# Qualys Cloud Platform (VM, PC) v8.x

## API Release Notes

Version 8.16

November 19, 2018

This new version of the Qualys Cloud Platform (VM, PC) includes improvements to the Qualys API. 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**

### URL to the Qualys API Server

Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located.

| Account Location | API Server URL |
|---|---|
| Qualys US Platform 1 | https://qualysapi.qualys.com |
| Qualys US Platform 2 | https://qualysapi.qg2.apps.qualys.com |
| Qualys US Platform 3 | https://qualysapi.qg3.apps.qualys.com |
| Qualys EU Platform 1 | https://qualysapi.qualys.eu |
| Qualys EU Platform 2 | https://qualysapi.qg2.apps.qualys.eu |
| Qualys India Platform 1 | https://qualysapi.qg1.apps.qualys.in |
| Qualys Private Cloud Platform | https://qualysapi.<customer_base_url> |

The Qualys API documentation and sample code use the API server URL for the Qualys US Platform 1. If your account is located on another platform, please replace this URL with the appropriate server URL for your account.

# New CVSS v3.0 Metrics Added to KnowledgeBase API

| | |
|---|---|
| APIs affected | /api/2.0/fo/knowledge_base/vuln/ |
| New or Updated API | Updated |
| DTD or XSD changes | Yes |

We updated the CVSS v2 and CVSS v3 sections of the KnowledgeBase API output. For both CVSS v2 and CVSS v3 we added the vector string. For CVSS v3 we renamed, added and removed metrics to match the CVSS v3 standard.

Update for CVSS v2:

- Added VECTOR STRING. This string captures the scores of individual metrics obtained for a vulnerability. For example: CVSS:2.0/AV:N/AC:H/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C.

Updates for CVSS v3:

- Added VECTOR STRING. This string captures the scores of individual metrics obtained for a vulnerability. For example:
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

Note - Vector strings for CVSS v2 and v3 will not appear if scores for any of the base metrics is 0 or null. The individual tags of base metrics with value 0 are not shown in output. For example, if CONFIDENTIALITY impact is 0 then output will not show the tag.

- Added PRIVILEGES REQUIRED. This metric represents the privileges required by an attacker in order to exploit the vulnerability. Possible values: 1 (None), 2 (Low), 3 (High)

- Added USER INTERACTION. This metric represents the user interactions required to exploit the vulnerability. Possible values: 1 (None), 2 (Required)

- Added SCOPE. This metric represents the impact on other components due to a vulnerability. Possible values: 1 (Unchanged), 2 (Changed)

- Added EXPLOIT CODE MATURITY. This metric represents the probability of exploiting a vulnerability based on the maturity of exploit code. Possible values: 4 (High), 3 (Functional), 2 (Proof of Concept), 1 (Unproven), 0 (Not Defined)

- Renamed ACCESS VECTOR to ATTACK VECTOR under CVSS v3 (not changed under CVSS v2). This metric represents network, local or physical access required to exploit a vulnerability. Possible values: 1 (Network), 2 (Adjacent Network), 3 (Local) and 4 (Physical)

- Renamed ACCESS COMPLEXITY to ATTACK COMPLEXITY under CVSS v3 (not changed under CVSS v2). This metric measures specialized access conditions required to exploit a vulnerability. Possible values: 1 (Low), 2 (High)

- Removed AUTHENTICATION and EXPLOITABILITY under CVSS v3 since these metrics only apply to CVSS v2.

## Sample - List vulnerabilities from the KnowledgeBase

API request:

```
curl -u "user:password" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/" >
output.txt
```

XML output:

```
...
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/knowledge_ba
se_vuln_list_output.dtd">
...
<VULN>
  <QID>38626</QID>
   ...
<CVSS>
  <BASE>2.6</BASE>
  <TEMPORAL>2</TEMPORAL>
  <VECTOR_STRING>
    CVSS:2.0/AV:N/AC:H/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C
  </VECTOR_STRING>
  <ACCESS>
    <VECTOR>3</VECTOR>
    <COMPLEXITY>3</COMPLEXITY>
  </ACCESS>
  <IMPACT>
    <CONFIDENTIALITY>2</CONFIDENTIALITY>
    <INTEGRITY>1</INTEGRITY>
    <AVAILABILITY>1</AVAILABILITY>
  </IMPACT>
  <AUTHENTICATION>1</AUTHENTICATION>
  <EXPLOITABILITY>2</EXPLOITABILITY>
  <REMEDIATION_LEVEL>1</REMEDIATION_LEVEL>
  <REPORT_CONFIDENCE>3</REPORT_CONFIDENCE>
</CVSS>
<CVSS_V3>
  <BASE>5.9</BASE>
  <TEMPORAL>5.3</TEMPORAL>
  <VECTOR_STRING>
    CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
  </VECTOR_STRING>
  <ATTACK>
    <VECTOR>1</VECTOR>
    <COMPLEXITY>2</COMPLEXITY>
  </ATTACK>
  <IMPACT>
    <CONFIDENTIALITY>3</CONFIDENTIALITY>
```

```
      <INTEGRITY>1</INTEGRITY>
      <AVAILABILITY>1</AVAILABILITY>
    </IMPACT>
    <PRIVILEGES_REQUIRED>1</PRIVILEGES_REQUIRED>
    <USER_INTERACTION>1</USER_INTERACTION>
    <SCOPE>1</SCOPE>
    <EXPLOIT_CODE_MATURITY>2</EXPLOIT_CODE_MATURITY>
    <REMEDIATION_LEVEL>1</REMEDIATION_LEVEL>
    <REPORT_CONFIDENCE>3</REPORT_CONFIDENCE>
  </CVSS_V3>
  ...
```

Updated DTD:

<platformURL>/api/2.0/fo/knowledge_base/vuln/knowledge_base_vuln_list_output.dtd

We updated the DTD to include the new elements (in bold).

```
...
<!ELEMENT CVSS (BASE, TEMPORAL?, VECTOR_STRING?, ACCESS?, IMPACT?,
AUTHENTICATION?, EXPLOITABILITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>
        <!ELEMENT VECTOR_STRING (#PCDATA)>
....
      <!ELEMENT CVSS_V3 (BASE, TEMPORAL?, VECTOR_STRING?, ATTACK?,
IMPACT?, PRIVILEGES_REQUIRED?, USER_INTERACTION?, SCOPE?,
EXPLOIT_CODE_MATURITY?, REMEDIATION_LEVEL?, REPORT_CONFIDENCE?)>
      <!ELEMENT ATTACK (VECTOR?, COMPLEXITY?)>
      <!ELEMENT PRIVILEGES_REQUIRED (#PCDATA)>
      <!ELEMENT USER_INTERACTION (#PCDATA)>
      <!ELEMENT SCOPE (#PCDATA)>
      <!ELEMENT EXPLOIT_CODE_MATURITY (#PCDATA)>
...
<!-- EOF -->
```

# Support for Scanning ESXi Hosts on vCenter

Looking for information on this feature? Our user guide will help you run Qualys Policy Compliance scans on your ESXi hosts through vCenter. Click here to download it.

We made API updates to support this feature:

VMware Authentication Record | vCenter Authentication Record | Option Profile API

## VMware Authentication Record

| | |
|---|---|
| APIs affected | /api/2.0/fo/auth/vmware/ |
| New or Updated API | Updated |
| DTD or XSD changes | No |

You can now specify login_type=vcenter in the API request when creating and updating VMware authentication records.

### Sample - Create VMware Authentication Record

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=create&title=VmWare-VCenter-Auth-
API&ips=10.10.10.110&login_type=vcenter&port=80"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-06-28T07:43:58Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>179933</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### Sample - List VMware Authentication Record

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&ids=179933"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_VMWARE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/auth_vmware_l
ist_output.dtd">
<AUTH_VMWARE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-28T07:44:32Z</DATETIME>
    <AUTH_VMWARE_LIST>
      <AUTH_VMWARE>
        <ID>179933</ID>
        <TITLE><![CDATA[VmWare-VCenter-Auth-API]]></TITLE>
        <PORT>80</PORT>
        <SSL_VERIFY><![CDATA[all]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.110</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-06-28T07:43:58Z</DATETIME>
          <BY>user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-06-28T07:43:58Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_VMWARE>
    </AUTH_VMWARE_LIST>
  </RESPONSE>
</AUTH_VMWARE_LIST_OUTPUT>
```

## vCenter Authentication Record

| | |
|---|---|
| APIs affected | /api/2.0/fo/auth/vcenter/ |
| New or Updated API | New |
| DTD or XSD changes | New |

Create, update, list and delete vCenter records for authenticating to ESXi hosts through vCenter. Note - To create a vCenter record using API, you need to first define the vCenter - ESXi mappings using the UI. Currently defining the mappings using API is not supported.

### Input Parameters

| Parameter | Description |
|---|---|
| action={action} | (Required) Specify create, update, delete (using POST) or list (using GET or POST). |
| echo_request={**0**\|1} | (Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included. |
| ids={value} | (Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated. |
| title={value} | (Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii). |
| comments={value} | (Optional to create or update record) User defined comments. Maximum of 1999 characters. |
| **Login credentials** | |
| username={value} | (Required to create record, optional to update record) The user name for a vCenter account. A maximum of 13 characters (ascii) may be specified. |
| password={value} | (To create record password or login_type=vault is required) The password for a vCenter account. Maximum 13 characters (ascii). |
| login_type={**basic**\|vault} | (To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See the API user guide. |
| port={value} | (Optional) The service communicates with ESXi web services on port 443 and another port can be configured. When unspecified, port 443 is used. |

| Parameter | Description |
|---|---|
| hosts={value} | (Optional) A list of FQDNs for the hosts that correspond to all ESXi host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated. |
| ssl_verify={value} | (Optional) Specify "all" for a complete SSL certificate validation. Specify "skip" if the host SSL certificate is self-signed or uses an SSL certificate signed by a custom root CA. Specify "none" for no SSL verification. |
| **Target Hosts** | |
| ips={value} | (Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated.<br><br>(Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.<br><br>This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request. |
| add_ips={value} | (Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated.<br><br>This parameter and the ips parameter cannot be specified in the same request. |
| remove_ips={value} | (Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.<br><br>This parameter and the ips parameter cannot be specified in the same request. |
| network_id={value} | (Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record. |

### Sample - Create vCenter Record

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=create&title=VCenter-Auth-Create
API&ips=10.10.10.110&login_type=basic&port=80&username=username&pa
ssword=password"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-06-28T07:47:47Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>179973</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### Sample - Update vCenter Record

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=update&ids=179973&add_ips=10.10.10.2-10.10.10.5"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-06-28T07:47:47Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>179973</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
```

```
  </RESPONSE>
</BATCH_RETURN>
```

### Sample - Delete vCenter Records

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=delete&ids=179973"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-06-28T07:47:47Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>179973</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### Sample - List vCenter Records

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&ids=179973"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_VCENTER_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/auth_vcenter
_list_output.dtd">
```

```
<AUTH_VCENTER_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-28T07:48:13Z</DATETIME>
    <AUTH_VCENTER_LIST>
      <AUTH_VCENTER>
        <ID>179973</ID>
        <TITLE><![CDATA[VCenter-Auth-Create API]]></TITLE>
        <USERNAME><![CDATA[username]]></USERNAME>
        <PORT>80</PORT>
        <SSL_VERIFY><![CDATA[none]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.110</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-06-28T07:47:47Z</DATETIME>
          <BY>user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-06-28T07:47:47Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_VCENTER>
    </AUTH_VCENTER_LIST>
  </RESPONSE>
</AUTH_VCENTER_LIST_OUTPUT>
```

New DTD:

<platformURL>/api/2.0/fo/auth/vcenter/auth_vcenter_list_output.dtd

```
<!-- QUALYS AUTH_VCENTER_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_VCENTER_LIST_OUTPUT (REQUEST?, RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
```

```
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, (AUTH_VCENTER_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_VCENTER_LIST (AUTH_VCENTER+)>
<!ELEMENT AUTH_VCENTER (ID, TITLE, USERNAME, PORT, SSL_VERIFY,
HOSTS?, IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, NETWORK_ID?,
CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>

<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT HOSTS (HOST+)>
<!ELEMENT HOST (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>
<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?,
VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_ACCOUNT_NAME?)>
```

```
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>
<!-- EOF -->
```

## Option Profile API

| | |
|---|---|
| APIs affected | /api/2.0/fo/subscription/option_profile |
| New or Updated API | Updated |
| DTD or XSD changes | No |

The vCenter map authentication option in the option profile, required to run an automated discovery scan (map) of ESXi hosts, can be set using the option profile API.

You can now specify map_authentication=vCenter in the API request when creating and updating VM option profiles. You an also set this to VMware-ESXi or none. Similarly, when importing option profiles, the <MAP_AUTHENTICATION> tag can be set to vCenter.

### Sample - Update option profile

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&id=25121&map_authentication=vCenter"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
```

```
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-26T09:51:15Z</DATETIME>
    <TEXT>Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>25121</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

### Sample - Import option profile

API request:

```
curl -H "X-Requested-With:curl demo2" -u "USERNAME:PASSWORD" -H
Content-Type:text/xml --data-binary "@/root/myfile.xml"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/?action=import
```

Note - "myfile.xml" contains the request POST data.

Request POST data:

```
...
 </VULNERABILITY_DETECTION>
    <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
    <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>
    </DISSOLVABLE_AGENT>
</SCAN>
<MAP>
    <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
    <TCP_PORTS>
        <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
    </TCP_PORTS>
    <UDP_PORTS>
        <UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
    </UDP_PORTS>
```

```
        <MAP_OPTIONS>
            <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
            <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
        </MAP_OPTIONS>
        <MAP_PERFORMANCE>
            <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
            <MAP_PARALLEL>
                <EXTERNAL_SCANNERS>4</EXTERNAL_SCANNERS>
                <SCANNER_APPLIANCES>4</SCANNER_APPLIANCES>
                <NETBLOCK_SIZE>65536 IPs</NETBLOCK_SIZE>
            </MAP_PARALLEL>
            <PACKET_DELAY>Long</PACKET_DELAY>
        </MAP_PERFORMANCE>
        <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
    </MAP>
    <ADDITIONAL>
        <HOST_DISCOVERY>
            <TCP_PORTS>
                <STANDARD_SCAN>1</STANDARD_SCAN>
    ...
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-05-03T08:33:58Z</DATETIME>
   <TEXT>Successfully imported Option profile for the subscription
Id nnnnnn</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>329725</KEY>
        <VALUE>OP for_vCenter authentication for ESX/ESXi host
discovery</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

# SCAP Last Scanned Date for Asset Search

| | |
|---|---|
| APIs affected | /api/2.0/fo/asset/host/?action=list |
| New or Updated API | Updated |
| DTD or XSD changes | Yes |

We have now introduced two new parameters to filter SCAP last scanned date when you download a list of hosts, based on the scan data available in the user's account.

