SaaS Detection and Response

Getting Started Guide
Version - 1.8.0

February 27, 2024

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

Table of Contents

About this Guide

Welcome to Qualys SaaS Detection and Response (SaaSDR)! 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

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/.

SaaS Detection and Response Overview

Qualys SaaS Detection and Response (SaaSDR) 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 SaaSDR

- 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

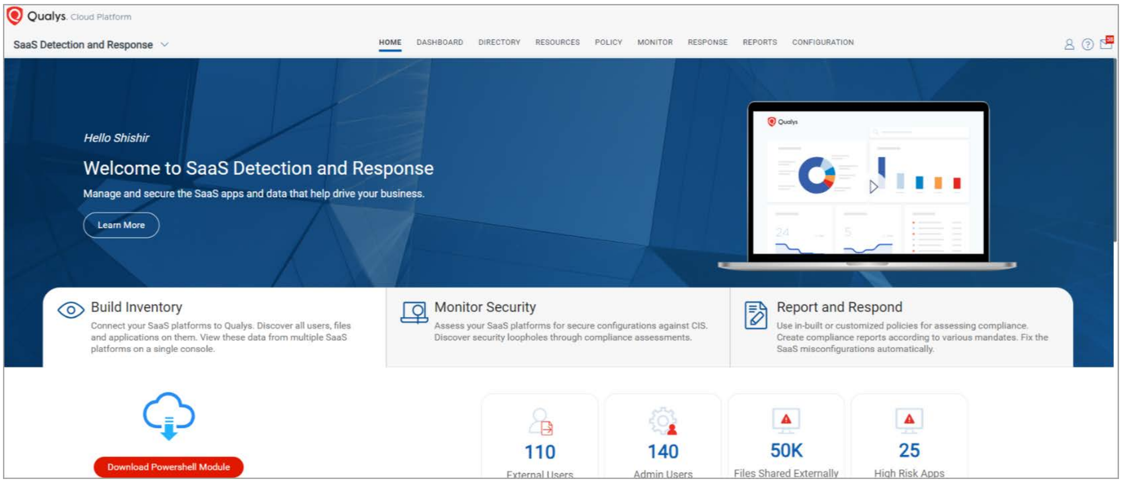
- Get visibility into apps that have given access to sensitive data and take steps to alert and block them

- 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 SaaSDR, 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 SaaSDR 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 (SaaSDR) 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 SaaSDR, 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

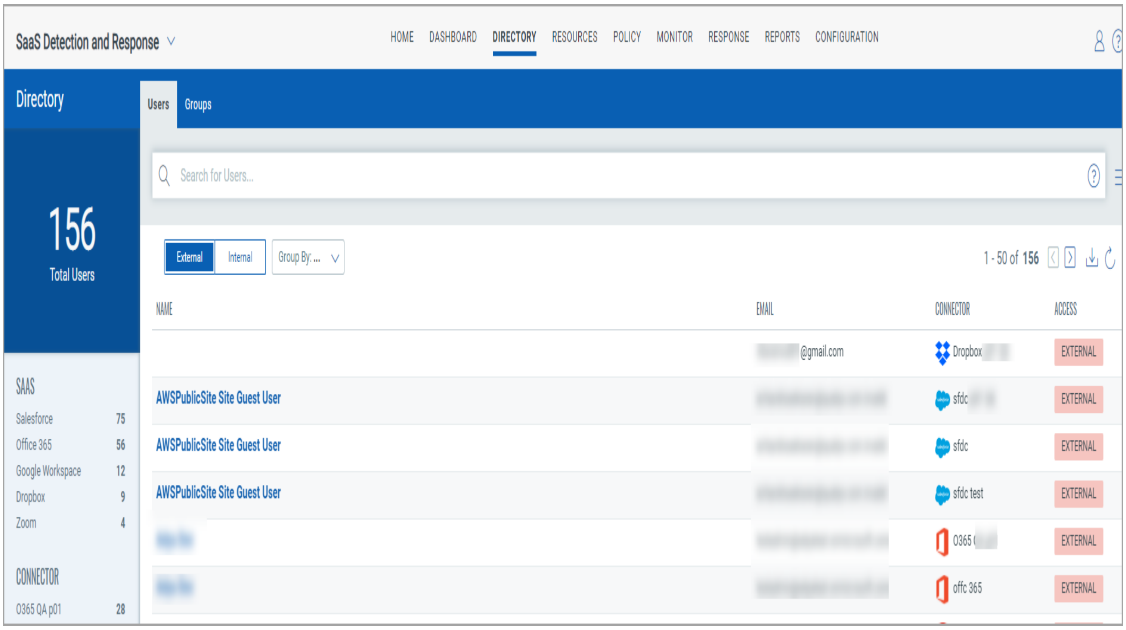
View all the Users and User Groups in your organization. Also, view all your resources, such as files and folders, third-party applications, and meetings identified from the scanned SaaS applications.

