Micro Focus
Fortify Static Code Analyzer Tools

Software Version: 19.2.0

Properties Reference Guide

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

© Copyright 2015 - 2019 Micro Focus or one of its affiliates

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.

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

This document was produced on October 01, 2019. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Preface

Contacting Micro Focus Fortify Customer Support

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://softwaresupport.softwaregrp.com

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:
https://software.microfocus.com/solutions/application-security

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

https://www.microfocus.com/support-and-services/documentation

Change Log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
19.2.0	Updated: Release date and version number
19.1.0	Updated: Release date and version number
18.20	Removed: • References to Fortify Process Designer (no longer supported) • References to the Fortify Software Security Center legacy user interface

Chapter 1: Fortify Static Code Analyzer Applications and Java IDE Plugin Properties

This chapter describes the properties used by the following Micro Focus Fortify Static Code Analyzer applications and Java IDE plugins:

- Micro Focus Fortify Audit Workbench
- Micro Focus Fortify Custom Rules Editor
- Micro Focus Fortify Plugins for Eclipse, IntelliJ, WebStorm, and Android Studio

The following table lists the Fortify Static Code Analyzer application acronyms used in this chapter.

Acronym	Fortify Static Code Analyzer Application / Plugin
AWB	Fortify Audit Workbench
CRE	Fortify Custom Rules Editor
ECP	Fortify Eclipse Complete Plugin
ERP	Fortify Eclipse Remediation Plugin
IAP	Fortify IntelliJ/Android Studio Analysis Plugin
IRP	Fortify IntelliJ/WebStorm/Android Studio Remediation Plugin

Where to Find the Properties Files

The location of the properties files varies for the different Micro Focus Fortify Static Code Analyzer tools. The following table provides the location of the properties files for tools described in this chapter.

Fortify Static Code Analyzer Tool	Property File Location
AWB, CRE	*<sca_install_dir>*/Core/config
ECP	*<eclipse_install_ dir>*/plugins/com.fortify.dev.ide.eclipse_ *<version>*/Core/config

Fortify Static Code Analyzer Tool	Property File Location
ERP	*<eclipse_install_ dir>*/plugins/com.fortify.plugin.remediation_ *<version>*/Core/config
IAP	*<user_home>*/.*<IDE_product_ name>*/config/plugins/FortifyAnalysis/config
IRP	*<user_home>*/.*<IDE_product_ name>*/config/plugins/Fortify/config

Fortify Properties (fortify.properties File)

Some of the properties described in this section already exist in the `fortify.properties` file, and some of them you must add yourself. The colored boxes in the Details column indicate which Micro Focus Fortify Static Code Analyzer tools use the property.

The following table describes the properties in the `fortify.properties` file.

Property	Details
com.fortify. audit.ui.DisableAddingFolders	If set to `true`, disables the add folder functionality. **Default:** `false` **Tools Affected:** | AWB | ECP | ERP | CRE | IAP | IRP |
com.fortify. audit.ui.DisableBugtrackers	If set to `true`, disables bug tracker integration. **Default:** `false` **Tools Affected:** | AWB | ECP | ERP | CRE | IAP | IRP |

Property	Details
com.fortify. audit.ui.DisableEditing CustomTags	If set to `true`, removes the ability to edit custom tags. **Default:** `false` **Tools Affected:** 	AWB	ECP	ERP	CRE	IAP	IRP
---	---	---	---	---	---	
com.fortify. audit.ui.DisableSuppress	If set to `true`, disables issue suppression. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. AuthenticationKey	Specifies the directory used to store the Micro Focus Fortify Software Security Center client authentication token. **Default:** `${com.fortify.WorkingDirectory}/config/tools` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. awb.Debug	If set to `true`, Fortify Audit Workbench runs in debug mode. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. awb.javaExtensions	Specifies the file extensions (comma-delimited) to treat as Java files during a scan. If no value is specified, Fortify Audit Workbench and the Fortify Eclipse Complete Plugin recognize `.java`, `.jsp`, and `.jspx` files as Java files. The property is used only to determine whether a project includes Java files and to add Java-specific controls to the Advanced Scan wizard. **Default:** none

For the **com.fortify.audit.ui.DisableEditingCustomTags** property, the Tools Affected highlighted are: AWB, ECP.

For the **com.fortify.audit.ui.DisableSuppress** property, the Tools Affected highlighted are: AWB, ECP.