You can now use two new parameters: scap_scan_since or no_scap_scan_since in the API request.

### Input Parameters

| Parameter | Description |
|---|---|
| action={list} | (Required) |
| scap_scan_since={date} | (Optional) Show hosts that were last scanned for SCAP since a certain date and time. Hosts that were the target of a SCAP scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2018-07-01" or "2018-01-25T23:12:00Z". |
| no_scap_scan_since={date} | (Optional) Show hosts not scanned for SCAP since a certain date and time. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2018-07-01" or "2018-01-25T23:12:00Z". |

### Sample 1

Let us view the SCAP last scanned date without any filter for a host with 10.10.10.42 IP address.

API request:

```
curl -u "username:password" -H "X-Requested-With: "
"http://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&
ips=10.10.10.42&details=All"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/host_list_outp
```

```
ut.dtd">
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2018-10-25T05:37:41Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>724310</ID>
                <IP>10.10.10.42</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[10-10-10-42.bogus.tld]]>
                </DNS>
                <NETBIOS>
                    <![CDATA[SYS_10_10_10_42]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 8.1]]>
                </OS>
                <LAST_COMPLIANCE_SCAN_DATETIME>2018-10-
24T07:00:36Z</LAST_COMPLIANCE_SCAN_DATETIME>
                <LAST_SCAP_SCAN_DATETIME>2018-08-
29T08:44:54Z</LAST_SCAP_SCAN_DATETIME>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

### Sample 2

Let us view the hosts that were last scanned for SCAP since a certain date and time.

API request:

```
curl -u "username:password" -H "X-Requested-With:"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&i
ps=10.10.10.42&details=All&scap_scan_since=2018-08-29"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://10.114.69.157:46445/api/2.0/fo/asset/host/host_list_outpu
t.dtd">
```

```
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2018-10-25T05:39:13Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>724310</ID>
                <IP>10.10.10.42</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[10-10-10-42.bogus.tld]]>
                </DNS>
                <NETBIOS>
                    <![CDATA[SYS_10_10_10_42]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 8.1]]>
                </OS>
                <LAST_COMPLIANCE_SCAN_DATETIME>2018-10-
24T07:00:36Z</LAST_COMPLIANCE_SCAN_DATETIME>
                <LAST_SCAP_SCAN_DATETIME>2018-08-
29T08:44:54Z</LAST_SCAP_SCAN_DATETIME>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

### Sample 3

Let us view the hosts that were not scanned for SCAP since a certain date and time.

API request:

```
curl -u "username:password" -H "X-Requested-With:"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&
ips=10.10.10.42&details=All&no_scap_scan_since=2018-08-30"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://10.114.69.157:46445/api/2.0/fo/asset/host/host_list_outpu
t.dtd">
```

```
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2018-10-25T05:46:03Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>724310</ID>
                <IP>10.10.10.42</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[10-10-10-42.bogus.tld]]>
                </DNS>
                <NETBIOS>
                    <![CDATA[SYS_10_10_10_42]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 8.1]]>
                </OS>
                <LAST_COMPLIANCE_SCAN_DATETIME>2018-10-
24T07:00:36Z</LAST_COMPLIANCE_SCAN_DATETIME>
                <LAST_SCAP_SCAN_DATETIME>2018-08-
29T08:44:54Z</LAST_SCAP_SCAN_DATETIME>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

### Sample 4: Asset Search Report

API request:

```
curl -u "username:password" -H "X-Requested-With:"
"action=search&output_format=xml&asset_groups=Winodws+7+Scap&last_
scap_scan_days=300&last_scap_scan_modifier=within"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/"
```

XML output:

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

<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysguard.p04.eng.sjc01.qualys.com/asset_search_report_
v2.dtd">
```

```
<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[qualys]]></COMPANY>
  <USERNAME>POC Manager</USERNAME>
  <GENERATION_DATETIME>2018-11-06T00:42:13Z</GENERATION_DATETIME>
  <TOTAL>26</TOTAL>
  <FILTERS>
    <ASSET_GROUPS>
      <ASSET_GROUP_TITLE><![CDATA[Winodws 7
Scap]]></ASSET_GROUP_TITLE>
    </ASSET_GROUPS>
    <FILTER_LAST_SCAP_SCAN_DATE><![CDATA[Within
300]]></FILTER_LAST_SCAP_SCAN_DATE>
  </FILTERS>
</HEADER>

<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.10.10.10]]></IP>
    <TRACKING_METHOD>IP address</TRACKING_METHOD>
    <DNS><![CDATA[bridge.qualys.com]]></DNS>
    <NETBIOS><![CDATA[WIN7-10-10]]></NETBIOS>
    <OPERATING_SYSTEM><![CDATA[Windows 7 Ultimate 64 bit Edition
Service Pack 1]]></OPERATING_SYSTEM>
    <OS_CPE><![CDATA[cpe:/o:microsoft:windows_7::sp1:x64-
ultimate:]]></OS_CPE>
    <LAST_SCAN_DATE>2018-10-18T20:55:10Z</LAST_SCAN_DATE>
    <LAST_COMPLIANCE_SCAN_DATE>2018-09-
14T21:57:53Z</LAST_COMPLIANCE_SCAN_DATE>
    <LAST_SCAP_SCAN_DATE>2018-08-
28T10:57:06Z</LAST_SCAP_SCAN_DATE>
    <FIRST_FOUND_DATE>2018-04-03T23:18:26Z</FIRST_FOUND_DATE>
  </HOST>
```

DTD Update:

<platformURL>/api/2.0/fo/asset/host/host_list_output.dtd

```
<!-- QUALYS HOST_OUTPUT DTD -->
<!ELEMENT HOST_LIST_OUTPUT (REQUEST?,RESPONSE)>
...
<!ELEMENT HOST (ID, IP?, TRACKING_METHOD?, NETWORK_ID?,
```

```
                DNS?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?,
TAGS?, METADATA?,LAST_VULN_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?,
LAST_VM_SCANNED_DURATION?,
LAST_VM_AUTH_SCANNED_DATE?,LAST_VM_AUTH_SCANNED_DURATION?,
LAST_COMPLIANCE_SCAN_DATETIME?, LAST_SCAP_SCAN_DATETIME?, OWNER?,
COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT TAGS (TAG*)>
<!ELEMENT TAG (TAG_ID?, NAME?)>
<!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT LAST_VULN_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_COMPLIANCE_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_SCAP_SCAN_DATETIME (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>
...
```

# Host List Detection API - New Filters for Last Detection Tested Date

| | |
|---|---|
| APIs affected | /api/2.0/fo/asset/host/vm/detection |
| New or Updated API | Updated |
| DTD or XSD changes | No |

The Host List Detection API includes 4 new filters based on when detections were last tested on a host (as part of a full scan or partial scan). You can filter the list to show detections tested since or before a particular date or number of days. The XML output already includes the LAST TEST DATETIME.

New input parameters are described below.

| Parameter | Description |
|---|---|
| detection_last_tested_since={date} | (Optional) Show only detections that were last tested on or after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.<br><br>You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a date range.<br><br>This parameter cannot be specified in the same request as detection_last_tested_since_days. |
| detection_last_tested_since_days={value} | (Optional) Show only detections that were last tested within the number of days you specify. For example, show detections last tested in the past 10 days.<br><br>You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a specific date range.<br><br>This parameter cannot be specified in the same request as detection_last_tested_since. |

| Parameter | Description |
|---|---|
| detection_last_tested_before={date} | (Optional) Show only detections that were last tested before a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2018-07-01" or "2018-01-25T23:12:00Z".<br><br>You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.<br><br>This parameter cannot be specified in the same request as detection_last_tested_before_days. |
| detection_last_tested_before_days={value} | (Optional) Show only detections that were last tested before the number of days you specify. For example, show detections last tested more than 30 days ago.<br><br>You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.<br><br>This parameter cannot be specified in the same request as detection_last_tested_before. |

### Sample - Show Detections Last Tested Before Date

In this example, the output will only include detections last tested before July 15, 2018

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&network_ids=1000&status=Active,Fixed,New,Re-
Opened&ips=10.10.10.10&detection_last_tested_before=2018-07-15"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/h
ost_list_vm_detection_output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-10-25T04:51:46Z</DATETIME>
    <HOST_LIST>
```

```
      <HOST>
        <ID>736670</ID>
        <IP>10.10.10.10</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <NETWORK_ID>1000</NETWORK_ID>
        <OS><![CDATA[Linux 2.2-2.6]]></OS>
        <NETBIOS><![CDATA[STORE123]]></NETBIOS>
        <LAST_SCAN_DATETIME>2018-07-
13T06:28:15Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2018-07-
13T06:26:02Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>300</LAST_VM_SCANNED_DURATION>
        <DETECTION_LIST>
          <DETECTION>
            <QID>12500</QID>
            <TYPE>Potential</TYPE>
            <SEVERITY>3</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[QID: 12500 detected on port 80 over
TCP - Apache/2.2.14 (Ubuntu)QID: 12500 detected on port 443 over
TCP - Apache/2.2.14 (Ubuntu)]]></RESULTS>
            <STATUS>New</STATUS>
            <FIRST_FOUND_DATETIME>2018-07-
13T06:26:02Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2018-07-
13T06:26:02Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2018-07-
13T06:26:02Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2018-07-
13T06:28:15Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2018-07-
13T06:28:15Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
          <DETECTION>
            <QID>12529</QID>
            <TYPE>Potential</TYPE>
            <SEVERITY>3</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[QID: 12529 detected on port 80 over
```

```
TCP - Apache/2.2.14 (Ubuntu)QID: 12529 detected on port 443 over
TCP - Apache/2.2.14 (Ubuntu)]]></RESULTS>
            <STATUS>New</STATUS>
            <FIRST_FOUND_DATETIME>2018-07-
13T06:26:02Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2018-07-
13T06:26:02Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2018-07-
13T06:26:02Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2018-07-
13T06:28:15Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2018-07-
13T06:28:15Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
...
```

### Sample - Show Detections Last Tested Since Number of Days

In this example, the output will only include detections last tested in the past 185 days.

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&network_ids=1000&status=Active,Fixed,New,Re-
Opened&ips=10.10.10.7&detection_last_tested_since_days=185"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/h
ost_list_vm_detection_output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-10-25T04:52:58Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>736667</ID>
        <IP>10.10.10.7</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
```

```
        <NETWORK_ID>1000</NETWORK_ID>
        <OS><![CDATA[Linux 2.2-2.6]]></OS>
        <NETBIOS><![CDATA[STORE]]></NETBIOS>
        <LAST_SCAN_DATETIME>2018-07-
13T06:28:15Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2018-07-
13T06:26:02Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>300</LAST_VM_SCANNED_DURATION>
        <DETECTION_LIST>
          <DETECTION>
            <QID>27000</QID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>21</PORT>
            <PROTOCOL>tcp</PROTOCOL>
            <SSL>0</SSL>
            <STATUS>New</STATUS>
            <FIRST_FOUND_DATETIME>2018-07-
13T06:26:02Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2018-07-
13T06:26:02Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2018-07-
13T06:26:02Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2018-07-
13T06:28:15Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2018-07-
13T06:28:15Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
          <DETECTION>
            <QID>27001</QID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>21</PORT>
            <PROTOCOL>tcp</PROTOCOL>
            <SSL>0</SSL>
            <RESULTS><![CDATA[anonymous &lt;NO_PASSWORD&gt;ftp
&lt;NO_PASSWORD&gt;]]></RESULTS>
            <STATUS>New</STATUS>
            <FIRST_FOUND_DATETIME>2018-07-
```

```
13T06:26:02Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2018-07-
13T06:26:02Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2018-07-
13T06:26:02Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2018-07-
13T06:28:15Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2018-07-
13T06:28:15Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
...
```

### Additional Sample Requests

Show only detections last tested on or after August 1, 2018.

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&network_ids=1000&status=Active,Fixed,New,Re-
Opened&ips=10.10.10.7&detection_last_tested_since=2018-08-01"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

Show only detections last tested between August 1st and October 1st.

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&network_ids=1000&status=Active,Fixed,New,Re-
Opened&ips=10.10.10.7&detection_last_tested_since=2018-08-
01&detection_last_tested_before=2018-10-01"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/
```

Show only detections last tested between 15 days ago through 30 days ago.

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&network_ids=1000&status=Active,Fixed,New,Re-
Opened&ips=10.10.10.7&detection_last_tested_since_days=30&detectio
n_last_tested_before_days=15"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/
```

# OS Authentication Instance-based Technology Discovery

| | |
|---|---|
| APIs affected | /api/2.0/fo/scan/compliance |
| New or Updated API | Updated |
| DTD or XSD changes | Yes |

We can now collect technology data using the underlying OS technology without creating authentication records.

