Qualys CloudView v1.x

Version 1.22.0

March 28, 2022

Here's what's new in Qualys CloudView 1.22.0!

Amazon Web Services

New controls for AWS Best Practices Policy
New controls for AWS Lambda Best Practices Policy
New controls for AWS Database Service Best Practices Policy
Permissions Needed for Lambda, EBS, EMR, Glue, and GuardDuty Resources
Creating User-Defined Control

Microsoft Azure

New controls for CIS Microsoft Azure Foundations Benchmark Policy
New controls for Azure Best Practices Policy

Google Cloud Platform

New controls for GCP Best Practices Policy

Qualys CloudView 1.22 brings you many more Improvements and updates! Learn more

Amazon Web Services

New controls for AWS Best Practices Policy

We have introduced the following new controls for AWS Best Practices Policy.

CID	Service	Resource	Title
339	EC2	EBS	Ensure EBS default encryption is enabled with customer managed key
332	Glue	Glue Data Catalog	Ensure Glue Data Catalog Encryption is enabled with SSE-KMS with customer-managed keys
273	EMR	EMR	Ensure block public access is enabled so that no port should have public access for EMR clusters
387	GuardDuty	GuardDuty	Ensure GuardDuty is enabled to specific org/region
294	KMS	KMS	Ensure KMS key policy does not contain wildcard (*) principal
289	VPC	VPC Security Group	Ensure every security groups rule has a description
322	EC2	EC2 Instance	Ensure Instance Metadata Service Version 1 is not enabled
323	MSK	MSK Cluster	Ensure MSK Cluster logging is enabled
399	IAM	IAM_USER	Ensure that all IAM users are members of at least one IAM group.
400	IAM	IAM_USER	Ensure an IAM User does not have access to the console
426	API Gateway	Rest API Gateway	Ensure Amazon API Gateway REST APIs are protected by AWS WAF
427	API Gateway	Rest API Gateway	Ensure client-side SSL certificates are used for HTTP backend authentication in AWS API Gateway REST APIs
428	API Gateway	Rest API Gateway	Ensure that SSL certificates associated with API Gateway REST APIs are rotated periodically
419	Cloudfront	Cloudfront	Ensure that AWS CloudFront distribution origins do not use insecure SSL protocols
429	Cloudfront	Cloudfront	Ensure AWS CloudFront distributions use improved security policies for HTTPS connections

CID	Service	Resource	Title
430	Cloudfront	Cloudfront	Ensure the traffic between the AWS CloudFront distributions and their origins is encrypted
431	Cloudfront	Cloudfront	Ensure your AWS Cloudfront distributions are using an origin access identity for their origin S3 buckets
433	EC2	EC2	Ensure EC2 Instances are using IAM Roles
434	EC2	EC2	Ensure no backend EC2 instances are running in public subnets
437	EC2	EC2	Ensure unused AWS EC2 key pairs are decommissioned.
439	EFS	EFS	Ensure that Elastic File System has restricted access and permissions
440	ElastiCache	ElastiCache	Ensure that the latest version of Memcached is used for AWS ElastiCache clusters
443	Route53	Route53	Ensure that Route 53 Hosted Zone has configured logging for DNS queries
444	Route53	Route53	Ensure that DNSSEC Signing is enabled for Route 53 Hosted Zones
445	Route53	Route53	Ensure that Route 53 domains have Privacy Protection enabled

New controls for AWS Lambda Best Practices Policy

We have introduced the following new controls for AWS Lambda Best Practices Policy.

CID	Service	Resource	Title
442	Lambda	Lambda	Ensure that your Amazon Lambda functions are configured to use enhanced monitoring
343	Lambda	Lambda	Ensure that AWS Lambda function is configured for function-level concurrent execution limit
344	Lambda	Lambda	Ensure that AWS Lambda function is configured for a Dead Letter Queue (DLQ)

New controls for AWS Database Service Best Practices Policy

We have introduced the following new controls for AWS Database Service Best Practices Policy.

