Fortify Software

What's New in Micro Focus Fortify Software 19.2.0

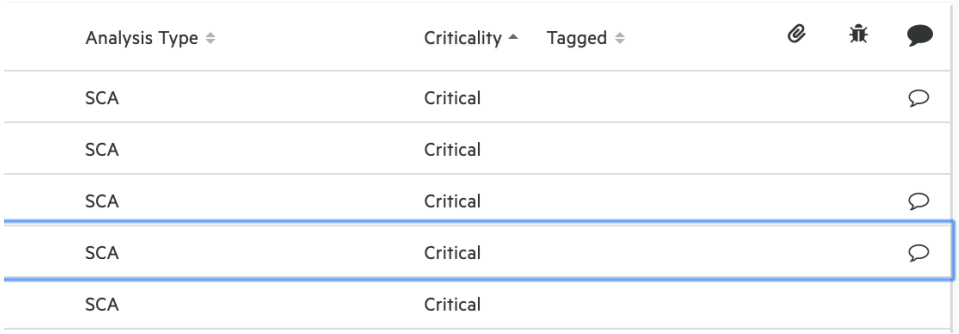
November 2019

This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

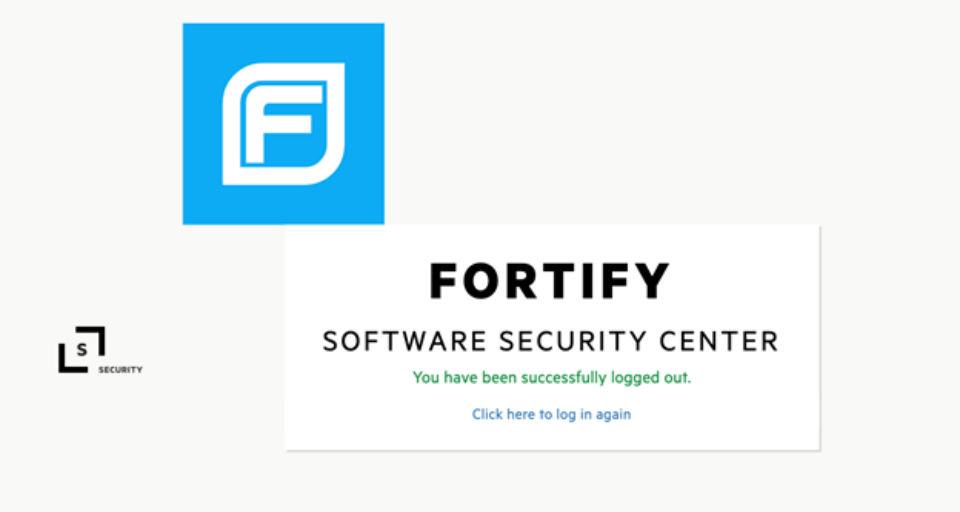
The following features have been added to Fortify Software Security Center.

Scan Issue View Now Includes a Comment Column



Session Logout Screens

A newly-integrated logout screen appears when users log out of Fortify Software Security Center. This also includes support for use with Fortify Software Security Center's SSO support.



- In this release there are new session logout screens. If you logged in as a local user, and you log out (or you are logged out because your session timed out), the session logout screen displays a link that you can use to return to the login screen.
- If you logged in using a SAML-based single sign-on account, which supports single sign-off, and you log off, the session logoff page gives you the option of logging out as a local user, or logging out from your SSO SAML account. For more detail, see "About Session Logout" in the user guide.
- If you logged in using a SAML-based single sign-on account and your session times out due to inactivity, a session logout dialog box gives you the options of signing out locally, signing out of your SAML account, or staying logged in.

Removal of Runtime Calls, Methods, and Parameters

Runtime calls, methods, and parameters were removed from Web Service endpoints, APIs, and command-line tools.

