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
AWS..................................................................................................................................... 7
Steps to Create AWS Connector ....................................................................................... 7
AWS Resource Inventory ................................................................................................. 12
Microsoft Azure ................................................................................................................ 14
Pre-requisites .................................................................................................................... 14
Steps to Create Azure Connector ...................................................................................... 15
Azure Resource Inventory ................................................................................................. 21
Google Cloud Platform .................................................................................................... 21
Steps to Create GCP Connector ....................................................................................... 21
GCP Resource Inventory ................................................................................................. 26

Securing Cloud Resources .............................................................................................. 27
Dashboard ......................................................................................................................... 27
Resources Details .............................................................................................................. 28
Instance Details ................................................................................................................ 29
View Security Group Information ..................................................................................... 32
Resources Misconfigurations ............................................................................................ 34

Policies and Controls ...................................................................................................... 38
AWS Best Practices Policy ............................................................................................... 38
CIS Amazon Web Services Foundations Benchmark ...................................................... 40
CIS Microsoft Azure Foundations Benchmark .............................................................. 42
CIS Google Cloud Platform Foundation Benchmark ...................................................... 44

Reports .............................................................................................................................. 45
Report Template and Reports .......................................................................................... 45
Mandate Based Reporting ............................................................................................... 45
Policy Based Report ......................................................................................................... 48

CloudView APIs .............................................................................................................. 53
Accessing APIs Using Swagger ....................................................................................... 53
What's more in CloudView................................................................. 55
Role-based Access Management....................................................... 55
Download Datalist........................................................................... 58
Choosing Data Range ...................................................................... 59
Saved Search.................................................................................. 59
Customize Dashboards .................................................................. 61
  How to Take Action ...................................................................... 61
  Adding custom widgets .............................................................. 61
  Refresh your view ...................................................................... 63
  Configure number of Resources, Controls ................................ 63
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 AWS and Azure policies
- Continuously assess and report on resource misconfigurations by checking against the controls from out-of-box policies
- Ability to view, filter and export misconfigurations.

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 access to 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>
<tr>
<td>Control</td>
<td>A configuration check. Each check applies to a specific service/resource. Here are some examples:</td>
</tr>
<tr>
<td>Service</td>
<td>A service is the high level grouping by functional area. Each service consists of different entities or resources.</td>
</tr>
</tbody>
</table>

- 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
<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>A resource is an entity that you can work with. Examples include an Amazon EC2 instance, IAM User, Security Group.</td>
</tr>
<tr>
<td>Control Passed</td>
<td>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.</td>
</tr>
<tr>
<td>Control Failed</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Passed</td>
<td>Resource is considered passed for a control if it's attribute is configured as per the desired configuration in the control.</td>
</tr>
<tr>
<td>Resource Failed</td>
<td>Resource is considered failed for a control if it's attribute is not configured as per the desired configuration in the control.</td>
</tr>
</tbody>
</table>
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, Azure and GCP connectors. We’ll walk you through the steps.

AWS

Configure AWS connectors for gathering resource information from your AWS account. It just takes a couple of minutes.

