Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.14

September 13, 2021 (Updated October 1, 2021)

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

Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API server URL for Qualys US Platform 1 (https://qualysapi.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

New Scan Parameters to Exclude Users and Groups from Unix Directory Integrity and Directory Search UDCs (Agent Only)

APIs affected	/api/2.0/fo/compliance/control/?action=list /api/2.0/fo/compliance/policy/?action=export /api/2.0/fo/compliance/policy/?action=import
New or Updated API	Updated
DTD or XSD changes	Yes

We've introduced 2 new scan parameters in the Unix Directory Integrity UDC and Unix Directory Search UDC. In previous releases, you were able to provide a list of users and groups to find files owned by those users/groups. Now you can find files owned by users/groups and exclude them. Simply choose the new "Exclude the user(s)" and "Exclude group(s)" options under Scan Parameters > File Owner in the UDC. Note that the exclude options are only supported by Cloud Agent. The scan data for the control evaluation is collected by the agent and then filtered by the agent.

Control List - Unix Directory Search UDC

When you list a Unix Directory Search UDC, you'll see the new scan parameters in the XML output with a value of true or false, indicating whether these options are enabled.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&ids=100045&details=All"
"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>2021-08-17T07:37:42Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100045</ID>
        <UPDATE_DATE>2021-08-17T07:31:10Z</UPDATE_DATE>
        <CREATED_DATE>2021-08-16T09:47:57Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[DS with exclude user and grp]]></STATEMENT>
        <CRITICALITY>
```

```
            <LABEL><![CDATA[MEDIUM]]></LABEL>
            <VALUE>2</VALUE>
          </CRITICALITY>
          <CHECK_TYPE><![CDATA[Unix Directory Search Check]]></CHECK_TYPE>
          <COMMENT><![CDATA[comment]]></COMMENT>
          <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
          <IGNORE_ERROR>0</IGNORE_ERROR>
          <SCAN_PARAMETERS>
              <BASE_DIR><![CDATA[/usr/]]></BASE_DIR>
              <SHOULD_DESCEND><![CDATA[false]]></SHOULD_DESCEND>
              <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>
              <FOLLOW_SYMLINK><![CDATA[false]]></FOLLOW_SYMLINK>
              <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
              <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
              <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
              <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
              <PERMISSIONS>
                  <SPECIAL>
                      <USER>any</USER>
                      <GROUP>any</GROUP>
                      <DELETION>any</DELETION>
                  </SPECIAL>
                  <USER>
                      <READ>any</READ>
                      <WRITE>any</WRITE>
                      <EXECUTE>any</EXECUTE>
                  </USER>
                  <GROUP>
                      <READ>any</READ>
                      <WRITE>any</WRITE>
                      <EXECUTE>any</EXECUTE>
                  </GROUP>
                  <OTHER>
                      <READ>any</READ>
                      <WRITE>any</WRITE>
                      <EXECUTE>any</EXECUTE>
                  </OTHER>
              </PERMISSIONS>
              <PERM_COND><![CDATA[all]]></PERM_COND>
              <TYPE_MATCH><![CDATA[d,f,l]]></TYPE_MATCH>
              <USER_OWNER><![CDATA[Ashuds]]></USER_OWNER>
              <GROUP_OWNER><![CDATA[Ashuds]]></GROUP_OWNER>
              <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
              <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE_
SEARCH>
              <EXCLUDE_USER_OWNER><![CDATA[true]]></EXCLUDE_USER_OWNER>
              <EXCLUDE_GROUP_OWNER><![CDATA[true]]></EXCLUDE_GROUP_OWNER>
```

```
            <DATA_TYPE>String List</DATA_TYPE>
            <DESCRIPTION><![CDATA[desc]]></DESCRIPTION>
          </SCAN_PARAMETERS>
          <TECHNOLOGY_LIST>
            <TECHNOLOGY>
              <ID>80</ID>
              <NAME>CentOS 7.x</NAME>
              <RATIONALE><![CDATA[rational]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
                  <OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[ashu]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
          </TECHNOLOGY_LIST>
        </CONTROL>
      </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Control List - Unix Directory Integrity UDC

When you list a Unix Directory Integrity UDC, you'll see the new scan parameters in the XML output with a value of true or false, indicating whether these options are enabled.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&ids=100046&details=All"
"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>2021-08-17T07:41:45Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100046</ID>
        <UPDATE_DATE>2021-08-17T07:31:51Z</UPDATE_DATE>
        <CREATED_DATE>2021-08-16T09:53:07Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
```

```
        <STATEMENT><![CDATA[DI exclude user and grp]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[CRITICAL]]></LABEL>
          <VALUE>4</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Unix Directory Integrity
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[comment]]></COMMENT>
        <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
        <AUTO_UPDATE>0</AUTO_UPDATE>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <SCAN_PARAMETERS>
            <BASE_DIR><![CDATA[/etc/]]></BASE_DIR>
            <SHOULD_DESCEND><![CDATA[false]]></SHOULD_DESCEND>

<INTEGRITY_CHECK_DEPTH_LIMIT><![CDATA[10]]></INTEGRITY_CHECK_DEPTH_LIMIT>
            <FOLLOW_SYMLINK><![CDATA[false]]></FOLLOW_SYMLINK>
            <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
            <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
            <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
            <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
            <TYPE_MATCH><![CDATA[f,l]]></TYPE_MATCH>
            <USER_OWNER><![CDATA[tanuDI]]></USER_OWNER>
            <GROUP_OWNER><![CDATA[tanuDI]]></GROUP_OWNER>

<INTEGRITY_CHECK_TIME_LIMIT><![CDATA[600]]></INTEGRITY_CHECK_TIME_LIMIT>

<INTEGRITY_CHECK_MATCH_LIMIT><![CDATA[512]]></INTEGRITY_CHECK_MATCH_LIMIT
>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE_
SEARCH>
            <EXCLUDE_USER_OWNER><![CDATA[true]]></EXCLUDE_USER_OWNER>
            <EXCLUDE_GROUP_OWNER><![CDATA[true]]></EXCLUDE_GROUP_OWNER>
            <DIGEST_HASH><![CDATA[MD5]]></DIGEST_HASH>
            <DATA_TYPE>String</DATA_TYPE>
            <DESCRIPTION><![CDATA[desc]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>80</ID>
            <NAME>CentOS 7.x</NAME>
            <RATIONALE><![CDATA[rational]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>no cd</CARDINALITY>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[USE_SCAN_VALUE]]></DEFAULT_VALUE>
```

```
                </DEFAULT_VALUES>
              </DATAPOINT>
              <USE_SCAN_VALUE>0</USE_SCAN_VALUE>
            </TECHNOLOGY>
          </TECHNOLOGY_LIST>
        </CONTROL>
      </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

DTD update:

We updated the DTD to include new elements EXCLUDE_USER_OWNER and EXCLUDE_GROUP_OWNER under SCAN_PARAMETERS.

