



Qualys CloudView v1.x

Version 1.8.0.0

June 5, 2019

Here's what's new in Qualys CloudView 1.8!

[New AWS Controls and CIS Google Cloud Platform Foundation Benchmark Support](#)

[Reports now Supported](#)

[Automatic Connector Creation in AssetView Enabled](#)

[New Widgets in Dashboard for Mandates and Policies](#)

New AWS Controls and CIS Google Cloud Platform Foundation Benchmark Support

We have now added a new policy titled CIS Google Cloud Platform Foundation Benchmark that supports 15 new controls for Google Cloud Platform (GCP). We have also introduced 11 new controls for AWS.

Go to Policies tab and click the policy title, the Controls pane then lists the controls. The details of the new controls that are available with CloudView 1.8.0.0 is listed below.

New Controls for AWS

CID	Policy	Resource	Control Title
58	AWS Best Practices	KMS	Ensure that the key expiry is set for CMKs with external key material.
59	AWS Best Practices	S3	Ensure "Block new public bucket policies" for a bucket is set to true.
60	AWS Best Practices	S3	Ensure that "Block public and cross-account access" if bucket has public policies for bucket is set to true.
61	AWS Best Practices	S3	Ensure that "Block new public ACLs and uploading public objects" for a bucket is set to true.
62	AWS Best Practices	S3	Ensure that "Remove public access granted through public ACLs" for a bucket is set to true
63	AWS Best Practices	Account	Ensure 'Block new public bucket policies' for an AWS Account is set to true.
64	AWS Best Practices	Account	Ensure 'Block public and cross-account access to buckets that have public policies' for an AWS Account is set to true.
65	AWS Best Practices	Account	Ensure 'Block new public ACLs and uploading public objects' for an account is set to true.
66	AWS Best Practices	Account	Ensure 'Remove public access granted through public ACLs' for an account is set to true.
67	AWS Best Practices	S3	Ensure Server Side Encryption (SSE) is enabled for S3 bucket.
68	AWS Best Practices	Certificates CIS v1.3.0-1.23	Ensure that all the expired SSL/TLS certificates stored in AWS IAM are removed: This control needs current date to evaluate. Not supported in current framework.

New Controls for GCP

CID	Policy	Resource	Control Title
52001	CIS Google Cloud Platform Foundation Benchmark	IAM & Admin	Ensure that there are only GCP-managed service account keys for each service account
52010	CIS Google Cloud Platform Foundation Benchmark	Storage	Ensure that object versioning is enabled on all the buckets Note: This control will be a part of next CIS release.
52023	CIS Google Cloud Platform Foundation Benchmark	Virtual Network	Ensure Private Google Access is enabled for all subnetwork in VPC Network
52024	CIS Google Cloud Platform Foundation Benchmark	Virtual Network	Ensure VPC Flow logs is enabled for every subnet in VPC Network
52030	CIS Google Cloud Platform Foundation Benchmark	Storage	Ensure that Cloud Storage bucket is not anonymously or publicly accessible
52031	CIS Google Cloud Platform Foundation Benchmark	Storage	Ensure that logging is enabled for Cloud storage buckets
52032	CIS Google Cloud Platform Foundation Benchmark	SQL	Ensure that Cloud SQL database instance requires all incoming connections to use SSL
52039	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure Kubernetes web UI / Dashboard is disabled
52040	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure `Automatic node repair` is enabled for Kubernetes Clusters
52041	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure Automatic node upgrades is enabled on Kubernetes Engine Clusters nodes
52043	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure Network policy is enabled on Kubernetes Engine Clusters
52045	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure Kubernetes Cluster is created with Alias IP ranges enabled
52046	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure PodSecurityPolicy controller is enabled on the Kubernetes Engine Clusters
52047	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure Kubernetes Cluster is created with Private cluster enabled
52049	CIS Google Cloud Platform Foundation Benchmark	Kubernetes Engine	Ensure default Service account is not used for Project access in Kubernetes Clusters

Controls Updated

Additionally, we have updated the following existing controls.

CID	Policy	Resource	Control Title
21	CIS AWS Policy	CloudTrail	Ensure the S3 bucket CloudTrail logs to is not publicly accessible (Change in Bucket policy part).
26	CIS AWS Policy	KMS	Ensure rotation is enabled for customer created CMK with AWS managed key material (Update in control logic).
28	CIS AWS Policy	CloudTrail	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA.
46	AWS Best Practices	S3	S3 Bucket Policy Grant Access to Everyone.
50028	CIS Microsoft Azure Foundations Benchmark	SQL Servers	Ensure that Advanced Data Security is enabled and Threat Detection is configured properly for a SQL server.