To list these results a new element OS_AUTH_BASED_TECHNOLOGY_LIST is now added to the COMPLIANCE_SCAN DTD and COMPLIANCE_SCAN_RESULT_OUTPUT DTD.

Below is the list of supported technologies:

Google Chrome

Internet Explorer (9, 10, 11)

IBM WebSphere MQ

Microsoft Office (2013, 2016)

Microsoft Office Access (2013, 2016)

Microsoft Office Excel (2013, 2016)

Microsoft Office Outlook (2013, 2016)

Microsoft Office PowerPoint (2013, 2016)

Microsoft Office Word (2013, 2016)

Mozilla Firefox

Splunk (6.x, 7.x)

### Sample - Scan Report (XML)

DTD Change:

```
<!-- QUALYS COMPLIANCE SCAN DTD -->
<!ELEMENT COMPLIANCE_SCAN (HEADER, ERROR?, AUTH_SCAN_ISSUES?,
APPENDIX)>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR
    number CDATA #IMPLIED
>
<!ELEMENT KEY (#PCDATA)>
<!ATTLIST KEY
    value CDATA #IMPLIED
>
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO,
USER_INFO, KEY+, ASSET_GROUPS?, OPTION_PROFILE?)>
<!ELEMENT NAME (#PCDATA)*>
<!ELEMENT GENERATION_DATETIME (#PCDATA)*>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY,
ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME?, ROLE)>
<!ELEMENT USERNAME (#PCDATA)*>
<!ELEMENT ROLE (#PCDATA)*>


<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED

>
<!ELEMENT AUTH_SCAN_ISSUES (AUTH_SCAN_FAILED*,
```

```
AUTH_SCAN_INSUFFICIENT*)>
<!ELEMENT AUTH_SCAN_FAILED (HOST_INFO*)>
<!ELEMENT AUTH_SCAN_INSUFFICIENT (HOST_INFO*)>
<!ELEMENT HOST_INFO (DNS, IP, NETBIOS, INSTANCE, CAUSE, NETWORK)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT CAUSE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>

<!ELEMENT APPENDIX (TARGET_HOSTS?, TARGET_DISTRIBUTION?,
AUTHENTICATION?, OS_AUTH_BASED_TECHNOLOGY_LIST?,
AUTH_DISCOVERY_INSTANCE_LIST?,
AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST?)>
<!ELEMENT TARGET_HOSTS (HOSTS_SCANNED?, EXCLUDED_HOSTS?,
HOSTS_NOT_ALIVE?, PAUSE_CANCEL_ACTION?, HOSTNAME_NOT_FOUND?,
HOSTS_SCAN_ABORTED?)>
<!ELEMENT HOSTS_SCANNED (#PCDATA)>
<!ELEMENT HOSTNAME_NOT_FOUND (#PCDATA)>
<!ELEMENT EXCLUDED_HOSTS (#PCDATA)>
<!ELEMENT HOSTS_NOT_ALIVE (#PCDATA)>
<!ELEMENT HOSTS_SCAN_ABORTED (#PCDATA)>
<!ELEMENT PAUSE_CANCEL_ACTION (HOSTS, ACTION, BY)>
<!ELEMENT ACTION (#PCDATA)>
<!ELEMENT BY (#PCDATA)>

<!ELEMENT TARGET_DISTRIBUTION (SCANNER+)>
<!ELEMENT SCANNER (NAME, HOSTS)>
<!ELEMENT HOSTS (#PCDATA)>


<!ELEMENT AUTHENTICATION (AUTH+)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE_LIST (AUTH_DISCOVERY_INSTANCE*)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST
(AUTH_DISCOVERY_INSTANCE_NOT_FOUND*)>
<!ELEMENT AUTH (TYPE?, (FAILED | SUCCESS | INSUFFICIENT)+)>
<!ELEMENT TYPE (#PCDATA)>

<!ELEMENT OS_AUTH_BASED_TECHNOLOGY_LIST (OS_AUTH_BASED_TECHNOLOGY*)>
<!ELEMENT OS_AUTH_BASED_TECHNOLOGY (TECHNOLOGY_FAMILY,
TECHNOLOGY_INSTANCE_LIST*)>
```

```
<!ELEMENT TECHNOLOGY_FAMILY (#PCDATA)>
<!ELEMENT TECHNOLOGY_INSTANCE_LIST (TECHNOLOGY_INSTANCE+)>
<!ELEMENT TECHNOLOGY_INSTANCE (TECHNOLOGY, INSTANCE_INFO_LIST*, IP)>
<!ELEMENT INSTANCE_INFO_LIST (INSTANCE_INFO*)>
<!ELEMENT TECHNOLOGY (#PCDATA)>
<!ELEMENT INSTANCE_INFO (#PCDATA)>
<!ATTLIST INSTANCE_INFO key CDATA #IMPLIED>

<!ELEMENT AUTH_DISCOVERY_INSTANCE (AUTH_TYPE, AUTH_PARAM_LIST?,
IP)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND (AUTH_TYPE, IP)>
<!ELEMENT AUTH_PARAM_LIST (AUTH_PARAM+)>
<!ELEMENT AUTH_TYPE (#PCDATA)>
<!ELEMENT AUTH_PARAM (#PCDATA)>
<!ATTLIST AUTH_PARAM name CDATA #IMPLIED>

<!ELEMENT FAILED (IP,INSTANCE?)>
<!ELEMENT SUCCESS (IP,INSTANCE?)>
<!ELEMENT INSUFFICIENT (IP,INSTANCE?)>
<!-- EOF -->
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_SCAN SYSTEM
"https://qualysapi.qualys.com/compliance_scan.dtd">
<COMPLIANCE_SCAN>
  <HEADER>
    <NAME><![CDATA[Compliance Scan Results]]></NAME>
    <GENERATION_DATETIME>2018-11-
07T00:38:05Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[Qualys, Inc.]]></NAME>
      <ADDRESS><![CDATA[919 E Hillsdale Blvd]]></ADDRESS>
      <CITY><![CDATA[Foster City]]></CITY>
      <STATE><![CDATA[California]]></STATE>
      <COUNTRY><![CDATA[United States of America]]></COUNTRY>
      <ZIP_CODE><![CDATA[94404]]></ZIP_CODE>
    </COMPANY_INFO>
    <USER_INFO>
      <NAME><![CDATA[Patrick Slimmer]]></NAME>
      <ROLE>Manager</ROLE>
    </USER_INFO>
```

```
    <KEY value="COMPANY"><![CDATA[Qualys, Inc.]]></KEY>
    <KEY value="DATE">2018-11-07T00:08:08Z</KEY>
    <KEY value="TITLE"><![CDATA[ScanWithAllTarget]]></KEY>
    <KEY value="TARGET">10.10.30.130, 10.10.34.123, 10.10.35.249,
10.10.36.126, 10.11.70.116</KEY>
    <KEY value="EXCLUDED_TARGET"><![CDATA[N/A]]></KEY>
    <KEY value="DURATION">00:22:02</KEY>
    <KEY value="SCAN_HOST">vs_seenu_ak-2 (Scanner 10.4.47-1,
Vulnerability Signatures 2.1.2111-1)</KEY>
    <KEY value="NBHOST_ALIVE">5</KEY>
    <KEY value="NBHOST_TOTAL">5</KEY>
    <KEY value="REPORT_TYPE">On-demand</KEY>
    <KEY value="OPTIONS">File Integrity Monitoring: Enabled,
Scanned Ports: Targeted Scan, Hosts to Scan in Parallel - External
Scanners: 15, Hosts to Scan in Parallel - Scanner Appliances: 30,
Total Processes to Run in Parallel: 10, HTTP Processes to Run in
Parallel: 10, Packet (Burst) Delay: Medium, Intensity: Normal,
Overall Performance: Normal, ICMP Host Discovery, Ignore RST
packets: Off, Ignore firewall-generated SYN-ACK packets: Off, Do
not send ACK or SYN-ACK packets during host discovery: Off</KEY>
    <KEY value="STATUS">FINISHED</KEY>
    <ASSET_GROUPS>
      <ASSET_GROUP>
        <ASSET_GROUP_TITLE><![CDATA[AG-
Gyan]]></ASSET_GROUP_TITLE>
      </ASSET_GROUP>
    </ASSET_GROUPS>
    <OPTION_PROFILE>
      <OPTION_PROFILE_TITLE
option_profile_default="0"><![CDATA[Initial PC
Options]]></OPTION_PROFILE_TITLE>
    </OPTION_PROFILE>
  </HEADER>
  <APPENDIX>
    <TARGET_HOSTS>
      <HOSTS_SCANNED>10.10.30.130, 10.10.34.123, 10.10.35.249,
10.10.36.126, 10.11.70.116</HOSTS_SCANNED>
    </TARGET_HOSTS>
    <TARGET_DISTRIBUTION>
      <SCANNER>
        <NAME><![CDATA[vs_seenu_ak-2]]></NAME>
        <HOSTS>10.10.30.130, 10.10.34.123, 10.10.35.249,
```

```
10.10.36.126, 10.11.70.116</HOSTS>
      </SCANNER>
    </TARGET_DISTRIBUTION>
    <AUTHENTICATION>
      <AUTH>
        <TYPE>Windows</TYPE>
        <SUCCESS>
          <IP>10.10.30.130, 10.10.34.123, 10.10.36.126</IP>
        </SUCCESS>
      </AUTH>
      <AUTH>
        <TYPE>SSH</TYPE>
        <SUCCESS>
          <IP>10.10.35.249, 10.11.70.116</IP>
        </SUCCESS>
      </AUTH>
      <AUTH>
        <TYPE>Apache Web Server</TYPE>
        <SUCCESS>
          <IP>10.10.35.249</IP>
          <INSTANCE><![CDATA[Apache
2.4:1:/etc/httpd/conf/httpd.conf]]></INSTANCE>
        </SUCCESS>
      </AUTH>
      <AUTH>
        <TYPE>MariaDB</TYPE>
        <SUCCESS>
          <IP>10.10.34.123</IP>
          <INSTANCE><![CDATA[Port: 3306, Database Name:
]]></INSTANCE>
        </SUCCESS>
      </AUTH>
      <AUTH>
        <TYPE>Tomcat Server</TYPE>
        <SUCCESS>
          <IP>10.10.35.249</IP>
          <INSTANCE><![CDATA[Apache TC 7 (Instance Path:
/usr/share/tomcat)]]></INSTANCE>
        </SUCCESS>
        <SUCCESS>
          <IP>10.10.35.249</IP>
          <INSTANCE><![CDATA[Apache TC 8 (Instance Path:
```

```
/opt/apache-tomcat-8.0.18/rapache-tomcat-8.0.18)]]></INSTANCE>
        </SUCCESS>
        <SUCCESS>
          <IP>10.10.35.249</IP>
          <INSTANCE><![CDATA[Apache TC 8 (Instance Path:
/root/apache-tomcat-8.5.20)]]></INSTANCE>
        </SUCCESS>
      </AUTH>
    </AUTHENTICATION>
    <OS_AUTH_BASED_TECHNOLOGY_LIST>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>IBM WebSphere MQ</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>IBM WebSphere MQ (Unix)</TECHNOLOGY>
            <INSTANCE_INFO_LIST>
              <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/mqm]]></INSTANCE_INFO>
            </INSTANCE_INFO_LIST>
            <IP>10.11.70.116</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Internet Explorer</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Internet Explorer 9</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.30.130</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Internet Explorer 10</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Internet Explorer 11</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.36.126</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
```

```
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Microsoft Office</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office 2013</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office 2016</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.36.126</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Microsoft Office
Access</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office Access 2013</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office Access 2016</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.36.126</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Microsoft Office
Excel</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office Excel 2013</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
```

```
            <TECHNOLOGY>Microsoft Office Excel 2016</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.36.126</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Microsoft Office
Outlook</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office Outlook 2013</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office Outlook 2016</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.36.126</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Microsoft Office
PowerPoint</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office PowerPoint
2013</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office PowerPoint
2016</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.36.126</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Microsoft Office
```

```
Word</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office Word 2013</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Microsoft Office Word 2016</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.36.126</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Mozilla Firefox</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Mozilla Firefox (Windows)</TECHNOLOGY>
            <INSTANCE_INFO_LIST />
            <IP>10.10.34.123</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
      <OS_AUTH_BASED_TECHNOLOGY>
        <TECHNOLOGY_FAMILY>Splunk</TECHNOLOGY_FAMILY>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Splunk 6.x (Unix)</TECHNOLOGY>
            <INSTANCE_INFO_LIST>
              <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/splunk6/splunk]]></INSTANCE_INFO>
            </INSTANCE_INFO_LIST>
            <IP>10.10.35.249</IP>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY>Splunk 7.x (Unix)</TECHNOLOGY>
            <INSTANCE_INFO_LIST>
              <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/splunk]]></INSTANCE_INFO>
            </INSTANCE_INFO_LIST>
```

```
            <IP>10.10.35.249</IP>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY>
    </OS_AUTH_BASED_TECHNOLOGY_LIST>
  </APPENDIX>
</COMPLIANCE_SCAN>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind.
Qualys makes no warranty that the information contained in this
report is complete or error-free. Copyright 2018, Qualys, Inc. //-
->
```

### Sample - Scan API

API request:

```
curl -u USERNAME:PASSWORD -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/?
action=fetch&scan_ref=compliance/1347709693.37303" >
apiOutputScanFetch.txt
```

