



Qualys Custom Assessment and Remediation

Release Notes

Version 1.6

January 25, 2023

Here's what's new in Qualys Custom Assessment and Remediation 1.6!

[Integration with GitHub for Script Creation](#)

[Ability to Re-run Script Jobs](#)

[All or Any Tags in Script Execution](#)

[New Public APIs](#)

Custom Assessment and Remediation 1.6 brings you some improvements and updates! [Learn more](#)

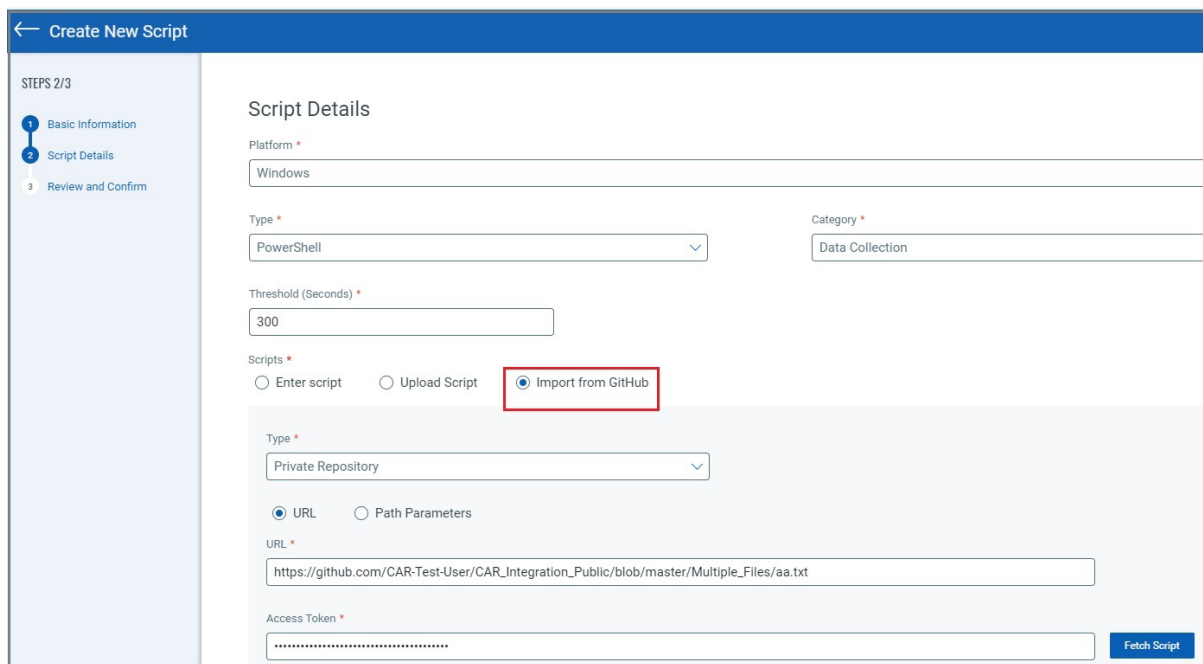
New Features

Integration with GitHub for Script Creation

With this release, CAR integrates with GitHub for an enhanced script creation workflow. Apart from the options to manually enter or select scripts from your local drives, CAR now includes a new option to leverage the public and private repositories in GitHub.

When you create a script, you can select the option to import a script from GitHub, specify whether you want to import from a private repository or a public repository, and then provide the link to the GitHub repository from which to import the script.

Note: You must provide an access token if you choose a private repository. It is recommended that you provide an access token that has no expiration limit.



The screenshot shows the 'Create New Script' form in the Qualys CAR interface. The form is divided into three steps: 1. Basic Information, 2. Script Details (current step), and 3. Review and Confirm. In the 'Script Details' section, the 'Platform' is set to 'Windows', the 'Type' is 'PowerShell', and the 'Category' is 'Data Collection'. The 'Threshold (Seconds)' is set to 300. Under the 'Scripts' section, the 'Import from GitHub' option is selected and highlighted with a red box. Below this, the 'Type' is set to 'Private Repository', and the 'URL' is 'https://github.com/CAR-Test-User/CAR_Integration_Public/blob/master/Multiple_Files/aa.txt'. The 'Access Token' field is empty, and a 'Fetch Script' button is visible at the bottom right.

You can also choose to auto-sync with GitHub, which syncs your scripts automatically with the specified GitHub repository every four hours. Thus, in case of any change that's made in the CAR scripts in GitHub, your scripts are automatically updated on the Qualys platform.

