Out-of-Band Configuration Assessment API v2

User Guide

Version 1.5

April 1, 2022

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

Table of Contents

Preface

This guide is intended for application developers who will use the Qualys Out-of-band Configuration Assessment API.

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 a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact 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 support information at www.qualys.com/support/.

Chapter 1 - Welcome

Welcome to Out-of-band Configuration Assessment API guide.

Get Started

Qualys API Framework - Learn the basics about making API requests. The base URL depends on the platform where your Qualys account is located.

API Conventions - Get tips on using the Curl command-line tool to make API requests.

Get API Notifications

Subscribe to our API Notifications RSS Feeds for announcements and latest news.

From our Community

Join our Community

API Notifications RSS Feeds

Qualys API Framework

The Qualys Out-of-band Configuration Assessment API uses the following framework.

Request URL

The URL for making API requests respects the following structure:

https://<baseurl>/<module>/<object>/<object_id>/<operation>

where the components are described below.

<baseurl>	The Qualys API gateway URL that you should use for API requests depends on the platform where your account is located. The gateway URL for Qualys US Platform 1 is: https://gateway.qg1.apps.qualys.com
<module>	The API module. For the OCA API, the module is: “oca”.
<object>	The module specific object.
<object_id>	(Optional) The module specific object ID, if appropriate.
<operation>	The request operation, such as provisioning an asset.

Qualys API 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 gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate gateway URL for your account.

API Conventions

Using Curl

Curl is a multi-platform command-line tool used to transfer data using multiple protocols. This tool is supported on many systems, including Windows, Unix, Linux and Mac. In this document Curl is used in the examples to build Qualys API requests using the HTTP over SSL (https) protocol, which is required.

Want to learn more? Visit https://curl.haxx.se/

The following Curl options are used according to different situations:

Option	Description
-X GET/POST/DELETE	The GET, POST, DELETE method are used as per requirement.
-H 'Authorization: Bearer <token>'	This option is used to provide a custom HTTP request header parameter for authentication. Provides the JSON Web Token (JWT) received from Qualys authentication API in the following format: Authorization: Bearer <token>
-H 'content-type: application/json'	Denotes that content is in JSON format.
-H 'Content-Type: text/plain'	Denotes that content is in text or plain format.
-d @request.json	Provide a request.json file for parameter input.
--data-urlencode	Used to encode spaces and special characters in the URL/Parameter values.

The sample below shows a typical Curl request using options mentioned above and how they interact with each other.

curl -X GET 'http://<api_gateway_url>/ocaapi/v2.0/technology/PolicyCompliance' -H 'Content-Type: application/json' -H 'Authorization: Bearer <token>'

Chapter 2 - Version 2 APIs

Note: The following APIs use token-based authentication.

OCA APIs

Fetch Authentication Token

/auth

[POST]

You must authenticate to the Qualys Cloud Platform using Qualys account credentials (username and password) and get the JSON Web Token (JWT) before you can start using the OCA APIs.

The Authentication API returns a JSON Web Token (JWT) which you can use for authentication during OCA API calls. The token expires in 4 hours. You must regenerate the token to continue using the OCA API.

HTTP Status Code

- 201: Created

- 401: Unauthorized user

- 404: Not Found

Parameters

username	The username of the Qualys user account for which you want to fetch OCA data.
password	The password of the Qualys user account for which you want to fetch OCA data.
token	The value should be set to True, to get the generated token.
ContentType	Should be "application/x-www-form-urlencoded"
gateway.qg1.apps.qualys.com	The API gateway URL to the Qualys API server where your account is located.

Sample

Request:

```
curl -X POST 'https://<api_gateway_url>/auth' -d
'username=username&password=password&token=true' -H 'ContentType:
application/x-www-form-urlencoded'
```

