Out-of-band Configuration Assessment
User Guide
Version 1.5

December 16, 2020
Table of Contents

About this Guide ........................................................................................................... 4
About Qualys .................................................................................................................. 4
Qualys Support ............................................................................................................... 4

OCA Overview ............................................................................................................. 5

Get Started ................................................................................................................... 6
Qualys Subscription and Modules required ................................................................. 6
Supported Technologies ............................................................................................... 7
Licensing ........................................................................................................................ 7
Provision Assets ............................................................................................................ 8
Upload Asset Configuration Data ................................................................................ 18
View Compliance Posture of Assets ........................................................................... 22
Policies and Reports in OCA .......................................................................................... 25
Manage Provisioned Assets ......................................................................................... 26

Troubleshooting .......................................................................................................... 31
Error Codes .................................................................................................................... 31
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 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 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 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.

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 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 configuration datapoints and controls and uses them for the assessment.

You can use OCA to assess the security of these critical and disconnected assets and include them in the overall 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.

Accessing the 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 compliance assessment. Also, you can run compliance report on these assets and view these reports in the Policy Compliance module.

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.
Supported Technologies

We are continuously adding to the list of supported technologies. To get a complete list view the Technologies tab in the OCA UI or use the Technology API.

Here are few of the supported technologies:

- Data Domain OS 5
- Fabric 7, 8
- FireEye CMS 7, 8
- IBM z/OS Security Server RACF 2
- Imperva WebApplication Firewall
- ACME Packet OS
- Juniper IVE 8
- HP Safeguard
- Cisco ACS 5
- ArubaOS 6
- ArubaOS 8
- Cisco UCS Manager 2
- Comware 5, 7
- HPE 3Par OS 3
- Symantec SGOS 6
- Cisco FTD 6
- Cisco WLC 8
- Riverbed SteelHead RiOS
- Riverbed SteelHead Interceptor 7
- HP FutureSmart (for HP Printers)
- HP Printers
- Samsung Printers

Licensing

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

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

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

Use these APIs to get a list of supported technologies and provision and manage your assets.

Get a list of Supported Technologies

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

HTTP Status Code

- 200: OK
- 404: Not Found
- 500: Internal Server Error

API request:

curl -X GET
"https://qualysguard.qualys.com/ocaapi/v1.0/technology/PolicyCompliance" -H "accept: application/json" -H "authorization: Basic
cw2VheXNfbWe3NTplc1RNTJmcmFw"

Response:

```
{
  "code": 200,
  "data": [
    {
      "items": [
        {
          "technology": "ACME Packet OS",
          "createdAt": "2019-01-21T07:06:07.000+0000",
          "updatedAt": "2019-01-21T07:06:07.000+0000",
          "technologyVersion": "ACME Packet OS"
        },
        {
          "technology": "ArubaOS",
          "createdAt": "2019-06-07T08:32:43.000+0000",
          "updatedAt": "2020-06-30T11:15:13.000+0000",
          "technologyVersion": "ArubaOS 6"
        },
        {
          "technology": "ArubaOS",
          "createdAt": "2020-07-30T10:13:03.000+0000",
          "updatedAt": "2020-07-30T10:13:03.000+0000",
          "technologyVersion": "ArubaOS 8"
        },
        {
          "technology": "Cisco ACS",
```
"createdAt": "2019-04-02T15:54:18.000+0000",
"updatedAt": "2019-04-02T15:54:18.000+0000",
"technologyVersion": "Cisco ACS 5"
},

{ "technology": "Cisco FTD",
"createdAt": "2019-09-13T07:01:13.000+0000",
"updatedAt": "2019-09-13T07:01:13.000+0000",
"technologyVersion": "Cisco FTD 6"
},

{ "technology": "Cisco UCS Manager",
"createdAt": "2019-06-07T08:32:43.000+0000",
"updatedAt": "2019-06-07T08:32:43.000+0000",
"technologyVersion": "Cisco UCS Manager 2"
},

{ "technology": "Cisco WLC",
"createdAt": "2019-09-13T07:01:12.000+0000",
"updatedAt": "2019-09-13T07:01:12.000+0000",
"technologyVersion": "Cisco WLC 8"
},

{ "technology": "Comware",
"createdAt": "2019-06-07T08:32:43.000+0000",
"updatedAt": "2019-06-07T08:32:43.000+0000",
"technologyVersion": "Comware 5"
},

