

The background of the cover is a dark, futuristic digital space. It features glowing blue and cyan light trails, circular patterns, and a central bright light source that creates a lens flare effect. The overall aesthetic is high-tech and cybernetic.

Bitdefender®

GravityZone

API GUIDE

Bitdefender Control Center API Guide

Publication date 2021.07.06

Copyright© 2021 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 2
 - 1.3. API Keys 4
 - 1.4. Authentication 5
 - 1.5. Errors reporting 5
- 2. Reference 8
 - 2.1. Accounts 8
 - 2.1.1. getAccountsList 8
 - 2.1.2. deleteAccount 11
 - 2.1.3. createAccount 12
 - 2.1.4. updateAccount 14
 - 2.1.5. configureNotificationsSettings 17
 - 2.1.6. getNotificationsSettings 20
 - 2.1.7. Objects 22
 - 2.2. Companies 26
 - 2.2.1. updateCompanyDetails 27
 - 2.2.2. getCompanyDetails 28
 - 2.3. Licensing 30
 - 2.3.1. getLicenseInfo 31
 - 2.3.2. setLicenseKey 33
 - 2.3.3. getMonthlyUsage 34
 - 2.3.4. getMonthlyUsagePerProductType 36
 - 2.4. Network 39
 - 2.4.1. getEndpointsList 39
 - 2.4.2. getManagedEndpointDetails 45
 - 2.4.3. createCustomGroup 51
 - 2.4.4. deleteCustomGroup 52
 - 2.4.5. getCustomGroupsList 53
 - 2.4.6. moveEndpoints 54
 - 2.4.7. deleteEndpoint 55
 - 2.4.8. moveCustomGroup 56
 - 2.4.9. getNetworkInventoryItems 57
 - 2.4.10. createScanTask 63
 - 2.4.11. createReconfigureClientTask 64
 - 2.4.12. getScanTasksList 69
 - 2.4.13. setEndpointLabel 72
 - 2.4.14. createScanTaskByMac 73
 - 2.5. Packages 74
 - 2.5.1. getInstallationLinks 75
 - 2.5.2. createPackage 77
 - 2.5.3. getPackagesList 86
 - 2.5.4. deletePackage 87
 - 2.5.5. getPackageDetails 88
 - 2.6. Policies 92



- 2.6.1. getPoliciesList 92
- 2.6.2. getPolicyDetails 94
- 2.7. Integrations 96
 - 2.7.1. getHourlyUsageForAmazonEC2Instances 96
 - 2.7.2. configureAmazonEC2IntegrationUsingCrossAccountRole 97
 - 2.7.3. generateAmazonEC2ExternalIdForCrossAccountRole 98
 - 2.7.4. getAmazonEC2ExternalIdForCrossAccountRole 99
 - 2.7.5. disableAmazonEC2Integration 100
- 2.8. Reports 101
 - 2.8.1. createReport 101
 - 2.8.2. getReportsList 120
 - 2.8.3. getDownloadLinks 123
 - 2.8.4. deleteReport 126
- 2.9. Push 127
 - 2.9.1. setPushEventSettings 127
 - 2.9.2. getPushEventSettings 130
 - 2.9.3. sendTestPushEvent 132
 - 2.9.4. getPushEventStats 133
 - 2.9.5. resetPushEventStats 135
 - 2.9.6. Event Types 136
 - 2.9.7. Push event JSON RPC messages 137
- 2.10. Incidents 186
 - 2.10.1. addToBlocklist 186
 - 2.10.2. getBlocklistItems 187
 - 2.10.3. removeFromBlocklist 190
 - 2.10.4. createIsolateEndpointTask 190
 - 2.10.5. createRestoreEndpointFromIsolationTask 191
- 2.11. Quarantine 192
 - 2.11.1. getQuarantineItemsList 193
 - 2.11.2. createRemoveQuarantineItemTask 200
 - 2.11.3. createEmptyQuarantineTask 202
 - 2.11.4. createRestoreQuarantineItemTask 203
 - 2.11.5. createRestoreQuarantineExchangeItemTask 204
 - 2.11.6. createAddFileToQuarantineTask 206
- 2.12. General 207
 - 2.12.1. getApiKeyDetails 207
- 3. API Usage Examples 209
 - 3.1. C# Example 209
 - 3.2. curl Example 210
 - 3.3. Python Example 211
 - 3.4. Node.js example 212
 - 3.5. PowerShell Example 213
 - 3.6. VBScript Example 216
- A. Appendices 220
 - A.1. API Error Codes 220

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>.

Here is an example of API call updating the company name inside Bitdefender Control Center:

```
{
  "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7",
  "jsonrpc": "2.0",
  "method": "updateCompanyDetails",
  "params": {
    "name": "My Company Name"
  }
}
```

For this call, the following response is sent back to the application:

```
{
  "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7",
  "jsonrpc": "2.0",
  "result": null
}
```

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: [CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/](#). The full URL of the API is obtained by adding the API name to the base URL.

The **CONTROL_CENTER_APIs_ACCESS_URL** is displayed in the **Access URL** field. To find this field click your username in the upper-right corner of the console and choose **My Account**. Go to the **Control Center API section**.


Control Center API	
Access URL:	<input type="text" value="https://cloud.gravityzone.bitdefender.com/api"/>

Currently, the following APIs are being exposed:

1. **Companies**, with the API URL:
[CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/companies](#).
2. **Licensing**, with the API URL:
[CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/licensing](#).
3. **Accounts**, with the API URL:
[CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/accounts](#).
4. **Network**, with the API URL:
[CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/network](#).

5. **Packages**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/packages.`
6. **Policies**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/policies.`
7. **Integrations**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/integrations.`
8. **Reports**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/reports.`
9. **Push**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/push.`
10. **Incidents**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/incidents.`
11. **Quarantine**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/quarantine.`
12. **General**, with the API URL:
`CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/general.`

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://gravityzone.bitdefender.com/> using your Bitdefender Control Center account.
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:

<input type="checkbox"/> Companies API	<input type="checkbox"/> Integrations API
<input type="checkbox"/> Licensing API	<input checked="" type="checkbox"/> Policies API
<input checked="" type="checkbox"/> Packages API	
<input checked="" type="checkbox"/> Network API	

Save Cancel

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

Key	Created
<input type="checkbox"/> [blurred key]	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: CONTROL_CENTER_APIS_ACCESS_URL/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.
 - `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.
 - `twoFactorAuthenticationStatus`, the status of the Two Factor Authentication (2FA), set to `True` if enabled for the account.
 - `companyName`, the name of the company of the user account.
 - `companyId`, the ID of the company of the user account.
- `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",
        "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
        },
        "companyName": "bitdefender",
        "companyId": "58541613aaed7090058b4567"
      },
      {
        "id": "585d3170aaed70b7048b4633",
        "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  
    },  
    "twoFactorAuthenticationStatus": true,  
    "companyName": "bitdefender",  
    "companyId": "58541613aaed7090058b4567"  
  }  
]  
}  
}
```

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.
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	The 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. The default value is 1 - Company Administrator. These are the available roles: <ul style="list-style-type: none">● 1 - Company Administrator.● 2 - Network Administrator.● 3 - Reporter.

Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> 5 - Custom. For this role, rights must be specified.
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"> <code>manageNetworks</code> Setting this to true implies <code>manageReports</code> right to true <code>manageUsers</code> <code>manageReports</code> <code>companyManager</code> <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",
    "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 email address for the account.



Parameter	Type	Optional	Description
password	String	Yes	The password for the account. 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.
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"> ● 1 - Company Administrator. ● 2 - Network Administrator. ● 3 - Reporter. ● 5 - Custom. For this role, rights must be specified.
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"> ● <code>manageNetworks</code> Setting this to True implies <code>manageReports</code> right to true ● <code>manageUsers</code> ● <code>manageReports</code> ● <code>companyManager</code> 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 <code>false</code> .
targetIds	Array	Yes	A list of IDs representing the targets to be managed by the user account.

Return value

This method returns a Boolean which is 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"> • <code>type</code>, the notification type, • <code>enabled</code>, <code>True</code> if the notification is enabled, <code>False</code> otherwise, • <code>visibilitySettings</code>, an object containing the visibility settings. For more information, refer to Notifications Visibility Options, • <code>configurationSettings</code>, notification specific configurations. This field depends on the notification type. For more information, refer to Relation Between Notification Type and configurationSettings.

Return value

This method returns a Boolean which is 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"]
        },
        "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" : []
    },
    "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 Configuration 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>



Note

- At least one visibility option from showInConsole, sendPerEmail must be set to True when the notification is enabled.
- The sendPerEmail, useCustomEmailDistribution and emails visibility options are not available for these notification types:



- 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"> ● <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 ● <code>threshold</code>, <code>integer</code>, the percentage of managed network objects infected by the same malware. Valid values are between 1 and 100
2 - License Expires	The <code>configurationSettings</code> parameter should not be set for this notification.
3 - Deployments have reached or exceeded license limit	<ul style="list-style-type: none"> ● <code>triggerSettings</code>, <code>integer</code>, the license status which triggers this notification. Set to 1 for Exceeded, or 2 for Reached and exceeded
4 - License Limit Is About To Be Reached	The <code>configurationSettings</code> parameter should not be set for this notification.
5 - Update Available	<ul style="list-style-type: none"> ● <code>showConsoleUpdate</code>, <code>boolean</code>, <code>True</code> to receive the notification for console updates, <code>False</code> otherwise ● <code>showPackageUpdate</code>, <code>boolean</code>, <code>True</code> to receive the notification for package updates, <code>False</code> otherwise ● <code>showProductUpdate</code>, <code>boolean</code>, <code>True</code> to receive the notification for product updates, <code>False</code> otherwise
9 - Exchange License Usage Limit Has Been Reached	The <code>configurationSettings</code> parameter should not be set for this notification.



Notification type	Available configurationSettings items with their type and possible values
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.
13 - Authentication Audit	The configurationSettings parameter should not be set for this notification.
17 - Antiphishing 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"> notUpdated, boolean, True to receive the notification when the Security Server is outdated, False otherwise reboot, boolean, True to receive the notification when the Security Server needs a reboot, False otherwise
24 - Product Registration Event	The configurationSettings parameter should not be set for this notification.



Notification type	Available configurationSettings items with their type and possible values
25 - Overloaded Security Server Event	<ul style="list-style-type: none"> • <code>useThreshold</code>, <code>boolean</code>, <code>True</code> to receive the notification when the scan load exceeds a custom threshold, <code>False</code> otherwise • <code>threshold</code>, <code>integer</code>, the minimum scan load necessary to issue this notification. Valid values are between 1 and 100
26 - Task Status	<ul style="list-style-type: none"> • <code>statusThreshold</code>, <code>integer</code>, the task status which triggers this notification. Set to 2 for any status, 3 for failed tasks
27 - Outdated Update Server	The <code>configurationSettings</code> parameter should not be set for this notification.
32 - Amazon EC2 Trial Expires in 7 Days	The <code>configurationSettings</code> parameter should not be set for this notification.
33 - Amazon EC2 Trial Expires Tomorrow	The <code>configurationSettings</code> parameter should not be set for this notification.
34 - Amazon EC2 Licensing event	The <code>configurationSettings</code> parameter should not be set for this notification.
35 - Amazon EC2 Cancelation event	The <code>configurationSettings</code> parameter should not be set for this notification.
36 - Amazon EC2 Invalid credentials	The <code>configurationSettings</code> parameter should not be set for this notification.

2.2. Companies

The Companies API includes several methods allowing the management of company accounts:

- `updateCompanyDetails` : updates company information, such as name.
- `getCompanyDetails` : retrieves the details of a company.

API url: CONTROL_CENTER_APIS_ACCESS_URL/v1.0/jsonrpc/companies

2.2.1. updateCompanyDetails

This method updates the details of a company account.

Parameters

Parameter	Type	Optional	Description
name	String	Yes	The company's name. It must be unique. If not set, the company's name will not be changed.
address	String	Yes	The company's address. If not set, the company's address will not be changed.
phone	String	Yes	The company's phone number. If not set, the company's phone number will not be changed.
enforce2FA	Boolean	Yes	An option that defines Two Factor Authentication (2FA) enforcement for all GravityZone user accounts in the company. Available values: <code>true</code> or <code>false</code> . The default value is <code>false</code> .

Return value

This method does not return any value.

Example

Request :

