Polaris

Contents

Understand Polaris

Product overview

What is Polaris

Polaris is a *collection of services* that make it easier to orchestrate and manage application security testing. It is specifically tailored to companies that need to do the following:

- Scan code in the cloud
- Incorporate application security testing into the DevOps pipeline
- Use a single interface for multiple types of security testing

What Polaris does

These are the capabilities available now:

- **Testing** –Upload and scan apps using static analysis and compositional analysis.
- **Issue Lifecycle Management** – Review, triage, dismiss, and eventually close issues discovered during security scans. You can do these things manually or programmatically (through Polaris APIs).
- **Analytics** – Review the overall risk posture of a project, an application, or the entire organization.
- **Automation** – Use REST APIs to incorporate security testing into the DevOps process in ways that speed up production.

How teams use Polaris

- Upload files to the cloud for automated security testing.
- Use the UI to triage and resolve issues found in the code.
- Use dashboards to monitor the security stance of applications and their constituent projects.

Achitecture: The Parts of Polaris

These are the ways you can use Polaris:

- Polaris Web UI. Entitlements, issue lifecycle management, testing, dashboards.
- Polaris API. Every task carried out in the web interface can be accomplished via API.

Entitlements on Polaris

An entitlement represents the ability to conduct a scan or use a service.

After an organization purchases entitlements, someone (an Application Super User) must associate an entitlement with an application before members can begin using tests and services. The entitlements that get associated will determine what types of scans and services are available for members who test that application.

Entitlements always contain several properties:

- The type of scan (SAST or SCA) or service.
- An expiration date

- Triage availability (first-time-only or never)

When members of an application choose a test type, the choices are set by the available entitlements.

Once an entitlement is associated with the application, members can scan as often as they want to – there is no limit on the number of tests.

The data model: Applications and Projects in Polaris

Polaris is organized around ***Applications*** and ***Projects*** .

An Application is a collection of as many as 100 Projects. Its boundaries don't necessarily align with the boundaries of a software product, and they don't need to. The Application can also be called the organizing principle of Polaris, because Projects and entitlements all must be associated with an Application.

A Project is a discrete body of code that is also a subcomponent of a larger codebase. It might correspond to one repository, but it doesn't have to. A test always runs on a single Project, and the resulting issues accumulate in the dashboard for that Project. Projects are always owned by a parent Application.

The Polaris web UI

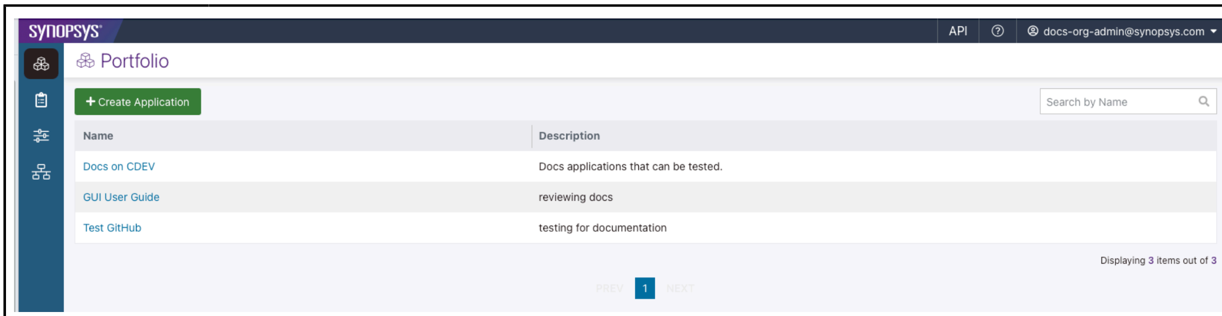
Polaris UI Overview

A summary of the Polaris UI features.

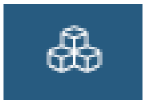
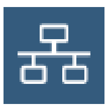
Navigation

Use the Top and Left Navigation bars to access Polaris functions.

Table 1: Top and Left Navigatation Bars



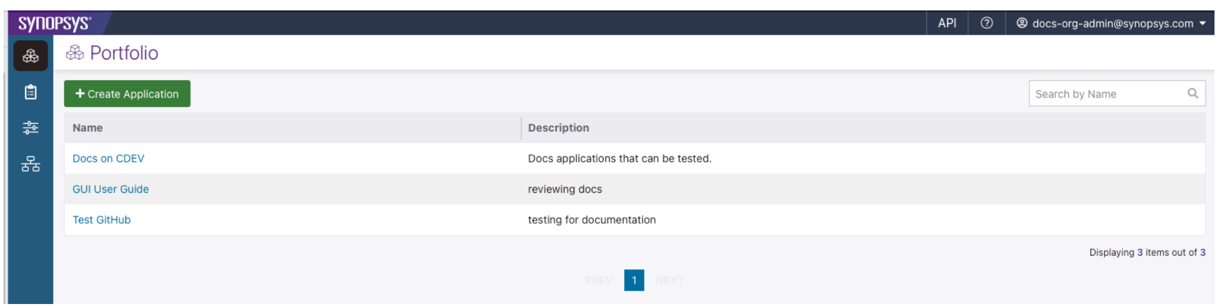
Top Nav	Use to perform basic functions in Polaris.
API	Link to Synopsys Developer Portal
	Find API and Polaris documentation. Submit support case or view your open cases.

Profile	Account sign in/out. Includes access to Account (edit info, reset password) manage your Notifications, Access Tokens, Downloads (Polaris CLI tool).
Left Nav	Use to access pages to set up applications and projects, run tests, and adminster Polaris.
	Portfolio Page on page 6 : Create and manage applications and projects. Allows you to drill down to issues and view tests run on projects.
	Tests Page on page 8 : Run tests on source code. Includes details about test, assessor comments, and issue counts.
	Dashboard : An executive level dashboard that shows the security status of your application and how your organization is using Polaris..
	Reports : Create an Issue Detail report for a specific project.
	Policies Page on page 9 : Create and manage policies (issue guidlines for organization and frequency of scan for projects).
	My Organization Page on page 10 : Admin only.

Portfolio Page

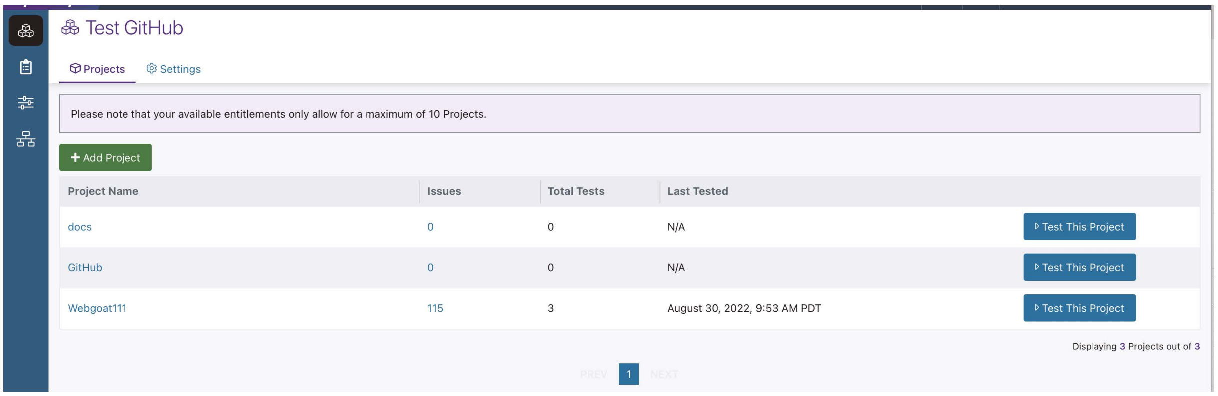
The Portfolio page allows you to create and manage applications.

Table 2: Portfolio Page



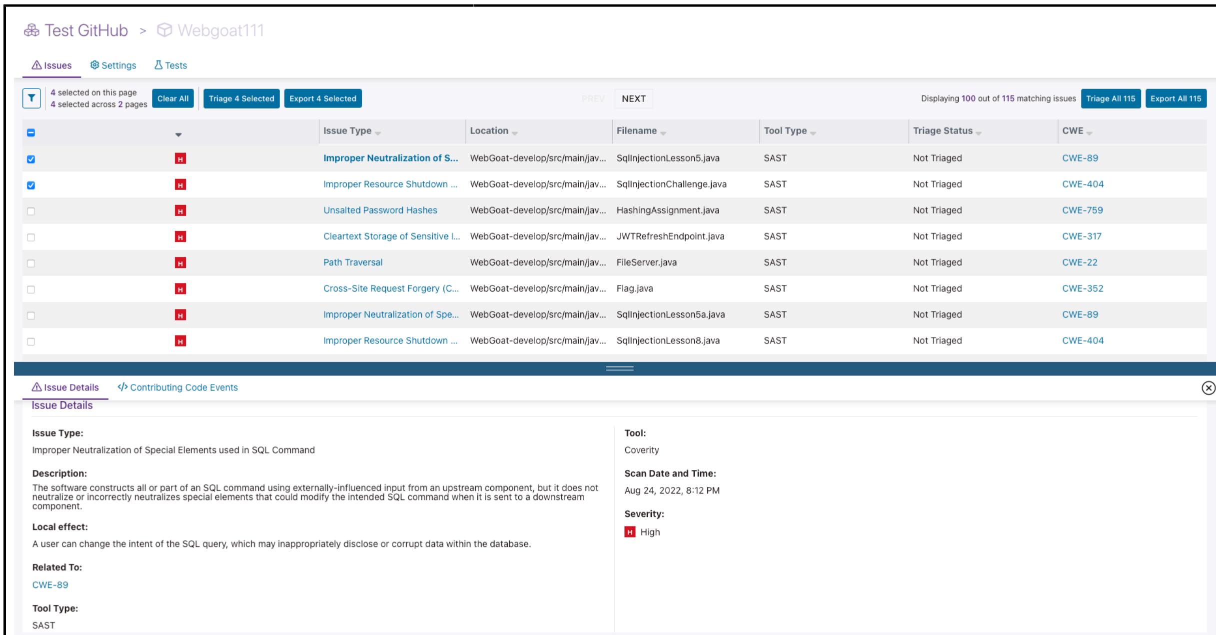
Create Application	Create a new application (set of projects).
Search by Name	Search applications by name.
Table fields	Lists all applications and descriptions. Click an application name to open the Table 3: (Portfolio) Application Page on page 7 .

Table 3: (Portfolio) Application Page



Projects tab	Lists all projects and descriptions in the application.
+ Add Project	Create a new project in the application.
Search by Name	Search projects by name.
Table fields	Click a project name to go to the Table 4: (Portfolio) Project Page on page 7.
Test This Project	Test the selected project. See How to Test on page 38.
Settings tab	Manage settings for applications.
General	Change name and description of Application. Add Tags.
Subscriptions	Edit application level status or SCA subscriptions.

Table 4: (Portfolio) Project Page



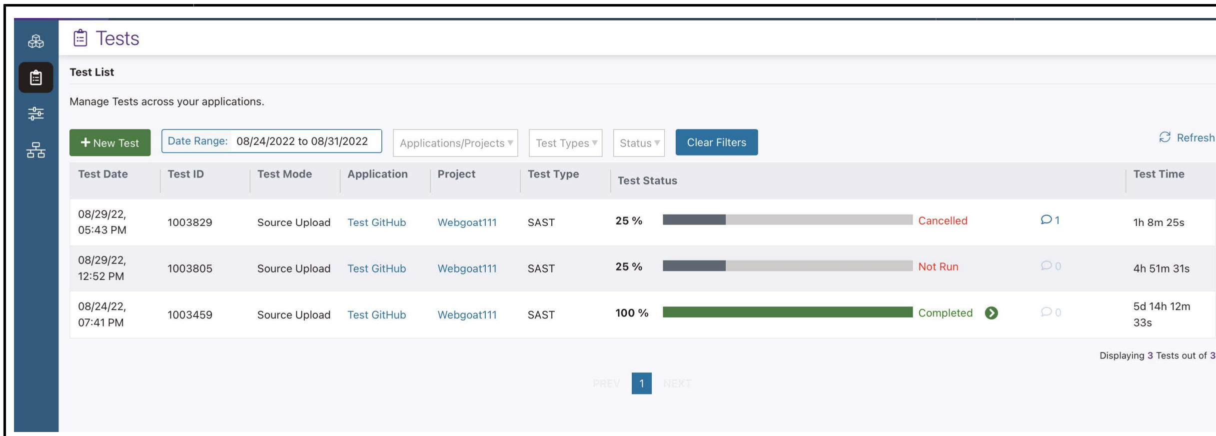
Issue tab	Lists issues in the project.

Clear All	
Triage Selected / ALL	Triages issues selected by checkbox or filter, or click ALL. See Ways to triage in Polaris on page 39
Export Selected / ALL	Export issues selected by checkbox or filler, or ALL. See How to Export Issues on page 41.
Table fields	**Issue Type:** Click on name to see *Issue Details* tab including Description, Local effect, Tool used, Scan date and time, and *Contributing Code Events* tab which includes path and support events check boxes.. Also listed in this field is Location, Filename, Tool Type, Triage Status, and CWE.
Settings tab	Manage settings for projects.
General	Edit Project Name and Description
Integration	• Use to set up Source Code Management (SCM) repository integration for project. See Integrate a Repository on page 37. • Select a JIRA Instance and a Jira Project to export issues to. (Available if Org Admin has set up integration.) See Set up Jira in an individual Project on page 41.
Policies	View policies for the project. Add an exisiting policy to the project.
Tests Tab	View SAST and SCA Test Id, Date and Status for that project.

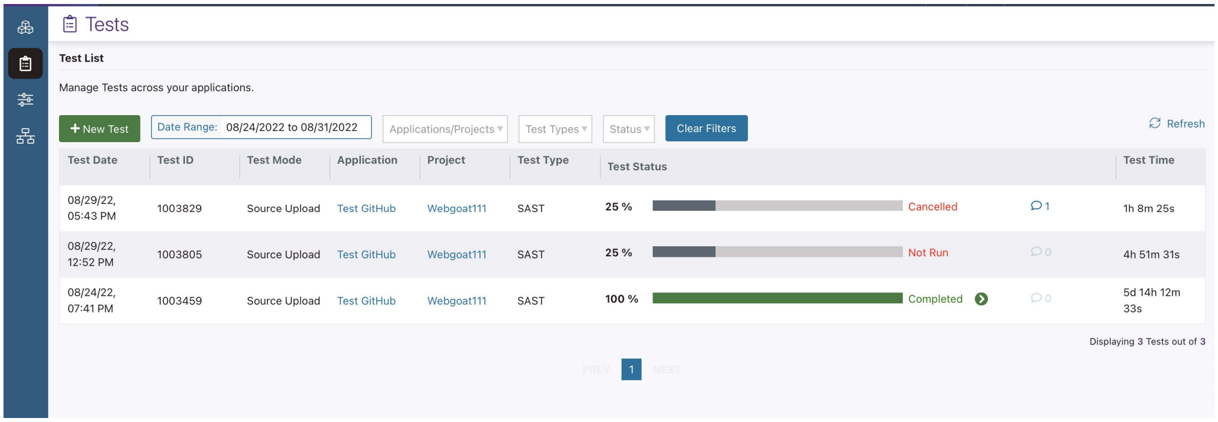
Tests Page

The Tests page allows you to manage and run rests on applications.

