Fortify Software

What's New in Micro Focus Fortify Software 22.1.0

June 2022

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.

Issue Correlation Details

If you have correlated issues in an application version, you can use the heading for the correlated issues icon (⇄) to sort listed issues based on whether or not they are correlated with other issues (see "Viewing Correlated Issues on the AUDIT Page" in the *Fortify Software Security Center User Guide*). You can also selectively list the issues with which a given issue is correlated (see "Auditing Correlated Issues" in the *Fortify Software Security Center User Guide*).

Targeted Rulepack Downloads

Previously, Fortify Software Security Center ignored the clientType parameter in Rulepack update requests. As a result, Rulepack clients received all Rulepacks available (both Fortify Static Code Analyzer and Fortify Security Assistant Rulepacks). Now, Fortify Software Security Center takes the clientType parameter into account for Rulepack update requests. For details, see "Updating Rulepacks from the Micro Focus Fortify Update Server" in the *Fortify Software Security Center User Guide*.

Updated Processing Rule: Ignore SCA Scans Performed in Quick Scan Mode

The processing rule for ignoring Fortify Static Code Analyzer scans performed in quick scan mode now also prevents the upload of Fortify Static Code Analyzer speed dial results performed with a setting of less than four. For details, see "Setting Analysis Results Processing Rules for Application Versions" in the *Fortify Software Security Center User Guide*.

Report Maintenance: New "Days to Preserve" Option

On the Scheduler page, the **Days to preserve** option was added in a new **Reports maintenance** section. This option enables you to specify the number of days Fortify Software Security Center retains generated reports. For more information, see "Configuring Job Scheduler Settings in the *Fortify Software Security Center User Guide*.

Pausing Job Execution

You can now control job execution by pausing (and then resuming) it using the **Pause job execution** option located on the Maintenance page (**ADMINISTRATION > Maintenance**). After you pause job execution, jobs (artifact processing, report generation, data export requests, and so on) that are currently running continue to completion. Any new jobs submitted are queued for processing once the **Pause job execution** check box is cleared and normal processing resumes. For more detail, see "Pausing and Resuming Job Execution" in the *Fortify Software Security Center User Guide*.

Requiring Comments for Specific Custom Tag Values

Administrators can now require comments for custom tags. When the "Require Comments" setting is checked, any changes to the custom tag will cause an additional comment box to appear for the custom tag and the Save button will be disabled until a comment is entered. For details, see "Adding Custom Tags to the System" in the *Fortify Software Security Center User Guide*.

Expanded Issue Counts

Previously, you could display 20, 50, or 100 issues at a time on the AUDIT page. Now, you can display up to 150 or 200 issues per page.

Kubernetes Updates

- Added support for Kubernetes 1.22
- Added support for Helm 3.8

Micro Focus Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

Kotlin for Android Support

You can now use the ScanCentral Client to package Kotlin for Android projects for remote translation using Gradle integration (`-bt gradle`).

New Command to Update ScanCentral Client

Using the new `update` command, you can update ScanCentral Client to the latest version on the ScanCentral Controller.

Get SSC Artifact Processing State Using Job Token

Using the `status` command, ScanCentral Client can retrieve the processing state of a job that uploaded the FPR to SSC.

Build Tool Updates

• Gradle 7.3

• MSBuild 14.0, 17.0, 17.1, and 17.2

Support for Multiple Client Versions on the Controller for Auto-Update

The Auto-Update feature now supports multiple versions of clients. Sensors and embedded clients will be updated by the versions available in the Controller, rather than the version of the Controller.

Micro Focus Fortify Static Code Analyzer

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

Operating System Updates

Fortify added support for the following operating systems and versions:

- macOS 12
- Windows 11

Compiler Updates

Fortify added support for the following compiler versions:

- Clang 13.1.6
- OpenJDK javac 17
- Swiftc 5.6
- cl (MSVC) 2015 and 2022

Build Tool Updates

Fortify added support for the following build tool versions:

- Gradle 7.4.x
- MSBuild 14.0, 17.0, 17.1 and 17.2
- Xcodebuild 13.3 and 13.3.1

Language and Framework Updates

- C# 10
- .NET 6.0
- C/C++ 20
- HCL 2.0
- Java 17
- TypeScript 4.4 and 4.5

Note: Rules for Terraform and Google Cloud Platform will be part of the Fortify Software Security Content 2022 R2 release.

Micro Focus Fortify Static Code Analyzer Tools

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

Visual Studio 2022 Support

The Fortify Extension for Visual Studio now supports Visual Studio 2022.

IntelliJ 2021.x Support

The Fortify Analysis Plugin for IntelliJ now supports IntelliJ 2021.x to 2021.3.

Import Standard Fortify Rulepacks from Filesystem

Use the **Options** menu in Fortify Audit Workbench, Fortify Eclipse Complete Plugin, and Fortify Extension for Visual Studio to import Fortify Rulepacks downloaded from the Customer Portal.

Compare LOC of Scanned Files Between Two FPRs

View LOC counts of analyzed files in an FPR (`-loc`) or compare LOC counts between two FPRs using FPRUtility (`-loc, -compareTo`).

Configurable Timeout for fortifyupdate

Configure the socket timeout for fortifyupdate using the `rulepackupdate.SocketReadTimeoutSeconds` property in the `server.properties` file. The default value is `180`.

New Search Modifier: shortfilename

In Fortify Audit Workbench and the Fortify Plugins for Eclipse, you can use `shortfilename` as a search modifier in Issue Templates to filter or hide issues that match the file name. For full path matches, continue to use the `file` search modifier.