For the **com.fortify.AuthenticationKey** property, the Tools Affected highlighted are: AWB, ECP, ERP, CRE, IAP, IRP.

For the **com.fortify.awb.Debug** property, the Tools Affected highlighted are: AWB.

Property	Details
	Tools Affected: 	AWB	ECP	ERP	CRE	IAP	IRP	 (AWB, ECP highlighted)
com.fortify. awb.LinuxFontAdjust	Specifies the font size to use on Linux platforms. Fortify Audit Workbench adds the specified size to original font size. **Default:** 0 **Tools Affected:** (AWB, ECP, CRE highlighted)
com.fortify. awb.MacFontAdjust	Specifies the size to tune font size for Mac platform. Fortify Audit Workbench adds the specified size to the original font size. **Default:** 2 **Tools Affected:** (AWB, ECP, CRE highlighted)
com.fortify. awb.WindowsFontAdjust	Specifies to tune font size for Windows platform. Fortify Audit Workbench adds the specified size to original font size. **Default:** 0 **Tools Affected:** (AWB, ECP, CRE highlighted)
com.fortify. Debug	If set to `true`, runs the Fortify Static Code Analyzer tools in debug mode. **Default:** `false` **Tools Affected:** (AWB, ECP, ERP highlighted)
com.fortify. DisableDescriptionXML Escaping	If set to `true`, disables XML escaping in issue descriptions (for example, changing " in XML/FVDL to "). **Default:** `false`

Property	Details
	Tools Affected: | AWB	ECP	ERP	CRE	IAP	IRP	

com.fortify. DisableExternalEntry Correlation	If set to `true`, parses URL in the ExternalEntries/Entry element in `audit.fvdl`.
	
	Default: `false`
	
	<pre>\<ExternalEntries>
	  \<Entry name="HTML Form" type="URL">
	  \<URL>/auth/PerformChangePass.action\</URL>
	  \<SourceLocation path="pages/content/
	   ChangePass.jsp" line="16" lineEnd="16"
	   colStart="0" colEnd="0"
	   snippet=
	   "1572130B944CEC7A3D98775A499AE8FA#pages/
	   content/ChangePass.jsp:16:16"/>
	  \</Entry>
	\</ExternalEntries></pre>
	Tools Affected:
	
	| AWB
		ECP	ERP	CRE	IAP	IRP	

com.fortify. DisableMinVirtCallConfidence Computation	If set to `true`, disables computing minimum virtual call confidence. Fortify Audit Workbench and the Fortify Eclipse Complete Plugin use this attribute to compute minimum virtual call confidence and enable issue filtering. For example, you can use it to filter out all issues that contain virtual call with confidence lower than 0.46. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. DisableRemovedIssue Persistance	If set to `true`, disables removed issue persistence (clears removed issues from the results file). **Default:** `false`

Property	Details
	Tools Affected: 	AWB	ECP	ERP	CRE	IAP	IRP	 (AWB, ECP highlighted)
com.fortify. DisableReportCategory Rendering	If set to `true`, disables rendering issue description into report. **Default:** `false` **Tools Affected:** (AWB, ECP highlighted) AWB, ECP, ERP, CRE, IAP, IRP
com.fortify. DisplayEventID	If set to `true`, displays the event ID in the issue node tooltip in the Issues view. **Default:** `false` **Tools Affected:** (AWB, ECP highlighted) AWB, ECP, ERP, CRE, IAP, IRP
com.fortify. eclipse.Debug	If set to `true`, runs the plugin in debug mode. **Default:** `false` **Tools Affected:** (ECP, ERP highlighted) AWB, ECP, ERP, CRE, IAP, IRP
com.fortify. InstallationUserName	Specifies the default user name for logging in to Fortify Software Security Center for the first time. **Default:** `${user.name}` **Tools Affected:** (AWB, ECP, ERP, CRE, IAP highlighted) AWB, ECP, ERP, CRE, IAP, IRP
com.fortify. locale	Specifies the Fortify locale (for rules and metadata only). Possible values are: `en` (English) `es` (Spanish) `ja` (Japanese)

