

---

# Micro Focus Fortify on Demand

Software Version: 22.4

## User Guide

Document Release Date: December 2022

Software Release Date: December 2022



## Legal Notices

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

<https://www.microfocus.com>

## Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice

© Copyright 2010- 2022 Micro Focus or one of its affiliates

## Trademark Notices

All trademarks, service marks, product names, and logos included in this document are the property of their respective owners.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on December 01, 2022. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

# Contents

Preface .....	13
Contacting Micro Focus Fortify on Demand Customer Support .....	13
For More Information .....	13
About the Documentation Set .....	13
Fortify Product Feature Videos .....	13
What's New .....	14
v22.4 .....	14
Engine and Rulepack Updates .....	14
New Features .....	14
Improvements .....	15
Chapter 1: Introduction .....	17
Fortify on Demand Overview .....	17
Security Rating System .....	18
Likelihood and Impact .....	18
Priority Order .....	19
Five-Star Assessment Rating .....	20
Service Level Objectives .....	20
Chapter 2: Getting Started .....	22
Before You Start .....	22
Logging In and Out of the Portal .....	22
Resetting Your Password .....	24
Navigating the Portal .....	24
Searching the Portal .....	26
Managing Your Account Settings .....	26
Editing Your Account Settings .....	27
Changing Your Account Password .....	28
Opting In To and Out Of Beta Features .....	29

Managing Notifications .....	30
Viewing Notifications .....	30
Creating an Individual Subscription .....	31
Creating a Global Subscription .....	34
Editing a Subscription .....	36
Deleting a Subscription .....	38
 Chapter 3: Managing Applications and Releases .....	 40
Structuring Applications and Releases .....	40
Managing an Application .....	43
Creating an Application .....	43
Viewing Application Details .....	50
Navigating the Application Overview Page .....	51
Filtering the Application Overview page .....	52
Editing Application Settings .....	53
Managing User Assignment to an Application .....	55
Viewing the Application Event Log .....	57
Deleting an Application .....	59
Managing a Release .....	59
Creating a Release .....	60
Viewing Release Details .....	61
Navigating the Release Overview Page .....	62
Release Overview Graphs .....	63
Overriding the Security Policy of a Release .....	68
Editing Release Settings .....	69
Deleting a Release .....	70
Viewing Applications in the Tenant .....	70
Navigating Your Applications Page .....	71
Filtering Your Applications Page .....	74
Viewing Releases in the Tenant .....	76
Navigating Your Releases Page .....	77
Filtering Your Releases Page .....	79
Searching Applications and Releases .....	80
Creating Deep Links .....	81
 Chapter 4: Running Assessments .....	 82



Static Assessments .....	82
Supported Languages .....	83
Supported Compilers .....	85
Supported Libraries, Frameworks, and Technologies .....	86
Preparing Static Assessment Files .....	89
File Requirements for Static Assessments .....	90
Fortify ScanCentral SAST .....	91
Preparing .NET Application Files .....	91
Preparing Java Application Files .....	93
Preparing JavaScript Technology/HTML/XML Files .....	95
Preparing Kotlin Application Files .....	95
Preparing ABAP (SAP) Application Files .....	95
Preparing C and C++ Application Files .....	98
Preparing Classic ASP, VBScript, and Visual Basic Application Files .....	99
Preparing COBOL Application Files .....	99
Preparing ColdFusion Markup Language (CFML) Application Files .....	100
Preparing Dockerfiles and Infrastructure as Code (IaC) Files .....	100
Preparing Go Application Files .....	100
Preparing PHP Application Files .....	101
Preparing Python Application Files .....	102
Preparing Ruby Application Files .....	103
Preparing Salesforce (Apex and Visualforce) Application Files .....	103
Preparing Scala Application Files .....	104
Preparing Android Application Files (Source Code) .....	105
Preparing iOS Application Files (Source Code) .....	105
Configuring a Static Scan .....	105
Submitting a Static Assessment .....	109
Uploading a Static Assessment Payload Through the Portal .....	109
Static Assessment Payload Validation .....	112
Dynamic Assessments .....	114
Preparing the Website for Dynamic Testing .....	114
Preparing Web API Files .....	115
Configuring a Dynamic Scan .....	118
Submitting a Dynamic Assessment .....	129
Scheduling the Dynamic Scan Through the Portal .....	130
Editing Dynamic Scan Settings .....	132
Continuous Application Monitoring .....	133
Configuring Application Monitoring .....	133
Canceling an Application Monitoring Scan .....	135

Viewing Application Monitoring Issues .....	135
Viewing Risk Profile Results .....	136
Mobile Assessments .....	137
Supported Platforms and Operating Systems .....	137
Mobile Assessment Preparation .....	138
Preparing Mobile Assessment Files .....	138
Preparing Android Application Files (Binary) .....	139
Preparing iOS Application Files (Binary) .....	139
Preparing the Backend for Mobile Testing .....	140
Configuring a Mobile Scan .....	141
Submitting a Mobile Assessment .....	145
Scheduling the Mobile Scan Through the Portal .....	145
Editing Mobile Scan Settings for an Ongoing Scan .....	148
Open Source Software Composition Analysis .....	148
Preparing Files for Open Source Scanning .....	149
Viewing Open Source Issues .....	151
Viewing Open Source Components in a Release .....	152
Viewing Open Source Components in a Tenant .....	152
Generating an Open Source Component Report .....	153
Entitlement Consumption .....	154
Managing Scans .....	154
Viewing Scans in the Tenant .....	154
Filtering Your Scans Page .....	156
Viewing Application Scans .....	157
Viewing Release Scans .....	159
Checking the Scan Status .....	160
Canceling a Scan .....	161
Resuming a Paused Scan .....	162
Viewing Help Center Tickets Linked to a Scan .....	163
Chapter 5: Remediating Vulnerabilities .....	165
Reviewing Issues .....	165
Viewing Application Issues .....	166
Navigating the Application Issues Page .....	167
Viewing Release Issues .....	169
Navigating the Release Issues Page .....	170
Filtering the Issues Page .....	173

Customizing Issue Filters and Groupings .....	175
Issue Details .....	177
Static Scan Issue Details .....	177
Open Source Scan Issue Details .....	181
Dynamic/Application Monitoring Scan Issue Details .....	183
Mobile Scan Issue Details .....	187
Remediating Issues .....	189
Editing an Issue .....	189
Editing Multiple Issues .....	191
Uploading Screenshots .....	193
Auditing Issue Remediation .....	195
Audit Workflow for Auditors .....	195
Audit Workflow for Developers .....	196
Audit Templates .....	197
Creating a Global Audit Template .....	197
Creating an Application Audit Template .....	200
Creating an Application Audit Template Filter for an Issue .....	203
Audit Template Usage and Examples .....	205
Dataflow Cleanse Rules .....	206
Creating a Global Dataflow Cleanse Rule .....	206
Creating an Application Dataflow Cleanse Rule .....	208
Dataflow Cleanse Rule Usage and Examples .....	210
Requesting a Remediation Scan .....	211
Chapter 6: Dashboards and Reports .....	213
Dashboards .....	213
Viewing Dashboards .....	213
Dashboard Graph Types .....	215
Gauge .....	215
List Grid .....	216
Summary .....	217
Trending Chart .....	217
Creating a Dashboard .....	218
Editing a Dashboard .....	220
Deleting a Dashboard .....	222
Reports .....	224
Viewing Reports .....	225

Accessing Reports for a Release .....	225
Accessing Reports for an Application .....	226
Accessing Your Reports Grid .....	227
Navigating Your Reports Page .....	227
Generating a Report .....	227
Completing the Report Generation Wizard .....	228
Scheduling Auto-Generated Reports .....	230
Templates .....	232
Creating a Custom Report Template .....	233
Editing a Custom Report Template .....	235
Deleting a Custom Report Template .....	236
Suppressing a System Report Template .....	236
Data Exports .....	236
Viewing Data Exports .....	237
Creating a Data Export Template .....	238
Generating a Data Export .....	242
Chapter 7: Administration .....	244
Portal Management .....	244
Configuring User Security .....	244
API Keys .....	247
Creating an API Key .....	247
API Key Roles .....	248
Editing or Deleting an API Key .....	249
Viewing Entitlements .....	251
Viewing the Administration Event Log .....	252
Managing Attributes .....	253
Adding an Attribute .....	254
Editing an Attribute .....	256
Deleting an Attribute .....	257
User Management .....	258
Roles and Permissions .....	258
Permissions .....	259
Tenant Level Permissions .....	259
Application Level Permissions .....	261
Default Roles .....	263
Viewing Roles .....	265
Creating a Role .....	266

Editing a Role .....	267
Deleting a Role .....	268
Users .....	269
Viewing Users .....	269
Creating a User .....	270
Editing a User Account .....	272
Managing Application Assignment to a User .....	273
Deleting a User Account .....	275
Groups .....	276
Viewing Groups .....	276
Creating a Group .....	277
Editing a Group .....	278
Managing Application Assignment for a Group .....	280
Deleting a Group .....	282
Policy Management .....	283
Creating a Security Policy .....	283
Setting the Security Policy .....	289
Deleting a Security Policy .....	290
Single Sign-On (SSO) .....	291
Configuring SSO in Fortify on Demand .....	292
Adding the Identity Provider Metadata .....	295
Downloading the Fortify on Demand Metadata .....	297
Configuring SSO in the Identity Provider .....	297
Troubleshooting Failed Logins .....	300
Vendor Management .....	301
Initiating a Relationship with Another Tenant .....	302
Accepting a Relationship Initiated by Another Tenant .....	303
Confirm a Relationship .....	303
Establish your Tenant as a Customer .....	304
Publishing a Vendor Management Report .....	304
Viewing Published Report .....	305
Chapter 8: Fortify on Demand API .....	306
API Authentication .....	306
API Scopes .....	308
Personal Access Tokens .....	309
Creating a Personal Access Token .....	309

Editing or Deleting a Personal Access Token .....	311
Viewing API Documentation through API Explorer .....	311
Testing API Endpoints through API Explorer .....	313
API Rate Limits .....	316
Chapter 9: Development Tools .....	319
Viewing Tools .....	322
Visual Studio Extension .....	323
Installing the Visual Studio Extension .....	323
Configuring the Visual Studio Extension .....	324
Uploading Code with the Visual Studio Extension .....	325
Opening Analysis Results with the Visual Studio Extension .....	331
Analysis Results in the Visual Studio Extension .....	333
Analysis Trace Icons .....	335
Reviewing Issues from the Visual Studio Extension .....	336
Auditing Issues from the Visual Studio Extension .....	337
Locating the Source Code Associated with Static Scan Issues .....	338
Logging Out .....	339
Uninstalling the Visual Studio Extension .....	339
Eclipse Plugin .....	339
Installing the Eclipse Plugin .....	340
Setting up Automatic Updates for the Eclipse Plugin .....	342
Configuring the Eclipse Plugin .....	343
Uploading Code with the Eclipse Plugin .....	343
Opening Analysis Results with the Eclipse Plugin .....	351
Analysis Results in the Eclipse Plugin .....	354
Analysis Trace Icons .....	355
Reviewing Issues from the Eclipse Plugin .....	356
Auditing Issues from the Eclipse Plugin .....	357
Locating the Source Code Associated with Static Scan Issues .....	358
Closing Analysis Results .....	359
IntelliJ Plugin .....	359
Installing the IntelliJ Plugin .....	359
Configuring the IntelliJ Plugin .....	360
Uploading Code with the IntelliJ Plugin .....	360
Opening Analysis Results with the IntelliJ Plugin .....	367
Analysis Results in the IntelliJ Plugin .....	368

Analysis Trace Icons .....	370
Reviewing Issues from the IntelliJ Plugin .....	371
Auditing Issues from the IntelliJ Plugin .....	372
Locating the Source Code Associated with Static Scan Issues .....	373
Uninstalling the IntelliJ Plugin .....	374
FoDUploader .....	374
Downloading FoDUploader .....	375
Running FoDUploader .....	375
Chapter 10: Integrations .....	381
Importing External Scans .....	381
Importing an On-Premises Scan .....	381
Importing a Software Bill of Materials .....	383
Deleting an Imported Scan .....	383
Bug Tracker Integration .....	384
Configuring Bug Tracker Integration .....	385
Submitting Issues to the Bug Tracker .....	387
Manually Linking an Issue .....	389
Secure Code Warrior Integration .....	392
Launching Secure Code Warrior Training .....	393
Slack Integration for Notifications .....	394
Configuring Slack Integration .....	394
Deleting Slack Integration .....	396
Source Control Integration .....	397
Configuring Source Control Integration with Bitbucket .....	397
Configuring Source Control Integration with GitHub .....	398
Tracking Configured Integrations .....	399
Training Courses .....	401
Viewing Training Courses .....	401
Assigning Training Courses .....	402
Viewing the Training Report .....	402
Webhooks .....	403
Configuring a Webhook .....	404
Webhook Requests and Responses .....	406
Viewing Webhook Deliveries .....	408

Chapter 11: Policies and Support .....	410
Maintenance Schedule and Software Updates .....	410
Data Retention Policy .....	411
Getting Support .....	412
Accessing Support Resources .....	412
Submitting a Help Center Ticket .....	413
Tracking your Help Center Tickets .....	414
Send Documentation Feedback .....	416



# Preface

## Contacting Micro Focus Fortify on Demand Customer Support

Contact Micro Focus Fortify on Demand Customer Support through the following ways:

- Start a live chat or create a support ticket in the Fortify on Demand Help Center, accessible from the Fortify on Demand portal.
- Call 1.800.893.8141 or 650.800.3233.

## For More Information

For more information about Fortify software products:

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

## About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

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

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the Micro Focus Community:

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

## Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

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

# What's New

This section describes new features, improvements, and other updates in each release.

## v22.4

### Engine and Rulepack Updates

#### **Fortify Software Security Content 2022 Update 3 Support**

(November 2022 update) Fortify on Demand has implemented Fortify Software Security Content 2022 update 3 from Fortify Security Research (SSR). For more information, see <https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements/43116/cyberres-fortify-software-security-content-2022-update-3>.

### New Features

#### **Debricked Open Source Software Composition Analysis Updates**

Debricked open source software composition analysis was introduced in Fortify on Demand 22.3. As part of the ongoing work to implement Debricked scanning in Fortify on Demand, the following updates have been made to the Debricked integration:

- Issue recommendations display additional information: the next non-vulnerable version and multiple reference links (if available).
- The event log records scan status of open source scans, including cancellation reasons for Debricked scans.
- Debricked scan summaries are available on the Scans pages. The scan summary displays the scan ID, scan started and completed dates, and the cancellation reason (if applicable).
- The API endpoint `GET /api/v3/open-source-scans/{scanId}/sbom` has been added for downloading SBOMs.
- The Open Source Components pages now display a merged view of FoD-initiated and imported Debricked scans.

#### **Microservice Attributes Support**

Fortify on Demand now supports creation of microservice attributes. As with application attributes, Security Leads can manage microservice attributes. Microservice attributes are restricted to the **Text** data type. Users can specify and update attribute values when creating and updating applications.

In conjunction, associated GET, PUT, and POST endpoints have been updated. Microservice attributes have been added to the applications data export.

#### **API Updates**

The following endpoints have been added:

- GET /api/v3/applications/{applicationId}/vulnerabilities/{Id} (get a list of vulnerabilities that have the same instance ID)

**Note:** {Id} is the issue ID and not the vulnerability ID {vulnId}.

- GET /api/v3/scans/{scanId}/fpr (download FPR)

The following endpoints have been added for managing personal access tokens:

- DELETE /api/v3/personal-access-tokens/{personalAccessTokenId} (delete a personal access token)
- GET /api/v3/personal-access-tokens/{personalAccessTokenId} (get a personal access token)
- PUT /api/v3/personal-access-tokens/{personalAccessTokenId} (update a personal access token)
- GET /api/v3/personal-access-tokens (get a list of personal access tokens)
- POST /api/v3/personal-access-tokens (create a personal access token)
- PUT /api/v3/personal-access-tokens/{personalAccessTokenId}/secret (create a new personal access token secret)

For information on other API updates in this release, see the rest of the release notes.

### Workflow-Driven Dynamic Scans

Dynamic Website assessments can now be run as Workflow-Driven Scans by adding workflow macros to the scan settings. A workflow macro is a recording of HTTP events when a user navigates a website using a Web Macro Recorder tool. Users can create workflow macros with Fortify WebInspect's Web Macro Recorder, available on the Tools page.

A Workflow-Driven Scan uses the audit only mode (no crawling) and is completely automated. Fortify WebInspect audits only those URLs recorded in the macro and does not follow any hyperlinks encountered during the audit. Supported macros are .webmacro files, Burp Proxy captures, and .har files.

**Note:** The application being scanned must be external facing. Activity recorded in a macro overrides other scan settings.

## Improvements

### Dynamic Scan Settings Update

The following updates have been made to dynamic scan settings to accommodate changes that users make to web applications and APIs across scans:

- Dynamic scan settings are now saved at the release level, not the application level.

**Note:** This change is applied to dynamic scan settings that are saved moving forward.

- Users can update dynamic scan settings for a release created using copy state.
- Uploaded API project files were locked for editing upon the successful completion of a dynamic scan. These fields are now editable.

### **Event Log Filtering**

Filtering by date has been added to the event log. The filter is set to the last 24 hours by default.

### **Support for Reusing Email Addresses across Tenants**

Email addresses can now be reused for user accounts across different tenants. Email addresses cannot be reused for user accounts within the same tenant. The user ID must be unique.

### **Data Export Updates**

The **Microservice** (microservice name) and **Audited timestamp** (the date and time an issue was last audited) columns have been added to the issues data export.

### **Removal of Container Scanning**

Fortify on Demand has removed the container scanning feature from the portal.

### **Your Applications Page Updates**

The following updates have been made to Your Applications page:

- The list of applications on Your Applications page is now grouped into three tabs; all applications, microservice applications, and non-microservice applications.
- The ability to simultaneously edit application attributes and user groups for multiple applications has been moved from Your Releases page to Your Applications page.

# Chapter 1: Introduction

This guide provides instructions on using Fortify on Demand to run application security testing in the cloud. This guide is intended for application security professionals and development teams.

This section contains the following topics:

- [Fortify on Demand Overview](#) ..... 17
- [Security Rating System](#) ..... 18
- [Service Level Objectives](#) ..... 20

## Fortify on Demand Overview

Fortify on Demand is a Software as a Service (SaaS) solution that enables your organization to easily and quickly build and expand a Software Security Assurance program. Fortify on Demand's software security testing incorporates advanced and updated application testing technologies with expert review, dedicated account management, and 24/7 support.

An application submitted to Fortify on Demand undergoes a security assessment where it is analyzed for various software security vulnerabilities. Fortify on Demand offers static, dynamic, and mobile assessments at several service levels. For applications already in production, the Continuous Application Monitoring service combines continuous dynamic vulnerability scanning and risk profiling to provide visibility into the risk facing your organization's external-facing application portfolio.

### Security Assessments

A static assessment analyzes an application's source code, bytecode, and/or binary code. A dynamic assessment analyzes a running web application. A mobile assessment analyzes the mobile application's binary (analysis of network and backend web server is also available).

The Fortify on Demand testing team conducts a thorough analysis of your application for security vulnerabilities, including:

- Application scanning: the application is scanned using Fortify software.
- Expert review: an automated or manual audit (depending on the assessment type) of the scan results is included to ensure the highest possible degree of accuracy.
- Remediation validation: an assessment includes at least one free remediation scan to validate that the issues found have been fixed. The remediation scan is run on the same application after changes have been made to remedy the vulnerabilities found in the baseline assessment.

Fortify on Demand uses a 5-star rating system to rate applications that have been assessed. The assessment results are delivered in several ways, including various views in the UI, customizable reports, and detailed data exports.

## Entitlements

Fortify on Demand security testing services are available through the purchase of entitlements in the form of assessment units or scans. Entitlements are valid for 12 months from the effective date of the order term.

Assessment units can be redeemed for single assessments or subscriptions of any assessment type; scan entitlements represent quantities of single assessments or subscriptions of a specific assessment type. Subscriptions allow unlimited assessments of selected applications during the subscription period.

Refer to your contract for specific entitlement details.

## Support

Fortify on Demand offers support through self-service resources and the Fortify on Demand Help Center, staffed 24/7 by a dedicated support team of Technical Account Managers (TAMs).

# Security Rating System

Fortify on Demand provides useful information about the vulnerability of your applications. To ensure that the results you receive are consistent, understandable, and actionable, Fortify on Demand uses the following reporting conventions to rate your applications:

Likelihood and Impact .....	18
Priority Order .....	19
Five-Star Assessment Rating .....	20

## Likelihood and Impact

The likelihood and impact ratings define the level of risk for each discovered vulnerability.

### Likelihood

Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

### Impact

Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage could be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

## Priority Order

Fortify on Demand defines the following six priority levels as a way to categorize the severity of vulnerabilities (also known as “issues”).

### Critical

Critical issues have high potential impact and high likelihood of occurring. Critical issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to an application. As such, immediately remediate critical issues.

SQL injection is an example of a critical issue.

### High

High-priority issues have high potential impact, but low likelihood of occurring. High-priority issues are often difficult to detect and exploit, but they can result in large asset damage. These issues represent a high security risk to an application. Remediate high-priority issues in the next scheduled patch release.

Hard-coded password is an example of a high issue.

### Medium

Medium-priority issues have a low potential impact, but high likelihood of occurring. Medium-priority issues are easy to detect and exploit, but they typically result in little asset damage. These issues represent a moderate security risk to your application. Remediate medium-priority issues in the next scheduled product update.

Path manipulation is an example of a medium issue.

### Low

Low-priority issues have low potential impact and low likelihood of occurring. Low-priority issues can be difficult to detect and exploit and typically result in little asset damage. These issues represent a minor security risk to your application. Remediate low-priority issues as time allows.

Dead code is an example of a low issue.

### Best Practices

"Best practices" indicates no significant vulnerabilities in your application, just minor issues that may be less than ideal for your type of application.

### Info

“Info” is the lowest priority level. Fortify on Demand provides information about your application that does not represent a vulnerability but may be of general interest.

## Five-Star Assessment Rating

The Fortify on Demand 5-star rating system provides an overview on the likelihood and impact of vulnerabilities present within an application. A perfect rating within this system would be 5-stars, indicating that no vulnerabilities were uncovered.

★☆☆☆☆ Fortify on Demand awards one star to applications that have undergone a security review that identifies critical (high likelihood and high impact) issues. Vulnerabilities that are trivial to exploit and have a high business or technical impact should never exist in business-critical software.

★★☆☆☆ Fortify on Demand awards two stars to applications that have undergone a security review that identifies no critical (high likelihood and high impact) issues. Vulnerabilities that have a high impact, even if they are non-trivial to exploit, should never exist in business critical software.

★★★☆☆ Fortify on Demand awards three stars to applications that have undergone a security review that identifies no high (low likelihood and high impact) issues and meets the requirements needed to receive two stars. Vulnerabilities that have a low impact, but are easy to exploit, should be considered carefully as they may pose a greater threat if an attacker exploits many of them as part of a concerted effort or leverages a low impact vulnerability as a stepping stone to mount a high-impact attack.

★★★★☆ Fortify on Demand awards four stars to applications that have undergone a security review that identifies no medium (high likelihood and low impact) issues and meets the requirements for three stars.

★★★★★ Fortify on Demand awards five stars, the highest rating, to applications that have undergone a security review that identifies no issues.

## Service Level Objectives

All assessments have a target turnaround time, represented by the service level objective (SLO) of the chosen assessment type. The SLO is specified in business days, based on the Fortify on Demand data center's time zone. The SLO is four hours to two business days for a static assessment, two to three business days for a dynamic assessment, and one to four days for a mobile assessment.

**Note:** The portal displays the SLO of the selected assessment type when you are setting up an assessment. For more information, see ["Configuring a Static Scan" on page 105](#), ["Configuring a Dynamic Scan" on page 118](#), and ["Configuring a Mobile Scan" on page 141](#).

If an assessment does not meet customary testing requirements, the testing team may pause the SLO timer while waiting for a response from the customer. The testing team is committed to promptly restarting the timer and testing as soon as possible.

If you have additional questions about SLOs and balancing your business timeline with an assessment service level, contact support.



**Note:** Service Level Agreements (SLAs) are specific contractual agreements with customers. The turnaround times may differ from defined SLOs. Service Level Agreements are defined in your customer statement of work (SOW) and include targets and liabilities if they are not met.

### **Service Level Objective Start and End Dates**

The SLO start and end dates are defined as follows:

- **Start Date:** The date the application assessment was requested to be started
- **End Date:** The date the results are available

### **Service Level Objective Exceptions**

A static assessment SLO does not apply to any of the following exceptions:

- Application has not been packaged correctly as per Fortify on Demand best practice guidelines
- The application payload exceeds 1,000MB

A dynamic or mobile assessment SLO does not apply to any of the following exceptions:

- Fortify on Demand is not provided continuous 24-hour per day access and fully operational test credentials to assess the application that is in scope.
- Fortify on Demand is not able to configure security testing tools to use a minimum of fifteen (15) concurrent connections continuously to assess a single application with an average response time of less than 600ms to an HTTP/HTTPS request
- Mobile binary is obfuscated or is not prepared as per Fortify on Demand best practice guidelines.

# Chapter 2: Getting Started

This section contains the following topics:

- [Before You Start](#) ..... 22
- [Logging In and Out of the Portal](#) ..... 22
- [Resetting Your Password](#) ..... 24
- [Navigating the Portal](#) ..... 24
- [Searching the Portal](#) ..... 26
- [Managing Your Account Settings](#) ..... 26
- [Managing Notifications](#) ..... 30

## Before You Start

Before you access Fortify on Demand, verify that you have the following:

- An active internet connection
- Portal credentials

**Note:** You will receive instructions for setting up your credentials in a welcome email. If you have not received the email, check your spam filter.

- Monitor with a minimum display resolution of 1280 x 720 (recommended 1920 x 1080)
- One of the following supported browsers installed:
  - Chrome latest version
  - Firefox Quantum latest version
  - Safari on Mac latest version (Safari on PC is not supported)
  - Edge latest version

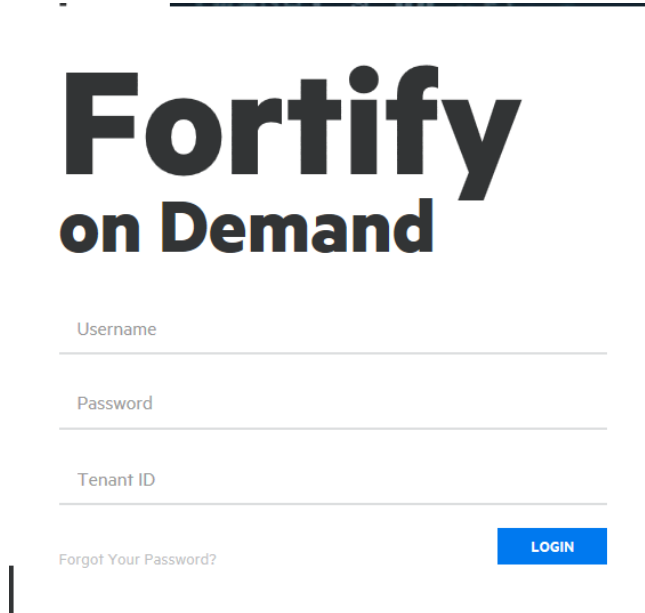
## Logging In and Out of the Portal

You can access the portal once you have received your portal credentials.

### Logging in to the Portal

To log in to the portal:

1. Type the portal URL that was provided with your user credentials in your browser's address bar.  
The login page appears.
2. Type your username, password, and tenant code.



**Note:** If you have logged in through SSO within the last 30 days, the SSO Login link is available to log back in.

3. Click **Login**.  
The landing page appears. If you have not set a challenge question and corresponding answer, you are redirected to your account settings page instead.

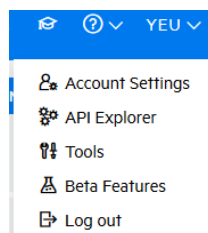
**Note:** If your organization has two factor authentication enabled, you are prompted to type a security code that you receive through SMS or email.

## Logging out of the Portal

Log out of the portal from the portal toolbar settings.

To log out of the portal:

1. Click your account name and select **Log Out**.

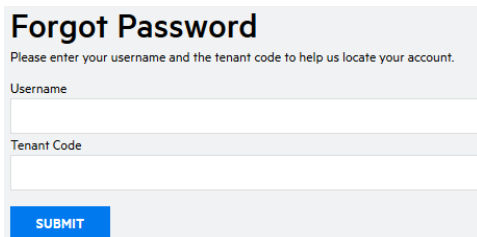


## Resetting Your Password

To reset a forgotten password:

1. Click **Forgot Your Password?** on the login page.

The Forgot Password page appears.



2. Type your username and tenant code.

3. Click **Submit**.

An email containing the password reset link is sent to the email address associated with the user account.

4. Click the link in the email.

The Reset Password page appears.

**Note:** If the password reset link has expired, follow the instructions in the email to request a new link.

5. In the **Password Challenge Answer** field, type the answer to the challenge question. If you do not have a password challenge question and answer, this step does not apply to you.

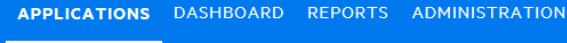
6. Type and retype the password.



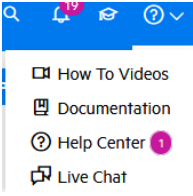

7. Click **Ok**.

The password is reset.

## Navigating the Portal

The portal pages share a common page layout. The following table describes general navigation in the portal.

Task	Action
Navigate to a parent view	Select one of the following views: 


Task	Action
<p>Access account settings and additional resources</p>	<p>Click your account name.</p> 
<p>Access portal search</p>	<p>Click . For more information, see "<a href="#">Searching the Portal</a>" on the next page.</p>
<p>Access portal notifications</p>	<p>Click . For more information see "<a href="#">Managing Notifications</a>" on page 30.</p>
<p>Access training courses</p>	<p>Click . For more information, see "<a href="#">Training Courses</a>" on page 401.</p>
<p>Access help resources</p>	<p>Click the help menu.</p> 
<p>Navigate to a page within a parent view</p>	<p>Click an icon on the sidebar.</p> 
<p>Access context-sensitive help</p>	<p>Click . A new window opens that displays the help topic for the feature.</p>
<p>Sort columns on a page</p>	<p>Click a column header. A white triangle in the header indicates the field being sorted and the sort order of your data. To reverse the order, click the header a second time.</p>
<p>Change the number</p>	<p>Click <b>25</b>, <b>50</b>, or <b>100</b>.</p>

Task	Action
of items displayed on a page	<p>Display: 25 <b>50</b> 100</p> <p><b>Note:</b> The <b>Discovered</b> tab on Your Applications page supports displaying 250 and 500 items per page.</p>
View another page in the list	<p>Click a page number or an arrow.</p> <p><b>1</b> 2 3 4 → → </p>

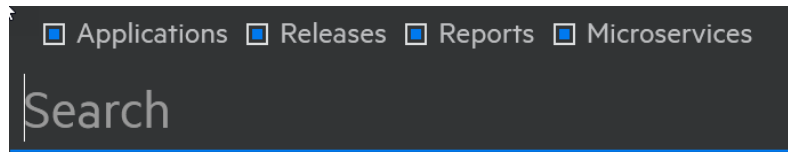
## Searching the Portal

Fortify on Demand provides several ways of locating a resource in the portal. You can use the **Search** box located in the portal toolbar to search for an application, release, microservice, or report at the tenant level.

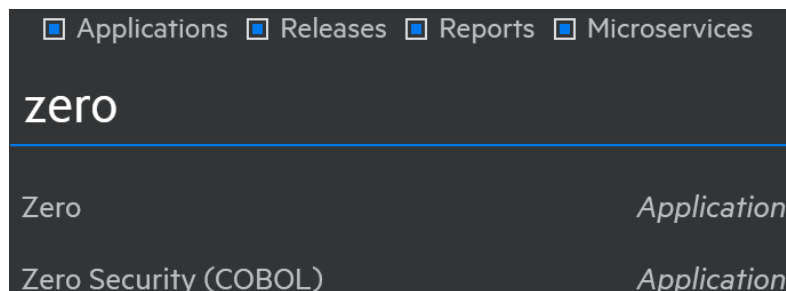
To search for an application, release, microservice, or report in the portal:

1. Click the  icon on the portal toolbar.

The search box appears. All item types are included in the search by default.



2. Clear one or more of the **Applications**, **Releases**, **Reports**, and **Microservices** check boxes to limit search results to the desired selection.
3. In the search box, type the full or partial name of the item that you want to search for. Search results appear in a drop-down list.



4. Make your selection from the list. The portal refreshes with your selection.

## Managing Your Account Settings

You can view and edit your account settings from the portal toolbar.

This section covers the following topics:

[Editing Your Account Settings](#) .....27

[Changing Your Account Password](#) ..... 28

[Opting In To and Out Of Beta Features](#) ..... 29

## Editing Your Account Settings

You can update your personal contact information, portal preferences, and password reset question and answer on the My Account page.

To edit your account settings:

1. Click your account name and select **Account Settings**.

The My Account page appears.

2. Update the fields as needed. Fields that are outlined in red must be completed.

Field	Description
First Name	Your first name
Last Name	Your last name
Phone Number	Your phone number
Date Format	Date format displayed: <b>MM/DD/YYYY, DD/MM/YYYY, YYYY/MM/DD</b>
Time Format	Time format displayed: <b>12 Hour AM/PM, 24 Hour</b>

Field	Description
Language	Language displayed: <b>English, Español, 日本語</b> <b>Note:</b> Your reports are generated in your selected language.
Password Challenge Question	A list of password challenge questions
Password Challenge Answer	Your case-insensitive answer to the selected password challenge question <b>Note:</b> You will not be able to save your account changes unless you have set a password challenge question and answer.
Reset Tour Popups	Replay user tour

3. Update your subscriptions in the **Email Subscriptions** section. Email subscriptions keep you up-to-date with Fortify on Demand events. You can sign up to receive notifications about releases and maintenance, security advisories, and relevant webinars and conferences.
4. Click **Save**.  
A confirmation message appears indicating that you have successfully saved your changes.

## Changing Your Account Password

You can change your account password on the My Account page.

**Note:** Passwords must be at least 16 characters long, not contain easy common password phrases, and have at least: 1 capital letter, 1 lower case letter, 1 number, and 1 special character.

To change your account password:

1. Click your account name and select **Account Settings**.  
The My Account page appears.



**My Account** CHANGE PASSWORD SAVE

First Name: You

Last Name: Huang

Phone Number: 7701234567

Username: HuangTam

Tenant: 30004

Email Subscriptions

Signup (Check to Subscribe)

Release and Maintenance Notifications

Events (Ex. Webinars, Conferences, etc)

Security Advisories and Research

The following settings determine what formats are used to display dates and times.

Changes to display formats will not be reflected until the next data refresh.

Date Format: YYYY/MM/DD

Time Format: 12 Hour AM/PM

Language: English

Password Challenge Question: What is your favorite pet's name?

Password Challenge Answer: .....

RESET TOUR POPUPS

2. Click **Change Password**.

The Change Password page appears.

**Change Password**

Type in your existing password

Old Password

New Password

Confirm New Password

OK BACK TO ACCOUNT

3. Type your current password in the **Old Password** field.
4. Type a new password in the **New Password** field.
5. Retype the new password in the **Confirm New Password** field.
6. Click **OK** button to change your password, or click **Back to Account** to exit the page.

## Opting In To and Out Of Beta Features

Fortify on Demand might release beta features to collect feedback on their implementation. You can opt in to and opt out of beta features for your account.

To manage beta features:

1. Click your account name and select **Beta Features**.  
The Beta Features page appears.

2. If beta features are available, move the slider from **No** to **Yes** to enable a beta feature and vice versa to disable it.

Click **Submit Feedback** to provide feedback. Your comments are appreciated.

## Managing Notifications

Fortify on Demand provides a robust in-product notifications engine to enable users to better monitor key activity in the portal, which is particularly important for large applications and user bases. Users are initially assigned system default global subscriptions for notable events (including when an application's Business Criticality is changed, when a failing release is promoted to production, and when scans of an application are started, paused, completed, or canceled). Users can conveniently access notifications for applications to which they have access from the portal toolbar.

Users can create individual subscriptions to receive additional notifications. Security Leads can create tenant level global subscriptions for all users, specific roles, or specific groups. The following notification trigger types are available:

- Application Monitoring updates: changes between the enabled and disabled states, new vulnerabilities, risk profile updates
- Application creation, updates, and deletion
- Release creation, updates—including promotion of failing releases to production, and deletion
- Scan status updates
- Issue updates
- Report generation

This section contains the following topics:


<a href="#">Viewing Notifications</a> .....	30
<a href="#">Creating an Individual Subscription</a> .....	31
<a href="#">Creating a Global Subscription</a> .....	34
<a href="#">Editing a Subscription</a> .....	36
<a href="#">Deleting a Subscription</a> .....	38

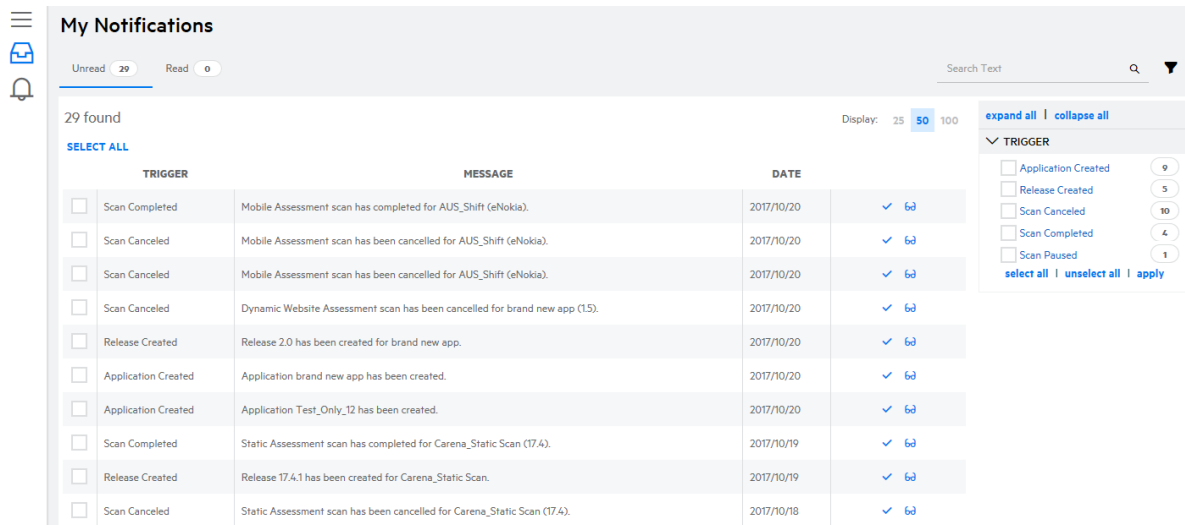
## Viewing Notifications

You can view notifications from any page in the portal. When a trigger event occurs for which you are subscribed, a number next to the Notifications icon on the toolbar is incremented. This number is a tally of your notifications that have not been marked as read.

**Note:** All notifications, read or unread, are deleted after three months.

To view notifications:

1. Click the  icon on the portal toolbar.  
The Notifications page appears, displaying a list of your unread notifications.



**My Notifications**

Unread **29** Read **0** Search Text

29 found Display: 25 **50** 100 expand all | collapse all



**TRIGGER**

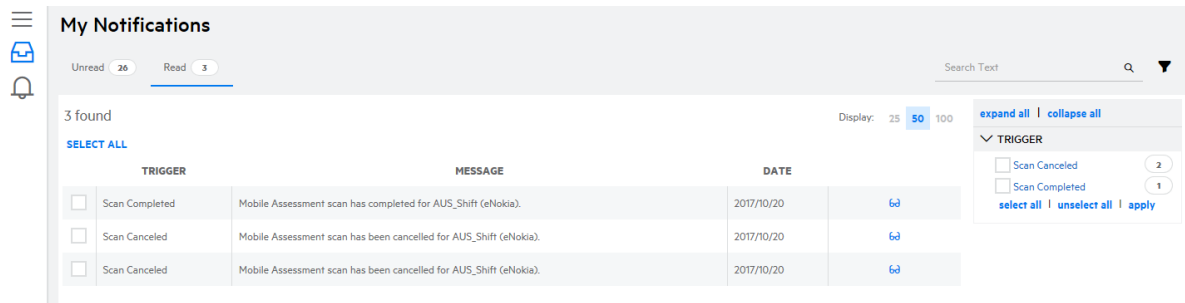
TRIGGER	MESSAGE	DATE	
<input type="checkbox"/> Scan Completed	Mobile Assessment scan has completed for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Dynamic Website Assessment scan has been cancelled for brand new app (1.5).	2017/10/20	✓ 6d
<input type="checkbox"/> Release Created	Release 2.0 has been created for brand new app.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application brand new app has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application Test_Only_T2 has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Completed	Static Assessment scan has completed for Carena_Static Scan (17.4).	2017/10/19	✓ 6d
<input type="checkbox"/> Release Created	Release 17.4.1 has been created for Carena_Static Scan.	2017/10/19	✓ 6d
<input type="checkbox"/> Scan Canceled	Static Assessment scan has been cancelled for Carena_Static Scan (17.4).	2017/10/18	✓ 6d

**TRIGGER**

- Application Created (9)
- Release Created (5)
- Scan Canceled (10)
- Scan Completed (4)
- Scan Paused (1)

select all | unselect all | apply

2. To view a notification in greater detail, click the  icon in the notification's action column. You are taken to the relevant application, release, or individual issue's page.
3. To mark a notification as read, click the  icon in the notification's action column. You can also filter the notification list and click **Mark as Read** to batch edit notifications.  
The notifications are moved to Read Notifications and removed from the tally.
4. To view notifications that you have previously marked as read, select the **Read** tab.  
The list of your read notifications appears.



**My Notifications**

Unread **26** Read **3** Search Text

3 found Display: 25 **50** 100 expand all | collapse all

**TRIGGER**

TRIGGER	MESSAGE	DATE	
<input type="checkbox"/> Scan Completed	Mobile Assessment scan has completed for AUS_Shift (eNokia).	2017/10/20	6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	6d

**TRIGGER**


- Scan Canceled (2)
- Scan Completed (1)

select all | unselect all | apply

## Creating an Individual Subscription

In addition to receiving global notifications, you can create your own subscriptions to receive notifications triggered by your specified criteria.

To create an individual subscription:

1. Click the  icon on the portal toolbar.  
The Notifications page appears.

**My Notifications**

Unread 29 Read 0

Search Text

29 found Display: 25 50 100

[SELECT ALL](#)

TRIGGER	MESSAGE	DATE	
<input type="checkbox"/> Scan Completed	Mobile Assessment scan has completed for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Dynamic Website Assessment scan has been cancelled for brand new app (1.5).	2017/10/20	✓ 6d
<input type="checkbox"/> Release Created	Release 2.0 has been created for brand new app.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application brand new app has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application Test_Only_12 has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Completed	Static Assessment scan has completed for Carena_Static Scan (17.4).	2017/10/19	✓ 6d
<input type="checkbox"/> Release Created	Release 17.4.1 has been created for Carena_Static Scan.	2017/10/19	✓ 6d
<input type="checkbox"/> Scan Canceled	Static Assessment scan has been cancelled for Carena_Static Scan (17.4).	2017/10/18	✓ 6d

expand all | collapse all

TRIGGER

- Application Created (9)
- Release Created (5)
- Scan Canceled (10)
- Scan Completed (4)
- Scan Paused (1)

[select all](#) | [unselect all](#) | [apply](#)

2. Click **Subscriptions**.

A list of your individual subscriptions appears.

**My Subscriptions**

My Subscriptions 2 Global Subscriptions 13

Search Text [+ NEW SUBSCRIPTION](#)

2 found Display: 25 50 100

TRIGGER	SCOPE	NOTE	
Issue New Comment	Application		6d <a href="#">edit</a> <a href="#">delete</a>
Issue Assigned To User	All Applications	Issue Assigned	6d <a href="#">edit</a> <a href="#">delete</a>

3. Click **+New Subscriptions**.

The Create Subscription modal window opens.

**Create Subscription** [Close]

**Options**  
Summary

Trigger  
(Choose One)

Scope  
All Applications

Note

Send Emails No

Send to Slack No

BACK NEXT SAVE

4. Complete the fields. Fields are required unless otherwise noted.

Field	Description
<b>Trigger</b>	Select the trigger type from the list
<b>Scope</b>	Select the scope to which the trigger will apply from the list: <b>All Applications</b> (default), <b>Application</b> , <b>Application Type</b> , <b>Application Attribute</b> , and <b>Business Criticality</b> .
<b>Note</b>	(Optional) Type a note for the subscription.
<b>Send Emails</b>	(Optional) Move the slider from <b>No</b> to <b>Yes</b> to enable sending email notifications. This option is only available for non-issue related notifications.
<b>Send to Slack</b>	(Optional) Move the slider from <b>No</b> to <b>Yes</b> to post notifications to Slack. This option is only available if Slack integration has been configured and is limited to Security Leads.


5. Click **Next**.  
If you selected a scope other than **All Applications**, the Scope page appears. Otherwise, skip to step 7.
6. Select the scope value and click **Next**.
7. Review the notification trigger settings and click **Save**.

The new subscription appears in your list of individual subscriptions.

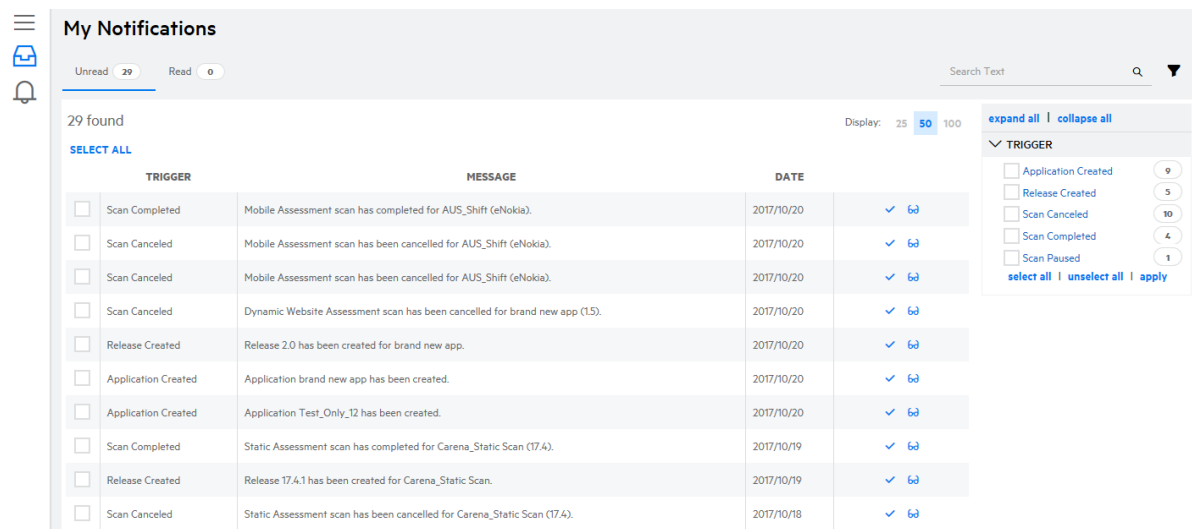
## Creating a Global Subscription

Security Leads can create tenant level global subscriptions for all users, specific roles, or specific groups.

To create a global subscription:

1. Click the  icon on the portal toolbar.

The Notifications page appears.



**My Notifications**

Unread 29 Read 0

Search Text

29 found

Display: 25 50 100

[expand all](#) | [collapse all](#)

TRIGGER

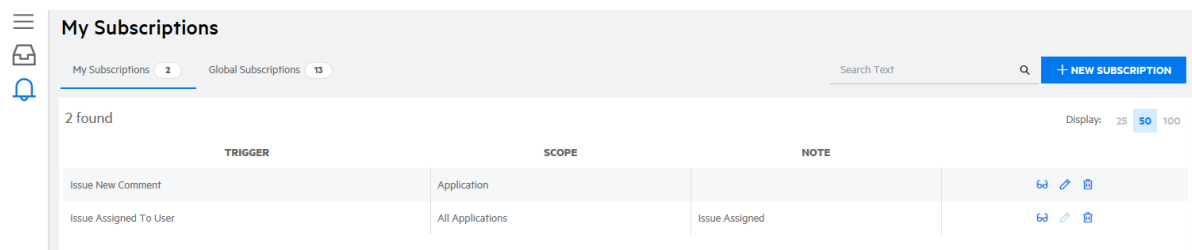
TRIGGER	MESSAGE	DATE	
<input type="checkbox"/> Scan Completed	Mobile Assessment scan has completed for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Dynamic Website Assessment scan has been cancelled for brand new app (15).	2017/10/20	✓ 6d
<input type="checkbox"/> Release Created	Release 2.0 has been created for brand new app.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application brand new app has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application Test_Only_12 has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Completed	Static Assessment scan has completed for Carena_Static Scan (17.4).	2017/10/19	✓ 6d
<input type="checkbox"/> Release Created	Release 17.4.1 has been created for Carena_Static Scan.	2017/10/19	✓ 6d
<input type="checkbox"/> Scan Canceled	Static Assessment scan has been cancelled for Carena_Static Scan (17.4).	2017/10/18	✓ 6d

Application Created 9  
Release Created 5  
Scan Canceled 10  
Scan Completed 4  
Scan Paused 1

[select all](#) | [unselect all](#) | [apply](#)

2. Click **Subscriptions**.

A list of your individual subscriptions appears.



**My Subscriptions**

My Subscriptions 2 Global Subscriptions 13

Search Text

2 found

Display: 25 50 100

[+ NEW SUBSCRIPTION](#)

TRIGGER	SCOPE	NOTE	
Issue New Comment	Application		6d 6d 6d
Issue Assigned To User	All Applications	Issue Assigned	6d 6d 6d

3. Select the **Global Subscriptions** tab.

A list of global subscriptions, including system-default global subscriptions, appears.

TRIGGER	SCOPE	CREATED BY	RECIPIENT	NOTE
Scan Resumed	All Applications	2, May (05-02) Tenant	Everyone	Default System Notification for Scan Resumed
Payload Has No Source Files	All Applications	2, May (05-02) Tenant	Everyone	Default System Notification for Payload Has No Source...
Application Business Criticality Updated	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ApplicationBusinessCrL...
Application Created	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ApplicationCreated
Falling Release Moved To Production	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for FallingReleaseMovedT...
Scan Canceled	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ScanCancelled
Network Scan Imported	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ScanImported
Scan Paused	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ScanPaused
Release SDLC Status Updated	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ReleaseSDLCStatusUp...
Release Created	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ReleaseCreated
Scan Completed	All Applications	2, May (05-02) Tenant	Everyone	System Default Notification for ScanComplete

4. **Click +New Subscription.**

The Create Subscription modal window opens.

5. Complete the fields. Fields are required unless otherwise noted.

Field	Description
<b>Trigger</b>	Select the trigger type from the list
<b>Recipient</b>	Select the subscription audience from the list: <b>Everyone</b> (default), <b>Group</b> , and

	<p><b>Role.</b> If you select <b>Group</b> or <b>Role</b>, select a specific group or role, respectively.</p> <p><b>Note:</b> Recipients are limited to users who have access to the application referenced in a notification.</p>
<b>Scope</b>	Select the scope to which the trigger will apply from the list: <b>All Applications</b> (default), <b>Application</b> , <b>Application Type</b> , <b>Application Attribute</b> , and <b>Business Criticality</b> .
<b>Note</b>	(Optional) Type a note for the subscription.
<b>Send Emails</b>	(Optional) Move the slider from <b>No</b> to <b>Yes</b> to enable sending email notifications. This option is only available for non-issue related notifications.
<b>Send to Slack</b>	(Optional) Move the slider from <b>No</b> to <b>Yes</b> to post notifications to Slack. This option is only available if Slack integration has been configured and is limited to Security Leads.

6. Click **Next**.

If you selected a scope other than **All Applications**, the Scope page appears. Otherwise, skip to step 8.

7. Select the scope value and click **Next**.


8. Review the notification trigger settings and click **Save**.

The new subscription appears in the list of global subscriptions.

## Editing a Subscription

You can edit the scope value of custom subscriptions if the scope type is not set to the default of **All Applications**.

To edit the scope of a custom subscription:

1. Click the  icon on the portal toolbar.

The Notifications page appears.



**My Notifications**

Unread 29 Read 0

Search Text

29 found Display: 25 50 100 expand all | collapse all

SELECT ALL

TRIGGER	MESSAGE	DATE	
<input type="checkbox"/> Scan Completed	Mobile Assessment scan has completed for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Canceled	Dynamic Website Assessment scan has been cancelled for brand new app (1.5).	2017/10/20	✓ 6d
<input type="checkbox"/> Release Created	Release 2.0 has been created for brand new app.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application brand new app has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Application Created	Application Test_Only_T2 has been created.	2017/10/20	✓ 6d
<input type="checkbox"/> Scan Completed	Static Assessment scan has completed for Carena_Static Scan (17.4).	2017/10/19	✓ 6d
<input type="checkbox"/> Release Created	Release 17.4.1 has been created for Carena_Static Scan.	2017/10/19	✓ 6d
<input type="checkbox"/> Scan Canceled	Static Assessment scan has been cancelled for Carena_Static Scan (17.4).	2017/10/18	✓ 6d

TRIGGER

- Application Created 9
- Release Created 5
- Scan Canceled 10
- Scan Completed 4
- Scan Paused 1

select all | unselect all | apply

2. Click **Subscriptions**.

A list of your existing individual subscriptions appears.

**My Subscriptions**

My Subscriptions 2 Global Subscriptions 13

Search Text + NEW SUBSCRIPTION

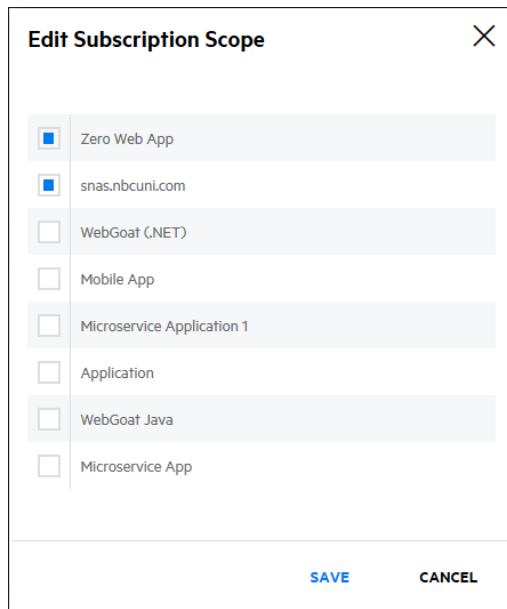
2 found Display: 25 50 100

TRIGGER	SCOPE	NOTE	
Issue New Comment	Application		6d ✎ 📄
Issue Assigned To User	All Applications	Issue Assigned	6d ✎ 📄

3. If you are editing an individual subscription, remain on the **My Subscriptions** tab. If you are a Security Lead who is editing a custom global subscription, select the **Global Subscriptions** tab.

4. Click the ✎ icon next to the subscription you want to edit.

The Edit Subscription Scope modal window opens.




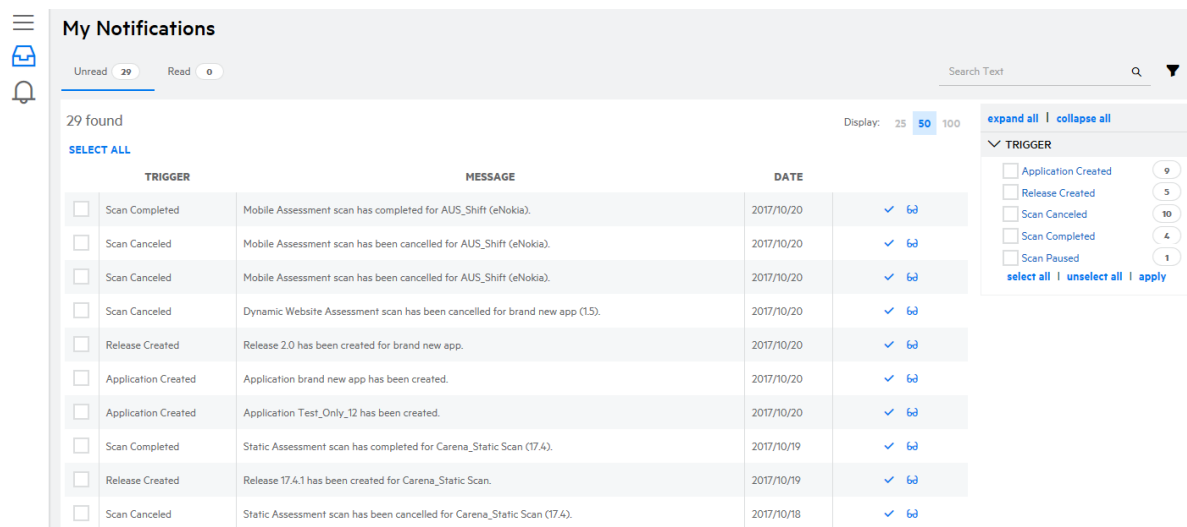
5. Select the new scope value and click **Save**.  
Your change to the subscription is saved.

## Deleting a Subscription

You can delete individual subscriptions that you created. Security Leads can delete all global subscriptions, including system default global subscriptions.

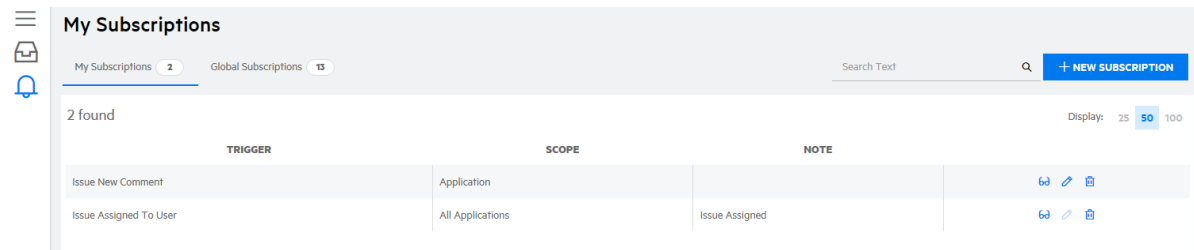
To delete a subscription:

1. Click the  icon on the portal toolbar.  
The Notifications page appears.



2. Click **Subscriptions**.

A list of your individual subscriptions appears.



3. If you are deleting an individual subscription, stay on the **My Subscriptions** tab. If you are deleting a global subscription, select the **Global Subscriptions** tab.
4. Click the icon next to the subscription you want to delete.  
A confirmation message appears.
5. Click **Yes** to confirm the deletion.  
The subscription is removed from the list of subscriptions.

# Chapter 3: Managing Applications and Releases

Security assessment results are organized according to applications and associated releases in Fortify on Demand. Users can manage applications and releases in the portal.

This section contains the following topics:

- [Structuring Applications and Releases](#) ..... 40
- [Managing an Application](#) ..... 43
- [Managing a Release](#) ..... 59
- [Viewing Applications in the Tenant](#) ..... 70
- [Viewing Releases in the Tenant](#) ..... 76
- [Searching Applications and Releases](#) ..... 80
- [Creating Deep Links](#) ..... 81

## Structuring Applications and Releases

Fortify on Demand defines an application and release for the purpose of security assessments.

### Application Definition

An application is a codebase. It serves as a top-level container for one or more releases.

Fortify on Demand defines an application in the following contexts:

For static assessments, an application is defined as a deployable unit of code consisting of a collection of source and/or byte code instruction files that:

- Can deliver some or all of the functionality of a business application
- Is written in the same technology family
- Is built on a single platform
- Does not include any loosely coupled components
- Can be configured to run on an application server (e.g., a Web Application Archive [WAR] or Enterprise Archive [EAR] file for a Java application or a solution in team foundation server for a .NET application)

A microservice as a small, modular service that runs as an independent, loosely coupled process and communicates through a well-defined, lightweight mechanism to serve a single function of a business application. For an application using a microservices architecture, a Static Subscription entitles a

customer to test up to 10 microservices that form some or all of the application. Each microservice must be packaged and submitted as a single ZIP file of 100 MB or less. For all other static assessment services, each microservice is considered a separate application.

The following conditions apply to microservice applications:

- Supported technology stacks are: Go, .NET, .NET Core, JAVA/J2EE, JS/TS/HTML, PHP, Python, and Ruby.
- Static scans submitted for multiple microservices are placed in a queue and will be scanned in the order in which they were queued.
- Third party libraries are always excluded when scanning microservices.

For dynamic assessments, an application is defined as a fully qualified domain name (FQDN). For example, for `www.microfocus.com`:

- `www.microfocus.com` is the FQDN and is the application.
- `www.microfocus.com/news/` is the same hostname and hence the same FQDN and so is the same application.
- `community.microfocus.com` is a different subdomain and hence a different FQDN and so is a different application.
- `www.microfocus.co.uk` is a different domain name and hence a different FQDN and so is a different application.

The application can only have a single authentication management system with the following exceptions:

- Forms authentication and single network authentication (basic/digest/NTLM) is allowed.
- Forms authentication, single network authentication and application generated authentication such as bearer tokens is allowed.

User logins may not be “daisy chained”. For example, two forms authentication mechanisms are not permitted.

For web API applications only, the customer must provide a definition of the API endpoints:

- Dynamic Assessments
  - REST API - OpenAPI JSON specification or Postman collection with valid values for all parameters and a hard coded and long-lived authentication token
- Dynamic+ Assessments
  - REST API - OpenAPI JSON specification or Postman collection
  - SOAP – single SOAP WSDL file

Working examples, with valid values for all parameters, must be provided.

For mobile assessments, an application is a single installable application for a single hardware platform. Mobile applications submitted for testing must be in the form of a compiled IPA (iOS) or APK (Android).

## Release Definition

A release is a particular iteration of a codebase. In Fortify on Demand, release versioning provides a useful way to differentiate and track scan activity. You can structure releases depending on your organization's reporting needs and development processes.

The following examples show how releases can be structured:

- Static assessments:
  - Create one main release, copied from an initial baseline release, for automated scans on builds from a continuous integration build server . Periodically, create branch releases for scenarios such as major deployments of code (using copy state), more detailed analysis (including 3rd party libraries and/or choosing manual audit for a baseline, or sandbox releases to do a one-time scan without affecting metrics).
  - Create a new release for every major product release (using copy state) and run scans during a release cycle before moving to the next release.
  - Create a release for every build. Fortify does not recommend this approach due to the lack of trending and increased overhead.
- Dynamic assessments:
  - Create a single release, based on the environment being scanned (development, staging, UAT, or production), for all scans. The release is usually named by the URL.
  - Create a new release for each major deployment (using copy state).
- Static plus dynamic assessments:
  - Implement the above examples by themselves or in combination. For example, you can implement the first static assessment example as the main approach, and either run dynamic scans against the main and major release branches or run dynamic scans against a separate release that is independent of static scans.
- Mobile assessments:
  - For assessments of only the mobile binary, implement the static assessment examples.
  - For assessments that include backend web services, implement the dynamic assessment examples.

In addition, you can assign different Software Development Life Cycle (SDLC) stages to a release to track it as it progresses through the SDLC. Fortify on Demand uses the following SDLC stages:

- Development
- QA/Test
- Production
- Retired

**Note:** New scans cannot be started for a retired release. If a release is retired while a scan is in progress, the scan will still finish.

## Managing an Application

You can create, view, and edit applications, depending on your user permissions.

This section covers the following topics:

<a href="#">Creating an Application</a>	43
<a href="#">Viewing Application Details</a>	50
<a href="#">Editing Application Settings</a>	53
<a href="#">Managing User Assignment to an Application</a>	55
<a href="#">Viewing the Application Event Log</a>	57
<a href="#">Deleting an Application</a>	59

### Creating an Application

Before you can start the initial security assessment of an application, you need to create a new application in Fortify on Demand.

To create an application:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **+New Application**.  
The Create Application wizard appears.
3. In the **Application Details** page, define the application. Fields are required, unless otherwise noted.

**Create Application**
✕

**Application Details**

Release Details

Application Attributes

User Groups

Summary

Application Name

Business Criticality

Application Type

Description

Email Notifications

Separate multiple email addresses with a semicolon or comma

BACK
NEXT
SAVE

Field	Description
<b>Application Name</b>	Type the name of your application.
<b>Business Criticality</b>	Select the application's level of importance: <ul style="list-style-type: none"> <li><b>High:</b> Security issues could have catastrophic consequences for the business.</li> <li><b>Medium:</b> Security issues would have non-trivial consequences, but ones which do not pose a life-or-death threat to the business.</li> <li><b>Low:</b> Security issues can be ignored or addressed gradually as time permits</li> </ul>
<b>Description</b>	(Optional) Type a description of the application that will help you manage multiple applications.
<b>Email Notifications</b>	(Optional) List the email addresses that will receive email notifications of scan status updates for the application. Separate multiple email addresses



Field	Description
	with a semicolon or comma.
<b>Application Type</b>	Select the application type: <b>Web / Thick-Client</b> or <b>Mobile</b> .
<b>Microservice Application</b>	Create a Help Center ticket to have the feature enabled. ( <b>Web / Thick-Client</b> applications only) Select the check box to scan the application as a microservice application.  <b>Important!</b> The designation of a microservice application is permanent and cannot be changed after the application has been created.

4. Click **Next**.
5. (Microservice applications only) In the **Microservices** page, type the name of a microservice in the text box and click **+**.

The microservice is added below. You can add up to 10 microservices.

**Note:** You can also add microservices to an application after it has been created.

**Create Application** [Close]

- ✓ Application Details
- Microservices**
- Release Details
- Application Attributes
- User Groups
- Summary

Microservices [Text Input] +

Define one or more microservices for this application (limit 3).

BACK NEXT SAVE

6. Click **Next**.
7. (Microservice applications only) If microservice attributes are configured for the tenant, in the **Microservices Attributes** page, specify the microservice attribute. Microservice attribute values are of text data type.

The screenshot shows a 'Create Application' dialog box. On the left is a sidebar with the following items: 'Application Details' (checked), 'Microservices' (checked), 'Microservice Attributes' (bolded and selected), 'Release Details', 'Application Attributes', 'User Groups', and 'Summary'. The main content area is titled 'Microservice Attributes' and contains a label 'MS Attr1' above a text input field. At the bottom right of the dialog, there are three buttons: 'BACK', 'NEXT', and 'SAVE'.

8. Click **Next**.
9. In the **Release Details** page, define a release of the application. The release represents a iteration of your application that will be tested. Fields are required, unless otherwise noted.

### Create Application ✕

- ✓ Application Details
- ✓ Microservices
- Release Details**
- Application Attributes
- User Groups
- Summary

Release Name

SDLC Status

Microservice

Owner

Description

BACK NEXT SAVE

Field	Description
<b>Release Name</b>	Type the name of your release.
<b>SDLC Status</b>	Select the Software Development Lifecycle from the list. The <b>Retired</b> option is not available.
<b>Microservice</b> (microservice applications only)	Select the microservice that will be linked to the release from the drop down list. A release must be linked to a microservice.
<b>Owner</b>	Select the owner from of the release. The owner will receive email notifications of scan status updates for the release.
<b>Description</b>	(Optional) Type a description that helps describe the release.

10. Click **Next**.
11. If custom application attributes are configured for the tenant, in the **Application Attributes** page, specify the application attributes.

**Create Application** [Close]

- ✓ Application Details
- ✓ Microservices
- ✓ Release Details
- Application Attributes**
- User Groups
- Summary

External  
(Choose One) [Dropdown Arrow]

Region  
(Choose One) [Dropdown Arrow]

BACK NEXT SAVE

12. Click **Next**.
13. If user groups have been configured for your tenant, in the **User Groups** page, select the groups that have access to the application. You can use the search box to search group names.

### Create Application ✕

- ✓ Application Details
- ✓ Microservices
- ✓ Release Details
- ✓ Application Attributes
- User Groups**
- Summary

Select groups that should have access to this application.

	GROUP NAME	ASSIGNED USERS
<input type="checkbox"/>	Lead Developer	0

[BACK](#) [NEXT](#) [SAVE](#)

14. Click **Next**.
15. In the **Summary** page, review the application settings.

**Create Application**

✓ Application Details  
✓ Microservices  
✓ Release Details  
✓ Application Attributes  
✓ User Groups  
**Summary**

**Application Details**

**Application Name**  
Microservice App

**Business Criticality**  
Low

**Application Description**  
(none)

**Application Type**  
Web / Thick-Client

**Microservice Application**  
Yes

**Email Notifications**  
(none)

**Application Attributes**

**Region**  
Americas

**Release Details**

**Release Name**  
v1

**SDLC Status**  
Development

**Microservice**  
M1

**Owner**  
Huang, Yeu-Li

**Release Description**  
(none)

**User Groups**

**Selected Groups**  
(none)

BACK NEXT SAVE

16. Click **Create Application**.

You are redirected to the Overview page of your new application's release.

## Viewing Application Details

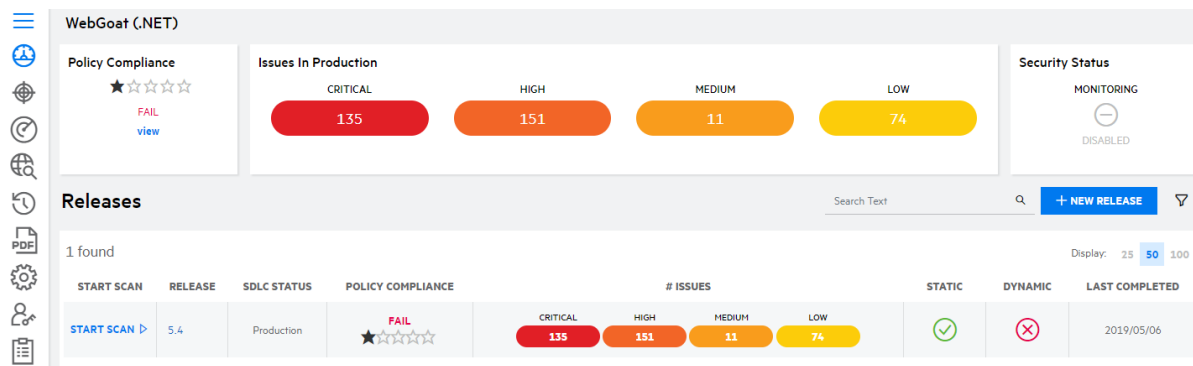
The Application Overview page displays an overview of the application and its releases. It serves as a dashboard for the application, offering a quick yet comprehensive snapshot of the application's production security risk. Here you can filter the application's releases, search for particular releases, create new releases, and start scans.

To view details of an application:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application that you want to view.

The Application Overview page appears. The page shows the following details about an application: production risk and policy compliance, security status, and a list of associated

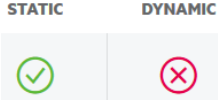
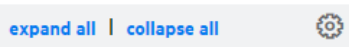
releases (sorted from the latest to the earliest last completed scan date by default).



## Navigating the Application Overview Page

The following table describes how to navigate the Application Overview page.

Task	Action
View the security policy applied to the application	Click <b>View</b> in the Policy Compliance box.
View combined metrics across the application's production releases	The <b>Policy Compliance</b> and <b>Issues in Production</b> boxes display the combined star rating and number of issues (including Application Monitoring issues) across an application's production releases .
View the application's security status	The <b>Security Status</b> box displays the Continuous Application Monitoring status.
Search the application's releases	Enter search word in the text box.
Create a release	Click + <b>New Release</b> .
Start a scan	Click <b>Start Scan</b> next to a release and select the scan type. The button is disabled for releases with the <b>Retired</b> SDLC status.
View additional release details	Click the release name.

Task	Action
View data composing part of a graph	Click a section of the graph.
View the most recent scan status for a release	<p>Hover over the relevant status icon. Click it to directly access the scan status details.</p>  <ul style="list-style-type: none"> <li>Scheduled scans display the scheduled start date.</li> <li>The completion date calculation is based on the start date + SLO of the chosen assessment type + pause time + weekends. In the event that a scan is past the SLO, the expected completion date displays "Long running scan on &lt;release&gt;. Contact us for details."</li> </ul>
Expand or collapse filters	Click  or the arrow next to the filter name.
Hide or display the filter list	Click ▼.
Remove applied filters	Click <b>X</b> or click <b>X Clear Filters</b> .

## Filtering the Application Overview page

By default, the Application Overview page displays all results . You can customize the data displayed by applying filters.

**Note:** A filter only appears in the filter list when the results contain multiple values for that filter.

To filter the Application Overview page:

- Click ▼ to display the filter list if it is not currently displayed.
- Expand the filters you want to apply.
- Select the filter values. The following table describes the Application Overview filters.

Filter	Description	Values
Dynamic Scan	Status of dynamic	Completed, Canceled, In Progress, Not Started



Filter	Description	Values
Status	scans	
Mobile Scan Status	Status of mobile scan	Completed, Canceled, In Progress, Not Started
Pass/Fail	User-defined Pass/Fail rating	Fail, Pass
Release Created Date	Date of release creation	
Scan Type	Type of scan	Static, Dynamic, Mobile, Network, Application Monitoring, Open Source
SDLC status	SDLC status of releases	Development, QA/Test, Production, Retired
Star Rating	5-star rating system	1, 2, 3, 4, 5
Static Scan Status	Status of static scans	Completed, Canceled, In Progress, Not Started

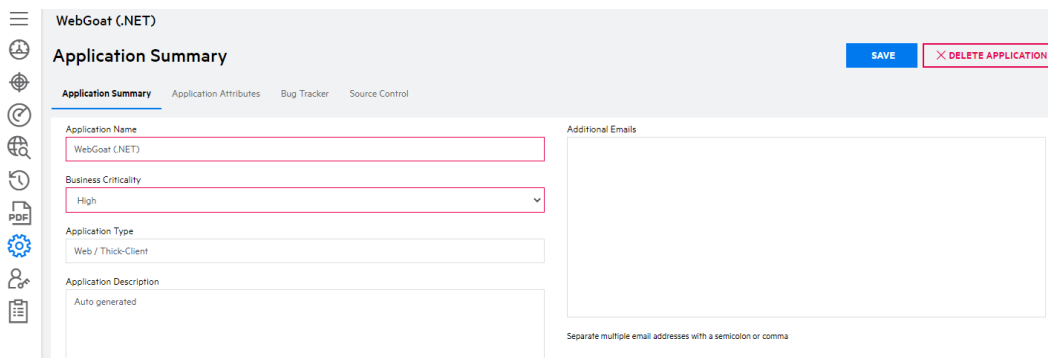
The page automatically refreshes with your filtered results. Applied filters are shown at the top of the page.

## Editing Application Settings

You can edit application settings after the application has been created.

To edit application settings:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application that you want to edit.
3. Click **Settings**.  
The Settings page appears.

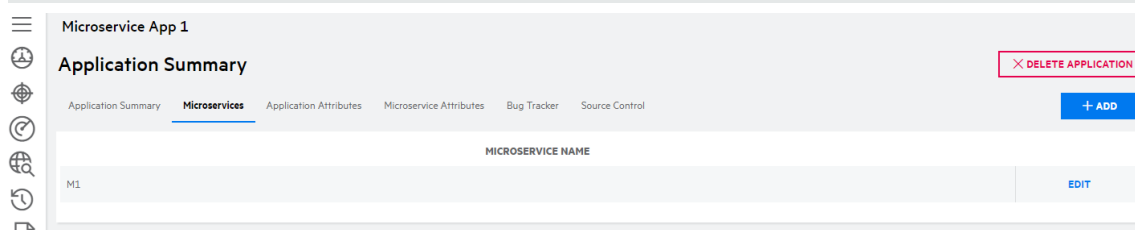


4. Select the tab that corresponds to the application settings you want to edit.
  - The **Application Summary** tab displays application details.

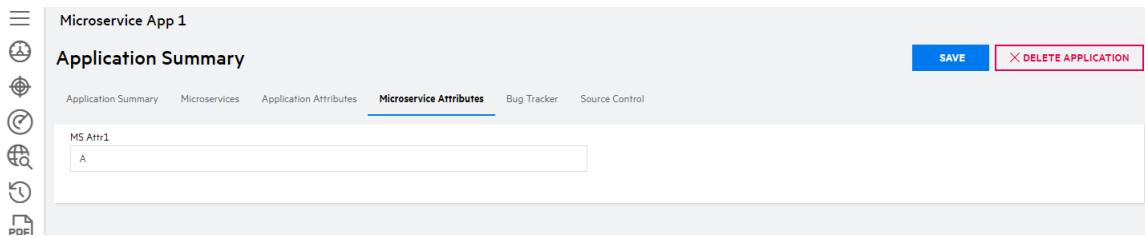
Field	Description
<b>Application Name</b>	Name of your application
<b>Business Criticality</b>	Business Criticality level
<b>Application Type</b>	Application type (not editable for microservice applications)
<b>Application Description</b>	(Optional) Description of the application that will help you manage multiple application
<b>Additional Emails</b>	(Optional) Email addresses that will receive notifications of activity related to the application

- (Microservice applications only) The **Microservices** tab displays existing microservices. You can add, edit, or delete microservices.

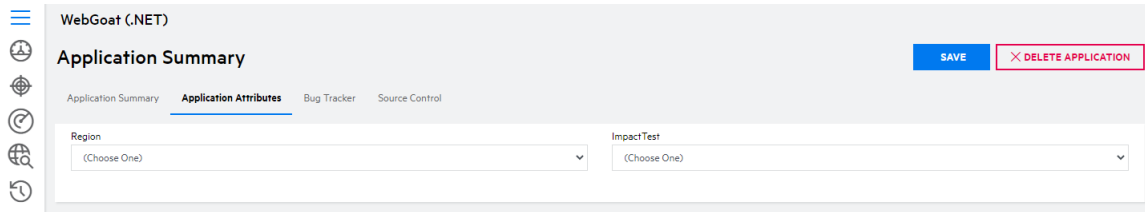
**Note:** You cannot delete a microservice that is tied to a release.



- (Microservice applications only) The **Microservice Attributes** tab displays microservice attributes. You edit microservice attribute values.



- The **Application Attributes** tab displays system attributes as well as custom attributes.



- The **Bug Tracker** tab displays configuration settings for bug tracker integration. For more information, see ["Bug Tracker Integration" on page 384](#).
- The **Source Control** tab displays configuration settings for source control integration. For more information, see ["Source Control Integration" on page 397](#).

5. Edit the application settings as desired.

6. Click **Save**.

The application settings are saved.

## Managing User Assignment to an Application

Users with the **Manage Users** permission can manage user access to an application at the application level.

**Note:** Security Leads have access to all applications and cannot be removed.

To manage user access to an application:

1. Select the **Applications** view.

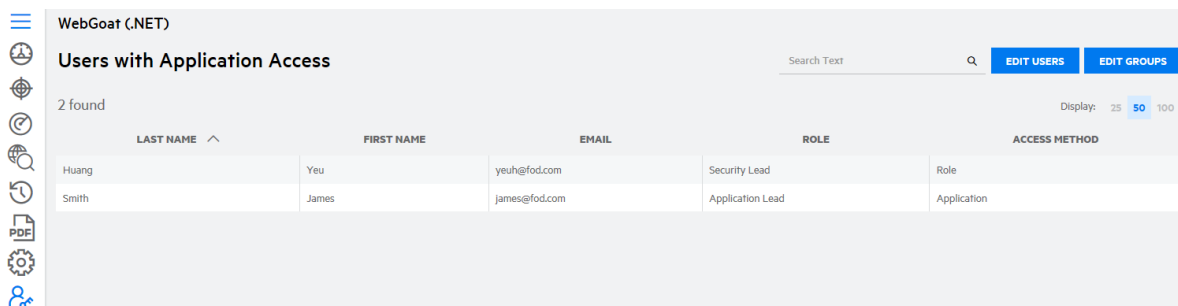
Your Applications page appears.

2. Click the name of application for which you want to edit user access.

The Application Releases page appears.

3. Click **Access**.

The Users with Application Access page appears, displaying the list of users with access to the application.

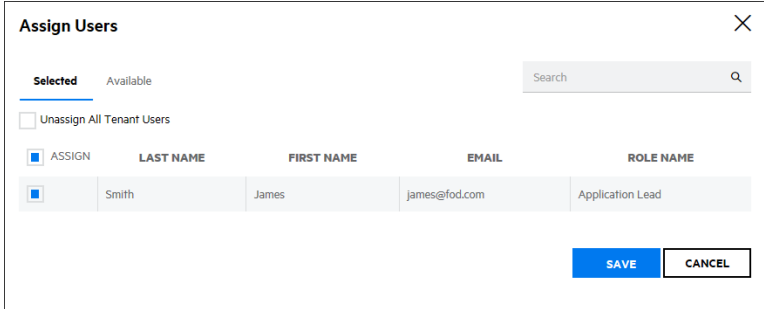


4. Click **Edit Users**.

The Assign Users window appears.

5. You can perform the following tasks:

Task	Procedure
Assign users to application	<p>a. Click <b>Edit Users</b>.</p> <p>The Assign Users window appears.</p> <p>b. Select the <b>Available</b> tab.</p> <div data-bbox="651 926 1409 1234" data-label="Image"> </div> <p>A list of non-Security Lead users that can be assigned to the application appears.</p> <p>c. Perform the following actions to select users:</p> <ul style="list-style-type: none"> <li>◦ Select the check box next to individual users.</li> <li>◦ Select the <b>ASSIGN</b> check box to select displayed users.</li> <li>◦ Select the <b>Assign All Tenant Users</b> check box to select all users.</li> </ul> <p>You can use the search field to filter the application list.</p>
Remove users from application	<p>a. Click <b>Edit Users</b>.</p> <p>The Assign Users window appears.</p> <p>b. Select the <b>Selected</b> tab.</p>

Task	Procedure
	<div data-bbox="652 310 1411 617"></div> <p data-bbox="652 646 1344 716">A list of non-Security Lead users that are assigned to the application appears.</p> <p data-bbox="613 741 1370 968">c. Perform the following actions to remove users:</p> <ul data-bbox="652 793 1370 968" style="list-style-type: none"><li>◦ Clear the check box next to individual users.</li><li>◦ Clear the <b>ASSIGN</b> check box to remove displayed users.</li><li>◦ Select the <b>Unassign All Tenant Users</b> check box to remove all users.</li></ul> <p data-bbox="652 989 1325 1020">You can use the search field to filter the application list.</p>

6. Click **Save**.

The changes to the application's assigned users are saved.

### Related Topics:

To manage user access to applications at the user level, see "[Managing Application Assignment to a User](#)" on page 273.

## Viewing the Application Event Log

Users with the **Manage Applications** permission can view an application's event log. An application's event log logs all event related to the application:

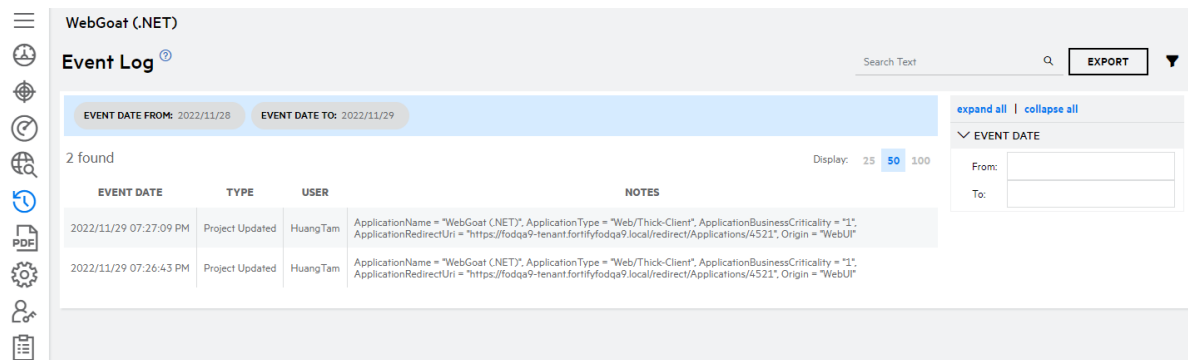
- application creation, updates, and deletion
- release creation, updates, and deletion
- addition and removal of user and group access to the application
- scan initiation, updates, and completion
- entitlement consumption
- report creation, publication, download, and deletion
- FPR downloads

- data exports
- advanced audit settings creation, updates, and deletion


To view an application's event log:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application for which you want to view the event log.
3. Click **Event Log**.

The Event Log page appears.



4. You can perform the following tasks:

Task	Action
Export the event log of the last 13 months	Click <b>Export</b> . A .csv file is saved locally to the folder specified in your browser settings.
Search the event log	Type a keyword or phrase in the search text field and click <b>Enter</b> .
Hide or display the filter list	Click <b>▼</b> .
Expand or collapse filters	Click <b>expand all   collapse all</b>  or the arrow next to the filter name.
Remove applied filters	Click <b>X</b> or click <b>Clear Filters</b> at the top of the page. The filter is set to the last 24 hours by default.

## Related Topics

For information about viewing all events that occur in your portal, see "[Viewing the Administration Event Log](#)" on page 252.

## Deleting an Application

Deleting an application removes all data associated with the application and cannot be undone. Application data is purged from Fortify on Demand after 72 hours. If an application was deleted in error, contact support within 72 hours of deleting the application.

**Note:** If you need to reuse the name of a deleted application, wait 72 hours after deleting the application before creating a new one.

To delete an application:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the application that you want to delete.
3. Click **Settings**.  
The **Application Summary** page appears.

The screenshot shows the 'Application Summary' page for 'WebGoat (.NET)'. The page has a sidebar with navigation icons and a main content area. The main content area has a header with 'WebGoat (.NET)' and 'Application Summary' (with sub-tabs for 'Application Attributes', 'Bug Tracker', and 'Source Control'). There are two buttons at the top right: 'SAVE' and 'X DELETE APPLICATION'. The form fields are: 'Application Name' (text input with 'WebGoat (.NET)'), 'Business Criticality' (dropdown menu with 'High'), 'Application Type' (text input with 'Web / Thick-Client'), and 'Application Description' (text area with 'Auto generated'). There is also an 'Additional Emails' text area. At the bottom, there is a note: 'Separate multiple email addresses with a semicolon or comma'.

4. Click **X Delete Application** .  
A confirmation message appears.
5. Click **Yes** to delete the application.  
You are returned to Your Applications page.

## Managing a Release

You can create, view, and edit releases, depending on your user permissions.

This section covers the following topics:

<a href="#">Creating a Release</a> .....	60
<a href="#">Viewing Release Details</a> .....	61

Overriding the Security Policy of a Release ..... 68  
Editing Release Settings ..... 69  
Deleting a Release ..... 70

## Creating a Release

You can create a new release of an existing application. When creating a new release, you have the option to start fresh or carry over vulnerabilities and other details from a previous release.

To create a new release:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the application for which you want to create a new release.
3. Click **+ New Release**.

The Create Release wizard appears.

**Create a Release** [Close]

### Release Details

Release Name [Text Box]

Release Description [Text Area]

SDLC Status [Dropdown: (Choose One)]

Copy State from Existing Release

**NEXT**

4. In the **Release Details** page, complete the fields as needed. Fields are required, unless otherwise noted:

Field	Description
<b>Release Name</b>	Type the name of your release.
<b>Release Description</b>	(Optional) Type a description that helps describe the release.
<b>SDLC Status</b>	Select the Software Development Life Cycle stage of the release: <b>Development</b> , <b>QA/Test</b> , <b>Production</b> . The <b>Retired</b> option is not available.



Field	Description
<b>Release Name</b>	Type the name of your release.
<b>Microservice</b> (microservice applications only)	Select the microservice that will be linked to the release from the drop down list. A release must be linked to a microservice; a microservice can be linked to multiple releases.
<b>Copy State from Existing Release</b> (enabled by default)	<p>(Optional) Select <b>Copy State from Existing Release</b> to carry over data from a previous release to the new one. The following data is copied: release owner, scan settings for all scan types, star rating, issue counts, and issue details (including issue history, bug tracker links, and attached screenshots).</p> <p><b>Note:</b> Only data from completed and imported scans are copied. Data from other scans, including scan settings from paused and in-progress scans, are not copied.</p>

- If you selected **Copy State from Existing Release**, click **Next**. Otherwise, skip to step 7.

- In the **Copy State from Existing Release** page, select the release that you want to carry over the vulnerabilities and other details from the list.
- Click **Save**.

You are redirected to the Overview page of the new release.

**Note:** If you selected to copy data from a previous release, the copy release data process can slow the screen refresh, so you might not see the Overview page immediately.

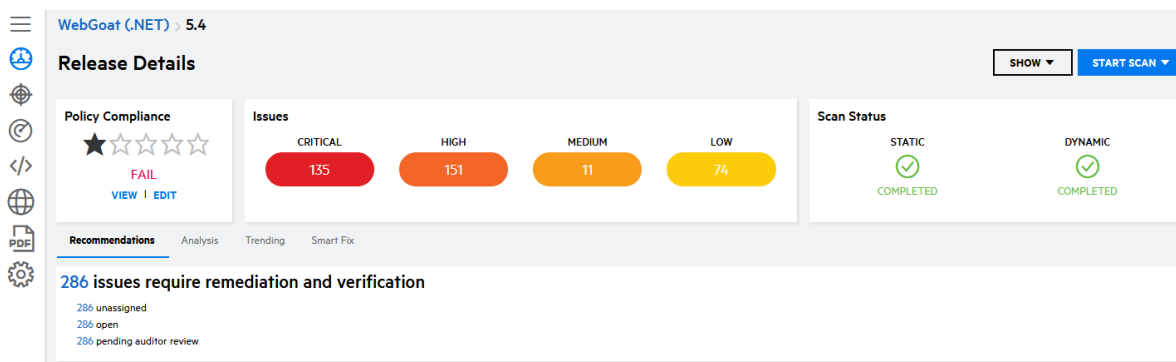
## Viewing Release Details

The Release Overview page displays an overview of the release. It serves as a dashboard for the release, offering a quick yet comprehensive snapshot of the release's security risk. Through a series of

easy-to-read visuals, you can see all the key metrics of your release. Many of the visual elements are clickable so that you can drill down into the data sets displayed.

To view details of a release:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears.
3. Click the name of the release that you want to view.  
The Release Overview page appears.




The top section of the Release Overview page summarizes all scan results for the release. The Policy Compliance box shows the Star Rating and Pass/Fail status. The Issues box shows the number of vulnerabilities at each severity level. The Scan Status box shows the most recent scan statuses for the release.

The tabs display several analyses of the scan results, with links to drill down into issues

## Navigating the Release Overview Page

The following table describes how to navigate the Release Overview page.

Task	Action
Show or hide fixed issues	Click <b>Show... Fixed</b> to switch between showing and hiding Fix Validated issues.
Show or hide suppressed issues	Click <b>Show... Suppressed</b> to switch between showing or hiding Suppressed issues.
Start a scan	Click <b>Start Scan</b> and select the scan type from the list. The button is disabled for releases with SDLC status of <b>Retired</b> .
View the most	Hover over the relevant status icon. Click it to directly access the scan status

Task	Action
recent scan status for the release	<p>details.</p>  <ul style="list-style-type: none"> <li>• Scheduled scans display the scheduled start date.</li> <li>• The completion date calculation is based on the start date + SLO of the chosen assessment type + pause time + weekends. In the event that a scan is past the SLO, the expected completion date displays "Long running scan on &lt;release&gt;. Contact us for details."</li> </ul>
View the security policy applied to the parent application	Click <b>View</b> in the Policy Compliance box.
Override the policy compliance	Click <b>Edit</b> in the Policy Compliance box.
View an analysis of scan results	Select a tab below the overview boxes. For more information, see <a href="#">"Release Overview Graphs" below</a>
View issues filtered by issue severity or scan type	Click the boxes in the Issue and Scan Status boxes.

## Release Overview Graphs

The tabs on the Release Overview page display visual representations of the scan results, with links to drill down into issues

- ["Recommendations" on the next page](#)
- ["Analysis" on page 65](#)
- ["Smart Fix \(static scans\)" on page 66](#)
- ["App Information \(mobile scans\)" on page 67](#)
- ["Reputation \(mobile scans\)" on page 67](#)

**Note:** Showing fixed and suppressed issues increases the vulnerabilities in the count. The updated count is also represented in the vulnerability graphs.

## Recommendations

The **Recommended Issues To Address** section lists why the release is failing the security policy. If specific issues are causing the release to fail, you can drill directly into those issues. If your policy requires a minimum scan frequency, that information is displayed here as well. Releases that are passing and do not have scan frequency requirements do not have this section.

**Recommendations**    Analysis    Smart Fix

---

**Recommended Issues To Address**

286 issues require remediation and verification

- 284 unassigned
- 284 open
- 2 in remediation
- 286 pending auditor review

Application monitoring is required by your security policy for this application

The **Trending** section displays a line graph of the release's vulnerability trends over time, measured in terms of the selected facet. Hover over a data point to view the count and type. Click a label to switch between showing or hiding that data set.



