Micro Focus
Fortify Static Code Analyzer

Software Version: 18.20

Installation Guide

Document Release Date: November 2018
Software Release Date: November 2018

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

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

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 only if the changes made affect product functionality.

Software Release / Document Version	Changes
18.20	Updated: • "Installing Fortify Static Code Analyzer and Applications" on page 13 - You are no longer required to have administrative privileges to install the Fortify Extension for Visual Studio 2013
18.10	Updated: • "About Installing Fortify Static Code Analyzer and Applications" on page 12 and "About Uninstalling Fortify Static Code Analyzer and Applications" on page 17 - Installer file names were changed for rebranding • "Removing Proxy Server Settings" on page 21 - Method to remove proxy settings is the same for Fortify Rulepack update server and Fortify Software Security Center
17.20	Added: • "About Upgrading Fortify Static Code Analyzer and Applications" on page 16 Updated: • "Installing Fortify Static Code Analyzer and Applications" on page 13 and "Installing Fortify Static Code Analyzer and Applications Silently (Unattended)" on page 14 - Installation of the sample source code projects is now optional

Chapter 1: Introduction

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

This section contains the following topics:

Intended Audience

This installation guide is intended for individuals who are responsible for installing or uninstalling Fortify Static Code Analyzer and Fortify Static Code Analyzer tools. This guide also describes basic post-installation tasks.

See the *Micro Focus Fortify Software System Requirements* document to be sure that your system meets the minimum requirements for each software component installation.

Fortify Security Content

Fortify Static Code Analyzer uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. Fortify releases quarterly Micro Focus Fortify Software Security Content updates. They are distributed as part of the subscription service through updates on the Fortify Customer Portal, automated tool updates, and software releases. Security content consists of Micro Focus Fortify Secure Coding Rulepacks and external metadata:

- Secure Coding Rulepacks describe general secure coding idioms for popular languages and public APIs.
- External metadata includes mappings from the Fortify Taxonomy to alternative categories (such as CWE, OWASP Top 10, and PCI DSS).

You can download the Fortify Security Content during the Windows installation. Alternatively, you can download or import previously downloaded Fortify Security Content with the fortifyupdate utility as a post-installation task (see "Updating Fortify Security Content" on page 22).

Fortify Static Code Analyzer Component Applications

The installation consists of Fortify Static Code Analyzer, which analyzes your build code according to a set of rules specifically tailored to provide the information necessary for the type of analysis performed.

A Fortify Static Code Analyzer installation might also include one or more of the following component applications:

- Micro Focus Fortify Audit Workbench—Provides a graphical user interface for Fortify Static Code Analyzer that helps you organize, investigate, and prioritize analysis results so that developers can fix security flaws quickly.
- Micro Focus Fortify Plugin for Eclipse—Adds the ability to scan and analyze the entire codebase of a project and apply software security rules that identify the vulnerabilities in your Java code from the Eclipse IDE. The results are displayed, along with descriptions of each of the security issues and suggestions for their elimination.
- Micro Focus Fortify Remediation Plugin for Eclipse—Works with Micro Focus Fortify Software Security Center for developers who want to remediate issues detected in source code from the Eclipse IDE.
- Micro Focus Fortify Extension for Visual Studio—Adds the ability to scan and locate security vulnerabilities in your solutions and projects 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. This extension also includes remediation functionality that works with audit results stored on a Fortify Software Security Center server.
- Micro Focus Fortify Analysis Plugin for IntelliJ and Android Studio—Adds the ability to run Fortify Static Code Analyzer scans on the entire codebase of a project and apply software security rules that identify the vulnerabilities in your code from the IntelliJ and Android Studio IDEs.
- Micro Focus Fortify Remediation Plugin for IntelliJ, WebStorm, and Android Studio—Works in the IntelliJ, WebStorm, and Android Studio IDEs and with Fortify Software Security Center to add remediation functionality to your security analysis.
- Micro Focus Fortify Jenkins Plugin—Provides the ability to analyze a project with Fortify Static Code Analyzer, upload analysis results to Fortify Software Security Center, and view details about the results from Jenkins.
- Micro Focus Fortify Custom Rules Editor—A tool to create and edit custom rules.
- Micro Focus Fortify Scan Wizard—Tool to quickly prepare a script that you can use to scan your code with Fortify Static Code Analyzer and optionally, upload the results directly to Fortify Software Security Center.

