HP Operations Orchestration

For Windows and Linux operating systems

Software Version: 10.00

HP Fortify Integration Guide

Document Release Date: October 2012

Software Release Date: October 2012

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

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

- Software Version number, which indicates the software version.
- 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.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Chapter 1

Introduction

This chapter includes:

Purpose of the OO — Fortify Integration

HP Fortify is part of the HP Enterprise Security Products and it offers a suite of products and services that identify, fix and protect against security vulnerabilities in software applications.

HP Fortify Supported Versions

Operations Orchestration Version	Fortify Version
OO Content Pack 10	3.50

Downloading OO Releases and Documents on HP Live Network

HP Live Network provides an Operations Orchestration Community page where you can find and download supported releases of OO and associated documents.

To download OO releases and documents, visit the following site:

https://hpln.hp.com/

Note: This site requires that you register for an HP Passport and sign-in.

To register for an HP Passport ID:

1. Go to: http://h20229.www2.hp.com/passport-registration.html

   Or

   Click the **New users - please register** link on the HP Passport login page.

2. On the HP Live Network page, click **Operations Orchestration**.

3. On the left-hand side, click **Operations Orchestration Content Packs**.

4. In the **Operations Orchestration Content Packs** box, click **Content**. The HP Passport and sign-in page appears.
5. Enter your user ID and Password to access to continue.
6. Click **HP Operations Orchestration 9.00**.
7. Search for the required HP Operations Orchestration Content Pack.

Chapter 2

Getting Started

Use Cases

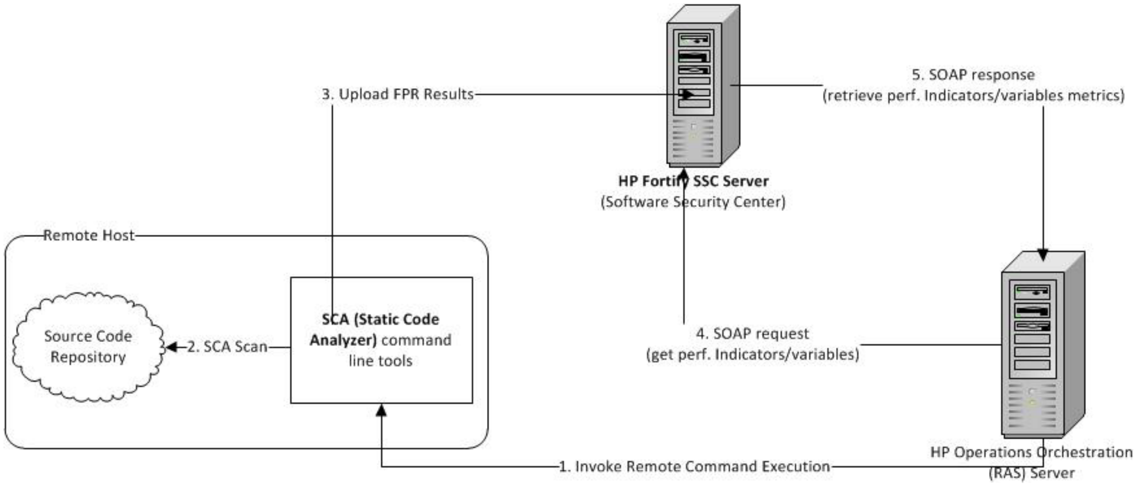
The following are the major use cases for the HP Fortify integration.

- **Extract Security Status** — As an Application Release Manager, I want to extract Fortify analysis data as part of an automated test/deployment process in order to verify that security policies are being followed for this application.
- **Capture Security Status for Auditing** — As an Application Security Specialist or Service Manager, I want to run an OO flow on demand to capture security scan results and current state in order to capture this data for auditing purposes.
- **Run a Scan** — As an Application Security Specialist or QA engineer, I want to run an SCA scan as part of an automated test/deployment process so that the process can be aborted or continued based on the scan results.

