



Hewlett Packard
Enterprise

HPE Security

Fortify Software Security Center

What's New

What's New in HPE Security Fortify Software Security Center 16.10

April 2016

This release of HPE Security Fortify Software Security Center includes the following new functions and features.

HPE Security Fortify Software Security Center

- Common Access Card (CAC) support
- Kerberos/SPENGO support
- Updated help when requesting a new account or logging in
- RESTful API v1 documentation
- REST API access with limited action tokens
- New CloudScan Controllers, CloudScan Sensors, and CloudScan Scan Requests interfaces
- Bugtracker support for Team Foundation Server
- Improved job management performance and reliability
- You can now cancel and change job priority (of prepared jobs)
- Improved performance for out of order scan processing
- Improved performance when deleting scan artifacts
- Unlock user accounts (Admin)
- Advanced "Copy From" options are now available when creating a new Application version
- Show more records on the dashboard on user request
- Administratively disable/enable legacy UI
- Change user passwords in the new UI
- Variables and Performance Indicators are now available in the Version level trend chart
- Aggregate/Filter/Group by all custom attributes at the global dashboard level
- Aggregate/Filter/Group by custom tags at the application version level



Hewlett Packard Enterprise

- User persistence across user sessions (some selections)
- Group by Folder on issue page
- Enable email alerts for logged in user
- Multiple LDAP configuration moved to Administration page and support for multiple LDAP servers added
- Syntax highlighting for Swift
- HPE Security branding

HPE Security Fortify Static Code Analyzer (SCA)

- Support for Objective-C++
- Performance improvement for the Higher Order analyzer
- Initial support for Swift
- Improved @ModelAttribute for SpringMVC
- Improved DOM/selector support for jQuery
- Xcode 7.3 support
- HPE Security branding
- Quality improvements for
 - Java translator
 - Javascript translator
 - Rule processing
 - JSP translator
 - C/C++ translator

HPE Security Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and WebInspect Agent

- Support for Syslog-NG connection using UDP, TCP, and TLS connections
- Support for event deep-link in the ESM CEF events
- Improvements to SLQi detection and prevention
- Performance improvements
- Bug fixes and stability improvements



HPE Security Fortify Static Code Analyzer Tools

- New Maven plugin with enhanced Maven support
- BIRT reporting for Visual Studio Plugin
- Improved usability of SCA Analysis and Translation errors for AWB and Eclipse plugin
- Group by FileType added to Audit Workbench
- Custom rules support for Security Assistant
- Xcode 7.x support
- Improved Team Foundation Server bugtracker integration for Visual Studio plugin
- Jenkins plugin now supports 1.652
- HPE Security branding