Property	Details
	`ko` (Korean)
	`pt_BR` (Brazilian Portuguese)
	`zh_CN` (Simplified Chinese)
	`zh_TW` (Traditional Chinese)
	Default: `en`
	Tools Affected:
	<table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. model.CheckSig	If set to `true`, verifies signature in FPR.
	If `com.fortify.model.UseIssueParseFilters` is set to `true`, then `com.fortify.model.MinimalLoad` is set to true, `com.fortify.model.IssueCutoffStartIndex` is not null, `com.fortify.model.IssueCutoffEndIndex` is not null, `com.fortify.model.IssueCutoffByCategoryStartIndex` is not null or
	`com.fortify.model.IssueCutoffByCategoryEndIndex` is not null, `com.fortify.model.CheckSig` is `false`, and the signature in FPRs are not verified.
	Default: `true` (normal) / `false` (minimum load)
	Tools Affected:
	<table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. model.CustomDescriptions Header	Specifies the custom prefix for the description header. It prepends the text in the `Description/Recommendation` header, so that you see "My Recommendations" instead of "Custom Recommendations."
	Note: To update description headers, Fortify recommends that you use the `<CustomDescriptionRule>` rule with the `<Header>` element text instead.
	Default: none

Property	Details
	Tools Affected: | AWB | ECP | ERP | CRE | IAP | IRP |
com.fortify. model.DisableChopBuildID	If set to `true`, does not shorten the build ID, even if the build ID exceeds 250 characters. **Default:** `false` **Tools Affected:** | AWB | ECP | ERP | CRE | IAP | IRP |
com.fortify. model.DisableContextPool	If set to `true`, disables loading of the `ContextPool` section of the `audit.fvdl` file. You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is set to `true`, then `com.fortify.model.DisableContextPool` is automatically set to `true`. **Default:** `false` **Tools Affected:** | AWB | ECP | ERP | CRE | IAP | IRP |
com.fortify. model.DisableDescription	If set to `true`, disables loading the `Description` section from `audit.fvdl`. You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is `true`, then `com.fortify.model.DisableDescription` is automatically set to `true`. **Default:** `false` **Tools Affected:** | AWB | ECP | ERP | CRE | IAP | IRP |

Property	Details
com.fortify. model.DisableEngineData	If set to `true`, disables loading the `EngineData` section of `audit.fvdl` to save memory when large FPR files are opened. This data is displayed on the **Analysis Information** tab of **Project Summary** view. The property is useful if too many analysis warnings occur during a scan. However, Fortify recommends that you instead set a limit for `com.fortify.model.MaxEngineErrorCount` to open FPR files that have many Fortify Static Code Analyzer warnings. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.DisableProgramInfo	You can configure this property if `com.fortify.model.MinimalLoad` is not `true`. If `com.fortify.model.MinimalLoad` is set to `true`, then this property is automatically set to `true`. If set to `true`, prevents loading of metatable from the `ProgramData` section of FPR files. If set to `false`, loads metatable from the FPR file. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.DisableProgramPoint	If set to `true`, disables loading of the `ProgramPoint` section from the `runtime.fvdl` file. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.DisableReplacement Parsing	If set to `true`, disables replacing conditional description. You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is `true`, then this

Property	Details
	property is automatically set to `true`. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP | | --- | --- | --- | --- | --- | --- |
com.fortify. model.DisableSnippets	If set to `true`, disables loading the `Snippets` section from the `audit.fvdl` file. You can configure this property if `com.fortify.model.MinimalLoad` is set to `false`. If `com.fortify.model.MinimalLoad` is set to `true`, then `com.fortify.model.DisableSnippets` is automatically set to `true`. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.DisableUnified Inductions	If set to `true`, disables loading the `UnifiedInductionPool` section from the `audit.fvdl` file. You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is set to `true`, then `com.fortify.model.DisableUnifiedInductions` is automatically set to `true`. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.DisableUnifiedPool	If set to `true`, disables loading the `UnifiedNodePool` section from the `audit.fvdl` file. You can configure this property if `com.fortify.model.MinimalLoad` is set to `false`. If `com.fortify.model.MinimalLoad` is `true`, then

Property	Details
	`com.fortify.model.DisableUnifiedPool` is automatically set to `true`. If the value is not specified or false, this property is set to none. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify.model.DisableUnifiedTrace	If set to `true`, disables loading the `UnifiedTracePool` section from the `audit.fvdl` file. You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is `true`, then `com.fortify.model.DisableUnifiedTrace` is automatically set to `true`. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify.model.EnablePathElement BaseIndexShift	If set to `true`, enables backward compatibility with pre-2.5 migrated projects. **Default:** none **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify.model.EnableSource Correlation	If set to `true`, takes data flow source into consideration for issue correlation. The default is `false` because correlations with runtime results might not be reliable with this setting enabled. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	

