OpenText™ Fortify on Demand

Software Version: 24.2

User Guide

Document Release Date: April 2024
Software Release Date: April 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

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

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

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

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

This document was produced for OpenText™ Fortify on Demand CE 24.2 on April 25, 2024. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting OpenText Fortify on Demand Customer Support

Contact OpenText Fortify on Demand Customer Support through the following ways:

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

For More Information

For more information about Fortify software products:

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

About the Documentation Set

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

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

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

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

Fortify Product Feature Videos

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

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

What's New

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

v24.2

Engine and Rulepack Updates

Fortify Software Security Content 2023 Update 4 Support (March 2024)

Fortify on Demand has implemented Fortify Software Security Content 2023 update 4 from Fortify Security Research (SSR). For more information, see https://community.microfocus.com/cyberres/fortify/w/announcements/46822/opentext-fortify-software-security-content-2023-update-4.

Fortify Audit Assistant 24.1 (February 2024)

Fortify on Demand has implemented Fortify Audit Assistant 24.1. Fortify Audit Assistant predicts whether or not the issues returned from Fortify Static Code Analyzer scan results represent true vulnerabilities.

Fortify WebInspect 23.2.0 Support (February 2024)

Fortify on Demand has implemented Fortify WebInspect 23.2.0 for scanning web applications. Fortify WebInspect 23.2.0 offers the following Event-based Web Macro Recorder updates:

- The Event-based Web Macro Recorder now supports the use of JavaScript during execution to detect and notify the Fortify WebInspect sensor of logout.
- The Event-based Web Macro Recorder now supports event handlers that react to unpredictable events, such as dialogs opening and popup DOM elements that steal focus.
- The Event-based Web Macro Recorder now supports the use of web storage keys that enable the application to determine and maintain state.

Announcements

Fortify Versioning Update

Beginning in 2024, Fortify product GA versions are transitioning to be in parity with OpenText release versioning. Product versions are based on the targeted release year and quarter. This change only impacts product versions that do not currently follow this versioning strategy.

For example:

2023 release versioning

- Fortify Static Code Analyzer 23.1.0 (release targeted for 2nd quarter 2023)
- Fortify Static Code Analyzer 23.2.0 (release targeted for 4th quarter 2023)

2024 release versioning, and beyond

- Fortify Static Code Analyzer 24.2.0 (release targeted for 2nd quarter 2024)
- Fortify Static Code Analyzer 24.4.0 (release targeted for 4th quarter 2024)

New Features

Auto Detect Technology Stack for Static Scans

An option to have Fortify on Demand determine the technology stack for a static scan payload has been added. **Auto Detect** is the default option when configuring scans for new releases. Upon scan completion, the scan summary and reports display the technology stack that was detected for the payload.

In conjunction, associated GET and POST endpoints have been updated.

If you are interested in enabling the auto detect feature for your tenant, contact support.

Download Login Macro for Authenticated Dynamic Scans

For completed Dynamic and Dynamic+ scans that included authentication, the login macro generated by the testing team is now available for download on the Scans pages. The login macro can be used to facilitate transitioning to DAST Automated scans.

> **Note:** The testing team does not offer services beyond providing the login macro used in the scan.

Debricked Integration Updates

- Debricked assessments now offer scanning for unmanaged dependencies not defined in manifest files by examining fingerprints of the application files (including binary files). Currently C# (.NET), Java, and Python are supported. Debricked scans include both fingerprint analysis and lock file analysis.

  > **Note:** Certain scan result details, such as dependency trees, are not available with Debricked fingerprint analysis.

- Open source scan issues are now mapped to OWASP 2021 and PCI 4.0 classifications.

Issue Attributes Support

Fortify on Demand now supports creation of issue attributes. Security Leads can manage issue attributes.

Users can specify attribute values when updating issues. Users can filter and group issues by issue attributes that are picklists. Issue attributes have been added to the issues data export.

Release Attributes Support

Fortify on Demand now supports creation of release attributes. Security Leads can manage release attributes.

Users can specify attribute values when creating and updating releases, including copy state releases. Users can filter releases by release attributes that are picklists. Release attributes have been added to the releases and scans data exports.

In conjunction, associated GET, PUT, and POST endpoints have been updated.

Specify Custom Fields Values for Azure DevOps Bug Tracking

For Azure DevOps projects with custom fields, users can specify default values for those custom fields through the bug tracker integration feature. Upon authentication to Azure DevOps on the **Bug Tracker** tab of the Application Settings page, the custom fields appear. If applicable, default values from Azure DevOps are populated. Required custom fields are marked in red. Users can override default values when submitting bugs.

Technology Stack Updates

The following technology stack options for static scans have been added:

- Go 1.21
- Java 21
- Python 5.0 (Django)

Full support will be available with the Fortify Static Code Analyzer 24.2.0 release.

Tool Download Updates

The following tool downloads were updated:

- Event-based Web Macro Recorder (February 2024)
- Fortify Audit Workbench (April 2024)
- Fortify ScanCentral SAST 23.2.1 (February 2024)

Other API Updates

Details for the most recent file upload have been added to `GET /api/v3/releases/{releaseId}/dynamic-scans/scan-setup`.

Improvements

Secure Code Warrior Integration Updates

Fortify on Demand has updated the Secure Code Warrior training integration to increase training offerings and provide links to educational resources.

- Modules are available for additional languages supported by Secure Code Warrior.
- The **Interactive Training** section on the **Recommendations** tab of the Issues page displays links to Secure Code Warrior videos as well as external educational resources.

Mobile Assessment Payload Validation Update

The following updates have been made to the mobile assessment payload validation process:

- Payload validation can be skipped for payloads greater than 500 MB.
- A progress bar is available during payload validation.

Other Updates

- For DAST Automated scan cancellations, hovering over the scan status icon in the portal displays a message to download the scan log. The scan log is available for download on the Scans pages.
- The Scan ID column has been added to the Scans pages.
- The **Fix Validated Date** (the date an issue was marked as fixed) column has been added to the issues data export.

Chapter 1: Introduction

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

This section contains the following topics:

Fortify on Demand Overview

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

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

Security Assessments

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

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

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

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

Entitlements

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

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

Refer to your contract for specific entitlement details.

Support

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

Security Rating System

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

Likelihood and Impact

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

Likelihood

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

Impact

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

Priority Order

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

Critical

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

SQL injection is an example of a critical issue.

High

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

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

Medium

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

Path manipulation is an example of a medium issue.

Low

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

Dead code is an example of a low issue.

Best Practices

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

Info

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

Five-Star Assessment Rating

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

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

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

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

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

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

Service Level Objectives

All assessments have a target turnaround time, represented by the service level objective (SLO) of the chosen assessment type. The SLO is specified in business days, based on the Fortify on Demand data center's time zone. The SLO is four hours to two business days for a static assessment, two to three business days for a dynamic assessment, and one to four 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 "Configuring a Static Scan" on page 108,"Configuring a Dynamic Scan" on page 129, and "Configuring a Mobile Scan" on page 157.

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

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

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

Service Level Objective Start and End Dates

The SLO start and end dates are defined as follows:

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

Service Level Objective Exceptions

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

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

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

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

Chapter 2: Getting Started

This section contains the following topics:

Before You Start

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

- An active internet connection
- Portal credentials

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

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

Logging In and Out of the Portal

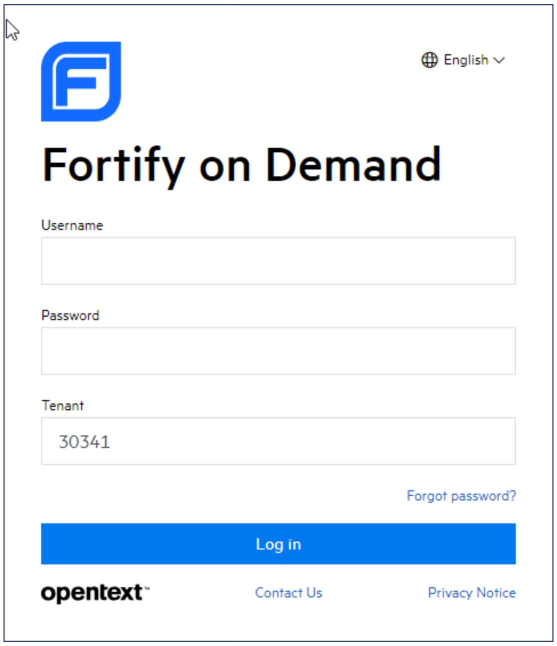
You can access the portal once you have received your portal credentials.

Logging in to the Portal

To log in to the portal:

1. Type the portal URL that was provided with your user credentials in your browser's address bar.

   The login page appears.
2. Type your username, password, and tenant code.



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

3. Click **Login**.

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

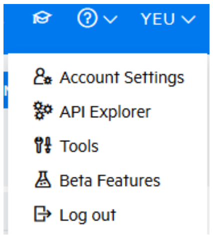
> **Note:** If your organization has two factor authentication enabled, you are prompted to type a security code that you receive through SMS or email.

Logging out of the Portal

Log out of the portal from the portal toolbar settings. Note that the portal automatically logs you out after a 20 minute period of inactivity.

To log out of the portal:

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

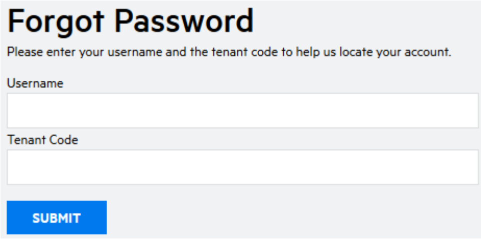


Resetting Your Password

To reset a forgotten password:

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

   The Forgot Password page appears.

   Forgot Password

   Please enter your username and the tenant code to help us locate your account.

   Username

   Tenant Code

2. Type your username and tenant code.
3. Click **Submit**.

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

4. Click the link in the email.

   The Reset Password page appears.

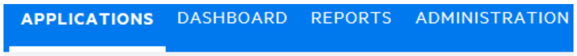
   > **Note:** If the password reset link has expired, follow the instructions in the email to request a new link.

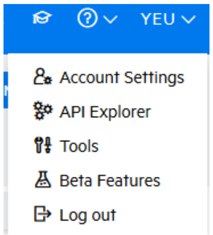
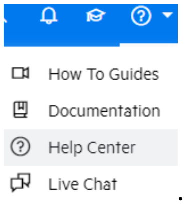
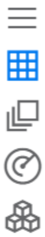
5. In the **Password Challenge Answer** field, type the answer to the challenge question. If you do not have a password challenge question and answer, this step does not apply to you.
6. Type and retype the password.
7. Click **Ok**.

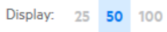
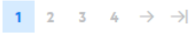
   The password is reset.

Navigating the Portal

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

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

Task	Action
Access account settings and additional resources	Click your account name on the toolbar.  YEU Account Settings API Explorer Tools Beta Features Log out
Access portal search	Click 🔍. For more information, see " Searching the Portal" on the next page.
Access portal notifications	Click 🔔29. For more information see "Managing Notifications" on page 30.
Access training courses	Click 🎓. For more information, see "Training Courses" on page 368.
Access help resources	Click the help menu. 
Navigate to a page within a parent view	Click an icon on the sidebar. 
Access context-sensitive help	Click ?. A new window opens that displays the help topic for the feature.
Sort columns on a page	Click a column header. A white triangle in the header indicates the field being sorted and the sort order of your data. To reverse the order, click the header a second time.
Change the number	Click **25**, **50**, or **100**.

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

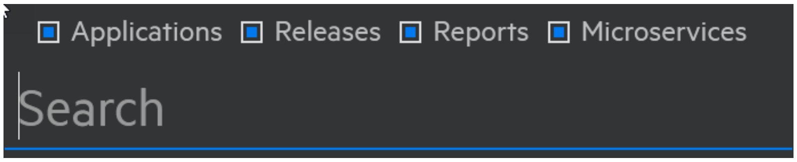
Searching the Portal

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

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

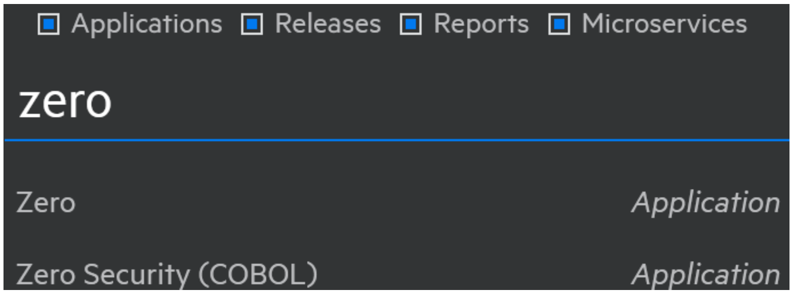
1. Click the 🔍 icon on the portal toolbar.

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

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

   Search results appear in a drop-down list.

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

Managing Your Account Settings

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

This section covers the following topics:

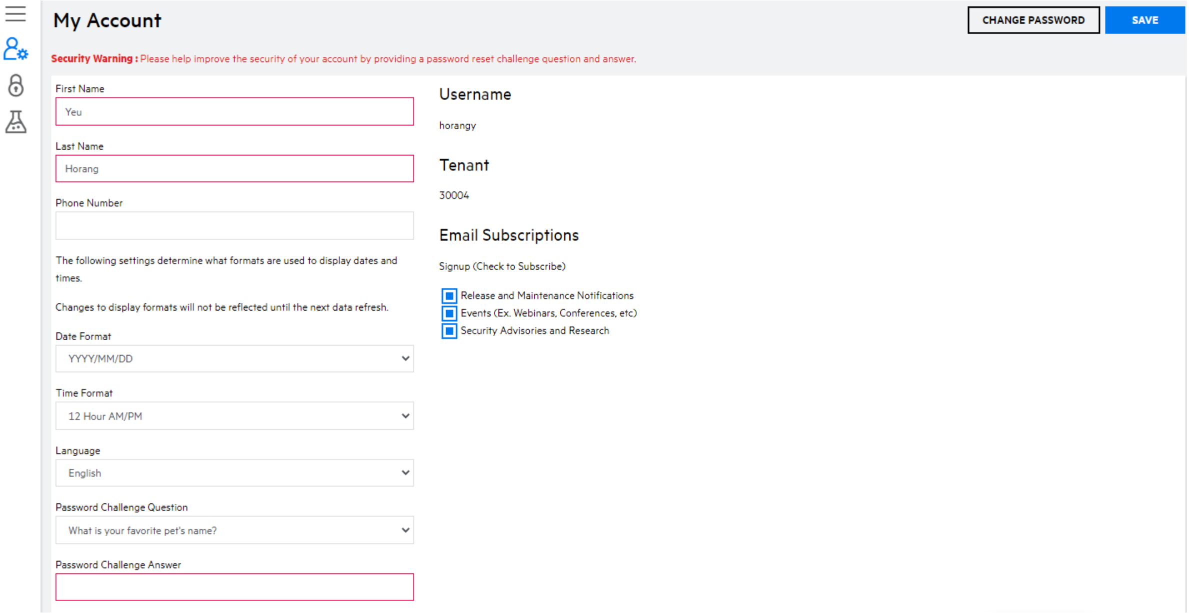
Editing Your Account Settings

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

To edit your account settings:

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

   The My Account page appears.



My Account

Security Warning : Please help improve the security of your account by providing a password reset challenge question and answer.

First Name: Yeu

Last Name: Horang

Phone Number:

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

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

Date Format: YYYY/MM/DD

Time Format: 12 Hour AM/PM

Language: English

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

Password Challenge Answer:

Username

horangy

Tenant

30004

Email Subscriptions

Signup (Check to Subscribe)

☑ Release and Maintenance Notifications
☑ Events (Ex. Webinars, Conferences, etc)
☑ Security Advisories and Research

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

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

Field	Description
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	Your case-insensitive answer to the selected password challenge question **Note:** You will not be able to 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 Fortify on Demand events. You can sign up to receive notifications about releases and maintenance, security advisories, and relevant webinars and conferences.
4. Click **Save**.

   A confirmation message appears indicating that you have successfully saved your changes.

Changing Your Account Password

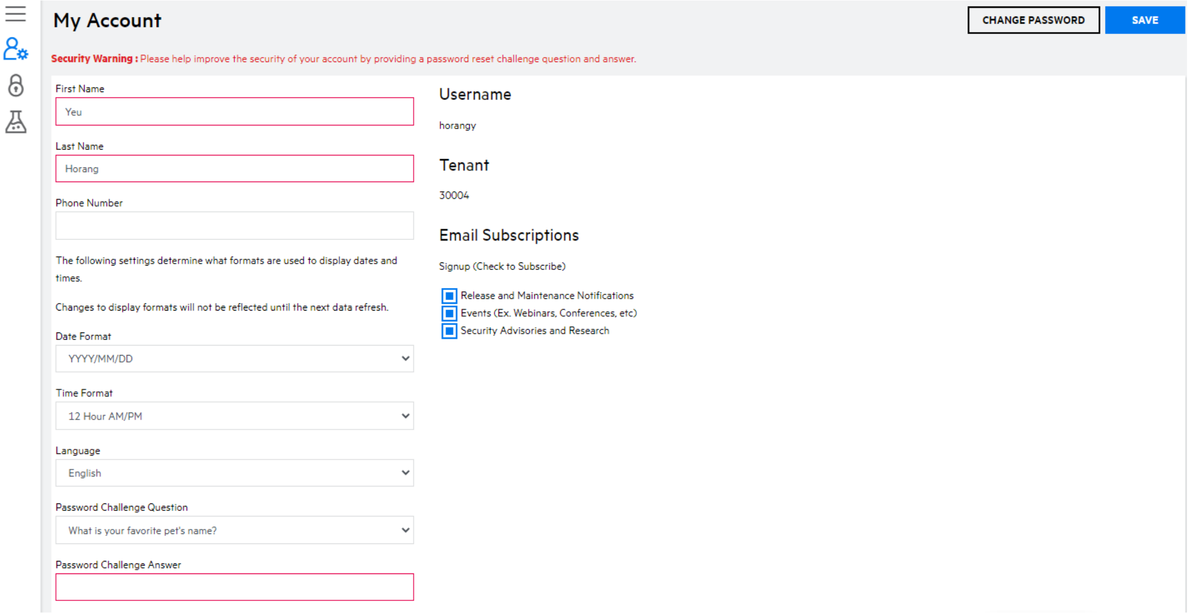
You can change your account password on the My Account page.

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

To change your account password:

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

   The My Account page appears.



My Account

Security Warning : Please help improve the security of your account by providing a password reset challenge question and answer.

First Name: Yeu

Last Name: Horang

Phone Number:

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

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

Date Format: YYYY/MM/DD

Time Format: 12 Hour AM/PM

Language: English

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

Password Challenge Answer:

Username

horangy

Tenant

30004

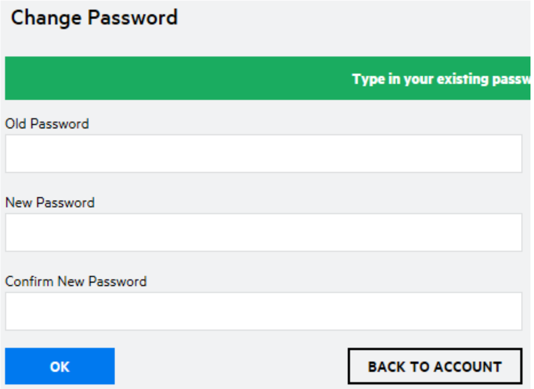
Email Subscriptions

Signup (Check to Subscribe)

☑ Release and Maintenance Notifications
☑ Events (Ex. Webinars, Conferences, etc)
☑ Security Advisories and Research

2. Click **Change Password**.

   The Change Password page appears.



Change Password

Type in your existing passw

Old Password:

New Password:

Confirm New Password:

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

Opting In To and Out Of Beta Features

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

To manage beta features:

1. Click your account name and select **Beta Features**.

   The Beta Features page appears.

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

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

Managing Notifications

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

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

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

This section contains the following topics:

Viewing Notifications

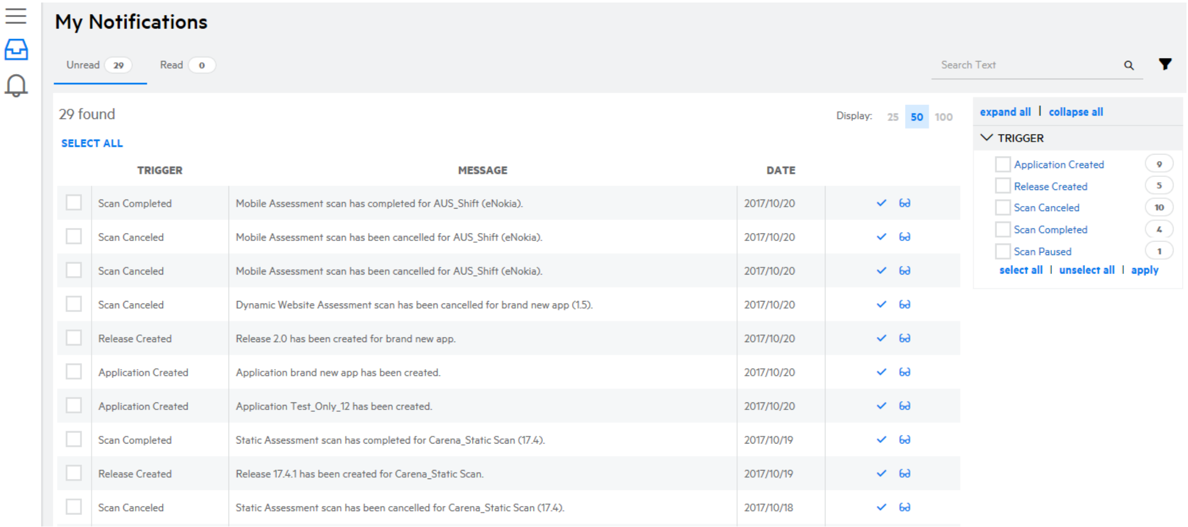
You can view notifications from any page in the portal. When a trigger event occurs for which you are subscribed, a number next to the Notifications icon on the toolbar is incremented. This number is a tally of your notifications that have not been marked as read.

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

To view notifications:

1. Click the 29 icon on the portal toolbar.

   The Notifications page appears, displaying a list of your unread notifications.

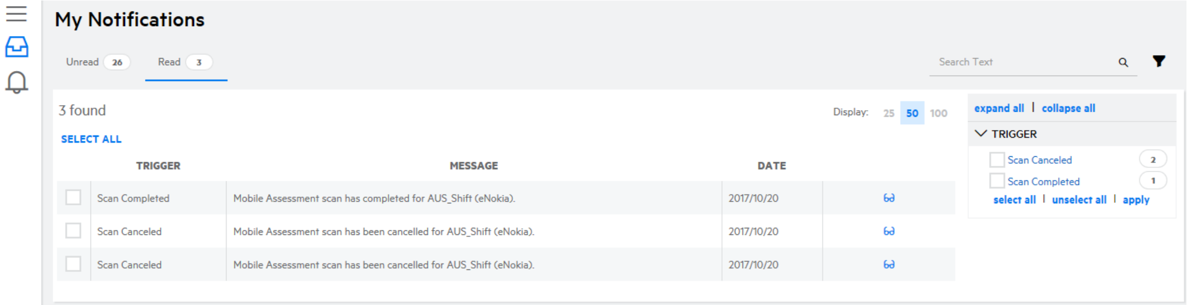


	TRIGGER	MESSAGE	DATE	
□	Scan Completed	Mobile Assessment scan has completed for AUS_Shift (eNokia).	2017/10/20	✓ 6d
□	Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	✓ 6d
□	Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20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

2. To view a notification in greater detail, click the 6d icon in the notification's action column. You are taken to the relevant application, release, or individual issue's page.
3. To mark a notification as read, click the ✓ icon in the notification's action column. You can also filter the notification list and click **Mark as Read** to batch edit notifications.

   The notifications are moved to Read Notifications and removed from the tally.
4. To view notifications that you have previously marked as read, select the **Read** tab.

   The list of your read notifications appears.



	TRIGGER	MESSAGE	DATE	
□	Scan Completed	Mobile Assessment scan has completed for AUS_Shift (eNokia).	2017/10/20	6d
□	Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	6d
□	Scan Canceled	Mobile Assessment scan has been cancelled for AUS_Shift (eNokia).	2017/10/20	6d

Creating an Individual Subscription

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

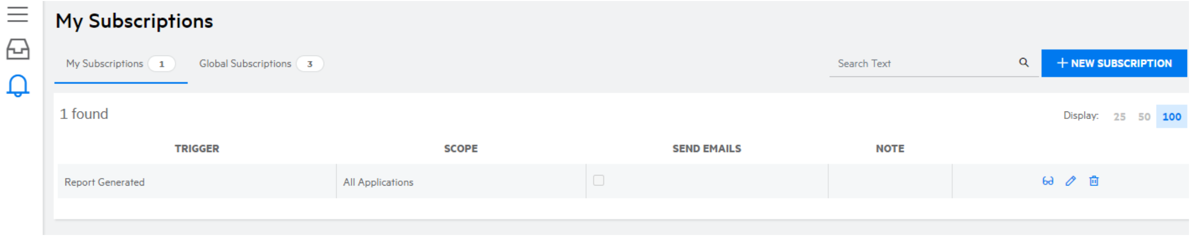
To create an individual subscription:

1. Click the 29 icon on the portal toolbar.

   The Notifications page appears.

2. Click **Subscriptions**.

   A list of your individual subscriptions appears.

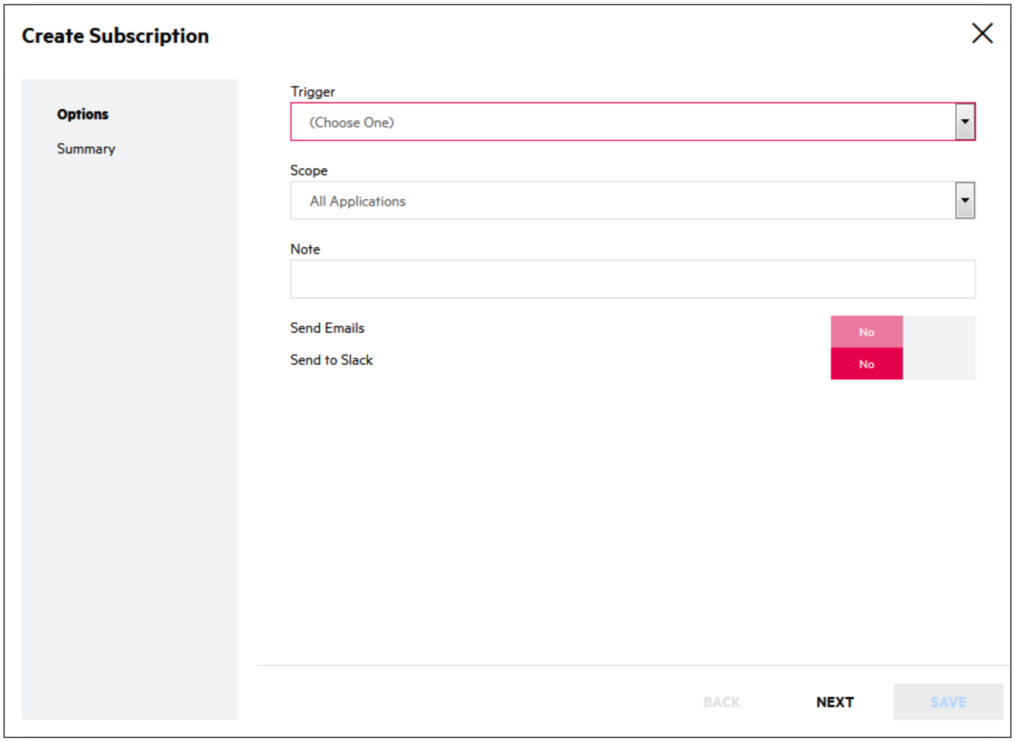


1 found

TRIGGER	SCOPE	SEND EMAILS	NOTE
Report Generated	All Applications	☐	

3. **Click +New Subscriptions.**

   The Create Subscription modal window opens.



Trigger: (Choose One)

Scope: All Applications

Note:

Send Emails: No

Send to Slack: No

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**, and **Business Criticality**.
Note	(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 only available for non-issue related notifications.
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.

Creating a Global Subscription

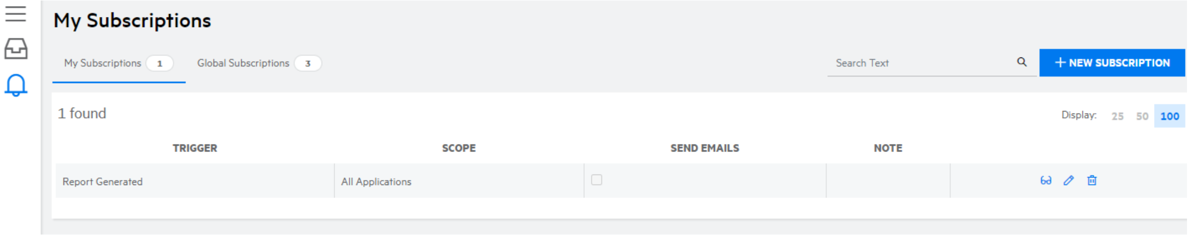
Security Leads can create tenant level global subscriptions for all users, specific roles, or specific groups.

To create a global subscription:

1. Click the 🔔29 icon on the portal toolbar.

   The Notifications page appears.
2. Click **Subscriptions**.

   A list of your individual subscriptions appears.



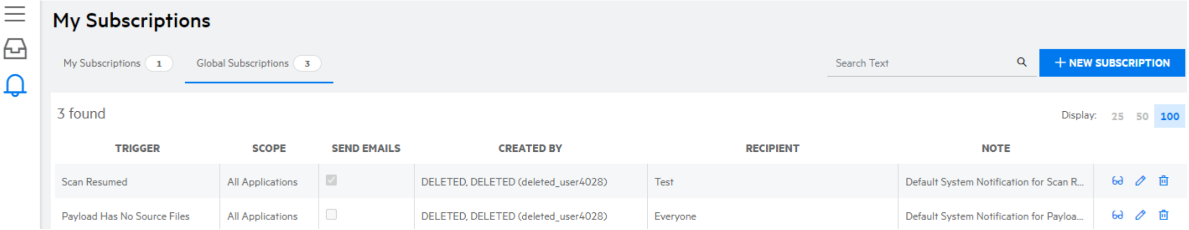
My Subscriptions

1 found

TRIGGER	SCOPE	SEND EMAILS	NOTE	
Report Generated	All Applications	□		

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

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



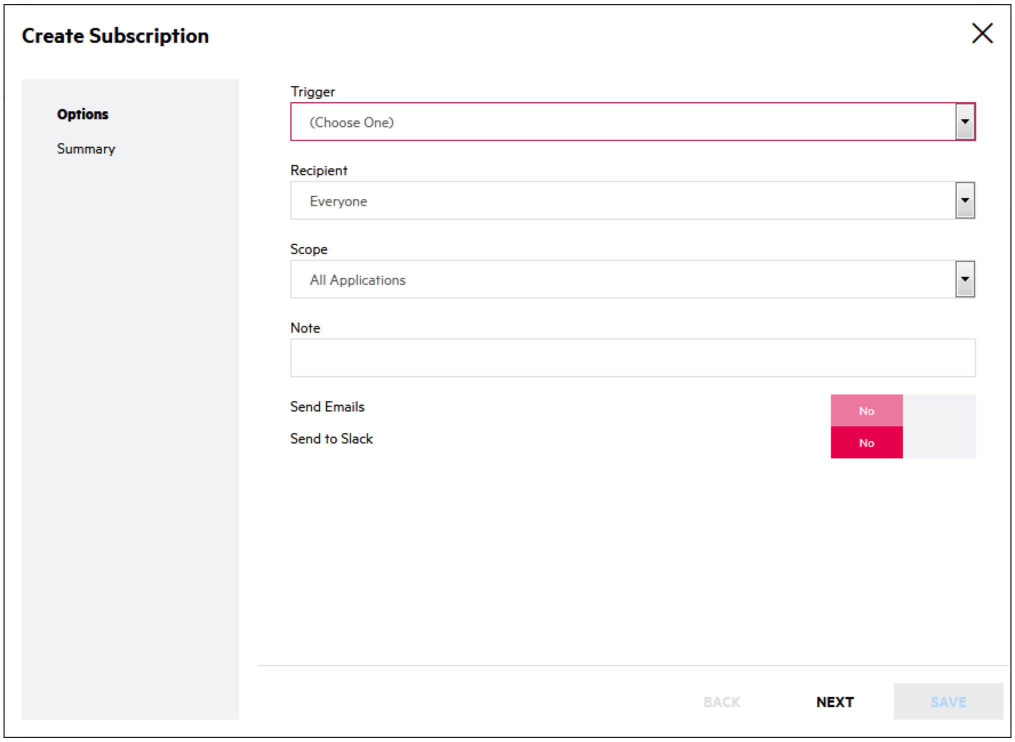
My Subscriptions

3 found

TRIGGER	SCOPE	SEND EMAILS	CREATED BY	RECIPIENT	NOTE	
Scan Resumed	All Applications	☑	DELETED, DELETED (deleted_user4028)	Test	Default System Notification for Scan R...	
Payload Has No Source Files	All Applications	□	DELETED, DELETED (deleted_user4028)	Everyone	Default System Notification for Payloa...	

4. **Click +New Subscription.**

The Create Subscription modal window opens.



Trigger: (Choose One)

Recipient: Everyone

Scope: All Applications

Note:

Send Emails: No

Send to Slack: No

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**, and **Business Criticality**.
Note	(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 non-issue related notifications.
Send to	(Optional) Move the slider from **No** to **Yes** to post notifications to Slack. This

Slack	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.

Editing a Subscription

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

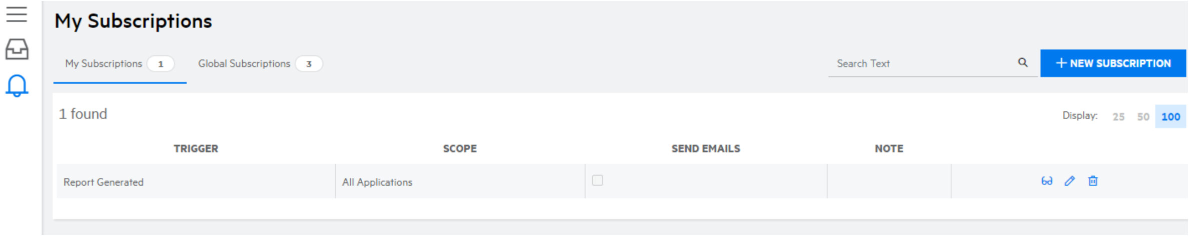
To edit subscriptions:

1. Click the 🔔29 icon on the portal toolbar.

   The Notifications page appears.

2. Click **Subscriptions**.

   A list of your custom subscriptions appears.

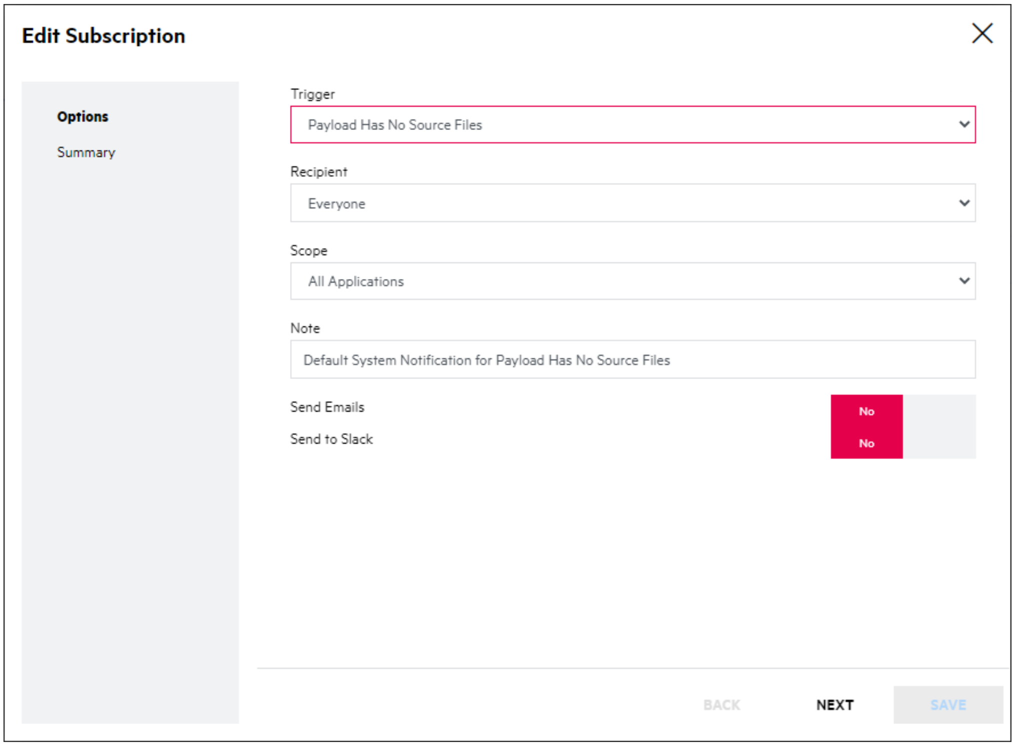


1 found

TRIGGER	SCOPE	SEND EMAILS	NOTE	
Report Generated	All Applications	□		

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 ✎ icon next to the subscription you want to edit.

   The Edit Subscription window appears.



Edit Subscription

Options

Summary

Trigger: Payload Has No Source Files

Recipient: Everyone

Scope: All Applications

Note: Default System Notification for Payload Has No Source Files

Send Emails: No

Send to Slack: No

5. Edit the fields as needed. For information on the fields, see "Creating an Individual Subscription" on page 31 and "Creating a Global Subscription" on page 33.

   Your subscription changes are saved.

Deleting a Subscription

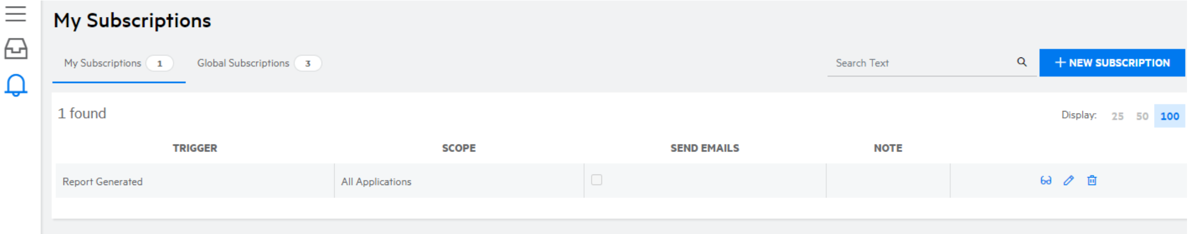
You can delete individual subscriptions that you created. Security Leads can delete all global subscriptions, including system default global subscriptions.

To delete a subscription:

1. Click the 🔔29 icon on the portal toolbar.

   The Notifications page appears.
2. Click **Subscriptions**.

   A list of your individual subscriptions appears.



My Subscriptions

1 found

TRIGGER	SCOPE	SEND EMAILS	NOTE
Report Generated	All Applications	□	

3. If you are deleting an individual subscription, stay on the **My Subscriptions** tab. If you are deleting a global subscription, select the **Global Subscriptions** tab.

4. Click the 🗑 icon next to the subscription you want to delete.

   A confirmation message appears.

5. Click **Yes** to confirm the deletion.

   The subscription is removed from the list of subscriptions.

Chapter 3: Managing Applications and Releases

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

This section contains the following topics:

Structuring Applications and Releases

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

Application Definition

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

Fortify on Demand defines an application in the following contexts:

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

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

A microservice as a small, modular service that runs as an independent, loosely coupled process and communicates through a well-defined, lightweight mechanism to serve a single function of a business application. For an application using a microservices architecture, a Static Subscription entitles a customer to test up to 10 microservices that form some or all of the application. Each microservice must be packaged and submitted as a single ZIP file of 100 MB or less. For all other static assessment services, each microservice is considered a separate application.

The following conditions apply to microservice applications:

- Supported technology stacks are: .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).

Release Definition

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

The following examples show how releases can be structured:

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

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

- Development
- QA/Test
- Production
- Retired

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

Managing an Application

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

This section covers the following topics:

Creating an Application

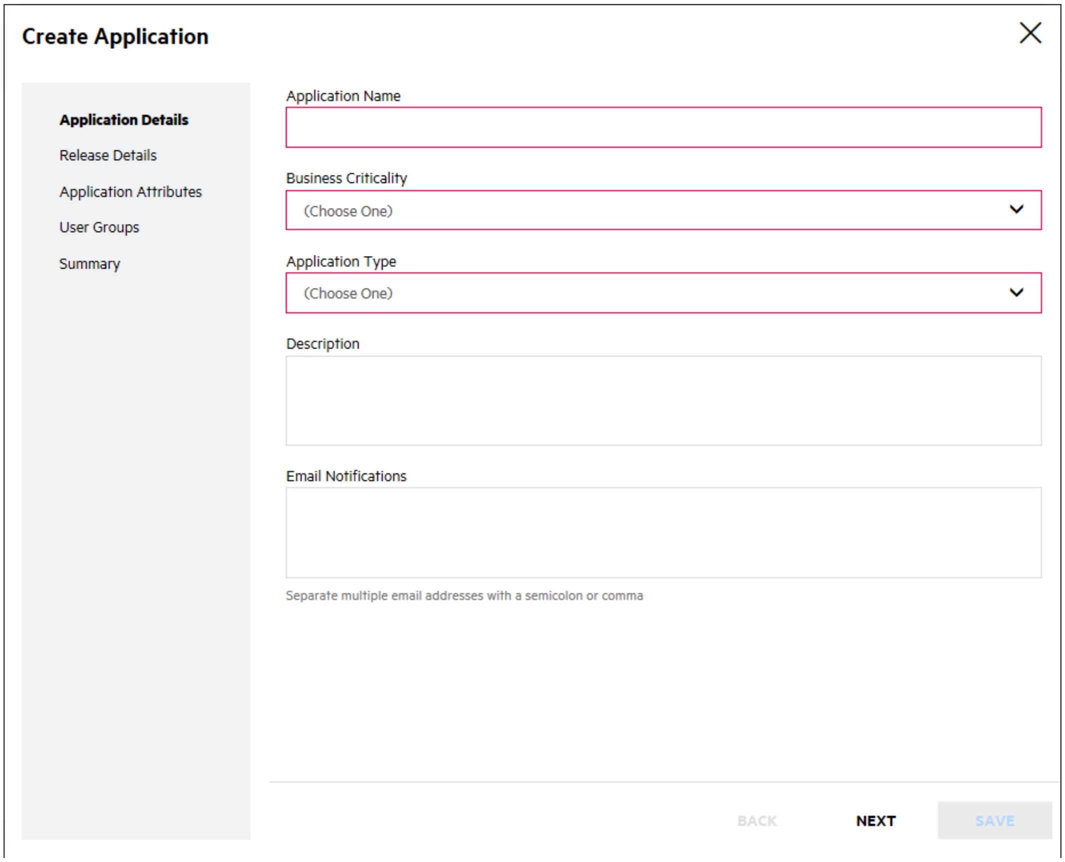
Before you can start the initial security assessment of an application, you need to create a new application in Fortify on Demand.

To create an application:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **+New Application**.

   The Create Application wizard appears.
3. In the **Application Details** page, define the application. Fields are required, unless otherwise noted.



Create Application

Application Name

Business Criticality

(Choose One)

Application Type

(Choose One)

Description

Email Notifications

Separate multiple email addresses with a semicolon or comma

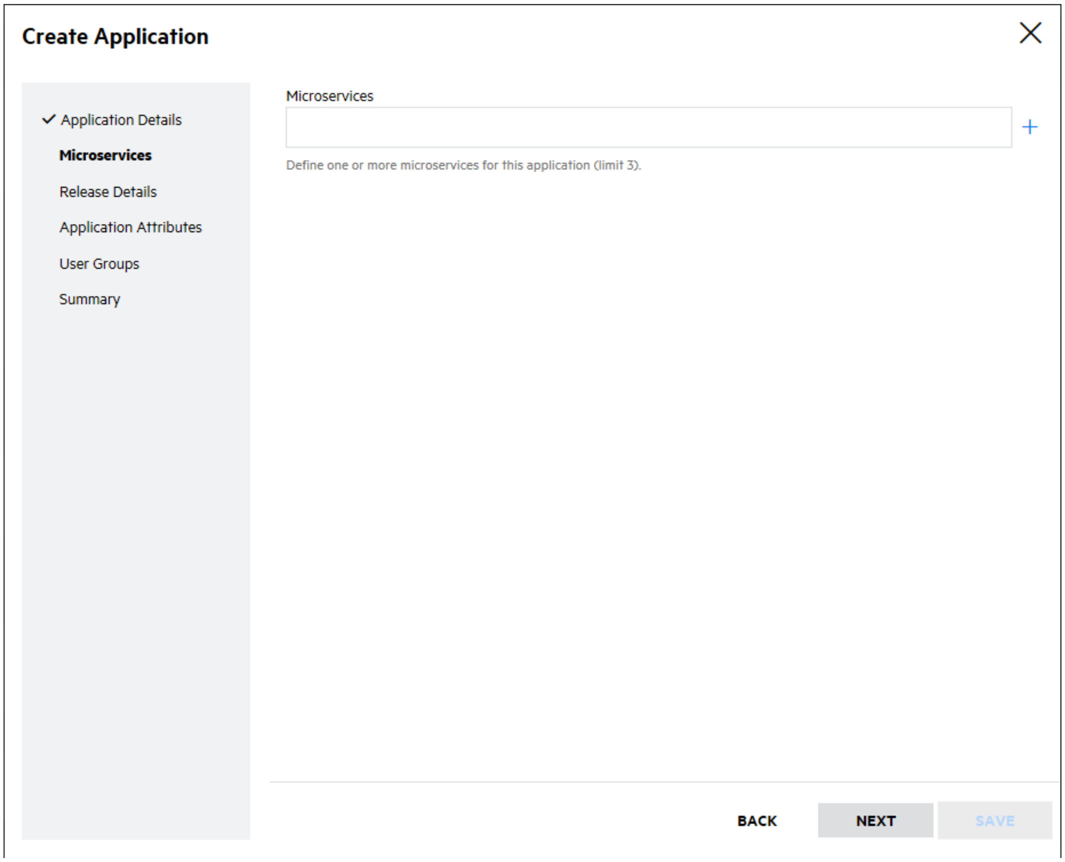
Field	Description
Application Name	Type the name of your application.
Business Criticality	Select the application's level of importance: - **High**: Security issues could have catastrophic consequences for the business. - **Medium**: Security issues would have non-trivial consequences, but ones which 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 will help you manage multiple applications.
Email Notifications	(Optional) List the email addresses that will receive email notifications of scan status updates for the application. Separate multiple email addresses

Field	Description
	with a semicolon or comma.
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 +.

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

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



Create Application

✓ Application Details

Microservices

Release Details

Application Attributes

User Groups

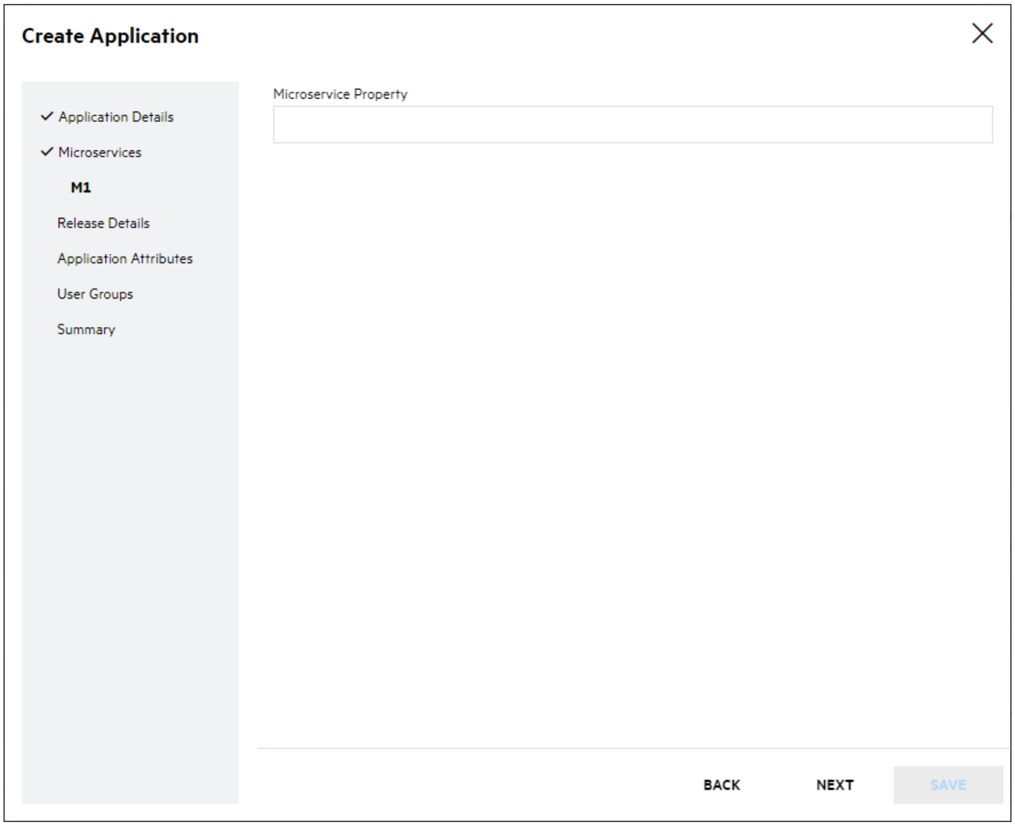
Summary

Microservices

+

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

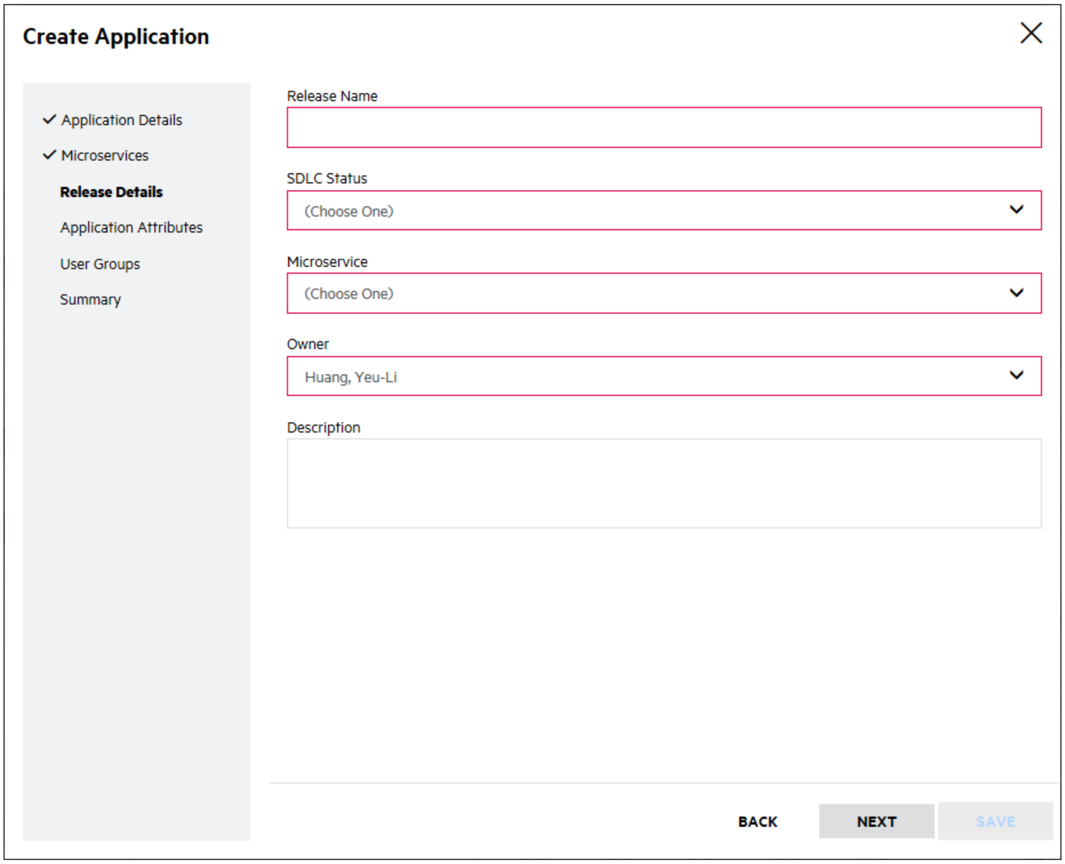
6. Click **Next**.
7. (Microservice applications only) If microservice attributes have been configured, specify the microservice attributes. Click **Next** to do this for each microservice you added earlier.



Create Application

Microservice Property

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



Create Application

Release Name

SDLC Status: (Choose One)

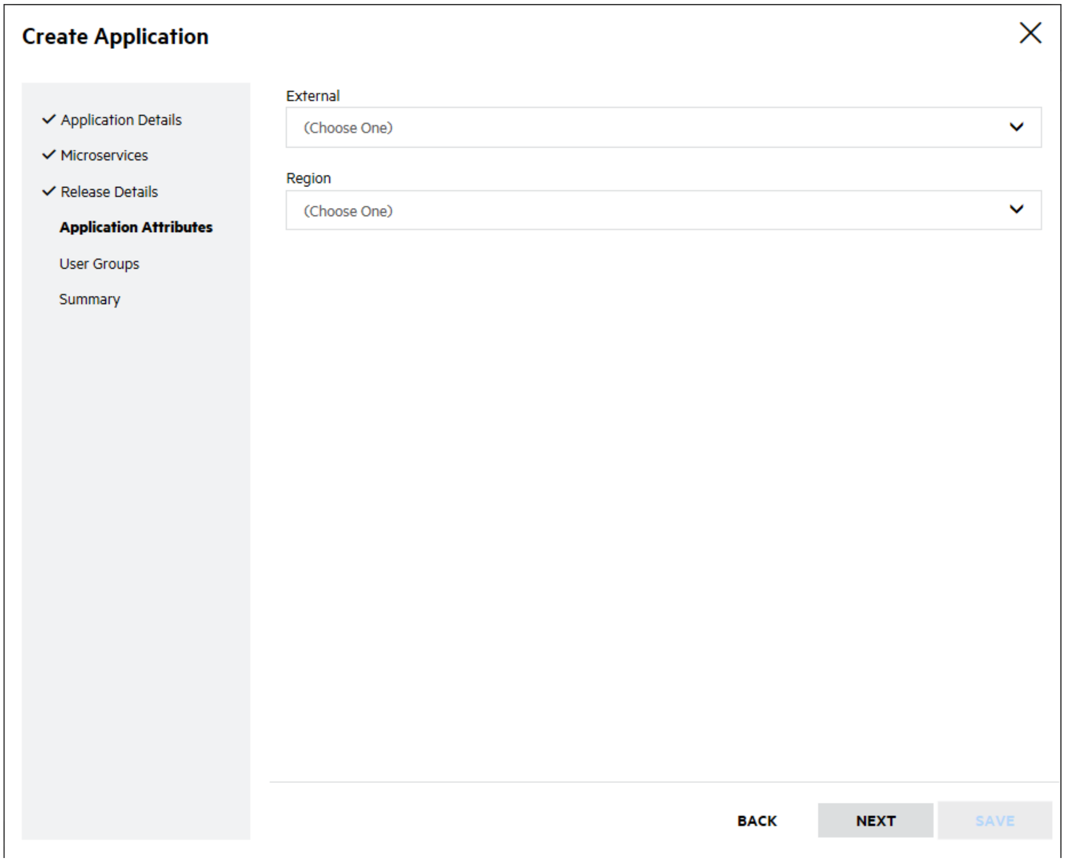
Microservice: (Choose One)

Owner: Huang, Yeu-Li

Description

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.

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

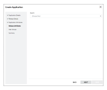


Create Application

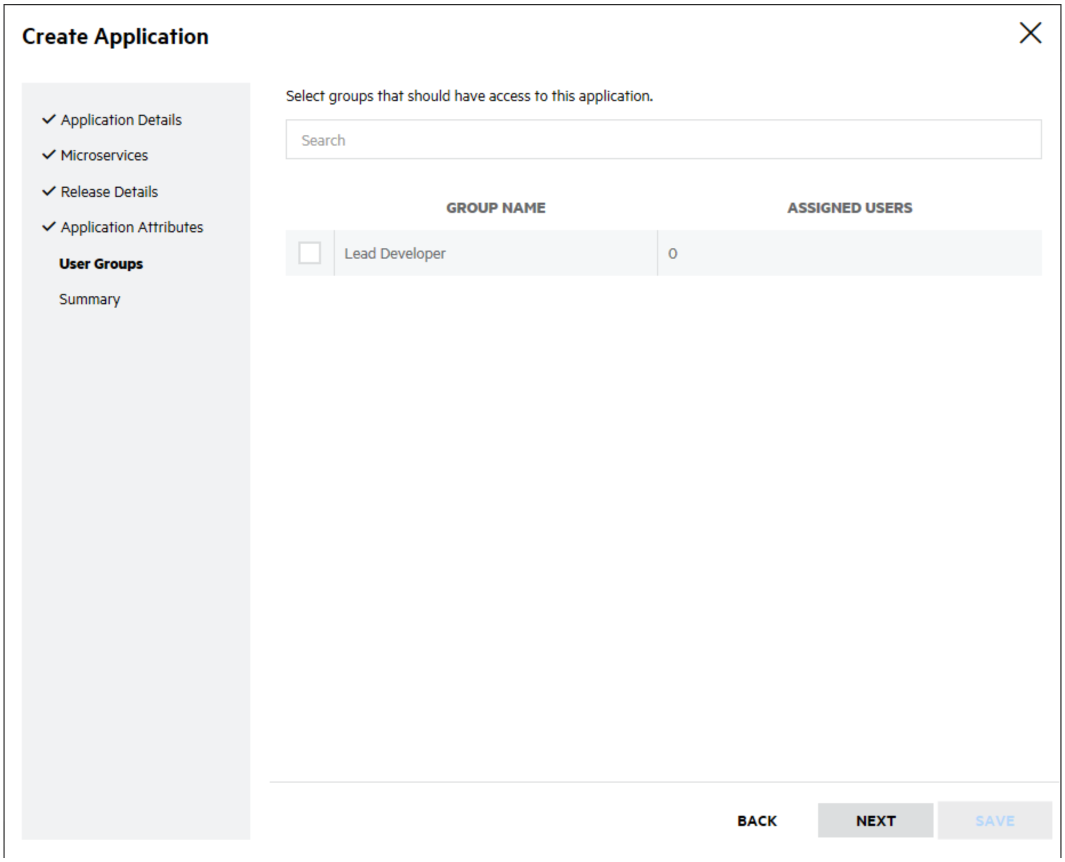
External
(Choose One)

Region
(Choose One)

12. Click **Next**.
13. If custom release attributes are configured for the tenant, in the **Release Attributes** page, specify the release attributes.



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

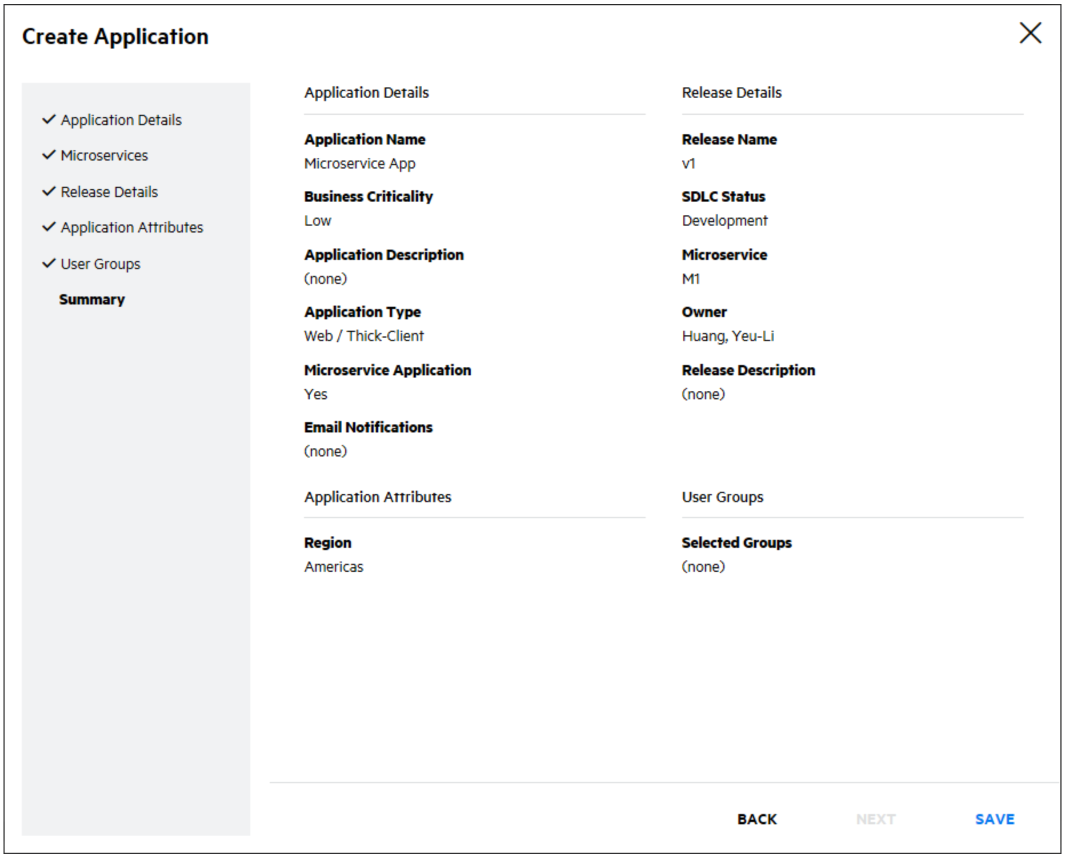


Create Application

Select groups that should have access to this application.

	GROUP NAME	ASSIGNED USERS
□	Lead Developer	0

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



Application Details

Application Name
Microservice App

Business Criticality
Low

Application Description
(none)

Application Type
Web / Thick-Client

Microservice Application
Yes

Email Notifications
(none)

Release Details

Release Name
v1

SDLC Status
Development

Microservice
M1

Owner
Huang, Yeu-Li

Release Description
(none)

Application Attributes

Region
Americas

User Groups

Selected Groups
(none)

17. Click **Create Application**.

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

Viewing Application Details

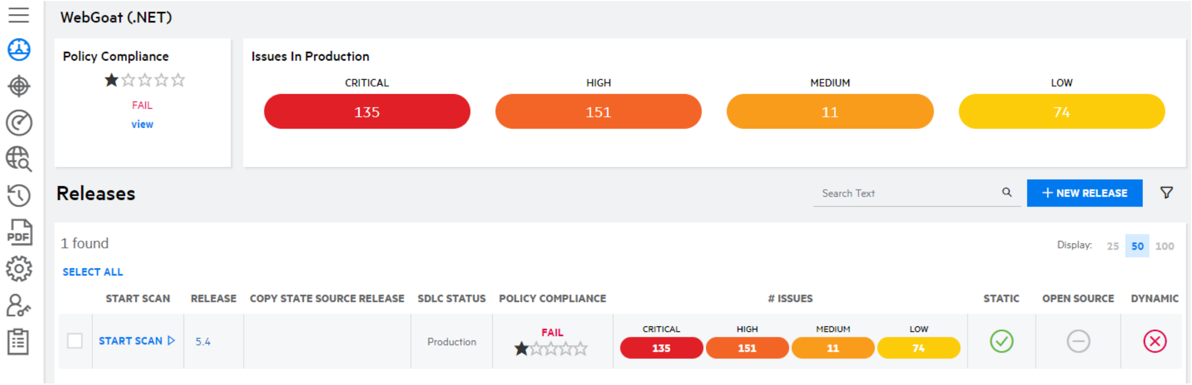
The Application Overview page displays an overview of the application and its releases. It serves as a dashboard for the application, offering a quick yet comprehensive snapshot of the application's production security risk. Here you can filter the application's releases, search for particular releases,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

To view details of an application:

1. Select the **Applications** view.

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

   The Application Overview page appears. The page shows the following details about an application: production risk and policy compliance, security status, and a list of associated releases (sorted from the latest to the earliest last completed scan date by default).

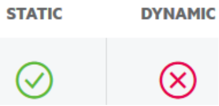


	START SCAN	RELEASE	COPY STATE SOURCE RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES	STATIC	OPEN SOURCE	DYNAMIC
□	START SCAN ▷	5.4		Production	FAIL ★☆☆☆☆	CRITICAL 135 HIGH 151 MEDIUM 11 LOW 74	✓	⊖	⊗

Navigating the Application Overview Page

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

Task	Action
View the security policy applied to the application	Click **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 number of issues (including Application Monitoring issues) across an application's production releases .
View the application's security status	The **Security Status** box displays the Continuous Application Monitoring status.
Search the application's releases	Enter search word in the 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.

Task	Action
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 icon. Click it to directly access the scan status details.  STATIC DYNAMIC ✓ ⊗ • 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."
Expand or collapse filters	Click expand all | collapse all ⚙ or the arrow next to the filter name.
Hide or display the filter list	Click ▼.
Remove applied filters	Click **X** or click **X Clear Filters**.

Filtering the Application Overview page

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

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

To filter the Application Overview page:

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

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

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

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

Editing Application Settings

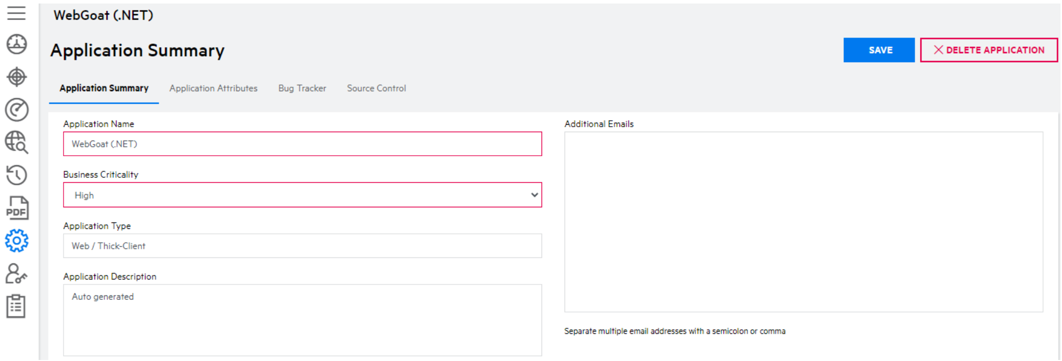
You can edit application settings after the application has been created.

To edit application settings:

1. Select the **Applications** view.

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

   The Settings page appears.



WebGoat (.NET)

Application Summary

Application Name: WebGoat (.NET)

Business Criticality: High

Application Type: Web / Thick-Client

Application Description: Auto generated

Additional Emails

Separate multiple email addresses with a semicolon or comma

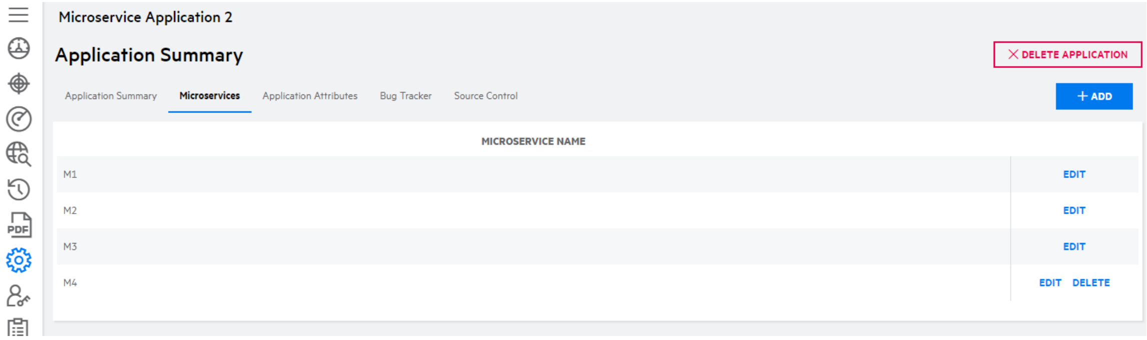
4. Select the tab that corresponds to the application settings you want to edit.

- The **Application Summary** tab displays application details.

Field	Description
Application Name	Name of your application
Business Criticality	Business Criticality level
Application Type	Application type (not editable for microservice applications)
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

- (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.

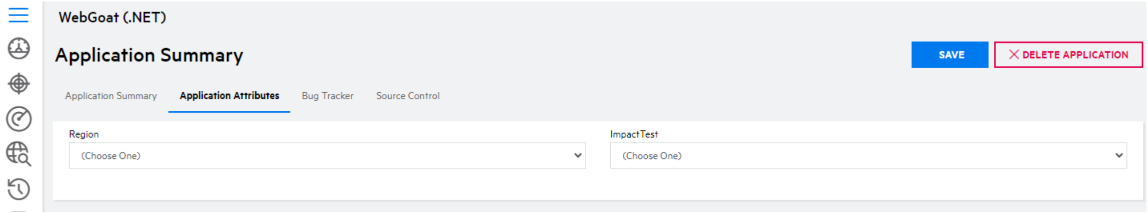


Microservice Application 2

Application Summary

MICROSERVICE NAME	
M1	EDIT
M2	EDIT
M3	EDIT
M4	EDIT DELETE

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



Region: (Choose One)

ImpactTest: (Choose One)

- The **Bug Tracker** tab displays configuration settings for bug tracker integration. For more information, see "Bug Tracker Integration" on page 341.
- The **Source Control** tab displays configuration settings for source control integration. For more information, see "Source Control Integration" on page 358.

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

   The application settings are saved.

Managing User Assignment to an Application

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

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

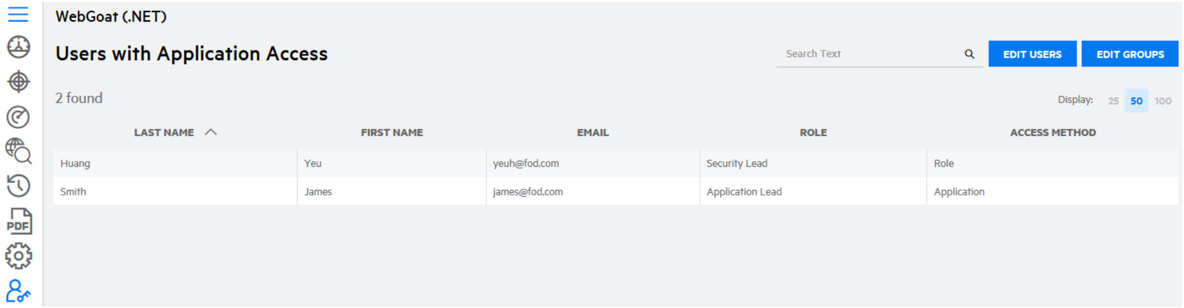
To manage user access to an application:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of application for which you want to edit user access.

   The Application Releases page appears.
3. Click **Access**.

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

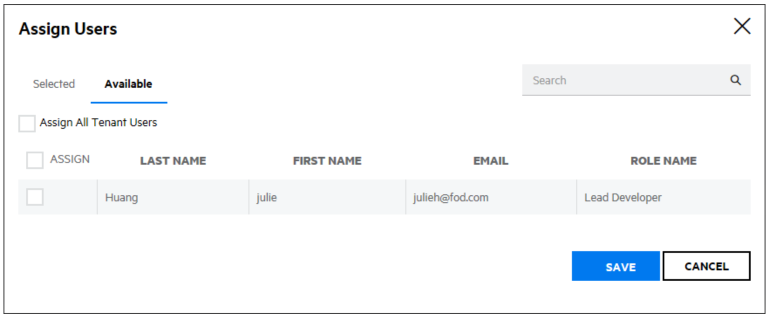
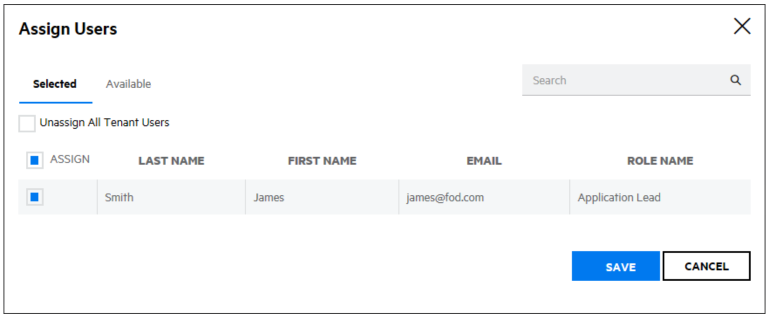


2 found

LAST NAME	FIRST NAME	EMAIL	ROLE	ACCESS METHOD
Huang	Yeu	yeuh@fod.com	Security Lead	Role
Smith	James	james@fod.com	Application Lead	Application

4. Click **Edit Users**.

   The Assign Users window appears.
5. You can perform the following tasks:

Task	Procedure
Assign users to application	a. Click **Edit Users**. The Assign Users window appears. b. Select the **Available** tab.  Assign Users Selected Available Search ☐ Assign All Tenant Users SAVE CANCEL ☐ ASSIGN — LAST NAME — FIRST NAME — EMAIL — ROLE NAME ☐ Huang — julie — julieh@fod.com — Lead Developer A list of non-Security Lead users that can be assigned to the application appears. c. 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	a. Click **Edit Users**. The Assign Users window appears. b. Select the **Selected** tab.  Assign Users Selected Available Search ☐ Unassign All Tenant Users SAVE CANCEL ☑ ASSIGN — LAST NAME — FIRST NAME — EMAIL — ROLE NAME ☑ Smith — James — james@fod.com — Application Lead A list of non-Security Lead users that are assigned to the application appears. c. Perform the following actions to remove users:

Task	Procedure
	◦ 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.

Related Topics:

To manage user access to applications at the user level, see "Managing Application Assignment to a User" on page 284.

Viewing the Application Event Log

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

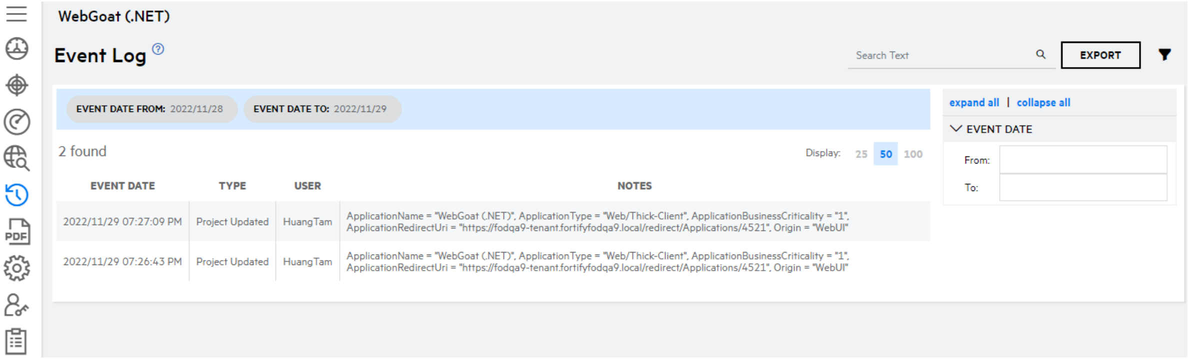
- application creation, updates, and deletion
- release creation, updates, and deletion
- addition and removal of user and group access to the application
- scan initiation, updates, and completion
- entitlement consumption
- report creation, publication, download, and deletion
- FPR downloads
- data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

To view an application's event log:

1. Select the **Applications** view.

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

   The Event Log page appears.



WebGoat (.NET)

Event Log

Search Text

EXPORT

EVENT DATE FROM: 2022/11/28 EVENT DATE TO: 2022/11/29

2 found

Display: 25 50 100

EVENT DATE	TYPE	USER	NOTES
2022/11/29 07:27:09 PM	Project Updated	HuangTam	ApplicationName = "WebGoat (.NET)", ApplicationType = "Web/Thick-Client", ApplicationBusinessCriticality = "1", ApplicationRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Applications/4521", Origin = "WebUI"
2022/11/29 07:26:43 PM	Project Updated	HuangTam	ApplicationName = "WebGoat (.NET)", ApplicationType = "Web/Thick-Client", ApplicationBusinessCriticality = "1", ApplicationRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Applications/4521", Origin = "WebUI"

expand all | collapse all

EVENT DATE

From:

To:

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 ▼.
Expand or collapse filters	Click **expand all** | **collapse all** ⚙ or the arrow next to the 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.

Related Topics

For information about viewing all events that occur in your portal, see "Viewing the Administration Event Log" on page 269.

Deleting an Application

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

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

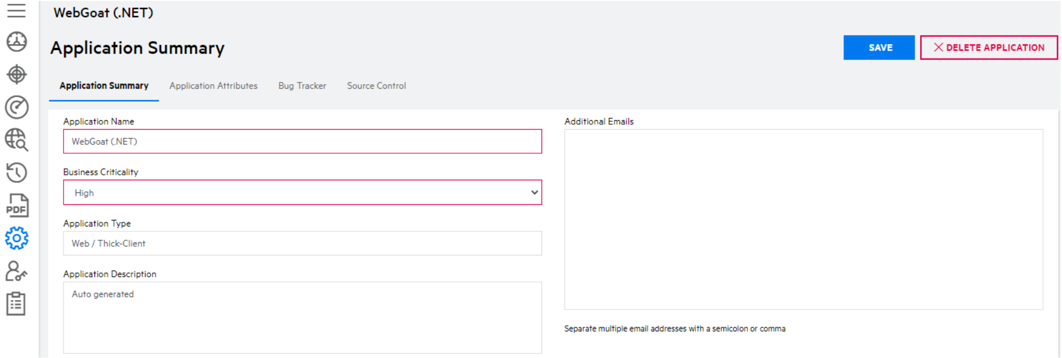
To delete an application:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click the application that you want to delete.

3. Click **Settings**.
   The **Application Summary** page appears.

   Application Name: WebGoat (.NET)

   Business Criticality: High

   Application Type: Web / Thick-Client

   Application Description: Auto generated

   Additional Emails:

   Separate multiple email addresses with a semicolon or comma

4. Click **X Delete Application** .

   A confirmation message appears.

5. Click **Yes** to delete the application.

   You are returned to Your Applications page.

Managing a Release

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

This section covers the following topics:

Creating a Release

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

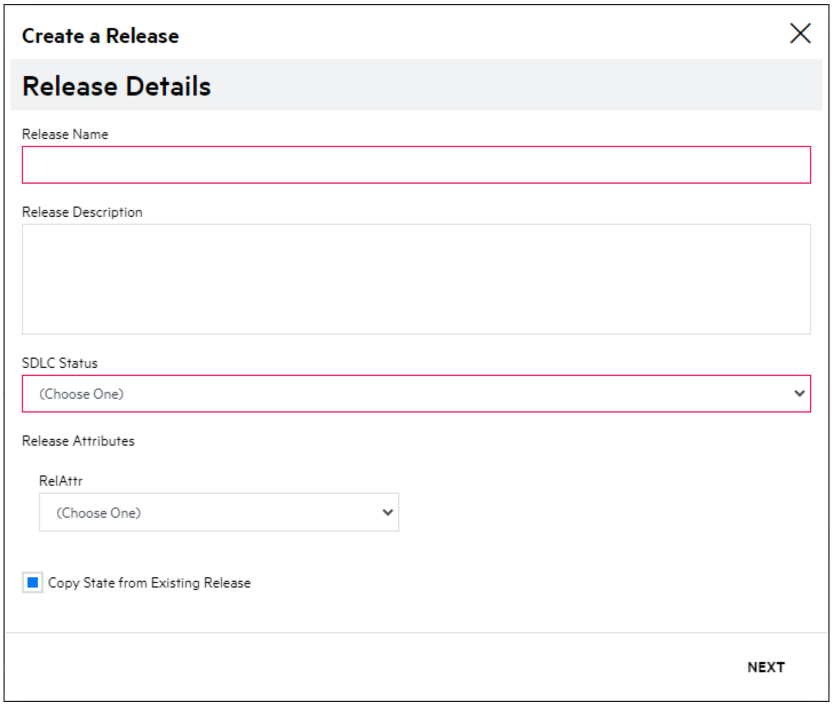
To create a new release:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click the application for which you want to create a new release.
3. Click **+ New Release**.

   The Create Release wizard appears.



Create a Release

Release Details

Release Name

Release Description

SDLC Status

(Choose One)

Release Attributes

RelAttr

(Choose One)

☑ Copy State from Existing Release

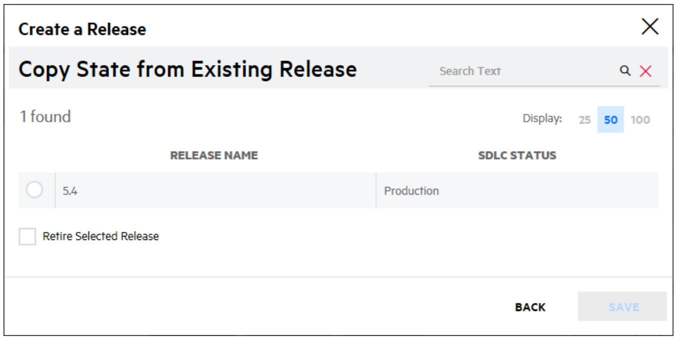
NEXT

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

Field	Description
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

Field	Description
Release Name	Type the name of your 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.



	RELEASE NAME	SDLC STATUS
○	5.4	Production

□ Retire Selected Release

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.

Viewing Release Details

The Release Overview page displays an overview of the release. It serves as a dashboard for the release, offering a quick yet comprehensive snapshot of the release's security risk. Through a series of easy-to-read visuals, you can see all the key metrics of your release. Many of the visual elements are clickable so that you can drill down into the data sets displayed.

To view details of a release:

1. Select the **Applications** view.

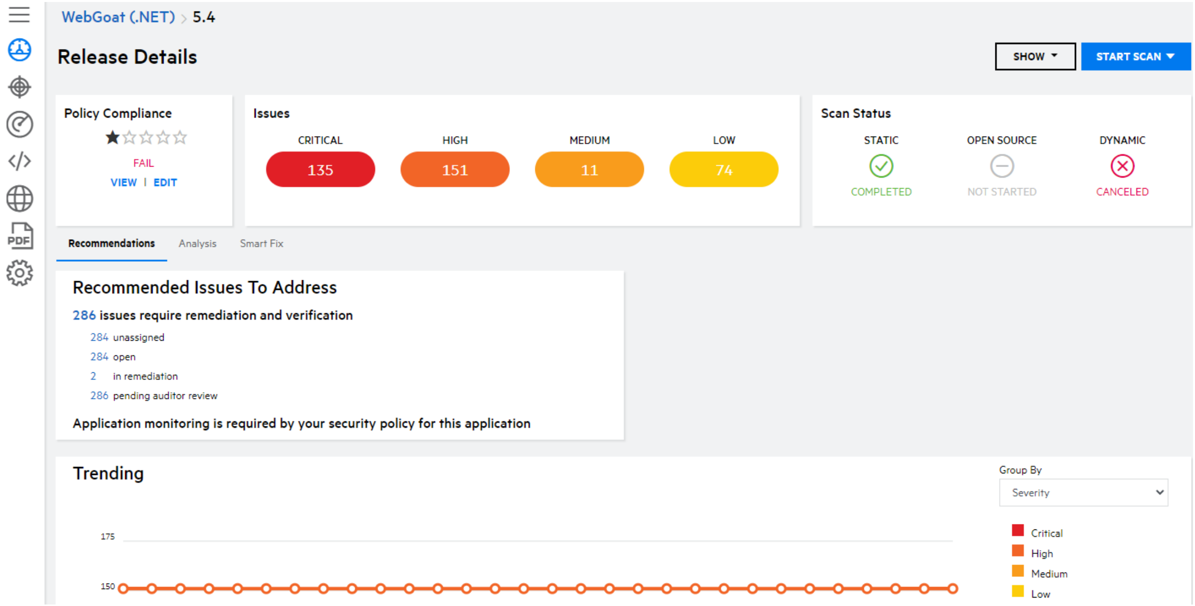
   Your Applications page appears.

2. Click **Your Releases**.

   Your Releases page appears.

3. Click the name of the release that you want to view.

   The Release Overview page appears.



WebGoat (.NET) > 5.4

Release Details

Policy Compliance ★☆☆☆☆ FAIL VIEW | EDIT

Issues

CRITICAL	HIGH	MEDIUM	LOW
135	151	11	74

Scan Status

STATIC	OPEN SOURCE	DYNAMIC
COMPLETED	NOT STARTED	CANCELED

Recommended Issues To Address

286 issues require remediation and verification

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

Application monitoring is required by your security policy for this application

Trending

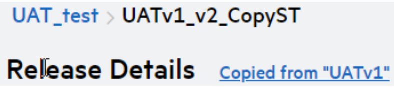
Group By: Severity

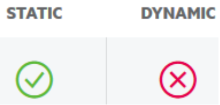
The top section of the Release Overview page summarizes all scan results for the release. The Policy Compliance box shows the Star Rating and Pass/Fail status. The Issues box shows the number of vulnerabilities at each severity level. The Scan Status box shows the most recent scan statuses for the release.

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

Navigating the Release Overview Page

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

Task	Action
View the copy state source (if applicable)	Click the link below the release name.  UAT_test > UATv1_v2_CopyST Release Details Copied from "UATv1"
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 Suppressed issues.

Task	Action
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 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."
View the security policy applied to the parent application	Click **View** in the Policy Compliance box.
Override the policy compliance	Click **Edit** in the Policy Compliance box.
View an analysis of scan results	Select a tab below the overview boxes. For more information, see "Release Overview Graphs" below
View issues filtered by issue severity or scan type	Click the links in the Issue and Scan Status boxes.

Release Overview Graphs

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

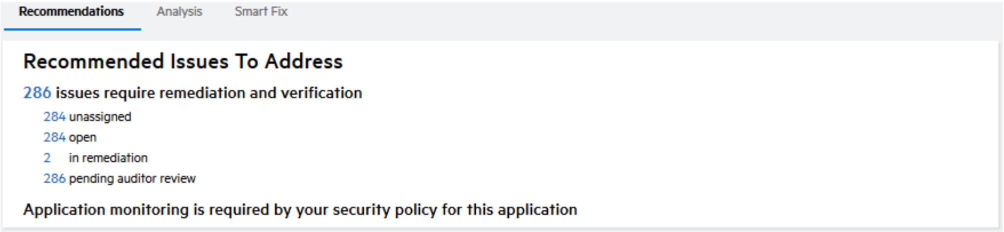
- "Recommendations" on the next page
- "Analysis" on page 63
- "Smart Fix (static scans)" on page 64

- "App Information (mobile scans)" on page 65
- "Reputation (mobile scans)" on page 65

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

Recommendations

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



Recommendations | Analysis | Smart Fix

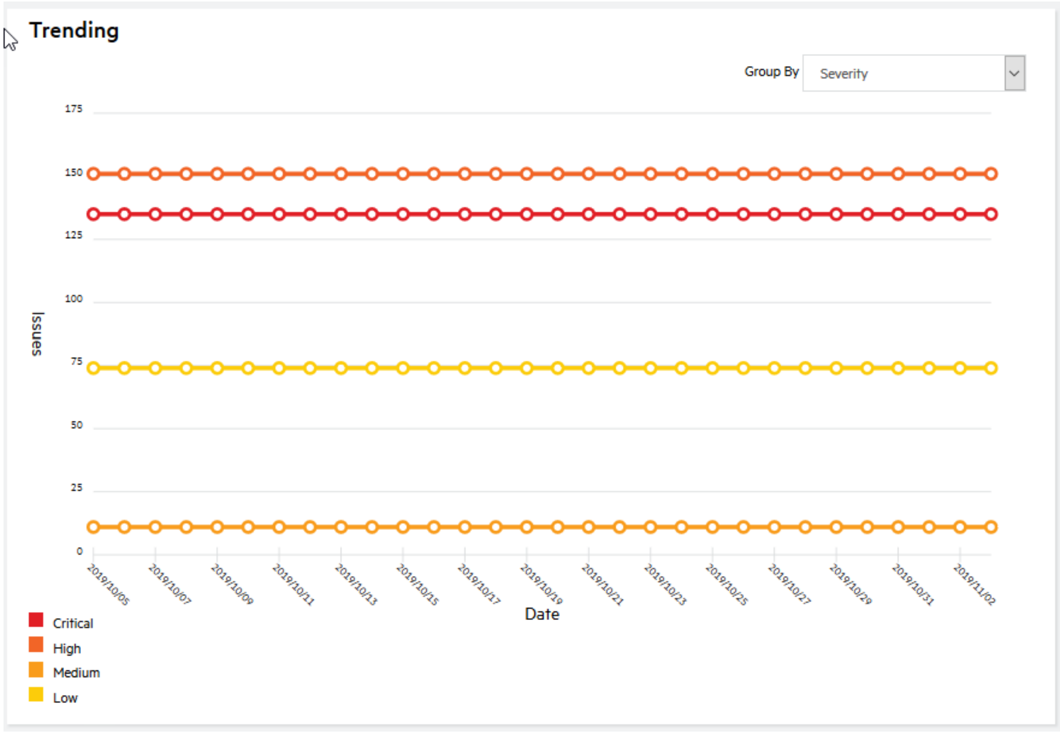
Recommended Issues To Address

286 issues require remediation and verification

284 unassigned
284 open
2 in remediation
286 pending auditor review

Application monitoring is required by your security policy for this application

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

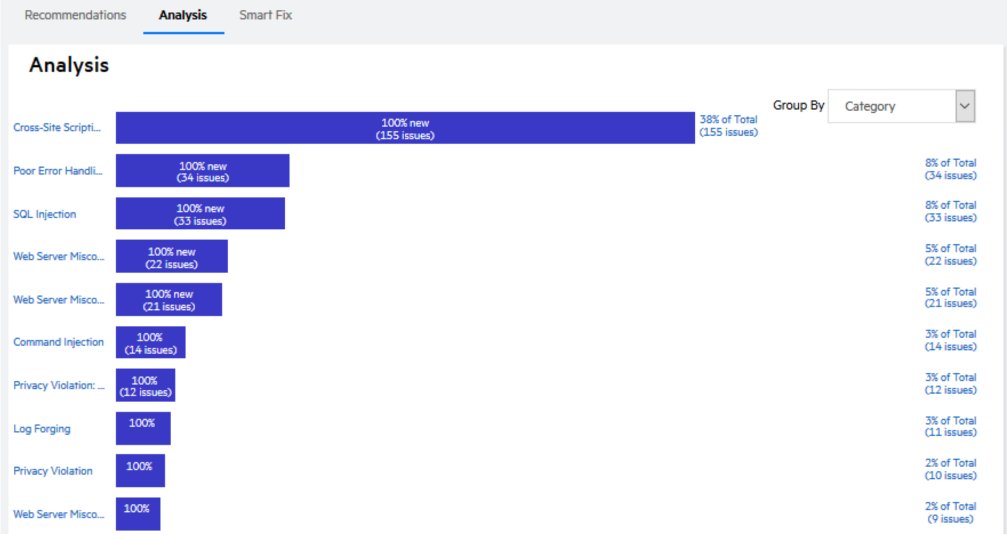


Facet	Description
Auditor Status	Auditor status of issues
Developer Status	Developer status of issues
Is Assigned	Assignment status of issues: **False**, **True**
Issue Status	Issue status: **New**, **Existing**, **Reopen**, and **Fixed**
Issue Suppressed	Suppression status of issues: **False**, **True**
Kingdom	Seven Pernicious Kingdoms classification
Severity	Issue severity: **Critical**, **High**, **Medium**, **Low**
OWASP 2017	OWASP Top 10 2017 classification
OWASP 2021	OWASP Top 10 2021 classification
OWASP ASVS 4.0	OWASP ASVS 4.0 classification
GDPR	GDPR classification from Fortify Software Security Research (SSR)
PCI 3.2	PCI 3.2 classification
PCI40	PCI 4.0 classification
PCISSF12	PCI SSF version 1.2
STIG52	DISA STIG 1.2 classification
FISMA	FISMA classification
Is Closed	Resolution status of issues: **False**, **True**
OWASP Mobile Top 10	OWASP Mobile Top 10 classification
Scan Type	Issue scan type: **Static**, **Dynamic**, **Mobile**

Analysis

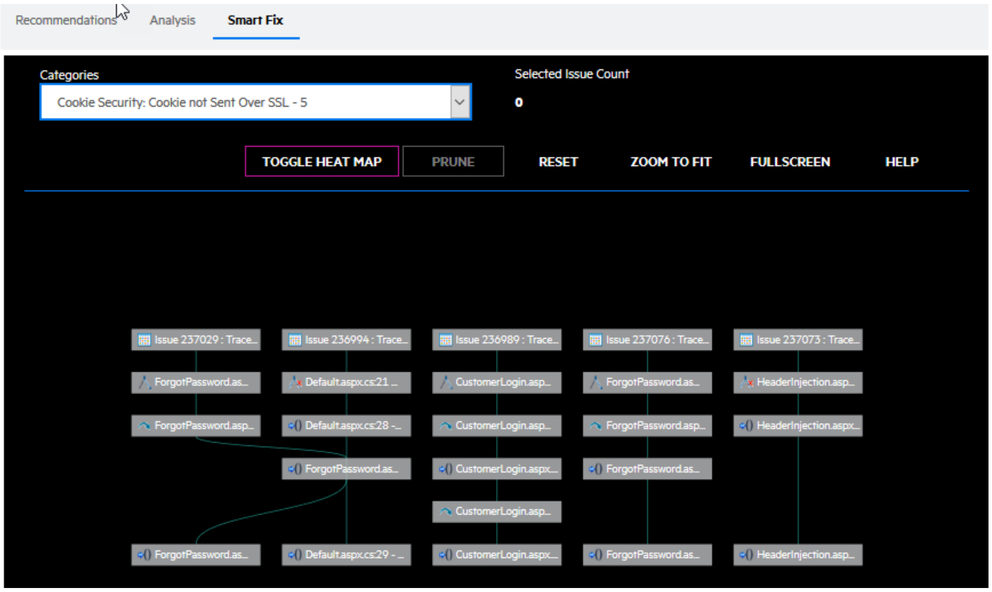
The **Analysis** tab displays a bar graph of the release's vulnerabilities divided into groups. The categories displayed depend on the Aggregation facet selected: **Assignment**, **Auditor status**, **Category**, **Developer Status**, **Scan Type**, and **OWASP 13**.

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



Smart Fix (static scans)

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

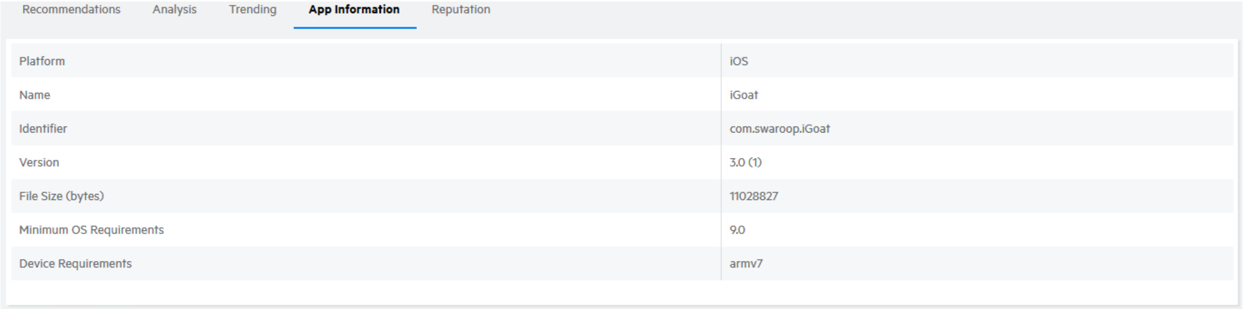


Select a vulnerability category in the **Categories** list to view its analysis trace diagram. You can interact with the diagram in the following ways:

- Scroll up and down to zoom in and out, respectively.
- Click a node to highlight shared paths.
- Click an issue icon to drill down into the issue.
- Manipulate the diagram using the toolbar commands:
  - **Toggle Heat Map**: enables / disables highlighting of data flows
  - **Prune** (available when a node is selected): narrows the diagram to the combined data flow of the selected issues
  - **Reset**: resets the diagram to the default view of the selected issue category
  - **Zoom To Fit**: resizes the entire diagram to fit in the display without resetting or pruning
  - **Full Screen**: expands the diagram in full screen mode

App Information (mobile scans)

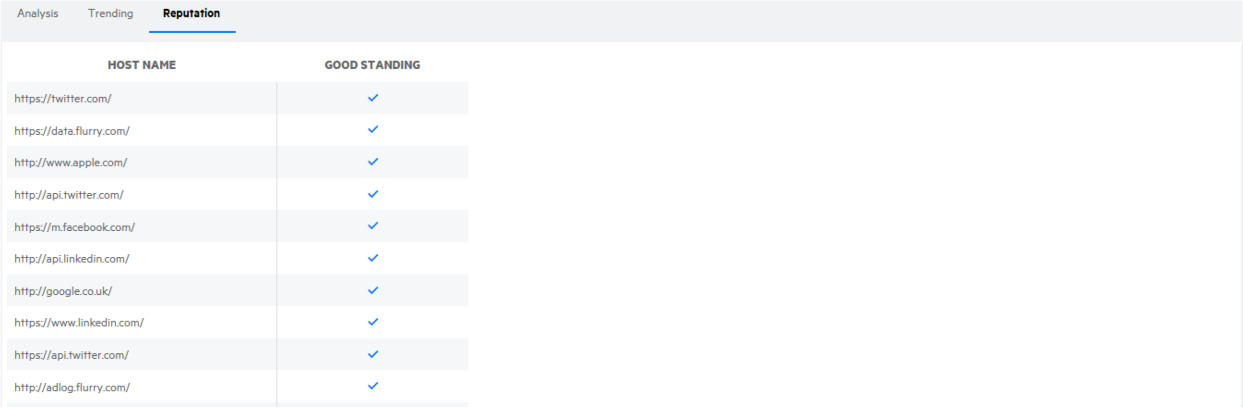
The **App Information** tab displays the following information about a mobile application's binary file: the platform, application name, identifier (package name), version, file size, minimum OS requirements, and device requirements.



