Qualys Integration with Azure Storage Blob
API User Guide

November 30, 2021
Table of Contents

About this guide................................................................................................4
About Qualys ........................................................................................................... 4
Qualys Support ........................................................................................................ 4

Introduction........................................................................................................ 5
Qualys Integrated Security Platform ....................................................................... 5
Pre-requisites ......................................................................................................... 7

Getting Started with Azure Storage Blob Integration................................. 8
Creating Storage Account ...................................................................................... 8

Configuring Integration with Qualys ............................................................... 14
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

Findings and Insights..................................................................................... 20
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

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/
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.
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.

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.

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.

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**
**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.

![Access Keys Section](image)
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:

<table>
<thead>
<tr>
<th>Platform</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>US POD 1</td>
<td>64.39.96.20</td>
</tr>
<tr>
<td>US POD 2</td>
<td>64.39.96.25</td>
</tr>
<tr>
<td>US POD 3</td>
<td>64.39.96.27</td>
</tr>
<tr>
<td>EU POD 1</td>
<td>64.39.100.20</td>
</tr>
<tr>
<td>EU POD 2</td>
<td>154.59.121.40</td>
</tr>
<tr>
<td>CA POD</td>
<td>64.39.97.25</td>
</tr>
<tr>
<td>India POD</td>
<td>103.216.98.25</td>
</tr>
</tbody>
</table>
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.
# Azure Storage Blob Integration with Qualys

## Configuring Integration with Qualys

### Input Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connectionString={value}</td>
<td>(Required) Provide the connection string assigned to the container in Azure Storage Blob.</td>
</tr>
<tr>
<td>minSeverity={value}</td>
<td>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.</td>
</tr>
<tr>
<td>baseCategory={IG</td>
<td>Potential</td>
</tr>
<tr>
<td>name={value}</td>
<td>(Required) Provide a unique name for the integration in the API request. The maximum length allowed for name is 50 characters.</td>
</tr>
<tr>
<td>resultSectionNeeded={true</td>
<td>false}</td>
</tr>
<tr>
<td>sendVulnInfo={true</td>
<td>false}</td>
</tr>
<tr>
<td>compressData={true</td>
<td>false}</td>
</tr>
<tr>
<td>containerName={value}</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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):

```json
{
  "connectionString": "BlobEndpoint=https://user_john.blob.core.windows.net/;SharedAccessSignature=sv=2019-12-12&ss=b&st=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:

```json
{
  "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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connectionString</td>
<td>Provide the connection string assigned to the container in Azure Storage Blob.</td>
</tr>
<tr>
<td>minSeverity</td>
<td>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.</td>
</tr>
<tr>
<td>baseCategory</td>
<td>Category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Storage Blob. 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.</td>
</tr>
<tr>
<td>name</td>
<td>Provide a unique name for the integration in the API request. The maximum length allowed for name is 50 characters.</td>
</tr>
<tr>
<td>resultSectionNeeded</td>
<td>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.</td>
</tr>
<tr>
<td>sendVulnInfo</td>
<td>Set this to true if you need the vulnerability information. If you want to exclude the vulnerability information, set this parameter to false.</td>
</tr>
<tr>
<td>compressData</td>
<td>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.</td>
</tr>
<tr>
<td>containerName</td>
<td>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.</td>
</tr>
</tbody>
</table>

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"
```
Azure Storage Blob Integration with Qualys
Configuring Integration with Qualys

```
"minSeverity": 4,
"baseCategory": "Potential",
"name": "Integration name",
"resultSectionNeeded": true,
"sendVulnInfo": true,
"compressData": false,
"containerName": "qualys-vm-findings"
```

**JSON output:**

```json
{
  "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:

```json
{
    "ServiceResponse": {
        "count": 1,
        "data": [
            {
                "integrationId": 5,
                "name": "Customer Name",
                "customerId": 176821,
                "customerUUID": "b35e0d4c-7636-e6f4-8244-551bbbec6140",
                "minSeverity": 4,
                "baseCategory": "Potential",
                "resultSectionNeeded": false,
                "sendVulnInfo": false,
                "compressData": false,
                "containerName": "qualys-vm-findings"
            }
        ],
        "responseCode": "SUCCESS"
    }
}
```

Delete Azure Storage Blob Integration Details

```bash
<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:**

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

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

**JSON output:**

```json
{
    "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.

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

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.
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.