{ "technology": "Comware",
"createdAt": "2019-06-07T08:32:43.000+0000",
"updatedAt": "2019-06-07T08:32:43.000+0000",
"technologyVersion": "Comware 7"
},

{ "technology": "Data Domain OS",
"createdAt": "2019-01-21T07:06:07.000+0000",
"updatedAt": "2019-01-21T07:06:07.000+0000",
"technologyVersion": "Data Domain OS 5"
},

{ "technology": "Brocade Fabric",
"createdAt": "2019-01-21T07:06:07.000+0000",
"updatedAt": "2019-06-26T12:11:08.000+0000",
"technologyVersion": "Fabric 7"}
"technology": "Brocade Fabric",
"createdAt": "2019-01-21T07:06:07.000+0000",
"updatedAt": "2019-06-26T12:11:08.000+0000",
"technologyVersion": "Fabric 8"
},

"technology": "FireEye CMS",
"createdAt": "2019-01-21T07:06:07.000+0000",
"updatedAt": "2020-08-27T10:15:52.000+0000",
"technologyVersion": "FireEye CMS 7"
},

"technology": "FireEye CMS",
"createdAt": "2019-01-21T07:06:07.000+0000",
"updatedAt": "2020-08-27T10:15:51.000+0000",
"technologyVersion": "FireEye CMS 8"
},

"technology": "HP Printers",
"createdAt": "2020-05-08T05:22:10.000+0000",
"updatedAt": "2020-05-08T05:22:10.000+0000",
"technologyVersion": "HP Printers"
},

"technology": "HP Safeguard",
"createdAt": "2019-04-02T15:54:19.000+0000",
"updatedAt": "2019-04-02T15:54:19.000+0000",
"technologyVersion": "HP Safeguard"
},

"technology": "HPE 3Par OS",
"createdAt": "2019-06-07T08:32:43.000+0000",
"updatedAt": "2019-06-20T01:15:52.000+0000",
"technologyVersion": "HPE 3Par OS 3"
},

"technology": "IBM z/OS",
"createdAt": "2020-06-30T11:15:13.000+0000",
"updatedAt": "2020-06-30T11:15:13.000+0000",
"technologyVersion": "IBM z/OS Security Server RACF 2"
},

"technology": "Imperva WebApplication Firewall",
Get Started
Provision Assets

"createdAt": "2019-01-21T07:06:07.000+0000",
"updatedAt": "2019-01-21T07:06:07.000+0000",
"technologyVersion": "Imperva WebApplication
Firewall"
},
{
"technology": "Juniper IVE",
"createdAt": "2019-01-21T07:06:07.000+0000",
"updatedAt": "2019-01-21T07:06:07.000+0000",
"technologyVersion": "Juniper IVE 8"
},
{
"technology": "Riverbed SteelHead",
"createdAt": "2020-06-30T11:15:13.000+0000",
"updatedAt": "2020-06-30T11:15:13.000+0000",
"technologyVersion": "Riverbed SteelHead
Interceptor 7"
},
{
"technology": "Riverbed SteelHead",
"createdAt": "2019-12-12T06:33:06.000+0000",
"updatedAt": "2019-12-12T06:33:06.000+0000",
"technologyVersion": "Riverbed SteelHead RiOS 9"
},
{
"technology": "Samsung Printers",
"createdAt": "2020-05-08T05:22:10.000+0000",
"updatedAt": "2020-05-08T05:22:10.000+0000",
"technologyVersion": "Samsung Printers"
},
{
"technology": "Symantec ProxySG",
"createdAt": "2019-06-07T08:32:43.000+0000",
"updatedAt": "2019-06-07T08:32:43.000+0000",
"technologyVersion": "Symantec SGOS 6"
}

Provision an Asset

Provision an asset by using the POST API call
Mandatory fields: hostIP, type, and technology
HTTP Status Code
- 200: OK
- 400: Bad Request
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

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

API request:
curl -X POST "https://qualysguard.qualys.com/ocaapi/v1.0/asset" -H "accept: application/json" -H "authorization: Basic cw2VheXNfbWe3NTplc1RNTJmcmFw" -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","netbios": "wpi-rwc01","type": "PolicyCompliance"}"

