



**Bitdefender**<sup>®</sup>

**GravityZone**

**API GUIDE**

## Bitdefender Control Center API Guide

Publication date 2019.05.15

Copyright© 2019 Bitdefender

### Legal Notice

**All rights reserved.** No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

**Warning and Disclaimer.** This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

**Trademarks.** Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.



# Table of Contents

- 1. Getting Started ..... 1
  - 1.1. Introduction ..... 1
  - 1.2. API Requests ..... 1
  - 1.3. API Keys ..... 3
  - 1.4. Authentication ..... 4
  - 1.5. Errors reporting ..... 4
- 2. Reference ..... 7
  - 2.1. Accounts ..... 7
    - 2.1.1. getAccountsList ..... 7
    - 2.1.2. deleteAccount ..... 10
    - 2.1.3. createAccount ..... 11
    - 2.1.4. updateAccount ..... 13
    - 2.1.5. configureNotificationsSettings ..... 16
    - 2.1.6. getNotificationsSettings ..... 19
    - 2.1.7. Objects ..... 21
  - 2.2. Network ..... 26
    - 2.2.1. getContainers ..... 27
    - 2.2.2. getNetworkInventoryItems ..... 29
    - 2.2.3. createScanTask ..... 37
    - 2.2.4. getScanTasksList ..... 39
    - 2.2.5. getEndpointsList ..... 41
    - 2.2.6. getManagedEndpointDetails ..... 47
    - 2.2.7. createCustomGroup ..... 53
    - 2.2.8. deleteCustomGroup ..... 54
    - 2.2.9. moveCustomGroup ..... 55
    - 2.2.10. moveEndpoints ..... 57
    - 2.2.11. deleteEndpoint ..... 58
    - 2.2.12. setEndpointLabel ..... 59
  - 2.3. Packages ..... 61
    - 2.3.1. getPackagesList ..... 61
    - 2.3.2. createPackage ..... 63
    - 2.3.3. deletePackage ..... 69
    - 2.3.4. getPackageDetails ..... 70
  - 2.4. Policies ..... 73
    - 2.4.1. getPoliciesList ..... 74
    - 2.4.2. getPolicyDetails ..... 76
  - 2.5. Reports ..... 77
    - 2.5.1. createReport ..... 78
    - 2.5.2. getReportsList ..... 93
    - 2.5.3. getDownloadLinks ..... 97
    - 2.5.4. deleteReport ..... 100
  - 2.6. Quarantine ..... 101
    - 2.6.1. getQuarantineItemsList ..... 101
    - 2.6.2. createRemoveQuarantineItemTask ..... 106
    - 2.6.3. createEmptyQuarantineTask ..... 107



|  |     |
|--|-----|
| 2.6.4. createRestoreQuarantineItemTask .....         | 109 |
| 2.6.5. createRestoreQuarantineExchangeItemTask ..... | 110 |
| 3. API Usage Examples .....                          | 113 |
| 3.1. C# Example .....                                | 113 |
| 3.2. curl Example .....                              | 114 |
| 3.3. Python Example .....                            | 115 |
| 3.4. Node.js example .....                           | 116 |

# 1. GETTING STARTED

## 1.1. Introduction

Bitdefender Control Center APIs allow developers to automate business workflows. The APIs are exposed using JSON-RPC 2.0 protocol specified here:

<http://www.jsonrpc.org/specification>.

Each API call targets a method and passes a set of parameters.

There are two types of parameters:

- required: MUST be always passed to the called method.
- optional: has a default value and can be omitted from the parameters list. Any optional parameter can be skipped, regardless its position in the parameters list.

## 1.2. API Requests

The API calls are performed as HTTP requests with JSON-RPC messages as payload. HTTP POST method MUST be used for each API call. Also, it is required that each HTTP request have the `Content-Type` header set to `application/json`.



### Note

The API is limited to maximum 10 requests per second per API key. If this limit is exceeded, subsequent requests are rejected and 429 HTTP status code is returned.

Bitdefender Control Center exposes multiple APIs targeting distinct areas in the product. Each API exposes a set of methods related to a designated product area. The base URL for all APIs is the machine hostname, domain or IP where GravityZone is installed : <https://YOUR-HOSTNAME/api/v1.0/jsonrpc/>. To obtain the full URL of the API, add the API name to the base URL.

Currently, the following APIs are being exposed:

1. **Accounts**, with the API URL:

<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/accounts>.

2. **Network**, with the API URL:  
<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network>.
3. **Packages**, with the API URL:  
<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/packages>.
4. **Policies**, with the API URL:  
<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/policies>.
5. **Reports**, with the API URL:  
<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/reports>.
6. **Quarantine**, with the API URL:  
<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/quarantine>.

The HTTP requests containing JSON RPC 2.0 can be performed on each API URL in order to consume the exposed functionality.

**Note**

Batch requests and notifications are not currently supported by Bitdefender Control Center.



### 1.3. API Keys

The API key is a unique key that is generated in **MyAccount** section of Bitdefender Control Center. Each API key allows the application to call methods exposed by one or several APIs. The allowed APIs are selected at the time the API key is generated.

To generate API keys:

1. Log in to <https://YOUR-HOSTNAME/> using your administrative account. Your account must have the following rights: Manage Networks, Manage Users, Manage Company and Manage Reports.
2. Click your username in the upper-right corner of the console and choose **My Account**.
3. Go to the **API keys** section and click the **+ Add** button at the upper side of the table.
4. Select the APIs that you want to use.

API key ✕

---

Enabled APIs:

Packages API  Policies API

Network API

Save
Cancel

5. Click **Save**. An API key will be generated for the selected APIs.

| <span style="float: left;">+ Add</span> <span style="float: right;">- Delete</span> <span style="float: right;">Refresh</span> |   |
|--|---|
| Key  | Created   |
| <input type="checkbox"/> <span style="background-color: #ccc; display: inline-block; width: 150px; height: 1em;"></span>       | Mon Apr 20 2015 07:32:59 GMT+0300 (GTB Daylight Time) |



### Important

By using the API keys, developers can access sensitive information such as packages and inventory. Please do not share or distribute your own generated API keys, in order to prevent the leaking of sensitive information!

## 1.4. Authentication

The API calls to Bitdefender Control Center are authenticated at HTTP protocol level using the HTTP Basic Authentication mechanism described here:

<http://tools.ietf.org/html/rfc2617>.

The client application is required to send the `Authorization` request header each time it performs a call to an API.

The `Authorization` header consists of the following elements:

1. The authorization method and a space as the prefix; in our case, this will always be equal to `Basic`.
2. A Base64 encoded string, generated from the combined `username:password` sequence.

In our case, the API key is set as username, and password is set as an empty string.

For example, if the API Key is equal to

`N8KzwcqVUxAI1RoPi5jyFJpKPlkDl9vF`, the Base64 encoding should be performed on the following string:

`N8KzwcqVUxAI1RoPi5jyFJpKPlkDl9vF:.` In this case, the content sent to the authorization header is

`Basic TjhLendjcVZVeEFJMVJvUGk1anlGS1BrUGxrRGw5dkY6.`

## 1.5. Errors reporting

Bitdefender Control Center returns an error if the requested API method is unable to perform the desired task.

Here is an example of error response for a failing API call:

```
{
```



```
"id": "4d77e2d9-f760-4c8a-ba19-53728f868d98",
"jsonrpc": "2.0",
"error": {
  "code": -32601,
  "message": "Method not found",
  "data": {
    "details": "The selected API is not available."
  }
}
```

The error code and error message are returned as specified in [JSON-RPC 2.0 Specification](#):

| Error            | Code   | Message          |
|------------------|--------|------------------|
| Parse error      | -32700 | Parse error      |
| Invalid Request  | -32600 | Invalid Request  |
| Method not found | -32601 | Method not found |
| Invalid params   | -32602 | Invalid params   |
| Server error     | -32000 | Server error     |

The full description of the error is placed in `data.details` member in the error message.

Also, the HTTP status code is set according to the type of errors:

| HTTP status            | Description   |
|------------------------|---|
| 401 Unauthorized       | is set if the authentication failed for the request (e.g. the API key is incorrect or missing)                                  |
| 403 Forbidden          | is set if the request is not authorized to consume the desired functionality (e.g. the API is not enabled for the used API key) |
| 405 Method Not Allowed | the HTTP method is other than POST  |
| 429 Too Many Requests  | more than 10 requests per second have been issued from the same IP address  |



200 HTTP status code is returned for successful requests or for requests that have failed due to server errors (e.g. a required parameter is not passed).

## 2. REFERENCE

### 2.1. Accounts

The Accounts API includes several methods allowing the management of user accounts:

- `getAccountsList` : lists existing user accounts.
- `deleteAccount` : deletes a user account.
- `createAccount` : creates a user account.
- `updateAccount` : updates a user account.
- `configureNotificationsSettings` : configures the user notification settings.
- `getNotificationsSettings` : returns the notifications settings.

API url: <https://YOUR-HOSTNAME/api/v1.0/jsonrpc/accounts>

#### 2.1.1. getAccountsList

This method lists the user accounts visible to the account which has generated the API key. It will return an empty list if there are no user accounts.



#### Note

When the accounts list is retrieved, the account which generated the API key **will be omitted**.

#### Parameters

| Parameter | Type   | Optional | Description   |
|-----------|--------|----------|---|
| page      | Number | Yes      | The results page number. The default value is 1.  |
| perPage   | Number | Yes      | The number of items displayed in a page. The upper limit is 100 items per page. Default value: 30 items per page. |

## Return value

This method returns an Object containing information regarding the user accounts. The returned object contains:

- `page` - the current page displayed
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `items` - the list of user accounts. Each entry in the list has the following fields:
  - `id`, the ID of the user account.
  - `userName`, the username of the user account.
  - `email`, the email of the user account.
  - `profile`, the profile information of the user account containing: `fullName`, `timezone` and `language`.
  - `role`, the role assigned for the user account. Possible values: 1 - Company Administrator, 2 - Network Administrator, 3 - Reporter, 5 - Custom.
  - `rights`, object containing the rights of the user account with true or false values whether the right is allowed for user or not.
- `total` - the total number of items

## Example

### Request :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "method": "getAccountsList",
  "params": {
    "perPage": 20,
    "page": 1
  }
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    "total": 2,
    "page": 1,
    "perPage": 20,
    "pagesCount": 1,
    "items": [
      {
        "id": "585d3170aaed70b7048b4633",
        "userName": "client",
        "email": "client@bitdefender.com",
        "profile": {
          "fullName": "Bitdefender User",
          "language": "en_US",
          "timezone": "Europe/Bucharest"
        },
        "role": 5,
        "rights": {
          "companyManager": false,
          "manageCompanies": false,
          "manageNetworks": true,
          "manageReports": true,
          "manageUsers": true
        }
      },
      {
        "id": "585d3170aaed70b7048b4633",
        "userName": "client2",
        "email": "client2@bitdefender.com",
        "profile": {
          "fullName": "Bitdefender User",
          "language": "en_US",
          "timezone": "Europe/Bucharest"
        },
        "role": 1,
        "rights": {
          "companyManager": true,
          "manageCompanies": false,
          "manageNetworks": true,
          "manageReports": true,
        }
      }
    ]
  }
}
```

```
        "manageUsers": true
      }
    ]
  }
}
```

## 2.1.2. deleteAccount

This method deletes a user account identified through the account ID.



### Note

The account that was used to create the API key cannot be deleted by using the API.

## Parameters

| Parameter | Type   | Optional | Description                               |
|-----------|--------|----------|---|
| accountId | String | No       | The ID of the user account to be deleted. |

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "method": "deleteAccount",
  "params": {
    "accountId": "585d3810aaed70cc068b45f8"
  }
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": null
}
```

### 2.1.3. createAccount

This method creates a user account with password.

#### Parameters

| Parameter | Type   | Optional | Description  |
|-----------|--------|----------|--|
| email     | String | No       | The email address for the new account.   |
| userName  | String | No       | The username for the account.  |
| profile   | Object | No       | An object containing profile information: <code>fullName</code> , <code>timezone</code> and <code>language</code> . <code>timezone</code> and <code>language</code> are optional.  |
| password  | String | Yes      | Password for the new account. If this value is omitted a password will be created and sent by email to the user. The password should be at least 6 characters in length and must contain at least one digit, one upper case, one lower case and one special character.   |
| role      | Number | Yes      | The role of the new account. Default value is 1 - Company Administrator. These are the available roles: <ul style="list-style-type: none"><li>● 1 - Company Administrator.</li><li>● 2 - Network Administrator.</li><li>● 3 - Reporter.</li><li>● 5 - Custom. For this role, rights must be specified.</li></ul> |

| Parameter | Type   | Optional | Description  |
|-----------|--------|----------|--|
| rights    | Object | Yes      | <p>An object containing the rights of a user account. This object should be set only when <code>role</code> parameter has the value 5 - Custom. When set for other roles, the values will be ignored and replaced with the rights specific to that role. The available rights are:</p> <ul style="list-style-type: none"><li>• <code>manageCompanies</code></li><li>• <code>manageNetworks</code> Setting this to true implies <code>manageReports</code> right to true</li><li>• <code>manageUsers</code></li><li>• <code>manageReports</code></li><li>• <code>companyManager</code></li></ul> <p>Each option has two possible values: true, where the user is granted the right, or false otherwise. Omitted values from the request are automatically set to false.</p> |
| targetIds | Array  | Yes      | A list of IDs representing the targets to be managed by the user account.  |

## Return value

This method returns a String: The ID of the created user account.

