OpenText™ Fortify on Demand

User guide

Version 26.4

PDF Generated on October 30, 2026

© Copyright 2026 Open Text

Table of Contents

User guide 6
1 Introduction 6
1.1 Security rating system 7
1.2 Service level objectives 10
2 Get started 10
2.1 Prerequisites 11
2.2 Access the portal 11
2.3 Navigate the portal 12
2.4 Manage account settings 14
2.5 Manage notifications 15
2.5.1 Manage subscriptions 16
2.6 Switch tenants 18
3 Manage 18
3.1 Application 18
3.1.1 Create an application 20
3.1.2 View application details 21
3.1.3 Edit application settings 23
3.1.4 Manage user assignment 24
3.1.5 Manage applications in the tenant 25
3.1.6 View event log 28
3.1.7 Delete an application 29
3.2 Release 29
3.2.1 Create a release 30
3.2.2 View release details 31
3.2.3 Edit release settings 36
3.2.4 Manage releases in the tenant 36
3.2.5 Delete a release 39
3.3 Search applications and releases 40
3.4 Create deep links 40
4 Run assessments 41
4.1 Static assessments 41
4.1.1 OpenText SAST requirements 41
4.1.1.1 Supported languages 41
4.1.1.2 Supported compilers 44
4.1.1.3 Supported libraries, frameworks, and technologies 44
4.1.2 Prepare static assessment files 50
4.1.2.1 Prerequisites 51
4.1.2.2 Install Fortify ScanCentral SAST client 51
4.1.2.3 Prepare .NET application files 52
4.1.2.4 Prepare Java application files 53
4.1.2.5 Prepare JavaScript/HTML/XML files 55
4.1.2.6 Prepare Kotlin application files 55

4.1.2.7 Prepare ABAP(SAP) application files 56
4.1.2.8 Prepare C and C++ application files 58
4.1.2.9 Prepare Classic ASP, VBScript, and Visual Basic application files 59
4.1.2.10 Prepare Dart and Flutter application files 60
4.1.2.11 Prepare ColdFusion Markup Language (CFML) application files 60
4.1.2.12 Prepare COBOL application files 61
4.1.2.13 Prepare Dockerfiles and Infrastructure as Code (IaC) files 61
4.1.2.14 Prepare Go application files 62
4.1.2.15 Prepare PHP application files 63
4.1.2.16 Prepare Python application files 63
4.1.2.17 Prepare Ruby application files 64
4.1.2.18 Prepare Solidity application files 64
4.1.2.19 Prepare Salesforce (Apex and Visualforce) application files 65
4.1.2.20 Prepare Scala application files 65
4.1.2.21 Prepare Android application files (source code) 65
4.1.2.22 Prepare iOS application files (source code) 66
4.1.3 Configure a static scan 66
4.1.4 Upload a static assessment payload 72
4.1.5 Static assessment payload validation 73
4.2 Open Source software composition analysis 74
4.2.1 Prepare Open Source assessment files 75
4.2.2 Upload a payload through the Portal 79
4.2.3 View components in a release 79
4.2.4 View components in a tenant 80
4.3 Dynamic assessments 81
4.3.1 Prepare the Website for Dynamic testing 81
4.3.2 Prepare Web API files 82
4.3.3 Set up Fortify on Demand Connect 85
4.3.4 Configure a Dynamic scan 86
4.3.5 Schedule a Dynamic scan 107
4.3.6 Edit scan settings 107
4.4 Mobile assessments 108
4.4.1 Supported platforms and operating systems 108
4.4.2 Prepare mobile assessment files 109
4.4.3 Manage a scan 111
4.5 Entitlement consumption 114
4.6 Manage scans 115
4.6.1 View and navigate scans 115
4.6.2 Navigate the scans page 121
4.6.3 Filter Your Scans page 124
4.6.4 Check the scan status 125
4.6.5 Cancel a scan 126
4.6.6 Resume a scan 127
4.6.7 View tickets 127
5 Remediate vulnerabilities 128

5.1 Review issues 129
5.1.1 View issues 129
5.1.2 Navigate the issues page 130
5.1.3 Filter and group the issues page 135
5.1.4 Customize issue filters and groupings 139
5.1.5 Assign attributes for an issue 140
5.2 Issue details 140
5.2.1 Static scan issue 141
5.2.2 Open source scan issue 142
5.2.3 Dynamic scan issue 143
5.2.4 Mobile scan issue 143
5.3 Update issues 144
5.4 Audit issue remediation 147
5.5 Audit and remediation with Fortify Remediation Aviator 148
5.6 Audit templates 149
5.6.1 Create a global audit template 150
5.6.2 Create an application audit template 152
5.6.3 Create an application audit template filter for an issue 154
5.6.4 Audit template usage and examples 155
5.7 Dataflow cleanse rules 155
5.7.1 Create a global dataflow cleanse rule 156
5.7.2 Create an application dataflow cleanse rule 159
5.7.3 Dataflow cleanse rule usage and examples 160
5.8 Request a remediation scan 161
6 Dashboards and reports 161
6.1 Dashboards 161
6.1.1 Dashboard types 162
6.2 Reports 163
6.2.1 View reports 164
6.2.2 Generate a report 166
6.2.3 Schedule auto-generated reports 167
6.2.4 Templates 167
6.2.5 Data exports 169
7 Administration 171
7.1 Portal management 171
7.1.1 Configure user security 171
7.1.2 Manage API keys 174
7.1.3 Manage attributes 177
7.1.4 Manage networks 181
7.1.5 View entitlements 182
7.1.6 View administration event log 182
7.1.7 Configure SAST 183
7.2 User management 185
7.2.1 Roles and permissions 185
7.2.1.1 Default roles 185

7.2.1.2 Manage roles 187
7.2.1.3 Permissions 188
7.2.2 Manage users 192
7.2.3 Manage groups 195
7.2.4 Configure System for Cross-domain Identity Management (SCIM) 197
7.3 Policy management 198
7.4 Single sign-on (SSO) 200
7.4.1 Configure SSO 200
7.4.2 Configure encryption 203
7.4.3 Configure identity provider metadata 204
7.4.3.1 Configure SSO in the identity provider 205
7.4.4 Download the metadata 209
7.4.5 Troubleshoot failed logins 209
7.5 Vendor management 209
7.5.1 Initiate a relationship 210
7.5.2 Accept a relationship 210
7.5.3 Publish a report 211
8 API 211
8.1 API authentication 213
8.2 API scopes 215
8.3 API rate limits 216
8.4 Personal access tokens 218
9 Tools 220
9.1 CICD tools 221
9.2 IDE tools 222
9.3 Scan preparation and tracking tools 224
9.4 View and download tools 225
10 Integrations 225
10.1 Bug tracker integration 226
10.2 External scan integration 229
10.3 Secure Code Warrior integration 230
10.4 Slack integration for notifications 231
10.5 Source control integration 232
10.6 Track configured integrations 233
10.7 Webhooks 234
11 Training 237
12 Policies 238
13 Support 240

User guide

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

- Introduction
- Get started
- Manage
- Run assessments
- Remediate vulnerabilities
- Dashboards and reports
- Administration
- API
- Tools
- Integrations
- Training
- Policies
- Support

1. Introduction

OpenText 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. OpenText Fortify on Demand's software security testing incorporates advanced and updated application testing technologies with expert review, dedicated account management, and 24/7 support.

Services

An application submitted to OpenText Fortify on Demand undergoes a security assessment where it is analyzed for various software security vulnerabilities. OpenText Fortify on Demand offers static, dynamic, mobile, and open source assessments at several service levels.

- 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).
- An open source software composition analysis analyzes open source components in the payload.

The 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 audit is performed on scan results to ensure the highest possible degree of accuracy. Some assessments types include a manual audit.
- 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.

OpenText 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.

Pricing

OpenText Fortify on Demand 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

OpenText Fortify on Demand offers support through self-service resources and the OpenText Fortify on Demand Help Center, staffed 24/7 by a dedicated support team.

This section contains the following topics:

- Security rating system
- Service level objectives

1.1. Security rating system

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

Likelihood and Impact

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

Likelihood and impact

Rating	Rating description
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

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

Priority order

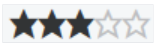
Priority level	Level description
Critical	Critical issues have high potential impact and high likelihood of occurring. Critical issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to an application. As such, immediately remediate critical issues.  **Example** SQL injection is 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.  **Example** Hard-coded password is 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.  **Example** Path manipulation is 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.  **Example** Dead code is 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. OpenText 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 OpenText 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.

Five-star rating assessment

Rating	Rating description
One star 	OpenText 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
Two stars 	OpenText 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.
Three stars 	OpenText 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.
Four stars 	OpenText 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.
Five stars 	OpenText Fortify on Demand awards five stars, the highest rating, to applications that have undergone a security review that identifies no issues.

1.2. 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 OpenText 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 business 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 Completing the Static Scan Setup, Completing the Dynamic Scan Setup, and Completing the Mobile Scan Setup.

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 according to OpenText Fortify on Demand best practice guidelines
- The application payload exceeds 1,000 MB

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

- The testing team is not provided continuous 24-hour per day access and fully operational test credentials to assess the application that is in scope
- The testing team 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 600 ms to an HTTP/HTTPS request
- Mobile binary is obfuscated or is not prepared according to OpenText Fortify on Demand best practice guidelines

2. Get started

OpenText Fortify on Demand is a cloud-based application security testing solution that helps organizations identify, prioritize, and remediate security vulnerabilities. Use this section to understand core functionality, navigate the platform, and get started with security assessments and vulnerability management. This guide provides the information you need to begin using Fortify on Demand effectively.

- Prerequisites
- Access the portal
- Navigate the portal

- Manage account settings
- Manage notifications
- Switch tenants

2.1. Prerequisites

Before you access OpenText Fortify on Demand, make sure that you have:

- An active internet connection.

Valid portal credentials

> **Note**
> You receive setup instructions in a welcome email. If you cannot find the email, check your spam or junk folder

- A Monitor with a minimum display resolution of 1280 x 720. A resolution of 1920 × 1080 is recommended.
- One of the following supported browsers installed:
  - Google Chrome (latest version)
  - Mozilla Firefox Quantum (latest version)
  - Safari on macOS (latest version)

    > **Note**
    > Safari on Windows is not supported.

  - Microsoft Edge (latest version)

2.2. Access the portal

You can access the portal after you receive your portal credentials.

Log in

To log in to the portal:

1. Enter the portal URL provided with your credentials in your browser's address bar.
   The login page opens.
2. Enter your **Username**, **Password**, and **Tenant** code.
   If you signed in through SSO within the last 30 days, the **SSO Login** option is available.
3. Click **Log in**.
   The portal landing page opens. If you have not configured a challenge question and answer, the **Account Settings** page opens instead.

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

Reset a password

Use this procedure if you forgot your password. To reset a password:

1. Click **Forgot Your Password?** on the login page.
   The **Forgot Password** page opens.
2. Enter your **Username** and **Tenant** code.
3. Click **Submit**.
   An email containing a password reset link is sent to the email address associated with your account.

4. Click the link in the email.
   The **Reset Password** page opens.

   > **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, enter the answer to your challenge question.
   If you have not configured a challenge question and answer, skip this step.
6. Enter and confirm your new password.
7. Click **OK**.
   The password is reset.

Log out

Log out of the portal from the portal toolbar settings. The portal automatically logs you out after 20 minutes of inactivity.

To log out of the portal:

1. Click your account name, then select **Log out**.

2.3. Navigate the portal

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

This table provides information about the tasks and action you can perform on the portal.

Portal tasks and action

Navigate tasks	Required action
Navigate to a parent view	Select the appropriate parent view.
Access account settings and additional resources	On the toolbar, click your account name.
Search the portal	On the toolbar, click search.
Access notifications	On the toolbar, click notifications.
Access training courses	On the toolbar, click training.
Access help resources	On the toolbar, click help to open the help menu.
Navigate to a page within a parent view	On the sidebar, click the appropriate navigation item.
Access context-sensitive help	Click. A new window opens that displays the help topic for the feature.
Sort page data	Click a column heading. An indicator in the heading shows the current sort field and sort order. Click the heading again to reverse the sort order.
Change the number of displayed items	Select **25**, **50**, or **100** items per page. **Note** The **Discovered** tab on the **Your Applications** page supports 250 and 500 items per page.
View another page of results	Click a page number or navigation arrow.

Search the portal

OpenText 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 search 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.

2.4. Manage account settings

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

Modify account settings

To edit your account settings:

1. Click your account name and select **Account Settings**.
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 formats are displayed in **MM/DD/YYYY**, **DD/MM/YYYY**, or **YYYY/MM/DD**
Time Format	Time format is displayed in **12 Hour AM/PM**, **24 Hour**
Language	Language displayed: **English**, **Español**, **日本語** **Note** Your reports are generated in your selected language.
Password Challenge Question	A list of password challenge questions
Password Challenge Answer	A case-insensitive answer to the selected password challenge question **Note** You cannot save your account changes unless you have set a password challenge question and answer.

3. Update your subscriptions in the **Email Subscriptions** section. Email subscriptions keep you up-to-date with OpenText Fortify on Demand events. You can sign up to receive notifications about releases and maintenance, security advisories, and relevant webinars and conferences.
4. To request for a new TOTP authenticator, click **Generate new QR code**. The Security Code screen appears.
    1. Scan the QR Code.
    2. Enter the TOTP verification code.
    3. Click **Submit** to verify the code.
5. Click **Save**.
   A confirmation message appears indicating that you have successfully saved your changes.

Change account password

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

Note

Passwords must:

- Be at least 16 characters long.
- Contain at least one uppercase letter.
- Contain at least one lowercase letter.
- Contain at least one number.
- Contain at least one special character.
- Not contain common or easily guessed password phrases.

To change your account password:

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

2.5. Manage notifications

OpenText 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 creation, updates, and deletion
- Release creation, updates including promotion of failing releases to production, and deletion
- Scan status updates
- Issue updates
- Report generation

View 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. On the portal toolbar, select **Notifications**.
   The **Notifications** page opens and displays your unread notifications.
2. To view notification details, select **View** in the notification's action column.
   The related application, release, or issue page opens.
3. To mark a notification as read, select **Mark as Read** in the notification's action column.
   You can also filter the notification list and select **Mark as Read** to update multiple notifications at once.

The notification moves to **Read Notifications** and is removed from the unread count.

4. To view notifications that you previously marked as read, select the **Read** tab.
   The list of read notifications appears.

2.5.1. Manage subscriptions

Users can create, edit, and delete individual subscriptions to receive notifications based on selected criteria. Security leads can also create, edit, and delete global subscriptions for all users, specific roles, or specific groups.

Create 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. On the portal toolbar, select **Notifications**.
   The Notifications page appears.
2. Click **Subscriptions**.
   A list of your individual subscriptions appears.
3. **Click +New Subscriptions.**
   The Create Subscription modal window opens.
4. Complete the fields. Fields are required unless otherwise noted.

Field	Description
Trigger	Select the trigger type from the list
Scope	Select the scope to which the trigger will apply from the list: **All Applications** (default), **Application**, **Application Type**, **Application Attribute**, **Business Criticality** and **All Releases Owned By Me**.
	(Optional) Type a note for the subscription.
Send Emails	(Optional) Move the slider from **No** to **Yes** to enable sending email notifications. This option is available for the **Issue Assigned To User** trigger and all non-issue triggers.
Send to Slack	(Optional) Move the slider from **No** to **Yes** 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.

Create 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. On the portal toolbar, select **Notifications**.
   The Notifications page appears.
2. Click **Subscriptions**.

A list of your individual subscriptions appears.

3. Select the **Global Subscriptions** tab.
   A list of global subscriptions, including system-default global subscriptions, appears.
4. Click **+New Subscription.**
   The Create Subscription modal window opens.
5. Complete the fields. Fields are required unless otherwise noted.

Field	Description
Trigger	Select the trigger type from the list
Recipient	Select the subscription audience from the list: **Everyone** (default), **Group**, and **Role**. If you select **Group** or **Role**, select a specific group or role, respectively. **Note** Recipients are limited to users who have access to the application referenced in a notification.
Scope	Select the scope to which the trigger will apply from the list: **All Applications** (default), **Application**, **Application Type**, **Application Attribute**, **Business Criticality** and **All Releases Owned By Me**.
	(Optional) Type a note for the subscription.
Send Emails	(Optional) Move the slider from **No** to **Yes** to enable sending email notifications. **Scan Canceled** and **Scan Paused** triggers have **Send Emails** permanently enabled.This option is available for the **Issue Assigned To User** trigger and all non-issue triggers.
Send to Slack	(Optional) Move the slider from **No** to **Yes** to post notifications to Slack. This option is 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.

Edit a subscription

You can edit custom subscriptions. If you are a Security lead, you can also edit global subscriptions.

To edit subscriptions:

1. On the portal toolbar, select **Notifications**.
   The Notifications page appears.
2. Click **Subscriptions**.
   A list of your custom subscriptions appears.

3. If you are editing a custom subscription, remain on the **My Subscriptions** tab.
   If you are a Security lead who is editing a global subscription, select the **Global Subscriptions** tab.
4. Click the edit icon next to the subscription you want to edit.
   The Edit Subscription window appears.
5. Edit the fields as needed.
   Your subscription changes are saved.

Delete 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. On the portal toolbar, select **Notifications**.
   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 delete 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.

2.6. Switch tenants

You can switch among the tenant accounts that you manage in a portal datacenter.

> **Note**
>
> This is a TAM-only feature.

To switch tenants:

1. Click your account name and select **Switch Tenants**. The Switch Tenants page appears.
2. Select the desired tenant from the list of your available tenants. The portal refreshes with the selected tenant's data.

3. Manage

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

- Application
- Release
- Search applications and releases
- Create deep links

3.1. Application

An application is a codebase. It serves as a top-level container for one or more releases. You can create, view, and edit applications, depending on your user permissions.

OpenText 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: .NET, .NET Core, C/C++, Go, JAVA/J2EE, JS/TS/HTML, PHP, Python, Scala, 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).

This section covers the following topics:

- Create an application
- View application details

- Edit application settings
- Manage user assignment
- Manage applications in the tenant
- View event log
- Delete an application

3.1.1. Create an application

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

Field	Description
Application Name	Type the name of your application.
Business Criticality	Select the application's level of importance: ○ **High**: Security issues could have catastrophic consequences for the business. ○ **Medium**: Security issues would have non-trivial consequences, but ones which do not pose a life-or-death threat to the business. ○ **Low**: Security issues can be ignored or addressed gradually as time permits
Description	(Optional) Type a description of the application that helps you manage multiple applications.
Email Notifications	(Optional) List the email addresses for receiving email notifications of scan status updates for the application. Separate multiple email addresses with a semicolon or comma.
Application Type	Select the application type: **Web / Thick-Client** or **Mobile**.
Microservice Application	Create a Help Center ticket to have the feature enabled. (**Web / Thick-Client** applications only) Select the check box to scan the application as a microservice application. **Important** 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 **add**.
   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.

6. Click **Next**.
7. (Microservice applications only) If microservice attributes have been configured, specify the microservice attributes. Click **Next** to do this for each microservice you added earlier.

1. 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.

Field	Description
Release Name	Type the name of your release.
SDLC Status	Select the Software Development Lifecycle from the list. The **Retired** option is not available.
Microservice (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.
Owner	Select the owner from of the release. The owner will receive email notifications of scan status updates for the release.
Description	(Optional Type a description that helps describe the release.

2. Click **Next**.
3. If custom application attributes are configured for the tenant, in the **Application Attributes** page, specify the application attributes and click **Next**.
4. If custom release attributes are configured for the tenant, in the **Release Attributes** page, specify the release attributes.
5. 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 and click **Next**.
6. In the **Summary** page, review the application settings.
7. Click **Create Application**.
   You are redirected to the Overview page of your new application's release.

3.1.2. View 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).

Navigate the page

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

Task	Action
View the security policy applied to the application	Click **View** in the Policy Compliance box.
View combined metrics across the application's production releases	The **Policy Compliance** and **Issues in Production** boxes display the combined star rating and issue count. Click **Critical**, **High**, **Medium**, or **Low** to view issue details by priority.
View the application's security status	Review the **Security Status** box.
Search the application's releases	Enter a search term in the search text box.
Create a release	Click **+ New Release**.
Start a scan	Click **Start Scan** next to a release and select the scan type. The button is disabled for releases with the **Retired** SDLC status.
View additional release details	Click the release name.
View data composing part of a graph	Click a section of the graph.
View the most recent scan status for a release	Hover over the relevant status and click it to open the scan status details. Scheduled scans display their scheduled start date.
Expand or collapse filters	Click **Expand All**, **Collapse All**, or the arrow next to the filter name.
Hide or display the filter list	Click **Hide Filters** or **Show Filters**.
Remove applied filters	Click **X** or **Clear Filters**.

Filter the page

By default, the Application Overview page displays all results. Apply filters to limit the data displayed.



Note

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

To filter the Application Overview page:

1. Click **Hide Filters** or **Show Filters** to display the filter list if it is not currently displayed.
2. Expand the filters that you want to apply.
3. Select the filter values. The following table describes the available filters.

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

The page refreshes automatically with the filtered results. Applied filters appear at the top of the page.

3.1.3. Edit 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.

Field	Description
Application Name	Name of your application
Business Criticality	Business Criticality level
Application Type	Application type
Application Description	(Optional) Description of the application that will help you manage multiple application
Additional Emails	(Optional) Email addresses that will receive notifications of activity related to the application

- The **Application Summary** tab displays application details.
- (Microservice applications only) The **Microservices** tab displays existing microservices. You can add, edit, or delete microservices, as well as edit microservice attribute values.

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

- 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.
- The **Application Defender** tab displays configuration settings for Application Defender integration. For more information see Fortify Application Defender Integration.
- The **Source Control** tab displays configuration settings for source control integration. For more information, see Source Control Integration.

5. Edit the application settings as desired.
6. Click **Save**.
   The application settings are saved.

3.1.4. Manage user assignment

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	1. Click **Edit Users**. The Assign Users window appears. 2. Select the **Available** tab. A list of non-Security Lead users that can be assigned to the application appears. 3. Perform the following actions to select users: ▪ Select the check box next to individual users. ▪ Select the **ASSIGN** check box to select displayed users. ▪ Select the **Assign All Tenant Users** check box to select all users. You can use the search field to filter the application list.
Remove users from application	1. Click **Edit Users**. The Assign Users window appears. 2. Select the **Selected** tab. A list of non-Security Lead users that are assigned to the application appears. 3. Perform the following actions to remove users: ▪ Clear the check box next to individual users. ▪ Clear the **ASSIGN** check box to remove displayed users. ▪ Select the **Unassign All Tenant Users** check box to remove all users. You can use the search field to filter the application list.

6. Click **Save**.
   The changes to the application's assigned users are saved.

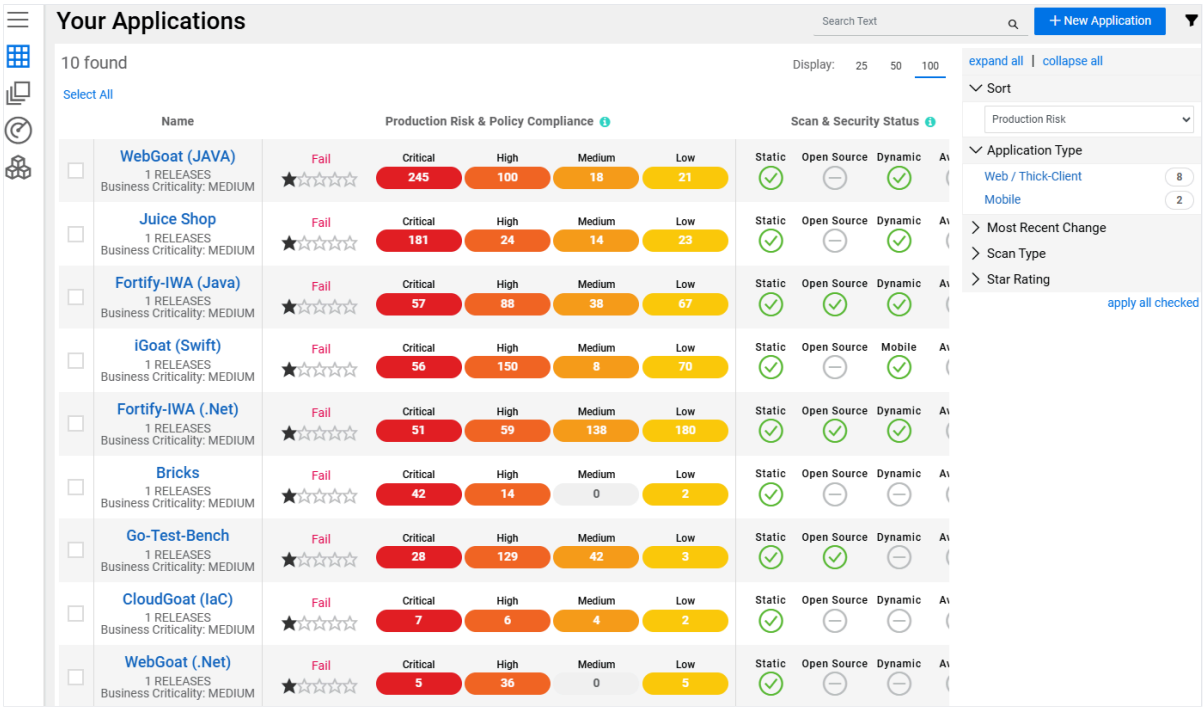
3.1.5. Manage applications in the tenant

You can review the security status of multiple applications simultaneously. Your Applications page is the default landing page after logging in to OpenText Fortify on Demand. It displays a high-level overview of your applications, 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.

Your Applications page



Navigate the page

The following table describes how to navigate **Your Applications** page.

Task	Action
Create an application	Click **+New Application**.
Search the application list	Type a keyword or phrase in the search text box and click **Enter**. To remove the search results, remove the search text or the applied filter. For more information, see Searching Applications and Releases.
Hide or display filter lists	Click **Hide Filters** or **Show Filters**.
Expand or collapse filters	Click **Expand All**, **Collapse All**, or the arrow next to the filter name.
Apply filters	Select filter values. The page refreshes automatically for some filters. For other filters, click **Apply**.
Remove applied filters	Click **X** next to an applied filter or click **Clear Filters**.
Filter applications by microservice designation	Select the desired tab.
Edit application attributes for multiple applications	Select the applications, click **Edit Attributes**, update the fields, and click **Save**. For more information, see Creating an Application.
Edit user groups for multiple applications	Select the applications, click **Edit Groups**, select the groups, and click **Append & Save** or **Overwrite & Save**. Users need both **Manage Applications** and **All Application Access** permissions to use **Overwrite & Save**.
View application details	Click the application name.
View the security policy applied to an application	Click the star rating.
View combined production metrics	Review the **Production Risk & Policy Compliance** column.
View the most recent scan status	Hover over the relevant status. Click it to open the scan status details.
View the most recent risk-relevant change	Review the **Most Recent Change** column.

Filter the page

By default, **Your Applications** page displays all applications. Applications are grouped by production, pre-production, and retired status, and then sorted by business criticality and issue severity.

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

Note

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

Filter	Description	Values
Application Type	Application type selected during application creation.	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	Status of mobile scans.	Scheduled, In Progress, Completed, Canceled, Waiting
Most Recent Change	Most recent change detected for an application.	User-defined categories
Pass/Fail	User-defined Pass/Fail rating.	Fail, Pass, Unassessed
Scan Type	Scan type.	Static, Dynamic, Mobile, Open Source
Sort	Sort order.	Production Risk, Most Recent Change, Application Name
Star Rating	Five-star rating.	1, 2, 3, 4, 5
Static Scan Status	Status of static scans.	In Progress, Completed, Canceled, Waiting
Custom application or microservice attribute	Picklist application or microservice attributes.	User-defined

3.1.6. View 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 **Export**. 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 **Enter**.
Hide or display the filter list	Click **Filter**.
Expand or collapse filters	Click **the expand/collapse icon** or the arrow next to a filter name.
Remove applied filters	Click **X** or click **Clear Filters** at the top of the page. The filter is set to the last 24 hours by default.

3.1.7. Delete an application

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



Note

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

3.2. Release

A release is a particular iteration of a codebase. In OpenText 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. You can create, view, and edit releases, depending on your user permissions.

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. This approach is not recommended 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 Software Development Life Cycle (SDLC) stages to a release to track it as it progresses through the SDLC. OpenText 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 still finishes.

This section covers the following topics:

- Create a release
- View release details
- Edit release settings
- Manage releases in the tenant
- Delete a release

3.2.1. Create 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.

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

Field	Description
Release Name	Type the name of your release.
Release Description	(Optional) Type a description that helps describe the release.
SDLC Status	Select the Software Development Life Cycle stage of the release: **Development**, **QA/Test**, **Production**. The **Retired** option is not available.
Release Attributes	Specify the release attributes.
Microservice (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.
Copy State from Existing Release	(Optional, selected by default) Select **Copy State from Existing Release** 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). **Note** Data from completed and imported scans are copied. Data from paused and in-progress scans, including scan settings, are not copied. Fix validated issues are not copied.

5. If you selected **Copy State from Existing Release**, click **Next**. Otherwise, skip to step 7.
6. 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.
7. 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.

3.2.2. View release details

The **Release Overview** page displays a dashboard-style overview of 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 the key metrics of your release. Many visual elements are interactive 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 scan results for the release.
   - The Policy Compliance box displays the Star Rating and Pass/Fail status.
   - The Issues box displays the number of vulnerabilities at each severity level. Click **Critical**, **High**, **Medium**, or **Low** to view the details of issues by priority. You can also search for an issue by its specific **Instance ID** on the Release Issues page.
   - The Scan Status box displays the most recent scan statuses for the release.
   - The tabs display visual representations of the scan results, with links to drill down into issues.

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

Task	Action
View the copy state source (if applicable)	Click the link below the release name.
Show or hide fixed issues	Select **Show >Fixed** to switch between showing and hiding Fix Validated issues.
Show or hide suppressed issues	Select **Show** > **Suppressed** to switch between showing and hiding False Positive Confirmed and Suppressed issues.
Start a scan	Click **Start Scan** and select the scan type from the list. The button is disabled for releases with SDLC status of **Retired**.
View the security policy applied to the application	Click **View** in the Policy Compliance box.
Override the policy compliance	Click **Edit** in the Policy Compliance box.
View the most recent scan status for the release	Hover over the relevant status icon. Click it to directly access the scan status details. ○ Scheduled scans display the scheduled start date. ○ 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 <release>. Contact us for details."
Drill down into issues filtered by issue severity or scan type	Click the visual elements in the Issue and Scan Status boxes.
Select a visual representation of the scan results for further analysis	Select a tab. For more information, see Release overview graphs.

