



Qualys Cloud Platform v3.x

API Release Notes

Version 3.0.1.0

April 10, 2020

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

[WAS API: Set a Default DNS Override for Web Application](#)

[WAS API: Added a New Scan Status "PROCESSING" for WAS Scans](#)

[AWS Security Hub Integration](#)

URL to 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 gateway URL for Qualys US Platform 1 (<https://gateway.qg1.apps.qualys.com>) in sample API requests. If you're on another platform, please replace this URL with the appropriate gateway URL for your account.

WAS API: Set a Default DNS Override for Web Application

API affected	<code>/qps/rest/3.0/create/was/webapp</code> <code>/qps/rest/3.0/update/was/webapp/<id></code> <code>/qps/rest/3.0/get/was/webapp/<id></code>
New or Updated APIs	Updated API
DTD or XSD changes	Yes

When creating or updating your web application, you can now set one of the DNS override records assigned to your web application as default using these APIs. The default DNS override setting is useful when you want to scan multiple web applications using the DNS override option. We will use the default DNS override record that you have set for your web applications to launch scan on them. This functionality is already supported from the WAS UI.

Permissions

- You must have the WAS module enabled.
- You must have the "API Access" and "Access WAS module" permissions enabled.
- The web application must be within your scope.

Input Parameters

Parameter	Description
<code>config.defaultDnsOverride.id</code> (Long)	(Optional) The ID of the default DNS override record.
<code>config.defaultDnsOverride.name</code> (Text)	(Optional) The name of the default DNS override.

Sample - Set default DNS override for a web application

API request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @- "https://qualysapi.qualys.com/qps/rest/3.0/create/was/webapp/" < file.xml
```

Note: "file.xml" contains the request POST data.

Request POST Data (file.xml):

```
<ServiceRequest>  
  <data>  
    <WebApp>
```

```
<name><![CDATA[My Web Application5]]></name>
<url><![CDATA[http://mywebapp.com]]></url>
<config>
  <defaultDnsOverride>
    <id>14620</id>
  </defaultDnsOverride>
</config>
</WebApp>
</data>
</ServiceRequest>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/3.0/wa
s/webapp.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <WebApp>
      <id>14321734</id>
      <name>
        <![CDATA[My Web Application5]]>
      </name>
      <url>
        <![CDATA[http://mywebapp.com]]>
      </url>
      ...
      <config>
        <defaultDnsOverride>
          <id>14620</id>
          <name>
            <![CDATA[eee]]>
          </name>
        </defaultDnsOverride>
      </config>
      <crawlingScripts>
        <count>0</count>
      </crawlingScripts>
    </WebApp>
  </data>
</ServiceResponse>
```

Sample - Update default DNS override record for a web application

API request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @- "https://qualysapi.qualys.com/qps/rest/3.0/update/was/webapp/1234" <file.xml
```

Note: "file.xml" contains the request POST data.

Request POST Data (file.xml):

```
<ServiceRequest>
  <data>
    <WebApp>
      <config>
        <defaultDnsOverride>
          <id>14620</id>
        </defaultDnsOverride>
      </config>
    </WebApp>
  </data>
</ServiceRequest>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/3.0/was/webapp.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <WebApp>
      <id>14321734</id>
    </WebApp>
  </data>
</ServiceResponse>
```

Sample - Get details of default DNS override for a web application

API request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @- "https://qualysapi.qualys.com/qps/rest/3.0/get/was/webapp/1234"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/3.0/was/webapp.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <WebApp>
      <id>14321734</id>
      ...
    <config>
      <defaultDnsOverride>
        <id>10820</id>
        <name><![CDATA[Demo-updated3]]></name>
      </defaultDnsOverride>
    </config>
    <climbingScripts>
      <count>0</count>
    </climbingScripts>
  </WebApp>
</data>
</ServiceResponse>
```

XSD Update

Changes in webapp.xsd (.../qps/xsd/3.0/was/webapp.xsd).

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">

  <!-- REQUEST -->
  <xs:element name="ServiceRequest">
    <xs:complexType>
      <xs:all>
        <xs:element name="filters" type="ServiceRequestFilters"
minOccurs="0"/>
        <xs:element name="preferences"
type="ServiceRequestPreferences" minOccurs="0"/>
        <xs:element name="data" type="ServiceRequestData"
minOccurs="0"/>
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="ServiceRequestFilters">
    <xs:sequence>
      <xs:element name="Criteria" type="Criteria"
```

```
maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>
...
<xs:complexType name="WebAppConfig">
  <xs:sequence>
    <xs:choice>
      <xs:element name="cancelScansAfterNHours" type="xs:int"
minOccurs="0" />
      <xs:element name="cancelScansAt" type="xs:string"
minOccurs="0" />
    </xs:choice>
    <xs:element name="defaultAuthRecord" type="WebAppAuthRecord"
minOccurs="0" />
    <xs:element name="defaultDnsOverride" type="DnsOverride"
minOccurs="0" />
  </xs:sequence>
</xs:complexType>
...
<xs:simpleType name="WasLastScanStatus">
  <xs:restriction base="xs:string">
    <xs:enumeration value="SUBMITTED" />
    <xs:enumeration value="RUNNING" />
    <xs:enumeration value="FINISHED" />
    <xs:enumeration value="TIME_LIMIT_EXCEEDED" />
    <xs:enumeration value="SCAN_NOT_LAUNCHED" />
    <xs:enumeration value="SCANNER_NOT_AVAILABLE" />
    <xs:enumeration value="ERROR" />
    <xs:enumeration value="CANCELED" />
    <xs:enumeration value="SERVICE_ERROR" />
    <xs:enumeration value="NO_HOST_ALIVE" />
    <xs:enumeration value="NO_WEB_SERVICE" />
    <xs:enumeration value="CANCELED_WITH_RESULTS" />
  </xs:restriction>
</xs:simpleType>
</xs:schema>
```