Table 5: Tests Page



+New Test	Run a test. See How to Test on page 38.
Date Range	Filter by dates.

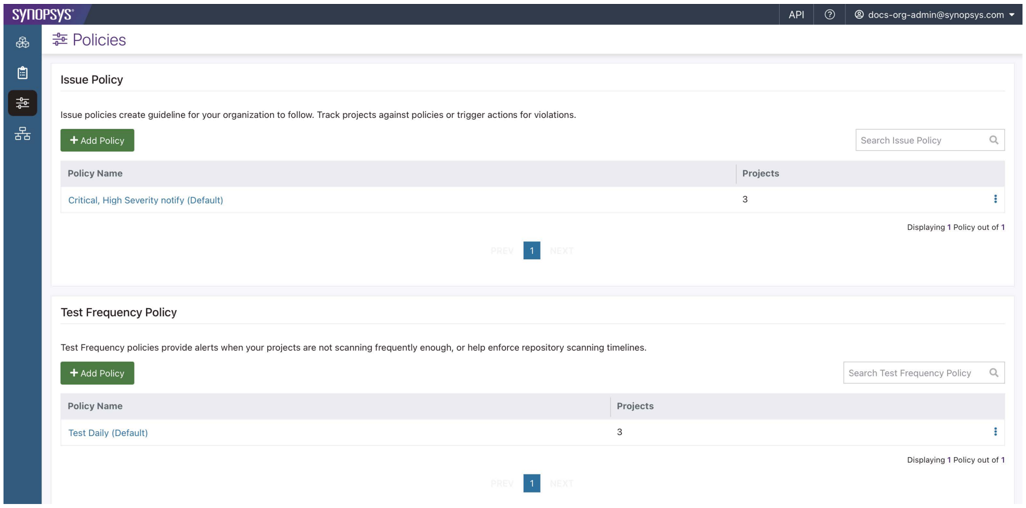


Appplications/ Projects	Pulldown menu to select and see application/projects tests.
Test Types	Pulldown menu to organize by type.
Status	Pulldown menu to organize by status in testing.
Clear Filters	
Refresh	Update the page.
Table fields	Test Date: Date and time stated Test ID: Test Mode: Source Upload . Application name. Click to see Table 3: (Portfolio) Application Page on page 7. Project: Click to see Table 4: (Portfolio) Project Page on page 7. Test Status: Show percentage, progress bar and where it Dialog icon : Click icon on test row to see comments from assessor for that test. Test Time: ??

Policies Page

The Policies page allows you to create policies for applications.

Table 6: Policies Page

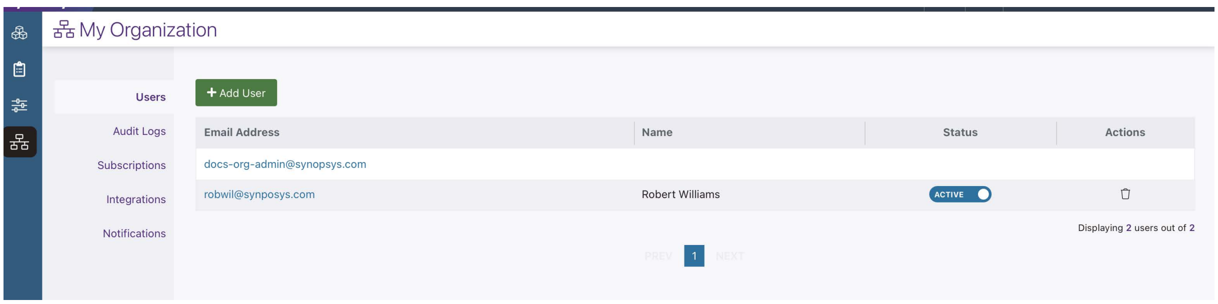


Issue Policy	Create guigelines for your organization to follow and track projects against policies or trigger actions for violations.
Add Policy (I)	Add an Issue policy.
Search	Search Issue Policy.
Table fields	Policy Name: Click name to view policy. Ellipse icon : Allows you to edit, duplicate, set as default (for your org) or delete that policy.
Test Frequency Policy	Provies alerts when your projects are not scanning frequently enough, or help enforce repository scanning timelines. For more detail, see Test Frequency Policies
Add Policy (TF)	Add a Test Frequency policy.
Search	Search Test Frequency Policy.
Table fields	Policy Name: Click name to view policy. Projects: How many projects use that policy. Ellipse icon : Allows you to edit, duplicate, set as default (for your org) or delete that policy.

My Organization Page

The My Organization page allows administrators to manage Polaris for the entire organizations including adding users, viewing audits, add subscriptions and manage notifications.

Table 7: My Organization Page



Users	• Add users to Polaris • See email and name of existing users. • Set Status to active or inactive • Delete (from) Polaris by clicking trash can icon.
Audit Logs	See system changes from the user interface and API. Users can filter results by date, event type, etc., and export audit log.
Subscriptions	Add and view subscriptions and see if active for all of Polaris.
Integrations	Set up Jira Integrations to be used across organization.
Notifications	Enable or disable email notifications for all users. (For individual accounts, see Profile>Account>Notifications).

Get Started

The Org Super User

Before you begin, we recommend reading the following:

- Product Overview
- Subscriptions and Entitlements
- Roles and permissions on Polaris
- Polaris data model

Goals

As your organization's Org Super User, start by doing the following:

- Invite members of your organization to sign into Polaris
- Make at least one member an Application Super User, so they can create the applications and projects that your members will join
- Decide whether to allow Polaris to send notifications to users

Review your personal settings

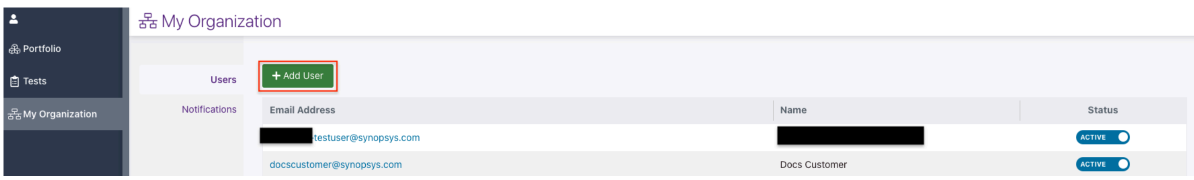
1. Navigate to your personal settings by clicking on your profile name in the top left corner of the browser tab.
2. Click **Account** on the left navigation bar.
3. Verify your profile information and make changes if you wish.
4. Click **Notifications**.
5. Review your notification settings.

   Use Checkboxes to select the types of email notifications you'd like to receive.

   Note: If an Org Super User turns off notifications globally, you won't receive any — even if you have requested them in the **Notifications** area.

Invite users to join Polaris

1. Navigate to **My Organization** > **Users.**
2. Click **Add User**.



3. Complete the form on the Add User page.

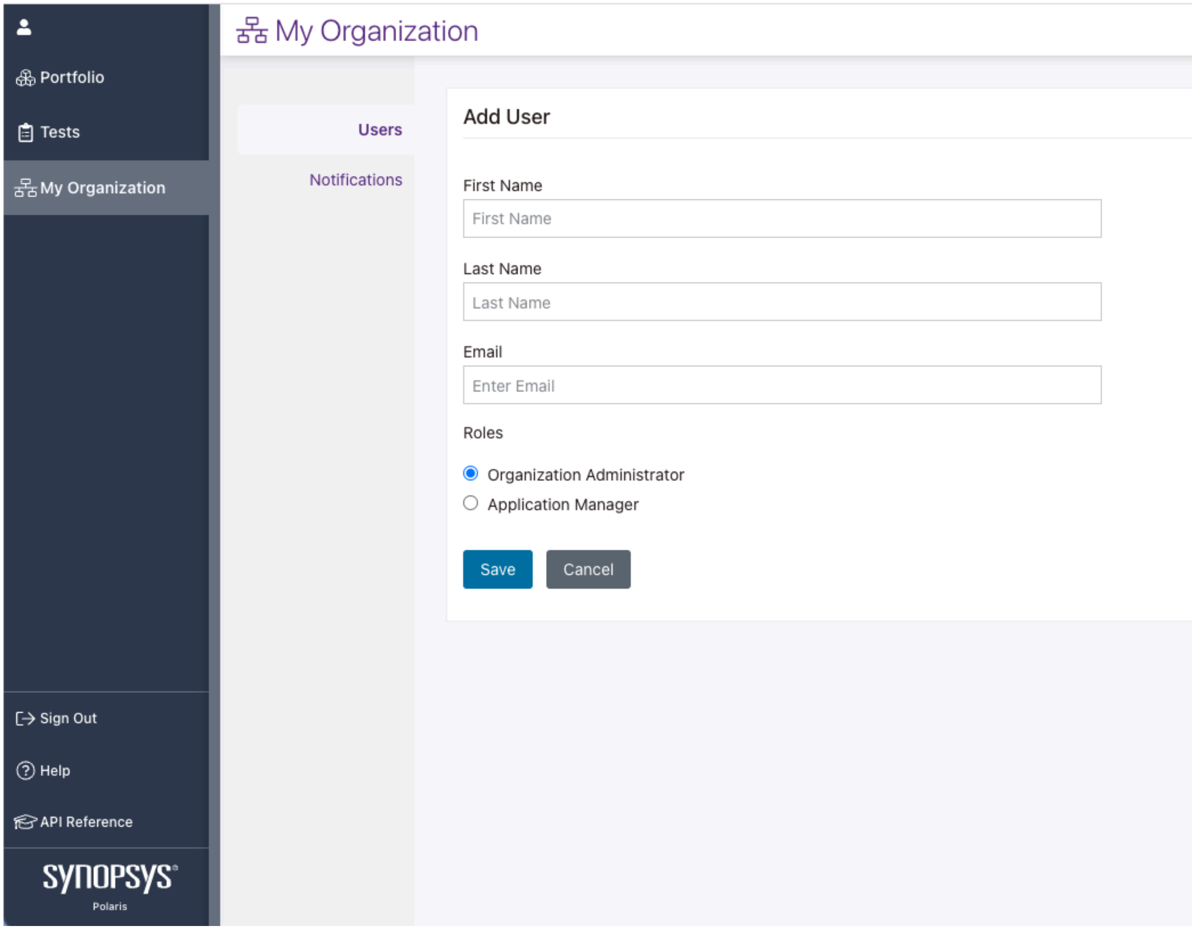


Table 8: 'Add User' fields

Field name	Description
Name	This should be the user's actual name.
Email	An email address in your company domain.
Roles	Select user's role.

4. Click **Save**.
5. Repeat for each user you wish to invite to Polaris.
   Users will receive an email invitation, similar to the one you received, with a link to help them create a password and sign in.

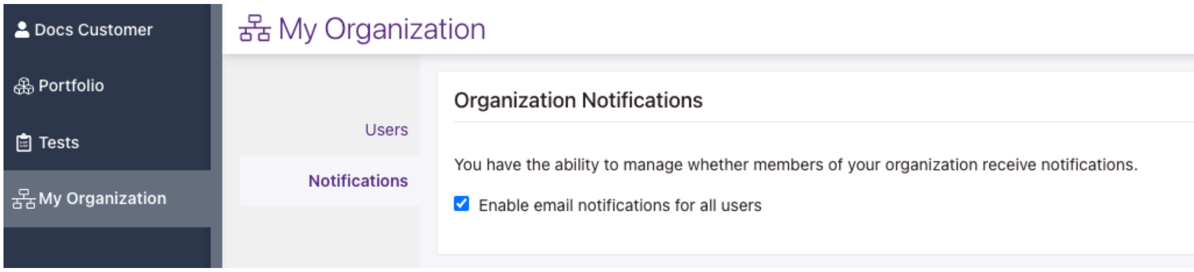
Create at least one Application Super User

1. From **My Organization** > **Users**.
2. Select the user whom you want to modify.
3. On the **Edit User** page, use radio buttons to select **Application Super User**.
4. Click **Save**
   The user will receive a notification of the role change.

Disable notifications if desired

Notifications are enabled for the organization by default but disabled for individual users. Users can decide which notifications to receive or they can decide not to receive notifications at all. An Org Super User can disable notifications for the entire organization.

1. If you wish to disable notifications for everyone, go to **My Organization** > **Notifications**
2. Uncheck the box that says Enable email notifications for all users



Get started: Application Super User

Before you begin, we recommend reading the following:

- Product Overview
- Subscriptions and Entitlements
- Roles and permissions on Polaris
- Polaris data model

Goals

As an Application super-user, you play an important part in bringing your team into Polaris.

By the end of this process, you will:

- Create at least one application
- Add projects to the application
- Add members to the application

Depending on the size of your organization, you may need to repeat the process.

Review your personal settings

1. Navigate to your personal settings by clicking on your profile name in the top left corner of the browser tab.
2. Click **Account** on the left navigation bar.
3. Verify your profile information and make changes if you wish.
4. Click **Notifications**.
5. Review your notification settings.

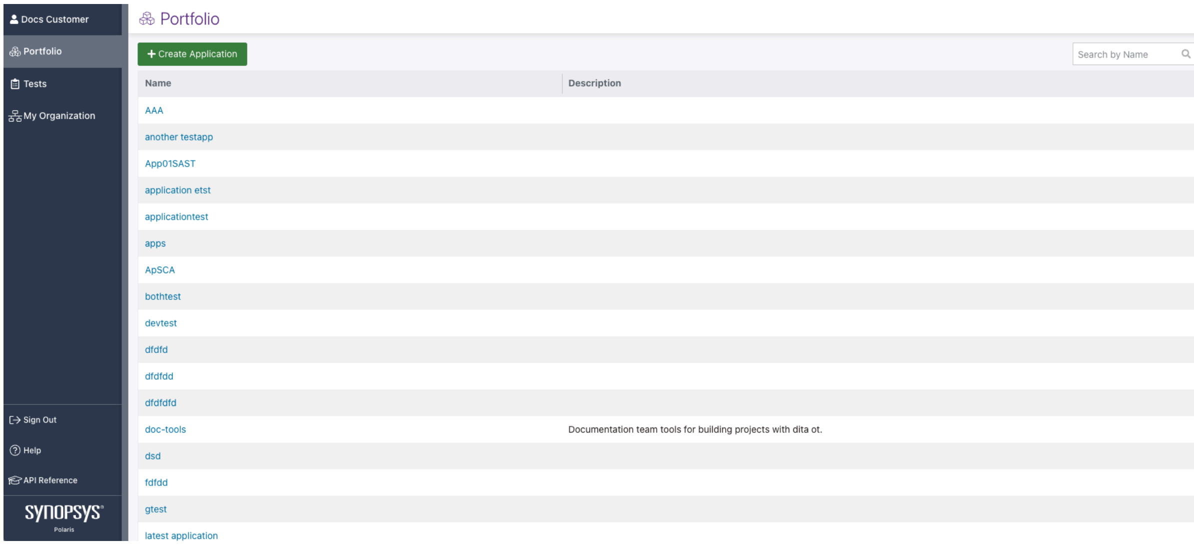
   Use Checkboxes to select the types of email notifications you'd like to receive.