HPE Security WebInspect

- **Site Explorer**

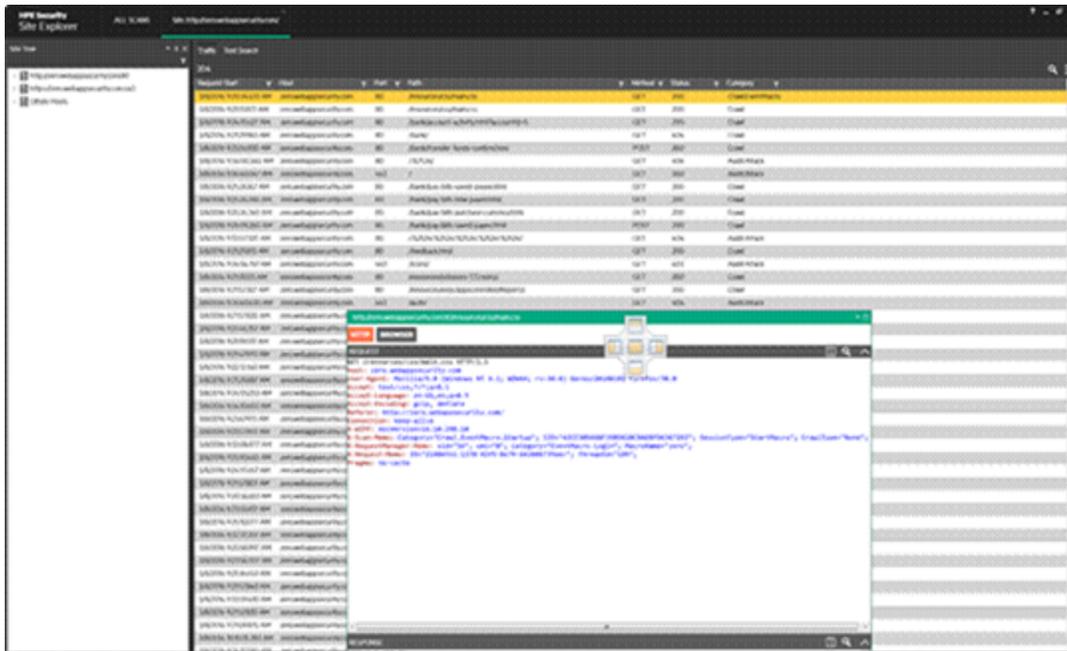
After working with customer feedback about numerous designs, we have begun to reimagine and restyle the WebInspect user interface (UI). To give our users a first glimpse at the new UI style and allow them to provide feedback, we have released our work as a separate tool that can be accessed from within WebInspect. The tool is called Site Explorer, and is available in this release as a technology preview. Although the work is not complete, users can view their own scan data, previously completed or currently running, inside the new UI. The vulnerability review section, however, has not been implemented and is not available in this version of the tool.

One of the top priorities for this UI redesign has been performance. Site Explorer runs as a separate process, allowing Windows to better distribute resources between the UI and the scanning engine. We have also created a new file type called the TSF which functions as a virtual database. The structure of this new format allows Site Explorer to load scan files in an incredibly short order, which will save users valuable time in triaging results.

To better accommodate our users of various skill levels, we have included multi-window capabilities and advanced search functionality throughout Site Explorer. Currently the site tree, traffic grid, and the detail views can be floated and docked to any part of the UI or moved to another screen as seen below. Additionally, the request/response for an open session can be cloned to create a duplicate request/response.



Hewlett Packard Enterprise



The traffic grid shows all of the traffic data from the scan. Each session can be drilled down into and parent sessions and related traffic are easily accessible. The traffic can be searched with plain text, using special commands such as server, type, or origin ID, or filtered based on the column data.

- **DOM Explorer**

DOM Explorer is another technology preview tool that customers can use to crawl single-page applications (SPAs) or other “Web 2.0” sites that make heavy use of JavaScript and other client-side technologies. The term DOM stands for Document Object Model and is defined by W3C as “a platform- and language-neutral interface that will allow programs and scripts to dynamically access and update the content, structure and style of documents.”

The modern concepts of SPAs and JavaScript-heavy pages have proven a challenge for the traditional crawling and script engines used in DAST products. In order to overcome these challenges, we returned to the drawing board, creating our own engine which can navigate and understand the frameworks of “Web 2.0” sites. This new engine will provide WebInspect unparalleled control over the state of the DOM, allowing WebInspect to perform advanced testing techniques not currently available on the market.

The DOM Explorer can be started either as an .exe or from the tools menu in WebInspect. Once started, users can enter a single URL to be scanned or use a login macro to authenticate and crawl the site. Instead of the usual site tree structure, users will see a DOM event tree listing the individual elements and events that are exercisable on the page. If possible, when a specific element is selected in the DOM tree, the affected area of the page will be highlighted in the browser view. The traffic that was captured from the crawl can be explored and saved as a workflow macro. This macro can be used in an audit-only scan in WebInspect to perform attacks against the site.

It is important to note that the DOM Explorer is a technology preview and is not 100% complete as a feature. We have released it as a technology preview to enable our customers to begin taking advantage of the new technology and to provide us feedback on its capabilities. As we continue to build out this functionality, it will eventually become a part of the default crawler behavior.



Hewlett Packard Enterprise

- **Updates to Traffic Viewer**

Several UI features and functionality that were developed for Site Explorer have also been added to the Traffic Viewer tool. For example, you can customize the detail views, drill down in the Traffic grid view to see related traffic, and use breadcrumbs to help you navigate the traffic for a resource in the traffic grid.

