Qualys Integration with AWS S3 Bucket

User Guide

August 24, 2023

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

Table of Contents

About this Guide

Welcome to Qualys Cloud Platform and the integration of Qualys Cloud Platform with AWS S3 Bucket! This guide will help you get acquainted with the Qualys solutions for integrating AWS S3 Bucket with Qualys Cloud 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 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/.

Introduction

Welcome to Qualys Cloud Platform that brings you solutions for securing your Cloud IT Infrastructure as well as your traditional IT infrastructure.

On Qualys Cloud Platform, you can view and retrieve vulnerability findings and compliance posture data using multiple methods such as interactive dashboards, reports, and APIs.

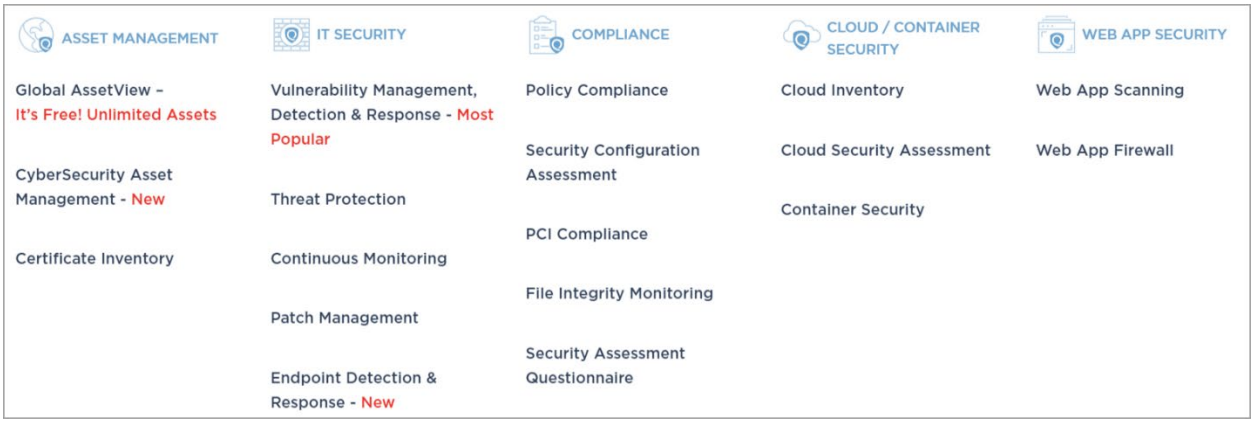
By integrating with AWS S3 Bucket, you get the data of your asset inventory directly on your AWS S3 storage in near real time, without having to run any API calls or generate any reports. CIPS (Cloud Integration Partner Service) proactively retrieves the data from Qualys Cloud Platform and transfers it to AWS S3 Bucket.

With the AWS S3 Bucket integration, you get a near real-time and up-to-date visibility of your security and compliance posture in your storage console. You can then use this data in correlation with other data in your cloud storage to know your exact security posture and take rapid remedial actions.

In this guide, you can find information about integrating Qualys findings with AWS S3 Bucket using CIPS (Cloud Integration Partner Service), so that you can use the findings further in your enterprise.

Qualys Integrated Security Platform

With Qualys Cloud Platform you get a single view of your security and compliance - in near real time. If you are new to Qualys, you can visit the Qualys Cloud Platform web page to know more about the platform.



Qualys Sensors

Qualys sensors, a core service of the Qualys Cloud Platform, make it easy to extend your security throughout your global enterprise. These sensors are remotely deployable, centrally managed and self-updating. They collect the data and automatically transmit it to the Qualys Cloud Platform, which has the computing power to continuously analyze and correlate the information in order to help you identify threats and eliminate vulnerabilities.

Virtual Scanner Appliances
Remote scan across your networks - hosts and applications

Cloud Agents
Continuous security view and platform for additional security

AWS Cloud Connectors
Sync cloud instances and its metadata

Internet Scanners
Perimeter scan for edge facing IPs and URLs

Web Application Firewalls
Actively defend intrusions and secure applications

Qualys Support for AWS S3 Bucket

You can now integrate with Amazon Simple Storage Service (Amazon S3), which is an object storage service. The service provides high scalability, data availability, security, and performance.

You can now access Qualys vulnerability assessment findings and Policy Compliance posture data in AWS S3 Bucket. By integrating the findings from Qualys Vulnerability Management (VM/VMDR) and Qualys Policy Compliance (PC) with AWS S3, you can get near real-time and up-to-date visibility of your security and compliance postures in AWS S3 console. These findings, gained by the correlation of Qualys information with other data in AWS S3, allow you to quickly detect risks and take rapid and automated remedial actions.

Currently, Qualys supports findings from only VM/VMDR and PC apps for AWS S3 Bucket integration.

Benefits

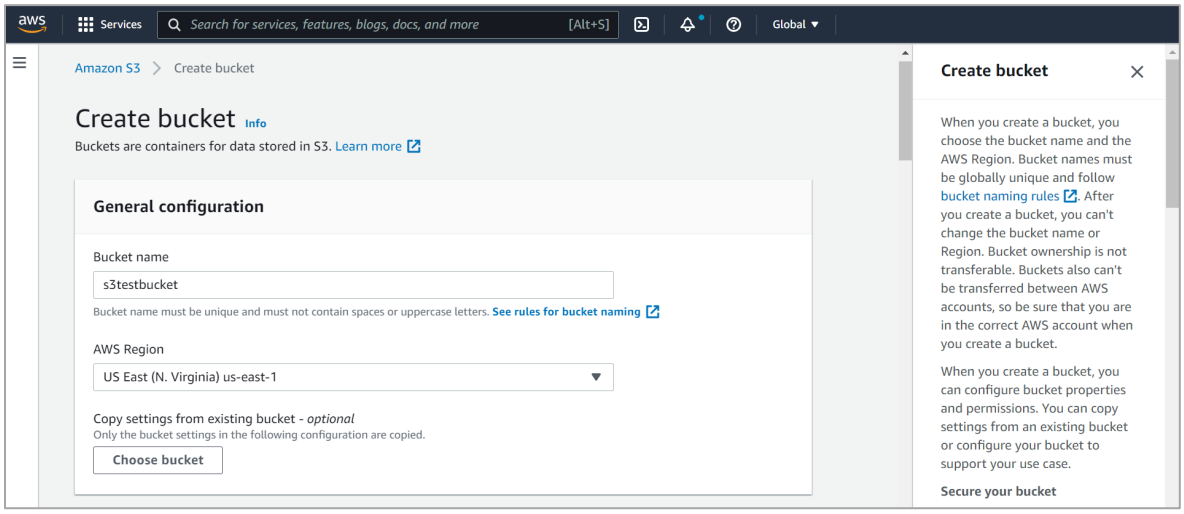
You get the following benefits on integrating with AWS S3 Bucket for VM/VMDR and PC data:

- Instantaneous and near real-time transfer of vulnerability and posture data to your preferred storage platform
- Automatic transfer of data to your storage platform without having to make any API calls. This eliminates the process of pulling large data from Qualys Cloud Platform using APIs.
- Easy and seamless postprocessing as the data is transferred in JSON format
- Flexibility to use this feature alongside the Qualys API services

