Qualys Flow

Getting Started Guide

February 12, 2024

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

Table of Contents

Introduction Qualys Flow

Thank you for your interest in the Qualys Flow application. Qualys Flow is a low-code/no-code cloud management platform that provides the ability to create customized workflows named QFlows within a few clicks. You can create a runtime custom control for AWS in the TotalCloud application.

You can create automation (QFlows) to achieve specific/use case based requirements without the knowledge of scripts. You can create a Security Orchestration Automation and Response (SOAR) playbook with QFlow.

A QFlow is a logical flow of events, data, and actions to get a specific output like an insight, a compliance check, a report, remediation, or an action. Qualys Flow helps in the automation of the cloud management process. You can build a QFlow using different nodes. Nodes are building blocks of a QFlow. Each node is used to perform a specific function such as collect AWS Inventory, AWS Action, data formatting etc. You can choose the specific node to perform the desired function.

With Qualys Flow, you can create

-a runtime custom control for AWS in the TotalCloud application.

-automation (QFlows) to achieve specific/use case-based requirements without the knowledge of scripts.

-a Security Orchestration Automation and Response (SOAR) playbook with QFlow.For example, the resource node decides which data should be fetched for modification; the action node decides the action that should be taken on selected data.

For example, the resource node decides which data should be fetched for modification; the action node decides the action that should be taken on selected data

Concepts and Terminologies

Get familiar with common terms used in the Qualys Flow application.

Terms	Description
QFlow	It is a logical flow of events, data, and actions in the form of nodes
Nodes	Basic building blocks of a QFlow
SOAR	Security Orchestration Automation and Response (SOAR) technology helps to coordinate, execute and automate tasks between different Qualys applications
Variables	Allow you to use the QFlow flexibly by using or overriding the values used throughout from a single place
Execution History	It is to view details of the status of nodes
Addons	It is used to add the additional resources data and filters

Get Started

You can create QFlows with the specific requirement in the Qualys Flow application. Using QFlows, you can create user-defined control (UDC) in TotalCloud or other integrated applications.

Know the Requirements

You can access the Qualys Flow application if you have TotalCloud and VMDR applications enabled for you.

User Roles and Permissions

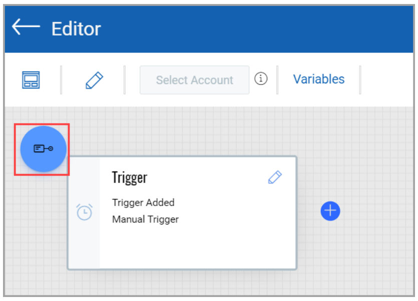
Each user has a predefined role that determines the actions they can perform. The Manager user has full privileges and permissions to create, execute, deploy, and delete the QFlows. The Manager user can grant permissions or roles to the sub-users based on the requirement.

Role	User Permissions
Manager	Full access to all permissions.
Qualys Flow Admin (CWE)	Create, edit, execute, delete, or deploy all the QFlows. List, read, assign tags, or remove tags for all the QFlows available in the account. Export, Import and clone QFlows.
Power Developer	Create, edit, execute, delete, or deploy their own QFlows. List, read, assign tags, remove tags for their own QFlows.
Developer	Create, edit, execute, or delete their own QFlows. List, read, assign tags, or remove tags for their own QFlows .
Deployer	List, read, execute, or deploy all the QFlows by using tags assigned by the Manager user.
Reader	List and read all the QFlows by using tags assigned by the Manager user.

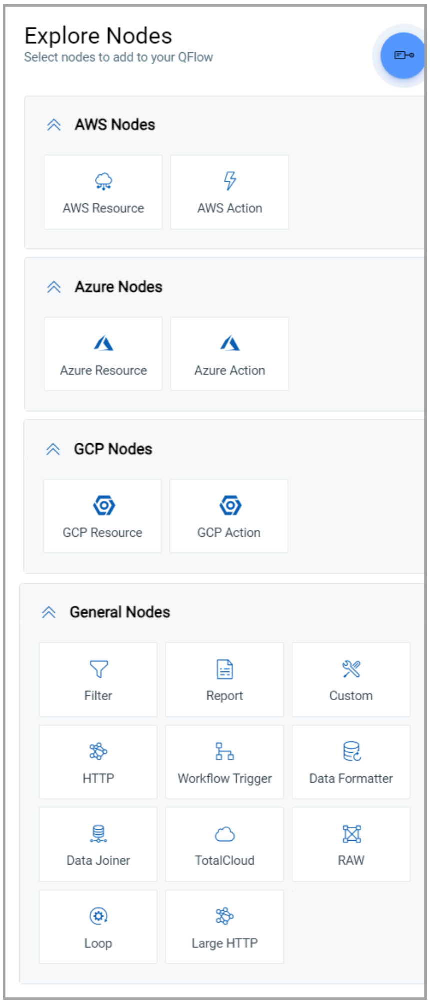
Know the Nodes

Qualys Flow application categorizes nodes based on the type of function they perform.

To access the nodes, log in to your Qualys Flow account. Go to the **EDITOR** tab and click the explore nodes icon located at the top left corner of Editor window.



The Explore Nodes pop-up window is displayed.



To know the function of these nodes, refer to the following table.

Node	Function
Trigger	By default, is the first node present in the editor for any QFlow. The trigger can be time-based, AWS event-based, manual, or TotalCloud control. **Schedule**: Use this option to trigger the QFlow at specific times. **Manual**: Use this option to trigger the QFlow at any instance of time by clicking the Run Now button. By default, the trigger is set to manual. **TotalCloud**: Use this option to sync the trigger of the QFlow with the trigger of the CSPM connector. **Event**: Use this option to trigger the workflow in response to AWS cloud events and connector CRUD events. The Events trigger works when the rule is configured at the event bridge of your AWS account.
AWS Nodes (Cloud-Specific Nodes)	
AWS Resource	It fetches the resources that belong to a specific AWS service. The node can access all AWS resources and AWS services available to you. For example, you can select the RDS service and use DB instances as a method in the AWS resource node to identify all available RDS DB instances.
AWS Action	It performs the action that you define in the selected resources; the actual automation is accomplished in this node. For example, after identifying the list of publicly available RDS DB instances, you can perform the action to delete those instances.
Azure Nodes (Cloud-Specific Nodes)	
Azure Resource	It fetches the resources that belong to a specific Azure service. The node can access all Azure services and resources available to you. It fetches all the resources provided by Azure Software Development Kit (SDK) that belong to a specific Azure service.
Azure Action	It performs the action you define on the selected resources; the actual automation is accomplished in this node. It performs all the actions that are part of Azure SDK defined in the selected resources.
GCP Nodes (Cloud-Specific Nodes)	
GCP Resource	It fetches the resources that belong to a specific GCP service. The node can access all GCP services and resources available to you. For example, you can select the Google Compute Engine for service, Instances for resources, and the specific API that you want to execute (For example, List to get all the VM instances under Google Compute Engine
GCP Action	It performs the action you define on the selected resources; the actual automation is accomplished in this node. The GCP Action node can perform any action that is available for a resource, in the GCP SDK.

General Nodes	
Filter	It performs filtering of the resources based on a set of conditions. You can combine criteria using logical AND/OR conditions to filter this data. For example, you can filter publicly available RDS DB instances from all RDS DB instances using the Filter node. Use the following filters based on various fields: **Param**: To filter the data based on metadata. **Date**: To filter the data based on a date, like resources created in the last 30 days. **Tags**: To filter the data based on tags. **Security Group**: To filter the data based on security group. **Netwrok ACLs**: To filter the data based on Access Control lists. **Function**: To filter the data based on functions. You can create functions using java codes.
Report	It allows users to generate and download reports of the selected data in CSV or JSON format.
Custom	It is used to write scripts to create complex filters, customize the selected data, data transformation like xml to json, etc. It supports javascript code, and some libraries of nodes.
HTTP	It makes HTTP(S) calls from a QFlow. This allows you to integrate with the third-party application or service that has an HTTP endpoint via API Calls. You can place the HTTP node anywhere in the QFlow.
Data Formatter	It takes in the output of the previous node as input and allows to format it as per requirement.
Data Joiner	It joins data from two previous nodes.
TotalCloud	It is the TotalCloud-specific node. When you want to use QFlow in the TotalCloud application, you need to add the TotalCloud node.
RAW	It is an API node that allows you to call any API function supported by the cloud service platform and perform the action on the resources.
Loop	It executes the defined process. It evaluates the exit expression or number of loops before determining to run again or move to the next node. This Loop node runs the defined process at least once, regardless of previous activities. You can select the number of loops from 1 and 10.
Large HTTP	It allows you to integrate the third-party application with an HTTP endpoint. Large HTTP nodes can be used to call APIs that return a large amount of data.

Creating QFlows

Using Qualys Flow application, you can create QFlows in two ways:

using a template or

using the editor (from scratch).

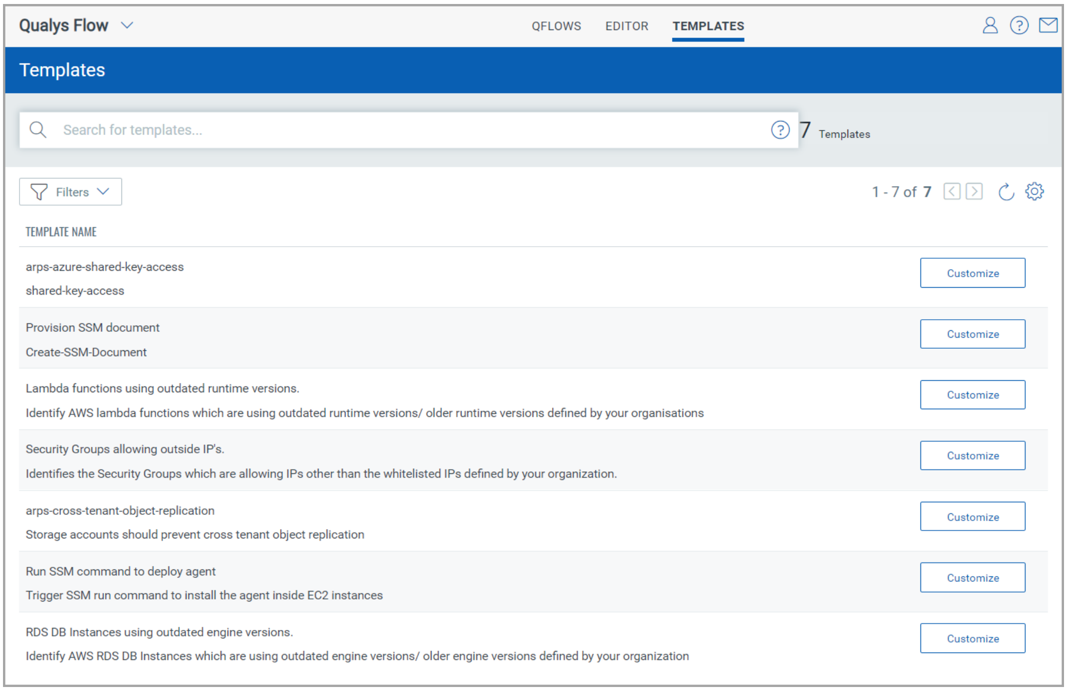
Creating a QFlow from a Template

You can use any suitable templates available for creating your own QFlow. You can select a template to adopt the QFlow. Let us take one use case, you want to identify the Security Groups which are allowing IPs other than the allowed IP's defined by your organization. You can directly use the template; you need to select the account and region and click Save. You can customize this template to suit your requirement.

For this QFlow you can use the **Security Group allowing outside IP's** template.