- **New Audit Setting to Suppress Off-site Vulnerabilities**

If your Web application includes links to hosts that are not in your Allowed Hosts list, WebInspect may identify passive vulnerabilities on those hosts. You can use the new Suppress Offsite Vulnerabilities to suppress all vulnerabilities against sessions for off-site hosts that are not in your Allowed Hosts list.

- **New Application Setting to Create Scan Data for Site Explorer**

During a scan, WebInspect creates a SQL Express database (.mdf) file or adds the scan to an existing SQL Server database (.mdf) file. However, Site Explorer uses a variation of the traffic session file (.tsf) format. You can use the Create Scan Data for Site Explorer setting to have WebInspect create a traffic file that can be displayed in Site Explorer.

HPE Security WebInspect Enterprise

- **WebInspect Enterprise REST API**

As part of the WebInspect Enterprise installation, a REST API service is installed. You can use the REST API to work with scans, scan settings files, scan schedules, projects, and other functions programmatically. The REST API includes a complete set of online documentation with code samples. For information about accessing the WebInspect Enterprise REST API and its documentation, see the HPE Security WebInspect Enterprise Installation and Implementation Guide.

- **Using SAN or Wildcard Certificates and Non-Standard Ports in IIS**

The WebInspect Enterprise Initialization Wizard does not overwrite certificate and port bindings that you create in IIS. As a result, you can use SAN or wildcard certificates and non-standard ports when configuring the WebInspect Enterprise Manager Web Service during initialization.

- **New Options for HTTPS Bindings for the Root Web Site in IIS**

If you have configured HTTPS bindings for the root web site in IIS, only those bindings will be listed in the Available Certificates. You will not be able to create a new binding for a web site in the WebInspect Enterprise Initialization Wizard. You can create a new binding only in IIS. Your options when configuring the WebInspect Enterprise Manager Web Service are now based on your IIS settings.

- **WebInspect Enterprise Manager Web Service Uses IIS Integrated Mode**

During upgrade, the WebInspect Enterprise Manager Web Service (WIE server) will be set up in IIS using the IIS integrated mode for the application pool. This means that the WebInspect Enterprise web site no longer needs to have ISAPI filters configured or ISAPI and CGI restrictions configured in IIS. Integrated mode does not use either of these elements. The WebInspect Enterprise Initialization Wizard will no longer warn you if these elements are not configured in IIS.

- **WebInspect Enterprise Installation and Implementation Guide**

The WebInspect Enterprise Installation Guide and the WebInspect Enterprise Implementation Guide



Hewlett Packard Enterprise

have been combined into a single guide. The new HPE Security WebInspect Enterprise Installation and Implementation Guide contains all of the information from the two guides.

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

650.735.2215

For More Information

For more information about HPE Security software products: <http://www.hpenterprisesecurity.com>



What's New in HP Fortify Software Security Center 4.40 and HP WebInspect 10.50 Products

November 2015

This release of HP Fortify Software Security Center includes the 10.50 release of WebInspect and WebInspect Enterprise. The WebInspect products were developed in conjunction with the 4.40 components and are an integral part of the HP Fortify Software Security Center 4.40 release.

Software Security Center (SSC)

- SSC now requires a case-sensitive collation for all databases.
- Performance improvements have resulted in decreased time for data purge, FPR processing, and report generation processing.
- SSC has an entirely redesigned user interface (UI) that's simpler and easier to navigate.
- The Dashboard now includes summary charts which, like tooltips, are visible when you move your cursor over findings for a "top risk maker."
- Entities that were termed "projects" in earlier versions are now termed "applications."
- Entities that were termed "project templates" in earlier versions are now termed "issue templates."
- SSA projects and process templates have not yet been migrated to the 4.40 user interface. However, for this release, you can work with SSA projects in the legacy user interface.
- The term "Collaboration Module" is no longer used.
- You have the choice of using the redesigned UI, the legacy UI (v4.30), or both.
- The **Runtime** and **CloudScan** tabs do not exist in the new UI. You can find this functionality in the legacy UI, but in order to use it, you must configure your Runtime and CloudScan connections in the new UI.
- The UI now contains an icon to alert you when application data displayed are not up to date. You can click this icon to refresh the data. The icon disappears when the refresh is complete.
- You cannot change the format for date and time display in the new UI. You must use the legacy Flex interface instead.
- You can now integrate SSC with SAML 2.0 or Oracle Identity Management providers for single sign-on.
- If your organization uses SAP NetWeaver Code Vulnerability Analyzer (CVA) to search for vulnerabilities in ABAP source code, you can now use the NetWeaver plugin to map your CVA scans to an SSC application version, and then import the results for investigation from SSC. SSC



