HP Fortify Static Code Analyzer

Software Version 4.10

Installation and Configuration Guide

Document Release Date: April 2014
Software Release Date: April 2014

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

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

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

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

Part Number: 1-181-2014-04-410-01

Contents

Preface

This guide describes how to install the HP Fortify Static Code Analyzer family of analyzers and applications.

HP Fortify Software Contact

If you have questions or comments about any part of this guide, contact HP Fortify Software at:

Technical Support

650.735.2215
fortifytechsupport@hp.com

Corporate Headquarters

Moffett Towers
1140 Enterprise Way
Sunnyvale, CA 94089

650.358.5600

contact@fortify.com

Website

http://www.hpenterprisesecurity.com

About the HP Fortify Software Security Center Documentation Set

The HP Fortify Software Security Center documentation set contains installation, user, and deployment guides for all HP Fortify Software Security Center products and components. It also includes technical notes and release notes that describe new features, known issues, and last-minute updates. The latest versions of these documents are available on the HP Software Product Manuals site:

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

Change Log

The following table tracks changes made to this guide.

Software Release-version	Date	Change
3.90-01	4/9/2013	Change Log and Introduction added.
4.10-01	3/23/2014	Updated release information.

Chapter 1: Introduction

This document contains installation and configuration instructions for HP Fortify Static Code Analyzer.

Intended Audience

This installation guide is intended for individuals who are responsible for installing or uninstalling the HP Fortify Static Code Analyzer suite of analyzers and application components.This guide also details basic post-installation tasks and configuration options.

Refer to the *HP Fortify Software Security Center System Requirements* document to ensure that your system meets the minimum requirements for each software component installation.

Note: This document does not cover the installation process for HP Fortify Software Security Center (Software Security Center). HP Fortify Software Security Center requires a separate installation procedure, which can be found in the *HP Fortify Software Security Center Installation and Configuration Guide*. Download this document from the HP Software Product Manuals site: http://support.openview.hp.com/selfsolve/manuals.

The HP Fortify Software Security Center Components

An HP Fortify Software Security Center installation consists of one or more of the following *analyzers*:

- HP Fortify Static Code Analyzer: Analyzes your build code according to a set of rules specifically tailored to provide the information necessary for the type of analysis performed.
- HP Fortify Runtime Application Protection: Monitors and protects deployed applications from common attacks, unintended use, and targeted hacking. In addition, best security practices, such as input verification and proper exception handling, can be consistently applied to deployed applications.
- HP Fortify SecurityScope: Identifies vulnerabilities in pre-deployment applications during the QA phase, preventing exposure to security flaws before they are exploited.

An HP Fortify Software Security Center installation may also include one or more of the following application tools:

- HP Fortify Audit Workbench: provides a graphical user interface for HP Fortify Static Code Analyzer that helps you organize, investigate, and prioritize analysis results so that security flaws can be fixed quickly.
- HP Fortify Plugin for Eclipse: integrates with the Eclipse development environment and adds the ability to scan and analyze the entire code base of a project and apply hundreds of software security rules that identify the vulnerabilities in your Java code. The results are displayed within the IDE, along with descriptions of each of the security issues and suggestions for their elimination.
- HP Fortify Eclipse Remediation Plug-in: integrates with the Eclipse development environment. The Eclipse Remediation Plug-in is a lightweight plug-in option for developers who need remediation functionality but do not need the scanning and auditing capabilities of Audit Workbench or the full Eclipse Plugin.
- HP Fortify for Package for Microsoft Visual Studio©: integrates with Visual Studio Premium and Visual Studio Professional to locate security vulnerabilities in your solutions and packages and displays the scan results in Visual Studio. The results include a list of issues uncovered, descriptions of the type of vulnerability each issue represents, and suggestions on how to fix them.
- HP Fortify Remediation Package for Visual Studio: integrates with Microsoft Visual Studio Premium and Visual Studio Professional integrated development environments (IDEs). The HP Fortify Remediation Package for Visual Studio is a lightweight plug-in option for developers who need remediation functionality but do not need the scanning and auditing capabilities of Audit Workbench or the full Visual Studio package.
- HP Fortify Extension for JDeveloper: integrates with the JDeveloper integrated development environment (IDE) and adds the ability to scan and analyze the entire code base of a project and apply hundreds of software security rules that identify the vulnerabilities in your code.

