

# Qualys WAS 4.6 New Features

We welcome some long awaited exciting new features with WAS 4.6. They are encompassed in what we call SmartScan. SmartScan allows for enhanced and advanced scanning of AJAX heavy web applications along with enhanced support for Single Page Applications (SPA) and also advanced frameworks such as AngularJS and bootstrap. We also are introducing enhanced support for Google Web Toolkit (GWT) and Direct Web Remoting (DWR) as well.

Please note that this is our first phase and limited release of these new features and capabilities. We will be releasing many enhancements to this SmartScan in upcoming WAS versions including, but not limited to; enhanced JSON formatted data testing, enhanced URL rewriting support along with additional framework support.

\*SmartScan will be available in limited release only for the first phase of deployment and will only be available upon request from Technical Account Managers (TAMs). This feature will require approval. Minimum dependencies are WAS 4.6, Portal 2.12 and Engine 3.15.

With this release we are also introducing additional sitemap reporting functionality as well as various bug fixes.

## Feature Highlights:

- **Introduction of SmartScan**
- **Enhanced Sitemap Reporting**
- **Enhanced Option Profile Scope Selection**

## SmartScan

SmartScan allows for enhanced and advanced scanning of AJAX heavy web applications along with enhanced support for Single Page Applications (SPA) and also advanced frameworks such as AngularJS and bootstrap. We also are introducing enhanced support for Google Web Toolkit (GWT) and Direct Web Remoting (DWR) as well.

Please note that this is our first phase and limited release of these new features and capabilities. We will be releasing many enhancements to this SmartScan in upcoming WAS versions including, but not limited to; enhanced JSON formatted data testing, enhanced URL rewriting support along with additional framework support.

\*SmartScan will be available in limited release only for the first phase of deployment and will only be available upon request from Technical Account Managers (TAMs).

This feature will require approval. Minimum dependencies are WAS 4.6, Portal 2.12 and Engine 3.15.

### Option Profile Create Dialog

When creating a new profile, if the SmartScan option has been enabled for the customer, the *Scan Parameters* step will display a new section SmartScan Support, that will explain to user what the feature is about and will propose a checkbox to enable the feature.

If the user checks the option, an additional setting *SmartScan Depth* will be displayed, with some explanation of the role of that setting. The default value for that setting will be set to 5.

Option Profile Creation

Turn help tips: On | Off Launch help

Step 2 of 5

1 Profile Details

2 Scan Parameters

3 Search Criteria

4 Comments

5 Review And Confirm

Please define how the scan will perform

User Agent

Example: Mozilla/4.04 (X11; I; SunOS 5.4 sun4m)

Request Parameter Set\*

Test Paramset (Default)

View Create

Document Type

☒ Ignore common binary files based on file extensions.

SmartScan Support

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

☒ Enable SmartScan Support

You can customize the number of actions that can be tested per page. Note the higher the number you set, the longer the scan duration.

SmartScan Depth\*

5

Behavior Settings

These settings define the threshold to be reached before stopping the scan. If you deactivate these settings, the scan will keep running no matter how many errors it will find.

Cancel

PreviousContinue

The *Review And Confirm* step will display the options selected by user:

- If user enabled the option:

**Option Profile Creation** Turn help tips: On | Off Launch help X

**Step 5 of 5**

- 1 Profile Details ✓
- 2 Scan Parameters ✓
- 3 Search Criteria ✓
- 4 Comments ✓
- 5 Review And Confirm

Review and confirm this Option Profile

**Scan Parameters**

Form Submission	Post & Get
Maximum crawl requests	300
Document Type	Ignore common binary files based on file extensions.
SmartScan Support	Enabled
SmartScan Depth	5
User Agent	—
Request Parameter Set	Initial Parameters (Default)
Scan Intensity	Low

**Processes to run in parallel**  
Total processes: 10  
HTTP processes: 2  
**HTTP request delay**  
Request delay: High

Bruteforce option Minimal

Cancel Previous Finish

- If user left the option disabled:

**Option Profile Creation** Turn help tips: On | Off Launch help X

**Step 5 of 5**

- 1 Profile Details ✓
- 2 Scan Parameters ✓
- 3 Search Criteria ✓
- 4 Comments ✓
- 5 Review And Confirm

Review and confirm this Option Profile

**Scan Parameters**

Form Submission	Post & Get
Maximum crawl requests	300
Document Type	Ignore common binary files based on file extensions.
SmartScan Support	Disabled
User Agent	—
Request Parameter Set	Initial Parameters (Default)
Scan Intensity	Low

**Processes to run in parallel**  
Total processes: 10  
HTTP processes: 2  
**HTTP request delay**  
Request delay: High

Bruteforce option Minimal

Cancel Previous Finish

## Option Profile View Dialog

Just like the review step, the *Scan Parameters* step in option profile View dialog will display the values selected for the SmartScan options.