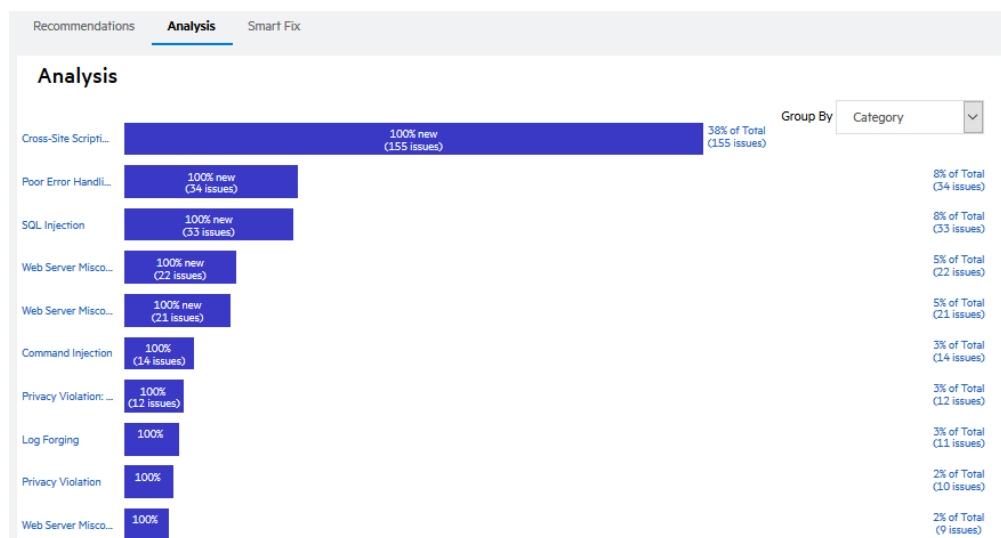
Facet	Description
<b>Auditor Status</b>	Auditor status of issues

Facet	Description
<b>Developer Status</b>	Developer status of issues
<b>Is Assigned</b>	Assignment status of issues: <b>False, True</b>
<b>Issue Status</b>	Issue status: <b>New, Existing, Reopen, and Fixed</b>
<b>Issue Suppressed</b>	Suppression status of issues: <b>False, True</b>
<b>Kingdom</b>	Seven Pernicious Kingdoms classification
<b>Severity</b>	Issue severity: <b>Critical, High, Medium, Low</b>
<b>OWASP 2017</b>	OWASP Top 10 2017 classification
<b>GDPR</b>	GDPR classification from Fortify Software Security Research (SSR)
<b>PCI 3.2</b>	PCI 3.2 classification
<b>FISMA</b>	FISMA classification
<b>Is Closed</b>	Resolution status of issues: <b>False, True</b>
<b>OWASP Mobile Top 10</b>	OWASP Mobile Top 10 classification
<b>Scan Type</b>	Issue scan type: <b>Static, Dynamic, Mobile</b>

## Analysis

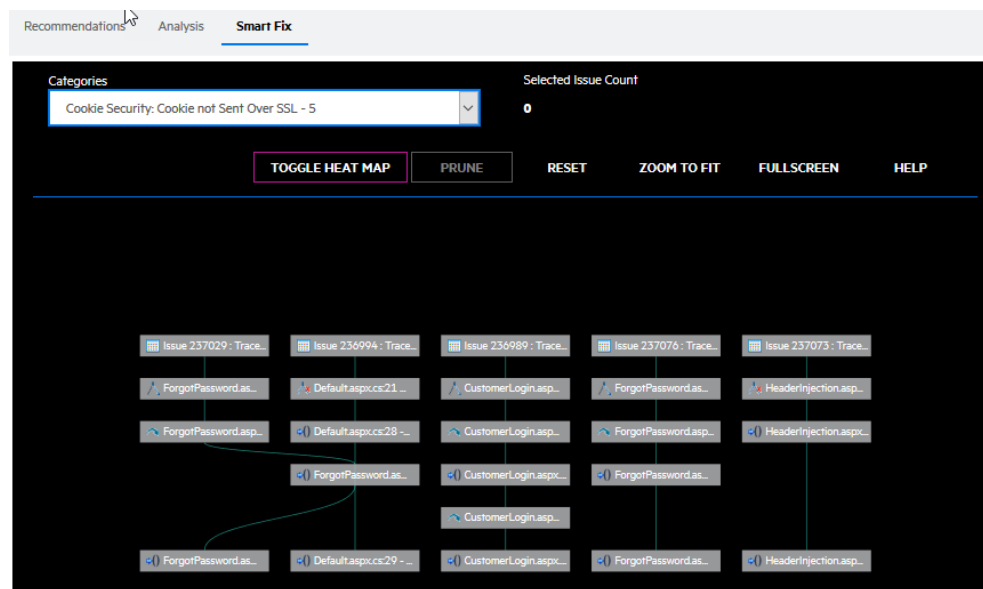
The **Analysis** tab displays a bar graph of the release's vulnerabilities divided into groups. The categories displayed depend on the Aggregation facet selected: **Assignment, Auditor status, Category, Developer Status, Scan Type, and OWASP 13**.

Drill down into a group by clicking any of the bars in the graph. For example, if you click the **Privacy Violation** bar in the **Category** facet, you are redirected to a filtered Issues page displaying privacy violation vulnerabilities.



### Smart Fix (static scans)

The **Smart Fix** tab is available once a static scan has been performed. It displays an analysis trace diagram that visualizes node execution order across static issues in a vulnerability category and provides insight into shared data flows across those issues. This information can help identify optimal fix locations and remediation strategies.



Select a vulnerability category in the **Categories** list to view its analysis trace diagram. You can interact with the diagram in the following ways:

- Scroll up and down to zoom in and out, respectively.
- Click a node to highlight shared paths.
- Click an issue icon to drill down into the issue.
- Manipulate the diagram using the toolbar commands:

- **Toggle Heat Map:** enables / disables highlighting of data flows
- **Prune** (available when a node is selected): narrows the diagram to the combined data flow of the selected issues
- **Reset:** resets the diagram to the default view of the selected issue category
- **Zoom To Fit:** resizes the entire diagram to fit in the display without resetting or pruning
- **Full Screen:** expands the diagram in full screen mode

### App Information (mobile scans)

The **App Information** tab displays the following information about a mobile application's binary file: the platform, application name, identifier (package name), version, file size, minimum OS requirements, and device requirements.

Recommendations	Analysis	Trending	<b>App Information</b>	Reputation
Platform				iOS
Name				iGoat
Identifier				com.swaroop.iGoat
Version				3.0 (1)
File Size (bytes)				11028827
Minimum OS Requirements				9.0
Device Requirements				armv7

### Reputation (mobile scans)

Fortify on Demand's Mobile Reputation service performs a reputation analysis of traffic endpoints discovered while testing a mobile application. The **Reputation** tab displays the analysis results. It lists all identified hosts and whether each is in good standing. Mobile scan results also include dedicated vulnerabilities for identified hosts not in good standing.

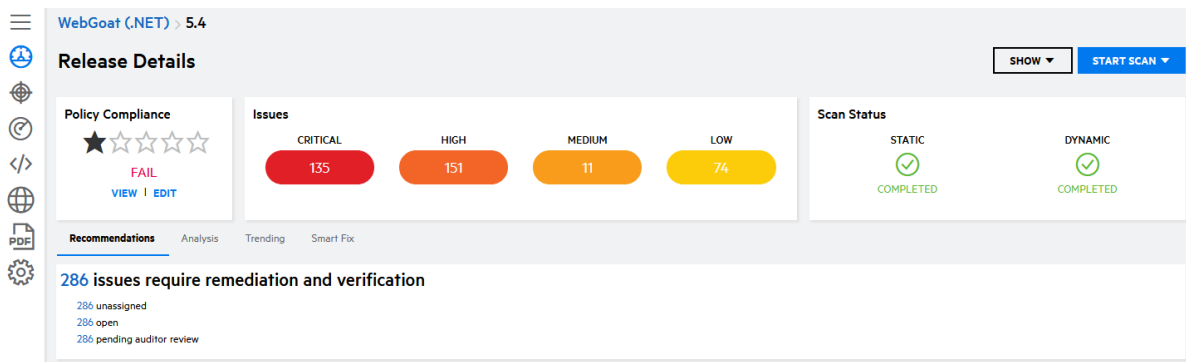
Analysis	Trending	<b>Reputation</b>
HOST NAME	GOOD STANDING	
https://twitter.com/	✓	
https://data.flurry.com/	✓	
http://www.apple.com/	✓	
http://api.twitter.com/	✓	
https://m.facebook.com/	✓	
http://api.linkedin.com/	✓	
http://google.co.uk/	✓	
https://www.linkedin.com/	✓	
https://api.twitter.com/	✓	
http://adlog.flurry.com/	✓	

## Overriding the Security Policy of a Release

Security Leads can manually override the security policy of a release by setting the release as passing or failing. This capability allows you to better reflect real-world exceptions process in the portal without artificially suppressing issues. The justification for the exception is logged in the application's event log. The status of the release automatically reverts to the official security policy on the next scan.

To override the security policy of a release:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application containing the release you want to edit.  
The Application Overview page appears.
3. Click the name of the release for which you want to override the security policy.  
The Release Overview page appears.



4. Click **EDIT** in the Policy Compliance box.  
The Compliance Override modal window appears.
5. Type the justification for changing the policy compliance results in the field.



6. Click **Set to Pass** or **Set to Fail**.  
You are returned to the Release Overview page. Your policy override is displayed in the Policy Compliance box.



## Related Topics:

- For information on Star Ratings, see ["Five-Star Assessment Rating" on page 20](#).
- For information on managing security policies, see ["Policy Management" on page 283](#).

## Editing Release Settings

You can edit release settings after a release has been created.

To edit the release settings:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears, displaying a list of your releases.
3. Select the release that you want to edit.
4. Click **Settings**.

The Release Summary page appears.

The screenshot shows the 'Release Summary' page for 'WebGoat (.NET) 5.4'. The page has a sidebar with navigation icons and a main content area. The main content area contains the following fields:

- Release Name:** A text input field containing '5.4'.
- SDLC Status:** A dropdown menu with 'Production' selected.
- Owner:** A dropdown menu with '(Choose One)' selected.
- Release Description:** A text area containing '5.4'.

At the top right of the main content area, there are two buttons: a blue 'SAVE' button and a red 'DELETE RELEASE' button.

5. Edit the Release Summary page as desired. Fields are required unless noted otherwise.

Field	Description
<b>Release Name</b>	Name of the release
<b>Microservice</b>	(Microservice applications only) Name of the microservice linked to the release
<b>SDLC Status</b>	Software Development Lifecycle stage of the release
<b>Owner</b>	Owner of the release who receives email notifications of scan status updates to the release
<b>Release Description</b>	(Optional) Description of the release that helps describe the release.

6. Click **Save** to save your changes.

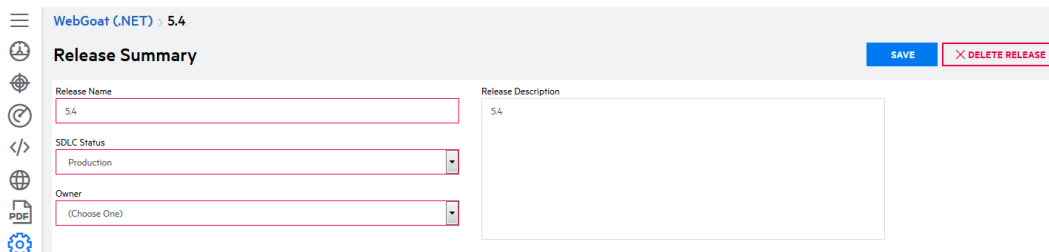
## Deleting a Release

Users with the **Create Applications** permission can delete a release. Deleting a release removes all data associated with the release and cannot be undone. Release data is purged from Fortify on Demand after 72 hours. If a release was deleted in error, contact support within 72 hours of deleting the release.

**Note:** If you need to reuse the name of a deleted release, wait 72 hours after deleting the release before creating a new one.

To delete a release:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears, displaying a list of your releases.
3. Click the release that you want to delete.
4. Click **Settings**.
5. Click **x Delete Release**.



The screenshot shows the 'Release Summary' page for 'WebGoat (.NET) > 5.4'. The page has a sidebar with navigation icons. The main content area has a 'Release Name' input field containing '5.4', an 'SDLC Status' dropdown menu set to 'Production', and an 'Owner' dropdown menu set to '(Choose One)'. To the right is a 'Release Description' text area containing '5.4'. At the top right of the form, there are two buttons: 'SAVE' and 'X DELETE RELEASE'.

6. Click **Yes**.  
You are returned to the Release Overview page.

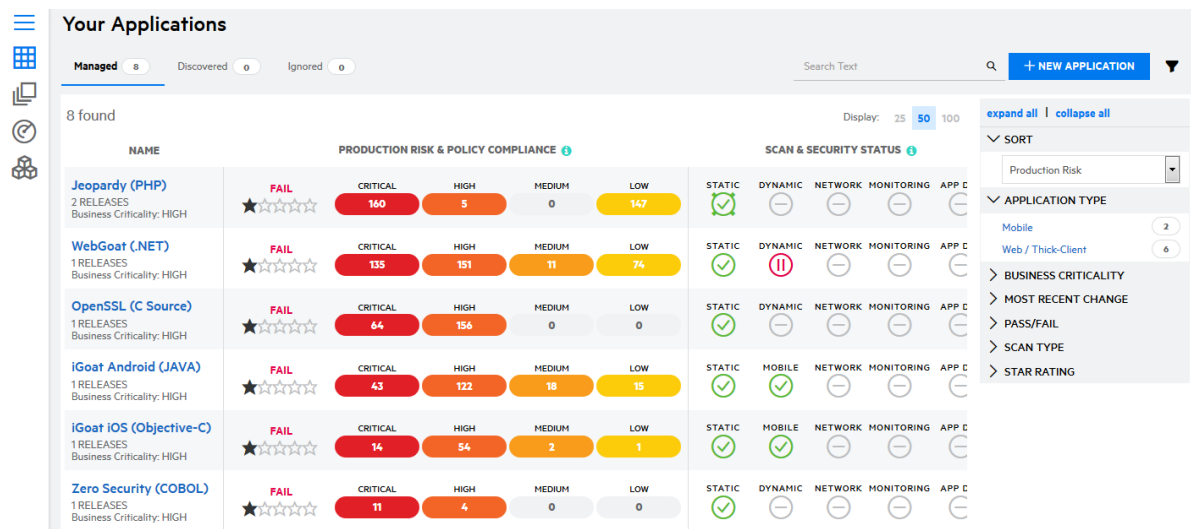
## Viewing Applications in the Tenant

You can review the security status of multiple applications simultaneously. Your Applications page is the default landing page after logging in to Fortify on Demand. It displays a high-level overview of your applications in Fortify on Demand, with a focus on the risk and policy compliance of production releases.

To view Your Applications page:


1. Select the **Applications** view.  
Your Applications page appears. The grid shows the following details about each application: application name, number of releases, business criticality, the combined star rating and number of issues across production releases, the most recent scan status across all releases, and the most

recent risk-relevant change.

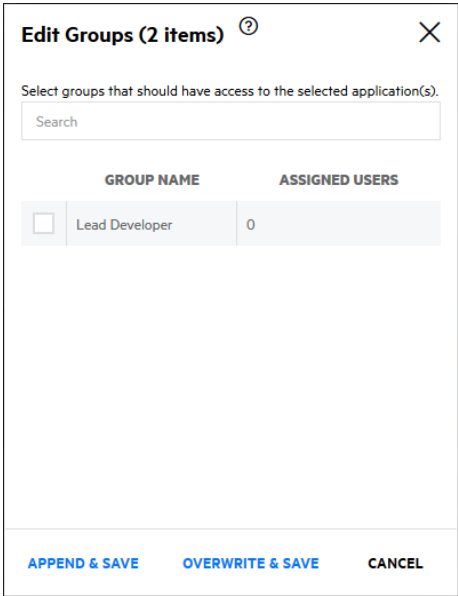



## Navigating Your Applications Page

The following table describes how to navigate Your Applications page.

Task	Action
Create an application	Click <b>+New Application</b> .
Search the application list	Type a keyword or phrase in the search text box and click <b>Enter</b> . To remove the search results, remove the text from the search box and click <b>Enter</b> or remove the applied filter.  For information on using the search text box, see <a href="#">"Searching Applications and Releases" on page 80</a> .
Hide or display filter lists	Click <b>▼</b> .
Expand or collapse filters	Click <b>expand all   collapse all</b>  or the arrow next to the filter name.
Remove applied filters	Click <b>X</b> or click <b>Clear Filters</b> at the top of the page.
Filter applications by microservice designation	Select the desired tab.

Task	Action
<p>Edit application attributes for multiple applications</p>	<div data-bbox="834 279 1500 338" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 10px; margin-right: 10px;">All 12</span> <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 10px; margin-right: 10px;">Microservice 0</span> <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 10px;">Non-Microservice 12</span> </div> <ol style="list-style-type: none"> <li>1. Select the check box next to individual applications or click <b>select all</b> to select all applications on the page.</li> <li>2. Click <b>Edit Attributes</b>.          The Edit Attribute window opens.         <div data-bbox="889 630 1411 1142" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span><b>Edit Attributes (2 items)</b></span> <span>✕</span> </div> <div style="margin-top: 10px;"> <p>Business Criticality  <input type="text" value="(Choose One)"/></p> <p>Region  <input type="text" value="(Choose One)"/></p> <p>ImpactTest  <input type="text" value="(Choose One)"/></p> </div> <div style="display: flex; justify-content: flex-end; gap: 20px; margin-top: 10px;"> <span>SAVE</span> <span>CANCEL</span> </div> </div> </li> <li>3. Update the fields as needed.</li> <li>4. Click <b>Save</b>.</li> </ol> <p>For more information on application attributes, see <a href="#">"Creating an Application" on page 43</a></p>
<p>Edit user groups for multiple applications</p>	<ol style="list-style-type: none"> <li>1. Select the check box next to individual applications or click <b>select all</b> to select all applications on the page.</li> <li>2. Click <b>Edit Groups</b>.          The Edit Groups window opens.</li> </ol>

Task	Action
	 <p>3. Select the groups that will be assigned to the applications.</p> <p>4. Click <b>Append &amp; Save</b> to add the selected groups to the existing assigned groups, or click <b>Overwrite &amp; Save</b> to replace the existing assigned groups with the selected groups (if no user groups are selected, all existing assigned groups are removed).</p> <p><b>Note:</b> Users must have both <b>Manage Applications</b> and <b>All Application Access</b> permissions to use <b>Overwrite &amp; Save</b>.</p> <p>For more information on groups, see <a href="#">"Groups" on page 276</a>.</p>
View details of an application	Click the application name.
View the security policy applied to an application	Click the star rating.
View combined metrics across an application's production releases	The <b>Production Risk &amp; Policy Compliance</b> column displays the combined star rating and number of issues (including Application

Task	Action
	Monitoring issues) across an application's production releases.
View the most recent scan status across an application's releases	<p>Hover over the relevant status icon. Click it to directly access the scan status details.</p>  <ul style="list-style-type: none"> <li>• Scheduled scans display the scheduled start date.</li> <li>• The expected completion date is calculated based on the scan start date + SLO of the chosen assessment type + pause time + weekends. In the event that a scan is past the SLO, the expected completion date displays "Long running scan. Contact us for details."</li> </ul>
View the most recent risk-relevant change for an application.	<p>The <b>Most Recent Change</b> column displays the most recent change from the following list:</p> <ul style="list-style-type: none"> <li>• Risk profile updated</li> <li>• Release created</li> <li>• Release deployed to production</li> <li>• New Application Monitoring vulnerabilities detected</li> <li>• New dynamic vulnerabilities detected</li> <li>• New static vulnerabilities detected</li> <li>• New mobile vulnerabilities detected</li> <li>• Business criticality updated</li> <li>• Release passing security policy</li> <li>• Release failing security policy</li> </ul>

## Filtering Your Applications Page

By default, Your Applications page displays all applications, which are sorted from top to bottom based on the following criteria:

- the group that the application belongs to, sorted by descending priority:
  - production: application with one or more production releases (sorted by Pass/Fail status, where failing > unassessed > passing)
  - pre-production: application with one or more dev/QA releases
  - retired: application with no production, dev, or QA releases
- within each group (production, pre-production, retired), the applications are sorted by business criticality (from high to low), followed by the number of issues by severity

You can limit the applications displayed as well as change the sort order by applying filters.

To filter Your Applications page:

1. Click ▼ to display the filter list if it is not currently displayed.
2. If desired, select the sort order from the **Sort** list. The values are: **Production Risk** (default), **Most Recent Change**, **Application Name (A to Z)**, and **Application Name (Z to A)**.
3. Expand the filters that you want to apply. The following table describes the application filters.

**Note:** A filter only appears in the filter list when the results contain multiple values for that filter.

Filter	Description	Values
Application Monitoring	Application Monitoring status of an application	Enabled (No issues), Enabled (Issues found), Not Enabled
Application Type	The application type, selected during the application creation process	Mobile, Web/Thick-Client
Business Criticality	Business Criticality of an application	High, Medium, Low
Has Microservices	Whether the application has microservices	false, true
Dynamic Scan Status	Status of dynamic scans	Scheduled, In Progress, Completed, Canceled, Waiting
Mobile Scan	Status of mobile	Scheduled, In Progress, Completed, Canceled, Waiting

Filter	Description	Values
Status	scans	
Most Recent Change	Category of the most recent change detected for an application	New Monitoring Vulnerabilities Detected, Release Passing Security Policy, Business Criticality Updated, Release Created, New Dynamic Vulnerabilities Detected, Release Failing Security Policy
Pass/Fail	User-defined Pass/Fail rating	Fail, Pass, Unassessed
Scan Type	Scan type	Static, Dynamic, Mobile, Open Source
Star Rating	5-star rating system	1, 2, 3, 4, 5
Static Scan Status	Status of static scans	In Progress, Completed, Canceled, Waiting

4. Select your desired filter values.

Your Applications page automatically refreshes with your filtered results. Applied filters are shown at the top of the page.

## Viewing Releases in the Tenant

In addition to reviewing multiple applications at once, you can also review the details of individual releases across multiple applications simultaneously. Your Releases page displays a high-level overview of your releases in Fortify on Demand.

To view Your Releases page:

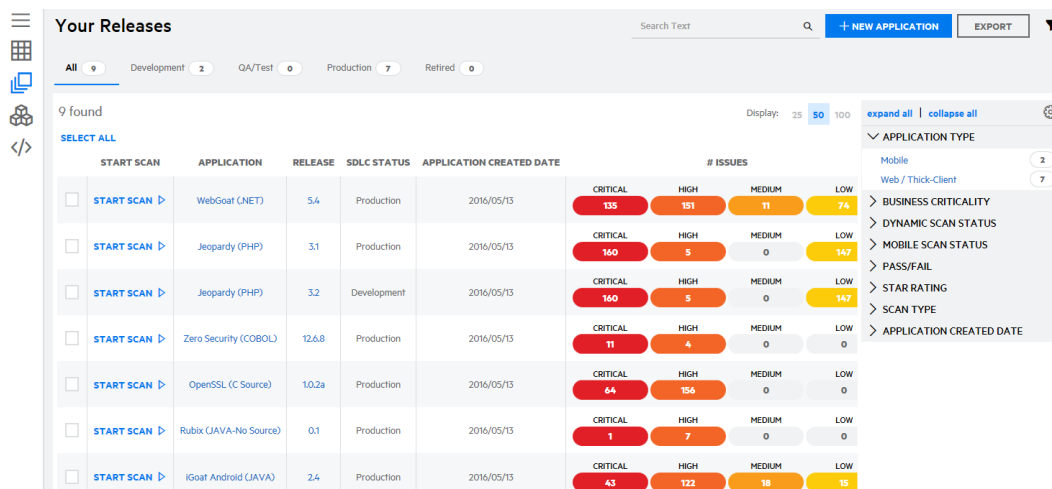
1. Select the **Applications** view.

Your Applications page appears.

2. Click **Your Releases**.

Your Releases page appears. The grid shows the following details about each release: application name, associated release name, number of issues found in the release, star rating, and current scan statuses.





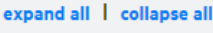


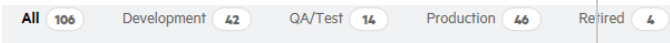



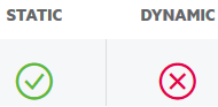
3. Select the tabs to filter releases by their SDLC status. The default SDLC status is **All**, which displays all of your releases. You can change the default SDLC status in your account settings.

## Navigating Your Releases Page

The following table describes how to navigate Your Releases page.

Task	Action
Create an application	Click <b>+New Application</b> .
Search the release list	Type a keyword or phrase in the search text box and click <b>Enter</b> . To remove the search results, remove the text from the search box and click <b>Enter</b> or remove the applied filter. For information, see " <a href="#">Searching Applications and Releases</a> " on page 80.
Export data as a .csv file	Click <b>Export</b> . A .csv file containing detailed information on all vulnerabilities is saved locally to a folder specified in your browser settings.  <b>Note:</b> The Export functionalities in the Tenant Dashboard, Your Releases, and Release Issues pages outputs the same column fields. Currently applied filters are also applied to the export.

Task	Action
Change the grid columns	<ol style="list-style-type: none"> <li>1. Click .</li> <li>2. Use the check boxes to make your selections.</li> <li>3. Click <b>Save</b>.</li> </ol>
Hide or display the filter list	Click  .
Expand or collapse filters	Click      or the arrow next to the filter name.
Remove applied filters	Click <b>X</b> or click <b>Clear Filters</b> at the top of the page.
Filter releases by SDLC status	<p>Select a tab corresponding to an SDLC status. The selected SDLC status is preserved when moving between views.</p> 
Sort the release list by column	Click a column header. The arrow next to the header indicates the sort order of the data. To reverse the order, click the header again.
Edit release attributes for multiple releases	<ol style="list-style-type: none"> <li>1. Select the check box next to individual releases or click <b>select all</b> to select all releases on the page.</li> <li>2. Click <b>Edit Attributes</b>. The Edit Attribute window opens. </li> <li>3. Update the fields as needed.</li> <li>4. Click <b>Save</b>.</li> </ol> <p>For more information on release attributes, see <a href="#">"Creating a Release" on page 60</a></p>
Start a scan	Click <b>Start Scan</b> and select the scan type.

Task	Action
View additional details of an application or release	Click an application or release name.
View the most recent scan status for a release	<p>Hover over a status icon. Click it to directly access the scan status details.</p>  <ul style="list-style-type: none"> <li>Scheduled scans display the scheduled start date.</li> <li>The completion date calculation is based on the start date + SLO of the chosen assessment type + pause time + weekends. In the event that a scan is past the SLO, the expected completion date displays "Long running scan on &lt;release&gt;. Contact us for details."</li> </ul>
View the security policy applied to a release's parent application	Click a star rating.

## Filtering Your Releases Page

By default, Your Releases page displays all of your releases. You can limit the releases displayed by applying filters.

To filter Your Releases page:

- Click ▼ to display the filter list if it is not currently displayed.
- Expand the filters you want to apply. The following table describes the release filters.

**Note:** A filter only appears in the filter list when releases have multiple values for that filter.

Filter	Definition	Values
Application Created Date	Date when the application was created.	< 7 days, < 30 days, < 90 days, < 180 days
Application Type	The application type, selected during	Mobile, Web/Thick-Client

Filter	Definition	Values
	the application creation process	
Business Criticality	Criticality of the applications	High, Medium, Low
Dynamic Scan Status	Status of dynamic scans	Not Started, Canceled, Completed, In Progress, Waiting
MicroserviceName	Microservice names	User-defined
Mobile Scan Status	Status of mobile scans	Not Started, Canceled, Completed, In Progress, Waiting
Pass/Fail	User-defined Pass/Fail rating	Fail, Pass
Scan Type	Scan type	Static, Dynamic, Mobile
SDLC Status	SDLC status of releases	Production, QA/Testm Development, Retired
Star Rating	5-star rating system	1, 2, 3, 4, 5
Static Scan Status	Status of static scans	In Progress, Completed, Canceled, Waiting

3. Select your desired filter values.

Your Releases page automatically refreshes with your filtered results. Applied filters are shown at the top of the page.

## Searching Applications and Releases

In addition to the top-level Search box that is available in the portal toolbar, you can also use the **Search Text** box available on each grid to search for application names, release names, keywords, and URLs within the display context of the grid.

### Searching Text

To search for an application or release in a grid:

1. Type the string that you want to search for in the **Search Text** box.

You do not need to type the entire string in the box. For example, if you are searching for an application named *Test App 1*:

- If you type **Test** in the box, your search results **will** include *Test App 1*.
  - If you type **Tes** in the box, your search results **will not** include *Test App 1*.
  - If you type **Tes\*** in the box, your search results **will** include *Test App 1*.
2. Click **Enter**.  
The page refreshes with your search results.
  3. Click the name of the desired application or release. The page refreshes with the selected application or release page and clears the search box.

## Removing the Search Results

To remove the applied search filter, perform one of the following:

- Remove the search string from the search box.
- Click the browser **Back** arrow.

## Creating Deep Links

Fortify on Demand supports deep linking to applications, releases, scans, and issues.

To create deep links, use the following path formats:

- Applications: `https://<fod_domain>/redirect/Applications/<application_id>`
- Releases: `https://<fod_domain>/redirect/Releases/<release_id>`
- Scans: `https://<fod_domain>/redirect/Scans/<scan_id>`
- Issues: `https://<fod_domain>.com/redirect/Issues/<issue_id>`

**Note:** The top of the issue details panel displays the issue ID.

`236127` <http://zero.webappsecurity.com:80/forc>

where `<fod_domain>` is the Fortify on Demand data center domain:

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

# Chapter 4: Running Assessments

Fortify on Demand offers comprehensive security testing across three assessment types: static, dynamic, and mobile.

This section contains the following topics:

- [Static Assessments](#) ..... 82
- [Dynamic Assessments](#) ..... 114
- [Mobile Assessments](#) ..... 137
- [Open Source Software Composition Analysis](#) ..... 148
- [Entitlement Consumption](#) ..... 154
- [Managing Scans](#) ..... 154

## Static Assessments

A static assessment analyzes an application’s source code, bytecode, or binaries for possible security vulnerabilities. Static assessments are powered by Micro Focus Fortify Static Code Analyzer. Static testing using Fortify Static Code Analyzer involves:

1. Translating the source code into an intermediate translated format
2. Analyzing the translated code

This section contains the following topics:

- [Supported Languages](#) ..... 83
- [Supported Compilers](#) ..... 85
- [Supported Libraries, Frameworks, and Technologies](#) ..... 86
- [Preparing Static Assessment Files](#) ..... 89
- [Configuring a Static Scan](#) ..... 105
- [Submitting a Static Assessment](#) ..... 109
- [Static Assessment Payload Validation](#) ..... 112

## Supported Languages

Micro Focus Fortify Static Code Analyzer supports the programming languages listed in the following table.

Language / Framework	Versions
.NET	5.0, 6.0
.NET Framework	2.0–4.8
.NET Core	2.0–3.1
ABAP/BSP	6  <b>Note:</b> Fortify ABAP Extractor is supported on a system running SAP release 7.02, SP level 0006.
ActionScript	3.0
Apex	36
C#	5, 6, 7, 8, 9, 10
C/C++	C11, C++11, C++14, C++17, C++20 (see <a href="#">"Supported Compilers" on page 85</a> )
Classic ASP (with VBScript)	2.0, 3.0
COBOL	IBM Enterprise COBOL for z/OS 6.1 (and earlier) with CICS, IMS, DB2, and IBM MQ  Micro Focus Visual COBOL 6.0  <b>Note:</b> COBOL translation requires that Microsoft Visual C++ 2017 Redistributable (x86) be installed on the system. This is not a requirement for Legacy COBOL Translation.
ColdFusion	8, 9, 10
Docker (Dockerfiles)	any
Go	1.12, 1.13, 1.14, 1.15, 1.16, 1.17

Language / Framework	Versions
	<p><b>Note:</b> Fortify Static Code Analyzer supports scanning Go code on Windows and Linux.</p>
HCL	<p>2.0</p> <p><b>Note:</b> HCL language support is specific to Terraform and supported cloud provider Infrastructure as Code (IaC) configurations.</p>
HTML	5 and earlier
Java (including Android)	7, 8, 9, 10, 11, 12, 13, 14, 17
JavaScript	ECMAScript 2015–2021
JSON	ECMA-404
JSP	1.2, 2.1
Kotlin	1.3.50, 1.4.20, 1.5.30
MXML (Flex)	4
Objective-C/C++	2.0 (see <a href="#">"Supported Compilers" on the next page</a> )
PHP	7.3, 7.4, 8.0
PL/SQL	8.1.6
Python	2.6, 2.7, 3.x (3.9 and earlier)
Ruby	1.9.3
Scala	<p>2.11, 2.12, 2.13</p> <p><b>Note:</b> Analyzing Scala code requires the Scala Fortify compiler plugin, which is available in the Maven Central Repository.</p>
Swift	5 (see <a href="#">"Supported Compilers" on the next page</a> for supported swiftc versions)
T-SQL	SQL Server 2005, 2008, 2012



Language / Framework	Versions
TypeScript	2.8, 3.x, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5
VBScript	2.0, 5.0
Visual Basic (VB.NET)	11, 14, 15.x, 16.0
Visual Basic	6.0
XML	1.0
YAML	1.2

## Supported Compilers

Micro Focus Fortify Static Code Analyzer supports the compilers listed in the following table.

Compiler	Versions	Operating Systems
gcc	GNU gcc 4.9, 5.x	Windows, Linux, macOS, AIX, Solaris
	GNU gcc 10.2.1	Windows, Linux, macOS
g++	GNU g++ 4.9, 5.x	Windows, Linux, macOS, AIX, Solaris
	GNU g++ 10.2.1	Windows, Linux, macOS
OpenJDK javac	9, 10, 11, 12, 13, 14, 17	Windows, Linux, macOS
	9, 10, 11, 12, 13	AIX, Solaris
Oracle javac	7, 8, 9	Windows, Linux, macOS
cl (MSVC)	2015, 2017, 2019, 2022	Windows
Clang	12.0.5, 13.0.0, 13.1.6 <sup>1</sup>	macOS
Swiftc	5.4, 5.4.2, 5.5, 5.5.1, 5.5.2, 5.6 <sup>1</sup>	macOS

<sup>1</sup>Fortify Static Code Analyzer supports applications built in the following Xcode versions: 12.5, 12.5.1, 13, 13.1, 13.2, 13.2.1, 13.3, 13.3.1.

## Supported Libraries, Frameworks, and Technologies

Micro Focus Fortify Static Code Analyzer supports the libraries, frameworks, and technologies listed in this section with dedicated Fortify Secure Coding Rulepacks and vulnerability coverage beyond core supported languages.

### Java

Adobe Flex Blaze DS	Apache Spring Security (Acegi)	IBM MQ	OpenCSV	Spring Data JPA
Ajanta	Apache Struts	IBM WebSphere	Oracle Application Development Framework (ADF)	Spring Data MongoDB
Amazon Web Services (AWS) SDK	Apache Tapestry	Jackson	Oracle BC4J	Spring Data Redis
Apache Axiom	Apache Tomcat	Java Annotations	Oracle JDBC	Spring HATEOAS
Apache Axis	Apache Torque	Java Excel API	Oracle OA Framework	Spring JMS
Apache Beehive NetUI	Apache Util	JavaMail	Oracle tcDataSet	Spring JMX
Apache Catalina	Apache Velocity	JAX-RS	Oracle XML Developer Kit (XDK)	Spring Messaging
Apache Cocoon	Apache Wicket	JAXB	OWASP Enterprise Security API (ESAPI)	Spring Security
Apache Commons	Apache Xalan	Jaxen	OWASP HTML Sanitizer	Spring Webflow
Apache ECS	Apache Xerces	JBoss	OWASP Java Encoder	Spring WebSockets
Apache Hadoop	ATG Dynamo	JDesktop	Plexus Archiver	Spring WS
Apache HttpComponents	Azure SDK	JDOM	Realm	Stripes
Apache Jasper	Castor	Jetty	Restlet	Sun JavaServer Faces (JSF)
Apache Log4j	Display Tag	JGroups	SAP Web Dynpro	Tungsten
Apache Lucene	Dom4j	json-simple	Saxon	Weblogic
Apache MyFaces	GDS AntiXSS	JTidy Servlet	SnakeYAML	WebSocket
Apache OGNL	Google Android	JXTA	Spring and Spring MVC	XStream
Apache ORO	Google Cloud Platform	JYaml	Spring Boot	YamlBeans
Apache POI	Google Web Toolkit	Liferay Portal	Spring Data Commons	ZeroTurnaround ZIP
Apache POI	Gson	MongoDB		Zip4J
Apache SLF4J	Hibernate	Mozilla Rhino		
Apache Slide	iBatis	MyBatis		
		Netscape LDAP API		

### Scala

Akka HTTP	Scala Slick
Scala Play	

## .NET

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

## C

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

## C++

Boost Smart Pointers	STL
MFC	WMI

## SQL

Oracle ModPLSQL

## PHP

ADODB	PHP Debug	PHP Mcrypt	PHP OpenSSL	PHP Smarty
Advanced PHP Debugging	PHP DOM	PHP Mhash	PHP PostgreSQL	PHP XML
CakePHP	PHP Extension	PHP Mysql	PHP Reflection	PHP XMLReader
	PHP Hash	PHP OCI8	PHP SimpleXML	PHP Zend

## JavaScript/TypeScript/HTML5

Angular	iOS JavaScript Bridge	Node.js Azure Storage	React Router	Underscore.js
Express JS	jQuery	Node.js Core	SAPUI5/OpenUI5	
Helmet	JS-YAML	React	Sequelize	

## Python

_mysql	Django	memcache-client	pylibmc	six
aiopg	httplib2	MySQLdb	PyMongo	Twisted Mail
Amazon Web Services (AWS) Lambda	Jinja2	psycopg2	PyYAML	urllib3
Azure Functions	libxml2	pycrypto	requests	WebKit
Graphene	lxml	pycurl	simplejson	

## Ruby

MySQL	SQLite	Thor
pg	Rack	

## Objective-C

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

## Swift

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

## COBOL

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

## Go

GORM  
logrus

## Configuration

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

## Universal

Regular Expression (Regex)

## Preparing Static Assessment Files

The first step in a static assessment is to prepare your application's source code and/or compiled files for scanning. To prevent rejection of the static assessment and get comprehensive and accurate scan results, prepare the files according to the instructions provided for the programming language or technology stack of the application.

### Related Topics:

For information on preparing files for open source software composition analysis, see ["Preparing Files for Open Source Scanning" on page 149](#).

This section contains the following topics:

<a href="#">File Requirements for Static Assessments</a>	90
<a href="#">Fortify ScanCentral SAST</a>	91
<a href="#">Preparing .NET Application Files</a>	91
<a href="#">Preparing Java Application Files</a>	93
<a href="#">Preparing JavaScript Technology/HTML/XML Files</a>	95

Preparing Kotlin Application Files .....	95
Preparing ABAP (SAP) Application Files .....	95
Preparing C and C++ Application Files .....	98
Preparing Classic ASP, VBScript, and Visual Basic Application Files .....	99
Preparing COBOL Application Files .....	99
Preparing ColdFusion Markup Language (CFML) Application Files .....	100
Preparing Dockerfiles and Infrastructure as Code (IaC) Files .....	100
Preparing Go Application Files .....	100
Preparing PHP Application Files .....	101
Preparing Python Application Files .....	102
Preparing Ruby Application Files .....	103
Preparing Salesforce (Apex and Visualforce) Application Files .....	103
Preparing Scala Application Files .....	104
Preparing Android Application Files (Source Code) .....	105
Preparing iOS Application Files (Source Code) .....	105

## File Requirements for Static Assessments

Applications submitted for static assessments must meet the following file requirements:

- Application files must be packaged in a non-password protected zip file. Other file extensions such as tarball, rar, tar, and 7z, are not supported.
- The maximum payload size is 5 GB for a monolithic application and 100 MB for a microservice application; free trials are restricted to a maximum payload size of 150 MB.
- The payload must contain at least one of the following file types:
  - Binary/compiled files  
Binary/compiled files are the debug compiled executable files produced by compiling your application's source code files and the executable library and resource files produced by third party dependencies that are used by your application.
  - Source code files  
Source code files are the text files compiled to produce the application files.
- Application files must meet specific requirements for the technology stack under which the application is submitted. Make sure to prepare the application files as instructed for that technology stack.
- In general, code submitted must be fully deployable. For example, this means that a JAR file must have executable code.

## Fortify ScanCentral SAST

Fortify offers a stand-alone Micro Focus Fortify ScanCentral SAST client for automatically packaging all necessary dependencies and source code required for a static scan. The following languages are supported for packaging: .NET and .NET Core (MSBuild projects), Go, Java (Gradle and Maven projects), PHP, and Python.

The latest version of the Fortify ScanCentral SAST client is available from the Tools page in the portal. Installation instructions are available in the README.txt file stored in the zip file.

For more information about using the Fortify ScanCentral SAST client, see the following links at [Fortify Software Security Center Documentation](#):

- [Fortify ScanCentral SAST Client and Sensor Software Requirements](#)

**Note:** If you need to run Java 8 on your build machine, contact support to request version 21.1.5 of the Fortify ScanCentral SAST client. This version is specific to Fortify on Demand and is compatible with Java 8. It also supports packaging of the files required for Debricked scanning.

- [Fortify ScanCentral SAST Supported Build Tools](#) (see the "Build Tools" section)
- [Fortify ScanCentral SAST Command-Line Options](#) (see the "Package Command" section)

**Note:** The stand-alone Fortify ScanCentral SAST client is a component of the on-premises Fortify ScanCentral SAST software and is used to package code to send to a Controller for scanning. The Fortify on Demand only uses the packaging feature of the Fortify ScanCentral SAST client.

## Preparing .NET Application Files

For .NET implementations (.NET, .NET Core, .NET Framework, and Xamarin), use one of the following methods to prepare your application files:

- ["Automated Code Packaging with Fortify ScanCentral SAST \(Recommended\)" below](#)
- ["Code Packaging with IDE Tools" on the next page](#)
- ["Manual Code Packaging" on the next page](#)

**Important!** Static scans of .NET applications use source mode scanning by default. Fortify strongly recommends providing source code, as source mode scanning produces more accurate and comprehensive scan results. In addition, as the scanning process can result in false positives, auditors use the source code to manually review issues. If source mode scanning is not an option, contact support to enable mixed mode (binary and source code) scanning.

## Automated Code Packaging with Fortify ScanCentral SAST (Recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your MSBuild project.

To package a MSBuild project with the Fortify ScanCentral SAST client:

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your MSBuild project. The basic syntax is: `scancentral package -bt msbuild -bf <build_file> -o <output_zip>`. For example, `scancentral package -bt msbuild -bf my.sln -o mypayload.zip`  
For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see ["Fortify ScanCentral SAST" on the previous page](#).

**Note:** Fortify ScanCentral SAST packaging is also built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see ["Development Tools" on page 319](#).

## Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see ["IDE Tool" on page 319](#).

## Manual Code Packaging

Manual code packaging consists of:

- Preparing source code files
- Preparing compiled files
- Creating a zip file containing the source code and compiled files

### Preparing Source Code Files

Source code consists of all projects for the application. A complete project contains the following:

- All necessary source code files (C/C++, C#, or VB.NET)
- All required reference libraries  
This includes those from relevant frameworks, NuGet packages, and third-party libraries.
- For C/C++ projects, include all necessary header files that do not belong to the Visual Studio or MSBuild installation.
- For ASP.NET and ASP.NET Core projects, include all the necessary ASP.NET page files  
The supported ASP.NET page types are ASPX, ASCX, ASAX, ASHX, ASMX, AXML, Master, CSHTML, VBHTML, BAML, and XAML.

**Important!** If you are working in the Visual Studio Developer Command Prompt, Fortify recommends that you run the `dotnet restore` command to make sure that all required reference libraries are downloaded and installed in the project. You must run this command from the top-level folder of the project.

### Preparing Compiled Files



**Note:** You do not need to provide compiled files for Xamarin applications.

- Clean and compile the application in **full** debug mode. Scan results of compiled files only include file names and line numbers if there are matching PDB files. Matching binary and PDB files must be present in the same folder; a binary is excluded if the matching PDB file is not present.

**Note:** If you are including third party libraries in scan results, matching PDB files are required.

- If source mode scanning will be used, provide only the dependencies from the debug build.
- If mixed mode scanning will be used, provide the debug build files, including all dependencies. Do not provide the obj and bin/release folders in order to avoid duplicate code in the payload.

### Creating a Zip File

Package the source code and debug build files in a zip file. Place the source code files in a separate root directory.

If the application contains Javascript, HTML, and/or XML components, simply include the JavaScript, HTML, and/or XML files in the payload to have them scanned.

### Preparing Java Application Files

For Java applications, use one of the following methods to prepare your application files:

- ["Automated Code Packaging with Fortify ScanCentral SAST \(Recommended\)"](#) below
- ["Code Packaging with IDE Tools \(Recommended\)"](#) on the next page
- ["Manual Code Packaging"](#) on the next page

**Important!** Static scans of Java applications use source mode scanning by default. Fortify strongly recommends providing source code, as source mode scanning produces more accurate and comprehensive scan results. In addition, as the scanning process can result in false positives, auditors use the source code to manually review issues. If source mode scanning is not an option, contact support to enable mixed mode (binary and source code) scanning.

### Automated Code Packaging with Fortify ScanCentral SAST (Recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your Gradle or Maven project.

To package a Gradle or Maven project with the Fortify ScanCentral SAST client:

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your Gradle or Maven project. The basic syntax is: `scancentral package -bt mvn|gradle -bf <build_file> -o <output_zip>`. For example, `scancentral package -bt mvn -bf pom.xml -o mypayload.zip`, `scancentral package -bt gradle -bf build.gradle -o mypayload.zip`

For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see ["Fortify ScanCentral SAST" on page 91](#).

**Note:** Fortify ScanCentral SAST packaging is also built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see ["Development Tools" on page 319](#).

## Code Packaging with IDE Tools (Recommended)

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see ["IDE Tool" on page 319](#).

## Manual Code Packaging

Manual code packaging consists of:

- Preparing source code files
- Preparing compiled files
- Creating a zip file containing the source code and compiled files

### Preparing Source Code Files

Provide the source code, along with any relevant Kotlin source code that is referenced by the Java application.

### Preparing Compiled Files

- Compile the application in debug mode (for example, run `javac -g` if you are using the `javac` compiler). Scan results of compiled files only include file names and line numbers if debug information is provided.
- JSP files must be part of a WAR file. Do not precompile JSP files.
- Package the application as a JAR, WAR, or EAR file.
- Provide only one copy of shared files to avoid duplicate code in the payload.
- If source mode scanning will be used, provide just the dependencies from the compiled files to minimize duplicate issues in scan results. Dependencies are usually found in the `WEB-INF/lib` folders (WAR) and the `lib` or `APP-INF/lib` folders (EAR).
- If mixed mode scanning will be used, provide all the compiled files, including dependencies.

### Creating a Zip File

Package the source code and compiled files in a zip file. You can include multiple JAR, WAR, and EAR files in the zip file. Do not include source code in JARs; place the source code files in a separate root directory.

If the application contains Javascript, HTML, and/or XML components, simply include the JavaScript, HTML, and/or XML files in the payload to have them scanned.

## Preparing JavaScript Technology/HTML/XML Files

For applications that consist of JavaScript, TypeScript, HTML, and/or XML files, package the files in a zip file. Include all production dependencies (for example, run `npm install --only=prod` if you are using npm). Upload the zip file under the **JS/TS/HTML** technology stack option. JS/TS/HTML is a catch-all option for simple web applications and web applications that primarily use JavaScript-related technologies.

If applicable, make sure to do the following:

- Include the `package.json` file.
- Provide only TypeScript source code, not transpiled TypeScript. For example, do not provide the `dist` folder generated when building an Angular project.

**Important!** Do not include minified JavaScript files of your source code, as minified code significantly diminishes the quality of scan results.

For applications that are built with different languages or technology stacks and contain Javascript, HTML, and/or XML files, package the application according to the instructions provided for the language or technology stack and simply include the JavaScript, HTML, and/or XML files in the package.

## Preparing Kotlin Application Files

For Kotlin applications, package the Kotlin source code files in a zip file, along with any relevant Java source code that is referenced by the Kotlin application. Include all dependencies; these are usually found in the `WEB-INF/lib` folders (WAR) and the `lib` or `APP-INF/lib` folders (EAR).

**Important!** Scanning of Kotlin source files is supported.

## Preparing ABAP (SAP) Application Files

ABAP code needs to be extracted from the SAP database and prepared for scanning. The Fortify ABAP Extractor tool is provided for downloading source code files to the presentation server.

### Importing the Transport Request

The Fortify ABAP Extractor is available on the Tools page in the portal (see ["Viewing Tools" on page 322](#)). The Fortify ABAP Extractor zip file contains the following files:

- `K900XXX.S9S` (where the "XXX" is the release number)
- `R900XXX.S9S` (where the "XXX" is the release number)

These files make up the SAP transport request that you must import into your SAP system from outside your local Transport Domain. Have your SAP administrator or an individual authorized to install transport requests on the system import the transport request.

The NSP files contain a program, a transaction (YSCA), and the program user interface. After you import them into your system, you can extract your code from the SAP database.

## Installation Note

The Fortify ABAP Extractor transport request was created on a system running SAP release 7.02, SP level 0006. If you are running a different SAP version and you get the transport request import error: Install release does not match the current version, then the transport request installation has failed.

To resolve this issue:

1. Re-run the transport request import.  
The Import Transport Request dialog box opens.
2. Click the **Options** tab.
3. Select the **Ignore Invalid Component Version** check box.
4. Complete the import procedure.

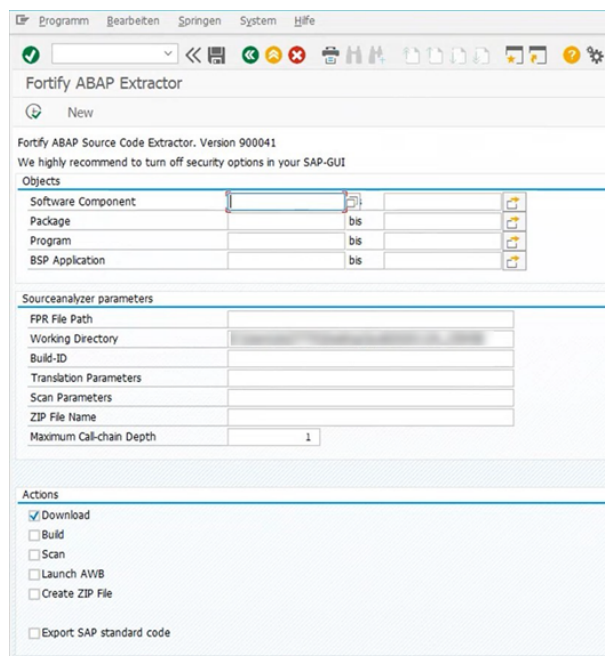
If this does not resolve the issue or if your system is running on an SAP version with a different table structure, Fortify recommends that you export your ABAP file structure using your own technology so that Fortify on Demand can scan the ABAP code.

## Running the Fortify ABAP Extractor

You need to use an account with permission to download files to the local system and execute operating system commands.

To run the Fortify ABAP Extractor:

1. Start the program from the transaction code or manually start the Extractor object.



2. Provide the start and end name for the range of software components, packages, programs, or BSP applications that you want to scan.

**Note:** You can specify multiple objects or ranges.

3. Specify your preferences for extracting the source code. Fields are required unless otherwise noted.

**Note:** Certain fields do not apply to Fortify on Demand usage. Only applicable fields are listed.

Field	Description
Working Directory	Type or select the directory where you want to store the extracted source code .
ZIP File Name	(Optional) Type a ZIP file name if you want your output in a compressed package.
Maximum Call-chain Depth	A global SAP-function F is not downloaded unless F was explicitly selected or unless F can be reached through a chain of function calls that start in explicitly-selected code and whose length is this number or less. Fortify recommends that you do not specify a value greater than 2 unless directed to do so by support.

4. Specify the actions to execute. Fields are required unless otherwise noted.

**Note:** Certain fields do not apply to Fortify on Demand usage. Only applicable fields are listed below.

Field	Description
Download	Select this check box to download the source code extracted from your SAP database.
Create ZIP file	(Optional) Select this check box to compress the output. You can also manually compress the output after the source code is extracted from your SAP database.
Export SAP standard code	(Optional) Select this check box to export SAP standard code in addition to custom code.

5. Click **Execute**.

### Fortify ABAP Extractor Notes

Because the Fortify ABAP Extractor program is executed online, you might receive a max dialog work process time reached exception if the volume of source files selected for extraction exceeds the allowable process run time. To work around this, download large projects as a series of

smaller Extractor tasks. For example, if your project consists of four different packages, download each package separately into the same project directory. If the exception occurs frequently, work with your SAP Basis administrator to increase the maximum time limit (`rdisp/max_wprun_time`).

When a PACKAGE is extracted from ABAP, the Fortify ABAP Extractor extracts everything from TDEVC with a `parentc1` field that matches the package name. It then recursively extracts everything else from TDEVC with a `parentc1` field equal to those already extracted from TDEVC. The field extracted from TDEVC is `devclass`.

The `devclass` values are treated as a set of program names and handled the same way as a program name, which you can provide.

Programs are extracted from TRDIR by comparing the name field with either:

- The program name specified in the selection screen
- The list of values extracted from TDEVC if a package was provided

The rows from TRDIR are those for which the name field has the given program name and the expression `LIKEprogramname` is used to extract rows.

This final list of names is used with `READ REPORT` to get code out of the SAP system. This method does read classes and methods out as well as merely `REPORTs`, for the record.

Each `READ REPORT` call produces a file in the temporary folder on the local system.

As source code is downloaded, the Fortify ABAP Extractor detects `INCLUDE` statements in the source. When found, it downloads the include targets to the local system.

### Packaging ABAP Source Code

If you did not have Fortify ABAP Extractor compress the output, package the downloaded source code files in a zip file.

### Preparing C and C++ Application Files

Fortify on Demand does not support direct scanning of C/C++ source code or their binaries. C/C++ code must be translated and packaged into an archive in your environment. This ensures consistency in translation regarding environmental variables and compilers used and alleviates the need for Fortify on Demand to reproduce your build environment. A translate-only version of Micro Focus Fortify Static Code Analyzer is provided for translating C/C++ code and packaging it for scanning.

### Installing Fortify Static Code Analyzer

The latest version of Fortify Static Code Analyzer is available on the Tools page in the portal (see ["Viewing Tools" on page 322](#)). You can download installers for Windows, macOS, and Linux operating systems. A valid license file is required to translate source code. Contact support to be issued a license, which will be available from the Tools page.

For installation and usage instructions, see the *Micro Focus Fortify Static Code Analyzer User Guide* at [Fortify Static Code Analyzer and Tools Documentation](#).

## Translating Code

1. In a command-line interface, change the directory to your normal build directory.
2. Execute the following command:

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

where <build\_command> is your build script.

Example:

```
sourceanalyzer -debug -verbose -logfile translate.log -b my_proj  
touchless make all
```

3. Verify that the project builds correctly by checking the console output for completion and the `translate.log` for errors.

## Packaging Translated Code

A Fortify Static Code Analyzer mobile build session (MBS) lets you translate a project on one machine and scan it on another. A mobile build session file (MBS file) includes all the files needed for the scan.

To generate and package an MBS file:

1. On the machine where the translation was done, issue the following command to generate a mobile build session:

```
sourceanalyzer -b <build-id> -export-build-session <file.mbs>  
where <file.mbs> is the file name you provide for the mobile build session.
```

2. Package the MBS file in the root of a zip file. Do not include other files (including additional MBS files) or directories; this might cause the scan to be cancelled.
3. Upload the zip file to Fortify on Demand under the **MBS/C/C++** technology stack option.

For more information about using Fortify Static Code Analyzer, see the *Micro Focus Fortify Static Code Analyzer User Guide* at [Fortify Static Code Analyzer and Tools Documentation](#).

## Preparing Classic ASP, VBScript, and Visual Basic Application Files

For Classic ASP, VBScript, and Visual Basic (VB6) applications, package the source code files in one zip file.

## Preparing COBOL Application Files

For COBOL applications, package the COBOL source code, the copybook files that the COBOL source code uses, and the SQL INCLUDE files that the COBOL source code references in one zip file.

Copybook and SQL INCLUDE files must retain the names used in the COBOL source code COPY statements.

Do not include copybook or SQL INCLUDE files in the directory or the subdirectory where the COBOL sources reside. Fortify recommends that you place your COBOL source code in a folder called `sources/` and your copybooks in a folder called `copybooks/`. Place these folders at the same level.

### Zip file

- sources/ folder
- copybooks/ folder

## Preparing ColdFusion Markup Language (CFML) Application Files

For CFML applications, package the source code files in one zip file.

## Preparing Dockerfiles and Infrastructure as Code (IaC) Files

Infrastructure as Code (IaC) configuration files and Dockerfiles can be submitted as stand-alone payloads. Package the files in a zip file and submit it under the **Infrastructure-As-Code/Dockerfile** technology stack. Supported file formats are: Dockerfile, JSON, XML, and YAML.

For containerized applications, package the application according to the instructions provided for the application's language or technology stack and include the Dockerfile in the package.

### Note:

Fortify Static Code Analyzer translates the following files as Dockerfiles: Dockerfile, dockerfile, \*.Dockerfile, and \*.dockerfile.

Fortify Static Code Analyzer accepts the following escape characters in Dockerfiles: backslash (\) and backquote (`). If the escape character is not set in the Dockerfile, then Fortify Static Code Analyzer assumes that the backslash is the escape character.

## Preparing Go Application Files

For Go applications, use one of the following methods to prepare your application files:

- ["Automated Code Packaging with Fortify ScanCentral SAST \(Recommended\)" below](#)
- ["Code Packaging with IDE Tools" on the next page](#)
- ["Manual Code Packaging" on the next page](#)

## Automated Code Packaging with Fortify ScanCentral SAST (Recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your Go project.

To package a Go project with the Fortify ScanCentral SAST client:

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your Go project. The basic syntax is: `scancentral package -bt none -o <output_zip>`. For example, `scancentral package -bt none -o mypayload.zip`



For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see ["Fortify ScanCentral SAST" on page 91](#).

**Note:** Fortify ScanCentral SAST packaging is also built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see ["Development Tools" on page 319](#).

## Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see ["IDE Tool" on page 319](#).

## Manual Code Packaging

Package the Go source code files in a zip file. Include dependencies that are not in the standard Go library. Make sure that these dependencies are in the Vendor folder.

The following dependency management systems built into Go are supported:

- Go modules (recommended)  
If your project uses Go modules, the project files (including the go.mod file) must be in the root of the zip file. Do not place the project files inside nested directories.
- GOPATH (deprecated in Go 1.13)

**Note:** The following entities are excluded from scanning:

- Vendor folder
- All projects defined by any go.mod files in subfolders
- All files with the `_test.go` suffix (unit tests)

## Preparing PHP Application Files

For PHP applications, use one of the following methods to prepare your application files:

- ["Automated Code Packaging with Fortify ScanCentral SAST \(Recommended\)" below](#)
- ["Code Packaging with IDE Tools" on the next page](#)
- ["Manual Code Packaging" on the next page](#)

## Automated Code Packaging with Fortify ScanCentral SAST (Recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your PHP project.

To package a PHP project with the Fortify ScanCentral SAST client:

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your PHP project. The basic syntax is: `scancentral package -bt none -hv <version> -o <output_zip>`. For example, `scancentral package -bt none -hv 7.1 -o mypayload.zip`  
For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see ["Fortify ScanCentral SAST" on page 91](#).

**Note:** Fortify ScanCentral SAST packaging is also built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see ["Development Tools" on page 319](#).

## Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see ["IDE Tool" on page 319](#).

## Manual Code Packaging

Package the source code files in one zip file. Make sure to include the `php.ini` file with the package. This file helps to identify where dependencies reside.

## Preparing Python Application Files

For Python applications, use one of the following methods to prepare your application files:

- ["Automated Code Packaging with Fortify ScanCentral SAST \(Recommended\)" below](#)

**Important!** Python microservices must be packaged using the Fortify ScanCentral SAST client

- ["Code Packaging with IDE Tools" on the next page](#)
- ["Manual Code Packaging" on the next page](#)

## Automated Code Packaging with Fortify ScanCentral SAST (Recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your Python project.

To package a Python project with the Fortify ScanCentral SAST client:

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your Python project. The basic syntax is: `scancentral package -bt none -o <output_zip>`. For example, `scancentral`

```
package -bt none -o mypayload.zip
```

For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see ["Fortify ScanCentral SAST" on page 91](#).

**Note:** Fortify ScanCentral SAST packaging is also built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see ["Development Tools" on page 319](#).

## Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see ["IDE Tool" on page 319](#).

## Manual Code Packaging

Package the source code files in one zip file. Include all standard and third-party modules and packages; these are found in the `lib` folder of the Python virtual environment (provide at a minimum the `site-packages` folder). Fortify on Demand does not support PYC files (compiled Python files).

**Note:** If your application uses a version of Python not listed in ["Supported Languages" on page 83](#), contact support to discuss your options.

## Preparing Ruby Application Files

For applications created in Ruby, package the entire application as it would be deployed and all source code files in one zip file .

## Preparing Salesforce (Apex and Visualforce) Application Files

To prepare Salesforce (Apex and Visualforce) applications:

- Download your Salesforce application from your Salesforce organization (org) where you develop and deploy it. The downloaded version of your application contains:
  - Apex classes in files with the `.cls` extension
  - Visualforce web pages in files with the `.page` extension
  - Apex code files called database “trigger” functions in files with the `.trigger` extension

Use the Force.com Migration Tool available on the Salesforce website to download your app from your org in the Salesforce cloud.

- If you customized the standard Salesforce database structures to support your app, use the `sf_extractor` tool provided with Micro Focus Fortify Static Code Analyzer to download a description of the changes. The tool creates a custom sObjects JSON file that you include with the source code files. This information is required to perform a more complete scan.

The latest version of Fortify Static Code Analyzer is available from the Tools page in the portal. The `sf_extractor` tool is located in the `<sca_install_dir>/Tools` directory. For installation

instructions and `sf_extractor` usage instructions, see the *Micro Focus Fortify Static Code Analyzer User Guide* at [Fortify Static Code Analyzer and Tools Documentation](#).

- Package the source code files in one zip file.

**Important!** Supported file extensions for the source code files are: `.cls`, `.trigger`, `.page`, and `.component`.

## Preparing Scala Application Files

Scala code must be translated and packaged into an archive in your environment. The Fortify Scala plugin and a translate-only version of Micro Focus Fortify Static Code Analyzer are available for translating Scala and packaging it code for scanning.

## Installing Fortify Static Code Analyzer

The latest version of Fortify Static Code Analyzer is available on the Tools page in the portal (see "[Viewing Tools](#)" on page 322). You can download installers for Windows, macOS, and Linux operating systems. A valid license file is required to translate source code. Contact support to be issued a license, which will be available from the Tools page.

For installation and usage instructions, see the *Micro Focus Fortify Static Code Analyzer User Guide* at [Fortify Static Code Analyzer and Tools Documentation](#).

## Translating Code

To translate Scala code, you must have the following: a standard Lightbend Enterprise Suite license and the Fortify Scala plugin from Lightbend. Contact Fortify on Demand support to obtain a license key. For instructions on downloading the plugin and translating Scala code, see the Lightbend documentation at <https://developer.lightbend.com/guides/fortify/>.

**Important!** If your application contains source code in a language other than Scala, submit the other source code in a separate assessment.

## Packaging Translated Code

A Fortify Static Code Analyzer mobile build session (MBS) lets you translate a project on one machine and scan it on another. A mobile build session file (MBS file) includes all the files needed for the scan.

To generate and package an MBS file:

1. On the machine where the translation was done, execute the following command to generate a mobile build session:  

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

where `<file.mbs>` is the file name you provide for the mobile build session.
2. Package the MBS file in the root of a zip file. Do not include other files (including additional MBS files) or directories; this will cause the scan to be cancelled.
3. Upload the zip file to Fortify on Demand under the **MBS/C/C++/Scala** technology stack option.

For more information about using Fortify Static Code Analyzer, see the *Micro Focus Fortify Static Code Analyzer User Guide* at [Fortify Static Code Analyzer and Tools Documentation](#).

## Preparing Android Application Files (Source Code)

For Android applications, package the Java or Kotlin source code files in one zip file. Include all dependencies that are required to build the Android code in the application project.

**Note:** Fortify Static Code Analyzer supports Xamarin. For instructions on preparing Xamarin application files, see "[Preparing .NET Application Files](#)" on page 91. Other third-party development libraries such as Cordova, Ionic Framework, PhoneGap, and Unity are not supported.

### Related Topics:

For information on preparing Android binary files for mobile assessments, see "[Preparing Android Application Files \(Binary\)](#)" on page 139.

## Preparing iOS Application Files (Source Code)

For iOS applications, prepare the source code files according to the following instructions:

- Applications must be buildable using xcodebuild from the command line.
- Make sure that any dependencies required to build the project are present in the payload and not accessed through dependency managers like a password-protected GitHub. The payload needs to be buildable in isolation.
- Remove any developer or environment-specific settings from your application
- If your project includes property list files in binary format, you must first convert them to XML format. You can do this with the Xcode `plutil` command.
- Make sure that the headers for third-party libraries are available.
- Objective-C++ projects must use the non-fragile Objective-C runtime (ABI version 2 or 3).

Package the source code files in one zip file.

**Note:** Fortify Static Code Analyzer supports Xamarin. For instructions on preparing Xamarin application files, see "[Preparing .NET Application Files](#)" on page 91. Other third-party development libraries such as Cordova, Ionic Framework, PhoneGap, and Unity are not supported.

### Related Topics:

For information on preparing iOS binary files for mobile assessments, see "[Preparing iOS Application Files \(Binary\)](#)" on page 139

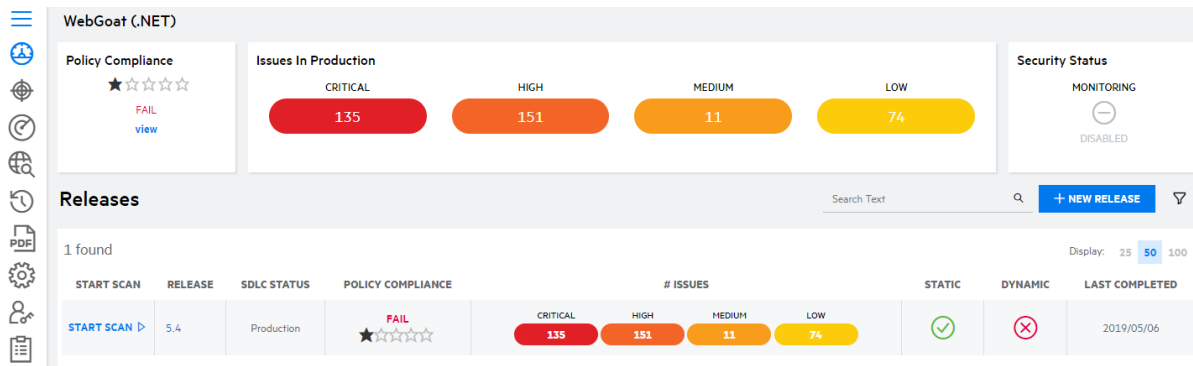
## Configuring a Static Scan

After preparing your application files for a static assessment, you need to configure the static scan settings. You only need to configure the static scan settings once per release as your settings are

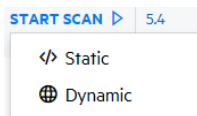
carried over to the next scan. You can edit settings as needed for subsequent assessments.

To configure a static scan:

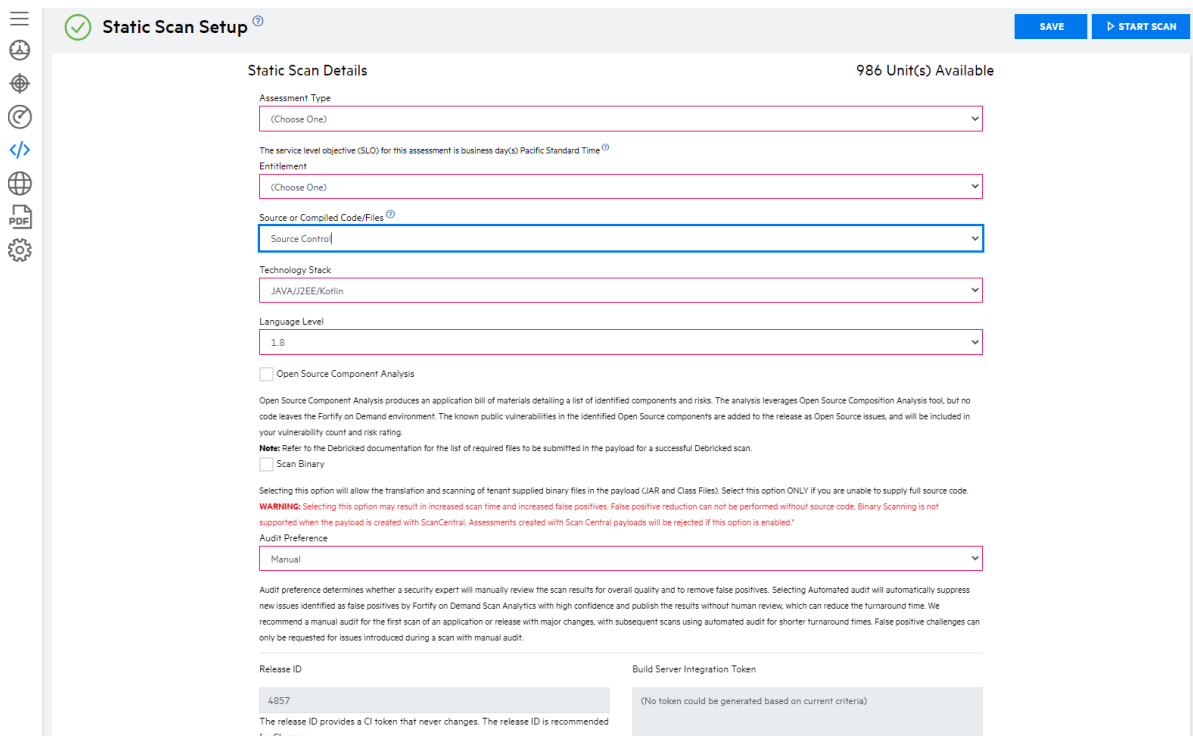
1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application.  
The Application Overview page appears.



3. Click **Start Scan** for the release that you want to have assessed and select **Static**.



The Static Scan Setup page appears.



4. Complete the fields as needed. Fields are required unless otherwise noted.

Field	Description
Assessment Type	<p>Select the assessment type. Only assessment types allowed by the organization's security policy are displayed.</p> <p>The SLO of the selected assessment type appears below the field.</p>
Entitlement	<p>Select the entitlement that the assessment will use. The field displays entitlements that are valid for the selected assessment type, including those available for purchase. Note that microservice applications are restricted to subscriptions. If the release has an active subscription, only options that do not consume entitlements are displayed.</p> <p><b>Note:</b> If you select an entitlement offered through a Dynamic Premium or Mobile Premium assessment, the assessment is activated and the full cost of the entitlement is deducted.</p>
Source or Compiled Code/Files	<p>Select the method of uploading the payload.</p> <ul style="list-style-type: none"> <li>• <b>Manual Upload</b> (default): Manually upload the payload from your local system.</li> <li>• <b>Source Control:</b> Upload the payload from a version control platform. This option is only available if source control has been configured. For more information, see "<a href="#">Source Control Integration</a>" on page 397.</li> </ul>
Technology Stack	<p>Select the application's technology stack. The languages available for selection depends on the application type (web/thick client or mobile) and whether the application is a microservice application.</p>
Language Level	<p>If applicable, select the technology stack's language level from the list.</p>
Open Source Component Analysis	<p>(Optional) Select the check box to include open source component analysis. No code leaves the Fortify on Demand environment. For more information on adding open source component analysis as part of a static scan, see "<a href="#">Open Source Software Composition Analysis</a>" on page 148.</p>
Scan Binary	<p><b>Note:</b> Contact support to enable the option.</p> <p>(Optional; Java/J2EE/Kotlin, .NET, and .NET Core technology stacks) Select the check box to have compiled and source code files scanned. Scanning binary files is not supported for ScanCentral-packaged payloads.</p>

	<p><b>Note:</b> If the source code inclusion requirement is enabled and this option is not selected, the scan will be cancelled if the payload does not contain source code.</p>
<p>Audit Preference</p>	<p>Select the audit preference.</p> <ul style="list-style-type: none"> <li>• <b>Manual:</b> A security expert manually reviews the scan results and removes false positives.</li> <li>• <b>Automated:</b> False positives identified by Fortify Scan Analytics with high confidence are automatically suppressed and results are published without manual review.</li> </ul> <p><b>Note:</b> Fortify Scan Analytics is only applied to new issues found in a scan using automated audit.</p> <p>The ability to select audit preference depends on the assessment type:</p> <ul style="list-style-type: none"> <li>• A Static single scan allows Automated only.</li> <li>• A Static subscription allows one Manual audit per application (not per release or microservice).</li> <li>• A Static+ single scan allows Manual only.</li> <li>• A Static+ subscription allows Automated or Manual audit for each assessment.</li> </ul>
<p>Scan third-party libraries for static security assessment</p>	<p><b>Note:</b> Contact support to enable the option.</p> <p>(Optional) Select the check box to have third party libraries scanned for vulnerabilities, which will be included in the scan results. This significantly increases the turnaround time. This option is not available for microservice applications.</p> <p><b>Note:</b> Selecting this option infers that your organization has received consent from all third-party vendors to scan their libraries.</p>
<p>Release ID</p>	<p>Once the static scan settings have been saved, the release ID can be used to submit a static scan using CICD tools. The release ID serves as a token that retrieves the most recently saved scan settings in the portal.</p> <p><b>Important!</b> The release ID replaces the BSI token. Migrate build configurations to the release ID at your earliest convenience.</p>



Build Server Integration	Once the static scan settings (assessment type, technology stack, language level, audit preference, open source component analysis, and include third party libraries) have been configured, a token is automatically populated in the <b>Build Server Integration</b> field. The token can be used to submit a static assessment using external tools.  <b>Note:</b> The BSI token is persistent across assessments of a release.
--------------------------	--

5. Click **Save**.  
Your static scan settings are saved.
6. If you have the Consume Entitlements permissions and selected a subscription entitlement, click **Start Subscription** to start the static assessment subscription and consume the entitlement without starting a scan.

**Note:** Contact support to enable the option.

**Note:** The assessment cost is deducted from the entitlement when a user starts the initial scan.

## Submitting a Static Assessment

Once you have packaged the application files and configured the static scan settings, upload the payload for scanning. You can submit a static assessment using the following methods:

- IDE plugin tools: Visual Studio Extension, Eclipse Plugin, IntelliJ Plugin, Fortify Extension for Visual Studio Code  
For more information, see ["IDE Tool" on page 319](#).
- Build server integration tools: FoDUploader, Fortify Azure DevOps Extension, Fortify on Demand Jenkins Plugin  
For more information, see ["CICD Tool" on page 320](#).
- Fortify on Demand API  
For more information, see ["Fortify on Demand API" on page 306](#).
- Manually through the portal  
For more information, see ["Uploading a Static Assessment Payload Through the Portal" below](#).

### Uploading a Static Assessment Payload Through the Portal

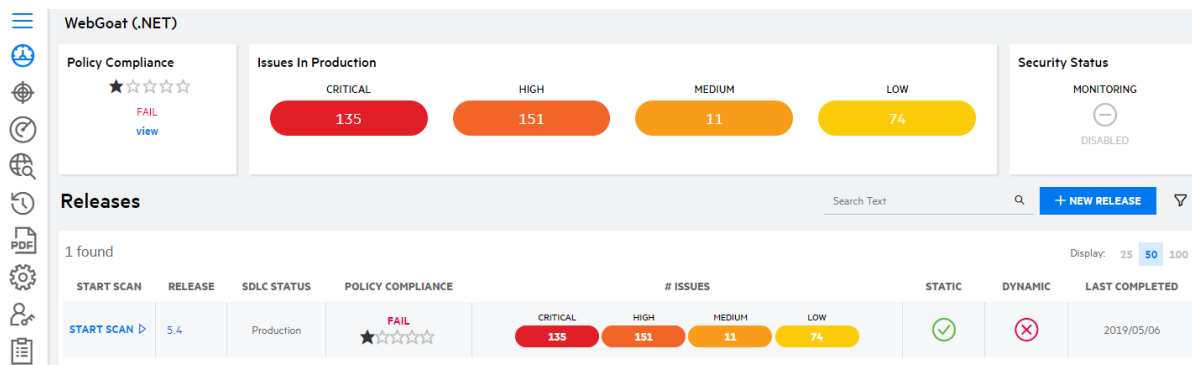
Fortify on Demand has a payload file size limit of 5 GB; web browser have their own file size limits (see your browser's documentation for details). As portal timeouts can occur when uploading large files, Fortify recommends uploading through the portal only if the file size is less than 500 MB.

You can submit multiple scans for an application, including those for the same release. An application can have one in progress static scan at a time. Additional scans are queued and then scanned in the order in which they were queued. Each application can have up to 30 scans in the queue.

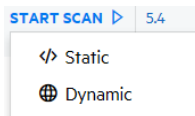
**Note:** If you have difficulties uploading through the portal, see ["Submitting a Static Assessment" on the previous page](#) for alternative methods of uploading your files. You can also create a Help Center ticket to discuss the most appropriate upload option.

To upload a static assessment payload through the portal:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application.  
The Application Overview page appears.



3. Click **Start Scan** for the release that you want to have assessed and select **Static** from the menu.



The Static Scan Setup page appears.

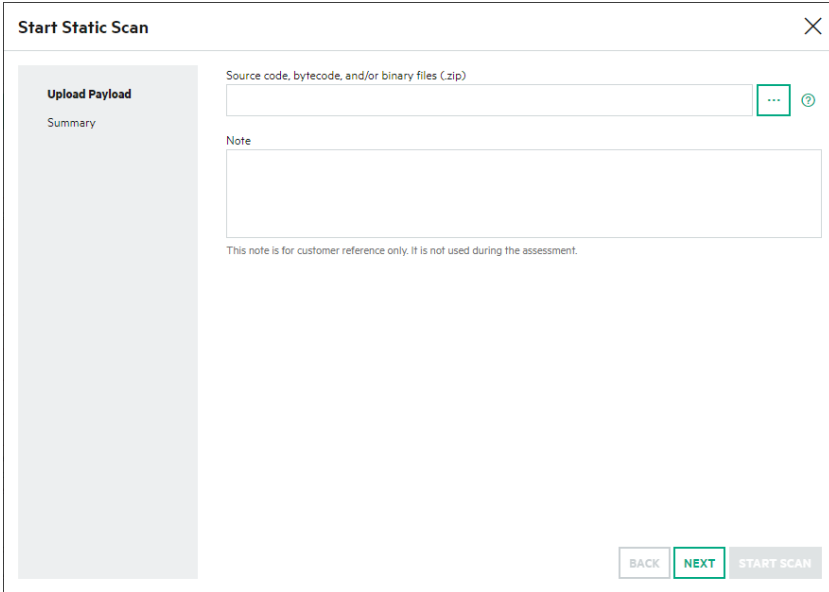

4. Click **Start Scan**.

**Note:** If the application has an active static scan, you are blocked from starting another scan.

The Start Static Scan window opens.

5. Perform the relevant task based on your method of upload:

Method of Upload	Procedure
------------------	-----------

<p>Manual upload</p>	 <p>a. Click ...</p> <p>b. Navigate to and select your zip file.</p>
<p>Source Control</p>	 <p>a. Select <b>Branch</b> or <b>Release</b> from the <b>Source Location</b> list.</p> <p>b. Select the specific branch or release.</p>

- In the **Note** field, type a description of the application.
- Click **Next**.  
A summary of the static scan setup values appears.
- Review the summary. If necessary, click **Back** and make any corrections. If the values are correct, click **Start Scan**.  
The zip file is uploaded. Once the upload is complete, you are returned to the Static Scan Setup page. The page indicates that a scan is in progress or queued.

**Note:** The portal automatically logs you out after a 20 minute period of inactivity.

## Static Assessment Payload Validation

After the payload has been uploaded, Fortify on Demand performs the following payload validation checks to ensure that the requirements have been met for the static testing team to start a static assessment:

- The zip file is valid and not corrupt.
- The payload contains file extensions that are supported by Fortify Static Code Analyzer. Supported file extensions are: ABAP, abap, appxmanifest, as, asax, ascx, ashx, asmx, asp, aspx, baml, bas, BSP, bsp, cbl, cfc, cfm, cfml, cls, cob, conf, Config, config, cpx, cs, cscfg, csdef, cshtml, ctl, ctp, dll, Dockerfile, dockerfile, erb, exe, frm, go, hcl, htm, html, inc, ini, java, jmod, js, jsff, json, jsp, jspf, jsp, jsx, kt, kts, Master, master, mxml, page, php, phtml, pkb, pkh, pks, plist, properties, py, razor, rb, scala, settings, sql, swift, tag, tagx, tf, tld, trigger, ts, tsx, vb, vbhtml, vbs, vbscript, wadcfg, wadcfgx, winmd, wsdd, wsdl, xaml, xcfg, xhtml, xmi, xml, xsd, yaml, yml.
- For .NET applications, the payload contains .dll or .exe files.
- For Java and Kotlin applications, the payload contains .class, .java, .jar, .jsp, .kt, .ktm, or .kts files.
- A Fortify ScanCentral SAST-packaged payload does not have the **Scan Binary** scan setting enabled.
- For Python microservice applications, Fortify ScanCentral SAST is used to package the payload.
- For technology stacks that require a mobile build session (MBS) file to be submitted, the payload contains only one .mbs file.
- For tenants that have enabled the source code inclusion requirement, the payload contains files in the following file formats:

Technology Stack	Source File Extension
.NET	.cs, .vb
ABAP	.abap
ASP	.asp
CFML	.cfm, .cfml, .cfc
COBOL	.cbl, .cob, .ccp, .cb2
Dockerfile/Infrastructure as Code	.dockerfile, .json, .xml, .yaml, dockerfile
Go	.go
JAVA/J2EE/Kotlin	.java, .kt, .ktm, .kts
JS/TS/HTML	.xsd, .xmi, .wsdd, .config, .cpx, .xcfg, .js, .ts
PHP	.php
PYTHON	.py
VB6	.vbs, .bas, .frm, .ctl, .cls

VBScript	.vbscript
Ruby	.rb

If any of the requirements is not met, the scan is automatically canceled and an email indicating the cancellation reason is sent. Upon acceptance of the file, the code is transferred to a secure server and analyzed.

## Dynamic Assessments

A dynamic assessment analyzes a running web application for security vulnerabilities. Dynamic assessments include automated testing powered by Micro Focus Fortify WebInspect, manual analysis, and Continuous Application Monitoring.

Dynamic testing using Fortify WebInspect involves the following modes:

- Crawl, the process by which Fortify WebInspect identifies the structure of the target website
- Audit, the actual vulnerability scan

This section contains the following topics:

<a href="#">Preparing the Website for Dynamic Testing</a>	114
<a href="#">Preparing Web API Files</a>	115
<a href="#">Configuring a Dynamic Scan</a>	118
<a href="#">Submitting a Dynamic Assessment</a>	129
<a href="#">Scheduling the Dynamic Scan Through the Portal</a>	130
<a href="#">Editing Dynamic Scan Settings</a>	132
<a href="#">Continuous Application Monitoring</a>	133
<a href="#">Configuring Application Monitoring</a>	133
<a href="#">Canceling an Application Monitoring Scan</a>	135
<a href="#">Viewing Application Monitoring Issues</a>	135
<a href="#">Viewing Risk Profile Results</a>	136

## Preparing the Website for Dynamic Testing

For all dynamic assessments, make the following preparations to facilitate the testing process:

- Confirm that your web application and user credentials are functioning before the assessment.
- Disable all multi-factor authentication controls for the duration of the testing window. This includes secondary authentication mechanisms such as SMS messages, email verifications, CAPTCHA, OATH Tokens, and physical tokens. Alternatively, the assessment can be performed

unauthenticated to evaluate the security of the application content available to unauthenticated users.

- Complete all functional and performance testing before the assessment and freeze the application's code for the duration of the testing window.
- As a standard precaution, Fortify recommends that you back up all of your data before beginning the testing process. When testing is complete, restore your data from a backup that is known to be good to avoid any chance of data corruption.
- Add the Fortify on Demand IP addresses to the allow list in firewalls, IPSs, IDSs, and WAFs to ensure the application can be scanned by the dynamic testing team. You can obtain the IP addresses from the Dynamic Scan Setup page in the portal. Adhoc addresses may be used with your consent only when conditions necessitate it.
- Provide the Fortify on Demand IP addresses to your security operations and network operations teams, so they know not to block the IP addresses if they see attacks being submitted against the site, which are part of planned recurring security scanning.

**Note:** As long as your website is accessible through the http/https default ports (80/443), you do not need to open any additional ports for the assessment.

The following task is optional and depends on the dynamic assessment type:

- Create workflow macros to run Dynamic Website assessments as Workflow-Driven Scans. A workflow macro is a recording of HTTP events when you navigate a Web site using a Web Macro Recorder tool. You can create workflow macros with Fortify WebInspect's Web Macro Recorder, available on the Tools page in the portal. For instructions on creating workflow macros, see the *Micro Focus Fortify WebInspect User Guide* at [Fortify WebInspect Documentation](#).

## Preparing Web API Files

If a dynamic assessment includes web API testing, you need to provide project files with working sample data for proper security testing. Prepare project files according to the following guidelines.

**Note:** If you do not have project files with working sample data, ask your QA and development teams for assistance in obtaining these files. They usually have collections of these files for testing web API functions.

### SOAP

- Provide a Web Service Definition Language (WSDL) file or URL.
- Provide request and response pairs in text or XML format or as a SoapUI project or Postman collection file.
- Requests must include valid parameter values to establish the baseline application behavior.
- If your API requires authentication, provide credentials that will be valid during the testing period.
- If you are submitting a SoapUI project or Postman collection file, configure authentication in the project file. You can also provide the information in the **Additional Notes** or **Additional Documentation** fields.

## REST

- Provide an API definition, such as an OpenAPI document file or URL or Postman collection file or URL.

**Note:** Postman environment files are not supported.

- Requests must include valid parameter values to establish the baseline application behavior.
- If your API requires authentication, provide credentials that will be valid during the testing period.
  - If you are providing a Postman collection, configure authentication in the Postman collection.

**Note:** Dynamic authentication is not supported.

- If you are providing an OpenAPI document, provide the credentials on the Dynamic Scan Setup page.

## Examples

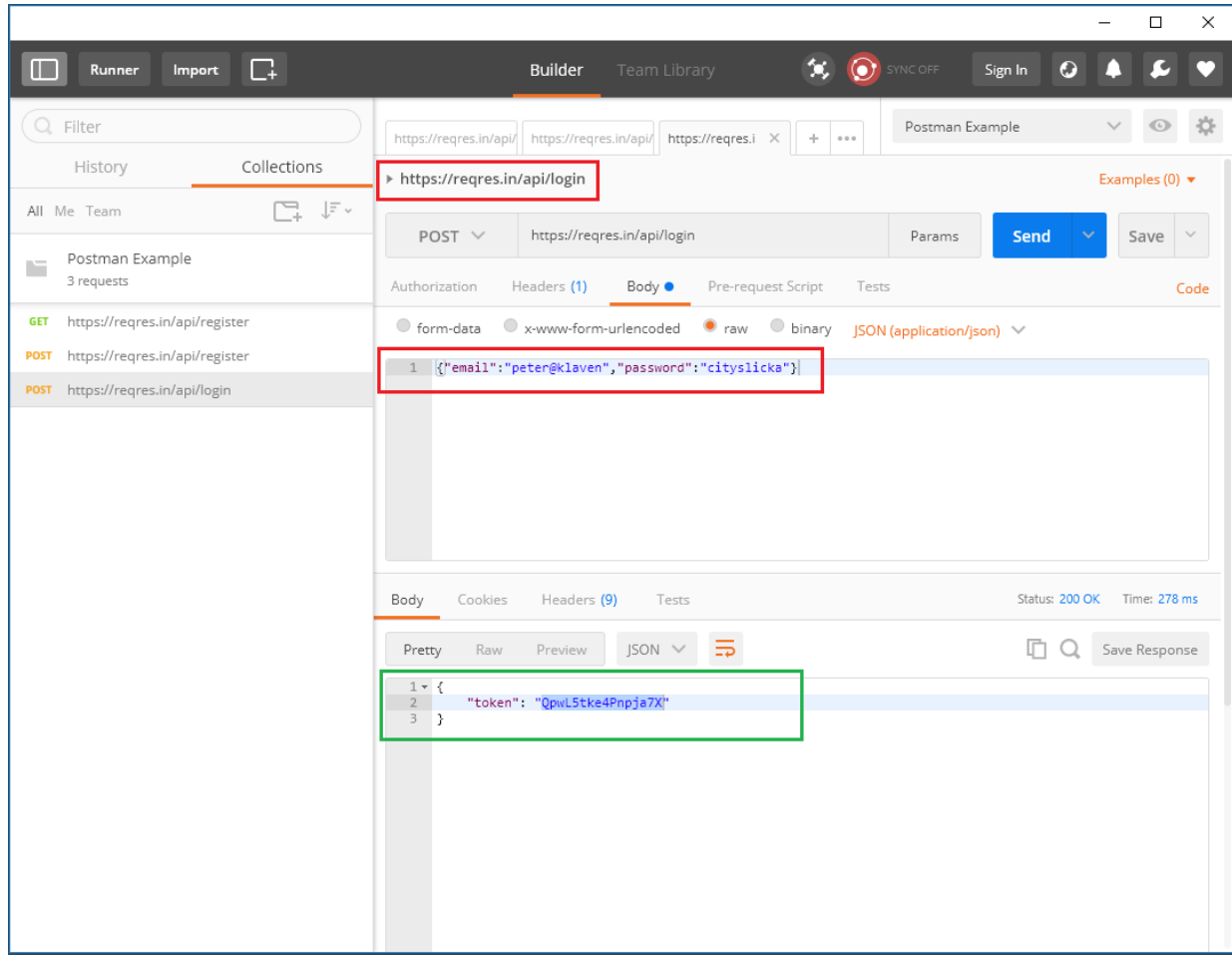
The following examples show project files with working sample data.

**Note:** Only input parameter values need to be provided—the responses are shown here for information only.

### Example 1 (REST)

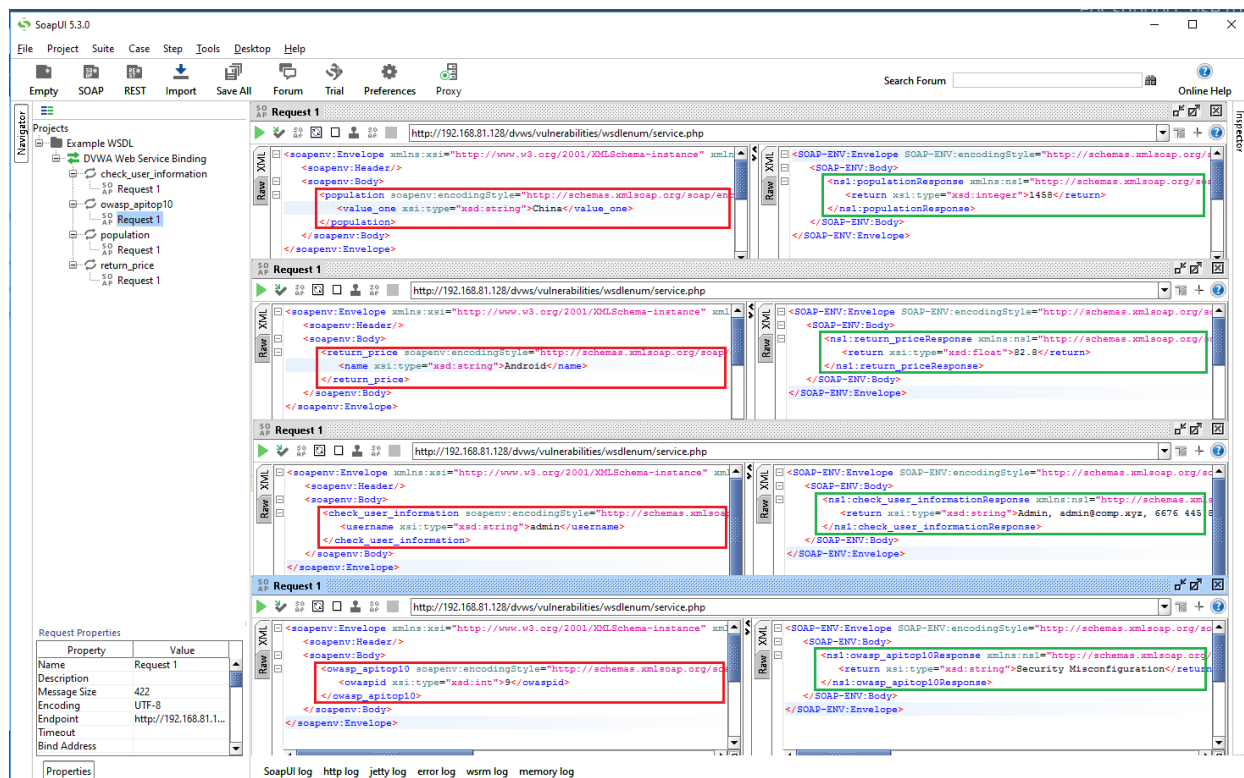
The following example shows a RESTful API endpoint that has been loaded in the Postman UI. The endpoint handles authentication for an application. The screen shows a request with the correct username and password input values (framed in red) and the response from the application (framed in green).





### Example 2 (SOAP)

The following example shows a WSDL file that has been loaded in the SOAPUI UI and updated with working parameter values. The screen shows four requests with the correct input values (framed in red) and the corresponding responses from the web service (framed in green).



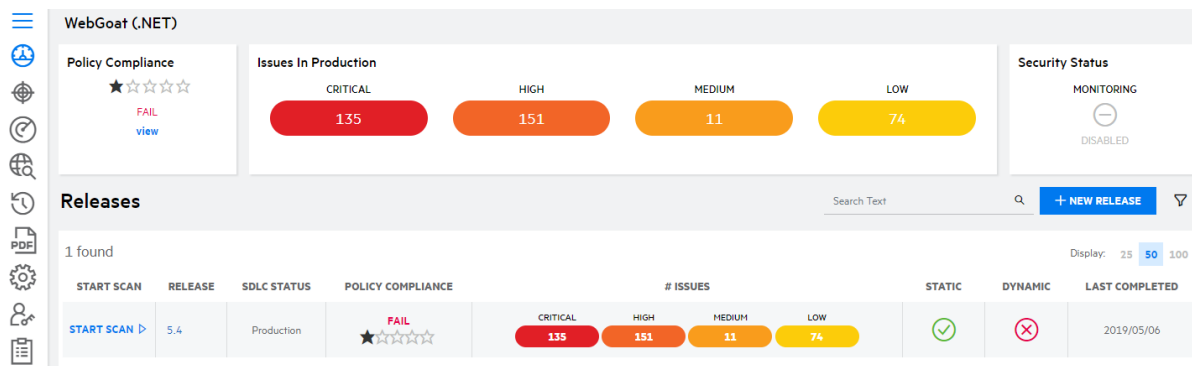
## Configuring a Dynamic Scan

After preparing your website for a dynamic assessment, you need to complete the Dynamic Scan Setup page. You only need to configure the dynamic scan settings once per release as the settings are carried over to the next scan. You can edit settings as needed for subsequent assessments.

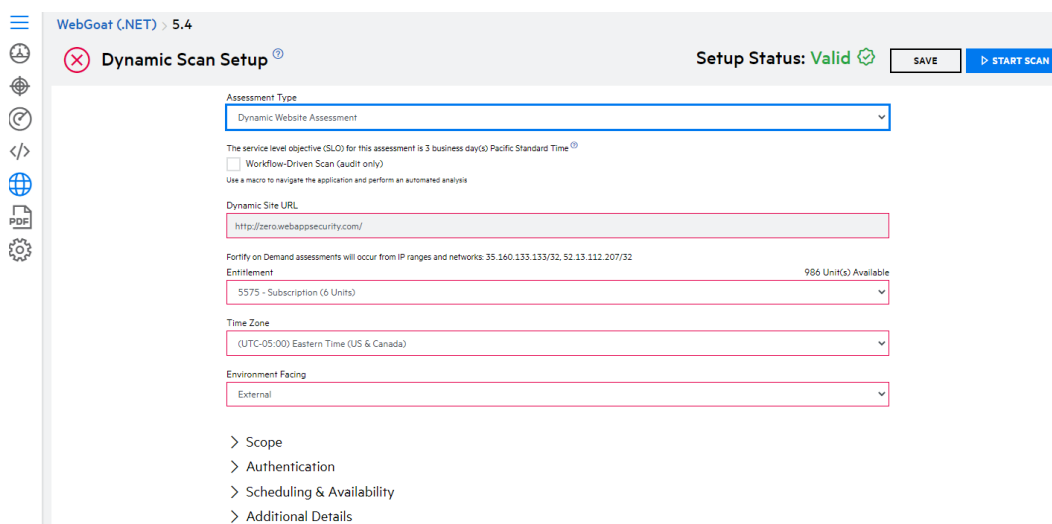
**Note:** Dynamic scan settings prior to 22.4 were saved at the application level. Save or update existing dynamic scan settings to have them saved at the release level.

