



Out-of-band Configuration Assessment

User Guide

May 24, 2022

Copyright 2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



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
OCA Dashboard	34
OCA Default Dashboard	34
OCA Printers Dashboard	37

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

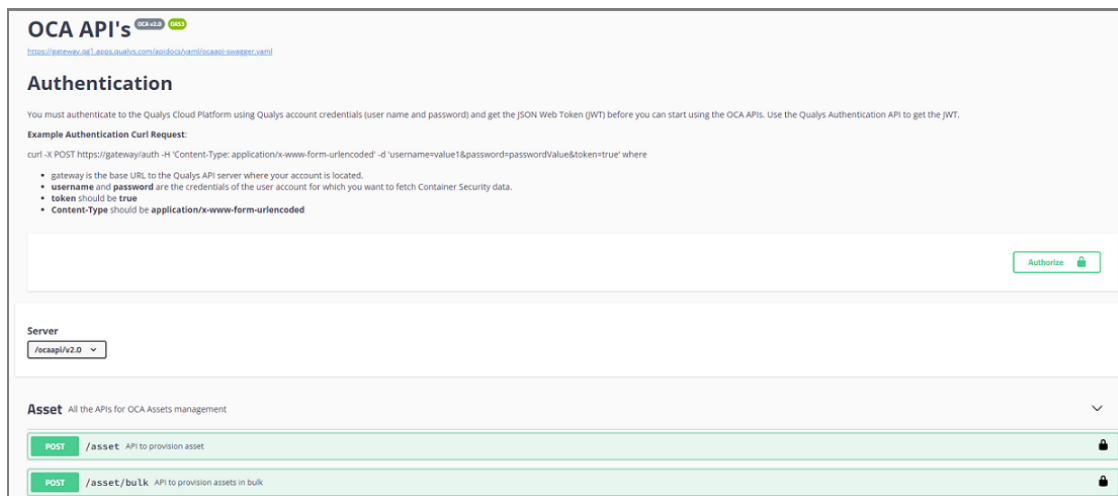
Currently OCA is supported through REST APIs only. Using the APIs you can upload the hosts and their metadata to the Qualys platform.

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 API gateway UI. An example of an API gateway UI link:
`https://<API gateway URL>/apidocs/ocaapi/v2.0/`

Click Authorize and use your Qualys account credentials log in to API gateway 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
- 401: Unauthorized user
- 404: Not Found
- 500: Internal Server Error

API 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

Provision an asset by using the POST API call

Mandatory fields: hostIP, type, and technology

HTTP Status Code

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

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."
}
```

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
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

API request:

```
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"
  }
}
```

Get Status of Assets Provisioned within given Timeframe

/assets/status/subscription/{number_of_days}

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

HTTP Status Code

- 200: OK
- 401: Unauthorized user
- 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".
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"
    }
  ]
}
}

```

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
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

API 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

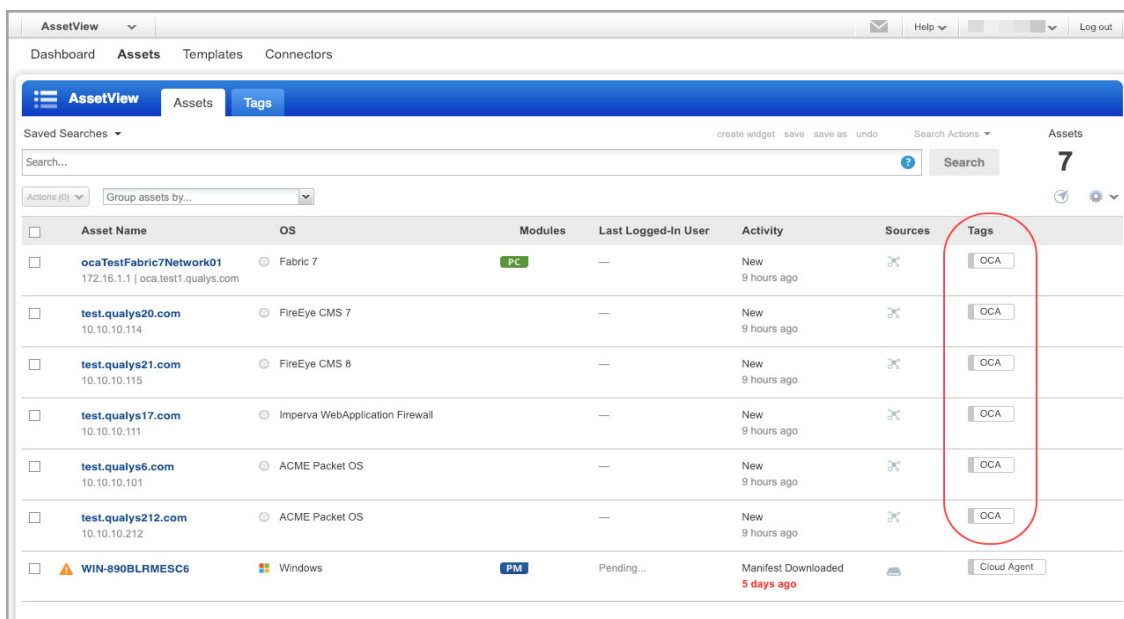
```
{
  "code": 200,
  "data": {
    "items": {
      "count": {
        "successfulProvisions": 4,
        "failedProvisions": 0,
        "skipppeProvisions": 0
      },
      "successfulProvisions": [
        {
          "uuid": "ccl1f2ce1-fb4c-40d9-84fe-6a41c33fd0a4",
          "ip": "44.45.36.65",
          "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": []
    }
  }
}
```


