Qualys.

Qualys Cloud Platform v2.x

Release Notes

Version 2.35.1
January 11, 2019

Here's what's new in Qualys Cloud Suite 2.35.1!

AV **AssetView**

Support for Azure Connectors

WAS **Web Application Scanning**

Configuring Password Visibility in Authentication Details

New Option for Custom Scan Performance

Qualys Cloud Platform 2.35.1 brings you many more Improvements and updates! Learn more

AV AssetView

Support for Azure Connectors

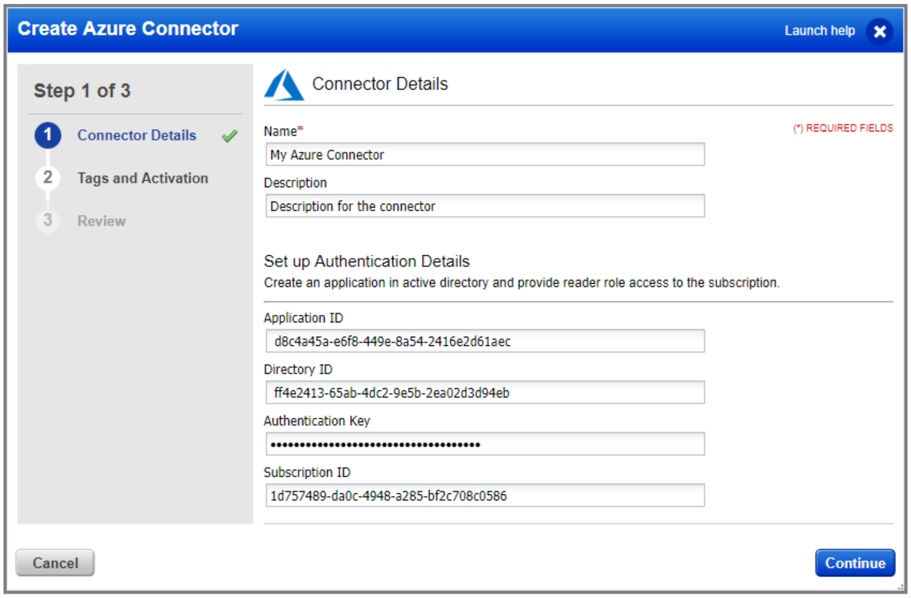
You can now configure Azure connectors for scanning Microsoft Azure resources for security issues using the Qualys Cloud Platform. Our connector wizard walks you through the steps. It just takes a couple of minutes.

Pre-requisites:

Before you create an Azure connector, ensure that you have the following permissions:
- Assign Azure Active Directory permissions to register an application with your Azure Active Directory.
- Check Azure Subscription permissions to assign the application to a role in your Azure subscription.

How to configure Azure connectors

Go to the Connectors > Azure tab, select Create Azure Connector and our wizard will walk you through the steps.



Connector Details

(*) REQUIRED FIELDS

Name*: My Azure Connector

Description: Description for the connector

Set up Authentication Details

Create an application in active directory and provide reader role access to the subscription.

Application ID: d8c4a45a-e6f8-449e-8a54-2416e2d61aec

Directory ID: ff4e2413-65ab-4dc2-9e5b-2ea02d3d94eb

Authentication Key: ••••••••••••••••••••••••••••••••••••

Subscription ID: 1d757489-da0c-4948-a285-bf2c708c0586

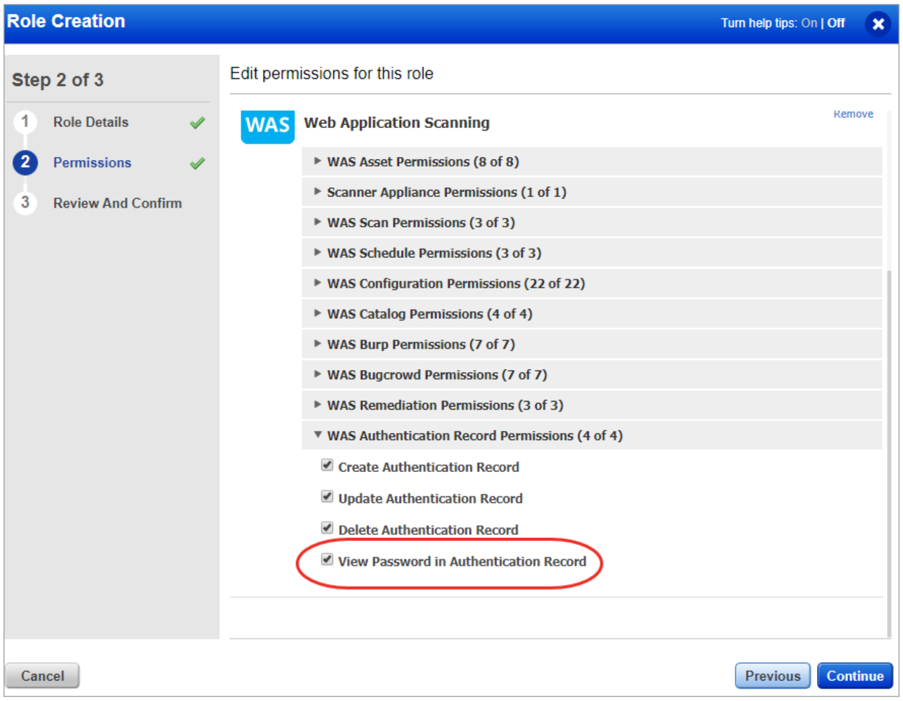
Provide a few connector details.
(1) Enter a name and description (optional) for your connector.
(2) Set up the authentication details and copy/paste the authentication details into the form.

