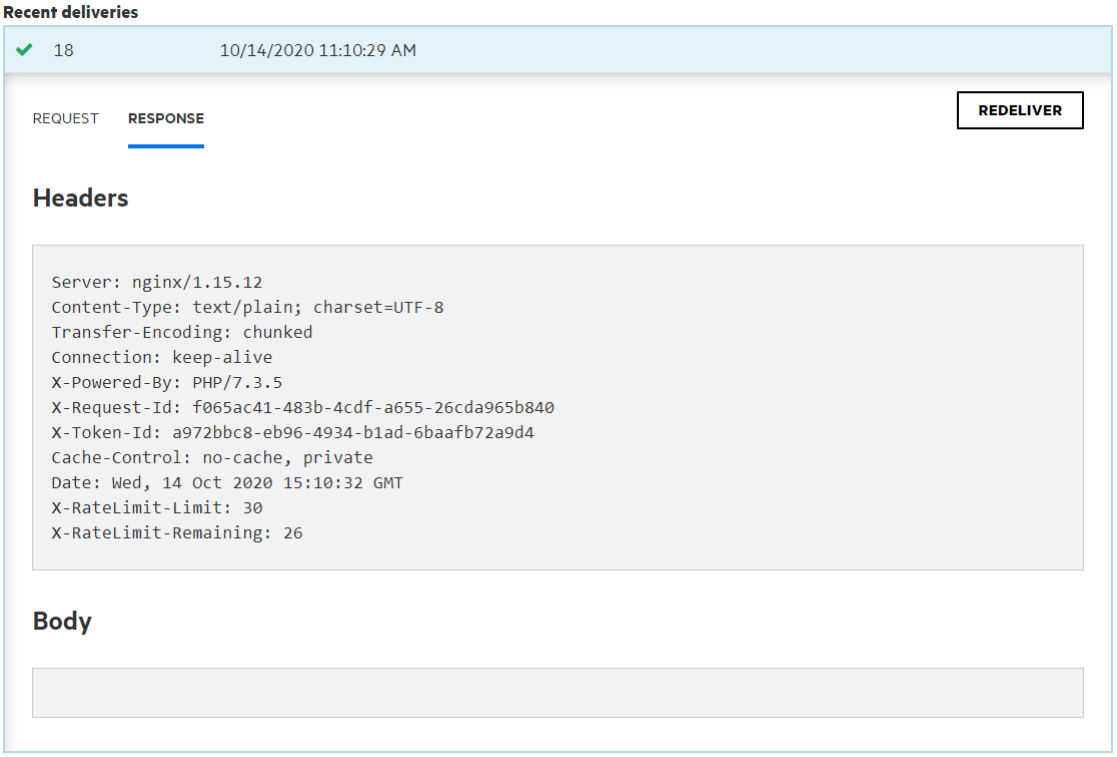


[Recent deliveries]には、最近配信されたペイロード(最大10個)のリストが表示されます。

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477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308

"Webhookを編集する" ページ313

Webhookペイロードの再配信

WebhookのペイロードURLに配信されるペイロードに影響する変更が行われた場合、ペイロードの再配信を要求できます。

Webhookペイロードの再配達を要求するには、次の手順に従います。

1. 管理者またはセキュリティリードとしてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(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. 左ペインで、 **設定(Configuration)**] を選択してから、 **Webhook (Webhooks)**] を選択します。

[Webhook (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308

"Webhookを編集する" ページ313

"Webhookペイロードの表示" ページ313

Webhookの削除

Webhookを削除するには、次の手順を実行します。

1. 管理者またはセキュリティリードとしてFortify Software Security Centerにログインし、OpenTextのヘッダで [管理(Administration)] をクリックします。
2. 左ペインで、 [設定(Configuration)] を選択してから、 [Webhook (Webhooks)] 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308

"Webhookを編集する" ページ313

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 318
変 数の作 成 319
変 数の構 文 319
パフォーマンスインジケータ 320
パフォーマンスインジケータの作 成 320
アラート定 義 321
アラートの作 成 322
アラートを編 集する 325
アラートの削 除 325
アラートの表 示とマーク 325

