Fortify On Demand Uploader Plugin

Plugin Information
View Fortify on Demand on the plugin site for more information.

Older versions of this plugin may not be safe to use. Please review the following warnings before using an older version:

- SSRF vulnerability
- Credentials stored in plain text

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. The Fortify on Demand Plugin enables users to upload code directly from Jenkins for Static Application Security Testing (SAST). This plugin features the following tasks:

Run a static assessment for each build triggered by Jenkins.
Monitor scan completion and poll for results. If the results do not meet the application security policy as set by the organization, the build can be marked as failed or unstable.

This plugin requires a Fortify on Demand account. For more information on Fortify on Demand and to request a free trial, go to https://software.microfocus.com/en-us/software/fortify-on-demand

This plugin is maintained by the Fortify on Demand team. If you have any issues, or enhancement requests or would like to contribute to the code please let us know through the GitHub Issues page.

Installation

Note: If your Jenkins server requires a proxy for web access, in the Jenkins Dashboard, select **Jenkins > Manage Jenkins > Manage Plugins**. Select the **Advanced** tab and configure your proxy settings.

1. Select the **Available** tab.
2. In the **Filter** search box, type “Fortify on Demand Uploader.” The plugin list refreshes with Fortify on Demand Uploader.
3. Select the plugin and click **Download now and install after restart**.

Setup

Create an API Key Pair or a Personal Access Token in Fortify on Demand

The Fortify on Demand Plugin connects to Fortify on Demand through the Fortify on Demand API. Authentication requires an API key and secret pair or a personal access token.

- To create an API key and secret pair: Within Fortify on Demand, navigate to the Settings page under the Administration view, and then to the **API** tab. Create an API key with the Start Scans permission. Make sure to copy the secret as it is only shown once.
  Note that only Security Leads can create API keys.
- To create a personal access token: Within Fortify on Demand, select your account name > **Personal Access Tokens**. Create a personal access token with the api-tenant scope. Make sure to copy the token as it is only shown once.

Generate a Build Server Integration (BSI) Token in Fortify on Demand

Within Fortify on Demand, navigate to the application release that you wish to assess, and then to the Static Scan Setup page. Configure the static assessment settings and the BSI token will be automatically generated. Make sure to save the settings.

Note that this procedure requires a user role with the Start Static Scans-Configure permission.

Configure Global Authentication Settings

1. In the Jenkins Dashboard, select **Jenkins > Manage Jenkins > Configure System**.
2. In the **Fortify on Demand** section, provide your data center's domain URL and API root URL.
3. Select the method of authentication:
   - **Use API Key for authentication**: Provide the API key and secret.
   - **Use Personal Access Token for authentication**: Provide your account username, your personal access token, and the tenant ID.
4. Click **Test Connection**. If the authentication is successful, a success message will appear.

Configure Fortify on Demand Static Assessment Tasks

The Fortify on Demand Plugin supports freestyle projects and pipelines.

Configure a Freestyle Project

The plugin adds the Fortify on Demand Static Assessment and Poll Fortify on Demand for Results post-build tasks.

1. In a freestyle project, click **Configure**.
2. In the **Post-build Actions** section, click **Add post-build action** and select **Add Fortify on Demand Static Assessment**.
3. Complete the following fields:

Field	Description
BSI Token	Provide the BSI token.
Configure Personal Access Token (optional)	Select this option to override the global authentication settings. Provide your account username, your personal access token, and the tenant ID.
Entitlement Preference	Select the entitlement preference: **Single Scan** or **Subscription**.
Purchase Entitlements (optional)	Select the check box to purchase an entitlement if the feature is enabled.
Bundled Assessment (optional)	Select the check box to specify the assessment is a part of a bundled assessment.
Prefer Remediation if Available (optional)	Select the check box to run a remediation scan if one is available.
Include all project files	Select the check box to include all project files in the zip file.

4. Click **Add post-build action** and select **Poll Fortify on Demand for Results.** Complete the following fields:

Field	Description
BSI Token	Provide the BSI token.
Configure Personal Access Token (optional)	Select this option to override the global authentication settings. Provide your account username, your personal access token, and the tenant ID.
Polling Interval	Type the length of time in minutes between polling Fortify on Demand to check if the scan has completed.
Action if Failing Security Policy	Select whether to take no action or mark the build as Failed or Unstable based on the application security policy as set by your organization.

5. Save the settings.

Configure a Pipeline

The Fortify on Demand Plugin adds the fodStaticAssessment and fodPollResults tasks. Use the Snippet Generator to create code for these tasks.

Note: The Pipeline Plugin needs to installed.

1. In a pipeline, click **Configure**.
2. In the **Pipeline** section, click **Pipeline Syntax**.
   The Snippet Generator appears.
3. Select **fodStaticAssessment** in the **Sample Step** list.
4. Complete the following fields:

Field	Description
BSI Token	Provide the BSI token.
Configure Personal Access Token (optional)	Select this option to override the global authentication settings. Provide your account username, your personal access token, and the tenant ID.
Entitlement Preference	Select the entitlement preference: **Single Scan** or **Subscription**.
Purchase Entitlements (optional)	Select the check box to purchase an entitlement if the feature is enabled.
Bundled Assessment (optional)	Select the check box to specify the assessment is a part of a bundled assessment.
Prefer Remediation if Available (optional)	Select the check box to run a remediation scan if one is available.
Include all project files	Select the check box to include all project files in the zip file.