WAS API: Added a New Scan Status "PROCESSING" for WAS Scans

The WAS Scan API Output will now show a new status "PROCESSING" for scans whose results are in processing in WAS. After the scan result is processed, the status of the scan is changed to Finished. This status is already used for scans launched from WAS UI.

API request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-  
"https://qualysapi.qualys.com/qps/rest/3.0/status/was/wasscan/1902350"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/3.0/was/wasscan.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
  <data>  
    <WasScan>  
      <id>1902350</id>  
      <status>PROCESSING</status>  
    </WasScan>  
  </data>  
</ServiceResponse>
```

AWS Security Hub Integration

APIs affected	/qps/rest/2.0/add/integration/amazon/securityhub/ /qps/rest/2.0/add/integration/amazon/securityhub/{id}/vm /qps/rest/2.0/update/integration/amazon/securityhub/{id} /qps/rest/2.0/update/integration/amazon/securityhub/{id}/vm /qps/rest/2.0/get/integration/amazon/securityhub/ /qps/rest/2.0/get/integration/amazon/securityhub/vm/ /qps/rest/2.0/get/integration/amazon/securityhub/{id}/vm/ /qps/rest/2.0/delete/integration/amazon/securityhub/{id} /qps/rest/2.0/delete/integration/amazon/securityhub/{id}/vm /qps/rest/2.0/delete/integration/amazon/securityhub/{id}/vm/reg ions
New or Updated APIs	New
DTD or XSD changes	Not Applicable

We have now introduced APIs (JSON) to fasten and simplify the integration process with AWS Security Hub. The integration process involves two quick steps: 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.

[Create Amazon Security Hub Integration](#)

[Configure Amazon Security Hub Integration](#)

[Update Amazon Security Hub Integration](#)

[Get Details of the Amazon Security Hub](#)

[Delete Amazon Security Hub Details](#)

Create Amazon Security Hub Integration

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

API request:

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

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

Request POST Data (integration.json):

```
{
  "name": "Demo Integration Name"
}
```

JSON output:

```
{
  "ServiceResponse": {
    "count": 1,
    "responseCode": "SUCCESS",
    "data": [
      "integrationId=40"
    ]
  }
}
```

Configure Amazon Security Hub Integration

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, regions, minimum severity level of the vulnerabilities that should be fetched from Qualys (VM/VMDR app) to be posted to Amazon Security Hub.

Input Parameters

Parameter	Description
vmConfigs	<p>Configuration details of the Amazon Security Hub in following format:</p> <pre>"vmConfigs": [{ "minSeverity": 1, "baseCategory": "Potential", "awsAccounts": [111111111111, 222222222222], "regions": ["eu-west-2", "eu-west-1"] }],</pre> <p>where,</p> <p>minSeverity: minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Amazon Security Hub</p> <p>baseCategory: category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Amazon Security Hub</p> <p>awsAccounts: AWS account ids that should be associated with the numbers of the Amazon Security Hub</p> <p>regions: regions associated with the Amazon Security Hub</p>

API request:

```
curl -u 'username:password' -X POST --header 'Content-Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/add/integration/amazon/securityhub/{id}/vm' --data '@integration.json'
```

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

Request POST Data (integration.json):

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

```

```
        22222222222222
    ],
    "regions": [
        "eu-west-2",
        "eu-west-1"
    ]
},
{
    "minSeverity": 3,
    "baseCategory": "Confirmed",
    "awsAccounts": [
        33333333333333,
        44444444444444
    ],
    "regions": [
        "eu-west-2",
        "eu-west-1"
    ]
}
]
}
```

JSON output:

```
{
  "ServiceResponse": {
    "count": 1,
    "responseCode": "SUCCESS",
    "data": [
      "VM successfully enabled for AWS security hub."
    ]
  }
}
```

Update Amazon Security Hub Integration

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: The unique integration identifier (id) of the Amazon Security Hub cannot be updated.