Response:


```
kyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJxdWF5c19hdzM5IiwibG9naW5SZXNwb25zZ
SI6IlNVQ0NFU1NGVUwiLCJzdWNjZXNzZnVsQXV0aGVudGljYXRpb25IYW5kbGVycyI
6WyJBdXRoSGFuZGxlcjJdLCJpc3MiOiJxYXMiLCJpcEFkZHJlc3MiOiIxMC4wLjIwM
y4xODQiLCJwb3J0YWxVc2VySWQiOjIzODczNDU1NCwidXNlcnR5cGUiOiJmbyIsInF
3ZWJVc2VySWQiOjM0NzkwMjYsImNyZWRlbnRpYWxUeXBlIjoiPRRzZXJuYW1lUGFzc
3dvcmRDcmVkZW50aWFsIiwiYXVkIjoicWFzIiwibW9kdWxlc0FsbG93ZWQiOlsiQUR
NSV4iLCJBU1NFVCBJTlZFTlRPUlkiLCJDRVJUVklFVyItIkZSRUUgQUdFTlQiLCJQQ
yBTQ0FOTkVSIiwiUFMiLCJRR1MiLCJDQSIsIkNFUlRfVklFVyIsIktCWCIsIk9DQSI
sIlBPUlRBTCBUQUdHSU5HIiwiVEhSRUFUIFBST1RFQ1QiLCJWTEFOIiwiVk0gQUdFT
```

lQiLCJQQVNTSVZFX1NDQU5ORVIiLAJSRVBPUlQgQ0VOVEVSIiwiU0NBX0FHRU5UIiw
iVk0gU0NBTk5FUiIsIkNTIiwiVEhSRUFUX1BST1RFQ1QiLCJWSVJUVUFMIFNDQU5OR
VIiLCJWTSIsIkFQSSIsIkNPTlRBSU5FUl9TRUAVUklUWSIsIkVDMiIsIkdMT0JBTF9
BSV9DTURCX1NZTkMiLCJDTE9VRFZKRVciLCJDTSJsIlBNIiwiU0NBTiBCWSBIT1NUT
kFNRSIsIkFTU0VUX01BTkFHRU1FTlQiLCJDT05USU5VT1VTIE1PTklUT1JJTkciLCJ
JVEFNIiwiUEMiLCJQQ0kiLCJRV0VCX1ZNIiwiU0VNIiwiU0VDVVJFQ09ORklHIl0sI
mF1dGhlbnRpY2F0aW9uTWV0aG9kIjoiQXV0aEhhbmRsZXIiLCJjdXN0d21lcklkIjo
xNDAzMjIyLCJzZXNzaW9uRXhwaXJhdGlvbiI6IjYwIiwidXNlclV1aWQiOiI0YzhhM
mYzNi1hZGNlLTU3NmYtODE1ZC1jNDFlZjUwOGNlNzAiLCJzdWJzY3JpcHRpb25Vd3l
kIjoiNmUyZjAwZDQtNGY2NS1jYjU2LTgyYjctNDk2NzlkMGFmMjRhIiwiaXNUZ3RFe
HBpcmVkIjoidHJ1ZSIsInN1YnNjcmlwdGlvbklkIjoxODYwOTgzLCJleHAiOjE1ODk
4OTYyMjRsImlhdCI6MTU4OTg4MTgyMSwianRpIjoiVEdULTEtenQ5N20wVjlwZWlPS
k1COENYT0ttamZHSENNelZHdE9icGdOaEZpWGE0UHpaSmpPSm9KSjBKSC1obDRCdXB
SaHFYRS1xYXMwMSK9.xbJrVhgdxj8A0LkiPMRWNgGiuqtI954ccpNBx1CvZVEcvIFU
J43kdw81KZIoL8Mm8qrq0f1DjhIDDz83gClZWw

Fetch List of Supported Technologies

/ocaapi/v2.0/technology/PolicyCompliance

[GET]

To get a list of supported technologies.

HTTP Status Code

- 200: OK

- 401: Unauthorized user

- 404: Not found

Header Parameters

authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request:

```
curl -X GET
'https://<api_gateway_url>/ocaapi/v2.0/technology/PolicyCompliance
' -H 'Content-Type: application/json' -H 'Authorization: Bearer
<token>'
```

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",
                "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

/ocaapi/v2.0/asset

[POST]

To add an asset.

HTTP Status Code

- 200: OK
- 400: Bad Request
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests

Input Parameters

dnsName	(Optional) Enter the domain name.
hostIP	(Required) Enter the host IP for the asset to be provisioned.
mac	(Optional) Enter mac address for the asset.
modelName	Enter the model name of the asset to be provisioned. This parameter input is not required if assetFlowType is set DEFAULT.
netbios	(Optional) Enter the netbios of the asset to be provisioned.
serialNumber	Enter the serial number of the asset to be provisioned. This parameter input is not required if assetFlowType is set DEFAULT.
technology	(Required) Technology name of the asset.
type	(Required) Manifest type of asset. Allowed values: PolicyCompliance
uuid	(Optional) The UUID of asset to be re-provisioned. This is required only during re-provisioning.