Steps to Create AWS Connector

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

Click Create policy in Attach Permissions policies section. This opens Policy Creation wizard in new tab. Select JSON and add the content mentioned below:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketPublicAccessBlock"
        ],
        "Resource": "*
    }
}
```

Click Review policy and provide a name for this policy (for example, BucketAccess). Click Save and close the tab. Go back to the Attach Permissions policies section.
In Attach Permissions policies section, refresh the policy list and select the policy you created (BucketAccess). Additionally, find the policy titled "SecurityAudit" and select the check box next to it. Click Next: tags and then Next: Review. Click Next: Tags.

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.

A unique external ID gets generated during connector creation. You can also use your own external ID (ensure that the external ID is numeric and the character length is from 9-96 characters).

Select Create Connector in AssetView check box (optional). 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.

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.

**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.

AWS Resource Inventory

Upon setting up the AWS connector, it starts discovering the resources that are present in your AWS account. The inventory and the metadata of the resources is pushed to Qualys portal. For list of the resources that are getting collected, refer Resources List. To fetch the updated resources, you need to select Run from the quick actions menu for the AWS connector.

What do you achieve?
- Get centralized visibility of services/resources across your multiple AWS accounts.
- Identify services/resources running your AWS account. For list of resources getting collected, refer Resources List.
- Identify the number of resources that are non-compliant.
- View resource details and their associations with other resources.
- Locate the resources by querying the resource attributed, account & region etc.
- Search tagged/untagged resources using AWS tags.
- Trend chart and time range will help you understand the how the resources are varied over the past 7, 30 days. You can also specify the custom range.
Resources List
CloudView will discover and fetch following AWS resources and their corresponding attributes.
- Subnet
- Network ACL
- Internet Gateway
- Load Balancer
- Instance
- Route Table
- S3 Bucket
- IAM User
- VPC
- Auto Scaling Group
- Security Group
- RDS
- EBS Volume
Microsoft Azure

Configure Microsoft Azure connectors for gathering resource information from your Microsoft Azure account. It just takes a couple of minutes.

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.
Azure Resource Inventory
Upon setting up the Azure connector, it starts discovering the resources that are present in your Azure account. The inventory and the metadata of the resources is pushed to Qualys portal. For list of the resources that are getting collected, refer Resources List. To fetch the updated resources, you need to select Run from the quick actions menu for the Azure connector.

Resources List
CloudView will discover and fetch following Azure resources and their corresponding attributes.
- SQL Server
- SQL Server Database
- Resource Group
- Virtual Network
- Virtual Machine
- Network Security Group

Google Cloud Platform
Configure a Google Cloud Platform (GCP) connector for gathering resource information from your Google Cloud Platform project. It just takes a couple of minutes.

Steps to Create GCP Connector
Go to the Configuration > Google Cloud Platform and then click Create Connector.
(1) Provide a name and description (optional) for your connector.

(2) You need to download the configuration file from the GCP console and then upload it to Qualys Cloud Platform to complete GCP connector creation.

(3) Click Create Connector.

That’s it! The connector will establish a connection with GCP to start discovering resources from each region.
Let us see the steps to download the configuration (JSON) file from GCP console and set up the required authentication details. You need to enable access to the necessary APIs from the API library.

**Enable Access to Compute Engine and Resource Manager API**

(1) Navigate to Google Cloud Platform (GCP) console.

(2) Select the organization.

(3) Select a project or create a new project. Ensure that you select the correct project.

(4) In the left sidebar, navigate to APIs and Services.
(5) Search Compute Engine API from the API Library, click Manage and then click Enable API. Similarly, also enable Cloud Resource Manager API, Compute Engine API, Kubernetes Engine API and Cloud SQL Admin API from the API library.

Similarly, enable Cloud Resource Manager API from the API library.

**Create Service Account and Download Configuration File**

(1) Login to the GCP console and select a project.

(2) From the left sidebar, navigate to IAM & admin > Service accounts and click CREATE SERVICE ACCOUNT. Provide a name and description (optional) for the service account and click Create.
(3) Choose Viewer role to assign at least reader permissions to the service account and click Continue.

![Google Cloud Platform interface with role selection]

(4) Click CREATE KEY and select JSON as Key type and click Create.