HP Fortify Architecture

The OO — Fortify integration consists of integrating with two Fortify subsystems:

- "SCA (Statistic Code Analyzer)" on page 10
- "SSC (Software Security Center)" on next page


3. Upload FPR Results
HP Fortify SSC Server
(Software Security Center)
5. SOAP response
(retrieve perf. Indicators/variables metrics)
Remote Host
Source Code Repository
2. SCA Scan
SCA (Static Code Analyzer) command line tools
4. SOAP request
(get perf. Indicators/variables)
HP Operations Orchestration (RAS) Server
1. Invoke Remote Command Execution

A typical workflow from OO requires the following steps:

1. Invoke a remote command execution operation on a remote host where the SCA tools are installed and we have a source code repository ready to be scanned.
2. Execute the SCA scan on the target source code repository.
3. Upload the FPR results to the SSC server (which may be on a different host).
4. Invoke a SOAP call to the SSC server from OO in order to extract the key performance indicators and variables.
5. SSC server issues a SOAP response back to the RAS server with the required metrics.

SSC (Software Security Center)

The SSC is a Java web application that is deployed on a Servlet container (for example, Tomcat) from where you can manage your projects, audit issues and generate reports with different performance indicators.

The integration with SSC will be implemented as a set of flows generated with **Web Service Wizard** from the WSDL exposed by the SSC server:

- **Get Performance Indicator** — the flow uses the **MostRecentMeasurementHistoryList** web service that retrieves the most recent value (from the latest snapshot) of the specified performance indicator name.
- **Get Performance Indicator Id** — the flow uses the **PerformanceIndicatorList** web service that retrieves the performance indicator id for the specified performance indicator name.
- **Get Performance Indicators** — the flow iterates over a list of performance indicators names and runs the **Get Performance Indicator** flow multiple times in order to get a list of multiple performance indicators values.
- **Get Project Version Id —** the flow uses the **ProjectList** and **ActiveProjectVersionList** web services in order to retrieve the id of the specified project and version.
- **Get Variable —** the flow uses the **MostRecentVariableHistoryList** web services in order to retrieve the most recent value (from the latest snapshot) of the specified variable name.

- **Get Variables** — the flow iterates over a list of variable names and runs the **Get Variable** flow multiple times in order to get a list of multiple variables values.

SCA (Statistic Code Analyzer)

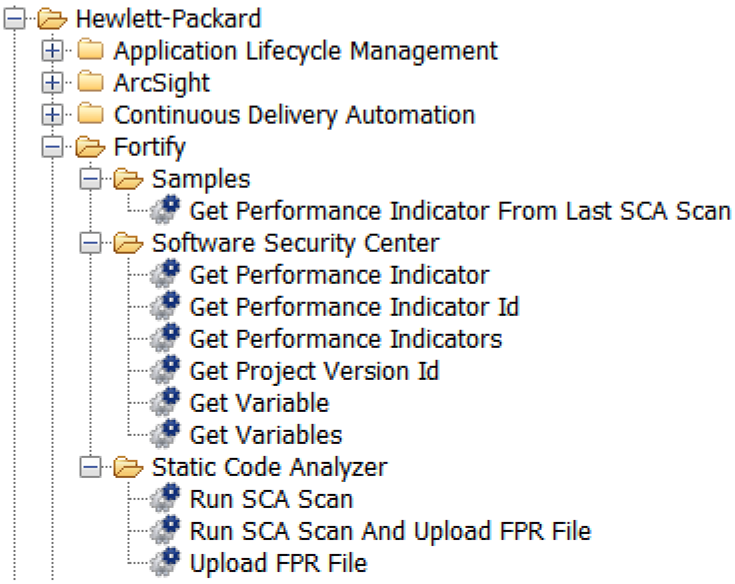
The SCA is a tool that is used for scanning a source code repository and producing an **.fpr** (Fortify project) file with the results.