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.



Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
<input type="checkbox"/> ocaTestFabric7Network01 172.16.1.1 oca.test1.qualys.com	Fabric 7	PC	—	New 9 hours ago	✕	OCA
<input type="checkbox"/> test.qualys20.com 10.10.10.114	FireEye CMS 7	—	—	New 9 hours ago	✕	OCA
<input type="checkbox"/> test.qualys21.com 10.10.10.115	FireEye CMS 8	—	—	New 9 hours ago	✕	OCA
<input type="checkbox"/> test.qualys17.com 10.10.10.111	Imperva WebApplication Firewall	—	—	New 9 hours ago	✕	OCA
<input type="checkbox"/> test.qualys6.com 10.10.10.101	ACME Packet OS	—	—	New 9 hours ago	✕	OCA
<input type="checkbox"/> test.qualys212.com 10.10.10.212	ACME Packet OS	—	—	New 9 hours ago	✕	OCA
<input type="checkbox"/> WIN-890BLRMESC6	Windows	PM	Pending...	Manifest Downloaded 5 days ago	☰	Cloud Agent

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
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

API 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"
    ]
  }
}
```

```
}
```

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
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

API 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"  
    ]  
  }  
}
```

Uploading command outputs in Bulk

This feature allows you to upload the output of all the individual commands or the configurations together. The bulk command upload API can consume the o/p of all the individual commands together. Thus, you can upload a single file containing the data for all the commands together. A single file with all the command o/p consolidated makes OCA more scalable for you to upload the data for multiple devices for multiple commands.

These commands need to be run on respective devices, and the consolidated output of these commands need to be uploaded to the Qualys platform in form of a text file.

Technologies that support only .xml and .json files as command output are not supported for the bulk command upload feature in the 1.8.0 release. E.g., HP Printers, Samsung Printers, Juniper JUNOS 15 to 18, ClearPass Policy Manager 6, Cisco UCS Manager 2, Juniper IVE 8, and Pulse Connect Secure 9.

Technology "Microsemi SyncServer 3" supports both .txt and .xml as a command output; the user can convert the .xml output in .txt format and use the bulk command upload feature for uploading the consolidated output.

Use JWT (Jason Web Token) in the Authorization tab of Postman, with Type as "Bearer Token"

The screenshot shows the Postman interface with the Authorization tab selected. The URL is `https://gateway.p04.eng.sjc01.qualys.com/ocaapi/v2.0/asset/db47d4c7-de0c-45ef-b67e-27d9c501aa9d/command/bulk/output/PolicyCompliance ...`. The Type is set to "Bearer Token" and the Token field contains a long alphanumeric string. A "Send" button is visible in the top right corner.

Enter any valid string in the key field and text file having command's output in the Value field. Outputs for all the supported commands for an asset should be sent in a single API call.

The screenshot shows the Postman interface with the Body tab selected. The URL is `https://gateway.p04.eng.sjc01.qualys.com/ocaapi/v2.0/asset/db47d4c7-de0c-45ef-b67e-27d9c501aa9d/command/bulk/output/PolicyCompliance`. The form-data type is selected. A table is shown with the following content:

KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/> file	output_ACME Packet OS.txt			
Key	Value	Description		

Headers must be in the following format to run this API..

Key	Value	Description
<input checked="" type="checkbox"/> User-Agent	PostmanRuntime/7.29.0	
<input checked="" type="checkbox"/> Accept	*/*	
<input checked="" type="checkbox"/> Accept-Encoding	gzip, deflate, br	
<input checked="" type="checkbox"/> Connection	keep-alive	
<input checked="" type="checkbox"/> accept	application/json	
<input checked="" type="checkbox"/> assetFlowType	DEFAULT	
<input checked="" type="checkbox"/> Authorization	Bearer eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ...	

