



# **SaaS Detection and Response**

Getting Started Guide  
Version - 1.8.0

February 27, 2024

Copyright 2024 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.  
919 E Hillsdale Blvd  
4th Floor  
Foster City, CA 94404  
1 (650) 801 6100



# Table of Contents

<b>About this Guide .....</b>	<b>4</b>
About Qualys .....	4
Qualys Support .....	4
<b>SaaS Detection and Response Overview .....</b>	<b>5</b>
How to get started .....	5
Home .....	6
<b>Create Connector.....</b>	<b>7</b>
Connector Actions .....	8
Connector Status .....	8
<b>Inventory Details .....</b>	<b>9</b>
View Directory .....	9
View Resources .....	10
<b>Policy .....</b>	<b>11</b>
Enable a Policy .....	11
Manage Policies .....	12
Control Library .....	13
Custom Policies .....	13
Manage Custom Policies .....	14
<b>Monitor SaaS Applications .....</b>	<b>15</b>
Monitor Compliance Posture .....	16
Events .....	17
<b>Security Misconfigurations .....</b>	<b>18</b>
Remediation for Office 365 .....	18
Creating a Remediation Job .....	18
<b>Response.....</b>	<b>22</b>
<b>Reports .....</b>	<b>24</b>
<b>Trusted Domains and Applications .....</b>	<b>26</b>
Add Domains and Applications as Trusted .....	26
Remove Domains and Applications from the Trusted List .....	26
<b>Customizable Dynamic Dashboard .....</b>	<b>27</b>

# About this Guide

Welcome to Qualys SaaS Detection and Response (SaaS DR)! We'll help you get acquainted with the Qualys solution to help enterprises with the security and compliance of their SaaS applications using the Qualys Cloud Security Platform.

## About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations, including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit [www.qualys.com](http://www.qualys.com)

## Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at [www.qualys.com/support/](http://www.qualys.com/support/).

# SaaS Detection and Response Overview

Qualys SaaS Detection and Response (SaaS DR) expands the capabilities of the Qualys Cloud Platform to help enterprises with the security and compliance of their SaaS applications. It will provide a single console for IT admins to connect to their critical SaaS applications, manage them centrally, secure data on these critical cloud apps, maintain compliance and manage costs. It is a tool for IT admins to manage SaaS sprawl effectively.

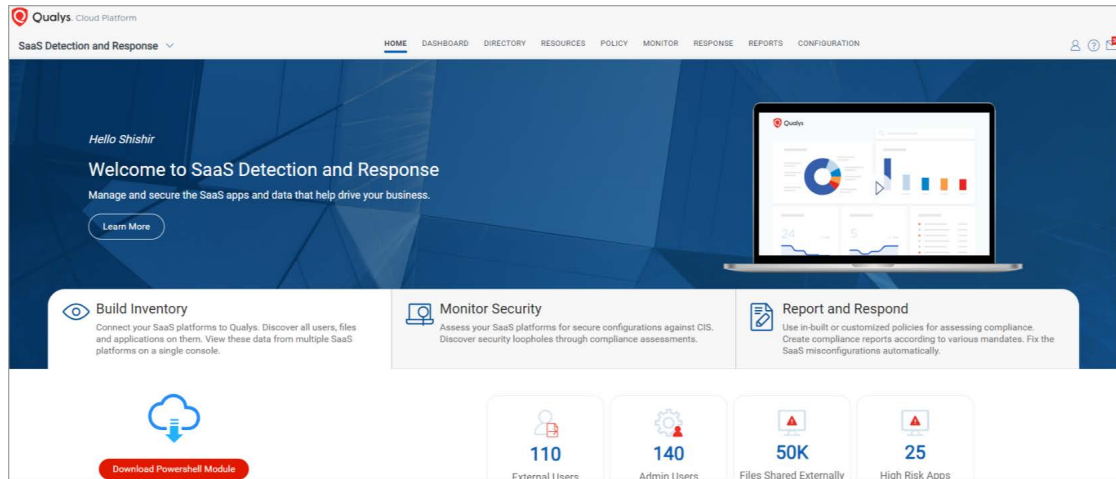
## Benefits of SaaS DR

- Provide a single console for IT admins to centrally secure their data no matter where it is
- Gets a consolidated view of external users who have access to internal documents and internal users that are sharing documents externally
- Get visibility into documents that are exposed and take steps to make them private
- Get visibility into apps that have given access to sensitive data and take steps to alert and block them
- Understand the compliance posture of your critical SaaS applications to ensure that you pass industry-standard benchmarks. Currently, we support the CIS Microsoft 365 Foundations Benchmark v3.0.0

## How to get started

With SaaS DR, you'll view all your resources, like files and folders, third-party applications, and meetings identified from the scanned SaaS applications, view the policy controls to monitor your compliance posture, and perform different actions on the existing reports.

## Home



## Configure a Connector

Just set up a connector with your SaaS applications, and that's it! We'll start discovering important information about your SaaS applications that will help you view and monitor the data on these applications.

