# Table of Contents

**About this Guide** .......................................................................................................................... 4  
About Qualys .............................................................................................................................................. 4  
Qualys Support ........................................................................................................................................... 4  

**CloudView Overview** ..................................................................................................................... 5  
Qualys Subscription and Modules required .......................................................................................... 5  
Concepts and Terminologies .................................................................................................................. 5  

**Get Started** ......................................................................................................................................... 7  
Create AWS Connector .......................................................................................................................... 7  
Create Azure Connector ......................................................................................................................... 10  

**Securing Cloud Resources** .............................................................................................................. 17  
Dashboard ............................................................................................................................................ 17  
Resources Details .................................................................................................................................... 18  
Resources Misconfigurations .................................................................................................................. 23  

**CloudView APIs** .................................................................................................................................. 26  
Accessing APIs Using Swagger .............................................................................................................. 26  
API List .................................................................................................................................................. 27
About this Guide

Welcome to Qualys CloudView! We’ll help you get acquainted with the Qualys solutions for securing your AWS resources 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 a 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/.
CloudView Overview

Qualys CloudView provides visibility and continuous security across all of your cloud environments.

With CloudView you’ll get these features:

- Discover and inventory assets and resources across all regions from multiple accounts and multiple cloud platforms
- Search resource metadata, view resource details and show associations across resources
- Out-of-box CIS Amazon Web Services Foundations Benchmark policy & AWS Best Practices policy to identify misconfigurations of S3 Buckets
- Continuously assess and report on resource misconfigurations by checking against the controls from out-of-box policies
- Ability to search misconfigurations by Account-ID, Regions

Qualys Subscription and Modules required

Check that you have these modules available in your subscription:

- CloudView
- Vulnerability Management (only if you want to view host vulnerability information)
- AssetView
- Cloud Agents for VM

If you need a module, please contact your Qualys Technical Account Manager (TAM).

Concepts and Terminologies

Get familiar with common terms used in CloudView.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>A set of configuration checks that will assess different resources collected from your cloud account.</td>
</tr>
</tbody>
</table>
| Control   | A configuration check. Each check applies to a specific service/resource. Here are some examples:  
  - MFA should be enabled for console user - applies to AWS IAM Service and IAM User Resource  
  - Password policy should have upper case letter enforced - applies to AWS IAM Service  
  - Security group should not allow inbound access on port 22 from 0.0.0.0 - applies to EC2/VPC services and Security Group Resource |
| Service   | A service is the high level grouping by functional area. Each service consists of different entities or resources. |
### Resource
A resource is an entity that you can work with. Examples include an Amazon EC2 instance, IAM User, Security Group.

### Control Passed
Each control is applicable to a specific resource type. For each control, applicable resources are collected. The control checks whether the particular attribute of a resource is configured as per best practices. The control is passed when the attribute that the control is checking is found configured as per the desired configuration for all the applicable resources collected.

### Control Failed
Control is considered failed when an attribute of the control being checked is not configured as per the desired configuration for any of the applicable resources collected.

### Resource Passed
Resource is considered passed for a control if its attribute is configured as per the desired configuration in the control.

### Resource Failed
Resource is considered failed for a control if its attribute is not configured as per the desired configuration in the control.
Get Started

Just set up a connector for your cloud environment and that’s it! We’ll start discovering resources that are present in your cloud account. You can create AWS connectors and Azure connectors. We’ll walk you through the steps.

Create AWS Connector

Go to the Configuration tab and select Create Connector > Amazon Web Services.

Provide a name and description (optional) for your connector. Then copy settings from the connector details: Qualys AWS Account ID and External ID. You’ll need these for creating your IAM role in AWS in the next step.
Launch your AWS console, and go to IAM > Roles and click Create Role. In the Create role window, choose “Another AWS account”. Paste in the Qualys account ID and the External ID that you copied in the previous step. Click Next: Permissions.