Reports Now Supported

You can now configure a report template and generate mandate and policy based reports to get the complete picture of the compliance posture of your AWS account.

Currently, we support report generation for policies and mandates only for AWS. The mandates we support are:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Cloud Control Matrix (CCM)
- ISO/IEC 27001:2013

Report Template and Reports

Create a custom template for the reports by telling us the settings. The report templates are saved and available to you. Every time you want to view the report, just select Run Report from the quick actions menu.

You can edit the report template to reconfigure or change the report settings. Depending on the criteria you define in the report template, you could generate two types of reports: Mandate Report and Policy Report.

Mandate Based Reporting

Mandates are regulatory requirements, best practice standards or compliance frameworks designed by Security/business driven certification communities and/or government bodies.

Launch the Mandate Based Report to view the compliance posture of the organization against selected Mandates. This allows you to choose any one mandates you have to comply with and get a view of compliance posture in terms of their selected policies.

The reports are meant only for viewing and currently, we do not support saving, downloading or publishing the reports.

Tell me the Steps

It's easy to create a custom report template.

1) Just go to Reports > Create New Template.

2) Provide a title and description (optional) to the report template.

3) Select the Mandate in the report type and then click Next.

-Select the Policy from the drop-down. You can select multiple policies.

-Select the Mandate from the drop-down. You can select only one mandate.

4) Select the account or connector you want to evaluate for compliance.

The screenshot shows the CloudView interface. At the top, the 'REPORTS' tab is selected. Below it, the 'Report Templates' section has a 'Create New Template' button circled in red with a red '1' next to it. The 'Create New Template' form is displayed, showing 'Step 1 of 3' with 'Basic Information' selected. The form fields are: 'Report Title' (My Custom Report Template, marked with a red '2'), 'Report Description' (Example Report), 'Report Type' (Mandate selected), 'Select Policies' (AWS Best Practices Policy, marked with a red '3'), 'Select Mandate' (Cloud Controls Matrix (CCM)), and 'Select Format' (On-Screen Report). A note at the bottom states: 'The On-Screen Report displays the latest data and is available only for viewing. The On-Screen Report cannot be saved.' Below the form is an 'Add Accounts' modal window showing a table of connectors.

CONNECTOR NAME	ACCOUNT ID	STATE
<input checked="" type="checkbox"/> My Sample Connec...	222222222222	Regions Discovered Last Synced On April 11, 2019 1:54 PM
<input checked="" type="checkbox"/> Example Connector	111111111111	Success Last Synced On April 11, 2019 1:55 PM
Test Connector aws	333333333333	Success Last Synced On April 11, 2019 1:55 PM

5) Review the configured report template settings in the Summary and then click Create Template and Run Report.

← Create New Template

Step 3 of 3

- 1 Basic Information
- 2 Accounts
- 3 Summary

Summary

Review the report configuration options.

Basic Information

TITLE:	My Custom Report Template
DESCRIPTION:	Example Report
POLICY:	AWS Best Practices Policy
MANDATE:	Cloud Controls Matrix (CCM)
FORMAT:	On-Screen Report

Accounts

ACCOUNTS: My Sample Connector (), Example Connector ()

The On-Screen Report displays the latest data and is available only for viewing. The On-Screen Report cannot be saved.

Cancel Previous **Create Template and Run Report** 5

Policy Based Report

Policies are set of controls. We provide ability to generate policy specific compliance report.

Similar to the steps for mandate based report, you could generate the policy based report by selecting appropriate policy and the account to be evaluated for compliance posture.

Automatic Connector Creation in AssetView Enabled

We now support automatic connector creation in AssetView module when you create or edit a connector in CloudView module.

Steps for New Connector

Go to the Configuration > Amazon Web Services and then click Create Connector.

← Create AWS Connector

Connector Details

Give your connector a name and provide a description (optional).

Name Required

Description

My AWS Connector

Specify cross account ARN

Follow steps on the right to create an IAM role in AWS that will give Qualys cross-account access to your AWS resources. Then enter the Role ARN below. Tip - You'll need the Qualys AWS account ID and external ID to complete the steps.

Qualys AWS ID External ID Required

205767712 Copy 1561809330969 Copy

Role ARN Required

e.g. arn:aws:iam::111111111111:role/testRole

☐ Create Connector in AssetView New Option

Select to automate creation of same connector in AssetView. Ensure that your account has the required permissions in AssetView module for the connector to be created in AssetView.

Cancel Create Connector

Selecting this check box will ensure that a replica of the current connector is created and available in AssetView module. This will save the efforts of connector creation steps in AssetView module.