DTD Change:

```
<!ELEMENT COMPLIANCE_SCAN_RESULT_OUTPUT (REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ATTLIST KEY
    value CDATA #IMPLIED
>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, COMPLIANCE_SCAN)>
<!ELEMENT COMPLIANCE_SCAN ((HEADER, ERROR?, AUTH_SCAN_ISSUES?,
APPENDIX)+)>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR
    number CDATA #IMPLIED
>
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO,
USER_INFO, KEY+, ASSET_GROUPS?, OPTION_PROFILE?)>
<!ELEMENT NAME (#PCDATA)*>
<!ELEMENT GENERATION_DATETIME (#PCDATA)*>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY,
ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
```

```
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME?, ROLE)>
<!ELEMENT USERNAME (#PCDATA)*>
<!ELEMENT ROLE (#PCDATA)*>

<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
<!ELEMENT AUTH_SCAN_ISSUES (AUTH_SCAN_FAILED*,
AUTH_SCAN_INSUFFICIENT*)>
<!ELEMENT AUTH_SCAN_FAILED (HOST_INFO*)>
<!ELEMENT AUTH_SCAN_INSUFFICIENT (HOST_INFO*)>
<!ELEMENT HOST_INFO (DNS, IP, NETBIOS, INSTANCE, CAUSE)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT CAUSE (#PCDATA)>

<!ELEMENT APPENDIX (TARGET_HOSTS?, TARGET_DISTRIBUTION?,
AUTHENTICATION?, OS_AUTH_BASED_TECHNOLOGY_LIST?,
AUTH_DISCOVERY_INSTANCE_LIST?,
AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST?)>
<!ELEMENT TARGET_HOSTS (HOSTS_SCANNED?, EXCLUDED_HOSTS?,
HOSTS_NOT_ALIVE?, PAUSE_CANCEL_ACTION?, HOSTNAME_NOT_FOUND?,
HOSTS_SCAN_ABORTED?)>
<!ELEMENT HOSTS_SCANNED (#PCDATA)>
<!ELEMENT HOSTNAME_NOT_FOUND (#PCDATA)>
<!ELEMENT EXCLUDED_HOSTS (#PCDATA)>
<!ELEMENT HOSTS_NOT_ALIVE (#PCDATA)>
<!ELEMENT HOSTS_SCAN_ABORTED (#PCDATA)>
<!ELEMENT PAUSE_CANCEL_ACTION (HOSTS, ACTION, BY)>
<!ELEMENT ACTION (#PCDATA)>
```

```
<!ELEMENT BY (#PCDATA)>

<!ELEMENT TARGET_DISTRIBUTION (SCANNER+)>
<!ELEMENT SCANNER (NAME, HOSTS)>
<!ELEMENT HOSTS (#PCDATA)>


<!ELEMENT AUTHENTICATION (AUTH+)>
<!ELEMENT AUTH (TYPE?, (FAILED | SUCCESS | INSUFFICIENT)+)>
<!ELEMENT TYPE (#PCDATA)>

<!ELEMENT OS_AUTH_BASED_TECHNOLOGY_LIST (OS_AUTH_BASED_TECHNOLOGY*)>
<!ELEMENT OS_AUTH_BASED_TECHNOLOGY (TECHNOLOGY_FAMILY,
TECHNOLOGY_INSTANCE_LIST*)>
<!ELEMENT TECHNOLOGY_FAMILY (#PCDATA)>
<!ELEMENT TECHNOLOGY_INSTANCE_LIST (TECHNOLOGY_INSTANCE+)>
<!ELEMENT TECHNOLOGY_INSTANCE (TECHNOLOGY, INSTANCE_INFO_LIST*, IP)>
<!ELEMENT INSTANCE_INFO_LIST (INSTANCE_INFO*)>
<!ELEMENT TECHNOLOGY (#PCDATA)>
<!ELEMENT INSTANCE_INFO (#PCDATA)>
<!ATTLIST INSTANCE_INFO key CDATA #IMPLIED>

<!ELEMENT AUTH_DISCOVERY_INSTANCE_LIST (AUTH_DISCOVERY_INSTANCE*)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE (AUTH_TYPE, AUTH_PARAM_LIST?,
IP)>

<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST
(AUTH_DISCOVERY_INSTANCE_NOT_FOUND*)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND (AUTH_TYPE, IP)>

<!ELEMENT AUTH_PARAM_LIST (AUTH_PARAM+)>
<!ELEMENT AUTH_TYPE (#PCDATA)>
<!ELEMENT AUTH_PARAM (#PCDATA)>
<!ATTLIST AUTH_PARAM name CDATA #IMPLIED>

<!ELEMENT FAILED (IP,INSTANCE?)>
<!ELEMENT SUCCESS (IP,INSTANCE?)>
<!ELEMENT INSUFFICIENT (IP,INSTANCE?)>
<!-- EOF -->
```

XML output:

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

```
<!DOCTYPE COMPLIANCE_SCAN_RESULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/complianc
e_scan_result_output.dtd">
<COMPLIANCE_SCAN_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-11-07T22:34:52Z</DATETIME>
    <COMPLIANCE_SCAN>
      <HEADER>
        <NAME><![CDATA[Compliance Scan Results]]></NAME>
        <GENERATION_DATETIME>2018-11-
07T22:34:53Z</GENERATION_DATETIME>
        <COMPANY_INFO>
          <NAME><![CDATA[Qualys, Inc.]]></NAME>
          <ADDRESS><![CDATA[919 E Hillsdale Blvd]]></ADDRESS>
          <CITY><![CDATA[Foster City]]></CITY>
          <STATE><![CDATA[California]]></STATE>
          <COUNTRY><![CDATA[United States of America]]></COUNTRY>
          <ZIP_CODE><![CDATA[94404]]></ZIP_CODE>
        </COMPANY_INFO>
        <USER_INFO>
          <NAME><![CDATA[Patrick Slimmer]]></NAME>
          <USERNAME>seenu_ak</USERNAME>
          <ROLE>Manager</ROLE>
        </USER_INFO>
        <KEY value="USERNAME">seenu_ak</KEY>
        <KEY value="COMPANY"><![CDATA[Qualys, Inc.]]></KEY>
        <KEY value="DATE">2018-11-07T00:08:08Z</KEY>
        <KEY value="TITLE"><![CDATA[ScanWithAllTarget]]></KEY>
        <KEY value="TARGET">10.10.30.130, 10.10.34.123,
10.10.35.249, 10.10.36.126, 10.11.70.116</KEY>
        <KEY value="EXCLUDED_TARGET"><![CDATA[N/A]]></KEY>
        <KEY value="DURATION">00:22:02</KEY>
        <KEY value="SCAN_HOST">vs_seenu_ak-2 (Scanner 10.4.47-1,
Vulnerability Signatures 2.1.2111-1)</KEY>
        <KEY value="NBHOST_ALIVE">5</KEY>
        <KEY value="NBHOST_TOTAL">5</KEY>
        <KEY value="REPORT_TYPE">On-demand</KEY>
        <KEY value="OPTIONS">File Integrity Monitoring: Enabled,
Scanned Ports: Targeted Scan, Hosts to Scan in Parallel - External
Scanners: 15, Hosts to Scan in Parallel - Scanner Appliances: 30,
Total Processes to Run in Parallel: 10, HTTP Processes to Run in
Parallel: 10, Packet (Burst) Delay: Medium, Intensity: Normal,
```

```
Overall Performance: Normal, ICMP Host Discovery, Ignore RST
packets: Off, Ignore firewall-generated SYN-ACK packets: Off, Do
not send ACK or SYN-ACK packets during host discovery: Off</KEY>
        <KEY value="STATUS">FINISHED</KEY>
        <ASSET_GROUPS>
          <ASSET_GROUP>
            <ASSET_GROUP_TITLE><![CDATA[AG-
Gyan]]></ASSET_GROUP_TITLE>
          </ASSET_GROUP>
        </ASSET_GROUPS>
        <OPTION_PROFILE>
          <OPTION_PROFILE_TITLE
option_profile_default="0"><![CDATA[Initial PC
Options]]></OPTION_PROFILE_TITLE>
        </OPTION_PROFILE>
      </HEADER>
      <APPENDIX>
        <TARGET_HOSTS>
          <HOSTS_SCANNED>10.10.30.130, 10.10.34.123, 10.10.35.249,
10.10.36.126, 10.11.70.116</HOSTS_SCANNED>
        </TARGET_HOSTS>
        <TARGET_DISTRIBUTION>
          <SCANNER>
            <NAME><![CDATA[vs_seenu_ak-2]]></NAME>
            <HOSTS>10.10.30.130, 10.10.34.123, 10.10.35.249,
10.10.36.126, 10.11.70.116</HOSTS>
          </SCANNER>
        </TARGET_DISTRIBUTION>
        <AUTHENTICATION>
          <AUTH>
            <TYPE>Windows</TYPE>
            <SUCCESS>
              <IP>10.10.30.130, 10.10.34.123, 10.10.36.126</IP>
            </SUCCESS>
          </AUTH>
          <AUTH>
            <TYPE>SSH</TYPE>
            <SUCCESS>
              <IP>10.10.35.249, 10.11.70.116</IP>
            </SUCCESS>
          </AUTH>
          <AUTH>
```

```
            <TYPE>Apache Web Server</TYPE>
            <SUCCESS>
              <IP>10.10.35.249</IP>
              <INSTANCE><![CDATA[Apache
2.4:1:/etc/httpd/conf/httpd.conf]]></INSTANCE>
            </SUCCESS>
          </AUTH>
          <AUTH>
            <TYPE>MariaDB</TYPE>
            <SUCCESS>
              <IP>10.10.34.123</IP>
              <INSTANCE><![CDATA[Port: 3306, Database Name:
]]></INSTANCE>
            </SUCCESS>
          </AUTH>
          <AUTH>
            <TYPE>Tomcat Server</TYPE>
            <SUCCESS>
              <IP>10.10.35.249</IP>
              <INSTANCE><![CDATA[Apache TC 7 (Instance Path:
/usr/share/tomcat)]]></INSTANCE>
            </SUCCESS>
            <SUCCESS>
              <IP>10.10.35.249</IP>
              <INSTANCE><![CDATA[Apache TC 8 (Instance Path:
/opt/apache-tomcat-8.0.18/rapache-tomcat-8.0.18)]]></INSTANCE>
            </SUCCESS>
            <SUCCESS>
              <IP>10.10.35.249</IP>
              <INSTANCE><![CDATA[Apache TC 8 (Instance Path:
/root/apache-tomcat-8.5.20)]]></INSTANCE>
            </SUCCESS>
          </AUTH>
        </AUTHENTICATION>
        <OS_AUTH_BASED_TECHNOLOGY_LIST>
         <OS_AUTH_BASED_TECHNOLOGY>
           <TECHNOLOGY_FAMILY>IBM WebSphere MQ</TECHNOLOGY_FAMILY>
           <TECHNOLOGY_INSTANCE_LIST>
             <TECHNOLOGY_INSTANCE>
               <TECHNOLOGY>IBM WebSphere MQ (Unix)</TECHNOLOGY>
               <INSTANCE_INFO_LIST>
                 <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/mqm]]></INSTANCE_INFO>
```

```
                    </INSTANCE_INFO_LIST>
                    <IP>10.11.70.116</IP>
                  </TECHNOLOGY_INSTANCE>
                </TECHNOLOGY_INSTANCE_LIST>
              </OS_AUTH_BASED_TECHNOLOGY>
               <OS_AUTH_BASED_TECHNOLOGY>
                 <TECHNOLOGY_FAMILY>Internet
Explorer</TECHNOLOGY_FAMILY>
                 <TECHNOLOGY_INSTANCE_LIST>
                   <TECHNOLOGY_INSTANCE>
                     <TECHNOLOGY>Internet Explorer 9</TECHNOLOGY>
                     <INSTANCE_INFO_LIST />
                     <IP>10.10.30.130</IP>
                   </TECHNOLOGY_INSTANCE>
                   <TECHNOLOGY_INSTANCE>
                     <TECHNOLOGY>Internet Explorer 10</TECHNOLOGY>
                     <INSTANCE_INFO_LIST />
                     <IP>10.10.34.123</IP>
                   </TECHNOLOGY_INSTANCE>
                   <TECHNOLOGY_INSTANCE>
                     <TECHNOLOGY>Internet Explorer 11</TECHNOLOGY>
                     <INSTANCE_INFO_LIST />
                     <IP>10.10.36.126</IP>
                   </TECHNOLOGY_INSTANCE>
                 </TECHNOLOGY_INSTANCE_LIST>
               </OS_AUTH_BASED_TECHNOLOGY>
               <OS_AUTH_BASED_TECHNOLOGY>
                <TECHNOLOGY_FAMILY>Microsoft Office</TECHNOLOGY_FAMILY>
                 <TECHNOLOGY_INSTANCE_LIST>
                   <TECHNOLOGY_INSTANCE>
                     <TECHNOLOGY>Microsoft Office 2013</TECHNOLOGY>
                     <INSTANCE_INFO_LIST />
                     <IP>10.10.34.123</IP>
                   </TECHNOLOGY_INSTANCE>
                   <TECHNOLOGY_INSTANCE>
                     <TECHNOLOGY>Microsoft Office 2016</TECHNOLOGY>
                     <INSTANCE_INFO_LIST />
                     <IP>10.10.36.126</IP>
                   </TECHNOLOGY_INSTANCE>
                 </TECHNOLOGY_INSTANCE_LIST>
               </OS_AUTH_BASED_TECHNOLOGY>
               <OS_AUTH_BASED_TECHNOLOGY>
```

```
            <TECHNOLOGY_FAMILY>Microsoft Office
Access</TECHNOLOGY_FAMILY>
            <TECHNOLOGY_INSTANCE_LIST>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office Access
2013</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.34.123</IP>
              </TECHNOLOGY_INSTANCE>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office Access
2016</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.36.126</IP>
              </TECHNOLOGY_INSTANCE>
            </TECHNOLOGY_INSTANCE_LIST>
          </OS_AUTH_BASED_TECHNOLOGY>
          <OS_AUTH_BASED_TECHNOLOGY>
            <TECHNOLOGY_FAMILY>Microsoft Office
Excel</TECHNOLOGY_FAMILY>
            <TECHNOLOGY_INSTANCE_LIST>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office Excel
2013</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.34.123</IP>
              </TECHNOLOGY_INSTANCE>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office Excel
2016</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.36.126</IP>
              </TECHNOLOGY_INSTANCE>
            </TECHNOLOGY_INSTANCE_LIST>
          </OS_AUTH_BASED_TECHNOLOGY>
          <OS_AUTH_BASED_TECHNOLOGY>
            <TECHNOLOGY_FAMILY>Microsoft Office
Outlook</TECHNOLOGY_FAMILY>
            <TECHNOLOGY_INSTANCE_LIST>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office Outlook
2013</TECHNOLOGY>
```

```
                <INSTANCE_INFO_LIST />
                <IP>10.10.34.123</IP>
              </TECHNOLOGY_INSTANCE>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office Outlook
2016</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.36.126</IP>
              </TECHNOLOGY_INSTANCE>
            </TECHNOLOGY_INSTANCE_LIST>
          </OS_AUTH_BASED_TECHNOLOGY>
          <OS_AUTH_BASED_TECHNOLOGY>
            <TECHNOLOGY_FAMILY>Microsoft Office
PowerPoint</TECHNOLOGY_FAMILY>
            <TECHNOLOGY_INSTANCE_LIST>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office PowerPoint
2013</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.34.123</IP>
              </TECHNOLOGY_INSTANCE>
              <TECHNOLOGY_INSTANCE>
                <TECHNOLOGY>Microsoft Office PowerPoint
2016</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.36.126</IP>
              </TECHNOLOGY_INSTANCE>
            </TECHNOLOGY_INSTANCE_LIST>
          </OS_AUTH_BASED_TECHNOLOGY>
          <OS_AUTH_BASED_TECHNOLOGY>
            <TECHNOLOGY_FAMILY>Microsoft Office
Word</TECHNOLOGY_FAMILY>
            <TECHNOLOGY_INSTANCE_LIST>
              <TECHNOLOGY_INSTANCE>
               <TECHNOLOGY>Microsoft Office Word 2013</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.34.123</IP>
              </TECHNOLOGY_INSTANCE>
              <TECHNOLOGY_INSTANCE>
               <TECHNOLOGY>Microsoft Office Word 2016</TECHNOLOGY>
                <INSTANCE_INFO_LIST />
                <IP>10.10.36.126</IP>
```

```
            </TECHNOLOGY_INSTANCE>
          </TECHNOLOGY_INSTANCE_LIST>
        </OS_AUTH_BASED_TECHNOLOGY>
        <OS_AUTH_BASED_TECHNOLOGY>
          <TECHNOLOGY_FAMILY>Mozilla Firefox</TECHNOLOGY_FAMILY>
          <TECHNOLOGY_INSTANCE_LIST>
            <TECHNOLOGY_INSTANCE>
              <TECHNOLOGY>Mozilla Firefox (Windows)</TECHNOLOGY>
              <INSTANCE_INFO_LIST />
              <IP>10.10.34.123</IP>
            </TECHNOLOGY_INSTANCE>
          </TECHNOLOGY_INSTANCE_LIST>
        </OS_AUTH_BASED_TECHNOLOGY>
        <OS_AUTH_BASED_TECHNOLOGY>
          <TECHNOLOGY_FAMILY>Splunk</TECHNOLOGY_FAMILY>
          <TECHNOLOGY_INSTANCE_LIST>
            <TECHNOLOGY_INSTANCE>
              <TECHNOLOGY>Splunk 6.x (Unix)</TECHNOLOGY>
              <INSTANCE_INFO_LIST>
                <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/splunk6/splunk]]></INSTANCE_INFO>
              </INSTANCE_INFO_LIST>
              <IP>10.10.35.249</IP>
            </TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_INSTANCE>
              <TECHNOLOGY>Splunk 7.x (Unix)</TECHNOLOGY>
              <INSTANCE_INFO_LIST>
                <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/splunk]]></INSTANCE_INFO>
              </INSTANCE_INFO_LIST>
              <IP>10.10.35.249</IP>
            </TECHNOLOGY_INSTANCE>
          </TECHNOLOGY_INSTANCE_LIST>
        </OS_AUTH_BASED_TECHNOLOGY>
      </OS_AUTH_BASED_TECHNOLOGY_LIST>
    </APPENDIX>
  </COMPLIANCE_SCAN>
</RESPONSE>
</COMPLIANCE_SCAN_RESULT_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind.
Qualys makes no warranty that the information contained in this
```

```
report is complete or error-free. Copyright 2018, Qualys, Inc. //-
->  //-->
```