- HP Fortify Remediation Plugin for IntelliJ: integrates with the IntelliJ Integrated Development Environment (IDE) and adds the ability to scan and analyze the entire code base of a project and apply hundreds of software security rules that identify the vulnerabilities in your code.

Related Documents

The following documents provide additional information about HP Fortify Static Code Analyzer:

- *HP Fortify Static Code Analyzer User Guide*

  This document provides instructions on using the analyzers to identify vulnerabilities in your code.
- *HP Fortify Static Code Analyzer Utilities User Guide*

  This document provides information on the command-line tools that provide additional management and access to the functions provided by SCA.

Chapter 2: Installation

This chapter covers the following topics:

- About Downloading the Software
- About Installing the HP Fortify Static Code Analyzer Suite
- About the Post-Installation Tasks
- Registering the ASPNET User
- Uninstalling HP Fortify Static Code Analyzer

About Downloading the Software

HP Fortify Software is available as a downloadable ISO file which can be mounted or buned to a DVV, or as a downloadable application or package. For details on obtaining a license for your software, go to the *HP Fortify Software Security Center System Requirements* document and refer to the "HP Fortify Software Licenses" section. For details on obtaining HP Fortify software, go to the *HP Fortify Software Security Center System Requirements* document and refer to the "Acquiring HP Fortify Software" section.

About Installing the HP Fortify Static Code Analyzer Suite

This section describes how to install the SCA suite of analyzers and applications. You will need a Fortify License file to complete the process.

Launching the Installation

To install the SCA suite:

1. Navigate to the directory containing the installer files. If you downloaded the ISO, the installer file is located in the directory for your operating system.

   Note: For more information on acquiring the software and license for your operating system, see the *HP Fortify Software Security Center System Requirements* document.
2. Run the installer file that corresponds to your operating system and system processor.
3. Follow the prompts to install the software.

Migrating from a Previous SCA Installation

The Windows installation of SCA enables you to migrate from a previous installation of SCA on your system. Migrating from a previous SCA installation preserves SCA artifact files.

You can migrate SCA artifacts from a previous installation through the InstallShield wizard, or by using the `scapostinstall` post-install tool. For information on using the post-install tool to migrate from a previous SCA install, see "Migrating Properties Files."

To migrate from a previous SCA installation through the InstallShield Wizard:

1. Go to the Setup Type dialog box and click **Yes**. Click **CCC**. The Migration dialog box appears.
2. Specify the location of your previous SCA installation on your system. Click **OK**.
3. View the results of the SCA migration in the SCA Post Installation Configuration Results dialog box. This dialog box displays the SCA artifacts that were migrated, and the location of the files. Click **Next** to proceed to the Rulepack update.

Updating SCA Rulepacks

The Windows installation offers the option to update the HP Fortify Secure Coding Rulepacks for your system. The Software Security Research group releases quarterly updates to Secure Coding Rulepacks, which drive the SCA analyzers. They are distributed as part of the subscription service through updates on the HP Fortify customer download site, automated tool updates, and software releases.

You can update SCA Rulepacks through the InstallShield wizard, or by using the `rulepackupdate` tool.

To update the SCA Rulepacks for your installation through the InstallShield Wizard:

1. Specify the URL address of the Rulepack server. To use HP Fortify's server for Rulepack updates, specify the URL as: `https://update.fortify.com`.
2. Specify the proxy of the Rulepack server. (This step is optional.)
3. Click **Next**. The Setup Type dialog box asks if you would like to download Rulepacks now. Select **Yes**, and then click **Next**.
4. View the results of the Rulepack update in the Rulepack Updater dialog box.

Installing the HP Fortify Plugin for Eclipse

To install the HP Fortify Plugin for Eclipse:

1. Install the SCA suite on your system, as described in the previous sections.

   Note: For Windows platforms, ensure that the Eclipse option was selected during installation.
2. Open Eclipse.
3. Select **Help - Software Updates - Manage Configuration**.
4. Click **Add an Extension Location**.
5. Select **<install_directory>/plugins/eclipse.**
6. Click **OK**.

The Secure Coding Rulepacks Plug-in menu appears.

About the Post-Installation Tasks

Post-installation tasks prepare you to start using the SCA analyzers and applications. These tasks include:

- Running the Post-Install Tool
- Migrating Properties Files
- Specifying a Locale
- Specifying a Proxy Server for Rulepack Updates
- Updating the Rulepack

If you are using the Microsoft .NET Framework, you might need to register the ASPNET user, described in the section Registering the ASPNET User.