Choose AWS policy to attach to role. Find the policy “SecurityAudit” and select the check box next to it. Click Next: Review.
Save AWS role and get the ARN. Enter a role name (e.g. QualysCVRole), click Create role. Then click on the saved role to view role details and copy the ARN value.

Go back to your AWS connector in Qualys CloudView and paste the Role ARN value into the connector details. Then click Create Connector.

That’s it! The connector will establish a connection with AWS to start discovering resources from each region and evaluate them against policies.

A unique external ID gets generated during connector creation. If you want to use your own external ID, use API to create the connector. For more details, refer to Example 4: Create AWS connector.
Want to create a role using CloudFormation?
Download the CloudFormation template from the Create AWS Connector window.

Follow the steps on the screen to create a stack and upload the template. When the stack is complete, copy the Role ARN from the output and paste it into the connector details.

Create Azure Connector
Let us see what permissions are needed to create Azure connector.

Pre-requisites
Before you create an Azure connector, ensure that you have the following permissions:
- Assign Azure Active Directory permissions to register an application with your Azure Active Directory
- Check Azure Subscription permissions to assign the application to a role in your Azure subscription

Assign Azure Active Directory permissions

Navigate to Azure Active Directory > User Settings and then ensure that the App registrations are allowed for your Azure subscription.

If your Azure subscriptions has the app registrations setting set to No, you need to check whether your account is an admin or user for the Azure AD account.
To check if your account is an admin, go to Overview and look at your user information.

If your account is assigned to the User role, but the app registration setting is restricted to admin users, you will not be permitted to register new apps. In such case, ask your administrator to either assign you to the global administrator role, or to enable users to register apps.

**Check Azure Subscription permissions**

In your azure subscription, your account must have Owner access role to assign an AD app to a reader role. If your account is assigned to the Contributor role, you do not have adequate permission and will receive an error when attempting to assign the service principal to a role.

To know the role assigned to you, select your account (refer image) and select My permissions. From the Subscription drop-down list, select the subscription for which you would want to check permissions and then click the “Click here to view complete access details for this subscription” link.
Steps to Create Azure Connector

On the Configuration tab, select Create Connector > Microsoft Azure.

Provide a name and description (optional) for your connector.

Next we’ll describe how to configure the application ID, directory ID, authentication key and subscription ID from the Microsoft Azure console to paste into your connector details.
Application ID
Create an application in Azure Active Directory. Log on to the Microsoft Azure console and go to Azure Active Directory in the left navigation pane, then App registrations. Click New application registration.

Provide these details:
Name: A name for the application (e.g. Azure connector)
Application type: Select Web app/API
Sign-on URL: Enter any valid URL. You can enter a URL that does not exist, but it must be in valid format.

Click Create. The newly created app is displayed in the list of applications.
Copy the Application ID and paste it into the connector details.

Directory ID
This is the unique identifier of your Azure Active Directory. In the Azure Active Directory blade, go to Properties. Copy the Directory ID and paste it into the connector details.
Authentication Key
You must provide permission to the new application to access the Windows Azure Service Management API and create a secret key.

Provide permission: Select the application that you created and go to Settings > Required permissions. Click Add > Select an API > Windows Azure Service Management API, and click Select.

Select required Delegated Permissions, click Select and then click Done.

Create secret key: Select the application that you created and go to Settings > Keys. Add a description and expiry duration for the new key and click Save. The value of the key appears in the Value field.

Copy the key value at this time. You won’t be able to retrieve the key later. Note down the secret key and store it securely with you. You’ll need to provide the key value with the application ID to log on as the application.
Subscription ID

Grant permission for the application to access subscriptions. Assign a role to the new application. The role defines the permissions for the new application to access subscriptions. Repeat these steps to add more subscriptions.

On the Microsoft Azure portal, navigate to Subscriptions.

Select the subscription for which you want to grant permission to the application, and choose Access Control (IAM). Go to Add > Select a role. Pick the role you want to give to the user. For example, the Reader role. A Reader can view everything, but cannot make any changes to the resources of a subscription.