## Build Inventory

View all the Users and User Groups in your organization. Also, view all your resources, like files and folders, third-party applications, and meetings identified from the scanned SaaS applications.

## Monitor Compliance

Enable and run the CIS Microsoft 365 Foundations Benchmark v3.0.0 policy for your connectors. View the policy controls to monitor your compliance posture.

## Fix Security Misconfigurations

Remediate the controls if any of the controls have a failed status for security posture for Office 365 subscriptions.

## Report and Respond

Perform different actions on the existing reports.

## Search your Inventory

Use our guided search capabilities and craft advanced queries combining multiple criteria to search all your resources and directories.

# Create Connector

Start by creating a connector to your SaaS application.

Supported connectors for this release:

- Microsoft Office 365

**Note:** Qualys SaaS DR supports Azure AD, Sharepoint, Onedrive, ExchangeOnline, Teams services for Microsoft Office 365.

- Salesforce (SFDC)

- Zoom

- Google Workspace

- Slack

- Dropbox

## Pre-requisites

- You must install Powershell Module for compliance assessment of Microsoft Office 365.

For more information on installing Powershell Module, click [here](#).

## Let's get started!

Choose SaaS Detection and Response (SaaS DR) from the app picker. You'll need the SaaS application credentials to create the connector.

The steps to create a connector depend on the SaaS application for which you want to create the connector. Refer to the [Create Connectors](#) section of the Online Help for information on configuring your connector.

The newly created connector appears in the **Configurations > Connectors** list. Here you can check the status and other details of the connector.

## You're ready!

Once the application is connected, a scan is initiated to pull metadata from the application. This step may take some time to complete based on the number of resources to be cataloged in your application.

## Connector Actions

Once a connector is added, the following actions can be performed:

**Edit** - You can edit properties for any connector.

**Enable/Disable** - You can enable or disable any connector for automatic Incremental Scan.

**Sync** - If any connector fails to sync because of some back-end errors, you can manually Sync the connector.

**Delete** - You can delete any existing connector.

**Re-Authenticate** - Whenever you move to a new version of SaaS DR, you must re-authenticate if the existing connector does not appear on the application UI.

## Connector Status

You can view the status of the connector once you create a connector. Types of statuses are:

- Pending
- Success
- Partial Success
- Error
- Unauthorized

To know the status of the connector scan, go to **Configuration > Connectors**.



# Inventory Details

View all the Users and User Groups in your organization. Also, view all your resources, such as files and folders, third-party applications, and meetings identified from the scanned SaaS applications.

## View Directory

Once your SaaS application is connected, a scan is initiated to pull metadata from the application. This step may take some time to complete based on the number of users and resources to be cataloged in your application.

As your scan progresses, the **Directory** tab populates with all the users and user groups in the company that have access to the SaaS applications.

Navigate to **Directory > Users** or **Groups** tab and view the list of all users and user details, what kind of access the user has: internal or external, the role of the user, and so on.

The screenshot shows the SaaS Detection and Response (SaaS DR) interface. The top navigation bar includes links for HOME, DASHBOARD, DIRECTORY (active), RESOURCES, POLICY, MONITOR, RESPONSE, REPORTS, and CONFIGURATION. The left sidebar shows the 'Directory' section with a 'Users' tab selected, displaying '156 Total Users'. Below this, a list of SaaS applications and their user counts is shown: Salesforce (75), Office 365 (56), Google Workspace (12), Dropbox (9), Zoom (4), and a 'CONNECTOR' section with '0365 QA p01' (28). The main content area displays a table of users with columns for NAME, EMAIL, CONNECTOR, and ACCESS. The table shows several users, including 'AWSPublicSite Site Guest User' and '0365 QA p01', with their respective connectors and access levels (EXTERNAL).

NAME	EMAIL	CONNECTOR	ACCESS
	@gmail.com	Dropbox	EXTERNAL
AWSPublicSite Site Guest User		sfdc	EXTERNAL
AWSPublicSite Site Guest User		sfdc	EXTERNAL
AWSPublicSite Site Guest User		sfdc test	EXTERNAL
		0365 QA p01	EXTERNAL
		0365 QA p01	EXTERNAL

As part of the SaaS connector scan, SaaS DR classifies users as:

- **Internal:** These are mainly the employees of an organization that have an account on the SaaS application.
- **External:** These are mainly the users outside an organization with whom data is shared.

Internal or External users are classified differently depending on the SaaS application you are connecting. Except for SFDC, the classification is the same for all other products.

## View Resources

A list of resources such as files, folders, third-party applications, and meeting details are displayed in the Resources tab. You can view details such as what kind of resource access, whom are the resources shared with, the owner, etc.