- If user enabled the option:

Option Profile View: aaat

View Mode

Profile Details

Scan Parameters

Search Criteria

Comments

Action Log

Please define how the scan will perform

General Settings

Form SubmissionPost & Get

Maximum crawl requests (the total number of links and forms to follow)300

User Agent—

Request Parameter SetTest Paramset

Document TypeIgnore common binary files based on file extensions.

SmartScan Support

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

SmartScan SupportEnabled

SmartScan Depth5

Performance Settings

Close

Save As..Edit

- If user left the option disabled:

Option Profile View: 5links - limited

View Mode

Profile Details

Scan Parameters

Search Criteria

Comments

Action Log

Please define how the scan will perform

Form SubmissionPost & Get

Maximum crawl requests (the total number of links and forms to follow)5

User Agent—

Request Parameter SetInitial Parameters

Document TypeIgnore common binary files based on file extensions.

SmartScan Support

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

SmartScan SupportDisabled

Performance Settings

Scan IntensityLow

Processes to run in parallel  
Total processes: 10

Close

Save As..Edit

## Option Profile Edit Dialog

The same step will be available, but this time with the *Enable SmartScan Support* checkbox checked if the option has been previously enabled. In this case, the *SmartScan Depth* setting will also be displayed, with proper value already set for the profile.

The image shows a screenshot of the 'Option Profile Edit' dialog for a profile named 'aat'. The dialog has a blue header bar with the title 'Option Profile Edit: aat' and a 'Turn help tips: On | Off' button with a 'Launch help' link and a close icon. On the left is a sidebar with a list of sections: 'Edit Mode' (selected), 'Profile Details', 'Scan Parameters' (highlighted in blue), 'Search Criteria', 'Comments', and 'Action Log'. The main content area is titled 'Please define how the scan will perform'. It contains several settings: 'Maximum crawl requests\*' with a value of 300; 'User Agent' with a text box containing 'Example: Mozilla/4.04 (X11; I; SunOS 5.4 sun4m)'; 'Request Parameter Set\*' with a dropdown menu showing 'Test Paramset (Default)' and buttons for 'View' and 'Create'; 'Document Type' with a checked checkbox for 'Ignore common binary files based on file extensions.'; 'SmartScan Support' section with a description, a checked checkbox for 'Enable SmartScan Support', and a 'SmartScan Depth\*' value of 5; and a 'Behavior Settings' section. At the bottom are three buttons: 'Cancel', 'Save As..', and 'Save'.

## Option Profile Save As

The SmartScan settings will be also copied over when a user performs a Save As action from the datalist or from the option profile view/edit dialogs.

## Existing Profiles

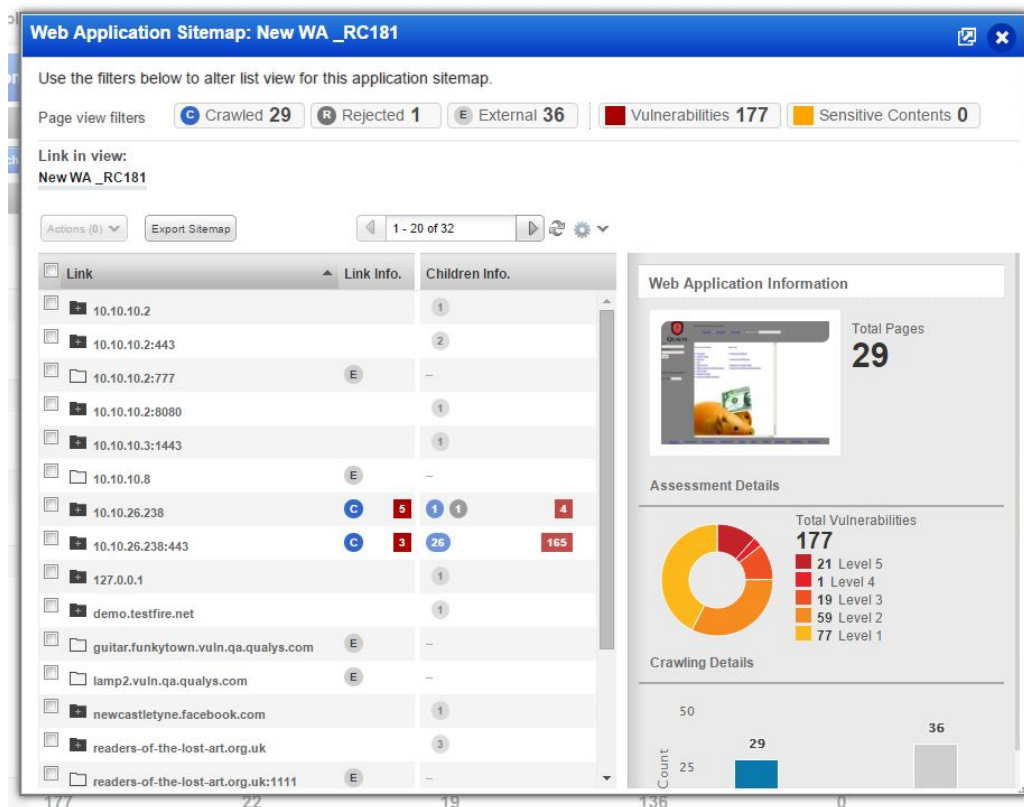
All existing profiles will have the *Enable SmartScan Support* option disabled by default. The *SmartScan Depth* value will be set to 5.