## Example

### Request :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "method": "createAccount",
  "params": {
    "email": "client@bitdefender.com",
    "userName": "Client"
    "profile": {
      "fullName": "Bitdefender User",
```



```
        "language": "en_US",
        "timezone": "Europe/Bucharest"
    },
    "password": "P@s4w0rd",
    "role": 5,
    "rights": {
        "manageNetworks": true,
        "manageReports": true,
        "manageUsers": false
    },
    "targetIds": [
        "585d2dc9aaed70820e8b45b4",
        "585d2dd5aaed70b8048b45ca"
    ]
}
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": "585d2dc9aaed70820abc45b4"
}
```

## 2.1.4. updateAccount

This method updates a user account identified through the account ID.

### Parameters

| Parameter | Type   | Optional | Description                               |
|-----------|--------|----------|---|
| accountId | String | No       | The ID of the user account to be updated. |
| email     | String | Yes      | The new email address for the account.    |
| userName  | String | Yes      | The new username for the user account.    |



| Parameter | Type   | Optional | Description  |
|-----------|--------|----------|--|
| password  | String | Yes      | The new password for the user account. The password should at least 6 characters in length and must contain at least one digit, one upper case, one lower case and one special character.  |
| profile   | Object | Yes      | An object containing profile information: <code>fullName</code> , <code>timezone</code> and <code>language</code> .  |
| role      | Number | Yes      | The new role of the user. These are the available roles: <ul style="list-style-type: none"> <li>● 1 - Company Administrator.</li> <li>● 2 - Network Administrator.</li> <li>● 3 - Reporter.</li> <li>● 5 - Custom. For this role, rights must be specified.</li> </ul>   |
| rights    | Object | Yes      | An object containing the rights of a user account. This object should be set only when <code>role</code> parameter has the value 5 - Custom. When set for other roles, the values will be ignored and replaced with the rights specific to that role. The available rights are: <ul style="list-style-type: none"> <li>● <code>manageCompanies</code></li> <li>● <code>manageNetworks</code> Setting this to True implies <code>manageReports</code> right to true</li> <li>● <code>manageUsers</code></li> <li>● <code>manageReports</code></li> <li>● <code>companyManager</code></li> </ul> Each option has two possible values: true, where the user is granted the right, or false otherwise. Omitted values from the request are automatically set to false. |
| targetIds | Array  | Yes      | A list of IDs representing the targets to be managed by the user account.  |

## Return value

This method returns a Boolean: True when the user account has been successfully updated.

## Example

### Request :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "method": "updateAccount",
  "params": {
    "accountId" : "585d3d3faaed70970e8b45ed",
    "email": "client@bitdefender.com",
    "profile": {
      "fullName": "Bitdefender User",
      "language": "en_US",
      "timezone": "Europe/Bucharest"
    },
    "password": "P@s4w0rd",
    "role": 5,
    "rights": {
      "manageNetworks": true,
      "manageReports": true,
      "manageUsers": false
    },
    "companyId": "58541613aaed7090058b4567",
    "targetIds": [
      "585d2dc9aaed70820e8b45b4",
      "585d2dd5aaed70b8048b45ca"
    ]
  }
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
```

```
"result": true
}
```

## 2.1.5. configureNotificationsSettings

This method configures the notification settings for a given user account.

### Parameters

| Parameter         | Type    | Optional | Description   |
|-------------------|---------|----------|---|
| accountId         | String  | Yes      | The ID of the account for which the notification settings are configured. If no value is provided, the settings will be applied to the account which generated the API key.   |
| deleteAfter       | Number  | Yes      | The number of days after which generated notifications will be automatically deleted. Valid values are between 1 and 365. The default value is 30 days.   |
| emailAddresses    | Array   | Yes      | A list of additional email addresses to be used when sending notifications.   |
| includeDeviceName | Boolean | Yes      | This option specifies whether the device name will be included in the notification sent by email, when it is available, or not. The value should be <code>True</code> to include the device name respectively <code>False</code> to not include it. The default value is <code>False</code> . |
| includeDeviceFQDN | Boolean | Yes      | This option specifies whether the FQDN will be included in the notification sent by email, when   |



| Parameter                          | Type  | Optional | Description   |
|------------------------------------|-------|----------|---|
|                                    |       |          | it is available, or not. The value should be <code>True</code> to include the FQDN respectively <code>False</code> to not include it. The default value is <code>False</code> .   |
| <code>notificationsSettings</code> | Array | Yes      | <p>A list of objects containing the notification settings to be configured. Only the specified notifications will be updated. Existing values are preserved for omitted settings. Each object should have the following structure:</p> <ul style="list-style-type: none"> <li>• <code>type</code>, the notification type,</li> <li>• <code>enabled</code>, <code>True</code> if the notification is enabled, <code>False</code> otherwise,</li> <li>• <code>visibilitySettings</code>, an object containing the visibility settings. For more information, refer to <a href="#">Notifications Visibility Options</a>,</li> <li>• <code>configurationSettings</code>, notification specific configurations. This field depends on the notification type. For more information, refer to <a href="#">Relation Between Notification Type and configurationSettings</a>.</li> </ul> |

## Return value

This method returns a Boolean: True if the notifications settings have been successfully configured.

## Example

### Request :

```
{
  "params": {
    "accountId": "55896b87b7894d0f367b23c8",
    "deleteAfter": 17,
    "includeDeviceName": true,
    "includeDeviceFQDN": true,
    "emailAddresses": ["example1@example.com"],
    "notificationsSettings": [
      {
        "type" : 1,
        "enabled" : true,
        "visibilitySettings" : {
          "sendPerEmail" : true,
          "showInConsole" : true,
          "useCustomEmailDistribution": false
        },
        "emails" : ["example2@example.com"],
        "logToServer" : true
      },
      {
        "configurationSettings" : {
          "threshold" : 15,
          "useThreshold" : true
        }
      }
    ]
  },
  "jsonrpc": "2.0",
  "method": "configureNotificationsSettings",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d68"
}
```

### Response :

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d68",
  "jsonrpc": "2.0",
  "result": true
}
```

## 2.1.6. getNotificationsSettings

This method returns the notifications settings.

### Parameters

| Parameter | Type   | Optional | Description   |
|-----------|--------|----------|---|
| accountId | String | Yes      | The ID of the account for which the notifications settings are retrieved. If not provided, the method will retrieve the notifications settings for the account which has generated the API key. |

### Return value

This method returns an Object containing the current notifications settings:

- `deleteAfter` - the number of days after which generated notifications will be automatically deleted
- `includeDeviceName` - a boolean that informs whether the device name will be included in the notification sent by email or not
- `includeDeviceFQDN` - a boolean that informs whether the device FQDN will be included in the notification sent by email or not
- `emailAddresses` - the list of additional email addresses to be used when sending notifications
- `notificationsSettings` - the list containing the settings for all available notifications. Each entry in the list has the following fields:
  - `type`, the notification type,
  - `enabled`, `True` if the notification is enabled, `False` otherwise,

- visibilitySettings, an object containing the configured visibility settings. For more information, refer to [Notifications Visibility Options](#),
- configurationSettings, notification specific configurations. For more information, refer to [Relation Between Notification Type and configurationSettings](#).

## Example

### Request :

```
{
  "params": {
    "accountId": "55896b87b7894d0f367b23c8"
  },
  "jsonrpc": "2.0",
  "method": "getNotificationsSettings",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
}
```

### Response :

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": {
    "deleteAfter": 21,
    "includeDeviceName": true,
    "includeDeviceFQDN": false,
    "emailAddresses": [
      "example1@example.com",
      "example2@example.com"
    ],
    "notificationsSettings": [
      {
        "type" : 1,
        "enabled" : true,
        "visibilitySettings" : {
          "sendPerEmail" : true,
          "showInConsole" : true,
          "useCustomEmailDistribution": false
        }
      }
    ]
  }
}
```





```

        "emails" : [],
        "logToServer" : true
    },
    "configurationSettings" : {
        "threshold" : 5,
        "useThreshold" : true
    }
},
{
    "type" : 3,
    "enabled" : false,
    "visibilitySettings" : {
        "sendPerEmail" : true,
        "showInConsole" : true,
        "useCustomEmailDistribution": false
        "emails" : [],
        "logToServer" : true
    }
},
...
]
}
}

```

## 2.1.7. Objects

### Notifications Visibility Options

You can use the `visibilitySettings` object to configure where notifications are visible. These are the available options:

| Visibility option          | Optional | Value   |
|----------------------------|----------|---|
| <code>showInConsole</code> | Yes      | True to display this notification in Control Center, False otherwise. If no value is specified it will be set to its previous value or False if a previous value was not set. |



| Visibility option          | Optional | Value  |
|----------------------------|----------|--|
| sendPerEmail               | Yes      | <p>True to send this notification by email, False otherwise. If no value is specified it will be set to its previous value or False if a previous value was not set.</p> <p>This option will take effect only if a SMTP server is configured in the <b>Configuration</b> page of Bitdefender Control Center.</p>   |
| useCustomEmailDistribution | Yes      | <p>True to send email notification to a custom emailing list, False otherwise. The notification will be sent by email to the distribution list only.</p> <p>If this option is set to True the sendPerEmail parameter must be specified and set to True.</p> <p>If no value is specified it will be set to its previous value or False if a previous value was not set.</p> |
| emails                     | Yes      | <p>A list of email addresses to receive the notification via email. When set, only these email addresses receive the notification. When useCustomEmailDistribution is set to True, this list must contain at least one valid email address.</p>  |
| logToServer                | No       | <p>boolean, True to send this notification on the configured syslog server, False otherwise. A syslog server must be configured in Control Center to receive this notification on the syslog server.</p>   |



| Visibility option | Optional | Value   |
|-------------------|----------|---|
|                   |          | <p>This option is available only if a Syslog server is configured in the <b>Configuration</b> page of Bitdefender Control Center.</p> <p>If no value is specified it will be set to its previous value or <code>False</code> if a previous value was not set.</p> |

**Note**

- At least one visibility option from `showInConsole`, `sendPerEmail`, `logToServer` (when available) must be set to `True` when enabling the notification.
- The `sendPerEmail`, `useCustomEmailDistribution` and `emails` visibility options are not available for these notification types:
  - 6 - Internet Connection
  - 7 - SMTP Connection
  - 22 - Product Modules Event

## Relation Between Notification Type and configurationSettings

| Notification type    | Available configurationSettings items with their type and possible values  |
|----------------------|--|
| 1 - Malware Outbreak | <ul style="list-style-type: none"> <li>● <code>useThreshold</code>, <code>boolean</code>, <code>True</code> to trigger this notification when the number of infected managed network objects exceeds a custom threshold, <code>False</code> otherwise</li> <li>● <code>threshold</code>, <code>integer</code>, the percentage of managed network objects infected by the same malware. Valid values are between 1 and 100</li> </ul> |
| 2 - License Expires  | The <code>configurationSettings</code> parameter should not be set for this notification.  |



| Notification type                                 | Available configurationSettings items with their type and possible values   |
|---|---|
| 3 - License Usage Limit Has Been Reached          | The configurationSettings parameter should not be set for this notification.  |
| 4 - License Limit Is About To Be Reached          | The configurationSettings parameter should not be set for this notification.  |
| 5 - Update Available                              | <ul style="list-style-type: none"> <li>● showConsoleUpdate, boolean, True to receive the notification for console updates, False otherwise</li> <li>● showPackageUpdate, boolean, True to receive the notification for package updates, False otherwise</li> <li>● showProductUpdate, boolean, True to receive the notification for product updates, False otherwise</li> </ul> |
| 6 - Internet Connection                           | The configurationSettings parameter should not be set for this notification.  |
| 7 - SMTP Connection                               | The configurationSettings parameter should not be set for this notification.  |
| 8 - Database Backup                               | <ul style="list-style-type: none"> <li>● onlyFailedEvents, boolean, True to receive the notification for failed backup events only, False otherwise</li> </ul>  |
| 9 - Exchange License Usage Limit Has Been Reached | The configurationSettings parameter should not be set for this notification.  |
| 10 - Invalid Exchange User Credentials            | The configurationSettings parameter should not be set for this notification.  |
| 11 - Upgrade Status                               | The configurationSettings parameter should not be set for this notification.  |
| 12 - Exchange Malware Detected                    | The configurationSettings parameter should not be set for this notification.  |



| Notification type                 | Available configurationSettings items with their type and possible values   |
|-----------------------------------|---|
| 13 - Authentication Audit         | The configurationSettings parameter should not be set for this notification.  |
| 14 - Certificate Expires          | The configurationSettings parameter should not be set for this notification.  |
| 15 - GravityZone Update           | The configurationSettings parameter should not be set for this notification.  |
| 16 - Antimalware Event            | The configurationSettings parameter should not be set for this notification.  |
| 17 - Antipshising Event           | The configurationSettings parameter should not be set for this notification.  |
| 18 - Firewall Event               | The configurationSettings parameter should not be set for this notification.  |
| 19 - ATC/IDS event                | The configurationSettings parameter should not be set for this notification.  |
| 20 - User Control Event           | The configurationSettings parameter should not be set for this notification.  |
| 21 - Data Protection Event        | The configurationSettings parameter should not be set for this notification.  |
| 22 - Product Modules Event        | The configurationSettings parameter should not be set for this notification.  |
| 23 - Security Server Status Event | <ul style="list-style-type: none"> <li>● notUpdated, boolean, True to receive the notification when the Security Server is outdated, False otherwise</li> <li>● reboot, boolean, True to receive the notification when the Security Server needs a reboot, False otherwise</li> <li>● stopped, boolean, True to receive the notification when the Security Server was powered off, False otherwise</li> </ul> |



| Notification type                             | Available configurationSettings items with their type and possible values  |
|---|--|
| 24 - Product Registration Event               | The configurationSettings parameter should not be set for this notification.   |
| 26 - Task Status                              | <ul style="list-style-type: none"> <li>statusThreshold, integer, the task status which triggers this notification. Set to 2 for any status, 3 for failed tasks</li> </ul>  |
| 27 - Outdated Update Server                   | The configurationSettings parameter should not be set for this notification.   |
| 28 - New Application In Application Inventory | The configurationSettings parameter should not be set for this notification.   |
| 29 - Blocked Application                      | <ul style="list-style-type: none"> <li>fromProductionMode, boolean, True to receive the notification for a blocked processes of an unauthorized application in Production Mode, False otherwise</li> <li>fromTestMode, boolean, True to receive the notification for a blocked processes of an unauthorized application in Test Mode, False otherwise</li> </ul> |
| 30 - Detected Memory Violation                | The configurationSettings parameter should not be set for this notification.   |
| 31 - Mobile Device Users Without EmailAddress | The configurationSettings parameter should not be set for this notification.   |

## 2.2. Network

The Network API allows managing the network structure through the following methods:

- `getContainers` : returns the network containers.
- `getNetworkInventoryItems` : returns network inventory items.
- `createScanTask` : returns true if the task was successfully created.

- `getScanTasksList` : returns the list of scan tasks.
- `getEndpointsList` : returns the list of endpoints.
- `getManagedEndpointDetails` : returns the details about a managed endpoint.
- `createCustomGroup` : creates a new group under an existing one or under **Computers and Groups**.
- `deleteCustomGroup` : deletes a custom group.
- `moveCustomGroup` : moves a custom group under another custom group.
- `moveEndpoints` : moves the specified list of endpoints to a custom group.
- `deleteEndpoint` : deletes a specified endpoint.
- `setEndpointLabel` : sets a label to an endpoint.

API url: <https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/{service}>

{service} is a placeholder that can hold specific values depending on the chosen API method. Please check the method documentation for the allowed services.

### 2.2.1. getContainers

This method returns network containers. It will return an empty list if the `parentId` is not a container or does not contain any other container within it.

