



Qualys Cloud Platform v3.x

API Release Notes

Version 3.16

August 24, 2023

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

[AM API: Added Support for TagSet Feature](#)

[CA API: Added Support for Agent Passive Sensor](#)

[CA API: Configure VM and PC Scan Interval Settings and Scan on Startup with API](#)

[CA API: Added Support for Software Composition Analysis \(SwCA\) Module for Native Agents](#)

[WAS API: New Field in Scan API Response](#)

[WAS API: New API for OWASP ZAP Findings](#)

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.

Qualys Cloud Platform 3.16 brings you API improvement and update!

[Issue Addressed](#)

AM API: Added Support for TagSet Feature

API affected	/qps/rest/2.0/create/am/tag/ /qps/rest/2.0/update/am/tag/<id>
New or Updated APIs	Updated
Operator	POST
DTD or XSD changes	Yes

With this release, we have updated the Create Tags API for TagSet feature introduced in CSAM.

Prerequisite:

Full or Trial CSAM subscription

Permissions:

Managers with full scope and other users will have the following permissions:-

- API Access
- Create User Tag
- Modify Dynamic Tag Rules

Sample - Create TagSet with ruleText

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --  
data-binary @-  
"qualys_base_url/qps/rest/2.0/create/am/tag/" < file.xml
```

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

Request POST data:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<ServiceRequest>  
  <data>  
    <Tag>  
      <name>public-tagset-05</name>  
      <ruleType>TAG_SET</ruleType>  
      <ruleText><?xml version="1.0" encoding="UTF-8"  
standalone="yes"?>  
<TAG_SET_TAG>  
  <INCLUDE_TAG>  
    <TAG_LIST>  
      <Tag>
```

```
        <PARENT>18890412</PARENT>
        <CHILD></CHILD>
    </Tag>
    <Tag>
        <PARENT>18890012</PARENT>
        <CHILD></CHILD>
    </Tag>
</TAG_LIST>
<SCOPE>ANY</SCOPE>
</INCLUDE_TAG>
<EXCLUDE_TAG>
    <TAG_LIST/>
    <SCOPE>ANY</SCOPE>
</EXCLUDE_TAG>
</TAG_SET_TAG>
</ruleText>
</Tag>
</data>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/tag.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <Tag>
            <id>25681812</id>
            <name>public-tagset-05</name>
            <parentTagId>25640613</parentTagId>
            <created>2023-06-19T19:59:07Z</created>
            <modified>2023-06-19T19:59:29Z</modified>
            <ruleText>
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TAG_SET_TAG>
    <INCLUDE_TAG>
        <TAG_LIST>
            <Tag>
                <PARENT>24571221</PARENT>
                <CHILD>24571222</CHILD>
            </Tag>
            <Tag>
                <PARENT>23828415</PARENT>
                <CHILD>23769612</CHILD>
            </Tag>
        </TAG_LIST>
    <SCOPE>ANY</SCOPE>
```

```
<INCLUDE_TAG>
<EXCLUDE_TAG>
  <TAG_LIST>
    <Tag>
      <PARENT>21536012</PARENT>
      <CHILD></CHILD>
    </Tag>
    <Tag>
      <PARENT>23191819</PARENT>
      <CHILD></CHILD>
    </Tag>
  </TAG_LIST>
  <SCOPE>ANY</SCOPE>
</EXCLUDE_TAG>
</TAG_SET_TAG>
</ruleText>
</Tag>
</data>
</ServiceResponse>
```

Sample - Update TagSet with ruleText

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --
data-binary @-
"qualys_base_url/qps/rest/2.0/update/am/tag/25681813"
< file.xml>
```

Request Post Data:

```
<ServiceRequest>
  <data>
    <Tag>
      <ruleType>TAG_SET</ruleType>
      <ruleText><?xml version="1.0" encoding="UTF-8" standalone="yes"?>
      <TAG_SET_TAG>
        <INCLUDE_TAG>
          <TAG_LIST>
            <Tag>
              <PARENT>18890412</PARENT>
              <CHILD></CHILD>
            </Tag>
            <Tag>
              <PARENT>18890012</PARENT>
              <CHILD></CHILD>
            </Tag>
          </TAG_LIST>
          <SCOPE>ANY</SCOPE>
```

```
</INCLUDE_TAG>
<EXCLUDE_TAG>
  <TAG_LIST/>
  <SCOPE>ANY</SCOPE>
</EXCLUDE_TAG>
</TAG_SET_TAG>
</ruleText>
</Tag>
</data>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/tag.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Tag>
      <id>25681813</id>
    </Tag>
  </data>
</ServiceResponse>
```

Updated XSD

```
<schema xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://am.oxm.api.portal.qualys.com/v2"
targetNamespace="http://am.oxm.api.portal.qualys.com/v2"
elementFormDefault="qualified">
  <complexType name="TagSimple">
    <sequence>
      <element name="id" type="long"/>
      <element name="name" type="string"/>
    </sequence>
  </complexType>
  <simpleType name="TagRuleType">
    <restriction base="string">
      <enumeration value="STATIC"/>
      <enumeration value="GROOVY"/>
      <enumeration value="OS_REGEX"/>
      <enumeration value="NETWORK_RANGE"/>
      <enumeration value="NETWORK_RANGE_ENHANCED"/>
      <enumeration value="NAME_CONTAINS"/>
      <enumeration value="INSTALLED_SOFTWARE"/>
      <enumeration value="OPEN_PORTS"/>
      <enumeration value="VULN_EXIST"/>
    </restriction>
  </simpleType>
</schema>
```

```
<enumeration value="ASSET_SEARCH"/>
<enumeration value="CLOUD_ASSET"/>
<enumeration value="BUSINESS_INFORMATION"/>
<enumeration value="GLOBAL_ASSET_VIEW"/>
<enumeration value="TAG_SET"/>
</restriction>
</simpleType>
...
</complexContent>
</complexType>
</schema>
```

CA API: Added Support for Agent Passive Sensor

API affected	<pre> /qps/rest/2.0/activate/am/asset/<id>?module=<value1> /qps/rest/2.0/activate/am//asset?module=<value1>,<value2> /qps/rest/2.0/deactivate/am/asset/<id>?module=<value1> /qps/rest/2.0/deactivate/am/asset?module=<value1>,<value2> /qps/rest/1.0/create/ca/agentactkey/<id> /qps/rest/1.0/update/ca/agentactkey/<id> </pre>
New or Updated APIs	Updated
Operator	POST
DTD or XSD changes	No

With this release, we have added support for Qualys Cloud Agent to work as a passive sensor to identify traffic in the subnet agent. To enable this ability, you can activate the Cloud Agent as Passive Sensor on single or multiple assets. You can also activate the Cloud Agent as Passive Sensor (CAPS) module while creating or updating the activation key.

The CAPS module is applicable only for Windows platform.

Note: This feature will be available only when the Windows agent binary with agent as passive sensor support will be available. For supported agent versions, refer to the Features by Agent Version section in the [Cloud Agent Platform Availability Matrix](#).

Sample - Activate a Single Agent

API request:

```

curl -u fo_username:password -X POST -H "Content-Type: text/xml" -H
"X-Requested-With: curl" --data-binary @single_activation.xml
"qualys_base_url/qps/rest/2.0/activate/am/asset/23058587?module=AGENT_CAP
S"

```

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

Contents of single_activation.xml:

```

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

```

Response:

```

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>

```

```
<Asset>
<id>23058587</id>
<name>DESKTOP</name>
<created>2023-03-31T12:29:40Z</created>
<modified>2023-06-20T09:46:35Z</modified>
<type>HOST</type>
<tags>
  <list>
    <TagSimple>
      <id>16xxxx14</id>
      <name>Cloud Agent</name>
    </TagSimple>
  </list>
</tags>
</Asset>
</data>
</ServiceResponse>
```

Sample - Activate Agents in Bulk

API request

```
curl -u fo_username:password -X POST -H "Content-Type: text/xml" -H
"Cache-Control: no-cache" --data-binary @activate_all_agents.xml
"qualys_base_url/qps/rest/2.0/activate/am/asset?module=AG
ENT_CAPS,AGENT_VM"
```

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

Contents of activate_all_agents.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">Cloud Agent</Criteria>
  </filters>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>2</count>
  <data>
    <Asset>
      <id>23058587</id>
      <name>DESKTOP-JJM2V3O.WORKGROUP</name>
      <created>2023-03-31T12:29:40Z</created>
```



```
<modified>2023-06-20T10:01:17Z</modified>
<type>HOST</type>
<tags>
  <list>
    <TagSimple>
      <id>25xxx12</id>
      <name>T1</name>
    </TagSimple>
    <TagSimple>
      <id>16xxxx14</id>
      <name>Cloud Agent</name>
    </TagSimple>
  </list>
</tags>
</Asset>
<Asset>
  <id>23xxx88</id>
  <name>qualys-virtual-machine</name>
  <created>2023-03-31T12:39:04Z</created>
  <modified>2023-06-20T10:00:52Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>16xxx814</id>
        <name>Cloud Agent</name>
      </TagSimple>
      <TagSimple>
        <id>24xxx448</id>
        <name>ST_1</name>
      </TagSimple>
    </list>
  </tags>
</Asset>
</data>
</ServiceResponse>
```

Sample - Deactivate Single Agent

API Request

```
curl -u fo_username:password -X POST -H "Content-Type: text/xml" --
data-binary @single_deactivation.xml
"qualys_base_url/qps/rest/2.0/deactivate/am/asset/23058587?module=AGENT_C
APS"
```

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

Contents of single_deactivation.xml

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

Response

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse  
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
  <data>  
    <Asset>  
      <id>13058587</id>  
      <name>DESKTOP-JJM2V30.WORKGROUPO</name>  
      <created>2023-03-31T12:29:40Z</created>  
      <modified>2023-06-23T13:22:04Z</modified>  
      <type>HOST</type>  
      <tags>  
        <list>  
          <TagSimple>  
            <id>253xxx12</id>  
            <name>T1</name>  
          </TagSimple>  
          <TagSimple>  
            <id>16xxx14</id>  
            <name>Cloud Agent</name>  
          </TagSimple>  
        </list>  
      </tags>  
    </Asset>  
  </data>  
</ServiceResponse>
```

Sample - Deactivate Agents in Bulk

API Request

```
curl -u fo_username:password -X POST -H "Content-Type: text/xml" -H  
"Cache-Control: no-cache" --data-binary @deactivate_all_agents.xml  
"qualys_base_url/qps/rest/2.0/deactivate/am/asset?module=  
AGENT_CAPS,AGENT_FIM"
```

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

Contents of deactivate_all_agents.xml

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