Platform	iOS
Name	iGoat
Identifier	com.swaroop.iGoat
Version	3.0 (1)
File Size (bytes)	11028827
Minimum OS Requirements	9.0
Device Requirements	armv7

Reputation (mobile scans)

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



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

Overriding the Security Policy of a Release

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

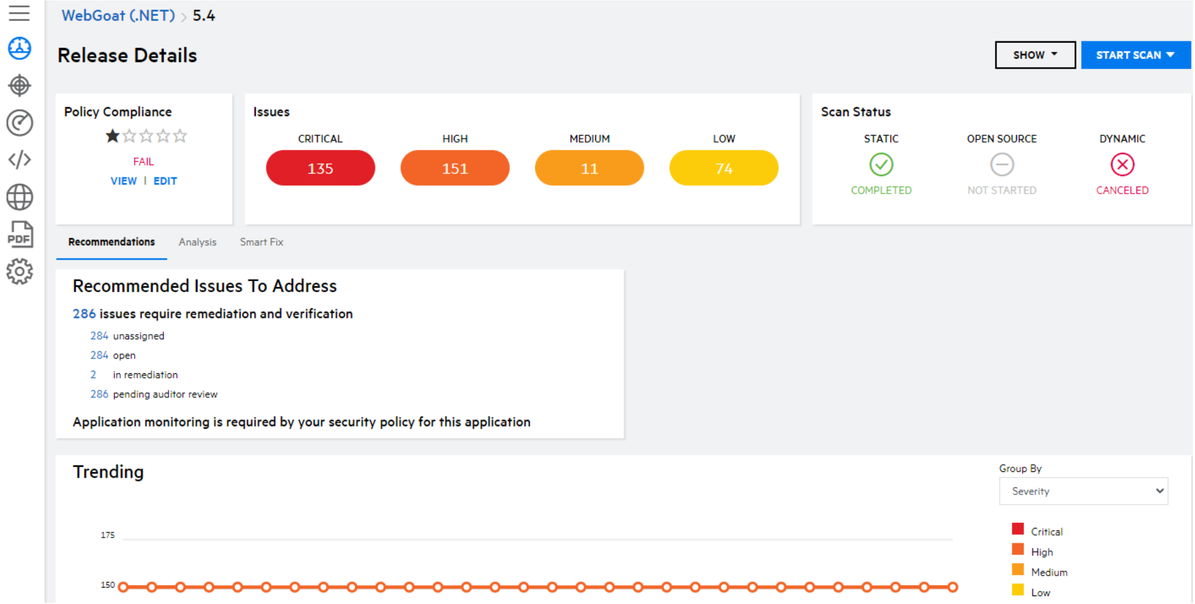
To override the security policy of a release:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of the application containing the release you want to edit.

   The Application Overview page appears.
3. Click the name of the release for which you want to override the security policy.

   The Release Overview page appears.



Recommended Issues To Address

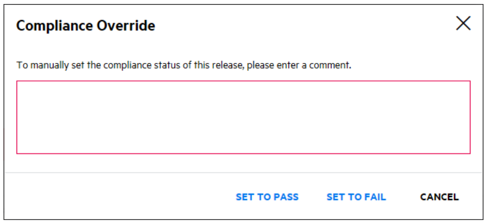
286 issues require remediation and verification

284 unassigned
284 open
2 in remediation
286 pending auditor review

Application monitoring is required by your security policy for this application

4. Click **EDIT** in the Policy Compliance box.

   The Compliance Override modal window appears.
5. Type the justification for changing the policy compliance results in the field.



To manually set the compliance status of this release, please enter a comment.

6. Click **Set to Pass** or **Set to Fail**.

   You are returned to the Release Overview page. Your policy override is displayed in the Policy Compliance box.

Related Topics:

- For information on Star Ratings, see"Five-Star Assessment Rating" on page 20.
- For information on managing security policies, see "Policy Management" on page 294.

Editing Release Settings

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

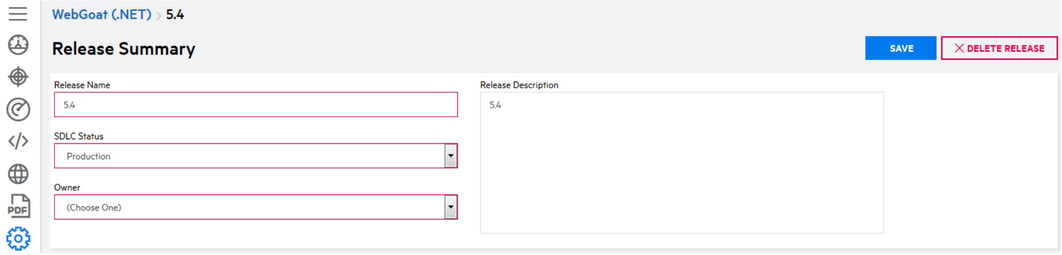
To edit the release settings:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **Your Releases**.

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

   The Release Summary page appears.



Release Name
5.4

SDLC Status
Production

Owner
(Choose One)

Release Description
5.4

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 Debricked. The setting cannot be reverted once it has been saved. The tenant must have active Debricked entitlements to successfully run Debricked scans after the switch. **Note:** If your tenant has inactive Sonatype entitlements and active Debricked entitlements, this option does not apply; open source are always powered by Debricked.
Release Description	(Optional) Description of the release that helps describe the release.

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

Deleting a Release

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

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

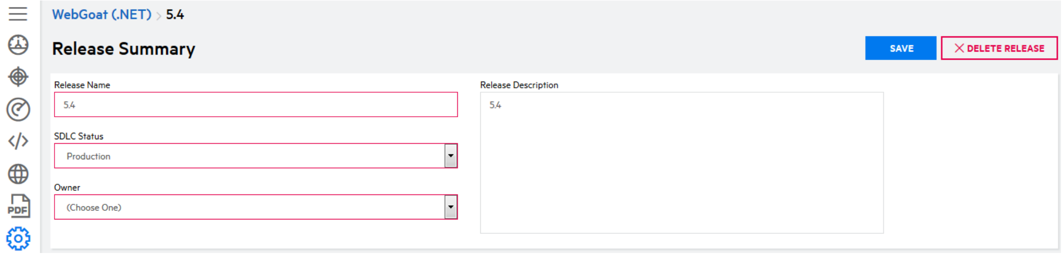
To delete a release:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears, displaying a list of your releases.

3. Click the release that you want to delete.
4. Click **Settings**.
5. Click **x Delete Release**.



WebGoat (.NET) > 5.4

Release Summary

Release Name: 5.4

SDLC Status: Production

Owner: (Choose One)

Release Description: 5.4

6. Click **Yes**.

   You are returned to the Release Overview page.

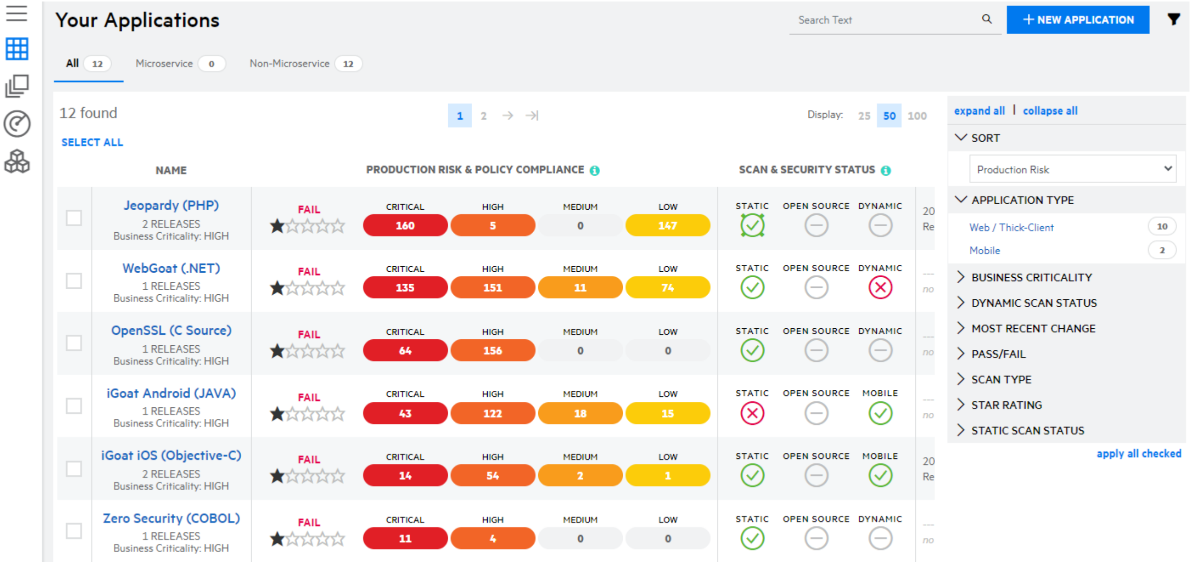
Viewing Applications in the Tenant

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

To view Your Applications page:

1. Select the **Applications** view.

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



Your Applications

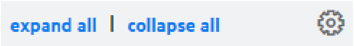
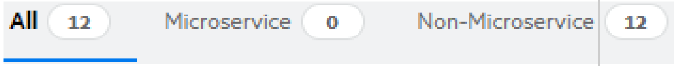
All 12 | Microservice 0 | Non-Microservice 12

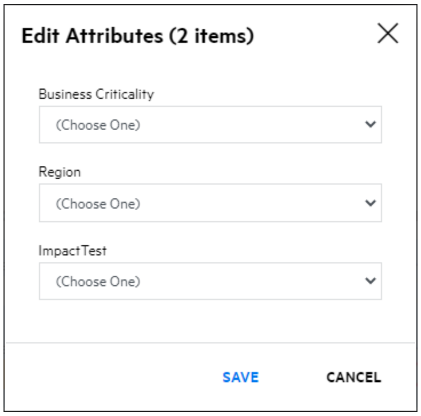
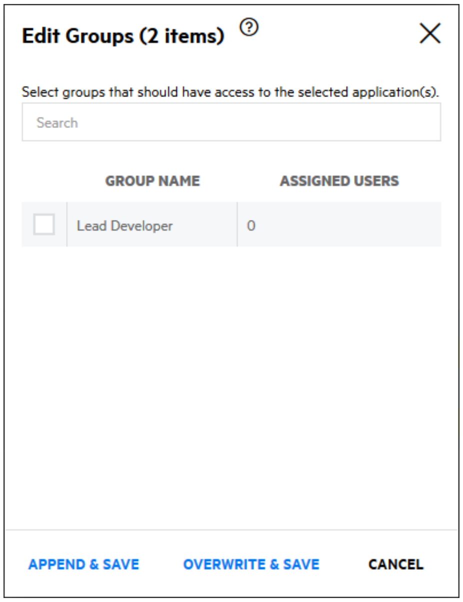
12 found

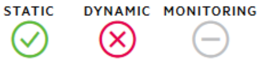
NAME	PRODUCTION RISK & POLICY COMPLIANCE					SCAN & SECURITY STATUS			
		CRITICAL	HIGH	MEDIUM	LOW	STATIC	OPEN SOURCE	DYNAMIC / MOBILE	
□ Jeopardy (PHP) 2 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆	160	5	0	147	✓	⊖	DYNAMIC ⊖	20 Re
□ WebGoat (.NET) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆	135	151	11	74	✓	⊖	DYNAMIC ✗	--- no
□ OpenSSL (C Source) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆	64	156	0	0	✓	⊖	DYNAMIC ⊖	--- no
□ iGoat Android (JAVA) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆	43	122	18	15	✗	⊖	MOBILE ✓	--- no
□ iGoat iOS (Objective-C) 2 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆	14	54	2	1	✓	⊖	MOBILE ✓	20 Re
□ Zero Security (COBOL) 1 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆	11	4	0	0	✓	⊖	DYNAMIC ⊖	--- no

Navigating Your Applications 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 text from the search box and click **Enter** or remove the applied filter. For information on using the search text box, see "Searching Applications and Releases" on page 79.
Hide or display filter lists	Click ▼.
Expand or collapse filters	Click  expand all | collapse all or the arrow next to the filter name.
Remove applied filters	Click **X** or click **Clear Filters** at the top of the page.
Filter applications by microservice designation	Select the desired tab.  All 12 Microservice 0 Non-Microservice 12
Edit application attributes for multiple applications	1. Select the check box next to individual applications or click **select all** to select all applications on the page. 2. Click **Edit Attributes**. The Edit Attribute window opens.

Task	Action
	 Edit Attributes (2 items) Business Criticality: (Choose One) Region: (Choose One) ImpactTest: (Choose One) 3. Update the fields as needed. 4. Click **Save**. For more information on application attributes, see "Creating an Application" on page 41
Edit user groups for multiple applications	1. Select the check box next to individual applications or click **select all** to select all applications on the page. 2. Click **Edit Groups**. The Edit Groups window opens.  Edit Groups (2 items) Select groups that should have access to the selected application(s). Search GROUP NAME | ASSIGNED USERS □ Lead Developer | 0 3. Select the groups that will be assigned to the applications.

Task	Action
	4. Click **Append & Save** to add the selected groups to the existing assigned groups, or click **Overwrite & Save** to replace the existing assigned groups with the selected groups (if no user groups are selected, all existing assigned groups are removed). **Note:** Users must have both **Manage Applications** and **All Application Access** permissions to use **Overwrite & Save**. For more information on groups, see "Groups" on page 287.
View details of an application	Click the application name.
View the security policy applied to an application	Click the star rating.
View combined metrics across an application's production releases	The **Production Risk & Policy Compliance** column displays the combined star rating and number of issues (including Application Monitoring issues) across an application's production releases.
View the most recent scan status across an application's releases	Hover over the relevant status icon. Click it to directly access the scan status details.  - Scheduled scans display the scheduled start date. - The expected completion date is calculated based on the scan start date + SLO of the chosen assessment type + pause time + weekends. In the event that a scan is past the SLO, the expected completion date displays "Long running scan. Contact us for details."

Task	Action
View the most recent risk-relevant change for an application.	The **Most Recent Change** column displays the most recent change from the following list: • Risk profile updated • Release created • Release deployed to production • New Application Monitoring vulnerabilities detected • New dynamic vulnerabilities detected • New static vulnerabilities detected • New mobile vulnerabilities detected • Business criticality updated • Release passing security policy • Release failing security policy

Filtering Your Applications Page

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

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

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

To filter Your Applications page:

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

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

Filter	Description	Values
Application Monitoring	Application Monitoring status of an application	Enabled (No issues), Enabled (Issues found), Not Enabled
Application Type	The application type, selected during the application creation process	Mobile, Web/Thick-Client
Business Criticality	Business Criticality of an application	High, Medium, Low
Has Microservices	Whether the application has microservices	false, true
Dynamic Scan Status	Status of dynamic scans	Scheduled, In Progress, Completed, Canceled, Waiting
Mobile Scan Status	Status of mobile scans	Scheduled, In Progress, Completed, Canceled, Waiting
Most Recent Change	Category of the most recent change detected for an application	New Monitoring Vulnerabilities Detected, Release Passing Security Policy, Business Criticality Updated, Release Created, New Dynamic Vulnerabilities Detected, Release Failing Security Policy
Pass/Fail	User-defined Pass/Fail rating	Fail, Pass, Unassessed
Scan Type	Scan type	Static, Dynamic, Mobile, Open Source
Star Rating	5-star rating system	1, 2, 3, 4, 5
Static Scan Status	Status of static scans	In Progress, Completed, Canceled, Waiting
<Custom application	Application attributes that are	User-defined

Filter	Description	Values
attribute>	picklists	
<Custom microservice attribute>	Microservice attributes that are picklists	User-defined

4. Select your desired filter values.

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

Viewing Releases in the Tenant

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

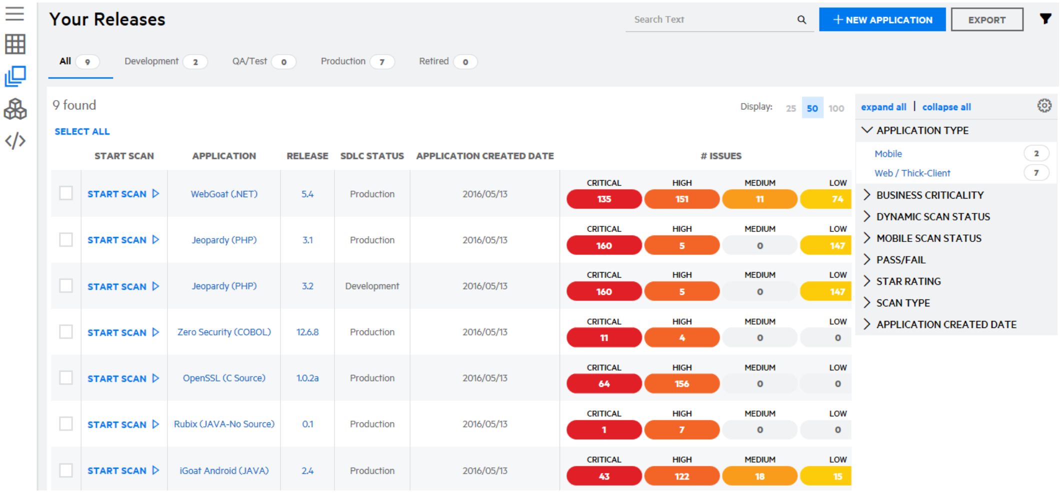
To view Your Releases page:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click **Your Releases**.

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



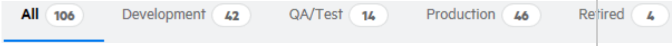
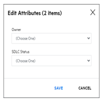
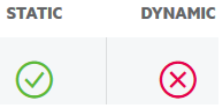
	START SCAN	APPLICATION	RELEASE	SDLC STATUS	APPLICATION CREATED DATE	# ISSUES			
						CRITICAL	HIGH	MEDIUM	LOW
□	START SCAN ▷	WebGoat (.NET)	5.4	Production	2016/05/13	135	151	11	74
□	START SCAN ▷	Jeopardy (PHP)	3.1	Production	2016/05/13	160	5	0	147
□	START SCAN ▷	Jeopardy (PHP)	3.2	Development	2016/05/13	160	5	0	147
□	START SCAN ▷	Zero Security (COBOL)	12.6.8	Production	2016/05/13	11	4	0	0
□	START SCAN ▷	OpenSSL (C Source)	1.0.2a	Production	2016/05/13	64	156	0	0
□	START SCAN ▷	Rubix (JAVA-No Source)	0.1	Production	2016/05/13	1	7	0	0
□	START SCAN ▷	iGoat Android (JAVA)	2.4	Production	2016/05/13	43	122	18	15

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

Navigating Your Releases Page

The following table describes how to navigate Your Releases page.

Task	Action
Create an application	Click **+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 text from the search box and click **Enter** or remove the applied filter. For information, see "Searching Applications and Releases" on page 79.
Export data as a .csv file	Click **Export**. A .csv file containing detailed information on all vulnerabilities is saved locally to a folder specified in your browser settings. **Note**: The Export functionalities in the Tenant Dashboard, Your Releases, and Release Issues pages outputs the same column fields. Currently applied filters are also applied to the export.
Change the grid columns	1. Click ⚙. 2. Use the check boxes to make your selections. 3. Click **Save**.
Hide or display the filter list	Click ▼.
Expand or collapse filters	Click expand all | collapse all ⚙ or the arrow next to the filter name.
Remove applied filters	Click **X** or click **Clear Filters** at the top of the page.
Filter releases by SDLC status	Select a tab corresponding to an SDLC status. The selected SDLC status is preserved when

Task	Action
	moving between views.  All 106 Development 42 QA/Test 14 Production 46 Retired 4
Sort the release list by column	Click a column header. The arrow next to the header indicates the sort order of the data. To reverse the order, click the header again.
Edit release attributes for multiple releases	1. Select the check box next to individual releases or click **select all** to select all releases on the page. 2. Click **Edit Attributes**. The Edit Attribute window opens.  Edit Attributes (2 items) Owner (Choose One) SDLC Status (Choose One) SAVE CANCEL 3. Update the fields as needed. 4. Click **Save**. For more information on release attributes, see "Creating a Release" on page 57
Start a scan	Click **Start Scan** and select the scan type.
View additional details of an application or release	Click an application or release name.
View the most recent scan status for a release	Hover over a 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

Task	Action
	expected completion date displays "Long running scan on <release>. Contact us for details."
View the security policy applied to a release's parent application	Click a star rating.

Filtering Your Releases Page

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

To filter Your Releases page:

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

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

Filter	Definition	Values
Application Created Date	Date when the application was created.	< 7 days, < 30 days, < 90 days, < 180 days
Application Type	The application type, selected during the application creation process	Mobile, Web/Thick-Client
Business Criticality	Criticality of the applications	High, Medium, Low
Dynamic Scan Status	Status of dynamic scans	Not Started, Canceled, Completed, In Progress, Waiting
MicroserviceName	Microservice names	User-defined
Mobile Scan Status	Status of mobile scans	Not Started, Canceled, Completed, In Progress, Waiting
Pass/Fail	User-defined Pass/Fail rating	Fail, Pass
Scan Type	Scan type	Static, Dynamic, Mobile

Filter	Definition	Values
SDLC Status	SDLC status of releases	Production, QA/Testm Development, Retired
Star Rating	5-star rating system	1, 2, 3, 4, 5
Static Scan Status	Status of static scans	In Progress, Completed, Canceled, Waiting
<Custom release attribute>	Release attributes that are picklists	User-defined

3. Select your desired filter values.

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

Searching Applications and Releases

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

Searching Text

To search for an application or release in a grid:

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

   Search Text

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

   - If you type **Test** in the box, your search results **will** include *Test App 1*.
   - If you type **Tes** in the box, your search results **will not** include *Test App 1*.
   - If you type **Tes*** in the box, your search results **will** include *Test App 1*.

2. Click **Enter**.

   The page refreshes with your search results.

3. Click the name of the desired application or release. The page refreshes with the selected application or release page and clears the search box.

Removing the Search Results

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

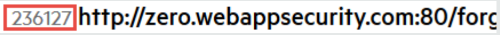
- Remove the search string from the search box.
- Click the browser **Back** arrow.

Creating Deep Links

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

To create deep links, use the following path formats:

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

> **Note:** The top of the issue details panel displays the issue ID.
>
> 
>
> 236127 **http://zero.webappsecurity.com:80/forg**

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

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

Chapter 4: Running Assessments

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

This section contains the following topics:

Static Assessments

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

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

This section contains the following topics:

Supported Languages

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

Language / Framework	Versions
.NET	5.0, 6.0, 7.0, 8.0
.NET Core	2.0–3.1
.NET Framework	2.0–4.8
ABAP/BSP	6
ActionScript	3.0
Apex	55–58
Bicep	0.12.x–0.15.x
C#	5, 6, 7, 8, 9, 10, 11, 12
C	C11, C17 (see "Supported Compilers" on page 84)
C++	C++11, C++14, C++17, C++20 (see "Supported Compilers" on page 84)
Classic ASP (with VBScript)	2.0, 3.0
COBOL	IBM Enterprise COBOL for z/OS 6.1 (or earlier), 6.2, and 6.3 with CICS, IMS, DB2, and IBM MQ Visual COBOL 6.0, 7.0, 8.0
ColdFusion	8, 9, 10
Dart	2.x (2.12 and later), 3.0
Docker (Dockerfiles)	any
Flutter	2.0–3.3
Go	1.12–1.20 **Note:** Fortify Static Code Analyzer supports analyzing Go code on

Language / Framework	**Versions**
	Windows and Linux.
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)	7–17
JavaScript	ECMAScript 2015–2023
JSON	ECMA-404
JSP	1.2, 2.1
Kotlin	1.3–1.8
MXML (Flex)	4
Objective-C/C++	2.0 (see "Supported Compilers" on the next page)
PHP	7.3, 7.4, 8.0, 8.1, 8.2
PL/SQL	8.1.6
Python	2.6, 2.7, 3.0–3.12
Ruby	1.9.3
Scala	2.11, 2.12, 2.13
Solidity	0.4.12–0.8.21
Swift	5–5.9 (see "Supported Compilers" on the next page for supported swiftc versions)
T-SQL	SQL Server 2005, 2008, 2012
TypeScript	2.8, 3.x, 4.x, 5.0

Language / Framework	Versions
VBScript	2.0, 5.0
Visual Basic (VB.NET)	11, 14, 15.x, 16.0
Visual Basic	6.0
XML	1.0
YAML	1.2

Supported Compilers

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

Compiler	Versions	Operating Systems
gcc	GNU gcc 6.x–10.4, 11	Windows, Linux, macOS
	GNU gcc 4.9, 5.x	Windows, Linux, macOS, AIX
g++	GNU g++ 6.x–10.4, 11	Windows, Linux, macOS
	GNU g++ 4.9, 5.x	Windows, Linux, macOS, AIX
OpenJDK javac	9, 10, 11, 12, 13, 14, 17	Windows, Linux, macOS, AIX
Oracle javac	7, 8, 9	Windows, Linux, macOS
cl (MSVC)	2015, 2017, 2019, 2022	Windows
Clang	14.0.0, 14.0.3, 15.0.0	macOS
Swiftc	5.7, 5.7.1, 5.8, 5.8.1, 5.9[1]	macOS

[1] Fortify Static Code Analyzer supports applications built in the following Xcode versions: 14, 14.0.1, 14.1, 14.2, 14.3, 14.3.1, 15, 15.0.1.

Supported Libraries, Frameworks, and Technologies

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

Java

- Adobe Flex Blaze DS
- Ajanta
- Amazon Web Services (AWS) SDK
- Android
- Android Jetpack
- Apache Axiom
- Apache Axis
- Apache Beam
- Apache Beehive NetUI
- Apache Catalina
- Apache Cocoon
- Apache Commons
- Apache ECS
- Apache Hadoop
- Apache HttpComponents
- Apache Jasper
- Apache Log4j
- Apache Lucene
- Apache MyFaces
- Apache OGNL
- Apache ORO
- Apache POI
- Apache SLF4J
- Apache Slide
- Apache Spring Security (Acegi)
- Apache Struts
- Apache Tapestry
- Apache Tomcat
- Apache Torque
- Apache Util
- Apache Velocity
- Apache Wicket
- Apache Xalan
- Apache Xerces
- ATG Dynamo
- Azure SDK
- Castor
- Display Tag
- Dom4j
- GDS AntiXSS
- Google Cloud
- Google Dataflow
- Google Guava
- Google Web Toolkit
- gRPC
- Gson
- Hibernate
- iBatis
- IBM MQ
- IBM WebSphere
- Jackson
- Jakarta Activation
- Jakarta EE (Java EE)
- Jasypt
- Java Annotations
- Java Excel API
- JavaMail
- JAX-RS
- JAXB
- Jaxen
- JBoss
- JDesktop
- JDOM
- Jetty
- JGroups
- json-simple
- JTidy Servlet
- JXTA
- JYaml
- Liferay Portal
- MongoDB
- Mozilla Rhino
- MyBatis
- Netscape LDAP API
- OpenCSV
- Oracle Application Development Framework (ADF)
- Oracle BC4J
- Oracle JDBC
- Oracle OA Framework
- Oracle tcDataSet
- Oracle XML Developer Kit (XDK)
- OWASP Enterprise Security API (ESAPI)
- OWASP HTML Sanitizer
- OWASP Java Encoder
- Plexus Archiver
- Realm
- Restlet
- SAP Web Dynpro
- Saxon
- SnakeYAML
- Spring
- Spring MVC
- Spring Boot
- Spring Data Commons
- Spring Data JPA
- Spring Data MongoDB
- Spring Data Redis
- Spring HATEOAS
- Spring JMS
- Spring JMX
- Spring Messaging
- Spring Security
- Spring Webflow
- Spring WebSockets
- Spring WS
- Stripes
- Sun JavaServer Faces (JSF)
- Tungsten
- Weblogic
- WebSocket
- XStream
- YamlBeans
- ZeroTurnaround ZIP
- 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
- 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 Mcrypt
- PHP Mhash
- PHP Mysql
- PHP OCI8
- PHP OpenSSL
- PHP PostgreSQL
- PHP Reflection
- PHP SimpleXML
- PHP Smarty
- PHP XML
- PHP XMLReader
- PHP Zend

JavaScript/TypeScript/HTML5

- Angular
- Apollo Server
- Express
- GraphQL.js
- Handlebars
- Helmet
- iOS JavaScript Bridge
- jQuery
- JS-YAML
- Mustache
- Node.js Azure Storage
- Node.js Core
- React
- React Native
- React Native Async Storage
- React Router
- SAPUI5/OpenUI5
- Sequelize
- Underscore.js
- Vue

Python

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

1Password

Actually Good Encryption (AGE)

Adafruit

Adobe

Airtable

Algolia

Alibaba (Aliyun)

Amazon (AWS, MWS)

Apple (macOS)

Apache HTTP

Asana

Atlassian

Authress

Basic access authentication

bcrypt

Beamer

Bearer token

Bitbucket

Bittrex

Brevo (Sendinblue)

Clojars

Code Climate

Codecov

Coinbase

Confluent

Contentful

Databricks

Datadog

Defined

DES

DigitalOcean

Docker

Doppler

Droneci

Dropbox

Duffel

Dynatrace

EasyPost

Encryption key

Etsy

Facebook

Fastly

Finicity

Finnhub

Flickr

Flutterwave

Frame.io

Freshbooks

Git

GitHub

GitLab

Gitter

GNOME

GNU (Bash)

GoCardless

Google (API, Google Cloud, OAuth)

Grafana

HashiCorp (Terraform, Vault)

Heroku

HexChat

HubSpot

Intercom

Java

JFrog (Artifactory)

JSON Web Token

KDE Wallet (Kwallet)

KeePass

Kraken

Kucoin

LaunchDarkly

Linear

LinkedIn

Lob

Mailchimp

Mailgun

Mapbox

Mattermost

MD5

MessageBird

Microsoft (Azure App Storage, Cosmos DB, Functions and Bitlocker, PowerShell, RDP, VBScript)

Microsoft (Outlook)

Mutt

MySQL

Netlify

New Relic

npm

NuGet

Okta

OpenVPN

Password in comment

Password in connection string

Password in PowerShell script

Password in URI

Password Safe

PayPal (Braintree)

Pidgin

Plaid

Planetscale

PostgreSQL

Postman

Prefect

Pulumi

PuTTY

PyPI

RapidAPI

Readme

RSA Security

Ruby (Ruby on Rails, RubyGems)

Sauce Labs

Secret key

Secure Shell Protocol (SSH)

Sendbird

SendGrid

Sentry

SHA1

SHA256

SHA512

Shippo

Shopify

Sidekiq

Slack

SonarQube

Square

Squarespace

StackHawk

Stripe

Sumologic

Telegram

Travis

Trello

Twilio

Twitch

Twitter

Typeform

Yandex

Zendesk

Preparing 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" on page 117.

This section contains the following topics:

Static Assessment File Requirements

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

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

Installing and Using the 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 Debricked 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. 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 *Fortify Software System Requirements*
- Supported build tools: "Fortify ScanCentral SAST Sensor Languages and Build Tools" in *Fortify Software System Requirements*
- Command-line options: "Package Command Options" in *Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*

Preparing .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 (Recommmended)" below
- "Code Packaging with IDE Tools" below
- "Manual Code Packaging" on the next page

Fortify Static Code Analyzer supports scanning .NET applications on Windows system only.

> **Important!** Source code is scanned by default. Fortify 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 (Recommmended)

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

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

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

   > **Important!** The MSBuild executable must be added to the PATH environment variable. Fortify recommends running theFortify ScanCentral SAST client from the Visual Studio command prompt, which sets the required .NET variables automatically.

> **Note:** Fortify ScanCentral SAST packaging is built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see "Integrations and Tools" on page 330.

Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see "IDE Tool" on page 331.

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

Preparing Source Code Files

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

- All necessary source code files (C/C++, C#, or VB.NET)
- All required reference libraries

  This includes those from relevant frameworks, NuGet packages, and third-party libraries.
- For C/C++ projects, include all necessary header files that do not belong to the Visual Studio or MSBuild installation.
- For ASP.NET and ASP.NET Core projects, include all the necessary ASP.NET page files

  The supported ASP.NET page types are ASPX, ASCX, ASAX, ASHX, ASMX, AXML, Master, CSHTML, VBHTML, BAML, and XAML.

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, Fortify recommends that you run the `dotnet restore` command to make sure that all required reference libraries are downloaded and installed in the project. You must run this command from the top-level folder of the project.

Preparing Compiled Files (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.

Creating 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.

Preparing Java Application Files

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

- "Automated Code Packaging with Fortify ScanCentral SAST (Recommmended)" below
- "Code Packaging with IDE Tools (Recommended)" below
- "Manual Code Packaging" below

> **Important!** Source code is scanned by default. Fortify 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 (Recommmended)

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

> **Note:** Fortify ScanCentral SAST packaging is built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see "Integrations and Tools" on page 330.

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

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your Gradle or Maven project. The basic syntax is: `scancentral package -bf <build_file> -o <output_zip>`. For example, `scancentral package -bf pom.xml -o mypayload.zip`, `scancentral package -bf build.gradle -o mypayload.zip`
   For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see "Installing and Using the Fortify ScanCentral SAST Client" on page 92.

Code Packaging with IDE Tools (Recommended)

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see "IDE Tool" on page 331.

Manual Code Packaging

Manual code packaging consists of:

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

Preparing Source Code Files

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

Preparing Compiled Files

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

Creating a Zip File

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

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

Preparing JavaScript Technology/HTML/XML Files

For applications that consist of JavaScript, TypeScript, HTML, and/or XML files, package the files in a zip file. Include all production dependencies. For example, run `npm install --only=prod` if you are using npm. Upload the zip file under the **JS/TS/HTML** technology stack option. For React Native mobile app projects, upload the zip file under the **React Native** option.

If applicable, make sure to do the following:

- Include the `package.json` file.
- Provide only TypeScript source code, not transpiled TypeScript. For example, do not provide the `dist` folder generated when building an Angular project.
- Do not include minified JavaScript files of your source code, as minified code significantly diminishes the quality of scan results.

For applications that are built with different languages or technology stacks and contain Javascript, HTML, and/or XML files, package the application according to the instructions provided for the language or technology stack and simply include the JavaScript, HTML, and/or XML files in the package. JS/TS/HTML is a catch-all option for simple web applications and web applications that primarily use JavaScript-related technologies.

Preparing Kotlin Application Files

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

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

Preparing ABAP (SAP) Application Files

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

Importing the Transport Request

The Fortify ABAP Extractor is available on the Tools page in the portal (see "Viewing and Downloading Tools" on page 340. The Fortify ABAP Extractor zip file contains the following files:

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

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

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

Installation Note

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

To resolve this issue:

1. Re-run the transport request import.

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

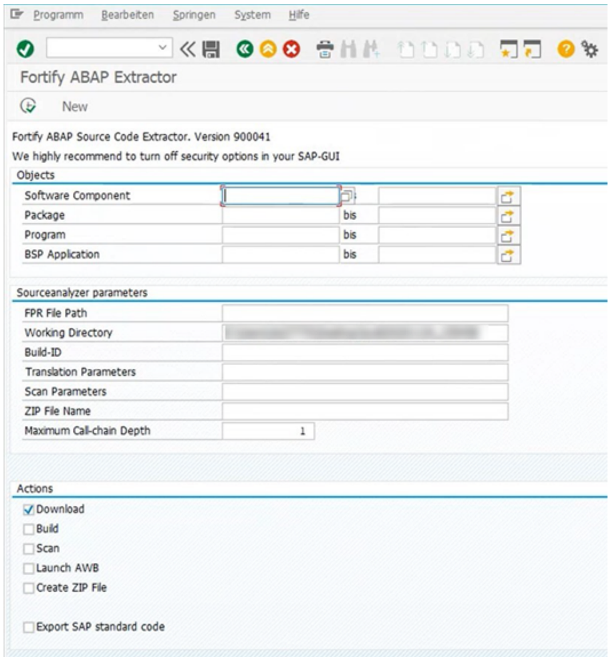
If this does not resolve the issue or if your system is running on an SAP version with a different table structure, Fortify recommends that you export your ABAP file structure using your own technology so that Fortify on Demand can scan the ABAP code.

Running the Fortify ABAP Extractor

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

To run the Fortify ABAP Extractor:

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



Fortify ABAP Source Code Extractor. Version 900041

We highly recommend to turn off security options in your SAP-GUI

Objects

Software Component			
Package		bis	
Program		bis	
BSP Application		bis	

Sourceanalyzer parameters

FPR File Path	
Working Directory	[redacted]
Build-ID	
Translation Parameters	
Scan Parameters	
ZIP File Name	
Maximum Call-chain Depth	1

Actions

☑ Download
□ Build
□ Scan
□ Launch AWB
□ Create ZIP File

□ Export SAP standard code

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

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

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

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

Field	Description
Working Directory	Type or select the directory where you want to store the extracted source code .
ZIP File Name	(Optional) Type a ZIP file name if you want your output in a compressed package.

Field	Description
Maximum Call-chain Depth	A global SAP-function F is not downloaded unless F was explicitly selected or unless F can be reached through a chain of function calls that start in explicitly-selected code and whose length is this number or less. Fortify recommends that you do not specify a value greater than 2 unless directed to do so by support.

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

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

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

5. Click **Execute**.

Fortify ABAP Extractor Notes

Because the Fortify ABAP Extractor program is executed online, you might receive a `max dialog work process time reached` exception if the volume of source files selected for extraction exceeds the allowable process run time. To work around this, download large projects as a series of smaller Extractor tasks. For example, if your project consists of four different packages, download each package separately into the same project directory. If the exception occurs frequently, work with your SAP Basis administrator to increase the maximum time limit (`rdisp/max_wprun_time`).

When a PACKAGE is extracted from ABAP, the Fortify ABAP Extractor extracts everything from `TDEVC` with a `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.

Packaging ABAP Source Code

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

Preparing C and C++ Application Files

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

Installing Fortify Static Code Analyzer

The latest version of Fortify Static Code Analyzer is available on the Tools page in the portal (see "Viewing and Downloading Tools" on page 340. You can download installers for Windows, macOS, and Linux operating systems. A valid license file is required to translate source code. Contact support to be issued a license, which will be available from the Tools page.

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

Translating Code

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

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

   where `<build_command>` is your build script.

   Example:

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

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

Packaging Translated Code

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

To generate and package an MBS file:

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

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

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

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

Preparing Classic ASP, VBScript, and Visual Basic Application Files

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

Preparing 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

Preparing COBOL Application Files

For COBOL applications, package the COBOL source code, the copybook files that the COBOL source code uses, and the SQL INCLUDE files that the COBOL source code references in one zip file. Copybook and SQL INCLUDE files must retain the names used in the COBOL source code `COPY` statements.

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

Zip file

- `sources/` folder
- `copybooks/` folder

Preparing ColdFusion Markup Language (CFML) Application Files

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

Preparing Dockerfiles and Infrastructure as Code (IaC) Files

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

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

Note:

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

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

Preparing Go Application Files

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

- "Automated Code Packaging with Fortify ScanCentral SAST (Recommmended)" on the next page
- "Code Packaging with IDE Tools" on the next page
- "Manual Code Packaging" on the next page

Automated Code Packaging with Fortify ScanCentral SAST (Recommmended)

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

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

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your Go project. The basic syntax is: `scancentral package -o <output_zip>`. For example, `scancentral package -o mypayload.zip`
   For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see "Installing and Using the Fortify ScanCentral SAST Client" on page 92.

> **Note:** Fortify ScanCentral SAST packaging is built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see "Integrations and Tools" on page 330.

Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see "IDE Tool" on page 331.

Manual Code Packaging

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

The following dependency management systems built into Go are supported:

- Go modules (recommended)

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

> **Note:** The following entities are excluded from scanning:
>
> - Vendor folder
> - All projects defined by any `go.mod` files in subfolders
> - All files with the `_test.go` suffix (unit tests)

Preparing PHP Application Files

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

- "Automated Code Packaging with Fortify ScanCentral SAST (Recommmended)" below
- "Code Packaging with IDE Tools" below
- "Manual Code Packaging" below

Automated Code Packaging with Fortify ScanCentral SAST (Recommmended)

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

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

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your PHP project. The basic syntax is: `scancentral package -hv <version> -o <output_zip>`. For example,
   `scancentral package -hv 7.1 -o mypayload.zip`
   For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see "Installing and Using the Fortify ScanCentral SAST Client" on page 92.

> **Note:** Fortify ScanCentral SAST packaging is built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see "Integrations and Tools" on page 330.

Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see "IDE Tool" on page 331.

Manual Code Packaging

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

Preparing Python Application Files

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

- "Automated Code Packaging with Fortify ScanCentral SAST (Recommmended)" on the next page

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

- "Code Packaging with IDE Tools" on the next page
- "Manual Code Packaging" on the next page

Automated Code Packaging with Fortify ScanCentral SAST (Recommmended)

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

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

1. Download the Fortify ScanCentral SAST client from the Tools page.
2. Install the Fortify ScanCentral SAST client on the build machine. Installation instructions are available in the README.txt file stored in the zip file.
3. In a command-line interface, run `scancentral.bat` to package your Python project. The basic syntax is: `scancentral package –o <output_zip>`. For example, `scancentral package –o mypayload.zip`
   For more information on using Fortify ScanCentral SAST, including additional command-line arguments, see "Installing and Using the Fortify ScanCentral SAST Client" on page 92.

> **Note:** Fortify ScanCentral SAST packaging is built in to the Fortify Extension for Visual Studio Code, Visual Studio Extension, Fortify Azure DevOps Extension, and Fortify on Demand Jenkins Plugin. For more information on using these tools, see "Integrations and Tools" on page 330.

Code Packaging with IDE Tools

The IDE plugins enable selection of project files and necessary dependencies for packaging. For more information on using IDE tools, see "IDE Tool" on page 331.

Manual Code Packaging

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

> **Note:** If your application uses a version of Python not listed in "Supported Languages" on page 82, contact support to discuss your options.

Preparing Ruby Application Files

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

Preparing Solidity Application Files

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

Fortify Static Code Analyzer 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.

Preparing 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.

Preparing Scala Application Files

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

Installing Fortify Static Code Analyzer

The latest version of Fortify Static Code Analyzer is available on the Tools page in the portal (see "Viewing and Downloading Tools" on page 340. You can download installers for Windows, macOS, and Linux operating systems. A valid license file is required to translate source code. Contact support to be issued a license, which will be available from the Tools page.

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

Translating Code

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

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

Packaging Translated Code

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

To generate and package an MBS file:

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

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

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

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

Preparing Android Application Files (Source Code)

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

Note: Fortify Static Code Analyzer supports Xamarin. For instructions on preparing Xamarin application files, see "Preparing .NET Application Files" on page 93. Other third-party development libraries such as Cordova, Ionic Framework, PhoneGap, and Unity are not supported.

Related Topics:

For information on preparing Android binary files for mobile assessments, see "Preparing Android Application Files (Binary)" on page 155.

Preparing iOS Application Files (Source Code)

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

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

Package the source code files in one zip file.

> **Note:** Fortify Static Code Analyzer supports Xamarin. For instructions on preparing Xamarin application files, see "Preparing .NET Application Files" on page 93. Other third-party development libraries such as Cordova, Ionic Framework, PhoneGap, and Unity are not supported.

Related Topics:

For information on preparing iOS binary files for mobile assessments, see "Preparing iOS Application Files (Binary)" on page 156

Configuring a Static Scan

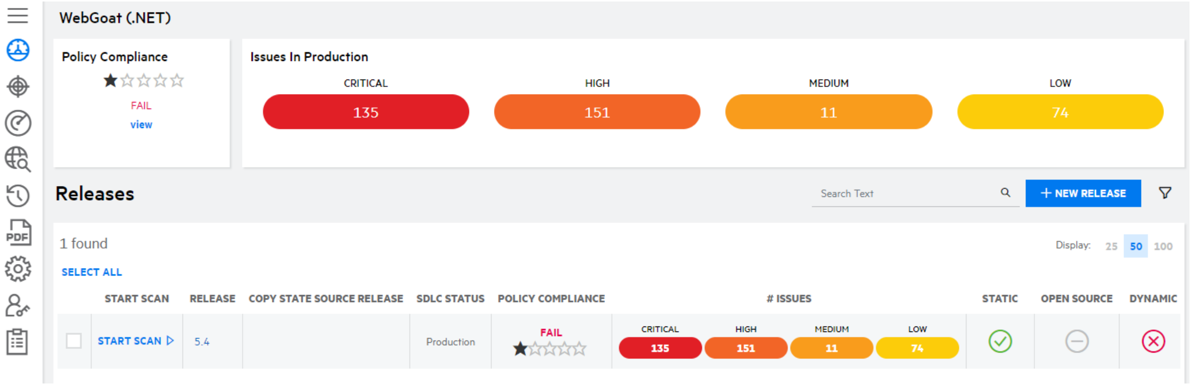
After preparing your application files for a static assessment, you need to configure the static scan settings. You only need to configure the static scan settings once per release as your settings are carried over to the next scan. You can edit settings as needed for subsequent assessments.

To configure a static scan:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of the application.

   The Application Overview page appears.



WebGoat (.NET)

Policy Compliance
★☆☆☆☆
FAIL
view

Issues In Production

CRITICAL	HIGH	MEDIUM	LOW
135	151	11	74

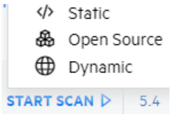
Releases

Search Text
+ NEW RELEASE

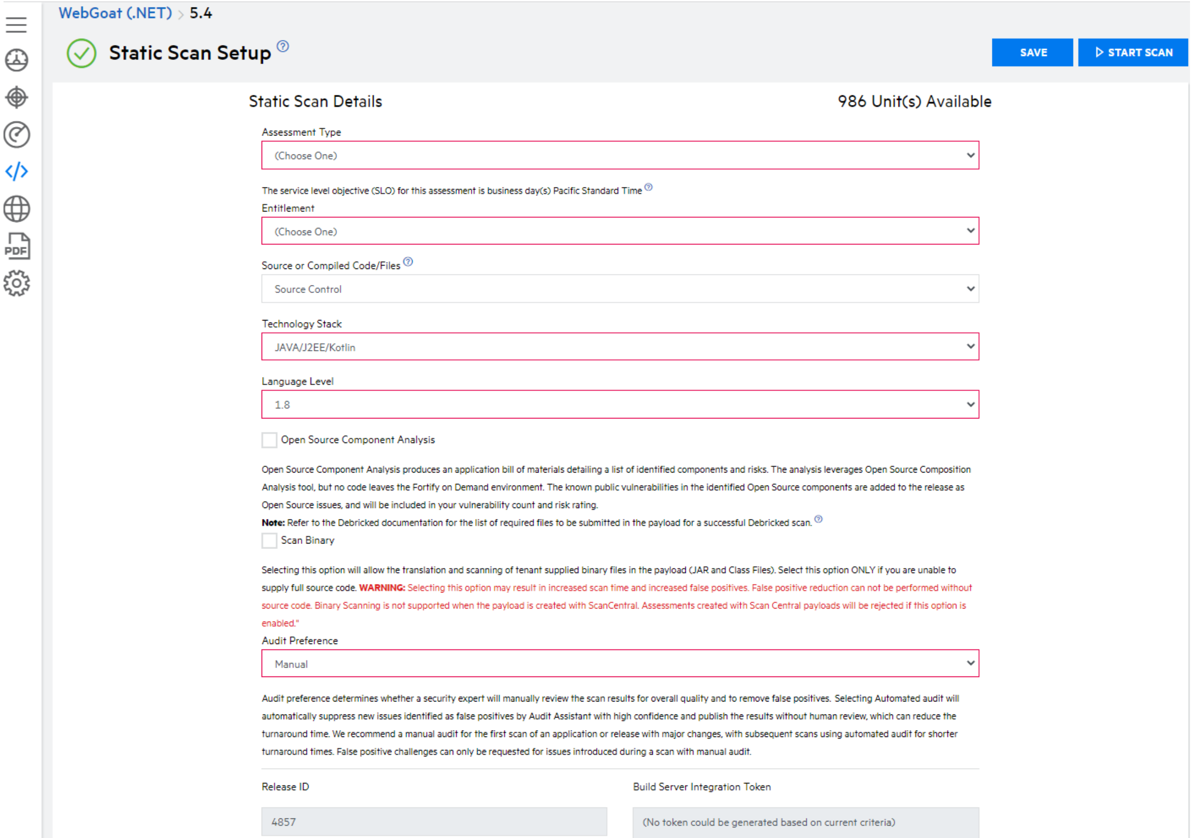
1 found
Display: 25 50 100
SELECT ALL

	START SCAN	RELEASE	COPY STATE SOURCE RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES	STATIC	OPEN SOURCE	DYNAMIC
□	START SCAN ▷	5.4		Production	FAIL ★☆☆☆☆	CRITICAL 135 HIGH 151 MEDIUM 11 LOW 74	✓	⊖	⊗

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



   The Static Scan Setup page appears.



WebGoat (.NET) > 5.4

Static Scan Setup

Static Scan Details

986 Unit(s) Available

Assessment Type: (Choose One)

The service level objective (SLO) for this assessment is business day(s) Pacific Standard Time

Entitlement: (Choose One)

Source or Compiled Code/Files: Source Control

Technology Stack: JAVA/J2EE/Kotlin

Language Level: 1.8

□ Open Source Component Analysis

Open Source Component Analysis produces an application bill of materials detailing a list of identified components and risks. The analysis leverages Open Source Composition Analysis tool, but no code leaves the Fortify on Demand environment. The known public vulnerabilities in the identified Open Source components are added to the release as Open Source issues, and will be included in your vulnerability count and risk rating.

Note: Refer to the Debricked documentation for the list of required files to be submitted in the payload for a successful Debricked scan.

□ Scan Binary

Selecting this option will allow the translation and scanning of tenant supplied binary files in the payload (JAR and Class Files). Select this option ONLY if you are unable to supply full source code. **WARNING:** Selecting this option may result in increased scan time and increased false positives. False positive reduction can not be performed without source code. Binary Scanning is not supported when the payload is created with ScanCentral. Assessments created with Scan Central payloads will be rejected if this option is enabled."

Audit Preference: Manual

Audit preference determines whether a security expert will manually review the scan results for overall quality and to remove false positives. Selecting Automated audit will automatically suppress new issues identified as false positives by Audit Assistant with high confidence and publish the results without human review, which can reduce the turnaround time. We recommend a manual audit for the first scan of an application or release with major changes, with subsequent scans using automated audit for shorter turnaround times. False positive challenges can only be requested for issues introduced during a scan with manual audit.

Release ID: 4857

Build Server Integration Token: (No token could be generated based on current criteria)

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. 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.
Source or Compiled	Select the method of uploading the payload. • **Manual Upload** (default): Manually upload the payload from your local

Code/Files	system. - **Source Control**: Upload the payload from a version control platform. This option is only available if source control has been configured. For more information, see "Source Control Integration" on page 358.
Technology Stack	Select the application's technology stack. The languages available for selection depends on the application type (web/thick client or mobile) and whether the application is a microservice application. If the auto detect feature is enabled, selecting **Auto Detect** has 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.
Open Source Component Analysis	(Optional) Select the check box to include open source component analysis. No code leaves the Fortify on Demand environment. For more information on adding open source component analysis as part of a static scan, see "Open Source Software Composition Analysis" on page 116.
Scan Binary	**Note:** Contact support to enable the option. (Optional; Java/J2EE/Kotlin,.NET, and .NET Core technology stacks) Select the check box to have compiled and source code files scanned. Scanning binary files is not supported for ScanCentral-packaged payloads. **Note:** If the source code inclusion requirement is enabled and this option is not selected, the scan will be cancelled if the payload does not contain source code.
Audit Preference	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.

	The ability to select 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.
Scan third-party libraries for static security assessment	**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.
Release ID	Once the static scan settings have been saved, the release ID can be used to submit a static scan using CICD tools. The release ID serves as a token that retrieves the most recently saved scan settings in the portal. **Important!** The release ID replaces the BSI token. Migrate build configurations to the release ID at your earliest convenience.
Build Server Integration	Once the static scan settings (assessment type, technology stack, language level, audit preference, open source component analysis, and include third party libraries) have been configured, a token is automatically populated in the **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.

5. Click **Save**.

   Your static scan settings are saved.

6. If you have the Consume Entitlements permissions and selected a subscription entitlement, click **Start Subscription** to start the static assessment subscription and consume the entitlement without starting a scan.

   Note: Contact support to enable the option.

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

Uploading a Static Assessment Payload Through the Portal

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, Fortify recommends uploading through the portal only if the file size is less than 500 MB. If you have difficulties uploading through the portal, see "Related Topics" on page 114 for alternative methods of uploading your files. You can also contact support to discuss the most appropriate upload option.

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

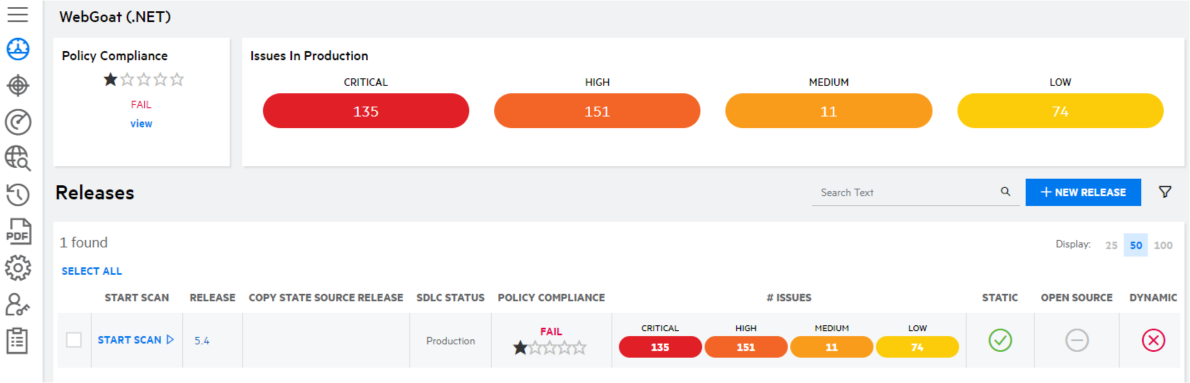
To upload a static assessment payload through the portal:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click the name of the application.

   The Application Overview page appears.



WebGoat (.NET)

Policy Compliance
★☆☆☆☆
FAIL
view

Issues In Production

CRITICAL	HIGH	MEDIUM	LOW
135	151	11	74

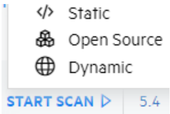
Releases

Search Text
+ NEW RELEASE

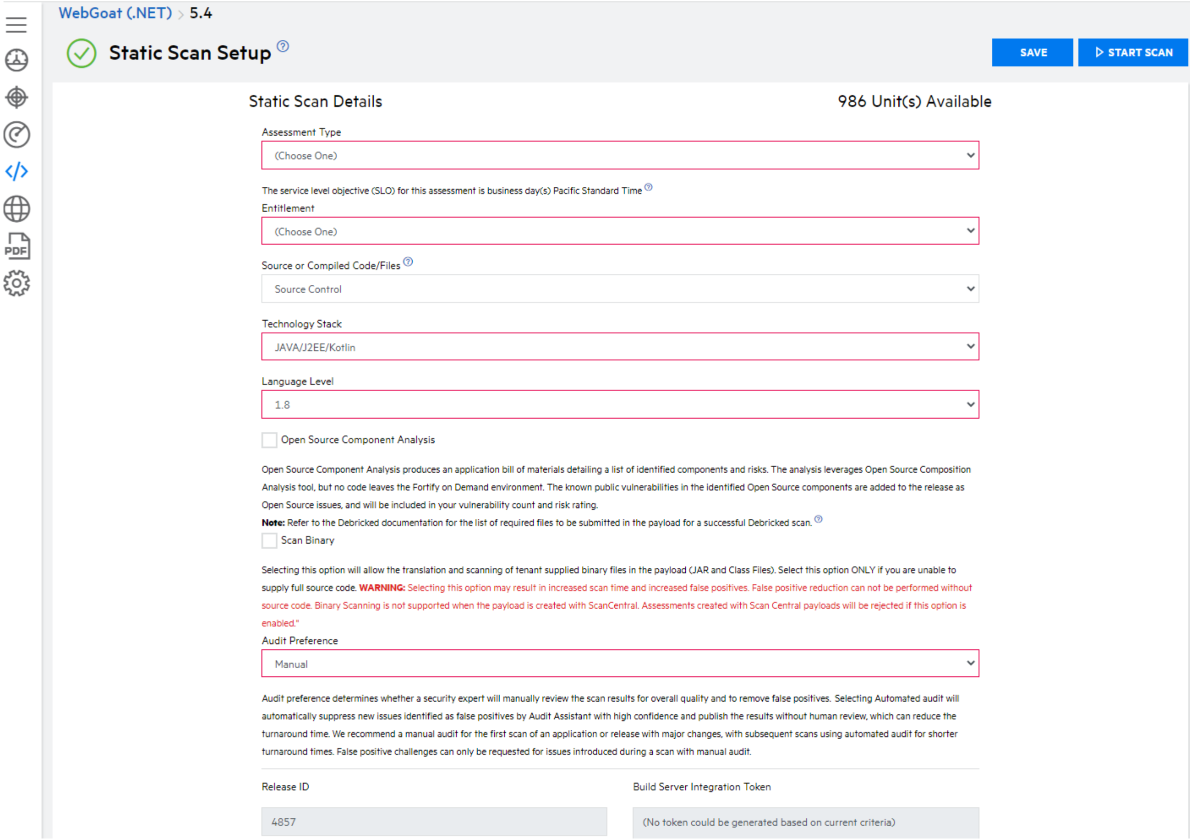
1 found
Display: 25 50 100
SELECT ALL

	START SCAN	RELEASE	COPY STATE SOURCE RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES	STATIC	OPEN SOURCE	DYNAMIC
□	START SCAN ▷	5.4		Production	FAIL ★☆☆☆☆	CRITICAL 135 HIGH 151 MEDIUM 11 LOW 74	✓	⊖	⊗

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.



Static Scan Setup

Static Scan Details

986 Unit(s) Available

Assessment Type: (Choose One)

The service level objective (SLO) for this assessment is business day(s) Pacific Standard Time

Entitlement: (Choose One)

Source or Compiled Code/Files: Source Control

Technology Stack: JAVA/J2EE/Kotlin

Language Level: 1.8

□ Open Source Component Analysis

Open Source Component Analysis produces an application bill of materials detailing a list of identified components and risks. The analysis leverages Open Source Composition Analysis tool, but no code leaves the Fortify on Demand environment. The known public vulnerabilities in the identified Open Source components are added to the release as Open Source issues, and will be included in your vulnerability count and risk rating.

Note: Refer to the Debricked documentation for the list of required files to be submitted in the payload for a successful Debricked scan.

□ Scan Binary

Selecting this option will allow the translation and scanning of tenant supplied binary files in the payload (JAR and Class Files). Select this option ONLY if you are unable to supply full source code. **WARNING:** Selecting this option may result in increased scan time and increased false positives. False positive reduction can not be performed without source code. Binary Scanning is not supported when the payload is created with ScanCentral. Assessments created with Scan Central payloads will be rejected if this option is enabled."

Audit Preference: Manual

Audit preference determines whether a security expert will manually review the scan results for overall quality and to remove false positives. Selecting Automated audit will automatically suppress new issues identified as false positives by Audit Assistant with high confidence and publish the results without human review, which can reduce the turnaround time. We recommend a manual audit for the first scan of an application or release with major changes, with subsequent scans using automated audit for shorter turnaround times. False positive challenges can only be requested for issues introduced during a scan with manual audit.

Release ID: 4857

Build Server Integration Token: (No token could be generated based on current criteria)

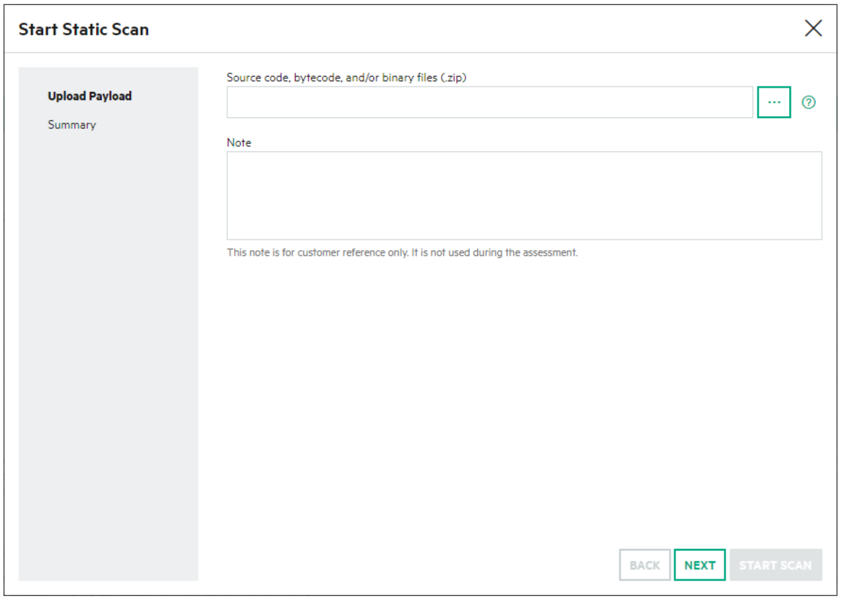
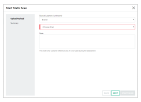
4. Click **Start Scan**.

> **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	 Start Static Scan Upload Payload Summary BACK NEXT START SCAN Source code, bytecode, and/or binary files (.zip) Note This note is for customer reference only. It is not used during the assessment. a. Click **....** b. Navigate to and select your zip file.
Source Control	 a. Select **Branch** or **Release** from the **Source Location** list. b. Select the specific branch or release.

6. In the **Note** 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 will begin 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 Extension for Visual Studio Code. For more information, see "IDE Tool" on page 331.
- Build server integration tools: FoDUploader, Fortify Azure DevOps Extension, Fortify on Demand Jenkins Plugin. For more information, see "CICD Tool" on page 330.
- Fortify on Demand API. For more information, see "Fortify on Demand API" on page 317.

Static Assessment Payload Validation

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

- The zip file is valid and not corrupt.
- The payload contains file extensions that are supported by Fortify Static Code Analyzer. Supported file extensions are: ABAP, abap, appxmanifest, as, asax, ascx, ashx, asmx, asp, aspx, baml, bas, 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.

Open Source Software Composition Analysis

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

- Debricked (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.

To enable open source software composition analysis, purchase Debricked entitlements through Fortify on Demand. An entitlement is redeemed for a Debricked subscription per application. While the static scan is in progress, the software composition analysis tool checks for open source components in the payload. Open source scan results identify direct and transitive dependencies along with associated security issues and licenses

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

This section contains the following topics:

Preparing 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.

Debricked File Requirements for Lock File Analysis

To reliably detect dependencies, Debricked uses one of the following approaches depending on the build system or package manager:

- Some package managers use a lock file to describe dependencies in a project (such as npm). Package managers usually automatically generate lock files. Debricked 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), Debricked 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 Debricked lock file.

  You can use one of the following methods to generate both native lock files and Debricked lock files:

  - (Recommended) Use the Fortify ScanCentral SAST client (22.1.2 or later) to generate the lock files along with the application files. Include the `-oss` option in the `package` command. Note that package generation is not dependent on successfully packaging the lock files.
  - (Recommended) Use the Debricked CLI to generate the lock files independently of the application files. For installation and usage instructions, see For more information, see README.FoD.md.
  - Manually generate the lock files.

    > **Tip:** If you are manually generating Debricked lock files, automate this process by adding the appropriate command to your CICD pipeline.

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

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

Language	Package Manager	Required File	Notes
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 README.FoD.md.

Language	Package Manager	Required File	Notes
			- 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

Language	Package Manager	Required File	Notes
			Java & Kotlin - Gradle, Maven and Bazel.

	Maven	`.debricked-maven-dependencies.tgf`
		`maven.debricked.lock`
			For instructions on generating the resolved dependency tree file, see Java & Kotlin - Gradle, Maven and Bazel.
			Note: `.debricked-maven-dependencies.txt` is generated by the Fortify ScanCentral SAST client, `maven.debricked.lock` is generated by the Debricked CLI.

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.

Language	Package Manager	Required File	Notes
	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 Fortify ScanCentral SAST client to package the payload.

Debricked File Requirements for Fingerprint Analysis

Debricked supports scanning for unmanaged dependencies not defined in manifest files by examining fingerprints of the application files (including binary files). Currently C# (.NET), Java, and Python are supported. Debricked requires the `debricked.fingerprints.txt` file, which is automatically generated by Fortify on Demand when submitting a Debricked scan. A Debricked scan includes both fingerprint analysis and lock file analysis.

For more information on Debricked file fingerprinting, see https://docs.debricked.com/tools-and-integrations/cli/debricked-cli/file-fingerprinting.

Sonatype File Requirements

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

Uploading an Open Source Assessment 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:

- Configure your static scan settings to include an open source scan and include the files required for open source scanning in your static assessment payload. This method is available for both Debricked and Sonatype. For more information, see "Configuring a Static Scan" on page 108.
- Upload a native or Debricked lock file and submit a Debricked-only scan. The following instructions describe how to submit a Debricked-only scan for a lock file.

> **Note:** You can submit a Debricked-only scan on third-party software bill of materials. For more information, see "Importing a Software Bill of Materials" on page 351.

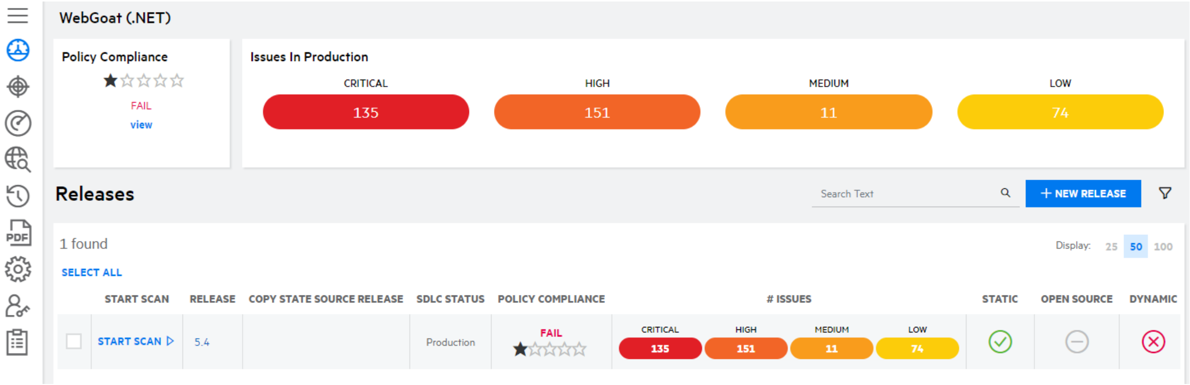
To scan:

1. Select the **Applications** view.

   Your Applications page appears.

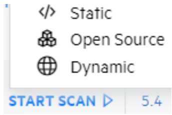
2. Click the name of the application.

   The Application Overview page appears.

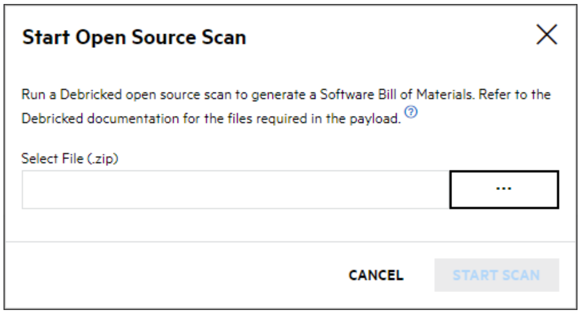


	START SCAN	RELEASE	COPY STATE SOURCE RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES CRITICAL	HIGH	MEDIUM	LOW	STATIC	OPEN SOURCE	DYNAMIC
□	START SCAN ▷	5.4		Production	FAIL ★☆☆☆☆	135	151	11	74	✓	⊖	⊗

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



   The Open Source Scan window appears.



Run a Debricked open source scan to generate a Software Bill of Materials. Refer to the Debricked documentation for the files required in the payload. ?

Select File (.zip)

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.

Viewing Open Source Components in a Release

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

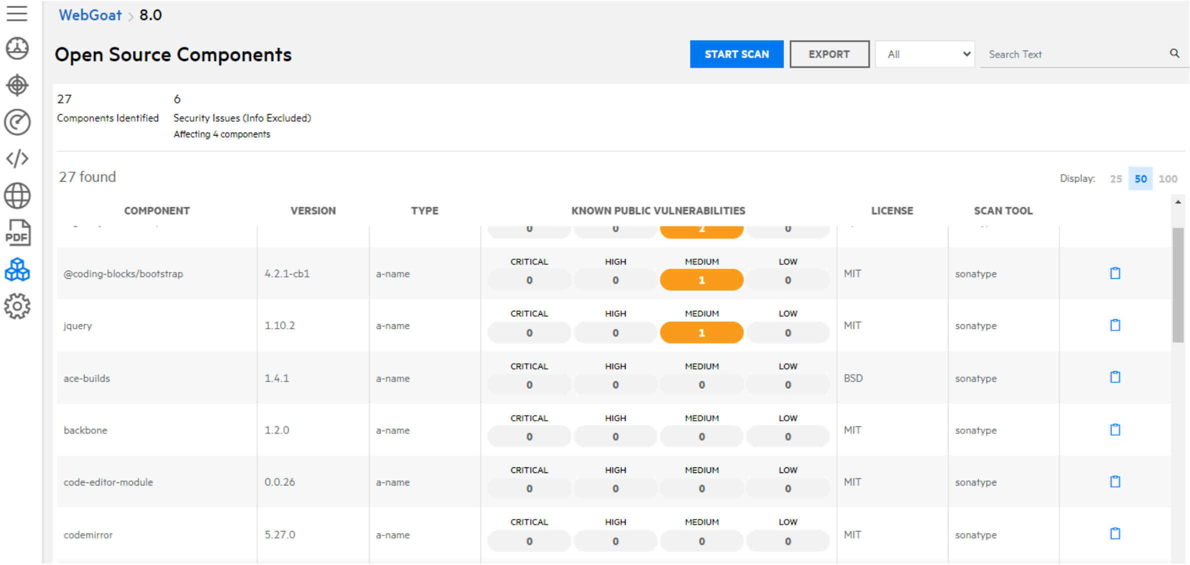
To view open source components for a release:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears.
3. Click **Open Source Components**.

   The Open Source Components page appears.



Open Source Components

27 Components Identified

6 Security Issues (Info Excluded)
Affecting 4 components

27 found

Display: 25 50 100

COMPONENT	VERSION	TYPE	KNOWN PUBLIC VULNERABILITIES				LICENSE	SCAN TOOL
			CRITICAL	HIGH	MEDIUM	LOW		
			0	0	2	0		
@coding-blocks/bootstrap	4.2.1-cb1	a-name	0	0	1	0	MIT	sonatype
jquery	1.10.2	a-name	0	0	1	0	MIT	sonatype
ace-builds	1.4.1	a-name	0	0	0	0	BSD	sonatype
backbone	1.2.0	a-name	0	0	0	0	MIT	sonatype
code-editor-module	0.0.26	a-name	0	0	0	0	MIT	sonatype
codemirror	5.27.0	a-name	0	0	0	0	MIT	sonatype

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

   The page refreshes with results from the selected source.

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**.
View issues filtered by package URL	Click the issue counts in each component row.

Viewing Open Source Components in a Tenant

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

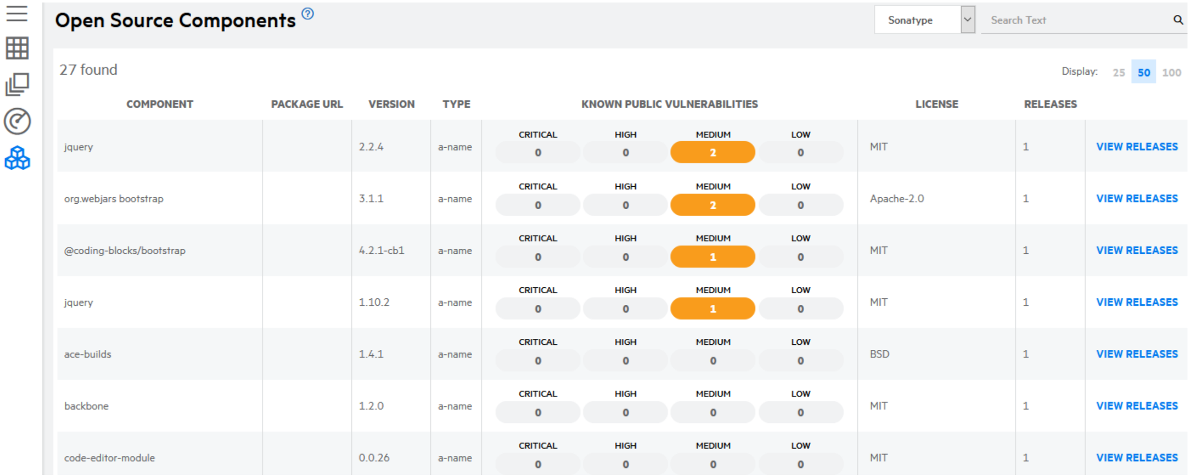
To view open source components across a tenant:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click **Open Source Components**.

   The Open Source Components page appears.



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

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**.
View the applications and corresponding releases that use a component.	Click **View Releases** in the row of a component.

Sonatype Integration End of Life

Fortify on Demand will remove the Sonatype open source software composition analysis offering in 2024. Data from Sonatype scans will be deleted in Fortify on Demand on January 31st, 2024.

Tenants that need to retain their Sontype scan data can perform the followings to migrate their data:

- Export the open source component list on the Open Source Component pages. The download is a CSV file.
- Run issue data exports filtered to include only open source issues.
- Tenants can have active Debricked and Sonatype entitlements at the same time in order to facilitate a one-time switch from Sonatype to Debricked. This switch applies per release. For more information, see "Editing Release Settings" on page 67.

  For releases that have switched from Sonatype to Debricked, upon completion of the first Debricked scan, Sonatype issue audit entries, comments, and evidence are copied over to Debricked issues that have matching CVE values. Sonatype data will not be copied over to subsequent Debricked scans.
- Contact support to request a one-time download of Sonatype issues.

Dynamic Assessments

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

Dynamic testing using Fortify WebInspect involves the following modes:

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

This section contains the following topics:

Preparing 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, Fortify recommends that you back up all of your data before beginning the testing process. When testing is complete, restore your data from a backup that is known to be good to avoid any chance of data corruption.
- Add the Fortify on Demand IP addresses to the allow list in firewalls, IPSs, IDSs, and WAFs to ensure the application can be scanned by the dynamic testing team. You can obtain the IP addresses from the Dynamic Scan Setup page in the portal. Adhoc addresses may be used with your consent only when conditions necessitate it.
- Provide the Fortify on Demand IP addresses to your security operations and network operations teams, so they know not to block the IP addresses if they see attacks being submitted against the site, which are part of planned recurring security scanning.
- 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 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 Fortify WebInspect's Event-based Web Macro Recorder, available on the Tools page in the portal. For instructions on creating workflow macros, see the *Fortify WebInspect Tools Guide* at Fortify WebInspect 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 Fortify WebInspect's Event-based Web Macro Recorder, available on the Tools page in the portal. For instructions on creating login macros, see the *Fortify WebInspect Tools Guide* at Fortify WebInspect Documentation.

Preparing Web API Files

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

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

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. Fortify WebInspect 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.

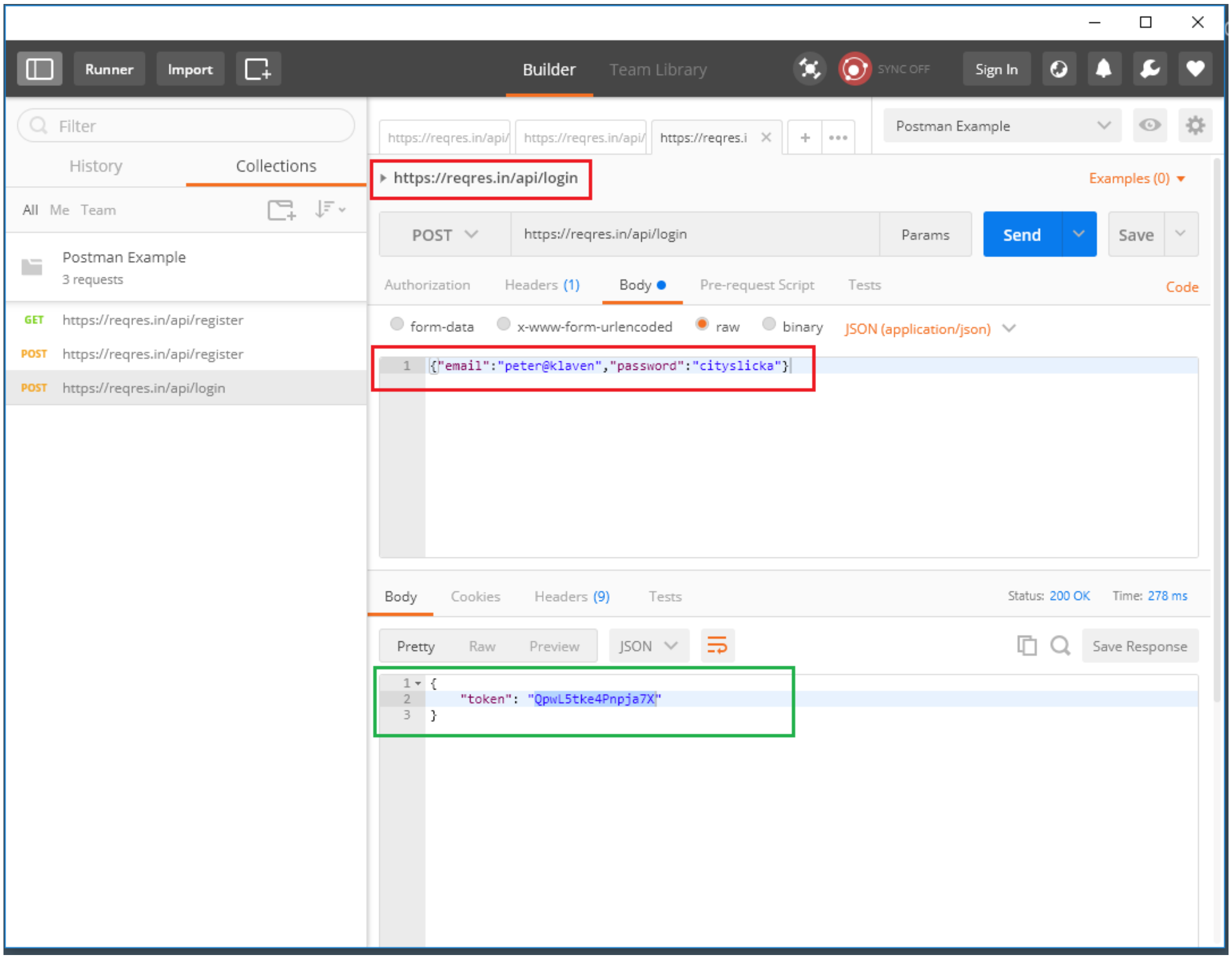
Examples

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).

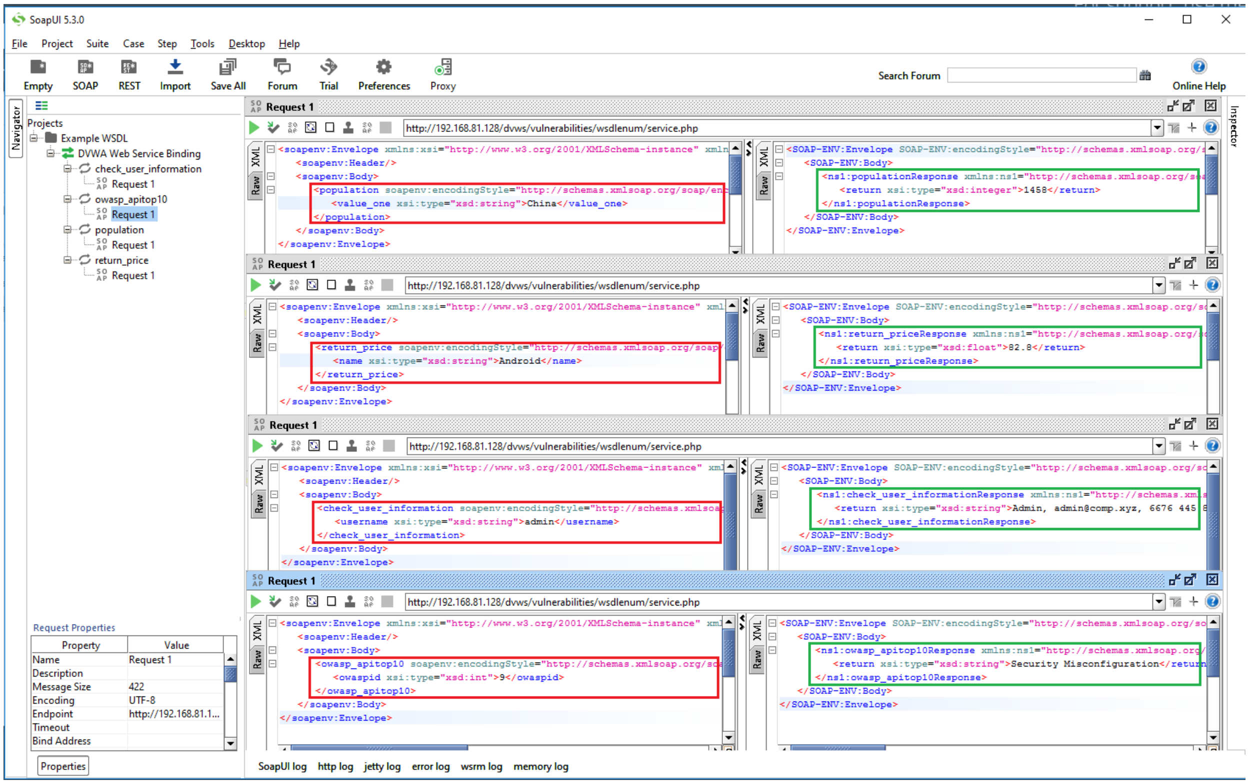


```
{"email":"peter@klaven","password":"cityslicka"}
```

```
{
    "token": "QpwL5tke4Pnpja7X"
}
```

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).



Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmln
   <soapenv:Header/>
   <soapenv:Body>
      <population soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/en
         <value_one xsi:type="xsd:string">China</value_one>
      </population>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/s
   <SOAP-ENV:Body>
      <ns1:populationResponse xmlns:ns1="http://schemas.xmlsoap.org/s
         <return xsi:type="xsd:integer">1458</return>
      </ns1:populationResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xml
   <soapenv:Header/>
   <soapenv:Body>
      <return_price soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/
         <name xsi:type="xsd:string">Android</name>
      </return_price>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/s
   <SOAP-ENV:Body>
      <ns1:return_priceResponse xmlns:ns1="http://schemas.xmlsoap.org/
         <return xsi:type="xsd:float">82.8</return>
      </ns1:return_priceResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xml
   <soapenv:Header/>
   <soapenv:Body>
      <check_user_information soapenv:encodingStyle="http://schemas.xmlsoa
         <username xsi:type="xsd:string">admin</username>
      </check_user_information>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/s
   <SOAP-ENV:Body>
      <ns1:check_user_informationResponse xmlns:ns1="http://schemas.xml
         <return xsi:type="xsd:string">Admin, admin@comp.xyz, 6676 445
      </ns1:check_user_informationResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xml
   <soapenv:Header/>
   <soapenv:Body>
      <owasp_apitop10 soapenv:encodingStyle="http://schemas.xmlsoap.org/so
         <owaspid xsi:type="xsd:int">9</owaspid>
      </owasp_apitop10>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/so
   <SOAP-ENV:Body>
      <ns1:owasp_apitop10Response xmlns:ns1="http://schemas.xmlsoap.org/
         <return xsi:type="xsd:string">Security Misconfiguration</retur
      </ns1:owasp_apitop10Response>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Request Properties

Property	Value
Name	Request 1
Description	
Message Size	422
Encoding	UTF-8
Endpoint	http://192.168.81.1...
Timeout	
Bind Address	

Setting Up Fortify on Demand Connect

You can use Fortify on Demand Connect to easily set up site-to-site VPN for dynamic assessments of internally facing web applications. 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: Fortify on Demand Connect is currently available in the AMS environment. If your tenant is not in the AMS environment, you can preview Fortify on Demand in a sandbox environment. Contact support if you are interested in trying out Fortify on Demand Connect.

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

To set up Fortify on Demand Connect:

1. Pull the 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 Fortify on Demand Connect network in Fortify on Demand. See "Adding a Fortify on Demand Connect Network" on page 266.
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.

Configuring 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.

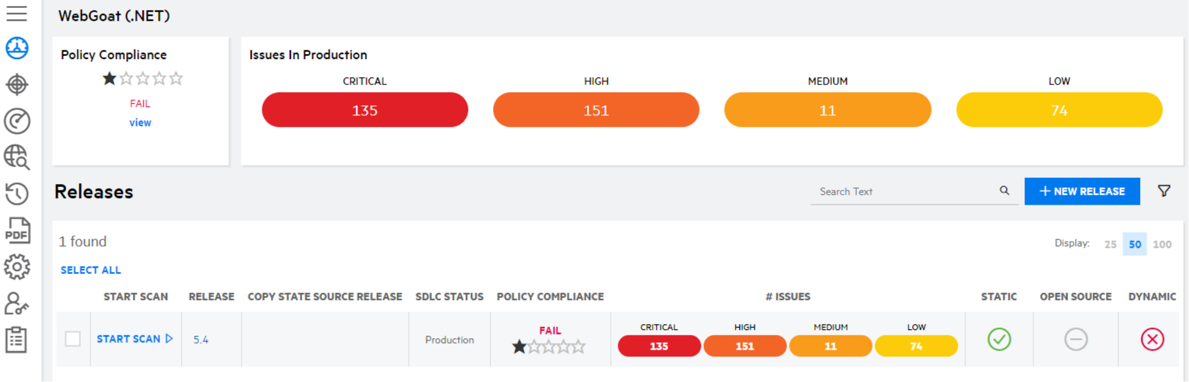
Note: Dynamic scan settings prior to 22.4 were saved at the application level. Save or update existing dynamic scan settings to have them saved at the release level.

To configure a dynamic scan:

1. Select the Applications view.

   Your Applications page appears.
2. Click the name of the application.

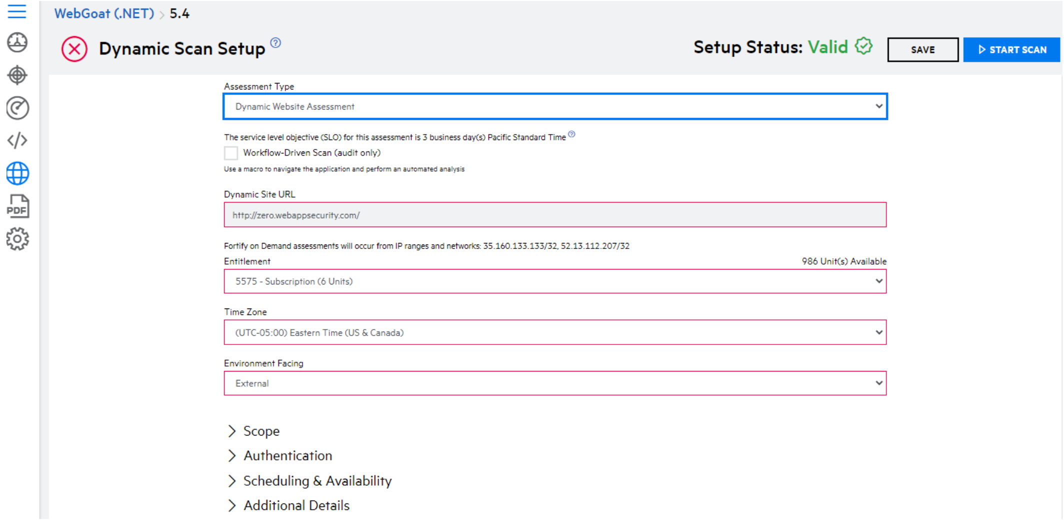
   The Application Overview page appears.



	START SCAN	RELEASE	COPY STATE SOURCE RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES CRITICAL	HIGH	MEDIUM	LOW	STATIC	OPEN SOURCE	DYNAMIC
□	START SCAN ▷	5.4		Production	FAIL ★☆☆☆☆	135	151	11	74	✓	⊖	⊗

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

The Dynamic Scan Setup page appears.



Assessment Type: Dynamic Website Assessment

The service level objective (SLO) for this assessment is 3 business day(s) Pacific Standard Time

□ Workflow-Driven Scan (audit only)

Use a macro to navigate the application and perform an automated analysis

Dynamic Site URL: http://zero.webappsecurity.com/

Fortify on Demand assessments will occur from IP ranges and networks: 35.160.133.133/32, 52.13.112.207/32

Entitlement: 5575 - Subscription (6 Units) — 986 Unit(s) Available

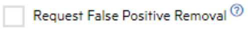
Time Zone: (UTC-05:00) Eastern Time (US & Canada)

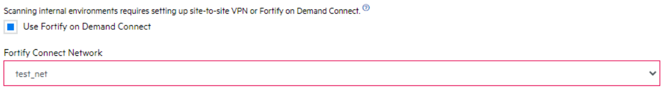
Environment Facing: External

> Scope
> Authentication
> Scheduling & Availability
> Additional Details

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.
Dynamic Site URL	• All Website types • API+	Provide your site's URL.

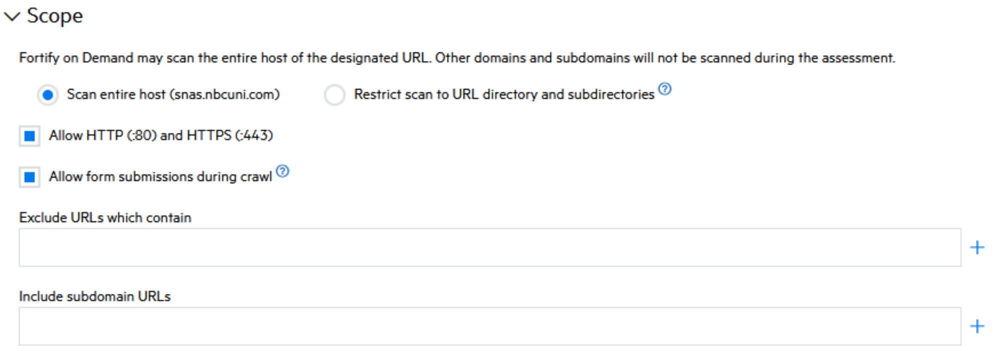
Field	Assessment Type	Description
Workflow-Driven Scan	• Website (Optional) • DAST Automated: Workflow-Driven Scan	A Workflow-Driven Scan uses the audit only mode (no crawling) and is completely automated. Fortify WebInspect audits only those URLs recorded in the macro and does not follow any hyperlinks 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 "Preparing the Website for Dynamic Testing" on page 125). Supported macros are `.webmacro` files, Burp Proxy captures, and `.har` files. **Note:** The application being scanned must be external facing. Activity recorded in a macro overrides other scan settings.
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.
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	DAST Automated	 ☐ Request False Positive Removal Select the check box to request false positive removal

Field	Assessment Type	Description
		by the testing team once per application. **Important!** Login macro generation and false positive removal are 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		 Scanning internal environments requires setting up site-to-site VPN or Fortify on Demand Connect. ☑ Use Fortify on Demand Connect Fortify Connect Network test_net (Optional) If the site is internal, select the check box to use Fortify on Demand Connect to set up site-to-site VPN, and then select the Fortify on Demand Connect network that has been configured for the site. For more information, see "Setting Up Fortify on Demand Connect " on page 128. **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.



Scope

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

● Scan entire host (snas.nbcuni.com) ○ Restrict scan to URL directory and subdirectories

☑ Allow HTTP (:80) and HTTPS (:443)

☑ Allow form submissions during crawl

Exclude URLs which contain

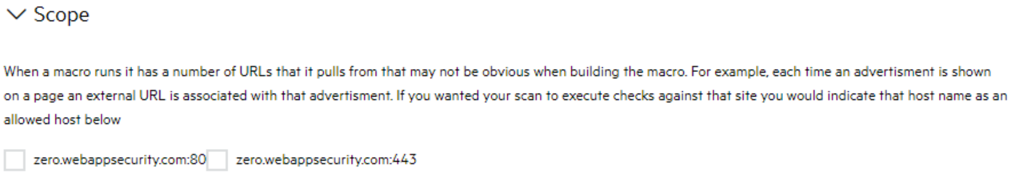
Include subdomain URLs

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	Select the check box to allow both HTTP and HTTPS scanning of the site (default).

Field	Description
HTTPS (:443)	**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.
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.
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 assessment) By default, 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.



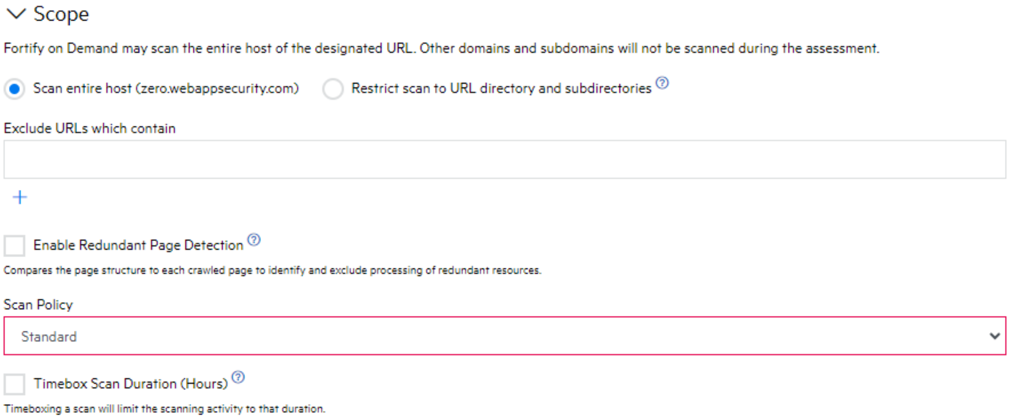
Scope

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

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

Scope (DAST Automated)

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



Scope

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

● Scan entire host (zero.webappsecurity.com) ○ Restrict scan to URL directory and subdirectories

Exclude URLs which contain

□ Enable Redundant Page Detection

Compares the page structure to each crawled page to identify and exclude processing of redundant resources.

Scan Policy

Standard

□ Timebox Scan Duration (Hours)

Timeboxing a scan will limit the scanning activity to that duration.