```
{
  "params": {
    "name": "Example LTD",
    "address": "Str Example No 1",
    "phone": "0040740000001"
  },
  "jsonrpc": "2.0",
  "method": "updateCompanyDetails",
  "id": "60357f0e-94da-463c-ba36-f50f2ef8c34f"
}
```

Response :

```
{
  "id": "60357f0e-94da-463c-ba36-f50f2ef8c34f",
  "jsonrpc": "2.0",
  "result": null
}
```

2.2.2. `getCompanyDetails`

This method retrieves the details of a company.

Parameters

No input parameters are required.

Return value

This method returns an Object containing the details of the selected company:

- `type` - the company type: 1 for Customer
- `name` - the name of the company
- `id` - the ID of the company
- `address` - the address of the company
- `phone` - the phone of the company
- `canBeManagedByAbove` - the security management status for the company: `true`, if the security can be managed by parent companies
- `enforce2FA` - a boolean specifying if the Two Factor Authentication (2FA) is enforced for user accounts belonging to the selected company
- `isSuspended` - company account status: `true`, if the company is suspended
- `createdAt` - a String representing the UTC date and time at which the company was created
- `country` - a String representing the country code in [ISO 3166](#) format. If the code is not specified, the String has the value `N/A`

- **state** - a String representing the country state code in [ISO 3166](#) format. If the code is not specified, the String has the value N/A
- **contactPerson** - an Object containing the details of the contact person:
 - **fullName**, their first name and surname
 - **email**, their business email address
 - **phoneNumber**, their business phone number
 - **companyRole**, their position in the company
- **riskScore** - an Object containing the following information about the company's security risks:
 - **value**, the company's security risk score value in percentage. It is broken down into misconfigurations, app vulnerabilities, human risks, and adjusted by the health industry modifier
 - **impact**, the company's security risk impact (Low, Medium, High)
 - **misconfigurations**, the percentage of misconfigurations in the company's security risk score
 - **appVulnerabilities**, the percentage of app vulnerabilities in the company's security risk score
 - **humanRisks**, the percentage of human risks in the company's security risk score
 - **industryModifier**, dynamically adjusts your company score based on CVEs discovered in your environment that have already been exploited at industry level

Example

Request :

```
{
  "params": {
  },
  "jsonrpc": "2.0",
  "method": "getCompanyDetails",
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810"
}
```

Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": {
    "type": 1,
    "name": "Example LTD",
    "id": "54aeab40b1a43dc0467b23e9",
    "address": "Str Example No 1",
    "phone": "0040740000001",
    "canBeManagedByAbove": true,
    "enforce2FA": true,
    "isSuspended": false,
    "createdAt": "2017-01-28T15:01:15",
    "country": "CA",
    "state": "CA-BC",
    "contactPerson": {
      "fullName": "Stephen Jhonson",
      "email": "stephen.jhonsons@example.email.com",
      "phoneNumber": "0040740000001",
      "companyRole": "Owner / President"
    },
    "riskScore": {
      "value": "87%",
      "impact": "High",
      "misconfigurations": "70%",
      "appVulnerabilities": "11%",
      "humanRisks": "19%",
      "industryModifier": "6%"
    }
  }
}
```

2.3. Licensing

The Licensing API contains the following methods, exposing the licensing related functionalities:

- [getLicenseInfo](#) : retrieves the license information for a company.
- [setLicenseKey](#) : sets the license key for a company.

- `getMonthlyUsage` : exposes a company's monthly license usage for endpoints and Exchange mailboxes, within a certain month.
- `getMonthlyUsagePerProductType` : exposes a company's monthly license usage for endpoints and Exchange mailboxes, within a certain month, for all available product types.

API url: CONTROL_CENTER_APIS_ACCESS_URL/v1.0/jsonrpc/licensing

2.3.1. getLicenseInfo

This method retrieves the license information for a company.

Parameters

No input parameters are required.

Return value

This method returns an Object containing the license details:

- `subscriptionType` - the company's subscription type: 1 for trial subscription, 2 for licensed subscription, 3 for monthly subscription, 4 for monthly license trial, 5 for monthly subscription trial, 6 for FRAT subscription
- `expiryDate` - the license expiry date
- `usedSlots` - the number of used seats
- `totalSlots` - the number of total seats for licensed subscriptions, or the number of reserved seats for child companies that inherited a monthly license from their parent company.
- `licenseKey` - the license key for trial or licensed subscriptions.
- `endSubscription` - the subscription end date. This option is available for companies with monthly subscription.
- `autoRenewPeriod` - the subscription auto renewal period in months. This option is available for companies with monthly subscription.
- `manageExchange` - True if the company is allowed to manage the Security for Exchange feature, false otherwise

- `manageEncryption` - True if the company is allowed to manage the Full Disk Encryption feature, false otherwise
- `manageRemoteEnginesScanning` - True if the company is allowed to manage the Security for Virtualized Environments feature, false otherwise
- `manageHyperDetect` - True if the company is allowed to manage the HyperDetect feature, false otherwise
- `manageSandboxAnalyzer` - True if the company is allowed to manage the Sandbox Analyzer feature, false otherwise
- `managePatchManagement` - True if the company is allowed to manage the Patch Management feature, false otherwise
- `manageEventCorrelator` - True if the company is allowed to manage the Endpoint Detection and Response feature, false otherwise.
- `manageEmailSecurity` - True if the company is allowed to manage the Email Security feature, false otherwise.
- `minimumUsage` - An Object containing types of licenses and the minimum number of slots which the company commits through legal agreement to use on a monthly basis:
 - `endpointMonthlyUsage`, the minimum number of endpoints that the client agreed to use from the main license.
- `assignedProductType` - The type of product assigned to the company:
 - 0, for Endpoint Security
 - 3, for Bitdefender EDRThe parameter is returned only when `subscriptionType` has one of these values:
 - 3, for monthly subscription
 - 5, for monthly subscription trial
- `additionalProductTypes` - An array of the product types that can be assigned to child companies:
 - 0, for Endpoint Security
 - 3, for Bitdefender EDRThe parameter is returned only when `subscriptionType` has one of these values:
 - 3, for monthly subscription
 - 5, for monthly subscription trial

Example

Request :

```
{
  "params": {
  },
  "jsonrpc": "2.0",
  "method": "getLicenseInfo",
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb"
}
```

Response :

```
{
  "id": "c67860e2-36cc-43bd-bc0f-f1061c180b52",
  "jsonrpc": "2.0",
  "result": {
    "subscriptionType": 1,
    "expiryDate": "2015-01-18T10:02:30",
    "usedSlots": 0,
    "licenseKey": "LICKY1",
    "endSubscription": "2020-04-14",
    "autoRenewPeriod": 12,
    "assignedProductType": 0,
    "additionalProductTypes": [0]
  }
}
```

2.3.2. setLicenseKey

This method sets the license key for a company.

Parameters

Parameter	Type	Optional	Description
licenseKey	String	No	The license key to be set.

Return value

This method does not return any value.

Example

Request :

```
{
  "params": {
    "licenseKey" : "TNB3AAA"
  },
  "jsonrpc": "2.0",
  "method": "setLicenseKey",
  "id": "48daf1bc-4078-411c-bf44-4f293e68f501"
}
```

Response :

```
{
  "id": "48daf1bc-4078-411c-bf44-4f293e68f501",
  "jsonrpc": "2.0",
  "result": null
}
```

2.3.3. getMonthlyUsage

This method exposes the monthly usage for a company in a target month. Returns only usage from endpoints with the default product type - Endpoint Security. If usage from other product types is needed, refer to the `getMonthlyUsagePerProductType` method.

Parameters

Parameter	Type	Optional	Description
targetMonth	String	Yes	The month for which the usage is returned. It should have the following format: mm/yyyy. The default value is the current month.

Return value

This method returns an Object containing the number of license seats used during the specified month, for each acquired service, or 0 if the queried company does not have a monthly license:

- `endpointMonthlyUsage` - the monthly usage for endpoints scanned with local engines.
- `emailSecurityMonthlyUsage` - the monthly usage for Email Security mailboxes.
- `exchangeMonthlyUsage` - the monthly usage for Exchange mailboxes.
- `encryptionMonthlyUsage` - the monthly usage for the encryption module.
- `atsMonthlyUsage` - the monthly usage for the sandboxAnalyzer and hyperDetect modules.
- `edrMonthlyUsage` - the monthly usage for the EDR module.
- `patchManagementMonthlyUsage` - the monthly usage for the patch management module.
- `sveVsMonthlyUsage` - the monthly usage for virtual servers scanned with Security Server.
- `sveVdiMonthlyUsage` - the monthly service usage (in hours) for virtual desktops scanned with Security Server.
- `minimumUsage` - An Object containing types of licenses and the minimum number of slots which the company commits through legal agreement to use on a monthly basis:
 - `endpointMonthlyUsage`, the minimum number of endpoints that the client agreed to use from the main license.

Example

Request :

```
{
  "params": {
    "targetMonth": "03/2015"
  },
}
```

```
"jsonrpc": "2.0",
"method": "getMonthlyUsage",
"id": "5087eab8-b74f-4a3e-85b3-4271e85890d4",
}
```

Response :

```
{
  "id": "5087eab8-b74f-4a3e-85b3-4271e85890d4",
  "jsonrpc": "2.0",
  "result": {
    "endpointMonthlyUsage": 101,
    "emailSecurityMonthlyUsage": 162,
    "exchangeMonthlyUsage": 15,
    "encryptionMonthlyUsage": 69,
    "atsMonthlyUsage": 25,
    "edrMonthlyUsage": 14,
    "patchManagementMonthlyUsage": 28,
    "sveVsMonthlyUsage": 5,
    "sveVdiMonthlyUsage": 30,
    "minimumUsage": {
      "endpointMonthlyUsage": 25
    }
  }
}
```

2.3.4. getMonthlyUsagePerProductType

The method exposes the monthly usage of a company in a target month. Returns the usage per product type, for all available product types.

Parameters

Parameter	Type	Optional	Description
targetMonth	String	Yes	The month for which the usage is returned. It should have the following format: mm/yyyy. The default value is the current month.

Return value

This method returns an Object containing the following:

- `usages` - An array of Objects that contain the number of license seats used during the specified month, for each acquired service and product type.