#### Services

This method requires you to place the {service} name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"
- `mobile`, for "Mobile Devices"

For example, the request URL for the `mobile` service is:

<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/mobile>

## Parameters

| Parameter | Type   | Optional | Description   |
|-----------|--------|----------|---|
| parentId  | String | Yes      | The ID of the container. If null, the top containers of the specified service type will be returned.  |
| viewType  | Number | Yes      | <p>The ID of the view type for the virtual environment inventory. The view type depends on the virtualization platform. In VMWare integrations, the available options are:</p> <ul style="list-style-type: none"><li>● 1 - Hosts and Clusters view (default)</li><li>● 2 - Virtual Machines view.</li></ul> <p>In Citrix, XenServer integrations, the available options are:</p> <ul style="list-style-type: none"><li>● 3 - Server view (default)</li><li>● 4 - Folder view.</li></ul> |

## Return value

This method returns an Array containing a list of objects that represent the network containers. Each object has the following fields:

- id - the ID of the container
- name - the name of the container

## Example

### Request :

```
{
  "params": {
    "parentId": "559bd17ab1a43d241b7b23c6",
    "viewType": 4
  },
  "jsonrpc": "2.0",
  "method": "getContainers",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
```



```
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": [
    {
      "id" : "5582c385b1a43deb7f7b23c6",
      "name" : "Xen Server"
    }
  ]
}
```

## 2.2.2. getNetworkInventoryItems

This method returns network inventory items.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines
```

### Parameters

| Parameter             | Type   | Optional | Description  |
|-----------------------|--------|----------|--|
| <code>parentId</code> | String | Yes      | The ID of the container for which the network items will be returned. If null, the items within the root custom group of the specified service are returned. |



| Parameter             | Type   | Optional | Description   |
|-----------------------|--------|----------|---|
| <code>filters</code>  | Object | Yes      | The filters to be used when querying the endpoints list. For information regarding the available filters and how to use them, refer to <a href="#">“Available Filters”</a> (p. 30).   |
| <code>viewType</code> | Number | Yes      | The ID of the view type. Each virtualization platform displays the inventory in specific views. In VMWare integrations, the available options are: <ul style="list-style-type: none"> <li>● 1 - Hosts and Clusters view (default)</li> <li>● 2 - Virtual Machines view.</li> </ul> In Citrix XenServer integrations, the available options are: <ul style="list-style-type: none"> <li>● 3 - Server view (default)</li> <li>● 4 - Folder view.</li> </ul> |
| <code>page</code>     | Number | Yes      | The results page number. Default page number is 1.  |
| <code>perPage</code>  | Number | Yes      | Number of items per page to be returned. The upper limit is 100 items per page. Default value: 30 items per page.   |

## Available Filters

You can use the `filters` parameter to query the inventory items by certain properties. Filters are structured in sections and subsections, described hereinafter. The query result is a list of network items that match ALL sections AND subsections, AND ANY selected filter in a subsection.

These are the available filtering options:

| Section           | Subsection | Filtering Options   |
|-------------------|------------|---|
| <code>type</code> |            | <ul style="list-style-type: none"> <li>● <code>groups</code> - a Boolean to filter all custom groups of endpoints. Default value: <code>False</code>.<br/>This filter is available for <code>computers</code> service.</li> </ul> |



| Section | Subsection | Filtering Options   |
|---------|------------|---|
|         |            | <ul style="list-style-type: none"> <li>● <b>computers</b> - a Boolean to filter all computers. <b>Default value:</b> <code>False</code>.<br/>This filter is available for <code>computers</code> service.</li> <li>● <b>virtualMachines</b> - a Boolean to filter all virtual machines. <b>Default value:</b> <code>False</code>.<br/>This filter is available for <code>computers</code> and <code>virtualmachines</code> services.</li> <li>● <b>clusters</b> - a Boolean to filter all Virtualization Clusters. <b>Default value:</b> <code>False</code>.<br/>This filter is available for <code>virtualmachines</code> service.</li> <li>● <b>hosts</b> - a Boolean to filter all Virtualization Hosts. <b>Default value:</b> <code>False</code>.<br/>This filter is available for <code>virtualmachines</code> service.</li> <li>● <b>dataCenters</b> - a Boolean to filter all Datacenters. <b>Default value:</b> <code>False</code>.<br/>This filter is available for <code>virtualmachines</code> service.</li> <li>● <b>vApps</b> - a Boolean to filter all vShield Apps. <b>Default value:</b> <code>False</code>.<br/>This filter is available for <code>virtualmachines</code> service.</li> <li>● <b>resourcePools</b> - a Boolean to filter all Resource Pools. <b>Default value:</b> <code>False</code>.<br/>This filter is available for <code>virtualmachines</code> service.</li> </ul> |



| Section  | Subsection | Filtering Options  |
|----------|------------|--|
|          |            | <ul style="list-style-type: none"> <li>● <b>folders</b> - a Boolean to filter all Virtualization Folders. Default value: <code>False</code>.<br/>This filter is available for <code>virtualmachines</code> service.</li> <li>● <b>pools</b> - a Boolean to filter all Virtualization Pools. Default value: <code>False</code>.<br/>This filter is available for <code>virtualmachines</code> service.</li> </ul>   |
| security | management | <ul style="list-style-type: none"> <li>● <b>managedWithBest</b> - a Boolean to filter all endpoints with the security agent installed on them. Default value: <code>False</code>.<br/>This filter is available for <code>computers</code> and <code>virtualmachines</code> services.</li> <li>● <b>managedExchangeServers</b> - a Boolean to filter all protected Exchange servers. Default value: <code>False</code>.<br/>This filter is available for <code>computers</code> and <code>virtualmachines</code> services.<br/>This filter requires a valid license key that covers the Security for Exchange security service.</li> <li>● <b>managedRelays</b> - a Boolean to filter all endpoints with Relay role. Default value: <code>False</code>.<br/>This filter is available for <code>computers</code> and <code>virtualmachines</code> services.</li> <li>● <b>securityServers</b> - a Boolean to filter all Security Servers. Default value: <code>False</code>.<br/>This filter is available for <code>computers</code> and <code>virtualmachines</code> services.</li> </ul> |



| Section | Subsection | Filtering Options   |
|---------|------------|---|
|         |            | <ul style="list-style-type: none"> <li> <b>managedWithNsx</b> - a Boolean to filter protected endpoints in VMware NSX data centers. Default value: <code>False</code>.<br/>                     This filter is available for <code>virtualmachines</code> service.<br/>                     This filter requires a valid virtualization license key.                 </li> <li> <b>managedWithVShield</b> - a Boolean to filter protected endpoints in VMware vShield environments. Default value: <code>False</code>.<br/>                     This filter is available for <code>virtualmachines</code> service.<br/>                     This filter requires a valid virtualization license key.                 </li> <li> <b>managedWithHvi</b> - a Boolean to filter all endpoints managed by HVI. Default value: <code>False</code>.<br/>                     This filter is available for <code>computers</code> and <code>virtualmachines</code> services.<br/>                     This filter requires a valid HVI license key.                 </li> </ul> |
| depth   |            | <ul style="list-style-type: none"> <li> <b>allItemsRecursively</b> - a Boolean to filter all endpoints recursively within the Network Inventory of a company. Default value: <code>False</code>.                 </li> </ul>  |
| details |            | <ul style="list-style-type: none"> <li> <b>ssid</b> - string, the SSID (Active Directory SID of the endpoint) used to filter the endpoints regardless of their protection status.                 </li> <li> <b>macs</b> - array, the list of MAC addresses used to filter the endpoints regardless of their protection status.                 </li> </ul>   |



**Important**

Some filters require a specific license to be active, otherwise they are ignored, resulting in an inaccurate API response.



## Return value

This method returns an Object containing information about the network items. The returned object contains:

- `page` - the current page
- `pagesCount` - the total number of pages
- `perPage` - the total number of items returned per page
- `total` - the total number of items
- `items` - an array containing the list of items. Each entry in the list has the following fields:
  - `id`, the ID of the network item,
  - `name`, the name of the network item,
  - `parentId`, the ID of the parent container,
  - `type`, the type of network item: 4 - Group, 5 - Computer, 6 - Virtual Machine, 8 - Virtualization Host, 9 - vShield App, 10 - Virtualization Cluster, 11 - Virtualization Datacenter, 12 - Resource Pool, 13 - Virtualization Pool,
  - `details`, more information about the item. This field is available for 5 - Computers and 6 - Virtual Machines. For information regarding the content of the details member please refer to [“The details member” \(p. 34\)](#).

## The details member

Some network inventory items contain a `details` member. This member exposes more information regarding the item. The information depends on the item type.

| Item type                                  | Details  |
|--|--|
| 5 (computer)<br>and<br>6 (virtual machine) | <ul style="list-style-type: none"> <li>● <code>label</code>, the label set to the endpoint</li> <li>● <code>fqdn</code>, the FQDN of the endpoint</li> <li>● <code>groupId</code>, the group ID of the endpoint</li> <li>● <code>isManaged</code>, boolean <code>True</code>, if this endpoint is managed</li> <li>● <code>machineType</code>, the type of the machine: (1 - computer, 2 - virtual machine, 0 - Other)</li> <li>● <code>operatingSystemVersion</code>, the OS version of the endpoint</li> </ul> |

| Item type | Details  |
|-----------|--|
|           | <ul style="list-style-type: none"><li>● <b>ip</b>, the IP address of the endpoint</li><li>● <b>macs</b>, the list of MAC addresses of the endpoint</li><li>● <b>ssid</b>, the Active Directory SID of the endpoint</li><li>● <b>managedWithBest</b>, boolean <code>True</code>, if BEST is installed on this endpoint</li><li>● <b>managedExchangeServer</b>, boolean <code>True</code>, if this endpoint is an Exchange Server</li><li>● <b>managedRelay</b>, boolean <code>True</code>, if this endpoint has Relay role</li><li>● <b>securityServer</b>, boolean <code>True</code>, if this endpoint is a Security Server</li><li>● <b>managedWithNsx</b>, boolean <code>True</code>, if this is an endpoint from a VMware NSX data center</li><li>● <b>managedWithVShield</b>, boolean <code>True</code>, if this is an endpoint from a VMware vShield environment</li><li>● <b>managedWithHvi</b>, boolean <code>True</code>, if this endpoint is managed by HVI</li></ul> |

## Example

### Request :

```
{
  "params": {
    "parentId": "23b19c39b1a43d89367b32ce",
    "page": 2,
    "perPage": 5,
    "filters": {
      "type": {
        "computers": true
      },
      "depth": {
        "allItemsRecursively": true
      }
    }
  },
  "jsonrpc": "2.0",
}
```

```
"method": "getNetworkInventoryItems",
"id": "301f7b05-ec02-481b-9ed6-c07b97de2b7b"
}
```

## Response :

```
{
  "id": "103d7b05-ec02-481b-9ed6-c07b97de2b7a",
  "jsonrpc": "2.0",
  "result": {
    page: 2,
    pageCount: 11,
    perPage: 2,
    total: 22
    items[
      {
        "id" : "21a295eeb1a43d8b497b23b7",
        "name" : "Computer 21",
        "type" : 2,
        "parentId": "21a295eeb1a43d8b497b22b7",
        "details" : {
          "label" : "endpoint 1",
          "fqdn": "endpoint1.local",
          "groupId": "5a5f4d36b1a43d5f097b23bb",
          "isManaged": true,
          "machineType": 2,
          "operatingSystemVersion": "Windows Server",
          "ip": "60.40.10.220",
          "macs": [
            "324935237335"
          ],
          "ssid": "",
        }
      },
      {
        "id" : "21a295eeb1a43d8b497b24b7",
        "name" : "Computer 22",
        "type" : 2,
        "parentId": "21a295eeb1a43d8b497b23b7",
        "details" : {
```



```
    "label" : "endpoint 2",
    "fqdn" : "endpoint2.local",
    "groupId" : "5a5f4d36b1a43d5f097b23bb",
    "isManaged" : true,
    "machineType" : 2,
    "operatingSystemVersion" : "Windows Server",
    "ip" : "60.40.10.220",
    "macs" : [
        "324935237346"
    ],
    "ssid" : "",
  },
}
]
}
}
```

### 2.2.3. createScanTask

This method creates a new scan task.



#### Note

Please note that the managed endpoints from `virtualmachines` service are also displayed in `computers` service under **Custom Group**. To avoid launching duplicate scan tasks we recommend you to use the endpoints from the `computers` service.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines
```

## Parameters

| Parameter | Type   | Optional | Description   |
|-----------|--------|----------|---|
| targetIds | Array  | No       | A list containing the IDs of endpoints or containers to scan.                                   |
| type      | Number | No       | The type of scan. Available options are: 1 - quick scan; 2 - full scan; 3 - memory scan         |
| name      | String | Yes      | The name of the task. If the parameter is not passed, the name will be automatically generated. |

## Return value

This method returns a Boolean: True when the task was successfully created

## Example

### Request :

```
{
  "params": {
    "targetIds": ["559bd17ab1a43d241b7b23c6",
                 "559bd17ab1a43d241b7b23c7"],
    "type": 1,
    "name": "my scan"
  },
  "jsonrpc": "2.0",
  "method": "createScanTask",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": True
}
```

```
}
```

## 2.2.4. getScanTasksList

This method returns the list of scan tasks.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines
```

### Parameters

| Parameter            | Type   | Optional | Description   |
|----------------------|--------|----------|---|
| <code>name</code>    | String | Yes      | The name of the task. Filters the list of tasks by task name.<br><br>Use the asterisk symbol (*) in front of the keyword to search its appearance anywhere in the name. If omitted, only results where the name starts with the keyword will be returned. |
| <code>status</code>  | Number | Yes      | The status of the task. Available options are: 1 - Pending; 2 - In progress; 3 - Finished.  |
| <code>page</code>    | Number | Yes      | The results page number. Default page number is 1.  |
| <code>perPage</code> | Number | Yes      | Number of items per page to be returned. The upper limit is 100 items per page. Default value: 30 items per page.   |

## Return value

This method returns an Object containing information about the tasks. The returned object contains:

- `page` - the results page number
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `total` - the total number of items
- `items` - the list of tasks. Each entry in the list has the following fields:
  - `id`, the ID of the task,
  - `name`, the name of the task,
  - `status`, the status of the task (as defined above),
  - `startDate`, the start date of the task

## Example

### Request :

```
{
  "params": {
    "status": 1,
    "page": 2,
    "perPage": 5
  },
  "jsonrpc": "2.0",
  "method": "getScanTasksList",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    page: 2,
  }
}
```