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、 **管理(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。
4. [新しい変数の作成(CREATE NEW VARIABLE)]ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明
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
```

`operator`には、標準的な数学演算子(+、-、*、/)、比較演算子(==、>、<)、三項演算子(?)を使用できます。

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、 **管理(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。
4. [新しいパフォーマンスインジケータの作成(CREATE NEW PERFORMANCE INDICATOR)] ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明
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` `operator`には、標準的な数学演算子(`+`、`-`、`*`、`/`)、比較演算子(`==`、`>`、`<`)、三項演算子(`?`)を使用できます。
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102
"アラートの削除" ページ325

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:

1. OpenTextのヘッダで、 **管理(Administration)**] をクリックします。
2. 左側のペインで、 **テンプレート(Templates)**] をクリックしてから、 **アラート(Alerts)**] を選択します。
   アラート(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. **アラート(Alerts)**] ツールバーで **新規(NEW)**] をクリックします。
4. **新しいアラートの作成(CREATE NEW ALERT)**] ダイアログボックスの **名前(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) **説明(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、 **アラートを有効にする(Enable Alert)**] チェックボックスをオフにします。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. **タイプ(Type)**] の横で、作成するアラートのタイプを選択します。

   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. **受信者(Recipients)**] の横で、次のいずれかを実行します。
   - アラートを自分にのみ送信するには、 **自分のみ(Me only)**] オプションを選択したままにします。
   - アプリケーションバージョンの割り当て先ユーザに割り当てられたユーザにアラートを送信するには、 **バージョンの割り当て先ユーザ(Version assignees)**] オプションを選択します。
   - (スケジュールされたアラートの場合のみ)アラートをすべてのFortify Software Security Centerユーザに送信するには、 **すべてのシステムユーザ(All system users)**] を選択します。

   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. [いつアラートを送信するか(Alert when)]リストから、パフォーマンスインジケータを選択します。
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 [いつアラートを送信するか(Alert when)]に設定された条件を満たすと、パフォーマンスインジケータアラートが1回だけトリガされます。たとえば、トリガ条件が [Critical Exposure Issues < 50]に設定されたアラートは、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。
    b. [アプリケーションバージョンの選択(SELECT APPLICATION VERSION)]ダイアログボックスの[アプリケーション(APPLICATION)]リストから、アラートを使用するアプリケーションを選択します。
    [バージョン(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102

"アラート定義" ページ321

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. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで [**管理(Administration)**] をクリックします。
2. 左側のペインで、 [**テンプレート(Templates)**] をクリックしてから、 [**アラート(Alerts)**] を選択します。
   [アラート(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、OpenTextのヘッダで [**管理(Administration)**] を選択します。
2. 左側のペインで、 [**テンプレート(Templates)**] を選択してから、 [**アラート(Alerts)**] を選択します。
   [アラート(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321

"アラートの作成" ページ322

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OpenText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。

- OpenText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リスト(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399を参 照 してください。

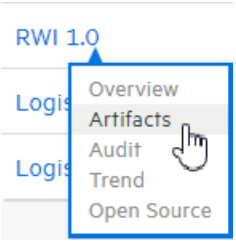
注 : Fortify Software Security Centerがデータベースにデータを追 加 すると、100,000文 字 を超 えるHTTP応 答 が切 り捨 てられます。このような応 答 は、最 後 が切 れているか、応 答 の他 の場 所 に`\n\n...\n\n`が含 まれるかのいずれかです。これは、ダウンロードされたスキャンには影 響 を及 ぼしません。これは、Fortify Software Security Centerの [AUDIT] ページに表 示 されるデータにのみ影 響 します。

重 要 Fortify Software Security Centerにアップロードするファイルは2 GB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177を参 照 してください。

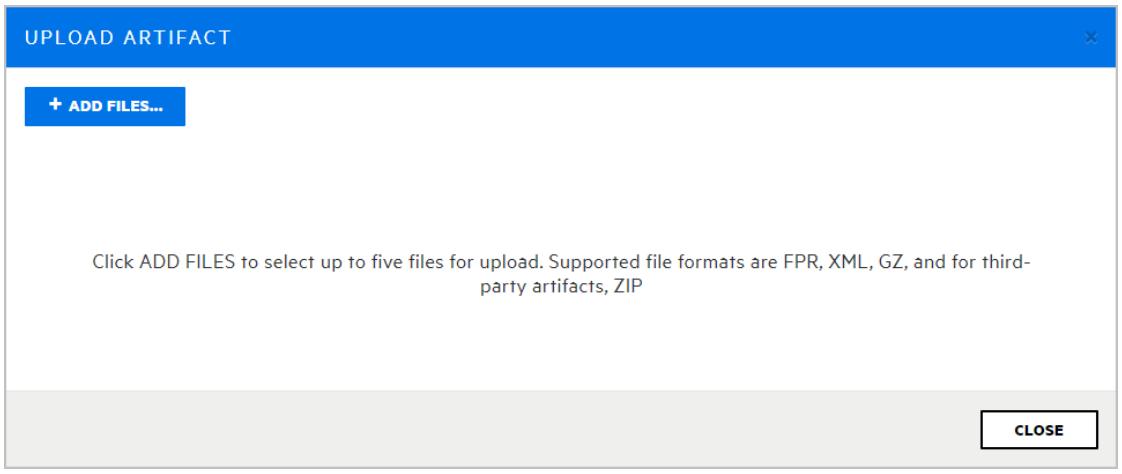
スキャンアーティファクト をFortify Software Security Centerデータベースにアップロードするには、次 の手 順 に従 います。

1. ダッシュボードで、または新 しいアプリケーションの場 合 は [アプリケーション (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 してから、ショートカットメニューから **[アーティファクト (Artifacts)]** を選 択 します。

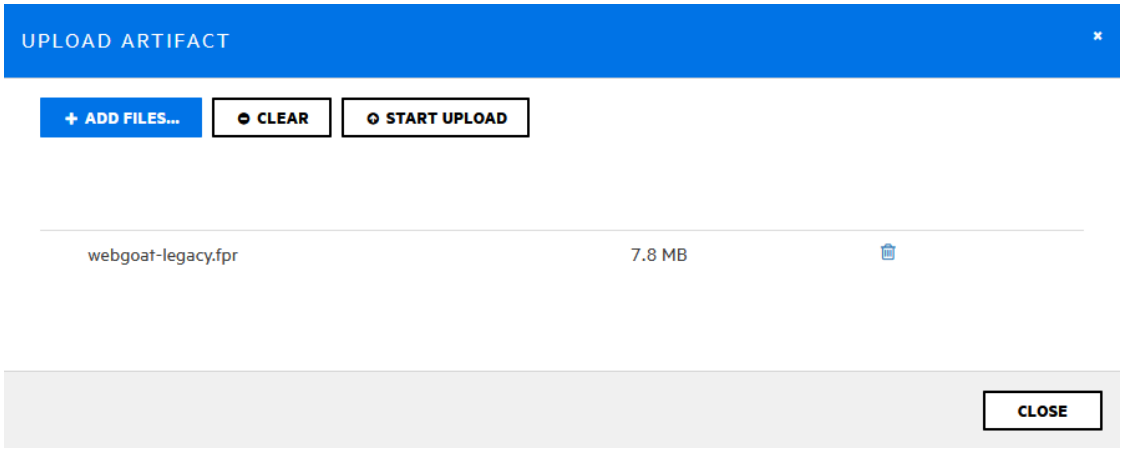


2. **[アーティファクト 履 歴 (ARTIFACT HISTORY)]** テーブルには、アプリケーションバージョン用 にアップロードされたスキャンアーティファクト すべてが一 覧 にされます。

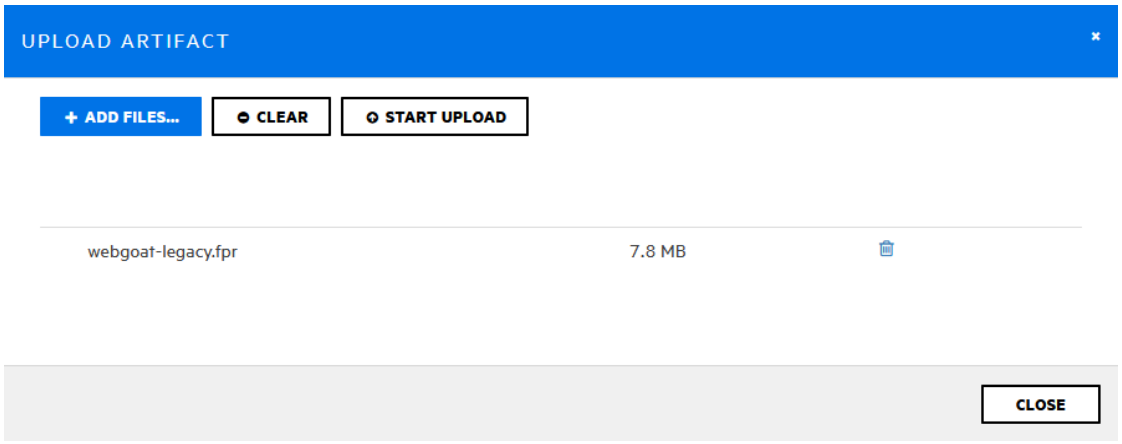
3. [ARTIFACT] をクリックします。



4. [アーティファクト のアップロード (UPLOAD ARTIFACT)] ダイアログボックスで、 **[+ファイルの追 加 (+ADD FILES)]** をクリックします。
5. アップロード する1つ以 上 (最 大 5つ)のアーティファクト ファイルに移 動して選 択します。



SonatypeまたはDebrickedのサード パーティパーサが有 効 になっている場 合 は、リスト からアーティファクト タイプを選 択 できます。



6. [アーティファクトのアップロード(UPLOAD ARTIFACT)]ダイアログボックスに、選択したファイルが一覧表示されます。
7. 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。
8. [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。
9. 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332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331

"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275

"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457

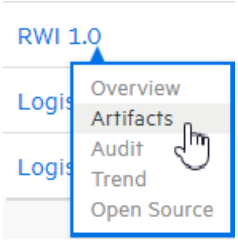
"アプリケーション名とバージョンを使用したFPRファイルのアップロード" ページ457

スキャンアーティファクトの詳細の表示

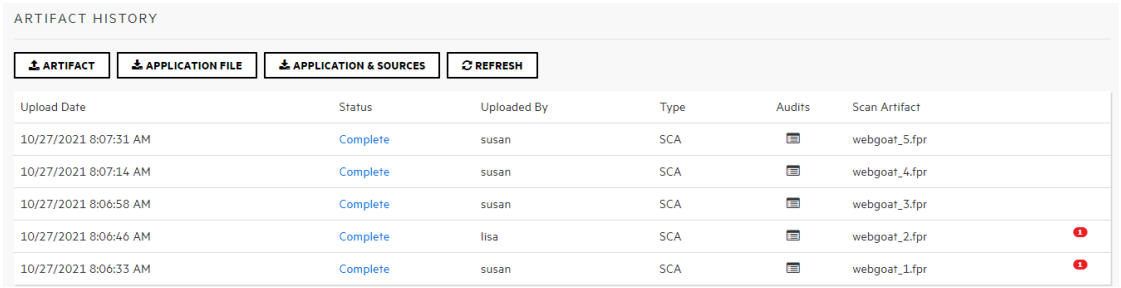
次の手順では、アップロードされたスキャンアーティファクトについて利用可能な詳細について説明します。(スキャンアーティファクトのアップロード方法については、"スキャンアーティファクトのアップロード" ページ327を参照してください)。

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。

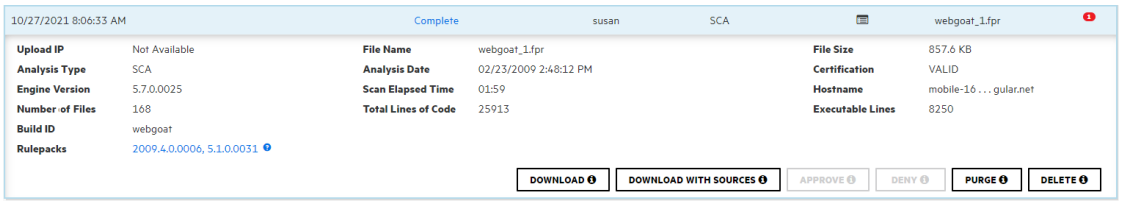
1. [Dashboard] または [Applications] ビューで、アーティファクトの詳細を表示するアプリケーションバージョンにカーソルを移動し、ショートカットメニューから **Artifacts**]を選択します。



[**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。

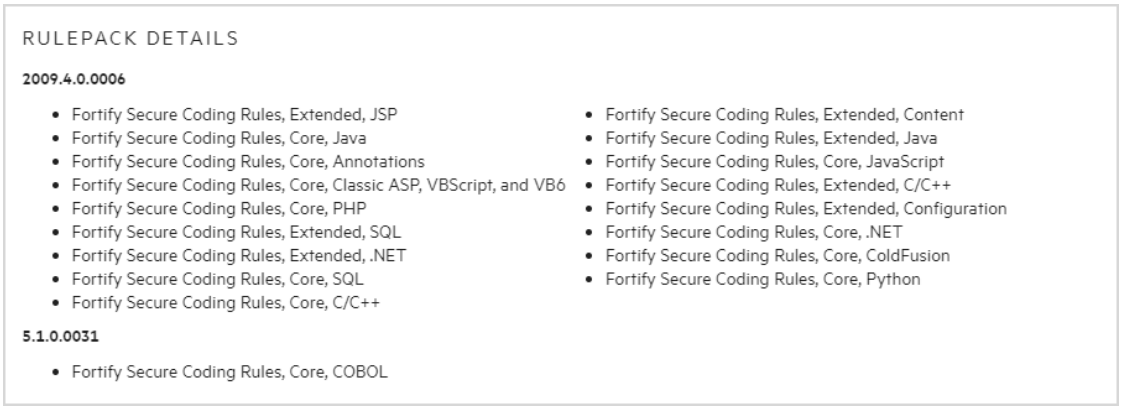
アップロードされたアーティファクトの処理中にエラーが発生した場合は、[**ARTIFACT HISTORY**] テーブルの [**Status**] 列に [**Error Processing**] と表示されます。右側の数字は、違反した処理ルールの数を示します。

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339

"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275

"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457

"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457

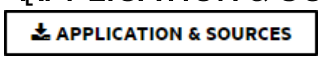
スキャンアーティファクトをダウンロードする

[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. OpenTextのヘッダで、 [アプリケーション(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、 [ダウンロード(Downloads)]フォルダで、ダウンロードされたFPRファイルをダブルクリックします。

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. OpenTextのヘッダで、 [アプリケーション(Applications)]をクリックします。
2. 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

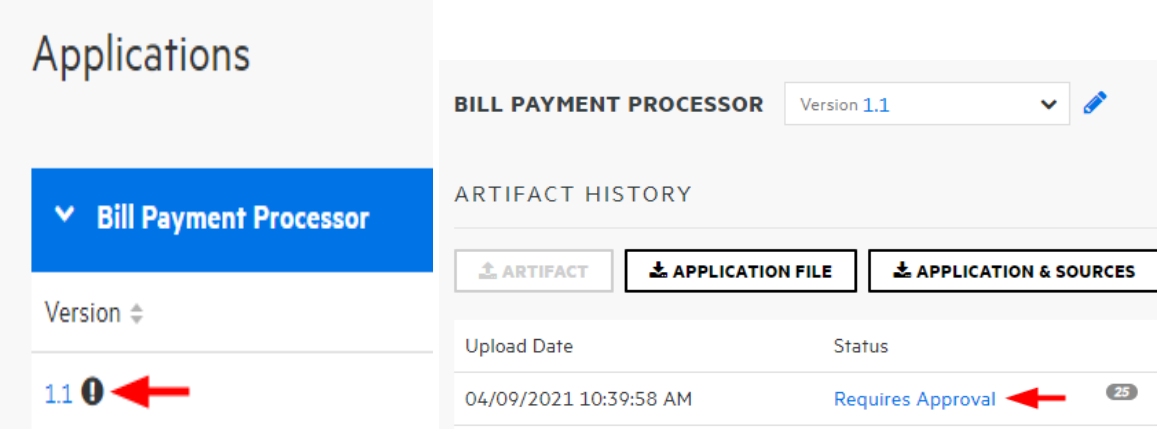
"スキャンアーティファクトのアップロード" ページ327

"アーティファクトの削除" ページ341

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275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。

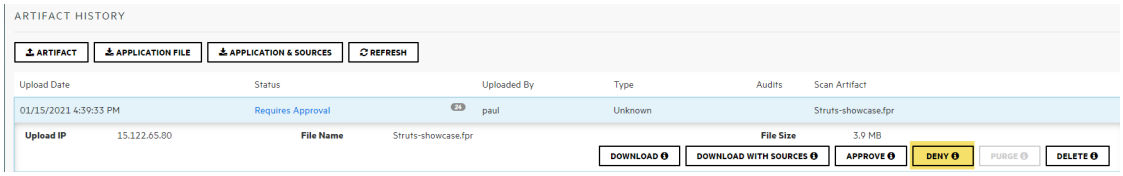
Fortify Software Security Center でアーティファクトの処理が続行されます。

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。

- OpenTextのヘッダで、 [ダッシュボード(Dashboard)]を選択します。

[問題統計(Issue Stats)]ページ(Fortify Software Security Centerのデフォルトの [ダッシュボード(Dashboard)]ビュー)の次の3つのポートレットには、ユーザが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。

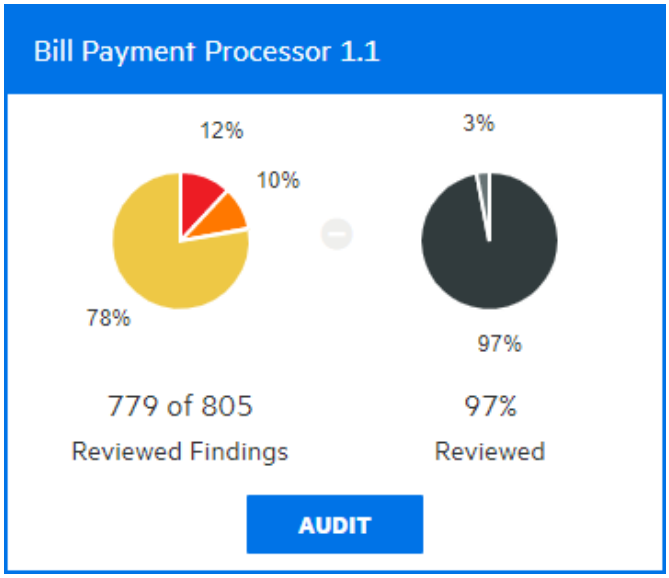
ポートレットとテーブルを同時に使用すると、どのくらい迅速に問題が確認および修正されるのかを確認できます。

[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。

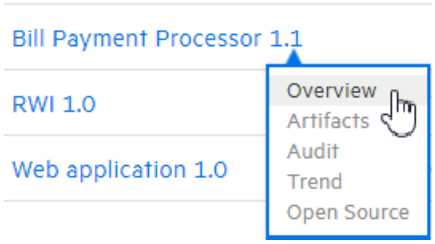


Fortify Software Security Centerに、バージョンのサマリ結果が表示されます。この例では、左側の円グラフに、このアプリケーションバージョンについて現在までに監査された結果の97%(779/805)のセキュリティ評価が表示されています。右側のグラフには、監査された結果の割合(97)と、まだ監査されていない結果の割合(3)が表示されています。

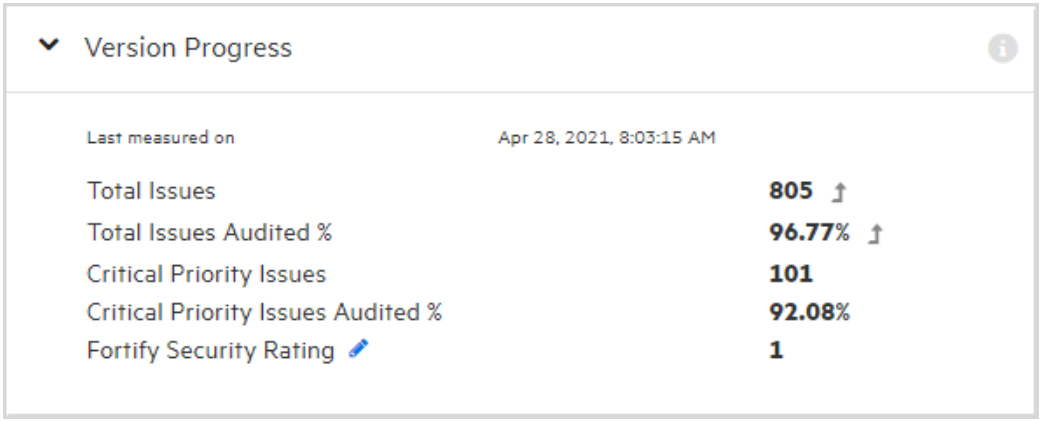
注: アプリケーションバージョンの [AUDIT] ページに移動するには、 [AUDIT] をクリックします。

[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。



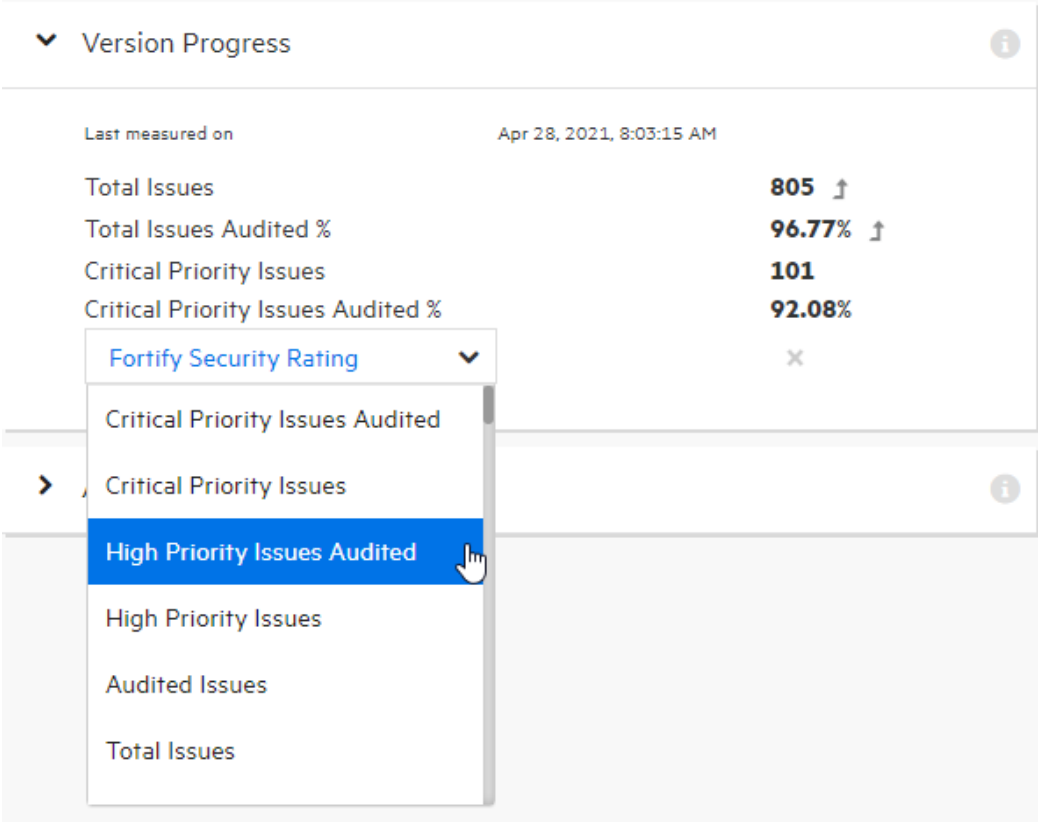
1. Fortifyのダッシュボードで、目的のバージョンのリンク上にカーソルを合わせ、ショートカットメニューから [**Overview**] を選択します。
2. [**Overview**] ページで、右側のペインが折りたたまれている場合は拡大します。



[**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。



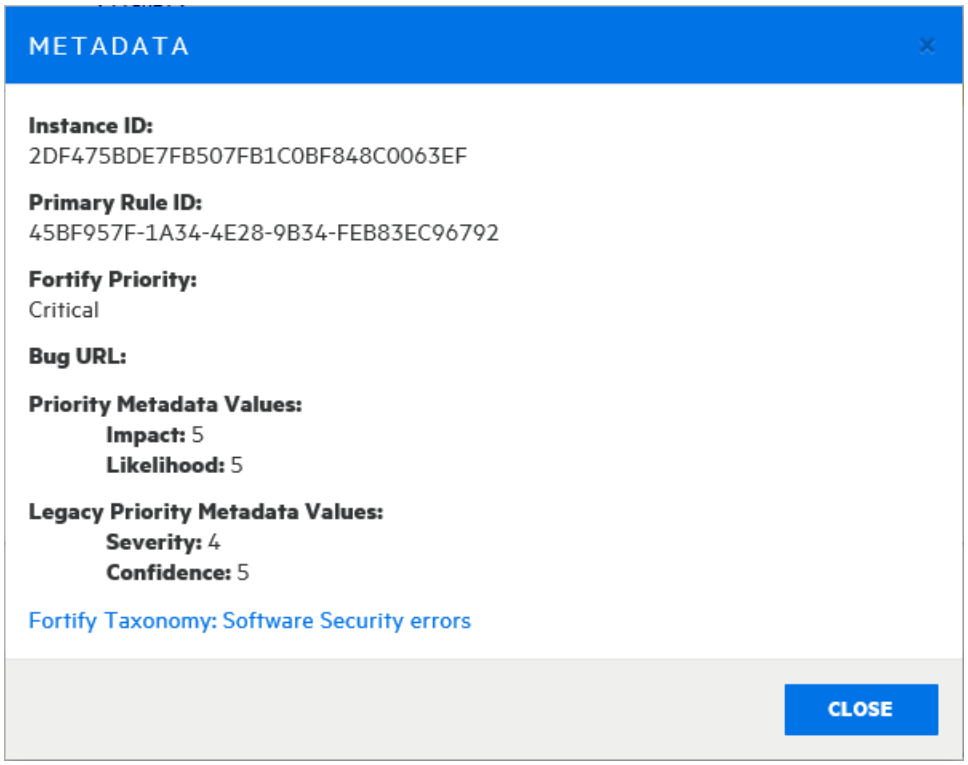
参照情報

"スキャン結 果 の監 査 " ページ358

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、『*OpenText™ 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、OpenTextのヘッダで **[管理(Administration)]** タブをクリックします。
2. 左ペインの **[メトリックとトラッキング(Metrics & Tracking)]** で、 **[ルールパック(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。
4. [Rulepackのインポート(IMPORT Rulepack)] ダイアログボックスで、 **[+ファイルの追加(+ADD FILES)]** をクリックします。
5. ドキュメントに移動して選択し、 **[アップロード開始(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それらに影響を及ぼすかどうかを確認してください。
- パージすると、分析日が同じか、それより前のアーティファクトがすべて削除されます。

次のすべての条件を満たすアーティファクトをパージできます。

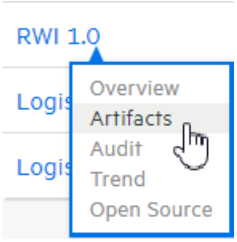
- まだパージされていない。
- 特定の分析エンジンタイプから生成されたスキャンが1つだけ入っているのではない。たとえば、アプリケーションバージョンに対してFortify Static Code Analyzerによって生成されたアーティファクトが1つしか存在しない場合は、パージできません。同じ分析エンジンからの2つのアーティファクトがアプリケーションバージョン用にアップロードされた場合は、その2つのアーティファクトのうちの古い方だけをパージできます。
- ステータスが次のいずれかである。

- PROCESS_COMPLETE
- ERROR_PURGING
- ERROR_DELETING

次 の場 合 は、アーティファクトをパージできません。

- 処 理 中 である。
- 処 理 中 にエラーが発 生 した。
- 分 析 エンジンタイプの最 新 のスキャンが含 まれている。

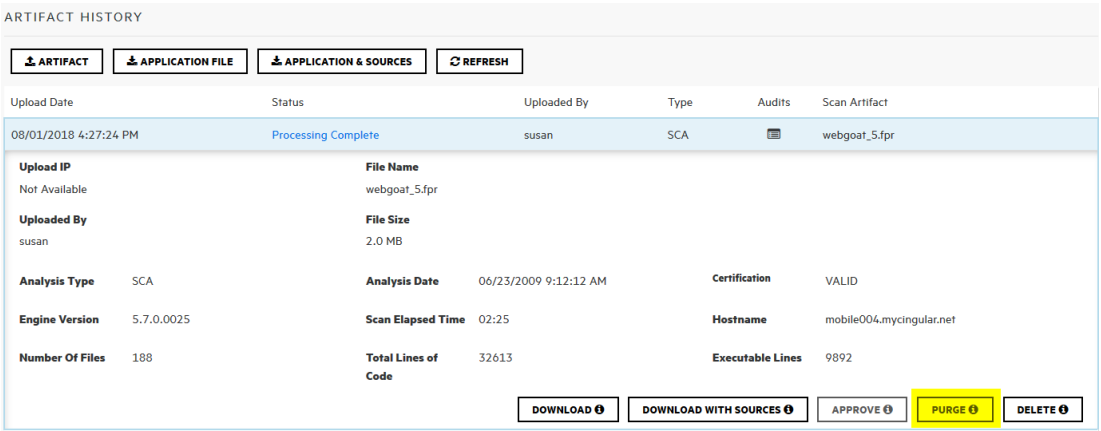
Fortify Software Security Centerデータベースからスキャンアーティファクト をパージするには、次 の手 順 に従 います。



1. [ダッシュボード (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 [**アーティファクト (Artifacts)**] を選 択 します。

   [**アーティファクト 履 歴 (ARTIFACT HISTORY)**] テーブルには、そのアプリケーション 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

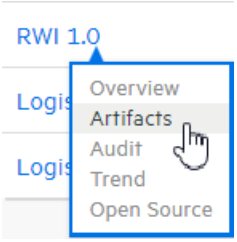
"アーティファクト の削 除" 下

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。

注 : 処 理 中 のアーティファクト やパージ済 みのアーティファクト は削 除 できません。

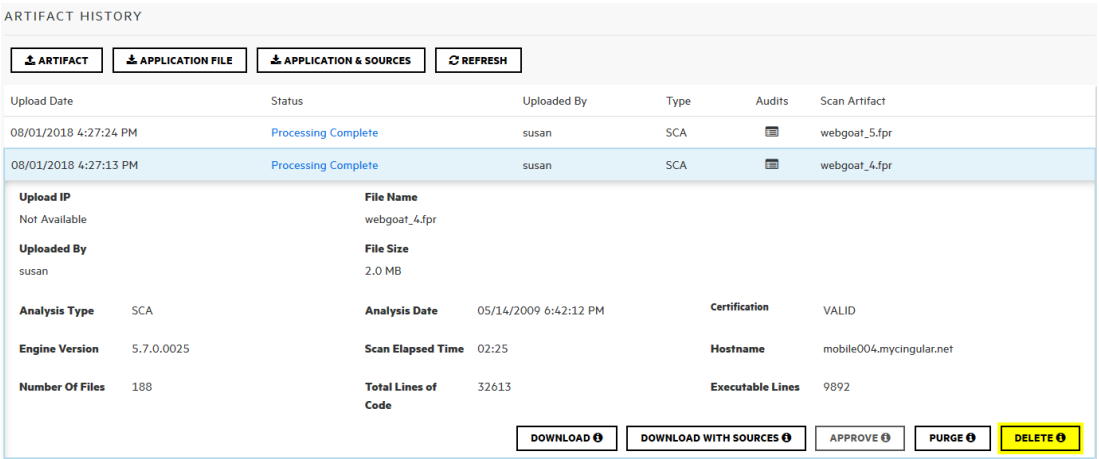
Fortify Software Security Centerデータベースからスキャンアーティファクト を削 除 するには:



1. [ダッシュボード (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 [アーティファクト (Artifacts)] を選 択します。

   [アーティファクト 履 歴 (ARTIFACT HISTORY)] テーブルには、そのアプリケーション 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339

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238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 345
監査する問題に関する情報の表示 345
フォルダに基づく問題の表示 347
ユーザに割り当てられた問題の表示 349
[OVERVIEW] および [AUDIT] ページに表示する問題をフィルタ処理する 349
問題の検索 352
検索修飾子 354
検索クエリの例 357
スキャン結果の監査 358
相関する問題の監査 366

抑止、削除、および非表示の問題について 367
フィルタセットを使用して表示問題を変更する 370
割り当てられた問題の優先度の上書き 371
問題に対して送信されたバグの表示 376
問題のバッチの監査 376
Audit Assistantの使用 377
Audit Assistantワークフロー 377
監査アシスタントについて 379
予測ポリシーについて 381
Fortify Audit Assistantの設定の更新 383
Audit Assistantの使用 384
Audit Assistantの設定 385
Fortify Audit Assistant認証トークンの取得 389
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 389
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 391
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 392
Audit Assistantの結果の確認 396
Audit Assistantのトレーニングについて 397
Fortify Software Security Centerでのグローバル検索 400
Webアプリケーションの被影響性分析について 402
被影響性分析の要件 402
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 403
オープンソースデータのエクスポート 404
Fortify Software Security CenterとFortify WebInspect Enterpriseの統合 405
Fortify Software Security CenterでのFortify WebInspectスキャン結果の表示 406
WebInspectの監査データ 408
誤検出 408
動的スキャン要求をFortify WebInspect Enterpriseに送信する 409
Fortify WebInspect Enterpriseの動的スキャン要求の処理 411
動的スキャン要求を編集およびキャンセルする 412
オープンソースデータの表示 413
監査(AUDIT)]ページからのオープンソースデータの表示 413
オープンソース(OPEN SOURCE)]ページからのオープンソースデータの表示 413

Debricked SBOMのダウンロード 415

現在の問題の状態について

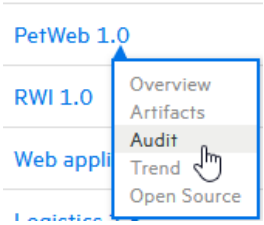
Fortify Software Security Centerでは、どの分析エンジン(アナライザ)があるアプリケーションバージョンの個々の問題を明らかにしたかを追跡し、新しい情報をアプリケーションバージョンの既存の結果本体にマージします。新しい監査情報がサーバにアップロードされたかまたは [AUDIT] ページに入力された後、Fortify Software Security Centerではその情報を特定の問題の既存の監査情報にマージします。また、Fortify Software Security Centerでは分析エンジンが問題を発見しなくなった後に「削除済み」として問題をマークします。

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。

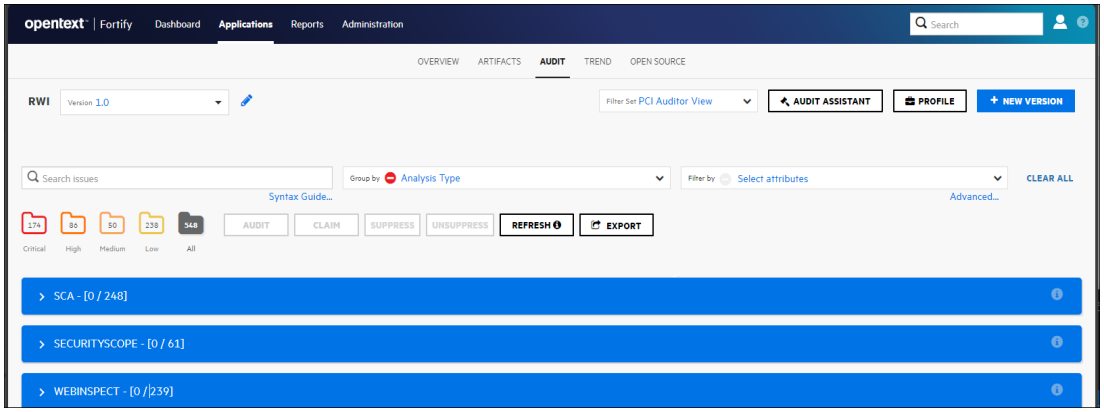
監査する問題に関する情報の表示

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("スキャンアーティファクトのアップロード" ページ327を参照してください)。

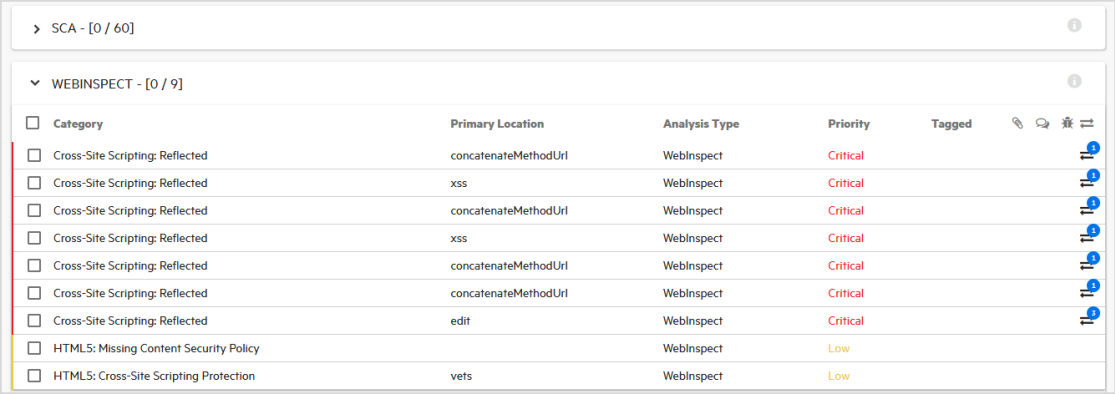


2. アプリケーションバージョンの [監査(AUDIT)] ページを開きます。
3. 監査する問題を選択的に表示するには、問題リストにフィルタを適用します。("[OVERVIEW] および [AUDIT] ページに表示する問題をフィルタ処理する" ページ349および"フォルダに基づく問題の表示" ページ347を参照してください)。



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。一覧にされている問題をソートするには、列見出しをクリックします。

注: 添付ファイルあり(Contains attachment)](列、**コメントあり(Contains comments)**](列、および **送信されたバグ(Bug submitted)**](列はソートできません。

列	説明
Category	発見された問題のカテゴリを表示します(ソートは英数字順です)。
主な場所(Primary Location)	スキャンされたファイルと、問題が検出されたコードの行を表示します(ソートは英数字順です)。
分析のタイプ(Analysis Type)	スキャンで使用される分析エンジンを表示します
優先度(Priority)	問題が示す相対的脅威を示します(ソートは高優先度から低優先度の順または低優先度から高優先度の順です)。
タグ付き(Tagged)	問題に適用されたカスタムタグ値がある場合は、その値を表示します。
添付ファイル(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
コメントあり(Contains comments)	問題にコメントが追加されたかどうかを示します

列	説明
送信されたバグ(Bug submitted)	問題に対して不具合が送信されたかどうかを示します
相関する問題あり(Has correlated issues)	問題の静的および動的な結果が相関しているかどうかを示します。問題がある場合は、表に2回(分析タイプごとに1回)表示されます。 それ以降の静的スキャンまたは動的スキャンで問題が修正済みである場合は、相関アイコンが削除されます。 (ソートでは、相関する問題が最初または最後に表示されます。)

参照情報

"スキャン結果の監査" ページ358

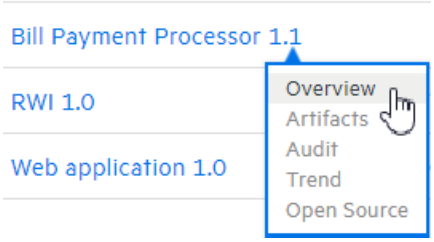
フォルダに基づく問題の表示

概要(OVERVIEW)]ページと 監査(AUDIT)]ページには、 **重大(Critical)**]リンク、 **高(High)**]リンク、 **中(Medium)**]リンク、 **低(Low)**]リンク、および **すべて(All)**]リンクが含まれています。これらのリンクは、Fortifyフォルダへの割り当てに基づいて問題を表示するために使用できます。デフォルトで、フォルダはFortify優先度値(および企業にもたらす潜在的リスク)に対応しますが、表示されるフォルダには、Fortify Audit Workbenchからフィルタセット(および問題テンプレート)に作成および追加されたカスタムフォルダを含めることができます(『Fortify Audit Workbenchユーザガイド』を参照してください)。

メモ: Fortify Audit Workbenchでフィルタセットおよびフォルダを編集または作成する場合、Fortify Audit WorkbenchとFortify Software Security Centerで使用される検索修飾子が一致しない場合があります。検索式に基づくすべての検索、フィルタ、またはフォルダが同じ結果を生成するとは限りません。また、検索式にOWASPやCWEなどの外部メタデータカテゴリが含まれている場合、Fortify Software Security CenterとFortify Audit Workbenchでは式が異なる場合があるため、結果が一致しないことがあります。一致する外部カテゴリが複数ある場合、Fortify Software Security Centerではそれらのいずれかと一致しますが、Fortify Audit Workbenchではすべての外部カテゴリとの完全一致を期待します。Fortify Software Security Centerで使用する問題テンプレートを編集または作成する際にこの問題が発生した場合は、カスタマサポートにお問い合わせください。

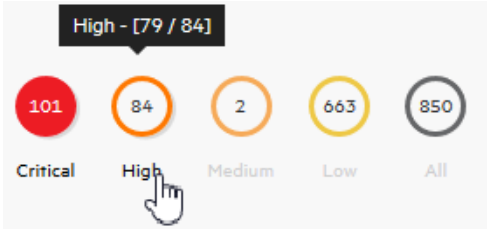
Fortifyフォルダ割り当てに基づいて 概要(OVERVIEW)]ページから問題を表示するには:

1. ダッシュボード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、 **概要(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。 **グループ条件(Group by)**]リストと **フィルタ条件(Filter by)**]リストの左側に、それぞれのフォルダ内の問題の総数が表示されます。デフォルトでは、すべての問題が表示されます。(フィルタ条件として使用する属性を選択すると、それに応じてフォルダに表示される数字も変更されます)。

2. 確認されたフォルダ内の問題の数を表示するには、カーソルをフォルダに移動します。

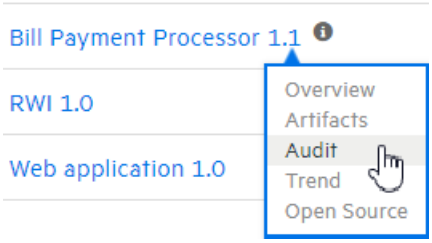


確認された問題の数が左側に表示され、問題の合計数が右側に表示されます。この例では、優先度が高い問題の合計数の79/84を確認できます。

3. 割り当てられたフォルダに基づいて [概要(OVERVIEW)]ページに問題チャートを表示するには、フォルダまたはフォルダラベルを選択します。

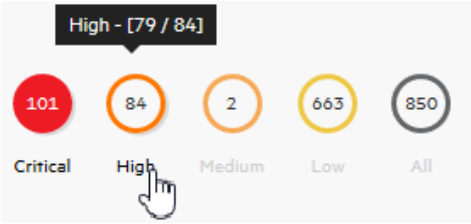
Fortifyフォルダ割り当てに基づいて [監査(AUDIT)]ページから問題を表示するには:

1. ダッシュボード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、 **監査(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は、それぞれの割り当てフォルダ内の問題の数が表示されます。デフォルトでは、すべての問題が表示されます。(フィルタ条件として使用する属性を選択すると、それに応じてフォルダに表示される数字も変更されます)。

2. 特定のフォルダに割り当てられている確認済みの問題の数を表示するには、カーソルをフォルダに移動します。



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. フォルダ割り当てに基づいて [監査(AUDIT)] ページに問題のリストを表示するには、フォルダを選択します。

参照情報

"[OVERVIEW] および [AUDIT] ページに表示する問題をフィルタ処理する" 下

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. OpenTextのヘッダで、 **[アプリケーション(Applications)]** をクリックします。
2. **[自分に割り当てられている問題(My assigned issues)]** チェックボックスを選択します。

   [アプリケーション(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368

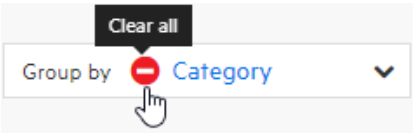
[OVERVIEW] および [AUDIT] ページに表示する問題をフィルタ処理する

[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370を参照してください。

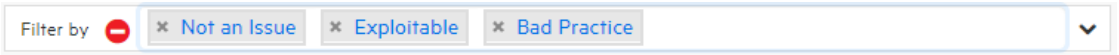
[OVERVIEW] ページまたは [AUDIT] ページに表示される問題をフィルタ処理するには:

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。



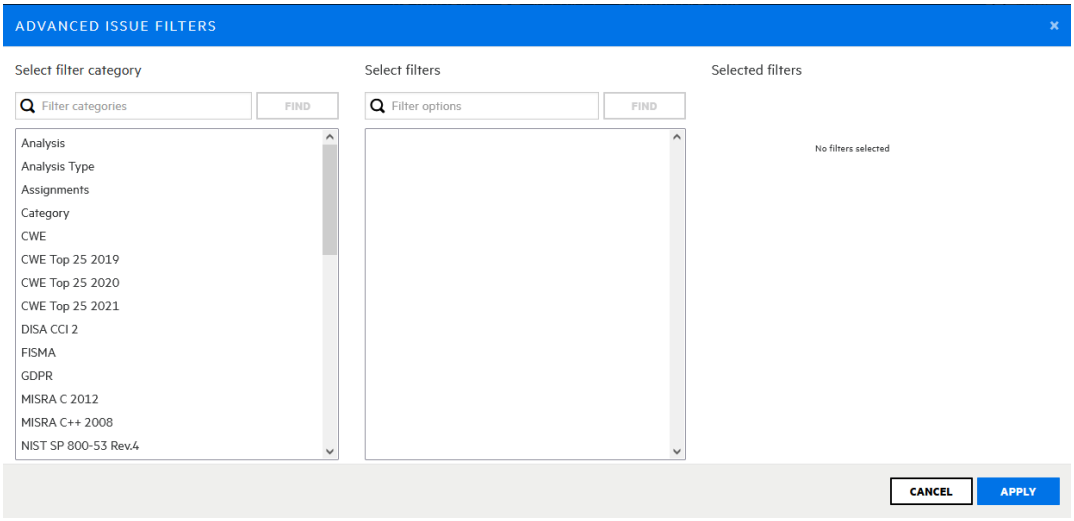
(選択した属性を削除するには、 [**Clear all**]アイコンをクリックします)。

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。(属性は一度に1つずつ選択する必要があります)。



(選択した属性を削除するには、その名前の横にあるx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。

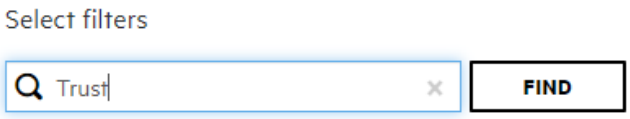


   b. [**高度な問題フィルタ(ADVANCED ISSUE FILTERS)**]ウィンドウの [**フィルタカテゴリの選択(Select filter category)**]リストからカテゴリを選択します。一覧にされるカテゴリを絞り込むには、 [**カテゴリのフィルタ処理(Filter categories)**]ボックスにテキスト文字列を入力して、 [**検索(FIND)**]をクリックします。

[フィルタの選択(Select filters)]リストには、選択したカテゴリで使用可能なフィルタが入っています。

c. [フィルタの選択(Select filters)]リストをさらに絞り込むには、[フィルタオプション(Filter options)]ボックスにテキスト文字列を入力して、[検索(FIND)]をクリックします。

[フィルタの選択(Select filters)]リストには、一致するテキストを含むフィルタが表示されます。

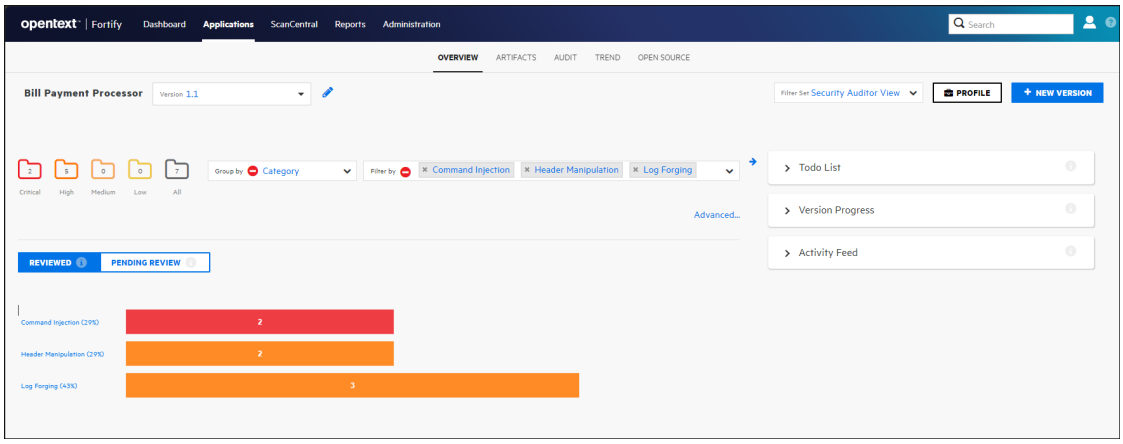


フィルタの完全なリストを再び表示するには、[Filter categories]ボックスのxをクリックします。

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。

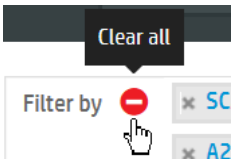
e. 別のフィルタカテゴリのフィルタを追加するには、これらの手順を繰り返します。

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. **[グループ条件(Group by)]**と**[フィルタ条件(Filter by)]**と高度なフィルタの選択をすべて消去するには、**[すべて消去(CLEAR ALL)]**をクリックします。
6. 相関する問題の表示については、"相関する問題の監査" ページ366を参照してください。

参照情報

"問題の検索" 下

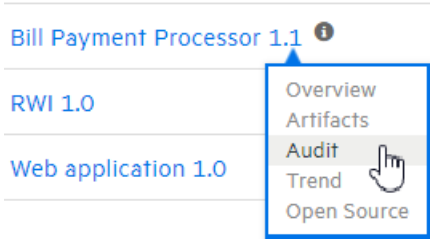
"フォルダに基づく問題の表示" ページ347

"Fortify Software Security Centerでのグローバル検索" ページ400

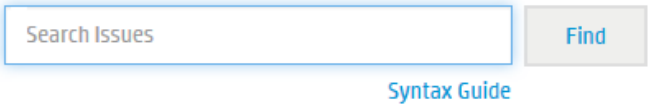
問題の検索

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概要テーブルで、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、**[監査(Audit)]**を選択します。



2. **[問題の検索(Search Issues)]**ボックスに、次の構文を使用して検索クエリを入力します。実行する比較の種類を指定するには、検索用語を区切り記号で囲みます。

比較	説明
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

比較	説明
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おり、そのタグに基づいて問題を検索したい場合は、次のフォーマットのいずれかを使用します。

- 値が設定されていない日付タグを検索するには:
  <DateCustomTag>: <none>
- (任意の)日付が設定されている日付タグを検索するには:
  <DateCustomTag>: !<none>
- 特定の日付の日付タグを検索するには:
  <DateCustomTag>: yyyy-mm-dd

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349

"検索クエリの例" ページ357

"Fortify Software Security Centerでのグローバル検索" ページ400

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

修飾子	説明
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。
[engine priority]	問題を特定したエンジンによって決定された元の優先度値に基づいて問題を検索します。
file	指定したファイルで、プライマリロケーションまたはシンクノード機能呼び出しが発生する問題を検索します。
[fortify priority order]	指定された優先度に一致する優先度レベルの問題を検索します。有効な値は、critical、high、medium、およびlowです。
historyuser	指定したユーザによって監査データが変更された問題を検索します。

修飾子	説明
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。[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。

修飾子	説明
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352

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
  ```

- 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352

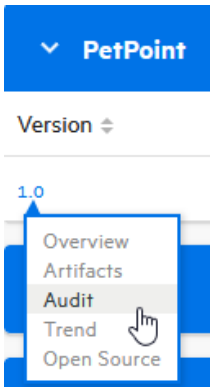
"検索修飾子" ページ354

スキャン結果の監査

注: 次の手順では、 監査(AUDIT)]ページからスキャン結果を監査する方法について説明します。オープンソースの結果を処理する場合は、 監査(AUDIT)]ページまたは オープンソース(OPENSOURCE)]ページからこれらを監査できます。

