



Qualys SaaS Detection and Response (SaaS DR)

Release Notes

Version 1.4.0

Aug 17, 2021

Here's what's new in SaaS Detection and Response 1.4.0!

[CIS Microsoft 365 Foundations Benchmark v1.3](#)

[Hardening Controls for Microsoft 365 to Defend Against UNC2452](#)

[Deep Coverage of Services on Microsoft 365](#)

[Events sub-tab in the Monitor Tab](#)

[Renaming G Suite to Google Workspace](#)

[Re-Authenticate to SaaS Application](#)

[Change in Control IDs](#)

CIS Microsoft 365 Foundations Benchmark v1.3

SaaS DR now supports the latest version of the CIS Microsoft 365 Foundation Benchmark. With the updated certified CIS policy, your Microsoft 365 subscription can be assessed for compliance with respect to the updated checks in the CIS policy.

Hardening Controls for Microsoft 365 to Defend Against UNC2452

In December 2020, FireEye uncovered and publicly disclosed a widespread campaign conducted by the threat group that is tracked as UNC2452. In some cases, the attacker compromised on-premises networks to gain unauthorized access to the victim's Microsoft 365 environment. In this release, we have included controls for mitigating this type of attacks. These controls are included in 'Microsoft Office 365 Best Practices' policy.

Deep Coverage of Services on Microsoft 365

With this release, Azure AD, Exchange Online, OneDrive and Teams services on Microsoft 365 can be assessed for compliance by using SaaS DR.

Events sub-tab in the Monitor Tab

Qualys SaaS DR 1.4.0 re-introduces the **Events** sub-tab under the **Monitor** tab with enhanced performance.

The Events sub-tab lists expected activities, authorized activities and activities that might have potential indication of unexpected behavior.

You can filter events based on their Type or Category from the left navigation pane.

QUALYS GUARD EXPRESS SUITE

SaaS Detection and Response

DASHBOARD DIRECTORY RESOURCES POLICY **MONITOR** CONFIGURATION

Monitor Controls **Events**

1.13K Total Events

Search... Last 30 Days

1 - 50 of 1128

NAME	CONNECTOR	TIME	ACTOR	IP	RESULT
UserLoggedIn	o365 events	Fri, 05 Mar 2021 05:20:37 GMT	testprod@qualyssscsmdev.com	137.117.100.130	SUCCESS
UserLoggedIn	o365 events	Fri, 05 Mar 2021 05:20:31 GMT	testprod@qualyssscsmdev.com	137.117.100.130	SUCCESS
UserLoggedIn	o365 events	Fri, 05 Mar 2021 05:20:23 GMT	testprod@qualyssscsmdev.com	137.117.101.166	SUCCESS
UserLoggedIn	o365 events	Fri, 05 Mar 2021 04:52:37 GMT	mfausertest@qualyssscsmdev.c	49.37.158.213	SUCCESS
UserLoggedIn	o365 events	Thu, 04 Mar 2021 17:44:11 GMT	testprod@qualyssscsmdev.com	137.117.100.130	SUCCESS
UserLoggedIn	o365 events	Thu, 04 Mar 2021 17:43:59 GMT	testprod@qualyssscsmdev.com	137.117.103.80	SUCCESS
UserLoggedIn	o365 events	Thu, 04 Mar 2021 15:42:01 GMT	testprod@qualyssscsmdev.com	137.117.103.80	SUCCESS

TYPE

- AADPowerShell... 537
- SettingsChange 501
- PermissionChange 56
- PowerShellMailb... 34

CATEGORY

- PowerShell 537
- ServicePrincipal 458
- User 54
- Application 41

Detail Page of User Activity Event

Qualys SaaS SDR 1.4.0 enables users to view the details of the user activity events. Under the **Events** sub-tab, click the event to view the details in JSON format.

The screenshot displays the Qualys Guard Express Suite interface. The main dashboard shows 263 Total Events. A table lists several 'UserLoggedIn' events from a '0365 p26 QA' connector on July 7, 2021. A detailed view of one event is shown on the right, including a description and the following JSON event data:

```
{
  "customerId": "146fb529-650e-dc6f-82f9-b7f2c761b97b",
  "connector": {
    "id": "1230",
    "type": "OFFICE365"
  },
  "sourceId": "e3b7acb2-c0bb-4569-8b0d-2f5746c14902",
  "name": "UserLoggedIn",
  "type": "AADPowerShellLogin",
  "category": "PowerShell",
  "serviceType": "AzureActiveDirectory",
  "dateTime": "2021-07-07T11:54:42Z",
  "actor": {
    "id": "1fbca7c7-5bea-4322-a2d9-21b9663d63b1",
    "email": "pcuser@QualysSSCMSDev.com"
  },
  "origin": {
    "ip": "103.216.98.78",
    "userAgent": "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.0; Win64; x64; Trident/4.0; .NET4.0E; .NET CLR 3.5.30729; .NET CLR 3.0.30729.54; .NET CLR 2.0.50727.30363)"
  }
}
```