HTTP Status Code

200: OK

400: Bad Request

401: Unauthorized user

403: Forbidden

404: Not Found

500: Internal Server Error

API request:

```
curl -X POST
'https://<api_gateway_url>/oacaapi/v2.0/asset/asset_uuid/command/bulk/output/PolicyCompliance'
-H 'accept: application/json'
-H 'assetFlowType: DEFAULT'
-H 'Authorization: Bearer <token>'
-H 'Content-Type: multipart/form-data'
-F 'data=@samplefile.txt;type=text/plain'
```

Sample 1 - Successful upload response

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

Sample 2 - Unsuccessful upload response

```
{
  "_error": {
    "code": 400,
    "message": "ERR-2070 - Invalid file format. Only txt file type is supported. Please upload a file appropriately"
  }
}
```

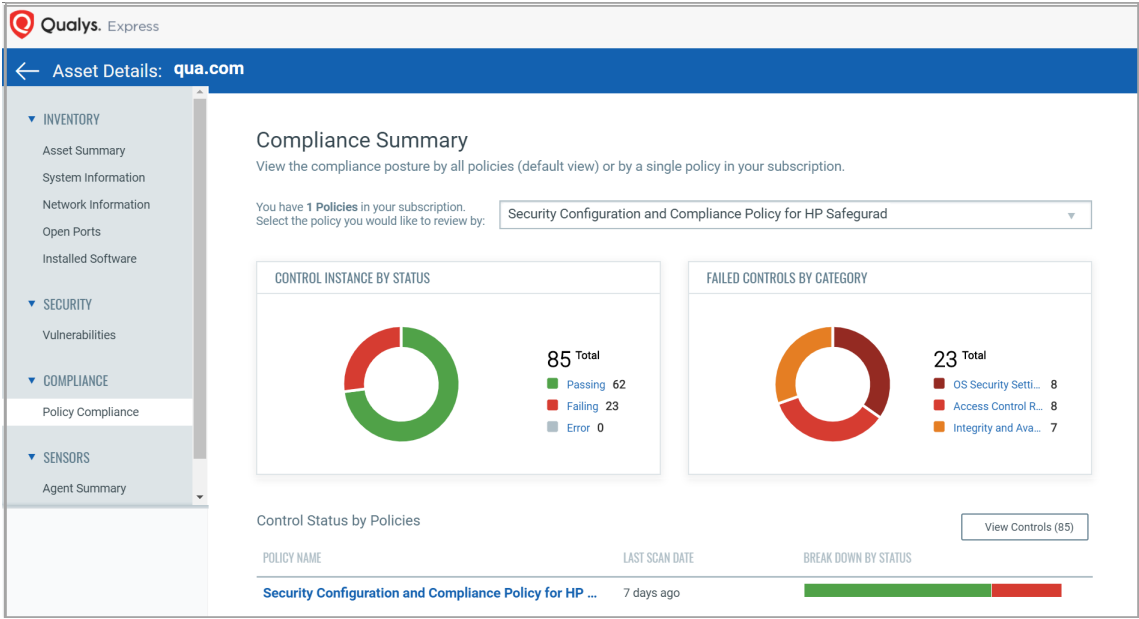
```
}  
}
```

View Compliance Posture of Assets

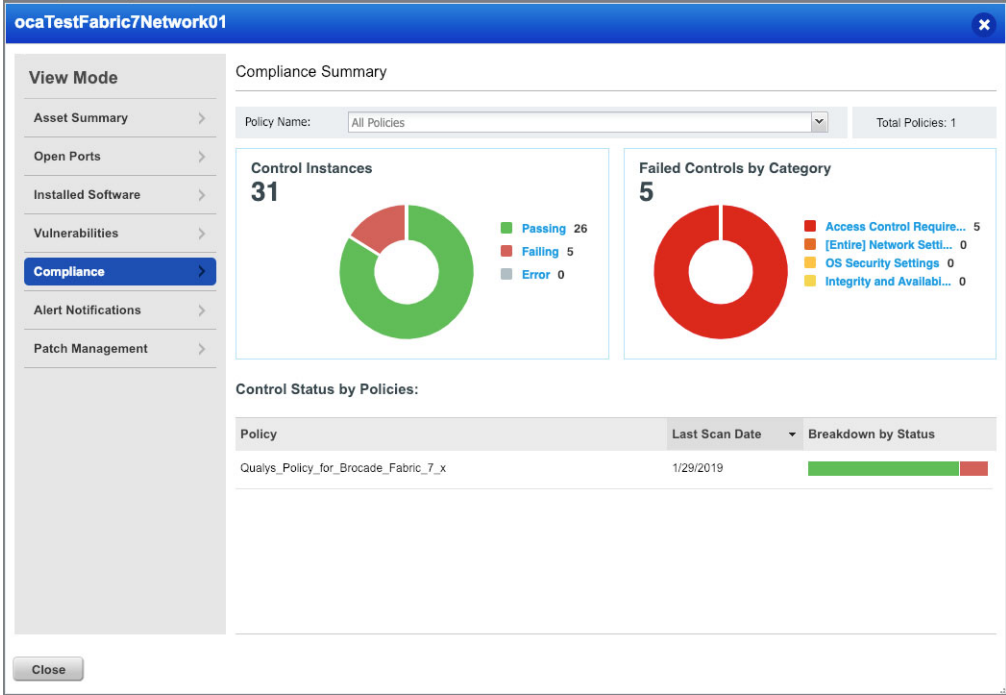
Now that you have uploaded data for the assets you can view the data against the policy compliance controls in OCA, AssetView and Policy Compliance modules.