```
<Criteria field="tagName" operator="EQUALS">Cloud
Agent</Criteria>
</filters>
</ServiceRequest>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">
<responseCode>SUCCESS</responseCode>
<count>3</count>
<data>
<Asset>
  <id>23058587</id>
  <name>DESKTOP-JJM2V30.WORKGROUPO</name>
  <created>2023-03-31T12:29:40Z</created>
  <modified>2023-06-23T15:37:16Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>253xxx2</id>
        <name>T1</name>
      </TagSimple>
      <TagSimple>
        <id>163xxx14</id>
        <name>Cloud Agent</name>
      </TagSimple>
    </list>
  </tags>
</Asset>
<Asset>
  <id>23058588</id>
  <name>qualys-virtual-machine</name>
  <created>2023-03-31T12:39:04Z</created>
  <modified>2023-06-23T16:04:10Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>163xxx4</id>
        <name>Cloud Agent</name>
      </TagSimple>
      <TagSimple>
        <id>253xxx12</id>
        <name>T1</name>
      </TagSimple>
    </list>
  </tags>
</Asset>
```

```
<TagSimple>
  <id>249xxx48</id>
  <name>ST_1</name>
</TagSimple>
</list>
</tags>
</Asset>
<Asset>
  <id>28712945</id>
  <name>CAUIK_windows_1xxxxx62_48</name>
  <created>2023-05-26T12:16:20Z</created>
  <modified>2023-06-23T17:13:43Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>16xxx814</id>
        <name>Cloud Agent</name>
      </TagSimple>
      <TagSimple>
        <id>25xxx12</id>
        <name>T1</name>
      </TagSimple>
    </list>
  </tags>
  <sourceInfo>
    <list>
      <Ec2AssetSourceSimple>
        <assetId>28xxxx5</assetId>
        <type>EC_2</type>
        <firstDiscovered>2023-05-26T12:16:20Z</firstDiscovered>
        <lastUpdated>2023-05-26T13:04:23Z</lastUpdated>
        <instanceId>i-12xxx52x281</instanceId>
        <instanceState>RUNNING</instanceState>
        <spotInstance>>false</spotInstance>
        <region>region_name</region>
        <zone>Classic</zone>
        <monitoringEnabled>>false</monitoringEnabled>
      </Ec2AssetSourceSimple>
    </list>
  </sourceInfo>
</Asset>
</data>
</ServiceResponse>
```

Sample - Create Activation Key

API request

```
curl -X POST -H "Content-Type: text/xml" -H "X-Requested-With: curl" -  
H "Authorization: Basic AbcdAbcdAbcdAbcdAbcd" -H "Cxml" -H "CacheControl:  
no-cache" --data-binary @key_create.xml  
"qualys_base_url/qps/rest/1.0/create/ca/agentactkey/"
```

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

Contents of key_create.xml

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceRequest>  
  <data>  
    <AgentActKey>  
      <title>ActKeyTest</title>  
      <countPurchased>0</countPurchased>  
      <expireDate>2024-12-05T23:05:42Z</expireDate>  
      <type>UNLIMITED</type>  
      <modules>  
        <list>  
          <ActivationKeyModule>  
            <license>VM_LICENSE</license>  
          </ActivationKeyModule>  
          <ActivationKeyModule>  
            <license>CAPS</license>  
          </ActivationKeyModule>  
        </list>  
      </modules>  
      <tags>  
        <list>  
          <Tag>  
            <id>119295614</id>  
            <name>Test_P04</name>  
          </Tag>  
        </list>  
      </tags>  
    </AgentActKey>  
  </data>  
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/1.0/ca/agentactkey  
.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
  <data>  
    <AgentActKey>
```

```
<id>9790601</id>
<activationKey>8xxx7d-exxx-xxxx-9xxb-07xxxxxx7</activationKey>
<status>ACTIVE</status>
<countPurchased>0</countPurchased>
<countUsed>0</countUsed>
<datePurchased>2023-06-20T09:57:19Z</datePurchased>
<type>UNLIMITED</type>
<title>ActKeyTest</title>
<networkId>0</networkId>
<isDisabled>>false</isDisabled>
<applyOnAgents>>false</applyOnAgents>
<modules>
  <list>
    <ActivationKeyModule>
      <license>VM_LICENSE</license>
    </ActivationKeyModule>
    <ActivationKeyModule>
      <license>CAPS</license>
    </ActivationKeyModule>
  </list>
</modules>
<suspendSelfPatch>>false</suspendSelfPatch>
</AgentActKey>
</data>
</ServiceResponse>
```

Sample - Update Activation Key

API request

```
curl -X POST -H "X-Requested-With: curl" -H "Authorization: Basic
AbcdAbcdAbcdAbcdAbcd" -H "Content-Type: text/xml" -H "Cache-Control:
no-cache" --data-binary @key_update.xml
"qualys_base_url/qps/rest/1.0/update/ca/agentactkey/<id>"
```

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

Contents of key_update.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
  <data>
    <AgentActKey>
      <id>9790601</id>
      <title>ActKeyTest</title>
      <countPurchased>0</countPurchased>
      <expireDate>2022-12-05T23:05:42Z</expireDate>
      <type>UNLIMITED</type>
      <modules>
        <list>
```

```
<ActivationKeyModule>
  <license>VM_LICENSE</license>
</ActivationKeyModule>
<ActivationKeyModule>
  <license>SWCA</license>
</ActivationKeyModule>
<ActivationKeyModule>
  <b>license</b><b>CAPS</b></license>
</ActivationKeyModule>
</list>
</modules>
<tags>
  <list>
    <Tag>
      <id>8054401</id>
      <name>Temp Tag</name>
    </Tag>
  </list>
</tags>
</AgentActKey>
</data>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/1.0/ca/agentactkey
.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AgentActKey>
      <id>9790601</id>
      <activationKey>8c510e7d-ec54-4f18-9f5b-
076d8a3fc207</activationKey>
      <status>ACTIVE</status>
      <countPurchased>0</countPurchased>
      <countUsed>0</countUsed>
      <datePurchased>2023-06-20T09:57:19Z</datePurchased>
      <type>UNLIMITED</type>
      <title>ActKeyTest</title>
      <networkId>0</networkId>
      <isDisabled>>false</isDisabled>
      <applyOnAgents>>false</applyOnAgents>
      <modules>
        <list>
          <ActivationKeyModule>
            <license>VM_LICENSE</license>
```

```
    </ActivationKeyModule>  
    <ActivationKeyModule>  
      <license>SWCA</license>  
    </ActivationKeyModule>  
    <ActivationKeyModule>  
      <b>license>CAPS</b>  
    </ActivationKeyModule>  
  </list>  
</modules>  
<suspendSelfPatch>>false</suspendSelfPatch>  
</AgentActKey>  
</data>  
</ServiceResponse>
```


CA API: Configure VM and PC Scan Interval Settings and Scan on Startup with API

API affected	/qps/rest/1.0/create/ca/agentconfig/ /qps/rest/1.0/update/ca/agentconfig/
New or Updated APIs	Updated
Operator	POST
DTD or XSD changes	Yes

With this release, you can configure scan interval settings for VM and PC scans in the configuration profile for the associated assets using APIs.

Input Parameters for VM Scan

Parameter	Mandatory/ Optional	Format	Description
dataCollectionInterval	Optional	Integer	Time lapse, in minutes, between completion of the previous scan and start of the next scan for the assets associated with this configuration profile. Range: 240-43200
scanDelay	Optional	Integer	Time added, in minutes, at the start of scanning for new installs and interval scanning. Range: 0-720 Value 0 (zero) means no delay added.
scanRandomize	Optional	Integer	Range of randomization, in minutes, added to Scan Delay to offset scanning. Range: 0-720
scanOnStartup	Optional	Boolean	Set this flag to define whether the agent runs the vulnerability scans automatically when the agent service starts. - If set to <code>true</code> , the agent to starts vulnerability scan automatically when agent service start. - If set to <code>false</code> , the agent does not start vulnerability scan automatically when the agent service starts. Note: Scan on startup functionality is supported only for Qualys Agent for Windows 5.1 or later.

Input Parameters for PC Scan

Parameter	Mandatory/ Optional	Format	Description
dataCollectionInterval	Optional	Integer	Time lapse, in minutes, between completion of the previous scan and start of the next scan for the assets associated with this configuration profile. Range: 240-43200
scanDelay	Optional	Integer	Time added, in minutes, at the start of scanning for new installs and interval scanning. Range: 0-720 Value 0 (zero) means no delay added.
scanRandomize	Optional	Integer	Range of randomization, in minutes, added to Scan Delay to offset scanning. Range: 0-720

Note: The parameters for VM and PC scan intervals are optional. However, if you have used the parameters while creating a configuration profiles in API, the parameters with the valid range must be used in API for updating the same configuration profile.

Sample - Create Configuration Profile

API request:

```
curl -X POST -H "Content-Type: text/xml" -H "Authorization: Basic
AbcdAbcdAbcdAbcdAbcd" -H "Xurl" -H "Cache-Control: no-cache" --databinary
@config_create.xml
"qualys_base_url/qps/rest/1.0/create/ca/agentconfig/"
```

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

Contents of config_create.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
<data>
  <AgentConfig>
    <name>Config profile created using api</name>
    <description>done using api</description>
    <priority></priority>
    <isDefault>0</isDefault>
    <suspendScanning>>false</suspendScanning>
    <tags>
      <includeTags>
        <list>
          <ConfigTag>
            <id>6xxxx18</id>
```

```

        <name>Tag1</name>
      </ConfigTag>
    </list>
  </includeTags>
  <includeResolution>ANY</includeResolution>
  <excludeTags></excludeTags>
  <excludeResolution>ANY</excludeResolution>
</tags>
<blackoutConfig>
  <settings>
    <list>
      <BlackoutConfig>
        <startHour>10</startHour>
        <endHour>16</endHour>
        <monday>0</monday>
        <tuesday>0</tuesday>
        <wednesday>1</wednesday>
        <thursday>0</thursday>
        <friday>0</friday>
        <saturday>0</saturday>
        <sunday>0</sunday>
      </BlackoutConfig>
    </list>
  </settings>
</blackoutConfig>
<performanceProfile>
  <settings>
    <list>
      <PerformanceLevelSettings>
        <key>INTERVAL_EVENT_PROVISION</key>
        <value>60</value>
      </PerformanceLevelSettings>
      <PerformanceLevelSettings>
        <key>INTERVAL_EVENT_UPLOAD_CHANGEList</key>
        <value>60</value>
      </PerformanceLevelSettings>
      <PerformanceLevelSettings>
        <key>FILE_UPLOAD_FRAGMENT_SIZE_IN_KB</key>
        <value>666</value>
      </PerformanceLevelSettings>
      <PerformanceLevelSettings>
        <key>AGENT_LOGGING_LEVEL</key>
        <value>Verbose</value>
      </PerformanceLevelSettings>
      <PerformanceLevelSettings>
        <key>CPU_LIMIT</key>
        <value>20</value>
      </PerformanceLevelSettings>
    </list>
  </settings>
</performanceProfile>