### Sample - Authentication Report

DTD Change:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE AUTHENTICATION REPORT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_AUTHENTICATION_REPORT (ERROR | (HEADER,
(BUSINESS_UNIT_LIST | ASSET_GROUP_LIST | ASSET_TAG_LIST |
IPS_LIST), APPENDIX?))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO,
USER_INFO, FILTERS)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY,
ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME?, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!ELEMENT FILTERS (BUSINESS_UNIT_LIST | ASSET_GROUP_LIST |
ASSET_TAG_LIST | (IPS_LIST,  NETWORK?))>

<!ELEMENT BUSINESS_UNIT_LIST (BUSINESS_UNIT*)>
<!ELEMENT BUSINESS_UNIT
(NAME|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FAILED|AUTH_NOT_ATTEMPTED
|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_PERCENTAGE
|NOT_ATTEMPTED_PERCENTAGE|TECHNOLOGY_LIST)*>
<!ELEMENT AUTH_PASSED (#PCDATA)>
<!ELEMENT AUTH_INSUFFICIENT (#PCDATA)>
<!ELEMENT AUTH_TOTAL (#PCDATA)>
```

```
<!ELEMENT PASSED_PERCENTAGE (#PCDATA)>

<!ELEMENT ASSET_TAG_LIST ((INCLUDED_TAGS, EXCLUDED_TAGS?) |
ASSET_TAG)>
<!ELEMENT ASSET_TAG
(INCLUDED_TAGS|EXCLUDED_TAGS|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FA
ILED|AUTH_NOT_ATTEMPTED|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCE
NTAGE|FAILED_PERCENTAGE|NOT_ATTEMPTED_PERCENTAGE|TECHNOLOGY_LIST)*
>
<!ELEMENT INCLUDED_TAGS (TAG_ITEM+)>
<!ATTLIST INCLUDED_TAGS scope (any|all) #REQUIRED>
<!ELEMENT EXCLUDED_TAGS (TAG_ITEM+)>
<!ATTLIST EXCLUDED_TAGS scope (any|all) #REQUIRED>
<!ELEMENT TAG_ITEM (#PCDATA)>

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP*)>
<!ELEMENT ASSET_GROUP
(NAME|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FAILED|AUTH_NOT_ATTEMPTED
|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_PERCENTAGE
|NOT_ATTEMPTED_PERCENTAGE|TECHNOLOGY_LIST)*>

<!ELEMENT IPS_LIST (IPS+)>
<!ELEMENT IPS
(NAME|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FAILED|AUTH_NOT_ATTEMPTED
|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_PERCENTAGE
|NOT_ATTEMPTED_PERCENTAGE|TECHNOLOGY_LIST)*>

<!ELEMENT AUTH_FAILED (#PCDATA)>
<!ELEMENT AUTH_NOT_ATTEMPTED (#PCDATA)>
<!ELEMENT AUTH_NOT_INSTALLED (#PCDATA)>
<!ELEMENT FAILED_PERCENTAGE (#PCDATA)>
<!ELEMENT NOT_ATTEMPTED_PERCENTAGE (#PCDATA)>

<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY*)>
<!ELEMENT TECHNOLOGY (NAME, HOST_LIST)>
<!ELEMENT HOST_LIST (HOST*)>
<!ELEMENT HOST (TRACKING_METHOD, IP, DNS?, NETBIOS?,
HOST_TECHNOLOGY?, INSTANCE?, STATUS, CAUSE?, NETWORK?, OS?,
LAST_AUTH?, LAST_SUCCESS?)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
```

```
<!ELEMENT HOST_TECHNOLOGY (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT CAUSE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT LAST_AUTH (#PCDATA)>
<!ELEMENT LAST_SUCCESS (#PCDATA)>

<!ELEMENT APPENDIX (OS_AUTH_BASED_TECHNOLOGY_HOST_LIST?)>
<!ELEMENT OS_AUTH_BASED_TECHNOLOGY_HOST_LIST
(OS_AUTH_BASED_TECHNOLOGY_HOST*)>
<!ELEMENT OS_AUTH_BASED_TECHNOLOGY_HOST (IP, DNS, NETBIOS,
TRACKING_METHOD, NETWORK?, OS, LAST_AUTH, LAST_SUCCESS,
TECHNOLOGY_INSTANCE_LIST)>

<!ELEMENT TECHNOLOGY_INSTANCE_LIST (TECHNOLOGY_INSTANCE+)>
<!ELEMENT TECHNOLOGY_INSTANCE (TECHNOLOGY_NAME, INSTANCE_INFO_LIST?)>
<!ELEMENT INSTANCE_INFO_LIST (INSTANCE_INFO+)>

<!ELEMENT TECHNOLOGY_NAME (#PCDATA)>
<!ELEMENT INSTANCE_INFO (#PCDATA)>
<!ATTLIST INSTANCE_INFO key CDATA #IMPLIED>
...
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_AUTHENTICATION_REPORT SYSTEM
"https://qualysguard.p04.eng.sjc01.qualys.com/compliance_authentic
ation_report.dtd">
<COMPLIANCE_AUTHENTICATION_REPORT>
  <HEADER>
    <NAME><![CDATA[preAllIPAuthReport - 20181107 -
20181107]]></NAME>
    <GENERATION_DATETIME>2018-11-
07T22:24:49Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[Qualys, Inc.]]></NAME>
      <ADDRESS><![CDATA[919 E Hillsdale Blvd]]></ADDRESS>
      <CITY><![CDATA[Foster City]]></CITY>
      <STATE><![CDATA[California]]></STATE>
      <COUNTRY><![CDATA[United States of America]]></COUNTRY>
```

```
      <ZIP_CODE><![CDATA[94404]]></ZIP_CODE>
    </COMPANY_INFO>
    <USER_INFO>
      <NAME><![CDATA[Patrick Slimmer]]></NAME>
      <ROLE>Manager</ROLE>
    </USER_INFO>
    <FILTERS>
      <IPS_LIST>
        <IPS>
          <NAME><![CDATA[10.10.36.126]]></NAME>
        </IPS>
        <IPS>
          <NAME><![CDATA[10.10.30.130]]></NAME>
        </IPS>
        <IPS>
          <NAME><![CDATA[10.10.35.249]]></NAME>
        </IPS>
        <IPS>
          <NAME><![CDATA[10.10.34.123]]></NAME>
        </IPS>
        <IPS>
          <NAME><![CDATA[10.11.70.116]]></NAME>
        </IPS>
      </IPS_LIST>
    </FILTERS>
  </HEADER>
  <IPS_LIST>
    <IPS>
      <NAME><![CDATA[10.10.36.126]]></NAME>
      <AUTH_PASSED>1</AUTH_PASSED>
      <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
      <AUTH_FAILED>0</AUTH_FAILED>
      <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
      <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
      <AUTH_TOTAL>1</AUTH_TOTAL>
      <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
      <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
      <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
      <TECHNOLOGY_LIST>
        <TECHNOLOGY>
          <NAME><![CDATA[Windows]]></NAME>
```

```
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.36.126]]></IP>
              <DNS><![CDATA[comw10es]]></DNS>
              <NETBIOS><![CDATA[COMW10ES]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[Windows
10]]></HOST_TECHNOLOGY>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
      </TECHNOLOGY_LIST>
    </IPS>
    <IPS>
      <NAME><![CDATA[10.10.30.130]]></NAME>
      <AUTH_PASSED>1</AUTH_PASSED>
      <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
      <AUTH_FAILED>0</AUTH_FAILED>
      <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
      <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
      <AUTH_TOTAL>1</AUTH_TOTAL>
      <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
      <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
      <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
      <TECHNOLOGY_LIST>
        <TECHNOLOGY>
          <NAME><![CDATA[Windows]]></NAME>
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.30.130]]></IP>
              <DNS><![CDATA[com-30-130]]></DNS>
              <NETBIOS><![CDATA[COM-30-130]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[Windows
7]]></HOST_TECHNOLOGY>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
      </TECHNOLOGY_LIST>
```

```
    </IPS>
    <IPS>
      <NAME><![CDATA[10.10.35.249]]></NAME>
      <AUTH_PASSED>5</AUTH_PASSED>
      <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
      <AUTH_FAILED>0</AUTH_FAILED>
      <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
      <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
      <AUTH_TOTAL>5</AUTH_TOTAL>
      <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
      <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
      <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
      <TECHNOLOGY_LIST>
        <TECHNOLOGY>
          <NAME><![CDATA[Apache Web Server]]></NAME>
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.35.249]]></IP>
              <DNS><![CDATA[]]></DNS>
              <NETBIOS><![CDATA[]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[Apache HTTP Server
2.4.x]]></HOST_TECHNOLOGY>

<INSTANCE><![CDATA[/etc/httpd/conf/httpd.conf]]></INSTANCE>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
        <TECHNOLOGY>
          <NAME><![CDATA[Tomcat Server]]></NAME>
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.35.249]]></IP>
              <DNS><![CDATA[]]></DNS>
              <NETBIOS><![CDATA[]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[Apache Tomcat
8.x]]></HOST_TECHNOLOGY>
              <INSTANCE><![CDATA[Apache TC 8, Instance
directory=/root/apache-tomcat-8.5.20]]></INSTANCE>
              <STATUS><![CDATA[Passed]]></STATUS>
```