New OWASP Top 10 2021 Report

Generate new OWASP Top 10 Report (2021) from the following tools:

- Fortify Audit Workbench
- Fortify Extension for Visual Studio
- Fortify Remediation Plugin for Eclipse
- BIRTReportGenerator

Micro Focus Fortify ScanCentral DAST

The following features have been added to Fortify ScanCentral DAST

User Configuration Restrictions

- New permissions allow you to bar scanning of specific domains or IP addresses.
- New Modify User permission required to allow user to modify a scan. A user who does not have this permission can only configure a scan URL, login macro, workflow macros, and network credentials. With this limited role, users can start scans, create scans from base settings, and view settings but not change them.

PostgresSQL Support

- Support for use of a PostgresSQL database.

Scan Import

- Import Scans into ScanCentral PostgresSQL database from Fortify WebInspect or Fortify WebInspect Enterprise.

Automated Deployment (Infrastructure as Code)

- Support for the fully automated deployment of ScanCentral DAST.

Rescan Button

- The Rescan button allows you to rescan and existing scan.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Support for HAR Files

Scanning with workflow macros ensures that important content is covered in a scan. WebInspect can now use HAR files for workflow scanning.

Out-of-Band Testing

WebInspect can now test for a new class of vulnerabilities called Out-of-Band or OAST vulnerabilities. Using the public Fortify OAST server, WebInspect can detect OAST vulnerabilities such as Log4Shell.

Engine 7.0 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 22.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 7.0.

MS SQL AD Authentication Support

WebInspect 22.1.0 can now use a MS SQL Database using AD Authentication.

Windows 11 Support

WebInspect 22.1.0 is now supported on the Windows 11 operating system.

Azure SQL Database Support

WebInspect 22.1.0 can now use an Azure SQL Database for storing scan data.

Sensor Support for Fortify WebInspect Enterprise 21.2.0

WebInspect 22.1.0 can be configured as a sensor for Fortify WebInspect 21.2.0.

Contact 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://www.microfocus.com/support

For More Information

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

What's New in Micro Focus Fortify Software 21.2.0

November 2021

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.

Static/Dynamic Issue Correlation Indicator

- In this release we introduce the static/dynamic issue correlation indicator. After static and dynamic scans are run on an application version and the results have been uploaded to Fortify Software Security Center, issues that were uncovered by both static and dynamic scans are tagged with the correlation (⇄) indicator on the AUDIT page.

ScanCentral SAST Controller Updates

- You can now place the ScanCentral SAST Controller into maintenance mode which prevents scans that are running on the sensor from losing data.
- You can shut down ScanCentral SAST Controller sensors individually or in a batch.

ScanCentral DAST Scans Support

- The Scans feature now includes both static and dynamic scan results

New Premium Quarterly Reports

- PCI SSF (Software Security Framework) 1.2 report
- CWE Top 25 report

LDAP Update

- You can now configure Fortify Software Security Center to invalidate tokens created by users who have been disabled in LDAP

Java 11 Deployment

- Software Security Center can be deployed in a Java 11 (or higher) environment

Kubernetes Updates

- Added support for Kubernetes 1.21
- Added support for Helm 3.6 and 3.7

Micro Focus Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

Support for the Fortify License and Infrastructure Manager

- You can now centrally manage your Fortify ScanCentral SAST licenses through the Fortify License and Infrastructure Manager.

MSBuild Integration Update

- With the 21.1.0 release of Fortify Static Code Analyzer, MSBuild integration was updated with support for .NET 5 and other new features. Fortify ScanCentral SAST now supports this new MSBuild integration functionality.

Go Language Support

- Added support for Go version 1.17.

Graceful Shutdown and Timer Support

- When shutting down Fortify ScanCentral SAST, the controller allows currently running scans to complete while keeping other scans from starting. Once the controller is running again, it will run the scans in the queue. In addition, a timeout can be set for long running scans that will cancel the scan if breached and free the sensor to pick up a new scan request.

Sensor Pool Assignment Improvement

- When starting up a sensor, you can assign it to a specific sensor pool without having to use the Fortify Software Security Center UI.

Micro Focus Fortify Static Code Analyzer

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

Fortify License and Infrastructure Manager

- For customers that use Fortify under the Concurrent Scanning license model, Fortify Static Code Analyzer can now use the Fortify License and Infrastructure Manager to obtain a license key rather than the traditional `fortify.license` file. This enables the correct sharing of the Fortify Scan Machine license metric between Fortify Static Code Analyzer and WebInspect instances. The option to use the traditional `fortify.license` file is still available.

Regular Expression (regex) Analysis

- The Fortify Static Code Analyzer Configuration analyzer can now detect vulnerabilities in file names and content using RegEx-based rules.

Operating System Updates

Fortify added support for the following operating systems and versions:

- IBM AIX 7.1
- Oracle Solaris SPARC 11.3
- Oracle Solaris x64 11.4
- Windows Server 2022

Compiler Updates

Fortify added support for the following compiler versions:

- gcc 10.2.1
- g++ 10.2.1
- Swiftc 5.4.2

Build Tool Updates

Fortify added support for the following build tool versions:

- Gradle 7.2
- Maven 3.8.2
- MSBuild 16.11
- Xcodebuild 12.5.1

C++ Updates

- Added support for gcc on Macintosh
- Added support for gcc version 10.2.1
- Added support for C++ 14 and 17

JavaScript Improvements

- Added support for ECMAScript 2021
- Added support for TypeScript 4.2 - 4.3
- Made Type inference improvements
- Added support for SAPUI5/OpenUI5
- Minified JS excluded from scan by default

Go Language Update

- Added support for Go 1.17

YAML Support

- Added support for translating YAML code

Kotlin Update

- Added support for Kotlin 1.5

PHP

- Completed support for PHP 8

Scala

- Eliminated the need for a separate license from Lightbend for Scala translations. A license key is still required to run the plugin. The key is now included in the Fortify distribution.