CID	Service	Resource	Title
432	DynamoDB	DynamoDB	Ensure that your Amazon DynamoDB tables are using backup and restore

Permissions Needed for Lambda, EBS, EMR, Glue, and GuardDuty Resources

The cross-account role associated with the AWS connector needs additional permissions to fetch information about Lambda, EBS, EMR, Glue, and GuardDuty resources. To fetch information about these resources in your cloud environment, you need to assign these additional permissions to the IAM role associated with the AWS connector.

You can create a new policy with the required permissions and attach the policy to the IAM role associated with the AWS connector. The detailed steps for policy creation and associating with the IAM role are listed in the CloudView online help.

Creating User-Defined Control

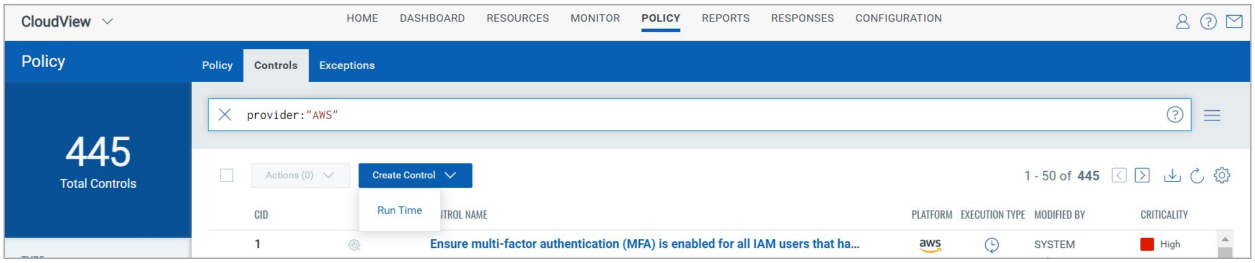
We have now introduced a new application Qualys Flow that allows you to create workflows (QFlows). You can create a customized control using the workflows created in the Qualys Flow application. Currently, we provide customization only for AWS.

You need specific permissions in CloudView and Qualys Flow applications for control customization. The details are listed in the Manage Custom Control Permissions section of the CloudView online help.

Customize Control Creation

Before you create a custom control, you need to create a QFlow in Qualys Flow application. To know the detailed steps, refer to Qualys Flow Getting Started Guide.

You can create a customized control using the QFlows created in Qualys Flow application. Go to **Policy** > **Controls** > **Amazon Web Services**. Click Create **Control** > **Run Time**.

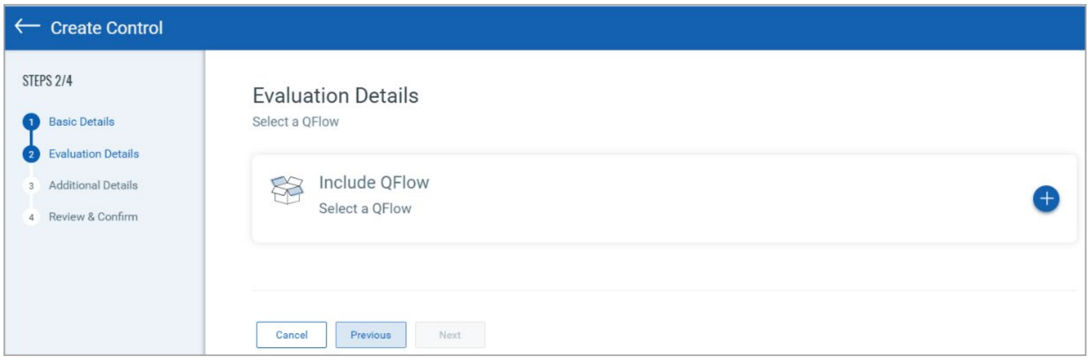


provider:"AWS"