Response:
{
    "code": 200,
    "data": {
        "assetUUID": "2b60e4bb-5edf-45f3-b558-6fadd4e22e51"
    },
    "message": "Request for Asset Provisioning sent Successfully."
}

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

Get Asset Status for Single Asset
See the current status of the provisioned asset. Provide the UUID of the required asset.
Mandatory field: Asset UUID

**HTTP Status Code**
- 200: OK
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

**API request:**
```bash
curl -X GET "https://qualysguard.qualys.com/ocaapi/v1.0/asset/2b60e4bb-5edf-45f3-b558-6fadd4e22e51/status" -H "accept: application/json" -H "authorization: Basic cw2VheXNfbWe3NTplc1RNTJmcmFw"
```

**Response:**
```json
{
   "code": 200,
   "data": {
      "status": "Provision Confirmed"
   }
}
```
Get Status of Assets Provisioned within given Timeframe

/assets/status/subscriptions/{number_of_days}

To get the status of the assets provisioned in your subscription within a given timeframe.

HTTP Status Code
- 200: OK
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

Input Parameters

| <number_of_days> | (Required) The time-frame for which you would like to fetch the data. You can specify a time-frame within the last 30 days only. |

Header Parameters

| assetFlowType | Provide asset flow type. The default value is "DEFAULT". |

Sample

Request:
curl -X GET "https://qualysguard.qualys.com/ocaapi/v1.0/assets/status/subscriptions/{number_of_days}" -H "accept: application/json" -H "authorization: Basic cw2VheXNfbWe3NTplc1RNTJmcmFw"

Response:

```json
{
  "code": 200,
  "data": [
    {
      "items": [
        {
          "assetUUID": "6xxx3x43-1970-4x93-x290-76x96862x393",
          "status": "Provision Confirmed"
        },
        {
          "assetUUID": "x3x77x64-x046-435x-x015-x55x3230x263",
          "status": "Provision Confirmed"
        },
        {
          "assetUUID": "3xx5411x-0xx6-4619-83xx-28221703xx57",
          "status": "Provision Confirmed"
        }
      ]
    }
  ]
}
```
Provision assets in bulk

You can provision more than one asset by attaching a text or csv 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 csv file to execute this API.

The header "technology,hostip,dnsname,mac,netbios,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.

Note: Using this API, you can provision up to 1000 assets.

HTTP Status Code
- 200: OK
- 400: Bad Request
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

API request:
```bash
curl -X POST
```
"https://qualysguard.qualys.com/ocaapi/v1.0/asset/bulk?manifest_types=PolicyCompliance" -H "accept: application/json" -H "authorization: Basic cw2VheXNfbWe3NTplclRNTJmcmFw" -H "Content-Type: multipart/form-data" -F "data=@Bulk_Provision.txt;type=text/plain"

Response:
{
  "code": 200,
  "data": {
    "items": {
      "count": {
        "successfulProvisions": 3,
        "failedProvisions": 0,
        "skipppedProvisions": 0
      },
      "successfulProvisions": [
        {
          "uuid": "b951414a-94a8-4166-83e7-5957209ae284",
          "ip": "18.10.11.75",
          "technology": "Comware 5"
        },
        {
          "uuid": "c5f333b3-344d-474f-b6f5-4784853ccff2",
          "ip": "19.10.11.76",
          "technology": "HPE 3Par OS 3"
        },
        {
          "uuid": "4032889b-97db-4f2c-9d61-f4b189784ef5",
          "ip": "18.10.11.76",
          "technology": "HPE 3Par OS 3"
        }
      ],
      "failedProvisions": [],
      "skipppedProvisions": []
    }
  }
}
**View 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 a login in the same subscription 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 asset configuration data for the offline devices against these asset UUIDs. The asset configuration data could be the output of certain commands executed on these assets or simply the configuration files on these assets.

The data submitted 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.

Get supported commands for a technology

See the commands for the specified technology.

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

Note: If you want to fetch supported commands for IBM z/OS Security Server RACF 2 technology, use IBM zOS Security Server RACF 2 in the API request (without the "/" special character).

HTTP Status Code
- 200: OK
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

API request:
```
curl -X GET "https://qualysguard.qualys.com/ocaapi/v1.0/technology/Fabric%207/command/PolicyCompliance" -H "accept: application/json" -H "authorization: Basic cw2VheXNfbWe3NTplc1RNTJmcmFw"
```

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

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.

