



# **Qualys Integration with Azure Storage Blob**

API User Guide

November 30, 2021

Copyright 2020 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



# Table of Contents

<b>About this guide.....</b>	<b>4</b>
About Qualys .....	4
Qualys Support .....	4
<b>Introduction.....</b>	<b>5</b>
Qualys Integrated Security Platform .....	5
Pre-requisites .....	7
<b>Getting Started with Azure Storage Blob Integration.....</b>	<b>8</b>
Creating Storage Account .....	8
<b>Configuring Integration with Qualys.....</b>	<b>14</b>
URL to the Qualys API Server .....	14
Enable Azure Storage Blob Integration .....	14
Update Azure Storage Blob Integration .....	16
Get Details of the Azure Storage Blob Integration .....	18
Delete Azure Storage Blob Integration Details .....	19
<b>Findings and Insights .....</b>	<b>20</b>
View Findings on Azure Storage Blob Console .....	20
Troubleshooting Tips .....	22

## About this guide

Welcome to Qualys Cloud Platform and integration of Qualys Cloud Platform with Azure Storage Blob! We'll help you get acquainted with the Qualys solutions for integrating Azure Storage Blob with 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](http://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 support information at [www.qualys.com/support/](http://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. In this guide, we'll be talking about integrating Qualys findings with Microsoft Azure Storage Blob that you can further use in your enterprise.

## Qualys Integrated Security Platform

With Qualys Cloud Platform you get a single view of your security and compliance - in real time. If you're new to Qualys we recommend you to visit the [Qualys Cloud Platform](#) web page to know more about our cloud platform.

 ASSET MANAGEMENT	 IT SECURITY	 COMPLIANCE	 CLOUD / CONTAINER SECURITY	 WEB APP SECURITY
Global AssetView - It's Free! Unlimited Assets	Vulnerability Management, Detection & Response - <b>Most Popular</b>	Policy Compliance	Cloud Inventory	Web App Scanning
CyberSecurity Asset Management - <b>New</b>	Threat Protection	Security Configuration Assessment	Cloud Security Assessment	Web App Firewall
Certificate Inventory	Continuous Monitoring	PCI Compliance	Container Security	
	Patch Management	File Integrity Monitoring		
	Endpoint Detection & Response - <b>New</b>	Security Assessment Questionnaire		

## Qualys Support for Azure Storage Blob

Azure Storage Blob provides you the flexibility to create data lakes and acts like a data store for cloud analytics. Azure Storage Blob also provides immense storage and multiple mechanisms to build powerful cloud-native and mobile apps.

You can now access Qualys vulnerability assessment findings in Azure Storage Blob. The Azure Storage Blob provides a comprehensive view of the high-priority security alerts and compliance status across their accounts. By integrating the findings from Qualys Vulnerability Management (VM/VMDR) with Azure Storage Blob, you can get near real-time, up-to-date visibility of your security posture in Azure Storage Blob console. These findings, gained by the correlation of Qualys information with other data in Azure Storage Blob, allow customers to quickly detect risks and take rapid, automated remedial actions.

Currently, we support findings from only VM/VMDR app in Azure Storage Blob integration.

## 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 up 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



Azure 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

## Pre-requisites

These options must be enabled for your Qualys user account.

- Ensure that you accept all the Qualys Terms and Conditions and reach out to the Qualys Support team for the integration process.

**Note:** You can access integration API only after accepting Terms and Conditions provided by Qualys.

- Qualys Applications: Vulnerability Management (VM/VMDR), Cloud Agent (CA). Ensure that you have executed scans and the scan reports (including vulnerability information) are available in your user account.

- Qualys Sensors: Virtual Scanner Appliances or Cloud Agents, as required

- Ensure API Access permission is enabled for the user account

- Manager or Unit Manager role

- Ensure that you create a storage account and provide access to Qualys.

## It's easy to get started

You might already be familiar with Qualys Cloud Suite, its features and user interface. If you're new to Qualys, we recommend these overview tutorials - it just takes a few minutes!