For Endpoint Security, the object contains the following members:

- `productType`, the product type.
- `endpointMonthlyUsage`, the monthly usage for endpoints scanned with local engines.
- `emailSecurityMonthlyUsage`, the monthly usage (mailboxes) for Email Security (mailboxes).
- `exchangeMonthlyUsage`, the monthly usage (mailboxes) for Exchange Protection.
- `encryptionMonthlyUsage`, the monthly usage for Full Disk Encryption.
- `atsMonthlyUsage`, the monthly usage for the Sandbox Analyzer and HyperDetect.
- `edrMonthlyUsage`, the monthly usage for the Endpoint Detection and Response (EDR).
- `patchManagementMonthlyUsage`, the monthly usage for Patch Management.
- `sveVsMonthlyUsage`, the monthly usage for virtual servers scanned with Security Server.
- `sveVdiMonthlyUsage`, the monthly service usage (in hours) for virtual desktops scanned with Security Server.

For Bitdefender EDR, the object contains the following members:

- `productType`, the product type.
- `endpointMonthlyUsage`, the monthly usage for endpoints scanned with local engines.

- `minimumUsage` - An Object containing types of licenses and the minimum number of slots which the company commits through legal agreement to use on a monthly basis:
 - `endpointMonthlyUsage`, the minimum number of endpoints that the client agreed to use from the main license.

If the queried company does not have a monthly license or subscription, the method returns 0.

Example

Request :

```
{
  "params": {
    "targetMonth": "03/2015",
  },
  "jsonrpc": "2.0",
  "method": "getMonthlyUsagePerProductType",
  "id": "5087eab8-b74f-4a3e-85b3-4271e85890d4",
}
```

Response :

```
{
  "id": "5087eab8-b74f-4a3e-85b3-4271e85890d4",
  "jsonrpc": "2.0",
  "result": {
    "usages": [{
      "endpointMonthlyUsage": 101,
      "emailSecurityMonthlyUsage": 162,
      "exchangeMonthlyUsage": 15,
      "encryptionMonthlyUsage": 69,
      "atsMonthlyUsage": 25,
      "edrMonthlyUsage": 14,
      "patchManagementMonthlyUsage": 28,
      "sveVsMonthlyUsage": 5,
      "sveVdiMonthlyUsage": 30,
      "productType": 0,
    }, {
      "endpointMonthlyUsage": 101,
      "productType": 3
    }
  ],
  "minimumUsage": {
    "endpointMonthlyUsage": 25
  },
}
```

2.4. Network

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

- `getEndpointsList` : returns the list of endpoints under the specified group.
- `getManagedEndpointDetails` : returns the properties of the specified endpoint.
- `createCustomGroup` : creates a new custom group.
- `deleteCustomGroup` : deletes a custom group.
- `getCustomGroupsList` : retrieves the list of groups under a specified group.
- `moveEndpoints` : moves the specified list of endpoints to a custom group.
- `deleteEndpoint` : deletes a specified endpoint.
- `moveCustomGroup` : moves a custom group under another custom group.
- `getNetworkInventoryItems` : returns network inventory items.
- `createScanTask` : launches a scan task on the specified endpoints or groups. The available scan types are: Quick Scan, Full Scan, Memory Scan and Custom Scan.
- `createReconfigureClientTask` : creates a new Reconfigure Client task.
- `getScanTasksList` : returns the list of scan tasks.
- `setEndpointLabel` : sets a label to an endpoint.
- `createScanTaskByMac` : generates scan tasks for managed endpoints identified by MAC address.

API url: CONTROL_CENTER_APIS_ACCESS_URL/v1.0/jsonrpc/network

2.4.1. `getEndpointsList`

This method returns the list of endpoints.

Parameters

Parameter	Type	Optional	Description
<code>parentId</code>	String	Yes	The ID of the target company or group. If not specified or set with a company ID, the method returns only the endpoints under Computers and Groups . Note! To retrieve information on Active Directory endpoints, use the “ getNetworkInventoryItems ” (p. 57) method.
<code>isManaged</code>	Boolean	Yes	The flag to list managed or unmanaged endpoints. By default, the parameter is not set and the method returns all the managed and unmanaged endpoints. If set on <code>True</code> , the method returns only managed endpoints.
<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.
<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 “ Available Filters ” (p. 40).

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"> ● <code>managedWithBest</code> - a Boolean to filter all endpoints with the security agent installed on them. Default value: <code>False</code>. ● <code>managedExchangeServers</code> - a Boolean to filter all protected Exchange servers. Default value: <code>False</code>. This filter requires a valid license key that covers the Security for Exchange security service. ● <code>managedRelays</code> - a Boolean to filter all endpoints with Relay role. Default value: <code>False</code>. ● <code>securityServers</code> - a Boolean to filter all Security Servers. Default value: <code>False</code>.
depth		<ul style="list-style-type: none"> ● <code>allItemsRecursively</code> - a Boolean to filter all endpoints recursively within the Network Inventory of a company. Default value: <code>False</code>.
details		<ul style="list-style-type: none"> ● <code>ssid</code> - string, the SSID (Active Directory SID of the endpoint) used to filter the endpoints regardless of their protection status. ● <code>macs</code> - array, the list of MAC addresses used to filter the endpoints regardless of their protection status. ● <code>name</code> - string, used for filtering the endpoints by name regardless of their protection status. Minimum required string length is three characters.



Important

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

The field `name` works with partial matching.

The filter returns the endpoints whose names are exact match or start with the specified value. To use the specified value as a suffix, use the asterisk symbol (*).

For example:

If name is `computer`, the API returns all endpoints whose names start with `computer`.

If name is `*puter`, then the API returns a list of all endpoints that contain `puter` in their names.

Return value

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

- `page` - the current page
- `pagesCount` - the total number of pages
- `perPage` - the total number of returned items per page
- `total` - the total number of items
- `items` - an array containing 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,
 - `isContainerHost`, boolean `True`, if this endpoint is a Container Host,
 - `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,

- **policy**, an Object informing about the policy active on the endpoint. The object contains the following fields:
 - **id** - a String uniquely identifying the active policy,
 - **name** - the name of the policy,
 - **applied** - a Boolean set to True if the policy is currently applied on the endpoint,
- **movingInfo**, an Object informing upon endpoint transfer from one company to another one. The object contains:
 - **state** - the endpoint moving status (0 - in progress, 1 - moved),
 - **destinationCompanyName** - the name of the company where the endpoint was moved.

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": 1,
        "operatingSystemVersion": "Windows Server 2016",
        "ip": "60.40.10.220",
        "macs": [
          "324935237335"
        ],
        "ssid": "",
        "policy": {
          "id": "6087c0a3da997c5c02249f1d",
          "name": "Default policy",
          "applied": True
        }
      },
      {
        "id" : "23a295d8b1a43d7c4a7b23c9",
        "name" : "Endpoint 2",
        "label" : "endpoint 2",
        "fqdn": "endpoint2.local",
        "groupId": "5a4f4d46b1a53d5f197b23aa",
        "isManaged": true,
        "machineType": 1,
        "operatingSystemVersion": "Windows 7",
        "ip": "60.40.10.221",
        "macs": [
          "325935237445"
        ],
      },
    ]
  }
}
```



```
    "ssid": "",
    "policy": {
      "id": "6084678418a9cf3f9c666c3a",
      "name": "Default policy",
      "applied": True
    },
    "movingInfo": {
      "state": 1,
      "destinationCompanyName": "Company Test"
    }
  }
]
}
```

2.4.2. getManagedEndpointDetails

This method returns detailed information, such as: details to identify the endpoint and the security agent, the status of installed protection modules.

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
- `companyId` - the ID of the company to which the endpoint belongs
- `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 address of the endpoint
- `lastSeen` - the date of the last synchronization with Control Center
- `machineType` - the type of the machine: 1 - computer, 2 - virtual machine, 3 - EC2 Instance, 0 - Other
- `agent` - an Object containing the following information about the agent installed on the endpoint:
 - `engineVersion`, the version of the scanning 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 engine to be used if the primary engine is unavailable when the task is sent. 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`, 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`, the version of the agent

- `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`, identifies which type of agent is installed on the endpoint:
 - 1 - Endpoint Security
 - 2 - Bitdefender Tools
 - 3 - BEST
- `group` - an Object pointing to 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`, a Boolean set to True if the policy is currently applied on the endpoint
- `modules` - an Object informing of the installed modules and their statuses. The fields have Boolean values, `True` - if the module is enabled, or `False` - if the module is disabled.

The available fields are:

- advancedThreatControl
 - antimalware
 - contentControl
 - deviceControl
 - firewall
 - powerUser
 - encryption
 - edrSensor
 - hyperDetect
 - patchManagement
 - relay
 - sandboxAnalyzer
 - exchange
 - advancedAntiExploit.
 - containerProtection.
 - networkAttackDefense.
- **label** - string, the label set to this endpoint
 - **moveState** - an integer reflecting the move state of the endpoint: 0 - no move operation, 1 - moved out of the company, 2 - moved into my company.
 - **managedWithBest** - a Boolean set to True if the agent (BEST) is installed on the endpoint.
 - **isContainerHost** - a Boolean set to True if the endpoint is a Container Host.
 - **managedExchangeServer** - a Boolean set to True if the endpoint is an Exchange Server
 - **managedRelay** - a Boolean set to True if the endpoint has Relay role
 - **securityServer** - a Boolean set to True if the endpoint is a Security Server

- **riskScore** - an Object containing the following information about the endpoint's security risks:
 - **value**, the endpoint's security risk score value in percentage. It is broken down into misconfigurations and app vulnerabilities
 - **impact**, the endpoint's security risk impact (Low, Medium, High)
 - **misconfigurations**, the percentage of misconfigurations in the endpoint's security risk score
 - **appVulnerabilities**, the percentage of app vulnerabilities in the endpoint's security risk score
 - **humanRisks**, the percentage of human risks in the endpoint's security risk score

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',
    'companyId': '5575a235d2172c65038b454e',
    '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,
  'networkAttackDefense': False
},
'policy': {
  'id': '5121da426803fa2d0e000017',
  'applied': True,
  'name': 'Default policy'
},
"label" : "endpoint label",
"moveState": 1,
"riskScore": {
  "value": "81%",
```

```
        "impact": "High",
        "misconfigurations": "70%",
        "appVulnerabilities": "11%",
        "humanRisks": "19%"
    }
}
}
```

2.4.3. createCustomGroup

This method creates a new custom group of endpoints.

Parameters

Parameter	Type	Optional	Description
groupName	String	No	The name for the new group
parentId	String	Yes	The ID of the parent container. If no parent ID is specified, the new group is created under the 'Computers and Groups' group.

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"
}
```

2.4.4. deleteCustomGroup

This method deletes a custom group.

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
}
```

2.4.5. getCustomGroupsList

This method retrieves the list of groups under a specified group.

Parameters

Parameter	Type	Optional	Description
parentId	String	Yes	The ID of the parent group for which the child groups will be listed. 'Computers and Groups' and 'Deleted' groups are returned if the passed parameter is null.