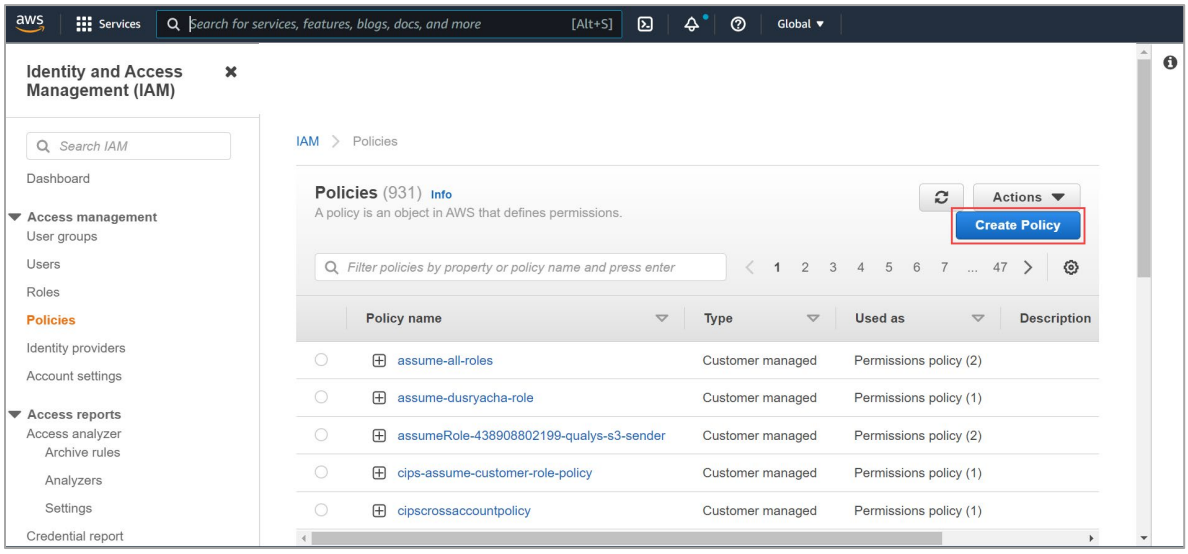
Configure an AWS S3 Integration

Perform the following steps to create a bucket with necessary permissions and configurations:

1. On the AWS portal, create an AWS S3 bucket.



2. Create a policy to give access with PutObject permissions to the bucket.



Here is a sample policy:

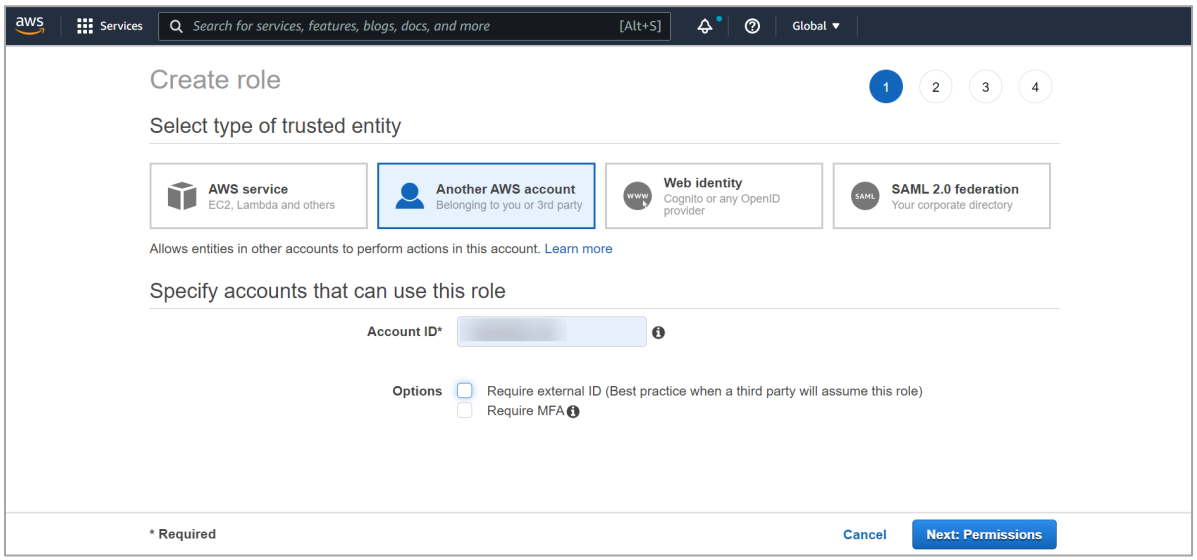
Policy to grant S3 bucket access

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
```

```
                ],
                "Resource": "arn:aws:s3:::sample-qualys-findings/*"
            }
        ]
    }
```

Note: 'sample-qualys-findings' is the bucketName.

3. Create a role on the AWS IAM console as follows:



a. Go to **Roles** and click **Create role**.

b. Select the **Another AWS account** role type.

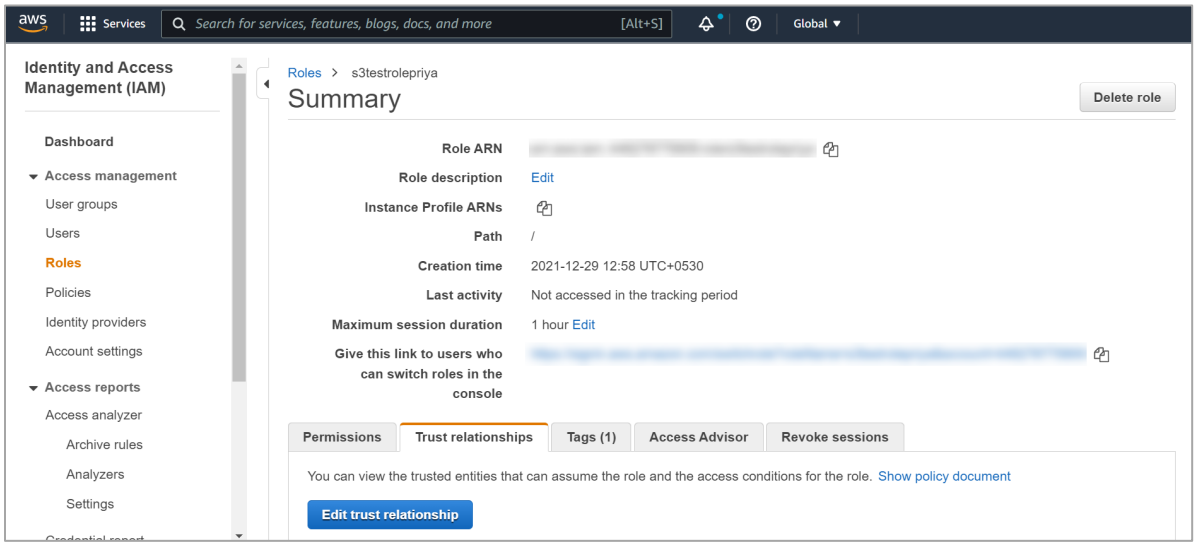
c. Provide your Qualys Account ID in the **Account ID** field.

d. Select **Permissions** and then attach the policy created above to this role.

e. (Optional) Choose **Tags**.

f. In the **Review** section, add role name, role description, and then click **Create role**.

4. Go to the created role and in the **Trust relationships** tab, click **Edit trust relationship** and add the Qualys AWS role ("arn:aws:iam::805950163170:role/QUALYS_ROLE_ASSUMING_CUSTOMER_ROLE") to the trust relationship.



Here is the sample trust relationship role:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS":
"arn:aws:iam::805950163170:role/QUALYS_ROLE_ASSUMING_CUSTOMER_ROLE
"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Note: In this example, 805950163170 is a Qualys account.

Note down the ARN of the role created by you (not the Qualys role ARN) for further use in the integration process.

5. Generate a JWT token by running the Generate JWT Token API.

6. Run the Register/Onboard Integration API to onboard/register the integration.
For more information, see:
   - For VM/VMDR: Register/Onboard an Integration
   - For PC: Register/Onboard an Integration

The response includes an integration ID and an external ID. The external ID needs to be added to the customer role created for adding Qualys AWS account to the trust relationship.

- **Integration ID**: Unique ID assigned to every integration with AWS S3 bucket
- **External ID**: <Qualys POD>-<Qualys Customer ID>-<random alphanumeric number>

Where,

- Qualys POD (preset by Qualys) refers to the Qualys Platform associated with your Qualys subscription. View Qualys Platform Identifier to know more about Qualys platforms.
- Qualys Customer ID (preset by Qualys) is your unique Qualys Customer ID.

7. Use the External ID generated from Step 4 in the Trust Relationship of your role.

   Note: The external ID needs to be added to the customer role which is created for adding Qualys AWS role to the trust relationship.

   a. Go to AWS IAM Console **> Roles**.

   b. Select the role and go to the **Trust relationships** tab.

   c. Click **Edit Trust Relationship**, add the following JSON in the **Condition JSON**, and then click **Update Trust Policy**.