```
            </HOST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.35.249]]></IP>
              <DNS><![CDATA[]]></DNS>
              <NETBIOS><![CDATA[]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[Apache Tomcat
8.x]]></HOST_TECHNOLOGY>
              <INSTANCE><![CDATA[Apache TC 8, Instance
directory=/opt/apache-tomcat-8.0.18/rapache-tomcat-
8.0.18]]></INSTANCE>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.35.249]]></IP>
              <DNS><![CDATA[]]></DNS>
              <NETBIOS><![CDATA[]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[Apache Tomcat
7.x]]></HOST_TECHNOLOGY>
              <INSTANCE><![CDATA[Apache TC 7, Instance
directory=/usr/share/tomcat]]></INSTANCE>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
        <TECHNOLOGY>
          <NAME><![CDATA[Unix/Cisco/Checkpoint Firewall]]></NAME>
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.35.249]]></IP>
              <DNS><![CDATA[]]></DNS>
              <NETBIOS><![CDATA[]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[CentOS
7.x]]></HOST_TECHNOLOGY>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
      </TECHNOLOGY_LIST>
    </IPS>
```

```
    <IPS>
      <NAME><![CDATA[10.10.34.123]]></NAME>
      <AUTH_PASSED>2</AUTH_PASSED>
      <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
      <AUTH_FAILED>0</AUTH_FAILED>
      <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
      <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
      <AUTH_TOTAL>2</AUTH_TOTAL>
      <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
      <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
      <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
      <TECHNOLOGY_LIST>
        <TECHNOLOGY>
          <NAME><![CDATA[Windows]]></NAME>
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.34.123]]></IP>
              <DNS><![CDATA[cw2k12sd-34-123]]></DNS>
              <NETBIOS><![CDATA[CW2K12SD-34-123]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[Windows 2012
Server]]></HOST_TECHNOLOGY>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
        <TECHNOLOGY>
          <NAME><![CDATA[MariaDB]]></NAME>
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.34.123]]></IP>
              <DNS><![CDATA[cw2k12sd-34-123]]></DNS>
              <NETBIOS><![CDATA[CW2K12SD-34-123]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[MariaDB
10.x]]></HOST_TECHNOLOGY>
              <INSTANCE><![CDATA[Port=3306, Database
Name=mysql]]></INSTANCE>
              <STATUS><![CDATA[Passed]]></STATUS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
```

```
        </TECHNOLOGY_LIST>
      </IPS>
      <IPS>
        <NAME><![CDATA[10.11.70.116]]></NAME>
        <AUTH_PASSED>1</AUTH_PASSED>
        <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
        <AUTH_FAILED>0</AUTH_FAILED>
        <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
        <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
        <AUTH_TOTAL>1</AUTH_TOTAL>
        <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
        <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
        <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <NAME><![CDATA[Unix/Cisco/Checkpoint Firewall]]></NAME>
            <HOST_LIST>
              <HOST>
                <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
                <IP><![CDATA[10.11.70.116]]></IP>
                <DNS><![CDATA[]]></DNS>
                <NETBIOS><![CDATA[]]></NETBIOS>
                <HOST_TECHNOLOGY><![CDATA[CentOS
6.x]]></HOST_TECHNOLOGY>
                <STATUS><![CDATA[Passed]]></STATUS>
              </HOST>
            </HOST_LIST>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </IPS>
    </IPS_LIST>
    <APPENDIX>
      <OS_AUTH_BASED_TECHNOLOGY_HOST_LIST>
        <OS_AUTH_BASED_TECHNOLOGY_HOST>
          <IP>10.10.30.130</IP>
          <DNS>com-30-130</DNS>
          <NETBIOS>COM-30-130</NETBIOS>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <OS>Windows 7 Ultimate 64 bit Edition Service Pack 1</OS>
          <LAST_AUTH>11/06/2018</LAST_AUTH>
          <LAST_SUCCESS>11/06/2018</LAST_SUCCESS>
          <TECHNOLOGY_INSTANCE_LIST>
            <TECHNOLOGY_INSTANCE>
```

```
            <TECHNOLOGY_NAME>Internet Explorer 9</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY_HOST>
      <OS_AUTH_BASED_TECHNOLOGY_HOST>
        <IP>10.10.34.123</IP>
        <DNS>cw2k12sd-34-123</DNS>
        <NETBIOS>CW2K12SD-34-123</NETBIOS>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS>Windows Server 2012 Standard 64 bit Edition</OS>
        <LAST_AUTH>11/06/2018</LAST_AUTH>
        <LAST_SUCCESS>11/06/2018</LAST_SUCCESS>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office PowerPoint
2013</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office Outlook
2013</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
           <TECHNOLOGY_NAME>Microsoft Office Excel 2013</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office 2013</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Mozilla Firefox (Windows)</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office Access
2013</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Internet Explorer 10</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office Word 2013</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY_HOST>
      <OS_AUTH_BASED_TECHNOLOGY_HOST>
        <IP>10.10.35.249</IP>
        <DNS></DNS>
        <NETBIOS></NETBIOS>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS>CentOS Linux 7.0.1406</OS>
        <LAST_AUTH>11/06/2018</LAST_AUTH>
```

```
        <LAST_SUCCESS>11/06/2018</LAST_SUCCESS>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Splunk 6.x (Unix)</TECHNOLOGY_NAME>
            <INSTANCE_INFO_LIST>
              <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/splunk6/splunk]]></INSTANCE_INFO>
            </INSTANCE_INFO_LIST>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Splunk 7.x (Unix)</TECHNOLOGY_NAME>
            <INSTANCE_INFO_LIST>
              <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/splunk]]></INSTANCE_INFO>
            </INSTANCE_INFO_LIST>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY_HOST>
      <OS_AUTH_BASED_TECHNOLOGY_HOST>
        <IP>10.10.36.126</IP>
        <DNS>comw10es</DNS>
        <NETBIOS>COMW10ES</NETBIOS>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS>Windows 10 Enterprise 64 bit Edition</OS>
        <LAST_AUTH>11/06/2018</LAST_AUTH>
        <LAST_SUCCESS>11/06/2018</LAST_SUCCESS>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office 2016</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office Word 2016</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
           <TECHNOLOGY_NAME>Microsoft Office Excel 2016</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office Outlook
2016</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Internet Explorer 11</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office PowerPoint
2016</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>Microsoft Office Access
```

```
2016</TECHNOLOGY_NAME>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY_HOST>
      <OS_AUTH_BASED_TECHNOLOGY_HOST>
        <IP>10.11.70.116</IP>
        <DNS></DNS>
        <NETBIOS></NETBIOS>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS>CentOS 6.9</OS>
        <LAST_AUTH>11/06/2018</LAST_AUTH>
        <LAST_SUCCESS>11/06/2018</LAST_SUCCESS>
        <TECHNOLOGY_INSTANCE_LIST>
          <TECHNOLOGY_INSTANCE>
            <TECHNOLOGY_NAME>IBM WebSphere MQ (Unix)</TECHNOLOGY_NAME>
            <INSTANCE_INFO_LIST>
              <INSTANCE_INFO key="Installation
Path"><![CDATA[/opt/mqm]]></INSTANCE_INFO>
            </INSTANCE_INFO_LIST>
          </TECHNOLOGY_INSTANCE>
        </TECHNOLOGY_INSTANCE_LIST>
      </OS_AUTH_BASED_TECHNOLOGY_HOST>
    </OS_AUTH_BASED_TECHNOLOGY_HOST_LIST>
  </APPENDIX>
</COMPLIANCE_AUTHENTICATION_REPORT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind.
Qualys makes no warranty that the information contained in this
report is complete or error-free. Copyright 2018, Qualys, Inc. //-
->
```

## Sample CSV Report

Scroll down to the APPENDIX section and you'll see the Technology Instance information.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.10.35.249 | Tomcat Server | Apache Tomcat 8.x | Apache TC | 10.10.35.249 | | | IP | Passed | '- | | | | |
| 10.10.35.249 | Tomcat Server | Apache Tomcat 7.x | Apache TC | 10.10.35.249 | | | IP | Passed | '- | | | | |
| 10.10.35.249 | Apache Web Ser | Apache HTTP Serve | /etc/httpc | 10.10.35.249 | | | IP | Passed | '- | | | | |
| 10.10.35.249 | Unix/Cisco/Chec | CentOS 7.x | | 10.10.35.249 | | | IP | Passed | '- | | | | |
| 10.10.34.123 | Windows | Windows 2012 Server | | 10.10.34.123 | cw2k12sd- | CW2K12SI | IP | Passed | '- | | | | |
| 10.10.34.123 | MariaDB | MariaDB 10.x | Port=3306 | 10.10.34.123 | cw2k12sd- | CW2K12SI | IP | Passed | '- | | | | |
| 10.11.70.116 | Unix/Cisco/Chec | CentOS 6.x | | 10.11.70.116 | | | IP | Passed | '- | | | | |
| APPENDIX | | | | | | | | | | | | | |
| Targets with OS authentication-based technologies | | | | | | | | | | | | | |
| Host IP | DNS Hostname | NetBIOS Hostname | Tracking M | OS | Last Auth | Last Succe | Host Tech | Instance | | | | | |
| 10.10.30.130 | com-30-130 | COM-30-130 | IP | Windows 7 Ultin | 11/06/201 | 11/06/201 | Internet E | Internet Explorer 9 | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Access 2013 | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office PowerPoint 2013 | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Outlook 2013 | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Word 2013 | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office 2013 | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Internet E | Internet Explorer 10 | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Mozilla Fi | Mozilla Firefox (Windows) | | | | | |
| 10.10.34.123 | cw2k12sd-34-123 | CW2K12SD-34-123 | IP | Windows Server | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Excel 2013 | | | | | |
| 10.10.35.249 | | | IP | CentOS Linux 7.( | 11/06/201 | 11/06/201 | Splunk 6.x | Splunk 6.x (Unix) (Installation Path: /opt/splunk6/splunk) | | | | | |
| 10.10.35.249 | | | IP | CentOS Linux 7.( | 11/06/201 | 11/06/201 | Splunk 7.x | Splunk 7.x (Unix) (Installation Path: /opt/splunk) | | | | | |
| 10.10.36.126 | comqaw10es | COMQAW10ES | IP | Windows 10 Ent | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office 2016 | | | | | |
| 10.10.36.126 | comqaw10es | COMQAW10ES | IP | Windows 10 Ent | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Word 2016 | | | | | |
| 10.10.36.126 | comqaw10es | COMQAW10ES | IP | Windows 10 Ent | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Excel 2016 | | | | | |
| 10.10.36.126 | comqaw10es | COMQAW10ES | IP | Windows 10 Ent | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Outlook 2016 | | | | | |
| 10.10.36.126 | comqaw10es | COMQAW10ES | IP | Windows 10 Ent | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office PowerPoint 2016 | | | | | |
| 10.10.36.126 | comqaw10es | COMQAW10ES | IP | Windows 10 Ent | 11/06/201 | 11/06/201 | Microsoft | Microsoft Office Access 2016 | | | | | |
| 10.10.36.126 | comqaw10es | COMQAW10ES | IP | Windows 10 Ent | 11/06/201 | 11/06/201 | Internet E | Internet Explorer 11 | | | | | |
| 10.11.70.116 | | | IP | CentOS 6.9 | 11/06/201 | 11/06/201 | IBM WebS | IBM WebSphere MQ (Unix) (Installation Path: /opt/mqm) | | | | | |

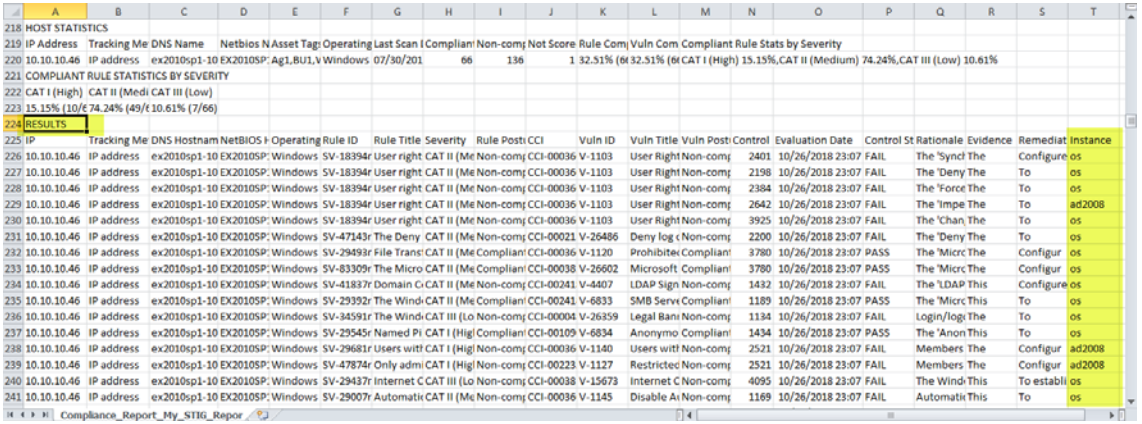
# New Instance column in STIG Report CSV

| | |
|---|---|
| APIs affected | N/A |
| New or Updated API | Updated (CSV output change only) |
| DTD or XSD changes | No |

A host can have multiple instances and you can now include the host instance in the STIG report. Simply choose “Instance” in the STIG report template from the UI to show this information in the CSV report output.

### Sample CSV Report

Scroll down to the RESULTS section and you'll see the new Instance column at the end.



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 218 | HOST STATISTICS | | | | | | | | | | | | | | | | | | | |
| 219 | IP Address | Tracking Me | DNS Name | Netbios N | Asset Tag | Operating | Last Scan I | Compliant | Non-comp | Not Score | Rule Com | Vuln Com | Compliant | Rule Stats by Severity | | | | | | |
| 220 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Ag1,BU1,V | Windows | 07/30/201 | 66 | 136 | 1 | 32.51% (6 | 32.51% (6 | CAT I (High) | 15.15%,CAT II (Medium) | | 74.24%,CAT III (Low) | | 10.61% | | |
| 221 | COMPLIANT RULE STATISTICS BY SEVERITY | | | | | | | | | | | | | | | | | | | |
| 222 | CAT I (High) | CAT II (Medi | CAT III (Low) | | | | | | | | | | | | | | | | | |
| 223 | 15.15% (10/6 | 74.24% (49/6 | 10.61% (7/66) | | | | | | | | | | | | | | | | | |
| 224 | RESULTS | | | | | | | | | | | | | | | | | | | |
| 225 | IP | Tracking Me | DNS Hostnam | NetBIOS H | Operating | Rule ID | Rule Title | Severity | Rule Posti | CCI | Vuln ID | Vuln Title | Vuln Posti | Control | Evaluation Date | Control St | Rationale | Evidence | Remediat | Instance |
| 226 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-18394r | User right | CAT II (Me | Non-comp | CCI-00036 | V-1103 | User Right | Non-comp | 2401 | 10/26/2018 23:07 | FAIL | The 'Synch | The | Configure | os |
| 227 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-18394r | User right | CAT II (Me | Non-comp | CCI-00036 | V-1103 | User Right | Non-comp | 2198 | 10/26/2018 23:07 | FAIL | The 'Deny | The | To | os |
| 228 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-18394r | User right | CAT II (Me | Non-comp | CCI-00036 | V-1103 | User Right | Non-comp | 2384 | 10/26/2018 23:07 | FAIL | The 'Force | The | To | os |
| 229 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-18394r | User right | CAT II (Me | Non-comp | CCI-00036 | V-1103 | User Right | Non-comp | 2642 | 10/26/2018 23:07 | FAIL | The 'Impe | The | To | ad2008 |
| 230 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-18394r | User right | CAT II (Me | Non-comp | CCI-00036 | V-1103 | User Right | Non-comp | 3925 | 10/26/2018 23:07 | FAIL | The 'Chan | The | To | os |
| 231 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-47143r | The Deny | CAT II (Me | Non-comp | CCI-00021 | V-26486 | Deny log ( | Non-comp | 2200 | 10/26/2018 23:07 | FAIL | The 'Deny | The | To | os |
| 232 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-29493r | File Trans | CAT II (Me | Compliant | CCI-00036 | V-1120 | Prohibited | Compliant | 3780 | 10/26/2018 23:07 | PASS | The 'Micro | The | Configur | os |
| 233 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-83309r | The Micro | CAT II (Me | Compliant | CCI-00038 | V-26602 | Microsoft | Compliant | 3780 | 10/26/2018 23:07 | PASS | The 'Micro | The | Configur | os |
| 234 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-41837r | Domain C | CAT II (Me | Non-comp | CCI-00241 | V-4407 | LDAP Sign | Non-comp | 1432 | 10/26/2018 23:07 | FAIL | The 'LDAP | This | Configure | os |
| 235 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-29392r | The Windo | CAT II (Me | Compliant | CCI-00241 | V-6833 | SMB Serve | Compliant | 1189 | 10/26/2018 23:07 | PASS | The 'Micro | This | To | os |
| 236 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-34591r | The Windo | CAT III (Lo | Non-comp | CCI-00004 | V-26359 | Legal Ban | Non-comp | 1134 | 10/26/2018 23:07 | FAIL | Login/logo | The | To | os |
| 237 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-29545r | Named Pi | CAT I (Hig | Compliant | CCI-00109 | V-6834 | Anonymo | Compliant | 1434 | 10/26/2018 23:07 | PASS | The 'Anon | This | To | os |
| 238 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-29681r | Users with | CAT I (Hig | Non-comp | CCI-00036 | V-1140 | Users with | Non-comp | 2521 | 10/26/2018 23:07 | FAIL | Members | The | Configur | ad2008 |
| 239 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-47874r | Only admi | CAT I (Hig | Non-comp | CCI-00223 | V-1127 | Restricted | Non-comp | 2521 | 10/26/2018 23:07 | FAIL | Members | The | Configur | ad2008 |
| 240 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-29437r | Internet C | CAT III (Lo | Non-comp | CCI-00038 | V-15673 | Internet C | Non-comp | 4095 | 10/26/2018 23:07 | FAIL | The Windo | This | To establi | os |
| 241 | 10.10.10.46 | IP address | ex2010sp1-10 | EX2010SP | Windows | SV-29007r | Automatic | CAT II (Me | Non-comp | CCI-00036 | V-1145 | Disable Au | Non-comp | 1169 | 10/26/2018 23:07 | FAIL | Automatic | This | To | os |

Compliance_Report_My_STIG_Repor

# New Search Filter Added to Scanner Appliance API

| | |
|---|---|
| APIs affected | /api/2.0/fo/appliance/ |
| New or Updated API | Updated |
| DTD or XSD changes | No |

You can now search scanner appliances by platform where scanners are deployed. You'll see the platform provider in the XML output when you also specify “include_cloud_info=1” and “output_mode=full” in the request.

Input Parameter:

| Parameter | Description |
|---|---|
| platform_provider | (Optional) Specify a platform to show scanners deployed on that platform. The valid values are: ec2, ec2_compat, gce, azure, vCenter.<br><br>ec2 - Amazon EC2, ec2_compat - OpenStack, gce - Google Cloud Platform, azure - Microsoft Azure Cloud Platform, vCenter - VMware vCenter |

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&type=virtual&platform_provider=ec2&include_cloud_info=1&outp
ut_mode=full"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

The output displays the scanners deployed on ec2 platform.