Return value

This method returns an Array containing the list of groups located under the specified parent. Each entry in the list has the following fields:

- id - the ID of the group
- name - the name of the group

Example

Request :

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

Response :

```
{
  "id": "8edf135b-f7cb-41f2-8b67-98054694f61e",
  "jsonrpc": "2.0",
  "result": [
    {
      "id" : "5582c385b1a43deb7f7b23c6",
      "name" : "myGroup1"
    },
    {
      "id" : "5582d3b3b1a43d897f7b23c8",
      "name" : "myGroup2"
    }
  ]
}
```

2.4.6. moveEndpoints

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

Parameters

Parameter	Type	Optional	Description
endpointIds	Array	No	The list of endpoints IDs
groupId	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  
}
```

2.4.7. 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.

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
}
```

2.4.8. moveCustomGroup

This method moves a custom group to another custom group.

Parameters

Parameter	Type	Optional	Description
groupId	String	No	The ID of the custom group to be moved
parentId	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
}
```

2.4.9. getNetworkInventoryItems

This method returns network inventory items.

Parameters

Parameter	Type	Optional	Description
parentId	String	Yes	The ID of the container for which the network items will be returned.
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 “Available Filters” (p. 58).
page	Number	Yes	The results page number. Default page number is 1.
perPage	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
type		<ul style="list-style-type: none"> • <code>groups</code> - a Boolean to filter all custom groups of endpoints. Default value: <code>False</code>. • <code>ec2Instances</code> - a Boolean to filter all Amazon EC2 Instances. Default value: <code>False</code>. • <code>computers</code> - a Boolean to filter all computers. Default value: <code>False</code>. • <code>virtualMachines</code> - a Boolean to filter all virtual machines. Default value: <code>False</code>.
security	management	<ul style="list-style-type: none"> • <code>managedWithBest</code> - a Boolean to filter all endpoints with the security agent installed on them. Default value: <code>False</code>. • <code>isContainerHost</code> - a Boolean to filter all endpoints with container host protection installed on them. Default value: <code>False</code>. This filter is available for <code>computers</code> and <code>virtualmachines</code> services. • <code>managedExchangeServers</code> - a Boolean to filter all protected Exchange servers. Default value: <code>False</code>. This filter requires a valid license key that covers the Security for Exchange security service. • <code>managedRelays</code> - a Boolean to filter all endpoints with Relay role. Default value: <code>False</code>.

Section	Subsection	Filtering Options
		<ul style="list-style-type: none"> ● <code>securityServers</code> - a Boolean to filter all Security Servers. Default value: <code>False</code>.
	<code>depth</code>	<ul style="list-style-type: none"> ● <code>allItemsRecursively</code> - a Boolean to filter all endpoints recursively within the Network Inventory of a company. Default value: <code>False</code>.
	<code>details</code>	<ul style="list-style-type: none"> ● <code>ssid</code> - string, the SSID (Active Directory SID of the endpoint) used to filter the endpoints regardless of their protection status. ● <code>macs</code> - array, the list of MAC addresses used to filter the endpoints regardless of their protection status. ● <code>name</code> - a String for filtering the items by name. Minimum required string length is three characters.



Important

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

The field `name` works with partial matching.

The filter returns the items whose names are exact match or start with the specified value. To use the specified value as a suffix, use the asterisk symbol (*).

For example:

If `name` is `computer`, the API returns all items whose names start with `computer`.

If `name` is `*puter`, then the API returns a list of all items that contain `puter` in their names.

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,
 - `companyId`, the ID of the parent company,
 - `type`, the type of network item: 4 - Group, 5 - Computer, 6 - Virtual Machine, 7 - EC2 Instance, 14 - Containers Group, 15 - Container Host Folder, 16 - Container.
 - `details`, more information about the item. This field is available for 1 - Companies, 5 - Computers, 6 - Virtual Machines, 7 - EC2 Instances and 16 - Containers. For information regarding the content of the details member please refer to [“The details member”](#) (p. 60).

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), 6 (virtual machine) and 7 (EC2 Instance)	<ul style="list-style-type: none"> ● <code>label</code>, the label set to the endpoint ● <code>fqdn</code>, the FQDN of the endpoint ● <code>groupId</code>, the group ID of the endpoint ● <code>isManaged</code>, boolean <code>True</code>, if this endpoint is managed ● <code>machineType</code>, the type of the machine: (1 - computer, 2 - virtual machine, 3 - EC2 Instance, 0 - Other) ● <code>operatingSystemVersion</code>, the OS version of the endpoint ● <code>ip</code>, the IP address of the endpoint ● <code>macs</code>, the list of MAC addresses of the endpoint ● <code>ssid</code>, the Active Directory SID of the endpoint ● <code>managedWithBest</code>, boolean <code>True</code>, if BEST is installed on this endpoint ● <code>isContainerHost</code>, boolean <code>True</code>, if this endpoint is a Container Host

Item type	Details
	<ul style="list-style-type: none">● <code>managedExchangeServer</code>, boolean True, if this endpoint is an Exchange Server● <code>managedRelay</code>, boolean True, if this endpoint has Relay role● <code>securityServer</code>, boolean True, if this endpoint is a Security Server● <code>policy</code> - an Object informing about the policy active on the endpoint. The object contains the following fields:<ul style="list-style-type: none">– <code>id</code>, a String uniquely identifying the active policy– <code>name</code>, the name of the policy– <code>applied</code>, a Boolean set to True if the policy is currently applied on the endpoint● <code>movingInfo</code> - an Object informing upon endpoint transfer from one company to another one. The object contains:<ul style="list-style-type: none">– <code>state</code>, the endpoint moving status (0 - in progress, 1 - moved)– <code>destinationCompanyName</code>, the name of the company where the endpoint was moved.

Example

Request :

```
{
  "params": {
    "parentId": "23b19c39b1a43d89367b32ce",
    "page": 2,
    "perPage": 1,
    "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,
    pagesCount: 11,
    perPage: 1,
    total: 11
    items[
      {
        "id" : "21a295eeb1a43d8b497b24b7",
        "name" : "Computer",
        "type" : 5,
        "parentId": "21a295eeb1a43d8b497b24b7",
        "companyId": "21a295eeb1a43d8b497b24b7",
        "details" : {
          "label" : "endpoint 2",
          "fqdn": "endpoint2.local",
          "groupId": "5a5f4d36b1a43d5f097b23bb",
          "isManaged": true,
          "machineType": 2,
          "operatingSystemVersion": "Windows Server",
          "ip": "60.40.10.220",
          "macs": [
            "324935237346"
          ],
          "ssid": ""
        }
      }
    ]
  }
}
```

```
}
```

2.4.10. createScanTask

This method creates a new scan task.

Parameters

Parameter	Type	Optional	Description
targetIds	Array	No	A list with the IDs of the targets to scan. The target ID can designate an endpoint or a container.
type	Number	No	The type of scan. Available options are: 1 - quick scan; 2 - full scan; 3 - memory scan; 4 - custom scan
name	String	Yes	The name of the task. If the parameter is not passed, the name will be automatically generated.
customScanSettings	Array	No	Object containing information such as scan depth and scan path(s). This object should be set only when <code>type</code> parameter has the value 4 - Custom scan. When set for other types, the values will be ignored. Parameter <code>\$customScanSettings</code> must contain the following properties: <code>int \$scanDepth</code> The scan profile. Available options: 1 - aggressive; 2 - normal; 3 - permissive <code>array \$scanPath</code> The list of target paths to be scanned

Return value

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

Example

Request :

```
{
  "params": {
    "targetIds": ["559bd17ab1a43d241b7b23c6",
                 "559bd17ab1a43d241b7b23c7"],
    "type": 4,
    "name": "my scan",
    "customScanSettings": {
      "scanDepth": 1,
      "scanPath": [
        "LocalDrives"
      ]
    }
  },
  "jsonrpc": "2.0",
  "method": "createScanTask",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

Response :

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

2.4.11. createReconfigureClientTask

This method creates a new Reconfigure Client task. With this task you can choose which modules to install on target agents.



Warning

The `networkMonitor` module is deprecated. It is recommended to use `networkAttackDefense` instead.

Parameters

Parameter	Type	Optional	Description
<code>targetIds</code>	Array	No	The endpoint or container IDs, for which you want to reconfigure the agents.
<code>scheduler</code>	Object	Yes	<p>The task scheduler settings.</p> <p>The object contains the following fields:</p> <ul style="list-style-type: none"> • <code>type</code>, an Integer with one of the following values: <ul style="list-style-type: none"> – 1 for immediate run (default) – 2 for scheduled <p>If <code>type</code> is 1, you can omit the other fields.</p> • <code>recurrence</code>, an Integer with one of the following values: <ul style="list-style-type: none"> – 1 for hourly. This value requires <code>everyHour</code> to be set. – 2 for daily. This value requires <code>startTime</code> to be set. – 3 for weekly. This value requires both <code>everyHour</code> and <code>startTime</code> to be set. • <code>everyHour</code>, an Integer between 1 and 23, representing the interval in hours between two task runs. • <code>startTime</code>, a string with the following format: <code>HH:mm</code>, representing the hour of the first task run. • <code>onWeekDay</code>, an Integer between 1 and 7, where 1 is Monday and 7 is Sunday. <p>If this parameter is omitted, the task runs immediately.</p>
<code>modules</code>	Object	Yes	<p>The modules to be enabled or disabled.</p> <p>The object contains the following fields:</p> <ul style="list-style-type: none"> • <code>antimalware</code>



Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> advancedThreatControl firewall contentControl deviceControl powerUser encryption advancedAntiExploit containerProtection edrSensor patchManagement networkAttackDefense <p>Each field may have the value 1 for enabled, or 0 for disabled.</p> <p>If the module is omitted, it is considered disabled.</p>
scanMode	Object	Yes	<p>The settings for the scanning engines.</p> <p>The object contains the following fields:</p> <ul style="list-style-type: none"> type, an Integer with one of the following values: <ul style="list-style-type: none"> 1 for automatic configuration (default) 2 for custom settings. This value requires the computers and vms fields <p>If omitted, the default values will be used.</p> <ul style="list-style-type: none"> vms, an Object described below. computers, an Object described below. <p>The objects computers and vms have the following fields:</p> <ul style="list-style-type: none"> main, an Integer with one of the following values: <ul style="list-style-type: none"> 1 for Central Scanning (with Security Server)



Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> - 2 for Hybrid Scanning (light engines) - 3 for Local Scanning (full engines) • <code>fallback</code>, an Integer with one of the following values: <ul style="list-style-type: none"> - 2 for Hybrid Scanning (light engines) - 3 for Local Scanning (full engines) <p>If <code>main</code> has the value 2 or 3, then <code>fallback</code> is not considered.</p>
<code>roles</code>	Object	Yes	<p>The roles to be enabled or disabled on the agent:</p> <ul style="list-style-type: none"> • <code>relay</code> with the following possible values: <ul style="list-style-type: none"> - 1 for enabled - 0 for disabled (default) • <code>exchange</code> with the following possible values: <ul style="list-style-type: none"> - 1 for enabled - 0 for disabled (default) <p>This role is available only with a valid Security for Exchange license.</p>
<code>productType</code>	Number	Yes	<p>This parameter determines the operation mode of the security agent. Possible values:</p> <ul style="list-style-type: none"> • 0 - for Detection and prevention mode, default for full endpoint security agents. • 3 - for EDR (Report only) mode, default for Bitdefender EDR agents. <p>For additional information, refer to “Parameter Info” (p. 67).</p>

Parameter Info

- Bitdefender EDR users can only run tasks that reconfigure target security agents to operate in EDR (Report only) mode; specifying `productType` is optional.