Select Azure AD user, group, or application in Assign Access to drop-down. Search for your application, and select it. Then click Save to finish assigning the role. You’ll see your application in the list of users assigned to a role for that scope.

Copy the subscription ID you noted and paste it into the connector details in the Qualys Azure Connector screen and then click Create Connector.
Securing Cloud Resources

Upon setting up your connector, it starts discovering the resources that are present in your cloud account. The resources inventory and the metadata of the resources is pushed to Qualys portal. You can navigate to the Resources tab to view the resources getting collected along with their details.

Dashboard

The Qualys CloudView application provides out-of-the box default AWS Security Overview Dashboard providing a summary of inventory and security posture across resources.

The default dashboard provides:
- Resource inventory - Route Tables, EC2 Instances, VPC, Subnets, IAM Users, etc
- Total evaluation failures i.e. the resources misconfigurations by control criticality
- Security posture at each region level showing resources and failures
- Top 5 Accounts with maximum control failures
- Top 5 Failed controls

Check out this sample dashboard
Resources Details

The Resources tab displays the information about various resources collected. It helps you to identify the number of resources for each type and the number of resources that have one or more control failures. You can click on a row to view the number of resources of a specific type. You can click on an individual resource to view the details. For each resource you will view the following information.

Resources Summary

The List View provides a summary of your resources, including the total resources and the number of failed resources for each resource type.

Let us consider an example of Instance (EC2 Instance) and Security Group resource type to view the resource details and information.
Instance Details

Click Instance type to drill-down into your AWS EC2 instances.

Then click on any EC2 Instance ID to see the number of detected vulnerabilities, resource associations, location and network information.
Vulnerability Details
Click on the Vulnerabilities count to get information about detected vulnerabilities.

The vulnerability related data is populated only if you are using a scanner appliance or Cloud Agent.
View Security Group Information
You could view more details about a security group resource. Go to Resources > Security Group, and then click the security group ID to view additional details about it.

View Security Group Associations
You can view various details about the associations such as the ID, region, state and so on.
**View Controls Evaluated**

You can view the controls that are evaluated for the resource and if the controls have passed or failed.
Resources Misconfigurations

CloudView compares controls from the out-of-box policies that define the desired configuration of a resource against the current configuration of the resource. If it finds a difference, then it marks the resource as failed for that particular control. Each control is evaluated against the applicable resources. If all the applicable resources are configured as per the desired configuration of the control, then the control is marked as Pass. If at least one of the applicable controls doesn’t comply with the control, then it is marked as failed. The Monitor tab will display all such misconfigurations.

Controls Evaluation View

(1) Total Resources - The unique number of resources evaluated against all the controls.
(2) Security Posture - How many control evaluations have passed and failed.
(3) Failures By Critically - Control evaluation failures by control criticality.

Each control is evaluated against the applicable resources which is represented by Total Resources. Number represented by green represents the number of pass resources that have the desired configuration as per the control. Number represented by red represents the number of failed resources.

Click on any control to get details of all the resources evaluated against the control.
Control Evaluation Details
Control details screen shows the number of resources evaluated against the control. For each resource it shows Unique Resource ID, Account ID, Region, etc. You can use the search filter to view pass/failed resources.

Resource Evidence
To get more details on why a resource failed, click the Evidence link to see actual values for the resource attributes.
**View Remediation Steps**
Click the Remediation Steps tab to learn the steps needed to fix the failure.

**View Control Evaluation Results per Account**
Quickly view how many controls are passed/failed by clicking the account filter.
CloudView APIs

Many CloudView features are available through REST APIs. You can use Swagger tool to access the REST APIs we support.

Accessing APIs Using Swagger

Swagger is a widely-adopted specification that allows for programmatically describing REST APIs. The Swagger UI provides all the details about the APIs and how to invoke them. This includes information like the HTTP verbs to use (GET, POST, PUT, etc.), the URL paths, allowable parameters and types, and so on.