```
pagesCount: 11,
perPage: 5,
total: 54
items[
  {
    "id" : "21a295eeb1a43d8b497b23b7",
    "name" : "task 1",
    "status": 1,
    "startDate": '2015-08-21T23:48:16'
  },
  {
    "id" : "21a295eeb1a43d8b497b23b8",
    "name" : "task 2",
    "status": 1,
    "startDate": '2015-08-21T10:21:15'
  },
]
}
```

### 2.2.5. getEndpointsList

This method returns the list of the endpoints.

To find the `parentId`, you must do several recursive calls to `getContainers` until the container with the endpoints is reached. The container ID from the response of `getContainers` should be used as `parentId` in this call. The same `viewType` used in `getContainers` should be used in this call.

#### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

`https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines`

## Parameters

| Parameter | Type    | Optional | Description   |
|-----------|---------|----------|---|
| parentId  | String  | Yes      | The ID of the container for which the endpoints list will be returned. If null, the endpoints within the root custom group of the specified service are returned.   |
| isManaged | Boolean | Yes      | The flag to list managed or unmanaged endpoints. By default, the parameter is not set and the method returns all managed and unmanaged endpoints. If set on <code>True</code> , the method returns only managed endpoints.  |
| viewType  | Number  | Yes      | The ID of the view type for the virtual environment inventory. The view type depends on the virtualization platform. In VMWare integrations, the available options are: <ul style="list-style-type: none"><li>● 1 - Hosts and Clusters view (default)</li><li>● 2 - Virtual Machines view.</li></ul> In Citrix, XenServer integrations, the available options are: <ul style="list-style-type: none"><li>● 3 - Server view (default)</li><li>● 4 - Folder view.</li></ul> |
| page      | Number  | Yes      | The results page number. Default page number is 1.  |
| perPage   | Number  | Yes      | The number of items displayed in a page. The upper limit is 100 items per page. Default value: 30 items per page.   |
| filters   | Object  | Yes      | The filters to be used when querying the endpoints list. For information regarding the available filters and how to use them, refer to <a href="#">“Available Filters” (p. 43)</a> .  |

## Available Filters

You can use the `filters` parameter to query the endpoints by certain properties. Filters are structured in sections and subsections, described hereinafter

The query result is a list of endpoints that match ANY selected filter in ALL sections AND subsections.

These are the available filtering options:

| Section  | Subsection | Filtering Options   |
|----------|------------|---|
| security | management | <ul style="list-style-type: none"> <li> <b>managedWithBest</b> - a Boolean to filter all endpoints with the security agent installed on them. Default value: <code>False</code>.<br/>           This filter is available for <code>computers</code> and <code>virtualmachines</code> services.         </li> <li> <b>managedExchangeServers</b> - a Boolean to filter all protected Exchange servers. Default value: <code>False</code>.<br/>           This filter is available for <code>computers</code> and <code>virtualmachines</code> services.<br/>           This filter requires a valid license key that covers the Security for Exchange security service.         </li> <li> <b>managedRelays</b> - a Boolean to filter all endpoints with Relay role. Default value: <code>False</code>.<br/>           This filter is available for <code>computers</code> and <code>virtualmachines</code> services.         </li> <li> <b>securityServers</b> - a Boolean to filter all Security Servers. Default value: <code>False</code>.<br/>           This filter is available for <code>computers</code> and <code>virtualmachines</code> services.         </li> <li> <b>managedWithNsx</b> - a Boolean to filter protected endpoints in VMware NSX data centers. Default value: <code>False</code>.         </li> </ul> |



| Section              | Subsection | Filtering Options  |
|----------------------|------------|--|
|                      |            | <p>This filter is available for <code>virtualmachines</code> service.</p> <p>This filter requires a valid virtualization license key.</p> <ul style="list-style-type: none"> <li>• <code>managedWithVShield</code> - a Boolean to filter protected endpoints in VMware vShield environments. Default value: <code>False</code>.</li> </ul> <p>This filter is available for <code>virtualmachines</code> service.</p> <p>This filter requires a valid virtualization license key.</p> <ul style="list-style-type: none"> <li>• <code>managedWithHvi</code> - a Boolean to filter all endpoints managed by HVI. Default value: <code>False</code>.</li> </ul> <p>This filter is available for <code>computers</code> and <code>virtualmachines</code> services.</p> <p>This filter requires a valid HVI license key.</p> |
| <code>depth</code>   |            | <ul style="list-style-type: none"> <li>• <code>allItemsRecursively</code> - a Boolean to filter all endpoints recursively within the Network Inventory of a company. Default value: <code>False</code>.</li> </ul>   |
| <code>details</code> |            | <ul style="list-style-type: none"> <li>• <code>ssid</code> - string, the SSID (Active Directory SID of the endpoint) used to filter the endpoints regardless of their protection status.</li> <li>• <code>macs</code> - array, the list of MAC addresses used to filter the endpoints regardless of their protection status.</li> </ul>  |



**Important**

Some filters require a specific license to be active, otherwise they are ignored, resulting in an inaccurate API response.

**Return value**

This method returns an Object containing information about the endpoints. The returned object contains:



- `page` - the current page displayed
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `total` - the total number of items
- `items` - the list of endpoints. Each entry in the list has the following fields:
  - `id`, the ID of managed endpoint,
  - `name`, the name of the endpoint,
  - `label`, the label set to this endpoint,
  - `fqdn`, the FQDN of the endpoint,
  - `groupId`, the group ID of the endpoint,
  - `isManaged`, boolean `True`, if this endpoint is managed,
  - `machineType`, the type of the machine: (1 - computer, 2 - virtual machine, 3 - EC2 Instance, 0 - Other),
  - `operatingSystemVersion`, the operating system version of the endpoint,
  - `ip`, the IP address of the endpoint,
  - `macs`, the MAC addresses of the endpoint,
  - `ssid`, the SSID (Active Directory SID) of the endpoint,
  - `managedWithBest`, boolean `True`, if BEST is installed on this endpoint,
  - `managedExchangeServer`, boolean `True`, if this endpoint is an Exchange Server,
  - `managedRelay`, boolean `True`, if this endpoint has Relay role,
  - `securityServer`, boolean `True`, if this endpoint is a Security Server,
  - `managedWithNsx`, boolean `True`, if this is an endpoint from a VMware NSX data center,
  - `managedWithVShield`, boolean `True`, if this is an endpoint from a VMware vShield environment,
  - `managedWithHvi`, boolean `True`, if this endpoint is managed by HVI

## Example

### Request :

```
{
  "params": {
```

```
"parentId": "23b19c39b1a43d89367b32ce",
"page": 2,
"perPage": 5,
"filters": {
  "security": {
    "management": {
      "managedWithBest": true,
      "managedRelays": true
    }
  }
},
"jsonrpc": "2.0",
"method": "getEndpointsList",
"id": "301f7b05-ec02-481b-9ed6-c07b97de2b7b"
}
```

## Response :

```
{
  "id": "103d7b05-ec02-481b-9ed6-c07b97de2b7a",
  "jsonrpc": "2.0",
  "result": {
    page: 2,
    pagesCount: 11,
    perPage: 5,
    total: 54
    items[
      {
        "id" : "21a295eeb1a43d8b497b23b7",
        "name" : "Endpoint 1",
        "label" : "endpoint 1",
        "fqdn": "endpoint1.local",
        "groupId": "5a5f4d36b1a43d5f097b23bb",
        "isManaged": true,
        "machineType": 2,
        "operatingSystemVersion": "Windows Server 2016",
        "ip": "60.40.10.220",
        "macs": [
          "324935237335"
        ]
      }
    ]
  }
}
```

```
    ],
    "ssid": "",
  },
  {
    "id" : "23a295d8b1a43d7c4a7b23c9",
    "name" : "Endpoint 2",
    "machineType": 2,
    "label" : "endpoint 2",
    "fqdn": "endpoint2.local",
    "groupId": "5a4f4d46b1a53d5f197b23aa",
    "isManaged": true,
    "machineType": 2,
    "operatingSystemVersion": "Windows 7",
    "ip": "60.40.10.221",
    "macs": [
      "325935237445"
    ],
    "ssid": "",
  }
]
}
```

## 2.2.6. getManagedEndpointDetails

This method returns detailed information, such as: the identification details for endpoint and security agent, the status of installed protection modules, and scanning reports and logs about a managed endpoint.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines>

## Parameters

| Parameter  | Type   | Optional | Description   |
|------------|--------|----------|---|
| endpointId | String | No       | The ID of the endpoint for which the details will be returned |

## Return value

This method returns an Object containing the details of the specified endpoint:

- `id` - the ID of managed endpoint
- `name` - the name of the endpoint
- `operatingSystem` - the operating system of the endpoint
- `state` - the power state of the machine: 1 - online, 2 - offline, 3 - suspended; 0 - unknown.
- `ip` - the IP of the endpoint
- `lastSeen` - the date of the last synchronization with Control Center
- `machineType` - the type of the machine: 1 - computer, 2 - virtual machine, 0 - Other
- `agent` - an object with the agent information from the endpoint.

Object description:

- `engineVersion`, string, the version of the engine
- `primaryEngine`, the first engine to be used when scanning for malware. It can have one of the following values:
  - 1 - for Central Scanning (Security Server)
  - 2 - for Hybrid Scanning (Light Engines)
  - 3 - for Local Scanning (Full Engines)
  - 0 - Unknown

- `fallbackEngine`, the first engine to be used when scanning for malware. It can have one of the following values:
  - 2 - for Hybrid Scanning (Light Engines)
  - 3 - for Local Scanning (Full Engines)
  - 0 - Unknown
- `lastUpdate`, the time and date of the last signatures update
- `licensed`, integer, the license status: 0 - pending authentication, 1 - active license, 2 - expired license, 6 - there is no license or not applicable
- `productOutdated`, a Boolean specifying whether the agent's version is the latest available or not
- `productUpdateDisabled`, a Boolean specifying if product updates are disabled
- `productVersion`, string, the version of the product
- `signatureOutdated`, a Boolean specifying if the antimalware signatures of the endpoint are outdated
- `signatureUpdateDisabled`, a Boolean specifying if the antimalware signature updates are disabled
- `type`, integer, the type of the endpoint. It can be:
  - 1 - Endpoint Security
  - 2 - Bitdefender Tools
  - 3 - BEST
- `group` - object, the group to which the endpoint belongs. The object contains the following fields:
  - `id`, the id of the group
  - `name`, the name of the group
- `malwareStatus` - an object informing of the status of the endpoint related to malware. The object has the following fields:

- `detection`, a Boolean indicating if malware was detected on the endpoint in the last 24 hours,
- `infected`, a Boolean informing if the antimalware was able to remove the infection or the endpoint is still infected
- `policy` - an Object informing about the active policy on the endpoint. The object contains:
  - `id`, the ID of the active policy,
  - `name`, the name of the policy,
  - `applied`, true if the policy is applied
- `hypervisorMemoryIntrospection` - object, information about hypervisor memory introspection. This object appears only if the endpoint is managed by HVI.

#### Object description:

- `status`, boolean, specifies if hypervisor memory introspection is enabled for the endpoint.
- `activeModules`, object, information about the modules for Hypervisor memory introspection. It contains `userMode`, boolean, indicating whether User Memory introspection is active and `kernelMode`, boolean, indicating whether Kernel Memory introspection is active for the endpoint.
- `securityServer`, object, information about the security server which protects the endpoint. It contains `name`, string, the name of the security server, `ip`, string, the IP of the security server and `Label`, string, the label associated with the server
- `isLicensed`, boolean, specifies if the endpoint is licensed for Hypervisor memory introspection
- `modules` - an Object informing of the installed modules and their statuses. These are the possible fields for the modules: `advancedThreatControl`, `antimalware`, `contentControl`, `deviceControl`, `firewall`, `powerUser`. The fields have Boolean values, `True` - if the module is enabled, or `False` - if the module is disabled.

- `label` - string, the label set to this endpoint
- `managedWithBest` - boolean True, if BEST is installed on this endpoint
- `managedExchangeServer` - boolean True, if this endpoint is an Exchange Server
- `managedRelay` - boolean True, if this endpoint has Relay role
- `securityServer` - boolean True, if this endpoint is a Security Server
- `managedWithNsx` - boolean True, if this is an endpoint from a VMware NSX data center
- `managedWithVShield` - boolean True, if this is an endpoint from a VMware vShield environment
- `managedWithHvi` - boolean True, if this endpoint is managed by HVI

## Example

### Request :

```
{
  "params": {
    "endpointId" : "54a28b41b1a43d89367b23fd"
  },
  "jsonrpc": "2.0",
  "method": "getManagedEndpointDetails",
  "id": "301f7b05-ec02-481b-9ed6-c07b97de2b7b"
}
```

### Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": {
    'id': '54a28b41b1a43d89367b23fd',
    'name': 'WIN-TGQDU499RS4',
    'operatingSystem': 'Windows Server 2008 R2 Datacenter',
    'state': 1,
  }
}
```

```
'ip': '10.10.24.154',
'lastSeen': '2015-06-22T13:46:59',
'machineType': 1,
'agent': {
  'engineVersion': '7.61184',
  'primaryEngine': 1,
  'fallbackEngine': 2,
  'lastUpdate': '2015-06-22T13:40:06',
  'licensed': 1,
  'productOutdated': False,
  'productUpdateDisabled': False,
  'productVersion': '6.2.3.569',
  'signatureOutdated': False,
  'signatureUpdateDisabled': False,
  'type': 3
},
'group': {
  'id': '5575a235d2172c65038b456d',
  'name': 'Custom Groups'
},
'malwareStatus': {
  'detection': False,
  'infected': False
},
'modules': {
  'advancedThreatControl': False,
  'antimalware': True,
  'contentControl': False,
  'deviceControl': False,
  'firewall': False,
  'powerUser': False
},
'hypervisorMemoryIntrospection': {
  'status': 'enabled',
  'activeModules': {
    'userMode': true,
    'kernelMode': false
  },
  'securityServer': {
    'name': 'Security Server',
    'ip': '192.168.0.100',
    'label': 'N/A'
  }
}
```



```
    },
    'isLicensed': true
  },
  'policy': {
    'id': '5121da426803fa2d0e000017',
    'applied': True,
    'name': 'Default policy'
  },
  "label" : "endpoint label"
}
}
```

## 2.2.7. createCustomGroup

This method creates a new custom group.

### Services

This method requires you to place the {service} name in the API URL. The allowed services are:

- computers, for "Computers and Virtual Machines"
- virtualmachines, for "Virtual Machines"

For example, the request URL for the virtual machines service is:

<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines>

### Parameters

| Parameter | Type   | Optional | Description  |
|-----------|--------|----------|--|
| groupName | String | No       | The name for the new group   |
| parentId  | String | Yes      | The ID of the parent group. If parentId is null, the new group is created under <b>Custom Groups</b> . |

### Return value

This method returns a String: the ID of the new created group.

## Example

### Request :

```
{
  "params": {
    "groupName": "myGroup",
    "parentId": "5582c0acb1a43d9f7f7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "createCustomGroup",
  "id": "9600512e-4e89-438a-915d-1340c654ae34"
}
```

### Response :

```
{
  "id": "9600512e-4e89-438a-915d-1340c654ae34",
  "jsonrpc": "2.0",
  "result": "5582c210b1a43d967f7b23c6"
}
```

## 2.2.8. deleteCustomGroup

This method deletes a custom group.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

`https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines`

## Parameters

| Parameter | Type    | Optional | Description  |
|-----------|---------|----------|--|
| groupId   | String  | No       | The ID of the custom group to be deleted   |
| force     | Boolean | Yes      | Force delete when group is not empty. By default, the parameter is set to <code>False</code> . |

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "groupId": "559bd17ab1a43d241b7b23c6",
    "force": true
  },
  "jsonrpc": "2.0",
  "method": "deleteCustomGroup",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.2.9. moveCustomGroup

This method moves a custom group to another custom group.

## Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

`https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines`

## Parameters

| Parameter             | Type   | Optional | Description                            |
|-----------------------|--------|----------|--|
| <code>groupId</code>  | String | No       | The ID of the custom group to be moved |
| <code>parentId</code> | String | No       | The ID of the destination custom group |

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "groupId": "559bd17ab1a43d241b7b23c6",
    "parentId": "559bd17ab1a85d241b7b23c6"
  },
  "jsonrpc": "2.0",
  "method": "moveCustomGroup",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.2.10. moveEndpoints

This method moves a list of endpoints to a custom group.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

`https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines`

### Parameters

| Parameter                | Type   | Optional | Description                     |
|--------------------------|--------|----------|---------------------------------|
| <code>endpointIds</code> | Array  | No       | The list of endpoints IDs       |
| <code>groupId</code>     | String | No       | The ID of the destination group |

### Return value

This method does not return any value.

### Example

#### Request :

```
{
  "params": {
    "endpointIds" : [
```

```
        "559bd152b1a43d291b7b23d8",
        "559bd152b1a43d291b7b2430"
    ],
    "groupId": "559bd17ab1a43d241b7b23c6"
},
"jsonrpc": "2.0",
"method": "moveEndpoints",
"id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.2.11. deleteEndpoint

This method deletes an endpoint.



### Note

Deleting an endpoint under Custom Groups moves it to the Deleted group. For managed endpoints, an Uninstall task is automatically generated. To permanently remove an endpoint, call the method twice using the same ID.

## Services

This method requires you to place the {service} name in the API URL. The allowed services are:

- computers, for "Computers and Virtual Machines"
- virtualmachines, for "Virtual Machines"

For example, the request URL for the virtual machines service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/network/virtualmachines
```

## Parameters

| Parameter  | Type   | Optional | Description            |
|------------|--------|----------|------------------------|
| endpointId | String | No       | The ID of the endpoint |

## Return value

This method does not return any value.

## Example

### Request :

```
{
  "params": {
    "endpointId" : "559bd152b1a43d291b7b23d8"
  },
  "jsonrpc": "2.0",
  "method": "deleteEndpoint",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": null
}
```

## 2.2.12. setEndpointLabel

This method sets a new label to an endpoint.

## Parameters

| Parameter  | Type   | Optional | Description  |
|------------|--------|----------|--|
| endpointId | String | No       | The endpoint ID.   |
| label      | String | No       | A string representing the label. The maximum allowed length is 64 characters. Enter an empty string to reset a previously set label. |

## Return value

This method returns a Boolean: True, when the label was successfully set.

## Example

### Request :

```
{
  "params": {
    "endpointId": "5a30e7730041d70cc09f244b",
    "label": "label with url http://test.com?a=12&b=wow"
  },
  "jsonrpc": "2.0",
  "method": "setEndpointLabel",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": true
}
```



## 2.3. Packages

The Packages API contains the following methods allowing the management of installation packages:

- `getPackagesList` : returns the list of available packages.
- `createPackage` : creates a new package and returns its ID.
- `deletePackage` : deletes a package.
- `getPackageDetails` : retrieves information about a package.

API url: [https://YOUR\\_HOSTNAME/api/v1.0/jsonrpc/packages](https://YOUR_HOSTNAME/api/v1.0/jsonrpc/packages)

### 2.3.1. getPackagesList

Returns the list of available packages.

#### Parameters

| Parameter            | Type   | Optional | Description   |
|----------------------|--------|----------|---|
| <code>page</code>    | Number | Yes      | The results page number. Default page number is 1.  |
| <code>perPage</code> | Number | Yes      | Number of items per page to be returned. The upper limit is 100 items per page. Default value: 30 items per page. |

#### Return value

This method returns an Object containing information about the packages. The returned object contains:

- `page` - the current page displayed
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `total` - the total number of items

- `items` - the list of packages. Each entry in the list has the following fields: `id`, the ID of the package; `name`, the name of the package; `type`, the type of the package. The type can have the following values:
  - 3 Security Server
  - 4 Bitdefender Endpoint Security Tools
  - 5 Sandbox Analyzer
  - 6 Network Sensor appliance for Sandbox Analyzer

## Example

### Request :

```
{
  "params": {
    "page": 1,
    "perPage": 5
  },
  "jsonrpc": "2.0",
  "method": "getPackagesList",
  "id": "696e1024-f94b-496a-9394-bee58b73c51f"
}
```

### Response :

```
{
  "id": "103d7b05-ec02-481b-9ed6-c07b97de2b7a",
  "jsonrpc": "2.0",
  "result": {
    "page": 1,
    "pagesCount": 1,
    "perPage": 5,
    "total": 1,
    "items": [
      {
        "id" : "55b8c1bfb1a43dd71071071b",
        "name" : "Package Test",
        "type": 3
      }
    ]
  }
}
```

```

    }
}

```

### 2.3.2. createPackage

This method creates an installation package.

#### Parameters

| Parameter   | Type   | Optional | Description  |
|-------------|--------|----------|--|
| packageName | String | No       | The name of the package.   |
| description | String | Yes      | The description of the package. If no value is passed, the description will be an empty string.  |
| language    | String | Yes      | The language of the package in the LL_CC format, where LL is the language and CC is the country. The supported languages are: en_US, es_ES, de_DE, fr_FR, ro_RO, pl_PL, pt_BR, it_IT, ru_RU. If not specified, the default value is en_US. |
| modules     | Object | Yes      | An object with the modules to be enabled/disabled. The keys can be: atc, firewall, contentControl, deviceControl, powerUser. The values can be 1 (enabled) or 0 (disabled). If the module is not sent, it will be considered disabled.     |
| scanMode    | Object | Yes      | An object with the scan mode settings.<br>Object description: <ul style="list-style-type: none"> <li>The accepted keys are: type, vms and computers. The type value can be 1 (automatic) or 2 (for custom mode).</li> </ul>                |



| Parameter             | Type   | Optional | Description  |
|-----------------------|--------|----------|--|
|                       |        |          | <ul style="list-style-type: none"> <li>• If <code>type</code> value is 2, then the <code>computers</code> respectively <code>vms</code> keys and values need to be sent, otherwise the default values will be filled by the system. The value for <code>computers</code> or <code>vms</code> is an object with the possible keys: <code>main</code> and <code>fallback</code>.</li> <li>• The values for <code>main</code> can be 1 (for Central Scanning (Security Server)), 2 (for Hybrid Scanning (Light Engines)) or 3 (for Local Scanning (Full Engines)).</li> <li>• The values for <code>fallback</code> can be 2 (for Hybrid Scanning (Light Engines)) or 3 (for Local Scanning (Full Engines)). If the value for <code>main</code> option is 2 or 3, the value of <code>fallback</code> will not be considered.</li> <li>• If this parameter is not sent, the values for automatic mode are saved.</li> </ul> |
| <code>settings</code> | Object | Yes      | <p>An object with other settings of the package. The values can be <code>scanBeforeInstall</code>, <code>uninstallPassword</code>, <code>customInstallationPath</code>, <code>customGroupId</code> and <code>vmsCustomGroupId</code>. The value for <code>scanBeforeInstall</code> can be 1 (enabled) or 0 (disabled). <code>uninstallPassword</code> should be a string and it should meet the complexity requirements: The password must be at least 6 characters in length and it must contain at least one digit, one upper</p>  |



| Parameter                      | Type   | Optional | Description  |
|--------------------------------|--------|----------|--|
|                                |        |          | <p>case, one lower case and one special character; and</p> <p><code>customInstallationPath</code> should be a valid Windows path where the package will be installed (this will work only for Windows operating systems).</p> <p><code>customGroupId</code> should be a string representing the ID of the custom group entity where the new endpoint should be deployed for the Computers and Virtual Machines View. <code>vmsCustomGroupId</code> should be a string representing the ID of the custom group entity where the new endpoint should be deployed for the Virtual Machines View. All values are optional.</p> |
| <code>roles</code>             | Object | Yes      | <p>An object containing the roles to be enabled or disabled:</p> <ul style="list-style-type: none"> <li>• <code>relay</code> with the following possible values: 1 for enabling the Relay role, and 0 to disable it. By default, the Relay role is disabled.</li> <li>• <code>exchange</code> with the following possible values: 1 for enabling the Exchange role, and 0 to disable it. By default, the Exchange role is disabled. This role is available only with a valid Security for Exchange license.</li> </ul>   |
| <code>deploymentOptions</code> | Object | Yes      | <p>An object containing installation options:</p> <ul style="list-style-type: none"> <li>• <code>type</code>, an integer indicating the entity to which the endpoint will connect to. This entity will deliver the installation kit and updates. Possible values are:</li> </ul>   |



| Parameter | Type | Optional | Description  |
|-----------|------|----------|--|
|           |      |          | <p>1 for regular deploy from the Bitdefender Update Server; 2 for deployments through a Relay.</p> <ul style="list-style-type: none"> <li>● <code>relayId</code>, a string representing the ID of an endpoint with the Relay role enabled. This field must be set when the <code>type</code> option is set to 2, meaning deploying using a Relay.</li> <li>● <code>useCustomCommunicationServer</code>, a boolean allowing you to choose if the endpoint will communicate with a specific Communication Server. Possible values are: <code>True</code> to specify a specific Communication Server, <code>False</code> to use the default Communication Server. This option may be set when the <code>deploy</code> option is 1, meaning regular deploy.</li> <li>● <code>communicationServer</code>, a string containing the IP or hostname of the custom Communication Server. This option must be set only when <code>useCustomCommunicationServer</code> is set to <code>True</code>.</li> <li>● <code>useCommunicationProxy</code>, a boolean allowing you to specify if the endpoint will use a proxy to communicate over the Internet. Possible values are: <code>True</code> to use a communication proxy, <code>False</code> otherwise.</li> <li>● <code>proxyServer</code>, a string representing the IP or domain name of the proxy server. Valid values are IP addresses</li> </ul> |



| Parameter | Type | Optional | Description   |
|-----------|------|----------|---|
|           |      |          | <p>in IPV4 or IPV6 format and domain names as defined under RFC 1035. This option is required when <code>useCommunicationProxy</code> is set to <code>True</code>.</p> <ul style="list-style-type: none"> <li>• <code>proxyPort</code>, an integer representing the port which allows access to the proxy server. Valid values are between 1 and 65535. This option is required when <code>useCommunicationProxy</code> is set to <code>True</code>.</li> <li>• <code>proxyUsername</code>, a string representing the username required for authentication with the proxy server. This option may be omitted if the proxy server does not require authentication.</li> <li>• <code>proxyPassword</code>, a string representing the password required for authentication on the proxy server. This option may be omitted if the proxy server does not require authentication.</li> </ul> |

### Return value

This method returns an Array containing an object with the ID of the created package and the status of the call, if successful.

### Example

**Request :**

```
{
  "params": {
```

```
"packageName": "a unique name",
"companyId": "54a1a1d3b1a43d2b347b23c1",
"description": "package description",
"language": "en_EN",
"modules": {
  "atc": 1,
  "firewall": 0,
  "contentControl": 1,
  "deviceControl": 0,
  "powerUser": 0
},
"scanMode": {
  "type": 2,
  "computers": {"main": 1, "fallback": 2},
  "vms": {"main": 2}
},
"settings": {
  "uninstallPassword": "mys3cre3tP@assword",
  "scanBeforeInstall": 0,
  "customInstallationPath": "c:\\mypath\\bitdefender",
  "customGroupId": "5a4dff50b1a43ded0a7b23c8",
  "vmsCustomGroupId": "5a4dff50b1a43ded0a7b23c7"
},
"roles": {
  "relay": 0,
  "exchange": 1
},
"deploymentOptions": {
  "type": 2,
  "relayId": "54a1a1s3b1a43e2b347s23c1",
  "useCommunicationProxy": true,
  "proxyServer": "10.12.13.14",
  "proxyPort": 123
}
},
"jsonrpc": "2.0",
"method": "createPackage",
"id": "426db9bb-e92a-4824-a21b-bba6b62d0a18"
}
```

**Response :**



```
{
  "id": "426db9bb-e92a-4824-a21b-bba6b62d0a18",
  "jsonrpc": "2.0",
  "result": [
    {
      u'records': ['551bb0aed5172cac5c8b4568'],
      u'success': True
    }
  ]
}
```

### 2.3.3. deletePackage

This method deletes a package identified through the provided package ID.

#### Parameters

| Parameter | Type   | Optional | Description                          |
|-----------|--------|----------|--------------------------------------|
| packageId | String | No       | The ID of the package to be deleted. |

#### Return value

This method does not return any value.

#### Example

##### Request :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "method": "deletePackage",
  "params": {
    "packageId": "5a37b660b1a43d99117b23c6"
  }
}
```

##### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": null
}
```

### 2.3.4. `getPackageDetails`

This method retrieves information about the configuration of a specific package identified through the provided ID.

#### Parameters

| Parameter              | Type   | Optional | Description  |
|------------------------|--------|----------|--|
| <code>packageId</code> | String | No       | The ID of the package for which details should be retrieved. |

#### Return value

This method returns an Object containing information about the packages. The response object contains:

- `packageName` - the name of the package.
- `description` - the description of the package.
- `language` - the language of the package in the LL\_CC format, where LL and CC are landugage and country international codes.
- `modules` - indicating the status of the modules present in the package. The object may contain the following members: `atc`, `firewall`, `contentControl`, `deviceControl`, `powerUser`. The values for each module are 1 (enabled) or 0 (disabled).
- `scanMode` - an object describing the scan mode settings and containing the following fields:
  - `type`, with the following values 1 (automatic) or 2 (for custom mode)
  - `computers`, an object with the possible fields: `main` for the main scanning engine and `fallback` for the fallback scanning engine. The values of these

fields can be 1 - Central Scanning with Security Server, 2 - Hybrid Scanning (Light Engines) or 3 - Local Scanning (Full Engines)

- `vms`, an object with the possible fields: `main` for the main scanning engine and `fallback` for the fallback scanning engine. The values of these fields can be 1 - Central Scanning with Security Server, 2 - Hybrid Scanning (Light Engines) or 3 - Local Scanning (Full Engines)
- `settings` - an object with other settings of the package containing the following fields: `scanBeforeInstall`, `customInstallationPath`, `customGroupId` and `vmsCustomGroupId`.
- `roles` - an object containing the enabled/disabled roles:
  - `relay` with the following possible values: 1 if enabled and 0 if disabled.
  - `exchange` with the following possible values: 1 if enabled, and 0 if disabled.
- `deploymentOptions` - an object containing installation options:
  - `type`, an integer indicating the entity to which the endpoint will connect to. This entity will deliver the installation kit and updates. Possible values are: 1 for regular deploy from the Bitdefender Update Server; 2 for deployments through a Relay.
  - `relayId`, a string representing the ID of an endpoint with the Relay role enabled. This field is returned if `type` option is set to 2, meaning deploying using a Relay.
  - `useCustomCommunicationServer`, a boolean specifying whether the endpoint communicates with a specific Communication Server.
  - `communicationServer`, a string containing the IP or hostname of the custom Communication Server. This option is returned only when `useCustomCommunicationServer` is set to `True`.
  - `useCommunicationProxy`, a boolean specifying whether the endpoint uses a proxy to communicate over the Internet. Possible values are: `True` to use a communication proxy, `False` otherwise.
  - `proxyServer`, a string representing the IP or domain name of the proxy server. Valid values are IP addresses in IPV4 or IPV6 format and domain names as defined under RFC 1035. This option is present when `useCommunicationProxy` is set to `True`.