NAME	OWNER	CONNECTOR	ACCESS	SHARED WITH	LAST MODIFIED ON
check incr 12/1 txt		stdc	INTERNAL	-	Jan 12, 2022 11:07 AM
check incr 12/1 txt		stdc	INTERNAL	-	Jan 12, 2022 11:07 AM
ext regression 1.5.0.docx document		Office 365	EXTERNAL	1	Jan 11, 2022 03:26 PM
ext regression 1.5.0.docx document		Office 365	EXTERNAL	1	Jan 11, 2022 03:26 PM
Document5.docx document		Office 365	INTERNAL	-	Dec 23, 2021 06:12 PM
Document5.docx document		Office 365	INTERNAL	-	Dec 23, 2021 06:12 PM

The **Files & Folders** tab lists the documents and folders in your company.

The **Applications** tab lists all the third-party applications installed by users in your company. You can view details like who has installed these applications using the company account and what permissions are granted. toggle between the Apps views to view this data grouped by the app name and the Users view to view the count of apps installed by each user.

The **Meetings** tab lists all the meetings and webinars conducted via applications such as Zoom. Note that the tab lists only those meetings with at least one recording. SaaSDR does not capture the meetings that do not have recordings.

**Note:** Qualys SaaSDR does not list ongoing meetings or meetings scheduled for the future.

For SaaSDR to list a meeting, the meeting should be concluded and have at least one cloud recording.

# Policy

Qualys provides best practices policies based on vendor's suggested best practices, industry practices, and some research. Currently, policies in the library are used for assessment purposes as they are. As we increase the content (number of controls) for each SaaS, we also offer to combine some of the CIS controls or best practices policies or vendor policies.

You can filter the policies provided out of the box under the 'System-defined' category. The user-defined policies (aka custom policies) are filtered under the 'User-defined' category. If the System-defined policies appear to be locked indicates that these policies cannot be changed.

## Enable a Policy

You can run policies and benchmarks defined for your SaaS application. The controls are validated, and the pass or fail status is displayed. Currently:

For Google Workspace, we support Best Practices.

For Zoom, we support CIS Benchmark and Zoom Best Practices.

For Salesforce, we support Best Practices.

For MS O365, we support CIS Benchmark and Microsoft Office 365 Best Practices.

Navigate to the **Policy** tab to view all the policies provided by Qualys. You can also enable or disable the policy for a connector.

SaaS Detection and Response

HOME DASHBOARD DIRECTORY RESOURCESPOLICYMONITORRESPONSEREPORTSCONFIGURATION

10  
Total Policies

SaaS

2  
Salesforce

2  
Google Workspace

3  
Office 365

3  
Zoom

POLICY TYPE

6  
System Defined

4  
User Defined

PolicyControls

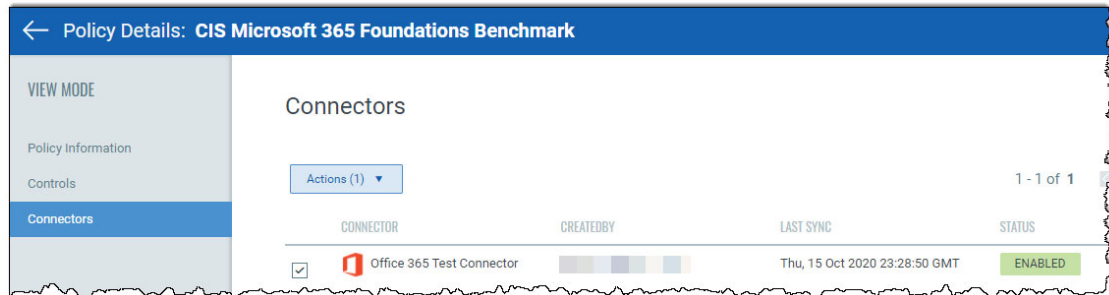
Search for Policies...