## Enhanced Sitemap Reporting

WAS 4.6 now allows the customer the ability to download all URLs for a site via the Sitemap feature and not have to navigate to each branch of the sitemap individually.

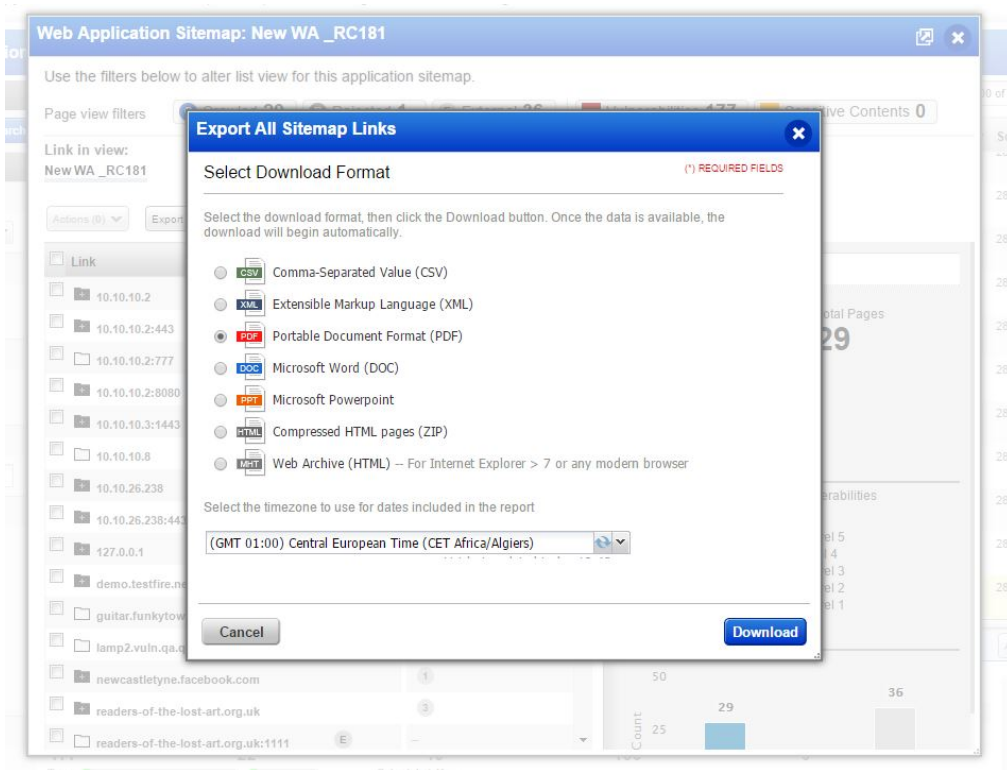
### Web Application / Scan Sitemap Dialog

The dialog used to display the sitemap for scans and web applications will have a new Export Sitemap button now always enabled.



Upon clicking, an Export Sitemap Links dialog will be displayed, proposing to the user the format to be used to download the sitemap links.

The format and timezone fields selected by default will depend on user preferences as set in their profile.



Format of the downloaded contents is the same when downloading current page, the only difference is that this time all the links will be downloaded with their absolute path.

Columns will therefore be:

Columns	Description
Link	Link absolute URL
Status	<b>CRAWLED, REJECTED, EXTERNAL.</b> There may be no status for links where vulns have been detected, but these links have not been marked as crawled.
# Sensitive Contents	Number of sensitive contents found in this link
# Vulnerabilities	Number of vulnerabilities found in this link
External links	Number of external links found "under" this link
Crawled links	Number of crawled links found "under" this link
Rejected links	Number of rejected links found "under" this link
Links Sensitive Contents	Number of sensitive contents found under this link
Links Vulnerabilities	Number of vulnerabilities found under this link

## Enhanced Option Profile Scope Selection

When creating or editing an Option Profile, under Search Criteria -> Detection Scope; if we choose "Custom" previously an error message implied that a user must enter an "include" search list. You could have still entered an "exclude" search list to exclude only, but the location of this error message was confusing. We have corrected and enhanced this functionality.

