Qualys Integration with AWS Security Hub

API User Guide

August 28, 2023

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

Table of Contents

About this guide 4

About Qualys 4
Qualys Support 4

Introduction 5

Qualys Integrated Security Platform 5
Pre-requisites 7

Enabling Qualys Apps in Amazon Security Hub 9

Enabling Amazon Security Hub for a Specific Region 9
Enabling Qualys Vulnerability Management on Amazon Security Hub Console 10

Configuring Integration with Qualys 12

URL to the Qualys API Server 13
Authentication for Gateway URLs 13
Create Amazon Security Hub Integration 13
Configure Amazon Security Hub Integration 15
Update Amazon Security Hub Integration 17
Get Details of the Amazon Security Hub Integration 20
Delete Amazon Security Hub Details 23

Findings and Insights 28

View Findings on AWS Console 28
Insights on AWS Console 29
Troubleshooting Tips 29

About this guide

Welcome to Qualys Cloud Platform and integration of Qualys Cloud Platform with Amazon Web Services! We'll help you get acquainted with the Qualys solutions for integrating your AWS Cloud 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

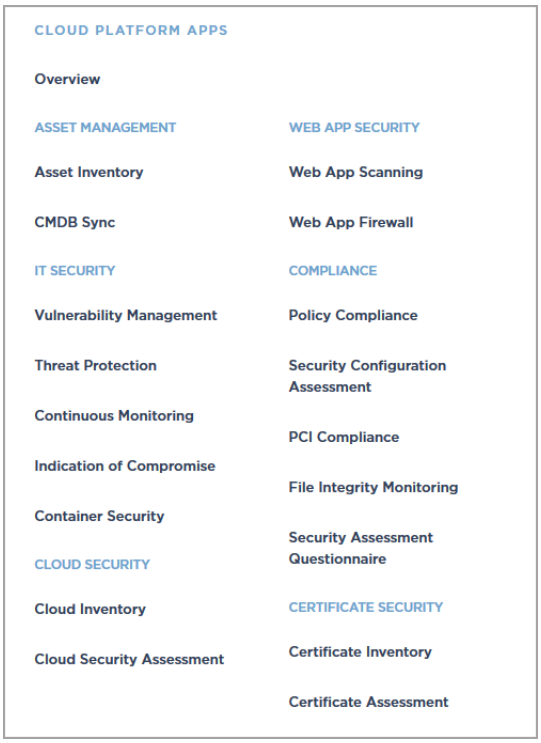
Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

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 securing your Amazon AWS EC2 infrastructure using Qualys.

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.

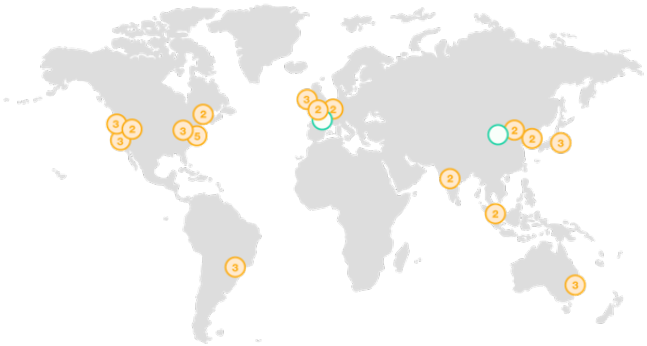


Qualys Support for AWS

You can now access Qualys vulnerability assessment findings in Amazon Security Hub. The Amazon Security Hub 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 Amazon Security Hub, you can get near real-time, up-to-date visibility of your security posture in Amazon console. These findings, gained by the correlation of Qualys information with other data in Amazon Security Hub, allow customers to quickly detect risks in their AWS environments and take rapid,automated remedial actions.

Qualys AWS Cloud support provides the following features:

- Secure EC2 Instances (IaaS) from vulnerabilities and check for regulatory compliance on OS and Applications (Database, Middleware)



- Gain continuous security using Cloud Agents, embed them into AMIs to get complete visibility

- Identify vulnerabilities for public facing IPs and URLs

- Secure Application using Application Scanning and Firewall solutions

- Vulnerability Scan

- Supports all AWS global regions including GovCloud

- Supports EC2 instances in Classic and VPC platform

- Qualys Cloud Agents certified to work in EC2

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

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

Pre-requisites

These options must be enabled for your Qualys user account.