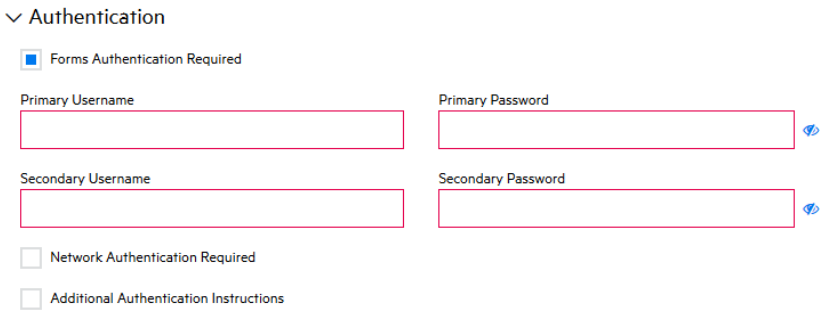
Field	Scan Type	Description
Scan entire host (<*URL*>)	Website	Select one of the following options: • **Scan entire host (<*URL*>)** (default): the entire host will be scanned **Example**: Given https://foo.com/home, the following URLs will be included: ◦ https://foo.com/ ◦ https://foo.com/contact-us.html ◦ 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**

Field	Scan Type	Description
		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. **Important!** 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

Field	Scan Type	Description
		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+ API)

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



Authentication

☑ Forms Authentication Required

Primary Username

Primary Password

Secondary Username

Secondary Password

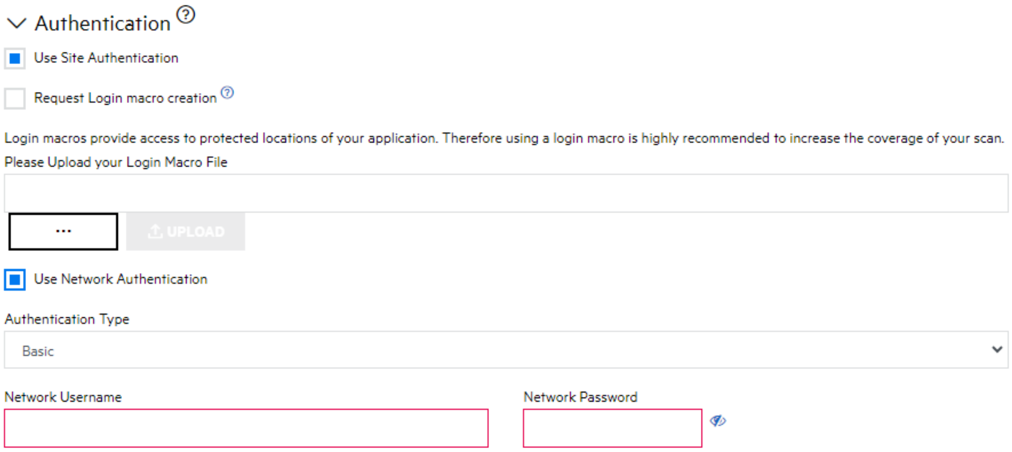
□ Network Authentication Required

□ Additional Authentication Instructions

Field	Description
Form Authentication	(Optional) Select the check box if form authentication is required. Provide user names and passwords for at least two users. To add more credentials, use the **Additional Notes** field at the bottom of this form.
Network 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. **Important!** 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.



Authentication

☑ Use Site Authentication

□ Request Login macro creation

Login macros provide access to protected locations of your application. Therefore using a login macro is highly recommended to increase the coverage of your scan.

Please Upload your Login Macro File

☑ Use Network Authentication

Authentication Type

Basic

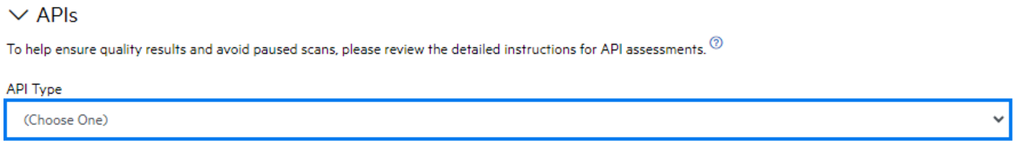
Network Username

Network Password

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" on page 125). **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.
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. **Important!** Login macro generation and false positive removal are 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 Network Authentication		(Optional) Select the check box if network authentication is required. Provide the authentication type, username, and password. **Note:** The scan will be canceled if network authentication fails.

APIs (Dynamic API, 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" on page 126.



APIs

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

API Type

(Choose One)

a. Select the API definition type in the **API Type** field: **Postman Collection**, **OpenAPI**, **GraphQL**, **gRPC**.

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

b. Perform the relevant task based on your API definition type:

API 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.
OpenAPI	Select **File** or **URL to the OpenAPI specification** and perform the relevant task based on your selection.
	File i. Click ... and browse to and select the OpenAPI document file. The JSON file format is accepted. If a file already exists, you can use the existing file or upload a new file. ii. 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 i. Provide the OpenAPI document URL. ii. 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.
GraphQL	Select **File** or **URL** and perform the relevant task based on your selection.
	File i. Click ... and browse to and select the GraphQL introspection file. The JSON file format is accepted. If a file already exists, you can use the existing file or upload a new file. ii. Select the API scheme in the **API Scheme Type** field: **HTTP**, **HTTPS**, **HTTP and HTTPS**.

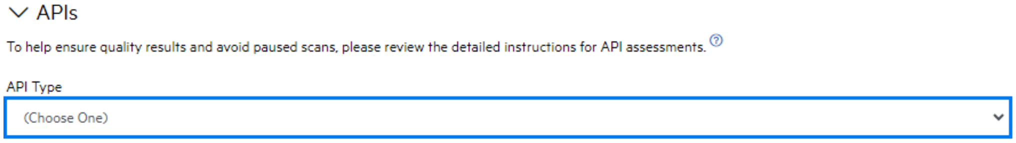
	iii. In the **API Host** field, provide the URL or hostname. iv. In the **API Service** field, provide the directory path for the API service.
	URL Provide the GraphQL introspection endpoint URL. **Note:** The GraphQL API must have introspection enabled to download the schema contents for the scan.
gRPC	i. Click ... and browse to and select the gRPC proto file. The PROTO file format is accepted. If a file already exists, you can use the existing file or upload a new file. ii. Select the API scheme in the **API Scheme Type** field: **HTTP**, **HTTPS**, **HTTP and HTTPS**. iii. In the **API Host** field, provide the URL or hostname. iv. In the **API Service** field, provide the directory path for the API service.

c. In the **Additional Instructions** field, provide additional instructions.

APIs (Dynamic+ API)

For information on preparing web API project files suitable for automated testing, see "Preparing Web API Files" on page 126.

a. To add instructions for scanning web APIs utilized by the site, click **APIs**.



APIs

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

API Type: (Choose One)

b. Select the API definition type in the **API Type** field: **SOAP**, **REST**, **GraphQL**, **gRPC**.

c. Perform the relevant task based on your API definition type:

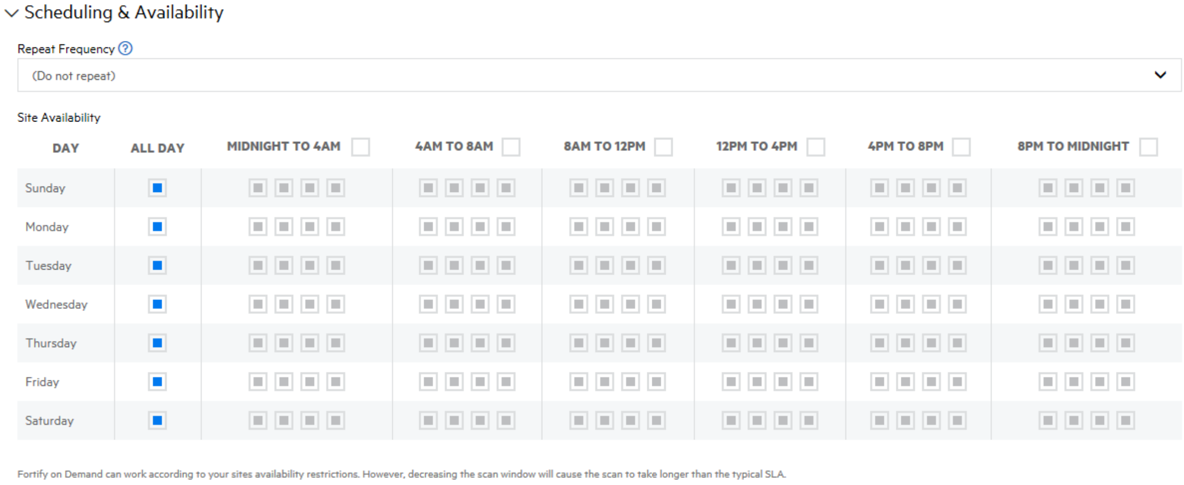
API Definition Type	Procedure
SOAP	i. Upload a WSDL file that contains working sample data. The JSON, WSDL, TXT, and XML file formats are accepted.

	ii. (Optional) In the **Additional Instructions** field, provide additional instructions, such as required headers, tokens, or authentication mechanisms. iii. (Optional) Provide the username and password or API key and password.
REST	i. Upload an API definition file that contains working sample data. The JSON, WSDL, TXT, and XML file formats are accepted. ii. (Optional) In the **Additional Instructions** field, provide additional instructions, such as required headers, tokens, or authentication mechanisms. iii. (Optional) Provide the username and password or API key and password.
GraphQL	Select **File** or **URL** and perform the relevant task based on your selection.
	File i. Click ... and browse to and select the GraphQL introspection file. The JSON file format is accepted. If a file already exists, you can use the existing file or upload a new file. ii. Select the API scheme in the **API Scheme Type** field: **HTTP**, **HTTPS**, **HTTP and HTTPS**. iii. In the **API Host** field, provide the URL or hostname. iv. In the **API Service** field, provide the directory path for the API service. v. In the **Additional Instructions** field, provide additional instructions.
	URL i. Provide the GraphQL introspection endpoint URL. **Note:** The GraphQL API must have introspection enabled to download the schema contents for the scan. ii. In the **Additional Instructions** field, provide additional instructions.
gRPC	i. Click ... and browse to and select the gRPC proto file. The PROTO file format is accepted. If a file already exists, you can use the existing file or upload a new file.

	ii. Select the API scheme in the **API Scheme Type** field: **HTTP**, **HTTPS**, **HTTP and HTTPS**. iii. In the **API Host** field, provide the URL or hostname. iv. In the **API Service** field, provide the directory path for the API service. v. In the **Additional Instructions** field, provide additional instructions.

Scheduling & Availability (all assessments)

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



Scheduling & Availability

Repeat Frequency

(Do not repeat)

Site Availability

DAY	ALL DAY	MIDNIGHT TO 4AM ☐	4AM TO 8AM ☐	8AM TO 12PM ☐	12PM TO 4PM ☐	4PM TO 8PM ☐	8PM TO MIDNIGHT ☐
Sunday	■	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣
Monday	■	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣
Tuesday	■	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣
Wednesday	■	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣
Thursday	■	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣
Friday	■	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣
Saturday	■	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣

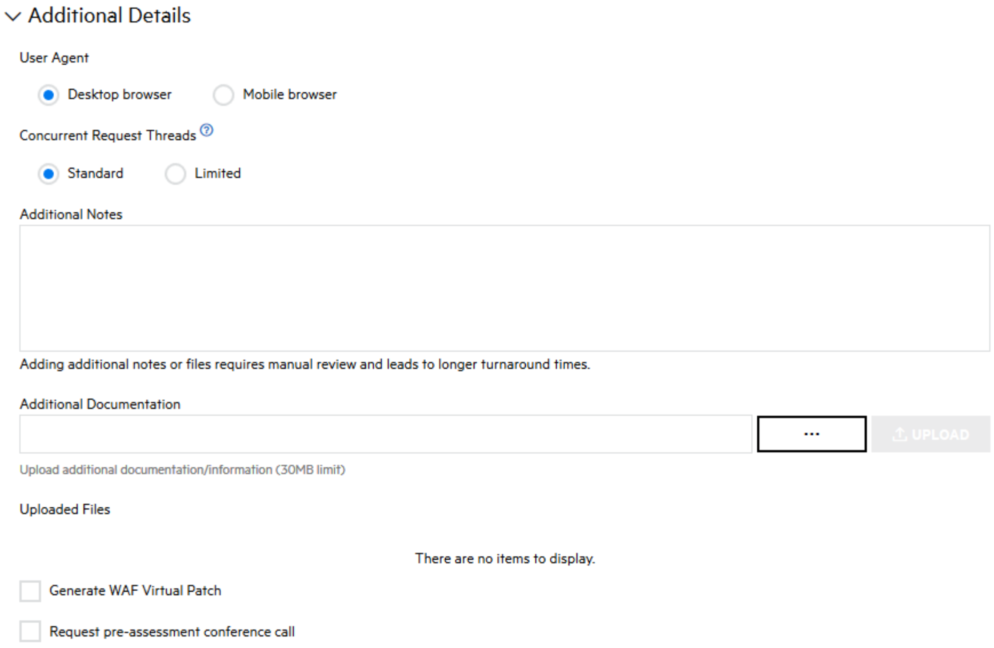
Fortify on Demand can work according to your sites availability restrictions. However, decreasing the scan window will cause the scan to take longer than the typical SLA.

Field	Description
Repeat Frequency	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 will only be scheduled if a valid entitlement for the selected

Field	Description
	assessment type exists at the time of the scheduling. • If a scan is canceled, no further scans will be scheduled. • If a scan is still in progress when the next scan is to be scheduled, Fortify on Demand will attempt once a day to reschedule the next scan until the scan date has passed. For example, if a monthly scheduled scan that starts on the 5th of the month is still in progress by the 5th of the next month, the next rescheduling attempt will take place seven days before the 5th of the 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**.



Additional Details

User Agent

● Desktop browser ○ Mobile browser

Concurrent Request Threads

● Standard ○ Limited

Additional Notes

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

Additional Documentation

Upload additional documentation/information (30MB limit)

Uploaded Files

There are no items to display.

□ Generate WAF Virtual Patch

□ Request pre-assessment conference call

Field	Description
User agent	Select the user agent type that will be used for the site: **Desktop browser** (default), **Mobile browser**
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 are displayed in the **Uploaded Files** section below. 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.

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.

Scheduling the Dynamic Scan Through the Portal

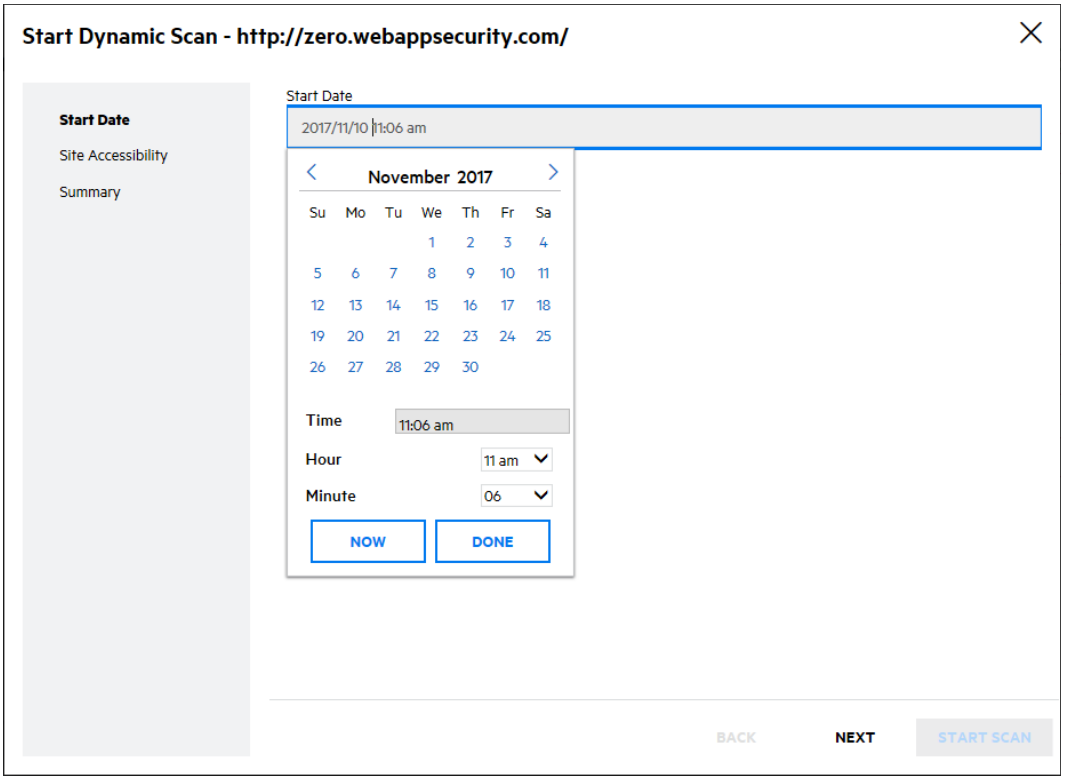
Once you have prepared your web application and configured the dynamic scan settings, you can schedule the dynamic scan. You can have only one in progress dynamic scan across all releases of an application.

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.



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

Start Date: 2017/11/10 11:06 am

Time: 11:06 am

Hour: 11 am

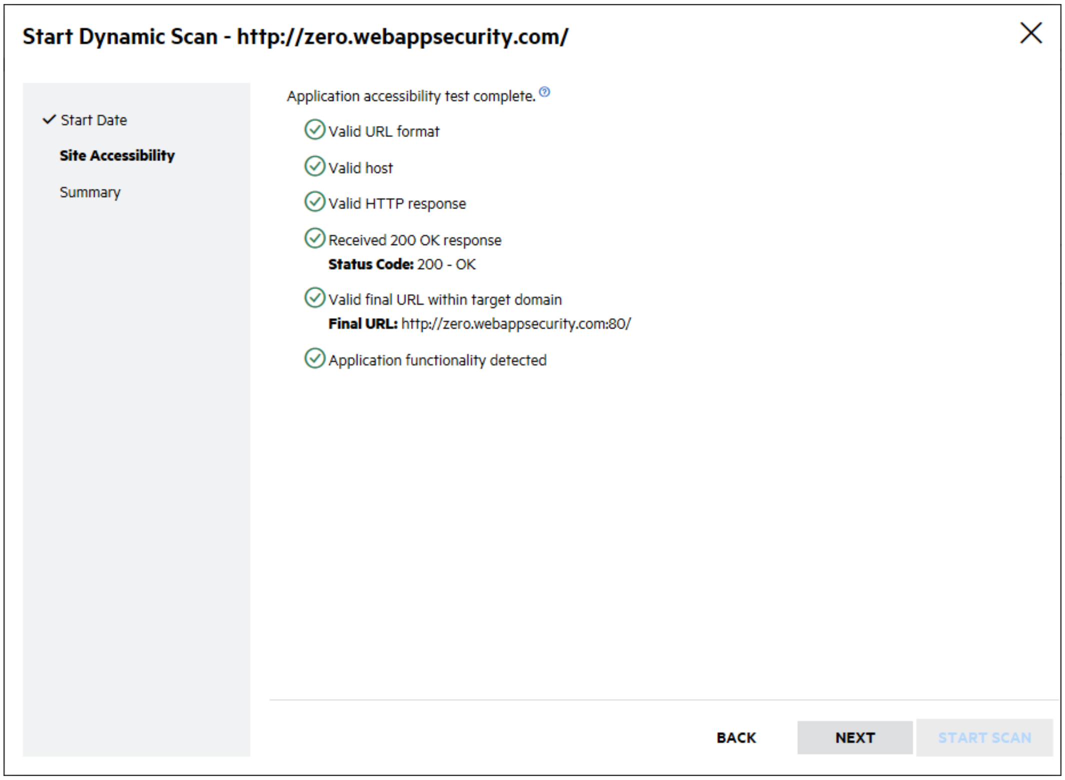
Minute: 06

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.
- 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.



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

Application accessibility test complete.

✓ Valid URL format

✓ Valid host

✓ Valid HTTP response

✓ Received 200 OK response
Status Code: 200 - OK

✓ Valid final URL within target domain
Final URL: http://zero.webappsecurity.com:80/

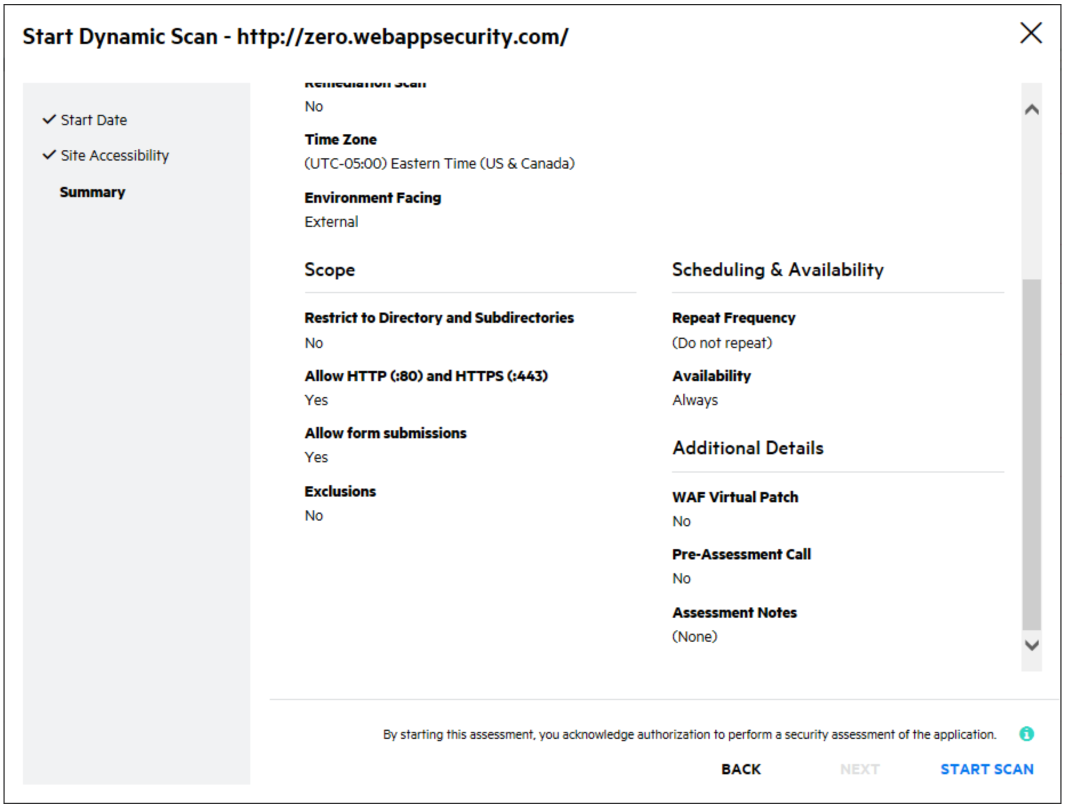
✓ Application functionality detected

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.



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

Remediation Scan
No

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

Environment Facing
External

Scope

Restrict to Directory and Subdirectories
No

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

Allow form submissions
Yes

Exclusions
No

Scheduling & Availability

Repeat Frequency
(Do not repeat)

Availability
Always

Additional Details

WAF Virtual Patch
No

Pre-Assessment Call
No

Assessment Notes
(None)

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

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.

Related Topics

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

- Build server integration tools: Fortify Azure DevOps Extension, Fortify on Demand Jenkins Plugin (coming soon). For more information, see "CICD Tool" on page 330.
- Fortify on Demand API. For more information, see "Fortify on Demand API" on page 317.

Editing Dynamic Scan Settings for Ongoing and Completed Scans

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.

Continuous Application Monitoring

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

This section contains the following topics:

Configuring Application Monitoring

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

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

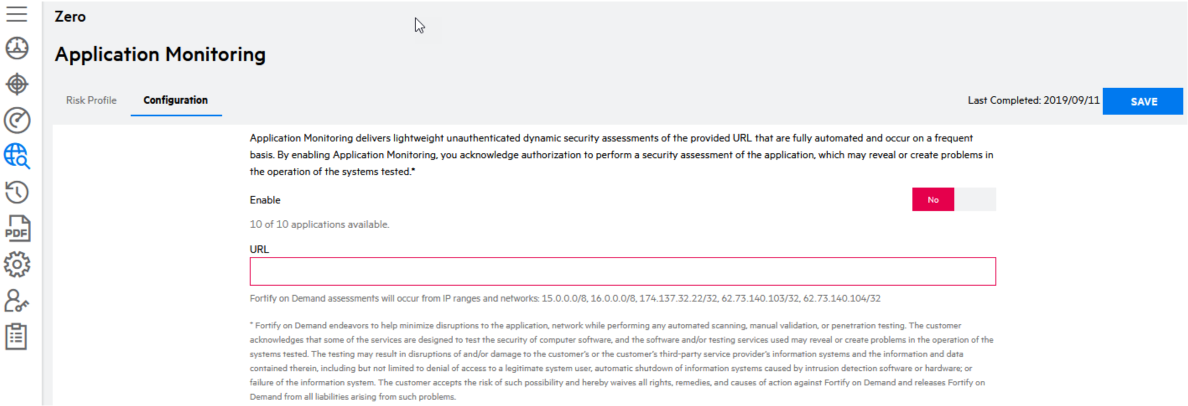
To configure Application Monitoring:

1. Select the **Applications** view.

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

   The Application Monitoring page appears.

   > **Note:** Users with the **View Applications** permission have view-only access.
4. Select the **Configuration** tab.



Zero

Application Monitoring

Application Monitoring delivers lightweight unauthenticated dynamic security assessments of the provided URL that are fully automated and occur on a frequent basis. By enabling Application Monitoring, you acknowledge authorization to perform a security assessment of the application, which may reveal or create problems in the operation of the systems tested.*

Enable: No

10 of 10 applications available.

URL

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

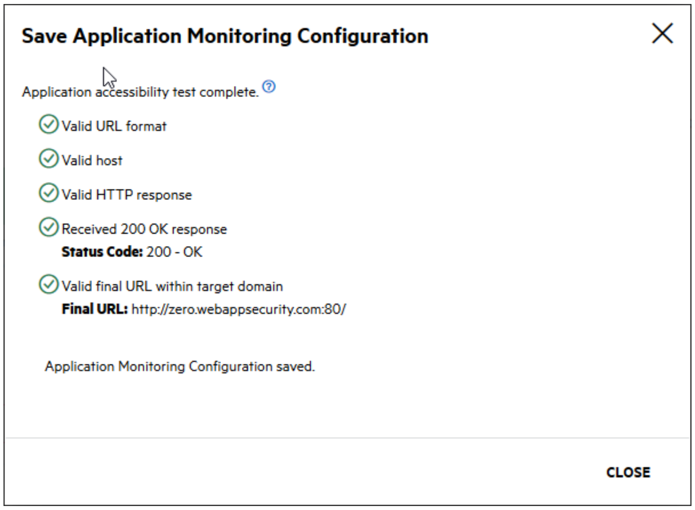
* Fortify on Demand endeavors to help minimize disruptions to the application, network while performing any automated scanning, manual validation, or penetration testing. The customer acknowledges that some of the services are designed to test the security of computer software, and the software and/or testing services used may reveal or create problems in the operation of the systems tested. The testing may result in disruptions of and/or damage to the customer's or the customer's third-party service provider's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shutdown of information systems caused by intrusion detection software or hardware; or failure of the information system. The customer accepts the risk of such possibility and hereby waives all rights, remedies, and causes of action against Fortify on Demand and releases Fortify on Demand from all liabilities arising from such problems.

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

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

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

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



Save Application Monitoring Configuration

Application accessibility test complete.

✓ Valid URL format

✓ Valid host

✓ Valid HTTP response

✓ Received 200 OK response
Status Code: 200 - OK

✓ Valid final URL within target domain
Final URL: http://zero.webappsecurity.com:80/

Application Monitoring Configuration saved.

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

8. Click **Close**.

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

Canceling an Application Monitoring Scan

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

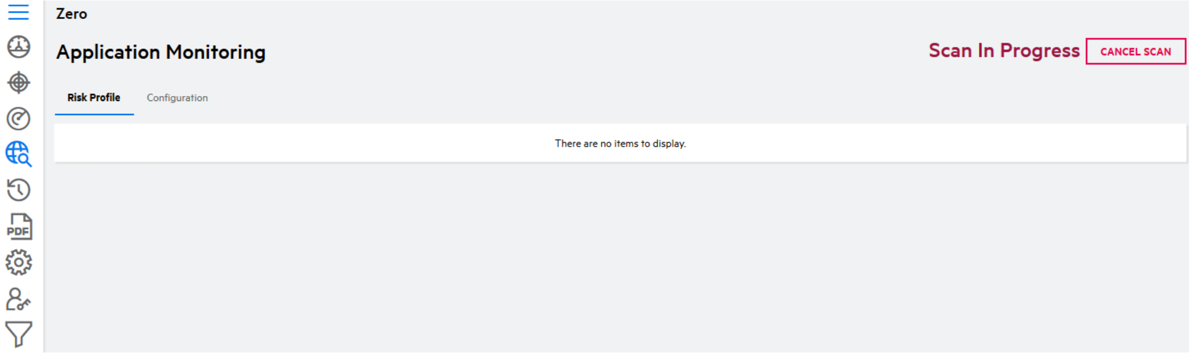
You can cancel an Application Monitoring scan from the Your Scans or Application Scans page (see "Canceling a Scan" on page 172) or the Application Monitoring page (see below).

To cancel an in progress Application Monitoring scan:

1. Select the **Applications** view.

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

   The Application Monitoring page appears.

   There are no items to display.
4. Click **Cancel Scan**.

   A confirmation message appears.
5. Click **Yes**.

   The in progress scan is cancelled.

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

Viewing Application Monitoring Issues

You can view Application Monitoring issues on the Application Issues page, which displays issues at the application level. For more information on viewing application issues, see "Viewing Application Issues" on page 177.

Viewing Risk Profile Results

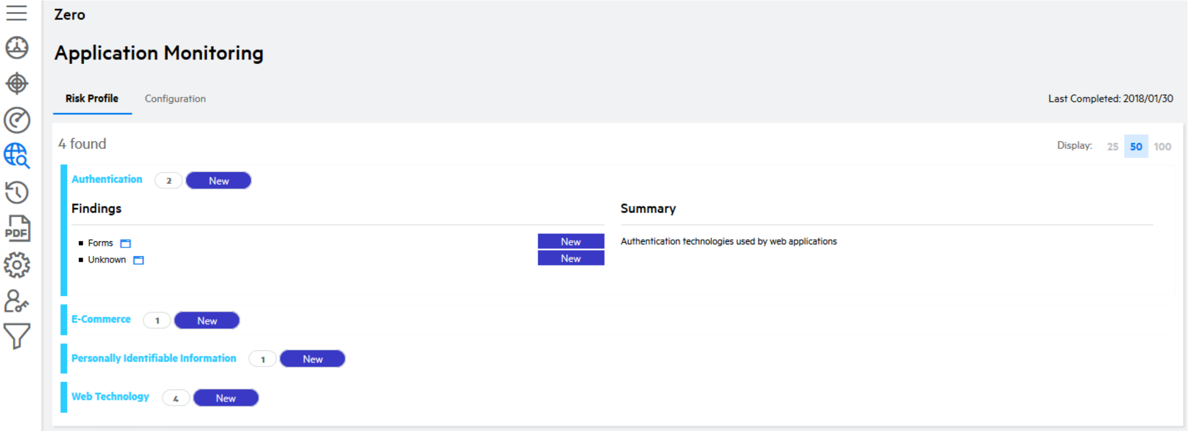
Risk profiling of an application searches for the following application characteristics: collection of personally identifiable information (PII), e-commerce functionality, authentication methods, and web technologies used in the application. You can view an application's risk profile from the most recent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

To view an application's risk profile:

1. Select the **Applications** view.

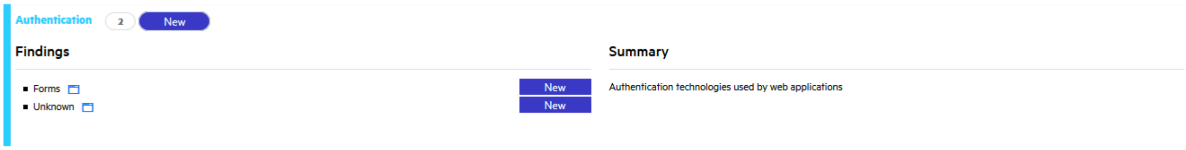
   Your Application page appears.
2. Click the name of an application that has Application Monitoring enabled and for which you want to view the risk profile.
3. Click **Application Monitoring**.

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



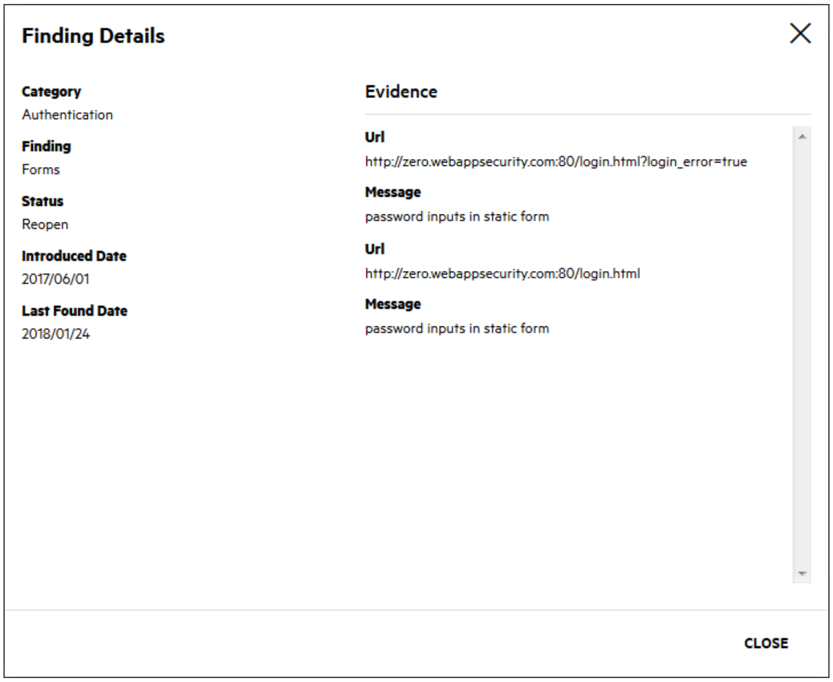
Authentication technologies used by web applications

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



Authentication technologies used by web applications

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



Finding Details

Category
Authentication

Finding
Forms

Status
Reopen

Introduced Date
2017/06/01

Last Found Date
2018/01/24

Evidence

Url
http://zero.webappsecurity.com:80/login.html?login_error=true

Message
password inputs in static form

Url
http://zero.webappsecurity.com:80/login.html

Message
password inputs in static form

Mobile Assessments

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

This section contains the following topics:

Supported Platforms and Operating Systems

Hardware Platforms

Fortify on Demand supports the following hardware platforms:

	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

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

	Mobile	Mobile+
Minimum iOS version (`MinimumOSVersion`)	N/A	Up to 15.7
Native iOS architecture	ARMv7, ARM64	ARMv7, ARM64
Minimum Android version (`android:minSdkVersion`)	N/A	Up to 32 (Android 12)
Native Android architecture	ARMv7, ARM64	ARMv7, ARM64

Preparing Mobile Assessment Files

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

This section contains the following topics:

Preparing Android Application Files (Binary)

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

- Make sure the application does not require MDM features.
- Provide the binary file in its entirety. Since only the submitted file is tested, features that require application updates are not supported.
- For assessments that include on-device testing (Mobile+), make sure that the submitted application can be installed and run on a physical device.

- To facilitate testing for Mobile+ assessments, disable any root detection, application tampering, or certificate pinning mechanisms. Leaving in these features might result in testing limitations that impact scan coverage.
- Mobile+ assessment of AAB files supports dynamic feature modules that have `<dist:fusing dist:include="true" />` specified in the manifest.
- **Important!** If you are submitting a subsequent scan of an application, either as a remediation scan or as a new scan, Fortify recommends keeping the application identifier (the package name) consistent in order to preserve the integrity of issue tracking between scans. The application identifier is used to calculate issue identifiers that track unique issues. Changing the application identifier between scans will result in many pre-existing issues showing up as “New” instead of “Existing” in the scan results.

Related Topics:

For information on uploading Android files for static assessments, see "Preparing Android Application Files (Source Code)" on page 107.

Preparing iOS Application Files (Binary)

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

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

  Important! The following distribution types are NOT supported:

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

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

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

Related Topics:

For information on preparing iOS source code files for upload, see "Preparing iOS Application Files (Source Code)" on page 107.

Preparing the Backend for Mobile Testing

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

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

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

Configuring a Mobile Scan

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

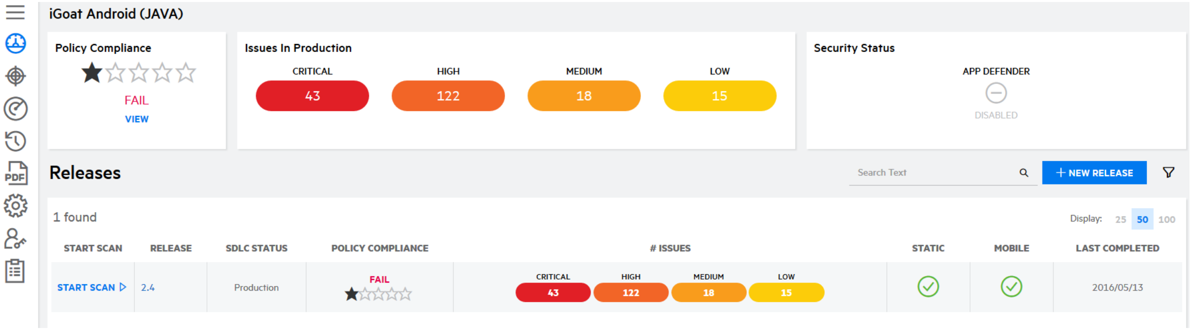
To set up a mobile scan:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click the name of the application.

   The Application Overview page appears.



iGoat Android (JAVA)

Policy Compliance: ★☆☆☆☆ FAIL VIEW

Issues In Production

CRITICAL	HIGH	MEDIUM	LOW
43	122	18	15

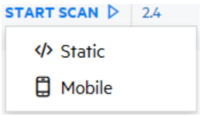
Security Status: APP DEFENDER DISABLED

Releases

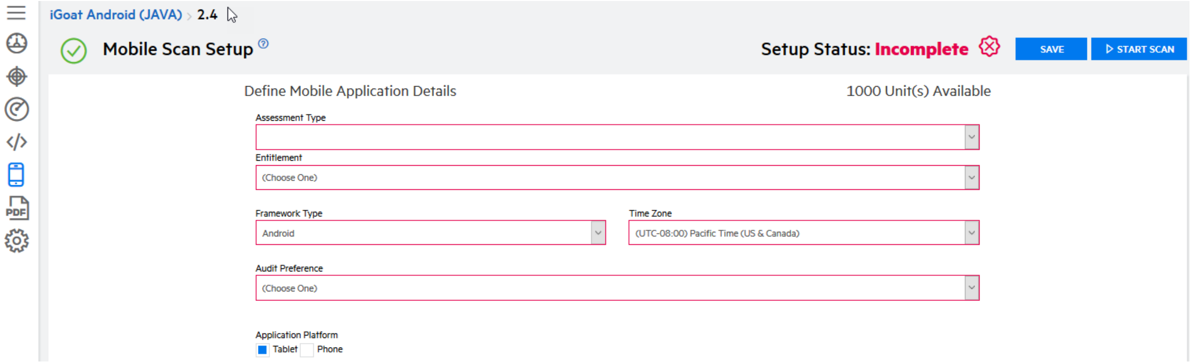
1 found

START SCAN	RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES	STATIC	MOBILE	LAST COMPLETED
START SCAN ▷	2.4	Production	FAIL ★☆☆☆☆	CRITICAL 43, HIGH 122, MEDIUM 18, LOW 15	✓	✓	2016/05/13

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.



iGoat Android (JAVA) > 2.4

Mobile Scan Setup

Setup Status: Incomplete

Define Mobile Application Details

1000 Unit(s) Available

Assessment Type:

Entitlement: (Choose One)

Framework Type: Android

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Audit Preference: (Choose One)

Application Platform: ■ Tablet □ Phone

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

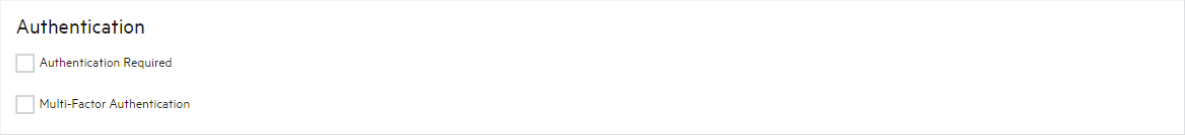
Field	Description
Assessment Type	Select the assessment type. Only assessment types allowed by the organization's security policy are displayed. The SLO of the selected assessment type appears below the field.
Entitlement	Select the entitlement that the assessment will use. The field displays entitlements 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.

Field	Description
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.
Application Platform	(Optional) Select your application's preferred platform: **Phone** and/or **Tablet**

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.



Authentication

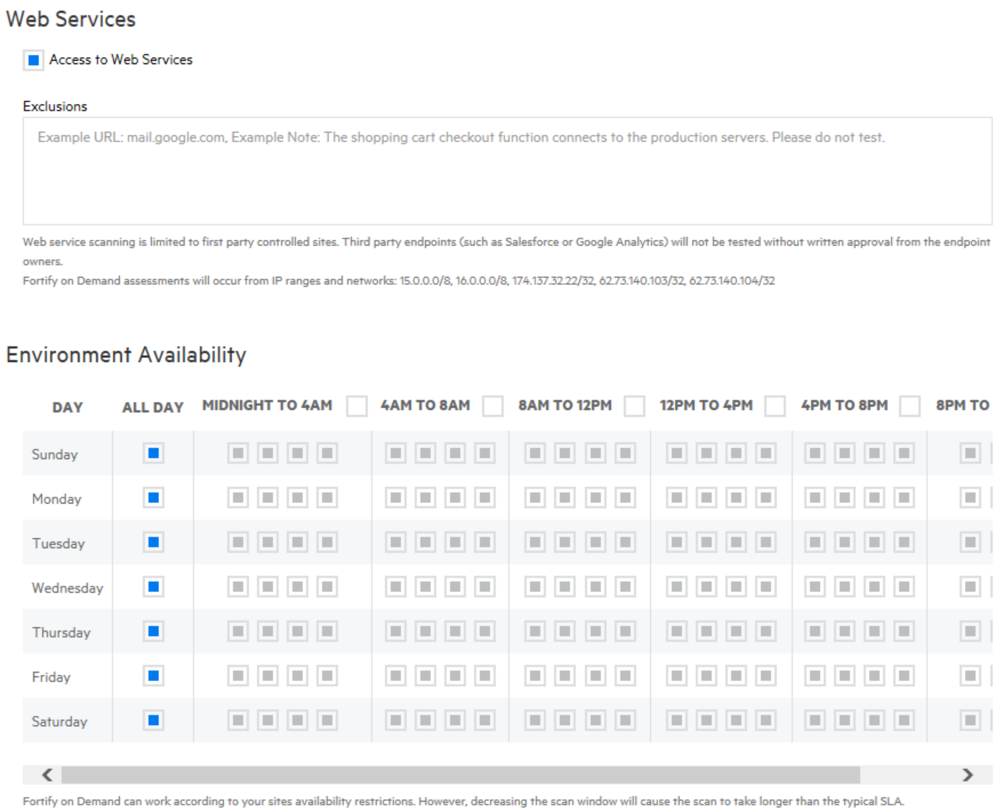
□ Authentication Required

□ Multi-Factor Authentication

Field	Description
Authentication	(Optional) Select the check box if authentication is required and enter user names and passwords of at least two users. To add more credentials, use the **Add additional [...] notes** field at the bottom of this form.
Multi-Factor Authentication	(Optional) Select the check box if multi-factor authentication is required and specify the details of your multi-factor authentication.

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

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



Web Services

☑ Access to Web Services

Exclusions

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

Web service scanning is limited to first party controlled sites. Third party endpoints (such as Salesforce or Google Analytics) will not be tested without written approval from the endpoint owners.
Fortify on Demand assessments will occur from IP ranges and networks: 15.0.0.0/8, 16.0.0.0/8, 174.137.32.22/32, 62.73.140.103/32, 62.73.140.104/32

Environment Availability

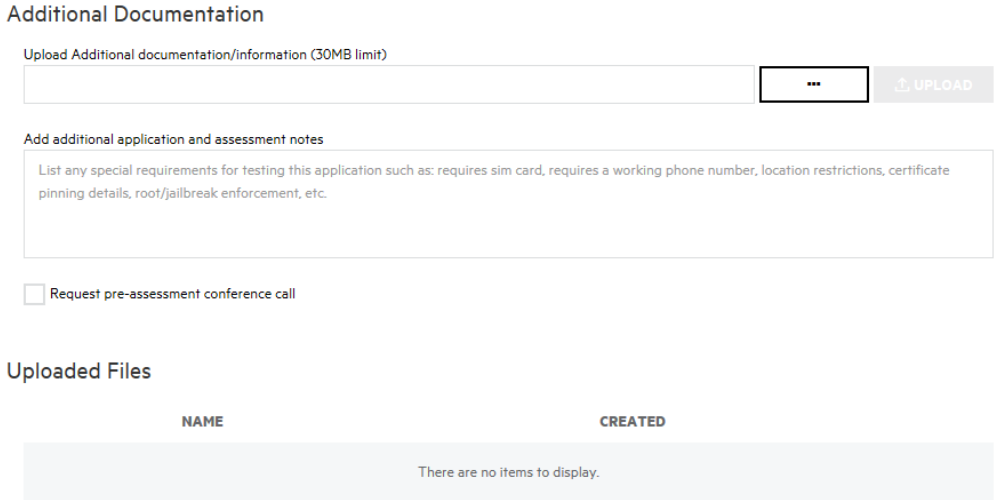
DAY	ALL DAY	MIDNIGHT TO 4AM ☐	4AM TO 8AM ☐	8AM TO 12PM ☐	12PM TO 4PM ☐	4PM TO 8PM ☐	8PM TO
Sunday	☑	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣
Monday	☑	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣
Tuesday	☑	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣
Wednesday	☑	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣
Thursday	☑	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣
Friday	☑	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣
Saturday	☑	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣ ▣ ▣ ▣	▣

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

Field	**Description**
Access to APIs	(Optional) Select the check box to allow Fortify on Demand to scan web APIs utilized by the application.
Exclusions	(Optional) List websites, backend web services, web APIs, or internal services the application talks to via HTTP/HTTPS that are to be excluded during the scan. This gives the testing team the correct context and boundaries for conducting the scan; domains not excluded that are discovered may be classified as vulnerabilities.
Environment Availability	Select the check boxes to indicate when the environment is available for testing. Use the local time of the time zone you specified above. Pausing and resuming testing causes the scan to take longer than the standard SLA typically allocated for a scan. Contact the support team for more information if you have site availability constraints. **Note:** Application modifications during blackout periods introduce uncertainty in the findings.

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

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



Additional Documentation

Upload Additional documentation/information (30MB limit)

Add additional application and assessment notes

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

□ Request pre-assessment conference call

Uploaded Files

NAME	CREATED
There are no items to display.	

Field	Description
Upload additional documentation/information (30MB limit)	(Optional) Upload documentation (30 MB limit) that facilitates testing of the application. Uploaded files are displayed in the **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.

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

Next Step:

"Scheduling the Mobile Scan Through the Portal" below

Scheduling the Mobile Scan Through the Portal

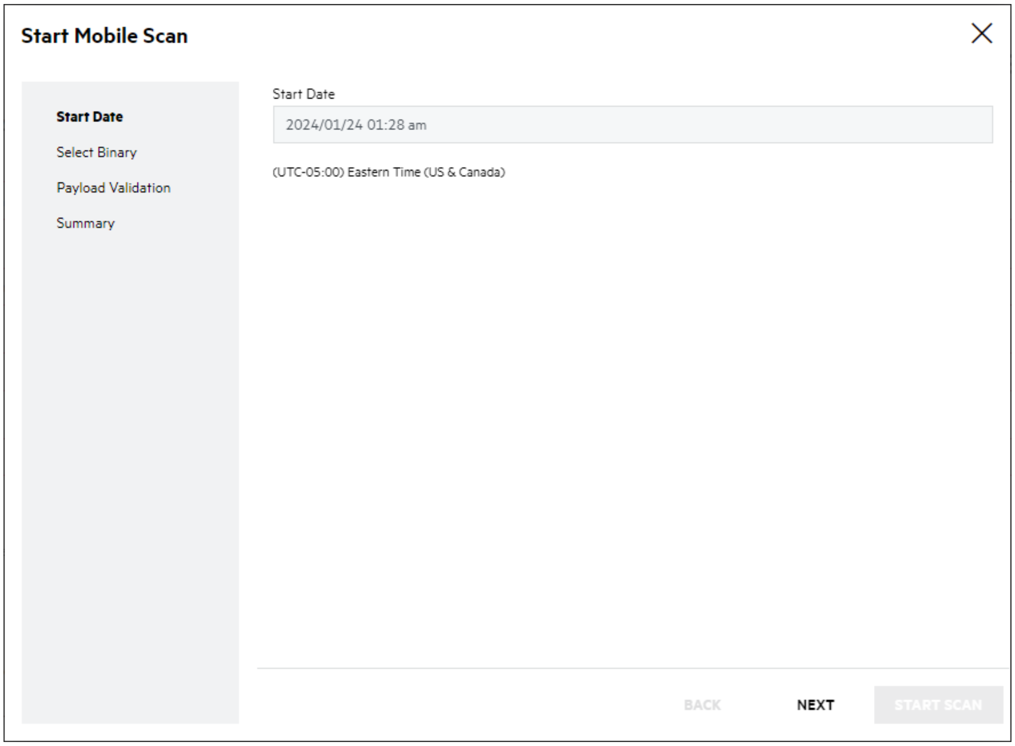
Once you have prepared your mobile application and configured the mobile scan settings, you can upload the payload and schedule the mobile scan. You can have only one in progress mobile scan across all releases of an application.

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.

   Start Mobile Scan

   Start Date: 2024/01/24 01:28 am

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

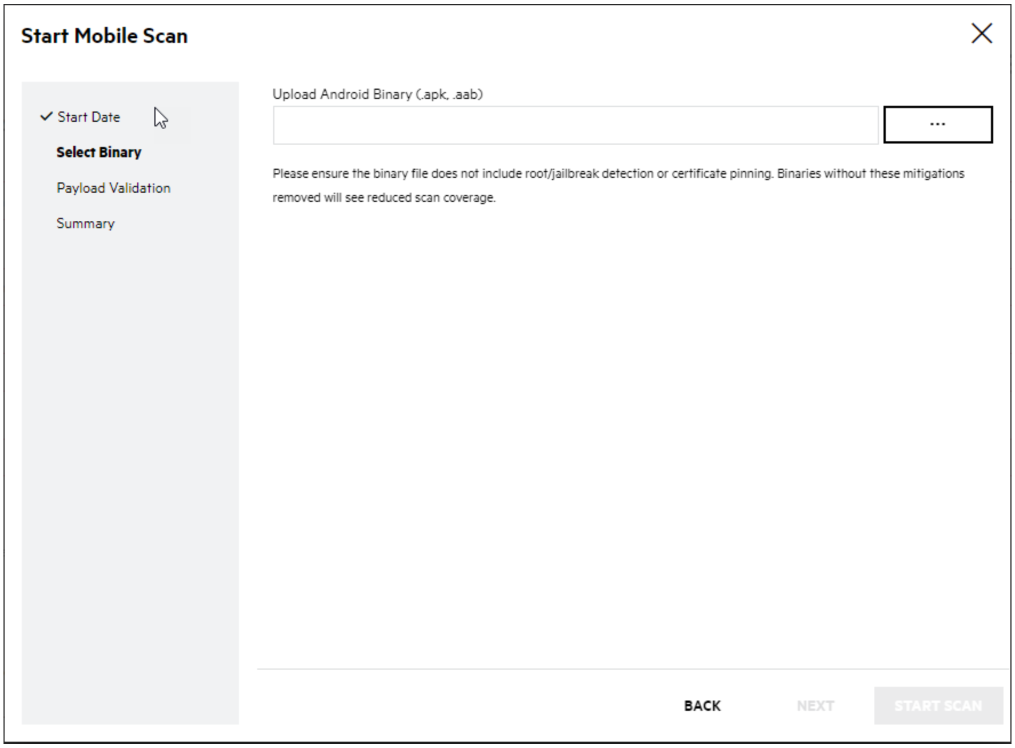
2. Click the **Start Date** field.

   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.

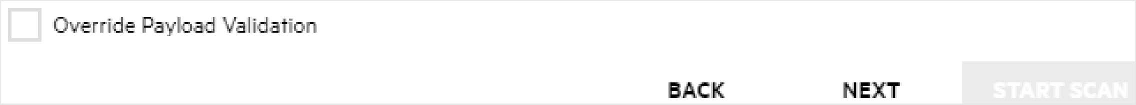


Upload Android Binary (.apk, .aab)

Please ensure the binary file does not include root/jailbreak detection or certificate pinning. Binaries without these mitigations removed will see reduced scan coverage.

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.

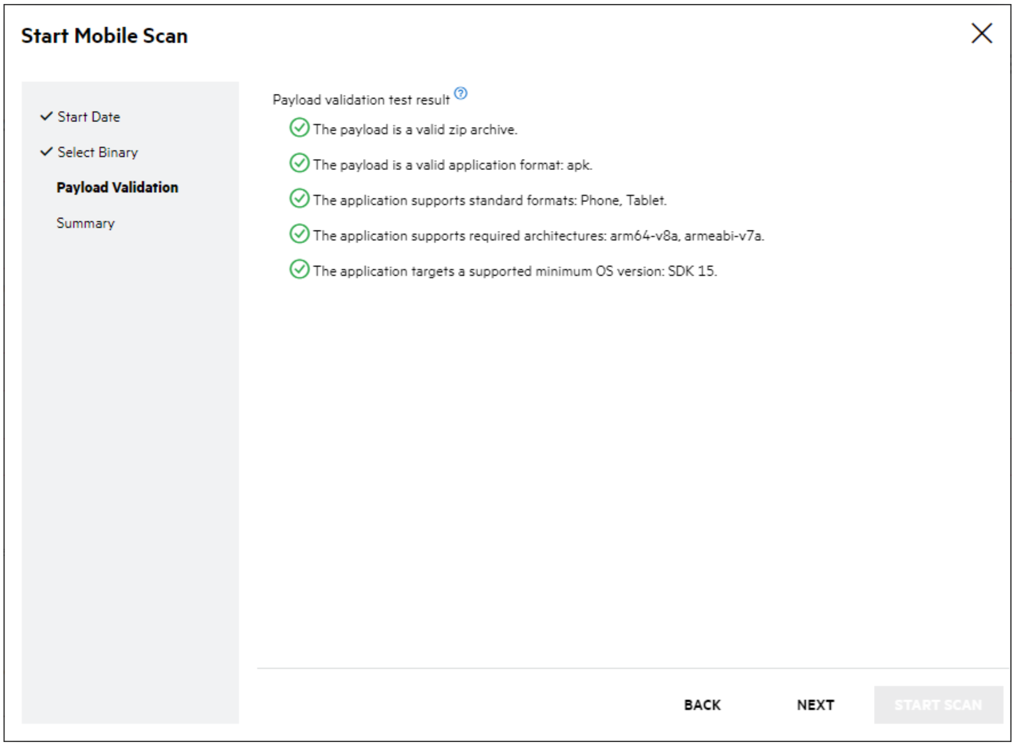


□ Override Payload Validation

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's bundle executable contains executable code. (Mobile+)
   - The IOS application's bundle executable is unencrypted. (Mobile+)
   - The iOS application's bundle executable runs on a physical device. (Mobile+)



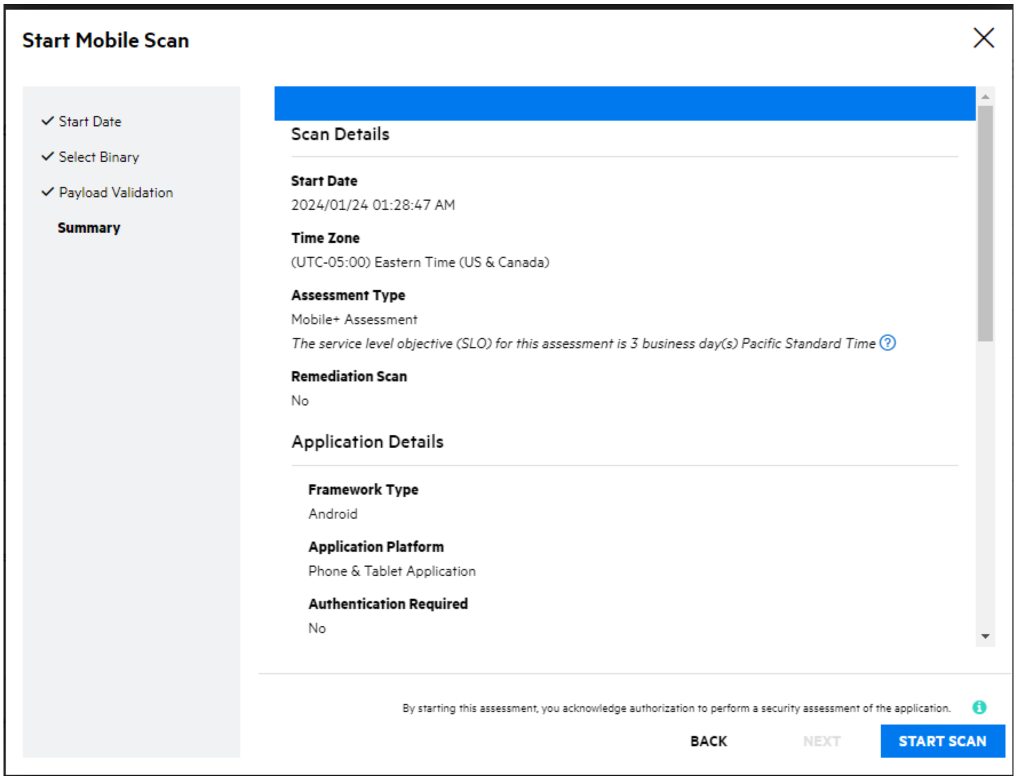
Payload validation test result

- ✓ The payload is a valid zip archive.
- ✓ The payload is a valid application format: apk.
- ✓ The application supports standard formats: Phone, Tablet.
- ✓ The application supports required architectures: arm64-v8a, armeabi-v7a.
- ✓ The application targets a supported minimum OS version: SDK 15.

Fortify 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.



Start Mobile Scan

Scan Details

Start Date
2024/01/24 01:28:47 AM

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

Assessment Type
Mobile+ Assessment
The service level objective (SLO) for this assessment is 3 business day(s) Pacific Standard Time

Remediation Scan
No

Application Details

Framework Type
Android

Application Platform
Phone & Tablet Application

Authentication Required
No

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

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.

Related Topics

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

- Fortify on Demand API. For more information, see "Fortify on Demand API" on page 317.

Editing Mobile Scan Settings for an Ongoing Scan

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

If you need to pause an in progress scan to edit the scan settings, create a Help Center ticket. The testing team will respond directly to the ticket with any updates. For more information on creating a Help Center ticket, see "Submitting a Help Center Ticket" on page 375.

Entitlement Consumption

The portal manages entitlement consumption. The available entitlement quantity is displayed on the Scan Setup pages. If you purchased scans, the number of available assessments is displayed. If you purchased assessment units, the unit cost of each assessment and the total number of available units across all entitlements are displayed.

When you start or schedule a scan, the cost is automatically deducted from your entitlement allotment. Single scans are deducted each time you perform a scan, whereas a subscription is deducted once and is then valid for the application until the subscription end date. You can identify an application that is under subscription because the entitlement cost is replaced with the subscription end date.

Additional entitlement information is available through the following sources:

- The entitlement consumption and active entitlements dashboard tiles. For more information, see "Dashboard Graph Types" on page 225.
- The entitlement consumption data export. For more information, see "Creating a Data Export Template" on page 249.
- Entitlements page under the Administration view. For more information, see "Viewing Entitlements" on page 268.

Managing Scans

You can manage scan activities at the tenant, application, and release levels. The Your Scans page displays scans across the tenant. Users can drill down into an application; the Applications Scans page displays scans ran against the application and the Release Scans page display scans ran against the release. The Scans pages, sharing a similar layout and functionality, provide a single view where users can review scan details and track scan progress.

This section contains the following topics:

Viewing All Scans

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

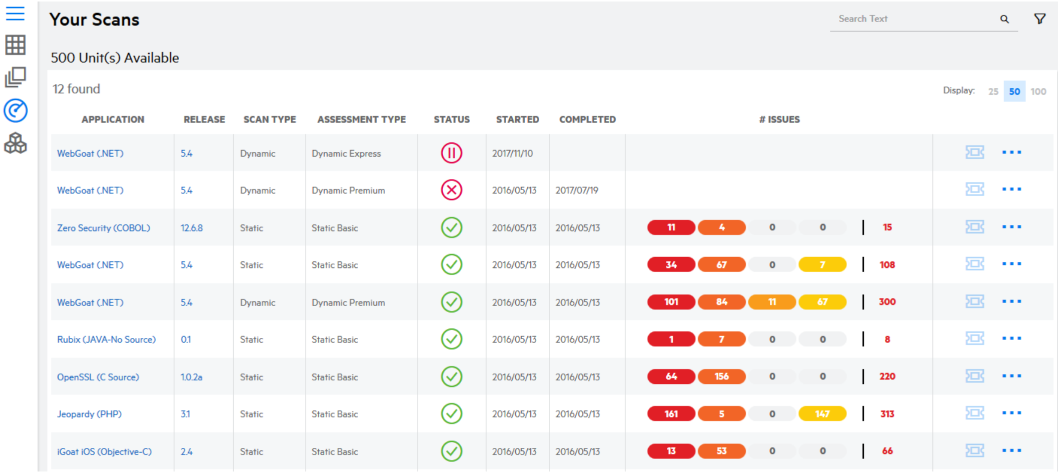
To view scans at the tenant level:

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.



Your Scans

500 Unit(s) Available

12 found

APPLICATION	RELEASE	SCAN TYPE	ASSESSMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES
WebGoat (.NET)	5.4	Dynamic	Dynamic Express	⏸	2017/11/10		
WebGoat (.NET)	5.4	Dynamic	Dynamic Premium	⊗	2016/05/13	2017/07/19	
Zero Security (COBOL)	12.6.8	Static	Static Basic	✓	2016/05/13	2016/05/13	11 4 0 0 | 15
WebGoat (.NET)	5.4	Static	Static Basic	✓	2016/05/13	2016/05/13	34 67 0 7 | 108
WebGoat (.NET)	5.4	Dynamic	Dynamic Premium	✓	2016/05/13	2016/05/13	101 84 11 67 | 300
Rubix (JAVA-No Source)	0.1	Static	Static Basic	✓	2016/05/13	2016/05/13	1 7 0 0 | 8
OpenSSL (C Source)	1.0.2a	Static	Static Basic	✓	2016/05/13	2016/05/13	64 156 0 0 | 220
Jeopardy (PHP)	3.1	Static	Static Basic	✓	2016/05/13	2016/05/13	161 5 0 147 | 313
iGoat iOS (Objective-C)	2.4	Static	Static Basic	✓	2016/05/13	2016/05/13	13 53 0 0 | 66

The following table describes how to navigate Your Scans page.

Viewing Application Scans

You can drill down into an application and view scans of only that application.

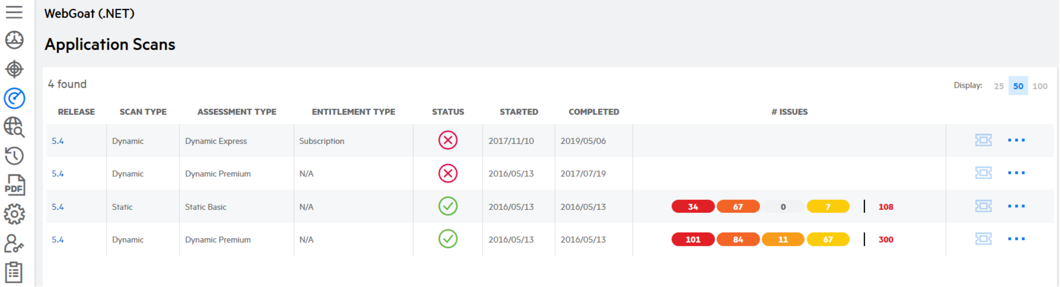
To view scans at the application level:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click the name of the application that you want to view scans ran against.
3. Click **Scans**.

   The Application Scans page appears, displaying scans ran against the application.



WebGoat (.NET)

Application Scans

4 found

RELEASE	SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES
5.4	Dynamic	Dynamic Express	Subscription	⊗	2017/11/10	2019/05/06	
5.4	Dynamic	Dynamic Premium	N/A	⊗	2016/05/13	2017/07/19	
5.4	Static	Static Basic	N/A	✓	2016/05/13	2016/05/13	34 67 0 7 | 108
5.4	Dynamic	Dynamic Premium	N/A	✓	2016/05/13	2016/05/13	101 84 11 67 | 300

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

Viewing Release Scans

You can drill down into a release and view scans of only that release.

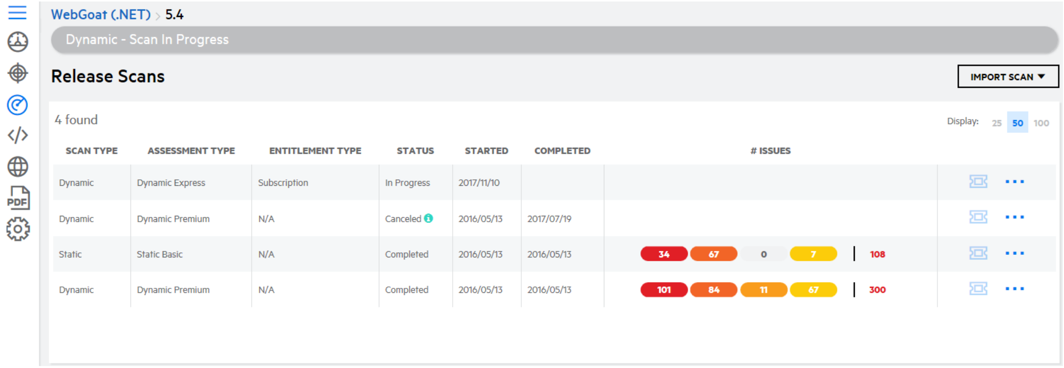
To view scans at the release level:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears.
3. Click the name of the release that you want to view scans ran against.
4. Click **Scans**.

   The Release Scans page appears, displaying scans ran against the release.



WebGoat (.NET) › 5.4

Dynamic - Scan In Progress

Release Scans

IMPORT SCAN ▼

4 found

Display: 25 50 100

SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES
Dynamic	Dynamic Express	Subscription	In Progress	2017/11/10		
Dynamic	Dynamic Premium	N/A	Canceled	2016/05/13	2017/07/19	
Static	Static Basic	N/A	Completed	2016/05/13	2016/05/13	34 67 0 7 | 108
Dynamic	Dynamic Premium	N/A	Completed	2016/05/13	2016/05/13	101 84 11 67 | 300

Navigating 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 "Searching Applications and Releases" on page 79.	Text search is only available on Your Scans page
Hide or display the filter list	Click ▼.	Filtering is only available on Your Scans page.

Task	Action	Notes
Expand or collapse filters	Click or the arrow next to the filter name.	
View Help Center tickets associated with a scan	Click 🎫.	
Request cancellation of an in progress scan	Click ... and select **Cancel Scan**. See "Canceling a Scan" on page 172.	
View scan summary	Click ... and select **Scan Summary**. The scan summary includes the scan ID and a comparison to the previous scan.	
View static scan notes	Click ... and select **Scan Notes**.	
Download scan results	Static, dynamic, and mobile: Click ... and select **Download Results**. Open source: Click ... and select **Download SBOM**.	
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	**Note:** 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.
Download dynamic scan site tree	Click ... and select **Download Site Tree**. Select **CSV** or **JSON** for the file type.	
View dynamic	Click ...and select **Detected Hosts**. Detected hosts are	

Task	Action	Notes
scan detected hosts	hosts that are referenced by the application but are not specified as allowed hosts.	
Download login macro used in dynamic scan	Click ... 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 ... and select **Download Scan Log**.	Scan log is available for DAST Automated scan.
Submit Debricked scan on SBOM	Click ... and select **Send to Debricked**. The SBOM must be available for download.	
Delete an imported scan	Click ... and **Cancel Imported Scan**. See "Deleting an Imported Scan" on page 352.	
Create a WAF export file	**Note:** 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" on page 373.

Filtering Your Scans page

You can limit the scans displayed on Your Scans page by applying filters. Filtering is only available at the tenant-level view.

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

To filter Your Scans page:

1. Navigate to Your Scans Page (see "Viewing All Scans" on page 167).
2. Click ▼ to display the filter list if it is not currently displayed.
3. Expand the filters that you want to apply.
4. Select your desired filter values. The following table describes the available filters.

Filter	Description	Values
Started on	Date range in which scans were started	
Completed on	Date range in which scans were completed	
Assessment type	Assessment type of the scan	
Entitlement Type	Entitlement type of the scan	Single Scan, N/A, Subscription, Remediation
Is Remediation	Whether the scan is a remediation scan	False, True
Release	Release associated with the scan	
Scan Status	Status of static, dynamic, mobile, and network scans	In Progress, Completed, Canceled, Waiting
Scan Type	Scan type	Static, Dynamic, Mobile, Network, Open Source, Application Monitoring

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

Checking the Scan Status

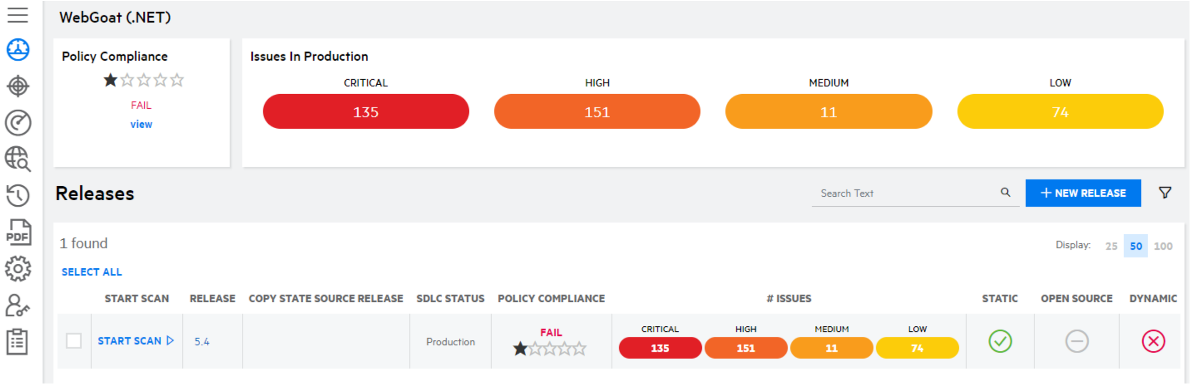
Release owners, scan submitters, and users on an application's notification list receive email notifications of the following scan status updates to an application: scan start, scan completion, scan cancellation, scan pause. You can also check the scan status in the portal.

To check a scan status for an application:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of the application for which you want to check the scan status.

The Application Overview page appears.



WebGoat (.NET)

Policy Compliance
★☆☆☆☆
FAIL
view

Issues In Production

CRITICAL	HIGH	MEDIUM	LOW
135	151	11	74

Releases

Search Text
+ NEW RELEASE

1 found

Display: 25 50 100

SELECT ALL

	START SCAN	RELEASE	COPY STATE SOURCE RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES	STATIC	OPEN SOURCE	DYNAMIC
□	START SCAN ▷	5.4		Production	FAIL ★☆☆☆☆	CRITICAL 135 HIGH 151 MEDIUM 11 LOW 74	✓	⊖	⊗

3. Hover over a scan status icon to view a tooltip with additional information about the most recent scan of that type across releases.
4. Click a status icon to directly access the scan status details:
   - Not Started: you are redirected to the relevant Scan Setup page.
   - Scheduled: you are redirected to the relevant Scan Setup page.
   - In Progress: you are redirected to the Release Scans page or the Application Scans page if a microservice application has queued static scans.
   - Queued: you are redirected to the relevant Scan Setup page.
   - Paused: you are redirected to the Help Center Tickets window on the Release Scans page.
   - Canceled: you are redirected to the relevant Scan Setup page.
   - Completed: you are redirected to the Release Issues page (static, dynamic, and mobile scans) or the Application Issues page (Application Monitoring scans), filtered by the relevant scan type.

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

Canceling a Scan

You might need to cancel a scan that has not been started or has been started but has not been completed. The portal automates processing of the cancellation request. The entitlement cost will be refunded if a refund is deemed appropriate.

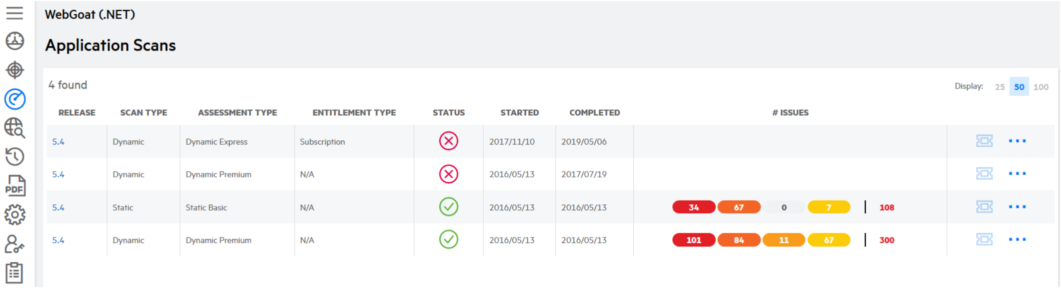
To cancel a scan:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of the application for which you want to cancel a scan.

   The Releases page appears.
3. Click **Scans**.

The Application Scans page appears.



WebGoat (.NET)

Application Scans

4 found

RELEASE	SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES	
5.4	Dynamic	Dynamic Express	Subscription	⊗	2017/11/10	2019/05/06		···
5.4	Dynamic	Dynamic Premium	N/A	⊗	2016/05/13	2017/07/19		···
5.4	Static	Static Basic	N/A	✓	2016/05/13	2016/05/13	34 67 0 7 | 108	···
5.4	Dynamic	Dynamic Premium	N/A	✓	2016/05/13	2016/05/13	101 84 11 67 | 300	···

4. Click ··· in the row of the scan and select **Cancel Scan**.

   A confirmation message displays.

5. Click **Yes** to confirm the scan cancellation.

   - For a scan with a **Queued** or **Scheduled** status, the scan is automatically canceled.
   - For a scan with an **In Progress** status:
     - If the scan is an application monitoring scan or static scan that has not been audited, it is automatically cancelled.
     - If the scan is a dynamic scan, mobile scan, or static scan under audit, a Help Center ticket is generated that includes the cancellation request and scan details. An email is sent to the 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.

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

Resuming a Paused Scan

The testing team will pause a scan if additional information is needed. Respond to the associated Help Center ticket so the scan can be resumed. Note that 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.

Viewing Help Center Tickets Linked to a Scan

You can directly view Help Center tickets linked to an active scan from the Your Scans, Application Scans, and Release Scans pages.

> **Note**: If a scan has been paused, you can access associated Help Center tickets from any release-level page by clicking the **Help Center Tickets** button located in the status bar.

To view Help Center tickets linked to an active scan:

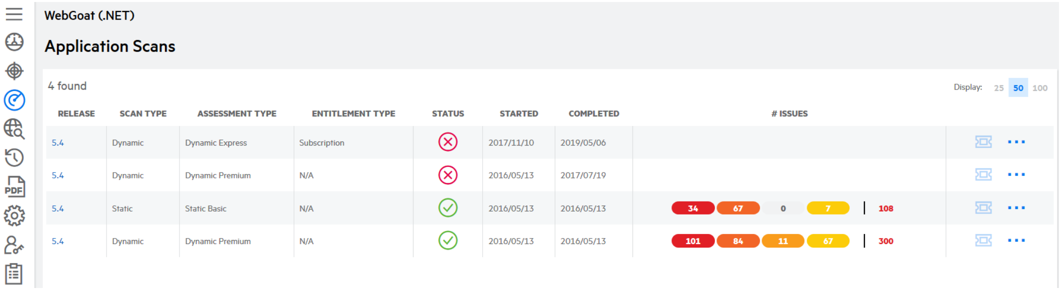
1. Select the **Applications** view.

   Your Applications page appears.

2. Click the name of the application.

3. Click **Scans**.

   The list of all scans ran against the application or release appears.



WebGoat (.NET)

Application Scans

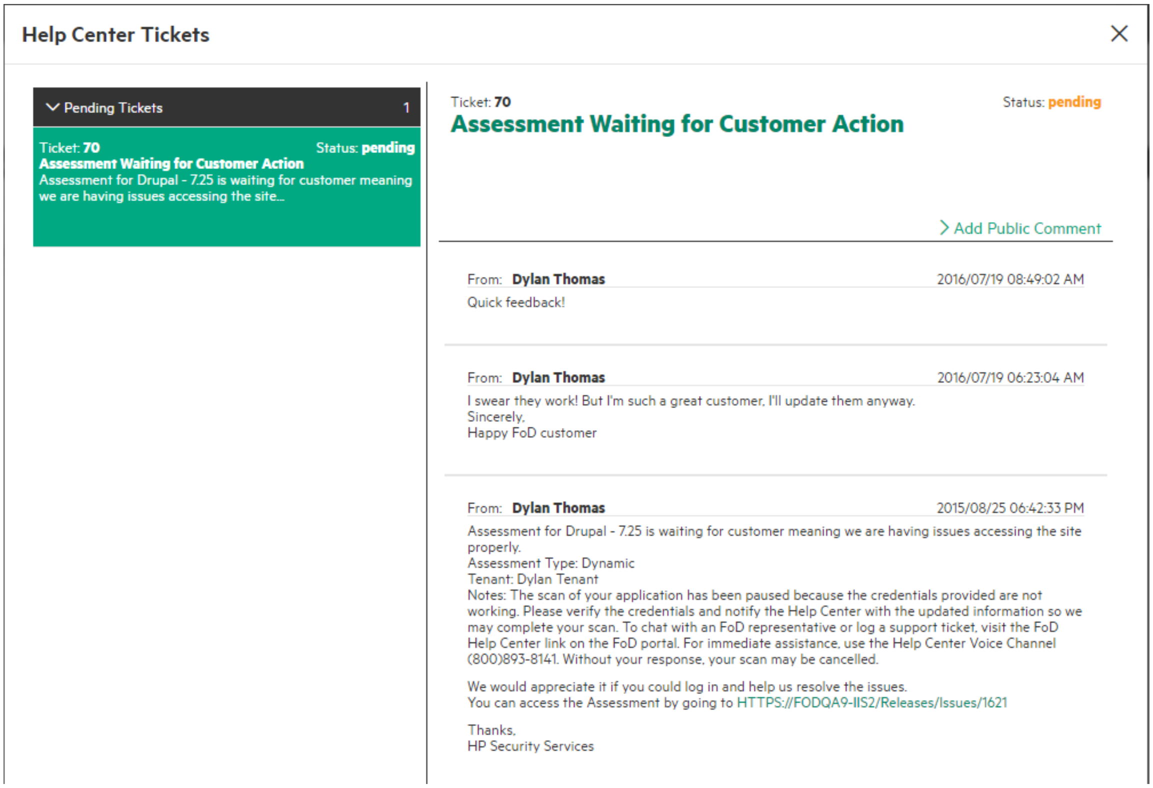
4 found

Display: 25 50 100

RELEASE	SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES		
5.4	Dynamic	Dynamic Express	Subscription	⊗	2017/11/10	2019/05/06			···
5.4	Dynamic	Dynamic Premium	N/A	⊗	2016/05/13	2017/07/19			···
5.4	Static	Static Basic	N/A	✓	2016/05/13	2016/05/13	34 67 0 7 | 108		···
5.4	Dynamic	Dynamic Premium	N/A	✓	2016/05/13	2016/05/13	101 84 11 67 | 300		···

4. Click the icon.

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



Help Center Tickets

Ticket: **70** Status: **pending**
Assessment Waiting for Customer Action
Assessment for Drupal - 7.25 is waiting for customer meaning we are having issues accessing the site...

Ticket: **70** Status: **pending**

Assessment Waiting for Customer Action

From: **Dylan Thomas** 2016/07/19 08:49:02 AM
Quick feedback!

From: **Dylan Thomas** 2016/07/19 06:23:04 AM
I swear they work! But I'm such a great customer, I'll update them anyway.
Sincerely,
Happy FoD customer

From: **Dylan Thomas** 2015/08/25 06:42:33 PM
Assessment for Drupal - 7.25 is waiting for customer meaning we are having issues accessing the site properly.
Assessment Type: Dynamic
Tenant: Dylan Tenant
Notes: The scan of your application has been paused because the credentials provided are not working. Please verify the credentials and notify the Help Center with the updated information so we may complete your scan. To chat with an FoD representative or log a support ticket, visit the FoD Help Center link on the FoD portal. For immediate assistance, use the Help Center Voice Channel (800)893-8141. Without your response, your scan may be cancelled.

We would appreciate it if you could log in and help us resolve the issues.
You can access the Assessment by going to HTTPS://FODQA9-IIS2/Releases/Issues/1621

Thanks,
HP Security Services

5. In the Pending tickets section, click a ticket to view its comments.
6. Click **Add Public Comment**.

   A text box appears below.
7. Type a comment that will be added to the ticket.
8. Click **+ Add Public Comment**.

   The comment is added to the ticket details in both the portal and Help Center.

Chapter 5: Remediating Vulnerabilities

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

This section contains the following topics:

Reviewing Issues

You can view detailed information about the issues that were found in a scan at both the application and release levels. The Application Issues page displays issues found across all releases of an application (excluding retired releases) as well as Application Monitoring issues. The Release Issues page displays issues found across all scans of a release.

The Application Issues and Release Issues pages, sharing a similar layout and functionality, provide a single, consolidated view of issue data. A page is split into three panels:

- The navigation panel displays a list of the issues. Issues are organized by severity, with a tab for each severity level and a tab for all issues.
- The issue details panel displays details of the issue selected in the navigation panel. Details are organized among several tabs. The tabs that are available depend on the scan type in which the issue was found.
- The audit panel is collapsible. It displays user-remediation fields of the issue selected in the navigation panel as well as the issue status, the date the issue was introduced, and the date the issue was last found.

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,

Status	Description
	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. By default, Fortify on Demand doesn't show **Fixed** vulnerabilities—only issues from the most recent scan of a given type. To see **Fixed** vulnerabilities, select **Show... Fixed** on the Release Overview and Issues pages.

This section contains the following topics:

Viewing Application Issues

You can view issues from all releases (excluding retired releases) of an application, along with Application Monitoring issues.

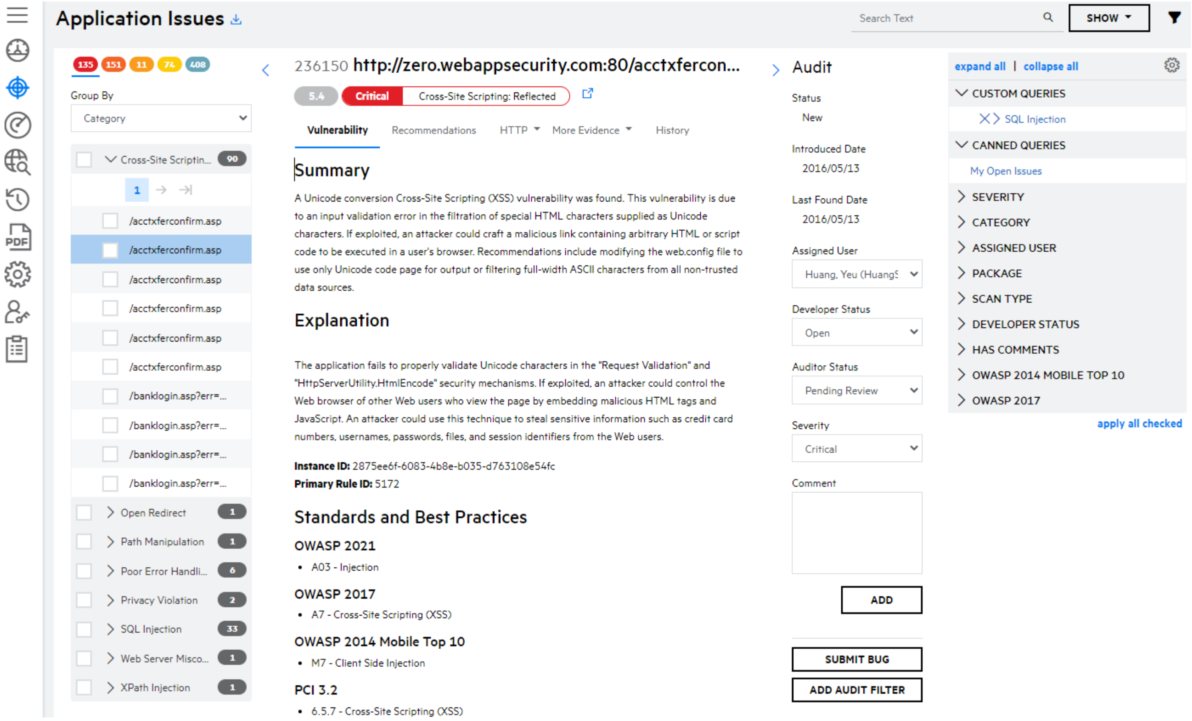
To view issues at the application level:

1. Select the **Applications** view.

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

   The Application Overview page appears.
3. Click **Issues**.

   The Application Issues page appears. Within a grouping, issues are sorted by file name, then line number. Issues with the same instance ID across multiple releases are combined in a single view.



236150 http://zero.webappsecurity.com:80/acctxfercon...

5.4 Critical Cross-Site Scripting: Reflected

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021
- A03 - Injection

OWASP 2017
- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10
- M7 - Client Side Injection

PCI 3.2
- 6.5.7 - Cross-Site Scripting (XSS)

Audit

Status
New

Introduced Date
2016/05/13

Last Found Date
2016/05/13

Assigned User
Huang, Yeu (Huang$

Developer Status
Open

Auditor Status
Pending Review

Severity
Critical

Comment

Viewing Release Issues

You can view issues from a release of an application, including open source scan issues and on-premises scan issues.

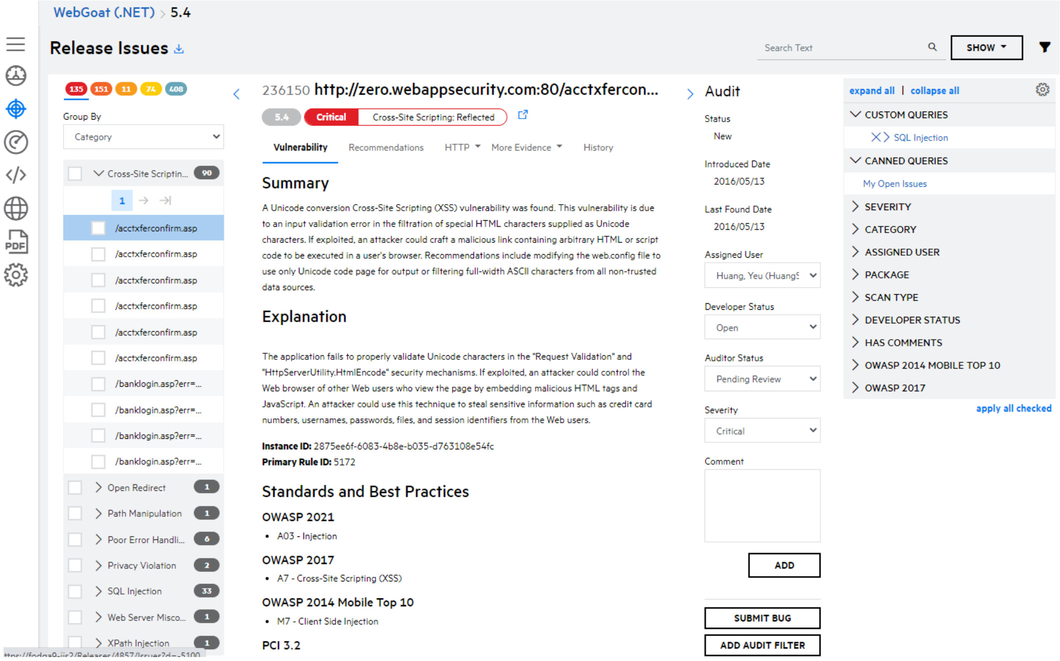
To view issues at the release level:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears.
3. Select a release from your list.
4. Click **Issues**.

   The Release Issues page appears. Within a grouping, issues are sorted by file name, then line number.



236150 http://zero.webappsecurity.com:80/acctxfercon...

5.4 Critical Cross-Site Scripting: Reflected

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021
- A03 - Injection

OWASP 2017
- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10
- M7 - Client Side Injection

PCI 3.2

Audit

Status: New
Introduced Date: 2016/05/13
Last Found Date: 2016/05/13
Assigned User: Huang, Yeu (HuangS
Developer Status: Open
Auditor Status: Pending Review
Severity: Critical
Comment:

Navigating the Issues Page

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

General Navigation

Task	Action
Export issue data	Click ⤓. 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**.
Hide or display the filter list	Click ▼.
Show or hide	Click **Show... Fixed** to switch between showing and hiding Fix Validated issues.

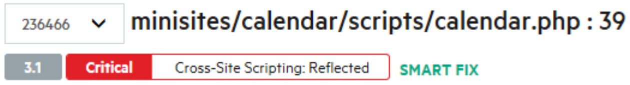
Task	Action
fixed issues	
Show or hide suppressed issues	Click **Show... Suppressed** to switch between showing or hiding Suppressed issues.
Save applied filters as query	Click **Save Query**.
Remove applied filters	Click **X** or **Clear Filters**.

Navigation Panel

Task	Action
Expand or collapse the panel	Click › or ‹.
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 the right and left 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

Task	Action
	issue specific to that release.  236466 ⌄ minisites/calendar/scripts/calendar.php : 39 3.1 Critical Cross-Site Scripting: Reflected SMART FIX
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"Issue Details " on page 186

Audit Panel

Task	Action
Expand or collapse the panel	Click > or <.
Edit an issue	Edit the available fields. For more information, see "Updating Issues" on page 198.
Submit an issue to a bug tracker	Click **Submit Bug**. For more information, see "Submitting Issues to the Bug Tracker" on page 344.
Add an audit filter for an issue	Click **Add Audit Filter**. For more information, see "Creating an Application Audit Template Filter for an Issue" on page 213.

Filter List

Task	Action
Expand or collapse filters	Click expand all | collapse all ⚙ or the arrow next to the filter name.
Apply a filter	Select a filter value. Click **Apply** if applicable. For more information, see "Filtering the Issues Page" on the next page.
Customize filter and grouping selections	Click ⚙. For more information, see "Customizing Issue Filters and Groupings" on page 184

Filtering the Issues Page

You can limit the issues displayed on the Application Issues page or the Release Issues page by applying filters.

To filter the Issues page:

1. Click ▼ to display the filter list if it is not currently displayed.
2. Expand the filter(s) you want to apply.
3. Select the filter values that you want to filter for. The following table describes issue filters and their values.

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

Filter	Description	Values
Assigned User	User defined	Not Set, User-defined
Auditor Status	Auditor issue remediation status. For more information, see "Audit Workflow for Auditors" on page 205.	Pending Review, Remediation Required, Remediation Referred, Risk Mitigated, Risk Accepted Not an Issue
Bug Submitted	Issue was submitted as a bug to a bug tracker.	False, True
Category	Issue category	
Canned Queries	Default queries	My Open Issues
Custom Queries	User-defined queries	User-defined
Developer Status	Developer issue remediation status.	Challenged, Open, IN Remediation, Remediated, Will Not Fix, Third Party Component
DISA STIG 4.11	DISA Application Security and Development STIG v4.11	

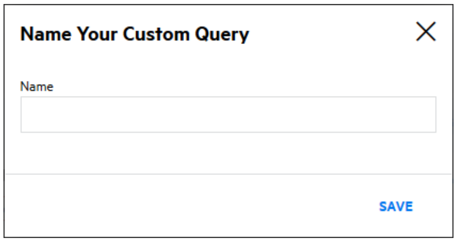
Filter	Description	Values
DISA STIG 5.1	DISA Application Security and Development STIG v5.1	
Has Attachments		False, True
Has Comments		False, True
Has Notes		False, True
Introduced Date	Original date of issue creation	
Issue Age	Number of days the issue has been present in the application. The categories are cumulative. For example, an issue that is counted as greater than 30 days old is also part of the count for greater than 10 days old.	>/< 5 days, >/< 10 days, >/< 30 days, >/< 60 days, >/< 45 days, >/< 90 days
OWASP 2013	OWASP top 10 2013 classification	
OWASP 2014 Mobile	OWASP mobile top 10 2014 classification	
OWASP 2017	OWASP top 10 2017 classification	
OWASP 2021	OWASP top 10 2021 classification	
OWASP ASVS 4.0	OWASP ASVS 4.0 classification	
Package		
Release	**Note:** The **Release** filter appears only on the Application Issues page. Release in which the issue was identified	
Scan Tool	Scan tool used to find issue	DAST, SAST, MAST, Debricked, Sonatype
Scan Type	Scan type to which issue belongs	Application Monitoring,

Filter	Description	Values
		Dynamic, Static, Mobile, Open Source
Severity	Issue severity	Critical, High, Medium, Low, Best Practice, Info
Status	Issue status	New, Existing, Reopen, Fixed/Fix Validated
<Custom issue attribute>	Issue attributes that are picklists	User-defined

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

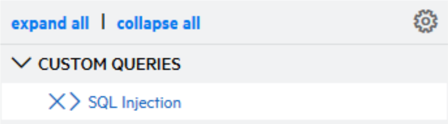
4. To save the currently applied filters for reuse, click **Save Query**.

   The Name Your Custom Query window opens.



5. Type a name for the query and click **Save**.

   Your saved custom query appears in the **Custom Queries** filter. You can reapply the query at any time by selecting the query from the filters list.



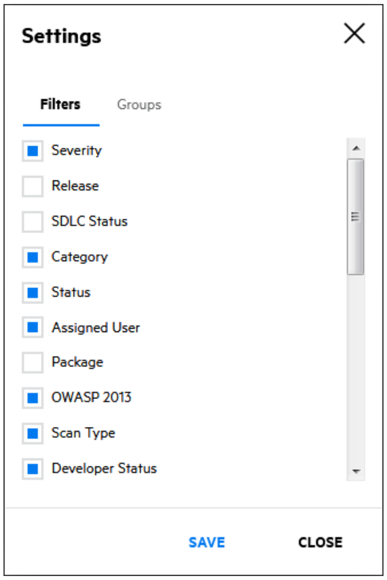
Customizing Issue Filters and Groupings

You can customize issue filters and groupings on the Application Issues or Release Issues page.

To customize issue filters and groupings:

1. In the audit panel, click ⚙.

   The Settings window appears.



☑ Severity
□ Release
□ SDLC Status
☑ Category
☑ Status
☑ Assigned User
□ Package
☑ OWASP 2013
☑ Scan Type
☑ Developer Status

2. Perform the relevant task:

Task	Procedure
Customize issue filters	a. Select the **Filters** tab. b. Select the check boxes next to filters you want to add. c. Deselect the check boxes next to filters you want to remove. d. 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 navgiation panel)	a. Select **Groups**. b. Select the check boxes next to values you want to add to the **Group By** list. c. Deselect the check boxes next to values you want to remove from the **Group By** list. d. Click **Save**. The Issues page refreshes with the new group values.

Issue Details

The issue details panel on the Application Issues or Release Issues page provides comprehensive issue details that help you analyze the vulnerabilities found in the application. The details are organized among several tabs. The available tabs depend on the scan type in which the issue was found.

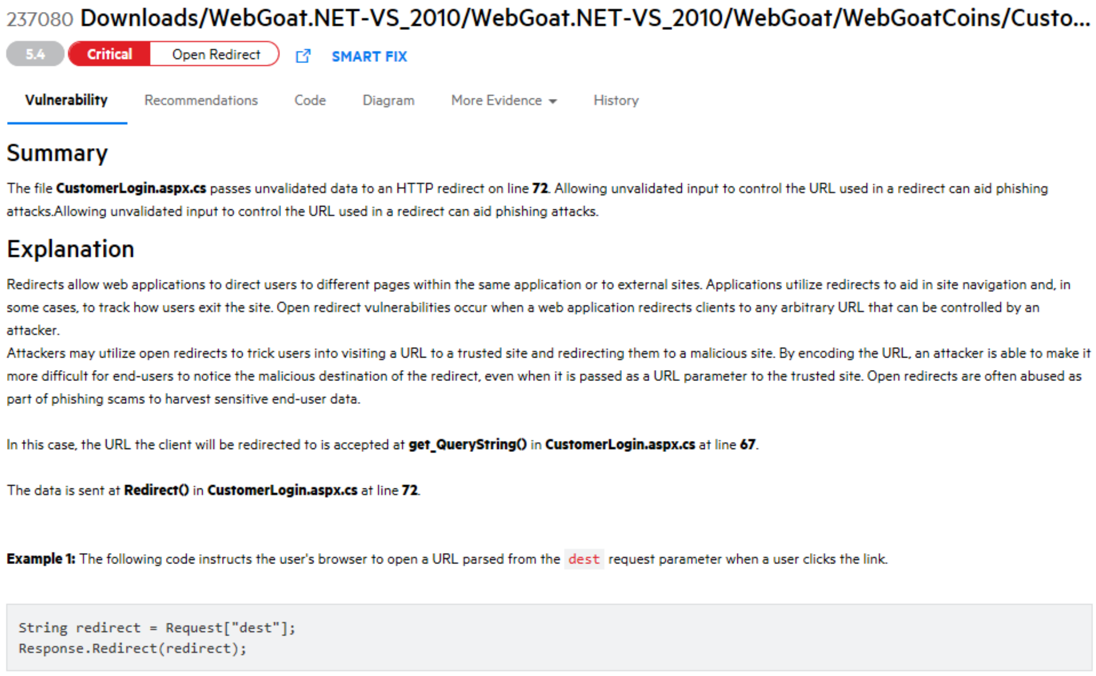
This section covers the following topics:

Static Scan Issue Details

The issue details panel for a static scan issue displays the issue ID, issue location, issue severity, and issue category across the top. Several tabs below provide additional information about the issue, including technical details, line of code (if source code was submitted), and an analysis trace diagram.

