Out-of-band Configuration Assessment

User Guide
Version 0.9

February 12, 2019

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide

Welcome to Qualys Out-of-Band Configuration Assessment! We'll help you get acquainted with the Qualys solutions for broadening the scope of vulnerability, configuration and compliance assessment beyond traditional remotely accessible and agent communicating hosts, using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

OCA Overview

Qualys Out-of-Band Configuration Assessment (OCA) provides a way to assess compliance posture of critical assets that cannot be reached remotely via an external tool or a scanner nor can a third-party agent be installed on them. For example, PLC networked systems or highly secretive banking hosts.

OCA module exposes REST APIs to upload the configuration data of such assets to the Qualys Platform. Then compliance or vulnerability signatures are executed on this configuration data and assessment reports can be generated in the same manner as of scanner-scanned assets.

Why you need it

The agent-based or agent-less remote assessment of these assets could be difficult for several reasons, namely:

- The asset owners may be very protective of the assets and related network infrastructure devices, appliances and the credentials to those systems. Due to which they would only provide the required evidence data to the audit/assessment team to validate the required vulnerability/configuration checks.

- The assets may not support secure remote access and provide only the console access.

- The assets could be in network segment that is not accessible to the scanners remotely.

- The assets are critical; hence, third-party agents cannot be installed on them due to memory issues or due to non-transparency of what data is pulled for the assessment.

Benefits

Qualys OCA enables you to secure these offline assets against mis-configurations and vulnerabilities.

OCA assesses these offline devices based on device configuration files and the output of the device config file of the commands instead of pulling the vulnerability and configuration data from the scanners or agents.

Configuration files of each asset are pushed to Qualys cloud platform using the 'Push data mechanism'. For some assets, a dump of the output of certain commands as per the assessment required can be pushed directly.

Qualys maintains a library of vulnerability signatures and configuration datapoints, controls and uses this for the assessment.

You can use OCA to assess the security of these critical and disconnected assets and include them in the overall Vulnerability, Risk and Compliance program, making it easy for both audit teams as well as the protective asset owners.

Get Started

Things to know before you get started with Out-of-Band Configuration Assessment.

Qualys Subscription and Modules required

You would require “Out-of-Band Configuration Assessment” (OCA) module enabled for your account. You also need to have access to AssetView (AV) module to view your assets and the Policy Compliance (PC) module to view compliance reports.

Out-of-Band Configuration Assessment APIs

Currently OCA is supported through REST APIs only. Using the APIs you can upload the hosts and their metadata to the Qualys platform.

Once the assets are created in Qualys, you can either push files containing the configuration parameters and values, or you can simply run the required commands on the assets, push the output to the Qualys platform.

These assets are displayed in the AssetView module where you can manage them as a part of overall Asset Inventory as well as include them in overall vulnerability and compliance assessment. Also, you can run compliance report on these assets and view these reports in the Policy Compliance module.

Supported Technologies

Currently we support the following technologies:

- Data Domain OS 5
- Fabric 7
- Fabric 8
- FireEye CMS 7
- FireEye CMS 8
- Imperva WebApplication Firewall
- ACME Packet OS
- Juniper IVE 8

Licensing

Qualys OCA is available for free for the existing PC and VM customers.

Customers can allocate a sub-set of PC/VM licenses for this module. The count of the IPs used for OCA would be reduced from the PC/VM license count.

Connect with your Technical account manager or Qualys support for more information.