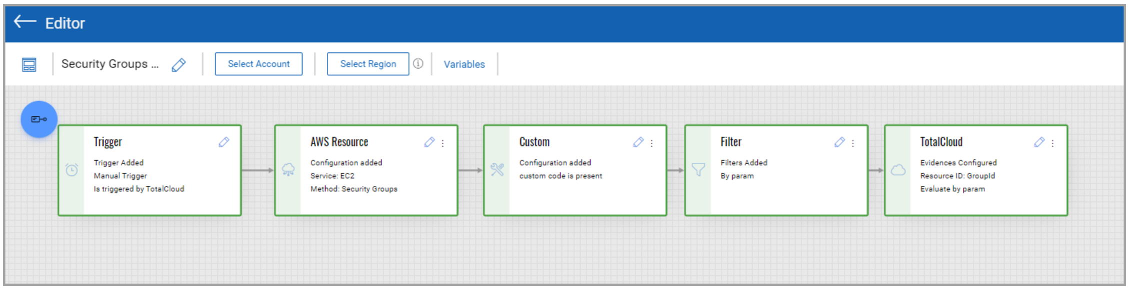
1. Navigate to **QFlows** tab > **Create QFlow** > **Using a template**.

2. Click **Select** to use the Security Group allowing outside IP's template.



TEMPLATE NAME	
arps-azure-shared-key-access shared-key-access	Customize
Provision SSM document Create-SSM-Document	Customize
Lambda functions using outdated runtime versions. Identify AWS lambda functions which are using outdated runtime versions/ older runtime versions defined by your organisations	Customize
Security Groups allowing outside IP's. Identifies the Security Groups which are allowing IPs other than the whitelisted IPs defined by your organization.	Customize
arps-cross-tenant-object-replication Storage accounts should prevent cross tenant object replication	Customize
Run SSM command to deploy agent Trigger SSM run command to install the agent inside EC2 instances	Customize
RDS DB Instances using outdated engine versions. Identify AWS RDS DB Instances which are using outdated engine versions/ older engine versions defined by your organization	Customize

The QFlow Template is displayed.



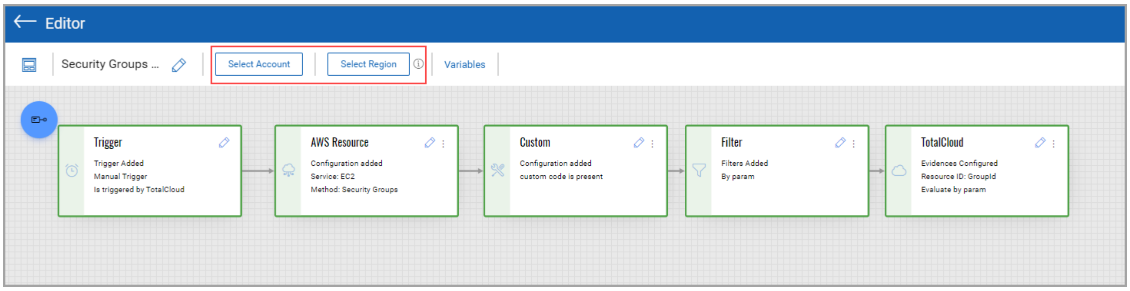
3. Select the account and a region to verify with a single account and region.

Tip: Qualys recommends to test and verify the QFlow with a single account and region before applying it to multiple accounts and regions. Once you are satisfied with the QFlow and outcome, you can deploy the QFlow on multiple accounts and regions.

The account and regions that are present in your subscription are populated while selecting account and region.

- Click **Select Account** to choose the account from the list, and then click **Apply**.

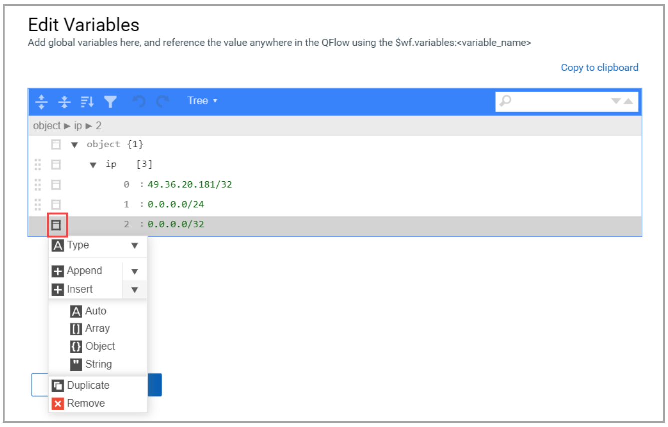
- Click **Select Region** to choose the region from the list, and then click **Apply**.



You can customize the QFlow as per your need. You can customize variables. You can add global variables and use this value as a reference anywhere in the QFlow using the $wf.variables:<variable_name>s.

Variable Type	Description
Auto	It automatically determined from the value and can be a string, number, boolean, or null
Array	It contains an ordered collection of values
Object	It contains an unordered set of key/value pairs
String	Field type is not determined from the value but always returned as a string

You can perform various actions on variables like Append, Insert, Duplicate, or Remove.



Edit Variables

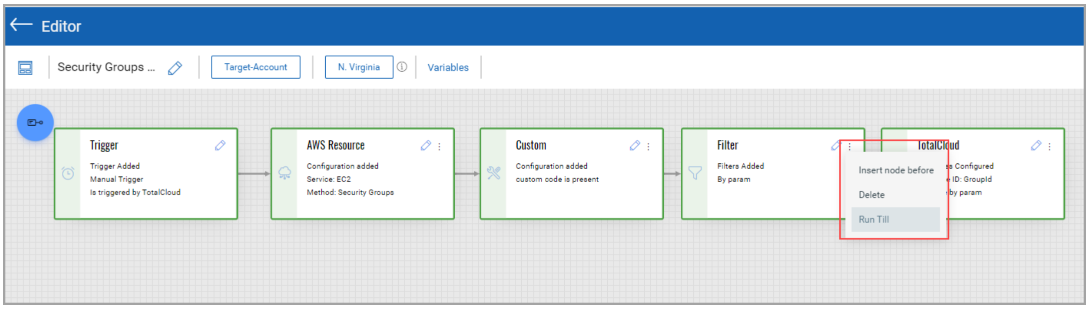
Add global variables here, and reference the value anywhere in the QFlow using the $wf.variables:<variable_name>

```
object ▶ ip ▶ 2
▼ object {1}
  ▼ ip   [3]
        0 : 49.36.20.181/32
        1 : 0.0.0.0/24
        2 : 0.0.0.0/32
```

4. Run and check the functionality of the node.

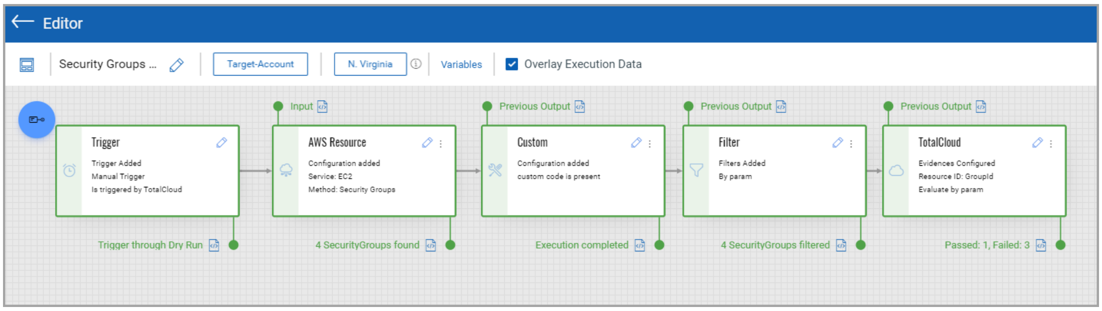
It is best practice to check the functionality of individual nodes before running the QFlow.

- Click the three dots present at the top right corner of the specific node to get the **Run till** option for running the QFlow till that specific node.

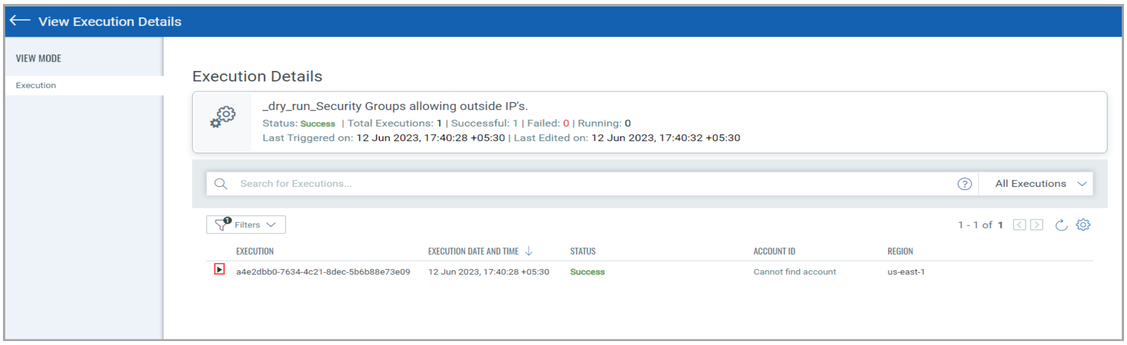


The status of the running of the QFlow is displayed. The status of the input and output of the node is displayed in green.

You can view the execution history by clicking the icon adjacent to status for the details of the node's output.



- Click the ▶ icon to view the details of execution details.

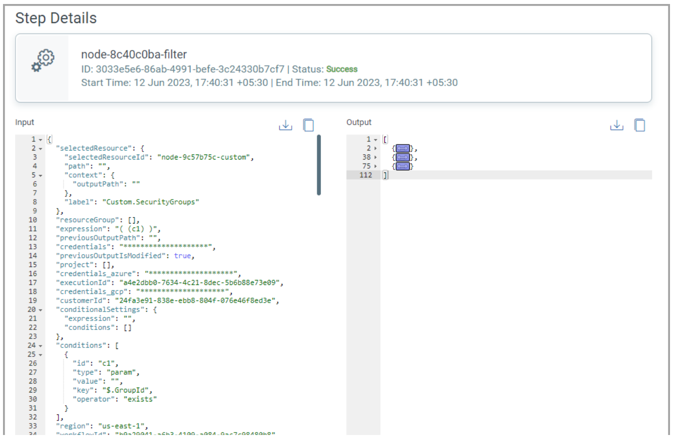


Execution Details

_dry_run_Security Groups allowing outside IP's.
Status: Success | Total Executions: 1 | Successful: 1 | Failed: 0 | Running: 0
Last Triggered on: 12 Jun 2023, 17:40:28 +05:30 | Last Edited on: 12 Jun 2023, 17:40:32 +05:30

	EXECUTION	EXECUTION DATE AND TIME	STATUS	ACCOUNT ID	REGION
▶	a4e2dbb0-7634-4c21-8dec-5b6b88e73e09	12 Jun 2023, 17:40:28 +05:30	Success	Cannot find account	us-east-1

For demonstration, we have shown the filter node's execution history. You can download the JSON file using icon or copy the JSON code in the clipboard using icon.



Step Details

node-8c40c0ba-filter
ID: 3033e5e6-86ab-4991-befe-3c24330b7cf7 | Status: Success
Start Time: 12 Jun 2023, 17:40:31 +05:30 | End Time: 12 Jun 2023, 17:40:31 +05:30

Input

```
{
  "selectedResource": {
    "selectedResourceId": "node-9c57b75c-custom",
    "path": "",
    "context": {
      "outputPath": ""
    },
    "label": "Custom.SecurityGroups"
  },
  "resourceGroup": [],
  "expression": "( (c1) )",
  "previousOutputPath": "",
  "credentials": "*******************",
  "previousOutputIsModified": true,
  "project": [],
  "credentials_azure": "*******************",
  "executionId": "a4e2dbb0-7634-4c21-8dec-5b6b88e73e09",
  "credentials_gcp": "*******************",
  "customerId": "24fa3e91-838e-ebb8-804f-076e46f8ed3e",
  "conditionalSettings": {
    "expression": "",
    "conditions": []
  },
  "conditions": [
    {
      "id": "c1",
      "type": "param",
      "value": "",
      "key": "$.GroupId",
      "operator": "exists"
    }
  ],
  "region": "us-east-1",
```

Output

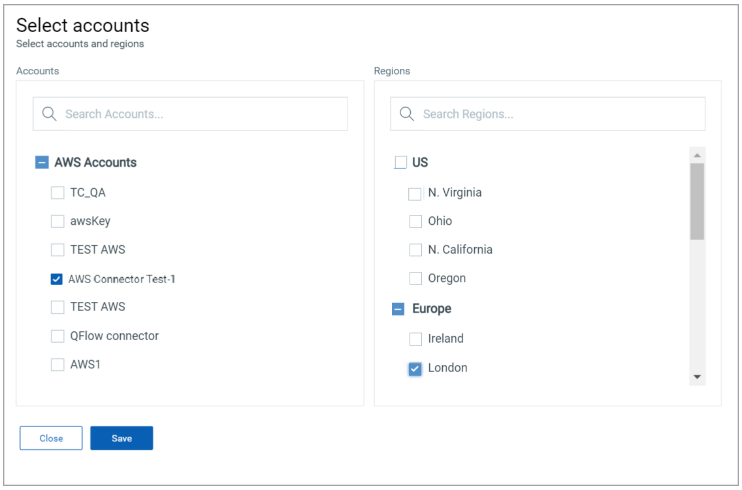
```
[
  {⋯},
  {⋯},
  {⋯}
]
```

Once you verify the functioning of your QFlow, you can save the QFlow.