The integration with the SCA is implemented as a set of **Remote Command Execution** flows:

- The **Run SCA Scan** flow executes a SCA scan on a source code repository. The flow is able to execute the SCA command local (on RAS) or remotely on a different server. The command is executed synchronously (the flow will wait until the command has completed, before returning the result).
- **Upload FPR File** flow uploads the **.fpr** file with the results on the SSC server. The **.fpr** file that is uploaded to the SSC server can exist on the local server (RAS) or on a remote server. The command is executed synchronously (the flow waits until the upload is finished, before returning the result).
- **Run SCA Scan And Upload FPR File** flow executes the two flows mentioned above in one step.

Location of the HP Fortify Integration Operations and Flows in OO Studio

The HP Fortify integration includes the following operations and flows in the OO Studio Library/Integrations/Fortify folder.



- Hewlett-Packard
  - Application Lifecycle Management
  - ArcSight
  - Continuous Delivery Automation
  - Fortify
    - Samples
      - Get Performance Indicator From Last SCA Scan
    - Software Security Center
      - Get Performance Indicator
      - Get Performance Indicator Id
      - Get Performance Indicators
      - Get Project Version Id
      - Get Variable
      - Get Variables
    - Static Code Analyzer
      - Run SCA Scan
      - Run SCA Scan And Upload FPR File
      - Upload FPR File

Chapter 3

Security

This section describes how security is handled by the Fortify integration.

It is recommended to use a secure shell connection (for example, SSH) when executing the SCA commands because sensitive data is sent as part of the commands arguments.

The SOAP calls that are used to communicate with the SSC server are using, by default, the WS-Security extension to authenticate the SOAP requests so the credentials of the SSC server are sent in SOAP headers as plain text. Therefore, it is recommended to use a secure connection (HTTP over SSL/TLS) when communicating to the SSC server.

Chapter 4

Troubleshooting

- If you encounter problems or warnings when running a SCA scan, re-run the command with the -debug option. This generates a file that can be used for further investigation. The file is named **sca.log** and can be found in the following directory:
  - On Windows: **C:\Documents and Settings\<username>\Local Settings\Application Data\Fortify\sca5.11\log**
  - On other platforms: **$HOME/.fortify/sca5.11/log**
- You can query the state of a SCA scan using the SCAState utility for up-to-date state analysis. Further information on how to use the command can be found in the following document: **HP_Fortify_SCA_Utilities_User_Guide_<version>.pdf**.
- The analysis process can be fine tuned with various configuration parameters defined in the **fortify.properties** and **fortify-sca.properties** files. Further information about the configuration options and the ordering of properties files can be found in the following document: **HP_Fortify_SCA_Install_and_Config_<version>.pdf**.

Chapter 5

OO Tools You Can Use with the Fortify – OO Integration

Following are OO tools that you can use with the Fortify integration:

- **RSFlowInvoke.exe and JRSFlowInvoke.jar**

  RSFlowInvoke (**RSFlowInvoke.exe** or the Java version, **JRSFlowInvoke.jar**) is a command-line utility that allows you to start a flow without using Central (although the Central service must be running). RSFlowInvoke is useful when you want to start a flow from an external system, such as a monitoring application that can use a command line to start a flow.

- **Web Services Wizard (wswizard.exe)**

  When you run the Web Services Wizard, you provide it with the WSDL for a given Web service. The WSDL string you provide as a pointer can be a file's location and name or a URL. The Web Services Wizard displays a list of the methods in the API of the Web service that you specify. When you run the wizard, pick the methods you want to use, and with one click for each method you have selected, the wizard creates an HP OO operation that can execute the method. This allows you to use the Web Services Wizard to create operations from your monitoring tool's API.

These tools are available in the Operations Orchestration home folder in **/Studio/tools/**.

Delete this text and replace it with your own content.