

## Qualys Cloud Suite 2.32.2

Version 2.32.2

April 23, 2018

Here's what's new in Qualys Cloud Suite 2.32.2!

### Web Application Scanning

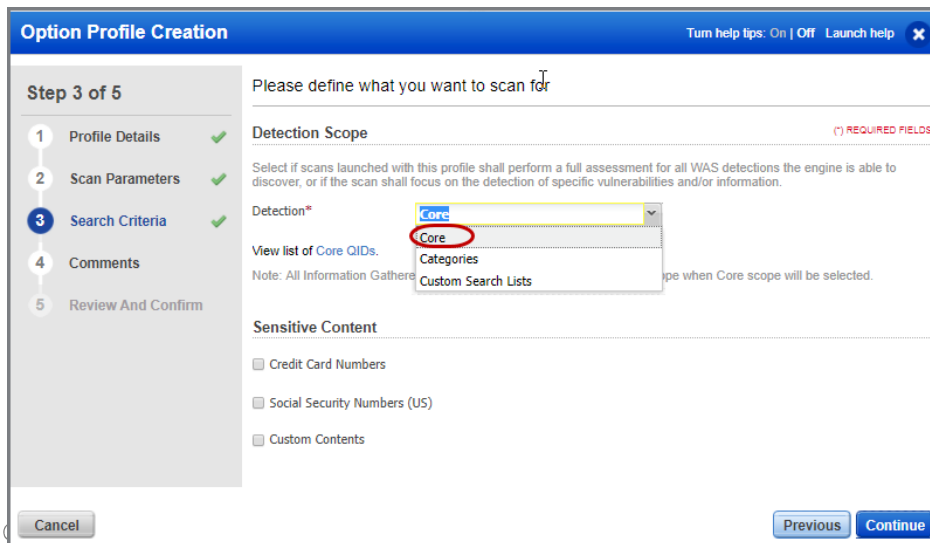
#### Changed Detection Scope from Complete to Core

We have now changed the detection scope from Complete to Core when you configure option profile for your WAS scan.

Up to now, the default detection scope in the WAS option profile has been 'Complete', meaning that all vulnerability detections (QIDs) were included in the scan. The default detection scope has now changed to 'Core'. At this point it's just a name change. All QIDs that were in 'Complete' are also in 'Core'.

The name has been changed to allow for more flexibility going forward. When a new WAS detection was introduced in the past - no matter how obscure or time consuming - the QID was automatically included in all scans that used the default detection scope. Going forward, the new QID may or may not be included the 'Core' detection scope. The inclusion of the QID will depend on the nature of the new detection.

Keep in mind you can still run scans with complete detection scope if desired. The functionality still exists. Simply use a dynamic search list. From the Search Criteria tab, select all checkboxes under Confirmed Severity, Potential Severity, and Information Severity. In your WAS option profile, then select "Custom Search Lists" for the detection scope and select that dynamic search list.



Go to Scans > Option Profile > New and when you define the detection scope in search criteria for the WAS scan, you will notice we have changed the label to Core. All the existing option profiles defined with detection scope as Complete will also be renamed to Core.

Note that your existing scans that defined the option profile with Complete detection scope will not be impacted by the label change and will retain detection scope as Complete.



## New Support for Cross-Account Role Authentication for EC2 Connectors

Qualys now supports the creation of EC2 connectors using a cross-account role. This allows you to grant Qualys access to your AWS EC2 instances without sharing your AWS security credentials. Qualys will access your AWS EC2 instances by assuming the IAM role that you create in your AWS account. This eliminates the overhead of management of IAM user keys in your Qualys subscription.

### Highlights

- Create new connectors using cross-account role authentication
- Upgrade existing connectors to use cross-account role authentication
- Support for key-based connectors will be discontinued after 180 days
- Automate creation using CloudFormation Template, downloadable from the UI
- REST API support to programmatically set up and update EC2 connectors
- Create only one connector for each unique AWS account. It's recommended that you merge multiple EC2 connectors into one by removing duplicate connectors before you upgrade to the cross-account role.

Learn more, refer to the [community doc](#) or follow [Securing Amazon Web Services with Qualys](#)

### AV Issue Addressed

Fixed an issue where the counts for vulnerabilities in Dashboard widgets did not correspond to list counts shown when the user clicks the widget to drill down to view details.