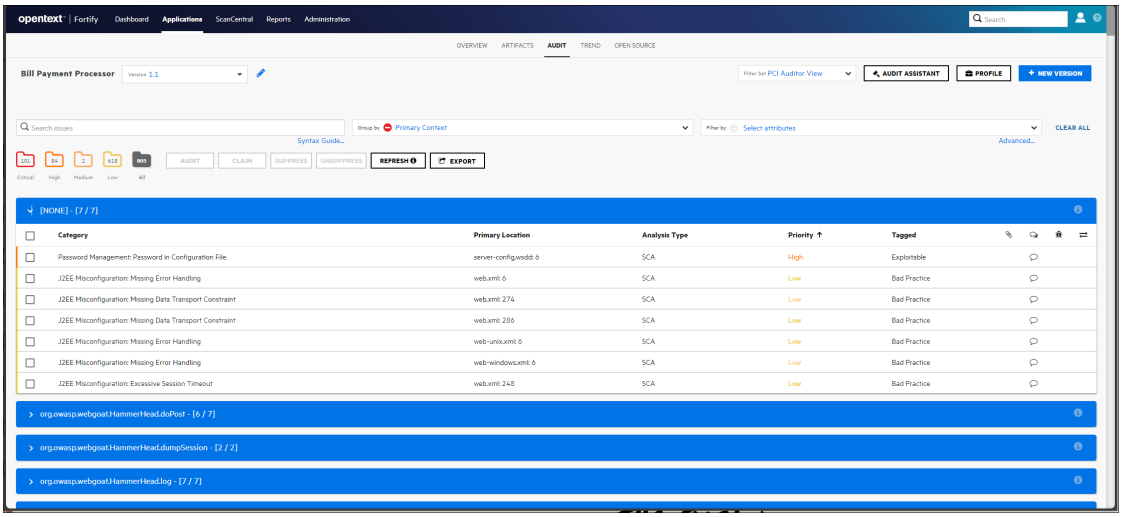
監査する問題を表示するには:

1. 監査するアプリケーションバージョンの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327を参照してください。



2. アプリケーションバージョンの 監査(AUDIT)]ビューを開きます。
   監査(AUDIT)]ビューのテーブルには、割り当てられたフォルダに基づいて問題が一覧にされます(デフォルトでは重大から低)。
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349および"フォルダに基づく問題の表示" ページ347を参照してください)。
4. 問題テーブルでグループ化の条件となる属性を選択した場合は、グループを展開し

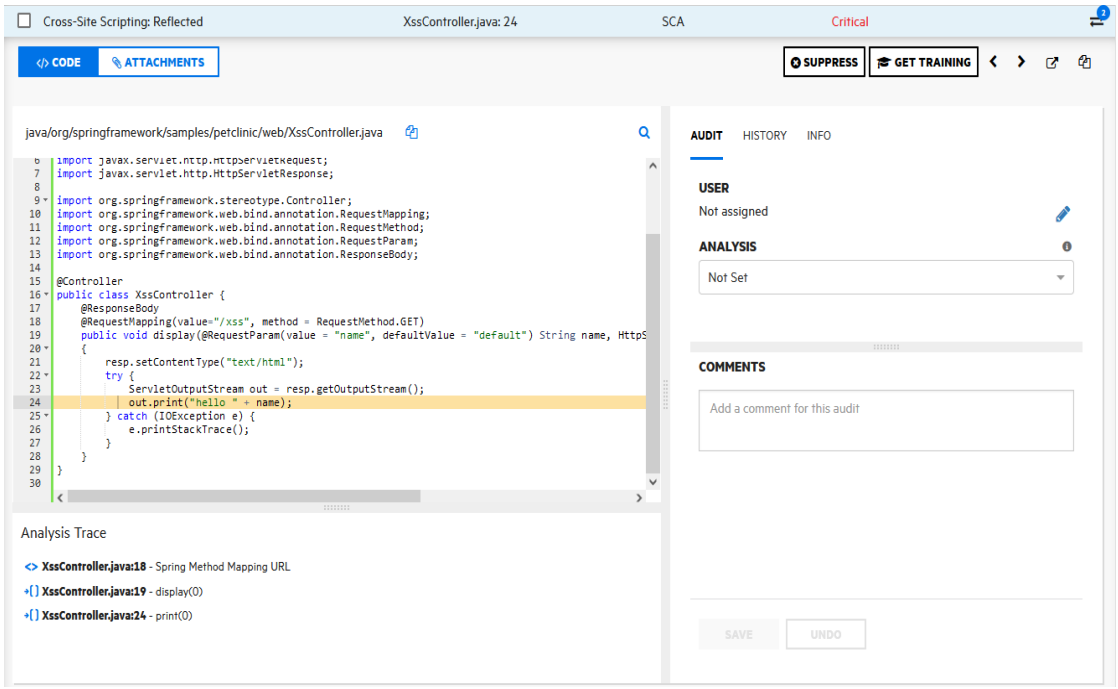
て、そこに含まれている問題を表示します。



問題を監査するには:

1. 問題を展開して詳細を表示するには、テーブル内の該当する行をクリックします。

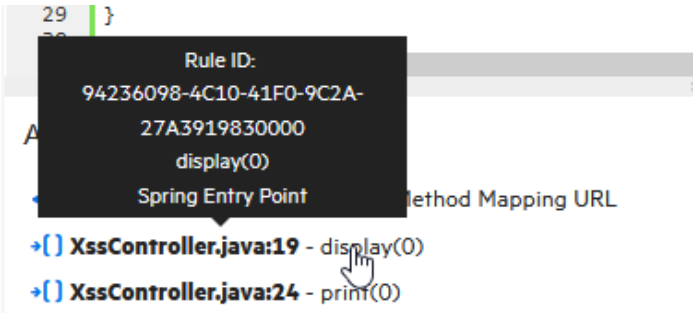
   次の画面キャプチャは、Fortify Static Code Analyzerのスキャン中に明らかにされた問題の詳細を示しています。WebInspectの検索結果の表示については、"Fortify Software Security CenterでのFortify WebInspectスキャン結果の表示" ページ406を参照してください。



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、**新しいタブで開く(Open in a new tab)**]ボタン()をクリックします。問題のリンクをコピーして後で簡単にアクセスするには、**Copy issue link to clipboard**]ボタン()をクリッ

クします。

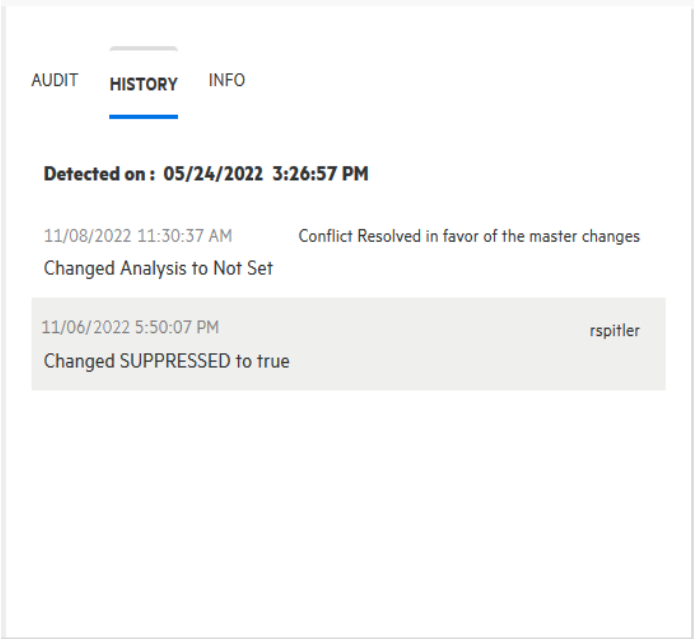
[コード(CODE)]タブには、問題に関連して、汚染されたデータがソースコードの中でたどってきたパスが表示されます。



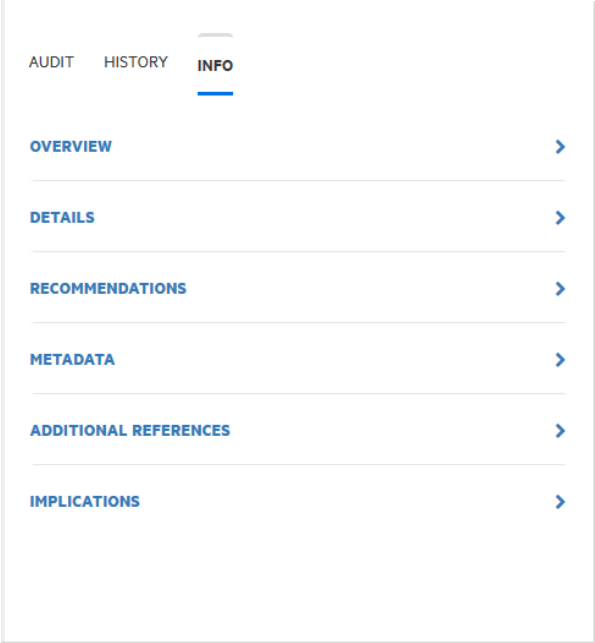
2. 汚染されたデータの経緯のステップに関するサマリの詳細を表示するには、[分析トレース(Analysis Trace)]の下で、そのステップにカーソルを移動します。
3. ステップに関連付けられているコードを表示するには、[Analysis Trace]の下のステップをクリックします。

   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. [コード(CODE)]タブの右上にある検索アイコンをクリックします。

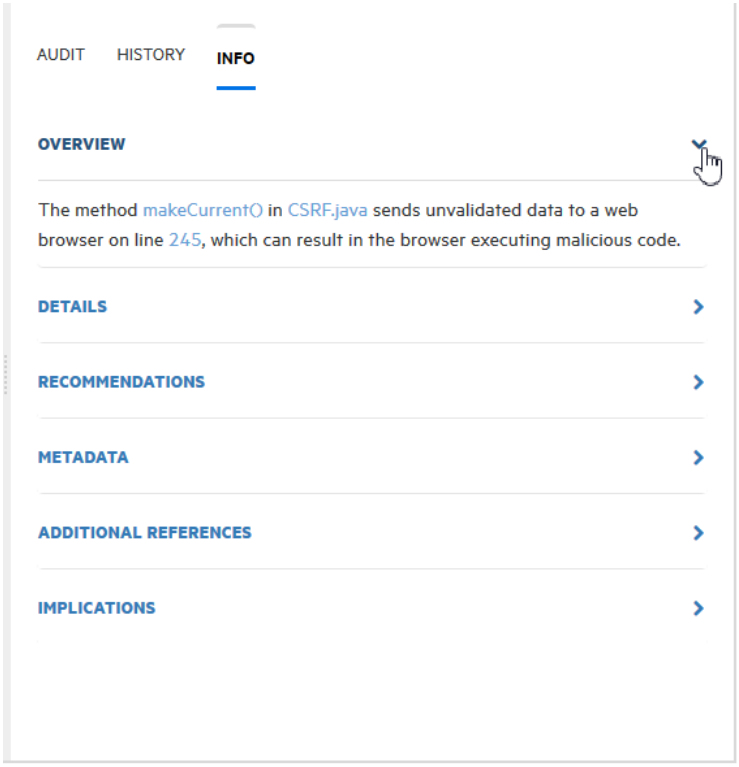
   b. 表示されるテキストボックスに文字列を入力します。[次へ(next)]のアイコンと[前へ(previous)]のアイコンを使用して、検索結果を移動します。



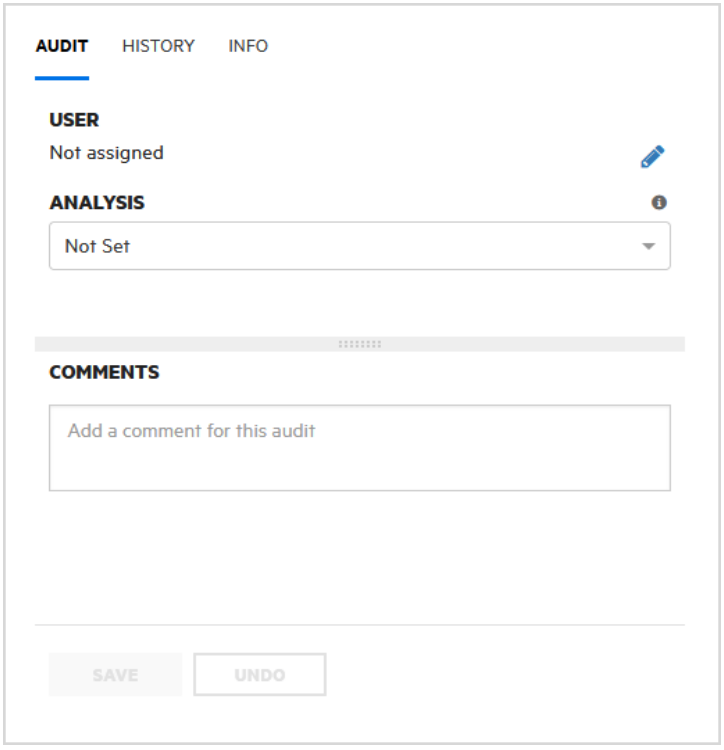
5. 問題について得られる監査履歴を表示するには、右側のペインの **履歴(HISTORY)**] タブを選択します。



6. 問題の概要、結果に関する詳細、改善に関する推奨事項、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 **情報(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(›)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 [監査(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、[抑止(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85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、[トレーニングを受ける(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web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. 左側のペインで [添付ファイル(ATTACHMENTS)]をクリックします。
    b. [ここをクリックして追加(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。

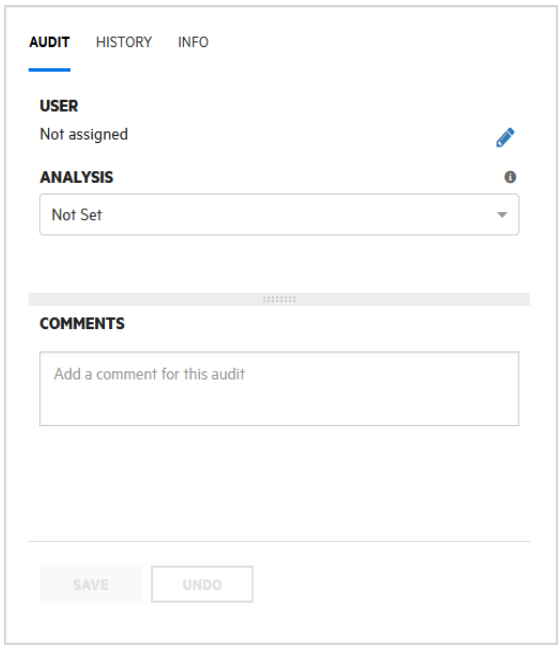
    サポートされているファイル形式は、TXT、LOG、DOC、DOCX、PDF、PPTX、JPG、JPEG、BMP、PNG、TIFF、GIF、ZIP、GZIP、TAR、および7ZIPです。(XML形式のドキュメントはサポートされていません)。

    注: ファイルサイズは3MBを超えないようにしてください。

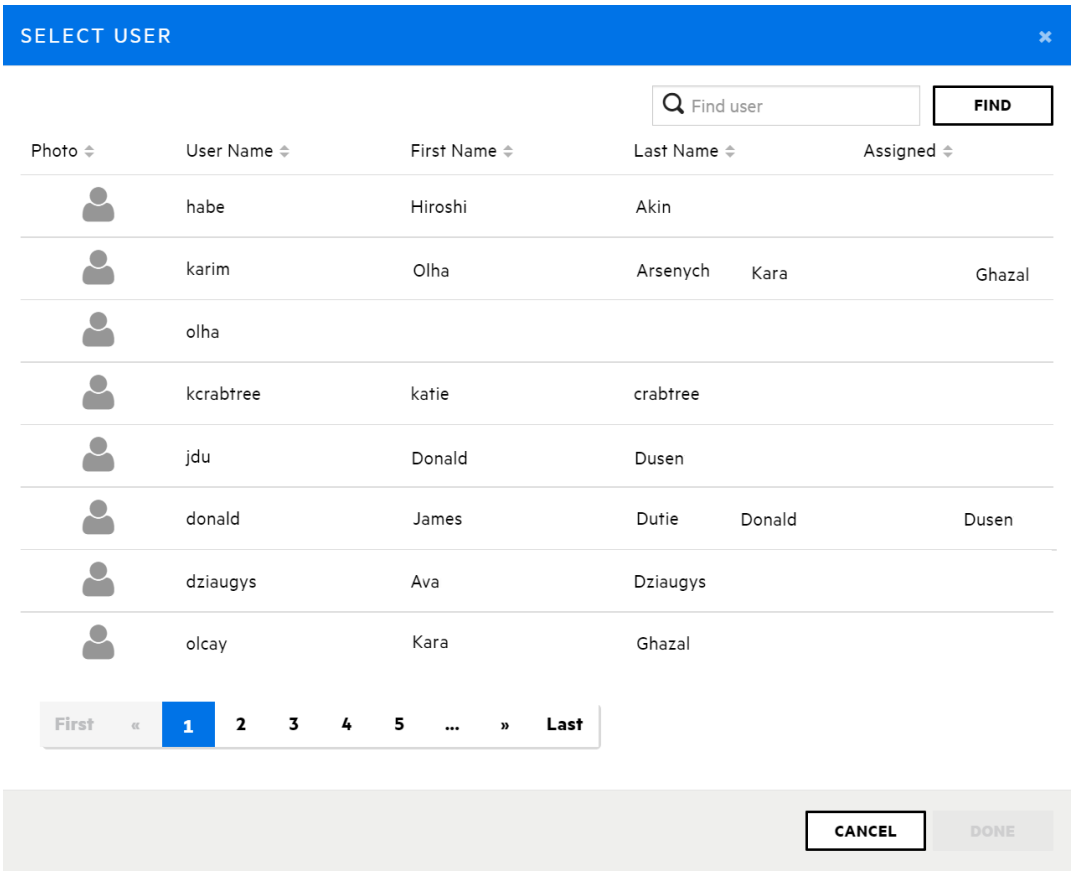
    d. (オプション) [説明(Description)]ボックスに、ファイルの説明を入力します。
    e. [SAVE]をクリックします。

    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。



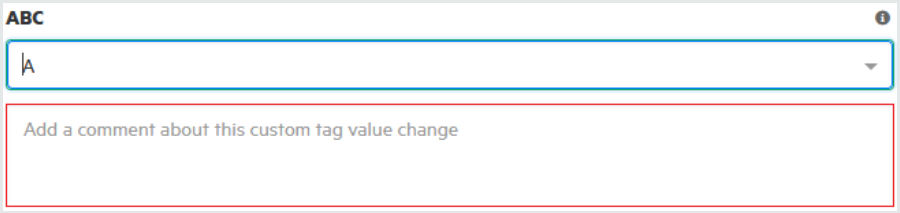
b. [ユーザの選択(SELECT USER)]ダイアログボックスから問題に割り当てるユーザを見つけるには、 **[ユーザの検索(Find user)]**ボックスにユーザ名の一部またはすべてを入力し、 **[検索(FIND)]**をクリックします。
c. 返された名前のリストで、問題に割り当てるユーザの名前をクリックします。
d. **[DONE]**をクリックします。

注: 割り当てられたユーザを削除して **[未割り当て(Not assigned)]**に戻すには、 **[ユーザの割り当て解除(Unassign User)]**アイコンをクリックします。または、割り当てられたユーザを別のユーザに置き換える場合は、 **[割り当てられたユーザの編集(Edit assigned user)]**アイコンを選択して、希望するユーザを選択します。

[監査(AUDIT)]タブに、選択したユーザ名とアバターが表示されます(使用可能な場合)。

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。Fortify Software Security Centerではこの問題は未監査として扱われます。
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、それらのタグの値を指定します。

注: 割り当てるカスタムタグに対してコメントが必要であると管理者が指定している場合は、カスタムタグの値リストの下に表示される赤枠のボックスにコメントを入力する必要があります。



注: Audit Assistantが問題を評価した場合は、右側のペインに追加のフィールド(**[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396を参照してください。

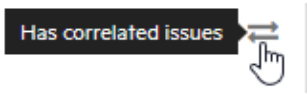
16. **[コメント(COMMENTS)]**ボックスに、この問題の監査に関するコメントを入力します。(監査設定を保存した後、 **[コメント(COMMENTS)]**セクションにはコメント、および以前に保存した他のコメントが一覧表示されます)。
17. **[AUDIT]**タブの下部にある **[SAVE]**をクリックします。

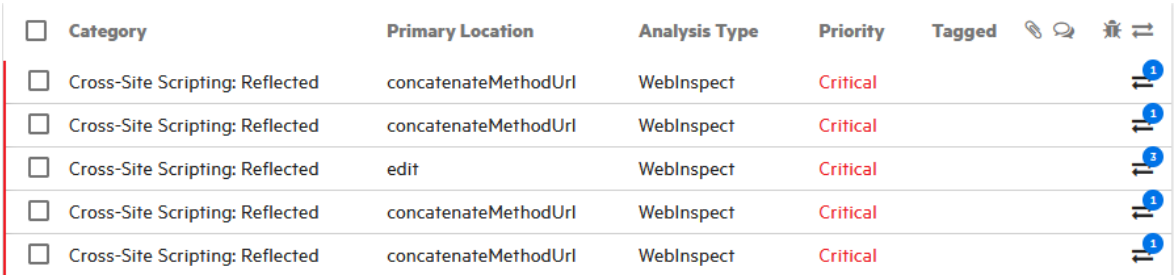
相関する問題の監査

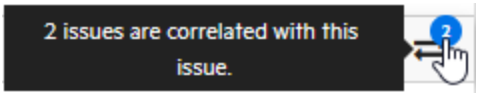
アプリケーションバージョン用にアップロードされたアーティファクトに、静的(Fortify Static Code Analyzer)分析と動的(WebInspect)分析の両方の結果が含まれる場合、複数の問題が相互に関連し合っている可能性があります。

ある問題が別の分析エンジンを使用して明らかになった他の1つ以上の問題と関連している場合、 **相関する問題あり(Has correlated issues)**]アイコンと、相関する問題の数が表示されます。これには、選択した問題をターゲットとするものと、それに由来するものの両方が含まれます。

他の問題と相関する問題を一覧にしてテーブルの上部に表示するには、 **相関する問題あり(Has correlated issues)**]アイコンを2回クリックします。



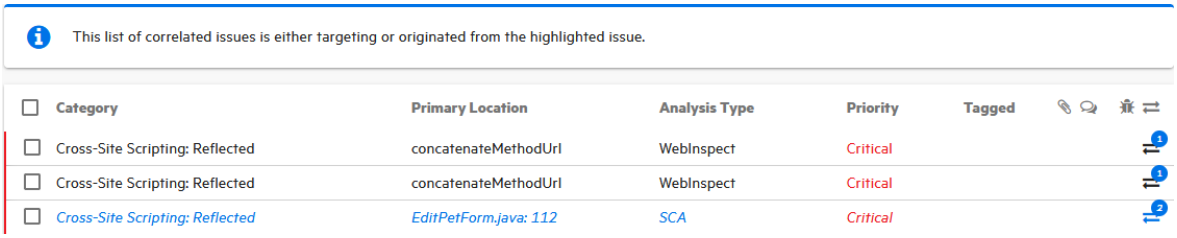




青い円に表示される数字は、ある問題と相関する問題の数を示します。

相関する問題を一覧にするには:

- 円または **相関する問題あり(Has correlated issues)**]アイコンをクリックします。



"スキャン結果の監査" ページ358の説明に基づいて、リストされている問題を監査できます。

注: 監査の後、開発者が、1つの問題に存在することが明らかになった根本的な問題を修正すると、相関関係にある残りの問題も修正されることがあります。

すべての問題のテーブルに戻るには、 [フィルタ条件(Filter by)]リストの右側にある [すべてクリア(CLEAR ALL)]をクリックします。

参照情報

"問題のバッチの監査" ページ376

"監査アシスタントについて" ページ379

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。

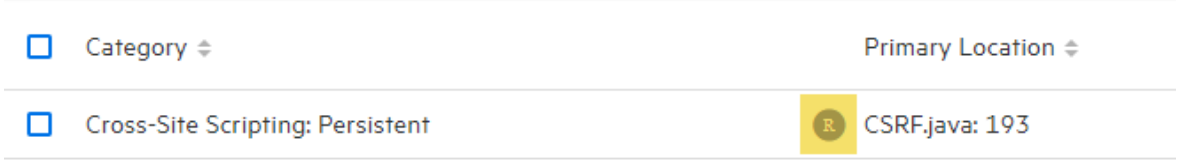
抑止された問題

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、"スキャン結果の監査" ページ358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" 次のページを参照してください。

削除された問題

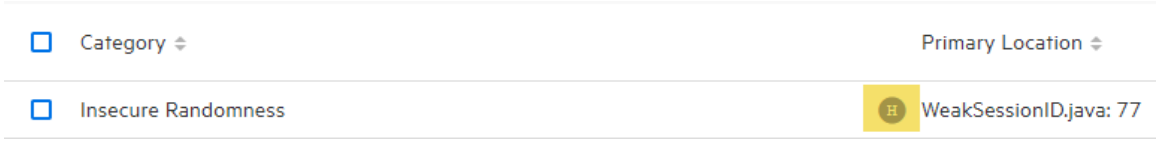
アプリケーションでスキャンが複数回実行されるうちに、問題が修正されたり古くなることがよくあります。Fortify Software Security Centerでスキャン結果がマージされると、以前のスキャンで見つかったが、最新の分析結果で明らかでなくなった問題が削除としてマークされます。



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" 次のページ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。

抑止された問題の表示

アプリケーションバージョンに関連する抑止された問題を表示するには、次の手順に従います。

1. [Dashboard]ビューまたは[Applications]ビューで、目的のアプリケーションバージョンのバージョンを選択します。
   Fortify Software Security Centerが選択したバージョンの[AUDIT]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。
   [APPLICATION PROFILE]ダイアログが開き、[ADVANCED OPTIONS]タブが開きます。
   チェックボックスの下にある[Issue counts by state, based on current selections]に、選択したアプリケーションバージョンに関連付けられているデータベース内の非表示、抑止、および削除された問題の数が表示されます。

   注: 選択したフィルタセットは、表示される抑止された問題の数には影響を与えません。たとえば、抑止された問題が選択したフィルタセットで非表示になっている場合でも、抑止された問題の数に含まれます。
3. [Show suppressed issues]チェックボックスを選択します。
4. [APPLY]、[CLOSE]の順にクリックします。

これで、 [AUDIT]ページには、抑止された問題すべてが表示されます。 [Primary Location]列で、抑止された各問題に「S」アイコンが付けられます。

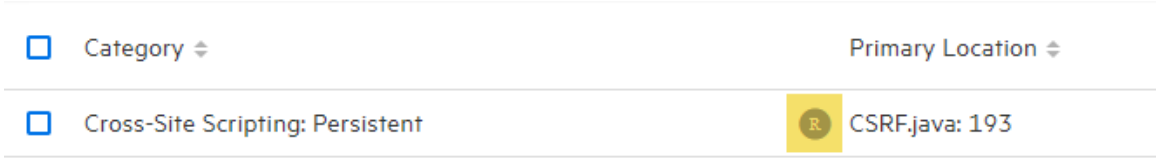
削除された問題の表示

Fortify Software Security Centerでアップロードしたスキャン結果がマージされると、以前の分析で見つかったが、最新の結果で明らかでなくなった問題が削除されます。

アプリケーションバージョンで削除された問題を表示するには、次の手順に従います。

1. [Dashboard]ビューまたは [Applications]ビューで、目的のアプリケーションバージョンのバージョン名を選択します。
   Fortify Software Security Centerが選択したバージョンの [AUDIT]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。
   [APPLICATION PROFILE]ダイアログが開き、 [ADVANCED OPTIONS]タブが開きます。
   チェックボックスの下にある [Issue counts by state, based on current selections]に、選択したアプリケーションバージョンに関連付けられているデータベース内の非表示、抑止、および削除された問題の数が表示されます。

   注: 選択したフィルタセットによって、削除された問題の表示数は影響を受けません。たとえば、抑止された問題が選択したフィルタセットで非表示になっている場合でも、削除された問題の数に含まれます。
3. [Show removed issues]チェックボックスを選択します。
4. [APPLY]、 [CLOSE]の順にクリックします。



[AUDIT]ページに、削除された問題がすべて表示されます。[Primary Location]列で、削除された各問題に「R」アイコンが付けられます。

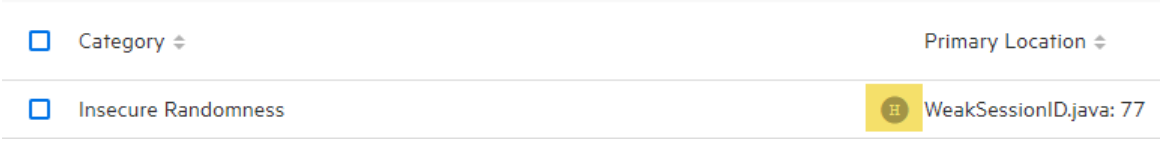
非表示の問題の表示

非表示の問題とは、Fortify Software Security Centerで、フィルタセットルールが現在有効なため表示されない問題です。

アプリケーションバージョンに関連する非表示の問題を明らかにするには、次の手順に従います。

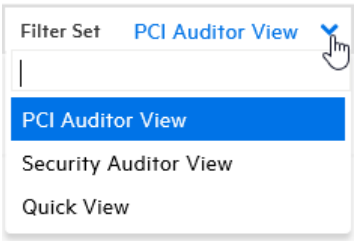
1. [Dashboard]ビューまたは [Applications]ビューで、目的のアプリケーションバージョンのバージョンを選択します。
   Fortify Software Security Centerが選択したバージョンの [AUDIT]ページを開きます。