Property	Details
com.fortify. model.ExecMemorySetting	Specifies the JVM heap memory size used by Fortify Audit Workbench to launch external utilities. **Default:** 600—iidmigrator 300—fortifyupdate **Tools Affected:** <table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. model.ForceIIDMigration	If set to true, forces running Instance ID migration during a merge. **Default:** false **Tools Affected:** <table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. model.FullReportFilenames	If set to true, uses full file name in reports. **Default:** false **Tools Affected:** <table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. model.IIDmigratorOptions	Specifies iidmigrator options (space-delimited values) run by FPRUtility, Fortify Audit Workbench, or the Fortify Eclipse Complete Plugin. **Default:** none **Tools Affected:** <table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. model.IssueCutoffByCategory StartIndex	Specifies the start index for issue cutoff by category. **Default:** 0

Property	Details
	Tools Affected: 	AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.IssueCutoffByCategory EndIndex	Specifies the end index for issue cutoff by category. **Default:** `java.lang.Integer.MAX_VALUE` **Tools Affected:** 	AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.IssueCutoffStartIndex	Specifies the start index for issue cutoff. Select the first issue (by number) to be loaded. **Default:** `0` **Tools Affected:** 	AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.IssueCutoffEndIndex	Determines the end index for issue cutoff. Select the last issue (by number) to be loaded. **Default:** `java.lang.Integer.MAX_VALUE` **Tools Affected:** 	AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.MaxEngineErrorCount	Determines how many reported Fortify Static Code Analyzer warnings are loaded. To allow an unlimited number, specify `-1`. Fortify recommends that you keep the default value of `3000` because this can speed up the load time of large FPR files. **Default:** `3000` **Tools Affected:** Also used by FPRUtility 	AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.MergeResolveStrategy	Specifies merge resolve strategy from: • `DefaultToMasterValue` (use primary project)

Property	Details
	• `DefaultToImportValue` (use secondary project) • `NoStrategy` (prompt for project to use) **Default:** `DefaultToMasterValue` **Tools Affected:** AWB · ECP · ERP · CRE · IAP · IRP
com.fortify. model.MinimalLoad	If set to `true`, minimizes the data loaded from an FPR file. **Default:** `false` **Tools Affected:** AWB · ECP · ERP · CRE · IAP · IRP
com.fortify. model.NProcessingThreads	Specifies the number of threads to process FPR files. If `com.fortify.model.PersistDataToDisk` is set to `true`, defaults to 1 thread. If the number specified exceeds the number of available processors: `int maxThreads=java.lang.Runtime.getRuntime().availableProcessors()`, then Fortify Static Code Analyzer tools use the number of available processors as the number of threads to process FPR files. **Default:** Number of available processors **Tools Affected:** Also used by FPRUtility AWB · ECP · ERP · CRE · IAP · IRP
com.fortify. model.PersistDataToDisk	If set to `true`, enables a persistence strategy to reduce the memory footprint and uses the disk drive to swap FPR data out of memory. **Default:** `false` **Tools Affected:** AWB · ECP · ERP · CRE · IAP · IRP

Property	Details
com.fortify. model.PersistenceBlockSize	If `com.fortify.model.PersistenceStrategy` is set to `CUSTOM`, `com.fortify.model.PersistenceBlockSize` specifies the number of attribute values that comprise a single block of attributes. These blocks are cached to disk and read back in as needed. A higher number decreases the total number of cache files, but increases the file size and the amount of memory that is read in each time. **Default:** 250 **Tools Affected:** AWB / ECP / ERP / CRE / IAP / IRP
com.fortify. model.PersistenceQueue Capacity	If `com.fortify.model.PersistenceStrategy` is set to `CUSTOM`, this property specifies the maximum number of attribute value blocks that can exist in the producer/consumer queue. **Default:** queue is unbounded **Tools Affected:** AWB / ECP / ERP / CRE / IAP / IRP
com.fortify. model.PriorityImpact Threshold	Specifies the threshold for issue impact. The valid values are 0.0F–5.0F. If the impact of an issue is greater than or equal to the threshold, the issue is considered High. If the impact of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows: • **Critical**—High Impact and High Likelihood • **High**—High Impact and Low Likelihood • **Medium**—Low Impact and High Likelihood • **Low**—Low Impact and Low Likelihood Also see com.fortify.model.PriorityLikelihoodThreshold **Default:** 2.5F **Tools Affected:** AWB / ECP / ERP / CRE / IAP / IRP