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 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 SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?, PATH_USER?, GROUP_NAME?, GROUP_NAME_LIMIT?,
BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?,
FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, PERMISSIONS?, PERM_COND?,
TYPE_MATCH?, USER_OWNER?,GROUP_OWNER?, SCRIPT_ID?, SCRIPT_NAME?,
OUTPUT_FILTER?, TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
FILE_CONTENT_CHECK_V2_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_MATCH_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?,
DISABLE_CASE_SENSITIVE_SEARCH?,EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?,
DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE, EVALUATE_AS_STRING?,
DESCRIPTION)>
```

```
<!ELEMENT PATH_TYPE (#PCDATA)>
<!ELEMENT REG_HIVE (#PCDATA)>
<!ELEMENT REG_KEY (#PCDATA)>
<!ELEMENT REG_VALUE_NAME (#PCDATA)>
<!ELEMENT FILE_PATH (#PCDATA)>
<!ELEMENT FILE_QUERY (#PCDATA)>
<!ELEMENT HASH_TYPE (#PCDATA)>
<!ELEMENT WMI_NS (#PCDATA)>
<!ELEMENT WMI_QUERY (#PCDATA)>
<!ELEMENT SHARE_USER (#PCDATA)>
<!ELEMENT PATH_USER (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_NAME_LIMIT (#PCDATA)>
<!ELEMENT BASE_DIR (#PCDATA)>
<!ELEMENT DEPTH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_DEPTH_LIMIT (#PCDATA)>
<!ELEMENT FILE_NAME_MATCH (#PCDATA)>
<!ELEMENT FILE_NAME_SKIP (#PCDATA)>
<!ELEMENT DIR_NAME_MATCH (#PCDATA)>
<!ELEMENT DIR_NAME_SKIP (#PCDATA)>
<!ELEMENT TIME_LIMIT (#PCDATA)>
<!ELEMENT MATCH_LIMIT (#PCDATA)>
<!ELEMENT WIN_FILE_SYS_OBJECT_TYPES (#PCDATA)>
<!ELEMENT MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN (#PCDATA)>
<!ELEMENT WIN_PERMISSION_USERS (#PCDATA)>
<!ELEMENT WIN_PERMISSION_MATCH (#PCDATA)>
<!ELEMENT SHOULD_DESCEND (#PCDATA)>
<!ELEMENT FOLLOW_SYMLINK (#PCDATA)>
<!ELEMENT PERMISSIONS (SPECIAL, USER, GROUP, OTHER)>
<!ELEMENT PERM_COND (#PCDATA)>
<!ELEMENT TYPE_MATCH (#PCDATA)>
<!ELEMENT USER_OWNER (#PCDATA)>
<!ELEMENT GROUP_OWNER (#PCDATA)>
<!ELEMENT DB_QUERY (#PCDATA)>
<!ELEMENT SCRIPT_ID (#PCDATA)>
<!ELEMENT SCRIPT_NAME (#PCDATA)>
<!ELEMENT OUTPUT_FILTER (#PCDATA)>

<!ELEMENT WIN_PERMISSIONS (WIN_BASIC_PERMISSIONS?,
WIN_ADVANCED_PERMISSIONS?)>
<!ELEMENT WIN_BASIC_PERMISSIONS (WIN_BASIC_PERMISSION_TYPE+)>
<!ELEMENT WIN_ADVANCED_PERMISSIONS (WIN_ADVANCED_PERMISSION_TYPE+)>
<!ELEMENT WIN_BASIC_PERMISSION_TYPE (#PCDATA)>
<!ELEMENT WIN_ADVANCED_PERMISSION_TYPE (#PCDATA)>

<!ELEMENT SPECIAL (USER, GROUP, DELETION)>
<!ELEMENT USER (#PCDATA|READ|WRITE|EXECUTE)*>
<!ELEMENT GROUP (#PCDATA|READ|WRITE|EXECUTE)*>
<!ELEMENT OTHER (READ, WRITE, EXECUTE)>
```