**Video Tutorials** get you familiar with basics

[Vulnerability Management Detection and Response. \(3 mins\)](#)

## Quick Steps: Integrating Azure Storage Blob with Qualys

Here's the user flow for integrating Qualys with Azure Storage Blob.

1 - [Getting Started with Azure Storage Blob Integration](#).

2 - [Configuring Integration with Qualys](#) using APIs available to configure integration with Qualys Cloud Platform.

3 - Configuring Insights on Azure Storage Blob Console (Optional).

**Helpful resources** Always up to date with the information you need

### From the Community

[Qualys Training](#) | Free self paced classes, video series, online classes

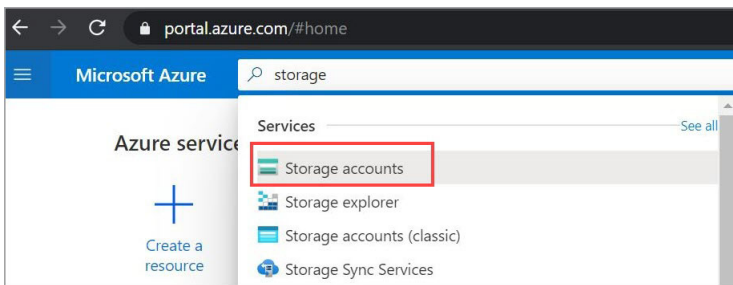
[Qualys Documentation](#) | Getting started guides, quick references, API docs

# Getting Started with Azure Storage Blob Integration

You need to create a separate account on Azure Storage Blob console and create a storage account and a container. Once you create a container, you can use the container details during integration. We'll walk you through the steps.

## Creating Storage Account

1. Login to Azure portal (<https://portal.azure.com/>) and search for Storage accounts in the search bar.





2. Click **Add** and then create a storage account with a unique name. Ensure that the type of storage account you choose is at least BlobStorage.

### Create storage account

#### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*

(New) test-resource-group

Create new

#### Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name \* ⓘ

qualyssecfindings ✓

Location \*

(Asia Pacific) West India

Performance ⓘ

☒ Standard ☐ Premium

Account kind ⓘ

BlobStorage

Replication ⓘ

Read-access geo-redundant storage (RA-GRS)

ⓘ Accounts with the selected kind, replication and performance type only support block and append blobs. Page blobs, file shares, tables, and queues will not be available

Review + create

< Previous

Next : Networking >

3. During storage account creation, use the following configuration:

- Secure transfer required: Enabled
- Allow Blob public access: Disabled
- Minimum TLS: 1.2

Click **Review+Create** to create the storage account.

The screenshot shows the 'Advanced' tab of the Azure Storage account creation wizard. The tabs at the top are Basics, Networking, Data protection, **Advanced**, Tags, and Review + create. The 'Security' section includes 'Secure transfer required' (radio buttons for Disabled and Enabled, with Enabled selected), 'Minimum TLS version' (a dropdown menu showing 'Version 1.2'), and 'Infrastructure encryption' (radio buttons for Disabled and Enabled, with Disabled selected). A blue information icon and text state: 'Sign up is currently required to enable infrastructure encryption on a per-subscription basis. [Sign up for infrastructure encryption](#)'. The 'Blob storage' section includes 'Allow Blob public access' (radio buttons for Disabled and Enabled, with Disabled selected), 'Blob access tier (default)' (radio buttons for Cool and Hot, with Cool selected), and 'NFS v3' (radio buttons for Disabled and Enabled, with Disabled selected). A blue information icon and text state: 'Sign up is currently required to utilize the NFS v3 feature on a per-subscription basis. [Sign up for NFS v3](#)'. The 'Data Lake Storage Gen2' section includes 'Hierarchical namespace' (radio buttons for Disabled and Enabled, with Disabled selected). At the bottom, there is a blue 'Review + create' button, a '< Previous' button, and a 'Next : Tags >' button.

4. Once you create a storage account, create a container with suitable name such as qualys-vm-findings. Note down the container name as this container name is required during integration with Qualys.