- 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

- AWS Security Hub must be enabled for the desired region

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)

Policy Compliance Overview (14 mins)

Quick Steps: Integrating Amazon Web Services with Qualys

Here's the user flow for integrating Qualys with AWS Security Hub.

1 - Enabling Qualys Apps in Amazon Security Hub: AWS Security Hub (enabled for region) > Integrations > Qualys VM product > Enable this Integration (Accept findings). Learn more.

2 - Configuring Integration with Qualys using APIs available to configure integration with Qualys Cloud Platform.

3 - Configuring Insights on AWS Console (Optional).

1. Enable Qualys Apps in Amazon Security Hub
2. Configure Integration steps with Qualys
3. Configure Insights on AWS (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

Qualys AWS EC2 Video Series | Learn how to discover and secure AWS assets

Enabling Qualys Apps in Amazon Security Hub

Enabling Amazon Security Hub integration involves the following two quick steps on AWS console.

Enabling Amazon Security Hub for a Specific Region

Enabling Qualys Vulnerability Management on Amazon Security Hub Console

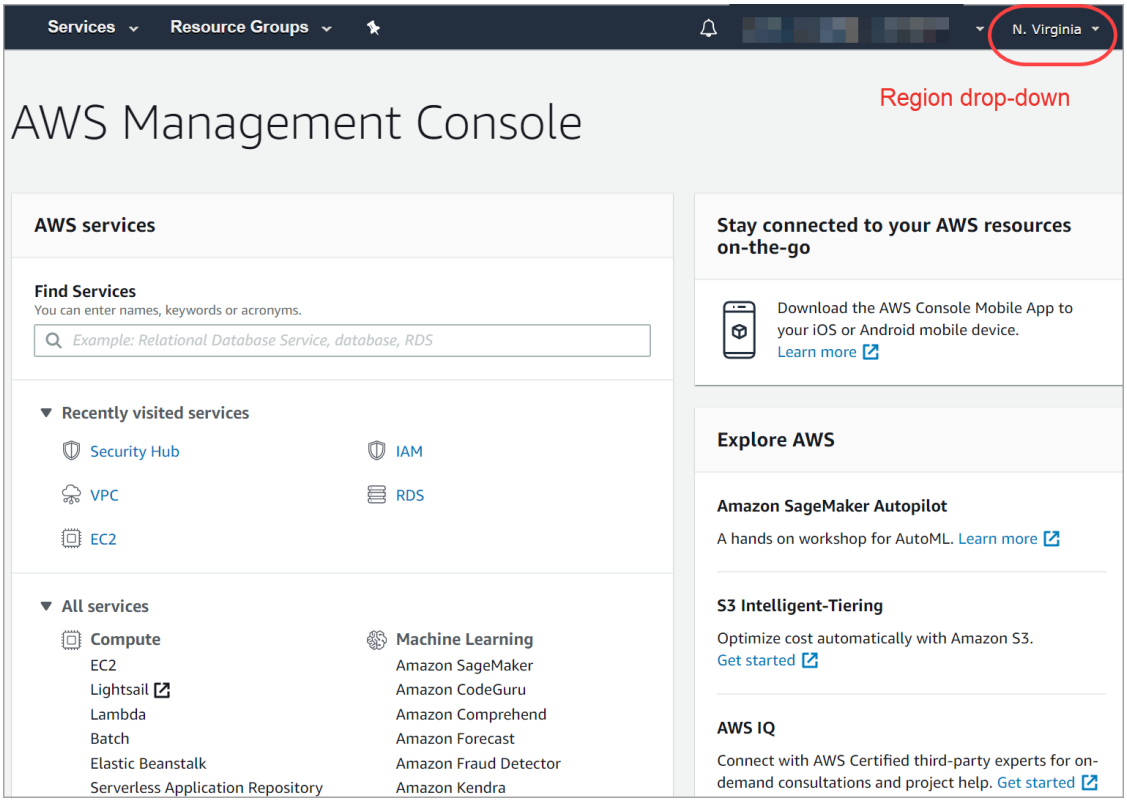
Enabling Amazon Security Hub for a Specific Region

You must enable Amazon Management Console for every region that needs to be assessed and included in the integration.