```
<!ELEMENT DELETION (#PCDATA)>
<!ELEMENT READ (#PCDATA)>
<!ELEMENT WRITE (#PCDATA)>
<!ELEMENT EXECUTE (#PCDATA)>

<!ELEMENT INTEGRITY_CHECK_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_OBJECT_TYPES (#PCDATA)>
<!ELEMENT DIGEST_HASH (#PCDATA)>
<!ELEMENT PERMISSION_MONITOR (#PCDATA)>
<!ELEMENT DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)>
<!ELEMENT EXCLUDE_USER_OWNER (#PCDATA)>
<!ELEMENT EXCLUDE_GROUP_OWNER (#PCDATA)>
...
```

Policy Export

When you export a policy that contains Unix Directory Search UDCs or Unix Directory Integrity UDCs (and you include show_user_controls=1 in the API request), then you'll see details for the UDCs in the output, including the new scan parameters.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=export&id=4152690&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/" >
exportUDCPolicywithDIDSusergrp.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>2021-08-17T09:15:31Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[DI-DS-Exclude-User-Group-Policy]]></TITLE>
    <EXPORTED><![CDATA[2021-08-17T09:15:31Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>80</ID>
            <NAME>CentOS 7.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
```

```
    <SECTIONS total="1">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[Untitled]]></HEADING>
            <CONTROLS total="2">
                <USER_DEFINED_CONTROL>
                    <ID>100046</ID>
                    <UDC_ID>5ed91f0f-b5b7-f017-836c-de0cb49e5030</UDC_ID>
                   <CHECK_TYPE>Unix Directory Integrity Check</CHECK_TYPE>
                    <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <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[DI exclude user and
grp]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[CRITICAL]]></LABEL>
                        <VALUE>4</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[comment]]></COMMENT>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                    <SCAN_PARAMETERS>
                        <BASE_DIR><![CDATA[/etc/]]></BASE_DIR>
                       <SHOULD_DESCEND><![CDATA[false]]></SHOULD_DESCEND>

<INTEGRITY_CHECK_DEPTH_LIMIT><![CDATA[10]]></INTEGRITY_CHECK_DEPTH_LIMIT>
                        <FOLLOW_SYMLINK><![CDATA[false]]></FOLLOW_SYMLINK>
                        <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
                        <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
                        <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
                        <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
                        <TYPE_MATCH><![CDATA[f,l]]></TYPE_MATCH>
                        <USER_OWNER><![CDATA[tanuDI]]></USER_OWNER>
                        <GROUP_OWNER><![CDATA[tanuDI]]></GROUP_OWNER>

<INTEGRITY_CHECK_TIME_LIMIT><![CDATA[600]]></INTEGRITY_CHECK_TIME_LIMIT>

<INTEGRITY_CHECK_MATCH_LIMIT><![CDATA[512]]></INTEGRITY_CHECK_MATCH_LIMIT
>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE_
SEARCH>
```

```
<EXCLUDE_USER_OWNER><![CDATA[true]]></EXCLUDE_USER_OWNER>

<EXCLUDE_GROUP_OWNER><![CDATA[true]]></EXCLUDE_GROUP_OWNER>
                        <DIGEST_HASH><![CDATA[MD5]]></DIGEST_HASH>
                        <DATA_TYPE>String</DATA_TYPE>
                        <DESCRIPTION><![CDATA[desc]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>80</ID>
                            <NAME>CentOS 7.x</NAME>

<EVALUATE><CTRL><DP><K>custom.unix_dir_integrity_check.3257398</K><L>0</L
><OP>re</OP><V><![CDATA[USE_SCAN_VALUE]]></V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[rational]]></RATIONALE>
                            <REMEDIATION><![CDATA[remedy]]></REMEDIATION>
                            <DATAPOINT>
                                <CARDINALITY>no cd</CARDINALITY>
                                <OPERATOR>re</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[USE_SCAN_VALUE]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                            <USE_SCAN_VALUE>1</USE_SCAN_VALUE>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
                <USER_DEFINED_CONTROL>
                    <ID>100045</ID>
                    <UDC_ID>09fc2bba-ecf7-4195-824a-0dcfe3b2b78e</UDC_ID>
                    <CHECK_TYPE>Unix Directory Search Check</CHECK_TYPE>
                   <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <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[DS with exclude user and
grp]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[MEDIUM]]></LABEL>
                        <VALUE>2</VALUE>
                    </CRITICALITY>
```

```
                        <COMMENT><![CDATA[comment]]></COMMENT>
                        <IGNORE_ERROR>0</IGNORE_ERROR>
                        <SCAN_PARAMETERS>
                            <BASE_DIR><![CDATA[/usr/]]></BASE_DIR>
                           <SHOULD_DESCEND><![CDATA[false]]></SHOULD_DESCEND>
                            <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>
                           <FOLLOW_SYMLINK><![CDATA[false]]></FOLLOW_SYMLINK>
                            <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
                            <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
                            <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
                            <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
                            <PERMISSIONS>
                                <SPECIAL>
                                    <SPECIAL_USER>any</SPECIAL_USER>
                                    <SPECIAL_GROUP>any</SPECIAL_GROUP>
                                    <SPECIAL_DELETION>any</SPECIAL_DELETION>
                                </SPECIAL>
                                <USER>
                                    <READ>any</READ>
                                    <WRITE>any</WRITE>
                                    <EXECUTE>any</EXECUTE>
                                </USER>
                                <GROUP>
                                    <READ>any</READ>
                                    <WRITE>any</WRITE>
                                    <EXECUTE>any</EXECUTE>
                                </GROUP>
                                <OTHER>
                                    <READ>any</READ>
                                    <WRITE>any</WRITE>
                                    <EXECUTE>any</EXECUTE>
                                </OTHER>
                            </PERMISSIONS>
                            <PERM_COND><![CDATA[all]]></PERM_COND>
                            <TYPE_MATCH><![CDATA[d,f,l]]></TYPE_MATCH>
                            <USER_OWNER><![CDATA[Ashuds]]></USER_OWNER>
                            <GROUP_OWNER><![CDATA[Ashuds]]></GROUP_OWNER>
                            <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
                            <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE_
SEARCH>

<EXCLUDE_USER_OWNER><![CDATA[true]]></EXCLUDE_USER_OWNER>

<EXCLUDE_GROUP_OWNER><![CDATA[true]]></EXCLUDE_GROUP_OWNER>
                            <DATA_TYPE>String List</DATA_TYPE>
                            <DESCRIPTION><![CDATA[desc]]></DESCRIPTION>
                        </SCAN_PARAMETERS>
```

```
                        <TECHNOLOGIES total="1">
                            <TECHNOLOGY>
                                <ID>80</ID>
                                <NAME>CentOS 7.x</NAME>

<EVALUATE><CTRL><DP><K>custom.dir_search_check.3257397</K><L>0</L><CD>con
tains</CD><OP>xre</OP><V><![CDATA[ashu]]></V></DP></CTRL></EVALUATE>
                                <RATIONALE><![CDATA[rational]]></RATIONALE>
                                <REMEDIATION><![CDATA[remedy]]></REMEDIATION>
                                <DATAPOINT>
                                    <CARDINALITY>contains</CARDINALITY>
                                    <OPERATOR>xre</OPERATOR>
                                    <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[ashu]]></DEFAULT_VALUE>
                                    </DEFAULT_VALUES>
                                </DATAPOINT>
                            </TECHNOLOGY>
                        </TECHNOLOGIES>
                        <REFERENCE_LIST/>
                    </USER_DEFINED_CONTROL>
                </CONTROLS>
            </SECTION>
        </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

DTD update:

We updated the DTD to include new elements EXCLUDE_USER_OWNER and EXCLUDE_GROUP_OWNER under SCAN_PARAMETERS.

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

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->
<!-- $Revision: 62328 $ -->
<!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 SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?, PATH_USER?, BASE_DIR?, SHOULD_DESCEND?,
DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?, FOLLOW_SYMLINK?,
FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, PERMISSIONS?, PERM_COND?, TYPE_MATCH?, USER_OWNER?,
GROUP_OWNER?, TIME_LIMIT?, MATCH_LIMIT?,
INTEGRITY_CHECK_TIME_LIMIT?,FILE_CONTENT_CHECK_V2_TIME_LIMIT?,
FILE_CONTENT_CHECK_V2_MATCH_LIMIT?,INTEGRITY_CHECK_MATCH_LIMIT?,
DISABLE_CASE_SENSITIVE_SEARCH?,EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?,
INTEGRITY_CHECK_OBJECT_TYPES?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, GROUP_NAME?,
SCRIPT_ID?, SCRIPT_NAME?, OUTPUT_FILTER?,
GROUP_NAME_LIMIT?, DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE,
EVALUATE_AS_STRING?, DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
<!ELEMENT REG_HIVE (#PCDATA)>
<!ELEMENT REG_KEY (#PCDATA)>
<!ELEMENT REG_VALUE_NAME (#PCDATA)>
<!ELEMENT FILE_PATH (#PCDATA)>
<!ELEMENT FILE_QUERY (#PCDATA)>
<!ELEMENT HASH_TYPE (#PCDATA)>
<!ELEMENT WMI_NS (#PCDATA)>
<!ELEMENT WMI_QUERY (#PCDATA)>
<!ELEMENT SHARE_USER (#PCDATA)>
<!ELEMENT PATH_USER (#PCDATA)>
<!ELEMENT BASE_DIR (#PCDATA)>
<!ELEMENT SHOULD_DESCEND (#PCDATA)>
<!ELEMENT DEPTH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_DEPTH_LIMIT (#PCDATA)>
<!ELEMENT FOLLOW_SYMLINK (#PCDATA)>
<!ELEMENT FILE_NAME_MATCH (#PCDATA)>
<!ELEMENT FILE_NAME_SKIP (#PCDATA)>
<!ELEMENT DIR_NAME_MATCH (#PCDATA)>
<!ELEMENT DIR_NAME_SKIP (#PCDATA)>
<!ELEMENT PERM_COND (#PCDATA)>
<!ELEMENT TYPE_MATCH (#PCDATA)>
<!ELEMENT USER_OWNER (#PCDATA)>
<!ELEMENT GROUP_OWNER (#PCDATA)>
<!ELEMENT TIME_LIMIT (#PCDATA)>
<!ELEMENT MATCH_LIMIT (#PCDATA)>
<!ELEMENT DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)>
<!ELEMENT EXCLUDE_USER_OWNER (#PCDATA)>
<!ELEMENT EXCLUDE_GROUP_OWNER (#PCDATA)>
...
```