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API

Sample

Sample Request body:

```
{
"dnsName": "string",
"hostIP": "string",
"mac": "string",
"modelName": "string",
"netbios": "string",
"serialNumber": "string",
"technology": "string",
"type": "string",
"uuid": "string"
}
```

API Request:

```
curl -X POST 'https://<api_gateway_url>/ocaapi/v2.0/asset' -H
'assetFlowType: DEFAULT' -H 'Content-Type: application/json' -H
'Authorization: Bearer <token>' -H 'Content-Type: text/plain' -d
@request.json
```

Response:

```
{
    "code": 200,
    "data": {
        "assetUUID": "663a040b-c9c7-4bee-b4a3-f4f8bf61b8a5"
    },
    "message": "Request for Asset Provisioning sent Successfully."
}
```

Fetch Asset Status using UUID

/ocaapi/v2.0/asset/<asset_uuid>/status

[GET]

Get the current provision status of an asset using UUID.

HTTP Status Code

- 200: OK

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

Input Parameters

asset_uuid	(Required) Provide the UUID of the asset.

Header Parameter

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Response:

```
curl -X GET
'https://<api_gateway_url>/ocaapi/v2.0/asset/<asset_uuid>/status'
-H 'assetFlowType: DEFAULT' -H 'Authorization: Bearer <token>'
```

Response when the provision is successful:

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

Response when the provision is not successful:

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

Fetch Supported Commands for a Technology

/ocaapi/v2.0/technology/<technology_name>/command/PolicyCompliance

[GET]

Get the commands for the specified technology.

HTTP Status Code

- 200: OK

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

Input Parameters

technology_name	(Required) The name of the technology for which the supported commands are to be fetched. 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).

Header Parameters

authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request:

```
curl -X GET
'https://<api_gateway_url>/ocaapi/v2.0/technology/<technology_name
>/command/PolicyCompliance' -H 'Authorization: Bearer <token>'
```

Response:

```
{
    "code": 200,
    "data": {
        "items": [
            "show running-config"
        ]
    }
}
```

Fetch Supported Commands based on Asset UUID

/ocaapi/v2.0/asset/<asset_uuid>/command/PolicyCompliance

[GET]

Get supported commands for a technology using asset UUID.

HTTP Status Code

- 200: OK

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

Input Parameters

asset_uuid	(Required) Provide the UUID of the asset.

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request:

```
curl -X GET
'https://<api_gateway_url>/ocaapi/v2.0/asset/<asset_uuid>/command/
PolicyCompliance' -H 'assetFlowType: DEFAULT' -H 'Authorization:
Bearer <token>'
```

Response:

```
{
    "code": 200,
    "data": {
        "items": [
            "show running-config"
        ]
    }
}
```

Upload Command Output for a UUID

/ocaapi/v2.0/asset/<asset_uuid>/command/output/PolicyCompliance

[POST]

Upload the supported command output to Qualys platform for an asset using UUID. These commands are uploaded in form of text file or string.

HTTP Status Code

- 200: OK

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

Input Parameters

command	(Required) The command output for commands generated using the Fetch Supported Commands for a Technology API.
asset_uuid	(Required) Provide the UUID of the asset.

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request for uploading data through file:

```
curl -X POST
'https://<api_gateway_url>/ocaapi/v2.0/asset/<asset_uuid>/command/
output/PolicyCompliance' -H 'assetFlowType: DEFAULT' -H
'Authorization: Bearer <token>' -F ' show running-
config=@file_path'
```

Request for uploading the data directly:

```
curl -X POST 'https:// <api_gateway_url>/ocaapi/v2.0/asset/<
asset_uuid >/command/output/PolicyCompliance -H 'assetFlowType:
DEFAULT' -H 'Authorization: Bearer <token> -F 'show running-
config=
version 6.5
enable secret "******"
enable bypass
hostname "Aruba001"
```

```
clock timezone GMT 0
banner motd ^
'
```

Response:

```
{
    "code": 200,
    "message": "Command Output Uploaded Successfully."
}
```

Delete an Asset using UUID

/ocaapi/v2.0/asset/<asset_uuid>

[DELETE]

To delete an asset using UUID.

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

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

- 503: Service Unavailable

Input Parameters

asset_uuid	(Required) Provide the UUID of the asset.