- `proxyPort`, an integer representing the port which allows access to the proxy server. Valid values are between 1 and 65535. This option is present when `useCommunicationProxy` is set to `True`.
- `proxyUsername`, a string representing the username required for authentication with the proxy server. This option may be omitted if the proxy server does not require authentication.

## Example

### Request :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "method": "getPackageDetails",
  "params": {
    "packageId": "5a37b660b1a43d99117b23c6"
  }
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    "packageName": "Package",
    "description": "package description",
    "language": "en_US",
    "modules": {
      "antimalware": 1,
      "avc": 1,
      "firewall": 0,
      "contentControl": 1,
      "deviceControl": 0,
      "powerUser": 0,
      "applicationControl": 0
    },
    "roles": {
```

```
        "relay":1,
        "exchange":0
    },
    "scanMode":{
        "type":2,
        "computers":{
            "main":1,
            "fallback":2
        },
        "vms":{
            "main":2
        }
    },
    "settings":{
        "scanBeforeInstall":false,
        "customInstallationPath":"c:\\mypath\\bitdefender",
        "customGroupId" : "5a4dff50b1a43ded0a7b23c8",
        "vmsCustomGroupId" : "5a4dff50b1a43ded0a7b23c7"
    },
    "deploymentOptions":{
        "type":1,
        "useCommunicationProxy":true,
        "proxyServer":"10.12.13.14",
        "proxyPort":123,
        "proxyUsername":"user",
        "useCustomCommunicationServer":true,
        "communicationServer":"10.12.13.14"
    }
}
}
```

## 2.4. Policies

The Policies API includes several methods allowing the management of security policies:

- [getPoliciesList](#) : retrieves the list of available policies.
- [getPolicyDetails](#) : retrieves the settings of a security policy.

API url: [https://YOUR\\_HOSTNAME/api/v1.0/jsonrpc/policies/{service}](https://YOUR_HOSTNAME/api/v1.0/jsonrpc/policies/{service})

`{service}` is a placeholder that can hold specific values depending on the chosen API method. Please check the method documentation for the allowed services.



### Note

Please note that a security policy can be applied on both computers and virtual machines. Therefore, the methods exposed using this API require only the `computers` service.

## 2.4.1. getPoliciesList

This method retrieves the list of available policies.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"

For example, the request URL for the `computers` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/policies/computers
```

### Parameters

| Parameter            | Type   | Optional | Description  |
|----------------------|--------|----------|--|
| <code>page</code>    | Number | Yes      | The results page. The default value is 1.                                  |
| <code>perPage</code> | Number | Yes      | How many items per page should be returned. The default value is 30 items. |

### Return value

This method returns an Object containing a list of policy objects. The result has the following structure:

- `page` - int, the current displayed page
- `pagesCount` - int, the total number of available pages
- `perPage` - int, the total number of returned items per page
- `total` - int, the total number of items

- `items` - array, the list of policies. Each entry in the list has the following fields:  
`id`, string, the ID of the policy, `name`, string, the name of the policy

## Example

### Request :

```
{
  "params": {
    "page": 1,
    "perPage": 2
  },
  "jsonrpc": "2.0",
  "method": "getPoliciesList",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
}
```

### Response :

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": {
    page: 1,
    pageCount: 2,
    perPage: 2,
    total: 4
    items[
      {
        "id" : "21a295eeb1a43d8b497b23b7",
        "name" : "Policy 1"
      },
      {
        "id" : "23a295d8b1a43d7c4a7b23c9",
        "name" : "Policy 2"
      }
    ]
  }
}
```

## 2.4.2. getPolicyDetails

This method retrieves all the information related to a security policy.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"

For example, the request URL for the `computers` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/policies/computers
```

### Parameters

| Parameter             | Type   | Optional | Description                         |
|-----------------------|--------|----------|-------------------------------------|
| <code>policyId</code> | String | No       | The ID of the policy to be queried. |

### Return value

This method returns an Object containing the details of the queried policy:

- `id` - the ID of the queried policy
- `name` - the name of the queried policy
- `createdBy` - the username of the user who created the policy
- `createDate` - the date when the policy was created
- `lastModifyDate` - the date when the policy was last modified
- `settings` - the settings of the policy

### Example

#### Request :

```
{
  "params": {
    "policyId" : "55828d66b1a43de92c712345"
  }
}
```



```
},
"jsonrpc": "2.0",
"method": "getPolicyDetails",
"id": "98409cc1-93cc-415a-9f77-1d4f681000b3"
}
```

### Response :

```
{
  "id": "47519d2d-92e0-4a1f-b06d-aa458e80f610",
  "jsonrpc": "2.0",
  "result": {
    "id": "5583c480b1a43ddc09712345",
    "name": "Test",
    "createdBy": "user@bitdefender.com",
    "createDate": "2015-06-19T10:27:59",
    "lastModifyDate": "2015-06-19T10:27:59",
    "settings": {
      ...
    }
  }
}
```

## 2.5. Reports

The Reports API includes several methods allowing the reports management:

- `createReport` : creates a new instant or scheduled report and returns the ID of the newly-created report.
- `getReportsList` : returns the list of reports.
- `getDownloadLinks` : returns the download links for a report.
- `deleteReport` : deletes the specified report and returns true on success or an error status code and error message on fail.

API url: <https://YOUR-HOSTNAME/api/v1.0/jsonrpc/reports>

## 2.5.1. createReport

This method creates a new instant or scheduled report, based on the parameters received, and returns the ID of the new created report.

The instant report is created and runs one-time-only at the API call.

The scheduled report is created at a later time and runs periodically, based on a predefined schedule.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/reports/virtualmachines
```

### Parameters

| Parameter         | Type   | Optional | Description   |
|-------------------|--------|----------|---|
| <code>name</code> | String | No       | The name of the report.   |
| <code>type</code> | Number | No       | The type of report. The acceptable values are: <ul style="list-style-type: none"><li>● 1 - Antiphishing Activity</li><li>● 2 - Blocked Applications</li><li>● 3 - Blocked Websites</li><li>● 5 - Data Protection</li><li>● 6 - Device Control Activity</li><li>● 7 - Endpoint Modules Status</li><li>● 8 - Endpoint Protection Status</li><li>● 9 - Firewall Activity</li><li>● 11 - Malware Activity</li></ul> |



| Parameter     | Type   | Optional | Description   |
|---------------|--------|----------|---|
|               |        |          | <ul style="list-style-type: none"> <li>● 12 - Malware Status</li> <li>● 14 - Network Status</li> <li>● 15 - On demand scanning</li> <li>● 16 - Policy Compliance</li> <li>● 17 - Security Audit</li> <li>● 18 - Security Server Status</li> <li>● 19 - Top 10 Detected Malware</li> <li>● 21 - Top 10 Infected Endpoints</li> <li>● 22 - Update Status</li> <li>● 25 - Virtual Machine Network Status</li> <li>● 26 - HVI Activity</li> </ul> |
| targetIds     | Array  | No       | A list with the IDs of the targets for which to create the report. The target ID can be any of the following: groups, containers or endpoints.  |
| scheduledInfo | Object | Yes      | The object that defines the schedule to run the report. If the parameter is omitted, an instant report is generated. For more information, please check the details of the <a href="#">scheduledInfo</a> object.  |
| options       | Object | Yes      | <p>The object that defines the options for creating the report. For these reports, the <code>options</code> object should not be set:</p> <ul style="list-style-type: none"> <li>● Endpoint Modules Status</li> <li>● Policy Compliance</li> <li>● Security Server Status</li> </ul> <p>For more information, please check the details of the <a href="#">options</a> object.</p>   |

| Parameter               | Type  | Optional | Description  |
|-------------------------|-------|----------|--|
| <code>emailsList</code> | Array | Yes      | A list of emails where to deliver the report. <code>emailsList</code> should not be set for an instant report. |

## Objects

### `scheduledInfo`

This object is used by the `createReport` call and it defines the schedule based on which the report will run.

The object contains a variable number of members, depending on the occurrence of the report:

| Name                    | Type    | Description  |
|-------------------------|---------|--|
| <code>occurrence</code> | integer | The member is mandatory.<br>Possible values: <ul style="list-style-type: none"><li>– 1 - for an instant report</li><li>– 2 - for hourly report</li><li>– 3 - for daily report</li><li>– 4 - for weekly report</li><li>– 5 - for monthly report</li><li>– 6 - for yearly report</li></ul> |
| <code>interval</code>   | integer | The member should be set only if <code>occurrence</code> has the value 2.<br>Possible values: <ul style="list-style-type: none"><li>– Any integer between 1 and 24, representing the interval (in hours) at which the report will run.</li></ul>   |
| <code>startHour</code>  | integer | The member should be set only if <code>occurrence</code> has the value 3, 4 or 5.<br>Possible values:  |

| Name        | Type    | Description  |
|-------------|---------|--|
|             |         | – Any integer between 0 and 23.  |
| startMinute | integer | The member should be set only if <code>occurrence</code> has the value 3, 4 or 5.<br>Possible values:<br>– Any integer between 0 and 59.   |
| days        | array   | The member should be set only if <code>occurrence</code> has the value 4.<br>Possible values of the array elements:<br>– Integers between 0 and 6, representing the days of the week, from 0 - Sunday to 6 - Saturday. |
| day         | integer | The member should be set only if <code>occurrence</code> has the value 5 or 6.<br>Possible values:<br>– An integer between 1 and 31, representing the day of the month.  |
| month       | integer | The member should be set only if <code>occurrence</code> has the value 6.<br>Possible values:<br>– An integer between 1 and 12, representing the month of the year.  |

### options

This object is used by the `createReport` call and contains a variable number of members, depending on the report type:

- **Antiphishing Activity**

The object must contain these members:



| Name              | Type    | Description   |
|-------------------|---------|---|
| reportingInterval | integer | The member is mandatory.<br>This value depends on the report occurrence.<br>For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |
| filterType        | integer | The member is mandatory.<br>Possible values:<br><ul style="list-style-type: none"> <li>- 0 - All endpoints</li> <li>- 1 - Only endpoints with blocked websites</li> </ul>     |

● **Blocked Applications**

The object must contain these members:

| Name              | Type    | Description   |
|-------------------|---------|---|
| reportingInterval | integer | The member is mandatory.<br>This value depends on the report occurrence.<br>For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |

● **Blocked Websites**

The object must contain these members:

| Name              | Type    | Description   |
|-------------------|---------|---|
| reportingInterval | integer | The member is mandatory.<br>This value depends on the report occurrence.<br>For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |
| filterType        | integer | The member is mandatory.<br>Possible values:<br><ul style="list-style-type: none"> <li>- 0 - All endpoints</li> <li>- 1 - Only endpoints with blocked websites</li> </ul>     |



- Data Protection**

The object must contain these members:

| Name              | Type    | Description  |
|-------------------|---------|--|
| reportingInterval | integer | The member is mandatory.<br>This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a>       |
| filterType        | integer | The member is mandatory.<br>Possible values:<br><ul style="list-style-type: none"> <li>- 0 - All endpoints</li> <li>- 1 - Only managed computers with blocked threats</li> </ul> |
| blockedEmails     | boolean | The member should be set only if filterType has the value 1.<br>Possible values:<br><ul style="list-style-type: none"> <li>- True</li> <li>- False</li> </ul>                    |
| blockedWebsites   | boolean | The member should be set only if filterType has the value 1.<br>Possible values:<br><ul style="list-style-type: none"> <li>- True</li> <li>- False</li> </ul>                    |

- Device Control Activity**

The object must contain these members:

| Name              | Type    | Description              |
|-------------------|---------|--------------------------|
| reportingInterval | integer | The member is mandatory. |



| Name | Type | Description  |
|------|------|--|
|      |      | This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |

● **Endpoint Protection Status**

The object must contain these members:

| Name                      | Type    | Description  |
|---------------------------|---------|--|
| <code>filterType</code>   | integer | The member is mandatory.<br>Possible values:<br><ul style="list-style-type: none"> <li>– 0 - All endpoints</li> <li>– 1 - Only endpoints filtered by the members described hereinafter.</li> </ul>   |
| <code>antivirusOn</code>  | boolean | The member should be set only if <code>filterType</code> has the value 1.<br>Possible values:<br><ul style="list-style-type: none"> <li>– <code>True</code>, to include in the report endpoints with antimalware protection enabled.</li> <li>– <code>False</code>, to exclude from the report endpoints with antimalware protection enabled.</li> </ul>   |
| <code>antivirusOff</code> | boolean | The member should be set only if <code>filterType</code> has the value 1.<br>Possible values:<br><ul style="list-style-type: none"> <li>– <code>True</code>, to include in the report endpoints with antimalware protection disabled.</li> <li>– <code>False</code>, to exclude from the report endpoints with antimalware protection disabled.</li> </ul> |
| <code>updated</code>      | boolean | The member should be set only if <code>filterType</code> has the value 1.  |



| Name                  | Type                 | Description   |
|-----------------------|----------------------|---|
|                       |                      | <p>Possible values:</p> <ul style="list-style-type: none"><li>- <code>True</code>, to include in the report updated endpoints.</li><li>- <code>False</code>, to exclude from the report updated endpoints.</li></ul>  |
| <code>disabled</code> | <code>boolean</code> | <p>The member should be set only if <code>filterType</code> has the value 1.</p> <p>Possible values:</p> <ul style="list-style-type: none"><li>- <code>True</code>, to include in the report endpoints with update disabled.</li><li>- <code>False</code>, to exclude from the report endpoints with update disabled.</li></ul> |
| <code>outdated</code> | <code>boolean</code> | <p>The member should be set only if <code>filterType</code> has the value 1.</p> <p>Possible values:</p> <ul style="list-style-type: none"><li>- <code>True</code>, to include in the report outdated endpoints.</li><li>- <code>False</code>, to exclude from the report outdated endpoints.</li></ul>                         |
| <code>online</code>   | <code>boolean</code> | <p>The member should be set only if <code>filterType</code> has the value 1.</p> <p>Possible values:</p> <ul style="list-style-type: none"><li>- <code>True</code>, to include in the report online endpoints.</li><li>- <code>False</code>, to exclude from the report online endpoints.</li></ul>                             |
| <code>offline</code>  | <code>boolean</code> | <p>The member should be set only if <code>filterType</code> has the value 1.</p> <p>Possible values:</p> <ul style="list-style-type: none"><li>- <code>True</code>, to include in the report offline endpoints.</li></ul>   |



| Name | Type | Description   |
|------|------|---|
|      |      | <ul style="list-style-type: none"> <li>- <code>False</code>, to exclude from the report offline endpoints.</li> </ul> |

● **Firewall Activity**

The object must contain these members:

| Name                           | Type    | Description  |
|--------------------------------|---------|--|
| <code>reportingInterval</code> | integer | The member is mandatory.<br>This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a>   |
| <code>filterType</code>        | integer | The member is mandatory.<br>Possible values: <ul style="list-style-type: none"> <li>- 0 - All endpoints</li> <li>- 1 - Only endpoints with the following blocked threats: traffic attempts and port scans.</li> </ul>  |
| <code>trafficAttempts</code>   | boolean | This member should be set only if <code>filterType</code> has the value 1.<br>Possible values: <ul style="list-style-type: none"> <li>- <code>True</code>, to include in the report endpoints with blocked traffic attempts.</li> <li>- <code>False</code>, to exclude from the report endpoints with blocked traffic attempts.</li> </ul> |
| <code>portScans</code>         | boolean | This member should be set only if <code>filterType</code> has the value 1.<br>Possible values: <ul style="list-style-type: none"> <li>- <code>True</code>, to include in the report endpoints with blocked port scans.</li> </ul>  |



| Name | Type | Description  |
|------|------|--|
|      |      | <ul style="list-style-type: none"> <li>- False, to exclude from the report endpoints with blocked port scans.</li> </ul> |

● **Malware Activity**

The object must contain these members:

| Name              | Type    | Description  |
|-------------------|---------|--|
| reportingInterval | integer | This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a>                           |
| filterType        | integer | The member is mandatory.<br>Possible values: <ul style="list-style-type: none"> <li>- 0 - All endpoints</li> <li>- 1 - Only endpoints with unresolved malware</li> </ul> |

● **Malware Status**

The object must contain these members:

| Name              | Type    | Description  |
|-------------------|---------|--|
| reportingInterval | integer | The member is mandatory.<br>This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |
| filterType        | integer | The member is mandatory.<br>Possible values: <ul style="list-style-type: none"> <li>- 0 - All endpoints</li> <li>- 1 - Only endpoints still infected</li> </ul>            |

● **Network Status**

The object must contain these members:

| Name                    | Type    | Description   |
|-------------------------|---------|---|
| <code>filterType</code> | integer | The member is mandatory.<br>Possible values:<br><ul style="list-style-type: none"> <li>– 0 - All endpoints</li> <li>– 1 - Only endpoints with issues</li> <li>– 2 - Only endpoints with unknown status</li> </ul> |

- **On demand scanning**

The object must contain these members:

| Name                           | Type    | Description   |
|--------------------------------|---------|---|
| <code>reportingInterval</code> | integer | The member is mandatory.<br>This value depends on the report occurrence.<br>For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |

- **Security Audit**

The object must contain these members:

| Name                           | Type    | Description   |
|--------------------------------|---------|---|
| <code>reportingInterval</code> | integer | The member is mandatory.<br>This value depends on the report occurrence.<br>For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |

- **Top 10 Detected Malware**

The object must contain these members:

| Name                           | Type    | Description              |
|--------------------------------|---------|--------------------------|
| <code>reportingInterval</code> | integer | The member is mandatory. |



| Name | Type | Description  |
|------|------|--|
|      |      | This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |

● **Top 10 Infected Endpoints**

The object must contain these members:

| Name              | Type    | Description   |
|-------------------|---------|---|
| reportingInterval | integer | The member is mandatory. This value depends on the report occurrence. For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |

● **Update Status**

The object must contain these members:

| Name     | Type    | Description  |
|----------|---------|--|
| updated  | boolean | Possible values: <ul style="list-style-type: none"> <li>- True, to include in the report updated endpoints.</li> <li>- False, to exclude from the report updated endpoints.</li> </ul>                           |
| disabled | boolean | Possible values: <ul style="list-style-type: none"> <li>- True, to include in the report endpoints with update disabled.</li> <li>- False, to exclude from the report endpoints with update disabled.</li> </ul> |
| outdated | boolean | Possible values: <ul style="list-style-type: none"> <li>- True, to include in the report outdated endpoints.</li> </ul>  |



| Name                        | Type                 | Description  |
|-----------------------------|----------------------|--|
|                             |                      | <ul style="list-style-type: none"> <li>- <code>False</code>, to exclude from the report outdated endpoints.</li> </ul>   |
| <code>pendingRestart</code> | <code>boolean</code> | Possible values: <ul style="list-style-type: none"> <li>- <code>True</code>, to include in the report endpoints that need to be restarted.</li> <li>- <code>False</code>, to exclude from the report endpoints that need to be restarted.</li> </ul> |

● **VM Network Protection Status**

The object must contain these members:

| Name                    | Type                 | Description  |
|-------------------------|----------------------|--|
| <code>filterType</code> | <code>integer</code> | The member is mandatory.<br>Possible values: <ul style="list-style-type: none"> <li>- 0 - All endpoints</li> <li>- 1 - Only protected endpoints</li> </ul> |

● **HVI Activity**

The object must contain these members:

| Name                           | Type                 | Description   |
|--------------------------------|----------------------|---|
| <code>reportingInterval</code> | <code>integer</code> | The member is mandatory.<br>This value depends on the report occurrence.<br>For more information, refer to <a href="#">Relation between reporting interval and recurrence</a> |



**Important**

The object should not be set for these reports:

- **Endpoint Modules Status**



- Policy Compliance
- Security Server Status

### Relation between reporting interval and recurrence

| occurrence         | reportingInterval   |
|--------------------|---|
| 2 - Hourly report  | Possible values:<br>- 0 - Today   |
| 3 - Daily report   | Possible values:<br>- 0 - Today<br>- 1 - Last day<br>- 2 - This Week  |
| 4 - Weekly report  | Possible values:<br>- 0 - Today<br>- 1 - Last day<br>- 2 - This Week<br>- 3 - Last Week<br>- 4 - This Month   |
| 5 - Monthly report | Possible values:<br>- 0 - Today<br>- 1 - Last day<br>- 2 - This week<br>- 3 - Last week<br>- 4 - This month<br>- 5 - Last month<br>- 6 - Last 2 months<br>- 7 - Last 3 months |

| occurrence        | reportingInterval                                      |
|-------------------|--|
|                   | - 8 - This year  |
| 6 - Yearly report | Possible values:<br>- 8 - This year<br>- 9 - Last year |

## Return value

This method returns a String: the ID of the created report.

## Example

### Request :