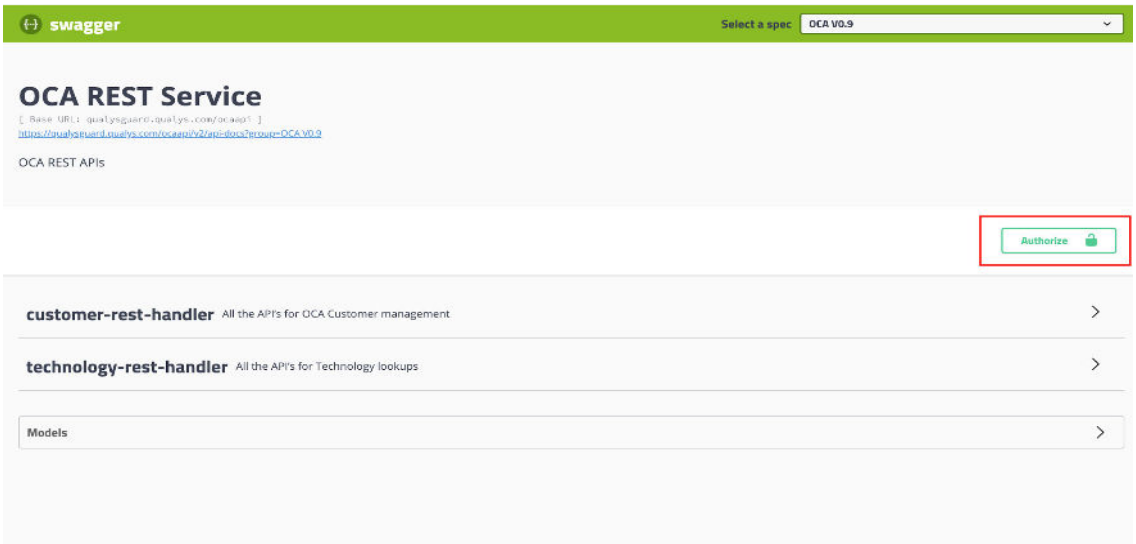
Provision Assets

Accessing the APIs

Access the Swagger UI using below link:

```
https://qualysguard.qualys.com/ocaapi/swagger-ui.html#/
```

Click Authorize and use your Qualys account credentials log in to swagger UI.



Getting a list of Supported Technologies

Before you provision an asset use this API to get a list of supported technologies.

API request:

```
curl -X GET
"https://qualysapi.qualys.com/ocaapi/v1.0/technology/PolicyCompliance" -H "accept: application/json" -H "authorization: Basic cXVheXNfbWQ3NTplc1RFNTJmcmFw"
```

Response:

```
[
"Data Domain OS 5",
"Fabric 7",
"Fabric 8",
"FireEye CMS 7",
"FireEye CMS 8",
"Imperva WebApplication Firewall",
```

```
"ACME Packet OS",
"Juniper IVE 8"
]
```

Provisioning an Asset

Provision an asset by using the POST API call

Mandatory fields: hostIP, network, type, and technology

Sample request body:

```
{
"technology" : "FireEye CMS 8",
"dnsName" : "wpi-rwc01.eng.com",
"hostIP" : "10.11.10.5",
"mac" : "10-20-09-90-44-30",
"network" : "eng",
"netbios": "wpi-rwc01",
"type":"PolicyCompliance"
}
```

API request:

```
curl -X POST "https://qualysapi.qualys.com/ocaapi/v1.0/asset" -H
"accept: application/json" -H "authorization: Basic
cXVheXNfaHMxMDpwY1F3ZWIxMjMj" -H "Content-Type: application/json"
-d "{\"technology\" : \"FireEye CMS 8\",\"dnsName\" : \"wpi-
rwc01.eng.com\",\"hostIP\" : \"10.11.10.5\",\"mac\" : \"10-20-09-
90-44-30\",\"network\" : \"eng\",\"netbios\": \"wpi-
rwc01\",\"type\":\"PolicyCompliance\"}"
```

Response:

```
{
"code": 200,
"data": {
"assetUUID": "abc123"
},
"message": "Provision Requested successfully"
}
```

Asset UUID returned in API response is used in executing other APIs as part of OCA processing.

Getting Asset Status

See the current status of the provisioned asset

Provide the UUID of the required asset.

Mandatory field: Asset UUID

API request:

```
curl -X GET
"https://qualysapi.qualys.com/ocaapi/v1.0/asset/abc123/status" -H
"accept: application/json" -H "authorization: Basic
cXVheXNfaHMxMDpwY1F3ZWIxMjMj"
```

Response:

```
{
"code": 200,
"data": {
"status": "Provision Confirmed"
}
}
```

Get a list of all assets

See the list of UUID for all assets provisioned in your account.