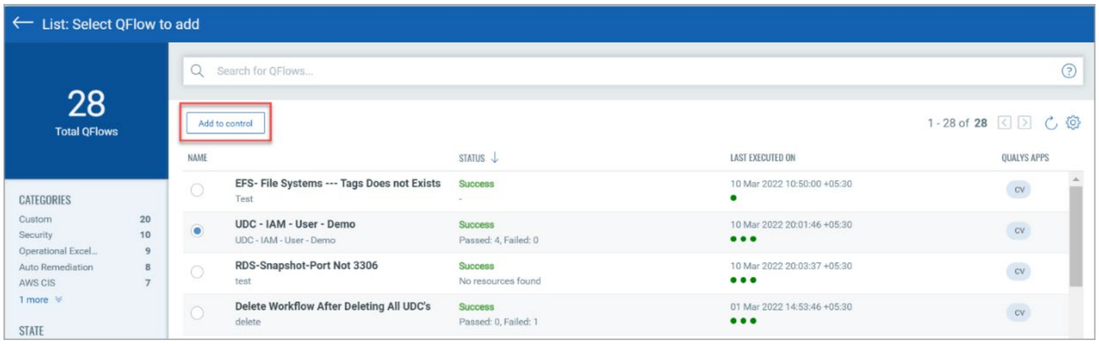
CID		...TROL NAME	PLATFORM	EXECUTION TYPE	MODIFIED BY	CRITICALITY
1		Ensure multi-factor authentication (MFA) is enabled for all IAM users that ha...	aws		SYSTEM	🟥 High

Provide the basic details for the control such as Name, Description, and Criticality, and click Next.

Click ⊕ icon to include QFlow that is created in Qualys Flow app.



Select the QFlow from the list, and click **Add to control**.



CATEGORIES	
Custom	20
Security	10
Operational Excel...	9
Auto Remediation	8
AWS CIS	7
1 more	

STATE

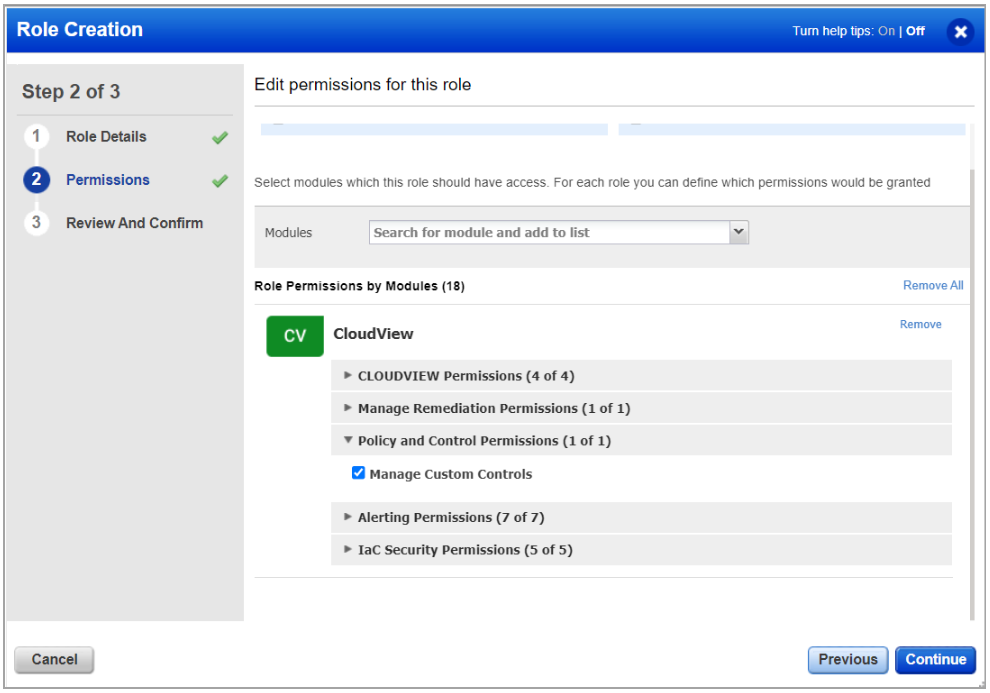
	NAME	STATUS	LAST EXECUTED ON	QUALYS APPS
○	EFS- File Systems --- Tags Does not Exists Test	Success -	10 Mar 2022 10:50:00 +05:30 ●	CV
●	UDC - IAM - User - Demo UDC - IAM - User - Demo	Success Passed: 4, Failed: 0	10 Mar 2022 20:01:46 +05:30 ●●●	CV
○	RDS-Snapshot-Port Not 3306 test	Success No resources found	10 Mar 2022 20:03:37 +05:30 ●●●	CV
○	Delete Workflow After Deleting All UDC's delete	Success Passed: 0, Failed: 1	01 Mar 2022 14:53:46 +05:30 ●●●	CV

Once the QFlow is added to the control, provide additional details, review the details, and click Create Control.