You can directly access the Swagger UI from the following URL:

http://<QualysURL>/cloudview-api/swagger-ui.html

For example, if your account is on US Platform 2


Qualys maintains multiple platforms. The Qualys URL that you should use for API requests depends on the platform where your account is located.

Qualys Platform URLs

<table>
<thead>
<tr>
<th>Platform Type</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys US Platform 1</td>
<td><a href="https://qualysguard.qualys.com">https://qualysguard.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 2</td>
<td><a href="https://qualysguard.qg2.apps.qualys.com">https://qualysguard.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 3</td>
<td><a href="https://qualysguard.qg3.apps.qualys.com">https://qualysguard.qg3.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys EU Platform 1</td>
<td><a href="https://qualysguard.qualys.eu">https://qualysguard.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys EU Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.eu">https://qualysapi.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys India Platform 1</td>
<td><a href="https://qualysguard.qg1.apps.qualys.in">https://qualysguard.qg1.apps.qualys.in</a></td>
</tr>
</tbody>
</table>
Do I need to Authenticate?
Authentication to the Qualys Cloud Platform is necessary before you try out the APIs.

Simply, click Authorize and provide the user name and password. You can now use the APIs!

API List
Here is the list of the APIs we currently support and a short description of what you can achieve through the API.

<table>
<thead>
<tr>
<th>API Objective</th>
<th>Operator</th>
<th>API Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Evaluations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get the list of</td>
<td>GET</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/evaluations/{accountId}</td>
<td>Provide the AWS account ID (required parameter) and get the list of evaluations for AWS Controls associated with the specified AWS account. You also need to specify the page number and the number of records to be returned per page.</td>
</tr>
<tr>
<td>evaluations for an</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get resource</td>
<td>GET</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/evaluations/{accountId}/</td>
<td>Get the resources evaluated for the specified AWS account ID (required parameter) and control ID (required parameter). You also need to specify the page number and the number of records to be returned per page.</td>
</tr>
<tr>
<td>evaluations for an</td>
<td></td>
<td>resources/{controlId}</td>
<td></td>
</tr>
<tr>
<td>account and control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get AWS account ID</td>
<td>GET</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/connectors/qualys AwsAccountId</td>
<td>Get the AWS account ID of Qualys.</td>
</tr>
<tr>
<td>Connector</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get the list of</td>
<td>GET</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/connectors</td>
<td>Get the list of all the connectors in AWS account you specify. You also need to specify the page number and the number of records to be returned per page.</td>
</tr>
<tr>
<td>connectors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get AWS account ID</td>
<td>GET</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/connectors/qualys AwsAccountId</td>
<td>Get the AWS account ID of Qualys.</td>
</tr>
<tr>
<td>Get connector details</td>
<td>GET</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/connectors/{connectorId}</td>
<td>Specify the connector ID and you can get the details of a connector.</td>
</tr>
<tr>
<td>Get error list</td>
<td>GET</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/connectors/{connectorId}/errors</td>
<td>Get the list of errors encountered when executing a specific connector. You also need to specify the page number and the number of records to be returned per page.</td>
</tr>
<tr>
<td>Create new connector</td>
<td>POST</td>
<td>https://&lt;QualysURL&gt;/cloudview-api/rest/1.5/aws/connectors</td>
<td>Specify the connector details such as qualysAccountId, arn, externalId, and so on and create a new connector.</td>
</tr>
</tbody>
</table>
Let us see few examples to understand how the REST APIs work.