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.



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

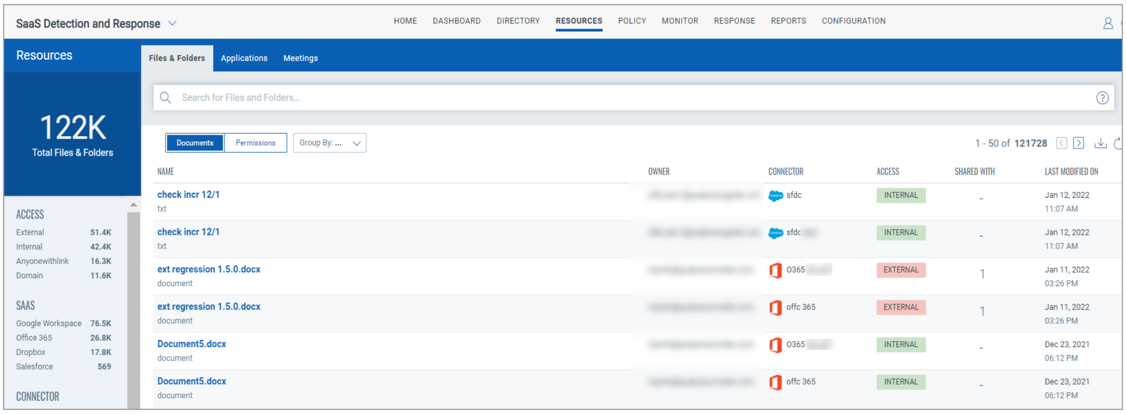
- **Internal**: These are mainly the employees of an organization that have an account on the SaaS application.

- **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.



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:

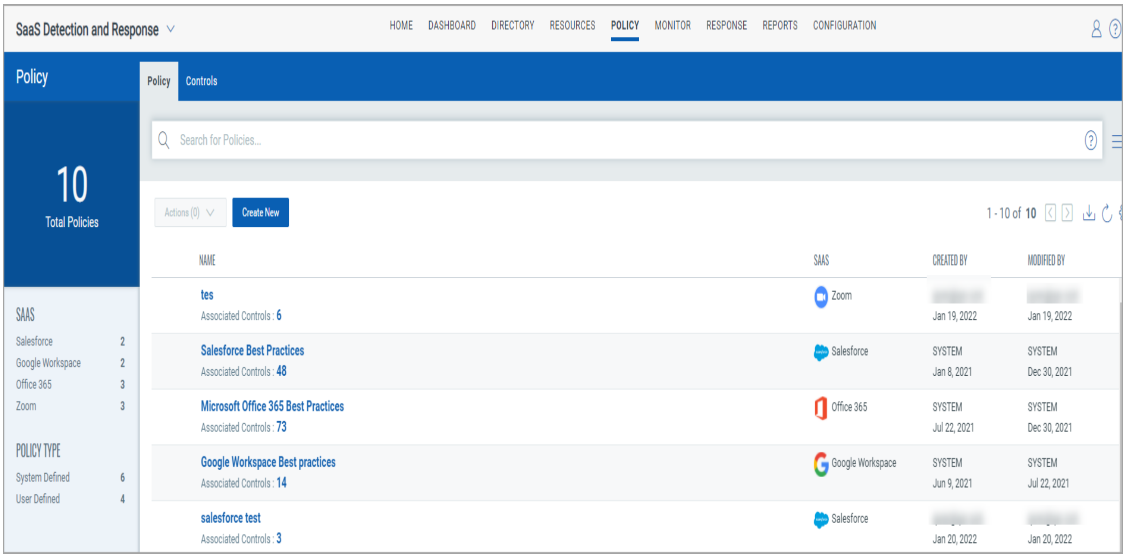
For Google Workspace, we support Best Practices.

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

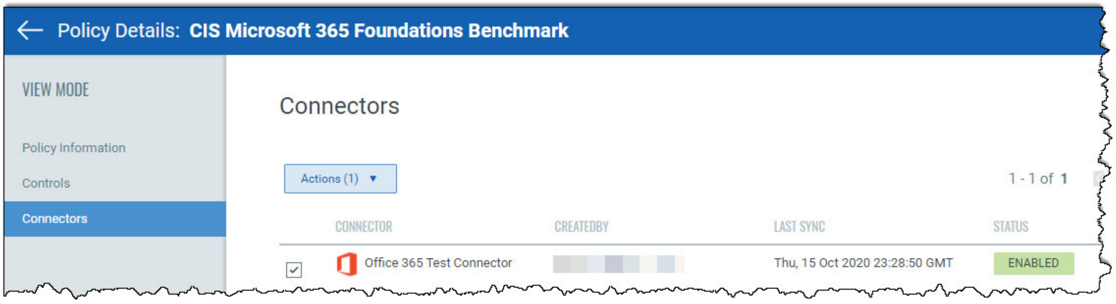
For Salesforce, we support Best Practices.