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。
   [APPLICATION PROFILE]ダイアログが開き、 [ADVANCED OPTIONS]タブが開きます。
   チェックボックスの下にある [Issue counts by state, based on current selections]に、選択したアプリケーションバージョンに関連付けられているデータベース内の非表示、抑止、および削除された問題の数が表示されます。
3. [Show hidden issues]チェックボックスを選択します。
4. [APPLY]、 [CLOSE]の順にクリックします。



これで、 [AUDIT]ページには、非表示の問題すべてが表示されます。 [Primary Location]列で、非表示の各問題に「H」アイコンが付けられます。

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には、 [概要(OVERVIEW)]ページ、 [監査(AUDIT)]ページ、および [オープンソース(OPEN SOURCE)]ページでのアプリケーションバージョンの問題の表示を変更するためのフィルタセットが用意されています:

- クイックビュー
  クイックビューフィルタセットを使用すると、 [重大]フォルダの問題(影響が大きくなる可能性と発生する可能性が高い)と [高]フォルダの問題(影響が大きくなる可能性が高く発生する可能性が低い)を表示できます。このフィルタセットは、最初に結果に注目することで最も差し迫った問題にすばやく対処できる便利なものです。
- セキュリティ監査人ビュー
  このビューには、監査すべき幅広いセキュリティ上の問題が示されます。セキュリティ監査人ビューフィルタには表示フィルタが含まれないので、すべての問題が表示されます。
- PCI監査人ビュー

このビューは、アプリケーションをPayment Card Industry Security Standards(支払いカード業界のセキュリティ標準)の順守に関して監査する責任を担う個人のために定義されています。

割り当てられた問題の優先度の上書き

スキャン結果が解析され、Fortify Software Security Centerにロードされると、サポートされている各エンジンタイプのスキャンパーサが各問題に優先度値を割り当てます。ただし、この優先度値には、影響を受けるコードまたはアプリケーションのフルコンテキストが反映されていません。影響を受けるコードの使用に関連する他の要因によっては、別の優先度を割り当てることが妥当な場合があります。たとえば、対象のコードのセクションがアプリケーション内で呼び出されることがない場合や、アプリケーションが小規模な部門による使用のみを目的としており、他のアプリケーションやシステムに接続されないため、特定された脆弱性の悪用の危険性が低い場合は、「重大」優先度値が割り当てられた脆弱性を「中」または「低」の優先度に分類したほうが妥当である可能性があります。このような使用例を可能にするために、Fortify Software Security Centerでは、問題に最初に割り当てられた優先度を信頼できるユーザが変更できるようになっています。このような優先度の変更は、生成されたレポートに反映されます。

注意 この機能を有効または無効にすると、システム内のデータによっては生成されるレポートや計算されるメトリックなどに影響が及ぶため、これを長期的な変更と見なす必要があります。有効または無効にする前に、計画している変更についてセキュリティリードと話し合ってください。

Fortify Software Security Center上で優先度の上書き機能を有効または無効にする

優先度の上書きは、Fortify Software Security Centerの新しい展開中にシステム上で有効にすることも、既存のFortify Software Security Centerインスタンス上で有効にすることもできます。

優先度の上書き機能を有効にする

優先度の上書き機能を有効にするには:

1. 管理(Administration)]ビューの左ペインで、 **設定(Configuration)**]を選択してから、 **問題の監査(Issue Audit)**]を選択します。
2. **優先度の上書きを有効にする(Enable priority override)**]チェックボックスをオンにします。
3. **保存(SAVE)**]をクリックします。
4. サーバを再起動します。

サーバの再起動後、この機能は有効になり、すべてのアプリケーションバージョンに適用されます。これで、 監査(AUDIT)]ページ上で、問題の詳細(監査(AUDIT)]タブ)に **優先度の上書き(PRIORITY OVERRIDE)**]リストタグが表示されます。

信頼されたユーザが問題優先度を上書きできるようにする

ユーザがこの機能を使用できるようにするには、それらのユーザのために「制限付きカスタムタグ値の編集」許可を含む新しいユーザ役割を作成します。これらの役割は、問題の優先度を正確に評価する知識と注意力を持つ信頼できるユーザにのみ付与します。ユーザ役割の作成方法については、"カスタム役割の作成" ページ228を参照してください。

注: 制限付きカスタムタグ値を編集する許可を持っているユーザ役割は、問題の優先度を上書きできます(システム定義のセキュリティリード役割は、すでに制限付きカスタムタグを編集する能力を持っています)。

優先度の上書き機能を無効にする

優先度の上書き機能を無効にするには:

1. 管理(Administration)]ビューの左ペインで、 **設定(Configuration)**]を選択してから、 **問題の監査(Issue Audit)**]を選択します。
2. **優先度の上書きを有効にする(Enable priority override)**]チェックボックスをオフにします。
3. **保存(SAVE)**]をクリックします。
4. サーバを再起動します。

サーバの再起動後に、この機能がシステム全体で無効になり、 **優先度の上書き(PRIORITY OVERRIDE)**]リストタグが問題の詳細に表示されなくなります。

監査中に優先度値を上書きする

監査中に問題の優先度値を上書きするには:

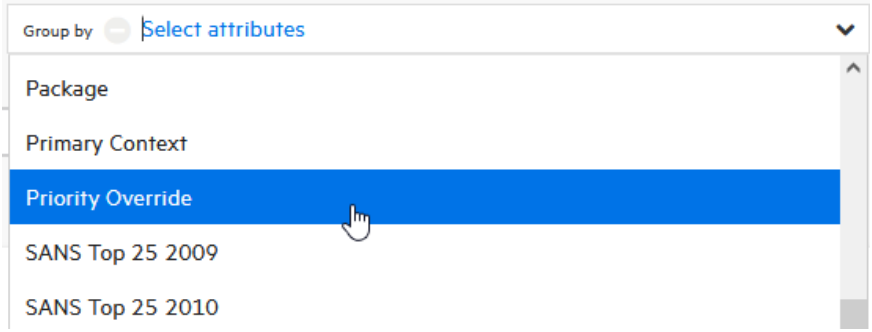
1. 監査(AUDIT)]ページで、問題を含む行を展開します。
2. 右側のペインの **監査(AUDIT)]**タブの **優先度の上書き(PRIORITY OVERRIDE)]**リストから、必要な優先度値を選択します。
3. (必須)リストの下の赤枠のボックスに、値を変更した理由を説明するコメントを入力します。

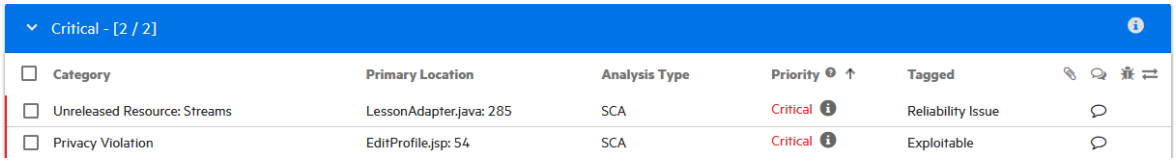
   注: 監査を保存する前に上書きを元に戻す場合は、ペインの下部にある **元に戻す(UNDO)]**をクリックします。

4. 新しい優先度値および関連付けられたコメントを保存するには、 **保存(SAVE)]**をクリックします。

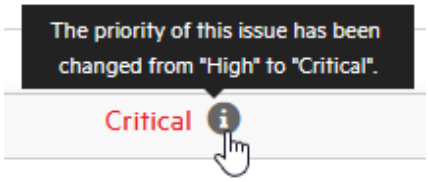
優先度値が変更された問題を表示する

自分および他のユーザが手動で割り当てた優先度値を持つ問題を表示するには、 **グループ別(Group by)]リストから 優先度の上書き(Priority Override)]**を選択します。





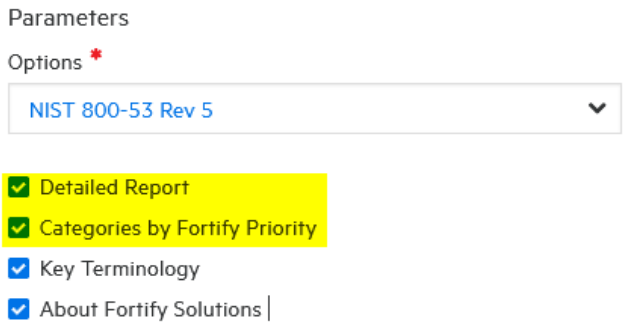
問題テーブルに、優先度が上書きされた問題がPRIORITY OVERRIDEタグ値別に一覧表示されます。優先度値が変更されていない問題は、 **未設定(Not Set)]**の下に分類されます。



優先度(Priority)]値がどのように変更されたのかを確認するには、情報アイコンの上にカーソルを移動します。

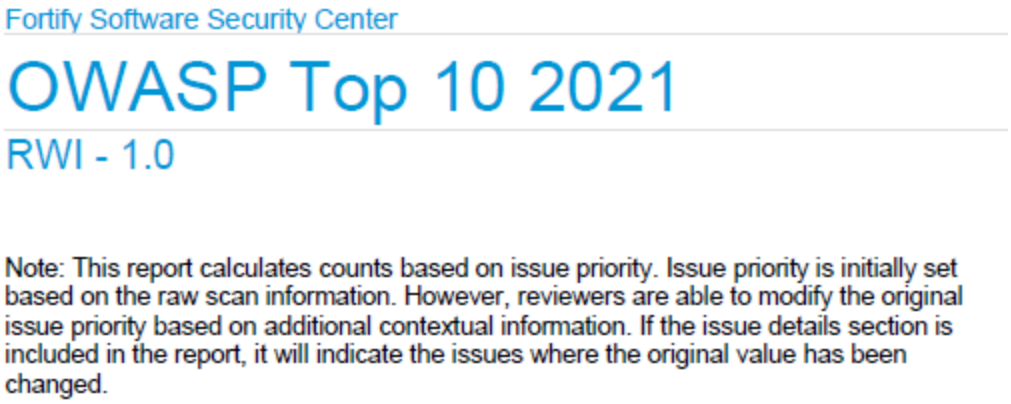
問題レポートでの優先度の上書き情報の表示

アプリケーションバージョンの監査で優先度上書きタグが使用された場合は、生成する問題レポートにその情報を含めることができます。

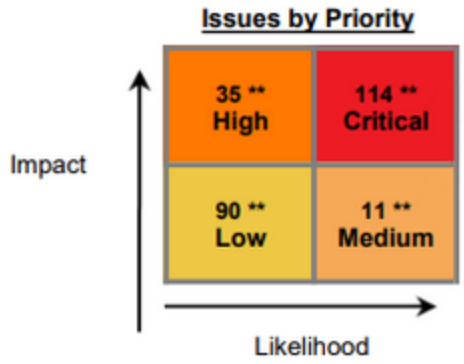


優先度の上書き情報を新しい問題レポートに含めるには、レポートのパラメータを指定するときに、**詳細なレポート(Detailed Report)**]および**Fortifyの優先度別のカテゴリ(Categories by Fortify Priority)**]チェックボックスをオンのままにします。

問題レポートに優先度値を上書きした問題が含まれている場合(かつ、**詳細なレポート(Detailed Report)**]および**Fortifyの優先度別のカテゴリ(Categories by Fortify Priority)**]オプションが選択されている場合)は、次に示すように、その効果のメモがカバーページに表示されます。



優先度の上書き機能が使用され、**詳細なレポート(Detailed Report)**]および**Fortifyの優先度別のカテゴリ(Categories by Fortify Priority)**]パラメータが(手動またはデフォルトで)選択されている場合は、**エグゼクティブサマリ(Executive Summary)**]の**優先度別の問題(Issues by Priority)**]キューブで、優先度値が変更されている問題に2つのアスタリスクが表示されます。



これらのレポートの **[問題の詳細(Issue Details)]** セクションには、現在の優先度値と元の優先度値が表示されます。

Path Manipulation ***Remediation Effort(Hrs): 0.5***	**Low** **Original: Critical**
Package: com.order.splc	

Location	Analysis Info	Analyzer
WEB-INF/src/java/com/order/splc/ConnFactory.java:20 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnFactory.ConnFactory() **In** WEB-INF/src/java/com/order/splc/ConnFactory.java:16	SCA
WEB-INF/src/java/com/order/splc/ConnectionFactory.java:30 Priority Override: Low Analysis: Not an Issue	**Sink:** java.io.FileInputStream.FileInputStream() **Enclosing Method:** ConnectionFactory() **Source:** java.lang.System.getProperty() **from** com.order.splc.ConnectionFactory.ConnectionFactory() **In** WEB-INF/src/java/com/order/splc/ConnectionFactory.java:26	SCA

元の優先度値に戻す

問題に対して最初から割り当てられた優先度値を上書きしてから保存したが、その優先度値を元の値に戻したい場合は、次のようにします。

1. **[監査(AUDIT)]** ページで、問題を含む行を展開します。
2. **[優先度の上書き(PRIORITY OVERRIDE)]** リストタグの右側で、元に戻すアイコン( )をクリックします。
3. (必須)リストの下の赤枠のボックスに、値を変更した理由を説明するコメントを入力します。
4. 新しい優先度値および関連付けられたコメントを保存するには、 **[保存(SAVE)]** をクリックします。

レポートには、エンジンによって設定された元の優先度(変更されていない場合)か、上書きされた値かに関係なく、現在有効な優先度値が反映されます。ユーザが優先度値を変更した場合は、これらのレポートには変更された値が表示されます。そうでない場合は、レポートに元の優先度が表示されます。

問題に対して送信されたバグの表示

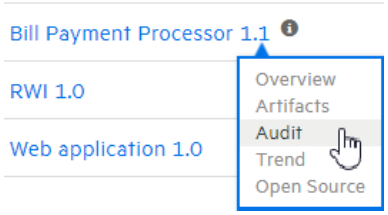
[AUDIT] ページの問題テーブルには、リストに表示された問題に対してバグが送信されたかどうかを示す [**Bug submitted**] 列 ( )列が含まれています。

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。

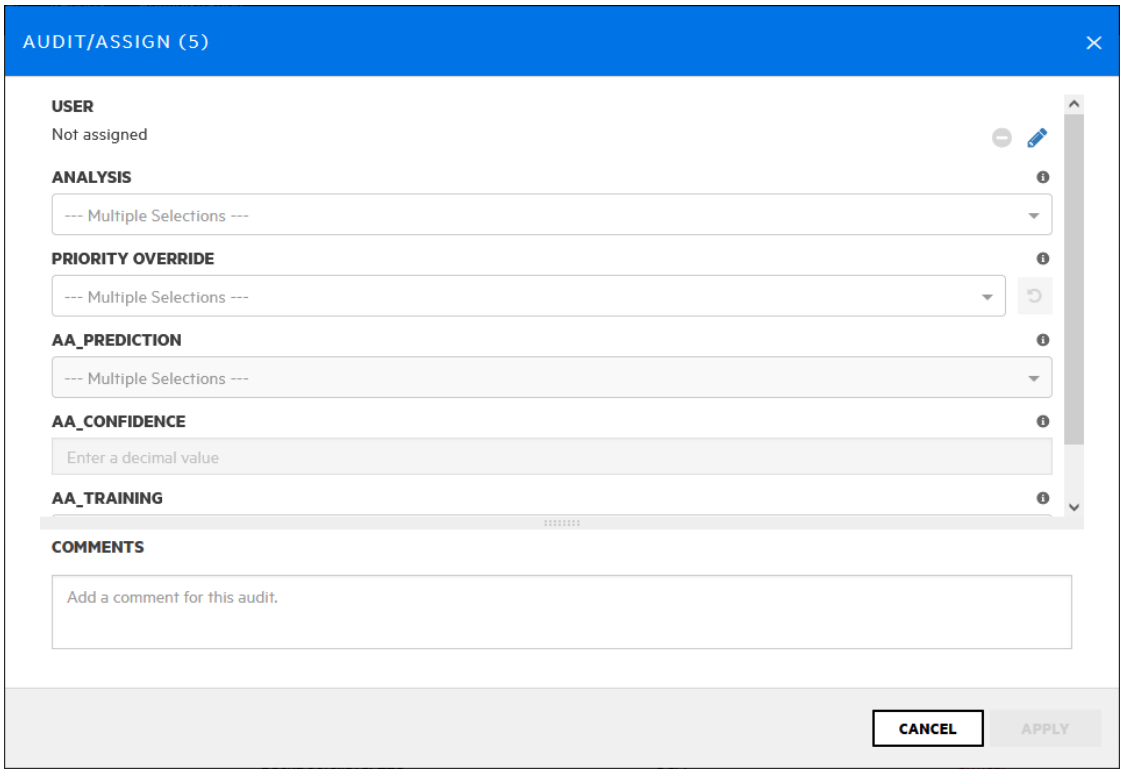
ヒント: バグを表示するには、バグトラッカーアプリケーションでサポートされているブラウザを使用する必要があります。

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. [ユーザの選択(SELECT USER)]ダイアログボックスを開くため、**[割り当てられたユーザの編集(Edit assigned user)]**アイコン🖉を選択します。
   b. これらの問題に割り当てるユーザを見つけるには、**[ユーザの検索(Find user)]**ボックスにユーザ名の一部またはすべてを入力し、**[検索(FIND)]**をクリックします。
   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

"スキャン結果の監査" ページ358

Audit Assistantの使用

次のセクションでは、Audit Assistantワークフローの概要について説明します。

Audit Assistantワークフロー

Fortify Audit Assistantを使用したワークフローは次のとおりです。

1. バージョン23.2.0以降にアップグレードした後に、Fortify Audit Assistantの設定を更新します。詳細については、"Fortify Audit Assistantの設定の更新" ページ383を参照してください。
2. Fortify Audit Assistantアカウントを取得します。
   a. https://analytics.fortify.comに移動します。

   b. **[アカウントが必要ですか? (Need an Account?)]** リンクをクリックします。

[**Fortify Audit Assistantテナントの要求(Request a Fortify Audit Assistant Tenant)**]ウィンドウが表示されます。

c. 会社情報を入力し、 [**購読(Subscribe)**]ボタンをクリックします。

情報の確認が完了すると、ようこそ電子メールが届きます。

3. Fortify Audit Assistantにログインして、1つ以上の予測ポリシーを作成します。詳細については、"予測ポリシーの定義" ページ382を参照してください。
4. Fortify Fortify Audit Assistantトークンを取得します。詳細については、"Fortify Audit Assistant認証トークンの取得" ページ389を参照してください。
5. Fortify Software Security CenterのAudit Assistant設定ページから、次の手順を実行します。
   - Fortify Audit Assistantへの接続を設定およびテストし、 [**ポリシーの更新(REFRESH POLICIES)**]をクリックして、 [**デフォルトの予測ポリシー(Default prediction policy)**]リストに値を自動入力します。
   - デフォルトの予測ポリシーを指定します。
   - (オプション)Audit Assistantで、未監査の問題をFortify Fortify Audit Assistantに自動的に送信して予測を実施できるようにします。
   - (オプション)Audit Assistantで、カスタムタグに予測値を自動的に適用できるようにします。

   詳細については、"Audit Assistantの設定" ページ385を参照してください。
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。このステップは「トレーニング」と呼ばれます。詳細については、「"Audit Assistantへのトレーニングデータの送信" ページ399」を参照してください。
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、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、Fortify Audit Assistantから認証トークンを取得し、そのトークンを使用してFortify Audit Assistant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Fortify Audit Assistantを準備し、データを送信し、Audit Assistant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" ページ381

"予測ポリシーの定義" ページ382

"Audit Assistantの設定" ページ385

"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391

"Audit Assistantへのトレーニングデータの送信" ページ399

"Audit Assistantの結果の確認" ページ396

監査アシスタントについて

Audit Assistantは、スキャンから返された問題が真の脆弱性であるかどうかを判断するのに役立つオプションのツールです。Audit Assistantがその判断を下すには、予測のベースラインを確立するためのデータが必要です。このデータは、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、Fortify on Demand監査官が行った決定に基づいています。このデータは、プールされて匿名化され、監査官が行った決定に基づいてトレーニングデータと組み合わせて使用できます。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。

次のセクションでは、認証トークンをOpenText Fortify Audit Assistantから取得し、そのトークンを使用してOpenText Fortify Software Security Centerへの接続を設定する方法について説明します。このセクションでは、新しいG2エンジンを搭載した最新バージョンのOpenText Fortify Audit Assistantにアップグレードする際の、Fortify Audit Assistantのベストプラクティスについても説明します。詳細については、「"Fortify Audit Assistantのベストプラクティス" 下」を参照してください。

以降のセクションでは、Audit Assistantのトレーニングの設定方法、データの送信方法、およびAudit Assistantの結果の確認方法について説明します。

参照情報

"Audit Assistantの設定" ページ385

"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391

"Audit Assistantの使用" ページ384

"予測ポリシーについて" ページ381

"予測ポリシーの定義" ページ382

"Audit Assistantへのトレーニングデータの送信" ページ399

"Audit Assistantの結果の確認" ページ396

Fortify Audit Assistantのベストプラクティス

OpenText Fortify Audit AssistantおよびOpenText Fortify Software Security Centerのバージョン23.2.0のリリースでは、重要なAudit Assistantエンジンが新たに導入されました。

Generation 2またはG2と呼ばれる新しいエンジンは、大幅に改善された予測エンジンを備えており、脆弱性評価でチームが下す決定により提供されるトレーニングデータといっそう調和がとれたものとなります。出力される結果はより正確で、環境内のアプリケーションとの関連性も高くなります。

このセクションでは、OpenText Fortify Audit Assistant G2エンジンの能力と正確さを最大限に有効活用する方法を説明します。

注: OpenText Fortify Software Security Centerをバージョン23.2.0 (またはそれ以上)に更新していない場合は、以前のOpenText Fortify Audit Assistantエンジン(G1)を引き続き利用できます。アップグレード後は、OpenText Fortify Audit AssistantのG1バージョンはサポートされなくなります。オフクラウドバージョンのAudit Assistantをインストールしたユーザも、OpenText Fortify Software Security Centerバージョン23.2.0以降と併用する場合は、G2バージョンにアップグレードする必要があります。

タグの一貫した使用

Fortify Audit Assistantは、予測を行う際にFALSE POSITIVEとEXPLOITABLEという2つのタグを使用します。

Audit Assistantを最大限に活用するには:

- 自分のタグをAudit Assistantタグにマップする: 悪用可能な脆弱性を特定するために使用するタグをAudit AssistantのEXPLOITABLEタグに、問題ではない脆弱性にラベルを付けるために使用するタグをAudit AssistantのFALSE POSITIVEタグにマップします。そうしない場合、Audit AssistはOpenText Fortify on Demand監査官による決定に基づくグローバルモデルを使用します。自分のタグがAudit Assistantタグにマップされている場合、自社の監査官が行う決定はグローバルモデルと組み合わせて使用され、ご利用のソフトウェア環境および意思決定プロセスに適した決定を考慮に入れることで結果を改善できます。
- 脆弱性への一貫したタグ付け: Fortify Audit Assistantを最大限に活用するには、監査官はAudit Assistantにマップされたタグを一貫して使用する必要があります。

詳細については、「"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" ページ392」を参照してください。

予測しきい値の管理

Audit Assistant インターフェイスで予測ポリシーを作成する場合、値を自分で変更した場合を除き、EXPLOITABLEまたはFALSE POSITIVEタグのデフォルトの予測信頼しきい値は80%に設定されます。これらの値は上下に調整できますが、調整する前にデフォルト設定をしばらく使用することをお勧めします。

Audit Assistant を使用するにつれて、提供するトレーニングデータが結果にプラスの影響を与え、最初のスキャンの結果が劇的に向上する可能性があります。

トレーニングが結果に与える影響を評価した後、ノイズが多すぎるのであれば、しきい値を調整できます。しきい値を高く設定するほど、Audit Assistantの予測に対する信頼が大きくなります。これにより、信頼しきい値を満たすか超える脆弱性だけがEXPLOITABLEまたはFALSE POSITIVEと特定されるようになるため、ヒット数が少なくなります。

詳細については、「"予測ポリシーについて" 次のページ」を参照してください。

監査官が行った決定を使用してモデルをトレーニングする

自社のタグからAudit Assistantタグへのマッピングと、監査済みスキャン結果の送信が済んでいる場合、自社の監査官が下す決定が考慮に入れられて、Audit Assistantの予想は組織の予測にさらに沿ったものとなります。

トレーニングデータを最大限に活用するには、EXPLOITABLEとFALSE POSITIVEの両方の評価を監査に含める必要があります。言語ごとに1,500以上の問題を送信すると、Audit Assistantの予測が大幅に改善されます。

注: 言語ごとに1,500の問題が必要であり、相当する数のEXPLOTABLEおよびFALSE POSITIVEが結果が含まれていなければなりません。すべての言語が同時にこのしきい値に達するとは限りません。

詳細については、「"Audit Assistantのトレーニングについて" ページ397」を参照してください。

予測ポリシーについて

Fortify Audit Assistantを使用してスキャン結果を予測するには、最初に少なくとも1つの予測ポリシーを定義する必要があります。予測ポリシーは、予測に対する信頼しきい値を確立するために使用されます。デフォルトの信頼しきい値は80%に設定されていますが、0 ~ 100%の間で10%単位で設定できます。信頼しきい値を上げると結果の信頼性が向上し、設定されたしきい値以上の結果のみに絞り込まれます。しきい値を調整することで、ソフトウェア環境に合わせて予測ポリシーを微調整できます。

次の2種類の信頼しきい値を設定できます。

- 誤検出(False Positive)
- 悪用可能(Exploitable)

最小信頼しきい値を満たしていない場合、予測は行われません。信頼しきい値未満の信頼レベルは不定で、Fortify Audit Assistantでは、設定された信頼レベルに基づく評価を提供できません。

注: Fortify Audit Assistant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、対象となるアプリケーションバージョンに対して予測ポリシーが指定されていない場合に使用されます。アプリケーションバージョンに予測ポリシーが指定されている場合、Fortify Audit Assistantはそのポリシーを使用して問題を評価します。

参照情報

"予測ポリシーの定義" 次のページ

"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389"Audit Assistantの設定" ページ385

"Audit Assistantの設定" ページ385

"監査アシスタントの自動予測について" ページ90

予測ポリシーの定義

Fortify Audit Assistantを使用するには、Fortify Audit Assistantでどの問題を悪用可能、誤検出、または不定として扱うかを判断するの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" 前のページ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 Audit Assistant (https://analytics.fortify.com)にログインするか、初めてセットアップする場合は、次の操作を実行します。

   メモ: Fortify Audit Assistantをオンプレミスで使用している場合、ログインにはインストールに固有のURLを使用します。

2. 画面の右上で、セレクタボタンから [**Audit Assistant G2**]を選択します。
3. OpenTextのヘッダで、 [**予測ポリシー(PREDICTION POLICIES)**]を選択します。 [予測ポリシー(Prediction Policies)] | [**追加(Add)**]ページが表示されます。
4. [**+追加(+ ADD)**]ボタンをクリックします。
5. [**詳細(Details)**]セクションで、次の操作を実行します。
   - 予測ポリシーの名前を [**名前(Name)**]フィールドに入力します。
   - (オプション)予測ポリシーの説明を [**説明(Description)**]フィールドに入力します。
   - Audit Assistantトレーニングデータセレクタから[Fortify]データを選択します。

   右側のペインには、Audit Assistantで [**悪用可能(Exploitable)**]または [**誤検出(False Positive)**]として処理する問題を設定するために使用する2つの信頼しきい値設定があります。

   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。使用可能な値は、 [**悪用可能(Exploitable)**]、 [**不定(悪用可能]しきい値未満) (Indeterminate (Below Exploitable threshold))**]、 [**問題でない(Not an Issue)**]、 [**不定(問題でない]しきい値未満) (Indeterminate (Below Not An Issue threshold))**]、および [**予測なし(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、Audit Assistantは問題を不定として扱い、 [**AA_Prediction**]値に [**予測なし(Not Predicted)**]を割り当てします。