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.

The screenshot shows the 'evaluated control details' view for the asset 'ocaTestFabric7Network01'. The left sidebar is identical to the previous screenshot. The main content area displays the following:

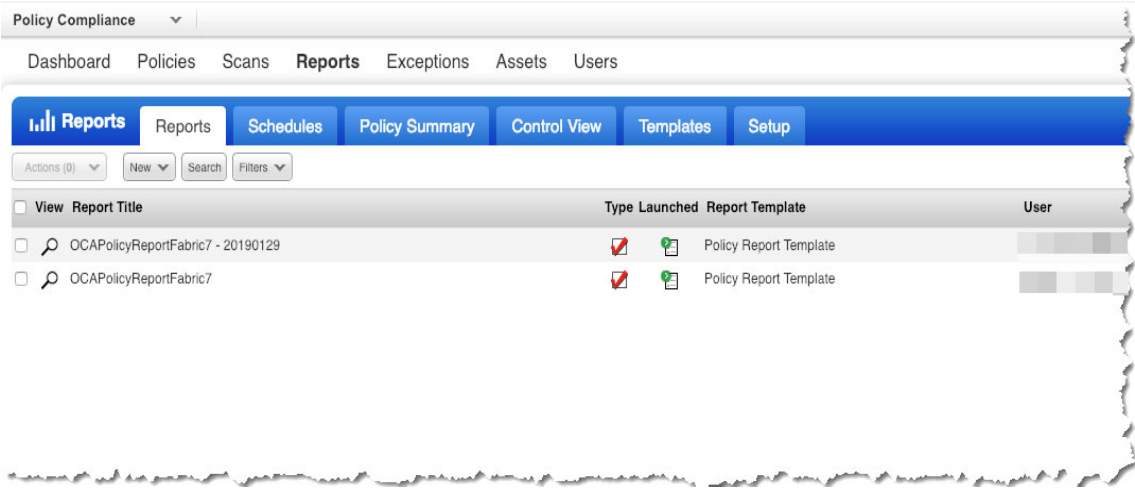
- Policy:** Qualys_Policy_for_Brocade_Fabric_7_x (dropdown), **Search** button.
- < Back to summary** (link), **31 Controls** (text with settings icon).
- Table of evaluated controls:**

CID	Statement	Policy	Posture	Category	Last Evaluated	Criticality
8579	Status of the Syslog Serv...	Qualys_Policy_for_Broca...	Pass	OS Security Settl...	10 hours ago	CRITICAL
10254	Status of the 'Minimum Pa...	Qualys_Policy_for_Broca...	Fail	Access Control R...	10 hours ago	CRITICAL
10258	Status of the password hi...	Qualys_Policy_for_Broca...	Pass	Access Control R...	10 hours ago	URGENT
10263	Status of the 'Account Loc...	Qualys_Policy_for_Broca...	Fail	Access Control R...	10 hours ago	URGENT
10413	Status of the requirement ...	Qualys_Policy_for_Broca...	Pass	OS Security Settl...	10 hours ago	MEDIUM
10502	Status of the 'Maximum P...	Qualys_Policy_for_Broca...	Fail	Access Control R...	10 hours ago	URGENT
10503	Status of the 'Minimum Pa...	Qualys_Policy_for_Broca...	Fail	Access Control R...	10 hours ago	URGENT
11878	Status of the 'Minimum Lo...	Qualys_Policy_for_Broca...	Pass	Access Control R...	10 hours ago	CRITICAL
11880	Status of the 'Minimum Sp...	Qualys_Policy_for_Broca...	Pass	Access Control R...	10 hours ago	CRITICAL

A 'Close' button is located at the bottom left of the window.

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
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error
- 503: Service Unavailable

API 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."
}
```

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

- 401: Unauthorized user
- 403: Forbidden
- 500: Internal Server Error
- 503: Service Unavailable

Sample Reprovisioning Request:

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

API 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": []
    }
  }
}
```

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
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

Sample Reprovisioning Request:

```
{
  "uuid": "4891f40f-32c2-47cf-9f2f-8eb0ca1bfc14",
  "technology" : "Fabric 7",
  "hostIP" : "23.42.52.55",
  "mac" : "23-42-55-54-22-11",
  "netbios": "Webtest.com",
  "type": "PolicyCompliance"
}
```

API 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\": \"Webtest.
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."
}
```

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
- 401: Unauthorized user
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

API 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,
        "skipppeProvisions": 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": []
    }
  }
}
```

Troubleshooting

Error Codes

ERR-2001 - CUSTOMER NOT FOUND

If any of the API calls are made before authorizing the Qualys credentials in API gateway 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 - ASSET NOT FOUND

Please check if the "asset_uuid" provided in the curl call or in API gateway 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 re-provisioning request rejected due to asset not found.