Add the relevant tags. We recommend you create at least one generic asset tag (for example Azure) and have the connector automatically apply that tag to all imported assets. You can add more tags to your Azure assets based upon discovered Azure metadata.
(3) Click Finish.

That's it! The connector will establish a connection with Microsoft Azure to start discovering resources from each region.

Configuring Password Visibility in Authentication Details

We have now introduced a new permission that allows you to enable or disable visibility of password when you fetch authentication record details. Enabling or disabling the View Password in Authentication Record permission decides if the password should be visible or masked when the user fetches the authentication record details.



Role Creation

Turn help tips: On | Off

Step 2 of 3

1 Role Details ✓

2 Permissions ✓

3 Review And Confirm

Edit permissions for this role

WAS Web Application Scanning

Remove

- WAS Asset Permissions (8 of 8)
- Scanner Appliance Permissions (1 of 1)
- WAS Scan Permissions (3 of 3)
- WAS Schedule Permissions (3 of 3)
- WAS Configuration Permissions (22 of 22)
- WAS Catalog Permissions (4 of 4)
- WAS Burp Permissions (7 of 7)
- WAS Bugcrowd Permissions (7 of 7)
- WAS Remediation Permissions (3 of 3)
- WAS Authentication Record Permissions (4 of 4)

☑ Create Authentication Record

☑ Update Authentication Record

☑ Delete Authentication Record

☑ View Password in Authentication Record

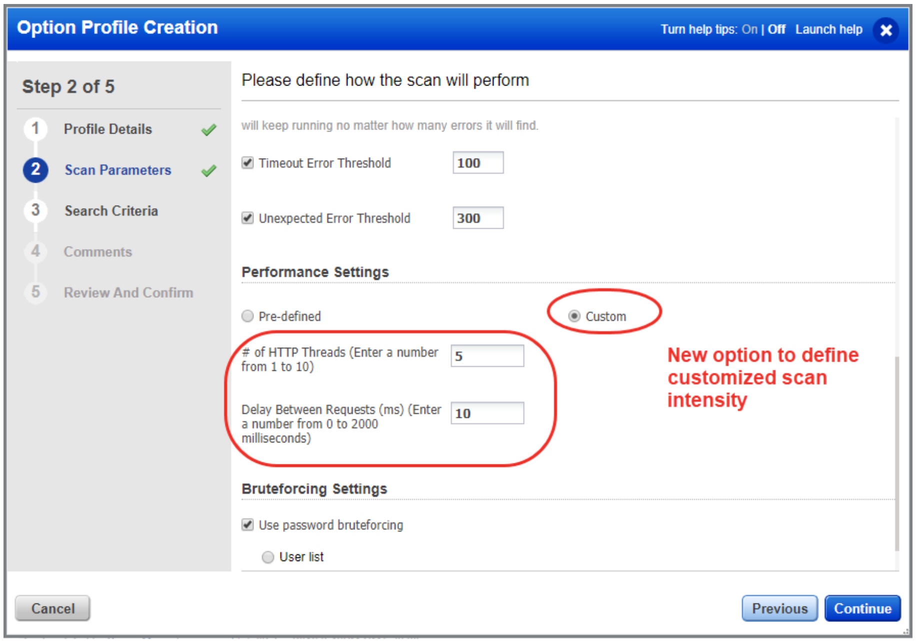
Go to Administration > Role Management. You'll find roles and their related permissions in the Role Management section. Select the role for which you want to configure the permission and select Edit from the Quick Actions menu.

The new permission is added to the WAS Authentication Record Permissions group.

You need to disable the "View Password in Authentication Record" and "View/download Selenium Script sensitive contents" (Web Asset) permissions to mask the password in the API response.

New Option for Custom Scan Performance

You can now configure and control the scan performance by defining the custom settings for scan performance in Option Profile settings. We have added Custom option that allows you to configure the scan performance settings such as number of threads to be used to scan each host and the delay between requests.



Please define how the scan will perform

will keep running no matter how many errors it will find.

☑ Timeout Error Threshold: 100

☑ Unexpected Error Threshold: 300

Performance Settings

○ Pre-defined ● Custom

# of HTTP Threads (Enter a number from 1 to 10): 5

Delay Between Requests (ms) (Enter a number from 0 to 2000 milliseconds): 10

New option to define customized scan intensity

Bruteforcing Settings

☑ Use password bruteforcing

○ User list

Go to Scans > Option Profiles and configure a new option profile or edit an existing option profile.

The Performance Settings in Scan Parameters pane display the new options.

Choose Custom option to define your own settings.

# of HTTP Threads: Define number of threads to be used to scan each host.

Delay Between Requests: Define duration of delay introduced by WAS in between the scanning engine requests sent to the applications server.

When you launch a scan, select the configured option profile and the scan performance automatically reflects the configured setting.

Issues addressed in this release

Qualys Cloud Platform 2.35.1 brings you many more improvements and updates.

CA Cloud Agent

- User-facing Change: New permissions are now available for limiting the module access for CA using UI or API.
- Fixed an issue where the user could not download the agents report from the agents list UI, when the user had more than 55K agents.
- Fixed an issue where the uninstall agent API failed when the agent had an invalid UUID.

WAS Web Application Scanning

- Users can now successfully ignore vulnerabilities and re-activate them manually.
- Ignored vulnerability belonging to Burp/Bugcrowd are now getting reactivated as per the time set by an user as expected.
- Now the days/date range set by user are visible in the UI for Burp/Bugcrowd detections.
- On the Detections list now the Ignore option is enabled for Bugcrowd on the Quick Action menu and Actions menu.
- We have fixed an issue where now we display correct vulnerability status for all findings after each scan.