Running the Post-Install Tool

SCA installs the post-install tool, `scapostinstall`, onto your system during the SCA installation. The `scapostinstall` tool allows you to perform two tasks: migrate properties files from a previous version of SCA, and configure SCA Rulepack updates settings on your system.

To run the post-install tool:

1. Navigate to the `bin` directory from the command line.
2. Enter `scapostinstall` to start the tool.

3. Enter `s` to display settings, `r` to return to a previous prompt, and `q` to exit the tool.

Migrating Properties Files

To migrate properties files from a previous version of SCA to the current version of SCA installed on your system:

1. Navigate to the `bin` directory from the command line.
2. Enter `scapostinstall` to start the tool.
3. Enter `1` to select `Migration`.
4. Enter `1` to select `SCA Migration`.
5. Enter the previous install directory.
6. Enter `1` to select `Migrate from an existing SCA installation`.
7. Enter `s` to confirm the settings.
8. Enter `2` to perform the migration.
9. Enter `y` to confirm.

Specifying a Locale

By default, the locale of an SCA installation is English.

To specify a different locale:

1. Navigate to the `bin` directory from the command line.
2. Enter `scapostinstall` to start the tool.
3. Enter `2` to select `Settings`.
4. Enter `1` to select `General`.
5. Enter `1` to select `Locale`.
6. Enter the locale code:
   - English: `en`
   - Japanese: `ja`
   - Korean: `ko`
   - Chinese, Simplified: `zh_CN`
   - Chinese, Traditional: `zh_TW`

Specifying a Proxy Server for Rulepack Updates

If your network uses a proxy server to reach the Rulepack update server, you must specify the proxy server with the post-install tool.

To specify a proxy for the Rulepack update server:

1. Navigate to the `bin` directory from the command line.
2. Enter `scapostinstall` to start the tool.
3. Enter `2` to select `Settings`.
4. Enter `2` to select `Rulepack Update`.
5. Enter `2` to select `Proxy Server Host`
6. Enter the name of the proxy server.
7. Enter `3` to select `Proxy Server Port`.

8. Enter the proxy server's port number.

Updating the Rulepacks

The runtime rulepacks are updated automatically during the Windows installation procedure. However, you can also download HP Fortify Secure Coding Rulepacks from the HP Fortify Customer Portal and then use the Rulepack Update tool to update your Secure Coding Rulepacks. This option is provided for installations on non-Windows platforms and for deployment environments that do not have access to the Internet during the installation procedure.

Use the Rulepack Update tool, `Rulepackupdate`, to update Rulepacks from either a remote server or a locally downloaded file.

See *About Downloading the Software* on page 8 for information about downloading Rulepacks.

To update Rulepacks:

1. Navigate to the `bin` directory from the command line.
2. Enter `rulepackupdate` to start the Rulepack Update tool.

   The system will respond with either an error message or a list of the Rulepacks that it has downloaded.

   If you have previously downloaded Rulepacks from the HP Fortify Customer Portal, run `rulepackupdate` with the `-import` option and the path to the directory where you downloaded the Rulepacks.

Registering the ASPNET User

If you are using the Microsoft .NET Framework, you might need to register the ASPNET user. If the Microsoft Internet Information Server (IIS) is installed first, the ASPNET user is created when .NET Framework is installed; otherwise, you must register.

To register the ASPNET user, run the command:

```
aspnet_regiis -i
```

Find the command under the .NET Framework installation directory. For example, it is often located at:

```
C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322
```

or

```
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
```

Uninstalling HP Fortify Static Code Analyzer

This section describes how to uninstall the SCA software.

Uninstalling on Windows Platforms

To uninstall SCA suite software on Windows, use the **Windows Add or Remove Programs** utility on the Control Panel:

1. Select **Start - Settings - Control Panel - Add or Remove Programs**.
2. In the list of programs, choose HP Fortify vX.XX, and then click **Remove**.