ERR-2003 - TECHNOLOGY NOT FOUND

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

ERR-2004 - ASSET(S) 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 re-provision the asset in this case by providing 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 API gateway 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 - ASSET ALREADY REVOKED

Please check if “asset_uuid” provided in curl call or in API gateway 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 API gateway 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 - MAXIMUM ALLOWED FILE SIZE IS 10 MB

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 API gateway-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 API gateway UI is a valid IP.

ERR-2037 - ASSET DATA MISMATCH

Re-provisioning 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 re-provision 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 API gateway-UI in batches of 100 if required.

ERR-2039 - ASSET IS REVOKED

Please check if “asset_uuid” provided in curl call or in API gateway 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.

ERR-2067 - Invalid file. The file contains invalid delimiters.

The file is invalid because it contains invalid delimiters or no delimiters. Verify and provide the file with correct delimiters.

ERR-2066 - Invalid file. The txt format is not supported for this asset's technology.

The file is invalid because the txt format is not supported for the asset's technology. Use the file with the supported format.

ERR-2069 - Key contains invalid characters. Special characters are not allowed in the key.

Please check if you entered an invalid character in the key.

ERR-2068 - Missing key. Key is mandatory when uploading a file.

Please make sure that you enter the key when you upload the file.

ERR-2068 - Multiple files received. Upload a single file after consolidating the output of multiple commands.

Please check if you uploaded multiple files for bulk command upload API. You must upload a single file at a time.

ERR- 2066 - Invalid file. Bulk command upload is not supported for this technology yet.

The error message is shown for the technologies which support command o/p in XML or in JSON format, which is not supported for the bulk command upload feature.

ERR-2052- Invalid file format. Only txt file type is supported. Please upload a file appropriately.

Please make sure that the file with only the txt type is uploaded.

OCA Dashboard

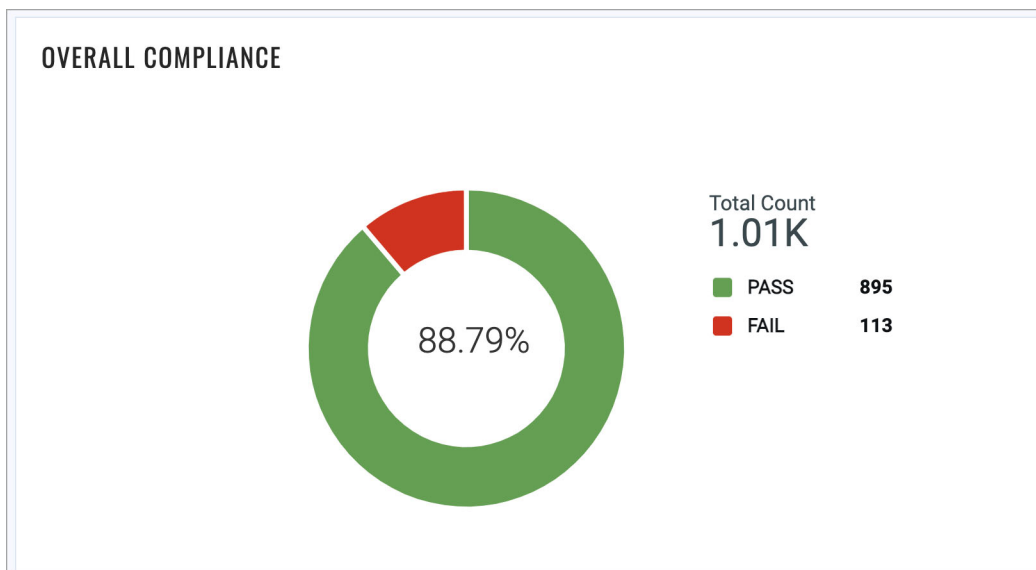
The Qualys OCA supports two dashboards (**Default Dashboard** and **Printers Dashboard**) with non-editable widgets like Overall Compliance, Failure by Criticality, Overall Compliance for Printers, Compliance Data for Printers, etc.

OCA Default Dashboard

The OCA default dashboard includes six non-editable widgets that display asset statistics and compliance posture related to all the assets provisioned through OCA.