Release overview graphs

The tabs on the Release Overview page display visual representations of scan results and provide links to related issues.

Note

Showing fixed and suppressed issues increases the vulnerability count. The updated count is also reflected in the vulnerability graphs.

Recommendations

The **Recommended Issues To Address** section lists why the release is failing the security policy. When specific issues cause the release to fail, you can drill down directly into those issues. If your policy requires a minimum scan frequency, that information also appears here. This section does not appear for releases that pass and have no scan frequency requirements.

The **Trending** section displays a line graph of vulnerability trends over time for the selected facet. Hover over a data point to view its count and type. Click a label to show or hide that data set.

Facet	Description
Auditor Status	Auditor status of issues.
CWE Top 25 2023, 2024, and 2025	Common Weakness Enumeration classifications.
CRA 2024	Cyber Resilience Act (CRA) 2024 classifications.
Developer Status	Developer status of issues.
FISMA (deprecated)	FISMA classification.
GDPR	GDPR classification from Fortify Software Security Research (SSR).
Is Assigned	Assignment status of issues: **False** or **True**.
Is Closed	Resolution status of issues: **False** or **True**.
Issue Status	Issue status: **New**, **Existing**, **Reopen**, or **Fixed**.
Is Suppressed	Suppression status of issues: **False** or **True**.
Kingdom	Seven Pernicious Kingdoms classification.
NIST SP 800-53 Rev 5	National Institute of Standards and Technology Special Publication 800-53.
OWASP ASVS 4.0 and 5.0	OWASP ASVS classifications.
OWASP 2017 and 2021	OWASP Top 10 classifications.
OWASP API Top 10 2023	OWASP API Top 10 2023 classification.
OWASP Top 10 2025	OWASP Top 10 2025 classification.
OWASP LLM 2025	OWASP LLM Top 10 2025 classification.
OWASP Mobile Top 10	OWASP Mobile Top 10 classification.
PCI40, PCIDSS401, PCISSF12	PCI 4.0, PCI 4.0.1, and PCI SSF 1.2 classifications.
Scan Type	Static, Dynamic, or Mobile.

Severity	Critical, High, Medium, or Low.
STIG52, STIG53, STIG61, STIG62, STIG63, STIG64	DISA STIG classifications.

Analysis

The **Analysis** tab displays a bar graph of vulnerabilities grouped by the selected aggregation facet: **Assignment**, **Auditor status**, **Category**, **Developer Status**, **Scan Type**, or **OWASP 13**.

Click a bar to open the Issues page filtered to that group. For example, clicking the **Privacy Violation** bar in the **Category** facet displays privacy violation vulnerabilities.

Smart Fix (static scans)

The **Smart Fix** tab is available after a static scan. It displays an analysis trace diagram that visualizes node execution order across static issues in a vulnerability category and shows shared data flows. Use this information to identify potential fix locations and remediation strategies.

Select a vulnerability category in **Categories** to view its analysis trace. You can scroll to zoom, click a node to highlight shared paths, and click an issue icon to open that issue. The toolbar provides these commands:

- **Toggle Heat Map**: Show or hide data-flow highlighting.
- **Prune** (when a node is selected): Show the combined data flow for the selected issues.
- **Reset**: Restore the default view for the selected issue category.
- **Zoom To Fit**: Resize the diagram to fit the display without resetting or pruning it.
- **Full Screen**: Expand the diagram to full screen.

App Information (mobile scans)

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

Reputation (mobile scans)

OpenText Fortify on Demand's Mobile Reputation service analyzes traffic endpoints discovered while testing a mobile application. The **Reputation** tab lists identified hosts and indicates whether each is in good standing. Mobile scan results also include vulnerabilities for hosts that are not in good standing.

Override the security policy of a release

Security Leads can manually set a release's policy status to passing or failing to reflect an exception without suppressing issues. The justification is recorded in the application's event log. The status reverts to the official policy result after the next scan.

To override the security policy of a release:

1. Select the **Applications** view.
   Your Applications page appears.
2. Click the application that contains the release.
   The Application Overview page appears.
3. Click the release for which you want to override the policy.
   The Release Overview page appears.
4. Click **Edit** in the Policy Compliance box.
   The Compliance Override window appears.
5. Enter the reason for changing the policy compliance result.
6. Click **Set to Pass** or **Set to Fail**.
   You return to the Release Overview page, where the override appears in the Policy Compliance box.

For information about star ratings, see Five-Star Assessment Rating. For information about managing security policies, see Policy Management.

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

Field	Description
Release Name	Name of the release
Microservice	(Microservice applications only) Name of the microservice linked to the release
SDLC Status	Software Development Lifecycle stage of the release
Owner	Owner of the release who receives email notifications of scan status updates to the release
Run Debricked Open Source Scan	(Available for tenants with Sonatype entitlements) Select the check box to switch the software composition analysis tool from Sonatype to Fortify SCA. The setting cannot be reverted once it has been saved. The tenant must have active Fortify SCA entitlements to successfully run Fortify SCA scans after the switch. **Note** If your tenant has inactive Sonatype entitlements and active Fortify SCA entitlements, your open sources scans are powered by Fortify SCA.
Release Description	(Optional) Description of the release that helps describe the release.

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

3.2.4. Manage releases in the tenant

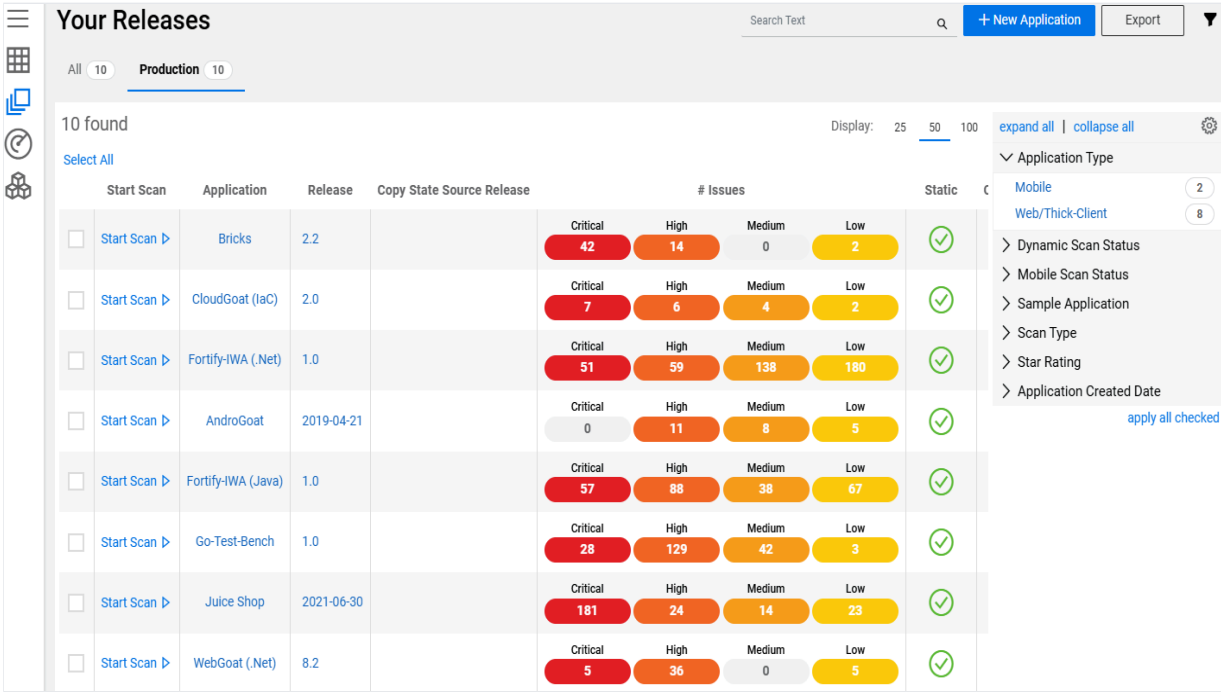
In addition to reviewing multiple applications at once, you can also review the details of individual releases across multiple applications simultaneously. Your Releases page displays a high-level overview of your releases in OpenText Fortify on Demand.

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.

Your Releases page



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.

Navigate the page

The following table describes how to navigate **Your Releases** page.

Task	Action
Create an application	Click **+New Application**.
Search the release list	Type a keyword or phrase in the search text box and click **Enter**. To remove the search results, remove the search text or the applied filter. For more information, see Searching Applications and Releases.
Export data as a CSV file	Click **Export**. A CSV file containing detailed vulnerability information is saved to the folder specified in your browser settings. Applied filters are included in the export.
Change the grid columns	Click **Columns**, select the columns to display, and click **Save**.
Hide or display the filter list	Click **Hide Filters** or **Show Filters**.
Expand or collapse filters	Click **Expand All**, **Collapse All**, or the arrow next to the filter name.
Apply filters	Select filter values. The page refreshes automatically for some filters. For other filters, click **Apply**.
Remove applied filters	Click **X** or **Clear Filters**.
Filter releases by SDLC status	Select the tab for the required SDLC status.
Sort the release list	Click a column header. Click the header again to reverse the sort order.
Edit release attributes for multiple releases	Select the releases, click **Edit Attributes**, update the fields, and click **Save**. For more information, see Creating a Release.
Start a scan	Click **Start Scan** and select the scan type.
View application or release details	Click an application or release name.
View the most recent scan status	Hover over a status. Click it to open the scan status details.
View the security policy applied to a release's parent application	Click the star rating.

Filter the page

By default, **Your Releases** page displays all releases. Apply filters to limit the releases displayed.

Note

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

Filter	Description	Values
Application Created Date	Date when the application was created.	Less than 7, 30, 90, or 180 days
Application Type	Application type selected during application creation.	Mobile, Web/Thick-Client
Business Criticality	Criticality of the application.	High, Medium, Low
Dynamic Scan Status	Status of dynamic scans.	Not Started, Canceled, Completed, In Progress, Waiting
Microservice Name	Microservice name.	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 the release.	Production, QA/Test, Development, Retired
Star Rating	Five-star rating.	1, 2, 3, 4, 5
Static Scan Status	Status of static scans.	In Progress, Completed, Canceled, Waiting
Custom release attribute	Picklist release attributes.	User-defined

3.2.5. Delete 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 OpenText Fortify on Demand after 72 hours.
If a release was deleted as an error, contact support within 72 hours of deleting the release.

Note

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

3.3. Search 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.

Search 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 enter the entire value. For example, if the application name is *Test App 1*:
   - Enter **Test** to return *Test App 1* in the search results.
   - Enter **Tes** and *Test App 1* is not returned.
   - Enter **Tes*** to return *Test App 1* in the search results.
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.

Remove 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.

3.4. Create deep links

OpenText 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.

where <*fod_domain*> is the following OpenText Fortify on Demand data center domain:

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

- FedRAMP: `fed.fortifygov.com`

4. Run assessments

OpenText Fortify on Demand offers comprehensive security testing across three assessment types:

- Static assessment
- Dynamic assessment
- Mobile assessment

This section includes the following:

- Static assessments
- Open Source software composition analysis
- Dynamic assessments
- Mobile assessments
- Entitlement consumption
- Manage scans

4.1. Static assessments

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

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

This section contains the following topics:

- OpenText SAST requirements
- Prepare static assessment files
- Configure a static scan
- Upload a static assessment payload
- Static assessment payload validation

4.1.1. OpenText SAST requirements



Note

Fortify SAST updates in OpenText Fortify on Demand can occur between major releases. Fortify SAST requirements are updated in the documentation for the major release. For more information on Fortify SAST releases, see the OpenText Static Application Security Testing and Tools Documentation.

This section contains the following topics:

- Supported languages
- Supported compilers
- Supported libraries, frameworks, and technologies

4.1.1.1. Supported languages

Fortify SAST supports the programming languages listed in the following table.

Language or framework	Version details
.NET (Core)	2.0-9.x
.NET Framework	2.0–4.8
ABAP/BSP	6.x, 7.x
ActionScript	3.0
Apex	55–61
Bicep	0.12.x–0.15.31
C#	5–13
C	C11, C17, C23 (see Compilers)
C++	C++11, C++14, C++17, C++20 (see Compilers)
Classic ASP (with VBScript)	2.0, 3.0
COBOL	IBM Enterprise COBOL for z/OS 6.1–6.3 (CICS, IMS, DB2, and IBM MQ) Visual COBOL 6.0–8.0
ColdFusion	8–10
Dart	2.12-3.1
Docker (Dockerfiles)	any
Flutter	2.0–3.13
Go	1.12–1.23
HCL	2.0 **Note** HCL language support is specific to Terraform and supported cloud provider Infrastructure as Code (IaC) configurations.

HTML	5 or earlier
Java (including Android)	7–21
JavaScript	ECMAScript 2015–2023
JSON	ECMA-404
JSP	1.2–2.1
Kotlin	1.3–2.0
MXML (Flex)	4
Objective-C/C++	2.0 (see Compilers)
PHP	7.3–8.3
PL/SQL	8–23
Python	2.6–2.7, 3.0–3.12
Ruby	1.x
Scala	2.11–2.13, 3.3–3.4
Solidity	0.4.12–0.8.21
Swift	5.0–5.10, 6.0 (see Compilers for supported swiftc versions)
T-SQL	SQL Server 2005, 2008, 2012
TypeScript	3.6–5.4
VBScript	2.0, 5.0
Visual Basic (VB.NET)	15.0–16.9
Visual Basic	6.0
XML	1.0
YAML	1.2

4.1.1.2. Supported compilers

Fortify SAST supports the compilers listed in the following table.

Compiler	Versions	Operating systems
gcc	GNU gcc 6.x–10.4, 11, 12, 13	Windows, Linux, macOS
	GNU gcc 4.9, 5.x	Windows, Linux, macOS, AIX
g++	GNU g++ 6.x–10.4, 11, 12, 13	Windows, Linux, macOS
	GNU g++ 4.9, 5.x	Windows, Linux, macOS, AIX
OpenJDK javac	9, 10, 11, 12, 13, 14, 17, 21	Windows, Linux, macOS, AIX
Oracle javac	7, 8, 9	Windows, Linux, macOS
cl (MSVC)	2015, 2017, 2019, 2022	Windows
Clang	14.0.3, 15.0.0, 16.0.0	macOS
Swiftc	5.8, 5.8.1, 5.9, 5.9.2, 5.10, 6.0, 6.0.2, 6.0.31	macOS

1Fortify SAST supports applications built in the following Xcode versions:

14.3, 14.3.1, 15, 15.0.1, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2

4.1.1.3. Supported libraries, frameworks, and technologies

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

Kotlin

Kotlin support includes all libraries covered for Java and the following Kotlin libraries.

Kotlin standard library

Scala

Scala support includes all libraries covered for Java and the following Scala libraries.

Akka HTTP Scala Play	Scala Slick

.NET

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

C

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

C++

Boost Smart Pointers MFC	STL WMI

SQL

Oracle ModPLSQL

PHP

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

JavaScript/TypeScript/HTML5

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

Python

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

Ruby

MySQL pg	Rack SQLite	Thor		

Objective-C

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

Swift

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

COBOL

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

Go

GORM logrus gRPC				

Configuration

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

Infrastructure as code: Amazon Web Services

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

Infrastructure as code: Microsoft Azure

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

Infrastructure as code: Google Cloud

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

Secrets

.netrc	Defined	HashiCorp (Terraform, Vault)	New Relic	Sendbird
1Password	DES	Heroku	npm	SendGrid
Actually Good Encryption (AGE)	DigitalOcean	HexChat	NuGet	Sentry
Adafruit	Docker	HubSpot	Okta	SHA1
Adobe	Doppler	Intercom	OpenVPN	SHA256
Airtable	Droneci	Java	Password in comment	SHA512
Algolia	Dropbox	JFrog (Artifactory)	Password in connection string	Shippo
Alibaba (Aliyun)	Duffel	JSON Web Token	Password in PowerShell script	Shopify
Amazon (AWS, MWS)	Dynatrace	KDE Wallet (Kwallet)	Password in URI	Sidekiq
Apple (macOS)	EasyPost	KeePass	Password Safe	Slack
Apache HTTP	Encryption key	Kraken	PayPal (Braintree)	SonarQube
Asana	Etsy	Kucoin	Pidgin	Square
Atlassian	Facebook	LaunchDarkly	Plaid	Squarespace
Authress	Fastly	Linear	Planetscale	StackHawk
Basic access authentication	Finicity	LinkedIn	PostgreSQL	Stripe
bcrypt	Finnhub	Lob	Postman	Sumologic
Beamer	Flickr	Mailchimp	Prefect	Telegram
Bearer token	Flutterwave	Mailgun	Pulumi	Travis
Bitbucket	Frame.io	Mapbox	PuTTY	Trello
Bittrex	Freshbooks	Mattermost	PyPI	Twilio
Brevo (Sendinblue)	Git	MD5	RapidAPI	Twitch
Clojars	GitHub	MessageBird	Readme	Twitter
Code Climate	GitLab	Microsoft (Azure App Storage, Cosmos DB, Functions and Bitlocker, PowerShell, RDP, VBScript)	RSA Security	Typeform
Codecov	Gitter	Microsoft (Outlook)	Ruby (Ruby on Rails, RubyGems)	Yandex
Coinbase	GNOME	Mutt	Sauce Labs	Zendesk
Confluent	GNU (Bash)	MySQL	Secret key	
Contentful	GoCardless	Netlify	Secure Shell Protocol (SSH)	
Databricks	Google (API, Google Cloud, OAuth)			
Datadog	Grafana			

4.1.2. Prepare static assessment files

The first step in a static assessment is to prepare your application's source code and/or compiled files. 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.



Note

For information on preparing files for open source software composition analysis, see Preparing Open Source Assessment Files.

This section contains the following topics:

- Prerequisites
- Install Fortify ScanCentral SAST client
- Prepare .NET application files
- Prepare Java application files
- Prepare JavaScript/HTML/XML files
- Prepare Kotlin application files
- Prepare ABAP(SAP) application files
- Prepare C and C++ application files
- Prepare Classic ASP, VBScript, and Visual Basic application files
- Prepare Dart and Flutter application files
- Prepare ColdFusion Markup Language (CFML) application files
- Prepare COBOL application files
- Prepare Dockerfiles and Infrastructure as Code (IaC) files
- Prepare Go application files
- Prepare PHP application files
- Prepare Python application files
- Prepare Ruby application files
- Prepare Solidity application files
- Prepare Salesforce (Apex and Visualforce) application files
- Prepare Scala application files
- Prepare Android application files (source code)
- Prepare iOS application files (source code)

4.1.2.1. Prerequisites

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, a JAR file must have functioning code.

4.1.2.2. Install Fortify ScanCentral SAST client

Fortify offers a stand-alone Fortify ScanCentral SAST client for automatically packaging all necessary dependencies and source code required for static scanning and the files required for OpenText open source scanning. The following languages are supported: .NET and .NET Core (MSBuild projects), Apex, Classic ASP, ColdFusion, Dockerfiles, Go, Java (Gradle and Maven projects), Javascript/Typescript, PHP, Python, and Ruby.

Important

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. OpenText Fortify on Demand uses only the packaging feature of the Fortify ScanCentral SAST client. Details that are relevant to packaging your source code has been provided.

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 Fortify Software Security Center Documentation. Select the documentation version that corresponds to your installed version.

- Software requirements: "Fortify ScanCentral SAST Client Software Requirements" in OpenText™ Application Security Software System Requirements
- Supported build tools: "Fortify ScanCentral SAST Sensor Languages and Build Tools" in OpenText Application Security Software System Requirements
- Command-line options: “Package Command” in OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide

4.1.2.3. Prepare .NET application files

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

- Automated code packaging with Fortify ScanCentral SAST (recommended)
- Code package with IDE tools
- Manual code packaging

Important

Source code is scanned by default. OpenText MSP Portal strongly recommends providing source code, as this 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 code scanning is not an option, contact support to enable binary/compiled code scanning.

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client.

Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Additional `package` command examples for .NET:

- dotnet project on Windows: `scancentral package -bt dotnet -o mypayload.zip`
- MSBuild project on Windows with CSPROJ file: `scancentral package -bf my.csproj -o mypayload.zip`

Code package 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 Tools.

Manual code packaging

Manual code packaging consists of:

- Preparing source code files
- Preparing compiled files (for binary/compiled code)
- Creating a zip file containing the source code and compiled files

Prepare 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.

In addition, make sure to do the following tasks to help reduce undesirable scan results:

- Include only one copy of your dependencies that are targeted to your specified .NET version.
- Do not provide the `obj` and `bin/release` folders in order to avoid duplicate code in the payload.

> **Note**
>
> If you are working in the Visual Studio Developer Command Prompt, make sure to 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 (for binary/compiled code)

- 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.

- 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.

Create a zip file

Package the source code and the 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.

4.1.2.4. Prepare Java application files

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

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Code packaging with IDE tools
- Manual code packaging

Important

Source code is scanned by default. OpenText MSP Portal strongly recommends providing source code, as this 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 code scanning is not an option, contact support to enable binary code scanning.

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .

Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Additional `package` command examples for Java:

- Maven project with a custom POM file: `scancentral package -bf myCustomPom.xml -o mypayload.zip`
- Gradle project with custom build parameter: `scancentral package -bc clean build -o mypayload.zip`

Code package 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 Tools.

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

Prepare source code files

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

Prepare 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.

Create 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.

4.1.2.5. Prepare JavaScript/HTML/XML files

JavaScript, HTML, and XML files can be submitted as stand-alone payloads under the **JS/TS/HTML** technology stack. **JS/TS/HTML** is a catch-all option for simple web applications and web applications that primarily use JavaScript-related technologies. React Native mobile applications are submitted under the **React Native** technology stack.

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 include the JavaScript, HTML, and/or XML files in the package.

Use the following method to prepare your application files:

- Automated code packaging with Fortify ScanCentral SAST (recommended)
- Code package with IDE tools
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>` ; for example, `scancentral package -o mypayload.zip` .

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .



Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Code package 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 Tools.

Manual code packaging

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.

In addition, 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.
- Do not include minified JavaScript files of your source code, as minified code significantly diminishes the quality of scan results.

4.1.2.6. Prepare 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.

4.1.2.7. Prepare 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.

Import the transport request

The Fortify ABAP Extractor is available on the Tools page in the portal (see View tools). 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.

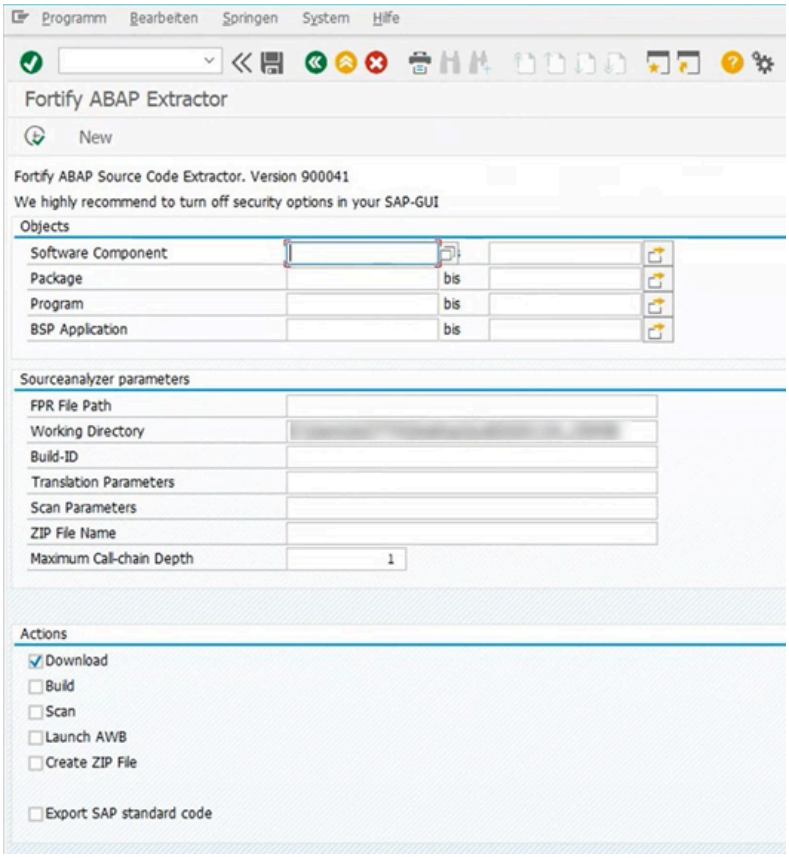
If this does not resolve the issue or if your system is running on an SAP version with a different table structure, OpenText recommends that you export your ABAP file structure using your own technology so that OpenText Fortify on Demand can scan the ABAP code.

Run 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 OpenText 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. You should 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 OpenText 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 `parentcl` field that matches the package name. It then recursively extracts everything else from `TDEVC` with a `parentcl` 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.

Package ABAP source code

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

4.1.2.8. Prepare C and C++ application files

OpenText 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 the testing team to reproduce your build environment. A translate-only version of Fortify SAST is provided for translating C/C++ code and packaging it for scanning.

Install OpenText SAST

The latest version of OpenText SAST is available on the Tools page in the portal. 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 is available from the Tools page.

For installation and usage instructions, see the OpenText Static Application Security Testing and Tools Documentation.

Translate 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.

Package translated code

A OpenText SAST 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 OpenText Fortify on Demand under the **MBS/C/C++/Scala** technology stack option.

For more information about using OpenText SAST, see the OpenText Static Application Security Testing and Tools Documentation.

4.1.2.9. Prepare Classic ASP, VBScript, and Visual Basic application files

For Classic ASP, VBScript, and Visual Basic (VB6) applications, use one of the following methods to prepare your application files:

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Code package with IDE tools
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .



Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Code package 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 Tools.

Manual code packaging

Package the source code files in one zip file.

4.1.2.10. Prepare Dart and Flutter application files

Package the source code files in a zip file. Include all dependencies.

Download the dependencies by running one of the following commands:

- For Flutter projects, use `flutter pub get`.
- For Dart-only projects, use `dart pub get`.

For example, to download the dependencies for a Flutter project that has the project root `myproject`, run the following commands:

```
cd myproject
flutter pub get
```

Important

If the project includes nested packages with different `pubspec.yaml` files, you must run `dart pub get` or `flutter pub get` for each package root.

Important

Make sure that the following are included in the project directory:

- The `pubspec.yaml` file, which specifies the dependencies
- The `.dart_tool` directory, which includes the `package_config.json` file automatically generated by the `pub` tool

4.1.2.11. Prepare ColdFusion Markup Language (CFML) application files

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

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client.

Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Manual code packaging

Package the source code files in one zip file.

4.1.2.12. Prepare COBOL application files

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

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -targs "-copydirs <copybooks>" -targs "-dialect <cobol_dialect>" o <output_zip>`; for example, `scancentral package -targs "-copydirs copybooks" -targs "-dialect COBOL390" o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client.



Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Manual code packaging

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. Place your COBOL source code in a folder named `sources/` and your copybooks in a folder named `copybooks/`. Place these folders at the same level in the root of the zip file.

4.1.2.13. Prepare Dockerfiles and Infrastructure as Code (IaC) files

Infrastructure as Code (IaC) configuration files and Dockerfiles can be submitted as stand-alone payloads under the **Infrastructure-As-Code/Dockerfile** technology stack.

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 SAST translates the following files as Dockerfiles: `Dockerfile`, `dockerfile`, `*.Dockerfile`, and `*.dockerfile`.

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

Use one of the following methods to prepare your application files:

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .



Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Manual code packaging

Package the files in a zip file and submit it under the **Infrastructure-As-Code/Dockerfile** technology stack.

4.1.2.14. Prepare Go application files

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

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Code packaging with IDE tools
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .



Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Code package 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 Tools.

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)

4.1.2.15. Prepare PHP application files

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

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Code packaging with IDE tools
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .

Note

Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Code package 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 Tools.

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.

4.1.2.16. Prepare Python application files

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

- Automated code packaging with Fortify ScanCentral SAST client (recommended)

  Important

  Python microservices must be packaged using the Fortify ScanCentral SAST client.

- Code packaging with IDE tools
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .

> **Note**
>
> Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Code package 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 Tools.

Manual code packaging

Fortify SAST processes PY files as Python source code. PYC files (compiled Python files) are not supported. Fortify SAST supports translation of the Django and Flask frameworks.

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).

> **Note**
>
> If your application uses a version of Python not listed in Supported languages, contact support to discuss your options.

4.1.2.17. Prepare Ruby application files

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

- Automated code packaging with Fortify ScanCentral SAST client (recommended)
- Manual code packaging

Automated code packaging with Fortify ScanCentral SAST client (recommended)

The Fortify ScanCentral SAST client automatically packages source code and all necessary dependencies in your project. You need to download the Fortify ScanCentral SAST client from the Tools page and install it on the build machine. Installation instructions are available in the README.txt file stored in the zip file.

In a command-line interface, navigate to the project's working directory and run the `package` command. The basic syntax is: `scancentral package -o <output_zip>`; for example, `scancentral package -o mypayload.zip`.

For more information on the Fortify ScanCentral SAST client and additional packaging options, see Installing and Using the Fortify ScanCentral SAST Client .

> **Note**
>
> Fortify ScanCentral SAST packaging is built in to the OpenText Fortify on Demand (FoD) IDE tools and CICD tools.

Manual code packaging

Package the entire application as it would be deployed and all source code files in one zip file.

4.1.2.18. Prepare Solidity application files

Package the source code files in a zip file. Include all dependencies.

Fortify SAST downloads compilers that are referenced in the code with the pragma statement from the Solidity compiler repository. If a file does not contain a pragma statement, then the default of ^0.8.0 is used.

4.1.2.19. Prepare Salesforce (Apex and Visualforce) application files

To prepare Salesforce (Apex and Visualforce) applications:

- Use the Ant Migration Tool available on the Salesforce website to download your application to your local computer from your Salesforce organization (org) where you develop and deploy it. Make sure that the project manifest files are set up correctly for the specified target in your `build.xml` file.
- 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
  - Visualforce component files with the `.component` extension
  - Objects with the `.object` extension
- Configure the retrieve targets using the Ant Migration Tool documentation. If your organization uses any apps from the app exchange, make sure that these are downloaded as packaged targets.s
- Package the source code files in one zip file.