```

```

    <key>THROTTLE_EVENT_COMM_DOWNLOAD</key>
    <value>100</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_DOWNLOAD_MANIFEST</key>
    <value>200</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>THROTTLE_EVENT_SCAN</key>
    <value>0</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>FILE_DOWNLOAD_FRAGMENT_SIZE_IN_KB</key>
    <value>1024</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_DOWNLOAD_SELF_PATCH</key>
    <value>900</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_EXECUTE_SETUP</key>
    <value>32400</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_DOWNLOAD_SNAPSHOT</key>
    <value>66</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>THROTTLE_EVENT_COMM_UPLOAD</key>
    <value>0</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_STATUS</key>
    <value>1000</value>
  </PerformanceLevelSettings>
  <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_CONFIG</key>
    <value>66</value>
  </PerformanceLevelSettings>
</list>
</settings>
</performanceProfile>
<vmScanInterval>
  <dataCollectionInterval>350</dataCollectionInterval>
  <scanDelay>220</scanDelay>
  <scanRandomize>330</scanRandomize>
  <scanOnStartup>true</scanOnStartup>
</vmScanInterval>
<pcScanInterval>

```

```

        <dataCollectionInterval>251</dataCollectionInterval>
        <scanDelay>10</scanDelay>
        <scanRandomize>79</scanRandomize>
    </pcScanInterval>
    <securitySetting>
        <vmScanMode>DPE</vmScanMode>
    </securitySetting>
</AgentConfig>
</data>
</ServiceRequest>

```

Response:

```

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/1.0/ca/agentconfig
.xsd">
<responseCode>SUCCESS</responseCode>
<count>1</count>
<data>
    <AgentConfig>
        <id>1522405</id>
        <name>Config profile created using api</name>
        <isDefault>0</isDefault>
        <createdDate>2023-05-14T15:31:42Z</createdDate>
        <createdBy>John Doe (john_doe)</createdBy>
        <description>done using api</description>
        <tags>
            <includeTags/>
            <includeResolution>ANY</includeResolution>
            <excludeTags/>
            <tagSetUuid>xxxabc-xx01-xxxb-axxx2-123123</tagSetUuid>
        </tags>
        <suspendScanning>false</suspendScanning>
        <preventAgentUpdate>false</preventAgentUpdate>
        <totalAgents>0</totalAgents>
        <inMemoryDbEnabled>false</inMemoryDbEnabled>
        <qgsEnabled>false</qgsEnabled>
        <blackoutConfig>
            <settings>
                <list>
                    <BlackoutConfig>
                        <startHour>10</startHour>
                        <endHour>16</endHour>
                        <monday>0</monday>
                        <tuesday>0</tuesday>
                        <wednesday>1</wednesday>
                        <thursday>0</thursday>

```

```

        <friday>0</friday>
        <saturday>0</saturday>
        <sunday>0</sunday>
    </BlackoutConfig>
</list>
</settings>
</blackoutConfig>
<performanceProfile>
    <settings>
        <list>
            <PerformanceLevelSettings>
                <key>INTERVAL_EVENT_PROVISION</key>
                <value>60</value>
            </PerformanceLevelSettings>
            ...
            <PerformanceLevelSettings>
                <key>INTERVAL_EVENT_CONFIG</key>
                <value>66</value>
            </PerformanceLevelSettings>
        </list>
    </settings>
</performanceProfile>
<securitySetting>
    <vmScanMode>DPE</vmScanMode>
</securitySetting>
<vmScanInterval>
    <dataCollectionInterval>350</dataCollectionInterval>
    <scanDelay>220</scanDelay>
    <scanRandomize>330</scanRandomize>
    <scanOnStartup>true</scanOnStartup>
</vmScanInterval>
<pcScanInterval>
    <dataCollectionInterval>251</dataCollectionInterval>
    <scanDelay>10</scanDelay>
    <scanRandomize>79</scanRandomize>
</pcScanInterval>
</AgentConfig>
</data>
</ServiceResponse>

```

Sample - Update Configuration Profile

API request:

```

curl -X POST -H "Content-Type: text/xml" -H "Authorization: Basic
AbcdAbcdAbcdAbcdAbcd" -H "X-Requested-With: curl" -H "Cache-Control:
no-cache" --data-binary @config_update.xml
"qualys_base_url/qps/rest/1.0/update/ca/agentconfig/"

```

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

Contents of config_update.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
<data>
  <AgentConfig>
    <id>1522403</id>
    <name>Config profile created using api</name>
    <description>updated using api</description>
    <priority>2</priority>
    <isDefault>0</isDefault>
    <suspendScanning>>false</suspendScanning>
    <tags>
      <includeTags>
        <list>
          <ConfigTag>
            <id>2xxx26</id>
            <name>TEMP tag</name>
          </ConfigTag>
        </list>
      </includeTags>
      <includeResolution>ANY</includeResolution>
      <excludeTags>
        <list/>
      </excludeTags>
      <excludeResolution>ANY</excludeResolution>
      <tagSetUuid>xxxxx2ce-xxx8-4xxx-xxxxxx90f2xxxx87</tagSetUuid>
    </tags>
  <blackoutConfig>
    <settings>
      <list/>
    </settings>
  </blackoutConfig>
  <performanceProfile>
    <settings>
      <list>
        <PerformanceLevelSettings>
          <key>INTERVAL_EVENT_PROVISION</key>
          <value>3600</value>
        </PerformanceLevelSettings>
        <PerformanceLevelSettings>
          <key>INTERVAL_EVENT_UPLOAD_CHANGEList</key>
          <value>5</value>
        </PerformanceLevelSettings>
        <PerformanceLevelSettings>
          <key>FILE_UPLOAD_FRAGMENT_SIZE_IN_KB</key>
          <value>1024</value>
        </PerformanceLevelSettings>
      </list>
    </settings>
  </performanceProfile>
</data>
</ServiceRequest>
```

```

</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>AGENT_LOGGING_LEVEL</key>
<value>Verbose</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>THROTTLE_EVENT_COMM_DOWNLOAD</key>
<value>20</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>INTERVAL_EVENT_DOWNLOAD_MANIFEST</key>
<value>10800</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>THROTTLE_EVENT_SCAN</key>
<value>20</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>FILE_DOWNLOAD_FRAGMENT_SIZE_IN_KB</key>
<value>1024</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>INTERVAL_EVENT_DOWNLOAD_SELF_PATCH</key>
<value>10800</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>INTERVAL_EVENT_EXECUTE_SETUP</key>
<value>32400</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>INTERVAL_EVENT_DOWNLOAD_SNAPSHOT</key>
<value>300</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>THROTTLE_EVENT_COMM_UPLOAD</key>
<value>20</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>INTERVAL_EVENT_STATUS</key>
<value>1000</value>
</PerformanceLevelSettings>
<PerformanceLevelSettings>
<key>INTERVAL_EVENT_CONFIG</key>
<value>10800</value>
</PerformanceLevelSettings>
</list>
</settings>
</performanceProfile>
<vmScanInterval>

```



```

        <dataCollectionInterval>500</dataCollectionInterval>
        <scanDelay>510</scanDelay>
        <scanRandomize>410</scanRandomize>
        <scanOnStartup>>false</scanOnStartup>
    </vmScanInterval>
    <pcScanInterval>
        <dataCollectionInterval>851</dataCollectionInterval>
        <scanDelay>500</scanDelay>
        <scanRandomize>500</scanRandomize>
    </pcScanInterval>
</AgentConfig>
</data>
</ServiceRequest>

```

Response:

```

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/1.0/ca/agentconfig
.xsd">
<responseCode>SUCCESS</responseCode>
<count>1</count>
<data>
    <AgentConfig>
        <id>1522403</id>
        <name>Config profile created using api</name>
        <isDefault>0</isDefault>
        <createdDate>2023-05-14T14:22:00Z</createdDate>
        <createdBy>John Doe (john_doe)</createdBy>
        <description>updated using api</description>
        <tags>
            <includeTags/>
            <includeResolution>ANY</includeResolution>
            <excludeTags/>
            <tagSetUuid>xxxxx173-2xxx-4f7a-bxxx7-dxxxxx8xx9</tagSetUuid>
        </tags>
        <suspendScanning>>false</suspendScanning>
        <preventAgentUpdate>>false</preventAgentUpdate>
        <priority>
            <priority>2</priority>
        </priority>
        <totalAgents>0</totalAgents>
        <inMemoryDbEnabled>>false</inMemoryDbEnabled>
        <qgsEnabled>>false</qgsEnabled>
        <blackoutConfig/>
        <performanceProfile>
            <settings>
                <list>

```

```

    <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_PROVISION</key>
    <value>3600</value>
    </PerformanceLevelSettings>
    ...
    <PerformanceLevelSettings>
    <key>INTERVAL_EVENT_CONFIG</key>
    <value>10800</value>
    </PerformanceLevelSettings>
  </list>
</settings>
</performanceProfile>
<securitySetting>
  <vmScanMode>AGENTUSER</vmScanMode>
</securitySetting>
<vmScanInterval>
  <dataCollectionInterval>500</dataCollectionInterval>
  <scanDelay>510</scanDelay>
  <scanRandomize>410</scanRandomize>
  <scanOnStartup>>false</scanOnStartup>
</vmScanInterval>
<pcScanInterval>
  <dataCollectionInterval>851</dataCollectionInterval>
  <scanDelay>500</scanDelay>
  <scanRandomize>500</scanRandomize>
</pcScanInterval>
</AgentConfig>
</data>
</ServiceResponse>

```

Updated XSD

XSD: <platform API server>/qps/xsd/1.0/ca/agentconfig.xsd

```

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

<schema xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://ca.oxm.api.portal.qualys.com/v1"
  elementFormDefault="qualified"
  xmlns:QG="http://ca.oxm.api.portal.qualys.com/v1"
  xmlns:jaxb="http://java.sun.com/xml/ns/jaxb"
  xmlns:xjc="http://java.sun.com/xml/ns/jaxb/xjc"
  jaxb:extensionBindingPrefixes="xjc"
  jaxb:version="2.1"
  xmlns:qcommon="http://oxm.api.portal.qualys.com/common" >

  <import namespace="http://oxm.api.portal.qualys.com/common"
  schemaLocation="http://oxm.api.portal.qualys.com/common/qualys_common.xsd"
  "/>

```

```

<include schemaLocation="configpriority.xsd"/>
<include schemaLocation="performanceprofile.xsd"/>
<include schemaLocation="agentblackoutconfig.xsd"/>
<include schemaLocation="tagset.xsd" />
<include schemaLocation="agentSecuritySetting.xsd" />
<b><include schemaLocation="vmscanintervalsetting.xsd" /></b>
<b><include schemaLocation="pcscanintervalsetting.xsd" /></b>