Hewlett Packard Enterprise

displays the individual CVA findings, identifies their source code file names and line numbers, assigns each a Fortify priority order, and displays them in the SSC UI for auditing.

- SSC now has robust, category-based search functionality that applies search terms across application versions, issues, reports, comments, and users. Its new search engine returns results almost instantaneously.
- To add an extra measure of security to BIRT reporting, you can create a database user account with read-only access to the SSC database, and then use the account credentials to configure BIRT reporting in SSC. For even greater security, you can also enable a strict mode for running reports in a separate Java process.
- If you are not an administrator and you need to change your own account information, including your password, you must revert to the legacy UI to make these changes. (See “Changing Your Account Information (Legacy UI)” in the documentation.)
- The new UI in this version does not support extensible custom tags, which enabled users to add new custom tag values during audits. The legacy UI still supports extensible custom tags, and allows users to use all the new values while performing an audit.
- The new UI does not support showing issue attachments. You must use the old UI for this functionality.
- If your single sign-on (SSO) server works with Security Assertion Markup Language (SAML), you can now integrate SSC with SAML 2.0.
- The legacy Flex interface does not work when run from WebLogic and accessed through Internet Explorer.

HP Fortify Static Code Analyzer (SCA)

- There are numerous fixes to the type inference engine for Java translation. As a result, many more expressions involving lambdas and type arguments are assessed correctly.
- Support has been added for iOS9 Objective-C applications in Xcode 7.
- Enhancements have been made to Higher Order Analyzer to improve performance and analysis capabilities.
- There is improved support and numerous bug fixes for JavaScript.
- SCAScanner has been updated with a `-liveprogress` option which displays a text window to provide a regularly updated interface of current scan progress and analyzer information. On Unix-like platforms, this feature uses the current terminal window if you use the `-nogui` option.
- Several Python bugs were fixed resulting in improved accuracy of analysis.
- Support has been added for all ColdFusion 9 and 10 tags and functions, as well as a number of syntax extensions. Future support is still needed for “components” and other ColdFusion 9 and 10 features.
- SSC now has extended support for Java coding and logic flaws.
- SAP ABAP support has been added for “Access Control: Authorization Bypass.”



Static Code Analyzer Tools

- A real-time, in-line Security Assistant Plugin for Eclipse has been added. The Security Assistant Plugin works with HP Fortify security content to provide alerts to potential security issues as you write your Java code.
- Support for Xcode Maven projects has been added to the HP Fortify Maven plugin.
- You can now run HP Fortify SCA scans on projects in the Xcode development environment (IDE) using the HP Fortify Scanning Plugin for Xcode.
- Audit Workbench now verifies all necessary permissions before downloading the FPR for collaborative audits. This feature helps to ensure that you can continue auditing results even if your connection to SSC is temporarily lost. Additionally, Audit Workbench can now recover when collaborative auditing loses connectivity to the server.
- Audit WorkBench and the Eclipse remediation plugin now provide BIRT reports. These are the same reports in content, look, and feel as the reports available in SSC. We will continue to expand the reports available in the other tools in future releases.
- The HP Fortify Maven plugin now supports CloudScan.
- The HP Fortify Jenkins plugin now supports Jenkins version 1.6.
- The Scan Wizard now supports Java bytecode.
- All tools now support Bugzilla 4.x.