To configure a dynamic scan:

1. Select the Applications view.  
Your Applications page appears.
2. Click the name of the application.  
The Application Overview page appears.



3. Click **Start Scan** for the release that you want to have assessed and select **Dynamic**. The Dynamic Scan Setup page appears.



4. Complete the required fields. All other fields are optional or set to default values.

Field	Description
Assessment Type	Select the assessment type. Only assessment types allowed by the organization's security policy are displayed.  The SLO of the selected assessment type appears below the field.  <b>Note:</b> The <b>Dynamic+ API</b> assessment is used for testing a web API where an OpenAPI definition or Postman collection is not available.
Workflow-Driven Scan (audit only)	(Optional, Dynamic Website) Select the check box to add a workflow macro and run the scan as a Workflow-Driven Scan. A Workflow-Driven Scan uses the audit only mode (no crawling) and is completely automated. Fortify WebInspect audits only those URLs recorded in the macro and does not follow any hyperlinks encountered during the audit. Supported macros are

Field	Description
	.webmacro files, Burp Proxy captures, and .har files. <b>Note:</b> The application being scanned must be external facing. Activity recorded in a macro overrides other scan settings.
Dynamic Site URL	(Dynamic Website, Dynamic+ Website, and Dynamic+ API assessments) Type your site's URL.
Entitlement	Select the entitlement that the assessment will use. The field displays entitlements that are valid for the selected assessment type, including those available for purchase. If the release has an active subscription, only options that do not consume entitlements are displayed.
Time Zone	Select your location's time zone, which is used to schedule the scan's start time.
Environment Facing	Select whether the site is internal or external.

- If needed, you can configure additional scan settings in the sections appearing below the required fields. The sections that are available depend on the assessment type selected.

### Scope (Dynamic Website, Dynamic+ Website, Dynamic+ API)

To edit the scope of the scan, click **Scope** and complete the fields as needed.

∨ Scope

Fortify on Demand may scan the entire host of the designated URL. Other domains and subdomains will not be scanned during the assessment.

Scan entire host (snas.nbcuni.com)  Restrict scan to URL directory and subdirectories <sup>?</sup>

Allow HTTP (:80) and HTTPS (:443)

Allow form submissions during crawl <sup>?</sup>

Exclude URLs which contain

 +

Include subdomain URLs

 +

Field	Description
Scan entire host (<URL>)	Select one of the following options: <ul style="list-style-type: none"> <li><b>Scan entire host (&lt;URL&gt;)</b> (default): the entire host will be scanned</li> </ul>

Field	Description
<p>Restrict scan to URL directory and subdirectories</p>	<p><b>Example:</b> Given https://foo.com/home, the following URLs will be included:</p> <ul style="list-style-type: none"> <li>○ https://foo.com/</li> <li>○ https://foo.com/contact-us.html</li> <li>○ https://foo.com/folder/</li> <li>○ https://foo.com/folder/folder2/page.aspx</li> <li>○ https://foo.com/home/folder/</li> <li>○ https://foo.com/home/index.html</li> </ul> <ul style="list-style-type: none"> <li>• <b>Restrict the scan to the URL directory and subdirectories:</b> only the directory denoted by the last slash in the URL and its subdirectories will be scanned. <b>If you select this option, make sure the last slash denotes the directory to which you want the scan to be restricted.</b></li> </ul> <p><b>Example:</b> Given https://foo.com/home/, the following URLs will be excluded:</p> <ul style="list-style-type: none"> <li>○ https://foo.com/</li> <li>○ https://foo.com/folder/</li> <li>○ https://foo.com/contact-us.html</li> <li>○ https://foo.com/folder/folder2/page.aspx</li> </ul>
<p>Allow HTTP (:80) and HTTPS (:443)</p>	<p>Select the check box to allow both HTTP and HTTPS scanning of the site (default).</p> <p><b>Example:</b> Given https://foo.com/home, if the <b>Scan entire host</b> option is selected, http://foo.com/ and its subdirectories will be included. If the <b>Restrict scan to URL directory and subdirectories</b> option is selected, only http://foo.com/home and its subdirectories will be included.</p>
<p>Allow form submissions during crawl</p>	<p>Select this option to allow form submissions during the crawl of the site (default). This uncovers additional application surface area that can then be examined for a more thorough scan.</p> <p>Deselecting this option does <b>not</b> prevent form submissions during vulnerability checks. Detection of many critical vulnerabilities, such as SQL injection and cross-site scripting, requires form submissions. To exclude</p>

Field	Description
	specific web functionalities from form submissions, specify those URLs in the <b>Exclude URLs that contain</b> field.
Exclude URLs that contain	<p>(Optional) Type a full or partial URL and click <b>+</b> to exclude URLs matching the string from being scanned. Add a new entry for each string. The field is not case-sensitive.</p> <p><b>Example:</b> https://foo.com/login.html, login.html</p>
Include URLs	<p>(Optional, Dynamic+ Website assessment) By default, Fortify on Demand does not scan URLs outside the provided top-level domain. To audit resources linked to the <b>Dynamic Site URL</b> domain, such as subdomains, APIs, and offsite resources, type the URL and click <b>+</b>. Add a new entry for each additional URL.</p> <p>Do not include URLs that are under the <b>Dynamic Site URL</b> domain, offsite domains, or third party applications.</p> <p><b>Example:</b> Given https://foo.com/home, valid URLs include:</p> <ul style="list-style-type: none"> <li>• www.foo.com (subdomain)</li> <li>• API.aws.com (API)</li> <li>• authfoo.com/login</li> <li>• api.foo.com</li> <li>• api.foo2.com</li> </ul>

### Scope (Dynamite Website with Workflow-Driven Scan)

To edit the scope of the scan, click **Scope**. A list of the hosts defined in the workflow macro appears. Select the hosts that will be scanned.

∨ Scope

When a macro runs it has a number of URLs that it pulls from that may not be obvious when building the macro. For example, each time an advertisement is shown on a page an external URL is associated with that advertisement. If you wanted your scan to execute checks against that site you would indicate that host name as an allowed host below

zero.webappsecurity.com:80  zero.webappsecurity.com:443

### (Authentication (Dynamic Website, Dynamic+ Website, Dynamic+ API)

To edit the authentication settings, click **Authentication** and complete the fields as needed.

▼ Authentication

Forms Authentication Required

Primary Username  Primary Password

Secondary Username  Secondary Password

Network Authentication Required

Additional Authentication Instructions

Field	Description
Form Authentication	(Optional) Select the check box if form authentication is required. Provide user names and passwords for at least two users. To add more credentials, use the <b>Additional Notes</b> field at the bottom of this form.
Network Required	(Optional) Select the check box if network authentication is required and provide a username and password.
Additional Authentication Instructions	(Optional) Select the check box if additional authentication is required, such as an account number or tenant code, and type instructions.  <b>Important!</b> Fortify on Demand does not support multi-factor authentication. Examples include authentication controls involving SMS messages, email verifications, CAPTCHA, OATH Tokens, and physical tokens.

**APIs (Dynamic API)**

For information on preparing web API project files suitable for automated testing, see "[Preparing Web API Files](#)" on page 115.

- To add instructions for scanning web APIs utilized by the site, click **APIs**.
- Select the API definition type: **Postman Collection (File)**, **Postman Collection (URL)**, **OpenAPI (File)**, **OpenAPI (URL)**.

**Note:** OpenAPI Specification versions 2.0 and 3.0 are supported.

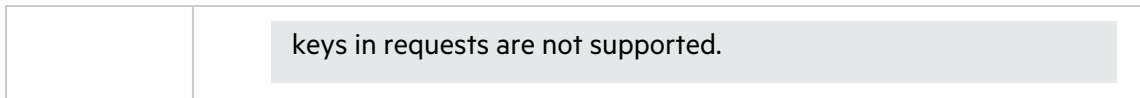
- Perform the relevant task based on your API definition type:

API Definition Type	Procedure

<p>Postman Collection (File)</p>	<p>∨ APIs</p> <p>To help ensure quality results and avoid paused scans, please review the detailed instructions for API assessments. ⓘ</p> <p>API Type</p> <p>Postman Collection (File)</p> <p>Please upload the Postman collection</p> <p>... <input type="button" value="UPLOAD"/></p> <p>Additional Instructions</p> <p>Describe required headers, tokens, authentication mechanisms, etc.</p> <p>i. Click ... and browse to and select the Postman collection file. The JSON file format is accepted. If a file already exists, you can use the existing file or upload a new file.</p>
<p>Postman Collection (URL)</p>	<p>∨ APIs</p> <p>To help ensure quality results and avoid paused scans, please review the detailed instructions for API assessments. ⓘ</p> <p>API Type</p> <p>Postman Collection (URL)</p> <p>Please provide a URL to the Postman collection</p> <p>Must use SSL with hostname</p> <p>Header Name <input type="text"/> Header Value (Leave Empty If Unchanged) <input type="text"/></p> <p>Additional Instructions</p> <p>Describe required headers, tokens, authentication mechanisms, etc.</p> <p>i. Provide the Postman collection URL.</p> <p>ii. If authentication is needed to access the URL, provide the header name in the <b>Header Name</b> and the credentials in <b>Header Value</b> fields. For example, provide Authorization in <b>Header Name</b> and Bearer &lt;token&gt; in <b>Header Value</b>. Not that this is separate from the credentials used to authenticate requests.</p> <p>Examples:</p> <pre>X-API-Key: &lt;apikey&gt; Authorization: &lt;apikey&gt; Authorization: Bearer &lt;token&gt;</pre> <p><b>Note:</b> If the credentials are passed as a query parameter, include</p>



	<p>it in the URL.</p>
OpenAPI (File)	<p>∨ APIs</p> <p>To help ensure quality results and avoid paused scans, please review the detailed instructions for API assessments. ⓘ</p> <p>API Type</p> <p>OpenAPI (File) ▾</p> <p>Please upload your OpenAPI specification json file</p> <p>... <input type="button" value="↑, UPLOAD"/></p> <p>API Key</p> <p>Additional Instructions</p> <p>Describe required headers, tokens, authentication mechanisms, etc.</p> <ol style="list-style-type: none"><li>i. Click ... and browse to and select the OpenAPI document file. The JSON file format is accepted. If a file already exists, you can use the existing file or upload a new file.</li><li>ii. If the API requires authentication, provide the API key value in the <b>API Key</b> field.</li></ol> <p><b>Note:</b> The supported security scheme is API key. Multiple API keys in requests are not supported.</p>
OpenAPI (URL)	<p>∨ APIs</p> <p>To help ensure quality results and avoid paused scans, please review the detailed instructions for API assessments. ⓘ</p> <p>API Type</p> <p>OpenAPI (URL) ▾</p> <p>Please provide a URL to your OpenAPI specification</p> <p>Must use SSL with hostname</p> <p>API Key</p> <p>Additional Instructions</p> <p>Describe required headers, tokens, authentication mechanisms, etc.</p> <ol style="list-style-type: none"><li>i. Provide the OpenAPI document URL.</li><li>ii. If the API requires authentication, provide the API key value in the <b>API Key</b> field.</li></ol> <p><b>Note:</b> The supported security scheme is API key. Multiple API</p>



d. In the **Additional Instructions** field, type additional instructions.

### APIs (Dynamic+ API)

For information on preparing web API project files suitable for automated testing, see "[Preparing Web API Files](#)" on page 115.

To add instructions for scanning web APIs utilized by the site, click **APIs** and complete the fields as needed.

APIs  
To help ensure quality results and avoid paused scans, please review the detailed instructions for API assessments. ⓘ

API Type

Please provide a project file that contains working sample data to describe the SOAP endpoints. SOAP UI WSDL file, Postman, or other API definition files are required for our team to understand and effectively test the application.

Additional Instructions

Username  Password

API Key  Password

Field	Description
API Type	a. Select the web API type: <b>SOAP, REST</b> . b. Upload a project file, such as a WSDL file or API definition file, that contains working sample data. The JSON, WSDL, TXT, and XML file formats are accepted.
Additional Instructions	(Optional) Type additional instructions, such as required headers, tokens, or authentication mechanisms.
Username, Password API Key, Password	(Optional) Provide the username and password or API key and password.

## Scheduling & Availability (all assessments)

To edit the scan frequency and site availability settings, click **Scheduling & Availability** and complete the fields as needed.

✓ Scheduling & Availability

Repeat Frequency ⓘ  
(Do not repeat) ▼

Site Availability

DAY	ALL DAY	MIDNIGHT TO 4AM <input type="checkbox"/>	4AM TO 8AM <input type="checkbox"/>	8AM TO 12PM <input type="checkbox"/>	12PM TO 4PM <input type="checkbox"/>	4PM TO 8PM <input type="checkbox"/>	8PM TO MIDNIGHT <input type="checkbox"/>
Sunday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tuesday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wednesday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thursday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Friday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Saturday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fortify on Demand can work according to your sites availability restrictions. However, decreasing the scan window will cause the scan to take longer than the typical SLA.

Field	Description
Repeat Frequency	<p>Select the scan's repeat frequency: <b>Do not repeat</b> (default), <b>2 weeks, 1 month, 2 months, 3 months, 4 months, 6 months, 12 months</b>. If you are requesting a single scan, keep the default value.</p> <p>Scheduled recurring scans are automated and subjected to the following stipulations:</p> <ul style="list-style-type: none"> <li>• Scheduling of a scan occurs seven days before the calculated scan date, which is determined by the start date of the previous scan and the repeat frequency. For example, if a monthly scheduled scan starts on the 5th of the month, the next scan will be scheduled for the 5th of the next month.</li> <li>• The entitlement is deducted at the time of scheduling.</li> <li>• A scan will only be scheduled if a valid entitlement for the selected assessment type exists at the time of the scheduling.</li> <li>• If a scan is canceled, no further scans will be scheduled.</li> <li>• If a scan is still in progress when the next scan is to be scheduled, Fortify on Demand will attempt once a day to reschedule the next scan until the scan date has passed. For example, if a monthly scheduled scan that starts on the 5th of the month is still in progress by the 5th of the next month, the next rescheduling attempt will take place seven days before the 5th of the</li> </ul>

Field	Description
	month after that.
Site Availability	Select the check boxes to indicate when the environment is available for testing. Use the local time of the time zone specified above. You must provide a minimum of a four hour window of availability during the week.  Pausing and resuming testing causes the scan to take longer than the standard SLO. Contact the support team for more information if you have site availability constraints.

### Additional Details (Dynamic Website, Dynamic+ Website, Dynamic+ API)

To add additional details about the scan, click **Additional Details**.

#### Additional Details

User Agent

Desktop browser  Mobile browser

Concurrent Request Threads ⓘ

Standard  Limited

Additional Notes

Adding additional notes or files requires manual review and leads to longer turnaround times.

Additional Documentation

...
📁 UPLOAD

Upload additional documentation/information (30MB limit)

Uploaded Files

There are no items to display.

Generate WAF Virtual Patch

Request pre-assessment conference call

Field	Description
User agent	Select the user agent type that will be used for the site: <b>Desktop browser</b> (default), <b>Mobile browser</b>
Concurrent request threads	Select the number of concurrent requests that will be used for the scan: <ul style="list-style-type: none"> <li><b>Standard</b> (default): 5 crawl requestor threads, 10 audit requestor threads, 20 second request timeout</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <b>Limited:</b> 2 crawl requestor threads, 3 audit requestor threads, 5 second request timeout</li> </ul> <p>Selecting the <b>Limited</b> option will reduce the scan load but will also cause the scan to take longer than the standard SLO.</p>
Additional Notes	<p>(Optional) Type additional information that the testing team needs to know before starting the assessment.</p> <p><b>Note:</b> Free form exclusions and whitelist notes have been migrated to this field.</p>
Additional Documentation	<p>(Optional) Upload documentation (30 MB limit) that facilitates testing of the application. Uploaded files are displayed in the <b>Uploaded Files</b> section below.</p> <p>Supported file types: DOC, DOCX, PPT, TXT, PDF, PPTX, ZIP, XLS, XLSX, CSV.</p>
Generate WAF Virtual Patch	<p><b>Note:</b> Contact support to enable the WAF feature.</p> <p>(Optional) Select the checkbox to generate an export of vulnerabilities to a web application firewall (WAF). The export is an XML file and is compatible with the following WAFs: Imperva and F5. Once the assessment is complete, you can download the file on the Scans page</p>
Request pre-assessment conference call	<p>(Optional, Dynamic Premium and Dynamic+ assessments) Select the check box to request a pre-assessment conference call. The check box is cleared after the assessment is completed.</p> <p><b>Note:</b> You cannot request a pre-assessment conference call for a scan scheduled within 72 hours.</p>

- Once you have configured the scan settings, click **Save**.
  - If the form is complete, the **Setup Status** is marked as **Valid**.
  - If the form is incomplete, the **Setup Status** is marked as **Incomplete**. A list of the issues appears at the top of the page. You can hover over the **x** icon next to **Setup Status** to display the list.

## Submitting a Dynamic Assessment

You can submit a dynamic assessment using the following methods:

- Fortify AzureDevOps Extension  
For more information, see ["CICD Tool" on page 320](#).
- Fortify on Demand API  
For more information, see ["Fortify on Demand API" on page 306](#).
- Manually in the portal  
For more information, see ["Scheduling the Dynamic Scan Through the Portal" below](#).

## Scheduling the Dynamic Scan Through the Portal

Once you have completed the Dynamic Scan Setup, you can schedule the dynamic scan. You can only have one in progress dynamic scan across all releases of an application

To schedule a dynamic scan:

1. Click **Start Scan**.

**Note:** If the application has an active dynamic scan, you are blocked from starting another scan.

The **Start Dynamic Scan** window opens, displaying the current time and geolocation.

Start Dynamic Scan - http://zero.webappsecurity.com/

Start Date

2017/11/10 | 11:06 am

November 2017

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Time 11:06 am

Hour 11 am

Minute 06

NOW DONE

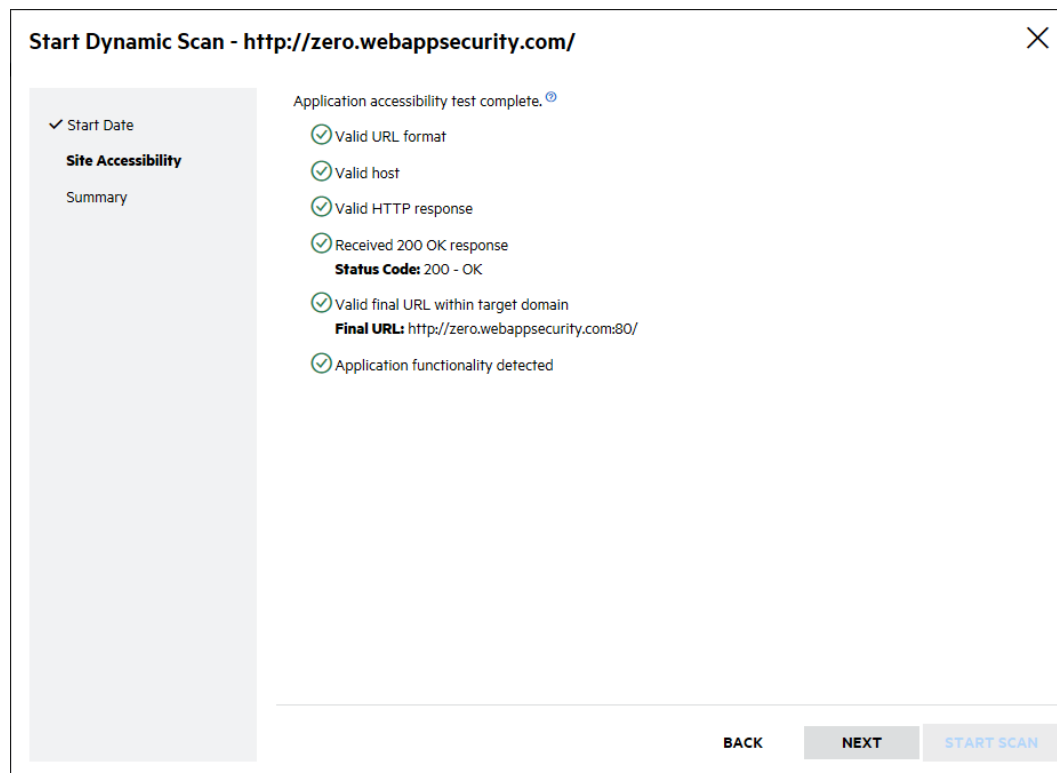
BACK NEXT START SCAN

2. Click the **Start Date** field.
  - Click **Now** to schedule a scan immediately.
  - Use the calendar to select a start date and time and click **Done**.

a. Click **Next**.

Results of a site accessibility check appears. The site accessibility check looks for the following criteria:

- The URL resolves.
- The DNS of the hostname resolves.
- Fortify on Demand receives a valid HTTP response.
- The server returns a valid response (the status code is listed).
- The final URL, if there are any redirects, is within the target domain (the final URL is listed).
- Whether the application has limited or complex application functionality (such as links , forms, or scripts).
- Whether updated credentials were provided if authentication is required.



Resolve any issues before starting your scan in order to prevent the assessment from being paused.

**Note:** The site accessibility check is not available for sites accessed through VPN.

3. Click **Next**.

A summary of the dynamic scan setup values appears.

**Start Dynamic Scan - http://zero.webappsecurity.com/**

✓ Start Date  
✓ Site Accessibility  
**Summary**

**Recurrence**  
No

**Time Zone**  
(UTC-05:00) Eastern Time (US & Canada)

**Environment Facing**  
External

**Scope**

**Restrict to Directory and Subdirectories**  
No

**Allow HTTP (:80) and HTTPS (:443)**  
Yes

**Allow form submissions**  
Yes

**Exclusions**  
No

**Scheduling & Availability**

**Repeat Frequency**  
(Do not repeat)

**Availability**  
Always

**Additional Details**

**WAF Virtual Patch**  
No

**Pre-Assessment Call**  
No

**Assessment Notes**  
(None)

By starting this assessment, you acknowledge authorization to perform a security assessment of the application. ⓘ

**BACK** **NEXT** **START SCAN**

4. Review the summary. If necessary, click **Back** and make any corrections. If the values are correct, click **Start Scan**.

Once the scan is started, the scan status changes to **Scheduled**. The scan will begin at your scheduled time. If you schedule recurring scans, the release will be scanned at the intervals you defined until you return to the **Dynamic Scan Setup** and change your request.

**Note:** Site availability restrictions can have a significant effect on the turnaround time. For example, you can expect a potential doubling of the testing window if you restrict the testing times to half the day. If you have any questions, create a Help Center ticket.

## Editing Dynamic Scan Settings

You can edit dynamic scan settings for scheduled scans that have not been started and paused scans. If you need to edit scan settings for an in progress scan, create a Help Center ticket to have the scan paused. The testing team will respond to the ticket.

The following fields cannot be edited after a dynamic scan has been scheduled:

- **Assessment Type.** Cancel the scan to edit the field.
- **Dynamic Site URL.** If the release does not have a completed scan, cancel the scan to edit the field. Otherwise, the field is locked (see the following explanation).

In addition, upon the successful completion of a dynamic scan, the following fields are set to values from the completed scan and locked for editing:



- **Dynamic Site URL**
- All fields in the **Scope** section
- Workflow-Driven Scan fields
- All fields in the **Authentication** section, with the exception of username and password fields.
- All fields in the **APIs** section, with the exception of username and password fields and uploaded project files.

To edit these fields, create another release using the copy state feature and reconfigure scan settings.

## Continuous Application Monitoring

Continuous Application Monitoring is included with any active dynamic subscription. Fortify on Demand performs lightweight dynamic scanning and risk profiling of an enrolled application at regular intervals. The automated, unauthenticated scans focus on OWASP Top 10 vulnerabilities and common environment or deployment issues. Fortify on Demand then provides a list of vulnerabilities and a detailed breakdown of the risk profile, enabling you to identify critically vulnerable applications that need immediate remediation.

This section contains the following topics:

### Configuring Application Monitoring

Continuous Application Monitoring is available with a dynamic assessment subscription. Users with the **Manage Applications** permission can configure Application Monitoring for an application.

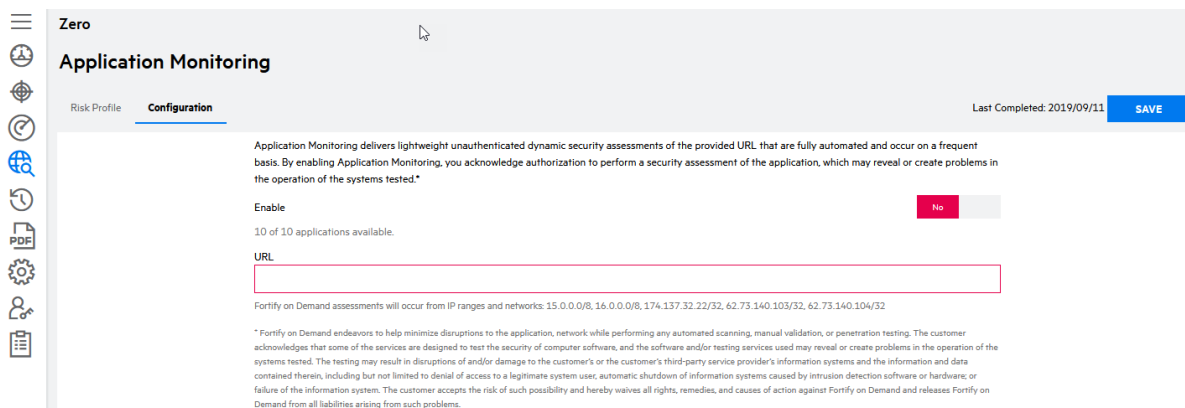
**Note:** An URL can have Application Monitoring enabled only once across all releases in an application.

To configure Application Monitoring:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of an application for which you want to enable application monitoring.
3. Click **Application Monitoring**.  
The Application Monitoring page appears.

**Note:** Users with the **View Applications** permission have view-only access.

4. Select the **Configuration** tab.

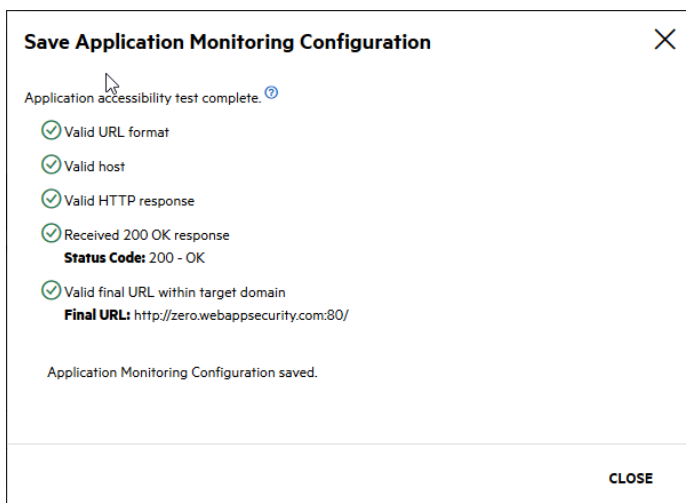


**Note:** Applications under dynamic subscriptions do not count towards the enrolled application quota.

5. Move the **Enable** slider from **No** to **Yes**.
6. In the **URL** field, type the URL that you are going to monitor.
7. Click **Save**.

If Application Monitoring is enabled, results of a site accessibility check appears. The site accessibility check looks for the following criteria:

- The URL resolves.
- The DNS of the hostname resolves.
- Fortify on Demand receives a valid HTTP response.
- The server returns a valid response (the status code is listed).
- The final URL, if there are any redirects, is within the target domain (the final URL is listed).



If any of the above fails, current Application Monitoring settings are not saved. Resolve all issues before configuring Application Monitoring.

8. Click **Close**.

Once Application Monitoring has been enabled, the URL will be scanned within the week. A scan will be cancelled if the site is not accessible at the time of the scan.

## Canceling an Application Monitoring Scan

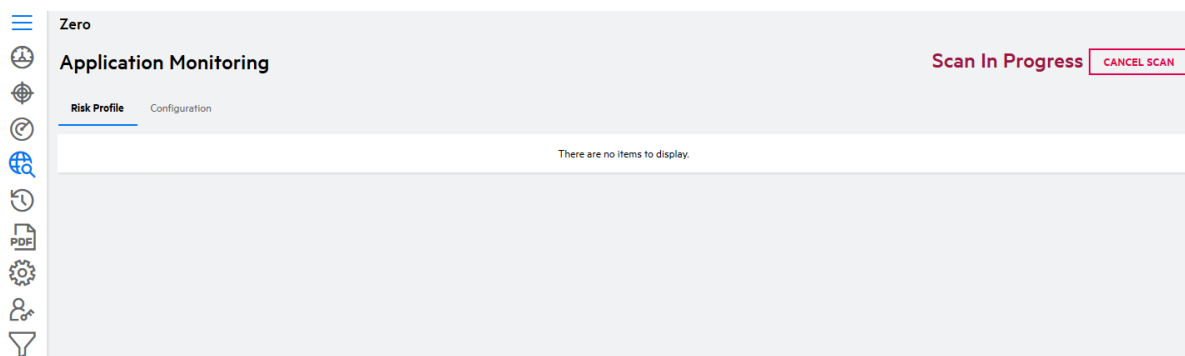
An in progress Application Monitoring scan is indicated by a **Scan In Progress** status on the top right of the Application Monitoring page. Users with the **Manage Applications** permission can cancel an in progress scan. An in progress scan is also automatically canceled when Application Monitoring is disabled.

You can cancel an Application Monitoring scan from the Your Scans or Application Scans page (see ["Canceling a Scan" on page 161](#)) or the Application Monitoring page (see below).

To cancel an in progress Application Monitoring scan:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of an application for that has an application monitoring scan in progress.
3. Click **Application Monitoring**.

The Application Monitoring page appears.



4. Click **Cancel Scan**.  
A confirmation message appears.
5. Click **Yes**.  
The in progress scan is cancelled.

**Note:** Cancelled Application Monitoring scans do not appear in any scan list.

## Viewing Application Monitoring Issues

You can view Application Monitoring issues on the Application Issues page, which displays issues at the application level. For more information on viewing application issues, see ["Viewing Application Issues" on page 166](#).

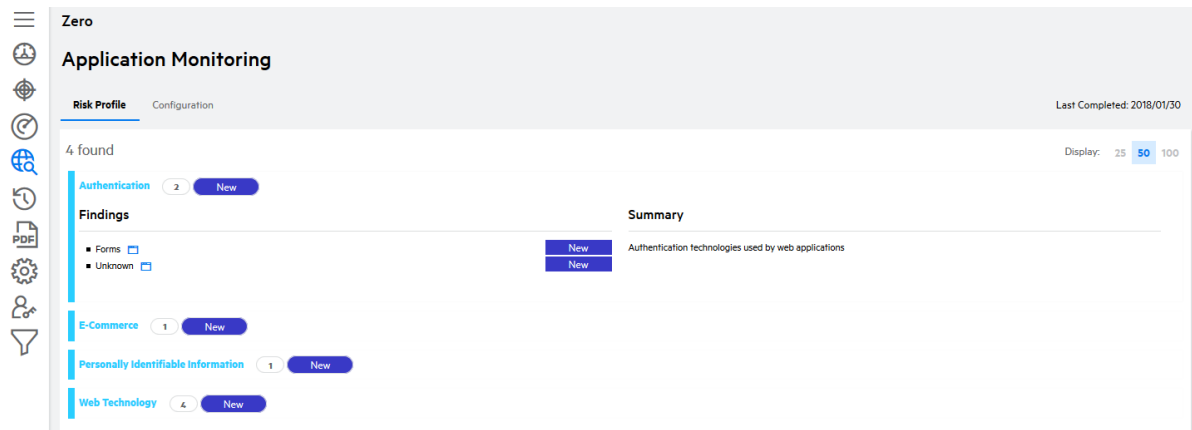
## Viewing Risk Profile Results

Risk profiling of an application searches for the following application characteristics: collection of personally identifiable information (PII), e-commerce functionality, authentication methods, and web technologies used in the application. You can view an application's risk profile from the most recent risk profile scan.

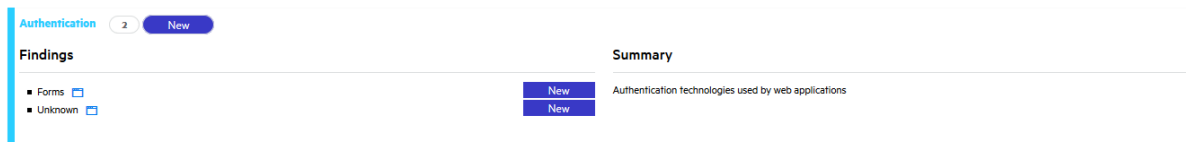
To view an application's risk profile:


1. Select the **Applications** view.  
Your Application page appears.
2. Click the name of an application that has Application Monitoring enabled and for which you want to view the risk profile.
3. Click **Application Monitoring**.

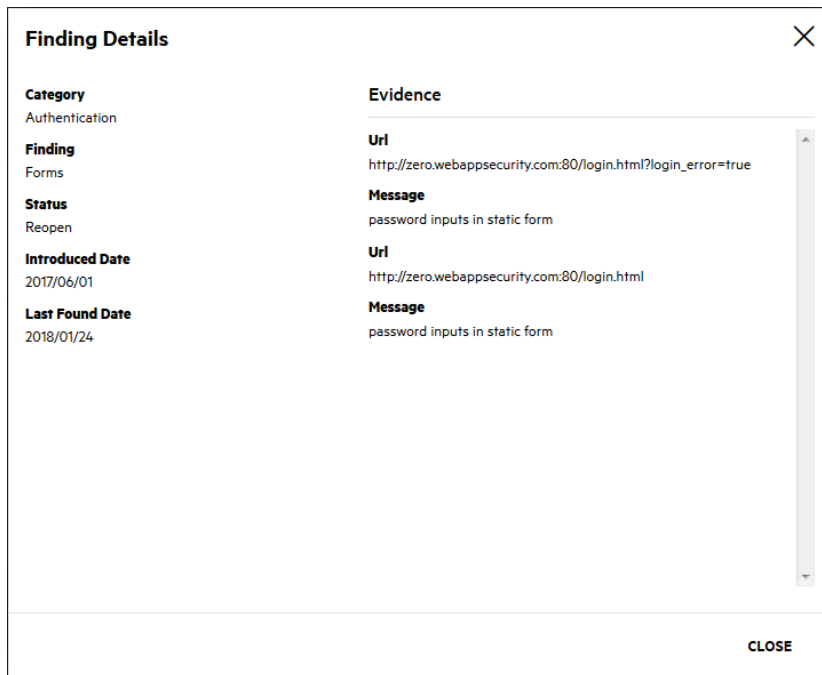
The Application Monitoring page appears. The **Risk Profile** tab displays the risk criteria found and the number of instances of each criterion.



4. Expand a risk criterion to view individual instances of that criterion.



5. Click  to open a window containing the instance details.



## Mobile Assessments

A mobile assessment tests a mobile application. It offers security testing across the client, the network, and the backend server. Fortify on Demand supports the following platforms: Android, iOS.

This section contains the following topics:

<a href="#">Supported Platforms and Operating Systems</a>	137
<a href="#">Mobile Assessment Preparation</a>	138
<a href="#">Configuring a Mobile Scan</a>	141
<a href="#">Submitting a Mobile Assessment</a>	145
<a href="#">Editing Mobile Scan Settings for an Ongoing Scan</a>	148

## Supported Platforms and Operating Systems

### Hardware Platforms

Fortify on Demand supports the following hardware platforms:

	<b>Mobile</b>	<b>Mobile+</b>
Phone (small format)	N/A	Yes
Tablet (large format)	N/A	Yes
SIM/cellular service	N/A	Yes
Hardware type (Apple Watch, Samsung Galaxy)	N/A	No

## Operating Systems and Architectures

Fortify on Demand supports the following operating systems and native architectures:

	<b>Mobile</b>	<b>Mobile+</b>
iOS version	N/A	Up to 15.7
Native iOS architecture	ARMv7, ARM64	ARMv7, ARM64
Android version	N/A	Up to Android 11
Native Android architecture	ARMv7, ARM64	ARMv7, ARM64

## Mobile Assessment Preparation

Before submitting your mobile assessment, you need to prepare your application for mobile testing. The number of tasks in the preparation process depends on the assessment type that is used for the application.

This section contains the following topics:

<a href="#">Preparing Mobile Assessment Files</a> .....	138
<a href="#">Preparing the Backend for Mobile Testing</a> .....	140

### Preparing Mobile Assessment Files

The first step in a mobile assessment is to prepare your mobile application's binary file for upload to Fortify on Demand. To ensure an effective analysis of the mobile application, prepare your files according to the instructions that are provided for the framework of the mobile application.

<a href="#">Preparing Android Application Files (Binary)</a> .....	139
<a href="#">Preparing iOS Application Files (Binary)</a> .....	139

## Preparing Android Application Files (Binary)

For Android applications, prepare your application's binary (.aab or .apk) file according to the following instructions:

- Make sure the application does not require MDM features.
- Provide the binary file in its entirety. Since only the submitted file is tested, features that require application updates are not supported.
- For assessments that include on-device testing (Mobile+), make sure that the submitted application can be installed and run on a physical device.
- To facilitate testing for Mobile+ assessments, disable any root detection, application tampering, or certificate pinning mechanisms. Leaving in these features might result in testing limitations that impact scan coverage.
- Mobile+ assessment of AAB files supports dynamic feature modules that have `<dist:fusing dist:include="true" />` specified in the manifest.
- **Important!** If you are submitting a subsequent scan of an application, either as a remediation scan or as a new scan, Fortify recommends keeping the application identifier (the package name) consistent in order to preserve the integrity of issue tracking between scans. The application identifier is used to calculate issue identifiers that track unique issues. Changing the application identifier between scans will result in many pre-existing issues showing up as “New” instead of “Existing” in the scan results.

### Related Topics:

For information on uploading Android files for static assessments, see ["Preparing Android Application Files \(Source Code\)" on page 105](#).

## Preparing iOS Application Files (Binary)

For iOS applications, prepare your application's binary (.ipa) file according to the following instructions.

- For assessment that include on-device testing (Mobile+), make sure that the submitted application can be installed and run on a physical device.
- To facilitate testing for Mobile+ assessments, disable any application tampering or certificate pinning mechanisms. Leaving in these features might result in testing limitations that impact scan coverage.
- Make sure the application does not require MDM features.
- Export the application for submittal using the following supported distribution types:
  - App Store submittal (the IPA must contain executable code, so make sure the **Include bitcode** checkbox is cleared when exporting the application)
  - Ad Hoc

- Enterprise
- Development

**Important!** The following distribution types are NOT supported:

- IPA download from the App Store. The IPA is encrypted to the user who downloaded it.
- App Store submittal with the "Include bitcode" setting. The IPA does not contain executable code.

Since only the submitted file is tested, features that require application updates are not supported.

**Note:** If you are submitting a subsequent scan of an application, either as a remediation scan or as a scan of a new version, Fortify recommends keeping the application identifier (the bundle identifier) consistent in order to preserve the integrity of issue tracking between scans. The application identifier is used to calculate issue identifiers that track unique issues. Changing the application identifier between scans will result in many pre-existing issues showing up as “New” instead of “Existing” in the scan results.

### Related Topics:

For information on preparing iOS source code files for upload, see ["Preparing iOS Application Files \(Source Code\)" on page 105](#).

## Preparing the Backend for Mobile Testing

For mobile assessments that include backend, web application testing, make the following preparations to facilitate the testing process:

- Confirm that your web application and/or user credentials are functioning before the assessment.
- Complete all functional and performance testing before the assessment and freeze your application's code for the duration of the security test engagement.
- As a standard precaution, Fortify recommends that you back up all of your data before beginning the testing process. When testing is complete, restore your data from a backup that is known to be good to avoid any chance of data corruption.
- The web application must be publicly accessible. Fortify on Demand does not support scanning over VPNs.
- Add the Fortify on Demand IP addresses to the allow list in firewalls, IPS, IDS and WAFs to ensure the application can be scanned by the mobile testing team. You can obtain the IP addresses from the Mobile Scan Setup page in the portal. Adhoc addresses may be used with your consent only when conditions necessitate it.
- Provide the Fortify on Demand IP addresses to your security operations and network operations teams, so they know not to block the IP addresses if they see attacks being submitted against the site, which are part of planned recurring security scanning.



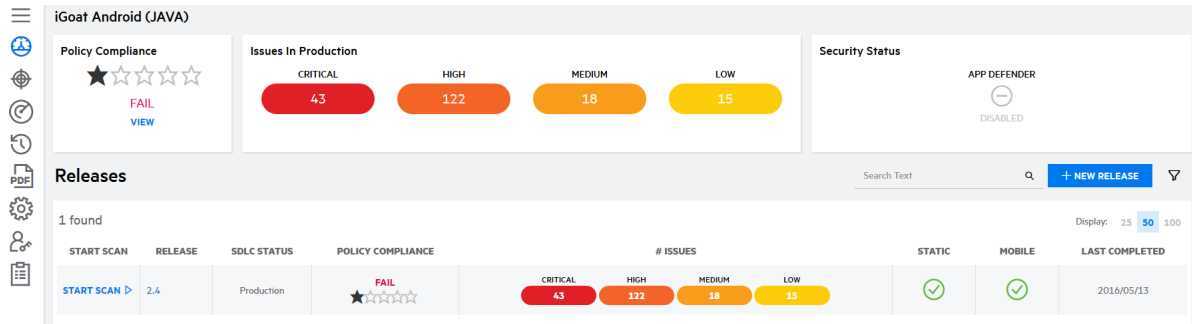
**Note:** As long as your website is accessible through the http/https default ports (80/443), you do not need to open any additional ports for the assessment.

## Configuring a Mobile Scan

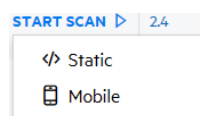
If this is the first time you are submitting a mobile assessment for a release, you need to complete the Mobile Scan Setup page. You only need to complete the page once per release as the settings are carried over to the next scan. You can edit settings as needed for subsequent assessments.

To set up a mobile scan:

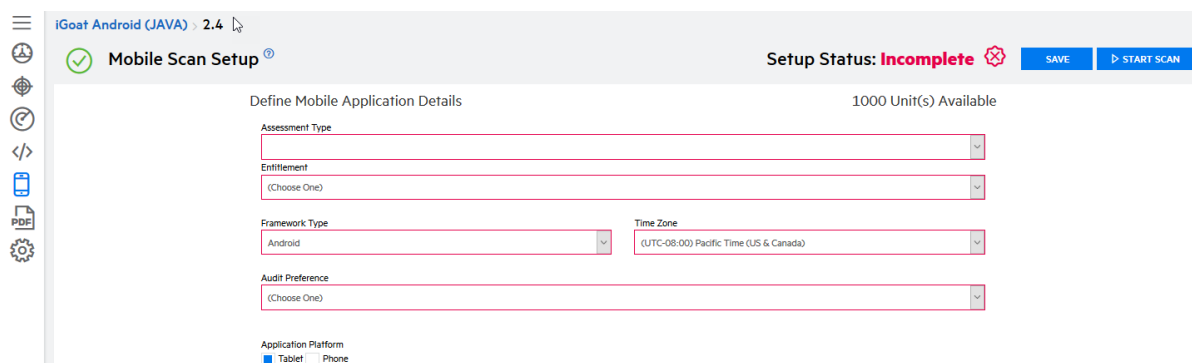
1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application.  
The Application Overview page appears.



3. Click **Start Scan** for the release that you want to have assessed and select **Mobile** from the menu.



The Mobile Scan Setup page appears.



4. Complete the fields as needed. Fields are required, unless otherwise noted.

Field	Description
Assessment Type	Select the assessment type. Only assessment types allowed by the organization's security policy are displayed.  The SLO of the selected assessment type appears below the field.
Entitlement	Select the entitlement that the assessment will use. The field displays entitlements that are valid for the selected assessment type, including those available for purchase. If the release has an active subscription, only options that do not consume entitlements are displayed.
Framework Type	Select the mobile OS: <b>iOS, Android, Windows</b> (Premium assessments only)
Time Zone	Select your location's time zone, which is used to schedule the scan's start time.
Audit Preference	Select the audit preference. The value is fixed at <b>Manual</b> for Mobile Standard, Mobile Premium, and Mobile+ assessments.  <b>Automatically publish (no audit)</b> - The scan results are automatically published upon scan completion.  <b>Manual</b> – The scan results are reviewed by auditors before being published.
Application Platform	(Optional) Select your application's preferred platform: <b>Phone</b> and/or <b>Tablet</b>

- If needed, you can configure additional scan settings in the sections appearing below the required fields. The sections that are available depend on the assessment type selected.

#### **Authentication (Mobile Standard, Mobile Premium, and Mobile+)**

To edit the authentication settings, complete the fields as needed in the **Authentication** section.

Authentication

Authentication Required

Multi-Factor Authentication

Field	Description
Authentication	(Optional) Select the check box if authentication is required and enter user names and passwords of at least two users. To add more credentials, use the <b>Add additional [...] notes</b> field at the bottom of this form.

Multi-Factor Authentication	(Optional) Select the check box if multi-factor authentication is required and specify the details of your multi-factor authentication.
-----------------------------	---

### APIs (Mobile Standard, Mobile Premium, and Mobile+)

To add details about web APIs, complete the fields as needed in the **APIs** section.

#### Web Services

Access to Web Services

#### Exclusions

Example URL: mail.google.com, Example Note: The shopping cart checkout function connects to the production servers. Please do not test.

Web service scanning is limited to first party controlled sites. Third party endpoints (such as Salesforce or Google Analytics) will not be tested without written approval from the endpoint owners.

Fortify on Demand assessments will occur from IP ranges and networks: 15.0.0.0/8, 16.0.0.0/8, 174.137.32.22/32, 62.73.140.103/32, 62.73.140.104/32

#### Environment Availability

DAY	ALL DAY	MIDNIGHT TO 4AM	4AM TO 8AM	8AM TO 12PM	12PM TO 4PM	4PM TO 8PM	8PM TO
Sunday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tuesday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wednesday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thursday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Friday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Saturday	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fortify on Demand can work according to your sites availability restrictions. However, decreasing the scan window will cause the scan to take longer than the typical SLA.

Field	Description
Access to APIs	(Optional) Select the check box to allow Fortify on Demand to scan web APIs utilized by the application.
Exclusions	(Optional) List websites, backend web services, web APIs, or internal services the application talks to via HTTP/HTTPS that are to be excluded during the scan. This gives the testing team the correct context and boundaries for conducting the scan; domains not excluded that are discovered may be classified as vulnerabilities.
Environment Availability	Select the check boxes to indicate when the environment is available for testing. Use the local time of the time zone you specified above.

Pausing and resuming testing causes the scan to take longer than the standard SLA typically allocated for a scan. Contact the support team for more information if you have site availability constraints.

**Note:** Application modifications during blackout periods introduce uncertainty in the findings.

### Additional Documentation (Mobile Standard, Mobile Premium, and Mobile+)

To add additional details about the scan, complete the fields as needed in the **Additional Documentation** section.

#### Additional Documentation

Upload Additional documentation/information (30MB limit)

...

Add additional application and assessment notes

List any special requirements for testing this application such as: requires sim card, requires a working phone number, location restrictions, certificate pinning details, root/jailbreak enforcement, etc.

Request pre-assessment conference call

#### Uploaded Files

NAME	CREATED
There are no items to display.	

Field	Description
Upload additional documentation/information (30MB limit)	(Optional) Upload documentation (30 MB limit) that facilitates testing of the application. Uploaded files are displayed in the <b>Uploaded Files</b> section below.  Supported File types: DOC, DOCX, PPT, TXT, PDF, PPTX, ZIP, XLS, XLSX, CSV.
Add additional application and assessment notes	(Optional) Add any more information that the testing team needs to know to successfully build your application.
Request pre-assessment conference call	(Optional, Premium and Mobile+ assessments only) Select the check box to request a pre-assessment conference call. The check box is cleared after the assessment is completed.  <b>Note:</b> You cannot request a pre-assessment conference call for a scan scheduled within 72 hours.

6. When you have completed the Mobile Scan Setup page, click **Save**.
  - If the form is complete, the **Setup Status** is marked as **Valid**.
  - If the form is incomplete, the **Setup Status** is marked as **Incomplete**. A list of the issues appears at the top of the page. You can also hover over the **x** icon next to **Setup Status** to display the list.

### Next Step:

["Scheduling the Mobile Scan Through the Portal" below](#)

## Submitting a Mobile Assessment

You can submit a mobile assessment using the following methods:

- Fortify on Demand API  
For more information, see ["Fortify on Demand API" on page 306](#).
- Manually in the portal  
For more information, see ["Scheduling the Mobile Scan Through the Portal" below](#).

### Scheduling the Mobile Scan Through the Portal

Once you have completed the Mobile Scan Setup, you can upload the payload and schedule the mobile scan. You can only have one in progress mobile scan across all releases of an application

To schedule a mobile scan:

1. Click **Start Scan**.

**Note:** If the application has an active mobile scan, you are blocked from starting another scan.

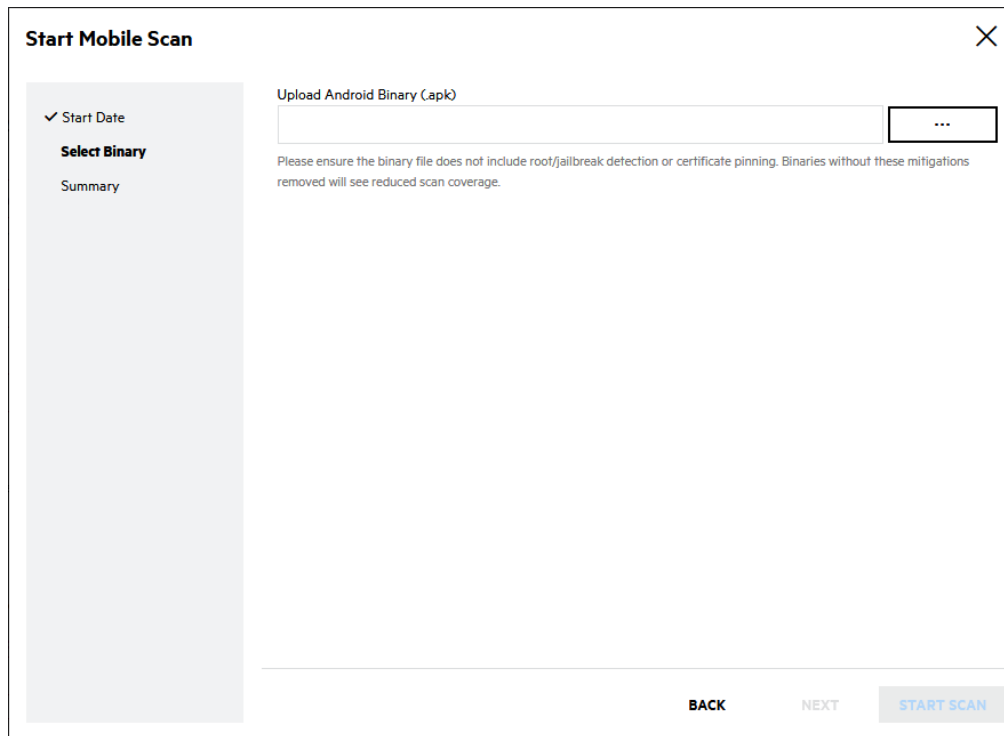
The Start Mobile Scan window opens.

The screenshot shows a mobile application dialog titled "Start Mobile Scan". On the left side, there is a vertical sidebar with three menu items: "Start Date", "Select Binary", and "Summary". The "Start Date" item is currently selected. The main content area displays the "Start Date" field with the value "2018/08/24 12:59 pm" and the time zone "(UTC-05:00) Eastern Time (US & Canada)". At the bottom of the dialog, there are three buttons: "BACK", "NEXT", and "START SCAN". The "START SCAN" button is highlighted in blue.

2. Click the **Start Date** field.
  - Click **Now** to schedule a scan immediately.
  - Use the calendar to select a start date and time and click **Done**.

**Note:** This step only applies to mobile scans that include backend testing.

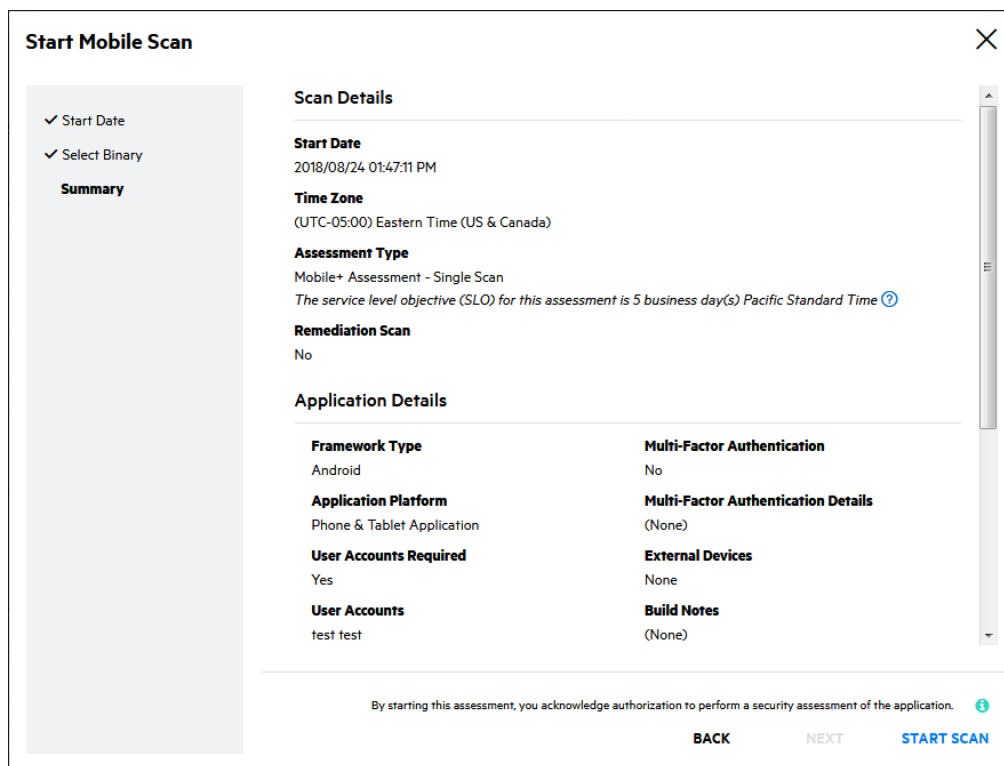
3. Click **Next**.  
The Submit Binary page appears.



4. Click ... and navigate to and select your binary file.

5. Click **Next**.

The Summary page appears.



6. Review the summary. If necessary, click **Back** and make any corrections. If the values are correct, click **Start Scan**.

Once the scan is started, the scan status changes to **Scheduled**. The scan will begin at your scheduled time.

#### **Mobile Scan Setup** <sup>2</sup>

**Note:** If you consumed a Premium Mobile entitlement, an associated static entitlement, named "<Mobile Premium Name> (Source)," is now available when you start a static scan.

## Editing Mobile Scan Settings for an Ongoing Scan

You can edit mobile scan settings for paused scans and scheduled scans that have not yet been started. Note that you cannot edit the **Assessment Type**, **Framework Type**, **Audit Preference**, and **Application Platform** fields. If you need to edit those fields, cancel the scan and resubmit the mobile assessment.

If you need to pause an in progress scan to edit the scan settings, create a Help Center ticket. The testing team will respond directly to the ticket with any updates. For more information on creating a Help Center ticket, see ["Submitting a Help Center Ticket" on page 413](#).

## Open Source Software Composition Analysis

Fortify on Demand offers open source software composition analysis in conjunction with static assessments. Applications are scanned using one of the following software composition analysis tools:

- Debricked
- Sonatype, in partnership with Fortify

The following languages are supported: C# (.NET), Go, Java, JavaScript, Kotlin, Objective-C, PHP, Python, Ruby, and Swift.

To enable open source scanning, purchase Debricked or Sonatype entitlements through Fortify on Demand. An entitlement is redeemed for an open source component analysis subscription per application. While the static scan is in progress, the software composition analysis tool checks for open source components in the payload. Open source scan results list identified open source components and associated security issues.

If you are interested in purchasing open source scan entitlements, contact your sales representative.

**Important!** Tenants can have only one open source scan entitlement type (Debricked or Sonatype) that is valid at a time.

This section contains the following topics:

[Preparing Files for Open Source Scanning](#) ..... 149



Viewing Open Source Issues .....	151
Viewing Open Source Components in a Release .....	152
Viewing Open Source Components in a Tenant .....	152
Generating an Open Source Component Report .....	153

## Preparing Files for Open Source Scanning

The files that are required in the payload for open source scanning depend on the software composition analysis tool that is being used.

### Debricked File Requirements

Debricked software composition analysis identifies direct and transitive dependencies (components) along with the associated security issues and licenses. To reliably detect dependencies, Debricked uses one of the following approaches depending on the build system or package manager:

- Some package managers use a lock file to describe dependencies in a project (such as npm). Package managers usually automatically generate lock files. Debricked natively supports scanning dependencies using lock files.
- For build systems or package managers or build systems that don't use a lock file (such as Maven, Gradle), for a successful scan in Fortify on Demand, Debricked requires a file describing the resolved dependency tree to be generated using the functionality of the build system or package manager.

**Important!** A Debricked scan is cancelled if no supported dependency manifests are present in the payload.

The following table describes the file requirements for Debricked scanning in Fortify on Demand.

Language	Package Manager	Required File	Notes
C#	NuGet	packages.lock.json	Set the MSBuild property <code>RestorePackagesWithLockFile</code> to <code>true</code> in the <code>.csproj</code> project file and run the Nuget restore command. For more information, see <a href="#">Enable repeatable package restores using a lock file</a> .
	Paket	paket.lock	paket.lock is automatically generated by Paket.
Go	Go dep	gopkg.lock	gopkg.lock is automatically generated

Language	Package Manager	Required File	Notes
			by dep.
	Go modules	.debricked-go-dependencies.txt	For instructions on generating the resolved dependency tree file, see <a href="https://debricked.com/docs/language-support/go.html#go-modules">https://debricked.com/docs/language-support/go.html#go-modules</a> .*
Java/Kotlin	Gradle	.debricked-gradle-dependencies.txt	For instructions on generating the resolved dependency tree file, see <a href="https://debricked.com/docs/language-support/java-kotlin.html#gradle">https://debricked.com/docs/language-support/java-kotlin.html#gradle</a> .*
	Maven	.debricked-maven-dependencies.tgf	For instructions on generating the resolved dependency tree file, see <a href="https://debricked.com/docs/language-support/java-kotlin.html#maven">https://debricked.com/docs/language-support/java-kotlin.html#maven</a> .*
JavaScript	npm	package-lock.json	The npm install command automatically generates package-lock.json unless disabled in a .npmrc file. The npm install --package-lock-only command generates package-lock.json without checking node_modules and downloading dependencies.
	Yarn	yarn.lock	yarn.lock is automatically generated by Yarn.
Objective-C	Cocoapods	podfile.lock	podfile.lock is automatically generated by Cocoapods.
PHP	Composer	composer.lock	composer.lock is automatically generated by Composer.
Python	Pipenv	Pipfile.lock	Pipfile.lock is automatically generated by Pipenv based upon the virtual environment for the project.
Ruby	RubyGems	Gemfile.lock	Gemfile.lock is automatically

Language	Package Manager	Required File	Notes
			generated by RubyGems.
Swift	Cocoapods	podfile.lock	podfile.lock is automatically generated by Cocoapods.

\* For Go (modules), Java (Gradle and Maven), PHP, and Python projects, Fortify recommends using version 22.1.2 or later of the Fortify ScanCentral SAST client to package the files required for Debricked scanning. Simply include the `-oss` option in the package command. Note that package generation is not dependent on successfully packaging the required files. For more information on the Fortify ScanCentral SAST client, see ["Fortify ScanCentral SAST" on page 91](#).

**Tip:** Fortify recommends the following best practices for successfully incorporating Debricked scanning into static assessments:

- If you are manually generating the resolved dependency tree files for Maven, Gradle or Go module projects, automate this process by adding the appropriate command to your CI/CD pipeline.
- In keeping with industry best practices, users should commit lock files and the resolved dependency tree files to the source control repository. This simplifies the process of preparing application files, especially if you are not using Fortify ScanCentral SAST client to package the payload.

## Sonatype File Requirements

For information on the file requirements for Sonatype scans, see <https://help.sonatype.com/iqserver/analysis>.

## Related Topics

For instructions on enabling open source scanning when configuring the static scan settings, see ["Configuring a Static Scan" on page 105](#).

## Viewing Open Source Issues

Open source issues are fully integrated into results views and reports. They are included in the dashboard metrics; issue counts on the Your Applications, Your Releases, and Overview pages; Issue pages export and issues data export; and associated API endpoints. Open source issues are mapped to the OWASP, PCI, and CWE industry-standard classifications.

For more information on open source issues, see ["Open Source Scan Issue Details" on page 181](#).

## Known Limitations

The following is a known limitation in the current release of the Debricked software composition analysis integration:

- Licenses for all component versions are displayed, instead of version-specific licenses.

## Viewing Open Source Components in a Release

You can view open source components found in the most recent scan for a release.

To view open source components for a release:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears.
3. Click **Open Source Components**.  
The Open Source Components page appears.

COMPONENT	PACKAGE URL	VERSION	TYPE	KNOWN PUBLIC VULNERABILITIES				LICENSE	SCAN TOOL
				CRITICAL	HIGH	MEDIUM	LOW		
jquery	pkg:a-name/jquery@2.1.4	2.1.4	a-name	0	1	5	0	MIT	sonatype
org.webjars.bootstrap	pkg:a-name/org.webjars%20bootstrap@3.1.1	3.1.1	a-name	0	0	5	0	Apache-2.0	sonatype
jquery		2.2.4	a-name	0	0	2	0	MIT	sonatype
@coding-blocks/bootstrap		4.2.1-cb1	a-name	0	0	1	0	MIT	sonatype
jquery		1.10.2	a-name	0	0	1	0	MIT	sonatype
jquery-form	pkg:a-name/jquery-form@3.5.0.0	3.5.0.0	a-name	0	0	1	0	GPL-2.0 MIT	sonatype
ace-builds	pkg:a-name/ace-builds@1.4.1	1.4.1	a-name	0	0	0	0	BSD	sonatype
backbone		1.2.0	a-name	0	0	0	0	MIT	sonatype

4. If results from multiple scan tools are available, select the source whose results you want to view from the drop-down list.  
The page refreshes with results from the selected source.

## Viewing Open Source Components in a Tenant

Users with the **View Third Party Apps** permission can view a tenant-wide summary of all identified open source components and the applications utilizing them.

To view open source components across a tenant:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Open Source Components**.  
The Open Source Components page appears.

COMPONENT	PACKAGE URL	VERSION	TYPE	KNOWN PUBLIC VULNERABILITIES				LICENSE	RELEASES	
				CRITICAL	HIGH	MEDIUM	LOW			
jquery		2.2.4	a-name	0	0	2	0	MIT	1	<a href="#">VIEW RELEASES</a>
org.webjars.bootstrap		3.1.1	a-name	0	0	2	0	Apache-2.0	1	<a href="#">VIEW RELEASES</a>
@coding-blocks/bootstrap		4.2.1-cb1	a-name	0	0	1	0	MIT	1	<a href="#">VIEW RELEASES</a>
jquery		1.10.2	a-name	0	0	1	0	MIT	1	<a href="#">VIEW RELEASES</a>
ace-builds		1.4.1	a-name	0	0	0	0	BSD	1	<a href="#">VIEW RELEASES</a>
backbone		1.2.0	a-name	0	0	0	0	MIT	1	<a href="#">VIEW RELEASES</a>
code-editor-module		0.0.26	a-name	0	0	0	0	MIT	1	<a href="#">VIEW RELEASES</a>

**Note:** Open source scan results from retired releases are excluded.

The following table describes how to navigate the Open Source Components page.

Task	Action
View results from specific scan tool	Select the scan tool results you want to view from the drop-down list.
Search the open source component list	Type a keyword or phrase in the search text field and press <b>Enter</b> .
View the applications and corresponding releases that use a component.	Click <b>View Releases</b> in the row of a component.

## Generating an Open Source Component Report

Open Source Component reports are available through the Fortify on Demand reporting functionality. You can generate a report using the Open Source Component report template or a custom report template. An Open Source Component report includes the following modules:

- Open Source Bill-of-Materials: a complete list of the components detected in your application
- Vulnerable Open Source Components: a list of components with known security issues

For more information on managing reports, see "[Reports](#)" on page 224.

## Entitlement Consumption

The portal manages entitlement consumption. The available entitlement quantity is displayed on the Scan Setup pages. If you purchased scans, the number of available assessments is displayed. If you purchased assessment units, the unit cost of each assessment and the total number of available units across all entitlements are displayed.

When you start or schedule a scan, the cost is automatically deducted from your entitlement allotment. Single scans are deducted each time you perform a scan, whereas a subscription is deducted once and is then valid for the application until the subscription end date. You can identify an application that is under subscription because the entitlement cost is replaced with the subscription end date.

Additional entitlement information is available through the following sources:

- The entitlement consumption and active entitlements dashboard tiles. For more information, see ["Dashboard Graph Types" on page 215](#).
- The entitlement consumption data export. For more information, see ["Creating a Data Export Template" on page 238](#).
- Entitlements page under the Administration view. For more information, see ["Viewing Entitlements" on page 251](#).

## Managing Scans

You can manage scan activities at the tenant, application, and release levels. The Your Scans page displays scans across the tenant. Users can drill down into an application; the Applications Scans page displays scans ran against the application and the Release Scans page display scans ran against the release. The Scans pages, sharing a similar layout and functionality, provide a single view where users can review scan details and track scan progress.

This section contains the following topics:

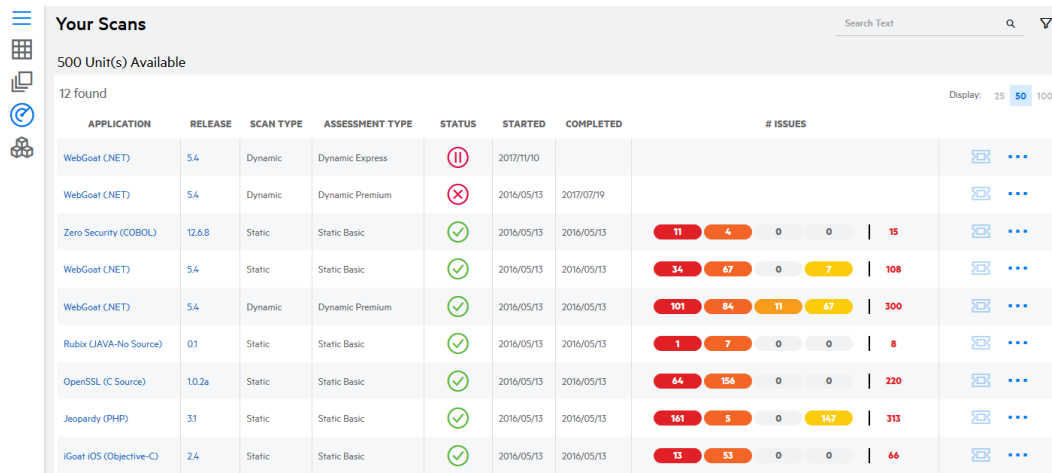
<a href="#">Viewing Scans in the Tenant</a>	154
<a href="#">Viewing Application Scans</a>	157
<a href="#">Viewing Release Scans</a>	159
<a href="#">Checking the Scan Status</a>	160
<a href="#">Canceling a Scan</a>	161
<a href="#">Resuming a Paused Scan</a>	162
<a href="#">Viewing Help Center Tickets Linked to a Scan</a>	163

### Viewing Scans in the Tenant


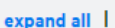




You can conveniently view scans across the tenant.

To view scans at the tenant level:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Scans**.  
Your Scans page appears. The number of available entitlements is shown at the top.



The following table describes how to navigate Your Scans page.

Task	Action
Search the scan list	Type a keyword or phrase in the search text box and click <b>Enter</b> . To remove the search results, remove the text from the search box and click <b>Enter</b> . For information, see <a href="#">"Searching Applications and Releases" on page 80</a> .
Hide or display the filter list	Click  .
Expand or collapse filters	Click     or the arrow next to the filter name.
View Help Center tickets associated with a scan	Click  .
Request cancellation of an in progress scan	Click  and select <b>Cancel Scan</b> . See <a href="#">"Canceling a Scan" on page 161</a> .
Delete an	Click  and <b>Cancel Imported Scan</b> . See <a href="#">"Deleting an Imported Scan" on</a>

Task	Action
imported scan	<a href="#">page 383</a> .
View scan summary	Click <b>...</b> and select <b>Scan Summary</b> . The scan summary includes the scan ID and a comparison to the previous scan.
View static scan notes	Click <b>...</b> and select <b>Scan Notes</b> .
Download scan results	Static, dynamic, and mobile: Click <b>...</b> and select <b>Download Results</b> . Open source: Click <b>...</b> and select <b>Download SBOM</b> .
Download manifest of static scan payload	Click <b>...</b> and select <b>Download Manifest</b> . The manifest lists uploaded files and excludes images, media files, and CSS files.
Download static scan payload	<b>Note:</b> Contact support to enable the download source code feature. Click <b>...</b> and select <b>Download Source Code</b> for a completed scan. The duration of availability is set by the " <a href="#">Data Retention Policy</a> " on <a href="#">page 411</a> .
Download dynamic scan site tree	Click <b>...</b> and select <b>Download Site Tree</b> . The download is a CSV file.
View dynamic scan detected hosts	Click <b>...</b> and select <b>Detected Hosts</b> . Detected hosts are hosts that are referenced by the application but are not specified as allowed hosts.
Create a WAF export file	<b>Note:</b> Contact support to enable the WAF feature. Click <b>...</b> and select <b>Send to WAF/IPS</b> . The export is an XML file.

## Filtering Your Scans Page

You can limit the scans displayed in Your Scans page by applying filters.

**Note:** A filter only appears in the filter list when the results contain multiple values for that filter.

To filter Your Scans page:



1. Click ▼ to display the filter list if it is not currently displayed.
2. Expand the filters that you want to apply.
3. Select your desired filter values. The following table describes the available filters.

Filter	Description	Values
Started on	Date range in which scans were started	
Completed on	Date range in which scans were completed	
Assessment type	Assessment type of the scan	
Entitlement Type	Entitlement type of the scan	Single Scan, N/A, Subscription, Remediation
Is Remediation	Whether the scan is a remediation scan	False, True
Release	Release associated with the scan	
Scan Status	Status of static, dynamic, mobile, and network scans	In Progress, Completed, Canceled, Waiting
Scan Type	Scan type	Static, Dynamic, Mobile, Network, Open Source, Application Monitoring

Your Scans page automatically refreshes with your filtered results. Applied filters are shown at the top of the page.

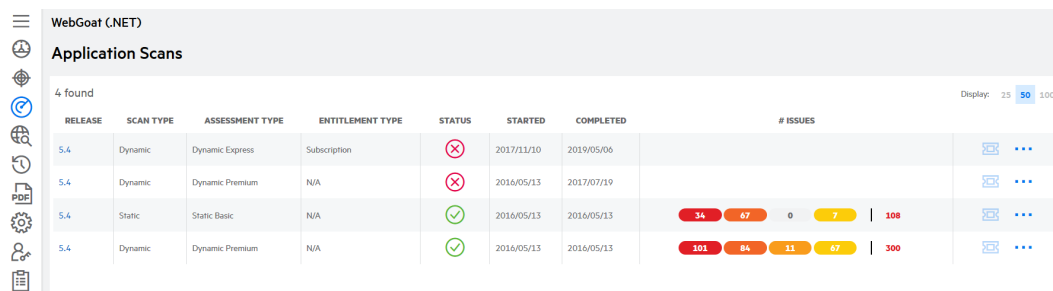
## Viewing Application Scans

You can drill down into an application and view scans of only that application.












To view scans at the application level:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application that you want to view scans ran against.
3. Click **Scans**.

The Application Scans page appears, displaying scans ran against the application.



The following table describes how to navigate the Application Scans page.

Task	Action
View Help Center tickets associated with a scan	Click  .
Request cancellation of an in progress scan	Click  and select <b>Cancel Scan</b> . See <a href="#">"Canceling a Scan" on page 161</a> .
View scan summary	Click  and select <b>Scan Summary</b> . The scan summary includes the scan ID and a comparison to the previous scan.
View static scan notes	Click  and select <b>Scan Notes</b> .
Download scan results	Static, dynamic, and mobile: Click  and select <b>Download Results</b> . Open source: Click  and select <b>Download SBOM</b> .
Download manifest of static scan payload	Click  and select <b>Download Manifest</b> . The manifest lists uploaded files and excludes images, media files, and CSS files.
Download dynamic scan site tree	Click  and select <b>Download Site Tree</b> . The download is a CSV file.
View dynamic scan detected hosts	Click  and select <b>Detected Hosts</b> . Detected hosts are hosts that are referenced by the application but are not specified as allowed hosts.
Delete an imported scan	Click  and <b>Cancel Imported Scan</b> . See <a href="#">"Deleting an Imported Scan" on page 383</a> .
Create a WAF export file	<b>Note:</b> Contact support to enable the WAF feature. Click  and select <b>Send to WAF/IPS</b> . The export is an XML file.

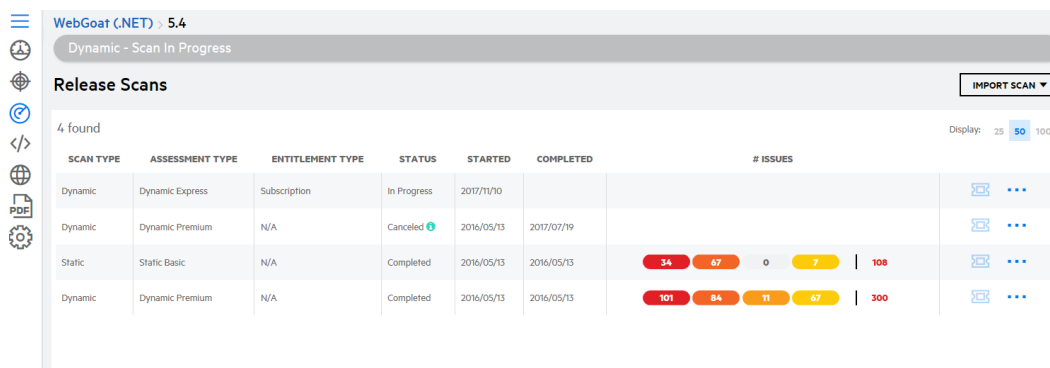
## Viewing Release Scans

You can drill down into a release and view scans of only that release.


To view scans at the release level:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears.
3. Click the name of the release that you want to view scans ran against.
4. Click **Scans**.

The Release Scans page appears, displaying scans ran against the release.



The following table describes how to navigate the Release Scans page.

Task	Action
Import a scan	Click <b>Import Scan</b> and select the scan type. Fortify on Demand supports on-premises scan results (" <a href="#">Importing an On-Premises Scan</a> " on page 381) and open source scan results (" <a href="#">Importing a Software Bill of Materials</a> " on page 383).
View Help Center tickets associated with the scan	Click  .
Request cancellation of an in progress scan	Click <b>...</b> and select <b>Cancel Scan</b> . See " <a href="#">Canceling a Scan</a> " on page 161.
View scan	Click <b>...</b> and select <b>Scan Summary</b> . The scan summary includes the scan ID and

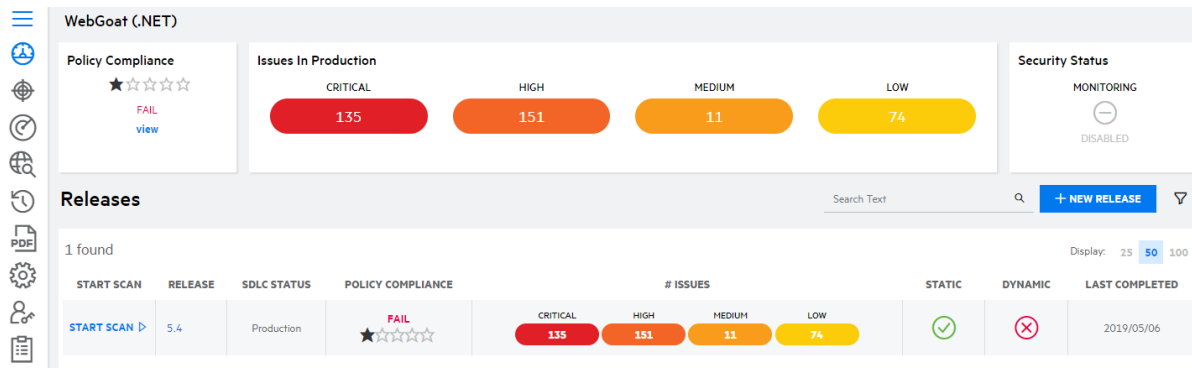
Task	Action
summary	a comparison to the previous scan
View static scan notes	Click <b>...</b> and select <b>Scan Notes</b> .
Download scan results	Static, dynamic, and mobile: Click <b>...</b> and select <b>Download Results</b> . Open source: Click <b>...</b> and select <b>Download SBOM</b> .
Download manifest of static scan payload	Click <b>...</b> and select <b>Download Manifest</b> . The manifest lists uploaded files and excludes images, media files, and CSS files.
Download static scan payload	<b>Note:</b> Contact support to enable the download source code feature. Click <b>...</b> and select <b>Download Source Code</b> for a completed scan. The duration of availability is set by the <a href="#">"Data Retention Policy" on page 411</a> .
Download dynamic scan site tree	Click <b>...</b> and select <b>Download Site Tree</b> . The download is a CSV file.
View dynamic scan detected hosts	Click <b>...</b> and select <b>Detected Hosts</b> . Detected hosts are hosts that are referenced by the application but are not specified as allowed hosts.
Delete an imported scan	Click <b>...</b> and <b>Cancel Imported Scan</b> . See <a href="#">"Deleting an Imported Scan" on page 383</a> .
Create a WAF export file	<b>Note:</b> Contact support to enable the WAF feature. Click <b>...</b> and select <b>Send to WAF/IPS</b> . The export is an XML file.

## Checking the Scan Status

Release owners, scan submitters, and users on an application's notification list receive email notifications of the following scan status updates to an application: scan start, scan completion, scan cancellation, scan pause. You can also check the scan status in the portal.

To check a scan status for an application:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application for which you want to check the scan status.  
The Application Overview page appears.



3. Hover over a scan status icon to view a tooltip with additional information about the most recent scan of that type across releases.
4. Click a status icon to directly access the scan status details:
  - Not Started: you are redirected to the relevant Scan Setup page.
  - Scheduled: you are redirected to the relevant Scan Setup page.
  - In Progress: you are redirected to the Release Scans page or the Application Scans page if a microservice application has queued static scans.
  - Queued: you are redirected to the relevant Scan Setup page.
  - Paused: you are redirected to the Help Center Tickets window on the Release Scans page.
  - Canceled: you are redirected to the relevant Scan Setup page.
  - Completed: you are redirected to the Release Issues page (static, dynamic, and mobile scans) or the Application Issues page (Application Monitoring scans), filtered by the relevant scan type.

## Canceling a Scan

You might need to cancel a scan that has not been started or has been started but has not been completed. The portal automates processing of the cancellation request. The entitlement cost will be refunded if a refund is deemed appropriate.

To cancel a scan:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application for which you want to cancel a scan.  
The Releases page appears.

3. Click **Scans**.

The Application Scans page appears.

RELEASE	SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES
5.4	Dynamic	Dynamic Express	Subscription	Failed	2017/11/10	2019/05/06	
5.4	Dynamic	Dynamic Premium	N/A	Failed	2016/05/13	2017/07/19	
5.4	Static	Static Basic	N/A	Passed	2016/05/13	2016/05/13	34 Critical, 67 High, 0 Medium, 7 Low, 108 Total
5.4	Dynamic	Dynamic Premium	N/A	Passed	2016/05/13	2016/05/13	191 Critical, 84 High, 31 Medium, 67 Low, 300 Total

4. Click **...** in the row of the scan and select **Cancel Scan**.

A confirmation message displays.

5. Click **Yes** to confirm the scan cancellation.

- For a scan with a **Queued** or **Scheduled** status, the scan is automatically canceled.
- For a scan with an **In Progress** status:
  - If the scan is an application monitoring scan or static scan that has not been audited, it is automatically cancelled.
  - If the scan is a dynamic scan, mobile scan, or static scan under audit, a Help Center ticket is generated that includes the cancellation request and scan details. An email is sent to the TAM who is assigned to the tenant along with testers who are assigned active tasks for the scan. The TAM or tester then manually cancels the scan.
- For a scan with a **Waiting** status, the scan is automatically canceled. An email is sent to the TAM who is assigned to the tenant along with testers who are assigned tasks for the scan.

Once a scan is cancelled, any Help Center tickets associated with the scan are marked as solved.

## Resuming a Paused Scan

The testing team will pause a scan if additional information is needed. Respond to the associated Help Center ticket so the scan can be resumed.

**Note:** Scans that have been paused for more than 21 consecutive days are automatically canceled. Any Help Center tickets associated with the scan are marked as solved.

To resume a paused scan:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the paused status icon in the **Scan & Security Status** column of the application.  
The Help Center tickets window appears.
3. Click the **Pending Tickets** section.  
Pending tickets for the scan appears.

4. Click a ticket to view its comments.
5. Click **Add Public Comment**.  
A text box appears below.
6. Type a comment that will be added to the ticket.
7. Click **+ Add Public Comment**.

The comment is added to the ticket details in both the portal and Help Center. Your assessment's status then reverts to **In Progress**.

**Note:** If you need to add an attachment to the ticket, you must do it through the Help Center.

## Viewing Help Center Tickets Linked to a Scan

You can directly view Help Center tickets linked to an active scan from the Your Scans, Application Scans, and Release Scans pages.


**Note:** If a scan has been paused, you can access associated Help Center tickets from any release-level page by clicking the **Help Center Tickets** button located in the status bar.

To view Help Center tickets linked to an active scan:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application.
3. Click **Scans**.

The list of all scans ran against the application or release appears.

RELEASE	SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES	
S.4	Dynamic	Dynamic Express	Subscription	⊗	2017/11/10	2019/05/06		📧 ...
S.4	Dynamic	Dynamic Premium	N/A	⊗	2016/05/13	2017/07/19		📧 ...
S.4	Static	Static Basic	N/A	⊙	2016/05/13	2016/05/13	34 Critical   67 High   0 Medium   7 Low   108 Total	📧 ...
S.4	Dynamic	Dynamic Premium	N/A	⊙	2016/05/13	2016/05/13	101 Critical   84 High   11 Medium   67 Low   300 Total	📧 ...

4. Click the  icon.  
The Help Center modal window opens, displaying all pending, open, and solved tickets associated with the scan.

The screenshot shows a 'Help Center Tickets' window. On the left, a sidebar lists 'Pending Tickets' with a count of 1. The main area displays the details for 'Ticket: 70' titled 'Assessment Waiting for Customer Action', with a status of 'pending'. A link to 'Add Public Comment' is visible. Three comments are shown, all from 'Dylan Thomas':

- Comment 1:** 2016/07/19 08:49:02 AM. Text: 'Quick feedback!'.
- Comment 2:** 2016/07/19 06:23:04 AM. Text: 'I swear they work! But I'm such a great customer, I'll update them anyway. Sincerely, Happy FoD customer'.
- Comment 3:** 2015/08/25 06:42:33 PM. Text: 'Assessment for Drupal - 7.25 is waiting for customer meaning we are having issues accessing the site properly. Assessment Type: Dynamic Tenant: Dylan Tenant Notes: The scan of your application has been paused because the credentials provided are not working. Please verify the credentials and notify the Help Center with the updated information so we may complete your scan. To chat with an FoD representative or log a support ticket, visit the FoD Help Center link on the FoD portal. For immediate assistance, use the Help Center Voice Channel (800)893-8141. Without your response, your scan may be cancelled. We would appreciate it if you could log in and help us resolve the issues. You can access the Assessment by going to [HTTPS://FODQA9-IIS2/Releases/Issues/1621](https://FODQA9-IIS2/Releases/Issues/1621) Thanks, HP Security Services'.

5. In the Pending tickets section, click a ticket to view its comments.
6. Click **Add Public Comment**.  
A text box appears below.
7. Type a comment that will be added to the ticket.
8. Click **+ Add Public Comment**.  
The comment is added to the ticket details in both the portal and Help Center.



# Chapter 5: Remediating Vulnerabilities

When the testing team completes the scan, it publishes the scan results in the portal. Log in to Fortify on Demand to view your scan results and remediate vulnerabilities found in your application.

This section contains the following topics:

- [Reviewing Issues](#) ..... 165
- [Issue Details](#) ..... 177
- [Remediating Issues](#) ..... 189
- [Auditing Issue Remediation](#) ..... 195
- [Audit Templates](#) ..... 197
- [Dataflow Cleanse Rules](#) ..... 206
- [Requesting a Remediation Scan](#) ..... 211

## Reviewing Issues

You can view detailed information about the issues that were found in a scan at both the application and release levels. The Application Issues page displays issues found across all releases of an application (excluding retired releases) as well as Application Monitoring issues. The Release Issues page displays issues found across all scans of a release.

The Application Issues and Release Issues pages, sharing a similar layout and functionality, provide a single, consolidated view of issue data. A page is split into three panels:

- The navigation panel displays a list of the issues. Issues are organized by severity, with a tab for each severity level and a tab for all issues.
- The issue details panel displays details of the issue selected in the navigation panel. Details are organized among several tabs. The tabs that are available depend on the scan type in which the issue was found.
- The audit panel is collapsible. It displays user-remediation fields of the issue selected in the navigation panel as well as the issue status, the date the issue was introduced, and the date the issue was last found.

Fortify on Demand divides issues according to the following statuses:

Status	Description
New	A vulnerability appeared for the first time in the latest scan.
Existing	A vulnerability in the latest scan has appeared in one or more previous scans,

Status	Description
	including the one immediately preceding the latest one.
<b>Reopen</b>	A vulnerability appeared in the latest scan and has appeared previously, but not in the scan immediately preceding the latest one. In other words, the issue appeared, then did not appear in one or more scans, thereby seeming to be fixed, and then later came back again.
<b>Fixed/Fixed Validated</b>	A vulnerability appeared at least once previously, but it was not identified in the latest scan. By default, Fortify on Demand doesn't show <b>Fixed</b> vulnerabilities—only issues from the most recent scan of a given type. To see <b>Fixed</b> vulnerabilities, select <b>Show... Fixed</b> on the Release Overview and Release Issues pages.

This section contains the following topics:

<a href="#">Viewing Application Issues</a>	166
<a href="#">Viewing Release Issues</a>	169
<a href="#">Filtering the Issues Page</a>	173
<a href="#">Customizing Issue Filters and Groupings</a>	175

## Viewing Application Issues

You can view issues from all releases (excluding retired releases) of an application, along with Application Monitoring issues.

To view issues at the application level:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application that you want to view.  
The Application Overview page appears.
3. Click **Issues**.  
The Application Issues page appears. Within a grouping, issues are sorted by file name, then line

number. Issues with the same instance ID across multiple releases are combined in a single view.

The screenshot displays the 'Application Issues' interface. On the left, a sidebar lists various issue categories with counts, such as 'Cross-Site Scripting' (900) and 'Open Redirect' (1). The main content area shows a specific issue with instance ID 236150, titled 'http://zero.webappsecurity.com:80/acctxfercon...'. It is categorized as 'Critical' and 'Cross-Site Scripting: Reflected'. The 'Summary' section explains that a Unicode conversion XSS vulnerability was found due to an input validation error. The 'Explanation' section details that the application fails to properly validate Unicode characters. Below this, 'Standards and Best Practices' lists OWASP 2021 (A03 - Injection), OWASP 2017 (A7 - Cross-Site Scripting (XSS)), OWASP 2014 Mobile Top 10 (M7 - Client Side Injection), and PCI 3.2 (6.5.7 - Cross-Site Scripting (XSS)). On the right, the 'Audit' section includes fields for Status (New), Introduced Date (2016/05/13), Last Found Date (2016/05/13), Assigned User (Huang, You (Huang)), Developer Status (Open), Auditor Status (Pending Review), and Severity (Critical). There are also buttons for 'ADD', 'SUBMIT BUG', and 'ADD AUDIT FILTER'.

## Navigating the Application Issues Page

The following tables describe how to navigate the Application Issues page.

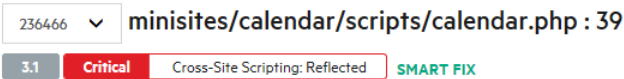
Task	Action
Export issue data	Click <a href="#">↓</a> . A link to download a CSV file is sent to the email address specified in your account settings. The link is valid for 7 days from the time the email is sent and can only be accessed by you.  <b>Note:</b> The Export functionalities in the Tenant Dashboard, Your Releases, Application Issues, and Release Issues pages output the same column fields. Currently applied filters are also applied to the export.
Search issues	Type a keyword or phrase in the search text field and press <b>Enter</b> .
Hide or display the filter list	Click <b>▼</b> .
Show or hide fixed issues	Click <b>Show... Fixed</b> to switch between showing and hiding Fix Validated issues.

Task	Action
Show or hide suppressed issues	Click <b>Show... Suppressed</b> to switch between showing or hiding Suppressed issues.
Save applied filters as query	Click <b>Save Query</b> .
Remove applied filters	Click <b>X</b> or <b>Clear Filters</b> .

### Navigation Panel

Task	Action
Expand or collapse the panel	Click <b>&gt;</b> or <b>&lt;</b> .
View issues by severity level	Select one of the following tabs: <b>Critical, High, Medium, Low, All</b> .
Group displayed issues by an attribute	Select a value from the <b>Group By</b> list. Within a group, issues are sorted by filename and then line number.
View more details about an issue	Click the issue description.
Select multiple issues	Select the check boxes next to issues.
Cycle through issues in a group	Click the right and left arrows <b>↔</b> .

### Issue Details Panel

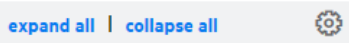

Task	Action
View a specific instance of an issue found in multiple releases	<p>Select the issue ID, specific to a release, from the drop-down list.</p> 

Task	Action
View analysis trace diagram of an issue along with others in the same category.	Click the <b>Smart Fix</b> link. A full screen view of Smart Fix appears that displays all issues in the selected issue's category, highlighting the selected issue's data flow.
View specific details of an issue	Select a tab. For more information, see " <a href="#">Issue Details</a> " on <a href="#">page 177</a>

## Audit Panel

Task	Action
Expand or collapse the panel	Click > or <.
Edit an issue	Edit the available fields. For more information, see " <a href="#">Remediating Issues</a> " on <a href="#">page 189</a> .

## Filter List

Task	Action
Expand or collapse filters	Click  or the arrow next to the filter name.
Apply a filter	Select a filter value. Click <b>Apply</b> if applicable. For more information, see " <a href="#">Filtering the Issues Page</a> " on <a href="#">page 173</a> .
Customize filter and grouping selections	Click  . For more information, see " <a href="#">Customizing Issue Filters and Groupings</a> " on <a href="#">page 175</a>

## Viewing Release Issues

You can view issues from a release of an application, including open source scan issues and on-premises scan issues.

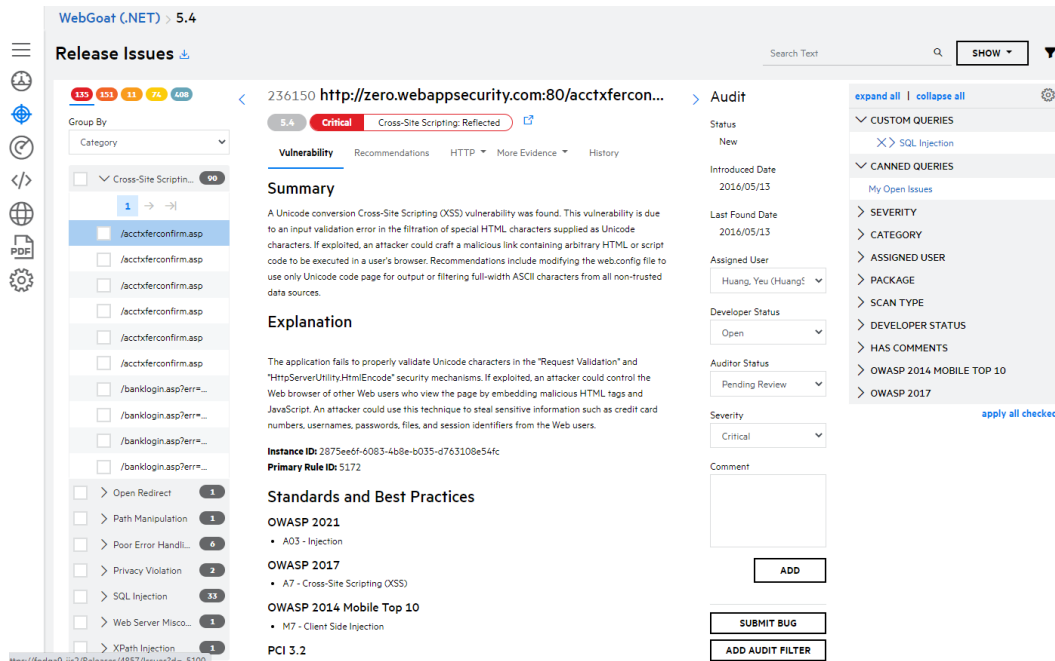
To view issues at the release level:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.

Your Releases page appears.

3. Select a release from your list.
4. Click **Issues**.

The Release Issues page appears. Within a grouping, issues are sorted by file name, then line number.



## Navigating the Release Issues Page

The following tables describe how to navigate the Release Issues page.

Task	Action
Export issue data	Click <a href="#">↓</a> . A link to download a CSV file is sent to the email address specified in your account settings. The link is valid for 7 days from the time the email is sent and can only be accessed by you.  <b>Note:</b> The Export functionalities in the Tenant Dashboard, Your Releases, Application Issues, and Release Issues pages output the same column fields. Currently applied filters are also applied to the export.
Search issues	Type a keyword or phrase in the search text field and press <b>Enter</b> .
Hide or display the filter list	Click <b>▼</b> .