Related Documents

This topic describes documents that provide information about Micro Focus Fortify software products.

> **Note:** You can find the Micro Focus Fortify Product Documentation at https://www.microfocus.com/support-and-services/documentation.

All Products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website.

Document / File Name	Description
About Micro Focus Fortify Product Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Micro Focus Fortify product documentation. **Note:** This document is included only with the product download.
Micro Focus Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf Fortify_Sys_Reqs_Help_<*version*>	This document provides the details about the environments and products supported for this version of Fortify Software.
Micro Focus Fortify Software Release Notes FortifySW_RN_<*version*>.txt	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Micro Focus Fortify Software <version> Fortify_Whats_New_<*version*>.pdf Fortify_Whats_New_Help_<*version*>	This document describes the new features in Fortify Software products.
Micro Focus Fortify Open Source and Third-Party License Agreements Fortify_OpenSrc_<*version*>.pdf Fortify_OpenSrc_<*version*>	This document provides open source and third-party software license agreements for software components used in Fortify Software.

Micro Focus Fortify Static Code Analyzer

The following documents provide information about Fortify Static Code Analyzer. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website.

Document / File Name	Description
Micro Focus Fortify Static Code Analyzer Installation Guide SCA_Install_<*version*>.pdf	This document contains installation instructions for Fortify Static Code Analyzer and Applications.

Document / File Name	Description
SCA_Install_Help_*<version>*	
Micro Focus Fortify Static Code Analyzer User Guide SCA_Guide_*<version>*.pdf SCA_Help_*<version>*	This document describes how to use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
Micro Focus Fortify Static Code Analyzer Performance Guide SCA_Perf_Guide_*<version>*.pdf SCA_Perf_Help_*<version>*	This document provides guidelines for selecting hardware to scan different types of codebases and offers tips for optimizing memory usage and performance.
Micro Focus Fortify Static Code Analyzer Custom Rules Guide SCA_Cust_Rules_Guide_*<version>*.zip SCA_Cust_Rules_Help_*<version>*	This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note:** This document is included only with the product download.
Micro Focus Fortify Audit Workbench User Guide AWB_Guide_*<version>*.pdf AWB_Help_*<version>*	This document describes how to use Fortify Audit Workbench to scan software projects and audit analysis results. This guide also includes how to integrate with bug trackers, produce reports, and perform collaborative auditing.
Micro Focus Fortify Plugins for Eclipse Installation and Usage Guide Eclipse_Plugins_Guide_*<version>*.pdf Eclipse_Plugins_Help_*<version>*	This document provides information about how to install and use the Fortify Complete and the Fortify Remediation Plugins for Eclipse.
Micro Focus Fortify Plugins for IntelliJ, WebStorm, and Android Studio Installation and Usage Guide IntelliJ_AndStud_Plugins_Guide_*<version>*.pdf IntelliJ_AndStud_Plugins_Help_*<version>*	This document describes how to install and use both the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio and the Fortify Remediation Plugin for IntelliJ IDEA, Android Studio, and WebStorm.
Micro Focus Fortify Jenkins Plugin Installation and Usage Guide Jenkins_Plugin_Guide_*<version>*.pdf Jenkins_Plugin_Help_*<version>*	This document provides how to install, configure, and use the plugin.

Document / File Name	Description
Micro Focus Fortify Security Assistant Plugin for Eclipse User Guide SecAssist_Eclipse_Guide_<*version*>.pdf SecAssist_Eclipse_Help_<*version*>	This document describes how to install and use Fortify Security Assistant plugin for Eclipse to provide alerts to security issues as you write your Java code.
Micro Focus Fortify Extension for Visual Studio User Guide VS_Ext_Guide_<*version*>.pdf VS_Ext_Help_<*version*>	This document provides information about how to install and use the Fortify extension for Visual Studio to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects.
Micro Focus Fortify Static Code Analyzer Tools Properties Reference Guide SCA_Tools_Props_Ref_<*version*>.pdf SCA_Tools_Props_Ref_Help_<*version*>	This document describes the properties used by Fortify Static Code Analyzer tools.

Chapter 2: Installation

This section contains the following topics:

About Downloading the Software

Fortify Static Code Analyzer and Applications is available as a downloadable application or package. For details on how to acquire the software and a license for the Fortify Software, see the *Micro Focus Fortify Software System Requirements* document.