New Requirement for Audit Assistant Custom Tag Mapping

When you map Audit Assistant analysis tag values to custom tag values, you must make sure that you assign at least one tag value to both the Non-Issue and True Issue categories. For details, see "Mapping Audit Assistant Analysis Tag Values to Software Security Center Custom Tag Values" in the user guide.

Exporting Data for All Application Versions

- You can now export data for all application versions to a CSV file. For details, see "Exporting Data to Comma-Separated Values Files" in the user guide.

Additional File Formats Supported for Attachment to Issues

- Now, in addition to files in JPG, JPEG, BMP, PNG, and GIF formats, you can attach files in DOC, DOCX, PPT,and PPTX formats.

PCI SSF Report & Issue Template

The PCI SSF compliance mappings supersede the old PCI DSS requirements. Fortify makes both types of reports and Issue Templates available for customers still leveraging DSS requirements.

New PCI Basic Seed Bundle

A new seed bundle is available for seeding the Fortify Software Security Center database. The optional PCI Basic seed bundle (`Fortify_PCI_SSF_Basic_Seed_Bundle-2019_Q3.zip`) adds a Payment Card Industry (PCI) Data Security Standard (DSS) process template and its associated report to the default set of issue templates and reports. PCI DSS will remain open for assessment of previously-started, and newly-started assessments initiated before June 2021, until October 2022. After October 2022, the new PCI Software Security Framework (SSF) will be the set of standards for evaluation.

This is in addition to the `Fortify_PCI_Basic_Seed_Bundle-2019_Q3.zip` file, which is still available. For more information about seed bundles, see "Unpacking and Deploying Fortify Software Security Center Software" in the user guide.

Micro Focus Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

Modular Analysis

Modular analysis allows you to pre-scan libraries and sub-libraries separately from your core project. You can then include these pre-scanned libraries when you scan the core project. Fortify Static Code Analyzer can follow dataflow through the libraries without including the source code of the libraries in the core application scan or requiring rules for these libraries. This results in a high quality scan without having to scan the dependencies each time you scan the core application.

Go Language

Added support for translating Go language version 1.12 source code on Windows and Linux platforms.

React

Added support for React 16.5 JavaScript library.

Java

Added support for Java 12.

Performance improvements

Fortify Static Code Analyzer now uses available cores in a more scalable fashion. Increasing the number of available cores may improve scan speeds. Similarly, increasing available memory may also improve scan speeds.

Micro Focus Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer Tools.

Fortify CloudScan .NET packaging support

Fortify CloudScan now supports packaging and scanning .NET solutions remotely (translation and analysis phases). The Fortify CloudScan client intelligently packages .NET solutions for remote translation and scanning outside of the build environment.

Other directly-parsed languages have been added to CloudScan.