- GravityZone BS / ABS / Elite users can only run tasks that reconfigure target security agents to operate in Detection and prevention mode; specifying `productType` is optional.
- GravityZone Ultra / Ultra Plus users can reconfigure target security agents to operate in both operation modes.
 - `productType` must be specified for EDR (Report only) mode reconfiguration.
 - In case of selecting endpoints running different operation modes, if `productType` is not specified, the EDR (Report only) endpoints will be reconfigured to run in Detection and prevention mode.
- The EDR (Report only) mode includes by default a set of predefined parameters that will overwrite user-specified options. Predefined parameters:
 - `modules`
 - `edrSensor` - true
 - `contentControl` - true
 - `networkAttackDefense` - true
 - `advancedThreatControl` - true
 - `other modules` - false
 - `scanMode` - n/a
 - `roles.exchange` - false

Return value

This method returns a Boolean which is True if the reconfigure task was created successfully for at least one target ID.

Example

Request :

```
{
  "params": {
    "targetIds": [
      "5d7244b10ea1de153817c072"
    ],
    "scheduler": {
      "type": 1
    },
    "modules": {
```



```
    "advancedThreatControl": 1,
    "firewall": 1,
    "contentControl": 1,
    "deviceControl": 1,
    "powerUser": 1,
    "encryption": 1,
    "advancedAntiExploit": 1,
    "containerProtection": 1,
    "edrSensor": 1,
    "patchManagement": 1,
    "networkAttackDefense": 1
  },
  "scanMode": {
    "type": 1
  },
  "roles": {
    "relay": 0,
    "exchange": 0
  },
  "productType": 0
},
"jsonrpc": "2.0",
"method": "createReconfigureClientTask",
"id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

Response :

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

2.4.12. getScanTasksList

This method returns the list of scan tasks.

Parameters

Parameter	Type	Optional	Description
name	String	Yes	The name of the task. Filter the list of tasks by task name. 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.
status	Number	Yes	The status of the task. Available options are: 1 - Pending; 2 - In progress; 3 - Finished.
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 tasks. 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 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'
      }
    ]
  }
}
```

2.4.13. 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 which is 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
}
```

2.4.14. createScanTaskByMac

Use this method to generate a scan task for managed endpoints identified by their MAC address.

Parameters

Parameter	Type	Optional	Description
macAddresses	Array	No	The list of mac addresses of the endpoints to be scanned. You can specify at most 100 MAC addresses at once
type	Number	No	The type of scan. Available options: 1 - quick scan; 2 - full scan; 3 - memory scan; 4 - custom scan
name	String	Yes	The name of the task. If the parameter is not passed, the name will be generated automatically.
customScanSettings	Array	No	Object containing information such as scan depth and scan path(s). This object should be set only when <code>type</code> parameter has the value 4 - Custom scan. When set for other types, the values will be ignored. Parameter <code>\$customScanSettings</code> must contain the following properties: <code>int \$scanDepth</code> The scan profile. Available options: 1 - aggressive; 2 - normal; 3 - permissive <code>array \$scanPath</code> The list of target paths to be scanned

Return value

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

Example

Request :

```
{
  "params": {
    "macAddresses": [
      "1c67da49e1a1",
      "8c67f849e1a8"
    ],
    "type": 4,
    "name": "my scan",
    "customScanSettings": {
      "scanDepth": 1,
      "scanPath": [
        "LocalDrives"
      ]
    }
  },
  "jsonrpc": "2.0",
  "method": "createScanTaskByMac",
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f"
}
```

Response :

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

2.5. Packages

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

- [getInstallationLinks](#) : returns the installation links and full kits for a package.

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

API url: CONTROL_CENTER_APIS_ACCESS_URL/v1.0/jsonrpc/packages

2.5.1. `getInstallationLinks`

This method returns the installation links and full kits for a package.

Parameters

Parameter	Type	Optional	Description
<code>packageName</code>	String	Yes	The name of the package. If no value is passed, all packages will be returned.

Return value

This method returns an Array containing the list of installation links for the requested package, or for all available packages if none specified explicitly. Each entry in the list has the following fields:

- `packageName` - the name of the package for which you need the installation links and kits
- `companyName` - the name of the company to which the package belongs
- `companyId` - the ID of the above-mentioned company
- `installLinkWindows` - the installation link for Windows operating systems
- `installLinkMac` - the installation link for macOS operating systems
- `installLinkLinux` - the installation link for Linux operating systems
- `fullKitWindowsX32` - the full kit for Windows x32 operating systems
- `fullKitWindowsX64` - the full kit for Windows x64 operating systems
- `fullKitLinuxX32` - the full kit for Linux x32 operating systems

- fullKitLinuxX64 - the full kit for Linux x64 operating systems

Example

Request :

```
{
  "params": {
    "packageName": "my package"
  },
  "jsonrpc": "2.0",
  "method": "getInstallationLinks",
  "id": "426db9bb-e92a-4824-a21b-bba6b62d0a18"
}
```

Response :

```
{
  "id": "426db9bb-e92a-4824-a21b-bba6b62d0a18",
  "jsonrpc": "2.0",
  "result": [{
    "packageName": "Pack1",
    "companyName": "TestC2",
    "companyId": "54a1a1d3b1a43d2b347b23c1",
    "installLinkWindows":
      "https://gravityzone.bitdefender.com \
      /Packages/BSTWIN/0/setupdownloader_[qwer=].exe",
    "installLinkMac":
      "https://gravityzone.bitdefender.com \
      /Packages/MAC/0/antivirus_for_mac_[qwer].pkg",
    "installLinkLinux":
      "https://gravityzone.bitdefender.com \
      /Packages/BSTNIX/0/0E_rWP/installer",
    "fullKitWindowsX32":
      "https://gravityzone.bitdefender.com/api/v1.0/http/downloadPack\
      ageFullKit?packageId=5f1ecd1be4be6142c3e9b32&downloadType=19",
    "fullKitWindowsX64":
      "https://gravityzone.bitdefender.com/api/v1.0/http/downloadPack\
      ageFullKit?packageId=5f1ecd1be4be6142c3e9b32&downloadType=20",
```



```
    "fullKitLinuxX32":
      "https://gravityzone.bitdefender.com/api/v1.0/http/downloadPack\
ageFullKit?packageId=5f1ecde1be4be6142c3e9b32&downloadType=21",
    "fullKitLinuxX64": \
      "https://gravityzone.bitdefender.com/api/v1.0/http/downloadPack\
ageFullKit?packageId=5f1ecde1be4be6142c3e9b32&downloadType=22"
  }
}
```

Request :

Download the full kit package using curl:

```
curl -fOJ -H "YOUR_API_KEY:" \
https://gravityzone.bitdefender.com/api/v1.0/http/\
downloadPackageFullKit?packageId=5645cba6f12a9a8c5e8b4748&\
downloadType=20
```

Equivalent with:

```
curl -fOJ -H "Authorization: Basic API_KEY_ENCODED_BASE64" \
https://gravityzone.bitdefender.com/api/v1.0/http/\
downloadPackageFullKit?packageId=5f1ecde1be4be6142c3e9b32&\
downloadType=20
```

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

2.5.2. createPackage

This method creates an installation package.



Warning

The `atc` module is deprecated. It is recommended to use `advancedThreatControl` instead.



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	<p>An object with the modules to be enabled/disabled. The keys can be:</p> <ul style="list-style-type: none"> • advancedThreatControl, • firewall, • contentControl, • deviceControl, • powerUser, • containerProtection, • advancedAntiExploit, • encryption, • patchManagement, • edrSensor, • networkAttackDefense. <p>The values can be 1 (enabled) or 0 (disabled). If the module is not sent, it will be considered disabled. For EDR (Report only), the modules parameter must have the default configuration: edrSensor, contentControl, networkAttackDefense and</p>



Parameter	Type	Optional	Description
			advancedThreatControl are set to 1 (enabled). All other modules are set to 0. For Detection and prevention, all modules have the default value 0.
scanMode	Object	Yes	<p>An object with the scan mode settings.</p> <p>Object description:</p> <ul style="list-style-type: none"> • The accepted keys are: <code>type</code>, <code>vms</code>, <code>computers</code>, and <code>ec2</code> if the AWS integration is set up. The <code>type</code> value can be 1 (automatic) or 2 (for custom mode). • If <code>type</code> value is 2, then the <code>computers</code>, <code>vms</code> and <code>ec2</code> keys and values need to be sent, otherwise the default values will be filled by the system. The value for <code>computers</code>, <code>vms</code> and <code>ec2</code> is an object with the possible keys: <code>main</code> and <code>fallback</code>. • 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)). • 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. • The <code>main</code> option for <code>ec2</code> can be only 1 (for Central Scanning (Security Server)).



Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> If this parameter is not sent, the values for automatic mode are saved.
settings	Object	Yes	<p>An object with other settings of the package. The values can be:</p> <ul style="list-style-type: none"> scanBeforeInstall, removeCompetitors, uninstallPassword, customInstallationPath, customGroupId. <p>The value for <code>scanBeforeInstall</code> can be 1 (enabled) or 0 (disabled). The value for <code>removeCompetitors</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 case, one lower case and one special character; and <code>customInstallationPath</code> should be a valid Windows path where the package will be installed (this will work only for Windows operating systems). <code>customGroupId</code> should be a string representing the ID of the custom group entity where the new endpoint should be deployed. All values are optional. For EDR (Report only), the settings parameter must have the default configuration: <code>removeCompetitors</code> and</p>



Parameter	Type	Optional	Description
			scanBeforeInstall are set to 0 (disabled).
roles	Object	Yes	<p>An object containing the roles to be enabled or disabled:</p> <ul style="list-style-type: none"> • <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. • <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 if the company's license covers the Security for Exchange security service as well.
deploymentOptions	Object	Yes	<p>An object containing installation options:</p> <ul style="list-style-type: none"> • <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: 1 for regular deploy from the Bitdefender Update Server; 2 for deployments through a Relay. • <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. • <code>useCommunicationProxy</code>, a boolean allowing you to specify if



Parameter	Type	Optional	Description
			<p>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.</p> <ul style="list-style-type: none"> ● <code>proxyServer</code>, 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 required when <code>useCommunicationProxy</code> is set to <code>True</code>. ● <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>. ● <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. ● <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.



Parameter	Type	Optional	Description
<code>productType</code>	Number	Yes	<p>This parameter determines the operation mode of the security agent. Possible values:</p> <ul style="list-style-type: none"> ● 0 - for Detection and prevention mode, default for full endpoint security agents. ● 3 - for EDR (Report only) mode, default for Bitdefender EDR agents. <p>For additional information, refer to “Parameter Info” (p. 83).</p>

Parameter Info

- Bitdefender EDR users can only create EDR (Report only) packages; specifying `productType` is optional.
- GravityZone BS / ABS / Elite users can only create Detection and prevention packages; specifying `productType` is optional.
- GravityZone Ultra / Ultra Plus users can create both EDR (Report only) and Detection and prevention packages; `productType` must be specified to create an EDR (Report only) package.
- The EDR (Report only) package includes by default a set of predefined parameters that will overwrite user-specified options. Predefined parameters:
 - `modules`
 - `edrSensor` - true
 - `contentControl` - true
 - `networkAttackDefense` - true
 - `advancedThreatControl` - true
 - other modules - false
 - `scanMode` - n/a
 - `settings.removeCompetitors` - false
 - `settings.scanBeforeInstall` - false
 - `roles.exchange` - false

Return value

This method returns an Object 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",
    "description": "package description",
    "language": "en_EN",
    "modules": {
      "advancedThreatControl": 1,
      "firewall": 0,
      "contentControl": 1,
      "deviceControl": 0,
      "powerUser": 0,
      "containerProtection": 0,
      "advancedAntiExploit": 0,
      "encryption": 0,
      "patchManagement": 0,
      "edrSensor": 0,
      "networkAttackDefense": 0
    },
    "scanMode": {
      "type": 2,
      "computers": {
        "main": 1,
        "fallback": 2
      },
      "vms": {
        "main": 2
      },
      "ec2": {
        "main": 1,
        "fallback": 2
      }
    },
    "settings": {
```



```
    "uninstallPassword": "mys3cre3tP@assword",
    "scanBeforeInstall": 0,
    "removeCompetitors": 1,
    "customInstallationPath": "c:\\mypath\\bitdefender",
    "customGroupId": "5a4dff50b1a43ded0a7b23c8"
  },
  "roles": {
    "relay": 0,
    "exchange": 1
  },
  "deploymentOptions": {
    "type": 2,
    "relayId": "54a1a1s3b1a43e2b347s23c1",
    "useCommunicationProxy": true,
    "proxyServer": "10.12.13.14",
    "proxyPort": 123
  },
  "productType": 0
},
"jsonrpc": "2.0",
"method": "createPackage",
"id": "426db9bb-e92a-4824-a21b-bba6b62d0a18"
}
```

Response :

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

2.5.3. getPackagesList

Returns the list of available packages.