Vulnerability

The **Vulnerability** tab displays the following technical details about the issue: issue summary; explanation of the execution and implications of the issue; instance ID and rule ID; and standards and best practices information from Fortify Software Security Research.



Summary

The file **CustomerLogin.aspx.cs** passes unvalidated data to an HTTP redirect on line **72**. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

Explanation

Redirects allow web applications to direct users to different pages within the same application or to external sites. Applications utilize redirects to aid in site navigation and, in some cases, to track how users exit the site. Open redirect vulnerabilities occur when a web application redirects clients to any arbitrary URL that can be controlled by an attacker.
Attackers may utilize open redirects to trick users into visiting a URL to a trusted site and redirecting them to a malicious site. By encoding the URL, an attacker is able to make it more difficult for end-users to notice the malicious destination of the redirect, even when it is passed as a URL parameter to the trusted site. Open redirects are often abused as part of phishing scams to harvest sensitive end-user data.

In this case, the URL the client will be redirected to is accepted at **get_QueryString()** in **CustomerLogin.aspx.cs** at line **67**.

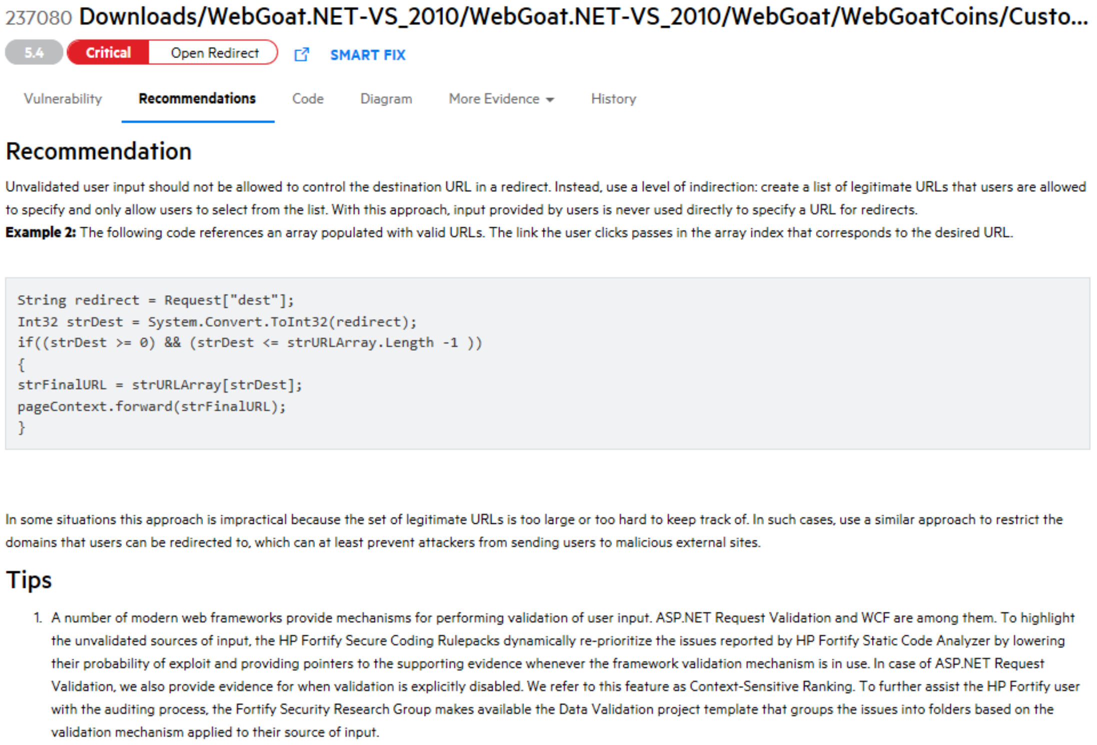
The data is sent at **Redirect()** in **CustomerLogin.aspx.cs** at line **72**.

Example 1: The following code instructs the user's browser to open a URL parsed from the `dest` request parameter when a user clicks the link.

```
String redirect = Request["dest"];
Response.Redirect(redirect);
```

Recommendations

The **Recommendations** tab displays recommendations to remediate the issue, along with tips and references for further research. If available, the **Interactive Training** section contains 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" on page 353.



Recommendation

Unvalidated user input should not be allowed to control the destination URL in a redirect. Instead, use a level of indirection: create a list of legitimate URLs that users are allowed to specify and only allow users to select from the list. With this approach, input provided by users is never used directly to specify a URL for redirects.

Example 2: The following code references an array populated with valid URLs. The link the user clicks passes in the array index that corresponds to the desired URL.

```
String redirect = Request["dest"];
Int32 strDest = System.Convert.ToInt32(redirect);
if((strDest >= 0) && (strDest <= strURLArray.Length -1 ))
{
strFinalURL = strURLArray[strDest];
pageContext.forward(strFinalURL);
}
```

In some situations this approach is impractical because the set of legitimate URLs is too large or too hard to keep track of. In such cases, use a similar approach to restrict the domains that users can be redirected to, which can at least prevent attackers from sending users to malicious external sites.

Tips

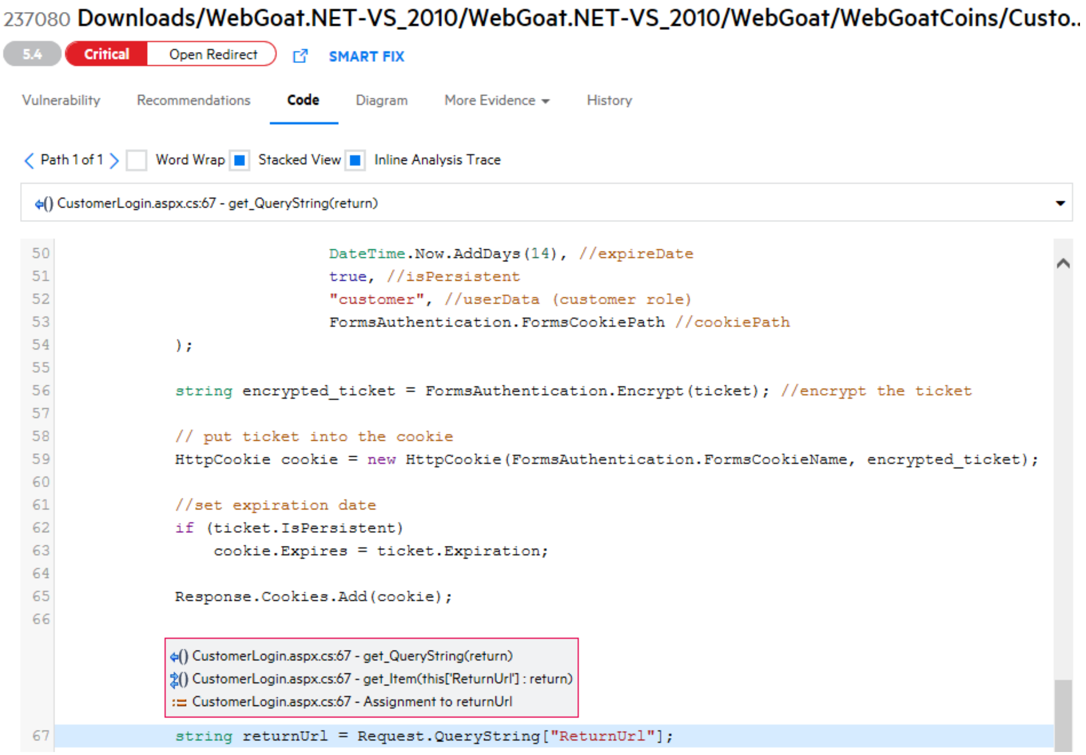
1. A number of modern web frameworks provide mechanisms for performing validation of user input. ASP.NET Request Validation and WCF are among them. To highlight the unvalidated sources of input, the HP Fortify Secure Coding Rulepacks dynamically re-prioritize the issues reported by HP Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. In case of ASP.NET Request Validation, we also provide evidence for when validation is explicitly disabled. We refer to this feature as Context-Sensitive Ranking. To further assist the HP Fortify user with the auditing process, the Fortify Security Research Group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

Code

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

- Enable or disable word wrap
- Cycle through multiple analysis traces, if applicable
- Switch between a stacked view of the code and tree view of the analysis trace alongside the code
- Jump to the line of code when selecting an analysis 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.



237080 Downloads/WebGoat.NET-VS_2010/WebGoat.NET-VS_2010/WebGoat/WebGoatCoins/Custo..

☐ Word Wrap ■ Stacked View ■ Inline Analysis Trace

() CustomerLogin.aspx.cs:67 - get_QueryString(return)

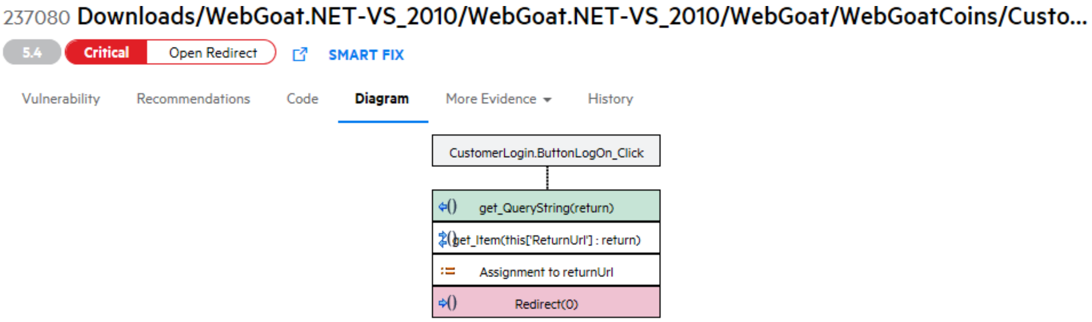
```
                DateTime.Now.AddDays(14), //expireDate
                true, //isPersistent
                "customer", //userData (customer role)
                FormsAuthentication.FormsCookiePath //cookiePath
);

string encrypted_ticket = FormsAuthentication.Encrypt(ticket); //encrypt the ticket

// put ticket into the cookie
HttpCookie cookie = new HttpCookie(FormsAuthentication.FormsCookieName, encrypted_ticket);

//set expiration date
if (ticket.IsPersistent)
    cookie.Expires = ticket.Expiration;

Response.Cookies.Add(cookie);

```

() CustomerLogin.aspx.cs:67 - get_QueryString(return)
() CustomerLogin.aspx.cs:67 - get_Item(this['ReturnUrl'] : return)
:= CustomerLogin.aspx.cs:67 - Assignment to returnUrl

```
string returnUrl = Request.QueryString["ReturnUrl"];
```

Diagram

The **Diagram** tab displays an analysis trace diagram of the issue.



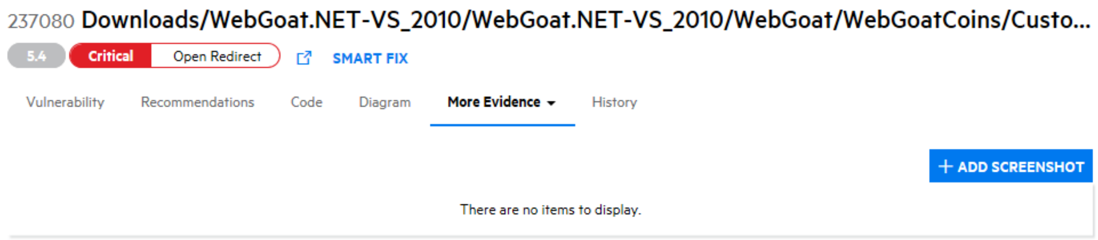
237080 Downloads/WebGoat.NET-VS_2010/WebGoat.NET-VS_2010/WebGoat/WebGoatCoins/Custo...

5.4
Critical
Open Redirect
SMART FIX
Vulnerability
Recommendations
Code
Diagram
More Evidence
History
CustomerLogin.ButtonLogOn_Click
() get_QueryString(return)
() get_Item(this['ReturnUrl'] : return)
:= Assignment to returnUrl
() Redirect(0)

More Evidence

The **More Evidence** tab contains notes and screenshots, which are accessed separately through the drop-down menu.

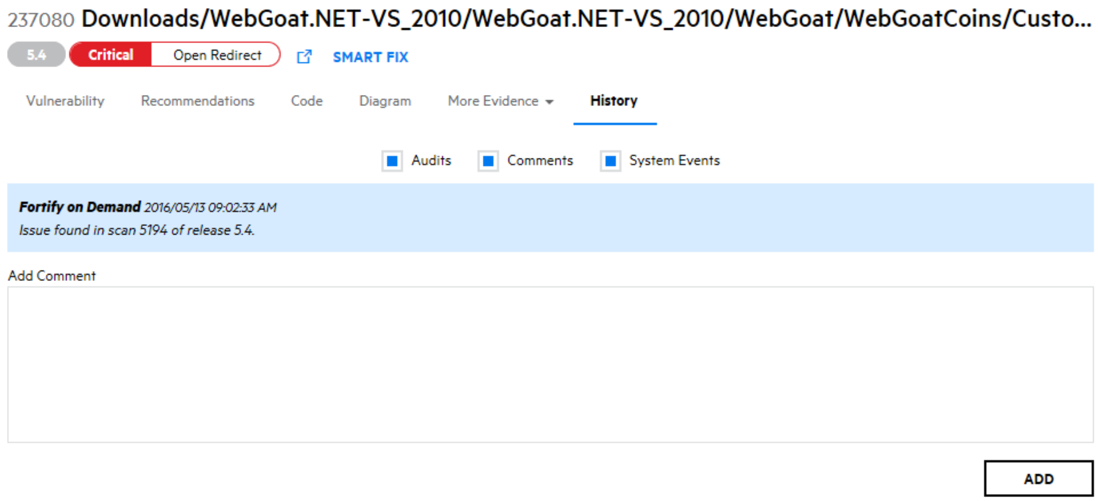
- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see "Uploading Screenshots" on page 204.



There are no items to display.

History

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



Fortify on Demand 2016/05/13 09:02:33 AM
Issue found in scan 5194 of release 5.4.

Open Source Scan Issue Details

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.

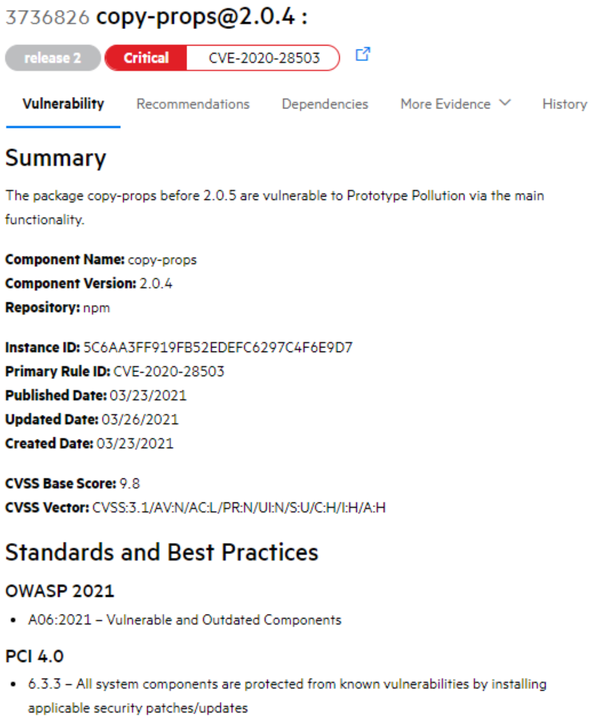
> **Note:** If an open source issue is found to be a non-active vulnerability based on the most recent Sonatype scan, the issues details panel displays the message "This vulnerability is no longer listed as an active vulnerability." The issue status is also marked as **Fix Validated**. This does not 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/
- Debricked: https://debricked.com/docs/security/security-about.html#data-refinement



3736826 copy-props@2.0.4 :

Summary

The package copy-props before 2.0.5 are vulnerable to Prototype Pollution via the main functionality.

Component Name: copy-props
Component Version: 2.0.4
Repository: npm

Instance ID: 5C6AA3FF919FB52EDEFC6297C4F6E9D7
Primary Rule ID: CVE-2020-28503
Published Date: 03/23/2021
Updated Date: 03/26/2021
Created Date: 03/23/2021

CVSS Base Score: 9.8
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Standards and Best Practices

OWASP 2021

- A06:2021 – Vulnerable and Outdated Components

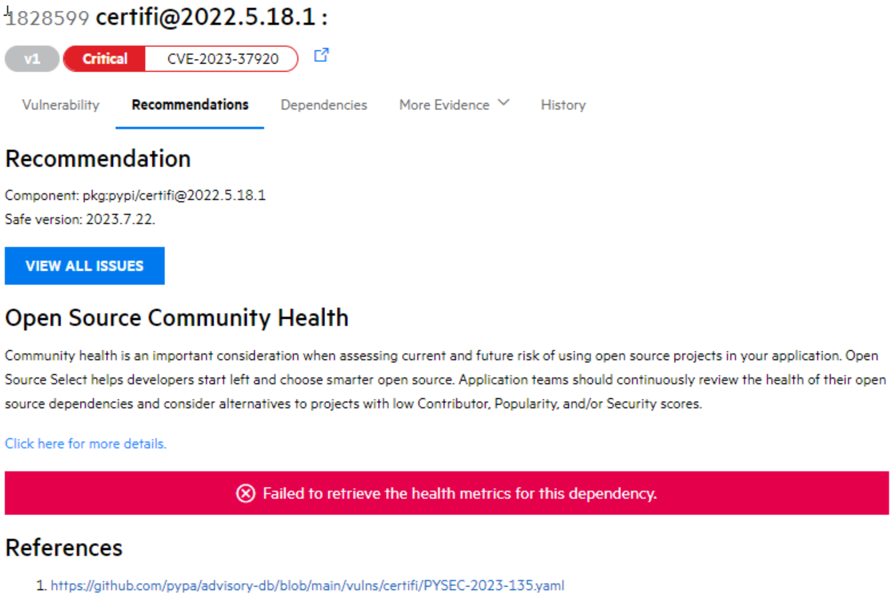
PCI 4.0

- 6.3.3 – All system components are protected from known vulnerabilities by installing applicable security patches/updates

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 Debricked issues. Open Source Select is a database of all open source projects on GitHub.



1828599 certifi@2022.5.18.1 :

Recommendation

Component: pkg:pypi/certifi@2022.5.18.1
Safe version: 2023.7.22.

Open Source Community Health

Community health is an important consideration when assessing current and future risk of using open source projects in your application. Open Source Select helps developers start left and choose smarter open source. Application teams should continuously review the health of their open source dependencies and consider alternatives to projects with low Contributor, Popularity, and/or Security scores.

Click here for more details.

Failed to retrieve the health metrics for this dependency.

References

1. https://github.com/pypa/advisory-db/blob/main/vulns/certifi/PYSEC-2023-135.yaml

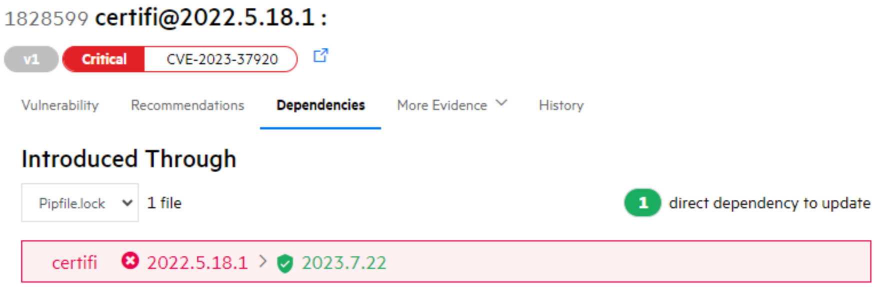
Dependencies (Debricked, CycloneDX)

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.

Fortify 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).



1828599 certifi@2022.5.18.1 :

CVE-2023-37920

Introduced Through

1 file

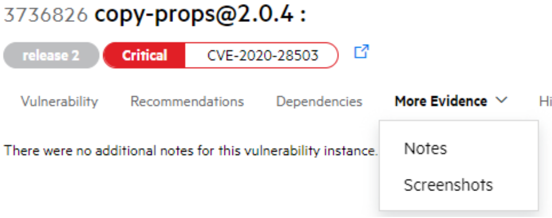
1 direct dependency to update

certifi ✗ 2022.5.18.1 > ✓ 2023.7.22

More Evidence

The **More Evidence** tab displays notes and screenshots, which are accessed separately through the drop-down menu.

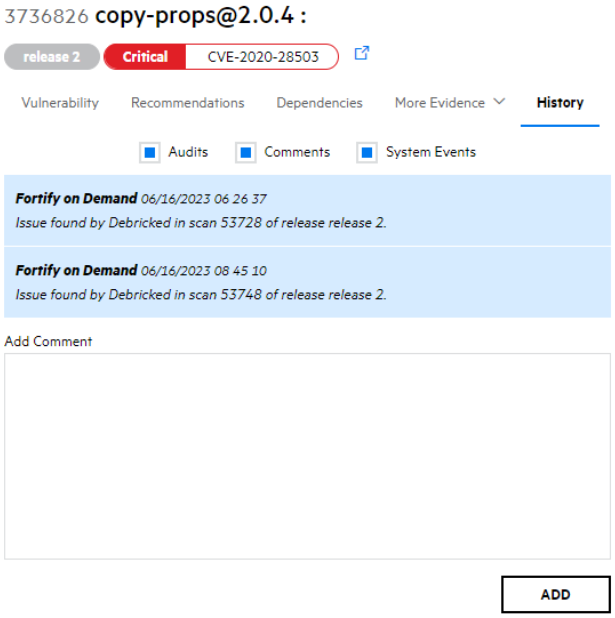
- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see "Uploading Screenshots" on page 204.



There were no additional notes for this vulnerability instance.

History

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



Fortify on Demand 06/16/2023 06 26 37
Issue found by Debricked in scan 53728 of release release 2.

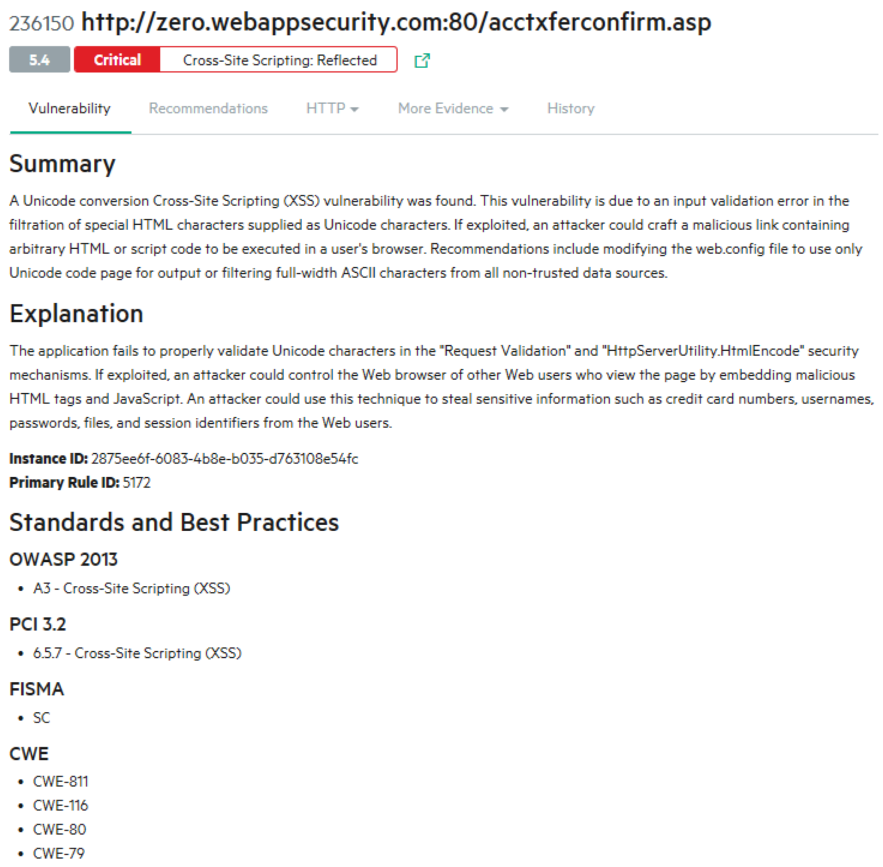
Fortify on Demand 06/16/2023 08 45 10
Issue found by Debricked in scan 53748 of release release 2.

Dynamic/Application Monitoring Scan Issue Details

The issues details panel for a dynamic scan issue or application monitoring issue displays the issue ID, issue location, issue severity, and issue category at the top. Several tabs below provide additional information about the vulnerability, including technical details, request, and response.

Vulnerability

The **Vulnerability** tab displays the following technical details about the issue: issue summary, including instance ID and rule ID of the issue; explanation of the execution and implications of the issue; and standards and best practices information from Fortify Software Security Research.



236150 **http://zero.webappsecurity.com:80/acctxferconfirm.asp**

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2013

- A3 - Cross-Site Scripting (XSS)

PCI 3.2

- 6.5.7 - Cross-Site Scripting (XSS)

FISMA

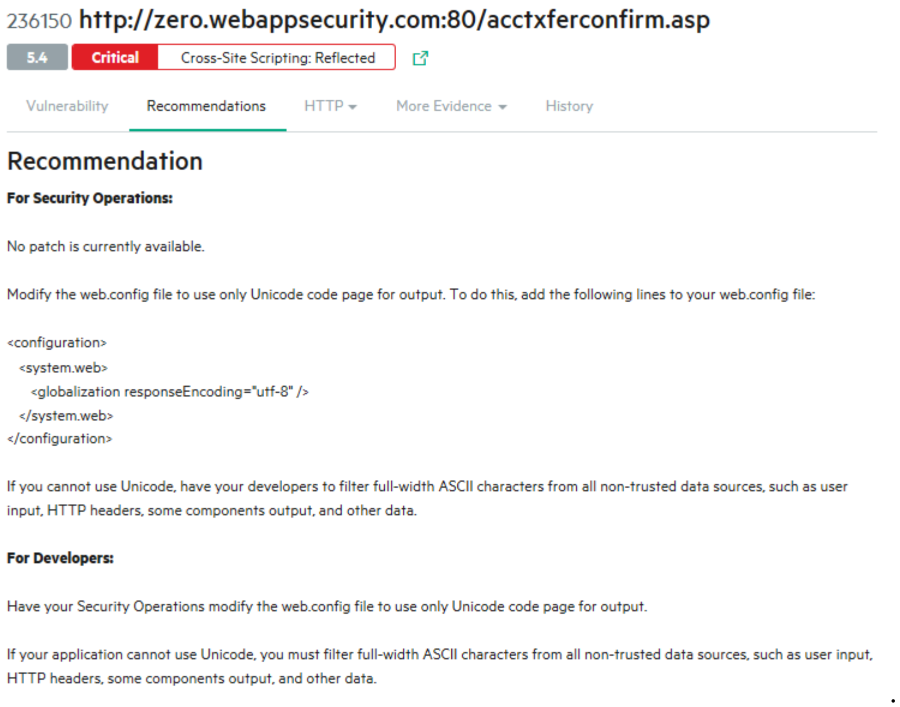
- SC

CWE

- CWE-811
- CWE-116
- CWE-80
- CWE-79

Recommendations

The **Recommendations** tab displays recommendations to remediate the issue, along with tips and references for further research. If available, the **Interactive Training** section contains a link to interactive training for the issue category, provided by Secure Code Warrior. For more information about Secure Code Warrior, see "Secure Code Warrior Integration" on page 353


236150 http://zero.webappsecurity.com:80/acctxferconfirm.asp
5.4
Critical
Cross-Site Scripting: Reflected
Vulnerability
Recommendations
HTTP
More Evidence
History

Recommendation

For Security Operations:

No patch is currently available.

Modify the web.config file to use only Unicode code page for output. To do this, add the following lines to your web.config file:

```
<configuration>
  <system.web>
    <globalization responseEncoding="utf-8" />
  </system.web>
</configuration>
```

If you cannot use Unicode, have your developers to filter full-width ASCII characters from all non-trusted data sources, such as user input, HTTP headers, some components output, and other data.

For Developers:

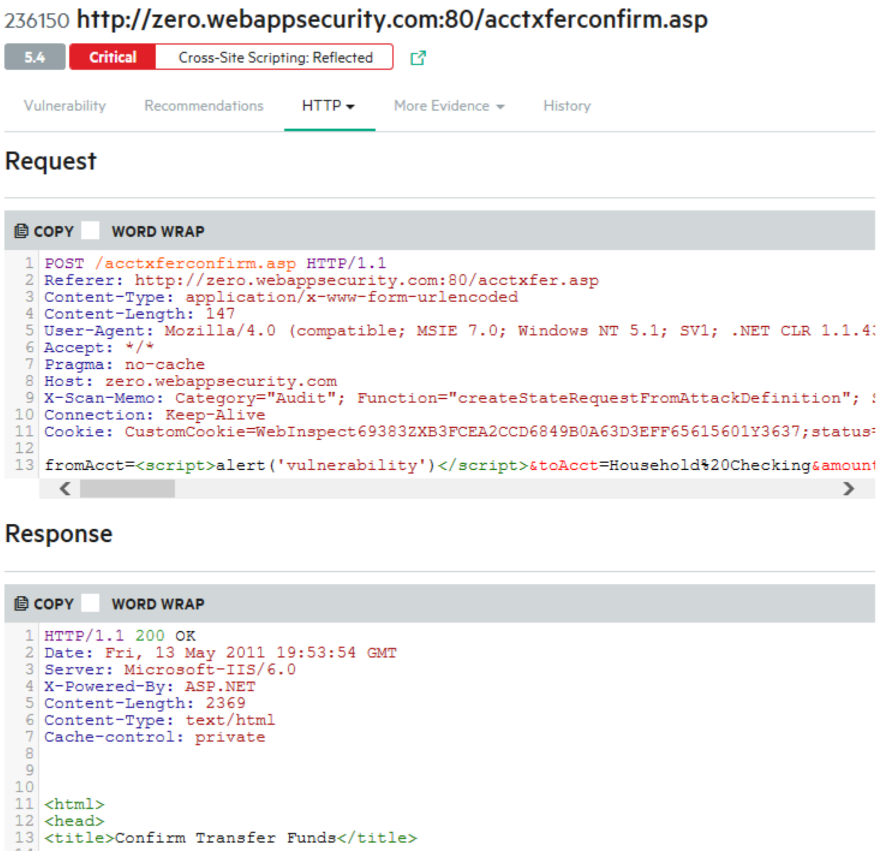
Have your Security Operations modify the web.config file to use only Unicode code page for output.

If your application cannot use Unicode, you must filter full-width ASCII characters from all non-trusted data sources, such as user input, HTTP headers, some components output, and other data.

HTTP

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

Available for Application Monitoring issues, the **Evidences** section lists the complete session traffic that found the issue.



236150 http://zero.webappsecurity.com:80/acctxferconfirm.asp

Request

```
POST /acctxferconfirm.asp HTTP/1.1
Referer: http://zero.webappsecurity.com:80/acctxfer.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 147
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4
Accept: */*
Pragma: no-cache
Host: zero.webappsecurity.com
X-Scan-Memo: Category="Audit"; Function="createStateRequestFromAttackDefinition";
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect69383ZXB3FCEA2CCD6849B0A63D3EFF65615601Y3637;status

fromAcct=<script>alert('vulnerability')</script>&toAcct=Household%20Checking&amoun
```

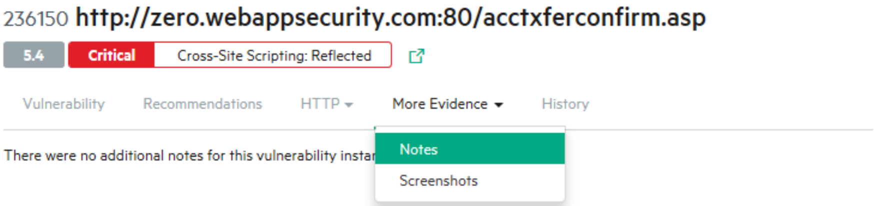
Response

```
HTTP/1.1 200 OK
Date: Fri, 13 May 2011 19:53:54 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 2369
Content-Type: text/html
Cache-control: private



<html>
<head>
<title>Confirm Transfer Funds</title>
```

More Evidence

The **More Evidence** tab displays notes and screenshots, which are accessed separately through the drop-down menu.

- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see "Uploading Screenshots" on page 204.

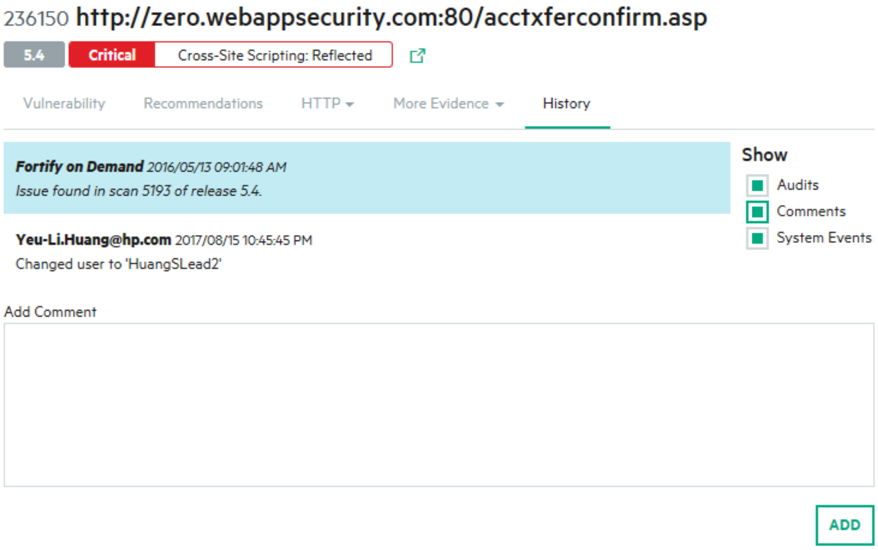


236150 http://zero.webappsecurity.com:80/acctxferconfirm.asp

There were no additional notes for this vulnerability insta

History

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



Fortify on Demand 2016/05/13 09:01:48 AM
Issue found in scan 5193 of release 5.4.

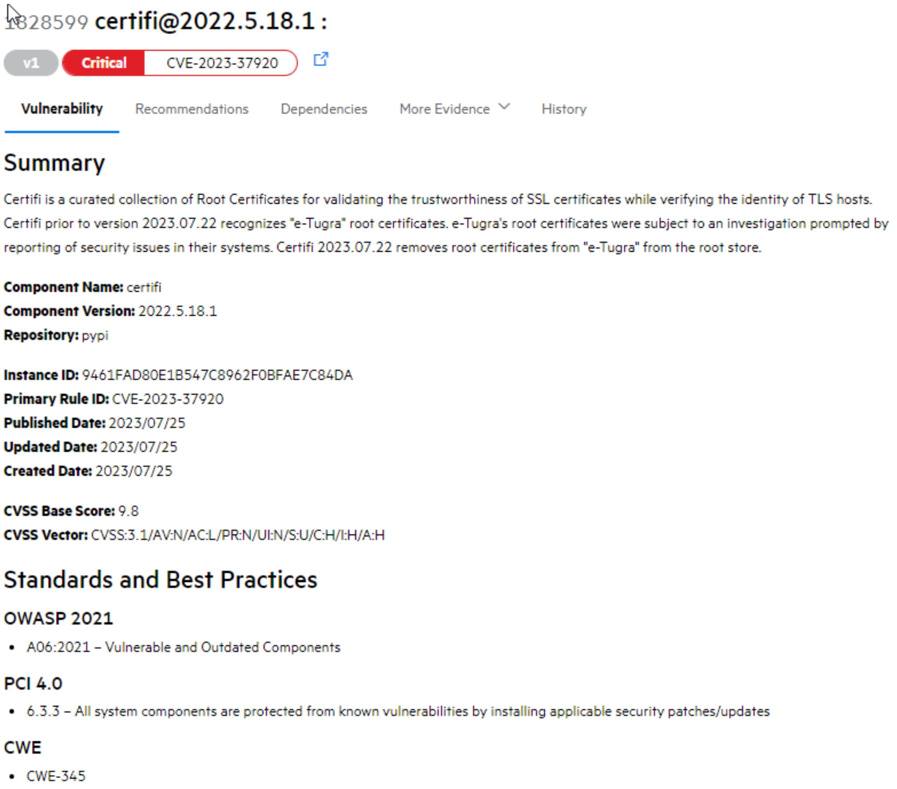
Yeu-Li.Huang@hp.com 2017/08/15 10:45:45 PM
Changed user to 'HuangSLead2'

Mobile Scan Issue Details

The issues details panel for a mobile scan issue displays the issue ID, issue location, issue severity, and issue category across the top. Several tabs below provide additional information about the issue.

Vulnerability

The **Vulnerability** tab displays the following technical details about the issue: issue summary; instance ID and rule ID; and explanation of the execution and implications of the issue.



1828599 certifi@2022.5.18.1 :

Summary

Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi prior to version 2023.07.22 recognizes "e-Tugra" root certificates. e-Tugra's root certificates were subject to an investigation prompted by reporting of security issues in their systems. Certifi 2023.07.22 removes root certificates from "e-Tugra" from the root store.

Component Name: certifi
Component Version: 2022.5.18.1
Repository: pypi

Instance ID: 9461FAD80E1B547C8962F0BFAE7C84DA
Primary Rule ID: CVE-2023-37920
Published Date: 2023/07/25
Updated Date: 2023/07/25
Created Date: 2023/07/25

CVSS Base Score: 9.8
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Standards and Best Practices

OWASP 2021

- A06:2021 – Vulnerable and Outdated Components

PCI 4.0

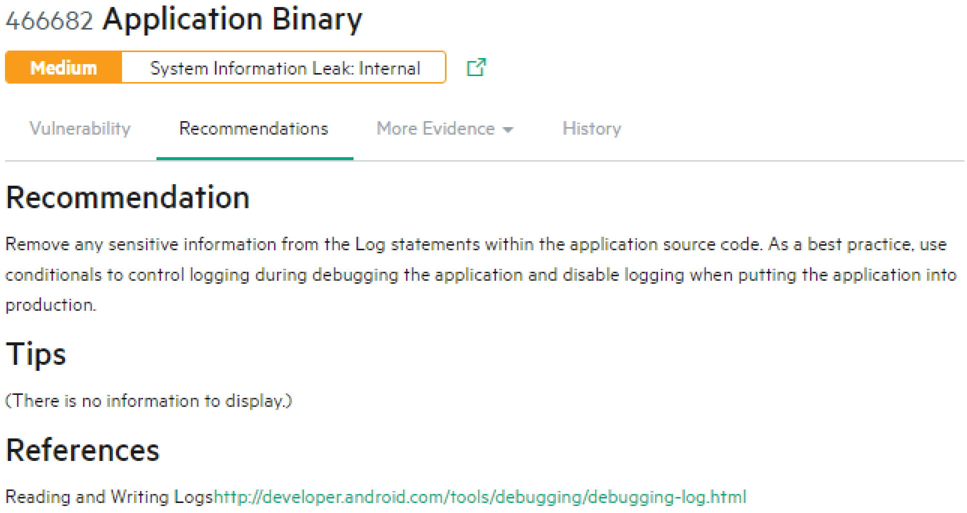
- 6.3.3 – All system components are protected from known vulnerabilities by installing applicable security patches/updates

CWE

- CWE-345

Recommendations

The **Recommendations** tab displays recommendations to remediate the issue, along with tips and references for further research. If available, the **Interactive Training** section contains a link to interactive training for the issue category, provided by Secure Code Warrior. For more information about Secure Code Warrior, see "Secure Code Warrior Integration" on page 353



466682 Application Binary

Recommendation

Remove any sensitive information from the Log statements within the application source code. As a best practice, use conditionals to control logging during debugging the application and disable logging when putting the application into production.

Tips

(There is no information to display.)

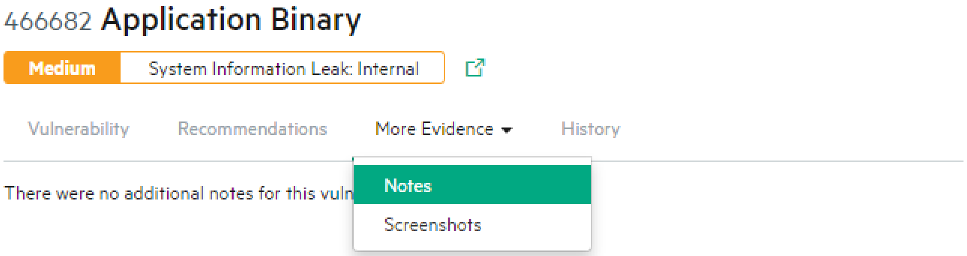
References

Reading and Writing Logshttp://developer.android.com/tools/debugging/debugging-log.html

More Evidence

The **More Evidence** tab contains notes and screenshots, which are accessed separately through the drop-down menu.

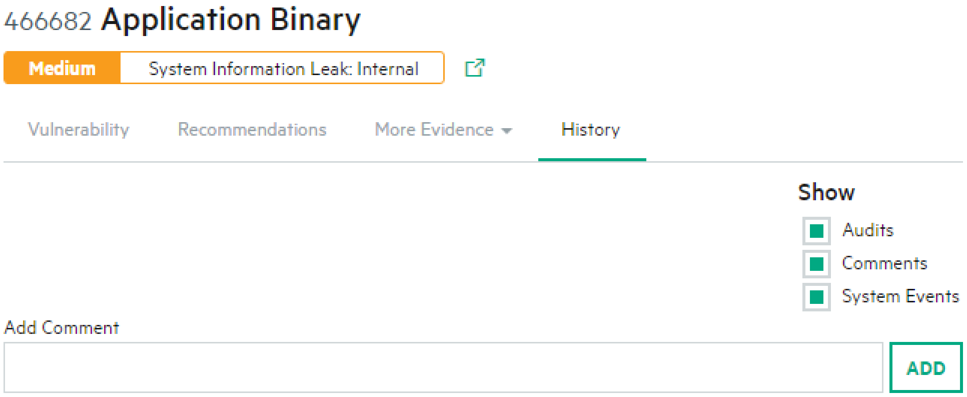
- The **Notes** section displays notes from the testing team about the issue.
- The **Screenshots** section allows you to upload screenshots that provide contextual information about the issue. For more information, see "Uploading Screenshots" on page 204.



There were no additional notes for this vuln

History

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



Updating 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.

This section contains the following topics:

Editing 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.

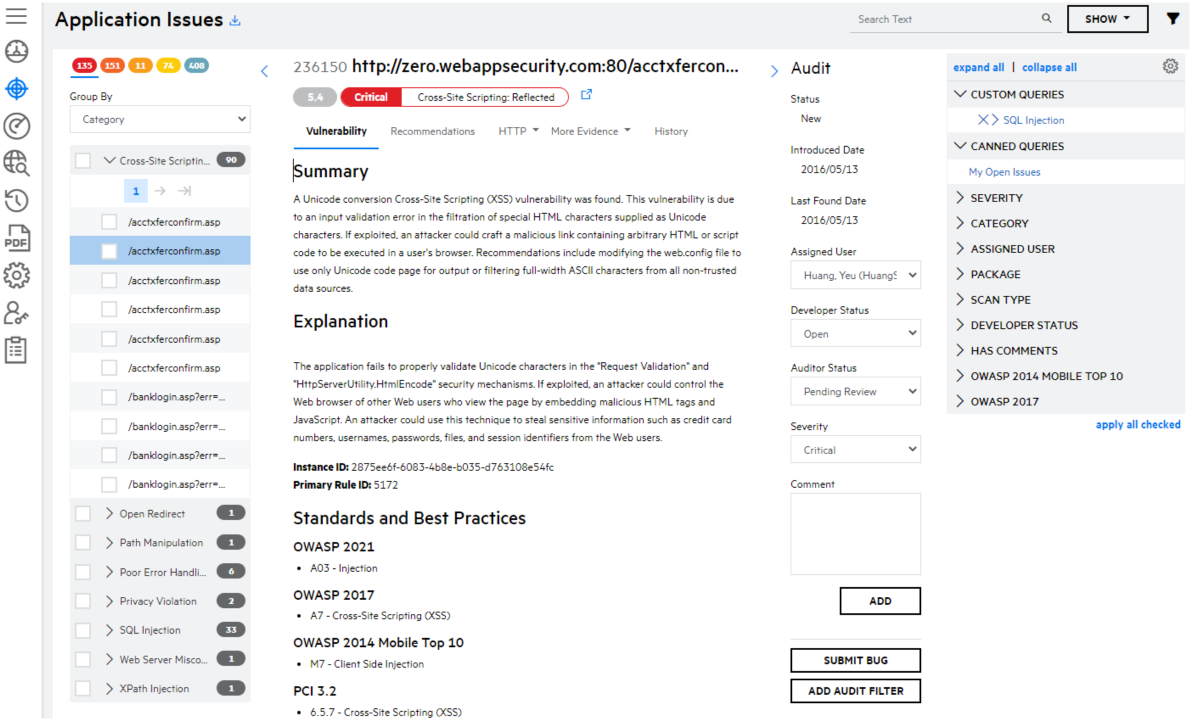
To edit an issue:

> **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**.



236150 http://zero.webappsecurity.com:80/acctxfercon...

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021
- A03 - Injection

OWASP 2017
- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10
- M7 - Client Side Injection

PCI 3.2
- 6.5.7 - Cross-Site Scripting (XSS)

Audit

Status: New
Introduced Date: 2016/05/13
Last Found Date: 2016/05/13
Assigned User: Huang, Yeu (Huang$
Developer Status: Open
Auditor Status: Pending Review
Severity: Critical
Comment:

   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 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.

Related Topics

"Submitting Issues to the Bug Tracker" on page 344

Editing 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.

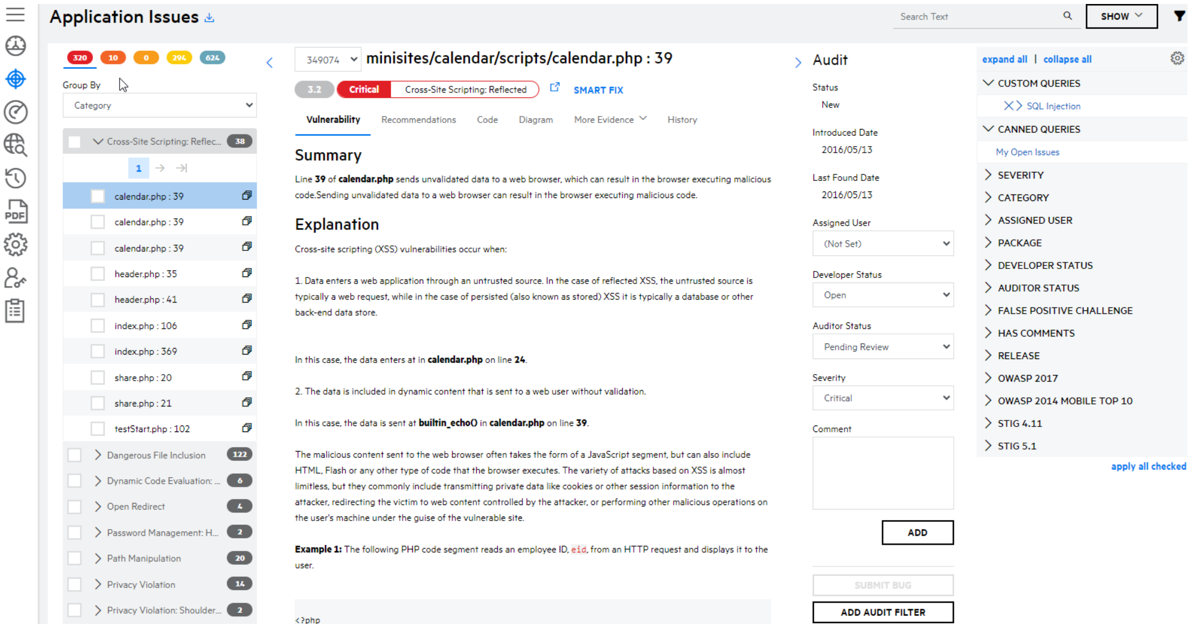
1. Select the **Applications** view.

   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**.



Summary

Line **39** of **calendar.php** sends unvalidated data to a web browser, which can result in the browser executing malicious code.Sending unvalidated data to a web browser can result in the browser executing malicious code.

Explanation

Cross-site scripting (XSS) vulnerabilities occur when:

1. Data enters a web application through an untrusted source. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store.

In this case, the data enters at in **calendar.php** on line **24**.

2. The data is included in dynamic content that is sent to a web user without validation.

In this case, the data is sent at **builtin_echo()** in **calendar.php** on line **39**.

The malicious content sent to the web browser often takes the form of a JavaScript segment, but can also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Example 1: The following PHP code segment reads an employee ID, `eid`, from an HTTP request and displays it to the user.

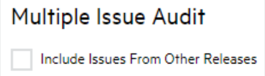
```
<?php
```

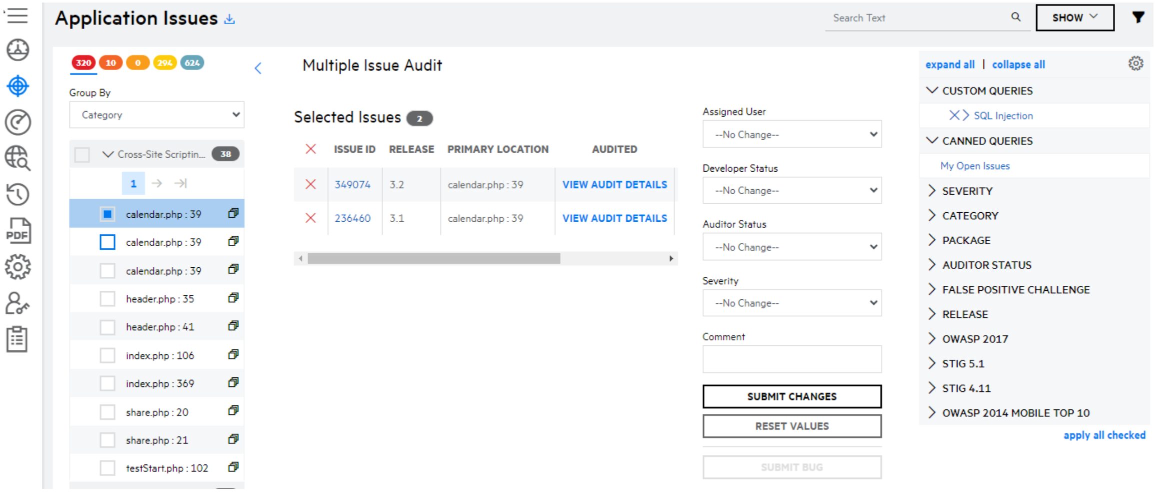
Status: New
Introduced Date: 2016/05/13
Last Found Date: 2016/05/13
Assigned User: (Not Set)
Developer Status: Open
Auditor Status: Pending Review
Severity: Critical
Comment:

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.

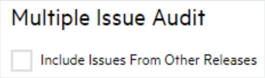
   > **Note:** On the Release Issues page, you can select the **Include Issues From Other Releases** check box to select all instances of the issue found in releases. Issues can be individually removed.
   >
   > 
   >



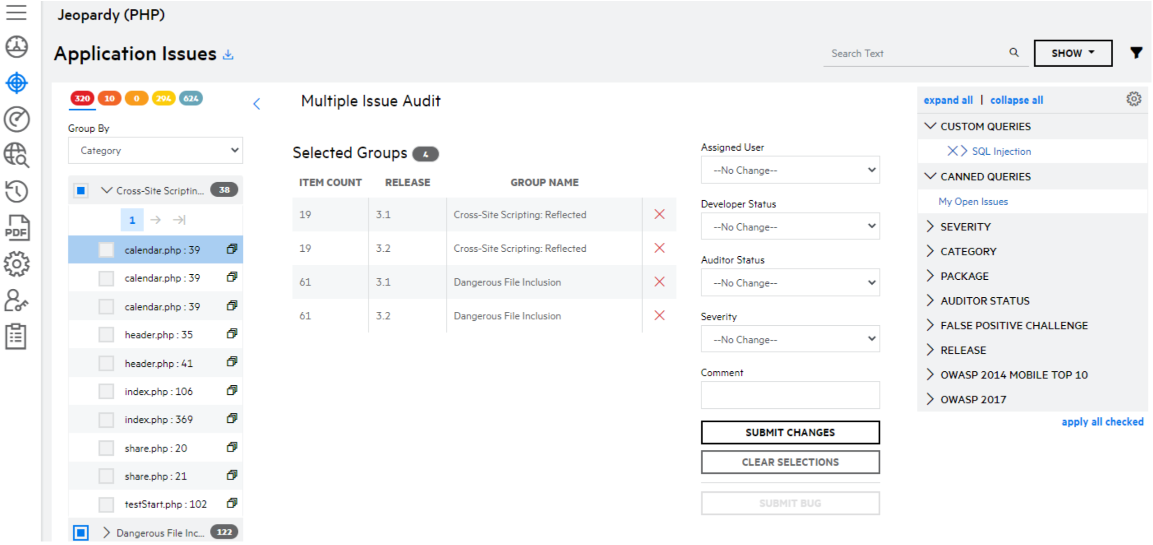
	ISSUE ID	RELEASE	PRIMARY LOCATION	AUDITED
✕	349074	3.2	calendar.php : 39	VIEW AUDIT DETAILS
✕	236460	3.1	calendar.php : 39	VIEW AUDIT DETAILS

- 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.


Multiple Issue Audit

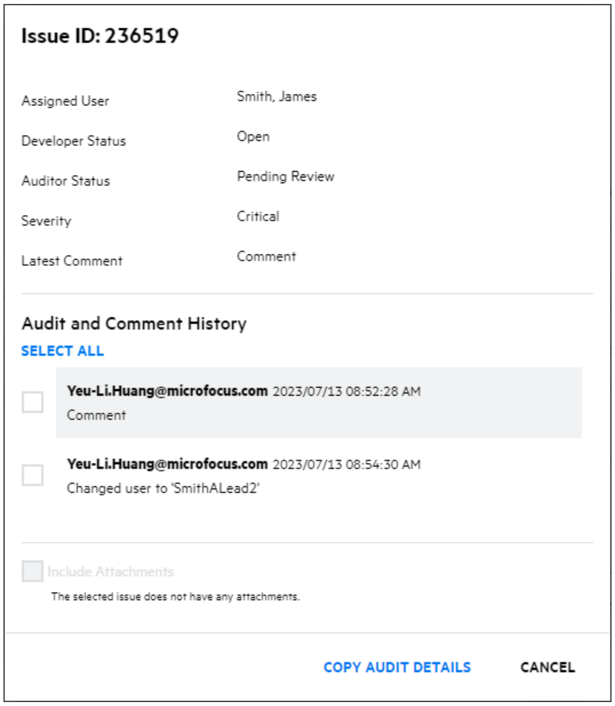
□ Include Issues From Other Releases



ITEM COUNT	RELEASE	GROUP NAME	
19	3.1	Cross-Site Scripting: Reflected	✕
19	3.2	Cross-Site Scripting: Reflected	✕
61	3.1	Dangerous File Inclusion	✕
61	3.2	Dangerous File Inclusion	✕

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**

Task	Description
	Status, **Severity**, and **Comments**.
Copy audit details from one issue to other issues	a. In the issues panel, click **View Audit Details** in the row of the issue that you want to copy. The Issue ID window appears.  Issue ID: 236519 Assigned User: Smith, James Developer Status: Open Auditor Status: Pending Review Severity: Critical Latest Comment: Comment Audit and Comment History □ Yeu-Li.Huang@microfocus.com 2023/07/13 08:52:28 AM Comment □ Yeu-Li.Huang@microfocus.com 2023/07/13 08:54:30 AM Changed user to 'SmithALead2' □ Include Attachments The selected issue does not have any attachments. b. Select the audit and comment entries that you want to copy. c. Select the **Include Attachments** check box to copy all attachments. d. 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. **Important!** 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.

Related Topics

"Submitting Issues to the Bug Tracker" on page 344

Uploading Screenshots

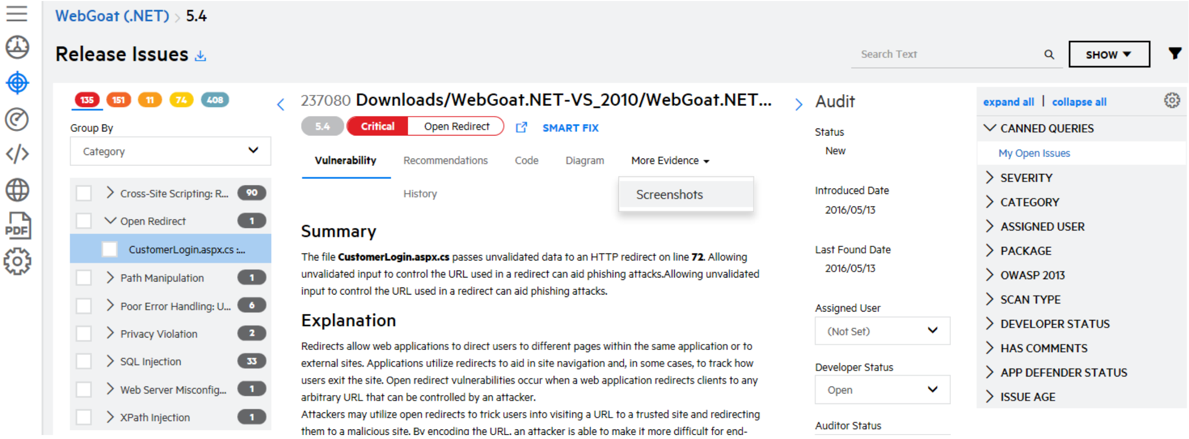
You can upload screenshots for an issue through the Application Issues or Release Issues page.

- Supported file types are.jpg, .gif, and .png.
- Files must be no larger than 3 MB.

There are two methods for uploading a screenshot: upload a saved file or copy and paste the image into the modal window.

To upload a screenshot for an issue:

1. In the issues detail panel, select the **More Evidence** tab > **Screenshots**.



Status: New

Introduced Date: 2016/05/13

Last Found Date: 2016/05/13

Assigned User: (Not Set)

Developer Status: Open

Auditor Status

Summary

The file **CustomerLogin.aspx.cs** passes unvalidated data to an HTTP redirect on line **72**. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

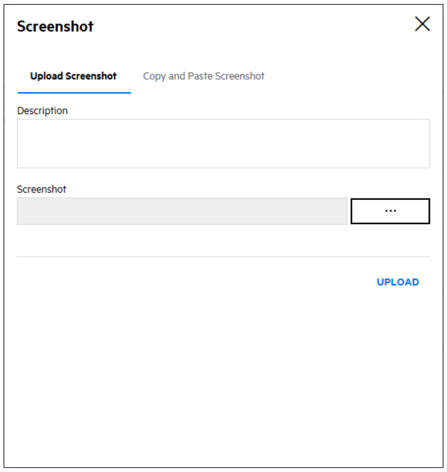
Explanation

Redirects allow web applications to direct users to different pages within the same application or to external sites. Applications utilize redirects to aid in site navigation and, in some cases, to track how users exit the site. Open redirect vulnerabilities occur when a web application redirects clients to any arbitrary URL that can be controlled by an attacker.

Attackers may utilize open redirects to trick users into visiting a URL to a trusted site and redirecting them to a malicious site. By encoding the URL, an attacker is able to make it more difficult for end-

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.

iii. Click **...** and browse to and select a screenshot.

iv. Click **Upload**.

- To copy and paste the screenshot:

  i. Select the **Copy and Paste Screenshot** tab.

  ii. (Optional) Type a description of the file.

  iii. Copy an image to your clipboard.

  iv. Select the box and press **Crtl+V** to paste the image from the clipboard.

  v. Click **Upload**.

  The uploaded screenshot details and icons for viewing, saving, and deleting the screenshot appears in the tab.

Icon	Description
👁	View the screenshot in the browser.
⤓	Open the screenshot or save it to your local system.
✕	Delete the screenshot.

Auditing Issue Remediation

Fortify on Demand enables an organization's development and security teams to audit issue remediation, where different user roles participate in the issue remediation workflow. Users with the **Edit Issues** permission, typically the development team, receive the issues and decide whether to remediate them or not. Users with the **Audit Issues** permission, typically the security team, validate the issues after the development team is finished and decide whether to suppress them or not . Users with the **View Issues** permission can view issues, but cannot make any changes.

This section contains the following topics:

Audit Workflow for Auditors

The following procedures describes the typical workflow that a security team follows for assigning new issues and reviewing closed issues.

Auditors from the security team need the Audit issue permission, which allows editing of the **Auditor Status** and **Severity** fields.

Assigning a New Issue

A new issue arrives in the queue with the following default values:

- **Developer Status**: **Open**
- **Users**: **(Not Set)**
- **Auditor Status**: **Pending Review**
- **Severity**: Fortify on Demand-ranked default

The security team reviews the issue and assigns it to a developer for remediation.

To assign a new issue to a developer for remediation:

1. Review an issue that has the **Developer Status** set as **Open**.
2. If needed, select a different issue severity from the **Severity** list. For more information on issue severity, see "Priority Order" on page 19.
3. Select the developer to be assigned the issue from the **User** list.

Reviewing Closed Issues

After working on the issue, the developer changes the **Developer Status** to a closed state (**Remediated**, **Will Not Fix**, **Third Party Component**). The issue then returns to the security team issue queue for auditing.

To review a closed issue:

1. Audit the change made to the closed issue.
2. Based on your assessment of the change, decide whether to suppress or not suppress the issue and select the corresponding reason from the **Auditor Status** list.
   - Not Suppressed: **Remediation Required**, **Remediation Deferred**, **Risk Mitigated**
   - Suppressed: **Risk Accepted**, **Not an Issue**
3. If you selected **Remediation Required**, reassign the issue to a developer.
4. Add any supporting comments.

Audit Workflow for Developers

The following procedures describe the typical workflow a development team follows for remediating and closing an issue.

Developers from the development team need the Edit issue permission, which allows editing of the **Developer Status** and **User** fields.

Remediating an Issue

The security team assigns an open issue to a developer for remediation.

To remediate an issue:

1. Set the **Developer Status** to **In Remediation**.
2. Review the issue and perform one of the following actions:

- Remediate the issue.
- Do not remediate the issue.

Closing an Issue

To close an issue:

1. Once you have finished working on the issue, set the **Developer Status** to **Remediated**, **Will Not Fix**, or **Third Party Component**.

   The issue is closed at this point.
2. Add any supporting comments.
3. Select the auditor to review the issue from the **User** list.

Audit Templates

Audit templates allow audit decisions to be systematically applied to static, dynamic, mobile, and open source scans. An audit template consists of custom filters that either suppress issues or change issue severity across all scans of the specified type.

An audit template can be created for each scan type at the global and application levels. Security Leads can manage global audit templates; users with the **Audit Issues** permission can manage audit templates for applications to which they have access.

> **Important!** Audit template is an advanced feature and can lead to significant changes in vulnerability metrics and reporting. Fortify strongly recommends that you review the documentation before using audit templates. If you have additional questions, contact the support team.

This section contains the following topics:

Creating a Global Audit Template

Security Leads can manage global audit templates. Global audit templates apply to all scans of the specified type across the tenant.

Audit templates are subjected to the following conditions:

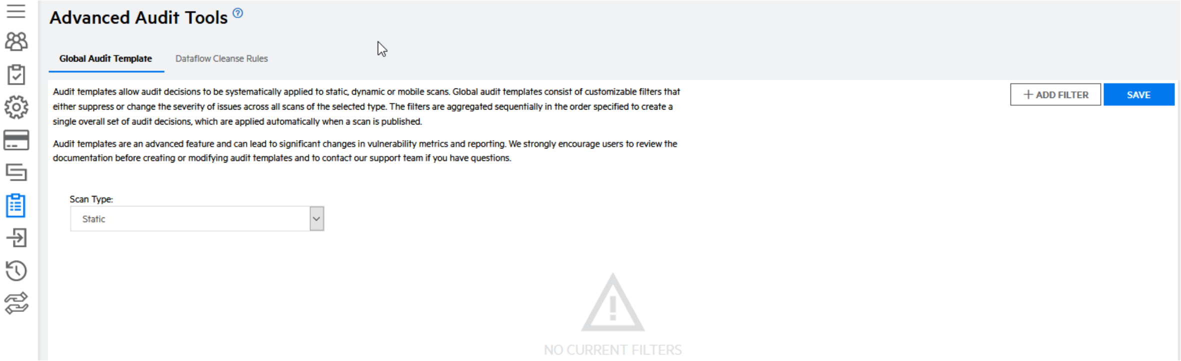
- Audit template filters are case insensitive.
- Newly created or modified audit template filters are applied to scans published moving forward.

To create a global audit template:

1. Select the **Administration** view.

   The User Management page appears.
2. Click **Audit Tools**.

   The Advanced Audit Tools page appears.

   Audit templates allow audit decisions to be systematically applied to static, dynamic or mobile scans. Global audit templates consist of customizable filters that either suppress or change the severity of issues across all scans of the selected type. The filters are aggregated sequentially in the order specified to create a single overall set of audit decisions, which are applied automatically when a scan is published.

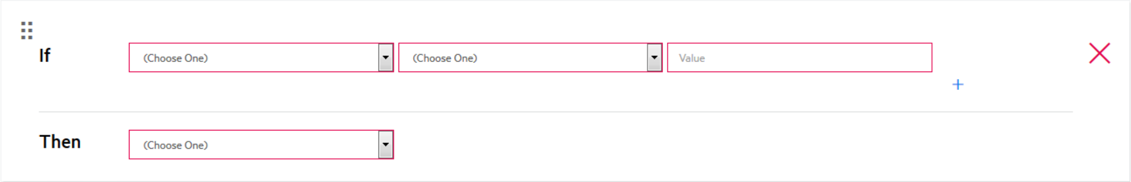
   Audit templates are an advanced feature and can lead to significant changes in vulnerability metrics and reporting. We strongly encourage users to review the documentation before creating or modifying audit templates and to contact our support team if you have questions.

   Scan Type: Static

   NO CURRENT FILTERS
3. On the **Global Audit Template** tab, select the scan type to which the global audit template will be applied from the **Scan Type** list.
4. Perform the following steps to add a filter. You can add multiple filters.

   a. Click **Add Filter**.

      A blank filter appears.

   b. Specify the filter conditions.

      i. In the **IF** row, select an issue attribute or a custom attribute for which to filter:

      > **Note:** Static, dynamic, and mobile issue attributes are set by Fortify Software Security Content. Open source issue attributes are set by Sonatype.

Field	Scan Type	Description
Severity	Static, dynamic, mobile, open source	Issue severity

Field	**Scan Type**	**Description**
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

ii. Select one of the following operators:

Operator	**Description**
Contains	Searches for results that contain the specified value

Operator	Description
Does Not Contain	Searches for results that do not contain the specified value
Equals	Searches for an exact match of the specified value
Does Not Equals	Searches for results that do not match the specified value

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

> **Note:** If you previously selected a custom picklist or boolean attribute and the **Equals** operator, the values are prepopulated.

iv. If needed, click **+** to create additional filter conditions.

v. Select **And** or **Or** to combine multiple filter conditions

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

Operator	Description
Suppress	Suppresses matching results
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.

Related Topics:

For information on creating an application audit template, see "Creating an Application Audit Template" below.

Creating an Application Audit Template

Users with the **Audit Issues** permission can manage audit templates for applications to which they have access. An application audit template applies to all scans of the specified type for the application.

Audit templates are subjected to the following conditions:

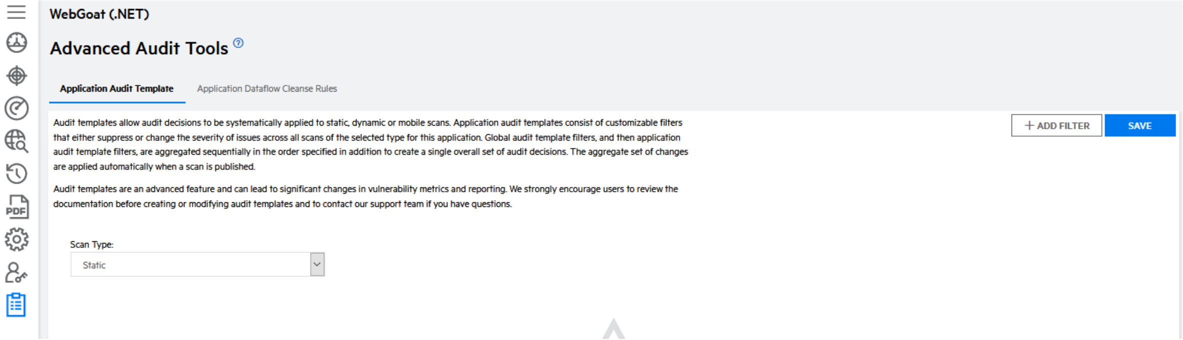
- Audit template filters are case-insensitive.
- Newly created or modified audit template filters are applied to scans published moving forward.

To create an application audit template:

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.


WebGoat (.NET)
Advanced Audit Tools
Application Audit Template
Application Dataflow Cleanse Rules
+ ADD FILTER
SAVE
PDF

Audit templates allow audit decisions to be systematically applied to static, dynamic or mobile scans. Application audit templates consist of customizable filters that either suppress or change the severity of issues across all scans of the selected type for this application. Global audit template filters, and then application audit template filters, are aggregated sequentially in the order specified in addition to create a single overall set of audit decisions. The aggregate set of changes are applied automatically when a scan is published.

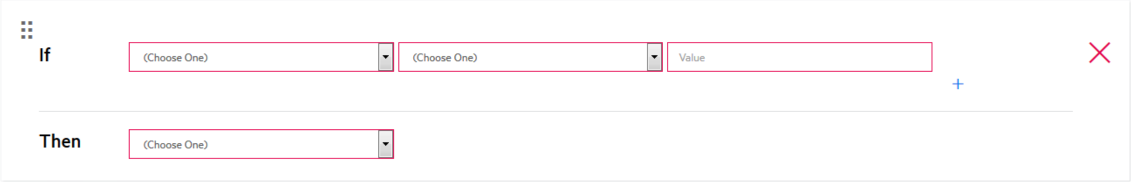
Audit templates are an advanced feature and can lead to significant changes in vulnerability metrics and reporting. We strongly encourage users to review the documentation before creating or modifying audit templates and to contact our support team if you have questions.

Scan Type: Static

4. On the **Application Audit Template** tab, select the scan type to which the application audit template will be applied from the **Scan Type** list.
5. Perform the following steps to add a filter. You can add multiple filters.

   a. Click **Add Filter**.

      A blank filter appears.



   b. Specify the filter conditions.

      i. In the **IF** row, select one of the following issue attributes for which to filter:

> **Note:** Static, dynamic, and mobile issue attributes are set by Fortify Software Security Content. Open source issue attributes are set by Sonatype.

Field	Scan Type	Description
Severity	Static, dynamic, mobile, open source	Issue severity.
Rule ID	Static, dynamic, mobile,	A unique identifier for the rule that identified an issue. You can find the Rule ID on the **Vulnerability** tab when viewing issue details.

Field	Scan Type	Description
	open source	
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

ii. Select one of the following operators:

Operator	Description
Contains	Searches for results that contain the specified value

Operator	Description
Does Not Contain	Searches for results that do not contain the specified value
Equals	Searches for an exact match of the specified value
Does Not Equals	Searches for results that do not match the specified value

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

iv. If needed, click **+** to create additional filter conditions.

v. Select **And** or **Or** to combine multiple filter conditions .

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

Operator	Description
Suppress	Suppresses matching results
Set Severity	Sets issue severity of matching results to the specified value

6. To rearrange the location of a filter, click ⠿ and drag the filter to your desired slot.
7. Once you are done adding and arranging filters, click **Save**.

   The application audit template is saved.

Related Topics:

For information on creating a global audit template, see "Creating a Global Audit Template" on page 207.

Creating an Application Audit Template Filter for an Issue

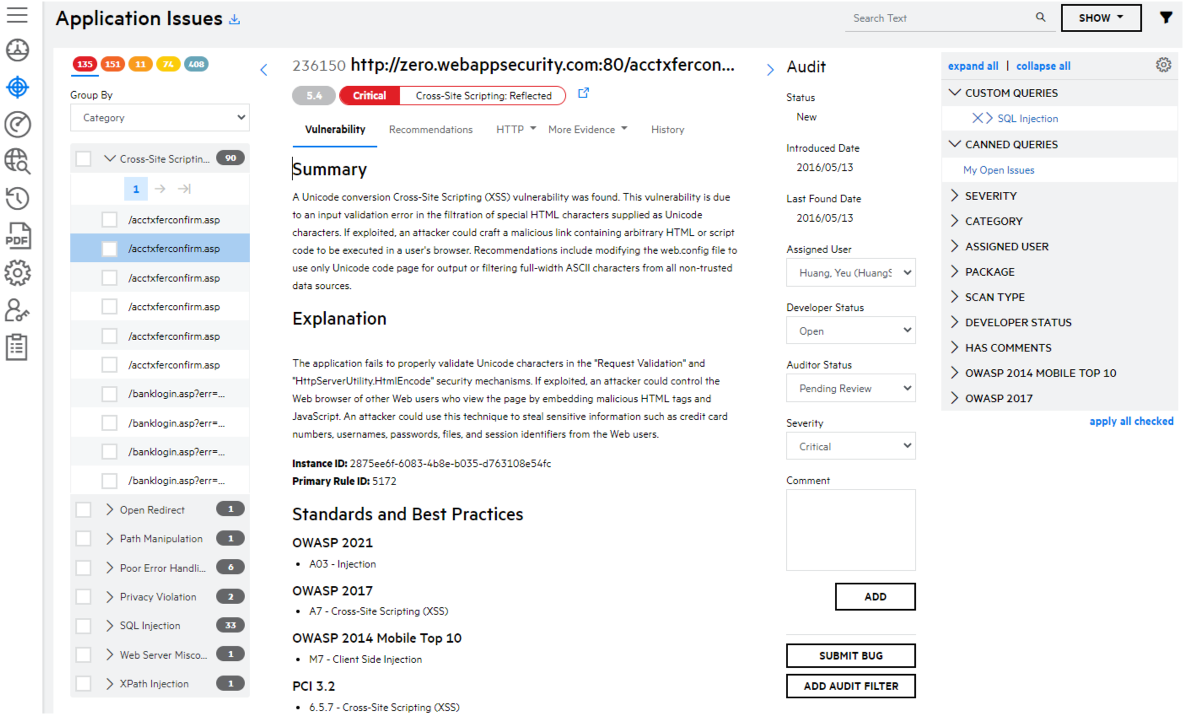
In addition to creating an application audit template from the ground up, users with the **Audit Issues** permission can create application audit template filters for an issue from the Issues page. This enables auditors to easily apply audit decisions to issues while reviewing them.

To create an application audit template filter for an issue:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of the application that you want to audit.

   The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page.



236150 http://zero.webappsecurity.com:80/acctxfercon...

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021
- A03 - Injection

OWASP 2017
- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10
- M7 - Client Side Injection

PCI 3.2
- 6.5.7 - Cross-Site Scripting (XSS)

Audit

Status: New
Introduced Date: 2016/05/13
Last Found Date: 2016/05/13
Assigned User: Huang, Yeu (HuangS
Developer Status: Open
Auditor Status: Pending Review
Severity: Critical
Comment:

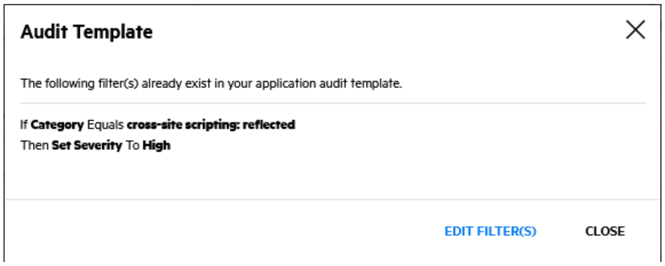
4. In the audit panel, click **Add Audit Filter**.

   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.

     Audit Template

     The following filter(s) already exist in your application audit template.

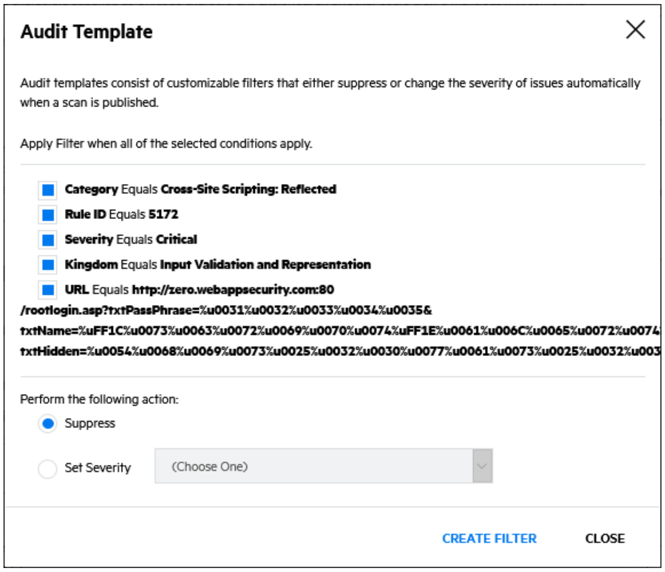
     If **Category** Equals **cross-site scripting: reflected**
     Then **Set Severity** To **High**

     i. Click **Edit Filter(s)**.

        You are redirected to the Application Audit Template page.

     ii. 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.



Audit Template

Audit templates consist of customizable filters that either suppress or change the severity of issues automatically when a scan is published.

Apply Filter when all of the selected conditions apply.

- ☑ **Category** Equals **Cross-Site Scripting: Reflected**
- ☑ **Rule ID** Equals **5172**
- ☑ **Severity** Equals **Critical**
- ☑ **Kingdom** Equals **Input Validation and Representation**
- ☑ **URL** Equals **http://zero.webappsecurity.com:80**

/rootlogin.asp?txtPassPhrase=%u0031%u0032%u0033%u0034%u0035&
txtName=%uFF1C%u0073%u0063%u0072%u0069%u0070%u0074%uFF1E%u0061%u006C%u0065%u0072%u0074
txtHidden=%u0054%u0068%u0069%u0073%u0025%u0032%u0030%u0077%u0061%u0073%u0025%u0032%u003

Perform the following action:

● Suppress

○ Set Severity (Choose One)

i. Select the filter conditions. Multiple conditions are joined with the AND operator.

ii. Select the audit action.

iii. Click **Create Filter**. Your application audit template filter is saved.

Audit Template Usage and Examples

Audit template filters are aggregated sequentially in the order in which they appear. Global audit templates filters are aggregated first, then application audit template filters, to create a single overall set of audit decisions that are applied automatically when a scan is published. Issue changes as a result of audit templates appear in the **History** tab of the issue details panel as **Audit** type events. Global audit and application audit changes are logged separately.

In general, Fortify recommends using category-based filters over rule-based filters, with the exception of a few scenarios where using rule-based filters might be more appropriate. For example, you might want to use rule ID-based filters to handle different remediation policies around SSL/TLS checks in dynamic scans.

As changes are made to categories and rules with each security content update, it is important to review your filters after each security content update and update the filters as necessary:

- New categories might be added.
- Category names might be changed. You will need to update any category-based filters to reflect the changed names.
- New rules might be added to categories. Existing category filters will also apply to new rules. Note that new rules might cover new, critical vulnerabilities that are distinctly different from existing rules in a category.
- Existing rules might be updated to reflect new guidance and industry standards. For example, the severity given to a vulnerability might increase due to new information about the vulnerability.

For more information on category and rule changes, see the Fortify Software Security Content quarterly updates from Fortify Software Security Research (SSR). You can access them from the Help Center.

The following examples show several filter combinations and how they are applied.

Example 1:

Audit template filters:

1. If **Severity Equals Critical**, then **Set Severity** to **High**
2. If **Severity Equals Critical**, then **Set Severity** to **Medium**

Result: Critical issues are set to Medium for the selected scan type.

Example 2:

Audit template filters:

1. If **Severity Equals Critical**, then **Set Severity** to **High**
2. If **Severity Equals High**, then **Set Severity** to **Medium.**

Result: Critical issues are set to High, High issues are to set Medium for the selected scan type.

Example 3:

Audit template filter: If **Rule ID Equals 11516**, then **Suppress**.

Result: Issues with rule ID 1156 are suppressed for the selected scan type

Example 4:

Global audit template filter: If **Severity Equals Critical**, then **Set Severity** to **High**

Application audit template filter: If **Severity Equals Critical**, then **Set Severity** to **Medium**

Result: Critical issues are set to High for all scans of the selected type, but Critical issues are set to Medium for scans of the selected type for the application above.

Dataflow Cleanse Rules

Dataflow cleanse rules describe validation logic and other actions that render tainted data (user-controlled input) cleansed. Dataflow cleanse rules are incorporated in a static scan to help Fortify Static Code Analyzer recognize cleansing functions. As a result, dataflow cleanse rules help prevent false positives around dataflow issues.

Dataflow cleanse rules can be created at the global and application levels. Security Leads can manage global dataflow cleanse rules; users with the **Audit Issues** permission can manage dataflow cleanse rules for applications to which they have access.

Important! Dataflow cleanse rule is an advanced feature and can lead to significant changes in vulnerabilities found in a scan. Fortify strongly recommends that you review the documentation before using dataflow cleanse rules. If you have additional questions, contact support.

This section contains the following topics:

Creating a Global Dataflow Cleanse Rule

Security Leads can manage global dataflow cleanse rules. Global dataflow cleanse rules apply to all static scans in the tenant.

Dataflow cleanse rules are subjected to the following conditions:

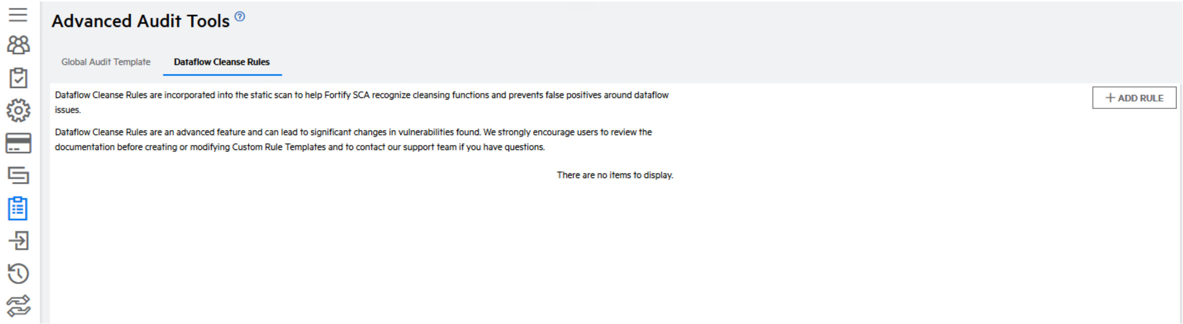
- Dataflow cleanse rules are case-sensitive and are restricted to alphanumeric characters.
- Dataflow cleanse rules are applied to scans that are started moving forward.

To create a global dataflow cleanse rule:

1. Select the **Administration** view.

   The User Management page appears.
2. Click **Audit Tools**.

   The Advanced Audit Tools page appears.
3. Select the **Dataflow Cleanse Rules** tab.

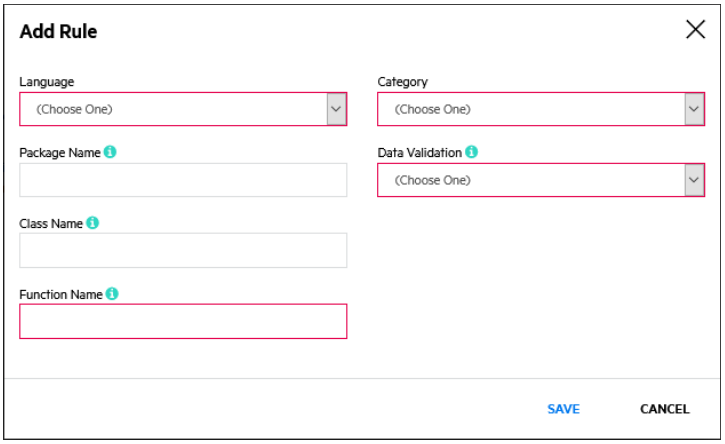
   

   Dataflow Cleanse Rules are incorporated into the static scan to help Fortify SCA recognize cleansing functions and prevents false positives around dataflow issues.

   Dataflow Cleanse Rules are an advanced feature and can lead to significant changes in vulnerabilities found. We strongly encourage users to review the documentation before creating or modifying Custom Rule Templates and to contact our support team if you have questions.

   There are no items to display.
4. Perform the following steps to add a rule. You can add multiple rules.
   1. Click **Add Rule**.

      The Add Rule window opens.



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

Note: Rules do not apply against interfaces or super classes.

Field	Description
Language	Select the technology stack.
Package Name	(Optional) Type the name of the package or namespace that contains the validation function. If you do not specify a package name, the rule only matches functions that are not inside a package.
Class Name	(Optional) Type the name of the class that contains the validation function. If you do not specify a class name, the rule only matches functions that are not inside a 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.

Field	Description
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)`

5. Once you are done adding rules, click **Save**.

   The global dataflow cleanse rules are saved.

Creating an Application Dataflow Cleanse Rule

Users with the **Audit Issues** permission can manage dataflow cleanse rules for applications to which they have access. Application dataflow cleanse rules apply to all static scans for the application.

Dataflow cleanse rules are subjected to the following conditions:

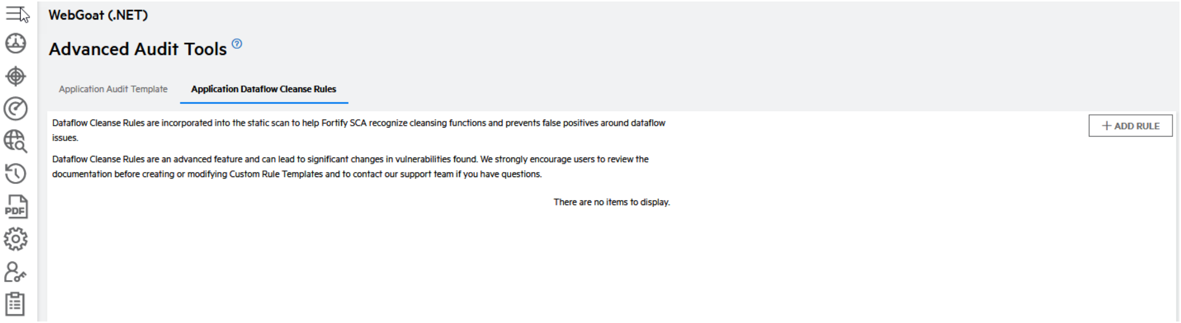
- Dataflow cleanse rules are case-sensitive and are restricted to alphanumeric characters.
- Dataflow cleanse rules are applied to scans that are started moving forward.

To create an application dataflow cleanse rule:

1. Select the **Application** view.

   Your Applications page appears.
2. Click the name of the application for which you want to create an application audit template.
3. Click **Audit Tools**.

   The Advanced Audit Tools page appears.
4. Select the **Dataflow Cleanse Rules** tab.


WebGoat (.NET)

Advanced Audit Tools

Application Audit Template
Application Dataflow Cleanse Rules
+ ADD RULE

Dataflow Cleanse Rules are incorporated into the static scan to help Fortify SCA recognize cleansing functions and prevents false positives around dataflow issues.

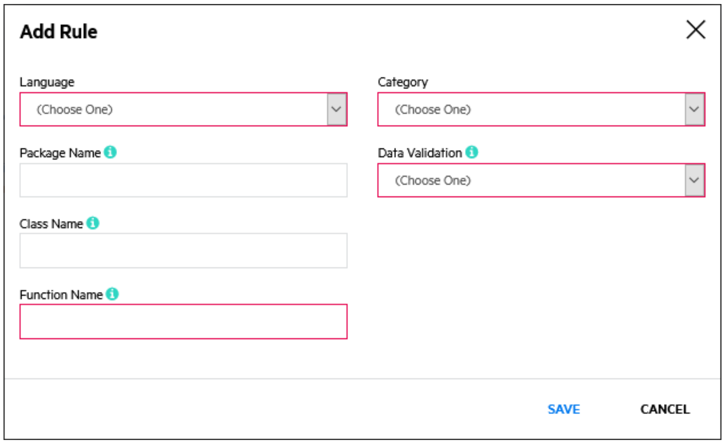
Dataflow Cleanse Rules are an advanced feature and can lead to significant changes in vulnerabilities found. We strongly encourage users to review the documentation before creating or modifying Custom Rule Templates and to contact our support team if you have questions.

There are no items to display.

5. Perform the following steps to add a rule. You can add multiple rules.

   a. Click **Add Rule**.

      The Add Rule window opens.


Add Rule

Language: (Choose One)

Category: (Choose One)

Package Name

Data Validation: (Choose One)

Class Name

Function Name

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

> **Note:** Rules do not apply against interfaces or super classes.

Field	Description
Language	Select the technology stack.
Package Name	(Optional) Type the name of the package or namespace that contains the validation function. If you do not specify a package name, the rule only matches functions that are not inside a package.
Class Name	(Optional) Type the name of the class that contains the validation function. If you do not specify a class name, the rule only matches functions that are not inside a class. To specify a nested class, use the dot notation (for example, `OuterClass.NestedClass`).

Field	Description
	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.

Dataflow Cleanse Rule Usage and Examples

Global and application dataflow cleanse rules are aggregated into a single set of rules that are applied during a scan. Issues that are removed based on rules do not appear in the FPR.

The following examples show several dataflow cleanse rules and how they are applied.

Example 1:

Language: **Java**

Package Name: `com.fortify.appsec`

Class name: `Validation`

Function Name: `validateAlphaNumeric`

Category: **SQL Injection**

Data Validation: **Return Value**

Result: The return value of the method is considered cleansed and will not be flagged as a SQL Injection issue.

Example 2:

Language: **Java**

Package Name: `java.util`

Class name: `Map`

Function Name: `clear`

Category: **SQL Injection**

Data Validation: **Object Function**

Result: The data is considered cleansed after a call to the `Map.clear()` method and will not be flagged as a SQL Injection issue.

Requesting a Remediation Scan

After changes have been made to fix the issues identified in the initial scan, you can request a remediation scan to verify whether the issues have been fixed. Assessments include one or more remediation scans:

- Single assessments include one remediation scan.
- Subscriptions include unlimited remediation scans during the remediation scan period.

Fortify on Demand typically limits a remediation scan to 30 days after the initial scan. Exceptions are noted in your contract.

Request a remediation scan by selecting **<assessment_type> - Remediation** on the Scan Setup page. The remediation scan must be performed on the same application. For example, if the initial scan was done on the pre-production site, the remediation scan must also be on the pre-production site. A remediation scan takes less time than a full initial scan.

Note: For a dynamic scan, the following fields are locked to the values specified in the initial scan: **Dynamic Site URL**, **Environment Facing**, **Scan entire host**, **Restrict scan to URL directory and subdirectories**, **Allow HTTP (:80) and HTTPS (:443)**, **Allow form submissions**, and **Exclude URLs which contain *<exclusion>***.

Chapter 6: Dashboards and Reports

Fortify on Demand delivers assessment results in a variety of formats for viewing and analyzing data.

Dashboards provide a visual display of key metrics. Users can configure multiple dashboards to display data that is relevant to their needs. While dashboards are useful for general summaries, users can get a detailed view of assessment results through reports. Fortify on Demand provides a comprehensive and customizable suite of reports.

This section contains the following topics:

Dashboards

A dashboard is made up of individual tiles that each present a specific facet of data as a visual element. You are initially provided with one of the following default dashboard configurations based on your user role:

- Development dashboard for Developer, Lead Developer, and Application Lead roles
- Security dashboard for Security Lead and TAM roles
- Management dashboard for Executive and Reviewer roles
- Management dashboard for custom roles

You can edit the default dashboard as well as create additional dashboards.

This section contains the following topics:

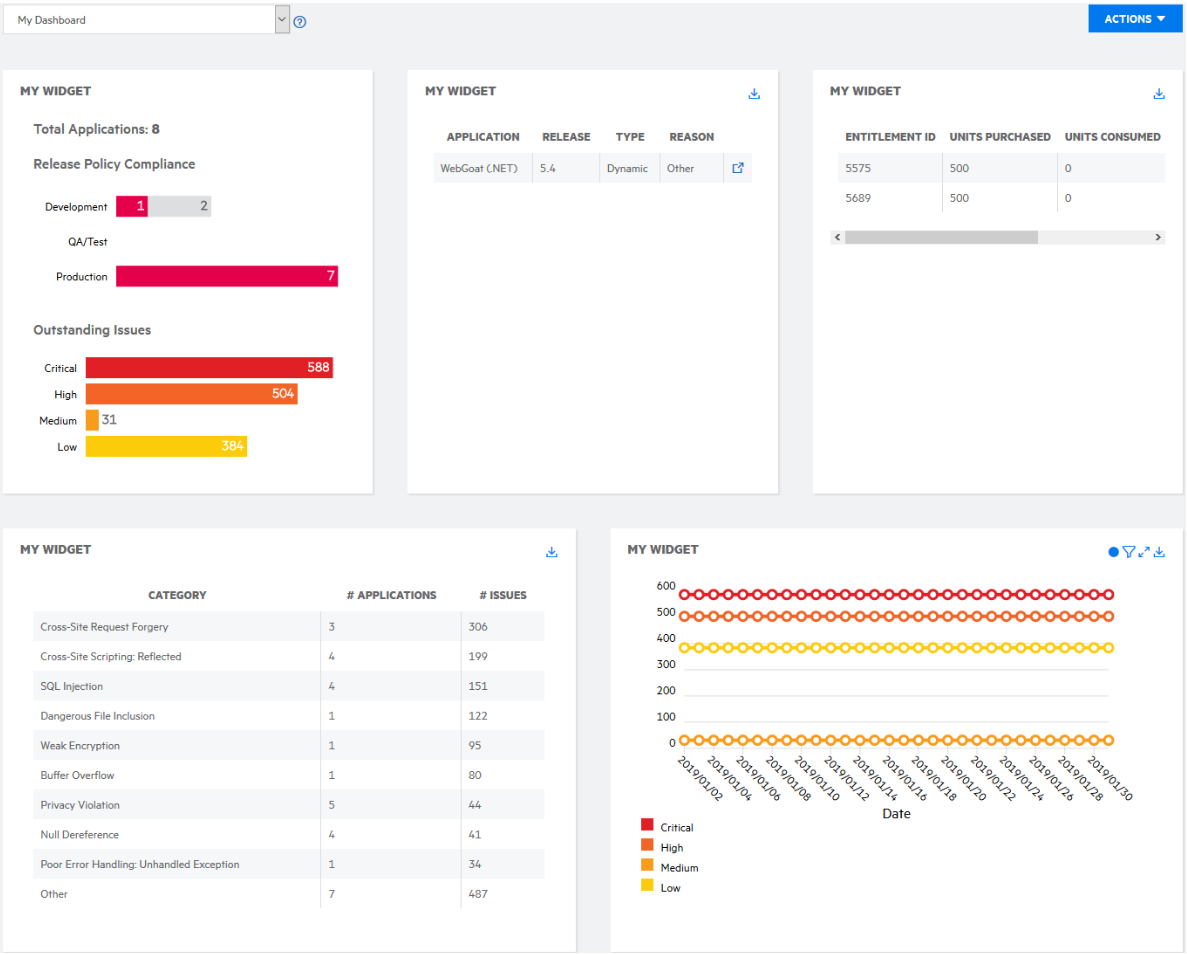
Viewing Dashboards

To view your dashboards:

1. Select the **Dashboard** view.

   The dashboard page appears. It displays the last dashboard that was loaded.

> **Note:** If you have not yet configured a dashboard, a default dashboard configuration based on your user role is loaded.



MY WIDGET

APPLICATION	RELEASE	TYPE	REASON
WebGoat (.NET)	5.4	Dynamic	Other

MY WIDGET

ENTITLEMENT ID	UNITS PURCHASED	UNITS CONSUMED
5575	500	0
5689	500	0

MY WIDGET

CATEGORY	# APPLICATIONS	# ISSUES
Cross-Site Request Forgery	3	306
Cross-Site Scripting: Reflected	4	199
SQL Injection	4	151
Dangerous File Inclusion	1	122
Weak Encryption	1	95
Buffer Overflow	1	80
Privacy Violation	5	44
Null Dereference	4	41
Poor Error Handling: Unhandled Exception	1	34
Other	7	487

2. Select the dashboard that you want to view from the drop-down list.

   The selected dashboard is loaded.