The screenshot shows the Azure portal interface. On the left, the breadcrumb is 'Home > qualyssecfindings'. Below it, the header says 'qualyssecfindings | Containers' with a storage account icon and name. There are links for '+ Container', 'Change access level', 'Restore containers', 'Refresh', and 'Delete'. A search bar says 'Search containers by prefix'. Below is a table with columns 'Name', 'Last modified', and 'Public access'. The table is empty, with a message: 'You don't have any containers yet. Click '+ Container' to get started.' On the right, a 'New container' dialog is open. It has a 'Name' field with 'qualys-vm-findings' and a green checkmark. Below is 'Public access level' with a dropdown showing 'Private (no anonymous access)'. A blue information icon and text state: 'The public access level is set to private because public access is disabled on this storage account.' There is an 'Advanced' section with a dropdown arrow. At the bottom are 'Create' and 'Discard' buttons.

5. Generate the connection string/shared access signature by specifying the relevant details. Following are minimum requirements:

- Allowed services: Blob
- Allowed resource type - Object
- Allowed permissions: Read, Write and List
- Select start and expiry date time as per your requirement
- Allowed protocol: Only HTTPS

Click **Generate the SAS and Connection String**

[Home](#) > [qualyssecfindings](#)

 **qualyssecfindings | Shared access signature** ×

Storage account

» A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time.

An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.

[Learn more](#)

Allowed services ⓘ  
☒ Blob

Allowed resource types ⓘ  
☐ Service ☐ Container ☒ Object

Allowed permissions ⓘ  
☒ Read ☒ Write ☐ Delete ☒ List ☐ Add ☐ Create ☐ Update ☐ Process

Blob versioning permissions ⓘ  
☐ Enables deletion of versions

Start and expiry date/time ⓘ  
Start    
End    
 ▼

Allowed IP addresses ⓘ

Allowed protocols ⓘ  
☒ HTTPS only ☐ HTTPS and HTTP

Preferred routing tier ⓘ  
☒ Basic (default) ☐ Microsoft network routing ☐ Internet routing  
**i** Some routing options are disabled because the endpoints are not published.


Signing key ⓘ  
 ▼

**Generate SAS and connection string**

**Note:** If the connection string expires, generate a new SAS and connection string and update the same with Qualys. With expired SAS token, Qualys won't be able to post the findings.

You could also locate the connection string in Access Keys section.

[Home](#) > [qualyssecfindings](#)


 **qualyssecfindings | Access keys** ×

Storage account


» Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines.  
[Learn more about regenerating storage access keys](#)

Storage account name

qualyssecfindings 

Show keys


**key1** 

Key

.....

Connection string

.....