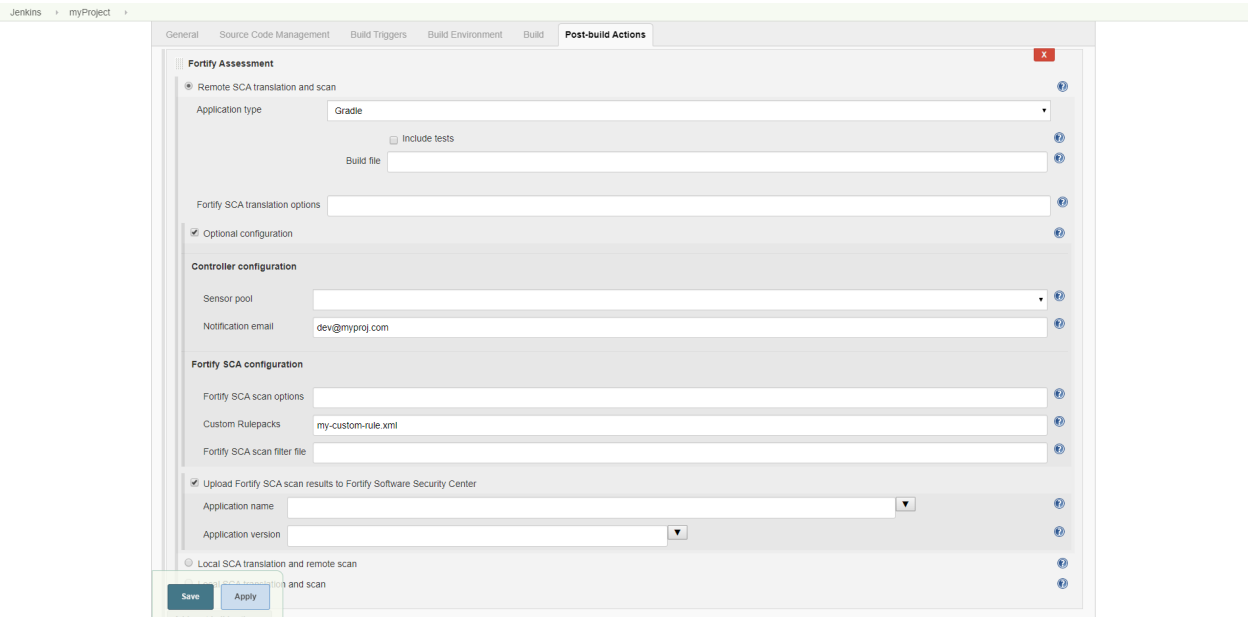
The following languages are supported in Fortify Static Code Analyzer, but are not available for remote translation: the C family of languages (C/C++/Objective-C/Swift), COBOL, and ActionScript.

Fortify SCA Visual Studio 2019 Extension w/ built-in CloudScan support

- Added Fortify extenstion for Visual Studio 2019
- Includes Fortify CloudScan support

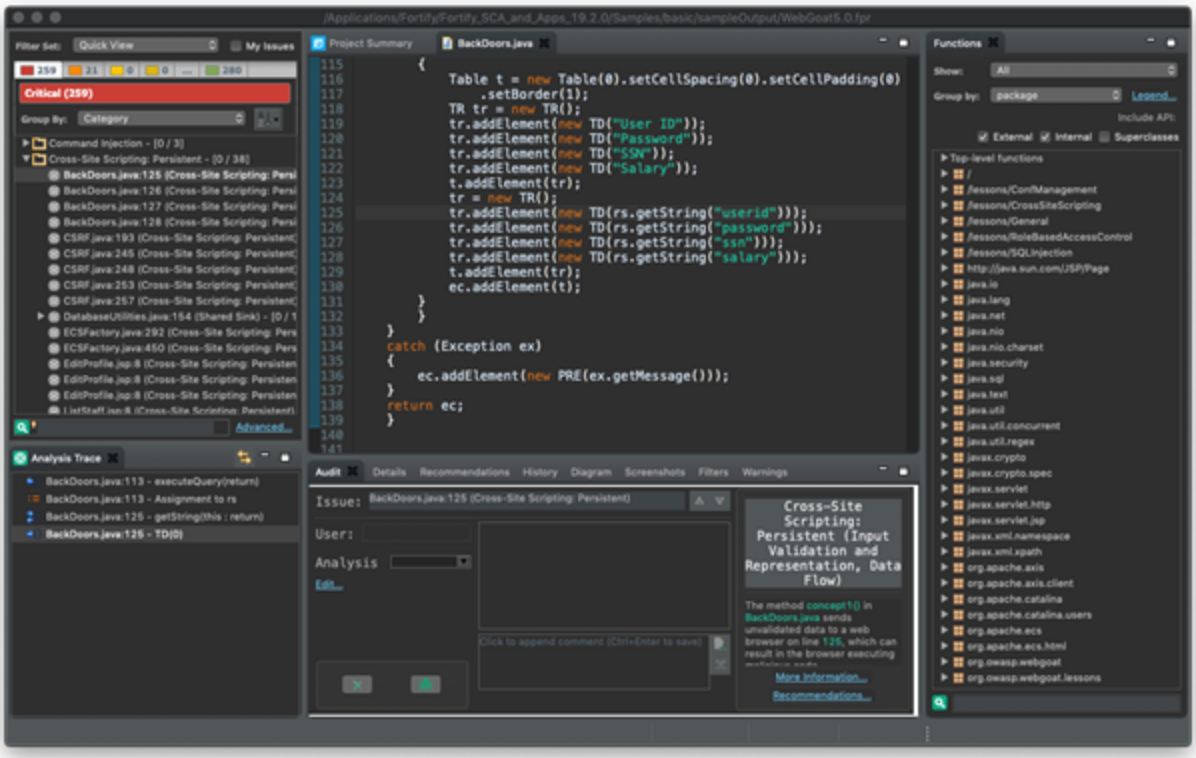
Fortify Jenkins plugin with w/ built-in CloudScan and 19.2.0 Fortify Static Code Analyzer support