The following table describes how to navigate the dashboard page.

Task	Action
Create a dashboard	Select **Actions** > **New Dashboard**. For more information, see "Creating a Dashboard" on page 228.
Edit the dashboard	Select **Actions** > **Edit Dashboard**. For more information, see "Editing a Dashboard" on page 230.
Generate a PDF of the dashboard	Select **Actions** > **Print**.

Display or hide data point markers	Click ● in a trending chart tile.
View filters applied to a tile	Click ▽.
Export data that makes up a tile	Click ⤓. A .csv file is saved locally to the folder specified in your browser settings.
View details of a scan	Click ↗ in a list grid tile.
Expand a tile	Click ⤢ in a trending chart tile.

Dashboard Graph Types

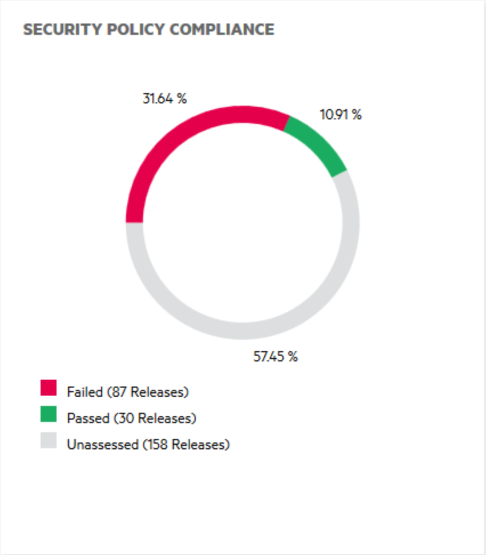
The following tile types are available in a dashboard:

- Gauge
- List Grid
- Summary
- Trending Chart

Gauge

The **Gauge** tile is a gauge graph summarizing one of the following data items: assessed releases, auditor status, developer status, entitlement consumption, issue assignment, and security compliance.

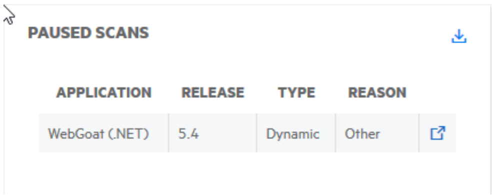
Data Item Type	Description
Assessed Releases	Assessment state of issues
Auditor Status	Auditor status of issues
Developer Status	Developer status of issues
Entitlement Consumption	Usage of active entitlements
Issue Assignment	Assignment state of issues
Security Compliance	Policy compliance status across releases



List Grid

The **List Grid** tile is a list or grid view of one of the following data items: active entitlements, canceled scans, completed scans, in progress scans, most prevalent issues, my issues, paused scans, and scheduled scans. For scans, the List Grid also contains links to the relevant Scan Setup page or Scans page.

Data Item Type	**Description**
Active entitlements	Active entitlements
Canceled scans	Scans that were canceled
Completed scans	Scans that were completed
In progress scans	Scans currently in progress
Most prevalent issues	Most prevalent issues across all applications
My issues	Issues assigned to the current user account
Paused scans	Scans paused by the testing team
Scheduled scans	Scans that have been scheduled

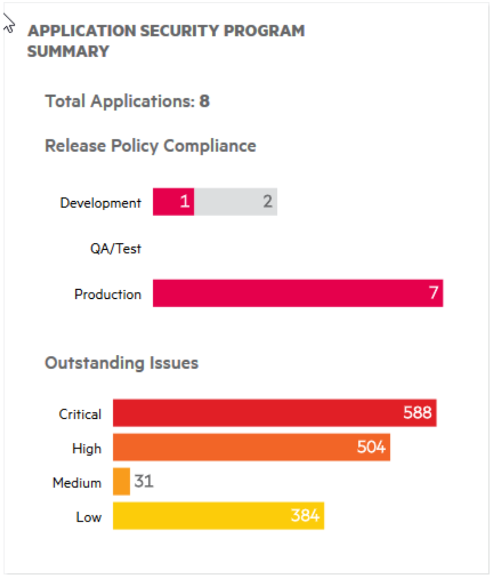


PAUSED SCANS

APPLICATION	RELEASE	TYPE	REASON
WebGoat (.NET)	5.4	Dynamic	Other

Summary

The **Summary** tile is a quick summary of the security risk of your releases. It shows the total number of applications in the portfolio and the following information about development, QA, and production releases: security policy compliance and outstanding issues (issues that are not fix validated or suppressed).


APPLICATION SECURITY PROGRAM SUMMARY

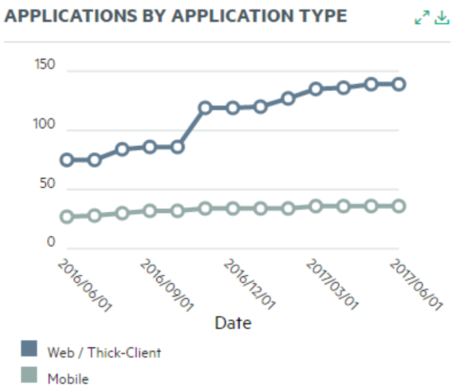
Total Applications: 8

Trending Chart

The **Trending Chart** tile is a line graph of one of the following data items over time: applications, entitlements, issues, releases, and scans. Data series are grouped by a specified attribute.

Note: Data points for all items are measured additively except for scans.

Data Item Type	Description
Applications	Number of applications, grouped by an application attribute
Entitlements	Number of entitlement units, grouped by units purchased, consumed, or available
Issues	Number of issues, grouped by an issue attribute
Releases	Number of releases, grouped by an application or release attribute
Scans	Number of scans, grouped by the scan status



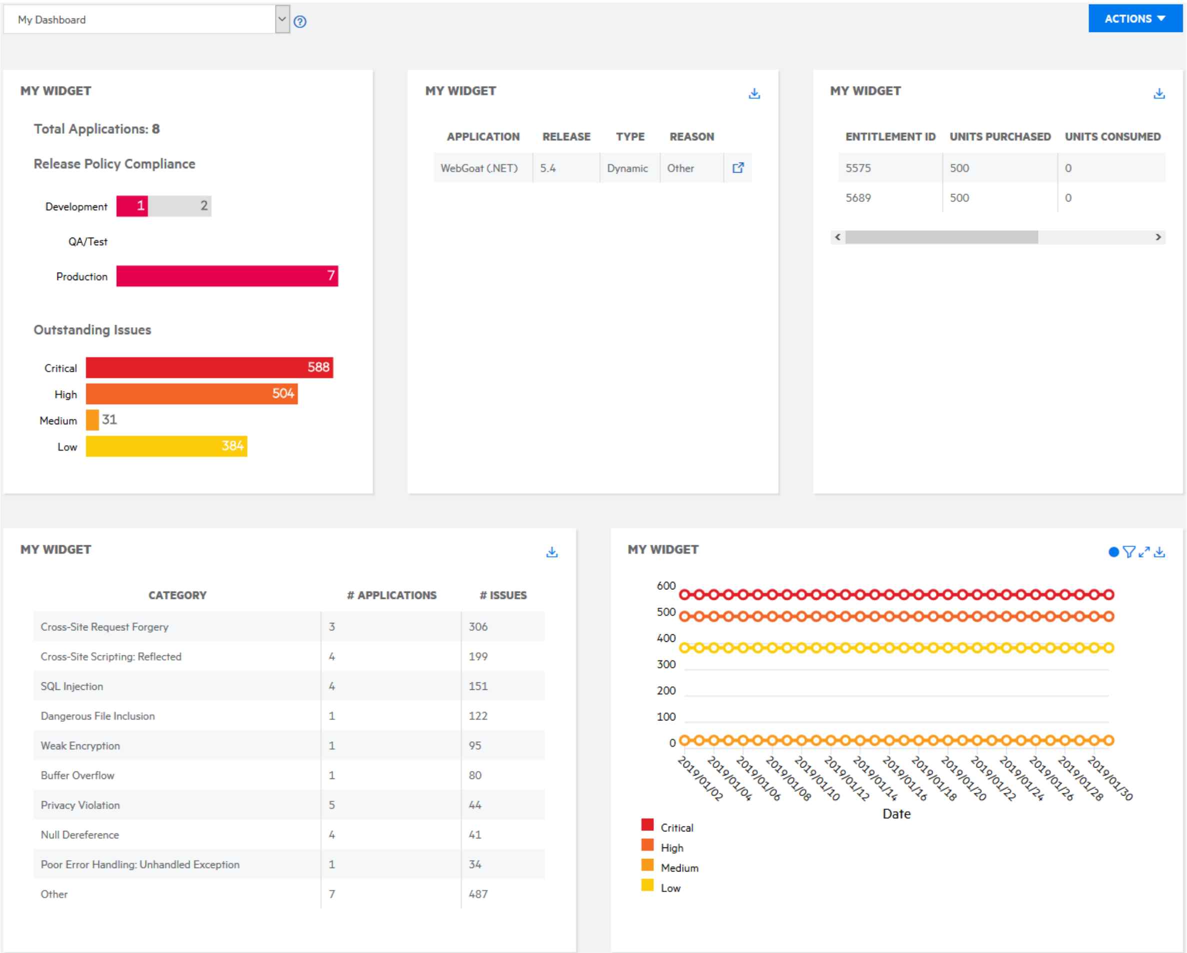
Creating a Dashboard

You can create additional dashboards for organizing different facets of data. You can have up to 10 dashboards.

To create a dashboard:

1. Select the **Dashboard** view.

   The dashboard page appears. It displays the last dashboard that was loaded.



My Dashboard

MY WIDGET

Total Applications: 8

Release Policy Compliance

Outstanding Issues

MY WIDGET

APPLICATION	RELEASE	TYPE	REASON
WebGoat (.NET)	5.4	Dynamic	Other

MY WIDGET

ENTITLEMENT ID	UNITS PURCHASED	UNITS CONSUMED
5575	500	0
5689	500	0

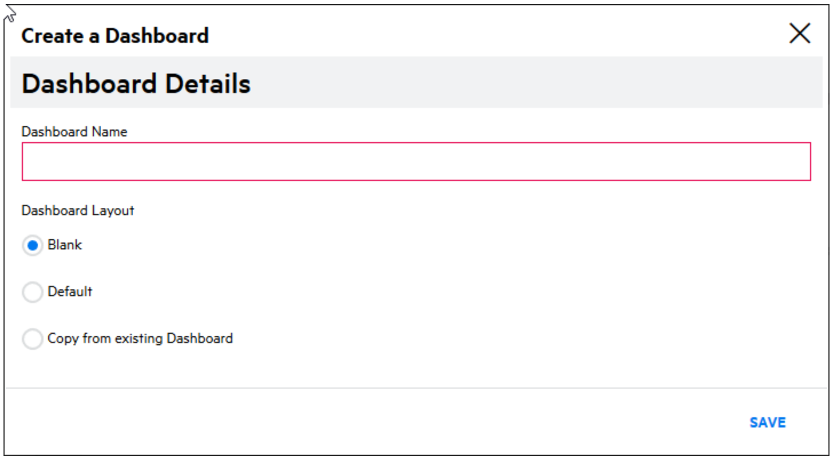
MY WIDGET

CATEGORY	# APPLICATIONS	# ISSUES
Cross-Site Request Forgery	3	306
Cross-Site Scripting: Reflected	4	199
SQL Injection	4	151
Dangerous File Inclusion	1	122
Weak Encryption	1	95
Buffer Overflow	1	80
Privacy Violation	5	44
Null Dereference	4	41
Poor Error Handling: Unhandled Exception	1	34
Other	7	487

MY WIDGET

2. Select **Actions** > **New Dashboard**.

   The Create a Dashboard window opens.



Create a Dashboard

Dashboard Details

Dashboard Name

Dashboard Layout

● Blank

○ Default

○ Copy from existing Dashboard

3. In the **Dashboard Name** field, type a name for the new dashboard.
4. Select the initial layout of the new dashboard:

- **Blank**: start with a blank dashboard
- **Default**: use the default dashboard configuration for your user role
- **Copy from existing Dashboard**: copy the layout of an existing dashboard

5. Click **Save**.

   The new dashboard appears.

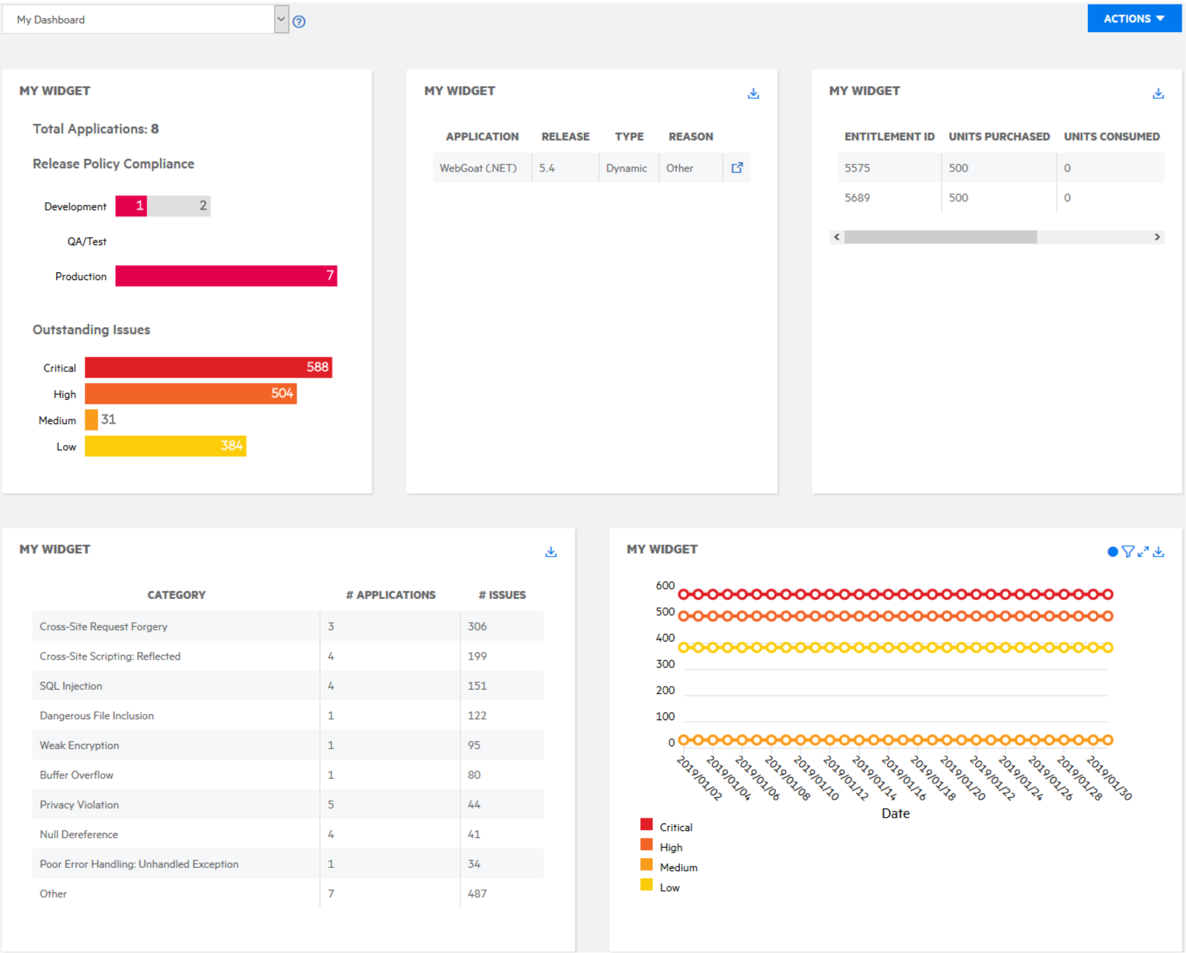
Editing a Dashboard

You can edit a dashboard by adding, editing, rearranging, and deleting rows and tiles. A dashboard can have up to ten tiles with a maximum of three tiles per row.

To edit a dashboard:

1. Select the **Dashboard** view.

   The dashboard page appears. It displays the last dashboard that was loaded.



MY WIDGET

APPLICATION	RELEASE	TYPE	REASON
WebGoat (.NET)	5.4	Dynamic	Other

MY WIDGET

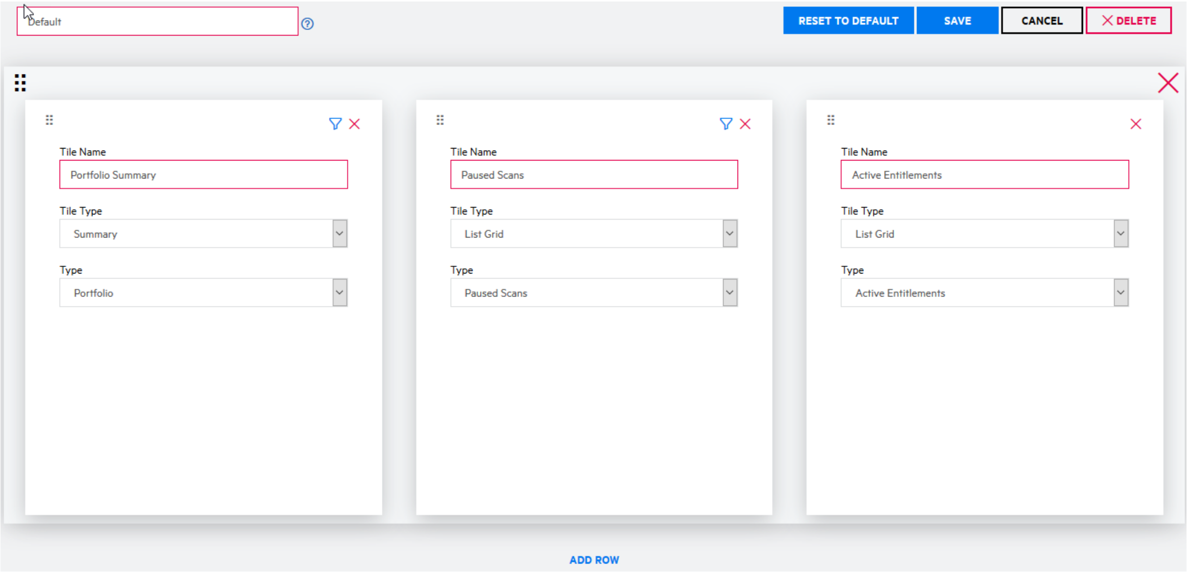
ENTITLEMENT ID	UNITS PURCHASED	UNITS CONSUMED
5575	500	0
5689	500	0

MY WIDGET

CATEGORY	# APPLICATIONS	# ISSUES
Cross-Site Request Forgery	3	306
Cross-Site Scripting: Reflected	4	199
SQL Injection	4	151
Dangerous File Inclusion	1	122
Weak Encryption	1	95
Buffer Overflow	1	80
Privacy Violation	5	44
Null Dereference	4	41
Poor Error Handling: Unhandled Exception	1	34
Other	7	487

2. Select the dashboard that you want to edit from the drop down list.
3. Select **Actions** > **Edit Dashboard**.

The dashboard refreshes in edit mode.



Default

Tile Name: Portfolio Summary
Tile Type: Summary
Type: Portfolio

Tile Name: Paused Scans
Tile Type: List Grid
Type: Paused Scans

Tile Name: Active Entitlements
Tile Type: List Grid
Type: Active Entitlements

4. Perform one or more following tasks to edit the dashboard:

Task	Procedure
Add a tile	a. Perform one of the following actions: ○ Click + in a row to add a tile (if available). ○ Click **Add Row** to add a tile in a new row (if available). **Note**: Each row can contain up to a maximum of three tiles. b. In the **Tile Name** field, type a name for the tile. c. Select the tile type from the **Tile Type** list. For a description of the tile types, see "Dashboard Graph Types" on page 225. d. Perform the relevant action based on the tile type you selected. ○ If you selected **Gauge**, select the data item to be represented from the **Type** list. ○ If you selected **List Grid**, select the data item to be represented from the **Type** list. ○ If you selected **Summary**, select the data item to be represented from the **Type** list. The current available value is **Portfolio**. ○ If you selected **Trending Chart**, select the data item to be represented from the **Data Type** list, select the time period of the graph from the **Resolution** list, and select the attributes by which to group the data from the **Group By** lists.

	e. If applicable, click ▽ and select the filter values to be applied. The filters that are available depend on the data item type selected.
Edit a tile	Choose an existing tile to edit and update the fields as needed.
Move a row/tile	Click ⠿ and drag the row/tile to the desired slot. **Note:** You can move a tile within a row, but you cannot move a tile to another row.
Delete a row/tile	Click × next to the row/tile.
Reset dashboard to the default configuration	Click **Reset to Default**.
Return to the view mode without saving changes	Click **Cancel**.

5. Click **Save**.

   The dashboard refreshes with your changes.

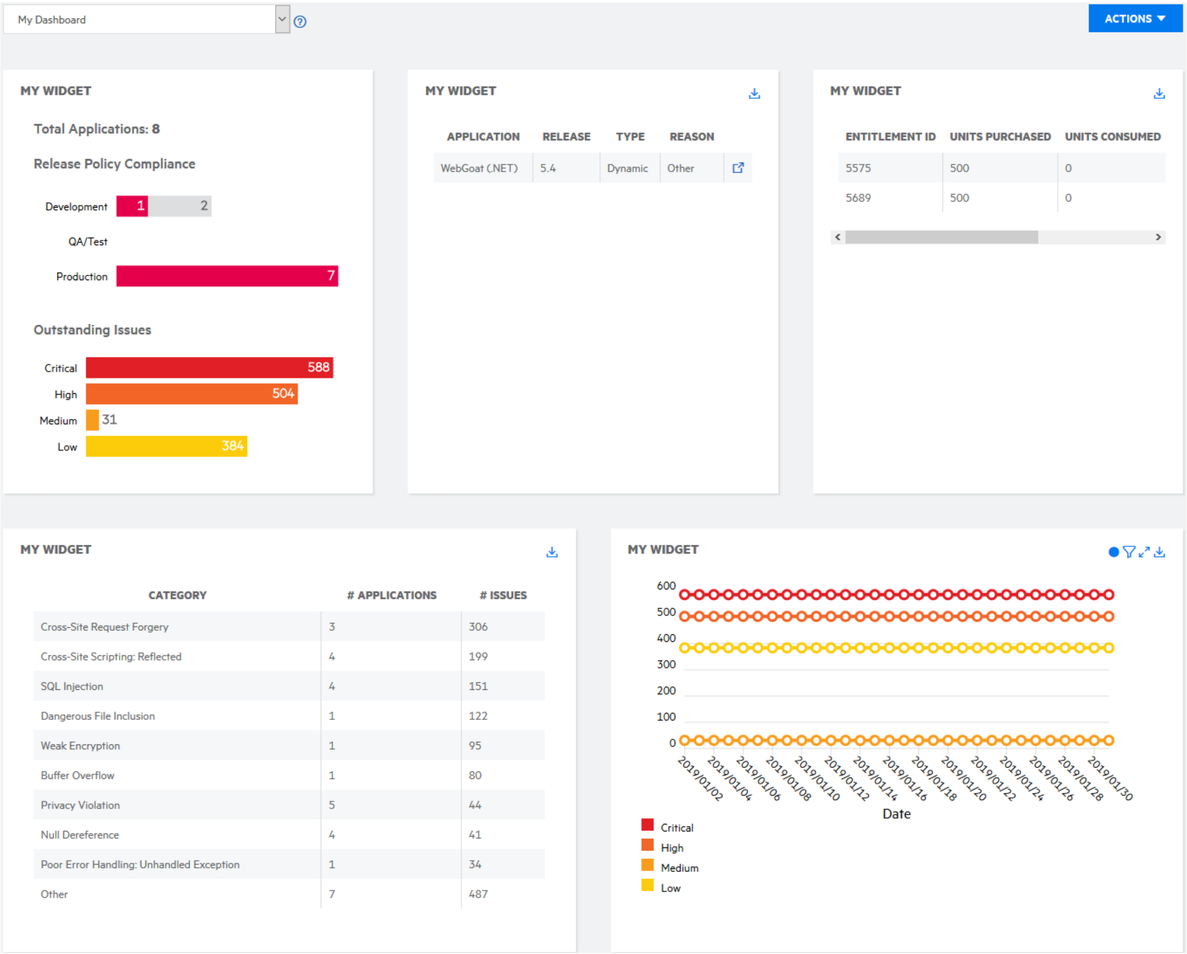
Deleting a Dashboard

To delete a dashboard, you must have at least one other dashboard. If you want to delete your only dashboard, you will need to first create another one.

To delete a dashboard:

1. Select the **Dashboard** view.

   The dashboard page appears. It displays the last dashboard that was loaded.



APPLICATION	RELEASE	TYPE	REASON
WebGoat (.NET)	5.4	Dynamic	Other

ENTITLEMENT ID	UNITS PURCHASED	UNITS CONSUMED
5575	500	0
5689	500	0

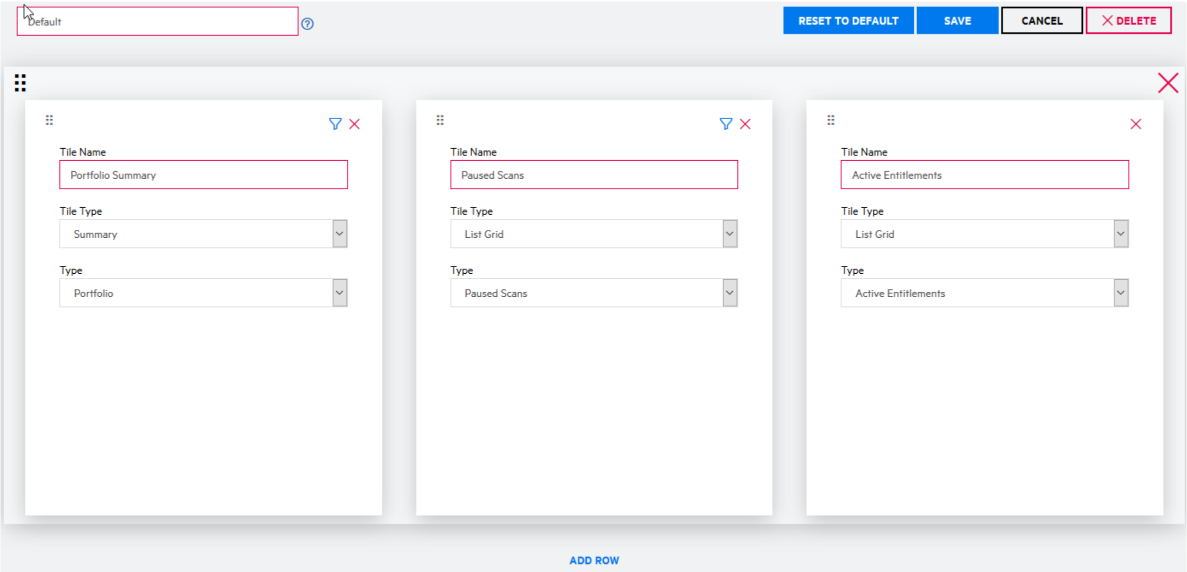
CATEGORY	# APPLICATIONS	# ISSUES
Cross-Site Request Forgery	3	306
Cross-Site Scripting: Reflected	4	199
SQL Injection	4	151
Dangerous File Inclusion	1	122
Weak Encryption	1	95
Buffer Overflow	1	80
Privacy Violation	5	44
Null Dereference	4	41
Poor Error Handling: Unhandled Exception	1	34
Other	7	487

2. Select the dashboard that you want to delete from the drop down list.

   The selected dashboard is loaded.

3. Select **Actions** > **Edit Dashboard**.

   The dashboard refreshes in edit mode.



Default

Tile Name: Portfolio Summary
Tile Type: Summary
Type: Portfolio

Tile Name: Paused Scans
Tile Type: List Grid
Type: Paused Scans

Tile Name: Active Entitlements
Tile Type: List Grid
Type: Active Entitlements

4. Click **Delete**.

   A confirmation message appears.

5. Click **Yes**.

   The dashboard is deleted.

Reports

Fortify on Demand offers the ability to generate detailed reports of assessment results. You can generate the following types of reports:

- Pre-defined system reports
- Custom reports
- Data exports of applications, releases, scans, issues, or entitlement consumption
- Vendor reports if you are using the Vendor Management feature

> **Note:** Open source component reports are available through the Fortify on Demand report functionality. You can use the Open Source Component system template to generate a report. The template includes the following modules:
>
> - Open Source Bill-of-Materials: a complete list of the components detected in your application
> - Vulnerable Open Source Components: a list of components with known security issues

This section contains the following topics:

Viewing Reports

There are two ways to view reports in the portal. One way is to go through the **Reports** view, where you can view all reports generated for all applications and releases in your tenant. The other way is to go through the **Applications** view, where you can drill down into each application and view reports pertaining to a specific application or release.

This section contains the following topics:

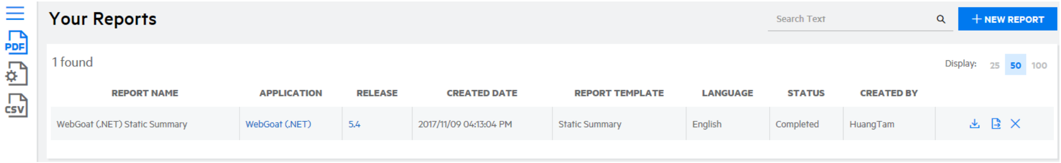
Viewing All Reports

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.



1 found

Display: 25 50 100

REPORT NAME	APPLICATION	RELEASE	CREATED DATE	REPORT TEMPLATE	LANGUAGE	STATUS	CREATED BY
WebGoat (.NET) Static Summary	WebGoat (.NET)	5.4	2017/11/09 04:13:04 PM	Static Summary	English	Completed	HuangTam

The following table describes how to navigate Your Reports page.

Task	Action
Create a report	Click **+New Report**.
Download a report	Click ⤓. The report is downloaded to the local folder specified in your browser settings.
Share a report with a tenant	Click 🗎. Sharing a report is available if you have established a relationship with another tenant. See "Vendor Management" on page 312.

Task	Action
	Note: Sharing a report that contains multiple releases is currently not available.
Delete a report	Click ×.
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 "Searching Applications and Releases" on page 79.

Viewing Application Reports

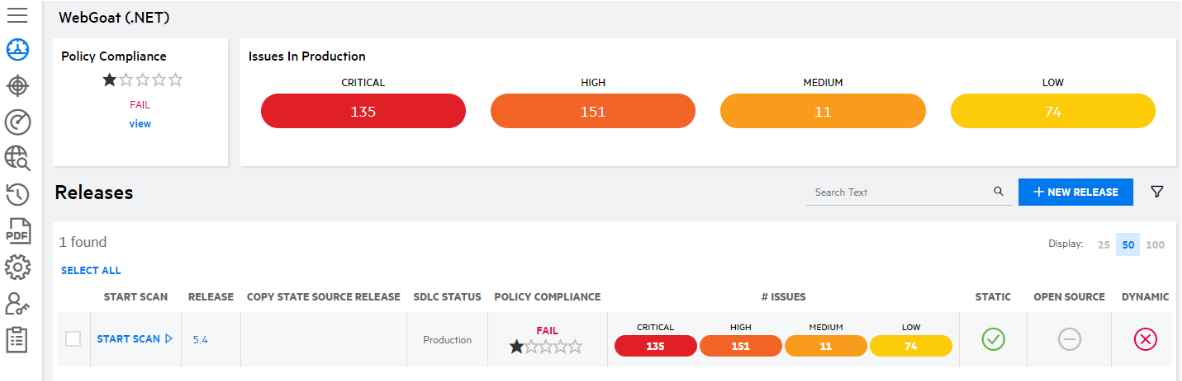
You can view reports for a selected application.

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.



WebGoat (.NET)

Policy Compliance
★☆☆☆☆
FAIL
view

Issues In Production

CRITICAL	HIGH	MEDIUM	LOW
135	151	11	74

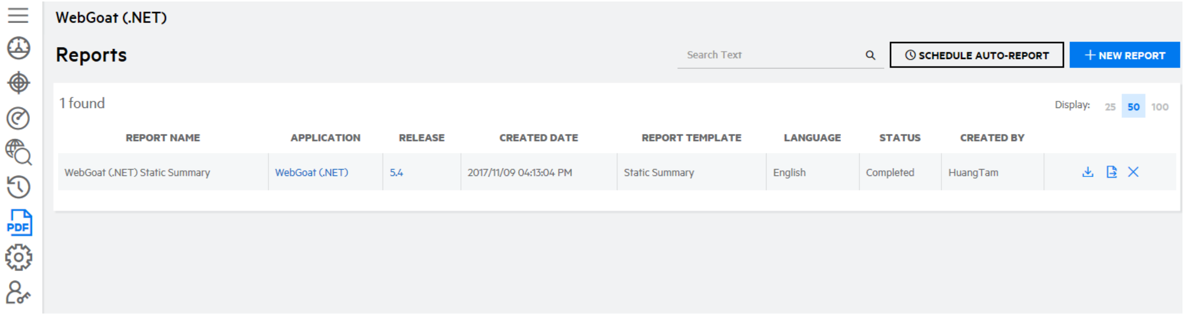
Releases

1 found

	START SCAN	RELEASE	COPY STATE SOURCE RELEASE	SDLC STATUS	POLICY COMPLIANCE	# ISSUES	STATIC	OPEN SOURCE	DYNAMIC
□	START SCAN ▷	5.4		Production	FAIL ★☆☆☆☆	CRITICAL 135 HIGH 151 MEDIUM 11 LOW 74	✓	⊖	⊗

3. Click **Reports**.

   The Reports page, displaying all reports for the application.



1 found

REPORT NAME	APPLICATION	RELEASE	CREATED DATE	REPORT TEMPLATE	LANGUAGE	STATUS	CREATED BY
WebGoat (.NET) Static Summary	WebGoat (.NET)	5.4	2017/11/09 04:13:04 PM	Static Summary	English	Completed	HuangTam

4. Select a report from the list.

Viewing Release Reports

You can drill down into an application and view reports for a selected release.

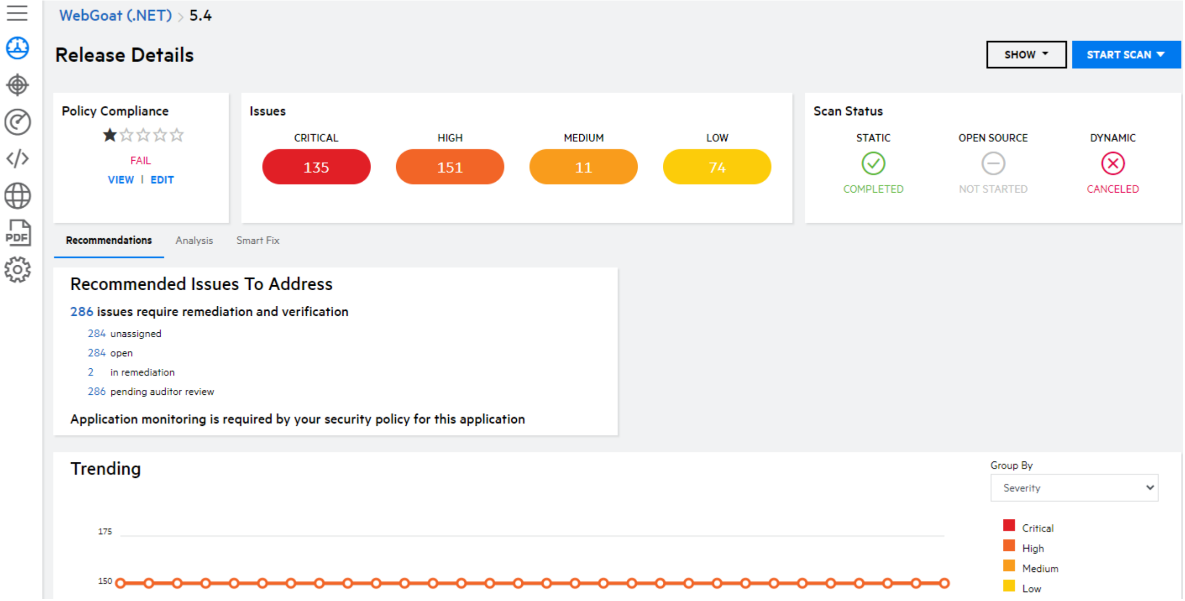
To view reports for a release:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears.
3. Click the name of the release that you want to view reports for.

   The Release Overview page appears.



Recommended Issues To Address

286 issues require remediation and verification

284 unassigned

284 open

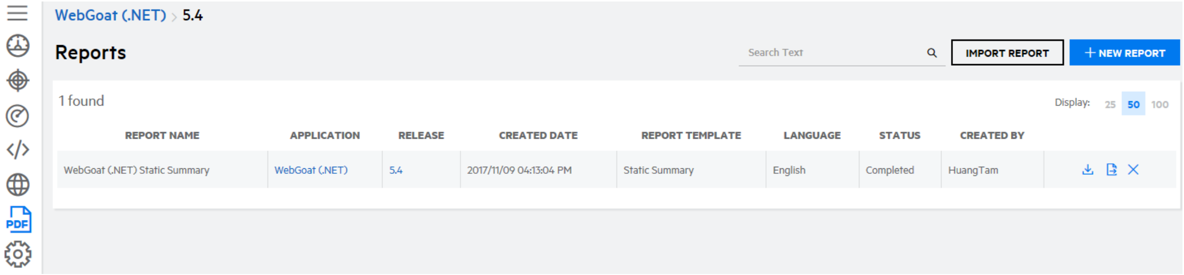
2 in remediation

286 pending auditor review

Application monitoring is required by your security policy for this application

4. Click **Reports**.

   The Reports page appears displaying all reports for the release.



1 found

REPORT NAME	APPLICATION	RELEASE	CREATED DATE	REPORT TEMPLATE	LANGUAGE	STATUS	CREATED BY
WebGoat (.NET) Static Summary	WebGoat (.NET)	5.4	2017/11/09 04:13:04 PM	Static Summary	English	Completed	HuangTam

5. Select a report from the list.

Generating a Report

Use a pre-defined report template or a custom report template to generate a report of a release. Reports are available in PDF and HTML formats. In the event a PDF report generation fails, the HTML version is automatically provided in place of the PDF version for your convenience.

To help avoid failures when generating extremely large PDF reports, you cannot generate PDF reports that include the **Analyst Trace**, **Request/Response**, or **Issues Details** template modules and contain more than 5000 issues. Either generate HTML reports or use an alternative report template with the modules removed and/or with additional filters that reduce the issue count.

Note: To generate reports in a certain language, the language must be selected in your account settings. For more information, see "Editing Your Account Settings" on page 27.

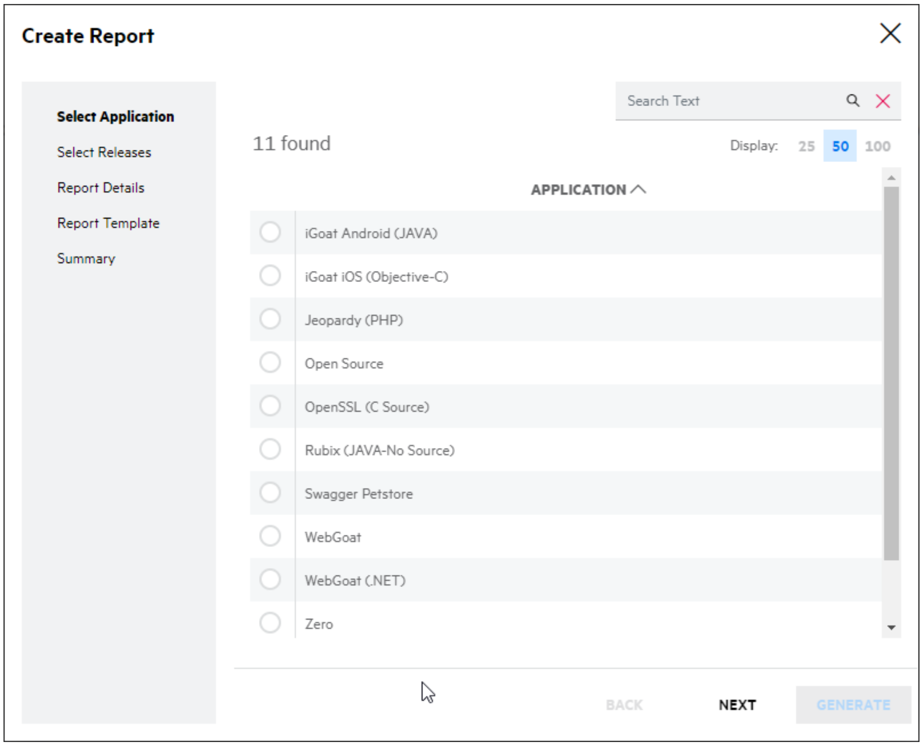
To generate a report:

Note: The following instructions describe how to generate reports on Your Reports page. You can also generate reports on the Application Reports and Release Reports pages.

1. Select the **Reports** view.

   Your Reports page appears.
2. Click **+New Report**.

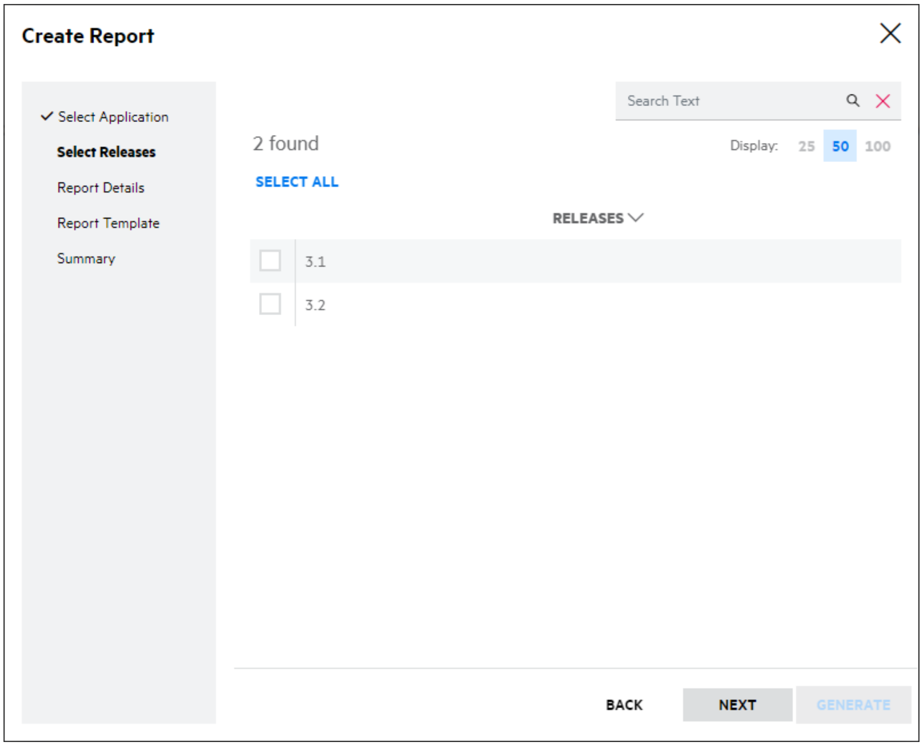
   The Create Report wizard appears.
3. **Select Application**: select the application and click **Next**.



11 found

APPLICATION
○ iGoat Android (JAVA)
○ iGoat iOS (Objective-C)
○ Jeopardy (PHP)
○ Open Source
○ OpenSSL (C Source)
○ Rubix (JAVA-No Source)
○ Swagger Petstore
○ WebGoat
○ WebGoat (.NET)
○ Zero

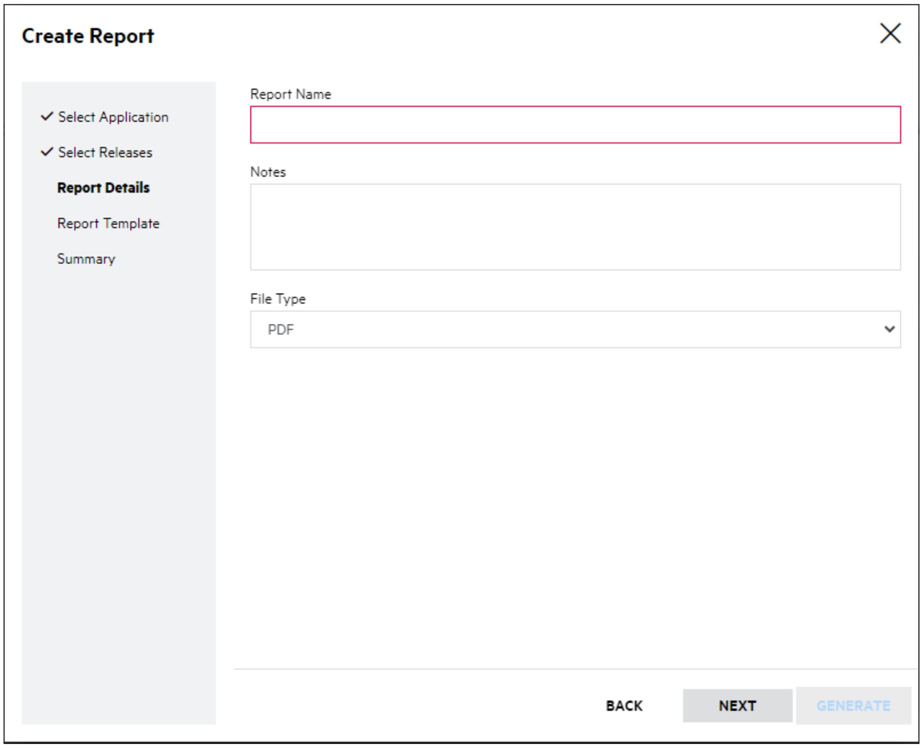
4. **Select Releases**: select the releases and click **Next**. If you select multiple releases, a report will be generated for each release and the reports will be packaged in a zip file.



2 found

RELEASES
□ 3.1
□ 3.2

5. **Report Details**: complete the fields and click **Next**. Fields are required unless otherwise noted.



Create Report

- ✓ Select Application
- ✓ Select Releases
- **Report Details**
- Report Template
- Summary

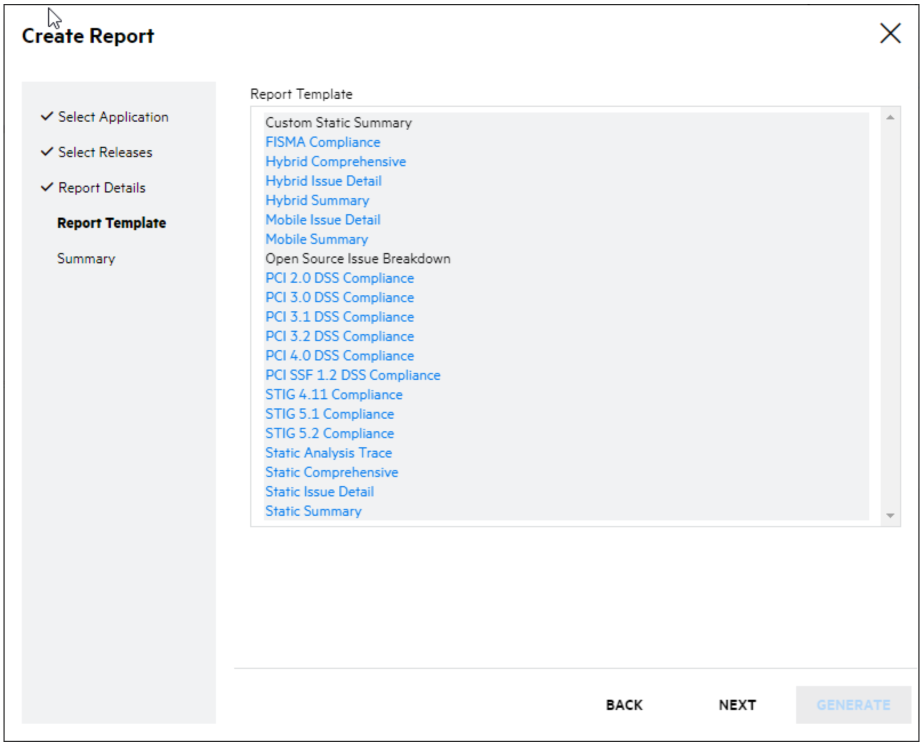
Report Name

Notes

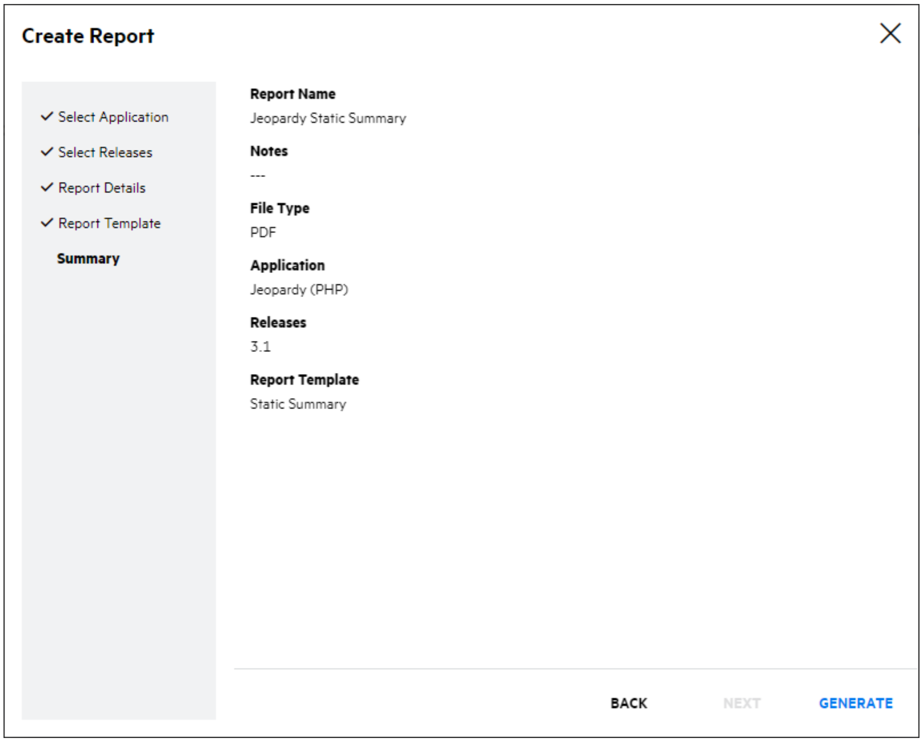
File Type: PDF

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**.



Report Name
Jeopardy Static Summary

Notes

File Type
PDF

Application
Jeopardy (PHP)

Releases
3.1

Report Template
Static Summary

You are redirected to the Reports page. The report is available once the "Completed" status appears.

> **Note:** You can click ☒ to delete a report while it is still being generated.

8. Click ⤓ in the row of the report once it has been generated.
9. A PDF or zip file (depending on the file type) is saved to the folder specified in your browser settings.

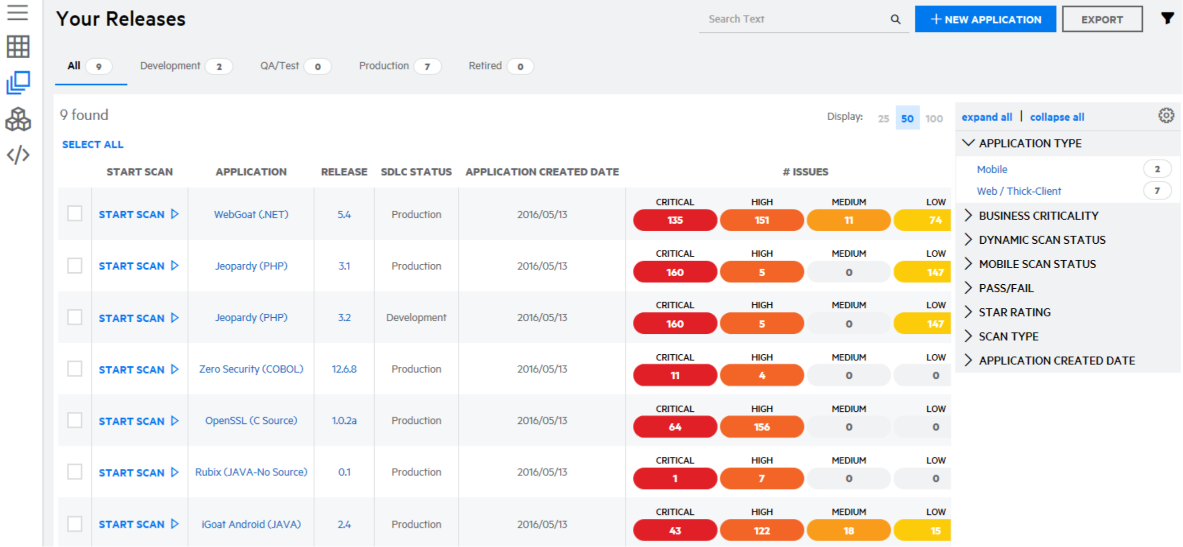
Scheduling Auto-Generated Reports

If you plan to run multiple assessments on the same application and you would like to generate the same reports each time, you can save time by using the auto-generated report function.

To schedule an auto-generated report:

1. Select the **Applications** view.

   Your Releases grid appears, displaying a list of your releases.



Your Releases

All 9 | Development 2 | QA/Test 0 | Production 7 | Retired 0

9 found

Display: 25 50 100

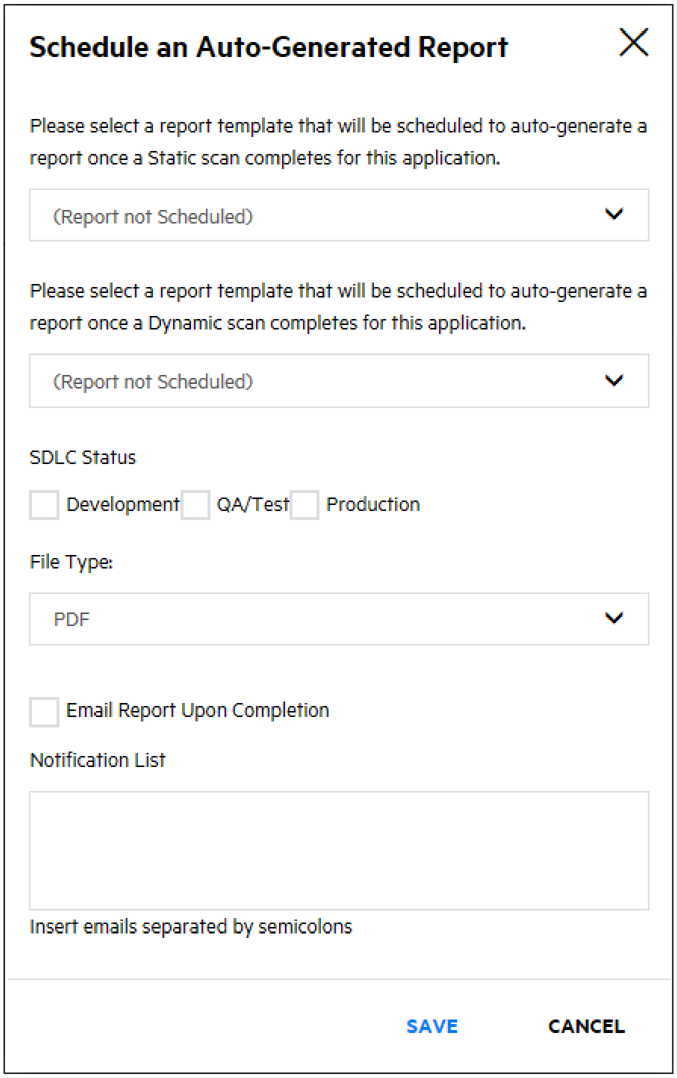
SELECT ALL

	START SCAN	APPLICATION	RELEASE	SDLC STATUS	APPLICATION CREATED DATE	CRITICAL	HIGH	MEDIUM	LOW
□	START SCAN ▷	WebGoat (.NET)	5.4	Production	2016/05/13	135	151	11	74
□	START SCAN ▷	Jeopardy (PHP)	3.1	Production	2016/05/13	160	5	0	147
□	START SCAN ▷	Jeopardy (PHP)	3.2	Development	2016/05/13	160	5	0	147
□	START SCAN ▷	Zero Security (COBOL)	12.6.8	Production	2016/05/13	11	4	0	0
□	START SCAN ▷	OpenSSL (C Source)	1.0.2a	Production	2016/05/13	64	156	0	0
□	START SCAN ▷	Rubix (JAVA-No Source)	0.1	Production	2016/05/13	1	7	0	0
□	START SCAN ▷	iGoat Android (JAVA)	2.4	Production	2016/05/13	43	122	18	15

2. Click the name of the application you want to schedule auto-generated reports for.
3. Click **Reports**.

   The Reports page appears.
4. Click **Schedule Auto-Report**.

   The Schedule an Auto-Generated Report modal window appears.



Schedule an Auto-Generated Report

Please select a report template that will be scheduled to auto-generate a report once a Static scan completes for this application.

(Report not Scheduled)

Please select a report template that will be scheduled to auto-generate a report once a Dynamic scan completes for this application.

(Report not Scheduled)

SDLC Status

□ Development □ QA/Test □ Production

File Type:

PDF

□ Email Report Upon Completion

Notification List

Insert emails separated by semicolons

5. Select the report template that will be used to generate a report upon completion of a static scan.
6. Select the report template that will be used to generate a report upon completion of a dynamic or mobile scan.
7. Select the SDLC status check box(es) that will trigger the report generation.
8. Select the report file type from the **File type** list.
9. To automatically distribute the reports to specified recipients, select **Email Report Upon Completion** and in the **Notification List** field, type the email addresses that will receive the reports.
10. Click **Save**.

    Your auto-generated report settings are saved.

Templates

Users with the Create Report permission can view, create, edit, and delete templates.

The Templates page displays a list of existing report templates, with links for viewing, copying / editing, and deleting templates. There are two types of report templates: system and custom.

System report templates exist for Application Monitoring, Static, Dynamic, Hybrid, and Mobile reports as well as ones for PCI, STIG, and FISMA compliance reports. System templates can be copied and suppressed, but not edited or deleted.

Fortify on Demand provides a **Template Wizard** for creating custom report templates. You can configure the report modules and filters to include in the template and use it to generate reports containing the information most useful to your organization. The custom report templates can be edited and deleted.

> **Use case**: If your report is for high-level management review and the people reading it do not want to see the details of your security assessment, you can select the **Static Summary** template. It includes: a title page, an executive summary, an issue breakdown, a list of issues by analysis type, and the OWASP Top 10. It does not include PCI reporting, comments on the issue details, or an analysis trace report (unless you add those).

This section covers the following topics:

Creating a Custom Report Template

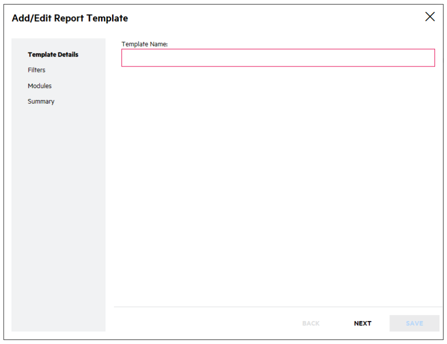
You can create a custom report template by either creating a report template from scratch or starting with one of the system template and modifying it to suit your needs.

To create a custom report template:

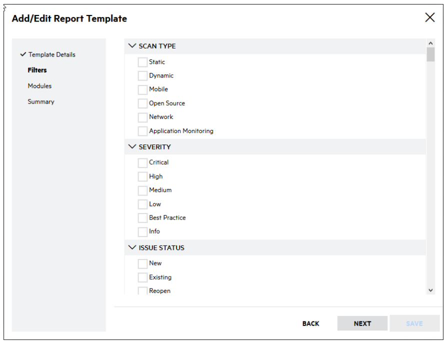
1. Select the **Reports** view.
2. Click the **Templates** icon.

   The Templates page appears.
3. Perform one of the following actions:
   - Click **+New Template** to create a template from scratch.
   - Click the ⧉ icon in the desired system template row to clone the template.

   The Add/Edit Report Template wizard appears.
4. **Template Details**: in the **Template Name** field, type the name of the new template and click **Next**.

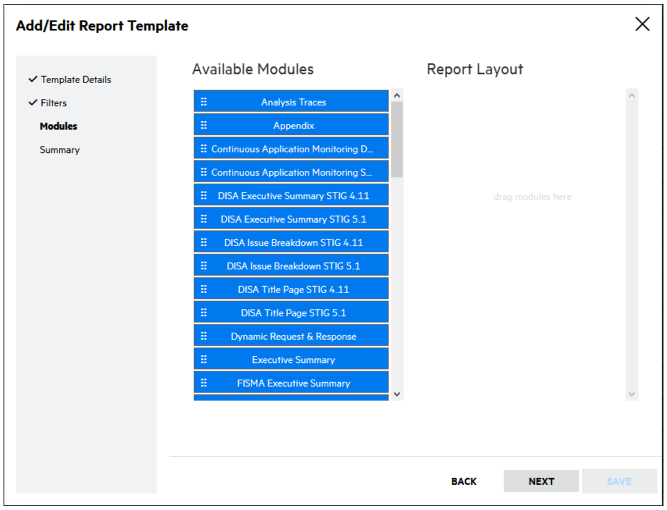


5. **Filters**: select the desired filters and click **Next**. Fields are required unless otherwise noted.

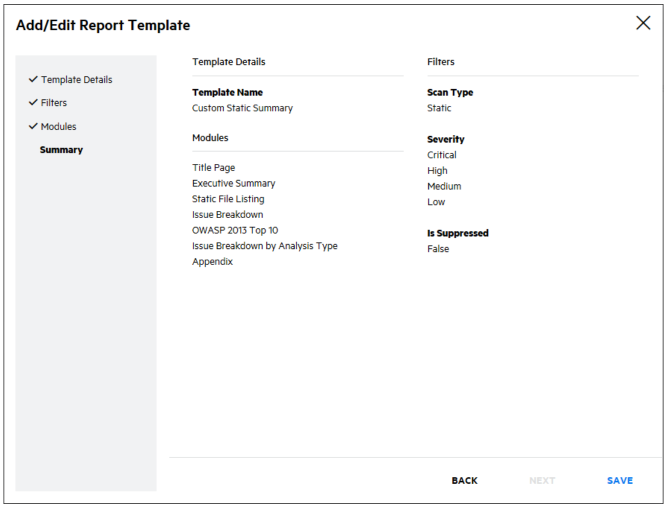


Field	Description
Scan Type	Scan type
Severity	(Optional) Severity of the issues
Issue Status	(Optional) Status of the issues **(New**, **Existing**, **Reopen**)
Developer Status	(Optional) Developer status of the issues
Auditor Status	(Optional) Auditor status of the issues
Issue Age	(Optional) Days since the issues were first introduced
Category	(Optional) Vulnerability category of the issues
Is Suppressed	(Optional) Suppression state of issues (default value is **False**)

6. **Modules**: select the report modules to include in the template and click **Next**.
   - Drag the modules that you want to include from the **Available Modules** column to the **Report Layout** column. The modules that are available depend on the selected scan type.
   - Drag and drop items in the **Reports Layout** column to change the order of the modules in the generated report.


Add/Edit Report Template
✓ Template Details
✓ Filters
Modules
Summary
Available Modules
Report Layout
Analysis Traces
Appendix
Continuous Application Monitoring D...
Continuous Application Monitoring S...
DISA Executive Summary STIG 4.11
DISA Executive Summary STIG 5.1
DISA Issue Breakdown STIG 4.11
DISA Issue Breakdown STIG 5.1
DISA Title Page STIG 4.11
DISA Title Page STIG 5.1
Dynamic Request & Response
Executive Summary
FISMA Executive Summary
drag modules here
BACK
NEXT
SAVE

7. **Summary**: review the summary of the template and click **Save**.



Template Details

Template Name
Custom Static Summary

Modules

Title Page
Executive Summary
Static File Listing
Issue Breakdown
OWASP 2013 Top 10
Issue Breakdown by Analysis Type
Appendix

Filters

Scan Type
Static

Severity
Critical
High
Medium
Low

Is Suppressed
False

The custom report template appears in the template list. If necessary, run a search of the name to find the template.

Editing a Custom Report Template

You can edit an existing custom report template through the Add/Edit Report Template wizard.

To edit a custom report template:

1. Select the **Reports** view.
2. Click **Templates**.

   The Templates page appears.
3. Click the ✎ icon in the row of the template that you want to edit.

   The Add/Edit Report Template wizard appears.

4. Edit the fields in each step of the wizard as needed. For more information, see "Creating a Custom Report Template" on page 244

   > **Note:** Removal of deprecated modules is permanent and cannot be undone after the template is saved.

5. Click **Save**.

   The template changes are saved.

Deleting a Custom Report Template

You can delete any of your custom report templates in your tenant.

To delete a custom report template:

1. Select the **Reports** view.
2. Click **Templates**.

   The **Templates** page appears.
3. Locate the custom template that you want to delete in the template list.
4. Click the × icon in the template row.

   A confirmation message appears.
5. Click **Yes** to delete the template.

Suppressing a System Report Template

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

1. Select the **Reports** view.
2. Click **Templates**.

   The **Templates** page appears.
3. Click the 👁 icon next to the system template that you want to suppress.

   A confirmation message appears.
4. Click **Yes** to confirm the system report template suppression.

   The system report template is shown as suppressed. You can click the ↶ icon to restore the system report template to users in the portal.

Data Exports

A data export is a complete list of relevant data for a specific category (applications, releases, scans, issues, or entitlement consumption) across the tenant. Users with the Export Data permission can generate data exports. The data export is provided as a CSV file.

This section covers the following topics:

Viewing Data Exports

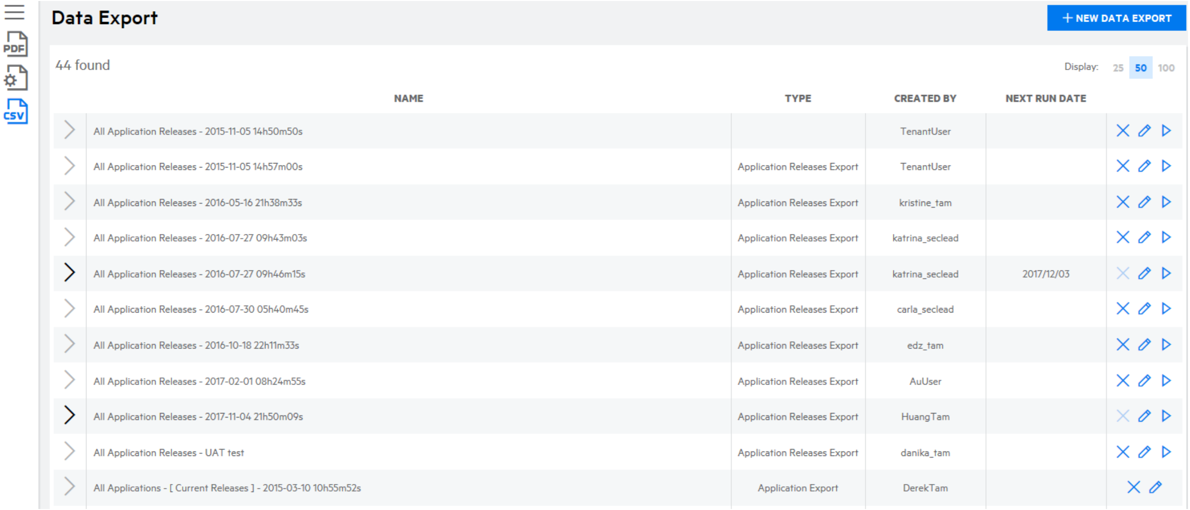
To view data exports:

1. Click the **Reports** view.

   Your Reports page appears

2. Click **Data Export**.

   The Data Export page appears.

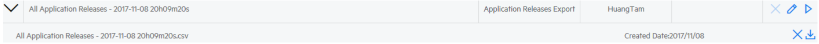


Data Export

44 found

	NAME	TYPE	CREATED BY	NEXT RUN DATE	
>	All Application Releases - 2015-11-05 14h50m50s		TenantUser		✕ ✎ ▷
>	All Application Releases - 2015-11-05 14h57m00s	Application Releases Export	TenantUser		✕ ✎ ▷
>	All Application Releases - 2016-05-16 21h38m33s	Application Releases Export	kristine_tam		✕ ✎ ▷
>	All Application Releases - 2016-07-27 09h43m03s	Application Releases Export	katrina_seclead		✕ ✎ ▷
>	All Application Releases - 2016-07-27 09h46m15s	Application Releases Export	katrina_seclead	2017/12/03	✕ ✎ ▷
>	All Application Releases - 2016-07-30 05h40m45s	Application Releases Export	carla_seclead		✕ ✎ ▷
>	All Application Releases - 2016-10-18 22h11m33s	Application Releases Export	edz_tam		✕ ✎ ▷
>	All Application Releases - 2017-02-01 08h24m55s	Application Releases Export	AuUser		✕ ✎ ▷
>	All Application Releases - 2017-11-04 21h50m09s	Application Releases Export	HuangTam		✕ ✎ ▷
>	All Application Releases - UAT test	Application Releases Export	danika_tam		✕ ✎ ▷
>	All Applications - [Current Releases] - 2015-03-10 10h55m52s	Application Export	DerekTam		✕ ✎

The following table describes how to navigate the Data Export page.

Task	Action
Create a data export template	Click **+Create Data Export**. For more information, see "Creating a Data Export Template" on the next page.
Generate a data export using an existing template	Click ▷ in the row of a template. For more information, see "Generating a Data Export" on page 253.
Edit a data export template	Click ✎ in the row of a template.
Delete a data export template	Click ✕ in the row of a template. You cannot delete a template if it has an existing data export.
View generated data exports for a template	Click > in the row of a template to view files that have been generated in the last three months for the template.  All Application Releases - 2017-11-08 20h09m20s | Application Releases Export | HuangTam All Application Releases - 2017-11-08 20h09m20s.csv | Created Date:2017/11/08

Task	Action
Delete a data export	Click ✕ in the row of a data export. If a data export is still running, it will be canceled.
Download a data export file	Click ⤓ in the row of a data export.

Creating a Data Export Template

A data export template is used as a basis for generating data exports. You can apply filters as well as schedule recurring data exports.

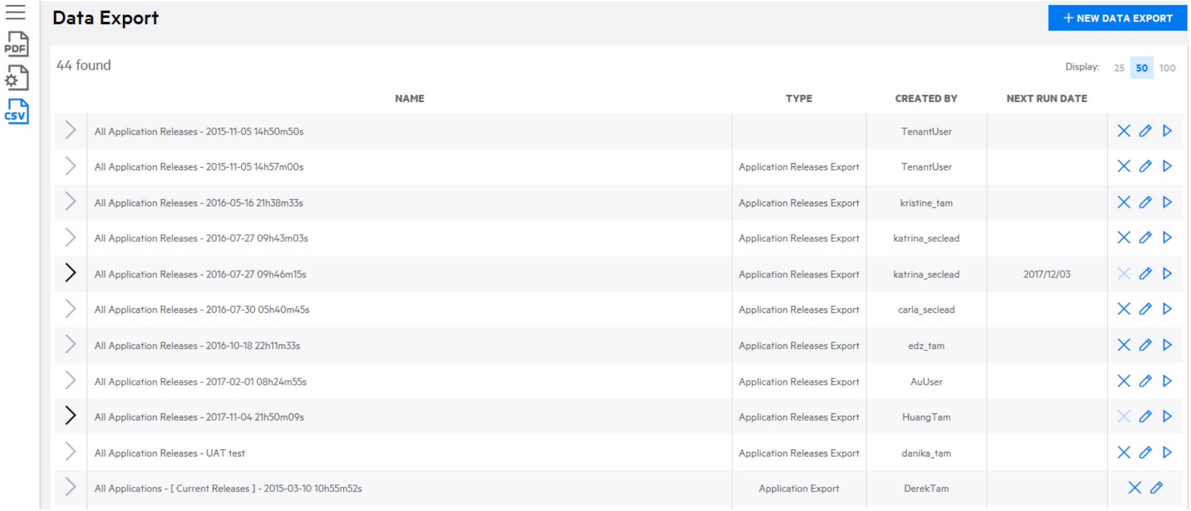
To create a data export template:

1. Click the **Reports** view.

   Your Reports page appears

2. Click **Data Export**.

   The Data Export page appears.

   44 found

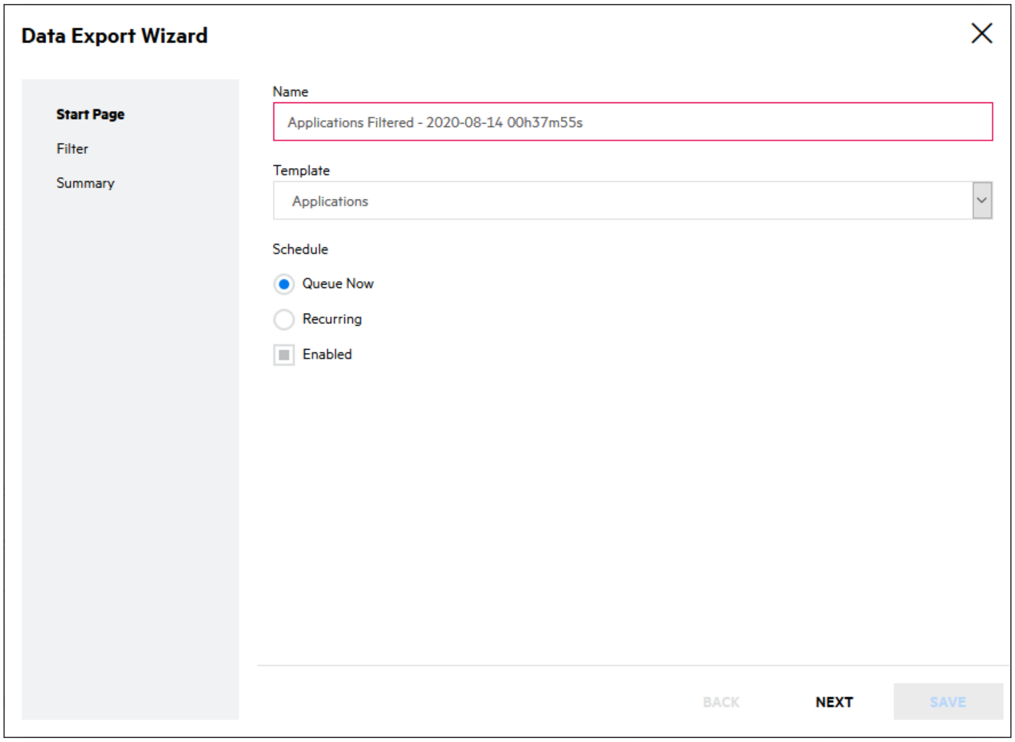
   Display: 25 **50** 100

NAME	TYPE	CREATED BY	NEXT RUN DATE
All Application Releases - 2015-11-05 14h50m50s		TenantUser	
All Application Releases - 2015-11-05 14h57m00s	Application Releases Export	TenantUser	
All Application Releases - 2016-05-16 21h38m33s	Application Releases Export	kristine_tam	
All Application Releases - 2016-07-27 09h43m03s	Application Releases Export	katrina_seclead	
All Application Releases - 2016-07-27 09h46m15s	Application Releases Export	katrina_seclead	2017/12/03
All Application Releases - 2016-07-30 05h40m45s	Application Releases Export	carla_seclead	
All Application Releases - 2016-10-18 22h11m33s	Application Releases Export	edz_tam	
All Application Releases - 2017-02-01 08h24m55s	Application Releases Export	AuUser	
All Application Releases - 2017-11-04 21h50m09s	Application Releases Export	HuangTam	
All Application Releases - UAT test	Application Releases Export	danika_tam	
All Applications - [Current Releases] - 2015-03-10 10h55m52s	Application Export	DerekTam	

3. Click **+Create Data Export**.

   The Data Export wizard appears.

4. **Start Page**: Complete the fields and click **Next**.



Data Export Wizard

Name

Applications Filtered - 2020-08-14 00h37m55s

Template

Applications

Schedule

● Queue Now

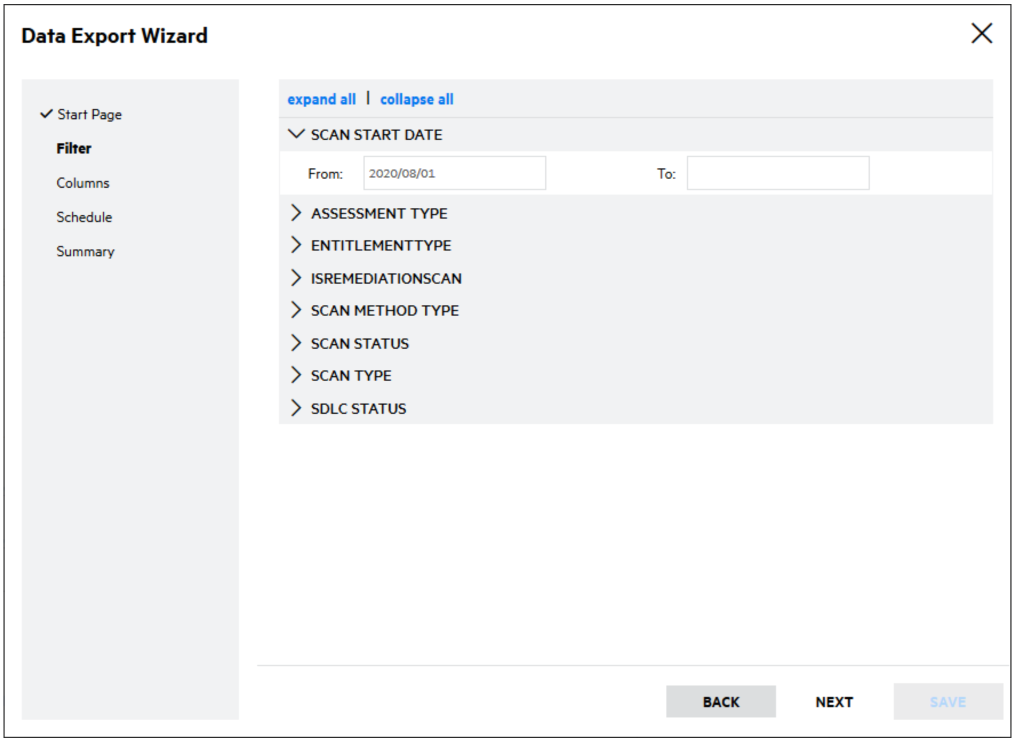
○ Recurring

☐ Enabled

Field	Description
Name	Type the name of the data export template.
Template	Select a data export template type: • **Applications** - list of applications • **Application Releases** - list of releases • **Scans** - list of scans • **Issues** -list of issues • **Entitlement Consumption** - list of scans where entitlements were consumed, including deleted, canceled, and in progress scans. **Note:** Filters are not available for the Entitlement Consumption template type.
Schedule	Select one of the following options for scheduling the data export: • **Queue Now** - queues the data export immediately • **Recurring** - generates the data export according to a schedule that you will specify in the wizard

	When this option is selected, the **Enabled** check box is available. Select the check box to have the data export automatically generated according to the schedule (default). Otherwise, you must manually generate the data export.

5. **Filter**: select the desired filters and click **Next**. The available filters are based on the template type selected.



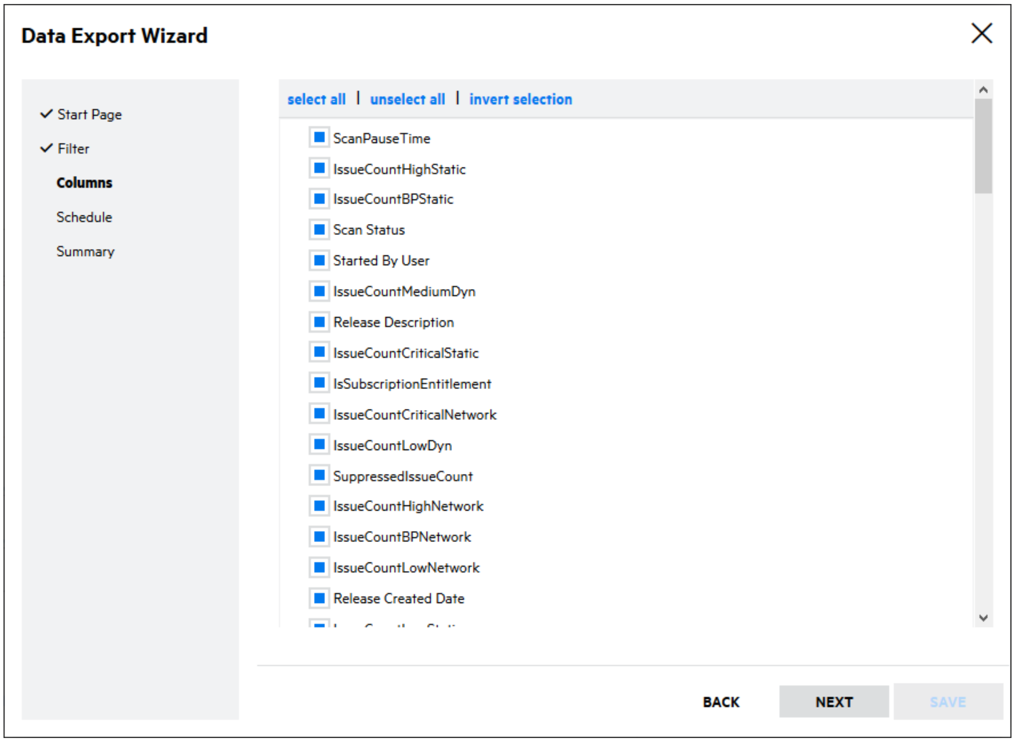
Data Export Wizard

SCAN START DATE

From: 2020/08/01 To:

> **Note:** The **Scan Start Date** filter is required for the scans data export; the **Introduced Date** filter is required for the issues data export.

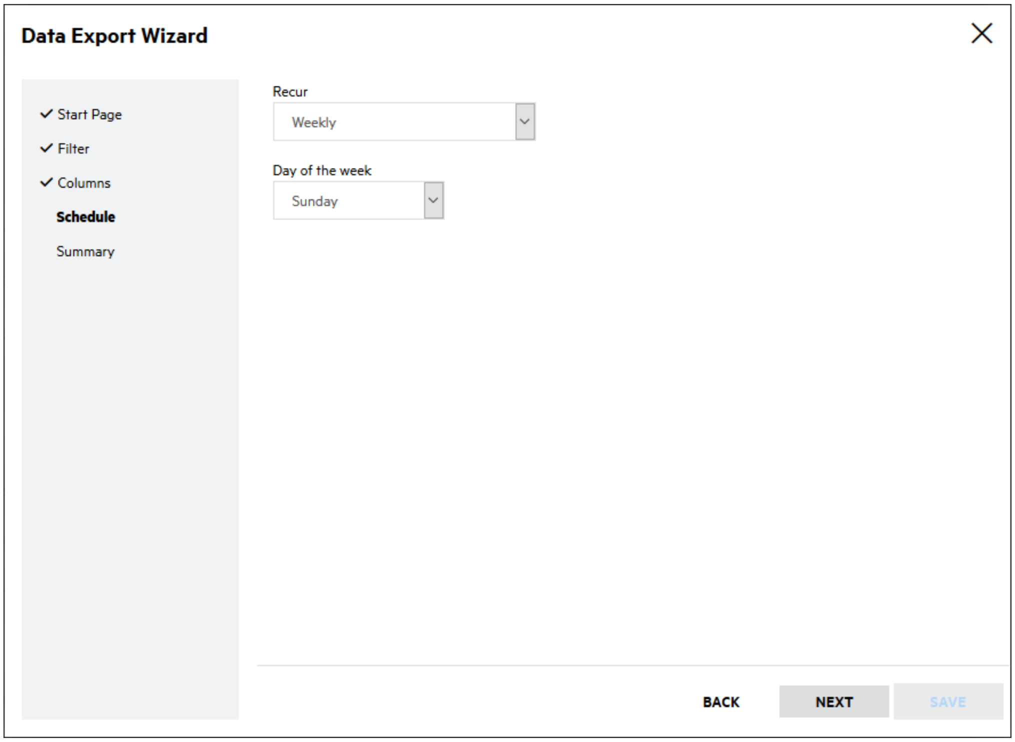
6. **Columns** (available for the scans and issues data exports): select the columns to include in the data export and click **Next**.



- ☑ ScanPauseTime
- ☑ IssueCountHighStatic
- ☑ IssueCountBPStatic
- ☑ Scan Status
- ☑ Started By User
- ☑ IssueCountMediumDyn
- ☑ Release Description
- ☑ IssueCountCriticalStatic
- ☑ IsSubscriptionEntitlement
- ☑ IssueCountCriticalNetwork
- ☑ IssueCountLowDyn
- ☑ SuppressedIssueCount
- ☑ IssueCountHighNetwork
- ☑ IssueCountBPNetwork
- ☑ IssueCountLowNetwork
- ☑ Release Created Date

7. **Schedule** (available for recurring data exports): select the repeat frequency and the day or date to generate the data export. Click **Next**.

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



Recur: Weekly

Day of the week: Sunday

8. Click **Next**.

9. **Summary**: review the summary of the data export and click **Save**.

   The data export template appears in the data export list.

Generating a Data Export

You generate a data export using an existing data export template.

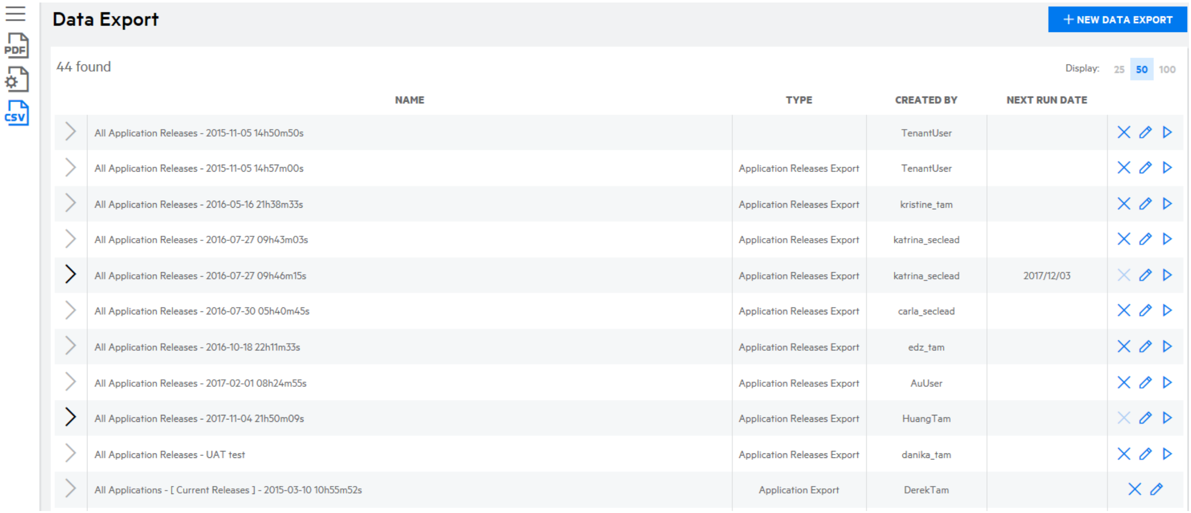
> **Note:** A data export only contains results of completed assessments at the time the data export is generated, with the exception of the Entitlement Consumption data export.

To generate a data export:

1. Click the **Reports** view.

   Your Reports page appears
2. Click **Data Export**.

   The Data Export page appears.



	NAME	TYPE	CREATED BY	NEXT RUN DATE	
>	All Application Releases - 2015-11-05 14h50m50s		TenantUser		✕ ✎ ▷
>	All Application Releases - 2015-11-05 14h57m00s	Application Releases Export	TenantUser		✕ ✎ ▷
>	All Application Releases - 2016-05-16 21h38m33s	Application Releases Export	kristine_tam		✕ ✎ ▷
>	All Application Releases - 2016-07-27 09h43m03s	Application Releases Export	katrina_seclead		✕ ✎ ▷
>	All Application Releases - 2016-07-27 09h46m15s	Application Releases Export	katrina_seclead	2017/12/03	✕ ✎ ▷
>	All Application Releases - 2016-07-30 05h40m45s	Application Releases Export	carla_seclead		✕ ✎ ▷
>	All Application Releases - 2016-10-18 22h11m33s	Application Releases Export	edz_tam		✕ ✎ ▷
>	All Application Releases - 2017-02-01 08h24m55s	Application Releases Export	AuUser		✕ ✎ ▷
>	All Application Releases - 2017-11-04 21h50m09s	Application Releases Export	HuangTam		✕ ✎ ▷
>	All Application Releases - UAT test	Application Releases Export	danika_tam		✕ ✎ ▷
>	All Applications - [Current Releases] - 2015-03-10 10h55m52s	Application Export	DerekTam		✕ ✎

3. Click ▷ in the row of a data export template.

   The data export is queued for generation.
4. Click > next to the template to view the generated data exports.

   A "Processing" status appears until the data export is available.

   > **Note:** You can click ✕ to cancel a long-running data export.
5. Click ⤓ in the row of the data export once it has been generated.

   A CSV file is saved to the folder specified in your browser settings.

Chapter 7: Administration

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

This section contains the following topics:

Portal Management

Security Leads can administer the portal, including configuring portal settings, configuring security, and reviewing the administration event log.

This section covers the following topics:

Configuring User Security

Security Leads can configure the following user security settings:

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

To configure user security settings:

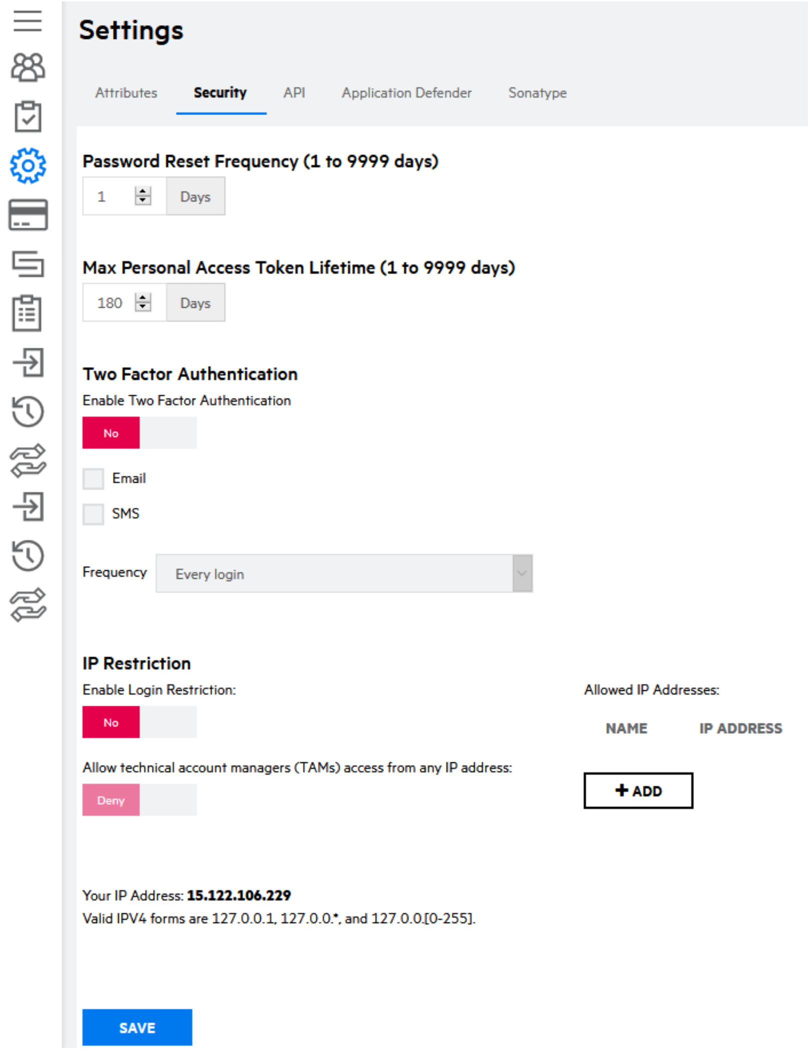
1. Select the **Administration** view.

   The User Settings page appears.

2. Click **Settings**.

   The Settings page appears.

3. Select the **Security** tab.



Password Reset Frequency (1 to 9999 days)

1 Days

Max Personal Access Token Lifetime (1 to 9999 days)

180 Days

Two Factor Authentication

Enable Two Factor Authentication

No

□ Email

□ SMS

Frequency: Every login

IP Restriction

Enable Login Restriction:

No

Allow technical account managers (TAMs) access from any IP address:

Deny

Allowed IP Addresses:

NAME	IP ADDRESS

Your IP Address: **15.122.106.229**

Valid IPV4 forms are 127.0.0.1, 127.0.0.*, and 127.0.0.[0-255].

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

<table>
<tr><td></td><td>of 180 days.</td></tr>
<tr><td>Two-Factor Authentication</td><td>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:
a. In the <b>Enable Two Factor Authentication</b> field, move the move the slider from <b>No</b> to <b>Yes</b> to enable two-factor authentication.
b. Select whether users can receive the login code by email, SMS, or both methods.
c. Select how often a user is prompted for a two factor authentication code from the <b>Frequency</b> list: <b>Every login</b>, <b>4 hours</b>, <b>8 hours</b>, <b>12 hours</b>, <b>24 hours</b>.</td></tr>
<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:
a. In the <b>Enable Login Restriction</b> field, move the move the slider from <b>No</b> to <b>Yes</b> to enable IP restriction.
b. In the <b>Allow technical account managers (TAMs) access from any IP address</b> field, move the slider from <b>No</b> to <b>Yes</b> to allow a TAM to access your tenant from any IP address.
c. 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 <b>+Add</b> and type a name for the IP address (special characters are not allowed) and the IP address. Valid IP address forms are 127.0.0.1, 127.0.0.*, and 127.0.0.[0-255].</td></tr>
<tr><td>Remove an existing IP address from the allowed list</td><td>Click <b>x</b> next to an IP address in the <b>Allow IP Addresses</b> list.</td></tr>
</table></td></tr>
</table>

5. Click **Save**.

Your user security settings are saved.

Managing API Keys

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

> **Note:** This section covers the management of API keys. For information on using the Fortify on Demand API, see "Fortify on Demand API" on page 317

This section covers the following topics:

Creating an API Key

Security Leads can create API keys.

To create an API key:

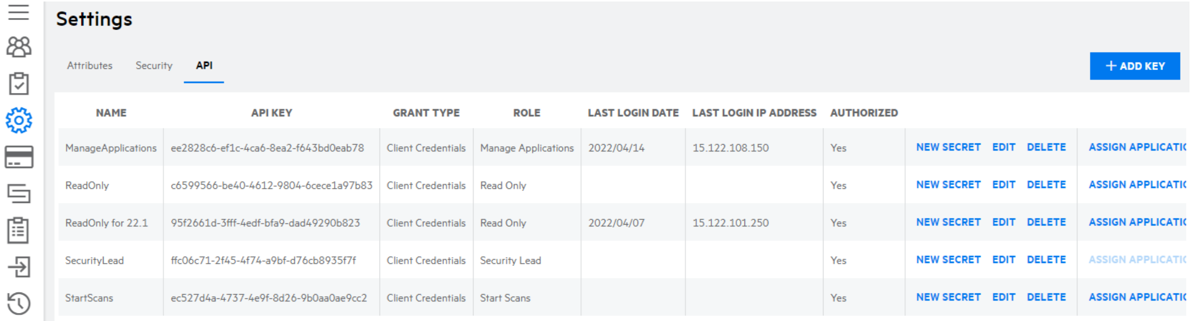
1. Select the **Administration** view.

   The User Management page appears.

2. Click **Settings**.

   The **Attributes** tab of the Settings page appears.

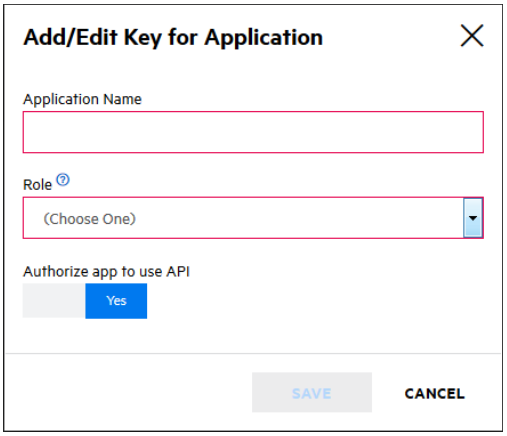
3. Select the **API** tab.



NAME	API KEY	GRANT TYPE	ROLE	LAST LOGIN DATE	LAST LOGIN IP ADDRESS	AUTHORIZED		
ManageApplications	ee2828c6-ef1c-4ca6-8ea2-f643bd0eab78	Client Credentials	Manage Applications	2022/04/14	15.122.108.150	Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
ReadOnly	c6599566-be40-4612-9804-6cece1a97b83	Client Credentials	Read Only			Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
ReadOnly for 22.1	95f2661d-3fff-4edf-bfa9-dad49290b823	Client Credentials	Read Only	2022/04/07	15.122.101.250	Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
SecurityLead	ffc06c71-2f45-4f74-a9bf-d76cb8935f7f	Client Credentials	Security Lead			Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
StartScans	ec527d4a-4737-4e9f-8d26-9b0aa0ae9cc2	Client Credentials	Start Scans			Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI

4. Click **+Add Key**.

   The **Add/Edit Key for Application** window opens.