**key2** 

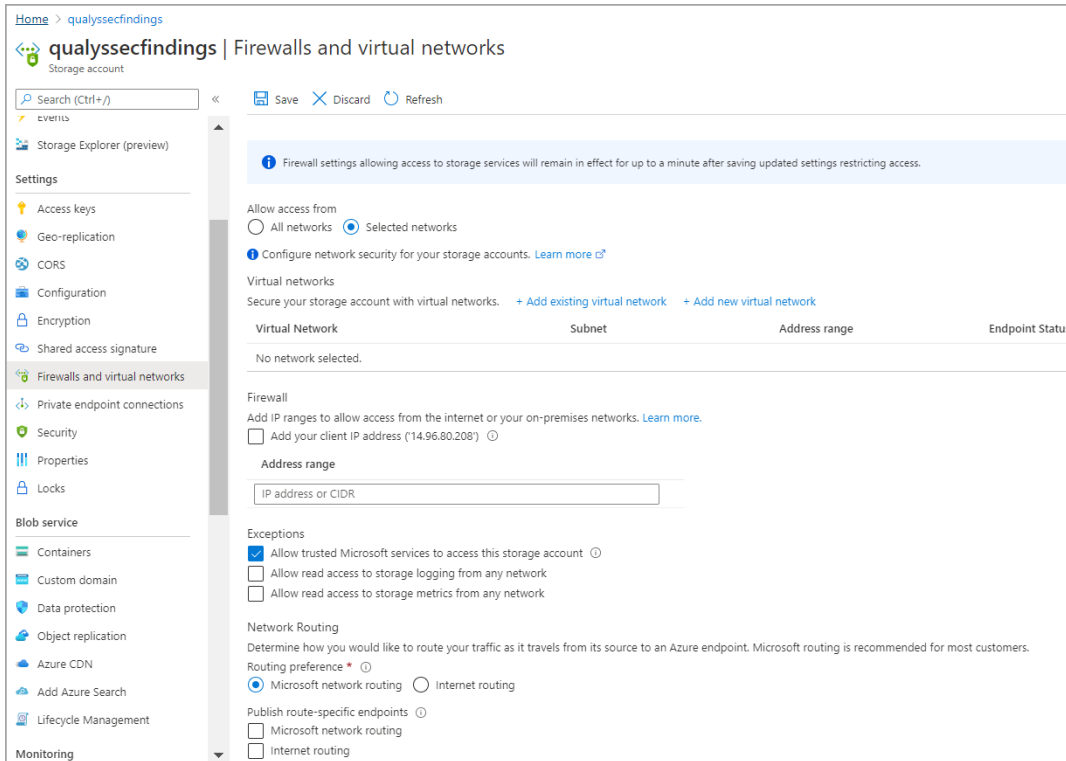
Key

.....

Connection string

.....

You can also modify Firewall and Virtual networks for enhanced security to allow ONLY Qualys source IP to access the storage account.



The Qualys source IP address that you could allow access to Storage account are listed below.

Platform	IP Address
US POD 1	64.39.96.20
US POD 2	64.39.96.25
US POD 3	64.39.96.27
EU POD 1	64.39.100.20
EU POD 2	154.59.121.40
CA POD	64.39.97.25
India POD	103.216.98.25

## Configuring Integration with Qualys

We provide APIs (JSON) to fasten and simplify the integration process with Azure Storage Blob. The integration process is a single step with Qualys using APIs: adding the Azure Storage Blob integration. Once you add it, you can use it to fetch details, update the existing configuration of Azure Storage Blob, or delete the Azure Storage Blob integration as well.

[Enable Azure Storage Blob Integration](#)

[Update Azure Storage Blob Integration](#)

[Get Details of the Azure Storage Blob Integration](#)

[Delete Azure Storage Blob Integration Details](#)

### 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 documentation uses the API URL for Qualys US Platform 1 (<https://qualysapi.qualys.com>) in sample API requests. If you're on another platform, please replace this URL with the appropriate Qualys API Server and URL for your account.

### Enable Azure Storage Blob Integration

**<Qualys\_API\_URL>/qps/rest/2.0/add/integration/azure/storage-blob/vm**

[POST]

The first step towards the integration is enabling Azure Storage Blob integration. To enable the Azure Storage Blob integration, you need to provide name and connection string in the API request body. The connection string can be obtained from that Azure Blob storage container you create. You can specify other optional parameters (base category, minimum severity, etc) as per your requirement.

Once you create the integration, the response provides an unique integration identifier (id) for the Azure Storage Blob integration.

## Input Parameters

Parameter	Description
connectionString={value}	(Required) Provide the connection string assigned to the container in Azure Storage Blob.
minSeverity={value}	The minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Storage Blob. 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 Azure Storage Blob.
baseCategory={IG Potential Confirmed}	Category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Storage Blob. 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.
name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for name is 50 characters.
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. If you want to exclude the compression, set this parameter to false. Batch and compress data saves on disk and network IO. By default, the compressData parameter is configured to true.
containerName={value}	Provide the name of the container, which was created under Azure Storage Blob account for this integration. You can find the vulnerability findings and vulnerability information in this container. If you do not provide container name, we use qualys-vm-findings by default. In such case, ensure that container with name qualys-vm-findings is created under Azure Storage Blob.