```
{
  "params": {
    "name": "My Report hourly",
    "type": 1,
    "targetIds": ["559bd17ab1a43d241b7b23c6",
                 "559bd17ab1a43d241b7b23c7"],
    "scheduledInfo": {
      "occurrence": 2,
      "interval": 4
    },
    "emailList": ["user@company.com",
                  "user2@company.com"]
  },
  "jsonrpc": "2.0",
  "method": "createReport",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Request :

```
{
  "params": {
    "name": "My Report daily",
```



```
"type": 8,
"targetIds": ["559bd17ab1a43d241b7b23c6",
              "559bd17ab1a43d241b7b23c7"],
"scheduledInfo": {
  "occurrence": 3,
  "startHour": 10,
  "startMinute": 30
},
"options": {
  "filterType": 1,
  "antivirusOn": true,
  "antivirusOff": false,
  "updated": true,
  "disabled": false,
  "outdated": false,
  "online": false,
  "offline": true
}
},
"jsonrpc": "2.0",
"method": "createReport",
"id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": "563c78e2b1a43d4043d60413"
}
```

## 2.5.2. getReportsList

This method returns the list of scheduled reports, according to the parameters received.

## Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `virtualmachines`, for "Virtual Machines"

For example, the request URL for the `virtual machines` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/reports/virtualmachines
```

## Parameters

| Parameter         | Type   | Optional | Description   |
|-------------------|--------|----------|---|
| <code>name</code> | String | Yes      | The name of the report.   |
| <code>type</code> | Number | No       | The report type. The available types are: <ul style="list-style-type: none"><li>• 1 - Antiphishing Activity</li><li>• 2 - Blocked Applications</li><li>• 3 - Blocked Websites</li><li>• 5 - Data Protection</li><li>• 6 - Device Control Activity</li><li>• 7 - Endpoint Modules Status</li><li>• 8 - Endpoint Protection Status</li><li>• 9 - Firewall Activity</li><li>• 11 - Malware Activity</li><li>• 12 - Malware Status</li><li>• 14 - Network Status</li><li>• 15 - On demand scanning</li><li>• 16 - Policy Compliance</li><li>• 17 - Security Audit</li><li>• 18 - Security Server Status</li></ul> |

| Parameter | Type   | Optional | Description  |
|-----------|--------|----------|--|
|           |        |          | <ul style="list-style-type: none"><li>● 19 - Top 10 Detected Malware</li><li>● 21 - Top 10 Infected Endpoints</li><li>● 22 - Update Status</li><li>● 25 - Virtual Machine Network Status</li><li>● 26 - HVI Activity</li></ul> |
| page      | Number | Yes      | The results page number. Default page number is 1.   |
| perPage   | Number | Yes      | The number of items displayed in a page. The upper limit is 100 items per page. Default value: 30 items per page.  |

## Return value

This method returns an Object containing information about the reports. The returned object contains:

- `page` - the current page displayed
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `items` - the list of reports. Each entry in the list has the following fields:
  - `ID`, the ID of the report
  - `name`, the name of the report
  - `type`, the report type, as described in the Parameters table
  - `occurrence`, the time interval when the report runs. The occurrence can be: 2 - hourly, 3 - daily, 4 - weekly or 5 - monthly. Please mind that value 1 (instant report) is excluded from the valid options.
- `total` - the total number of items

## Example

**Request :**

```
{
  "params": {
    "type": 2,
    "page": 2,
    "perPage": 4
  },
  "jsonrpc": "2.0",
  "method": "getReportsList",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

## Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    "page": 2,
    "pagesCount": 11,
    "perPage": 5,
    "total": 54
    "items": [
      {
        'id': '5638cdceb1a43d46137b23c6',
        'name': 'My report 1',
        'occurrence': 2,
        'type': 2
      },
      {
        'id': '5638d7f8b1a43d49137b23c9',
        'name': 'My report 2',
        'occurrence': 4,
        'type': 2
      },
      {
        'id': u'563b271bb1a43d21077b23c8',
        'name': 'My report 3',
        'occurrence': 4,
        'type': 2
      }
    ]
  }
}
```

```
{
  {
    'id': '563a289eb1a43d2f617b23c6',
    'name': 'My report 4',
    'occurrence': 2,
    'type': 2
  }
}
]
```

### 2.5.3. getDownloadLinks

This method returns an Object with information regarding the report availability for download and the corresponding download links.

The instant report is created one time only and available for download for less than 24 hours.

Scheduled reports are generated periodically and all report instances are saved in the GravityZone database.

#### Parameters

| Parameter | Type   | Optional | Description   |
|-----------|--------|----------|---------------|
| reportId  | String | No       | The report ID |

#### Return value

This method returns an Object containing information for downloading the report. The returned object contains:

- `readyForDownload` - boolean, `True` if the report is ready to be downloaded or `False` otherwise
- `lastInstanceUrl` - string, The URL for downloading the last instance of an instant or scheduled report. It will be present in the response only if `readyForDownload` is `True`. The downloaded result is an archive with two files: a CSV and a PDF. Both files refer to the same last instance of the report.

**Note**

To access this URL, the HTTP basic authentication header (username:password pair) needs to be sent, where the username it is your API key and the password is a an empty string. For more information, refer to [1.3 Authentication](#) section for details.

- `allInstancesUrl` - string, The URL downloads an archive with all generated instances of the scheduled report. The field will be present in the response only if `readyForDownload` is `True` and the report is a scheduled one. The downloaded result is an archive with a pair of files for each instance of the report: a CSV and a PDF file. Both files refer to the same instance of the report.

**Note**

To access this URL, the HTTP basic authentication header (username:password pair) needs to be sent, where the username it is your API key and the password is a an empty string. For more information, refer to [1.3 Authentication](#) section for details.

## Example

### Request :

```
{
  "params": {
    "reportId": "5638d7f8b1a43d49137b23c9"
  },
  "jsonrpc": "2.0",
  "method": "getDownloadLinks",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87g"
}
```

### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    "readyForDownload": True,
  }
}
```

```
"allInstancesUrl":
  "https://YOUR-HOSTNAME/api/
  v1.0/http/downloadReportZip?reportId=
  5645cba6f12a9a8c5e8b4748&
  allInstances=1&serviceType=1",
"lastInstanceUrl":
  "https://YOUR-HOSTNAME/api/
  v1.0/http/downloadReportZip?reportId=
  5645cba6f12a9a8c5e8b4748&
  allInstances=0&serviceType=1",
}
}
```

## Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    "readyForDownload": False
  }
}
```

## Request :

Eg: Download the report using curl:

```
curl -f0 -u "YOUR_API_KEY:" \
https://YOUR-HOSTNAME/api/v1.0/http/\
downloadReportZip?reportId=5645cba6f12a9a8c5e8b4748&\
allInstances=0&serviceType=1 > lastReportInstances.zip
```

Equivalent with:

```
curl -f0 -H "Authorization: Basic API_KEY_ENCODED_BASE64" \
https://YOUR-HOSTNAME/api/v1.0/http/\
downloadReportZip?reportId=5645cba6f12a9a8c5e8b4748&\
allInstances=0&serviceType=1 > lastReportInstances.zip
```

Where `API_KEY_ENCODED_BASE64` is your API key encoded using base64.

## 2.5.4. deleteReport

The method deletes a report by its ID.

### Parameters

| Parameter | Type   | Optional | Description   |
|-----------|--------|----------|---------------|
| reportId  | String | No       | The report ID |

### Return value

This method returns a Boolean: True when the report was successfully deleted.

### Example

#### Request :

```
{
  "params": {
    "reportId": "5638d7f8b1a43d49137b23c9"
  },
  "jsonrpc": "2.0",
  "method": "deleteReport",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87g"
}
```

#### Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": True
}
```



```
}
```

## 2.6. Quarantine

The Quarantine API contains the following methods allowing the management of quarantine items.