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

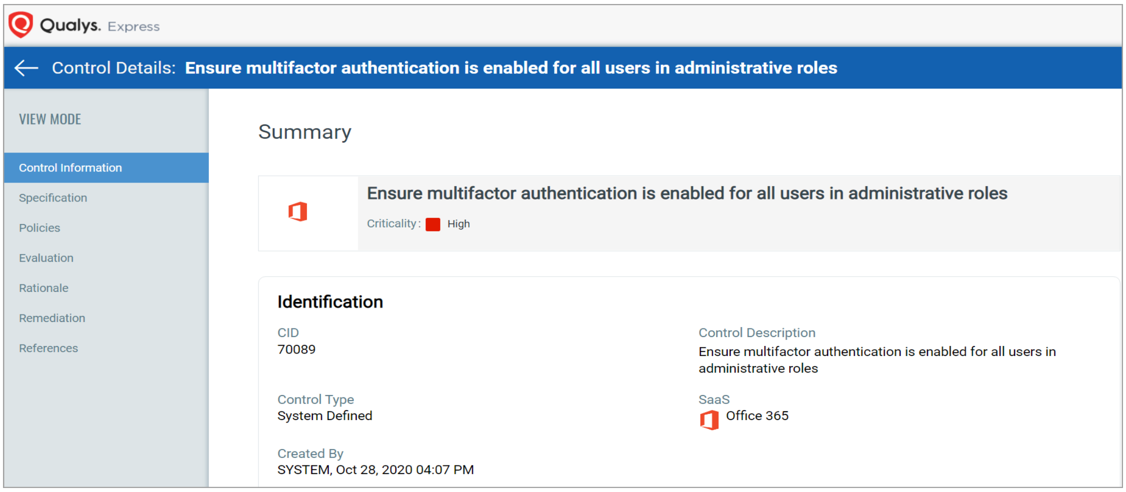
Navigate to the **Policy** tab to view all the policies provided by Qualys. You can also enable or disable the policy for a connector.



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 SaaSDR 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

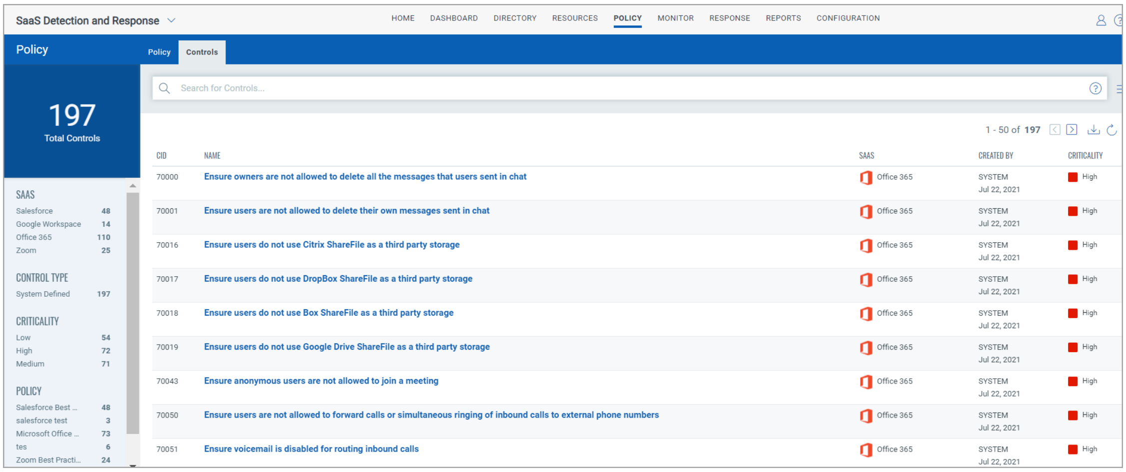
On the Policy List page, there are warnings for different scenarios.

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.



Custom Policies

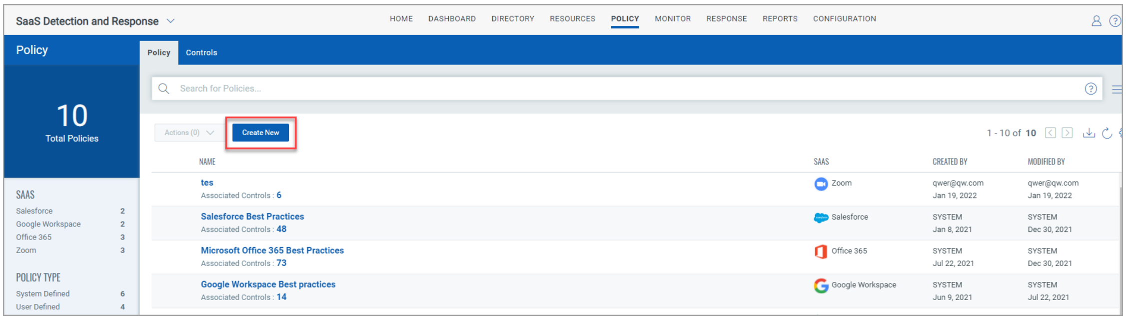
On top of CIS, Qualys provides best practices policies based on vendors' suggested best practices, industry practices, and research. Currently, policies in the library are used for assessment purposes as they are. As we increase the content (number of controls) for each SaaS, we also offer to combine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