Task	Action
Show or hide fixed issues	Click <b>Show... Fixed</b> to switch between showing and hiding Fix Validated issues.
Show or hide suppressed issues	Click <b>Show... Suppressed</b> to switch between showing or hiding Suppressed issues.
Save applied filters as query	Click <b>Save Query</b> .
Remove applied filters	Click <b>X</b> or <b>Clear Filters</b> .

## Navigation Panel

Task	Action
Expand or collapse the navigation panel	Click <b>&gt;</b> or <b>&lt;</b> .
View issues by severity level or all issues	Select one of the following tabs: <b>Critical, High, Medium, Low, All</b> .
Group displayed issues by an attribute	Select a value from the <b>Group By</b> list.
View more details about an issue	Click the issue description.
Select multiple	Select the check boxes next to issues.

Task	Action
issues	
Cycle through issues in a group (collapsed view)	Click the right and left arrows $\leftrightarrow$ .

### Issue Details Panel

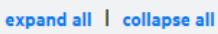


Task	Action
View an issue in a new window.	Click <a href="#">↗</a> .  <b>Note:</b> The URL in the new window is a deep link to the issue.
View analysis trace diagram of an issue along with others in the same category.	Click the <b>Smart Fix</b> link. A full screen view of Smart Fix appears that displays all issues in the selected issue's category, highlighting the selected issue's data flow.
View specific details of an issue	Select a tab. For more information, see " <a href="#">Issue Details</a> " on <a href="#">page 177</a> .

### Audit Panel

Task	Action
Expand or collapse the audit panel	Click $>$ or $<$ .
Edit an issue	Edit the available fields. For more information, see " <a href="#">Remediating Issues</a> " on <a href="#">page 189</a> .



## Filter List

Task	Action
Expand or collapse filters	Click   or the arrow next to the filter name.
Apply a filter	Select a filter value. Click <b>Apply</b> if applicable. For more information, see <a href="#">"Filtering the Issues Page"</a> below.
Customize filter and grouping selections	Click  . For more information, see <a href="#">"Customizing Issue Filters and Groupings"</a> on page 175.

## Filtering the Issues Page

You can limit the issues displayed on the Application Issues page or the Release Issues page by applying filters.

To filter the Issues page:

1. Click ▼ to display the filter list if it is not currently displayed.
2. Expand the filter(s) you want to apply.
3. Select the filter values that you want to filter for. The following table describes issue filters and their values.

**Note:** A filter only appears in the filter list when the results contain multiple values for that filter.

Filter	Description	Values
Assigned User	User defined	Not Set, User-defined
Auditor Status	Auditor issue remediation status. For more information, see <a href="#">"Audit Workflow for Auditors"</a> on page 195.	Pending Review, Remediation Required, Remediation Referred, Risk Mitigated, Risk Accepted Not an Issue
Bug Submitted	Issue was submitted as a bug to a bug tracker.	False, True
Category	Issue category	
Canned Queries	Default queries	My Open Issues

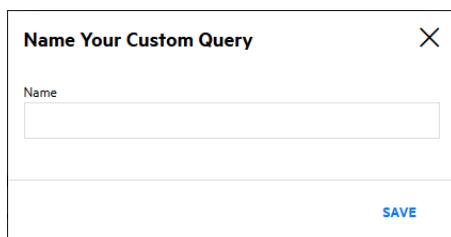
Filter	Description	Values
Custom Queries	User-defined queries	User-defined
Developer Status	Developer issue remediation status.	Challenged, Open, IN Remediation, Remediated, Will Not Fix, Third Party Component
DISA STIG 4.11	DISA Application Security and Development STIG v4.11	
DISA STIG 5.1	DISA Application Security and Development STIG v5.1	
Has Attachments		False, True
Has Comments		False, True
Introduced Date	Original date of issue creation	
Issue Age	Number of days the issue has been present in the application. The categories are cumulative. For example, an issue that is counted as greater than 30 days old is also part of the count for greater than 10 days old.	>/< 5 days, >/< 10 days, >/< 30 days, >/< 60 days, >/< 45 days, >/< 90 days
OWASP 2013	OWASP top 10 2013 classification	
OWASP 2014 Mobile	OWASP mobile top 10 2014 classification	
OWASP 2017	OWASP top 10 2017 classification	
OWASP 2021	OWASP top 10 2021 classification	
Package		
Release	<b>Note:</b> The <b>Release</b> filter appears only on the	

Filter	Description	Values
	Application Issues page. Release in which the issue was identified	
Scan Tool	Scan tool used to find issue	DAST, SAST, MAST, Debricked, Sonatype
Scan Type	Scan type to which issue belongs	Application Monitoring, Dynamic, Static, Mobile, Open Source
Severity	Issue severity	Critical, High, Medium, Low, Best Practice, Info
Status	Issue status	New, Existing, Reopen, Fixed/Fix Validated

The Issues page automatically refreshes with your filtered results. Applied filters are shown at the top of the page.

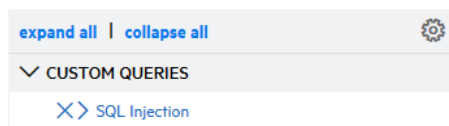
4. To save the currently applied filters for reuse, click **Save Query**.

The Name Your Custom Query window opens.



5. Type a name for the query and click **Save**.


Your saved custom query appears in the **Custom Queries** filter. You can reapply the query at any time by selecting the query from the filters list.

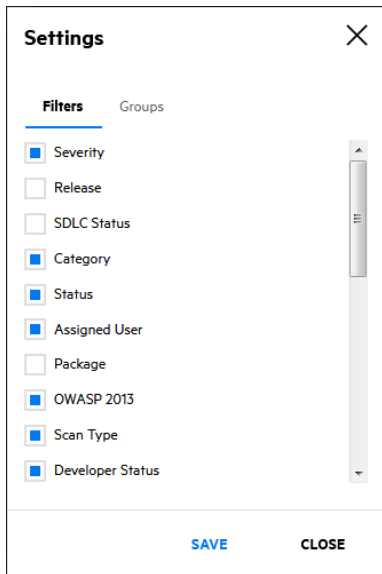


## Customizing Issue Filters and Groupings

You can customize issue filters and groupings on the Application Issues or Release Issues page.

To customize issue filters and groupings:

1. In the audit panel, click .  
The Settings window appears.



2. Perform the relevant task:

Task	Procedure
Customize issue filters	<ol style="list-style-type: none"> <li>Select the <b>Filters</b> tab.</li> <li>Select the check boxes next to filters you want to add.</li> <li>Deselect the check boxes next to filters you want to remove.</li> <li>Click <b>Save</b>.</li> </ol> <p>The Issues page refreshes with the new filters in the filters list.</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p><b>Note:</b> A filter only appears in the filter list when the results contain multiple values for that filter.</p> </div>
Customize issue groupings ( <b>Group By</b> options in the navigation panel)	<ol style="list-style-type: none"> <li>Select <b>Groups</b>.</li> <li>Select the check boxes next to values you want to add to the <b>Group By</b> list.</li> <li>Deselect the check boxes next to values you want to remove from the <b>Group By</b> list.</li> </ol>

Task	Procedure
	d. Click <b>Save</b> .  The Issues page refreshes with the new group values.

## Issue Details

The issue details panel on the Application Issues or Release Issues page provides comprehensive issue details that help you analyze the vulnerabilities found in the application. The details are organized among several tabs. The available tabs depend on the scan type in which the issue was found.

This section covers the following topics:

<a href="#">Static Scan Issue Details</a> .....	177
<a href="#">Open Source Scan Issue Details</a> .....	181
<a href="#">Dynamic/Application Monitoring Scan Issue Details</a> .....	183
<a href="#">Mobile Scan Issue Details</a> .....	187

### Static Scan Issue Details

The issue details panel for a static scan issue displays the issue ID, issue location, issue severity, and issue category across the top. Several tabs below provide additional information about the issue, including technical details, line of code (if source code was submitted), and an analysis trace diagram.

#### Vulnerability

The **Vulnerability** tab displays the following technical details about the issue: issue summary; explanation of the execution and implications of the issue; instance ID and rule ID; and standards and best practices information from Fortify Software Security Research.

237080 Downloads/WebGoat.NET-VS\_2010/WebGoat.NET-VS\_2010/WebGoat/WebGoatCoins/Custo...

5.4 Critical Open Redirect SMART FIX

Vulnerability Recommendations Code Diagram More Evidence History

## Summary

The file **CustomerLogin.aspx.cs** passes unvalidated data to an HTTP redirect on line **72**. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

## Explanation

Redirects allow web applications to direct users to different pages within the same application or to external sites. Applications utilize redirects to aid in site navigation and, in some cases, to track how users exit the site. Open redirect vulnerabilities occur when a web application redirects clients to any arbitrary URL that can be controlled by an attacker.

Attackers may utilize open redirects to trick users into visiting a URL to a trusted site and redirecting them to a malicious site. By encoding the URL, an attacker is able to make it more difficult for end-users to notice the malicious destination of the redirect, even when it is passed as a URL parameter to the trusted site. Open redirects are often abused as part of phishing scams to harvest sensitive end-user data.

In this case, the URL the client will be redirected to is accepted at **get\_QueryStringO** in **CustomerLogin.aspx.cs** at line **67**.

The data is sent at **RedirectO** in **CustomerLogin.aspx.cs** at line **72**.

**Example 1:** The following code instructs the user's browser to open a URL parsed from the **dest** request parameter when a user clicks the link.

```
String redirect = Request["dest"];
Response.Redirect(redirect);
```

## Recommendations

The **Recommendations** tab displays recommendations to remediate the issue, along with tips and references for further research. If available, the **Interactive Training** section contains a link to interactive training for the issue category, provided by Secure Code Warrior. For more information about Secure Code Warrior, see "[Secure Code Warrior Integration](#)" on page 392.

237080 Downloads/WebGoat.NET-VS\_2010/WebGoat.NET-VS\_2010/WebGoat/WebGoatCoins/Custo...

5.4 Critical Open Redirect SMART FIX

Vulnerability Recommendations Code Diagram More Evidence History

## Recommendation

Unvalidated user input should not be allowed to control the destination URL in a redirect. Instead, use a level of indirection: create a list of legitimate URLs that users are allowed to specify and only allow users to select from the list. With this approach, input provided by users is never used directly to specify a URL for redirects.

**Example 2:** The following code references an array populated with valid URLs. The link the user clicks passes in the array index that corresponds to the desired URL.

```
String redirect = Request["dest"];
Int32 strDest = System.Convert.ToInt32(redirect);
if((strDest >= 0) && (strDest <= strURLArray.Length - 1 ))
{
    strFinalURL = strURLArray[strDest];
    pageContext.forward(strFinalURL);
}
```

In some situations this approach is impractical because the set of legitimate URLs is too large or too hard to keep track of. In such cases, use a similar approach to restrict the domains that users can be redirected to, which can at least prevent attackers from sending users to malicious external sites.

## Tips

1. A number of modern web frameworks provide mechanisms for performing validation of user input. ASP.NET Request Validation and WCF are among them. To highlight the unvalidated sources of input, the HP Fortify Secure Coding Rulepacks dynamically re-prioritize the issues reported by HP Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. In case of ASP.NET Request Validation, we also provide evidence for when validation is explicitly disabled. We refer to this feature as Context-Sensitive Ranking. To further assist the HP Fortify user with the auditing process, the Fortify Security Research Group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

## Code

The **Code** tab displays the specific code where the issue was found. Users can perform the following actions to more easily review code:

- Enable or disable word wrap
- Cycle through multiple analysis traces, if applicable
- Switch between a stacked view of the code and tree view of the analysis trace alongside the code
- Jump to the line of code when selecting an analysis trace node in the tree view
- Enable and disable showing the inline analysis trace

**Note:** To view all issues in the selected issue's category, click the **Smart Fix** link.

237080 Downloads/WebGoat.NET-VS\_2010/WebGoat.NET-VS\_2010/WebGoat/WebGoatCoins/Custo..

The screenshot shows the Fortify Code tab interface. At the top, there is a navigation bar with tabs for Vulnerability, Recommendations, Code (selected), Diagram, More Evidence, and History. Below the navigation bar, there are controls for Path 1 of 1, Word Wrap (unchecked), Stacked View (checked), and Inline Analysis Trace (checked). The main area is a code editor displaying C# code from CustomerLogin.aspx.cs. The code includes comments for expiration date, persistence, and cookie path. A red box highlights a list of analysis traces at the bottom of the code editor, with the first trace selected and highlighted in blue. The selected trace is: CustomerLogin.aspx.cs:67 - get\_QueryString(return).

```
50         DateTime.Now.AddDays(14), //expireDate
51         true, //isPersistent
52         "customer", //userData (customer role)
53         FormsAuthentication.FormsCookiePath //cookiePath
54     );
55
56     string encrypted_ticket = FormsAuthentication.Encrypt(ticket); //encrypt the ticket
57
58     // put ticket into the cookie
59     HttpCookie cookie = new HttpCookie(FormsAuthentication.FormsCookieName, encrypted_ticket);
60
61     //set expiration date
62     if (ticket.IsPersistent)
63         cookie.Expires = ticket.Expiration;
64
65     Response.Cookies.Add(cookie);
66
67     string returnUrl = Request.QueryString["ReturnUrl"];
```

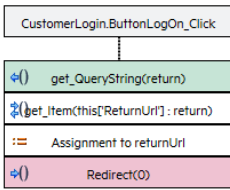
## Diagram

The **Diagram** tab displays an analysis trace diagram of the issue.

237080 Downloads/WebGoat.NET-VS\_2010/WebGoat.NET-VS\_2010/WebGoat/WebGoatCoins/Custo...

5.4 Critical Open Redirect SMART FIX

Vulnerability Recommendations Code **Diagram** More Evidence History



```
graph TD; A[CustomerLogin.ButtonLogOn_Click] --> B[get_QueryString(return)]; B --> C[get_Item(this.ReturnUrl) : return]; C --> D[Assignment to returnUrl]; D --> E[Redirect(0)];
```

## More Evidence

The **More Evidence** tab contains notes and screenshots, which are accessed separately through the drop-down menu.

- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see ["Uploading Screenshots" on page 193](#).

237080 Downloads/WebGoat.NET-VS\_2010/WebGoat.NET-VS\_2010/WebGoat/WebGoatCoins/Custo...

5.4 Critical Open Redirect SMART FIX

Vulnerability Recommendations Code Diagram **More Evidence** History

+ ADD SCREENSHOT

There are no items to display.

## History

The **History** tab displays a log of the following issue events: audit changes, comments, and system events (status changes, copy state actions). You can filter the log by the event type (audit, comment, or system event).

237080 Downloads/WebGoat.NET-VS\_2010/WebGoat.NET-VS\_2010/WebGoat/WebGoatCoins/Custo...

5.4 Critical Open Redirect SMART FIX

Vulnerability Recommendations Code Diagram More Evidence **History**

Audits  Comments  System Events

**Fortify on Demand** 2016/05/13 09:02:33 AM  
Issue found in scan 5194 of release 5.4.

Add Comment

ADD



## Open Source Scan Issue Details

The issues details panel for an open source scan issue displays the issue ID, issue location, issue severity, and rule ID at the top. Several tabs below provide additional information about the issue.

**Note:** If an open source issue is found to be a non-active vulnerability based on the most recent Sonatype scan, the issues details panel displays the message "This vulnerability is no longer listed as an active vulnerability." The issue status is also marked as **Fixed Validated**. This does not apply to issues associated with open source components that have been removed.

### Vulnerability

The **Vulnerability** tab displays the following technical details about the issue: vulnerability data from the scan tool used; instance ID and rule ID; file locations; and standards and best practices information from Fortify Software Security Research.

For more information on the vulnerability data from the scan tools, see the following documentation:

- Sonatype: <https://guides.sonatype.com/iqserver/technical-guides/sonatype-vuln-data/>
- Debricked: <https://debricked.com/docs/security/security-about.html#data-refinement>

**Note:** CVSS vector and file location details are currently not available for Debricked issues.

1481099 @coding-blocks/bootstrap@4.2.1-cb1 : bootstrap.bundle...

8.0 Medium CVE-2019-8331

Vulnerability Recommendations More Evidence History

#### Summary

In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

**Component Name:** @coding-blocks/bootstrap

**Component Version:** 4.2.1-cb1

**Repository:** a-name

**Instance ID:** CSF97DAE9B764E0691541A21690EFCF1

**Primary Rule ID:** CVE-2019-8331

**CVSS Base Score:** 6.1

**CVSS Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/CL:T/L:A/N

#### File Locations

- WebGoat-develop/docs/vendor/bootstrap/js/bootstrap.bundle.min.js

#### Standards and Best Practices

OWASP 2017

- A9 - Using Components with Known Vulnerabilities

PCI 3.2

- 6.2 - Known Vulnerabilities

CWE

- CWE-79

### Recommendations

The **Recommendations** tab displays remediation information and references for further research.

**Note:** A Nexus IQ license is no longer needed to view remediation information provided by Sonatype.

1481099 @coding-blocks/bootstrap@4.2.1-cb1 : bootst...

8.0 Medium CVE-2019-8331

Vulnerability Recommendations More Evidence History

### Explanation

The `bootstrap` package is vulnerable to Cross-Site Scripting (XSS). The `setContent` method in the `tooltip.js` file accepts JavaScript within the input parameters without properly sanitizing the data in the elements that are being rendered on the webpage. This could lead to Cross-Site Scripting (XSS). \*Advisory Deviation Notice:\* The Sonatype security research team discovered that the root cause of the vulnerability is in 4.0.0-alpha.2, not in 4.3.0 as the advisory states.

### Detection

The application is vulnerable by using this component.

### Recommendation

We recommend upgrading to a version of this component that is not vulnerable to this specific issue.

### Next Non-Vulnerable Version

4.5.1

### Greatest Non-Vulnerable Version

4.5.2

### Links

1. <https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/>
2. <https://github.com/twbs/bootstrap/pull/28236>
3. <https://iq.nexus.equifax.com/assets/index.html#/vulnerabilities/CVE-2019-8331>

## More Evidence

The **More Evidence** tab displays notes and screenshots, which are accessed separately through the drop-down menu.

- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see "[Uploading Screenshots](#)" on page 193.

1481099 @coding-blocks/bootstrap@4.2.1-cb1 : bootstrap.bundl...

8.0 Medium CVE-2019-8331

Vulnerability Recommendations More Evidence History

There were no additional notes for this vuln

Notes  
Screenshots

## History

The **History** tab displays a log of the following events related to the issue: audit changes, comments, and system events (status changes, copy state actions). You can filter the log by the event type (audit, comment, or system event).

1481099 @coding-blocks/bootstrap@4.2.1-cb1 : bootstrap.bundl...

8.0 Medium CVE-2019-8331

Vulnerability Recommendations More Evidence ▾ History

Audits  Comments  System Events

**Fortify on Demand** 2019/05/13 11 47 49 AM  
Issue found in scan 26296 of release 8.0.

Add Comment

ADD

## Dynamic/Application Monitoring Scan Issue Details

The issues details panel for a dynamic scan issue or application monitoring issue displays the issue ID, issue location, issue severity, and issue category at the top. Several tabs below provide additional information about the vulnerability, including technical details, request, and response.

### Vulnerability

The **Vulnerability** tab displays the following technical details about the issue: issue summary, including instance ID and rule ID of the issue; explanation of the execution and implications of the issue; and standards and best practices information from Fortify Software Security Research.

236150 <http://zero.webappsecurity.com:80/acctxferconfirm.asp>

5.4

Critical

Cross-Site Scripting: Reflected



Vulnerability

Recommendations

HTTP ▾

More Evidence ▾

History

## Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

## Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

**Instance ID:** 2875ee6f-6083-4b8e-b035-d763108e54fc

**Primary Rule ID:** 5172

## Standards and Best Practices

### OWASP 2013

- A3 - Cross-Site Scripting (XSS)

### PCI 3.2

- 6.5.7 - Cross-Site Scripting (XSS)

### FISMA

- SC


### CWE

- CWE-811
- CWE-116
- CWE-80
- CWE-79

## Recommendations

The **Recommendations** tab displays recommendations to remediate the issue, along with tips and references for further research. If available, the **Interactive Training** section contains a link to interactive training for the issue category, provided by Secure Code Warrior. For more information about Secure Code Warrior, see "[Secure Code Warrior Integration](#)" on page 392

236150 <http://zero.webappsecurity.com:80/acctxferconfirm.asp>

5.4 **Critical** Cross-Site Scripting: Reflected 

Vulnerability **Recommendations** HTTP  More Evidence  History

## Recommendation

### For Security Operations:

No patch is currently available.

Modify the web.config file to use only Unicode code page for output. To do this, add the following lines to your web.config file:

```
<configuration>
  <system.web>
    <globalization responseEncoding="utf-8" />
  </system.web>
</configuration>
```

If you cannot use Unicode, have your developers to filter full-width ASCII characters from all non-trusted data sources, such as user input, HTTP headers, some components output, and other data.

### For Developers:

Have your Security Operations modify the web.config file to use only Unicode code page for output.


If your application cannot use Unicode, you must filter full-width ASCII characters from all non-trusted data sources, such as user input, HTTP headers, some components output, and other data.

## HTTP

The **HTTP** tab displays the content, headers, and parameters of the request and response, which are accessed separately through the drop-down menu.

Available for Application Monitoring issues, the **Evidences** section lists the complete session traffic that found the issue.

236150 <http://zero.webappsecurity.com:80/acctxferconfirm.asp>

5.4 **Critical** Cross-Site Scripting: Reflected 

Vulnerability Recommendations **HTTP** More Evidence History

## Request

```
COPY WORD WRAP
1 POST /acctxferconfirm.asp HTTP/1.1
2 Referer: http://zero.webappsecurity.com:80/acctxfer.asp
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 147
5 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4
6 Accept: */*
7 Pragma: no-cache
8 Host: zero.webappsecurity.com
9 X-Scan-Memo: Category="Audit"; Function="createStateRequestFromAttackDefinition"; :
10 Connection: Keep-Alive
11 Cookie: CustomCookie=WebInspect69383ZXB3FCEA2CCD6849B0A63D3EFF65615601Y3637;status=
12
13 fromAcct=<script>alert('vulnerability')</script>&toAcct=Household%20Checking&amount=
```

## Response


```
COPY WORD WRAP
1 HTTP/1.1 200 OK
2 Date: Fri, 13 May 2011 19:53:54 GMT
3 Server: Microsoft-IIS/6.0
4 X-Powered-By: ASP.NET
5 Content-Length: 2369
6 Content-Type: text/html
7 Cache-control: private
8
9
10
11 <html>
12 <head>
13 <title>Confirm Transfer Funds</title>
```

## More Evidence

The **More Evidence** tab displays notes and screenshots, which are accessed separately through the drop-down menu.

- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see ["Uploading Screenshots" on page 193](#).

236150 <http://zero.webappsecurity.com:80/acctxferconfirm.asp>

5.4 **Critical** Cross-Site Scripting: Reflected 

Vulnerability Recommendations HTTP **More Evidence** History

There were no additional notes for this vulnerability instance.

- Notes
- Screenshots

## History

The **History** tab displays a log of the following issue events: audit changes, comments, and system events (status changes, copy state actions). You can filter the log by the event type (audit, comment, or system event).

236150 <http://zero.webappsecurity.com:80/acctxferconfirm.asp>

5.4 **Critical** Cross-Site Scripting: Reflected

Vulnerability Recommendations HTTP More Evidence History

**Fortify on Demand** 2016/05/13 09:01:48 AM  
Issue found in scan 5193 of release 5.4.

**Yeu-Li.Huang@hp.com** 2017/08/15 10:45:45 PM  
Changed user to 'HuangSLead2'

**Show**

- Audits
- Comments
- System Events

Add Comment

**ADD**

## Mobile Scan Issue Details

The issues details panel for a mobile scan issue displays the issue ID, issue location, issue severity, and issue category across the top. Several tabs below provide additional information about the issue.

### Vulnerability

The **Vulnerability** tab displays the following technical details about the issue: issue summary; instance ID and rule ID; and explanation of the execution and implications of the issue.

466682 **Application Binary**

**Medium** System Information Leak: Internal

Vulnerability Recommendations More Evidence History

### Summary

The application calls methods of the Log class. Messages passed to these methods (Log.v(), Log.d(), Log.i(), Log.w(), and Log.e()) are stored in a series of circular buffers on the device. By default, a maximum of four 16 KB rotated logs are kept in addition to the current log. The logged data can be read using Logcat on the device. When using platforms prior to Android 4.1 (Jelly Bean), the log data is not sandboxed per application; any application installed on the device has the capability to read data logged by other applications.

### Explanation

Data logged by the application may be sensitive in nature or disclose information that may aid an attacker to further attacks against users of the mobile application or the backend services that the application communicates with. Logging identified using the following API calls: Log.d


Log.e  
Log.i  
Log.v  
Log.w

**Instance ID:** ebe90b1a-ef13-3b38-a7e0-7761d872b615  
**Primary Rule ID:** M169

## Recommendations

The **Recommendations** tab displays recommendations to remediate the issue, along with tips and references for further research. If available, the **Interactive Training** section contains a link to interactive training for the issue category, provided by Secure Code Warrior. For more information about Secure Code Warrior, see ["Secure Code Warrior Integration" on page 392](#)

### 466682 Application Binary

**Medium** System Information Leak: Internal 

Vulnerability Recommendations More Evidence ▾ History

#### Recommendation

Remove any sensitive information from the Log statements within the application source code. As a best practice, use conditionals to control logging during debugging the application and disable logging when putting the application into production.

#### Tips

(There is no information to display.)

#### References

Reading and Writing Logs <http://developer.android.com/tools/debugging/debugging-log.html>

## More Evidence

The **More Evidence** tab contains notes and screenshots, which are accessed separately through the drop-down menu.

- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see ["Uploading Screenshots" on page 193](#).

### 466682 Application Binary

**Medium** System Information Leak: Internal 

Vulnerability Recommendations More Evidence ▾ History

There were no additional notes for this vulnerability.

Notes

Screenshots

## History

The **History** tab displays a log of the following issue events: audit changes, comments, and system events (status changes, copy state actions). You can filter the log by the event type (audit, comment, or system event).



## 466682 Application Binary

Medium

System Information Leak: Internal



Vulnerability

Recommendations

More Evidence ▾

History

### Show

- Audits
- Comments
- System Events

Add Comment

ADD

## Remediating Issues

Using the information provided in your scan results, remediate the vulnerabilities that were found. You can edit issues at both the application and release levels for the purpose of tracking remediation efforts.

This section contains the following topics:

<a href="#">Editing an Issue</a>	189
<a href="#">Editing Multiple Issues</a>	191
<a href="#">Uploading Screenshots</a>	193

## Editing an Issue

Users with the Edit issues permission can edit an issue's developer status and assigned user. Users with the Audit permission can also edit an issue's auditor status and severity.

To edit an issue:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application with issues that you want to edit.  
The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page:
  - To navigate to the Application Issues page:
    - i. Click **Issues**.  
The Application Issues page appears.

The screenshot displays the 'Application Issues' interface. On the left, a navigation panel shows a list of issues grouped by category, with 'Cross-Site Scripting' selected. The main content area shows details for a specific issue (ID: 236150) titled 'http://zero.webappsecurity.com:80/acctxfercon...'. The issue is marked as 'Critical' and 'Cross-Site Scripting: Reflected'. The 'Summary' section describes a Unicode conversion XSS vulnerability. The 'Explanation' section details the application's failure to validate Unicode characters. The 'Standards and Best Practices' section lists relevant OWASP and PCI standards. The 'Audit' panel on the right includes fields for Status, Introduced Date, Last Found Date, Assigned User, Developer Status, Auditor Status, Severity, and a Comment field. There are also buttons for 'ADD', 'SUBMIT BUG', and 'ADD AUDIT FILTER'.

- To navigate to the Release Issues page:
  - i. Click the name of a release.
  - ii. Click **Issues**.

The Release Issues page appears.

This screenshot is identical to the one above, showing the 'Release Issues' page. It highlights the same 'Critical' XSS vulnerability details, including the summary, explanation, and standards, as well as the audit panel with its various filters and controls.

4. In the navigation panel, select the issue that you want to edit. If you are on the Application Issues page, select a specific instance of an issue found in multiple releases by selecting select the issue ID, specific to the release, from the drop down list in the issue details panel.

5. In the audit panel, select the user to be assigned the issue from the **User** list.
6. Select the issue's development status from the **Developer Status** list. The default value is **Open**. Statuses fall under an open or closed state.
  - If you are reviewing the issue, select **In Remediation**.
  - If you have remediated the issue, select **Remediated**.
  - If you have decided not to remediate the issue, select **Will Not Fix**.
  - If the issue is in third-party code, select **Third Party Component**.
7. Select the issue's audit status from the **Auditor Status** list. The default state is **Pending Review**. Statuses fall under a non-suppressed or suppressed state.
  - Not Suppressed: **Remediation Required, Remediation Deferred, Risk Mitigated**
  - Suppressed: **Risk Accepted, Not an Issue**
8. To change the default issue severity, select a different severity from the **Severity** list. For more information on issue severity, see ["Priority Order" on page 19](#).
9. Type any supporting comments in the **Comment** field and click **Add**.
10. Refresh the Issues page to see your changes. If an issue is not suppressed, it remains on the Issues page. If an issue is suppressed, it is hidden on the Issues page and only appears when **Show... Suppressed** is selected.

## Related Topics

["Submitting Issues to the Bug Tracker" on page 387](#)

## Editing Multiple Issues

You can edit multiple issues at the same time.

To edit multiple issues:

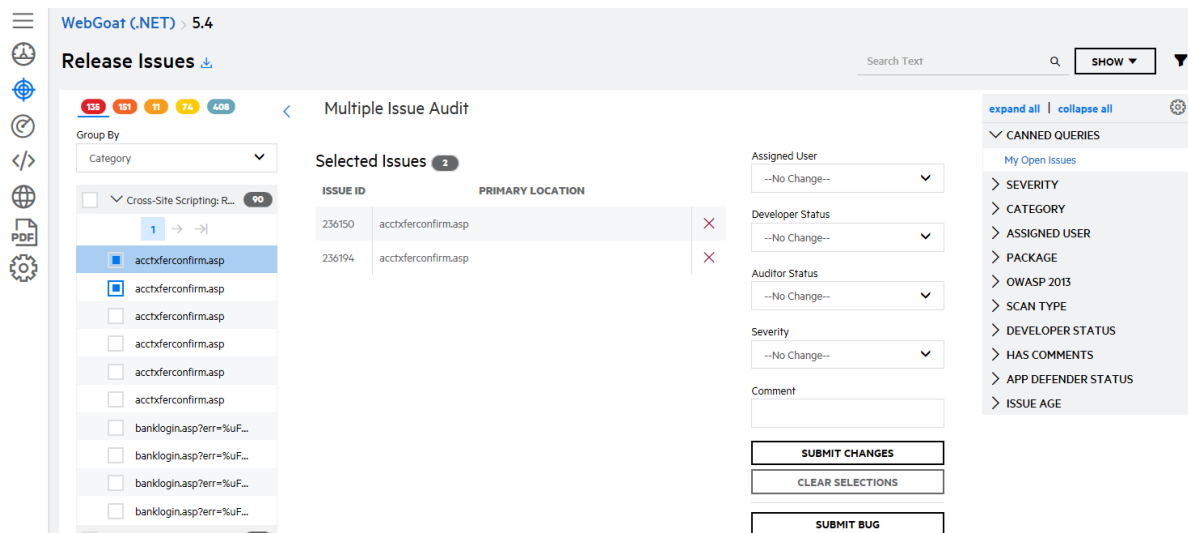
1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application with issues that you want to edit.  
The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page:
  - To navigate to the Application Issues page:
    - i. Click **Issues**.  
The Application Issues page appears.

- To navigate to the Release Issues page:
  - i. Click the name of a release.
  - ii. Click **Issues**.

The Release Issues page appears.

4. In the navigation panel, select the check boxes next to the issues that you want to edit. You can select the check box next to a group name to select all issues in the group.

**Note:** If you are on the Application Issues page, selecting the check box next to an issue found in multiple releases selects all instances of the issue.



5. In the audit panel, edit the fields as desired. The following fields are available for editing: **Assigned User**, **Developer Status**, **Auditor Status**, **Severity**, and **Comments**.
6. Click **Submit Change**.

## Related Topics

["Submitting Issues to the Bug Tracker" on page 387](#)

## Uploading Screenshots

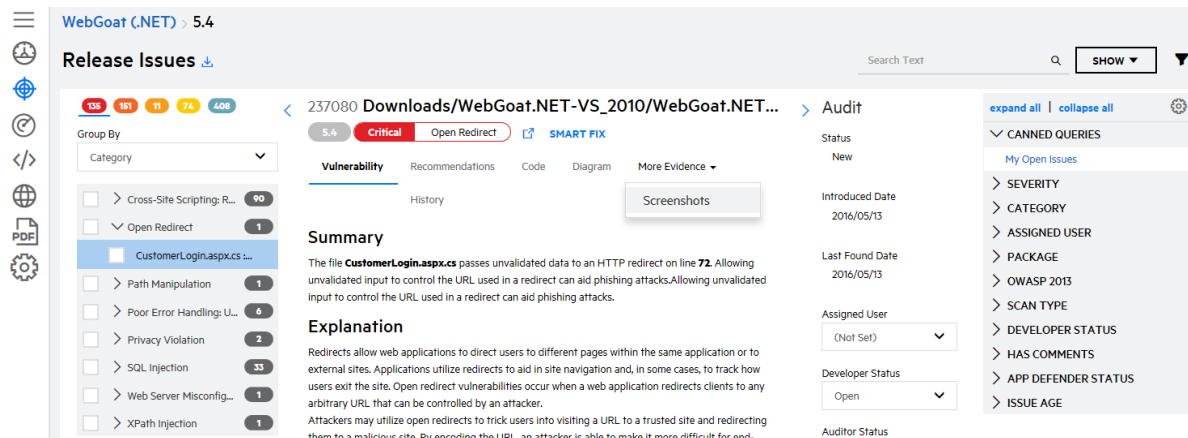
You can upload screenshots for an issue through the Application Issues or Release Issues page.

- Supported file types are .jpg, .gif, and .png.
- Files must be no larger than 3 MB.

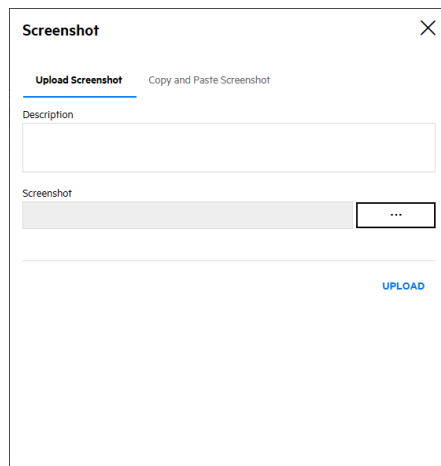
There are two methods for uploading a screenshot: upload a saved file or copy and paste the image into the modal window.

To upload a screenshot for an issue:

1. In the issues detail panel, select the **More Evidence** tab > **Screenshots**.






2. Click **+Add Screenshot**.  
The Screenshot modal window appears.



3. Choose one of the following ways to upload the screenshot:
  - To upload a file:
    - i. Select the **Upload Screenshot** tab.
    - ii. (Optional) Type a description of the file.
    - iii. Click **...** and browse to and select a screenshot.
    - iv. Click **Upload**.
  - To copy and paste the screenshot:
    - i. Select the **Copy and Paste Screenshot** tab.
    - ii. (Optional) Type a description of the file.
    - iii. Copy an image to your clipboard.
    - iv. Select the box and press **Ctrl+V** to paste the image from the clipboard.
    - v. Click **Upload**.

The uploaded screenshot details and icons for viewing, saving, and deleting the screenshot appears in the tab.

Icon	Description
	View the screenshot in the browser.
	Open the screenshot or save it to your local system.
	Delete the screenshot.

## Auditing Issue Remediation

Fortify on Demand enables an organization's development and security teams to audit issue remediation, where different user roles participate in the issue remediation workflow. Users with the **Edit Issues** permission, typically the development team, receive the issues and decide whether to remediate them or not. Users with the **Audit Issues** permission, typically the security team, validate the issues after the development team is finished and decide whether to suppress them or not. Users with the **View Issues** permission can view issues, but cannot make any changes.

This section contains the following topics:

<a href="#">Audit Workflow for Auditors</a> .....	195
<a href="#">Audit Workflow for Developers</a> .....	196

### Audit Workflow for Auditors

The following procedures describes the typical workflow that a security team follows for assigning new issues and reviewing closed issues.

Auditors from the security team need the Audit issue permission, which allows editing of the **Auditor Status** and **Severity** fields.

#### Assigning a New Issue

A new issue arrives in the queue with the following default values:

- **Developer Status: Open**
- **Users: (Not Set)**
- **Auditor Status: Pending Review**
- **Severity:** Fortify on Demand-ranked default

The security team reviews the issue and assigns it to a developer for remediation.

To assign a new issue to a developer for remediation:

1. Review an issue that has the **Developer Status** set as **Open**.
2. If needed, select a different issue severity from the **Severity** list. For more information on issue severity, see "[Priority Order](#)" on page 19.
3. Select the developer to be assigned the issue from the **User** list.

## Reviewing Closed Issues

After working on the issue, the developer changes the **Developer Status** to a closed state (**Remediated, Will Not Fix, Third Party Component**). The issue then returns to the security team issue queue for auditing.

To review a closed issue:

1. Audit the change made to the closed issue.
2. Based on your assessment of the change, decide whether to suppress or not suppress the issue and select the corresponding reason from the **Auditor Status** list.
  - Not Suppressed: **Remediation Required, Remediation Deferred, Risk Mitigated**
  - Suppressed: **Risk Accepted, Not an Issue**
3. If you selected **Remediation Required**, reassign the issue to a developer.
4. Add any supporting comments.

## Audit Workflow for Developers

The following procedures describe the typical workflow a development team follows for remediating and closing an issue.

Developers from the development team need the Edit issue permission, which allows editing of the **Developer Status** and **User** fields.

### Remediating an Issue

The security team assigns an open issue to a developer for remediation.

To remediate an issue:

1. Set the **Developer Status** to **In Remediation**.
2. Review the issue and perform one of the following actions:
  - Remediate the issue.
  - Do not remediate the issue.

### Closing an Issue

To close an issue:



1. Once you have finished working on the issue, set the **Developer Status** to **Remediated, Will Not Fix**, or **Third Party Component**.

The issue is closed at this point.

2. Add any supporting comments.
3. Select the auditor to review the issue from the **User** list.

## Audit Templates

Audit templates allow audit decisions to be systematically applied to static, dynamic, mobile, and open source scans. An audit template consists of custom filters that either suppress issues or change issue severity across all scans of the specified type.

An audit template can be created for each scan type at the global and application levels. Security Leads can manage global audit templates; users with the **Audit Issues** permission can manage audit templates for applications to which they have access.

**Important!** Audit template is an advanced feature and can lead to significant changes in vulnerability metrics and reporting. Fortify strongly recommends that you review the documentation before using audit templates. If you have additional questions, contact the support team.

This section contains the following topics:

<a href="#">Creating a Global Audit Template</a> .....	197
<a href="#">Creating an Application Audit Template</a> .....	200
<a href="#">Creating an Application Audit Template Filter for an Issue</a> .....	203
<a href="#">Audit Template Usage and Examples</a> .....	205

## Creating a Global Audit Template

Security Leads can manage global audit templates. Global audit templates apply to all scans of the specified type across the tenant.

Audit templates are subjected to the following conditions:

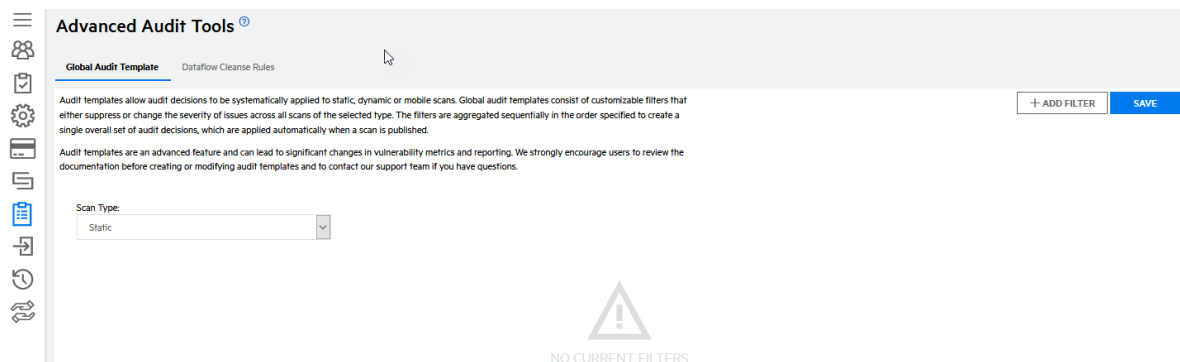
- Audit template filters are case insensitive.
- Newly created or modified audit template filters are applied to scans published moving forward.

To create a global audit template:

1. Select the **Administration** view.  
The User Management page appears.

2. Click **Audit Tools**.

The Advanced Audit Tools page appears.

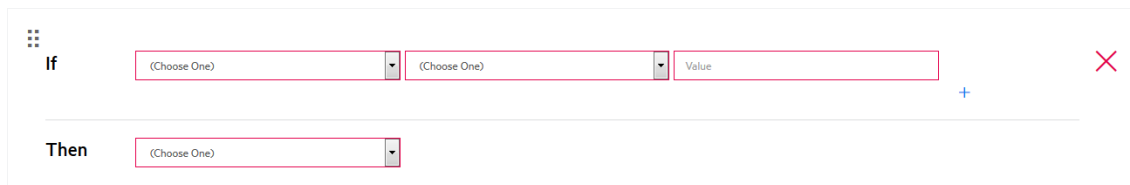


3. On the **Global Audit Template** tab, select the scan type to which the global audit template will be applied from the **Scan Type** list.

4. Perform the following steps to add a filter. You can add multiple filters.

a. Click **Add Filter**.

A blank filter appears.



b. Specify the filter conditions.

i. In the **IF** row, select an issue attribute or a custom attribute for which to filter:

**Note:** Static, dynamic, and mobile issue attributes are set by Fortify Software Security Content. Open source issue attributes are set by Sonatype.

Field	Scan Type	Description
Severity	Static, dynamic, mobile, open source	Issue severity
Rule ID	Static, dynamic, mobile, open source	A unique identifier for the rule that identified an issue. You can find the Rule ID on the <b>Vulnerability</b> tab of the issue details panel.
Kingdom	Static,	Seven Pernicious Kingdoms classification

Field	Scan Type	Description
	dynamic, mobile	
Category	Static, dynamic, mobile	Vulnerability category, which contains one or more rule IDs. A filter based on a category will be applied to all rule IDs belonging to that category.
<Custom Application Attribute>	Static, dynamic, mobile	Custom attributes in your tenant (picklist, text, and boolean)
Component Name	Open source	Component name
Component Version	Open source	Component version

ii. Select one of the following operators:

Operator	Description
Contains	Searches for results that contain the specified value
Does Not Contain	Searches for results that do not contain the specified value
Equals	Searches for an exact match of the specified value
Does Not Equals	Searches for results that do not match the specified value

iii. Enter the value for the issue attribute. Wildcards are not accepted.

**Note:** If you previously selected a custom picklist or boolean attribute and the **Equals** operator, the values are prepopulated.


iv. If needed, click **+** to create additional filter conditions.

v. Select **And** or **Or** to combine multiple filter conditions

c. In the **THEN** row, select one of the following audit actions to apply to matching results:

Operator	Description
Suppress	Suppresses matching results

Operator	Description
Set Severity	Sets issue severity of matching results to the specified value

- To rearrange the location of a filter, click  and drag the filter to your desired slot.
- Once you are done adding and arranging filters, click **Save**.  
The global audit template is saved.

### Related Topics:

For information on creating an application audit template, see "[Creating an Application Audit Template](#)" below.

## Creating an Application Audit Template

Users with the **Audit Issues** permission can manage audit templates for applications to which they have access. An application audit template applies to all scans of the specified type for the application.

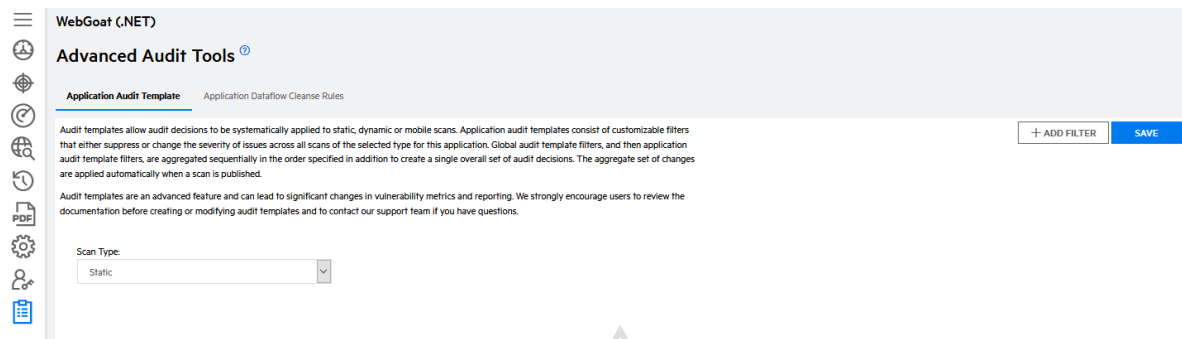
Audit templates are subjected to the following conditions:

- Audit template filters are case-insensitive.
- Newly created or modified audit template filters are applied to scans published moving forward.

To create an application audit template:

- Select the **Application** view.  
Your Applications page appears.
- Click the name of the application for which you want to create an application audit template.
- Click **Audit Tools**.

The Advanced Audit Tools page appears.



4. On the **Application Audit Template** tab, select the scan type to which the application audit template will be applied from the **Scan Type** list.
5. Perform the following steps to add a filter. You can add multiple filters.
  - a. Click **Add Filter**.

A blank filter appears.

- b. Specify the filter conditions.
  - i. In the **IF** row, select one of the following issue attributes for which to filter:

**Note:** Static, dynamic, and mobile issue attributes are set by Fortify Software Security Content. Open source issue attributes are set by Sonatype.

Field	Scan Type	Description
Severity	Static, dynamic, mobile, open source	Issue severity.
Rule ID	Static, dynamic, mobile, open source	A unique identifier for the rule that identified an issue. You can find the Rule ID on the <b>Vulnerability</b> tab when viewing issue details.
Kingdom	Static, dynamic, mobile	Seven Pernicious Kingdoms classification.
Category	Static, dynamic, mobile	Vulnerability category, which contains one or more rule IDs. A filter based on a category will be applied to all rule IDs belonging to that category.
File	Static	Full file path
Package	Static	Package or namespace
Source	Static	Dataflow source function
Sink	Static	Dataflow sink function

Field	Scan Type	Description
URL	Dynamic, mobile	Issue URL
Body	Dynamic, mobile	HTTP message body
Headers	Dynamic, mobile	HTTP request header
Parameters	Dynamic, mobile	HTTP query parameters
Component Name	Open source	Component name
Component Version	Open source	Component version

ii. Select one of the following operators:

Operator	Description
Contains	Searches for results that contain the specified value
Does Not Contain	Searches for results that do not contain the specified value
Equals	Searches for an exact match of the specified value
Does Not Equals	Searches for results that do not match the specified value


iii. Enter the value for the issue attribute. Wildcards are not accepted.

iv. If needed, click **+** to create additional filter conditions.

v. Select **And** or **Or** to combine multiple filter conditions .

c. In the **THEN** row, select one of the following audit actions to apply to matching results:

Operator	Description
Suppress	Suppresses matching results
Set Severity	Sets issue severity of matching results to the specified value

6. To rearrange the location of a filter, click  and drag the filter to your desired slot.
7. Once you are done adding and arranging filters, click **Save**.  
The application audit template is saved.

## Related Topics:

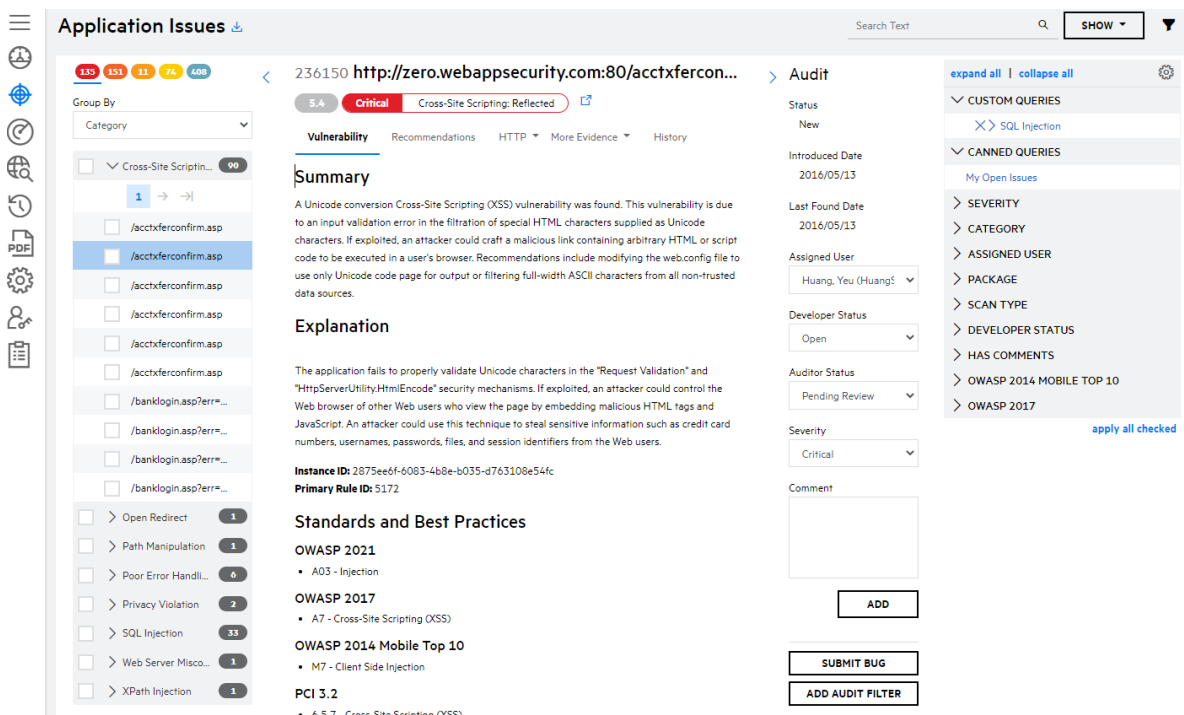
For information on creating a global audit template, see "[Creating a Global Audit Template](#)" on page 197.

## Creating an Application Audit Template Filter for an Issue

In addition to creating an application audit template from the ground up, users with the **Audit Issues** permission can create application audit template filters for an issue from the Issues page. This enables auditors to easily apply audit decisions to issues while reviewing them.

To create an application audit template filter for an issue:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application that you want to audit.  
The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page.



The screenshot displays the Fortify Application Issues interface. On the left, a sidebar shows a list of categories with counts, including 'Cross-Site Scripting' (90) and 'Open Redirect' (1). The main content area shows a vulnerability for 'Cross-Site Scripting: Reflected' on the URL 'http://zero.webappsecurity.com:80/acctxfercon...'. The vulnerability is marked as 'Critical' and has a 'Primary Rule ID' of 5172. The 'Summary' section explains that a Unicode conversion XSS vulnerability was found due to an input validation error. The 'Explanation' section details that the application fails to properly validate Unicode characters. The 'Standards and Best Practices' section lists OWASP 2021 (A03 - Injection), OWASP 2017 (A7 - Cross-Site Scripting (XSS)), OWASP 2014 Mobile Top 10 (M7 - Client Side Injection), and PCI 3.2 (6.5.7 - Cross-Site Scripting (XSS)). On the right, an 'Audit' panel is visible, showing filters for Status (New), Introduced Date (2016/05/13), Last Found Date (2016/05/13), Assigned User (Huang, Yeu (Huang)), Developer Status (Open), Auditor Status (Pending Review), and Severity (Critical). There are buttons for 'ADD', 'SUBMIT BUG', and 'ADD AUDIT FILTER'.

4. In the audit panel, click **Add Audit Filter**.





## Audit Template Usage and Examples

Audit template filters are aggregated sequentially in the order in which they appear. Global audit templates filters are aggregated first, then application audit template filters, to create a single overall set of audit decisions that are applied automatically when a scan is published. Issue changes as a result of audit templates appear in the **History** tab of the issue details panel as **Audit** type events. Global audit and application audit changes are logged separately.

In general, Fortify recommends using category-based filters over rule-based filters, with the exception of a few scenarios where using rule-based filters might be more appropriate. For example, you might want to use rule ID-based filters to handle different remediation policies around SSL/TLS checks in dynamic scans.

As changes are made to categories and rules with each security content update, it is important to review your filters after each security content update and update the filters as necessary:

- New categories might be added.
- Category names might be changed. You will need to update any category-based filters to reflect the changed names.
- New rules might be added to categories. Existing category filters will also apply to new rules. Note that new rules might cover new, critical vulnerabilities that are distinctly different from existing rules in a category.
- Existing rules might be updated to reflect new guidance and industry standards. For example, the severity given to a vulnerability might increase due to new information about the vulnerability.

For more information on category and rule changes, see the Fortify Software Security Content quarterly updates from Fortify Software Security Research (SSR). You can access them from the Help Center.

The following examples show several filter combinations and how they are applied.

### Example 1:

Audit template filters:

1. If **Severity Equals Critical**, then **Set Severity to High**
2. If **Severity Equals Critical**, then **Set Severity to Medium**

Result: Critical issues are set to Medium for the selected scan type.

### Example 2:

Audit template filters:

1. If **Severity Equals Critical**, then **Set Severity to High**
2. If **Severity Equals High**, then **Set Severity to Medium.**

Result: Critical issues are set to High, High issues are to set Medium for the selected scan type.

### Example 3:

Audit template filter: If **Rule ID Equals 11516**, then **Suppress.**

Result: Issues with rule ID 1156 are suppressed for the selected scan type

**Example 4:**

Global audit template filter: If **Severity Equals Critical**, then **Set Severity** to **High**

Application audit template filter: If **Severity Equals Critical**, then **Set Severity** to **Medium**

Result: Critical issues are set to High for all scans of the selected type, but Critical issues are set to Medium for scans of the selected type for the application above.

## Dataflow Cleanse Rules

Dataflow cleanse rules describe validation logic and other actions that render tainted data (user-controlled input) cleansed. Dataflow cleanse rules are incorporated in a static scan to help Fortify Static Code Analyzer recognize cleansing functions. As a result, dataflow cleanse rules help prevent false positives around dataflow issues.

Dataflow cleanse rules can be created at the global and application levels. Security Leads can manage global dataflow cleanse rules; users with the **Audit Issues** permission can manage dataflow cleanse rules for applications to which they have access.

**Important!** Dataflow cleanse rule is an advanced feature and can lead to significant changes in vulnerabilities found in a scan. Fortify strongly recommends that you review the documentation before using dataflow cleanse rules. If you have additional questions, contact support.

This section contains the following topics:

<a href="#">Creating a Global Dataflow Cleanse Rule</a> .....	206
<a href="#">Creating an Application Dataflow Cleanse Rule</a> .....	208
<a href="#">Dataflow Cleanse Rule Usage and Examples</a> .....	210

### Creating a Global Dataflow Cleanse Rule

Security Leads can manage global dataflow cleanse rules. Global dataflow cleanse rules apply to all static scans in the tenant.

Dataflow cleanse rules are subjected to the following conditions:

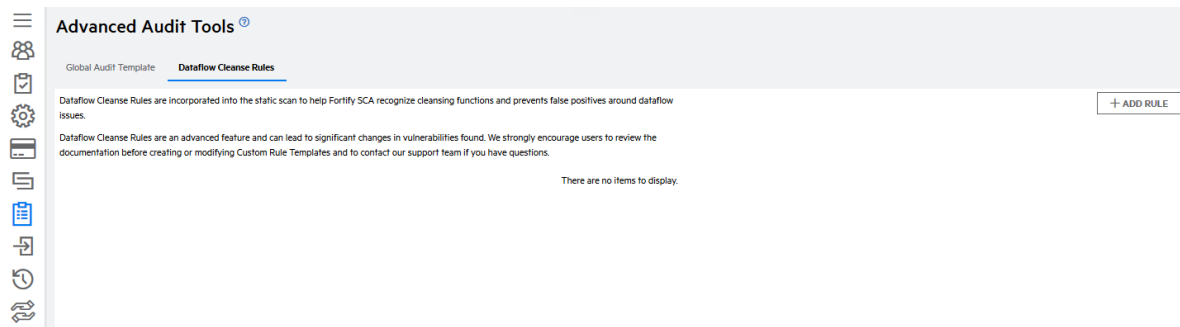
- Dataflow cleanse rules are case-sensitive and are restricted to alphanumeric characters.
- Dataflow cleanse rules are applied to scans that are started moving forward.

To create a global dataflow cleanse rule:

1. Select the **Administration** view.  
The User Management page appears.
2. Click **Audit Tools**.

The Advanced Audit Tools page appears.

3. Select the **Dataflow Cleanse Rules** tab.



4. Perform the following steps to add a rule. You can add multiple rules.

- a. Click **Add Rule**.

The Add Rule window opens.

- b. Complete the fields as needed. Fields are required unless otherwise noted.

**Note:** Rules do not apply against interfaces or super classes.

Field	Description
Language	Select the technology stack.
Package Name	(Optional) Type the name of the package or namespace that contains the validation function. If you do not specify a package name, the rule only matches functions that are not inside a package.
Class Name	(Optional) Type the name of the class that contains the validation function. If you do not specify a class name, the rule only matches functions that are not inside a

Field	Description
	<p>class. To specify a nested class, use the dot notation (for example, <code>OuterClass.NestedClass</code>).</p> <p><b>Note:</b> For .NET languages, the convention for the class name of a generic class is to append the class name with an @ and the number of type parameters. Example: for <code>System.Func&lt;T, TResult&gt;</code>, the class name would be <code>Func@2</code>.</p>
Function Name	Type the name of the validation function.
Category	Select the vulnerability category that is remediated by the validation function.
Data Validation	Select the data that has been validated by the function: <ul style="list-style-type: none"><li>◦ <b>Return Value:</b> use this option to refer to value in <code>value = web.getWebInput(foo, bar)</code></li><li>◦ <b>Object Function:</b> use this option to refer to web in <code>value = web.getWebInput(foo, bar)</code> or object in <code>object = new MyObject()</code></li><li>◦ <b>Argument:</b> use this option when referring to arguments of the function. Arguments are indexed beginning with 0. For example, specify 1 to refer to bar in <code>value = web.getWebInput(foo, bar)</code></li></ul>

5. Once you are done adding rules, click **Save**.

The global dataflow cleanse rules are saved.

## Creating an Application Dataflow Cleanse Rule

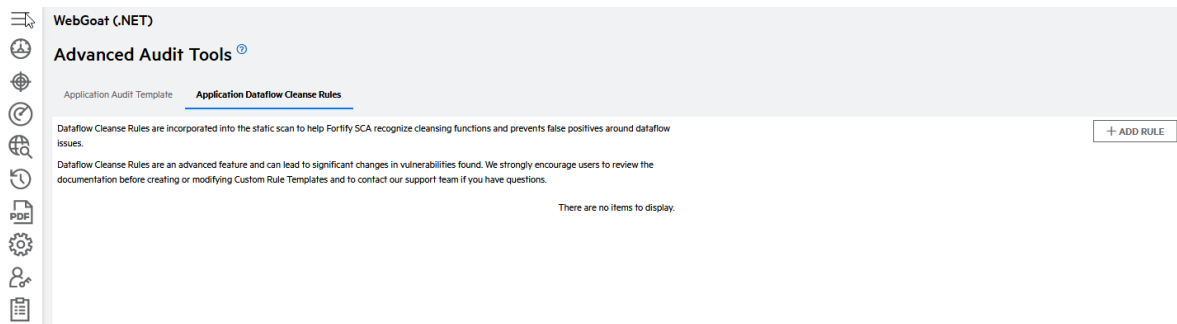
Users with the **Audit Issues** permission can manage dataflow cleanse rules for applications to which they have access. Application dataflow cleanse rules apply to all static scans for the application.

Dataflow cleanse rules are subjected to the following conditions:

- Dataflow cleanse rules are case-sensitive and are restricted to alphanumeric characters.
- Dataflow cleanse rules are applied to scans that are started moving forward.

To create an application dataflow cleanse rule:

1. Select the **Application** view.  
Your Applications page appears.
2. Click the name of the application for which you want to create an application audit template.
3. Click **Audit Tools**.  
The Advanced Audit Tools page appears.
4. Select the **Dataflow Cleanse Rules** tab.



5. Perform the following steps to add a rule. You can add multiple rules.
  - a. Click **Add Rule**.

The Add Rule window opens.

**Add Rule** ✕

<p>Language <span style="color: #0070C0;">?</span></p> <input style="width: 90%; border: 1px solid #ccc;" type="text" value="(Choose One)"/>	<p>Category</p> <input style="width: 90%; border: 1px solid #ccc;" type="text" value="(Choose One)"/>
<p>Package Name <span style="color: #0070C0;">?</span></p> <input style="width: 90%; border: 1px solid #ccc;" type="text"/>	<p>Data Validation <span style="color: #0070C0;">?</span></p> <input style="width: 90%; border: 1px solid #ccc;" type="text" value="(Choose One)"/>
<p>Class Name <span style="color: #0070C0;">?</span></p> <input style="width: 90%; border: 1px solid #ccc;" type="text"/>	
<p>Function Name <span style="color: #0070C0;">?</span></p> <input style="width: 90%; border: 1px solid #ccc;" type="text"/>	

SAVE
CANCEL

- b. Complete the fields as needed. Fields are required unless otherwise noted.

**Note:** Rules do not apply against interfaces or super classes.

Field	Description
Language	Select the technology stack.
Package Name	(Optional) Type the name of the package or namespace that contains the validation function. If you do not specify a package name, the rule only matches functions

Field	Description
	that are not inside a package.
Class Name	<p>(Optional) Type the name of the class that contains the validation function. If you do not specify a class name, the rule only matches functions that are not inside a class. To specify a nested class, use the dot notation (for example, OuterClass.NestedClass).</p> <p><b>Note:</b> For .NET languages, the convention for the class name of a generic class is to append the class name with an @ and the number of type parameters. Example: for <code>System.Func&lt;T, TResult&gt;</code>, the class name would be <code>Func@2</code>.</p>
Function Name	Type the name of the validation function.
Category	Select the vulnerability category that is remediated by the validation function.
Data Validation	<p>Select the data that has been validated by the function:</p> <ul style="list-style-type: none"> <li>◦ <b>Return Value:</b> use this option to refer to value in <code>value = web.getWebInput(foo, bar)</code></li> <li>◦ <b>Object Function:</b> use this option to refer to web in <code>value = web.getWebInput(foo, bar)</code> or object in <code>object = new MyObject()</code></li> <li>◦ <b>Argument:</b> use this option when referring to arguments of the function. Arguments are indexed beginning with 0. For example, specify 1 to refer to bar in <code>value = web.getWebInput(foo, bar)</code></li> </ul>

- Once you are done adding rules, click **Save**.

The application dataflow cleanse rules are saved.

## Dataflow Cleanse Rule Usage and Examples

Global and application dataflow cleanse rules are aggregated into a single set of rules that are applied during a scan. Issues that are removed based on rules do not appear in the FPR.

The following examples show several dataflow cleanse rules and how they are applied.

Example 1:

Language: **Java**  
Package Name: `com.fortify.appsec`  
Class name: `Validation`  
Function Name: `validateAlphaNumeric`  
Category: **SQL Injection**  
Data Validation: **Return Value**

Result: The return value of the method is considered cleansed and will not be flagged as a SQL Injection issue.

**Example 2:**

Language: **Java**  
Package Name: `java.util`  
Class name: `Map`  
Function Name: `clear`  
Category: **SQL Injection**  
Data Validation: **Object Function**

Result: The data is considered cleansed after a call to the `Map.clear()` method and will not be flagged as a SQL Injection issue.

## Requesting a Remediation Scan

After changes have been made to fix the issues identified in the initial scan, you can request a remediation scan to verify whether the issues have been fixed. Assessments include one or more remediation scans:

- Single assessments include one remediation scan.
- Subscriptions include unlimited remediation scans during the remediation scan period.

Fortify on Demand typically limits a remediation scan to 30 days after the initial scan. Exceptions are noted in your contract.

Request a remediation scan by selecting **<assessment\_type> - Remediation** on the Scan Setup page. The remediation scan must be performed on the same application. For example, if the initial scan was done on the pre-production site, the remediation scan must also be on the pre-production site. A remediation scan takes less time than a full initial scan.

**Note:** For a dynamic scan, the following fields are locked to the values specified in the initial scan: **Dynamic Site URL, Environment Facing, Scan entire host, Restrict scan to URL directory and**

**subdirectories, Allow HTTP (:80) and HTTPS (:443), Allow form submissions, and Exclude URLs which contain <exclusion>.**



# Chapter 6: Dashboards and Reports

Fortify on Demand delivers assessment results in a variety of formats for viewing and analyzing data.

Dashboards provide a visual display of key metrics. Users can configure multiple dashboards to display data that is relevant to their needs. While dashboards are useful for general summaries, users can get a detailed view of assessment results through reports. Fortify on Demand provides a comprehensive and customizable suite of reports.

This section contains the following topics:

- [Dashboards](#) ..... 213
- [Reports](#) ..... 224

## Dashboards

A dashboard is made up of individual tiles that each present a specific facet of data as a visual element. You are initially provided with one of the following default dashboard configurations based on your user role:

- Development dashboard for Developer, Lead Developer, and Application Lead roles
- Security dashboard for Security Lead and TAM roles
- Management dashboard for Executive and Reviewer roles
- Management dashboard for custom roles

You can edit the default dashboard as well as create additional dashboards.

This section contains the following topics:

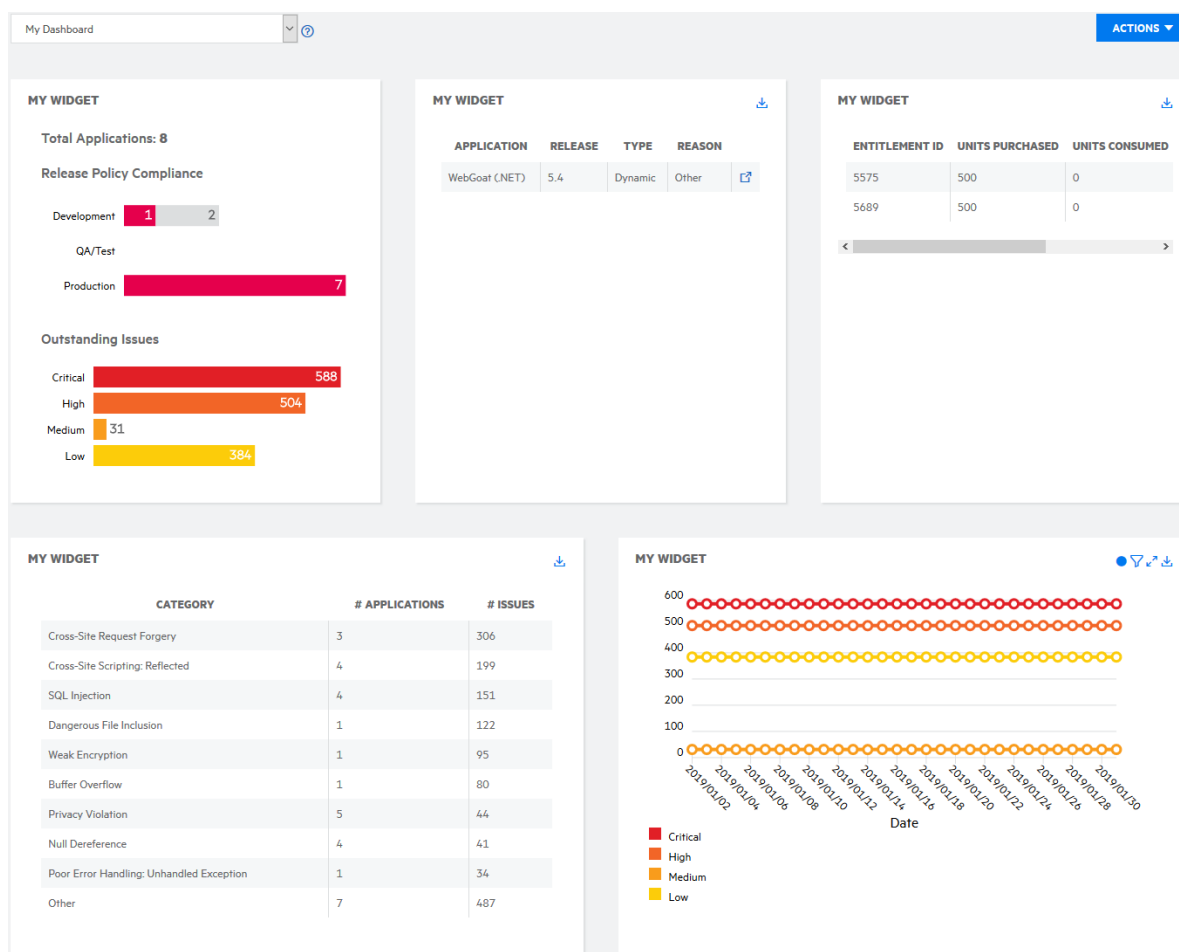
- [Viewing Dashboards](#) ..... 213
- [Dashboard Graph Types](#) ..... 215
- [Creating a Dashboard](#) ..... 218
- [Editing a Dashboard](#) ..... 220
- [Deleting a Dashboard](#) ..... 222

## Viewing Dashboards

To view your dashboards:

1. Select the **Dashboard** view.  
The dashboard page appears. It displays the last dashboard that was loaded.






**Note:** If you have not yet configured a dashboard, a default dashboard configuration based on your user role is loaded.



2. Select the dashboard that you want to view from the drop-down list.  
The selected dashboard is loaded.

The following table describes how to navigate the dashboard page.

Task	Action
Create a dashboard	Select <b>Actions</b> > <b>New Dashboard</b> . For more information, see <a href="#">"Creating a Dashboard"</a> on page 218.
Edit the dashboard	Select <b>Actions</b> > <b>Edit Dashboard</b> . For more information, see <a href="#">"Editing a Dashboard"</a> on page 220.
Generate a PDF of the dashboard	Select <b>Actions</b> > <b>Print</b> .

Display or hide data point markers	Click  in a trending chart tile.
View filters applied to a tile	Click  .
Export data that makes up a tile	Click  . A .csv file is saved locally to the folder specified in your browser settings.
View details of a scan	Click  in a list grid tile.
Expand a tile	Click  in a trending chart tile.

## Dashboard Graph Types

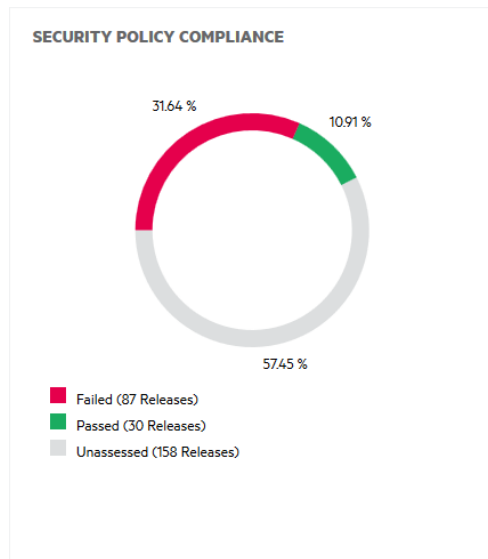
The following tile types are available in a dashboard:

- Gauge
- List Grid
- Summary
- Trending Chart

### Gauge

The **Gauge** tile is a gauge graph summarizing one of the following data items: assessed releases, auditor status, developer status, entitlement consumption, issue assignment, and security compliance.

Data Item Type	Description
Assessed Releases	Assessment state of issues
Auditor Status	Auditor status of issues
Developer Status	Developer status of issues
Entitlement Consumption	Usage of active entitlements
Issue Assignment	Assignment state of issues
Security Compliance	Policy compliance status across releases



## List Grid

The **List Grid** tile is a list or grid view of one of the following data items: active entitlements, canceled scans, completed scans, in progress scans, most prevalent issues, my issues, paused scans, and scheduled scans. For scans, the List Grid also contains links to the relevant Scan Setup page or Scans page.

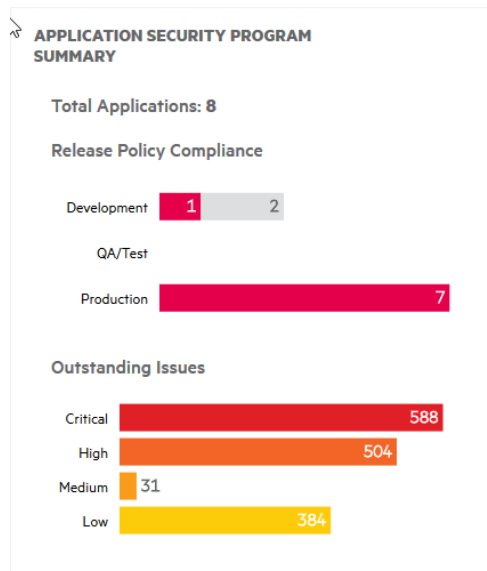
Data Item Type	Description
Active entitlements	Active entitlements
Canceled scans	Scans that were canceled
Completed scans	Scans that were completed
In progress scans	Scans currently in progress
Most prevalent issues	Most prevalent issues across all applications
My issues	Issues assigned to the current user account
Paused scans	Scans paused by the testing team
Scheduled scans	Scans that have been scheduled

**PAUSED SCANS**

APPLICATION	RELEASE	TYPE	REASON	
WebGoat (NET)	5.4	Dynamic	Other	<a href="#">🔗</a>

## Summary

The **Summary** tile is a quick summary of the security risk of your releases. It shows the total number of applications in the portfolio and the following information about development, QA, and production releases: security policy compliance and outstanding issues (issues that are not fixed validated or suppressed).

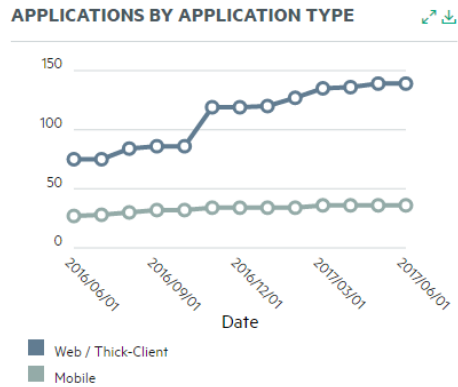


## Trending Chart

The **Trending Chart** tile is a line graph of one of the following data items over time: applications, entitlements, issues, releases, and scans. Data series are grouped by a specified attribute.

**Note:** Data points for all items are measured additively except for scans.

Data Item Type	Description
Applications	Number of applications, grouped by an application attribute
Entitlements	Number of entitlement units, grouped by units purchased, consumed, or available
Issues	Number of issues, grouped by an issue attribute
Releases	Number of releases, grouped by an application or release attribute
Scans	Number of scans, grouped by the scan status



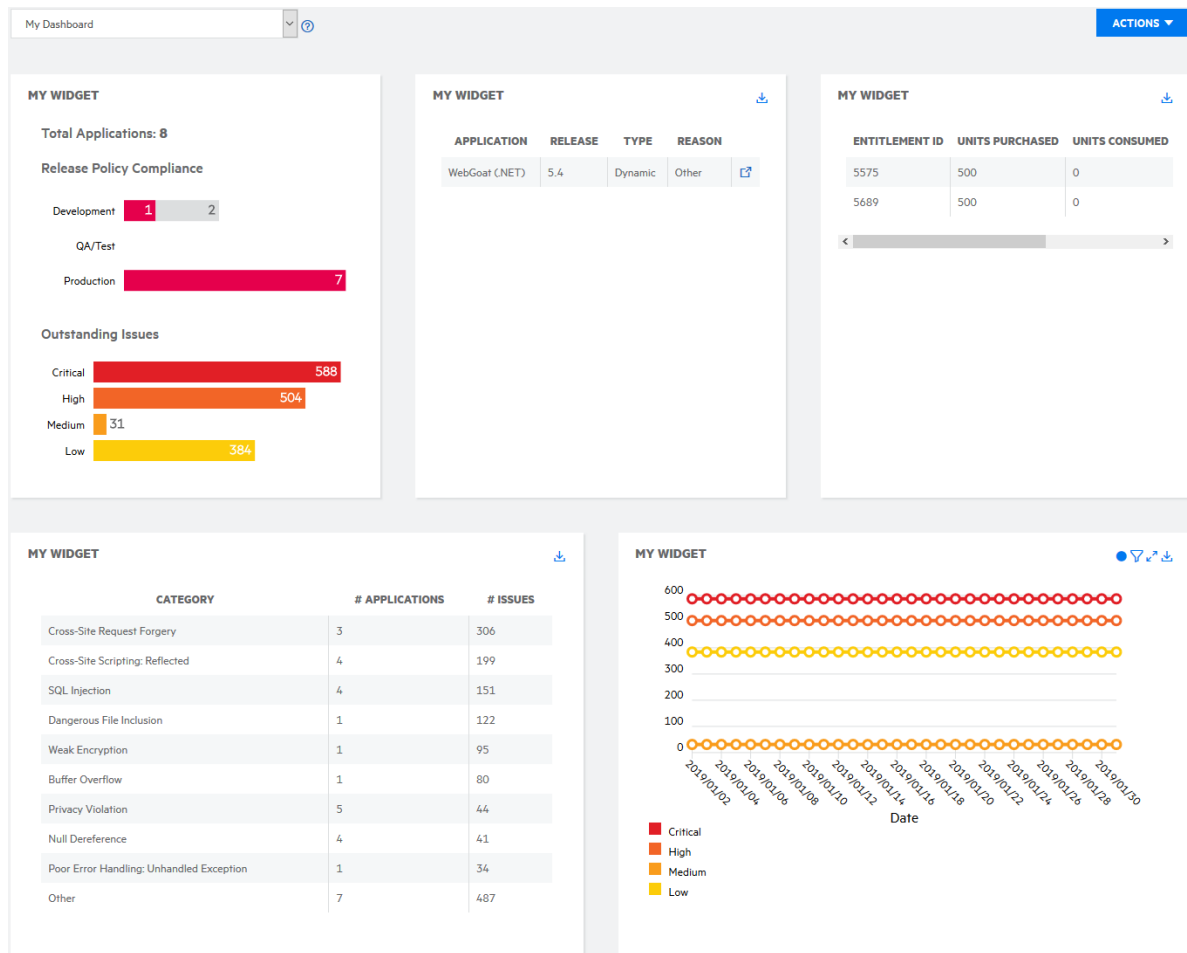
## Creating a Dashboard

You can create additional dashboards for organizing different facets of data. You can have up to 10 dashboards.

To create a dashboard:

1. Select the **Dashboard** view.

The dashboard page appears. It displays the last dashboard that was loaded.



2. Select **Actions > New Dashboard**.

The Create a Dashboard window opens.

The 'Create a Dashboard' dialog box includes the following elements:

- Dashboard Name:** A text input field with a pink border.
- Dashboard Layout:** Three radio button options:
  - Blank
  - Default
  - Copy from existing Dashboard
- SAVE:** A blue button at the bottom right.

3. In the **Dashboard Name** field, type a name for the new dashboard.

4. Select the initial layout of the new dashboard:

- **Blank:** start with a blank dashboard
  - **Default:** use the default dashboard configuration for your user role
  - **Copy from existing Dashboard:** copy the layout of an existing dashboard
5. Click **Save**.  
The new dashboard appears.

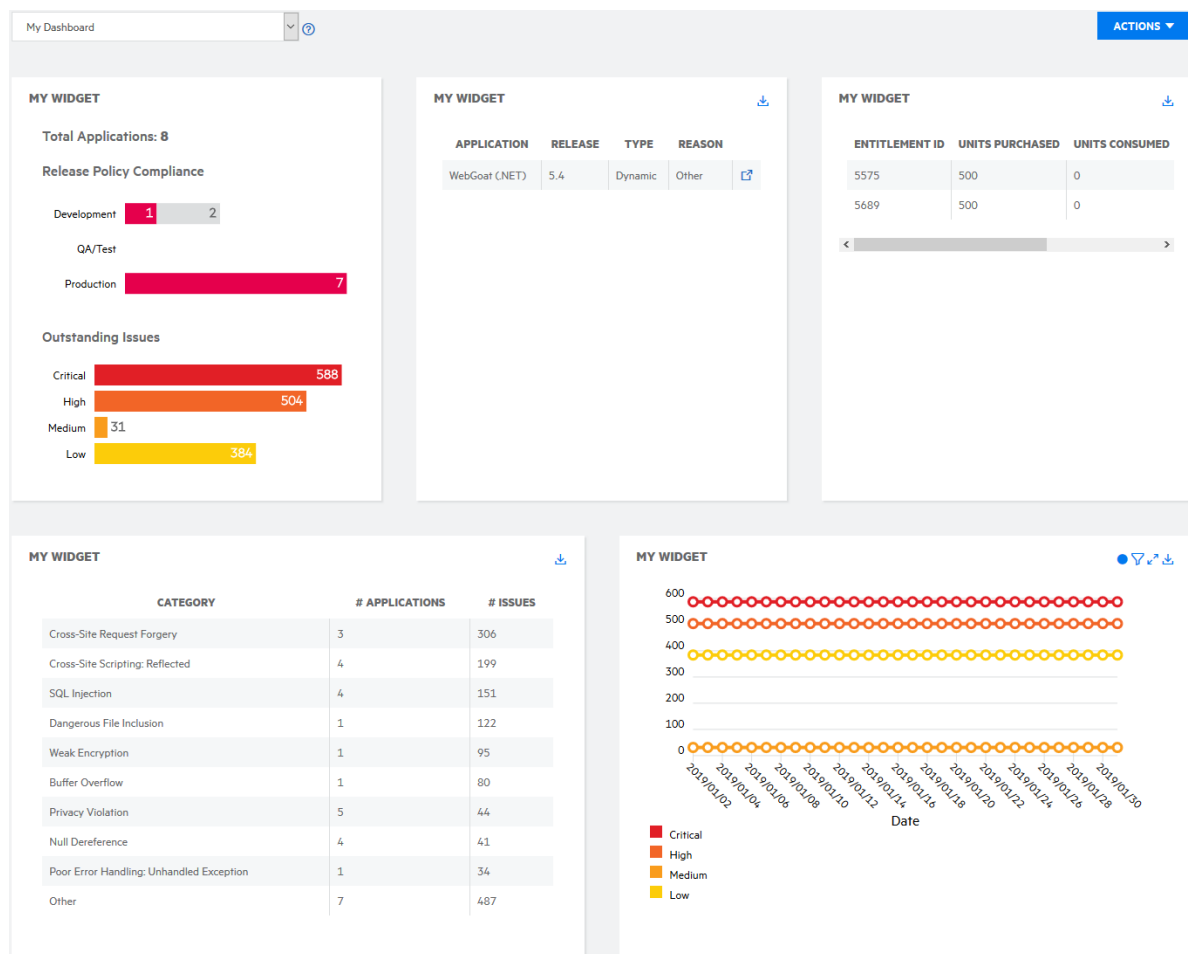
## Editing a Dashboard

You can edit a dashboard by adding, editing, rearranging, and deleting rows and tiles. A dashboard can have up to ten tiles with a maximum of three tiles per row.

To edit a dashboard:

1. Select the **Dashboard** view.

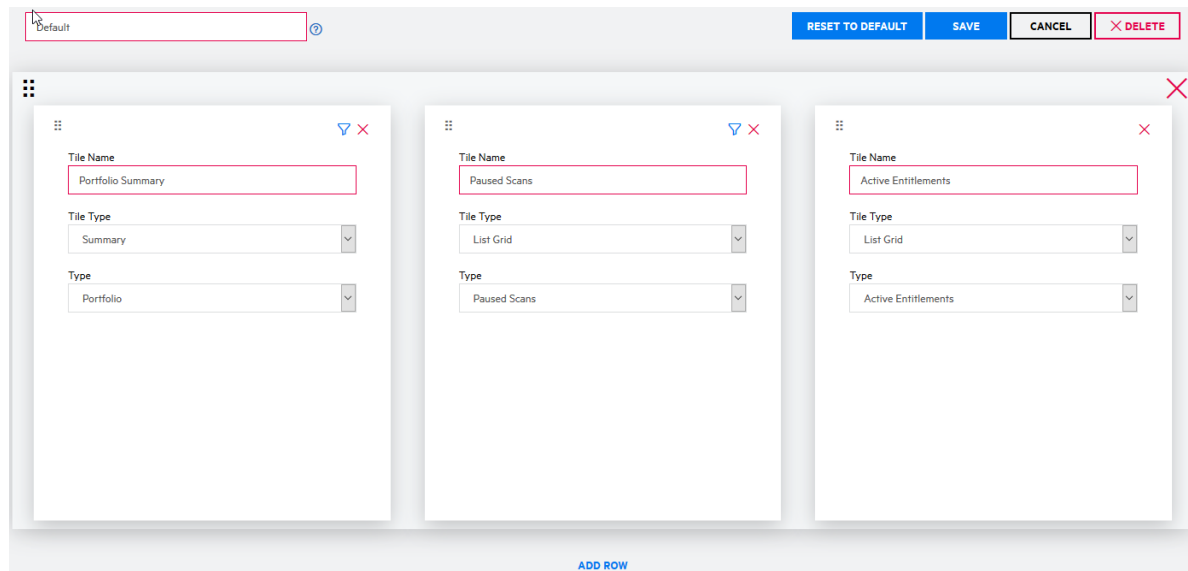
The dashboard page appears. It displays the last dashboard that was loaded.



2. Select the dashboard that you want to edit from the drop down list.
3. Select **Actions > Edit Dashboard**.






The dashboard refreshes in edit mode.



4. Perform one or more following tasks to edit the dashboard:

Task	Procedure
Add a tile	<ol style="list-style-type: none"> <li>a. Perform one of the following actions: <ul style="list-style-type: none"> <li>◦ Click <b>+</b> in a row to add a tile (if available).</li> <li>◦ Click <b>Add Row</b> to add a tile in a new row (if available).</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"><b>Note:</b> Each row can contain up to a maximum of three tiles.</div> </li> <li>b. In the <b>Tile Name</b> field, type a name for the tile.</li> <li>c. Select the tile type from the <b>Tile Type</b> list. For a description of the tile types, see "<a href="#">Dashboard Graph Types</a>" on page 215.</li> <li>d. Perform the relevant action based on the tile type you selected. <ul style="list-style-type: none"> <li>◦ If you selected <b>Gauge</b>, select the data item to be represented from the <b>Type</b> list.</li> <li>◦ If you selected <b>List Grid</b>, select the data item to be represented from the <b>Type</b> list.</li> <li>◦ If you selected <b>Summary</b>, select the data item to be represented from the <b>Type</b> list. The current available value is <b>Portfolio</b>.</li> <li>◦ If you selected <b>Trending Chart</b>, select the data item to be represented from the <b>Data Type</b> list, select the time period of the graph from the <b>Resolution</b> list, and select the attributes by which to group the data from the <b>Group By</b> lists.</li> </ul> </li> </ol>

	e. If applicable, click  and select the filter values to be applied. The filters that are available depend on the data item type selected.
Edit a tile	Choose an existing tile to edit and update the fields as needed.
Move a row/tile	Click  and drag the row/tile to the desired slot. <b>Note:</b> You can move a tile within a row, but you cannot move a tile to another row.
Delete a row/tile	Click  next to the row/tile.
Reset dashboard to the default configuration	Click <b>Reset to Default</b> .
Return to the view mode without saving changes	Click <b>Cancel</b> .

5. Click **Save**.

The dashboard refreshes with your changes.

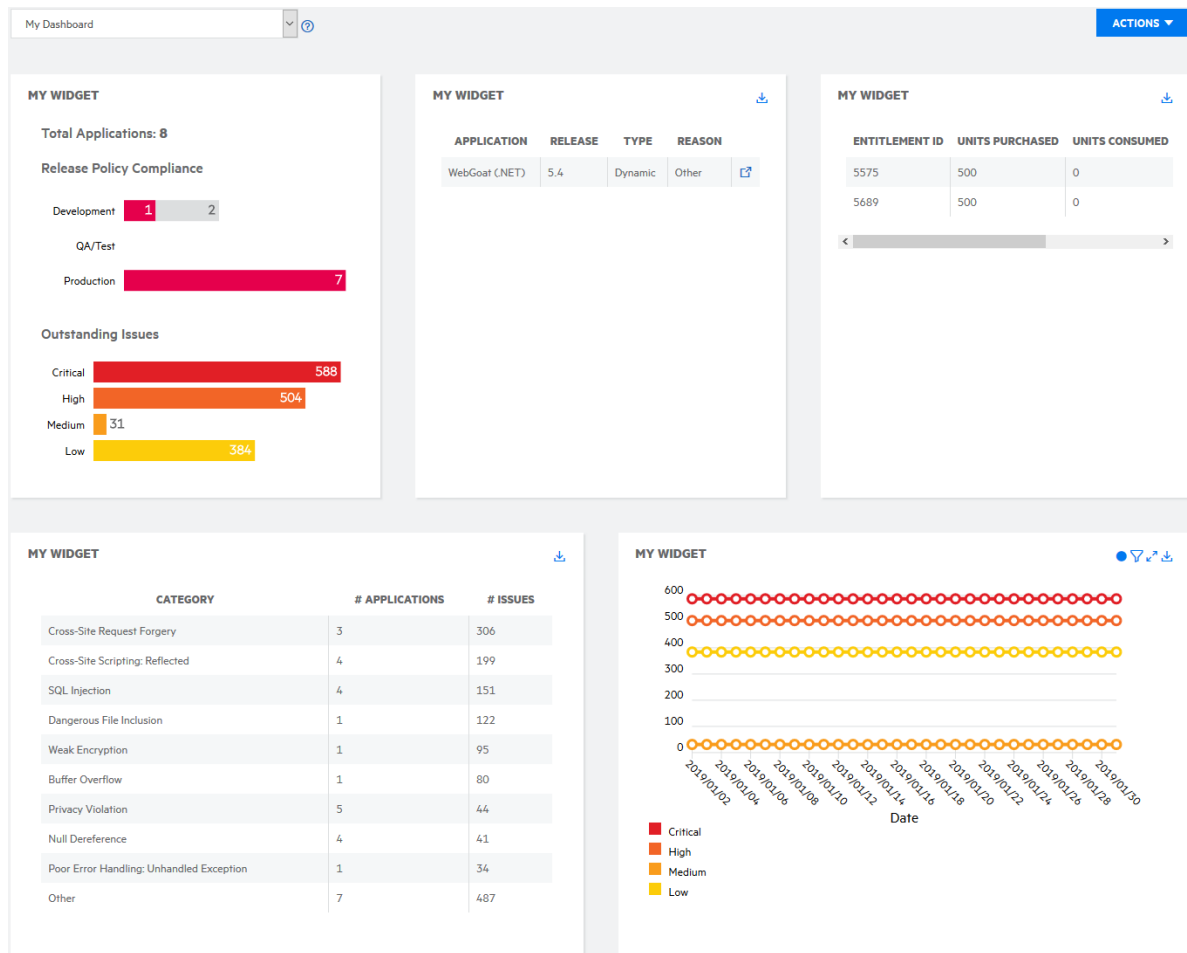
## Deleting a Dashboard

To delete a dashboard, you must have at least one other dashboard. If you want to delete your only dashboard, you will need to first create another one.

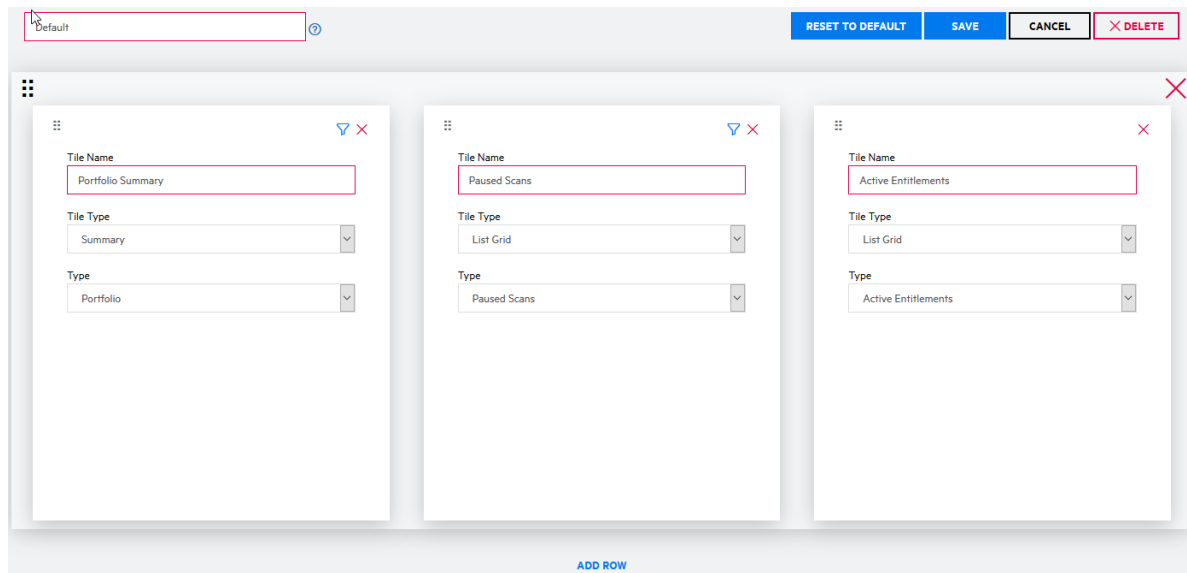
To delete a dashboard:

1. Select the **Dashboard** view.

The dashboard page appears. It displays the last dashboard that was loaded.



2. Select the dashboard that you want to delete from the drop down list.  
The selected dashboard is loaded.
3. Select **Actions** > **Edit Dashboard**.  
The dashboard refreshes in edit mode.



4. Click **Delete**.  
A confirmation message appears.
5. Click **Yes**.  
The dashboard is deleted.

## Reports

Fortify on Demand offers the ability to generate detailed reports of assessment results. You can generate the following types of reports:

- pre-defined system reports
- customized reports
- data exports of applications, releases, scans, issues, or entitlement consumption
- vendor reports if you are using the Vendor Management feature

This section contains the following topics:

<a href="#">Viewing Reports</a> .....	225
<a href="#">Generating a Report</a> .....	227
<a href="#">Scheduling Auto-Generated Reports</a> .....	230
<a href="#">Templates</a> .....	232
<a href="#">Data Exports</a> .....	236

## Viewing Reports

There are two ways to view reports in the portal. One way is to go through the **Reports** view, where you can view all reports generated for all applications and releases in your tenant. The other way is to go through the **Applications** view, where you can drill down into each application and view reports pertaining to a specific application or release.