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request:

```
curl -X DELETE
'https://<api_gateway_url>/ocaapi/v2.0/asset/<asset_uuid>' -H
'assetFlowType: DEFAULT' -H 'Authorization: Bearer <token>'
```

Response:

```
{
    "code": 200,
    "data": {
        "assetUUID": "663a040b-c9c7-4bee-b4a3-f4f8bf61b8a5"
    },
    "message": "Asset(s) Revoked Successfully."
}
```

Provision Assets in Bulk

/ocaapi/v2.0/asset/bulk

[POST]

To provision more than one asset.

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

HTTP Status Code

- 200: OK

- 400: Bad Request

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

Input Parameters

data	(Required) File containing the entries of asset to be provisioned. Accepted Files: .csv and .txt. Example: bulk_provision.csv or bulk_provision.txt
manifest_types	(Required) Manifest type of asset. Allowed values: PolicyCompliance

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request:

```
curl -X POST
'https://<api_gateway_url>/ocaapi/v2.0/asset/bulk?manifest_types=P
olicyCompliance' -H 'assetFlowType: DEFAULT' -H 'Authorization:
Bearer <token>' -H 'Content-Type: multipart/form-data' -F
'data=@file_path'
```

Response: Unsuccessful upload response

```
{
    "_error": {
        "code": 400,
        "message": "ERR-2052 - [txt,csv] are supported
```

```
extension.Please upload file appropriately"
    }
}
```

Response: Successful upload response


```
{
  "code": 200,
  "data": {
    "items": {
      "count": {
        "successfulProvisions": 4,
        "failedProvisions": 0,
        "skipppedProvisions": 0
      },
      "successfulProvisions": [
        {
          "uuid": "cc1f2ce1-fb4c-40d9-84fe-6a41c33fd0a4",
          "ip": "44.45.36.65",
          "technology": "Fabric 7"
        },
        {
          "uuid": "ae99b9d3-d1eb-4004-bea8-4270ac94732c",
          "ip": "44.45.38.89",
          "technology": "Fabric 8"
        },
        {
          "uuid": "a793043b-5a3b-4007-90f6-be695ec52eb9",
          "ip": "45.45.34.66",
          "technology": "Fabric 7"
        },
        {
          "uuid": "51f1ee4a-9f0e-4531-9d3a-5cde9901ce1b",
          "ip": "44.45.37.62",
          "technology": "Fabric 8"
        }
      ],
      "failedProvisions": [],
      "skippedProvisions": []
    }
  }
}
```

Delete Assets in Bulk

/ocaapi/v2.0/asset/revoke/bulk

[DELETE]

To delete more than one assets.

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

HTTP Status Code

- 200: OK

- 400: Bad Request

- 401: Unauthorized user

- 403: Forbidden

- 503: Service Unavailable

Input Parameters

assetList	(Required) List of assets_UUID to be deleted.

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Sample request body:

```
{
  "assetList": [
    "4x5xx573-x145-4182-916x-x3997x9xx259",
    "5xxxx860-25x1-4x8x-x336-8x20x6x163xx"
  ]
}
```

Request:

```
curl -X DELETE
'http://<api_gateway_url>/ocaapi/v2.0/asset/revoke/bulk' -H
'assetFlowType: DEFAULT' -H 'Content-Type: application/json' -H
'Authorization: Bearer <token>' -H 'Content-Type: text/plain' -d
@request.json
```

Response:


```
{
    "code": 200,
    "data": {
        "items": {
            "successfulRevoke": [
                "4x5xx573-x145-4182-916x-x3997x9xx259",
                "5xxxx860-25x1-4x8x-x336-8x20x6x163xx"
            ],
            "failedRevoke": []
        }
    }
}
    }
}
```

Re-Provision Asset

/ocaapi/v2.0/asset

[POST]

To re-provision an asset.

Note: Values for these fields cannot be changed: hostIP, type, technology. All the other fields can be updated and the asset can be reprovisioned.

HTTP Status Code

- 200: OK

- 400: Bad Request

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

Input Parameters

dnsName	(Optional) Enter the domain name.
hostIP	(Required) Enter the host IP for the asset to be re-provisioned.
mac	(Optional) Enter mac address for the asset.
modelName	Enter the model name of the asset to be re-provisioned. This parameter input is not required if assetFlowType is set DEFAULT.
netbios	(Optional) Enter the netbios of the asset to be re-provisioned.
serialNumber	Enter the serial number of the asset to be re-provisioned. This parameter input is not required if assetFlowType is set DEFAULT.
technology	(Required) Technology name of the asset.
type	(Required) Manifest type of asset. Allowed values: PolicyCompliance
uuid	(Required) The UUID of asset to be re-provisioned. This is required only during re-provisioning.