Configuration Scanning

- JSON scanning enabled by default
- Added YAML scanning

Micro Focus Fortify Static Code Analyzer Tools

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

ScanCentral SAST Support

- Added Remote Translation capability to Fortify Scan Wizard, and the Fortify Eclipse Plugins
- Added ability to configure Fortify ScanCentral SAST and launch local and remote translations and scans from the Fortify Eclipse Complete Plugin running an advanced analysis.

New PCI SSF Report

Generate new PCI SSF Report (version 1.2) from the following tools:

- Fortify Audit Workbench
- Fortify Visual Studio Extension
- Fortify Eclipse Plugins (Complete and Remediation)
- BIRTReportGenerator

Micro Focus Fortify ScanCentral DAST

The following features have been added to Fortify ScanCentral DAST.

Correlated Issues

- ScanCentral DAST can now uncover correlations between DAST and SAST results and forward the information to Fortify Software Security Center. Correlated results are displayed in the Fortify Software Security Center AUDIT View.

Scan Visualization Update

- Selected scan visualizations can be opened in a new browser tab rather than using Site Explorer.

Client-Side Certificate Support

- Upload a certificate and password for use when running a scan. If a scan requires the certificate, ScanCentral DAST will download and install it.
- Enable Redundant Page Detection and use it when running a scan.

Scan Priority Level

- All scans can be assigned a priority level.
- When a scan is queued because there isn't a free sensor and a scan with a lower priority is running, the lower-priority scan will be shut down so the scan with the higher priority can run. The scan with the lower priority will restart when a sensor becomes available.

Azure SQL Support

- The ScanCentral DAST Configuration Tool now supports Azure SQL and Azure Managed SQL.
- The ScanCentral DAST container now supports Azure SQL and Azure Managed SQL.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

API Discovery

With the new API Discovery, any Swagger or OpenAPI schema detected during a scan will have its endpoints added to the existing scan and authentication will be applied to the endpoints with our automatic state detection. In addition, probes will be sent to default locations of popular API frameworks to discover schemas.

Two-factor Authentication

Two-factor Authentication is a common requirement in enterprises and can be a burden to the security tester to get a bypass or to manually scan. WebInspect now offers the ability to automate Two-factor Authentication scans. This is accomplished by installing a lightweight Android app onto a phone or emulator that can capture SMS and Email tokens and pass them back to the scanner for authentication. Once configured, there is no need for user interaction.

Automatic State Detection

WebInspect now automatically detects and configures state for Oauth, JWT, and Bearer Tokens during a scan.

Engine 6.1 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.2.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.1.

Improved DOM XSS Detection

WebInspect 21.2.0 has new DOM XSS detection capabilities for analyzing client-side code for XSS. This will allow for improved XSS attack performance and the ability to detect client-side only attacks, such as XSS in DOM fragments.

Web Fuzzer Tool

The Web Fuzzer Tool lets you run Fuzzing tests that submit random or sequential data to various areas of an application to uncover security vulnerabilities. For example, when searching for buffer

overflows, a tester can generate data of various sizes and send it to one of the application entry points to observe how the application handles it.

Micro Focus Fortify WebInspect Enterprise

The following features have been added to the Fortify WebInspect sensor used in WebInspect Enterprise.

Note: WebInspect Enterprise 21.2.0 is scheduled for release in the latter half of December 2021.

API Discovery

With the new API Discovery function in WebInspect, any Swagger or OpenAPI schema detected during a scan will have its endpoints added to the existing scan and authentication will be applied to the endpoints with our automatic state detection. In addition, probes will be sent to default locations of popular API frameworks to discover schemas.

Automatic State Detection

WebInspect now automatically detects and configures state for Oauth, JWT, and Bearer Tokens during a scan.

Engine 6.1 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.2.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.1.

Improved DOM XSS Detection

WebInspect 21.2.0 has new DOM XSS detection capabilities for analyzing client-side code for XSS. This will allow for improved XSS attack performance and the ability to detect client-side only attacks, such as XSS in DOM fragments.

What's New in Micro Focus Fortify Software 21.1.0

July 2021

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.

Oracle: JDBC Driver Requirement

If you use Oracle as your Fortify Software Security Center database, you no longer need to manually add the JDBC driver. The installer now includes the JDBC Thin Driver (ojdbc8.jar).

Autoconfigure Update

You no longer need to provide `db.driver.class`, `db.dialect`, or `db.like.specialCharacters` to deploy SSC using autoconfiguration (**<app_context>.autoconfig file**). Deployment works for all databases if you provide values for `db.username`, `db.password`, and `jdbc.url` only.

Required Attribute Alert

If an administrator creates a new required attribute, Fortify Software Security Center alerts you to the addition so that you can specify a value for it in an application version.

Export Open Source Results

You can now export your open source data to a comma-separated file.

DENY Button for Artifacts

There is now a DENY button for artifacts that require approval but were uploaded by mistake. The denied results will not be merged with the application version but can be retained as part of the record.