This section contains the following topics:

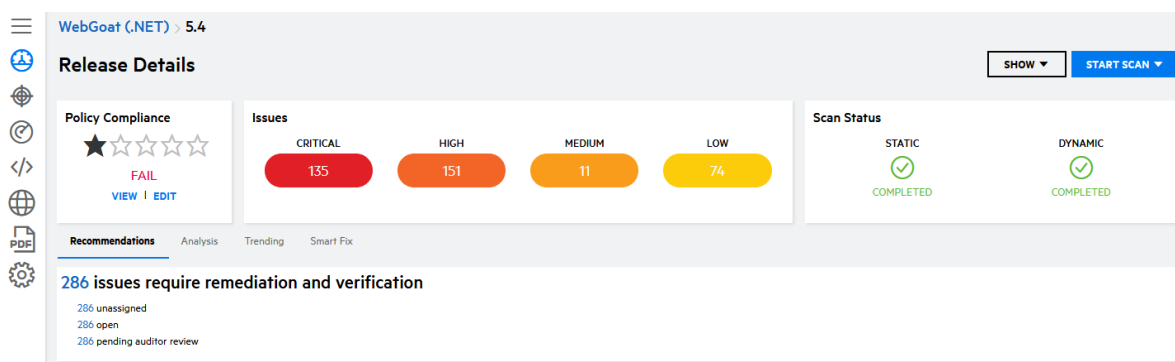
<a href="#">Accessing Reports for a Release</a> .....	225
<a href="#">Accessing Reports for an Application</a> .....	226
<a href="#">Accessing Your Reports Grid</a> .....	227

### Accessing Reports for a Release

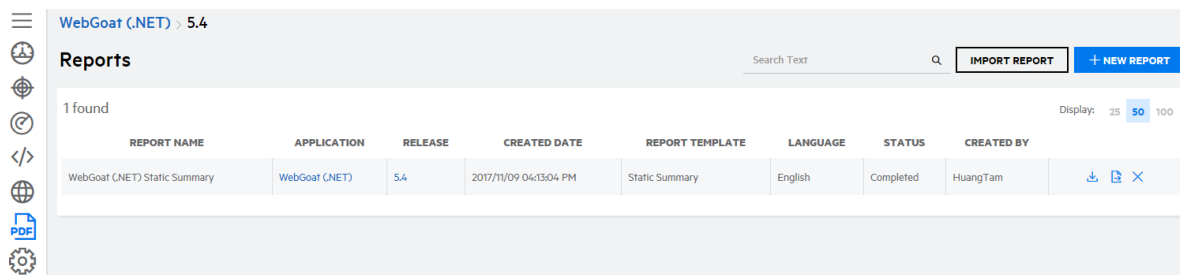
At the release level, the Reports page displays all reports that apply to the selected release.

To access all reports that apply to a release:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears.
3. Click the name of the release that you want to view reports for.  
The Release Overview page appears.



4. Click **Reports**.  
The Reports page appears displaying all reports for the release.



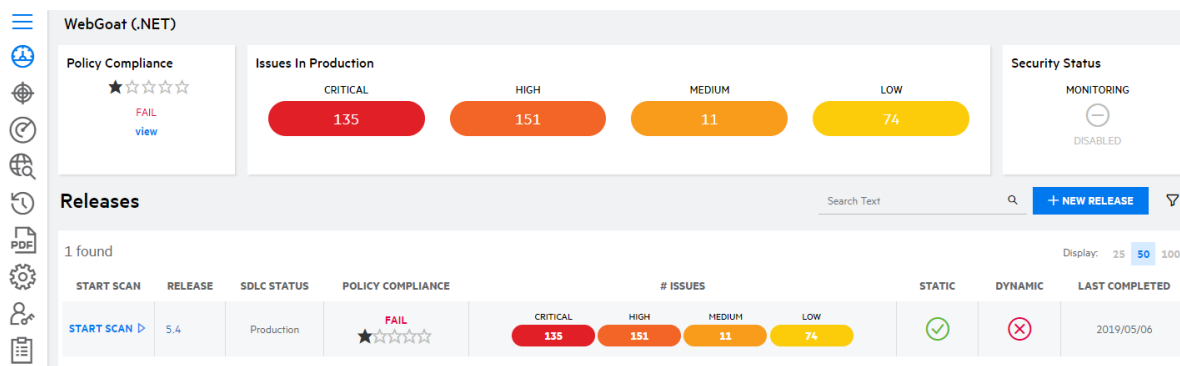
5. Select a report from the list.

## Accessing Reports for an Application

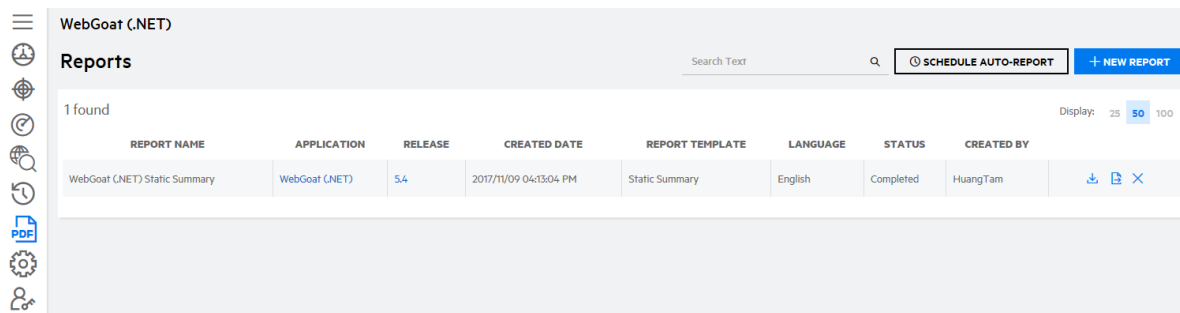
At the application level, the Reports page displays all reports for the selected application.

To access all reports that apply to an application:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application for which you want to view reports.  
The Application Overview page appears.



3. Click **Reports**.  
The Reports page, displaying all reports for the application.



4. Select a report from the list.

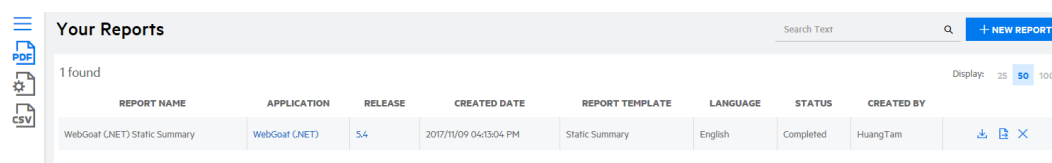
## Accessing Your Reports Grid

Your Reports grid is the default landing page of the Report view. It lists all reports generated for all applications and releases. On this page, you can see the application and release with which each report is associated, the date and time when the report was generated, the report type, and the status of the report generation.

To access reports for all applications and releases in your tenant:

1. Select the **Reports** view.

Your Reports page appears, displaying a list of reports that have been generated for your tenant.



## Navigating Your Reports Page

The following table describes how to navigate Your Reports page.

Task	Action
Create a Report	Click <b>+New Report</b> . Opens the Report Generation Wizard.
Download a report	Click <a href="#">↓</a> . The report is downloaded to the local folder specified in your browser settings.
Share a report with a tenant	Click <a href="#">🔗</a> . The icon appears only if you have established a relationship with another tenant (such as a vendor). See <a href="#">"Vendor Management" on page 301</a> .
Delete a report	Click <a href="#">✕</a> . Note that you can delete a report before it has finished processing.
Search the reports list	Type a keyword or phrase in the <b>Search Text</b> field and click <b>Enter</b> . To remove the search results, Click the <b>X</b> .  For information on using the <b>Search Text</b> box, see <a href="#">"Searching Applications and Releases" on page 80</a> .

## Generating a Report

Use a pre-defined report template or a custom report template to generate a report of a release. Reports are available in PDF and HTML formats. In the event a PDF report generation fails, the HTML version is automatically provided in place of the PDF version for your convenience.

To help avoid failures when generating extremely large PDF reports, you cannot generate PDF reports that include the **Analyst Trace**, **Request/Response**, or **Issues Details** template modules and contain more than 5000 issues. Either generate HTML reports or use an alternative report template with the modules removed and/or with additional filters that reduce the issue count.

**Note:** To generate reports in a certain language, the language must be selected in your account settings. For more information, see ["Editing Your Account Settings" on page 27](#).

To generate a report:

1. Navigate to one of the following pages: Your Reports page, the Application Report page, or the Release Reports page. For more information, see ["Viewing Reports" on page 225](#).
2. Click **+New Report** to start the Report Generation Wizard.

## Completing the Report Generation Wizard

Complete the fields as needed. Fields are required, unless otherwise noted:

### Application/ Release (Step 1 of 4)

Select the application name and release that you want to create a report for.

The screenshot shows the 'Create Report' wizard interface. On the left, there is a sidebar with navigation options: 'Select Release', 'Report Details', 'Report Template', and 'Summary'. The main area displays a search bar with 'Search Text' and a magnifying glass icon. Below the search bar, it indicates '8 found' and 'Display: 25 50 100'. The main content is a table with two columns: 'APPLICATION' and 'RELEASE'. Each row has a radio button in the first column. The table lists the following applications and releases:

APPLICATION	RELEASE
<input type="radio"/> Zero Security (COBOL)	12.6.8
<input type="radio"/> WebGoat (.NET)	5.4
<input type="radio"/> Rubix (JAVA-No Source)	0.1
<input type="radio"/> OpenSSL (C Source)	1.0.2a
<input type="radio"/> Jeopardy (PHP)	3.1
<input type="radio"/> Jeopardy (PHP)	3.2
<input type="radio"/> iGoat IOS (Objective-C)	2.4
<input type="radio"/> iGoat Android (JAVA)	2.4

At the bottom of the interface, there are three buttons: 'BACK', 'NEXT', and 'GENERATE'.

1. Click the radio button to make your selection.
2. Click **Next**.

### Report Details (Step 2 of 4)

The second step is to define report details.



### Field Descriptions

Field	Description
<b>Report Name</b>	Name your Report.
<b>Notes</b>	(Optional) Add notes about the report that help you manage your reports.
<b>File Type</b>	Select the file type you would like your report to appear in. Available values are PDF and HTML.

- Click **Next**.

### Report Template (Step 3 of 4)

Select the report template you want to generate from the list of templates available for the release.

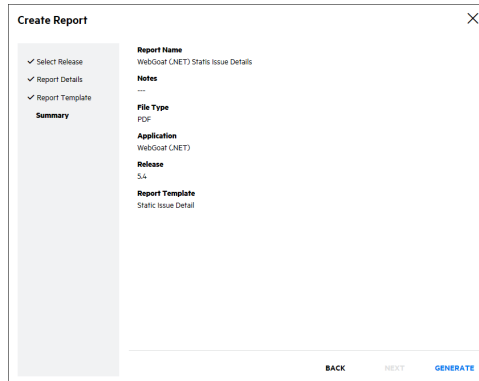
- Pre-defined report templates are highlighted.
- Custom templates you have defined appear in black type.
- If your release has only static analysis data, only static report templates appear in the list.
- If you have done only a dynamic analysis of this release, only the relevant dynamic report templates will appear as options.

- Click **Next**.


## Review Step 4 of 4

Review the information on the Review window. If everything is as you intended

1. Click **Generate**.



The new report appears on the report list with a status of **Queued**. The status changes to **Completed** once the report has been generated.

**Note:** To delete the report before processing has completed, click .

## Scheduling Auto-Generated Reports

If you plan to run multiple assessments on the same application and you would like to generate the same reports each time, you can save time by using the auto-generated report function.

To schedule an auto-generated report:

1. Select the **Applications** view.  
**Your Releases** grid appears, displaying a list of your releases.

The screenshot shows the 'Your Releases' dashboard. At the top, there is a search bar and buttons for '+ NEW APPLICATION' and 'EXPORT'. Below the search bar, there are filters for 'All' (9), 'Development' (2), 'QA/Test' (0), 'Production' (7), and 'Retired' (0). The main content area shows '9 found' and a 'SELECT ALL' link. The table has columns for 'START SCAN', 'APPLICATION', 'RELEASE', 'SDLC STATUS', 'APPLICATION CREATED DATE', and '# ISSUES'. The '# ISSUES' column is broken down into 'CRITICAL', 'HIGH', 'MEDIUM', and 'LOW' counts. A sidebar on the right contains a filter menu for 'APPLICATION TYPE' with categories like 'Mobile' (2) and 'Web / Thick-Client' (7), and other expandable sections like 'BUSINESS CRITICALITY', 'DYNAMIC SCAN STATUS', 'MOBILE SCAN STATUS', 'PASS/FAIL', 'STAR RATING', 'SCAN TYPE', and 'APPLICATION CREATED DATE'.

START SCAN	APPLICATION	RELEASE	SDLC STATUS	APPLICATION CREATED DATE	# ISSUES				
<input type="checkbox"/>	<a href="#">START SCAN</a>	WebGoat (.NET)	5.4	Production	2016/05/13	CRITICAL 135	HIGH 151	MEDIUM 11	LOW 74
<input type="checkbox"/>	<a href="#">START SCAN</a>	Jeopardy (PHP)	3.1	Production	2016/05/13	CRITICAL 160	HIGH 5	MEDIUM 0	LOW 147
<input type="checkbox"/>	<a href="#">START SCAN</a>	Jeopardy (PHP)	3.2	Development	2016/05/13	CRITICAL 160	HIGH 5	MEDIUM 0	LOW 147
<input type="checkbox"/>	<a href="#">START SCAN</a>	Zero Security (COBOL)	12.6.8	Production	2016/05/13	CRITICAL 11	HIGH 4	MEDIUM 0	LOW 0
<input type="checkbox"/>	<a href="#">START SCAN</a>	OpenSSL (C Source)	1.0.2a	Production	2016/05/13	CRITICAL 64	HIGH 155	MEDIUM 0	LOW 0
<input type="checkbox"/>	<a href="#">START SCAN</a>	Rubix (JAVA-No Source)	0.1	Production	2016/05/13	CRITICAL 1	HIGH 7	MEDIUM 0	LOW 0
<input type="checkbox"/>	<a href="#">START SCAN</a>	iGoat Android (JAVA)	2.4	Production	2016/05/13	CRITICAL 43	HIGH 122	MEDIUM 18	LOW 15

2. Click the name of the application you want to schedule auto-generated reports for.
3. Click **Reports**.  
The Reports page appears.
4. Click **Schedule Auto-Report**.  
The Schedule an Auto-Generated Report modal window appears.

### Schedule an Auto-Generated Report ✕

Please select a report template that will be scheduled to auto-generate a report once a Static scan completes for this application.

(Report not Scheduled) ▼

Please select a report template that will be scheduled to auto-generate a report once a Dynamic scan completes for this application.

(Report not Scheduled) ▼

SDLC Status

Development  QA/Test  Production

File Type:

PDF ▼

Email Report Upon Completion

Notification List

Insert emails separated by semicolons

[SAVE](#) [CANCEL](#)

5. Select the report template that will be used to generate a report upon completion of a static scan.
6. Select the report template that will be used to generate a report upon completion of a dynamic or mobile scan.
7. Select the SDLC status check box(es) that will trigger the report generation.
8. Select the report file type from the **File type** list.
9. To automatically distribute the reports to specified recipients, select **Email Report Upon Completion** and in the **Notification List** field, type the email addresses that will receive the reports.
10. Click **Save**.  
Your auto-generated report settings are saved.

## Templates

Users with the Create Report permission can view, create, edit, and delete templates.

The Templates page displays a list of existing report templates, with links for viewing, copying / editing, and deleting templates. There are two types of report templates: system and custom.

System report templates exist for Application Monitoring, Static, Dynamic, Hybrid, and Mobile reports as well as ones for PCI, STIG, and FISMA compliance reports. System templates can be copied and suppressed, but not edited or deleted.

Fortify on Demand provides a **Template Wizard** for creating custom report templates. You can configure the report modules and filters to include in the template and use it to generate reports containing the information most useful to your organization. The custom report templates can be edited and deleted.

**Use case:** If your report is for high-level management review and the people reading it do not want to see the details of your security assessment, you can select the **Static Summary** template. It includes: a title page, an executive summary, an issue breakdown, a list of issues by analysis type, and the OWASP Top 10. It does not include PCI reporting, comments on the issue details, or an analysis trace report (unless you add those).


This section covers the following topics:

<a href="#">Creating a Custom Report Template</a> .....	233
<a href="#">Editing a Custom Report Template</a> .....	235
<a href="#">Deleting a Custom Report Template</a> .....	236
<a href="#">Suppressing a System Report Template</a> .....	236

## Creating a Custom Report Template

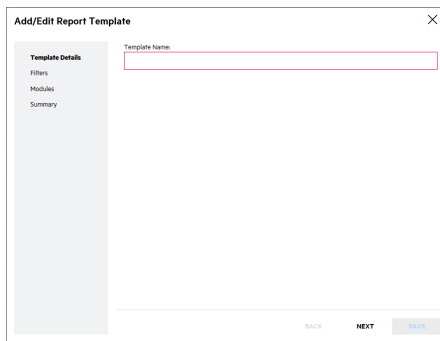
You can create a custom report template by either creating a report template from scratch or starting with one of the system template and modifying it to suit your needs.

To create a custom report template:

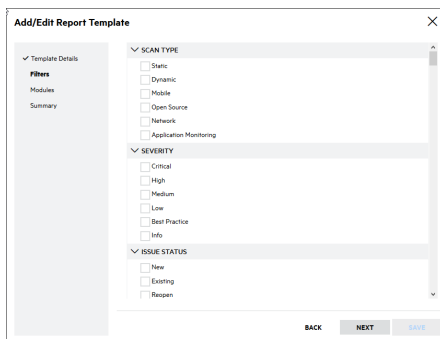
1. Select the **Reports** view.
2. Click the **Templates** icon.  
The Templates page appears.
3. Perform one of the following actions:
  - Click **+New Template** to create a template from scratch.
  - Click the  icon in the desired system template row to clone the template.

The Add/Edit Report Template wizard appears.

4. **Template Details:** in the **Template Name** field, type the name of the new template and click **Next**.



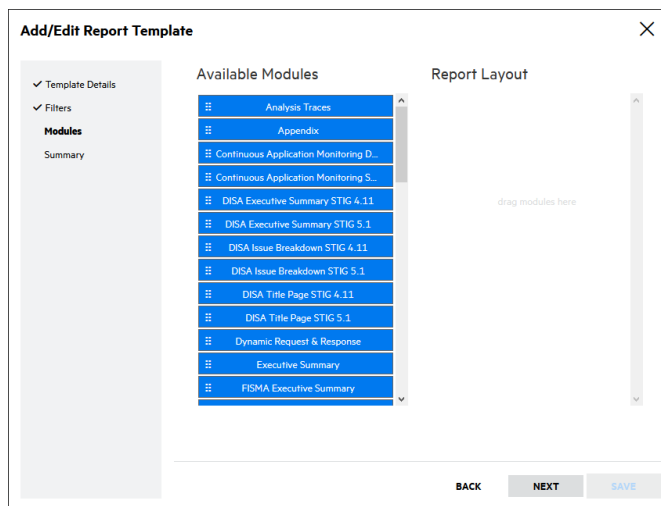
5. **Filters:** select the desired filters and click **Next**. Fields are required unless otherwise noted.



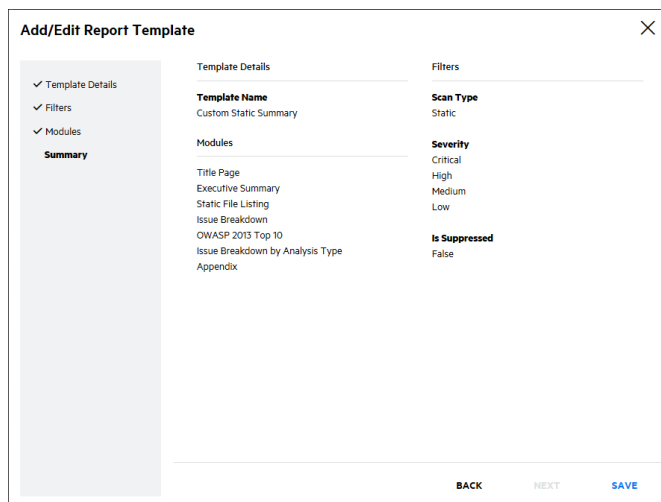
Field	Description
Scan Type	Scan type
Severity	(Optional) Severity of the issues
Issue Status	(Optional) Status of the issues ( <b>New, Existing, Reopen</b> )
Developer Status	(Optional) Developer status of the issues
Auditor Status	(Optional) Auditor status of the issues
Issue Age	(Optional) Days since the issues were first introduced
Category	(Optional) Vulnerability category of the issues
Is Suppressed	(Optional) Suppression state of issues (default value is <b>False</b> )

6. **Modules:** select the report modules to include in the template and click **Next**.

- Drag the modules that you want to include from the **Available Modules** column to the **Report Layout** column. The modules that are available depend on the selected scan type.
- Drag and drop items in the **Reports Layout** column to change the order of the modules in the generated report.



7. **Summary:** review the summary of the template and click **Save**.




The custom report template appears in the template list. If necessary, run a search of the name to find the template.

## Editing a Custom Report Template

You can edit an existing custom report template through the Add/Edit Report Template wizard.

To edit a custom report template:

1. Select the **Reports** view.
2. Click **Templates**.  
The Templates page appears.
3. Click the  icon in the row of the template that you want to edit.  
The Add/Edit Report Template wizard appears.

4. Edit the fields in each step of the wizard as needed. For more information, see "[Creating a Custom Report Template](#)" on page 233


**Note:** Removal of deprecated modules is permanent and cannot be undone after the template is saved.

5. Click **Save**.  
The template changes are saved.

## Deleting a Custom Report Template



You can delete any of your custom report templates in your tenant.

To delete a custom report template:

1. Select the **Reports** view.
2. Click **Templates**.  
The **Templates** page appears.
3. Locate the custom template that you want to delete in the template list.
4. Click the  icon in the template row.  
A confirmation message appears.
5. Click **Yes** to delete the template.

## Suppressing a System Report Template

Security Leads can prevent users in the portal from viewing or using a system report template in report generation by suppressing the system template.

1. Select the **Reports** view.
2. Click **Templates**.  
The **Templates** page appears.
3. Click the  icon next to the system template that you want to suppress.  
A confirmation message appears.
4. Click **Yes** to confirm the system report template suppression.  
The system report template is shown as suppressed. You can click the  icon to restore the system report template to users in the portal.

## Data Exports

A data export is a complete list of relevant data for a specific category (applications, releases, scans, issues, or entitlement consumption) across the tenant. Users with the Export Data permission can generate data exports. The data export is provided as a CSV file.

This section covers the following topics:



## Viewing Data Exports

To view data exports:

1. Click the **Reports** view.  
Your Reports page appears
2. Click **Data Export**.  
The Data Export page appears.



The screenshot shows the 'Data Export' page with a table of export templates. The table has columns for NAME, TYPE, CREATED BY, and NEXT RUN DATE. Each row includes action icons for delete (X), edit (pencil), and view (chevron right). A '+ NEW DATA EXPORT' button is in the top right. On the left, there are icons for PDF, CSV, and a settings gear.

NAME	TYPE	CREATED BY	NEXT RUN DATE
All Application Releases - 2015-11-05 14h50m50s		TenantUser	
All Application Releases - 2015-11-05 14h57m00s	Application Releases Export	TenantUser	
All Application Releases - 2016-05-16 21h38m33s	Application Releases Export	kristine_tam	
All Application Releases - 2016-07-27 09h43m03s	Application Releases Export	katrina_seclead	
All Application Releases - 2016-07-27 09h46m15s	Application Releases Export	katrina_seclead	2017/12/03
All Application Releases - 2016-07-30 05h40m45s	Application Releases Export	carla_seclead	
All Application Releases - 2016-10-18 22h11m33s	Application Releases Export	edz_tam	
All Application Releases - 2017-02-01 08h24m55s	Application Releases Export	AuUser	
All Application Releases - 2017-11-04 21h50m09s	Application Releases Export	HuangTam	
All Application Releases - UAT test	Application Releases Export	danika_tam	
All Applications - [ Current Releases ] - 2015-03-10 10h55m52s	Application Export	DerekTam	

The following table describes how to navigate the Data Export page.

Task	Action
Create a data export template	Click <b>+Create Data Export</b> . For more information, see <a href="#">"Creating a Data Export Template"</a> on the next page.
Generate a data export using an existing template	Click <b>&gt;</b> in the row of a template. For more information, see <a href="#">"Generating a Data Export"</a> on page 242.
Edit a data export template	Click <b>✎</b> in the row of a template.
Delete a data export template	Click <b>✕</b> in the row of a template. You cannot delete a template if it has an existing data export.
View generated data exports for a template	Click <b>&gt;</b> in the row of a template to view files that have been generated in the last three months for the template.

The small screenshot shows a row for 'All Application Releases - 2017-11-08 20h09m20s' with a dropdown menu open. The menu shows a file named 'All Application Releases - 2017-11-08 20h09m20s.csv' with a 'Created Date: 2017/11/08' and a download icon.

Task	Action
Delete a data export	Click  in the row of a data export.
Download a data export file	Click  in the row of a data export.

## Creating a Data Export Template

A data export template is used as a basis for generating data exports. You can apply filters as well as schedule recurring data exports.

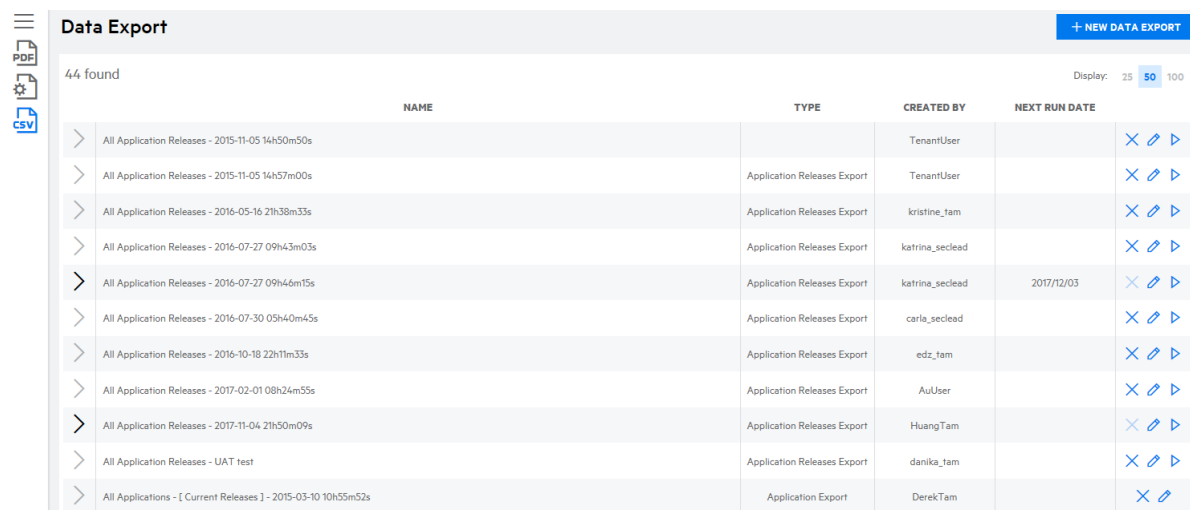
To create a data export template:

1. Click the **Reports** view.

































Your Reports page appears

2. Click **Data Export**.

The Data Export page appears.



The screenshot shows the 'Data Export' page with a table of 44 found items. The table has columns for NAME, TYPE, CREATED BY, and NEXT RUN DATE. Each row includes a chevron icon on the left and delete, edit, and refresh icons on the right. A '+ NEW DATA EXPORT' button is visible in the top right corner.

	NAME	TYPE	CREATED BY	NEXT RUN DATE	
>	All Application Releases - 2015-11-05 14h50m50s		TenantUser		  
>	All Application Releases - 2015-11-05 14h57m00s	Application Releases Export	TenantUser		  
>	All Application Releases - 2016-05-16 21h38m33s	Application Releases Export	kristine_tam		  
>	All Application Releases - 2016-07-27 09h43m03s	Application Releases Export	katrina_seclead		  
>	All Application Releases - 2016-07-27 09h44m15s	Application Releases Export	katrina_seclead	2017/12/03	  
>	All Application Releases - 2016-07-30 05h40m45s	Application Releases Export	cerla_seclead		  
>	All Application Releases - 2016-10-18 22h11m33s	Application Releases Export	edt_tam		  
>	All Application Releases - 2017-02-01 08h24m55s	Application Releases Export	AuUser		  
>	All Application Releases - 2017-11-04 21h50m09s	Application Releases Export	HuangTam		  
>	All Application Releases - UAT test	Application Releases Export	danika_tam		  
>	All Applications - [ Current Releases ] - 2015-03-10 10h55m52s	Application Export	DerekTam		 

3. Click **+Create Data Export**.

The Data Export wizard appears.

4. **Start Page:** Complete the fields and click **Next**.

Field	Description
<b>Name</b>	Type the name of the data export template.
<b>Template</b>	<p>Select a data export template type:</p> <ul style="list-style-type: none"> <li>• <b>Applications</b> - list of applications</li> <li>• <b>Application Releases</b> - list of releases</li> <li>• <b>Scans</b> - list of scans</li> <li>• <b>Issues</b> -list of issues</li> <li>• <b>Entitlement Consumption</b> - list of scans where entitlements were consumed, including deleted, canceled, and in progress scans.</li> </ul> <p><b>Note:</b> Filters are not available for the Entitlement Consumption template type.</p>
<b>Schedule</b>	<p>Select one of the following options for scheduling the data export:</p> <ul style="list-style-type: none"> <li>• <b>Queue Now</b> - queues the data export immediately</li> <li>• <b>Recurring</b> - generates the data export according to a schedule that you will specify in the wizard</li> </ul>

When this option is selected, the **Enabled** check box is available. Select the check box to have the data export automatically generated according to the schedule (default). Otherwise, you must manually generate the data export.

5. **Filter:** select the desired filters and click **Next**. The available filters are based on the template type selected.

**Data Export Wizard** [Close]

Start Page  
**Filter**  
Columns  
Schedule  
Summary

expand all | collapse all

SCAN START DATE

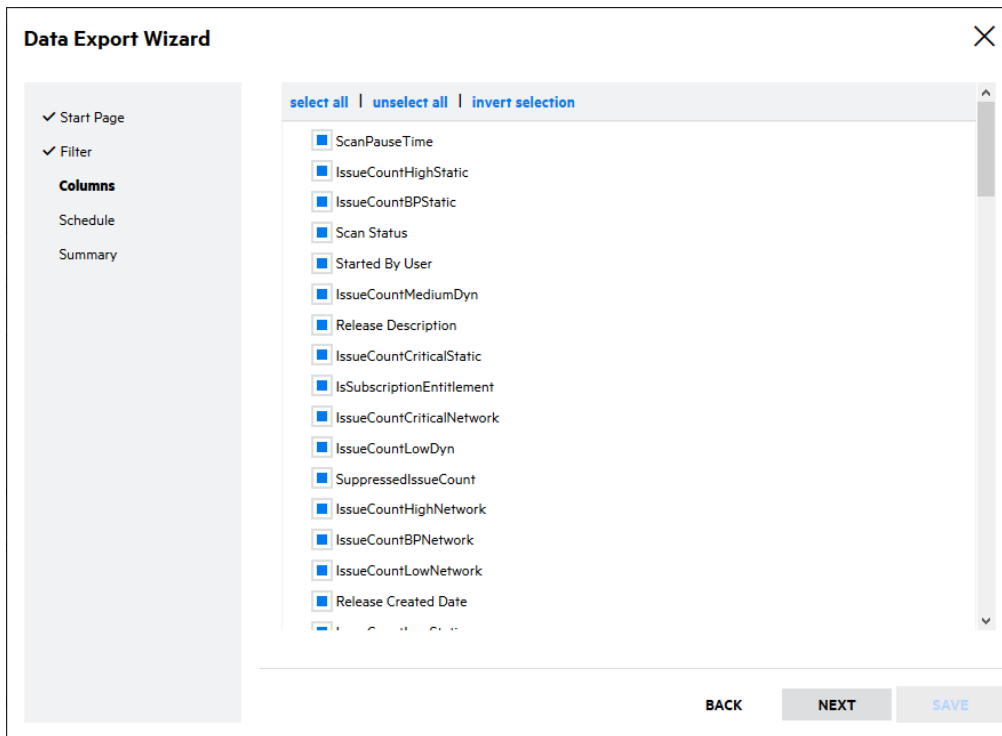
From: 2020/08/01 To: [ ]

> ASSESSMENT TYPE  
> ENTITLEMENTTYPE  
> ISREMIATIONSCAN  
> SCAN METHOD TYPE  
> SCAN STATUS  
> SCAN TYPE  
> SDLC STATUS

BACK NEXT SAVE

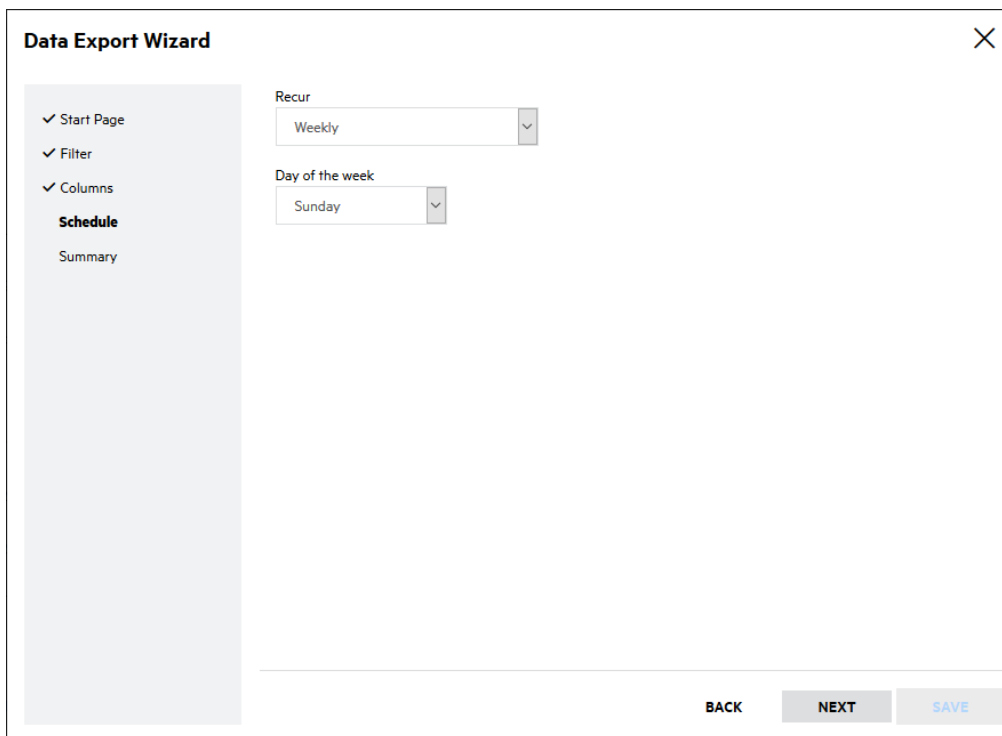
**Note:** The **Scan Start Date** filter is required for the scans data export; the **Introduced Date** filter is required for the issues data export.

6. **Columns** (available for the scans and issues data exports): select the columns to include in the data export and click **Next**.



7. **Schedule** (available for recurring data exports): select the repeat frequency and the day or date to generate the data export. Click **Next**.




**Note:** Data exports run at 24:00 server time.



8. Click **Next**.

- Summary:** review the summary of the data export and click **Save**.

The template appears in the data export list. The following action icons are available:

Icon	Action
	Queue the data export.
	Edit the template.
	Delete the template.

If a data export is being queued, a "Processing" status appears until the data export is ready for download.

## Generating a Data Export

You generate a data export using an existing data export template.

**Note:** A data export only contains results of completed assessments at the time the data export is generated, with the exception of the Entitlement Consumption data export.

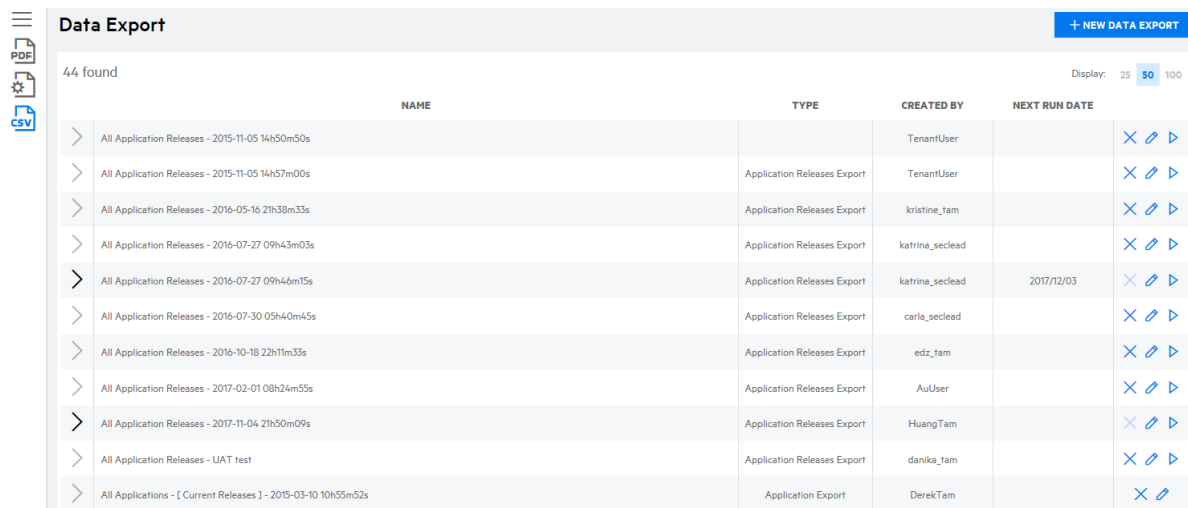
To generate a data export:

- Click the **Reports** view.


Your Reports page appears

- Click **Data Export**.

The Data Export page appears.



Data Export				+ NEW DATA EXPORT
44 found				Display: 25 <b>50</b> 100
	NAME	TYPE	CREATED BY	NEXT RUN DATE
>	All Application Releases - 2015-11-05 14h50m50s		TenantUser	
>	All Application Releases - 2015-11-05 14h57m00s	Application Releases Export	TenantUser	
>	All Application Releases - 2016-05-16 21h38m33s	Application Releases Export	kristine_tam	
>	All Application Releases - 2016-07-27 09h43m03s	Application Releases Export	katrina_seclead	
>	All Application Releases - 2016-07-27 09h44m15s	Application Releases Export	katrina_seclead	2017/12/03
>	All Application Releases - 2016-07-30 05h40m45s	Application Releases Export	cerla_seclead	
>	All Application Releases - 2016-10-18 22h11m33s	Application Releases Export	edt_tam	
>	All Application Releases - 2017-02-01 08h24m55s	Application Releases Export	AuUser	
>	All Application Releases - 2017-11-04 21h50m09s	Application Releases Export	HuangTam	
>	All Application Releases - UAT test	Application Releases Export	danika_tam	
>	All Applications - [ Current Releases ] - 2015-03-10 10h55m52s	Application Export	DerekTam	

- Click  in the row of a data export template.

The data export is queued for generation.

4. Click [>](#) next to the template to view the generated data exports.  
A "Processing" status appears until the data export is ready for download.
5. Click [↓](#) in the row of the data export once it has been generated.  
A CSV file is saved locally to a folder specified in your browser settings.

# Chapter 7: Administration

Administration of your tenant is performed from the portal. Access and privileges are determined by the user role.

This section contains the following topics:

- [Portal Management](#) .....244
- [User Management](#) .....258
- [Policy Management](#) .....283
- [Single Sign-On \(SSO\)](#) .....291
- [Vendor Management](#) .....301

## Portal Management

Security Leads can administer the portal, including configuring portal settings, configuring security, and reviewing the administration event log.

This section covers the following topics:

- [Configuring User Security](#) .....244
- [API Keys](#) .....247
- [Viewing Entitlements](#) .....251
- [Viewing the Administration Event Log](#) .....252
- [Managing Attributes](#) .....253

## Configuring User Security

Security Leads can configure the following user security settings:

- Password reset frequency
- Maximum personal access token lifetime
- Two-factor authentication
- IP restrictions

To configure user security settings:

1. Select the **Administration** view.  
The User Settings page appears.
2. Click **Settings**.



The Settings page appears.

3. Select the **Security** tab.

**Settings**

Attributes **Security** API Application Defender Sonatype

**Password Reset Frequency (1 to 9999 days)**  
1 Days

**Max Personal Access Token Lifetime (1 to 9999 days)**  
180 Days

**Two Factor Authentication**  
Enable Two Factor Authentication  
 No  
 Email  
 SMS  
Frequency: Every login

**IP Restriction**  
Enable Login Restriction:  No  
Allowed IP Addresses:  

NAME	IP ADDRESS
<b>+ ADD</b>	

  
Allow technical account managers (TAMs) access from any IP address:  
 Deny

Your IP Address: **15.122.106.229**  
Valid IPV4 forms are 127.0.0.1, 127.0.0.\*, and 127.0.0.[0-255].

**SAVE**

4. Edit the fields as needed.

Section	Procedure
Password Expiration Frequency	To specify the password reset frequency for new passwords: In the <b>Password Reset Frequency</b> field, specify the password reset frequency. The new value overrides the default value of 180 days.
Maximum Personal Access Token Lifetime	To specify the maximum personal access token lifetime for new PATs: In the <b>MAX Personal Access Token Lifetime</b> field, specify the maximum personal access token lifetime. The new value overrides the default value of 180 days.

<p>Two-Factor Authentication</p>	<p>Protect user accounts by configuring two-factor authentication. Once it is configured, all users will be required to log in using two-factor authentication.</p> <p>To configure two-factor authentication:</p> <ol style="list-style-type: none"> <li>In the <b>Enable Two Factor Authentication</b> field, move the slider from <b>No</b> to <b>Yes</b> to enable two-factor authentication.</li> <li>Select whether users can receive the login code by email, SMS, or both methods.</li> <li>Select how often a user is prompted for a two factor authentication code from the <b>Frequency</b> list: <b>Every login, 4 hours, 8 hours, 12 hours, 24 hours.</b></li> </ol>						
<p>IP Restrictions</p>	<p>Limit access to the tenant by restricting access to users logging in from particular IP addresses.</p> <p>To restrict access to particular IP addresses:</p> <ol style="list-style-type: none"> <li>In the <b>Enable Login Restriction</b> field, move the slider from <b>No</b> to <b>Yes</b> to enable IP restriction.</li> <li>In the <b>Allow technical account managers (TAMs) access from any IP address</b> field, move the slider from <b>No</b> to <b>Yes</b> to allow a TAM to access your tenant from any IP address.</li> <li>Perform the following tasks to manage the IP addresses that have access to the tenant:</li> </ol> <table border="1" data-bbox="550 1234 1409 1736"> <thead> <tr> <th data-bbox="553 1241 753 1304">Task</th> <th data-bbox="761 1241 1406 1304">Procedure</th> </tr> </thead> <tbody> <tr> <td data-bbox="553 1314 753 1499">Add an IP address to the allowed list</td> <td data-bbox="761 1314 1406 1499">Click <b>+Add</b> and type a name for the IP address (special characters are not allowed) and the IP address. Valid IP address forms are 127.0.0.1, 127.0.0.*, and 127.0.0.[0-255].</td> </tr> <tr> <td data-bbox="553 1509 753 1730">Remove an existing IP address from the allowed list</td> <td data-bbox="761 1509 1406 1730">Click <b>x</b> next to an IP address in the <b>Allow IP Addresses</b> list.</td> </tr> </tbody> </table>	Task	Procedure	Add an IP address to the allowed list	Click <b>+Add</b> and type a name for the IP address (special characters are not allowed) and the IP address. Valid IP address forms are 127.0.0.1, 127.0.0.*, and 127.0.0.[0-255].	Remove an existing IP address from the allowed list	Click <b>x</b> next to an IP address in the <b>Allow IP Addresses</b> list.
Task	Procedure						
Add an IP address to the allowed list	Click <b>+Add</b> and type a name for the IP address (special characters are not allowed) and the IP address. Valid IP address forms are 127.0.0.1, 127.0.0.*, and 127.0.0.[0-255].						
Remove an existing IP address from the allowed list	Click <b>x</b> next to an IP address in the <b>Allow IP Addresses</b> list.						

5. Click **Save**.

Your user security settings are saved.

## API Keys

API keys are used to authenticate to the Fortify on Demand API. Security Leads can manage API keys.

**Note:** This section covers the management of API keys. For information on using the Fortify on Demand API, see "[Fortify on Demand API](#)" on page 306

This section covers the following topics:

<a href="#">Creating an API Key</a>	247
<a href="#">API Key Roles</a>	248
<a href="#">Editing or Deleting an API Key</a>	249

### Creating an API Key

Security Leads can create API keys.

To create an API key:

1. Select the **Administration** view.  
The User Management page appears.
2. Click **Settings**.  
The **Attributes** tab of the Settings page appears.
3. Select the **API** tab.

NAME	PRODUCTION RISK & POLICY COMPLIANCE	SCAN & SECURITY STATUS
Jeopardy (PHP) 2 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL: 160, HIGH: 5, MEDIUM: 0, LOW: 147	STATIC: ✓, DYNAMIC: ⊖, MONITORING: ⊖, 201 Rel
WebGoat (NET) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL: 135, HIGH: 151, MEDIUM: 11, LOW: 74	STATIC: ✓, DYNAMIC: ✗, MONITORING: ⊖, no r
OpenSSL (C Source) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL: 64, HIGH: 156, MEDIUM: 0, LOW: 0	STATIC: ✓, DYNAMIC: ⊖, MONITORING: ⊖, no r
iGoat Android (JAVA) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL: 43, HIGH: 122, MEDIUM: 18, LOW: 15	STATIC: ✗, MOBILE: ✓, MONITORING: ⊖, no r
iGoat iOS (Objective-C) 2 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL: 14, HIGH: 54, MEDIUM: 2, LOW: 1	STATIC: ✓, MOBILE: ✓, MONITORING: ⊖, 201 Rel
Zero Security (COBOL) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL: 11, HIGH: 4, MEDIUM: 0, LOW: 0	STATIC: ✓, DYNAMIC: ⊖, MONITORING: ⊖, no r

4. Click **+Add Key**.  
The **Add/Edit Key for Application** window opens.

The screenshot shows a dialog box titled "Add/Edit Key for Application" with a close button (X) in the top right corner. It contains three main sections: 1. "Application Name" with a text input field. 2. "Role" with a dropdown menu showing "(Choose One)". 3. "Authorize app to use API" with two radio buttons, the "Yes" one being selected. At the bottom of the dialog are two buttons: "SAVE" and "CANCEL".

5. Complete the fields. Fields are required unless otherwise noted.

Field	Description
<b>Application Name</b>	Name of your application.
<b>Role</b>	Select the role that has the appropriate API Key permissions. See <a href="#">"API Key Roles"</a> below.
<b>Authorize app to use API</b>	Select <b>Yes</b> to enable the key. Select <b>No</b> to disable key if it is not in use.

6. Click **Save**.

The Secret Key window opens.

7. Copy your Base64 encoded secret code. The secret code is only shown once.

8. Click **Close**.

The new API key appears in the API key list.

**Note:** By default, an API key has access to all applications. See ["Editing or Deleting an API Key" on the next page](#) for information on assigning applications to an API key.

## API Key Roles

A dedicated API key is associated with a role having a predefined, unmodifiable set of permissions. API keys have access to all applications in a tenant; applications can be assigned to API keys to update application access.

The following table lists the permission set of each API key role.

Role	Permissions	Usage Example
Security Lead	All permissions	Full access to all AppSec program functionality and associated

Role	Permissions	Usage Example
		infrastructure
Manage Applications	View Third Party Apps, Manage Applications, Audit Issues, Create Reports, Start Static/Dynamic/Mobile Scans	Integration with full-featured custom or internal systems without the ability to manage users
Start Scans	View Third Party Apps, View Applications, View Issues, View Reports, Start Static/Dynamic/Mobile Scans	Continuous integration and build servers
Read Only	View Third Party Apps, View Applications, View Issues, View Reports	Data import into vulnerability management or Governance, Risk Management, and Compliance (GRC) systems

## Editing or Deleting an API Key

Security Leads can perform the following tasks for API keys:

- Generate a new secret
- Edit API key settings
- Assign and unassign applications


**Note:** API keys with the Security Lead role have access to all applications; this cannot be changed.

- Delete API keys

To make changes to an API key:

1. Select the **Administration** view.  
The User Management page appears.
2. Click **Settings**.  
The **Attributes** tab of the Settings page appears.
3. Select the **API** tab.

4. You can perform the following tasks:

Task	Procedure
Generate new secret	<ol style="list-style-type: none"> <li>Click <b>New Secret</b>. A confirmation message appears</li> <li>Click <b>Yes</b>. This will void the current secret.</li> </ol>
Edit API key settings	<ol style="list-style-type: none"> <li>Click <b>Edit</b>. The Add/Edit Key for Application window opens.</li> <li>Edit the fields as needed.</li> </ol>
Delete API key	<ol style="list-style-type: none"> <li>Click <b>Delete</b>. A confirmation message appears.</li> <li>Click <b>Yes</b>.</li> </ol>
Assign applications to API key	<ol style="list-style-type: none"> <li>Click <b>Assign Applications</b>.</li> <li>Select the <b>Available</b> tab. </li> <li>Perform the following actions to select applications:                             <ul style="list-style-type: none"> <li>○ Select the check box next to individual applications.</li> <li>○ Select the <b>ASSIGN</b> check box to select displayed applications.</li> </ul> </li> </ol>

Task	Procedure																				
	<ul style="list-style-type: none"> <li>○ Select the <b>Assign All Tenant Applications</b> check box to select all applications.</li> </ul> <p>You can use the search field to filter the application list.</p> <p>d. Click <b>Save</b>.</p>																				
<p>Unassign applications from API key</p>	<p>a. Click <b>Assign Applications</b>.</p> <p>b. Select the <b>Selected</b> tab.</p> <div data-bbox="672 627 1411 1270" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Assign Applications</b> <span style="float: right;">✕</span></p> <p><b>Selected</b> Available <span style="float: right;">Search <input type="text"/></span></p> <p><input type="checkbox"/> Unassign All Tenant Applications</p> <p><input checked="" type="checkbox"/> <b>ASSIGN</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30px;"></th> <th style="text-align: left;">APPLICATION</th> </tr> </thead> <tbody> <tr><td><input checked="" type="checkbox"/></td><td>iGoat Android (JAVA)</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>iGoat iOS (Objective-C)</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Jeopardy (PHP)</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>OpenSSL (C Source)</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Rubix (JAVA-No Source)</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>WebGoat</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>WebGoat (NET)</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Zero</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Zero Security (COBOL)</td></tr> </tbody> </table> <p style="text-align: right;"><b>SAVE</b> <b>CANCEL</b></p> </div> <p>c. Perform the following actions to remove applications:</p> <ul style="list-style-type: none"> <li>○ Clear the check box next to individual applications.</li> <li>○ Clear the <b>ASSIGN</b> check box to remove displayed applications.</li> <li>○ Select the <b>Unassign All Tenant Applications</b> check box to remove all applications.</li> </ul> <p>You can use the search field to filter the application list.</p> <p>d. Click <b>Save</b>.</p>		APPLICATION	<input checked="" type="checkbox"/>	iGoat Android (JAVA)	<input checked="" type="checkbox"/>	iGoat iOS (Objective-C)	<input checked="" type="checkbox"/>	Jeopardy (PHP)	<input checked="" type="checkbox"/>	OpenSSL (C Source)	<input checked="" type="checkbox"/>	Rubix (JAVA-No Source)	<input checked="" type="checkbox"/>	WebGoat	<input checked="" type="checkbox"/>	WebGoat (NET)	<input checked="" type="checkbox"/>	Zero	<input checked="" type="checkbox"/>	Zero Security (COBOL)
	APPLICATION																				
<input checked="" type="checkbox"/>	iGoat Android (JAVA)																				
<input checked="" type="checkbox"/>	iGoat iOS (Objective-C)																				
<input checked="" type="checkbox"/>	Jeopardy (PHP)																				
<input checked="" type="checkbox"/>	OpenSSL (C Source)																				
<input checked="" type="checkbox"/>	Rubix (JAVA-No Source)																				
<input checked="" type="checkbox"/>	WebGoat																				
<input checked="" type="checkbox"/>	WebGoat (NET)																				
<input checked="" type="checkbox"/>	Zero																				
<input checked="" type="checkbox"/>	Zero Security (COBOL)																				

## Viewing Entitlements

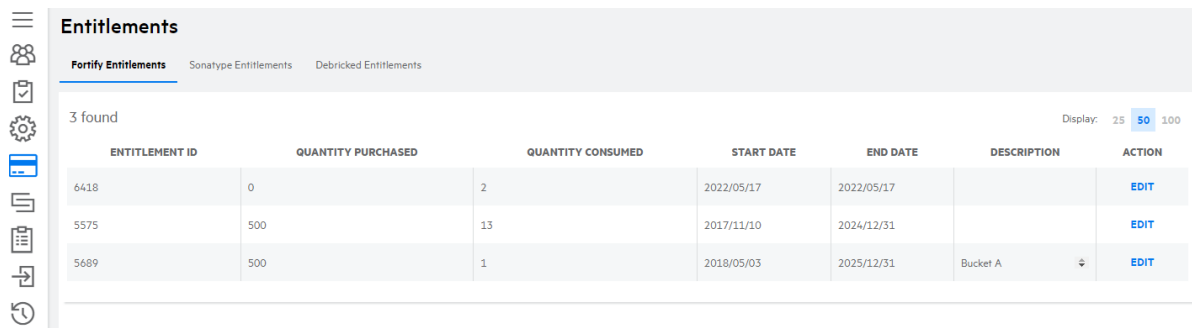
Security Leads can view a list of expired and active entitlements for the tenant as well as add descriptions to entitlements.

To view entitlements for the tenant:

1. Select the **Administration** view.  
The User Management page appears.

2. Click **Entitlements**.

The Entitlement page appears. The **Fortify Entitlements** tab displays Fortify on Demand entitlements; the **Sonatype Entitlements** tab displays Sonatype entitlements; the **Debricked Entitlements** tab displays Debricked entitlements.



ENTITLEMENT ID	QUANTITY PURCHASED	QUANTITY CONSUMED	START DATE	END DATE	DESCRIPTION	ACTION
6418	0	2	2022/05/17	2022/05/17		EDIT
5575	500	13	2017/11/10	2024/12/31		EDIT
5689	500	1	2018/05/03	2025/12/31	Bucket A	EDIT

3. You can perform the following task:

Task	Procedure
Add or edit the entitlement description	Click <b>Edit</b> in the row of an entitlement and provide a description. The description is limited to 50 characters.

## Viewing the Administration Event Log

Security Leads can view the administration event log. The administration event log logs all application-related events as well as the following administration-related events:

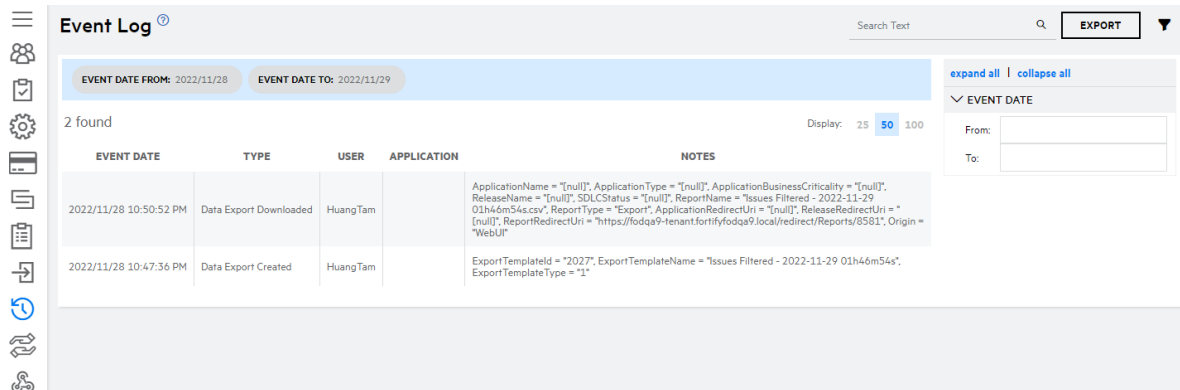
- user login success or failure and user logout
- user creation, updates, and deletion
- group creation, updates, and deletion
- role creation, updates, and deletion
- dashboard and event log exports
- API Key and personal access token creation, updates, deletion, and new secret generation
- API authentication success or failure
- Changes to administration settings and SSO settings

To view the administration event log:


1. Select the **Administration** view.  
The User Management page appears.
2. Click **Event Log**.



The Event Log page appears.



3. You can perform the following tasks:

Task	Action
Export the event log of the last 13 months	Click <b>Export</b> . A .csv file is saved locally to the folder specified in your browser settings.
Search the event log	Type a keyword or phrase in the search text field and click <b>Enter</b> .
Hide or display the filter list	Click <b>▼</b> .
Expand or collapse filters	Click <b>expand all   collapse all</b>  or the arrow next to the filter name.
Remove applied filters	Click <b>X</b> or click <b>Clear Filters</b> at the top of the page. The filter is set to the last 24 hours by default.

### Related Topics:

For information about viewing events related to a specific application, see ["Viewing the Application Event Log" on page 57](#).

## Managing Attributes

Attributes provide additional information about applications; they are used as filters to help track applications, releases, and issues. Attributes are for informational purposes and do not affect the assessment process in any way.

Security Leads can add, edit, and delete attributes. System-level attributes are pre-defined and can not be deleted; certain system attributes are editable.

The following attribute types are available:

- Application attributes. Applications attributes are both system and custom attributes.
- Microservice attributes. Microservice attributes are custom attributes.
- Release attributes. Release attributes are system attributes.
- Issue attributes. Issue attributes are system attributes. The following issue attributes are editable: **Auditor Status (Open)**, **Auditor Status (Closed)**, **Developer Status (Open)**, and **Developer Status (Closed)**.

This section covers the following topics:

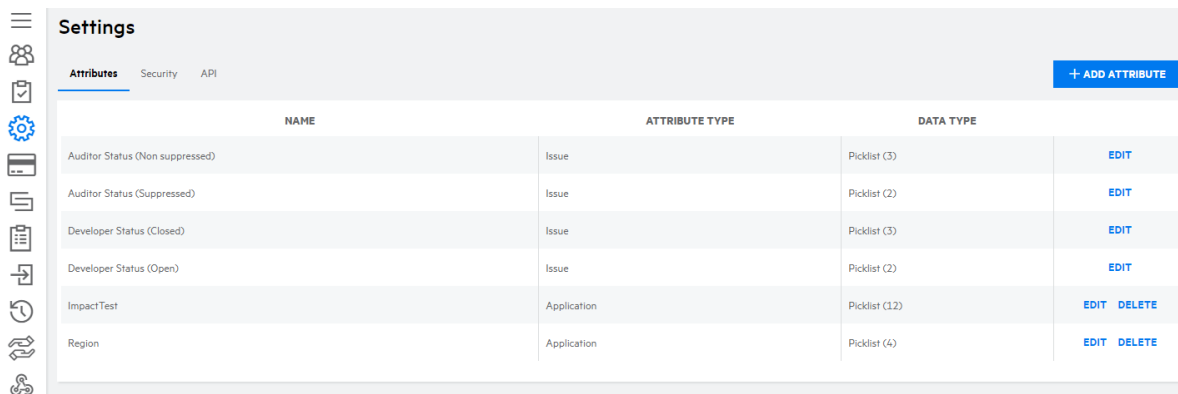
<a href="#">Adding an Attribute</a> .....	254
<a href="#">Editing an Attribute</a> .....	256
<a href="#">Deleting an Attribute</a> .....	257

## Adding an Attribute

Security Leads can add microservice and application attributes.

To add an attribute:

1. Select the **Administration** view.  
The User Settings page appears.
2. Click **Settings**.  
The **Attributes** tab of the Settings page appears.



NAME	ATTRIBUTE TYPE	DATA TYPE	
Auditor Status (Non suppressed)	Issue	Picklist (3)	<a href="#">EDIT</a>
Auditor Status (Suppressed)	Issue	Picklist (2)	<a href="#">EDIT</a>
Developer Status (Closed)	Issue	Picklist (3)	<a href="#">EDIT</a>
Developer Status (Open)	Issue	Picklist (2)	<a href="#">EDIT</a>
ImpactTest	Application	Picklist (1,2)	<a href="#">EDIT</a> <a href="#">DELETE</a>
Region	Application	Picklist (4)	<a href="#">EDIT</a> <a href="#">DELETE</a>

3. Click **+Add Attribute**.  
The Attribute Definition window appears.

4. Complete the following fields. Fields are required unless otherwise noted.

Field	Description
Name	Specify the name of the new attribute.
Attribute Type	Select the attribute type. Microservice attributes are restricted to the <b>Text</b> data type.
Data Type	Select the data type: <ul style="list-style-type: none"> <li>• <b>Picklist</b>: this attribute type allows selection of a value from a list. You need to define the possible values for the attribute, which appear as a drop-down list for that attribute.</li> <li>• <b>Text</b>: this attribute type allows free form text. This is the best type to use if you want to assign a ticket number or other identifier that is specific to each new release.</li> <li>• <b>Boolean</b>: this attribute type allows selection of binary values (<b>true/false</b>).</li> <li>• <b>Date</b>: this attribute type allows selection of a date from a calendar.</li> <li>• <b>User</b>: this attribute type allows selection of a user from a list of all active users for the tenant.</li> </ul>
Required	(Optional) Select the check box to designate the attribute as required.
Editable only by Security Leads	(Optional) Select the check box to restrict its usage to Security Leads. This option supersedes the <b>Manage Application</b> permission. <p><b>Note:</b> Selecting this precludes making an attribute required, as it would break the <b>Create Application</b> permission for non-Security Leads.</p>

5. Click **Save**.

The new attribute appears in the attribute list.

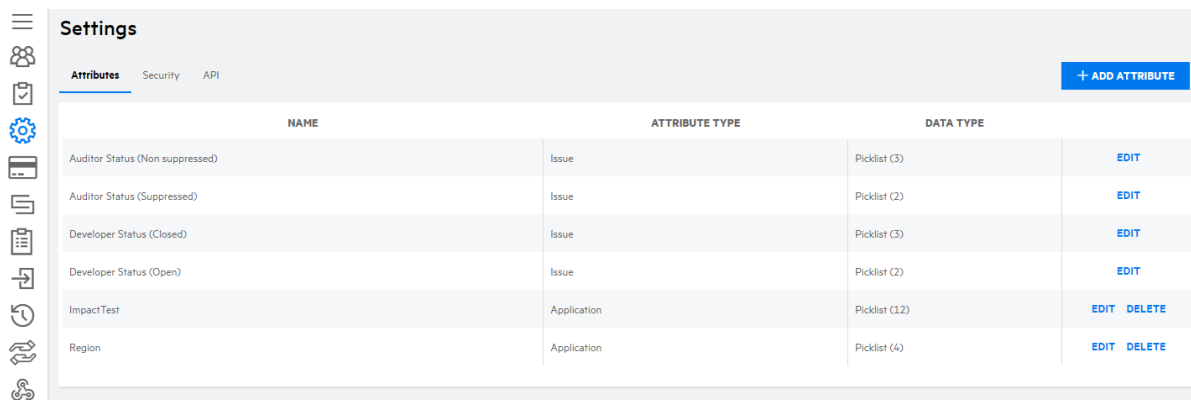
## Editing an Attribute

Security Leads can edit picklist values and certain settings for existing attributes. You can not change the attribute name or attribute type.

**Note:** You can edit the values of issue attributes. For the **Developer Status (Open)** attribute, the default values of **Open** and **In Remediation** are non-editable.

To edit an attribute:

1. Select the **Administration** view.  
The User Settings page appears.
2. Click **Settings**.  
The **Attributes** tab of the Settings page appears.



NAME	ATTRIBUTE TYPE	DATA TYPE	
Auditor Status (Non suppressed)	Issue	Picklist (3)	<a href="#">EDIT</a>
Auditor Status (Suppressed)	Issue	Picklist (2)	<a href="#">EDIT</a>
Developer Status (Closed)	Issue	Picklist (3)	<a href="#">EDIT</a>
Developer Status (Open)	Issue	Picklist (2)	<a href="#">EDIT</a>
Impact Test	Application	Picklist (1,2)	<a href="#">EDIT</a> <a href="#">DELETE</a>
Region	Application	Picklist (4)	<a href="#">EDIT</a> <a href="#">DELETE</a>

3. Click **Edit** in the row of the attribute that you want to edit.  
The **Attribute Definition** page displays.

4. Edit the fields as needed. The fields vary depending on the data type.

Data Type	Available Actions
Picklist	<ul style="list-style-type: none"> <li>• Click <b>+</b> to add a new value.</li> <li>• Use the <b>^</b> <b>v</b> to reorder the listed values.</li> <li>• Click <b>⌂</b> to sort values alphabetically.</li> <li>• Click <b>x</b> to remove a value from the list.</li> </ul>
Picklist, Text, Boolean, Date, User	<p>Select or deselect the following check boxes:</p> <ul style="list-style-type: none"> <li>• <b>Required:</b> designate the attribute as required.</li> <li>• <b>Editable only by Security Leads:</b> Restrict attribute usage to Security Leads. This option supersedes the <b>Manage Application</b> permission.</li> </ul> <p><b>Note:</b> Selecting this precludes making an attribute required, as it would break the <b>Create Application</b> permission for non-Security Leads.</p>

5. Click **Save**.

Your attribute changes are saved

## Deleting an Attribute

You can delete custom attributes. System-level attributes cannot be deleted.

To delete an attribute:

1. Select the **Administration** view.  
The User Settings page appears.
2. Click **Settings**.  
The **Attributes** tab of the Settings page appears.

NAME	ATTRIBUTE TYPE	DATA TYPE	
Auditor Status (Non suppressed)	Issue	Picklist (3)	EDIT
Auditor Status (Suppressed)	Issue	Picklist (2)	EDIT
Developer Status (Closed)	Issue	Picklist (3)	EDIT
Developer Status (Open)	Issue	Picklist (2)	EDIT
ImpactTest	Application	Picklist (12)	EDIT DELETE
Region	Application	Picklist (4)	EDIT DELETE

3. Click **Delete** in the row of the attribute that you want to edit.  
A confirmation message appears.
4. Click **Yes**.  
The attribute and all associated values are deleted.

## User Management

Security Leads and users with the Manage Users permissions can manage users in Fortify on Demand. Security Leads can perform all user administration tasks. Users with the Manage Users permissions can manage user accounts and groups, but cannot manage roles.

This section covers the following topics:

<a href="#">Roles and Permissions</a> .....	258
<a href="#">Users</a> .....	269
<a href="#">Groups</a> .....	276

## Roles and Permissions

User actions in Fortify on Demand are controlled by roles. Roles are collections of permissions that specify the actions that can be performed. Each user is assigned to a specific role. Security Leads can manage roles, including assigning users to roles and creating, editing, and deleting roles.

Fortify on Demand is deployed with six default roles. Organizations can also define custom roles to better serve their needs. Custom roles can be used to align user roles with existing roles in an organization or expand or limit user responsibilities. Small organizations might want roles with

increased permissions; large or highly structure organizations might want roles with more restricted permissions.

This section covers the following topics:

<a href="#">Permissions</a> .....	259
<a href="#">Default Roles</a> .....	263
<a href="#">Viewing Roles</a> .....	265
<a href="#">Creating a Role</a> .....	266
<a href="#">Editing a Role</a> .....	267
<a href="#">Deleting a Role</a> .....	268

## Permissions

Permissions specify the actions a user can perform. Fortify on Demand permissions are divided into two types: tenant level permissions and application level permissions.

- **Tenant Level Permissions** are permissions that are applied at the tenant level, such as managing users, exporting data, and downloading tools. For a detailed list of tenant level permissions, see ["Tenant Level Permissions" below](#).
- **Application Level Permissions** are permissions that are applied to applications, such as creating applications, starting scans, editing issues, and managing reports. For a detailed list of Application Level Permissions, see ["Application Level Permissions" on page 261](#).

### Tenant Level Permissions

The following table lists the tenant level permissions that are available for a role. Any tenant level permission except Administration, which is tied to the Security Lead role, can be assigned to a custom role.

Category	Permissions	Actions Allowed
Administration	N/A (limited to Security Leads)	<ul style="list-style-type: none"> <li>• Manage security policies</li> <li>• Manage attributes</li> <li>• <a href="#">Configure user security</a></li> <li>• Manage API keys</li> <li>• <a href="#">Configure SSO</a></li> <li>• View administration event log</li> <li>• Manage roles</li> <li>• Manage global audit templates</li> <li>• <a href="#">Download static scan payload for all applications</a></li> </ul>

Category	Permissions	Actions Allowed
Application Access	<ul style="list-style-type: none"> <li><b>Manual</b> - Applications are not assigned by default. Applications must be assigned to a user or group. If <b>Manual</b> is selected, <b>Manage Users</b>, <b>Export Data</b>, <b>Vendor Management</b>, are set to <b>Deny</b>.</li> <li><b>All</b> - Access to all applications. No restrictions on tenant level permissions.</li> </ul>	Determined by the application level permissions assigned to the role
Manage Users	<b>Deny, Allow</b> (requires <b>Application Access</b> be set to <b>All</b> )	<ul style="list-style-type: none"> <li><a href="#">Add, edit, and delete users</a> (only Security Leads can edit other Security Leads)</li> <li>Export user data</li> <li><a href="#">Manage groups</a></li> <li>Assign training courses to users</li> <li>View training report</li> </ul>
Export Data	<b>Deny, Allow</b> (requires <b>Application Access</b> be set to <b>All</b> )	<ul style="list-style-type: none"> <li>View Data Exports tab</li> <li>Create data exports</li> <li>Edit data export templates</li> <li>Delete data export templates</li> <li>Generate data exports</li> <li>Download data exports</li> <li>Delete data export files</li> </ul>
Vendor Management	<b>Deny, Allow</b> (requires <b>Application Access</b> be set to <b>All</b> )	<ul style="list-style-type: none"> <li><a href="#">Verify and Approve Vendor</a></li> <li><a href="#">Request to be Vendor</a></li> <li><a href="#">Publish Report to Vendor</a></li> </ul>
Download Tools	<b>Deny, Allow</b>	View Tools page
Access Training	<b>Deny, Allow</b>	<a href="#">Take training courses</a>
View Third Party Apps	<b>Deny, Allow</b>	View open source components in use across all applications



Category	Permissions	Actions Allowed
Configure Webhooks	<b>Deny, Allow</b> (requires <b>Application Access</b> be set to <b>All</b> )	Manage webhooks

### Application Level Permissions

The following table lists the application level permissions that are available for a role. Any application level permission can be assigned to a custom role.

Category	Permissions	Actions Allowed
Applications	<b>View, Manage, Create</b>	<p>View</p> <ul style="list-style-type: none"> <li>View issues, scans, and reports</li> <li>View Application Monitoring configuration and risk profile</li> <li>Download scan results (FPRs and SBOMs)</li> </ul> <p>Manage</p> <ul style="list-style-type: none"> <li>All <b>View</b> permission actions</li> <li>Edit application settings (except for application name)</li> <li>View users assigned to application</li> <li>Create release</li> <li>Edit release settings</li> <li>Configure Application Monitoring and cancel Application Monitoring scan</li> <li>View and export application event log</li> <li>Import scan results (FPRs and SBOMs)</li> </ul> <p>Create</p> <ul style="list-style-type: none"> <li>All <b>Manage</b> permission actions</li> <li>Create new application</li> <li>Edit application name</li> <li>Delete application</li> <li>Delete release</li> </ul>
Issues	<b>View, Edit, Audit</b>	View

Category	Permissions	Actions Allowed
		<ul style="list-style-type: none"> <li>• Add and delete screenshot</li> <li>• Export the issues list</li> </ul> <p>Edit</p> <ul style="list-style-type: none"> <li>• All <b>View</b> actions</li> <li>• Edit <b>Assigned User</b> and <b>Developer Status</b> fields, add comment</li> <li>• Submit bug</li> </ul> <p>Audit</p> <ul style="list-style-type: none"> <li>• All <b>Edit</b> actions</li> <li>• Edit <b>Severity</b> and <b>Auditor Status</b> fields</li> <li>• Create and edit application audit template</li> </ul>
Reports	<b>View, Create</b>	<p>View</p> <ul style="list-style-type: none"> <li>• View main reports</li> <li>• Download main reports</li> <li>• View vendor reports</li> <li>• Download vendor reports</li> <li>• Export tenant dashboard</li> <li>• Export Your Releases page</li> </ul> <p>Create</p> <ul style="list-style-type: none"> <li>• Create reports</li> <li>• Delete reports</li> <li>• View report templates</li> <li>• Create report templates</li> <li>• Edit report templates</li> </ul>
Start Dynamic Scans	<b>Deny, Configure, Allow</b>	<p>Configure</p> <ul style="list-style-type: none"> <li>• <a href="#">Edit Dynamic Scan Setup page</a></li> </ul> <p>Allow</p> <ul style="list-style-type: none"> <li>• <a href="#">Schedule dynamic scan</a></li> </ul>

Category	Permissions	Actions Allowed
		<ul style="list-style-type: none"> <li>• <a href="#">Cancel dynamic scan</a></li> </ul>
Start Static Scans	<b>Deny, Configure, Allow</b>	Configure <ul style="list-style-type: none"> <li>• <a href="#">Edit Static Scan Setup page</a></li> </ul> Allow <ul style="list-style-type: none"> <li>• <a href="#">Upload static scan payload</a></li> <li>• <a href="#">Cancel static scan</a></li> <li>• <a href="#">Download static scan payload for assigned applications</a></li> </ul>
Start Mobile Scans	<b>Deny, Configure, Allow</b>	Configure <ul style="list-style-type: none"> <li>• <a href="#">Edit Mobile Scan Setup page</a></li> </ul> Allow <ul style="list-style-type: none"> <li>• <a href="#">Schedule mobile scan</a></li> <li>• <a href="#">Cancel mobile scan</a></li> </ul>
Consume Entitlements	<b>Deny, Allow</b>	Consume entitlements when starting a scan

## Default Roles

Fortify on Demand is configured with six default roles. Default roles can be edited or deleted with the exception of the Security Lead and Developer roles.

- **Security Lead**—Full access. The Security Lead has access to all applications and can perform all tasks, including creating applications and releases, working with data, auditing issues, and managing reports. The Security Lead is the only role that has the Administration permission, which includes the ability to manage roles, security policies, and other administrative settings.
- **Developer**—Limited access. The Developer has access to applications assigned to the user. The Developer can work with issue data and manage reports. The Developer is the default role for new users.
- **Lead Developer**—Medium-level access. The Lead Developer can create new applications, but only has access to applications assigned to the user. The Lead Developer can work with issue data, start scans, and manage reports.
- **Application Lead**—Medium-level access. The Application Lead has the same access as the Lead Developer, plus the ability to audit issues.
- **Executive**—Read-only access. The Executive has read-only access to applications assigned to the user.
- **Reviewer**—Read-only access. The Reviewer has read-only access to all applications.

The following table lists the permission set for each default role.

Permission	Security Lead	Developer	Lead Developer (Editable)	Application Lead (Editable)	Executive (Editable)	Reviewer (Editable)
<b>Tenant Level Permissions</b>						
Administration	X					
Application Access	All	Manual	Manual	Manual	Manual	All
Manage Users	X					
Export Data	X					
Vendor Management	X					
Download Tools	X	X	X	X		
Access Education	X	X	X	X	X	X
View Third Party Apps	X					
Configure Webhooks	X					
<b>Application Level Permissions</b>						
Applications	Create	View	Create	Create	View	View
Issues	Audit	Edit	Edit	Audit	View	View
Reports	Create	Create	Create	Create	View	View
Start Dynamic Scans	Start	Deny	Start	Start	Deny	Deny
Start Static Scans	Start	Deny	Start	Start	Deny	Deny

Permission	Security Lead	Developer	Lead Developer (Editable)	Application Lead (Editable)	Executive (Editable)	Reviewer (Editable)
Start Mobile Scans	Start	Deny	Start	Start	Deny	Deny
Configure Build Server	X					
Consume Entitlements	X	X	X	X	X	X

## Viewing Roles

To view the roles in your tenant:

1. Select the **Administration** view.  
The User Management page appears.
2. Select the **Roles** tab.

The screenshot shows the 'User Management' interface with the 'Roles' tab selected. A search bar and '+ ADD ROLE' button are visible. Below, a table lists 6 roles with their assigned users and application access levels.

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	EDIT VIEW USERS DELETE
Developer	0	Manual	EDIT VIEW USERS DELETE
Executive	0	Manual	EDIT VIEW USERS DELETE
Lead Developer	0	Manual	EDIT VIEW USERS DELETE
Reviewer	0	All	EDIT VIEW USERS DELETE
Security Lead	2	All	EDIT VIEW USERS DELETE

The following table describes how to navigate the **Roles** tab.

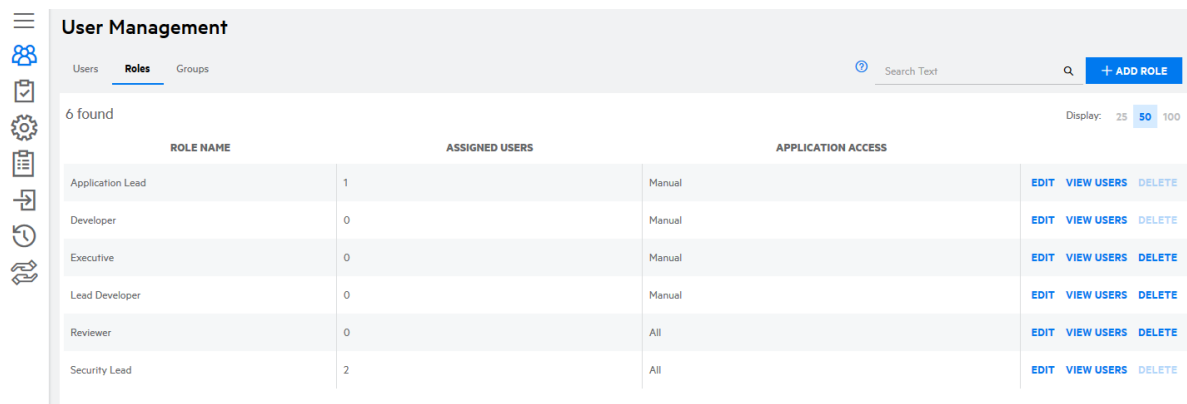
Task	Action
Search the role list	Type a keyword or phrase in the search field and press <b>Enter</b> . To remove the search results, remove the text from the search field and press <b>Enter</b> .
Create a role	Click <b>Add Role</b> . For more information, see " <a href="#">Creating a Role</a> " on the next page.
View users assigned to a role	Click <b>View Users</b> in the action column.

Task	Action
Edit a role	Click <b>Edit</b> in the action column. For more information, see <a href="#">"Editing a Role" on the next page.</a>
Delete a role	Click <b>Delete</b> in the action column. For more information, see <a href="#">"Deleting a Role" on page 268.</a>

## Creating a Role

To create a role:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Select the **Roles** tab.



The screenshot shows the 'User Management' interface with the 'Roles' tab selected. A table lists six roles with their assigned users and application access. The table has columns for Role Name, Assigned Users, and Application Access. Each row includes 'EDIT', 'VIEW USERS', and 'DELETE' action links.

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	<a href="#">EDIT</a> <a href="#">VIEW USERS</a> <a href="#">DELETE</a>
Developer	0	Manual	<a href="#">EDIT</a> <a href="#">VIEW USERS</a> <a href="#">DELETE</a>
Executive	0	Manual	<a href="#">EDIT</a> <a href="#">VIEW USERS</a> <a href="#">DELETE</a>
Lead Developer	0	Manual	<a href="#">EDIT</a> <a href="#">VIEW USERS</a> <a href="#">DELETE</a>
Reviewer	0	All	<a href="#">EDIT</a> <a href="#">VIEW USERS</a> <a href="#">DELETE</a>
Security Lead	2	All	<a href="#">EDIT</a> <a href="#">VIEW USERS</a> <a href="#">DELETE</a>

3. Click **+ Add Role**.  
The Add/Edit Role window appears.

**Add/Edit Role** ⓘ

Role Name

**Tenant Level Permissions**

Application Access	Manual	All
Manage Users	Deny	
Export Data	Deny	
Vendor Management	Deny	
Download Tools	Deny	
Access Training	Deny	
View Third Party Apps	Deny	

**Application Level Permissions**

Applications	View	Manage	Create
Issues	View	Edit	Audit
Reports	View	Create	
Start Dynamic Scans		Deny	
Start Static Scans		Deny	
Start Mobile Scans		Deny	

SAVE CANCEL

4. In the **Role Name** field, type the name of the new role.
5. Select tenant and application level permissions for the role. For more information on specific permissions, see ["Permissions" on page 259](#).
6. Click **Save**.  
The new role appears in the role list.

## Editing a Role

To edit a role:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Select the **Roles** tab.

**User Management**

Users **Roles** Groups

Search Text  + ADD ROLE

6 found Display: 25 50 100

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	EDIT VIEW USERS DELETE
Developer	0	Manual	EDIT VIEW USERS DELETE
Executive	0	Manual	EDIT VIEW USERS DELETE
Lead Developer	0	Manual	EDIT VIEW USERS DELETE
Reviewer	0	All	EDIT VIEW USERS DELETE
Security Lead	2	All	EDIT VIEW USERS DELETE

3. Click **Edit** in the row of the role that you want to edit.  
The Add/Edit Role modal window appears.

**Note:** The permission sets of the Security Lead and Developer roles cannot be edited.

4. Edit the fields as needed.
5. Click **Save**  
The role changes are saved.

## Deleting a Role

The Security Lead and Developer roles and roles to which users are assigned cannot be deleted.

To delete a role:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Select the **Roles** tab.

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	EDIT VIEW USERS DELETE
Developer	0	Manual	EDIT VIEW USERS DELETE
Executive	0	Manual	EDIT VIEW USERS DELETE
Lead Developer	0	Manual	EDIT VIEW USERS DELETE
Reviewer	0	All	EDIT VIEW USERS DELETE
Security Lead	2	All	EDIT VIEW USERS DELETE

3. Click **Delete** in the row of the role that you want to delete.



A confirmation message appears.

4. Click **Yes**.

The role is deleted.

## Users

Users with the Manage Users permissions can manage users and groups.

This section covers the following topics:

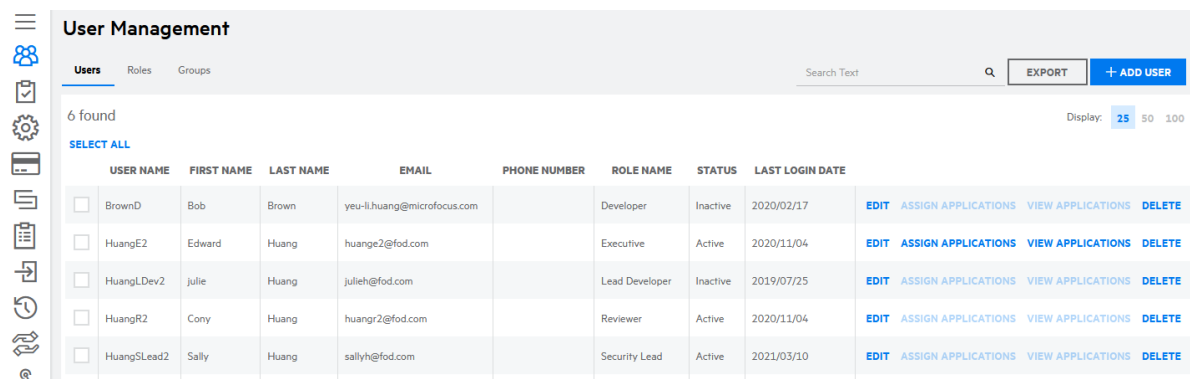
Viewing Users .....	269
Creating a User .....	270
Editing a User Account .....	272
Managing Application Assignment to a User .....	273
Deleting a User Account .....	275

### Viewing Users

To view the users in your tenant:

1. Select the **Administration** view.

The **Users** tab of the User Management page appears.



The following table describes how to navigate the **Users** tab.

Task	Action
Search the user list	Type a word or phrase in the search field and press <b>Enter</b> . To remove the search results, remove the text from the search field and press <b>Enter</b> .
Export the user list.	Click <b>Export</b> . A CSV file containing details of all users is saved locally to a folder specified in your browser settings.

Task	Action
Add a user	Click <b>Add User</b> . For more information, see " <a href="#">Creating a User</a> " below.
Assign and unassign applications	Click <b>Assign Applications</b> in the action column. For more information, see " <a href="#">Managing Application Assignment to a User</a> " on page 273.
View applications assigned to a user	Click <b>View Applications</b> in the action column.
Edit a user	Click <b>Edit</b> in the action column. For more information, see " <a href="#">Editing a User Account</a> " on page 272.
Delete a user	Click <b>Delete</b> in the action column. For more information, see " <a href="#">Deleting a User Account</a> " on page 275.

## Creating a User

To create a user:

1. Select the **Administration** view.

The **Users** tab of the User Management page appears.

The screenshot shows the 'User Management' page with the 'Users' tab selected. The interface includes a search bar, 'EXPORT' and '+ ADD USER' buttons, and a table with 6 columns: USER NAME, FIRST NAME, LAST NAME, EMAIL, PHONE NUMBER, ROLE NAME, STATUS, and LAST LOGIN DATE. There are also 'EDIT', 'ASSIGN APPLICATIONS', 'VIEW APPLICATIONS', and 'DELETE' links for each user row.

USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangE2	Edward	Huang	huang2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

2. Click **+ Add User**.

The Add/Edit User window appears.

### Add/Edit User ✕

User Name

Email

First Name

Last Name

Phone Number

Role

Inactive

Select groups that the user(s) should be a member.

GROUP NAME	ASSIGNED USERS

SAVE
CANCEL

3. Complete the fields as needed. Fields are required unless otherwise noted.

Field	Description
<b>User Name</b>	Type a unique username. The username cannot be changed after the user is created.
<b>Email</b>	Type the user's email address.
<b>First Name</b>	Type the user's first name.
<b>Last Name</b>	Type the user's last name.
<b>Phone Number</b>	(Optional) Type the user's phone number. Hyphens and other separators are not accepted.
<b>Role</b>	Select the user role (default role is <b>Developer</b> ). For more information on user roles, see <a href="#">Roles and Permissions</a> .
<b>Inactive</b>	(Optional) Select the check box to mark the user as inactive. The user will be unable to log in to Fortify on Demand.

4. (Optional) Select the groups to which the user will be assigned. You can use the search box to filter the group list.
5. Click **Save**.

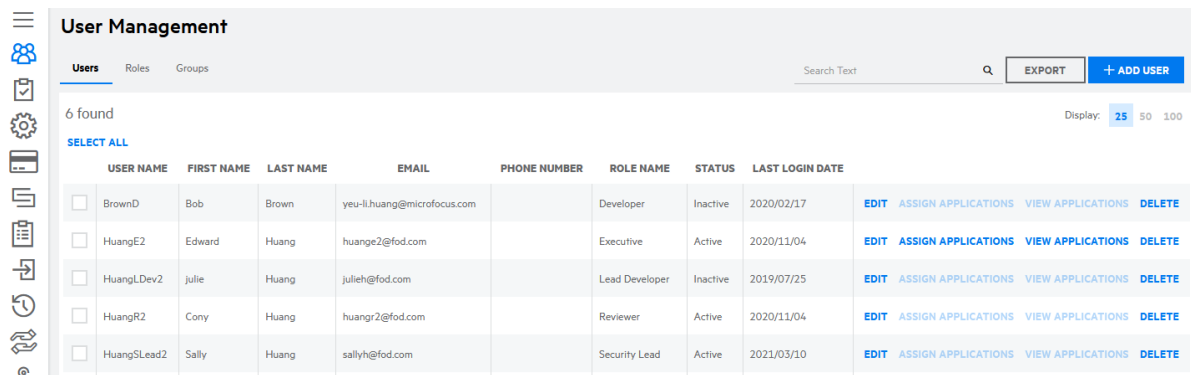
The new user appears in the user list.

## Editing a User Account

You can edit an existing user account, including resetting the user's password.

1. Select the **Administration** view.

The **Users** tab of the User Management page appears.

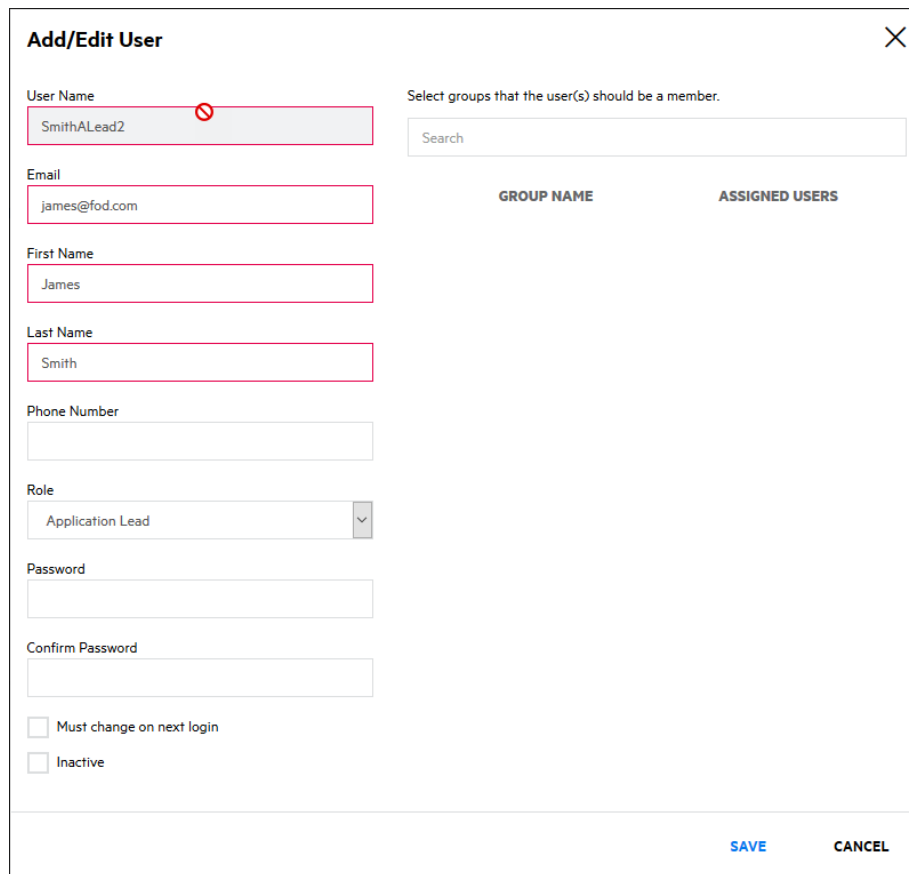


The screenshot shows the 'User Management' interface. At the top, there are tabs for 'Users', 'Roles', and 'Groups'. A search bar and 'EXPORT' button are visible. Below the tabs, it says '6 found' and 'Display: 25 50 100'. A 'SELECT ALL' link is present. The main table has columns: USER NAME, FIRST NAME, LAST NAME, EMAIL, PHONE NUMBER, ROLE NAME, STATUS, LAST LOGIN DATE, and a set of action links (EDIT, ASSIGN APPLICATIONS, VIEW APPLICATIONS, DELETE). The table contains five rows of user data.

USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

2. Click **Edit** in the row of the user whom you want to edit.

The Add/Edit User window opens.



The screenshot shows the 'Add/Edit User' window. It has a close button (X) in the top right. The form contains several input fields: 'User Name' (SmithALead2), 'Email' (james@fod.com), 'First Name' (James), 'Last Name' (Smith), 'Phone Number', 'Role' (Application Lead), 'Password', and 'Confirm Password'. There are also checkboxes for 'Must change on next login' and 'Inactive'. A section on the right is titled 'Select groups that the user(s) should be a member.' and contains a search bar and a table with columns 'GROUP NAME' and 'ASSIGNED USERS'. At the bottom right, there are 'SAVE' and 'CANCEL' buttons.

3. Edit the fields as needed. The following fields are used for resetting a user's password.

4.

Field	Description
<b>Password</b>	Type a new password for the user. The password needs to meet complexity requirements.
<b>Confirm Password</b>	Retype the same password.
<b>Must change on next login</b>	Select the check box to require the user to change the password the next time the user logs in.

5. Click **Save**.  
The user changes are saved.

## Managing Application Assignment to a User

Users with the **Manage Users** permission can manage application access to a user from the Administration view.

To manage application access to a user:

1. Select the **Administration** view.

The **User** tab of the User Management page appears.

The screenshot shows the 'User Management' page with the 'Users' tab selected. A search bar and 'EXPORT' and '+ ADD USER' buttons are visible. Below the search bar, it says '6 found' and 'Display: 25 50 100'. A 'SELECT ALL' link is present. The table below has the following data:

	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
<input type="checkbox"/>	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

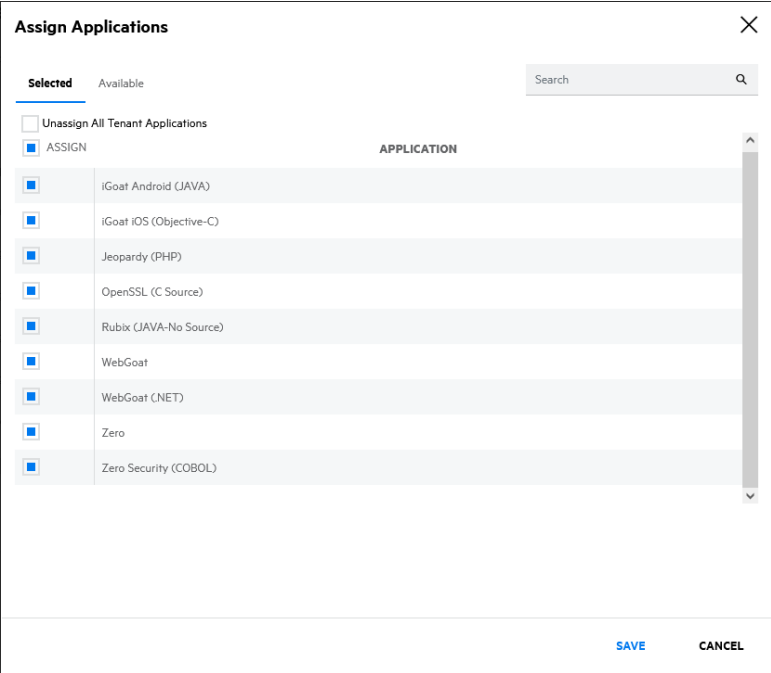
2. Click **Assign Applications** in the row of the user for whom you want to edit application access.  
The Assign Application window appears.