Actions (0)Create New

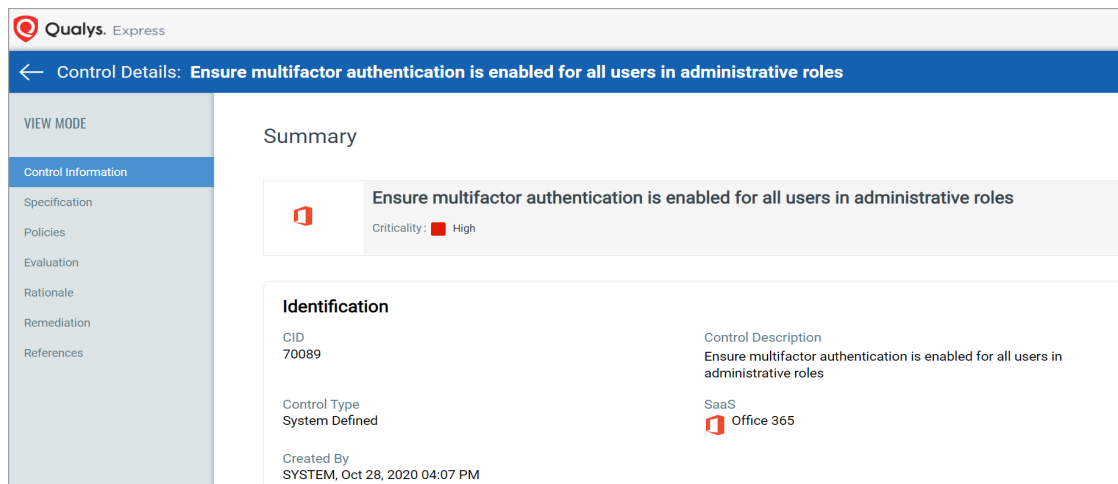
1 - 10 of 10

NAME	SaaS	CREATED BY	MODIFIED BY
tes Associated Controls : 6	Zoom		
Salesforce Best Practices Associated Controls : 48	Salesforce	SYSTEM Jan 8, 2021	SYSTEM Dec 30, 2021
Microsoft Office 365 Best Practices Associated Controls : 73	Office 365	SYSTEM Jul 22, 2021	SYSTEM Dec 30, 2021
Google Workspace Best practices Associated Controls : 14	Google Workspace	SYSTEM Jun 9, 2021	SYSTEM Jul 22, 2021
salesforce test Associated Controls : 3	Salesforce		

Click on the policy to open it in the View Mode and navigate to the **Connectors** tab. Select a connector and from the Actions menu, enable or disable the policy for this connector.



The Controls tab lists all controls and their details, such as SaaS, criticality, etc. Click on any control to view details specific to that control.



Once you enable a policy for a connector, you can view your compliance posture in the Monitor tab.

**Note:** For the following controls to be evaluated in SaaS DR accurately, enable the "Apps that don't use modern authentication" setting in Microsoft 365 Admin Center > SharePoint > Policies > Access Control: 70123, 70124, 70125, 70105, 70100, 70095.

**Note:** You must have a Microsoft 365 E5 license to evaluate the following four controls: 70098, 70099, 70112, and 70113.

## Manage Policies

You can perform the following activities on the policies:

- Viewing policy details
- Re-evaluating a policy

## Viewing a policy

To view a policy, select an existing policy, go to Actions > View.

The View Mode displays policy details such as Basic Details, SaaS application, Created By, Modified By, associated Controls, and so on.

## Re-evaluating a policy

You can re-evaluate all controls associated with a policy.

To re-evaluate controls of a policy, select an existing policy, go to Actions > Re-evaluate.

If the Re-evaluate button is disabled, refer to [Connector Warnings](#).

## Connector Warnings

On the Policy List page, there are warnings for different scenarios.

Take necessary actions based on the type of warning prompted.

## Control Library

The controls library is displayed under the **Policy > Controls** tab.

This page lists the out-of-the-box controls for different SaaS apps.

SaaS Detection and Response					
HOME DASHBOARD DIRECTORY RESOURCES <b>POLICY</b> MONITOR RESPONSE REPORTS CONFIGURATION					
Policy Controls					
197 Total Controls					
Search for Controls...					
1 - 50 of 197					
ID	NAME	SaaS	CREATED BY	CRITICALITY	
70000	Ensure owners are not allowed to delete all the messages that users sent in chat	Office 365	SYSTEM Jul 22, 2021	High	
70001	Ensure users are not allowed to delete their own messages sent in chat	Office 365	SYSTEM Jul 22, 2021	High	
70016	Ensure users do not use Citrix ShareFile as a third party storage	Office 365	SYSTEM Jul 22, 2021	High	
70017	Ensure users do not use DropBox ShareFile as a third party storage	Office 365	SYSTEM Jul 22, 2021	High	
70018	Ensure users do not use Box ShareFile as a third party storage	Office 365	SYSTEM Jul 22, 2021	High	
70019	Ensure users do not use Google Drive ShareFile as a third party storage	Office 365	SYSTEM Jul 22, 2021	High	
70043	Ensure anonymous users are not allowed to join a meeting	Office 365	SYSTEM Jul 22, 2021	High	
70050	Ensure users are not allowed to forward calls or simultaneous ringing of inbound calls to external phone numbers	Office 365	SYSTEM Jul 22, 2021	High	
70051	Ensure voicemail is disabled for routing inbound calls	Office 365	SYSTEM Jul 22, 2021	High	

## Custom Policies

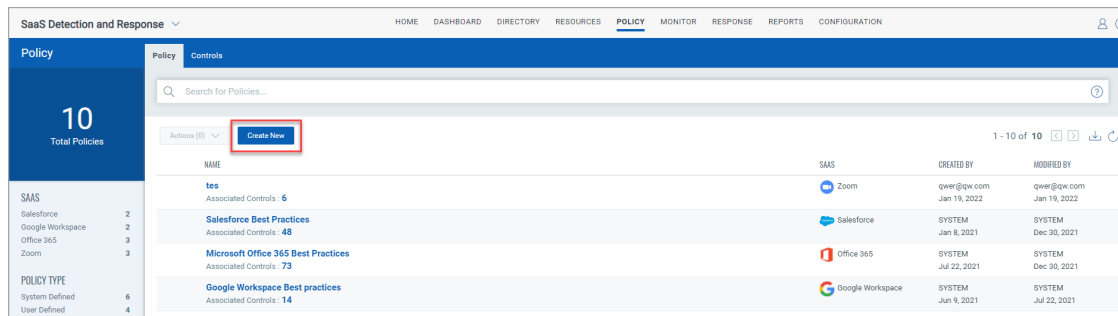
On top of CIS, Qualys provides best practices policies based on vendors' suggested best practices, industry practices, and research. Currently, policies in the library are used for assessment purposes as they are. As we increase the content (number of controls) for each SaaS, we also offer to combine some of the CIS controls, or best practices policies, or vendor policies.