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
authorization	(Required) The token that was generated using the Fetch Authentication Token API

Sample

Request:

```
curl -X POST "https://<api_gateway_url>/ocaapi/v2.0/asset" -H
"accept: application/json" -H "assetFlowType: DEFAULT" -H
"Authorization: Bearer <token>" -H "Content-Type:
application/json" -d "{\"technology\":\"Fabric
7\",\"dnsName\":\"Fabric 7
ASSET\",\"hostIP\":\"23.42.52.55\",\"netbios\":\"Web-
test.com\",\"mac\":\"23-42-55-54-22-
11\",\"type\":\"PolicyCompliance\",\"uuid\":\"4891f40f-32c2-47cf-
9f2f-8eb0ca1bfc14\"}"
```

Response:

```
{
  "code": 200,
  "data": {
    "assetUUID": "4891f40f-32c2-47cf-9f2f-8eb0ca1bfc14"
  },
  "message": "Request for Asset Reprovisioning sent Successfully."
}
```

Re-Provision Assets in Bulk

/ocaapi/v2.0/asset/bulk

[POST]

To re-provision an asset in bulk.

Note: Values for these fields cannot be changed: hostIP, type, technology. All the other fields can be updated and the asset can be reprovisioned.

HTTP Status Code

- 200: OK

- 400: Bad Request

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

Input Parameters

data	(Required) File containing the entries of asset to be provisioned. Accepted Files: .csv and .txt. Example: bulk_provision.csv or bulk_provision.txt
manifest_types	(Required) Manifest type of asset. Allowed values: PolicyCompliance

Header Parameters

assetFlowType	Provide asset flow type. The default value is "DEFAULT".
Authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request:

```
curl -X POST
'https://<api_gateway_url>/ocaapi/v2.0/asset/bulk?manifest_types=P
olicyCompliance' -H 'assetFlowType: DEFAULT' -H 'Authorization:
Bearer <token>' -H 'Content-Type: multipart/form-data' -F
'data=@file_path'
```

Response:

```
{
    "code": 200,
    "data": {
```

```
        "items": {
            "count": {
                "successfulProvisions": 2,
                "failedProvisions": 0,
                "skipppedProvisions": 0
            },
            "successfulProvisions": [
                {
                   "uuid": "4b5fb573-c145-4182-916a-a3997f9ff259",
                    "ip": "111.1.8.21",
                    "technology": "Comware 7"
                },
                {
                   "uuid": "5eafe860-25d1-4f8c-a336-8b20a6b163ad",
                    "ip": "111.1.8.20",
                    "technology": "Comware 7"
                }
            ],
            "failedProvisions": [],
            "skippedProvisions": []
        }
    }
}
```

Get status of assets provisioned within given timeframe

/ocaapi/v2.0/assets/status/subscription/{number_of_days}

[GET]

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

HTTP Status Code

- 200: OK

- 401: Unauthorized user

- 403: Forbidden

- 404: Not Found

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".
authorization	(Required) The token that was generated using the Fetch Authentication Token API.

Sample

Request:

```
curl -X GET
'https://<api_gateway_url>/ocaapi/v2.0/assets/status/subscription/
{number_of_days}' -H 'assetFlowType: DEFAULT' -H 'Authorization:
Bearer <token>' -H 'Content-Type: application/json'
```

Response:

```
{
  "code": 200,
  "data": {
    "items": [
      {
        "assetUUID": "3xxxxxx9-245x-4531-x7xx-x84x6386x04x",
        "status": "Provision Confirmed"
      },
      {
        "assetUUID": "56x98x40-2563-4x56-8789-85x7x6x67112",
        "status": "Provision Confirmed"
```

```
      },
      {
        "assetUUID": "9x5x267x-048x-4612-x3xx-768x346x6f7x",
        "status": "Provision Confirmed"
      },
      {
        "assetUUID": "640xxxxx-x725-46x2-956x-8028x9x6xx24",
        "status": "Provision Confirmed"
      }
    ]
  }
}
```