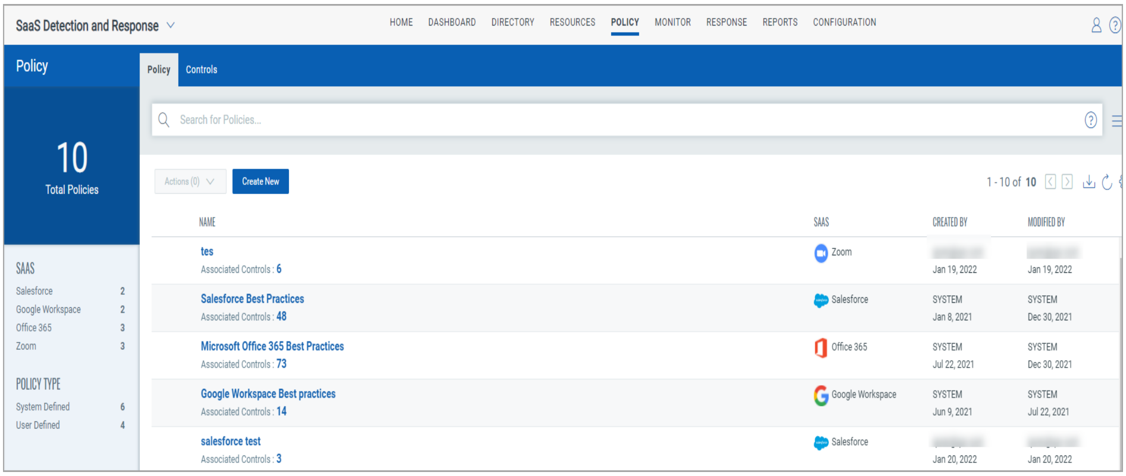
- Re-evaluating a policy

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

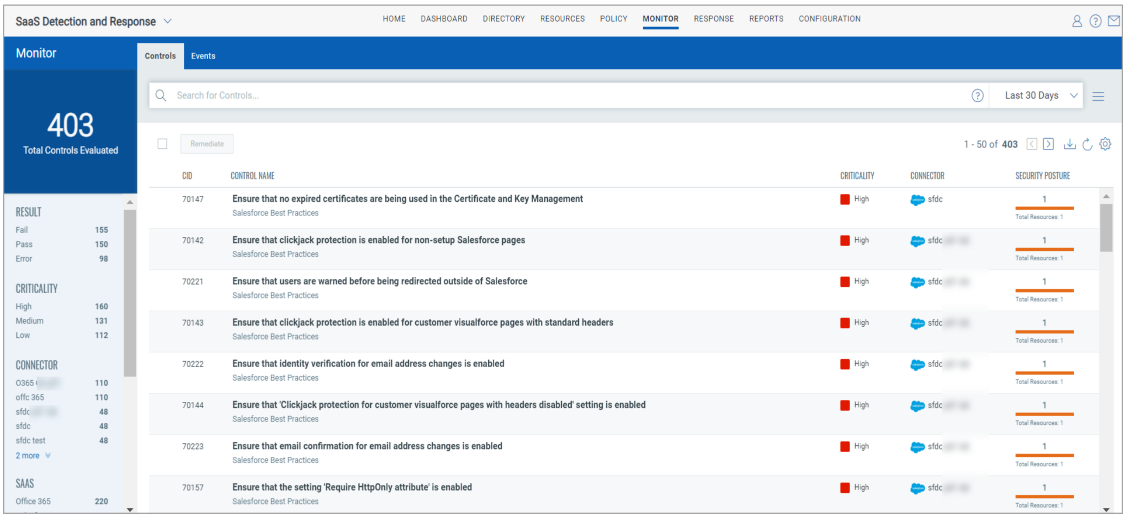
Monitor SaaS Applications

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.