<!-- DATA -->
<complexType name="AgentConfig">
  <sequence>
    <element name="id" type="long" minOccurs="1"/>
    <element name="uuid" type="string" minOccurs="1"/>
    <element name="name" type="string" minOccurs="1"/>
    <element name="isDefault" type="int" minOccurs="1"/>
    <element name="created_date" type="dateTime" minOccurs="1"/>
    <element name="created_by" type="string" minOccurs="1"/>
    <element name="description" type="string" minOccurs="1"/>
    <element name="tags" type="QG:tagset" minOccurs="1"/>
    <element name="suspendScanning" type="boolean" minOccurs="1"/>
    <element name="preventAgentUpdate" type="boolean"
minOccurs="1"/>
    <element name="priority" type="QG:ConfigPriority"
minOccurs="1"/>
    <element name="totalAgents" type="long" minOccurs="1"/>
    <element name="inMemoryDbEnabled" type="boolean"
minOccurs="1"/>
    <element name="qgsEnabled" type="boolean" minOccurs="0"/>
    <element name="qgsGroupName" type="string" minOccurs="0"/>
    <element name="blackoutConfig" type="QG:AgentBlackoutConfig"
minOccurs="0" />
    <element name="performanceProfile"
type="QG:AgentPerformanceProfile" minOccurs="1"/>
    <element name="securitySetting" type="QG:SecuritySetting"
minOccurs="1"/>
    <b><element name="vmScanInterval" type="QG:VmScanIntervalConfig"
minOccurs="1"/></b>
    <b><element name="pcScanInterval" type="QG:PcScanIntervalConfig"
minOccurs="1"/></b>
  </sequence>
</complexType>
</schema>

```

CA API: Added Support for Software Composition Analysis (SwCA) Module for Native Agents

API affected	/qps/rest/2.0/activate/am/asset/<id>?module=<value1> /qps/rest/2.0/activate/am//asset?module=<value1>,<value2> /qps/rest/2.0/deactivate/am/asset/<id>?module=<value1> /qps/rest/2.0/deactivate/am/asset?module=<value1>,<value2> /qps/rest/1.0/create/ca/agentactkey/ /qps/rest/1.0/update/ca/agentactkey/<id>
New or Updated APIs	Updated
Operator	POST
DTD or XSD changes	No

With this release, we have added support for to activate Software Composition Analysis (SwCA) on for Windows and Linux native agents. To enable this ability, you can activate the SwCA module on single or multiple assets. You can also activate the SwCA module while creating or updating the activation key.

SwCA is supported only for Windows and Linux Platform and can be activated only when VM is activated for the agent.

Note: This feature will be available only when the Windows and Linux agent binaries with SwCA scan support will be available. For supported agent versions, refer to the Features by Agent Version section in the [Cloud Agent Platform Availability Matrix](#).

Sample - Activate a Single Agent

API request:

```
curl -u fo_username:password -X POST -H "Content-Type: text/xml" -H
  "X-Requested-With: curl" --data-binary @single_activation.xml
  "qualys_base_url/qps/rest/2.0/activate/am/asset/23058587?module=AGENT_Sw
  CA"
```

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

Contents of single_activation.xml:

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

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">
```

```

<responseCode>SUCCESS</responseCode>
<count>1</count>
<data>
  <Asset>
    <id>23058587</id>
    <name>DESKTOP</name>
    <created>2023-03-31T12:29:40Z</created>
    <modified>2023-06-15T10:11:55Z</modified>
    <type>HOST</type>
    <tags>
      <list>
        <TagSimple>
          <id>21111650</id>
          <name>Tag Tag</name>
        </TagSimple>
        <TagSimple>
          <id>11111814</id>
          <name>Cloud Agent</name>
        </TagSimple>
      </list>
    </tags>
  </Asset>
</data>
</ServiceResponse>

```

Sample - Activate Agents in Bulk

API request:

```

curl -u fo_username:password -X POST -H "Content-Type: text/xml" -H
"Cache-Control: no-cache" --data-binary @activate_all_agents.xml
"qualys_base_url/qps/rest/2.0/activate/am/asset?module=AGENT_SwCA,AGENT_F
IM"

```

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

Contents of activate_all_agents.xml:

```

<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">Cloud Agent</Criteria>
  </filters>
</ServiceRequest>

```

Response:

```

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">

```

```

<responseCode>SUCCESS</responseCode>
<count>83</count>
<data>
  <Asset>
    <id>1xxx8xx4</id>
    <name>cent-os-instance-2xxxxx8-1xxx</name>
    <created>2022-09-15T06:56:25Z</created>
    <modified>2023-06-12T09:23:46Z</modified>
    <type>HOST</type>
    <tags>
      <list>
        <TagSimple>
          <id>11112814</id>
          <name>Cloud Agent</name>
        </TagSimple>
        <TagSimple>
          <id>11112416</id>
          <name>6APR-01</name>
        </TagSimple>
      </list>
    </tags>
    <sourceInfo>
      <list>
        <AssetSource/>
        <OciAssetSourceSimple>
          <assetId>1xxxxxx4</assetId>
          <type>OCI</type>
          <firstDiscovered>2022-09-15T06:56:25Z</firstDiscovered>
          <lastUpdated>2022-09-15T06:56:25Z</lastUpdated>
          <ociId>randomxxx</ociId>
          <state>RUNNING</state>
        </OciAssetSourceSimple>
      </list>
    </sourceInfo>
  </Asset>
  <Asset>
    <id>2xxxxxx2</id>
    <name>AWS_Connector_Agent</name>
    <created>2023-02-28T00:00:00Z</created>
    <modified>2023-06-07T12:28:33Z</modified>
    <type>HOST</type>
    <tags>
      <list>
        <TagSimple>
          <id>1xxx2xx4</id>
          <name>Cloud Agent</name>
        </TagSimple>
        <TagSimple>
          <id>2xxxxxx2</id>

```

```

        <name>TAG_UNINSTALL</name>
    </TagSimple>
</list>
</tags>
<sourceInfo>
    <list>
    <AssetSource/>
    <Ec2AssetSourceSimple>
        <assetId>2xxxxxx2</assetId>
        <type>EC_2</type>
        <firstDiscovered>2023-02-22T09:07:02Z</firstDiscovered>
        <lastUpdated>2023-03-30T05:23:53Z</lastUpdated>
        <reservationId>r-00bxxxxxxx25d25</reservationId>
        <availabilityZone>us-east-1b</availabilityZone>
        <privateDnsName>ip-10-xx-11-xxx.abc.com</privateDnsName>
        <publicDnsName>ec2-3-111-111-206.xxxx.amazonaws.com
        </publicDnsName>
        <localHostname>ip-10-11-11-224.abc.com</localHostname>
        <instanceId>i-00fxxxxxxxx8xx0</instanceId>
        <instanceType>t2.micro</instanceType>
        <createdDate>2023-02-22T08:57:59Z</createdDate>
        <instanceState>RUNNING</instanceState>
        <groupId>sg-00a25f18xxxxxaf6</groupId>
        <groupName>test_group_name1</groupName>
        <spotInstance>false</spotInstance>
        <accountId>123456789876</accountId>
        <subnetId>subnet-080234xxxxx9098e</subnetId>
        <vpcId>vpc-0ae6777xxxxxd8446</vpcId>
        <region>region_name</region>
        <zone>VPC</zone>
        <imageId>ami-0dfxxxxx50277af</imageId>
        <publicIpAddress>3.222.2xx.2xx</publicIpAddress>
        <privateIpAddress>xx.22.xx.224</privateIpAddress>
        <macAddress>xx:6e:xx:xx:xx:59</macAddress>
        <monitoringEnabled>false</monitoringEnabled>
    </Ec2AssetSourceSimple>
    </list>
</sourceInfo>
</Asset>
....
<Asset>
    <id>28712945</id>
    <name>windows_test_48</name>
    <created>2023-05-26T12:16:20Z</created>
    <modified>2023-06-08T11:13:33Z</modified>
    <type>HOST</type>
    <tags>
        <list>

```

```

    <TagSimple>
      <id>161111814</id>
      <name>Cloud Agent</name>
    </TagSimple>
    <TagSimple>
      <id>25111622</id>
      <name>DT01</name>
    </TagSimple>
  </list>
</tags>
<sourceInfo>
  <list>
    <AssetSource/>
    <Ec2AssetSourceSimple>
      <assetId>28111145</assetId>
      <type>EC_2</type>
      <firstDiscovered>2023-05-26T12:16:20Z</firstDiscovered>
      <lastUpdated>2023-05-26T13:04:23Z</lastUpdated>
      <instanceId>i-65xxxxx81</instanceId>
      <instanceState>RUNNING</instanceState>
      <spotInstance>false</spotInstance>
      <region>us-east-1</region>
      <zone>Classic</zone>
      <monitoringEnabled>false</monitoringEnabled>
    </Ec2AssetSourceSimple>
  </list>
</sourceInfo>
</Asset>
</data>
</ServiceResponse>

```

Sample - Deactivate Single Agent

API request:

```

curl -u fo_username:password -X POST -H "Content-Type: text/xml" --
data-binary @single_deactivation.xml
"qualys_base_url/qps/rest/2.0/deactivate/am/asset/29607283?module=AGENT_S
wCA"

```

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

Contents of single_deactivation.xml

```

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

```

Response:

```

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

```



```

<ServiceResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">
<responseCode>SUCCESS</responseCode>
<count>1</count>
<data>
<Asset>
  <id>29607283</id>
  <name>SwCA_Window1</name>
  <created>2023-06-21T12:28:10Z</created>
  <modified>2023-06-23T05:41:51Z</modified>
  <type>HOST</type>
  <tags>
  <list>
  <TagSimple>
    <id>25798012</id>
    <name>swcal</name>
  </TagSimple>
  <TagSimple>
    <id>16541442</id>
    <name>Cloud Agent</name>
  </TagSimple>
  <TagSimple>
    <id>25788238</id>
    <name>swca</name>
  </TagSimple>
  </list>
  </tags>
</Asset>
</data>
</ServiceResponse>

```

Sample - Deactivate Agents in Bulk

API request:

```

curl -u fo_username:password -X POST -H "Content-Type: text/xml" -H
"Cache-Control: no-cache" --data-binary @deactivate_all_agents.xml
"qualys_base_url/qps/rest/2.0/deactivate/am/asset?module=
AGENT_SwCA,AGENT_FIM"

```

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

Contents of deactivate_all_agents.xml:

```

<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
<filters>
  <Criteria field="tagName" operator="EQUALS">Cloud
Agent</Criteria>

```

```
</filters>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/2.0/am/asset.xsd">
<responseCode>SUCCESS</responseCode>
<count>5</count>
<data>
<Asset>
  <id>27525950</id>
  <name>test_windows_1684134911049_38</name>
  <created>2023-05-15T07:15:19Z</created>
  <modified>2023-06-23T09:09:19Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>25797813</id>
        <name>swca_Expired</name>
      </TagSimple>
      <TagSimple>
        <id>14034213</id>
        <name>Cloud Agent</name>
      </TagSimple>
    </list>
  </tags>
</Asset>
<Asset>
  <id>27528553</id>
  <name>test_windows_1684134911049_44</name>
  <created>2023-05-15T07:15:18Z</created>
  <modified>2023-06-23T09:09:19Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>25797813</id>
        <name>swca_Expired</name>
      </TagSimple>
      <TagSimple>
        <id>14034213</id>
        <name>Cloud Agent</name>
      </TagSimple>
    </list>
  </tags>
```

```

</Asset>
<Asset>
  <id>27528335</id>
  <name>test_windows_1684134911049_66</name>
  <created>2023-05-15T07:15:19Z</created>
  <modified>2023-06-23T09:09:19Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>14034213</id>
        <name>Cloud Agent</name>
      </TagSimple>
      <TagSimple>
        <id>25797813</id>
        <name>swca_Expired</name>
      </TagSimple>
    </list>
  </tags>
</Asset>
<Asset>
  <id>27530942</id>
  <name>test_windows_1684134911049_50</name>
  <created>2023-05-15T07:15:16Z</created>
  <modified>2023-06-23T09:08:05Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>25797813</id>
        <name>swca_Expired</name>
      </TagSimple>
      <TagSimple>
        <id>14034213</id>
        <name>Cloud Agent</name>
      </TagSimple>
    </list>
  </tags>
</Asset>
<Asset>
  <id>27520940</id>
  <name>test_windows_1684134911049_38</name>
  <created>2023-05-15T07:15:16Z</created>
  <modified>2023-06-23T09:09:18Z</modified>
  <type>HOST</type>
  <tags>
    <list>
      <TagSimple>
        <id>14034213</id>

