Hewlett Packard
Enterprise

HPE Security
Fortify Static Code Analyzer

Software Version: 17.10

Installation Guide

IMPORTANT NOTICE

Certain versions of documents ("Material") accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development 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. HPE 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 HPE 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.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

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.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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.protect724.hpe.com/community/fortify/fortify-product-documentation

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

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

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

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products:
http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security 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 HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

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
17.10	Updated: • "About Uninstalling Fortify Static Code Analyzer and Applications" on page 15 - Described the new prompt to remove all application settings • "Specifying a Proxy Server for Security Content Updates" on page 18 and "Specifying a Proxy Server for Fortify Software Security Center" on page 19 - Added instructions for how to remove proxy server settings
16.20	Updated: • "Installing Fortify Static Code Analyzer and Applications" on page 11 and "Installing Fortify Static Code Analyzer and Applications Silently (Unattended)" on page 13 - Updates made for installing the Fortify Visual Studio Package for Visual Studio 2015 without administrative privileges
16.10	Updated: • "Specifying a Locale" on page 18 - Added Brazilian Portuguese

Chapter 1: Introduction

This document contains installation instructions for HPE Security Fortify Static Code Analyzer (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 *HPE Security Fortify Software System Requirements* document to ensure that your system meets the minimum requirements for each software component installation.

HPE Security Fortify Software Security Content

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

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

You can download the security content during the Windows installation or with the fortifyupdate utility as a post-installation task.

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:

- HPE Security 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.
- HPE Security 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.
- HPE Security Fortify Remediation Plugin for Eclipse—Works with HPE Security Fortify Software Security Center (Fortify Software Security Center) for developers who want to remediate issues detected in source code from the Eclipse IDE.
- HPE Security Fortify Package for Visual Studio—Adds the ability to scan and 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. This package also includes remediation functionality that works with Fortify Software Security Center.
- HPE Security 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.
- HPE Security Fortify Remediation Plugin for IntelliJ and Android Studio—Works in the IntelliJ and Android Studio IDEs and Fortify Software Security Center to add remediation functionality to your security analysis.
- HPE Security Fortify Remediation Extension for JDeveloper—Works with Fortify Software Security Center for developers who want to remediate issues detected in source code in the JDeveloper IDE.
- HPE Security Fortify Security Assistant—Integrates with the Eclipse development environment to detect security issues as you write code.
- HPE Security Fortify Jenkins Plugin—Provides the ability to upload analysis results to Fortify Software Security Center and view details about the results from Jenkins.
- HPE Security Fortify Custom Rules Editor—Tool for creating and editing custom rules.
- HPE Security 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.
- HPE Security Fortify Scanning Plugin for Xcode—Enables you to run Fortify Static Code Analyzer scans on projects from the Xcode development environment.

Related Documents

This topic describes documents that provide information about HPE Security Fortify Static Code Analyzer.

Note: The Protect724 site location is https://www.protect724.hpe.com/community/fortify/fortify-product-documentation.

All Products

The following documents provide general information for all products.

Document / File Name	Description	Location
HPE Security Fortify Software System Requirements HPE_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Software Release Notes HPE_FortifySW_RN_<*version*>.txt	This document provides an overview of the changes made to HPE Security Fortify Software for this release and important information not included elsewhere in the product documentation.	Included on the Protect724 site
What's New in HPE Security Fortify Software <version> HPE_Whats_New_<*version*>.pdf	This document describes the new features in HPE Security Fortify Software products.	Included on the Protect724 site
HPE Security Fortify Open Source and Third-Party License Agreements HPE_OpenSrc_<*version*>.pdf	This document provides open source and third-party software license agreements for software components used in HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Glossary HPE_Glossary.pdf	This document provides definitions for HPE Security Fortify Software terms.	Included with product download and on the Protect724 site

HPE Security Fortify Static Code Analyzer

The following documents provide information about Static Code Analyzer.

Document / File Name	Description	Location
HPE Security Fortify Static Code Analyzer User Guide HPE_SCA_Guide_<*version*>.pdf HPE_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.	Included with product download and on the Protect724 site

Document / File Name	Description	Location
HPE Security Fortify Static Code Analyzer Installation Guide HPE_SCA_Install_<*version*>.pdf HPE_SCA_Install_Help_<*version*>	This document contains installation instructions for Fortify Static Code Analyzer and Applications.	Included with product download and on the Protect724 site
HPE Security Fortify Static Code Analyzer Performance Guide HPE_SCA_Perf_Guide_<*version*>.pdf PDF only; no help file	This document provides guidelines for selecting hardware to scan different types of codebases and offers tips for optimizing memory usage and performance.	Included with product download and on the Protect724 site
HPE Security Fortify Static Code Analyzer Custom Rules Guide HPE_SCA_Cust_Rules_Guide_<*version*>.zip PDF only; no help file	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.	Included with product download