Sample 1: 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 -u 'username:password' -X POST --header 'Content-Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/update/integration/amazon/securityhub/{id}' --data '@integration.json'
```

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

Request POST Data (integration.json):

```
{
  "name": "New Qualys Demo"
}
```

JSON output:

```
{
  "ServiceResponse":{
    "data":[
      "AWS security hub integration successfully updated."
    ],
    "responseCode":"SUCCESS",
    "count":1
  }
}
```

Sample 2: 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 POST request.

API request:

```
curl -u 'username:password' -X PUT --header 'Content-Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/update/integration/amazon/secu'
```

```
rityhub/{123456}/vm' --data '@integration.json'
```

where, 123456 is the unique integration identifier (id) 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:

```
{
  "ServiceResponse":{
    "count":1,
    "responseCode":"SUCCESS",
    "data":[
      "AWS accounts and their VM configuration successfully updated."
    ]
  }
}
```

Get Details of the Amazon Security Hub

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.

Currently, we can only fetch details for the VM/VMDR app. We will soon support fetch details for more apps.

Sample 1: 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 -u 'username:password' -X GET --header 'Content-Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/get/integration/amazon/securityhub/'
```

JSON output:

```
{
  "ServiceResponse": {
    "count": 1,
    "responseCode": "SUCCESS",
    "data": [
      "{VM={name='Updated Qualys Demo Name',
integrationId=49,
customerId=223822,
vmConfigs=[
{awsAccountId=111111111111,
severity=3,
category=Potential,
regions=[eu-west-2, eu-west-1]},
{
awsAccountId=222222222222,
severity=3,
category=Potential,
regions=[eu-west-1]}
{awsAccountId=333333333333,
severity=3,
category=Confirmed,
regions=[eu-west-2, eu-west-1]},
{awsAccountId=444444444444,
severity=3,
category=Confirmed,
regions=[eu-west-2, eu-west-1]]}"
    ]
  }
}
```

```
}
}
```

Sample 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 -u 'username:password' -X GET --header 'Content-
Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/get/integration/amazon/securit
yhub/vm/'
```

OR

```
curl -u 'username:password' -X GET --header 'Content-
Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/get/integration/amazon/securit
yhub/{id}/vm/'
```

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

JSON output:

```
{
  "ServiceResponse":{
    "count":1,
    "responseCode":"SUCCESS",
    "data":[
      "{name='Updated Qualys Demo Name',
integrationId=34,
customerId=223822,
vmConfigs=[
{awsAccountId=111111111111,
severity=3,
category=Potential,
regions=[eu-west-2, eu-west-1]},
{awsAccountId=222222222222,
severity=3,
category=Potential,
regions=[eu-west-1]}
{awsAccountId=333333333333,
severity=3,
category=Confirmed,
regions=[eu-west-2, eu-west-1]},
{awsAccountId=444444444444,
severity=3,
category=Confirmed,
```

```
regions=[eu-west-2, eu-west-1]]}]}"
  ]
}
}
```

Delete Amazon Security Hub Details

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

Sample 1: Delete the Amazon Security Hub integration

API request:

```
curl -u 'username:password' -X DELETE --header 'Content-
Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/delete/integration/amazon/secu
rityhub/{123456}'
```

where, 123456 is the unique integration identifier (id) of the Amazon Security Hub

JSON output:

```
{
  "ServiceResponse":{
    "data":[
      "AWS security hub integration successfully deleted."
    ],
    "responseCode":"SUCCESS",
    "count":1
  }
}
```

Sample 2: Delete the accounts associated with the Amazon Security Hub

API request:

```
curl -u 'username:password' -X POST --header 'Content-
Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/delete/integration/amazon/secu
rityhub/{123456}/vm'
```

where, 123456 is the unique integration identifier (id) of the Amazon Security Hub

JSON output:

```
{
  "ServiceResponse":{
    "data":[
      "AWS accounts successfully deleted from AWS security hub
integration."
    ],
    "responseCode":"SUCCESS",
    "count":2
  }
}
```

Sample 3: Delete the regions associated with the Amazon Security Hub

API request:

```
curl -u 'username:password' -X POST --header 'Content-
Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/delete/integration/amazon/secu
rityhub/{123456}/vm/regions --data '@integration.json'
```

where, 123456 is the unique integration identifier (id) of the Amazon Security Hub

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

Request POST Data (integration.json):

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

JSON output:

```
{
  "ServiceResponse" : {
    "count":1,
    "responseCode":"SUCCESS",
    "data" : [ "Regions successfully deleted from AWS accounts in AWS
security hub integration." ],
  }
}
```