4.1.2.20. Prepare 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 Fortify SAST are available for translating Scala and packaging it code for scanning.

Install OpenText SAST

The latest version of OpenText SAST is available on the Tools page in the portal. 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 is available from the Tools page.

For installation and usage instructions, see the OpenText Static Application Security Testing and Tools Documentation.

Translate code

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

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

Package translated code

A OpenText SAST 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 OpenText Fortify on Demand under the **MBS/C/C++/Scala** technology stack option.

For more information about using OpenText SAST, see the OpenText Static Application Security Testing and Tools Documentation.

4.1.2.21. Prepare 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 SAST supports Xamarin. For instructions on preparing Xamarin application files, see Preparing .NET Application Files. 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).

4.1.2.22. Prepare 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 SAST supports Xamarin. For instructions on preparing Xamarin application files, see Preparing .NET Application Files. 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).

4.1.3. Configure 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.

Field	Required	Description
Assessment type	Yes	Select the assessment type. Only assessment types allowed by the organization's security policy are displayed. The service-level objective (SLO) of the selected assessment type appears below the field.
Entitlement	Yes	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. **Note** ○ 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. ○ If you have a developer-type entitlement, this field displays only the IDs associated with that entitlement type.

Audit preference	Yes	Select the audit preference. ○ **Manual**: False positives identified by Fortify Audit Assistant with high confidence are automatically suppressed. A security expert then manually reviews the scan results. ○ **Automated**: False positives identified by Fortify Audit Assistant with high confidence are automatically suppressed and results are published without manual review. **Note** Fortify Audit Assistant is only applied to new issues found in a scan. False Positive Challenge is not available for new issues found in a scan using automated audit. The ability to select the audit preference depends on the assessment type: ○ A Static single scan allows Automated only. ○ A Static subscription allows one Manual audit per application (not per release or microservice). ○ A Static+ single scan allows Manual only. ○ A Static+ subscription allows Automated or Manual audit for each assessment.

Fortify Remediation Aviator	No	For scans using Automated audit, select the check box to have Fortify Remediation Aviator audit results and provide enhanced remediation assistance. This option is selected by default if Fortify Remediation Aviator is allowed in the security policy; if it is not allowed the option is disabled. This service consumes 1 additional assessment unit. No entitlement is deducted if the Fortify Remediation Aviator service is not performed. For more information on Fortify Remediation Aviator, see Audit and Remediation with Fortify Remediation Aviator.
Software Composition Analysis	No	Select the check box to include open source software composition analysis. No code leaves the OpenText Fortify on Demand environment. For more information on adding software composition analysis as part of a static scan, see Open Source Software Composition Analysis.
Scan third-party libraries for static security assessment	No	**Note** Contact support to enable the option. (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. **Note** Selecting this option infers that your organization has received consent from all third-party vendors to scan their libraries.

If needed, you can configure additional scan settings in the sections appearing below the required fields.

Click **Advanced Settings** and complete the fields as needed.

Field	Description
Scan policy	Select the scan policy to be used for the scan. Available policies include: • **Security**: This is the default scan policy, which excludes issues related to code quality, dataflow from sources that are typically trusted, and issues that are typically noisy from the analysis results. Use this policy to focus code remediation on the security issues. • **DevOps**: This scan policy expands on the security policy by excluding additional issues that might be considered noise and reducing more low priority issues. Use this scan policy when scan speed is a priority and developers review results directly, without any intermediate auditing. Issues that remain after you apply this scan policy are probably serious security issues that require remediation. This DevOps scan policy does not automatically include any customization made to the local security scan policy. • **FoD (Legacy)**: FoD (Legacy) consists of the Classic policy combined with FoD-specific filters and represents the configuration that FoD offered prior to the introduction of scan policies in this release. **Note** If a scan already exists for the application or release, the default policy is FoD (Legacy).
Technology stack	Select the application's technology stack. The languages available for selection depend on the application type (web/thick client or mobile) and whether the application is a microservice application. If the auto detect feature is enabled, selecting **Auto Detect** has OpenText Fortify on Demand determine the technology stack based on the payload content.
Language level	If applicable, select the technology stack's language level from the list.

- Click **Legacy Settings** and complete the field as needed.

Field	Description	**Deprecation Note**
Build server integration	Once the static scan settings (assessment type, technology stack, language level, audit preference, software composition analysis) have been configured, a token is automatically populated in the **Build Server Integration** field. The token can be used to submit a static assessment using external tools. **Note** The BSI token is persistent across assessments of a release.	The release ID replaces the BSI token. Migrate build configurations to the release ID at the earliest convenience.
Source control	Select the method of uploading the payload. ○ **Manual Upload** (default): Manually upload the payload from your local system. ○ **Source Control**: Upload the payload from a version control platform. This option is available if source control has been configured. For more information, see Source Control Integration.	This feature is planned to be deprecated. You should migrate legacy source control integrations to pipelines on the applicable version control platforms at the earliest convenience. For more information, see CICD Tools.

Scan binary	**Note** Contact support to enable the option. (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 Fortify ScanCentral SAST-packaged payloads. **Note** If the source code inclusion requirement is enabled and this option is not selected, the scan are cancelled if the payload does not contain source code.	

1. Click **DevOps & IDE integration** to view the release ID. 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.
2. Click **Save**.
   Your static scan settings are saved.
3. If you have the Consume Entitlements permission and selected a subscription entitlement, click **Start Subscription** to start the static assessment subscription and consume the entitlement immediately. The assessment cost is deducted from the entitlement when a user starts the initial scan.

Note
Contact support to enable the option.

4.1.4. Upload a static assessment payload

Once you have packaged the application files and configured the static scan settings, upload the payload for scanning. The maximum payload size limit is 5 GB. Web browsers have their own maximum size limits (see your browser documentation for details).

As portal timeouts can occur when uploading large files, you should upload through the portal only if the file size is less than 500 MB. If you have difficulties uploading through the portal, see Related Topics for alternative methods of uploading your files.

You can have one in progress static scan for a release. You can submit multiple scans for an application, including ones for the same release. 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.

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
Manual upload	1. Click .... 2. Navigate to and select your zip file.
Source Control	1. Select **Branch** or **Release** from the **Source Location** list. 2. Select the specific branch or release.

6. In the field, type a description of the application.
7. Click **Next**.
   A summary of the static scan setup values appears.
8. Review the summary. If necessary, click **Back** and make any corrections. If the values are correct, click **Start Scan**.
   Once the upload of the zip file is complete, you are redirected to the Release Scans page; your new scan status is **Queued**. The scan begins once it moves to the front of the queue.

Related topics

In addition to using the portal, you can submit a static assessment using the following methods:

- IDE plugin tools: Visual Studio Extension, Eclipse Plugin, IntelliJ Plugin, Fortify Extensions for Visual Studio Code. For more information, see IDE Tool.
- Build server integration tools: FoDUploader, Fortify Azure DevOps Extension, OpenText Fortify on Demand Jenkins Plugin. For more information, see CICD Tool.
- OpenText Fortify on Demand API. For more information, see OpenText Fortify on Demand API.

4.1.5. Static assessment payload validation

After the payload has been uploaded, OpenText 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 SAST. Supported file extensions are: ABAP, abap, appxmanifest, as, asax, ascx, ashx, asmx, asp, aspx, baml, bas, bicep, BSP, bsp, cbl, cfc, cfm, cfml, class, cls, cob, conf, Config, config, cpx, cs, cscfg, csdef, cshtml, ctl, ctp, dart, dll, Dockerfile, dockerfile, erb, exe, frm, go, hcl, htm, html, inc, ini, jar, java, jmod, js, jsff, json, jsp, jspf, jspx, jsx, kt, kts, Master, master, mbs, mxml, page, php, phtml, pkb, pkh, pks, plist, properties, py, razor, rb, scala, settings, sol, sql, swift, tag, tagx, tf, tld, trigger, ts, tsx, vb, vbhtml, vbs, vbscript, wadcfg, wadcfgx, winmd, wsdd, wsdl, xaml, xcfg, xhtml, xmi, xml, xsd, yaml, yml.
- 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, the payload is packaged using the Fortify ScanCentral SAST client.
- 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, .tf, .yaml, dockerfile
Go	.go
JAVA/J2EE/Kotlin	.java, .kt, .ktm, .kts
JS/TS/HTML	.xsd, .xmi, .wsdd, .config, .cpx, .xcfg, .js , .ts
PHP	.php
PYTHON	.py
VB6	.vbs, .bas, .frm, .ctl, .cls
VBScript	.vbscript
Ruby	.rb

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.

4.2. Open Source software composition analysis

OpenText Fortify on Demand offers Open Source software composition analysis in conjunction with a static assessment or as a separate assessment. Applications are scanned using one of the following software composition analysis tools:

- Fortify SCA (offered with static assessments and as a separate assessment)
- Sonatype (offered with static assessments, not available for purchase)

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

Purchase Fortify SCA entitlements to enable open source software composition analysis. An entitlement is redeemed for one Fortify SCA subscription per application. Upon submitting an open source scan, the software composition analysis tool checks for open source components in the payload. Open source scan results identify direct and transitive dependencies along with associated security issues and licenses

Tenants that do not have active Sonatype entitlements receive five complementary Fortify SCA scans per static subscription. Complementary scans are limited to the subscription period. Complementary scans are void once tenants purchase open source scan entitlements.

If you are interested in purchasing Fortify SCA entitlements, contact your sales representative.

This section contains the following topics:

- Prepare Open Source assessment files
- Upload a payload through the Portal
- View components in a release

- View components in a tenant

4.2.1. Prepare Open Source assessment files

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

Fortify SCA file requirements for lock file analysis

To reliably detect dependencies, Fortify SCA 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. Fortify SCA supports scanning dependencies using native lock files.
- For build systems or package managers or build systems that don't use a lock file (such as Maven and Gradle), Fortify SCA requires a file describing the resolved dependency tree to be generated using the functionality of the build system or package manager. This file is referred to as a Fortify SCA lock file.
  You can use one of the following methods to generate both native lock files and Fortify SCA lock files:
  - (Recommended) Use the Fortify ScanCentral SAST client (22.1.2 or later) to generate the lock files along with the application files. Add the `-oss` option to the `package` command to invoke the Fortify SCA CLI and add the lock files to the package. Note that package generation is not dependent on successfully packaging the lock files.
  - (Recommended) Run the Fortify SCA CLI to generate the lock files independently of the application files. For installation and usage instructions, see README.FoD.md.
  - Manually generate the lock files. You can automate this process by adding the appropriate command to your CICD pipeline.

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

> **Important**
>
> A Fortify SCA scan is canceled if the required lock file is not present in the payload.

Language	Package manager	Required file	**Notes (if not using the Fortify ScanCentral SAST client)**
C#	NuGet	`packages.lock.json`	Use one of the following methods to generate the lock file: • Run `debricked resolve` from the Debricked CLI. For more information, see C# - Nuget, Paket. • Run `dotnet restore --use-lock-file` from the .NET CLI. For more information, see Enable repeatable package restore using lock file. • Set the MSBuild property `RestorePackagesWithLockFile` to `true` in the `.csproj` project file and run the Nuget `restore` command. For more information, see Enable repeatable package restore using lock file.
	Paket	`paket.lock`	`paket.lock` is automatically generated by Packet.
Go	Go Dep	`gopkg.lock`	`gopkg.lock` is automatically generated by dep. **Note** Go Dep updates will not be made as Go Dep is deprecated.

	Go modules	`gomod.debricked.lock`	For instructions on generating the resolved dependency tree file, see Go - Go Modules, Go Dep, Bazel.
Java/Kotlin	Bazel	WORKSPACE	WORKSPACE is automatically generated by Bazel.
		(Recommended) `maven_install.json`	Use `rules_jvm_external` to generate `maven_install.json`, where all dependencies are pinned to their respective versions. For more information, see A repository rule for calculating transitive Maven dependencies.
	Gradle	`gradle.debricked.lock`	For instructions on generating the resolved dependency tree file, see Java & Kotlin - Gradle, Maven and Bazel.
	Maven	`maven.debricked.lock`	For instructions on generating the resolved dependency tree file, see Java & Kotlin - Gradle, Maven and Bazel.
JavaScript	Bower	`bower.debricked.lock`	For instructions on generating the resolved dependency tree file, see JavaScript - NPM, Yarn, Bower.
	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	pip	`<file_name>.pip.debricked.lock`	For instructions on generating the resolved dependency tree file, see Python - Pip, Pipenv.
	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 generated by RubyGems.
Swift	Cocoapods	`podfile.lock`	`podfile.lock` is automatically generated by Cocoapods.

In keeping with industry best practices, you should commit lock files to the source control repository. This simplifies the process of preparing application files, especially if you are not using the Fortify ScanCentral SAST client to package the payload.

Fortify SCA file requirements for fingerprint analysis

Fortify SCA supports scanning for unmanaged dependencies not defined in manifest files by examining fingerprints of the application files, including binary files (with some exclusions for non-relevant files). The `debricked.fingerprints.txt` file must be provided; this file is automatically generated by OpenText Fortify on Demand when submitting a Fortify SCA scan. A Fortify SCA scan includes both fingerprint analysis and lock file analysis. For more information on Fortify SCA file fingerprinting, including the currently supported languages, see File fingerprinting.

In some instances, the package and/or version resulting from file fingerprinting might differ from the dependency used in your application. You can ensure the results are correct by excluding fingerprinting of a certain file or path. To do so, add the correct dependency to a manifest file. CycloneDX SBOM using the Fortify SCA CLI. Alternatively, generate a `debricked-config.yaml` file to override results. For more information on excluding dependencies, see Manage or override results.

Sonatype File Requirements

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

4.2.2. Upload a payload through the Portal

The method of uploading an open source payload depends on whether the open source assessment is included with the static assessment or is run separately:

- To include the open source assessment with the static scan assessment, configure your static scan settings to include an open source scan. Include the required open source files in your static assessment payload. This method is available for both Fortify SCA and Sonatype. For more information, see Configuring a Static Scan.
- To run separately the open source assessment, upload a native or Fortify SCA lock file. The following instructions describe how to submit the Fortify SCA-only scan.

> **Note**
> You can submit Fortify SCA assessments on third-party software bill of materials. For more information, see Import a Software Bill of Materials.

To submit the Fortify SCA-only 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 Open Source.
   The Open Source Scan window appears.
4. Click **...**.
5. Navigate to and select your zip file containing the lock file. The zip file can contain either the static assessment payload or just the lock file.
6. Click **Start Scan**.
   Once the upload of the zip file is complete, you are redirected to the Release Scans page; your new scan status is **Queued**. The scan will begin once it moves to the front of the queue.

4.2.3. View 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.
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.

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

Task	Action
Export the open source component list	Click **Export**. 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.
View results from specific scan tool	Select the scan tool 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 **Enter**.
Filter and sort by column values	Click one of the following column headings: **Component**, **License**, **Scan Tool**, **Scope**, and **Type**
View issues filtered by package URL	Click the issue counts in each component row.
View component's package URL and Open Source Select link	Click the **Details** icon.

4.2.4. View 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.

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

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

Task	Action
Export the open source component list	Click **Export**. 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.
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 **Enter**.
Filter and sort by column values	Click one of the following column headings: **Component**, **License**, **Scan Tool**, **Scope**, and **Type**
View the applications and corresponding releases that use a component.	Click **View Releases** in the row of a component.
View component's package URL and Open Source Select link	Click the **Details** icon.

4.3. Dynamic assessments

A dynamic assessment analyzes a running web application for security vulnerabilities. Dynamic assessments include automated testing powered by OpenText DAST and manual analysis.

Dynamic testing using OpenText DAST involves the following modes:

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

This section contains the following topics:

- Prepare the Website for Dynamic testing
- Prepare Web API files
- Set up Fortify on Demand Connect
- Configure a Dynamic scan
- Schedule a Dynamic scan
- Edit scan settings

4.3.1. Prepare the Website for Dynamic testing

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

- Confirm that the web application and user credentials are functioning before the assessment. If the web application uses client certificate authentication, contact support.
- 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, OpenText MSP Portal 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 OpenText 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 OpenText 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.
- 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.
- For internal sites, use OpenText Fortify on Demand Connect to set up site-to-site VPN. For more information, see Set up Fortify on Demand Connect.

For dynamic assessments that utilize automation during the scanning process, make the following preparations:

- Create workflow macros to run scans 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 OpenText DAST's Event-based Web Macro Recorder, available on the Tools page in the portal. For instructions on creating workflow macros, see the OpenText™ Dynamic Application Security Testing Tools Guide at OpenText DAST documentation.
- Create login macros for authentication. A login macro is a recording of the events that occur when you access and log in to a Web site using a Web Macro Recorder tool. You can create login macros with OpenText DAST's Event-based Web Macro Recorder, available on the Tools page in the portal. For instructions on creating login macros, see the OpenText™ Dynamic Application Security Testing Tools Guide at OpenText DAST documentation.

> **Note**
> If you using the API and switching from a Dynamic assessment type to a DAST Automated assessment type, upload the login macro through the portal before starting the scan.

4.3.2. Prepare 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.

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.

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.

gRPC

- Provide a proto file. If additional imports are needed, they must be combined with the primary proto file into a "master" proto file. gRPC proto files must be self-contained. Any imports must be to internally recognized resources and not to user-generated files. OpenText DAST cannot identify file paths from imported proto files.

GraphQL

- Provide a GraphQL introspection file or URL. The GraphQL API must have introspection enabled to download the schema contents for the scan.

Examples

The following examples show project files with working sample data.

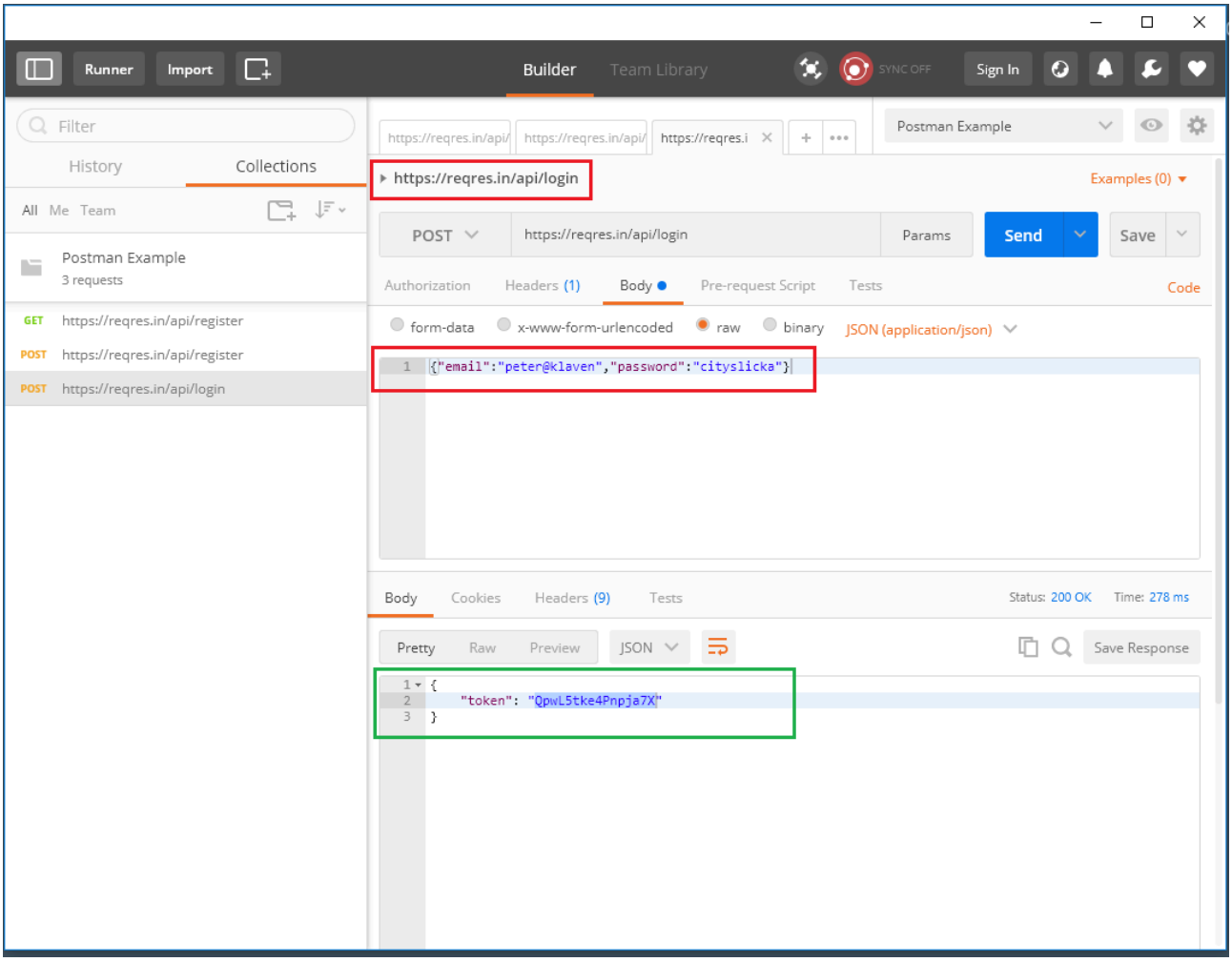


Note

Only input parameter values need to be provided, the responses are shown here for information only.

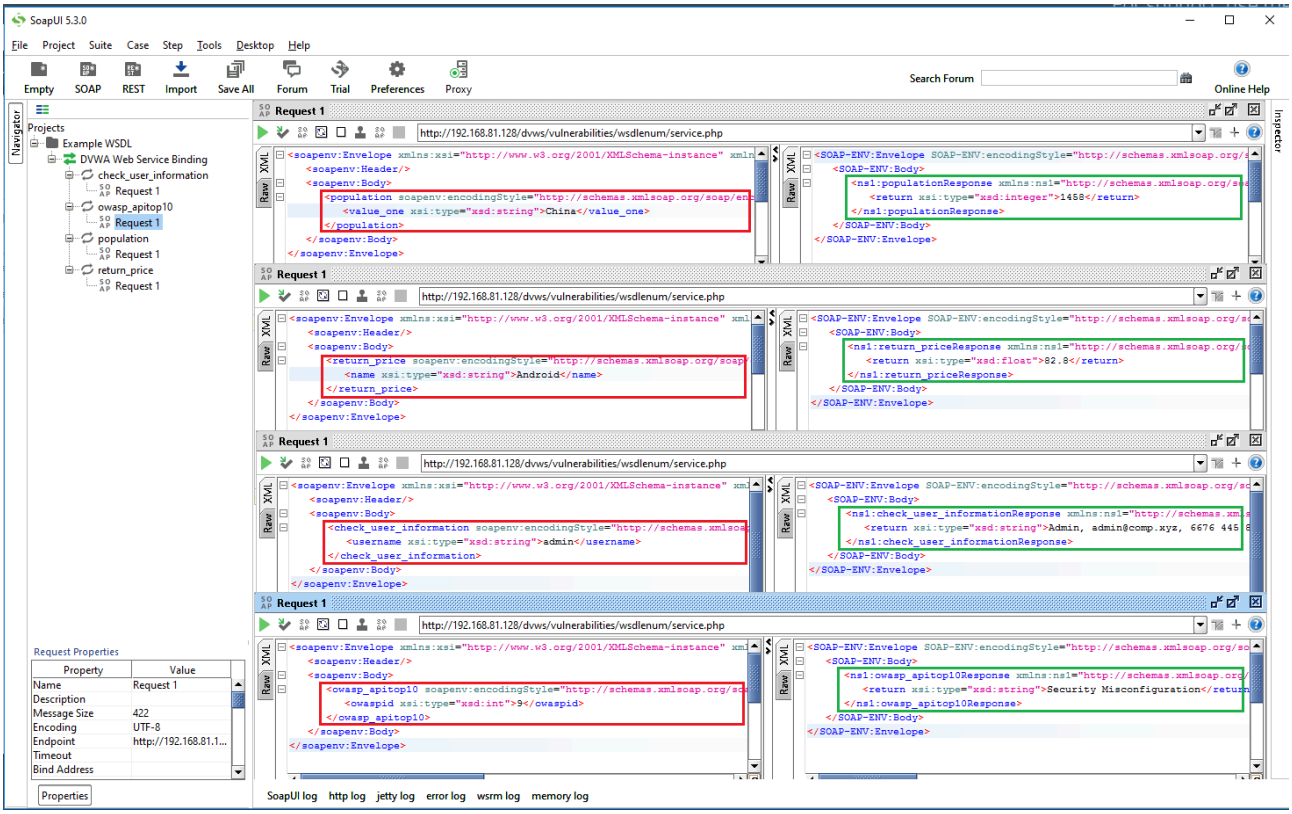
Example 1 (REST)

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).



4.3.3. Set up Fortify on Demand Connect

You can use OpenText Fortify on Demand Connect to easily set up site-to-site VPN for dynamic assessments of internally facing web applications. OpenText Fortify on Demand Connect implements an OpenVPN server and client configuration to create secure site-to-site connections. You need to install the OpenVPN client, available as a Docker container.

Note

Concurrent scans share the Connect tunnel's capacity and can cause scan pauses or reduced performance. Stagger scans to reduce load, or contact Support for capacity guidance.

The following instructions assume that you have familiarity with installing, configuring, and using Docker.

To set up OpenText Fortify on Demand Connect:

1. Pull the OpenText Fortify on Demand Connect Docker image on Docker Hub. Access to the Fortify Docker repository requires credentials and is granted through your Docker ID. To access the Fortify Docker repository, email your Docker ID to mfi-fortifydocker@opentext.com.
2. Install the Docker container on a Linux x86_64 machine. The machine must meet the following requirements:
    - Minimum supported Docker Engine version: 20.10.17
    - Access to the internally facing application
3. (Security leads) Add a OpenText Fortify on Demand Connect network in OpenText Fortify on Demand.
4. (Security leads) Copy the docker command for the network and run it on the machine before the dynamic scan is scheduled. The following is an example docker command:

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

The container ID is returned if the docker command was successful.

4.3.4. Configure a Dynamic scan

After preparing your web application 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	Assessment type	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. **Note** The **Dynamic+ API** assessment is used for testing a web API where a definition file is not available.
Scan type	DAST Automated	Select the dynamic scan type: ○ Website: this scan is similar to a Dynamic Website scan. ○ Workflow-Driven Scan: this scan is similar to a Dynamic Website scan that utilizes a workflow macro. ○ API: this scan is similar to a Dynamic API scan.

Workflow-driven scan	○ Website (Optional) ○ DAST Automated: Workflow-Driven Scan	A Workflow-Driven Scan uses the audit only mode (no crawling) and is completely automated. OpenText DAST audits only those URLs recorded in the macro and does not follow any hyperlinks encountered during the audit. For the Website assessment, you need to select the check box to run the scan as a Workflow-Driven Scan. Upload the workflow macro (see Prepare the Website for Dynamic Testing). Supported macros are `.webmacro` files, Burp Proxy captures, and `.har` files. **Note** ○ For Dynamic and DAST Automated scans in the tenant portal, the default maximum workflow macro file size has been extended from 30 MB to 90 MB. ○ The application being scanned must be external facing. Activity recorded in a macro overrides other scan settings.

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. **Note** ○ Switching from Dynamic or Dynamic+ assessment to DAST Automated assessment does not consume assessment units. However, switching from DAST Automated assessment to another assessment consumes the cost of the new assessment. ○ This field displays only the Fortify entitlement IDs. For Developer, Sonatype and Debricked applications, entitlement ID is not 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.

Request false positive removal (optional)	DAST automated	Select the check box to request false positive removal by the testing team once per application. This option is selected by default if DAST Automated add-ons are allowed in the security policy; if it is not allowed the option is disabled. **Important** Login macro generation and false positive removal are offered as an optional service that is available once per application and consumes 1 additional assessment unit. **Important** If you want to request both login macro generation and false positive removal, you must select both options together; once a scan that includes either option has completed, both options will be disabled for subsequent scans.
Use Fortify on Demand Connect (optional)		(Optional) If the site is internal, select the check box to use OpenText Fortify on Demand Connect to set up site-to-site VPN, and then select the OpenText Fortify on Demand Connect network that has been configured for the site. For more information, see Set up Connect. **Important** A connection must be initialized between the VPN client and the VPN server before scheduling the scan.

5. 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.

Field	Description
Scan entire host (<*URL*>)	Select one of the following options: • **Scan entire host (<*URL*>)** (default): the entire host will be scanned **Example**: Given https://foo.com/home, the following URLs will be included: - https://foo.com/ - https://foo.com/contact-us.html - https://foo.com/folder/ - https://foo.com/folder/folder2/page.aspx - https://foo.com/home/folder/ - https://foo.com/home/index.html • **Restrict the scan to the URL directory and subdirectories**: only the directory denoted by the last slash in the URL and its subdirectories will be scanned. **If you select this option, make sure the last slash denotes the directory to which you want the scan to be restricted.** **Example**: Given https://foo.com/home/, the following URLs will be excluded: - https://foo.com/ - https://foo.com/folder/ - https://foo.com/contact-us.html - https://foo.com/folder/folder2/page.aspx
Restrict scan to URL directory and subdirectories	
Allow HTTP (:80) and HTTPS (:443)	Select the check box to allow both HTTP and HTTPS scanning of the site (default). **Example**: Given https://foo.com/home, if the **Scan entire host** option is selected, http://foo.com/ and its subdirectories will be included. If the **Restrict scan to URL directory and subdirectories** option is selected, only http://foo.com/home and its subdirectories will be included. **Note** This field is not applicable for **Dynamic** and **Dynamic + Website Assessment** assessment types.

Allow form submissions during crawl	Select the check box 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. Not selecting the check box does **not** prevent form submissions during vulnerability checks. Detection of many critical vulnerabilities, such as SQL injection and cross-site scripting, requires form submissions. To exclude specific web functionalities from form submissions, specify those URLS in the **Exclude URLS that contain** field. **Note** For **Dynamic** and **Dynamic + Website Assessment** assessment types, this field is **disabled** and cannot be modified.
Exclude URLS that contain	(Optional) Provide a full or partial URL and click to exclude URLs matching the string from being scanned. Add a new entry for each string. The field is not case-sensitive. **Example**: https://foo.com/login.html, login.html
Include URLs	(Optional, **Dynamic+ Website, Dynamic Website** assessments) By default, OpenText Fortify on Demand does not scan URLs outside the provided top-level domain. To audit resources linked to the **Dynamic Site URL** domain, such as subdomains, APIs, and offsite resources, type the URL and click . Add a new entry for each additional URL. Do not include URLs that are under the **Dynamic Site URL** domain, offsite domains, or third party applications. **Example**: Given https://foo.com/home, valid URLs include: • www.foo.com (subdomain) • API.aws.com (API) • authfoo.com/login • api.foo.com • api.foo2.com

- **Scope (Dynamic Website as 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 (DAST Automated)**
  To edit the scope of the scan, click **Scope** and complete the fields as needed.