Note: You can view the findings reported by Qualys only for those regions for which Amazon Management Console is enabled.

Let us see the steps to enable Amazon Management Console for a region.

1 - Go to AWS Management Console.



2 - Select the region to be enabled from the upper right-hand corner and click the region.

3 - Click **Go to Security Hub**.

The Welcome to AWS Security Hub page is displayed.

4 - Ensure that you retain the default options checked-in and click **Enable Security Hub**.

The Amazon Security Hub is then enabled for the selected region.

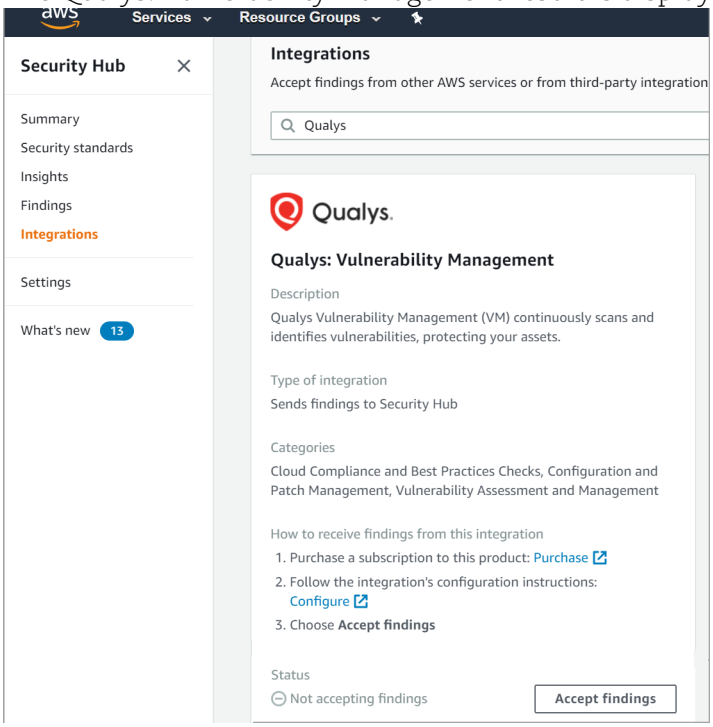
Enabling Qualys Vulnerability Management on Amazon Security Hub Console

1 - Go to Amazon Security Hub Console.

2 - Go to **Integrations** tab.

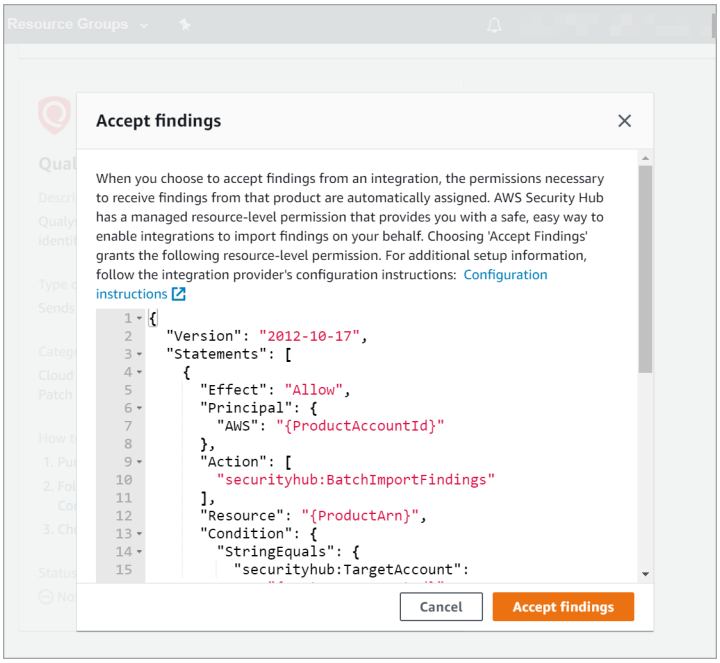
3 - Type Qualys in Filter integrations search box.

The Qualys: Vulnerability Management result is displayed.