```
<?xml version="1.0" encoding="UTF-8"?>
...
 <IS_CLOUD_DEPLOYED>0</IS_CLOUD_DEPLOYED>
        <CLOUD_INFO>
          <PLATFORM_PROVIDER>ec2</PLATFORM_PROVIDER>
          <EC2_INFO>
            <INSTANCE_ID>i-02441120f4e14e32c</INSTANCE_ID>
            <INSTANCE_TYPE>m3.medium</INSTANCE_TYPE>
            <AMI_ID>ami-2d4ed53a</AMI_ID>
            <ACCOUNT_ID>205767712438</ACCOUNT_ID>
            <INSTANCE_REGION>US East (N. Virginia)</INSTANCE_REGION>
            <INSTANCE_AVAILABILITY_ZONE>us-east-
1c</INSTANCE_AVAILABILITY_ZONE>
            <INSTANCE_ZONE_TYPE>Classic</INSTANCE_ZONE_TYPE>
            <IP_ADDRESS_PRIVATE>10.181.43.219</IP_ADDRESS_PRIVATE>
```

```
            <HOSTNAME_PRIVATE>ip-10-181-43-
219.ec2.internal</HOSTNAME_PRIVATE>
            <API_PROXY_SETTINGS>
              <SETTING>Enabled</SETTING>
              <PROXY>
                <PROTOCOL>http</PROTOCOL>
                <IP_ADDRESS>1.1.1.1</IP_ADDRESS>
                <HOSTNAME>test_hostname.com</HOSTNAME>
                <PORT>234</PORT>
                <USER>*****</USER>
              </PROXY>
            </API_PROXY_SETTINGS>
          </EC2_INFO>...
...
```

# New API: List Superseding Patches for an Asset

| | |
|---|---|
| API affected | /api/2.0/fo/asset/patch/index.php |
| New or Updated APIs | New |
| DTD or XSD changes | Yes |

We have now introduced a new API: Patch Supersede API that lets you view the list of all superseding patches that will fix detections on a specific host.

### Input Parameters

The new input parameters are described below.

| Parameter | Description |
|---|---|
| host_id={value} | (Required) The output lists all the superseding patches that will fix the detections on a single host instance. Specify the ID for the host to include in the report. A valid host ID must be entered. |
| output_format=xml | (Optional) The output format: xml (the default) |

### Sample 1: Sample XML for inserting an HTTP header

API request:

```
curl -u "USERNAME:PASSWORD" -X "GET" -H "Content-Type: text/xml"
"host_id=136801&output_format=xml"
"https://qualysapi.qualys.com/api/2.0/fo/asset/patch/index.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE PATCH_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/patch/host_patches.
dtd">
<PATCH_LIST_OUTPUT>
  <RESPONSE>
    <SUBSCRIPTION_ID>3058</SUBSCRIPTION_ID>
    <HOST_ID>136801</HOST_ID>
    <IP>10.10.25.249</IP>
    <DNS><![CDATA[ora11107-25-249]]></DNS>
    <NETBIOS><![CDATA[ORA11107-25-249]]></NETBIOS>
    <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
    <OS_CPE><![CDATA[]]></OS_CPE>
    <NETWORK><![CDATA[Star Trek]]></NETWORK>
```

```
    <PATCH_INFO_LIST>
      <PATCH_INFO>
        <DETECTION_QIDS>
          <QID cve_ids=""><![CDATA[19883]]></QID>
        </DETECTION_QIDS>
        <PATCH_QID cve_ids=""><![CDATA[19883]]></PATCH_QID>
        <PATCH_SEVERITY>4</PATCH_SEVERITY>
       <PATCH_TITLE><![CDATA[Oracle 11.1.0.7 on Microsoft Windows
- General Update Multiple Issues (Patch #54)]]></PATCH_TITLE>
        <PATCH_VENDOR_ID><![CDATA[11.1.0.7 Patch 54 -
32bit,11.1.0.7 Patch 54 - 64bit]]></PATCH_VENDOR_ID>
        <PATCH_RELEASE_DATE>2013-10-15
00:00:00</PATCH_RELEASE_DATE>
        <PATCH_LINKS>
          <LINK
os_sw="Windows"><![CDATA[https://support.oracle.com/epmos/faces/ui
/patch/PatchDetail.jspx?patchId=17363759]]></LINK>
          <LINK
os_sw="Windows"><![CDATA[https://support.oracle.com/epmos/faces/ui
/patch/PatchDetail.jspx?patchId=17363760]]></LINK>
        </PATCH_LINKS>
      </PATCH_INFO>
    </PATCH_INFO_LIST>
  </RESPONSE>
</PATCH_LIST_OUTPUT>
```

### New DTD

<base_url>/api/2.0/fo/asset/patch/host_patches.dtd.

```
<!-- QUALYS PATCH_LIST_OUTPUT DTD -->
<!-- $Revision: $ -->
<!ELEMENT PATCH_LIST_OUTPUT (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>
```

```
<!ELEMENT RESPONSE (SUBSCRIPTION_ID, HOST_ID, IP, DNS, NETBIOS,
OS, OS_CPE, NETWORK?, PATCH_INFO_LIST)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT PATCH_INFO_LIST (PATCH_INFO+)>
<!ELEMENT PATCH_INFO (DETECTION_QIDS, PATCH_QID, PATCH_SEVERITY,
PATCH_TITLE, PATCH_VENDOR_ID, PATCH_RELEASE_DATE, PATCH_LINKS? )>
<!ELEMENT DETECTION_QIDS (QID+)>
<!ELEMENT QID (#PCDATA)>
<!ATTLIST QID cve_ids CDATA #IMPLIED>
<!ELEMENT PATCH_QID (#PCDATA)>
<!ATTLIST PATCH_QID cve_ids CDATA #IMPLIED>
<!ELEMENT PATCH_SEVERITY (#PCDATA)>
<!ELEMENT PATCH_TITLE (#PCDATA)>
<!ELEMENT PATCH_VENDOR_ID (#PCDATA)>
<!ELEMENT PATCH_RELEASE_DATE (#PCDATA)>
<!ELEMENT PATCH_LINKS (LINK+)>
<!ELEMENT LINK (#PCDATA)>
<!ATTLIST LINK os_sw CDATA #IMPLIED>
<!-- EOF -->
```

# New API: Scanner Details

| | |
|---|---|
| API affected | /api/2.0/fo/scan/scanner |
| New or Updated APIs | New |
| DTD or XSD changes | Yes |

The new Scanner Details API helps you identify the scanner used to scan a particular IP address at a given time. This is supported for vulnerability scans only. This new API is especially useful when you're scanning a large number of IPs using a pool of scanners and you're not sure which scanner was used to scan a particular host.

The XML output will show the IP address scanned with the scan reference number, scan date, the scanner identifier (external scanner or scanner appliance name), scanner type (extranet or appliance) and scanner software versions.

Permissions - Manager role is required

### Input Parameters

The new input parameters are described below.

| Parameter | Description |
|---|---|
| action=list | (Required) |
| scan_date_since={value} | (Required) Include scans started since a certain date. Specify the date in YYYY-MM-DD format. The date must be less than or equal to today's date. |
| scan_date_to={value} | (Optional) Include scans started up to a certain date. Specify the date in YYYY-MM-DD format. The date must be later than or equal to scan_date_since, and less than or equal to today's date. |
| ips={value} | (Required) The IP addresses you want scanner details for. You may enter a combination of IPs and ranges. Multiple entries are comma separated. |
| output_format=XML | (Optional) The output format: XML (the default) |

### Sample - List scanner details for certain IPs

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&ips=10.10.10.2-10.10.10.7,10.10.10.10
&scan_date_since=2018-05-24&scan_date_to=2018-09-28"
"https://qualysapi.qualys.com/api/2.0/fo/scan/scanner/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_SCANNERS_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/scanner/scanner_list
_output.dtd">
<IP_SCANNERS_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-11-08T21:49:51Z</DATETIME>
    <IP_SCANNERS_OUTPUT>
      <IP_SCANNED>
        <IP>10.10.10.7</IP>
        <SCAN_REF>scan/1527197914.13102</SCAN_REF>
        <SCAN_DATE>2018-05-24T21:39:08Z</SCAN_DATE>
        <SCANNER_IDENTIFIER>external scanner</SCANNER_IDENTIFIER>
        <SCANNER_TYPE>extranet</SCANNER_TYPE>
        <ML_VERSION>ML-9.7.20-1</ML_VERSION>
        <VULNSIGS_VERSION>VULNSIGS-2.4.182-2</VULNSIGS_VERSION>
      </IP_SCANNED>
      <IP_SCANNED>
        <IP>10.10.10.10</IP>
        <SCAN_REF>scan/1527197914.13102</SCAN_REF>
        <SCAN_DATE>2018-05-24T21:39:08Z</SCAN_DATE>
        <SCANNER_IDENTIFIER>external scanner</SCANNER_IDENTIFIER>
        <SCANNER_TYPE>extranet</SCANNER_TYPE>
        <ML_VERSION>ML-9.7.20-1</ML_VERSION>
        <VULNSIGS_VERSION>VULNSIGS-2.4.182-2</VULNSIGS_VERSION>
      </IP_SCANNED>
      <IP_SCANNED>
        <IP>10.10.10.7</IP>
        <SCAN_REF>scan/1538093810.64913</SCAN_REF>
        <SCAN_DATE>2018-09-28T00:19:25Z</SCAN_DATE>
        <SCANNER_IDENTIFIER>Esxi_4_Network</SCANNER_IDENTIFIER>
        <SCANNER_TYPE>appliance</SCANNER_TYPE>
        <ML_VERSION>ML-9.10.21-1</ML_VERSION>
        <VULNSIGS_VERSION>VULNSIGS-2.4.284-2</VULNSIGS_VERSION>
      </IP_SCANNED>
      <IP_SCANNED>
        <IP>10.10.10.10</IP>
        <SCAN_REF>scan/1538093810.64913</SCAN_REF>
        <SCAN_DATE>2018-09-28T00:19:25Z</SCAN_DATE>
        <SCANNER_IDENTIFIER>Esxi_4_Network</SCANNER_IDENTIFIER>
```

```
            <SCANNER_TYPE>appliance</SCANNER_TYPE>
            <ML_VERSION>ML-9.10.21-1</ML_VERSION>
            <VULNSIGS_VERSION>VULNSIGS-2.4.284-2</VULNSIGS_VERSION>
          </IP_SCANNED>
        </IP_SCANNERS_OUTPUT>
      </RESPONSE>
    </IP_SCANNERS_LIST_OUTPUT>
```