**API Examples**

**Example 1: Get the list of all the control evaluations (passed and failed) for a specified AWS account**

Request URL: GET https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}

Sample URL:

```
```

where:

- `accountId` (required): 11111111111 is sample AWS account ID associated with the connector
- `pageNo` (required): 1 is the page to be returned
- `pageSize`: 50 is the number of records to be returned per page

**Sample Response:**

```
{
  "content": [
    {
      "controlName": "Ensure IAM Password Policy is Enabled",
      "policyName": "CIS Amazon Web Services Foundations Benchmark",
      "criticality": "HIGH",
      "service": "IAM",
      "result": "PASS",
      "controlId": "6",
```
Example 2: Get the list of all the failed control evaluations for a specific AWS account

In earlier example we provided both passed and failed control for a specified AWS account. Let us now filter failed controls using following request.

**Request URL:** GET https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}?filter=control.result:{FAIL}&pageNo=1&pageSize=50

**Sample URL:**

```
```

where:

- **accountId** (required): 11111111111 is sample AWS account ID associated with the connector
- **filter=control.result:FAIL or PASS** depending on the type of control evaluations you want to filter
- **pageNo** (required): 1 is the page to be returned
- **pageSize**: 50 is the number of records to be returned per page
Sample Response:

```json
{
   "content": [
      {
         "controlName": "Ensure IAM password policy requires at least one uppercase letter",
         "policyName": "CIS Amazon Web Services Foundations Benchmark",
         "criticality": "HIGH",
         "service": "IAM",
         "result": "FAIL",
         "controlId": "7",
         "passedResources": 0,
         "failedResources": 1
      },
      {
         "controlName": "Ensure IAM password policy require at least one symbol",
         "policyName": "CIS Amazon Web Services Foundations Benchmark",
         "criticality": "HIGH",
         "service": "IAM",
         "result": "FAIL",
         "controlId": "9",
         "passedResources": 0,
         "failedResources": 1
      },
      ...
   ],
   "last": true,
   "totalPages": 1,
   "totalElements": 33,
   "first": true,
   "sort": null,
   "numberOfElements": 33,
   "size": 50,
   "number": 0
}
```
Example 3: Get the resources evaluated by specifying AWS account ID and control ID

Request URL: GET https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}?resources/{conrolId}&pageNo=1&pageSize=50

Sample URL:

where:
- accountId (required): 11111111111 is sample AWS account ID associated with the connector
- 44 is the control Id
- pageNo (required): 1 is the page to be returned
- pageSize: 50 is the number of records to be returned per page

Sample Response:

```json
{
  "content": [
    {
      "resourceId": "sg-474f6a39",
      "region": "us-west-2",
      "accountId": "11111111111",
      "evaluatedOn": "2018-07-16T05:42:16+0000",
      "evidences": [
        {
          "settingName": "Number of Inbound Rules",
          "actualValue": "1",
          "expectedValue": ""
        },
        {
          "settingName": "Number of Outbound Rules",
          "actualValue": "1",
          "expectedValue": ""
        }
      ],
      "resourceType": "VPC_SECURITY_GROUP",
      "result": "FAIL"
    },
    {
      "resourceId": "sg-acd511c4",
      "region": "us-east-2",
      "accountId": "11111111111",
      "evaluatedOn": "2018-07-16T05:42:19+0000",
      "evidences": [
```
CloudView APIs
API List

{
    "settingName": "Number of Inbound Rules ",
    "actualValue": "1",
    "expectedValue": ""
},
{
    "settingName": "Number of Outbound Rules ",
    "actualValue": "1",
    "expectedValue": ""
}
"resourceType": "VPC_SECURITY_GROUP",
"result": "FAIL"
},

Example 4: Create AWS connector
Request URL: POST https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors
Request Body

{    "arn": "<specify role arn>",
    "description": "<give description for the connector>",
    "externalId": "<external ID of your connector>",
    "name": "<name for the connector>",
    "qualysAccountId": "805950163170"
}

where:
-arn: Specify the ARN of the cross-account role you created in your AWS account.
-description is optional and you can give a short description stating the purpose of the connector you want to create.
-externalId: Specify the external ID that you have provided in AWS while creating the cross-account role.
-name is the name for the connector you want to create.

Sample Response:

201 Created

The response code 201 is returned when the connector is successfully created.