5. To save the QFlow, click **Save**.

6. Associate your QFlow with AWS Accounts and Regions.

- Select the AWS **Accounts** and **Regions** from the list and click **Save**.



Select accounts

Select accounts and regions

Accounts

- ▬ AWS Accounts
  - □ TC_QA
  - □ awsKey
  - □ TEST AWS
  - ☑ AWS Connector Test-1
  - □ TEST AWS
  - □ QFlow connector
  - □ AWS1

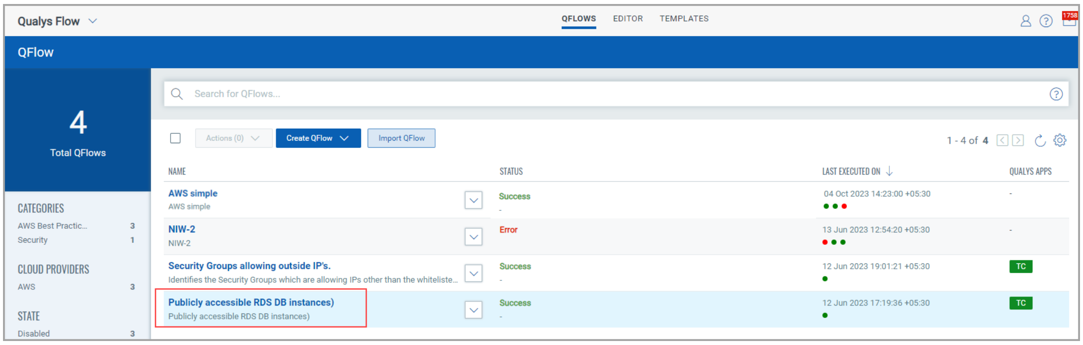
Regions

- □ US
  - □ N. Virginia
  - □ Ohio
  - □ N. California
  - □ Oregon
- ▬ Europe
  - □ Ireland
  - ☑ London

Your QFlow is ready. You can now create user-defined control in the TotalCloud application.

Viewing Your QFlows

You can view your created QFlow in the QFlows tab.



NAME	STATUS	LAST EXECUTED ON ↓	QUALYS APPS
AWS simple AWS simple	Success -	04 Oct 2023 14:23:00 +05:30 ●●●	-
NIW-2 NIW-2	Error	13 Jun 2023 12:54:20 +05:30 ●●●	-
Security Groups allowing outside IP's. Identifies the Security Groups which are allowing IPs other than the whiteliste...	Success -	12 Jun 2023 19:01:21 +05:30 ●	TC
Publicly accessible RDS DB instances) Publicly accessible RDS DB instances)	Success -	12 Jun 2023 17:19:36 +05:30 ●	TC

The QFlows tab displays the total count of QFlows at the top left corner and filters based on your created categories. From the search bar, you can search your QFlow by typing the name of your QFlow.

In the details of the QFlow, you can see status like Success, Never Executed, or Error. You can view the latest three execution of the QFlow with three color code dots.

Color Code	Description
Green	QFlow execution is successful
Red	QFlow execution is failed
Yellow	QFlow execution is running

Proceed with section Managing Your QFlows

Creating a QFlow from Scratch

1. Log in to your QFlow account. Navigate to **QFlows** tab > **Create QFlow** > **From scratch**. Add the basic details like the AWS Account's name and Description.

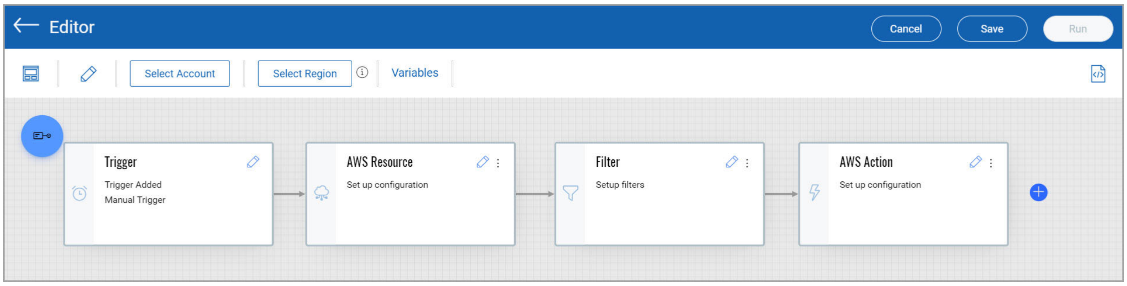
2. By default, the Trigger node is present as the first node in the QFlow. Configure the settings for the triggering.

3. Select the Resource node to get the resource from your cloud platform.

4. Select an AWS Account and a Region

5. Use Filter node to filter the resources to get specific output.

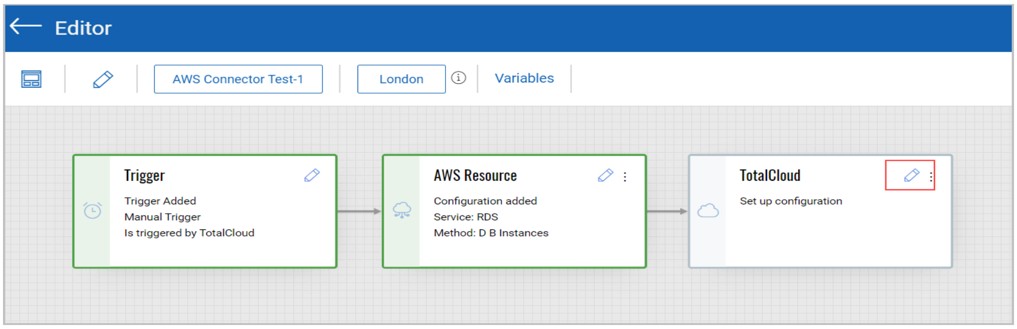
6. Use the Action node to remediate the filtered output if your QFlow executes the action.



Sample Example of Creating a QFlow

Let's create a QFlow to identify publicly accessible RDS DB instances.

For this QFlow, you need an AWS Resource node (accessing all RDS RB instances) and a TotalCloud node (filtering out publicly accessible RDS DB instances).



Following are the steps to create the QFlow.

Step 1: Add basic details

Step 2: Add a Triggering method

Step 3. Add a Resource Node

Step 4: Select an AWS Account and a Region

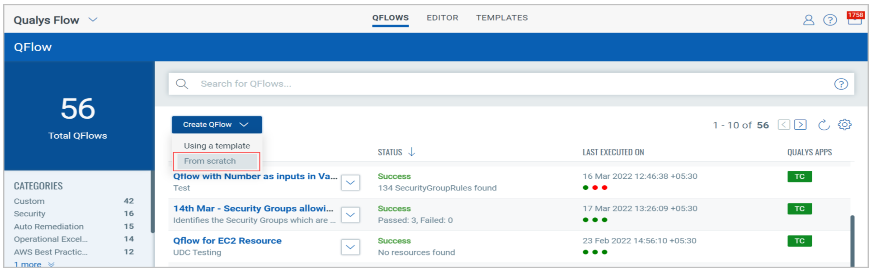
Step 5: Add the TotalCloud node

Step 6: Run and check the functionality of nodes

Step 1: Add basic details

1. Log in to your Qualys Flow account.

2. On the **QFlows** tab, go to **Create QFlow** and click **From scratch**.

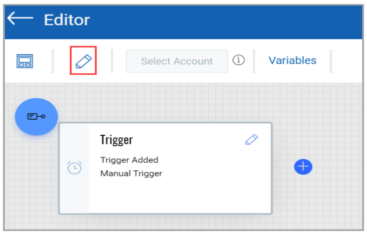


CATEGORIES

Custom	42
Security	16
Auto Remediation	15
Operational Excel...	14
AWS Best Practic...	12
1 more	

	STATUS	LAST EXECUTED ON	QUALYS APPS
Qflow with Number as inputs in Va... Test	Success 134 SecurityGroupRules found	16 Mar 2022 12:46:38 +05:30	TC
14th Mar - Security Groups allowi... Identifies the Security Groups which are ...	Success Passed: 3, Failed: 0	17 Mar 2022 13:26:09 +05:30	TC
Qflow for EC2 Resource UDC Testing	Success No resources found	23 Feb 2022 14:56:10 +05:30	TC

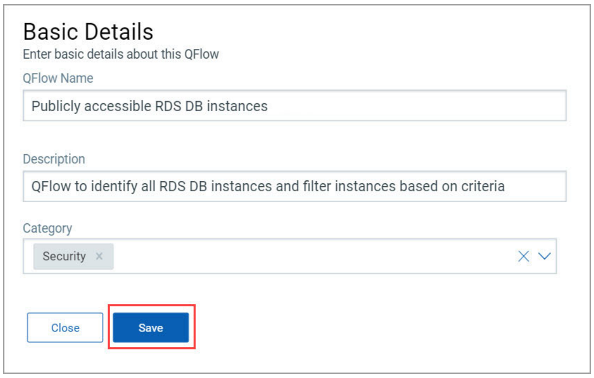
3. From the Editor window, click the ⊕ icon to enter the basic details of the QFlow.



4. Provide a **QFlow Name** and **Description** for your QFlow.

5. Select Security as **Category** from the list.

Note: You can select multiple categories from the list. These categories are filters you can apply while searching for specific QFlow among the multiple QFlow available on the QFlows tab.



Basic Details

Enter basic details about this QFlow

QFlow Name: Publicly accessible RDS DB instances

Description: QFlow to identify all RDS DB instances and filter instances based on criteria

Category: Security

Step 2: Add a Triggering method

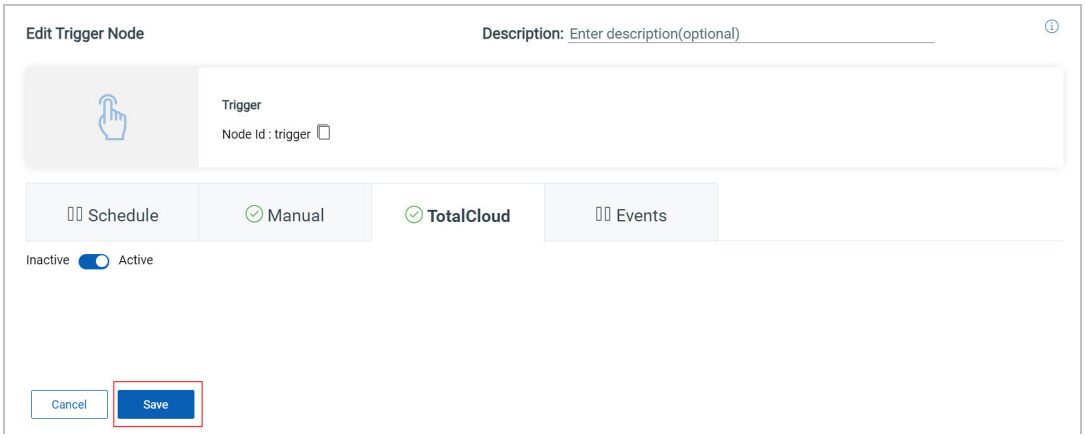
The Trigger node is the first node in any QFlow and is set to manual trigger by default. The Trigger node defines the time of the execution of the QFlow. You need to set it to TotalCloud. For more details on nodes, refer to Know the Nodes.