Policy Import

In this sample we are importing a policy to the user's account from an XML file.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -H Content-
Type:text/xml --data-binary "@API_Import_Policy_withUDC.xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=import
&title=My_Policy&create_user_controls=1"
```

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>2021-08-19T21:17:17Z</DATETIME>
    <TEXT>Successfully imported compliance policy</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>4162711</VALUE>
      </ITEM>
      <ITEM>
        <KEY>TITLE</KEY>
        <VALUE>My_Policy</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Schema update (ImportableControl.xsd):

The ImportableControl.xsd schema is used when importing and exporting controls. We added EXCLUDE_USER_OWNER and EXCLUDE_GROUP_OWNER under SCAN_PARAMETERS.

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

...

    <xs:element name="SCAN_PARAMETERS">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="PATH_TYPE" minOccurs="0" maxOccurs="1" />
```

```
                  <xs:element ref="REG_HIVE" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="REG_KEY" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="REG_VALUE_NAME" minOccurs="0"
maxOccurs="1" />
                   <xs:element ref="FILE_PATH" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="FILE_QUERY" minOccurs="0" maxOccurs="1" />
                   <xs:element ref="HASH_TYPE" minOccurs="0" maxOccurs="1" />
                    <xs:element ref="WMI_NS" minOccurs="0" maxOccurs="1" />
                   <xs:element ref="WMI_QUERY" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="SHARE_USER" minOccurs="0" maxOccurs="1" />
                   <xs:element ref="PATH_USER" minOccurs="0" maxOccurs="1" />
                    <xs:element ref="BASE_DIR" minOccurs="0" maxOccurs="1" />
                    <xs:element ref="SHOULD_DESCEND" minOccurs="0"
maxOccurs="1" />
                   <xs:element ref="DEPTH_LIMIT" minOccurs="0" maxOccurs="1"
/>
                 <xs:element ref="INTEGRITY_CHECK_DEPTH_LIMIT" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="FOLLOW_SYMLINK" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="FILE_NAME_MATCH" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="FILE_NAME_SKIP" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="DIR_NAME_MATCH" minOccurs="0"
maxOccurs="1" />
                 <xs:element ref="DIR_NAME_SKIP" minOccurs="0" maxOccurs="1"
/>
                   <xs:element ref="PERMISSIONS" minOccurs="0" maxOccurs="1"
/>
                   <xs:element ref="PERM_COND" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="TYPE_MATCH" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="USER_OWNER" minOccurs="0" maxOccurs="1" />
                   <xs:element ref="GROUP_OWNER" minOccurs="0" maxOccurs="1"
/>
                  <xs:element ref="TIME_LIMIT" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="INTEGRITY_CHECK_TIME_LIMIT" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="FILE_CONTENT_CHECK_V2_TIME_LIMIT"
minOccurs="0" maxOccurs="1" />
                   <xs:element ref="MATCH_LIMIT" minOccurs="0" maxOccurs="1"
/>
                 <xs:element ref="INTEGRITY_CHECK_MATCH_LIMIT" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="FILE_CONTENT_CHECK_V2_MATCH_LIMIT"
minOccurs="0" maxOccurs="1" />
                   <xs:element ref="WIN_FILE_SYS_OBJECT_TYPES" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN"
```

```
minOccurs="0" maxOccurs="1" />
                <xs:element ref="WIN_PERMISSION_USERS" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="WIN_PERMISSION_MATCH" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="WIN_PERMISSIONS" minOccurs="0"
maxOccurs="1" />
               <xs:element ref="GROUP_NAME" minOccurs="0" maxOccurs="1" />
                <xs:element ref="GROUP_NAME_LIMIT" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="INTEGRITY_CHECK_OBJECT_TYPES"
minOccurs="0" maxOccurs="1" />
                <xs:element ref="DISABLE_CASE_SENSITIVE_SEARCH"
minOccurs="0" maxOccurs="1" />
                <xs:element ref="EXCLUDE_USER_OWNER" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="EXCLUDE_GROUP_OWNER" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="DIGEST_HASH" minOccurs="0" maxOccurs="1"
/>
...

    <xs:element name="EXCLUDE_USER_OWNER">
        <xs:simpleType>
            <xs:restriction base="xs:boolean">
                <xs:pattern value="true"/>
                <xs:pattern value="false"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="EXCLUDE_GROUP_OWNER">
        <xs:simpleType>
            <xs:restriction base="xs:boolean">
                <xs:pattern value="true"/>
                <xs:pattern value="false"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
...
```

New UDC "Unix File Content Check (Agent Only)" with Wildcard Support

APIs affected	/api/2.0/fo/compliance/control/?action=list /api/2.0/fo/compliance/policy/?action=export /api/2.0/fo/compliance/policy/?action=import
New or Updated API	Updated
DTD or XSD changes	Yes

We've introduced a new User Defined Control (UDC) called "Unix File Content Check (Agent Only)" which supports wildcard file search and provides several additional scan parameter options than the original version of the Unix File Content Check UDC. This new UDC can only be evaluated by the Linux Cloud Agent. Please note that there are no changes to the existing Unix File Content Check UDC.

To support the new UDC, we added elements to the XML output and DTDs for Control List Output, Policy Export Output and the ImportableControl.xsd schema.

Control List

When you list controls and you have the new UDC control type, you'll see the CHECK_TYPE "Unix File Content Check V2" in the XML output. You'll also see the new scan parameters for Time Limit and Match Limit.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&ids=100050&details=All"
"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>2021-08-17T11:24:20Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100050</ID>
        <UPDATE_DATE>2021-08-17T05:43:09Z</UPDATE_DATE>
        <CREATED_DATE>2021-08-17T05:43:09Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
```

```
        <STATEMENT><![CDATA[FC UDC with wildcard]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Unix File Content Check V2]]></CHECK_TYPE>
        <COMMENT><![CDATA[comment file content udc for agents only with
wildcard characters]]></COMMENT>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <SCAN_PARAMETERS>
            <FILE_QUERY><![CDATA[qualys]]></FILE_QUERY>
            <BASE_DIR><![CDATA[/root]]></BASE_DIR>
            <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>
            <FOLLOW_SYMLINK><![CDATA[true]]></FOLLOW_SYMLINK>
            <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
            <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
            <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
            <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>

<FILE_CONTENT_CHECK_V2_TIME_LIMIT><![CDATA[300]]></FILE_CONTENT_CHECK_V2
_TIME_LIMIT>

<FILE_CONTENT_CHECK_V2_MATCH_LIMIT><![CDATA[50]]></FILE_CONTENT_CHECK_V2
_MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE_
SEARCH>
            <DATA_TYPE>String List</DATA_TYPE>
            <DESCRIPTION><![CDATA[desc]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>80</ID>
            <NAME>CentOS 7.x</NAME>
            <RATIONALE><![CDATA[rational]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[qusly]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
    </CONTROL_LIST>
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

DTD update:

We updated the DTD to include new elements under SCAN_PARAMETERS.

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 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 SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?, PATH_USER?, GROUP_NAME?, GROUP_NAME_LIMIT?,
BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?,
FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, PERMISSIONS?, PERM_COND?,
TYPE_MATCH?, USER_OWNER?,GROUP_OWNER?, SCRIPT_ID?, SCRIPT_NAME?,
OUTPUT_FILTER?,
TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
FILE_CONTENT_CHECK_V2_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_MATCH_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?,
DISABLE_CASE_SENSITIVE_SEARCH?,EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?,
DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE, EVALUATE_AS_STRING?,
DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
<!ELEMENT REG_HIVE (#PCDATA)>
<!ELEMENT REG_KEY (#PCDATA)>
<!ELEMENT REG_VALUE_NAME (#PCDATA)>
<!ELEMENT FILE_PATH (#PCDATA)>
<!ELEMENT FILE_QUERY (#PCDATA)>
<!ELEMENT HASH_TYPE (#PCDATA)>
<!ELEMENT WMI_NS (#PCDATA)>
<!ELEMENT WMI_QUERY (#PCDATA)>
<!ELEMENT SHARE_USER (#PCDATA)>
```