WebInspect Version 10.50

- **Privilege Escalation**

WebInspect can now test whether a lower-privilege user can gain access to pages and capabilities that should be available only to a user with higher-privilege rights. It does so by using two separate login macros to crawl the site for both users and then comparing the results to identify pages that the lower-privilege user does not have a link to but can access by direct navigation. With this capability, customers can now automate even more of their dynamic testing. For more information, see “About Privilege Escalation Scans” in the WebInspect help.

- **Traffic Viewer Tool**

As a first step towards moving to a new style of user interface, the WebInspect team has created the new Traffic Viewer tool. This tool displays the traffic monitor data and will eventually replace the proxy tool. It is available in both WebInspect and WebInspect Enterprise, allowing traffic monitor data to be captured by a WebInspect Enterprise scan for the first time. Having a separate tool to visualize the data means that customers can split the applications between multiple screens to visualize the scan progress or vulnerabilities while simultaneously parsing the traffic data. For more information, refer to the Traffic Viewer tool online help or the Tools Guide for WebInspect Products.

- **Selenium Support**



Hewlett Packard Enterprise

WebInspect 10.20 made it possible for customers to use the WebInspect application program interface (API) to automate the capture of traffic from their Selenium scripts and translate it into a workflow macro. Over the last year, several customers asked us for improved integration with Selenium scripts to make it a more native integration. In this release, we have added native support for Selenium integrated development environment (IDE) scripts for use as both automated login macros and workflow macros. Customers who have other teams in their company using Selenium scripts for automated testing can now reuse those scripts to enhance the coverage of their WebInspect scans. For more information, see “Using Macros” in the WebInspect help.

- **Updates to the WebInspect API**

As a part of our commitment to creating the most robust and flexible dynamic application security product on the market, we continue to expand our API with each release. In WebInspect 10.50, we have added the ability to modify any input fields in a macro which have been “parameterized” to allow for a change in the value before the scan is initiated. This eliminates the need to bring up the user interface and modify the password as it expires every few months; instead, the new password can simply be supplied as a part of the command line or API call. For more information, see “WebInspect API” in the WebInspect help.

- **Link Sources Settings**

WebInspect 10.50 includes a new Link Sources crawler settings page that allows users to select Pattern-based or DOM-based link parsing, and to customize which DOM-based link sources are ignored during a crawl. These settings may be useful in preventing potentially large volumes of bad links from cluttering the crawl and resulting in extremely long scan times. For more information, see “Crawl Settings: Link Sources” in the WebInspect help.

- **New Audit Engines**

WebInspect includes a new Directory Extension audit engine. Directory extension checking involves adding extensions to directories and removing the trailing slash to find archived directories left on the server. WebInspect attempts to locate all directories that have been left on your server that could be used by an attacker.

WebInspect includes a new File Prefix audit engine. Network administrators and developers often leave backup files and scripts on the web server. These files commonly contain information that can be used to breach a site's security. Prefix checking involves affixing a value to file names, and then looking for older or backup versions stored on the site.

WebInspect Enterprise Version 10.50

- **Macro Repository**

Customers working with WebInspect Enterprise 10.50 now have the option of storing their login or workflow macros as an artifact inside a project version. Each macro can be downloaded for modification or use, overwritten by uploading a newer version, or referenced as a part of the scan



Hewlett Packard Enterprise

wizard. As with all items in WebInspect Enterprise, access to these macros can be controlled using the permissions model to prevent unauthorized users from downloading or modifying them.

- **New Project Version Wizard**

WebInspect Enterprise 10.50 includes a new wizard for creating new project versions. Customers no longer need to shift to the Software Security Center (SSC) portal just to create a new project version for scanning. The wizard prompts the user to choose which organization and group the project version belongs to in WebInspect Enterprise so an administrator is not needed to move it after creation.

- **Privilege Escalation**

For a description, see [WebInspect Version 10.50](#). For more information, see “About Privilege Escalation Scans” in the WebInspect Enterprise Thin Client Download help.

- **Traffic Viewer Tool**

For a description, see [WebInspect Version 10.50](#). For more information, refer to the Traffic Viewer tool online help or the Tools Guide for WebInspect Products.