Some policies provided out of the box are filtered under the 'System-defined' category. You can filter the user-defined policies (aka custom policies) under the 'User-defined' category. System-defined policies are shown as locked, indicating that you cannot change these policies. You can either create a new policy or edit an existing policy.

**Note:** This feature is only available for users with a trial or full subscription of the application and not for users with a free subscription.

You can create a new policy by **Policy** tab > **Create New**.

The newly created policies appear under the **Policy** Tab.



## Manage Custom Policies

You can perform the following activities on user-defined policies:

- Editing existing user-defined policies
- Deleting a user-defined policy
- Viewing policy details
- Re-evaluating a policy

**Note:** Editing and deleting options are only allowed for user-defined (custom) policies.

# Monitor SaaS Applications

You can run policies and benchmarks defined for your SaaS application. The controls are validated, and the pass or fail status is displayed.

Navigate to the **Policy** tab to view all the policies provided by Qualys. From here, you can also enable or disable the policy.

NAME	SaaS	CREATED BY	MODIFIED BY
<b>tes</b> Associated Controls: 6	Zoom	Jan 19, 2022	Jan 19, 2022
<b>Salesforce Best Practices</b> Associated Controls: 48	Salesforce	SYSTEM Jan 8, 2021	SYSTEM Dec 30, 2021
<b>Microsoft Office 365 Best Practices</b> Associated Controls: 73	Office 365	SYSTEM Jul 22, 2021	SYSTEM Dec 30, 2021
<b>Google Workspace Best Practices</b> Associated Controls: 14	Google Workspace	SYSTEM Jun 9, 2021	SYSTEM Jul 22, 2021
<b>salesforce test</b> Associated Controls: 3	Salesforce	Jan 20, 2022	Jan 20, 2022

Navigate to the Monitor tab to monitor your compliance posture in real-time.

CID	CONTROL NAME	CRITICALITY	CONNECTOR	SECURITY POSTURE
70147	Ensure that no expired certificates are being used in the Certificate and Key Management Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70142	Ensure that clickjack protection is enabled for non-setup Salesforce pages Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70221	Ensure that users are warned before being redirected outside of Salesforce Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70143	Ensure that clickjack protection is enabled for customer visualforce pages with standard headers Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70222	Ensure that identity verification for email address changes is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70144	Ensure that 'Clickjack protection for customer visualforce pages with headers disabled' setting is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70223	Ensure that email confirmation for email address changes is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70157	Ensure that the setting 'Require HttpOnly attribute' is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1

## Monitor Compliance Posture

In the **Monitor** tab, you can monitor your compliance posture in real-time for each connector. View details such as connector type and the security posture at a glance.

The screenshot shows the 'Monitor' tab in the SaaS Detection and Response interface. The top navigation bar includes links for HOME, DASHBOARD, DIRECTORY, RESOURCES, POLICY, MONITOR (active), RESPONSE, REPORTS, and CONFIGURATION. The left sidebar displays a summary of 403 total controls evaluated, categorized by result (Fail: 198, Pass: 150, Error: 98) and criticality (High: 160, Medium: 131, Low: 112). It also lists connectors (Office 365, sfdc, sfdc test) and SaaS applications (Office 365).

The main content area shows a table of controls with the following columns: DID, CONTROL NAME, CRITICALITY, CONNECTOR, and SECURITY POSTURE. The table lists 10 controls, all with a 'High' criticality and 'sfdc' connector. Each control has a 'Security Posture' column showing a score of 1 and a 'Total Resources' of 1. A 'Remediate' button is visible at the top left of the table.

DID	CONTROL NAME	CRITICALITY	CONNECTOR	SECURITY POSTURE
70147	Ensure that no expired certificates are being used in the Certificate and Key Management Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70142	Ensure that clickjack protection is enabled for non-setup Salesforce pages Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70221	Ensure that users are warned before being redirected outside of Salesforce Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70143	Ensure that clickjack protection is enabled for customer visualforce pages with standard headers Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70222	Ensure that identity verification for email address changes is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70144	Ensure that 'Clickjack protection for customer visualforce pages with headers disabled' setting is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70223	Ensure that email confirmation for email address changes is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1
70157	Ensure that the setting 'Require HttpOnly attribute' is enabled Salesforce Best Practices	High	sfdc	1 Total Resources: 1

From the **Security Posture** column, you can drill down to view details of each control and their pass or fail status. Click on each control to view further control details, such as remediation, evidence, etc.



