



Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.13.2

August 19, 2021 (Updated September 2, 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

[Use System Authentication Records In Vulnerability Scans](#)

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.

Use System Authentication Records In Vulnerability Scans

APIs affected	<code>/api/2.0/fo/subscription/option_profile/vm/?action=create update</code> <code>/api/2.0/fo/subscription/option_profile/vm/?action=list</code> <code>/api/2.0/fo/subscription/option_profile/vm/?action=export</code> <code>/api/2.0/fo/subscription/option_profile/vm/?action=import</code>
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, you can start using system created authentication records from Policy Compliance in your vulnerability scans. Instance discovery and record creation will continue to be based on compliance scan data discovered for running instances when this option is selected in your compliance option profile. Once system authentication records are created, they can be used in compliance scans and in vulnerability scans. System authentication records will be used in addition to user created authentication records when authentication is enabled for your scans.

Good to Know

- Your subscription must include both PC and VM/VMDR, and the hosts being scanned must be present in both.
- New VM option profile settings allow you to 1) include system-created records for vulnerability scans, and 2) determine whether to send system records or user records when there are 2 records for the same instance configuration. Don't forget that you must enable authentication in the VM option profile. Use the "authentication" input parameter and specify one or more technologies for the hosts you want to scan.
- Only system authentication records for technologies supported in VM will be included in vulnerability scans.
- System authentication records have the owner "System" and will appear on your authentication records list in the UI.

Create/Update Option Profile

We added new input parameters for the VM option profile for including system records in vulnerability scans. The same parameters are already supported in the PC option profile.

Input Parameters

Use these input parameters when creating or editing a VM option profile. Refer to the [Qualys API \(VM,PC\) User Guide](#) for details on all available input parameters.

Parameter	Description
include_system_auth={0 1}	<p>(Optional to create or update option profile record) Specify include_system_auth=1 to include system created authentication records in scans along with user created records.</p> <p>When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. This identifies which record to use if you have a system created record and a user created record for the same instance configuration. When include_system_auth=0, the user created record will be selected for scans by default.</p>
use_system_auth_on_duplicate={0 1}	<p>(Optional to create or update option profile record) Specify use_system_auth_on_duplicate=1 to use the system created authentication record if you have a system record and user record for the same instance configuration.</p> <p>The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if “include_system_auth=1”.</p>
use_user_auth_on_duplicate={0 1}	<p>(Optional to create or update option profile record) Specify use_user_auth_on_duplicate=1 to use the user created authentication record if you have a system record and user record for the same instance.</p> <p>The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if “include_system_auth=1”.</p>

Sample Create Option Profile

In this sample, we're creating a new option profile and including system authentication records in scans. If there's a duplicate record (system created and user created), then the system created record will be used.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=sample_op&scan_tcp_ports=standard&scan_udp_ports=sta
ndard&vulnerability_detection=complete&basic_information_gathering=all&in
clude_system_auth=1&use_system_auth_on_duplicate=1&authentication=Unix,Or
acle,Windows"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-07-09T11:42:24Z</DATETIME>
    <TEXT>Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>112755</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update Option Profile

In this sample, we're updating an existing option profile to include system authentication records.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&title=sample_op&include_system_auth=1&use_system_auth_on_d
uplicate=1"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

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

```
<RESPONSE>
  <DATETIME>2021-07-09T11:42:24Z</DATETIME>
  <TEXT>Option profile successfully updated.</TEXT>
  <ITEM_LIST>
    <ITEM>
      <KEY>ID</KEY>
      <VALUE>112755</VALUE>
    </ITEM>
  </ITEM_LIST>
</RESPONSE>
</SIMPLE_RETURN>
```