- **Selenium Support**

For a description, see [WebInspect Version 10.50](#). For more information, see the following topics in the WebInspect Enterprise Thin Client Download help:

- Configuring Web Site Scans Using a Predefined Template
- Configuring Mobile Web Site Scans Using a Mobile Template
- Configuring Native Scans Using a Mobile Template
- Link Sources Settings

For a description, see [WebInspect Version 10.50](#). For more information, see “Crawl Settings: Link Sources” in the WebInspect Enterprise Thin Client Download help.



What's New in HP Fortify Software Security Center 4.30 and HP WebInspect 10.40 Products

April 2015

This release of HP Fortify Software Security Center includes the 10.40 release of WebInspect and WebInspect Enterprise. The WebInspect products were developed in conjunction with the 4.30 components and are an integral part of the HP Fortify Software Security Center 4.30 release.

HP Fortify Software Security Center 4.30

- Using the new Administration section of the user interface (UI), you can now:
 - Specify many of the settings that were previously in the configuration tool.
 - Use a wizard to create new applications and versions.
 - Generate reports.
 - Create and manage alerts.
 - Filter, group, and aggregate Bar charts, Trend charts, and Table charts by custom attributes.
- Data purging performance has been greatly improved.
- FPR processing performance has been greatly improved.

HP Fortify Static Code Analyzer 4.30

- Core Ruby 1.9 is now fully supported. (It is no longer a technology preview.)
- Java Bytecode is now supported. Enable it using the following properties:

```
com.fortify.sca.fileextensions.class=BYTECODE
```

```
com.fortify.sca.fileextensions.jar=ARCHIVE
```

During the translation phase, specify the jar files and any source files you want to scan.

- Django 1.7 is now supported. Enable it using the following properties:



Hewlett Packard Enterprise

```
-Dcom.fortify.sca.limiters.MaxPassthroughChain Depth=8
```

```
-Dcom.fortify.sca.limiters.MaxChainDepth=8
```

Note: Do not change the value of these properties. Other values are not currently supported. Do not set these values when scanning non-Django projects as they could negatively impact performance.

During the translation phase, set the switch:

```
-django-template-dirs path/to/template/dirs
```

- The ABAP Parser now supports all ABAP constructs.
- Higher Order Analyzer is provided as a technology preview. For languages other than Java, it enables SCA to perform analysis on higher order functions such as lambdas. To enable languages for higher order analysis, add a comma-delimited list of languages to the `fortify-sca.properties` file. For example:

```
com.fortify.sca.Phase0HigherOrder.Languages=javascript,ruby,python
```

To enable type inference for languages that are enabled for higher order analysis, add a comma-delimited list of languages to the `fortify-sca.properties` file. For example:

```
com.fortify.sca.TypeInferenceLanguages=javascript,ruby,python
```

- Xcode 6.0, 6.1, and 6.2 are now supported.
 - Xcode 5.0, 5.1, 6.0, 6.1, and 6.2 on Mac OS X 10.9 and 10.10 are supported.
 - Projects targeting any processor architecture, not only i386, are supported.
 - SCA no longer requires that `xcodebuild` command lines include “`-sdk iphonesimulator`”.
- Build integration with the `llvm-gcc` compiler has been removed; SCA no longer recognizes `llvm-gcc` as the name of a compiler.
- Build integration with Xcode 4.5 and 4.6 has been removed.

HP Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and WebInspect Agent

The installation of Runtime agents for the following products has been greatly simplified:



Hewlett Packard Enterprise

- Runtime Application Protection (RTAP)
- WebInspect Agent
- HP ArcSight Application View

HP Fortify GUI Tools

- Bug tracking support has been added for Application Lifecycle Manager 12 and Jira 6. GUI Tool properties are described in the *HP Fortify Static Code Analyzer Tools Properties Reference Guide*
- There is a new scanning plugin for IntelliJ 13 and Android Studio.
- Microsoft has deprecated command-line support for Visual Studio 2015. Microsoft will need to reestablish command-line support before HP can address this.