This new plugin includes native Fortify CloudScan support and new scan options that support Fortify Static Code Analyzer 19.2.0. Available for download: https://plugins.jenkins.io/fortify.



Audit Workbench

- Dark Theme
  To enable the dark theme, navigate to: *Options -> Appearance -> Dark Theme* in Fortify Audit Workbench.



- Syntax highlighting support for TypeScript, YAML, Less and JSON.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Simplified API Scanning

Scanning APIs, which are documented via the OpenAPI (Swagger) API description format, have been simplified. You can leverage this feature from the API Scan option of the Basic Scan Wizard or from the WebInspect API or CLI.

Advanced API Scanning – Postman

Run functioning Postman collections for advanced API scanning scenarios where unique workflows, complicated authentication, or specific parameter values are required.

Response State Patterns

Handles complex scenarios where an application requires passing data from a response into a subsequent request. You can build response state rules from the *Scan Settings > HTTP Parsing* option.

Macro Auto-gen Improvements

The underlying macro auto-gen engine has been upgraded and signatures have been improved, resulting in improved accuracy and performance of our macro auto generation technology.

Macro Validation Improvements

The underlying macro validation engine has been improved, resulting in greater accuracy in validating macros.

Usability Improvements

- Improved support for high resolution monitors.
- Some scan settings have been simplified to reduce confusion.

Common Access Card (CAC) Improvements

Many highly restricted applications leverage common access cards as a part of their two-factor authentication protocol. CAC coverage provides better support when scanning applications in these sensitive environments.

Selenium Webdriver - Tech Preview

A selenium WebDriver enables tighter integration of Fortify WebInspect into your pipeline in this Technical Preview. This integration allows Fortify WebInspect to automatically run selenium binaries, detect the tested surface area of the application, and then test for vulnerabilities.

Updated Vuln Retest - Tech Preview

Improvements to the accuracy of our vulnerability retest engines have been made. The Technical Preview of these updated capabilities are available via the API and CLI. Updated endpoints allow for testing all detected vulnerabilities, vulnerabilities by severity, or even individual vulnerabilities by unique identifier.

Micro Focus Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Silverlight Dependency Removal

To provide more flexibility, WebInspect Enterprise no longer requires Internet Explorer with Silverlight for proper operation. Customers using modern browsers like Chrome and Firefox will be prompted to install the WIE Desktop Client which will allow them configure and visualize scans.

Free-Standing Macro Recorder with Macro Engine 5.0

While we work to complete integration of the updated Web Macro Recorder with Macro Engine 5.0 throughout the product, we want to provide you with a free-standing version of the new tool. You can download the free-standing Web Macro Recorder tool from the Software Support Online portal. The tool provides both WebInspect Enterprise and WebInspect customers with an easy way to record macros without changing default settings.