```
"StringEquals": {
    "sts:ExternalId": "US_POD_1-71-36da0dcf-43d7-4014-82a7-47ce22a0db57"
}
```

   Where, `sts:ExternalId` is the externalId received in the response of the Onboarding POST API.

   The updated trust relationship looks like the following:

   Customer trust relationship role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS":
    "arn:aws:iam::805950163170:role/QUALYS_ROLE_ASSUMING_CUSTOMER_ROLE
    "
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "US_POD_1-71-36da0dcf-43d7-4014-
82a7-47ce22a0db57"
                }
            }
        }
    ]
}
```

8. Run the Validate Integration API to enable the AWS S3 bucket integration with Qualys. For more information, see:
    - For VM/VMDR: Validate an Integration
    - For PC: Validate an Integration

Integration for VM/VMDR

By integrating VM/VMDR with AWS S3 Bucket, you get the vulnerability findings for your asset inventory directly on your AWS S3 Bucket in near real time, without having to run any API calls or generate any reports.

The integration allows you to get a near real-time and up-to-date visibility of your security posture in your storage console and take rapid remedial actions.

Prerequisites

- Ensure that you accept all the Qualys Terms and Conditions. Reach out to the Qualys Support team for the integration process.
- **Qualys Applications**: You must have enabled Vulnerability Management (VM/VMDR) and Cloud Agent (CA) for your subscription. Ensure that you have executed scans and the scan reports (including vulnerability information) are available in your user account.
- **Qualys Sensors**: You must have Virtual Scanner Appliances or Cloud Agents, as required.
- **Permissions**: The API Access permission must be enabled for your account.
- **Role**: You must have the Manager or Unit Manager role

APIs for Creating and Managing the Integration

The following are the APIs for creating and managing the integration:

API	URL	Operator	Description
Generate a JWT Token	/auth	POST	Generates a new JWT token.
Register/Onboard Integration	/partner-integration/aws/s3/vm	POST	Registers an integration.
Validate Integration	/partner-integration/aws/s3/{id}/vm/validate	PATCH	Enables the integration.
Update Integration	/partner-integration/aws/s3/{id}/vm	PUT	Updates integration details such as bucket name, bucket region, minSeverity, baseCategory, name, resultSectionNeeded, sendVulnInfo, compressData, and roleArn of the AWS S3 bucket with Qualys.
Get Details of an Integration	/partner-integration/aws/s3/vm	GET	Gets details of a particular AWS S3 bucket integration.

	/partner-integration/aws/s3/{id}/vm		
De-Register/Delete Integration	/partner-integration/aws/s3/{id}/vm	DELETE	Removes a customer association by deleting the integration details or deregistering the customer.

URL to the Qualys API Server

Before you proceed with the APIs, you need to know the Qualys API gateway. The Qualys gateway URL you should use for API requests depends on the Qualys platform where your account is located.

Gateway base URLs for different Qualys pods can be found at:
https://www.qualys.com/platform-identification/

This document uses <qualys_gateway_url> in sample API requests. Replace this URL with the appropriate Qualys API gateway URL (for example, https://gateway.qg1.apps.qualys.com) for your account.

Generate a JWT Token

Generates a new JWT token for authentication.

URL	/auth
Operator	POST

API Request

```
curl -X POST
"<qualys_gateway_url>/auth"
-d "username=value1&password=passwordValue&token=true"
-H "ContentType: application/x-www-form-urlencoded"
```

Output

a JWT token

(Pass this token in the rest of the APIs for Authorization. It is valid for 4 hours once generated. Once it is expired, you have to regenerate it.)

Register/Onboard an Integration

Registers an integration.

URL	/partner-integration/aws/s3/vm
Operator	POST

Input Parameters

Parameter	Description
bucketName={value}	(Required) Provide the name of the AWS S3 bucket being used for integration.
bucketRegion={value}	(Required) Provide the region where the AWS S3 bucket is located.
roleArn={value}	(Required) Specify the ARN of the cross-account role which you created in your AWS account.
name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for the name is 50 characters.
minSeverity={value}	The minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the AWS S3 bucket. By default, it is configured to severity level 3 and above. For example, if you set the value to 1, all findings with severity level 1 to 5 are fetched and available on AWS S3 bucket.
baseCategory={IG|Potential|Confirmed}	Category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the AWS S3. The valid values are **IG**, **Confirmed**, and **Potential**. • By default, it is configured to **Confirmed**. In this case, only confirmed vulnerabilities are included. • If you configure the baseCategory as **Potential**, both Potential and Confirmed vulnerabilities are included. • If you configure the baseCategory as **IG**, all three categories: **IG**, **Potential** and **Confirmed** vulnerabilities are included.
resultSectionNeeded={true|false}	Set this to true to include the result section in the finding. If you want to exclude the result section, set this parameter to false. By default, the resultSectionNeeded parameter is configured to false.
sendVulnInfo={true|false}	Set this to true if you need the vulnerability information. If you want to exclude the vulnerability information, set this parameter to false. By default, the sendVulnInfo parameter is configured to false.

compressData={true|false}	Set this to true to compress the data in the response. It saves on disk and network IO. If you want to exclude the compression, set this parameter to false. By default, the compressData parameter is configured to true.
sendAlerts	(Boolean) Set to true to receive ProActive alert notifications.
errorEmails	When sendAlerts is set to true, provide the email list for ProActive Alert notifications. Add upto aList of maximum 5 email addresses as comma-separated values.