List Option Profile

In this sample, we are listing a single option profile specified by the profile ID. In the XML output, you'll see new tags for system created authentication records.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/?
action=list&id=112754"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/optio
n_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>112754</ID>
      <GROUP_NAME>
        <![CDATA[sample_op1]]>
      </GROUP_NAME>
      <GROUP_TYPE>user</GROUP_TYPE>
      <USER_ID>
        <![CDATA[Joe User (joe_user)]]>
      </USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>123456</SUBSCRIPTION_ID>
      <IS_DEFAULT>0</IS_DEFAULT>
      <IS_GLOBAL>0</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>2021-07-09T11:33:57Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TCP_PORTS>
```

```
        <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
        <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
    </TCP_PORTS>
    <UDP_PORTS>
        <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
    </UDP_PORTS>
    <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
</PORTS>
<SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
<PERFORMANCE>
    <PARALLEL_SCALING>0</PARALLEL_SCALING>
    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
    <HOSTS_TO_SCAN>
        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
        <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
    </HOSTS_TO_SCAN>
    <PROCESSES_TO_RUN>
        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
        <HTTP_PROCESSES>10</HTTP_PROCESSES>
    </PROCESSES_TO_RUN>
    <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>

    </PERFORMANCE>
    <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
    <VULNERABILITY_DETECTION>
        <COMPLETE>
            <![CDATA[complete]]>
        </COMPLETE>
        <DETECTION_INCLUDE>
            <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
            <OVAL_CHECKS>0</OVAL_CHECKS>
        </DETECTION_INCLUDE>
    </VULNERABILITY_DETECTION>
    <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
    <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
</DISSOLVABLE_AGENT>
<SYSTEM_AUTH_RECORD>
    <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_SYSTEM_AUTH>1</ON_DUPLICATE_USE_SYSTEM_AUTH>
    </INCLUDE_SYSTEM_AUTH>
</SYSTEM_AUTH_RECORD>
</SCAN>

...

```

Export Option Profile

In this sample, we are exporting a single option profile specified by the profile ID. In the XML output, you'll see new tags for system created authentication records.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET  
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?action=export&option_profile_id=112754"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE OPTION_PROFILES SYSTEM  
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/option_profile_info.dtd">  
<OPTION_PROFILES>  
  <OPTION_PROFILE>  
    <BASIC_INFO>  
      <ID>112754</ID>  
      <GROUP_NAME>  
        <![CDATA[sample_op]]>  
      </GROUP_NAME>  
      <GROUP_TYPE>user</GROUP_TYPE>  
      <USER_ID>  
        <![CDATA[Joe User (joe_user)]]>  
      </USER_ID>  
      <UNIT_ID>0</UNIT_ID>  
      <SUBSCRIPTION_ID>123456</SUBSCRIPTION_ID>  
      <IS_DEFAULT>0</IS_DEFAULT>  
      <IS_GLOBAL>0</IS_GLOBAL>  
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>  
      <UPDATE_DATE>2021-07-09T12:32:05Z</UPDATE_DATE>  
    </BASIC_INFO>  
    <SCAN>  
      <PORTS>  
        <TCP_PORTS>  
          <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>  
          <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>  
        </TCP_PORTS>  
        <UDP_PORTS>  
          <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>  
        </UDP_PORTS>  
        <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>  
      </PORTS>  
      <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>  
      <PERFORMANCE>  
        <PARALLEL_SCALING>0</PARALLEL_SCALING>  
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
```



```

        <HOSTS_TO_SCAN>
            <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
            <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
            <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
            <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>

    </PERFORMANCE>
    <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
    <VULNERABILITY_DETECTION>
        <COMPLETE>
            <![CDATA[complete]]>
        </COMPLETE>
        <DETECTION_INCLUDE>
            <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
            <OVAL_CHECKS>0</OVAL_CHECKS>
        </DETECTION_INCLUDE>
    </VULNERABILITY_DETECTION>
    <AUTHENTICATION>
        <![CDATA[Windows,Unix,Oracle,Oracle Listener,SNMP,VMware]]>
    </AUTHENTICATION>
    <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
    <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
    </DISSOLVABLE_AGENT>
    <SYSTEM_AUTH_RECORD>
        <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
    </INCLUDE_SYSTEM_AUTH>
    </SYSTEM_AUTH_RECORD>
</SCAN>
...

