Qualys API Release Notes

Version 8.10.2

Qualys 8.10.2 includes improvements to the Qualys API, giving you more ways to integrate your programs and API calls with Qualys Vulnerability Management (VM) and Qualys Policy Compliance (PC). Looking for our API user guides? Just log in to your Qualys account and go to Help > Resources.

What's New

Introducing New User Administrator Role

VM - Host List Detection API - Processed Timestamp

VM - Scan Results DTD - Optional elements added

PC - Enable/Disable Controls in Policies

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.

Introducing New User Administrator Role

Manager users can now create a new user role: User administrator. Users with this role will only have access to users, assets groups, business units and distribution groups.

What can User Administrator do?

-Create and edit all types of users except Manager and User Administrator.
-View asset groups and list of users.

The user administrator does not have permission to delete: users, business units, distribution groups, or asset groups. Only a Manager user can create, edit and delete a user administrator.

Once a user is assigned a user administrator role, you cannot change the role of the user. Promotion or demotion of user role is not permitted. Similarly, you cannot assign user administrator role to an existing user.

Examples

Create Administrator User

To create a new user with user administrator role, set the parameter user_role=administrator.

API Request:

```
curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl" -d
"action=add&send_email=0&user_role=administrator&business_unit=Unassigned
&first_name=Chris&last_name=Woods&title=Security+Consultant&phone=2126667
777&fax=2126667778&email=chris@mycompany.com&address1=500+Char
les_Avenue&address2=Suite+1260&city=New+York&country=United+States+of+Ame
rica&state=New+York&zip_code=10004&time_zone_code=US-NY"
"https://qualysapi.qualys.com/msp/user.php"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE USER_OUTPUT SYSTEM
"https://qualysapi.qualys.com/user_output.dtd">
<USER_OUTPUT>
 <API name="user.php" username="Chris_woods" at="2017-07-27T04:31:23Z" />
 <RETURN status="SUCCESS">
   <MESSAGE>Chris_woods user has been successfully created.</MESSAGE>
 </RETURN>
 <USER>
   <USER_LOGIN>Chris_woods</USER_LOGIN>
   <PASSWORD>12345</PASSWORD>
 </USER>
```

```
</USER_OUTPUT>
```

List Administrator User

You can view the list of all administrator users in your account.

API Request:

```
curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/msp/user_list.php"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
...
<USER>
     <USER_LOGIN>Chris_woods</USER_LOGIN>
     <USER_ID>147501</USER_ID>
     <CONTACT_INFO>
       <FIRSTNAME><![CDATA[Chris]]></FIRSTNAME>
       <LASTNAME><![CDATA[Woods]]></LASTNAME>
       <TITLE><![CDATA[Security Consultant]]></TITLE>
       <PHONE><![CDATA[2126667777]]></PHONE>
       <FAX><![CDATA[2126667778]]></FAX>
       <EMAIL><![CDATA[chris@mycompany.com]]></EMAIL>
       <COMPANY><![CDATA[Network]]></COMPANY>
       <ADDRESS1><![CDATA[500 Charles_Avenue]]></ADDRESS1>
       <ADDRESS2><![CDATA[Suite 1260]]></ADDRESS2>
       <CITY><![CDATA[New York]]></CITY>
       <COUNTRY>United States of America</COUNTRY>
       <STATE>New+York</STATE>
       <ZIP_CODE><![CDATA[10004]]></ZIP_CODE>
       <TIME_ZONE_CODE><![CDATA[US-NY]]></TIME_ZONE_CODE>
     </CONTACT_INFO>
     <USER_STATUS>Active</USER_STATUS>
     <CREATION_DATE>2017-07-27T04:31:23Z</CREATION_DATE>
     <LAST_LOGIN_DATE>N/A</LAST_LOGIN_DATE>
     <USER_ROLE>User Administrator</USER_ROLE>
     <BUSINESS_UNIT><![CDATA[Unassigned]]></BUSINESS_UNIT>
     <UNIT_MANAGER_POC>0</UNIT_MANAGER_POC>
     <MANAGER_POC>0</MANAGER_POC>
     <UI_INTERFACE_STYLE>standard_blue</UI_INTERFACE_STYLE>
     <PERMISSIONS>
       <CREATE_OPTION_PROFILES>0</CREATE_OPTION_PROFILES>
       <PURGE_INFO>0</PURGE_INFO>
       <ADD_ASSETS>0</ADD_ASSETS>
       <EDIT_REMEDIATION_POLICY>0</EDIT_REMEDIATION_POLICY>
       <EDIT_AUTH_RECORDS>0</EDIT_AUTH_RECORDS>
```

```
        </PERMISSIONS>
        <NOTIFICATIONS>
          <LATEST_VULN>weekly</LATEST_VULN>
          <MAP>ags</MAP>
          <SCAN>none</SCAN>
          <DAILY_TICKETS>0</DAILY_TICKETS>
        </NOTIFICATIONS>
      </USER>
....
```