About Installing Fortify Static Code Analyzer and Applications

This section describes how to install Fortify Static Code Analyzer and applications. You need a Fortify license file to complete the process. You can use the standard install wizard or you can perform the installation silently. You can also perform a text-based installation on non-Windows systems. For best performance, install Fortify Static Code Analyzer on the same local file system where the code that you want to scan resides.

> **Note:** On non-windows systems, you must install Fortify Static Code Analyzer and applications as a user that has a home directory with write permission. Do not install Fortify Static Code Analyzer and applications as a non-root user that has no home directory.

After you complete the installation, see "Post-Installation Tasks" on page 19 for additional steps you can perform to complete your system setup. You can also configure settings for runtime analysis, output, and performance of Fortify Static Code Analyzer and its components by updating the installed configuration files. For information about the configuration options for Fortify Static Code Analyzer, see the *Micro Focus Fortify Static Code Analyzer User Guide*. For information about configuration options for Fortify Static Code Analyzer component applications, see the *Micro Focus Fortify Static Code Analyzer Tools Properties Reference Guide*.

Installing Fortify Static Code Analyzer and Applications

To install Fortify Static Code Analyzer and Applications:

1. Run the installer file that corresponds to your operating system:
   - Windows: `Fortify_SCA_and_Apps_<version>_windows_x64.exe`
   - macOS: `Fortify_SCA_and_Apps_<version>_osx_x64.app.zip`
   - Linux: `Fortify_SCA_and_Apps_<version>_linux_x64.run`
   - Solaris: `Fortify_SCA_<version>_solaris_x86.run` or `Fortify_SCA_<version>_solaris10_sparc.run`
   - HP-UX: `Fortify_SCA_<version>_hpux_ia64.run`
   - AIX: `Fortify_SCA_<version>_aix_x64.run`

   where <*version*> is the software release version.
2. Accept the license agreement, and then click **Next**.
3. Choose where to install Fortify Static Code Analyzer and applications, and then click **Next**.

   > **Note:** If you are using Micro Focus Fortify CloudScan, you must specify a location that does not include spaces in the path.

4. (Optional) Select the components to install, and then click **Next**.

   > **Note:** Component selection is not available for all operating systems.

5. If you are installing the Fortify extension for Visual Studio 2015 or 2017, you are prompted to specify whether to install the extensions for the current install user or for all users.

   The default is to install the extensions for the current install user.
6. Specify the path to the `fortify.license` file, and then click **Next**.
7. Specify the settings required to update your security content.

   To update the security content for your installation:

   > **Note:** For installations on non-Windows platforms and for deployment environments that do not have access to the Internet during installation, you can update the security content using the fortifyupdate utility. See "Updating Fortify Security Content" on page 22.

   a. Specify the URL address of the update server. To use the Fortify Rulepack update server for security content updates, specify the URL as: `https://update.fortify.com`.
   b. (Optional) Specify the proxy host and port number of the update server.
   c. Click **Next**.
8. Specify if you want to migrate from a previous installation of Fortify Static Code Analyzer on your system.

   Migrating from a previous Fortify Static Code Analyzer installation preserves Fortify Static Code Analyzer artifact files.

> **Note:** You can also migrate Fortify Static Code Analyzer artifacts using the `scapostinstall` command-line utility. For information on how to use the post-install tool to migrate from a previous Fortify Static Code Analyzer installation, see "Migrating Properties Files" on page 19.

To migrate artifacts from a previous installation:

a. In the **SCA Migration** step, select **Yes**, and then click **Next**.
b. Specify the location of the existing Fortify Static Code Analyzer installation on your system, and then click **Next**.

9. Specify if you want to install sample source code projects, and then click **Next**.

   Descriptions of the samples are available in both the *Micro Focus Fortify Static Code Analyzer User Guide* and the *Micro Focus Fortify Audit Workbench User Guide*.

   > **Note:** If you do not install the samples and decide later that you want to install them, you must uninstall and then re-install Fortify Static Code Analyzer and Applications.

10. Click **Next** to proceed to install Fortify Static Code Analyzer and applications.
11. After Fortify Static Code Analyzer is installed, select **Update security content after installation** if you want to update the security content, and then click **Finish**.

    The Security Content Update Result window displays the security content update results.

Installing Fortify Static Code Analyzer and Applications Silently (Unattended)

A silent installation enables you to complete the installation without any user prompts. To install silently, you need to create an option file to provide the necessary information to the installer. Using the silent installation, you can replicate the installation parameters on multiple machines. When you install Fortify Static Code Analyzer and Applications silently, the installer does not download the Micro Focus Fortify Software Security Content. For instructions on how to download the Fortify Security Content, see "Updating Fortify Security Content" on page 22.