```

```

        <name>Cloud Agent</name>
    </TagSimple>
</TagSimple>
    <id>25797813</id>
    <name>swca_Expired</name>
</TagSimple>
</list>
</tags>
</Asset>
</data>
</ServiceResponse>

```

Sample - Create Activation Key

API request:

```

curl -X POST -H "Content-Type: text/xml" -H "X-Requested-With: curl" -
H "Authorization: Basic AbcdAbcdAbcdAbcdAbcd" -H "Cxml" -H "CacheControl:
no-cache" --data-binary @key_create.xml
"qualys_base_url/qps/rest/1.0/create/ca/agentactkey/<id>"

```

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

Contents of key_create.xml:

```

<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
  <data>
    <AgentActKey>
      <title>ActivationKeyTest</title>
      <countPurchased>0</countPurchased>
      <expireDate>2024-12-05T23:05:42Z</expireDate>
      <type>UNLIMITED</type>
      <modules>
        <list>
          <ActivationKeyModule>
            <license>VM_LICENSE</license>
          </ActivationKeyModule>
          <ActivationKeyModule>
            <license>SWCA</license>
          </ActivationKeyModule>
        </list>
      </modules>
    </data>
  </ServiceRequest>
</list>
</tags>
</list>
  <Tag>
    <id>111111614</id>
    <name>Test_P04</name>
  </Tag>
</list>

```

```

    </tags>
  </AgentActKey>
</data>
</ServiceRequest>

```

Response:

```

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/1.0/ca/agentactkey
.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AgentActKey>
      <id>9711114</id>
      <activationKey>cxxxx7a-e9x-4df5-xx0d-0x5x05xx33b</activationKey>
      <status>ACTIVE</status>
      <countPurchased>0</countPurchased>
      <countUsed>0</countUsed>
      <datePurchased>2023-06-15T10:44:56Z</datePurchased>
      <type>UNLIMITED</type>
      <title>ActivationKeyTest</title>
      <networkId>0</networkId>
      <isDisabled>>false</isDisabled>
      <applyOnAgents>>false</applyOnAgents>
      <modules>
        <list>
          <ActivationKeyModule>
            <license>VM_LICENSE</license>
          </ActivationKeyModule>
          <ActivationKeyModule>
            <license>SWCA</license>
          </ActivationKeyModule>
        </list>
      </modules>
      <suspendSelfPatch>>false</suspendSelfPatch>
    </AgentActKey>
  </data>
</ServiceResponse>

```

Sample - Update Activation Key API

API request:

```

curl -X POST -H "X-Requested-With: curl" -H "Authorization: Basic
AbcdAbcdAbcdAbcdAbcd" -H "Content-Type: text/xml" -H "Cache-Control:
no-cache" --data-binary @key_update.xml
"qualys_base_url/qps/rest/1.0/update/ca/agentactkey/<id>"

```

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

Request POST data:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
  <data>
    <AgentActKey>
      <id>9765401</id>
      <title>KeyNewSwcaUpdated</title>
      <countPurchased>0</countPurchased>
      <expireDate>2022-12-05T23:05:42Z</expireDate>
      <type>UNLIMITED</type>
      <modules>
        <list>
          <ActivationKeyModule>
            <license>VM_LICENSE</license>
          </ActivationKeyModule>
          <ActivationKeyModule>
            <license>SWCA</license>
          </ActivationKeyModule>
        </list>
      </modules>
      <tags>
        <list>
          <Tag>
            <id>80111101</id>
            <name>Temp Tag</name>
          </Tag>
        </list>
      </tags>
    </AgentActKey>
  </data>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/1.0/ca/agentactkey
.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AgentActKey>
      <id>9765401</id>
      <activationKey>c3xxxxd-8759-4xx-axxx-xxxx7da9ff48</activationKey>
      <status>ACTIVE</status>
      <countPurchased>0</countPurchased>
      <countUsed>0</countUsed>
```

```
<datePurchased>2023-06-15T10:01:39Z</datePurchased>
<type>UNLIMITED</type>
<title>KeyNewSwcaUpdated</title>
<networkId>0</networkId>
<isDisabled>>false</isDisabled>
<applyOnAgents>>false</applyOnAgents>
<modules>
<list>
  <ActivationKeyModule>
    <license>VM_LICENSE</license>
  </ActivationKeyModule>
  <ActivationKeyModule>
    <license>SWCA</license>
  </ActivationKeyModule>
</list>
</modules>
<suspendSelfPatch>>false</suspendSelfPatch>
</AgentActKey>
</data>
</ServiceResponse>
```

WAS API: New Field in Scan API Response

API affected	/qps/rest/3.0/search/was/wasscan /qps/rest/3.0/status/was/wasscan/<id> /qps/rest/3.0/download/was/wasscan/<id> /qps/rest/3.0/status/was/wasscan/<id>
New or Updated APIs	Updated
DTD or XSD changes	Yes

With this release, we have added a new field in the API response—<consolidatedStatus> in the scan APIs that matches the **Status** of the scan in the **Scan List** tab in Web Application Scanning.

Sample - Search Scans in a Specific Status in the User’s Account

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
data-binary @-
"qualys_base_url/qps/rest/3.0/search/was/wasscan" <
file.xml
```

Note: “file.xml” contains the request POST data.

Request POST data

```
<ServiceRequest>
<filters>
<Criteria field="status" operator="EQUALS">RUNNING</Criteria>
</filters>
</ServiceRequest>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.0
/was/wasscan.xsd">
<responseCode>SUCCESS</responseCode>
<count>2</count>
<hasMoreRecords>>false</hasMoreRecords>
<data>
<WasScan>
<id>13101</id>
<name>
<![CDATA[Vulnerability Scan - 2017-02-24]]>
```



```
</name>
<reference>was/1298538355659.20994</reference>
<type>VULNERABILITY</type>
<mode>ONDEMAND</mode>
<profile>
<id>1072</id>
<name>
  <![CDATA[Initial WAS Options]]>
</name>
</profile>
<launchedDate>2017-02-24T10:05:55Z</launchedDate>
<launchedBy>
<id>123056</id>
<username>username</username>
<firstName>
  <![CDATA[John]]>
</firstName>
<lastName>
  <![CDATA[Smith]]>
</lastName>
</launchedBy>
<status>RUNNING</status>
</WasScan>
<WasScan>
<id>13102</id>
<name>
<![CDATA[Vulnerability Scan - 2017-02-24]]>
</name>
<reference>was/1298541157873.20995</reference>
<type>VULNERABILITY</type>
<mode>ONDEMAND</mode>
<profile>
<id>1072</id>
<name>
  <![CDATA[Initial WAS Options]]>
</name>
</profile>
<launchedDate>2017-02-24T10:52:37Z</launchedDate>
<launchedBy>
<id>123056</id>
<username>username</username>
<firstName>
  <![CDATA[John]]>
</firstName>
<lastName>
  <![CDATA[Smith]]>
</lastName>
</launchedBy>
<status>RUNNING</status>
```

```
    <consolidatedStatus>RUNNING</consolidatedStatus>
  </WasScan>
</data>
</ServiceResponse>
```

Sample - Get Details for a Scan with Specified Scan ID

API Request

```
curl -n -u "USERNAME:PASSWORD"
"qualys_base_url/qps/rest/3.0/get/was/wasscan/1447989"
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.0/was/wasscan.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <WasScan>
      <id>1447989</id>
      <name>
        <![CDATA[My Vulnerability Scan]]>
      </name>
      <reference>was/1446408743390.1856849</reference>
      <type>VULNERABILITY</type>
      <mode>ONDEMAND</mode>
      <progressiveScanning>DISABLED</progressiveScanning>
      <multi>>false</multi>
      <target>
        <webApp>
          <id>2431279</id>
          <name>
            <![CDATA[127.0.0.1]]>
          </name>
          <url>
            <![CDATA[http://127.0.0.1/]]>
          </url>
        </webApp>
        <scannerAppliance>
          <type>EXTERNAL</type>
        </scannerAppliance>
        <cancelOption>SPECIFIC</cancelOption>
      </target>
      <profile>
        <id>28147</id>
        <name>
```

```

    <![CDATA[My Option Profile]]>
  </name>
</profile>
<options>
  <count>15</count>
  <list>
    <WasScanOption>
      <name>My Authentication Record</name>
      <value>
        <![CDATA[None]]>
      </value>
    </WasScanOption>
    <WasScanOption>
      <name>Unexpected Error Threshold</name>
      <value>
        <![CDATA[48]]>
      </value>
    </WasScanOption>
    <WasScanOption>
      <name>Sensitive Content: Credit Card
Numbers</name>
      <value>
        <![CDATA[false]]>
      </value>
    </WasScanOption>
    . . .
    <WasScanOption>
      <name>Target URL</name>
      <value>
        <![CDATA[http://127.0.0.1/]]>
      </value>
    </WasScanOption>
  </list>
</options>
<launchedDate>2017-11-01T20:12:23Z</launchedDate>
<launchedBy>
  <id>2226741</id>
  <username>user_ak1</username>
  <firstName>
    <![CDATA[Amy]]>
  </firstName>
  <lastName>
    <![CDATA[Kim]]>
  </lastName>
</launchedBy>
<status>CANCELED</status>
<consolidatedStatus>CANCELED</consolidatedStatus>
<cancelMode>USER</cancelMode>
<canceledBy>

```

```
        <id>9872437571</id>
        <username>user_bb5</username>
    </canceledBy>
    <sendMail>true</sendMail>
    <sendOneMail>true</sendOneMail>
    </WasScan>
</data>
</ServiceResponse>
```