API request:

```
curl -X GET
"https://qualysapi.qualys.com/ocaapi/v1.0/asset?page=0&size=10" -H
"accept: application/json" -H "authorization: Basic
cXVheXNfaHMxMDpwY1F3ZWIxMjMj"
```

Response:

```
[
  {
    "id": "abc123",
    "name": "wpi-rwc01.eng.com",
    "activationModules": null,
    "host": {
      "operatingSystem": "FireEye CMS 8",
      "networkInterfaces": [
        {
          "address": "/10.11.10.5"
        }
      ]
```

```
      }
    },
    {
      "id": "def456",
      "name": "wpi-rwc01.eng.com",
      "activationModules": null,
      "host": {
        "operatingSystem": "FireEye CMS 8",
        "networkInterfaces": [
          {
            "address": "/10.11.10.5"
          }
        ]
      }
    }
]
```

Provision assets in bulk

You can provision more than one asset by attaching a text file with information for all fields required to provision an asset.

The “data” key is a mandatory field that can accept a text file or plain text to execute this API . Swagger-UI accepts only files, however CURL calls can accept string as well under “data” key. There is a certain format that needs to be followed.

The header “technology,dnsname,hostip,mac,network,netbios,type,uuid” needs to be given as first line before giving any asset details as the header is mandatory to execute this API call successfully. The uuid field is mandatory only in case of reprovisioning of an asset.

API request:

```
curl -X POST "https://qualysapi.qualys.com/ocaapi/v1.0/asset/bulk"
-H "accept: application/json" -H "authorization: Basic
cXVheXNfaHMxMDpwY1F3ZWIxMjMj" -H "Content-Type: multipart/form-
data" -F "data=@Bulk_Provision.txt;type=text/plain"
```

Response:

```
{
  "code": 200,
  "data": {
    "items": {
      "count": {
        "successfulProvisions": 3,
        "failedProvisions": 0
      },
```

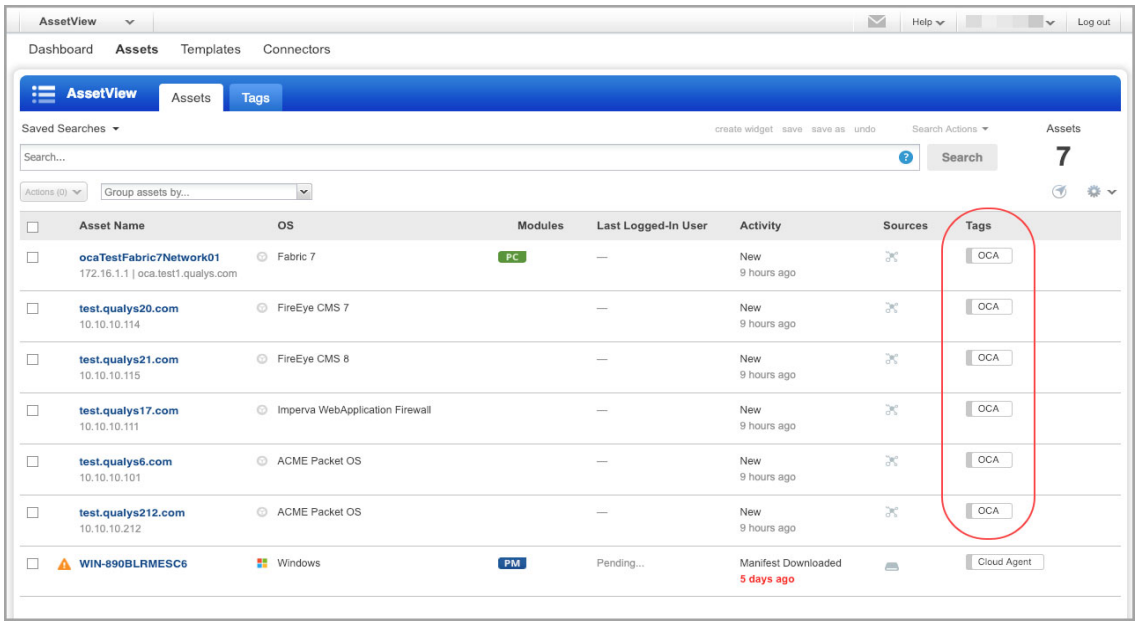
```
      "successfulProvisions": [
        {
          "uuid": "hif567",
          "ip": "11.30.11.2",
          "network": "eng-pc1234",
          "technology": "FireEye CMS 8"
        },
        {
          "uuid": "jkl987",
          "ip": "11.12.10.15",
          "network": "eng-pc123",
          "technology": "FireEye CMS 8"
        },
        {
          "uuid": "mln587",
          "ip": "10.12.11.11",
          "network": "eng-pc12",
          "technology": "Fabric 8"
        }
      ],
      "failedProvisions": []
    }
  }
}
```

Viewing provisioned assets in AssetView module

Once the assets are successfully provisioned, you can navigate to the AssetView module on Qualys UI to see all the provisioned assets and their details.