Parameters

Parameter	Type	Optional	Description
page	Number	Yes	The page number of results. 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 An object with information about the packages. The response 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. It can be 3 for SVA, 4 for Bitdefender Endpoint Security Tools.

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
      }
    ]
  }
}
```

2.5.4. 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
}
```

2.5.5. getPackageDetails

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



Warning

The `atc` module is deprecated and it will be removed from API in the near future.

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 language and country international codes.
- `modules` - indicating the status of the modules present in the package. The object may contain the following members: `antimalware`, `advancedThreatControl` and `atc`, `firewall`, `contentControl`, `deviceControl`, `powerUser`, `containerProtection`, `advancedAntiExploit`, `encryption`, `patchManagement`, `edrSensor`, `networkAttackDefense`. The value for each module is either 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`,
 - `removeCompetitors`,
 - `customInstallationPath`,
 - `customGroupId`.

- `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.
 - `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.
- `productType` - the assigned product type. This field determines the operation mode of the security agent. Possible values:
 - 0, for Detection and prevention
 - 3, for EDR (Report only)

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,
      "advancedThreatControl": 1,
      "atc": 1,
      "firewall": 0,
      "contentControl": 1,
      "deviceControl": 0,
      "powerUser": 0,
      "containerProtection": 0,
      "advancedAntiExploit": 0,
      "encryption": 0,
      "patchManagement": 0,
      "edrSensor": 0,
      "networkAttackDefense": 0
    },
    "roles": {
      "relay": 1,
      "exchange": 0
    },
    "scanMode": {
      "type": 2,
      "computers": {
        "main": 1,
        "fallback": 2
      }
    }
  }
}
```

```
    },
    "vms": {
        "main": 2
    }
},
"settings": {
    "scanBeforeInstall": false,
    "removeCompetitors": true,
    "customInstallationPath": "c:\\mypath\\bitdefender",
    "customGroupId": "5a4dff50b1a43ded0a7b23c8",
},
"deploymentOptions": {
    "type": 1,
    "useCommunicationProxy": true,
    "proxyServer": "10.12.13.14",
    "proxyPort": 123,
    "proxyUsername": "user"
},
"productType": 0
}
}
```

2.6. 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: [CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/policies](#)

2.6.1. getPoliciesList

This method retrieves the list of available policies.

Parameters

Parameter	Type	Optional	Description
page	Number	Yes	The page of results. 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 a list of policy objects. The result 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 policies. Each entry in the list has the following fields:
 - `id`, the ID of the policy,
 - `name`, the name of the policy,
 - `companyId`, the ID of the company which owns the policy,
 - `companyName`, the name of the company which owns 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",
        "companyId" : "55896b87b7894d0f367b23c6",
        "companyName" : "Company Test"
      },
      {
        "id" : "23a295d8b1a43d7c4a7b23c9",
        "name" : "Policy 2",
        "companyId" : "55896b87b7894d0f367b23c6",
        "companyName" : "Company Test"
      }
    ]
  }
}
```

2.6.2. getPolicyDetails

This method retrieves all information related to a security policy.

Parameters

Parameter	Type	Optional	Description
policyId	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 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": {
      ...
    }
  }
}
```

```
}  
}  
}
```

2.7. Integrations

The Integrations API includes several methods allowing the third party integration management:

- `getHourlyUsageForAmazonEC2Instances` : exposes the hourly usage for each Amazon instance category (micro, medium etc.).
- `configureAmazonEC2IntegrationUsingCrossAccountRole` : configures the Amazon EC2 integration using the provided Amazon Resource Name of a valid AWS Cross-Account Role.
- `generateAmazonEC2ExternalIdForCrossAccountRole` : generates the External ID required to configure the AWS Cross-Account Role.
- `getAmazonEC2ExternalIdForCrossAccountRole` : returns the External ID required to configure the AWS Cross-Account Role.
- `disableAmazonEC2Integration` : disables the previously configured Amazon EC2 integration.

API url: [CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/integrations](#)

2.7.1. `getHourlyUsageForAmazonEC2Instances`

This method exposes the hourly usage for each Amazon instance category (micro, medium etc.).

Parameters

Parameter	Type	Optional	Description
<code>targetMonth</code>	String	Yes	The month for which the usage is returned. The month will be provided in the following format: mm/yyyy. The default value is the current month.

Return value

This method returns an Object containing the hourly usage for each instance category.

Example

Request :

```
{
  "params": {
    "targetMonth": "03/2015"
  },
  "jsonrpc": "2.0",
  "method": "getHourlyUsageForAmazonEC2Instances",
  "id": "5087eab8-b74f-4a3e-85b3-4271e85890d4"
}
```

Response :

```
{
  "id": "5087eab8-b74f-4a3e-85b3-4271e85890d4",
  "jsonrpc": "2.0",
  "result": {
    "micro": 11,
    "medium": 157
  }
}
```

2.7.2. configureAmazonEC2IntegrationUsingCrossAccountRole

This method configures the Amazon EC2 integration using the provided Amazon Resource Name of a valid AWS Cross-Account Role.

For details regarding the integration steps, refer to [this KB article](#).

Parameters

Parameter	Type	Optional	Description
crossAccountRoleArn	String	No	The Amazon Resource Name of a valid AWS Cross-Account Role

Return value

This method does not return any value.

Example

Request :

```
{
  "params": {
    "crossAccountRoleArn" :
      "arn:aws:iam::111222345123:role/test"
  },
  "jsonrpc": "2.0",
  "method":
    "configureAmazonEC2IntegrationUsingCrossAccountRole",
  "id": "5c6df60c-786a-4ea3-8ff3-b6e52b42aa46"
}
```

Response :

```
{
  "id": "5c6df60c-786a-4ea3-8ff3-b6e52b42aa46",
  "jsonrpc": "2.0",
  "result": null
}
```

2.7.3. generateAmazonEC2ExternalIdForCrossAccountRole

This method generates the External ID required to configure the AWS Cross-Account Role.

The Cross-Account Role will be used to configure the Amazon EC2 Integration.



Important

Use this method only when you need to generate a new External ID. Generating a new External ID will invalidate the existing integration. For retrieving the External ID use the `getAmazonEC2ExternalIdForCrossAccountRole` API method.

Parameters

No input parameters are required.

Return value

This method returns a String: the External ID.

Example

Request :

```
{
  "params": {
  },
  "jsonrpc": "2.0",
  "method": "generateAmazonEC2ExternalIdForCrossAccountRole",
  "id": "5c6df60c-786a-4ea3-8ff3-b6e52b42aa46"
}
```

Response :

```
{
  "id": "5c6df60c-786a-4ea3-8ff3-b6e52b42aa46",
  "jsonrpc": "2.0",
  "result": "5e93f474a30a2db85dd6046d6d5fg188"
}
```

2.7.4. `getAmazonEC2ExternalIdForCrossAccountRole`

This method returns the External ID required to configure the AWS Cross-Account Role.

Parameters

No input parameters are required.

Return value

This method returns a String: the External ID. If no External ID was generated, this method will return null.

Example

Request :

```
{
  "params": {
  },
  "jsonrpc": "2.0",
  "method": "getAmazonEC2ExternalIdForCrossAccountRole",
  "id": "5c6df60c-786a-4ea3-8ff3-b6e52b42aa46"
}
```

Response :

```
{
  "id": "5c6df60c-786a-4ea3-8ff3-b6e52b42aa46",
  "jsonrpc": "2.0",
  "result": "5e93f474a30a2db85dd6046d6d5fg188"
}
```

2.7.5. disableAmazonEC2Integration

This method disables the previously configured Amazon EC2 integration.

Parameters

No input parameters are required.

Return value

This method does not return any value.

Example

Request :

```
{
  "params": {
  },
  "jsonrpc": "2.0",
  "method": "disableAmazonEC2Integration",
  "id": "97114e95-f36b-4206-bca0-6fb41bb47575"
}
```

Response :