VM - Host List Detection API - Processed Timestamp

The Host List Detection API v2 (../api/2.0/fo/asset/host/vm/detection/) now supports processed timestamp for each detection. You can now filter detections that were processed before/after a specific date using dectection_processed_before and dectection_processed_after parameters.

Parameter	Description
action=list	(Required) GET or POST method may be used.
dectection_processed_before={date}	(Optional) Show only detections which are processed before a certain date and time. Specify the date in YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
dectection_processed_after={date}	(Optional) Show only detections which are processed after a certain date and time. Specify the date in YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.

DTD update:

```
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
<!ELEMENT HOST_LIST_VM_DETECTION_OUTPUT (REQUEST?,RESPONSE)>
...
<!ELEMENT DETECTION_LIST (DETECTION+)>
<!ELEMENT DETECTION (QID, TYPE, SEVERITY?, PORT?, PROTOCOL?, FQDN?, SSL?,
INSTANCE?,RESULTS?, STATUS?,FIRST_FOUND_DATETIME?,
LAST_FOUND_DATETIME?,TIMES_FOUND?,LAST_TEST_DATETIME?,
LAST_UPDATE_DATETIME?,LAST_FIXED_DATETIME?,
FIRST_REOPENED_DATETIME?, LAST_REOPENED_DATETIME?, TIMES_REOPENED?,
SERVICE?, IS_IGNORED?, IS_DISABLED?, AFFECT_RUNNING_KERNEL?,
LAST_PROCESSED_DATETIME? )>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT RESULTS (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!ELEMENT LAST_TEST_DATETIME (#PCDATA)>
<!ELEMENT LAST_UPDATE_DATETIME (#PCDATA)>
```

```
<!ELEMENT LAST_FIXED_DATETIME (#PCDATA)>
<!ELEMENT FIRST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT LAST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT TIMES_REOPENED (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT IS_IGNORED (#PCDATA)>
<!ELEMENT IS_DISABLED (#PCDATA)>
<!ELEMENT AFFECT_RUNNING_KERNEL (#PCDATA)>
<!ELEMENT LAST_PROCESSED_DATETIME (#PCDATA)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->
```

Example

API request:

```
curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl" -d
"action=list&ips=10.10.10.28&detection_processed_before=2017-07-
31&detection_processed_after=2017-07-30&status=New,Active,Re-
Opened,Fixed"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

XML output:

```
...
<DETECTION>
           <QID>38094</QID>
           <TYPE>Potential</TYPE>
           <SEVERITY>2</SEVERITY>
           <PORT>3389</PORT>
           <PROTOCOL>tcp</PROTOCOL>
           <SSL>0</SSL>
           <RESULTS><![CDATA[Detected service win_remote_desktop and os
WINDOWS XP SERVICE PACK 2-3]]></RESULTS>
           <STATUS>Active</STATUS>
           <FIRST_FOUND_DATETIME>2016-10-
02T11:47:17Z</FIRST_FOUND_DATETIME>
         <LAST_FOUND_DATETIME>2017-07-30T15:31:07Z</LAST_FOUND_DATETIME>
           <TIMES_FOUND>431</TIMES_FOUND>
           <LAST_TEST_DATETIME>2017-07-30T15:31:07Z</LAST_TEST_DATETIME>
           <LAST_UPDATE_DATETIME>2017-07-
30T15:31:29Z</LAST_UPDATE_DATETIME>
         <LAST_FIXED_DATETIME>2017-07-30T15:30:25Z</LAST_FIXED_DATETIME>
           <IS_IGNORED>0</IS_IGNORED>
           <IS_DISABLED>0</IS_DISABLED>
           <LAST_PROCESSED_DATETIME>2017-07-
30T15:31:29Z</LAST_PROCESSED_DATETIME>
```

```
          </DETECTION>
          <DETECTION>
            <QID>38229</QID>
            <TYPE>Potential</TYPE>
            <SEVERITY>3</SEVERITY>
            <PORT>3389</PORT>
            <PROTOCOL>tcp</PROTOCOL>
            <SSL>0</SSL>
          <RESULTS><![CDATA[3 consecutive connection attempts failed after
a total number of 43 successful connections.]]></RESULTS>
            <STATUS>Fixed</STATUS>
            <FIRST_FOUND_DATETIME>2016-11-
20T17:11:34Z</FIRST_FOUND_DATETIME>
          <LAST_FOUND_DATETIME>2017-07-01T15:28:25Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>13</TIMES_FOUND>
            <LAST_TEST_DATETIME>2017-07-30T15:31:07Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2017-07-
30T15:31:30Z</LAST_UPDATE_DATETIME>
          <LAST_FIXED_DATETIME>2017-07-01T15:28:56Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2017-07-
30T15:31:29Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
```

VM - Scan Results DTD - Optional elements added

We've added 2 optional elements to Scan Results DTD (scan-1.dtd) for internal use. Users will not see these elements in scan results XML output, unless the QRDI Vulnerabilities Beta feature is enabled for the subscription.

New scan-1.dtd:

New optional elements RESULT_DEBUG and RESULT_ERRORS appear in bold below.

```
<!-- QUALYS SCAN DTD -->
<!ELEMENT SCAN ((HEADER | ERROR | IP)+)>
<!ATTLIST SCAN
    value CDATA #REQUIRED
>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR
    number CDATA #IMPLIED
>
<!-- INFORMATION ABOUT THE SCAN -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, ASSET_TAG_LIST?, OPTION_PROFILE?)>
<!ELEMENT KEY (#PCDATA)>
<!ATTLIST KEY
    value CDATA #IMPLIED
>

<!-- NAME of the asset group with the TYPE attribute with possible values
of (DEFAULT | EXTERNAL | ISCANNER) -->
<!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
>

<!-- TAGSET -->
<!ELEMENT ASSET_TAG_LIST (INCLUDED_TAGS?, EXCLUDED_TAGS?)>
<!ELEMENT INCLUDED_TAGS (ASSET_TAG+)>
<!ELEMENT EXCLUDED_TAGS (ASSET_TAG+)>
<!ELEMENT ASSET_TAG (#PCDATA)>
<!ATTLIST INCLUDED_TAGS scope (any|all) #REQUIRED>
<!ATTLIST EXCLUDED_TAGS scope (any|all) #REQUIRED>

<!-- IP -->
<!ELEMENT IP (OS?, OS_CPE?, NETBIOS_HOSTNAME?, INFOS?, SERVICES?, VULNS?,
PRACTICES?, NETWORK?)>
<!ATTLIST IP
```