Make sure you log in to your Qualys account using the same credentials you used to provision assets.

Pick AssetView in the module picker and navigate to the Assets tab. You'll see the OCA tag applied to all the assets you provisioned using the OCA API.



Upload Asset Configuration Data

Once the assets are provisioned, you can now upload the output of the device config file for the offline devices against these asset UUIDs. The data returned to Qualys is consumed by the policy compliance controls which evaluates the data and reports are generated to see how secure these assets or offline devices are.

The commands need to be executed manually on the devices and the output for each command in form of the text file or string is sent to our API. The API will then evaluate the data and generate Compliance report.

These commands are specific to each technology we support and relevant APIs are exposed which you need to run to find supported commands for a technology.

Getting supported commands for a technology

See the commands for the specified technology

The mandatory fields of this API call are Technology Name and Type.

API request:

```
curl -X POST
"https://qualysapi.qualys.com/ocaapi/v1.0/technology/Fabric%207/co
mmand/PolicyCompliance" -H "accept: application/json" -H
"authorization: Basic cXVheXNfaHMxMDpwY1F3ZWIxMjMj"
```

Response:

```
[
  "tsclockserver",
  "snmpconfig --show snmpv1",
  "configshow -all",
  "userConfig --show admin",
  "userConfig --show root",
  "userConfig --show user",
  "version",
  "syslogadmin --show -ip"
]
```

Getting supported commands based on UUID

Get supported commands based on asset UUID

The mandatory fields of this API calls are Asset UUID and Type.

API request:

```
curl -X GET
"https://qualysapi.qualys.com/ocaapi/v1.0/asset/abc123/command/Pol
```

```
icyCompliance" -H "accept: application/json" -H "authorization:
Basic cXVheXNfaHMxMDpwY1F3ZWIxMjMj"
```

Response:

```
{
  "code": 200,
  "data": {
    "items": [
      "tsclockserver",
      "snmpconfig --show snmpv1",
      "configshow -all",
      "userConfig --show admin",
      "userConfig --show root",
      "userConfig --show user",
      "version",
      "syslogadmin --show -ip"
    ]
  }
}
```

Uploading command outputs

Once you have the supported command from earlier APIs, these commands need to be run on respective devices and outputs of these commands need to be uploaded to Qualys platform in form of text file or string. For this purpose, you use a POST API call which accepts three mandatory fields Command as Key, Text file / String as value and authorization (ie Basic Auth header) which are Qualys credentials.

This particular API is not supported via Swagger-UI in this OCA release due to the SpringFox dependency, which needs to support Open API v3 in their next release. For now, this API needs to be run using Postman or CURL only.

Use Qualys credentials in the Authorization tab of Postman, with Type as “Basic Auth”.

Enter the supported command in the Key field and text file/string having command's output in the Value field. Outputs for all the supported commands for an asset can be sent in a single API call or separate API calls..

Headers must be in the following format to run this API. The Authorization header is generated using provided credentials..

Sample 1 - Successful upload response

```
{
    "code": 200,
    "message": "Successfully uploaded command outputs"
}
```

Sample 2 - Failed upload response

```
{
    "_error":
   {
        "code": 400,
        "message": "ERR-2018 - Invalid  received as following
commands = [show running-config al]"
    }
}
```

Sample CURL call with Text and File as keys for FireEye

```
curl -X POST \
https://qualysapi.qualys.com/ocaapi/v1.0/asset/3f0eac6f-6140-41cf-
a136-eed7373d766f/command/output/PolicyCompliance \
```

```
  -H 'Accept: application/json' \
  -H 'Authorization: Basic cXVheXNfaHM1OnFhdGVtcDEyMw==' \
  -H 'content-type: multipart/form-data; boundary=----
WebKitFormBoundary7MA4YWxkTrZu0gW' \
  -F 'tsclockserver=@C:\sclockserver.txt' \
  -F 'version=@C:\version.txt' \
  -F 'syslogdipshow=syslog.1        10.170.65.31'
```