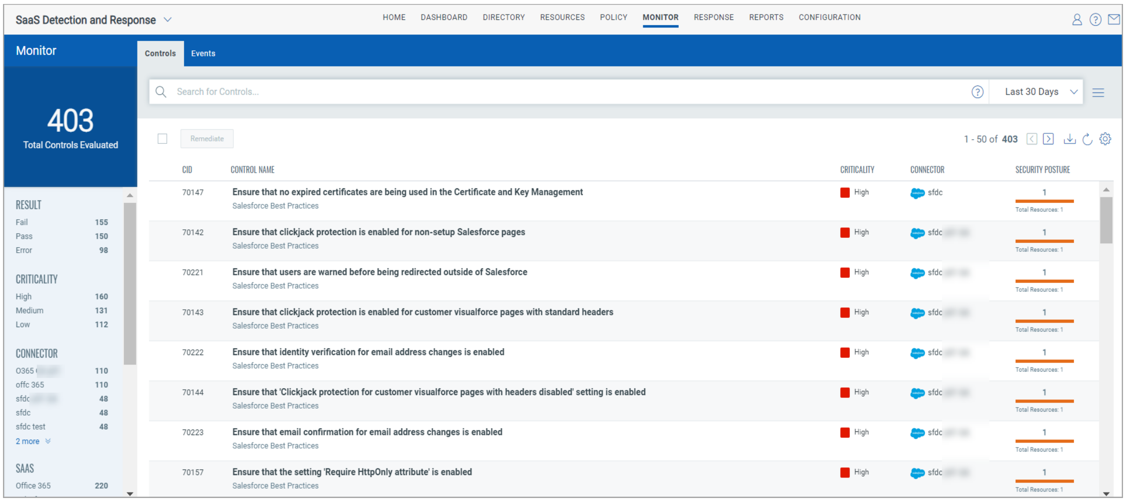


Navigate to the Monitor tab to monitor your compliance posture in real-time.



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.



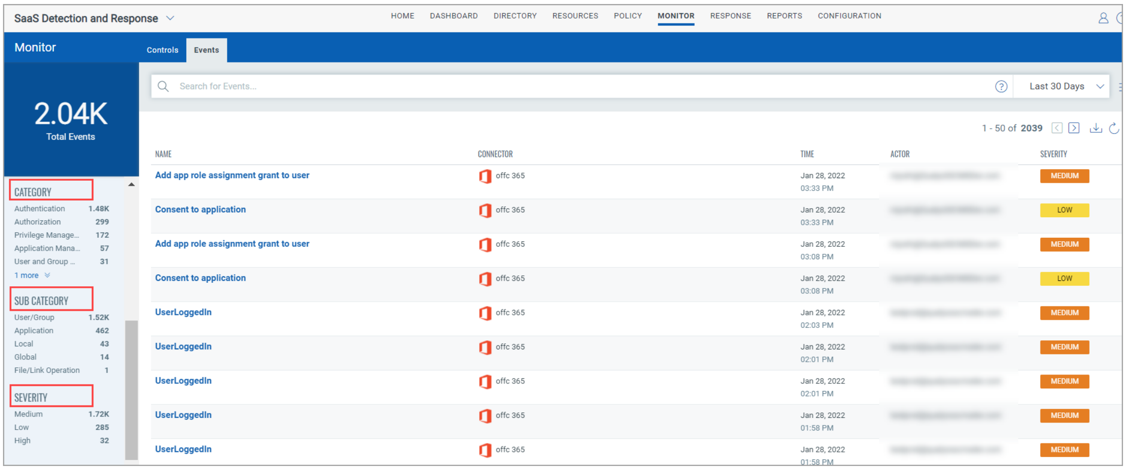
From the **Security Posture** column, you can drill down to view details of each control and their pass or fail status. Click on each control to view further control details, such as remediation, evidence, etc.

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.



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

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

SaaSDR 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 SaaSDR 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.

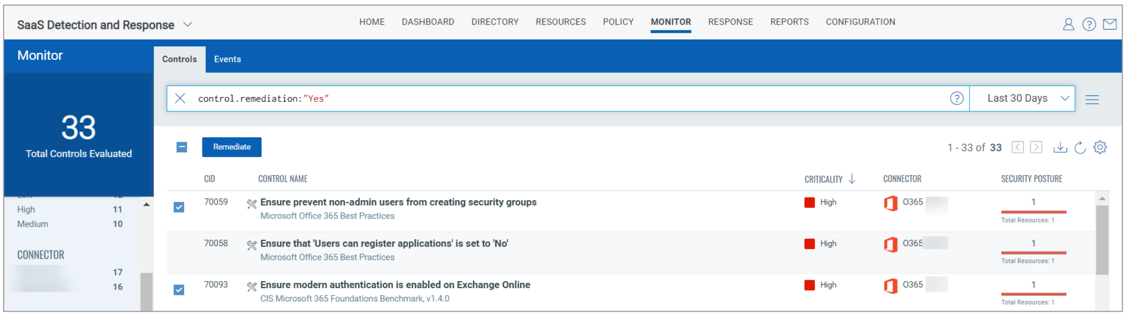
Remediation for Office 365

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.