4 - Click **Accept findings**.

The resource policies are displayed.



5 - Click **Accept findings** on the resource policies to complete the integration from AWS console. These resource policies define the permissions that the Amazon Security Hub needs to receive findings from the product. For more information, check Managing AWS Security Hub Product Integrations.

Once you complete the integration steps with Qualys, you can view the findings on AWS console.

Configuring Integration with Qualys

We provide APIs (JSON) to fasten and simplify the integration process with Amazon Security Hub. The integration process involves two quick steps with Qualys using APIs: creating the Amazon Security Hub integration and configuring the Amazon Security Hub integration. Once you configure it, you can use it to fetch details, update the existing configuration of Amazon Security Hub, or delete the Amazon Security Hub integration as well.

New Integrations

For new integrations, use the create API first and then configure VM/VMDR app. Once you have created Amazon Security Hub Integrations, then they can get unique integration Id using the GET API and then can update VM config i.e severity level, category, additional AWS accounts, and regions using the update API.

Create Amazon Security Hub Integration

Configure Amazon Security Hub Integration

Update Amazon Security Hub Integration

Get Details of the Amazon Security Hub Integration

Delete Amazon Security Hub Details

Existing Integrations

For existing Amazon Security Hub Integrations you can get/fetch unique integration Id using the GET API. You can update VM config i.e severity level, category, additional AWS accounts, and regions using the update API.

Update Amazon Security Hub Integration

Get Details of the Amazon Security Hub Integration

Delete Amazon Security Hub 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 document uses <qualys_gateway_url> in sample API requests. If you're on another platform, please replace this URL with the appropriate Qualys API Gateway URL(for example, https://gateway.qg1.apps.qualys.com for US POD1) for your account.

Authentication for Gateway URLs

You must authenticate to the Qualys Cloud Platform using Qualys account credentials (user name and password) and get the JSON Web Token (JWT) before you can start using the Gateway URLs. Use the Qualys Authentication API to get the JWT.

For example,

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

The Authentication API returns a JSON Web Token (JWT) which you can use for authentication during Container Security API calls. The token expires in 4 hours. You must regenerate the token to continue using the APIs.

Create Amazon Security Hub Integration

/partner-integration/aws/security-hub

[POST]

The first step towards the integration is creation of Amazon Security Hub integration. To create the Amazon Security Hub integration, you need to provide an unique name for integration in the API request body. Once you create the Amazon Security Hub integration, the response provides an unique integration identifier (id) for the Amazon Security Hub.

Input Parameters

Parameter	Description
name= {value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for name is 50 characters.
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.

Create Amazon Security Hub Integration

API request:

```
curl -X POST --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-hub' --data
'@integration.json'
-H "Authorization: Bearer <token>"
```

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

Request POST Data (integration.json):

```
{
 "name": "Demo Integration Name"
 "sendAlerts": true,
  "errorEmails":
 [
  "<email address 1>",
  "<email address 2>"
 ]
}
```

JSON output:

```
{
 "integrationId=40"
}
```

Configure Amazon Security Hub Integration

/partner-integration/aws/security-hub/{id}/vm

[POST]

The next step after you create the Amazon Security Hub integration is to configure it and enable integration with the VM/VMDR app. During the configuration, you need to provide the AWS account details such as AWS account ids, base category, regions, minimum severity level of the vulnerabilities that should be fetched from Qualys (VM/VMDR app) to be posted to Amazon Security Hub. Once you complete the configuration steps, the Amazon Security Hub Integration is enabled with VM/VMDR app.

Input Parameters

Parameter	Description
`id={value}`	(Required) Unique identifier (id) assigned to the Amazon Security Hub integration.

vmConfigs	Configuration details of the Amazon Security Hub in following format:
	`"vmConfigs":[`
	`{`
	`"minSeverity":1,`
	`"baseCategory":"Potential",`
	`"awsAccounts":[`
	`"111111111111",`
	`"222222222222"`
	`],`
	`"regions":[`
	`"eu-west-2",`
	`"eu-west-1"`
	`]`
	`},`
	where,
	minSeverity: minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Amazon Security Hub. 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 Amazon Security Hub.
	baseCategory: category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Amazon Security Hub. The valid values are 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.
	awsAccounts: List of AWS account ids for which AWS Security Hub is enabled.
	regions: List of AWS regions where Amazon Security Hub is enabled. As AWS Security Hub is regional service, you need to add all regions that are enabled for AWS Security Hub.