Uninstalling on Other Platforms

To uninstall SCA software on Mac OS X, Linux, and Unix platforms:

1. Back up your configuration, including any important files you have created.
2. Manually delete the installation directory using the following command:

   ```
   rm -rf <install_directory>/
   ```

Chapter 3: Configuration Options

The chapter covers the following topics:

- About Software Security Center Properties Files
- About the Ordering of Properties Files
- fortify.properties Configuration Options
- fortify-sca.properties Configuration Options
- fortify-sca-quickscan.properties Configuration Options
- fortify-ide.properties Configuration Options

About Software Security Center Properties Files

The Software Security Center installer places a set of properties files on your system during installation. Properties files contain a list of configurable runtime analysis, output, and performance for Software Security Center components. Some properties files configure behavior and set parameter values globally for all Software Security Center components. Other properties files are specific to one component; setting parameters for a specific analyzer or scan mode, for example. These parameters contained within the properties files affect analysis, output, and performance of the component.

The installed properties files contain Software Security Center default values. HP Fortify recommends consulting with your project leads before opening and modifying parameters within the properties files. All properties files can be edited using a text editor.

Upon opening and inspecting the properties files, you will see that each parameter consists of a pair of strings: the first string stores the key or name of the parameter; the second string stores the value.

About the Ordering of Properties FilesAbout the Ordering of Properties Files

```
#this is a brief description about the locale parameter
com.fortify.locale=en
```

As shown above, the `com.fortify.locale=en` parameter sets the locale for Software Security Center components. The parameter key is `com.fortify.locale`, and the value is set to `en` for English. A brief description of the parameter also appears as a comment.

The following illustrates the syntax for the parameter key and value within the properties file:

```
#when performing a scan of a website from Visual Studio, setting this property to
true will cause SCA
#to translate the default ASP output instead of running the aspnet_compiler (it
is recommended to manually
#clean this cache before use of this setting)
#com.fortify.VS.SkipASPPrecompilation=true
```

Disabled parameters are commented out of the properties file. To enable these parameters, simply remove the comment symbol (#) and save the properties file. The following illustrates a disabled parameter:

As shown above, the `com.fortify.VSSkipASPPrecompilation` parameter is disabled within the properties file, and is not part of the configuration.

The following table describes the role of each Software Security Center properties file:

Table 1: Properties Files

Name of .properties File	Role
`fortify.properties`	Defines the global configuration parameters for Software Security Center components. These parameters set values for all components.
`fortify-ide.properties`	Defines the configuration parameters for Software Security Center Integrated Development Environment (IDE) plug-ins.
`fortify-sca.properties` (for Windows installations) `.fortify-sca.properties` (for non-Windows installations)	Defines the configuration parameters for SCA.
`fortify-sca-quickscan.properties`	Defines the configuration parameters applicable for a quick scan for SCA.

About the Ordering of Properties Files

Software Security Center processes properties in a specific order, using this order to override any previously set properties with the values that you specify. You should keep this processing order in mind when making changes to the properties files.

Property definitions are processed in the following order:

1. Properties specified on the command line have the highest priority and can be specified during any scan.
2. Properties specified in the `fortify-sca-quickscan.properties` file are processed second, but only when the `-quick` option is used to operate in Quick Scan mode. If Quick Scan is not invoked, this file is ignored.
3. Properties specified in the local `fortify.properties` file are processed third. Change values in this file on a scan-by-scan basis to fine-tune your installation.
4. Properties specified in the global `fortify-sca.properties` file are processed last. You should edit this file if you want to change the property values on a more permanent basis for all scans.

fortify.properties Configuration Options

The `fortify.properties` file defines global parameters for all Software Security Center components. The `fortify.properties` file installed on your system contains parameters set to Software Security Center default values. You can modify these parameter values by editing the file.

The `fortify.properties` file is located in either your Windows user directory or your Unix home directory.

The following table summarizes the parameters found in the `fortify.properties` file:

Table 2: HP fortify.properties Global Properties

Property Name / Default Value	Description
`com.fortify.Debug / false`	Places Software Security Center components in debug mode.
`com.fortify.awb.Debug / false`	Places HP Fortify Audit Workbench in debug mode.
`com.fortify.eclipse.Debug / false`	Places the HP Fortify Plugin for Eclipse in debug mode.
`com.fortify.VS.Debug / false`	Places the HP Fortify for Package for Microsoft Visual Studio© in debug mode.
`com.fortify.SCAExecutablePath /`(none)	Specifies the path to the working directory of any installed client tools, such as Audit Workbench and Secure Coding Plug-ins.
`com.fortify.WorkingDirectory /`(none)	Specifies the path to the Windows Local Application Data shell folder on your system. This is typically `C:\Documents and Settings\<user>\Local Settings\Application Data com.fortify.WorkingDirectory=${win32.LocalAppdata}/Fortify`
`com.fortify.InstallationUserName / ${user.name}`	Specifies the username for this installation.
`com.fortify.locale / en`	Specifies the installation locale.
`com.fortify.VS.RequireASPPrecompilation / true`	Set this parameter to `false` to allow the scan to continue even if the ASP Pre-Compilation fails when performing a scan of a website from Visual Studio in headless mode.
`com.fortify.VS.SkipASPPrecompilation / false`	Set this parameter to `true` to allow SCA to translate the default ASP output instead of running the aspnet_compiler when performing a scan of a website from HP Fortify Visual Studio Package. HP Fortify recommends manually cleaning this cache before enabling this setting.
`com.fortify.DisableProgramInfo / false`	Set this parameter to `true` to disable the use of the Code Navigation features in Audit Workbench and improve runtime memory usage.
`com.fortify.VS.DisableCIntegration / false`	Set this parameter to `true` to disable integration with C/C++ builds in HP Fortify Visual Studio Package.
`com.fortify.AuthenticationKey / ${com.fortify.WorkingDirectory}/config/tools`	Stores the Software Security Center client authentication token.
`com.fortify.model.CheckSig / false`	Specifies the path used to store the Software Security Center client authentication token.
`com.fortify.model.MinimalLoad / false`	Minimizes the data loaded from an FPR. Set this property to `true` to load only basic issue information.

Table 2: HP fortify.properties Global Properties (Continued)

Property Name / Default Value	Description
`com.fortify.model.UseIssueParseFilters / false`	Defers to the filter settings in the `IssueParseFilters.properties` file.
`com.fortify.model.EnableElementBaseIndexShift / (none)`	Set this value to true if you require backwards compatibility with pre-2.5 migrated projects.
`com.fortify.visualstudio.vm.args / (none)`	Specifies the default virtual machine arguments to use when Visual Studio plug-in runs Java commands.
`enable.clean.transaction.resource / (none)`	Set this property to `true` to prevent a quartz/spring bug when cron trigger is happened, some threadlocal resource is not released, resulting in a "Pre-bound JDBC Connection found!" error. Set this property to true when this problem occurs.
`com.fortify.tools.iidmigrator.scheme / (none)`	Set this property to migrate IIDs created with different versions of SCA. This is generally handled by SCA. If you need to override the mapping scheme, please consult HP Fortify customer support.
`max.file.path.length / 255`	Set the maximum number of characters for your file path.
`com.fortify.model.MergeResolveStrategy / DefaultToMasterValue`	Define which .FPR project (default or imported) should be used as the base when resolving merge conflicts. Possible values are: 'DefaultToMasterValue', 'DefaultToImportValue', or 'DefaultToMasterValue'.
`com.fortify.RemovedIssuePersistenceLimit / 1000`	Set the Removed Issue Persistence Limit. By default, the value is 1000, but can be increased appreciably.
`com.fortify.model.ExecMemorySetting / 1200M`	Set the amount of memory allocated for processes required by HP Fortify Audit Workbench (i.e., iidmigrator, events2fpr, etc.)
`com.fortify.model.IssueCutoffStartIndex / (none)`	Set the number of issues loaded. Select the first issue (by number) to be loaded.
`com.fortify.model.IssueCutoffEndIndex / (none)`	Used with `com.fortify.model.IssueCutoffStartIndex` this parameter allows you to select the last issue to be loaded (by number). Select the first issue (by number) to be loaded.
`com.fortify.model.IssueCutoffByCategoryStartIndex /`	Set this property to a value that represents the minimum number of issues a category should contain. Categories that contain fewer issues than set here are not displayed. Use in conjunction with to select a range of values.

`com.fortify.model.IssueCutoffByCategoryEndIndex /`	Set this property to a value that represents the maximum number of issues a category should contain. Categories that contain more issues than set here are not displayed. Use in conjunction with to select a range of values. For example:
	`com.fortify.model.IssueCutoffByCategoryStartIndex=10`
	`com.fortify.model.IssueCutoffByCategoryEndIndex=20`
	The example above loads categories which have between 10 and 19 issues in them.

fortify-sca.properties Configuration Options

SCA uses the parameter values defined in the `fortify-sca.properties` file to perform scans on your software projects.