## Enable Azure Storage Blob Integration

### API request:

```
curl -u 'username:password' -X POST --header 'Content-Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/add/integration/azure/storage-
```

```
blob/vm' --data '@integration.json'
```

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

#### Request POST Data (integration.json):

```
{
  "connectionString":
  "BlobEndpoint=https://user_john.blob.core.windows.net/;SharedAccessSignat
  ure=sv=2019-12-12&ss=b&srt=co&sp=rwx&se=2020-09-04T22:36:36Z&st=2020-09-
  04T14:36:36Z&spr=https&sig=key%ckd%3D",
  "minSeverity": 4,
  "baseCategory": "Potential",
  "name": "Integration name",
  "resultSectionNeeded": true,
  "sendVulnInfo": true,
  "compressData": true,
  "containerName": "qualys-vm-findings"
}
```

#### JSON output:

```
{
  "ServiceResponse": {
    "count": 1,
    "data": [
      "integrationId=5"
    ],
    "responseCode": "SUCCESS"
  }
}
```

## Update Azure Storage Blob Integration

<Qualys\_API\_URL>/qps/rest/2.0/update/integration/azure/storage-blob/{integrationId}/vm [PUT]

Once you enable the Azure Storage Blob integration, you can update the name, connectionString, baseCategory, resultSectionNeeded and other parameters of the Azure Storage Blob with Qualys.



## Input Parameters

Parameter	Description
connectionString={value}	Provide the connection string assigned to the container in Azure Storage Blob.
minSeverity={value}	The minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Storage Blob. For example, if you set the value to 1, all findings with severity level 1 to 5 are fetched and available on Azure Storage Blob.
baseCategory={IG Potential Confirmed}	Category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Storage Blob. The valid values are IG, Confirmed, and Potential. 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.
name={value}	Provide a unique name for the integration in the API request. The maximum length allowed for name is 50 characters.
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.
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.
compressData={true false}	Set this to true to compress the data in the response. If you want to exclude the compression, set this parameter to false. Batch and compress data saves on disk and network IO.
containerName={value}	Provide the name of the container, which was created under Azure Storage Blob account for this integration. You can find the vulnerability findings and vulnerability information in this container.

## Update Azure Storage Blob Integration details

Let us now see an example to update the configuration details of the Azure Storage Blob integration. Provide the configuration details to be updated in the PUT request.

### API request:

```
curl -u 'username:password' -X PUT --header 'Content-Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/update/integration/azure/storage-blob/{integrationId}/vm' --data '@integration.json'
```

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

### Request PUT Data (integration.json):

```
{
  "connectionString":
  "BlobEndpoint=https://user_john.blob.core.windows.net/;SharedAccessSignat
```

```
ure=sv=2019-12-12&ss=b&srt=co&sp=rwx&se=2020-09-04T22:36:36Z&st=2020-09-04T14:36:36Z&spr=https&sig=key%ckd%3D",
  "minSeverity": 4,
  "baseCategory": "Potential",
  "name": "Integration name",
  "resultSectionNeeded": true,
  "sendVulnInfo": true,
  "compressData": false,
  "containerName": "qualys-vm-findings"
}
```

#### JSON output:

```
{
  "ServiceResponse": {
    "count": 1,
    "data": [
      "Azure Storage Blob integration successfully updated."
    ],
    "responseCode": "SUCCESS"
  }
}
```

## Get Details of the Azure Storage Blob Integration

<Qualys\_API\_URL>/qps/rest/2.0/get/integration/azure/storage-blob/{integrationId}/vm  
[GET]

<Qualys\_API\_URL>/qps/rest/2.0/get/integration/azure/storage-blob/vm [GET]

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

Currently, you can only fetch details for the VM/VMDR app.

### Get integration details of the Azure Storage Blob integration

Let us now see an example to fetch the integration details of Azure Storage Blob integration.