Property	Details
com.fortify. model.PriorityLikelihood Threshold	Specifies the threshold for issue likelihood. The valid values are 0.0F–5.0F. If the likelihood of an issue is greater than or equal to the threshold, the issue is considered High. If the likelihood of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows: • **Critical**—High Impact and High Likelihood • **High**—High Impact and Low Likelihood • **Medium**—Low Impact and High Likelihood • **Low**—Low Impact and Low Likelihood Also see com.fortify.model.PriorityImpactThreshold **Default:** `2.5F` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. model.report.targetEnv	Specifies the target environment to generate RTF format reports. You can control RTF format generation with the following setting: `com.fortify.model.report.targetEnv=<format>` where *<format>* is: • `xp`—Sets the options required for RTF documents to display correctly in Microsoft Word XP (2002) and later. • `word2000`— Sets the options required for RTF documents to display correctly in Microsoft Word 2000 and Microsoft Word 97. • `openOffice`—Sets the options required for RTF documents to display correctly in OpenOffice.Org Writer. • `mac`— Sets the options required for RTF documents to display correctly in Microsoft Word for Mac. **Defaults:** • Windows—`xp` • Linux—`openOffice` • macOS—`mac`

Property	Details
	Tools Affected: | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify.model.report.useSystemLocale	If set to `true`, uses system locale for report output. If set to `false`, uses `com.fortify.locale` in the `fortify.properties` file. If a value is not specified, the tool uses `java.util.Locale.getDefault()`. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify.model.ReportLineLimit	Specifies the character limit for each issue code snippet in reports. **Default:** `500` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify.model.UseIIDMigrationFile	Specifies the full path of the instance ID migration file to use. **Default:** none **Tools Affected:** Also used by FPRUtility | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify.model.UseIssueParseFilters	If set to `true`, respects the settings in the `IssueParseFilters.properties` configuration file. This file is in the following directories: **AWB**—`<sca_install_dir>/Core/config` **ECP**—`<eclipse_install_dir>/plugins/com.fortify.dev.ide.eclipse_<version>/Core/config` **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	

Property	Details
com.fortify. model.UseOldIIDMigration Attributes	If set to `true`, uses attributes of old issues during instance ID migration while merging similar issues of old and new scans. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP
---	---	---	---	---	---	
com.fortify. remediation.PaginateIssues	If set to `true` or if no value is specified, the remediation plugins use pagination during issue download. If set to `false`, these plugins download all issues at once. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP
---	---	---	---	---	---	
com.fortify. remediation.PaginationCount	If `com.fortify.remediation.PaginateIssues` is set to `true`, specifies the page count. **Default:** `1000` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP
---	---	---	---	---	---	
com.fortify. RemovedIssuePersistanceLimit	Specifies how many removed issues to keep when you save an FPR. **Default:** `1000` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP
---	---	---	---	---	---	
com.fortify. SCAExecutablePath	Specifies file path to `sourceanalyzer.exe`. **Note:** The Fortify Static Code Analyzer and Applications installer sets this property during installation and it only requires modification if you manually move the executable files.

Tools Affected highlighted cells:
- UseOldIIDMigrationAttributes: **AWB**, **ECP**
- PaginateIssues: **ERP**, **IRP**
- PaginationCount: **ERP**, **IRP**
- RemovedIssuePersistanceLimit: **AWB**, **ECP**

Property	Details
	Default: `<sca_install_dir>`/bin/sourceanalyzer.exe **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. search.defaultSyntaxVer	Determines whether to use the AND and OR operators in searches. These are enabled in search syntax by default. • To block the use of the AND and OR operators, set the value to 1. • To use ANDs and ORs without parentheses, set the value to 2. **Default:** 2 **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. StoreOriginalDescriptions	If set to `true`, stores original plain text issue descriptions (before parsing) as well as the parsed ones with tags replaced with specific values. **Default:** `false` **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. taintFlagBlacklist	Specifies taint flags to exclude (comma-delimited values). **Default:** none **Tools Affected:** | AWB	ECP	ERP	CRE	IAP	IRP	
com.fortify. tools.iidmigrator.scheme	Set this property to migrate instance IDs created with different versions of Fortify Static Code Analyzer using a custom matching scheme. This is generally handled by Fortify Static Code Analyzer. If you need a custom matching scheme, contact Micro Focus Fortify Customer Support. **Default:** none