## Events

You can view and filter the events related to Salesforce, Dropbox, and Office 365 according to the service types. You can view the events of varying criticality related to the user, application, and files. This view helps IT admins and Security Operations teams monitor any unusual activities.

To view any user activity, go to **Monitor > Events**.

You can filter the activities by clicking on any Category, Sub Category, or, Severity options available in the left navigation pane. The filter depends on the variations of the events appearing in the list.

NAME	CONNECTOR	TIME	ACTOR	SEVERITY
Add app role assignment grant to user	office 365	Jan 28, 2022 03:33 PM		MEDIUM
Consent to application	office 365	Jan 28, 2022 03:33 PM		LOW
Add app role assignment grant to user	office 365	Jan 28, 2022 03:08 PM		MEDIUM
Consent to application	office 365	Jan 28, 2022 03:08 PM		LOW
UserLoggedIn	office 365	Jan 28, 2022 02:03 PM		MEDIUM
UserLoggedIn	office 365	Jan 28, 2022 02:01 PM		MEDIUM
UserLoggedIn	office 365	Jan 28, 2022 02:01 PM		MEDIUM
UserLoggedIn	office 365	Jan 28, 2022 01:58 PM		MEDIUM
UserLoggedIn	office 365	Jan 28, 2022 01:58 PM		MEDIUM

To view the details of the User Activity Event, click the Event.

The detail page will show a pop-up in JSON view.

SaaS DR monitors Salesforce logs, Dropbox logs and Office365 logs for events (as recommended by CISA) such as:

- Failed login
- Update Application Permission
- Update Group
- Set domain authentication.
- Add admin role to a member
- Remove admin role

And a lot more!

To know more about Office 365 logs for events, click [here](#).

# Security Misconfigurations

Qualys SaaS DR enables you to remediate the controls that have a failed status for security posture for Office 365 subscriptions.


For now, you can fix security misconfigurations for Office 365 without having to separately log in to the Admin Center of Office 365.

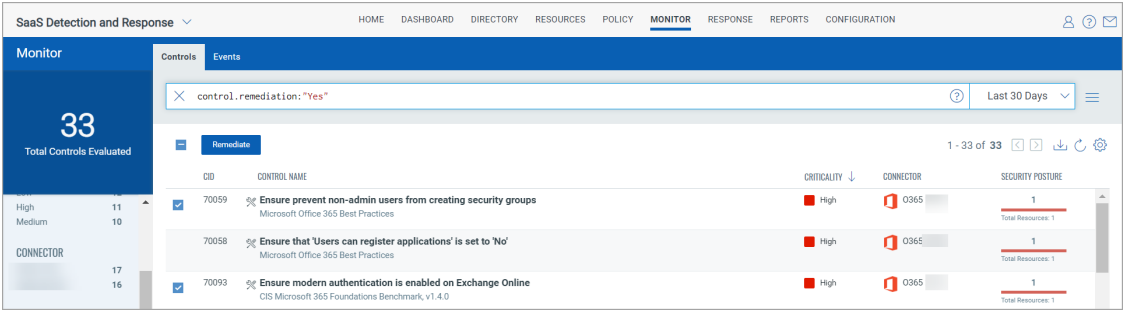
## Remediation for Office 365

For Office 365 subscriptions, you can remediate the controls that have a failed status for security posture.

To remediate a control, go to the **Monitor > Controls** tab, select the control you want to remediate, and click **Remediate**.

**Note:** You can only fix tenant-level misconfigurations without logging into the Office 365 admin center. To filter the tenant-level misconfiguration, use the **control.remediation:** "Yes" search token to filter the remediable controls.

Only the controls with the  icon are remediable:  
Select the required controls you want to remediate from the list of available controls.



## Creating a Remediation Job

Once you click **Remediate**, you can create a remediation job.

1. On the Basic Information window, enter the **Name** and **Description** and click **Next**.

The **SaaS** and the **Connector** fields are auto-populated.

← Create New: Remediation Job

STEPS 1/3

- 1 Basic Information
- 2 Select Controls
- 3 Review and Confirm

**Basic Information**  
Add details of the remediation job here.

Name \*  
Remediate Controls

Description  
  
250/250 characters remaining

SaaS \*  
Office 365

Connector \*  
O365 2103

Cancel Next

2. On the Select Controls window, click **Next** if all the details appear correctly.  
Or,

**Optional:** You can choose to remove controls or add new controls.

**Remove controls:** Select one or more controls available in the list and click **Remove Selected** or use the Remove control icon to remove control.