Alternatively, you can also choose to manually initiate a sync with GitHub as per your requirement.

The API Rate limit is 60 requests per hour if you use API calls for public GitHub repositories (configured without access token) and 5000 per hour for private GitHub repositories (configured with access token). These rate limits are as per the GitHub API documentation.

For more information, refer to [Resources in the REST API](#).

Ability to Re-run Script Jobs

You can now re-run script jobs that have already been executed on assets. This new capability enables you to re-assess your assets after making necessary changes in a script. When you re-run a job, the script is run on all the assets that are included in the previously run jobs.

| TIME | JOB NAME | | PLATFORM | SEVERITY | SCRIPT CATEGORY |
|---|---------------------------------|-------------------------|-----------------------|--|-----------------|
| 09:00:41 AM | | | PowerShell | | |
| <input checked="" type="checkbox"/> 15 hours ago 05:30:04 AM | Windowspython-1674000004 | Quick Actions | WINDOWS Python | ■ ■ ■ ■ ■ | Remediation |
| 15 hours ago 05:30:02 AM | Auto_script | View Details | WINDOWS PowerShell | ■ ■ ■ ■ ■ | Data Backup |
| 19 hours ago 01:30:00 AM | Auto_script_22062022 | Delete | WINDOWS PowerShell | ■ ■ ■ ■ ■ | Data Backup |
| 21 hours ago 11:30:03 PM | Windowspython | View Schedule Details | WINDOWS Python | ■ ■ ■ ■ ■ | Remediation |
| a day ago 10:29:58 PM | Auto_script_13092022 | Re-run on all assets | WINDOWS Python | ■ ■ ■ ■ ■ | Data Backup |
| | | Re-run on failed assets | | | |

You also have the option to run the script only on the assets on which the script job failed. This option is available only if the script fails on some or all of the assets.

All or Any Tags for Script Execution

This release enables you to choose any or all the asset tags for script execution to define the scope of your script.

Select Assets

Select the assets you want this job to deploy patches on

Include the Assets
+

Add the assets on which you want to execute this script.

Include host having the selected tags
Any
+

Script execution will occur if host has 'any' of the selected tags

All
Any

☐ Exclude host for the tags

Cancel Execute Script

If you select **All**, the script is executed on the hosts that are included in all of the selected tags. Whereas if you select **Any**, the script is executed on the hosts that are included in any one of the selected tags.

Example: You want to run a script and you have selected the asset tags T1, T2, and T3 to define the scope of the script execution. If you select **Any**, the script runs on the hosts that are a part of any of the tags – T1, or T2, or T3. If you select **All**, the script runs only on those hosts that are included in all of the selected tags – T1, T2, and T3.

New Public APIs

This release adds the following new public APIs:

- Count number of scripts
- Count number of jobs
- Count number of asset jobs
- Count number of schedules
- Count number of assets
- Fetch jobs by script name or script ID

- Fetch asset jobs details for a given job name or job ID

Refer to the [CAR API Release Notes](#) for more information.

Known Issue

CAR does not support UTF-16 character set. The probability of such characters being in executable code is less. It is recommended that you do not use special characters that are beyond UTF-8 character range.

Issues Addressed

- Earlier, CAR APIs could fetch less than 10,000 (9999 jobs or asset jobs) per page. Starting this release, you can use the 'searchAfter' parameter in order to fetch more than 10,000 records of assets, jobs, and asset jobs.

For this parameter to function accurately, use the 'sort' parameter to sort assets, script jobs, or asset jobs by using a filter that has unique values such as ID or name. Each asset/job/asset job is returned with an identifier called 'sortValue'. In the subsequent API request, to fetch records beyond the current page size, provide the sortValue of an asset, job, or asset job to the searchAfter parameter to fetch records after the specific ID.

The 'searchAfter' parameter is supported for the following APIs:

- sm/v2/jobs/search
- sm/v2/assetjobs/search
- sm/v1/assets/search

To understand this better, let's consider this example:

You have 15000 jobs in your account. The first API request will only return 9999 jobs. To get jobs beyond 9999, in a subsequent API request, provide the sortValue of the 9999th job in the searchAfter parameter. The second API request will fetch the remaining job starting from the 10000th job.

For better performance, it is recommended that you use smaller page sizes of 1000 to 2000 records.

- Downloading an asset job report from the asset jobs page used to fail with the "Gateway Timeout error" message. This issue has been fixed and now the correct asset job details are fetched when a report is downloaded for asset jobs.