New Reports

The premium report bundle now includes three new issue reports:

- DISA STIG 5.1
- NIST 800-53 Revision 5 (Accessed through the FISMA Compliance: FIPS-200 report template)

- CWE Top 25 2020

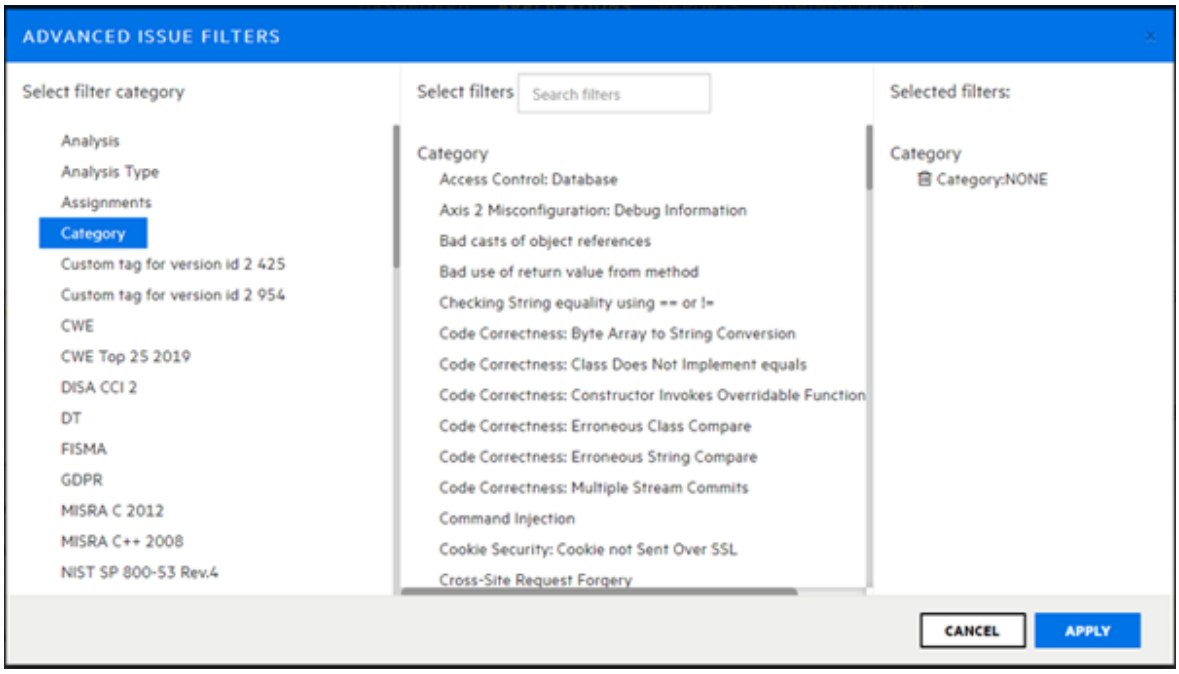
StartTLS Support for LDAP

StartTLS is now supported as a connection method to LDAP servers.

Enhanced Issue Filtering

Issue filtering from the OVERVIEW and AUDIT pages now includes enhancements.

You can now filter issues based on their category.



Kubernetes Support

- Added support for Kubernetes version 1.20.
- Added support for versions 3.4 and 3.5 of the Helm command-line tool.

Service Integrations Support

- Added support for Azure DevOps Server 2020

Micro Focus Fortify ScanCentral SAST

Improved Job Processing Messages

Previously, when a job was assigned to a sensor, the Controller sent the email message "ScanCentral job request accepted." After the job was completed, the Controller sent the email message "ScanCentral job completed."

Now, when the Controller accepts a job, it sends the email message "ScanCentral job request accepted." After the job is assigned to a sensor, the Controller sends the email message

"ScanCentral job request assigned." Finally, after the job is completed, the Controller sends the email message "ScanCentral job completed."

New -debug Option

The `-debug` option, which enables debug logging on clients and sensors, was added in this release.

-upload Option Required for Scans When Fortify Software Security Center is in Lockdown Mode

Previously, if Fortify Software Security Center was in lockdown mode, you could run a scan even if you failed to specify the `-upload` option in the ScanCentral command. The results shown for the scan on the **SCANCENTRAL > SAST** tab in Fortify Software Security Center left out the application version and the scan was not uploaded. Now, if Fortify Software Security Center is in lockdown mode, and you try to start a scan without using the `-upload` option, client execution fails with an error.

Improved Sensor Cleanup

Now, the clean-up process on a sensor machine invokes the `sourceanalyzer -clean` command to remove Fortify Static Code Analyzer internal files related to the job.

Maven Remote Translation

You can now specify custom settings files for Maven remote translation.

New Email Properties

Two new properties in the `config.properties` file allow you to specify which outgoing email domains to use for outgoing emails and which domains are disallowed.

Micro Focus Fortify Static Code Analyzer

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

.NET

Added support for the following languages and frameworks:

- .NET 5.0
- C# 9
- ASP.NET Blazor

To improve MSBuild integration, the custom msbuild executable and its assemblies were replaced by a Fortify-specific .targets file and task assemblies. These changes favorably impact translations under MSBuild Integration performed by the system's MSBuild tool.

MSBuild Support Update

Added support for version 16.8 and 16.9.

Go

- Added support for Go versions 1.15 and 1.16.
- Added support for the GOPROXY environment variable.

Java

- Updated JSP translation produces fewer false positives
- Improved bytecode analysis

JavaScript

Added support for the following languages and frameworks:

- TypeScript 4.1
- Angular 10 and 11

Kotlin

Added support for Kotlin 1.4.20.

PHP

Added support for PHP 7.2, 7.3, 7.4, and 8.0.

Python

Added support for the following languages and frameworks:

- Python 3.9
- Django 3.1

Swift/Obj-C

Added support for Xcode 12.4.

Operating Systems (Linux)

Added support for the following Linux servers:

- SUSE Linux Enterprise Server 15.
- Red Hat Enterprise Linux 8.2.
- CentOS Linux 7.6-1810 and 8.2-2004.
- Ubuntu 20.04.1 LTS.