```
    value CDATA #REQUIRED
    name CDATA #IMPLIED
    status CDATA #IMPLIED
>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT NETBIOS_HOSTNAME (#PCDATA)>
<!-- CATEGORIES OF INFO, SERVICE, VULN or PRACTICE -->
<!ELEMENT CAT (INFO+ | SERVICE+ | VULN+ | PRACTICE+)>
<!ATTLIST CAT
    value CDATA #REQUIRED
    fqdn CDATA #IMPLIED
    port CDATA #IMPLIED
    protocol CDATA #IMPLIED
    misc CDATA #IMPLIED
>
<!-- IP INFORMATIONS -->
<!ELEMENT INFOS (CAT)+>
<!ELEMENT INFO (TITLE, LAST_UPDATE?, PCI_FLAG, INSTANCE?,
                VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?,
                DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?,
CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?, COMPLIANCE?,
CORRELATION?, RESULT?, RESULT_ERRORS?, RESULT_DEBUG?)>
<!ATTLIST INFO
    severity CDATA #IMPLIED
    standard-severity CDATA #IMPLIED
    number CDATA #IMPLIED
>
<!-- MAP OF SERVICES -->
<!ELEMENT SERVICES (CAT)+>
<!ELEMENT SERVICE (TITLE, LAST_UPDATE?, PCI_FLAG, INSTANCE?,
VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?, DIAGNOSIS?,
DIAGNOSIS_COMMENT?, CONSEQUENCE?, CONSEQUENCE_COMMENT?, SOLUTION?,
SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, RESULT?)>
<!ATTLIST SERVICE
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
    number CDATA #IMPLIED
>
<!-- VULNERABILITIES -->
<!ELEMENT VULNS (CAT)+>
<!ELEMENT VULN (TITLE, LAST_UPDATE?, CVSS_BASE?,
CVSS_TEMPORAL?,CVSS3_BASE?, CVSS3_TEMPORAL?, PCI_FLAG, INSTANCE?,
                VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?,
                DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?,
CONSEQUENCE_COMMENT?,SOLUTION?, SOLUTION_COMMENT?, COMPLIANCE?,
CORRELATION?, RESULT?, RESULT_ERRORS?, RESULT_DEBUG?)>
<!-- number is Qualys numeric ID -->
```

```
<!-- cveid is the CVE identification code (if any) -->
<!-- severity is Qualys severity level 1 to 5 (possibly customized)  -->
<!-- standard-severity is the original Qualys severity level 1 to 5 if it
has been customized by the user -->
<!ATTLIST VULN
    number CDATA #REQUIRED
    cveid CDATA #IMPLIED
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
>

<!-- Required Element -->

<!ELEMENT TITLE (#PCDATA)>

<!-- Optional Elements -->

<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>

<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS3_BASE (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL (#PCDATA)>
<!ELEMENT PCI_FLAG (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
<!ELEMENT VENDOR_REFERENCE (ID,URL)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (ID,URL)>

<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID+)>
<!ELEMENT BUGTRAQ_ID (ID,URL)>

<!ELEMENT DIAGNOSIS (#PCDATA)>
<!ELEMENT DIAGNOSIS_COMMENT (#PCDATA)>
<!ELEMENT CONSEQUENCE (#PCDATA)>
<!ELEMENT CONSEQUENCE_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
```

```
COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!ELEMENT REF (#PCDATA)>
<!ELEMENT DESC (#PCDATA)>
<!ELEMENT LINK (#PCDATA)>

<!ELEMENT MALWARE (MW_SRC)+>
<!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
<!ELEMENT MW_LIST (MW_INFO)+>
<!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?,
MW_LINK?)>
<!ELEMENT MW_ID (#PCDATA)>
<!ELEMENT MW_TYPE (#PCDATA)>
<!ELEMENT MW_PLATFORM (#PCDATA)>
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>

<!ELEMENT INSTANCE (#PCDATA)>

<!-- if format is set to "table" -->
<!-- tab '\t' is the col separator -->
<!-- and new line '\n' is the end of row -->
<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT format CDATA #IMPLIED>