← Create New: Remediation Job

STEPS 2/3

- 1 Basic Information
- 2 Select Controls
- 3 Review and Confirm

**Select Controls**  
Choose the failing controls to add to the remediation job.

Controls (2)

Remove Selected

<input type="checkbox"/>	CID	NAME	REMEDIATION ACTION	CRITICALITY	
<input type="checkbox"/>	70059	Ensure prevent non-admin users from creating security groups	Set-MsolCompanySettings -Us...	High	<input type="checkbox"/>
<input checked="" type="checkbox"/>	70093	Ensure modern authentication is enabled on Exchange Online	Set-OrganizationConfig -OAuth...	High	<input type="checkbox"/>

Cancel Previous Next

**Add controls:** You can also add controls when creating the remediation job using the **Add Controls** icon as highlighted below:

← Create New: Remediation Job

STEPS 2/3

- 1 Basic Information
- 2 Select Controls
- 3 Review and Confirm

Select Controls

Choose the failing controls to add to the remediation job.

Controls (2)

Remove Selected

<input type="checkbox"/>	CID	NAME	REMEDIATION ACTION	CRITICALITY	↓
<input type="checkbox"/>	70059	Ensure prevent non-admin users from creating security groups	Set-MsolCompanySettings -Us...	High	×
<input type="checkbox"/>	70093	Ensure modern authentication is enabled on Exchange Online	Set-OrganizationConfig -OAuth...	High	×

Cancel Previous Next

3. Review the controls and click **Next**.

4. On the Review and Confirm window, confirm the details and click **Create**.

← Create New: Remediation Job

STEPS 3/3

- 1 Basic Information
- 2 Select Controls
- 3 Review and Confirm

Review and Confirm

You're all done! Review your selection and click Submit. This remediation job will be created and added to your remediation jobs list.

Basic Information

Name	test	Description	-
SaaS	Office 365	Connector	0365 2103

Selected Controls

CID	NAME	REMEDIATION ACTION	CRITICALITY	↓
70059	Ensure prevent non-admin users from creating security groups	Set-MsolCompanySettings -Us...	High	×
70093	Ensure modern authentication is enabled on Exchange Online	Set-OrganizationConfig -OAuth...	High	×

Cancel Previous Create

Once you initiate the remediation, the compliance scan automatically reflects the latest compliance posture. The status of the controls changes based on the scan results once the remediation is successful.

You can view the status of remediated jobs under the **Response > Remediation Jobs** tab.

SaaS Detection and Response

HOME DASHBOARD DIRECTORY RESOURCES POLICY MONITOR RESPONSE REPORTS CONFIGURATION

Response

Remediation Jobs

Search...

1 - 6 of 6

NAME	STATUS	CONNECTOR	CREATED BY	NUMBER OF CONTROLS COMPLETED
Remediate 70015	Completed	Office 365	Jan 28, 2022	1 of 1
Remediate 70059	Completed	Office 365	Jan 28, 2022	1 of 1
Remediate 70058	Completed	Office 365	Jan 28, 2022	1 of 1
	Completed	Office 365	Jan 28, 2022	1 of 1
Remediate 70184 Exchange	Completed	Office 365	Jan 28, 2022	1 of 1

6  
Total Remediation Jobs

STATUS

Completed 6

OWNER

6

# Response

In the **Response** tab, you can check the status of different response activities.

Go to the **Remediation Jobs** sub-tab to check the remediation jobs used to fix the misconfigurations on your SaaS tenants. You can view the progress and status of the remediation job(s) and export the details from the **Response** tab > **Remediation Jobs** sub-tab.

By default, the remediation job is in the **Disabled** state. You must enable it to get started.

SaaS Detection and Response

HOME DASHBOARD DIRECTORY RESOURCES POLICY MONITOR **RESPONSE** REPORTS CONFIGURATION

**Response**

Remediation Jobs

68  
Total Remediation Jobs

STATUS

Cancelled	5
Completed	60
Disabled	2
Pending Evaluati...	1

Search for Jobs...

Enable

1 - 50 of 68

NAME	STATUS	CONNECTOR	CREATED BY	NUMBER OF CONTROLS COMPLETED
<input checked="" type="checkbox"/> [Redacted]	Disabled	O365	Mar 14, 2022	0 of 1
[Redacted]	Completed	O365	Mar 14, 2022	0 of 11
[Redacted]	Completed	O365	Mar 14, 2022	12 of 23

# Reports

SaaS Detection and Response allows you to view all the application reports. The **Reports** tab lists all the existing reports.

REPORT NAME	STATUS	SaaS	FORMAT	CREATED ON	CREATED BY	EXPIRES ON
[Icon]	Completed	Google Workspace	PDF	Jan 28, 2022 04:00 PM	[Icon]	Feb 4, 2022 04:00 PM
[Icon]	Completed	Office 365	PDF	Jan 24, 2022 04:46 PM	[Icon]	Jan 31, 2022 04:46 PM
[Icon]	Completed	Office 365	PDF	Jan 24, 2022 10:39 AM	[Icon]	Jan 31, 2022 10:39 AM
[Icon]	Completed	Office 365	CSV	Jan 24, 2022 10:38 AM	[Icon]	Jan 31, 2022 10:38 AM

You can perform different actions on an existing report:

Create Report - The newly created report appears on the landing page of On-Demand Reports.

To perform other actions on existing reports, go to Actions (1) drop-down menu:

- Run report
- Edit report template
- Delete

User can also download the report using the download icon.