Sample CURL call with Text and File as keys for Fabric

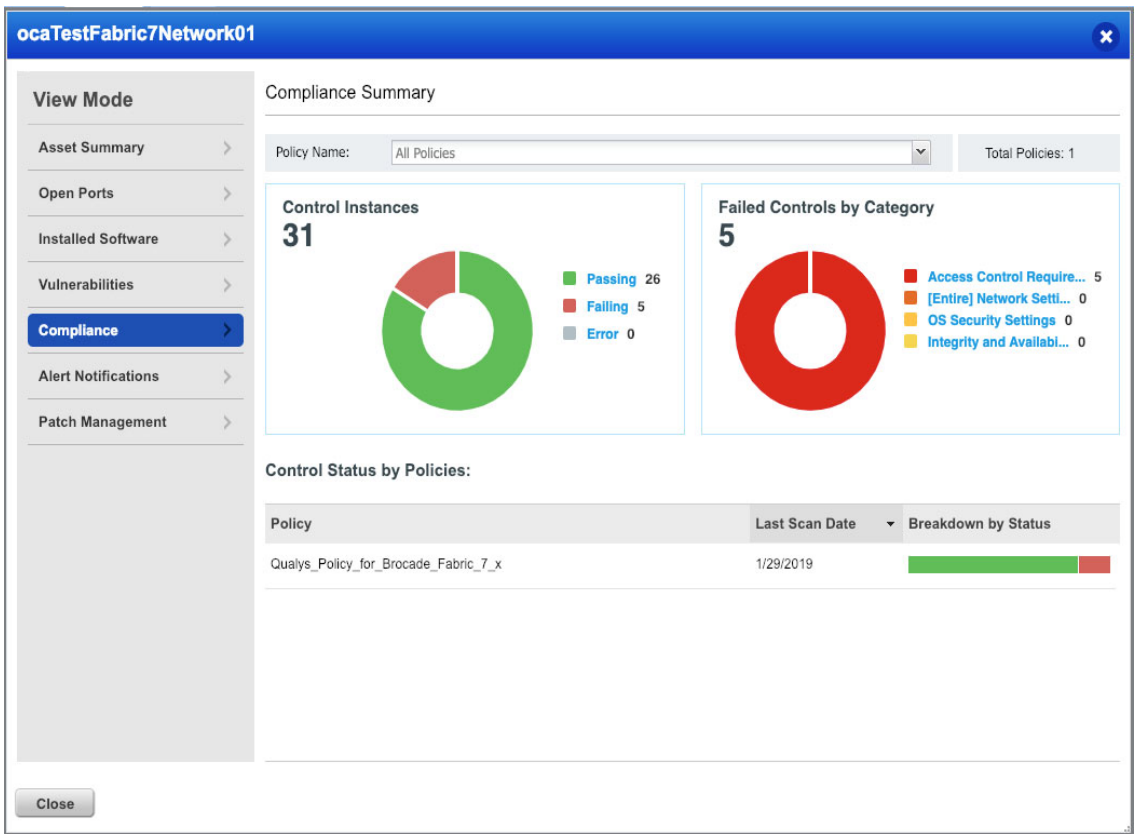
```
curl -X POST \
https://qualysguard.qualys.com/ocaapi/v1.0/asset/f559d20c-1f3f-
4204-81ca-b79ca816f950/command/output/PolicyCompliance \
  -H 'Accept: application/json' \
  -H 'Authorization: Basic cXVheXNfbWQ3NTplc1RFNTJmcmFw' \
  -H 'content-type: multipart/form-data; boundary=----
WebKitFormBoundary7MA4YWxkTrZu0gW' \
  -F 'tsclockserver=Active NTP Server 10.170.158.11
Configured NTP Server List
10.170.158.11;10.170.158.12;10.150.114.234
' \
  -F 'version=Kernel: 2.6.14.2
Fabric OS: v7.0.1b
Made on: Wed May 9 17:23:53 2012
Flash: Sat Nov 22 20:17:59 2014
BootProm: 1.0.15'
```