The `fortify-sca.properties` file installed on your system contains parameters set to default values. You can modify these parameter values specific to SCA operation by editing the file, located at the following location on your system:

`<install directory>/Core/config`

The following table summarizes the parameters found in the `fortify-sca.properties` file:

fortify-sca-quickscan.properties Configuration Options

Table 3: SCA properties Global Properties

Parameter / Default Value	Description
`com.fortify.sca.ProjectRoot` / Default folder created during installation. This varies by platform.	Specifies the folder that stores intermediate files generated during a scan.
`com.fortify.sca.DefaultAnalyzers` / (None)	Specifies the types of analysis to perform. By default, this parameter is commented out, and all analysis types are utilized during scans. The acceptable values for this parameter are: `dataflow`, `semantic`, `controlflow`, `configuration`, `structural`, `nullptr`, and `content`.
`com.fortify.sca.SuppressLowSeverity` / `true`	Sets SCA to ignore low severity issues found during a scan.
`com.fortify.sca.LowSeverityCutoff` / `1.0`	Specifies the cutoff level for severity suppression. Any issues found with a lower severity value than the one specified with this parameter are ignored by SCA.
`com.fortify.sca.DefaultJarsDirs` / `default_jars`	Includes the JAR files that are added to SCA's `CLASSPATH` before any JARS specified using -cp or -classpath sourceanalyzer command line options. These JARS are located in `<Fortify_Home>/Core/default_jars` and its subdirectories. These JARS are not required by SCA in order to translate Java/JSP files but are provided as a convenience for users analyzing J2EE Web applications. You can configure SCA so that it does not use `com.fortify.sca.DefaultJarsDir` by setting `com.fortify.sca.DontUseDefaultJars` to `True`.
`com.fortify.sca.CustomRulesDir` / `${com.fortify.Core}/config/customrules`	Set the directory used to search for custom rules. If this is set, the default directory is not searched.
`com.fortify.sca.DontUseDefaultJars` / `false`	Set this value to True if you do not want to use the default JAR files in SCA's `CLASSPATH`. SCA will only use the JAR files specified on the sourceanalyzer command line using `-cp` or `-classpath`.

Table 3: SCA properties Global Properties (Continued)

Parameter / Default Value	Description
`com.fortify.sca.DefaultFileTypes` / `java,jsp,jspx,sql,cfm,php,pks,pkh,pkb,xml,config,properties,dll,exe,inc,asp,vbscript,js,ini,bas,cls,vbs, frm,ctl,html,htm,xsd, wsdd,xmi,cfml,cfc`	Specifies the types of file extensions to include in the SCA scan.
`com.fortify.sca.CustomRulesDir` / (none)	Specifies the directory with SCA custom rules. If you use this parameter and specify a different directory, the default directory `Core/config/customrules` will not be used.
`com.fortify.sca.fileextensions.<extension>` / The list of supported file extensions	Determines how SCA handles the specified file extension. This list can be added to so that SCA will understand new file extensions.
`com.fortify.sca.jsp.UseNativeParser` / `true`	Set SCA to use the native parser.
`com.fortify.sca.SqlLanguage` / `TSQL`	Set the SQL language variant.
`com.fortify.sca.compilers.<compiler>` / The list of supported compilers	Instructs SCA how to handle custom-named compilers.
`com.fortify.sca.DaemonCompilers` / The list of supported compilers	Determines which compilers are translated during an SCA scan.
`com.fortify.sca.IndirectCallGraphBuilder` / (None)	Determines when to call graph builders during an SCA scan. You can specify the following call graph builders: `com.fortify.sca.analyzer.callgraph.VirtualCGBuilder;` `com.fortify.sca.analyzer.callgraph.J2EEIndirectCGBuilder;` `com.fortify.sca.analyzer.callgraph.JNICGBuilder;` `com.fortify.sca.analyzer.callgraph.StoredProcedureResolver;` `com.fortify.sca.analyzer.callgraph.JavaWSCGBuilder;` `com.fortify.sca.analyzer.callgraph.StrutsCGBuilder;` `com.fortify.sca.analyzer.callgraph.DotNetWSCGBuilder;` `com.fortify.sca.analyzer.callgraph.SqlServerSPResolver`
`com.fortify.sca.DisableFunctionPointers` / `false`	Disables function pointers during the SCA scan.
`com.fortify.sca.DisableGlobals` / `false`	Disables function pointers and global parameters set by the `fortify.properties` file.
`com.fortify.sca.DisableDeadCodeElimination` / `false`	Set this property to `true` to disable the use of the Code Navigation features in Audit Workbench and improve runtime memory usage.
`com.fortify.sca.DeadCodeIgnoreTrivialPredicates` / `true`	Instructs SCA to ignore dead code. Dead code is a computer programming term for code in the source code of a program which is executed but whose result is never used in any other computation

