Hewlett Packard Enterprise

Fortify on Demand TFS Integration

# HPE Security Fortify on Demand Team Foundation Server Integration

HPE Security Fortify on Demand supports build server integration with many solutions. This document details support for Team Foundation Server. It covers the installation and configuration of our TFS integration script that leverages the XAML build definitions available in Visual Studio.

**Features**

Fortify on Demand static security assessment for builds triggered by TFS
Assessment Options

- Standard assessment consisting of a scan by Fortify SCA followed by a manual review of the results to remove false positives
- Express assessment that does a less thorough security check of the application in a shorter period of time
- Automatically audited assessment that replaces the manual audit with automatic false positive suppression using Fortify Scan Analytics
- Sonatype scan to identify Open Source components and provide information on known vulnerabilities, along with recommended versions and licensing information

**Requirements**

Fortify on Demand integration with Team Foundation Server (TFS) requires two components.

| Resource | Location | Purpose |
|---|---|---|
| FodUpload.jar | TFS Server | Facilitates authenticated, secure, transport of a ZIP-packaged software application for Static Analysis to a specified Application/Release in the Fortify on Demand Portal |
| FoDSubmission.ps1 | TFS Server | Collects and packages build output, provides a manner of passing credentials and assessment details from Visual Studio to the FodUpload utility |

- The Team Foundation Server must have the Java JVM installed to execute the FodUpload.jar
- The Team Foundation Server must have outbound HTTPS access to the Fortify on Demand Portal
- The Fortify on Demand account used for submission must have access to the target application in the portal

February 2016

### Server Installation

1. Download FodUpload.jar from the Fortify on Demand Portal at **Administration->Tools.**
2. Locate FodSubmission.ps1 that was downloaded with these instructions from the **Customer Software** section of the **Help Center.**
3. Copy FodUpload.jar and FoDSubmission.ps1 files to the TFS server. The default directory is **C:\BuildScripts** this may be anywhere the TFS user may read and write. Note the directory for your build process template in Visual Studio.

### Client Installation

1. Ensure the target project/solution will build successfully on the Team Foundation Server.
2. Identify the corresponding application and associated release in the Fortify on Demand Portal from the list of **Applications**. Select the **Release** by name. Select the **build sever** option and specify appropriate values from the dropdowns to generate the **Upload URL** (See figure 1).
3. Create a XAML Build Definition under **Team Explorer -> Builds -> XAML Build Definitions.** You may opt to have multiple build definitions submitting to FoD, depending on your desired schedule. (See figure 2.)
4. Script settings are configured under the Process setting. FoD integration may occur post-build, or after tests
   – Configure the post-action script path as deployed on the server, default: **C:\BuildScripts\FoDSubmission.ps1**
   – Configure the post-action script arguments:

| Argument | Purpose |
|---|---|
| -Source | Designates the root directory of the build project |
| -Username | Fortify on Demand portal User Name |
| -Password | Fortify on Demand portal Password |
| -UploadURL | From step 2 above |

*Example*

-source "$(TF_BUILD_BUILDDIRECTORY)" -Username "UserName" -Password "P@ssword" –UploadURL “https://www.hpfod.com/bsi2.aspx?tid=1234&tc=tenant&pv=123456&payloadType=ANALYSIS_PAYLOAD&astid=123&ts=.NET&ll=4.5"