6. 予測信頼しきい値スライダ、 [**悪用可能(Exploitable)**]、および [**誤検出(False Positive)**]を、環境内で実行されているアプリケーションに対して許容可能なレベルに設定します。

注: 信頼しきい値の値を高く設定するほど、 [悪用可能(Exploitable)]または [誤検出(False Positive)]として識別される問題の数が増えます。環境に最適な結果を得るには、まずデフォルトの信頼しきい値(80%)を使用し、必要に応じて調整します。

7. [**保存(SAVE)**]をクリックします。

参照情報

"予測ポリシーについて" ページ381

"Audit Assistantの設定" ページ385

"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389

Fortify Audit Assistantの設定の更新

Fortify Software Security Centerをバージョン23.2.0以降にアップグレードしたら、Fortify Audit Assistant 23.2.0以降と連携できるように設定を行う必要があります。Fortify Audit Assistantでは第2世代の(G2)予測エンジンが追加されており、Fortify Software Security Center 23.2.0以降ではこれを使用する必要があります。

Fortify Audit AssistantへのFortify Software Security Center接続を更新するには:

1. G2予測ポリシーを1つ以上作成します。詳細については、"予測ポリシーの定義" 前のページを参照してください。

   注: Fortify Audit Assistant 23.2.0より前のバージョンで作成された予測ポリシーは使用できません。Fortify Software Security Centerをバージョン23.2.0以降にアップグレードすると、第1世代(G1)のポリシーは使用できなくなります。それらはアップグレード中に削除されます。G2エンジンで動作する新しい予測ポリシーを作成する必要があります。

2. OpenTextのヘッダで、 [**管理(Administration)**]をクリックします。
3. 左ペインで、 [**設定(Configuration)**]をクリックして、 [**Audit Assistant**]をクリックします。

   [Audit Assistant]ページが表示されます。
4. [**Audit Assistantを有効にする(Enable Audit Assistant)**]チェックボックスをオンにします。
5. [**ポリシーの更新(Refresh Policies)**]ボタンをクリックし、設定を保存します。

   Audit Assistantが正しく設定されると、 [Audit Assistantのポリシーの更新(AUDIT ASSISTANT REFRESH POLICIES)]ウィンドウが表示され、「更新に成功しました(Refresh was successful)」というメッセージが表示されます。これで、SSCのすべての予測ポリシーが一貫します。 [OK]をクリックします。
6. [デフォルトの予測ポリシー(Default prediction policy)]ボックスで、デフォルトとして使用するポリシーを選択します。予測ポリシーをアプリケーションバージョンに割り当てない場合、ここで選択したデフォルトが使用されます。 [**保存(SAVE)**]をクリックします。

7. (オプション)アプリケーションバージョンレベルで予測ポリシーを設定できるようにするには、 **特定のアプリケーションバージョンのポリシーを有効にする(Enable specific application version policies)**] チェックボックスをオンにします。
8. (オプション)プロジェクト内の未監査の問題にFortify Audit Assistantで予測を自動的に適用するには、 **自動予測を有効にする(Enable auto-prediction)**] チェックボックスをオンにします。
9. (オプション)Fortify Audit Assistantで予測値をカスタムタグに自動的に適用するには、 **自動適用を有効にする(Enable auto-apply)**] チェックボックスをオンにします。

Audit Assistantの使用

次のセクションでは、Audit Assistantワークフローの概要について説明します。

Audit Assistantワークフロー

Fortify Audit Assistantを使用したワークフローは次のとおりです。

1. バージョン23.2.0以降にアップグレードした後に、Fortify Audit Assistantの設定を更新します。詳細については、"Fortify Audit Assistantの設定の更新" 前のページを参照してください。
2. Fortify Audit Assistantアカウントを取得します。
   a. https://analytics.fortify.comに移動します。

   b. **アカウントが必要ですか? (Need an Account?)**] リンクをクリックします。
   Fortify Audit Assistantテナントの要求(Request a Fortify Audit Assistant Tenant)] ウィンドウが表示されます。
   c. 会社情報を入力し、 **購読(Subscribe)**] ボタンをクリックします。
   情報の確認が完了すると、ようこそ電子メールが届きます。
3. Fortify Audit Assistantにログインして、1つ以上の予測ポリシーを作成します。詳細については、"予測ポリシーの定義" ページ382を参照してください。
4. Fortify Fortify Audit Assistantトークンを取得します。詳細については、"Fortify Audit Assistant認証トークンの取得" ページ389を参照してください。
5. Fortify Software Security CenterのAudit Assistant設定ページから、次の手順を実行します。

- Fortify Audit Assistantへの接続を設定およびテストし、 **ポリシーの更新(REFRESH POLICIES)**]をクリックして、 **デフォルトの予測ポリシー(Default prediction policy)**]リストに値を自動入力します。
- デフォルトの予測ポリシーを指定します。
- (オプション)Audit Assistantで、未監査の問題をFortify Fortify Audit Assistantに自動的に送信して予測を実施できるようにします。
- (オプション)Audit Assistantで、カスタムタグに予測値を自動的に適用できるようにします。

  詳細については、"Audit Assistantの設定" 下を参照してください。

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。このステップは「トレーニング」と呼ばれます。詳細については、「"Audit Assistantへのトレーニングデータの送信" ページ399」を参照してください。
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、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、Fortify Audit Assistantから認証トークンを取得し、そのトークンを使用してFortify Audit Assistant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Fortify Audit Assistantを準備し、データを送信し、Audit Assistant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" ページ381

"予測ポリシーの定義" ページ382

"Audit Assistantの設定" 下

"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391

"Audit Assistantへのトレーニングデータの送信" ページ399

"Audit Assistantの結果の確認" ページ396

Audit Assistantの設定

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

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

1. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで **管理(Administration)**]を選択します。
2. 左ペインで、 **設定(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
Audit Assistantを有効にする(Enable Audit Assistant)]チェックボックス	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 Audit Assistantから取得した認証トークンをここに貼り付けます。トークンの取得手順については、 **トークンの取得方法(How do I get a token?)**]を選択します。または、"Fortify Audit Assistant認証トークンの取得" ページ389を参照してください。
* Fortify Audit AssistantサーバURL	Fortify Audit AssistantサーバのURLを指定します。
Audit Assistantにプロキシを使用(Use SSC proxy for Audit Assistant)	すべてのFortify Software Security Center統合にプロキシを設定してある場合("Fortify Software Security Center統合のプロキシの設定" ページ132を参照)、このチェックボックスを選択すると、Fortify Audit Assistantに対してそのプロキシを使用できます。

4. Fortify Audit Assistantサーバへの接続をテストするには、 **接続のテスト(TEST CONNECTION)**]をクリックします。
   接続が正常にテストされたら、先に進んで、 **監査設定(Audit settings)**]セクションで次の設定をします。
5. **ポリシーの更新(REFRESH POLICIES)**]をクリックして、 **デフォルトの予測ポリシー(Default prediction policy)**]リストに、Fortify Audit Assistantサーバ上の現在のサーバポリシーを入力します。

> **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 Audit Assistant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 **ポリシーの更新(REFRESH POLICIES)**]をクリックするたびに、Fortify Audit Assistantから受け取る新しい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。

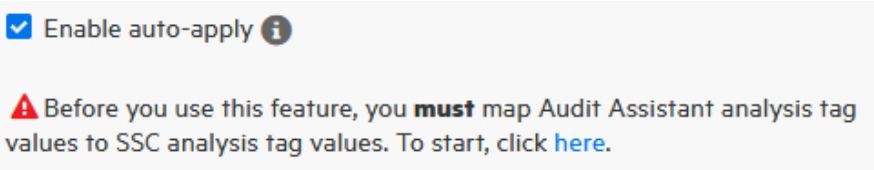
6. **Default prediction policy**]リストから、すべてのアプリケーションバージョンに適用する予測ポリシーの名前を選択します。(ポリシーはFortify Audit Assistantで定義されます)。
7. 予測ポリシーをアプリケーションバージョンレベルで指定し、デフォルトのグローバル予測ポリシーを上書きする場合は、 **特定のアプリケーションバージョンのポリシーを有効にする(Enable specific application version policies)**]を選択します。それ以外の場合、Fortify Audit Assistantは前のステップで指定したデフォルトのグローバル予測ポリシーを使用します。

注: アプリケーションバージョンのポリシーは、 [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスから指定できます。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389を参照してください。

8. 未監査の問題をFortify Software Security Centerで自動的にFortify Audit Assistantに送信して評価が行われるようにするには、 **自動予測を有効にする(Enable auto-prediction)**]チェックボックスをオンにします。その後、 [アプリケーションプロファイル(APPLICATION PROFILE)]ウィンドウから、アプリケーションバージョンごとにこの機能を有効にする必要があります。(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" ページ90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の [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスを開き、そこでも自動予測を有効にします。

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、 **自動適用を有効にする(Enable auto-apply)**]チェックボックスをオンにします。その後、 [アプリケーションプロファイル(APPLICATION PROFILE)]ウィンドウから、アプリケーションバージョン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の [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスを開き、そこでも自動適用を有効にします。

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。

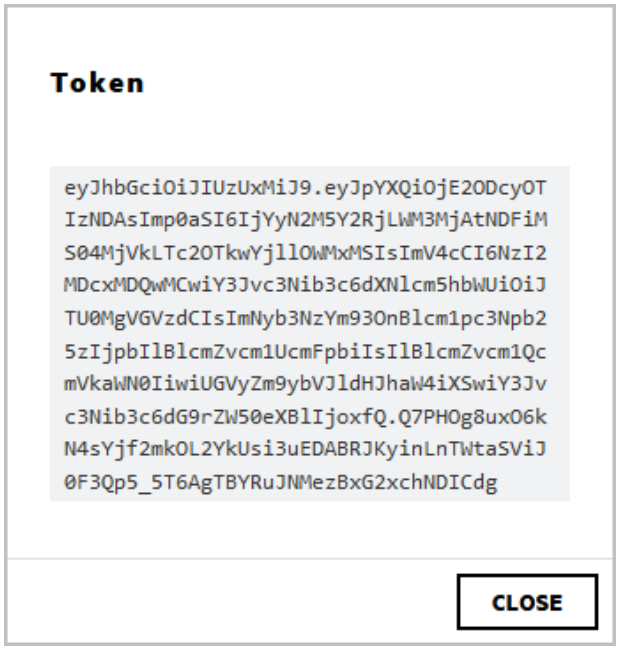
10. **自動適用を有効にする(Enable auto-apply)**] チェックボックスがオンにしてあり、Audit Assistant分析タグの値をFortify Software Security Center Analysisタグ値にすぐにマップしたい場合は、 **こちら(here)**] リンクをクリックして **カスタムタグ(Custom Tags)**] ページに移動し、"Fortify Software Security Centerカスタムタグ値へのAudit Assistant分析タグ値のマッピング" ページ392に記載されている手順に従います。
11. **保存(SAVE)**] をクリックします。

Fortify Audit Assistant認証トークンの取得

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

Fortify Audit Assistant認証トークンを取得するには:

1. Fortify Audit Assistantにログオンします。
2. OpenTextのヘッダで、 **管理(ADMINISTRATION)**]をクリックし、 **トークン(TOKENS)**]を選択します。
3. トークン(Tokens)]ページで、 **+追加(+ADD)**]をクリックします。
4. **名前(Name)**]フィールドに、生成するトークンの名前を入力します。
5. **保存(SAVE)**]をクリックします。
   トークン(Tokens)]ページに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。



7. トークン(Tokens)]ウィンドウで、トークンテキストを選択してコピーし、 **閉じる(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" ページ385を参照してください)。

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

Fortify Audit Assistantを設定する際に **特定のアプリケーションバージョンのポリシーを有効にする(Enable specific application version policies)**]を選択した場合は、アプリケーションバージョンのデフォルト設定を上書きすることができます。これを選択しなかった

場合は、すべてのアプリケーションバージョンでデフォルト設定が使用されます。アプリケーションバージョンレベルでデフォルト設定を上書きする機能を使用したい場合は、"Audit Assistantの設定" ページ385を参照してください。

アプリケーションバージョンに対してFortify Audit Assistantオプションを設定するには:

1. アプリケーションで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385を参照してください)。
2. ダッシュボードから、Fortify Audit Assistantオプションを設定するアプリケーションバージョンを選択します。
3. [監査(AUDIT)]ページで、 **[プロファイル(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385を参照してください)。それ以外の場合、Fortify 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、Fortify Audit Assistantはデフォルトの予測ポリシーを使用します。
6. このアプリケーションバージョンの監査されていない問題を評価のためにFortify Audit Assistantサーバに送信するには **[自動予測を有効にする(Enable auto-prediction)]**をオンにします。

   注: [自動予測を有効にする(Enable auto-prediction)]および **[自動適用を有効にする(Enable auto-apply)]**チェックボックスは、これらの監査設定がシステム全体で有効になっている場合にのみ使用できます。("Audit Assistantの設定" ページ385を参照してください)。
7. マップされたカスタムタグ値に予測値がFortify Audit Assistantによって自動的に適用されるようにするには、 **[自動適用を有効にする(Enable auto-apply)]**チェックボックスをオンにします。
8. **[適用(APPLY)]**をクリックします。
9. Fortify Software Security Centerにより、これらのオプションの保存を確認するメッセージが表示されます。 **[OK]**をクリックします。
10. **[CLOSE]**をクリックします。

参照情報

"Audit Assistantの設定" ページ385

アプリケーションバージョンの自動適用と自動予測を有効にする

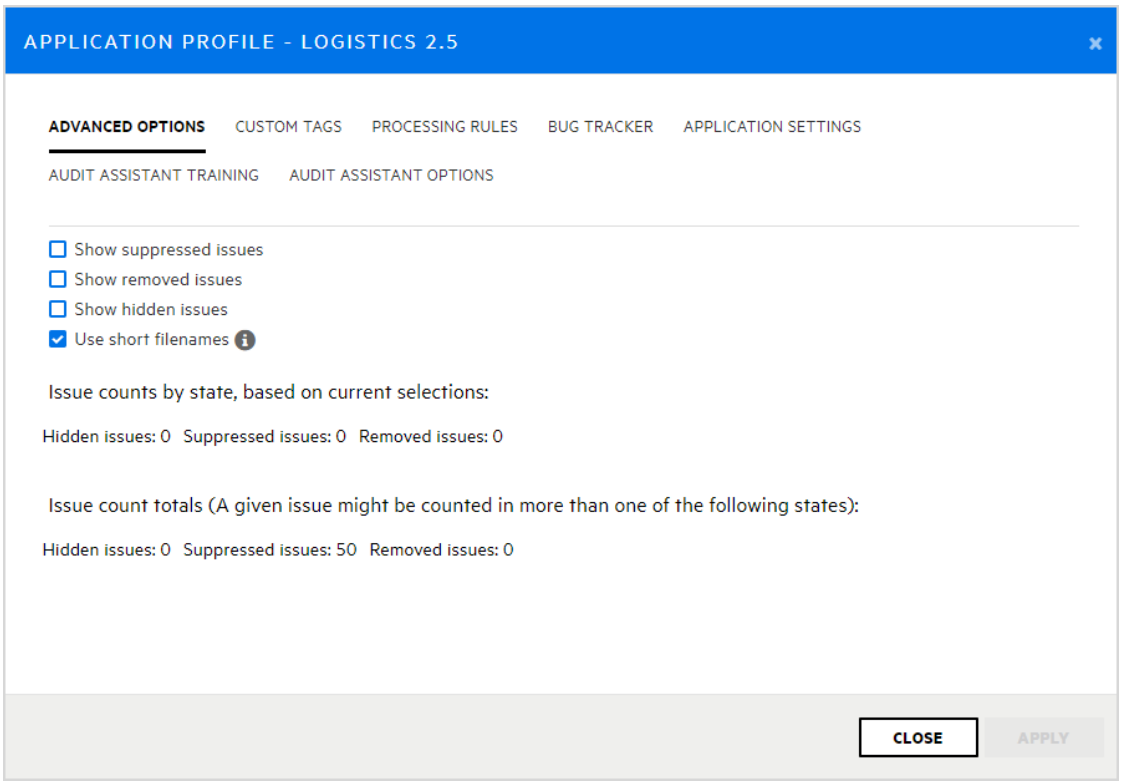
管理者がFortify Audit Assistantを設定し、自動適用をシステム全体で有効にし、[管理(Administration)]ビューの[カスタムタグ(Custom Tags)]セクションで適切なプライマリタグフィールドをマップしてある場合、ユーザは特定のアプリケーションバージョンに対して自動適用を有効にできます。

自動適用をアプリケーションバージョンで有効にした場合、Fortify Audit Assistantを使用して静的分析の問題に関する予測を要求すると、Fortify Software Security Centerがそれらの予測をカスタムタグ値に適用します。

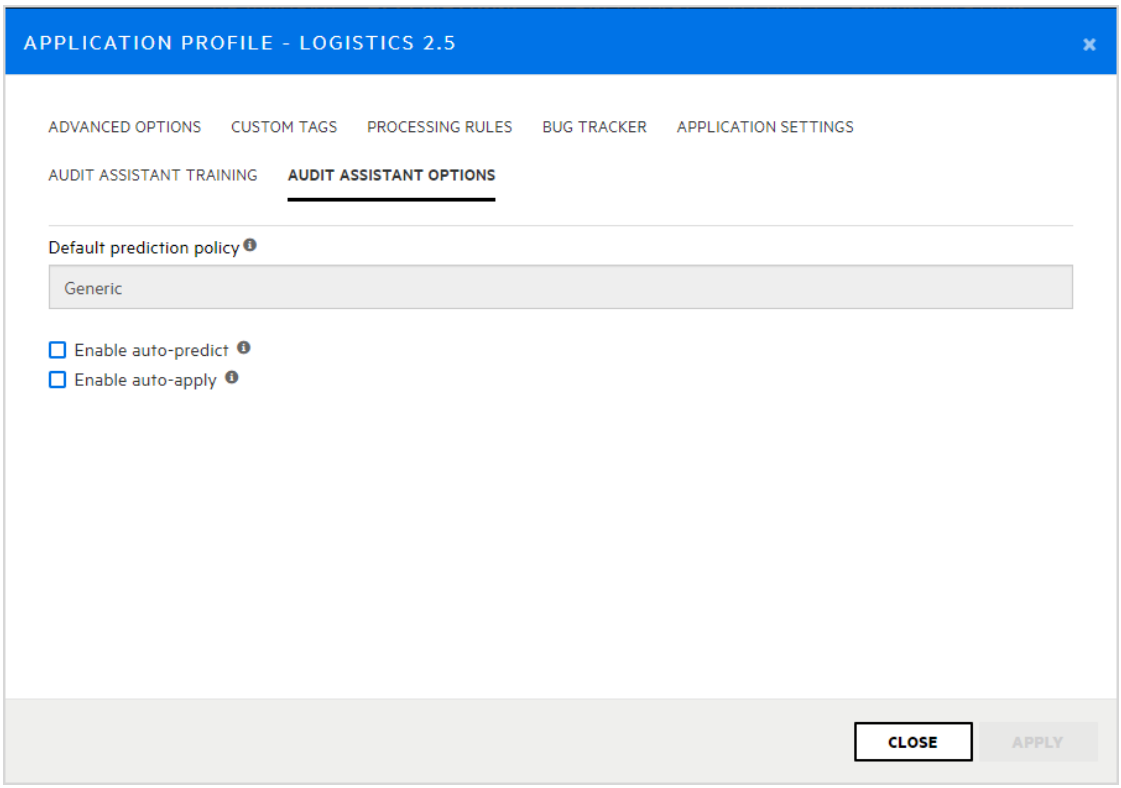
Fortify Audit Assistantが自動的にカスタムタグ値を問題に適用すると、その問題のために保存されたメタデータは、それがFortify Audit Assistantによって監査されたことを示します。カスタムタグ名の横にグレーの小槌が表示されて、ユーザはFortify Audit Assistantがその問題を予測したことを確認できます。

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. 未監査の問題をFortify Audit Assistantで自動的に評価するには、**自動予測を有効にする(Enable auto-predict)**]チェックボックスをオンにします。(自動予測の詳細については、"監査アシスタントの自動予測について" ページ90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385

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

Fortify Audit AssistantをFortify Software Security Centerと一緒に使用するには、Fortify Audit Assistant分析タグ値をリストタイプのFortify Software Security Centerカスタムタグ値にマップする必要があります。Fortify Audit Assistant分析タグ値は、Fortify

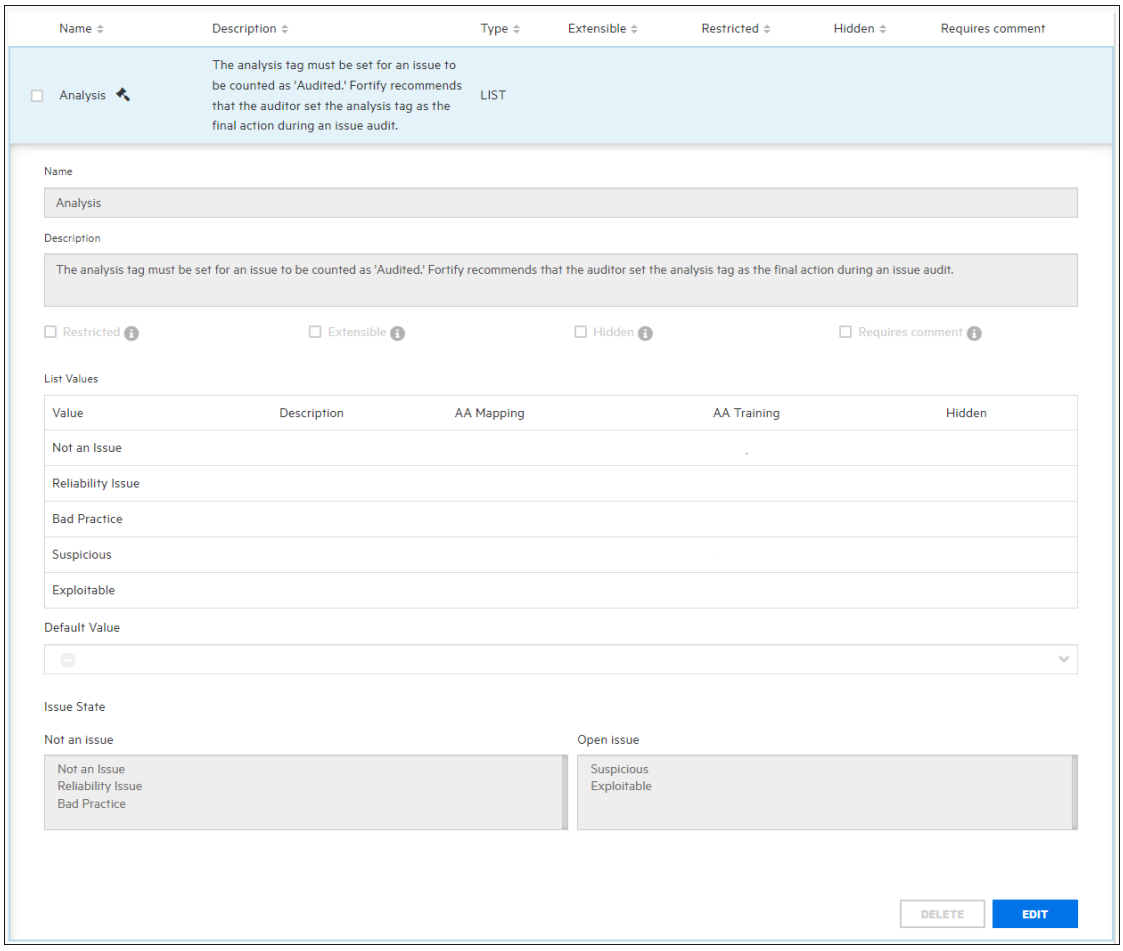
Software Security Centerと一緒にインストールされ、脆弱性を監査済みとして識別するために必要な「分析(Analysis)」カスタムタグにマップすることもできますが、その目的のために別のリストタイプのカスタムタグを選択することもできます。

Fortify Audit Assistantの設定時に「自動適用を有効にする(Enable auto-apply)」チェックボックスをオンにした場合、どのFortify Audit Assistant分析タグ値をリストタイプのカスタムタグ値に自動的に適用するのかを、AAに通知することもできます。

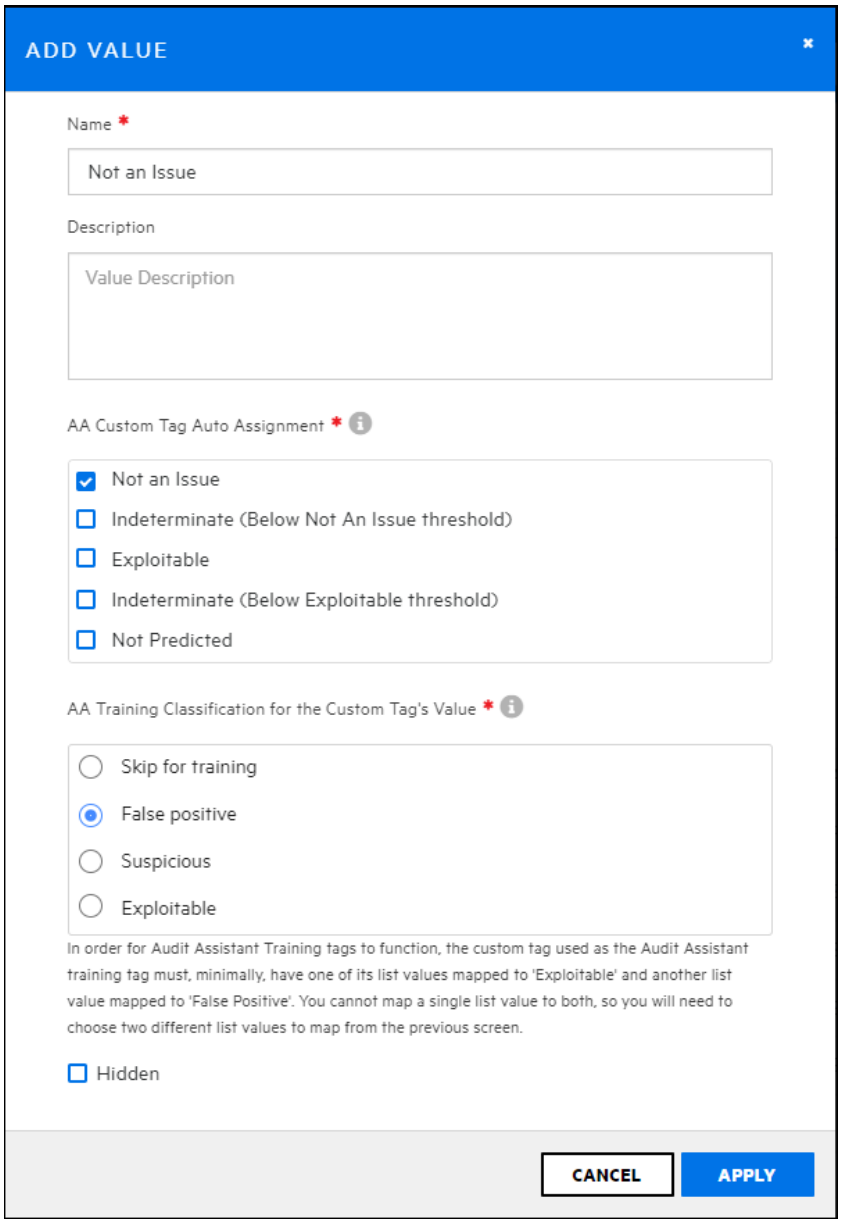
メモ: カスタムタグ値をまだ作成していない場合は、値を作成してFortify Audit Assistantにマップする方法について、"カスタムタグ値の追加" ページ287を参照してしてください。デフォルトの「分析(Analysis)」カスタムタグか自分で作成したカスタムタグを使用している場合は、このセクションの手順に従います。

Fortify Audit Assistant分析タグ値をリストタイプのFortify Software Security Centerカスタムタグ値にマップするには:

1. OpenTextのメニューバーで、**「管理(Administration)」**をクリックします。
2. 左ペインで、**「テンプレート(Templates)」**をクリックし、**「カスタムタグ(Custom Tags)」**をクリックします。
   「カスタムタグ(Custom Tags)」ページにカスタムタグが一覧表示されます。
3. 値を編集するタグの行をクリックします。
   行が展開されて、タグの詳細が表示されます。