HTTP Status Code
- 200: OK
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

API request:
```bash
curl -X GET
"https://qualysguard.qualys.com/ocaapi/v1.0/asset/2b60e4bb-5edf-45f3-b558-6fadd4e22e51/command/PolicyCompliance" -H "accept: application/json" -H "authorization: Basic cw2VheXNfbWe3NTplc1RNTJmcmFw"
```

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

Once you have the list of 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 four mandatory fields, Command names as Key, output file / String as value, UUID of the asset which is provisioned successfully and authorization (i.e., 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.
HTTP Status Code
200: OK
403: Forbidden
404: Not Found
500: Internal Server Error

Sample 1 - Successful upload response
{
   "code": 200,
   "message": "Command Output Uploaded Successfully."
}

Sample 2 - Failed upload response
{
   "_error": {
      "code": 400,
      "message": "ERR-2018 - Invalid command received as following commands = [show running-config al]"
   }
}

Sample CURL call with File type in keys for FireEye

curl -X POST \
https://qualysguard.qualys.com/ocaapi/v1.0/asset/3f0eac6f-6140-41cf-al36-eed7373d766f/command/output/PolicyCompliance \
   -H 'Accept: application/json' \
   -H 'Authorization: Basic cw2VheXNfbWe3NTplc1RNTJmcmFw==' \
   -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 type in 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 cw2VheXNfbWe3NTplc1RNTJmcmFw' \
   -H 'content-type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW' \
   -F 'tsclockserver=Active NTP Server 10.170.158.11 Configured NTP Server List

Configured NTP Server List
Get Started
View Compliance Posture of Assets

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 OCA, 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 OCA module, click on the Assets tab. Select the required asset and from the Quick Action menu, click View Details. Navigate to COMPLIANCE > Policy Compliance to see the summary of passed and failed controls. These controls are evaluated against the data uploaded through the text 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.

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.

Delete Assets

Delete a provisioned OCA asset. Asset UUID is a mandatory field.

Note: When you delete an asset, all the configuration data and reports related to the asset are also deleted.

HTTP Status Code
- 200: OK
- 400: Bad Request
- 403: Forbidden
- 500: Internal Server Error
- 503: Service Unavailable

API request:

```
curl -X DELETE "https://qualysguard.qualys.com/ocaapi/v1.0/asset/2b60e4bb-5edf-45f3-b558-6fadd4e22e51" -H "accept: application/json" -H "authorization: Basic cw2VheXNfbWe3NTplc1RNTJmcmFw"
```

Response:

```
{
    "code": 200,
    "data": {
        "assetUUID": "2b60e4bb-5edf-45f3-b558-6fadd4e22e51"
    },
    "message": "Asset(s) Revoked Successfully."
}
```

Delete Assets in Bulk

Delete multiple provisioned OCA assets.

Note: When you delete an asset, all the configuration data and reports related to the asset are also deleted.

HTTP Status Code
- 200: OK
- 400: Bad Request
- 403: Forbidden
- 500: Internal Server Error
- 503: Service Unavailable

**Sample Reprovisioning Request:**

```json
{
    "assetList": [
        "x3x96x3x-eb09-4a26-817d-1ed08bd1739b","xx64209x-b526-48f9-9733-2b3ce675c4f0","943x39xx-4d20-4372-8a1d-8a5b3b3b5c7b"
    ]
}
```

**API request:**

```
curl -X DELETE
"https://qualysguard.qualys.com/ocaapi/v1.0/asset/revoke/bulk" -H
"accept: application/json" -H "assetFlowType: DEFAULT" -H
"authorization: Basic cXVheXNfYXQ3NjpRQXR1bXBAMTIz" -H "Content-Type: application/json" -d "{ \"assetList\": [ \"x3x96x3x-eb09-4a26-817d-1ed08bd1739b\",\"xx64209x-b526-48f9-9733-2b3ce675c4f0\",\"943x39xx-4d20-4372-8a1d-8a5b3b3b5c7b\"]}"
```

**Response:**

```json
{
    "code": 200,
    "data": {
        "items": {
            "successfulRevoke": [
                "x3x96x3x-eb09-4a26-817d-1ed08bd1739b",
                "xx64209x-b526-48f9-9733-2b3ce675c4f0",
                "943x39xx-4d20-4372-8a1d-8a5b3b3b5c7b"
            ],
            "failedRevoke": []
        }
    }
}
```