Field	Scan Type	Description
Scan entire host (<*URL*>)	Website	Select one of the following options: • **Scan entire host (<*URL*>)** (default): the entire host will be scanned **Example**: Given https://foo.com/home, the following URLs will be included: - https://foo.com/ - https://foo.com/contact-us.html - https://foo.com/folder/ - https://foo.com/folder/folder2/page.aspx - https://foo.com/home/folder/ - https://foo.com/home/index.html • **Restrict the scan to the URL directory and subdirectories**: only the directory denoted by the last slash in the URL and its subdirectories will be scanned. **If you select this option, make sure the last slash denotes the directory to which you want the scan to be restricted.** **Example**: Given https://foo.com/home/, the following URLs will be excluded: - https://foo.com/ - https://foo.com/folder/ - https://foo.com/contact-us.html - https://foo.com/folder/folder2/page.aspx
Restrict scan to URL directory and subdirectories		
Exclude URLS that contain	Website	(Optional) Provide a full or partial URL and click to exclude URLs matching the string from being scanned. Add a new entry for each string. The field is not case-sensitive. **Example**: https://foo.com/login.html, login.html

Enable Redundant page detection	• Website • Workflow-Driven Scan	Select the check box to enable comparison of page structure to determine the level of similarity, allowing the sensor to identify and exclude processing of redundant resources. **Note** Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan.

Scan Policy	Policies differ by scan type	Select the policy (collection of vulnerability checks and attack methodologies that the sensor deploys against a Web application): **Standard**: A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities such as SQL Injection and Cross-Site Scripting as well as poor error handling and weak SSL configuration at the web server, web application server, and web application layers. **Criticals and Highs**: Use the Criticals and Highs policy to quickly scan your web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers. **Passive Scan**: The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature. **Api**: The API policy contains checks that target various issues relevant to an API security assessment. This includes various injection attacks, transport layer security, and privacy violation, but does not include checks to detect client-side issues and attack surface discovery such as directory enumeration or backup file search checks. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy is not intended for scanning

		applications that consume Web APIs.
Timebox Scan Duration (Hours)	• Website • API	Specify the maximum duration of the scan. If the scan is not completed at the end of the specified duration, the scan is terminated and partial results are available. If the scan is completed during the specified duration, then complete results are available. Incremental scanning is not supported.

- **Authentication (Dynamic Website, Dynamic+ Website, Dynamic Manual, Dynamic+ API, Dynamic+, DAST Manual)**
  To edit the authentication settings, click **Authentication** and complete the fields as needed.

  Note
  Saved values in the passwords fields are obfuscated once the settings.

Field	Description
Form Authentication Required	(Optional) Select the check box if form authentication is required. Provide user names and passwords for at least two users. **Note** For authentication during **Dynamic+ Assessment** and **Dynamic Manual Assessment**, you can provide three additional user names, passwords and roles. To provide additional user names, passwords and roles, click plus at the bottom of the form. Role is an optional field which can accept up to 32 characters. **Note** Make preparations so that the user credentials remain valid for the scan duration, such as increasing the password expiration duration. The scan will be canceled if site authentication fails. Specifying the same credentials for multiple concurrently active scans might lead to delays or inaccurate results (due to account lockout, password changes, or other events). To avoid this issue, make sure that scans that are active at the same time have distinct credentials. If available, select the **Generate unique authentication** check box if self-registration is required.

Enable 2FA	Select the check-box to enable 2FA. Once enabled, select the 2FA mode. • Email: When **Email** is selected, a **2FA Inbox** drop-down appears for each user, displayed to the right of the **Role** text box. - You can assign a different inbox to each user, allowing them to receive their 2FA verification emails in the inbox you specify. • TOTP: When **TOTP** is selected, choose one of the following options: - **Upload Image**: Upload the QR code image file. The supported file formats are JPEG and PNG. - **Enter Text**: Enter the TOTP secret key. **Note** You can use only one method. If you enter the secret key, you cannot upload a QR code, and vice versa.
Network Authentication Required	(Optional) Select the check box if network authentication is required. 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. **Note** OpenText Fortify on Demand does not support multi-factor authentication. Examples include authentication controls involving SMS messages, email verifications, CAPTCHA, OATH Tokens, and physical tokens.

- **Authentication (DAST Automated)**
  To edit the authentication settings, click **Authentication** and complete the fields as needed.

  Note
  Saved values in the passwords fields are obfuscated. You can clear password fields and provide new values if needed.

Field	Scan Type	Description
Use Site Authentication	Website	(Optional) Select the check box if site authentication is required. Upload the login macro (see Preparing the Website for Dynamic Testing). **Note** Make preparations so that the user credentials remain valid for the scan duration, such as increasing the password expiration duration. The scan will be canceled if site authentication fails. Specifying the same credentials for multiple concurrently active scans might lead to delays or inaccurate results (due to account lockout, password changes, or other events). To avoid this issue, make sure that scans that are active at the same time have distinct credentials.

Request Login macro creation	Website	Select the check box to request generation of a login macro by the testing team once per application. Upon scan completion, the login macro will be available for download on the Scans page. This option is selected by default if DAST Automated add-ons are allowed in the security policy; if it is not allowed the option is disabled. **Note** Login macro generation and false positive removal are offered as an optional service that is available once per application and consumes 1 additional assessment unit. **Note** If you want to request both login macro generation and false positive removal, you must select both options together; upon completion of a scan that includes either option, both options will be disabled for subsequent scans.
Use Network Authentication		(Optional) Select the check box if network authentication is required. Provide the authentication type, username, and password. **Note** The scan is canceled if network authentication fails.

- **APIs (DAST Automated: API)**
  To add instructions for scanning web APIs utilized by the site, click **APIs**. For information on preparing web API project files suitable for automated testing, see Preparing Web API Files.
  Select the API definition type in the **API Type** field: **Postman Collection**, **OpenAPI**.

Note

OpenAPI Specification versions 2.0 and 3.0 are supported.

PI Definition Type	Procedure
Postman	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.

Postman Collection (URL)	1. Provide the Postman collection URL.
	2. If authentication is needed to access the URL, provide the header name in the **Header Name** and the credentials in **Header Value** fields. For example, provide `Authorization` in **Header Name** and `Bearer <token>` in **Header Value**. Not that this is separate from the credentials used to authenticate requests.
	Examples:
	`X-API-Key: <apikey>`
	`Authorization: <apikey>`
	`Authorization: Bearer <token>`
	Note
	If the credentials are passed as a query parameter, include it in the URL.

OpenAPI	Select **File** or **URL to the OpenAPI specification** and perform the relevant task based on your selection.
	File • 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. • If the API requires authentication, provide the API key value in the **API Key** field. **Note** The supported security scheme is API key. Multiple API keys in requests are not supported.
	URL to the OpenAPI specification • Provide the OpenAPI document URL. • If the API requires authentication, provide the API key value in the **API Key** field. **Note** The supported security scheme is API key. Multiple API keys in requests are not supported.

Perform the relevant task based on your API definition type.

- In the **Additional Instructions** field, provide additional instructions.
- **APIs (Dynamic API, Dynamic API+, DAST Manual)**
  For information on preparing web API project files suitable for automated testing, see Preparing Web API Files.
  To add instructions for scanning web APIs utilized by the site, click **APIs**.
  Select the API definition type in the **API Type** field: **SOAP**, **REST, Postman.**
  Perform the relevant task based on your API definition type.

API definition type	Procedure
SOAP	• Upload a WSDL file that contains working sample data. The JSON, WSDL, TXT, and XML file formats are accepted. • (Optional) In the **Additional Instructions** field, provide additional instructions, such as required headers, tokens, or authentication mechanisms. • (Optional) Provide the username and password or API key and password.
REST	• Upload an API definition file that contains working sample data. The JSON, WSDL, TXT, and XML file formats are accepted. • (Optional) In the **Additional Instructions** field, provide additional instructions, such as required headers, tokens, or authentication mechanisms. • (Optional) Provide the username and password or API key and password.
Postman	• Upload an API definition file that contains working sample data. The JSON, WSDL, TXT, and XML file formats are accepted. • In the **Select File Type** field, select the file type as either Workflow, Auth, Environment or Globals. The workflow file is mandatory, while the other file types are optional. • (Optional) In the **Additional Instructions** field, provide additional instructions, such as required headers, tokens, or authentication mechanisms. • (Optional) Provide the username and password or API key and password.

- **Scheduling & Availability (Dynamic Website, Dynamic+ Website, Dynamic API, Dynamic+ API)**
  To edit the scan frequency and site availability settings, click **Scheduling & Availability** and complete the fields as needed.

Field	Description
Repeat frequency	Select the scan's repeat frequency: **Do not repeat** (default), **2 weeks**, **1 month**, **2 months**, **3 months**, **4 months**, **6 months**, **12 months**. If you are requesting a single scan, keep the default value. Scheduled recurring scans are automated and subjected to the following stipulations: • 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. • The entitlement is deducted at the time of scheduling. • A scan is scheduled if a valid entitlement for the selected assessment type exists at the time of the scheduling. • If a scan is canceled, no further scans are scheduled. • If a scan is still in progress when the next scan is to be scheduled, OpenText Fortify on Demand attempts 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 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. **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. Contact support 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**.

Field	Description
Concurrent request threads	Select the number of concurrent requests that will be used for the scan: • **Standard** (default): 5 crawl requestor threads, 10 audit requestor threads, 20 second request timeout • **Limited**: 2 crawl requestor threads, 3 audit requestor threads, 5 second request timeout Selecting the **Limited** option will reduce the scan load but will also cause the scan to take longer than the standard SLO.
Additional notes	(Optional) Type additional information that the testing team needs to know before starting the assessment. **Note** Free form exclusions and whitelist notes have been migrated to this field.
Additional documentation	(Optional) Upload documentation (30 MB limit) that facilitates testing of the application. Uploaded files appear in the **Uploaded Files** section below. You can also download files that were previously submitted for dynamic assessments. Supported file types: DOC, DOCX, PPT, TXT, PDF, PPTX, ZIP, XLS, XLSX, CSV.
Generate WAF virtual patch	**Note** Contact support to enable the WAF feature. (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
Request pre-assessment conference call	(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. **Note** You cannot request a pre-assessment conference call for a scan scheduled within 72 hours. This feature is deprecated for 25.4 version and will not be available starting from 26.1 version.

6. 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.

4.3.5. Schedule a Dynamic scan

Once you have prepared your web application and configured the dynamic scan settings, you can schedule the dynamic scan. You can 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 time zone.
2. Click the **Start Date** field.
   Click **Now** to schedule a scan immediately or use the calendar to select a start date and time, then click **Done**.
3. Click **Next**.
   Site accessibility check results appear. The site accessibility check looks for the following criteria:
   - The URL resolves.
   - The DNS of the hostname resolves.
   - OpenText 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 scan from being paused.

   > **Note**
   > The site accessibility check is available for website scans (with the exception of sites accessed through VPN).

4. Click Next.
   A summary of the dynamic scan setup values appears.
5. Review the summary. If necessary, click **Back** and make any corrections. If the values are correct, click **Start Scan**.
   You are redirected to Release Scans page; your new scan has a **Scheduled** status. 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 update your dynamics scan settings.

In addition to using the portal, you can submit a dynamic assessment using the following methods:

- Build server integration tools: Fortify Azure DevOps Extension, OpenText Fortify on Demand Jenkins Plugin. For more information, see CICD Tool.
- OpenText Fortify on Demand API. For more information, see OpenText Fortify on Demand API.

4.3.6. Edit 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.

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

- **Dynamic Site URL**
- **Scan Type**
- All fields in the **Scope** section (except for DAST Automated scans)
- 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.



Note

If you are switching from a Dynamic assessment type to a DAST Automated assessment type, you can edit dynamic scan settings. The DAST Automated scan settings must match the Dynamic assessment scan settings. For example, if the release's original assessment type was Dynamic Website, the new assessment type must be DAST Automated Website.

If your API definition type is a GraphQL URL, switching from Dynamic API to DAST Automated is supported only through the portal.

4.4. Mobile assessments

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

This section contains the following topics:

- Supported platforms and operating systems
- Prepare mobile assessment files
- Manage a scan

4.4.1. Supported platforms and operating systems

Hardware platforms

OpenText Fortify on Demand supports the following hardware platforms:

Platform	**Mobile**	Mobile+
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

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

Operating system	**Mobile**	Mobile+
Minimum iOS version (`MinimumOSVersion`)	N/A	Up to 18.5
Native iOS architecture	ARMv7, ARM64	ARMv7, ARM64
Minimum Android version (`android:minSdkVersion`)	N/A	Up to 33 (Android 13)
Native Android architecture	ARMv7, ARM64	ARMv7, ARM64

4.4.2. Prepare mobile assessment files

Prepare the mobile application binary and, when applicable, the backend before submitting a mobile assessment. Follow the requirements for your platform and assessment type.

Android application files (binary)

> **Note**
>
> Applications that require language or regional settings to be configured at the device level are not supported. Applications that include language- or region-specific content, or allow users to configure these settings within the application, are supported.

Prepare the Android application binary (.aab or .apk) as follows:

- Make sure the application does not require MDM features.
- Provide the complete binary. Only the submitted file is tested, so features that require application updates are not supported.
- For Mobile+ assessments, make sure the application can be installed and run on a physical device.
- For Mobile+ assessments, disable root detection, application tampering, and certificate pinning mechanisms. These features can limit testing and scan coverage.
- For Mobile+ assessment of AAB files, dynamic feature modules must specify `<dist:fusing dist:include="true" />` in the manifest.

> **Important**
>
> If you submit a subsequent scan, keep the application identifier (package name) consistent to preserve issue tracking between scans. Changing it can cause existing issues to appear as new issues in scan results.

For information about preparing Android source code files for static assessments, see Preparing Android Application Files (Source Code).

iOS application files (binary)

> **Note**
>
> Applications that require language or regional settings to be configured at the device level are not supported. Applications that include language- or region-specific content, or allow users to configure these settings within the application, are supported.

Prepare the iOS application binary (.ipa) as follows:

- For Mobile+ assessments, make sure the application can be installed and run on a physical device.
- For Mobile+ assessments, disable application tampering and certificate pinning mechanisms. These features can limit testing and scan coverage.
- Make sure the application does not require MDM features.
- Export the application using a supported distribution type: App Store submission, Ad Hoc, Enterprise, or Development. For App Store submission, clear **Include bitcode** so the IPA contains executable code.
- Do not submit an IPA downloaded from the App Store; it is encrypted for the user who downloaded it. App Store submissions with **Include bitcode** enabled are also unsupported because the IPA does not contain executable code.
- Provide the complete binary. Only the submitted file is tested, so features that require application updates are not supported.

> **Important**
>
> Keep the application identifier consistent across scans. Changing it can cause existing issues to appear as new issues in scan results.

> **Note**
>
> Before installation, the IPA is re-signed with entitlements required for assessment and installation on test devices. Re-signing can remove entitlements required by application features or trigger integrity protections. If critical functionality is affected, the scan may be paused while the Mobile Application Security Testing (MAST) team investigates and recommends workarounds.

For information about preparing iOS source code files for upload, see Preparing iOS Application Files (Source Code).

Prepare the backend for mobile testing

For mobile assessments that include backend or web application testing, prepare the backend as follows:

- Confirm that the web application and user credentials work before the assessment.
- Complete functional and performance testing, then freeze the application's code for the duration of the security test.
- Back up your data before testing. After testing, restore it from a known-good backup to avoid potential data corruption.
- Make the web application publicly accessible. Scanning over VPNs is not supported.
- Add the OpenText Core Application Security IP addresses, available on the Mobile Scan Setup page, to the allow lists for your firewalls, IPS, IDS, and WAF. Share the addresses with your security and network operations teams so they do not block planned scan traffic. Ad hoc addresses may be used with your consent when needed.

> **Note**
>
> If your website is accessible through the default HTTP and HTTPS ports (80 and 443), you do not need to open additional ports for the assessment.

4.4.3. Manage a scan

Configure, schedule, monitor, and update mobile scans throughout the assessment lifecycle. You can manage scan settings, upload scan payloads, submit assessments, and modify eligible scan configurations after submission.

Configure a 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: **iOS**, **Android**, **Windows** (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 **Manual** for Mobile Standard, Mobile Premium, and Mobile+ assessments. **Automatically publish (no audit)** - The scan results are automatically published upon scan completion. **Manual** – The scan results are reviewed by auditors before being published.

5. 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.

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, select +. You can add up to six user names and passwords. **Important** Specifying the same credentials for multiple concurrently active scans might lead to delays or inaccurate results (due to account lockout, password changes, or other events). For example, you might schedule scans for the Android and iOS versions of an app at the same time. To avoid this issue, make sure that scans that are active at the same time have distinct credentials.
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.

Field	Description
Access to APIs	(Optional) Select the check box to allow OpenText 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.

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 **Uploaded Files** 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. **Note** You cannot request a pre-assessment conference call for a scan scheduled within 72 hours. This feature is deprecated for 25.4 version and will not be available starting from 26.1 version.

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.

Schedule a scan

Once you have prepared your mobile application and configured the mobile scan settings, you can upload the payload and schedule the mobile scan. You can 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.
2. Click the **Start Date** field.
    Click **Now** to schedule a scan immediately or use the calendar to select a start date and time, then click **Done**.

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

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

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

   > **Note**
   > The **Override Payload Validation** check box appears for payloads greater than 500 MB. Select the **Override Payload Validation** check box to skip the mobile payload validation.

5. Click **Next**.
   Payload validation results appear. Payload validation looks for the following criteria:
   - The payload is a valid zip archive. (Mobile, Mobile+)
   - The payload is a valid application format. (Mobile, Mobile+)
   - The application supports standard device formats. (Mobile+)
   - The application supports required architectures. (Mobile+)
   - The application targets a supported minimum operating system version. (Mobile+)
   - The iOS application package contains compiled code. *(Mobile+)*
   - The code in the iOS application package is not encrypted. *(Mobile+)*
   - The iOS application can run on a physical device. *(Mobile+)*

   OpenText MSP Portal recommends resolving any issues before starting your scan in order to prevent the scan from being canceled. In some cases, the testing team can proceed with the scan in spite of validation failures. Select **Override validation failures** to continue to the next step. For more information on overriding validation failures, contact support.
6. Click **Next**.
   The Summary page appears.
7. Review the summary. If necessary, click **Back** and make any corrections. If the values are correct, click **Start Scan**.
   You are redirected to the Release Scans page, your new scan has a **Scheduled** status. The scan will begin at your scheduled time.

   > **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.

In addition to using the portal, you can submit a mobile assessment using the following method:

- OpenText Fortify on Demand API. For more information, see API.

Edit 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** and **Audit Preference** 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 Support.

4.5. 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.

- The entitlement consumption data export.
- Entitlements page under the Administration view.

4.6. Manage 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:

- View and navigate scans
- Navigate the scans page
- Filter Your Scans page
- Check the scan status
- Cancel a scan
- Resume a scan
- View tickets

4.6.1. View and navigate scans

View scans across applications and releases. Search scans, review scan details, download results and artifacts, update scan attributes, and perform scan-specific actions based on the scan type.

View all scans

You can view scans for all your applications at the tenant level.

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	In the search box, type a keyword or phrase and press **Enter**. To clear the search, delete the text and press **Enter** again.
Hide or display the filter list	Click **Filter**.
Expand or collapse filters	Click **Expand** or **Collapse**, or select the arrow next to a filter name.
View Help Center tickets associated with a scan	Click **Help Center Tickets**.
Request cancellation of an in progress scan	Click **More Actions** and select **Cancel Scan**.
View scan summary	Click **More Actions** and select **Scan Summary**. The summary includes the scan ID and a comparison with the previous scan.
View static scan notes	Click **More Actions** and select **Scan Notes**..
Download scan results	For static, dynamic, and mobile scans, click **More Actions** and select **Download Results**. For open-source scans, select **Download SBOM**, then choose **CycloneDX** or **SPDX**.
Download manifest of static scan payload	Click **More Actions** and select **Download Manifest**. The manifest lists uploaded files and excludes images, media files, and CSS files.
Download static scan payload	Contact support to enable the download source code feature. Click and select **Download Source Code** for a completed scan.
Edit attributes	Select one or more scans and click **Edit Attributes**, or click **More Actions** and select **Edit Attributes**.  **Note** You can add or update values for scan-type custom attributes.

Download dynamic scan site tree	Click **More Actions** and select **Download Site Tree**. Dynamic scans and Mobile+ Assessment scans support site tree downloads. • Dynamic + Website Assessment: Displays **Automatic** and **Manual** scan mode options if a manual site tree was uploaded. • Dynamic Manual Assessment: Displays only **Manual**. • Mobile+ Assessment: Display only **Manual**. If the selected scan mode is Automatic, select CSV or JSON as the file type. If the selected scan mode is Manual, the file type is .txt.
View dynamic scan detected hosts	Click **More Actions** and select **Detected Hosts**. Detected hosts are referenced by the application but are not included in the list of allowed hosts.
Submit Fortify SCA scan on SBOM	Click **More Actions** and select **Send to Debricked**. The SBOM must be available for download.
Delete an imported scan	Click **More Actions** and select **Cancel Imported Scan**.
Create a WAF export file	Contact Support to enable the WAF feature. Then click **More Actions** and select **Send to WAF/IPS**. The export is generated as an XML file.

View 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 **Help Center Tickets**.
Request cancellation of an in progress scan	Click **More Actions** and select **Cancel Scan**.
View scan summary	Click and select **Scan Summary**. The scan summary includes the scan ID and a comparison to the previous scan. For static scans that use Automated audit, the summary also includes **Remaining Aviator Issue Processing Quota**. See Audit and Remediation with Fortify Remediation Aviator.
View static scan notes	Click **More Actions** and select **Scan Notes**.
Download scan results	Static, dynamic, and mobile: Click **More Actions** and select **Download Results**. Open source: Click and select **Download SBOM**. To download CycloneDX, select **CycloneDX**. To download SPDX, select **SPDX**.
Download manifest of static scan payload	Click and select **Download Manifest**. The manifest lists uploaded files and excludes images, media files, and CSS files.
Edit attributes	Select one or more scans and click **Edit Attributes**, or click **More Actions** and select **Edit Attributes**. **Note** You can add or update values for scan-type custom attributes.
Download dynamic scan site tree	Click **More Actions** and select **Download Site Tree**. **Dynamic scans and Mobile+ Assessment scans** support downloading the site tree. • Dynamic + Website Assessment: Displays **Automatic** and **Manual** scan mode options if a manual site tree was uploaded. • Dynamic Manual Assessment: Displays only **Manual**. • Mobile+ Assessment: Display only **Manual**. If the selected scan mode is Automatic, select CSV or JSON as the file type. If the selected scan mode is Manual, the file type is .txt.

View dynamic scan detected hosts	Click **More Actions** and select **Detected Hosts**. Detected hosts are hosts that are referenced by the application but are not specified as allowed hosts.
Submit Debricked scan on SBOM	Click **More Actions** and select **Send to Debricked**. The SBOM must be available for download.
Delete an imported scan	Click **More Actions** and **Cancel Imported Scan**.
Create a WAF export file	Contact Support to enable the WAF feature. Then click **More Actions** and select **Send to WAF/IPS**. The export is generated as an XML file.

View 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 **Import Scan** and select the scan type. OpenText Fortify on Demand supports on-premises scan results (Import an on-premises scan) and open source scan results (Import a Software Bill of Materials).
View Help Center tickets associated with the scan	Click **Help Center Tickets**.
Request cancellation of an in progress scan	Click **More Actions** and select **Cancel Scan**.
View scan summary	Click **More Actions** and select **Scan Summary**. The scan summary includes the scan ID and a comparison to the previous scan
View static scan notes	Click **More Actions** and select **Scan Notes**.
Download scan results	Static, dynamic, and mobile: Click **More Actions** and select **Download Results**. Open source: Click and select **Download SBOM**. To download CycloneDX, select **CycloneDX**. To download SPDX, select **SPDX**.
Download manifest of static scan payload	Click and select **Download Manifest**. The manifest lists uploaded files and excludes images, media files, and CSS files.
Download static scan payload	Contact support to enable the download source code feature. Click **More Actions** and select **Download Source Code** for a completed scan.
Edit attributes	Select one or more scans and click **Edit Attributes**, or click **More Actions** and select **Edit Attributes**. **Note** You can add or update values for scan-type custom attributes.

Download dynamic scan site tree	Click **More Actions** and select **Download Site Tree**. **Dynamic scans and Mobile+ Assessment scans** support downloading the site tree. • Dynamic + Website Assessment: Displays **Automatic** and **Manual** scan mode options if a manual site tree was uploaded. • Dynamic Manual Assessment: Displays only **Manual**. • Mobile+ Assessment: Display only **Manual**. If the selected scan mode is Automatic, select CSV or JSON as the file type. If the selected scan mode is Manual, the file type is .txt.
View dynamic scan detected hosts	Click **More Actions** and select **Detected Hosts**. Detected hosts are hosts that are referenced by the application but are not specified as allowed hosts.
Download login macro	Click **More Actions** and select Download login macro.
Download logs file failed DAST Automated scans	Click **More Actions** and select **Detected Hosts**. Detected hosts are referenced by the application but are not included in the list of allowed hosts.
Submit Debricked scan on SBOM	Click **More Actions** and select **Send to Debricked**. The SBOM must be available for download.
Delete an imported scan	Click **More Actions** and **Cancel Imported Scan**.
Create a WAF export file	Contact Support to enable the WAF feature. Then click **More Actions** and select **Send to WAF/IPS**. The export is generated as an XML file.

4.6.2. Navigate the scans page

The following tables describe how to navigate Your Scans page, Application Scans page, and Release Scans page. The Scans pages share the same features except where noted.

Task	Action	Notes
Search the scan list	Type a keyword or phrase in the search text box and click **Enter**. To remove the search results, remove the text from the search box and click **Enter**. For information, see Search Applications and Releases.	Text search is only available on Your Scans page
Hide or display the filter list	Click **Filter**.	Filtering is available on Your Scans page. It is not available on other Scans pages. For more information, see Filter options on Your Scans page.
Expand or collapse filters	Click **expand all** or **collapse all** 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 **More options** and select **Cancel Scan**. See Cancel an in progress scan.	
View scan summary	Click **More options** and select **Scan Summary**. The scan summary includes the scan ID and a comparison to the previous scan.	
View static scan notes	Click **More options** and select **Scan Notes**.	
Download scan results	Static, dynamic, and mobile: Click **More options** and select **Download Results**. Open source: Click **More options** and select **Download SBOM**. To download CycloneDX, select **CycloneDX**. To download SPDX, select **SPDX**.	
Download manifest of static scan payload	Click **More options** and select **Download Manifest**. The manifest lists uploaded files and excludes images, media files, and CSS files.	
Download static scan payload	Contact support to enable the download source code feature. Click and select **Download Source Code** for a completed scan.	Downloading static scan payload is only available on Your Scans page and Releases page.

Edit attributes	Either select one or more scans from the list and click **Edit Attributes** or click **More options** and select **Edit Attributes.** **Note** You can select one or more scans from the Scans list view and add custom attribute values. The **Edit Attributes** window displays the scan-type attributes, where you can enter or update values as needed.	
Download dynamic scan site tree	Click **More options** and select **Download Site Tree**. **Note** Dynamic+ Website assessment displays two scan mode options "Automatic" and "Manual" if a manual site tree is uploaded. Dynamic Manual assessment displays only "Manual" option. Select **CSV** or **JSON** for the file type if the selected scan mode is "Automatic". If the selected scan mode is "Manual", the file type must be **.txt**.	
View dynamic scan detected hosts	Click **More options** and select **Detected Hosts**. Detected hosts are hosts that are referenced by the application but are not specified as allowed hosts.	
Download login macro used in dynamic scan	Click **More options** and select **Download Login Macro**.	Login macro is available for the following scan types: DAST Automated Website, Dynamic, Dynamic+

Download scan log for failed dynamic scan	Click **More options** and select **Download Scan Log**.	Scan log is available for DAST Automated scan.
Submit Fortify SCA scan on SBOM	Click **More Actions** and select **Send to Debricked**. The SBOM must be available for download.	
Delete an imported scan	Click **More options** and **Cancel Imported Scan**. See Delete an imported scan.	
Create a WAF export file	Contact support to enable the WAF feature. Click ▪▪▪ and select **Send to WAF/IPS**. The export is an XML file.	

Note

The duration of availability for downloads is set by the Data retention policy.

4.6.3. Filter Your Scans page

You can limit the scans displayed on Your Scans page by applying filters. The following filter and grouping options are available on Your Scans page:

Note

For a filter to appear in the filter list, the results need to contain multiple values for that filter.

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 Policy	Scan policy type used for the scan	Security, DevOps, Classic , FoD (Legacy)
Scan Tool	Tool used to produce the scan, as extracted from imported scan metadata	WebUI, FAA, FCLI and other supported scan-producing tools represented in your scan results
Scan Type	Scan type	Static, Dynamic, Mobile, Network, Open Source

4.6.4. Check the scan status

You can check the scan status in the portal. Release owners, scan submitters, and users on an application's notification list also receive email notifications of the following scan status updates: scan start, scan completion, scan cancellation, scan pause, and False Positive Challenge submission and completion.



Note

The available scan statuses depend on the assessment type. There is a limit of 25 in progress scans per tenant.

- **Static**: An application can have one in progress static scan for a release (maximum of two in progress per application). 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.
- **Open source**: An application can have one in progress Fortify SCA scan for a release (maximum of two in progress per application). Additional scans are queued and then scanned in the order in which they were queued
- **Dynamic**: An application can have one in progress dynamic scan at a time. Scans cannot be queued.
- **Mobile**: An application can have one in progress mobile scan at a time. Scans cannot be queued.

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, filtered by the relevant scan type.