Technology Previews

Document / File Name	Description	Location
HPE Security Fortify Static Code Analyzer Higher Order Analysis Technology Preview HPE_SCA_HighOrderAnalysis_TP_<*version*>.pdf PDF only; no help file	This document describes the Fortify Static Code Analyzer Higher Order Analyzer.	Included with product download and on the Protect724 site
HPE Security Fortify Static Code Analyzer AngularJS Technology Preview HPE_SCA_AngularJS_TP_<*version*>.pdf PDF only; no help file	This document describes the Fortify Static Code Analyzer support for AngularJS.	Included with product download and on the Protect724 site

Chapter 2: Installation

This section contains the following topics:

About Downloading the Software

HPE Security Fortify Static Code Analyzer and Applications is available as a downloadable application or package. For details on how to obtain a license for the HPE Security Fortify Software, see the *HPE Security 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 an HPE Security 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.

Note: For more information about how to acquire the software and license for your operating system, see the *HPE Security Fortify Software System Requirements* document.

After you complete the installation, see "Post-Installation Tasks" on page 17 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 *HPE Security Static Code Analyzer User Guide*. For information about configuration options for Fortify Static Code Analyzer component applications, see the *HPE Security 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: `HPE_Security_Fortify_SCA_and_Apps_<version>_windows_x64.exe`
   - Mac OS: `HPE_Security_Fortify_SCA_and_Apps_<version>_osx_x64.app.zip`
   - Unix or Linux: `HPE_Security_Fortify_SCA_and_Apps_<version>_linux_x64.run`

- Solaris: `HPE_Security_Fortify_SCA_<version>_solaris_x86.run` or `HPE_Security_Fortify_SCA_<version>_solaris10_sparc.run`
- HP-UX: `HPE_Security_Fortify_SCA_<version>_hpux_ia64.run`
- AIX: `HPE_Security_Fortify_SCA_<version>_aix_x64.run`

where <*version*> is the software release version.

2. Accept the license agreement and click **Next**.
3. Choose where to install Fortify Static Code Analyzer and applications, and then click **Next**.

   Note: If you are using HPE Security Fortify CloudScan, you must specify a location that does not include spaces in the path.

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

   Notes:

   - You must have administrative privileges to install the Fortify Visual Studio Package for Visual Studio 2012 and Visual Studio 2013.
   - If you have administrative privileges and are upgrading from a previous version of the Fortify Visual Studio Package for any supported version of Visual Studio, the installer will overwrite the existing Fortify Visual Studio Package.

     However, if you do not have administrative privileges and you are upgrading the Fortify Visual Studio Package for Visual Studio 2015, you must first uninstall the Fortify Visual Studio Package for Visual Studio 2015 before installing this version.
   - Component selection is not available for all operating systems.

5. Specify the path to the `fortify.license` file, and then click **Next**.
6. 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 Security Content" on page 20.

   a. Specify the URL address of the update server. To use the Fortify Customer Portal 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**.

7. 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 17.

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**.

8. Click **Next** to proceed to install Fortify Static Code Analyzer and applications.
9. 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 security content. For instructions on how to download the security content, see "Updating Security Content" on page 20.

Note: If you do not have administrative privileges and you are upgrading from a previous version of the Fortify Visual Studio Package for Visual Studio 2015, HPE recommends that you uninstall the previous version of the Fortify Visual Studio Package before you install Fortify Static Code Analyzer and Applications. Otherwise, because the installer cannot uninstall the previous version without administrative privileges, you will have two Fortify Visual Studio Packages installed in Visual Studio 2015.

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 require a proxy server, add the following lines:

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

   c. Add 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.

Example of an options file:

```
fortify_license_path=C:\Users\admin\Desktop\fortify.license
UpdateProxyServer=web-proxy.abc.company.com
UpdateProxyPort=8080
MigrateSCA=0
enable-components=AWB_group,VS2015
installdir=C:\HPE_Security_Fortify
```

d. 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: `HPE_Security_Fortify_SCA_and_Apps_<version>_windows_x64.exe`, then save your options file with the name `HPE_Security_Fortify_SCA_and_Apps_<version>_windows_x64.exe.options`.

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

Windows	`HPE_Security_Fortify_SCA_and_Apps_<version>_windows_x64.exe --mode unattended`
Unix or Linux	`./HPE_Security_Fortify_SCA_and_Apps_<version>_linux_x64.run --mode unattended`
Mac OS	You must uncompress the zip file before running the command. `HPE_Security_Fortify_SCA_and_Apps_<version>_osx_x64.app/Contents/MacOS/installbuilder.sh --mode unattended --optionfile <full_path_to_option_file>`

Note: You can also perform a silent installation of Fortify Static Code Analyzer for AIX, HP-UX, and Solaris. On these operating systems, replace the installer file in the previous table with the appropriate one for your operating system.