To install Fortify Static Code Analyzer silently:

1. Create an options file.

   a. Create a text file that contains the following line:

   ```
   fortify_license_path=<license_file_location>
   ```

   where <*license_file_location*> is the full path to your `fortify.license` file.

   b. If you are using a different location for the Fortify Security Content updates than the default of `https://update.fortify.com`, add the following line:

   ```
   UpdateServer=<update_server_url>
   ```

c. If you require a proxy server, add the following lines:

   ```
   UpdateProxyServer=<proxy_server>
   UpdateProxyPort=<port_number>
   ```

d. If you do not want to install the sample source code projects, add the following line:

   ```
   InstallSamples=0
   ```

e. Add more information, as needed, to the options file.

   For list of installation options that you can add to your options file, type the installer file name and the `--help` option. This command displays the command-line options preceded with a double dash and optional file parameters enclosed in angle brackets. For example, if you want to see the progress of the install displayed at the command line, add `unattendedmodeui=minimal` to your options file.

   The following options file example specifies the location of the license file, the location and proxy information for obtaining the Fortify Security Content, a request to migrate from a previous release, installation of Audit Workbench, installation of Fortify Extension for Visual Studio 2017 for all users, and the location of the Fortify Static Code Analyzer and Applications installation directory:

   ```
   fortify_license_path=C:\Users\admin\Desktop\fortify.license
   UpdateServer=https://internalserver.abc.com
   UpdateProxyServer=webproxy.abc.company.com
   UpdateProxyPort=8080
   MigrateSCA=1
   enable-components=AWB_group,VS2017
   VS_all_users=1
   installdir=C:\Fortify
   ```

2. Save the options file in the same directory as the installer using the same name as the installation file with the `.options` file extension.

   For example, if the installer file name is: `Fortify_SCA_and_Apps_<version>_windows_x64.exe`, then save your options file with the name `Fortify_SCA_and_Apps_<version>_windows_x64.exe.options`.

3. Run the silent install command for your operating system:

Windows	`Fortify_SCA_and_Apps_<version>_windows_x64.exe --mode unattended`
Linux	`./Fortify_SCA_and_Apps_<version>_linux_x64.run --mode unattended`

macOS	You must uncompress the zip file before you run the command. `Fortify_SCA_and_Apps_<version>_osx_x64.app/Contents/MacOS/installbuilder.sh --mode unattended --optionfile <full_path_to_option_file>`
AIX, HP-UX, and Solaris	`./Fortify_SCA_<version>_<platform>.run --mode unattended`

Installing Fortify Static Code Analyzer and Applications in Text-Based Mode on Non-Windows Platforms

You perform a text-based installation on the command line. During the installation, you are prompted for information required to complete the installation. Text-based installations are not supported on Windows systems.

To perform a text-based installation of Fortify Static Code Analyzer and Applications, run the text-based install command for your operating system as listed in the following table.

Linux	`./Fortify_SCA_and_Apps_<version>_linux_x64.run --mode text`
macOS	You must uncompress the provided zip file before you run the command. `Fortify_SCA_and_Apps_<version>_osx_x64.app/Contents/MacOS/installbuilder.sh --mode text`
AIX, HP-UX, and Solaris	`./Fortify_SCA_<version>_<platform>.run --mode unattended`

About Upgrading Fortify Static Code Analyzer and Applications

To upgrade Fortify Static Code Analyzer and Applications, you can either:

- Uninstall the existing version and then install the new version
- Install the new version without uninstalling the existing version. You can have multiple versions of Fortify Static Code Analyzer installed on the same system.

  If you have multiple versions installed on the same system, the most recently installed version is invoked when you run the command from the command line. Scanning source code from the Secure Code Plugins also uses the most recently installed version of Fortify Static Code Analyzer.

When you install the new version, you are asked if you want to migrate settings from a previous installation. This migration preserves Fortify Static Code Analyzer artifact files.

Notes About Upgrading the Fortify Extension for Visual Studio

If you have administrative privileges and are upgrading from a previous version of the Fortify Static Code Analyzer for any supported version of Visual Studio, the installer will overwrite the existing Micro Focus Fortify Extension for Visual Studio. If the previous version was installed without administrative privileges, the installer will also overwrite the existing Fortify Extension for Visual Studio without requiring administrative privileges.