You can associate this control to a user-defined policy to be evaluated for the custom policy.

Required Permissions

We have added new permissions to allow you to create user-defined control. The Manage Custom Control under the Policy and Control Permissions must be enabled to create new user-defined controls, create a copy of an existing run-time control, and delete user-defined controls.



Edit permissions for this role

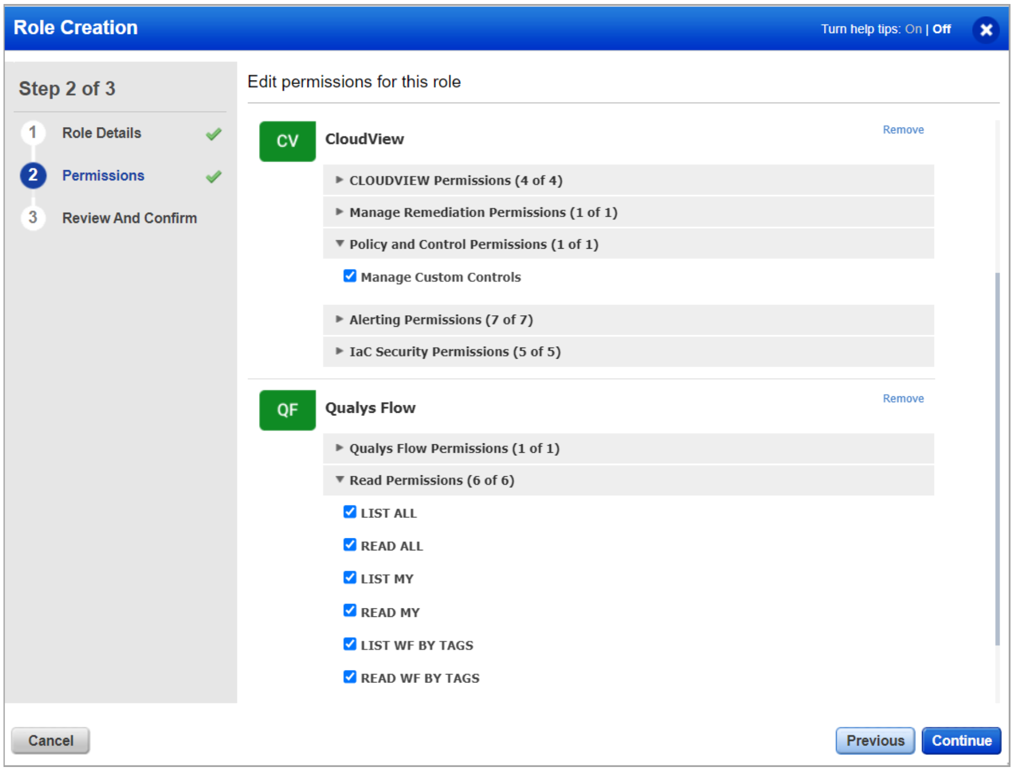
Select modules which this role should have access. For each role you can define which permissions would be granted

Role Permissions by Modules (18)

CloudView

- CLOUDVIEW Permissions (4 of 4)
- Manage Remediation Permissions (1 of 1)
- Policy and Control Permissions (1 of 1)
  - ☑ Manage Custom Controls
- Alerting Permissions (7 of 7)
- IaC Security Permissions (5 of 5)

For creating QFlow-based control, the Read Permissions must be enabled in Qualys Flow application.