```

Import Option Profile

In this sample, we're importing an option profile from an XML file to the user's account.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -H "content-type:
text/xml" -X POST --data-binary @Export_OP.xml
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=import"
```

Note: The Export_OP.xml file contains the request POST data.

Request POST Data:

```
<?xml version="1.0" encoding="UTF-8" ?>
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>91815</ID>
      <GROUP_NAME>
        <![CDATA[sample_op]]>
      </GROUP_NAME>
      <GROUP_TYPE>user</GROUP_TYPE>
      <USER_ID>
        <![CDATA[Joe User (joe_user)]]>
      </USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>123456</SUBSCRIPTION_ID>
      <IS_DEFAULT>0</IS_DEFAULT>
      <IS_GLOBAL>0</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>2021-06-29T11:46:20Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TCP_PORTS>
          <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
          <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
        </TCP_PORTS>
        <UDP_PORTS>
          <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
        </UDP_PORTS>
        <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
      </PORTS>
      <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
```

```
<EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
<SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
</HOSTS_TO_SCAN>
<PROCESSES_TO_RUN>
  <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
  <HTTP_PROCESSES>10</HTTP_PROCESSES>
</PROCESSES_TO_RUN>
<PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>

  </PERFORMANCE>
  <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
  <VULNERABILITY_DETECTION>
    <COMPLETE>
      <![CDATA[complete]]>
    </COMPLETE>
    <DETECTION_INCLUDE>
      <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
      <OVAL_CHECKS>0</OVAL_CHECKS>
    </DETECTION_INCLUDE>
  </VULNERABILITY_DETECTION>
  <AUTHENTICATION>
    <![CDATA[Windows,Unix,Oracle,Oracle Listener,SNMP,VMware]]>
  </AUTHENTICATION>
  <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
  <DISSOLVABLE_AGENT>
    <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
</DISSOLVABLE_AGENT>
<SYSTEM_AUTH_RECORD>
  <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_SYSTEM_AUTH>1</ON_DUPLICATE_USE_SYSTEM_AUTH>
  </INCLUDE_SYSTEM_AUTH>
</SYSTEM_AUTH_RECORD>
</SCAN>

...
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-03T11:17:43Z</DATETIME>
    <TEXT>Successfully imported Option profile for the subscription Id
```