> **Note:** If you do not have administrative privileges and you are upgrading the Fortify Extension for Visual Studio 2015 or 2017 that was previously installed using an administrative privileged user account, you must first uninstall the Fortify Extension for Visual Studio from Visual Studio 2015 or 2017 using an administrative privilege account.

About Uninstalling Fortify Static Code Analyzer and Applications

This section describes how to uninstall Fortify Static Code Analyzer and Applications. You can use the standard install wizard or you can perform the uninstallation silently. You can also perform a text-based uninstallation on non-Windows systems.

Uninstalling Fortify Static Code Analyzer and Applications

Uninstalling on Windows Platforms

To uninstall the Fortify Static Code Analyzer and applications software:

1. Select **Start > Control Panel > Add or Remove Programs**.
2. From the list of programs, select **Fortify SCA and Applications <*version*>**, and then click **Remove**.
3. You are prompted to indicate whether to remove all application settings. Do one of the following:
   - Click **Yes** to remove the application setting folders for the tools associated with the version of Fortify Static Code Analyzer that you are uninstalling. The Fortify Static Code Analyzer (`sca<version>`) folder is not removed.
   - Click **No** to retain the application settings on your system.

Uninstalling on Other Platforms

To uninstall Fortify Static Code Analyzer software on macOS, Unix, and Linux platforms:

1. Back up your configuration, including any important files you have created.
2. Run the uninstall command located in the `<sca_install_dir>` for your operating system:

Unix or Linux	`Uninstall_FortifySCAandApps_<version>.exe`

macOS	`Uninstall_FortifySCAandApps_<version>.app`

3. You are prompted to indicate whether to remove all application settings. Do one of the following:
   - Click **Yes** to remove the application setting folders for the tools associated with the version of Fortify Static Code Analyzer that you are uninstalling. The Fortify Static Code Analyzer (`sca<version>`) folder is not removed.
   - Click **No** to retain the application settings on your system.

Uninstalling Fortify Static Code Analyzer and Applications Silently

To uninstall Fortify Static Code Analyzer silently:

1. Navigate to the installation directory.
2. Type one of the following commands based on your operating system:

Windows	`Uninstall_FortifySCAandApps_<version>.exe --mode unattended`
Unix or Linux	`./Uninstall_FortifySCAandApps_<version>.run --mode unattended`
macOS	`Uninstall_FortifySCAandApps_<version>.app/Contents/MacOS/installbuilder.sh --mode unattended`

Note: The uninstaller removes the application setting folders associated with the version of Fortify Static Code Analyzer that you are uninstalling.

Uninstalling Fortify Static Code Analyzer and Applications in Text-Based Mode on Non-Windows Platforms

To uninstall Fortify Static Code Analyzer in text-based mode, run the text-based install command for your operating system, as follows:

1. Navigate to the installation directory.
2. Type one of the following commands based on your operating system:

Unix or Linux	`./Uninstall_FortifySCAandApps_<version>.run --mode text`
macOS	`Uninstall_FortifySCAandApps_<version>.app/Contents/MacOS/installbuilder.sh --mode text`

Chapter 3: Post-Installation Tasks

Post-installation tasks prepare you to start using Fortify Static Code Analyzer and tools.

This section contains the following topics:

Running the Post-Install Tool

To run the Fortify Static Code Analyzer post-install tool:

1. Navigate to the `bin` directory from the command line.
2. At the command prompt, type `scapostinstall`.
3. Type one of the following:
   - To display settings, type `s`.
   - To return to a previous prompt, type `r`.
   - To exit the tool, type `q`.

Migrating Properties Files

To migrate properties files from a previous version of Fortify Static Code Analyzer to the current version of Fortify Static Code Analyzer installed on your system:

1. Navigate to the `bin` directory from the command line.
2. At the command prompt, type `scapostinstall`.
3. Type `1` to select `Migration`.
4. Type `1` to select `SCA Migration`.
5. Type `1` to select `Migrate from an existing Fortify installation`.
6. Type `1` to select `Set previous Fortify installation directory`.
7. Type the previous install directory.
8. Type `s` to confirm the settings.

9. Type `2` to perform the migration.
10. Type `y` to confirm.

Specifying a Locale

English is the default locale for a Fortify Static Code Analyzer installation.