![Create key interface with JSON selection]

A message saying “Private key saved to your computer” is displayed and the JSON file is downloaded to your computer. Click Close and then click Done.

Upload the configuration (JSON) file and click Create Connector to complete GCP connector creation in Qualys Cloud Platform.
GCP Resource Inventory

Upon setting up the Google Cloud Platform (GCP) connector, it starts discovering the resources that are present in your GCP account. The inventory and the metadata of the resources is pushed to Qualys portal. For list of the resources that are getting collected, refer Resources List. To fetch the updated resources, you need to select Run from the quick actions menu for the GCP connector.

Resources List

CloudView will discover and fetch following GCP resources and their corresponding attributes.

- VM Instances
- Networks
- Firewall Rules
- Subnetworks
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 Dashboard providing a summary of inventory and security posture across resources. We also support Microsoft Azure dashboard.

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. You could also use the filters in the left pane to narrow down resources per region or account.
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.

The Evaluation Summary tells you the following facts as well:
- First Evaluated: The date when the control was evaluated for the first time.
- Last Evaluated: The latest date when the control was evaluated.
- Last Reopened: The latest date when the control evaluation result is changed from pass to fail.

- Last Fixed: The latest date when the control evaluation control result is changed from fail to pass.

**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.
Policies and Controls

CloudView continuously discovers resources and ensures resources are compliant in relation to respective Benchmark & Best Practices policy provided out-of-box.

The Policies tab lists the policies we currently support.

AWS Best Practices Policy
CIS Amazon Web Services Foundations Benchmark
CIS Microsoft Azure Foundations Benchmark
CIS Google Cloud Platform Foundation Benchmark

AWS Best Practices Policy

We support controls for following AWS resources:

S3 Controls
RDS Controls
Account

S3 Controls
CID 45: S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users
CID 46: Ensure S3 Bucket Policy does not allow anonymous (public) access to S3 bucket
CID 47: Ensure access logging is enabled for S3 buckets
CID 48: Ensure versioning is enabled for S3 buckets
CID 57: Ensure that bucket policy enforces encryption in transit
CID 59: Ensure "Block new public bucket policies" for a bucket is set to true.
CID 60: Ensure that "Block public and cross-account access" if bucket has public policies for bucket is set to true.
CID 61: Ensure that "Block new public ACLs and uploading public objects" for a bucket is set to true.
CID 62: Ensure that "Remove public access granted through public ACLs" for a bucket is set to true.
CID 63: Ensure 'Block new public bucket policies' for an AWS Account is set to true.
CID 64: Ensure 'Block public and cross-account access to buckets that have public policies' for an AWS Account is set to true.
CID 65: Ensure 'Block new public ACLs and uploading public objects' for an account is set to true.
CID 66: Ensure 'Remove public access granted through public ACLs' for an account is set to true.
CID 67: Ensure Server Side Encryption (SSE) is enabled for S3 bucket.

**RDS Controls**
CID 51: Ensure that Public Accessibility is set to No for Database Instances
CID 52: Ensure DB snapshot is not publicly visible
CID 53: Ensure Encryption is enabled for the database Instance
CID 54: Ensure database Instance snapshot is encrypted
CID 55: Ensure auto minor version upgrade is enabled for a Database Instance
CID 56: Ensure database Instance is not listening on to a standard/default port

**IAM**
CID 58: Ensure that the key expiry is set for CMKs with external key material.
CID 68: 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.
CIS Amazon Web Services Foundations Benchmark

We support controls for following AWS resources:

Identity and Access Management (IAM) Controls

CloudTrail Controls

VPC Controls

Config Controls

Identity and Access Management (IAM) Controls

CID 1: Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
CID 2: Ensure console credentials unused for 90 days or greater are disabled
CID 3: Ensure access keys unused for 90 days or greater are disabled
CID 4: Ensure access key1 is rotated every 90 days or less
CID 5: Ensure access key2 is rotated every 90 days or less
CID 6: Ensure IAM Password Policy is Enabled
CID 7: Ensure IAM password policy requires at least one uppercase letter
CID 8: Ensure IAM password policy require at least one lowercase letter
CID 9: Ensure IAM password policy require at least one symbol
CID 10: Ensure IAM password policy require at least one number
CID 11: Ensure IAM password policy requires minimum length of 14 or greater
CID 12: Ensure IAM password policy prevents password reuse
CID 13: Ensure IAM password policy expires passwords within 90 days or less
CID 14: Ensure no root account access key exists
CID 15: Ensure MFA is enabled for the root account
CID 16: Ensure hardware MFA is enabled for the root account