API Request

```
curl -H 'Authorization: Bearer <token>'
'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/s3/vm' --data '@integration.json'
```

Note: "integration.json" contains the request POST data.

Request POST Data (integration.json)

```
{
    "bucketName": "qualys-vm-findings",
    "bucketRegion": "us-east-1",
    "minSeverity": 4,
    "baseCategory": "Potential",
    "name": "Sample Name or Sample integration",
    "resultSectionNeeded": true,
    "sendVulnInfo": true,
    "compressData": true,
    "roleArn": "arn:aws:iam::xxxxxxxx:role/policy-role"
    "sendAlerts": true,
    "errorEmails":
        [
         "<email address 1>",
         "<email address 2>"
        ]
}
```

Output

```
{
    "integrationId": 5,
    "externalId": "US_POD_1-1-xxxxxxxx-xxxx-xxxx-xxxxxx-xxxxxxxxxxxx"
}
```

Validate an Integration

Enables the integration.

URL	/partner-integration/aws/s3/{id}/vm/validate
Operator	PATCH

Input Parameters

Platform	IP Address
id={value}	(Required) Provide the unique integration ID associated with AWS S3 bucket.

API Request

```
curl -H 'Authorization: Bearer <token>' -X PATCH
'<qualys_gateway_url>/partner-integration/aws/s3/{id}/vm/validate'
```

where, id is the unique identifier for each customer.

Output

```
{
    "messsage": "AWS S3 VM integration successfully validated."
}
```

Update an Integration

Updates the integration details such as bucket name, bucket region, minSeverity, baseCategory, name, resultSectionNeeded, sendVulnInfo, compressData, and roleArn of the AWS S3 bucket with Qualys.

Note: You can also regenerate the externalID using this API, if needed. If you regenerate the externalID using this API, you need to edit the trust relationship again. For more information, see Appendix: Editing Trust Relationship after Regenerating External ID.

URL	/partner-integration/aws/s3/{id}/vm Where, id is IntegrationID provided by Qualys.
Operator	PUT

Input Parameters

Parameter	Description
bucketName={value}	Provide the name of the AWS S3 bucket being used for integration.
bucketRegion={value}	Provide the region where the AWS S3 bucket is located.

roleArn={value}	(Required) Specify the ARN of the cross-account role which you created in your AWS account.
name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for the name is 50 characters.
minSeverity={value}	The minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the AWS S3 bucket. By default, it is configured to severity level 3 and above. For example, if you set the value to 1, all findings with severity level 1 to 5 are fetched and available on AWS S3 bucket.
baseCategory={IG|Potential|Confirmed}	Category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the AWS S3. Thevalid values are **IG**, **Confirmed**, and **Potential**. • By default, it is configured to **Confirmed**. In this case, only confirmed vulnerabilities are included. • If you configure the baseCategory as **Potential**, both Potential and Confirmed vulnerabilities are included. • If you configure the baseCategory as **IG**, all three categories: **IG**, **Potential** and **Confirmed** vulnerabilities are included.
resultSectionNeeded={true|false}	Set this to true to include the result section in the finding. If you want to exclude the result section, set this parameter to false. By default, the resultSectionNeeded parameter is configured to false.
sendVulnInfo={true|false}	Set this to true if you need the vulnerability information. If you want to exclude the vulnerability information, set this parameter to false. By default, the sendVulnInfo parameter is configured to false.
compressData={true|false}	Set this to true to compress the data in the response. It saves on disk and network IO. If you want to exclude the compression, set this parameter to false. By default, the compressData parameter is configured to true.
regenerateExternalId	Set this to true if you want to regenerate the external ID. The default value is set to false.
sendAlerts	(Boolean) Set to true to receive ProActive alert notifications.

errorEmails	When sendAlerts is set to true, provide the email list for ProActive Alert notifications. Add upto aList of maximum 5 email addresses as comma-separated values.

Sample 1: Update AWS S3 Integration Details Using Integration ID

This example is for updating the configuration details of the AWS S3 bucket integration by providing the integration ID in the request.

API Request

```
curl -X PUT
--header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/s3/{id}/vm'
--data '@integration.json'
-H "Authorization: Bearer <token>"
```

Note: “integration.json” contains the request PUT data.

Request PUT Data (integration.json)

```
{
    "bucketName": "qualys-vm-findings",
    "bucketRegion": "us-east-1",
    "minSeverity": 2,
    "baseCategory": "Confirmed",
    "name": "Customer Name or integration name",
    "resultSectionNeeded": true,
    "sendVulnInfo": true,
    "compressData": true,
    "roleArn": "arn:aws:iam::xxxxxxxxx:role/policy-role",
    "regenerateExternalId": false
    "sendAlerts": true,
    "errorEmails":
        [
         "<email address 1>",
         "<email address 2>"
        ]
}
```

Output

```
{
    "messsage": "AWS S3 VM integration successfully updated."
}
```

Sample 2: Update AWS S3 Integration with 'Regenerate External ID'

This sample is for updating the configuration details of the AWS S3 bucket integration by setting regenerateExternalId to true.

API Request

```
curl -X PUT
--header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/s3/{id}/vm'
--data '@integration.json'
-H "Authorization: Bearer <token>"
```

Note: “integration.json” contains the request PUT data.

Request PUT Data (integration.json)

```
{
    "bucketName": "qualys-vm-findings",
    "bucketRegion": "us-east-1",
    "minSeverity": 2,
    "baseCategory": "Confirmed",
    "name": "Customer Name or integration name",
    "resultSectionNeeded": true,
    "sendVulnInfo": true,
    "compressData": true,
    "roleArn": "arn:aws:iam::xxxxxxxx:role/policy-role",
    "regenerateExternalId": true
}
```

Output

```
{
    "message": "AWS S3 VM Integration successfully updated.",
    "externalId": "US_POD_1-1- xxxxxxxx-xxxx-xxxx-xxxxxx-xxxxxxxxxxxxx"
}
```

Get Details of an Integration

When you want to get details of a particular AWS S3 bucket integration, you can fetch the configuration and integration details using the unique integration identifier (id) of the AWS S3 integration. You can fetch the configuration and integration details with or without the unique integration identifier (id) of the AWS S3 bucket integration.