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

What's New in Micro Focus Fortify Software 19.1.0

May - June 2019

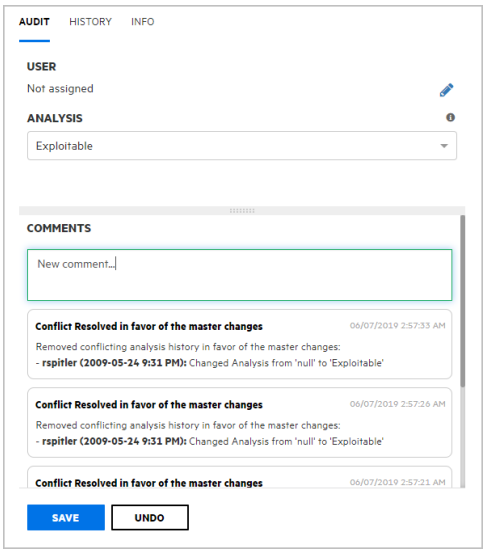
This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

UI / Usability Updates

- The COMMENTS section has been moved. Previously, you posted and viewed comments from the COMMENTS & HISTORY tab. Now you can post and view comments on the AUDIT tab in the right panel of the issue details section.



- Audit Page: Rulepack content is now divided into separate sections. Details / Recommendations / Metadata / References / etc are now found in the Info tab.
- The new version selector has a three-column layout for selecting application versions. It was designed to accommodate thousands of application versions.

Micro Focus Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

TypeScript

TypeScript language support now includes:

- Higher Order Analysis (HOA) performance improvements
- Support for TypeScript 3.0, 3.1 and 3.2

Python

Python language support now includes:

- Support for Python 3.7
- Support for Django 2.x
- Performance improvements

Gradle

Gradle support now includes Gradle 4.x.

Angular

Angular support now includes Angular 7.

Java

Java support now includes Java 10 and Java 11.

ECMAScript

Fortify Static Code Analyzer now supports ECMAScript 2018.

Higher Order Analyzer

Higher Order Analyzer is on by default for JavaScript and TypeScript applications. When Higher Order Analyzer is enabled, Fortify Static Code Analyzer is able to better track dataflow issues and uncover more vulnerabilities.

Micro Focus Fortify CloudScan

Fortify CloudScan now ships with a utility to package source code, dependencies, and Fortify Static Code Analyzer translation instructions. You no longer have to install Fortify Static Code Analyzer locally or on the build server. The packaging utility allows you to centralize your Fortify infrastructure and create a consistent approach across languages.

- You no longer have to install and run Fortify Static Code Analyzer on the build server for the following languages: Java, JavaScript, Ruby, Python, and PHP.
- The packaging utility packages everything necessary, including dependencies, and sends the package directly to the CloudScan CLI. The CloudScan CLI then sends it on to the sensors, which perform both translation and scanning phases of the analysis.
- The packaging utility intelligently sets what were previously manual translation options. Simply provide the location of the build file (build.gradle / pom.xml). No other configuration options are required for build integration.
- This new Fortify CloudScan utility supports auto packaging using the Gradle or Maven build tools.

Micro Focus Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer Tools.

Fortify Jenkins Plugin

- Post-build action analyzes the source with Fortify Static Code Analyzer, updates security content, uploads analysis results to Fortify Software Security Center, and fails the build based on uploaded results processed by Fortify Software Security Center.
- Provides native pipeline support for source code analysis with Fortify Static Code Analyzer, security content update, and uploads to Fortify Software Security Center.
- Snippet generator makes it easy to generate the pipeline code necessary to add a Fortify task to a pipeline script.
- Displays Fortify security analysis results for each job that includes a history trend and the latest issues from Fortify Software Security Center. Navigates to individual issues on Fortify Software Security Center for detailed analysis.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Simplified API Scanning

We have dramatically simplified scanning APIs that are documented using the OpenAPI (Swagger) API description format. You can use the API Scan option in the Basic Scan Wizard or leverage this feature from the WebInspect API or CLI.

Advanced API Scanning – Postman

Fortify WebInspect can now directly run your functioning Postman collections for more advanced API scanning scenarios where unique workflows, complicated authentication, or specific parameter values are required.

Response State Patterns

Fortify WebInspect can now handle complex scenarios where an application requires passing data from a response into a subsequent request. To build response state rules, go to **Scan Settings > HTTP Parsing**.