```
123456</TEXT>
  <ITEM_LIST>
    <ITEM>
      <KEY>111234</KEY>
      <VALUE>New Option Profile</VALUE>
    </ITEM>
  </ITEM_LIST>
</RESPONSE>
</SIMPLE_RETURN>
```

Option Profile Info DTD Update

The DTD was updated to reorder some of the elements (in bold) to match the XML output. Note that this same DTD is used by vulnerability and compliance option profiles.

DTD: <platform>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL,
INSTANCE_DATA_COLLECTION?, OS_BASED_INSTANCE_DISC_COLLECTION?)>
<!ELEMENT BASIC_INFO (ID, GROUP_NAME, GROUP_TYPE, USER_ID, UNIT_ID,
SUBSCRIPTION_ID, IS_DEFAULT?, IS_GLOBAL?, IS_OFFLINE_SYNCABLE?,
UPDATE_DATE?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_TYPE (#PCDATA)>
<!ELEMENT USER_ID (#PCDATA)>
<!ELEMENT UNIT_ID (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT IS_DEFAULT (#PCDATA)>
<!ELEMENT IS_GLOBAL (#PCDATA)>
<!ELEMENT IS_OFFLINE_SYNCABLE (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)>

<!ELEMENT SCAN (PORTS?, SCAN_DEAD_HOSTS?, CLOSE_VULNERABILITIES?,
PURGE_OLD_HOST_OS_CHANGED?, PERFORMANCE?, LOAD_BALANCER_DETECTION?,
PASSWORD_BRUTE_FORCING?, VULNERABILITY_DETECTION?, AUTHENTICATION?,
ADDL_CERT_DETECTION?, DISSOLVABLE_AGENT?, SCAN_RESTRICTION?,
DATABASE_PREFERENCE_KEY?, SYSTEM_AUTH_RECORD?, LITE_OS_SCAN?,
CUSTOM_HTTP_HEADER?, HOST_ALIVE_TESTING?, ETHERNET_IP_PROBING?,
FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?,
TEST_AUTHENTICATION?)>

...

<!ELEMENT DISSOLVABLE_AGENT (DISSOLVABLE_AGENT_ENABLE,
PASSWORD_AUDITING_ENABLE?, WINDOWS_SHARE_ENUMERATION_ENABLE,
WINDOWS_DIRECTORY_SEARCH_ENABLE?)>
```

```
<!ELEMENT DISSOLVABLE_AGENT_ENABLE (#PCDATA)>
<!ELEMENT PASSWORD_AUDITING_ENABLE (HAS_PASSWORD_AUDITING_ENABLE?,
CUSTOM_PASSWORD_DICTIONARY?)>
<!ELEMENT HAS_PASSWORD_AUDITING_ENABLE (#PCDATA)>
<!ELEMENT CUSTOM_PASSWORD_DICTIONARY (#PCDATA)>
<!ELEMENT WINDOWS_SHARE_ENUMERATION_ENABLE (#PCDATA)>
<!ELEMENT WINDOWS_DIRECTORY_SEARCH_ENABLE (#PCDATA)>

<!ELEMENT SCAN_RESTRICTION (SCAN_BY_POLICY?)>
<!ELEMENT SCAN_BY_POLICY (POLICY+)>
<!ELEMENT POLICY (ID, TITLE)>

<!ELEMENT DATABASE_PREFERENCE_KEY (MSSQL?, ORACLE?, SYBASE?, POSTGRESQL?,
SAPIQ?, DB2?)>
<!ELEMENT MSSQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT ORACLE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SYBASE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT POSTGRESQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SAPIQ (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB2 (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB_UDC_RESTRICTION (#PCDATA)>
<!ELEMENT DB_UDC_LIMIT (#PCDATA)>

<!ELEMENT SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION|INCLUDE_SYSTEM_AUTH)>
<!ELEMENT ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST,
IBM_WAS_DISCOVERY_MODE?, ORACLE_AUTHENTICATION_TEMPLATE?)>
<!ELEMENT AUTHENTICATION_TYPE_LIST (AUTHENTICATION_TYPE+)>
<!ELEMENT AUTHENTICATION_TYPE (#PCDATA)>
<!ELEMENT IBM_WAS_DISCOVERY_MODE (#PCDATA)>
<!ELEMENT ORACLE_AUTHENTICATION_TEMPLATE (ID, TITLE)>
<!ELEMENT INCLUDE_SYSTEM_AUTH
(ON_DUPLICATE_USE_USER_AUTH|ON_DUPLICATE_USE_SYSTEM_AUTH)>
<!ELEMENT ON_DUPLICATE_USE_USER_AUTH (#PCDATA)>
<!ELEMENT ON_DUPLICATE_USE_SYSTEM_AUTH (#PCDATA)>

<!ELEMENT LITE_OS_SCAN (#PCDATA)>
<!ELEMENT CUSTOM_HTTP_HEADER (VALUE?, DEFINITION_KEY?,
DEFINITION_VALUE?)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT DEFINITION_KEY (#PCDATA)>
<!ELEMENT DEFINITION_VALUE (#PCDATA)>

<!ELEMENT HOST_ALIVE_TESTING (#PCDATA)>

<!ELEMENT ETHERNET_IP_PROBING (#PCDATA)>

<!ELEMENT FILE_INTEGRITY_MONITORING (AUTO_UPDATE_EXPECTED_VALUE?)>
...
```