#### API request:

```
curl -u 'username:password' -X GET
'https://qualysapi.qualys.com/qps/rest/2.0/get/integration/azure/storage-
blob/{integrationId}/vm'
OR
```

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

```
curl -u 'username:password' -X GET
'https://qualysapi.qualys.com/qps/rest/2.0/get/integration/azure/storage-
blob/vm'
```

JSON output:

```
{
  "ServiceResponse": {
    "count": 1,
    "data": [
      "{integrationId=5,
        name='Customer Name',
        customerId=176821,
        customerUUID='b35e0d4c-7636-e6f4-8244-551bbb6c6140',
        minSeverity=4,
        baseCategory=Potential,
        resultSectionNeeded=false,
        sendVulnInfo=false,
        compressData=false,
        containerName= 'qualys-vm-findings'}"
    ],
    "responseCode": "SUCCESS"
  }
}
```

## Delete Azure Storage Blob Integration Details

<Qualys\_API\_URL>/qps/rest/2.0/delete/integration/azure/storage-blob/{integrationId}/vm [DELETE]

For an Azure Storage Blob integration, you could delete the integration using the unique identifier associated with the integration.

### Delete the Azure Storage Blob integration

API request:

```
curl -u 'username:password' -X DELETE
'https://qualysapi.qualys.com/qps/rest/2.0/delete/integration/azure/stora
ge-blob/{integrationId}/vm '
```

where, integrationId is the unique integration identifier of the Azure Storage Blob

JSON output:

```
{
  "ServiceResponse": {
    "count": 1,
    "data": [
      "Azure Storage Blob integration successfully deleted."
    ],
    "responseCode": "SUCCESS"
  }
}
```

# Findings and Insights

Let us see the detailed steps for viewing findings and insights on Azure Storage Blob console.

[View Findings on Azure Storage Blob Console](#)

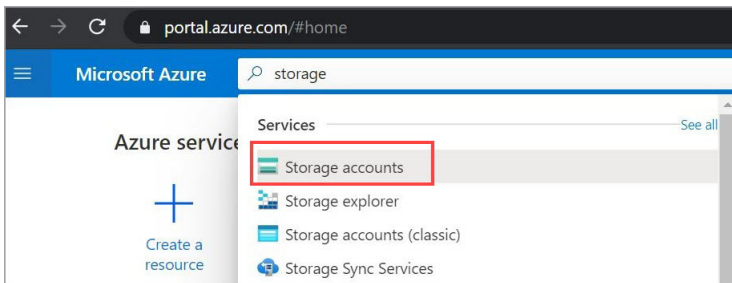
[Troubleshooting Tips](#)

## View Findings on Azure Storage Blob Console

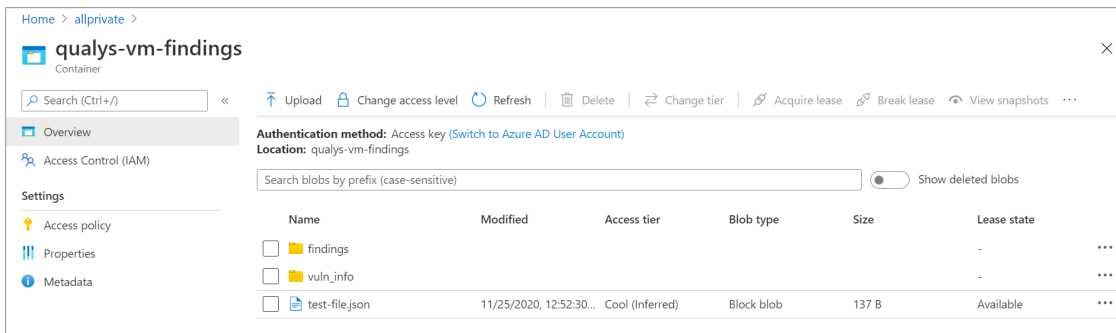
Before you view findings on Azure Storage Blob console, ensure that you have met the pre-requisites, completed all the configurations with Azure and Qualys, and have findings available in your Qualys subscription.

Let us see the detailed steps to view the findings.

1. Login to Azure portal (<https://portal.azure.com/>) and search for Storage accounts in the search bar.



2. Locate the container you associated with the integration. See the directories for findings, vuln\_info (if enabled through APIs) and a test file, which Qualys uses for validation of connection string.