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 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, run the text-based install command for your operating system:

Unix or Linux	`./HPE_Security_Fortify_SCA_and_Apps_<version>_linux_x64.run --mode text`

	where <*version*> is the software release version.
Mac OS	You must uncompress the provided zip file before running the command. `HPE_Security_Fortify_SCA_and_Apps_<version>_osx_x64.app/Contents/MacOS/installbuilder.sh --mode text` where <*version*> is the software release version.

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 **HPE Security 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 Mac OS, 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_HPESecurityFortifySCAandApps_<version>.exe`
Mac OS	`Uninstall_HPESecurityFortifySCAandApps_<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_HPESecurityFortifySCAandApps_<version>.exe --mode unattended`
Unix or Linux	`./Uninstall_HPESecurityFortifySCAandApps_<version>.run --mode unattended`
Mac OS	`Uninstall_HPESecurityFortifySCAandApps_ <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_HPESecurityFortifySCAandApps_<version>.run --mode text`
Mac OS	`Uninstall_HPESecurityFortifySCAandApps_ <version>.app/Contents/MacOS/installbuilder.sh --mode text`

Chapter 3: Post-Installation Tasks

Post-installation tasks prepare you to start using the Fortify Static Code Analyzer analyzers and applications.

This section contains the following topics:

Running the Post-Install Tool

To run the 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. To select `Migration`, type `1`.
4. To select `SCA Migration`, type `1`.
5. To select `Migrate from an existing Fortify installation`, type `1`.
6. To select `Set previous Fortify installation directory`, type `1`.
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. To select `Settings`, type `2`.
4. To select `General`, type `1`.
5. To select `Locale`, type `1`.
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`

Specifying a Proxy Server for Security Content Updates

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

To specify a proxy for security content updates:

1. Navigate to the `bin` directory from the command line.
2. At the command prompt, type `scapostinstall`.
3. To select `Settings`, type `2`.
4. To select `Fortify Update`, type `2`.
5. To select `Proxy Server Host`, type `2`, and then type the name of the proxy server.
6. To select `Proxy Server Port`, type `3`, and then type the proxy server port number.
7. (Optional) You can also specify the proxy server user name (option `4`) and password (option `5`).

Removing Proxy Server Settings for Security Content Updates

If you previously specified proxy server settings for the Fortify update server and it is no longer required, you can remove these settings.

To remove the proxy settings for 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. Type `2` to select `Proxy Server Host`, and then type `-` (hyphen) to remove the proxy server setting.
6. Type `3` to select `Proxy Server Port`, and then type `-` (hyphen) to remove the proxy server port number.
7. To remove the proxy server username (option `4`) and password (option `5`), type `-` (hyphen) for each setting.

Specifying a Proxy Server for Fortify Software Security Center

If your network uses a proxy server to reach the Fortify Software Security Center server, you must specify the proxy server with the post-install tool.

To specify proxy 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. To select `Settings`, type `2`.
4. To select `Software Security Center Settings`, type `3`.
5. To select `Server URL`, type `1`, and then type the Fortify Software Security Center server URL.
6. To select `Proxy Server`, type `2`, and then type the proxy server path.
7. To select `Proxy Server Port`, type `3`, and then type the proxy server port number.
8. (Optional) You can also specify the following:
   - The proxy server username (option `4`) and password (option `5`)
   - 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 for Fortify Software Security Center

If you previously specified proxy server settings to reach the Fortify Software Security Center and it is no longer required, you can remove these settings.

To remove the proxy 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 `2` to select `Proxy Server`, and then type `-` (hyphen) to remove the proxy server path.
6. Type `3` to select `Proxy Server Port`, and then type `-` (hyphen) to remove the proxy server port number.
7. To remove the proxy server username (option `4`) and password (option `5`), type `-` (hyphen) for each setting.

Updating Security Content

Security content (Secure Coding Rulepacks and metadata) is updated automatically during the Windows installation procedure. However, you can also download security content from the Fortify Customer Portal, 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 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 security content from the Fortify Customer Portal, run `fortifyupdate` with the `-import` option and the path to the directory where you downloaded the security content zip file.

For more detailed instructions about the fortifyupdate utility, see the *HPE Security Static Code Analyzer User Guide*.

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 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\Framework\v2.0.50727
```

or

```
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 (HPE Security Fortify Static Code Analyzer 17.10)

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 HPFortifyTechPubs@hpe.com.

We appreciate your feedback!