4. 画面の右下隅で、 **編集(EDIT)**]をクリックします。
   行の最後に、テーブル内の値の 編集(EDIT)]アイコン(✎)が表示されます。
5. 値の 編集(EDIT)]アイコン(✎)をクリックします。
   値の追加(ADD VALUE)]ダイアログボックスが表示されます。



6. Fortify Audit Assistantを使用するようにFortify Software Security Centerが設定され、自動適用が有効になっている場合、[値の追加(ADD VALUE)]ダイアログには[AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)]セクションと、[カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)]セクションが表示されます。
7. 新しい値が[AAカスタムタグの自動割り当て(AA Custom Tag Auto Assignment)]セクションのAudit Assistantの予測値と一致する場合は、そのチェックボックスをオンにすると、選択したAudit Assistantの予測値にそのリスト値が自動的にマップされます。これにより、アプリケーションバージョンの[プロファイル]の[**Audit Assistantオプション(Audit Assistant Options)**]セクションで[**自動適用を有効にする(Enable auto-apply)**]を選択しているすべてのアプリケーションバージョンに対して、自動監

査が有効になります。

8. Fortify Audit Assistantモデルのトレーニング時に新しい値を使用する場合は、 [カスタムタグ値のAAトレーニング分類(AA Training Classification for the Custom Tag's Value)] セクションでラジオボタンを選択します。Fortify Audit Assistantトレーニングタグが機能するには、少なくとも2つのリスト値をAudit Assistantトレーニングタグにマップする必要があります。1つは [誤検出(False Positive)] Fortify Audit Assistantトレーニングタグにマップされ、もう1つのリスト値は [悪用可能(Exploitable)] Fortify Audit Assistantトレーニングタグにマップされる必要があります。
9. 追加のリスト値をマップするには、ステップ6 ~ 9を繰り返します。
10. Fortify Audit Assistantトレーニングタグにマップする必要があるすべてのリスト値を編集し終えたら、 **[適用(APPLY)]** をクリックして、 **[保存(SAVE)]** をクリックします。

参照情報

"Audit Assistantの設定" ページ385

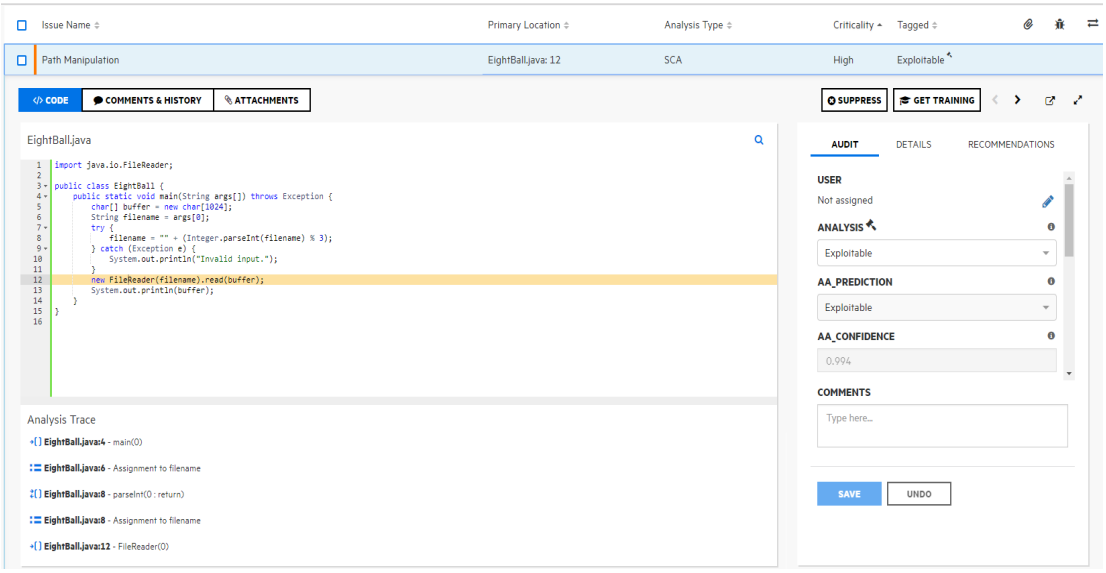
"カスタムタグ値の追加" ページ287

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。("フォルダに基づく問題の表示" ページ347と" [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349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0.994は、99.4%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379

"スキャン結果の監査" ページ358

Audit Assistantのトレーニングについて

ユーザは、スキャン結果の監査時に監査官が行った決定を使用してAudit Assistantをトレーニングできます。ユーザが提供するトレーニングデータを使用することにより、Fortify Audit Assistantは、ユーザの環境内で実行されているアプリケーションに対してより正確で関連性の高い予測を行えます。ユーザが送信するデータは、監査済みのスキャン結果に基づいて生成および計算される機密でないメタデータです。

デフォルトでは、 [Audit Assistantトレーニングタグ(Audit Assistant Training Tag)]として他のカスタムタグが選択されていない場合、プライマリカスタムタグが [Audit Assistantトレーニングタグ(Audit Assistant Training Tag)]として設定されます。

トレーニングデータをFortify Audit Assistantに提供するようにFortify Software Security Centerを設定するには:

- [Audit Assistantトレーニングタグ(Audit Assistant Training Tag)]として使用するカスタムタグを選択します。デフォルトの[分析(Analysis)]カスタムタグを使用するか、自分で作成したタグを選択できます。カスタムタグを選択しない場合、Fortify Audit Assistantではプライマリタグが使用されます。詳細については、"Audit Assistantトレーニングタグの選択" 下を参照してください。
- カスタムタグ値をFortify Audit Assistantのトレーニングタグ値にマップします。詳細については、"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" ページ392を参照してください。
- トレーニングデータをFortify Audit Assistantに送信します。詳細については、"Audit Assistantへのトレーニングデータの送信" 次のページを参照してください。

参照情報

Audit Assistantトレーニングタグの選択

Audit Assistantトレーニングタグの選択

Fortify Audit Assistantトレーニングを設定するときに、Fortify Audit Assistantのトレーニングに使用するカスタムタグを選択する必要があります。カスタムタグを選択しない場合は、プライマリタグが使用されます。

Audit Assistantトレーニングタグを選択するには:

1. 管理者としてFortify Software Security Centerにログインし、OpenTextのヘッダで[**アプリケーション(Applications)**]を選択します。
2. [アプリケーション(Applications)]ページで、アプリケーションバージョンを選択し、表示されるメニューから[**監査(Audit)**]を選択します。
   [監査(Audit)]ページが表示されます。
3. [監査(Audit)]ページで、[**プロファイル(PROFILE)**]ボタンを選択します。
   [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスが表示されます。
4. [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスで、[**カスタムタグ(CUSTOM TAGS)**]を選択します。
5. [分析(Analysis)]カスタムタグとユーザが作成したカスタムタグを含むテーブルが表示されます。[Audit Assistantトレーニングタグ(Audit Assistant Training Tag)]として使用するカスタムタグを選択します。
6. [**AAトレーニングタグの選択(SELECT AA TRAINING TAG)**]ボタンをクリックします。
   [Audit Assistantトレーニングタグの選択(SELECT AUDIT ASSISTANT TRAINING TAG)]ダイアログが表示されます。

選択したカスタムタグがトレーニング用にまだ設定されていない場合、 [AAトレーニングタグの選択(SELECT AA TRAINING TAG)] 選択ボックスには **[未設定(Not Set)]** と表示されます。

7. **[AAトレーニングタグの選択(SELECT AA TRAINING TAG)]** 選択ボックスをクリックし、選択ボックスのリストからAudit Assistantトレーニングタグとして使用するカスタムタグを選択します。

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。以前のバージョンのFortify Audit Assistantでは、Fortify Software Security Center環境から転送されたデータはすべて匿名化され、G1モデルのトレーニングために使用されました。Fortify Audit Assistantのバージョン23.2.0以降では、ユーザのデータをFortify Audit Assistantで使用して、ユーザの環境で実行されているアプリケーションに関してより正確かつ関連性のある予測を行うことができるようになります。ユーザが送信するデータは、監査済みのスキャン結果に基づいて生成および計算される機密でないメタデータです。

デフォルトでは、Audit Assistantトレーニングタグが未選択か [未設定(Not Set)] に設定されている場合、プライマリカスタムタグがFortify Audit Assistantトレーニングタグとして使用されます。

トレーニングデータをFortify Audit Assistantに送信するには:

1. [ダッシュボード(Dashboard)] から、目的のアプリケーションバージョンにカーソルを合わせて、アクションメニューを表示します。そのアプリケーションバージョンの [概要(OVERVIEW)]、 [アーティファクト(ARTIFACTS)]、 [監査(AUDIT)]、または [トレンド(TREND)] ページを選択します。
2. アプリケーションバージョンツールバーで、 **[プロファイル(PROFILE)]** ボタンをクリックします。
3. [アプリケーションプロファイル(APPLICATION PROFILE)] ダイアログボックスで、 **[Audit Assistantトレーニング(AUDIT ASSISTANT TRAINING)]** タブをクリックします。

   > **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385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。

   [トレーニング用のデータ最終送信(Data last sent for training)] フィールドが、現在の日時で更新されます。
5. トレーニングデータを送信すると、 **[トレーニング用のデータ最終送信(Data last sent for training)]** フィールドに更新された日時が表示されます。

6. [アプリケーションプロファイル(APPLICATION PROFILE)]ダイアログボックスを閉じます。
7. アプリケーションバージョンツールバーで [アーティファクト(ARTIFACTS)]をクリックし、アップロードの [ステータス(Status)]フィールドが [完了(Complete)]になっているかどうかを確認します。

処理が完了したら、 [監査(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" ページ396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379

"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391

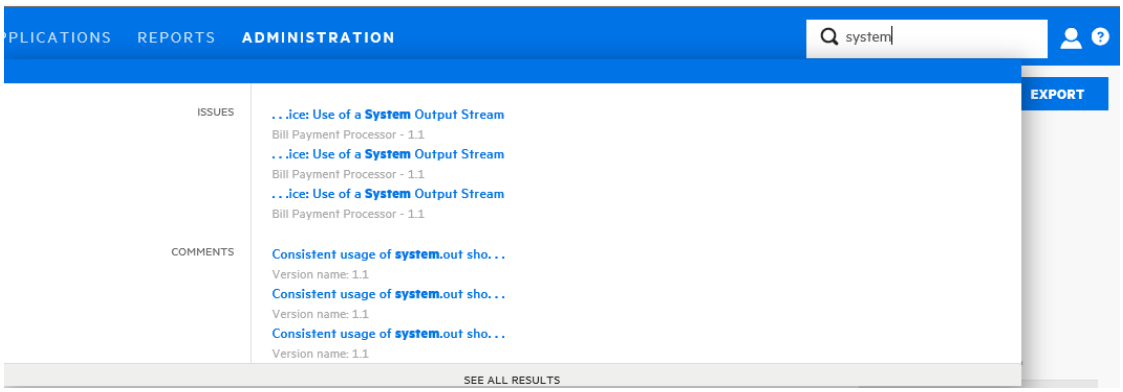
Fortify Software Security Centerでのグローバル検索

Fortify Software Security Centerユーザインタフェースの場所に関係なく、OpenTextヘッダのグローバル [検索(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70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。

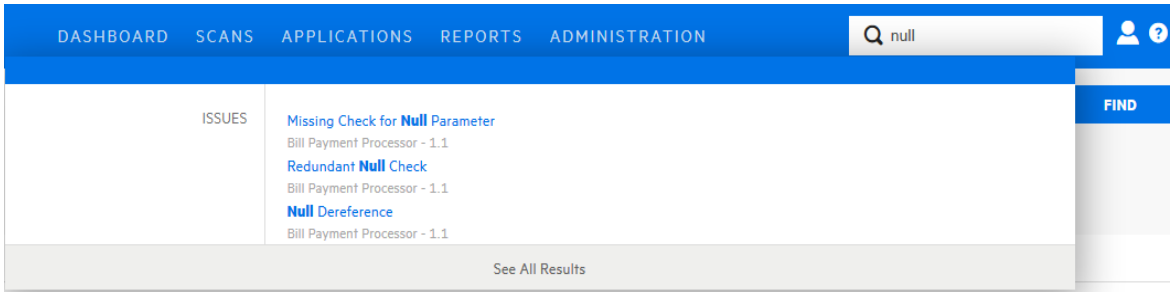


   Fortify Software Security Centerは、検索文字列に一致する最初のいくつかの項目をカテゴリ別に表示します。アプリケーションのバージョンも表示されます。
2. リストされている特定の項目に移動するには、項目をクリックします。

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

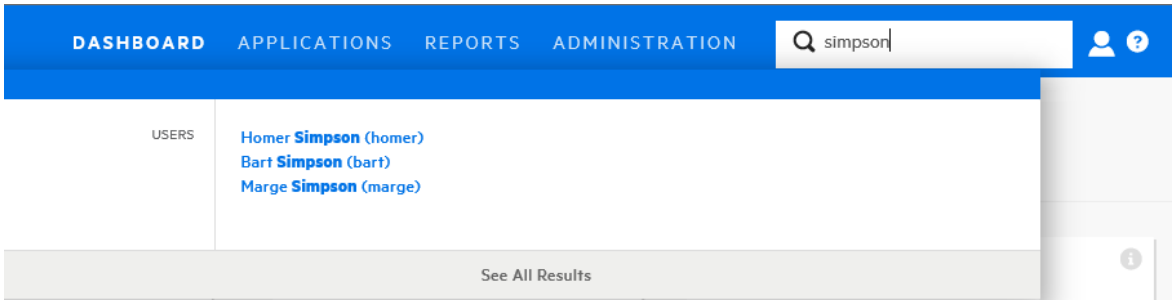


表示された結果から問題を選択すると、Fortify Software Security Centerで対応するバージョンページが表示され、問題のフルビューが展開されます。

[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。

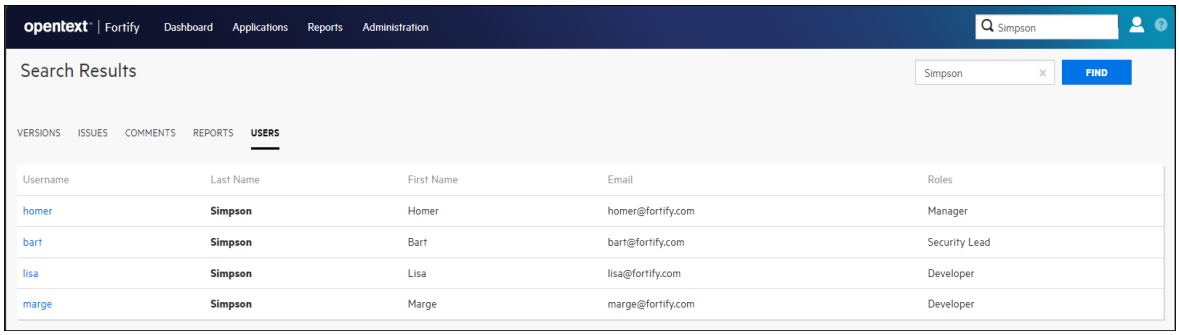
注: 問題の検索結果には、削除、非表示、または抑止された問題が含まれます。選択した項目が[AUDIT]ページに表示されない場合は、アプリケーションバージョンの表示設定をチェックして、[ADVANCED OPTIONS]タブで適切なフラグが有効になっているか確認し、削除、非表示、および抑止された問題を表示します。手順については、"問題の表示設定の設定" ページ368を参照してください。

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[管理(Administration)]ビューでユーザアカウントの詳細が表示されます。

[すべての結果を表示(See All Results)]を選択すると、Fortify Software Security Centerで[検索結果(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 263

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

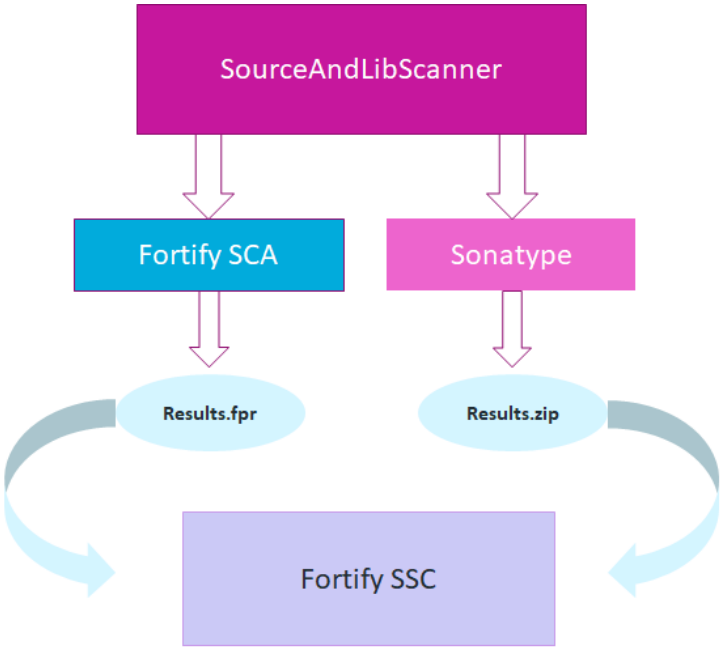
プラグインをダウンロードして設定する方法については、"Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ178を参照してください)。

- Fortify SourceAndLibScanner

  SourceAndLibScannerを取得するには、https://marketplace.microfocus.com/cyberres/content/fortify-sourceandlibscannerにアクセスしてください。

  SourceAndLibScannerのソフトウェア要件、およびツールのインストールおよび使用方法については、SourceAndLibScannerユーティリティにパッケージされている『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178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 Fortify Static Code Analyzer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スキャンまたはSonatypeライブラリスキャンを実行してから、結果をFortify Software Security Centerにアップロードする方法の詳細については、『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。

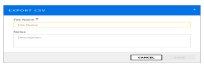
   注: SourceAndLibScannerを使用して開始されたFortify Static Code Analyzerスキャンによって明らかにされた問題は、Sonatypeの検出結果のコンテキストでのみ重大です。この結果、 [AUDIT]ページでデフォルトでは非表示になります。

5. [オープンソース(OPEN SOURCE)]ページからの結果を監査します。Sonatypeの問題は [監査(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 [オープンソース(OPEN SOURCE)]ページでのみ表示され、 **[呼び出し済み(Invoked)]**、 **[制御可能(Controllable)]**、および **[証拠(Evidence)]**フィールドで表されます。

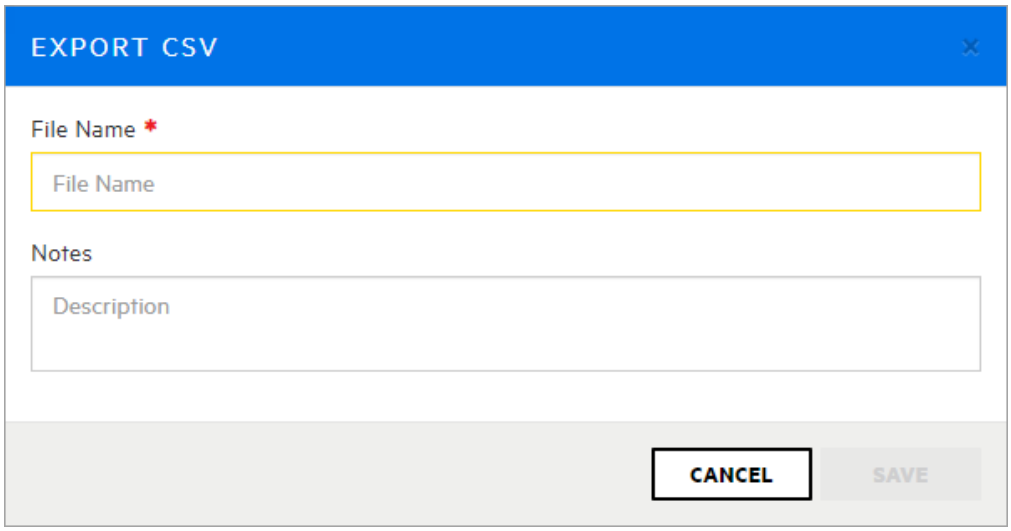
オープンソースデータのエクスポート

[オープンソースコンポーネント(OPEN SOURCE COMPONENTS)]ページに表示されるオープンソースデータをエクスポートするには:

1. Fortify Software Security Centerでアプリケーションバージョンのオープンソースデータをアップロードした後に、そのアプリケーションバージョンの [オープンソースコンポーネント(OPEN SOURCE COMPONENTS)]ページに移動します。



2. [CSVのエクスポート(EXPORT CSV)]ダイアログボックスを開くには、 [オープンソースコンポーネント(OPEN SOURCE COMPONENTS)]テーブルの上で **[エクスポート(EXPORT)]**をクリックします。



3. [ファイル名 (File Name)] ボックスに、生成するCSVファイルの名前を入力します。
4. (オプション) [Notes] ボックスに、生成されたファイルに関連付けるメモを入力します。
5. [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. OpenTextのヘッダで、 [レポート (Reports)] をクリックします。
   b. [データエクスポート (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135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327)。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

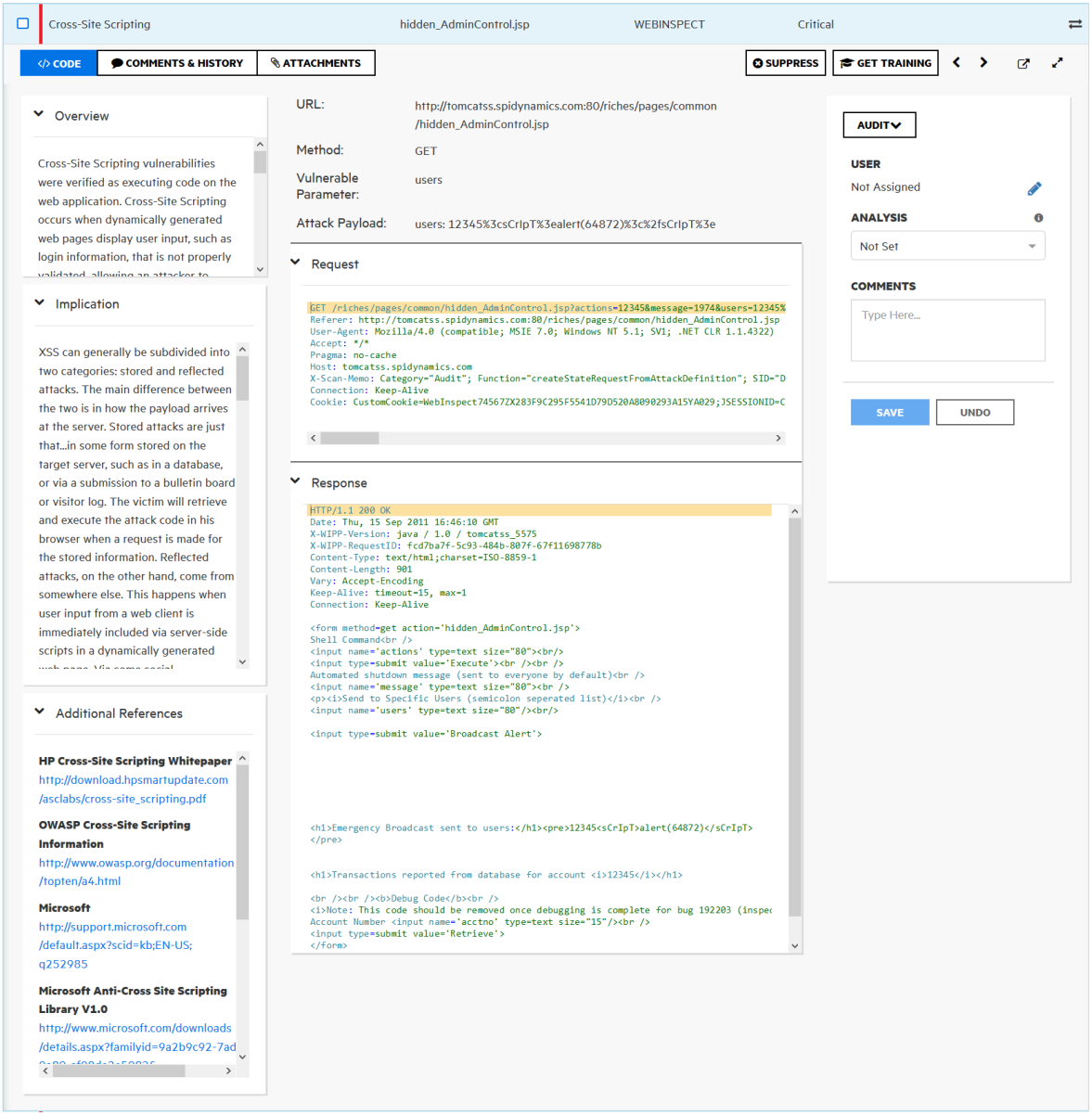
Method: 攻撃に使用されるHTTPメソッド(GET、PUT、POSTなど)

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。



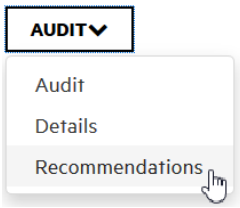
[Steps] タブは、ステップがWebInspectの結果ファイルに含まれている場合にのみ使用できます。

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、"スキャン結果の監査" ページ358を参照してください。

WebInspectの監査データ

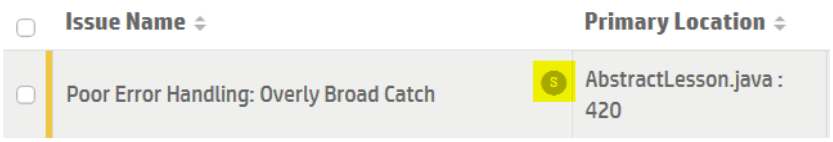
スクリーンショットに加えて、次の種類の監査データがWebInspectからFortify Software Security Centerに転送されます。

- **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では 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

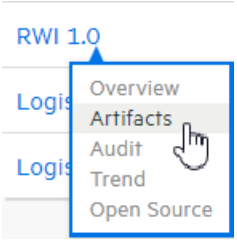
"問題の表示設定の設定" ページ368

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。
3. 動的スキャン(DYNAMIC SCAN) - <APPLICATION VERSION> (DYNAMIC SCAN - <*APPLICATION VERSION*>)]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。

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

ダイナミックスキャン属性 * (必須フィールド)	説明
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" 次のページを参照してください。

参照情報

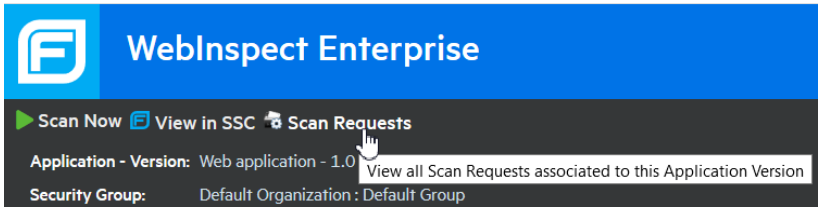
"Fortify Software Security CenterでのFortify WebInspectスキャン結果の表示" ページ 406

Fortify WebInspect Enterpriseの動的スキャン要求の処理

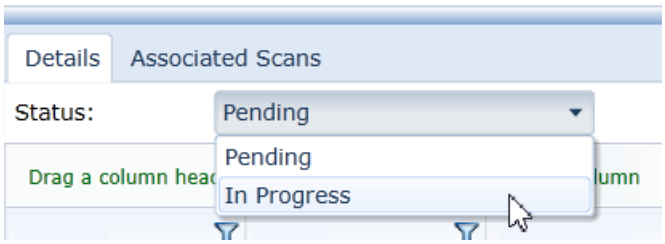
管理者またはアプリケーションセキュリティテスタの役割を持っている場合は、Fortify WebInspect Enterpriseを起動して、Fortify Software Security Centerユーザが送信した動的スキャン要求を表示および処理できます。

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、『OpenText™ 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『OpenText™ 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409

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409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。
3. [動的スキャン要求(Dynamic Scan Request)] ダイアログボックスで、動的スキャン属性の値を編集してから、 [送信(Submit)] をクリックします。

動的スキャン要求をキャンセルする

保留中の動的スキャン要求をキャンセルするには、次の手順に従います。

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。

オープンソースデータの表示

Fortify Software Security Center用のDebrickedまたはSonatypeパーサプラグインをダウンロードして、インストールし、有効にしたら("Debricked結果を表示するためのFortify Software Security Centerの準備" ページ180と"Sonatype結果を表示するためのFortify Software Security Centerの準備" ページ178を参照)、アプリケーションバージョンに関する、Fortify Software Security Centerにアップロードされたオープンソース脆弱性データを表示できます。アプリケーションバージョンのアップロードされた結果は、 監査(AUDIT)]ページまたは オープンソース(OPEN SOURCE)]ページから表示できます。