Note: At a later time, if you do not want to link your QFlow with the CSPM connector, you can set it to manual trigger; in this way, you can execute the QFlow manually as per your requirement.

1. Click the ✎ icon to input the trigger method.

The Edit Trigger Node pop-up window is displayed.

2. Click **TotalCloud** trigger, toggle to **Active** and click **Save**.



Edit Trigger Node

Description: Enter description(optional)

Trigger

Node Id : trigger

Inactive ● Active

Step 3. Add a Resource Node

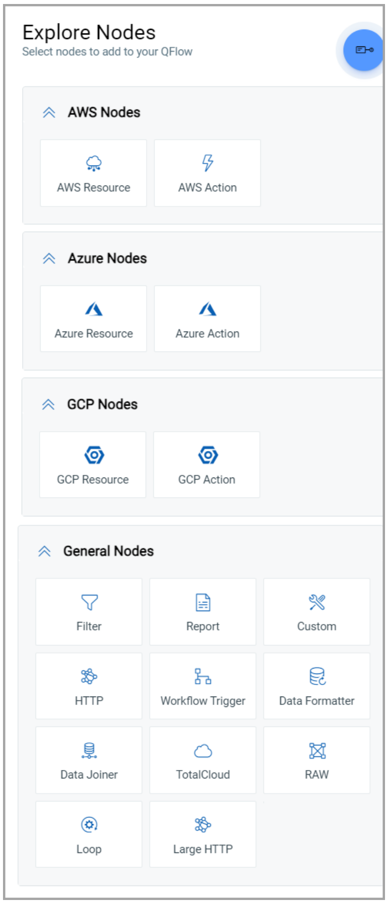
Use this node to select the resources for finding all DB instances. Set the configuration. For more details on nodes, refer to Know the Nodes.

To find out all DB resources, follow these steps:

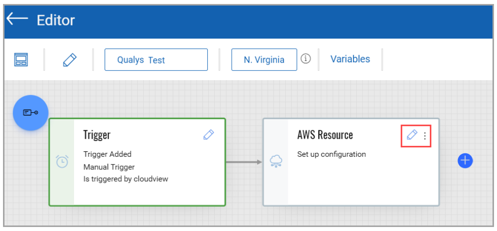
1. To add the Resource node, click the ⊕ icon.

2. On the Explore Nodes pop-up window, go to **AWS Nodes**, select **AWS Resource** node

.



AWS Resource node is added in the Editor.

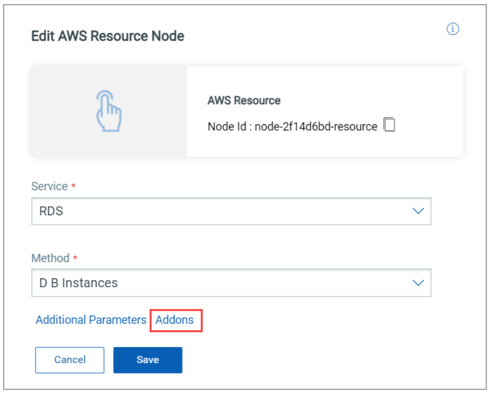


3. Click the ✎ icon on the node to set up the configuration.

The Edit AWS Resource Node pop-up window is displayed.

4. Select RDS as **Service** and DB Instances as **Method** from the list.

5. Click **Addons** to select the additional resources that are linked with your resource.



Edit AWS Resource Node

AWS Resource
Node Id : node-2f14d6bd-resource

Service *
RDS

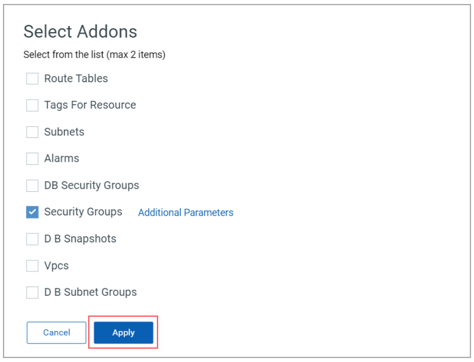
Method *
D B Instances

Additional params are like filters that could be added to the cloud API calls that could narrow down the results returned. This is particularly useful if the data set is large (>100 objects).

Addons are additional API calls made to the cloud to fetch the details of resources that are related to the actualy API call configured in the resource node.

For example, in the case of DB instances, security groups are linked to these DB instances as Addons. These security groups may be allowing public IPs on the databases. You can also add those security groups to the resource node to get information about these resources. Based on your selected service, addons are auto-populated..

6. On the Select Addons window, select **Security Groups** from the list and click **Apply**.



Select Addons
Select from the list (max 2 items)

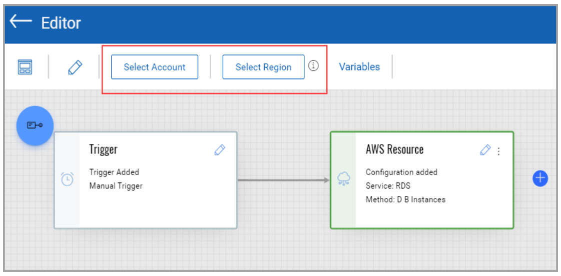
☐ Route Tables
☐ Tags For Resource
☐ Subnets
☐ Alarms
☐ DB Security Groups
☑ Security Groups
☐ D B Snapshots
☐ Vpcs
☐ D B Subnet Groups

Step 4: Select an AWS Account and a Region

Qualys recommends testing and verifying the QFlow with a single account and region before applying it to multiple accounts and regions. Once you are satisfied with the QFlow and outcome, you can deploy the QFlow on multiple accounts and regions.

1. Click **Select Account** to choose the account from the list and then click **Apply**.

2. Click **Select Region** to choose the region from the list and then click **Apply**.



Step 5: Add the TotalCloud node

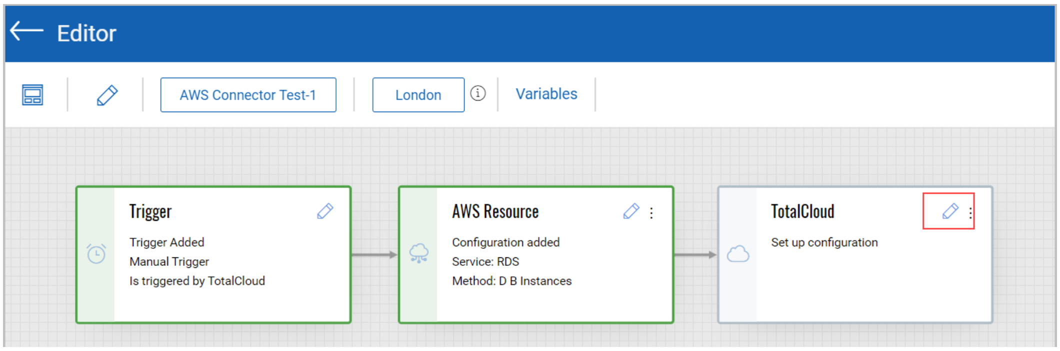
Use TotalCloud node to take the output from the resource node and filter publicly available RDS DB instances. For more details on nodes, refer to Know the Nodes.

To find out all publicly available RDS DB resources, follow these steps

1. Click the ⊕ icon placed after the resource node.

2. On the Explore Nodes pop-up window, from **General Nodes**, select **TotalCloud** node.

3. Click the ✎ icon on the TotalCloud node to set up the configuration.



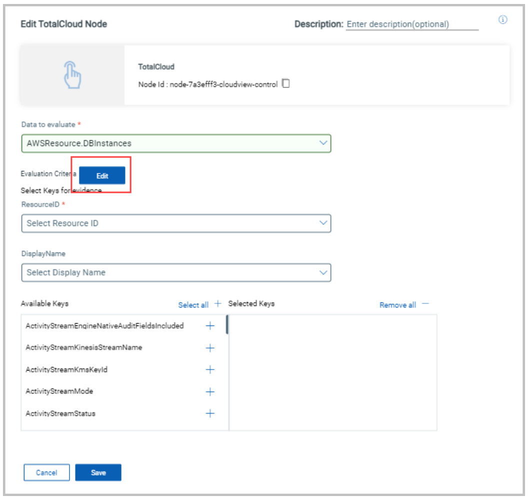
4. On Edit ControlView Control Node pop-up window, from the list for **Data to evaluate** field, select AWSResource.DBInstances.

To view all the publicly available instances, you need to apply two filter types:

- param filter with publicly accessible key

- security group filter that may have given access to public IP

5. From Evaluation Criteria, click **Edit**.



Edit TotalCloud Node

Description: Enter description(optional)

TotalCloud

Node Id : node-7a3efff3-cloudview-control

Data to evaluate *

AWSResource.DBInstances

Evaluation Criteria

Select Keys for evidence

ResourceID *

Select Resource ID

DisplayName

Select Display Name

Available Keys

ActivityStreamEngineNativeAuditFieldsIncluded

ActivityStreamKinesisStreamName

ActivityStreamKmsKeyId

ActivityStreamMode

ActivityStreamStatus

Selected Keys

The Evaluation Criteria window is displayed to enter the details of both the filters.

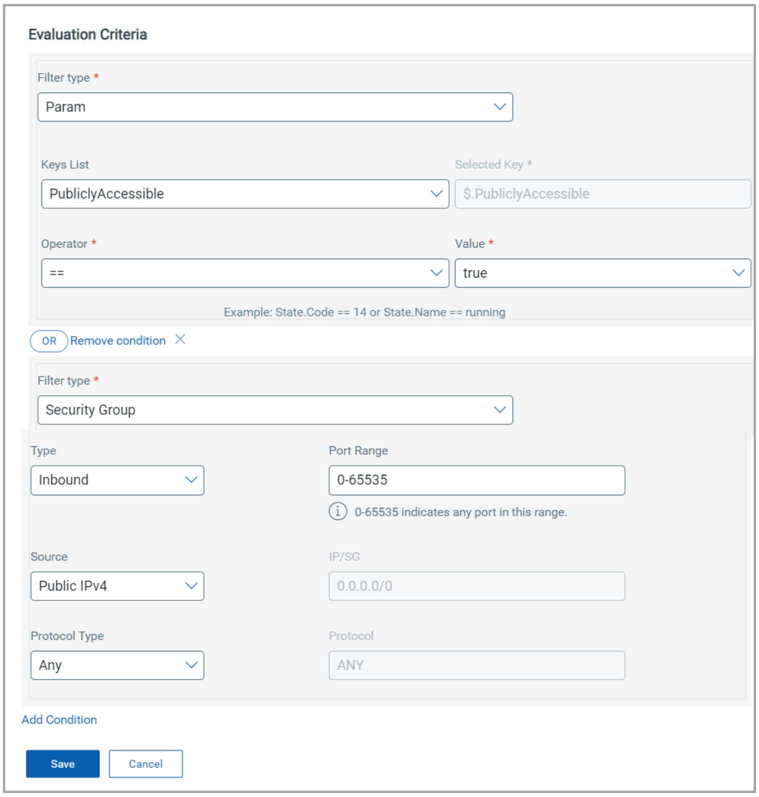
6. Select **Filter type** as Param.

7. Select **Key** as PubliclyAccessible from the list, the **Operator** as **==** and write **Value** as **true**.

8. Click the **Add Condition** and select **OR** to apply the Security Group Filter Type.

9. To check for any publicly accessed IP which may be part of the security group, select **Filter type** as Security Group.

10. Select **Type** as Inbound, **Port Range** as All, **Source** as Public IPv4, **IP/SG** as 0.0.0.0/0, **Protocol Type** as Any, **Protocol** as ANY and click **Save**.



Evaluation Criteria

Filter type * Param

Keys List PubliclyAccessible

Selected Key * $.PubliclyAccessible

Operator * ==

Value * true

Example: State.Code == 14 or State.Name == running

Filter type * Security Group

Type Inbound

Port Range 0-65535

0-65535 indicates any port in this range.