**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, 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.
HTTP Status Code
- 200: OK
- 400: Bad Request
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

Sample Reprovisioning Request:
```
{
    "uuid": "2x60x4xx-5edf-45f3-b558-6fadd4e22e51",
    "technology": "FireEye CMS 8",
    "hostIP": "10.11.10.5",
    "mac": "10-20-09-90-44-30",
    "netbios": "acd",
    "type": "PolicyCompliance"
}
```

API request:
curl -X POST "https://qualysguard.qualys.com/ocaapi/v1.0/asset" -H "accept: application/json" -H "authorization: Basic cw2VheXNfWe3NTplc1RNTJmcmFw" -H "Content-Type: application/json" -d "{"uuid": "2x60x4xx-5edf-45f3-b558-6fadd4e22e51","technology": "FireEye CMS 8","hostIP": "10.11.10.5","mac": "10-20-09-90-44-30","netbios": "acd","type": "PolicyCompliance"}" 

Response:
```
{
    "code": 200,
    "data": {
        "assetUUID": "2x60x4xx-5edf-45f3-b558-6fadd4e22e51"
    },
    "message": "Request for Asset Reprovisioning sent Successfully."
}
```

Reprovision Assets in Bulk
Values for these fields cannot be changed: hostIP, type, technology
All the other fields can be updated and the assets can be reprovisioned.
The Bulk asset reprovisioning is done using the same API POST call used to provision an assets in bulk. The only difference comes in the request where you need to include the asset UUID as part of asset reprovisioning request.

**HTTP Status Code**
- 200: OK
- 400: Bad Request
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

**API Request:**
```
curl -X POST
"https://qualysguard.qualys.com/ocaapi/v1.0/asset/bulk?manifest_types=PolicyCompliance" -H "accept: application/json" -H "assetFlowType: DEFAULT" -H "authorization: Basic cXVheXNfYXQ3NjpRQXRlbXBAMTIz" -H "Content-Type: multipart/form-data" -F "data=@file.txt;type=text/plain"
```

**Response:**
```
{
    "code": 200,
    "data": {
        "items": {
            "count": {
                "successfulProvisions": 2,
                "failedProvisions": 0,
                "skippedProvisions": 0
            },
            "successfulProvisions": [
                {
                    "uuid": "34419070-8659-4686-a66f-21e8b07fb075",
                    "ip": "45.55.54.65",
                    "technology": "Fabric 7"
                },
                {
                    "uuid": "639409b5-137f-4509-afdl-f687416426ca",
                    "ip": "44.55.56.65",
                    "technology": "Fabric 7"
                }
            ]
        }
    }
}
```
Get Started
Manage Provisioned Assets
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",
"type": "PolicyCompliance",
"technology": "FireEye CMS 7",
"revoked": false
}
]

In case of provision, if there are existing asset(s) under logged in customer having
matching hostIP then existing 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 for each asset detail used in bulk file does not miss any mandatory field.

For provisioning one asset, these are the mandatory fields:

- `hostIP`, `type`, `technology`

Note: For bulk provisioning assets, technology and hostIP are mandatory fields and are supposed to be passed in the input file whereas type is already passed along with the API.

For provisioning asset in bulk, these 6 data fields must be provided in this order:

```
technology, hostip, dnsname, mac, netbios, uuid
Comware 5, 18.10.11.75, api-kwc01.eng.com, 10:00:00:00:01:61, NetBios60,
```

Note: If you are provisioning using a file then you can skip uuid as it is mandatory only in case of reprovisioning.

For reprovisioning asset in bulk, these 6 data fields must be provided in this order:

```
technology, hostip, dnsname, mac, netbios, uuid
Comware 5, 18.10.11.75, api-kwc01.eng.com, 10:00:00:00:01:61, NetBios60, 8951414a-94a8-4166-83e7-5957209ae2df
```

**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.

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 or Technology data were not matching. Please check if one of hostIP 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,hostip,dnsname,mac,netbios,uuid
Please check the header provided in the request file matches with the expected header provided in response.

ERR-2046 - Asset Provision Failed
Asset provisioning failed due to incorrect subscription settings. Please contact Qualys support for more information.