Pre-requisite Permission: User needs access to EC2 Connector page in AssetView module and 'Manage Asset Data Connectors' permission enabled in AssetView permissions.

You could enable this option for an existing connector as well.

Steps for Existing Connectors

Go to Configuration > Amazon Web Services and select the connector for which you would want to enable the option. From the quick actions menu, select View and go to Connector Information tab and click Edit.

The screenshot shows the 'Connector Summary: Example Connector' page. On the left is a 'View Mode' sidebar with 'Connector Summary', 'Connector Information', and 'Last Job Summary'. The main content area is titled 'aws Cloud Connector Information'. It contains a table of connector details and a form for editing. A red arrow points from the text 'Click Edit' to the 'Edit' button in the top right corner. Another red circle highlights the 'Create Connector in AssetView' checkbox, with the text 'New Option' next to it.

← Connector Summary: Example Connector

View Mode

- Connector Summary
- Connector Information
- Last Job Summary

aws Cloud Connector Information

Connector Name:	Example Connector
Description:	
Qualys AWS ID:	205
External ID:	154
ARN:	arn:
Connector ID:	5a4
Connector created in AV:	false

Edit Connector [X]

Connector Details

Connector Name Required
Example Connector

Description

Authorization Details

Qualys AWS ID
205767712 [Copy](#)

External ID Required
1541059434508 [Copy](#)

Cross Account ARN Required
arn:aws:iam::383031258652:role/QualysCloudViewRole_1


☐ Create Connector in AssetView **New Option**

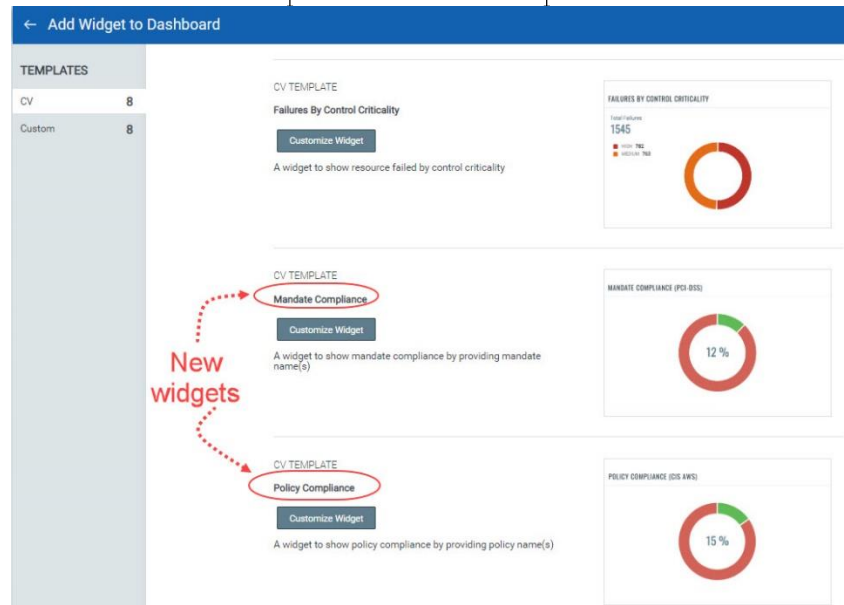
Select to automate creation of same connector in AssetView. Ensure that your account has the required permissions in AssetView module for the connector to be created in AssetView.

[Cancel](#) [Save](#)

New Widgets in Dashboard for Mandates and Policies

We have now introduced new widgets that you can add to your dashboard to get a quick glimpse of your mandate and policy posture.

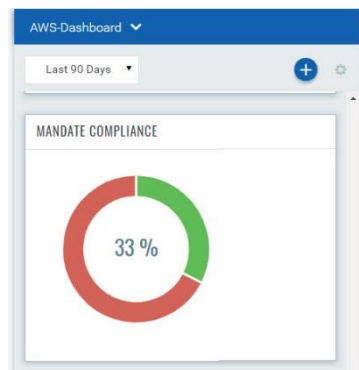
Go to Dashboards and click  (Add widget) icon and select the required widget template. Let us consider the example of mandate compliance. Click Customize Widget.



The query for the widget is predefined. You could modify the query as per your need and generate the customized widget.

You could also view the preview the widget by clicking Test and Preview button before you click Add to the dashboard.

Mandate Widget



The mandate widget tells you the evaluation of resources in your AWS account against the selected mandates.

The green part refers to the pass percentage while the red part tells you the percentage of failed resources.

Policy Widget



The policy widget tells you the evaluation of the resources in your AWS account against the selected policies.

The green part refers to the pass percentage while the red part tells you the percentage of failed resources.