Source Public IPv4

IP/SG 0.0.0.0/0

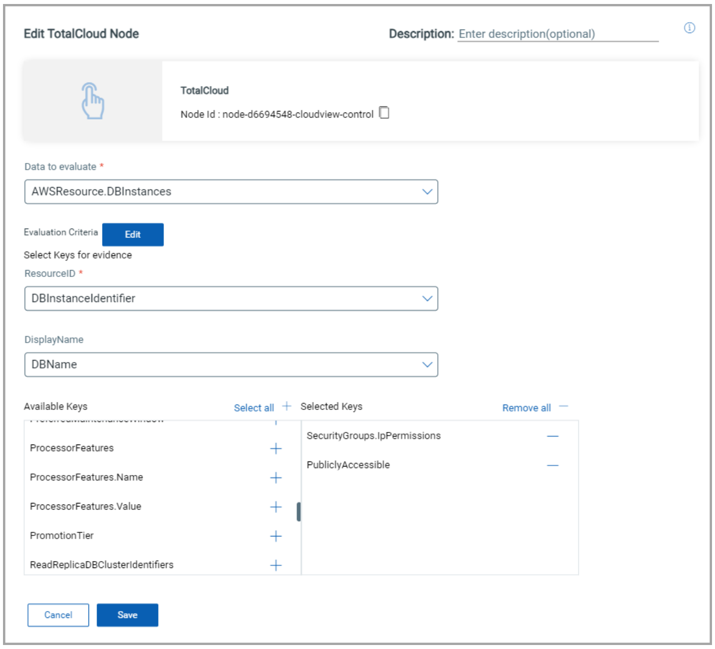
Protocol Type Any

Protocol ANY

The Edit TotalCloud Node window is updated with the applied filters.

11. From Select Keys for evidence field, select **ResourceID** as DBInstanceIdentifier and **DisplayName** as DBName

12. From **Available Keys**, select PubliclyAccessible and **SecurityGroups.IpPermissions** then click **Save**.



Edit TotalCloud Node

Description: Enter description(optional)

TotalCloud

Node Id : node-d6694548-cloudview-control

Data to evaluate *: AWSResource.DBInstances

Evaluation Criteria

Select Keys for evidence

ResourceID *: DBInstanceIdentifier

DisplayName: DBName

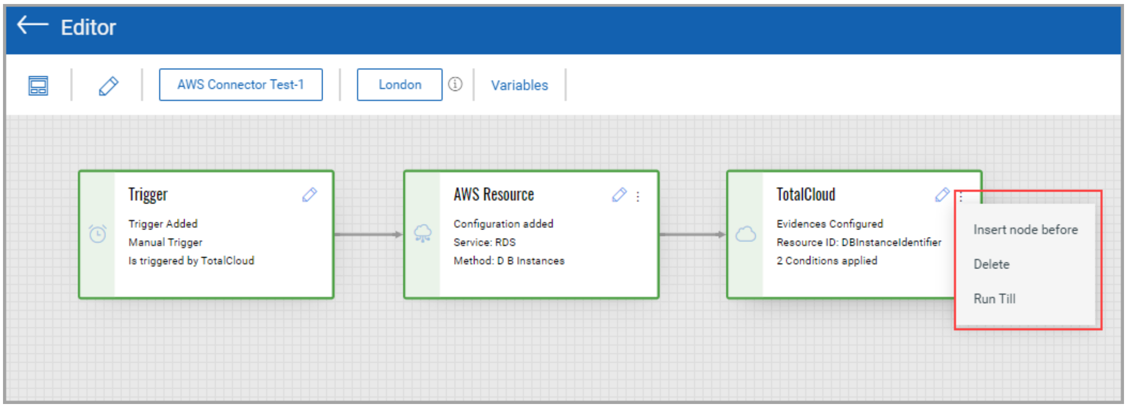
Available Keys	Selected Keys
ProcessorFeatures	SecurityGroups.IpPermissions
ProcessorFeatures.Name	PubliclyAccessible
ProcessorFeatures.Value	
PromotionTier	
ReadReplicaDBClusterIdentifiers	

Now you have created QFlow. It is ready for testing and running.

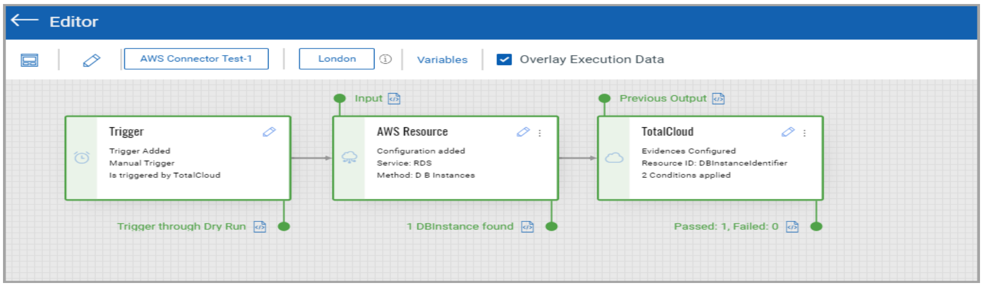
Step 6: Run and check the functionality of nodes

It is best practice to check the functionality of individual nodes before running the QFlow. It avoids data loss if any node is not working correctly because of some configuration error.

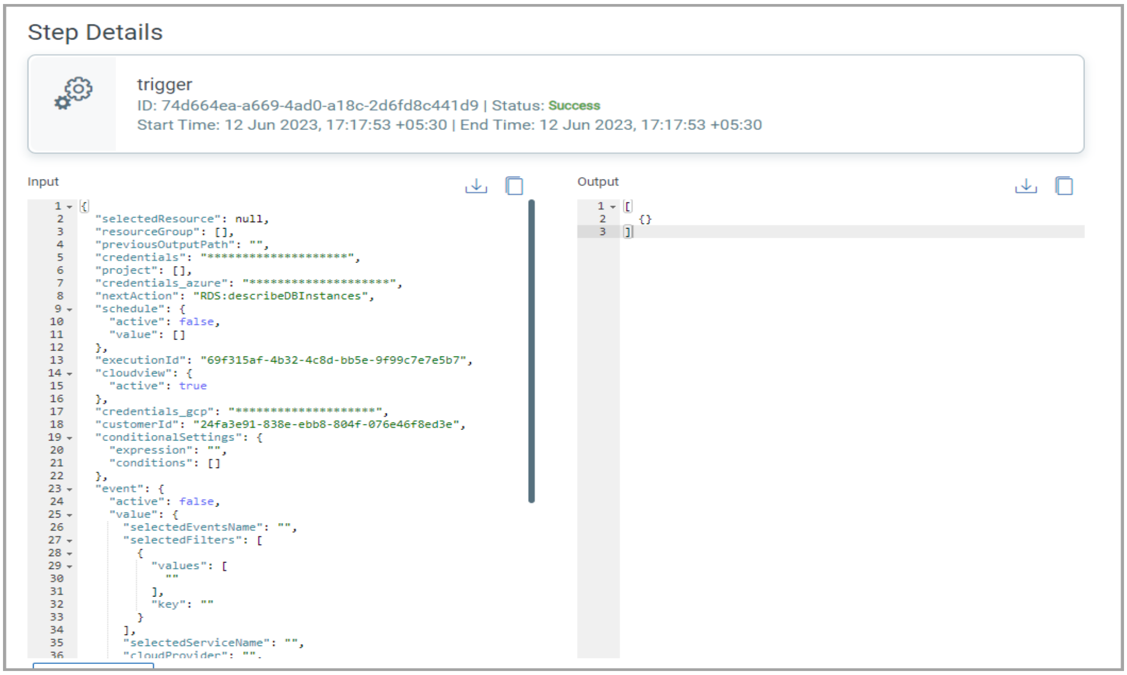
1. Click the three dots present at the top right corner of the specific node to get the **Run till** option for running the QFlow till that specific node.



The status of the running of the QFlow is displayed. The status of the input and output of the node is displayed in green.



You can view the execution history by clicking the 🗎 icon adjacent to status for the details of the node's output. For demonstration, we have shown the trigger node's execution history.



Step Details

trigger
ID: 74d664ea-a669-4ad0-a18c-2d6fd8c441d9 | Status: Success
Start Time: 12 Jun 2023, 17:17:53 +05:30 | End Time: 12 Jun 2023, 17:17:53 +05:30

Input

```
{
  "selectedResource": null,
  "resourceGroup": [],
  "previousOutputPath": "",
  "credentials": "********************",
  "project": [],
  "credentials_azure": "********************",
  "nextAction": "RDS:describeDBInstances",
  "schedule": {
    "active": false,
    "value": []
  },
  "executionId": "69f315af-4b32-4c8d-bb5e-9f99c7e7e5b7",
  "cloudview": {
    "active": true
  },
  "credentials_gcp": "********************",
  "customerId": "24fa3e91-838e-ebb8-804f-076e46f8ed3e",
  "conditionalSettings": {
    "expression": "",
    "conditions": []
  },
  "event": {
    "active": false,
    "value": {
      "selectedEventsName": "",
      "selectedFilters": [
        {
          "values": [
            ""
          ],
          "key": ""
        }
      ],
      "selectedServiceName": "",
      "cloudProvider": "",
```

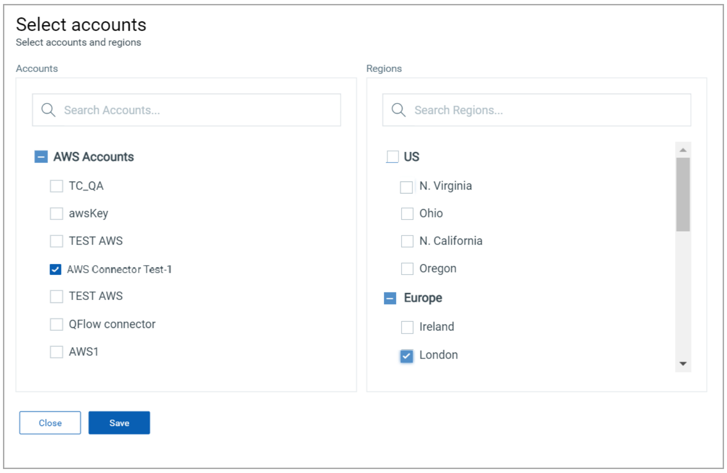
Output

```
[
  {}
]
```

Once you verify the functioning of your QFlow, you can save the QFlow.

Step 7: Associate your QFlow with AWS Accounts and Regions

1. To save the QFlow, click Save.
2. Select the AWS **Accounts** and **Regions** from the list and click **Save**.



Select accounts
Select accounts and regions

Accounts

Search Accounts...

- AWS Accounts
  - □ TC_QA
  - □ awsKey
  - □ TEST AWS
  - ☑ AWS Connector Test-1
  - □ TEST AWS
  - □ QFlow connector
  - □ AWS1

Regions

Search Regions...

- □ US
  - □ N. Virginia
  - □ Ohio
  - □ N. California
  - □ Oregon
- Europe
  - □ Ireland
  - ☑ London

Your QFlow is ready. You can now create user-defined control in the TotalCloud application.

Managing Your QFlows

There are multiple actions that you can perform on your QFlows, such as

View Your QFlows

Use of QFlows in TotalCloud Application

Export Your QFlows

Clone Your QFlows

Import Your QFlows

Pre-requisites

To use the export, clone, and import features, you must be on Qualys Cloud Platform 3.16.1 or later. Contact Qualys support for more details.

Role Based Access Control (RBAC)

Manager users and CWE Admin users can use these features, you need the following access to be enabled in your account through the Administration application.

Export QFlows: **Read Permission** > **QFlow Export Access**

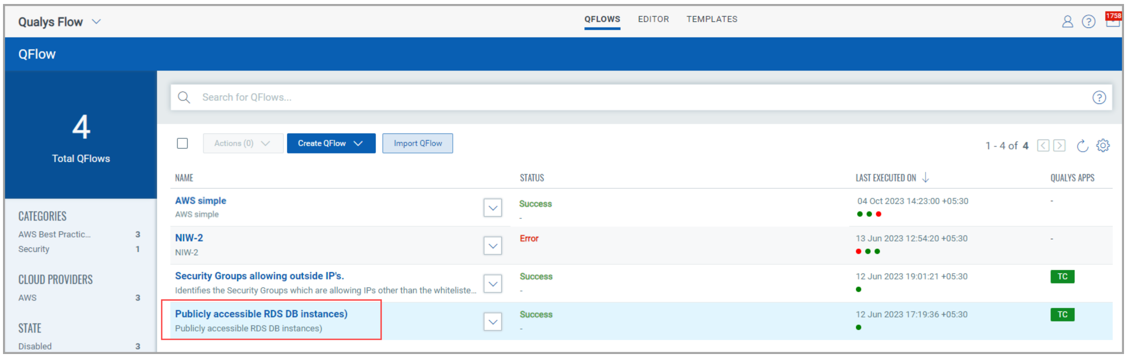
Clone Your QFlows: **Write Permission** > **QFlow Clone Access**

Import Your QFlows: **Write Permission** > **QFlow Import Access**. To know more about how to edit the role, refer to Administration Online help.