**Note:** The link is unavailable if a user is assigned to a role with the **All Application Access** permission.

3. You can perform the following tasks:

Task	Procedure
Assign applications to user	a. Select the <b>Available</b> tab.

Task	Procedure				
	<div data-bbox="643 310 1409 982" style="border: 1px solid black; padding: 10px;"> <p><b>Assign Applications</b> <span style="float: right;">✕</span></p> <p>Selected <u>Available</u> <span style="float: right;">Search <input type="text" value=""/> <input type="button" value="Q"/></span></p> <p><input type="checkbox"/> Assign All Tenant Applications</p> <p><input type="checkbox"/> ASSIGN <span style="margin-left: 100px;">APPLICATION</span></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30px;"><input type="checkbox"/></td> <td>Swagger Petstore</td> </tr> <tr> <td><input type="checkbox"/></td> <td>user access test</td> </tr> </table> <p style="text-align: right;"><input type="button" value="SAVE"/> <input type="button" value="CANCEL"/></p> </div> <p>b. Perform the following actions to select applications:</p> <ul style="list-style-type: none"> <li>○ Select the check box next to individual applications.</li> <li>○ Select the ASSIGN check box to select displayed applications.</li> <li>○ Select the <b>Assign All Tenant Applications</b> check box to select all applications.</li> </ul> <p>You can use the search field to filter the application list.</p>	<input type="checkbox"/>	Swagger Petstore	<input type="checkbox"/>	user access test
<input type="checkbox"/>	Swagger Petstore				
<input type="checkbox"/>	user access test				
Remove applications from user	<p>a. Click <b>Assign Applications</b>.</p> <p>b. Select the <b>Selected</b> tab.</p>				

Task	Procedure
	<div data-bbox="643 310 1409 978"></div> <p data-bbox="602 1010 1409 1331">c. Perform the following actions to remove applications:</p> <ul data-bbox="643 1062 1409 1276" style="list-style-type: none"><li>○ Clear the check box next to individual applications.</li><li>○ Clear the <b>ASSIGN</b> check box to remove displayed applications.</li><li>○ Select the <b>Unassign All Tenant Applications</b> check box to remove all applications.</li></ul> <p data-bbox="643 1297 1409 1331">You can use the search field to filter the application list.</p>

4. Click **Save**.

The changes to the user's assigned applications are saved.

## Related Topics

To manage user access to applications at the application level, see ["Managing User Assignment to an Application" on page 55](#).

## Deleting a User Account

To delete a user account:

1. Select the **Administration** view.

The **Users** tab of the User Management page appears.

USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangLDev2	Julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

2. Click **Delete** in the row of the user whom you want to delete.

A confirmation message appears.

3. Click **Yes**.

The user is deleted.

**Note:** When a user is deleted, occurrences of the user name, full name, email, and phone number are removed except when necessary for referential integrity and replaced with an unique user ID.

## Groups

Users can be sorted into groups to which applications can be assigned. This allow streamlining of application assignment. Groups can be designed around business groups, regions, or other organizational structure.

This section covers the following topics:

<a href="#">Viewing Groups</a>	276
<a href="#">Creating a Group</a>	277
<a href="#">Editing a Group</a>	278
<a href="#">Managing Application Assignment for a Group</a>	280
<a href="#">Deleting a Group</a>	282

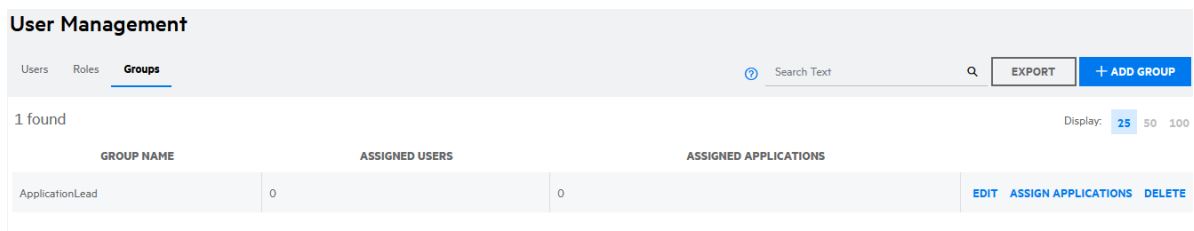
### Viewing Groups

To view the groups in your tenant:

1. Select the **Administration** view.  
The User Management page appears.



2. Select the **Groups** tab.



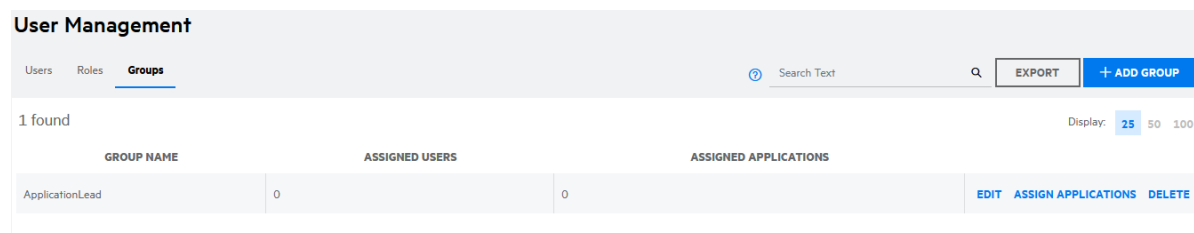
The following table describes how to navigate the **Groups** tab.

Task	Action
Search the group list	Type a keyword or phrase in the search field and press <b>Enter</b> . To remove the search results, remove the text from the search field and press <b>Enter</b> .
Export data as a .csv file	Click <b>Export</b> . A .csv file containing user group details is saved locally to a folder specified in your browser settings.
Add a group	Click <b>Add Group</b> . For more information, see <a href="#">"Creating a Group" below</a> .
Edit a group name and assigned users	Click <b>Edit</b> in the action column. For more information, see <a href="#">"Editing a Group" on the next page</a> .
Assign and unassign applications	Click <b>Assign Applications</b> in the action column. For more information, see <a href="#">"Managing Application Assignment for a Group" on page 280</a> .
Delete a group	Click <b>Delete</b> in the action column. For more information, see <a href="#">"Deleting a Group" on page 282</a> .

## Creating a Group

To create a group

1. Select the **Administration** view.  
The User Management page appears.
2. Select the **Groups** tab.



3. Click **+Add Group**.

The Add/Edit Group window appears.

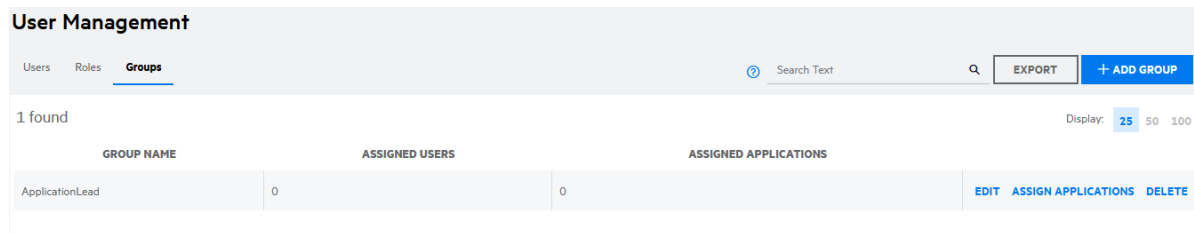
	LAST NAME	FIRST NAME	EMAIL	ROLE NAME
<input type="checkbox"/>	Brown	Bob	yeu-li.huang@microfocus.com	Developer
<input type="checkbox"/>	Huang	Edward	huange@fod.com	Executive
<input type="checkbox"/>	Huang	julie	julieh@fod.com	Lead Developer
<input type="checkbox"/>	Smith	James	james@fod.com	Application Lead

4. In the **Group Name** field, type the name of the new group.
5. Perform the following actions to select applications:
  - Select the check box next to individual users.
  - Select the **ASSIGN** check box to select displayed users.
  - Select the **Assign All Tenant Applications** check box to select all users.
6. Click **Save**.  
The new group appears in the group list.

## Editing a Group


To edit a group name as well as manage user assignment for a group:

1. Select the **Administration** view.  
The User Management page appears.
2. Select the **Groups** tab.



3. Click **Edit** in the row of the group that you want to edit.  
The Add/Edit Group window opens
4. You can perform the following tasks:

Task	Procedure
Edit the group name	In the <b>Group Name</b> field, type the new name of the group.
Assign users to group	<p>a. Select the <b>Available</b> tab.</p> <div data-bbox="646 819 1409 1564" data-label="Image"> </div> <p>b. Perform the following actions to select applications:</p> <ul style="list-style-type: none"> <li>○ Select the check box next to individual users.</li> <li>○ Select the <b>ASSIGN</b> check box to select displayed users.</li> <li>○ Select the <b>Assign All Tenant Users</b> check box to select all users.</li> </ul>

Task	Procedure
	You can use the search field to filter the user list.
Unassign users from group	<p>a. Select the <b>Selected</b> tab.</p>  <p>b. Perform the following actions to remove users:</p> <ul style="list-style-type: none"> <li>○ Clear the check box next to individual users.</li> <li>○ Clear the <b>ASSIGN</b> check box to remove displayed users.</li> <li>○ Select the <b>Unassign All Tenant Users</b> check box to remove all users.</li> </ul> <p>You can use the search field to filter the user list.</p>

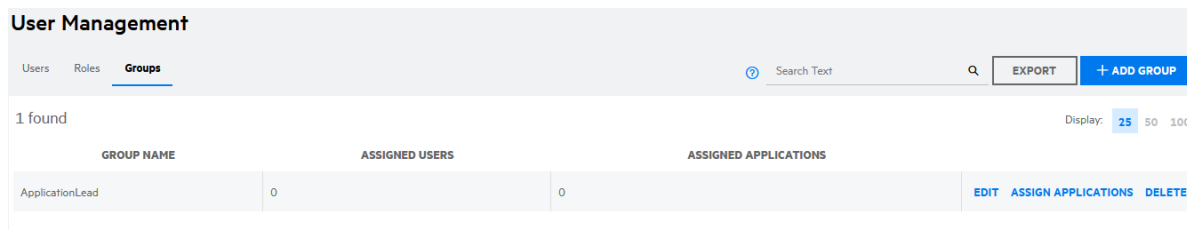
5. Click **Save**.  
Your group changes are saved.

## Managing Application Assignment for a Group

Users with the **Manage Users** permission can manage application assignment for a group from the Administration view.

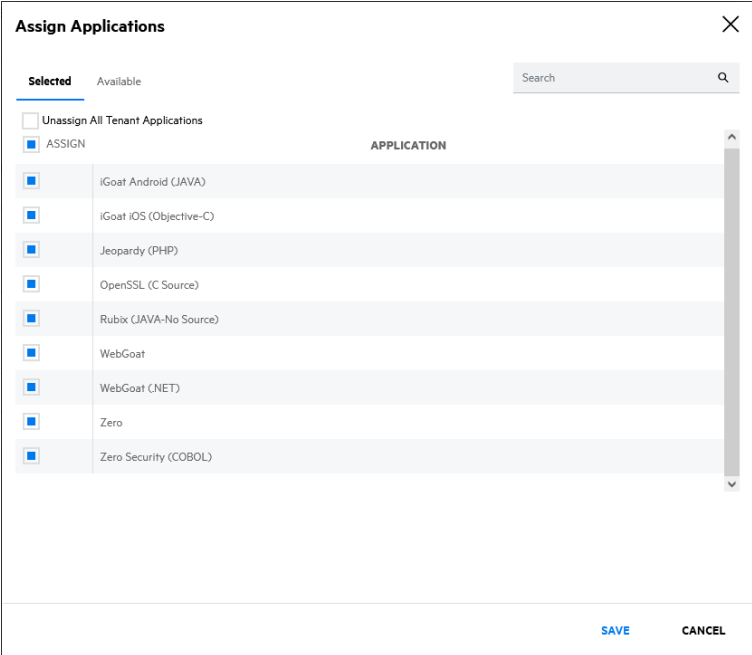
To manage application assignment for a group:

1. Select the **Administration** view.  
The User Management page appears.
2. Select the **Groups** tab.



3. Click **Assign Applications** in the row of the group to which you want to assign applications.  
The Assign Applications window opens.
4. You can perform the following tasks:

Task	Procedure
Assign applications to group	<p>a. Click <b>Assign Applications</b>.</p> <p>b. Select the <b>Available</b> tab.</p> <div data-bbox="662 415 1409 1066" data-label="Image"></div> <p>c. Perform the following actions to select applications:</p> <ul style="list-style-type: none"><li>◦ Select the check box next to individual applications.</li><li>◦ Select the <b>ASSIGN</b> check box to select displayed applications.</li><li>◦ Select the <b>Assign All Tenant Applications</b> check box to select all applications.</li></ul> <p>You can use the search field to filter the application list.</p> <p>d. Click <b>Save</b>.</p>
Unassign applications from group	<p>a. Click <b>Assign Applications</b>.</p> <p>b. Select the <b>Selected</b> tab.</p>

Task	Procedure
	<div data-bbox="662 310 1409 961"></div> <p data-bbox="623 995 1393 1262">c. Perform the following actions to remove applications:</p> <ul data-bbox="667 1045 1393 1262" style="list-style-type: none"><li>○ Clear the check box next to individual applications.</li><li>○ Clear the <b>ASSIGN</b> check box to remove displayed applications.</li><li>○ Select the <b>Unassign All Tenant Applications</b> check box to remove all applications.</li></ul> <p data-bbox="662 1283 1333 1314">You can use the search field to filter the application list.</p> <p data-bbox="623 1335 792 1367">d. Click <b>Save</b>.</p>

5. Click **Save**.

The changes to the group's assigned applications are saved.

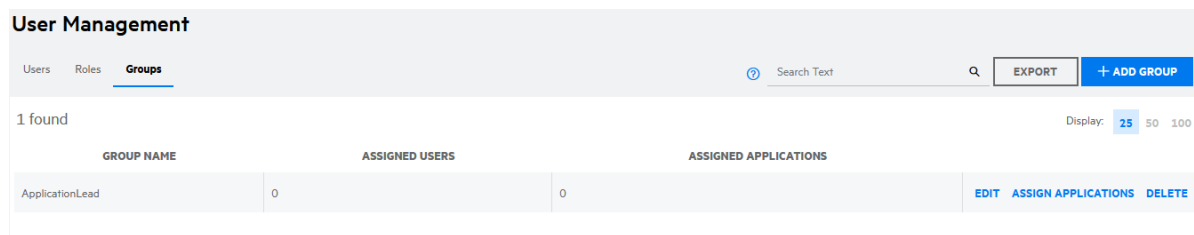
## Deleting a Group

To delete a group:

1. Select the **Administration** view.

The **User Management** page appears.

2. Select the **Groups** tab.



3. Click **Delete** in the row of the group that you want to delete.  
A confirmation message appears.
4. Click **Yes**.  
The group is deleted.

## Policy Management

Security Leads can configure how security policies are applied to applications in a tenant. They can also create and manage custom security policies.

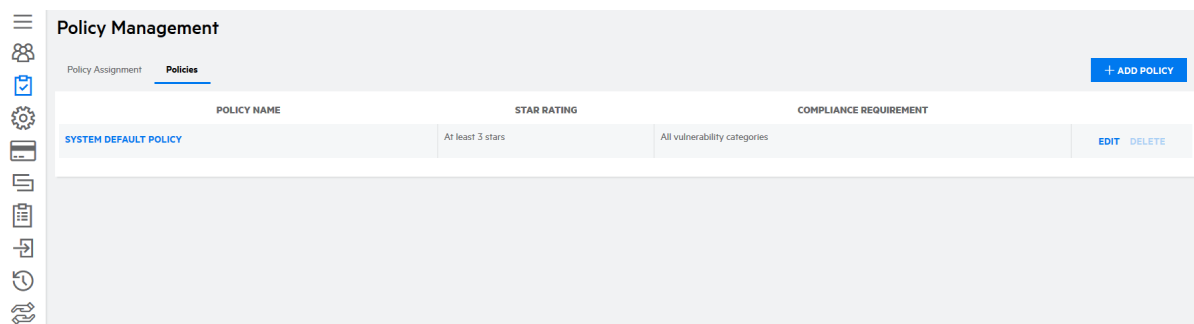
This section covers the following topics:

<a href="#">Creating a Security Policy</a>	283
<a href="#">Setting the Security Policy</a>	289
<a href="#">Deleting a Security Policy</a>	290

### Creating a Security Policy

To create a custom security policy:

1. Select the **Administration** view.  
The User Management page appears.
2. Click **Policy Management**.  
The **Scope** tab of the Policy Management page appears.
3. Select the **Policies** tab.



4. Click **+Add Policy**.

The **Add/Edit Policy** wizard appears.

The screenshot shows the 'Add/Edit Policy' wizard interface. On the left is a sidebar with a 'Policy Details' section highlighted. The main content area contains four form fields: 'Policy Name' with the value 'New Policy', 'Star Rating' with a dropdown menu showing 'At least 3 stars', 'Application Monitoring' with a dropdown menu showing 'Not required', and 'Compliance Requirement' with a dropdown menu showing 'All vulnerability categories'. At the bottom right of the form are three buttons: 'BACK', 'NEXT', and 'SAVE'.

5. On the Policy Details page, complete the following fields:

Field	Description
Policy Name	Type a name for the policy.
Star Rating	Select the minimum star rating an application must be awarded to be determined as passing.
Application Monitoring	Select whether Application Monitoring is required or not. If it is required, then a production release will fail if Application Monitoring is not enabled for the application.
Compliance Requirement	Select which vulnerabilities are included when determining the pass/ fail status of an application. You can retain the default value of all vulnerabilities or only include issues tagged with a specific compliance requirement, such as OWASP 2021 or PCI 3.2.  <b>Note:</b> The pass/fail status incorporates Application Monitoring and open source issues.

6. Click **Next**.

7. On the Assessment Types page, select which assessment types are available to applications that have the policy applied.



**Add/Edit Policy**

✓ Policy Details

**Assessment Types**

Development Releases

QA/Test Releases

Production Releases

Summary

**Allowed Assessment Types**

Allow All Assessment Types

**Static**

Static Analysis - Single Scan

Static Analysis - Subscription

Static Assessment - Single Scan

Static Assessment - Subscription

Static Basic - Single Scan

Static Basic - Subscription

Static+ Assessment - Single Scan

Static+ Assessment - Subscription

**Dynamic**

Dynamic Basic - Single Scan

Dynamic Basic - Subscription

Dynamic Express - Single Scan

BACK NEXT SAVE

- **Allow All Assessment Types** is selected by default. Leave it selected to have the security policy allow all assessment types, including ones added after the policy has been created.
- Deselect **Allow All Assessment Types** to individually select assessment types.

**Note:** If an application undergoes a policy update and has an active subscription or available remediation for an assessment type that is not allowed by the current policy, the subscription or remediation will still be available until it expires or is used.

8. Click **Next**.
9. On the Development Releases page, complete the fields that apply to Development status releases:

Field	Description
Remediation Grace Period (0 - 365 Days)	<p>Specify the issue remediation grace period for each issue severity level. When an issue found in a Development release is within its grace period, it will not affect the pass/ fail status of the release.</p> <p><b>Note:</b> The star rating specified above determines the issue severity levels displayed.</p>
Required Scan Frequency (0 - 365 Days)	<p>Specify the required scan frequency of each scan type. If a Development release has not completed a scan within the designated period of the scan type, it will fail. The value of 0 means no scan is required.</p>

10. Click **Next**.
11. On the QA/Test Releases page, complete the fields that apply to QA/Test status releases:

Field	Description
Remediation Grace Period (0 - 365 Days)	<p>Specify the issue remediation grace period for each issue severity level. When an issue found in a QA/Test release is within its grace period, it will not affect the pass/ fail status of the release.</p> <p><b>Note:</b> The star rating specified above determines the issue severity levels displayed.</p>
Required Scan Frequency (0 - 365 Days)	<p>Specify the required scan frequency of each scan type. If a QA/Test release has not completed a scan within the designated period of the scan type, it will fail. The value of 0 means no scan is required.</p>

12. Click **Next**.
13. On the Production Releases page, complete the fields that apply to Production status releases:

Field	Description
Remediation Grace Period (0 - 365 Days)	<p>Specify the issue remediation grace period for each issue severity level. When an issue found in a Production release is within its grace period, it will not affect the pass/ fail status of the release.</p> <p><b>Note:</b> The star rating specified above determines the issue severity levels displayed.</p>
Required Scan Frequency (0 - 365 Days)	<p>Specify the required scan frequency of each scan type. If a Production release has not completed a scan within the designated period of the scan type, it will fail. The value of 0 means no scan is required.</p>

14. Click **Next**.
15. On the Summary page, review the policy settings.

**Add/Edit Policy**

✓ Policy Details  
✓ Assessment Types  
✓ Development Releases  
✓ QA/Test Releases  
✓ Production Releases

**Summary**

**Policy Details**  
**Policy Name**  
New Policy  
**Star Rating**  
At least 3 stars  
**Compliance Requirement**  
All vulnerability categories  
**Application Monitoring**  
Required

**Development Releases**  
**Remediation Grace Period**  
Critical: 0 days  
High: 0 days  
**Required Scan Frequency**  
Static: None  
Dynamic: None  
Mobile: None

**QA/Test Releases**  
**Remediation Grace Period**  
Critical: 0 days  
High: 0 days  
**Required Scan Frequency**  
Static: None  
Dynamic: None  
Mobile: None

**Production Releases**  
**Remediation Grace Period**  
Critical: 0 days  
High: 0 days  
**Required Scan Frequency**

BACK NEXT SAVE

16. Click **Save**.

The new policy appears in the **Policies** tab.

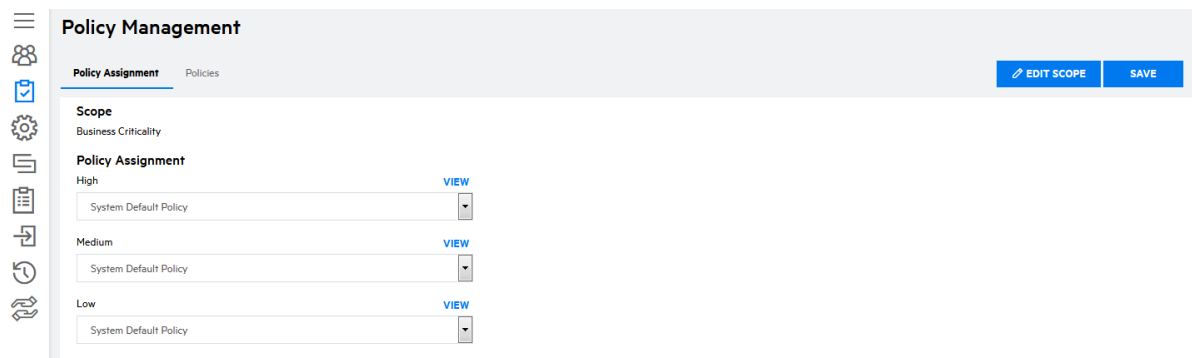
### Related Topics:

- For information on Star Ratings, see ["Five-Star Assessment Rating" on page 20](#).
- For information on manually overriding the Pass/Fail settings, see ["Overriding the Security Policy of a Release" on page 68](#).

## Setting the Security Policy

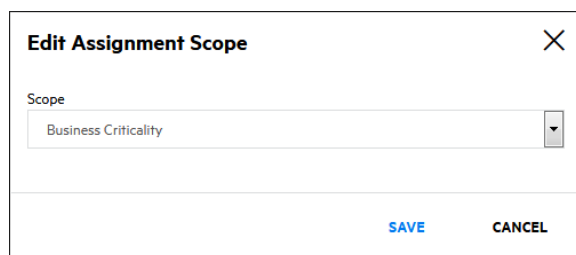
To set the security policy for your tenant:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Click **Policy Management**.  
The **Policy Assignment** tab of the **Policy Management** page appears.



3. Click **Edit**.

The **Edit Assignment Scope** modal window opens.



4. Select the scope for determining how policies are applied from the **Scope** list. Only one scope can be applied per tenant. The available values are:
  - **Business Criticality**: groups applications according to their assigned Business Criticality level. For more information on Business Criticality levels, see ["Creating an Application" on page 43](#).
  - **Application Type**: groups applications as web / thick-client or mobile.
  - **Application Attribute**: groups applications based on the values of the application attribute that you select from the **Attribute** list. This value is invalid if no application attributes have been created in the tenant.

**Note:** The selection is limited to picklist type attributes that have ten or less values.

5. Click **Save**.

You are returned to the **Scope** tab.

6. Select the policy that will be assigned to each value of the selected scope.

7. Click **Save**.

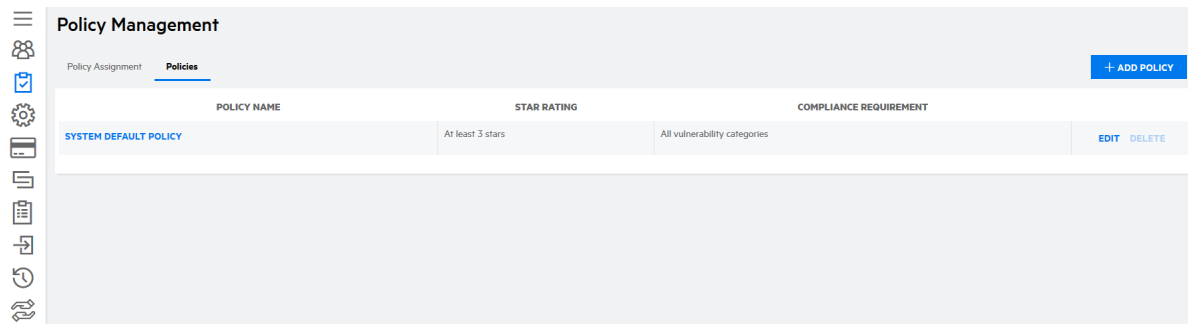
Your security policy settings are saved.

## Deleting a Security Policy

You can delete a custom security policy that is currently not in use. The Fortify on Demand default policy can be edited but not be deleted.

To delete a custom security policy:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Click **Policy Management**.  
The **Scope** tab of the **Policy Management** page appears.
3. Select the **Policies** tab.



4. Click **Delete** in the row of the policy you want to delete.  
A confirmation message appears.
5. Click **Yes**.  
The policy is deleted.

## Single Sign-On (SSO)

Single Sign-On (SSO) eliminates the need to maintain separate credentials for Fortify on Demand and helps administrators seamlessly manage user access and provisioning. Fortify on Demand supports SSO integration with existing identity providers through the SAML 2.0 standard for federated identity.

Fortify on Demand supports the following SAML 2.0 bindings:

- POST and Redirect bindings for SAML authentication requests from Fortify on Demand to the identity provider
- POST binding for SAML assertion responses from the identity provider to Fortify on Demand

Security Leads can configure SSO for the tenant. SSO configuration consists of the following tasks:

- Configuring SSO in Fortify on Demand. For instructions, see ["Configuring SSO in Fortify on Demand" on the next page](#).
- Adding the identity provider metadata to Fortify on Demand. For instructions, see ["Adding the Identity Provider Metadata" on page 295](#).
- Downloading the Fortify on Demand metadata. For instructions, see ["Downloading the Fortify on Demand Metadata" on page 297](#)
- Configuring SSO in your identity provider. For instructions, see ["Configuring SSO in the Identity Provider" on page 297](#).

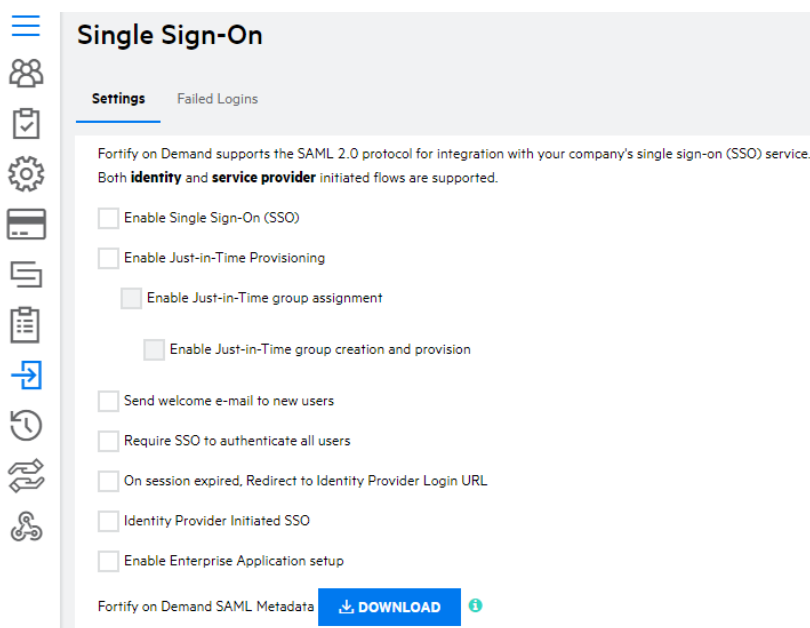
## Configuring SSO in Fortify on Demand

Configure the Fortify on Demand SSO settings and map the Fortify on Demand attribute names to the identity provider attribute names.

To configure the Fortify on Demand SSO settings:

1. Select the **Administration** view.  
The User Management page appears.

2. Click **Single Sign-On**.  
The Single Sign-On page appears.



3. Select the desired check boxes:

Field	Description
Enable Single Sign-on (SSO)	This option enables SSO.
Enable Just-in-Time Provisioning	This option allows the automatic creation or update of Fortify on Demand user accounts for users who authenticate through your identify provider.
Enable Just in Time group assignment	<b>Enable Just-in-Time Provisioning</b> must be selected. This option allows the automatic update of Fortify on Demand user group assignments through your identity provider.



Field	Description
Enable Just in Time group creation and provision	<p><b>Enable Just-in-Time Provisioning</b> and <b>Enable Just in Time group assignment</b> must be selected. This option allows the automatic creation of Fortify on Demand user groups through your identity provider.</p>
Send welcome e-mail to new users	<p>New users who are created through the portal will receive a welcome email. However, the welcome email includes password setup instructions that do not apply to users who authenticate through SSO. If this option is not selected, welcome emails are not sent to any new users .</p>
Require SSO to Authenticate All Users	<p>This option requires all users to use SSO. If this option is not selected, users may log in to Fortify on Demand using SSO authentication or username and password on the standard login page.</p> <p><b>Note:</b> Enabling this option prevents the use of some specialized clients and integrations that use the Fortify on Demand Web API because the Web API has limited support for SAML authentication tokens. For example, the iOS client requires non-SSO credentials to connect to Fortify on Demand. The recommended approach in this case is to generate a strong, random password (minimum 32 characters) that can be used as a “personal access token” for non-SSO authentication.</p>
On session expired, Redirect to Identity Provider Login URL	<p>This option has users redirected to their identity provider login page after the session expires or when the user logs out. This feature requires cookies to be enabled in the browser and a user login session within the last 30 days.</p>
Identity Provider Initiated SSO	<p>Fortify on Demand recommends the service provider-initiated SAML authentication flow, but supports both service provider-initiated and identity provider-initiated flows. If this option is not selected, users log in to Fortify on Demand using the SSO Login URL provided on this page. Fortify on Demand then makes a service provider-initiated request to the identity provider to authenticate the user. If this option is selected, the identity provider-initiated flow is used. Users log in by connecting directly to the identity provider and are redirected to Fortify on Demand after successful authentication.</p>

Field	Description
Enable Enterprise Application setup	<p>If your organization has multiple tenants, this option enables authentication through a single identity provider.</p> <p><b>Note:</b> If you select this option and have an existing SSO configuration, you will need to download the updated Fortify on Demand metadata and import it into the identity provider, and reimport the identity provider metadata into Fortify on Demand. Alternatively, you can append <code>?t=&lt;ssologinurlguid&gt;</code> to both the <b>Identity Provider Name</b> in the Fortify on Demand SSO settings and the service provider name in the identity provider settings, where <code>&lt;ssologinurlguid&gt;</code> is a unique identifier found in the SSO Login URL.</p>

- In the **Attributes** section, map the attribute names expected by Fortify on Demand to those configured in the identify provider. Each attribute name defined here must match the exact **Name** value of the attribute used by the identity provider, and is often defined as a full schema URL. Some identity providers also send a shorter **FriendlyName** value for the attribute, which can also be used in the attribute mapping. For descriptions of each attribute, see ["Configuring SSO in the Identity Provider" on page 297](#).

**Attributes** ⓘ

Attribute	Name
User Name	<input type="text"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Email	<input type="text"/>
Mobile Number	<input type="text"/>
Groups	<input type="text"/>
Role	<input type="text"/>

Enable Custom Security Lead Mapping

Custom Mapping

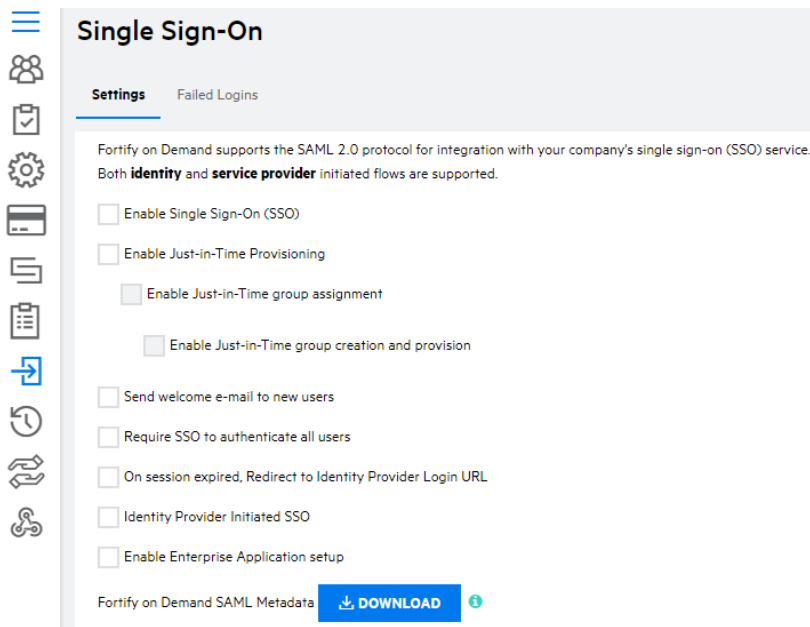
- Select **Enable Custom Security Lead Mapping** to map a custom value (instead of the default "Security Lead" value) to the Security Lead role in SAML assertion. Type that value in the **Custom Mapping** field. Note that this invalidates the default "Security Lead" value used for the mapping.
- Click **Save**.  
Your SSO settings are saved.

## Adding the Identity Provider Metadata

Add the identity provider metadata by importing it into Fortify on Demand or manually configuring it.

To add the identity provider metadata:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Click **Single Sign-On**.  
The Single Sign-On page appears.



3. In the **Configure Identity Provider** section, select the method of adding the identity provider metadata:
  - **Import Identity Provider Metadata**
  - **Edit Manually**

### Configure Identity Provider

Import Identity Provider Metadata

Edit Manually

Identity Provider Name

Identity Provider Login URL

Authentication Request Binding

Limit to Values Supported by Identity Provider

SAML Request Signing Algorithm

SHA-1  SHA-256

Identity Provider Certificate

SSO Login URL ?

4. Follow the instructions for the method that you selected.
  - Import the identity provider metadata:
    - i. Click the browse button.
    - ii. Navigate to and select the .xml file.
    - iii. Click **Import**.
  - Manually configure the identity provider metadata:
    - i. Complete the fields with the information of your identity provider:
      - **Identity Provider Name**
      - **Identity Provider Login URL**
      - **Authentication Request Binding** (select **Limit to Values Supported by Identity Provider** to use the bindings supported by the identity provider)
      - **SAML Request Signing Algorithm**
      - **Identity Provider Certificate**

**Note:** Once SSO is configured, users will need to use the link in the **SSO Login URL** box to log in to Fortify on Demand.

5. Click **Save**.

The identity provider metadata is added to Fortify on Demand.

## Downloading the Fortify on Demand Metadata

Download the Fortify on Demand metadata file to help configure your identity provider to respond to authentication requests from Fortify on Demand. The Fortify on Demand metadata file includes the Assertion Consumer Service URLs, the Fortify on Demand certificate, and the entity ID (also known as the service provider name).

To download the Fortify on Demand metadata file:

1. Select the **Administration** view.

The User Management page appears.

2. Click **Single Sign-On**.

The Single Sign-On page appears.



3. Click **Download**.

The Fortify on Demand metadata file is saved to a local folder specified in your browser settings.

**Note:** The metadata is also available as a URL to support configuration in identity providers that support automatic metadata retrieval. The metadata is accessed using the absolute path “/SAML” on the portal site (for example, "https://ams.fortify.com/SAML"). The metadata URL does not require authentication, so it can be accessed by the identity provider without supplying Fortify on Demand credentials.

## Configuring SSO in the Identity Provider

Fortify on Demand supports any identity provider that conforms to the SAML 2.0 specifications for browser-based authentication flows. Use the following instructions as a guideline for configuring your identity provider for use with Fortify on Demand.

Most required information about the Fortify on Demand service provider can be obtained from the SAML metadata, and many identity providers allows importing the metadata rather than configuring all the settings manually.

To configure SSO in the identity provider:

1. Accept authentication requests from Fortify on Demand.

The identity provider must accept authentication requests sent from the Fortify on Demand service provider name. The service provider name is "https://<tenant\_host>/SAML," where the <tenant\_host> is your Fortify on Demand datacenter (for example, "https://ams.fortify.com/SAML"). You can obtain the service provider name from the Fortify on Demand SAML metadata.

Fortify on Demand signs all authentication requests, so you may also choose to validate the signature against the SAML certificate provided in the Fortify on Demand SAML metadata.

**Note:** Prior to version 5.2, Fortify on Demand used a service provider name that was incompatible with some identity providers. If you set up SSO authentication prior to version 5.2, you can keep the "urn:fortify:FodServiceProvider" service provider name for backward compatibility with the existing identity provider configuration. You are encouraged to migrate to the new service provider name at the earliest convenience.

2. Sign all SAML assertions.

All SAML assertions sent to Fortify on Demand must be signed using the identity provider certificate specified in the Fortify on Demand SSO settings. Fortify on Demand accepts signatures on either the entire SAML response or just the assertion contained in the response.

**Note:** Fortify on Demand does not support encrypted assertions.

3. Make sure the identity provider's system clock is set properly, preferably from a central time source service such as NIST.

Most SAML assertions contain a valid time period specified by the identity provider. Fortify on Demand checks the time period against its system clock when the assertion is received. Fortify on Demand allows a maximum of 3 minutes clock skew to account for differences in the clock settings. If the assertion is received more than 3 minutes after the expiration time specified in the assertion, then the assertion is rejected.

4. Set the URL where the identity provider will send the SAML assertion response after a user is authenticated

The URL is known as the Assertion Consumer Service URL. It might have a different term, such as "Reply URL," depending on the identity provider. You can obtain the URL from the Fortify on Demand SAML metadata.

5. Define the identity claim attributes to include in the SAML assertion.

Fortify on Demand uses the claim attributes in the SAML assertion to get information about the authenticated user.

Every assertion must contain a User Name attribute, which identifies the user to Fortify on Demand. The value must be unique across Fortify on Demand, so you should use an identifier that is unique to your organization, such as an email address.

**Note:** Some systems use the **NameID** value in the Subject element of the SAML assertion to pass the user identifier. Fortify on Demand does not support use of **NameID**, so you must also map an attribute for User Name.

The following attributes are used for Just-In-Time (JIT) Provisioning. Attributes are required when creating a new Fortify on Demand user. When updating an existing Fortify on Demand user, all attributes are optional and existing values are retained for unspecified attributes.

Attribute	Required	Description
Email	Yes	Email address of the user. The value can be the same as the User Name value, but is not required. You can map both User Name and Email to the same attribute in the Fortify on Demand SSO settings.
First Name	Yes	First name of the user.
Last Name	Yes	Last name of the user.
Mobile Number	No	Mobile phone number of the user.
Role	No	User role. The value must be a plain text string that matches a role name (case-insensitive) in Fortify on Demand. If a value is not provided, the <b>Developer</b> role is set for a new user. If the value does not match a role name, an error is returned.
Group	No	User group. The value must be a plain text string (maximum 50 characters and case-insensitive). If the value does not match an existing user group in Fortify on Demand, the user group will be created if the portal SSO option <b>Enable Just-in-Time group creation and provision</b> is selected.  <b>Note:</b> If a user logs in using SSO and the Groups attribute is empty in the SAML assertion, any existing user group assignments will be removed.
provision_user	Yes	Specifies whether or not a user is automatically created in Fortify on Demand if not found. If the value is set to TRUE, then a new user is created. If the value is set to FALSE or not provided, then a user is not created and the login request will fail if the user does not already exist in Fortify on Demand.  <b>Note:</b> If a value is not provided and JIT Provisioning is enabled in the portal, provision_user defaults to TRUE.
update_user	No	Specifies whether or not an existing user's details in Fortify on

Attribute	Required	Description
		<p>Demand are automatically updated from the attribute values in the SAML assertion. If the value is set to TRUE, then user details are automatically updated. If the value is set to FALSE, then user details are not updated.</p> <p>If a value is not provided, the value of the <code>provision_user</code> attribute is used. You can specify both to control creating and updating separately. For example, you might want to manually create users in the portal, but have user details updated from the assertion values.</p>
mtt	No	<p>If the portal SSO option <b>Enable Enterprise Application setup</b> is selected, this attribute is required.</p> <p>Unique identifier found in the SSO Login URL, enclosed in quotation marks. For example, given the URL <code>https://ams.fortify.com/SSO/Login/c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc</code>, the identifier is <code>c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc</code>.</p>

**Note:** You must configure Fortify on Demand to recognize the attributes used by the identity provider. See ["Configuring SSO in Fortify on Demand" on page 292](#).

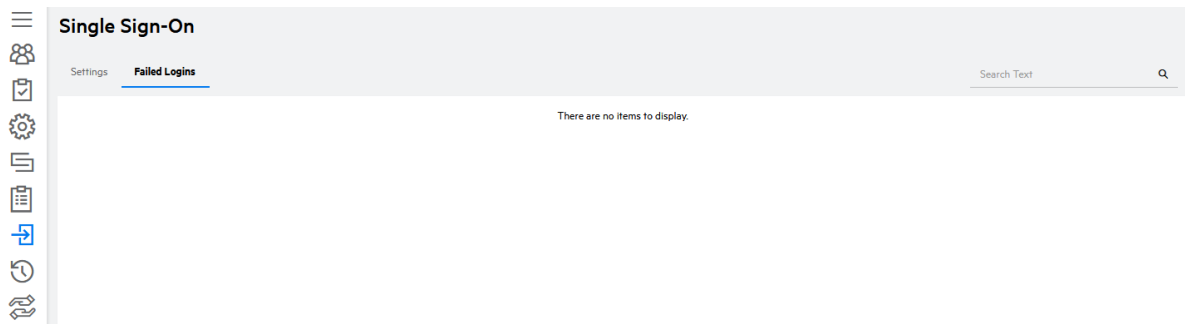
## Troubleshooting Failed Logins

Troubleshooting a failed SSO authentication request can be a difficult task because the actual values passed in the SAML assertion are hidden from the user. To assist with troubleshooting efforts, the portal provides a log of failed SAML assertions. Failed assertions are deleted after 30 days.

To view a log of failed SAML Assertions:

1. Select the **Administration** view.  
The User Management page appears.
2. Click **Single Sign-On**.  
The Single Sign-On page appears.
3. Select the **Failed Logins** tab.  
The failed SAML assertion log appears.





The grid contains the following columns:

- Received Time - The time that the SAML assertion was received.
  - IP Address – The IP address of that client that requested authentication.
  - Username – The username that was specified in the assertion, if one was found.
  - Reason – A brief description of the reason why the SAML assertion was rejected.
4. Click the **Raw Assertion** link for any failed login to open an XML view of the decoded SAML assertion.

The page displays the details of the assertion, including the time that the assertion was issued by the identity provider, the attributes and values that were provided, the valid time period and audience, and the certificate used to sign the assertion.

## Vendor Management

If you would like to share your assessment results with a vendor your company does business with, or with another division of your company, you can do so through the portal, as long as each entity has its own tenant with Fortify on Demand. Relationships between tenants must be initiated by one tenant and confirmed by the other; no one can establish a connection to your tenant without your permission.

Also, each link goes in only one direction. That is, if you would like to share your reports, you must initiate a link to another tenant. If that tenant would like to share its reports with you, it must *also* initiate a link. The **Vendor Report** link is only visible after the sharing relationship is successful, and reports are shared.

Note: You are only sharing your assessment results, your code is not being shared.

### This section covers the following topics:

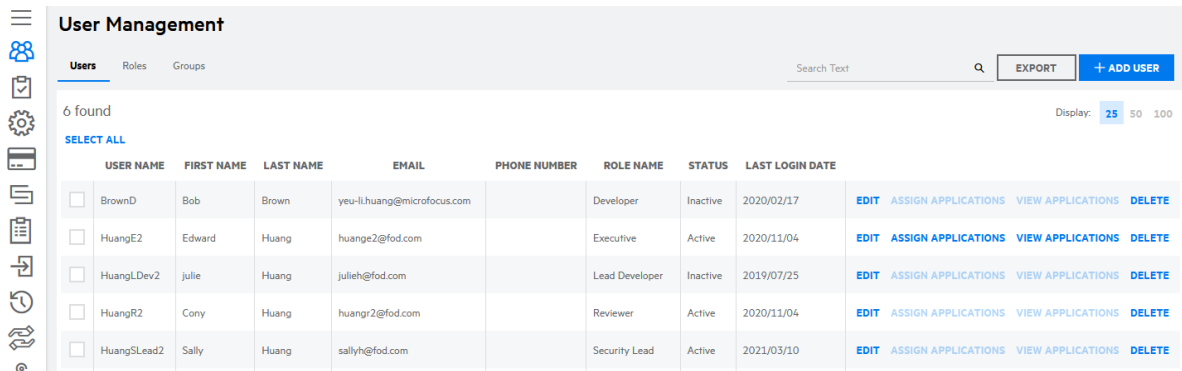
- [Initiating a Relationship with Another Tenant](#)
- [Accepting a Relationship Initiated by Another Tenant](#)
- [Publishing a Vendor Management Report](#)
- [Viewing Published Report](#)

## Initiating a Relationship with Another Tenant

To establish your tenant as a “Vendor” (that is, one that can send reports to other tenants):

1. Select the **Administration** view.

The **User Management** page appears.



The screenshot shows the 'User Management' interface. It includes a sidebar with navigation icons, a search bar, and an 'EXPORT' button. Below the search bar, it indicates '6 found' and a 'Display' dropdown set to '25'. A 'SELECT ALL' link is present above the table. The table lists users with columns for USER NAME, FIRST NAME, LAST NAME, EMAIL, PHONE NUMBER, ROLE NAME, STATUS, and LAST LOGIN DATE. Each row has a checkbox and a set of action links: EDIT, ASSIGN APPLICATIONS, VIEW APPLICATIONS, and DELETE.

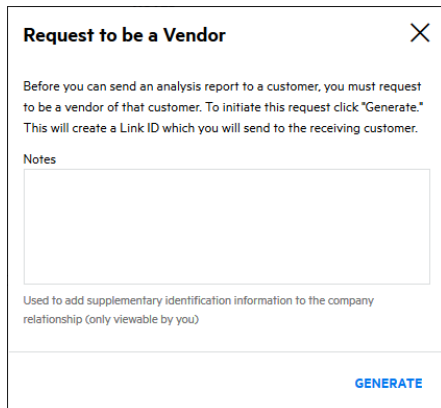
	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
<input type="checkbox"/>	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangLDev2	Julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

2. Click **Vendors**.
3. Select the **Customers** tab.

**Note:** "My Vendors" means tenants you can receive reports from, and “Customers” means tenants you can send reports to.

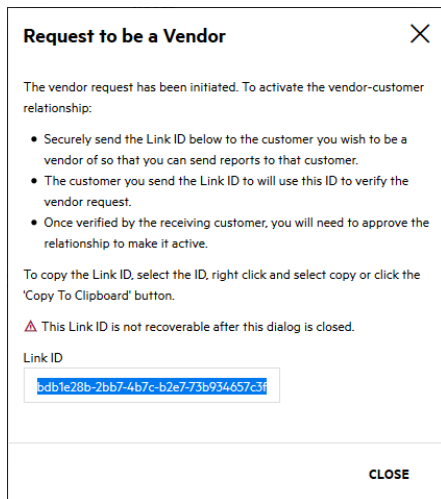
4. Click **Request to be a Vendor**.

Use the optional **Notes** box to add information about the vendor-customer relationship.



The dialog box titled 'Request to be a Vendor' contains the following text: 'Before you can send an analysis report to a customer, you must request to be a vendor of that customer. To initiate this request click "Generate." This will create a Link ID which you will send to the receiving customer.' Below this is a 'Notes' section with a text area. At the bottom, there is a 'GENERATE' button.

5. Click **Generate**, to display the **Link ID number**.



6. Copy the **Link ID number**,
7. Send the link, via email or other secure transfer, to the appropriate contact at the company or tenant you would like to connect with.
8. Click **Close**.

## Accepting a Relationship Initiated by Another Tenant

Accepting a relationship initiated by another tenant is a two-step process.

- ["Confirm a Relationship" below](#)
- ["Establish your Tenant as a Customer" on the next page](#)

### Confirm a Relationship

To confirm a relationship with another tenant who has sent a request to you:

1. Select the **Administration** view.

The **User Management** page appears.

**User Management**

Users Roles Groups Search Text [EXPORT] + ADD USER

6 found Display: 25 50 100

SELECT ALL

	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
<input type="checkbox"/>	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
<input type="checkbox"/>	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

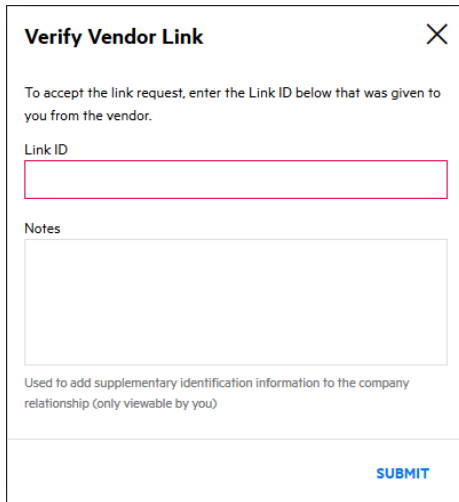
2. Click **Vendors**.

The **Vendor Management** page opens, displaying the **My Vendors** and **Customers** tabs. In this context, “Vendors” means tenants you can receive reports from, and “Customers” means tenants you can send reports to.

## Establish your Tenant as a Customer

To establish your tenant as a “Customer” (that is, one that can receive reports from other tenants):

1. Click **My Vendors**.
2. Click **Verify Vendor Link**.



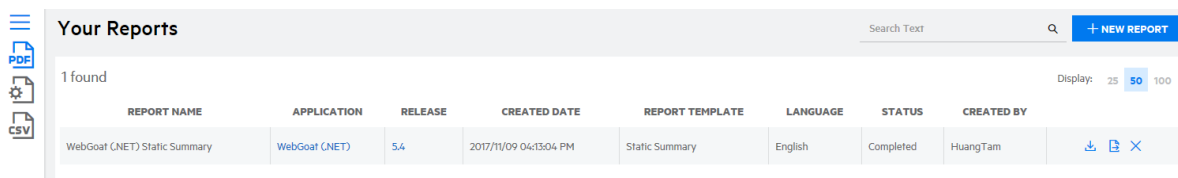
3. Paste the **Link ID** you received from the other tenant.
4. (Optional) Add supplementary notes about the company relationship (For example: subsidiary, or AUS division). These notes are viewable only to you.
5. Click **Submit**.

## Publishing a Vendor Management Report

Once you have established a relationship with another tenant in Fortify on Demand, you can “publish” your reports so that tenant can review them.

To share a report with an approved vendor:

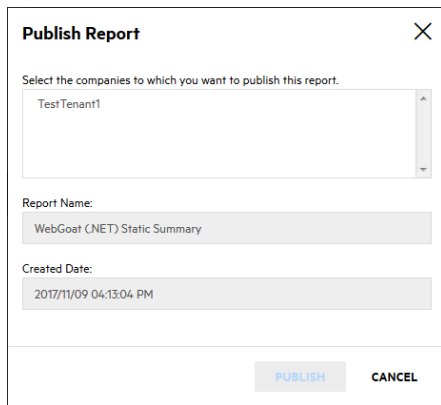
1. Select the **Reports** page.  
A new screen appears, with a list of all reports that have been generated for your tenant.
2. Click the name of the report you want to share. The page refreshes with the **Reports Details** below the reports list.



REPORT NAME	APPLICATION	RELEASE	CREATED DATE	REPORT TEMPLATE	LANGUAGE	STATUS	CREATED BY
WebGoat (NET) Static Summary	WebGoat (NET)	5.4	2017/11/09 04:13:04 PM	Static Summary	English	Completed	HuangTam

3. Click .

The **Publish Report** window appears. If you have relationships established with other tenants, those tenants' names appear in the white box.



4. Select the tenant name to which you want to send the report, and click **Publish**.

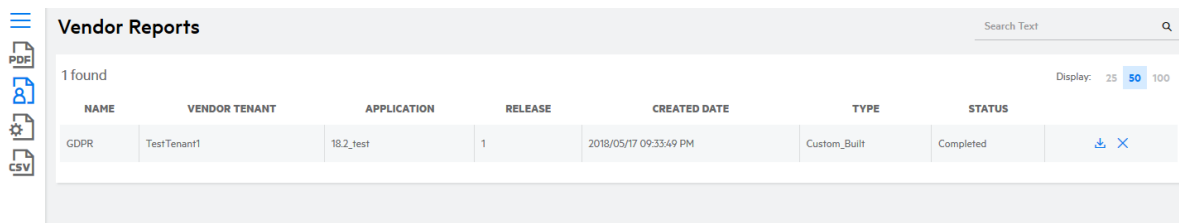
A note appears informing you that the report has been queued for publishing and will be sent to the other tenant.



## Viewing Published Report

After another tenant has published a report to you (that is, “shared” a report with your tenant), you may view that report by following these steps:

1. Select the **Reports** page.
2. Click **Vendor Report**.

A **Report List** appears, showing the reports that have been shared with you by other tenants.



NAME	VENDOR TENANT	APPLICATION	RELEASE	CREATED DATE	TYPE	STATUS	Action
GDPR	TestTenant1	18.2_test	1	2018/05/17 09:33:49 PM	Custom_Built	Completed	 

3. Highlight a report from the list, click **Download Report** in the **Action** column.

A note appears informing you that the report is available to you in PDF format in your system Downloads folder.

Note: If **Vendor Report** does not appear in the list of report types screen, that means no reports have yet been shared by another tenant. Check to make sure that you and the other tenant have both completed all the steps required to create a successful sharing relationship and that a specific report has been “published” to you.

# Chapter 8: Fortify on Demand API

Fortify on Demand provides a RESTful Application Programming Interface (API) that allow users to carry out various tasks and access application and release data. The latest version of the API is version 3. The API root URL is determined by the tenant's data center:

Data Center	API Root URL
AMS	https://api.ams.fortify.com
EMEA	https://api.emea.fortify.com
APAC	https://api.apac.fortify.com
Trial	https://api.trial.fortify.com
FedRAMP	https://api.fed.fortifygov.com/

**Note:** The Fortify on Demand API does not support cross-origin resource sharing (CORS).

This section contains the following topics:

- [API Authentication](#) ..... 306
- [API Scopes](#) ..... 308
- [Personal Access Tokens](#) ..... 309
- [Viewing API Documentation through API Explorer](#) ..... 311
- [Testing API Endpoints through API Explorer](#) ..... 313
- [API Rate Limits](#) ..... 316

## API Authentication

Authentication of Fortify on Demand API requests is through a bearer token. Obtain a bearer token by sending a request to the token endpoint.

To authenticate Fortify on Demand API calls:

1. Make a POST request to the token endpoint `<datacenter_root_url>/oauth/token` with the following body parameters:

**Note:** For a list of data center API root URLs, see ["Fortify on Demand API" above](#).

Body Parameter	Description
scope	Scopes granted to an access token (in lower case). Separate multiple scope values with a space. For a list of scopes, see <a href="#">"API Scopes" on the next page</a> .
grant_type	Grant type (in lower case): <ul style="list-style-type: none"><li>password: user credentials (Resource Owner Password Credentials)</li><li>client_credentials: API key and secret</li></ul>
username	Account username as <code>&lt;tenant_code&gt;\&lt;username&gt;</code> . Your tenant code and username are displayed in your account settings. Enclose the username with quotation marks to escape special characters.
password	Account password or personal access token. Enclose the password with quotation marks to escape special characters.  <b>Note:</b> SSO users are restricted to using personal access tokens.  <b>Note:</b> If a personal access token is used as a password and the specified scopes do not make up a subset of the personal access token's allowed scopes, the authentication will fail. For more information on personal access tokens, see <a href="#">"Personal Access Tokens" on page 309</a> .
client_id	API key
client_secret	API secret

A token in a JSON response named "access\_token" is returned.

2. Use this token in the Authorization header as a Bearer token:

```
Authorization: Bearer {token}
```

The following is an example request to get a bearer token using user credentials:

```
curl --request POST 'https://api.ams.fortify.com/oauth/token' \  
--form 'scope="api-tenant"' \  
--form 'grant_type="password"' \  
--form 'username="myTenantCode\myUsername"' \  
--form 'password="myPassword"'
```

The following is an example request to get a bearer token using an API key and secret.

```
curl --request POST 'https://api.ams.fortify.com/oauth/token' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data-urlencode 'scope=api-tenant' \  
--data-urlencode 'grant_type=client_credentials' \  
--data-urlencode 'client_id=myApiKey' \  
--data-urlencode 'client_secret=myApiSecret'
```

## API Scopes

Scopes limit the access that is granted to access tokens. They do not grant additional permissions beyond what a user currently has. You can view the details of an endpoint in API Explorer to see its allowed scopes.

The following table lists the available scopes:

Scope	Description
api-tenant	Grants access to all endpoints
start-scans	Configure and start static, dynamic, and mobile scans; import static and dynamic scans
manage-apps	Manage applications
view-apps	View applications
manage-issues	Manage issues
view-issues	View issues
manage-reports	Manage reports
view-reports	View reports
manage-users	Manage users
view-users	View users
manage-notifications	Manage notifications
view-tenant-data	View data at the tenant level



## Personal Access Tokens

Personal access tokens are unique keys tied to the user who generated them. They function as alternate passwords that are used to authenticate to the API; they have the user's permissions and can be further restricted with scopes. Using personal access tokens bypasses two-factor authentication and SSO requirements set in the portal.

**Note:** Personal access tokens cannot be used to log in to the portal.

Personal access tokens provide a flexible and secure method of authentication for integrations with Fortify on Demand. Users can have multiple tokens with different scopes for specific needs, specify token expiration dates, and disable tokens at any time.

Fortify on Demand sends email and portal notifications 14 days before a personal access token expires. An expired personal access token cannot be used unless a new secret is generated.

This section covers the following topics:

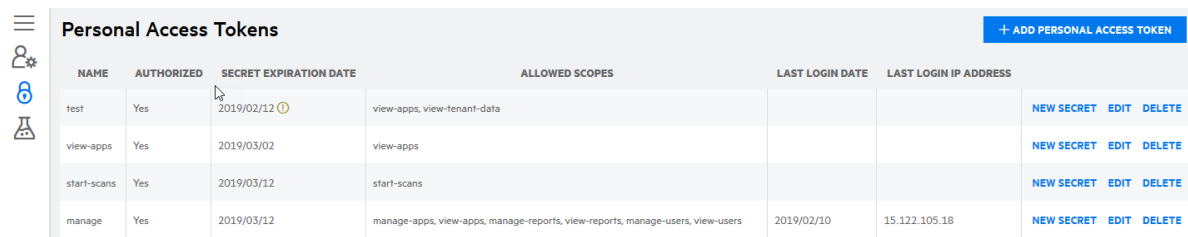
<a href="#">Creating a Personal Access Token</a>	309
<a href="#">Editing or Deleting a Personal Access Token</a>	311

## Creating a Personal Access Token

To create a personal access token:

1. Click your account name and select **Personal Access Tokens**.

The Personal Access Tokens page appears.



NAME	AUTHORIZED	SECRET EXPIRATION DATE	ALLOWED SCOPES	LAST LOGIN DATE	LAST LOGIN IP ADDRESS	
test	Yes	2019/02/12	view-apps, view-tenant-data			NEW SECRET EDIT DELETE
view-apps	Yes	2019/03/02	view-apps			NEW SECRET EDIT DELETE
start-scans	Yes	2019/03/12	start-scans			NEW SECRET EDIT DELETE
manage	Yes	2019/03/12	manage-apps, view-apps, manage-reports, view-reports, manage-users, view-users	2019/02/10	15.122.105.18	NEW SECRET EDIT DELETE

2. Click **+Add Personal Access Token**.

The Add/Edit Personal Access Token window opens.

3. Complete the fields. Fields are required unless otherwise noted.

Field	Description
<b>Name</b>	Type a name for the token.
<b>Authorize to use API</b>	The token is enabled by default. Move the slider to <b>No</b> to disable the token.
<b>Secret Expiration Date, Secret Expiration Days</b>	Use the calendar to select an expiration date or type the number of days after which a secret expires. The token will expire at 00:00 PT of the date you set. The expiration date cannot exceed the maximum lifetime as set by the portal.
<b>Allowed Scopes</b>	Select the allowed scopes for the token. For more information on scopes, see <a href="#">"API Scopes" on page 308</a> .

4. Click **Save**.  
The Secret Key window opens.
5. Copy your Base64 encoded secret. The secret is only shown once.
6. Click **Close**.  
The new token appears in the personal access token list.

## Editing or Deleting a Personal Access Token

To edit or delete a personal access token:

1. Click your account name and select **Personal Access Tokens**.

The Personal Access Tokens page appears.

NAME	AUTHORIZED	SECRET EXPIRATION DATE	ALLOWED SCOPES	LAST LOGIN DATE	LAST LOGIN IP ADDRESS	
test	Yes	2019/02/12	view-apps, view-tenant-data			NEW SECRET EDIT DELETE
view-apps	Yes	2019/03/02	view-apps			NEW SECRET EDIT DELETE
start-scans	Yes	2019/03/12	start-scans			NEW SECRET EDIT DELETE
manage	Yes	2019/03/12	manage-apps, view-apps, manage-reports, view-reports, manage-users, view-users	2019/02/10	15.122.105.18	NEW SECRET EDIT DELETE

2. You can perform the following tasks:

Task	Procedure
Generate a new secret	<ol style="list-style-type: none"><li>a. Click <b>New Secret</b>. The New Secret window opens.</li><li>b. Use the calendar to select an expiration date or type the number of days after which a secret expires. The token will expire at 00:00 PT of the date you set. The expiration date cannot exceed the maximum lifetime as set by the portal.</li><li>c. Click <b>Create</b>. This will void the current secret.</li></ol>
Edit the token	<ol style="list-style-type: none"><li>a. Click <b>Edit</b>. The Add/Edit Personal Access Token window opens.</li><li>b. Edit the fields as needed. You cannot edit the current secret's expiration date.</li></ol>
Delete the token	<ol style="list-style-type: none"><li>a. Click <b>Delete</b>. A confirmation message appears.</li><li>b. Click <b>Yes</b>.</li></ol>

## Viewing API Documentation through API Explorer

Fortify on Demand API documentation is provided in the form of API Explorer. API Explorer is built on the Swagger (OpenAPI) framework and is available directly from the portal. This allows the API to be self-documenting and interactive; users can instantly view the latest updates to the API and test calls, as well as use the JSON description of the API to generate stubs and SDKs in different programming languages through open source tools like Swagger Editor and Swagger Codegen.

To view API Explorer:

1. Click your account name on the toolbar and select **API Explorer**.

The API Explorer page opens in a new window, displaying a list of resources.

Authenticate		access_token	Get JSON	
<b>Fortify on Demand Web API Explorer</b>				
ApplicationMonitoring	Show/Hide	List Operations	Expand Operations	
Applications	Show/Hide	List Operations	Expand Operations	
Attributes	Show/Hide	List Operations	Expand Operations	
DigitalDiscovery	Show/Hide	List Operations	Expand Operations	
DynamicScans	Show/Hide	List Operations	Expand Operations	
LookuptItems	Show/Hide	List Operations	Expand Operations	
MobileScans	Show/Hide	List Operations	Expand Operations	
MultiFactorAuthorizationCode	Show/Hide	List Operations	Expand Operations	
NetworkScans	Show/Hide	List Operations	Expand Operations	
Notifications	Show/Hide	List Operations	Expand Operations	
OpenSourceComponents	Show/Hide	List Operations	Expand Operations	
Releases	Show/Hide	List Operations	Expand Operations	
Reports	Show/Hide	List Operations	Expand Operations	
StaticScans	Show/Hide	List Operations	Expand Operations	
TenantEntitlements	Show/Hide	List Operations	Expand Operations	
TenantHeatMaps	Show/Hide	List Operations	Expand Operations	

2. Explore the resources in greater detail:

- Click **GET JSON** at the top of the API Explorer page. The browser displays the JSON description of the API.

```
{
  "swagger": "2.0",
  "info": {
    "version": "v3",
    "title": "Fortify on Demand Web API Explorer",
    "host": "16.103.234.237",
    "schemes": [
      "http"
    ],
    "paths": {
      "/api/v3/applications/{applicationId}": {
        "get": {
          "tags": [
            "Applications"
          ],
          "summary": "Retrieves an individual application by id",
          "operationId": "ApplicationsV3_GetApplication",
          "consumes": [
            "application/json"
          ],
          "produces": [
            "application/json",
            "application/xml",
            "text/xml"
          ],
          "parameters": [
            {
              "name": "applicationId",
              "in": "path",
              "description": "The application id",
              "required": true,
              "type": "integer",
              "format": "int32"
            }
          ],
          "responses": {
            "200": {
              "description": "Ok",
              "schema": {
                "$ref": "#/definitions/Application"
              }
            },
            "401": {
              "description": "Unauthorized"
            },
            "404": {
              "description": "Not Found"
            },
            "500": {
              "description": "InternalServerError",
              "deprecated": false,
              "put": {
                "tags": [
                  "Applications"
                ],
                "summary": "Update an application",
                "operationId": "ApplicationsV3_PutApplication",
                "consumes": [
                  "application/json",
                  "text/json",
                  "application/xml",
                  "text/xml"
                ],
                "application/x-www-form-urlencoded",
                "multipart/form-data"
              ],
              "produces": [
                "application/json",
                "text/json",
                "application/xml",
                "text/xml"
              ],
              "parameters": [
                {
                  "name": "applicationId",
                  "in": "path",
                  "description": "The application id",
                  "required": true,
                  "type": "integer",
                  "format": "int32"
                },
                {
                  "name": "requestModel",
                  "in": "body",
                  "description": "The application data",
                  "required": true,
                  "schema": {
                    "$ref": "#/definitions/PutApplicationRequest"
                  }
                }
              ],
              "responses": {
                "200": {
                  "description": "Ok",
                  "schema": {
                    "$ref": "#/definitions/PutApplicationResponse"
                  }
                },
                "400": {
                  "description": "BadRequest",
                  "schema": {
                    "$ref": "#/definitions/PutApplicationResponse"
                  }
                },
                "401": {
                  "description": "Unauthorized"
                },
                "403": {
                  "description": "Forbidden"
                },
                "404": {
                  "description": "Not Found"
                },
                "422": {
                  "description": "UnprocessableEntity",
                  "schema": {
                    "$ref": "#/definitions/PutApplicationResponse"
                  }
                },
                "500": {
                  "description": "InternalServerError",
                  "deprecated": false,
                  "delete": {
                    "tags": [
                      "Applications"
                    ],
                    "summary": "Deletes an application",
                    "operationId": "ApplicationsV3_Delete",
                    "consumes": [
                      "application/json",
                      "text/json",
                      "application/xml",
                      "text/xml"
                    ],
                    "parameters": [
                      {
                        "name": "applicationId",
                        "in": "path",
                        "description": "The application id",
                        "required": true,
                        "type": "integer",
                        "format": "int32"
                      }
                    ],
                    "responses": {
                      "200": {
                        "description": "Ok",
                        "schema": {
                          "$ref": "#/definitions/DeleteApplicationResponse"
                        }
                      },
                      "401": {
                        "description": "Unauthorized"
                      },
                      "403": {
                        "description": "Forbidden"
                      },
                      "404": {
                        "description": "Not Found"
                      },
                      "500": {
                        "description": "InternalServerError",
                        "deprecated": false
                      }
                    }
                  }
                }
              }
            }
          }
        }
      },
      "/api/v3/applications": {
        "get": {
          "tags": [
            "Applications"
          ],
          "summary": "Retrieve a collection of applications",
          "operationId": "ApplicationsV3_GetApplications",
          "consumes": [
            "application/json",
            "text/json",
            "application/xml",
            "text/xml"
          ],
          "parameters": [
            {
              "name": "filters",
              "in": "query",
              "description": "cpA delimited list of field filters.</p>\r\n\r\nField name and value should be separated by a colon (:).</p>\r\n\r\nMultiple fields should be separated by a plus (+). Example, fieldname1=value&fieldname2=value\r\n\r\n",
              "required": false,
              "type": "string"
            },
            {
              "name": "orderBy",
              "in": "query",
              "description": "The field name to order the results by.",
              "required": false,
              "type": "string"
            },
            {
              "name": "fields",
              "in": "query",
              "description": "Comma separated list of fields to return.",
              "required": false,
              "type": "string"
            },
            {
              "name": "offset",
              "in": "query",
              "description": "Offset of the starting record. 0 indicates the first record.",
              "required": false,
              "type": "integer",
              "format": "int32"
            },
            {
              "name": "limit",
              "in": "query",
              "description": "Maximum records to return. The maximum value allowed is 50.",
              "required": false,
              "type": "integer",
              "format": "int32"
            }
          ],
          "responses": {
            "200": {
              "description": "Ok",
              "schema": {
                "$ref": "#/definitions/ApplicationListResponse"
              }
            },
            "400": {
              "description": "BadRequest",
              "schema": {
                "$ref": "#/definitions/ErrorResponse"
              }
            },
            "401": {
              "description": "Unauthorized"
            },
            "500": {
              "description": "InternalServerError",
              "deprecated": false,
              "post": {
                "tags": [
                  "Applications"
                ],
                "summary": "Create a new application and release",
                "operationId": "ApplicationsV3_PostApplication",
                "consumes": [
                  "application/json",
                  "text/json",
                  "application/xml",
                  "text/xml",
                  "application/x-www-form-urlencoded",
                  "multipart/form-data"
                ],
                "produces": [
                  "application/json",
                  "text/json",
                  "application/xml",
                  "text/xml"
                ],
                "parameters": [
                  {
                    "name": "requestModel",
                    "in": "body",
                    "description": "The application data",
                    "required": true,
                    "schema": {
                      "$ref": "#/definitions/PostApplicationRequest"
                    }
                  }
                ],
                "responses": {
                  "204": {
                    "description": "No Content"
                  },
                  "201": {
                    "description": "Created",
                    "schema": {
                      "$ref": "#/definitions/PostApplicationResponse"
                    }
                  },
                  "400": {
                    "description": "BadRequest",
                    "schema": {
                      "$ref": "#/definitions/ErrorResponse"
                    }
                  },
                  "401": {
                    "description": "Unauthorized"
                  },
                  "422": {
                    "description": "UnprocessableEntity",
                    "schema": {
                      "$ref": "#/definitions/ErrorResponse"
                    }
                  },
                  "500": {
                    "description": "InternalServerError",
                    "deprecated": false
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}
```

You can paste or import the JSON file in a code generator tool that supports Swagger, such as [Swagger Editor](#) or [Swagger Codegen](#), and generate client stubs or SDKs.

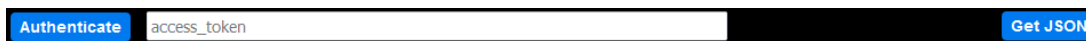
- Click **Show/Hide** to switch between showing and hiding the endpoints.
- Click **List Operations** to view a resource's endpoints.
- Click **Expand Operations** to view the descriptions of all the resource's endpoints.
- Click an endpoint to view its description.

## Testing API Endpoints through API Explorer

You can test the version 3 API endpoints in API Explorer.

**Important!** POST, PUT, and DELETE methods in API Explorer modify the tenant data in the portal.

1. Click **Authenticate** at the top of the API Explorer page.



A modal window opens where you provide your authentication credentials.

Real data will be accessed and modified using the "Try it out!" button for each endpoint.

**Exercise extra caution with Post, Put, and Delete endpoints as these will affect production data!**

[Help with Authentication](#)

Grant Type  
password

Scope  
api-tenant

Username

Password

Tenant

If your tenant requires two-factor authentication enter the Security Code

Close Submit

2. Select the method of authentication from the **Grant Type** list:
  - **password**: the user account credentials in the portal
  - **client\_credentials**: the API keys generated in the portal
3. In the **Scope** field, type the scopes that will be granted to an access token. Separate multiple scope values with a space. For a list of scopes, see ["API Scopes" on page 308](#).
4. Provide your authentication credentials:

<b>Method of Authentication</b>	<b>Procedure</b>
<b>client_credentials</b>	<ol style="list-style-type: none"><li>a. In the <b>Client ID</b> field, type the API Key. For information on creating an API key, see <a href="#">"Creating an API Key" on page 247</a>.</li><li>b. In the <b>Client Secret</b> field, type the API secret.</li></ol>
<b>password</b>	<p><b>Note:</b> You can obtain your tenant code and username from your account settings.</p> <ol style="list-style-type: none"><li>a. In the <b>Username</b> field, type your account username.</li><li>b. In the <b>Password</b> field, type your account password or your personal access token.</li></ol> <p><b>Note:</b> If a personal access token is used and the specified scopes are not a subset of the personal access token's allowed scopes, the authentication will fail.</p> <ol style="list-style-type: none"><li>c. In the <b>Tenant</b> field, type your tenant code.</li><li>d. (Required if two-factor authentication is enabled) In the <b>Security Code</b> field, type the security code you received as part of two-factor authentication.</li></ol>

5. Click **Submit**.

An access token is generated for the session.

6. Expand an endpoint and complete the parameters in the fields provided.

GET /api/v3/applications/{applicationId} Retrieves an individual application by id

Response Class (Status 200)  
Ok

Model | Model Schema

```
{
  "applicationId": 0,
  "applicationName": "string",
  "applicationDescription": "string",
  "applicationCreatedDate": "2016-05-20T16:01:36.708Z",
  "businessCriticalityTypeId": 0,
  "businessCriticalityType": "string",
  "emailList": "string",
  "applicationTypeId": 0,
  "applicationType": "string",
  "attributes": {}
}
```

Response Content Type: application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
applicationId	<input type="text" value="(required)"/>	The application id	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
401	Unauthorized		
404	NotFound		
500	InternalServerError		

7. Click **Try it out!**.

The response is displayed below.

Try it out! [Hide Response](#)

**Curl**

```
curl -X GET --header 'Accept: application/json' --header 'Authorization: Bearer gAAAAH21jER2935DMsX8qvA2q6qyhpPh8c0VeDfNo_9KqeqnWz
```

**Request URL**

```
http://16.103.234.237/api/v3/applications/4191
```

**Response Body**

```
{
  "applicationId": 4191,
  "applicationName": "Test Application",
  "applicationDescription": null,
  "applicationCreatedDate": "2016-01-26T10:23:22.717",
  "businessCriticalityTypeId": 3,
  "businessCriticalityType": "Low",
  "emailList": null,
  "applicationTypeId": 1,
  "applicationType": "Web_Thick_Client",
  "attributes": null
}
```

**Response Code**

```
200
```

**Response Headers**

```
{
  "pragma": "no-cache",
  "date": "Thu, 19 May 2016 14:14:34 GMT",
  "server": "Microsoft-IIS/8.5",
  "x-powered-by": "ASP.NET",
  "content-type": "application/json; charset=utf-8",
  "expires": "-1",
  "cache-control": "no-cache",
  "content-length": "296",
  "x-ua-compatible": "IE=Edge"
}
```

## API Rate Limits

Fortify on Demand implements API rate limiting on a per endpoint and per user or key basis.

The following endpoints are unthrottled:

- PUT /api/v3/releases/{releaseId}/dynamic-scans/import-scan
- POST /api/v3/releases/{releaseId}/mobile-scans/start-scan
- PUT /api/v3/releases/{releaseId}/mobile-scans/import-scan
- POST /api/v3/releases/{releaseId}/static-scans/start-scan
- PUT /api/v3/releases/{releaseId}/static-scans/import-scan

The following table lists the rate limits for throttled endpoints.

Endpoint	Max Requests	Seconds
POST /api/v3/applications	6	30



Endpoint	Max Requests	Seconds
PUT /api/v3/applications/{applicationId:int}	1	30
GET /api/v3/eventlogs/download	1	300
POST /api/v3/releases	6	30
PUT /api/v3/releases/{releaseld:int}	1	30
POST /api/v3/releases/{releaseld:int}/dynamic-scans/start-scan	1	30
GET /api/v3/releases/{releaseld:int}/fpr	1	30
<b>Note:</b> The rate limit is per scan type.		
GET /api/v3/releases/{releaseld:int}/vulnerabilities/{vulnId}/all-data	1	1
POST /api/v3/releases/{releaseld:int}/vulnerabilities/bug-link	1	5
POST /api/v3/releases/{releaseld:int}/vulnerabilities/bulk-edit	1	5
Other endpoints	10	1

## Tracking Rate Limits

When calling an API endpoint, the response HTTP header provides the rate limit and how quickly you are approaching the rate limit:

- X-Rate-Limit-Limit: the maximum number of requests
- X-Rate-Limit-Remaining: the number of requests remaining
- X-Rate-Limit-Reset: the number of seconds until the rate limit resets

When you reach the rate limit for an API endpoint, the API returns an HTTP 429 "Too Many Requests" response status code along with a response message such as:

```
{
  "errors": [
    {
      "errorCode": null,
      "message": "Rate limit of 1 request(s) every 15 second(s) has been exceeded"
    }
  ]
}
```

```
}
```

## Best Practices To Avoid Rate Limiting

To avoid rate limiting when calling the API, use the following best practices to reduce and regulate the number of API requests:

- Cache frequently used data.  
For API endpoints that are frequently used, cache the API responses and load the cached responses when requesting the data.
- Eliminate any unnecessary API calls.  
Examine requests obtaining data that isn't being utilized and requests submitting data to Fortify on Demand without any changes.
- Regulate the request rate  
If you regularly reach the rate limit, consider including a process that regulates the rate of your requests so that they fall within the given rate limits. You can regulate the request rate statically by setting a fixed request rate or dynamically by tracking requests and regulating them when approaching the rate limit.

# Chapter 9: Development Tools

Fortify on Demand offers a variety of development tools to help your organization integrate application security testing into your DevOps processes.

The following Integrated Development Environment (IDE) tools enable developers to upload code from IDEs to Fortify on Demand for static testing:

IDE Tool	Description	More Information
Eclipse Plugin	Eclipse plugin for uploading code to Fortify on Demand for static testing	<a href="#">"Eclipse Plugin" on page 339</a>
IntelliJ IDEA Plugin	IntelliJ IDEA plugin for uploading code to Fortify on Demand for static testing	<a href="#">"IntelliJ Plugin" on page 359</a>
Visual Studio Extension	Visual Studio extension for uploading code to Fortify on Demand for static testing	<a href="#">"Visual Studio Extension" on page 323</a>
Fortify Extension for Visual Studio Code	Visual Studio Code extension for uploading code to Fortify on Demand for static testing	<a href="#">Visual Studio Marketplace for Visual Studio 2017, 2019</a> <a href="#">Visual Studio Marketplace for Visual Studio 2022</a>
Fortify Security Assistant for Eclipse	Fortify Security Assistant for Eclipse provides alerts to potential security issues in Java files as you write code. <sup>1</sup>  It includes semantic and intra-class dataflow analyzers to detect: <ul style="list-style-type: none"><li>• Potentially dangerous uses of functions and APIs</li><li>• Issues caused by tainted data reaching vulnerable functions and APIs at the intra-class level</li></ul>	<a href="#">Fortify Marketplace</a>
Fortify Security	Fortify Security Assistant for IntelliJ and	<a href="#">JetBrains Marketplace</a>

IDE Tool	Description	More Information
Assistant for IntelliJ and Android Studio	<p>Android Studio provides alerts to potential security issues in Java files as you write code.<sup>1</sup></p> <p>It includes structural and configuration analyzers to detect:</p> <ul style="list-style-type: none"> <li>• Potentially dangerous uses of functions and APIs</li> <li>• Insecure application configurations in property and XML files</li> </ul>	
Fortify Security Assistant for Visual Studio	<p>Fortify Security Assistant for Visual Studio provides alerts to potential security issues in C# (.cs), Razor (.cshtml), WebForms (.aspx), and .config, .xml, and .ini files as you write code.<sup>1</sup></p> <p>It includes structural and configuration analyzers to detect:</p> <ul style="list-style-type: none"> <li>• Potentially dangerous uses of functions and APIs</li> <li>• Insecure application configuration</li> </ul>	<p><a href="#">Visual Studio Marketplace for Visual Studio 2017, 2019</a></p> <p><a href="#">Visual Studio Marketplace for Visual Studio 2022</a></p>

<sup>1</sup>Fortify Security Assistant requires a valid license file to scan for issues and to install or update Fortify security content. Fortify on Demand offers a license valid for up to 10 developers per each application that is under an active static assessment subscription. The license is valid for all Fortify Security Assistant versions.

The following Continuous Integration and Continuous Delivery (CICD) integration tools enable static and dynamic testing to be integrated into existing build automation:

CICD Tool	Description	More Information
FoDUploader	Stand-alone utility for uploading code from a build server to Fortify on Demand for static testing	<a href="#">"FoDUploader" on page 374</a>
Fortify on Demand Jenkins Plugin	Jenkins plugin for uploading code to Fortify on Demand and submitting static scans as build tasks	<a href="#">Jenkins page</a>
Fortify Azure DevOps Extension	Azure DevOps extension for:	<a href="#">Visual Studio Marketplace</a>

CICD Tool	Description	More Information
	<ul style="list-style-type: none"> <li>Uploading code to Fortify on Demand and submitting static scans as build and release tasks</li> <li>Submitting dynamic scans as build and release tasks</li> </ul>	

Other tools include:

Tool	Description	More Information
Fortify Static Code Analyzer	Translate-only version of Fortify Static Code Analyzer for translating C/C++ and Scala code and packaging it for scanning  <b>Note:</b> Fortify Static Code Analyzer requires a valid license file to translate source code.	<a href="#">Fortify Static Code Analyzer and Tools Documentation</a>
Fortify ABAP Extractor	SAP transport request for downloading source code files to the presentation server	<a href="#">"Preparing ABAP (SAP) Application Files" on page 95</a>
Fortify ScanCentral SAST client	Stand-alone Fortify ScanCentral SAST client for packaging source code	<a href="#">"Fortify ScanCentral SAST" on page 91</a>
Fortify WebInspect Web Macro Recorder	Stand-alone utility for creating workflow macros	<a href="#">Fortify WebInspect Documentation</a>
Fortify FoD-SSC Sync	Stand-alone utility for automated, scheduled synchronization of Fortify on Demand applications, releases, and scans with Fortify Software Security Center (SSC)	<a href="#">GitHub</a>
Fortify Bug Tracker	Stand-alone utility for submitting Fortify on Demand issues to bug trackers	<a href="#">GitHub</a>
Fortify CI Tools	Docker container for simplifying integration of Fortify static application security testing for DevSecOps pipelines that use configurable runners to execute CICD workflows	<a href="#">Docker Hub</a>

This section contains the following topics:

<a href="#">Viewing Tools</a>	322
<a href="#">Visual Studio Extension</a>	323
<a href="#">Eclipse Plugin</a>	339
<a href="#">IntelliJ Plugin</a>	359
<a href="#">FoDUploader</a>	374

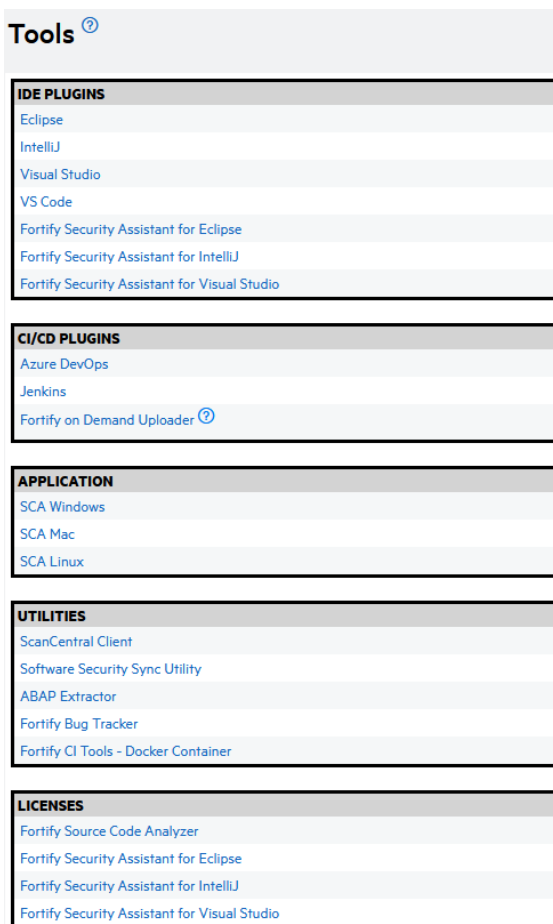
## Viewing Tools

You can view a list of the tools available for use with Fortify on Demand.

To view the available tools:

1. Click your account name and select **Tools** from the list.

The Tools page appears.



2. Click the links for installers, licenses, and usage instructions.

**Note:** Usage of the tools does not require a license except for the following:

- Fortify Static Code Analyzer: contact support to request a license if you need to scan C, C++, and Scala code.
- Fortify Security Assistant: contact support to request a license if you have an active static subscription.

## Visual Studio Extension

Fortify on Demand provides a Visual Studio extension so that you can upload code for static scans and open analysis results for remediation.

This section contains the following topics:

<a href="#">Installing the Visual Studio Extension</a>	323
<a href="#">Configuring the Visual Studio Extension</a>	324
<a href="#">Uploading Code with the Visual Studio Extension</a>	325
<a href="#">Opening Analysis Results with the Visual Studio Extension</a>	331
<a href="#">Analysis Results in the Visual Studio Extension</a>	333
<a href="#">Analysis Trace Icons</a>	335
<a href="#">Reviewing Issues from the Visual Studio Extension</a>	336
<a href="#">Auditing Issues from the Visual Studio Extension</a>	337
<a href="#">Locating the Source Code Associated with Static Scan Issues</a>	338
<a href="#">Logging Out</a>	339
<a href="#">Uninstalling the Visual Studio Extension</a>	339

## Installing the Visual Studio Extension

**Note:** These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To install the Visual Studio extension:

1. In Visual Studio, access the dialog box to manage extensions.
2. Search the Visual Studio Marketplace for Fortify on Demand.
3. Download and install the Fortify on Demand Visual Studio extension.

**Note:** To install this extension as an administrator and allow all users to use the extension, download the VSIX file from the Visual Studio Marketplace and then install it using VSIXInstaller with the /admin option from the Command Prompt.

## Configuring the Visual Studio Extension

You can configure how the Visual Studio extension connects to Fortify on Demand and specify the location of the Fortify ScanCentral client executable.

To configure the Visual Studio extension:

1. From the Visual Studio Fortify extension menu, select **Options**.

The screenshot shows the 'Fortify on Demand Options' dialog box. It features a blue title bar with the text 'Fortify on Demand Options' and a close button. The main area contains several configuration sections: 'Default API Root URL' with a dropdown menu showing 'https://api.ams.fortify.com' and a 'Clear Portal History' link; 'Disable SSL Validation' and 'Use Proxy' checkboxes; a 'Proxy Configuration' section with 'Proxy URL' and 'Proxy Port' text boxes, and a 'Proxy Authentication' section with 'Proxy Username' and 'Proxy Password' text boxes; and a 'ScanCentral SAST' section with a 'File Path' text box and a browse button. At the bottom are 'OK' and 'Cancel' buttons.

2. In the **Default API Root URL** box, enter the Fortify on Demand API Root URL.  
To obtain this URL, see ["Fortify on Demand API" on page 306](#) or contact a TAM.
3. To enable the extension to accept any server certificate, select the **Disable SSL Validation** check box.

**Note:** For security reasons, selecting this option is not recommended.

4. If you require a proxy server (and you have not yet configured a proxy in the Windows Internet options), select **Use Proxy**, and then follow these steps:
  - a. In the **Proxy URL** box, type the URL for your proxy server.
  - b. In the **Proxy Port** box, type the port for the proxy server.



- c. If you require authentication for your proxy server, select **Proxy Authentication** and provide the authentication credentials.
5. If you are using Fortify ScanCentral client to package your code, you can specify the executable location under **ScanCentral SAST**.

You can download the Fortify ScanCentral client from the Tools page (see ["Viewing Tools" on page 322](#)). For installation instructions, see the README.txt file included in the downloaded ZIP.

**Note:** If you do not specify the location of the Fortify ScanCentral client here, then the first time you upload your project to Fortify on Demand using ScanCentral packaging, you are prompted to specify the location.

6. Click **OK**.

## Uploading Code with the Visual Studio Extension

Before you start, make sure that you have the following:

- Your Fortify on Demand login credentials

**Note:** To upload your code, you must have the Start Static Scan permission.

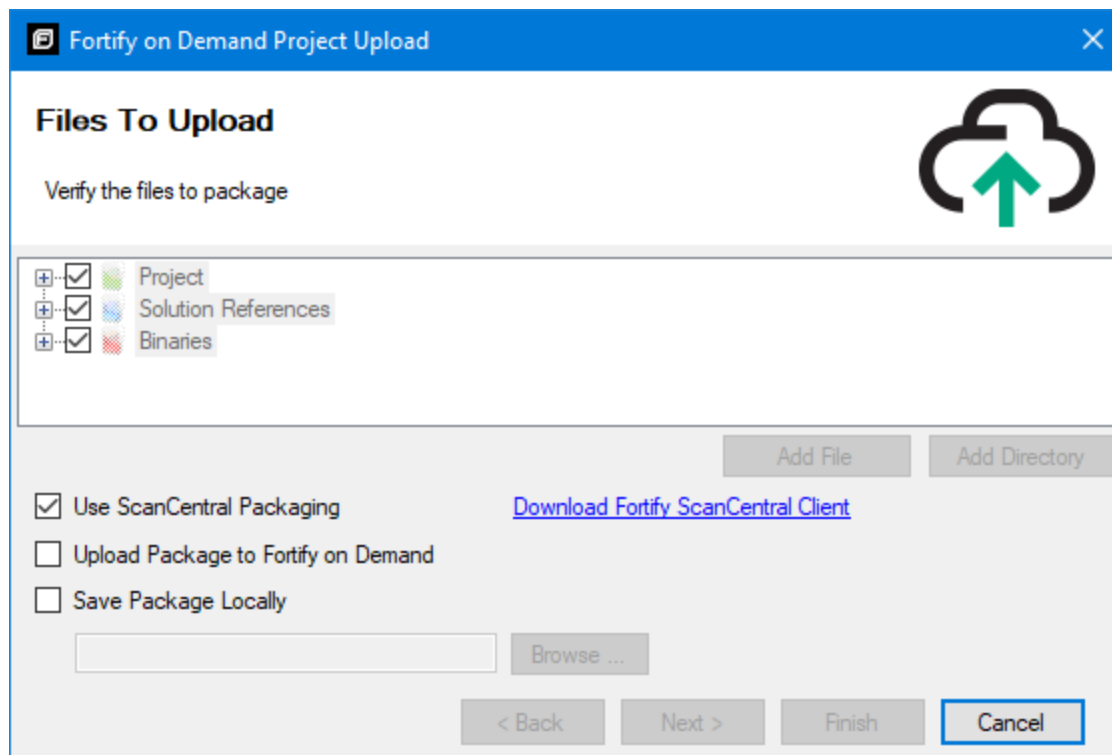
- A solution open in Visual Studio
- To include a Debricked open source scan for this solution, make sure your solution includes the file described in [Preparing Files for Open Source Scanning](#) before you upload the code to Fortify on Demand.

Additionally, in the following procedure, clear the **Use ScanCentral Packaging** check box and manually verify that all the files to package are selected including the required file prepared for open source scanning.

To upload source code to Fortify on Demand from Visual Studio:

1. From the Visual Studio Fortify extension menu, select **Upload Projects to Fortify on Demand**. The Fortify on Demand Project Upload wizard opens.

### **Files to Upload**

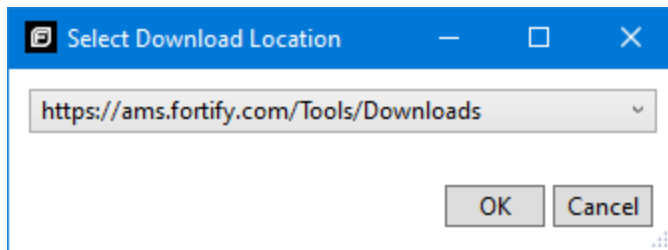


2. Select all the files you want to upload.

**Note:** These options are not available if you are using the Fortify ScanCentral client to automatically package the code.

- a. (Optional) To include a file that is not listed, click **Add File**, and then browse to and select a file to add to your package.  
The wizard now displays an **Extra Files** node and shows the full path to the file you added.
  - b. (Optional) To include a directory that is not listed, click **Add Directory**, and then browse to and select the directory to add to your package.  
The wizard now displays an **Extra Directories** node and shows the directory you added.
3. To automatically package the project with Fortify ScanCentral client, select **Use ScanCentral Packaging**.  
Fortify ScanCentral client can automatically package all the necessary dependencies and source code required for the scan.  
To use this feature, you must have a local copy of the Fortify ScanCentral client. To download the Fortify ScanCentral client from the Tools page:

- a. Click **Download Fortify ScanCentral Client**.



- b. Select a location from which to download the Fortify ScanCentral client and click **OK**.
- c. Log in to Fortify on Demand and download the Fortify ScanCentral Client utility from the Tools page.

For instructions on how to install the Fortify ScanCentral client, see the README.txt file included in the downloaded ZIP.

4. To upload the package to Fortify on Demand, select the **Upload Package to Fortify on Demand** check box.
5. To save the package to a local directory:
  - a. Select the **Save Package Locally** check box, click **Browse**, and then navigate to a folder where you want to save the package.
  - b. Click **Save**.
6. Click **Next**.