- `getQuarantineItemsList` : retrieves the list of available quarantined items related to a company.
- `createRemoveQuarantineItemTask` : creates a task to remove quarantined items.
- `createEmptyQuarantineTask` : creates a task to empty the quarantined items list.
- `createRestoreQuarantineItemTask` : creates a task to restore quarantined items.
- `createRestoreQuarantineExchangeItemTask` : creates a task to restore exchange quarantined items.

API url: [CONTROL\\_CENTER\\_APIs\\_ACCESS\\_URL/v1.0/jsonrpc/quarantine](#)

### 2.6.1. getQuarantineItemsList

This method retrieves the list of quarantined items available for a company.

An item can be a file or an Microsoft Exchange object.

#### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"
- `exchange`, for "Security for Exchange"

For example, the request URL for the `exchange` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/quarantine/exchange
```

## Parameters

| Parameter  | Type   | Optional | Description   |
|------------|--------|----------|---|
| endpointId | String | Yes      | The ID of the computer for which you want to retrieve the quarantined items. If not passed, the method returns the items quarantined in the entire network. |
| page       | Number | Yes      | The results page. The default value is 1.   |
| perPage    | Number | Yes      | The number of items displayed in a page. The upper limit is 100 items per page. Default value is 30 items per page.   |

## Return value

This method returns an Array containing objects with the quarantined items. Each entry in the array has the following structure:

- `page` - the current displayed page
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `total` - the total number of items
- `items` - the list of quarantined items. Each entry in the list has the following fields:
  - `id`, the ID of the quarantined item,
  - `quarantinedOn`, the date and time when the object was quarantined,
  - `actionStatus`, the status of the action taken on the quarantined file: (0 - None; 1 - Pending remove; 2 - Pending restore; 3 - Remove failed; 4 - Restore failed; 16 - Pending save; 17 - Failed save) ,
  - `endpointId`, the ID of the endpoint on which the threat was detected,
  - `endpointName`, the name of endpoint on which the threat was detected,
  - `endpointIP`, the IP of endpoint on which the threat was detected,
  - `canBeRestored`, has the value `True` if the restore operation is allowed, `False` otherwise,
  - `companyId`, the company ID,



- details, more information related to the quarantined item. For information regarding the content of the details member, refer to [“Contents of details” \(p. 103\)](#).

## Contents of details

For the `Computers` and `Virtual Machines` service, the `details` field has this structure:

| Field name            | Data type | Description  |
|-----------------------|-----------|--|
| <code>filePath</code> | String    | Path to the infected or suspicious file on the endpoint it was detected on |

For `Security for Exchange` service, the `details` field has this structure:

| Field name                  | Data type | Description  |
|-----------------------------|-----------|--|
| <code>detectionPoint</code> | Integer   | The level where the detection took place. Possible values: <ul style="list-style-type: none"> <li>● 0 - transport</li> <li>● 1 - mailbox</li> <li>● 2 - folder</li> <li>● 3 - on demand</li> </ul>   |
| <code>itemType</code>       | Integer   | The quarantined object type. Possible values: <ul style="list-style-type: none"> <li>● 0 - attachment</li> <li>● 1 - email</li> </ul>  |
| <code>threatStatus</code>   | String    | The status of the object when scan is complete. The status shows if an email is spam or contains unwanted content, or if an attachment is malware infected, suspect of being infected, unwanted or unscannable. Possible values are: <ul style="list-style-type: none"> <li>● 0 - spam</li> <li>● 1 - suspected</li> </ul> |

| Field name | Data type | Description   |
|------------|-----------|---|
|            |           | <ul style="list-style-type: none"><li>● 2 - infected</li><li>● 3 - attachment detection</li><li>● 4 - content detection</li><li>● 5 - unscannable</li></ul>   |
| email      | Object    | <ul style="list-style-type: none"><li>● senderIP, a String containing the sender's IP address</li><li>● senderEmail, a String consisting in the sender's email address, as it appears in the email header <b>fieldFrom</b></li><li>● subject, a String with the subject of the quarantined email</li><li>● recipients, an Array with the recipients, as they appear in the email header fields <b>To</b> and <b>Cc</b></li><li>● realRecipients, an Array containing the email addresses of the intended recipients</li></ul> |

## Example

### Request :

```
{
  "params": {
    "companyId": "55896b87b7894d0f367b23c6",
    "endpointId": "55896b87b7894d0f367b23c5",
    "page": 1,
    "perPage": 2
  },
  "jsonrpc": "2.0",
  "method": "getQuarantineItemsList",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
}
```

### Response :

This response example is for computers service:

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": {
    page: 1,
    pageCount: 2,
    perPage: 2,
    total: 4
    items[{
      "id": "5b7d219ab1a43d170b7b23c6",
      "quarantinedOn": "2018-09-08T11:40:58",
      "actionStatus": 2,
      "endpointId": "55896b87b7894d0f367b23c5",
      "endpointName": "Computer 1",
      "endpointIP": "248.49.248.122",
      "threatName": "Virus 0",
      "canBeRestored": false,
      "details": {
        "filePath": "c:\\Virus0\\virus0.exe"
      }
    }
  ]
}
```

This response example is for exchange service:

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": {
    page: 1,
    pageCount: 2,
    perPage: 2,
    total: 4
    items[{
      "id": "5b7d219bb1a43d170b7b23ee",
      "quarantinedOn": "2018-09-13T11:40:59",
      "actionStatus": 0,
      "companyId": "55896b87b7894d0f367b23c6",
      "endpointId": "55896b87b7894d0f367b23c5",
      "endpointName": "Computer 1",
      "endpointIP": "57.238.160.118",
      "endpointAvailable": true,

```

```
"threatName": "Threat1",
"details": {
  "threatStatus": 4,
  "itemType" : 0,
  "detectionPoint": 1,
  "email": {
    "senderIP": "185.36.136.238",
    "senderEmail": "test@test.com",
    "subject":
      "Test subject_5b7d2128b1a43da20c7b23c6",
    "recipients": [
      "receiver1@test.com", "
      receiver2@test.com",
    ]
    "realRecipients": [
      "receiver1@test.com", "
      receiver2@test.com"
    ]
  }
}
}]
}
```

## 2.6.2. createRemoveQuarantineItemTask

This method creates a new task to remove items from quarantine.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `exchange`, for "Security for Exchange"
- `computers`, for "Computers and Virtual Machines"

For example, the request URL for the `computers` service is:

`https://YOUR-HOSTNAME/api/v1.0/jsonrpc/quarantine/computers`

## Parameters

| Parameter          | Type  | Optional | Description                      |
|--------------------|-------|----------|----------------------------------|
| quarantineItemsIds | Array | No       | The list of quarantine items IDs |

## Return value

This method returns a Boolean: True when the task was successfully created.

## Example

### Request :

```
{
  "params": {
    "quarantineItemsIds": [
      "63896b87b7894d0f367b23c6",
      "65896b87b7894d0f367b23c6"
    ]
  },
  "jsonrpc": "2.0",
  "method": "createRemoveQuarantineItemTask",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
}
```

### Response :

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": True
}
```

## 2.6.3. createEmptyQuarantineTask

This method creates a new task to empty the quarantine.

## Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `exchange`, for "Security for Exchange"
- `computers`, for "Computers and Virtual Machines"

For example, the request URL for the `computers` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/quarantine/computers
```

## Parameters

No input parameters are required.

## Return value

This method returns a Boolean: True when the task was successfully created.

## Example

### Request :

```
{
  "params": {},
  "jsonrpc": "2.0",
  "method": "createEmptyQuarantineTask",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
}
```

### Response :

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": True
}
```



## 2.6.4. createRestoreQuarantineItemTask

This method creates a new task to restore items from the quarantine.

### Services

This method requires you to place the `{service}` name in the API URL. The allowed services are:

- `computers`, for "Computers and Virtual Machines"

For example, the request URL for the `computers` service is:

```
https://YOUR-HOSTNAME/api/v1.0/jsonrpc/quarantine/computers
```

### Parameters

| Parameter                         | Type    | Optional | Description  |
|-----------------------------------|---------|----------|--|
| <code>quarantineItemsIds</code>   | Array   | No       | The list of IDs for the quarantined items. You can restore maximum 100 items once.   |
| <code>locationToRestore</code>    | String  | Yes      | The absolute path to the folder where the items will be restored. If the parameter is not set, the original location will be used.   |
| <code>addExclusionInPolicy</code> | Boolean | Yes      | Exclude the files to be restored from future scans. Exclusions do not apply to items with the <b>Default Policy</b> assigned. The default value for this parameter is <code>False</code> . |

### Return value

This method returns a Boolean: True when the task was successfully created.

### Example

**Request :**

```
{
  "params": {
    "quarantineItemsIds": [
      "63896b87b7894d0f367b23c6",
      "65896b87b7894d0f367b23c6"
    ],
    "locationToRestore": "C:\\RestoreDirectory"
    "addExclusionInPolicy": true
  },
  "jsonrpc": "2.0",
  "method": "createRestoreQuarantineItemTask",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
}
```

### Response :

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": True
}
```

## 2.6.5. createRestoreQuarantineExchangeItemTask

This method creates a new task to restore items from the quarantine for Exchange Servers.

### Services

This method requires you to place the {service} name in the API URL. The allowed services are:

- exchange, for "Security for Exchange"

For example, the request URL for the exchange service is:

<https://YOUR-HOSTNAME/api/v1.0/jsonrpc/quarantine/exchange>

## Parameters

| Parameter          | Type   | Optional | Description  |
|--------------------|--------|----------|--|
| quarantineItemsIds | Array  | No       | The list of IDs for the quarantined items. You can restore maximum 100 items once.   |
| username           | String | No       | The username of an Microsoft Exchange user. The username must include the domain name.                                     |
| password           | String | No       | The password of an Exchange user   |
| email              | String | Yes      | The email address of the Exchange user. This parameter is necessary when the email address is different from the username. |
| ewsUrl             | String | Yes      | The Exchange Web Services URL .The EWS URL is necessary when the Exchange Autodiscovery does not work.                     |

## Return value

This method returns a Boolean: True when the task was successfully created

## Example

### Request :

```
{
  "params": {
    "quarantineItemsIds": [
      "63896b87b7894d0f367b23c6",
      "65896b87b7894d0f367b23c6"
    ],
    "username": "user@domain",
    "password": "userPassword"
  },
  "jsonrpc": "2.0",
  "method": "createRestoreQuarantineExchangeItemTask",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
```



```
}
```

**Response :**

```
{  
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",  
  "jsonrpc": "2.0",  
  "result": True  
}
```

## 3. API USAGE EXAMPLES

The following API usage examples make use of the following generated API key: "UjlMS+0m1l9IUZjpyJG8gbnv2Mta4T".

### 3.1. C# Example

In the following example, we list the endpoints from a specified container using C#.

```
/** This example makes use of the json-rpc-csharp project:
 * https://github.com/adamashton/json-rpc-csharp
 */

String apiURL =
    "https://{domain}/api/v1.0/jsonrpc/";

// Make a request on the companies API.
Client rpcClient = new Client(apiURL + "network/computers");

String apiKey = "UjlMS+0m1l9IUZjpyJG8gbnv2Mta4T";
String userPassString = apiKey + ":";
String authorizationHeader = System.Convert.ToBase64String(
    System.Text.Encoding.UTF8.GetBytes(userPassString));

rpcClient.Headers.Add("Authorization",
    "Basic " + authorizationHeader);

JToken parameters = new JObject();
parameters["parentId"] = "55d43258b1a43ddf107baad4";
parameters["isManaged"] = True;
parameters["page"] = 1;
parameters["perPage"] = 2;

Request request = rpcClient.NewRequest(
    "getEndpointsList", parameters);

Response response = rpcClient.Rpc(request);
```

```
if (response.Result != null) {
    JToken result = response.Result;
    Console.WriteLine(response.ToString());
}
```

## 3.2. curl Example

In the following example, we get the list of containers for the mobile service in the Network API.

```
curl -i \
-H "Authorization: \
Basic VWpsTVMrMG0xbDlJVVpqcGpXeUpHOGdibnYyTXRhNFQ6" \
-H "Content-Type: application/json" \
-d '{"id": "123456789", "jsonrpc": "2.0",
"method": "getContainers", "params": []}' \
-X POST \
https://{domain}/api/v1.0/jsonrpc/network/mobile

HTTP/1.1 200 OK
Date: Wed, 10 Jan 2015 13:25:30 GMT
Content-Length: 103
Content-Type: application/json; charset=utf-8

{"id": "123456789", "jsonrpc": "2.0", "result":
  [{"id": "55d43258b1a43ddf107b23d8", "name": "Custom Groups"}]}
```

### 3.3. Python Example

Now, we will query the list of available packages.

```
import base64
import pyjsonrpc
import requests
import simplejson

# Generate Authorization header from API key
apiKey = "UjlMS+0m1l9IUZjppjWyJG8gbnv2Mta4T"
encodedUserPassSequence = base64.b64encode(apiKey + ":")
authorizationHeader = "Basic " + encodedUserPassSequence

json = pyjsonrpc.create_request_json("getPackagesList")
result = requests.post(
    "https://{domain}/api/v1.0/jsonrpc/packages",
    json,
    verify=False,
    headers = {
        "Content-Type": "application/json",
        "Authorization": authorizationHeader
    })

jsonResult = simplejson.loads(result.content)

print jsonResult
```

Output:

```
{'jsonrpc': '2.0',
 'id': '61f4dadac-bd10-448d-af35-16d45a188d9e',
 'result': {
 'items': [
 {'type': 3, 'id': '55d4325cb1a43ddf107b241b',
 'name': 'Default Security Server Package'},
 {'type': 4, 'id': '55d43e34b1a43db5187b23c6',
 'name': 'My package'}]
 , 'total': 2,
 'page': 1,
 'perPage': 30,
```

```
'pagesCount': 0}
}
```

### 3.4. Node.js example

In this example, we will make the exact previous call, only this time we will use Node.js

```
// Using the request module:
// npm install request
var request = require('request');

request({
  uri: "https://{domain}/ \
    api/v1.0/jsonrpc/packages",
  method: "POST",
  headers: {
    'Authorization':
      "Basic VWpsTVMrMG0xbDlJVVpqcGpXeUpHOGdibnYyTXRhNFQ6"
  },
  json: {
    "id": "123456789",
    "jsonrpc": "2.0",
    "method": "getPackagesList",
    "params": []
  }
}, function(response, body) {
  console.log(body);
});

// Output:

// {'jsonrpc': '2.0',
//  'id': '61f4dadcb10-448d-af35-16d45a188d9e',
//  'result': {
//    'items': [
//      {'type': 3, 'id': '55d4325cb1a43ddf107b241b',
//      'name': 'Default Security Server Package'},
```





```
// {'type': 4, 'id': '55d43e34b1a43db5187b23c6',  
// 'name': 'My package'}}]  
// , 'total': 2,  
// 'page': 1,  
// 'perPage': 30,  
// 'pagesCount': 0}  
// }
```