CID 17: Ensure IAM policies are attached only to groups or roles
CID 18: Avoid the use of the root account
CID 26: Ensure rotation for customer created CMKs is enabled
CID 49: Ensure a support role has been created to manage incidents with AWS Support
CID 50: Ensure IAM policies that allow full administrative privileges are not created
CloudTrail Controls
CID 19: Ensure CloudTrail is enabled in all regions
CID 20: Ensure CloudTrail log file validation is enabled
CID 21: Ensure the S3 bucket CloudTrail logs to is not publicly accessible
CID 22: Ensure CloudTrail trails are integrated with CloudWatch Logs
CID 24: Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket
CID 25: Ensure CloudTrail logs are encrypted at rest using KMS CMKs
CID 27: Ensure a log metric filter and alarm exist for unauthorized API calls
CID 28: Ensure a log metric filter and alarm exist for Management Console sign-in without MFA
CID 29: Ensure a log metric filter and alarm exist for usage of "root" account
CID 30: Ensure a log metric filter and alarm exist for IAM policy changes
CID 31: Ensure a log metric filter and alarm exist for CloudTrail configuration changes
CID 32: Ensure a log metric filter and alarm exist for AWS Management Console authentication failures
CID 33: Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs
CID 34: Ensure a log metric filter and alarm exist for S3 bucket policy changes
CID 35: Ensure a log metric filter and alarm exist for AWS Config configuration changes
CID 36: Ensure a log metric filter and alarm exist for security group changes
CID 37: Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)
CID 38: Ensure a log metric filter and alarm exist for changes to network gateways
CID 39: Ensure a log metric filter and alarm exist for route table changes
CID 40: Ensure a log metric filter and alarm exist for VPC changes

VPC Controls
CID 41: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22
CID 42: Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389
CID 43: Ensure VPC flow logging is enabled in all VPCs
CID 44: Ensure the default security group of every VPC restricts all traffic

Config Controls
CID 23: Ensure AWS Config is enabled in all regions
CIS Microsoft Azure Foundations Benchmark

We support controls for following Azure resources:

- Security Centre Controls
- Storage Accounts Controls
- SQL Servers Controls
- Logging and Monitoring Controls
- Networking Controls
- Virtual Machines Controls
- Controls for Other Security Considerations

**Security Centre Controls**

CID 50015: Ensure that standard pricing tier is selected
CID 50004: Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'
CID 50005: Ensure ASC Default policy setting Monitor System Updates is not Disabled
CID 50006: Ensure ASC Default policy setting Monitor OS Vulnerabilities is not Disabled
CID 50007: Ensure ASC Default policy setting Monitor OS Endpoint Protection is not Disabled
CID 50008: Ensure ASC Default policy setting Monitor Disk Encryption is not Disabled
CID 50009: Ensure ASC Default policy setting Monitor Network Security Groups is not Disabled
CID 50010: Ensure ASC Default policy setting Monitor Web Application Firewall is not Disabled
CID 50016: Ensure ASC Default policy setting Enable Next Generation Firewall(NGFW) Monitoring is not Disabled
CID 50017: Ensure ASC Default policy setting Monitor Vulnerability Assessment is not Disabled
CID 50018: Ensure ASC Default policy setting Monitor SQL Auditing is not Disabled
CID 50025: Ensure ASC Default policy setting Monitor SQL Encryption is not Disabled
CID 50019: Ensure ASC Default policy setting Monitor JIT Network Access is not Disabled
CID 50003: Ensure ASC Default policy setting Monitor Application Whitelisting is not Disabled
CID 50014: Ensure ASC Default policy setting Monitor SQL Auditing is not Disabled
CID 50020: Ensure that 'Security contact emails' is set
CID 50021: Ensure that security contact 'Phone number' is set
CID 50022: Ensure that 'Send me emails about alerts' is set to 'On'
CID 50023: Ensure that 'Send email also to subscription owners' is set to 'On'

**Storage Accounts Controls**
CID 50011: Ensure that Secure transfer required for a Storage Account is set to Enabled
CID 50012: Ensure that 'Public access level' is set to Private for blob containers

**SQL Servers Controls**
CID 50013: Ensure that 'Auditing' is set to 'On'
CID 50013: Ensure that 'AuditActionGroups' in 'auditing' policy for a SQL server is set properly
(This will be part of next release of CIS benchmark)
CID 50028: Ensure that 'Threat Detection' is set to 'On'
CID 50028: Ensure that 'Threat Detection types' is set to 'All'
CID 50028: Ensure that 'Send alerts to' is set
CID 50028: Ensure that 'Email service and co-administrators' is 'Enabled'
CID 50013: Ensure that 'Auditing' Retention is 'greater than 90 days'
CID 50028: Ensure that 'Threat Detection' Retention is 'greater than 90 days'
CID 50035: Ensure that Azure Active Directory Admin is configured for a SQL Server
CID 50027: Ensure SQL server's TDE protector is encrypted with BYOK (Use your own key)
(This will be part of next release of CIS benchmark)

**Logging and Monitoring Controls**
CID 50024: Ensure that a Log Profile exists
CID 50024: Ensure that Activity Log Retention is set 365 days or greater
CID 50024: Ensure Audit Profile Captures all the activities
(This will be part of next release of CIS benchmark)