WebInspect Version 10.40

- **WebInspect Software Development Kit (SDK)**

After the successful release of the WebInspect API a year ago, customers asked for deeper integration with WebInspect to get the most out of the product. The WebInspect team has developed a full SDK so that customers can write their own vulnerability checks, called custom agents, for direct consumption by the WebInspect engines. The SDK is distributed as a Visual Studio starter kit and includes documentation, code samples, and templates to assist users in writing their custom agents. Once created, custom agents can be published to WebInspect or WebInspect Enterprise to be used in scans. For more information, see the “About the WebInspect SDK” topic in the WebInspect help.

- **Merge Scan Files**

An option has been added to the WebInspect command line utility that allows customers to merge the results of multiple scans into a single scan. Users can now split large websites into smaller scans and merge the results back together. For more information, see the “Command Line Execution” topic in the WebInspect help.

- **Vulnerability Rollup**

Application developers reuse code to the extent that sometimes every page in an application uses the same code. If a reused piece of code, such as a search bar, has a vulnerability, then WebInspect may report that vulnerability dozens or even hundreds of times. Users can now roll up all of these vulnerabilities into a single parent vulnerability for easier reporting to management and development. For more information, see the “About Vulnerability Rollup” topic in the WebInspect help.

- **SmartUpdate – Checks and Policies Tabs**

Users can now easily identify which policies will be affected by an addition or change in a vulnerability check when they run HP SmartUpdate. Two new tabs on the SmartUpdate window, **Checks** and **Policies**, allow users to see which policies are affected by a specific check or which checks are affected in a given policy. This information helps users understand whether the



Hewlett Packard Enterprise

differences between scans are due to a change in WebInspect or a change in the application being scanned. For more information, see the “SmartUpdate” topic in the WebInspect help.

- **WebInspect Feedback Program**

The WebInspect team has built a telemetry server and added telemetry functionality to WebInspect, which allows customers to choose to send important **generic** information about how the application is performing. This information will help the engineering and research teams more quickly identify ways to improve the product for higher quality results.

- **Additional Supported Systems**

WebInspect now supports Windows Server 2012 R2, SQL Server 2012 SP2, and ALM 12 as well as Internet Explorer 11 and Firefox 33.

- **Performance**

The WebInspect team has been focusing on performance improvements over the last few releases. Customers may again notice a decrease in scan times as further updates and fine tuning have resulted in additional performance gains with WebInspect 10.40.

Webinspect Enterprise Version 10.40

- **WebInspect Enterprise Search**

WebInspect Enterprise is designed for companies to run and store dynamic scans on all of their applications, no matter how many that may be. However, the security professionals running the scans may not be familiar with every project and may not have re-scanned a particular URL for a year or more. WebInspect Enterprise now gives users a way to search for information such as application names, version names, and URLs. Now, even with 1000 applications stored in their WebInspect Enterprise server, users can find exactly what they are looking for quickly and easily. For more information, see the WebInspect Enterprise Web Console help.

- **Scan Template Change Inheritance**

Any changes made to scan templates can now be propagated out to currently scheduled scans that use the template being updated. Customers can now change the settings of large numbers of scheduled scans without needing to modify each schedule individually. For more information, see the “Scan Template - Scan: General” topic in the WebInspect Enterprise Web Console help.

- **SSC Scan Request Data Harvesting**

Now, when a user creates a scan from an SSC scan request, the URL will be copied over for them automatically. WebInspect Enterprise determines the start URL from the data in the Scan Request that was sent from SSC. The Scan Wizard opens and the Start URL field is auto-filled with the URL from the scan request. The URL, Username, and Password fields are also right-clickable to allow users to copy the data to the clipboard. For more information, see the “Using Scan Requests from SSC” topic in the WebInspect Enterprise Web Console help.

- **Server Setup Verification Checks**



Hewlett Packard Enterprise

As a part of the WebInspect Enterprise installation, checks will now be run to validate that the server has been set up correctly and that users have the correct permissions. This will help customers avoid needless support calls or odd behavior of their installation. For more information, see the *WebInspect Enterprise Installation Guide*.