Sample - Download Results of a Scan with the Specified ID

API Request

```
curl -n -u "USERNAME:PASSWORD"
    "qualys_base_url/qps/rest/3.0/download/was/wasscan/174726"
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<WasScan xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.0/was/wasscan.xsd">
    <id>5674957</id>
    <name>
        <![CDATA[Web prog scan 2 Enable in schedule vuln Run #102]]>
    </name>
    <reference>was/1679053816084.1806719</reference>
    <type>VULNERABILITY</type>
    <mode>SCHEDULED</mode>
    <progressiveScanning>ENABLED</progressiveScanning>
    <multi>>false</multi>
    <target>
        <webApp>
            <id>18859236</id>
            <name>
                <![CDATA[Ravi Web for Progressive scan BO setting
Enable123]]>
            </name>
            <url>
                <![CDATA[http://10.xx.xx.45:8080/bodgeit/login.jsp]]>
            </url>
        </webApp>
        ...
    </target>
    <profile>
        <id>1379083</id>
        <name>
            <![CDATA[1 link OP]]>
        </name>
```

```
</profile>
<options>
  <count>16</count>
  <list>
    <WasScanOption>
      <name>Web Application Authentication Record Name</name>
      <value>
        <![CDATA[New Paramterized selenium for Auth record]]>
      </value>
    </WasScanOption>
    ...
    <WasScanOption>
      <name>Sensitive Content: Social Security Numbers
(US) </name>
      <value>
        <![CDATA[false]]>
      </value>
    </WasScanOption>
  </list>
</options>
<launchedDate>2023-03-17T11:52:10Z</launchedDate>
<launchedBy>
  <id>151899098</id>
  <username>quays_xq94</username>
  <firstName>
    <![CDATA[John]]>
  </firstName>
  <lastName>
    <![CDATA[Doe]]>
  </lastName>
</launchedBy>
<status>FINISHED</status>
<consolidatedStatus>NO_HOST_ALIVE</consolidatedStatus>
<endScanDate>2023-03-17T11:52:13Z</endScanDate>
<scanDuration>3</scanDuration>
<summary>
  <resultsStatus>NO_HOST_ALIVE</resultsStatus>
  <authStatus>NOT_USED</authStatus>
</summary>
...
</stats>
<vulns>
  <count>0</count>
</vulns>
<sensitiveContents>
  <count>0</count>
</sensitiveContents>
<igs>
  <count>0</count>
```

```
</igs>  
<sendMail>true</sendMail>  
<enableWAFAuth>false</enableWAFAuth>  
</WasScan>
```

Sample - View Status of a Scan with the Specified ID

API Request

```
curl -n -u "USERNAME:PASSWORD"  
"qualys_base_url/qps/rest/3.0/status/was/wasscan/1902350"
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse  
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.  
0/was/wasscan.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
  <data>  
    <WasScan>  
      <id>1902350</id>  
      <status>FINISHED</status>  
      <consolidatedStatus>NO_HOST_ALIVE</consolidatedStatus>  
      <summary>  
        <resultsStatus>NO_HOST_ALIVE</resultsStatus>  
        <authStatus>NONE</authStatus>  
      </summary>  
    </WasScan>  
  </data>  
</ServiceResponse>
```

Updated 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="Criteria">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="field" type="xs:string"/>
      <xs:attribute name="operator">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="CONTAINS"/>
            <xs:enumeration value="IN"/>
            <xs:enumeration value="EQUALS"/>
            <xs:enumeration value="NOT EQUALS"/>
            <xs:enumeration value="GREATER"/>
            <xs:enumeration value="LESSER"/>
            <xs:enumeration value="NONE"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="ServiceRequestPreferences">
  <xs:all>
    <xs:element name="startFromId" type="xs:long" minOccurs="0"/>
    <xs:element name="startFromOffset" type="xs:int" minOccurs="0"/>
    <xs:element name="limitResults" type="xs:int" minOccurs="0"/>
  </xs:all>
</xs:complexType>

<xs:complexType name="ServiceRequestData">
  <xs:sequence>
    <xs:element name="WasScan" type="WasScan" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

<!-- RESPONSE -->
<xs:element name="ServiceResponse">

```

```

        <xs:complexType>
          <xs:sequence>
            <xs:element name="responseCode" type="ResponseCode"/>
            <xs:element name="responseErrorDetails"
type="ResponseErrorObject" minOccurs="0"/>
            <xs:element name="count" type="xs:int" minOccurs="0"/>
            <xs:element name="hasMoreRecords" type="xs:boolean"
minOccurs="0"/>
            <xs:element name="lastId" type="xs:long" minOccurs="0"/>
            <xs:element name="data" type="ServiceResponseData"
minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      .....
      <xs:complexType name="ResponseErrorObject">
        <xs:sequence>
          <xs:element name="errorMessage" type="xs:string"/>
          <xs:element name="errorResolution" type="xs:string"
minOccurs="0"/>
          <xs:element name="internalErrorCodeId" type="xs:int"
minOccurs="0"/>
        </xs:sequence>
      </xs:complexType>

      <xs:complexType name="ServiceResponseData">
        <xs:sequence>
          <xs:element ref="WasScan" minOccurs="0" maxOccurs="unbounded"
/>
        </xs:sequence>
      </xs:complexType>

      <!-- DATA -->
      <xs:complexType name="WasScan">
        <xs:all>
          <xs:element name="id" type="xs:long" minOccurs="0"/>
          <xs:element name="name" type="Cdata" minOccurs="0"/>
          <xs:element name="reference" type="xs:string" minOccurs="0"/>
          <xs:element name="type" type="WasScanType" minOccurs="0"/>
          <xs:element name="mode" type="WasScanMode" minOccurs="0"/>
          <xs:element name="multi" type="xs:boolean" minOccurs="0"/>
          <xs:element name="progressiveScanning"
type="ProgressiveScanningOption" minOccurs="0"/>
          <xs:element name="target" type="WasScanTarget" minOccurs="0"/>
          <xs:element name="profile" type="WasScanOptionProfile"
minOccurs="0"/>
          <xs:element name="cancelAfterNHours" type="xs:int"
minOccurs="0"/>
          <xs:element name="cancelTime" type="xs:string" minOccurs="0"/>

```



```

        <xs:element name="options" type="WasScanOptionList"
minOccurs="0"/>
        <xs:element name="launchedDate" type="xs:dateTime"
minOccurs="0"/>
        <xs:element name="launchedBy" type="User" minOccurs="0"/>
        <xs:element name="status" type="WasScanStatus" minOccurs="0"/>
        <xs:element name="consolidatedStatus"
type="WasScanResultStatus" minOccurs="0"/>
        <xs:element name="cancelMode" type="CancelMode"
minOccurs="0"/>
        <xs:element name="canceledBy" type="User" minOccurs="0"/>
        <xs:element name="endScanDate" type="xs:dateTime"
minOccurs="0"/>
        <xs:element name="scanDuration" type="xs:long" minOccurs="0"/>
        <xs:element name="summary" type="WasScanSummary"
minOccurs="0"/>
        <xs:element name="stats" type="WasScanStats" minOccurs="0"/>
        <xs:element name="vulns" type="WasScanVulnList"
minOccurs="0"/>
        <xs:element name="sensitiveContents"
type="WasScanSensitiveContentList" minOccurs="0"/>
        <xs:element name="igs" type="WasScanIgList" minOccurs="0"/>
        <xs:element name="sendMail" type="xs:boolean" default="true"
minOccurs="0"/>
        <xs:element name="sendOneMail" type="xs:boolean"
default="false" minOccurs="0"/>
        <xs:element name="enableWAFAuth" type="xs:boolean"
default="false" minOccurs="0"/>
        <xs:element name="cancelWithResults" type="xs:boolean"
default="false" minOccurs="0"/>
    </xs:all>
</xs:complexType>
<xs:element name="WasScan" type="WasScan" />
.....
<xs:simpleType name="WasScanStatus">
    <xs:restriction base="xs:string">
        <xs:enumeration value="SUBMITTED"/>
        <xs:enumeration value="RUNNING"/>
        <xs:enumeration value="FINISHED"/>
        <xs:enumeration value="ERROR"/>
        <xs:enumeration value="CANCELED"/>
    </xs:restriction>
</xs:simpleType>
.....
<xs:simpleType name="WasScanResultStatus">
    <xs:restriction base="xs:string">
        <xs:enumeration value="NOT_USED"/>
        <xs:enumeration value="TO_BE_PROCESSED"/>
        <xs:enumeration value="NO_HOST_ALIVE"/>
    </xs:restriction>
</xs:simpleType>

```

```
<xs:enumeration value="NO_WEB_SERVICE"/>
<xs:enumeration value="SERVICE_ERROR"/>
<xs:enumeration value="TIME_LIMIT_REACHED"/>
<xs:enumeration value="SCAN_INTERNAL_ERROR"/>
<xs:enumeration value="SCAN_RESULTS_INVALID"/>
<xs:enumeration value="SUCCESSFUL"/>
<xs:enumeration value="PROCESSING"/>
<xs:enumeration value="TIME_LIMIT_EXCEEDED"/>
<xs:enumeration value="SCAN_NOT_LAUNCHED"/>
<xs:enumeration value="SCANNER_NOT_AVAILABLE"/>
<xs:enumeration value="SUBMITTED"/>
<xs:enumeration value="RUNNING"/>
<xs:enumeration value="FINISHED"/>
<xs:enumeration value="CANCELED"/>
<xs:enumeration value="CANCELING"/>
<xs:enumeration value="ERROR"/>
<xs:enumeration value="DELETED"/>
<xs:enumeration value="CANCELED_WITH_RESULTS"/>
</xs:restriction>
</xs:simpleType>
.....
</xs:complexType>

<xs:complexType name="SSLDataProp">
  <xs:all>
    <xs:element name="name" type="xs:string" minOccurs="0" />
    <xs:element name="value" type="xs:string" minOccurs="0" />
    <xs:element name="protocol" type="xs:string" minOccurs="0" />
  </xs:all>
</xs:complexType>

</xs:schema>
```

WAS API: New API for OWASP ZAP Findings

API affected	/qps/rest/3.0/import/was/owaspzap/ /qps/rest/3.0/search/was/owaspzapfinding/ /qps/rest/3.0/count/was/owaspzapfinding/ /qps/rest/3.0/get/was/owaspzapfinding/id/
New or Updated APIs	New
DTD or XSD changes	Yes

With this release, we have added API support for importing OWASP ZAP reports and save the findings discovered by OWASP ZAP tool with the findings discovered by WAS. You can also search for the specific OWASP findings, details of the finding, and total number of OWASP ZAP findings in your scope.

Import OWASP ZAP Findings

API affected	/qps/rest/3.0/import/was/owaspzap/
New or Updated APIs	New
Operator	POST
DTD or XSD changes	Yes

Input Parameters

Parameter	Mandatory/ Optional	Format	Description
webAppId	Mandatory	Integer	The web application ID. This element is assigned by the service and required for an update request.
purgeResults	Optional	Boolean	Set to false to indicate if all previous issues for the web application should be retained. By default, it is set to false.
closeUnreportedIssues	Optional	Boolean	Set to false to indicate if all previous issues for the web application should be marked as fixed and should not be reported. By default, it is set to false.
fileName	Optional	String	Name of the owasp file to be imported. If name is not specified, default format for the file name is API-ImportOwaspZap-dd-mmm-yy hh:mm:ss

Sample - Import OWASP ZAP Findings

API Request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --  
data-binary @-  
"qualys_base_url/qps/rest/3.0/import/was/owaspzap" <file.xml>
```