**Networking Controls**
CID 50029: Disable RDP access on Network Security Groups from Internet (ANY IP)
CID 50031: Disable SSH access on Network Security Groups from Internet (ANY IP)
CID 50002: Ensure that SQL server access is restricted from the internet

**Virtual Machines Controls**
CID 50032: Ensure that all the vm disks are encrypted

**Controls for Other Security Considerations**
CID 50030: Ensure that the expiry date is set on all Secrets
CID 50026: Ensure keyvault is recoverable
(This will be part of next release of CIS benchmark)

**CIS Google Cloud Platform Foundation Benchmark**

We support controls for following Google Cloud Platform (GCP) resources:

**IAM & Admin**
52001: Ensure that there are only GCP-managed service account keys for each service account

**Storage**
52010: Ensure that object versioning is enabled on all the buckets (Note: This control will be a part of next CIS release.)
52030: Ensure that Cloud Storage bucket is not anonymously or publicly accessible
52031: Ensure that logging is enabled for Cloud storage buckets

**Virtual Network**
52023: Ensure Private Google Access is enabled for all subnetwork in VPC Network
52024: Ensure VPC Flow logs is enabled for every subnet in VPC Network

**SQL**
52032: Ensure that Cloud SQL database instance requires all incoming connections to use SSL

**Kubernetes Engine**
52039: Ensure Kubernetes web UI / Dashboard is disabled
52040: Ensure `Automatic node repair` is enabled for Kubernetes Clusters
52041: Ensure Automatic node upgrades is enabled on Kubernetes Engine Clusters nodes
52043: Ensure Network policy is enabled on Kubernetes Engine Clusters
52045: Ensure Kubernetes Cluster is created with Alias IP ranges enabled
52046: Ensure PodSecurityPolicy controller is enabled on the Kubernetes Engine Clusters
52047: Ensure Kubernetes Cluster is created with Private cluster enabled
52049: Ensure default Service account is not used for Project access in Kubernetes Clusters
Reports

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 in terms of the underlying Security baseline 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.

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

![Image of a custom report template](image)

![Image of report statistics](image)

**Policy Based Report**

Policies are set of controls. We provide ability to generate policy specific compliance report. We support report generation for policies and mandates only for AWS.

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 Policy in the report type, select the Policy from the drop-down and then click Next. You can select multiple policies.
4) Select the account or connector you want to evaluate for compliance.

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

Use Go to options to navigate to the different sections of the report.

Report Info:
- Created Date: April 11, 2019 2:54 PM
- Created By: John Doe
- Username: user_john

Accounts:
- My Sample Connector: 111111111111
- Example Connector: 222222222222

Report Summary:
- Controls: 46
- Total Evaluations: 1417
- Passes: 1

Report Statistics:
- Overall Policy Posture:
  - Pass: 97.73% (138 of 1417)
  - Fail: 2.27% (34 of 1417)
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


API Examples

You can view examples and details on API usage in our CloudView API User Guide.
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</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!
What’s more in CloudView

We also provide you with many more quick features such as downloading data in CSV format, saving your search queries, using date filters.

Role-based Access Management

Qualys CloudView is subject to Role-Based Access Control. Users are granted access to features and functions based on Roles. These Roles are a consolidate of fine grained Permissions.

A set of Permissions are grouped together as a Role. A User is assigned one, or more, Roles. The sum of the Permissions that are granted a User represent all the rights to access features and functions that a User has.

You can:
- Block or provide UI access to CloudView module
- Provide UI access to CloudView module with restricted permissions (read-only user)
- Provide full UI access to CloudView module with all permissions

Permissions: Only users with access to Administration module can create sub-users with reader role.

What can the Reader User do?
The user with reader role can
- View connectors
- Monitor controls, policies and resources
- Create and edit dashboards

However, the user with reader role cannot create connector or evaluate controls, policies.
Quick Steps

1) Create a User in Vulnerability Management (Navigate to Vulnerability Management module from module picker and then go to Users tab to create a new user).

2) Create a role in Administration utility (Navigate to Administration utility from module picker and then go to Role Management tab).

Let us consider scenarios to configure different level of access for users. You could create different roles or modify permissions for an existing role.

Access

These permissions do not refer to a specific feature or function but determine if access to the interface as a whole is allowed for a user.

UI Access: Allow or deny a given user account access to the graphical user interface. This permission must be in at least one Role for a user to be able to log into Qualys' web site and use the Qualys CloudView module.