Macro Auto-gen Improvements

We've upgraded the underlying macro auto-gen engine and we've improved our signatures. You should see improved accuracy and performance of our macro auto generation technology.

Macro Validation Improvements

The underlying engine for our macro validation feature has been improved. You should note improved accuracy in validating macros.

Usability Improvements

We've addressed some usability concerns on two fronts. First, we've improved WebInspect's support for high resolution monitors. Second, we've begun simplifying some of our scan settings to avoid customer confusion.

Common Access Card (CAC) Improvements

Many highly-restricted applications leverage common access cards as a part of their two-factor authentication protocol. We've broadened our CAC coverage to better support our customers who are scanning applications in these sensitive environments.

Verify Site Improvements

We've improved the Verify Site API endpoint to support more advanced detection of application complexity, and to provide a measurement of application response time that can be used to predict potential for long running scans.

Free-Standing Macro Recorder with Macro Engine 5.0

While we work to complete integration of the updated Web Macro Recorder with Macro Engine 5.0 throughout the product, we want to provide you with a free-standing version of the new tool. You can download the free-standing Web Macro Recorder tool from the Software Support Online portal. The tool provides both WebInspect Enterprise and WebInspect customers with an easy way to record macros without changing default settings.

Selenium Webdriver - Tech Preview

To allow customers to more tightly integrate WebInspect into their pipelines, we've built a Selenium WebDriver integration. This integration allows WebInspect to automatically run Selenium binaries, detect the tested surface area of the application, and then test for vulnerabilities.

Updated Vuln Retest - Tech Preview

We're improving the accuracy of our vulnerability retest engines. In 19.2.0 we're releasing a technical preview of these updated capabilities which are available via the API and CLI. The updated endpoints allow for testing all detected vulnerabilities, vulnerabilities by severity, or even individual vulnerabilities by unique identifier.

Micro Focus Fortify WebInspect Enterprise

The following feature has been added to Fortify WebInspect Enterprise.

New API Endpoints

New SmartUpdate endpoints provide a way of:

- Getting a list of all SmartUpdate occurrences
- Getting details or status of a specific SmartUpdate
- Starting the SmartUpdate process to download the latest SecureBase changes and sensor versions

What's New in Micro Focus Fortify Software 18.20

November 2018

This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

SSC Scalability

- The persistence layer has been optimized to accommodate additional SCA scans
- The format of the issue fields has been made more efficient when storing and retrieving
- Total issue size has been reduced
- Adding new scans is typically 10-30% faster

Audit Page Redesign (Phase 1)

- Fortify Priority Order (Critical / High / Medium / Low) appears on the Audit and Overview screens. Clicking these folders allows you to view the associated issues.
- Issue Details and Recommendations are now accessed from the tabs on the Audit page
- Adding comments to individual issues no longer requires going to the Assign screen; comments can be submitted directly in the Audit page

Audit Assistant Auto-Predict

- You can now set automatic predictions for application versions. You can enable this feature on the **ADMINISTRATION -> Configuration -> Audit Assistant** page by checking the **Enable auto predict** check box in the application version Profile window
- New predictions are automatically requested when new issues are uploaded to an application version

Note: Audit Assistant does not re-predict on issues in application versions when a previous prediction was made. Create a new application version to reset this functionality.

Application Security Training

When viewing security issues, a "Get Training" link will take you to contextual application security training provided by Secure Code Warrior.

- Contextually correct application security training has been designed to integrate with any application security training provider. The current iteration includes integration to Secure Code Warrior.
- A current list of the full mapping between Secure Code Warrior and Fortify Software Security Center is available from customer support

Request Dynamic Scans (Fortify WebInspect Enterprise) Migrated to the Current User Interface

The dynamic scan request feature in the legacy user interface has been migrated to the current user interface

Micro Focus Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

Apple Update

Support for the latest releases of the following components:

- Swift 4.2
- Xcode 10
- Objective-C/C++

TypeScript

Added the ability to scan TypeScript applications. TypeScript is a superset of JavaScript that adds optional static typing to the language.