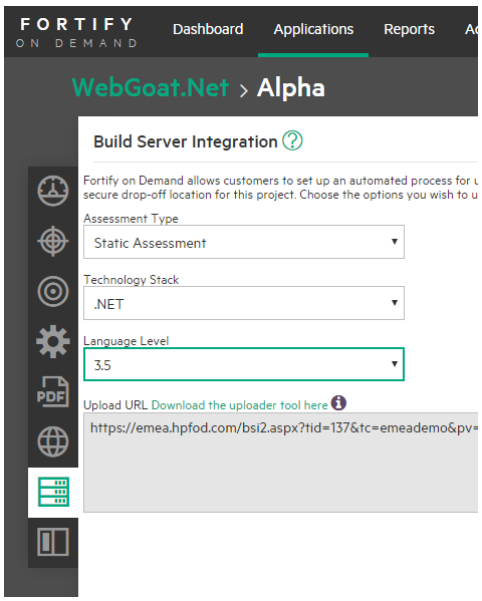


***Figure 1 Build Server Option***

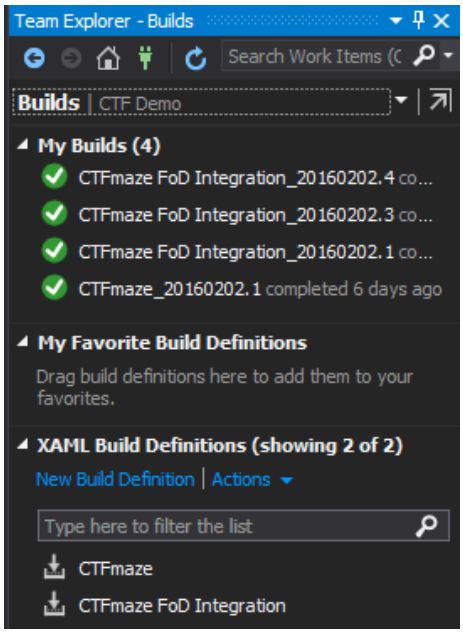


***Figure 2 XAML Build Definitions***

**Testing**

1. Manually trigger your build definition to test. Errors during the post-build process will indicate a failure in submission to FoD. See figure 3 and figure 4. In the event of a post-build error please check that the command is properly formatted, including quotation marks, the Upload URL is valid, and the portal credentials are correct.
2. Login to the Fortify on Demand Portal to verify that the assessment has been submitted. You should see the static scan status as 'In Progress'


***Figure 3 Successful build and Fortify on Demand submission***

**Additional Options**

Proxy configuration may be added with the following:

| Argument | Purpose |
|---|---|
| -ProxyURL | Internal proxy address |
| -ProxyUserName | Proxy username (Optional) |
| -ProxyPassword | Proxy password (Optional) |
| -NTworkstationName | NT workstation name (Optional) |
| -NTdomain | NT domain name (Optional) |

A range of security assessment options can be specified by the following:

| Argument | Purpose |
|---|---|
| -ExpressScan | Express assessment that does a less thorough security check of the application in a shorter period of time |
| -AutomatedAudit | Automatically audited assessment that replaces the manual audit with automatic false positive suppression using Fortify Scan Analytics |
| -SonatypeReport | Sonatype scan to identify Open Source components and provide information on known vulnerabilities, along with recommended versions and licensing information |

*Example*

-source "$(TF_BUILD_BUILDDIRECTORY)" -username "UserName" -password "P@ssword" **–ExpressScan –AutomatedAudit –SonatypeReport** –UploadURL "https://www.hpfod.com/bsi2.aspx?tid=1234&tc=tenant&pv=123456&payloadType=ANALYSIS_PAYLOAD&astid=123&ts=.NET&ll=4.5"

Please note the quotation marks are required.

Further details on these additional options may be found under 'Running FoD Upload.jar' in the Fortify on Demand User Guide available in the **Help Cente**r of the Fortify on Demand Customer Portal.

Note that express assessment and automatically audited assessments are beta features that must be enabled by your Fortify on Demand Technical Account Manager (TAM).

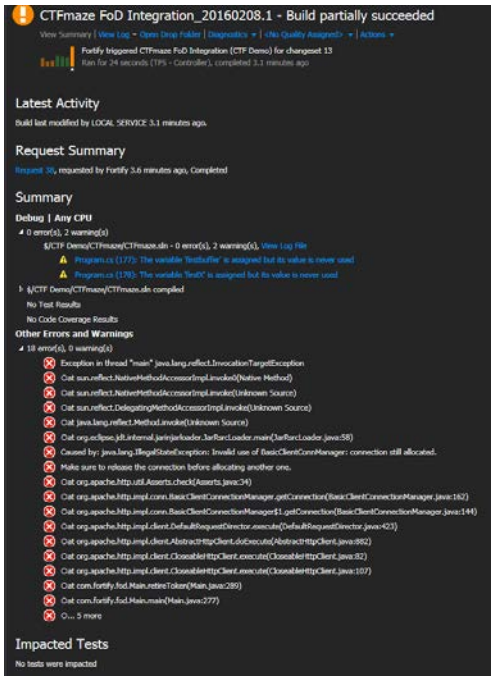


***Figure 4 Successful build and failed Fortify on Demand submission***

**Learn more at**
hpe.com/software/fortifyondemand