Note

DAST Automated and Fortify SCA scans can have partial results; the scan status icon for completed scans that have partial results is highlighted in orange;

4.6.5. Cancel a scan

If you 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 is 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.
4. Click **More options** 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 a 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 testing team, who then manually cancels the scan.
   - For a scan with a **Waiting** status, the scan is automatically canceled. An email is sent to the testing team.



Note

Once a scan is cancelled, any Help Center tickets associated with the scan are marked as solved.

4.6.6. Resume a scan

The testing team pauses a scan if additional information is needed. Respond to the associated Help Center ticket so the scan can be resumed. Pausing and resuming testing causes the scan to take longer than the standard SLO.

> **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.

1. Click your account name.
2. Select Help Center.
   The Help Center opens in a separate window.
3. Click View Tickets.
   A new screen appears, with a list of tickets submitted. Each ticket has a status, listed in the left-hand column. Possible statuses are **New**, **Open**, **Pending**, and **Solved**.
4. Click Show Pending.
   The list now shows only tickets that require action from your organization.

   > **Note**
   >
   > Your total number of Pending tickets appears as a red numeral above the Help Center link at the top of the page.

5. Click Reply and type your response to the question.
   As soon as you send a response, your assessment's status reverts to In Progress.

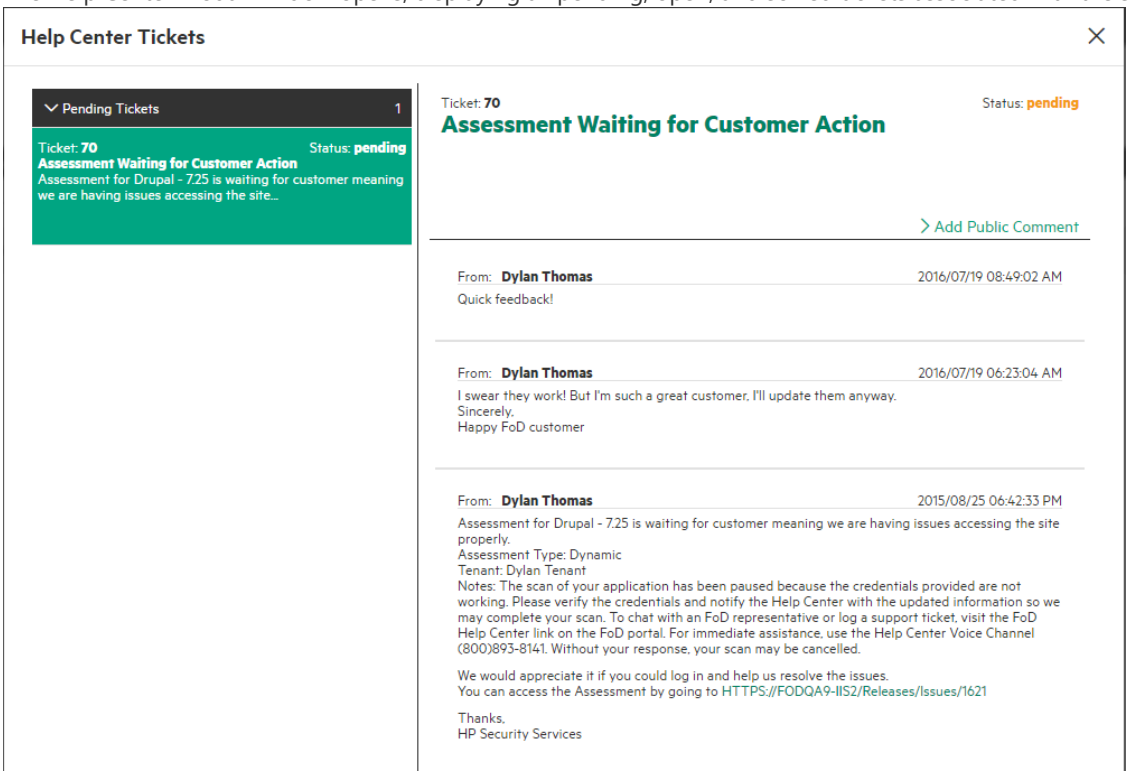
4.6.7. View tickets

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.
4. Click the icon.
   The Help Center modal window opens, displaying all pending, open, and solved tickets associated with the scan.



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.

5. Remediate vulnerabilities

When the testing team completes the scan, it publishes the scan results in the portal. Log in to OpenText Fortify on Demand to view your scan results and remediate vulnerabilities found in your application.

- Review issues
- Issue details
- Update issues
- Audit issue remediation
- Audit and remediation with Fortify Remediation Aviator
- Audit templates
- Dataflow cleanse rules
- Request a remediation scan

5.1. Review 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). 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.

Issues have one of 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, including the one immediately preceding the latest one.
Reopen	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.
Fixed/Fix Validated	A vulnerability appeared at least once previously, but it was not identified in the latest scan. **Fixed** vulnerabilities are hidden by default. To see **Fixed** vulnerabilities, select **Show... Fixed** on the Release Overview and Issues pages.

This section contains the following topics:

- View issues
- Navigate the issues page
- Filter and group the issues page
- Customize issue filters and groupings
- Assign attributes for an issue

5.1.1. View issues

View and manage security issues at both the application and release levels.

View application issues

You can view issues from all releases (excluding retired releases) of an application.

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. You can deselect individual issues when the group is selected.

View 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. You can deselect individual issues when the group is selected.

5.1.2. Navigate the issues page

The following tables describe how to navigate the Application Issues and the Release Issues pages.

General navigation

Task	Action
Submit false positive challenges	Click **Submit Challenge**. The **Submit False Positive Challenge** permission is required.
Export issue data	Click **Download** . 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. **Note** 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 **Enter**.
Show or hide fixed issues	Click **Show... Fixed** to switch between showing and hiding Fix Validated issues.
Show or hide suppressed issues	Click **Show... Suppressed** to switch between showing or hiding False Positive Confirmed and Suppressed issues.
Hide or display the filter list	Click **Filter**.
Customize filter and grouping options	Click **Setting**. Your selections determine the options shown on the Issues page.
Expand or collapse filters	Click **expand all** or **collapse all** or the arrow next to the filter name.
Apply a filter	Select desired filter values below the filter name. The page automatically refreshes with the filtered results. For some filters, click **apply** to refresh the page.
Save applied filters as query	Click **Save Query**. The Name Your Custom Query window appears. Type a name for the query and click **Save**. Your saved query appears in the **Canned Queries** filter.
Remove applied filters	Click **X** or **Clear Filters**.
Task	**Action**

Submit false positive challenges	Click **Submit Challenge**. The **Submit False Positive Challenge** permission is required.
Export issue data	Click **Download** . 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. **Note** 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 **Enter**.
Show or hide fixed issues	Click **Show... Fixed** to switch between showing and hiding Fix Validated issues.
Show or hide suppressed issues	Click **Show... Suppressed** to switch between showing or hiding False Positive Confirmed and Suppressed issues.
Hide or display the filter list	Click **Filter**.
Customize filter and grouping options	Click **Setting**. Your selections determine the options shown on the Issues page.
Expand or collapse filters	Click **expand all** or **collapse all** or the arrow next to the filter name.
Apply a filter	Select desired filter values below the filter name. The page automatically refreshes with the filtered results. For some filters, click **apply** to refresh the page.
Save applied filters as query	Click **Save Query**. The Name Your Custom Query window appears. Type a name for the query and click **Save**. Your saved query appears in the **Canned Queries** filter.
Remove applied filters	Click **X** or **Clear Filters**.

Navigation panel

Task	Action
Expand or collapse the panel	Click **navigation arrows**.
View issues by severity level	Select one of the following tabs: **Critical**, **High**, **Medium**, **Low**, **All**.
Group displayed issues by an attribute	Select a value from the **Group By** 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 though issues in a group	Click **navigation arrows** .

Task	Action
Expand or collapse the panel	Click **navigation arrows**.
View issues by severity level	Select one of the following tabs: **Critical**, **High**, **Medium**, **Low**, **All**.
Group displayed issues by an attribute	Select a value from the **Group By** 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 though issues in a group	Click **navigation arrows** .

Issue details panel

Task	Action
View a specific instance of an issue found in multiple releases	Select the issue ID, specific to a release, from the drop-down list. The issue details panel on the Release Issues page defaults to the issue specific to that release.
View analysis trace diagram of an issue along with others in the same category.	Click the **Smart Fix** 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 View issue details.
Task	**Action**
View a specific instance of an issue found in multiple releases	Select the issue ID, specific to a release, from the drop-down list. The issue details panel on the Release Issues page defaults to the issue specific to that release.
View analysis trace diagram of an issue along with others in the same category.	Click the **Smart Fix** 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 Viewing Issue Details.

Audit panel

Task	Action
Expand or collapse the panel	Click **navigation arrows**.
Edit an issue	Edit the available fields. For more information, see Update issues.
Submit an issue to a bug tracker	Click **Submit Bug**. For more information, see Submit issues to the bug tracker.
Add an audit filter for an issue	Click **Add Audit Filter**. For more information, see Create an application audit template filter for an issue.
Assign attributes for an issue	Click **Assign Attributes**. For more information, see Assign an attribute for an issue.
Task	**Action**
Expand or collapse the panel	Click **navigation arrows**.
Edit an issue	Edit the available fields. For more information, see Updating Issues.
Submit an issue to a bug tracker	Click **Submit Bug**. For more information, see Submit issues to the bug tracker.
Add an audit filter for an issue	Click **Add Audit Filter**. For more information, see Creating an Application Audit Template Filter for an Issue.
Assign attributes for an issue	Click **Assign Attributes**. For more information, see Assigning an Attribute for an Issue.

5.1.3. Filter and group the issues page

The following filter and grouping options are available on the Issues page:

Note

For a filter to appear in the filter list, the filter needs to be enabled (see Customizing Issue Filters and Groupings) and the results need to contain multiple values for that filter.

Filter and group	Description	Values
App Defender Status	Whether issue category is supported by Application Defender	Eligible, Not Eligible
Assigned user	User defined	Not Set, User-defined
Audited timestamp	Date of last update to the **Auditor Status** (filter only)	
Auditor status	Auditor issue remediation status.	• Unsuppressed system values: Pending Review, Remediation Required, Remediation Referred, Risk Mitigated, Suspicious, Proposed Not an Issue **Note** Suspicious and Proposed Not an Issue are set by Fortify Remediation Aviator. • Suppressed system values: Risk Accepted, Not an Issue, Aviator Auditor Status Suppressed • User-defined
Bug submitted	Issue was submitted as a bug to a bug tracker	False, True
Category	Issue category	
Canned queries	Default queries (filter-only option)	My Open Issues
Custom Queries	Saved custom queries (filter-only option)	User-defined
CRA 2024	Cyber Resilience Act (CRA) 2024 classification	
CWE	Common Weakness Enumeration classification	

CWE Top 25 2023	Common Weakness Enumeration Top 25 2023 classification	
CWE Top 25 2024	Common Weakness Enumeration Top 25 2024 classification	
CWE Top 25 2025	Common Weakness Enumeration Top 25 2025 classification	
Developer Status	Developer issue remediation status	• System values: Challenged, Open, In Remediation, Remediated, Will Not Fix, Third Party Component • User-defined
DISA STIG 6.1	DISA Application Security and Development STIG 6.1	
DISA STIG 6.2	DISA Application Security and Development STIG 6.2	
DISA STIG 6.3	DISA Application Security and Development STIG 6.3	
DISA STIG 6.4	DISA Application Security and Development STIG 6.4	
False Positive Challenge		Not Set, Challenged, Issue Confirmed
FISMA	FISMA classification (deprecated)	
Fortify Remediation Aviator	Audited by Fortify Remediation Aviator	False, True
Has attachments		False, True
Has comments		False, True
Has notes		False, True
Introduced date	Original date of issue creation (filter only)	

Remediation grace period	The remaining or overdue days. The field is applicable to issues with developer status category 'Open' only.	
Is suppressed	Issue is suppressed (filter only)	False, True
Issue age	Number of days the issue has been present in the application (filter only). 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
Microservice		
NIST SP 800-53 Rev. 5	National Institute of Standards and Technology Special Publication 800-53	
OWASP 2014 Mobile	OWASP mobile top 10 2014 classification	
OWASP 2017	OWASP top 10 2017 classification	
OWASP 2021	OWASP top 10 2021 classification	
OWASP 2025	OWASP top 10 2025 classification	
OWASP LLM Top 10 2025	OWASP LLM top 10 2025 classification	
OWASP API Top 10 2023	OWASP API top 10 2023 classification	
OWASP ASVS 4.0	OWASP ASVS 4.0 classification	
OWASP ASVS 5.0	OWASP ASVS 5.0 classification	
OWASP Mobile Top 10 2024	OWASP mobile top 10 2024 classification	
Package	Package or namespace	
PCI 4.0	PCI 4.0 classification	

PCI DSS 4.0.1	PCI 4.0.1 classification	
PCI SSF1.2	PCI SSF 1.2 classification	
Release	Release in which the issue was identified (filter only) **Note** The **Release** filter appears only on the Application Issues page.	
Scan tool	Scan tool used to find issue	DAST, DAST (Manual), SAST, MAST, Debricked, Sonatype
Scan type	Scan type to which issue belongs	Dynamic, Static, Mobile, Open Source
Scope	Production or non-production dependency (Fortify SCA scans)	
Severity	Issue severity (filter only)	Critical, High, Medium, Low, Best Practice, Info
Sink	Dataflow sink function, applicable for static scan issues	
Source	Dataflow source function, applicable for static scan issues	
Status	Issue status	New, Existing, Reopen, Fixed/Fix Validated
<Custom attribute>	Custom attributes	User-defined

5.1.4. Customize issue filters and groupings

You can customize issue filters and groupings shown 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	1. Select the **Filters** tab. 2. Select the check boxes next to filters you want to add. 3. Deselect the check boxes next to filters you want to remove. 4. Click **Save**. The Issues page refreshes with the new filters in the filters list. **Note** A filter only appears in the filter list when the results contain multiple values for that filter.
Customize issue groupings (**Group By** options in the navigation panel)	1. Select **Groups**. 2. Select the check boxes next to values you want to add to the **Group By** list. 3. Deselect the check boxes next to values you want to remove from the **Group By** list. 4. Click **Save**. The Issues page refreshes with the new group values.

5.1.5. Assign attributes for an issue

Attributes are informational only and do not influence the assessment process. Users with the necessary permissions can assign attributes to an issue from the Issues page.

To assign attributes for an issue:

1. Select the **Applications** view.
   Your Applications page appears.
2. Click the name of the application for which you want to assign attributes.
   The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page.
4. In the audit panel, click **Assign Attributes**.
   The Assign Attributes window appears.
5. Perform the relevant task:
   1. Select **group.**
   2. Enter the issue attributes.
   3. Click **Save**. The attributes are saved.

5.2. 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:

- Static scan issue
- Open source scan issue

- Dynamic scan issue
- Mobile scan issue

5.2.1. Static scan issue

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.

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 links to interactive training for the issue category, video about the issue category, and other educational resources. The **Interactive Training** section is powered by Secure Code Warrior. For more information about Secure Code Warrior, see Secure Code Warrior Integration.

Code

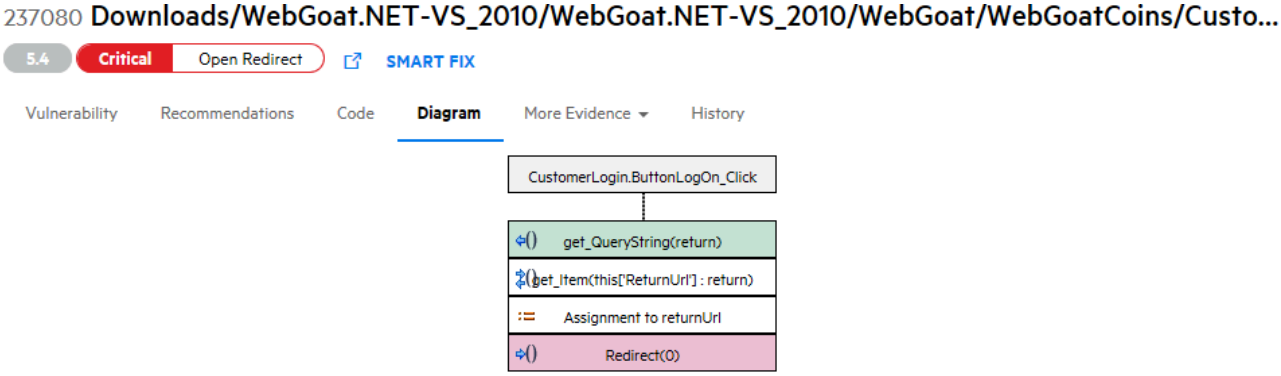
The Code tab displays the specific code where the issue was found. Users can perform the following actions to more easily review code:

- 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 trade 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.

Diagram

The Diagram tab displays an analysis trace diagram of the issue.
For example:



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 Upload screenshots.

History

The **History** tab displays a log of the following issue events: audit changes, comments, and system events (status changes, copy state actions, and False Positive Challenge results). You can filter the log by the event type (audit, bug tracker, comment, or system event).

5.2.2. Open source scan issue

The issues details panel for a 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 **Fix 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 links:

- Sonatype: https://guides.sonatype.com/iqserver/technical-guides/sonatype-vuln-data/
- Fortify SCA: https://debricked.com/docs/security/security-about#data-refinement

> **Note**
>
> In the Vulnerabilities API endpoint, Debricked issues are returned with the **CheckId** field populated as **Malware CVE.**

Recommendations

The Recommendations tab displays remediation information and references for further research. Click **View All Issues** to see all issues filtered by the package URL in the release.

In addition, Open Source Select health metrics are graphically displayed for Fortify SCA issues. Open Source Select is a database of all open source projects on GitHub.

Dependencies (Fortify SCA, CycloneDX)

The **Dependencies** tab displays a visualized dependency tree for the vulnerable component. A dependency tree appears for each root node (direct dependency) that contains the vulnerable component.

> **Note**
>
> Dependency trees are not available for SBOMs without dependency details and the `debricked.fingerprints.txt` file.

OpenText MSP Portal recommends reviewing the dependency tree and using the root fix solution to resolve the issue. A root fix contains the next version of the direct dependency that does not contain a vulnerable version of the affected dependency. In simpler terms, the root fix is a solution to a dependency vulnerability that starts at the root of the dependency tree. For more information on using root fix, see How do I manually solve a vulnerability with the Root fix solution?.

- For an issue found in different lock files, selecting a lock file from the drop-down list displays the full path of the selected lock file.
- A dependency tree can be expanded and collapsed.
- Vulnerable nodes are marked in red.

- The number of dependency trees displayed are the number of root nodes that have a known safe version or are lockfile-only fixes. A lockfile-only fix means that you can regenerate the lockfile in your repository and the vulnerability will be resolved. You do not need to update the direct dependency; instead reinstall the same version (for example: run yarn update and generate a new `yarn.lock` file).

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 Upload 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, and False Positive Challenge results). You can filter the log by the event type (audit, bug tracker, comment, or system event).

5.2.3. Dynamic scan issue

The issues details panel for a dynamic scan 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.

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.

HTTP

The **HTTP** tab displays the content, headers, and parameters of the request and response, which are accessed separately through the drop-down menu.

The **Evidences** section lists the complete session traffic that found the issue.

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 Upload screenshots.

History

The **History** tab displays a log of the following issue events: audit changes, comments, and system events (status changes, copy state actions, and False Positive Challenge results). You can filter the log by the event type (audit, bug tracker, comment, or system event).

5.2.4. Mobile scan issue

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.

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.

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 Upload screenshots.

History

The **History** tab displays a log of the following issue events: audit changes, comments, and system events (status changes, copy state actions, and False Positive Challenge results). You can filter the log by the event type (audit, bug tracker, comment, or system event).

5.3. Update issues

Using the information provided in your scan results, remediate the vulnerabilities that were found. You can update issues at both the application and release levels for the purpose of tracking remediation efforts.

Edit an issue

You can edit issues on both the Application Issues and the Release Issues pages. 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:

> **Note**
>
> The following instructions describe how to edit an issue on the Application Issues page. Selecting and updating issues works the same way on the Release Issues page.

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. Click **Issues**.
   The Application Issues page appears.
4. In the navigation panel, select the issue that you want to edit. If the issue is found in multiple releases, select a specific instance by selecting the issue ID, which is specific to the release, from the drop down list in the issue details panel.
5. In the audit panel, edit the fields as needed.

Field	Description
Assigned User	Select the user to be assigned the issue
Developer Status	Select the issue's development status. The default value is **Open**. Statuses fall under an open or closed state. ○ If you are reviewing the issue, select **In Remediation**. ○ If you do not believe that the issue is valid, select **False Positive Challenge**. See Submitting a False Positive Challenge for more information on the False Positive Challenge process. ○ 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**.
Auditor Status	Select the issue's audit status. 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**
Severity	Select a different severity to change the default issue severity.
Comment	Type any supporting comments in the **Comment** field and click **Add**.

6. Refresh the Issues page to see your issue changes.



Note

If an issue was suppressed, it is hidden on the Issues page and only appears when **Show... Suppressed** is selected.

Edit multiple issues

You can bulk edit multiple issues on both the Application Issues and the Release Issues pages.

To edit multiple issues:



Note

The following instructions describe how to edit multiple issues on the Application Issues page. Selecting and updating issues works the same way on the Release Issues page.

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. Click **Issues**.
   The Application Issues page appears.
4. Perform the following actions to select multiple issues:
   - In the navigation panel, select the check boxes next to the issues.

     Note
     On the Release Issues page, you can select the **Include Issues From Other Releases** check box to select all instances of the issue found in releases. Issues can be individually removed.

   - In the navigation panel, select the check box next to a group name to select all issues in the group.

     Note
     On the Release Issues page, you can select the **Include Issues From Other Releases** check box to select issues found in the same release as a separate group. Release groups can be individually removed.

5. Perform the following tasks to edit audit fields:

Task	Description
Manually edit audit fields	In the audit panel, edit the fields as needed. The following fields are available for editing: **Assigned User**, **Developer Status**, **Auditor Status**, **Severity**, and **Comments**.
Copy audit details from one issue to other issues	1. In the issues panel, click **View Audit Details** in the row of the issue that you want to copy. The Issue ID window appears. 2. Select the audit and comment entries that you want to copy. 3. Select the **Include Attachments** check box to copy all attachments. 4. Click **Copy Audit Details**. You are redirected to the Issues page. The audit values, along with selected audit entries, comments, and attachments, are applied to the other selected issues. **Note** Selected issues must have matching instance identifiers, otherwise you will not be able to proceed with copying audit details.

6. Click **Submit Changes**.
   The Issues page refreshes with your issue changes.

Upload 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:
     1. Select the **Upload Screenshot** tab.
     2. (Optional) Type a description of the file.
     3. Click **...** and browse to and select a screenshot.
     4. Click **Upload**.
   - To copy and paste the screenshot:
     1. Select the **Copy and Paste Screenshot** tab.
     2. (Optional) Type a description of the file.
     3. Copy an image to your clipboard.
     4. Select the box and press **Crtl+V** to paste the image from the clipboard.
     5. Click **Upload**.

5.4. Audit issue remediation

OpenText 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.

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.

Assign 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**: OpenText 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.
3. Select the developer to be assigned the issue from the **User** list.

Review 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.

Remediate 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:
    - If you do not believe that the issue is valid, flag the issue as a false positive. See Submitting a False Positive Challenge for more information on the False Positive Challenge process.
    - Remediate the issue.
    - Do not remediate the issue.

Close 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.

5.5. Audit and remediation with Fortify Remediation Aviator

The Fortify Remediation Aviator service leverages Generative Artificial Intelligence (GAI) with a third-party Large Language Model (LLM) to audit results and provide enhanced remediation guidance. Remediation guidance consists of comments added to scan results and includes code snippets.

Fortify Remediation Aviator is applied to scan results after the initial Fortify Audit Assistant audit. Fortify Remediation Aviator content is added to the scan results and imported to OpenText Fortify on Demand. The content is available in the portal and API.

Availability and Coverage

- Fortify Remediation Aviator is available for static assessments with Automated audit.
- For details on supported technology stacks, categories, and file types, see Fortify Static Code Analyzer and Tools.
- In the case of exceptionally large scan results and/or scan results with an exceptionally large number of issues in one category, Fortify Remediation Aviator might be restricted to a subset of issues in each category.

Issue processing quota

- Each new application starts with a 10,000-issue quota. The quota is consumed as Fortify Remediation Aviator audits issues, which are processed in batches by severity.
- The quota is replenished by 1,000 issues each month, up to the 10,000-issue maximum. Unused quota carries forward, subject to the maximum. Tenant users can view the remaining quota under **Remaining Aviator Issue Processing Quota** in the Scan summary.

  Example
  - If 500 issues are used from a 10,000-issue quota, the next month's quota is 10,000.
  - If 3,000 issues are used from a 10,000-issue quota, the next month's quota is 8,000.

- If the remaining quota is insufficient, the **Fortify Remediation Aviator Service Status** field in the scan summary displays: **Aviator scan could not start because the remaining quota is insufficient. Review your quota and rerun the scan.**

Note

If the Aviator service times out, the **Fortify Remediation Aviator Service Status** field displays: **Fortify Remediation Aviator service timed out and stopped. No results were applied. Rerun the scan.**

Audit and remediation guidance

Fortify Remediation Aviator reviews issues with the **Auditor Status** of **Pending Review**. Fortify Remediation Aviator updates the **Auditor Status** and adds notes. These actions are logged in the **History** tab of the issue details panel on the Issues pages. Audit actions are logged as **Audits**; remediation guidance are logged as **Comments**.

- False positives are marked as **Not an Issue** and automatically suppressed.
- Tentative false positives are marked as **Proposed Not An Issue** and are not suppressed.
- True positives are marked as **Remediation Required**. Remediation assistance consists of additional comments, including code snippets.
- Tentative true positives are marked as **Suspicious** and are not suppressed.
- Issues in unsupported frameworks, languages, or categories remain as **Pending Review**.

For more information on filtering and grouping issues, see Navigate the Issues page.

SAST-DAST correlation

SAST-DAST correlation uses Fortify Remediation Aviator to identify relationships between findings in SAST and DAST scan results. The capability is available only to customers who have Fortify Remediation Aviator and SAST and DAST subscriptions.

SAST-DAST correlation is a post-processing activity that is independent of SAST and DAST scan execution. It is automatically triggered when a release contains valid SAST and DAST FPR files with findings that are new, not suppressed, not fix-validated or removed, and not previously correlated.

For information about the correlation analysis performed by Fortify Remediation Aviator, see Fortify Remediation Aviator.

5.6. 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. You should review the documentation before using audit templates. If you have additional questions, contact the support team.

This section contains the following topics:

- Create a global audit template
- Create an application audit template
- Create an application audit template filter for an issue
- Audit template usage and examples

5.6.1. Create 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.
    1. Click **Add Filter**.
       A blank filter appears.
    2. Specify the filter conditions.
        1. 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 **Vulnerability** tab of the issue details panel.
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.
<Custom Application Attribute>	Static, dynamic, mobile	Custom attributes in your tenant (picklist, text, and boolean)
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
File Location	Open source	File location

2. 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

3. 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.

4. If needed, click **+** to create additional filter conditions.
5. Select **And** or **Or** to combine multiple filter conditions

3. In the THEN row, select one of the following audit actions to apply to matching results.

Operator	Description
Suppress	Suppresses the matching results. You can select the following auditor status to be applied when suppression occurs automatically. ▪ Pending Review ▪ Risk Accepted ▪ An an Issue ▪ Aviator Auditor Status Suppressed
Set Severity	Sets issue severity of matching results to the specified value.

5. To rearrange the location of a filter, click and drag the filter to your desired slot.
6. Once you are done adding and arranging filters, click **Save**.
   The global audit template is saved.

5.6.2. Create 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:

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. 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.
   1. Click **Add Filter**.
      A blank filter appears.
   2. Specify the filter conditions.
      1. 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 **Vulnerability** 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
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
File Location	Open source	File location

2. 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

3. Enter the value for the issue attribute. Wildcards are not accepted.

4. If needed, click **+** to create additional filter conditions.
5. Select **And** or **Or** to combine multiple filter conditions.

3. In the THEN row, select one of the following audit actions to apply to matching results.

Operator	Description
Suppress	Suppresses the matching results. You can select the following auditor status to be applied when suppression occurs automatically. ▪ Pending Review ▪ Risk Accepted ▪ An an Issue ▪ Aviator Auditor Status Suppressed
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.

5.6.3. Create 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.
4. In the audit panel, click **Add Audit Filter**.
   The Audit Template window appears.
5. Perform the relevant task. If the selected issue has existing filters that apply, those filters are displayed. You can edit the filters.



Note
If multiple filters apply and one of them is a suppression, only that filter is displayed.

   1. Click **Edit Filter(s)**.
      You are redirected to the Application Audit Template page.
   2. Edit the existing filters as necessary.
      If the selected issue does not have any filters that apply, you can create a new filter from a list of predefined conditions that apply to the issue.
   3. Select the filter conditions. Multiple conditions are joined with the AND operator.
   4. Select the audit action. For **Suppress**, the available options are 'Pending Review', 'Risk Accepted', 'Not an Issue' and 'Aviator Auditor Status Suppressed'. For **Set Severity**, the available options are 'Critical', 'High', 'Medium' and 'Low'.
   5. Click **Create Filter**. Your application audit template filter is saved.

5.6.4. 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, use 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.

5.7. 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 SAST 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. OpenText MSP Portal 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:

- Create a global dataflow cleanse rule
- Create an application dataflow cleanse rule
- Dataflow cleanse rule usage and examples

5.7.1. Create 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.
    1. Click **Add Rule**.
       The Add Rule window opens.
    2. 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 class. To specify a nested class, use the dot notation (for example, `OuterClass.NestedClass`). **Note** 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 `System.FuncT, TResult`, theclass name would be `Func@2`.
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:
	▪ **Return Value**: use this option to refer to `value` in `value = web.getWebInput(foo, bar)`
	▪ **Object Function**: use this option to refer to `web` in `value = web.getWebInput(foo, bar)` or `object` in `object = new MyObject()`
	▪ **Argument**: use this option when refering to arguments of the function. Arguments are indexed beginning with 0. For example, specify 1 to refer to `bar` in `value = web.getWebInput(foo, bar)`
	Example:
	`string filename = UploadedFile.FileName();`
	`if (Validators.IsValidFileName(filename))`
	`{`
	`System.IO.File.Delete(filename);`
	`}`
	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:
	Example1:
	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 an SQL Injection issue.
	Example2:
	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() menthod and is not flagged as an SQL Injection issue.