The findings directory has subdirectories for each date which contain the findings in the files with specific file naming format.

**Authentication method:** Access key ([Switch to Azure AD User Account](#))  
**Location:** [qualys-vm-findings](#) / findings

Search blobs by prefix (case-sensitive) ☐ Show deleted blobs

Name	Modified	Access tier	Blob type	Size	Lease state
<input type="checkbox"/> [.]					
<input type="checkbox"/> 2020-11-09					-
<input type="checkbox"/> 2020-11-26					-

3. Go to a specific folder and view the findings detected on that date.

[Upload](#)
[Change access level](#)
[Refresh](#)
[Delete](#)
[Change tier](#)
[Acquire lease](#)
[Break lease](#)
[View snapshots](#)

**Authentication method:** Access key ([Switch to Azure AD User Account](#))  
**Location:** [qualys-vm-findings](#) / [findings](#) / 2020-11-26

Search blobs by prefix (case-sensitive) ☐ Show deleted blobs

Name	Modified	Access tier	Blob type	Size
<input type="checkbox"/> [.]				
<input type="checkbox"/> 0f217e37-6f41-4946-958d-0238a0190b22.json	11/26/2020, 11:27:03 AM	Cool (Inferred)	Block blob	6.92 KiB
<input type="checkbox"/> 27e5e952-25a7-495f-93fe-876a715fd056.json	11/26/2020, 12:07:00 PM	Cool (Inferred)	Block blob	6.92 KiB
<input type="checkbox"/> 3e74742c-0180-4c8e-81ef-e5017a925258.json	11/26/2020, 12:19:56 PM	Cool (Inferred)	Block blob	6.92 KiB
<input type="checkbox"/> 710da0ea-2f6c-490c-8be1-46670d8fab9f.json	11/26/2020, 11:58:56 AM	Cool (Inferred)	Block blob	6.92 KiB
<input type="checkbox"/> 7ab30f68-6561-40a7-a0e2-f61afb18ec2d.json	11/26/2020, 11:30:38 AM	Cool (Inferred)	Block blob	6.92 KiB
<input type="checkbox"/> 89a8ecce-1c4b-4b93-a70e-c0be77a26ce8.json	11/26/2020, 11:30:46 AM	Cool (Inferred)	Block blob	6.92 KiB
<input type="checkbox"/> 91496a99-880a-43a9-a44d-2047bf74c22e.json	11/26/2020, 11:33:30 AM	Cool (Inferred)	Block blob	6.92 KiB
<input type="checkbox"/> 96e557b0-e0a5-43f9-8ca6-306b7a05fe07.json	11/26/2020, 11:31:33 AM	Cool (Inferred)	Block blob	6.92 KiB

If you have enabled vuln\_info, you can locate data under vuln\_info directory with separate file for each QID with specific file naming format.

**Authentication method:** Access key ([Switch to Azure AD User Account](#))  
**Location:** [qualys-vm-findings](#) / vuln\_info

Search blobs by prefix (case-sensitive) ☐ Show deleted blobs

Name	Modified	Access tier	Blob type	Size
<input type="checkbox"/> [.]				
<input type="checkbox"/> qid-100001.json	11/26/2020, 12:35:44 PM	Cool (Inferred)	Block blob	4.36 KiB

## Troubleshooting Tips

Let us see scenarios that will help you debug the common issues.

### **Scenario: Qualys Findings not visible in Qualys subscription**

Workaround: To view Qualys findings in your subscription ensure the following:

- Qualys sensors are deployed on the endpoints
- Vulnerability scans are conducted

### **Scenario: Qualys Findings not visible on Azure Storage Blob console**

Workaround: To view Qualys findings on Azure Storage Blob console ensure the following:

- Qualys sensors are deployed on the endpoints
- Vulnerability assessment and findings are available in your Qualys subscription
- Integration configuration with Qualys and Azure Storage Blob console is complete

For any such issues related to Azure Storage Blob Integration with Qualys, reach out to [Qualys Support](#).