<!ELEMENT RESULT_ERRORS (#PCDATA)>

<!ELEMENT RESULT_DEBUG (#PCDATA)>

<!-- SECURITY TIPS -->
<!ELEMENT PRACTICES (CAT+)>
<!ELEMENT PRACTICE (TITLE, LAST_UPDATE?, CVSS_BASE?, CVSS_TEMPORAL?,
CVSS3_BASE?, CVSS3_TEMPORAL?, PCI_FLAG, INSTANCE?,
VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?, DIAGNOSIS?,
DIAGNOSIS_COMMENT?, CONSEQUENCE?, CONSEQUENCE_COMMENT?, SOLUTION?,
SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, RESULT?, RESULT_ERRORS?,
RESULT_DEBUG?)>
<!ATTLIST PRACTICE
    number CDATA #REQUIRED
```

```
            cveid CDATA #IMPLIED
            severity CDATA #REQUIRED
            standard-severity CDATA #IMPLIED
        >

        <!-- EOF -->
```

PC - Enable/Disable Controls in Policies

This release gives users the ability to enable/disable controls for policies. We've updated the Policy Import/Export APIs to support this capability.

Policy Export output - The new tag <IS_CONTROL_DISABLE> was added to the policy export output and the policy_export_output.dtd has been updated. This tag indicates whether a control is disabled (value set to 1) or enabled (value set to 0).

Policy Export API

Sample shows how to export a policy with controls that are enabled/disabled.

API request:

```
curl -u "USER:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=export&id=156059&show_appendix=1&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

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>2017-08-09T19:59:56Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[Windows for control active inactive]]></TITLE>
    <EXPORTED><![CDATA[2017-08-09T19:59:55Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>1</ID>
            <NAME>Windows XP desktop</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="3">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[First Section]]></HEADING>
            <CONTROLS total="5">
                <CONTROL>
                    <ID>1045</ID>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
```

```
                        </CRITICALITY>
                       <IS_CONTROL_DISABLE><![CDATA[1]]></IS_CONTROL_DISABLE>
                        <TECHNOLOGIES total="1">
                            <TECHNOLOGY>
                                <ID>1</ID>
                                <NAME>Windows XP desktop</NAME>

<EVALUATE><CTRL><DP><K>services.general.clipbook</K><OP>ge</OP><V>0</V><F
V set="0">161803399999999</FV><FV set="0">2</FV><FV set="0">3</FV><FV
set="1">314159265358979</FV><FV set="1">4</FV></DP></CTRL></EVALUATE>
                            </TECHNOLOGY>
                        </TECHNOLOGIES>
                    </CONTROL>
                    <CONTROL>
                        <ID>1048</ID>
                        <CRITICALITY>
                            <LABEL><![CDATA[CRITICAL]]></LABEL>
                            <VALUE>4</VALUE>
                        </CRITICALITY>
                       <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                        <TECHNOLOGIES total="1">
                            <TECHNOLOGY>
                                <ID>1</ID>
                                <NAME>Windows XP desktop</NAME>

<EVALUATE><CTRL><DP><K>secman.system.clearpageonshut</K><OP>eq</OP><V>1</
V><FV set="1">0</FV><FV set="0">1</FV><FV
set="0">314159265358979</FV></DP></CTRL></EVALUATE>
                            </TECHNOLOGY>
                        </TECHNOLOGIES>
                    </CONTROL>
                    <CONTROL>
                        <ID>1052</ID>
                        <CRITICALITY>
                            <LABEL><![CDATA[CRITICAL]]></LABEL>
                            <VALUE>4</VALUE>
                        </CRITICALITY>
                       <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                        <TECHNOLOGIES total="1">
                            <TECHNOLOGY>
                                <ID>1</ID>
                                <NAME>Windows XP desktop</NAME>