```
<!ELEMENT PATH_USER (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_NAME_LIMIT (#PCDATA)>
<!ELEMENT BASE_DIR (#PCDATA)>
<!ELEMENT DEPTH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_DEPTH_LIMIT (#PCDATA)>
<!ELEMENT FILE_NAME_MATCH (#PCDATA)>
<!ELEMENT FILE_NAME_SKIP (#PCDATA)>
<!ELEMENT DIR_NAME_MATCH (#PCDATA)>
<!ELEMENT DIR_NAME_SKIP (#PCDATA)>
<!ELEMENT TIME_LIMIT (#PCDATA)>
<!ELEMENT MATCH_LIMIT (#PCDATA)>
<!ELEMENT WIN_FILE_SYS_OBJECT_TYPES (#PCDATA)>
<!ELEMENT MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN (#PCDATA)>
<!ELEMENT WIN_PERMISSION_USERS (#PCDATA)>
<!ELEMENT WIN_PERMISSION_MATCH (#PCDATA)>
<!ELEMENT SHOULD_DESCEND (#PCDATA)>
<!ELEMENT FOLLOW_SYMLINK (#PCDATA)>
<!ELEMENT PERMISSIONS (SPECIAL, USER, GROUP, OTHER)>
<!ELEMENT PERM_COND (#PCDATA)>
<!ELEMENT TYPE_MATCH (#PCDATA)>
<!ELEMENT USER_OWNER (#PCDATA)>
<!ELEMENT GROUP_OWNER (#PCDATA)>
<!ELEMENT DB_QUERY (#PCDATA)>
<!ELEMENT SCRIPT_ID (#PCDATA)>
<!ELEMENT SCRIPT_NAME (#PCDATA)>
<!ELEMENT OUTPUT_FILTER (#PCDATA)>

<!ELEMENT WIN_PERMISSIONS (WIN_BASIC_PERMISSIONS?,
WIN_ADVANCED_PERMISSIONS?)>
<!ELEMENT WIN_BASIC_PERMISSIONS (WIN_BASIC_PERMISSION_TYPE+)>
<!ELEMENT WIN_ADVANCED_PERMISSIONS (WIN_ADVANCED_PERMISSION_TYPE+)>
<!ELEMENT WIN_BASIC_PERMISSION_TYPE (#PCDATA)>
<!ELEMENT WIN_ADVANCED_PERMISSION_TYPE (#PCDATA)>

<!ELEMENT SPECIAL (USER, GROUP, DELETION)>
<!ELEMENT USER (#PCDATA|READ|WRITE|EXECUTE)*>
<!ELEMENT GROUP (#PCDATA|READ|WRITE|EXECUTE)*>
<!ELEMENT OTHER (READ, WRITE, EXECUTE)>
<!ELEMENT DELETION (#PCDATA)>
<!ELEMENT READ (#PCDATA)>
<!ELEMENT WRITE (#PCDATA)>
<!ELEMENT EXECUTE (#PCDATA)>

<!ELEMENT INTEGRITY_CHECK_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)>
...
```

Policy Export

When you export a policy that contains the new UDC control type (and you include show_user_controls=1 in the API request), then you'll see details for the UDC in the output. The UDC will have CHECK_TYPE "Unix File Content Check V2". You'll also see the new scan parameters for Time Limit and Match Limit.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=export&id=4152698&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/" >
exportNewFCUDCPolicy.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>2021-08-17T12:16:05Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[FC new UDC Policy]]></TITLE>
    <EXPORTED><![CDATA[2021-08-17T12:16:05Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>80</ID>
            <NAME>CentOS 7.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="1">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[Untitled]]></HEADING>
            <CONTROLS total="1">
                <USER_DEFINED_CONTROL>
                    <ID>100050</ID>
                    <UDC_ID>05f4deb1-94f3-584d-8385-d57f4a440678</UDC_ID>
                    <CHECK_TYPE>Unix File Content Check V2</CHECK_TYPE>
                   <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <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[FC UDC with wildcard]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[comment file content udc for agents
only with wildcard characters]]></COMMENT>
                    <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                    <SCAN_PARAMETERS>
                        <FILE_QUERY><![CDATA[qualys]]></FILE_QUERY>
                        <BASE_DIR><![CDATA[/root]]></BASE_DIR>
                        <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>
                        <FOLLOW_SYMLINK><![CDATA[true]]></FOLLOW_SYMLINK>
                        <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
                        <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
                        <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
                        <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>

<FILE_CONTENT_CHECK_V2_TIME_LIMIT><![CDATA[300]]></FILE_CONTENT_CHECK_V2
_TIME_LIMIT>

<FILE_CONTENT_CHECK_V2_MATCH_LIMIT><![CDATA[50]]></FILE_CONTENT_CHECK_V2
_MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE_
SEARCH>
                        <DATA_TYPE>String List</DATA_TYPE>
                        <DESCRIPTION><![CDATA[desc]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>80</ID>
                            <NAME>CentOS 7.x</NAME>

<EVALUATE><CTRL><DP><K>custom.file_content_check_v2.3259396</K><L>0</L><C
D>contains</CD><OP>xre</OP><V><![CDATA[qusly]]></V></DP></CTRL></EVALUATE
>
                            <RATIONALE><![CDATA[rational]]></RATIONALE>
                            <REMEDIATION><![CDATA[remedy]]></REMEDIATION>
                            <DATAPOINT>
                                <CARDINALITY>contains</CARDINALITY>
                                <OPERATOR>xre</OPERATOR>
                                <DEFAULT_VALUES total="1">
```

```
<DEFAULT_VALUE><![CDATA[qusly]]></DEFAULT_VALUE>
                                  </DEFAULT_VALUES>
                              </DATAPOINT>
                          </TECHNOLOGY>
                      </TECHNOLOGIES>
                      <REFERENCE_LIST/>
                  </USER_DEFINED_CONTROL>
              </CONTROLS>
          </SECTION>
      </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

DTD update:

We updated the DTD to include new elements under SCAN_PARAMETERS.

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

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->
<!-- $Revision: 62328 $ -->
<!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 SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?, PATH_USER?, BASE_DIR?, SHOULD_DESCEND?,
DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?, FOLLOW_SYMLINK?,
FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, PERMISSIONS?, PERM_COND?, TYPE_MATCH?, USER_OWNER?,
GROUP_OWNER?, TIME_LIMIT?, MATCH_LIMIT?,
INTEGRITY_CHECK_TIME_LIMIT?,FILE_CONTENT_CHECK_V2_TIME_LIMIT?,
FILE_CONTENT_CHECK_V2_MATCH_LIMIT?,INTEGRITY_CHECK_MATCH_LIMIT?,
DISABLE_CASE_SENSITIVE_SEARCH?,EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?,
INTEGRITY_CHECK_OBJECT_TYPES?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
```

```
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, GROUP_NAME?,
SCRIPT_ID?, SCRIPT_NAME?, OUTPUT_FILTER?,
GROUP_NAME_LIMIT?, DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE,
EVALUATE_AS_STRING?, DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
<!ELEMENT REG_HIVE (#PCDATA)>
<!ELEMENT REG_KEY (#PCDATA)>
<!ELEMENT REG_VALUE_NAME (#PCDATA)>
<!ELEMENT FILE_PATH (#PCDATA)>
<!ELEMENT FILE_QUERY (#PCDATA)>
<!ELEMENT HASH_TYPE (#PCDATA)>
<!ELEMENT WMI_NS (#PCDATA)>
<!ELEMENT WMI_QUERY (#PCDATA)>
<!ELEMENT SHARE_USER (#PCDATA)>
<!ELEMENT PATH_USER (#PCDATA)>
<!ELEMENT BASE_DIR (#PCDATA)>
<!ELEMENT SHOULD_DESCEND (#PCDATA)>
<!ELEMENT DEPTH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_DEPTH_LIMIT (#PCDATA)>
<!ELEMENT FOLLOW_SYMLINK (#PCDATA)>
<!ELEMENT FILE_NAME_MATCH (#PCDATA)>
<!ELEMENT FILE_NAME_SKIP (#PCDATA)>
<!ELEMENT DIR_NAME_MATCH (#PCDATA)>
<!ELEMENT DIR_NAME_SKIP (#PCDATA)>
<!ELEMENT PERM_COND (#PCDATA)>
<!ELEMENT TYPE_MATCH (#PCDATA)>
<!ELEMENT USER_OWNER (#PCDATA)>
<!ELEMENT GROUP_OWNER (#PCDATA)>
<!ELEMENT TIME_LIMIT (#PCDATA)>
<!ELEMENT MATCH_LIMIT (#PCDATA)>
<!ELEMENT DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)>
<!ELEMENT EXCLUDE_USER_OWNER (#PCDATA)>
<!ELEMENT EXCLUDE_GROUP_OWNER (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)>
...
```