View Compliance Posture of Assets

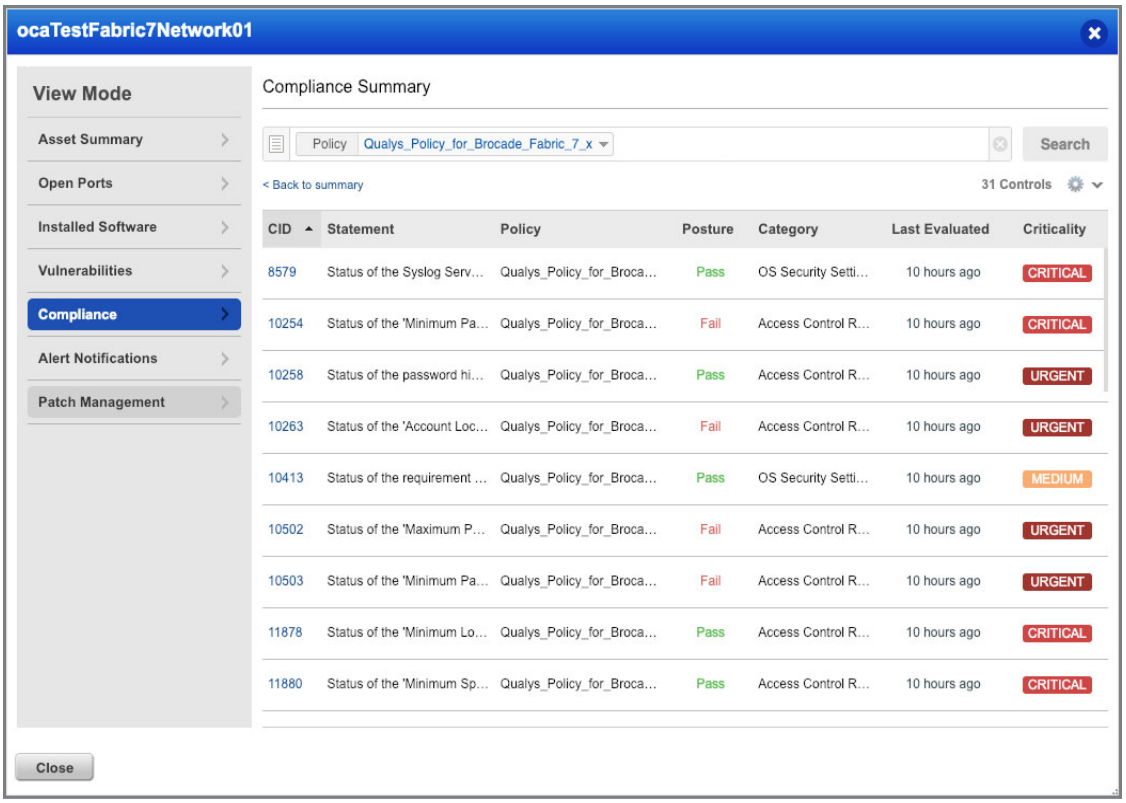
Now that you have uploaded data for the assets you can view the data against the policy compliance controls in the AssetView and Policy Compliance modules.

Log in to your Qualys account using the same credentials you used to provision assets and upload the output of the device config file.

In the AssetView module under the Assets tab you can see all the OCA assets. Using the Quick Action menu open the Assets Details and navigate to the Compliance tab to see the summary of passed and failed controls. These controls were evaluated against the data uploaded through the text file.