5. Once you are done adding rules, click **Save**.
   The global dataflow cleanse rules are saved.

5.7.2. Create 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.
    1. Click **Add Rule**.
       The Add Rule window opens.
    2. 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 class. To specify a nested class, use the dot notation (for example, `OuterClass.NestedClass`). **Note** 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 `System.Func<T, TResult>`, theclass name would be `Func@2`.
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: ▪ **Return Value**: use this option to refer to `value` in `value = web.getWebInput(foo, bar)` ▪ **Object Function**: use this option to refer to `web` in `value = web.getWebInput(foo, bar)` or `object` in `object = new MyObject()` ▪ **Argument**: use this option when refering to arguments of the function. Arguments are indexed beginning with 0. For example, specify 1 to refer to `bar` in `value = web.getWebInput(foo, bar)`

6. Once you are done adding rules, click **Save**.
   The application dataflow cleanse rules are saved.

5.7.3. 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 is not 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 is not flagged as a SQL Injection issue.

5.8. Request 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.
- The remediation scan period is 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

Some dynamic scan fields are locked for editing. For more information see Edit scan settings.

6. Dashboards and reports

OpenText 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. OpenText Fortify on Demand provides a comprehensive and customizable suite of reports.

- Dashboards
- Reports

6.1. Dashboards

OpenText Fortify on Demand provides dashboards that help you view and analyze application security data. Dashboards provide an overview of your application security program and key vulnerability metrics.

A dashboard includes:

- Data points for key metrics.
- Charts that visualize specific aspects of tenant data.
- Tiles that you can resize.

For information about the available dashboards and their charts, see Dashboard Types.

When you open the Dashboard view, the default dashboard is displayed. Use the dashboard selection list to switch dashboards.

Task	Action
Dashboard tasks	
Set the current dashboard as the default	Click **Mark as default**.
Filter dashboard charts	Select one or more values from the application and release filters, such as application type, business criticality, microservices, pass/fail, star rating, and SDLC status.
Print the dashboard	Click the **Print** icon on the toolbar. The dashboard opens in the browser print view, where you can print or save it.
Tile tasks	
Adjust a tile size	Hover over a tile border, then click and drag the handles.
Chart tasks	
Drill down into chart data	Point to a visual element and click when the pointer changes to a hand.

Limitations

- You cannot create new dashboards or customize existing dashboards.
- Issue counts in charts do not account for uniqueness.
- CSV export is supported for most chart types, but it is not available for all charts.
- You can filter and download chart data where applicable.

6.1.1. Dashboard types

The following dashboard types are available. Each dashboard presents charts that help you monitor coverage, risk, remediation activity, and program performance.

Program dashboard

The Program dashboard provides a high-level overview of your application security program. It includes:

- **Program overview:** Summarizes the current security posture and key activity across the program.
- **Application scan coverage:** Shows how broadly applications are covered by security scans.
- **Release scan coverage:** Shows how broadly releases are covered by security scans.
- **Scans requiring attention:** Highlights scans that need follow-up or corrective action.
- **DevSecOps automation maturity:** Indicates the adoption of automated security practices in development workflows.
- **Scan workflow adoption:** Shows how teams use and incorporate scanning workflows.
- **Application count by language:** Breaks down applications according to the programming languages they use.
- **Scan activity trend:** Shows how scan activity changes over time.
- **Entitlements:** Summarizes the entitlements available to and consumed by the organization.

Remediation dashboard

The Remediation dashboard highlights remediation activity and progress toward resolving risk. Use it to compare review and remediation coverage, monitor remediation times, and identify recurring issues. It includes:

- **Review coverage by severity:** Shows the proportion of issues reviewed in each severity category.
- **Review coverage by scan type:** Compares review coverage for DAST, SAST, MAST, and SCA findings.
- **Mean time to remediate:** Shows the average time taken to resolve issues.
- **Remediation coverage by severity:** Shows the proportion of issues remediated in each severity category.
- **Remediation coverage by scan type:** Compares remediation coverage for DAST, SAST, MAST, and SCA findings.
- **Mean time to remediate by severity:** Compares average remediation time across severity categories.
- **Issue remediation trend:** Shows how remediation activity changes over time.
- **Issue reopened rate:** Shows how often remediated issues are reopened.
- **Frequently reopened issues:** Identifies issues that are reopened repeatedly and may require additional investigation.
- **SAST Aviator adoption:** Shows the use of SAST Aviator capabilities across the program.
- **SAST Aviator return on investment (ROI):** Summarizes the value gained from using SAST Aviator capabilities.

Risk exposure dashboard

The Risk exposure dashboard focuses on identifying and assessing risk across the program. Use it to examine open issues, compliance, release risk, and software composition risk. It includes:

- **Release by compliance policy:** Shows how releases are distributed according to compliance policy results. Retired releases are excluded.
- **Open issues by severity:** Shows the number of open issues in each severity category.
- **Releases by star rating:** Shows how releases are distributed by star rating. Retired releases are excluded.
- **Usage overview by scan type:** Shows scan usage across Static, Dynamic, Open Source, and Mobile testing.
- **Open source security risk:** Summarizes risk identified in open source components.
- **Issue density:** Shows the concentration of issues in the application and release portfolio.
- **Most prevalent issues:** Identifies the issues that occur most frequently across the program.

Interactive charts provide links that you can use to drill down into data sets. Trending charts do not render until sufficient data is available.

6.2. Reports

OpenText Fortify on Demand offers the ability to generate detailed reports of assessment results. You can generate pre-defined system reports, custom reports, data exports, and vendor reports if you use the Vendor Management feature.



Note

Open source component reports are available through the OpenText Fortify on Demand report functionality. Use the Open Source Component system template to generate a report. The template includes Open Source Bill-of-Materials and Vulnerable Open Source Components modules.

Filter Your Reports page

By default, the Your Reports page displays reports created during the last seven days. Apply filters to limit the reports displayed.



Note

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

Filter	Description	Values
Application	Application associated with the report.	User-defined.
Created Date Range	Date when the report was generated.	
Created By	User who generated the report.	User-defined.
Release	Release associated with the report.	
Report Template	Report template type.	System-defined or user-defined.
Status	Report generation status.	Queued, Started, or Completed.

This section describes how to view reports and access reports for specific applications or releases.

- View reports
- Generate a report
- Schedule auto-generated reports
- Templates
- Data exports

6.2.1. View reports

There are two ways to view reports in the portal:

- Use the **Reports** view to view all reports generated for applications and releases in your tenant.
- Use the **Applications** view to select an application and view reports for a specific application or release.

View all reports

Your Reports page is the default landing page of the Report view, where you can view reports for all your applications at the tenant level.

To view reports at the tenant level:

1. Select the Reports view.
   Your Reports page appears. The page displays the application and release that the report is for, the date and time of report creation, the report type, the status of the report generation, and the user who generated the report.

The following table describes how to navigate Your Reports page.

Task	Action
Search the reports list	Type a keyword or phrase in the **Search Text** field and click **Enter**. To remove the search results, Click the X. For information on using the **Search Text** box, see About Searching Applications.
Import a custom report	Click **Import**.
Create a report	Click **+New Report**.
Hide or display filter lists	Click **Filter**.
Expand or collapse filters	Click **expand all** or **collapse all** or the arrow next to the filter name.
Apply filters	Select desired filter values below the filter name. The page automatically refreshes with the filtered results. For some filters, click **apply** to refresh the page.
Remove applied filters	Click **X** next to each applied filter or click **Clear Filters**.
Download a report	Click **download**. The report is downloaded to the local folder specified in your browser settings.
Delete a report	Click **delete**.
Share a report with a tenant	Click share. Sharing a report is available if you have established a relationship with another tenant. See Vendor Management. **Note** Sharing a report that contains multiple releases is currently not available.

View application reports

You can view reports for a selected application.

To view reports for 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 displays all reports for the application.
4. Select a report from the list.

View release reports

You can view reports for a selected release.

To view reports for 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 for which you want to view reports.
   The Release Overview page appears.
4. Click Reports.
   The Reports page displays all reports for the release.
5. Select a report from the list.

6.2.2. Generate 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.

> **Note**
>
> In the event a PDF report generation fails, the HTML version is automatically provided in place of the PDF version.

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.

To generate a report on Your Reports page :

1. Select the **Reports** view.
   Your Reports page appears.
2. Click +New Report.
   The Create Report wizard appears.
3. **Select Application**: select the application and click **Next**.
4. **Select Releases**: select the releases and click **Next**. If you select multiple releases, a report will be generated for each release and the reports will be packaged in a zip file.
5. **Report Details**: complete the fields and click **Next**. Fields are required unless otherwise noted.

Field	Description
Report Name	Provide the name of the report.
Notes	Provide notes for the report.
File Type	Select the file type of the report: **PDF**, **HTML**.

6. **Report Template**: select a report template type and click **Next**.
   - System report templates appear in blue; custom report templates appear in black.
   - If your release has only static issue data, only static report templates are available.

- If your release has only dynamic issue data, only dynamic report templates are available.

7. **Summary**: review the summary of the report and click **Generate**.
   You are redirected to the Reports page. The report is available once the "Completed" status appears.

   > **Note**
   > Click **Delete** to remove a report that is still being generated.

8. Click **Download** in the report row after the report generation completes.
9. A PDF or zip file (depending on the file type) is saved to the folder specified in your browser settings.

6.2.3. Schedule auto-generated reports

If you plan to run multiple assessments on the same application and you need 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.
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.
5. Select the report template to generate a report after a **static scan** completes.
6. Select the report template to generate a report after a **dynamic or mobile scan** completes.
7. Select the template to generate a report upon completion of an Open Source scan.

   > **Note**
   > This applies to both Debricked and Sonatype scans.

- Select the SDLC status check box(es) that triggers the report generation.
- Select the report file type from the **File type** list.
- To automatically distribute the reports to specified recipients, select **Email Report Upon Completion** and in the **Notification List** field, type the email addresses that receives the reports.
- Click **Save**.
  Your auto-generated report settings are saved.

6.2.4. Templates

Users with the Create Report permission can view, create, edit, and delete report templates. The Templates page lists existing report templates. There are two types of report templates:

- System: System report templates are available for Dynamic, Hybrid, Mobile, PCI, STIG, and FISMA reports. You can copy and suppress system templates, but you cannot edit or delete them.
- Custom: OpenText Fortify on Demand provides a **Template Wizard** for creating custom report templates. Configure the report modules and filters to include in the template, and then use the template to generate reports that contain the information most useful to your organization. You can edit and delete custom report templates.

> **Note**
>
> **Use case**: For a high-level management report, select the **Static Summary** template. It includes a title page, executive summary, issue breakdown, issues by analysis type, and the OWASP Top 10. It does not include PCI reporting, comments on issue details, or an analysis trace report unless you add those modules.

Create a custom report template

Create a custom report template from scratch or copy a system template and modify it.

To create a custom report template:

1. Select the Reports view.
2. Click Templates.
   The Templates page appears.
3. Perform one of the following actions:
   - Click **+New Template** to create a template from scratch.
   - Click **Copy** in the desired system template row to copy the template.

   The Add/Edit Report Template wizard appears.
4. On the **Template Details** page, enter a name in the **Template Name** field and click **Next**.
5. On the **Filters** page, select the required 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: **New**, **Existing**, or **Reopen**.
Developer Status	(Optional) Developer status of the issues.
Auditor Status	(Optional) Auditor status of the issues.
Issue Age	(Optional) Number of days since the issues were first introduced.
Category	(Optional) Vulnerability category of the issues.
Is Suppressed	(Optional) Suppression state of the issues. The default value is **False**.
False Positive Challenge	(Optional) False Positive Challenge status of the issues.

6. On the **Modules** page, 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 available modules depend on the selected scan type.
   - Drag and drop items in the **Report Layout** column to change the order of the modules in the generated report.
7. On the **Summary** page, review the template details and click **Save**.
   The custom report template appears in the template list. If necessary, search for the template by name.

Edit a custom report template

Edit an existing custom report template in 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 **Edit** in the row of the template that you want to edit.
   The Add/Edit Report Template wizard appears.
4. Edit the fields in each wizard step as needed, and then click **Save**.

> **Note**
> Removing deprecated modules is permanent and cannot be undone after you save the template.

The template changes are saved.

Delete a custom report template

You can delete any custom report template 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 **Delete** in the template row.
   A confirmation message appears.
5. Click **Yes** to delete the template.

Suppress a system report template

Security Leads can prevent users from viewing or using a system report template during report generation by suppressing the template.

To suppress a system report template:

1. Select the Reports view.
2. Click Templates.
   The Templates page appears.
3. Click **Suppress** next to the system template that you want to suppress.
   A confirmation message appears.
4. Click **Yes** to confirm the suppression.
   The system report template is shown as suppressed. To make it available again, click **Restore** next to the template.

6.2.5. Data exports

A data export is a complete list of data for a specific category across the tenant. Categories include applications, releases, scans, issues, and entitlement consumption. Users with the Export Data permission can generate data exports. Each data export is provided as a CSV file.

This topic describes how to view data exports, create data export templates, and generate data exports.

View 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 following table describes the actions available on the Data Export page.

Task	Action
Create a data export template	Click **+New Data Export**.
Generate a data export using an existing template	Click **Run Export Now** in the template row.
Edit a data export template	Click **Edit** in the template row.
Delete a data export template	Click **Delete** in the template row. You cannot delete a template that has an existing data export.
View generated data exports for a template	Click **Expand** in the template row. The page displays files generated for the template during the last three months.
Delete a data export	Click **Delete** in the data export row. If the data export is running, the action cancels it.
Download a data export file	Click **Download** in the data export row.

Create a data export template

Use a data export template to define the data included in an export. You can apply filters and schedule recurring exports.

To create a data export template:

1. Click the Reports view, and then click **Data Export**.
   The Data Export page appears.
2. Click **+New Data Export**.
   The Data Export wizard appears.
3. On the **Start Page**, complete the fields and click **Next**.

Field	Description
Name	Enter a name for the data export template.
Template	Select Applications, Application Releases, Scans, Issues, or Entitlement Consumption.
Schedule	Select **Queue Now** or **Recurring**. Recurring exports can be enabled for automatic generation.

4. On the **Filter** page, select the required filters and click **Next**. The available filters depend on the template type.

   Note
   The **Scan Start Date** filter is required for scans. The **Introduced Date** filter is required for issues. The **Start Date** filter is required for entitlement consumption.

5. On the **Columns** page, select the columns to include in scans and issues data exports, and click **Next**.
6. For a recurring data export, select the repeat frequency and day or date on the **Schedule** page, and then click **Next**.

> **Note**
> Data exports run at 24:00 server time.

7. On the **Summary** page, review the data export details and click **Save**.
   The data export template appears in the data export list.

Generate a data export

Generate a data export from an existing data export template.

> **Note**
> A data export contains only the results of completed assessments available when the export is generated. The Entitlement Consumption data export is an exception.

To generate a data export:

1. Click the Reports view, and then click **Data Export**.
   The Data Export page appears.
2. Click **Run Export Now** in the data export template row.
   The data export is queued for generation.
3. Click **Expand** next to the template to view the generated data exports.
   The status is **Processing** until the data export is available.

   > **Note**
   > To cancel a long-running data export, click **Delete**.

4. After the data export is generated, click **Download** in the data export row.
   The browser saves the CSV file to the folder specified in its settings.

7. Administration

Administration of your tenant is performed from the portal. Access and privileges are determined by the user role.

7.1. 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:

- Configure user security
- Manage API keys
- Manage attributes
- Manage networks
- View entitlements
- View administration event log
- Configure SAST

7.1.1. Configure user security

Security Leads can configure the following user security settings:

- Password reset frequency
- Maximum personal access token lifetime
- Two-factor authentication

- IP restrictions

> **Note**
> The IP restrictions feature is disabled for 24.3.

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.
4. Edit the fields as needed.

Section	Procedure
Password expiration frequency	To specify the password reset frequency for new passwords: In the **Pasword Reset Frequency** 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 **MAX Personal Access Token Lifetime** field, specify the maximum personal access token lifetime. The new value overrides the default value of 180 days.
Two-factor authentication	Protect user accounts by configuring two-factor authentication. Once it is configured, all users will be required to log in using two-factor authentication. To configure two-factor authentication: 1. In the **Enable Two Factor Authentication** field, move the move the slider from **No** to **Yes** to enable two-factor authentication. 2. Select whether users can receive the login code by email, SMS, TOTP or all three methods. When you try to log in for the first time after the TOTP is enabled by the security lead, a new Fortify on Demand page with QR code will appear. 3. Select how often a user is prompted for a two factor authentication code from the **Frequency** list: **Every login**, **4 hours**, **8 hours**, **12 hours**, **24 hours**.

<table>
<tr>
<td>Ip restrictions</td>
<td>Limit access to the tenant by restricting access to users logging in from particular IP addresses.
To restrict access to particular IP addresses:
1. In the Enable Login Restriction field, move the move the slider from No to Yes to enable IP restriction.
2. In the Allow technical account managers (TAMs) access from any IP address field, move the slider from No to Yes to allow a TAM to access your tenant from any IP address.
3. Perform the following tasks to manage the IP addresses that have access to the tenant.
<table>
<tr><th>Task</th><th>Procedure</th></tr>
<tr><td>Add an IP address to the allowed list</td><td>Click +Add 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>Remove an existing IP address from the allowed list</td><td>Click x next to an IP address in the Allow IP Addresses list.</td></tr>
</table>
</td>
</tr>
</table>

5. Click **Save**.
   Your user security settings are saved.

7.1.2. Manage API keys

API keys are used to authenticate to the OpenText Fortify on Demand API. Security Leads can manage API keys.

> **Note**
>
> This section covers the management of API keys. For information on using the OpenText Fortify on Demand API, see Application Programming Interface (API).

Create 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.
4. Click **+Add Key**.
   The **Add/Edit Key for Application** window opens.
5. Complete the fields. Fields are required unless otherwise noted.

Field	Description
Application Name	Name of your application.
Role	Select the role that has the appropriate API key permissions. See API key roles.
Authorize app to use API	Select **Yes** to enable the key. Select **No** to disable the 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 shown only 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 for information on assigning applications to an API key.

Edit or delete 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	1. Click **New Secret**. A confirmation message appears. 2. Click **Yes**. This voids the current secret.
Edit API key settings	1. Click **Edit**. The Add/Edit Key for Application window opens. 2. Edit the fields as needed.
Delete API key	1. Click **Delete**. A confirmation message appears. 2. Click **Yes**.
Assign applications to API key	1. Click **Assign Applications**. 2. Select the **Available** tab.  3. Perform the following actions to select applications: ▪ Select the check box next to individual applications. ▪ Select the **ASSIGN** check box to select displayed applications. ▪ Select the **Assign All Tenant Applications** check box to select all applications. Use the search field to filter the application list. 4. Click **Save**.
Unassign applications from API key	1. Click **Assign Applications**. 2. Select the **Selected** tab.  3. Perform the following actions to remove applications: ▪ Clear the check box next to individual applications. ▪ Clear the **ASSIGN** check box to remove displayed applications. ▪ Select the **Unassign All Tenant Applications** check box to remove all applications. Use the search field to filter the application list. 4. Click **Save**.

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 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
Manage Users	View User IDs, View User Groups, Manage User IDs, Manage User Groups	Integration with full-featured custom or internal systems with the ability to manage users

7.1.3. Manage attributes

Attributes provide additional information about applications; they are used as filters to help track applications, releases, micro services, issues and scans . 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)**.
- Scan attributes: Scan attributes are custom attributes.

Add 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.

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. The available options are: ○ Application ○ Microservice ○ Release ○ Issue ○ Scan
Data type	Select the data type: ○ **Picklist**: 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. ○ **Text**: 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. ○ **Boolean**: this attribute type allows selection of binary values (**true/false**). ○ **Date**: this attribute type allows selection of a date from a calendar. ○ **User**: this attribute type allows selection of a user from a list of all active users for the tenant.
Required (optional)	Select the check box to designate the attribute as required. This field is not available for issue and scan attributes.
Editable only by Security Leads (optional)	Select the check box to restrict its usage to Security Leads. This option supersedes the **Manage Application** permission. **Note** Selecting this precludes making an attribute required, as it would break the **Create Application** permission for non-Security Leads.
Specify the default value	Enter the default value based on the selected data type. If the **Data Type** is **Picklist**, you can select a default value from the list. **Note** This field is applicable only when the **Required** and **Editable only by Security Leads** fields are both enabled.

5. Click **Save**.
   The new attribute appears in the attribute list.

Edit an attribute

Security Leads can edit picklist values and certain settings for existing attributes. You cannot 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.
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	○ Click + to add a new value. ○ Use ^ v to reorder the listed values. ○ Click to sort values alphabetically. ○ Click X to remove a value from the list.
Picklist, Text, Boolean, Date, User	Select or deselect the following check boxes: ○ **Required**: designate the attribute as required. ○ **Editable only by Security Leads**: Restrict attribute usage to Security Leads. This option supersedes the **Manage Application** permission. **Note** Selecting this precludes making an attribute required, as it would break the **Create Application** permission for non-Security Leads.

5. Click **Save**.
   Your attribute changes are saved.

Delete 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.

3. Click **Delete** in the row of the attribute that you want to delete.
   A confirmation message appears.
4. Click **Yes**.
   The attribute and all associated values are deleted.

7.1.4. Manage networks

OpenText Fortify on Demand Connect is used to establish site-to-site VPN for dynamic assessments. Security Leads can manage OpenText Fortify on Demand Connect networks, which are used to register VPN clients with the VPN server.

Add a OpenText Fortify on Demand Connect network

Security Leads can add OpenText Fortify on Demand Connect networks, which are referenced in the site-to-site VPN configuration.

To add a OpenText Fortify on Demand Connect network:

1. Select the **Administration** view.
   The User Settings page appears.
2. Click **Settings**.
   The **Attributes** tab of the Settings page appears.
3. Select the **OpenText Fortify on Demand Connect** tab.
4. Click **+Add Network**.
   The Add Network window appears.
5. Complete the following fields. Fields are required unless otherwise noted.

Field	Description
Network Name	Specify the network name.
User Name	Specify a OpenText Fortify on Demand Connect network username.
Password	Specify a OpenText Fortify on Demand Connect network password. Allowed characters are uppercase and lowercase letters and numbers.
Confirm Password	Specify the password again.

6. Click **Save**.
   The new network appears in the network list. The **View Docker Commands** link contains the code for the Docker command to run the VPN client and initialize the connection between the VPN client and the VPN server.

Delete a OpenText Fortify on Demand Connect network

Security Leads can delete OpenText Fortify on Demand Connect networks.



Note

OpenText Fortify on Demand Connect networks cannot be edited. To update an existing network, delete the network and add a new one.

To delete a OpenText Fortify on Demand Connect network:

1. Select the **Administration** view.
   The User Settings page appears.
2. Click **Settings**.
   The **Attributes** tab of the Settings page appears.
3. Select the **OpenText Fortify on Demand Connect** tab.

4. Click **Delete** in the row of the network that you want to delete.
   A confirmation message appears.
5. Click **Yes**.
   The network is deleted.

7.1.5. View entitlements

Security leads can view a list of expired and active entitlements for the tenant.

To view entitlements for the tenant:

1. Select the **Administration** view.
   The User Management page appears.
2. Click **Entitlements**.
   The Entitlements page appears. The page displays details such as 'Entitlement ID', 'Entitlement Type', 'Analysis Type', 'Quality Purchased', 'Developer Count', 'Quantity Consumed', 'Start Date', 'End Date', 'Reminder Date', 'Description' and 'Action'.
3. You can perform the following tasks.

Task	Procedure
Add or edit the entitlement description	Click **Edit** in the row of an entitlement and provide a description. The description is limited to 50 characters.
Add or edit email reminders for expiring entitlements	Click **Edit Reminders**. Complete the following fields: ○ **First Reminder (days)**: Select the number of days before an entitlement expires at which the reminder will be sent. ○ **Second Reminder (days)**: If you want to add another reminder, select the check box and select the number of days before an entitlement expires at which the reminder will be sent. ○ **Email To**: Specify email addresses separated by a comma. Once set up, the reminders are applied to every entitlement in the tenant.

7.1.6. View 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 **Export**. 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 **Enter**
Hide or display the filter list	Select **Filters**
Expand or collapse filters	Click the arrow next to a filter category to expand or collapse it
Remove applied filters	Click **X** or click **Clear Filters** at the top of the page. The filter is set to the last 24 hours by default

7.1.7. Configure SAST

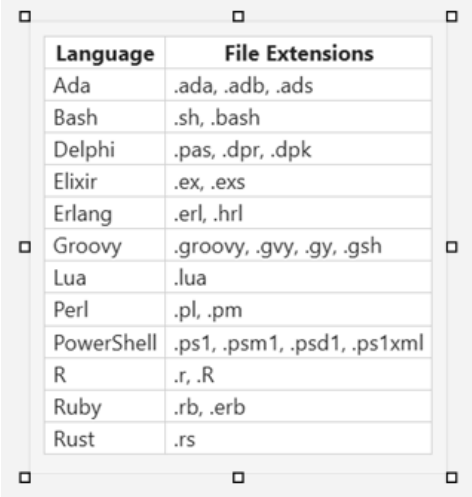
Security leads can configure the auditor status, enabling customers to manage it themselves.

To configure the Fortify Remediation Aviator auditor status.

1. Select the **Administration** view.
   The User Settings page appears.
2. Click **Settings**.
   The **Attributes** tab of the Settings page appears.
3. Select the **SAST** tab.
4. Specify values for the fields. All fields are mandatory unless otherwise noted.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Enable AI-Powered SAST</td><td>Select the check-box and accept the agreement to enable AI-powered SAST.

SAST has introduced AI-powered scanning support for the following 12 programming languages.



This capability is built on the next-generation SAST architecture, which enables significantly faster onboarding of additional languages in future releases. To align with this enhancement, OpenText Fortify on Demand has added support for scanning these languages using the new architecture.

Note
If the agreement is accepted, the check-box is selected and the setting is saved at the tenant level. If the agreement is not accepted, the check-box remains unselected.</td></tr>
<tr><td colspan="2">Configure Aviator Auditor Status</td></tr>
<tr><td>Tier</td><td>Indicates the Aviator tier:
• Tier1 - Languages such as Java and .Net
• Tier2 - Rest of the languages</td></tr>
<tr><td>Aviator outcome</td><td>Indicates the Aviator outcome.</td></tr>
<tr><td>Auditor Status</td><td>Select the Aviator status. Based on the selected status, Aviator configures the auditor status.</td></tr>
</table>

Language	File Extensions
Ada	.ada, .adb, .ads
Bash	.sh, .bash
Delphi	.pas, .dpr, .dpk
Elixir	.ex, .exs
Erlang	.erl, .hrl
Groovy	.groovy, .gvy, .gy, .gsh
Lua	.lua
Perl	.pl, .pm
PowerShell	.ps1, .psm1, .psd1, .ps1xml
R	.r, .R
Ruby	.rb, .erb
Rust	.rs

1. Click **Save** to save the configuration mappings. You can configure the mappings to any auditor status available in the portal.

7.2. User management

Security Leads and users with the Manage Users permissions can manage users in OpenText 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:

- Roles and permissions
- Manage users
- Manage groups
- Configure System for Cross-domain Identity Management (SCIM)

7.2.1. Roles and permissions

User actions in OpenText 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.

Six default roles are available. 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:

- Default roles
- Manage roles
- Permissions

7.2.1.1. Default roles

OpenText 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**	**Application lead**	Executive	Reviewer
Tenant level permissions						
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					
Application level permissions						
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

Start Mobile scans	Start	Deny	Start	Start	Deny	Deny
Configure build server	X					
Submit false positive challenge	X					
Consume entitlements	X	X	X	X	X	X

7.2.1.2. Manage roles

Use the Roles tab to view and manage tenant roles.

To view roles in your tenant:

1. Select the **Administration** view.
   The User Management page appears.
2. Select the **Roles** tab.

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 **Enter**. To remove the search results, remove the text from the search field and press **Enter**.
Create a role	Click + **Add Role**. For instructions, see Create a role.
View users assigned to a role	Click **View Users** in the action column.
Edit a role	Click **Edit** in the action column. For instructions, see Edit a role.
Delete a role	Click **Delete** in the action column. For instructions, see Delete a role.

Create a role

To create a role:

1. Select the **Administration** view.
   The **User Management** page appears.
2. Select the **Roles** tab.
   The Roles tab appears.
3. Click **+ Add Role**.
   The Add/Edit Role window appears.
4. In the **Role Name** field, enter the name of the new role.

5. Select tenant-level and application-level permissions for the role. For information about permissions, see Permissions.
6. Click **Save**.
   The new role appears in the role list.

Edit a role

To edit a role:

1. Select the **Administration** view.
   The **User Management** page appears.
2. Select the **Roles** tab.
3. Click **Edit** in the row of the role that you want to edit.
   The Add/Edit Role window appears.

   > **Note**
   > You cannot edit the permission sets for the security lead or developer roles.

4. Edit the fields as needed.
5. Click **Save**.
   Your changes are saved.

Delete a role

You cannot delete the security lead or developer roles, or a role that has assigned users.

To delete a role:

1. Select the **Administration** view.
   The **User Management** page appears.
2. Select the **Roles** tab.
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.

7.2.1.3. Permissions

Permissions specify the actions a user can perform. OpenText Fortify on Demand permissions are divided into two types:

- **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.
- **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.