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

Request POST data:

```
<ServiceRequest>  
  <data>  
    <webAppId>29120395</webAppId>  
    <purgeResults>>false</purgeResults>  
    <closeUnreportedIssues>>false</closeUnreportedIssues>  
    <fileName>testOwaspFile</fileName>  
    <owaspZapXml>  
      <OWASPZAPReport programName="OWASP ZAP" version="Dev Build"  
generated="Thu, 17 Nov 2022 11:03:08">  
        <site name="https://www.googletagservices.com"  
host="www.googletagservices.com" port="443" ssl="true">  
          <alerts>  
            <alertitem>  
              <pluginid>10035</pluginid>  
              <alertRef>10035</alertRef>  
              <alert>Strict-Transport-Security Header NotSet</alert>  
              <name>Strict-Transport-Security Header Not Set</name>  
              <riskcode>1</riskcode>  
              <confidence>3</confidence>  
              <riskdesc>Low (High)</riskdesc>  
              <confidencedesc>High</confidencedesc>  
              <desc>HTTP Strict Transport Security (HSTS) is a web  
security policy mechanism whereby a web server declares that complying  
user agents (such as a web browser) are to interact with it using only  
secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF  
standards track protocol and is specified in RFC 6797.</desc>  
              <instances>  
                <instance>  
  
            </instance>  
          </alerts>  
        </site>  
      </OWASPZAPReport>  
    </owaspZapXml>  
  </data>  
</ServiceRequest>  
  
<uri>https://www.googletagservices.com/tag/js/gpt.js</uri>  
  <method>GET</method>  
  <param></param>  
  <attack></attack>  
  <evidence></evidence>  
  <requestheader>GET  
https://www.googletagservices.com/tag/js/gpt.js HTTP/1.1  
Host: www.googletagservices.com  
Connection: keep-alive  
sec-ch-ua: &quot;Google Chrome&quot;;v=&quot;107&quot;;  
&quot;Chromium&quot;;v=&quot;107&quot;;  
&quot;Not=A?Brand&quot;;v=&quot;24&quot;;
```

```
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows";
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://jsonlint.com/
Accept-Language: en-US,en;q=0.9
```

```
</requestheader>
<requestbody></requestbody>
<responseheader>HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/javascript
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-
gpt-scs";
Report-To: {"group": "ads-gpt-
scs", "max_age": 2592000, "endpoints": [{"url": "https://csp.withgoogle.com/csp/report-to/ads-gpt-scs"}]}
Timing-Allow-Origin: *
Content-Length: 80512
Date: Thu, 17 Nov 2022 05:20:21 GMT
Expires: Thu, 17 Nov 2022 05:20:21 GMT
Cache-Control: private, max-age=900, stale-while-revalidate=3600
ETag: "1394 / 793 of 1000 / last-modified: 1668639967";
X-Content-Type-Options: nosniff
Server: sffe
X-XSS-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443";
ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443";
ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443";
ma=2592000; v="46,43";
```

```
</responseheader>
<responsebody>(function (E) )
</responsebody>
</instance>
</instances>
<count>1</count>
<solution>Ensure that your web server, application server, load balancer,
etc. is configured to enforce Strict-Transport-Security.</solution>
<otherinfo></otherinfo>
```

```
<reference>https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Tra
nsport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
```

```
http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
http://caniuse.com/stricttransportsecurity
http://tools.ietf.org/html/rfc6797</reference>
    <cweid>319</cweid>
    <wascid>15</wascid>
    <sourceid>8</sourceid>
    <tags>
        <tag>
            <tag>OWASP_2021_A05</tag>
            <link>https://owasp.org/Top10/A05_2021-
Security_Misconfiguration/</link>
        </tag>
        <tag>
            <tag>OWASP_2017_A06</tag>
            <link>https://owasp.org/www-project-
top-ten/2017/A6_2017-Security_Misconfiguration.html</link>
        </tag>
    </tags>
</alertitem>
<alertitem>
    <pluginid>10027</pluginid>
    <alertRef>10027</alertRef>
    <alert>Information Disclosure - Suspicious
Comments</alert>
    <name>Information Disclosure - Suspicious
Comments</name>
    <riskcode>0</riskcode>
    <confidence>1</confidence>
    <riskdesc>Informational (Low)</riskdesc>
    <confidencedesc>Low</confidencedesc>
    <desc>The response appears to contain suspicious
comments which may help an attacker. Note: Matches made within script
blocks or files are against the entire content not only comments.</desc>
    <instances>
        <instance>
<uri>https://www.googletagservices.com/tag/js/gpt.js</uri>
            <method>GET</method>
            <param></param>
            <attack></attack>
            <evidence>db</evidence>
            <requestheader>GET
https://www.googletagservices.com/tag/js/gpt.js HTTP/1.1
Host: www.googletagservices.com
Connection: keep-alive
sec-ch-ua: &quot;Google Chrome&quot;;v=&quot;107&quot;;
&quot;Chromium&quot;;v=&quot;107&quot;;
&quot;Not=A?Brand&quot;;v=&quot;24&quot;;
sec-ch-ua-mobile: ?0
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows";
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://jsonlint.com/
Accept-Language: en-US,en;q=0.9

</requestheader>

<requestbody></requestbody>
<responseheader>HTTP/1.1 200 OK

Vary: Accept-Encoding
Content-Type: text/javascript
</responseheader>

<responsebody>(function(E))

</responsebody>

</instance>
<instance>

<uri>https://www.googletagservices.com/tag/js/gpt.js</uri>
<method>GET</method>
<param></param>
<attack></attack>
<evidence>query</evidence>
<requestheader>GET

https://www.googletagservices.com/tag/js/gpt.js HTTP/1.1

Host: www.googletagservices.com

Connection: keep-alive

sec-ch-ua: "Google Chrome";v="107";,
"Chromium";v="107";,
"Not=A?Brand";v="24";

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36

sec-ch-ua-platform: "Windows";

Accept: */*

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: script

Referer: https://jsonlint.com/

Accept-Language: en-US,en;q=0.9

</requestheader>

<requestbody></requestbody>
<responseheader>HTTP/1.1 200 OK

Vary: Accept-Encoding
Content-Type: text/javascript

```
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=&quot;ads-
gpt-scs&quot;;
Report-To: {&quot;group&quot;:&quot;ads-gpt-
scs&quot;, &quot;max_age&quot;:2592000, &quot;endpoints&quot;:[{&quot;url&
quot;:&quot;https://csp.withgoogle.com/csp/report-to/ads-gpt-scs&quot;}] }
Timing-Allow-Origin: *
Content-Length: 80512
Date: Thu, 17 Nov 2022 05:20:21 GMT
Expires: Thu, 17 Nov 2022 05:20:21 GMT
Cache-Control: private, max-age=900, stale-while-revalidate=3600
ETag: &quot;1394 / 793 of 1000 / last-modified: 1668639967&quot;;
X-Content-Type-Options: nosniff
Server: sffe
X-XSS-Protection: 0
Alt-Svc: h3=&quot;;443&quot;; ma=2592000,h3-29=&quot;;443&quot;;
ma=2592000,h3-Q050=&quot;;443&quot;; ma=2592000,h3-Q046=&quot;;443&quot;;
ma=2592000,h3-Q043=&quot;;443&quot;; ma=2592000,quic=&quot;;443&quot;;
ma=2592000; v=&quot;46,43&quot;;
```

```
</responseheader>
```

```
<responsebody>(function (E) {var
```

```
window=this..});
```

```
</responsebody>
```

```
</instance>
```

```
</instances>
```

```
<count>2</count>
```

```
<solution>Remove all comments that return
information that may help an attacker and fix any underlying problems they
refer to.</solution>
```

```
<otherinfo>The following pattern was used:
\bDB\b and was detected in the element starting with: &quot;var
aa,ba=function(a){var b=0;return function(){return
b<lt;a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=&quot;function&quot;=
=typeof Objec&quot;;, see evidence field for the suspicious
comment/snippet.</otherinfo>
```

```
<reference></reference>
```

```
<cweid>200</cweid>
```

```
<wascid>13</wascid>
```

```
<sourceid>8</sourceid>
```

```
<tags>
```

```
<tag>
```

```
<tag>OWASP_2021_A01</tag>
```

```
<link>https://owasp.org/Top10/A01_2021-
Broken_Access_Control</link>
```

```
</tag>
```

```
<tag>
```

```
<tag>OWASP_2017_A03</tag>
```

```
<link>https://owasp.org/www-project-
```



```
top-ten/2017/A3_2017-Sensitive_Data_Exposure.html</link>
  </tag>
</tags>
</alertitem>
</alerts>
</site>
</OWASPZAPReport>
</owaspZapXml>
</data>
</ServiceRequest>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.0/was/owaspzap.x
sd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <OwaspZap>
      <id>2001</id>
      <webApp>
        <id>29120395</id>
        <name>
          <![CDATA[Import Zap finding Web appl]]>
        </name>
        <url>
          <![CDATA[http://10.10.60.90]]>
        </url>
      </webApp>
      <alerts>
        <list>
          <AlertItem>
            <alertRef>10027</alertRef>
          </AlertItem>
          <AlertItem>
            <alertRef>10035</alertRef>
          </AlertItem>
        </list>
      </alerts>
      <fileName>testOwaspFile</fileName>
      <errorRecords>
        <count>0</count>
      </errorRecords>
    </OwaspZap>
  </data>
</ServiceResponse>
```

Search OWASP ZAP Findings

API affected	/qps/rest/3.0/search/was/owaspzap/
New or Updated APIs	New
Operator	POST
DTD or XSD changes	Yes

With the search findings API, you can retrieve list of OWASP ZAP findings found in web applications in your scope.

Input Parameters

Parameter	Mandatory/ Optional	Format	Description
id	Optional	Integer	ID of the finding.
uniqueId	Optional	String	The 36-bit unique id assigned to the finding.
name	Optional	String	Name of the detection finding.
alertRef	Optional	String	Reference of OWASP ZAP alert
webApp.id	Optional	Iteger	ID of the web application on which the finding was detected.
webApp.name	Optional	String	Name of the web application on which the finding was detected.
webApp.tags	Optional	Integer	The tags associated with the web application being scanned. Note: This parameter supports operator="NONE".
webApp.tags.id	Optional	Integer	The tag ID assigned to web application being scanned.
webApp.tags.name	Optional	String	Name of the tag associated with the web application on which the finding was detected.

Note: These parameters are optional and act as filters. When multiple parameters are specified, you can use AND to combine the filters.

Sample - Search OWASP ZAP Finding

API Request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
data-binary @-
"qualys_base_url/qps/rest/3.0/search/was/owaspzapfinding" < file.xml
```