Add/Edit Key for Application

Application Name

Role

(Choose One)

Authorize app to use API

Yes

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" below.
Authorize app to use API	Select **Yes** to enable the key. Select **No** to disable key if it is not in use.

6. Click **Save**.

   The Secret Key window opens.

7. Copy your Base64 encoded secret code. The secret code is only shown once.
8. Click **Close**.

   The new API key appears in the API key list.

> **Note:** By default, an API key has access to all applications. See "Editing or Deleting an API Key" on the next page for information on assigning applications to an API key.

API Key Roles

A dedicated API key is associated with a role having a predefined, unmodifiable set of permissions. API keys have access to all applications in a tenant; applications can be assigned to API keys to update application access.

The following table lists the permission set of each API key role.

Role	Permissions	Usage Example
Security Lead	All permissions	Full access to all AppSec program functionality and associated

Role	Permissions	Usage Example
		infrastructure
Manage Applications	View Third Party Apps, Manage Applications, Audit Issues, Create Reports, Start Static/Dynamic/Mobile Scans	Integration with full-featured custom or internal systems without the ability to manage users
Start Scans	View Third Party Apps, View Applications, View Issues, View Reports, Start Static/Dynamic/Mobile Scans	Continuous integration and build servers
Read Only	View Third Party Apps, View Applications, View Issues, View Reports	Data import into vulnerability management or Governance, Risk Management, and Compliance (GRC) systems

Editing or Deleting an API Key

Security Leads can perform the following tasks for API keys:

- Generate a new secret
- Edit API key settings
- Assign and unassign applications

> **Note:** API keys with the Security Lead role have access to all applications; this cannot be changed.

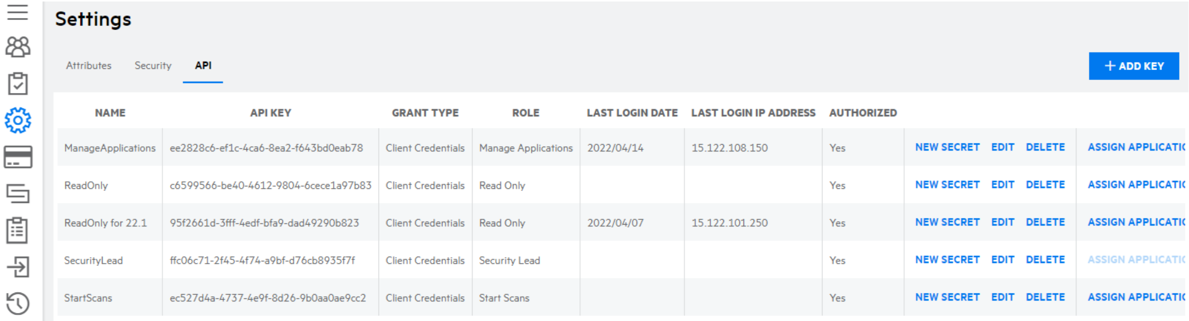
- Delete API keys

To make changes to an API key:

1. Select the **Administration** view.

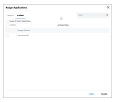
   The User Management page appears.
2. Click **Settings**.

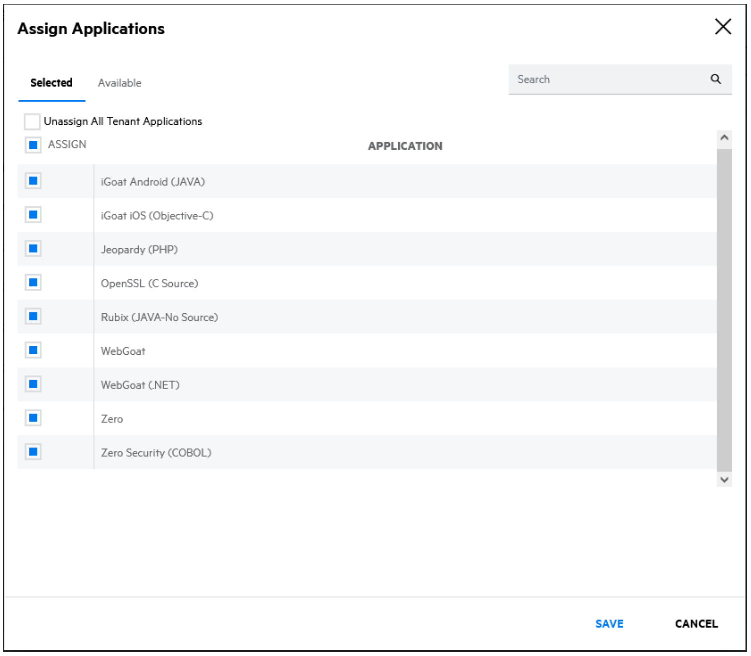
   The **Attributes** tab of the Settings page appears.
3. Select the **API** tab.



NAME	API KEY	GRANT TYPE	ROLE	LAST LOGIN DATE	LAST LOGIN IP ADDRESS	AUTHORIZED		
ManageApplications	ee2828c6-ef1c-4ca6-8ea2-f643bd0eab78	Client Credentials	Manage Applications	2022/04/14	15.122.108.150	Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
ReadOnly	c6599566-be40-4612-9804-6cece1a97b83	Client Credentials	Read Only			Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
ReadOnly for 22.1	95f2661d-3fff-4edf-bfa9-dad49290b823	Client Credentials	Read Only	2022/04/07	15.122.101.250	Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
SecurityLead	ffc06c71-2f45-4f74-a9bf-d76cb8935f7f	Client Credentials	Security Lead			Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI
StartScans	ec527d4a-4737-4e9f-8d26-9b0aa0ae9cc2	Client Credentials	Start Scans			Yes	NEW SECRET EDIT DELETE	ASSIGN APPLICATI

4. You can perform the following tasks:

Task	Procedure
Generate new secret	a. Click **New Secret**. A confirmation message appears b. Click **Yes**. This will void the current secret.
Edit API key settings	a. Click **Edit**. The Add/Edit Key for Application window opens. b. Edit the fields as needed.
Delete API key	a. Click **Delete**. A confirmation message appears. b. Click **Yes**.
Assign applications to API key	a. Click **Assign Applications**. b. Select the **Available** tab.  c. 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. You can use the search field to filter the application list. d. Click **Save**.

Task	Procedure
Unassign applications from API key	a. Click **Assign Applications**. b. Select the **Selected** tab.  Assign Applications Selected Available Search SAVE CANCEL □ Unassign All Tenant Applications ☑ ASSIGN APPLICATION ☑ iGoat Android (JAVA) ☑ iGoat iOS (Objective-C) ☑ Jeopardy (PHP) ☑ OpenSSL (C Source) ☑ Rubix (JAVA-No Source) ☑ WebGoat ☑ WebGoat (.NET) ☑ Zero ☑ Zero Security (COBOL) c. 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. You can use the search field to filter the application list. d. Click **Save**.

Managing Attributes

Attributes provide additional information about applications; they are used as filters to help track applications, releases, and issues. Attributes are for informational purposes and do not affect the assessment process in any way.

Security Leads can add, edit, and delete attributes. System-level attributes are pre-defined and can not be deleted; certain system attributes are editable.

The following attribute types are available:

- Application attributes. Applications attributes are both system and custom attributes.
- Microservice attributes. Microservice attributes are custom attributes.
- Release attributes. Release attributes are system attributes.
- Issue attributes. Issue attributes are system attributes. The following issue attributes are editable: **Auditor Status (Open)**, **Auditor Status (Closed)**, **Developer Status (Open)**, and **Developer Status (Closed)**.

This section covers the following topics:

Adding an Attribute

Security Leads can add microservice and application attributes.

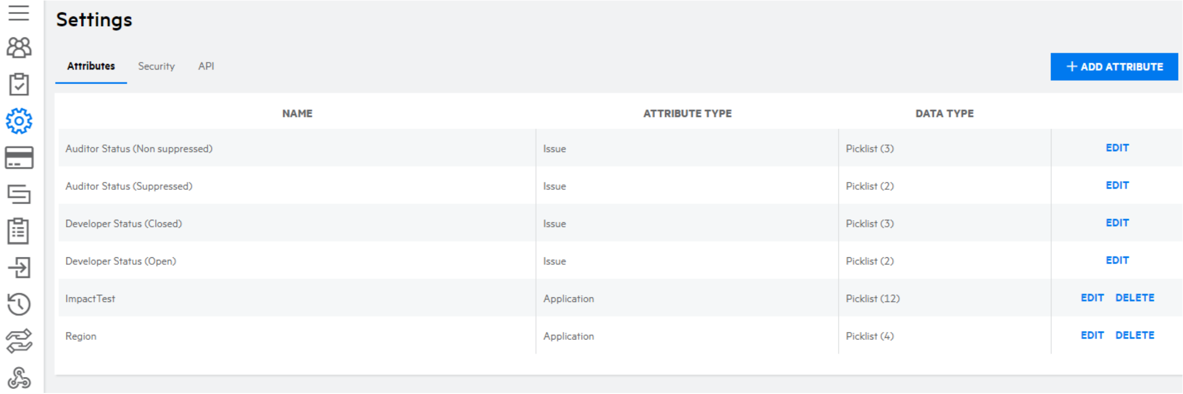
To add an attribute:

1. Select the **Administration** view.

   The User Settings page appears.

2. Click **Settings**.

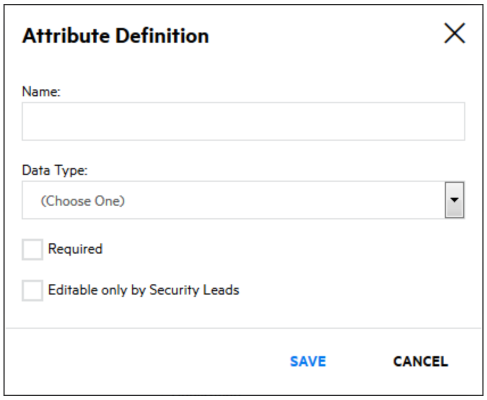
   The **Attributes** tab of the Settings page appears.



NAME	ATTRIBUTE TYPE	DATA TYPE	
Auditor Status (Non suppressed)	Issue	Picklist (3)	EDIT
Auditor Status (Suppressed)	Issue	Picklist (2)	EDIT
Developer Status (Closed)	Issue	Picklist (3)	EDIT
Developer Status (Open)	Issue	Picklist (2)	EDIT
ImpactTest	Application	Picklist (12)	EDIT DELETE
Region	Application	Picklist (4)	EDIT DELETE

3. Click **+Add Attribute**.

   The Attribute Definition window appears.



Attribute Definition

Name:

Data Type:
(Choose One)

□ Required

□ Editable only by Security Leads

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.
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 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.

5. Click **Save**.

   The new attribute appears in the attribute list.

Editing an Attribute

Security Leads can edit picklist values and certain settings for existing attributes. You can not change the attribute name or attribute type.

> **Note:** You can edit the values of issue attributes. For the **Developer Status (Open)** attribute, the default values of **Open** and **In Remediation** are non-editable.

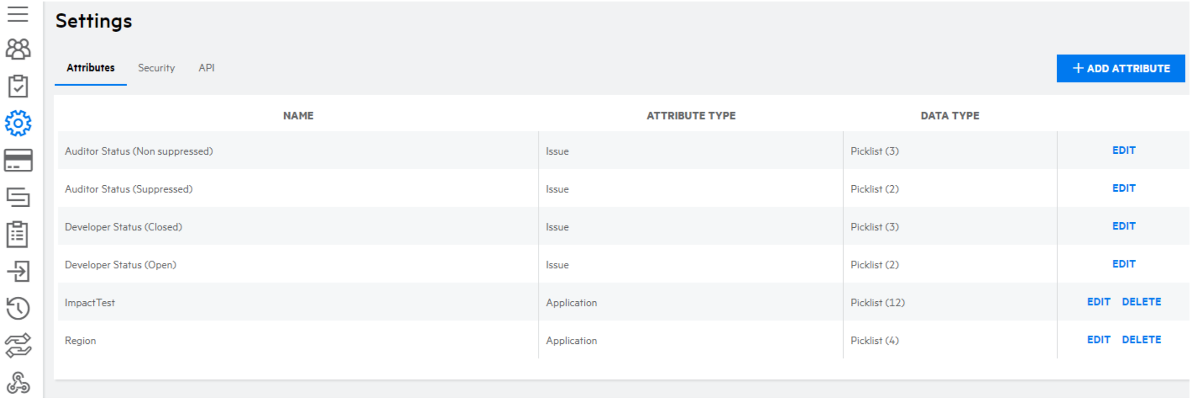
To edit an attribute:

1. Select the **Administration** view.

   The User Settings page appears.

2. Click **Settings**.

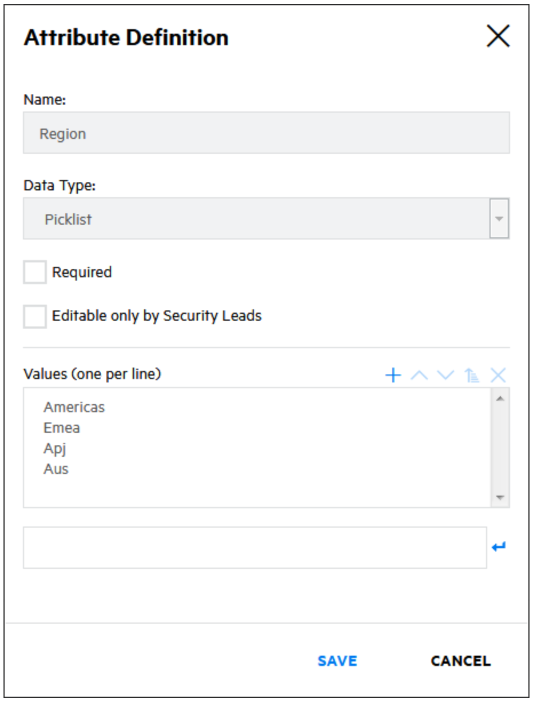
   The **Attributes** tab of the Settings page appears.



NAME	ATTRIBUTE TYPE	DATA TYPE	
Auditor Status (Non suppressed)	Issue	Picklist (3)	EDIT
Auditor Status (Suppressed)	Issue	Picklist (2)	EDIT
Developer Status (Closed)	Issue	Picklist (3)	EDIT
Developer Status (Open)	Issue	Picklist (2)	EDIT
ImpactTest	Application	Picklist (12)	EDIT DELETE
Region	Application	Picklist (4)	EDIT DELETE

3. Click **Edit** in the row of the attribute that you want to edit.

   The **Attribute Definition** page displays.



Attribute Definition

Name: Region

Data Type: Picklist

□ Required

□ Editable only by Security Leads

Values (one per line)

Americas
Emea
Apj
Aus

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 the ︿ ﹀ to reorder the listed values. • Click ⇅ to sort values alphabetically. • Click × 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

Deleting an Attribute

You can delete custom attributes. System-level attributes cannot be deleted.

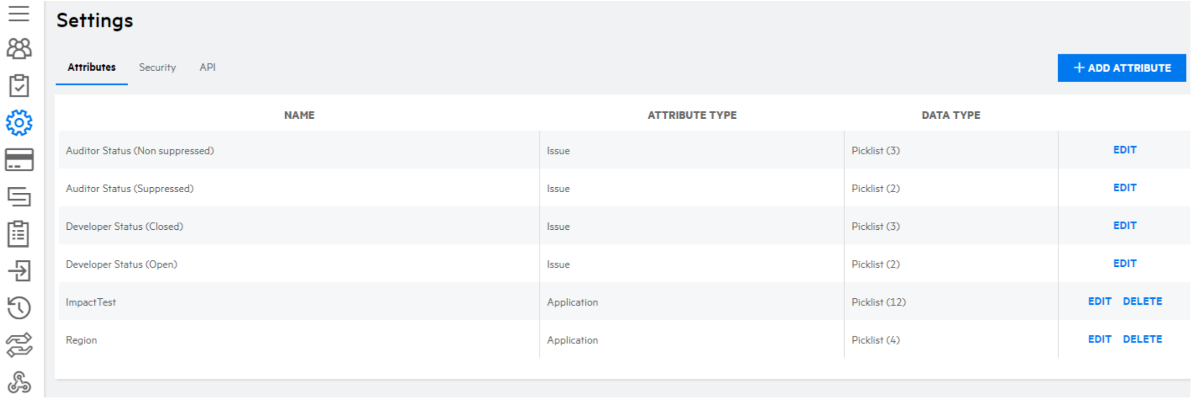
To delete an attribute:

1. Select the **Administration** view.

   The User Settings page appears.

2. Click **Settings**.

   The **Attributes** tab of the Settings page appears.



Settings

NAME	ATTRIBUTE TYPE	DATA TYPE	
Auditor Status (Non suppressed)	Issue	Picklist (3)	EDIT
Auditor Status (Suppressed)	Issue	Picklist (2)	EDIT
Developer Status (Closed)	Issue	Picklist (3)	EDIT
Developer Status (Open)	Issue	Picklist (2)	EDIT
ImpactTest	Application	Picklist (12)	EDIT DELETE
Region	Application	Picklist (4)	EDIT DELETE

3. Click **Delete** in the row of the attribute that you want to edit.

   A confirmation message appears.

4. Click **Yes**.

   The attribute and all associated values are deleted.

Managing Fortify on Demand Connect Networks

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

> **Note:** Fortify on Demand Connect is available for preview in a sandbox environment. Contact support if you are interested in trying out Fortify on Demand Connect.

Adding a Fortify on Demand Connect Network

Security Leads can add Fortify on Demand Connect networks.

To add a Fortify on Demand Connect network:

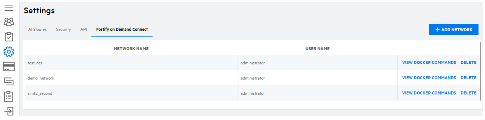
1. Select the **Administration** view.

   The User Settings page appears.

2. Click **Settings**.

   The **Attributes** tab of the Settings page appears.

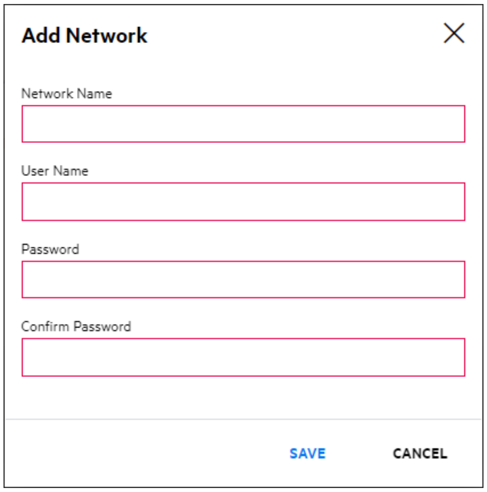
3. Select the **Fortify on Demand Connect** tab.



NETWORK NAME	USER NAME	
test_net	administrator	VIEW DOCKER COMMANDS DELETE
demo_network	administrator	VIEW DOCKER COMMANDS DELETE
simt2_second	administrator	VIEW DOCKER COMMANDS DELETE

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 Fortify on Demand Connect network username.
Password	Specify a Fortify on Demand Connect network password. Allowed characters are upper and lower case 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 is available that contains the code for the docker command to run the VPN client and initialize the connection between the VPN client and the VPN server.

Deleting a Fortify on Demand Connect Network

Security Leads can delete Fortify on Demand Connect networks.

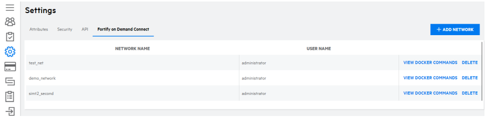
Note: Fortify on Demand Connect networks cannot be edited. If you need to update an existing network, you need to delete the network and add a new one.

To delete aFortify 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 **Fortify on Demand Connect** tab.

   Settings

NETWORK NAME	USER NAME	
test_net	administrator	VIEW DOCKER COMMANDS DELETE
demo_network	administrator	VIEW DOCKER COMMANDS DELETE
simt2_second	administrator	VIEW DOCKER COMMANDS DELETE

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.

Viewing Entitlements

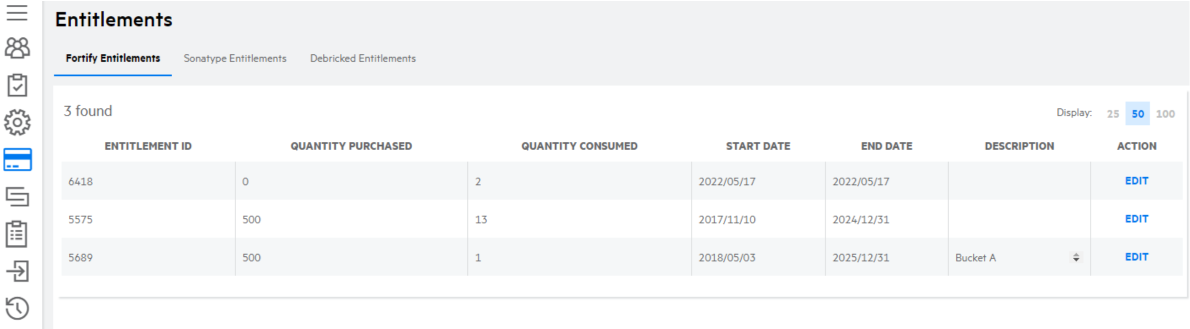
Security Leads can view a list of expired and active entitlements for the tenant as well as add descriptions to entitlements.

To view entitlements for the tenant:

1. Select the **Administration** view.

   The User Management page appears.
2. Click **Entitlements**.

   The Entitlement page appears. The **Fortify Entitlements** tab displays Fortify on Demand entitlements; the **Sonatype Entitlements** tab displays Sonatype entitlements; the **Debricked Entitlements** tab displays Debricked entitlements.

   Entitlements

   3 found

ENTITLEMENT ID	QUANTITY PURCHASED	QUANTITY CONSUMED	START DATE	END DATE	DESCRIPTION	ACTION
6418	0	2	2022/05/17	2022/05/17		EDIT
5575	500	13	2017/11/10	2024/12/31		EDIT
5689	500	1	2018/05/03	2025/12/31	Bucket A	EDIT

3. You can perform the following task:

Task	Procedure
Add or edit the entitlement description	Click **Edit** in the row of an entitlement and provide a description. The description is limited to 50 characters.

Viewing the Administration Event Log

Security Leads can view the administration event log. The administration event log logs all application-related events as well as the following administration-related events:

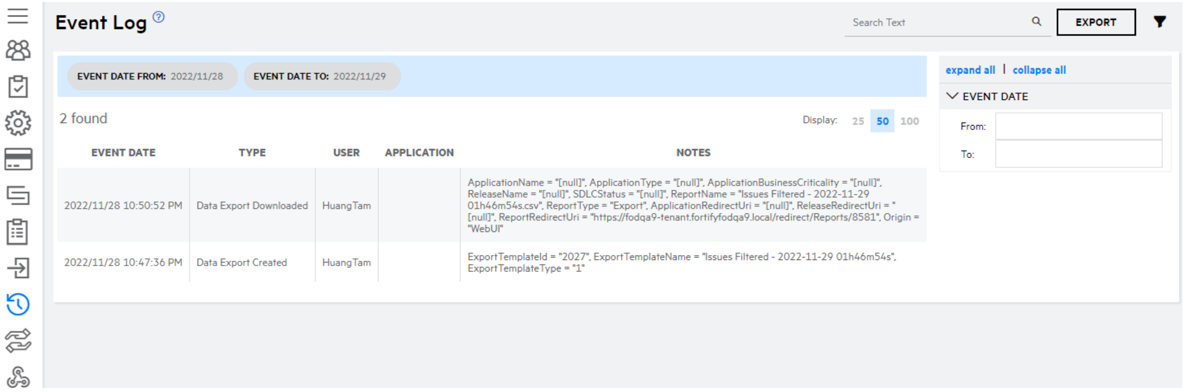
- user login success or failure and user logout
- user creation, updates, and deletion
- group creation, updates, and deletion
- role creation, updates, and deletion
- dashboard and event log exports
- API Key and personal access token creation, updates, deletion, and new secret generation
- API authentication success or failure
- Changes to administration settings and SSO settings

To view the administration event log:

1. Select the **Administration** view.

   The User Management page appears.
2. Click **Event Log**.

   The Event Log page appears.

   EVENT DATE FROM: 2022/11/28 EVENT DATE TO: 2022/11/29

   2 found

EVENT DATE	TYPE	USER	APPLICATION	NOTES
2022/11/28 10:50:52 PM	Data Export Downloaded	HuangTam		ApplicationName = "[null]", ApplicationType = "[null]", ApplicationBusinessCriticality = "[null]", ReleaseName = "[null]", SDLCStatus = "[null]", ReportName = "Issues Filtered - 2022-11-29 01h46m54s.csv", ReportType = "Export", ApplicationRedirectUri = "[null]", ReleaseRedirectUri = "[null]", ReportRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Reports/8581", Origin = "WebUI"
2022/11/28 10:47:36 PM	Data Export Created	HuangTam		ExportTemplateId = "2027", ExportTemplateName = "Issues Filtered - 2022-11-29 01h46m54s", ExportTemplateType = "1"

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**.

Task	Action
Hide or display the filter list	Click ▼.
Expand or collapse filters	Click expand all | collapse all or the arrow next to the 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.

Related Topics:

For information about viewing events related to a specific application, see "Viewing the Application Event Log" on page 55.

User Management

Security Leads and users with the Manage Users permissions can manage users in Fortify on Demand. Security Leads can perform all user administration tasks. Users with the Manage Users permissions can manage user accounts and groups, but cannot manage roles.

This section covers the following topics:

Roles and Permissions

User actions in Fortify on Demand are controlled by roles. Roles are collections of permissions that specify the actions that can be performed. Each user is assigned to a specific role. Security Leads can manage roles, including assigning users to roles and creating, editing, and deleting roles.

Fortify on Demand is deployed with six default roles. Organizations can also define custom roles to better serve their needs. Custom roles can be used to align user roles with existing roles in an organization or expand or limit user responsibilities. Small organizations might want roles with increased permissions; large or highly structure organizations might want roles with more restricted permissions.

This section covers the following topics:

Permissions

Permissions specify the actions a user can perform. Fortify on Demand permissions are divided into two types: tenant level permissions and application level permissions.

- **Tenant Level Permissions** are permissions that are applied at the tenant level, such as managing users, exporting data, and downloading tools. For a detailed list of tenant level permissions, see "Tenant Level Permissions" below.
- **Application Level Permissions** are permissions that are applied to applications, such as creating applications, starting scans, editing issues, and managing reports. For a detailed list of Application Level Permissions, see "Application Level Permissions" on page 273.

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 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**,	Determined by the application level permissions assigned to the role

Category	Permissions	Actions Allowed
	Export Data, **Vendor Management**, are set to **Deny**. - **All** - Access to all applications. No restrictions on tenant level permissions.	
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

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 • View Application Monitoring configuration and risk profile • 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 • Configure Application Monitoring and cancel Application Monitoring scan • 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

Category	Permissions	Actions Allowed
		- 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

Category	Permissions	Actions Allowed
		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
Consume Entitlements	**Deny**, **Allow**	Consume entitlements when starting a scan

Default Roles

Fortify on Demand is configured with six default roles. Default roles can be edited or deleted with the exception of the Security Lead and Developer roles.

- **Security Lead**—Full access. The Security Lead has access to all applications and can perform all tasks, including creating applications and releases, working with data, auditing issues, and managing reports. The Security Lead is the only role that has the Administration permission, which includes the ability to manage roles, security policies, and other administrative settings.
- **Developer**—Limited access. The Developer has access to applications assigned to the user. The Developer can work with issue data and manage reports. The Developer is the default role for new users.
- **Lead Developer**—Medium-level access. The Lead Developer can create new applications, but only has access to applications assigned to the user. The Lead Developer can work with issue data, start scans, and manage reports.
- **Application Lead**—Medium-level access. The Application Lead has the same access as the Lead Developer, plus the ability to audit issues.
- **Executive**—Read-only access. The Executive has read-only access to applications assigned to the user.
- **Reviewer**—Read-only access. The Reviewer has read-only access to all applications.

The following table lists the permission set for each default role.

Permission	Security Lead	Developer	Lead Developer (Editable)	Application Lead (Editable)	Executive (Editable)	Reviewer (Editable)
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

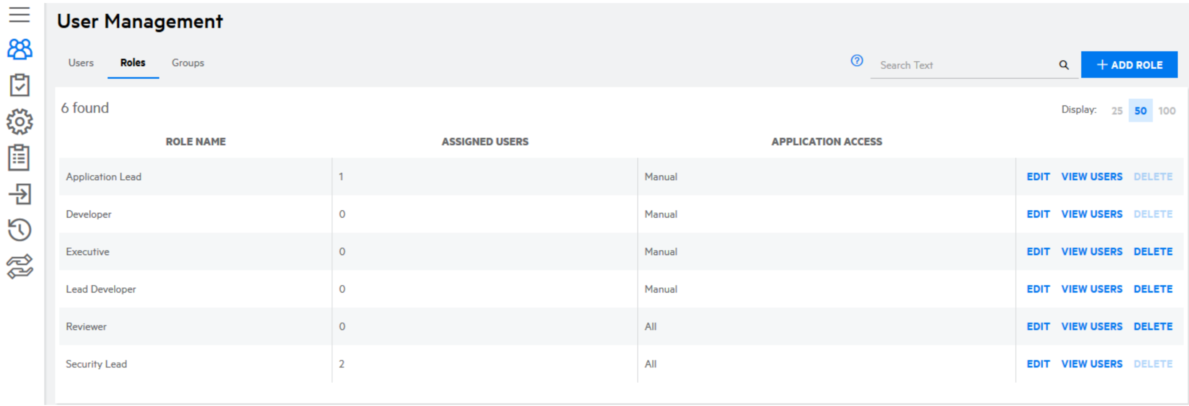
Permission	Security Lead	Developer	Lead Developer (Editable)	Application Lead (Editable)	Executive (Editable)	Reviewer (Editable)
Configure Build Server	X					
Consume Entitlements	X	X	X	X	X	X

Viewing Roles

To view the roles in your tenant:

1. Select the **Administration** view.

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



User Management

6 found

Display: 25 50 100

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	EDIT VIEW USERS DELETE
Developer	0	Manual	EDIT VIEW USERS DELETE
Executive	0	Manual	EDIT VIEW USERS DELETE
Lead Developer	0	Manual	EDIT VIEW USERS DELETE
Reviewer	0	All	EDIT VIEW USERS DELETE
Security Lead	2	All	EDIT VIEW USERS DELETE

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 more information, see "Creating a Role" on the next page.
View users assigned to a role	Click **View Users** in the action column.
Edit a role	Click **Edit** in the action column. For more information, see "Editing a Role" on page 279.

Task	Action
Delete a role	Click **Delete** in the action column. For more information, see "Deleting a Role" on page 280.

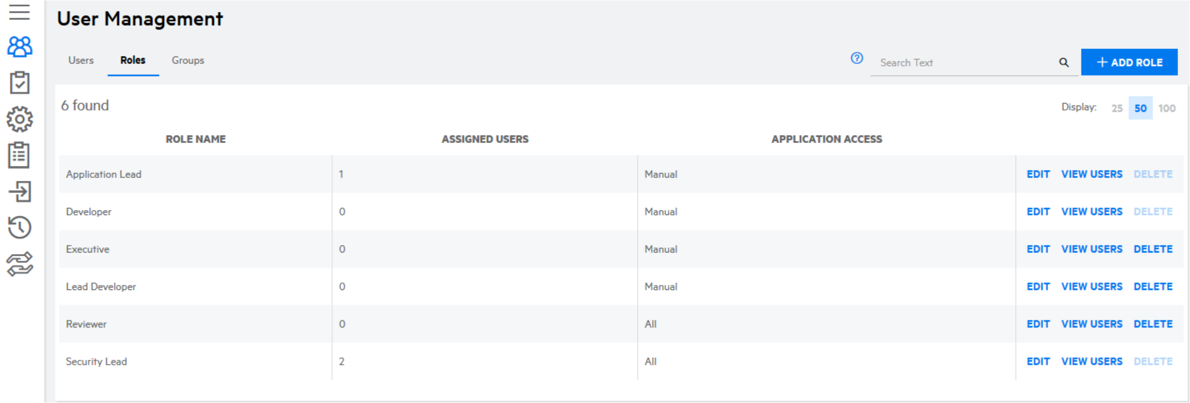
Creating a Role

To create a role:

1. Select the **Administration** view.

   The **User Management** page appears.

2. Select the **Roles** tab.



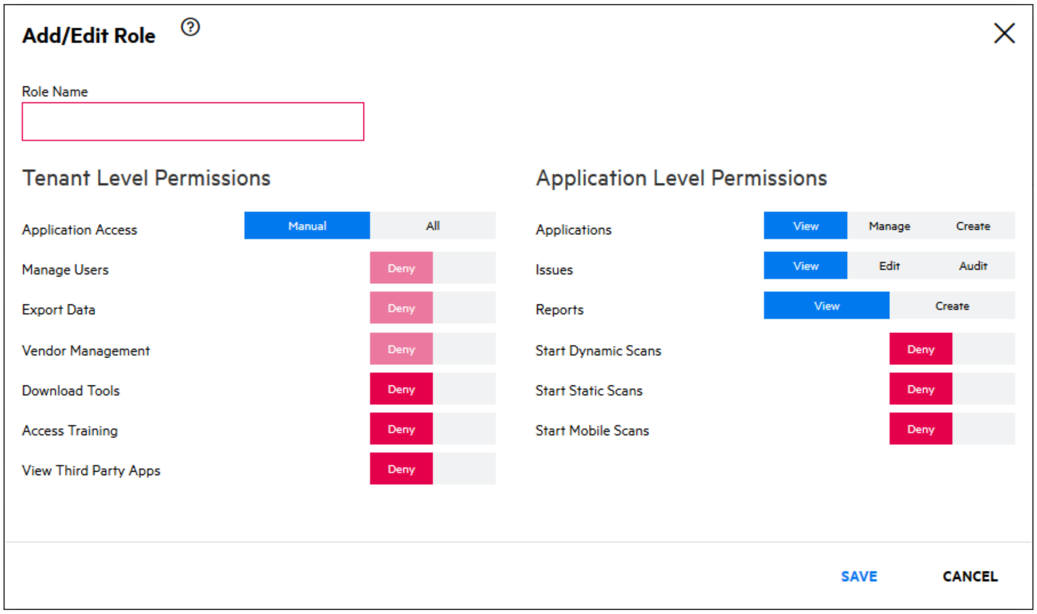
User Management

6 found

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	EDIT VIEW USERS DELETE
Developer	0	Manual	EDIT VIEW USERS DELETE
Executive	0	Manual	EDIT VIEW USERS DELETE
Lead Developer	0	Manual	EDIT VIEW USERS DELETE
Reviewer	0	All	EDIT VIEW USERS DELETE
Security Lead	2	All	EDIT VIEW USERS DELETE

3. Click **+ Add Role**.

   The Add/Edit Role window appears.



Add/Edit Role

Role Name

Tenant Level Permissions

Application Access	Manual / All
Manage Users	Deny
Export Data	Deny
Vendor Management	Deny
Download Tools	Deny
Access Training	Deny
View Third Party Apps	Deny

Application Level Permissions

Applications	View / Manage / Create
Issues	View / Edit / Audit
Reports	View / Create
Start Dynamic Scans	Deny
Start Static Scans	Deny
Start Mobile Scans	Deny

4. In the **Role Name** field, type the name of the new role.

5. Select tenant and application level permissions for the role. For more information on specific permissions, see "Permissions" on page 271.
6. Click **Save**.

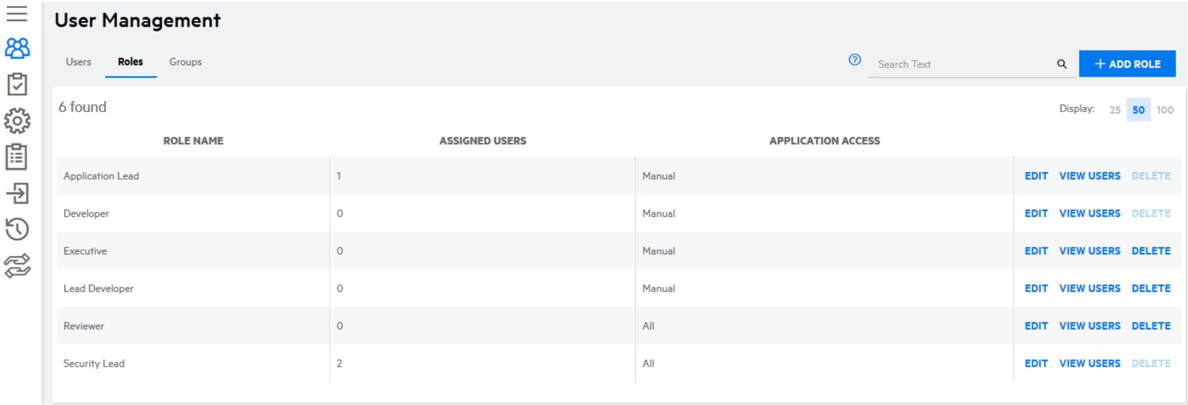
   The new role appears in the role list.

Editing a Role

To edit a role:

1. Select the **Administration** view.

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



User Management

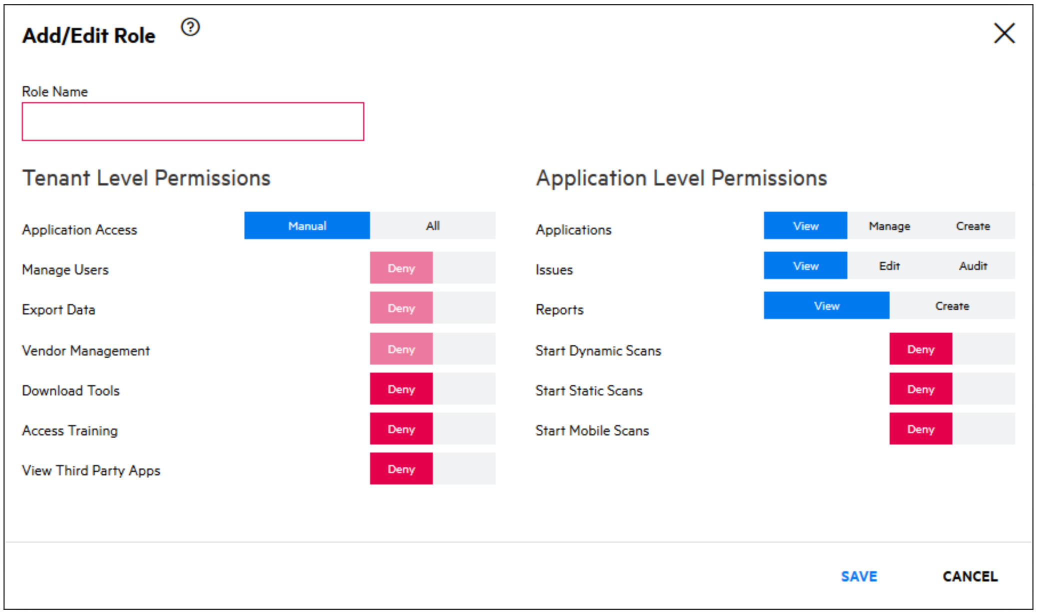
6 found

Display: 25 50 100

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	EDIT VIEW USERS DELETE
Developer	0	Manual	EDIT VIEW USERS DELETE
Executive	0	Manual	EDIT VIEW USERS DELETE
Lead Developer	0	Manual	EDIT VIEW USERS DELETE
Reviewer	0	All	EDIT VIEW USERS DELETE
Security Lead	2	All	EDIT VIEW USERS DELETE

3. Click **Edit** in the row of the role that you want to edit.

   The Add/Edit Role modal window appears.



Add/Edit Role

Role Name

Tenant Level Permissions

Application Access	Manual	All
Manage Users	Deny	
Export Data	Deny	
Vendor Management	Deny	
Download Tools	Deny	
Access Training	Deny	
View Third Party Apps	Deny	

Application Level Permissions

Applications	View	Manage	Create
Issues	View	Edit	Audit
Reports	View	Create	
Start Dynamic Scans	Deny		
Start Static Scans	Deny		
Start Mobile Scans	Deny		

Note: The permission sets of the Security Lead and Developer roles cannot be edited.

4. Edit the fields as needed.
5. Click **Save**

   The role changes are saved.

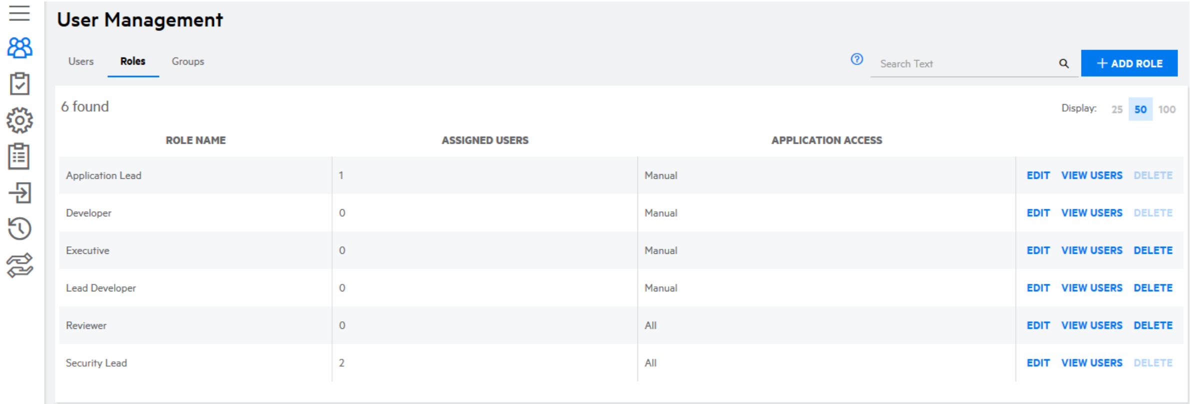
Deleting a Role

The Security Lead and Developer roles and roles to which users are assigned cannot be deleted.

To delete a role:

1. Select the **Administration** view.

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



6 found

ROLE NAME	ASSIGNED USERS	APPLICATION ACCESS	
Application Lead	1	Manual	EDIT VIEW USERS DELETE
Developer	0	Manual	EDIT VIEW USERS DELETE
Executive	0	Manual	EDIT VIEW USERS DELETE
Lead Developer	0	Manual	EDIT VIEW USERS DELETE
Reviewer	0	All	EDIT VIEW USERS DELETE
Security Lead	2	All	EDIT VIEW USERS DELETE

3. Click **Delete** in the row of the role that you want to delete.

   A confirmation message appears.
4. Click **Yes**.

   The role is deleted.

Users

Users with the Manage Users permissions can manage users and groups.

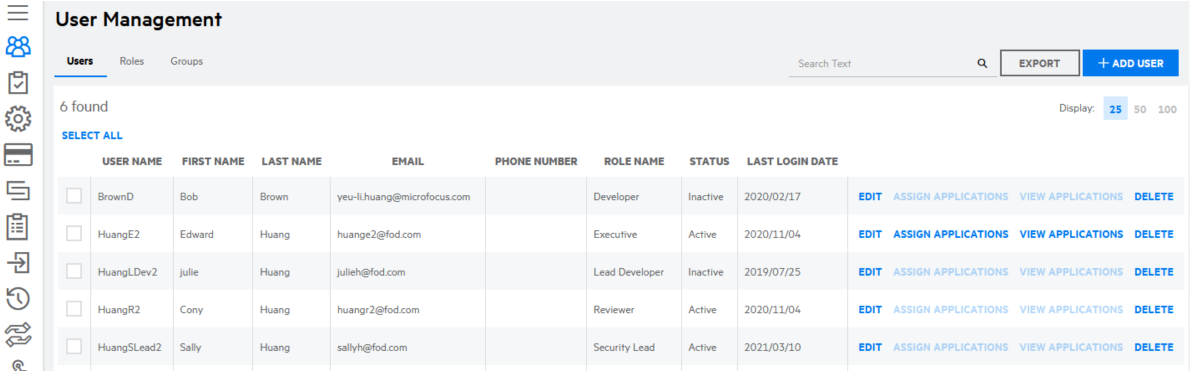
This section covers the following topics:

Viewing Users

To view the users in your tenant:

1. Select the **Administration** view.

   The **Users** tab of the User Management page appears.



	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE				
□	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE

The following table describes how to navigate the **Users** tab.

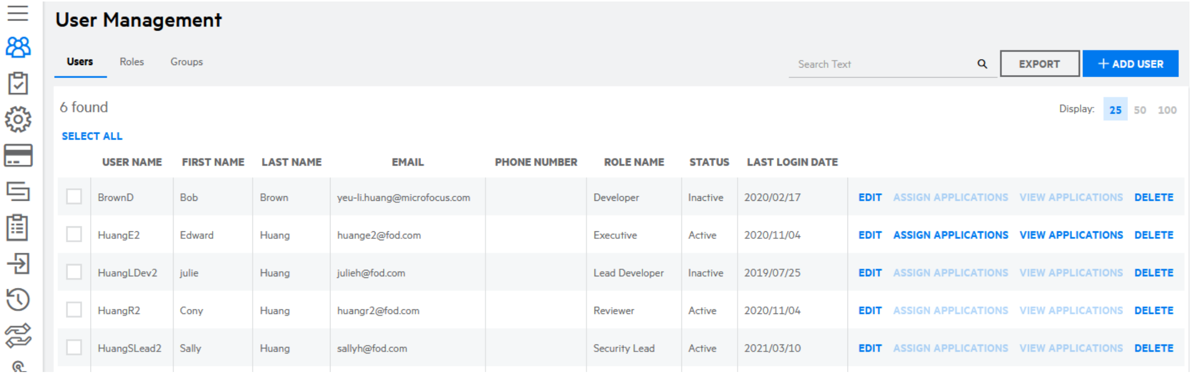
Task	Action
Search the user list	Type a word or phrase in the search field and press **Enter**. To remove the search results, remove the text from the search field and press **Enter**.
Export the user list.	Click **Export**. A CSV file containing details of all users is saved locally to a folder specified in your browser settings.
Add a user	Click **Add User**. For more information, see "Creating a User " below.
Assign and unassign applications	Click **Assign Applications** in the action column. For more information, see "Managing Application Assignment to a User" on page 284.
View applications assigned to a user	Click **View Applications** in the action column.
Edit a user	Click **Edit** in the action column. For more information, see "Editing a User Account" on page 283.
Delete a user	Click **Delete** in the action column. For more information, see "Deleting a User Account" on page 287.

Creating a User

To create a user:

1. Select the **Administration** view.

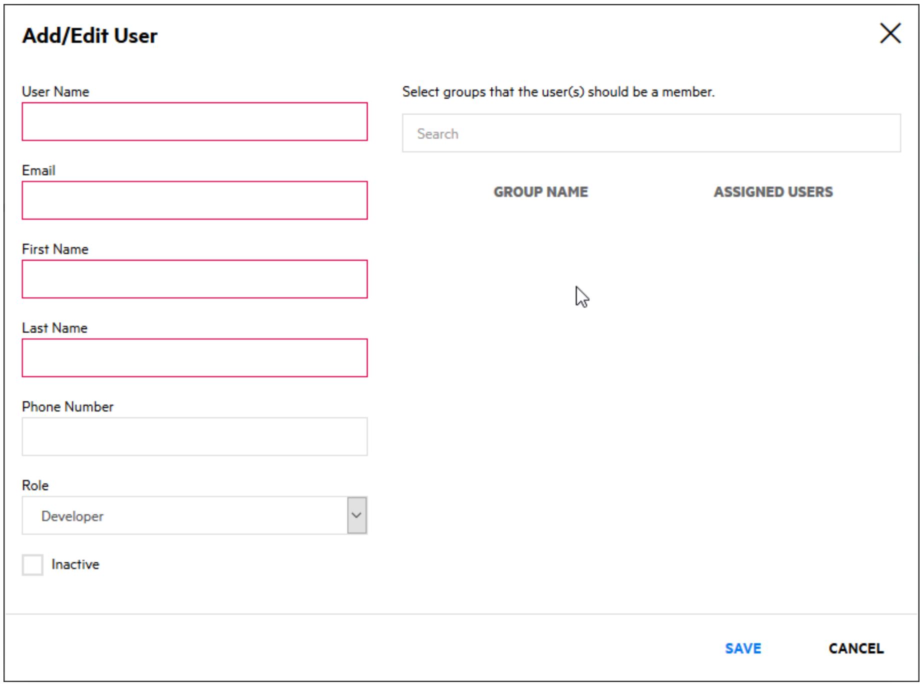
   The **Users** tab of the User Management page appears.



	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE				
□	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE

2. Click **+ Add User**.

   The Add/Edit User window appears.



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

Field	Description
User Name	Type a unique username. The username cannot be changed after the user is created.
Email	Type the user's email address.
First Name	Type the user's first name.

Field	Description
Last Name	Type the user's last name.
Phone Number	(Optional) Type the user's phone number. Hyphens and other separators are not accepted.
Role	Select the user role (default role is **Developer**). For more information on user roles, see Roles and Permissions.
Inactive	(Optional) Select the check box to mark the user as inactive. The user will be unable to log in to Fortify on Demand.

4. (Optional) Select the groups to which the user will be assigned. You can use the search box to filter the group list.
5. Click **Save**.

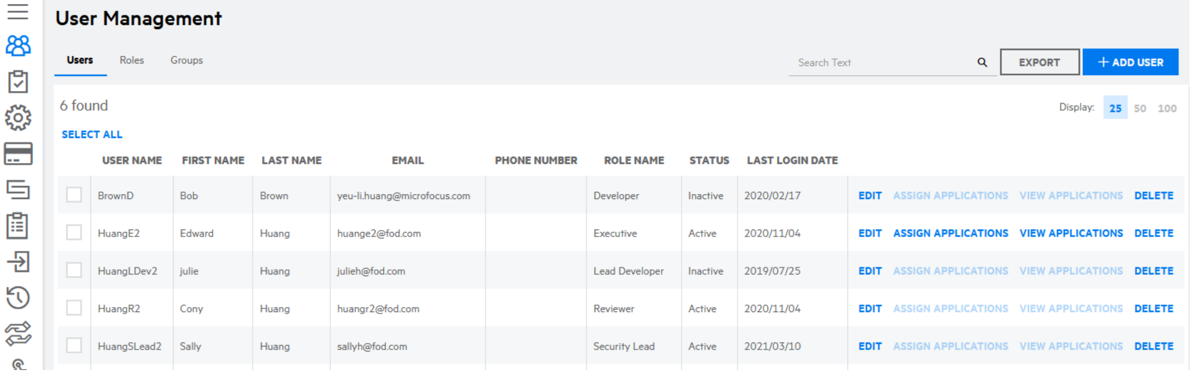
   The new user appears in the user list.

Editing a User Account

You can edit an existing user account, including resetting the user's password.

1. Select the **Administration** view.

   The **Users** tab of the User Management page appears.



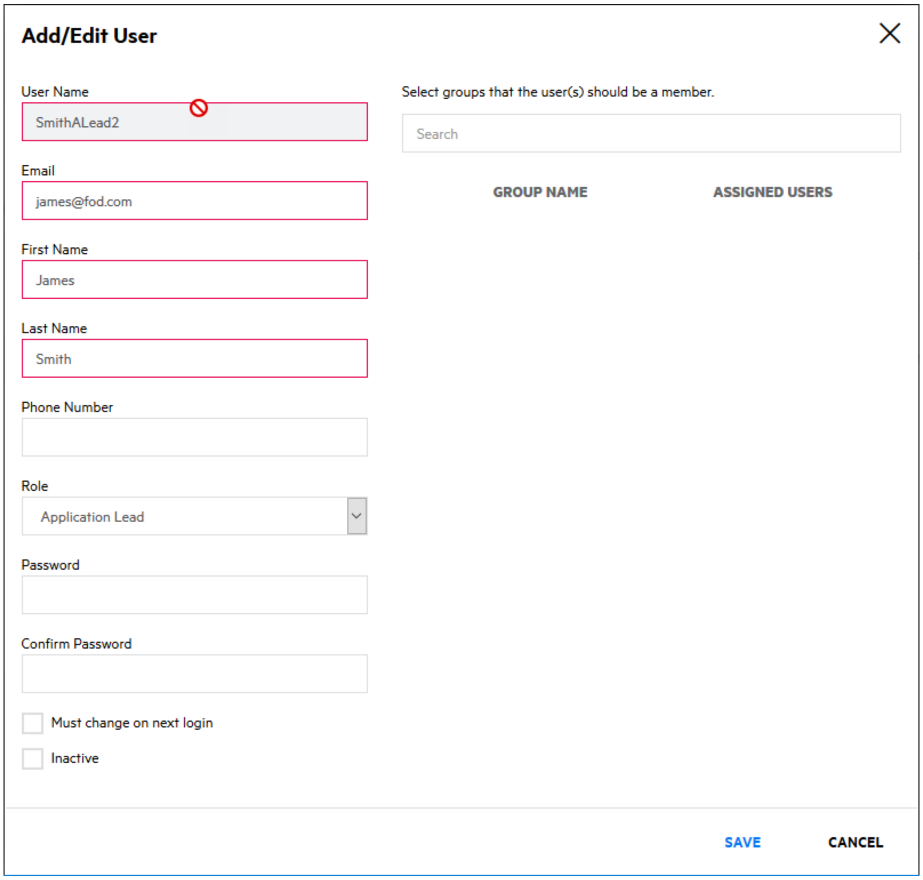
User Management

6 found

	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE				
□	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE

2. Click **Edit** in the row of the user whom you want to edit.

   The Add/Edit User window opens.



User Name: SmithALead2

Email: james@fod.com

First Name: James

Last Name: Smith

Phone Number:

Role: Application Lead

Password:

Confirm Password:

□ Must change on next login

□ Inactive

3. Edit the fields as needed. The following fields are used for resetting a user's password.
4.

Field	Description
Password	Type a new password for the user. The password needs to meet complexity requirements.
Confirm Password	Retype the same password.
Must change on next login	Select the check box to require the user to change the password the next time the user logs in.

5. Click **Save**.

   The user changes are saved.

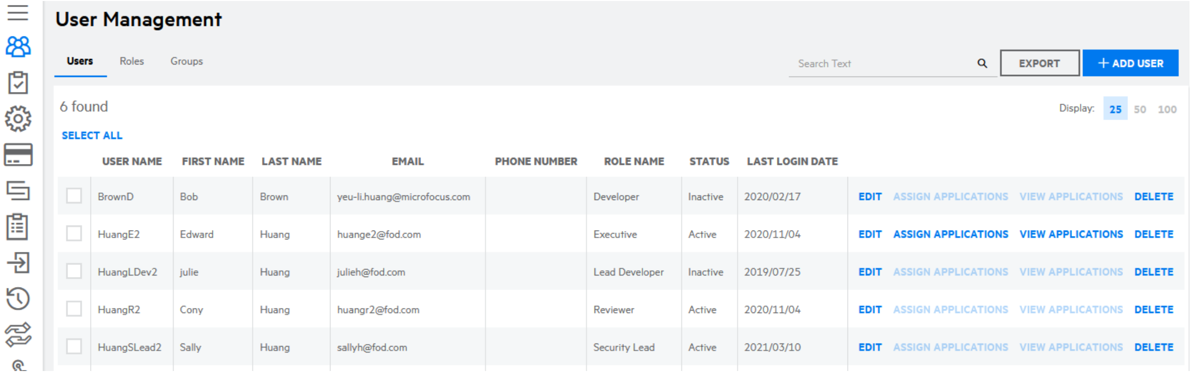
Managing Application Assignment to a User

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

To manage application access to a user:

1. Select the **Administration** view.

   The **User** tab of the User Management page appears.



User Management

6 found

Display: 25 50 100

SELECT ALL

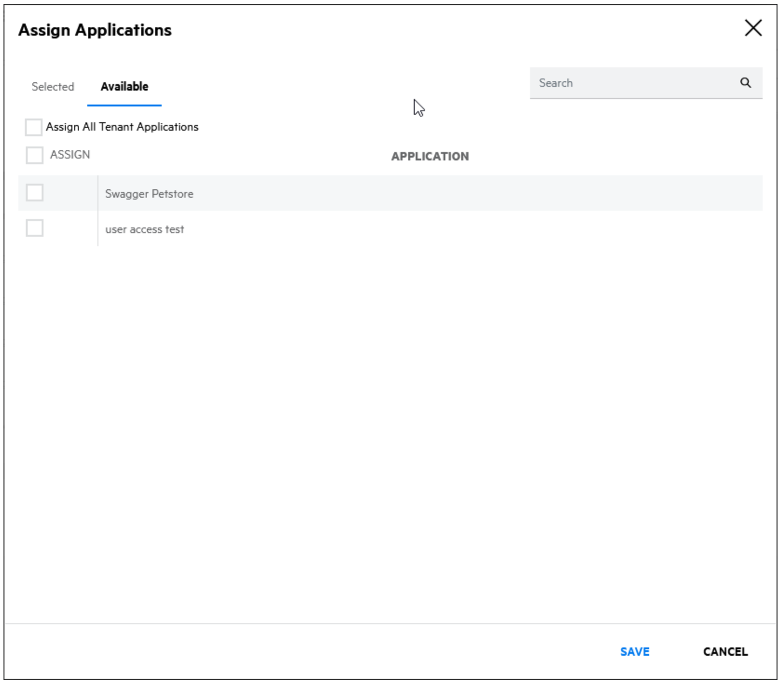
	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
□	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

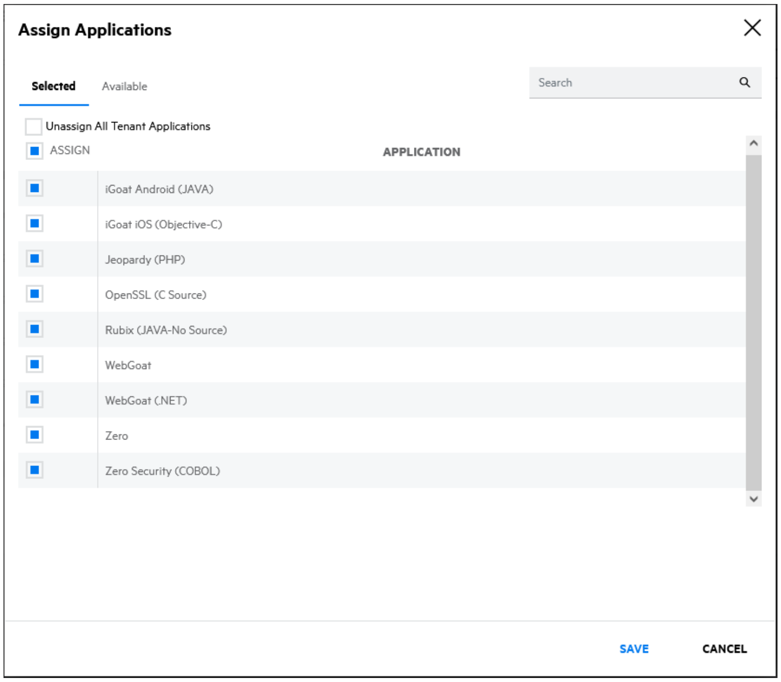
2. Click **Assign Applications** in the row of the user for whom you want to edit application access.

   The Assign Application window appears.

> **Note:** The link is unavailable if a user is assigned to a role with the **All Application Access** permission.

3. You can perform the following tasks:

Task	**Procedure**
Assign applications to user	a. Select the **Available** tab.  Assign Applications Selected Available Search □ Assign All Tenant Applications □ ASSIGN APPLICATION □ Swagger Petstore □ user access test SAVE CANCEL b. Perform the following actions to select applications:

Task	Procedure
	○ 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. You can use the search field to filter the application list.
Remove applications from user	a. Click **Assign Applications**. b. Select the **Selected** tab.  Assign Applications Selected Available Search ☐ Unassign All Tenant Applications ☑ ASSIGN APPLICATION ☑ iGoat Android (JAVA) ☑ iGoat iOS (Objective-C) ☑ Jeopardy (PHP) ☑ OpenSSL (C Source) ☑ Rubix (JAVA-No Source) ☑ WebGoat ☑ WebGoat (.NET) ☑ Zero ☑ Zero Security (COBOL) SAVE CANCEL c. 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. You can use the search field to filter the application list.

4. Click **Save**.

   The changes to the user's assigned applications are saved.

Related Topics

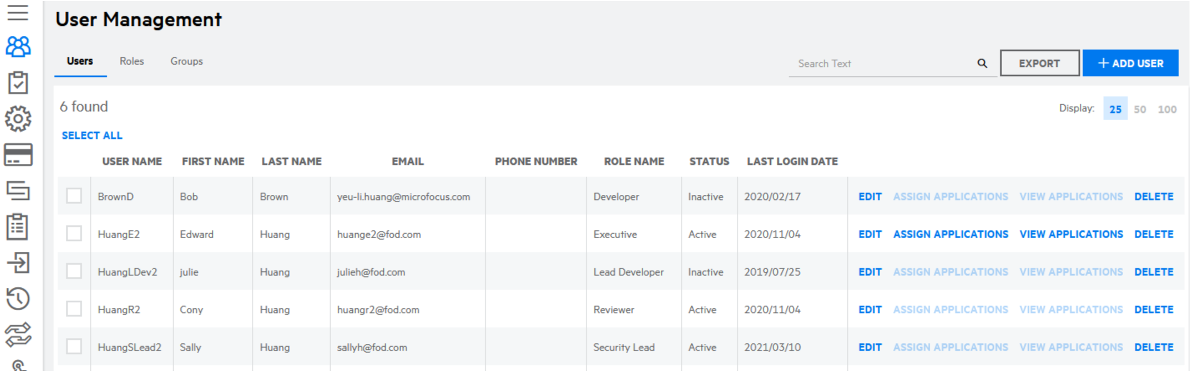
To manage user access to applications at the application level, see "Managing User Assignment to an Application" on page 53.

Deleting a User Account

To delete a user account:

1. Select the **Administration** view.

   The **Users** tab of the User Management page appears.



User Management

6 found

	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE				
□	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE

2. Click **Delete** in the row of the user whom you want to delete.

   A confirmation message appears.

3. Click **Yes**.

   The user is deleted.

> **Note:** When a user is deleted, occurrences of the user name, full name, email, and phone number are removed except when necessary for referential integrity and replaced with an unique user ID.

Groups

Users can be sorted into groups to which applications can be assigned. This allow streamlining of application assignment. Groups can be designed around business groups, regions, or other organizational structure.

This section covers the following topics:

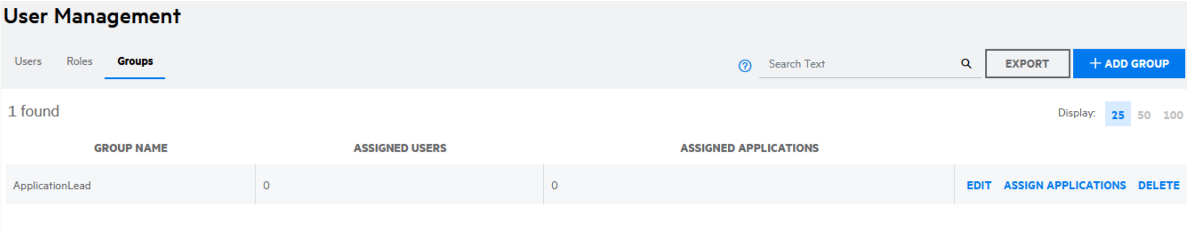
Viewing Groups

To view the groups in your tenant:

1. Select the **Administration** view.

   The User Management page appears.

2. Select the **Groups** tab.



User Management

1 found

GROUP NAME	ASSIGNED USERS	ASSIGNED APPLICATIONS
ApplicationLead	0	0

The following table describes how to navigate the **Groups** tab.

Task	Action
Search the group list	Type a keyword or phrase in the search field and press **Enter**. To remove the search results, remove the text from the search field and press **Enter**.
Export data as a .csv file	Click **Export**. A .csv file containing user group details is saved locally to a folder specified in your browser settings.
Add a group	Click **Add Group**. For more information, see "Creating a Group" below.
Edit a group name and assigned users	Click **Edit** in the action column. For more information, see "Editing a Group" on the next page.
Assign and unassign applications	Click **Assign Applications** in the action column. For more information, see "Managing Application Assignment for a Group" on page 291.
Delete a group	Click **Delete** in the action column. For more information, see "Deleting a Group" on page 293.

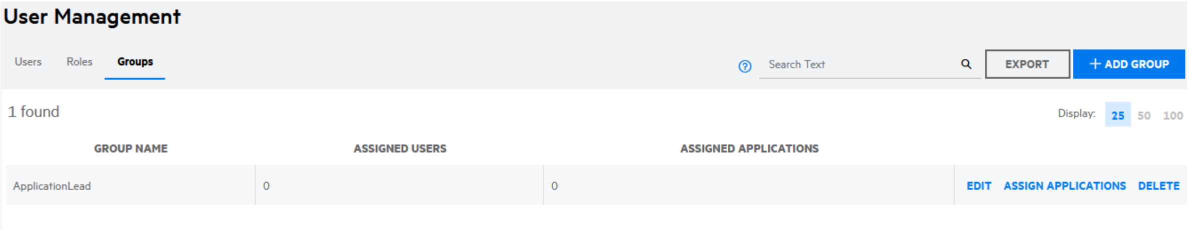
Creating a Group

To create a group

1. Select the **Administration** view.

   The User Management page appears.

2. Select the **Groups** tab.

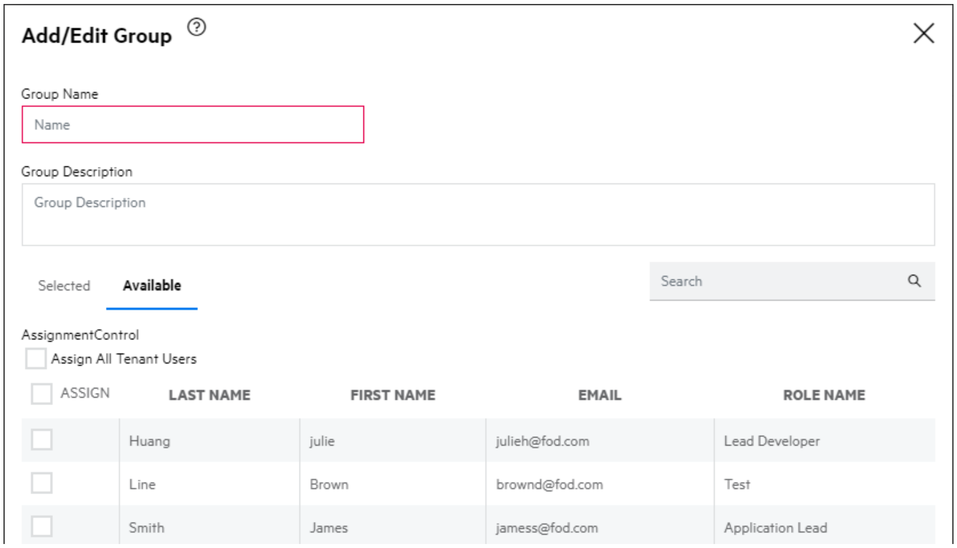


1 found

GROUP NAME	ASSIGNED USERS	ASSIGNED APPLICATIONS
ApplicationLead	0	0

3. Click **+Add Group**.

   The Add/Edit Group window appears.



□ ASSIGN	LAST NAME	FIRST NAME	EMAIL	ROLE NAME
□	Huang	julie	julieh@fod.com	Lead Developer
□	Line	Brown	brownd@fod.com	Test
□	Smith	James	jamess@fod.com	Application Lead

4. In the **Group Name** field, specify the name of the group.
5. (Optional) In the **Group Description** field, specify a description of the group.
6. You can perform the following actions to select applications:

   - Select the check box next to individual users.
   - Select the **ASSIGN** check box to select displayed users.
   - Select the **Assign All Tenant Applications** check box to select all users.

7. Click **Save**.

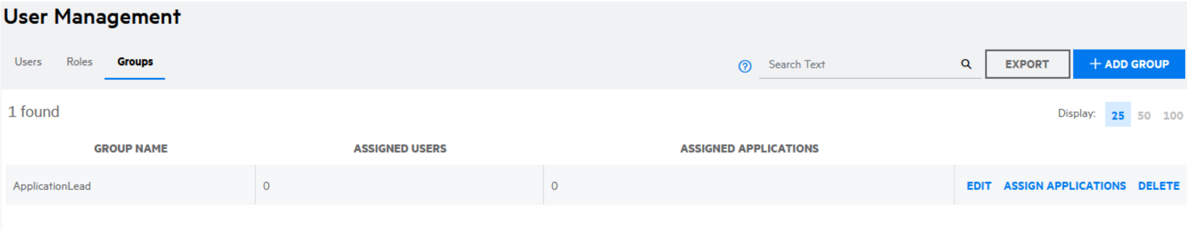
   The new group appears in the group list.

Editing a Group

To edit a group name as well as manage user assignment for a group:

1. Select the **Administration** view.

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



User Management

1 found

Display: 25 50 100

GROUP NAME	ASSIGNED USERS	ASSIGNED APPLICATIONS	
ApplicationLead	0	0	EDIT ASSIGN APPLICATIONS DELETE

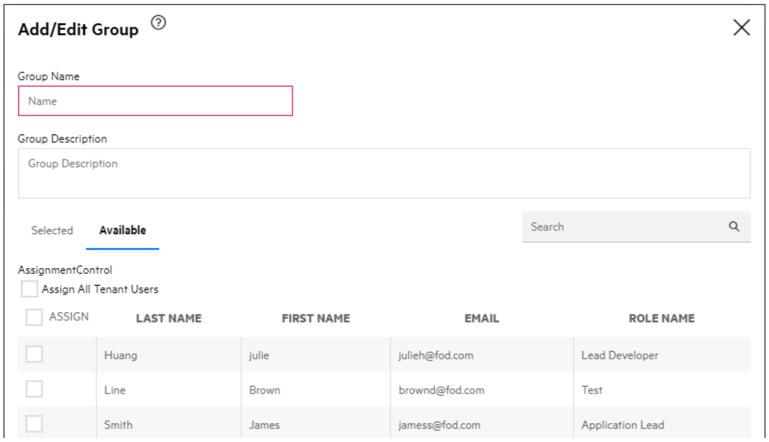
3. Click **Edit** in the row of the group that you want to edit.

   The Add/Edit Group window opens

4. You can perform the following tasks:

<table>
<tr><th>Task</th><th>Procedure</th></tr>
<tr><td>Edit the group name</td><td>In the <b>Group Name</b> field, type the new name of the group.</td></tr>
<tr><td>Assign users to group</td><td>

a. Select the **Available** tab.



Add/Edit Group

Group Name: Name

Group Description: Group Description

AssignmentControl

□ Assign All Tenant Users

□ ASSIGN	LAST NAME	FIRST NAME	EMAIL	ROLE NAME
□	Huang	julie	julieh@fod.com	Lead Developer
□	Line	Brown	brownd@fod.com	Test
□	Smith	James	jamess@fod.com	Application Lead

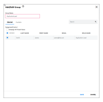
b. Perform the following actions to select applications:

- Select the check box next to individual users.
- Select the **ASSIGN** check box to select displayed users.
- Select the **Assign All Tenant Users** check box to select all users.

You can use the search field to filter the user list.

</td></tr>
<tr><td>Unassign users from group</td><td>

a. Select the **Selected** tab.



b. Perform the following actions to remove users:

- Clear the check box next to individual users.

</td></tr>
</table>

Task	Procedure
	○ 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 user list.

5. Click **Save**.

   Your group changes are saved.

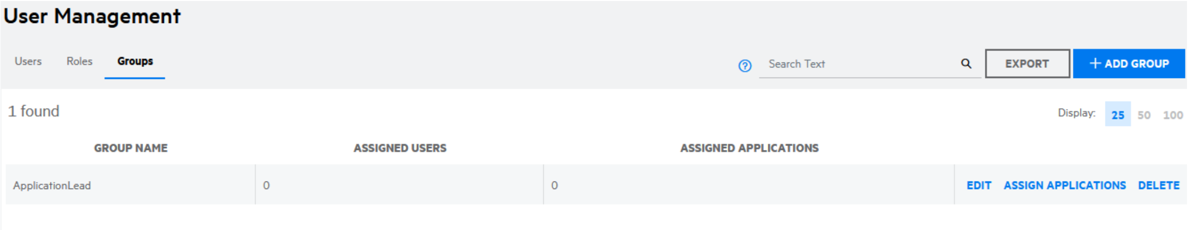
Managing Application Assignment for a Group

Users with the **Manage Users** permission can manage application assignment for a group from the Administration view.

To manage application assignment for a group:

1. Select the **Administration** view.

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



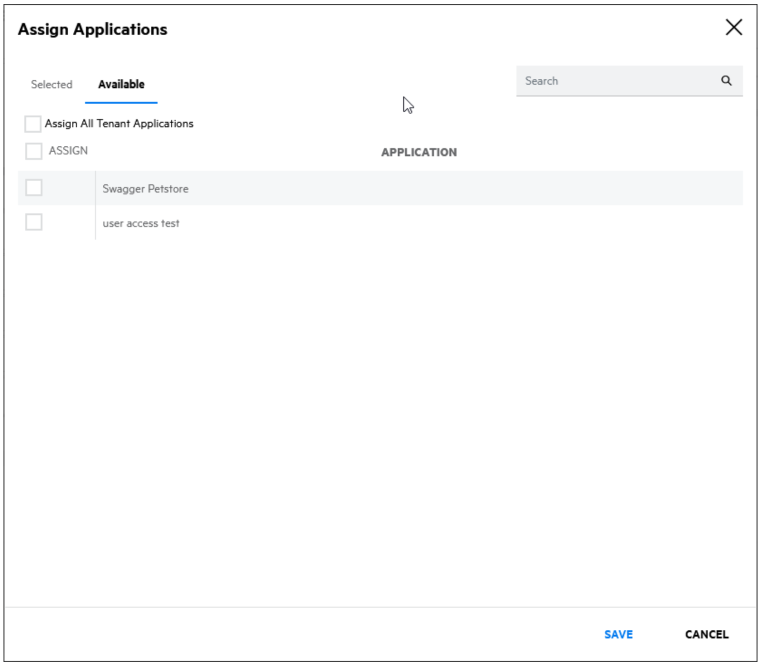
1 found

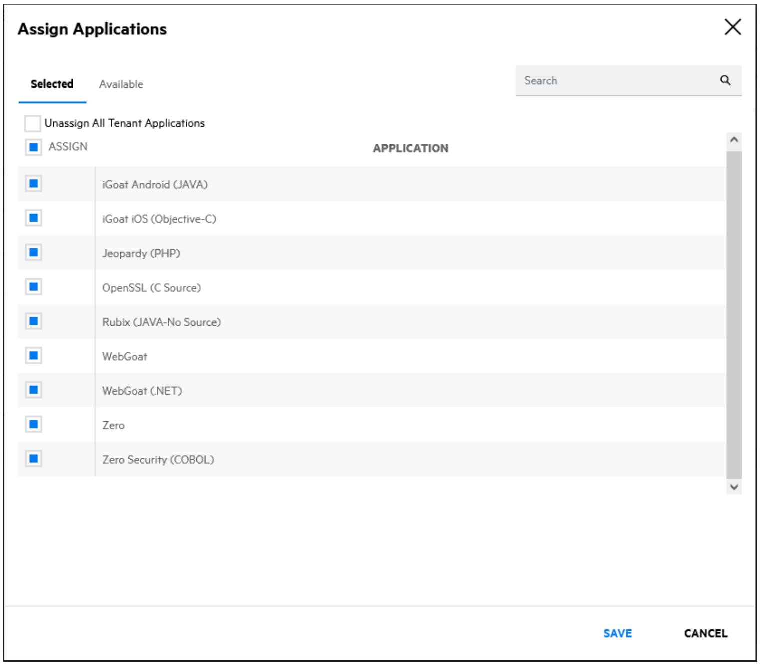
GROUP NAME	ASSIGNED USERS	ASSIGNED APPLICATIONS	
ApplicationLead	0	0	EDIT ASSIGN APPLICATIONS DELETE

3. Click **Assign Applications** in the row of the group to which you want to assign applications.

   The Assign Applications window opens.
4. You can perform the following tasks:

Task	Procedure
Assign applications to group	a. Click **Assign Applications**. b. Select the **Available** tab.

Task	Procedure
	 Assign Applications Selected Available Search □ Assign All Tenant Applications □ ASSIGN APPLICATION □ Swagger Petstore □ user access test SAVE CANCEL c. 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. You can use the search field to filter the application list. d. Click **Save**.
Unassign applications from group	a. Click **Assign Applications**. b. Select the **Selected** tab.

<table>
<tr><th>Task</th><th>Procedure</th></tr>
<tr><td></td><td>


□ Unassign All Tenant Applications

ASSIGN	APPLICATION
■	iGoat Android (JAVA)
■	iGoat iOS (Objective-C)
■	Jeopardy (PHP)
■	OpenSSL (C Source)
■	Rubix (JAVA-No Source)
■	WebGoat
■	WebGoat (.NET)
■	Zero
■	Zero Security (COBOL)

c. 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.

You can use the search field to filter the application list.

d. Click **Save**.
</td></tr>
</table>

5. Click **Save**.

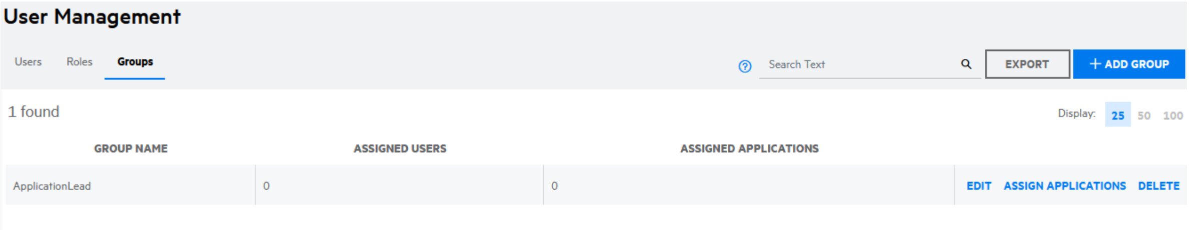
   The changes to the group's assigned applications are saved.

Deleting a Group

To delete a group:

1. Select the **Administration** view.

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



1 found

GROUP NAME	ASSIGNED USERS	ASSIGNED APPLICATIONS	
ApplicationLead	0	0	EDIT ASSIGN APPLICATIONS DELETE

3. Click **Delete** in the row of the group that you want to delete.

   A confirmation message appears.

4. Click **Yes**.

   The group is deleted.

Policy Management

Security Leads can configure how security policies are applied to applications in a tenant. They can also create and manage custom security policies.

This section covers the following topics:

Creating a Security Policy

To create a custom security policy:

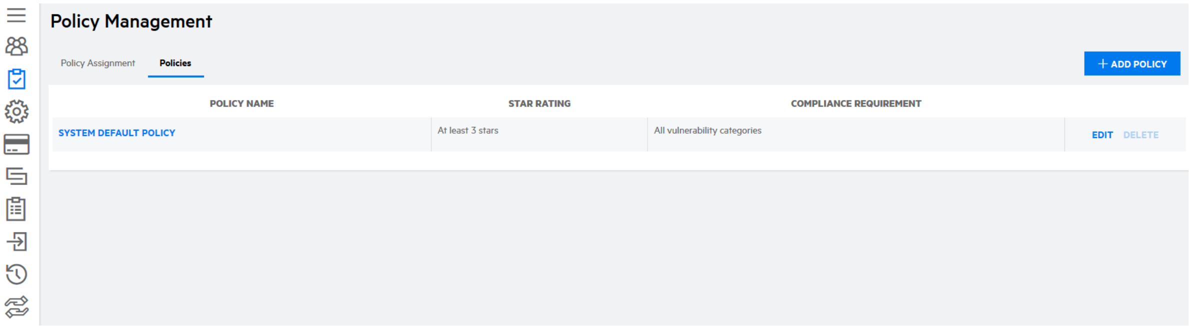
1. Select the **Administration** view.

   The User Management page appears.

2. Click **Policy Management**.

   The **Scope** tab of the Policy Management page appears.

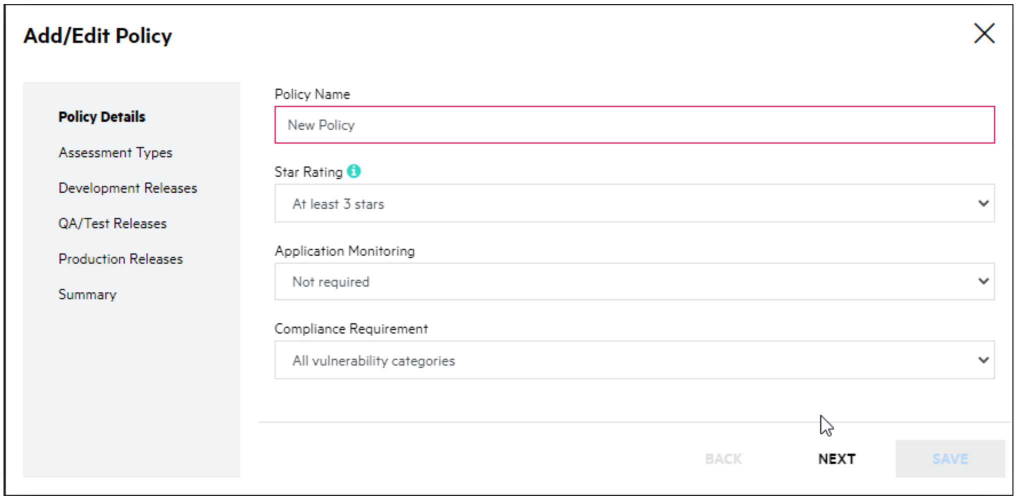
3. Select the **Policies** tab.



POLICY NAME	STAR RATING	COMPLIANCE REQUIREMENT	
SYSTEM DEFAULT POLICY	At least 3 stars	All vulnerability categories	EDIT DELETE

4. Click **+Add Policy**.

The **Add/Edit Policy** wizard appears.



Add/Edit Policy

Policy Name: New Policy

Star Rating: At least 3 stars

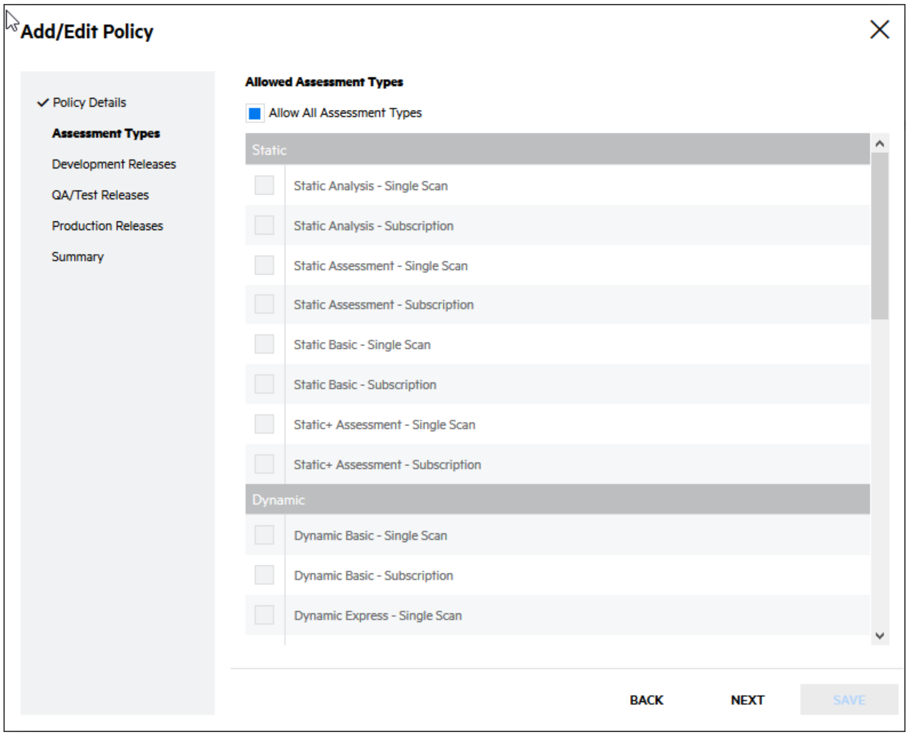
Application Monitoring: Not required

Compliance Requirement: All vulnerability categories

5. On the Policy Details page, complete the following fields:

Field	Description
Policy Name	Type a name for the policy.
Star Rating	Select the minimum star rating an application must be awarded to be determined as passing.
Application Monitoring	Select whether Application Monitoring is required or not. If it is required, then a production release will fail if Application Monitoring is not enabled for the application.
Compliance Requirement	Select which vulnerabilities are included when determining the pass/ fail status of an application. You can retain the default value of all vulnerabilities or only include issues tagged with a specific compliance requirement, such as OWASP 2021 or PCI 3.2. **Note:** The pass/fail status incorporates Application Monitoring and open source issues.

6. Click **Next**.
7. On the Assessment Types page, select which assessment types are available to applications that have the policy applied.



Allowed Assessment Types

☑ Allow All Assessment Types

Static

- □ Static Analysis - Single Scan
- □ Static Analysis - Subscription
- □ Static Assessment - Single Scan
- □ Static Assessment - Subscription
- □ Static Basic - Single Scan
- □ Static Basic - Subscription
- □ Static+ Assessment - Single Scan
- □ Static+ Assessment - Subscription

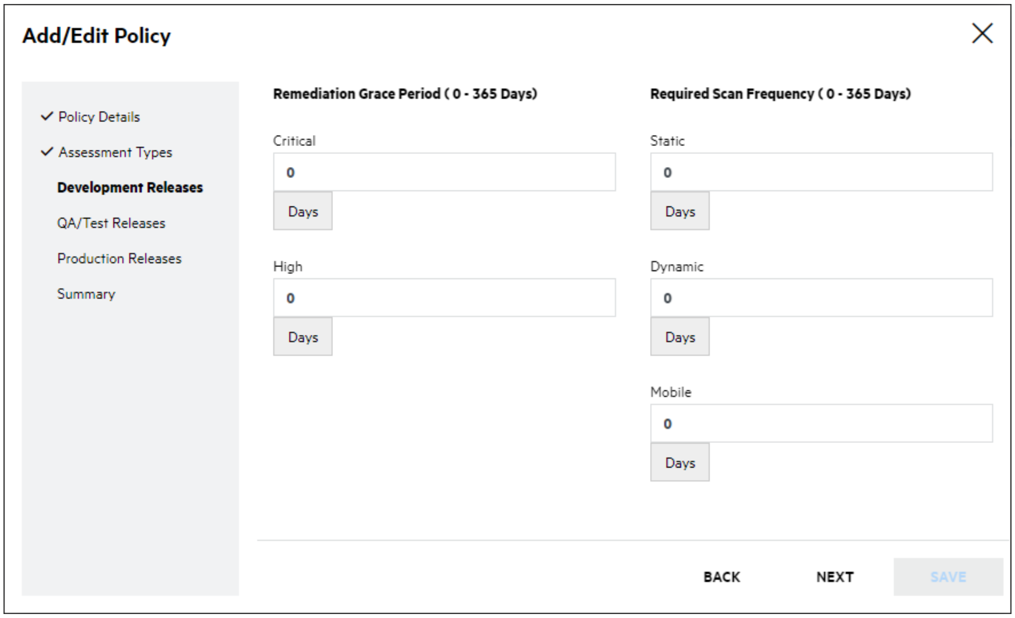
Dynamic

- □ Dynamic Basic - Single Scan
- □ Dynamic Basic - Subscription
- □ Dynamic Express - Single Scan

- **Allow All Assessment Types** is selected by default. Leave it selected to have the security policy allow all assessment types, including ones added after the policy has been created.
- Deselect **Allow All Assessment Types** to individually select assessment types.

> **Note:** If an application undergoes a policy update and has an active subscription or available remediation for an assessment type that is not allowed by the current policy, the subscription or remediation will still be available until it expires or is used.

8. Click **Next**.
9. On the Development Releases page, complete the fields that apply to Development status releases:



Add/Edit Policy

Remediation Grace Period (0 - 365 Days)

Critical: 0 Days

High: 0 Days

Required Scan Frequency (0 - 365 Days)

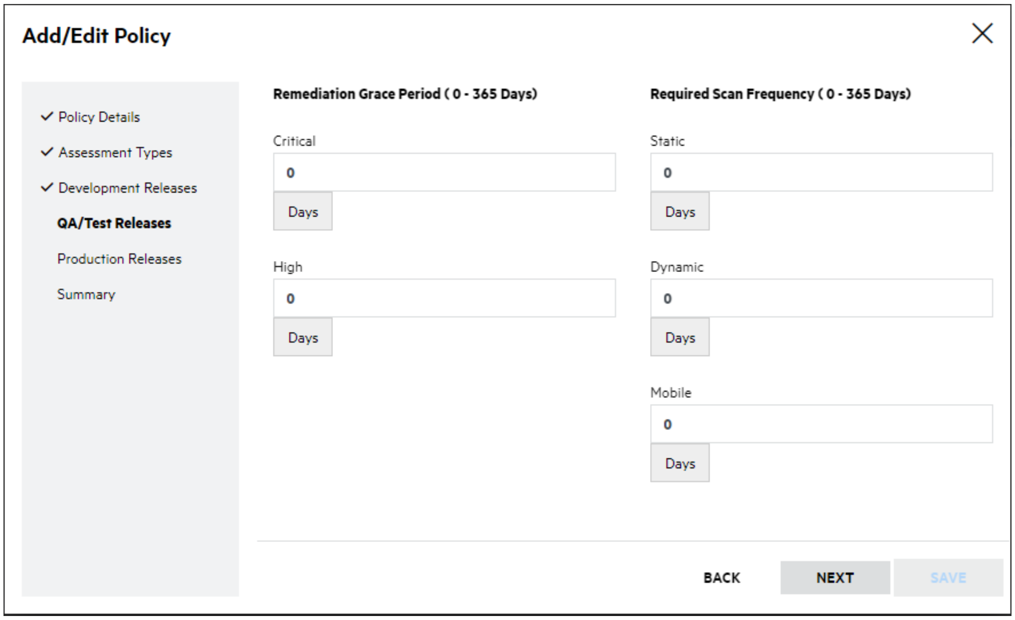
Static: 0 Days

Dynamic: 0 Days

Mobile: 0 Days

Field	Description
Remediation Grace Period (0 - 365 Days)	Specify the issue remediation grace period for each issue severity level. When an issue found in a Development release is within its grace period, it will not affect the pass/ fail status of the release. **Note:** The star rating specified above determines the issue severity levels displayed.
Required Scan Frequency (0 - 365 Days)	Specify the required scan frequency of each scan type. If a Development release has not completed a scan within the designated period of the scan type, it will fail. The value of 0 means no scan is required.

10. Click **Next**.
11. On the QA/Test Releases page, complete the fields that apply to QA/Test status releases:



Remediation Grace Period (0 - 365 Days)

Critical: 0 Days

High: 0 Days

Required Scan Frequency (0 - 365 Days)

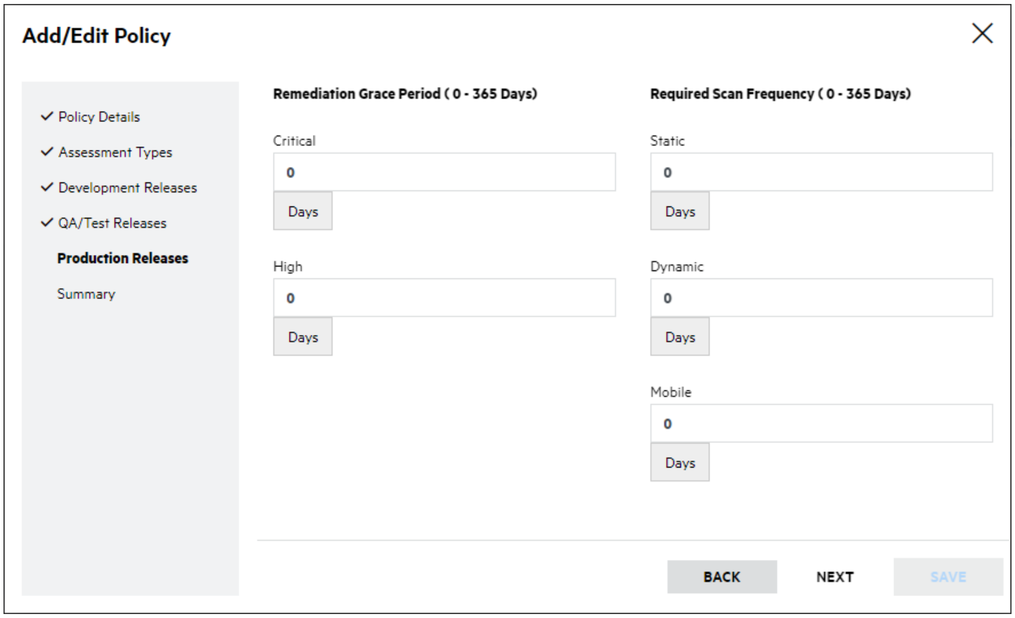
Static: 0 Days

Dynamic: 0 Days

Mobile: 0 Days

Field	Description
Remediation Grace Period (0 - 365 Days)	Specify the issue remediation grace period for each issue severity level. When an issue found in a QA/Test release is within its grace period, it will not affect the pass/ fail status of the release. **Note:** The star rating specified above determines the issue severity levels displayed.
Required Scan Frequency (0 - 365 Days)	Specify the required scan frequency of each scan type. If a QA/Test release has not completed a scan within the designated period of the scan type, it will fail. The value of 0 means no scan is required.

12. Click **Next**.
13. On the Production Releases page, complete the fields that apply to Production status releases:



Add/Edit Policy

✓ Policy Details
✓ Assessment Types
✓ Development Releases
✓ QA/Test Releases
Production Releases
Summary

Remediation Grace Period (0 - 365 Days)

Critical: 0 Days

High: 0 Days

Required Scan Frequency (0 - 365 Days)

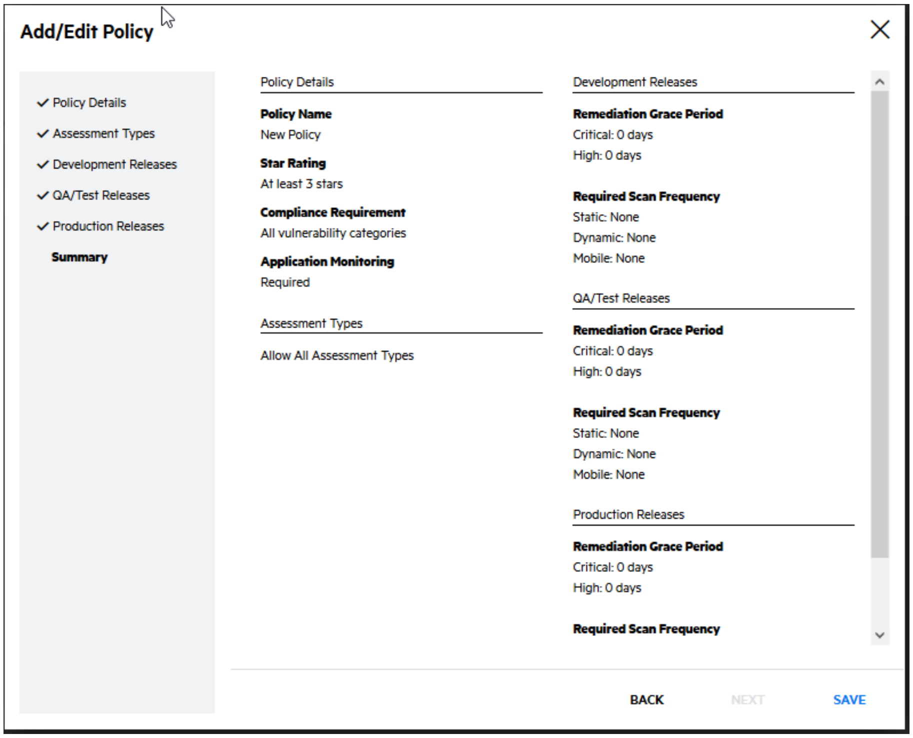
Static: 0 Days

Dynamic: 0 Days

Mobile: 0 Days

Field	Description
Remediation Grace Period (0 - 365 Days)	Specify the issue remediation grace period for each issue severity level. When an issue found in a Production release is within its grace period, it will not affect the pass/ fail status of the release. **Note:** The star rating specified above determines the issue severity levels displayed.
Required Scan Frequency (0 - 365 Days)	Specify the required scan frequency of each scan type. If a Production release has not completed a scan within the designated period of the scan type, it will fail. The value of 0 means no scan is required.