Property	Details
	Tools Affected:
	<table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. UseSourceProjectTemplate	If set to `true`, forces the use of filter sets and folders from the issue template associated with the secondary project. The filter sets and folders from the primary project are used by default. **Default:** `false` **Tools Affected:** Also used by FPRUtility <table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>
com.fortify. WorkingDirectory	Specifies the working directory that contains all user configuration and working files for all Fortify Static Code Analyzer components. To configure this property, you must have write access to the directory. **Defaults:** • Windows—`${win32.LocalAppdata}/Fortify` • Unix—`${user.home}/.fortify` **Tools Affected:** <table><tr><td>AWB</td><td>ECP</td><td>ERP</td><td>CRE</td><td>IAP</td><td>IRP</td></tr></table>

Chapter 2: Fortify Extension for Visual Studio Properties

This section describes the properties used by the Micro Focus Fortify Extension for Visual Studio. The properties are listed in alphabetical order based on the files in which they belong.

This section contains the following topics:

Fortify Properties (fortify.properties File)

Some of the properties described here already exist in the `fortify.properties` file, and some of them you must add yourself. The `fortify.properties` file is in the `<sca_install_dir>\Core\config` directory.

The following table describes the properties in the `fortify.properties` file.

Property	Details
com.fortify. audit.ui.DisableBugtrackers	If set to `true`, disables bug tracker integration. **Default:** `false`
com.fortify. audit.ui.DisableSuppress	If set to `true`, disables issue suppression. **Default:** `false`
com.fortify. AuthenticationKey	Specifies the directory used to store the Micro Focus Fortify Software Security Center client authentication token. **Default:** `${com.fortify.WorkingDirectory}/config/tools`
com.fortify. Debug	If set to `true`, runs all Fortify Static Code Analyzer tools in debug mode. **Default:** `false`
com.fortify. model.CustomDescriptionsHeader	Specifies the custom prefix for the description header. It prepends the text in the `Description/Recommendation` header, so that you see "My Recommendations" instead of

Property	Details
	"Custom Recommendations."
	Note: To update description headers, Fortify recommends that you use the `<CustomDescriptionRule>` rule with the `<Header>` element text instead.
	Default: none
com.fortify. model.ForceIIDMigration	If set to `true`, forces running Instance ID migration during a merge.
	Default: `false`
com.fortify. model.PriorityImpactThreshold	Specifies the threshold for issue impact. The valid values are 0.0F–5.0F. If the impact of an issue is greater than or equal to the threshold, the issue is considered High. If the impact of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows:
	• **Critical**—High Impact and High Likelihood
	• **High**—High Impact and Low Likelihood
	• **Medium**—Low Impact and High Likelihood
	• **Low**—Low Impact and Low Likelihood
	Also see com.fortify.model.PriorityLikelihoodThreshold
	Default: `2.5F`
com.fortify. model.PriorityLikelihoodThreshold	Specifies the threshold for issue likelihood. The valid values are 0.0F–5.0F. If the likelihood of an issue is greater than or equal to the threshold, the issue is considered High. If the likelihood of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows:
	• **Critical**—High Impact and High Likelihood
	• **High**—High Impact and Low Likelihood
	• **Medium**—Low Impact and High Likelihood
	• **Low**—Low Impact and Low Likelihood
	Also see com.fortify.model.PriorityImpactThreshold
	Default: 2.5F

Property	Details
com.fortify. model.UseIIDMigrationFile	Specifies the full path of the instance ID migration file to use. **Default:** none
com.fortify. SCAExecutablePath	Specifies file path to `sourceanalyzer.exe`. **Note:** The Fortify Static Code Analyzer and Applications installer sets this property during installation and it only requires modification if you manually move the executable files. **Default:** `<sca_install_dir>/bin/sourceanalyzer.exe`
com.fortify. search.defaultSyntaxVer	Determines whether to use the AND and OR operators in searches. These are enabled in search syntax by default. • To block the use of the AND and OR operators, set the value to 1. • To use ANDs and ORs without parentheses, set the value to 2. **Default:** 2
com.fortify. tools.iidmigrator.scheme	Set this property to migrate instance IDs created with different versions of Fortify Static Code Analyzer using a custom matching scheme. This is generally handled by Fortify Static Code Analyzer. If you need a custom matching scheme, contact Micro Focus Fortify Customer Support. **Default:** none
com.fortify. visualstudio.vm.args	Specifies JVM options. **Default:** `-Xmx256m`
com.fortify. VS.Debug	If set to `true`, runs the Fortify Extension for Visual Studio in debug mode. **Default:** `false`
com.fortify. VS.DisableCIntegration	If set to `true`, disables C/C++ build integration in Visual Studio. **Default:** `false`
com.fortify. VS.disableMigrationCheck	If set to `true`, disables instance ID migration checking. **Default:** `false`