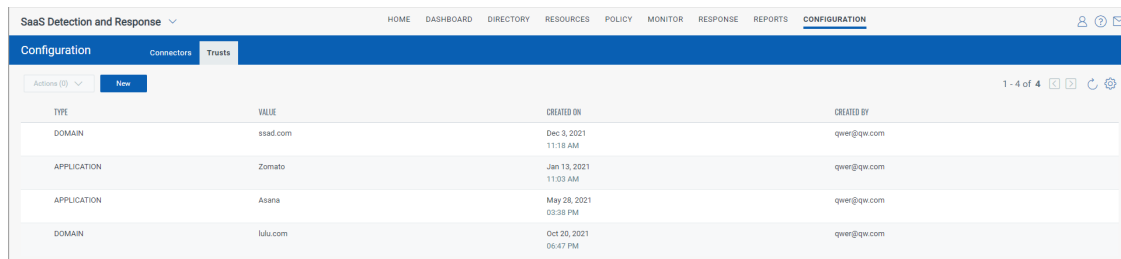
The report can be downloaded in two options: CSV and PDF format.

# Trusted Domains and Applications

When you work closely with members of a different domain, you might want to add resources of that domain as trusted resources. For example, when working with company XYZ on a project, you might share resources with members of this company. Qualys SaaS DR allows you to add domains and applications you trust to a Trusted list. Once included in the list, you can use the Non Trusted or Is Trusted filters in the **Resources > Applications** tab to view resources from other domains.

## Add Domains and Applications as Trusted

You can add domains and applications to the trusted list by navigating to the **Configuration > Trusts** tab and clicking **New**.



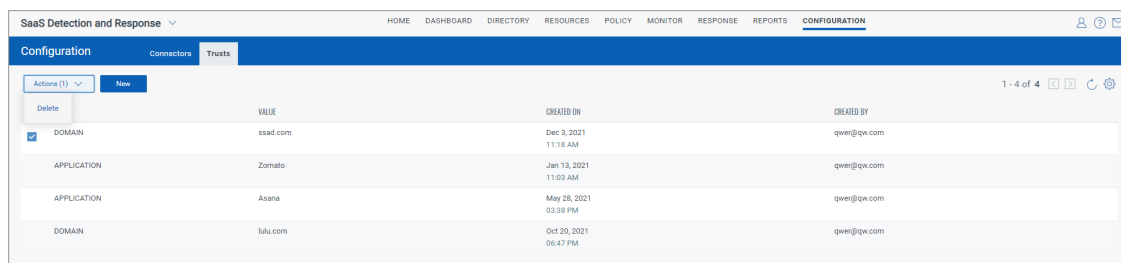
The screenshot shows the 'Configuration' page with the 'Trusts' tab selected. A table lists four trusted resources. The first row is a domain 'ssad.com' added on Dec 3, 2021. The next two rows are applications 'Zomato' and 'Asana' added on Jan 13, 2021 and May 28, 2021 respectively. The final row is a domain 'lulu.com' added on Oct 20, 2021. All resources were created by 'qwer@qw.com'.

TYPE	VALUE	CREATED ON	CREATED BY
DOMAIN	ssad.com	Dec 3, 2021 11:18 AM	qwer@qw.com
APPLICATION	Zomato	Jan 13, 2021 11:03 AM	qwer@qw.com
APPLICATION	Asana	May 28, 2021 03:38 PM	qwer@qw.com
DOMAIN	lulu.com	Oct 20, 2021 06:47 PM	qwer@qw.com

The **Trusts** tab lists the newly created trust.

## Remove Domains and Applications from the Trusted List

You can remove a previously added domain/application from the trusted list by navigating to the **Configuration > Trusts** tab.



This screenshot is identical to the previous one, but the first row (DOMAIN: ssad.com) has a blue checkbox selected in the left margin, indicating it is chosen for an action. The 'Actions' dropdown menu is open, showing 'Delete' as the selected option.

TYPE	VALUE	CREATED ON	CREATED BY
<input checked="" type="checkbox"/> DOMAIN	ssad.com	Dec 3, 2021 11:18 AM	qwer@qw.com
APPLICATION	Zomato	Jan 13, 2021 11:03 AM	qwer@qw.com
APPLICATION	Asana	May 28, 2021 03:38 PM	qwer@qw.com
DOMAIN	lulu.com	Oct 20, 2021 06:47 PM	qwer@qw.com

Select the applications/domains you wish to remove from the list and then click **Actions > Delete** to remove them from the list.



# Customizable Dynamic Dashboard

Dashboards help you visualize your data in a central, customizable dashboard and share the compliance status of your environment in real-time.

Qualys SaaS DR integrates with Unified Dashboard (UD) to bring information from all Qualys applications into a single place for visualization. UD provides a powerful, new dashboarding framework and platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

Qualys SaaS DR offers several dashboards out-of-the-box. Each dashboard displays a short description of the information it offers. You can also easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your view.

See the Unified Dashboard help for more information.