   (If all the checkboxes are disabled, it means an Org Super User has turned off notifications for the organization. You won't be able to make changes and won't receive notifications.)

Create an application and add projects

1. Go to Portfolio on the left sidebar.

2. Click **Create Application**.



3. Click the Step One tab and enter the necessary application details.

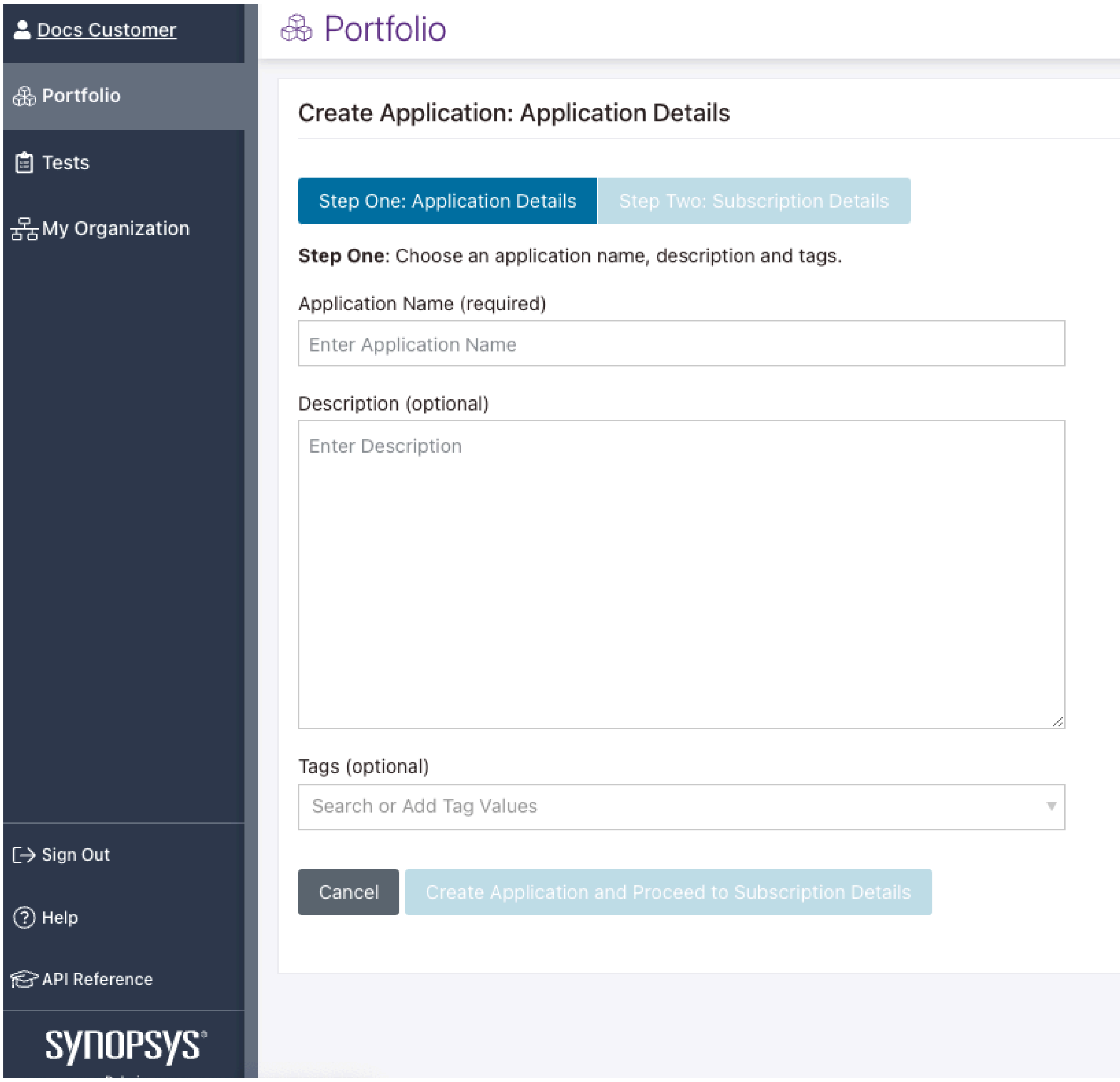
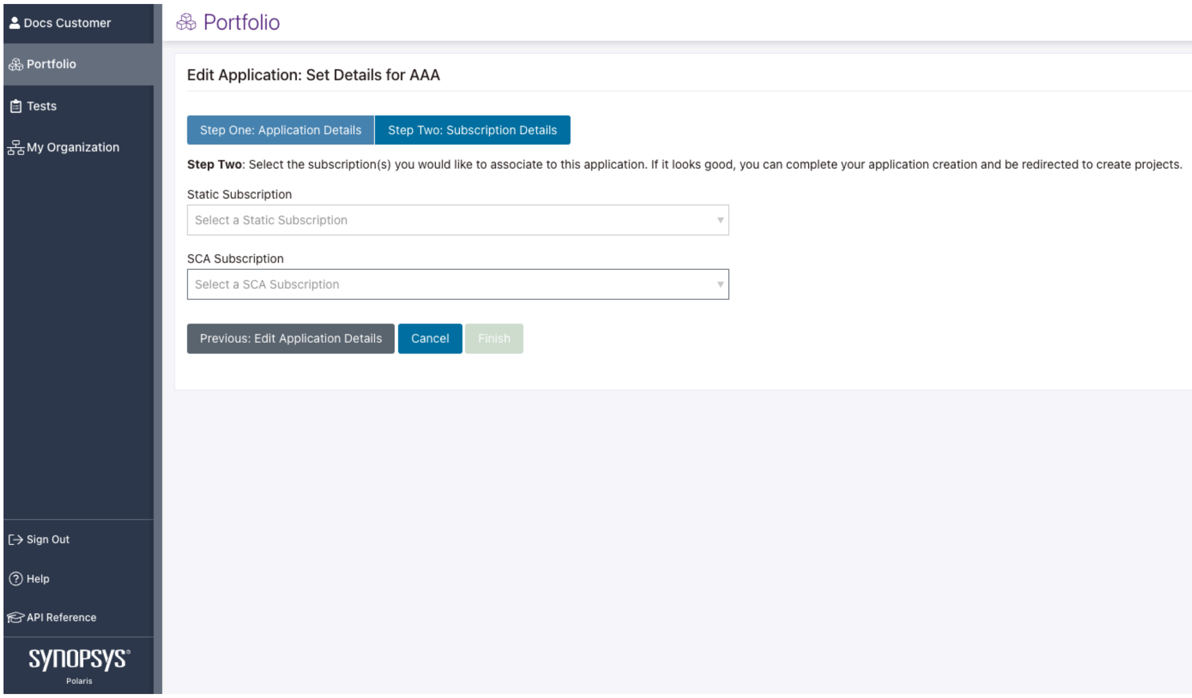


Table 9: 'Application Details' fields

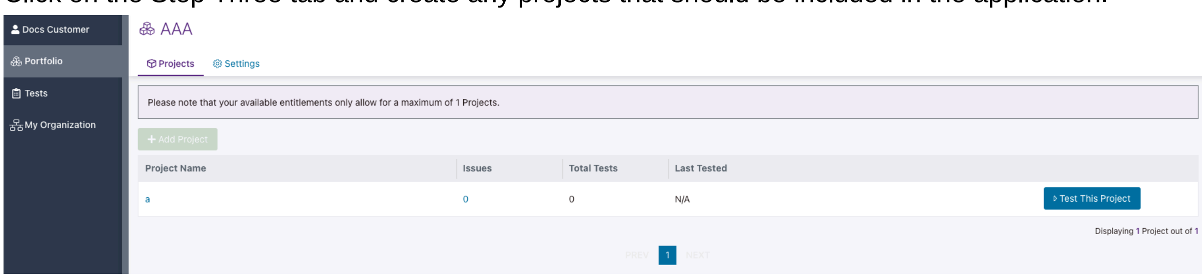
Field name	Description
Application Name	The name must be unique within your organization.
Description	A short description of the application that will be useful to users from your organization.
Tags	You can create any tags necessary to classify your applications. This is useful for grouping applications when they all belong to a larger program.

4. Click on the Step Two tab. And choose the entitlements and subscription associated with the application.



You must choose one test type for SCA and one for SAST. The entitlement should provide the desired number of projects and a triage type suitable for the project.

5. Click on the Step Three tab and create any projects that should be included in the application.



6. To create a project, enter a name and description.

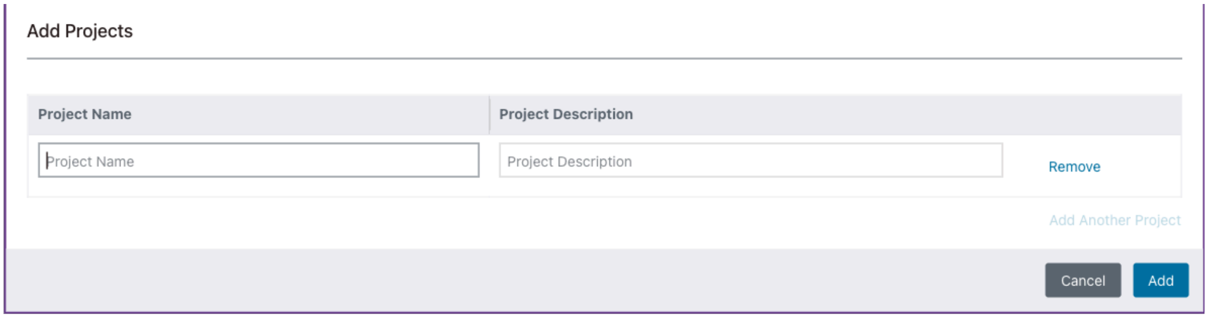


Table 10: 'Create Project' fields

Field name	Description
Project Name	Each name must be unique within the organization.
Description	The description should be useful to members of your application.

>

7. Click **Finish**.

Add members to the Application

1. In your new application, navigate to Settings and then click Members.

   Note the following:

   - Members can only be added at the application level.
   - You can only select members who have already been added to the organization by the Org Super User.

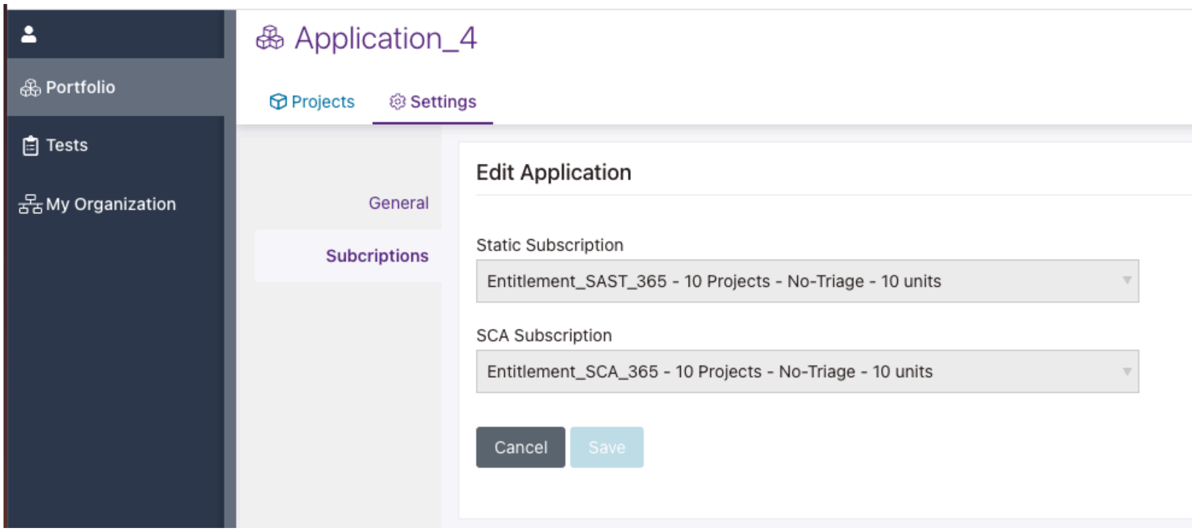
2. Select a member to add to the application.
3. Select a role for the new member. This completes the task and adds the new member to the list below the form.
4. Repeat the process until you've added all the users.

   Note that members are added at the application level and have access to all the projects included in the application.

Change the entitlements for an Application

1. From within the Application, go to **Settings**.

2. Select Subscriptions from the let-hand navigation bar.



3. Use pulldown menus to select SAST and SCA subscriptions.
   You must choose both SAST and SCA for each Application.
4. Click **Save**.

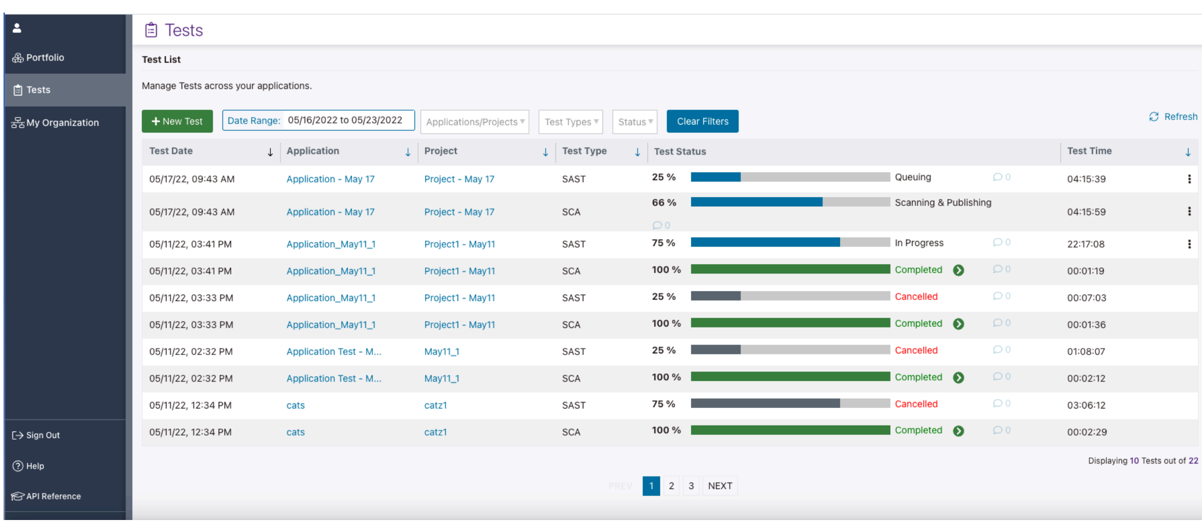
Upload files and start testing

See How to Test on page 38

Monitor tests and get test results

1. Navigate to Tests in the left-hand navigation menu.
2. If numerous tests are showing, you might need to filter to see your test. First try filtering on test status, for tests that are still running.