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)	• Manage security policies • Manage attributes • Configure user security • Manage API keys • Configure Application Defender • Configure SSO • View administration event log • Manage roles • Manage global audit templates • Download static scan payload for all applications
Application access	• **Manual** - Applications are not assigned by default. Applications must be assigned to a user or group. If **Manual** is selected, **Manage Users**, **Export Data**, **Vendor Management**, are set to **Deny**. • **All** - Access to all applications. No restrictions on tenant level permissions.	Determined by the application level permissions assigned to the role
Manage users	**Deny**, **Allow** (requires **Application Access** be set to **All**)	• Add, edit, and delete users (only security leads can edit other security leads) • Export user data • Manage groups • Assign training courses to users • View training report
Export data	**Deny**, **Allow** (requires **Application Access** be set to **All**)	• View Data Exports tab • Create data exports • Edit data export templates • Delete data export templates • Generate data exports • Download data exports • Delete data export files
Vendor management	**Deny**, **Allow** (requires **Application Access** be set to **All**)	• Verify and Approve Vendor • Request to be Vendor • Publish Report to Vendor

Download tools	**Deny**, **Allow**	View Tools page
Access training	**Deny**, **Allow**	Take training courses
View Third Party Apps	**Deny**, **Allow**	View open source components in use across all applications
Configure Webhooks	**Deny**, **Allow** (requires **Application Access** be set to **All**)	Manage webhooks
Dashboards	**View**, **Create**	View new dashboards Manage new dashboards (upcoming)

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	**View**, **Manage**, **Create**	View • View issues, scans, and reports • Download scan results (FPRs and SBOMs) Manage • All **View** permission actions • Edit application settings (except for application name) • View users assigned to application • Create release • Edit release settings • Delete release • View and export application event log • Import scan results (FPRs and SBOMs) Create • All **Manage** permission actions • Create new application • Edit application name • Delete application
Issues	**View**, **Edit**, **Audit**	View • Add and delete screenshot • Export the issues list Edit • All **View** actions • Edit **Assigned User** and **Developer Status** fields, add comment • Submit bug Audit • All **Edit** actions • Edit **Severity** and **Auditor Status** fields • Create and edit application audit template

Reports	**View**, **Create**	View • View main reports • Download main reports • View vendor reports • Download vendor reports • Export tenant dashboard • Export Your Releases page Create • Create reports • Delete reports • View report templates • Create report templates • Edit report templates
Start Dynamic scans	**Deny**, **Configure**, **Allow**	Configure • Edit Dynamic Scan Setup page Allow • Schedule dynamic scan • Cancel dynamic scan
Start Static scans	**Deny**, **Configure**, **Allow**	Configure • Edit Static Scan Setup page Allow • Upload static scan payload • Cancel static scan • Download static scan payload for assigned applications
Start Mobile scans	**Deny**, **Configure**, **Allow**	Configure • Edit Mobile Scan Setup page Allow • Schedule mobile scan • Cancel mobile scan
Submit false positive challenge	**Deny**, **Allow**	Submit false positive challenges
Consume entitlements	**Deny**, **Allow**	Consume entitlements when starting a scan

7.2.2. Manage users

Users with the **manage users** permission can manage tenant user accounts and their application access.

View users

To view users in your tenant:

1. Select the **Administration** view.
   The **Users** tab of the User Management page appears and displays the user list.

The following table describes the actions available on the **Users** tab.

Task	Action
Search the user list	Enter a word or phrase in the search field and press **Enter**. To clear the search results, remove the text and press **Enter**.
Export the user list	Click **Export**. A CSV file containing user details is saved to the folder specified in your browser settings.
Add a user	Click **Add User** to open the Add/Edit User window. See Create a user.
Manage applications assigned to a user	Click **Assign Applications** in the user's row. See Manage application assignment to a user.
View applications assigned to a user	Click **View Applications** in the action column.
Edit a user	Click **Edit** in the action column. See Edit a user account.
Delete a user	Click **Delete** in the action column. See Delete a user account.

Create a User

To create a user:

1. Select the **Administration** view.
   The **Users** tab of the User Management page appears.
2. Click **+ Add User**.
   The Add/Edit User window appears.
3. Complete the fields as needed. Fields are required unless otherwise noted.

Field	Description
User Name	Enter a unique username. You cannot change the username after creating the user.
Email	Enter the user's email address.
First Name	Enter the user's first name.
Last Name	Enter the user's last name.
Phone Number	Optional. Enter the user's phone number. Hyphens and other separators are not accepted.
Role	Select a role. The default role is **Developer**. For more information, see Manage Roles.
Password never expires	Optional. Select the check box to make the password permanent.
Inactive	Optional. Select the check box to prevent the user from signing in.

4. Optional. Select the groups to assign to the user. Use the search box to filter the group list.
5. Click **Save**.
   The new user appears in the user list.

Edit 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.
2. Click **Edit** in the row of the user you want to edit.
   The Add/Edit User window appears.
3. Edit the fields as needed. To reset a user's password, use these fields.

Field	Description
Password	Enter a new password that meets the complexity requirements.
Confirm Password	Enter the same password again.
Must change on next login	Select the check box to require the user to change the password at the next sign-in.
Password never expires	Select the check box if the password should not expire.
Inactive	Select the check box to make the user inactive.
Reset TOTP code	Select the check box to reset the user's TOTP code.

4. Click **Save**.
   The user changes are saved.

Manage application assignment to a user

Users with the **Manage Users** permission can manage a user's application access from the Administration view.

To manage application access for a user:

1. Select the **Administration** view.
   The Users tab of the User Management page appears.
2. Click **Assign Applications** in the row of the user.
   The Assign Application window appears.

   > **Note**
   > This action is unavailable if the user is assigned to a role with the **All Application Access** permission.

3. To assign applications, select the **Available** tab and select applications using one of these options:
   - Select the check box next to each application.
   - Select the **ASSIGN** check box to select the displayed applications.
   - Select **Assign All Tenant Applications** to select all applications.

   Use the search field to filter the application list.
4. To remove applications, select the **Selected** tab and clear applications using one of these options:
   - Clear the check box next to each application.
   - Clear the **ASSIGN** check box to remove the displayed applications.
   - Select **Unassign All Tenant Applications** to remove all applications.

   Use the search field to filter the application list.
5. Click **Save**.
   The user's application assignments are saved.

To manage user access to applications from the application level, see Manage user assignment.

Delete a user account

To delete a user account:

1. Select the **Administration** view.
   The Users tab of the User Management page appears.
2. Click **Delete** in the row of the user you want to delete.
   A confirmation message appears.
3. Click **Yes**.
   The user is deleted.

   > **Note**
   > When you delete a user, the user's name, full name, email address, and phone number are removed except where needed for referential integrity. Those values are replaced with a unique user ID.

7.2.3. Manage groups

Groups organize users and make it easier to assign applications. You can create groups based on business units, regions, or other organizational structures. Users with the **Manage Users** permission can manage groups.

View groups

To view groups in your tenant:

1. Select the **Administration** view.
   The User Management page appears.
2. Select the **Groups** tab.
   The Groups tab appears.

The following table describes the actions available on the **Groups** tab.

Task	Action
Search the group list	Enter a keyword or phrase in the search field and press **Enter**. To clear the search results, remove the text and press **Enter**.
Export the group list	Click **Export**. A CSV file containing group details is saved to the folder specified in your browser settings.
Add a group	Click **+ Add Group**. See Create a group .
Edit a group	Click **Edit** in the action column. See Edit a group.
Assign or unassign applications	Click **Assign Applications** in the action column. See Manage application assignment for a group.
Delete a group	Click **Delete** in the action column. See Delete a group.

Create a group

To create a group:

1. Select the **Administration** view.
   The User Management page appears.
2. Select the **Groups** tab.
   The Groups tab appears.
3. Click **+ Add Group**.
   The Add/Edit Group window appears.
4. Enter a name in **Group Name**. Optionally, enter a description in **Group Description**.
5. Select users to assign to the group. You can select individual users, select the **ASSIGN** check box to select the displayed users, or select **Assign All Tenant Users** to select all users.
6. Click **Save**.
   The new group appears in the group list.

Edit a group

To edit a group name or manage its assigned users:

1. Select the **Administration** view, and then select the **Groups** tab.
   The Groups tab appears.
2. Click **Edit** in the row of the group that you want to edit.
   The Add/Edit Group window appears.
3. To edit the group name, enter the new name in **Group Name**.
4. To assign users, select the **Available** tab. Select individual users, select **ASSIGN** to select displayed users, or select **Assign All Tenant Users** to select all users. Use the search field to filter the user list.
5. To remove users, select the **Selected** tab. Clear individual users, clear **ASSIGN** to remove displayed users, or select **Unassign All Tenant Users** to remove all users. Use the search field to filter the user list.
6. Click **Save**.
   Your group changes are saved.

Manage 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, and then select the **Groups** tab.
   The Groups tab appears.
2. Click **Assign Applications** in the row of the group.
   The Assign Applications window appears.

   > **Note**
   > This action is unavailable if the user is assigned to a role with the **All Application Access** permission.

3. To assign applications, select the **Available** tab. Select individual applications, select **ASSIGN** to select displayed applications, or select **Assign All Tenant Applications** to select all applications. Use the search field to filter the application list.
4. To remove applications, select the **Selected** tab. Clear individual applications, clear **ASSIGN** to remove displayed applications, or select **Unassign All Tenant Applications** to remove all applications. Use the search field to filter the application list.
5. Click **Save**.
   The changes to the group's assigned applications are saved.

For information about assigning multiple groups simultaneously, see **Multi-Editing Groups from the Applications Page**.

Delete 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.

7.2.4. Configure System for Cross-domain Identity Management (SCIM)

Configuring System for Cross-domain Identity Management (SCIM) enables automated user provisioning from your identity provider, in accordance with the SCIM 2.0 standard.

To configure SCIM:

1. Select the **Administration** view.
   The User Management page appears.
2. Select the **SCIM Integration** tab.

Specify values for the fields. All fields are mandatory unless otherwise noted.

Task	Action
Enable SCIM Integration	Select the check-box to generate a token for the first time.
SCIM endpoint URL	The endpoint URL for your identity provider's SCIM configuration. It is automatically generated and cannot be edited. To copy the URL, click the copy icon.
Generate a new token	Click **Generate new token** to generate the token.
Bearer Token	The generated bearer token, which is in encrypted format. To copy this token, click the copy icon.
Save	Click **Save** to save the settings.

7.3. Policy management

Security leads can configure how security policies apply to tenant applications and create, edit, and delete custom security policies.

Create a security policy

To create a custom security policy:

1. Select the **Administration** view, click **Policy Management**, and then select the **Policies** tab.
   The Policies tab appears.
2. Click **+ Add Policy**.
   The Add/Edit Policy wizard appears.
3. On the **Policy Details** page, complete the fields and click **Next**.

Field	Description
Policy Name	Enter a name for the policy.
Star Rating	Select the minimum star rating an application must receive to pass. For details, see Five-star assessment rating.
Compliance Requirement	Choose which vulnerabilities determine pass/fail status. Include all vulnerabilities or only issues tagged with a selected compliance requirement, such as OWASP 2021, OWASP 2025, or PCI 3.2. **Note** The pass/fail status includes open source issues.

4. On the **Assessment Types** page, choose which assessment types are available to applications with this policy. **Allow All Assessment Types** is selected by default and includes assessment types added later. To restrict the available types, clear this check box and select the allowed types. Click **Next**.

> **Note**
> If an application has an active subscription or available remediation for an assessment type that the updated policy does not allow, it remains available until it expires or is used.

5. On the **Add-On Services** page, select the add-on services available to applications with this policy. Restrictions do not affect applications that had add-on services enabled before the policy was applied.

Option	Description
Allow SAST Aviator	Allow SAST Aviator in scan settings. This option is selected by default when SAST Aviator is enabled for the tenant. If it ran before a policy restriction was applied, it remains available in the application's scan settings.
Allow DAST Automated add-ons	Allow DAST Automated add-ons in scan settings. This option is selected by default when DAST Automated assessments are enabled for the tenant.

   On the **Development Releases**, **QA/Test Releases**, and **Production Releases** pages, configure the settings for each release status and click **Next** after each page.
   - **Remediation Grace Period** (0–365 days): Set a grace period by issue severity. Issues within the grace period do not affect the release's pass/fail status. The selected star rating determines which severity levels appear.
   - **Required Scan Frequency** (0–365 days): Set how often each scan type must complete. A release fails if it has not completed a required scan within the specified period. A value of 0 means no scan is required
6. On the **Summary** page, review the policy settings and click **Save**.
   The new policy appears on the Policies tab.

To manually override a release's Pass/Fail status, see Override the security policy of a release.

Set a 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 appears.
3. Click **Edit**.
   The Edit Assignment Scope window opens.
4. Select a scope. Only one scope can be applied per tenant.
   - **Business Criticality**: Group applications by their assigned criticality. For more information, see Create an application.
   - **Application Type**: Group applications by type, such as Web/Thick-Client or Mobile.
   - **Application Attribute**: Group applications by the values of a selected application attribute. This option is unavailable if the tenant has no application attributes. Only picklist attributes with ten or fewer values are available.
5. Click **Save**.
   You return to the Policy Assignment tab.
6. Select the policy to assign to each value in the selected scope.
7. Click **Save**.
   Your security policy settings are saved.

Delete a security policy

You can delete a custom security policy only when it is not in use. You can edit the default policy, but you cannot delete it.

To delete a custom security policy:

1. Select the **Administration** view and click **Policy Management**.
   The Policy Management page appears.
2. Select the **Policies** tab.
3. Click **Delete** in the row of the policy that you want to delete.
   A confirmation message appears.
4. Click **Yes**.
   The policy is deleted.

7.4. Single sign-on (SSO)

Single sign-on (SSO) eliminates the need to maintain separate credentials for OpenText Fortify on Demand and helps administrators seamlessly manage user access and provisioning. OpenText Fortify on Demand supports SSO integration with existing identity providers through the SAML 2.0 standard for federated identity.

OpenText Fortify on Demand supports the following SAML 2.0 bindings:

- POST and Redirect bindings for SAML authentication requests from OpenText Fortify on Demand to the identity provider.
- POST binding for SAML assertion responses from the identity provider to OpenText Fortify on Demand.

> **Important**
>
> The system sends an automatic email notification to the security leads whenever tenant SSO settings are modified.

Security leads can configure SSO for the tenant. SSO configuration consists of the following tasks:

- Configure SSO
- Configure encryption
- Configure identity provider metadata
- Download the metadata
- Troubleshoot failed logins

7.4.1. Configure SSO

Configure the OpenText Fortify on Demand SSO settings and map the OpenText Fortify on Demand attribute names to the identity provider attribute names.

To configure the OpenText 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)	Enables single sign-on (SSO).
Enable SCIM Provisioning	Enables user and group provisioning through SCIM. You cannot save the SSO configuration if this option is selected and SCIM is not configured. **Note** **Enable SCIM Provisioning** and **Enable Just-in-Time Provisioning** are optional but mutually exclusive. You can enable only one of these options at a time.
Enable Just-in-Time Provisioning	Automatically creates or updates OpenText Fortify on Demand user accounts for users who authenticate through your identify provider.
Enable Just in Time group assignment	Automatically updates OpenText Fortify on Demand group assignments through your identity provider. **Enable Just-in-Time Provisioning** must be enabled.
Enable Just in Time group creation and provision	**Enable Just-in-Time Provisioning** and **Enable Just in Time group assignment** must be selected. This option allows the automatic creation of OpenText Fortify on Demand user groups through your identity provider.
Send welcome e-mail to new users	Sends a welcome email to users created through the portal. The welcome email contains password setup instructions that do not apply to users authenticated through SSO. If this option is cleared, welcome emails are not sent to any new users.

Require SSO to Authenticate	Requires all users to authenticate using SSO. If this option is cleared, users can sign in using either SSO or their username and password on the standard sign-in page. **Note** This option can affect specialized clients and integrations that rely on the OpenText Fortify on Demand Web API because support for SAML authentication tokens is limited. For example, the iOS client requires non-SSO credentials. In this scenario, OpenText recommends generating a strong random password of at least 32 characters for non-SSO authentication. ○ **Domains or Users to exclude from SSO login**: Available only when **Require SSO to Authenticate** is enabled. Click **Edit** to specify domains or email addresses that are exempt from SSO authentication, and then click **Save**. **Note** This option is disabled when **Require SSO to Authenticate** is not selected.
On session expired, Redirect to Identity Provider Login URL	Redirects users to the identity provider login page when a session expires or when users sign out. This feature requires browser cookies and a login session within the previous 30 days.
Identity Provider Initiated SSO	Supports both service provider-initiated and identity provider-initiated SAML authentication flows. If this option is cleared, users sign in using the SSO Login URL and OpenText Fortify on Demand initiates authentication with the identity provider. If this option is selected, users authenticate directly with the identity provider and are then redirected to OpenText Fortify on Demand.

Enable Enterprise Application setup	Enables authentication through a single identity provider for organizations that use multiple tenants. **Note** If an existing SSO configuration is in place, you must update and reimport the metadata for both OpenText Fortify on Demand and the identity provider. Alternatively, append `?t=sso_login_url_guid` to both the **Identity Provider Name** and the service provider name, where `sso_login_url_guide` is the unique identifier in the SSO Login URL.

4. In the **Attributes** section, map the attribute names expected by OpenText 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 the Identity Provider.
5. Select **Enable Custom Security Lead Mapping** to map a custom value to the Security Lead role in SAML assertion. Type that value in the **Custom Mapping** field.

   Note
   This invalidates the default "Security Lead" value used for the mapping.

6. Click **Save**.
   Your SSO settings are saved. Whenever the tenant SSO settings are modified, the system also sends an automatic email notification to the security leads.

7.4.2. Configure encryption

Configure encryption for OpenText Fortify on Demand SSO.

To configure encryption:

1. Select the **Administration** view.
   The User Management page appears.
2. Click **Single Sign-On**.
   The Single Sign-On page appears.
3. In the **Encryption** section, select the **Enable Encryption** check box to add a new encryption certificate.
4. To add a new certificate, click **Add.** The certificate is created with the following details:
   - Certificate Name
   - Certificate Start Date
   - Certificate End Date

Note

- For first time encryption set up, a default certificate with 1 year is displayed. You can delete that certificate and generate a new one if needed.
- If encryption is enabled and you attempt to save the SAML configuration without having created any certificates, an error message will be displayed.
- When there are multiple tenants within Fortify on Demand that share the same identity provider, each tenant may create different encryption certificates. However, only one of these encryption certificates is uploaded to the identity provider (IDP).
- If encryption is enabled for one tenant, it will also affect all other tenants that share the same Identity Provider (IDP). Therefore, encryption should be enabled for all of those tenants as well. However, you can upload the certificate from any one tenant to the IDP, and decryption will automatically work for all other tenants in Fortify on Demand.

1. You can download a valid certificate as .crt file. To download the certificate, click **Download**. You cannot download the expired certificates or the certificates which are about to expire. In such a scenario, you can also add a new certificate.
2. To delete the certificate, click **Delete.**

5. Click **Save**.
   The encryption details are added to OpenText Fortify on Demand.

Note

After creating a SAML encryption certificate, it becomes part of the SAML metadata. In addition to the signature certificate, you can access the encryption certificate when you download the Core Application Security SAML metadata.

6. From a security perspective, it is recommended that you rotate SAML encryption certificates regularly and create a replacement certificate before the active certificate expires.
   For first-time encryption setup, a default certificate with a one-year validity period is displayed. You can delete that certificate and generate a new one if needed.
   - If encryption is enabled and you attempt to save the SAML configuration without any active certificates, an error message is displayed.
   - When there are multiple tenants within that share the same identity provider, each tenant may create different encryption certificates. However, only one of these encryption certificates is uploaded to the identity provider (IdP).
     If encryption is enabled for one tenant, it also affects all other tenants that share the same identity provider. Therefore, encryption should be enabled for all of those tenants as well. However, you can upload the certificate from any one tenant to the IdP, and decryption will automatically work for all other tenants in Fortify on Demand.

7.4.3. Configure identity provider metadata

Configure the metadata exchange between your identity provider and the application. This metadata enables the application and identity provider to communicate securely and authenticate users through SSO.

Add metadata

Add the identity provider metadata by importing it into OpenText 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**
4. Follow the instructions for the method that you selected.

    > **Note**
    > Once SSO is configured, users needs to use the link in the **SSO Login URL** box to log in to OpenText Fortify on Demand.

    - Import the identity provider metadata:
        1. Click the browse button.
        2. Navigate to and select the .xml file.
        3. Click **Import**.
    - Manually configure the identity provider metadata:
        1. 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**
5. Click **Save**.
   The identity provider metadata is added to OpenText Fortify on Demand.

7.4.3.1. Configure SSO in the identity provider

OpenText 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 OpenText Fortify on Demand.

Most required information about the OpenText 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 OpenText Fortify on Demand.
   The identity provider must accept authentication requests sent from the OpenText Fortify on Demand service provider name. The service provider name is "https://<*tenant_host*>/SAML," where the <*tenant_host*> is your datacenter (for example,"https://ams.fortify.com/SAML"). You can obtain the service provider name from the OpenText Fortify on Demand SAML metadata.
   OpenText Fortify on Demand signs all authentication requests, so you may also choose to validate the signature against the SAML certificate provided in the OpenText Fortify on Demand SAML metadata.

   > **Note**
   > Prior to version 5.2, OpenText 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 OpenText Fortify on Demand must be signed using the identity provider certificate specified in the OpenText Fortify on Demand SSO settings. OpenText Fortify on Demand accepts signatures on either the entire SAML response or just the assertion contained in the response.

> **Note**
> OpenText 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. OpenText Fortify on Demand checks the time period against its system clock when the assertion is received. OpenText 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 OpenText Fortify on Demand SAML metadata.
5. Define the identity claim attributes to include in the SAML assertion. OpenText 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 OpenText Fortify on Demand. The value must be unique across OpenText 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. OpenText 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 OpenText Fortify on Demand user. When updating an existing OpenText 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 OpenText 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 OpenText Fortify on Demand. If a value is not provided, the **Developer** 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 OpenText Fortify on Demand, the user group will be created if the portal SSO option **Enable Just-in-Time group creation and provision** is selected. **Note** 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 OpenText 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 OpenText Fortify on Demand. **Note** 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 OpenText Fortify on 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. If a value is not provided, the value of the provision_user 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.
mtt	No	If the portal SSO option **Enable Enterprise Application setup** is selected, this attribute is required. Unique identifier found in the SSO Login URL, enclosed in quotation marks. For example, given the URL https://ams.fortify.com/SSO/Login/c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc, the identifier is c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc.

Important

You must also configure OpenText Fortify on Demand to recognize the attributes used by the identity provider. See Configuring SSO Settings.

7.4.4. Download the metadata

Download the OpenText Fortify on Demand metadata file to help configure your identity provider to respond to authentication requests from OpenText Fortify on Demand. The metadata file includes the Assertion Consumer Service URLs, the OpenText Fortify on Demand certificate, and the entity ID (also known as the service provider name).

To download the OpenText 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 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 OpenText Fortify on Demand credentials.

7.4.5. Troubleshoot 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.

> **Note**
>
> 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.

7.5. 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 OpenText 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.

You are only sharing your assessment results, your code is not being shared.



Important

Vendors are the tenants from which you can receive reports, and **Customers** are the tenants to which you can send reports.

This section covers the following topics:

- Initiate a relationship
- Accept a relationship
- Publish a report

7.5.1. Initiate a relationship

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.
2. Click **Vendors**.
3. Select the **Customers** tab.



Note

Vendors identifies the tenants that send reports to you, and **Customers** identifies the tenants that receive reports from you.

4. Click **Request to be a Vendor**.
   Use the optional **Notes** box to add information about the vendor-customer relationship.
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**.

7.5.2. Accept a relationship

Accepting a relationship initiated by another tenant is a two-step process.

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.
2. Click **Vendors**.

The Vendor Management page opens, displaying the My Vendors and Customers tabs.



Note

Vendors are the tenants from which you can receive reports, and **Customers** are the tenants to which you can send reports.

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**.

7.5.3. Publish a report

Once you have established a relationship with another tenant in OpenText Fortify on Demand, you can publish your reports for the tenant to review.

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.
3. 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.

View 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.
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.
Verify that both tenants have completed the required sharing configuration and that the report has been published to your tenant.

8. API

OpenText 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 and API root URL

Data center	API root URL
AMS	https://api.ams.fortify.com
EMEA	https://api.emea.fortify.com
APAC	https://api.apac.fortify.com
SGP	https://api.sgp.fortify.com
FedRAMP	https://api.fed.fortifygov.com
Trial	https://api.trial.fortify.com

Note

The OpenText Fortify on Demand API does not support cross-origin resource sharing (CORS).

View API documentation

OpenText Fortify on Demand API documentation through **API Explorer**. API Explorer is based on the **OpenAPI (Swagger)** framework and is available directly from the portal. API Explorer enables you to:

- View the latest API definitions
- Explore available resources and endpoints
- Test API requests interactively
- Download the API specification in JSON format
- Generate client stubs and SDKs using tools such as Swagger Editor or Swagger Codegen

To view API Explorer:

1. Click your account name on the toolbar.
2. Select **API Explorer**.
   The **API Explorer** page opens in a new window and displays the available API resources.
3. 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":[],"produces":
["application/json","text/json","application/xml","text/xml"],"parameters":[{"name":"applicationId","in":"path","description":"The application
id","required":true,"type":"integer","format":"int32"}],"responses":{"200":{"description":"Ok","schema":{"$ref":"#/definitions/Application"}},"401":
{"description":"Unauthorized"},"404":{"description":"NotFound"},"500":{"description":"InternalServerError"}},"deprecated":false},"put":{"tags":["Applications"],"summary":"Update an
application","operationId":"ApplicationsV3_PutApplication","consumes":["application/json","text/json","application/xml","text/xml","application/x-www-form-
urlencoded","multipart/form-data"],"produces":["application/json","text/json","application/xml","text/xml"],"parameters":[{"name":"applicationId","in":"path","description":"The
application id","required":true,"type":"integer","format":"int32"},{"name":"requestModel","in":"body","description":"The application data","required":true,"schema":
{"$ref":"#/definitions/PutApplicationRequest"}}],"responses":{"200":{"description":"Ok","schema":{"$ref":"#/definitions/PutApplicationResponse"}},"400":
{"description":"BadRequest","schema":{"$ref":"#/definitions/PutApplicationResponse"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":
{"description":"NotFound"},"422":{"description":"UnprocessableEntity","schema":{"$ref":"#/definitions/PutApplicationResponse"}},"500":
{"description":"InternalServerError"}},"deprecated":false},"delete":{"tags":["Applications"],"summary":"Deletes an application","operationId":"ApplicationsV3_Delete","consumes":
[],"produces":["application/json","text/json","application/xml","text/xml"],"parameters":[{"name":"applicationId","in":"path","description":"The application
id","required":true,"type":"integer","format":"int32"}],"responses":{"200":{"description":"Ok","schema":{"$ref":"#/definitions/DeleteApplicationResponse"}},"400":
{"description":"BadRequest","schema":{"$ref":"#/definitions/DeleteApplicationResponse"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":
{"description":"NotFound"},"500":{"description":"InternalServerError"}},"deprecated":false}},"/api/v3/applications":{"get":{"tags":["Applications"],"summary":"Retrieve a collection
of applications","operationId":"ApplicationsV3_GetApplications","consumes":[],"produces":["application/json","text/json","application/xml","text/xml"],"parameters":
[{"name":"filters","in":"query","description":"<p>A delimited list of field filters.</p>\r\n<p>Field name and value should be separated by a colon (:).</p>\r\n<p>Multiple fields
should be separated by a plus (+). Example, fieldname1:value+fieldname2:value</p>","required":false,"type":"string"},{"name":"orderBy","in":"query","description":"The field name to
order the results by.","required":false,"type":"string"},{"name":"fields","in":"query","description":"Comma separated list of fields to return.","required":false,"type":"string"},
{"name":"offset","in":"query","description":"Offset of the starting record. 0 indicates the first record.","required":false,"type":"integer","format":"int32"},
{"name":"limit","in":"query","description":"Maximum records to return. The maximum value allowed is 50.","required":false,"type":"integer","format":"int32"}],"responses":{"200":
{"description":"Ok","schema":{"$ref":"#/definitions/ApplicationListResponse"}},"400":{"description":"BadRequest","schema":{"$ref":"#/definitions/ErrorResponse"}},"401":
{"description":"Unauthorized"},"500":{"description":"InternalServerError"}},"deprecated":false},"post":{"tags":["Applications"],"summary":"Create a new application and
release","operationId":"ApplicationsV3_PostApplication","consumes":["application/json","text/json","application/xml","text/xml","application/x-www-form-urlencoded","multipart/form-
data"],"produces":[],"parameters":[{"name":"requestModel","in":"body","description":"The application data","required":true,"schema":
{"$ref":"#/definitions/PostApplicationRequest"}}],"responses":{"204":{"description":"No Content"},"201":{"description":"Created","schema":
{"$ref":"#/definitions/PostApplicationResponse"}},"400":{"description":"BadRequest","schema":{"$ref":"#/definitions/ErrorResponse"}},"401":{"description":"Unauthorized"},"422":
{"description":"UnprocessableEntity","schema":{"$ref":"#/definitions/ErrorResponse"}},"500":
```


   - 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** or **Hide** to show or hide resource endpoints.
- Click **List Operations** to view the endpoints for a resource.
- Click **Expand Operations** to view endpoint descriptions for a resource.
- Click an endpoint to view detailed information about the operation.

Test API endpoints in 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.

To run a test request:

1. Click **Authenticate** at the top of the API Explorer page.
2. From the **Grant Type** list, select an authentication method:

- **password**: Authenticates using your portal user account credentials.
- **client_credentials**: Authenticates using an API key and secret.

3. In the **Scope** field, enter the scopes to grant to the access token.
   Separate multiple scopes with a space. For a list of available scopes, see **API scopes**.
4. Provide the required authentication information for the selected grant type.
5. Authenticate using the following:
    1. Client credentials:
        1. In the **Client ID** field, enter the API key.
           For information about creating an API key, see **Create an API key**.
        2. In the **Client Secret** field, enter the API secret.
    2. User account:
        1. In the **Username** field, enter your user name.
        2. In the **Password** field, enter your password or personal access token.
           If you use a personal access token, the requested scopes must be a subset of the token's permitted scopes. Otherwise, authentication fails.
        3. In the **Tenant** field, enter your tenant code.
           You can find your tenant code and user name in your account settings.
        4. If two-factor authentication is enabled, enter the verification code in the **Security Code** field.
        5. If the verification code was generated by a Time-Based One-Time Password (TOTP) authenticator application, select **Use TOTP**.

1. Click **Submit**.
   An access token is generated for the current session.
2. Expand an endpoint and complete the parameters in the fields provided.
3. Click **Try it out!**.
   The response is displayed below.

8.1. API authentication

Authentication of OpenText Fortify on Demand API requests is through a bearer token. Obtain a bearer token by sending a request to the token endpoint.

To authenticate OpenText 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 Application Programming Interface (API).

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 API Scopes.
`grant_type`	Grant type (in lower case): ○ `password` : user credentials (Resource Owner Password Credentials) ○ `client_credentials` : API key and secret
`username`	Account username as `<tenant_code>\<username>` . 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. **Note** SSO users are restricted to using personal access tokens. **Note** 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 fails. For more information on personal access tokens, see Creating a Personal Access Token.
`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'
```

8.2. 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

8.3. API rate limits

OpenText 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	Maximum requests	Seconds
POST /api/v3/applications	6	30
PUT /api/v3/applications/{applicationId:int}	1	30
GET /api/v3/eventlogs/download	1	300
POST /api/v3/releases	6	30
PUT /api/v3/releases/{releaseId:int}	1	30
POST /api/v3/releases/{releaseId:int}/dynamic-scans/start-scan	1	30
GET /api/v3/releases/{releaseId:int}/fpr **Note** The rate limit is per scan type.	1	30
GET /api/v3/releases/{releaseId:int}/vulnerabilities/{vulnId}/all-data	1	1
POST /api/v3/releases/{releaseId:int}/vulnerabilities/bug-link	1	5
POST /api/v3/releases/{releaseId:int}/vulnerabilities/bulk-edit	1	5
Other endpoints	10	1

Track 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 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 OpenText 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.