```
{
  "id": "97114e95-f36b-4206-bca0-6fb41bb47575",
  "jsonrpc": "2.0",
  "result": null
}
```

2.8. 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 scheduled 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: [CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/reports](#)

2.8.1. 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.

Parameters

Parameter	Type	Optional	Description
name	String	No	The name of the report.
type	Number	No	The type of report. One of the following values can be passed: <ul style="list-style-type: none"> ● 1 - Antiphishing Activity ● 2 - Blocked Applications ● 3 - Blocked Websites ● 5 - Data Protection ● 6 - Device Control Activity ● 7 - Endpoint Modules Status ● 8 - Endpoint Protection Status ● 9 - Firewall Activity ● 12 - Malware Status ● 13 - Monthly License Usage ● 14 - Network Status ● 15 - On demand scanning ● 16 - Policy Compliance ● 17 - Security Audit ● 18 - Security Server Status ● 19 - Top 10 Detected Malware ● 21 - Top 10 Infected Endpoints ● 22 - Update Status ● 23 - Upgrade Status



Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> ● 24 - AWS Monthly Usage ● 29 - Email Security Usage ● 30 - Endpoint Encryption Status ● 31 - HyperDetect Activity ● 32 - Network Patch Status ● 33 - Sandbox Analyzer Failed Submissions ● 34 - Network Incidents
targetIds	Array	No	<p>A list with the IDs of the targets for which to create the report. The targets depend on the report type.</p> <p>For these reports, the target must not be set:</p> <ul style="list-style-type: none"> ● Monthly License Usage ● AWS Monthly Usage <p>For the other report types, the target ID can be of any type: group, containers, endpoints.</p>
scheduledInfo	Object	Yes	<p>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 scheduledInfo object.</p>
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"> ● Endpoint Modules Status ● Policy Compliance ● Security Server Status ● Upgrade Status



Parameter	Type	Optional	Description
			For more information, please check the details of the options object.
emailsList	Array	Yes	A list of emails where to deliver the report. emailsList 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
occurrence	integer	<p>The member is mandatory.</p> <p>Possible values:</p> <ul style="list-style-type: none"> - 1 - for an instant report - 2 - for hourly report - 3 - for daily report - 4 - for weekly report - 5 - for monthly report - 6 - for yearly report <p>For 13 - Monthly License Usage, 24 - AWS Monthly Usage and 29 - Email Security Usage reports the possible values are only 4 - weekly report and 5 - monthly report.</p>
interval	integer	<p>The member should be set only if <code>occurrence</code> has the value 2.</p> <p>Possible values:</p>

Name	Type	Description
		<ul style="list-style-type: none">Any integer between 1 and 24, representing the interval (in hours) at which the report will run.
startHour	integer	The member should be set only if <code>occurrence</code> has the value 3, 4 or 5. Possible values: <ul style="list-style-type: none">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. Possible values: <ul style="list-style-type: none">Any integer between 0 and 59.
days	array	The member should be set only if <code>occurrence</code> has the value 4. Possible values of the array elements: <ul style="list-style-type: none">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. Possible values: <ul style="list-style-type: none">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. Possible values: <ul style="list-style-type: none">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
<code>reportingInterval</code>	integer	The member is mandatory. This value depends on the report occurrence. For more information, refer to Relation between reporting interval and recurrence
<code>filterType</code>	integer	The member is mandatory. Possible values: <ul style="list-style-type: none">– 0 - All endpoints– 1 - Only endpoints with blocked websites

- **Blocked Applications**

The object must contain these members:

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

- **Blocked Websites**

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 Relation between reporting interval and recurrence
filterType	integer	The member is mandatory. Possible values: – 0 - All endpoints – 1 - Only endpoints with blocked websites

- **Data Protection**

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 Relation between reporting interval and recurrence
filterType	integer	The member is mandatory. Possible values: – 0 - All endpoints – 1 - Only managed computers with blocked threats
blockedEmails	boolean	The member should be set only if filterType has the value 1. Possible values: – True – False
blockedWebsites	boolean	The member should be set only if filterType has the value 1.



Name	Type	Description
		Possible values: - True - False

● **Device Control Activity**

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 Relation between reporting interval and recurrence

● **Endpoint Protection Status**

The object must contain these members:

Name	Type	Description
filterType	integer	The member is mandatory. Possible values: - 0 - All endpoints - 1 - Only endpoints filtered by the members described hereinafter.
antivirusOn	boolean	The member should be set only if filterType has the value 1. Possible values: - True, to include in the report endpoints with antimalware protection enabled. - False, to exclude from the report endpoints with antimalware protection enabled.

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

● **Firewall Activity**

The object must contain these members:

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



Name	Type	Description
		<ul style="list-style-type: none"> - True, to include in the report endpoints with blocked traffic attempts. - False, to exclude from the report endpoints with blocked traffic attempts.
portScans	boolean	<p>This member should be set only if filterType has the value 1.</p> <p>Possible values:</p> <ul style="list-style-type: none"> - True, to include in the report endpoints with blocked port scans. - False, to exclude from the report endpoints with blocked port scans.

● **Malware Status**

The object must contain these members:

Name	Type	Description
reportingInterval	integer	<p>The member is mandatory.</p> <p>This value depends on the report occurrence. For more information, refer to Relation between reporting interval and recurrence</p>
filterType	integer	<p>The member is mandatory.</p> <p>Possible values:</p> <ul style="list-style-type: none"> - 0 - All endpoints - 1 - Only endpoints still infected
detailedExport	array	<p>The member is optional.</p> <p>Possible values:</p> <ul style="list-style-type: none"> - 1 - Include Endpoint Malware Status in PDF file

- **Monthly License Usage**

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 Relation between reporting interval and recurrence
skipSummary	boolean	The member is optional. An option defining if the CSV file of the Monthly License Usage report (<code>type = 13</code>) should include the Summary section. By default, the parameter is set to <code>False</code> , meaning the CSV file includes the Summary.

- **AWS Monthly Usage**

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 Relation between reporting interval and recurrence

- **Network Status**

The object must contain these members:

Name	Type	Description
filterType	integer	The member is mandatory. Possible values: – 0 - All endpoints



Name	Type	Description
		<ul style="list-style-type: none"> - 1 - Only endpoints with issues - 2 - Only endpoints with unknown status

- **On demand scanning**

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 Relation between reporting interval and recurrence

- **Security Audit**

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 Relation between reporting interval and recurrence

- **Top 10 Detected Malware**

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 Relation between reporting interval and recurrence

- **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 Relation between reporting interval and recurrence

- **Update Status**

The object must contain these members:

Name	Type	Description
updated	boolean	Possible values: <ul style="list-style-type: none">– True, to include in the report updated endpoints.– False, to exclude from the report updated endpoints.
disabled	boolean	Possible values: <ul style="list-style-type: none">– True, to include in the report endpoints with update disabled.– False, to exclude from the report endpoints with update disabled.
outdated	boolean	Possible values: <ul style="list-style-type: none">– True, to include in the report outdated endpoints.– False, to exclude from the report outdated endpoints.
pendingRestart	boolean	Possible values: <ul style="list-style-type: none">– True, to include in the report endpoints that need to be restarted.



Name	Type	Description
		– False, to exclude from the report endpoints that need to be restarted.

● **VM Network Protection Status**

The object must contain these members:

Name	Type	Description
<code>filterType</code>	integer	The member is mandatory. Possible values: – 0 - All endpoints – 1 - Only protected endpoints

● **Email Security Usage**

The object must contain these members:

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

● **HyperDetect Activity**

The object must contain these members:

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



- **Network Patch Status**

The object must contain these members:

Name	Type	Description
filterType	integer	The member is mandatory. Possible values: <ul style="list-style-type: none"> – 0 - All available patches – 1 - Only patches visible in Patch Inventory

- **Sandbox Analyzer Failed Submissions**

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 Relation between reporting interval and recurrence

- **Network Incidents**

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 Relation between reporting interval and recurrence



Important

The object should not be set for these reports:

- **Endpoint Modules Status**
- **License Status**



- Upgrade Status
- Policy Compliance
- Security Server Status
- Endpoint Encryption Status

Relation between reporting interval and recurrence

occurrence	reportingInterval
2 - Hourly report	Possible values: – 0 - Today
3 - Daily report	Possible values: – 0 - Today – 1 - Last day – 2 - This Week
4 - Weekly report	Possible values: – 0 - Today – 1 - Last day – 2 - This Week – 3 - Last Week – 4 - This Month For 13 - Monthly License Usage, 24 - AWS Monthly Usage and 29 - Email Security Usage reports the possible value is only 4 - This Month.
5 - Monthly report	Possible values: – 0 - Today – 1 - Last day – 2 - This week – 3 - Last week

occurrence	reportingInterval
	<ul style="list-style-type: none">- 4 - This month- 5 - Last month- 6 - Last 2 months- 7 - Last 3 months- 8 - This year <p>For 13 - Monthly License Usage, 24 - AWS Monthly Usage and 29 - Email Security Usage reports the possible values are only 4 - This month, 5 - Last month and 8 - This year.</p>
6 - Yearly report	<p>Possible values:</p> <ul style="list-style-type: none">- 8 - This year- 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"  
}
```

2.8.2. getReportsList

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

Parameters

Parameter	Type	Optional	Description
name	String	Yes	The name of the report.
type	Number	Yes	The report type. The available types are: <ul style="list-style-type: none">● 1 - Antiphishing Activity● 2 - Blocked Applications● 3 - Blocked Websites● 5 - Data Protection● 6 - Device Control Activity● 7 - Endpoint Modules Status● 8 - Endpoint Protection Status● 9 - Firewall Activity● 12 - Malware Status● 13 - Monthly License Usage● 14 - Network Status● 15 - On demand scanning● 16 - Policy Compliance● 17 - Security Audit● 18 - Security Server Status● 19 - Top 10 Detected Malware



Parameter	Type	Optional	Description
			<ul style="list-style-type: none"> ● 21 - Top 10 Infected Endpoints ● 22 - Update Status ● 23 - Upgrade Status ● 24 - AWS Monthly Usage ● 30 - Endpoint Encryption Status ● 31 - HyperDetect Activity ● 32 - Network Patch Status ● 33 - Sandbox Analyzer Failed Submissions ● 34 - Network Incidents ● 29 - Email Security Usage
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
  }
}
```

2.8.3. 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 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 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://gravityzone.bitdefender.com/api/
v1.0/http/downloadReportZip?reportId=
5645cba6f12a9a8c5e8b4748&
allInstances=1&serviceType=1",
    "lastInstanceUrl":
      "https://gravityzone.bitdefender.com/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://gravityzone.bitdefender.com/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.

2.8.4. 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 which is 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
}
```

2.9. Push

The Event Push Service API includes several methods allowing the management of real time sent notifications.

- [setPushEventSettings](#) : configures which notifications should be pushed to the web service.
- [getPushEventSettings](#) : displays which events are sent to the web service.
- [sendTestPushEvent](#) : sends test event.
- [getPushEventStats](#) : displays various push event statistics and errors.
- [resetPushEventStats](#) : resets the push event statistics and errors.

API url: [CONTROL_CENTER_APIS_ACCESS_URL/v1.0/jsonrpc/push](#)

2.9.1. setPushEventSettings

This method sets the push event settings.



Important

Event Push Service requires the HTTP collector running on the third-party platforms to support SSL with TLS 1.2 or higher, to send events successfully.

Parameters

Parameter	Type	Optional	Description
status	Number	No	0 - disabled, 1 - enabled
serviceType	String	No	Type of the web service. Valid values: jsonRPC, splunk and cef



Parameter	Type	Optional	Description
serviceSettings	Array	No	Specific settings for each service type. For information regarding the service settings, refer to “Service Type Settings” (p. 128)
subscribeToEventTypes	Array	No	List of event types to be sent to the web service

Service Type Settings

Service Type	Service Settings
jsonRPC	<ul style="list-style-type: none"> • <code>url</code> - a String representing the Web service URL • <code>requireValidSslCertificate</code> - a Boolean to validate the SSL certificate of the web service: <code>True</code> to perform the validation, <code>False</code> otherwise • <code>authorization</code> - a String representing the authorization header
splunk	<ul style="list-style-type: none"> • <code>url</code> - a String representing the Web service URL • <code>requireValidSslCertificate</code> - a Boolean to validate the SSL certificate of the web service: <code>True</code> to perform the validation, <code>False</code> otherwise • <code>splunkAuthorization</code> - a String representing the Splunk authorization header
cef	<ul style="list-style-type: none"> • <code>url</code> - a String representing the Web service URL • <code>requireValidSslCertificate</code> - a Boolean to validate the SSL certificate of the web service: <code>True</code> to perform the validation, <code>False</code> otherwise • <code>authorization</code> - a String representing the CEF basic authorization header

Return value

This method returns a Boolean which is True when the settings were saved successfully.