View Your QFlows

You can view your created QFlow in the QFlows tab.

The QFlows tab displays the total count of QFlows at the top left corner and filters based on your created categories. From the search bar, you can search your QFlow by typing the name of your QFlow.



4
Total QFlows

CATEGORIES
AWS Best Practic... 3
Security 1

CLOUD PROVIDERS
AWS 3

STATE
Disabled 3

NAME	STATUS	LAST EXECUTED ON	QUALYS APPS
AWS simple AWS simple	Success -	04 Oct 2023 14:23:00 +05:30 ●●●	-
NIW-2 NIW-2	Error	13 Jun 2023 12:54:20 +05:30 ●●●	-
Security Groups allowing outside IP's. Identifies the Security Groups which are allowing IPs other than the whiteliste...	Success -	12 Jun 2023 19:01:21 +05:30 ●	TC
Publicly accessible RDS DB instances) Publicly accessible RDS DB instances)	Success -	12 Jun 2023 17:19:36 +05:30 ●	TC

In the details of the QFlow, you can see a status like Success, Never Executed, or Error. You can view the latest three execution of the QFlow with three color code dots.

Color Code	Description
Green	QFlow execution is successful.
Red	QFlow execution is failed.
Yellow	QFlow execution is running.

Export Your QFlows

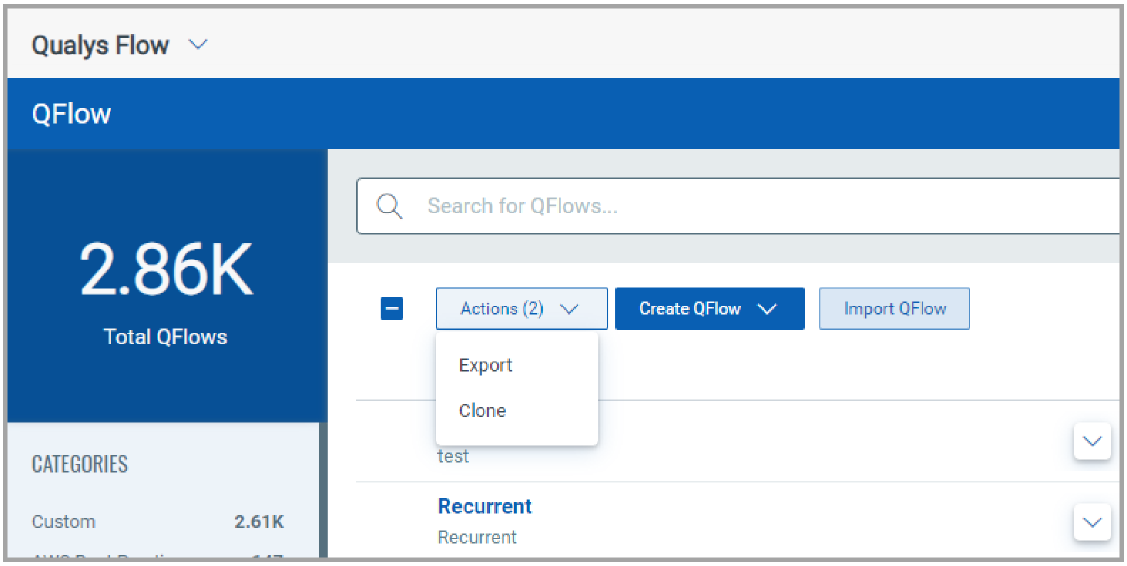
The export feature allows you to download QFlows in JSON format, which can be imported. It is easier to export QFlows from one account and import them in another account than re-creating the same QFlows manually. Once the QFlows are imported, the connectors and any such HTTP authentication details need to be re-configured and saved. It is possible to export up to 10 QFlows in a single JSON file.

You can use the Export function to download your QFlows to your local machine.

Note: When exporting, we remove authentication information from the HTTP node to ensure security best practices are followed.

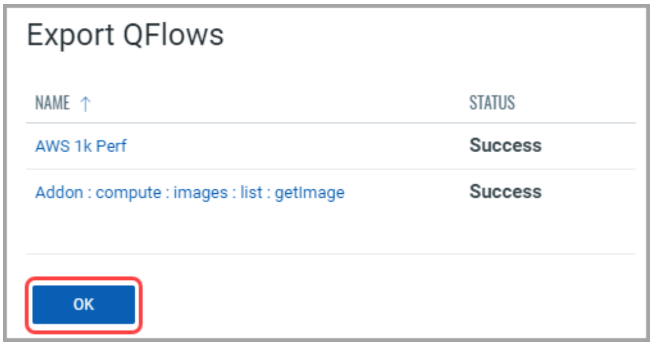
Follow these steps to export QFlows:

1. Navigate to the QFlows tab, select the QFlows you want to export, and click Export from the Actions menu.



A list of QFlows that are exported is displayed.

2. Click OK to continue the export process.


Export QFlows

NAME ↑	STATUS
AWS 1k Perf	Success
Addon : compute : images : list : getImage	Success

QFlows are exported in JSON format.

3. Save the file in a suitable location on your machine.

Now that you have exported your QFlows, you can use these QFlows using the import function. You need to configure connectors and HTTP authentication details after importing the QFlows. The exported QFlows JSON file is named as the qualys_export-timestamp appended (for example qflows-export-1696589891052.json).

Clone Your QFlows

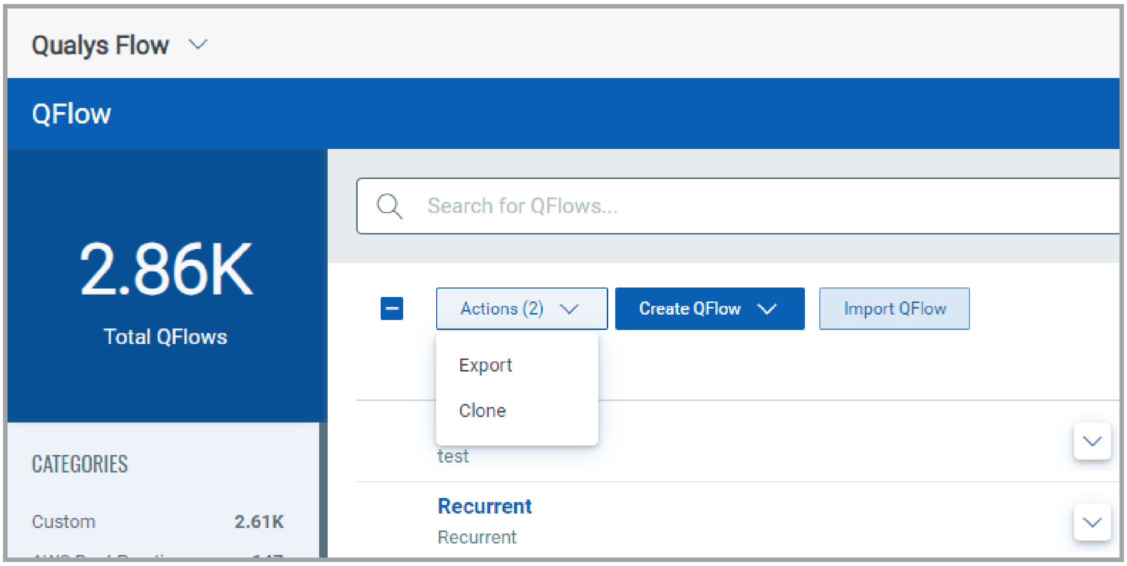
Cloning QFlows is a faster way to address multiple similar use cases, saving you the effort of creating separate QFlows from scratch.

A single QFlow can be cloned multiple times and edited to suit your requirements. You can now create an exact copy of your QFlows using the Clone function without the connector details.

The cloned QFlow is named as the original QFlow with _cloned_ timestamp appended. After cloning a QFlow, you can change its name by clicking on the current name and editing it. When cloning AWS_DB_Instances, the resulting QFlow is named AWS_DB_Instances_cloned_1690881080384. This naming convention is followed for all cloned QFlows.

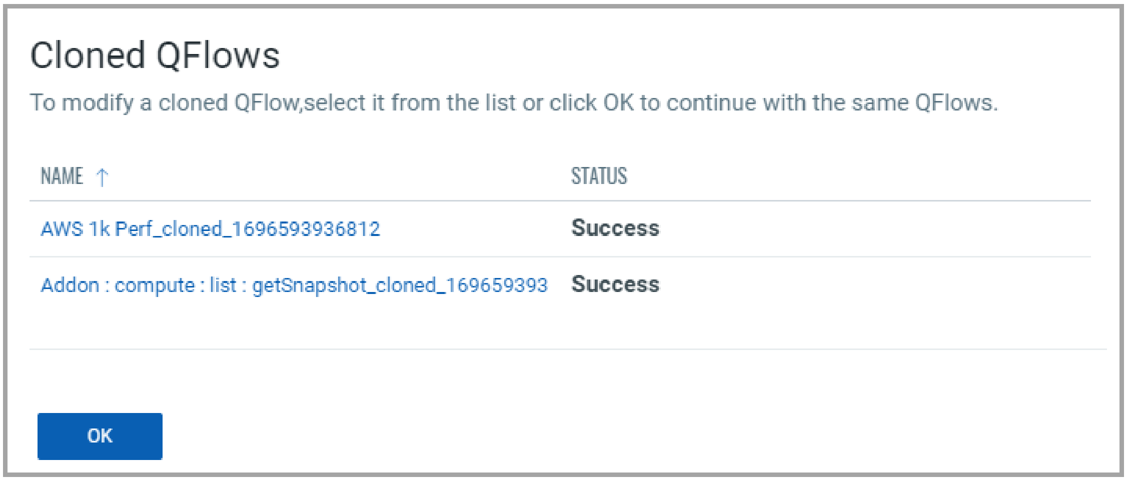
Follow these steps to clone QFlows:

1. Navigate to the **QFlows** tab, select the QFlows you want to clone, and click **Clone** from the Actions menu.



A list of QFlows that are cloned is displayed.

2. Click **OK** to continue the export process.



Cloned QFlows

To modify a cloned QFlow,select it from the list or click OK to continue with the same QFlows.

NAME ↑	STATUS
AWS 1k Perf_cloned_1696593936812	Success
Addon : compute : list : getSnapshot_cloned_169659393	Success

QFlows are cloned.After cloning your QFlows, customize them by configuring connectors and HTTP authentication details.

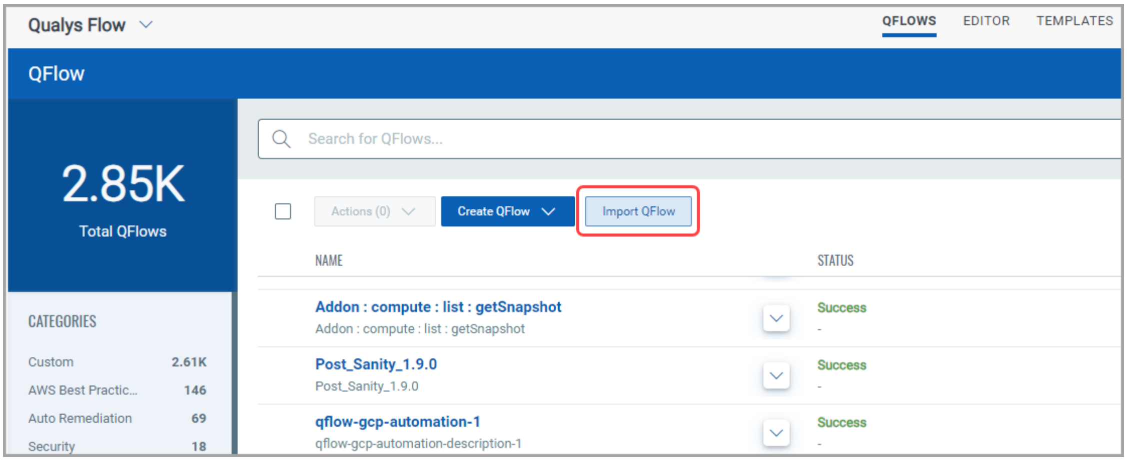
Import Your QFlows

QFlows that are exported as JSON files from a Qualys user account can be imported into your account. Complex QFlows can be imported rather than building them from scratch. Once the QFlows are imported, the connectors and any such HTTP authentication details needs to be re-configured and saved.