API Access: Allow or deny a given user account access to the Application Programming Interface. This permission may impact custom integration projects that were built around a customer's Qualys service by a 3rd party.
Scenario 1: Provide full UI access to CloudView module with all permissions

![Image of Role Creation wizard with full UI access permissions]

Ensure that the role has UI access permission and CLOUDVIEW Readonly Access, CLOUDVIEW UI Access enabled

Once you configure the permissions for a role, assign the role to the required users, and the users will gain access as per the configured permissions.

Scenario 2: Provide UI access to CloudView module with restricted permissions (read-only user)

![Image of Role Creation wizard with restricted UI access permissions]

Once you configure the permissions for a role, assign the role to the required users, and the users will gain access as per the configured permissions.
Download Datalist

By downloading datalist to your local system you can easily manage the list outside of the Qualys platform and share them with other users. You can download results in CSV format.

The datalist that is available for download includes resources (grouped view and resource view), controls, control evaluations, and connectors list.

The download is limited to 5,000 records.

1) Use our search to narrow down your results.

2) Select Download from the Tools menu.

3) Click Download. That's it!

Select the Change timezones for dates included in a report checkbox and select the required timezone to convert the dates in the CSV report to the desired timezone.
Choosing Data Range

Narrow down your search results for controls using our new date filter. The new date filter provides 8 options: Today, Yesterday, Last 7 days, Last 30 days, Last 90 days, This Month, Last Month, and Specific range. Depending on the date option you choose, the search results displays controls that are evaluated within the chosen date range.

Go to Monitor tab, type your search query in the search pane and then choose the date filter to further filter your search results.

Saved Search

You can easily save your searches for reuse and share them with other users. Enter your search query and then click Save this Search Query.
Give your search a title.

Choose Load/manage Saved Searches to use one of the searches you previously saved.

Delete any saved search you're no longer interested in.
Customize Dashboards

Dashboards help you visualize your assets. You can add widgets with search queries to see exactly what you’re interested in. You can also export and import Dashboard and Widget configurations, from the Tools menu, to a file in a json format allowing you to share them between accounts or within the Qualys community.

Each dashboard is a collection of widgets showing resource data of interest. You can create multiple dashboards and switch between them.

You can personalize the default dashboard - add widgets, resize them, move them around to change the layout. Use the menu to manage your dashboards.

How to Take Action

Here’s a quick look at your dashboard options. :

Take actions on the entire dashboard set the default, create dashboard, change layout, delete, print, export dashboard, import dashboard and import widget.

Take actions on a single widget: edit widget, delete widget, refresh widget data, create template from widget, export widget.

Adding custom widgets

1) Start by clicking the Add Widget button on your dashboard.

2) Pick one of our templates: CV pane has five default templates to choose from - or choose Custom pane to create your own widget. Let us consider an example of creating customized bar widget for Azure resources.
3) Each widget is unique. Define your custom settings. For some you’ll select query data source, a query, group by option, limit and layout - count, table, bar graph, pie chart.

a - Choose widget type: Count, Table, Column, Pie
b - Choose data source from the dropdown. For example: Azure Resources.
c - Provide a name for your widget.
d - Type your search query using pre-defined tokens.

The Preview pane displays the preview of your widget.

4) Click Add to Dashboard to view the widget in the dashboard. You could view the preview of the widget using the Test and Preview button.

From the Actions menu on the dashboard, you can also import and export widget configurations to a file in a json format, allowing you to share the widgets between accounts or within the Qualys community.

**Resizing and layout.**

Resize any widget horizontally, drag & drop widgets to change the layout. Refresh your view.

1) Click the Tools icon on your dashboard.
2) Select Edit Dashboard Layout
3) Adjust the width for any widget or drag the widget to a new location.
4) Click OK to save your changes.
Refresh your view

You might want to see the latest data for a particular widget. Select the widget menu and choose Refresh.

To refresh all widgets in one go, choose the Refresh Dashboard option from the Tools menu and all the widgets on the dashboard will be refreshed.

Configure number of Resources, Controls

You might also want to choose the number of resources or controls displayed in your Live Feed widget. You can choose to display: Top 10, Top 5, or Top 3 failed controls or resources.