If this is the first time you selected **Use ScanCentral Packaging** to package your code and you have not configured the location of the Fortify ScanCentral client executable, do the following:

- a. In the Select Fortify ScanCentral executable dialog, navigate to the Fortify ScanCentral client executable file.
- b. Click **Open**.

If you did not select the **Upload Package Fortify on Demand** check box, the package is saved locally. Click **Finish**.

### Enter FoD Login Credentials

If you selected to upload the package, the **Enter FoD Login Credentials** page is displayed. If you have already logged in to Fortify on Demand, then the next step is to select an application and release (see "[Select a Release](#)" on page 329).

1. In the **API Root URL** box, type the API Root URL.  
To obtain this URL, see "[Fortify on Demand API](#)" on page 306 or contact a TAM.
2. Provide your login credentials. Use one of the two methods described in the following table.

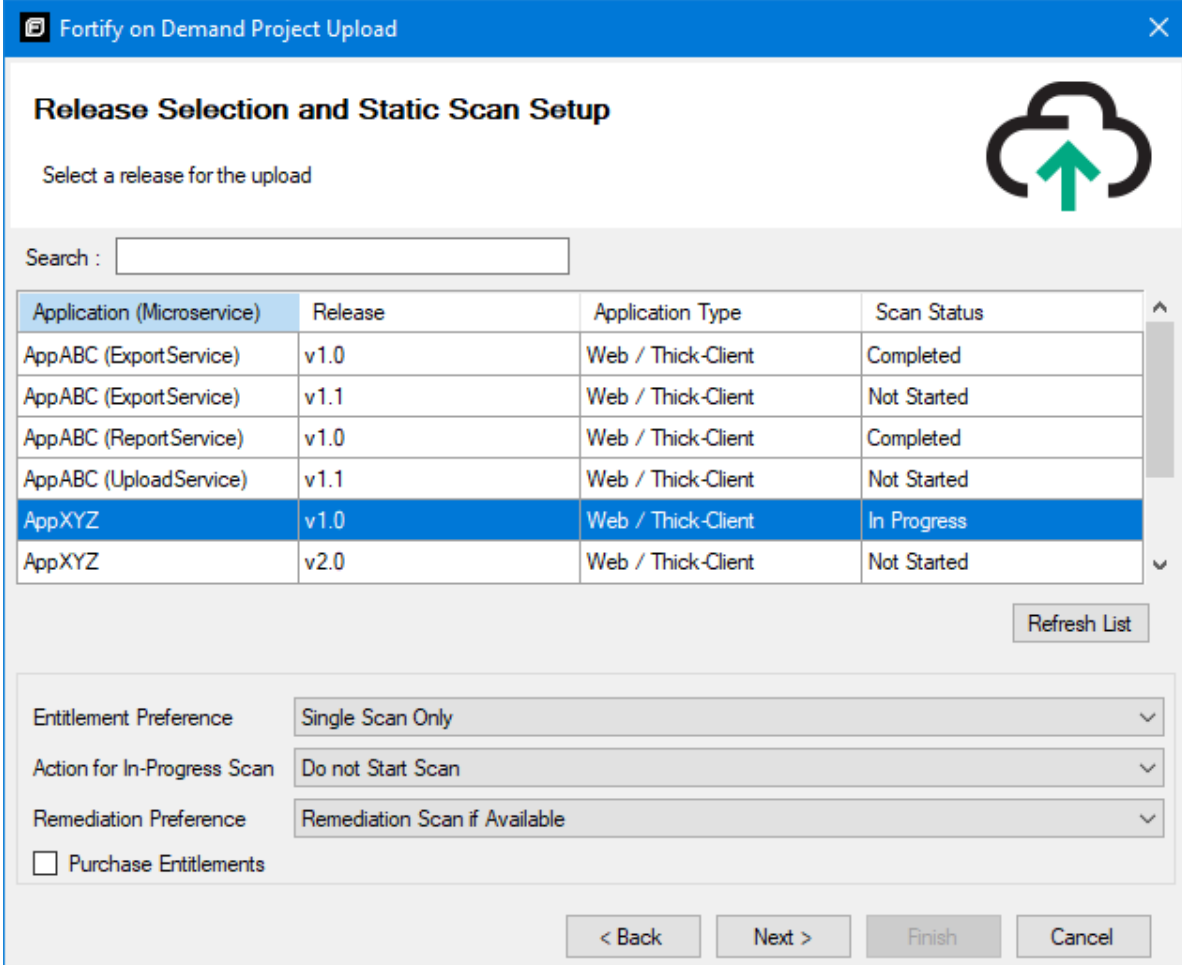
Login Method	Procedure
Provide your Fortify on Demand credentials.	a. Provide your <b>Username, Password,</b> and <b>Tenant ID</b> .

Login Method	Procedure
	<p>b. To save your credentials, select the <b>Remember Login Credentials</b> check box.</p> <div data-bbox="954 447 1403 590" style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> For security reasons, the Visual Studio extension does not save your password.</p> </div> <p>c. To configure your network preferences, click <b>Connection Settings</b>.</p>
<p>Use Single Sign On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.</p>	<p>a. Select <b>Use Identity Provider</b>.</p> <p>b. In the <b>SSO Login URL</b> box, type the URL provided by your Security Lead.</p> <p>c. To configure your network preferences, click <b>Connection Settings</b>.</p>

3. Click **Next**.
4. If your tenant requires two-factor authentication, then do the following:
  - a. Select a delivery method for the security code (**SMS** or **Email**), and click **OK**.
  - b. Obtain the security code delivered using the method you selected.
  - c. Enter the code in the **Security Code** box, and then click **OK**.  
The Visual Studio extension allows you three attempts to enter the security code. If necessary, click **Resend Code** to have a new security code sent to you.

## Select a Release

1. Select the application and release to which you want to upload.



The screenshot shows a dialog box titled "Fortify on Demand Project Upload" with a close button in the top right corner. The main heading is "Release Selection and Static Scan Setup". Below the heading is a sub-heading "Select a release for the upload" and a cloud icon with a green arrow pointing up. A search box is located below the sub-heading. A table with four columns (Application (Microservice), Release, Application Type, Scan Status) lists several application releases. The row for "AppXYZ v1.0" is highlighted in blue. Below the table is a "Refresh List" button. At the bottom, there are three dropdown menus for "Entitlement Preference" (Single Scan Only), "Action for In-Progress Scan" (Do not Start Scan), and "Remediation Preference" (Remediation Scan if Available). There is also a checkbox for "Purchase Entitlements". At the very bottom are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Application (Microservice)	Release	Application Type	Scan Status
AppABC (ExportService)	v1.0	Web / Thick-Client	Completed
AppABC (ExportService)	v1.1	Web / Thick-Client	Not Started
AppABC (ReportService)	v1.0	Web / Thick-Client	Completed
AppABC (UploadService)	v1.1	Web / Thick-Client	Not Started
AppXYZ	v1.0	Web / Thick-Client	In Progress
AppXYZ	v2.0	Web / Thick-Client	Not Started

To quickly find an application and release, type the name or partial name of an application or release in the **Search** box. The search is case-sensitive. To clear the search results, clear the **Search** box.

**Note:** To refresh the list of applications, click **Refresh List**.

2. Select an **Entitlement Preference** from the list.  
If multiple entitlements are available, the scan will use the oldest entitlement. If the release has an active subscription, the scan will use the active subscription.
3. From the **Action for In-Progress Scan** list, select what should happen if the selected release scan status is **In Progress**.  
You can choose to not start the scan, cancel the in-progress scan and start the new scan, or queue the new scan.
4. From the **Remediation Preference** list, select whether to run a remediation scan.
5. To purchase entitlements for this scan (if available), select the **Purchase Entitlements** check box.

6. Select the appropriate assessment type from the **Assessment Type** list.

**Note:** Steps 6 through 9 are only applicable if the selected release does not have scan settings configured yet. The fields described in these steps are hidden if the scan settings are already configured.

7. Specify the **Technology Stack** and the **Language Level**.  
Alternatively, you can click **Autodetect** and the technology stack and language level fields are automatically populated.
8. If you want open source libraries identified in the analysis (and if this feature is available), select the **Open Source Component Analysis** check box.  
This produces a report of identified open source components and known vulnerabilities using Sonatype.
9. To specify additional advanced scanning and auditing preferences, click **Advanced**.

Make selections for the options described in the following table.

Option	Description
Audit Preference	<p>This option is only available if enabled for your tenant.</p> <p>The audit preference settings are:</p> <ul style="list-style-type: none"> <li>• <b>Manual</b>—A security expert manually reviews the scan results and removes false positives</li> <li>• <b>Automated</b>—False positives identified by Fortify Scan Analytics with high confidence are automatically suppressed and results are published without manual review. This can reduce the turnaround time.</li> </ul>

Option	Description
Include third-party libraries for static security assessment	Authorizes Fortify on Demand to assess the code for vulnerabilities to include in reports, vulnerability count, and risk rating.  Selecting this option indicates that your organization has received consent from all third-party vendors to scan their libraries.

- Click **Next**.  
A status bar shows your upload progress.
- After the upload is complete, click **Finish**.  
Information about the IDE (name and version) used for this upload is saved and shown in the scan summary.

## Opening Analysis Results with the Visual Studio Extension

From Visual Studio, you can open Fortify on Demand analysis results for an application and release to remediate and audit.

**Note:** If you already have analysis results open, you can use this procedure to close the current analysis results and open the analysis results for a different application and release.

To open the analysis results:

- From the Visual Studio Fortify extension menu, select **Open Analysis Results**.  
The Fortify on Demand Open Analysis Results wizard opens.

### Enter FoD Login Credentials

**Note:** If you have already logged in to Fortify on Demand, then the next step is to select an application and release (see "[Select a Release](#)" on the next page).

- In the **API Root URL** box, type the API Root URL.  
To obtain this URL, see "[Fortify on Demand API](#)" on page 306 or contact a TAM.
- Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none"><li>Provide your <b>Username, Password, and Tenant ID</b>.</li><li>To save your credentials, select the <b>Remember Login Credentials</b> check box.</li></ol>

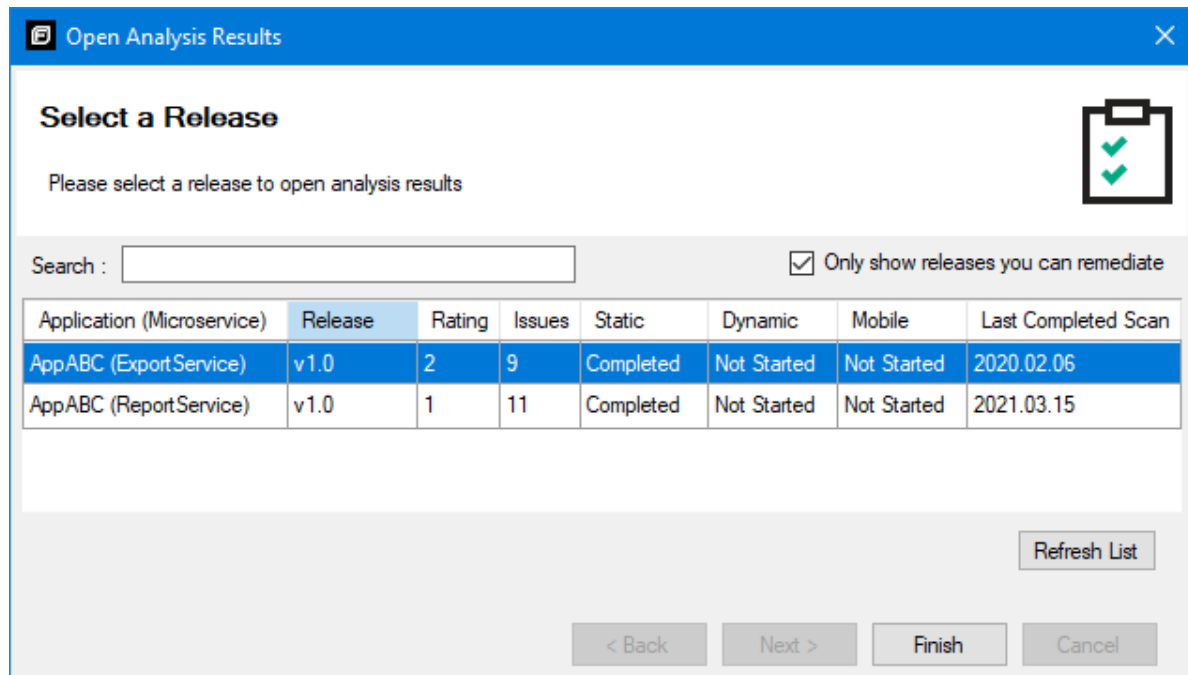
Login Method	Procedure
	<p><b>Note:</b> For security reasons, the Visual Studio extension does not save your password.</p> <p>c. To configure your network preferences, click <b>Connection Settings</b>.</p>
<p>Use Single Sign On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.</p>	<p>a. Select <b>Use Identity Provider</b>.</p> <p>b. In the <b>SSO Login URL</b> box, type the URL provided by your Security Lead.</p> <p>c. To configure your network preferences, click <b>Connection Settings</b>.</p>

3. Click **Next**.
4. If your tenant requires two-factor authentication, then do the following:
  - a. Select a delivery method for the security code (**SMS** or **Email**), and click **OK**.
  - b. Obtain the security code delivered using the method you selected.
  - c. Enter the code in the **Security Code** box, and then click **OK**.  
The Visual Studio extension allows you three attempts to enter the security code. If necessary, click **Resend Code** to have a new security code sent to you.

**Select a Release**



1. Select an application and release for the analysis results you want to open.



You can only open results for a release that has had at least one successfully completed scan. Clear the **Only show releases you can remediate** check box to see all applications and releases.

To quickly find an application and release, type the name or partial name of an application or release in the **Search** box. The search is case-sensitive. To clear the search results, clear the **Search** box.

**Note:** To refresh the list of applications, click **Refresh List**.

2. Click **Finish**.

The analysis results are displayed in the Fortify windows. See "[Analysis Results in the Visual Studio Extension](#)" below for a description of the Fortify windows.

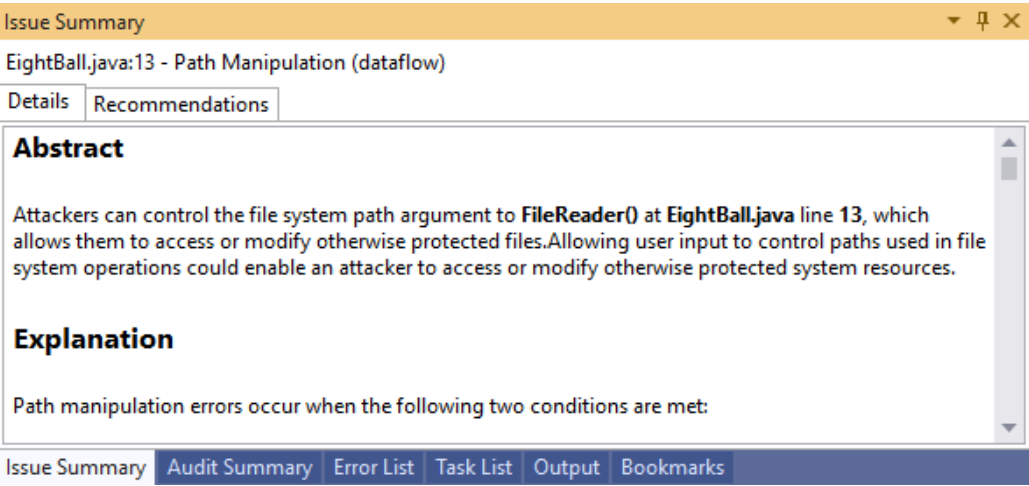
## Analysis Results in the Visual Studio Extension

After the analysis results are opened, the Visual Studio extension displays four audit-focused windows. The **Analysis Results** window displays the results. The **Analysis Trace**, **Issue Summary**, and **Audit Summary** windows are open, but do not contain any information until you select an issue from the **Analysis Results** window.

**Note:** To open a Fortify window that is not currently visible, select **Show Windows** from the Fortify extension menu and select the window you want to open.

The following table describes the Fortify windows.









Window	Description
Analysis Results	<p>The <b>Analysis Results</b> window provides a way to group and select the issues to audit.</p> <p>The color-coded tabs in the <b>Analysis Results</b> group the issues by severity level. The last tab contains all issues. The <b>Group By</b> list options sort the issues into subfolders. The option you select is applied to all visible folders.</p> <p><b>Note:</b> If you close this window, the analysis results are closed. To re-open analysis results, select <b>Open Analysis Results</b> from the Fortify extension menu.</p>
Analysis Trace	<p>The content of this window depends on the scan type:</p> <ul style="list-style-type: none"><li>• <b>Static Analysis Results</b>—After you select an issue in the <b>Analysis Results</b> window, the <b>Analysis Trace</b> window displays the relevant trace output. This is a set of program points that show how the analyzer found the issue. For dataflow and control flow issues, the set is presented in the order executed. For dataflow issues, this evidence is the path that the tainted data follows from the source function to the sink function. See the following descriptions of the analysis trace icons.</li><li>• <b>Dynamic Analysis Results</b>—After you select an issue in the <b>Analysis Results</b> view, the <b>Analysis Trace</b> view displays details about the request parameters.</li></ul> <p>This window also provides an abstract that briefly describes the issue.</p>
Issue Summary	<p>After you select an issue in the <b>Analysis Results</b> window, the <b>Issue Summary</b> window provides detailed information about the issue. The <b>Details</b> tab provides an abstract of the issue, a detailed explanation and might also include examples with descriptive text and code samples. The <b>Recommendations</b> tab displays recommendations to remediate the issue, along with tips and references for further research.</p>













Window	Description
	
Audit Summary	<p>After you select an issue in the <b>Analysis Results</b> window, the <b>Audit Summary</b> window displays audit information for the selected issue and you can edit the issue, add comments, and review the audit history. For more information, see <a href="#">"Auditing Issues from the Visual Studio Extension"</a> on page 337.</p>

The text editor window is where the Visual Studio extension displays the source code (if available) for static scans or the request and response details for dynamic scans. The text editor opens after you select an issue in the **Analysis Results** window.

## Analysis Trace Icons


The analysis trace icons described in the following table show how dataflow moves in the section of the source code or execution order.

Icon	Description	Icon	Description
	Data is assigned to a field or variable		Tainted data is returned from a function
	Information is read from a source external to the code such as an HTML form or a URL		A pointer is created
	Data is assigned to a globally scoped field or variable		A pointer is dereferenced
	A comparison is made		The scope of a variable ends

Icon	Description	Icon	Description
	The function call receives tainted data		The execution jumps
	The function call returns tainted data		A branch is taken in the code execution
	<p>Passthrough, tainted data passes from one place to another</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Note:</b> This is typically shown as <code>functionA(x : y)</code> to indicate that data is transferred from x to y. The x and y values are one of the following:</p> <ul style="list-style-type: none"> <li>• An argument index</li> <li>• <code>return</code>—The return value of a function</li> <li>• <code>this</code>—The instance of the current object</li> <li>• A specific object field or key</li> </ul> </div>		A branch is not taken in the code execution
	An alias is created for a memory location		Generic
	Data is read from a variable		A runtime source, sink, or validation step
	Data is read from a global variable		Taint change

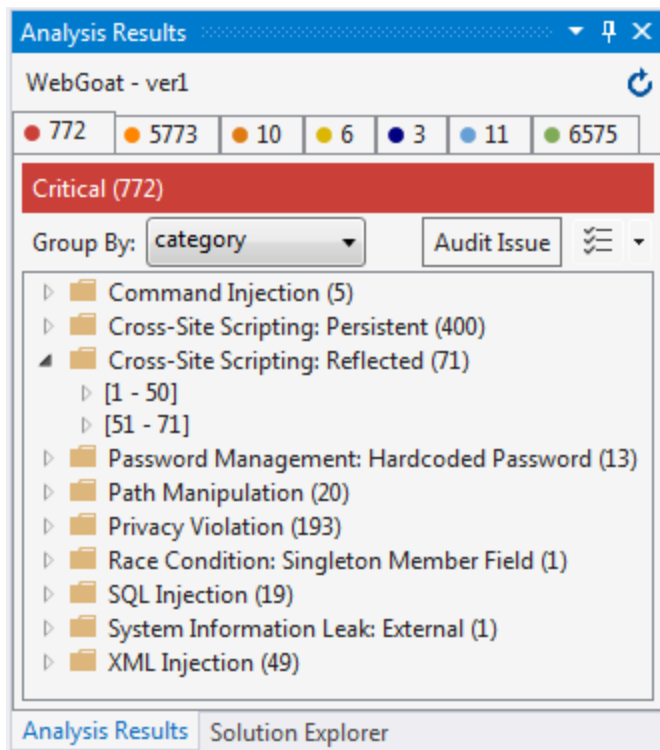
## Reviewing Issues from the Visual Studio Extension

To view and select issues:


1. From the **Group By** list, select a value to use to sort issues in all visible folders into groups. The default grouping is **category**.
2. Click a colored tab to view the associated issues. The issue type subfolders listed on each folder (tab) are based on the selected **Group By** value.
3. To show suppressed or fixed issues, click the  icon.

4. To view the list of issues in a subfolder, expand the subfolder.

The Visual Studio extension retrieves the corresponding issues from Fortify on Demand.



**Note:** If a folder contains more than 50 issues, the issues are grouped into subfolders in blocks of 50 with folder names that indicate which issues are included. For example, if a folder contains 71 issues, the first 50 issues are in a subfolder labeled **[1-50]** and the next set of issues are in a subfolder labeled **[51-71]**.

5. To see any updates to the analysis results made on Fortify on Demand, click **Refresh** .
6. Select an issue.

The **Analysis Trace**, **Issue Summary**, and **Audit Summary** windows display information about the selected issue.

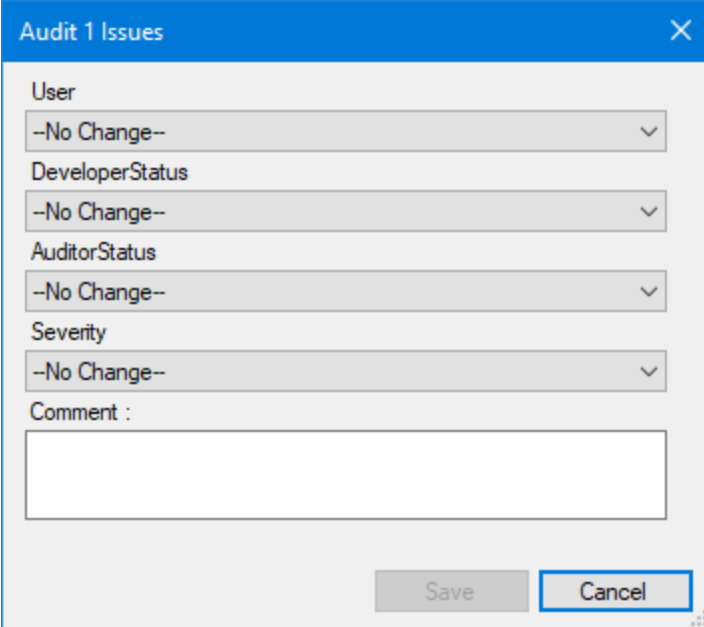
## Auditing Issues from the Visual Studio Extension

If you have the Edit Issues permission, you can assign a user, set the developer status, and add comments for issues in the **Audit Summary** window. If you have the Audit Issues permission, you can also edit an issue's auditor status and severity.

**Note:** You can edit one or more issues from the **Analysis Results** window or you can edit one selected issue in the **Audit Summary** window.

To audit an issue:

1. From the issues list in the **Analysis Results**, select the check box to the left of the issue.  
To make the same edit to multiple issues, select the check box to the left of each issue you want to audit.
2. Click **Audit Issue**.



The screenshot shows a dialog box titled "Audit 1 Issues". It features four dropdown menus for "User", "DeveloperStatus", "AuditorStatus", and "Severity", all currently set to "--No Change--". Below these is a text area for "Comment". At the bottom right, there are "Save" and "Cancel" buttons.

3. From the **User** list, select the user to assign to the issue.
4. To change the issue's development status, select the status from the **DeveloperStatus** list
5. To change the auditor status, select the status from the **AuditorStatus** list.
6. To change the issue severity, select an issue severity from the **Severity** list. For more information on issue severity, see ["Priority Order" on page 19](#).
7. To add a comment for the issue, type your comment in the **Comment** box.
8. Click **Save**.

The extension saves your changes for the application and release on the Fortify on Demand server.

## Locating the Source Code Associated with Static Scan Issues

You can use the Visual Studio extension to locate security-related issues in your code.

To jump to the line of source code that contains the issue selected in the Visual Studio extension:

1. Select an issue in the **Analysis Results** window or select a line in the **Analysis Trace** window.
2. If the source code is not available in the analysis results opened from Fortify on Demand, do the following:
  - a. In the Set Source Path dialog box, click **Browse**.
  - b. Select the location of the folder that contains the source code, and then click **OK**.
  - c. Click **OK** to close the Set Source Path dialog box.

The Visual Studio extension jumps to the line of code associated with the issue in a downloaded copy of the source code.

**Note:** If the source code is a downloaded copy from Fortify on Demand, the file name is `<original_filename> - Downloaded.<extension>`.

## Logging Out

To log out of Fortify on Demand:

- From the Visual Studio Fortify extension menu, select **Log Out of Fortify on Demand**.  
The analysis results are closed, and you are logged out from the Fortify on Demand server.

## Uninstalling the Visual Studio Extension

**Note:** These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To uninstall the Fortify on Demand Visual Studio extension:

1. In Visual Studio, access the dialog box to manage extensions.
2. Select **Fortify on Demand Extension for Visual Studio** and click **Uninstall**.
3. Click **Yes** to confirm the uninstall.
4. Click **Restart Now** to restart Visual Studio.

## Eclipse Plugin

Fortify on Demand provides the Eclipse plugin so that you can upload code for static analysis and open analysis results for remediation.

This section contains the following topics:

<a href="#">Installing the Eclipse Plugin</a>	340
<a href="#">Setting up Automatic Updates for the Eclipse Plugin</a>	342
<a href="#">Configuring the Eclipse Plugin</a>	343
<a href="#">Uploading Code with the Eclipse Plugin</a>	343
<a href="#">Opening Analysis Results with the Eclipse Plugin</a>	351
<a href="#">Analysis Results in the Eclipse Plugin</a>	354
<a href="#">Analysis Trace Icons</a>	355
<a href="#">Reviewing Issues from the Eclipse Plugin</a>	356

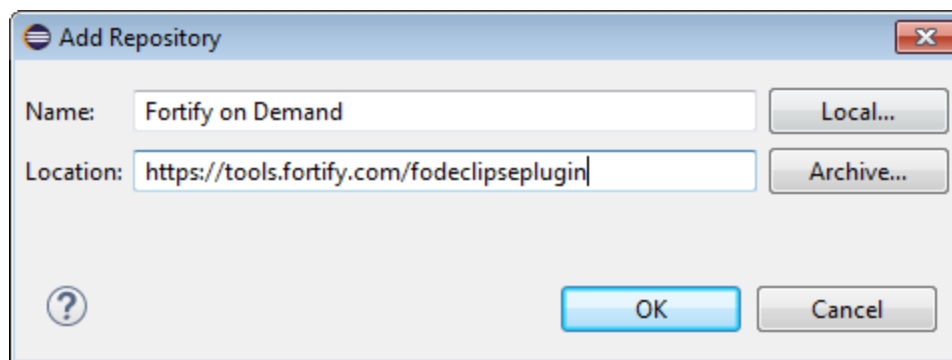
Auditing Issues from the Eclipse Plugin .....	357
Locating the Source Code Associated with Static Scan Issues .....	358
Closing Analysis Results .....	359

## Installing the Eclipse Plugin

You can obtain the Eclipse plugin directly from the Fortify on Demand server. The following instructions describe how to do this. Alternatively, you can download the plugin from the Eclipse Marketplace (<http://marketplace.eclipse.org>) and install it using the Eclipse Marketplace Client.

To install the Eclipse plugin:

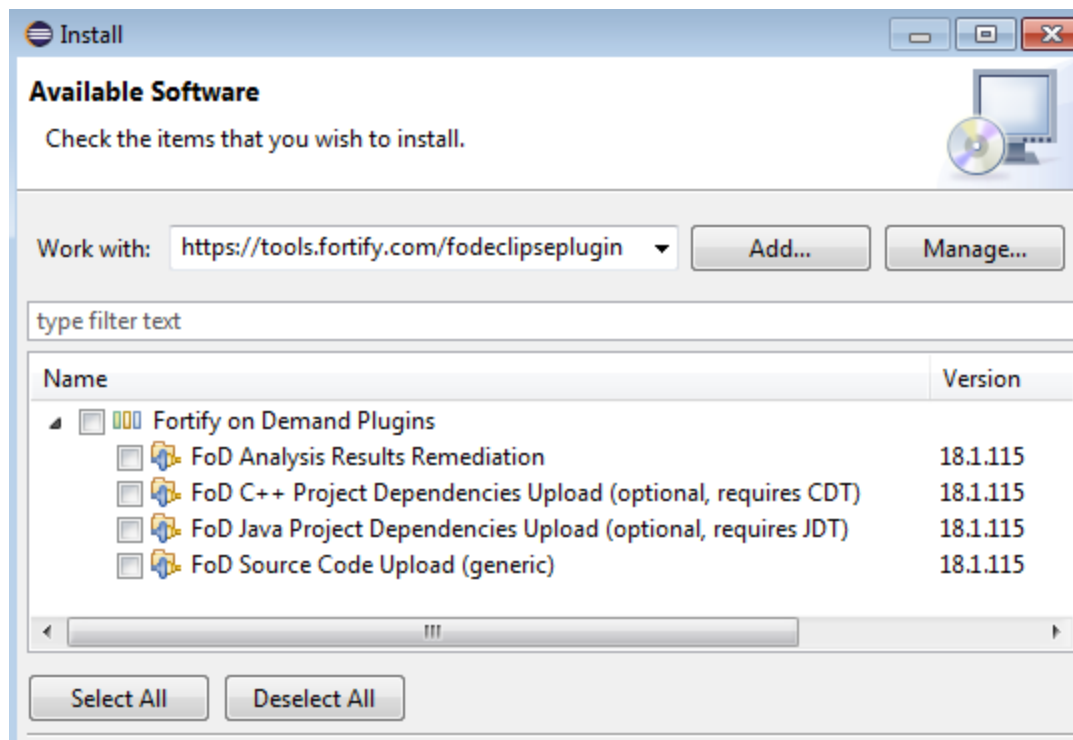
1. From Eclipse, select **Help > Install New Software**.  
The install wizard starts at the **Available Software** page.
2. Click **Add**.
3. (Optional) In the **Name** box, type a name for the update site.
4. In the **Location** box, type `https://tools.fortify.com/fodeclipseplugin`.



**Note:** You might need to configure a proxy in Eclipse to reach the location.

5. Click **OK**.  
The **Work with** box displays your new repository.
6. Expand the **Fortify on Demand Plugins** node.





7. Select one or more of the following the check boxes for the tools you want to install:
  - **FoD Analysis Results Remediation** enables you to review analysis results for an application and release so you can audit and remediate issues in your code.
  - **FoD C++ Project Dependencies Upload (optional, requires CDT)** automatically finds all included library references and adds them to your package. You do not need this tool if you do not use a CDT environment to create C++ projects in Eclipse. You may, however, install the plugin anyway. If you leave the **Contact all update sites during install to find required software** option selected, it automatically installs necessary libraries from the official Eclipse update site.
  - **FoD Java Project Dependencies Upload (optional, requires JDT)** automatically finds JAR files from your classpath library containers that reference JAR files outside of the workspace—such as JRE or libraries referenced from a Maven or Ivy repository— and includes them in the package. Note that this is done recursively for all dependent projects. Typically, you already have JDT installed, so Micro Focus recommends that you install this plugin. For example, if you use RAD you already have JDT.
  - **FoD Source Code Upload (generic)** enables you to package projects from your workspace. It finds project dependencies.
8. Click **Next**.

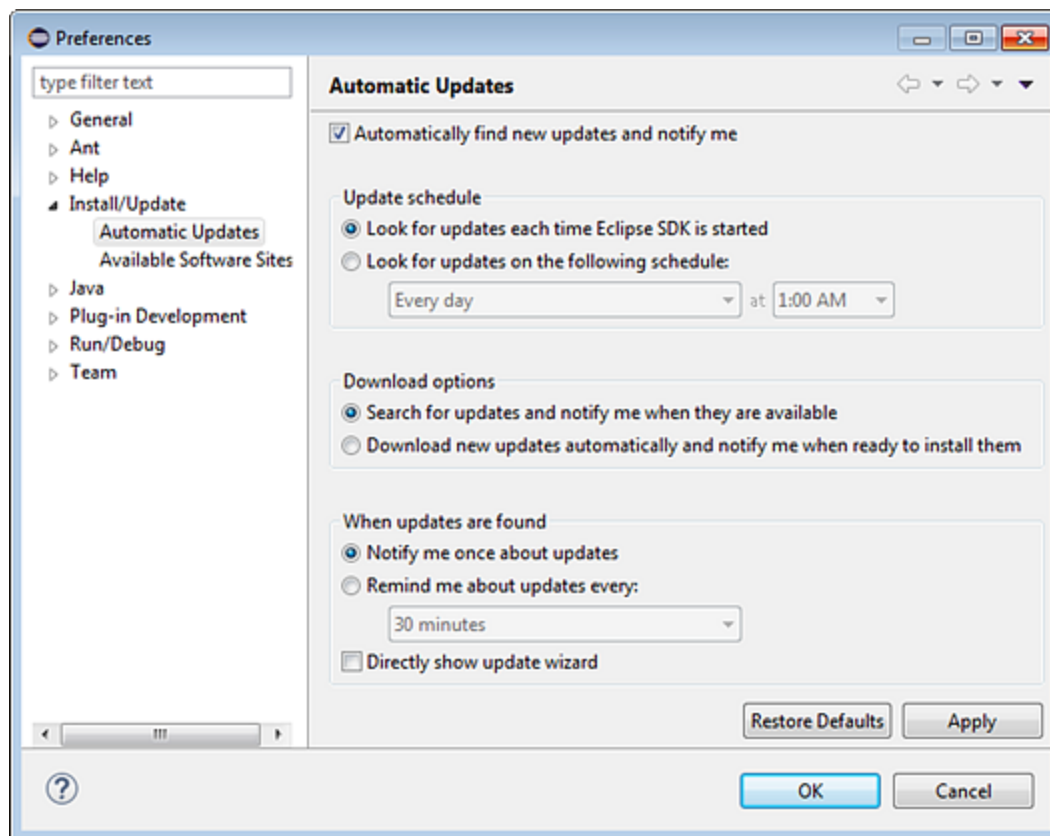
The install wizard lists the items to be installed.
9. Click **Next**.
10. Read the **End User License Agreement**, and then select **I accept the terms of the license agreement**.
11. Click **Finish**.

12. When the installer prompts you to restart Eclipse, click **Yes**.  
The Eclipse menu bar now includes the **Fortify** menu.

## Setting up Automatic Updates for the Eclipse Plugin

To set up an automatic update notification in Eclipse:

1. Open the **Eclipse Preferences** dialog.  
If you need help with this, see the **Eclipse Help**.
2. Select **Available Software Sites**, and make sure that the Fortify on Demand update site <https://tools.fortify.com/fodeclipseplugin> is selected.
3. Select **Automatic Updates**, and then select the **Automatically find new updates and notify me** check box.



4. Select the notification options you want.  
If an update is available, you will see a notification icon in the tray at the bottom of the Eclipse window.

## Configuring the Eclipse Plugin

You can configure options for uploading source code and for communicating with Fortify on Demand at any time.

To configure Eclipse plugin options:

1. From the Eclipse menu bar, select **Fortify > Configure Fortify on Demand Plugin**.
2. To change the amount of time to wait for communicating with Fortify on Demand before giving up, type the time in seconds in the **HTTP Timeout** box.

Valid values for HTTP timeout are 0 through 21600 (6 hours). A value of 0 indicates that there is no timeout. The default HTTP timeout is 120 seconds (2 minutes).

3. To change the size of the individual pieces that is uploaded to Fortify on Demand, type the size in kilobytes in the **Upload Chunk Size** box.

The packaged source code is uploaded in chunks for optimal performance and reliability. The valid chunk size values are 1 through 10000 Kb. To upload a large file with a stable connection, you can specify larger chunks sizes. To upload a small file with a connection that is not as reliable (for example, a wireless connection), use the default chunk size of 64 Kb or smaller.

4. To enable the plugin to accept any server certificate, select the **Disable SSL Validation** check box.

**Note:** For security reasons, selecting this option is not recommended.

5. Click **OK**.

## Uploading Code with the Eclipse Plugin

Before you start, make sure you have the following:

- Your Fortify on Demand login credentials

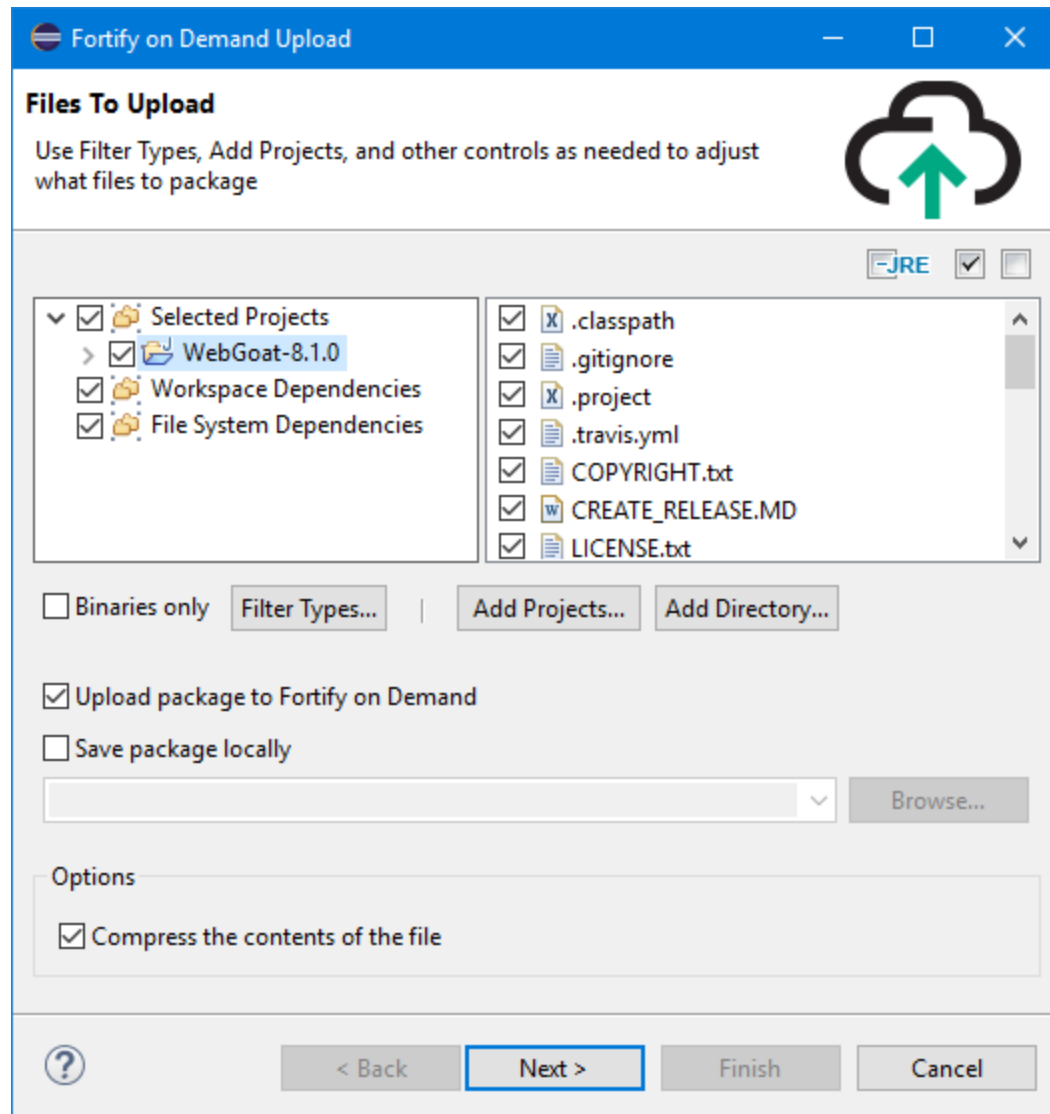
**Note:** To upload your code, you must have the Start Static Scan permission.

- One or more projects open in Eclipse

To upload source code to Fortify on Demand from Eclipse:

1. In Eclipse, select **Fortify > Upload Projects to Fortify on Demand**.  
The Fortify on Demand Upload wizard opens.

### Files to Upload (page 1 of 3)



In the left panel, the tree view lists the following items:

- **Selected Projects**—Projects and folders you selected for upload
- **Workspace Dependencies**—Dependent projects that were detected and added automatically
- **File System Dependencies**—Dependent Java and C++ libraries that are not in the workspace  
These libraries are typically needed to scan your code correctly. Micro Focus recommends that you include them in your package.

The right panel displays the files contained in the folder selected in the left panel.

2. To refine the items to upload, perform one or more of the procedures described in the following table.

<b>Item Upload Refinement</b>	<b>Procedure</b>
Remove JRE files from the upload package.	<ul style="list-style-type: none"> <li>• Click <b>-JRE</b>.</li> </ul>
Omit specific files located in an item listed in the tree view.	<ol style="list-style-type: none"> <li>a. Select an item in the tree view.</li> <li>b. Clear the check boxes for the files you want exclude from your upload package.</li> </ol>
Upload only binary files (EAR, EXE, CLASS, DLL, JAR, and WAR files).	<ul style="list-style-type: none"> <li>• Select the <b>Binaries only</b> check box.</li> </ul>
Upload only specific file types.	<ol style="list-style-type: none"> <li>a. Click <b>Filter Types</b>.</li> <li>b. In the Select Types dialog box, select the check boxes for the file types that you want to upload.</li> <li>c. To include file types not listed, in the <b>Other extensions</b> box, type the extensions for any additional file types to upload. If you want to list more than one extension, separate them with commas.</li> <li>d. Click <b>OK</b>.</li> </ol> <p>The extensions you select are displayed under the <b>Filter Types</b> button.</p>
Upload one or more additional projects.	<ol style="list-style-type: none"> <li>a. Click <b>Add Projects</b>.</li> <li>b. In the Folder Selection dialog box, navigate to and select the additional project to upload and click <b>OK</b>.</li> </ol>
Upload additional external resources.	<ol style="list-style-type: none"> <li>a. Click <b>Add Directory</b>.</li> <li>b. In the Browse for Folder dialog box, navigate to and select the resources to upload, and then click <b>OK</b>.</li> </ol> <p>After you add a folder, you can select specific files within it.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>◦ Subfolders are included.</li> </ul> </div>

Item Upload Refinement	Procedure
	<ul style="list-style-type: none"><li>○ Folders with native Unicode symbols in them are not supported.</li></ul>

3. To upload the package to your Fortify on Demand server, leave the **Upload package to Fortify on Demand** check box selected.
4. To save the package to a local directory, select the **Save package locally** check box and then do the following:
  - a. Click **Browse** and then navigate to and select a local folder.
  - b. Type a name for the package, and then click **Save**.
5. To reduce the size of the package, leave the **Compress the contents of the file** check box selected.

Although this reduces the size of the package to be uploaded, the packaging process takes longer.
6. Do one of the following:
  - If you selected the **Save package locally** check box and cleared the **Upload package to Fortify on Demand** check box, click **Finish**.
  - To upload the package to your Fortify on Demand server, click **Next** to proceed to the **Fortify on Demand Login Credentials** page.

### Fortify on Demand Login Credentials (page 2 of 3)

Fortify on Demand Upload

### Fortify on Demand Login Credentials

No username specified  
No tenant specified

API Root URL:

[Clear Portal History](#)

Fortify on Demand Credentials

Username:

Password:

Tenant ID:

Use Identity Provider

SSO Login URL:

Remember Login Credentials

[Configure Network Connection](#)

1. In the **API Root URL** box, type an API Root URL.  
To obtain this URL, see ["Fortify on Demand API" on page 306](#) or contact a TAM.
2. Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none"><li>a. Provide your <b>Username, Password, and Tenant ID.</b></li><li>b. To save your credentials, select the <b>Remember Login Credentials</b> check box. <div style="background-color: #f0f0f0; padding: 5px;"><b>Note:</b> For security reasons, the Eclipse plugin does not save your password.</div></li><li>c. To configure your network preferences, click <b>Configure Network Connection</b>, and then follow the instructions provided by Eclipse help.</li></ol>

Login Method	Procedure
	<p><b>Note:</b> If your organization uses the NTLM proxy, specify a domain\user name instead of only a user name for authentication. Instead of using the <b>Native</b> provider option in Eclipse, Micro Focus suggests that you use the <b>Manual</b> option and specify your data manually.</p>
<p>Use Single Sign-On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.</p>	<ol style="list-style-type: none"> <li>a. Select <b>Use Identity Provider</b>.</li> <li>b. In the <b>SSO Login URL</b> box, type the URL provided by your Security Lead.</li> <li>c. To configure your network preferences, click <b>Configure Network Connection</b>, and then follow the instructions provided by Eclipse help.</li> <li>d. Provide your proxy information.</li> </ol> <p><b>Note:</b> For Linux platforms, you might need to provide your proxy information in the <code>eclipse.ini</code> file. Add the following two lines at the end of the file:</p> <pre>-Dnetwork.proxy_host=&lt;proxyhost&gt; -Dnetwork.proxy_port=&lt;port&gt;</pre> <p>Restart Eclipse.</p> <p>For more information, see <a href="http://www.eclipse.org/swt/faq.php#browserproxy">http://www.eclipse.org/swt/faq.php#browserproxy</a>.</p>

3. Click **Next**.
4. If your tenant requires two-factor authentication, then do the following:
  - a. In the Two-Step Verification dialog box, select a delivery method for the security code (**SMS** or **Email**) and click **OK**.
  - b. After you obtain the security code delivered using the method you selected, type the code in the **Security Code** box and click **OK**.

The plugin allows you three attempts to provide the security code. If necessary, click **Resend Code** to have a new security code sent to you.



### Release Selection and Static Scan Setup (page 3 of 3)


1. Select the application and release for your upload package.

The screenshot shows a window titled "Fortify on Demand Upload" with a sub-header "Release Selection and Static Scan Setup". Below the sub-header is a description: "Specify Entitlement Preference, Action for In-Progress Scan, Remediation Preference, and the Entitlement Purchase selection for this package". To the right of the description is a cloud icon with a green arrow pointing up. Below this is a search box with the label "Search:" and three icons: a green plus sign, a yellow double arrow, and a yellow dollar sign. Below the search box is a table with four columns: "Application (Microservice)", "Release", "Application Type", and "Scan Status". The table contains five rows of data. Below the table are three dropdown menus for "Entitlement Preference", "Action For In-Progress Scan", and "Remediation Preference". There is also a checkbox for "Purchase Entitlements" and a checkbox for "Upload in background". At the bottom of the dialog are buttons for "< Back", "Next >", "Finish", and "Cancel".


Application (Microservice)	Release	Application Type	Scan Status
AppABC (ExportService)	v1.0	Web_Thick_Client	Canceled
AppABC (ExportService)	v1.1	Web_Thick_Client	Not Started
AppABC (ReportService)	v1.0	Web_Thick_Client	Canceled
AppABC (UploadService)	v1.1	Web_Thick_Client	Not Started

If you have permission, you can create a new release for an existing application.

To quickly find an application and release, type the name or partial name of an application or release in the **Search** box and press **Enter**. The search is case-insensitive. To clear the search results, clear the **Search** box, and then press **Enter**.

**Note:** To refresh the list of applications, click **Refresh** .

To create a new release for an existing application:

- a. Click **Create New Release** .
- The Create a Release dialog box opens.
- b. Select an application from the **Application** list.
- c. In the **Release Name** box, type a unique name for the release.  
Valid characters include letters, digits, underscores, and spaces.

- d. (Optional) Type a description for the new release.
  - e. From the **SDLS Status** list, select the Software Development Lifecycle.
  - f. Select **Copy State from Existing Release** to copy vulnerabilities and other details from a previous release to the new one, and then select the release that you want to copy from the list.
  - g. Click **OK**.
2. Select an **Entitlement Preference** from the list.  
If multiple entitlements are available, the scan will use the oldest entitlement. If the release has an active subscription, the scan will use the active subscription.
  3. From the **Action for In-Progress Scan** list, select what should happen if the selected release scan status is **In Progress**.  
You can choose to not start the scan, cancel the in-progress scan and start the new scan, or queue the new scan.
  4. From the **Remediation Preference** list, select whether to run a remediation scan.
  5. To purchase entitlements for this scan (if available), select the **Purchase Entitlements** check box.
  6. Select an assessment type from the **Assessment Type** list.

**Note:** Steps 6 through 9 (shown under **Static Scan Details**) are only applicable if the selected release does not have scan settings configured yet. The fields described in these steps are hidden if the scan settings are already configured.

Static Scan Details

999865 Unit(s) Available

Assessment Type: Static Assessment - Subscription (4 Units)

[Autodetect](#)

Technology Stack: JAVA/J2EE

Language Level: 11

Open Source Component Analysis

▶ Advanced

To upload your project, you must select an assessment type that is less than or equal to the entitlements that you have available.

7. Specify the **Technology Stack** and the **Language Level**.  
These fields display the values automatically detected for the selected Eclipse project. The **Autodetect** command can identify Java, C/C++, PYTHON, Ruby, and CFML projects. If you have previously used the Eclipse plugin, the technology stack and language level that you used previously are restored.

8. If you want open source libraries for Java and .NET applications identified in the analysis (and if this feature is available), select the **Open Source Component Analysis** check box.

This produces a report of identified open source components and known vulnerabilities using Sonatype.

9. To specify additional advanced scanning and auditing preferences, click **Advanced**, and then make selections for the options described in the following table.

Option	Description
Audit Preference	This option is only available if enabled for your tenant. The audit preference settings are: <ul style="list-style-type: none"><li>• <b>Manual</b>—A security expert manually reviews the scan results and removes false positives</li><li>• <b>Automated</b>—False positives identified by Fortify Scan Analytics with high confidence are automatically suppressed and results are published without manual review. This can reduce the turnaround time.</li></ul>
Include third-party libraries for static security assessment	Authorizes Fortify on Demand to assess the code for vulnerabilities to include in reports, vulnerability count, and risk rating. Selecting this option indicates that your organization has received consent from all third-party vendors to scan their libraries.

10. To upload your package in the background, leave the **Upload in background** check box selected.

**Note:** Packaging the contents occurs in the foreground, but the upload is performed in the background.

11. Click **Finish** to upload your code to Fortify on Demand.

Information about the IDE (name and version) used for this upload is saved and shown in the scan summary.

## Opening Analysis Results with the Eclipse Plugin

From the Eclipse IDE, you can open Fortify on Demand analysis results for an application and release to remediate and audit.

**Note:** If you already have analysis results open, you can use this procedure to close the current analysis results and open the analysis results for a different application and release.

To open the analysis results:

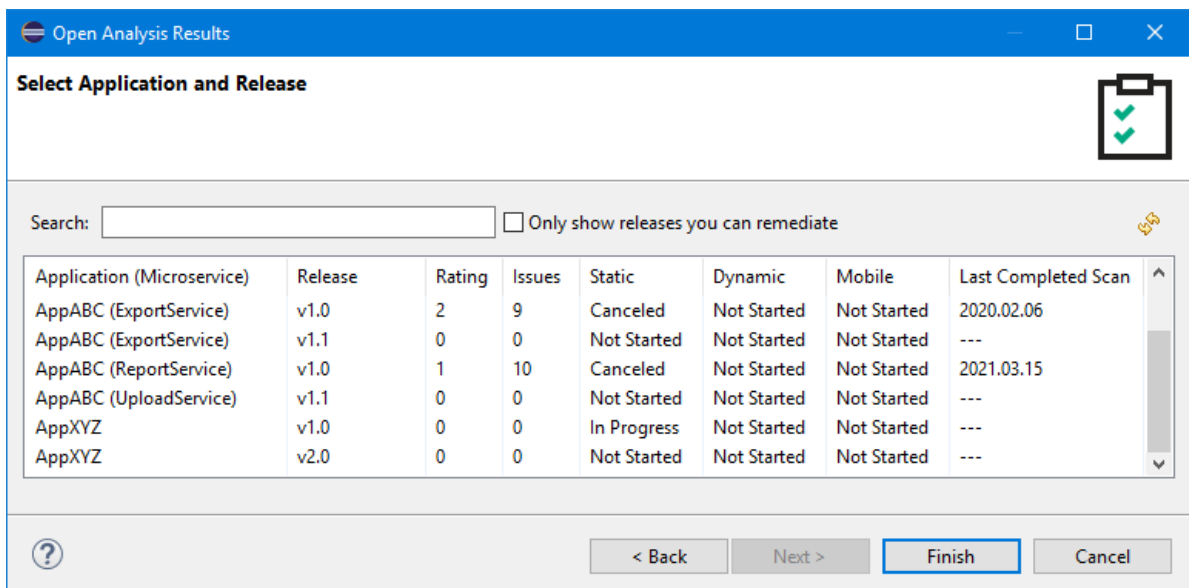
1. In Eclipse, select **Fortify > Open Analysis Results**.  
The Fortify on Demand Open Analysis Results wizard opens.
2. In the **API Root URL** box, type an API Root URL.  
To obtain this URL, see "[Fortify on Demand API](#)" on page 306 or contact a TAM.
3. Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
<p>Provide your Fortify on Demand credentials.</p>	<ol style="list-style-type: none"> <li>a. Provide your <b>Username, Password, and Tenant ID</b>.</li> <li>b. To save your credentials, select the <b>Remember Login Credentials</b> check box.                             <div data-bbox="646 684 1401 785" style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> For security reasons, the Eclipse plugin does not save your password.</p> </div> </li> <li>c. To configure your network preferences, click <b>Configure Network Connection</b>, and then follow the instructions provided by Eclipse help.                             <div data-bbox="646 947 1401 1171" style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> If your organization uses the NTLM proxy, specify a domain\user name instead of only a user name for authentication. Instead of using the <b>Native</b> provider option in Eclipse, Micro Focus suggests that you use the <b>Manual</b> option and specify your data manually.</p> </div> </li> </ol>
<p>Use Single Sign-On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.</p>	<ol style="list-style-type: none"> <li>a. Select <b>Use Identity Provider</b>.</li> <li>b. In the <b>SSO Login URL</b> box, type the URL provided by your Security Lead.</li> <li>c. To configure your network preferences, click <b>Configure Network Connection</b>, and then follow the instructions provided by Eclipse help.</li> <li>d. Provide your proxy information.                             <div data-bbox="646 1535 1401 1866" style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> For Linux platforms, you might need to provide your proxy information in the <code>eclipse.ini</code> file. Add the following two lines at the end of the file:</p> <pre style="margin: 0;">-Dnetwork.proxy_host=&lt;proxyhost&gt; -Dnetwork.proxy_port=&lt;port&gt;</pre> <p>Restart Eclipse.</p> <p>For more information, see</p> </div> </li> </ol>


Login Method	Procedure
	<a href="http://www.eclipse.org/swt/faq.php#browserproxy">http://www.eclipse.org/swt/faq.php#browserproxy</a> .

4. Click **Next**.
5. If your tenant requires two-factor authentication, then do the following:
  - a. In the Two-Step Verification dialog box, select a delivery method for the security code (**SMS** or **Email**) and click **OK**.
  - b. After you obtain the security code delivered using the method you selected, type the code in the **Security Code** box and click **OK**.

The plugin allows you three attempts to provide the security code. If necessary, click **Resend Code** to have a new security code sent to you.
6. Select an application and release for the analysis results you want to open.



You can only open results for a release that has had at least one successfully completed scan. Clear the **Only show releases you can remediate** check box to see all applications and releases. To quickly find an application and release, type the name or partial name of an application or release in the **Search** box and press **Enter**. The search is case-insensitive. To clear the search results, clear the **Search** box, and then press **Enter**.

**Note:** To refresh the list of applications, click **Refresh** .

7. Click **Finish**.

The analysis results are displayed in the Fortify perspective. See "[Analysis Results in the Eclipse Plugin](#)" on the next page for a description of this perspective.

## Analysis Results in the Eclipse Plugin

After the analysis results are opened, the Fortify perspective displays four audit-focused views. The **Analysis Results** view displays the results. The **Analysis Trace**, **Audit Summary**, and **Issue Summary** views are open, but do not contain any information until you select an issue from the **Analysis Results** view. You can also open audit-related views in other perspectives, such as the Java perspective or the C/C++ perspective, and rearrange the views. You might decide to use the audit views only, and stay within a customized development perspective.

**Note:** To open a Fortify view that is not currently visible, select **Fortify > Show View** and select the view you want to open.

The following table describes the Fortify perspective views.

View	Description
Analysis Results	<p>The <b>Analysis Results</b> view provides a way to group and select the issues to audit. This view also displays the relevant trace output for issues (see the following description of the <b>Analysis Trace</b> view).</p> <p>The color-coded tabs in the <b>Analysis Results</b> group the issues by severity level. The last tab contains all issues. The <b>Group By</b> list options sort the issues into subfolders. The option you select is applied to all visible folders.</p> <p><b>Note:</b> If you close this view, the analysis results are closed. To re-open analysis results, select <b>Fortify &gt; Open Analysis Results</b>.</p>
Analysis Trace	<p><b>For Static Analysis Results</b>—After you select an issue in the <b>Analysis Results</b> view, the <b>Analysis Trace</b> view displays the relevant trace output. This is a set of program points that show how the analyzer found the issue. For dataflow and control flow issues, the set is presented in the order executed. For dataflow issues, this evidence is the path that the tainted data follows from the source function to the sink function. See the following descriptions of the analysis trace icons.</p> <p><b>For Dynamic Analysis Results</b>—After you select an issue in the <b>Analysis Results</b> view, the <b>Analysis Trace</b> view displays details about the request parameters.</p> <p>This view also provides an abstract that briefly describes the issue.</p>
Audit Summary	<p>After you select an issue in the <b>Analysis Results</b> view, the <b>Audit Summary</b> view displays audit information for the selected issue. You can edit issue information, add comments, and review the audit history. For more information, see <a href="#">"Auditing Issues from the Eclipse Plugin" on page 357</a>.</p>







View	Description
Issue Summary	After you select an issue in the <b>Analysis Results</b> view, the <b>Issue Summary</b> view provides detailed information about the issue. The <b>Details</b> tab provides an abstract of the issue, a detailed explanation, and might also include examples with descriptive text and code samples, and the scan type (static, dynamic, or mobile). The <b>Recommendations</b> tab displays recommendations to remediate the issue, along with tips and references for additional research.

The Eclipse text editor view is where the Eclipse plugin displays the source code (if available) for static scans or the request and response details for dynamic scans. The text editor opens after you select an issue in the **Analysis Results** view.

### Analysis Trace Icons


The analysis trace icons described in the following table show how dataflow moves in the section of the source code or execution order.

Icon	Description	Icon	Description
	Data is assigned to a field or variable		Tainted data is returned from a function
	Information is read from a source external to the code such as an HTML form or a URL		A pointer is created
	Data is assigned to a globally scoped field or variable		A pointer is dereferenced
	A comparison is made		The scope of a variable ends
	The function call receives tainted data		The execution jumps
	The function call returns tainted data		A branch is taken in the code execution
	Passthrough, tainted data passes from one place to another  <b>Note:</b> This is typically shown as <code>functionA(x : y)</code> to indicate that data is transferred from x to y.		A branch is not taken in the code execution

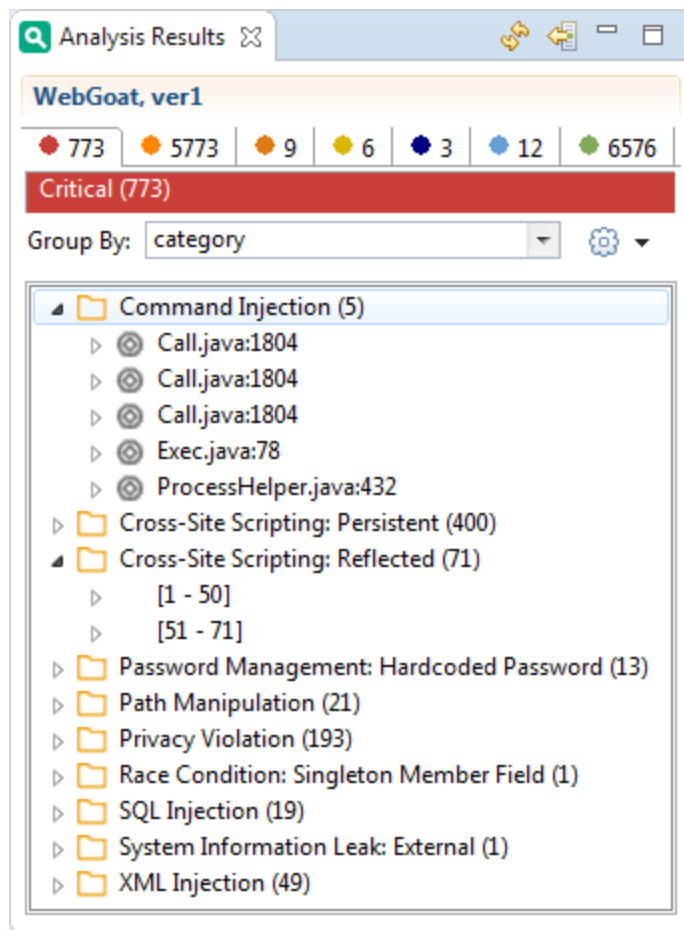
Icon	Description	Icon	Description
	<p>The x and y values are one of the following:</p> <ul style="list-style-type: none"> <li>• An argument index</li> <li>• <code>return</code>—The return value of a function</li> <li>• <code>this</code>—The instance of the current object</li> <li>• A specific object field or key</li> </ul>		
	An alias is created for a memory location		Generic
	Data is read from a variable		A runtime source, sink, or validation step
	Data is read from a global variable		Taint change

## Reviewing Issues from the Eclipse Plugin

To view and select issues:


1. From the **Group By** list, select a value to use to sort issues in all visible folders into groups. The default grouping is **category**.
2. Click a colored tab to view the associated issues.  
The issue type subfolders listed on each folder (tab) are based on the selected **Group By** value.
3. To show suppressed or fixed issues, click the  icon.
4. To view the list of issues in a subfolder, expand the subfolder.  
The Eclipse plugin retrieves the corresponding issues from Fortify on Demand.





#### Notes:

- If a folder contains more than 50 issues, the issues are grouped into subfolders in blocks of 50 with folder names that indicate which issues are included. For example, if a folder contains 71 issues, the first 50 issues are in a subfolder labeled **[1-50]** and the next set of issues are in a subfolder labeled **[51-71]**.
- Multiple trace paths for a single issue are shown in separate **Trace <num>** subfolders.

5. To see any updates to the analysis results made on Fortify on Demand, click **Refresh** .
6. Select an issue.

The **Analysis Trace**, **Audit Summary**, and **Issue Summary** views display information about the selected issue.

## Auditing Issues from the Eclipse Plugin

If you have the Edit Issues permission, you can assign a user, set the developer status, and add comments for issues in the **Audit Summary** view. If you have the Audit Issues permission, you can also edit the issue's auditor status and severity.

To audit an issue:

1. Make sure that the **Audit Summary** view is open.
2. From the issues list in the **Analysis Results**, select an issue.  
You can select multiple issues in the **Analysis Results** view to make the same edits to multiple issues.
3. In the **Audit Summary** view, select the user to assign to the issue from **User** list.
4. To change the issue's development status, select the status from the **DeveloperStatus** list
5. To change the auditor status, select the status from the **AuditorStatus** list.
6. To change the issue severity, select an issue severity from the **Severity** list. For more information on issue severity, see ["Priority Order" on page 19](#).
7. To add a comment for the issue, type your comment in the box at the bottom of the **Comments** area, and then click **Add Comment**.  
Your comment is displayed in the **Comments** section.

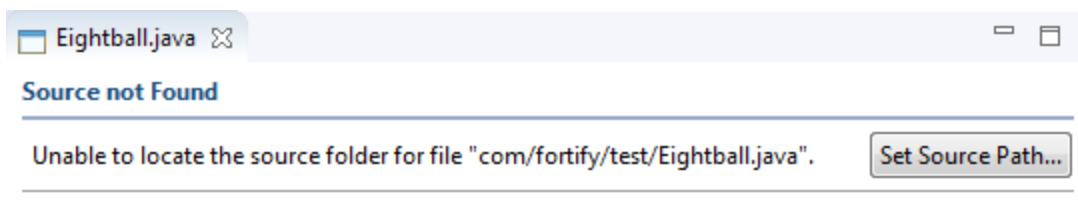
The plugin saves your changes for the application and release on the Fortify on Demand server.

## Locating the Source Code Associated with Static Scan Issues

You can use the Eclipse plugin to locate security-related issues in your code.

To jump to the line of source code that contains the issue selected in the Eclipse plugin:

1. Select an issue in the **Analysis Results** view or select a line in the **Analysis Trace** view.
2. If the source code is not available in the analysis results opened from Fortify on Demand, do the following:



- a. In the Text Editor, click **Set Source Path**.
- b. In the Set Source Path dialog box, click **Browse**.
- c. Select the location of the folder that contains the source code, and then click **OK**.
- d. Click **OK** to close the Set Source Path dialog box.

Eclipse highlights the line of code associated with the issue.

**Note:** If the source code shown is a downloaded copy from Fortify on Demand, the file name is prepended with `Remote<yyyy-mm-dd>` - where the `<yyyy-mm-dd>` is the date the file was last scanned. The downloaded copy is not writable.

## Closing Analysis Results

To close the analysis results for an application and release:

- In the **Analysis Results** view, click the  icon.

The analysis results are closed and you are logged out from the Fortify on Demand server.

## IntelliJ Plugin

Fortify on Demand provides the IntelliJ plugin so that you can upload code for static analysis and open analysis results for remediation.

**Note:** This plugin works with Android Studio and other JetBrains IDEs as listed in the JetBrains Marketplace. The procedures in this section reference the IntelliJ IDEA interface and the instructions might be slightly different for the other IDEs.

This section contains the following topics:

<a href="#">Installing the IntelliJ Plugin</a>	359
<a href="#">Configuring the IntelliJ Plugin</a>	360
<a href="#">Uploading Code with the IntelliJ Plugin</a>	360
<a href="#">Opening Analysis Results with the IntelliJ Plugin</a>	367
<a href="#">Analysis Results in the IntelliJ Plugin</a>	368
<a href="#">Analysis Trace Icons</a>	370
<a href="#">Reviewing Issues from the IntelliJ Plugin</a>	371
<a href="#">Auditing Issues from the IntelliJ Plugin</a>	372
<a href="#">Locating the Source Code Associated with Static Scan Issues</a>	373
<a href="#">Uninstalling the IntelliJ Plugin</a>	374

## Installing the IntelliJ Plugin

To install the IntelliJ plugin:

1. From IntelliJ, open the Settings dialog box as follows:
  - On Windows or Linux, select **File > Settings**.
  - On macOS, select **<IDE\_name> > Preferences**.
2. In the left pane, select **Plugins**.
3. Select the **Marketplace** tab, and then in the search box type Fortify on Demand.

4. Click **Install**.
5. Click **OK**.
6. To activate the plugin, click **Restart IDE**.

The menu bar now includes the **Fortify** menu.

## Configuring the IntelliJ Plugin

You can configure options for uploading source code and for communicating with Fortify on Demand at any time.

To configure IntelliJ plugin options:

1. From the IntelliJ menu bar, select **Fortify > Configure Fortify on Demand plugin**.
2. To change the amount of time to wait for communicating with Fortify on Demand before giving up, type the time in seconds in the **HTTP Timeout** box.

Valid values for HTTP timeout are 0 through 21600 (6 hours). A value of 0 indicates that there is no timeout. The default HTTP timeout is 120 seconds (2 minutes).

3. To change the size of individual pieces that are uploaded to Fortify on Demand, type the size in kilobytes in the **Upload chunk size** box.

The packaged source code is uploaded in chunks for optimal performance and reliability. The valid chunk size values are 1 through 10000 Kb. To upload a large file with a stable connection, you can specify larger chunks sizes. To upload a small file with a connection that is not as reliable (for example, a wireless connection), use the default chunk size of 64 Kb or smaller.

4. To enable the plugin to accept any server certificate, select the **Disable SSL Validation** check box.

**Note:** For security reasons, selecting this option is not recommended.

5. Click **OK**.

## Uploading Code with the IntelliJ Plugin

Before you start, make sure you have the following:

- Your Fortify on Demand login credentials

**Note:** To upload your code, you must have the Start Static Scan permission.

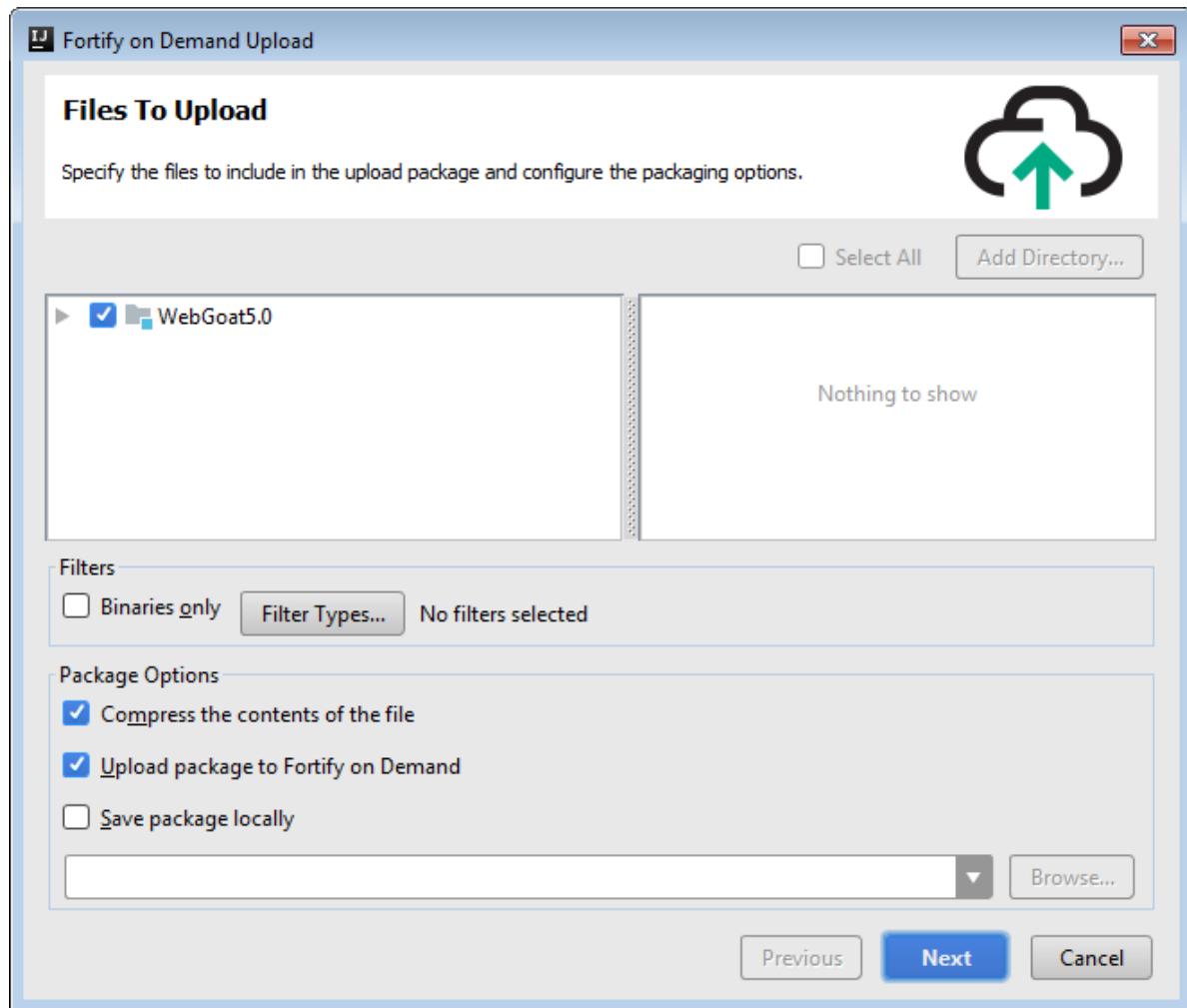
- A project open in IntelliJ

To upload source code to Fortify on Demand from IntelliJ:

1. In IntelliJ, select **Fortify > Upload project to Fortify on Demand**.

The Fortify on Demand Upload wizard opens.

## Files to Upload



The left pane displays all the open modules.

- To refine the files to upload, perform one or more of the procedures described in the following table.

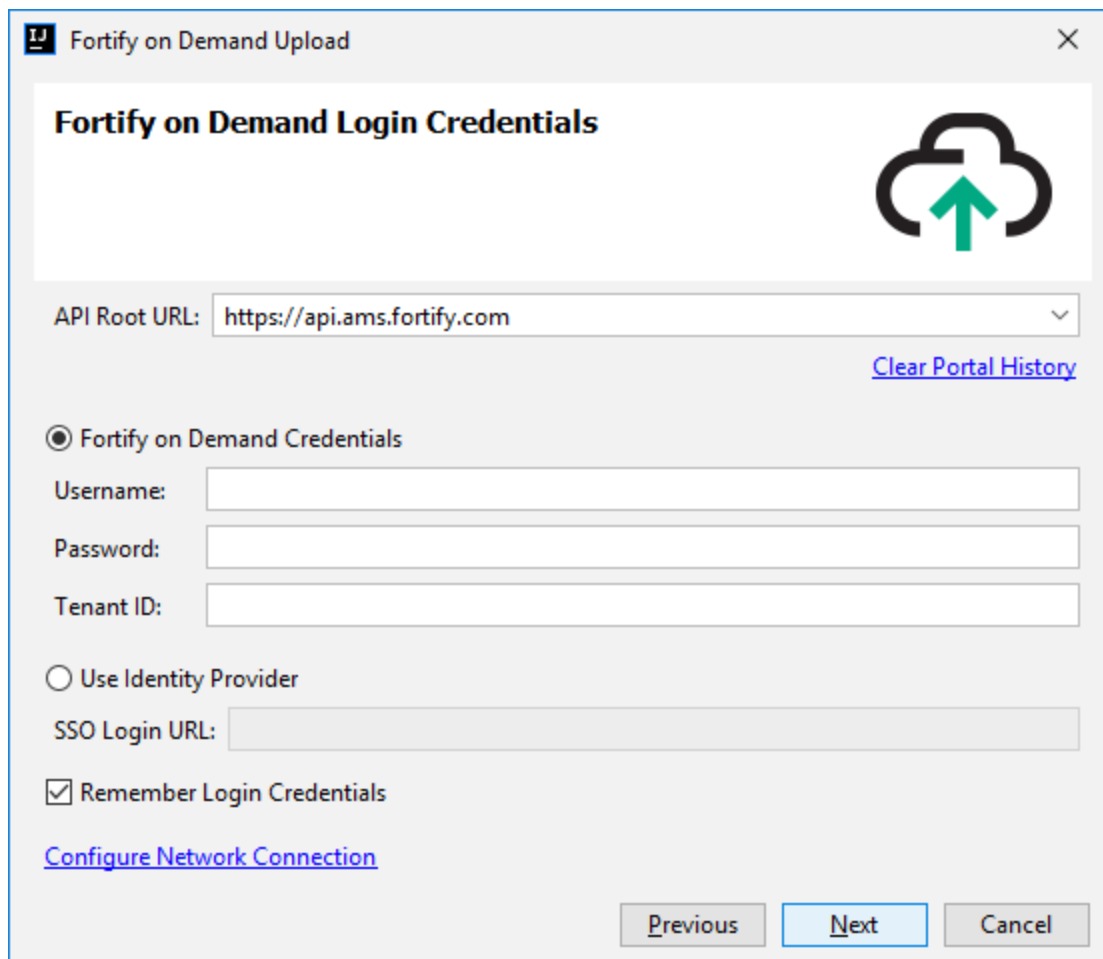
File Upload Refinement	Procedure
Omit specific modules.	<ul style="list-style-type: none"> <li>In the left pane, clear the check box for the module you want to exclude from your upload package.</li> </ul>
Omit specific files located in a module listed in the left pane.	<ol style="list-style-type: none"> <li>Select a folder in the left pane.</li> <li>In the right pane, clear the check boxes for the files you want exclude from your upload package.</li> </ol>
Upload only binary files (EAR, EXE, CLASS, DLL, JAR, and WAR files).	<ul style="list-style-type: none"> <li>Select the <b>Binaries only</b> check box.</li> </ul>

File Upload Refinement	Procedure
Upload only specific file types.	<ol style="list-style-type: none"><li>a. Click <b>Filter Types</b>.</li><li>b. In the Select Types dialog box, select the check boxes for the file types that you want to upload.</li><li>c. Click <b>OK</b>.</li></ol>
Upload additional external resources.	<ol style="list-style-type: none"><li>a. Click <b>Add Directory</b>.</li><li>b. In the Browse for Folder dialog box, navigate to and select the resources to upload, and then click <b>Open</b>. After you add a folder, you can select specific files within it.</li></ol> <div data-bbox="786 762 1401 980" style="background-color: #f0f0f0; padding: 10px;"><p><b>Notes:</b></p><ul style="list-style-type: none"><li>◦ Subfolders are included.</li><li>◦ Folders with native Unicode symbols in the name are not supported.</li></ul></div>

3. To reduce the size of the package, leave the **Compress the contents of the file** check box selected.  
Although this reduces the size of the package to be uploaded, the packaging process takes longer.
4. To upload the package to your Fortify on Demand server, leave the **Upload package to Fortify on Demand** check box selected.
5. To save the package to a local directory, do the following:
  - a. Select the **Save package locally** check box
  - b. Click **Browse**.
  - c. Navigate to and select a folder.
  - d. Click **Save**.
6. Do one of the following:
  - If you selected the **Save package locally** check box and cleared the **Upload package to Fortify on Demand** check box, click **Finish**.
  - To upload the package to your Fortify on Demand server, click **Next**.

## Fortify on Demand Login Credentials

If you selected to upload the package, the **Fortify on Demand Login Credentials** page is displayed. If you have already logged in to Fortify on Demand, then the next step is to select an application and release (see "[Release Selection and Static Scan Setup](#)" on page 365).



The screenshot shows a dialog box titled "Fortify on Demand Upload" with a close button (X) in the top right corner. The main heading is "Fortify on Demand Login Credentials" next to a cloud icon with a green arrow pointing up. Below this is a dropdown menu for "API Root URL:" containing the text "https://api.ams.fortify.com". To the right of the dropdown is a link "Clear Portal History". There are two radio button options: "Fortify on Demand Credentials" (which is selected) and "Use Identity Provider". Under "Fortify on Demand Credentials" are three text input fields labeled "Username:", "Password:", and "Tenant ID:". Under "Use Identity Provider" is a text input field labeled "SSO Login URL:". There is a checked checkbox labeled "Remember Login Credentials" and a link "Configure Network Connection". At the bottom are three buttons: "Previous", "Next" (highlighted in blue), and "Cancel".

1. In the **API Root URL** box, type the API Root URL.  
To obtain this URL, see "[Fortify on Demand API](#)" on page 306 or contact a TAM.
2. Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none"><li>a. Provide your <b>Username</b>, <b>Password</b>, and <b>Tenant ID</b>.</li><li>b. To save your credentials, select the <b>Remember Login Credentials</b> check box.</li></ol> <p><b>Note:</b> For security reasons, the plugin does</p>

Login Method	Procedure
	<p data-bbox="797 310 1403 373">not save your password.</p> <p data-bbox="756 394 1414 506">c. To configure your proxy network preferences, click <b>Configure Network Connection</b>, and then follow the instructions provided by IntelliJ IDEA help.</p>
Use Single Sign-On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.	<p data-bbox="756 541 1159 573">a. Select <b>Use Identity Provider</b>.</p> <p data-bbox="756 594 1409 667">b. In the <b>SSO Login URL</b> box, type the URL provided by your Security Lead.</p>

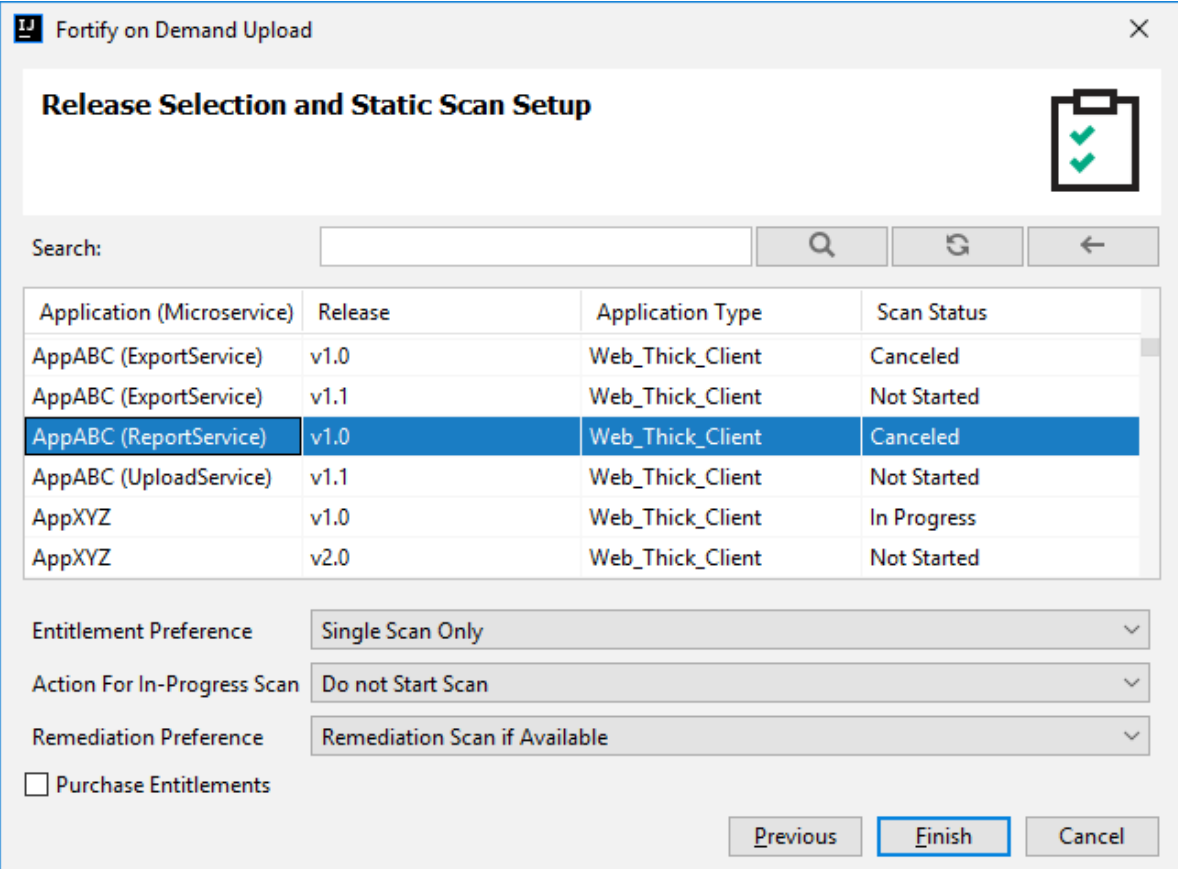
3. Click **Next**.
4. If your tenant requires two-factor authentication, then do the following:
  - a. In the Two-Step Verification dialog box, select a delivery method for the security code (**SMS** or **Email**), and click **OK**.
  - b. Obtain the security code delivered using the method you selected.
  - c. Enter the code in the **Security Code** box, and then click **OK**.

The plugin allows you three attempts to enter the security code. If necessary, click **Resend Code** to have a new security code sent to you.



## Release Selection and Static Scan Setup

1. Select the application and release for your upload package.



The screenshot shows the 'Fortify on Demand Upload' dialog box with the title 'Release Selection and Static Scan Setup'. It features a search bar, a table of application releases, and several configuration options.


Application (Microservice)	Release	Application Type	Scan Status
AppABC (ExportService)	v1.0	Web_Thick_Client	Canceled
AppABC (ExportService)	v1.1	Web_Thick_Client	Not Started
AppABC (ReportService)	v1.0	Web_Thick_Client	Canceled
AppABC (UploadService)	v1.1	Web_Thick_Client	Not Started
AppXYZ	v1.0	Web_Thick_Client	In Progress
AppXYZ	v2.0	Web_Thick_Client	Not Started

Configuration options:

- Entitlement Preference: Single Scan Only
- Action For In-Progress Scan: Do not Start Scan
- Remediation Preference: Remediation Scan if Available
- Purchase Entitlements

Buttons: Previous, Finish, Cancel

To quickly find an application and release, type the name or partial name of an application or release in the **Search** box, and then press **Enter**. The search is case-insensitive. To clear the search results, clear the **Search** box, and then press **Enter**.

**Note:** To refresh the list of applications, click **Refresh** .

2. Select an **Entitlement Preference** from the list.  
If multiple entitlements are available, the scan will use the oldest entitlement. If the release has an active subscription, the scan will use the active subscription.
3. From the **Action for In-Progress Scan** list, select what should happen if the selected release scan status is **In Progress**.  
You can choose to not start the scan, cancel the in-progress scan and start the new scan, or queue the new scan.
4. From the **Remediation Preference** list, select whether to run a remediation scan.
5. To purchase entitlements for this scan (if available), select the **Purchase Entitlements** check box.

6. Select an assessment type from the **Assessment Type** list.

**Note:** Steps 6 through 9 (shown under **Static Scan Details**) are only applicable if the selected release does not have scan settings configured yet. The fields described in these steps are hidden if the scan settings are already configured.

**Static Scan Details** ⬆

999865 Unit(s) Available

Assessment Type Static Assessment - Subscription (4 Units) ⌵

Technology Stack JAVA/J2EE ⌵

Language Level 11 ⌵

Open Source Component Analysis

Audit Preference Manual ⌵

Include third-party libraries for static security assessment (will lead to longer turnaround times)

To upload your project, you must select an assessment type that is less than or equal to the entitlements that you have available.

7. Specify the **Technology Stack** and the **Language Level**.
8. If you want open source libraries for Java and .NET applications identified in the analysis (and if this feature is available), select the **Open Source Component Analysis** check box.

This produces a report of identified open source components and known vulnerabilities using Sonatype.

9. To specify additional advanced scanning and auditing preferences, make selections for the options described in the following table.

Option	Description
Audit Preference	<p>This option is only available if enabled for your tenant.</p> <p>The audit preference settings are:</p> <ul style="list-style-type: none"> <li>• <b>Manual</b>—A security expert manually reviews the scan results and removes false positives</li> <li>• <b>Automated</b>—False positives identified by Fortify Scan Analytics with high confidence are automatically suppressed and results are published without manual review. This can reduce the turnaround time.</li> </ul>
Include third-party libraries for security assessment	<p>Authorizes Fortify on Demand to assess the code for vulnerabilities to include in reports, vulnerability count, and risk rating.</p> <p>Selecting this option indicates that your organization has received consent from all third-party vendors to scan their libraries.</p>

10. Click **Finish** to upload your code to Fortify on Demand.

Information about the IDE (name and version) used for this upload is saved and shown in the scan summary.

## Opening Analysis Results with the IntelliJ Plugin

From the IntelliJ, you can open Fortify on Demand analysis results for an application and release to remediate.

**Note:** If you already have analysis results open, you can use this procedure to close the current analysis results and open the analysis results for a different application and release.

To open the analysis results:

1. In IntelliJ, select **Fortify > Open Analysis Results**.

The Fortify on Demand Open Analysis Results wizard opens.

- a. In the **API Root URL** box, type the API Root URL.

To obtain this URL, see "[Fortify on Demand API](#)" on page 306 or contact a TAM.

- b. Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none"><li>i. Provide your <b>Username, Password</b>, and <b>Tenant ID</b>.</li><li>ii. To save your credentials, select the <b>Remember Login Credentials</b> check box. <div data-bbox="834 1241 1403 1346" style="background-color: #f0f0f0; padding: 5px;"><b>Note:</b> For security reasons, the plugin does not save your password.</div></li><li>iii. To configure your proxy network preferences, click <b>Configure Network Connection</b>, and then follow the instructions provided by IntelliJ IDEA help.</li></ol>
Use Single Sign-On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.	<ol style="list-style-type: none"><li>i. Select <b>Use Identity Provider</b>.</li><li>ii. In the <b>SSO Login URL</b> box, type the URL provided by your Security Lead.</li></ol>

- c. Click **Next**.

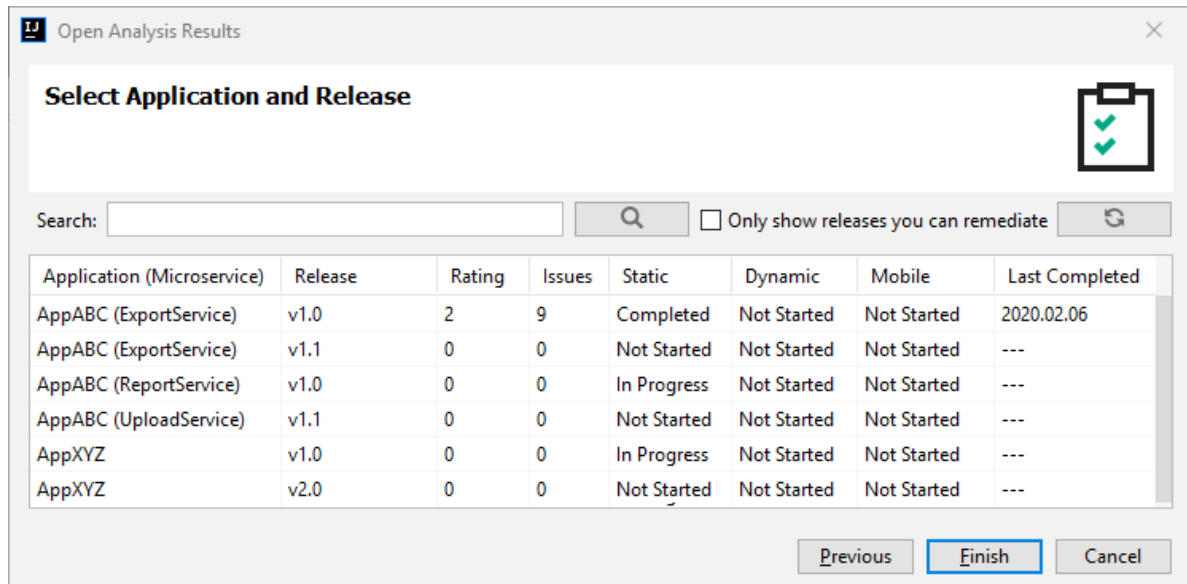
- d. If your tenant requires two-factor authentication, then do the following:

- i. In the Two-Step Verification dialog box, select a delivery method for the security code (**SMS** or **Email**), and click **OK**.

- ii. Obtain the security code delivered using the method you selected.
- iii. Enter the code in the **Security Code** box, and then click **OK**.


The plugin allows you three attempts to enter the security code. If necessary, click **Resend Code** to have a new security code sent to you.

2. Select an application and release for the analysis results you want to open.



You can only open results for an application and release that has had at least one successfully completed scan. Clear the **Only show releases you can remediate** check box to see all applications and releases.

To quickly find an application and release, type the name or partial name of an application or release in the **Search** box, and then press **Enter**. The search is case-insensitive. To clear the search results, clear the **Search** box, and then press **Enter**.

**Note:** To refresh the list of applications, click **Refresh** .

3. Click **Finish**.

The analysis results are displayed in the Fortify windows. See "[Analysis Results in the IntelliJ Plugin](#)" [below](#) for a description of the Fortify windows.

## Analysis Results in the IntelliJ Plugin

After the analysis results are opened, the IntelliJ Plugin displays four audit-focused windows. The **Analysis Results** window displays the results. The **Analysis Trace**, **Audit Summary**, and **Issue Summary** windows are visible, but do not contain any information until you select an issue from the **Analysis Results** window.

**Note:** To open a Fortify window that is not currently visible, select **Fortify > Show View** and select the window you want to open.

The following table describes the Fortify windows.





View	Description
Analysis Results	<p>The <b>Analysis Results</b> window provides a way to group and select the issues to audit. This view also displays the relevant trace output for issues (see the following description of the <b>Analysis Trace</b> window).</p> <p>The color-coded tabs in the <b>Analysis Results</b> group the issues by severity level. The last tab contains all issues. The <b>Group By</b> list options sort the issues into subfolders. The option you select is applied to all visible folders.</p>
Analysis Trace	<p><b>For Static Analysis Results</b>—After you select an issue in the <b>Analysis Results</b> window, the <b>Analysis Trace</b> window displays the relevant trace output. This is a set of program points that show how the analyzer found the issue. For dataflow and control flow issues, the set is presented in the order executed. For dataflow issues, this evidence is the path that the tainted data follows from the source function to the sink function. See the following descriptions of the analysis trace icons.</p> <p><b>For Dynamic Analysis Results</b>—After you select an issue in the <b>Analysis Results</b> window, the <b>Analysis Trace</b> window displays details about the request parameters.</p> <p>This window also provides an abstract that briefly describes the issue.</p>
Audit Summary	<p>After you select an issue in the <b>Analysis Results</b> view, the <b>Audit Summary</b> view displays audit information for the selected issue. You can edit issue information, add comments, and review the audit history. For more information, see <a href="#">"Auditing Issues from the IntelliJ Plugin" on page 372</a>.</p>
Issue Summary	<p>After you select an issue in the <b>Analysis Results</b> window, the <b>Issue Summary</b> window provides detailed information about the issue. The <b>Details</b> tab provides an abstract of the issue, a detailed explanation, and might also include examples with descriptive text and code samples, and the scan type (static, dynamic, or mobile).</p> <p>The <b>Recommendations</b> tab displays recommendations to remediate the issue, along with tips and references for additional research.</p>

The Editor is where the IntelliJ plugin displays the source code (if available) for static scans or the request and response details for dynamic scans. The Editor opens after you select an issue in the **Analysis Results** window.

## Analysis Trace Icons


The analysis trace icons described in the following table show how dataflow moves in the section of the source code or execution order.