You can export QFlows from your other account and import them.

Note: After importing a QFlow, it needs to be saved with connectors and HTTP authentication details (if applicable).

1. Navigate to the **QFlows** tab > **Import QFlow** and follow the wizard to upload the QFlow.



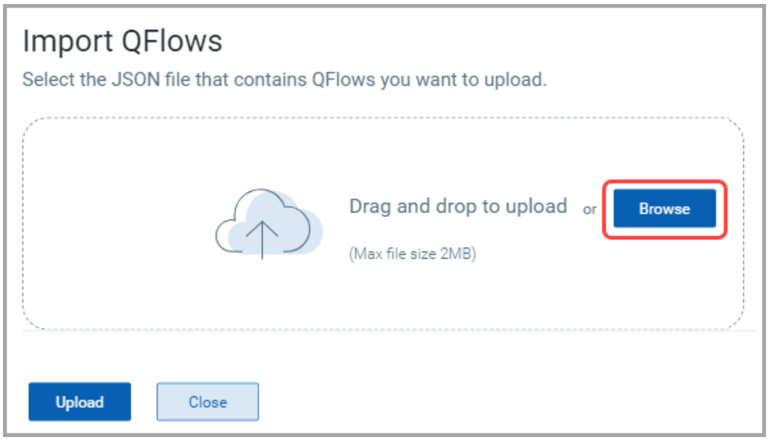
CATEGORIES

Custom	2.61K
AWS Best Practic...	146
Auto Remediation	69
Security	18

NAME	STATUS
Addon : compute : list : getSnapshot Addon : compute : list : getSnapshot	Success -
Post_Sanity_1.9.0 Post_Sanity_1.9.0	Success -
qflow-gcp-automation-1 qflow-gcp-automation-description-1	Success -

2. Click **Browse** and select the file containing QFlows in JSON format.

Note: You can use the QFlows exported from your other account. You need to configure connectors and HTTP authentication details after importing the QFlows.

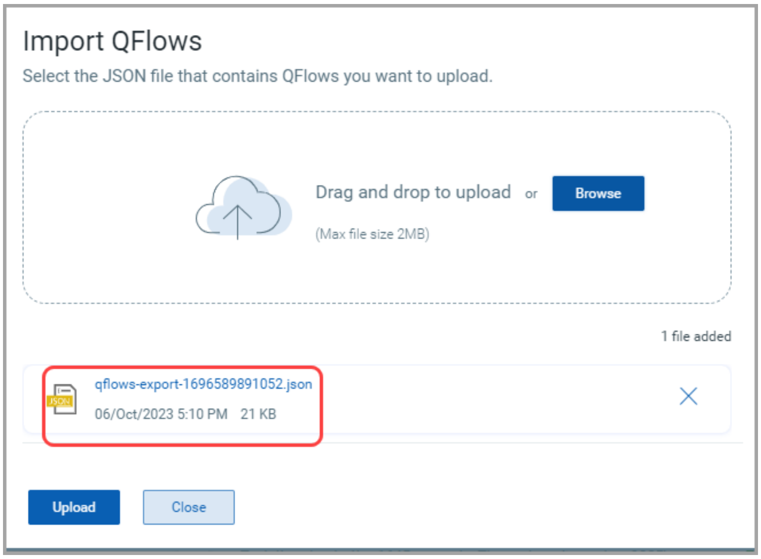


Import QFlows

Select the JSON file that contains QFlows you want to upload.

Your uploaded JSON file is listed.

3. To upload the QFlows in JSON file, click Upload.



Import QFlows

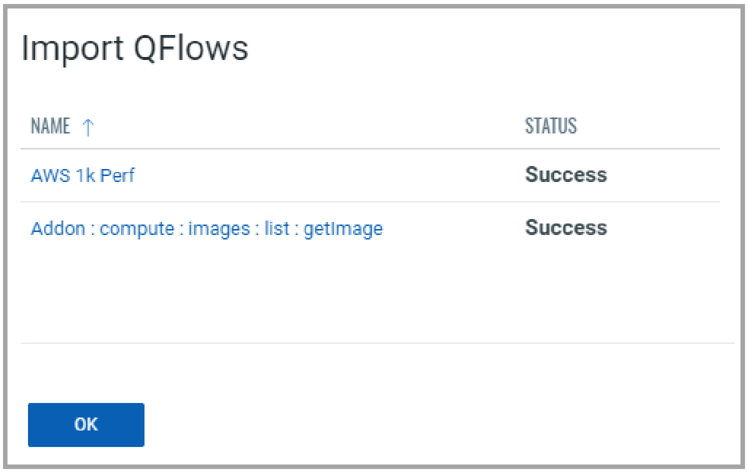
Select the JSON file that contains QFlows you want to upload.

qflows-export-1696589891052.json

06/Oct/2023 5:10 PM 21 KB

The list of imported QFlows is displayed.

4. Click **OK** to continue.



Import QFlows

NAME ↑	STATUS
AWS 1k Perf	Success
Addon : compute : images : list : getImage	Success

The imported QFlows are listed in the QFlows tab.

Once you have imported the QFlows, you can edit and customize them according to your specific requirements.You need to configure connectors as per your requirements.

Use of QFlows in TotalCloud Application

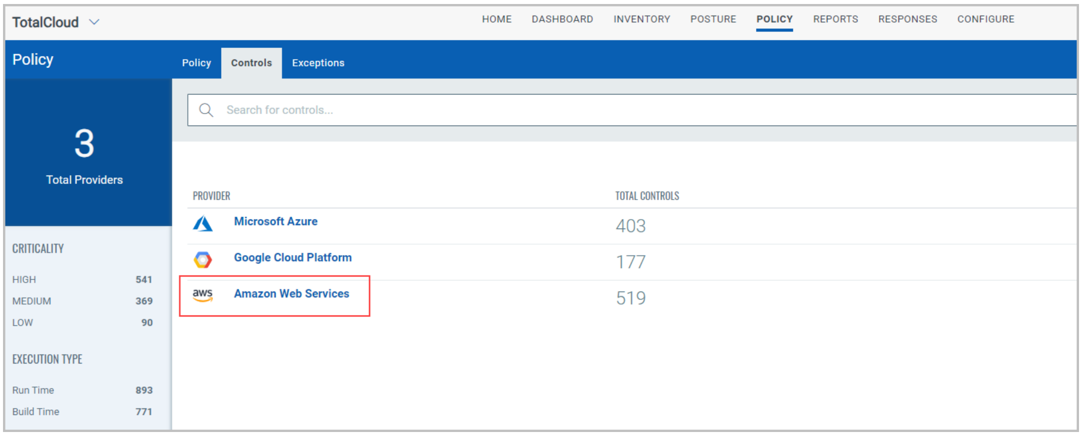
A policy is a collection of controls used to measure and report compliance for a set of resources. You could use the policies we provide or build your own policy. System-defined control is a predefined control provided by Qualys. Now you can create your own user-defined control using QFlow.

Create Your Own Control

To create a user-defined control (UDC), you need the required permissions at TotalCloud application.

Here are the steps to create your own control:

1. Navigate to TotalCloud from the application menu and navigate to **Policy** tab > **Controls** > **Amazon Web Services**.

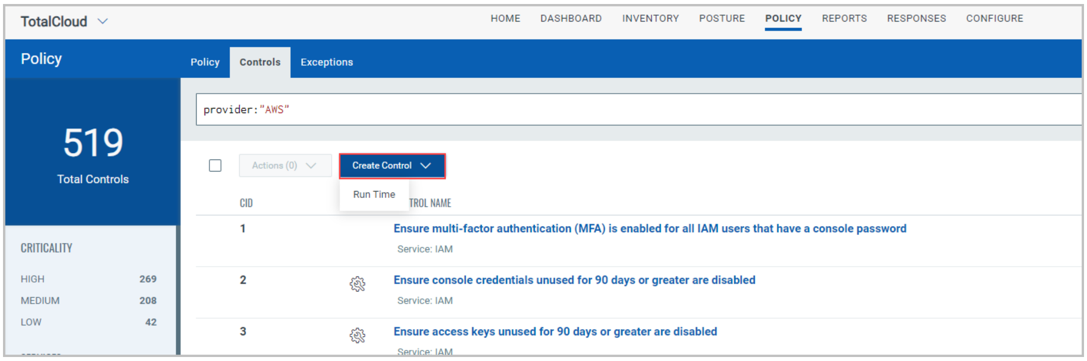


CRITICALITY	
HIGH	541
MEDIUM	369
LOW	90

EXECUTION TYPE	
Run Time	893
Build Time	771

PROVIDER	TOTAL CONTROLS
Microsoft Azure	403
Google Cloud Platform	177
Amazon Web Services	519

2. Click **Create Control** > **Runtime.**

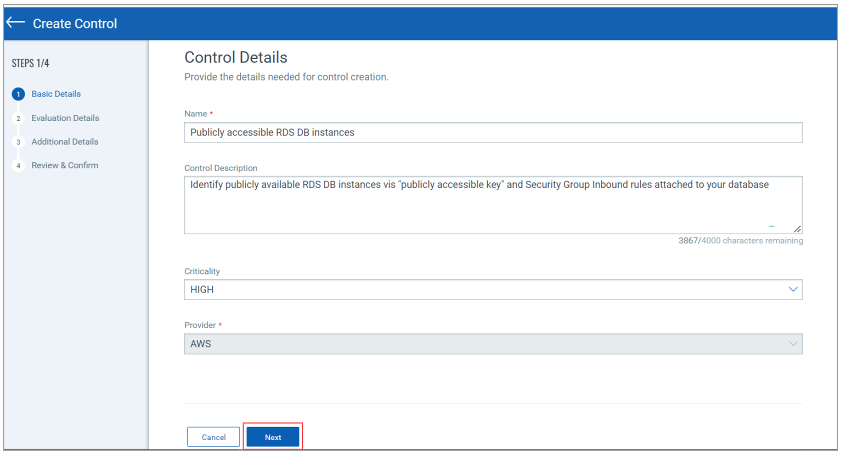


provider:"AWS"

CRITICALITY	
HIGH	269
MEDIUM	208
LOW	42

CID	TROL NAME
1	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password Service: IAM
2	Ensure console credentials unused for 90 days or greater are disabled Service: IAM
3	Ensure access keys unused for 90 days or greater are disabled Service: IAM

3. Provide the basic details for the control such as **Name**, **Description**, select the **Criticality** and cloud **Provider**, and click **Next**.



Create Control

STEPS 1/4

1. Basic Details
2. Evaluation Details
3. Additional Details
4. Review & Confirm

Control Details

Provide the details needed for control creation.