14. Click **Next**.
15. On the Summary page, review the policy settings.



Policy Details

Policy Name
New Policy

Star Rating
At least 3 stars

Compliance Requirement
All vulnerability categories

Application Monitoring
Required

Assessment Types

Allow All Assessment Types

Development Releases

Remediation Grace Period
Critical: 0 days
High: 0 days

Required Scan Frequency
Static: None
Dynamic: None
Mobile: None

QA/Test Releases

Remediation Grace Period
Critical: 0 days
High: 0 days

Required Scan Frequency
Static: None
Dynamic: None
Mobile: None

Production Releases

Remediation Grace Period
Critical: 0 days
High: 0 days

Required Scan Frequency

16. Click **Save**.

    The new policy appears in the **Policies** tab.

Related Topics:

- For information on Star Ratings, see "Five-Star Assessment Rating" on page 20.
- For Information on manually overriding the Pass/Fail settings, see "Overriding the Security Policy of a Release" on page 66.

Setting the Security Policy

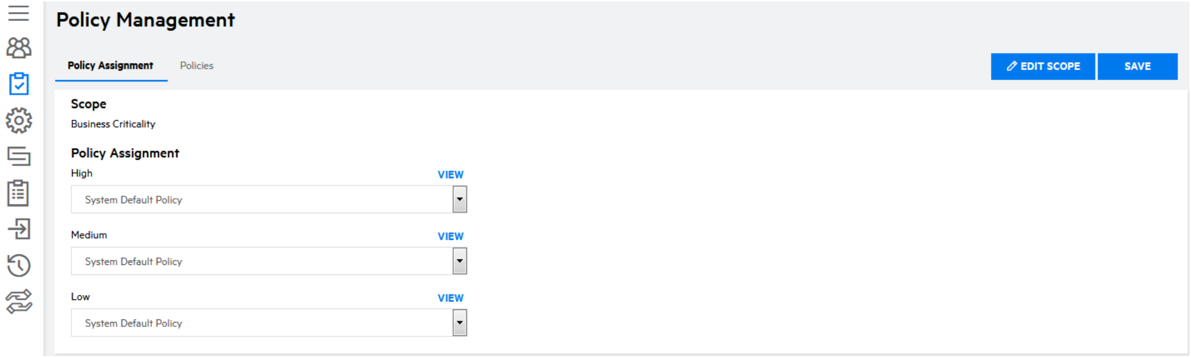
To set the security policy for your tenant:

1. Select the **Administration** view.

   The **User Management** page appears.

2. Click **Policy Management**.

   The **Policy Assignment** tab of the **Policy Management** page appears.



Policy Management

Policy Assignment | Policies

Scope
Business Criticality

Policy Assignment

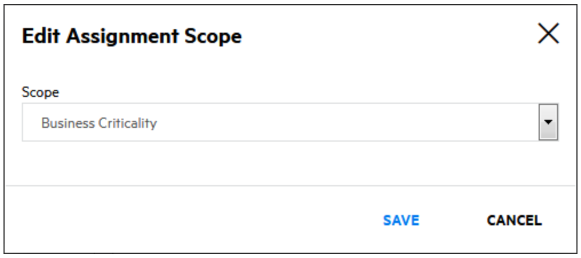
High: System Default Policy (VIEW)

Medium: System Default Policy (VIEW)

Low: System Default Policy (VIEW)

3. Click **Edit**.

   The **Edit Assignment Scope** modal window opens.



Edit Assignment Scope

Scope: Business Criticality

4. Select the scope for determining how polices are applied from the **Scope** list. Only one scope can be applied per tenant. The available values are:

   - **Business Criticality**: groups applications according to their assigned Business Criticality level. For more information on Business Criticality levels, see "Creating an Application" on page 41.

   - **Application Type** :groups applications as web / thick-client or mobile.

   - **Application Attribute**: groups applications based on the values of the application attribute that you select from the **Attribute** list. This value is invalid if no application attributes have been created in the tenant.

     Note: The selection is limited to picklist type attributes that have ten or less values.

5. Click **Save**.

   You are returned to the **Scope** tab.

6. Select the policy that will be assigned to each value of the selected scope.

7. Click **Save**.

   Your security policy settings are saved.

Deleting a Security Policy

You can delete a custom security policy that is currently not in use. The Fortify on Demand default policy can be edited but not be deleted.

To delete a custom security policy:

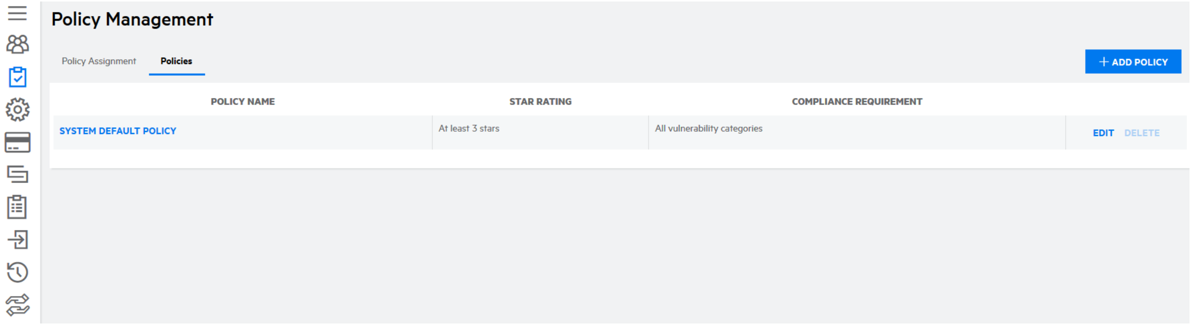
1. Select the **Administration** view.

   The **User Management** page appears.

2. Click **Policy Management**.

   The **Scope** tab of the **Policy Management** page appears.

3. Select the **Policies** tab.

   Policy Management

POLICY NAME	STAR RATING	COMPLIANCE REQUIREMENT	
SYSTEM DEFAULT POLICY	At least 3 stars	All vulnerability categories	EDIT DELETE

4. Click **Delete** in the row of the policy you want to delete.

   A confirmation message appears.

5. Click **Yes**.

   The policy is deleted.

Single Sign-On (SSO)

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

Fortify on Demand supports the following SAML 2.0 bindings:

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

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

- Configuring SSO in Fortify on Demand. For instructions, see "Configuring SSO in Fortify on Demand" on the next page.
- Adding the identity provider metadata to Fortify on Demand. For instructions, see "Adding the Identity Provider Metadata" on page 306.
- Downloading the Fortify on Demand metadata. For instructions, see "Downloading the Fortify on Demand Metadata" on page 308
- Configuring SSO in your identity provider. For instructions, see "Configuring SSO in the Identity Provider" on page 308.

Configuring SSO in Fortify on Demand

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

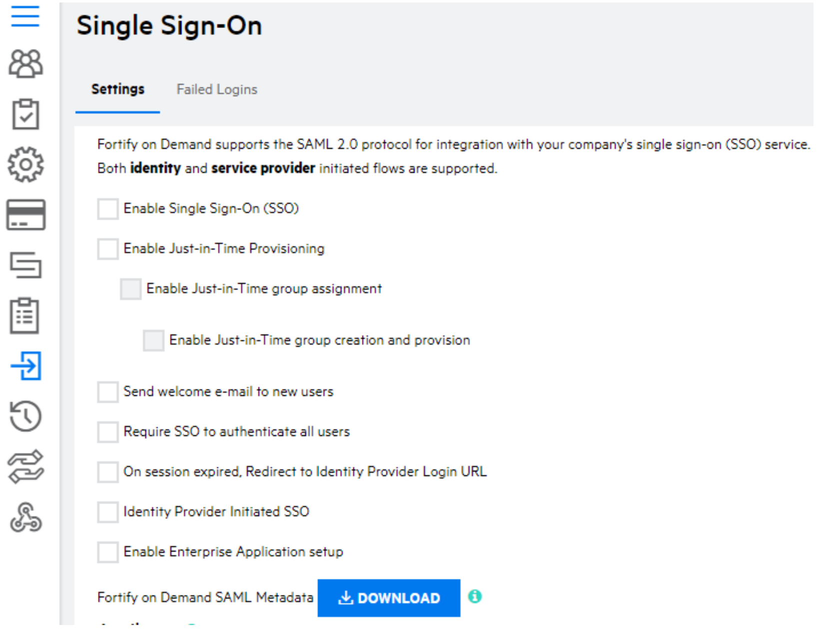
To configure the Fortify on Demand SSO settings:

1. Select the **Administration** view.

   The User Management page appears.

2. Click **Single Sign-On**.

   The Single Sign-On page appears.



Single Sign-On

Fortify on Demand supports the SAML 2.0 protocol for integration with your company's single sign-on (SSO) service. Both **identity** and **service provider** initiated flows are supported.

□ Enable Single Sign-On (SSO)

□ Enable Just-in-Time Provisioning

□ Enable Just-in-Time group assignment

□ Enable Just-in-Time group creation and provision

□ Send welcome e-mail to new users

□ Require SSO to authenticate all users

□ On session expired, Redirect to Identity Provider Login URL

□ Identity Provider Initiated SSO

□ Enable Enterprise Application setup

Fortify on Demand SAML Metadata

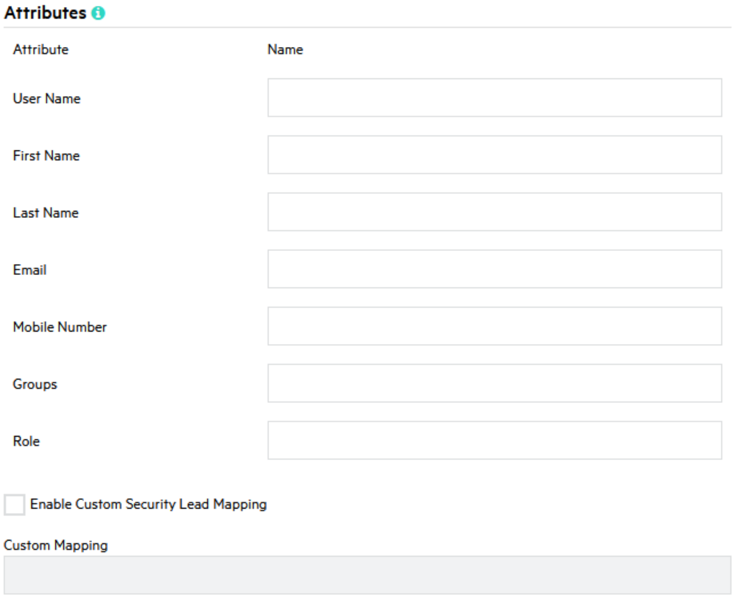
3. Select the desired check boxes:

Field	Description
Enable Single Sign-on (SSO)	This option enables SSO.
Enable Just-in-Time Provisioning	This option allows the automatic creation or update of Fortify on Demand user accounts for users who authenticate through your identify provider.
Enable Just in Time group assignment	**Enable Just-in-Time Provisioning** must be selected. This option allows the automatic update of Fortify on Demand user group assignments through your identity provider.

Field	Description
Enable Just in Time group creation and provision	**Enable Just-in-Time Provisioning** and **Enable Just in Time group assignment** must be selected. This option allows the automatic creation of Fortify on Demand user groups through your identity provider.
Send welcome e-mail to new users	New users who are created through the portal will receive a welcome email. However, the welcome email includes password setup instructions that do not apply to users who authenticate through SSO. If this option is not selected, welcome emails are not sent to any new users .
Require SSO to Authenticate All Users	This option requires all users to use SSO. If this option is not selected, users may log in to Fortify on Demand using SSO authentication or username and password on the standard login page. **Note:** Enabling this option prevents the use of some specialized clients and integrations that use the Fortify on Demand Web API because the Web API has limited support for SAML authentication tokens. For example, the iOS client requires non-SSO credentials to connect to Fortify on Demand. The recommended approach in this case is to generate a strong, random password (minimum 32 characters) that can be used as a “personal access token” for non-SSO authentication.
On session expired, Redirect to Identity Provider Login URL	This option has users redirected to their identity provider login page after the session expires or when the user logs out. This feature requires cookies to be enabled in the browser and a user login session within the last 30 days.
Identity Provider Initiated SSO	Fortify on Demand recommends the service provider-initiated SAML authentication flow, but supports both service provider-initiated and identity provider-initiated flows. If this option is not selected, users log in to Fortify on Demand using the SSO Login URL provided on this page. Fortify on Demand then makes a service provider-initiated request to the identity provider to authenticate the user. If this option is selected, the identity provider-initiated flow is used. Users log in by connecting directly to the identity provider and are redirected to Fortify on Demand after successful authentication.

Field	Description
Enable Enterprise Application setup	If your organization has multiple tenants, this option enables authentication through a single identity provider. **Note:** If you select this option and have an existing SSO configuration, you will need to download the updated Fortify on Demand metadata and import it into the identity provider, and reimport the identity provider metadata into Fortify on Demand. Alternatively, you can append `?t=`*`<sso_login_url_guid>`* to both the **Identity Provider Name** in the Fortify on Demand SSO settings and the service provider name in the identity provider settings, where *`<sso_login_url_guid>`* is a unique identifier found in the SSO Login URL.

4. In the **Attributes** section, map the attribute names expected by Fortify on Demand to those configured in the identify provider. Each attribute name defined here must match the exact **Name** value of the attribute used by the identity provider, and is often defined as a full schema URL. Some identity providers also send a shorter **FriendlyName** value for the attribute, which can also be used in the attribute mapping. For descriptions of each attribute, see "Configuring SSO in the Identity Provider" on page 308.



Attributes

Attribute	Name
User Name	
First Name	
Last Name	
Email	
Mobile Number	
Groups	
Role	

□ Enable Custom Security Lead Mapping

Custom Mapping

5. Select **Enable Custom Security Lead Mapping** to map a custom value (instead of the default "Security Lead" value) to the Security Lead role in SAML assertion. Type that value in the **Custom Mapping** field. Note that this invalidates the default "Security Lead" value used for the mapping.

6. Click **Save**.

   Your SSO settings are saved.

Adding the Identity Provider Metadata

Add the identity provider metadata by importing it into Fortify on Demand or manually configuring it.

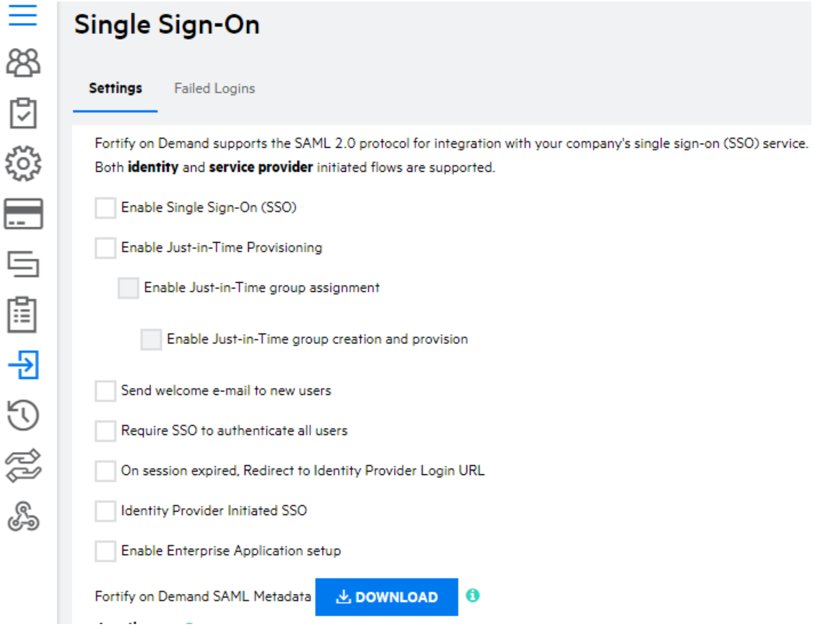
To add the identity provider metadata:

1. Select the **Administration** view.

   The **User Management** page appears.

2. Click **Single Sign-On**.

   The Single Sign-On page appears.

   Fortify on Demand supports the SAML 2.0 protocol for integration with your company's single sign-on (SSO) service. Both **identity** and **service provider** initiated flows are supported.

   □ Enable Single Sign-On (SSO)

   □ Enable Just-in-Time Provisioning

   □ Enable Just-in-Time group assignment

   □ Enable Just-in-Time group creation and provision

   □ Send welcome e-mail to new users

   □ Require SSO to authenticate all users

   □ On session expired, Redirect to Identity Provider Login URL

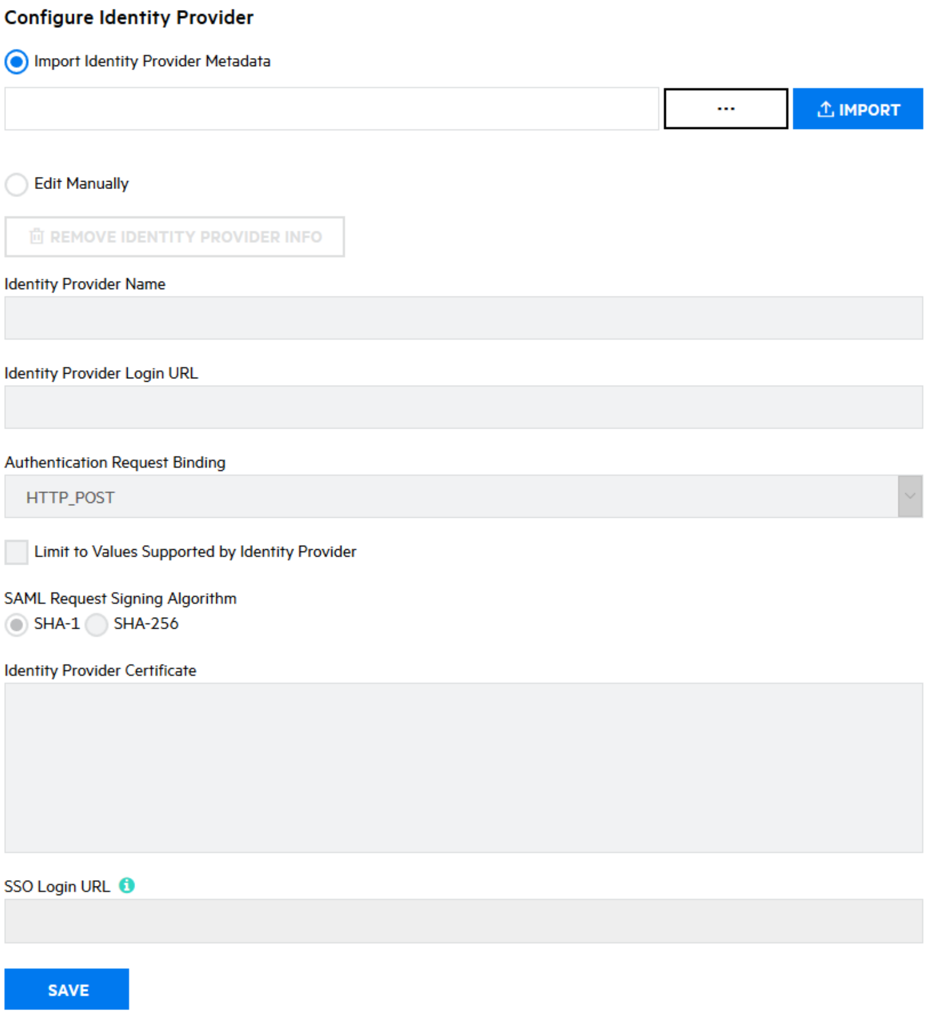
   □ Identity Provider Initiated SSO

   □ Enable Enterprise Application setup

   Fortify on Demand SAML Metadata

3. In the **Configure Identity Provider** section, select the method of adding the identity provider metadata:

   - **Import Identity Provider Metadata**
   - **Edit Manually**



Configure Identity Provider

● Import Identity Provider Metadata

○ Edit Manually

Identity Provider Name

Identity Provider Login URL

Authentication Request Binding: HTTP_POST

□ Limit to Values Supported by Identity Provider

SAML Request Signing Algorithm: ● SHA-1 ○ SHA-256

Identity Provider Certificate

SSO Login URL

4. Follow the instructions for the method that you selected.
   - Import the identity provider metadata:
     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**

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

5. Click **Save**.

   The identity provider metadata is added to Fortify on Demand.

Downloading the Fortify on Demand Metadata

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

To download the Fortify on Demand metadata file:

1. Select the **Administration** view.

   The User Management page appears.

2. Click **Single Sign-On**.

   The Single Sign-On page appears.

3. Click **Download**.

   The Fortify on Demand metadata file is saved to a local folder specified in your browser settings.

   > **Note:** The metadata is also available as a URL to support configuration in identity providers that support automatic metadata retrieval. The metadata is accessed using the absolute path “/SAML” on the portal site (for example, "https://ams.fortify.com/SAML"). The metadata URL does not require authentication, so it can be accessed by the identity provider without supplying Fortify on Demand credentials.

Configuring SSO in the Identity Provider

Fortify on Demand supports any identity provider that conforms to the SAML 2.0 specifications for browser-based authentication flows. Use the following instructions as a guideline for configuring your identity provider for use with Fortify on Demand.

Most required information about the Fortify on Demand service provider can be obtained from the SAML metadata, and many identity providers allows importing the metadata rather than configuring all the settings manually.

To configure SSO in the identity provider:

1. Accept authentication requests from Fortify on Demand.

   The identity provider must accept authentication requests sent from the Fortify on Demand service provider name. The service provider name is “https://*<tenant_host>*/SAML,” where the *<tenant_host>* is your Fortify on Demand datacenter (for example,"https://ams.fortify.com/SAML”). You can obtain the service provider name from the Fortify on Demand SAML metadata.

   Fortify on Demand signs all authentication requests, so you may also choose to validate the signature against the SAML certificate provided in the Fortify on Demand SAML metadata.

   > **Note:** Prior to version 5.2, Fortify on Demand used a service provider name that was incompatible with some identity providers. If you set up SSO authentication prior to version 5.2, you can keep the “urn:fortify:FodServiceProvider” service provider name for backward compatibility with the existing identity provider configuration. You are encouraged to migrate to the new service provider name at the earliest convenience.

2. Sign all SAML assertions.

   All SAML assertions sent to Fortify on Demand must be signed using the identity provider certificate specified in the Fortify on Demand SSO settings. Fortify on Demand accepts signatures on either the entire SAML response or just the assertion contained in the response.

   > **Note:** Fortify on Demand does not support encrypted assertions.

3. Make sure the identity provider's system clock is set properly, preferably from a central time source service such as NIST.

   Most SAML assertions contain a valid time period specified by the identity provider. Fortify on Demand checks the time period against its system clock when the assertion is received. Fortify on Demand allows a maximum of 3 minutes clock skew to account for differences in the clock settings. If the assertion is received more than 3 minutes after the expiration time specified in the assertion, then the assertion is rejected.

4. Set the URL where the identity provider will send the SAML assertion response after a user is authenticated

   The URL is known as the Assertion Consumer Service URL. It might have a different term, such as "Reply URL," depending on the identity provider. You can obtain the URL from the Fortify on Demand SAML metadata.

5. Define the identity claim attributes to include in the SAML assertion.

   Fortify on Demand uses the claim attributes in the SAML assertion to get information about the authenticated user.

   Every assertion must contain a `User Name` attribute, which identifies the user to Fortify on Demand. The value must be unique across Fortify on Demand, so you should use an identifier that is unique to your organization, such as an email address.

   > **Note:** Some systems use the **NameID** value in the Subject element of the SAML assertion to pass the user identifier. Fortify on Demand does not support use of **NameID**, so you must also map an attribute for `User Name`.

The following attributes are used for Just-In-Time (JIT) Provisioning. Attributes are required when creating a new Fortify on Demand user. When updating an existing Fortify on Demand user, all attributes are optional and existing values are retained for unspecified attributes.

Attribute	Required	Description
`Email`	Yes	Email address of the user. The value can be the same as the `User Name` value, but is not required. You can map both `User Name` and `Email` to the same attribute in the Fortify on Demand SSO settings.
`First Name`	Yes	First name of the user.
`Last Name`	Yes	Last name of the user.
`Mobile Number`	No	Mobile phone number of the user.
`Role`	No	User role. The value must be a plain text string that matches a role name (case-insensitive) in Fortify on Demand. If a value is not provided, the **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 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 Fortify on Demand if not found. If the value is set to TRUE, then a new user is created. If the value is set to FALSE or not provided, then a user is not created and the login request will fail if the user does not already exist in Fortify on Demand. **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 Fortify on

Attribute	Required	Description
		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`.

Note: You must configure Fortify on Demand to recognize the attributes used by the identity provider. See "Configuring SSO in Fortify on Demand" on page 303.

Troubleshooting Failed Logins

Troubleshooting a failed SSO authentication request can be a difficult task because the actual values passed in the SAML assertion are hidden from the user. To assist with troubleshooting efforts, the portal provides a log of failed SAML assertions. Failed assertions are deleted after 30 days.

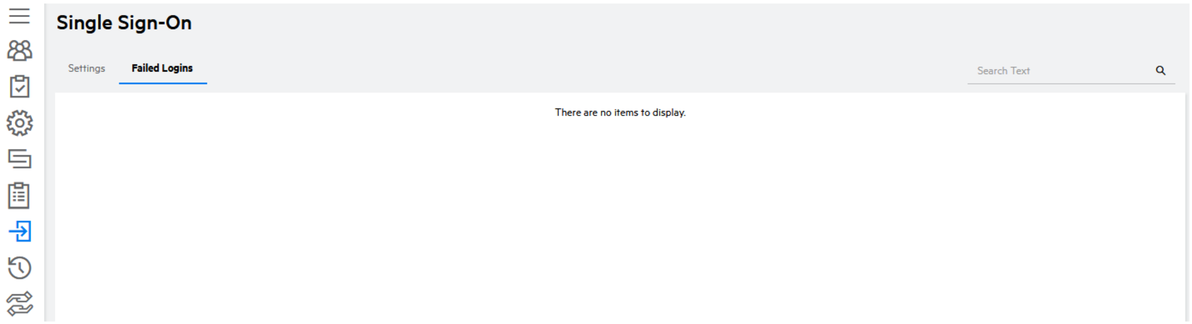
To view a log of failed SAML Assertions:

1. Select the **Administration** view.

   The User Management page appears.
2. Click **Single Sign-On**.

   The Single Sign-On page appears.
3. Select the **Failed Logins** tab.

   The failed SAML assertion log appears.



There are no items to display.

The grid contains the following columns:

- Received Time - The time that the SAML assertion was received.
- IP Address – The IP address of that client that requested authentication.
- Username – The username that was specified in the assertion, if one was found.
- Reason – A brief description of the reason why the SAML assertion was rejected.

4. Click the **Raw Assertion** link for any failed login to open an XML view of the decoded SAML assertion.

   The page displays the details of the assertion, including the time that the assertion was issued by the identity provider, the attributes and values that were provided, the valid time period and audience, and the certificate used to sign the assertion.

Vendor Management

If you would like to share your assessment results with a vendor your company does business with, or with another division of your company, you can do so through the portal, as long as each entity has its own tenant with Fortify on Demand. Relationships between tenants must be initiated by one tenant and confirmed by the other; no one can establish a connection to your tenant without your permission.

Also, each link goes in only one direction. That is, if you would like to share your reports, you must initiate a link to another tenant. If that tenant would like to share its reports with you, it must *also* initiate a link. The **Vendor Report** link is only visible after the sharing relationship is successful, and reports are shared.

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

This section covers the following topics:

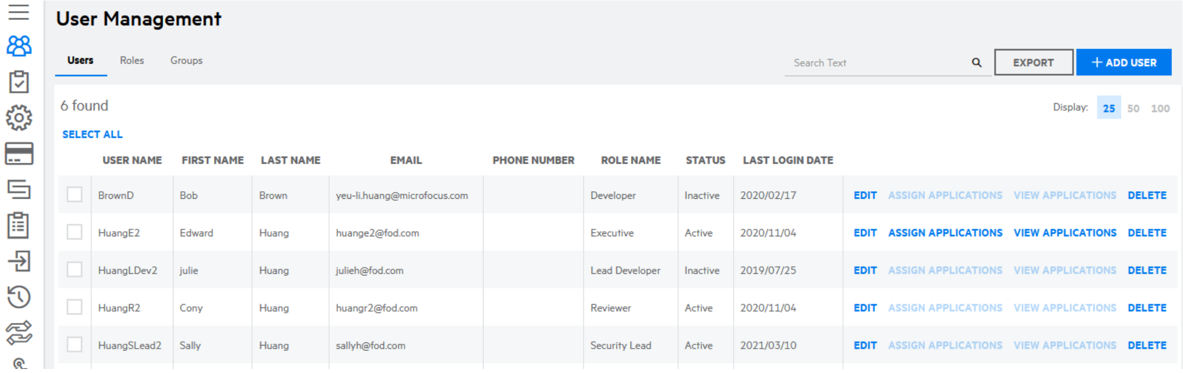
- Initiating a Relationship with Another Tenant
- Accepting a Relationship Initiated by Another Tenant
- Publishing a Vendor Management Report
- Viewing Published Report

Initiating a Relationship with Another Tenant

To establish your tenant as a “Vendor” (that is, one that can send reports to other tenants):

1. Select the **Administration** view.

   The **User Management** page appears.

   6 found

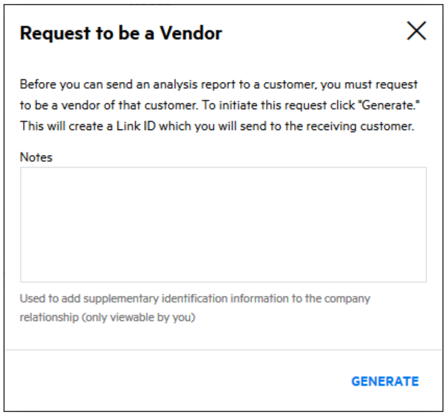
	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE				
□	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE
□	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT	ASSIGN APPLICATIONS	VIEW APPLICATIONS	DELETE

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

   > **Note:** "My Vendors" means tenants you can receive reports from, and “Customers” means tenants you can send reports to.

4. Click **Request to be a Vendor**.

   Use the optional **Notes** box to add information about the vendor-customer relationship.

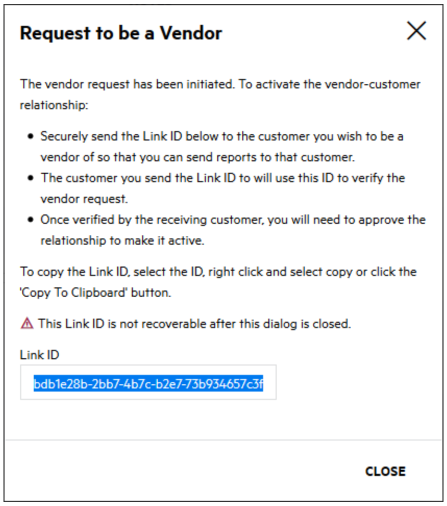
   Request to be a Vendor

   Before you can send an analysis report to a customer, you must request to be a vendor of that customer. To initiate this request click "Generate." This will create a Link ID which you will send to the receiving customer.

   Notes

   Used to add supplementary identification information to the company relationship (only viewable by you)

5. Click **Generate**, to display the**Link ID number**.



Request to be a Vendor

The vendor request has been initiated. To activate the vendor-customer relationship:

- Securely send the Link ID below to the customer you wish to be a vendor of so that you can send reports to that customer.
- The customer you send the Link ID to will use this ID to verify the vendor request.
- Once verified by the receiving customer, you will need to approve the relationship to make it active.

To copy the Link ID, select the ID, right click and select copy or click the 'Copy To Clipboard' button.

⚠ This Link ID is not recoverable after this dialog is closed.

Link ID

bdb1e28b-2bb7-4b7c-b2e7-73b934657c3f

6. Copy the **Link ID number**,
7. Send the link, via email or other secure transfer, to the appropriate contact at the company or tenant you would like to connect with.
8. Click **Close**.

Accepting a Relationship Initiated by Another Tenant

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

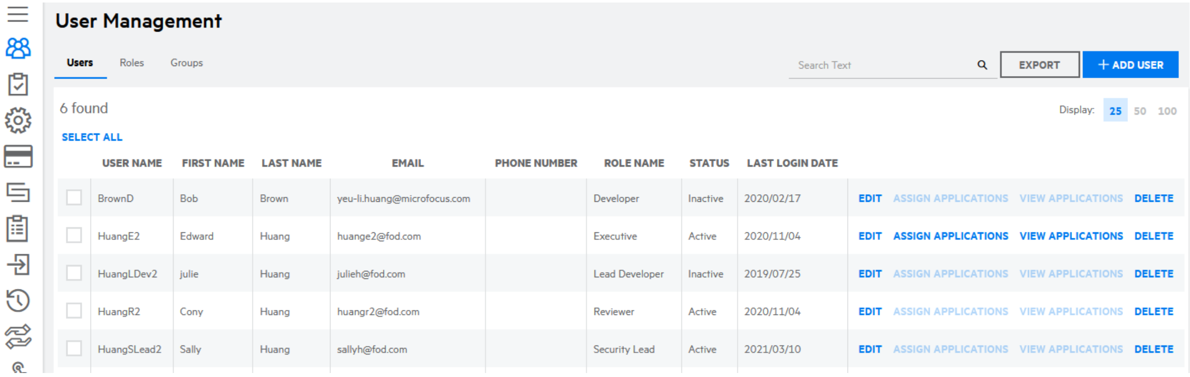
- "Confirm a Relationship" below
- "Establish your Tenant as a Customer" on the next page

Confirm a Relationship

To confirm a relationship with another tenant who has sent a request to you:

1. Select the **Administration** view.

   The **User Management** page appears.



6 found

	USER NAME	FIRST NAME	LAST NAME	EMAIL	PHONE NUMBER	ROLE NAME	STATUS	LAST LOGIN DATE	
□	BrownD	Bob	Brown	yeu-li.huang@microfocus.com		Developer	Inactive	2020/02/17	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangE2	Edward	Huang	huange2@fod.com		Executive	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangLDev2	julie	Huang	julieh@fod.com		Lead Developer	Inactive	2019/07/25	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangR2	Cony	Huang	huangr2@fod.com		Reviewer	Active	2020/11/04	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE
□	HuangSLead2	Sally	Huang	sallyh@fod.com		Security Lead	Active	2021/03/10	EDIT ASSIGN APPLICATIONS VIEW APPLICATIONS DELETE

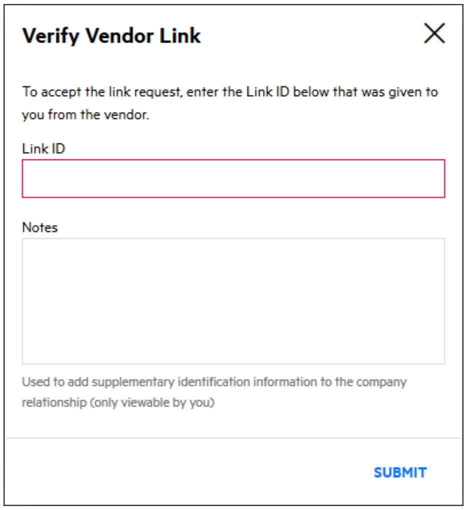
2. Click **Vendors**.

The **Vendor Management** page opens, displaying the **My Vendors** and **Customers** tabs. In this context, “Vendors” means tenants you can receive reports from, and “Customers” means tenants you can send reports to.

Establish your Tenant as a Customer

To establish your tenant as a “Customer” (that is, one that can receive reports from other tenants):

1. Click **My Vendors**.
2. Click **Verify Vendor Link**.



Verify Vendor Link

To accept the link request, enter the Link ID below that was given to you from the vendor.

Link ID

Notes

Used to add supplementary identification information to the company relationship (only viewable by you)

3. Paste the **Link ID** you received from the other tenant.
4. (Optional) Add supplementary notes about the company relationship (For example: subsidiary, or AUS division). These notes are viewable only to you.
5. Click **Submit**.

Publishing a Vendor Management Report

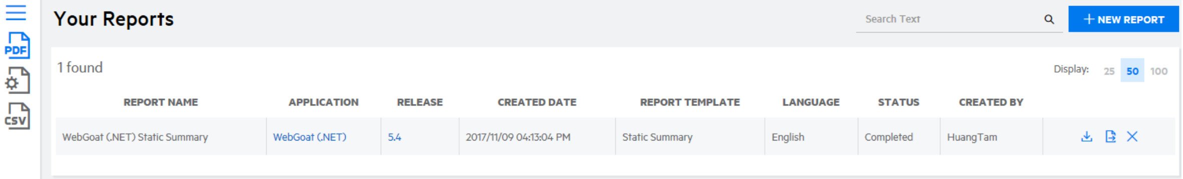
Once you have established a relationship with another tenant in Fortify on Demand, you can “publish” your reports so that tenant can review them.

To share a report with an approved vendor:

1. Select the **Reports** page.

   A new screen appears, with a list of all reports that have been generated for your tenant.

2. Click the name of the report you want to share. The page refreshes with the **Reports Details** below the reports list.



Your Reports

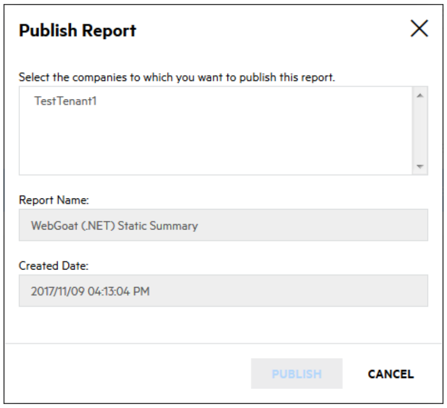
1 found

Display: 25 50 100

REPORT NAME	APPLICATION	RELEASE	CREATED DATE	REPORT TEMPLATE	LANGUAGE	STATUS	CREATED BY
WebGoat (.NET) Static Summary	WebGoat (.NET)	5.4	2017/11/09 04:13:04 PM	Static Summary	English	Completed	HuangTam

3. Click .

   The **Publish Report** window appears. If you have relationships established with other tenants, those tenants' names appear in the white box.



Publish Report

Select the companies to which you want to publish this report.

TestTenant1

Report Name: WebGoat (.NET) Static Summary

Created Date: 2017/11/09 04:13:04 PM

4. Select the tenant name to which you want to send the report, and click **Publish**.

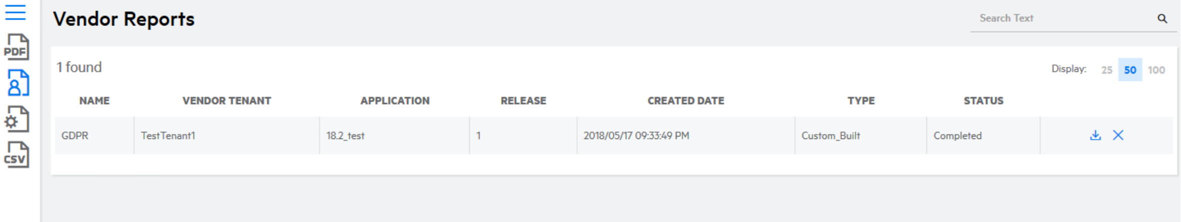
   A note appears informing you that the report has been queued for publishing and will be sent to the other tenant.

Viewing Published Report

After another tenant has published a report to you (that is, "shared" a report with your tenant), you may view that report by following these steps:

1. Select the **Reports** page.
2. Click **Vendor Report**.

   A **Report List** appears, showing the reports that have been shared with you by other tenants.



Vendor Reports

1 found

NAME	VENDOR TENANT	APPLICATION	RELEASE	CREATED DATE	TYPE	STATUS	
GDPR	TestTenant1	18.2_test	1	2018/05/17 09:33:49 PM	Custom_Built	Completed	⤓ ✕

3. Highlight a report from the list, click **Download Report** in the **Action** column.

   A note appears informing you that the report is available to you in PDF format in your system Downloads folder.

Note: If **Vendor Report** does not appear in the list of report types screen, that means no reports have yet been shared by another tenant. Check to make sure that you and the other tenant have both completed all the steps required to create a successful sharing relationship and that a specific report has been "published" to you.

Chapter 8: Fortify on Demand API

Fortify on Demand provides a RESTful Application Programming Interface (API) that allow users to carry out various tasks and access application and release data. The latest version of the API is version 3. The API root URL is determined by the tenant's data center:

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

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

This section contains the following topics:

API Authentication

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

To authenticate Fortify on Demand API calls:

1. Make a POST request to the token endpoint `<datacenter_root_URL>/oauth/token` with the following body parameters:

   Note: For a list of data center API root URLs, see "Fortify on Demand API" above.

Body Parameter	**Description**
`scope`	Scopes granted to an access token (in lower case). Separate multiple scope values with a space. For a list of scopes, see "API Scopes" on the next page.
`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 will fail. For more information on personal access tokens, see "Personal Access Tokens" on page 320.
`client_id`	API key
`client_secret`	API secret

A token in a JSON response named "access_token" is returned.

2. Use this token in the Authorization header as a Bearer token:

```
Authorization: Bearer {token}
```

The following is an example request to get a bearer token using user credentials:

```
curl --request POST 'https://api.ams.fortify.com/oauth/token' \
--form 'scope="api-tenant"' \
--form 'grant_type="password"' \
--form 'username="myTenantCode\\myUsername"' \
--form 'password="myPassword"'
```

The following is an example request to get a bearer token using an API key and secret.

```
curl --request POST 'https://api.ams.fortify.com/oauth/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'scope=api-tenant' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_id=myApiKey' \
--data-urlencode 'client_secret=myApiSecret'
```

API Scopes

Scopes limit the access that is granted to access tokens. They do not grant additional permissions beyond what a user currently has. You can view the details of an endpoint in API Explorer to see its allowed scopes.

The following table lists the available scopes:

Scope	**Description**
api-tenant	Grants access to all endpoints
start-scans	Configure and start static, dynamic, and mobile scans; import static and dynamic scans
manage-apps	Manage applications
view-apps	View applications
manage-issues	Manage issues
view-issues	View issues
manage-reports	Manage reports
view-reports	View reports
manage-users	Manage users
view-users	View users
manage-notifications	Manage notifications
view-tenant-data	View data at the tenant level

Personal Access Tokens

Personal access tokens are unique keys tied to the user who generated them. They function as alternate passwords that are used to authenticate to the API; they have the user's permissions and can be further restricted with scopes. Using personal access tokens bypasses two-factor authentication and SSO requirements set in the portal.

> **Note:** Personal access tokens cannot be used to log in to the portal.

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

Fortify on Demand sends email and portal notifications 14 days before a personal access token expires. An expired personal access token cannot be used unless a new secret is generated.

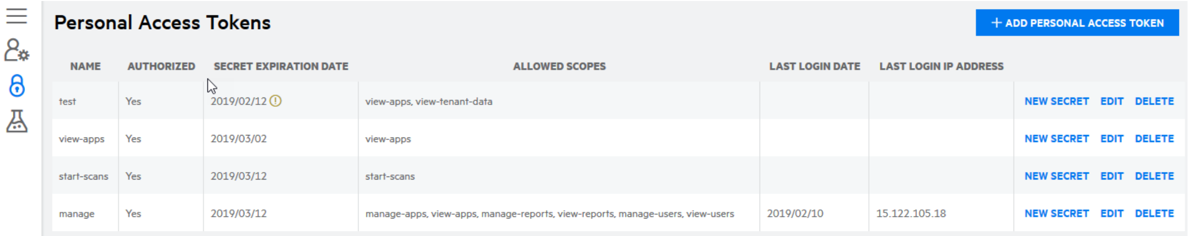
This section covers the following topics:

Creating a Personal Access Token

To create a personal access token:

1. Click your account name and select **Personal Access Tokens**.

   The Personal Access Tokens page appears.

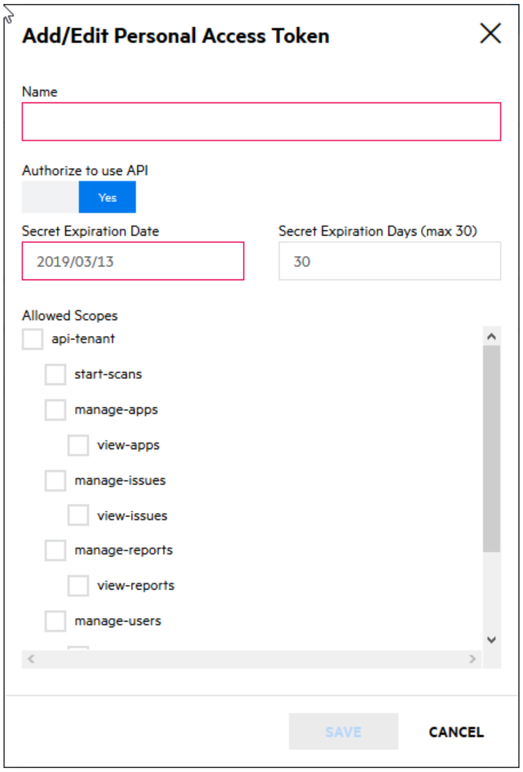


Personal Access Tokens

NAME	AUTHORIZED	SECRET EXPIRATION DATE	ALLOWED SCOPES	LAST LOGIN DATE	LAST LOGIN IP ADDRESS	
test	Yes	2019/02/12 ⓘ	view-apps, view-tenant-data			NEW SECRET EDIT DELETE
view-apps	Yes	2019/03/02	view-apps			NEW SECRET EDIT DELETE
start-scans	Yes	2019/03/12	start-scans			NEW SECRET EDIT DELETE
manage	Yes	2019/03/12	manage-apps, view-apps, manage-reports, view-reports, manage-users, view-users	2019/02/10	15.122.105.18	NEW SECRET EDIT DELETE

2. Click **+Add Personal Access Token**.

   The Add/Edit Personal Access Token window opens.



Add/Edit Personal Access Token

Name

Authorize to use API: Yes

Secret Expiration Date: 2019/03/13

Secret Expiration Days (max 30): 30

Allowed Scopes

- □ api-tenant
  - □ start-scans
  - □ manage-apps
    - □ view-apps
  - □ manage-issues
    - □ view-issues
  - □ manage-reports
    - □ view-reports
  - □ manage-users

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. Move the slider to **No** to 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. 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" on page 319.

4. Click **Save**.

   The Secret Key window opens.

5. Copy your Base64 encoded secret. The secret is only shown once.

6. Click **Close**.

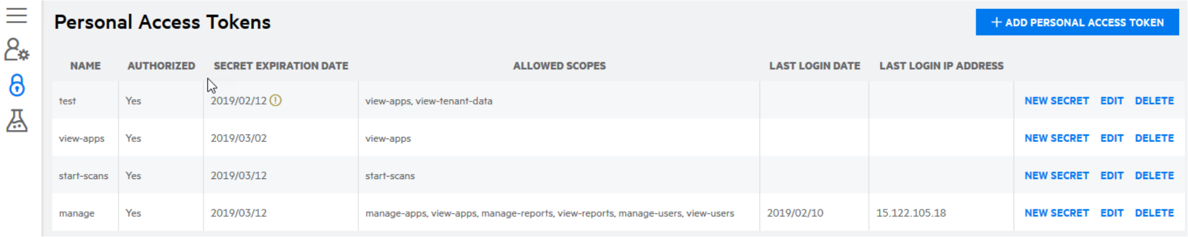
   The new token appears in the personal access token list.

Editing or Deleting a Personal Access Token

To edit or delete a personal access token:

1. Click your account name and select **Personal Access Tokens**.

   The Personal Access Tokens page appears.



Personal Access Tokens

NAME	AUTHORIZED	SECRET EXPIRATION DATE	ALLOWED SCOPES	LAST LOGIN DATE	LAST LOGIN IP ADDRESS	
test	Yes	2019/02/12 ⓘ	view-apps, view-tenant-data			NEW SECRET EDIT DELETE
view-apps	Yes	2019/03/02	view-apps			NEW SECRET EDIT DELETE
start-scans	Yes	2019/03/12	start-scans			NEW SECRET EDIT DELETE
manage	Yes	2019/03/12	manage-apps, view-apps, manage-reports, view-reports, manage-users, view-users	2019/02/10	15.122.105.18	NEW SECRET EDIT DELETE

2. You can perform the following tasks:

Task	Procedure
Generate a new secret	a. Click **New Secret**. The New Secret window opens. b. Use the calendar to select an expiration date or type the number of days after which a secret expires. The token will expire at 00:00 PT of the date you set. The expiration date cannot exceed the maximum lifetime as set by the portal. c. Click **Create**. This will void the current secret.
Edit the token	a. Click **Edit**. The Add/Edit Personal Access Token window opens. b. Edit the fields as needed. You cannot edit the current secret's expiration date.
Delete the token	a. Click **Delete**. A confirmation message appears. b. Click **Yes**.

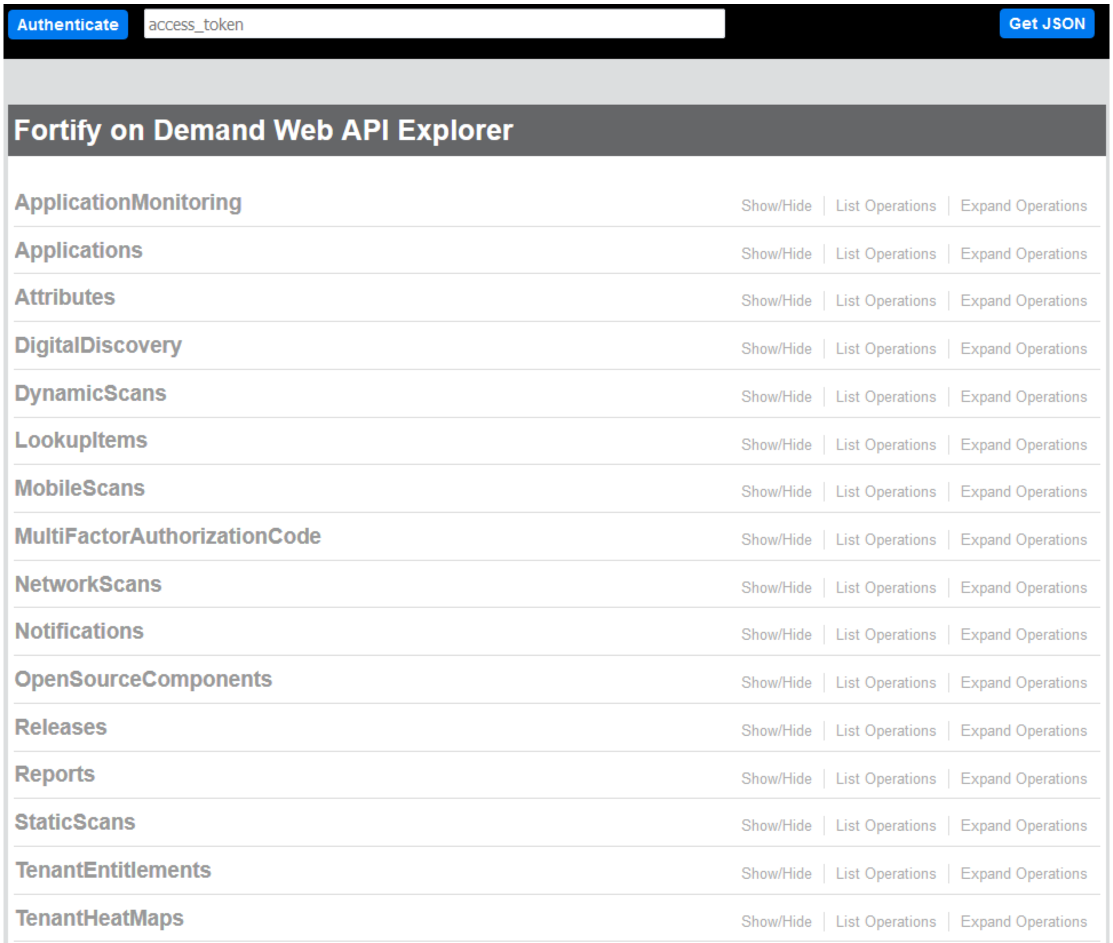
Viewing API Documentation through API Explorer

Fortify on Demand API documentation is provided in the form of API Explorer. API Explorer is built on the Swagger (OpenAPI) framework and is available directly from the portal. This allows the API to be self-documenting and interactive; users can instantly view the latest updates to the API and test calls, as well as use the JSON description of the API to generate stubs and SDKs in different programming languages through open source tools like Swagger Editor and Swagger Codegen.

To view API Explorer:

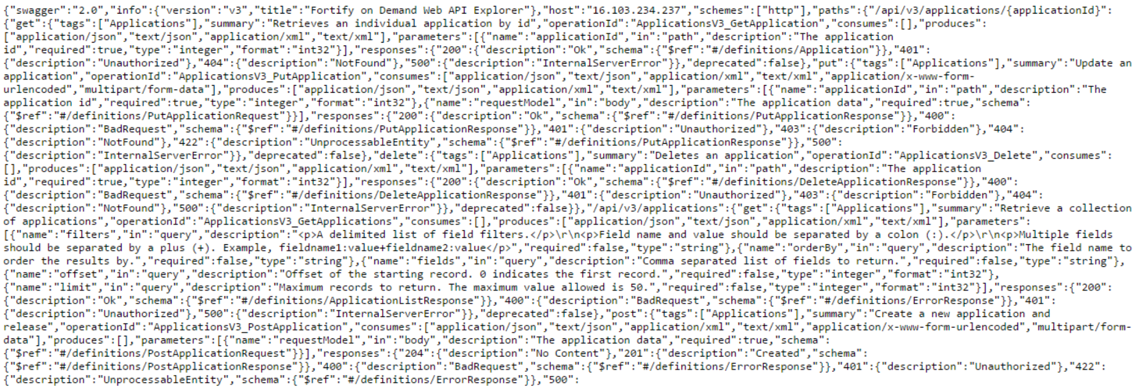
1. Click your account name on the toolbar and select **API Explorer**.

   The API Explorer page opens in a new window, displaying a list of resources.



2. Explore the resources in greater detail:

   - Click **GET JSON** at the top of the API Explorer page. The browser displays the JSON description of the API.



```
{"swagger":"2.0","info":{"version":"v3","title":"Fortify on Demand Web API Explorer"},"host":"16.103.234.237","schemes":["http"],"paths":{"/api/v3/applications/{applicationId}":
{"get":{"tags":["Applications"],"summary":"Retrieves an individual application by id","operationId":"ApplicationsV3_GetApplication","consumes":[],"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.

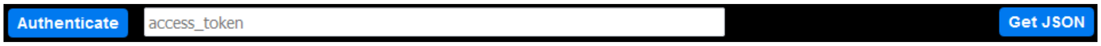
- Click **Show/Hide** to switch between showing and hiding the endpoints.
- Click **List Operations** to view a resource's endpoints.
- Click **Expand Operations** to view the descriptions of all the resource's endpoints.
- Click an endpoint to view its description.

Testing API Endpoints through API Explorer

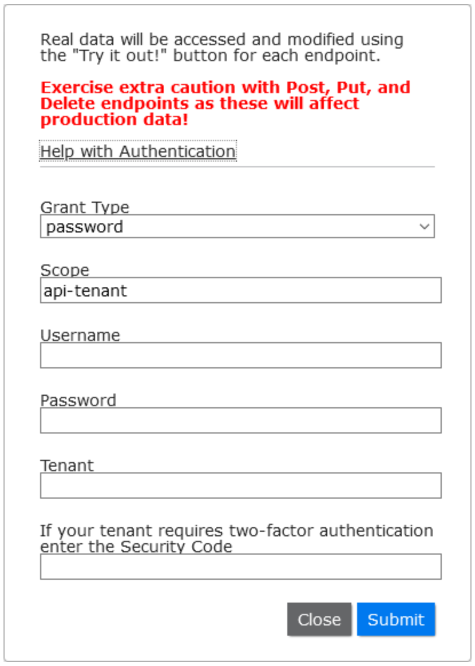
You can test the version 3 API endpoints in API Explorer.

> **Important!** POST, PUT, and DELETE methods in API Explorer modify the tenant data in the portal.

1. Click **Authenticate** at the top of the API Explorer page.

   A modal window opens where you provide your authentication credentials.

   Real data will be accessed and modified using the "Try it out!" button for each endpoint.

   Exercise extra caution with Post, Put, and Delete endpoints as these will affect production data!

   Help with Authentication

   Grant Type: password

   Scope: api-tenant

   Username

   Password

   Tenant

   If your tenant requires two-factor authentication enter the Security Code

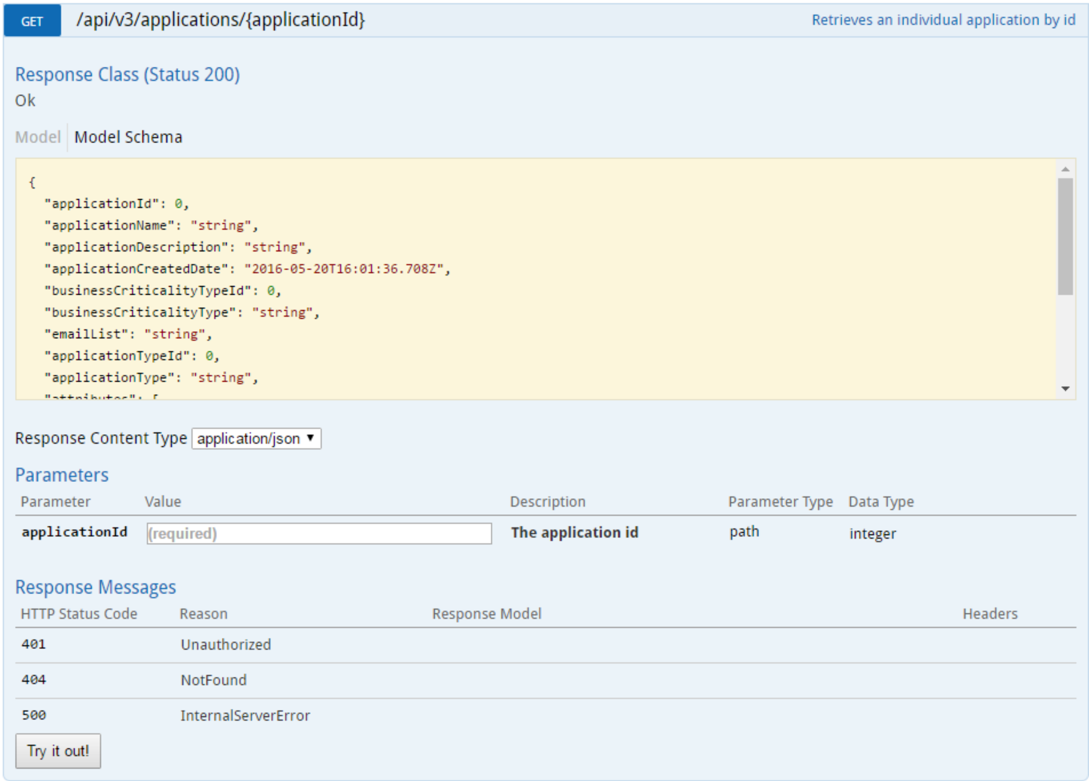
2. Select the method of authentication from the **Grant Type** list:
   - **password**: the user account credentials in the portal
   - **client_credentials**: the API keys generated in the portal
3. In the **Scope** field, type the scopes that will be granted to an access token. Separate multiple scope values with a space. For a list of scopes, see "API Scopes" on page 319.
4. Provide your authentication credentials:

Method of Authentication	**Procedure**
client_ credentials	a. In the **Client ID** field, type the API Key. For information on creating an API key, see "Creating an API Key" on page 257. b. In the **Client Secret** field, type the API secret.
password	**Note:** You can obtain your tenant code and username from your account settings. a. In the **Username** field, type your account username. b. In the **Password** field, type your account password or your personal access token. **Note:** If a personal access token is used and the specified scopes are not a subset of the personal access token's allowed scopes, the authentication will fail. c. In the **Tenant** field, type your tenant code. d. (Required if two-factor authentication is enabled) In the **Security Code** field, type the security code you received as part of two-factor authentication.

5. Click **Submit**.

   An access token is generated for the session.

6. Expand an endpoint and complete the parameters in the fields provided.



GET /api/v3/applications/{applicationId} Retrieves an individual application by id

Response Class (Status 200)

Ok

Model | Model Schema

```
{
  "applicationId": 0,
  "applicationName": "string",
  "applicationDescription": "string",
  "applicationCreatedDate": "2016-05-20T16:01:36.708Z",
  "businessCriticalityTypeId": 0,
  "businessCriticalityType": "string",
  "emailList": "string",
  "applicationTypeId": 0,
  "applicationType": "string",
  "attributes": [
```

Response Content Type application/json ▾

Parameters

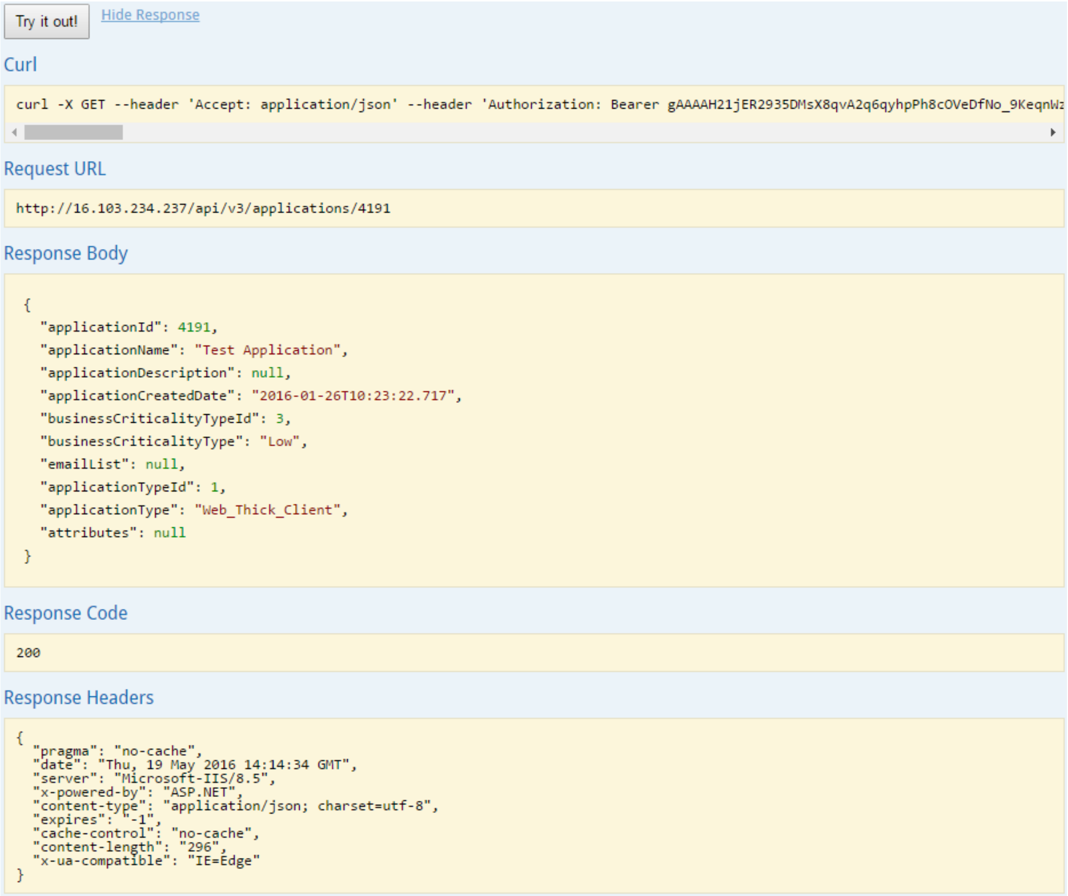
Parameter	Value	Description	Parameter Type	Data Type
applicationId	(required)	**The application id**	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
401	Unauthorized		
404	NotFound		
500	InternalServerError		

7. Click **Try it out!**.

   The response is displayed below.



Curl

```
curl -X GET --header 'Accept: application/json' --header 'Authorization: Bearer gAAAAH21jER2935DMsX8qvA2q6qyhpPh8cOVeDfNo_9KeqnWz
```

Request URL

```
http://16.103.234.237/api/v3/applications/4191
```

Response Body

```
{
  "applicationId": 4191,
  "applicationName": "Test Application",
  "applicationDescription": null,
  "applicationCreatedDate": "2016-01-26T10:23:22.717",
  "businessCriticalityTypeId": 3,
  "businessCriticalityType": "Low",
  "emailList": null,
  "applicationTypeId": 1,
  "applicationType": "Web_Thick_Client",
  "attributes": null
}
```

Response Code

```
200
```

Response Headers

```
{
  "pragma": "no-cache",
  "date": "Thu, 19 May 2016 14:14:34 GMT",
  "server": "Microsoft-IIS/8.5",
  "x-powered-by": "ASP.NET",
  "content-type": "application/json; charset=utf-8",
  "expires": "-1",
  "cache-control": "no-cache",
  "content-length": "296",
  "x-ua-compatible": "IE=Edge"
}
```

API Rate Limits

Fortify on Demand implements API rate limiting on a per endpoint and per user or key basis.

The following endpoints are unthrottled:

- PUT/api/v3/releases/{releaseId}/dynamic-scans/import-scan
- POST /api/v3/releases/{releaseId}/mobile-scans/start-scan
- PUT /api/v3/releases/{releaseId}/mobile-scans/import-scan
- POST /api/v3/releases/{releaseId}/static-scans/start-scan
- PUT /api/v3/releases/{releaseId}/static-scans/import-scan

The following table lists the rate limits for throttled endpoints.

Endpoint	Max Requests	Seconds
POST /api/v3/applications	6	30

Endpoint	Max Requests	Seconds
PUT /api/v3/applications/{applicationId:int}	1	30
GET /api/v3/eventlogs/download	1	300
POST /api/v3/releases	6	30
PUT /api/v3/releases/{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

Tracking Rate Limits

When calling an API endpoint, the response HTTP header provides the rate limit and how quickly you are approaching the rate limit:

- X-Rate-Limit-Limit: the maximum number of requests
- X-Rate-Limit-Remaining: the number of requests remaining
- X-Rate-Limit-Reset: the number of seconds until the rate limit resets

When you reach the rate limit for an API endpoint, the API returns an HTTP 429 "Too Many Requests" response status code along with a response message such as:

```
{
  "errors": [
    {
      "errorCode": null,
      "message": "Rate limit of 1 request(s) every 15 second(s) has been
exceeded"
    }
  ]
}
```

Best Practices To Avoid Rate Limiting

To avoid rate limiting when calling the API, use the following best practices to reduce and regulate the number of API requests:

- Cache frequently used data.

  For API endpoints that are frequently used, cache the API responses and load the cached responses when requesting the data.

- Eliminate any unnecessary API calls.

  Examine requests obtaining data that isn't being utilized and requests submitting data to Fortify on Demand without any changes.

- Regulate the request rate

  If you regularly reach the rate limit, consider including a process that regulates the rate of your requests so that they fall within the given rate limits. You can regulate the request rate statically by setting a fixed request rate or dynamically by tracking requests and regulating them when approaching the rate limit.

Chapter 9: Integrations and Tools

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

This section contains the following topics:

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 Tool	Description	More Information
FoDUploader	Stand-alone utility for uploading code from a build server to Fortify on Demand for static scanning	Github
Fortify on Demand Jenkins Plugin	Jenkins plugin for uploading code to Fortify on Demand and submitting static scans as build tasks	Fortify on Demand Jenkins Plugin Documentation
Fortify Azure DevOps Extension	Azure DevOps extension for: • Uploading code to Fortify on Demand and submitting static scans as build and release tasks • Submitting dynamic scans as build and release tasks	Fortify Azure DevOps Extension Documentation
Fortify Bitbucket PIpelines	Collection of Bitbucket pipelines for: • Uploading code to Fortify on Demand and	Bitbucket

CICD Tool	Description	More Information
	submitting static scans	
Fortify GitHub Actions	Collection of GitHub actions for: - Uploading code to Fortify on Demand and submitting static scans	GitHub
Fortify GitLab CI Templates	Collection of GitLab templates for: - Uploading code to 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 execute CICD workflows	Docker Hub

IDE Tools

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

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

IDE Tool	Description	More Information
Eclipse Plugin	Eclipse plugin for uploading code to Fortify on Demand for static scanning and opening scan results for remediation	Fortify on Demand Plugin for Eclipse
IntelliJ IDEA Plugin	IntelliJ IDEA plugin for uploading code to Fortify on Demand for static scanning and opening scan results for remediation	Fortify on Demand Plugin for IntelliJ IDEA
Visual Studio Extension	Visual Studio extension for uploading code to Fortify on Demand for static scanning and opening scan results for remediation	Fortify on Demand Extension for Visual Studio
Fortify Extension for Visual Studio Code	Visual Studio Code extension for uploading code for static scanning	Fortify Visual Studio Code Extension Documentation

IDE Tool	Description	More Information
Fortify Security Assistant for Eclipse	Fortify Security Assistant for Eclipse provides alerts to potential security issues in Java files as you write code.[1] 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 for IntelliJ and Android Studio	Fortify Security Assistant for IntelliJ and Android Studio provides alerts to potential security issues in Java files as you write code.[1] 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 IDEA Documentation
Fortify Security Assistant for Visual Studio	Fortify Security Assistant for Visual Studio provides alerts to potential security issues in C# (.cs) , Razor (.cshtml), WebForms (.aspx), .config, .xml, and .ini files as you write code.[1] 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

[1] Fortify Security Assistant requires a valid license file to scan for issues and to install or update Fortify security content. Fortify on Demand offers a license valid for up to 10 developers per each application that is under an active static assessment subscription. The license is valid for all Fortify Security Assistant versions.

FoDUploader

Fortify on Demand provides a build server integration (BSI) tool called FoDUploader to help you upload application code from a build server. FoDUploader runs from the command-line on all major operating systems and thus can easily be integrated into a build script.

The benefits of using FoDUploader include:

- Sending files to Fortify on Demand without size limitations aside from those specified in "Static Assessment File Requirements" on page 91
- Transmitting files securely from a client workstation to Fortify on Demand
- Transmitting through a proxy, if required
- API key pair or PAT authentication

Downloading FoDUploader

FoDUploader is available as a Java application named `FoDUpload.jar`. `FoDUpload.jar` and its source code is hosted at https://github.com/fod-dev/fod-uploader-java.

Running FoDUploader

Prerequisite: Java 8 or later must be installed.

To run FoDUploader:

In a command-line interface, run `FodUpload.jar` with the appropriate arguments. You can also insert the command in your build script to integrate with your build server. The basix syntax is:

```
java -jar FoDUpload.jar -z "<zip_file_path>" {-ac <key> <secret>|-uc
<username> <password>} {-rid <relID>|-bsi <token>} -purl <purl> -aurl
<aurl> -tc <tcode> -ep
{1|SingleScanOnly|2|SubscriptionOnly|3|SingleScanFirstThenSubscription|4|Su
bscriptionFirstThenSingleScan}
```

If the command is properly executed, the command-line displays the bytes sent and the upload status. Otherwise, the command-line displays an error message indicating the part of the command that is incorrect.

FoDUploader Arguments

The following table describes the FoDUploader arguments. Arguments can be specified in any order.

Note: Flag arguments are false by default. Include a flag to set it to true—you do not need to specify `true` or `false`.

Note: Arguments are for version 5.4.1. Details on the latest release is available at https://github.com/fod-dev/fod-uploader-java.

Argument	Short Name	Required	Description
-zipLocation	-z	Yes	Location of the zip file. Enclose the path with quotation marks to escape special characters.
-entitlementPreferenceType	-ep	Yes	Entitlement preference: 1/SingleScanOnly, 2/SubscriptionOnly, 3/SingleScanFirstThenSubscription, 4/SubscriptionFirstThenSingleScan If multiple entitlements are available, the scan will use the oldest entitlement. If the release has an active subscription, the scan will use the active subscription.
-apiCredentials	-ac	Yes[1]	API key and secret.
-userCredentials	-uc	Yes[1]	Your user credentials. Enclose the username and password separately with quotation marks to escape special characters.
-bsiToken	-bsi	Yes[2]	BSI token.
-releaseId	-rid	Yes[2]	Release ID. The release must have saved scan settings in the portal for the release ID to be used as a token.
-portalurl	-purl	Yes[3]	Domain URL.
-apiurl	-aurl	Yes[3]	API root URL.
-tenantCode	-tc	Yes[3]	Tenant code if using user credentials.
- assessmentTypeId	-at	Yes[4]	Assessment type ID.

Argument	Short Name	Required	Description
-entitlement	-eid	Yes [4]	Entitlement ID.
-technologyStackId	-ts	Yes [4]	Technology stack as an integer: 32 (Auto Detect) 1 (.NET), 23 (.Net Core), 2 (ABAP), 21 (Apex/Visualforce), 3 (ASP), 5 (CFML), 6 (COBOL), 29 (Dart/Futter) 22 (Go), 27 (Infrastructure-As-Code/Dockerfile), 7 (JAVA/J2EE/Kotlin), 16 (JS/TS/HTML), 18 (MBS/C/C++/Scala), 9 (PHP), 10 (PYTHON), 28 (React Native), 17 (Ruby), 12 (Swift/Objective C/C++), 11 (VB6), 14 (VBScript)
-languageLevelId	-l	Yes[4]	Language level as an integer: • .NET: 2 (2.0), 3 (3.0), 4 (3.5), 5 (4.0), 11 (4.5), 15 (4.6), 16 (4.7), 30, (4.8), 32 (5.0), 33 (6.0), 35 (7.0), 38 (8.0) • .NET Core: 23 (1.0), 24 (1.1), 25 (2.0), 26 (2.1), 27 (2.2), 28 (3.0), 29 (3.1) • Java: 8 (1.5), 9 (1.6), 10 (1.7), 12 (1.8), 17 (1.9), 19 (10), 20 (11), 21 (12), 22 (13), 31 (14), 34(17), 39 (21) • Python: 13 (2), 14 (2 Django), 18 (3), 37 (4.2 Django), 40 (5.0 Django)
-auditPreferenceId	-a	Yes[4]	Audit preference: Manual, Automated
-isBinaryScan	-bs	No[4]	Scan compiled and source code

Argument	Short Name	Required	Description
			(the feature must be enabled).
-allowopenSourceComponentAnalysis	-os	No[4]	Include open source component analysis
-remediationScanPreferenceType	-rp	No	Remediation scan preference: 0/RemediationScanIfAvailable, 1/RemediationScanOnly, 2/NonRemediationScanOnly (default)
-inProgressScanActionType	-pp	No	If an in-progress scan exists, the action to take for the new scan: 0/DoNotStartScan (default), 1/CancelScanInProgress, 2/Queue This only applies if the in-progress scan can be automatically cancelled.
-pollingInterval	-I	No	Length of time in minutes between polling Fortify on Demand for the scan status. Polling stops once a scan is canceled, completed, or paused. If the polling interval is not set or set to 0, no polling is done. Exit codes: • 0 = success, scan completed and passed policy • 1 = failure, scan completed and failed policy • 3 = failure, scan canceled • 4 = failure, scan paused
-purchaseEntitlement	-purchase	No	Purchase an entitlement if none is available (the feature needs to be

Argument	Short Name	Required	Description
			enabled).
-allowPolicyFail	-apf	No	Return exit(0) instead of exit(1) if the scan fails the security policy specified in Fortify on Demand
-proxy	-P	No	Proxy connection details (order dependent): • The proxy host defined with a protocol (such as http) • The account credentials on the proxy server • The proxy server’s domain name for NTLM authentication • The proxy server's host name for NTLM authentication
-notes	-n	No	Adds notes about the scan.
-help	-h	No	Prints the help dialog.
-version	-v	No	Prints the FoDUploader version.

[1] Use either API credentials or user credentials.

[2] Use either release ID or BSI token. If both are provided, then the scan settings that are retrieved from the release ID will be used.

[3] Required if BSI token is not provided.

[4] Required if neither release ID nor BSI token is provided. Provided values override existing release ID or BSI token settings.

Examples

Command-line examples:

```
java -jar FodUpload.jar -z package.zip -purl https://ams.fortify.com -aurl
https://api.ams.fortify.com -tc AcmeCo -uc myUsername myPersonalAccessToken
-rid 123456 -ep 2
```

```
C:\Program Files (x86)\Java\jre-9\bin\java.exe -jar C:\fod_
upload\FodUpload.jar -z c:\Build\Input\applicationFiles.zip -uc john-doe
pswd!@#$ -P http://192.168.56.1:808 proxyuser1 proxyuserpassword -bsi
eyJ0ZW5hbnRJZCI6NSwidGVuYW50Q29kZSI6InR0MSIsInJlbGVhc2VJZCI6NDQwNiwicGF5bG9
hZFR5cGUiOiJBTkFMWVNJU19QQVlMT0FEIiwiYXNzZXNzbWVudFR5cGVJZCI6MTIwLCJ0ZWNobm
9sb2d5VHlwZSI6IkFwZXhfVmlzdWFsZm9yY2UiLCJ0ZWNobm9sb2d5VHlwZUlkIjoyMSwidGVja
G5vbG9neVZlcnNpb24iOm51bGwsInRlY2hub2xvZ3lWZXJzaW9uSWQiOm51bGwsImF1ZGl0UHJl
ZmVyZW5jZSI6Ik1hbnVhbCIsImF1ZGl0UHJlZmVyZW5jZUlkIjoxLCJpbmNsdWRlVGhpcmRQYXJ
0eSI6ZmFsc2UsImluY2x1ZGVPcGVuU291cmNlQW5hbHlzaXMiOmZhbHNlLCJzY2FuUHJlZmVyZW
5jZSI6IlN0YW5kYXJkIiwic2NhblByZWZlcmVuY2VJZCI6MSwicG9ydGFsVXJpIjoiaHR0cHM6L
y9mb2RxYTktdGVuYW50LmZvcnRpZnlmb2RxYTkubG9jYWwiLCJhcGlVcmkiOiJodHRwOi8vMTYu
MTAzLjIzNC4yMzcifQ== -ep 1
```

Usage notes:

`java` is the path of the Java executable.

- If `java.exe` is in the directory from which the command is run or if the `java.exe` directory is included in the file system path, simply reference `java` as the path.
- If the `java.exe` is not in the path, the full path is required (for example, `C:\Program Files (x86)\Java\jre-9\bin\java.exe`).

The `-jar` operator informs `java.exe` that it is working with a JAR file for the rest of the command set.

`FoDUpload.jar` is the path of the `FoDUpload.jar` tool.

- If `FodUpload.jar` is in the directory from which the command is being run, simply reference `FoDUpload.jar` as the path.
- If `FodUpload.jar` is in a different directory, the full path is required (for example, `C:\fod_upload\fodupload.jar`).

Scan Preparation and Tracking Tools

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

Static Scanning Tool	Description	More Information
Fortify Static Code Analyzer	Translate-only version of Fortify Static Code Analyzer for translating C/C++ and Scala code and packaging it for scanning **Note:** Fortify Static Code Analyzer requires a valid license file to translate source code.	Fortify Static Code Analyzer and Tools Documentation
Fortify ABAP Extractor	SAP transport request for downloading source code files to the presentation server	"Preparing ABAP (SAP) Application

Static Scanning Tool	Description	More Information
		Files" on page 97
Fortify ScanCentral SAST client	Stand-alone Fortify ScanCentral SAST client for packaging source code	"Installing and Using the Fortify ScanCentral SAST Client" on page 92
Fortify Audit Workbench	Tool for viewing and auditing FPR files	Fortify Static Code Analyzer and Tools Documentation

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

Dynamic Scanning Tool	Description	More Information
Fortify WebInspect Workflow Macro Recorder	Stand-alone utility for creating workflow macros	Fortify WebInspect Documentation
Fortify WebInspect Login Macro Recorder	Stand-alone utility for creating login macros	Fortify WebInspect Documentation
Fortify FoD-SSC Sync	Stand-alone utility for automated, scheduled synchronization of Fortify on Demand applications, releases, and scans with Fortify Software Security Center (SSC)	GitHub
Fortify Bug Tracker	Stand-alone utility for submitting Fortify on Demand issues to bug trackers	GitHub

Tracking tools include:

Tool	Description	More Information
Fortify FoD-SSC Sync	Stand-alone utility for automated, scheduled synchronization of Fortify on Demand applications, releases, and scans with Fortify Software Security Center (SSC)	GitHub
Fortify Bug Tracker	Stand-alone utility for submitting Fortify on Demand issues to bug trackers	GitHub

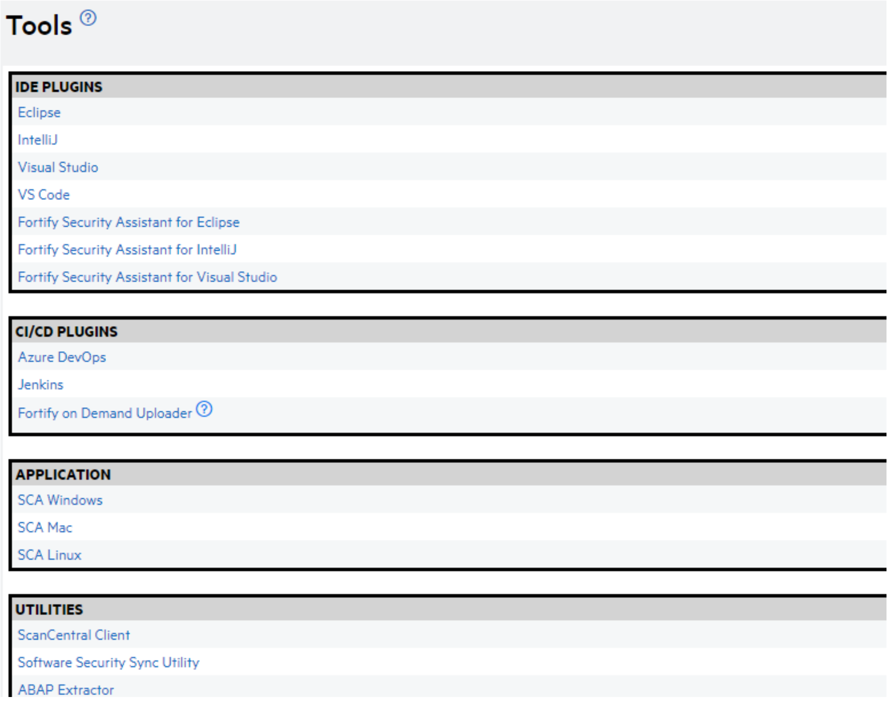
Viewing and Downloading Tools

You can view and download the tools available for use with Fortify on Demand.

To view the available tools:

1. Click your account name and select **Tools** from the list.

   The Tools page appears.



Tools

IDE PLUGINS
- Eclipse
- IntelliJ
- Visual Studio
- VS Code
- Fortify Security Assistant for Eclipse
- Fortify Security Assistant for IntelliJ
- Fortify Security Assistant for Visual Studio

CI/CD PLUGINS
- Azure DevOps
- Jenkins
- Fortify on Demand Uploader

APPLICATION
- SCA Windows
- SCA Mac
- SCA Linux

UTILITIES
- ScanCentral Client
- Software Security Sync Utility
- ABAP Extractor

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

Chapter 9: Portal Integrations

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

This section contains the following topics:

Bug Tracker Integration

For tenants that want to link vulnerability results to their bug tracking tools, Fortify on Demand offers bug tracker integration for the latest versions of the following bug trackers:

- OpenText Application Lifecycle Management (ALM)
- OpenText Application Lifecycle Management Octane (ALM Octane)
- Jira
- Bugzilla
- Azure DevOps/Azure DevOps Server.

Users can submit issues as bugs to a supported bug tracker and manage the bugs directly from the portal. For non-supported bug trackers, users can manually add bug tracker links to issues.

This section contains the following topics:

Configuring Bug Tracker Integration

Bug tracker integration is configured at the application level. You must establish a connection between Fortify on Demand and your bug tracker server (VPN is not an option for establishing the connection). The server will need a dedicated user account for adding and closing bugs.

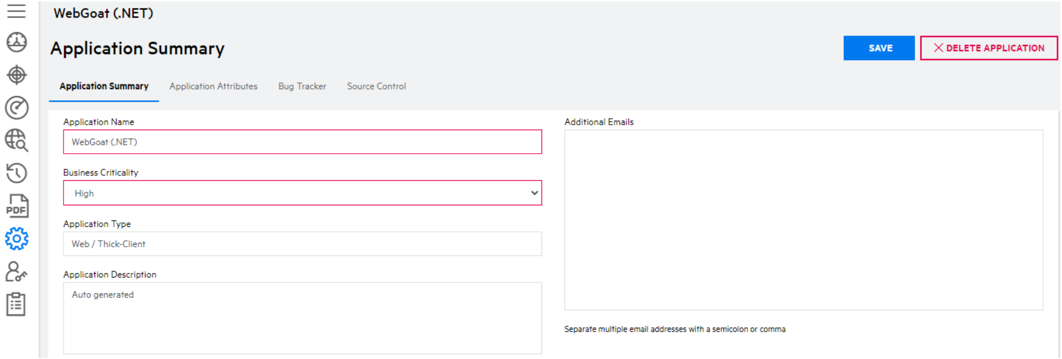
To configure bug tracker integration for an application:

1. Select the **Applications** view.

   Your Applications page displays.
2. Click the application for which you want to configure bug tracker integration.

   The application Overview page appears.
3. Click **Settings**.

   The Settings page appears.



WebGoat (.NET)

Application Summary

Application Name: WebGoat (.NET)

Business Criticality: High

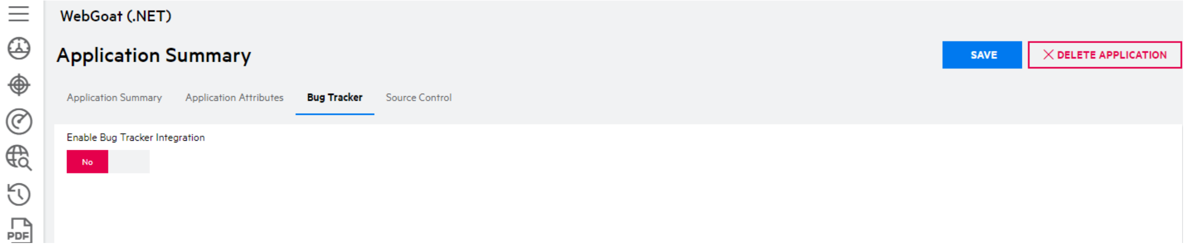
Application Type: Web / Thick-Client

Application Description: Auto generated

Additional Emails

Separate multiple email addresses with a semicolon or comma

4. Select the **Bug Tracker** tab.



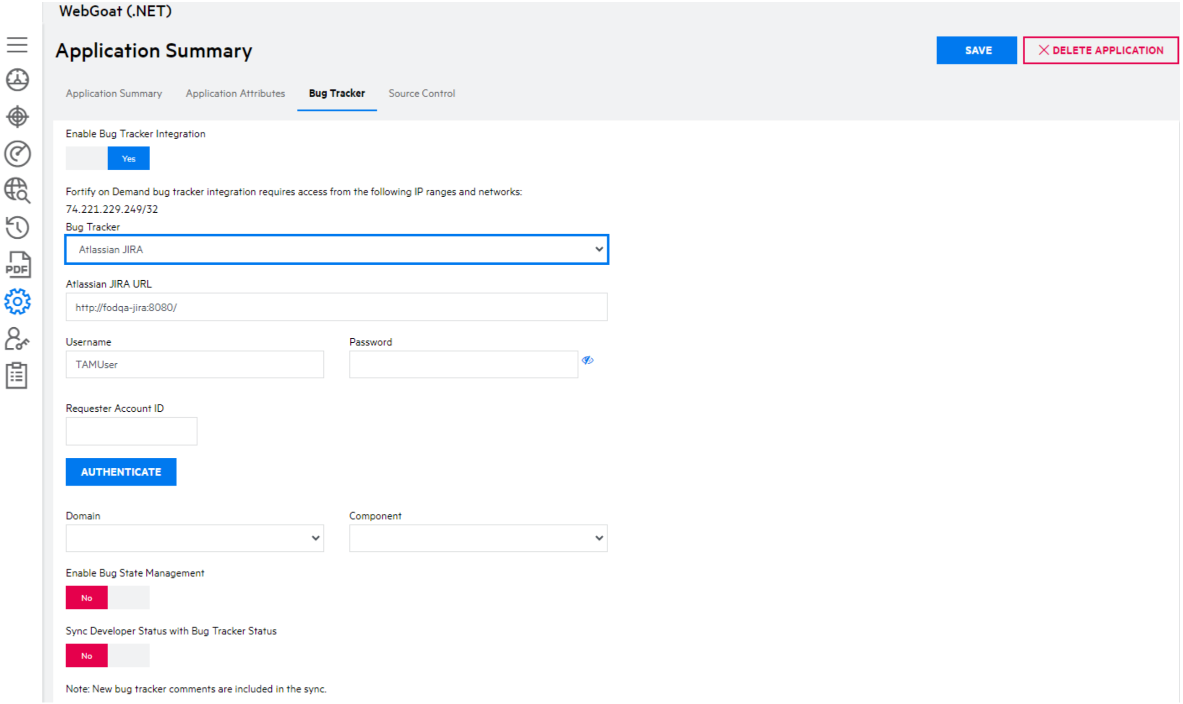
WebGoat (.NET)

Application Summary

Enable Bug Tracker Integration: No

5. Move the **Enable Bug Tracker Integration** slider from **No** to **Yes** to enable bug tracker integration.
6. Select your bug tracker from the **Bug Tracker** list.

   If you selected a supported bug tracker, additional fields appear below. The field names are based on the bug tracker selected.



WebGoat (.NET)

Application Summary

Enable Bug Tracker Integration: Yes

Fortify on Demand bug tracker integration requires access from the following IP ranges and networks:
74.221.229.249/32

Bug Tracker: Atlassian JIRA

Atlassian JIRA URL: http://fodqa-jira:8080/

Username: TAMUser

Password

Requester Account ID

Domain

Component

Enable Bug State Management: No

Sync Developer Status with Bug Tracker Status: No

Note: New bug tracker comments are included in the sync.

7. In the **URL** field, type the URL of your bug tracker site.

8. In the **Username** and **Password** fields, type the login credentials that will be used to log in to the bug tracker site.

   If you have a cloud JIRA instance where the Reporter field is required, in the **Requester Account ID** field, type the user ID associated with the provided **Username**.

   > **Important!** Atlassian 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.

9. Click **Authenticate**.

   An "Authenticated" message appears if the authentication was successful. The list of categories from the bug tracker site is also populated.

   > **Tip:** If you are having trouble authenticating to the bug tracker, see the following troubleshooting tips:
   >
   > - Check that the bug tracker instance is publicly accessible. For example, you can test the accessibility of a Jira instance with the command `curl -D- -u <Jira_userid>:<Jira_password> http://<host>.atlassian.net/rest`
   > - Enable the bug tracker API, if applicable.
   > - Check that the account used to log in to the bug tracker has permission to access the bug tracker API.
   > - Add the Fortify on Demand IP addresses to the allow list in firewalls, IPSs, IDSs, and WAFs. The IP addresses are displayed on the Bug Tracker tab.

10. Select the default category to which application's issues will be submitted. Fields are specific to the selected bug tracker.

    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**

11. Move the **Enable Bug State Management** slider to **Yes** to enable bug state management. When bug state management is enabled, Fortify on Demand will automatically set bugs to the status listed in the following table once the linked issues have been marked as **Fix Validated** or **Suppressed**. A bug that is linked to multiple issues will not be closed unless all issues are **Fix Validated** or **Suppressed**.

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

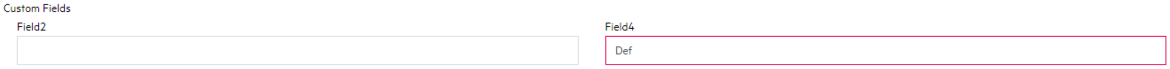
> **Note:** Fortify on Demand does not reopen bugs that are linked to reopened issues.

12. (Available for Azure DevOps and JIRA) When Bug State Management is enabled, move the **Sync Developer Status with Bug Tracker Status** slider to **Yes** to sync the Fortify on Demand **Developer Status** values with the bug tracker status values. Map the bug tracker status values to the **Developer Status** values.

    > **Note:** The **Developer Status** field of a submitted issue can no longer be edited in Fortify on Demand, as the **Developer Status** is automatically synced with the bug tracker status value. New bug tracker comments are included in the sync.

13. (Available for Azure DevOps) Specify default values for custom fields when submitting bugs. If applicable, default values from Azure DevOps are populated. Required custom fields are marked in red.

    To reset field values to Azure DevOps default values, clear the fields.



Custom Fields
Field2
Field4
Def

14. Click **Save**.

    Your bug tracker settings are saved.

Submitting Issues to the Bug Tracker

Once bug tracker integration is configured for an application, a user with Application Access and Edit Issues permissions can submit Fortify on Demand issues as bugs to the bug tracker. The portal prevents issues from being submitted more than once.

To submit issues to the bug tracker:

1. Select the **Applications** view.

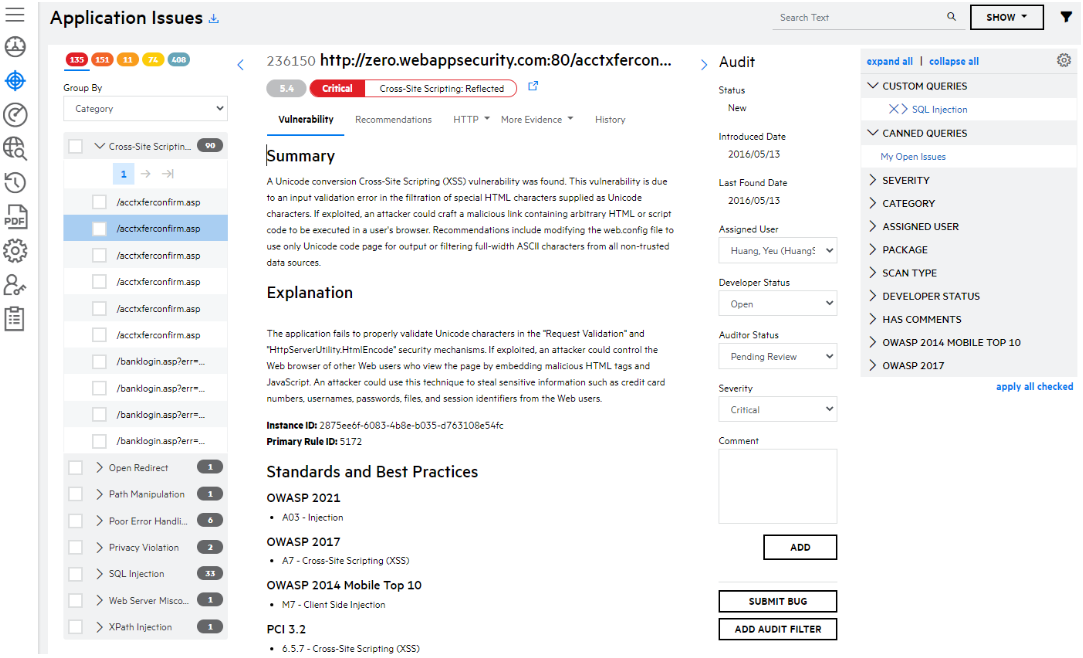
   Your Applications page appears.
2. Click the name of the application with issues that you want to submit to a bug tracker.

   The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page:

- To navigate to the Application Issues page:

  i. Click **Issues**.

  The Application Issues page appears.



236150 http://zero.webappsecurity.com:80/acctxfercon...

Cross-Site Scripting: Reflected

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021
- A03 - Injection

OWASP 2017
- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10
- M7 - Client Side Injection

PCI 3.2
- 6.5.7 - Cross-Site Scripting (XSS)

Audit

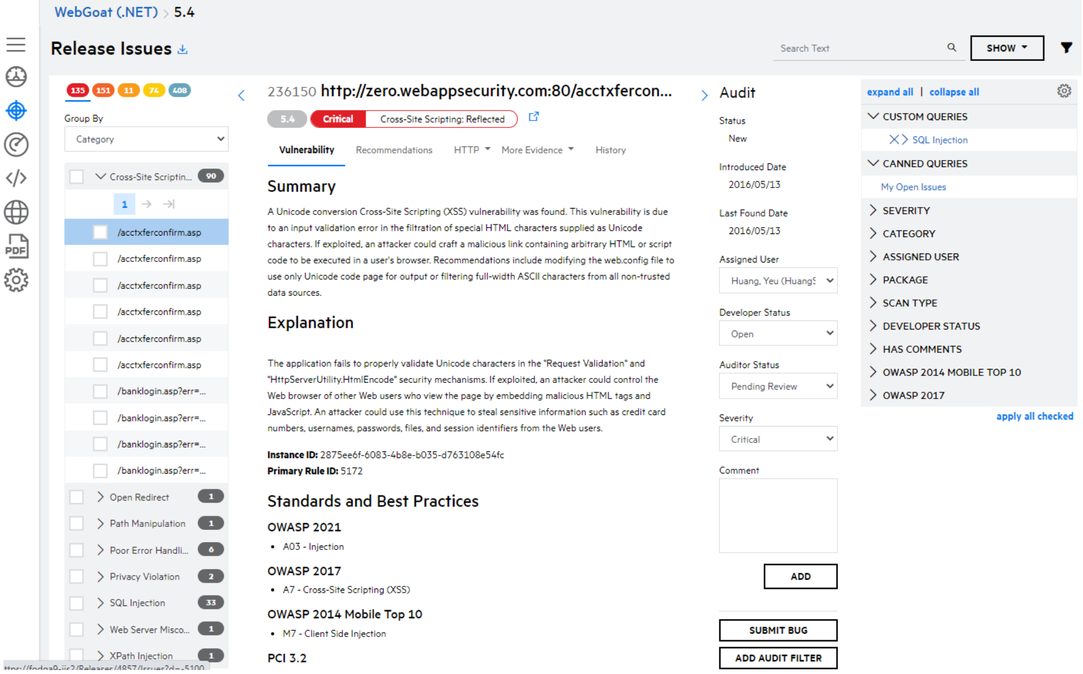
Status: New
Introduced Date: 2016/05/13
Last Found Date: 2016/05/13
Assigned User: Huang, Yeu (HuangS
Developer Status: Open
Auditor Status: Pending Review
Severity: Critical
Comment:

- To navigate to the Release Issues page:

  i. Click the name of a release.

  ii. Click **Issues**.

  The Release Issues page appears.



236150 http://zero.webappsecurity.com:80/acctxfercon...

Cross-Site Scripting: Reflected

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021
- A03 - Injection

OWASP 2017
- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10
- M7 - Client Side Injection

PCI 3.2

Audit

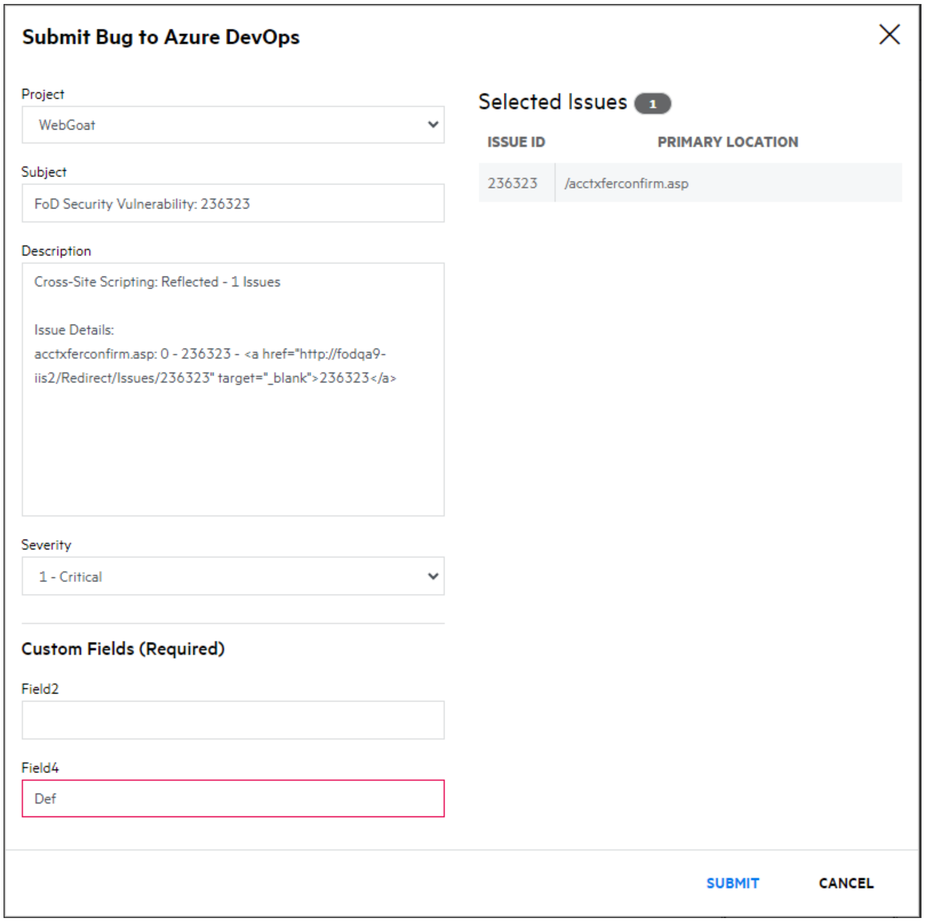
Status: New
Introduced Date: 2016/05/13
Last Found Date: 2016/05/13
Assigned User: Huang, Yeu (HuangS
Developer Status: Open
Auditor Status: Pending Review
Severity: Critical
Comment:

4. In the navigation panel, select one or more issues that you want to submit. To batch submit issues, select the check boxes next to the issues you want to edit.

   > **Note**: If you are on the Application Issues page, selecting the check box next to an issue found in multiple releases selects all instances of the issue.

5. In the audit panel, click **Submit Bug**.

   The Submit Bug to <bug_tracker> window opens. The fields are populated with default values, including issue summaries. You can edit the default values.



Submit Bug to Azure DevOps

Project: WebGoat

Subject: FoD Security Vulnerability: 236323

Description:

Cross-Site Scripting: Reflected - 1 Issues

Issue Details:
acctxferconfirm.asp: 0 - 236323 - <a href="http://fodqa9-iis2/Redirect/Issues/236323" target="_blank">236323</a>

Severity: 1 - Critical

Custom Fields (Required)

Field2:

Field4: Def

Selected Issues 1

ISSUE ID	PRIMARY LOCATION
236323	/acctxferconfirm.asp

6. 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.

7. Click **Submit**.

   You are returned to the Issues page. If the issue submission is pending, the audit panel displays a **Bug Pending** status. Once the issue submission is complete, the audit panel displays a **View Bug** button that links to the issue's bug tracker URL.

> **Note:** When a release is copied, issues in the bug tracker are updated. Links to the newly copied issues are added to the issue descriptions in the bug tracker.

Manually Linking an Issue

You can manually add a bug tracker link to the issue in the portal. This allows tenants using other bug trackers to track external bugs associated with Fortify on Demand issues.

To link a Fortify on Demand issue with an unsupported bug tracker:

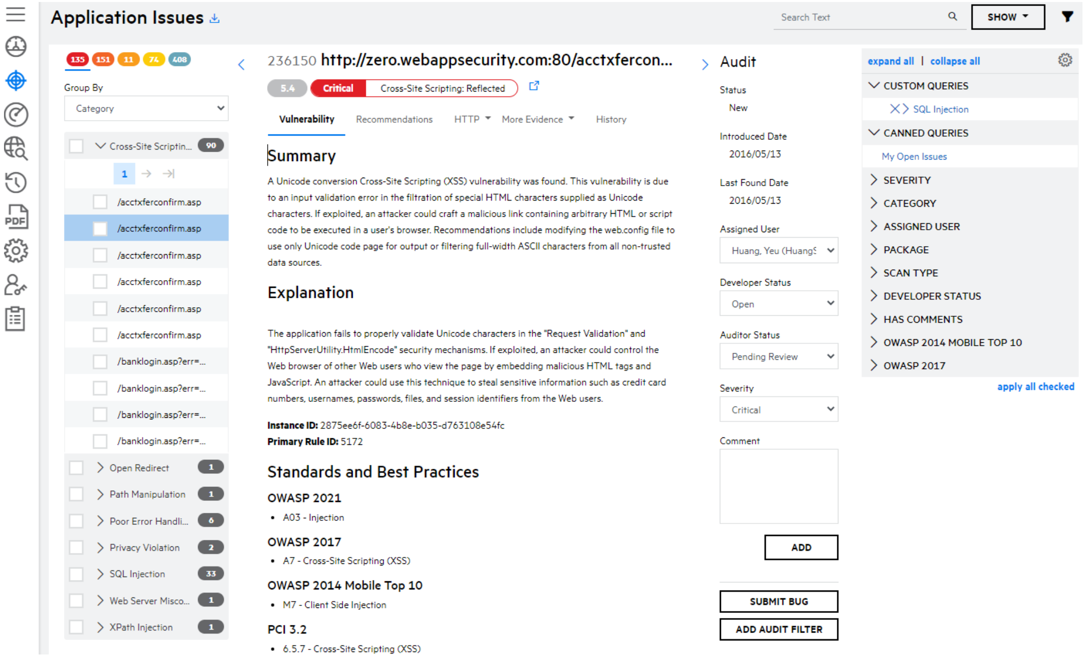
1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of the application with issues that you want to submit to a bug tracker.

   The Application Overview page appears.
3. Navigate to the Application Issues or Release Issues page:
   - To navigate to the Application Issues page:

     i. Click **Issues**.

     The Application Issues page appears.



Application Issues

236150 http://zero.webappsecurity.com:80/acctxfercon...

5.4 Critical Cross-Site Scripting: Reflected

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021
- A03 - Injection

OWASP 2017
- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10
- M7 - Client Side Injection

PCI 3.2
- 6.5.7 - Cross-Site Scripting (XSS)

Audit

Status: New

Introduced Date: 2016/05/13

Last Found Date: 2016/05/13

Assigned User: Huang, Yeu (HuangS

Developer Status: Open

Auditor Status: Pending Review

Severity: Critical

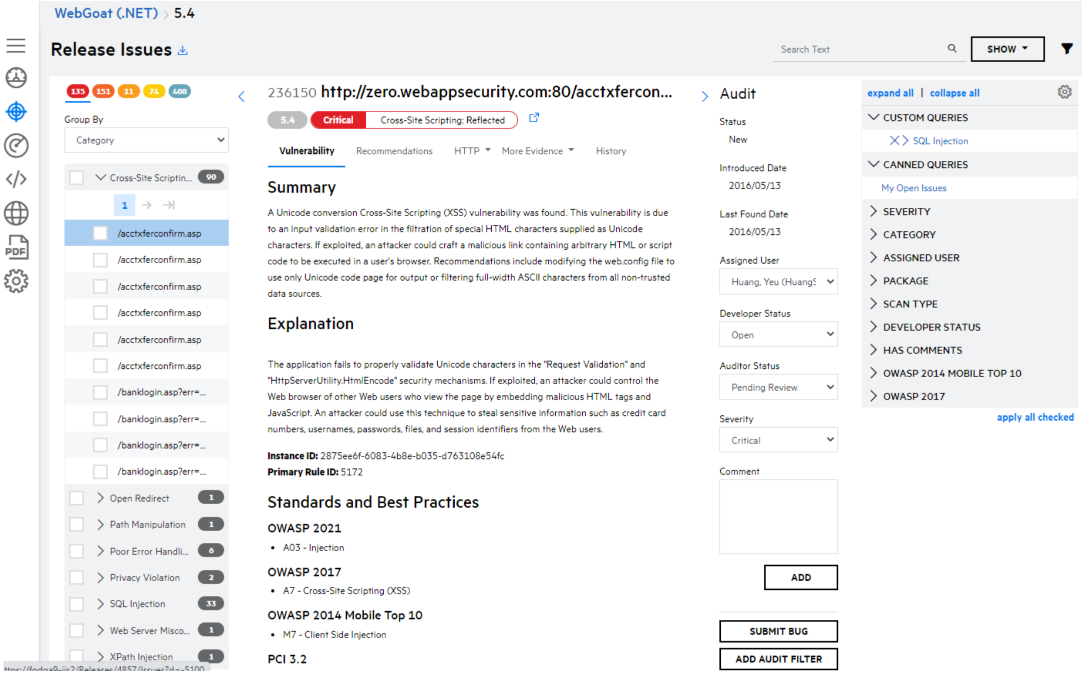
Comment

   - To navigate to the Release Issues page:

     i. Click the name of a release.

     ii. Click **Issues**.

The Release Issues page appears.



236150 http://zero.webappsecurity.com:80/acctxfercon...

Summary

A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include modifying the web.config file to use only Unicode code page for output or filtering full-width ASCII characters from all non-trusted data sources.

Explanation

The application fails to properly validate Unicode characters in the "Request Validation" and "HttpServerUtility.HtmlEncode" security mechanisms. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript. An attacker could use this technique to steal sensitive information such as credit card numbers, usernames, passwords, files, and session identifiers from the Web users.

Instance ID: 2875ee6f-6083-4b8e-b035-d763108e54fc
Primary Rule ID: 5172

Standards and Best Practices

OWASP 2021

- A03 - Injection

OWASP 2017

- A7 - Cross-Site Scripting (XSS)

OWASP 2014 Mobile Top 10

- M7 - Client Side Injection

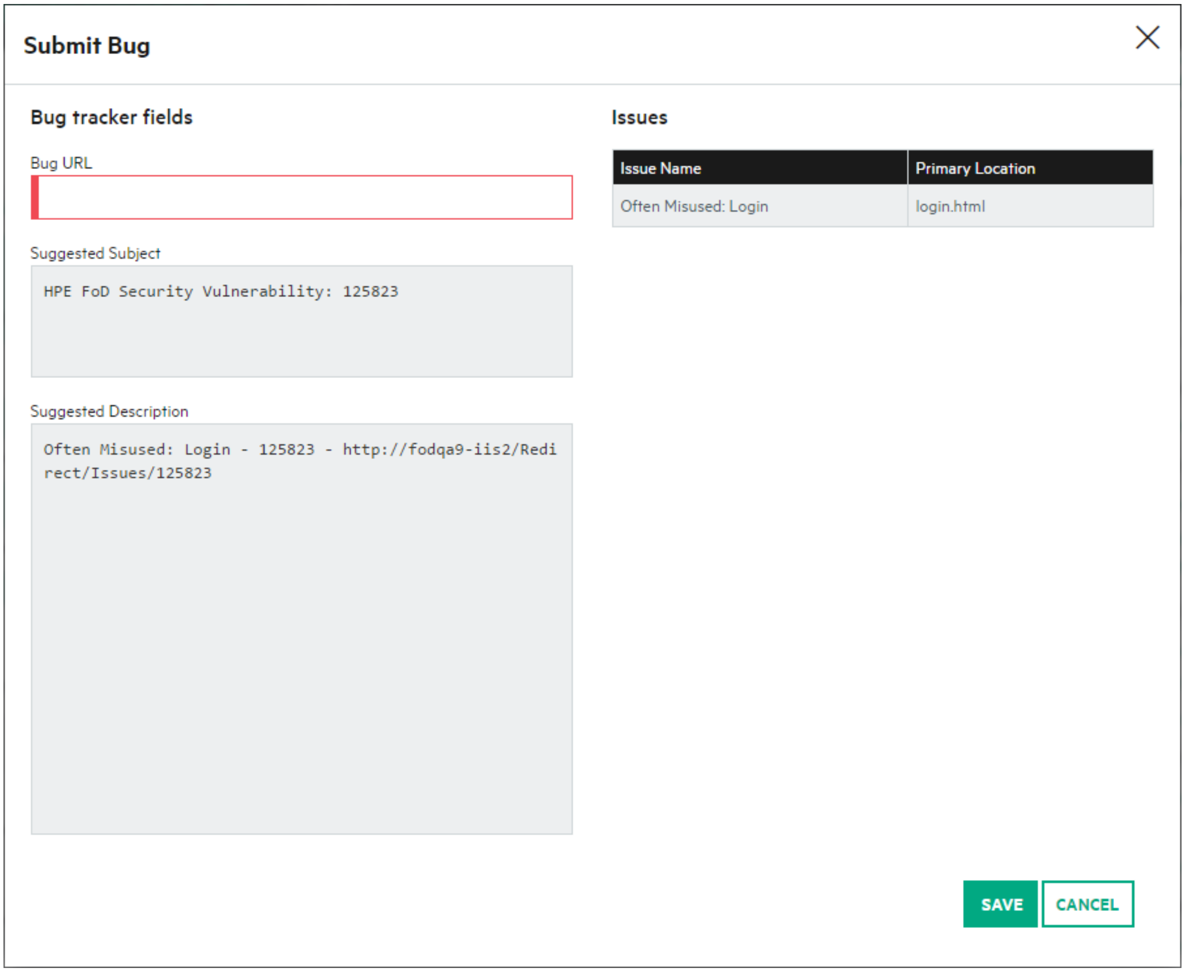
PCI 3.2

Audit

Status: New
Introduced Date: 2016/05/13
Last Found Date: 2016/05/13
Assigned User: Huang, Yeu (HuangS
Developer Status: Open
Auditor Status: Pending Review
Severity: Critical
Comment:

4. In the navigation panel, select one or more issues that you want to submit. To batch submit issues, select the check boxes next to the issues you want to edit.
5. Click **Submit Bug**.

   The Submit Bug modal window appears.



Submit Bug

Bug tracker fields

Bug URL

Suggested Subject