   Depending on the size of your project, a test may take a number of hours to finish running. When the test is complete the progress bar shows 100 percent and a green circle enclosing a greater-than symbol appears to the right of the progress bar on the Test List page.



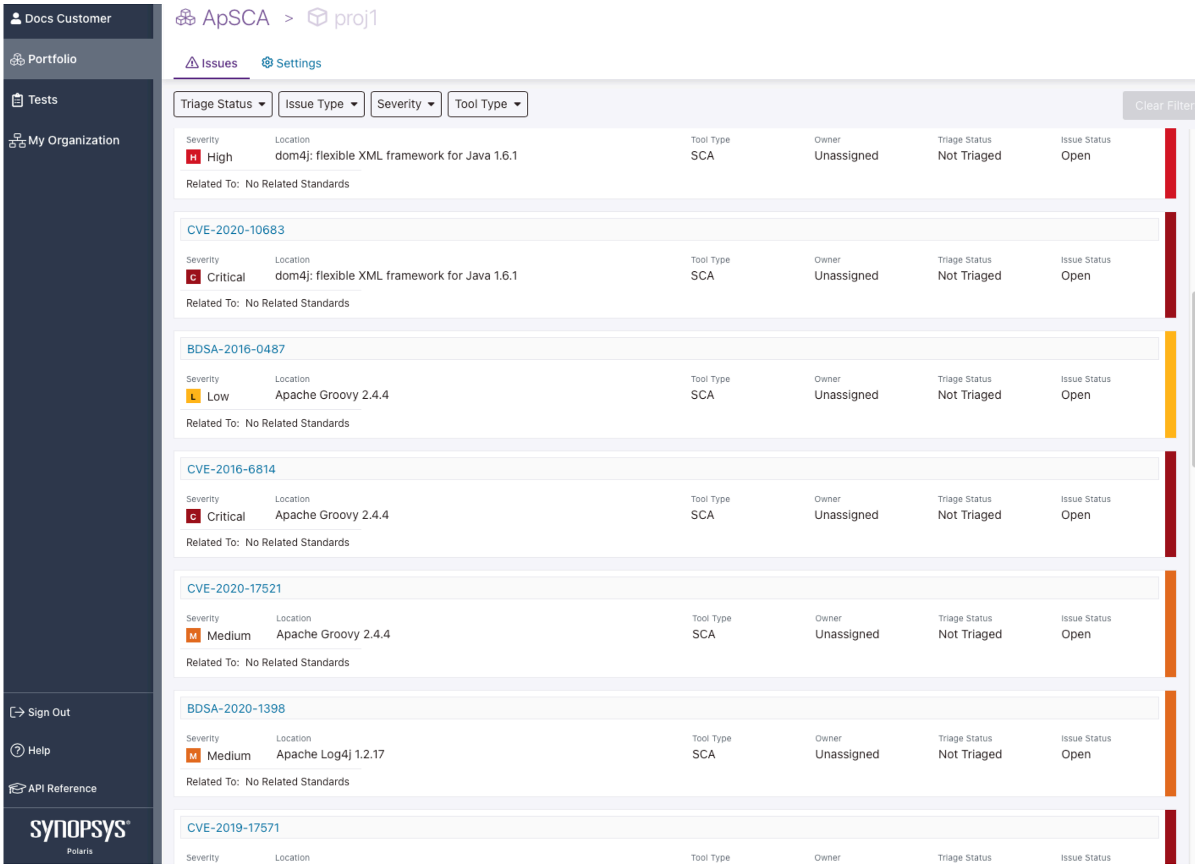
3. After the test is complete, click the green arrow to the right of the progress bar to see test results.

Filter and review the issues

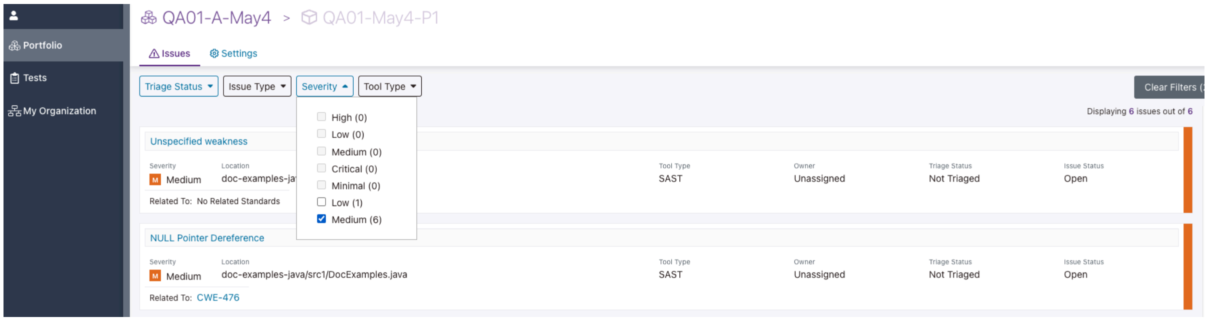
You can review issues in the following ways:

- Select a test on the Test List page, to see the issues found in that test.
- Navigate to the Issues tab in a project to see all its current issues.

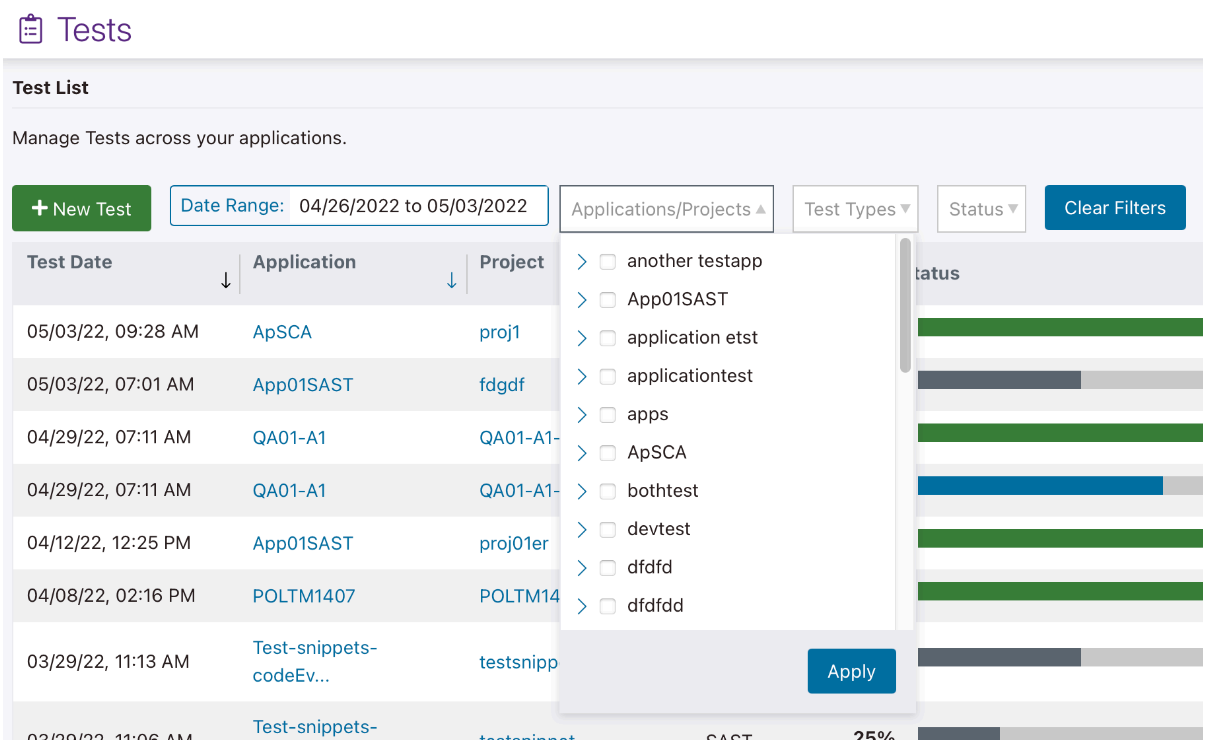
Either method will result in a similar list of issues.



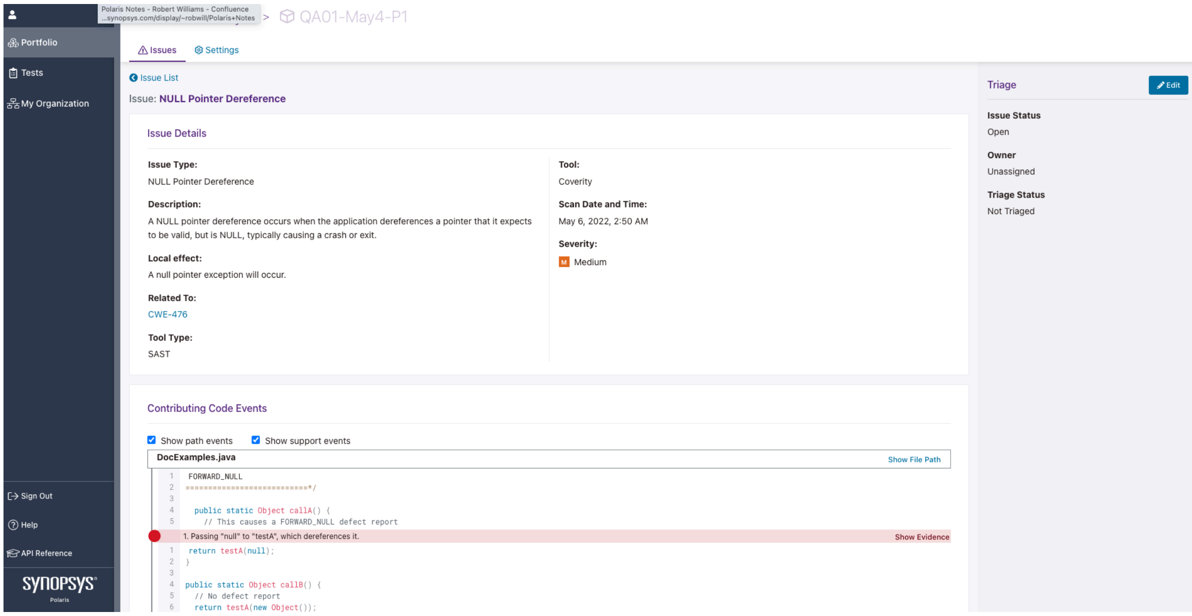
1. Use the pull-down menus at the top to filter the results according to issue type, severity, and triage status. (For example you might want to see all the un-triaged issues, or all that are un-triaged and high severity.)



Pull down each tab and use checkboxes to indicate the kinds of issues you want to see.

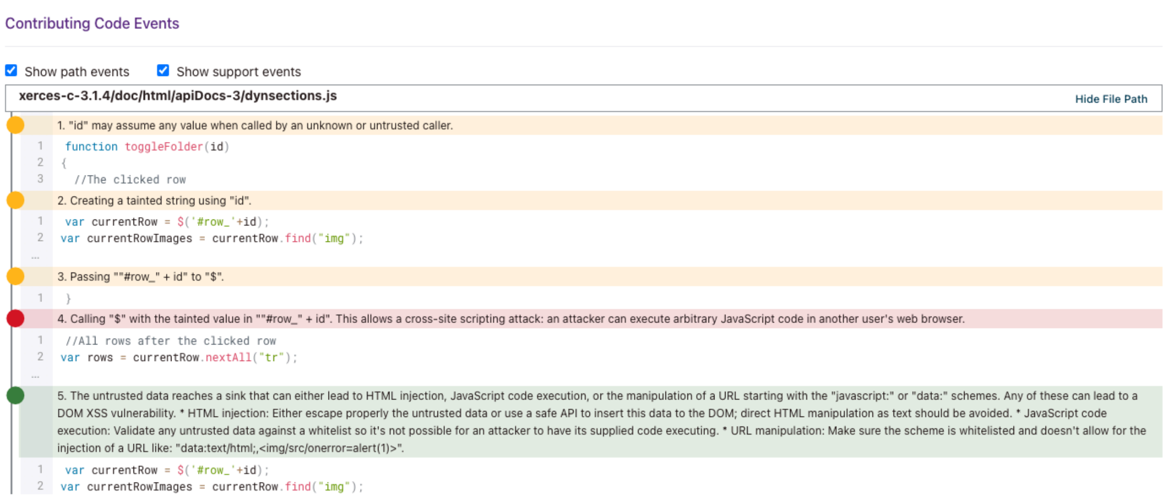


2. After narrowing the issue list to your desired results, click any issue in the list for a more detailed view.



The detailed view of the issue includes:

- A description of the issue and its local effects (i.e. the risk it poses when present in your code)
- A link to the Common Weakness Enumeration page, if any
- The name of the tool that discovered the issue
- Time of the test
- Contributing code events (snippet of the code where the issue was identified). Click "Show support events" to see what is contributing to the vulnerability.



Use the issue view whenever you need to dig into an individual issue.

Triage

There's more than one way to triage issues in Polaris. See Ways to triage in Polaris on page 39 for all the details

Get started: Application Admin

Before you begin, we recommend reading the following:

- Product Overview
- Subscriptions and Entitlements
- Roles and permissions on Polaris
- Polaris data model

Depending on the size of your organization, the applications and projects might already be set up by the Application Super User, or you might still have some work to do. This tutorial will give you an overview of all the tasks you might need or want to do as an Application Admin.