URL	/partner-integration/aws/s3/vm /partner-integration/aws/s3/{id}/vm
Operator	GET

API Request

```
curl -X GET
'<qualys_gateway_url>/partner-integration/aws/s3/{id}/vm'
-H "Authorization: Bearer <token>"
```

If you are not aware of the integration ID, use the following request to fetch details without the integration ID:

```
curl -X GET
'<qualys_gateway_url>/partner-integration/aws/s3/vm'
-H "Authorization: Bearer <token>"
```

Output

```
{
    "integrationId": 1,
    "customerId": 71,
    "customerUUID": "b35e0d4c-7636-e6f4-8244-551bbbec6140",
    "bucketName": "qualys-vm-findings",
```

```
    "bucketRegion": "us-east-1",
    "minSeverity": 4,
    "baseCategory": "Potential",
    "name": "Sample Name or Sample integration",
    "resultSectionNeeded": true,
    "sendVulnInfo": true,
    "compressData": true,
    "externalId": "US_POD_1-1-36da0dcf-43d7-4014-82a7-47ce22a0db57",
    "roleArn": "arn:aws:iam::43890899:role/policy-role",
    "integrationValidated": false
    "sendAlerts": true,
    "errorEmails":
       [
         "<email address 1>",
         "<email address 2>"
       ]

}
```

De-Register/Delete an Integration

You can remove a customer association by deleting the integration details or deregistering the customer. You need to provide the integration Id to identify the integration to be deleted.

URL	/partner-integration/aws/s3/{id}/vm
Operator	DELETE

Input Parameters

Parameter	Description
id={value}	(Required) Provide the unique integration ID associated with the AWS S3 bucket.

API Request

```
curl -X DELETE
'<qualys_gateway_url>/partner-integration/aws/s3/{id}/vm
-H "Authorization: Bearer <token>"
```

Output

```
{
    "messsage": "AWS S3 VM integration successfully deleted."
}
```

Integration for Policy Compliance (PC)

By integrating PC with AWS S3 Bucket, you get posture data of your asset inventory directly on your AWS S3 Bucket in near real time, without having to run any API calls or generate any compliance reports. CIPS (Cloud Integration Partner Service) proactively retrieves the posture data from Qualys Policy Compliance and transfers it to AWS S3 Bucket.

Note: Currently, this integration is supported only for Policy Compliance (PC) and not for SCA subscriptions.

Prerequisites

- The CIPS service must be enabled for your subscription. Qualys Support enables it for your account. Reach out to the Qualys Support team for the integration process.
- **Qualys applications**: You must have enabled for your subscription: Policy Compliance (PC) and Cloud Agent (CA).
- **Qualys Sensors**: You must have Virtual Scanner Appliances or Cloud Agents, as required.
- **Permissions**: The API Access permission must be enabled for your account.
- **Role**: You must have the Manager or Unit Manager role.
- **Platform version:** You must be on Qualys Cloud Platform version QWEB-10.21.1.0 or later.

APIs for Creating and Managing the Integration

The following are the APIs for creating and managing the integration:

API	URL	Operator	Description
Register/Onboard an Integration	/partner-integration/aws/s3/pc	POST	Registers an integration.
Validate Integration	/partner-integration/aws/s3/{id}/pc/validate	PATCH	Enables the integration.
Update Integration	/partner-integration/aws/s3/{id}/pc	PUT	Updates integration details such as bucket name, bucket region, name, compressData, and roleArn of the AWS S3 bucket with Qualys.
Get Details of Integration	/partner-integration/aws/s3/pc /partner-integration/aws/s3/{id}/pc	GET	Gets details of a particular AWS S3 bucket integration.

De-Register/Delete Integration	/partner-integration/aws/s3/{id}/pc	DELETE	Removes a customer association by deleting the integration details or deregistering the customer.

URL to the Qualys API Server

Before you proceed with the APIs, you need to know the Qualys API Server. The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This document uses <qualys_base_url> in sample API requests. Replace this URL with the appropriate Qualys API Server and URL for your account.

Register/Onboard an Integration

Registers an integration.

URL	/partner-integration/aws/s3/pc
Operator	POST

Request Body Fields

Parameter	Description
bucketName={value}	(Required) Provide the name of the AWS S3 bucket being used for integration.
bucketRegion={value}	(Required) Provide the region where the AWS S3 bucket is located.
roleArn={value}	(Required) Specify the ARN of the cross-account role which you created in your AWS account.
name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for the name is 50 characters.

API Request

```
curl -H 'Authorization: Bearer <token>'
'Content-Type:application/json'
'<qualys_base_url>/partner-integration/aws/s3/pc' --data '@integration.json'
```

Note: "integration.json" contains the request POST data.

Request POST Data (integration.json)

```
{
    "name": "AWS S3 PC integarion for quays_aa15",
    "bucketName": "qualys-pc-data",
    "bucketRegion": "ap-south-1",
```

```
    "roleArn": "arn:aws:iam::xxxxxxxxxxxx:role/aa-15-pc-aws-s3-role"
}
```

Output

```
{
    "integrationId": 5,
    "externalId": "US_POD_1-1- xxxxxxxx-xxxx-xxxx-xxxxxx-xxxxxxxxxxxx"
}
```

Validate an Integration

Enables an integration.

URL	/partner-integration/aws/s3/{id}/pc/validate
Operator	PATCH

Input Parameters

Platform	IP Address
id={value}	(Required) Provide the unique integration ID associated with AWS S3 bucket.

API Request

```
curl -H 'Authorization: Bearer <token>' -X PATCH
'<qualys_base_url>/partner-integration/aws/s3/{id}/pc/validate'
```

where, id is the unique integration ID for each customer.

Output

```
{
    "messsage": "AWS S3 PC integration successfully validated."
}
```

Update an Integration

Updates the integration details such bucket name, bucket region, name, compressData, and roleArn of the AWS S3 bucket with Qualys.

Note: You can also regenerate the external ID using this API if needed. If you have regenerated the "externalID" using this API, you need to edit the trust relationship again. For more information, see Appendix: Editing Trust Relationship after Regenerating External ID.

URL	/partner-integration/aws/s3/{id}/pc where, id is the IntegrationID provided by Qualys.
Operator	PUT

Input Parameters

Parameter	Description
bucketName={value}	Provide the name of the AWS S3 bucket being used for integration.
bucketRegion={value}	Provide the region where the AWS S3 bucket is located.
roleArn={value}	(Required) Specify the ARN of the cross-account role which you created in your AWS account.
name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for the name is 50 characters.
compressData={true|false}	Set this to true to compress the data in the response. It saves on disk and network IO. If you want to exclude the compression, set this parameter to false. By default, the compressData parameter is configured to true.
regenerateExternalId	Set this to true if you want to regenerate the external ID. The default value is set to false.

Sample 1: Update AWS S3 Integration Details Using Integration ID

This example is for updating the configuration details of the AWS S3 bucket integration by providing the integration ID in the request.

API Request

```
curl -X PUT
--header 'Content-Type:application/json'
'<qualys_base_url>/partner-integration/aws/s3/{id}/pc'
--data '@integration.json'
-H "Authorization: Bearer <token>"
```

Note: “integration.json” contains the request PUT data.

Request PUT Data (integration.json)

```
{
    "name": "Customer Name or integration name",
    "compressData": true,
    "bucketName": "qualys-pc-data",
    "bucketRegion": "us-east-1",
    "roleArn": "arn:aws:iam::xxxxxxxx:role/policy-role",
    "regenerateExternalId": false
}
```

Output

```
{
    "messsage": "AWS S3 PC integration successfully updated."
}
```

Sample 2: Update AWS S3 Integration with 'Regenerate External ID'

This sample is for updating the configuration details of the AWS S3 bucket integration by setting regenerateExternalId to true.