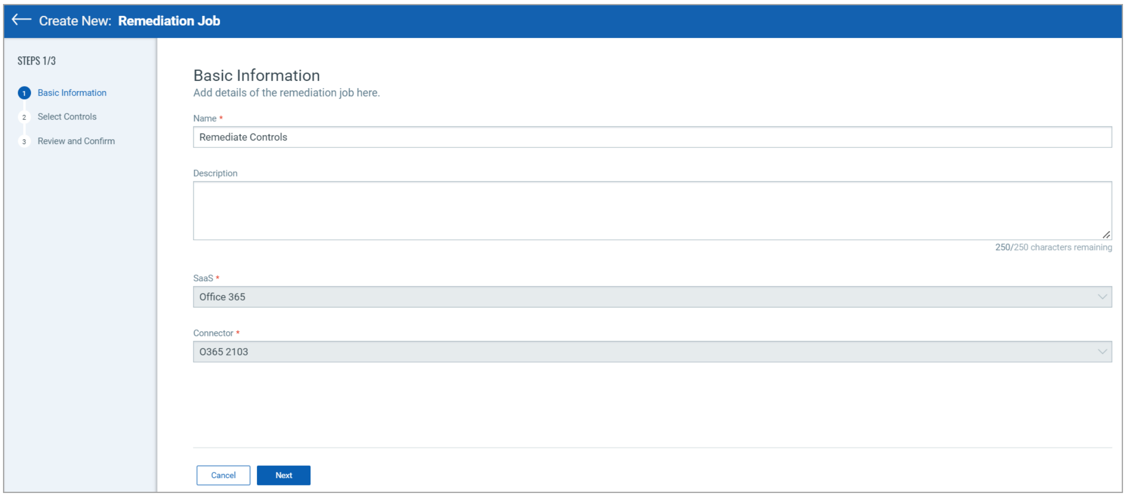


Creating a Remediation Job

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

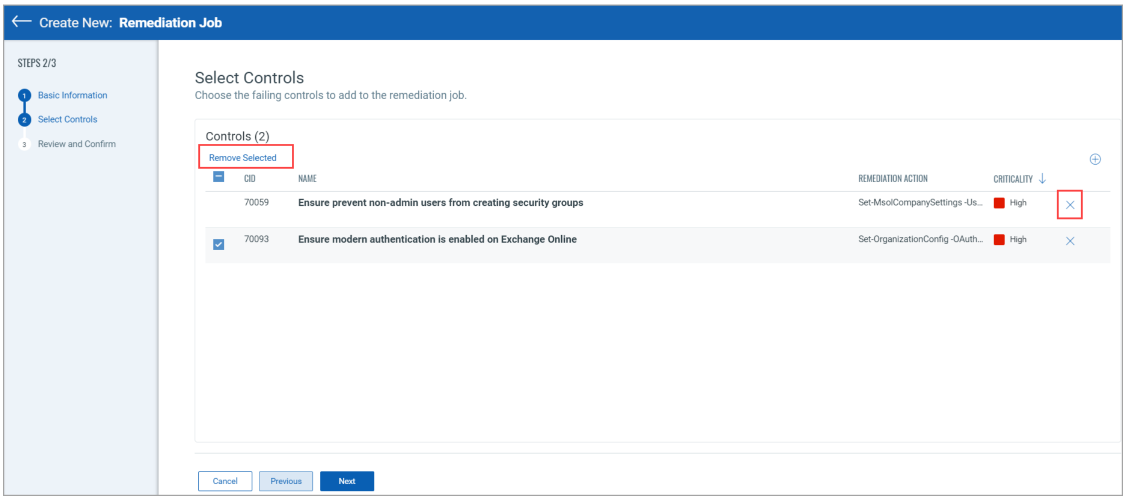
1. On the Basic Information window, enter the **Name** and **Description** and click **Next**.