監査(AUDIT)]ページからのオープンソースデータの表示

監査(AUDIT)]ページからオープンソース脆弱性結果を表示するには:

1. OpenTextのヘッダで、 アプリケーション(Applications)]をクリックします。
2. 目的のアプリケーションの行を展開し、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。
3. 監査(AUDIT)]ページの グループ化条件(Group By)]リストから、 分析タイプ(Analysis Type)]を選択します。
4. DEBRICKED]ヘッダまたは SONATYPE]ヘッダを展開してから、結果を調べる行を展開します。

表示されたDebricked脆弱性データを解釈する方法の詳細については、Debrickedのドキュメントを参照してください(https://debricked.com/docs)。表示されるSonatype脆弱性データを解釈する方法については、Sonatypeのドキュメントを参照してください。

オープンソース結果の監査

オープンソース結果を監査する方法については、"スキャン結果の監査" ページ358を参照してください。

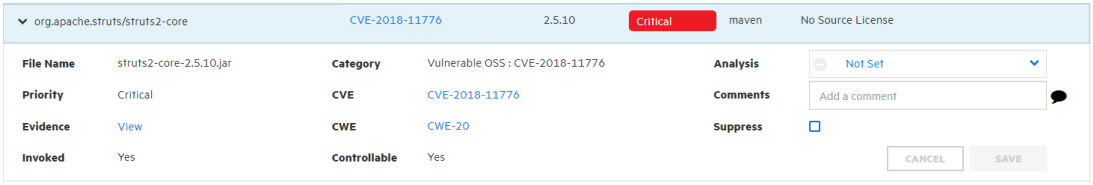
オープンソース(OPEN SOURCE)]ページからのオープンソースデータの表示

オープンソース(OPEN SOURCE)]ページからオープンソース結果を表示するには:

1. OpenTextのヘッダで、 アプリケーション(Applications)]をクリックします。
2. オープンソースの結果がアップロードされているアプリケーションバージョンを選択します。
3. 監査(AUDIT)]ページヘッダで、 オープンソース(OPEN SOURCE)]をクリックします。

注: オープンソース(OPEN SOURCE)]ページは、選択したアプリケーションバージョンに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。
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	脆弱性が呼び出された場合や制御可能な場合の証拠へのリンク。
CWE	Common Weakness Enumeration。このリンク(もしあれば)をクリックすると、Common Weakness EnumerationのWebサイトが開き、発見されたソフトウェアの弱点タイプの詳細が表示されます。
抑止する(Suppress)	問題に懸念がないと思う場合は、このチェックボックスをオンにします。問題の抑止の詳細については、"抑止、削除、および非表示の問題について" ページ367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

フィールド	説明
	どうかが表示されます。
制御可能 (Controllable)	このフィールドには、ユーザが制御する入力がメソッドまたは関数に到達したかどうかが表示されます。

表示されたDebricked脆弱性データを解釈する方法の詳細については、Debrickedのドキュメントを参照してください(https://debricked.com/docs)。

参照情報

"Debricked結果を表示するためのFortify Software Security Centerの準備" ページ180

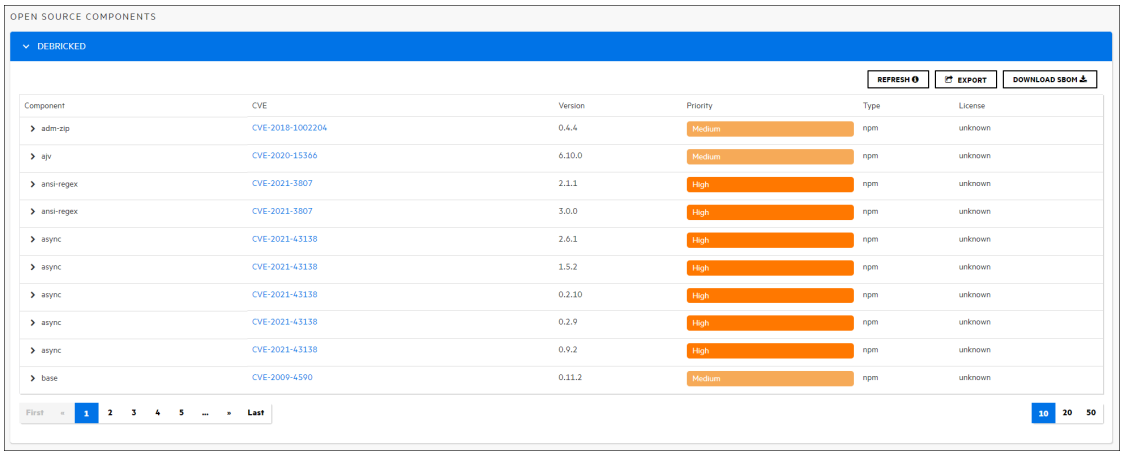
Debricked SBOMのダウンロード

Software Bill of Materials (SBOM)は、ソフトウェアアプリケーションに含まれるソフトウェアの依存関係のリストです。これには、直接的な依存関係に加えて、直接的な依存関係で使用される依存関係(間接的または遷移的な依存関係とも呼ばれる)も含まれます。SBOMでは、ソフトウェアの構築時に使用されるサプライチェーン関係が説明されます。SBOMは、CycloneDX形式です。

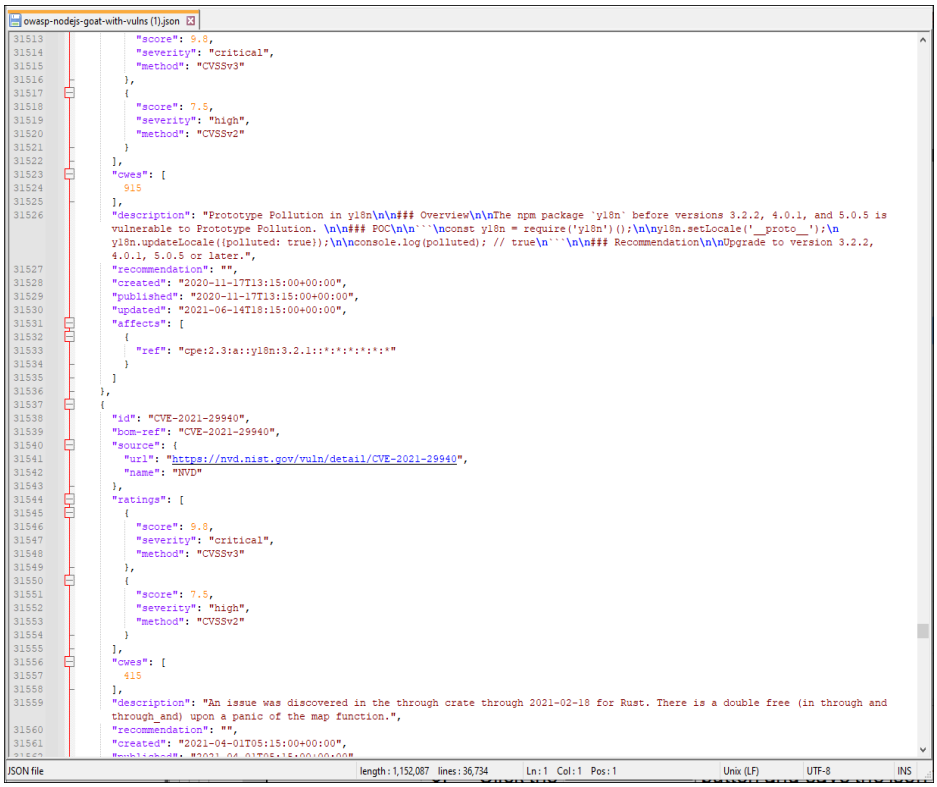
Debricked Bill of Materialsをjsonファイルとしてダウンロードして、使用しているオープンソースコンポーネントを評価できます。SBOMで提供される情報を使用すると、使用しているバージョンがプロジェクトに対して安全か、それとも別のバージョンやオープンソースパッケージ、別のオープンソースパッケージに変更する必要があるかどうかを決定できます。

Debricked SBOMをダウンロードするには:

1. OpenTextのヘッダで、 **[アプリケーション(Applications)]** をクリックします。
2. オープンソースの結果がアップロードされているアプリケーションバージョンを選択します。
   [監査(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。
4. **[Debricked]** グループを展開します。



5. DOWNLOAD SBOM ボタンをクリックして、jsonファイルを保 存します。
6. テキスト エディタでjsonファイルを開き、Software Bill of Materialsを表 示します。



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134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 418
ScanCentral SASTスキャン要求の詳細の表示 419
ScanCentral SASTスキャン要求の優先順位付け 421
ScanCentral SASTスキャン要求のキャンセル 422
ScanCentral SASTセンサ情報の表示 422
ScanCentral Controller情報の表示 424
- コントローラの停止 424
- ScanCentral SAST Controllerを保守モードにする 425
- センサの安全なシャットダウン 426
- ScanCentral SASTコントローラを保守モードから削除する 426

ScanCentral SASTセンサプールについて 427
- 定義済みのセンサプール 427
- ScanCentral SASTセンサプールの作成 428
- ScanCentral SASTセンサのプール間での移動 430
- ScanCentralプールの削除 431

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、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

役割	許可
表示のみ	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。

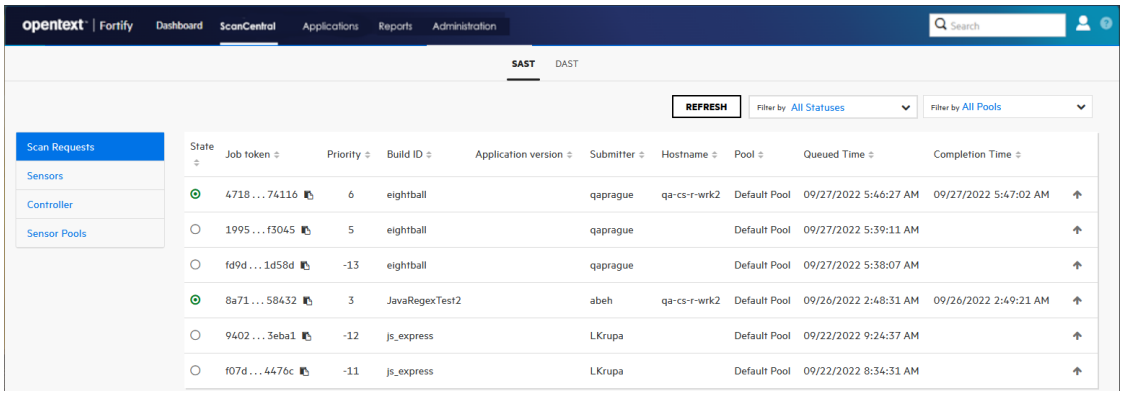
1. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **ユーザ(Users)**]、 **役割(Roles)**]の順に選択します。
   Roles]テーブルに、ユーザに割り当てることができるすべての役割のリストが表示されます。
3. 特定の役割でユーザが実行できるアクションをすべて表示するには、その役割の行をクリックします。

ScanCentral SASTスキャン要求の詳細の表示

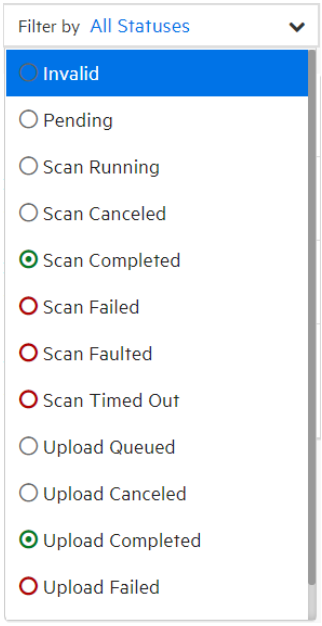
ScanCentral SASTスキャン要求の詳細を表示します。

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、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

1. OpenTextのヘッダで、 **SCANCENTRAL**]をクリックし、 **SAST**]タブを選択します。
   スキャン要求(Scan Requests)]ページに、すべてのスキャン要求とそれぞれの詳細が一覧表示されます。

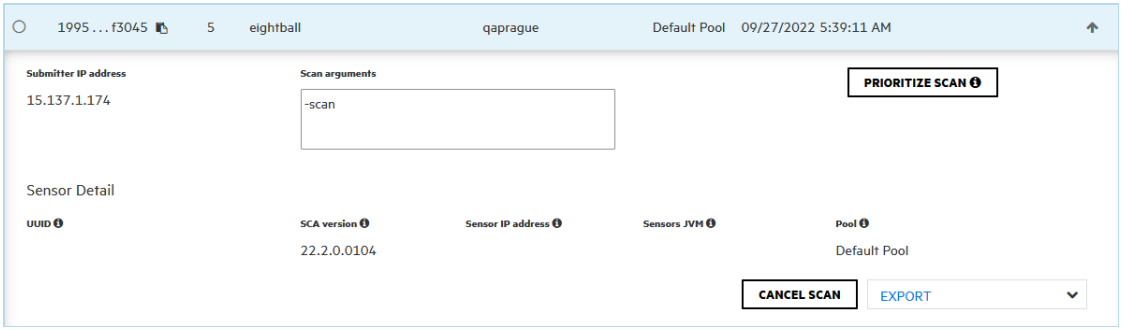


可能性のあるスキャン要求の状態は次のとおりです。



スキャン要求の真の状態を確認するには、カーソルを状態インジケータアイコンに移動します。

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、**フィルタ条件(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スキャン要求の優先順位付け" 下

"ScanCentral SASTスキャン要求のキャンセル" 次のページ

"ScanCentral SASTセンサ情報の表示" 次のページ

"ScanCentral Controller情報の表示" ページ424

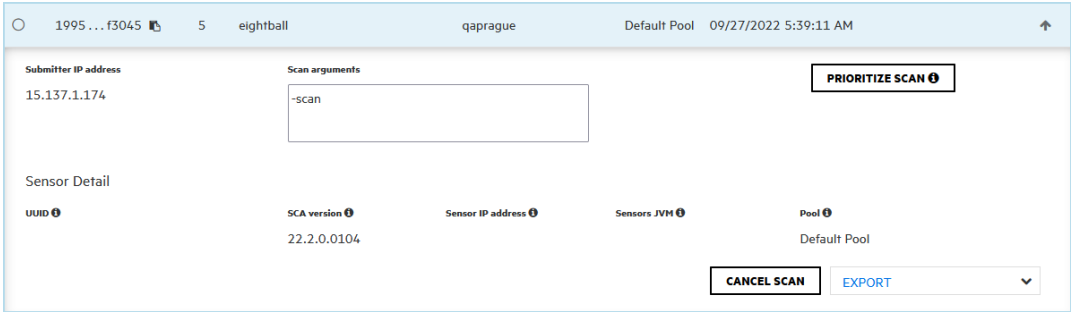
ScanCentral SASTスキャン要求の優先順位付け

特定のスキャンプールに複数のスキャン要求が割り当てられており、そのうちの1つを他のすべての要求より先に実行したい場合は、その要求を優先して、そのプールのジョブキューの先頭に移動します。

スキャン要求に優先順位を付けるには:

1. OpenTextのヘッダで、 [SCANCENTRAL]をクリックします。
   [SAST]ページが開き、 [スキャン要求(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. 左側の [フィルタ条件(Filter by)]リストから、 [保留中(Pending)]を選択します。
   [優先度(Priority)]列内の数字は、スキャンジョブが実行される順序を示します。この数字が小さいほど、プール内でスキャンが早く実行されます。たとえば、優先度が-10のスキャン要求は、同じプール内の優先度が-2のスキャン要求より前に実行されます。
3. 次のいずれかを実行します。

a. 最初に実行したいスキャン要求の行を展開します。



b. [スキャンの優先順位付け(PRIORITIZE SCAN)]をクリックします。
または、最初に実行したいスキャン要求の行の右端にある上向き矢印()をクリックすることもできます。

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、『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。

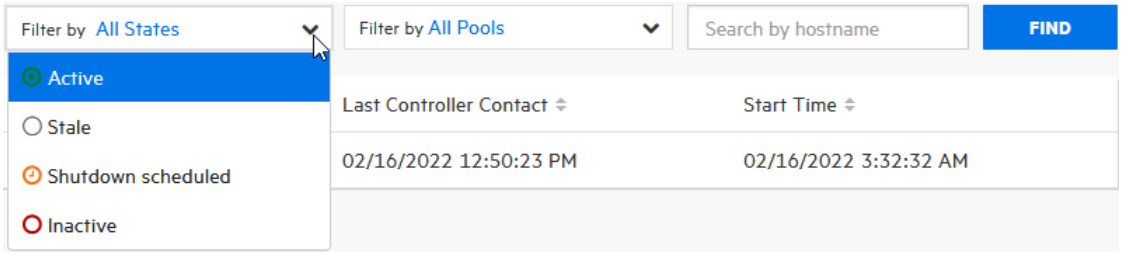
1. OpenTextのヘッダで、 [SCANCENTRAL]をクリックします。
[SAST]ページが開き、 [スキャン要求(Scan Requests)]タブにすべてのスキャン要求が一覧表示されます。
2. 現在の状態に基づいて表示された要求をフィルタ処理するには、 [Filter by]リストから [Pending]を選択します。
3. キャンセルする保留中のスキャン要求の行を展開します。
4. 右下の [CANCEL SCAN]をクリックします。
Fortify Software Security Centerに、要求のキャンセルを確認するメッセージが表示されます。
5. キャンセルを確認します。
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

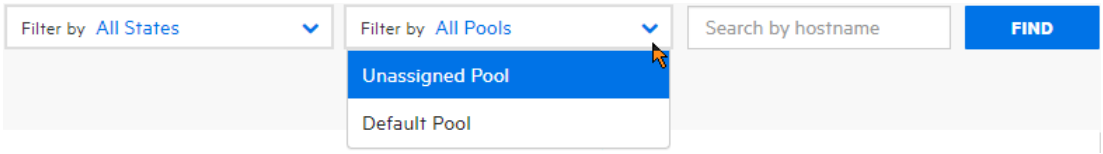
ScanCentral SASTセンサの状態とアクティビティに関する現在の情報を表示します。

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、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

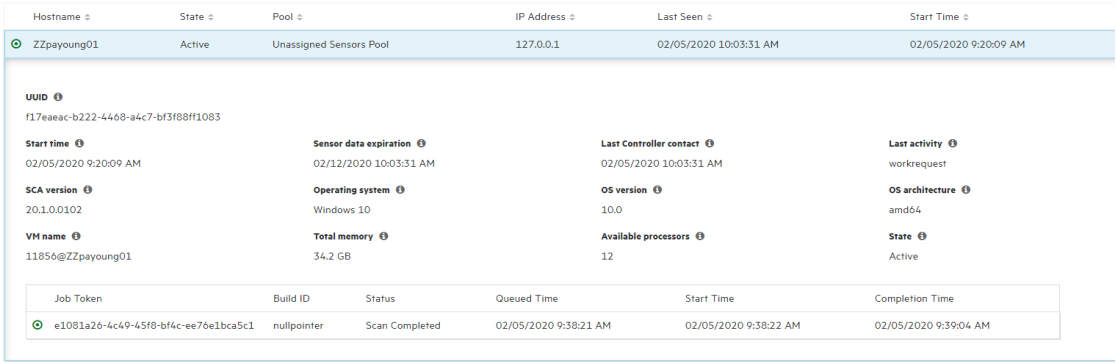
1. OpenTextのヘッダで、 [SCANCENTRAL]をクリックします。
2. [SAST]タブを選択します。
3. 左側のペインで、 [Sensors]を選択します。



4. 現在の状態([アクティブ(Active)]、 [非アクティブ(Inactive)]、 [古い(Stale)]、または [定期シャットダウン(Shutdown scheduled)])に基づいて表示されるセンサをフィルタ処理するには、最初の [フィルタ条件(Filter by)]リストから状態を選択します。([すべての状態(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

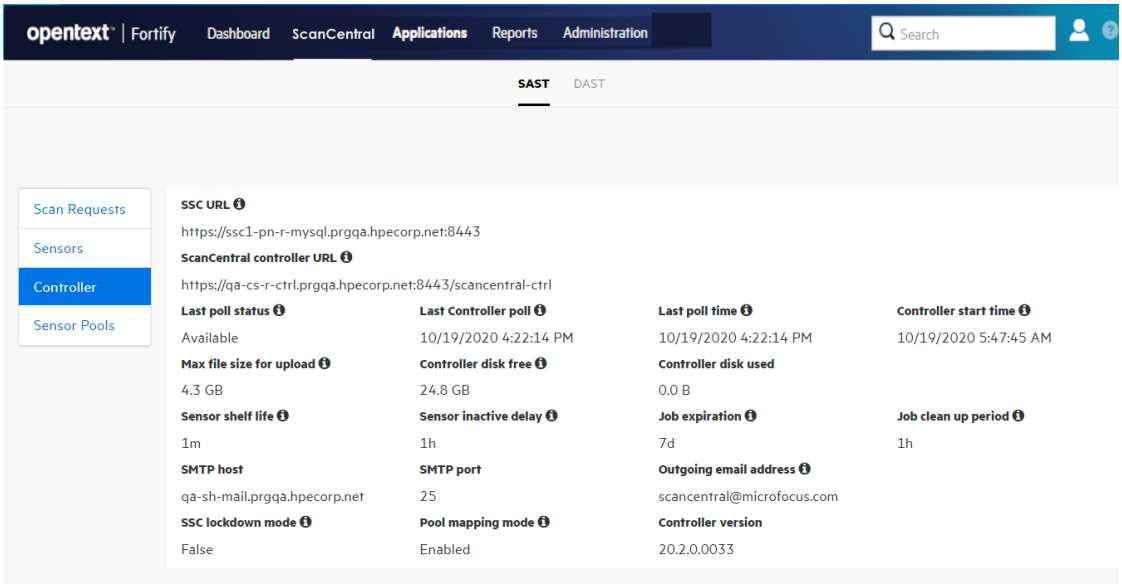
"ScanCentral SASTスキャン要求の詳細の表示" ページ419

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、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

1. OpenTextのヘッダで、 [**SCANCENTRAL**]をクリックします。
2. 左側のペインで、 [**コントローラ(Controller)**]を選択します。



3. 表示される各値については、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419

"ScanCentral SASTスキャン要求のキャンセル" ページ422

"ScanCentral SASTセンサ情報の表示" ページ422

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. 管理者としてFortify Software Security Centerにログオンし、OpenText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、[**コントローラ(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(1ページの「ScanCentral SAST Controllerを保守モードにする」"ScanCentral SAST Controllerを保守モードにする" 前のページを参照)、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. 管理者としてFortify Software Security Centerにログオンし、OpenText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. 管理者としてFortify Software Security Centerにログオンし、OpenText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、 [コントローラ(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" ページ425

"コントローラの停止" ページ424

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" 次のページ

"ScanCentral SASTの許可" ページ418

"ScanCentralプールの削除" ページ431

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、『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. OpenText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. 新しいプールの作成(CREATE NEW POOL)]ダイアログボックスを開くには: [+新しいプール(+ NEW POOL)]をクリックします。

   注:

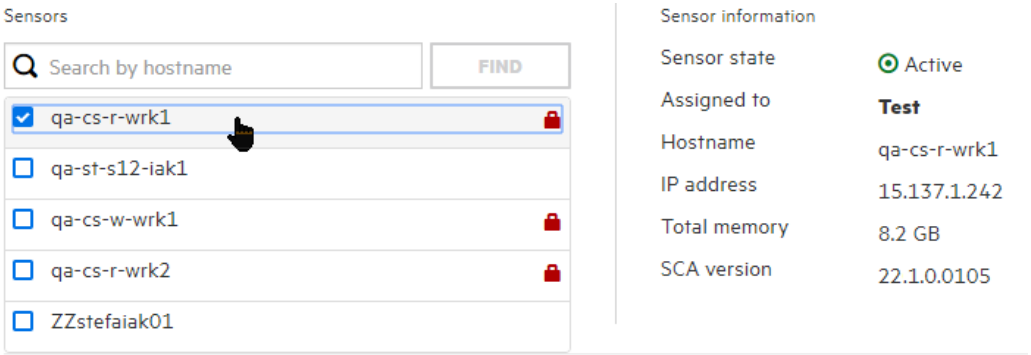
   [+新しいプール(+ NEW POOL)]ボタンが無効になっている場合は、Fortify Software Security Centerがコントローラに接続されていないことを意味します。このボタンが無効になっている場合は、 [SCANCENTRAL SAST CONFIGURATION]設定を確認します("Fortify Software Security CenterにおけるScanCentral SASTモニタリングの設定" ページ134を参照)。

5. [名前(Name)]ボックスに、新しいプールの名前を入力します。プール名の最初の文字はUnicode英数字である必要があります(小文字または大文字のa ~ z、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 [センサ情 報 (Sensor information)] セクションには、センサに関 する基 本 情 報 (センサが現 在 割り当 てられているプールなど)が一 覧 表 示されます。



8. 特 定 のセンサを検 索 するには、表 の上 部 にある検 索 ボックスにそのホスト名 を入 力し、 [検 索 (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。

       [アプリケーションバージョンの選 択 (SELECT APPLICATION VERSION)] ダイアログボックスの [アプリケーション (APPLICATION)] ペイン (左 側) で、このプールに割り当 てるアプリケーションを選 択します。

    b. [バージョン (VERSIONS)] ペイン (中 央) には、選 択したアプリケーションのすべてのアクティブなバージョンが一 覧 表 示されます。

    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" 次のページ

"ScanCentral SASTセンサ情報の表示" ページ422

ScanCentral SASTセンサのプール間での移動

ScanCentral SASTセンサをプール間で移動させるには:

1. OpenTextのヘッダで、[SCANCENTRAL]を選択します。
2. Fortify Software Security CenterがScanCentral SASTおよびScanCentral DASTの両方と統合されている場合は、[SAST]タブを選択してScanCentral SASTの[スキャン要求(Scan Requests)]ページを開きます。
3. 左側のペインで、[Sensor Pools]を選択します。
4. [センサプール(SENSOR POOLS)]ページで、別のプールに割り当てるセンサを含むセンサプールを選択します。
5. [プールの編集(EDIT POOL)]をクリックします。
6. [プールの編集: <pool name> (EDIT POOL: *<pool name>*)]ダイアログボックスの[センサ(Sensors)]で、別のプールに割り当てるセンサのチェックボックスをオフにします。
7. [保存(SAVE)]をクリックします。
8. [センサプール(SENSOR POOLS)]ページで、現在割り当てられていないセンサを割り当てるセンサプールを選択し、"ScanCentral SASTセンサプールの作成" ページ428に記載されている手順に従って、現在割り当てられていないセンサを割り当てます。

参照情報

"ScanCentral SASTセンサプールについて" ページ427

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. OpenTextのヘッダで、 [**SCANCENTRAL**]を選択します。
2. ScanCentralの [スキャン要求(Scan Requests)]ページの左ペインで、 [**センサプール(Sensor Pools)**]を選択します。
   [センサプール(Sensor Pools)]ページが開き、 [**センサプール(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422

"ScanCentral SASTセンサプールの作成" ページ428

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135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 432
ScanCentral DASTへの動的スキャン要求の送信 434
KafkaをFortify ScanCentral DASTの監査履歴変更の同期 434

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. OpenTextのヘッダで、 **管理(Administration)**]を選択します。
2. 左ペインで、 **ユーザ(Users)**]、 **役割(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、『*OpenText™ 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135

"ScanCentral DASTの許可" ページ432

KafkaをFortify ScanCentral DASTの監査履歴変更の同期

Fortify Software Security Centerにおいて、[監査(AUDIT)]ページで管理され、ScanCentral DASTに発行される問題のことを、結果と呼びます。

Fortify Software Security CenterでKafkaを設定すると、抑止された問題、優先度の上書き、分析タグの設定に関する監査履歴の変更を、Fortify ScanCentral DASTに同期できます。Fortify Software Security CenterでKafkaを設定する方法については、「"Kafkaの設定" ページ106」を参照してください。

Fortify Software Security Centerで問題を監査するとき、バックグラウンドプロセスは、監査をKafkaトピックに発行するよう要求します。Fortify ScanCentral DASTは監査を処理し、抑止された問題、優先度の上書き、分析タグの設定を[スキャン(Scans)]ビューとスキャンの視覚化に反映します。

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。

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440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. [管理(Administration)]ビューの左ペインから、[テンプレート(Templates)]を選択して、[レポートライブラリ(Report Libraries)]を選択します。
   [レポートライブラリ(Report Libraries)]ページには、システム内のすべてのレポートライブラリが一覧表示されます。
2. [新しいライブラリテンプレートのインポート(IMPORT NEW LIBRARY TEMPLATE)]ダイアログボックスを開くには、[インポート(IMPORT)]をクリックします。
3. (オプション) [説明(Description)]ボックスに、インポートするライブラリの説明を入力します。
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