<EVALUATE><CTRL><DP><K>accessctrl.devices.allowformatejectremovabledevice
</K><OP>eq</OP><V>0</V><FV set="1">0</FV><FV set="1">1</FV><FV
set="1">2</FV><FV set="1">314159265358979</FV></DP></CTRL></EVALUATE>
                            </TECHNOLOGY>
                        </TECHNOLOGIES>
                    </CONTROL>
```

```
                <CONTROL>
                    <ID>1060</ID>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
                    </CRITICALITY>
                   <IS_CONTROL_DISABLE><![CDATA[1]]></IS_CONTROL_DISABLE>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>1</ID>
                       <NAME>Windows XP desktop</NAME>
<EVALUATE><CTRL><DP><K>services.remoteaccess.netmeetingremotedesktop</K><
OP>in</OP><V>4:161803399999999:314159265358979</V><FV set="1">2</FV><FV
set="1">3</FV><FV set="1">314159265358979</FV><FV
set="1">4</FV></DP></CTRL></EVALUATE>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                </CONTROL>
...
```

DTD update:

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->

<!ELEMENT POLICY_EXPORT_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, POLICY)>
<!ELEMENT POLICY (TITLE, DESCRIPTION?, LOCKED?, EXPORTED, COVER_PAGE?,
STATUS?, TECHNOLOGIES, SECTIONS, APPENDIX?)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT DESCRIPTION (#PCDATA)>
<!ELEMENT LOCKED (#PCDATA)>
<!ELEMENT EXPORTED (#PCDATA)>
<!ELEMENT COVER_PAGE (#PCDATA)>

<!ELEMENT SECTIONS (SECTION*)>
<!ATTLIST SECTIONS total CDATA #IMPLIED>
```

```
<!ELEMENT SECTION (NUMBER, HEADING, CONTROLS)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT HEADING (#PCDATA)>

<!ELEMENT CONTROLS ((CONTROL|USER_DEFINED_CONTROL)*)>
<!ATTLIST CONTROLS total CDATA #IMPLIED>
<!ELEMENT CONTROL (ID, CRITICALITY?, IS_CONTROL_DISABLE?,
REFERENCE_TEXT?, TECHNOLOGIES)>
<!ELEMENT ID (#PCDATA)>

<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT IS_CONTROL_DISABLE (#PCDATA)>
<!ELEMENT REFERENCE_TEXT (#PCDATA)>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT TECHNOLOGIES (TECHNOLOGY*)>
<!ATTLIST TECHNOLOGIES total CDATA #IMPLIED>
<!ELEMENT TECHNOLOGY (ID, NAME?, EVALUATE?, RATIONALE?, DATAPOINT?,
USE_SCAN_VALUE?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT EVALUATE (CTRL*)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT CTRL (AND|OR|NOT|DP)+>
<!ELEMENT AND (AND|OR|NOT|DP)+>
<!ELEMENT OR (AND|OR|NOT|DP)+>
<!ELEMENT NOT (AND|OR|NOT|DP)+>
<!ELEMENT DP (K|OP|CD|L|V|FV)+>
<!ELEMENT K (#PCDATA)>
<!ELEMENT OP (#PCDATA)>
<!ELEMENT CD (#PCDATA)>
<!ELEMENT L (#PCDATA)>
<!ELEMENT V (#PCDATA)>
<!ELEMENT FV (#PCDATA)>
<!ATTLIST FV set CDATA #IMPLIED>
...
```

Policy Import API

Sample shows how to import a policy with controls that are enabled/disabled.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo2" -H Content-
Type:text/xml --data-binary "@Policy_Import.xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=import
&title=API_Import_IDPolicy_withUDC_15022047"
```

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>2017-08-09T20:05:11Z</DATETIME>
    <TEXT>Successfully imported compliance policy</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>156208</VALUE>
      </ITEM>
      <ITEM>
        <KEY>TITLE</KEY>
        <VALUE>API_Import_IDPolicy_withUDC_15022047</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```