Edit permissions for this role

CloudView

- ▸ CLOUDVIEW Permissions (4 of 4)
- ▸ Manage Remediation Permissions (1 of 1)
- ▾ Policy and Control Permissions (1 of 1)
  - ☑ Manage Custom Controls
- ▸ Alerting Permissions (7 of 7)
- ▸ IaC Security Permissions (5 of 5)

Qualys Flow

- ▸ Qualys Flow Permissions (1 of 1)
- ▾ Read Permissions (6 of 6)
  - ☑ LIST ALL
  - ☑ READ ALL
  - ☑ LIST MY
  - ☑ READ MY
  - ☑ LIST WF BY TAGS
  - ☑ READ WF BY TAGS

New Tokens

We have added the following search tokens to find customized controls that are created using QFlows.

- qflow.name to find controls created from QFlow with the specified name.
- qflow.id to find controls created from QFlow with specified QFlow Uuid.

Microsoft Azure

New controls for CIS Microsoft Azure Foundations Benchmark Policy

We have introduced the following new controls for CIS Microsoft Azure Foundations Benchmark Policy.

CID	Service	Resource	Title
50336	Storage Account	Storage Account	Ensure That Storage Account Access Keys are Periodically Regenerated
50313	Azure SQL	SQL server	Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account
50314	Azure SQL	SQL server	Ensure that Vulnerability Assessment setting 'Periodic recurring scans' to 'on' for each SQL server
50315	Azure SQL	SQL server	Ensure that Vulnerability Assessment setting 'Send scan reports to' is configured for a SQL server
50321	Azure SQL	SQL server	Ensure that Vulnerability Assessment Setting 'Also send email notifications to admins and subscription owners' is Set for Each SQL Server
50335	MYSQL Flexible Server	MYSQL Flexible Server	Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server

New controls for Azure Best Practices Policy

We have introduced the following new controls for Azure Best Practices Policy.

CID	Service	Resource	Title
50334	Spring Cloud	Spring Cloud	Ensure that Diagnostic settings is enabled for azure spring cloud resource service
50333	Spring Cloud	Spring Cloud	Ensure that Application Insights are enabled for azure spring cloud service
50331	Spring Cloud	Spring Cloud App	Ensure that azure spring cloud service apps have end to end TLS enabled
50332	Spring Cloud	Spring Cloud App	Ensure that azure spring cloud service apps have HTTPS enabled

CID	Service	Resource	Title
50329	Application Insights	Application Insights	Ensure that Application Insights components block log ingestion and querying from public networks
50328	Application Insights	Application Insights	Ensure that Classic Application Insights retention Period is 90 days or more
50327	Load Balancer	Load Balancer	Ensure that SKU of the load balancer is Standard
50330	CDN	CDN Endpoint	Ensure that protocol used by CDN profile endpoints is HTTPS
50324	Web Application Firewall	Front Door WAF	Ensure that Front Door WAF prevents message lookup in Log4j2
50325	Web Application Firewall	WAF web Policy	Ensure that Application Gateway WAF prevents message lookup in Log4j2
50339	App Service	Web App	Ensure that App Services web applications have always-on feature enabled
50340	Azure Image	Azure Image	Ensure zone resiliency is turned on for all Azure Image
50341	App Service	Web App	Ensure web sockets are disabled for Azure App Service
50342	Azure Image	Azure Image	Ensure 'ReadOnly' cache is enabled on OS disks with read heavy operations to get higher read IOPS for Azure Image
50344	App Service	Web App	Ensure that IP restriction rules are configured for Azure App Service
50345	Azure Synapse Analytics	Synapse Workspace	Ensure data exfiltration protection is enabled for Azure Synapse Workspace
50346	Azure Image	Azure Image	Ensure Hyper-V generation uses v2 for Azure Image
50347	Azure Cache For Redis	Redis Cache	Ensure firewall rules reject internet access for Azure Redis Cache
50348	Azure Synapse Analytics	Synapse Workspace	Ensure that public network access is disabled for Azure Synapse Workspace

Google Cloud Platform

New controls for GCP Best Practices Policy

We have introduced the following control for GCP Best Practices Policy.

CID	Service	Resource	Title
52168	Network Security	Cloud Armor	Ensure that Cloud Armor prevents message lookup in Log4j2

Issues addressed in this release

- We have now fixed an issue where the region field was getting incorrectly set for account-level controls in reports.