8.4. Personal access tokens

Personal access tokens provide an alternative method for authenticating to the API. Each token is unique to the user who creates it and inherits that user's permissions. You can further restrict a token by assigning specific scopes.

Personal access tokens bypass two-factor authentication (2FA) and single sign-on (SSO) requirements configured in the portal.

> **Note**
> Personal access tokens can be used only for API authentication. You cannot use them to sign in to the portal.

Personal access tokens provide a flexible and secure method of authentication for integrations with OpenText Fortify on Demand. Users can have multiple tokens with different scopes for specific needs, specify token expiration dates, and disable tokens at any time.

OpenText Fortify on Demand sends email and portal notifications 14 days before a personal access token expires.

> **Note**
> After a token expires, you cannot use it for authentication. To continue using the token, generate a new secret.

Create 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.
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
Name	Type a name for the token.
Authorize to use API	The token is enabled by default. Disable the token.
Secret Expiration Date, **Secret Expiration Days**	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. **Note** The expiration date cannot exceed the maximum lifetime as set by the portal.
Allowed Scopes	Select the allowed scopes for the token. For more information on scopes, see API Scopes.

- Click **Save**.
  The Secret Key window opens.
- Copy your Base64 encoded secret.

  Note
  The secret is only shown once.

- Click **Close**.
  The new token appears in the personal access token list.

Edit or delete 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.

2. You can perform the following tasks:

Task	Procedure
Generate a new secret	• Click **New Secret**. The New Secret window opens. • 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. • Click **Create**. This will void the current secret.
Edit the token	• Click **Edit**. The Add/Edit Personal Access Token window opens. • Edit the fields as needed. You cannot edit the current secret's expiration date.
Delete the token	• Click **Delete**. A confirmation message appears. • Click **Yes**.

9. Tools

OpenText Fortify on Demand offers a variety of tools to help your organization integrate application security testing into your DevOps processes.

- CICD tools
- IDE tools
- Scan preparation and tracking tools
- View and download tools

9.1. CICD tools

The following Continuous Integration and Continuous Delivery (CICD) integration tools enable static and dynamic testing to be integrated into existing build automation:

CICD tools

CICD tool	Tools description	More information
OpenText Fortify on Demand Uploader	Stand-alone utility for uploading code from a build server to OpenText Fortify on Demand for static scanning	• GitHub
Fortify Azure DevOps Extension	Azure DevOps extension for: • Uploading code to OpenText Fortify on Demand and submitting static scans as build and release tasks • Submitting dynamic scans as build and release tasks	• Visual Studio Marketplace • Documentation
Fortify on Demand Jenkins Plugin	Jenkins plugin for uploading code to OpenText Fortify on Demand and submitting static scans as build tasks	• Jenkins • Documentation
Fortify CLI	Command-line utility for interacting with various Fortify products	• GitHub repository
Fortify Bitbucket Pipelines	Collection of Bitbucket pipelines for: • Uploading code to OpenText Fortify on Demand and submitting static scans	• Bitbucket • Documentation
Fortify GitHub Actions	Collection of GitHub actions for: • Uploading code to OpenText Fortify on Demand and submitting static scans	• GitHub Marketplace • Documentation
Fortify GitLab CI Templates	Collection of GitLab templates for: • Uploading code to OpenText Fortify on Demand and submitting static scans	• GitLab
Fortify CI Tools	Docker container for simplifying integration of Fortify static application security testing for DevSecOps pipelines that use configurable runners to run CICD workflows	• Docker Hu

9.2. IDE tools

The following Integrated Development Environment (IDE) tools enable developers to upload code from IDEs to OpenText Fortify on Demand for static testing:



Note

Documentation for each IDE tool is now available as a stand-alone guide.

IDE tools

IDE tool	Tools description	More information
Fortify on Demand Plugin for Eclipse	Eclipse plugin for uploading code to OpenText Fortify on Demand for static scanning and opening scan results for remediation	Fortify on Demand Plugin for Eclipse
Core Application Security Plugin for IntelliJ IDEA	IntelliJ IDEA plugin for uploading code to OpenText Fortify on Demand for static scanning and opening scan results for remediation	Core Application Security Plugin for IntelliJ IDEA
Fortify on Demand Extension for Visual Studio	Visual Studio extension for uploading code to OpenText Fortify on Demand for static scanning and opening scan results for remediation	Fortify on Demand Extension for Visual Studio
Core Application Security Remediation Extension for Visual Studio Code	Visual Studio Code extension to view and audit issues directly from an application release in OpenText Fortify on Demand	Core Application Security Remediation Extension for Visual Studio Code
Fortify Extensions for Visual Studio Code Analysis	Visual Studio Code extension for uploading code for static scanning	Fortify Visual Studio Code Extension Documentation
Fortify Security Assistant Plugin for Eclipse Documentation	Eclipse plugin that provides alerts to potential security issues in Java files as you write code.* It includes semantic and intra-class dataflow analyzers to detect: • Potentially dangerous uses of functions and APIs • Issues caused by tainted data reaching vulnerable functions and APIs at the intra-class level	Fortify Security Assistant Plugin for Eclipse Documentation
Fortify Security Assistant Plugin for IntelliJ Documentation	IntelliJ IDEA plugin that provides alerts to potential security issues in Java files as you write code.* It includes structural and configuration analyzers to detect: • Potentially dangerous uses of functions and APIs • Insecure application configurations in property and XML files	Fortify Security Assistant Plugin for IntelliJ Documentation

Fortify Security Assistant Extension for Visual Studio Documentation	Visual Studio extension that provides alerts to potential security issues in C# (.cs) , Razor (.cshtml), WebForms (.aspx), .config, .xml, and .ini files as you write code.* It includes structural and configuration analyzers to detect: • Potentially dangerous uses of functions and APIs • Insecure application configuration	Fortify Security Assistant Extension for Visual Studio Documentation

*Fortify Security Assistant requires a valid license file to scan for issues and to install or update Fortify security content. The license is valid for all Fortify Security Assistant versions.

9.3. Scan preparation and tracking tools

The following tools are used to prepare application source code for static scanning.

Static scanning tool

Static scanning tool	Tools description	More information
OpenText SAST	Translate-only version of Fortify SAST for translating C/C++ and Scala code and packaging it for scanning **Note** Fortify SAST requires a valid license file to translate source code	OpenText Static Application Security Testing and Tools Documentation
Fortify ABAP Extractor	SAP transport request for downloading source code files to the presentation server	Preparing ABAP (SAP) Application Files
Fortify ScanCentral SAST client	Stand-alone Fortify ScanCentral SAST client for packaging source code	Fortify ScanCentral SAST
Fortify Audit Workbench	Tool for viewing and auditing FPR files	OpenText Static Application Security Testing and Tools Documentation

The following tools are used to prepare web applications for dynamic scanning.

Dynamic scanning tool

Dynamic scanning tool	Tools description	More information
Workflow macro recorder	Stand-alone utility for creating workflow macros	OpenText Dynamic Application Security Testing Documentation
Login macro recorder	Stand-alone utility for creating login macros	OpenText Dynamic Application Security Testing Documentation

Tracking tools include.

Tracking tool

Tracking tool	Tools description	More information
Software security sync utility	Stand-alone utility for automated, scheduled synchronization of OpenText Fortify on Demand applications, releases, and scans with Fortify Software Security Center (SSC)	GitHub
OpenText Fortify on Demand Bug Tracker	Stand-alone utility for submitting OpenText Fortify on Demand issues to bug trackers	GitHub

9.4. View and download tools

You can view and download the tools available for use with OpenText 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 most tools does not require a license. Contact support to request a license if you meet the following conditions:

- Fortify SAST: when you want to scan C, C++, and Scala code
- Fortify Audit Workbench: when you want to view FPR files
- Fortify Security Assistant: when you have an active static subscription

10. Integrations

OpenText Fortify on Demand offers a variety of integrations that are managed through the portal.

This section contains the following topics:

- Bug tracker integration
- External scan integration
- Secure Code Warrior integration
- Slack integration for notifications

- Source control integration
- Track configured integrations
- Webhooks

10.1. Bug tracker integration

Bug tracker integration lets you link vulnerabilities to supported bug tracking systems and manage bug lifecycles directly from the portal. You can submit issues as bugs, track their status, and synchronize issue updates with the following supported bug trackers:

- Application Quality Management (formerly ALM)
- Software Delivery Management Octane (formerly ALM Octane)
- Jira
- Bugzilla
- Azure DevOps and Azure DevOps Server

If you use an unsupported bug tracker, you can manually link external bugs to issues in the portal.

Configure bug tracker integration

Bug tracker integration is configured at the application level. You must establish a connection between OpenText Fortify on Demand and your bug tracker server. The server needs a dedicated user account for adding and closing bugs.

> **Note**
> VPN is not an option for establishing the connection.

To configure bug tracker integration for an application:

1. Go to **Applications**.
2. Select the application that you want to configure.
3. Click **Settings**.
4. Select the **Bug Tracker** tab.
5. Turn on **Enable Bug Tracker Integration**.
6. Select a bug tracker from the **Bug Tracker** list.
7. Enter the required connection details:
    - Bug tracker URL
    - Username
    - Password"

    > **Important**
    > Atlassian ended support for basic authentication with password and cookie-based authentication for REST APIs.
    > Microsoft ended support for basic authentication with password for REST APIs.

    > **Note**
    > If you use a cloud Jira instance that requires a Reporter field, enter the **Requester Account ID** associated with the specified username.

8. 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 OpenText 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.

8. Select the default category to which application's issues are submitted. Fields are specific to the selected bug tracker.
   ValueEdge/ALM Octane: **Project** and **Workspace**
   ALM.Net: **Domain** and **Project**
   Jira: **Project** and **Component**
   Bugzilla: **Product** and **Component**
   Azure DevOps/Azure DevOps Server: **Project**
9. Turn on **Enable Bug State Management** to automatically update bug statuses in your bug tracker when linked issues are marked as **Fix Validated** or **Suppressed**. OpenText Fortify on Demand updates bugs to the corresponding status shown in the following table. If a bug is linked to multiple issues, the bug remains open until all linked issues are marked as **Fix Validated** or **Suppressed**.

Note

OpenText Fortify on Demand does not automatically reopen bugs when linked issues are reopened.

Bug tracker and closed status

Bug tracker	Closed status
ALM Octane	Fixed (phase.defect.fixed)
ALM	Fixed
Jira	Done
Azure DevOps/Azure DevOps Server	Resolved
ALM.Net	Fixed (phase.defect.fixed)
Bugzilla	Status: Resolved Resolution: Fixed

1. **(Optional) For Azure DevOps and Jira:** Turn on **Sync Developer Status with Bug Tracker Status**.
   Map bug tracker status values to the corresponding **Developer Status** values. When synchronization is enabled, OpenText Fortify on Demand automatically updates the **Developer Status** field and synchronizes new bug tracker comments.

Note

You can no longer edit the Developer Status field manually.

2. **(Optional) For Azure DevOps:** Configure default values for custom fields used when submitting bugs.

Required custom fields are highlighted. Azure DevOps default values are populated when available. To restore the default values, clear the configured values.

3. Click **Save**.
   Your bug tracker settings are saved.

Submit issues to a bug tracker

After you configure bug tracker integration, users with **Application Access** and **Edit Issues** permissions can submit issues as bugs. The portal prevents duplicate submissions.

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
4. Go to **Applications**.
5. Select an application.
6. Open one of the following pages:
   - **Application Issues**
   - **Release Issues**
7. 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.

1. 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.

9. OpenText Fortify on Demand supports custom fields in ALM, Jira, and Azure DevOps. If the bug tracker contains custom fields, those fields appear in the **Custom Values (Required)** section. Complete the fields.
10. 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.

Link an issue to an unsupported bug tracker

If your bug tracker is not supported, you can manually associate a bug URL with an issue.

To link a OpenText Fortify on Demand issue with an unsupported bug tracker:

1. Go to **Applications**.
2. Select an application.
3. Open the **Application Issues** or **Release Issues** page.
4. Select one or more issues.
5. Click **Submit Bug**.
6. Enter the bug URL in the **Bug URL** field.

7. Click **Save**.

After the link is added, the portal displays a **View Bug** link that opens the associated bug record.

10.2. External scan integration

You can import scan results from external sources into OpenText Fortify on Demand to manage scan results from multiple sources in a single view. OpenText Fortify on Demand supports import of the following scan types:

- On-premises Fortify SAST and Fortify DAST scan results
- Open source scan results that conform to the CycloneDX 1.4, 1.5, 1.6 and 1.7 standard

Import an on-premises scan

You can import on-premises Fortify SAST and Fortify DAST scan results into OpenText Fortify on Demand. Upon importing an FPR or SARIF:

- The scan start and complete times use the scan date in the FPR or SARIF.
- Global and Application Audit Templates are applied.
- The instance ID is used to track issues across imports.
  For example, if you import an FPR or SARIF into an empty release, all imported issues have **New** status. If you import the same FPR or SARIF again, all issues changes from **New** to **Existing**. If you then import a different FPR or SARIF, the issue statuses change as follows:
  - Issues that exist in both the release and the latest FPR or SARIF have the **Existing** status.
  - Issues that only exist in the latest FPR or SARIF have the **New** status.
  - Issues that exist in the release but do not exist in the latest FPR or SARIF have the **Fixed** status.
- Suppressed issues in the FPR or SARIF that are not present in the release are imported and suppressed. Suppression status is ignored for issues in the FPR or SARIF that are present in the release.

> **Note**
> FPRs or SARIFs with a scan date older than the most recently completed scan of the same type are not accepted.

To import a static FPR, dynamic FPR or a static SARIF:

1. Go to **Applications**.
2. Click **Your Releases**.
3. Select the release.
4. Click **Scans**.
5. Select **Import Scan Dynamic** or **Import Scan Static**.
6. Select the file format:
   - **FPR**
   - **SARIF**

   > **Note**
   > SARIF file support is available only for static scan types.
7. Browse to and select the FPR or SARIF file.
8. 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 "WebInspect (Imported)" assessment type for Fortify SAST or "SCA (Imported)" assessment type for Fortify SAST.

Import a Software Bill of Materials

Users with the **Manage Applications** permission can import software bill of materials (SBOM) files generated by third-party tools.
An SBOM must meet the following requirements to be imported:

- The SBOM is a JSON file that conforms to the CycloneDX 1.4, 1.5, 1.6 and 1.7 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 a software bill of materials:

1. Go to **Applications**.
2. Click **Your Releases**.
3. Select the release.
4. Click **Scans**.
5. Select **Import Scan Open Source**.
   The **Import Open Source Scan** window opens.
6. Select the SBOM file.
7. (Optional) Select **Run a Debricked scan to add vulnerability and license information**.
   When the import completes:
   - One Fortify Core SCA entitlement is redeemed.
   - A Fortify Core SCA subscription is created for the application.

   You can also submit the SBOM for scanning later by selecting **Send to Debricked** on the **Scans** page.
8. Click **Next**. Results appear on the **Issues** page.

Delete an imported scan

Users with the **Manage Applications** permission can delete imported scan result files.

> **Note**
> You cannot delete an imported scan if a newer imported scan of the same type exists.

To delete an imported scan:

1. Go to **Applications**.
2. Select the application.
3. Click **Scans**.
   The page displays all scans associated with the application.

   > **Note**
   > You can filter the scan list to view only scans run against a release by clicking the release name on the Application Releases page.

4. Locate the imported scan and click **Cancel Imported Scan**.
5. Click **Yes** to confirm.
   The imported scan and all associated issues are deleted.

10.3. Secure Code Warrior integration

OpenText Fortify on Demand has partnered with Secure Code Warrior to provide free interactive training for supported vulnerability categories to OpenText 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.

OpenText 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 Secure Code Warrior.

Launch 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.
7. In the **Interactive Training** section, you can perform the following tasks:
   - To start a training module, click **Launch Training**.
   - To watch a video about the issue category, click **Watch Video**.
   - To learn more about the issue category, click the links for external educational resources.

> **Note**
> If the issue does not belong to a supported vulnerability category, you are redirected to the Secure Code Warrior home page.

10.4. Slack integration for notifications

OpenText 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.

Configure Slack integration

You can configure Slack integration by configuring one or more webhooks for the tenant. Before you begin, make sure that you have permission to manage apps and integrations in the Slack workspace.

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. If prompted, sign in to the Slack workspace that you want to connect.
5. Select the workspace from the workspace list.
6. Select the channel or direct message destination for notifications.
7. Click **Authorize** to authorize OpenText Fortify on Demand to access your Slack account.

A "Slack Integration Successful" message appears. You can now enable posting notiifcations to the channel. For more information on enabling posting notifications to Slack, see Create an individual subscription and Create a global subscription.

Delete Slack integration

You can remove a Slack integration from either Slack or OpenText Fortify on Demand.

Workspace owners and users with permission to manage apps can remove authorizations or remove the OpenText Fortify on Demand from the Slack workspace. Removing authorizations causes Slack notifications to fail.

To remove Slack authorizations:

1. Go to **AdministrationIntegrations**.
2. Expand the **Slack** section.
3. Select the authorization link for the integration.
4. In Slack, remove specific authorizations or remove the application from the workspace.

To delete an integration from OpenText Fortify on Demand:

1. Select the **Administration** view.
   The **User Management** page appears.
2. Click **Integrations**.
   The **Integrations** page appears.
3. Expand the **Slack** section.
4. Delete the integration from the corresponding row.

10.5. Source control integration



Important

Source control integration through the portal is a legacy integration. This feature is planned to be **deprecated**. Existing users should migrate source control integrations to pipelines on the applicable version control platforms at the earliest convenience. Fortify offers pipeline templates for various version control platforms, including Bitbucket, GitHub, and GitLab. For more information, see CICD Tools.

OpenText Fortify on Demand supports source control integration with GitHub and Bitbucket. After you configure the integration for an application, the platform can retrieve source code from repositories for static assessments, and you can select a repository branch or release when starting a static assessment.

The following languages are supported: Java, JavaScript, .NET, PHP, and Python. The requirements for preparing your code for upload to OpenText Fortify on Demand remain the same as described in Preparing Static Assessment Files. For .NET and Java, you should pre-compile your files and upload them to a release to ensure acceptance of the payload.

Configure source control integration with GitHub

The GitHub integration uses the OpenText Fortify on Demand GitHub marketplace application, which is unique to each data center.



Note

GitHub Enterprise is not supported.

To configure source control integration with GitHub:

- Go to **Applications**.
- Select the application that you want to configure.
- Click **Settings**.
- Select the **Source Control** tab.
- From **Source Code Management Platform**, select **GitHub**.
- Click **Authenticate**.
- Authorize OpenText Fortify on Demand to access your GitHub account.
- From **Organization**, select the organization that owns the repository.
- From **Repository**, select the repository that you want to link to the application.
- Click **Save**.

Configure 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. Go to **Applications**.
2. Select the application that you want to configure.
3. Click **Settings**.
4. Select the **Source Control** tab.
5. From **Source Code Management Platform**, select **Bitbucket**.
6. In **Client Key** and **Client Secret**, enter the OAuth consumer key and secret from Bitbucket.
7. Configure the OAuth consumer in Bitbucket:

- Select **This is a private consumer**.
- Set the callback URL to:

  ```
  https://<fod_domain>/Redirect/OAuth/
  ```

- Use the appropriate domain:
  - US: `ams.fortify.com`
  - EMEA: `emea.fortify.com`
  - APAC: `apac.fortify.com`
  - FedRAMP: `fed.fortifygov.com`
- Grant read permissions for:
  - Account
  - Workspace membership
  - Projects
  - Repositories

    For more information on adding an OAuth consumer in Bitbucket, see the Integrate another application through OAuth section of the Bitbucket documentation.

1. Click **Authenticate**.
2. Authorize the OpenText Fortify on Demand application to access your account.
3. From **Team**, select the team that owns the repository.
4. From **Repository**, select the repository that you want to link to the application.
5. Click **Save**.

10.6. Track configured integrations

Security Leads can view integrations configured by users across applications in OpenText Fortify on Demand. Supported integration types include:

- Bug tracker
- Source control
- 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.

4. Perform one of the following actions:
    - For **Slack** integrations, remove specific authorizations or delete webhooks. For more information, see Delete Slack integration.
    - For **Bug Tracker** integrations, select an application link to open the application's bug tracker settings. For more information, see Configure Bug Tracker integration.
    - For **Source Control** integrations, select an application link to open the application's source control settings. For more information, see Source Control integration

10.7. Webhooks

Webhooks enable OpenText Fortify on Demand to send notifications to an external web server when scan events occur. Users with the **Configure Webhooks** permission can create webhooks that trigger for specific scan events, including:

- Scan started
- Scan paused
- Scan resumed
- Scan canceled
- Scan completed

When a subscribed event occurs, OpenText Fortify on Demand sends an HTTP POST request containing event data to the configured webhook URL. Webhooks can be used as an alternative to polling in CI/CD pipelines that incorporate scanning.

Configure a Webhook

Users with the **Configure Webhooks** permission can configure webhooks for the tenant. You must assign a webhook to at least one release.

To configure a webhook:

1. Select the **Administration** view.
2. Click **Webhooks**.
3. Click **Add Webhooks**.
4. Complete the fields as needed. Fields are required, unless otherwise noted.

Field	Description
Payload URL	URL that receives webhook POST requests. For example, `https://7e9ea9dc.ngrok.io/payload`.
Description	Optional description for the webhook.
Secret	Optional secret used to validate webhook requests. OpenText Fortify on Demand uses the HMAC-SHA256 algorithm to generate a signature that is included in the `X-FOD-Signature` request header. **Tip** 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`.
Monitor all application releases	○ Set to **Yes** to monitor all application releases. ○ Set to **No** to monitor individual releases (default). You can specify releases to monitor after the webhook has been configured.
Active	○ Set to **Yes** to enable the delivery of webhook requests (default). ○ Set to **No** to disable the delivery of webhook requests.

5. Select which scan events must 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, clck **Edit** in the row of the webhook.
   The Assign Releases window appears.
9. Select the releases that the webhook will monitor and click **Save**.
   The webhook is now assigned to the selected releases.

View Webhook deliveries

Users with the **Configure Webhooks** permission can view webhook delivery details, including HTTP requests, payloads, and responses.

To view the list of webhook deliveries:

1. Select the **Administration** view.
   The User Management page appears.
2. Click **Webhooks**.
   The Webhooks page appears.
3. Select the **Webhook Deliveries** tab.
   A list of webhook deliveries appear.

   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.

Webhook requests and responses

OpenText 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, OpenText Fortify on Demand verifies 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: 4F837B0AE04303E975BBCF9FFBBC09E00160138357 57BD611C20F7930711980F
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 OpenText 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=CRuQJLoiFx9ay1UV88ufH83vCOjq1PL0JNOwY59v; expires=Fri, 02-Jul-2021 18:08:29 GMT; Max-Age=7200; path=/; httponly
Server = nginx/1.14.2
```

11. Training

OpenText Fortify on Demand partners with **Security Innovation** to provide secure software development training courses.

Review your contract to verify whether training courses are included. To add training courses to your subscription, contact your sales representative.



Note

Enable pop-ups and cookies in your browser to access training courses.

Assign training courses

You can assign available training curricula to yourself. If you have the **Manage Users** permission, you can also assign curricula to all active users in the tenant.

Training courses are organized into curricula and must be assigned at the curriculum level.

To assign a training curriculum:

1. Click the **Training** icon on the portal toolbar.
   The **Training** page opens.
2. Select the **Assignment** tab.
   - If you have the **Manage Users** permission, the page displays all active users and their assigned curricula.
   - Otherwise, only your user account and assigned curricula are displayed.
3. Click **Edit** next to a user.
   The **Course Curriculum** dialog box opens.
4. Select the curricula that you want to assign.
5. Click **Save**.
   The **Assignment** tab displays the updated assignments.

View training courses

You can view and access the courses assigned to you. To view your assigned training courses:

1. Click the **Training** icon on the portal toolbar.
   The **Training** page opens.
2. On the **Courses** tab, review the assigned courses.
   The page displays the following information:
   - Course name
   - Curriculum
   - Module ID
   - Completion status

- Last attempted date
- Passed date
- Course link

3. Choose one of the following actions:
   - **Start Course** to begin a course.
     Starting a course resets the completion status but does not reset the passed date.
   - **Resume Course** to continue a course from your previous session.
   - **Browse Course** to review course content without affecting the completion status or passed date.
4. Click **Yes** when prompted.
   The course opens in a new window.

> **Important**
> Close the course window when finished to ensure that course results are recorded correctly.

View the training report

If you have the **Manage Users** permission, you can monitor training activity and course completion across the tenant.

To generate a training report:

1. Click the **Training** icon on the portal toolbar.
   The **Training** page opens.
2. Select the **Report** tab.
   The report includes the following information:
   - Percentage of assigned courses that have been completed
   - Training progress charts:
     - **Education Status**: Number of courses that are completed, in progress, or not started
     - **Top Courses**: Courses with the highest time spent
     - **Top Users**: Users with the highest training activity
     - **Most Popular**: Most frequently accessed courses
   - **Training Details** grid showing:
     - User
     - Assigned course
     - Course status
     - Last access date
     - Last completion date
3. Click **Export** to download the **Training Details** grid as a CSV file.
   Any applied search filters are included in the exported file.

12. Policies

Review the OpenText Fortify on Demand policies for information about portal administration and maintenance. If you have additional questions, consult the support resources.

Maintenance and updates

OpenText Fortify on Demand provides the following information regarding maintenance schedule and software updates.

Maintenance schedule

To help customers plan for scheduled maintenance, OpenText 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 OpenText Fortify on Demand.

The maintenance window for each data center is set using the following time zones.

The maintenance window for each data center is set using the following time zones:

Data center	Maintenance time zone
AMS	ET (Eastern Time)
EMEA	GMT (Greenwich Mean Time)
APAC	AET (Australian Eastern Time)

For additional details about scheduled maintenance in other environments, contact support.

Software updates

OpenText Fortify on Demand determines whether and when to develop, release, and apply software upgrades to the OpenText 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 OpenText Fortify on Demand anticipates a service interruption due to a software upgrade, OpenText Fortify on Demand may implement a SaaS upgrade at any time without notice to the customer. OpenText Fortify on Demand aims to use the monthly scheduled maintenance window to apply major software updates.

Security content updates to expand and improve OpenText Fortify on Demand's ability to identify vulnerabilities are a key component of the OpenText 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. OpenText 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. OpenText recommends users to stay up-to-date with the latest security intelligence by following the Cybersecurity Blog.

Data retention policy

OpenText Fortify on Demand has implemented the following data retention policy for customers as of the v18.4 release. OpenText encourages customers to review and download any files outside the data retention windows that they wish to retain.

Data retention policy

Product resources	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	Not applicable	3 months
Data exports (global Reports page)	.csv	3 months
Event logs	.csv	13 months
User-generated reports	.pdf, .html	2 years
Fortify scan result files	.fpr	2 years
Software bill of materials (SBOM) files	.json	2 years
Site tree exports	.csv	2 years
Application data	Not applicable	Customer controlled*
Release data	Not applicable	Customer controlled*
Issue data	Not applicable	Customer controlled*
User data	Not applicable	Customer controlled*

*You are responsible for creation and deletion of the specified data as long as you maintain an active status with OpenText Fortify on Demand. You 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 OpenText Fortify on Demand service, the termination data retrieval period is 30 days.

For more information, contact support.

13. Support

OpenText Fortify on Demand offers support through self-service resources and the Help Center, staffed 24/7 by a dedicated support team. The self-servic resources include video demonstrations, a knowledge base, and product documentation. If you have an unresolved issue, start a live chat with support or submit a support ticket in the Help Center send a request to the dedicated FEDRamp support email. You can call support at 800.893.8141 or 650.800.3233 if internet access is unavailable.

Access support resources

Support resources are available through the portal. The portal contains direct links to how-to videos, the HTML user guide, live chat, and the Help Center. The Help Center is OpenText Fortify on Demand's support ticket system. It also hosts the knowledge base and the user guide in PDF format.



Note

You can directly log in to the Help Center through the relevant URL using your OpenText Fortify on Demand credentials:

- AMS: https://helpcenter.ams.fortify.com
- EMEA: https://helpcenter.emea.fortify.com
- APAC: https://helpcenter.apac.fortify.com
- SGP: https://fodsgp.zendesk.com/

To access support resources:

Click the help menu and select one of the following:

- **How To Guides** - opens how-to video guides, part of the Fortify Digital Learning offerings
- **Documentation** - opens the user guide
- **Help Center** - opens the Help Center
- **Live Chat** - opens the Live Chat window where you can chat with support 24/7

Submit a support ticket

To submit a support ticket in the Help Center:

1. Click the help menu and select **Help Center**.
2. Click **Submit a Ticket**. **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 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.

Track a support ticket

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**.
2. Click **View Tickets**.
   Your tickets are displayed. Tickets have one of the following statuses:
    - **Open** - Your request has been received and assigned to support who is working to resolve it.
    - **Awaiting your reply** - The assigned support has a follow-up question for you. Tickets that are set to **Pending** typically remain that way until you respond and provide the information support needs to continue resolving the issue.
    - **Solved** - Support has resolved the 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 support team is still working on.
    - **Awaiting your reply**- Show tickets that require action from your organization.
    - **Solved** - Show tickets that have been resolved.

© Copyright 2026 Open Text

For more info, visit https://docs.microfocus.com