API Request

```
curl -X PUT
--header 'Content-Type:application/json'
'<qualys_base_url>/partner-integration/aws/s3/{id}/pc'
--data '@integration.json'
-H "Authorization: Bearer <token>"
```

Note: “integration.json” contains the request PUT data.

Request PUT Data (integration.json)

```
{
    "name": "Customer Name or integration name",
    "compressData": true,
    "bucketName": "qualys-pc-data",
    "bucketRegion": "us-east-1",
    "roleArn": "arn:aws:iam::43890899:role/policy-role",
    "regenerateExternalId": true
}
```

Output

```
{
    "message": "AWS S3 PC Integration successfully updated.",
    "externalId": "US_POD_1-1- xxxxxxxx-xxxx-xxxx-xxxxxx-xxxxxxxxxxxxx"
}
```

Get Details of an Integration

When you want to get details of a particular AWS S3 bucket integration, you can fetch the configuration and integration details using the unique integration identifier (id) of the AWS S3 integration. You can fetch the configuration and integration details with or without the unique integration identifier (id) of the AWS S3 bucket integration.

URL	/partner-integration/aws/s3/pc /partner-integration/aws/s3/{id}/pc
Operator	GET

API Request

```
curl -X GET
'<qualys_base_url>/partner-integration/aws/s3/{id}/pc'
-H "Authorization: Bearer <token>"
```

If you are not aware of the integration ID, use the following request to fetch details without the integration ID.

```
curl -X GET
'<qualys_base_url>/partner-integration/aws/s3/pc'
```

```
-H "Authorization: Bearer <token>"
```

Output

```
{
    "name": "Customer Name or integration name",
    "compressData": true,
    "bucketName": "qualys-pc-data",
    "bucketRegion": "us-east-1",
    "roleArn": "arn:aws:iam::xxxxxxxx:role/policy-role",
    "integrationValidated": true
}
```

De-Register/Delete an Integration

Removes a customer association by deleting the integration details or deregistering the customer. You need to provide the integration Id to identify the integration to be deleted.

URL	/partner-integration/aws/s3/{id}/pc
Operator	DELETE

Input Parameters

Parameter	Description
id={value}	(Required) Provide the unique integration ID associated with the AWS S3 bucket.

API Request

```
curl -X DELETE
'<qualys_base_url>/partner-integration/aws/s3/{id}/pc
-H "Authorization: Bearer <token>"
```

Output

```
{
    "messsage": "AWS S3 PC integration successfully deleted."
}
```

Add Policies to CIPS

After enabling the CIPS service for your subscription and integrating your storage platform with Qualys, you need to add the required policies to CIPS using the dedicated APIs. Once you add the policies, CIPS proactively retrieves the posture data from PC and pushes it to your storage in near real time in JSON format.

Note: The posture data is transferred only for the policies that are added to CIPS.

You can filter the posture data being transferred to your storage as required by defining a filter configuration in CIPS. For example, you can define a filter to get the data for only "Failed" postures, reducing the filtering efforts during post-processing.

Qualys provides you with dedicated APIs for adding policies to CIPS, deleting policies, getting a list of policies added to CIPS, managing filter configuration, etc.

What are the Steps?

You need to perform the following steps before CIPS starts sending posture data to your cloud storage platform.

1. Add the required policies to CIPS using the 'Add Policy' API. For more information, see Add a Policy.

   Note: You can add up to 100 policies to CIPS.

2. Create a filter to limit the posture data transferred to your cloud storage platform, using the 'Create Filter Configuration' API. For more information, see Create Filter Configuration.

   You can filter posture data based on the posture status (Failed, Passed, or Error) and whether to exclude evidence data or not. If no filter is created, the entire posture data for the added policies is transferred.

3. Run a PC scan.

   As the scan runs and generates posture data, CIPS proactively retrieves the posture data and pushes it to your cloud storage.

Note: CIPS synchronizes with the filter configuration every two hours. Therefore, any modifications to the filter configuration reflect in CIPS after 0 to 2 hours, depending on when you have modified the filter before the next synchronization run.

APIs for Adding Policies to CIPS and Filtering the Posture Data

Use the following APIs to add and manage policies on CIPS, and define a filter configuration to limit the posture data transferred to your cloud storage platform:

API	URL	Operator	Description
Generate a JWT Token	/auth	POST	Generates a new JWT token for authentication.
Add a Policy	/pcas/cips/config/policy	POST	Adds a policy to CIPS.

Delete a Policy	/pcas/cips/config/policy	DELETE	Deletes a policy from CIPS.
Create Filter Configuration	/pcas/cips/config	POST	Lets you define a filter to limit the data sent to your storage platform.
Update the Filter Configuration	/pcas/cips/config	PUT	Lets you modify the filter configuration.
Get Filter Details	/pcas/cips/config	GET	Fetches the filter data, such as filter configuration and a list of policies on which the filter is applied.

Generate a JWT Token

Generates a new JWT token for authentication.

URL	/auth
Operator	POST

Parameters

Parameter	Mandatory/Optional	Data Type	Description
username	Mandatory	string	Specify the username.
password	Mandatory	string	Specify the password.

Request

```
curl -X POST
"<qualys_base_url>/auth
-d "username=value1&password=passwordValue&token=true"
-H "ContentType: application/x-www-form-urlencoded"
```

Response

A JWT Token

Add a Policy

Adds a policy to CIPS.

URL	/pcas/cips/config/policy
Operator	POST

Request

```
curl -X POST
"<qualys_base_url>/pcas/cips/config/policy"
-H "accept: */*"
-H "Authorization: Bearer <token>"
-H "Content-Type:application/json"
-d "[{"policy": [4771746,3606517,4342692,1109776]
}]"
```

Response

Response code 202

Policy added successfully.

Delete a Policy

Deletes a policy from CIPS.

URL	/pcas/cips/config/policy
Operator	DELETE

Request

```
curl -X DELETE
"<qualys_base_url>/pcas/cips/config"
-H "accept: */*"
-H "Authorization: Bearer <token>"
-H "Content-Type:application/json"
-d "[{"policy": [4771746,3606517,4342692,1109776]
```

Response

Response code 202

Policy deleted successfully.

Create Filter Configuration

Lets you define a filter to limit the data sent to your cloud storage platform.

URL	/pcas/cips/config
Operator	POST

Request

```
curl -X POST
"<qualys_base_url>/pcas/cips/config"
-H "accept: */*"
-H "Authorization: Bearer <token>"
-H "Content-Type:application/json"
-d
"[{"includeEvidenceData": false,"includeFailPosture": true,"includePassPosture"
: true,"includeErrorPosture": true}]"
```

Response

```
{
    "subscriptionId": 3068,
    "includeEvidenceData": false,
    "includeFailPosture": true,
    "includePassPosture": true,
    "includeErrorPosture": true,
    "lastUpdated": "2022-11-14T06:34:26.148+00:00",
}
```

Update the Filter Configuration

Lets you modify the filter configuration.