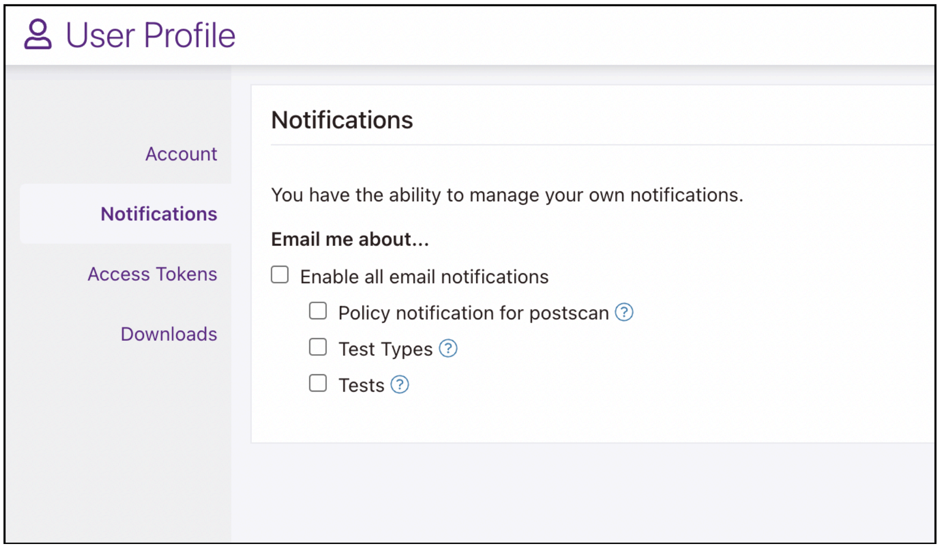
By the end of this tutorial, you will:

- Review your personal settings
- Add projects to your application
- Add members to your application
- Change the entitlements for an application
- Upload an application and start testing
- Monitor test results
- Filter and review issues
- Triage issues

Review your personal settings

1. Navigate to your personal settings by clicking on your profile name in the top right corner of the browser tab.
2. Select **Account** .
3. Verify your profile information and make changes if you wish.
4. Select **Notifications** from the left-hand navigation.

5. Review your notification settings.



Use Checkboxes to select the types of email notifications you'd like to receive.

(If you can't make changes, it means an Org Super User has turned off notifications for the organization. You won't be able to change settings and won't receive notifications.)

Create a project in your application

1. Navigate to **Applications**.
2. Click **Add Project**.
3. Complete the text fields.

Table 11: 'Add Project' fields

Field name	Description
Name	Must be unique within your organization.
Description	The description only needs to be useful to members of your organization.
Tags	Any applicable labels created by you to organize your applications and projects.

Add members to an application

1. From within the application, navigate to **Settings**.
2. Select Members on the left-hand navbar.
3. Use pull-down menus to choose a role and a new user.

Users must already be invited to the org before you add them to the project Application.

- For more about roles, see Roles and permissions on Polaris.

Note: For the first release, only Org-level roles will be available. Choose Org Super User or Application Super User.

4. Click **Save**.

Change the entitlements for an Application

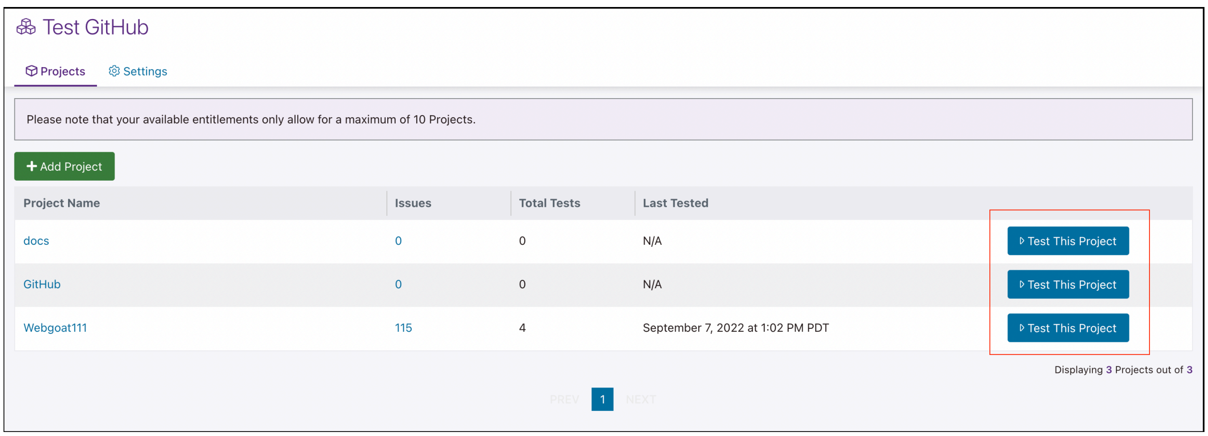
1. From within the Application, go to **Settings**.
2. Select Test Types from the let-hand navigation bar.
3. Use pulldown menus to select SAST and SCA entitlements.
4. You must choose both SAST and SCA for each Application
5. Click **Save**.

Upload files and start testing

Before uploading, see the limitations for uploads on the Support page. There are guidelines for file type and size.

To scan a project, you must first upload your files to Polaris. Here's how.

1. Navigate to **Portfolio**.
2. Select an application.
3. Choose a project from the project list and select **Test This Project** an the appropriate row.



4. Use pulldown menus to select the application and project.
5. Use checkboxes to select test types. (The options depend on what your App Super User has made available for the project.)
6. Submit the files you want to test by dragging and dropping into the browser window. Or click **browse files** and use the file chooser in your operating system to select files.
7. After the upload completes, click Begin Test.

   You can monitor the progress of tests any time by navigating to **Tests** on the left-hand navbar. Test status is shown there, with the most recent tests listed first, and you can filter by criteria such as when tests occurred, the type of test, and the project that it belongs to.

   Note: If it is the first scan for your project, you might receive email communications from the Synopsys team that require a response in order for testing to finish.

Monitor tests and get test results

1. Navigate to Tests in the left-hand navigation menu.

2. If numerous tests are showing, you might need to filter to see your test. First try filtering on test status, for new tests.

   Depending on the size of your project, a test may take a number of hours to finish running. When the test is complete the progress bar shows 100 percent and a green circle enclosing an arrow appears to the right of the progress bar on the Test List page.

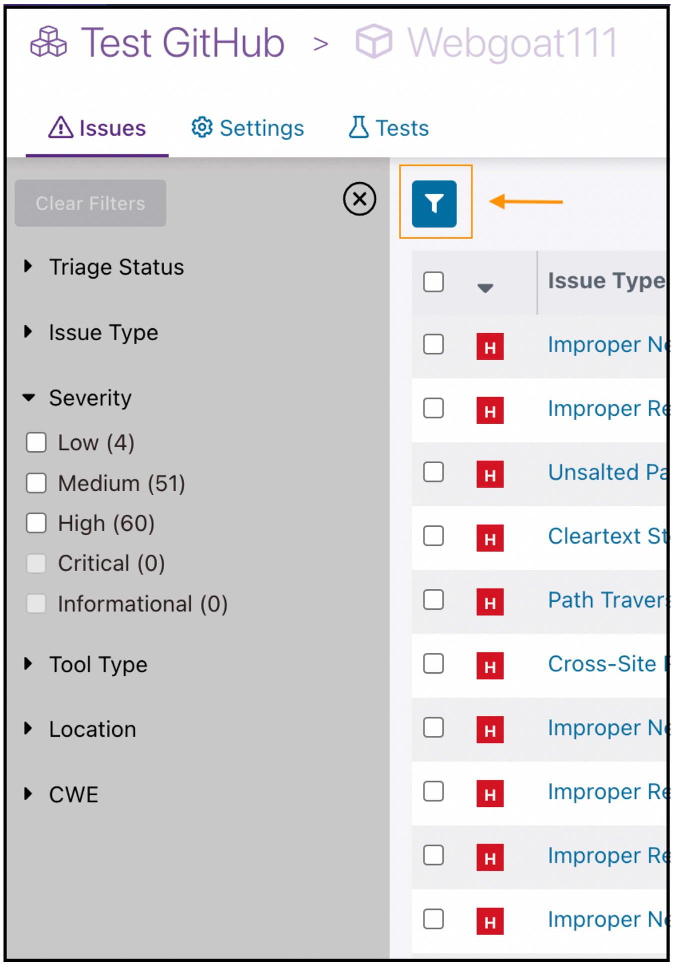
3. To see test results, click the arrow.

Filter and review the issues

You can get to the issues in either of the following ways:

- Select a test on the **Test List** page, to see the issues found in that test.
- Navigate to the project and then select the **Issues** tab.

1. To use filters, click the box with the funnel-shaped icon.



You can open each collapsible section and use checkboxes to indicate the kinds of issues you want to see. Try filtering the results according to issue type, severity, and triage status. (For example you might want to see all the un-triaged issues, or all that are un-triaged and high severity.)

2. After narrowing the issue list to your desired results, click any issue in the list for a more detailed view.

   The detailed view of the issue includes:

   - A description of the issue and its local effects (i.e. the risk it poses when present in your code)
   - A link to the Common Weakness Enumeration page, if any
   - The name of the tool that discovered the issue
   - Time of the test
   - Contributing code events (snippet of the code where the issue was identified)

   Use the issue view whenever you need to dig into an individual issue.

Triage

There's more than one way to triage issues in Polaris. See Ways to triage in Polaris on page 39 for all the details

Get started: Contributor

Before you begin, we recommend reading the following:

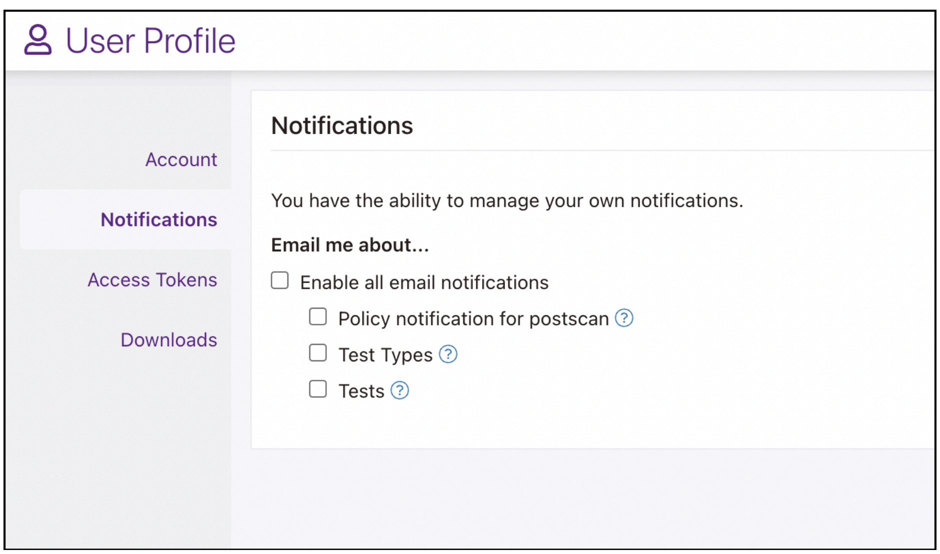
- Product Overview
- Subscriptions and Entitlements
- Roles and permissions on Polaris
- Polaris data model

By the end of this process, you'll complete the following tasks.

- Review user settings
- Upload an application and Create SAST and SCA tests
- Filter and review issues
- Triage issues

Review your personal settings

1. Navigate to your personal settings by clicking on your profile name in the top right corner of the browser tab.
2. Select **Account** .
3. Verify your profile information and make changes if you wish.
4. Select **Notifications** from the left-hand navigation.
5. Review your notification settings.



Use Checkboxes to select the types of email notifications you'd like to receive.

(If you can't make changes, it means an Org Super User has turned off notifications for the organization. You won't be able to change settings and won't receive notifications.)

Monitor tests and get test results

1. Navigate to Tests in the left-hand navigation menu.
2. If numerous tests are showing, you might need to filter to see your test. First try filtering on test status, for new tests.

   Depending on the size of your project, a test may take a number of hours to finish running. When the test is complete the progress bar shows 100 percent and a green circle enclosing an arrow appears to the right of the progress bar on the Test List page.

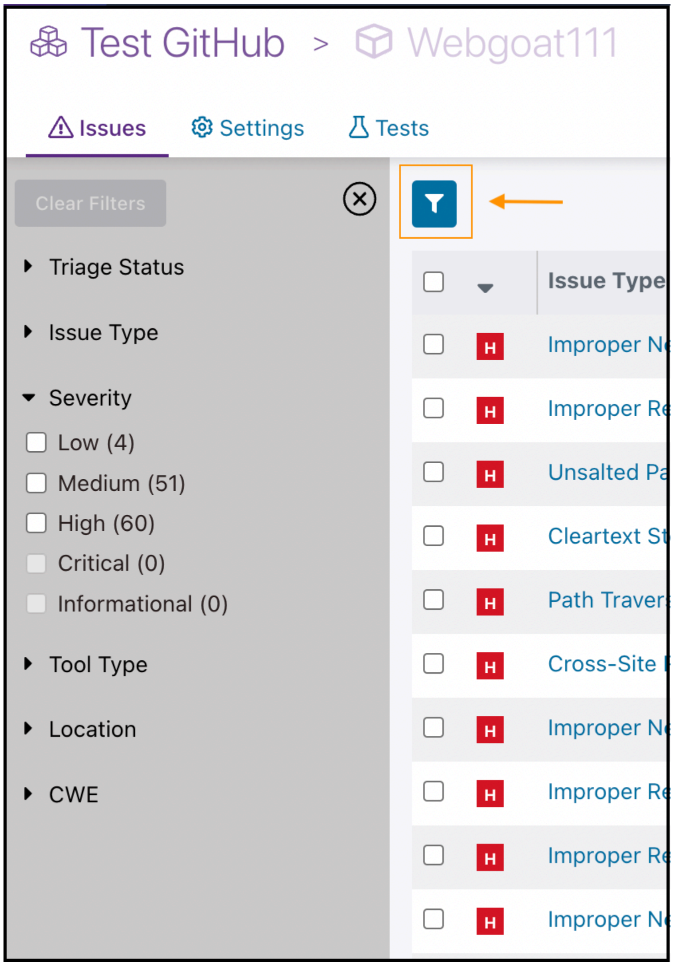
3. To see test results, click the arrow.

Filter and review the issues

You can get to the issues in either of the following ways:

- Select a test on the **Test List** page, to see the issues found in that test.
- Navigate to the project and then select the **Issues** tab.

1. To use filters, click the box with the funnel-shaped icon.



   You can open each collapsible section and use checkboxes to indicate the kinds of issues you want to see. Try filtering the results according to issue type, severity, and triage status. (For example you might want to see all the un-triaged issues, or all that are un-triaged and high severity.)