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

Request POST data:

```
<ServiceRequest>
<filters>
  <Criteria field="id" operator="EQUALS">1002</Criteria>
</filters>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.0/was/owaspzapfi
nding.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>>false</hasMoreRecords>
  <data>
    <OwaspZapFinding>
      <id>1002</id>
      <uniqueId>f2b03430-87d5-450b-98c5-6ce210b41e8c</uniqueId>
      <findingType>OWASPZAP</findingType>
      <pluginid>10035</pluginid>
      <alertRef>10035</alertRef>
      <alert>Strict-Transport-Security Header Not Set</alert>
      <name>Strict-Transport-Security Header Not Set</name>
      <riskcode>1</riskcode>
      <confidence>3</confidence>
      <riskdesc>Low (High)</riskdesc>
      <confidencedesc>High</confidencedesc>
      <desc>HTTP Strict Transport Security (HSTS) is a web security
policy mechanism whereby a web server declares that complying user agents
(such as a web browser) are to interact with it using only secure HTTPS
connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards
track protocol and is specified in RFC 6797.</desc>
      <count>1</count>
      <solution>Ensure that your web server, application server, load
balancer, etc. is configured to enforce Strict-Transport-
Security.</solution>
      <reference>https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Tra
nsport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security-Headers
http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
http://caniuse.com/stricttransportsecurity
http://tools.ietf.org/html/rfc6797</reference>
      <cweid>319</cweid>
      <wascid>15</wascid>
      <sourceid>8</sourceid>
```

```
<tags>
  <list>
    <OwaspZapTag>
      <tag>OWASP_2021_A05</tag>
      <link>https://owasp.org/Top10/A05_2021-
Security_Misconfiguration/</link>
    </OwaspZapTag>
    <OwaspZapTag>
      <tag>OWASP_2017_A06</tag>
      <link>https://owasp.org/www-project-top-
ten/2017/A6_2017-Security_Misconfiguration.html</link>
    </OwaspZapTag>
  </list>
</tags>
<instances>
  <list>
    <Instance>

<uri>https://www.googletagservices.com/tag/js/gpt.js</uri>
      <method>GET</method>
      <requestheader>GET
https://www.googletagservices.com/tag/js/gpt.js HTTP/1.1
Host: www.googletagservices.com
Connection: keep-alive
sec-ch-ua: &quot;Google Chrome&quot;;v=&quot;107&quot;;
&quot;Chromium&quot;;v=&quot;107&quot;;
&quot;Not=A?Brand&quot;;v=&quot;24&quot;;
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
sec-ch-ua-platform: &quot;Windows&quot;;
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://jsonlint.com/
Accept-Language: en-US,en;q=0.9

</requestheader>
      <responseheader>HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/javascript
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=&quot;ads-
gpt-scs&quot;;
Report-To: {&quot;group&quot;:&quot;ads-gpt-
scs&quot;;&quot;max_age&quot;:2592000,&quot;endpoints&quot;:[{&quot;url&q
uot;:&quot;https://csp.withgoogle.com/csp/report-to/ads-gpt-scs&quot;}]}}
Timing-Allow-Origin: *
```

```
Content-Length: 80512
Date: Thu, 17 Nov 2022 05:20:21 GMT
Expires: Thu, 17 Nov 2022 05:20:21 GMT
Cache-Control: private, max-age=900, stale-while-revalidate=3600
ETag: "1394 / 793 of 1000 / last-modified: 1668639967"
X-Content-Type-Options: nosniff
Server: sffe
X-XSS-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"

</responseheader>
      </Instance>
    </list>
  </instances>
</OwaspZapFinding>
</data>
</ServiceResponse>
```

Search OWASP ZAP Findings Count

API affected	qps/rest/3.0/count/was/owaspzapfinding
New or Updated APIs	New
Operator	POST
DTD or XSD changes	Yes

With the count OWASP ZAP finding API, you can retrieve the count of OWASP ZAP findings for a selected criteria.

Input Parameters

Parameter	Mandatory/ Optional	Format	Description
id	Optional	Integer	ID of the finding.
uniqueId	Optional	String	The 36-bit unique ID assigned to the finding.
name	Optional	String	Name of the detection finding.
alertRef	Optional	String	Reference of OWASP ZAP alert
webApp.id	Optional	Integer	ID of the web application on which the finding was detected.
webApp.name	Optional	String	Name of the web application on which the finding was detected.
webApp.tags	Optional	Integer	The tags associated with the web application being scanned. Note: This parameter supports operator="NONE".
webApp.tags.id	Optional	Integer	The tag ID assigned to web application being scanned.
webApp.tags.name	Optional	String	Name of the tag associated with the web application on which the finding was detected.

Note: These parameters are optional and act as filters. When multiple parameters are specified, you can use AND to combine the filters.

Sample - Count OWASP ZAP Finding

API Request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
data-binary @-
"qualys_base_url/qps/rest/3.0/count/was/owaspzapfinding" < file.xml
```

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

Request POST data:

```
<ServiceRequest>
<filters>
  <Criteria field="id" operator="EQUALS">1002</Criteria>
</filters>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.0/was/owaspzapfi  
nding.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
</ServiceResponse>
```

Search OWASP ZAP Findings Details

API affected	qps/rest/3.0/get/was/owaspzapfinding/<id>
New or Updated APIs	New
Operator	GET
DTD or XSD changes	Yes

With this API, you can retrieve details of a specific OWASP ZAP finding.

Sample - Search OWASP ZAP Finding Details

API Request:

```
curl -n -u "USERNAME:PASSWORD"  
"qualys_base_url/qps/rest/3.0/get/was/owaspzapfinding/1001"
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="qualys_base_url/qps/xsd/3.0/was/owaspzapfi  
nding.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
  <data>  
    <OwaspZapFinding>  
      <id>1001</id>  
      <uniqueId>a2e825d4-db9d-49a9-842a-4c22fab555eb</uniqueId>  
      <findingType>OWASPZAP</findingType>  
      <pluginid>10027</pluginid>  
      <alertRef>10027</alertRef>  
      <alert>Information Disclosure - Suspicious Comments</alert>  
      <name>Information Disclosure - Suspicious Comments</name>  
      <riskcode>0</riskcode>  
      <confidence>1</confidence>  
      <riskdesc>Informational (Low)</riskdesc>  
      <confidencedesc>Low</confidencedesc>  
      <desc>The response appears to contain suspicious comments which  
may help an attacker. Note: Matches made within script blocks or files are  
against the entire content not only comments.</desc>  
      <count>2</count>
```

```
<solution>Remove all comments that return information that may
help an attacker and fix any underlying problems they refer to.</solution>
<otherinfo>The following pattern was used: \bDB\b and was
detected in the element starting with: &quot;var aa,ba=function(a){var
b=0;return function(){return
b&amp;lt;a.length?(done:!1,value:a[b++]):{done:!0}}},ca=&quot;function&qu
ot;==typeof Objec&quot;;, see evidence field for the suspicious
comment/snippet.</otherinfo>
  <cweid>200</cweid>
  <wascid>13</wascid>
  <sourceid>8</sourceid>
  <tags>
    <list>
      <OwaspZapTag>
        <tag>OWASP_2017_A03</tag>
        <link>https://owasp.org/www-project-top-
ten/2017/A3_2017-Sensitive_Data_Exposure.html</link>
      </OwaspZapTag>
      <OwaspZapTag>
        <tag>OWASP_2021_A01</tag>
        <link>https://owasp.org/Top10/A01_2021-
Broken_Access_Control/</link>
      </OwaspZapTag>
    </list>
  </tags>
  <instances>
    <list>
      <Instance>
<uri>https://www.googletagservices.com/tag/js/gpt.js</uri>
      <method>GET</method>
      <evidence>query</evidence>
      <requestheader>GET
https://www.googletagservices.com/tag/js/gpt.js HTTP/1.1
Host: www.googletagservices.com
Connection: keep-alive
sec-ch-ua: &quot;Google Chrome&quot;;v=&quot;107&quot;;
&quot;Chromium&quot;;v=&quot;107&quot;;
&quot;Not=A?Brand&quot;;v=&quot;24&quot;;
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
sec-ch-ua-platform: &quot;Windows&quot;;
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://jsonlint.com/
Accept-Language: en-US,en;q=0.9
```



```
</requestheader>
                                <responseheader>HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/javascript
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=&quot;ads-gpt-scs&quot;;
Report-To: {&quot;group&quot;:&quot;ads-gpt-scs&quot;;&quot;max_age&quot;:2592000,&quot;endpoints&quot;:[{&quot;url&quot;:&quot;https://csp.withgoogle.com/csp/report-to/ads-gpt-scs&quot;}]}}
Timing-Allow-Origin: *
Content-Length: 80512
Date: Thu, 17 Nov 2022 05:20:21 GMT
Expires: Thu, 17 Nov 2022 05:20:21 GMT
Cache-Control: private, max-age=900, stale-while-revalidate=3600
ETag: &quot;1394 / 793 of 1000 / last-modified: 1668639967&quot;;
X-Content-Type-Options: nosniff
Server: sffe
X-XSS-Protection: 0
Alt-Svc: h3=&quot;;:443&quot;; ma=2592000,h3-29=&quot;;:443&quot;; ma=2592000,h3-Q050=&quot;;:443&quot;; ma=2592000,h3-Q046=&quot;;:443&quot;; ma=2592000,h3-Q043=&quot;;:443&quot;; ma=2592000,quic=&quot;;:443&quot;; ma=2592000; v=&quot;46,43&quot;;
```

```
</responseheader>
```

```
</Instance>
<Instance>
```

```
<uri>https://www.googletagservices.com/tag/js/gpt.js</uri>
                                <method>GET</method>
                                <evidence>db</evidence>
                                <requestheader>GET
https://www.googletagservices.com/tag/js/gpt.js HTTP/1.1
Host: www.googletagservices.com
Connection: keep-alive
sec-ch-ua: &quot;Google Chrome&quot;;v=&quot;107&quot;;&quot;Chromium&quot;;v=&quot;107&quot;;&quot;Not=A?Brand&quot;;v=&quot;24&quot;;
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
sec-ch-ua-platform: &quot;Windows&quot;;
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://jsonlint.com/
Accept-Language: en-US,en;q=0.9
```

```
</requestheader>
      <responseheader>HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/javascript
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=&quot;ads-gpt-scs&quot;;
Report-To: {&quot;group&quot;:&quot;ads-gpt-scs&quot;;&quot;max_age&quot;:2592000,&quot;endpoints&quot;:[{&quot;url&quot;:&quot;https://csp.withgoogle.com/csp/report-to/ads-gpt-scs&quot;}]}
Timing-Allow-Origin: *
Content-Length: 80512
Date: Thu, 17 Nov 2022 05:20:21 GMT
Expires: Thu, 17 Nov 2022 05:20:21 GMT
Cache-Control: private, max-age=900, stale-while-revalidate=3600
ETag: &quot;1394 / 793 of 1000 / last-modified: 1668639967&quot;;
X-Content-Type-Options: nosniff
Server: sffe
X-XSS-Protection: 0
Alt-Svc: h3=&quot;;443&quot;; ma=2592000,h3-29=&quot;;443&quot;; ma=2592000,h3-Q050=&quot;;443&quot;; ma=2592000,h3-Q046=&quot;;443&quot;; ma=2592000,h3-Q043=&quot;;443&quot;; ma=2592000,quic=&quot;;443&quot;; ma=2592000; v=&quot;46,43&quot;;

</responseheader>
      </Instance>
    </list>
  </instances>
</OwaspZapFinding>
</data>
</ServiceResponse>
```

Issue Addressed

- We have resolved the issue of an error occurrence while trying to fetch the WAS schedule scan information using API.