To change the locale for your Fortify Static Code Analyzer installation:

1. Navigate to the `bin` directory from the command line.
2. At the command prompt, type `scapostinstall`.
3. Type `2` to select `Settings`.
4. Type `1` to select `General`.
5. Type `1` to select `Locale`.
6. Type one of the following locale codes:
   - English: `en`
   - Spanish: `es`
   - Japanese: `ja`
   - Korean: `ko`
   - Brazilian Portuguese: `pt_BR`
   - Simplified Chinese: `zh_CN`
   - Traditional Chinese: `zh_TW`

Configuring for Security Content Updates

Specify how you want to obtain Micro Focus Fortify Software Security Content. You must also specify proxy information if it is required to reach the server.

To specify settings for Fortify Security Content updates:

1. Navigate to the `bin` directory from the command line.
2. At the command prompt, type `scapostinstall`.
3. Type `2` to select `Settings`.
4. Type `2` to select `Fortify Update`.
5. To change the Fortify Rulepack update server URL, type `1` and then type the URL.

   The default Fortify Rulepack update server URL is `https://update.fortify.com`.

6. To specify a proxy for Fortify Security Content updates, do the following:
   a. Type `2` to select `Proxy Server Host`, and then type the name of the proxy server.
   b. Type `3` to select `Proxy Server Port`, and then type the proxy server port number.
   c. (Optional) You can also specify the proxy server user name (option `4`) and password (option `5`).

Configuring the Connection to Fortify Software Security Center

Specify how to connect to Micro Focus Fortify Software Security Center. If your network uses a proxy server to reach the Fortify Software Security Center server, you must specify the proxy information.

To specify settings for connecting to Fortify Software Security Center:

1. Navigate to the `bin` directory from the command line.
2. At the command prompt, type `scapostinstall`.
3. Type `2` to select `Settings`.
4. Type `3` to select `Software Security Center Settings`.
5. Type `1` to select `Server URL`, and then type the Fortify Software Security Center server URL.

   For example, `https://mywebserver/ssc`.
6. To specify proxy settings for the connection, do the following:
   a. Type `2` to select `Proxy Server`, and then type the proxy server path.
   b. Type `3` to select `Proxy Server Port`, and then type the proxy server port number.
   c. To specify the proxy server username and password, use option `4` for the username and option `5` for the password.
7. (Optional) You can also specify the following:
   - Whether to update security content from your Fortify Software Security Center server (option `6`)
   - The Fortify Software Security Center user name (option `7`)

Removing Proxy Server Settings

If you previously specified proxy server settings for the Fortify Security Content update server or Micro Focus Fortify Software Security Center and it is no longer required, you can remove these settings.

To remove the proxy settings for Fortify Security Content updates or Fortify Software Security Center:

1. Navigate to the `bin` directory from the command line.
2. At the command prompt, type `scapostinstall`.
3. Type `2` to select `Settings`.
4. Type `2` to select `Fortify Update` or type `3` to select `Software Security Center Settings`.

5. Type the number that corresponds to the proxy setting you want to remove, and then type - (hyphen) to remove the setting.
6. Repeat step 5 for each proxy setting you want to remove.

Updating Fortify Security Content

Micro Focus Fortify Software Security Content (Secure Coding Rulepacks and metadata) is updated automatically during the Windows installation procedure. However, you can also download Fortify Security Content from the Fortify Rulepack update server, and then use the fortifyupdate utility to update it. This option is provided for installations on non-Windows platforms and for deployment environments that do not have access to the Internet during installation.

Use the fortifyupdate utility to update Fortify Security Content from either a remote server or a locally downloaded file.

To update security content:

1. Open a command window.
2. Navigate to the `<sca_install_dir>/bin` directory.
3. At the command prompt, type `fortifyupdate`.

   If you have previously downloaded the Fortify Security Content from the Fortify Customer Portal, run `fortifyupdate` with the `-import` option and the path to the directory where you downloaded the zip file.

For more detailed instructions about the fortifyupdate utility, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

Registering ASP.NET Applications

If you are using the .NET Framework, you might need to register ASP.NET applications. If the Internet Information Services (IIS) server is installed first, then ASP.NET 4 is automatically registered with IIS when the .NET Framework is installed; otherwise, you must register.

To register the ASPNET user, run the following command:

```
aspnet_regiis -i
```

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

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319
```

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 Installation Guide (Fortify Static Code Analyzer 18.20)

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!