2. After narrowing the issue list to your desired results, click any issue in the list for a more detailed view.

   The detailed view of the issue includes:

   - A description of the issue and its local effects (i.e. the risk it poses when present in your code)
   - A link to the Common Weakness Enumeration page, if any
   - The name of the tool that discovered the issue
   - Time of the test
   - Contributing code events (snippet of the code where the issue was identified)

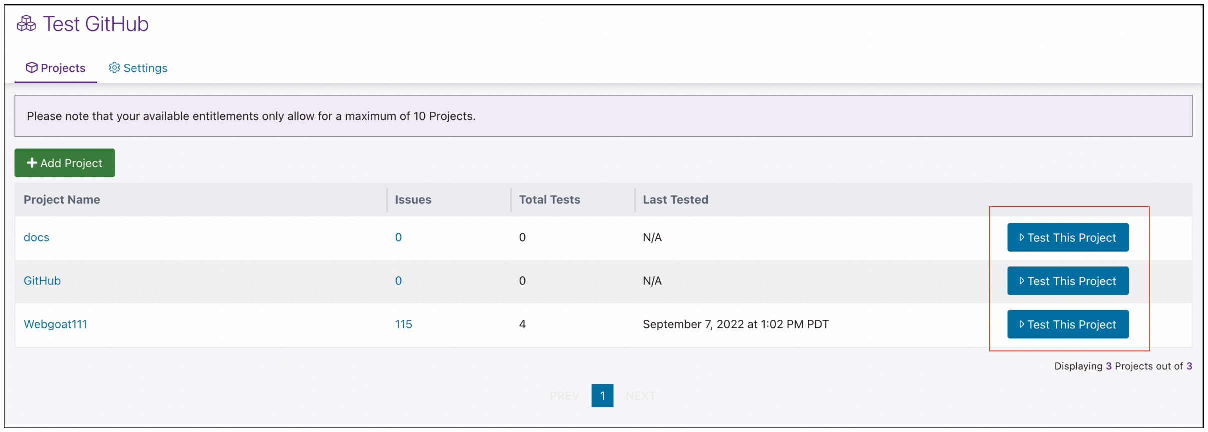
   Use the issue view whenever you need to dig into an individual issue.

Upload files and start testing

Before uploading, see the limitations for uploads on the Support page. There are guidelines for file type and size.

To scan a project, you must first upload your files to Polaris. Here's how.

1. Navigate to **Portfolio**.
2. Select an application.
3. Choose a project from the project list and select **Test This Project** an the appropriate row.



4. Use pulldown menus to select the application and project.
5. Use checkboxes to select test types. (The options depend on what your App Super User has made available for the project.)
6. Submit the files you want to test by dragging and dropping into the browser window. Or click **browse files** and use the file chooser in your operating system to select files.
7. After the upload completes, click Begin Test.

   You can monitor the progress of tests any time by navigating to **Tests** on the left-hand navbar. Test status is shown there, with the most recent tests listed first, and you can filter by criteria such as when tests occurred, the type of test, and the project that it belongs to.

   Note: If it is the first scan for your project, you might receive email communications from the Synopsys team that require a response in order for testing to finish.

Triage

There's more than one way to triage issues in Polaris. See Ways to triage in Polaris on page 39 for all the details

Get started: Observer

Before you begin, we recommend reading the following:

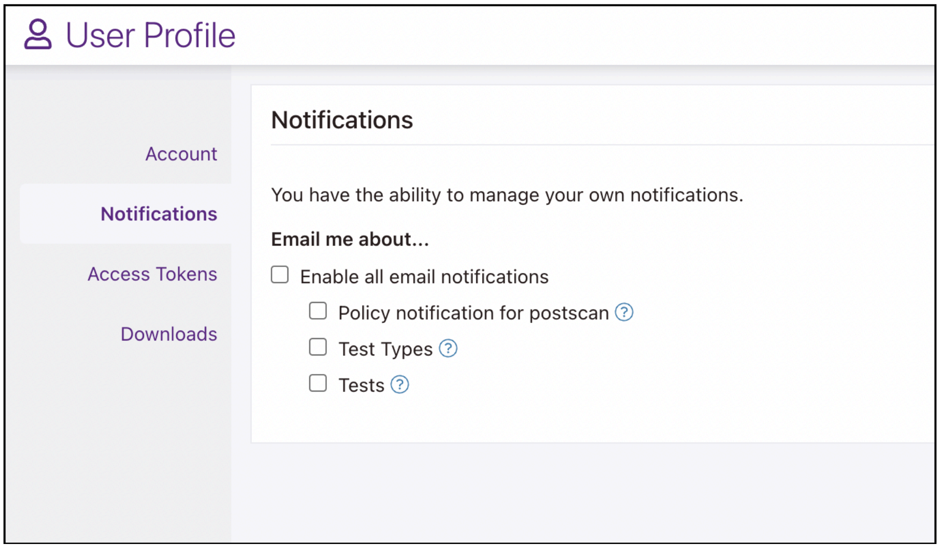
- Product Overview
- Subscriptions and Entitlements
- Roles and permissions on Polaris
- Polaris data model

By the end of this process, you'll complete the following tasks.

- Review user settings
- Upload an application and Create SAST and SCA tests
- Filter and review issues
- Triage issues

Review your personal settings

1. Navigate to your personal settings by clicking on your profile name in the top right corner of the browser tab.
2. Select **Account** .
3. Verify your profile information and make changes if you wish.
4. Select **Notifications** from the left-hand navigation.
5. Review your notification settings.



Use Checkboxes to select the types of email notifications you'd like to receive.

(If you can't make changes, it means an Org Super User has turned off notifications for the organization. You won't be able to change settings and won't receive notifications.)

Monitor tests and get test results

1. Navigate to Tests in the left-hand navigation menu.
2. If numerous tests are showing, you might need to filter to see your test. First try filtering on test status, for new tests.

   Depending on the size of your project, a test may take a number of hours to finish running. When the test is complete the progress bar shows 100 percent and a green circle enclosing an arrow appears to the right of the progress bar on the Test List page.

3. To see test results, click the arrow.

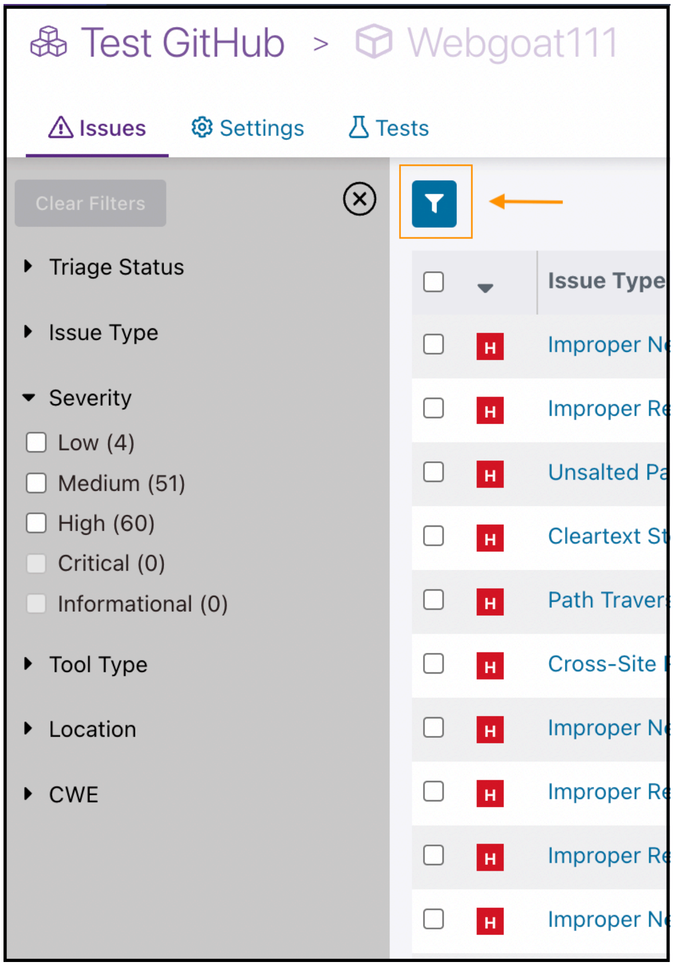
Filter and review the issues

You can get to the issues in either of the following ways:

- Select a test on the **Test List** page, to see the issues found in that test.

- Navigate to the project and then select the **Issues** tab.

1. To use filters, click the box with the funnel-shaped icon.



You can open each collapsible section and use checkboxes to indicate the kinds of issues you want to see. Try filtering the results according to issue type, severity, and triage status. (For example you might want to see all the un-triaged issues, or all that are un-triaged and high severity.)

2. After narrowing the issue list to your desired results, click any issue in the list for a more detailed view.

   The detailed view of the issue includes:

   - A description of the issue and its local effects (i.e. the risk it poses when present in your code)
   - A link to the Common Weakness Enumeration page, if any
   - The name of the tool that discovered the issue
   - Time of the test
   - Contributing code events (snippet of the code where the issue was identified)

   Use the issue view whenever you need to dig into an individual issue.

How-to

How-do-I: Org-level users

How-do-I

This page contains quick instructions for a number of tasks that you might want to find.

Question	Who	Location	How to do it
Change my personal notification settings	Any user	**Account** > **Notifications**	**1.** Use Checkboxes to select the types of notifications you'd like to receive. **2.** If all the checkboxes are disabled, it means the Org Super User has turned off notifications for the organization. If you made selections before notifications were disabled, they are saved and will be applied if notifications are enabled in the future.

Question	Who	Location	How to do it
Create an application	Org Super User Application Super User	**Portfolio**	1. Click **Create Application**. 2. Click the Step One tab and enter the necessary application details. 3. Click on the Step Two tab. And choose the entitlements and subscription associated with the application. 4. Click **Finish**. 5. Create any projects that should be included in the application.
Create an individual new user	Org Super User	**MyOrganization** > **Users**	1. Go to **MyOrganization** > **Users** and click **Create New User**. 2. In the Create New User Page, complete the fields for Name, Email, Global Role and Groups. 3. Click Create.
Disable notifications	Org Super User	**My Organization** > **Notifications**	Uncheck the box that says **Enable email notifications for all users**
Give a user an org-level role or update information	Org Super User	**MyOrganization** > **Users**	Select a user to modify.

Question	Who	Location	How to do it
Deactivate a user	Org Super User	**My Organization > Users**	Move the toggle under the **Status** column to the left. Deactivated users will be listed as **Inactive** and appear greyed-out. They will not be able to access your Organization's Polaris.
Export Issues to Downloand as a CSV or JSON files	Any user	**Tests>Select Project>Issue List**	**1.** From Issues List, select individual issues or skip to 2 and use "Export All". **2.** Click "Export 1 Selected" (how many selected issues will appear on button) or "Export All". **3.** Under **Export to:** select File. **4.** From **File Type:** pulldown select either CSV or JSON. **5.** Click **Export** button.
View Assessor Comments	Any user	**Test**	Under **Test Status**, click on number next to the comment icon.
Export Audit Logs	Org Super User	**My Organization->Audit Logs**	Filter by Date Range, Event Type and/or User's Email. Click **Export.**

Integrate a Repository

Source Code Management (SCM) Repository integrations on Polaris supports the following:

- GitHub
- GitHub Enterprise
- GitLab

Git integrations allow users to run scheduled SAST + SCA scans on a daily or weekly basis. Users may also choose to run tests on-demand using the UI. When new issues/vulnerabilities are found, the user gets an email to manually action the issue or to manually apply the following

- SCA: Upgrade or Patch guidance
- SAST: Newly disclosed vulnerabilities

Note: This integration is on a project level / one repository per project.

Steps for Integrating a single SMC Repository to a Project

This allows you to select the repository when creating a new test for the project, see . . Only one repository can be used per project.

1. From Application, select a Project and navigate to Settings > Integrations.
2. Select the repository source type: GitHub, GitHub Enterprise, or GitLab.
3. Enter the Repository URL.
4. Enter the Repository Access Token.

   Depending on your choice for source above, you will need to generate an access token then paste it into the text field. Instructions for generating access tokens can be found in the GitHub, GitHub Enterprise and GitLab online documentation. The scope settings you select for the access token should allow repository access.

   For example, this link describes how to create a GitHub personal access token. Following is an example token:

   ```
   ghp_b8vffEJBcAwSO4JJv0y3FzKoivuEo71d4DaX
   ```

   For GitHub Enterprise, here.

   For GitLab, here.
5. Click **Test your Connection**. A spinning circle indicates the test is in progress.
6. Once the test is complete, you should either see either a green checkbox and text indicating a successful connection, or a circled red X and text indicating an unsuccessful connection.

   If your connection is unsuccessful, check the following:

   a. Make sure you have a good network connection.
   b. Check the repository URL and Repository Access Token to make sure they are accurate.
7. If your connection is successful, click **Save**, or use Cancel to cancel the setup.
8. You can then scan on demand (see Select files and start testing) or schedule automatic testing (weekly or daily), see Test Frequency Policies.

How to Test

See Ways to triage in Polaris on page 39 for details about these selection methods.

Select files and start testing

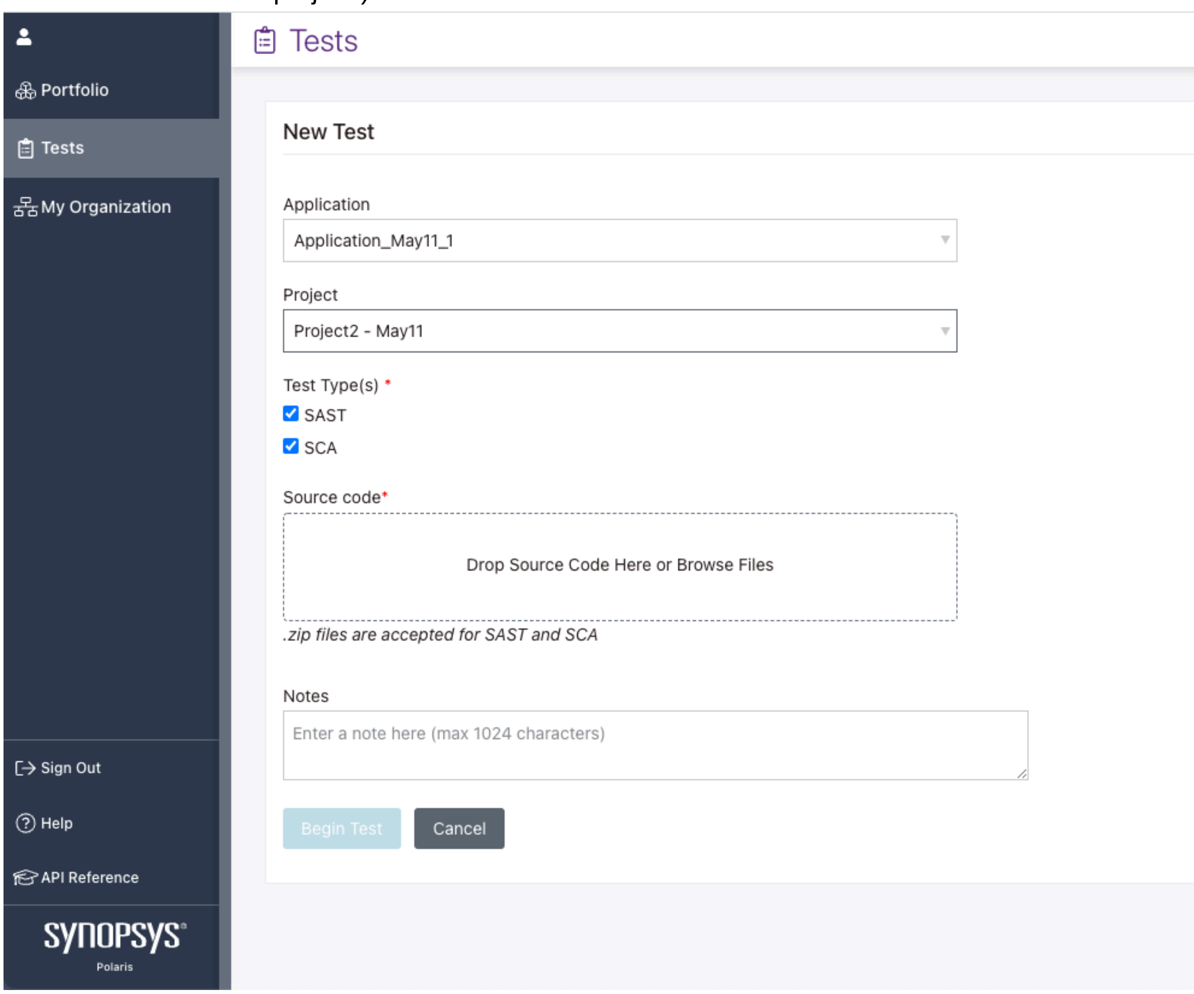
Before uploading, see the limitations for uploads on the Support page. There are guidelines for file type and size.