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

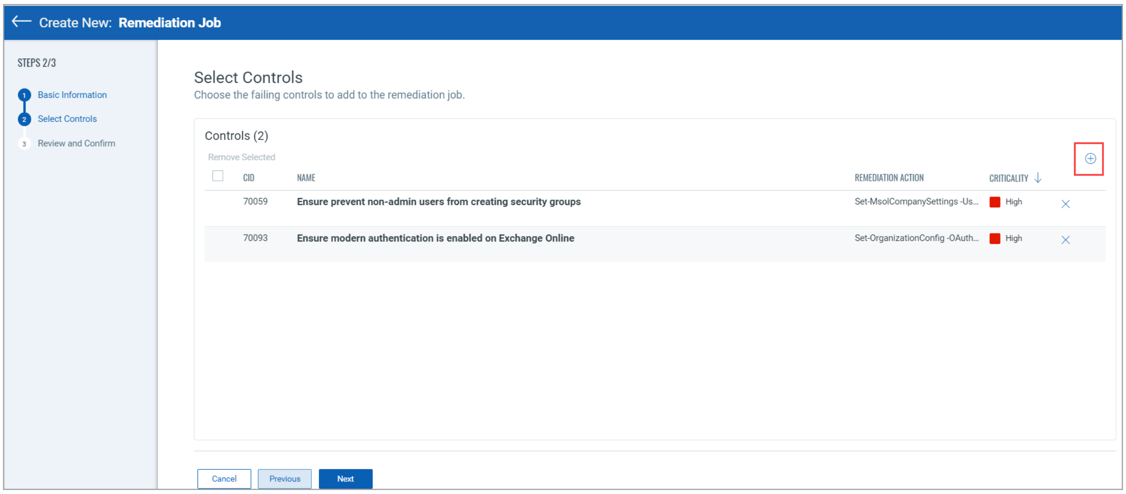


2. On the Select Controls window, click **Next** if all the details appear correctly.
Or,

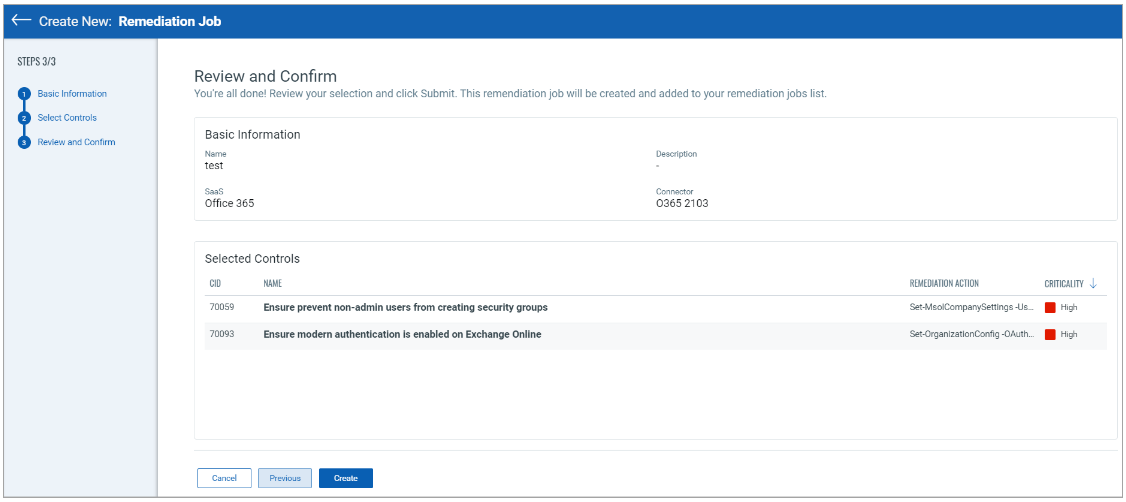
Optional: You can choose to remove controls or add new controls.
Remove controls: Select one or more controls available in the list and click **Remove Selected** or use the Remove control icon to remove control.



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

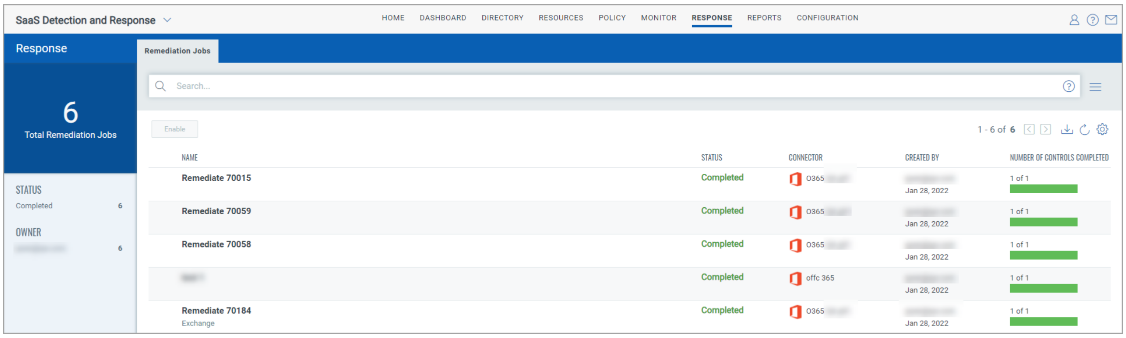


3. Review the controls and click **Next**.
4. On the Review and Confirm window, confirm the details and click **Create**.



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.