Name *: Publicly accessible RDS DB instances

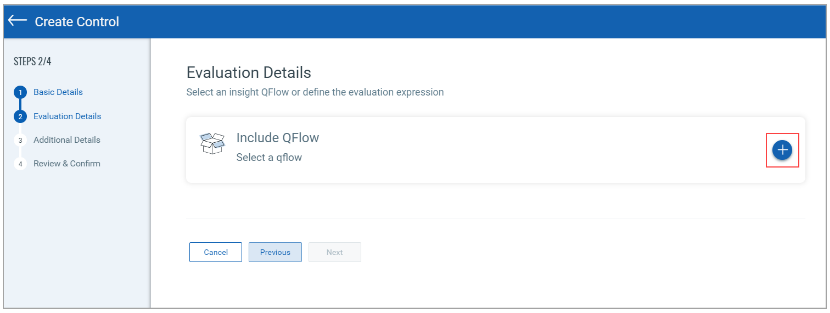
Control Description: Identify publicly available RDS DB instances vis "publicly accessible key" and Security Group Inbound rules attached to your database

3867/4000 characters remaining

Criticality: HIGH

Provider *: AWS

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



Create Control

STEPS 2/4

1. Basic Details
2. Evaluation Details
3. Additional Details
4. Review & Confirm

Evaluation Details

Select an insight QFlow or define the evaluation expression

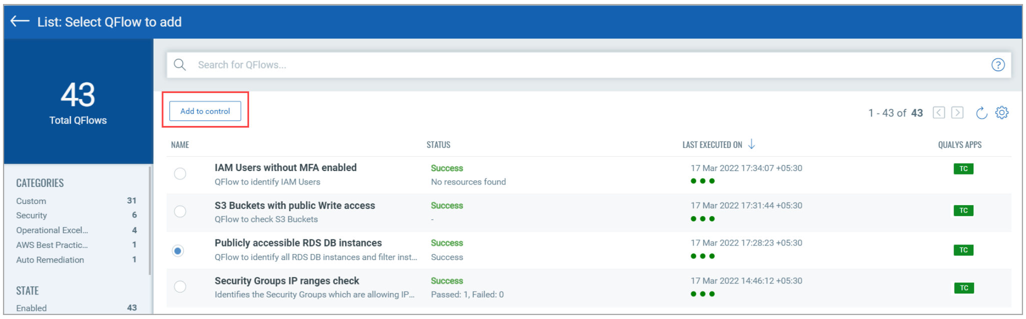
Include QFlow

Select a qflow

The list of your created QFlows is displayed.

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

For this case, select Publicly accessible RDS DB instances.



List: Select QFlow to add

43
Total QFlows

CATEGORIES

Custom	31
Security	6
Operational Excel...	4
AWS Best Practic...	1
Auto Remediation	1

STATE

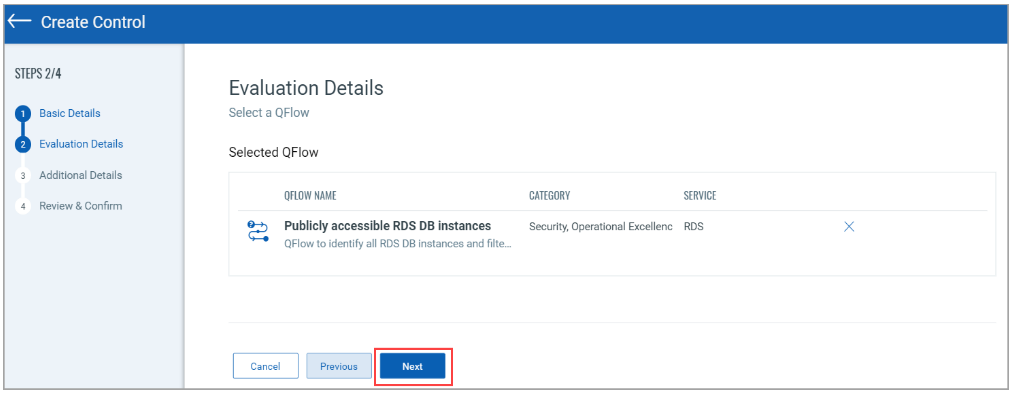
Enabled	43

Search for QFlows...

1 - 43 of 43

	NAME	STATUS	LAST EXECUTED ON	QUALYS APPS
○	IAM Users without MFA enabled QFlow to identify IAM Users	Success No resources found	17 Mar 2022 17:34:07 +05:30	TC
○	S3 Buckets with public Write access QFlow to check S3 Buckets	Success -	17 Mar 2022 17:31:44 +05:30	TC
●	Publicly accessible RDS DB instances QFlow to identify all RDS DB instances and filter inst...	Success Success	17 Mar 2022 17:28:23 +05:30	TC
○	Security Groups IP ranges check Identifies the Security Groups which are allowing IP...	Success Passed: 1, Failed: 0	17 Mar 2022 14:46:12 +05:30	TC

6. The QFlow is added in the control; click **Next**.



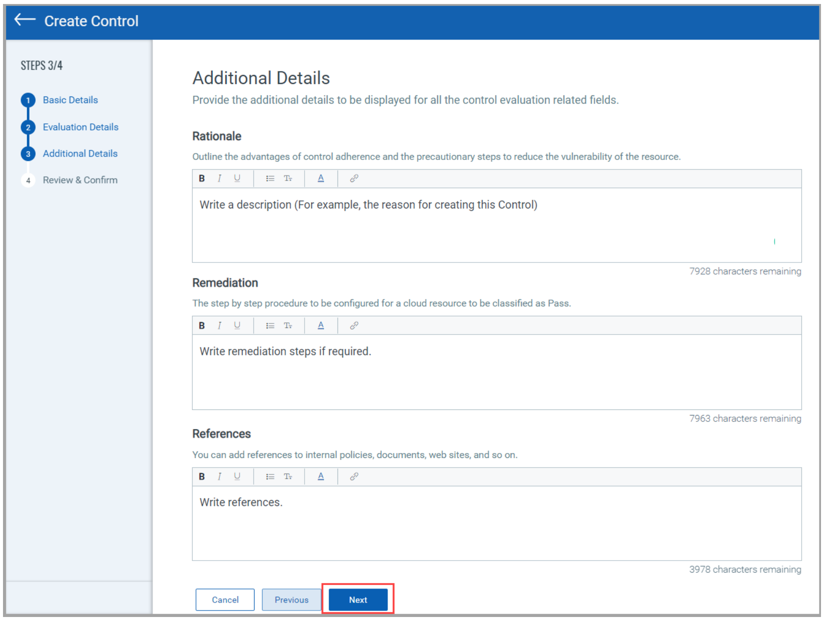
Evaluation Details

Select a QFlow

Selected QFlow

QFLOW NAME	CATEGORY	SERVICE
Publicly accessible RDS DB instances QFlow to identify all RDS DB instances and filte...	Security, Operational Excellenc	RDS

7. Fill in the additional details for your reference, like the objective of adding this control in **Rationale**, remediation steps if you want to suggest in **Remediation**, **References** and click **Next**. These fields are optional.



Additional Details

Provide the additional details to be displayed for all the control evaluation related fields.

Rationale

Outline the advantages of control adherence and the precautionary steps to reduce the vulnerability of the resource.

Write a description (For example, the reason for creating this Control)

7928 characters remaining

Remediation

The step by step procedure to be configured for a cloud resource to be classified as Pass.

Write remediation steps if required.

7963 characters remaining

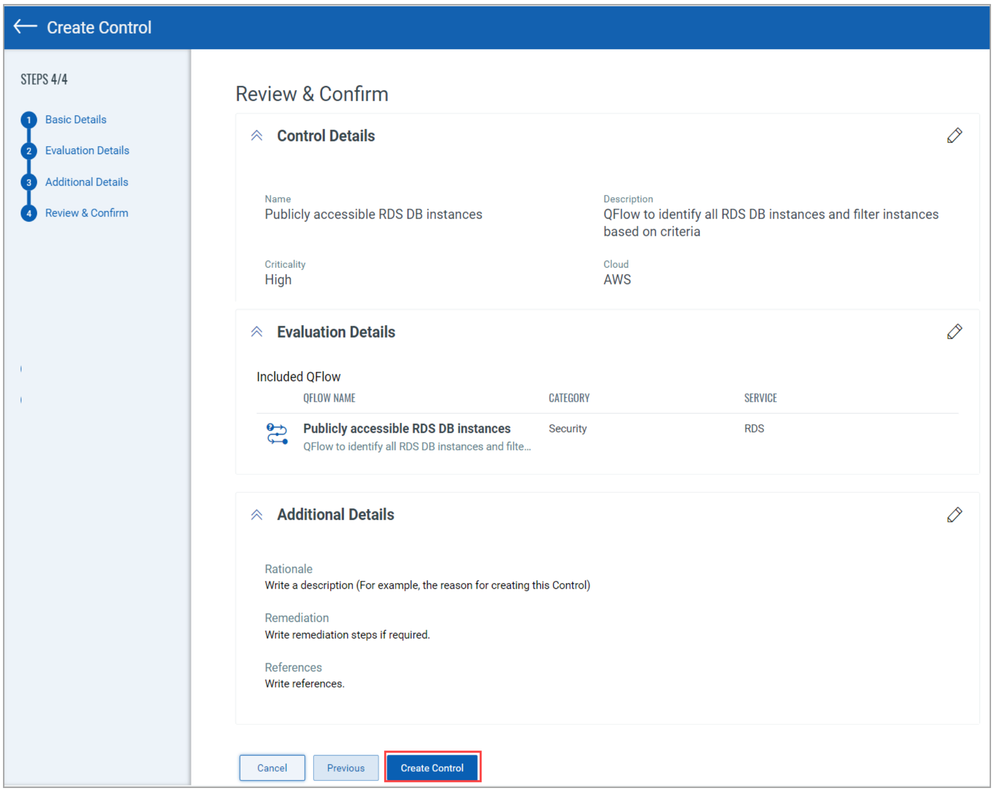
References

You can add references to internal policies, documents, web sites, and so on.

Write references.

3978 characters remaining

8. Review the details of your control and click **Create Control**.



Review & Confirm

Control Details

Name
Publicly accessible RDS DB instances

Description
QFlow to identify all RDS DB instances and filter instances based on criteria

Criticality
High

Cloud
AWS

Evaluation Details

Included QFlow

QFLOW NAME	CATEGORY	SERVICE
Publicly accessible RDS DB instances QFlow to identify all RDS DB instances and filte...	Security	RDS

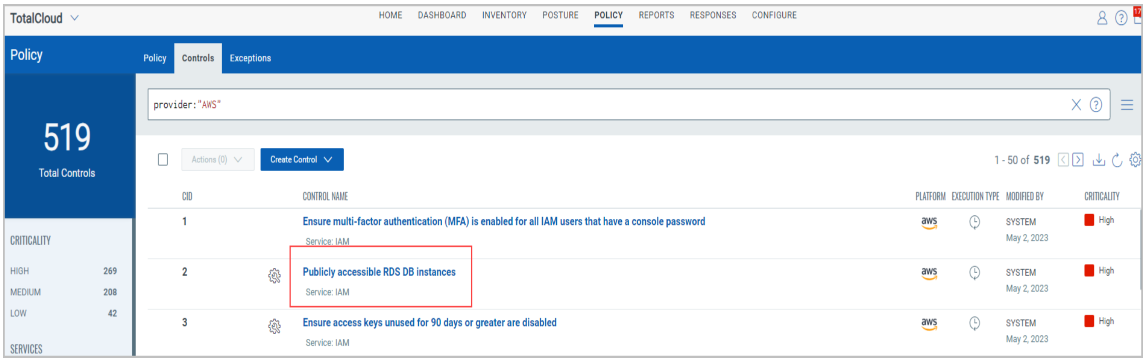
Additional Details

Rationale
Write a description (For example, the reason for creating this Control)

Remediation
Write remediation steps if required.

References
Write references.

You have successfully created the control.



provider:"AWS"

519
Total Controls

CRITICALITY

HIGH	269
MEDIUM	208
LOW	42

SERVICES

1 - 50 of 519

CID		CONTROL NAME	PLATFORM	EXECUTION TYPE	MODIFIED BY	CRITICALITY
1		Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password Service: IAM	aws		SYSTEM May 2, 2023	🟥 High
2		Publicly accessible RDS DB instances Service: IAM	aws		SYSTEM May 2, 2023	🟥 High
3		Ensure access keys unused for 90 days or greater are disabled Service: IAM	aws		SYSTEM May 2, 2023	🟥 High

Now you have successfully created the control to identify publicly available RDS database instances; you can use this control in your policy. For more details, refer to the Build Your Own Policy topic in TotalCloud User Guide.

References

For more details on Qualys TotalCloud, refer to TotalCloud Online help.