### New DTD

<base_url>/api/2.0/fo/scan/scanner/scanner_list_output.dtd

```
<!-- QUALYS SCANNER_LIST_OUTPUT.DTD -->
<!-- $Revision$ -->
<!ELEMENT IP_SCANNERS_LIST_OUTPUT (REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, IP_SCANNERS_OUTPUT?)>
<!ELEMENT IP_SCANNERS_OUTPUT (IP_SCANNED*)>
<!ELEMENT IP_SCANNED (IP, SCAN_REF, SCAN_DATE, SCANNER_IDENTIFIER,
SCANNER_TYPE, ML_VERSION, VULNSIGS_VERSION)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT SCAN_REF (#PCDATA)>
<!ELEMENT SCAN_DATE (#PCDATA)>
<!ELEMENT SCANNER_IDENTIFIER (#PCDATA)>
<!ELEMENT SCANNER_TYPE (#PCDATA)>
<!ELEMENT ML_VERSION (#PCDATA)>
<!ELEMENT VULNSIGS_VERSION (#PCDATA)>

<!-- EOF -->
```

# Agent UDC Support (coming soon!)

| | |
|---|---|
| APIs affected | /api/2.0/fo/compliance/control/?action=list<br>/api/2.0/fo/compliance/policy/?action=export |
| New or Updated API | Updated (DTD/XSD update only) |
| DTD changes | Yes |
| XSD changes | Yes |

New Agent UDC Support will be announced soon via the Qualys Technology blog once remaining components are released.

**DTD/XSD updates you'll see now:**

We've added the new USE_AGENT_ONLY and AUTO_UPDATE elements to the Control List Output DTD, Policy Export Output DTD and the ImportableControl.xsd schema.

**Updates you'll see once Agent UDC Support is available:**

The XML output may include the USE_AGENT_ONLY element for these Windows and Unix control types: Directory Search Control and Directory Integrity Control.

The XML output may include the AUTO_UPDATE element for these Windows and Unix control types: File Integrity Control and Directory Integrity Control.

USE_AGENT_ONLY has a value of 1 in the XML output when the "Use agent scan only" option is enabled for the control. When enabled, we'll evaluate the control using scan data collected from a cloud agent scan only. USE_AGENT_ONLY has a value of 0 when this option is not enabled for the control.

AUTO_UPDATE has a value of 1 in the XML output when the "Auto update expected value" option is enabled for the control. When enabled, we'll replace the control's expected value for posture evaluation with the actual value collected from the cloud agent scan. AUTO_UPDATE has a value of 0 when this option is not enabled for the control.

## List Compliance Controls

We added the new USE_AGENT_ONLY and AUTO_UPDATE elements to the XML output and updated the DTD.

API request:

```
curl -u username:password -H "X-Requested-With: curl" -d
"action=list&ids=100023"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML output:

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

```
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-10-05T10:23:54Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100023</ID>
        <UPDATE_DATE>2018-11-16T06:27:14Z</UPDATE_DATE>
        <CREATED_DATE>2018-11-16T06:27:14Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Directory Integrity Check]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Windows Directory Integrity
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[test]]></COMMENT>
        <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
        <AUTO_UPDATE>1</AUTO_UPDATE>
        <IGNORE_ERROR>0</IGNORE_ERROR>
...
```

DTD update:

DTD: <platform>/api/2.0/fo/compliance/control/control_list_output.dtd

```
<!-- QUALYS CONTROL_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT CONTROL_LIST_OUTPUT (REQUEST?,RESPONSE)>
...
<!ELEMENT RESPONSE (DATETIME, (CONTROL_LIST|ID_SET)?, WARNING?)>
<!ELEMENT CONTROL_LIST (CONTROL+)>
<!ELEMENT CONTROL (ID, UPDATE_DATE, CREATED_DATE, CATEGORY, SUB_CATEGORY,
STATEMENT, CRITICALITY?, DEPRECATED?, DEPRECATED_DATE?,
CHECK_TYPE?, COMMENT?, USE_AGENT_ONLY?, AUTO_UPDATE?, IGNORE_ERROR?,
IGNORE_ITEM_NOT_FOUND?, SCAN_PARAMETERS?, TECHNOLOGY_LIST,
FRAMEWORK_LIST?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)>
<!ELEMENT CREATED_DATE (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT SUB_CATEGORY (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
```

```
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT DEPRECATED (#PCDATA)>
<!ELEMENT DEPRECATED_DATE (#PCDATA)>
<!ELEMENT CHECK_TYPE (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT USE_AGENT_ONLY (#PCDATA)>
<!ELEMENT AUTO_UPDATE (#PCDATA)>
<!ELEMENT IGNORE_ERROR (#PCDATA)>
<!ELEMENT IGNORE_ITEM_NOT_FOUND (#PCDATA)>
...
```

## Export Policy to XML

You can export a compliance policy from your account to an XML file. You must specify the input parameter show_user_controls=1 to include UDCs in the output.

API request:

```
curl -u username:password -H "X-Requested-With: curl" -d
"action=export&id=1448425&show_user_controls=1&show_appendix=0"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/">UDCWIND.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_export_
output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-10-05T10:41:43Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[Windows_Linux_UDC_Policy]]></TITLE>
    <EXPORTED><![CDATA[2018-10-05T10:41:43Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="3">
        <TECHNOLOGY>
            <ID>45</ID>
            <NAME>Red Hat Enterprise Linux 6.x</NAME>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>52</ID>
            <NAME>AIX 7.x</NAME>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>81</ID>
            <NAME>Red Hat Enterprise Linux 7.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
```

```
        <SECTIONS total="1">
            <SECTION>
                <NUMBER>1</NUMBER>
                <HEADING><![CDATA[ddd]]></HEADING>
                <CONTROLS total="4">
                    <USER_DEFINED_CONTROL>
                        <ID>100041</ID>
                        <UDC_ID>929a8c4e-5057-e3f3-8225-e92d4076f499</UDC_ID>
                        <CHECK_TYPE>Unix Directory Search Check</CHECK_TYPE>
                        <CATEGORY>
                            <ID>3</ID>
                          <NAME><![CDATA[Access Control Requirements]]></NAME>
                        </CATEGORY>
                        <SUB_CATEGORY>
                            <ID>1010</ID>
                            <NAME><![CDATA[Account Creation/User
    Management]]></NAME>
                        </SUB_CATEGORY>
                        <STATEMENT><![CDATA[Directory Search]]></STATEMENT>
                        <CRITICALITY>
                            <LABEL><![CDATA[SERIOUS]]></LABEL>
                            <VALUE>3</VALUE>
                        </CRITICALITY>
                        <COMMENT><![CDATA[]]></COMMENT>
                        <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
                        <AUTO_UPDATE>0</AUTO_UPDATE>
                        <IGNORE_ERROR>0</IGNORE_ERROR>
    ...
```

DTD update:

DTD: <platform>/api/2.0/fo/compliance/policy/policy_export_output.dtd

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->
<!ELEMENT POLICY_EXPORT_OUTPUT (REQUEST?, RESPONSE)>
...
<!ELEMENT USER_DEFINED_CONTROL (ID, UDC_ID, CHECK_TYPE, CATEGORY,
SUB_CATEGORY, STATEMENT, CRITICALITY?, COMMENT?, USE_AGENT_ONLY?,
AUTO_UPDATE?, IGNORE_ERROR, IGNORE_ITEM_NOT_FOUND?, SCAN_PARAMETERS,
REFERENCE_TEXT?, TECHNOLOGIES, REFERENCE_LIST)>
<!ELEMENT UDC_ID (#PCDATA)>
<!ELEMENT CHECK_TYPE (#PCDATA)>

<!ELEMENT CATEGORY (ID, NAME)>
<!ELEMENT SUB_CATEGORY (ID, NAME)>

<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT USE_AGENT_ONLY (#PCDATA)>
```

```
<!ELEMENT AUTO_UPDATE (#PCDATA)>
<!ELEMENT IGNORE_ERROR (#PCDATA)>
<!ELEMENT IGNORE_ITEM_NOT_FOUND (#PCDATA)>
...
```

## Export Control to XML

When you export a Windows or Unix Directory Search Control or Directory Integrity Control from your account to XML you'll see USE_AGENT_ONLY in the XML output.

When you export a Windows or Unix File Integrity Control or Directory Integrity Control from your account to XML you'll see AUTO_UPDATE in the XML output.

XML output:

```
<CONTROL_LIST total="1">
    <CONTROL>
        <ID>100027</ID>
        <UDC_ID>aac7a25a-67e9-7ca1-838c-03e98981451f</UDC_ID>
        <CHECK_TYPE>Unix Directory Search Check</CHECK_TYPE>
        <CATEGORY>
            <ID>3</ID>
            <NAME><![CDATA[Access Control Requirements]]></NAME>
        </CATEGORY>
        <SUB_CATEGORY>
            <ID>1010</ID>
            <NAME><![CDATA[Account Creation/User Management]]></NAME>
        </SUB_CATEGORY>
        <STATEMENT><![CDATA[Directory Search-RHEL_Linux_UDC]]></STATEMENT>
        <CRITICALITY>
            <LABEL><![CDATA[SERIOUS]]></LABEL>
            <VALUE>3</VALUE>
        </CRITICALITY>
        <COMMENT><![CDATA[]]></COMMENT>
        <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
        <AUTO_UPDATE>0</AUTO_UPDATE>
        <IGNORE_ERROR>0</IGNORE_ERROR>
...
```

Schema update:

The ImportableControl.xsd schema is used when importing and exporting controls. It was updated to include the new elements USE_AGENT_ONLY and AUTO_UPDATE.

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

...
    <xs:element name="CONTROL">
```

```
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ID" minOccurs="0" maxOccurs="1" />
                <xs:element ref="UDC_ID" minOccurs="0" maxOccurs="1" />
                <xs:element ref="CHECK_TYPE" maxOccurs="1" />
                <xs:element ref="CATEGORY" minOccurs="0" maxOccurs="1" />
               <xs:element ref="SUB_CATEGORY" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="STATEMENT" maxOccurs="1" />
                <xs:element ref="CRITICALITY" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="COMMENT" minOccurs="0" maxOccurs="1" />
                <xs:element ref="USE_AGENT_ONLY" minOccurs="0"
maxOccurs="1" />
               <xs:element ref="AUTO_UPDATE" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="IGNORE_ERROR" maxOccurs="1" />
                <xs:element ref="IGNORE_ITEM_NOT_FOUND" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="SCAN_PARAMETERS" maxOccurs="1" />
                <xs:element ref="TECHNOLOGY_LIST" maxOccurs="1" />
                <xs:element ref="REFERENCE_LIST" maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
...
    <xs:element name="USE_AGENT_ONLY">
        <xs:simpleType>
            <xs:restriction base="xs:integer">
                <xs:enumeration value="0" />
                <xs:enumeration value="1" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
...
<xs:element name="AUTO_UPDATE">
        <xs:simpleType>
            <xs:restriction base="xs:integer">
                <xs:enumeration value="0" />
                <xs:enumeration value="1" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
...
```