### Option Profile Dialog

The Search Criteria > Detection Scope section has been updated as follows:

- Text has been added to introduce to user the option.
- A Detection component has replaced the “*focus the scan to specific vulnerabilities*”, and proposes the options Complete vs. Custom as a drop down element instead of radio buttons.

In Creation mode, the option selected by default is Complete.

The screenshot shows the 'Option Profile Creation' dialog box, specifically 'Step 3 of 5: Search Criteria'. The dialog has a blue header bar with the title 'Option Profile Creation' and a close button. On the left, a vertical sidebar shows the progress of the five steps: 1. Profile Details, 2. Scan Parameters, 3. Search Criteria (current step), 4. Comments, and 5. Review And Confirm. The main area is titled 'Please define what you want to scan for'. Under the 'Detection Scope' section, there is a text box with a red asterisk and the text '(\*) REQUIRED FIELDS'. Below this, a description states: 'Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.' The 'Detection\*' dropdown menu is currently set to 'Complete'. Below this is the 'Sensitive Content' section, which contains three checkboxes: 'Credit Card Numbers', 'Social Security Numbers (US)', and 'Custom Contents', all of which are unchecked. At the bottom of the dialog, there are three buttons: 'Cancel', 'Previous', and 'Continue'.

In both creation and edit mode, when the user selects Custom, the following elements are displayed below the Detection component:

- The search lists to include
- The search lists to exclude
- An additional text message above the search lists to exclude, that explains how the excluded search lists will be used



**Option Profile Creation** Turn help tips: On | Off Launch help

**Step 3 of 5**

1 Profile Details ✓  
2 Scan Parameters ✓  
3 Search Criteria ✓  
4 Comments  
5 Review And Confirm

Please define what you want to scan for

**Detection Scope** (\*) REQUIRED FIELDS

Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.

Detection\* Custom

Include vulnerabilities associated in search lists below. Add search list | Create static list | Create dynamic list

Select search lists defining the list of QIDs the engine shall not try to detect. This list will be deducted from the list of included QIDs, or from the complete list of QIDs if no search lists were specified as included search lists.

Exclude vulnerabilities associated in search lists below. Add search list | Create static list | Create dynamic list

**Sensitive Content**

☐ Credit Card Numbers

Cancel Previous Continue

If the user clicks the Next button, the validation is performed, and if no search lists have been selected:

- The 2 search lists components are highlighted in red
- An error message is displayed on top of search lists to include component to request user to specify at least one search list

**Option Profile Edit: WASUI-6330** Turn help tips: On | Off Launch help

**Edit Mode**

Profile Details >  
Scan Parameters >  
Search Criteria ⚠  
Comments >  
Action Log >

Please define what you want to scan for

**Detection Scope** (\*) REQUIRED FIELDS

Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.

Detection\* Custom

**At least one search list or excluded search list must be selected.**

Include vulnerabilities associated in search lists below. Add search list | Create static list | Create dynamic list

(No Search List selected)

Select search lists defining the list of QIDs the engine shall not try to detect. This list will be deducted from the list of included QIDs, or from the complete list of QIDs if no search lists were specified as included search lists.

Exclude vulnerabilities associated in search lists below. Add search list | Create static list | Create dynamic list

(No Search List selected)

**Sensitive Content**

☐ Credit Card Numbers

Cancel Save As.. Save

Comment: No comment has been yet posted.

By selecting at least one search list, the error message is removed and the two search lists are be marked as valid.

Option Profile Edit: WASUI-6330

Turn help tips: On | Off Launch help

Edit Mode

Profile Details

Scan Parameters

Search Criteria

Comments

Action Log

Please define what you want to scan for

Detection Scope

(\*) REQUIRED FIELDS

Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.

Detection\* Custom

Include vulnerabilities associated in search lists below. Add search list Create static list Create dynamic list

Compliance

Dynamic

Tue Sep 08 2015

View

Remove

Select search lists defining the list of QIDs the engine shall not try to detect. This list will be deducted from the list of included QIDs, or from the complete list of QIDs if no search lists were specified as included search lists.

Exclude vulnerabilities associated in search lists below. Add search list Create static list Create dynamic list

(No Search List selected)

Sensitive Content

☐ Credit Card Numbers

Cancel

Save As.. Save