To scan a project, you must first upload your files to Polaris. Here's how.

1. There are two ways to start a test

- Go to **Portfolio**>**Application**>**Projec**t and click **Run a Test**.
- Go to **Tests**>click **New Test** button.

2. On **New Test** page, choose the Application and Project you want to test from pulldowns.
3. Use check-boxes to select **Test Type(s)**. (The options depend on what your App Super User has made available for the project.)



4. Use the check-boxes to select a source code location. You can either:
   a) Select **Code Upload**. Submit the files you want to test by dragging and dropping into the browser window. Or click **browse files** and use the file chooser in your operating system to select files.
   b) Select **Repository** then test your connection. If this option is not available, see Integrate a Repository on page 37.
5.
6. After the upload or repository connction completes, click **Begin Test**.

   You can monitor the progress of tests any time by navigating to **Tests** on the left-hand navbar. Test status is shown there, with the most recent tests listed first, and you can filter by criteria such as when tests occurred, the type of test, and the project that it belongs to.

   Note: If it is the first scan for your project, you might receive email communications from the Synopsys team that require a response in order for testing to finish.

Ways to triage in Polaris

In the issue list you can triage issues in several ways:

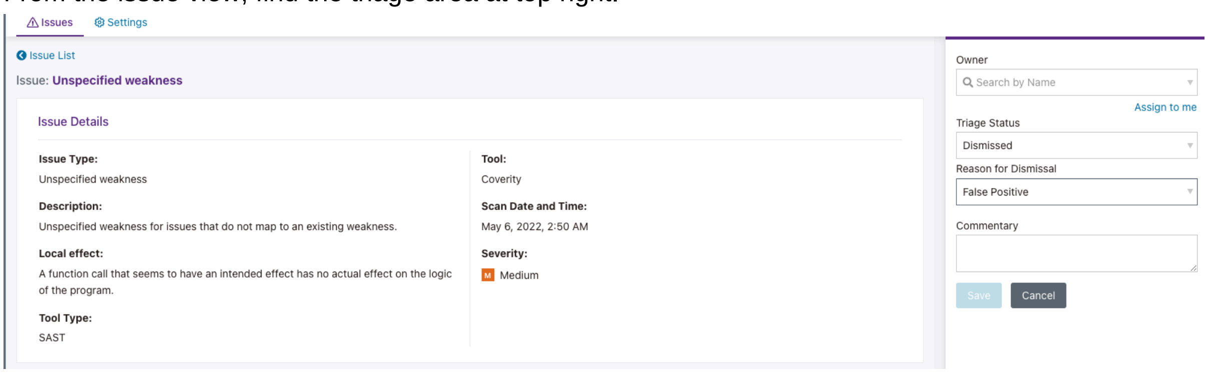
- Triage individual issues
- Batch triage by manually selecting multiple issues
- Batch triage by filtering
- Triage all

You'll need to use all of these, so we explain each approach in this page.

Triage individual issues

You might decide to review an issue independently to decide whether to dismiss it. In such cases, you can triage a single issue from within the issue view.

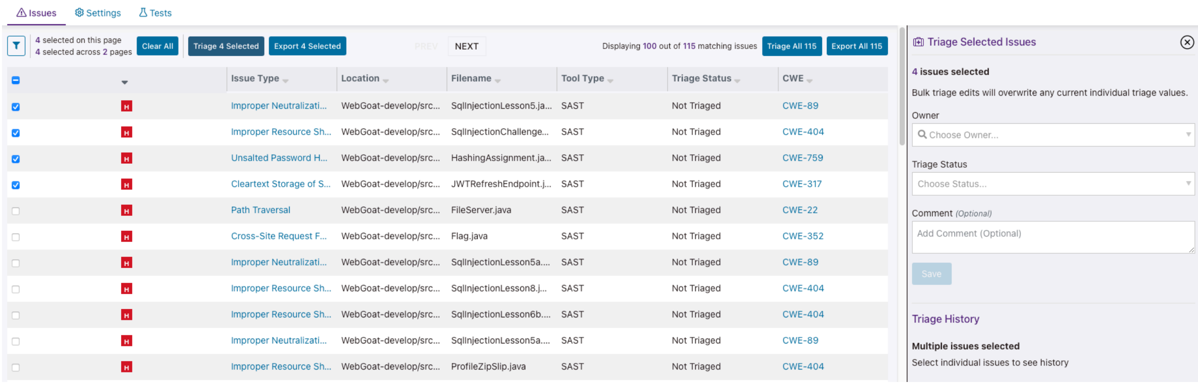
1. From the issue list, select an individual issue to review and triage.
2. From the issue view, find the triage area at top right.



3. In the **Owner** field, assign yourself or search by name to designate another member of the project.
4. Choose a **Triage Status** from the pulldown menu.
5. If the Triage Status is **Dismissed**, choose a reason from the **Reason for Dismissal** pulldown menu.
6. Enter a comment in the text box if you want to explain the reason for the status you chose. This is optional.
7. Click **Save**.

Batch triage by manually selecting multiple issues

1. From the issue list, check the box on the left margin next to all the relevant issues.



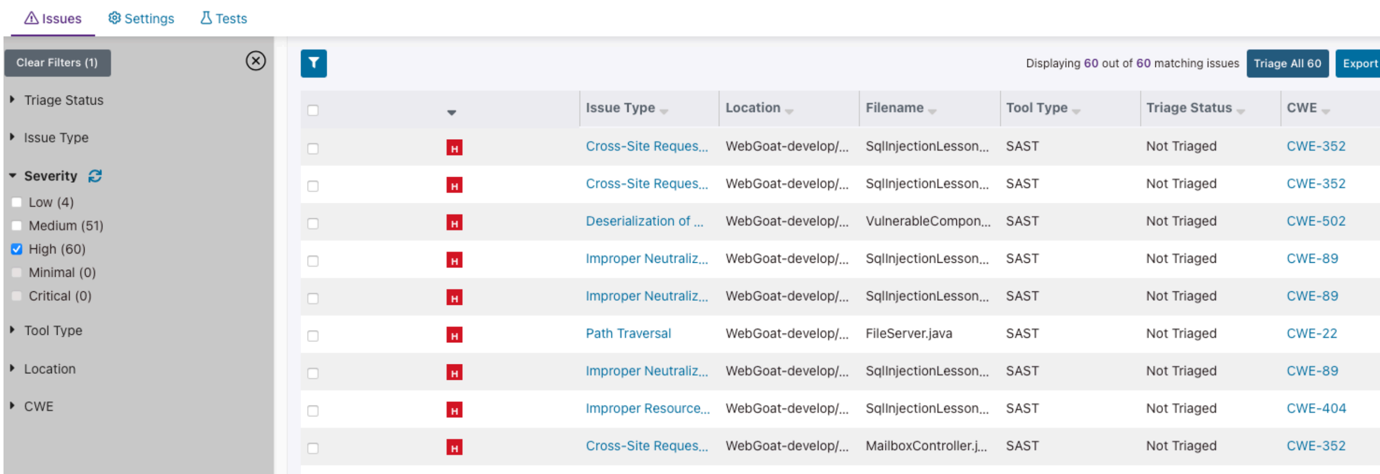
2. Click **Triage Selected**.
3. In the **Owner** field, assign yourself or search by name to designate another member of the project
4. Choose a **Triage Status** from the pulldown menu.
5. If the Triage Status is Dismissed, choose **Reason for Dismissal** from pulldown menu.
6. Enter a comment in the text box if you want to explain the reason for the status you chose. This is optional.
7. Click **Save**.
   The triage status and comments are applied to all selected issues.

Batch triage by filtering

You can triage batches of issues either by filtering or by selecting them manually.

1. Select a group of issues from the issue list by filtering.

   To filter, use the pull-down menus at the top of the page to choose issues according to issue type, severity, and triage status. (For example you might want to see all the un-triaged issues, or all that are un-triaged and high severity.) If you don't set any filters, you can triage all issues in the list.



   Note that each choice in the pulldown menu is followed by a number – This tells you how many issues you are selecting when you check the box. If the number is zero, there are no issues to select.

2. Click **Triage All** . In this example there are 60.
3. In the **Owner** field, assign the issues to yourself or search by name to assign another member of the project.
4. Choose a **Triage Status** from the pulldown menu.
5. If the Triage Status is Dismissed, use the **Reason for Dismissal** pulldown menu to choose a reason.
6. Enter a comment in the text box if you want to explain the reason for the status you chose. This is optional.
7. Click **Save**.
   The triage status and comments are applied to all selected issues.

How to Export Issues

In the issue list you can export issues to file (CSV/JSON) or Jira :

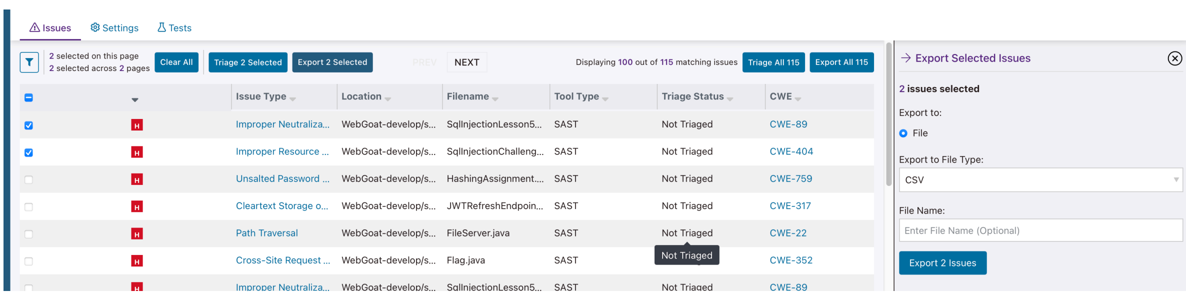
- Export individual issues
- Batch triage by manually selecting multiple issues
- Batch triage by filtering
- Export all

See Ways to triage in Polaris on page 39 for details about these selection methods.

Export Issues to Download as a CSV or JSON files

.

1. Select issue or issues.



2. Under **Export to:** select File.
3. From **File Type:** pulldown select either CSV or JSON.
4. Click **Export** button.

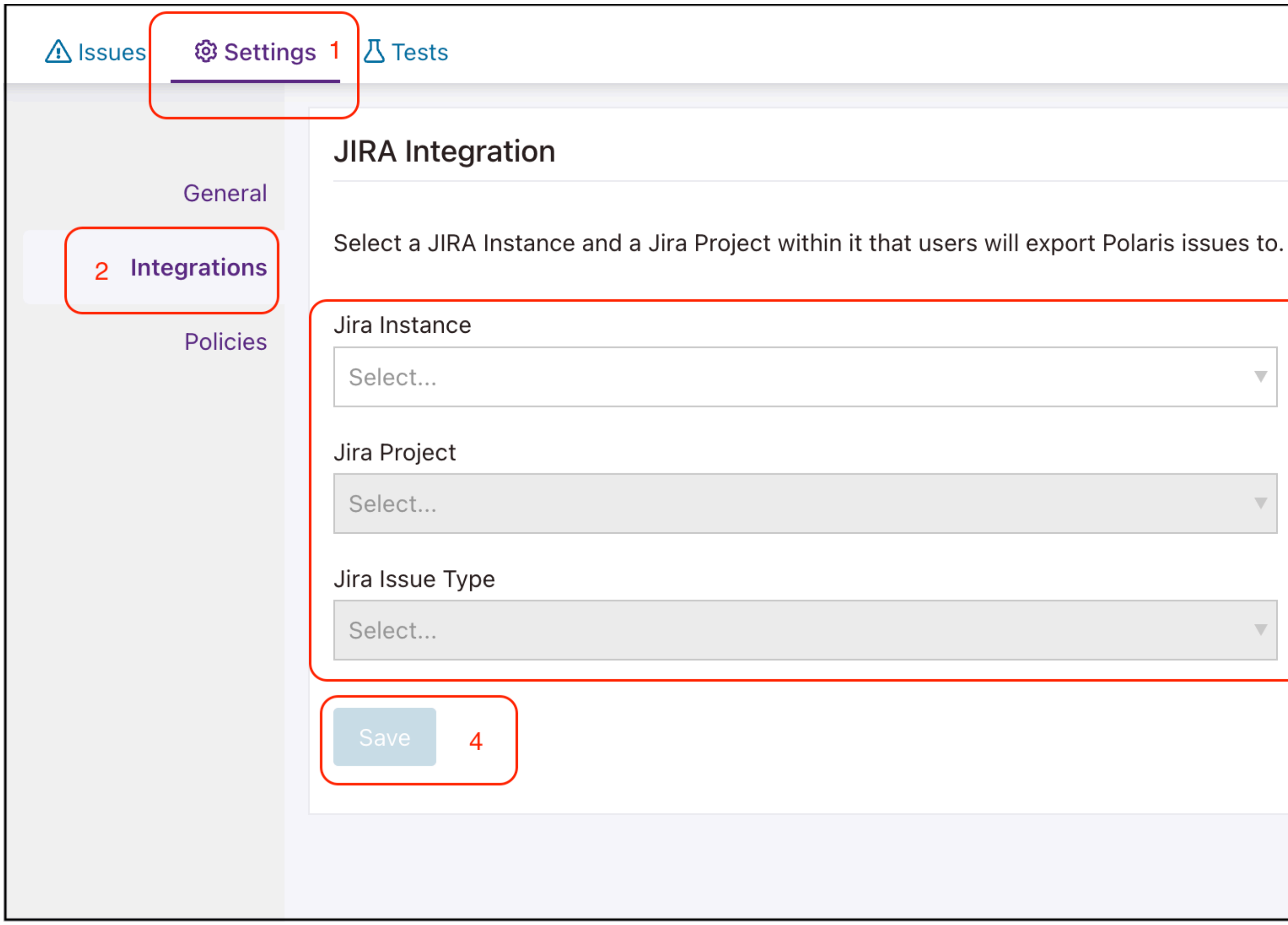
Set up Jira in an individual Project

Before members of your team can export issues to Jira, your Polaris project must be associated with a Jira instance and with a single Jira project within that instance. A Polaris Org Admin can set up Jira exports in the project.