Table 3: SCA properties Global Properties (Continued)

Parameter / Default Value	Description
com.fortify.sca.DeadCodeFilter / true	Instructs SCA to filter dead code during scans. Dead code is a computer programming term for code in the source code of a program which is executed but whose result is never used in any other computation
com.fortify.scaSolverTimeout / 15	Instructs SCA to timeout after the specified time period.
com.fortify.FVDLDisableProgramData / false	Excludes the ProgramData section from the analysis results file (FVDL output file).
com.fortify.FVDLDisableSnippets / false	Excludes code snippets from the analysis results (FVDL output file).
com.fortify.FVDLDisableDescriptions / false	Excludes descriptions from the analysis results.
com.fortify.FVDLDisableStyleSheets / ${com.fortify.Core}/resources/sca/fvdl2html.xsl	Specifies the style sheet for the analysis results.
com.fortify.sca.ClobberLogFile / false	Sets SCA to overwrite the log file for each new scan.
com.fortify.sca.LogFile / ${com.fortify.sca.ProjectRoot}/sca/log/sca.log	Specifies the location of the log file for SCA.
com.fortify.sca.PrintPerformanceDataAfterScan /	Sets the post-scan logging option. If SCA is in debug mode, this will be automatically set to true.
com.fortify.sca.cpfe.command / ${com.fortify.Core}/private-bin/sca/cpfe	Specifies the CPFE binary (version 3.9) to be used in translation phase. ***Do not modify.***
com.fortify.sca.cpfe.new.command / ${com.fortify.Core}/private-bin/sca/cpfe441	Specifies the new binary (version 4.4.1) to be used in translation phase. ***Do not modify.***
com.fortify.sca.cpfe.options / --remove_unneeded_entities --supress_vtbl -tused	Adds options to CPFE command line invoked by SCA when translating C/C++ code. You can use any options supported by CPFE, but make sure you understand the impact of the desired options before altering this property.
com.fortify.sca.cpfe.file.option / --gen_c_file_name	Sends the name of the NST output file to the CPFE. ***Do not modify.***
com.fortify.sca.cpfe.dont.fix.cctor.option / false	Determines whether or not the CPFE should perform additional processing steps when it translates copy constructor calls in C++ code. When this value is false, the extra processing steps are done. ***Do not modify.***
com.fortify.sca.DisplayProgress / true	Allows SCA to display progress through the user interface during a scan.
com.fortify.sca.findbugs.maxheap / (None)	Sets a maximum amount of issues to log during an SCA scan.

Table 3: SCA properties Global Properties (Continued)

Parameter / Default Value	Description
com.fortify.sca.AllocationWebServicesURL / https://per-use.fortify.com/services/GasAllocationService	Specifies the URL of Web services for SCA.
com.fortify.sca.CfmlUndefinedVariablesAreTainted / false	Instructs undefined variables in CFML pages to be considered tainted by SCA.
com.fortify.sca.AddImpliedMethods / true	Set SCA to generate implied methods when implementation by inheritance is encountered.

SCA performs scans to identify issues within software project. SCA also offer a less-intensive scan known as a quick scan. This option scans the project in Quick Scan Mode, using the parameter values in the `fortify-sca-quickscan.properties` file. By default, Quick Scan searches for high-confidence, high-severity issues only. For more information about Quick Scan Mode, see the *HP Fortify Audit Workbench User's Guide*.

The following table describes the properties that tune default scanning performance. These properties have different defaults for Quick Scan mode, which can be adjusted by editing the `fortify-sca-quickscan.properties` file. If you want to use the recommended tuning parameters, you do not need to edit this file; however, you may find that you want to experiment with other settings to fine-tune your specific application.

Remember that properties in this file are processed only if you specify the `-quick` option on the command line when invoking your scan.

The `fortify-sca-quickscan.properties` file installed on your system contains parameters set to default values. You can modify these parameter values by editing the file, located at the following location on your system:

`<install directory>/Core/config`

The following table provides two sets of default values. The first value is the default value for normal scans. The second value is the default value for quick scans. If only one default value is shown, the value is valid for both normal scans and quick scans. The following table summarizes the parameters found in the `fortify-sca-quickscan.properties` file.