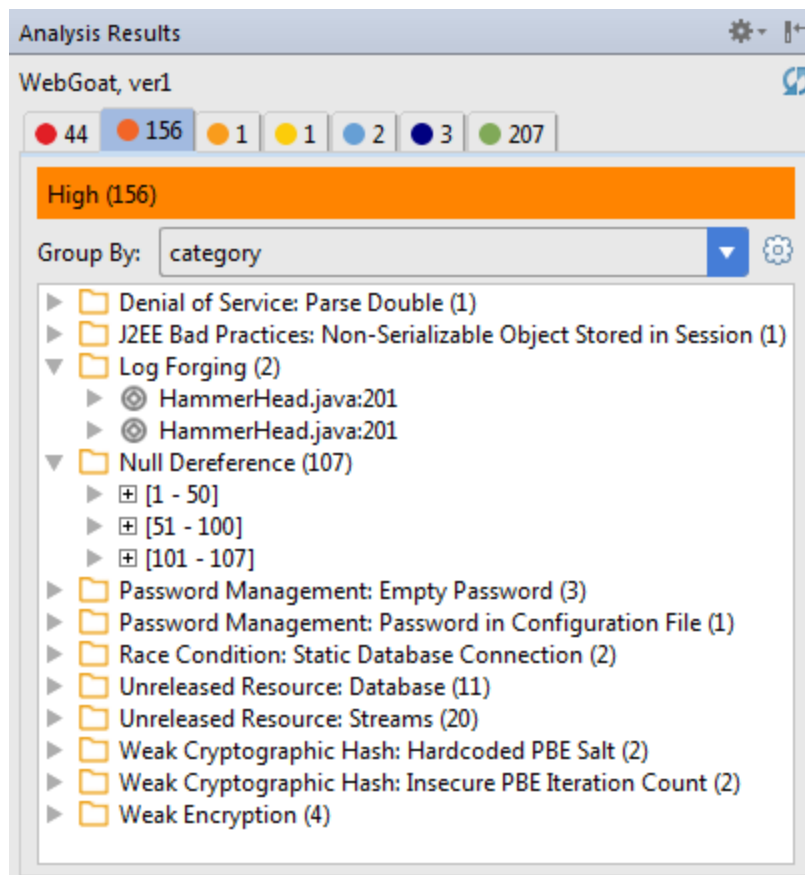
Icon	Description	Icon	Description
	Data is assigned to a field or variable		Tainted data is returned from a function
	Information is read from a source external to the code such as an HTML form or a URL		A pointer is created
	Data is assigned to a globally scoped field or variable		A pointer is dereferenced
	A comparison is made		The scope of a variable ends
	The function call receives tainted data		The execution jumps
	The function call returns tainted data		A branch is taken in the code execution
	<p>Passthrough, tainted data passes from one place to another</p> <p><b>Note:</b> This is typically shown as <code>functionA(x : y)</code> to indicate that data is transferred from x to y. The x and y values are one of the following:</p> <ul style="list-style-type: none"> <li>• An argument index</li> <li>• <code>return</code>—The return value of a function</li> <li>• <code>this</code>—The instance of the current object</li> <li>• A specific object field or key</li> </ul>		A branch is not taken in the code execution
	An alias is created for a memory		Generic

Icon	Description	Icon	Description
	location		
	Data is read from a variable		A runtime source, sink, or validation step
	Data is read from a global variable		Taint change

## Reviewing Issues from the IntelliJ Plugin

To view and select issues:

1. From the **Group By** list, select a value to use to sort issues in all visible folders into groups.  
The default grouping is **category**.
2. Click a colored tab to view the associated issues.  
The issue type subfolders listed are based on the selected **Group By** value.
3. To show suppressed or fixed issues, click **Set visibility options** ().
4. To view the list of issues in a subfolder, expand the subfolder.  
The IntelliJ plugin retrieves the corresponding issues from Fortify on Demand.



**Note:** If a folder contains more than 50 issues, the issues are grouped into subfolders in blocks of 50 with folder names that indicate which issues are included. For example, if a folder contains 71 issues, the first 50 issues are in a subfolder labeled **[1-50]** and the next set of issues are in a subfolder labeled **[51-71]**.

5. To see any updates to the analysis results made on Fortify on Demand, click **Refresh** (↻).
6. Select an issue.

The **Analysis Trace**, **Audit Summary**, and **Issue Summary** windows display information about the selected issue.

## Auditing Issues from the IntelliJ Plugin

If you have the Edit Issues permission, you can assign a user, set the developer status, and add comments for issues in the **Audit Summary** view. If you have the Audit Issues permission, you can also edit the issue's auditor status and severity.

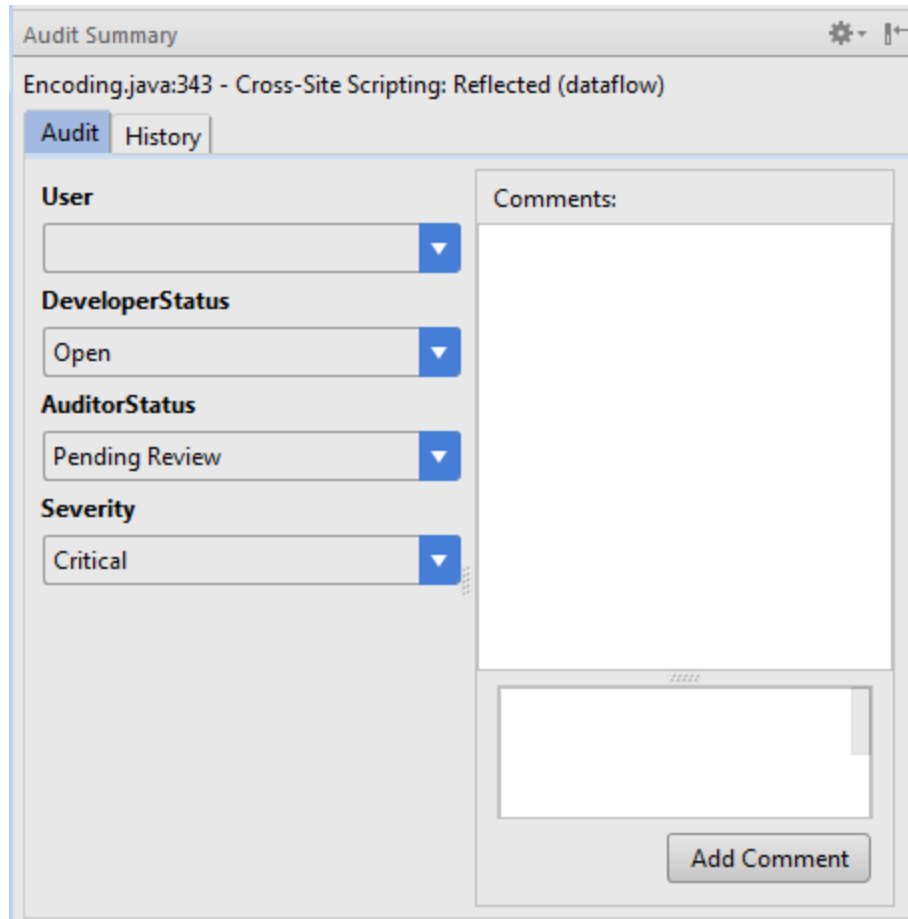
To audit an issue:

1. Make sure that the **Audit Summary** view is open.
2. From the issues list in the **Analysis Results**, select an issue.



You can select multiple issues in the **Analysis Results** view to make the same edits to multiple issues.

3. In the **Audit Summary** view, select the user to assign to the issue from **User** list.



4. To change the issue's development status, select the status from the **DeveloperStatus** list.
5. To change the auditor status, select the status from the **AuditorStatus** list.
6. To change the issue severity, select an issue severity from the **Severity** list. For more information about issue severity, see ["Priority Order" on page 19](#).
7. To add a comment for the issue, type your comment in the box at the bottom of the **Comments** area, and then click **Add Comment**.

Your comment is displayed in the **Comments** section.

The plugin saves your changes for the application and release on the Fortify on Demand server.

## Locating the Source Code Associated with Static Scan Issues

You can use the IntelliJ plugin to locate security-related issues in your code.

To jump to the line of source code that contains the issue selected in the IntelliJ IDEA plugin:

- Select an issue in the **Analysis Results** window or select a line in the **Analysis Trace** window.

If the issue is located in source code available in the current project, IntelliJ plugin opens the relevant file in the Editor. Otherwise, the IntelliJ plugin attempts to download the source code from Fortify on Demand and if the relevant file is available, it is opened in the Editor.

**Note:** If the file was downloaded, the file name is prepended with `Remote<yyyy-mm-dd>-` where the `<yyyy-mm-dd>` is the date the file was last scanned.

The IntelliJ plugin highlights the line of code associated with the issue.

## Uninstalling the IntelliJ Plugin

To uninstall the Fortify on Demand IntelliJ IDEA plugin:

1. From IntelliJ, open the Settings dialog box as follows:
  - On Windows or Linux, select **File > Settings**.
  - On macOS, select **<IDE\_name> > Preferences**.
2. In the left pane, select **Plugins**.
3. From the **Plugins** list, select **Fortify on Demand**.
4. In the **Fortify on Demand** pane on the right, select **Uninstall**.
5. Click **Yes** to confirm that you want to uninstall the plugin.
6. In the **Fortify on Demand** pane on the right, click **Restart IntelliJ IDEA**.

## FoDUploader

Fortify on Demand provides a build server integration (BSI) tool called FoDUploader to help you upload applications from a build server. FoDUploader runs from the command-line on all major operating systems and thus can easily be integrated into a build script.

The benefits of using FoDUploader include:

- Sending files to Fortify on Demand without a size limitation
- Transmitting files securely from a client workstation to Fortify on Demand
- Transmitting through a proxy, if required
- API key pair or PAT authentication

**Note:** If you are building an application entirely within the Visual Studio, Eclipse, or IntelliJ IDE, you can use the IDE plugins to upload the application and start a static scan.

This section covers the following topics:

<a href="#">Downloading FoDUploader</a> .....	375
<a href="#">Running FoDUploader</a> .....	375

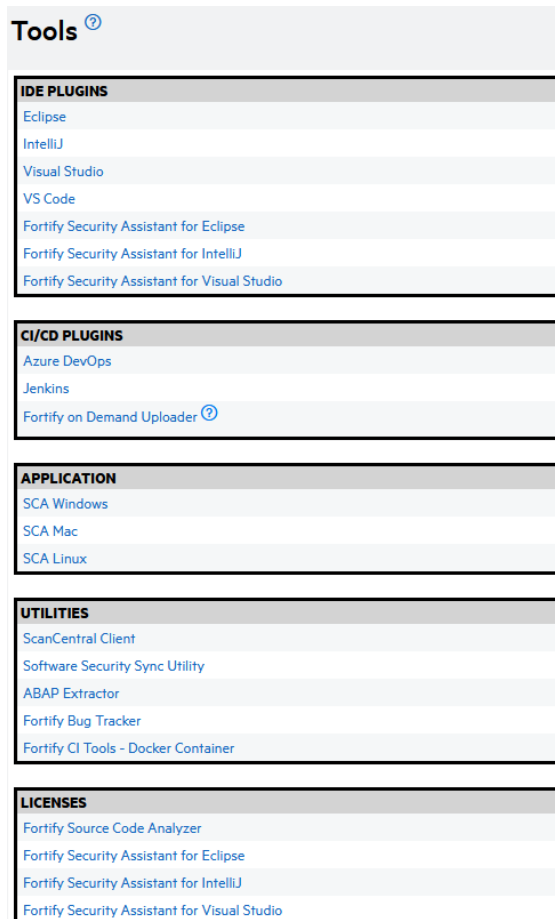
## Downloading FoDUploader

FoDUploader is available as a Java application named `FoDUpload.jar`.

To download the FoDUploader tool:

1. Click your account name and select **Tools** from the list.

The Tools page appears.



2. Click the Fortify on Demand Uploader link to access the FoDUploader GitHub page, where you can download `FoDUpload.jar` as well as the source code.

## Running FoDUploader

You must have Java 8 or later installed before running FoDUploader.

**Note:** The following instructions refer to version 5.4.0. See <https://github.com/fod-dev/fod-uploader-java> for the latest release.

To run FoDUploader:

In a command-line interface, run `FoDUpload.jar` with the appropriate arguments. You can also insert the command in your build script to integrate with your build server. The basic syntax is:

```
java -jar FoDUpload.jar -z "<zip_file_path>" {-ac <key> <secret>|-uc
<username> <password>} {-rid <relID>|-bsi <token>} -purl <purl> -aurl
<aurl> -tc <tcode> -ep
{1|SingleScanOnly|2|SubscriptionOnly|3|SingleScanFirstThenSubscription|4|Su
bscriptionFirstThenSingleScan}
```

If the command is properly executed, the command-line displays the bytes sent and the upload status. Otherwise, the command-line displays an error message indicating the part of the command that is incorrect.

## FoDUploader Arguments

The following table describes the FoDUploader arguments. Arguments can be specified in any order.

**Note:** Flag arguments are false by default. Include a flag to set it to true—you do not need to specify true or false.

Argument	Short Name	Required	Description
-zipLocation	-z	Yes	Location of the zip file. Enclose the path with quotation marks to escape special characters.
-entitlementPreferenceType	-ep	Yes	Entitlement preference: 1/SingleScanOnly, 2/SubscriptionOnly, 3/SingleScanFirstThenSubscription, 4/SubscriptionFirstThenSingleScan  If multiple entitlements are available, the scan will use the oldest entitlement. If the release has an active subscription, the scan will use the active subscription.
-apiCredentials	-ac	Yes <sup>1</sup>	API key and secret.
-userCredentials	-uc	Yes <sup>1</sup>	Your user credentials. Enclose the username and password

Argument	Short Name	Required	Description
			separately with quotation marks to escape special characters.
-bsiToken	-bsi	Yes <sup>2</sup>	BSI token.
-releaseld	-rid	Yes <sup>2</sup>	Release ID. The release must have saved scan settings in the portal for the release ID to be used as a token.
-portalurl	-purl	Yes <sup>3</sup>	Domain URL.
-apiurl	-aurl	Yes <sup>3</sup>	API root URL.
-tenantCode	-tc	Yes <sup>3</sup>	Tenant code if using user credentials.
- assessmentTypeld	-at	Yes <sup>4</sup>	Assessment type ID.
-entitlement	-eid	Yes <sup>4</sup>	Entitlement ID.
-technologyStackId	-ts	Yes <sup>4</sup>	<p>Technology stack as an integer: 1 (.NET), 23 (.Net Core), 2 (ABAP), 21 (Apex/Visualforce), 3 (ASP), 5 (CFML), 6 (COBOL), 22 (Go), 27 (Infrastructure-As-Code/Dockerfile), 7 (JAVA/J2EE/Kotlin), 16 (JS/TS/HTML), 18 (MBS/C/C++/Scala), 9 (PHP), 10 (PYTHON), 17 (Ruby), 12 (Swift/Objective C/C++), 11 (VB6), 14 (VBScript)</p> <p>1 (.NET), 23 (.Net Core), 2 (ABAP), 21 (Apex/Visualforce), 3 (ASP), 5 (CFML), 6 (COBOL), 22 (Go), 27 (Infrastructure-As-Code/Dockerfile), 7 (JAVA/J2EE), 16 (JS/TS/HTML), 18</p>

Argument	Short Name	Required	Description
			(MBS/C/C++/Scala), 9 (PHP), 10 (PYTHON), 17 (Ruby), 12 (Swift/Objective C/C++), 11 (VB6), 14 (VBScript)
-languageLevelId	-l	Yes <sup>4</sup>	Language level as an integer: <ul style="list-style-type: none"> <li>.NET: 2 (2.0), 3 (3.0), 4 (3.5), 5 (4.0), 11 (4.5), 15 (4.6), 16 (4.7), 30, (4.8), 32 (5.0), 33 (6.0)</li> <li>.NET Core: 23 (1.0), 24 (1.1), 25 (2.0), 26 (2.1), 27 (2.2), 28 (3.0), 29 (3.1)</li> <li>Java: 8 (1.5), 9 (1.6), 10 (1.7), 12 (1.8), 17 (1.9), 19 (10), 20 (11), 21 (12), 22 (13), 31 (14), 34(17)</li> <li>Python: 13 (2), 14 (2 Django), 18 (3)</li> </ul>
-auditPreferenceId	-a	Yes <sup>4</sup>	Audit preference: Manual, Automated
-isBinaryScan	-bs	No <sup>4</sup>	Scan compiled and source code (the feature must be enabled).
-allowopenSourceComponentAnalysis	-os	No <sup>4</sup>	Include open source component analysis
-remediationScanPreferenceType	-rp	No	Remediation scan preference: 0/RemediationScanIfAvailable, 1/RemediationScanOnly, 2/NonRemediationScanOnly (default)
-inProgressScanActionType	-pp	No	If an in-progress scan exists, the action to take for the new scan:

Argument	Short Name	Required	Description
			0/DoNotStartScan (default), 1/CancelScanInProgress, 2/Queue  This only applies if the in-progress scan can be automatically cancelled.
-purchaseEntitlement	-purchase	No	Purchase an entitlement if none is available (the feature needs to be enabled).
-allowPolicyFail	-apf	No	Return exit(0) instead of exit(1) if the scan fails the security policy specified in Fortify on Demand
-pollingInterval	-l	No	Length of time in minutes between polling Fortify on Demand for the scan status. Polling stops once a scan is cancelled, completed, or paused. If the polling interval is not set or set to 0, no polling is done.
-proxy	-P	No	Proxy connection details (order dependent): <ul style="list-style-type: none"> <li>• The proxy host defined with a protocol (such as http)</li> <li>• The account credentials on the proxy server</li> <li>• The proxy server's domain name for NTLM authentication</li> <li>• The proxy server's host name for NTLM authentication</li> </ul>
-notes	-n	No	Adds notes about the scan.
-help	-h	No	Prints the help dialog.
-version	-v	No	Prints the FoDUploader version.

- <sup>1</sup> Use either API credentials or user credentials.
- <sup>2</sup> Use either release ID or BSI token. If both are provided, then the scan settings that are retrieved from the release ID will be used.
- <sup>3</sup> Required if BSI token is not provided.
- <sup>4</sup> Required if neither release ID nor BSI token is provided. Provided values override existing release ID or BSI token settings.

## Examples

Command-line examples:

```
java -jar FodUpload.jar -uc tenantuser tenantpassword -z my_payload.zip -rid 1111 -ep 1 -P http://192.168.56.1:808 proxyuser1 proxyuserpassword -rp 0 -pp 0
```

```
C:\Program Files (x86)\Java\jre-9\bin\java.exe -jar C:\fod_upload\FodUpload.jar -uc john-doe pswd!@#$ -z c:\Build\Input\applicationFiles.zip -bsi eyJ0ZW5hbnRjZCI6NSwidGVuYW50Q29kZSI6InR0MSIsInJlbGVhc2VJZCI6NDQwNiwicGF5bG9hZFR5cGUiOiJBTkFMWVNJU19QOVlMT0FEIiwiaXNzZXNzbWVudFR5cGVJZCI6MTIwLCJ0ZWNo9sb2d5VHlwZSI6IkFwZXhfVmlzdWFsZm9yY2UiLCJ0ZWNo9sb2d5VHlwZUlkIjoyMSwidGVjaG5vbG9neVZlcnNpb24iOm51bGwsInRlY2hub2xvZ3lWZXJzaW9uSWQiOm51bGwsImF1ZGl0UHJlZmVyZW5jZSI6Ik1hbnVhbCI6ImF1ZGl0UHJlZmVyZW5jZUlkIjoxLCJpbmNsdWRlVGhpcmRQYXJ0eSI6ZmFsc2UsImluY2x1ZGVpcGVuU291cmNlQW5hbHlzaXMiOmZhbHN1LCJzY2FuUHJlZmVyZW5jZSI6I1N0Y5kYXJkIiwic2NhbnlByZWZlcmVuY2VJZCI6MSwicG9ydGFsVXJpIjoiaHR0cHM6Ly9mb2R5YXJktdGVuYW50LmZvcnR5Zm9yY2kubG9jYXNzLCJhcGlvcmk0IjodHRwOi8vMTYuMTAzLjIzNC4yMzcifQ== -ep 1 -rp 0 -pp 0
```

Usage notes:

java is the path of the Java executable.

- If java.exe is in the directory from which the command is run or if the java.exe directory is included in the file system path, simply reference java as the path.
- If the java.exe is not in the path, the full path is required (for example, C:\Program Files (x86)\Java\jre-9\bin\java.exe).

The -jar operator informs java.exe that it is working with a JAR file for the rest of the command set.

FodUpload.jar is the path of the FoDUpload.jar tool.

- If FodUpload.jar is in the directory from which the command is being run, simply reference FodUpload.jar as the path.
- If FodUpload.jar is in a different directory, the full path is required (for example, C:\fod\_upload\fodupload.jar).



# Chapter 10: Integrations

This section contains the following topics:

- [Importing External Scans](#) ..... 381
- [Bug Tracker Integration](#) ..... 384
- [Secure Code Warrior Integration](#) ..... 392
- [Slack Integration for Notifications](#) ..... 394
- [Source Control Integration](#) ..... 397
- [Tracking Configured Integrations](#) ..... 399
- [Training Courses](#) ..... 401
- [Webhooks](#) ..... 403

## Importing External Scans

You can import scan results from external sources into Fortify on Demand to manage scan results from multiple sources in a single view. Fortify on Demand supports import of the following scan types:

- On-premises Fortify Static Code Analyzer and Fortify WebInspect scan results
- Open source scan results that conform to the CycloneDX 1.4 standard

This section contains the following topics:

- [Importing an On-Premises Scan](#) ..... 381
- [Importing a Software Bill of Materials](#) ..... 383
- [Deleting an Imported Scan](#) ..... 383

## Importing an On-Premises Scan

You can import on-premises static (Micro Focus Fortify Static Code Analyzer) and dynamic (Micro Focus Fortify WebInspect) scan results into Fortify on Demand. Upon importing an FPR:

- The scan start and complete times use the scan date in the FPR.
- Global and Application Audit Templates are applied.
- The instance ID provided by Fortify Static Code Analyzer or Fortify WebInspect is used to track issues across imported FPRs. Fortify on Demand does not check for duplicate FPRs.

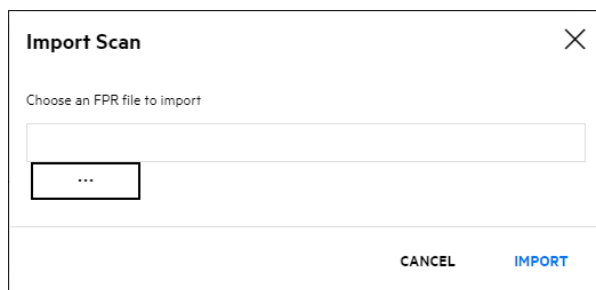
For example, if you import an FPR into an empty release, all imported issues will have the **New** status. If you import the same FPR again, all issues will change from **New** to **Existing**. If you then import a different FPR, the issue statuses will change as follows:

- Issues that exist in both the release and the latest FPR will have the **Existing** status.
- Issues that only exist in the latest FPR will have the **New** status.
- Issues that exist in the release but do not exist in the latest FPR have the **Fixed** status.
- Suppressed issues in the FPR that are not present in the release are imported and suppressed. Suppression status is ignored for issues in the FPR that are present in the release.

**Note:** FPRs with a scan date older than the most recently completed scan of the same type are not accepted.

To import a static or dynamic FPR:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears.
3. Click the release for which you want to import an FPR.  
The Release Overview page appears.
4. Click **Scans**.  
The **Release Scans** page appears.
5. Select **Import Scan>Dynamic | Static**.  
The Import Scan window opens.



6. Click ... and navigate to and select the FPR file.
7. Click **Next**.  
Once the import is complete, the results appear on the Issues page. The scan appears on the Release Scans page with a "Completed" status and "Imported (WebInspect)" or "Imported (SCA)" assessment type.

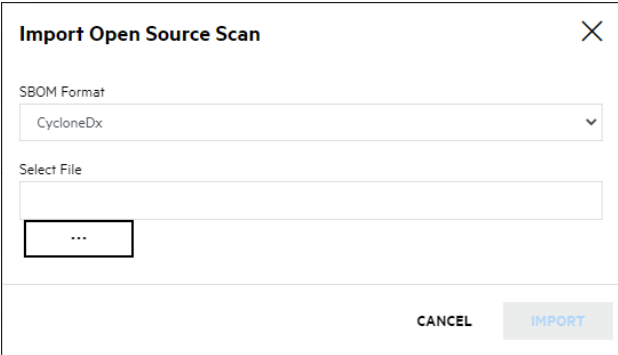
## Importing a Software Bill of Materials

Users with the **Manage Applications** permission can import open source scan results, also known as software bill of materials (SBOM). An SBOM must meet the following requirements to be imported:

- The SBOM is a JSON file that conforms to the CycloneDX 1.4 standard.
- The SBOM contains a single `tools` entry under the `metadata` object.
- The SBOM version is higher than the version of the most recently imported SBOM.

To import an open source scan:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears.
3. Click the release for which you want to import an open source scan.  
The Release Overview page appears.
4. Click **Scans**.  
The Release Scans page appears.
5. Select **Import Scan > Open Source**.  
The Import Open Source Scan window opens.



The screenshot shows a dialog box titled "Import Open Source Scan" with a close button (X) in the top right corner. Inside the dialog, there is a dropdown menu labeled "SBOM Format" with "CycloneDx" selected. Below this is a "Select File" field with a file selection button (three dots). At the bottom of the dialog, there are two buttons: "CANCEL" and "IMPORT".

6. Click ... and navigate to and select the SBOM.
7. Click **Next**.  
Once the import is complete, the results appear on the Issues page. The scan appears on the Release Scans page with a "Completed" status and "<toolName> (Imported)" assessment type.

## Deleting an Imported Scan

Users with the Manage Applications permission can delete imported scan results files. A scan cannot be deleted if a subsequent scan of the same type has been imported.

To delete an imported scan:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application for which you want to delete the most recent imported scan.  
The Application Releases page appears.
3. Click **Scans**.  
The Application Scans page appears, displaying scans ran against the application.

RELEASE	SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES
S.4	Dynamic	Dynamic Express	Subscription	Failed	2017/11/10	2019/05/06	
S.4	Dynamic	Dynamic Premium	N/A	Failed	2016/05/13	2017/07/19	
S.4	Static	Static Basic	N/A	Passed	2016/05/13	2016/05/13	34 Critical, 67 High, 0 Medium, 7 Low, 108 Total
S.4	Dynamic	Dynamic Premium	N/A	Passed	2016/05/13	2016/05/13	101 Critical, 84 High, 11 Medium, 67 Low, 300 Total

**Note:** You can filter the scan list to only view scans ran against a release by clicking the name of the release from the Application Releases page.

4. Click **Cancel Imported Scan** in the action column of the imported scan.  
A confirmation message displays.
5. Click **Yes** to confirm the scan cancellation.  
The scan is deleted, along with all issues associated with the scan.

## Bug Tracker Integration

For tenants that want to link vulnerability results to their bug tracking tools, Fortify on Demand offers bug tracker integration for the latest versions of the following bug trackers:

- Micro Focus Application Lifecycle Management (ALM)
- Micro Focus Application Lifecycle Management Octane (ALM Octane)
- Jira
- Bugzilla
- Azure DevOps/Azure DevOps Server.

Users can submit issues as bugs to a supported bug tracker and manage the bugs directly from the portal. For non-supported bug trackers, users can manually add bug tracker links to issues.

This section contains the following topics:

<a href="#">Configuring Bug Tracker Integration</a>	385
<a href="#">Submitting Issues to the Bug Tracker</a>	387
<a href="#">Manually Linking an Issue</a>	389

## Configuring Bug Tracker Integration

Bug tracker integration is configured at the application level. You must establish a connection between Fortify on Demand and your bug tracker server (VPN is not an option for establishing the connection). The server will need a dedicated user account for adding and closing bugs.

To configure bug tracker integration for an application:

1. Select the **Applications** view.  
Your Applications page displays.
2. Click the application for which you want to configure bug tracker integration.  
The application Overview page appears.
3. Click **Settings**.  
The Settings page appears.

The screenshot shows the 'Application Summary' settings page for 'WebGoat (.NET)'. The page has a sidebar with navigation icons and a main content area. The main content area has a header with 'WebGoat (.NET)' and 'Application Summary' (with 'SAVE' and 'DELETE APPLICATION' buttons). Below the header are tabs for 'Application Summary', 'Application Attributes', 'Bug Tracker', and 'Source Control'. The 'Application Summary' tab is active, showing fields for 'Application Name' (WebGoat (.NET)), 'Business Criticality' (High), 'Application Type' (Web / Thick-Client), and 'Application Description' (Auto generated). There is also a large text area for 'Additional Emails' with a note: 'Separate multiple email addresses with a semicolon or comma'.

4. Select the **Bug Tracker** tab.

The screenshot shows the 'Bug Tracker' settings page for 'WebGoat (.NET)'. The page has a sidebar with navigation icons and a main content area. The main content area has a header with 'WebGoat (.NET)' and 'Application Summary' (with 'SAVE' and 'DELETE APPLICATION' buttons). Below the header are tabs for 'Application Summary', 'Application Attributes', 'Bug Tracker', and 'Source Control'. The 'Bug Tracker' tab is active, showing a toggle for 'Enable Bug Tracker Integration' set to 'No'.

5. Move the **Enable Bug Tracker Integration** slider from **No** to **Yes** to enable bug tracker integration.
6. Select your bug tracker from the **Bug Tracker** list.  
If you selected a supported bug tracker, additional fields appear below. The field names are based on the bug tracker selected.

Enable Bug Tracker Integration

Yes

Fortify on Demand bug tracker integration requires access from the following IP ranges and networks: 74.221.229.249/32

Bug Tracker

Atlassian JIRA

Atlassian JIRA URL

Username Password

AUTHENTICATE

Domain Component

Enable Bug State Management

No

7. In the **URL** field, type the URL of your bug tracker site.
8. In the **Username** and **Password** fields, type the login credentials that will be used to log in to the bug tracker site.

If you have a cloud JIRA instance where the Reporter field is required, in the **Requester Account ID** field, type the user ID associated with the provided **Username**.

**Important!** Atlassian has ended support for basic authentication with passwords and cookie-based authentication for REST APIs.

9. Click **Authenticate**.

An "Authenticated" message appears if the authentication was successful. The list of categories from the bug tracker site is also populated.

**Tip:** If you are having trouble authenticating to the bug tracker, see the following troubleshooting tips:

- Check that the bug tracker instance is publicly accessible. For example, you can test the accessibility of a Jira instance with the command `curl -D- -u <Jira_userid>:<Jira_password> http://<host>.atlassian.net/rest`
- Enable the bug tracker API, if applicable.
- Check that the account used to log in to the bug tracker has permission to access the bug tracker API.
- Add the Fortify on Demand IP addresses to the allow list in firewalls, IPSs, IDSs, and WAFs. The IP addresses are displayed on the Bug Tracker tab.

10. Select the default category to which application's issues will be submitted. Fields are specific to the selected bug tracker.

ALM Octane, ALM.Net: **Domain** and **Project**

Jira: **Project** and **Component**

Bugzilla: **Product** and **Component**

Azure DevOps/Azure DevOps Server: **Project**

11. Move the **Enable Bug State Management** slider from No to **Yes** to enable bug state management. When bug state management is enabled, Fortify on Demand will automatically set bugs to the status listed in the following table once the linked issues have been marked as **Fixed Validated** or **Suppressed**. A bug that is linked to multiple issues will not be closed unless all issues are **Fixed Validated** or **Suppressed**.

Bug Tracker	Closed Status
ALM Octane	Fixed (phase.defect.fixed)
ALM	Fixed
Jira	Done
Azure DevOps/Azure DevOps Server	Resolved
Bugzilla	Status: Resolved, Resolution: Fixed

**Note:** Fortify on Demand does not reopen bugs that are linked to reopened issues.

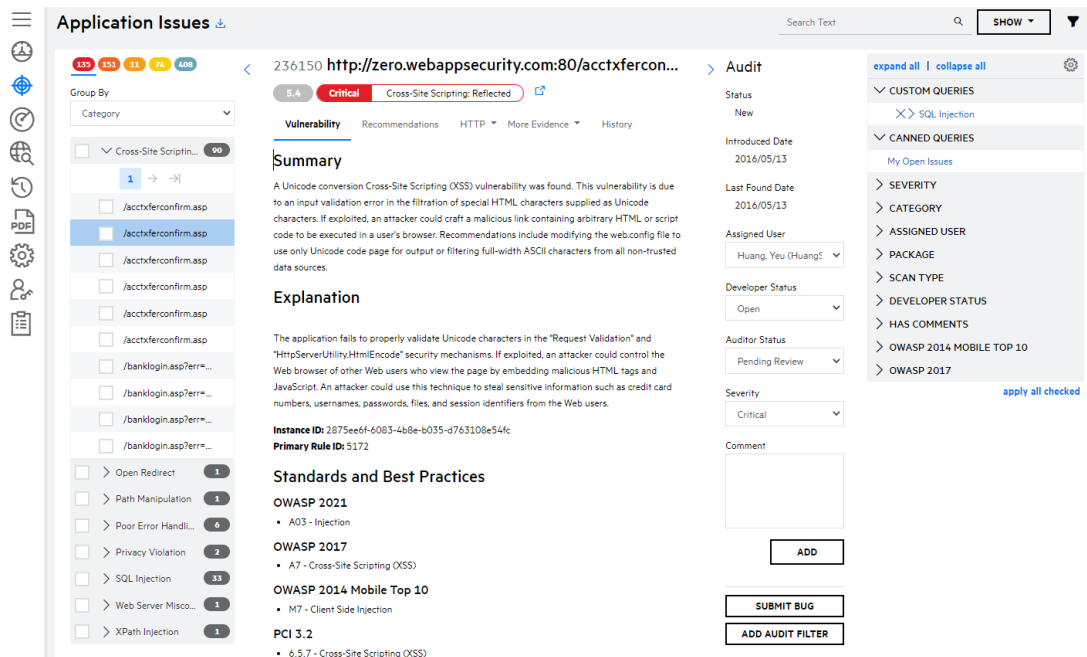
12. Click **Save**.  
Your bug tracker settings are saved.

## Submitting Issues to the Bug Tracker

Once bug tracker integration is configured for an application, a user with Application Access and Edit Issues permissions can submit Fortify on Demand issues as bugs to the bug tracker. The portal prevents issues from being submitted more than once.

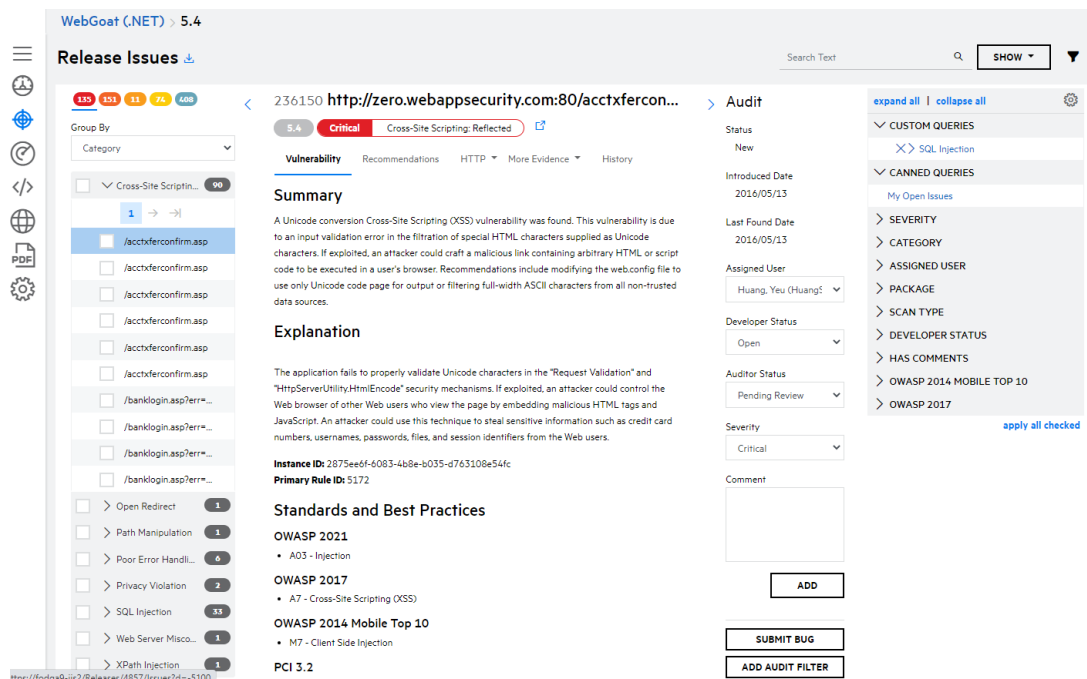
To submit issues to the bug tracker:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application with issues that you want to submit to a bug tracker.  
The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page:
  - To navigate to the Application Issues page:
    - i. Click **Issues**.  
The Application Issues page appears.



- To navigate to the Release Issues page:
  - i. Click the name of a release.
  - ii. Click **Issues**.

The Release Issues page appears.



4. In the navigation panel, select one or more issues that you want to submit. To batch submit issues, select the check boxes next to the issues you want to edit.



**Note:** If you are on the Application Issues page, selecting the check box next to an issue found in multiple releases selects all instances of the issue.

5. In the audit panel, click **Submit Bug**.

The Submit Bug to <bug\_tracker> window opens. The fields are populated with default values, including issue summaries. You can edit the default values.

ISSUE ID	PRIMARY LOCATION
237080	CustomerLogin.aspx.cs : 72

6. Fortify on Demand supports custom fields in ALM and Jira. If the bug tracker contains required custom fields, those fields appear in the **Custom Values (Required)** section. Complete the fields.

7. Click **Submit**.

You are returned to the Issues page. If the issue submission is pending, the audit panel displays a **Bug Pending** status. Once the issue submission is complete, the audit panel displays a **View Bug** button that links to the issue's bug tracker URL.

**Note:** When a release is copied, issues in the bug tracker are updated. Links to the newly copied issues are added to the issue descriptions in the bug tracker.

## Manually Linking an Issue

You can manually add a bug tracker link to the issue in the portal. This allows tenants using other bug trackers to track external bugs associated with Fortify on Demand issues.

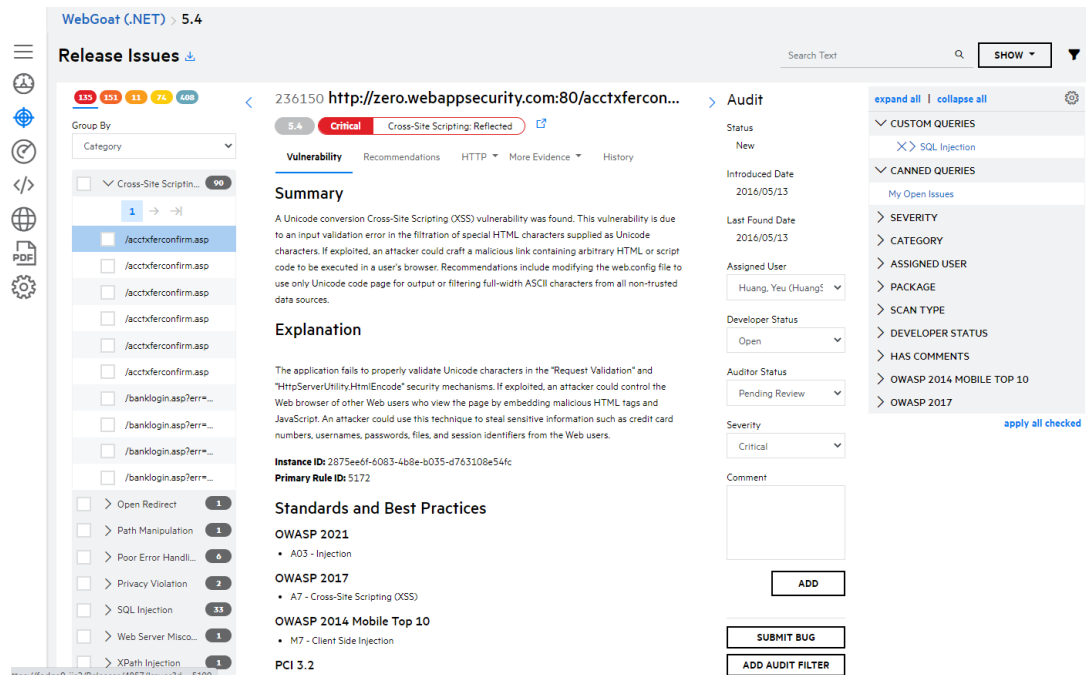
To link a Fortify on Demand issue with an unsupported bug tracker:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application with issues that you want to submit to a bug tracker.  
The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page:
  - To navigate to the Application Issues page:
    - i. Click **Issues**.  
The Application Issues page appears.

The screenshot displays the Fortify on Demand interface for an application issue. On the left, a sidebar shows a list of issues categorized by severity (Critical, High, Medium, Low) and type (Cross-Site Scripting, Open Redirect, Path Manipulation, etc.). The main content area shows a detailed view of a 'Critical' issue titled 'Cross-Site Scripting: Reflected' with a URL 'http://zero.webappsecurity.com:80/acctxfercon...'. The issue summary states: 'A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.' The explanation further details the application's failure to validate Unicode characters. Standards and Best Practices are listed, including OWASP 2021 (A03 - Injection), OWASP 2017 (A7 - Cross-Site Scripting (XSS)), OWASP 2014 Mobile Top 10 (M7 - Client Side Injection), and PCI 3.2 (6.5.7 - Cross-Site Scripting (XSS)). The right-hand 'Audit' panel shows the issue's status as 'New', introduced on 2016/05/13, and assigned to 'Huang, You (Huang)'. The severity is 'Critical'. There are buttons for 'ADD', 'SUBMIT BUG', and 'ADD AUDIT FILTER'.

- To navigate to the Release Issues page:
  - i. Click the name of a release.
  - ii. Click **Issues**.

The Release Issues page appears.



4. In the navigation panel, select one or more issues that you want to submit. To batch submit issues, select the check boxes next to the issues you want to edit.
5. Click **Submit Bug**.

The Submit Bug modal window appears.

### Submit Bug ✕

#### Bug tracker fields

Bug URL

Suggested Subject  
HPE FoD Security Vulnerability: 125823

Suggested Description  
Often Misused: Login - 125823 - http://fodqa9-iis2/Redirect/Issues/125823

#### Issues

Issue Name	Primary Location
Often Misused: Login	login.html

6. In the **Bug URL** field, type the bug tracker link that you want to add to the issue.
7. Click **Save**.

Once the issue submission is complete, the audit panel displays a **View Bug** button that links to the issue's bug tracker URL.

## Secure Code Warrior Integration

Fortify on Demand has partnered with Secure Code Warrior to provide free interactive training for supported vulnerability categories to Fortify on Demand customers. When viewing an issue, users can launch a training module from the **Launch Training** link in the **Recommendations** tab of the Issue Details panel.

A module consists of short, hands-on challenges in which users analyze software design and code for the vulnerability and then remediate or mitigate the vulnerability. Sample modules are available in all vulnerability categories supported by Secure Code Warrior. Modules are hierarchically organized by category, subcategory, and language.

Fortify on Demand does not share user and organization information with Secure Code Warrior. Additional training is available for purchase from Secure Code Warrior. For more information, see <https://www.securecodewarrior.com/>.

## Launching Secure Code Warrior Training

To launch Secure Code Warrior training for an issue:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click **Your Releases**.  
Your Releases page appears.
3. Select a release from your list.
4. Click **Issues**.  
The Release Issues page appears.
5. In the navigation panel, select an issue in an issue category where Secure Code Warrior training is available.
6. Select the **Recommendations** tab.

The screenshot displays the Fortify on Demand interface for a security issue. The top navigation bar shows 'WebGoat (.NET) > 5.4'. The main content area is titled 'Release Issues' and shows a list of issues. The selected issue is '237075 Downloads/WebGoat.NET-VS\_2010/WebGoat.N...' with a severity of 'Critical' and a category of 'Privacy Violation'. The 'Recommendations' tab is active, showing a recommendation to enforce good privacy management. Below the recommendation, there are 'Tips' for auditing privacy violations. On the right side, there is an 'Audit' panel with various filters and a 'LAUNCH TRAINING' button at the bottom.

7. In the **Interactive Training** section, click **Launch Training**.  
The Secure Code Warrior training module appears in a new window.

## Slack Integration for Notifications

Fortify on Demand offers Slack integration for posting notifications to Slack. Security Leads can configure one or more webhooks for the tenant. Once webhooks have been configured, Security Leads can enable posting notifications to Slack when creating notification subscriptions.

This section contain the following topics:

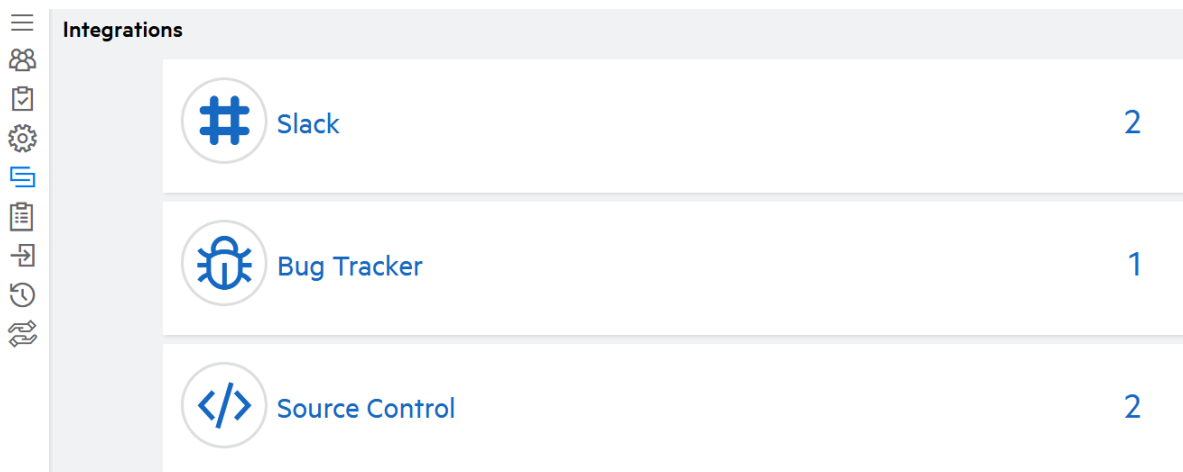
<a href="#">Configuring Slack Integration</a> .....	394
<a href="#">Deleting Slack Integration</a> .....	396

### Configuring Slack Integration

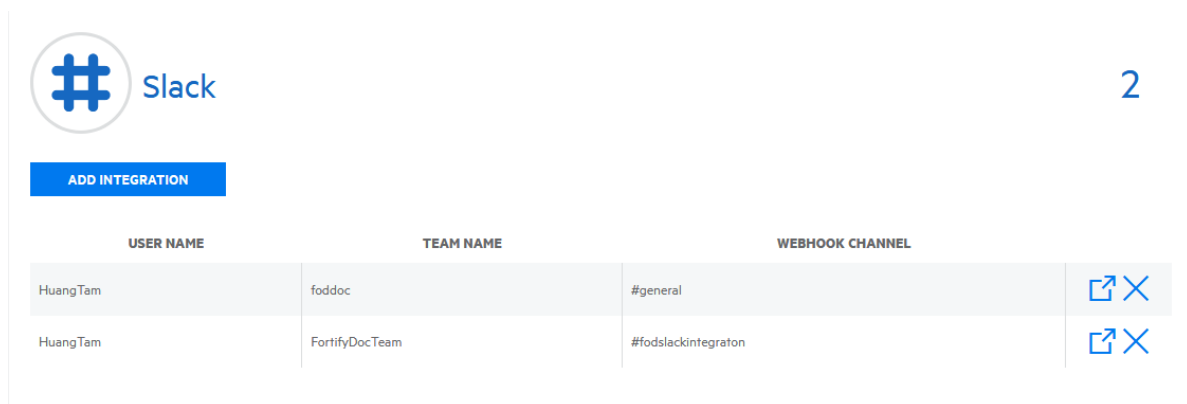
You can configure Slack integration by configuring one or more webhooks for the tenant.

To configure a webhook:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Click **Integrations**.  
The **Integrations** page appears.



3. Expand the **Slack** section.

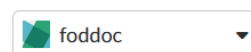


4. Click **Add Integration**.

- If you are currently not signed in to a workspace, you are redirected to the Slack workspace sign in page.
- If you are currently signed in to one or more workspaces, you are redirected to the authorization page.

**Note:** You must have permission to manage apps and integrations for the workspace

5. If you are not signed in to the workspace to which you want to connect, complete the sign-in process. Otherwise, skip to the next step.
6. Select the workspace, if not already selected, from the list on the top right side of the authorization page.



On foddoc, Fortify on Demand would like to:

Confirm your identity on foddoc

Post to

Cancel

Authorize

7. Select the channel or user direct message to which notifications will be posted. The available values are the channels and user accounts to which you have access.
8. Click **Authorize** to authorize Fortify on Demand to access your Slack account.

You are redirected to Fortify on Demand. A "Slack Integration Successful" message appears. You can now enable posting notifications to the channel. For more information on enabling posting notifications to Slack, see ["Creating an Individual Subscription" on page 31](#) and ["Creating a Global Subscription" on page 34](#).

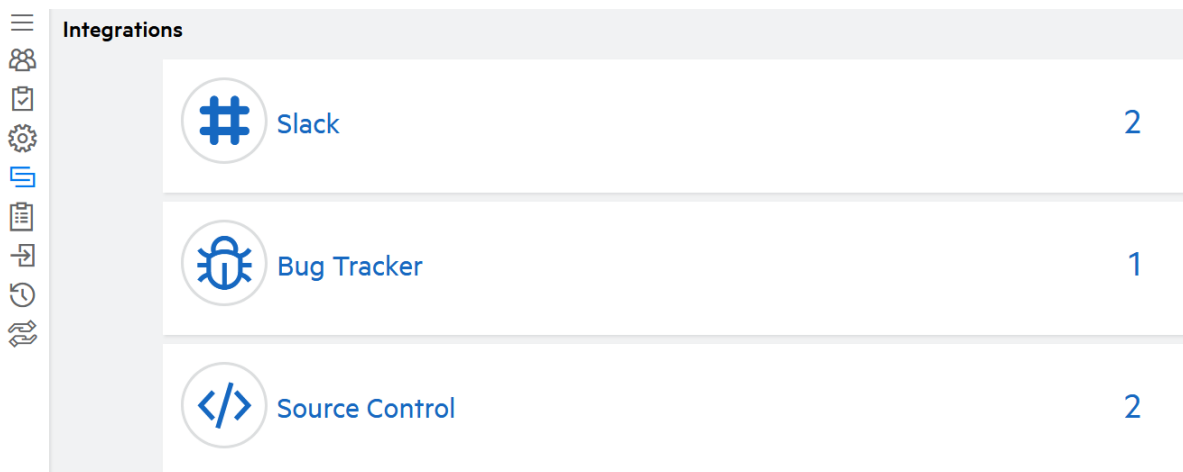
## Deleting Slack Integration

You can delete a Fortify on Demand Slack integration in the following ways:

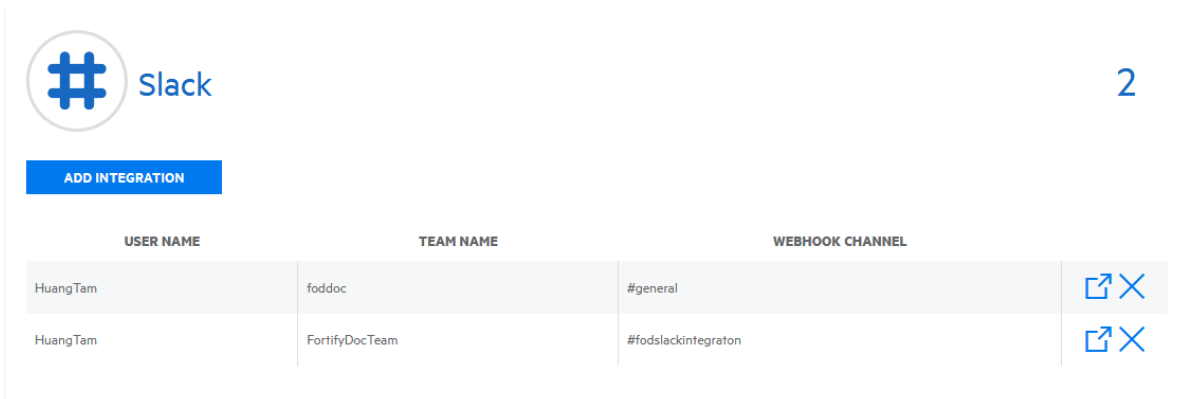
- Slack workspace owners and users who have permission to manage apps can remove specific authorizations or remove the Fortify on Demand application from the Slack workspace. This will cause posts to Slack to fail.
- Security Leads can delete webhooks in Fortify on Demand.

To delete a Slack integration:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Click **Integrations**.  
The **Integrations** page appears.



3. Expand the **Slack** section.



4. Perform the following tasks depending on your preferences and user permissions:



- To remove authorizations in Slack:
  - i. Click [↗](#) in the row of the webhook.  
You are redirected to the Fortify on Demand page in your workspace app directory.  
**Note:** You can also access the page from the Slack workspace.
  - ii. Remove specific authorizations or remove the application to remove all authorizations.  
For more information about removing applications from Slack, see the [Remove apps and custom integrations from your workspace](#) section of the Slack documentation.
- To remove a webhook in Fortify on Demand:
  - i. Click [✕](#) in the row of the webhook.  
The webhook is deleted.

## Source Control Integration

Fortify on Demand offers source control integration with the following source control platforms: GitHub and Bitbucket. This enables Fortify on Demand to pull source code from repositories on those platforms for static assessments.

The following languages are supported: Java, JavaScript, .NET, PHP, and Python. The requirements for preparing your code for upload to Fortify on Demand remain the same as described in ["Preparing Static Assessment Files" on page 89](#).

**Note:** For .NET and Java, Fortify recommends pre-compiling your files and uploading them to a release to ensure acceptance of the payload.

Source control integration is configured at the application level. Once it is configured, users can select a branch or release to upload when starting a static assessment.

This section contain the following topics:

<a href="#">Configuring Source Control Integration with Bitbucket</a> .....	397
<a href="#">Configuring Source Control Integration with GitHub</a> .....	398

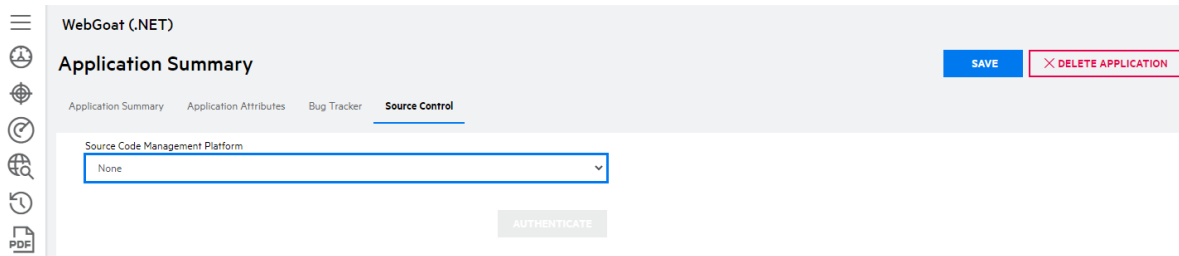
### Configuring Source Control Integration with Bitbucket

The Bitbucket integration requires the addition of an OAuth consumer in Bitbucket.

To configure source control integration with Bitbucket:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application that you want to edit.
3. Click **Settings**.  
The Application Summary page appears.

4. Select the **Source Control** tab.



5. Select **Bitbucket** from the **Source Code Management Platform** list.

6. In the **Client Key** and **Client Secret** fields, type the OAuth consumer key and secret as generated in Bitbucket.

To generate the key and secret, add an OAuth consumer in Bitbucket. When configuring the consumer, make sure to do the following:

- Set the callback URL to `https://<fod_domain>/Redirect/OAuth/`, where `<fod_domain>` is the Fortify on Demand domain and scheme.
  - US: `ams.fortify.com`
  - EMEA: `emea.fortify.com`
  - APAC: `apac.fortify.com`
  - FedRAMP: `fed.fortifygov.com`
- Assign read permission to the account, team membership, projects, and repositories.

For more information on adding an OAuth consumer in Bitbucket, see the [Integrate another application through OAuth](#) section of the Bitbucket documentation.

7. Click **Authenticate**.

If the authentication was successful, you are redirected to the Bitbucket site.

8. Authorize the Fortify on Demand application to access your account.

The **Team** and **Repository** fields are populated. The **Team** field lists your user account and all teams whose repositories you have access to.

9. Select the team that owns the repository that will be linked to the application from the **Team** list.

10. Select the repository from the **Repository** list.

11. Click **Save**.

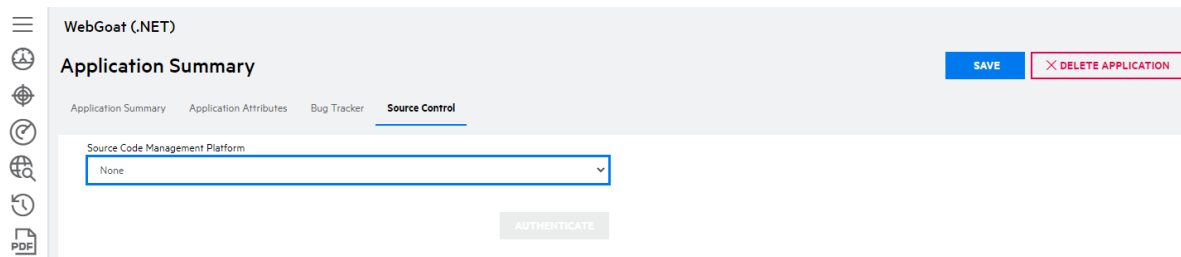
Your source control integration settings are saved.

## Configuring Source Control Integration with GitHub

The GitHub integration uses the Fortify on Demand Github marketplace application, which is unique to each data center. Source control integration with GitHub Enterprise is not available.

To configure source control integration with GitHub:

1. Select the **Applications** view.  
Your Applications page appears.
2. Click the name of the application that you want to edit.
3. Click **Settings**.  
The Application Summary page appears.
4. Select the **Source Control** tab.



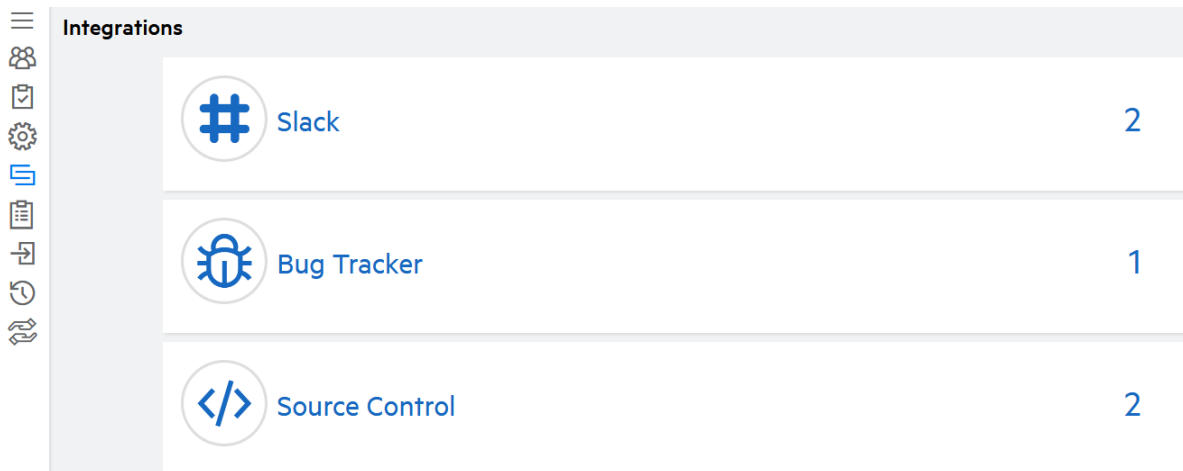
5. Select **GitHub** from the **Source Code Management Platform** list.
6. Click **Authenticate**.  
If the authentication was successful, you are redirected to the GitHub site.
7. Authorize the Fortify on Demand application to access your account.  
The **Organization** and **Repository** fields are populated. The **Organization** field lists your user account and all organizations whose repositories you have access to.
8. Select the organization that owns the repository that will be linked to the application from the **Organization** list.
9. Select the repository from the **Repository** list.
10. Click **Save**.  
Your source control integration settings are saved.

## Tracking Configured Integrations

Security Leads can track user-configured integrations with external tools across all applications in Fortify on Demand. Currently, the integrations available for tracking are: bug tracker, source control, and Slack.

To track user-configured integrations across the tenant:

1. Select the **Administration** view.  
The **User Management** page appears.
2. Click **Integrations**.  
The **Integrations** page appears.



3. Expand the sections that you want to view.

**Slack** 3

**ADD INTEGRATION**

USER NAME	TEAM NAME	WEBHOOK CHANNEL	
HuangTam	foddoc	#general	<a href="#">↗</a> <a href="#">✕</a>
HuangTam	FortifyDocTeam	#fodslackintegraton	<a href="#">↗</a> <a href="#">✕</a>
HuangTam	Fortify	@yeu-li.huang729	<a href="#">↗</a> <a href="#">✕</a>

---

**Bug Tracker** 1

APPLICATION	BUG TRACKER	USER NAME	URL
WebGoat (.NET)	Atlassian JIRA	TAMUser	http://fodqa-jira:8080/

---

**Source Control** 2

APPLICATION	MANAGEMENT PLATFORM
Test Web App	GitHub
WebGoat (.NET)	GitHub

4. You can perform the following actions:

- Slack: Click the links in the row of a webhook to remove specific authorizations or delete the webhook. For more information, see "[Deleting Slack Integration](#)" on page 396.
- Bug Tracker: Click the link in an application row to be redirected to the application's bug tracker settings. For more information, see "[Bug Tracker Integration](#)" on page 384.
- Source Control: Click the link in an application row to be redirected to the application's source control settings. For more information, see "[Source Control Integration](#)" on page 397


## Training Courses

Fortify on Demand has partnered with Security Innovation to provide secure development training courses. Review your contract to verify if they are included. If you are interested in adding courses, contact your sales representative.

This feature requires pop-ups and cookies to be enabled for the portal.

### Viewing Training Courses

To view your assigned training courses:

1. Click the  icon on the portal toolbar.

The Training page appears. The Courses tab displays the list of your assigned courses with the following information: course name, parent curriculum, module ID, course completion status, last attempted date, passed date, and course link.

Training									
Courses			Report	Assignment	Search Text				Q
COURSE NAME	CURRICULUM	MODULE ID	STATUS	LAST ATTEMPTED DATE	PASSED DATE				
AWA 101 - Fundamentals of Application Security	Fundamental	12	Incomplete	2019/02/26	2018/05/17	<a href="#">Start Course</a>	<a href="#">Resume Course</a>		
COD 101 - Fundamentals of Secure Development	Fundamental	13	Browsed	2019/02/16	2019/02/16				
COD 153 - Fundamentals of Secure AJAX Code	Fundamental	11				<a href="#">Start Course</a>			
IC	Miscellaneous	2	Incomplete	2019/02/16		<a href="#">Start Course</a>	<a href="#">Resume Course</a>		

2. Perform one of the following actions:

- Click the **Start Course** link in the row of a course to start the course.

Starting a course will reset the completion status but not the passed date. Close the course window when you are done to ensure results are properly recorded.

- Click the **Resume Course** link in the row of a course to continue from where you left off.
- Click the **Browse Course** link in the row of a course to view the contents without affecting the completion status or the passed date.

A confirmation message appears.


3. Click **Yes**.











The course appears in a new window.

## Assigning Training Courses


You can assign training courses available to your tenant to yourself. In addition, users with the **Manage Users** permissions can assign training courses to all active users in the tenant. Courses are grouped into different types of curricula and are assigned as a curriculum.

To assign training courses to yourself or another user:

1. Click the  icon on the portal toolbar.  
The Training page appears.
2. Select the **Assignment** tab.

Training						
Courses		Report		Assignment		
Search Text <input type="text"/>						
USER NAME	FIRST NAME	LAST NAME	EMAIL	ROLE	COURSE CURRICULUM	
AndyTest	Andrew	Schmit	andrew.schmit@hpe.com	Security Lead	Creating Secure Code, Miscellaneous	
dwayneAppLead	Dwayne	Whiteside	Dwayne.Whiteside@hpe.com	Application Lead	Creating Secure Code, Miscellaneous	
DwayneDev	Dwayne	Whiteside	Dwayne.whiteside1@hpe.com	Developer	Creating Secure Code, Fundamental	
DwayneExec	Dwayne	Whiteside	dwayne.whiteside2@hpe.com	Executive		
DwayneLeadDev	Dwayne	Whiteside	dwayne.whiteside3@hpe.com	Lead Developer		
DwaynePWtest	Dwayne	Whiteside	dwayne.whiteside@hpe.com	Developer	Miscellaneous	
dwayneRev	Dwayne	Whiteside	Dwayne.Whiteside3@hp.com	Reviewer		
DwayneSecLead	Dwayne	Whiteside	DWhiteside@hp.com	Security Lead	Fundamental	
tcappetto_dev	Tim	Cappetto	tcappetto@hpe.com	Developer	Creating Secure Code	
tcappetto_seclead	Tim	Cappetto	tcappetto2@hpe.com	Security Lead		


If your role has the **Manage Users** permission, the list of active users and their assigned curricula in the tenant appears. Otherwise, you only see your user account and assigned curricula.

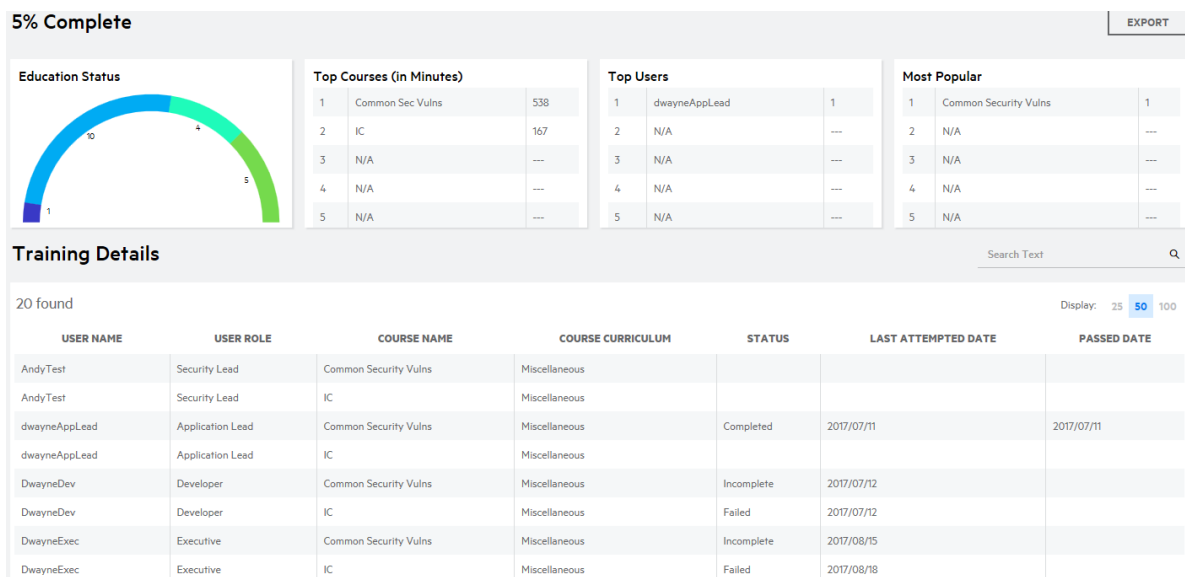
3. Click  next to a user.  
The Course Curriculum modal window appears.
4. Select the check boxes next to the curricula that you want to assign to the user.  
Click **Save**.  
The **Assignment** tab displays the saved changes.

## Viewing the Training Report

Users with the **Manage Users** permission can track user progress in assigned training courses across the tenant by viewing the training progress report. The report provides a tenant-level summary of user activity and a list of course completion statuses per user.

To view the training report:

1. Click the  icon on the portal toolbar.  
The Training page appears.
2. Select the **Report** tab.



The tab displays the following information:

- The percentage of assigned courses that were completed
  - Charts summarizing user progress and trends:
    - **Education Status:** the number of courses that are completed, in progress, or have not been started
    - **Top Courses:** the most active courses in terms of minutes spent
    - **Top Users:** the most active users in terms of courses taken
    - **Most Popular:** the courses that have been taken the most
  - The **Training Details** grid displaying in each row the tenant user, the assigned course, the course progress status, the last course access date, and the last course completion date.
3. Click **Export** to export the **Training Details** grid as a CSV file. Search results are applied to the export.

## Webhooks

Webhooks provide a way for notifications to be delivered to an external web server when scans are updated in Fortify on Demand. Users with the **Configure Webhooks** permission can configure webhooks to trigger when a subscribed event occurs. The following events are available: scan start, scan pause, scan resumption, scan cancellation, and scan completion. When an event to which a webhook is subscribed occurs, Fortify on Demand sends an HTTP POST payload to the webhook's configured URL. Webhooks can be used in place of polling in CI/CD pipelines that incorporate scanning.

This section contains the following topics:

[Configuring a Webhook](#) ..... 404

Webhook Requests and Responses .....406

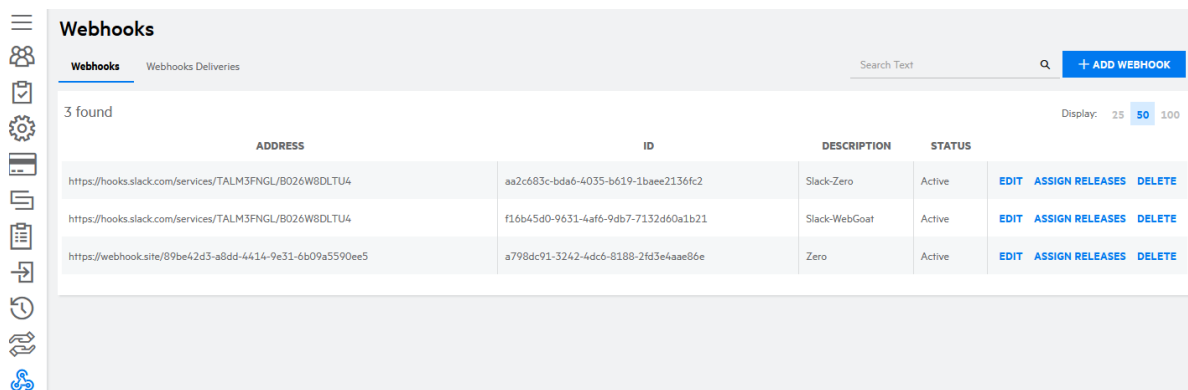
Viewing Webhook Deliveries .....408

## Configuring a Webhook

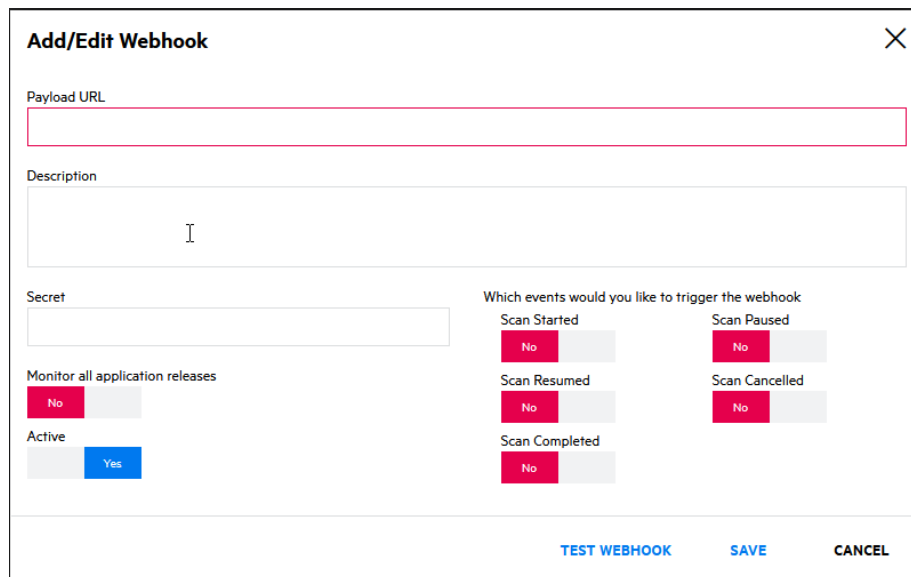
Users with the **Configure Webhooks** permission can configure webhooks for the tenant. A webhook must be assigned to a minimum of one release.

To configure a webhook:

1. Select the **Administration** view.  
The User Management page appears.
2. Click **Webhooks**.  
The Webhooks page appears.



3. Click **Add Webhooks**.  
The Add/Edit Webhooks window appears.



4. Complete the fields as needed. Fields are required, unless otherwise noted.



Field	Description
Payload URL	Type the URL of the server that will receive the webhook POST requests. For example, <code>https://7e9ea9dc.ngrok.io/payload</code> .
Description	(Optional) Type a phrase that describes the webhook.
Secret	<p>(Optional) Type a secret that can be used to validate that webhook requests sent to the payload URL are from Fortify on Demand. The HMAC-SHA256 algorithm is used in combination with the secret to calculate a hash of the payload body. The output is the HMAC and is included in the header of a request as X-FOD-Signature.</p> <p><b>Tip:</b> To validate the webhook request, calculate the HMAC by hashing the raw payload body using the HMAC-SHA256 algorithm in combination with the secret, then hex-encoding the hash. Verify that the output matches the value of X-FOD-Signature.</p>
Monitor all application releases	<ul style="list-style-type: none"> <li>• Set to <b>Yes</b> to monitor all application releases.</li> <li>• Set to <b>No</b> to monitor individual releases (default). You can specify releases to monitor after the webhook has been configured.</li> </ul>
Active	<ul style="list-style-type: none"> <li>• Set to <b>Yes</b> to enable the delivery of webhook requests (default).</li> <li>• Set to <b>No</b> to disable the delivery of webhook requests.</li> </ul>

5. Select which scan events will trigger the webhook.
6. Click **Test Webhook** to ping the payload URL.  
A "Successfully sent a ping event" message appears if the webhook was configured correctly.
7. Click **Save**.  
The new webhook appears in the list of webhooks.

**Note:** You can search webhooks by address, description and full ID. Partial string match is supported for address and description.

8. If you chose to monitor individual releases, click **Edit** in the row of the webhook.  
The Assign Releases window appears.

**Assign Releases** [X]

Selected Available Search [Q]

13 found Display: 25 50 100

	APPLICATION	RELEASE
<input type="checkbox"/>	iGoat Android (JAVA)	2.4
<input type="checkbox"/>	iGoat iOS (Objective-C)	2.4
<input type="checkbox"/>	iGoat iOS (Objective-C)	3.0
<input type="checkbox"/>	Jeopardy (PHP)	3.1
<input type="checkbox"/>	Jeopardy (PHP)	3.2
<input type="checkbox"/>	OpenSSL (C Source)	1.0.2a
<input type="checkbox"/>	Petstore	v1
<input type="checkbox"/>	Rubix (JAVA-No Source)	0.1
<input type="checkbox"/>	Swagger Petstore	v1
<input type="checkbox"/>	WebGoat	8.0
<input type="checkbox"/>	WebGoat (.NET)	5.4
<input type="checkbox"/>	Zero	v1
<input type="checkbox"/>	Zero Security (COBOL)	12.6.8

[SAVE] [CANCEL]

9. Select the releases that the webhook will monitor and click **Save**.  
The webhook is now assigned to the selected releases.

## Webhook Requests and Responses

Fortify on Demand sends information about webhook events as HTTP POST requests with the JSON payload as the body of the request.

**Note:** SSL verification is enabled by default. If the payload Url is HTTPS, Fortify on Demand will verify SSL certificates when sending webhook requests.

### Request Example

The following example shows a request with a hash signature in the header as X-FOD-Signature and the JSON payload.

Header:

```
connection: close
expect: 100-continue
content-length: 324
host: webhook.site
content-type: application/json; charset=utf-8
x-fod-signature:
4F837B0AE04303E975BBBCF9FFBBC09E0016013835757BD611C20F7930711980F
x-fod-deliveryid: f8d97b5e-4cae-414b-aa84-8de766f8116f
```

Payload:

```
{
  "deliveryId": "f8d97b5e-4cae-414b-aa84-8de766f8116f",
  "eventName": "scan_started",
  "payload": {
    "scanId": 31278,
    "tenantId": 1126,
    "applicationId": 14155,
    "applicationName": "Zero",
    "releaseId": 16149,
    "releaseName": "v1",
    "scanType": "dynamic"
  },
  "webhookId": "a798dc91-3242-4dc6-8188-2fd3e4aae86e",
  "triggeredAt": "2021-07-02T16:08:28.5496187Z"
}
```

### Response Example:

The following example shows the response received by Fortify on Demand.

```
Transfer-Encoding = chunked
Vary = Accept-Encoding
X-Request-Id = e9cbce0c-108f-46e9-b2cc-89f6f0104dca
X-Token-Id = 89be42d3-a8dd-4414-9e31-6b09a5590ee5
Cache-Control = no-cache, private
Date = Fri, 02 Jul 2021 16:08:29 GMT
Set-Cookie = laravel_session=CRuQJLoiFx9ay1UV88ufH83vCOjq1PL0JN0wY59v;
expires=Fri, 02-Jul-2021 18:08:29 GMT; Max-Age=7200; path=/; httponly
Server = nginx/1.14.2
```

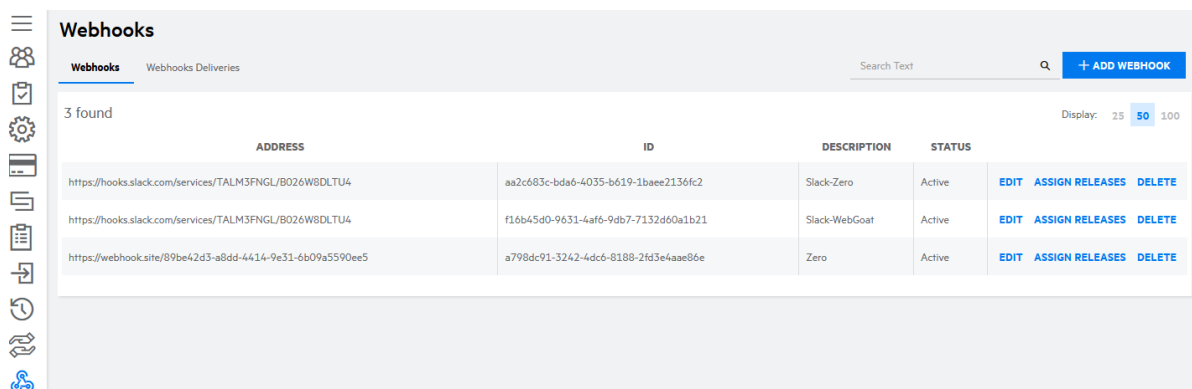
## Viewing Webhook Deliveries

Users with the **Configure Webhooks** permission can view details of the webhook deliveries, including the HTTP request (including the payload) and the response.

To view the list of webhook deliveries:

1. Select the **Administration** view.  
The User Management page appears.

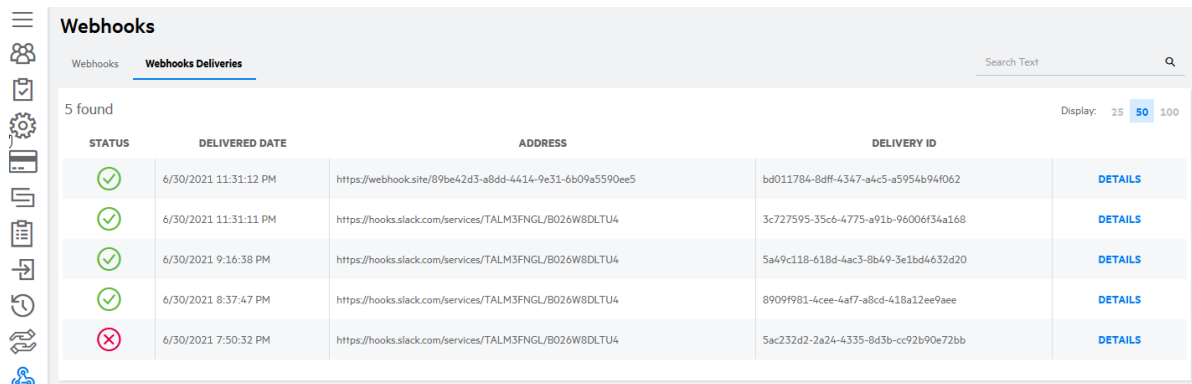
2. Click **Webhooks**.  
The Webhooks page appears.



The screenshot shows the 'Webhooks' page with a search bar and a '+ ADD WEBHOOK' button. A table lists 3 webhooks with columns for ADDRESS, ID, DESCRIPTION, and STATUS. Each row has links for EDIT, ASSIGN RELEASES, and DELETE.

ADDRESS	ID	DESCRIPTION	STATUS	
https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	aa2c683c-bda6-4035-b619-1baee2136fc2	Slack-Zero	Active	<a href="#">EDIT</a> <a href="#">ASSIGN RELEASES</a> <a href="#">DELETE</a>
https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	f16b45d0-9631-4af6-9db7-7132d60a1b21	Slack-WebGoat	Active	<a href="#">EDIT</a> <a href="#">ASSIGN RELEASES</a> <a href="#">DELETE</a>
https://webhook.site/89be42d3-a8dd-4414-9e31-6b09a5590ee5	a798dc91-3242-4dc6-8188-2fd3e4aae86e	Zero	Active	<a href="#">EDIT</a> <a href="#">ASSIGN RELEASES</a> <a href="#">DELETE</a>

3. Select the **Webhook Deliveries** tab.  
A list of webhook deliveries appear.



The screenshot shows the 'Webhook Deliveries' page with a search bar. A table lists 5 deliveries with columns for STATUS, DELIVERED DATE, ADDRESS, and DELIVERY ID. Each row has a 'DETAILS' link.

STATUS	DELIVERED DATE	ADDRESS	DELIVERY ID	
✓	6/30/2021 11:31:12 PM	https://webhook.site/89be42d3-a8dd-4414-9e31-6b09a5590ee5	bd011784-8dff-4347-a4c5-a5954b94f062	<a href="#">DETAILS</a>
✓	6/30/2021 11:31:11 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	3c727595-35c6-4775-a91b-96006f34a168	<a href="#">DETAILS</a>
✓	6/30/2021 9:16:38 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	5a49c118-618d-4ac3-8b49-3e1bd4632d20	<a href="#">DETAILS</a>
✓	6/30/2021 8:37:47 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	8909f81-4cee-4af7-a8cd-418a12ee9aee	<a href="#">DETAILS</a>
✗	6/30/2021 7:50:32 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	5ac232d2-2a24-4335-8d3b-cc92b90e72bb	<a href="#">DETAILS</a>

**Note:** You can search webhook deliveries by address (partial string match supported) and full ID.

4. Click **Details** in the row of a webhook delivery.  
The Webhook Delivery window appears, containing the HTTP request and the response.  
Request:

### Webhook Delivery

	8909f981-4cee-4af7-a8cd-418a12ee9aee	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	6/30/2021, 11:37:47 PM
--	--------------------------------------	--	------------------------

**Request**    Response

#### Headers

```
X-FOD-DeliveryId = 8909f981-4cee-4af7-a8cd-418a12ee9aee  
X-FOD-Signature = 6B5D3EF8315ADFE4728ADCC40ACCE437CB5F215CF8D386B3622B5C6A3EC53A4D
```

#### Content

```
["deliveryId":"8909f981-4cee-4af7-a8cd-418a12ee9aee","eventName":"scan_completed","payload":  
{"scanId":"31246","tenantId":"1126","applicationId":"12237","applicationName":"WebGoat","releaseId":"12672","releaseName":"8.0","scanType":"static","notes":"Scan Job Id 12549 : FPR  
IMPORT SUCCESSFUL AND AUTOMATICALLY RELEASED"},"webhookId":"f16b45d0-9631-4af6-9db7-7132d60a1b21","triggeredAt":"2021-07-01T03:37:47.3105424Z"}]
```

Response:

### Webhook Delivery

	3c727595-35c6-4775-a91b-96006f34a168	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	7/1/2021, 2:31:11 AM
--	--------------------------------------	--	----------------------

Request    **Response**

#### Headers

```
x-frame-options = SAMEORIGIN  
x-xss-protection = 0  
vary = Accept-Encoding  
referrer-policy = no-referrer  
x-slack-backend = r  
strict-transport-security = max-age=31536000; includeSubDomains; preload  
Date = Thu, 01 Jul 2021 06:31:50 GMT
```

#### Content

# Chapter 11: Policies and Support

For more information on Fortify on Demand, review the Fortify on Demand policies and support resources.

This section contains the following topics:

- [Maintenance Schedule and Software Updates](#) ..... 410
- [Data Retention Policy](#) ..... 411
- [Getting Support](#) ..... 412

## Maintenance Schedule and Software Updates

Fortify on Demand provides the following information regarding maintenance schedule and software updates.

### Maintenance Schedule

To help customers plan for scheduled maintenance, Fortify on Demand reserves predefined time frames to be used on an as-needed basis: a weekly two (2) hour window (Thursday 00:00 to 02:00) and one (1) monthly forty-eight (48) hour window (Saturday 00:00 to Sunday 00:00). These maintenance windows will be used on an as-needed basis and in the vast majority of instances will have no impact on users' ability to access or leverage functionality in Fortify on Demand.

The maintenance window for each data center is set using the following time zones:

Data Center	Maintenance Time Zone
AMS	US Eastern Time
EMEA	Greenwich Mean Time
APAC	Australian Eastern Time

For additional details about scheduled maintenance in other environments, contact a TAM.

### Software Updates

Fortify on Demand determines whether and when to develop, release, and apply software upgrades to the Fortify on Demand platform and/or supporting components. Major releases are typically made available on a quarterly basis, with minor releases and patches made available on an as-needed basis. Unless Fortify on Demand anticipates a service interruption due to a software upgrade, Fortify on

Demand may implement a SaaS upgrade at any time without notice to the customer. Fortify on Demand aims to use the monthly scheduled maintenance window to apply major software updates.

Security content updates to expand and improve Fortify on Demand's ability to identify vulnerabilities are a key component of the Fortify on Demand service. Security content updates are developed by the Fortify Software Security Research (SSR) team and are typically released at the end of each calendar quarter. Fortify on Demand typically deploys updated security content within several weeks of public availability. Security content updates may be deployed outside of the quarterly updates in response to significant new threats or zero-day vulnerabilities. Fortify recommends Fortify users to stay up-to-date with the latest security intelligence by following the Micro Focus Security Research blog at <https://community.microfocus.com/cyberres/b/off-by-on-software-security-blog>.

## Data Retention Policy

Fortify on Demand has implemented the following data retention policy for customers as of the v18.4 release. Fortify on Demand encourages customers to review and download any files outside the data retention windows that they wish to retain.

Resource	File Type	Retention Period
Data exports (Application and Release Issues pages)	.csv	7 days
Source code	.zip	15 days
Mobile application binaries	.ipa, .apk	30 days
Notifications	-	3 months
Data exports (global Reports page)	.csv	3 months
Event log	.csv	13 months
User-generated reports	.pdf, .html	2 years
Fortify scan result files	.fpr	2 years
Software bill of materials (SBOM)	.json	2 years
Site trees	.csv	2 years
Application data	-	Customer controlled*
Release data	-	Customer controlled*
Issue data	-	Customer controlled*
User data	-	Customer controlled*

\*The customer is responsible for creation and deletion of the specified data as long as the customer maintains an active status with Fortify on Demand. The customer can delete an application, release, or user at any time. Issue data associated with an application or release is also deleted. Upon termination of the Fortify on Demand service, the termination data retrieval period is 30 days.

For more information, please contact a TAM.

## Getting Support

Fortify on Demand offers support through self-service resources and the Fortify on Demand Help Center, staffed 24/7 by a dedicated support team of TAMs. The self-service resources include video demonstrations, a knowledge base, and product documentation. If you did not find what you were looking for, start a live chat with a TAM or submit a support ticket in the Help Center. You can call support at 800.893.8141 or 650.800.3233 if internet access is unavailable.

This section contains the following topics:

## Accessing Support Resources

You can access support resources through the portal. The portal contains direct links to how-to videos, online help, live chat, and the Help Center. The Help Center is Fortify on Demand's support ticket system. It also hosts PDF versions of the User Guide and Release Notes, the knowledge base, and video library.

**Note:** You can directly log in to the Help Center through the relevant URL using your Fortify on Demand credentials:

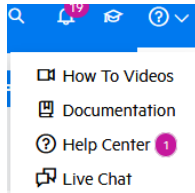
- AMS: <https://helpcenter.ams.fortify.com>
- EMEA: <https://helpcenter.emea.fortify.com>
- APAC: <https://helpcenter.apac.fortify.com>

To access support resources:

1. Click the help menu and select one of the following:
  - **How To Videos** - redirects you to video demonstrations on using Fortify on Demand
  - **Documentation** - opens the online help
  - **Help Center** - redirects you to the Help Center
  - **Live Chat** - opens the Live Chat window where you can chat with a Fortify on Demand TAM



24/7



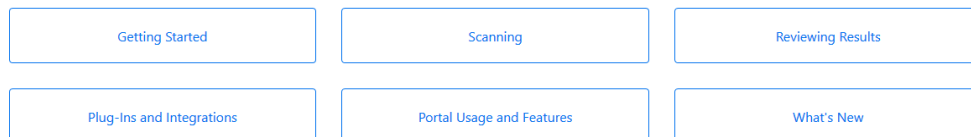
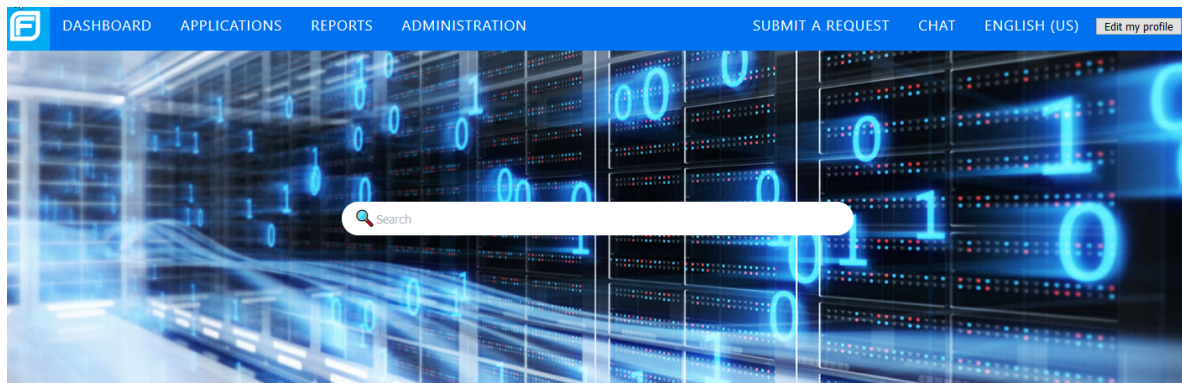
## Submitting a Help Center Ticket

Submit a support ticket in the Help Center.

To submit a Help Center ticket:

1. Click the help menu and select **Help Center**.

The Help Center opens in a new window.



2. Click **Submit a Ticket**.  
The **Submit A Request** form appears.
3. Select the ticket type from the drop-down list:
  - **Create Ticket** - get help with a general product question or a tenant-specific issue
  - **FoD Defect Submission** - report a Fortify on Demand bug or issue
  - **FoD Enhancement Submission** - request an enhancement
4. Complete the fields displayed for the selected ticket type. Provide as many details as possible.
5. Click **Submit**.  
A message at the top of the page indicates that your Help Center ticket was submitted.

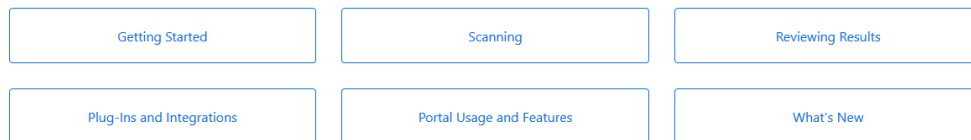
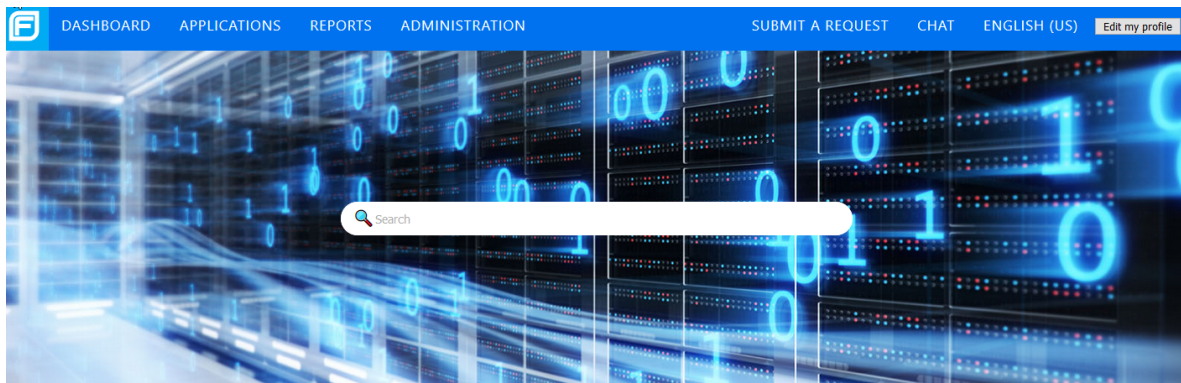
## Tracking your Help Center Tickets

You can track support tickets submitted for your tenant in the Help Center. You can only view tickets that you have submitted, are assigned to, and are copied on (if you are on an application's notification list you are automatically added to tickets linked with the application).

To track your Help Center tickets:

1. Click the help menu and select **Help Center**.

You are redirected to the Help Center.



2. Click **View Tickets**.

Your tickets are displayed. Tickets have one of the following statuses:

- **Open** - Your request has been received and assigned to a TAM who is working to resolve it.
  - **Awaiting your reply** - The assigned TAM has a follow-up question for you. Tickets that are set to Pending typically remain that way until you respond and provide the information the TAM needs to continue resolving the ticket.
  - **Solved** - The TAM has resolved the support issue. Solved tickets are closed automatically seven days after they have been set to Solved. Until a ticket is closed, you can reopen the ticket.
  - **Closed** - The ticket is complete and can't be reopened. If you need additional support for the original ticket, create a follow-up request.
3. To limit the number of tickets you view, filter your list with the **Status** filters:
    - **Any** - Show all tickets.
    - **Open** - Show tickets that the Fortify on Demand team is still working on.

- **Awaiting your reply**- Show tickets that require action from your organization.
- **Solved** - Show tickets that have been resolved.

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email.

**Note:** If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Micro Focus Fortify Customer Support at <https://www.microfocus.com/support> so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

## **Feedback on User Guide (Fortify on Demand 22.4)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [fortifydocteam@microfocus.com](mailto:fortifydocteam@microfocus.com).

We appreciate your feedback!