Policy Import

In this sample we are importing a policy to the user's account from an XML file.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -H Content-
Type:text/xml --data-binary "@API_Import_Policy_withUDC.xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=import
&title=My_Policy&create_user_controls=1"
```

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>2021-08-19T21:17:17Z</DATETIME>
    <TEXT>Successfully imported compliance policy</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>4162711</VALUE>
      </ITEM>
      <ITEM>
        <KEY>TITLE</KEY>
        <VALUE>My_Policy</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Schema update (ImportableControl.xsd):

The ImportableControl.xsd schema is used when importing and exporting controls. We added "Unix File Content Check V2" under CHECK_TYPE, and we added new scan parameters.

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

    <xs:element name="CONTROL_LIST">
        <xs:complexType>
            <xs:sequence>
                <xs:element maxOccurs="unbounded" ref="CONTROL" />
            </xs:sequence>
           <xs:attribute name="total" use="required" type="xs:integer" />
```

```
            </xs:complexType>
        </xs:element>

...

        <xs:element name="CHECK_TYPE">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Registry Key Existence" />
                    <xs:enumeration value="Registry Value Existence" />
                    <xs:enumeration value="Registry Value Content Check" />
                    <xs:enumeration value="Registry Permission" />
                   <xs:enumeration value="Window File/Directory Existence" />
                  <xs:enumeration value="Window File/Directory Permission" />
                    <xs:enumeration value="Unix File/Directory Permission" />
                    <xs:enumeration value="Unix File Content Check" />
                    <xs:enumeration value="Unix File/Directory Existence" />
                    <xs:enumeration value="Window File Integrity Check" />
                    <xs:enumeration value="Unix File Integrity Check" />
                    <xs:enumeration value="WMI Query Check" />
                    <xs:enumeration value="Share Access Check" />
                    <xs:enumeration value="Unix Directory Search Check" />
                    <xs:enumeration value="Windows Directory Search Check" />
                    <xs:enumeration value="Windows Group Membership Check" />
                   <xs:enumeration value="Windows Directory Integrity Check"
/>
                    <xs:enumeration value="Unix Directory Integrity Check" />
                    <xs:enumeration value="MS SQL Database Check" />
                    <xs:enumeration value="Oracle Database Check" />
                    <xs:enumeration value="Sybase Database Check" />
                    <xs:enumeration value="PostgreSQL Database Check" />
                    <xs:enumeration value="SAP IQ Database Check" />
                    <xs:enumeration value="Windows File Content Check" />
                    <xs:enumeration value="DB2 Database Check" />
                    <xs:enumeration value="Unix File Content Check V2" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
...

        <xs:element name="SCAN_PARAMETERS">
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="PATH_TYPE" minOccurs="0" maxOccurs="1" />
                    <xs:element ref="REG_HIVE" minOccurs="0" maxOccurs="1" />
                    <xs:element ref="REG_KEY" minOccurs="0" maxOccurs="1" />
                    <xs:element ref="REG_VALUE_NAME" minOccurs="0"
maxOccurs="1" />
                    <xs:element ref="FILE_PATH" minOccurs="0" maxOccurs="1" />
```

```
                <xs:element ref="FILE_QUERY" minOccurs="0" maxOccurs="1" />
                 <xs:element ref="HASH_TYPE" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="WMI_NS" minOccurs="0" maxOccurs="1" />
                 <xs:element ref="WMI_QUERY" minOccurs="0" maxOccurs="1" />
                <xs:element ref="SHARE_USER" minOccurs="0" maxOccurs="1" />
                 <xs:element ref="PATH_USER" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="BASE_DIR" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="SHOULD_DESCEND" minOccurs="0"
maxOccurs="1" />
                  <xs:element ref="DEPTH_LIMIT" minOccurs="0" maxOccurs="1"
/>
               <xs:element ref="INTEGRITY_CHECK_DEPTH_LIMIT" minOccurs="0"
maxOccurs="1" />
                  <xs:element ref="FOLLOW_SYMLINK" minOccurs="0"
maxOccurs="1" />
                  <xs:element ref="FILE_NAME_MATCH" minOccurs="0"
maxOccurs="1" />
                  <xs:element ref="FILE_NAME_SKIP" minOccurs="0"
maxOccurs="1" />
                  <xs:element ref="DIR_NAME_MATCH" minOccurs="0"
maxOccurs="1" />
               <xs:element ref="DIR_NAME_SKIP" minOccurs="0" maxOccurs="1"
/>
                  <xs:element ref="PERMISSIONS" minOccurs="0" maxOccurs="1"
/>
                  <xs:element ref="PERM_COND" minOccurs="0" maxOccurs="1" />
                 <xs:element ref="TYPE_MATCH" minOccurs="0" maxOccurs="1" />
                 <xs:element ref="USER_OWNER" minOccurs="0" maxOccurs="1" />
                  <xs:element ref="GROUP_OWNER" minOccurs="0" maxOccurs="1"
/>
                 <xs:element ref="TIME_LIMIT" minOccurs="0" maxOccurs="1" />
                 <xs:element ref="INTEGRITY_CHECK_TIME_LIMIT" minOccurs="0"
maxOccurs="1" />
                   <xs:element ref="FILE_CONTENT_CHECK_V2_TIME_LIMIT"
minOccurs="0" maxOccurs="1" />
                  <xs:element ref="MATCH_LIMIT" minOccurs="0" maxOccurs="1"
/>
               <xs:element ref="INTEGRITY_CHECK_MATCH_LIMIT" minOccurs="0"
maxOccurs="1" />
                   <xs:element ref="FILE_CONTENT_CHECK_V2_MATCH_LIMIT"
minOccurs="0" maxOccurs="1" />
                  <xs:element ref="WIN_FILE_SYS_OBJECT_TYPES" minOccurs="0"
maxOccurs="1" />
                  <xs:element ref="MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN"
minOccurs="0" maxOccurs="1" />
                  <xs:element ref="WIN_PERMISSION_USERS" minOccurs="0"
maxOccurs="1" />
                  <xs:element ref="WIN_PERMISSION_MATCH" minOccurs="0"
maxOccurs="1" />
```

```
                <xs:element ref="WIN_PERMISSIONS" minOccurs="0"
maxOccurs="1" />
               <xs:element ref="GROUP_NAME" minOccurs="0" maxOccurs="1" />
                <xs:element ref="GROUP_NAME_LIMIT" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="INTEGRITY_CHECK_OBJECT_TYPES"
minOccurs="0" maxOccurs="1" />
                <xs:element ref="DISABLE_CASE_SENSITIVE_SEARCH"
minOccurs="0" maxOccurs="1" />
                <xs:element ref="EXCLUDE_USER_OWNER" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="EXCLUDE_GROUP_OWNER" minOccurs="0"
maxOccurs="1" />
                 <xs:element ref="DIGEST_HASH" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="PERMISSION_MONITOR" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="DATA_TYPE" maxOccurs="1" />
                <xs:element ref="EVALUATE_AS_STRING" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="DESCRIPTION" maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>

...

    <xs:element name="FILE_CONTENT_CHECK_V2_TIME_LIMIT">
        <xs:simpleType>
            <xs:restriction base="xs:integer">
                <xs:minInclusive value="60"/>
                <xs:maxInclusive value="1800"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

...

    <xs:element name="FILE_CONTENT_CHECK_V2_MATCH_LIMIT">
        <xs:simpleType>
            <xs:restriction base="xs:integer">
                <xs:minInclusive value="1"/>
                <xs:maxInclusive value="2048"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

...
```