Configure Amazon Security Hub Integration

API request:

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

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

Request POST Data (integration.json):

```
{
   "vmConfigs":[
      {
         "minSeverity":1,
         "baseCategory":"Potential",
         "awsAccounts":[
             "111111111111",
             "222222222222" ],
         "regions":[
            "eu-west-2",
            "eu-west-1"
         ]
      },

      {
         "minSeverity":3,
         "baseCategory":"Confirmed",
         "awsAccounts":[
             "333333333333",
             "444444444444"
         ],
         "regions":[
            "eu-west-2",
            "eu-west-1"
         ]
      }
   ]
}
```

JSON output:

```
{
         "VM successfully enabled for AWS security hub.
}
```

Update Amazon Security Hub Integration

/partner-integration/aws/security-hub/{id} [POST]

/partner-integration/aws/security-hub/{id}/vm [PUT]

Once you configure the Amazon Security Hub integration, you can update the name, integration or configuration details of the Amazon Security Hub integration with Qualys.

Note: If integration created but not enabled (VM Configuration is not done) for particular AWS account, it gets enabled during the update request (PUT) and the details are updated as well.

Input Parameters

Parameter	Description
`id={value}`	(Required) Unique identifier (id) assigned to the Amazon Security Hub integration. The unique integration identifier (id) of the Amazon Security Hub cannot be updated.

vmConfigs	Configuration details of the Amazon Security Hub in following format:
	`"vmConfigs":[`
	`{`
	`"minSeverity":1,`
	`"baseCategory":"Potential",`
	`"awsAccounts":[`
	`"111111111111",`
	`"222222222222"`
	`],`
	`"regions":[`
	`"eu-west-2",`
	`"eu-west-1"`
	`]`
	`},`
	where,
	minSeverity: minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Amazon Security Hub. 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 Amazon Security Hub.
	baseCategory: category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Amazon Security Hub. The valid values are 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.
	awsAccounts: List of AWS account ids for which AWS Security Hub is enabled.
	regions: regions enabled with Amazon Security Hub. As AWS Security Hub is regional service, you need to add all regions that are enabled for AWS Security Hub.

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.

Note:

- If you mention regions that are not enabled for Amazon Security Hub in the request, the regions are skipped. Only regions that are enabled for Amazon Security Hub are updated.

- The minSeverity, baseCategory and regions are optional parameters.

Update Name of the Amazon Security Hub Integration

Let us see an example to update the name of the Amazon Security Hub integration. Provide the new name for the Amazon Security Hub integration in the request.

API request:

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

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

Request POST Data (integration.json):

```
{
 "name": "New Qualys Demo"
 "sendAlerts": true,
  "errorEmails":
 [
  "<email address 1>",
  "<email address 2>"
 ]
}
```

JSON output:

```
{    "message": "AWS security hub VM integration successfully updated."}
```

Update configuration details of the Amazon Security Hub integration

Let us now see an example to update the configuration details of the Amazon Security Hub integration. Provide the configuration details to be updated in the PUT request.

API request:

```
curl -X PUT --header 'Content-Type:application/json'
'<qualys_gateway_url>//partner-integration/aws/security-hub/{id}/vm' --
data '@integration.json'
```

where, id is the unique integration identifier of the Amazon Security Hub

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

Request PUT Data (integration.json):

```
{
   "vmConfigs":[
      {
         "minSeverity":1,
         "baseCategory":"Potential",
         "awsAccounts":[
             "111111111111",
             "222222222222"],
         "regions":[
```

```
                "eu-west-2",
                "eu-west-1"
            ]
        },
        {
            "minSeverity":3,
            "baseCategory":"Confirmed",
            "awsAccounts":[
                 "333333333333",
                 "444444444444"
            ],
            "regions":[
                "eu-west-2",
                "eu-west-1"
            ]
        }
    ]
}
```

JSON output:

```
{    "message": "AWS accounts and their VM configuration successfully
updated."}
```

Get Details of the Amazon Security Hub Integration

/partner-integration/aws/security-hub [GET]

/partner-integration/aws/security-hub/vm/ [GET]

When you want to get details of a particular Amazon Security Hub integration, you can fetch the configuration and integration details using the unique integration identifier (id) of the Amazon Security Hub integration. For existing integrations, you can fetch the configuration and integration details with or without the unique integration identifier (id) of the Amazon Security Hub integration.