5. Click **Generate Pipeline Script.** Copy the code and add it to your pipeline script.
6. Select **fodPollResults** in the **Sample Step** list.
7. Complete the following fields:

Field	Description
BSI Token	Provide the BSI token.
Configure Personal Access Token (optional)	Select this option to override the global authentication settings. Provide your account username, your personal access token, and the tenant ID.
Polling Interval	Type the length of time in minutes between polling Fortify on Demand to check if the scan has completed.
Action if Failing Security Policy	Select whether to take no action or mark the build as Failed or Unstable based on the application security policy as set by your organization.

8. Click **Generate Pipeline Script**. Copy the code and add it to your pipeline script.
9. Save the settings.

Run the Build

Run the build. Diagnostic information is available in the console output. The console output will display a success message if the assessment was successfully submitted. The Fortify on Demand Scans page will display an in-progress scan for the release.

Additional Considerations For Maven Users

For the most complete assessment of your application it is important to ensure all dependencies for deployment are satisfied. Maven provides a simple means of outputting these libraries by the **maven-dependency-plugin**. The section, **<excludeGroupIds>** may be used to ensure test framework code, for example, is not included.

Example POM Section:

POM Plugins Entry

```
<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-dependency-plugin</artifactId>
  <version>2.6</version>
  <executions>
    <execution>
      <id>copy-dependencies</id>
      <phase>prepare-package</phase>
      <goals>
        <goal>copy-dependencies</goal>
      </goals>
      <configuration>
        <outputDirectory>target/classes/lib</outputDirectory>
        <overWriteIfNewer>true</overWriteIfNewer>
        <excludeGroupIds>
          junit,org.easymock,${project.groupId}
        </excludeGroupIds>
      </configuration>
    </execution>
    <execution>
      <phase>generate-sources</phase>
      <goals>
        <goal>sources</goal>
      </goals>
    </execution>
  </executions>
  <configuration>
    <verbose>true</verbose>
    <detail>true</detail>
    <outputDirectory>${project.build.directory}</outputDirectory>
  </configuration>
</plugin>

...


<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-source-plugin</artifactId>
  <executions>
    <execution>
      <id>attach-sources</id>
      <goals>
        <goal>jar</goal>
      </goals>
    </execution>
  </executions>
</plugin>
```

Known Limitations

- The 2.0.9 (Obsolete) plugin version is slow to populate the pull down menu's in Redhat 7 machines. Please wait a minute or two and the first field should populate.

Change Log

Version 3.0.12 (4-05-2019)

The Jenkins Plugin now supports pipelines. The fodStaticAssessment and fodPollResults tasks have been added; they mirror the Fortify on Demand post-build actions in freestyle projects.

Version 3.0.11 (3-22-2019)

- Fixed SSRF vulnerability

Version 3.0.1 (10-9-2017)

Upgrade Note: - please be aware that builds will need to be reconfigured with the BSI Url/Token.

- Scans are now configured with the BSI Url/Token from the Static Scan Setup page of the release to be scanned in the Fortify on Demand Portal.

Version 2.0.6 (1-6-2017)

- Fixed bug that causes plugin to crash configuration pages when incomplete information was saved.

Version 2.0 (4-28-2016)

- Fixed bug when that causes plugin to crash when particular proxy configurations cause authentication to fail.
- Finalized update to FoD API V3

Version 1.10 (4-28-2016)

__Bug Fix:__ This release addresses a rare issue in which release information may not be retrieved for certain applications.

- Corrected encoding issue for application names which can prevent release information calls from working properly
- Additional validation for global polling interval
- Removed unsupported language level settings for .NET and Java

Version 1.09 (4-25-2016)

- Code changes to resolve distributed Jenkins defect (credit to Ruud Senden)
- Minor language support changes in preparation for potential new mobile assessment types

Version 1.08 (4-15-2016)

- Added support for Jenkins proxy configuration
- Added connection configuration test button that validates reachability of the portal and tests credentials

Version 1.07 (4-6-2016)

- Added option to include/exclude identified third-party libraries from analysis results
- Changed order, and description, of advanced options for consistency with the Fortify on Demand portal
- Polling for results is no longer default. Applications set to poll will reflect your organization's security policy in Jenkins via build stability.
- Minor branding changes

Version 1.06

__Bug Fix:__ This release addresses a bug where the Assessment Type may not correctly set under certain conditions

- Assessment Type no longer has a suggested default selection; the user must choose the proper type for enabled entitlement
- Added .NET as a supported language to Sonatype help text

Version 1.05

Upgrade Note: - please ensure you reconfigure any existing builds so that the filer filter may be set by the plugin; this functionality has changed with this version.

- Added support for all language/assessment types except MBS and C/C++, which require pre-processing with Fortify SCA prior to submission to Fortify on Demand
- Files selected for upload are automatically set based on language type and Fortify on Demand requirements; users may opt to package all files, including extraneous types like media, under advanced options. Using the automated default is *highly* encouraged
- The result report link added with the Detailed Reports option now refers to the Overview page in the Customer Portal

Version 1.04

Upgrade Note: - please ensure you reconfigure any existing builds so that *Assessment Type* may be set by the plugin as this field is new with this version.

- Static-related assessment types may be selected at upload, defaults to "Static Assessment"
- API calls for information lookup are now more resilient with retries, and have additional logging of any issues, e.g. lack of assessment entitlement

Version 1.03

- Star rating and total issue count display in the standard log results
- Detailed build log table output includes a deep link to the FoD customer portal for the application release, issue counts by criticality, and Fortify on Demand star rating
- Minor code cleanup for readability

Version 1.02

- Minor branding changes
- Updated UI API token secret validation due to changed 5.0 portal format

Version 1.01

- Initial release