Note: Setup in individual projects is only possible after the organization administrator has set up the integration with Jira.

1. **In the Polaris UI, navigate to Portfolios by clicking the logo at the top left. Then open your application and select a project.**

2. **Click Settings on the top menu, and then select Integrations from the left-hand navbar.**
3. **Use the Jira Instance pull-down menu to select the Jira instance.**
4. **Then use the Jira Project text box to select a project. (It will offer choices after you start to type.)**
5. **Use the Jira Project Issue Types pulldown menu to select an issue type.** All issues exported to Jira will have the type chosen here.



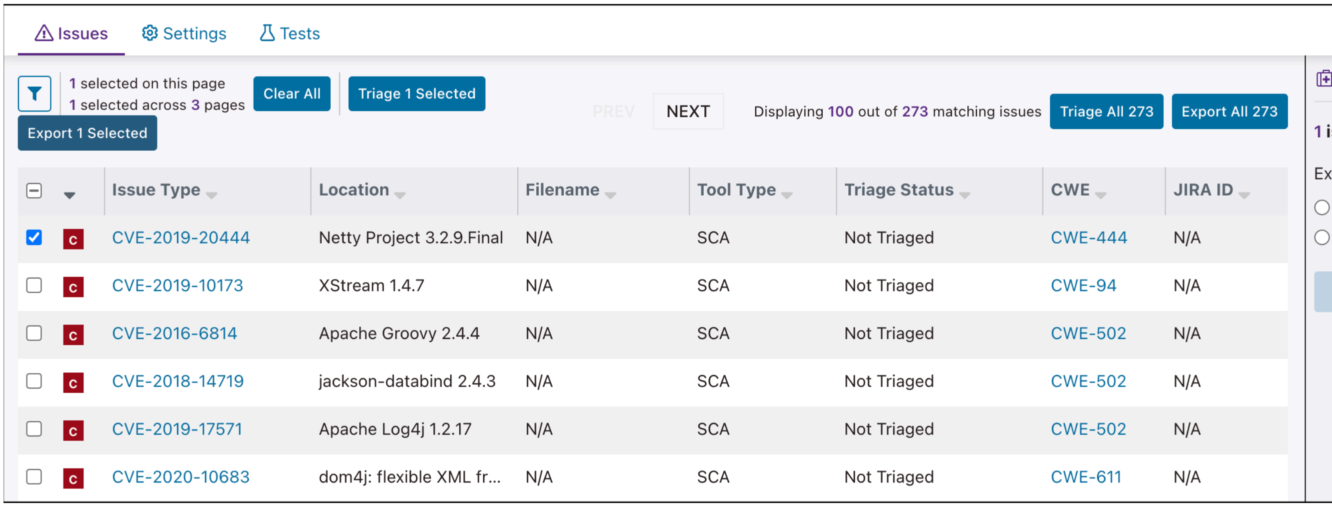
6. **Click Save** This sets the Jira instance and project that issues will be exported to. Project admins can edit these settings.

How to export issues to Jira

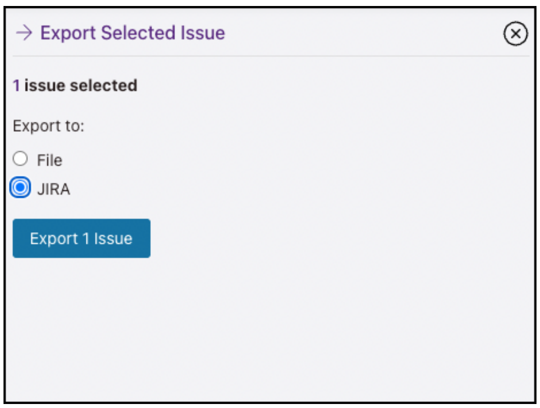
You can export one issues at a time to Jira, if your organization uses a Jira integration and if the project is set up to use Jira.

You can export individual issues from within the issue view. The issue will be exported to the Jira project associated with your Polaris project and in the issue type specified in your settings.

1. From the issue view in Polaris, select one individual issue for which you would like to open a Jira ticket.



2. Select **Export 1 Selected**.
3. In the **Export Selected Issue** pane, on the right-hand margin, select **Jira**.



4. Click **Export 1 issue**.

Reference

Release Notes

Everything that's new in Polaris

Beta release

- For the Beta release, Polaris won't recognize your email address if you use uppercase letters when signing in. Remember to use all lowercase.
- See the Support Information page for limitations regarding upload size and file formats.
- All users will be assigned the Org Super User role for the Beta release. Additional roles will become available in a subsequent release.

- It's possible for an Org Super User to delete himself or herself. If you have only one Super User and that person leaves the organization or gets deleted, Synopsys can invite another person to be the Organization Super User. Open a support request.
- It's not possible to open a case on the Synopsys Community for this product during the Beta program. For support, address an email to **polarisbeta@synopsys.com**.com. For more info, see Need more help?

Polaris support information

Supported platforms

Polaris APIs are compatible with any operating system and hardware that can connect to the Polaris server or APIs via HTTPS.

Browser support

The Polaris web UI can be accessed using a variety of browsers.

Browser	Versions	Provider
Firefox	Latest and latest - 1	Versions supported by Mozilla
Google Chrome	Latest and latest - 1	Versions supported by Google
Microsoft Edge	Latest and latest - 1	Versions supported by Windows 10
Safari	Latest and latest - 1	Versions supported by Apple

NOTE: Internet Explorer is not supported.

Table 12: Supported file types and tests

Name	Description
Languages	• Java • JavaScript • C# • Python • PHP • Ruby

Name	Description
Package managers	• Gradle • Maven • NuGet
On-demand test types	• SAST static application security testing • SCA software composition analysis

Table 13: Upload limitations

Type	Size limits
Single file	1 GB
ZIP file	2 GB
Maximum file count	20,000 files

Terms and definitions for Polaris

Application
A collection of up to five projects. The application is the organizing principal in Polaris. Code projects have to be part of an application, and members are associated with one or more applications, where they're allowed to test and view results.

Application Admin
Manages access and settings for the application. The Application Admin doesn't automatically have admin permissions or even membership in other apps.

Application Contributor
Frequently scans code and triages issues.

Application Observer
Able to review and monitor ongoing tests, test results, issues in all projects belonging to the application, and dashboard showing the status of the application and its projects.

Audit Log
Tracks system changes from the user interface and APIs.

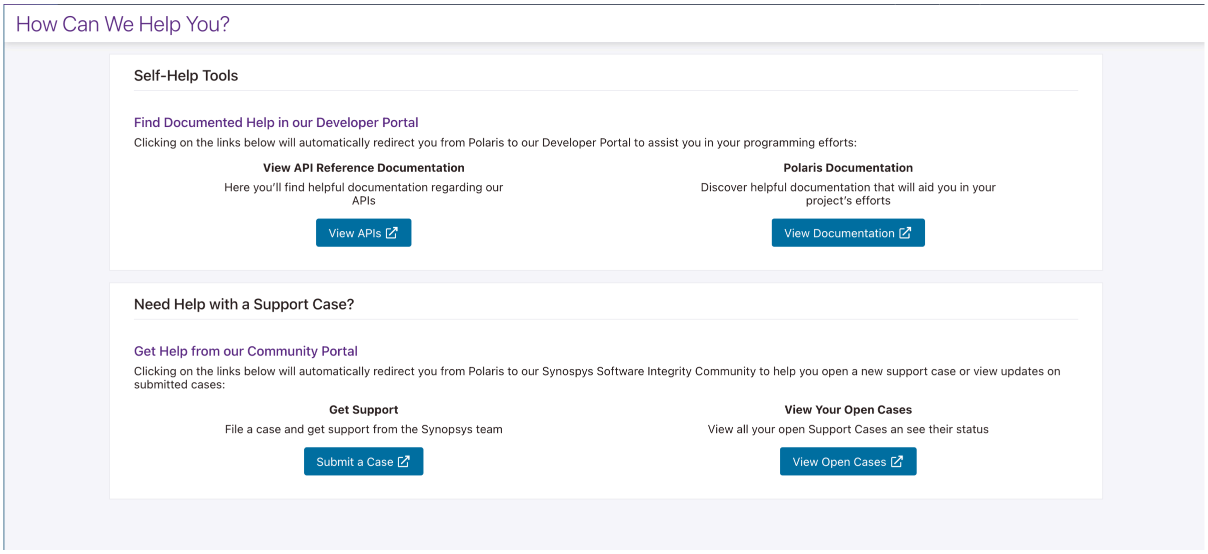
CVE
Common vulnerabilities and exposures. A system that provides reference numbers to publicly known information security vulnerabilities. Maintained by the National Cybersecurity FFDRC.

CWE/SANS
Common weakness enumeration. A list of frequently occurring defects in software and

	hardware security, maintained by the National Cybersecurity FFDRC.
entitlement	The ability to use a specific type of test or set of tests on a particular project. Your organization purchases entitlements so its members will be able to run tests.
issue	Any defect or vulnerability in software. Usually used to describe issues detected by a test.
Application Super User	The member of an organization who can create, delete, and modify applications. The Org Application manager has access to all applications and projects in an organization.
Org Super User	The member of your organization who has access to all the functions of Polaris and can access all the applications and projects. An Org Super User sets up your organization and invites other members to begin using Polaris. An organization must have at least one Org Super User.
OWASP	Open Web Application Security Project. A non-profit foundation that focuses on application security.
Project	A project is a discrete body of code that is also a subcomponent of a larger codebase. It might correspond to one repository, but it doesn't have to. Tests run against projects, and the resulting issues accumulate in the dashboard for that project.
SAST	Static analysis security testing. A solution that analyzes source code without executing it and finds security vulnerabilities. Coverity is one example a SAST tool.
SCA	Software composition analysis. SCA describes solutions that scan code and detect the presence of known software libraries written either by open-source projects or vendors. After scanning code, an SCA application helps to manage any security, quality, and license compliance risks associated with the libraries it discovered.
test	Execution of a tool or the attempt to execute a tool in Polaris.
triage	Involves the decision to dismiss an issue, or not. When issues are dismissed by a member of your team, the potential reasons are False Positive, Intentional, and Other (requires an explanatory comment).

Still need help?

Contact Synopsys Customer Support



If you have questions or need support, click the help icon at the top right from anywhere in the Polaris app: ?

From the help window, you can open a support ticket, monitor support tickets, find documentation, or go to the Synopsys Community.

Use the Polaris app to sign into resources on the Help page

When you sign into the Polaris app, you can access the following resources without signing in a second time:

- SIG Support
- Synopsys Community

For best results, always sign into the app and use the help icon when you want to go to one of the resources in the list above. You won't be required to sign into those other resources. If you already have an account at one of those sites, *using the same email that you use to sign into Polaris*, all your existing issues and messages will still be there.

Synopsys support can help if you have issues with accounts that you think should be linked, but that aren't

Note the following:

- Polaris credentials don't work when typed into the sign-in fields on Synopsys Community. (Unless you have used the same password for all your accounts — which you should not do.)
- Changing your password in Polaris doesn't change your password on the Synopsys Community site.

Roles and permissions

Roles and Permissions in your organization are divided into two levels: global and application.This pages describes all the roles, and what they are allowed to do.

Global roles

- *Org Super User* — The person who sets up your organization's Polaris account and manages users and groups within it. Each organization has at least one Organization Super User. If that superuser leaves the organization, Synopsys admins can invite another person to be the Organization Super User.
- *Application Super User* — Has full access to all applications within the organization.
- *No global permissions* — Most users don't have global-level permissions, but receive application-level permissions from an Application Admin.

Application roles

- *Application Admin* — The owner of one or more applications.
- *Contributor* — A member of an application, usually someone who frequently tests code.
- *Observer* — Is able to monitor all the information related to a project, but cannot run tests and triage issues.

Roles and permissions tables

Table 14: Global roles and permissions

	Global roles			
	Organization Super User	**Application Super User**	**No global role**	**Notes**
My Organization				
Access this area		✗	✗	
Add and edit users	✓	✗	✗	
Manage global notification settings	✓	✗	✗	
Applications				
Access this area	✓	✓	✓	
View all Applications in the organization	✓	✓	✗	
View only Applications of which they are a member	⊖		✓	Organization Super Users and Application Super Users are, by default, members of all Applications in the Organization.
Create new Applications (including changes to Entitlements)	✓	✓	✗	

	Global roles			
	Organization Super User	**Application Super User**	**No global role**	**Notes**
Edit Applications (Members, Projects, Settings)	✔	✔	✖	
Tests				
Access this area	✔	✔	✔	
View all tests in the organization	✔	✔	✖	
View only tests from Projects in which they are a member of the parent application	⛔		✔	*Organization Super Users and Application Super Users are, by default, members of <u>all</u> Applications in the Organization.*
Start, stop, and modify a test.	✔	✔	✔	*Depends on their Application Role – Admins and Contributors can start, stop, and modify tests for the Application.* Observers cannot.
User profile				
Can Access this area	✔	✔	✔	
View and edit account	✔	✔	✔	
Reset password	✔	✔	✔	*The notification types (Applications, Entitlements, Tests) will depend on the Application Role(s) the user holds.*
Application role				
Can be an Administrator	✔	✔	✔	
Can be a Contributor	⛔		✔	
Can be an Observer			✔	Organization Super Users and Application Super Users are automatically assigned Application Administrator privileges for all Applications in their Organization; therefore, they cannot hold a lesser role for an Application

Table 15: Application-level permissions

	Application role		
	Application Administrator	**Contributor**	**Observer**
Summary			
Can access this area	✓	✓	✓
Projects			
Can access this area	✓	✓	✓
Create new Projects	✓	✗	✗
View all Projects in the Application	✓	✓	✓
View Project summary	✓	✓	✓
View Project issues	✓	✓	✓
Triage issues (bulk triage, assign issue owner, change triage status, comment)	✓	✓	✗
View Project settings	✓	✗	✗
Edit Project name and description	✓	✗	✗
Settings tab			
Can access this section	✓	✗	✗
Edit Application name	✓	✗	✗
View and manage members	✓	✗	✗
View and renew Subscriptions and Entitlements	✓	✗	✗
Delete the Application	✓	✗	✗