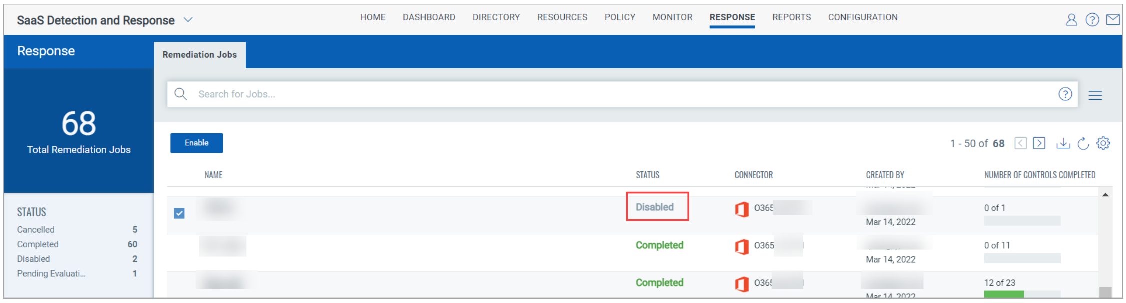


Response

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

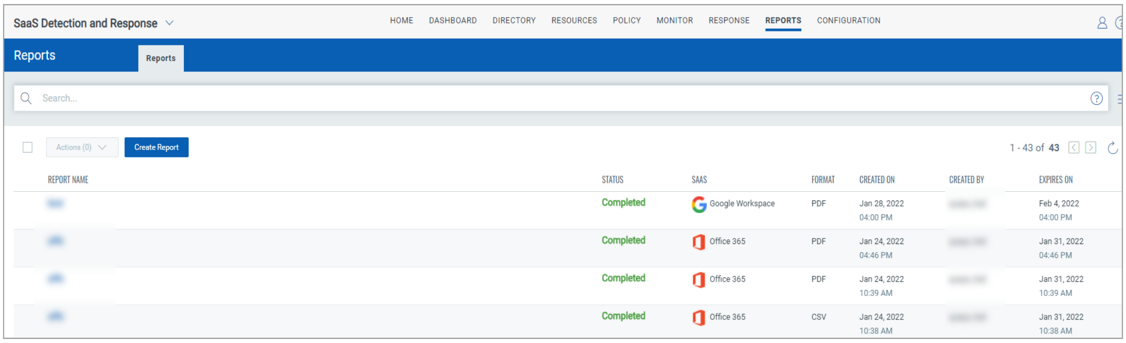
Go to the **Remediation Jobs** sub-tab to check the remediation jobs used to fix the misconfigurations on your SaaS tenants. You can view the progress and status of the remediation job(s) and export the details from the **Response** tab > **Remediation Jobs** sub-tab.

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



Reports

SaaSDR allows you to view all the application reports. The **Reports** tab lists all the existing reports.



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.

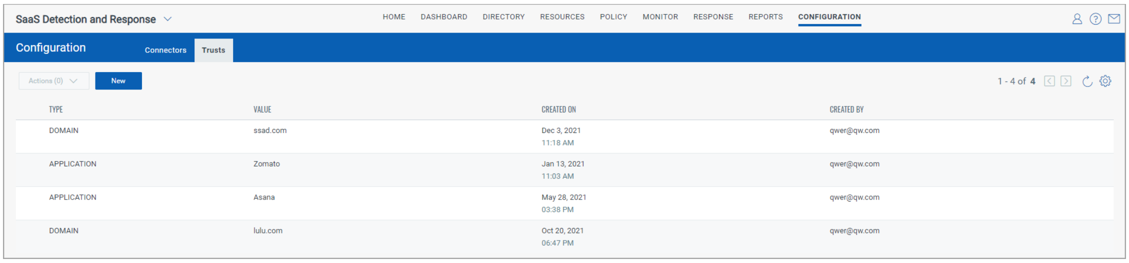
The report can be downloaded in two options: CSV and PDF format.

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 SaaSDR 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

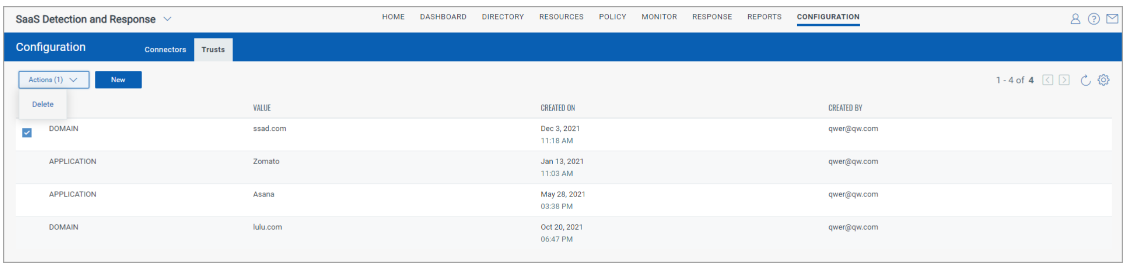
You can add domains and applications to the trusted list by navigating to the **Configuration** > **Trusts** tab and clicking **New**.



The **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.



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 SaaSDR 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 SaaSDR 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.