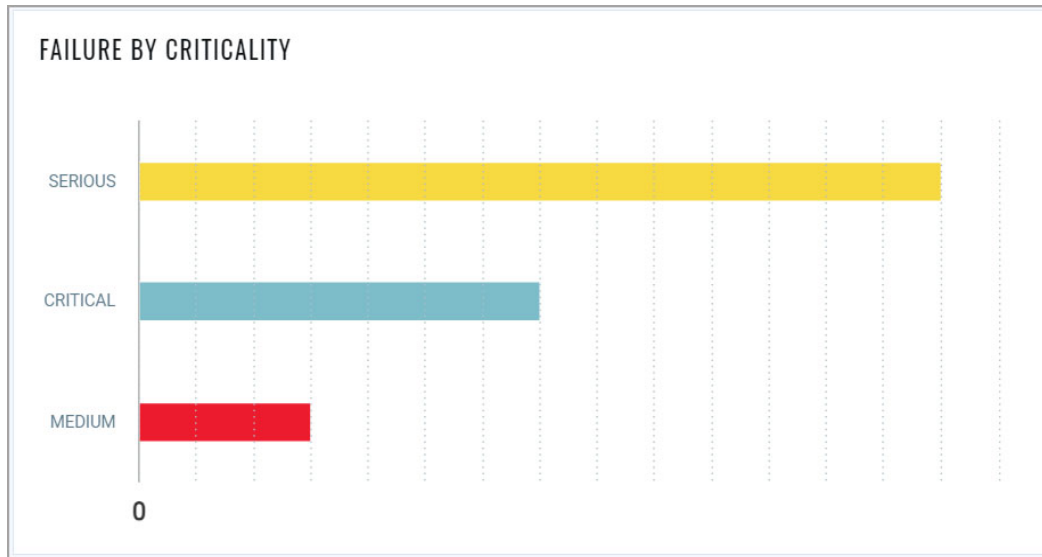
Overall Compliance

This non-editable widget displays the overall compliance data based on passed and failed control count for all the assets including printers.



Failure by Criticality

This non-editable widget uses a statistical graph to display number of failed controls by criticality - MEDIUM, CRITICAL, SERIOUS.



Top Failing Policies

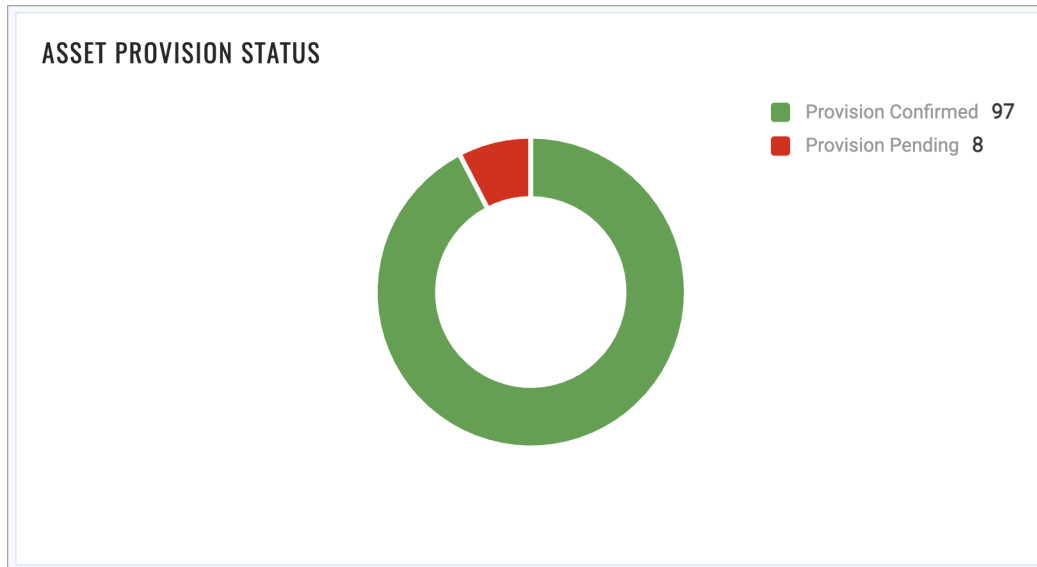
This non-editable widget displays the top failing policies.

TOP FAILING POLICIES

TITLE	LAST EVALUATED	MODIFIED	COMPLIANCE	
Security Configuration and Compliance Policy for ArubaOS 6.x (OCA) v.2.0	Feb 17, 2021	Feb 10, 2021	<div><div></div><div></div></div>	72.41%
OCA policy	Dec 23, 2020	Dec 23, 2020	<div><div></div><div></div></div>	95.45%