Renaming G Suite to Google Workspace

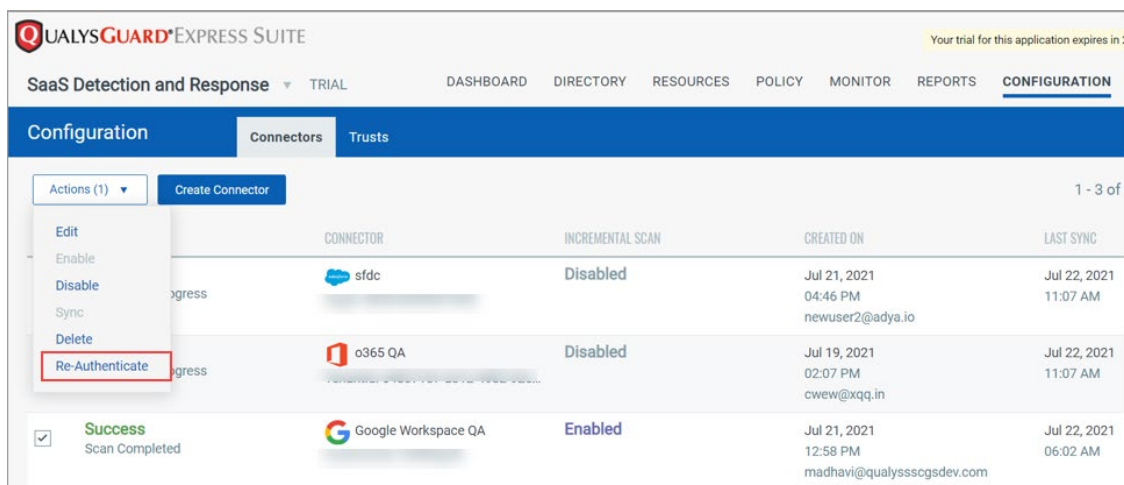
After Google's official announcement, G Suite SaaS application in Qualys SaaS SDR is updated to **Google Workspace** SaaS application.

Re-Authenticate to SaaS Application

You might need to re-authenticate to the SaaS applications in the following scenarios:

1. You have upgraded to a new version of SaaS DR and cannot find the existing connector on the application UI.
2. A new scope is added.
3. Change in the password of SaaS login that was used to create a connector.
4. Navigate to **Configuration** > **Connectors** tab and select the connector you want to re-authenticate.
5. Go to **Actions** drop-down menu and click **Re-Authenticate**.
Re-Authenticate option will be enabled for connectors in any state except Pending state.

Note: You can select only one connector at a time.



The screenshot shows the Qualys Guard Express Suite interface. The top navigation bar includes 'SaaS Detection and Response', 'TRIAL', 'DASHBOARD', 'DIRECTORY', 'RESOURCES', 'POLICY', 'MONITOR', 'REPORTS', and 'CONFIGURATION'. The 'CONFIGURATION' tab is active, and the 'Connectors' sub-tab is selected. A table lists connectors with columns for 'CONNECTOR', 'INCREMENTAL SCAN', 'CREATED ON', and 'LAST SYNC'. A dropdown menu is open over the table, showing options: 'Edit', 'Enable', 'Disable', 'Sync', 'Delete', and 'Re-Authenticate'. The 'Re-Authenticate' option is highlighted with a red box. Below the table, a success message 'Success Scan Completed' is visible.

CONNECTOR	INCREMENTAL SCAN	CREATED ON	LAST SYNC
sfdc	Disabled	Jul 21, 2021 04:46 PM newuser2@adya.io	Jul 22, 2021 11:07 AM
o365 QA	Disabled	Jul 19, 2021 02:07 PM cwev@xqq.in	Jul 22, 2021 11:07 AM
Google Workspace QA	Enabled	Jul 21, 2021 12:58 PM madhavi@qualyscgsgsdev.com	Jul 22, 2021 06:02 AM

If the re-authentication attempt fails, the Status column displays an error that says "Authentication Failure". Upon a successful authentication, sync is initiated and the newly authorized connector is made available on the UI.

Change in Control IDs

We have changed identifiers of certain controls in the SaaS DR controls library.

For example, 9036, 9037, 9038, 9018, 9012, 9007 control IDs are replaced by 70123, 70124, 70125, 70105, 70100, 70095 respectively, to mention a few.