Table 4: HP fortify-sca-quickscan.properties Global Properties

Property Name / Default Value	Description
com.fortify.sca.FilterSet / (None) Quick Scan value: `Critical Exposure`	When set to `Critical Exposure`, this property runs rules only for the high-severity filter set. Running only a subset of the defined rules allows the SCA scan to complete more quickly. This causes SCA to run only those rules that can cause issues identified in the named filter set, as defined by the default project template for your application. For more information about filter sets, see the *HP Fortify Audit Workbench User Guide*.
com.fortify.sca.FPRDisableSrcHtml / False Quick Scan value: `True`	Disables source code rendering into the FPR file. Disables SCA from generating marked-up source code files during a scan. When set to `true`, this property prevents the generation of marked-up source files. If you plan to upload FPRs that are generated as a result of a quick scan, you must set this property to `false`.

Table 4: HP fortify-sca-quickscan.properties Global Properties (Continued)

Property Name / Default Value	Description

`com.fortify.sca.limiters.Constraint PredicateSize /`
`50000`
 	
Quick Scan value: `10000`
	Specifies the size limit for complex calculations in the Buffer Analyzer. Skips calculations that are bigger than the specified size value in the Buffer Analyzer to improve scanning time.

`com.fortify.sca.BufferConfidence InconclusiveOnTimeout /`
`true`
 	
Quick Scan value: `false`
	Instructs SCA to skip complex calculations in the Buffer Analyzer to improve scanning time.

`com.fortify.sca.limiters.MaxChainDepth /`
`5`
 	
Quick Scan value: `4`
	Controls the maximum call depth through which the Dataflow Analyzer tracks tainted data. Increasing this value increases the coverage of data flow analysis, and results in longer analysis times. **Note:** Call depth refers to the maximum call depth on a data flow path between a taint source and sink, rather than call depth from the program entry point, such as `main()`.

`com.fortify.sca.limiters.MaxTaintDefFor Var /`
`1000`
 	
Quick Scan value: `500`
	Sets a complexity limit for DataFlow analysis. DataFlow will incrementally decrease precision of analysis on functions that exceed this complexity metric for a given precision level.

`com.fortify.sca.limiters.MaxTaintDefFor VarAbort /`
`4000`
 	
Quick Scan value: `1000`
	Sets a hard limit for function complexity. If complexity of a function exceeds this limit at the lowest precision level, the analyzer skips analysis of the function.

`com.fortify.sca.DisableGlobals /` `false`	Instructs SCA to not track tainted data through the global variables set with the `fortify.properties` file.
`com.fortify.sca.CtrlflowSkipJSPs /` `false`	Instructs SCA to skip ControlFlow analysis on JSPs.
`com.fortify.sca.NullPtrMaxFunctionTime /300000` Quick Scan value: `30000`	Sets the time limit (in milliseconds) for Null Pointer analysis on a single function. Setting it to a shorter limit decreases overall scanning time.

`com.fortify.sca.CtrlflowMaxFunctionTime /`
`600000`
 	
Quick Scan value: `30000`
	Sets the time limit (in milliseconds) for ControlFlow analysis on a single function.

`com.fortify.sca.TrackPaths /` (Not set) Quick Scan value: `NoJSP`	Disables path tracking for Control flow analysis. Path tracking provides more detailed reporting for issues, but requires more scanning time. You can disable this for JSP only by setting it to `NoJSP`. Specify `None` to disable all functions.
`com.fortify.sca.translator.java. Incremental /` `false`	Instructs SCA to translate Java source files one at a time instead of all at once when this property is set to True. SCA will use less memory while translating files but will process the files more slowly.

fortify-ide.properties Configuration Options

The `fortify-ide.properties file` defines configuration settings for Audit Workbench. This component allows you to examine the scan results produced by Software Security Center analyzers, such as SCA. The `fortify-ide.properties` file installed on your system contains parameters set to default values. You can modify these parameter values by editing the file, located at the following location on your system:

`<install directory>/Core/config`

The following table summarizes the parameters in the `fortify-ide.properties` file:

Table 5: HP fortify-ide.properties Global Properties

Property Name / Default Value	Description
`rulepack.days` / `15`	Sets the number of days before performing an automatic update of Rulepacks.
`rulepack.auto.update` / `true`	Enables automatic updating of Rulepacks.
`override.results.path` / (None)	Overrides the saved FPR location to a new location: `${user.home}`