Qualys Patch Management v2.4

API Release Notes

Version 2.4

June 20, 2023 (Updated on August 09, 2023)

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

In some of the API Release Notes, the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) is used in sample API requests.

For this API Release Notes, instead of providing any platform-specific URL, <qualys_base_url> is mentioned in the sample API requests.

If you are on another platform, replace this URL with the appropriate gateway URL for your account.

New API to Get Patch Insights Data

API affected	pm/v1/remediation/insights
Status	New
Operator	POST
DTD or XSD changes	Not applicable

With this release, we have introduced this new API to provide a QID remediation plan. You can fetch the patch insights data based on the "assetid" and "qid" combination that you enter. With this data, you can get details about the patches that can be used to remediate the QIDs you entered.

Input Parameter

By providing a single set or an array of "assetid" and "qid" the following input parameters, you can fetch patch insights data, that enables you to know about the patches that can remediate the QIDs.

Field Name	Mandatory (Y/N)	Data Type	Description
`assetid`	Yes	Integer	Enter the target asset ID.
`qid`	Yes	Integer	Enter the qid that needs to be remediated for the assetid that you entered.

Sample - Get a remediation plan for QIDs and Assets

API Request (JSON format):

```
curl -X 'POST' \ '<qualys_base_url>/pm/v1/remediation/insights' \ -H
'accept: application/json' \ -H 'Authorization: Bearer <<jwt token>>' \ -
H 'Content-Type: application/json' \ -d '[ { "assetId": 28695733, "qid":
241298 } ]'
```

Response:

Example: Response is for Linux "assetid' and 'qid' combination that you entered


```
 [
{
  "qid": 241298,
  "qidTitle": "Red Hat Update for kernel security (RHSA-2023:1470)",
  "assetId": 28695733,
  "assetUUID": "07e884c6-890c-4ce7-b1c7-dbdd0c360569",
```

```
    "assetName": "localhost.localdomain",
    "assetPlatform": "Linux",
    "assetOperatingSystem": "Red Hat Enterprise Linux 9.0",
    "assetLicenseStatus": "Full",
    "statusMessage": "The provided Asset is fully licensed. All patch
information is available.",
    "patches": [
      {
        "qualysPatchId": "4908bae0-1dd8-3757-8c53-e54048b11ce2",
        "patchTitle": "RHSA-2023:1470: kernel security, bug fix, and
enhancement update",
        "category": "Security",
        "vendorSeverity": "Important",
        "bulletin": null,
        "kb": null,
        "advisory": "RHSA-2023:1470",
        "notification": null,
        "associatedQIDs": [
          "241298"
        ],
        "cve": [
          "CVE-2022-4744",
          "CVE-2022-4269",
          "CVE-2023-0266"
        ],
        "downloadUrls": null,
        "packages": [
          "kernel-zfcpdump-modules-extra-5.14.0-
162.22.2.el9_1.noarch.rpm",
          "kernel-tools-libs-devel-5.14.0-162.22.2.el9_1.noarch.rpm",
          "kernel-modules-5.14.0-162.22.2.el9_1.noarch.rpm",
          "python3-perf-5.14.0-162.22.2.el9_1.x86_64.rpm",
          ...
          "kernel-modules-extra-5.14.0-162.22.2.el9_1.noarch.rpm",
          "kernel-debug-modules-extra-5.14.0-162.22.2.el9_1.noarch.rpm"
        ]
      }
    ]
  }
]
```

New API to Generate Patch Insights Report

API affected	pm/v1/report/remediation/insights
Status	New
Operator	POST
DTD or XSD changes	Not Applicable

With this release, we have introduced this new API to generate the patch insights report. The report is generated based on the "assetid" and "qid" combination that you provide. From this report, you can get details about the patches that can remediate the QIDs.

Input Parameter

By providing a single set or an array of "assetid" and "qid" of the following input parameters, you can generate the patch insights report. .

Field Name	Mandatory (Y/N)	Data Type	Description
`assetid`	Yes	Integer	Enter the target asset ID.
`qid`	Yes	Integer	Enter the qid that needs to be remediated for the assetid that you entered.

Sample - Get a remediation plan for QIDs and Assets in report format

API Request (JSON format):

```
curl -X 'POST' \
  '<qualys_base_url>/pm/v1/report/remediation/insights' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer <<jwt token>>' \
  -H 'Content-Type: application/json' \
  -d '[
  {
    "assetId": 28695733,
    "qid": 241298
  }
]'
```

Response:

```
{
  "reportId": "e23a6bbc-8949-451c-ae4e-19fa281deada"
}
```

Download Patch Insights Report

API affected	pm/v1/report/{reportId}/download
Status	Updated
Operator	GET
DTD or XSD changes	Not Applicable

With this release, you can now download patch insights report for the reportId you provide. The response for this API is a link from where you can download the patch insights report. The report is in the CSV format.