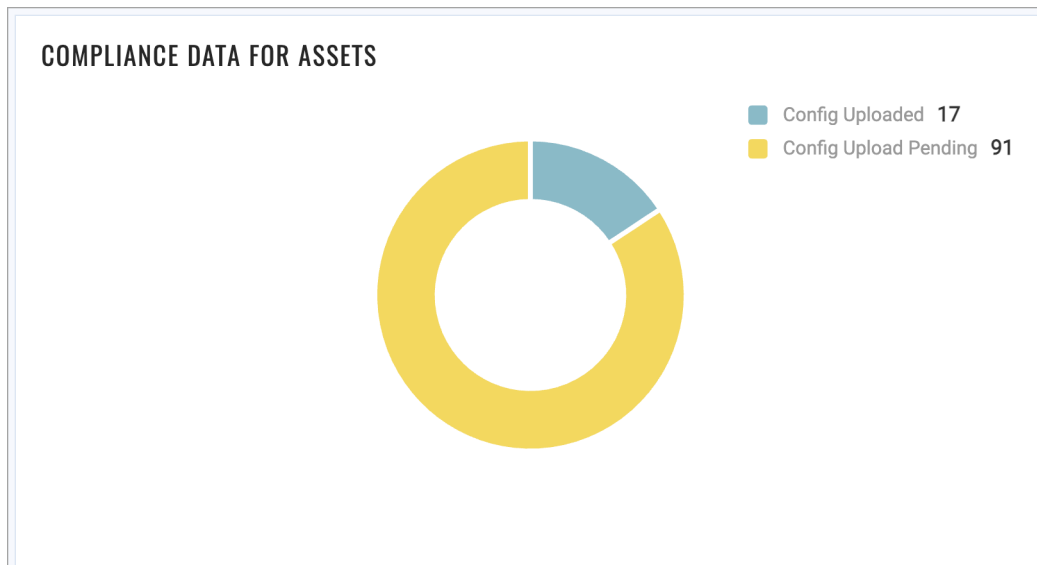
Asset Provision Status

This non-editable widget displays the status of asset provisioning by the status - Provision Confirmed and Provision Pending.



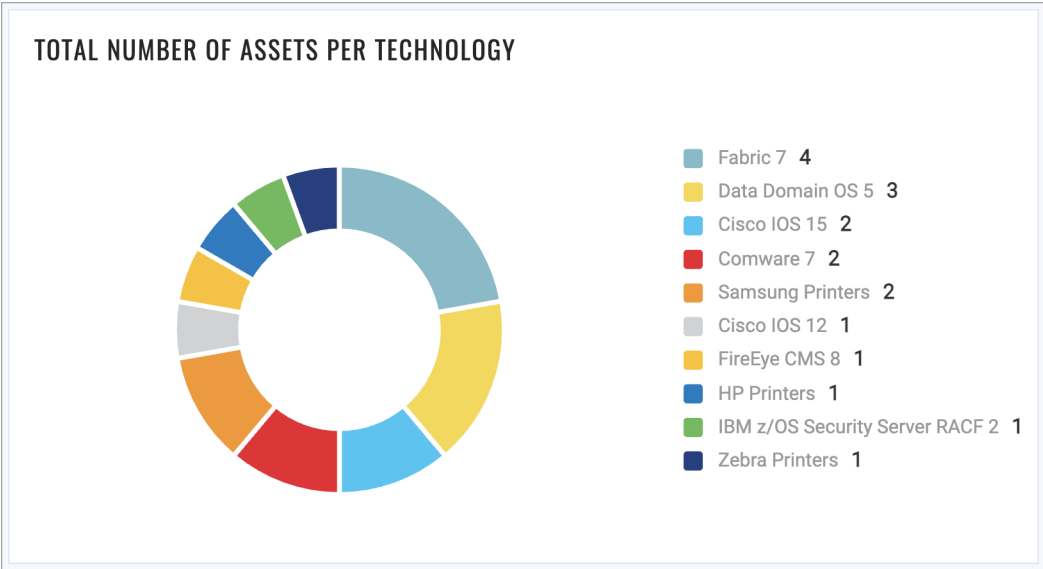
Compliance Data for Assets

This non-editable widget displays if the upload of asset configuration data to Qualys is pending or is completed.



Total number of Assets per technology

This non-editable widget displays the total number of assets per technology.

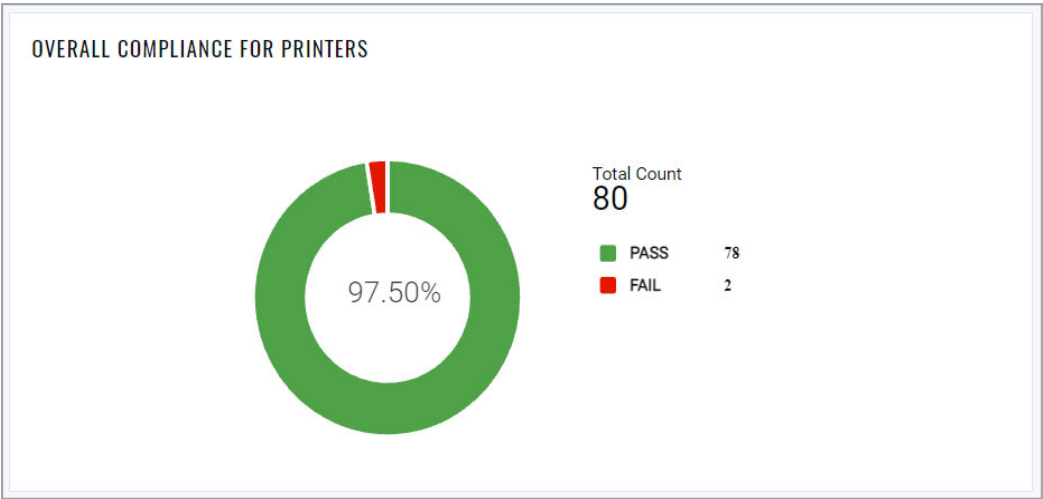


OCA Printers Dashboard

The Printers OCA Dashboard includes four non-editable widgets that display essential asset data, compliance posture of HP, Samsung Printers provisioned via HP's JetAdvantage and HP Security Manager plug in.