Micro Focus Visual COBOL (Technology Preview)

Added support for Micro Focus Visual COBOL 6.0.

C/C++ (Technology Preview)

Improved support for constructs in C++11 using new Clang-based translation.

Speed Dial (Technology Preview)

- Added level 3 and 4 support.
- Improved intermediate development scan speeds by up to 50% (with a reduction in reported issues).
- Reduced scan time for typed languages such as Java and C/C++.
- Level 4 support provides a full scan.

Micro Focus Fortify Static Code Analyzer Tools

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

ScanCentral SAST Support in Secure Code Plugins

- ScanCentral SAST support added to Eclipse Complete Plugin, IntelliJ Analysis Plugin, and Visual Studio Extension.
- You can now submit ScanCentral SAST scan requests from the plugins.
- Added support for both local translation (send MBS file for scan phase) and remote translation (send package for both translation and scan phases).

Java 11 Runtime Support

- All tools and secure code plugins can be run in a Java 11 runtime environment.

Syntax Highlighting for Additional Languages in Audit Workbench

- Adds syntax highlighting for the following languages: ABAP, Apex, ASP, C# and ASP.NET, COBOL, Cold Fusion, Go, Kotlin, Objective C, PHP, Python, Ruby, Scala, Swift, VB.NET, Visual Basic 6.0 and configuration files.

Improved Merge Behavior in Visual Studio Extension

- Adds the ability to choose to merge with or overwrite a previous scan result.
- If an issue template is specified for the scan (configured as default or via additional scan option), the issue template from the new scan will be saved in the merged FPR.
- Set the merge option in **Fortify > Options > Project Configuration > Advanced Scan Options**. Select or clear the **Merge with Previous Scan** checkbox.

New Versions of Reports

- DISA STIG 5.1
- NIST 800-53 Revision 5
- CWE Top 25 2020

These can be generated from Fortify Audit Workbench, the secure code plugins, and the BIRTReportGenerator command-line interface.

Updated IDE Support

- Added support for Eclipse versions 2020-x and 2021-x in Micro Focus Fortify Plugins for Eclipse.
- Added support for Eclipse version 2021-x in Micro Focus Fortify Security Assistant Plugin for Eclipse.
- Added support for versions 4.x of Android Studio in Micro Focus Fortify Plugins for JetBrains IDEs and Android Studio.

Service Integrations

- Added support for Azure DevOps Server 2020.

Micro Focus Fortify ScanCentral DAST

The following features have been added to Fortify ScanCentral DAST.

Functional Application Security Testing (FAST)

FAST provides a CI/CD-friendly way to capture traffic from functional tests and send it to ScanCentral DAST for targeted DAST scanning.

API Scanning with Postman

In 21.1.0, ScanCentral DAST continues to simplify API scanning with its Postman integration. A new workflow in the WebInspect sensor automatically detects the authentication requests and excludes them from attack by default. There are also improvements to Oauth2.0 support.

Hacker Level Insights

Hacker Level Insights is a new framework that exposes those insights about an application that are interesting from a security perspective, but not necessarily a vulnerability. Detection of JavaScript client-side frameworks is included in 21.1.0.

Data Retention Policies

Configuring data retention policies at the application or scan level allows automatic purging of stale data to support ScanCentral DAST database maintenance and system performance in high usage environments.

Deny Intervals

ScanCentral DAST supports application and scan-level deny intervals when currently running scans are paused or forced to complete, and new scans do not start.

Base Settings

Base Settings provide ScanCentral DAST administrators the ability to apply scan setting templates across all applications or specific applications.

Policy Import

ScanCentral DAST supports using custom policies at both the application level and scan level.

Alerting

A messaging framework displays information about the quality and performance of scans in progress.

SiteExplorer Download

A link is provided in ScanCentral DAST to download SiteExplorer for visualization of a scan.

Horizontal Scaling (Technology Preview)

Horizontal scaling of sensor script engines provides dramatically faster scanning.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

HTTP/2 Support

Modern applications have begun leveraging HTTP/2 to improve the user experience with improved speed and more efficient client/server communication. WebInspect now supports applications that use HTTP/2 technology.

API Scanning with Postman

WebInspect continues to simplify API scanning with its Postman integration. A new workflow in the sensor automatically detects the authentication requests and excludes them from attack by default. There are also improvements to Oauth2.0 support.

Hacker Level Insights

Hacker Level Insights is a new framework that exposes those insights about an application that are interesting from a security perspective but may not necessarily be a vulnerability. Detection of JavaScript client-side frameworks is included in 21.1.0.

Engine 6.0 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.0.

Masked Parameters in TruClient

The Web Macro Recorder with Macro Engine 6.0 allows values for parameters such as password to be masked so they are hidden from view.

Simplified User Agent Selection

Selection of a User Agent in settings during scan configuration is now applied to both TruClient macros and the scan settings.

Alerting

Alert-level scan log messages provide information about the quality and performance of scans in progress.

OpenSSL

The OpenSSL technical preview is now the default SSL/TLS implementation in WebInspect. This integration provides support for TLS 1.3, and provides an option for customers whose system administrators may be restricting the Microsoft SCHANNEL stack.

Micro Focus Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Engine 6.0 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.0.

Masked Parameter in TruClient

The Web Macro Recorder with Macro Engine 6.0 allows values for parameters such as password to be masked so they are hidden from view.

Simplified User Agent Selection

Selection of a User Agent in Advanced Settings during scan configuration are now applied to both TruClient macros and the scan settings.