New Authentication Support for Nginx

APIs affected	/api/2.0/fo/auth/nginx/
New or Updated API	New
DTD or XSD changes	New

Nginx authentication is now supported for compliance scans. The new Nginx Authentication API (api/2.0/fo/auth/nginx/) lets you list, create, update, and delete Nginx authentication records. User permissions for this API are the same as other authentication record APIs.

List Nginx Records

Use the new Nginx Authentication Record List API (/api/2.0/fo/auth/nginx/?action=list) to list only Nginx records.

Input Parameters

Parameter	Description
action=list	(Required) Specify list (using GET or POST) to list records.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list" "https://qualysapi.qualys.com/api/2.0/fo/auth/nginx"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx/auth_nginx_list_outpu
t.dtd">
<AUTH_NGINX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-08-02T13:57:09Z</DATETIME>
    <AUTH_NGINX_LIST>
           <AUTH_NGINX>
                <ID>228028</ID>
                <TITLE>
                    <![CDATA[Nginx second]]>
                </TITLE>
                <IP_SET>
                    <IP>10.11.12.13</IP>
                </IP_SET>
                <UNIX_BIN_PATH>
                    <![CDATA[/usr/local/nginx/sbin/nginx]]>
```

```
                    </UNIX_BIN_PATH>
                    <UNIX_CONF_PATH>
                        <![CDATA[/usr/local/nginx/conf/nginx.conf]]>
                    </UNIX_CONF_PATH>
                    <UNIX_PREFIX_PATH>
                        <![CDATA[/usr/local/nginx]]>
                    </UNIX_PREFIX_PATH>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2021-07-29T06:15:12Z</DATETIME>
                        <BY>joe_user</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2021-07-29T07:20:17Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_NGINX>
            </AUTH_NGINX_LIST>
            <GLOSSARY>
                <USER_LIST>
                    <USER>
                        <USER_LOGIN>joe_user</USER_LOGIN>
                        <FIRST_NAME>Joe</FIRST_NAME>
                        <LAST_NAME>User</LAST_NAME>
                    </USER>
                </USER_LIST>
            </GLOSSARY>
        </RESPONSE>
    </AUTH_NGINX_LIST_OUTPUT>
```

API Sample - List the Nginx Application Record by ID

Use the Nginx Authentication Record List API (/api/2.0/fo/auth/nginx/) to list a specific record by ID.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&ids=1157716"
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/auth_records.dtd">
<AUTH_NGINX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-08-13T11:27:06Z</DATETIME>
    <AUTH_NGINX_LIST>
      <AUTH_NGINX>
```

```
          <ID>1157716</ID>
          <TITLE><![CDATA[Nginx_10.11.12.13]]></TITLE>
          <IP_SET>
            <IP>10.11.12.13</IP>
          </IP_SET>
          <UNIX_BIN_PATH><![CDATA[/opt/nginx142/nginx]]></UNIX_BIN_PATH>

<UNIX_CONF_PATH><![CDATA[/opt/nginx142/nginx.conf]]></UNIX_CONF_PATH>
          <CREATED>
            <DATETIME>2021-08-13T09:28:07Z</DATETIME>
            <BY>joe_user</BY>
          </CREATED>
          <LAST_MODIFIED>
            <DATETIME>2021-08-13T09:28:07Z</DATETIME>
          </LAST_MODIFIED>
        </AUTH_NGINX>
      </AUTH_NGINX_LIST>
    </RESPONSE>
</AUTH_NGINX_LIST_OUTPUT>
```

New DTD:

DTD: <platform>/api/2.0/fo/auth/auth_nginx_list_output.dtd

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_NGINX_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, (AUTH_NGINX_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_NGINX_LIST (AUTH_NGINX+)>

<!ELEMENT AUTH_NGINX (ID,
TITLE,IP_SET?,UNIX_BIN_PATH?,UNIX_CONF_PATH?,UNIX_PREFIX_PATH?,NETWORK_ID
?,CREATED,LAST_MODIFIED,COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
```

```
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT UNIX_BIN_PATH (#PCDATA)>
<!ELEMENT UNIX_CONF_PATH (#PCDATA)>
<!ELEMENT UNIX_PREFIX_PATH (#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)>

<!-- EOF -->
```

Create/Update Nginx Records

Use these parameters to create or update a Nginx authentication record.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
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).
ips={value}	(Required to create record) Enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated.
add_ips={value}	(Optional and valid only to update record) Add IPs to the IP list for an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid only to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
unix_bin_path={value}	(Optional) Absolute path of the Nginx binary file location.
unix_conf_path={value}	(Optional) The path to the Nginx configuration file on your Unix hosts.
unix_prefix_path	(Optional) The path to the Nginx configuration file on your Unix hosts.

Example: Create Nginx Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&ips=1.2.3.4&
title=API_Nginx&unix_bin_path=/usr/local/nginx/sbin/nginx&unix_conf_path=
/usr/local/nginx/conf/nginx.conf
&unix_prefix_path=/usr/local/nginx"
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx/"
```

Response:

```
<?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>2021-08-13T11:36:30Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1157719</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Example: Update Nginx Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=update&ids=229028&ips=10.10.10.10&title=Test
Nginx&unix_bin_path=/usr/local/nginx/sbin/nginx&unix_conf_path=/usr/local
/nginx/conf/nginx.conf&unix_prefix_path=/usr/local/nginx"
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx"
```

Response:

```
<?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>2021-08-03T03:15:35Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>229028</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Delete Nginx Records

Use these parameters to delete authentication records.

Input Parameters

Parameter	Description
action=delete	(Required) POST method may be used.
ids={value}	(Required) Nginx authentication record IDs for the records you want to delete. Multiple records are comma separated.

Example: Delete Nginx Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=delete&ids=5146728,5146726"
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx/"
```

Response:

```
<?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>2021-08-27T11:38:07Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>5146726</ID>
          <ID>5146728</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Posture Info API - <INSTANCE> Tag Format in CDATA

APIs affected	/api/2.0/fo/compliance/posture/info/
New or Updated API	Updated
DTD or XSD changes	No

With this release, for the Posture Info API the **<INSTANCE >** tag value format has changed from plain XML to CDATA.

Sample - Posture Info in XML Format

This sample shows the <INSTANCE> tag with a new value format: CDATA (in bold).

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&policy_id=3232467&details=Light&truncation_limit=500000&show
_remediation_info=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-08-25T16:00:53Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>10753247</ID>
        <HOST_ID>4624652</HOST_ID>
        <CONTROL_ID>100673</CONTROL_ID>
        <TECHNOLOGY_ID>174</TECHNOLOGY_ID>
        <INSTANCE><![CDATA[os]]></INSTANCE>
        <STATUS>Passed</STATUS>
        <REMEDIATION>N/A</REMEDIATION>

...
```