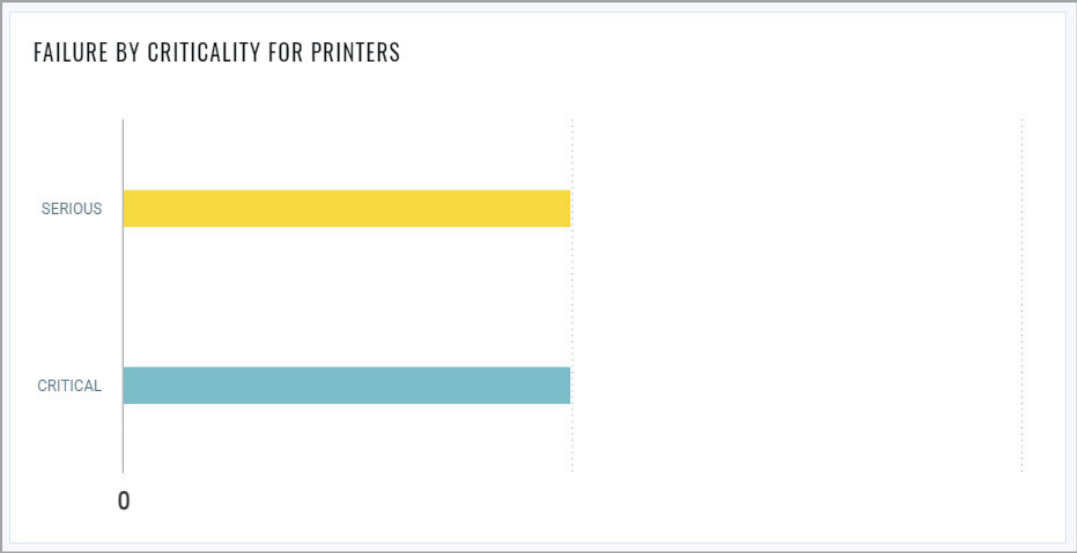
Overall Compliance for Printers

This non-editable widget displays the compliance assessment of printers with respect to number of controls passing and failing.



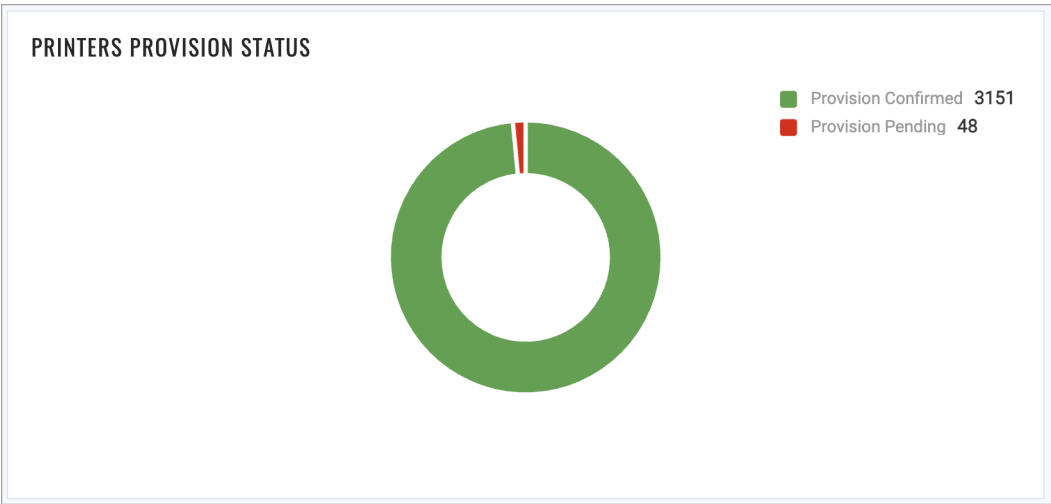
Failure by Criticality for Printers

This non-editable widget uses a statistical graph to display number of failed controls by criticality - MEDIUM, CRITICAL, SERIOUS.



Printers Provision Status

This non-editable widget displays the status of printer assets provisioning - Provision Confirmed or Provision Pending.



Compliance Data for Printers

This non-editable widget displays if the upload of printer configuration data to Qualys is pending or is completed.