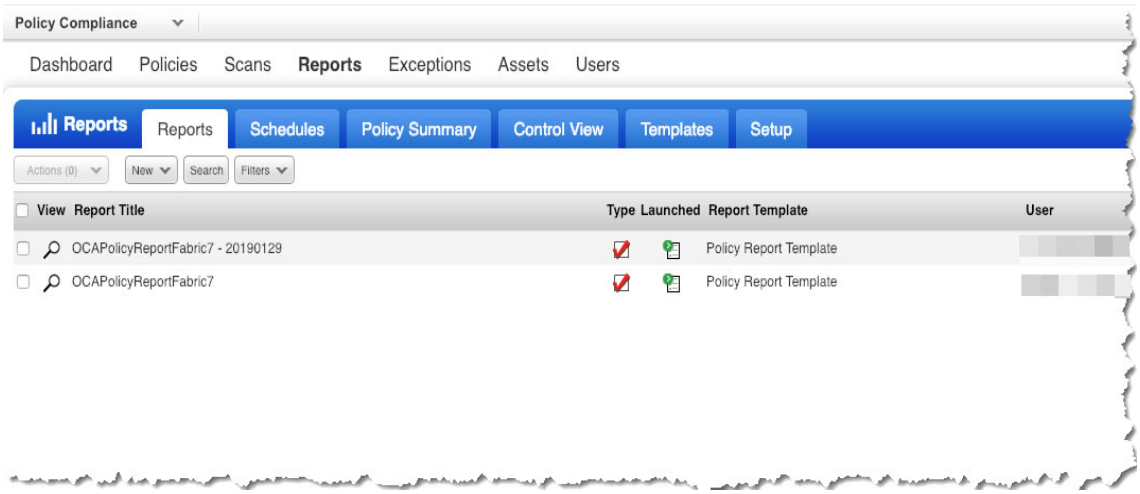


Click on the Policy name to view the evaluated control details.



You can also view the Compliance report from the Policy Compliance module.

From the module picker go to the Policy Compliance module and navigate to the Reports tab. Here you can view or download the compliance report to see detailed control evaluation of your data.



Policies and Reports in OCA

You can generate assessment reports similar to the data collected from Qualys agents or traditional Qualys scanners once the signature evaluation is completed on the uploaded data.

The evaluation report displays the OCA assessment in the same format as that of other assets in the environment. The reports can be generated according to different frameworks. All the controls added for OCA supported technologies are mapped with mandates such as GDPR, PCIDSS, HIPAA, etc. This also enables you to generate mandate-based reports.

Manage Provisioned Assets

You can manage (delete or reprovision) your provisioned assets using APIs.

Deleting Assets

Delete a provisioned OCA asset.

Asset UUID is a mandatory field.

API request:

```
curl -X DELETE
"https://qualysapi.qualys.com/ocaapi/v1.0/asset/abc123" -H
"accept: application/json" -H "authorization: Basic
cXVheXNfaHMxMDpwY1F3ZWIxMjMj"
```

Response:

```
{
  "code": 200,
  "data": {
    "assetUUID": "abc123"
  },
  "message": "Successfully revoked"
}
```

Reprovision Assets

In case you want to edit the asset information of a provisioned asset you need to reprovision the asset.

Values for these fields cannot be changed: hostIP, network, type, technology

All the other fields can be updated and the asset can be reprovisioned.

The Asset reprovision API is done using the same API POST call used to provision an asset. The only difference comes in the request body where you need to include the asset UUID as part of asset reprovisioning request.

Sample Reprovisioning Request Body:

```
{
"uuid": "abc123",
"technology" : "FireEye CMS 8",
"hostIP" : "10.11.10.5",
"mac" : "10-20-09-90-44-30",
"network" : "eng1",
"netbios": "acd",
"type":"PolicyCompliance"
}
```

API request:

```
curl -X POST "https://qualysapi.qualys.com/ocaapi/v1.0/asset" -H
"accept: application/json" -H "authorization: Basic
cXVheXNfaHMxMDpwY1F3ZWIxMjMj" -H "Content-Type: application/json"
-d "{\"uuid\": \"abc123\",\"technology\" : \"FireEye CMS
8\",\"hostIP\" : \"10.11.10.5\",\"mac\" : \"10-20-09-90-44-
30\",\"network\" : \"eng1\",\"netbios\":
\"acd\",\"type\":\"PolicyCompliance\"}"
```

Response:

```
{
  "code": 200,
  "data": {
    "assetUUID": "abc123"
  },
  "message": "Reprovision Requested successfully"
}
```

Troubleshooting

Error Codes

ERR-2001 - CUSTOMER NOT FOUND

If any of the API calls are made before authorizing the Qualys credentials in Swagger UI.

Please wait for a minute as it takes some time to sync customer just enabled for OCA to be eligible for provisioning assets under it.

ERR-2002 - AGENT NOT FOUND

Please check if the “asset_uuid” provided in the curl call or in Swagger UI is an existing asset UUID. API to get all assets can be used to find all asset UUIDs that are provisioned successfully. This could be returned when reprovisioning request rejected due to agent not found.

ERR-2003 - TECHNOLOGY NOT FOUND

Please check if “technology” provided in curl call or in Swagger UI is valid. Also check API to get supported technologies for valid value. The technology name field is case sensitive.