URL	/pcas/cips/config
Operator	PUT

Request

```
curl -X PUT
"<qualys_base_url>/pcas/cips/config"
-H "accept: */*"
-H "Authorization: Bearer <token>"
-H "Content-Type:application/json"
-d
"[{"includeEvidenceData": false,"includeFailPosture": false,"includePassPosture
": true,"includeErrorPosture": true}}]"
```

Response

```
{
    "subscriptionId": 3068,
    "includeEvidenceData": false,
    "includeFailPosture": false,
    "includePassPosture": true,
    "includeErrorPosture": true,
    "lastUpdated": "2022-11-14T06:34:26.148+00:00",
}
```

Get Filter Details

Fetches the filter data such as filter configuration and a list of policies on which the filter is applied.

URL	/pcas/cips/config
Operator	GET

Request

```
curl -X GET
"<qualys_base_url>/pcas/cips/config"
```

```
-H "accept: */*"
-H "Authorization: Bearer <token>"
-H "Content-Type:application/json"
```

Response


```
{
    "id": 1001,
    "subscriptionId": 3068,
    "includeEvidenceData": false,
    "includeFailPosture": true,
    "includePassPosture": true,
    "includeErrorPosture": true,
    "lastUpdated": "2022-11-14T06:34:26.148+00:00",
    "policy": [
        1109776,
        3606517,
        4342692,
        4771746,
        3523484
    ]
```

Sample: Posture Data Transferred using CIPS

The following sample shows the posture data transferred by CIPS to your storage platform:


```
{
    "hostId": 10404430,
    "dns": "doctom1.rdlab.in03.qualys.com",
    "ip": "10.115.120.97",
    "trackingMethod": "4",
    "os": "CentOS Linux 7.5.1804",
    "osCpe": null,
    "complianceLastScanData": "2023-01-16T10:47:05Z",
    "customerUuid": "0a387e70-8b26-78ff-8145-017b816fa17f",
    "customerId": 250021,
    "assetId": 31680291,
    "policy": [
        {
            "id": 3567540,
            "posture": [
                {
                    "id": 25214933,
                    "controlId": 1071,
                    "controlStatement": "Status of the 'Minimum Password Length'
setting",
                    "controlReference": "",
                    "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the following lines:
\n\nPASS_MIN_LEN <required value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD
requirement is \"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then the most
restrictive must be satisfied.",
                    "technologyId": 80,
                    "instance": "os",
                    "posture": "Passed",
                    "postureModifiedDate": "2023-01-13T07:08:18Z",
                    "evaluationDate": "2023-01-16T10:49:43Z",
                    "lastPosture": "Passed",
                    "firstEvaluatedDate": "2023-01-13T07:08:18Z",
                    "failDateFirstFound": null,
                    "failDateLastFound": null,
                    "passedDateFirstFound": "2023-01-13T07:08:18Z",
                    "passedDateLastFound": "2023-01-16T10:49:43Z",
```

```
                    "evidence": "{\"description\":\"The following Integer value
\\u003cB\\u003eX\\u003c/B\\u003e indicates the current value of the
\\u003cB\\u003ePASS_MIN_LEN\\u003c/B\\u003e setting as defined within the
\\u003cB\\u003e/etc/login.defs\\u003c/B\\u003e file.\",\"expectedValues\":[\"greater
than or equal
to\\n0\"],\"actualValues\":[\"5\"],\"extendedEvidence\":\"\\n\\n\\u003d\\u003d\\u003d\
\u003d\\u003d\\u003dExtended Evidence\\u003d\\u003d\\u003d\\u003d\\u003d\\u003d:\\nRow
1:File name,Setting,Value\\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\\n\",\"causeOfFailure\":{\"missing\":{\"logic\":\"DP\
",\"value\":[]},\"unexpected\":{\"value\":[\"5\"]}},\"scanParameter\":\"\"}"
                },
                {
                    "id": 25214934,
                    "controlId": 1072,
                    "controlStatement": "Status of the 'Minimum Password Age'
setting",
                    "controlReference": "at CL 1072 second(https://www.google.com),at
CL 1072(https://www.qualys1.com)",
                    "remediation": "To set the value for this setting edit the
'/etc/login.defs' file:\nAdd or edit the value of 'PASS_MIN_DAYS' setting according to
the needs of business.\n\nExample: \nPASS_MIN_DAYS 7 \n\nModify user parameters for
all users with a password set to match, with the following command:\n# chage --mindays
7 <user>",
                    "technologyId": 80,
                    "instance": "os",
                    "posture": "Passed",
                    "postureModifiedDate": "2023-01-13T07:08:18Z",
                    "evaluationDate": "2023-01-16T10:49:43Z",
                    "lastPosture": "Passed",
                    "firstEvaluatedDate": "2023-01-13T07:08:18Z",
                    "failDateFirstFound": null,
                    "failDateLastFound": null,
                    "passedDateFirstFound": "2023-01-13T07:08:18Z",
                    "passedDateLastFound": "2023-01-16T10:49:43Z",
                    "evidence": "{\"description\":\"The following Integer value
\\u003cb\\u003eX\\u003c/b\\u003e indicates the current
\\u003cb\\u003ePASS_MIN_DAYS\\u003c/b\\u003e setting within the
\\u003cb\\u003e/etc/login.defs\\u003c/b\\u003e file.\",\"expectedValues\":[\"greater
than or equal
to\\n0\"],\"actualValues\":[\"0\"],\"extendedEvidence\":\"\\n\\n\\u003d\\u003d\\u003d\
\u003d\\u003d\\u003dExtended Evidence\\u003d\\u003d\\u003d\\u003d\\u003d\\u003d:\\nRow
1:File name,Setting,Value\\nRow
```

```
2:/etc/login.defs,PASS_MIN_DAYS,0\\n\",\"causeOfFailure\":{\"missing\":{\"logic\":\"DP
\",\"value\":[]},\"unexpected\":{\"value\":[\"0\"]}},\"scanParameter\":\"\"}"
                },
                {
                    "id": 25214935,
                    "controlId": 1073,
                    "controlStatement": "Status of the 'Maximum Password Age' setting
(expiration) / Accounts having the 'password never expires' flag set",
                    "controlReference": "at CL 1 1073(https://www.google.com)",
                    "remediation": "To specify password maximum age for new accounts,
edit the file \"/etc/login.defs\" and add or correct the following line, replacing
[DAYS] appropriately: \n\nPASS_MAX_DAYS [DAYS]\n\nThe DoD requirement is 60.",
                    "technologyId": 80,
                    "instance": "os",
                    "posture": "Passed",
                    "postureModifiedDate": "2023-01-13T07:08:18Z",
                    "evaluationDate": "2023-01-16T10:49:43Z",
                    "lastPosture": "Passed",
                    "firstEvaluatedDate": "2023-01-13T07:08:18Z",
                    "failDateFirstFound": null,
                    "failDateLastFound": null,
                    "passedDateFirstFound": "2023-01-13T07:08:18Z",
                    "passedDateLastFound": "2023-01-16T10:49:43Z",
                    "evidence": "{\"description\":\"The following Integer value
\\u003cb\\u003eX\\u003c/b\\u003e indicates the current status of the
\\u003cb\\u003ePASS_MAX_DAYS\\u003c/b\\u003e setting as defined within the
\\u003cb\\u003e/etc/login.defs\\u003c/b\\u003e
file.456\",\"expectedValues\":[\"greater than or equal
to\\n0\"],\"actualValues\":[\"99999\"],\"extendedEvidence\":\"\\n\\n\\u003d\\u003d\\u0
03d\\u003d\\u003d\\u003dExtended
Evidence\\u003d\\u003d\\u003d\\u003d\\u003d\\u003d:\\nRow 1:File
name,Setting,Value\\nRow
2:/etc/login.defs,PASS_MAX_DAYS,99999\\n\",\"causeOfFailure\":{\"missing\":{\"logic\":
\"DP\",\"value\":[]},\"unexpected\":{\"value\":[\"99999\"]}},\"scanParameter\":\"\"}"
                },
                {
                    "id": 25214936,
                    "controlId": 1091,
                    "controlStatement": "Status of the number of days before a [Prompt
user] password expiration warning prompt is displayed at login",
                    "controlReference": "at CL 1(https://www.qualys.com)",
```

```
                    "remediation": "# Edit file '/etc/login.defs' to configure
'PASS_WARN_AGE' setting according to the business needs and organization's security
policies.\nPASS_WARN_AGE <number>\n\n# Example\nPASS_WARN_AGE 7",
                    "technologyId": 80,
                    "instance": "os",
                    "posture": "Passed",
                    "postureModifiedDate": "2023-01-13T07:08:18Z",
                    "evaluationDate": "2023-01-16T10:49:43Z",
                    "lastPosture": "Passed",
                    "firstEvaluatedDate": "2023-01-13T07:08:18Z",
                    "failDateFirstFound": null,
                    "failDateLastFound": null,
                    "passedDateFirstFound": "2023-01-13T07:08:18Z",
                    "passedDateLastFound": "2023-01-16T10:49:43Z",
                    "evidence": "{\"description\":\"The following Integer value
\\u003cb\\u003eX\\u003c/b\\u003e indicates the current
\\u003cb\\u003ePASS_WARN_AGE\\u003c/b\\u003e setting within the
\\u003cb\\u003e/etc/login.defs\\u003c/b\\u003e file on the
host.456\",\"expectedValues\":[\"greater than or equal
to\\n0\"],\"actualValues\":[\"7\"],\"extendedEvidence\":\"\\n\\n\\u003d\\u003d\\u003d\
\u003d\\u003d\\u003dExtended Evidence\\u003d\\u003d\\u003d\\u003d\\u003d\\u003d:\\nRow
1:File name,Setting,Value\\nRow
2:/etc/login.defs,PASS_WARN_AGE,7\\n\",\"causeOfFailure\":{\"missing\":{\"logic\":\"DP
\",\"value\":[]},\"unexpected\":{\"value\":[\"7\"]}},\"scanParameter\":\"\"}"
                },
                {
                    "id": 25214937,
                    "controlId": 1117,
                    "controlStatement": "Status of the 'inetd' or 'xinetd' service",
                    "controlReference": "at CL 1117 first(https://www.qualys.com),at
CL 1117 second(https://www.google.com)",
                    "remediation": "The \"xinetd\" service can be disabled with the
following commands: \n\n# chkconfig xinetd off\n# service xinetd stop",
                    "technologyId": 80,
                    "instance": "os",
                    "posture": "Passed",
                    "postureModifiedDate": "2023-01-13T07:08:18Z",
                    "evaluationDate": "2023-01-16T10:49:43Z",
                    "lastPosture": "Passed",
                    "firstEvaluatedDate": "2023-01-13T07:08:18Z",
                    "failDateFirstFound": null,
                    "failDateLastFound": null,
                    "passedDateFirstFound": "2023-01-13T07:08:18Z",
```

```
                    "passedDateLastFound": "2023-01-16T10:49:43Z",
                    "evidence": "{\"description\":\"The following List String value(s)
\\u003cb\\u003eX\\u003c/b\\u003e indicate the current status of the
\\u003cb\\u003exinetd\\u003c/b\\u003e service.456\",\"expectedValues\":[\"matches
regular expression
list\\n.*\"],\"actualValues\":[\"161803399999999\"],\"extendedEvidence\":\"\\n\\n\\u00
3d\\u003d\\u003d\\u003d\\u003d\\u003dExtended
Evidence\\u003d\\u003d\\u003d\\u003d\\u003d:\\nRow 1:Service
Name,Status\\n\",\"causeOfFailure\":{\"missing\":{\"logic\":\"DP\",\"value\":[]},\"une
xpected\":{\"value\":[]}},\"scanParameter\":\"\"}"
                }
            ]
        }
    ]
}
```