What's New in Micro Focus Fortify Software 20.2.0

November 2020

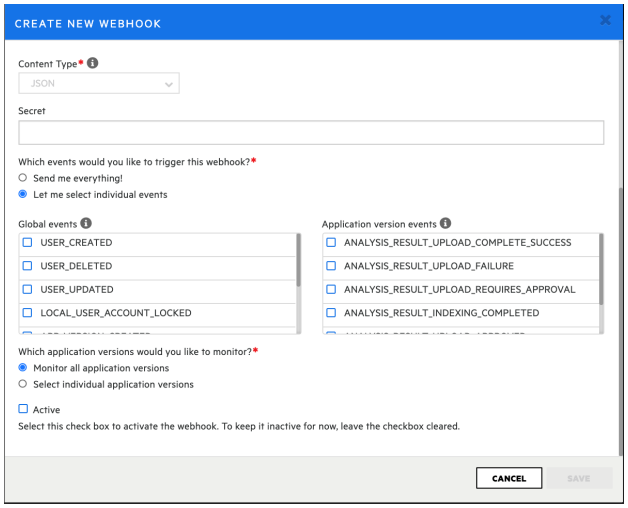
This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

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

Webhooks

The latest version of Fortify Software Security Center includes a new Webhook feature in the Administrative section. Use it to create hooks for system and application version events directly in the UI or API. When available, Webhooks can be helpful in updating external pipelines with Fortify Software Security Center data. This feature will drive our next generation of build failure workflows in the continuous integration plugins that we currently offer.

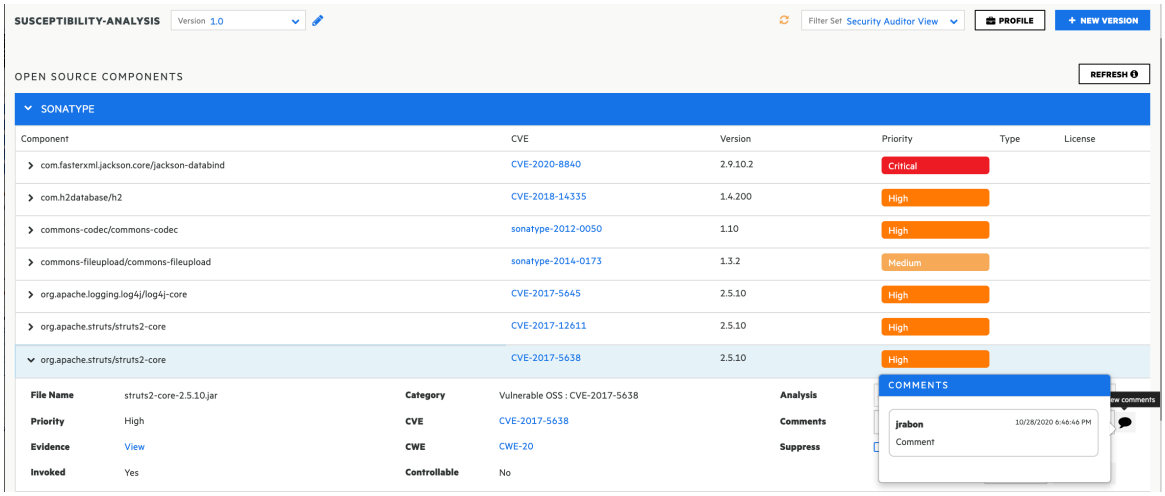


General Performance Improvements

- Ahead-of-time compilation reduces the time needed to download the JavaScript for our user interface. Our testing indicates a 40% reduction in the overall package size.
- The Issue endpoint has been refactored for better direct API performance.

Open Source Components View

A new Open Source Components view appears on the Open Source tab of the Issues page. This view displays Sonatype open source issues. The user can audit these issues directly in the view. This view also includes two new fields: Invoked and Controllable. These fields indicate whether the Sonatype-identified method or function(s) were called or user-controlled input reached this function/method in your custom code.



OWASP ASVS v4.0 Report

The OWASP ASVS v4.0 report provides an easy way to consolidate the list of requirements for secure software development as defined by this standard.

ScanCentral DAST

ScanCentral DAST joins the family! The ScanCentral tab in Fortify Software Security Center now has both SAST and DAST options. WebInspect customers can now orchestrate dynamic testing and automation from within Fortify Software Security Center.

Java 11 Support

Support for Java 11 in combination with Tomcat 9. See the *Micro Focus Software System Requirements* document for more information.

Fortify ScanCentral SAST

Product Name Change

With the introduction of Fortify ScanCentral DAST (for dynamic scans), Fortify ScanCentral was re-named ScanCentral SAST. For information about Fortify ScanCentral DAST, see the *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide*.

JavaScript Packaging Improvement

There is a new parameter available in the ScanCentral SAST client to include npm dependencies, when they are not present in the current working directory. Users can add `-scan-node-modules` to ScanCentral SAST client command. ScanCentral SAST will download the node modules and include them for translation and analysis. If this flag is not present, even if the node modules are there, we exclude them by default.

Quality Improvements

- ScanCentral SAST has improved support for multiple versions of Fortify Static Code Analyzer. When scanning resources are unavailable for a particular client version, more informative error messages will be issued.
- The auto upgrade feature now patches all connected ScanCentral SAST clients, avoiding the need to manually install the patches multiple times.
- ScanCentral SAST standalone clients receive both patch upgrades and major version upgrades (controller is upgraded).
- Embedded ScanCentral SAST clients from Fortify Static Code Analyzer will not automatically upgrade to the new version, but do receive patches.
- Custom build parameters that are required for software compilation are now included and invoked by ScanCentral SAST clients. Previously, the default build invocation parameters for supported build tools was used.