ERR-2004 - AGENT ALREADY EXISTS

Existing assets found while provisioning request",

"items":


```
[
{
"uuid": "ff9dfe3e-5c35-4a42-b04c-bf17ab114ed9",
"customerUUID": "65deb424-9a37-ff75-8017-2efc0a5aad0b",
"dnsName": "wpi-rwc01.eng.com",
"hostIP": "10.11.10.5",
"mac": "10-20-09-90-44-30",
"netbios": "wpi-rwc01",
"network": "eng",
"type": "PolicyCompliance",
"technology": "FireEye CMS 7",
"revoked": false
}
]
```


In case of provision, if there are existing asset(s) under logged in customer within requested network i.e “eng” having matching hostIP or netbios or dnsName or mac, the matching assets are returned as a list with their metadata including UUID. It is possible to reprovision the asset in this case by providing also UUID as part of request body after picking up most appropriate UUID from the list returned in response body.

ERR-2017 - INVALID PROVISION REQUEST

Please check each provision request to be sure you're not missing a mandatory field.

For provision asset, these 4 fields must be provided in this order:

```
technology, hostIP, network, type
```

For provision asset in bulk, these 7 fields must be provided in this order:

```
technology, dnsName, hostIp, mac, network, netbios, type
```

For reprovision asset, these 8 fields must be provided in this order:

```
technology, dnsName, hostIp, mac, network, netbios, type, uuid
```

Non-mandatory fields like mac and netbios can be skipped by using successive commas. Example:

```
technology,dnsname,hostip,mac,network,netBios,type
FireEye CMS 8,api-kwc01.eng.com,91.11.80.6,,eng1,,PolicyCompliance
```

ERR-2018 - INVALID COMMAND RECEIVED

Please check the commands being passed as keys to curl call. API to get supported commands for an asset can be used to verify this.

ERR-2023 - FAILED IN FETCH COMMANDS

Your session may have expired. Please try again by logging out and logging back in.

ERR-2027 - INVALID MANIFEST TYPE

Please check if "type" field provided in curl call or in Swagger UI is "PolicyCompliance".

ERR-2030 - INVALID CONTENT TYPE

The content-type for HTTP request is "multipart/form-data".

The content-type for the individual file part is "plain/text".

For example: Received=application/zip

Please check value for "data" key which must be either string or a file whose mime type is "plain/text".

ERR-2031 - AGENT ALREADY REVOKED

Please check if "asset_uuid" provided in curl call or in Swagger UI is revoked already. API to check individual asset status can be used to verify this.

ERR-2032 - IP NOT ALLOWED

Found blocked IP while provisioning (e.g. 127.0.0.0). Please check if "IP" provided in curl call or in Swagger UI is not a blocked IP. Following IP ranges are blocked:

```
"0.0.0.0-0.255.255.255",
"127.0.0.0-127.255.255.255",
```

```
"224.0.0.0-239.255.255.255",
"255.0.0.0-255.255.255.255"
```

ERR-2034 - EXCEEDED MAX FILE SIZE

Please check the Content-Length of HTTP request has not exceeded 10 MB which is maximum allowed.

ERR-2035 - MANIFEST NOT ASSIGNED

Please check “type” provided in curl call or in Swagger-UI was also provided during provision request for given asset UUID. API to get all assets shows “activationModules” as PC for type “PolicyCompliance” and this can be used to verify this detail.

ERR-2036 - INVALID IP

Found invalid IP while provisioning (e.g. 1a.11.10.5). Please check if “IP” provided in curl call or in Swagger UI is a valid IP.

ERR-2037 - AGENT DATA MISMATCH

Reprovisioning request rejected as one of IP, Technology, Network data were not matching. Please check if one of hostIP, network or technology has not been modified in reprovision as these are not allowed to change once provisioned. In such a scenario, please revoke the asset and provision new asset.

ERR-2038 - EXCEEDED MAX BATCH SIZE

The total number of assets that can be provisioned in bulk using a single API call cannot exceed 100 records. Please send multiple bulk provision requests using Curl or Swagger-UI in batches of 100 if required.

ERR-2039 - AGENT IS REVOKED

Please check if “asset_uuid” provided in curl call or in Swagger UI is not revoked. API to get an asset status can be used to verify this.

ERR-2041 - INVALID BULK REQUEST HEADER

Expected Header = technology,dnsname,hostip,mac,network,netbios,type,uuid

Please check the header provided as first line in CURL call or in Swagger UI which has to match the expected header provided in response body.