Subscription API - Changes to Export/Import User Preferences for Scanner User Account

APIs affected	/api/2.0/fo/user_prefs/?action=export /api/2.0/fo/user_prefs/?action=import
New or Updated API	Updated
DTD or XSD changes	No

Now when using the Subscription API to export user preferences for a user account with a Scanner user role, you'll see the following INFO keys in the XML output. Also, you can include these INFO keys when importing user preferences for a Scanner user account.

fo.can.edit.ntauth={0|1} - A value of 1 indicates the "Create/edit authentication records/vaults" permission is enabled, and 0 means it's disabled.

fo.manage.virtual.scanner={0|1} - A value of 1 indicates the "Manage virtual scanner appliances" permission is enabled, and 0 means it's disabled.

Sample - Export User Preferences

In this sample, we're exporting user preferences for a Scanner user account with user ID #1234567. Specify the user ID for the account you want to export as part of the API request.

API request:

```
curl -u "username:password" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/user_prefs/?action=export&user_i
d=1234567" > export_user_prefs.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE RECORD SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/user_prefs/user_pref.dtd">
<RECORD>
  <USER>
    <INFO key="user_id"><![CDATA[1234567]]></INFO>
    <INFO key="username"><![CDATA[joe_user]]></INFO>
    <INFO key="subscription_id"><![CDATA[123456]]></INFO>
    <INFO key="firstname"><![CDATA[Joe]]></INFO>
    <INFO key="lastname"><![CDATA[User]></INFO>
    <INFO key="title"><![CDATA[Scanner User]]></INFO>
    <INFO key="company"><![CDATA[Qualys, Inc.]]></INFO>
    <INFO key="addr1"><![CDATA[919 E Hillsdale Blvd]]></INFO>
    <INFO key="city"><![CDATA[Foster City]]></INFO>
```

```
    <INFO key="zipcode"><![CDATA[94404]]></INFO>
    <INFO key="state"><![CDATA[California]]></INFO>
    <INFO key="country"><![CDATA[United States of America]]></INFO>
    <INFO key="phone"><![CDATA[6508016100]]></INFO>
    <INFO key="email"><![CDATA[joe_user@qualys.com]]></INFO>
    <INFO key="user_status"><![CDATA[4]]></INFO>
    <INFO key="created_by"><![CDATA[jane_user]]></INFO>
    <INFO key="creation_date"><![CDATA[2021-04-14 13:45:47]]></INFO>
    <INFO key="updated_by"><![CDATA[jane_user]]></INFO>
    <INFO key="update_date"><![CDATA[2021-04-14 14:00:51]]></INFO>
    <INFO key="user_role"><![CDATA[74]]></INFO>
    <INFO key="scan_complete_notification"><![CDATA[off]]></INFO>
    <INFO key="scan_notification"><![CDATA[on]]></INFO>
    <INFO key="exception_notification"><![CDATA[no_notification]]></INFO>
    <INFO key="map_notification"><![CDATA[on]]></INFO>
    <INFO key="latest_vulnerabilities"><![CDATA[weekly]]></INFO>
    <INFO key="report_notification"><![CDATA[no_notification]]></INFO>
    <INFO key="vuln_lang"><![CDATA[en]]></INFO>
    <INFO key="user_assigned_report_quota"><![CDATA[7516192768]]></INFO>
    <INFO key="uuid"><![CDATA[12c3d45d-bd67-8910-1234-
f5678701234d]]></INFO>
    <INFO key="business_unit"><![CDATA[Unassigned]]></INFO>
    <INFO key="subscription_type"><![CDATA[Express Suite]]></INFO>
  <FO>
    <SCAN>
      <INFO key="storage.auto_delete_time_scan"><![CDATA[13]]></INFO>
      <INFO key="storage.auto_delete_time_map"><![CDATA[13]]></INFO>
    </SCAN>
    <REPORTS />
    <REMEDIATION />
    <USERS>
      <INFO key="password.change_time"><![CDATA[1618407947]]></INFO>
      <INFO key="fo.can.access.gui"><![CDATA[1]]></INFO>
      <INFO key="api.can.access.api"><![CDATA[0]]></INFO>
      <INFO
key="fo.landing.is_kb"><![CDATA[fo.landing.is_dashboard]]></INFO>
      <INFO key="ui.pwd_reset"><![CDATA[1]]></INFO>
      <INFO key="secmanage.katana.accepted-toc"><![CDATA[false]]></INFO>
      <INFO key="fo.user.dateformat"><![CDATA[mdy]]></INFO>
      <INFO key="fo.manage.virtual.scanner"><![CDATA[1]]></INFO>
      <INFO key="fo.can.access.vm"><![CDATA[1]]></INFO>
      <INFO key="fo.can.add.asset"><![CDATA[1]]></INFO>
      <INFO key="fo.can.create.option_profile"><![CDATA[1]]></INFO>
      <INFO key="fo.can.purge.host"><![CDATA[1]]></INFO>
      <INFO key="fo.can.edit.ntauth"><![CDATA[1]]></INFO>
    </USERS>
   </FO>
  </USER>
</RECORD>
```

Sample - Import User Preferences

When importing user preferences from an XML file to your subscription, you can include the Info keys for "Create/edit authentication records/vaults" and "Manage virtual scanner appliances" for a Scanner user account.

When a user_id is specified as part of the import request, we'll update the specified user account with the preferences in the XML file. When a user_id is not specified in the request, we'll create a new user account in your subscription with the user preferences.

In the following sample, we're updating the user account with user ID #1234567.

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
--data-binary @export_user_prefs.xml
"https://qualysapi.qualys.com/api/2.0/fo/user_prefs/?action=import&user_i
d=1234567" > import_user_prefs.xml
```

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>2021-08-30T00:46:04Z</DATETIME>
    <TEXT>Successfully imported user prefs</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>login</KEY>
        <VALUE>joe_user</VALUE>
      </ITEM>
      <ITEM>
        <KEY>user_id</KEY>
        <VALUE>1234567</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Updates to Control List Output DTD

We added new optional elements (in bold) to the Control List Output DTD for future use.

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 SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?, PATH_USER?, GROUP_NAME?, GROUP_NAME_LIMIT?,
BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?,
FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, PERMISSIONS?, PERM_COND?,
TYPE_MATCH?, USER_OWNER?,GROUP_OWNER?, SCRIPT_ID?, SCRIPT_NAME?,
OUTPUT_FILTER?, TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
FILE_CONTENT_CHECK_V2_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_MATCH_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?,
DISABLE_CASE_SENSITIVE_SEARCH?,EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?,
DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE, EVALUATE_AS_STRING?,
DESCRIPTION)>

...

<!ELEMENT SCRIPT_ID (#PCDATA)>
<!ELEMENT SCRIPT_NAME (#PCDATA)>
<!ELEMENT OUTPUT_FILTER (#PCDATA)>

...
```

Issues Addressed

- We fixed an issue where the XML output of the Network List API had format issues, such as some tags repeated in the output. Now the XML output shows results in the proper format.
- We fixed an issue where customers were unable to update schedule scans via API.