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

Get configuration details of the Amazon Security Hub integration

Let us now see an example to fetch the configuration details of Amazon Security Hub integration.

API request:

```
curl -X GET --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-hub/49'
-H "Authorization: Bearer <token>"
OR
```

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

```
curl -X GET --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-hub/'
-H "Authorization: Bearer <token>"
```

JSON output:


```
{
    "name": "TestAWSSecurityHubIntegration01",
    "integrationId": 684,
    "customerId": xxxxxx,
    "sendResolvedVulns": true,
    "sendAlerts": false,
    "errorEmails": [
        "<email address 1>"
    ],
    "vmConfigs": [
        {
            "awsAccountId": "xxxxxxxxxxxx",
            "severity": 1,
            "category": "Confirmed",
            "regions": [
                "eu-west-1",
                "us-west-2"
            ]
        }
    ]
}
```


Get integration details of the Amazon Security Hub with VM/VMDR

Let us now see an example to fetch the integration details of Amazon Security Hub with VM/VMDR app.

API request:

```
curl -X GET --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-hub/vm/'
-H "Authorization: Bearer <token>"
OR

curl -X GET --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-hub/{id}/vm/'
-H "Authorization: Bearer <token>"
```

where, id is the unique integration identifier of the Amazon Security Hub

JSON output:


```
{
    "name": "NMTestAWSSecurityHubIntegration01",
    "integrationId": 684,
    "customerId": 715423,
    "sendResolvedVulns": true,
    "sendAlerts": false,
    "errorEmails": [
```

```
            "<email address 1>"
        ],
        "vmConfigs": [
            {
                "awsAccountId": "xxxxxxxxxxxx",
                "severity": 1,
                "category": "Confirmed",
                "regions": [
                    "eu-west-1",
                    "us-west-2"
                ]
            }
        ]
    }
```

Delete Amazon Security Hub Details

/partner-integration/aws/security-hub/id [DELETE]

/partner-integration/aws/security-hub/{id}/vm [POST]

For an Amazon Security Hub integration, you could delete the following:

- Amazon Security Hub integration

- AWS accounts associated with the Amazon Security Hub

- regions associated with the Amazon Security Hub

Note: If you have only single region associated with the AWS account used for integration, you cannot delete the region. Deletion of region for an AWS account used for integration is possible only if there are multiple regions associated with the AWS account.

Delete the Amazon Security Hub integration

API request:

```
curl -X DELETE --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-hub/{id}'
-H "Authorization: Bearer <token>"
```

where, id is the unique integration identifier of the Amazon Security Hub

JSON output:

```
{    "message": "AWS security hub VM integration successfully deleted."}
```

Delete the accounts associated with the Amazon Security Hub

API request:

```
curl -X POST --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-hub/{id}/vm'
-H "Authorization: Bearer <token>"
```

where, id is the unique integration identifier of the Amazon Security Hub

Request POST Data (integration.json):

```
{
  "awsAccounts": [
       "111111111111",
       "222222222222"
  ]
}
```

JSON output:

```
{    "message": "AWS security hub VM integration successfully deleted."}
```

Delete the regions associated with the Amazon Security Hub

API request:

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

where, id is the unique integration identifier of the Amazon Security Hub
Note: “integration.json” contains the request POST data.