Findings and Insights

Let's see the detailed steps for viewing VM and PC findings and insights on AWS S3 console.

View Findings on AWS S3 Console

You can view the Qualys findings on the AWS console. Before you view findings on AWS S3 console, ensure that you have met the pre-requisites, completed all the configurations with AWS S3 and Qualys, and have data available in your Qualys subscription.

VM findings:

In the 'qualys_vm_findings/' directory, Qualys creates date-wise sub-directories in the YYYY-MM-DD format. In these directories, you can see VM findings in the <UUID>.gz or <UUID>.json format depending on whether compression is enabled or not.

Folder structure in the S3 bucket:

- Folder 1: findings/<YYYY-MM-DD>/
- Folder 2 : vuln_info/vm
- File: test-file.gz (This file is used for connection validation by Qualys.)

PC Posture Data:

In the 'qualys_pc_posture_info/' directory, Qualys creates date-wise sub-directories in YYYY-MM-DD format. In these directories, you can see PC postures in format <UUID>.gz or <UUID>.json depending on whether compression is enabled or not. These postures are batched; hence they might contain posture info for multiple assets.

Folder structure in the S3 bucket:

- Folder 1: qualys_pc_posture_info/<YYYY-MM-DD>/
- File 2: test-file.gz/test-file.json

Troubleshooting Tips

The following scenarios help you debug the common issues:

Scenario	Workaround
Qualys Findings are not visible in Qualys subscription	To view Qualys findings in your subscription, ensure the following: • Qualys sensors are deployed on the endpoints • Vulnerability or PC scans are performed
Qualys Findings are not visible on AWS S3 console	To view Qualys findings on AWS S3 console, ensure the following: • Vulnerability assessment and findings are available in your Qualys subscription.

	• Policies are added to CIPS, PC scans are performed, and posture data is generated. • The integration configuration between Qualys and AWS S3 console is complete.

For any such issues related to AWS S3 bucket Integration with Qualys, reach out to Qualys Support.

Appendix: Editing Trust Relationship After Regenerating External ID

Perform the following steps to edit the trust relationship after regenerating the external ID:

1. Run the 'Update an Integration' API with the 'regenerateExternalId' field set to true. Note down the externalId received in the API Response.
2. Go to AWS IAM Console > **Roles**.
3. Open the role for which the externalId is changed.
4. Under **Trust Relationships**, click **Edit trust policy**, update the 'sts: ExternalId' field, and click **Update policy**.
5. Run the Validate Integration API to validate the integration.