```
HPE FoD Security Vulnerability: 125823
```

Suggested Description

```
Often Misused: Login - 125823 - http://fodqa9-iis2/Redi
rect/Issues/125823
```

Issues

Issue Name	Primary Location
Often Misused: Login	login.html

6. In the **Bug URL** field, type the bug tracker link that you want to add to the issue.
7. Click **Save**.

   Once the issue submission is complete, the audit panel displays a **View Bug** button that links to the issue's bug tracker URL.

External Scan Integration

You can import scan results from external sources into Fortify on Demand to manage scan results from multiple sources in a single view. Fortify on Demand supports import of the following scan types:

- On-premises Fortify Static Code Analyzer and Fortify WebInspect scan results
- Open source scan results that conform to the CycloneDX 1.4 standard

This section contains the following topics:

Importing an On-Premises Scan

You can import on-premises Fortify Static Code Analyzer and Fortify WebInspect scan results into Fortify on Demand. Upon importing an FPR:

- The scan start and complete times use the scan date in the FPR.
- Global and Application Audit Templates are applied.
- The instance ID provided by Fortify Static Code Analyzer or Fortify WebInspect is used to track issues across imported FPRs. Fortify on Demand does not check for duplicate FPRs.

  For example, if you import an FPR into an empty release, all imported issues will have the **New** status. If you import the same FPR again, all issues will change from **New** to **Existing**. If you then import a different FPR, the issue statuses will change as follows:

  - Issues that exist in both the release and the latest FPR will have the **Existing** status.
  - Issues that only exist in the latest FPR will have the **New** status.
  - Issues that exist in the release but do not exist in the latest FPR have the **Fixed** status.
- Suppressed issues in the FPR that are not present in the release are imported and suppressed. Suppression status is ignored for issues in the FPR that are present in the release.

Note: FPRs with a scan date older than the most recently completed scan of the same type are not accepted.

To import a static or dynamic FPR:

1. Select the **Applications** view.

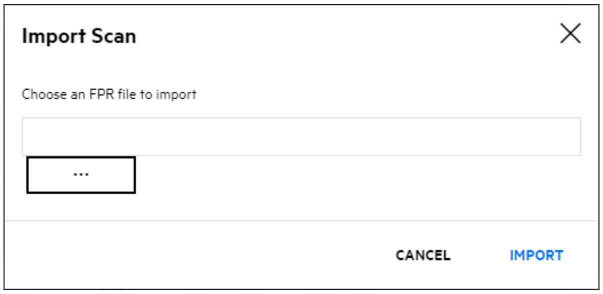
   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears.
3. Click the release for which you want to import an FPR.

   The Release Overview page appears.
4. Click **Scans**.

   The **Release Scans** page appears.
5. Select **Import Scan>Dynamic | Static**.

   The Import Scan window opens.



Import Scan

Choose an FPR file to import

6. Click … and navigate to and select the FPR file.
7. Click **Next**.

   Once the import is complete, the results appear on the Issues page. The scan appears on the Release Scans page with a "Completed" status and "Imported (WebInspect)" or "Imported (SCA)" assessment type.

Importing a Software Bill of Materials

Users with the **Manage Applications** permission can import open source scan results, known as software bill of materials (SBOM), from third parties. An SBOM must meet the following requirements to be imported:

- The SBOM is a JSON file that conforms to the CycloneDX 1.4 standard.
- The SBOM contains a single `tools` entry under the `metadata` object.
- The SBOM version is higher than the version of the most recently imported SBOM.

To import a software bill of materials:

1. Select the **Applications** view.

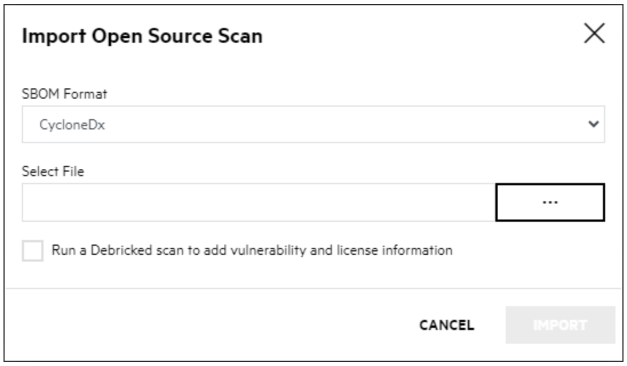
   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears.
3. Click the release for which you want to import an open source scan.

   The Release Overview page appears.
4. Click **Scans**.

   The Release Scans page appears.
5. Select **Import Scan>Open Source**.

   The Import Open Source Scan window opens.

   Import Open Source Scan

   SBOM Format: CycloneDx

   Select File

   □ Run a Debricked scan to add vulnerability and license information

6. Click … and navigate to and select the SBOM.
7. If you want to submit a Debricked scan on the SBOM, select **Run a Debricked scan to add vulnerability and license information**.

> **Note:** If this option is selected, a Debricked entitlement will be redeemed for a Debricked subscription assessment. The Debricked subscription is valid for scans on SBOMs imported under the application.

> **Note:** You can submit a Debricked scan at a later time if needed. On the Scans page, locate the imported SBOM and select **Send to Debricked**.

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 "<toolName> (Imported)" assessment type.

Deleting an Imported Scan

Users with the Manage Applications permission can delete imported scan results files. A scan cannot be deleted if a subsequent scan of the same type has been imported.

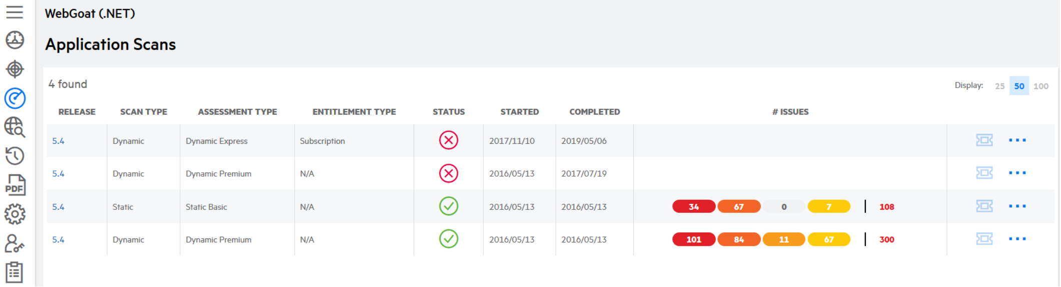
To delete an imported scan:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click the name of the application for which you want to delete the most recent imported scan.

   The Application Releases page appears.
3. Click **Scans**.

   The Application Scans page appears, displaying scans ran against the application.



WebGoat (.NET)

Application Scans

4 found

Display: 25 50 100

RELEASE	SCAN TYPE	ASSESSMENT TYPE	ENTITLEMENT TYPE	STATUS	STARTED	COMPLETED	# ISSUES		
5.4	Dynamic	Dynamic Express	Subscription	⊗	2017/11/10	2019/05/06			⋯
5.4	Dynamic	Dynamic Premium	N/A	⊗	2016/05/13	2017/07/19			⋯
5.4	Static	Static Basic	N/A	✓	2016/05/13	2016/05/13	34 67 0 7 | 108		⋯
5.4	Dynamic	Dynamic Premium	N/A	✓	2016/05/13	2016/05/13	101 84 11 67 | 300		⋯

> **Note**: You can filter the scan list to only view scans ran against a release by clicking the name of the release from the Application Releases page.

4. Click **Cancel Imported Scan** in the action column of the imported scan.

   A confirmation message displays.
5. Click **Yes** to confirm the scan cancellation.

   The scan is deleted, along with all issues associated with the scan.

Secure Code Warrior Integration

Fortify on Demand has partnered with Secure Code Warrior to provide free interactive training for supported vulnerability categories to Fortify on Demand customers. When viewing an issue, users can launch a training module from the **Launch Training** link in the **Recommendations** tab of the Issue Details panel.

A module consists of short, hands-on challenges in which users analyze software design and code for the vulnerability and then remediate or mitigate the vulnerability. Sample modules are available in all vulnerability categories supported by Secure Code Warrior. Modules are hierarchically organized by category, subcategory, and language.

Fortify on Demand does not share user and organization information with Secure Code Warrior. Additional training is available for purchase from Secure Code Warrior. For more information, see https://www.securecodewarrior.com/.

Launching Secure Code Warrior Training

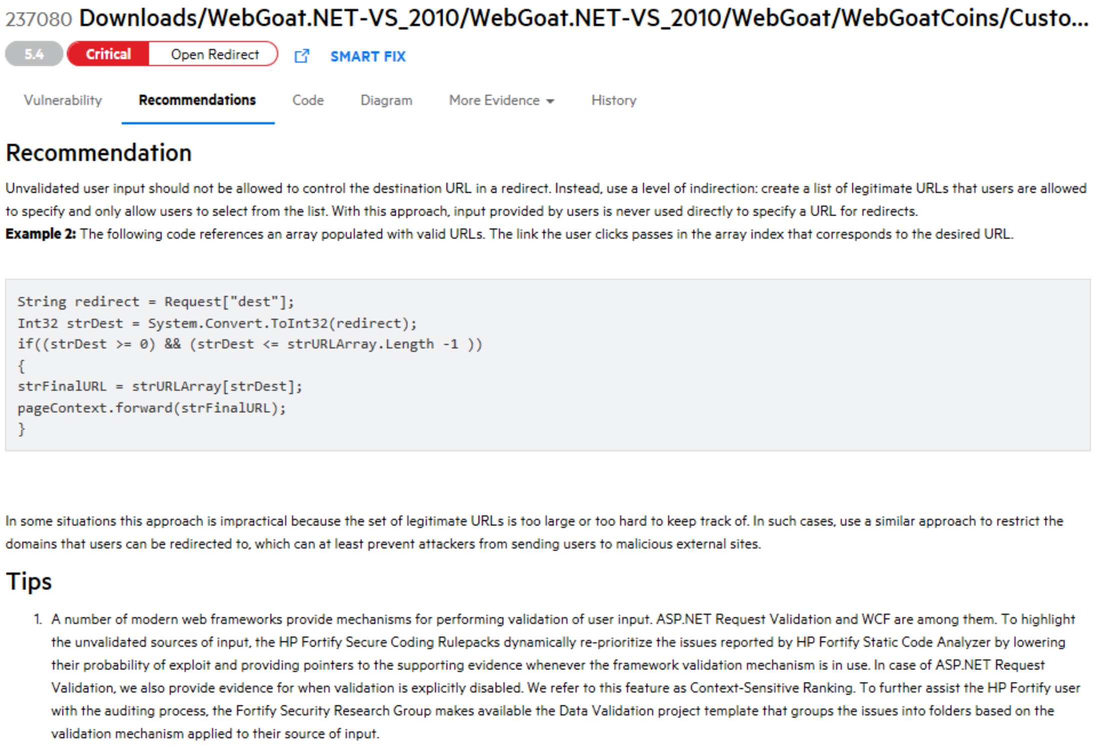
To launch Secure Code Warrior training for an issue:

1. Select the **Applications** view.

   Your Applications page appears.
2. Click **Your Releases**.

   Your Releases page appears.
3. Select a release from your list.
4. Click **Issues**.

   The Release Issues page appears.
5. In the navigation panel, select an issue in an issue category where Secure Code Warrior training is available.
6. Select the **Recommendations** tab.



Recommendation

Unvalidated user input should not be allowed to control the destination URL in a redirect. Instead, use a level of indirection: create a list of legitimate URLs that users are allowed to specify and only allow users to select from the list. With this approach, input provided by users is never used directly to specify a URL for redirects.

Example 2: The following code references an array populated with valid URLs. The link the user clicks passes in the array index that corresponds to the desired URL.

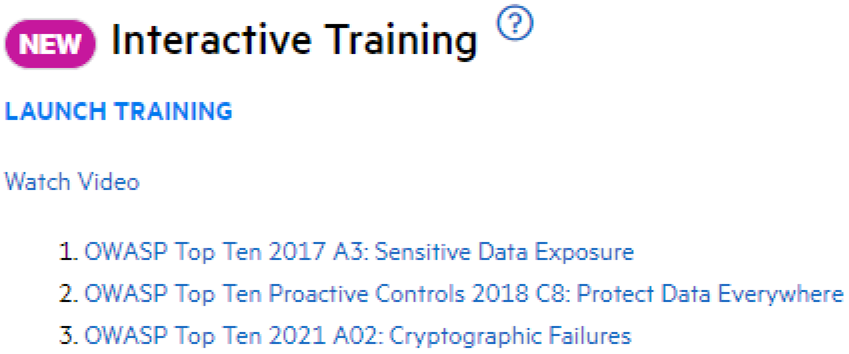
```
String redirect = Request["dest"];
Int32 strDest = System.Convert.ToInt32(redirect);
if((strDest >= 0) && (strDest <= strURLArray.Length -1 ))
{
strFinalURL = strURLArray[strDest];
pageContext.forward(strFinalURL);
}
```

In some situations this approach is impractical because the set of legitimate URLs is too large or too hard to keep track of. In such cases, use a similar approach to restrict the domains that users can be redirected to, which can at least prevent attackers from sending users to malicious external sites.

Tips

1. A number of modern web frameworks provide mechanisms for performing validation of user input. ASP.NET Request Validation and WCF are among them. To highlight the unvalidated sources of input, the HP Fortify Secure Coding Rulepacks dynamically re-prioritize the issues reported by HP Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. In case of ASP.NET Request Validation, we also provide evidence for when validation is explicitly disabled. We refer to this feature as Context-Sensitive Ranking. To further assist the HP Fortify user with the auditing process, the Fortify Security Research Group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

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.



1. OWASP Top Ten 2017 A3: Sensitive Data Exposure
2. OWASP Top Ten Proactive Controls 2018 C8: Protect Data Everywhere
3. OWASP Top Ten 2021 A02: Cryptographic Failures

> **Note:** If the issue does not belong to a supported vulnerability category, you are redirected to the Secure Code Warrior home page.

Slack Integration for Notifications

Fortify on Demand offers Slack integration for posting notifications to Slack. Security Leads can configure one or more webhooks for the tenant. Once webhooks have been configured, Security Leads can enable posting notifications to Slack when creating notification subscriptions.

This section contain the following topics:

Configuring Slack Integration

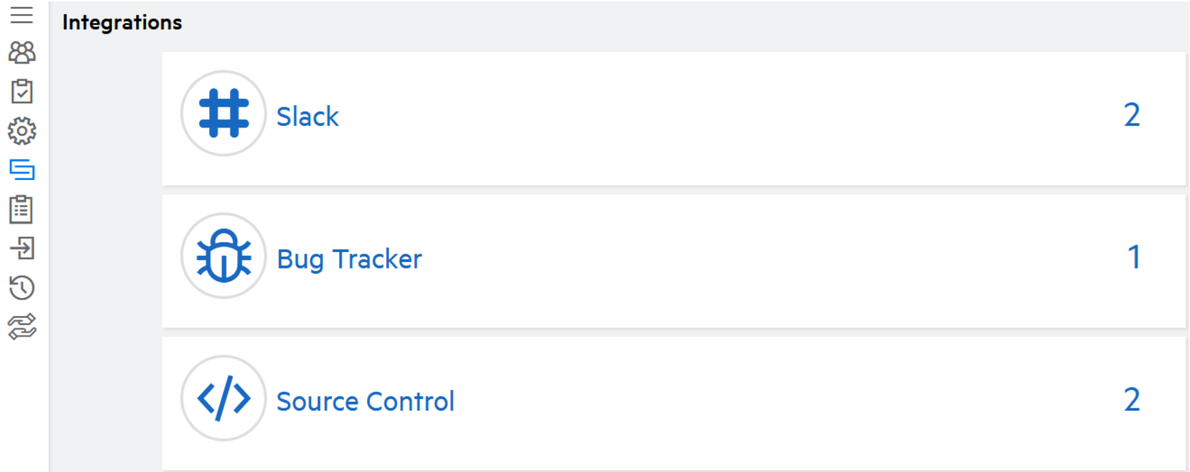
You can configure Slack integration by configuring one or more webhooks for the tenant.

To configure a webhook:

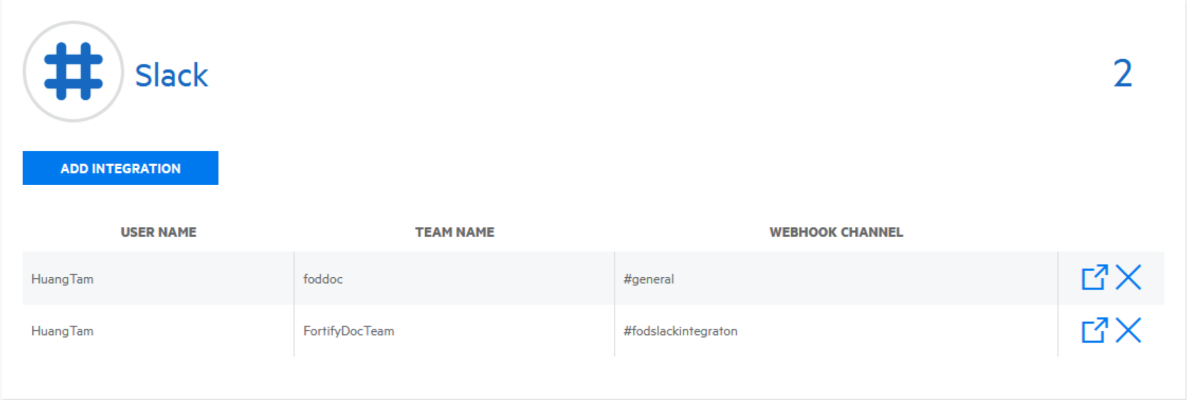
1. Select the **Administration** view.

   The **User Management** page appears.
2. Click **Integrations**.

   The **Integrations** page appears.



3. Expand the **Slack** section.



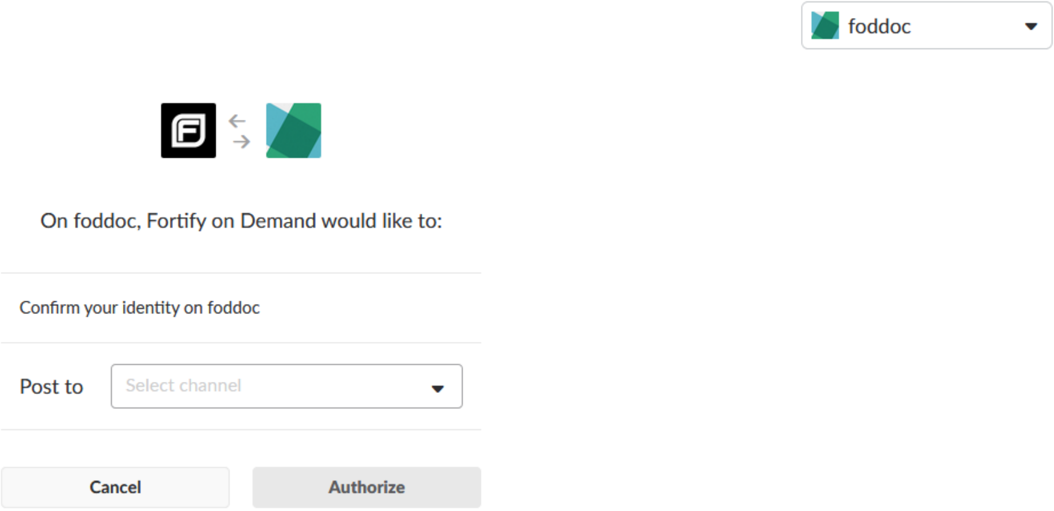
USER NAME	TEAM NAME	WEBHOOK CHANNEL
HuangTam	foddoc	#general
HuangTam	FortifyDocTeam	#fodslackintegraton

4. Click **Add Integration**.
   - If you are currently not signed in to a workspace, you are redirected to the Slack workspace sign in page.

- If you are currently signed in to one or more workspaces, you are redirected to the authorization page.

> **Note:** You must have permission to manage apps and integrations for the workspace

5. If you are not signed in to the workspace to which you want to connect, complete the sign-in process. Otherwise, skip to the next step.
6. Select the workspace, if not already selected, from the list on the top right side of the authorization page.



On foddoc, Fortify on Demand would like to:

Confirm your identity on foddoc

7. Select the channel or user direct message to which notifications will be posted. The available values are the channels and user accounts to which you have access.
8. Click **Authorize** to authorize Fortify on Demand to access your Slack account.

   You are redirected to Fortify on Demand. A "Slack Integration Successful" message appears. You can now enable posting notiifcations to the channel. For more information on enabling posting notifications to Slack, see "Creating an Individual Subscription" on page 31 and "Creating a Global Subscription" on page 33.

   .

Deleting Slack Integration

You can delete a Fortify on Demand Slack integration in the following ways:

- Slack workspace owners and users who have permission to manage apps can remove specific authorizations or remove the Fortify on Demand application from the Slack workspace. This will cause posts to Slack to fail.
- Security Leads can delete webhooks in Fortify on Demand.

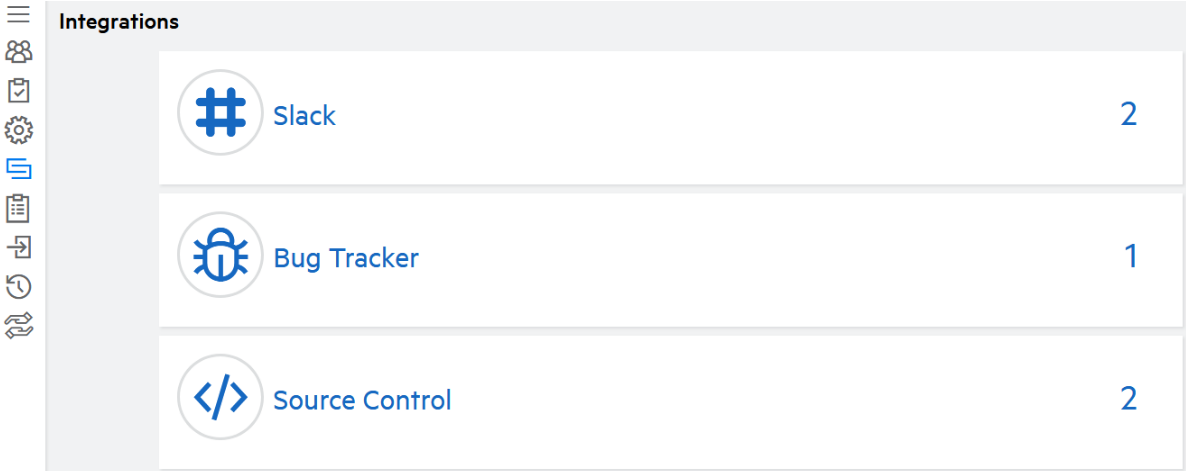
To delete a Slack integration:

1. Select the **Administration** view.

   The **User Management** page appears.

2. Click **Integrations**.

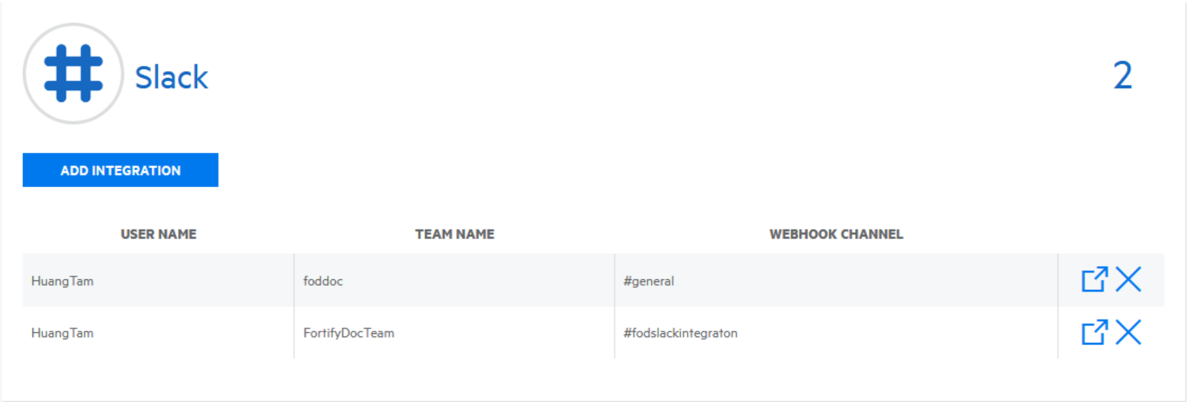
   The **Integrations** page appears.



Integrations

Slack	2
Bug Tracker	1
Source Control	2

3. Expand the **Slack** section.



Slack 2

ADD INTEGRATION

USER NAME	TEAM NAME	WEBHOOK CHANNEL	
HuangTam	foddoc	#general	↗ ×
HuangTam	FortifyDocTeam	#fodslackintegraton	↗ ×

4. Perform the following tasks depending on your preferences and user permissions:

   - To remove authorizations in Slack:

     i. Click ↗ in the row of the webhook.

        You are redirected to the Fortify on Demand page in your workspace app directory.

        > **Note:** You can also access the page from the Slack workspace.

     ii. Remove specific authorizations or remove the application to remove all authorizations. For more information about removing applications from Slack, see the Remove apps and custom integrations from your workspace section of the Slack documentation.

   - To remove a webhook in Fortify on Demand:

     i. Click × in the row of the webhook.

        The webhook is deleted.

Source Control Integration

Important! Source control integration through the portal is a legacy integration. Usage of this integration is not recommended as it 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" on page 330.

Fortify on Demand offers source control integration through the portal for GitHub and Bitbucket. This enables Fortify on Demand to pull source code from repositories on those platforms for static assessments.

The following languages are supported: Java, JavaScript, .NET, PHP, and Python. The requirements for preparing your code for upload to Fortify on Demand remain the same as described in "Preparing Static Assessment Files" on page 91. For .NET and Java, Fortify recommends pre-compiling your files and uploading them to a release to ensure acceptance of the payload.

Source control integration is configured at the application level. Once it is configured, users can select a branch or release to upload when starting a static assessment.

This section contain the following topics:

Configuring Source Control Integration with Bitbucket

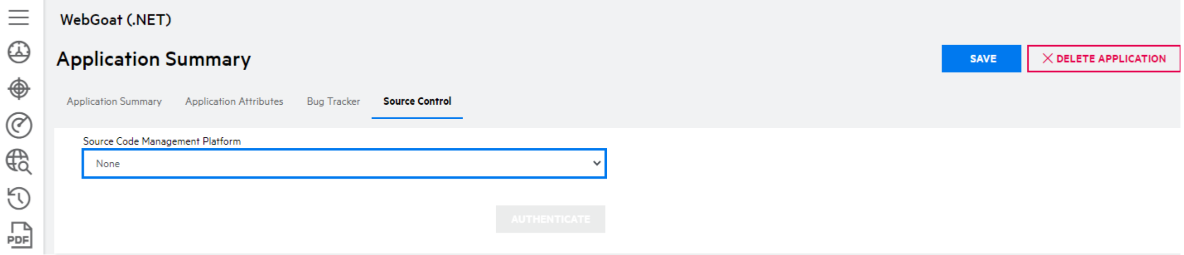
The Bitbucket integration requires the addition of an OAuth consumer in Bitbucket.

To configure source control integration with Bitbucket:

1. Select the **Applications** view.

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

   The Application Summary page appears.
4. Select the **Source Control** tab.



Source Code Management Platform: None

5. Select **Bitbucket** from the **Source Code Management Platform** list.

6. In the **Client Key** and **Client Secret** fields, type the OAuth consumer key and secret as generated in Bitbucket.

   To generate the key and secret, add an OAuth consumer in Bitbucket. When configuring the consumer, make sure to do the following:

   - Set the callback URL to `https://<fod_domain>/Redirect/OAuth/`, where `<fod_domain>` is the Fortify on Demand domain and scheme.
     - US: `ams.fortify.com`
     - EMEA: `emea.fortify.com`
     - APAC: `apac.fortify.com`
     - FedRAMP: `fed.fortifygov.com`
   - Assign read permission to the account, workspace membership, projects, and repositories.

   For more information on adding an OAuth consumer in Bitbucket, see the Integrate another application through OAuth section of the Bitbucket documentation.

   > **Tip:** Make sure that the **This is a private consumer** check box is selected in your workspace OAuth consumer settings.

7. Click **Authenticate**.

   If the authentication was successful, you are redirected to the Bitbucket site.

8. Authorize the Fortify on Demand application to access your account.

   The **Team** and **Repository** fields are populated. The **Team** field lists your user account and all teams whose repositories you have access to.

9. Select the team that owns the repository that will be linked to the application from the **Team** list.
10. Select the repository from the **Repository** list.
11. Click **Save**.

    Your source control integration settings are saved.

Configuring Source Control Integration with GitHub

The GitHub integration uses the Fortify on Demand Github marketplace application, which is unique to each data center. Source control integration with GitHub Enterprise is not available.

To configure source control integration with GitHub:

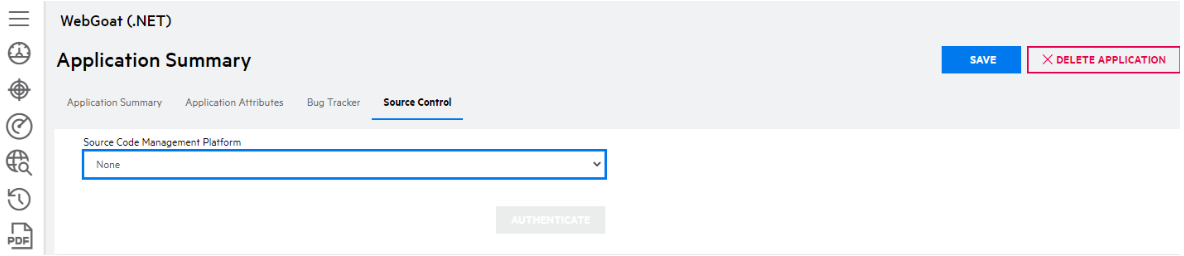
1. Select the **Applications** view.

   Your Applications page appears.

2. Click the name of the application that you want to edit.
3. Click **Settings.**

   The Application Summary page appears.

4. Select the **Source Control** tab.



Source Code Management Platform: None

5. Select **Github** from the **Source Code Management Platform** list.
6. Click **Authenticate**.

   If the authentication was successful, you are redirected to the GitHub site.
7. Authorize the Fortify on Demand application to access your account.

   The **Organization** and **Repository** fields are populated. The **Organization** field lists your user account and all organizations whose repositories you have access to.
8. Select the organization that owns the repository that will be linked to the application from the **Organization** list.
9. Select the repository from the **Repository** list.
10. Click **Save**.

    Your source control integration settings are saved.

Tracking Configured Integrations

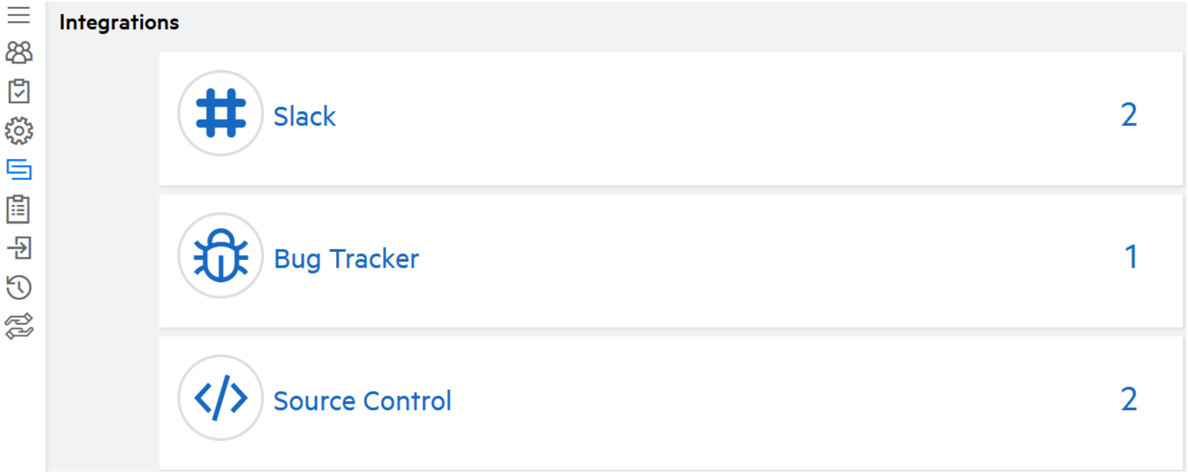
Security Leads can track user-configured integrations with external tools across all applications in Fortify on Demand. Currently, the integrations available for tracking are: bug tracker, source control, and Slack.

To track user-configured integrations across the tenant:

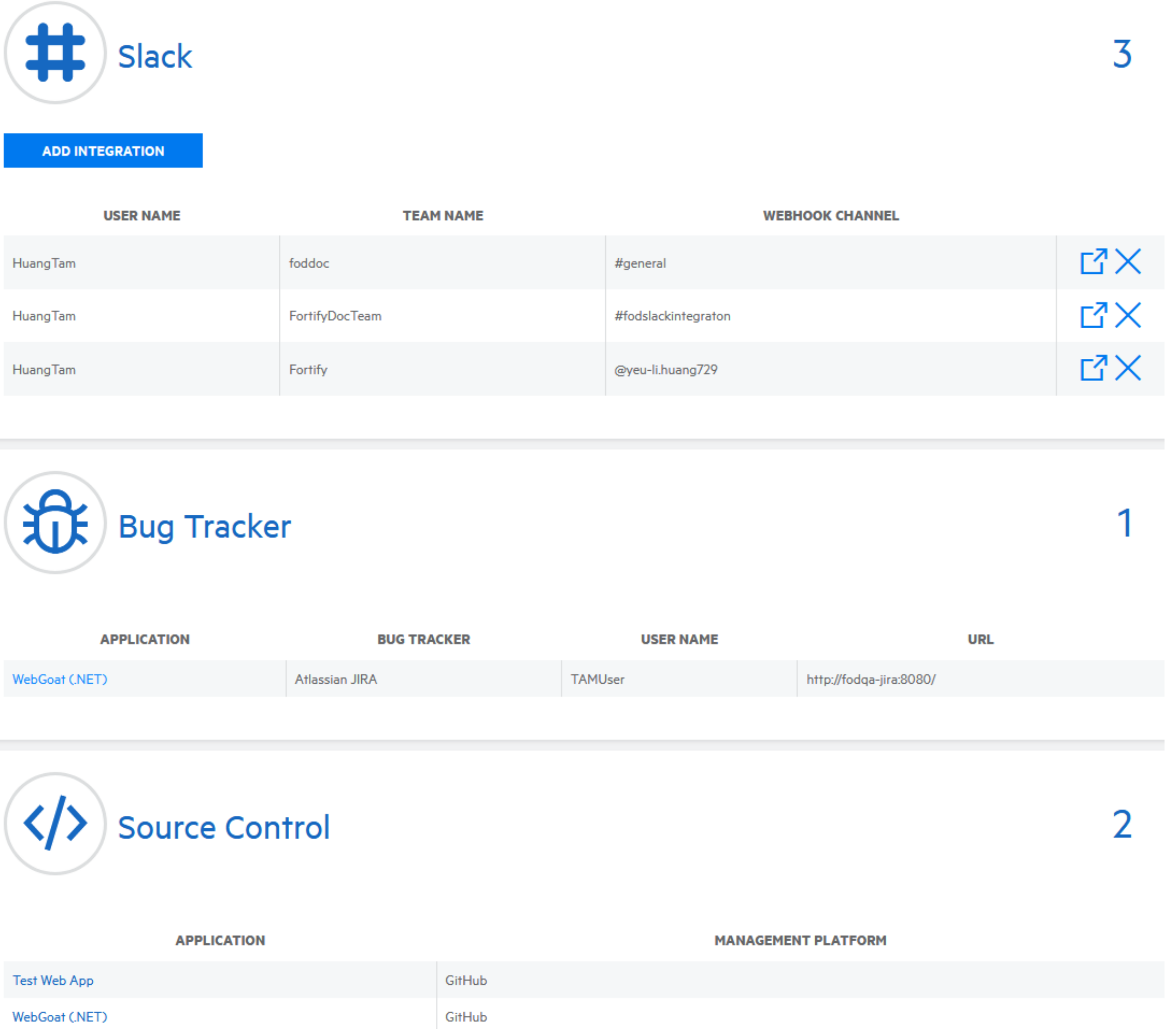
1. Select the **Administration** view.

   The **User Management** page appears.
2. Click **Integrations**.

   The **Integrations** page appears.



3. Expand the sections that you want to view.



USER NAME	TEAM NAME	WEBHOOK CHANNEL	
HuangTam	foddoc	#general	
HuangTam	FortifyDocTeam	#fodslackintegraton	
HuangTam	Fortify	@yeu-li.huang729	

APPLICATION	BUG TRACKER	USER NAME	URL
WebGoat (.NET)	Atlassian JIRA	TAMUser	http://fodqa-jira:8080/

APPLICATION	MANAGEMENT PLATFORM
Test Web App	GitHub
WebGoat (.NET)	GitHub

4. You can perform the following actions:

- Slack: Click the links in the row of a webhook to remove specific authorizations or delete the webhook. For more information, see "Deleting Slack Integration" on page 356.
- Bug Tracker: Click the link in an application row to be redirected to the application's bug tracker settings. For more information, see "Bug Tracker Integration" on page 341.
- Source Control: Click the link in an application row to be redirected to the application's source control settings. For more information, see "Source Control Integration" on page 358

Webhooks

Webhooks provide a way for notifications to be delivered to an external web server when scans are updated in Fortify on Demand. Users with the **Configure Webhooks** permission can configure webhooks to trigger when a subscribed event occurs. The following events are available: scan start, scan pause, scan resumption, scan cancellation, and scan completion. When an event to which a webhook is subscribed occurs, Fortify on Demand sends an HTTP POST payload to the webhook's configured URL. Webhooks can be used in place of polling in CICD pipelines that incorporate scanning.

This section contain the following topics:

Configuring a Webhook

Users with the **Configure Webhooks** permission can configure webhooks for the tenant. A webhook must be assigned to a minimmum of one release.

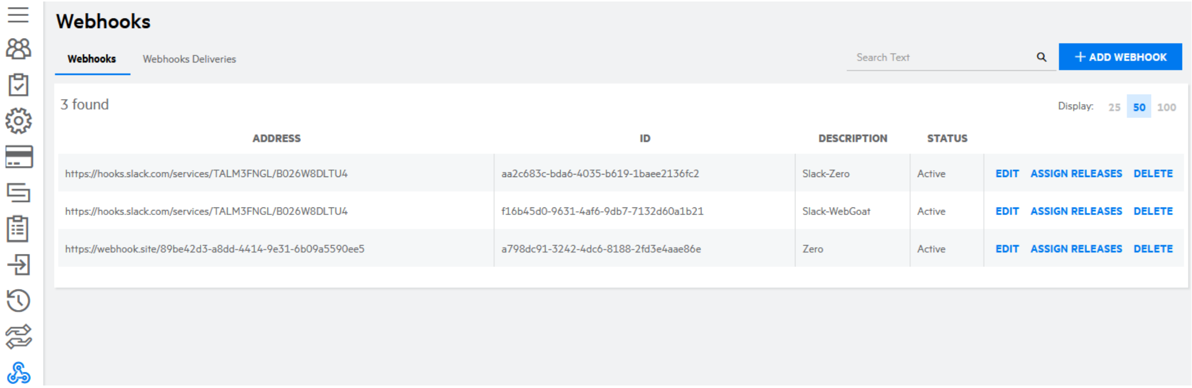
To configure a webhook:

1. Select the **Administration** view.

   The User Management page appears.

2. Click **Webhooks**.

   The Webhooks page appears.

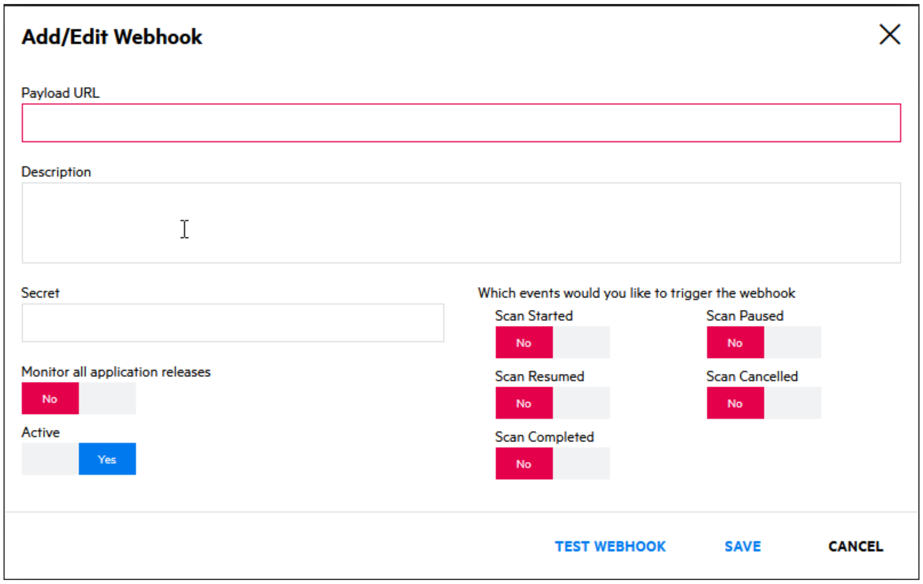


3 found

ADDRESS	ID	DESCRIPTION	STATUS	
https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	aa2c683c-bda6-4035-b619-1baee2136fc2	Slack-Zero	Active	EDIT ASSIGN RELEASES DELETE
https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	f16b45d0-9631-4af6-9db7-7132d60a1b21	Slack-WebGoat	Active	EDIT ASSIGN RELEASES DELETE
https://webhook.site/89be42d3-a8dd-4414-9e31-6b09a5590ee5	a798dc91-3242-4dc6-8188-2fd3e4aae86e	Zero	Active	EDIT ASSIGN RELEASES DELETE

3. Click **Add Webhooks**.

   The Add/Edit Webhooks window appears.



Add/Edit Webhook

Payload URL

Description

Secret

Monitor all application releases: No

Active: Yes

Which events would you like to trigger the webhook

Scan Started: No

Scan Paused: No

Scan Resumed: No

Scan Cancelled: No

Scan Completed: No

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

Field	**Description**
Payload URL	Type the URL of the server that will receive the webhook POST requests. For example, `https://7e9ea9dc.ngrok.io/payload`.
Description	(Optional) Type a phrase that describes the webhook.
Secret	(Optional) Type a secret that can be used to validate that webhook requests sent to the payload URL are from Fortify on Demand. The HMAC-SHA256 algorithm is used in combination with the secret to calculate a hash of the payload body. The output is the HMAC and is included in the header of a request as `X-FOD-Signature`. **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.

Field	Description
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 will trigger the webhook.
6. Click **Test Webhook** to ping the payload URL.

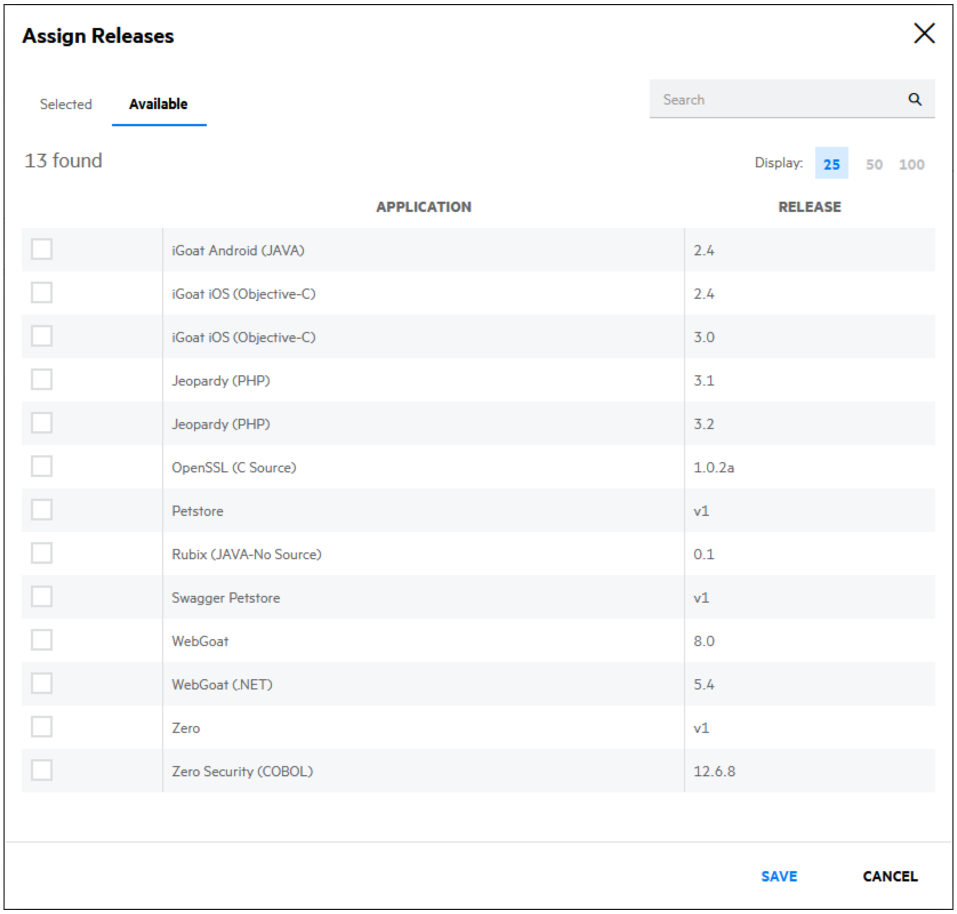
   A "Successfully sent a ping event" message appears if the webhook was configured correctly.
7. Click **Save**.

   The new webhook appears in the list of webhooks.

   > **Note:** You can search webhooks by address, description and full ID. Partial string match is supported for address and description.

8. If you chose to monitor individual releases, clck **Edit** in the row of the webhook.

   The Assign Releases window appears.



13 found

	APPLICATION	RELEASE
□	iGoat Android (JAVA)	2.4
□	iGoat iOS (Objective-C)	2.4
□	iGoat iOS (Objective-C)	3.0
□	Jeopardy (PHP)	3.1
□	Jeopardy (PHP)	3.2
□	OpenSSL (C Source)	1.0.2a
□	Petstore	v1
□	Rubix (JAVA-No Source)	0.1
□	Swagger Petstore	v1
□	WebGoat	8.0
□	WebGoat (.NET)	5.4
□	Zero	v1
□	Zero Security (COBOL)	12.6.8

9. Select the releases that the webhook will monitor and click **Save**.

   The webhook is now assigned to the selected releases.

Webhook Requests and Responses

Fortify on Demand sends information about webhook events as HTTP POST requests with the JSON payload as the body of the request.

> **Note:** SSL verification is enabled by default. If the payload Url is HTTPS, Fortify on Demand will verify SSL certificates when sending webhook requests.

Request Example

The following example shows a request with a hash signature in the header as `X-FOD-Signature` and the JSON payload.

Header:

```
connection: close
expect: 100-continue
content-length: 324
host: webhook.site
content-type: application/json; charset=utf-8
x-fod-signature:
4F837B0AE04303E975BBCF9FFBBC09E0016013835757BD611C20F7930711980F
x-fod-deliveryid: f8d97b5e-4cae-414b-aa84-8de766f8116f
```

Payload:

```
{
  "deliveryId": "f8d97b5e-4cae-414b-aa84-8de766f8116f",
  "eventName": "scan_started",
  "payload": {
    "scanId": 31278,
    "tenantId": 1126,
    "applicationId": 14155,
    "applicationName": "Zero",
    "releaseId": 16149,
    "releaseName": "v1",
    "scanType": "dynamic"
  },
  "webhookId": "a798dc91-3242-4dc6-8188-2fd3e4aae86e",
  "triggeredAt": "2021-07-02T16:08:28.5496187Z"
}
```

Response Example:

The following example shows the response received by Fortify on Demand.

```
Transfer-Encoding = chunked
Vary = Accept-Encoding
X-Request-Id = e9cbce0c-108f-46e9-b2cc-89f6f0104dca
X-Token-Id = 89be42d3-a8dd-4414-9e31-6b09a5590ee5
Cache-Control = no-cache, private
Date = Fri, 02 Jul 2021 16:08:29 GMT
Set-Cookie = laravel_session=CRuQJLoiFx9ay1UV88ufH83vCOjq1PL0JNOwY59v;
expires=Fri, 02-Jul-2021 18:08:29 GMT; Max-Age=7200; path=/; httponly
Server = nginx/1.14.2
```

Viewing Webhook Deliveries

Users with the **Configure Webhooks** permission can view details of the webhook deliveries, including the HTTP request (including the payload) and the response.

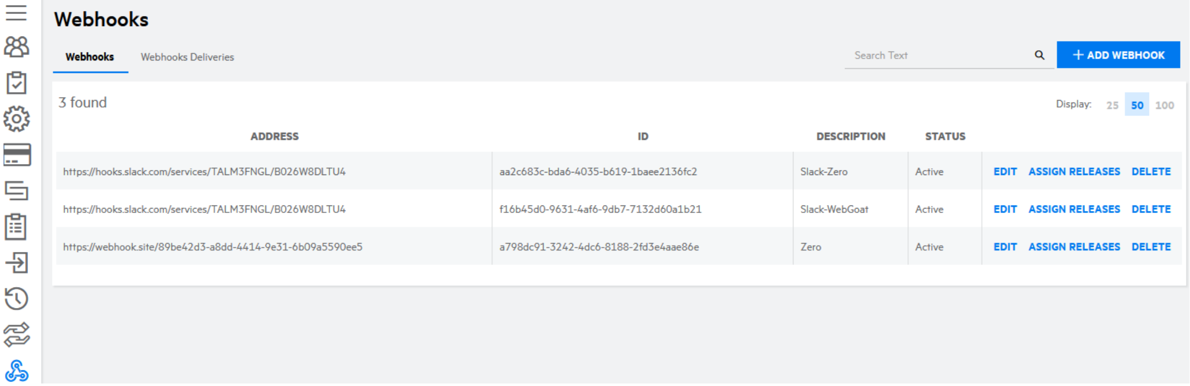
To view the list of webhook deliveries:

1. Select the **Administration** view.

   The User Management page appears.

2. Click **Webhooks**.

   The Webhooks page appears.

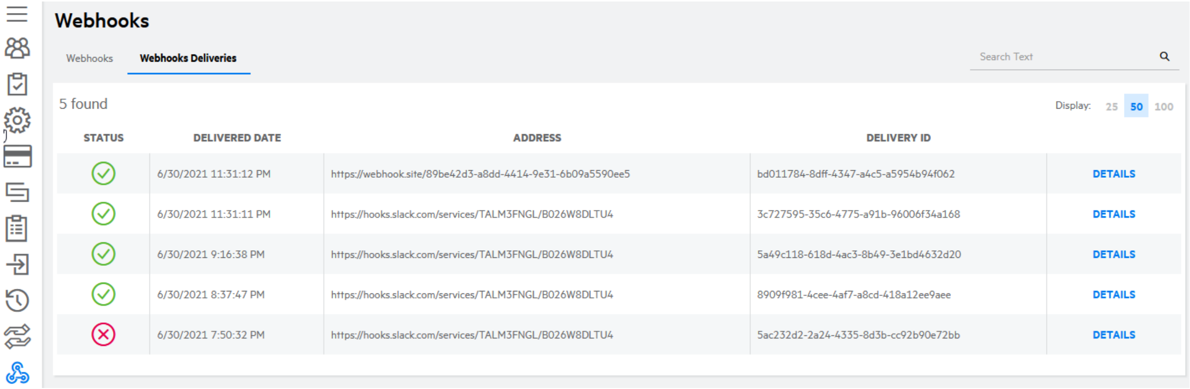


3 found

ADDRESS	ID	DESCRIPTION	STATUS	
https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	aa2c683c-bda6-4035-b619-1baee2136fc2	Slack-Zero	Active	EDIT ASSIGN RELEASES DELETE
https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	f16b45d0-9631-4af6-9db7-7132d60a1b21	Slack-WebGoat	Active	EDIT ASSIGN RELEASES DELETE
https://webhook.site/89be42d3-a8dd-4414-9e31-6b09a5590ee5	a798dc91-3242-4dc6-8188-2fd3e4aae86e	Zero	Active	EDIT ASSIGN RELEASES DELETE

3. Select the **Webhook Deliveries** tab.

   A list of webhook deliveries appear.



5 found

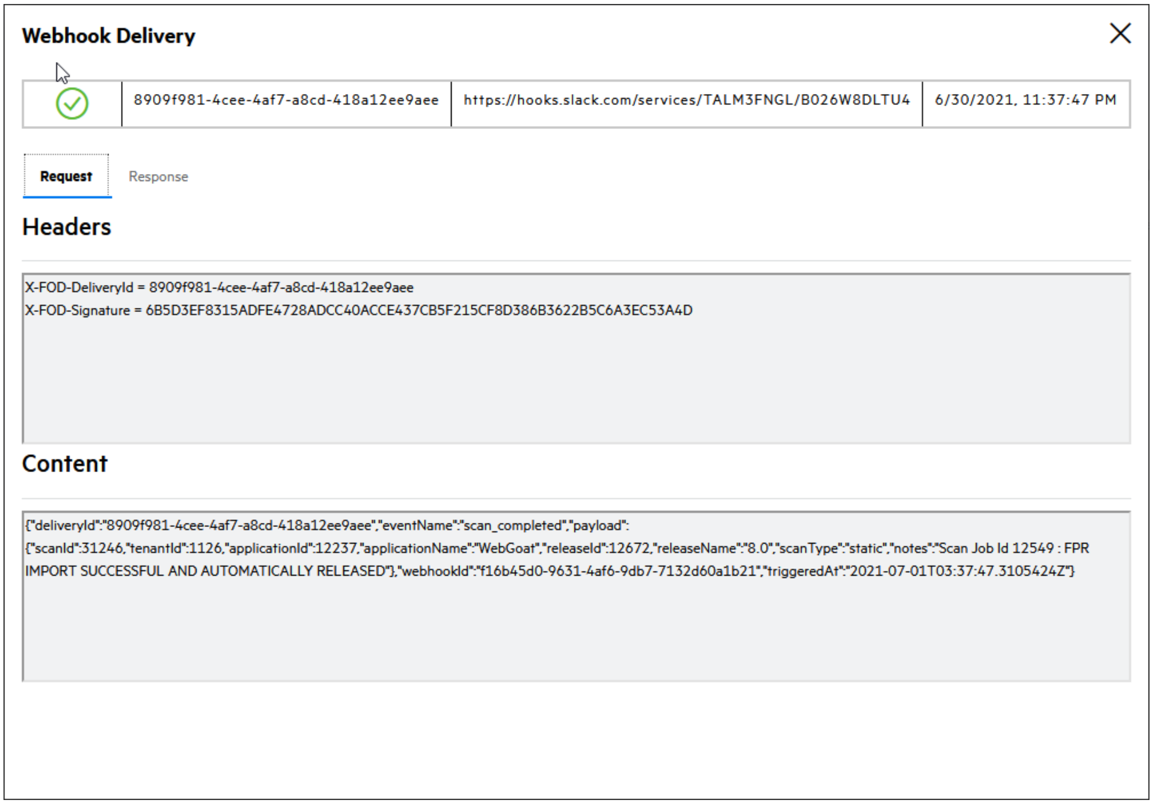
STATUS	DELIVERED DATE	ADDRESS	DELIVERY ID	
✓	6/30/2021 11:31:12 PM	https://webhook.site/89be42d3-a8dd-4414-9e31-6b09a5590ee5	bd011784-8dff-4347-a4c5-a5954b94f062	DETAILS
✓	6/30/2021 11:31:11 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	3c727595-35c6-4775-a91b-96006f34a168	DETAILS
✓	6/30/2021 9:16:38 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	5a49c118-618d-4ac3-8b49-3e1bd4632d20	DETAILS
✓	6/30/2021 8:37:47 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	8909f981-4cee-4af7-a8cd-418a12ee9aee	DETAILS
☒	6/30/2021 7:50:32 PM	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	5ac232d2-2a24-4335-8d3b-cc92b90e72bb	DETAILS

> **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 reponse.

   Request:



✓	8909f981-4cee-4af7-a8cd-418a12ee9aee	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	6/30/2021, 11:37:47 PM

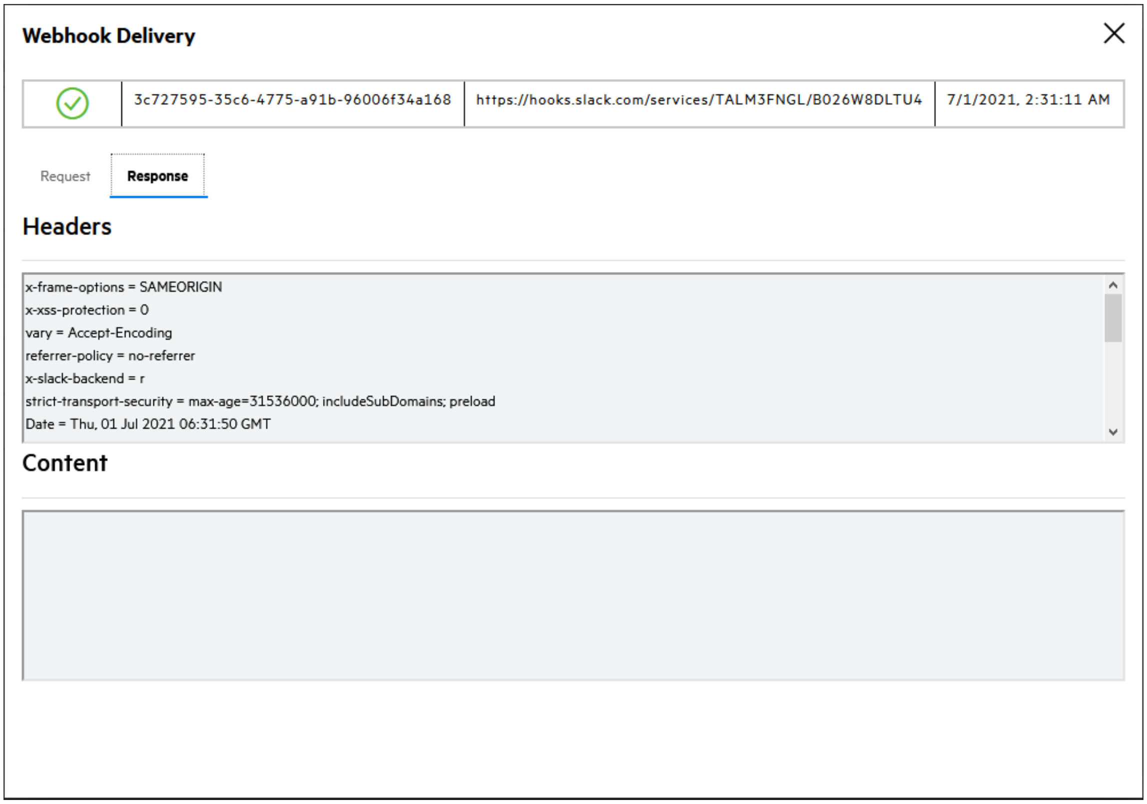
Headers

```
X-FOD-DeliveryId = 8909f981-4cee-4af7-a8cd-418a12ee9aee
X-FOD-Signature = 6B5D3EF8315ADFE4728ADCC40ACCE437CB5F215CF8D386B3622B5C6A3EC53A4D
```

Content

```
{"deliveryId":"8909f981-4cee-4af7-a8cd-418a12ee9aee","eventName":"scan_completed","payload":
{"scanId":31246,"tenantId":1126,"applicationId":12237,"applicationName":"WebGoat","releaseId":12672,"releaseName":"8.0","scanType":"static","notes":"Scan Job Id 12549 : FPR
IMPORT SUCCESSFUL AND AUTOMATICALLY RELEASED"},"webhookId":"f16b45d0-9631-4af6-9db7-7132d60a1b21","triggeredAt":"2021-07-01T03:37:47.3105424Z"}
```

   Response:



✓	3c727595-35c6-4775-a91b-96006f34a168	https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4	7/1/2021, 2:31:11 AM

Headers

```
x-frame-options = SAMEORIGIN
x-xss-protection = 0
vary = Accept-Encoding
referrer-policy = no-referrer
x-slack-backend = r
strict-transport-security = max-age=31536000; includeSubDomains; preload
Date = Thu, 01 Jul 2021 06:31:50 GMT
```

Content

Training Courses

Fortify on Demand has partnered with Security Innovation to provide secure development training courses . Review your contract to verify if they are included. If you are interested in adding courses, contact your sales representative.

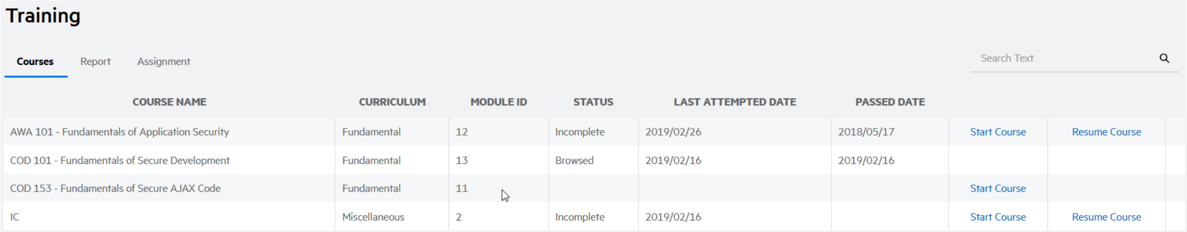
This feature requires pop-ups and cookies to be enabled for the portal.

Viewing Training Courses

To view your assigned training courses:

1. Click the icon on the portal toolbar.

   The Training page appears. The Courses tab displays the list of your assigned courses with the following information: course name, parent curriculum, module ID, course completion status, last attempted date, passed date, and course link.



COURSE NAME	CURRICULUM	MODULE ID	STATUS	LAST ATTEMPTED DATE	PASSED DATE		
AWA 101 - Fundamentals of Application Security	Fundamental	12	Incomplete	2019/02/26	2018/05/17	Start Course	Resume Course
COD 101 - Fundamentals of Secure Development	Fundamental	13	Browsed	2019/02/16	2019/02/16		
COD 153 - Fundamentals of Secure AJAX Code	Fundamental	11				Start Course	
IC	Miscellaneous	2	Incomplete	2019/02/16		Start Course	Resume Course

2. Perform one of the following actions:
   - Click the **Start Course** link in the row of a course to start the course.

     > Starting a course will reset the completion status but not the passed date. Close the course window when you are done to ensure results are properly recorded.

   - Click the **Resume Course** link in the row of a course to continue from where you left off.
   - Click the **Browse Course** link in the row of a course to view the contents without affecting the completion status or the passed date.

   A confirmation message appears.
3. Click **Yes**.

   The course appears in a new window.

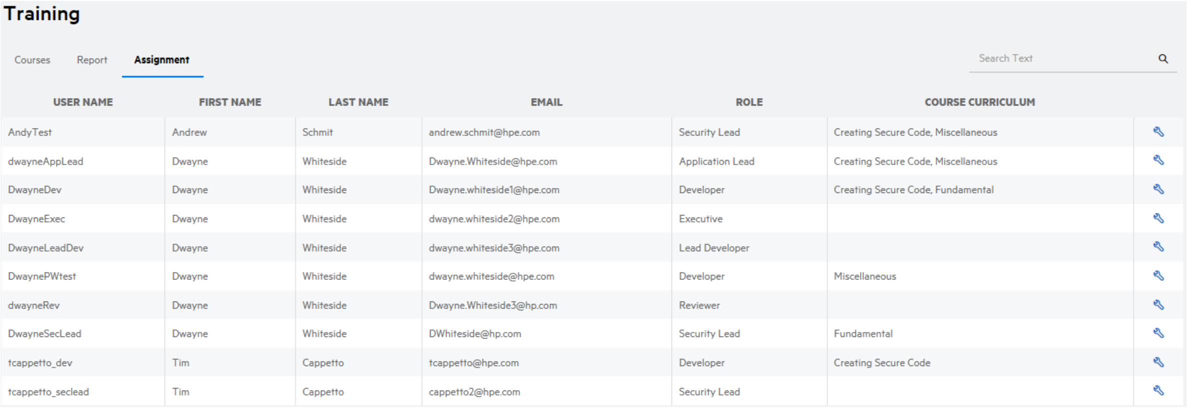
Assigning Training Courses

You can assign training courses available to your tenant to yourself. In addition, users with the **Manage Users** permissions can assign training courses to all active users in the tenant. Courses are grouped into different types of curricula and are assigned as a curriculum.

To assign training courses to yourself or another user:

1. Click the 🎓 icon on the portal toolbar.

   The Training page appears.
2. Select the **Assignment** tab.



USER NAME	FIRST NAME	LAST NAME	EMAIL	ROLE	COURSE CURRICULUM	
AndyTest	Andrew	Schmit	andrew.schmit@hpe.com	Security Lead	Creating Secure Code, Miscellaneous	🔧
dwayneAppLead	Dwayne	Whiteside	Dwayne.Whiteside@hpe.com	Application Lead	Creating Secure Code, Miscellaneous	🔧
DwayneDev	Dwayne	Whiteside	Dwayne.whiteside1@hpe.com	Developer	Creating Secure Code, Fundamental	🔧
DwayneExec	Dwayne	Whiteside	dwayne.whiteside2@hpe.com	Executive		🔧
DwayneLeadDev	Dwayne	Whiteside	dwayne.whiteside3@hpe.com	Lead Developer		🔧
DwaynePWtest	Dwayne	Whiteside	dwayne.whiteside@hpe.com	Developer	Miscellaneous	🔧
dwayneRev	Dwayne	Whiteside	Dwayne.Whiteside3@hp.com	Reviewer		🔧
DwayneSecLead	Dwayne	Whiteside	DWhiteside@hp.com	Security Lead	Fundamental	🔧
tcappetto_dev	Tim	Cappetto	tcappetto@hpe.com	Developer	Creating Secure Code	🔧
tcappetto_seclead	Tim	Cappetto	cappetto2@hpe.com	Security Lead		🔧

If your role has the **Manage Users** permission, the list of active users and their assigned curricula in the tenant appears. Otherwise, you only see your user account and assigned curricula.

3. Click ✎ next to a user.

   The Course Curriculum modal window appears.

4. Select the check boxes next to the curricula that you want to assign to the user.

   Click **Save**.

   The **Assignment** tab displays the saved changes.

Viewing the Training Report

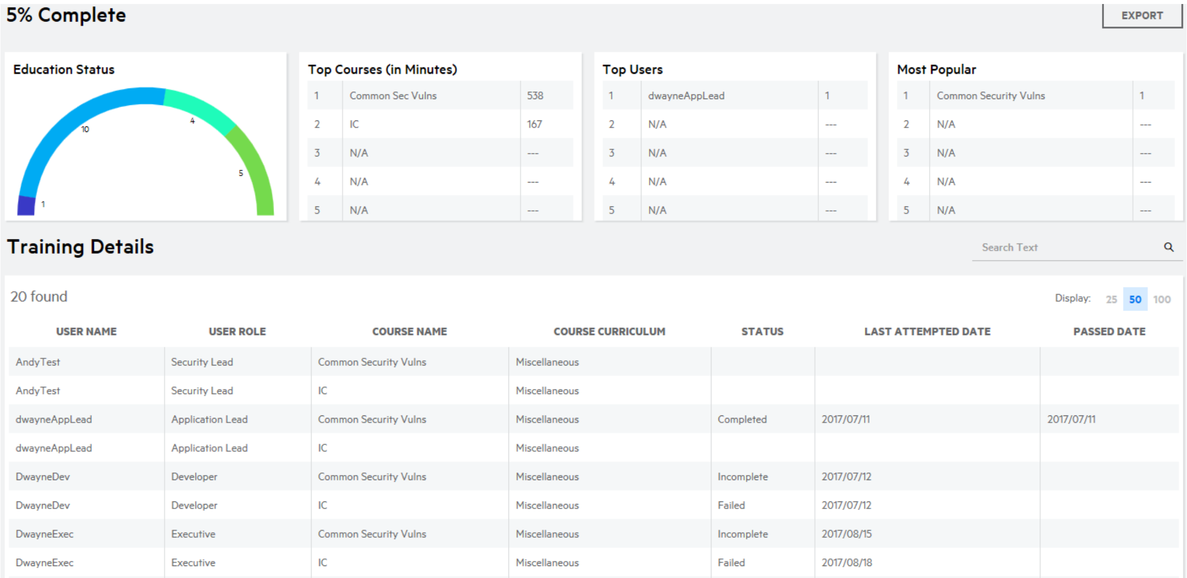
Users with the **Manage Users** permission can track user progress in assigned training courses across the tenant by viewing the training progress report. The report provides a tenant-level summary of user activity and a list of course completion statuses per user.

To view the training report:

1. Click the 🎓 icon on the portal toolbar.

   The Training page appears.

2. Select the **Report** tab.



5% Complete

Education Status

Top Courses (in Minutes)

1	Common Sec Vulns	538
2	IC	167
3	N/A	---
4	N/A	---
5	N/A	---

Top Users

1	dwayneAppLead	1
2	N/A	---
3	N/A	---
4	N/A	---
5	N/A	---

Most Popular

1	Common Security Vulns	1
2	N/A	---
3	N/A	---
4	N/A	---
5	N/A	---

Training Details

20 found

USER NAME	USER ROLE	COURSE NAME	COURSE CURRICULUM	STATUS	LAST ATTEMPTED DATE	PASSED DATE
AndyTest	Security Lead	Common Security Vulns	Miscellaneous			
AndyTest	Security Lead	IC	Miscellaneous			
dwayneAppLead	Application Lead	Common Security Vulns	Miscellaneous	Completed	2017/07/11	2017/07/11
dwayneAppLead	Application Lead	IC	Miscellaneous			
DwayneDev	Developer	Common Security Vulns	Miscellaneous	Incomplete	2017/07/12	
DwayneDev	Developer	IC	Miscellaneous	Failed	2017/07/12	
DwayneExec	Executive	Common Security Vulns	Miscellaneous	Incomplete	2017/08/15	
DwayneExec	Executive	IC	Miscellaneous	Failed	2017/08/18	

The tab displays the following information:

- The percentage of assigned courses that were completed
- Charts summarizing user progress and trends:
  - **Education Status**: the number of courses that are completed, in progress, or have not been started
  - **Top Courses**: the most active courses in terms of minutes spent

    - **Top Users**: the most active users in terms of courses taken
    - **Most Popular**: the courses that have been taken the most

  - The **Training Details** grid displaying in each row the tenant user, the assigned course, the course progress status, the last course access date, and the last course completion date.

3. Click **Export** to export the **Training Details** grid as a CSV file. Search results are applied to the export.

Chapter 10: Policies and Support

For more information on Fortify on Demand, review the Fortify on Demand policies and support resources.

This section contains the following topics:

Maintenance Schedule and Software Updates

Fortify on Demand provides the following information regarding maintenance schedule and software updates.

Maintenance Schedule

To help customers plan for scheduled maintenance, Fortify on Demand reserves predefined time frames to be used on an as-needed basis: a weekly two (2) hour window (Thursday 00:00 to 02:00) and one (1) monthly forty-eight (48) hour window (Saturday 00:00 to Sunday 00:00). These maintenance windows will be used on an as-needed basis and in the vast majority of instances will have no impact on users' ability to access or leverage functionality in Fortify on Demand.

The maintenance window for each data center is set using the following time zones:

Data Center	Maintenance Time Zone
AMS	US Eastern Time
EMEA	Greenwich Mean Time
APAC	Australian Eastern Time

For additional details about scheduled maintenance in other environments, contact support.

Software Updates

Fortify on Demand determines whether and when to develop, release, and apply software upgrades to the Fortify on Demand platform and/or supporting components. Major releases are typically made available on a quarterly basis, with minor releases and patches made available on an as-needed basis. Unless Fortify on Demand anticipates a service interruption due to a software upgrade, Fortify on

Demand may implement a SaaS upgrade at any time without notice to the customer. Fortify on Demand aims to use the monthly scheduled maintenance window to apply major software updates.

Security content updates to expand and improve Fortify on Demand's ability to identify vulnerabilities are a key component of the Fortify on Demand service. Security content updates are developed by the Fortify Software Security Research (SSR) team and are typically released at the end of each calendar quarter. Fortify on Demand typically deploys updated security content within several weeks of public availability. Security content updates may be deployed outside of the quarterly updates in response to significant new threats or zero-day vulnerabilities. Fortify recommends Fortify users to stay up-to-date with the latest security intelligence by following the OpenText Security Research blog at https://community.microfocus.com/cyberres/b/off-by-on-software-security-blog.

Data Retention Policy

Fortify on Demand has implemented the following data retention policy for customers as of the v18.4 release. Fortify on Demand encourages customers to review and download any files outside the data retention windows that they wish to retain.

Resource	**File Type**	**Retention Period**
Data exports (Application and Release Issues pages)	.csv	7 days
Source code	.zip	15 days
Mobile application binaries	.ipa, .apk	30 days
Notifications	-	3 months
Data exports (global Reports page)	.csv	3 months
Event log	.csv	13 months
User-generated reports	.pdf, .html	2 years
Fortify scan result files	.fpr	2 years
Software bill of materials (SBOM)	.json	2 years
Site trees	.csv	2 years
Application data	-	Customer controlled*
Release data	-	Customer controlled*
Issue data	-	Customer controlled*
User data	-	Customer controlled*

*The customer is responsible for creation and deletion of the specified data as long as the customer maintains an active status with Fortify on Demand. The customer can delete an application, release, or user at any time. Issue data associated with an application or release is also deleted. Upon termination of the Fortify on Demand service, the termination data retrieval period is 30 days.

For more information, please contact support.

Getting Support

Fortify on Demand offers support through self-service resources and the Fortify on Demand Help Center, staffed 24/7 by a dedicated support team of TAMs. The self-service resources include video demonstrations, a knowledge base, and product documentation. If you did not find what you were looking for, start a live chat with support or submit a support ticket in the Help Center. You can call support at 800.893.8141 or 650.800.3233 if internet access is unavailable.

This section contains the following topics:

Accessing Support Resources

Support resources are available through the portal. The portal contains direct links to how-to videos, online help, live chat, and the Help Center. The Help Center is Fortify on Demand's support ticket system. It also hosts PDF versions of the User Guide and Release Notes and the knowledge base.

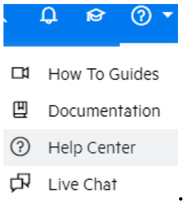
Note: You can directly log in to the Help Center through the relevant URL using your Fortify on Demand credentials:

- AMS: https://helpcenter.ams.fortify.com
- EMEA: https://helpcenter.emea.fortify.com
- APAC: https://helpcenter.apac.fortify.com
- SGP: https://fodsgp.zendesk.com/

To access support resources:

1. Click the help menu and select one of the following:
    - **How To Guides** - opens Fortify on Demand how-to video guides, part of the Fortify Digital Learning offerings.
    - **Documentation** - opens the online help
    - **Help Center** -opens the Help Center
    - **Live Chat** - opens the Live Chat window where you can chat with Fortify on Demand support

24/7



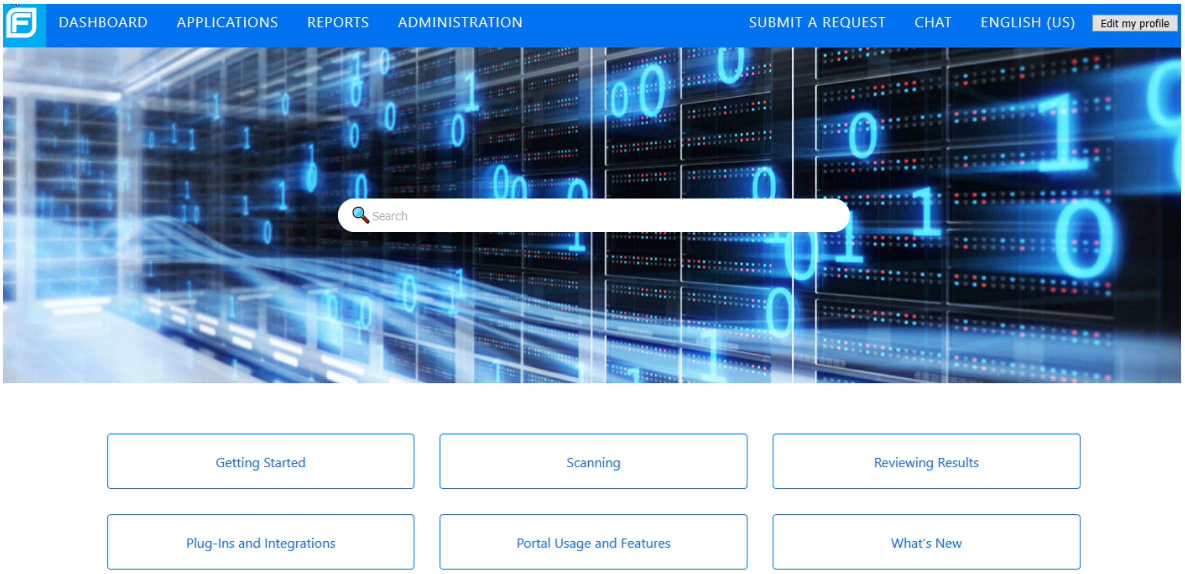
Submitting a Help Center Ticket

Submit a support ticket in the Help Center.

To submit a Help Center ticket:

1. Click the help menu and select **Help Center**.

   The Help Center opens in a new window.

2. Click **Submit a Ticket**.

   The **Submit A Request** form appears.
3. Select the ticket type from the drop-down list:
   - **Create Ticket** - get help with a general product question or a tenant-specific issue
   - **FoD Defect Submission** - report a Fortify on Demand bug or issue
   - **FoD Enhancement Submission** - request an enhancement
4. Complete the fields displayed for the selected ticket type. Provide as many details as possible.
5. Click **Submit**.

   A message at the top of the page indicates that your Help Center ticket was submitted.

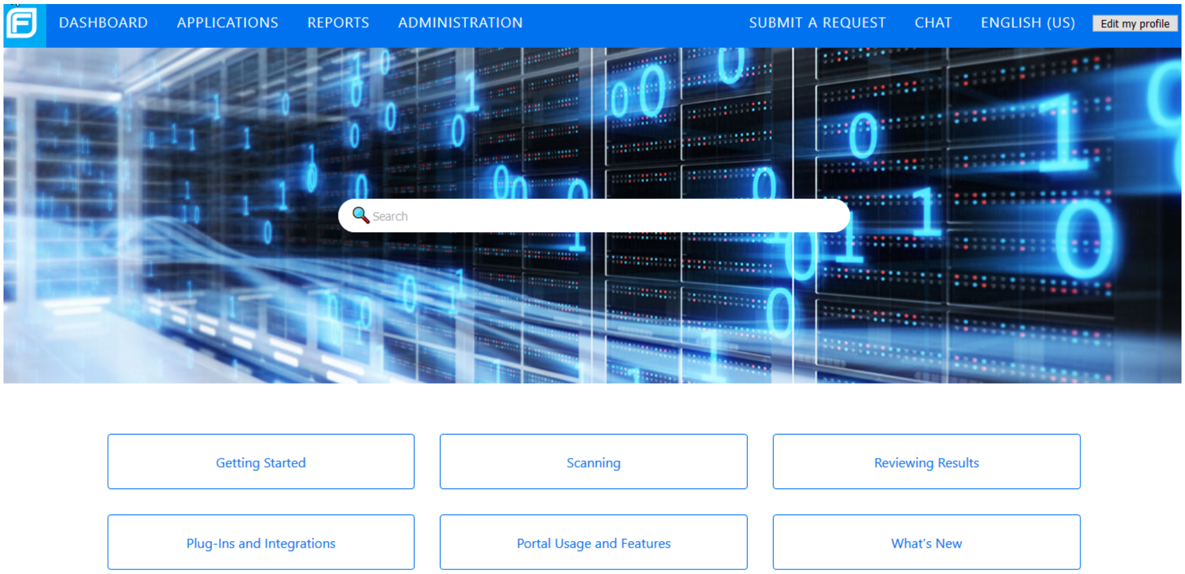
Tracking your Help Center Tickets

You can track support tickets submitted for your tenant in the Help Center. You can only view tickets that you have submitted, are assigned to, and are copied on (if you are on an application's notification list you are automatically added to tickets linked with the application).

To track your Help Center tickets:

1. Click the help menu and select **Help Center**.

   You are redirected to the Help Center.

2. Click **View Tickets**.

   Your tickets are displayed. Tickets have one of the following statuses:

   - **Open** - Your request has been received and assigned to 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 Fortify on Demand team is still working on.
   - **Awaiting your reply**- Show tickets that require action from your organization.
   - **Solved** - Show tickets that have been resolved.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Customer Support at https://www.microfocus.com/support so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify on Demand 24.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to mfi-fortifydocteam@opentext.com.

We appreciate your feedback!