Micro Focus Fortify Static Code Analyzer

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

Java

- Support added for Java 14
- Native support for Lombok added. It is not necessary to use “delombok” anymore
- Support added for Kotlin interoperability

  If your project contains Java code that refers to Kotlin code, include all the source directories in the translation command so that the Kotlin function calls are correctly resolved

.NET

- Now uses MSBuild 16.6
- Added Generics Type support

Swift/Obj C

- Added support for XCode up to version 11.7
- JavaScript

JavaScript

- Support added for TypeScript 3.3- 4.0
- Support added for ECMAScript 2019 and 2020

Kotlin

- Added full support for Kotlin 1.3.50
- Kotlin support is no longer a Technology Preview
- Added Kotlin Java Interoperability

  If your project contains Kotlin and Java source code, you can use the Java source to resolve any Kotlin types that refer to Java files
- Added Kotlin for Android support

Go

- Added support for Go Modules
- Refactoring of Go translation which allows easier translation and takes away the need to have Go installed on the translation machine

COBOL

- Added support for IBM Enterprise COBOL up to version 6.1

Python

- Added support for Python 3.8
- Improved imports support for Python

Docker

- Added support for running Fortify Static Code Analyzer in a Docker container
- Added support for scanning Docker configuration files

ABAP Extractor

- Improved performance
- Added option to block the download of SAP standard code

Modular Analysis (Technology Preview)

- Updated to include control flow analysis

Speed Dial (Technology Preview)

The first version of Speed Dial provides a selection of configuration files to select the breadth and depth of the desired Fortify Static Code Analyzer scan.

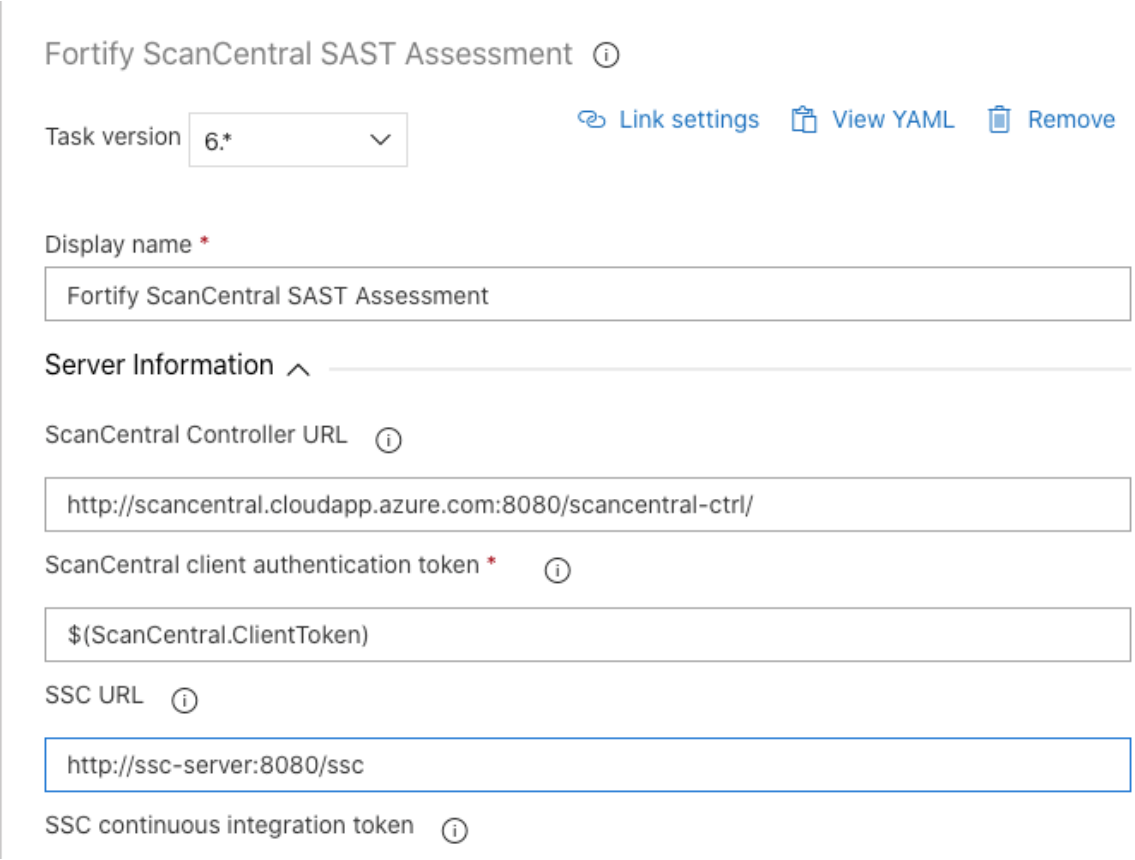
Micro Focus Fortify Static Code Analyzer Tools

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

Azure DevOps

- New ScanCentral SAST Task

With the new Azure DevOps task, you can programmatically install the ScanCentral SAST client from the controller to configure and use the ScanCentral SAST client to orchestrate remote scanning from Azure DevOps. This works for both hosted and local build agents.