Property	Details
com.fortify. VS.DisableReferenceLibDirs AndExcludes	If set to `true`, disables using references added to a project. **Default:** `false`
com.fortify. VS.ListProjectProperties	If set to `true`, lists the Visual Studio project properties in a log file. **Default:** `false`
com.fortify. VS.NETFrameworkRoot	Specifies the file path to the .NET Framework root. **Default:** none
com.fortify. WorkingDirectory	Specifies the working directory that contains all user configuration and working files for all Fortify Static Code Analyzer components. To configure this property, you must have write access to the directory. **Default:** `${win32.LocalAppdata}/Fortify`

TFS Configuration Property

The `TFSconfiguration.properties` file is in the Fortify working directory in the `config\VS<vs_version>-<sca_version>` directory.

> **Note:** The `TFSconfiguration.properties` file is created only after the first time you configure a connection to your Team Foundation Server/Azure DevOps Server from the Fortify Extension for Visual Studio.

The following property is in the `TFSconfiguration.properies` file:

`server.url`
Default: none

Details: Specifies the Team Foundation Server or Azure DevOps Server location.

Chapter 3: Shared Server Properties

This chapter describes the properties used by all Micro Focus Fortify Static Code Analyzer command-line tools, standalone applications, and plugins.

Server Properties (server.properties File)

Because some of the values in this file are encrypted (such as proxy user name and password), you must use the scapostinstall tool to configure these properties. For information about how to use the scapostinstall tool, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

Other properties are updated using command-line tools, standalone applications (such as Fortify Audit Workbench), and remediation plugins. Fortify recommends that you use these tools to edit the properties in this file instead of editing the file manually.

The following table describes the properties in the `server.properties` file.

Property	Details
autoupgrade.server	Specifies the Fortify Static Code Analyzer and Applications automatic update server. This enables users to check for new versions of the Fortify Static Code Analyzer and Applications installer on a web server and run the installer if an update is available. **Default:** `http://localhost:8180/ssc/update-site/installers`
install.auto.upgrade	If set to `true`, enables Fortify Audit Workbench automatic update feature. **Default:** `false`
oneproxy.http.proxy.port	Specifies the proxy server port to access bug trackers. **Default:** none
oneproxy.http.proxy.server	Specifies the proxy server name to access bug trackers. **Default:** none
oneproxy.https.proxy.port	Specifies the proxy server port to access bug trackers through an SSL connection. **Default:** none

Property	Details
oneproxy.https.proxy.server	Specifies the proxy server name to access bug trackers through an SSL connection. **Default:** none
rp.update.from.manager	If set to `true`, updates security content from the Fortify Software Security Center instead of from the Fortify Rulepack update server. **Default:** `false`
rulepack.auto.update	If set to `true`, updates security content automatically. **Default:** `false`
rulepack.days	Specifies the interval (in days) between security content updates. **Default:** 15
rulepackupdate.proxy.port	Specifies the proxy server port to access the Fortify Rulepack update server (`uploadclient.proxy.port` is used if `rp.update.from.manager` is set to `true`). **Default:** none
rulepackupdate.proxy.server	Specifies proxy server name to access the Fortify Rulepack update server (`uploadclient.proxy.server` is used if `rp.update.from.manager` is set to `true`). **Default:** none
rulepackupdate.server	Specifies the Fortify Rulepack update server location. **Default:** `https://update.fortify.com`
uploadclient.proxy.port	Specifies the proxy server port to access the Fortify Software Security Center server. **Default:** none
uploadclient.proxy.server	Specifies the proxy server name to access the Fortify Software Security Center server. **Default:** none
uploadclient.server	Specifies the URL of the Fortify Software Security Center server. **Default:** `http://localhost:8180/ssc`

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Properties Reference Guide (Fortify Static Code Analyzer Tools 19.2.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to FortifyDocTeam@microfocus.com.

We appreciate your feedback!