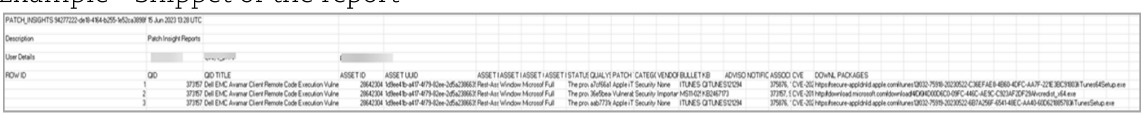
Sample - To download patch insights report

API Request (JSON format):

```
curl -X 'GET' \
  '<qualys_base_url>/pm/v1/report/e23a6bbc-8949-451c-ae4e-
19fa281deada/download' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer <<jwt token>>'
```

The report is downloaded in the CSV format.

Example - Snippet of the report



PATCH_INSIGHTS 94277222-de18-4164-b255-1e52ca3898f	15 Jun 2023 13:28 UTC																				
Description	Patch Insight Reports																				
User Details	[illegible]	[illegible]	[illegible]																		
ROW ID	QID	QID TITLE	ASSET ID	ASSET UUID	ASSET I	ASSET I	ASSET I	ASSET I	STATUS	QUALYS	PATCH	CATEG	VENDOR	BULLET	KB	ADVISO	NOTIFIC	ASSOC	CVE	DOWNL	PACKAGES
1	373157	Dell EMC Avamar Client Remote Code Execution Vulne	28642304	1d9ee41b-a417-4f79-82ee-2d5a238663	Rest-Ass	Window	Microsof	Full	The pro	a7cf66a1	Apple iT	Security	None	ITUNES-	QITUNES121294			375876, '	CVE-202	https://secure-appldnld.apple.com/itunes12/032-75918-20230522-C36EFAE8-4B60-4DFC-AA7F-221E3BC91803/iTunes64Setup.exe	
2	373157	Dell EMC Avamar Client Remote Code Execution Vulne	28642304	1d9ee41b-a417-4f79-82ee-2d5a238663	Rest-Ass	Window	Microsof	Full	The pro	36e5bea	Vulnerat	Security	Importar	MS11-02	KB2467173			373157, 5	CVE-201	http://download.microsoft.com/download/4/D/4/4D00D6C0-09FC-446C-AE9C-C923AF2DF29/vcredist_x64.exe	
3	373157	Dell EMC Avamar Client Remote Code Execution Vulne	28642304	1d9ee41b-a417-4f79-82ee-2d5a238663	Rest-Ass	Window	Microsof	Full	The pro	aab7731	Apple iT	Security	None	ITUNES-	QITUNES121294			375876, '	CVE-202	https://secure-appldnld.apple.com/itunes12/032-75919-20230522-6B7A256F-6541-48EC-AA40-60D621885783/iTunesSetup.exe	

Response Code Change for Create Deployment Job API

API affected	pm/v1/deploymentjob
Status	Updated
Operator	POST
DTD or XSD changes	Not Applicable

With this release, when you create a Windows or Linux deployment job, when the request is successful, you get a 201 response code instead of 200.

Response:

Example: Response for Windows deployment job

```
Response Code: 201
{
  "customerId": "c8f2006c-3f0a-5d94-83c7-2ac1dc78063b",
  "id": "b0d854bb-ebd4-4ad8-b0f2-ffb0f0901ce4",
  "schemaVersion": "1.0",
  "name": "Test Windows Job ",
  "type": "Install",
  "status": "Disabled",
  "assetIds": [
    "6812d21a-7dff-469b-8f97-c24ba00dad80"
  ],
  "assetTagIds": [],
  "matchAllTagIds": [],
  "exclusionTagIds": [],
  "exclusionAssetIds": [],
  "coAuthorUserIds": [],
  "approvedPatches": [
    "75af58d9-2798-37ae-9048-bf5c82f3b6b2"
  ],
  "disabledPatches": null,
  "patchCount": 1,
  "scheduleType": "On-demand",
  "startDateTime": "2023-6-14 04:24:35 AM",
  "recurring": false,
  "recurringWeekDays": "",
  "dayOfMonth": null,
  "recurringDayOfMonth": null,
  "recurringWeekDayOfMonth": null,
  "timezoneType": "SPECIFIC_TZ",
  "timezone": "UTC",
  "timeout": -1,
  "timeoutUnit": "HOURS",
  "preDeployment": {
```

```
    "userMessage": "",
    "description": "",
    "deferment": {
      "count": 3,
      "interval": 1,
      "intervalUnit": "HOURS"
    }
  },
  "duringDeployment": {
    "userMessage": "",
    "description": ""
  },
  "postDeployment": {
    "suppressReboots": false,
    "rebootOption": {
      "userMessage": "",
      "description": "",
      "deferment": {
        "count": 3,
        "interval": 1,
        "intervalUnit": "HOURS"
      }
    },
    "rebootCountdown": {
      "interval": 15,
      "intervalUnit": "MINUTES",
      "userMessage": "Reboot countdown started",
      "description": "The system reboot is initiated. It will reboot
automatically after the timer countdown."
    },
    "onComplete": {
      "userMessage": "",
      "description": ""
    }
  },
  "description": "",
  "createdBy": {
    "user": {
      "id": "30ce0a0f-05b4-db48-8296-b7dd8a6d2943",
      "name": "quays_vy59"
    },
    "date": 1686716671364
  },
  "updatedBy": {
    "user": null,
    "date": null
  },
  "deletedBy": {
    "user": null,
```

```
    "date": null
  },
  "assetCount": null,
  "opportunisticDownloads": null,
  "filterType": "Any",
  "exclusionFilterType": "Any",
  "taggedAssetCount": 0,
  "minimizeWindow": false,
  "dynamicPatchesQQL": "",
  "isDynamicPatchesQQL": false,
  "dynamicQQLType": 1,
  "platform": "Windows",
  "continueOnPatchFailure": false,
  "preDeployActions": null,
  "postDeployActions": null,
  "applicableAssetCount": 0,
  "monthlyRecurringType": null,
  "patchTuesdayPlusXDays": null,
  "recurringLastDayOfMonth": false,
  "jobCategory": 3,
  "jobTriggerStatus": null,
  "completionPercent": null,
  "totalAssetCount": null,
  "assetResultReceivedCount": null,
  "jobSource": 3,
  "readOnly": false,
  "notification": null,
  "linkedJobId": null,
  "linkedToJob": null,
  "linkedJobs": null,
  "jobStartCountdown": null,
  "passwordAction": null
}
```

Changed Response Codes for Invalid or Incorrect Request Values

Before the Patch Management 2.4.0.0 release, if you provided incorrect request values for the APIs, a 500 response code was shown.

With this release, we have changed the response codes of the Patch Management public APIs as per the API standards. It enables you to understand incorrect or invalid request values better. As a result, you can troubleshoot and fix the API requests to get the correct response.

If you provide an incorrect base URL or incorrect query parameters, you get the 404 response code. If you provide invalid input parameters, you get a 400 response code.

Response Code Examples

Negative Page size:

```
{
  "_error": {
    "code": 400,
    "errorCode": "2007",
    "message": "Invalid argument: pageSize"
  }
}
```

Negative sorting:

```
{
  "_error": {
    "code": 400,
    "errorCode": "2504",
    "message": "Sorting cannot be performed without adding the Group By
field."
  }
}
```

Empty Job Id:

```
{
  "_error": {
    "code": 400,
    "errorCode": "3005",
    "message": "Input parameters cannot be null or empty"
  }
}
```

Negative page no:

```
{
  "_error": {
    "code": 400,
    "errorCode": "2007",
    "message": "Invalid argument: pageNumber"
  }
}
```

Limit in a negative value:

```
{
  "_error": {
    "code": 400,
    "errorCode": "<errorCode>",
    "message": "Invalid argument: limit"
  }
```

Invalid patch Id:

```
{
  "_error": {
    "code": 404,
    "errorCode": "3546",
    "message": "Provided patchId not found."
  }
}
```

Invalid deployment job Id:

```
{
  "_error": {
    "code": 404,
    "errorCode": "2006",
    "message": "A deployment job with ID: <Job ID> does not exist in the
database."
  }
}
```

Invalid report id:

```
{
  "_error": {
    "code": 404,
    "errorCode": "2242",
    "message": "The report for reportId:<Report ID> does not exist in the
database"
  }
}
```

Updated API to Fetch Linux Patch Report

API affected	pm/v1/report/patch?platform=Linux
Status	Updated
Operator	GET
DTD or XSD changes	No

With this release, we have updated the patch report API to fetch the reports for the patches on Linux assets.

Sample - To get patch report for Linux assets

API Request (JSON format):

```
curl -X 'GET' \
  '<qualys_base_url>/pm/v1/report/patch?platform=Linux' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer <<jwt token>>'
```

Response:

```
{  "reportId": "a8bd5290-cbb4-4900-b8f3-666a31f417c1"
}
```