.NET Update

- MSBuild support has been changed to reflect the direction Microsoft has set for .NET
- MSBuild integration is now the only build integration used to translate .NET applications

- When translation is invoked from the Visual Studio extension or devenv on the command line, MSBuild integration is used
- In addition to translating Visual Studio Solutions, you can now translate individual Visual Studio Projects
- Added support for delegate and function modeling
- Improved support for rules surfaces more vulnerabilities in .NET applications

Python

The new Python translator supports both Python 2 and Python 3 applications. The new Python translator is used by default, but the legacy Python 2.x translator is still available with a command line option.

The new Python translator provides:

- Improved support for Python 3
- Support for Python 2.x applications
- Improved support for Django 1.8

The legacy Python 2 Translator:

Fortify Static Code Analyzer uses the new Python translator by default. To use the legacy translator, specify it on the command line.

Scanning Python 3 Applications:

By default, Fortify Static Code Analyzer assumes you are scanning Python 2.x applications. To scan Python 3 applications, specify the Python version on the command line:

```
-python-version 3
```

Node.js

We added support for scanning Node.js 10.x applications.

Angular

This initial release of Angular support enables scanning Angular 2, 4, 5 and 6 applications.

Java 9

Major defects were fixed in our Java 9 support, resulting in the discovery of more complex vulnerabilities in Java 9 applications.

Logging

With this release, we provide a major update to the logging infrastructure. There are now two different log files:

- Standard log file (sca.log): provides information you can use when troubleshooting
- Fortify Support log (sca_FortifySupport.log): provides information that may be helpful to the customer support or development team

Micro Focus Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer Tools.

Fortify Jenkins Plugin

An improved version of the Fortify Jenkins Plugin. It includes the following features and capabilities:

- Full translation and analysis capabilities
- Ability to upload your results to Fortify Software Security Center
- Supported application types include:
  - Java
  - Maven
  - Gradle
  - .NET (msbuild / devenv)
  - Other (directly input any Fortify Static Code Analyzer command)
  - Ability to fail or mark builds as unstable using the Fortify Software Security Center search criteria

MSBuild Integration Enhancements

With this new, enhanced version, you can continue to use devenv or msbuild as you always have. The devenv invocations are now converted to msbuild options automatically. In addition, this new version:

- Provides increased consistency in the Fortify Static Code Analyzer translation / analysis phases
- No longer requires the Fortify Extension for Visual Studio or Visual Studio in order to scan .NET solutions (.NET framework is required to be installed). To scan from the Visual Studio IDE, the Fortify Extension for Visual Studio is still required
- No longer requires admin privilege to install Fortify Extension for Visual Studio forVisual Studio 2013

For example, the following command:

```
sourceanalyzer –b test devenv Sample.sln /REBUILD
```

will be converted to:

```
sourceanalyzer –b test msbuild Sample.sln /t:rebuild
```

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Checks over WebSockets

The Fortify WebInspect engines can now examine the data traversing WebSockets. This allows us to detect vulnerabilities in modern applications leveraging WebSockets for advanced communication.

Pause-resume Scan Capability on the Command Line

The command line has been updated to support pause/resume of running scans. When you use the Fortify WebInspect command line interface for automation, you will gain greater flexibility, control, and improved parity withexisting API functionality.

Micro Focus Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Improved Sensor Stability

Improvements to thread management in the Fortify WebInspect Enterprise sensors result in significant improvements to sensor stability, reliability, and greater up time.

API Improvements

The following enhancements have been made to the API:

- Existing scan templates may be overridden with workflow and login macros.
- SSC Project Versions can be assigned to any security group.
- When using the temporary file upload endpoint, Fortify WebInspect Enterprise automatically

creates a file identifier rather than requiring your input.

- Endpoints now list which parameters are required or optional.

SmartUpdate

SmartUpdate just got smarter. Now, instead of downloading the entire package, you select the language and version number you require, reducing the amount of content you need to download.