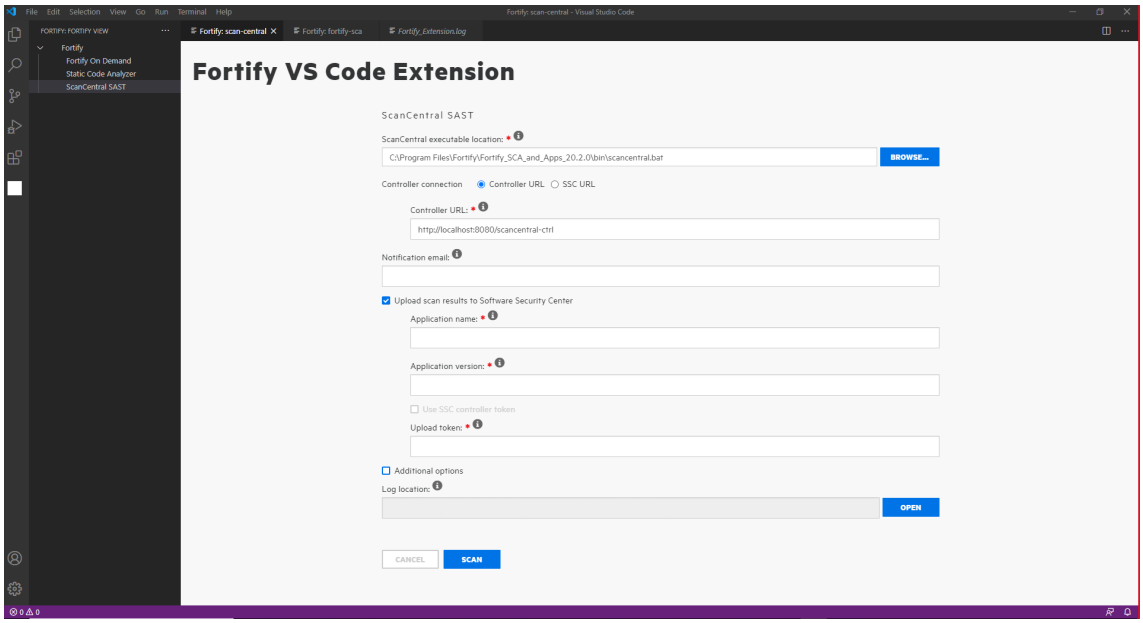


- New ScanCentral DAST Task

In Azure DevOps, this task allows you to automate and orchestrate remote dynamic (WebInspect) scans from the ScanCentral DAST module inside of Fortify Software Security Center.

Visual Studio Code

Fortify is happy to welcome the Fortify Visual Studio Code Extension to our IDE plugin family. In this first release, local Fortify Static Code Analyzer scans, remote scans via ScanCentral, and remote scans via Fortify on Demand are all supported.



Token Authentication in all the Tools

Fortify has introduced token-based authentication to Fortify Static Code Analyzer from Audit Workbench and the Visual Studio, Eclipse, and IntelliJ plugins.

Support for OWASP ASVS v4.0 Report

Support has been added for OWASP ASVS v4.0 reports.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Automatic Detection of Single-page Applications

Fortify continues to improve usability with time-saving features that eliminate manual configuration of scans. WebInspect 20.2.0 detects when applications use modern frameworks such as Angular and React and automatically adjusts its configuration to provide the best coverage.

For more information, read the Help topic and watch the "SPA Scanning Improvements" video on the Fortify Unplugged YouTube channel.

Redundant Page Detection

Applications with lots of redundant content, such as content management systems and catalog sites, can cause unnecessarily long-running scans. With WebInspect 20.2.0, you can use an advanced redundant page detection algorithm to reduce these scan times.

For more information, read the Help and watch "Handling Redundant Content with WebInspect 20.2" on the Fortify Unplugged YouTube channel for more information.

ADFS CBT Support

Per advice from Microsoft, many organizations are implementing a channel binding token (CBT) to secure Active Directory Federation Services (ADFS) authentication. WebInspect 20.2.0 now supports this extended protection mechanism. Look at Scan Settings under `Network Authentication > Method > ADFS CBT` to use this new feature, and reference the Help topic for details.

Engine 5.1 Updates

Fortify continues to evolve its engines to improve coverage and performance. WebInspect 20.2.0 provides a faster crawl and audit, and better application support from the web macro recorder. Finally, as a sneak peak of things to come in 2021, the Web Macro Recorder with Macro Engine 5.1 now attempts to detect and display client-side frameworks that are used in the target application. For more information, read the Help.

OpenSSL Technical Preview

WebInspect 20.2.0 introduces a technical preview of our OpenSSL integration. This integration provides support for TLS 1.3, and provides an option for customers whose system administrators may be restricting the Microsoft SCHANNEL stack. The setting may be enabled in the UI at `Edit > Application Settings > General`.

ScanCentral DAST

Fortify is excited to release a new DAST orchestration and automation platform integrated right into Software Security Center 20.2.0! For more information, watch our "Introduction to ScanCentral DAST" video on the Fortify Unplugged YouTube channel.

Micro Focus Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Automatic Detection of Single-page Applications

Fortify continues to improve usability with time-saving features that eliminate manual configuration of scans. The WebInspect 20.2.0 sensor detects when applications use modern frameworks such as Angular and React, and automatically adjusts its configuration to provide the best coverage.

For more information, read the Help topic and watch the "SPA Scanning Improvements" video on the Fortify Unplugged YouTube channel.

Redundant Page Detection

Applications with lots of redundant content, such as content management systems and catalog sites, can cause unnecessarily long-running scans. With the WebInspect 20.2.0 sensor, you can use an advanced redundant page detection algorithm to reduce these scan times.

For more information, read the Help topic and watch “Handling Redundant Content with WebInspect 20.2” on the Fortify Unplugged YouTube channel.

ADFS CBT Support

Per advice from Microsoft, many organizations are implementing a channel binding token(CBT) to secure Active Directory Federation Services (ADFS) authentication. The WebInspect 20.2.0 sensor now supports this extended protection mechanism. For more information, read the Help topic.

Contact 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://www.microfocus.com/support

For More Information

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