Request POST Data (integration.json):

```
{
   "vmRegionConfigs":[
      {
         "awsAccounts":[
             "111111111111",
             "222222222222"
         ],
         "regions":[
            "eu-west-2"
         ]
      }
   ]
}
```

JSON output:

```
{    "message": "Regions successfully deleted from AWS accounts in AWS
security hub VM integration."}
```

Delete the multiple regions associated with multiple accounts of the Amazon Security Hub Integration

API request:

```
curl -X POST --header 'Content-Type:application/json'
'<qualys_gateway_url>/partner-integration/aws/security-
hub/{id}/vm/regions --data '@integration.json'
```

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

where, id is the unique integration identifier of the Amazon Security Hub

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

Request POST Data (integration.json):

```
{
   "vmRegionConfigs":[
      {
         "awsAccounts":[
             "111111111111",
              "222222222222"
         ],
         "regions":[
            "us-west-2"
         ]

      },
      {
         "awsAccounts":[
            "33333333333"
         ],
         "regions":[
            "us-west-2",
            "us-west-1"
         ]

      }]
}
```

JSON output:

```
{    "message": "Regions successfully deleted from AWS accounts in AWS
security hub VM integration."}
```

Findings and Insights

Let us the see the detailed steps for viewing findings and insights on AWS console.

View Findings on AWS Console

Insights on AWS Console

Troubleshooting Tips

View Findings on AWS Console

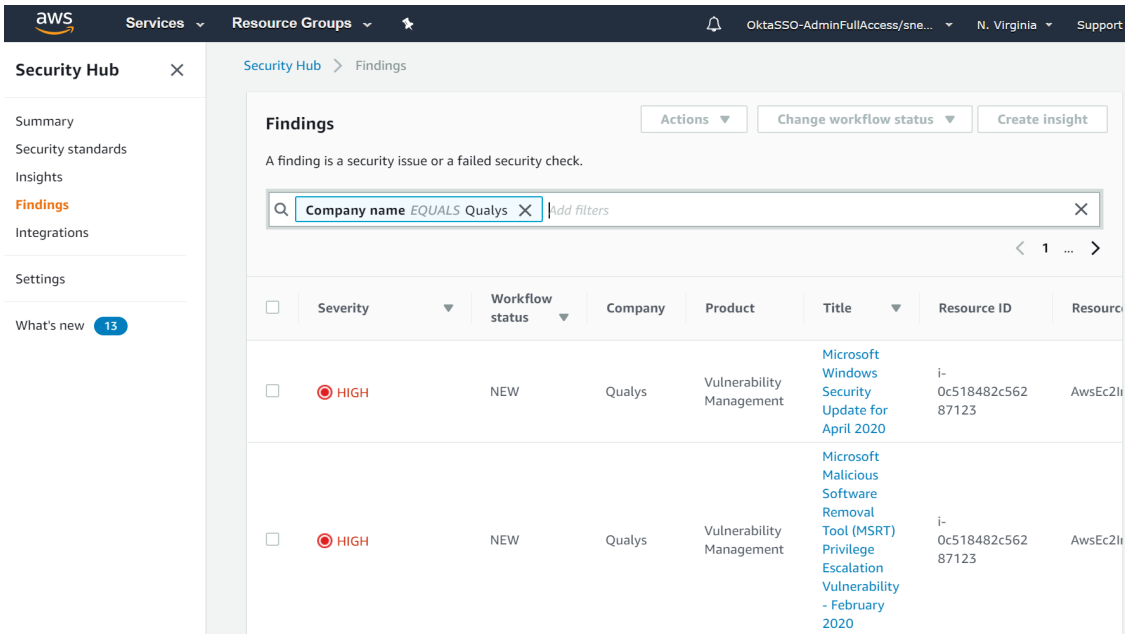
Before you view findings on AWS console, ensure that you have met the pre-requisites, completed all the configurations with AWS and Qualys, and have findings available in your Qualys subscription. For more information on findings, refer to Managing Findings.

Let us the see the detailed steps to view the findings.

1 - Go to Amazon Security Hub Console.

2 - Click Findings tab.

3 - Use pre-defined filters to view the findings. For example: Company name EQUALS Qualys.



You could click on the Title hyperlink of a finding to know more details about the finding.

Insights on AWS Console

To view Qualys-specific pre-defined filters or insights, you need to download the Cloud Formation template that we provide on the Qualys GitHub.

GitHub Link for Cloud Formation template: https://github.com/Qualys

Once you install the Cloud Formation template, the insights related Qualys findings are populated on AWS console.

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 AWS console

Workaround: To view Qualys findings on AWS 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 AWS console is complete

For any such issues related to Amazon Security Hub Integration with Qualys, reach out to Qualys Support.