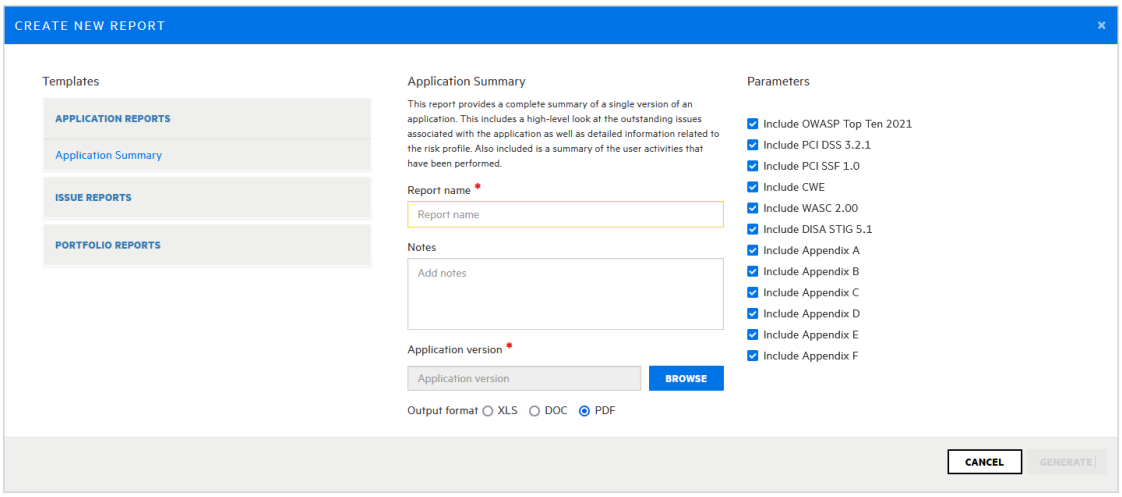
"Fortify Software Security Centerへの破壊的ライブラリおよびテンプレートのアップロードの防止" ページ184

"レポートを生成して表示する" 下

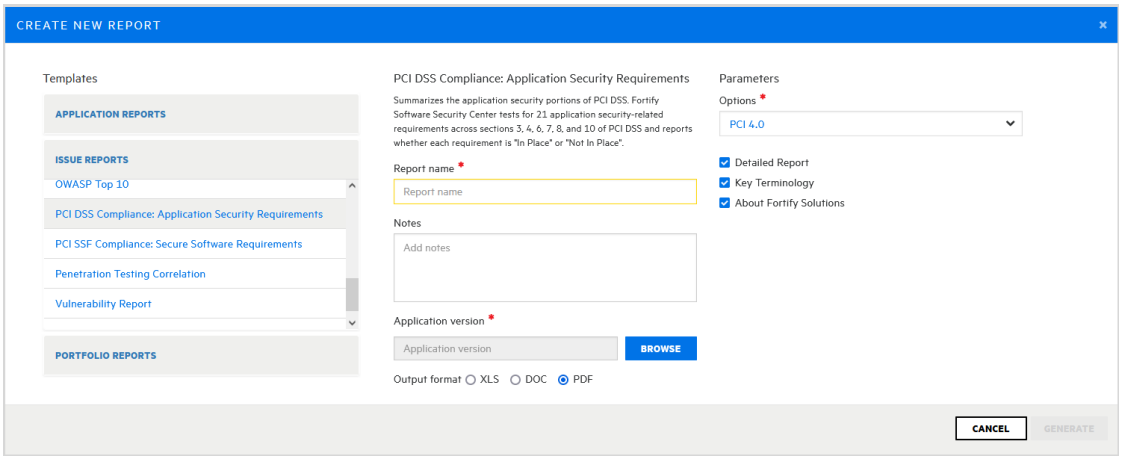
レポートを生成して表示する

Fortify Software Security Center レポートを生成して表示するには:

1. OpenTextのヘッダで、[レポート(Reports)]をクリックします。
2. [新しいレポートの作成(CREATE NEW REPORT)]ダイアログボックスを開くには、[レポート(Reports)]ページのツールバーで[+新しいレポート(+ NEW REPORT)]をクリックします。

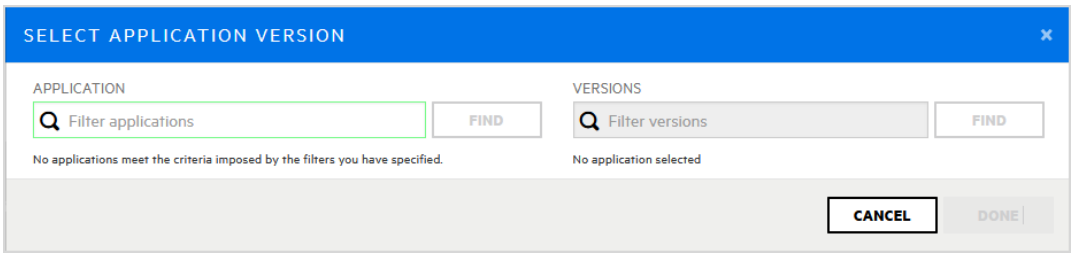


3. 使用するレポートテンプレートに移動して選択します。



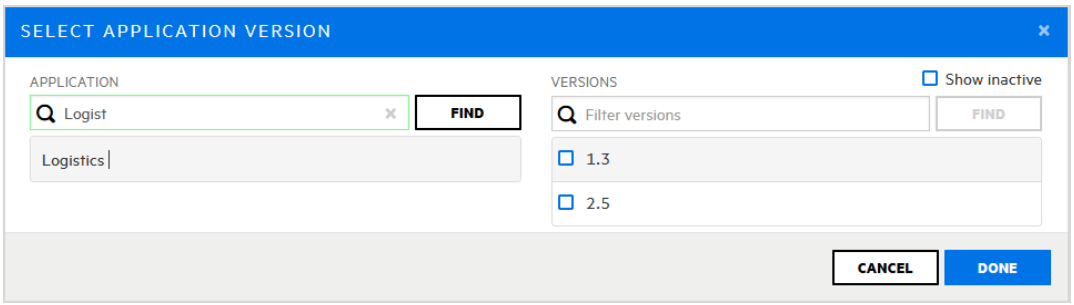
右側のペインには、選択したテンプレートの設定フィールドが表示されます。

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. レポートに含めるアプリケーションバージョンを指定するには:
   a. **[アプリケーションバージョン(Application version)]**で、**参照(BROWSE)**をクリックします。



   b. **[アプリケーションバージョンの選択(SELECT APPLICATION VERSION)]**ダイアログボックスの**[アプリケーション(APPLICATION)]**で、一覧に表示されているアプリケーションの1つを選択するか、**[アプリケーションのフィルタ(Filter applications)]**ボックスにアプリケーション名の一部または全体を入力してから名

前を選択します。

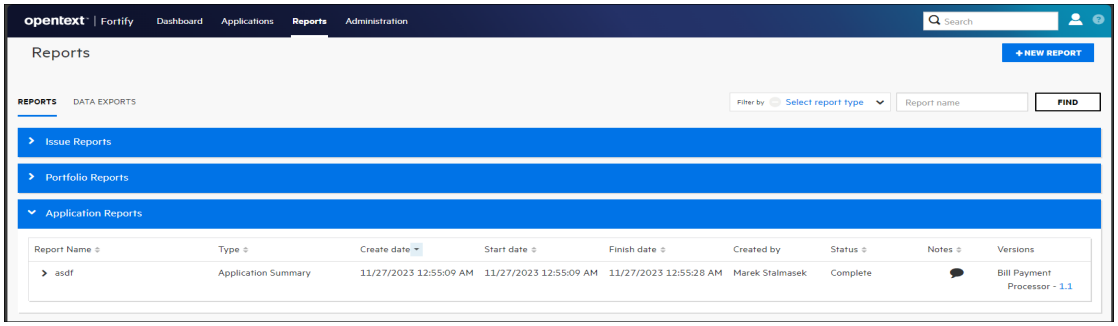


選択したアプリケーションのアクティブなバージョンが [**バージョン(VERSIONS)**] の下に表示されます。

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。)

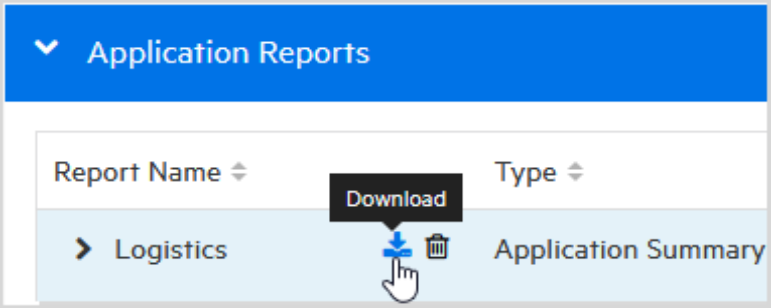
d. [**DONE**] をクリックします。

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. レポートをダウンロードして表示するには、カーソルをレポート名に移動し、 **[ダウンロード]** アイコン をクリックします。

レポートをシステムから自動的に削除する前にFortify Software Security Centerがレポートを保持する日数を指定する方法については、"ジョブスケジューラの設定" ページ 135を参照してください。

参照情報

"レポートテンプレートをダウンロードする" 次のページ

"レポート定義のインポート" ページ443

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バージョンについては、『Fortifyソフトウェアシステム要件』ドキュメントを参照してください。

   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" 次のページ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443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、『Fortifyソフトウェアシステム要件』ドキュメントを参照してください。

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。
   https://download.eclipse.org/birt/downloads/drops
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

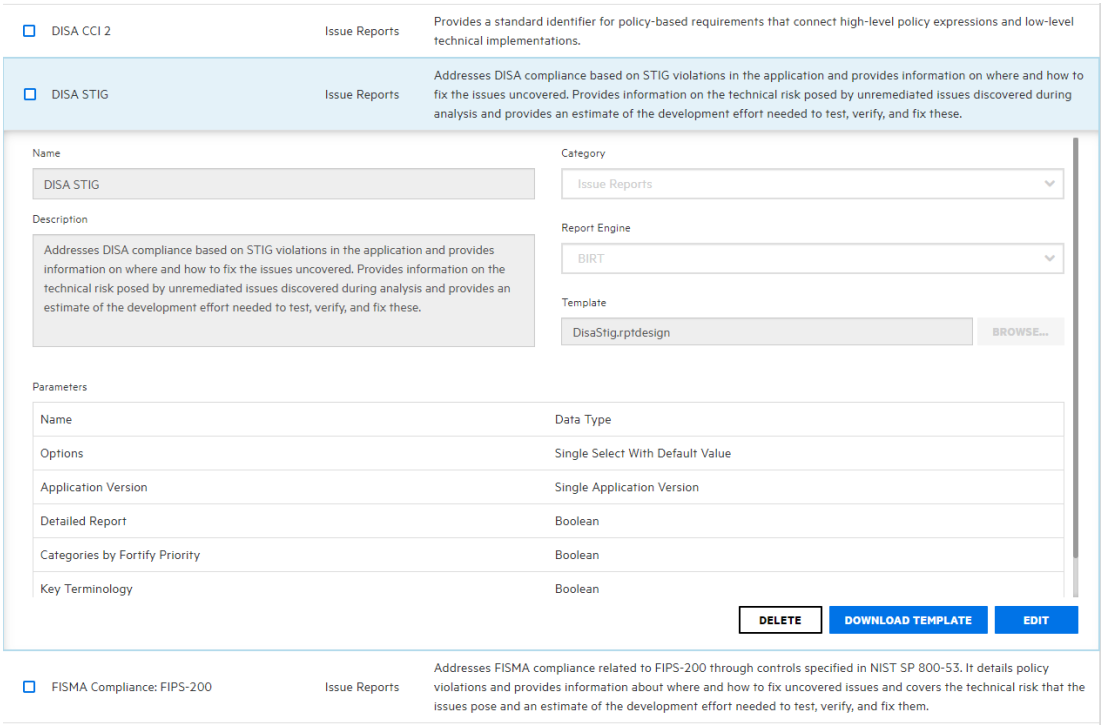
Fortify Software Security Center レポートテンプレートを変更のためにダウンロードできます。

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。

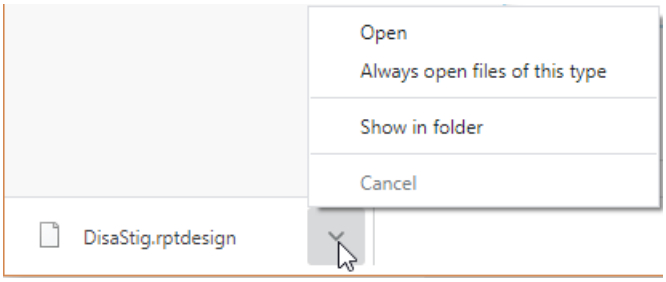
注: 「Options」という名前のパラメータをBIRTレポートで変更することはできません。

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. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
2. 左側のペインで、 **テンプレート(Templates)**]を展開して、 **レポート(Reports)**]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" ページ443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436

カスタマイズされたBIRTレポートのXLSX形式による生成とダウンロード

カスタマイズされたBIRTレポートをXLSX形式でダウンロードするには:

1. OpenTextのヘッダで、 **管理(Administration)**]をクリックします。
2. 左ペインで、 **テンプレート(Templates)**]を展開し、 **レポートテンプレート(Report Templates)**]を選択します。
   レポート(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. カスタマイズされた、目的のレポートテンプレートの行をクリックします。
4. **編集(EDIT)**]をクリックします。
5. **パラメータの追加(ADD PARAMETER)**]をクリックします。
6. 新規パラメータの追加(ADD NEW PARAMETER)]ダイアログボックスで、次の表で説明する情報を入力します。

フィールド	説明
名前(Name)	カスタマイズされたレポートテンプレートのパラメータに対応するパラメータの名前を入力します。
説明(Description)	(オプション)パラメータの説明を入力します。
識別子(Identifier)	`enableXlsxGeneration`と入力すると、カスタマイズされたレポートテンプレートにXLSX出力形式が追加されます。
データ型(Data Type)	**ブール値(Boolean)**]を選択します。

7. **適用(APPLY)**]をクリックします。
8. **保存(SAVE)**]をクリックして変更を適用します。
9. OpenTextのヘッダで、 **レポート(Reports)**]をクリックします。
10. **+新規レポート(+ NEW REPORT)**]をクリックします。
11. テンプレート(Templates)]ペインで、すでに設定した、カスタマイズされたレポートテンプレートを選択します。
12. **レポート名(Report name)**]ボックスに、カスタマイズされたBIRTレポートの名前を入力します。
13. カスタマイズされたBIRTレポートをXLSX形式で生成するには、 **出力形式(Output format)**]の横にある **XLSX**]を選択します。
14. **生成(GENERATE)**]をクリックします。

Fortify Software Security Centerで、カスタマイズされたBIRTレポートが **[レポート (Reports)]** テーブルに追加されます。レポートの生成が完了すると、 **[ステータス (Status)]** フィールドに「**完了 (Complete)**」と表示されます。

15. レポートをダウンロードして表示するには、 **[ダウンロード (DOWNLOAD)]** をクリックします。

    カスタマイズされたBIRTレポートが、XLSX形式でダウンロードされます。

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、レポート定義ファイルをFortify Software Security Centerにインポートできます。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. OpenTextのヘッダで、 **[管理 (Administration)]** をクリックします。
2. 左ペインで、 **[テンプレート (Templates)]** を選択し、 **[レポートテンプレート (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。
4. **[新しいレポートテンプレートのインポート (IMPORT NEW REPORT TEMPLATE)]** ダイアログボックスで、次の表に示す情報を入力します。

フィールド	説明
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。

フィールド	説明
Template	ファイル名の拡張子 `rptdesign` 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436

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。Fortify Software Security Centerサーバで使用できるトークンタイプは複数あります。それぞれが異なる機能を提供し、通常は、時間制限がある少数のアクションからなるセット用です。たとえば、`AnalysisUploadToken`トークンでは、ユーザがインターフェイ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

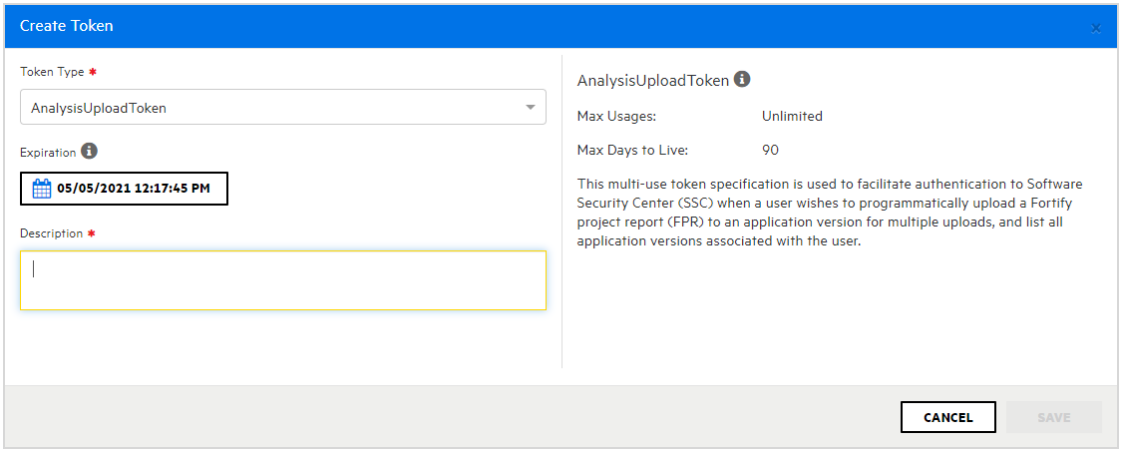
認証トークンは、Fortify Software Security Centerの [管理(Administration)]ビューかコマンドラインインタフェースから生成できます。自分のトークンの詳細を見ることができるのは、自分だけです。Fortify Software Security Center管理者は、作成するトークンの有効期限を延長できますが、そのトークンの最大有効日数を超えることはできません。

注: あらゆるタイプのトークンを作成できますが、トークンで実行するよう定められたアクションを実行するために必要な許可がない場合、そのトークンを使用できません。

[管理(Administration)]ビューからのトークンの生成

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、 **[管理(Administration)]**を選択します。
2. 左ペインで、 **[ユーザ(Users)]**セクションを展開し、 **[トークン管理(Token Management)]**を選択します。
3. **[トークン管理(Token Management)]**ツールバーで、 **[新規(New)]**をクリックして、[トークンの作成(Create Token)]ダイアログボックスを開きます。
4. **[トークンタイプ(Token Type)]**リストから、作成するトークンのタイプを選択します。
   使用可能なトークンタイプのリストを表示するには、"コマンドラインからトークンを生成する" ページ447の表を参照してください。

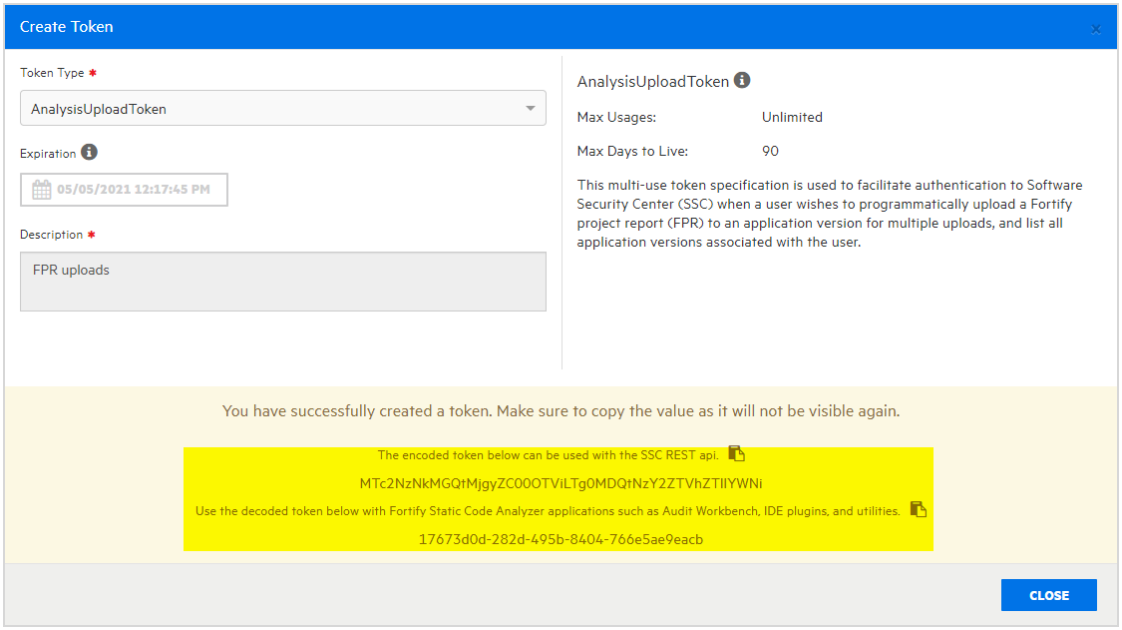


[Create Token] ダイアログボックスには、選択したトークンタイプの説明が右側のペインに表示されます。

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。)

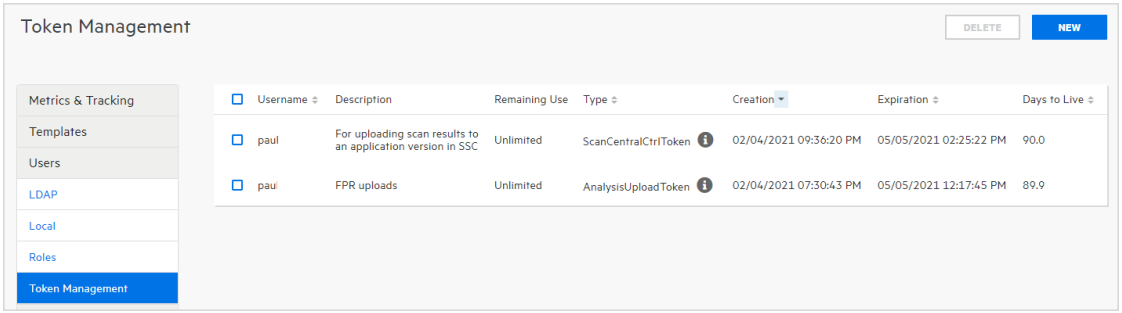
注: デフォルトでは、有効期限の値は、選択したトークンタイプに対して有効な最大日数に設定されます。これをそれより前の日付に設定すると、トークンの有効期限は短くなります。.

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
AutomationToken	発行元ユーザに許可されているほとんどのREST APIエンドポイントにアクセスする機能を提供します。長期的な自動化での使用に適しています。 最大使用量: 無制限 最大有効期限: 365日 **注意** このトークンが提供するアクセスと許容される最大有効期限を考えると、APIの誤用や意図しない使用のリスクを減らすため、特別な注意を払ってトークンのセキュリティを確保する必要があります。このトークンの計画的な使用を評価し、環境のリスクに対する許容度に基づいてその有効期限を制限することを推奨します。
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

オプション	説明
PurgeProjectVersionToken	すべてのアプリケーションバージョンのリストをプログラムで要求し、アプリケーションバージョンを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 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453.

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、 **管理(Administration)**]を選択します。
2. 左ペインで、 **ユーザ(Users)**]セクションを展開し、 **トークン管理(Token Management)**]を選択します。
   トークン管理(Token Management)]ページには、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445

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、 **管理(Administration)**]を選択します。
2. 左ペインで、 **ユーザ(Users)**]セクションを展開し、 **トークン管理(Token Management)**]を選択します。
   トークン管理(Token Management)]ページには、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445

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 450
fortifyclientクライアントオプションとパラメータの一覧 452
アップロード認証トークンについて 452
fortifyclient認証トークンの一覧 454
トークンの無効化 454
アプリケーションバージョンの一覧表示 455
アプリケーションバージョンのパージ 456
FPRのアップロードについて 456
FPRのダウンロードについて 458
コンテンツバンドルのインポート 460
監査添付ファイルをダウンロードする 461

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 451
fortifyclient認証トークン 451

fortifyclient HTTPタイムアウト 451

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 では、<ssc_url>は、このトピックで説 明 するように、正 しい形 式 のFortify Software Security Center URLを表 しています。

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 HTTPタイムアウト

fortifyclientに対 して、接 続 、読 み取り、および書 き込みのHTTPタイムアウトを設 定できます。どのタイムアウトについても、最 大 範 囲 は1から2147483秒 です。

次 の表 に、HTTPタイムアウトを変 更 するために使 用 できる環 境 変 数 を示 します。

環境変数	説明
FORTIFYCLIENT_CONNECT_TIMEOUT_SEC	クライアントが接 続 を確 立 するためのHTTP接 続 タイムアウトを秒 単 位 で指 定 します。 デフォルト値 は10秒 です。

環境変数	説明
FORTIFYCLIENT_READ_TIMEOUT_SEC	クライアントが応答を受信するためのHTTP読み込みタイムアウトを秒単位で指定します。 デフォルト値は600秒です。
FORTIFYCLIENT_WRITE_TIMEOUT_SEC	クライアントが要求本文を配信するためのHTTP書き込みタイムアウトを秒単位で指定します。 デフォルト値は60秒です。

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 452
fortifyclient認証トークンでのDaysToLiveの指定 453

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 [管理(Administration)]ビューから取得するか、fortifyclientを使用して取得できます。次の手順では、fortifyclient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。 [管理(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445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" ページ451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。
2. プロンプトが表示されたら、<account_name>のパスワードを入力します。
   fortifyclientがトークンを返します。
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 <account_name> -password <password> -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451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:

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> -
   password <password>
   ```

   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451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。

このユーティリティは、すべての`fortifyclient`認証トークンのID、所有者、作成日、有効期限を含むリストを返します。

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、 **管理(Administration)**]を選択します。
2. 左ペインで、 **[ユーザ(Users)**]セクションを展開し、 **[トークン管理(Token Management)**]を選択します。
3. **[トークン管理(Token Management)**]ページで、削除するトークンが表示されてい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451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445

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452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451を参照)、*<token>*は、有効なfortifyclient認証トークンです。

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> -authtoken <token>
```

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451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458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452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 457
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 457

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451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455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451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456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 459
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 459

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> -authtoken <token> 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451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
<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455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> -authtoken <token> 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451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
<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> -authtoken <token> 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451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
<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> -authtoken <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451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
<token>	有効なfortifyclient認証トークンを表します

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、『Fortifyソフトウェアシステム要件』ドキュメントを参照してください)。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 462
コンポーネントのセットアップ 463
実装 463
プラグインメソッドとメソッドコール 465
Plugin Helper 470
エラー処理 471
ほぼステートレス 471
バグトラッカプラグインのデバッグ 471
カスタマイズしたバグトラッカープラグインの展開 472

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172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470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462

付録C: Fortify Software Security Centerの設定の自動化

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。autoconfig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。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、プロパティファイルだけではなく`secret.key`ファイルも移動する必要があります。

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(`fortify.home`に作成されるディレクトリの名前)。ファイル名はアプリケーションコンテキスト名と一致していなければなりません(Fortify Software Security Centerの場合は*<app_context>*`.autoconfig`)。ただし、ROOTコンテキストの場合は例外です(`_default_.autoconfig`)。
2. 次の項目を*<app_context>*`.autoconfig`ファイルに、YAML形式で追加します。

   注: 使用するデータベースエンジンのプロパティのみをコピーし、各プロパティの前にあるハッシュ記号(#)を削除してください。

```
 appProperties:
   # <fortify.home>/<app_context >/conf/app.propertiesのプロパティをすべて含めます。# 例: 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:
   # パスを環境に合った適切な場所に変更します -
   '/home/ssc/bundles/Fortify_Process_Seed_Bundle-2024_Q2_<build>.zip'
   - '/home/ssc/bundles/Fortify_PCI_Basic_Seed_Bundle-2024_Q2_
   <build>.zip' - '/home/ssc/bundles/Fortify_PCI_SSF_Basic_Seed_Bundle-
   2024_Q2_<build>.zip' - '/home/ssc/bundles/Fortify_Report_Seed_
   Bundle-2024_Q2_<build>.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. fortify.licenseファイルのコピーを<*fortify.home*>フォルダに配置します。
5. Tomcatサーバを起動します。
6. <*app_context*>.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、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 24.2.0)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@opentext.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。