Example

Request :

```
{
  "params": {
    "status": 1,
    "serviceType": "jsonRPC",
    "serviceSettings": {
      "url": "http://example.com",
      "authorization": "Bearer sfasdfw34243",
      "requireValidSslCertificate": true
    },
    "subscribeToEventTypes": {
      "modules": true,
      "sva": true,
      "registration": true,
      "supa-update-status": true,
      "av": true,
      "aph": true,
      "fw": true,
      "avc": true,
      "uc": true,
      "dp": true,
      "sva-load": true,
      "task-status": true,
      "exchange-malware": true,
      "network-sandboxing": true,
      "adcloud": true,
      "exchange-user-credentials": true,
      "endpoint-moved-out": true,
      "endpoint-moved-in": true,
      "troubleshooting-activity": true,
      "uninstall": true,
      "install": true,
      "hwid-change": true,
      "new-incident": true,
    }
  }
}
```

```
        "antiexploit": true,  
        "network-monitor": true,  
        "ransomware-mitigation": true  
    }  
},  
"jsonrpc": "2.0",  
"method": "setPushEventSettings",  
"id": "ad12cb61-52b3-4209-a87a-93a8530d91cb"  
}
```

Response :

```
{  
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb",  
  "jsonrpc": "2.0",  
  "result": true  
}
```

2.9.2. getPushEventSettings

This method gets the push event settings.

Parameters

No input parameters are required.

Return value

This method returns an Object containing the push event settings

Example

Request :

```
{  
  "params": {},  
  "jsonrpc": "2.0",  
  "method": "getPushEventSettings",  
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb"  
}
```

```
}
```

Response :

```
{
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb",
  "jsonrpc": "2.0",
  "result": {
    "status": 1,
    "serviceType": "jsonRPC",
    "serviceSettings": {
      "url": "http://example.com",
      "authorization": "Bearer sfasdfw34243",
      "requireValidSslCertificate": true
    },
    "subscribeToEventTypes": {
      "modules": true,
      "sva": true,
      "registration": true,
      "supa-update-status": true,
      "av": true,
      "aph": true,
      "fw": true,
      "avc": true,
      "uc": true,
      "dp": true,
      "sva-load": true,
      "task-status": true,
      "exchange-malware": true,
      "network-sandboxing": true,
      "adcloud": true,
      "exchange-user-credentials": true,
      "endpoint-moved-out": true,
      "endpoint-moved-in": true,
      "troubleshooting-activity": true,
      "uninstall": true,
      "install": true,
      "hwid-change": true,
      "new-incident": true,
      "antiexploit": true,
    }
  }
}
```

```
        "network-monitor": true,  
        "ransomware-mitigation": true  
    }  
}  
}
```

2.9.3. sendTestPushEvent

This method sends a test event.

Test events always have the `_testEvent_` property set to `true`.

Parameters

Parameter	Type	Optional	Description
<code>eventType</code>	String	No	Event type
<code>data</code>	Object	Yes	Test events are created from templates. This parameter can be used to replace data in the event template.

Return value

This method returns an Object containing the details of the sent event and a Boolean that marks the event as a test.

Example

Request :

```
{  
  "params": {  
    "eventType": "av",  
    "data": {  
      "malware_name": "Test malware name"  
    }  
  },  
  "jsonrpc": "2.0",  
  "method": "sendTestPushEvent",  
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb"  
}
```



```
}
```

Response :

```
{
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb",
  "jsonrpc": "2.0",
  "result": {
    "companyId": "59a14b271da197c6108b4567",
    "computer_name": "FC-WIN7-X64-01",
    "computer_fqdn": "fc-win7-x64-01",
    "computer_ip": "10.17.46.196",
    "computer_id": "59a1604e60369e06733f8abb",
    "product_installed": "BEST",
    "malware_type": "file",
    "malware_name": "Test malware name",
    "file_path": "C:\\eicar0000001.txt",
    "hash":
      "8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1",
    "final_status": "deleted",
    "timestamp": "2017-09-08T12:01:36.000Z",
    "module": "av",
    "_testEvent_": true
  }
}
```

2.9.4. getPushEventStats

This method gets the push event statistics and errors.

The configuration error occurs when the HTTP collector does not use an SSL certificate, or the `setPushEventSettings` method is not using an authorization header generated by the HTTP collector. You must meet these prerequisites to successfully use Event Push Service.



Warning

The field `errorMessages` can count only 100 messages that are not sent via Event Push Service due to communication errors. Once the counter exceeds 100 such events, Event Push Service will automatically stop sending events, and it will reset

`serviceSettings.status` field from `getPushEventsSettings` method to 0.

Parameters

No input parameters are required.

Return value

This method returns an Object containing the push event statistics.

Example

Request :

```
{
  "params": {},
  "jsonrpc": "2.0",
  "method": "getPushEventStats",
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb"
}
```

Response :

```
{
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb",
  "jsonrpc": "2.0",
  "result": {
    "count": {
      "events": 6945,
      "testEvents": 8,
      "sentMessages": 8,
      "errorMessages": 0
    },
    "error": {
      "configurationError": 0,
      "connectionError": 0,
      "statusCode2xx": 0,
      "statusCode300": 0,
      "statusCode400": 0,
      "statusCode500": 0,
    }
  }
}
```

```
        "timeout": 0,  
        "serviceError": 0  
    },  
    "lastUpdateTime": "2017-10-13T18:45:28"  
}
```

2.9.5. resetPushEventStats

This method resets the push event statistics and errors.

Parameters

No input parameters are required.

Return value

This method returns a Boolean which is True when the statistics were reset successfully.

Example

Request :

```
{  
  "params": {},  
  "jsonrpc": "2.0",  
  "method": "resetPushEventStats",  
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb"  
}
```

Response :

```
{  
  "id": "ad12cb61-52b3-4209-a87a-93a8530d91cb",  
  "jsonrpc": "2.0",  
  "result": true  
}
```

2.9.6. Event Types

This table displays types of events based on modules, types of tasks or actions, or status indicators. For each type of event you can view the common category name and the JSON variable used in API. Click the category name to view the details sent for such events.

Event category in GravityZone	Event identifier in API
Cloud AD Integration	adcloud
Antiphishing	aph
Antimalware	av
Advanced Threat Control (ATC)	avc
Data Protection	dp
Exchange Malware Detection	exchange-malware
Exchange License Usage Limit Has Been Reached	exchange-organization-info
Exchange User Credentials	exchange-user-credentials
Firewall	fw
Hyper Detect event	hd
Product Modules Status	modules
Sandbox Analyzer Detection	network-sandboxing
Product Registration	registration
Outdated Update Server	supa-update-status
Overloaded Security Server	sva-load
Security Server Status	sva
Antiexploit Event	antiexploit
Network Attack Defense Event	network-monitor
Task Status	task-status
User Control/Content Control	uc



Event category in GravityZone	Event identifier in API
Storage Antimalware Event	storage-antimalware
Install Agent	install
Uninstall Agent	uninstall
Hardware ID Change	hwid-change
Endpoint moved in	endpoint-moved-in
Endpoint moved out	endpoint-moved-out
Troubleshooting activity	troubleshooting-activity
Device Control	device-control
Ransomware activity detection	ransomware-mitigation
New Incident	new-incident

2.9.7. Push event JSON RPC messages

Events are submitted in calls to the "addEvents" function. This function takes one parameter: "events", which is an array of event objects documented below.

HTTP requests can be verified using the Event-Push-Service-Md5 header. The header is obtained by hashing the Api Key and the message body as follows:
 header_value = md5(api_key, md5(message_body))

Cloud AD Integration

This event is generated when Control Center is synchronizing with an Active Directory domain.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: adcloud
companyId	string	yes	Company identifier
syncerId	string	yes	AD Integrator identifier
issueType	integer	yes	AD Synchronization issue type

Name	Type	Mandatory	Description
isProtectedEntityId	integer	no	Is protected entity ID (only for uninstall)
lastAdReportDate	timestamp	no	Last AD synchronization date

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "syncerId": "59b7d9bfa849af3a1465b7e3",
        "issueType": 0,
        "lastAdReportDate": "2017-09-14T08:03:49.671Z",
        "module": "adcloud"
      }
    ]
  },
  "id": 1505376232077
}
```

Antiphishing

This notification informs you each time the endpoint agent detects a known phishing attempt when accessing a web page.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier . Value: <code>aph</code>
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN

Name	Type	Mandatory	Description
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
aph_type	string	yes	Values: phishing, fraud, untrust
url	string	yes	Malware url
status	string	yes	Values: aph_blocked, reportOnly
last_blocked	timestamp	yes	Last timestamp this malware was blocked
count	integer	yes	How many times this malware was detected

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-EXCHANGE-01",
        "computer_fqdn": "fc-exchange-01.fc.dom",
        "computer_ip": "192.168.0.1",
        "computer_id": "59b7d9bfa849af3a1465b7e4",
        "product_installed": "BEST",
        "aph_type": "phishing",
        "url": "http://example.com/account/support/",
        "status": "aph_blocked",
        "last_blocked": "2017-09-14T08:49:43.000Z",
        "count": 1,
        "module": "aph"
      }
    ]
  },
  "id": 1505378984190
}
```

Antimalware

This event generated each time Bitdefender detects malware on an endpoint in your network.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: av
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
malware_type	string	yes	Type of the detected malware: file, http, cookie, pop3, smtp, process, boot, registry, stream
malware_name	string	yes	Malware name
hash	string	no	Malware file sha256 hash
final_status	string	yes	Final status of the action taken on the file: ignored, still present, deleted, blocked, quarantined, disinfected, restored
container_id	string	no	The identifier of the container entity
container_host	string	no	The name of the host that manages the container entity
file_path	string	yes	Malware file path
timestamp	timestamp	yes	Timestamp when the malware was detected
signaturesNumber	string	no	signatures Number

Name	Type	Mandatory	Description
taskScanType	integer	no	taskScanType
scanEngineType	integer	no	scanEngineType

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-WIN7-X64-01",
        "computer_fqdn": "fc-win7-x64-01",
        "computer_ip": "10.17.46.196",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "malware_type": "file",
        "malware_name": "EICAR-Test-File (not a virus)",
        "file_path": "C:\\\\eicar0000001.txt",
        "hash": "8b3f191819931d1f2cef7289239b5f77c00b079
847b9c2636e56854d1e5eff71",
        "final_status": "deleted",
        "timestamp": "2017-09-08T12:01:36.000Z",
        "module": "av"
      }
    ]
  },
  "id": 1504872097787
}
```

Advanced Threat Control (ATC)

This event is created whenever a potentially dangerous applications is detected and blocked on an endpoint.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: avc
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
exploit_type	string	yes	Values: IDS APP, AVC APP, AVC Exploit
exploit_path	string	yes	Exploit file path
process_command_line	string	no	The command line parameters of the detected process
parent_process_id	integer	no	The pid of the parent of the detected process
parent_process_path	string	no	The path of the parent process of the detection
status	string	yes	Values: avc_blocked, avc_allowed, avc_disinfected
last_blocked	timestamp	yes	Last timestamp this application/exploit was blocked
count	integer	yes	How many times this application/exploit was detected

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
```

```

    {
      "companyId": "59a14b271da197c6108b4567",
      "computer_name": "FC-WIN7-X64-01",
      "computer_fqdn": "fc-win7-x64-01",
      "computer_ip": "192.168.0.1",
      "computer_id": "59a1604e60369e06733f8abb",
      "product_installed": "BEST",
      "exploit_type": "AVC Blocked Exploit",
      "exploit_path": "C:\\Users\\admin\\Desktop\\Tool
s\\avcsim\\win32\\avcsim32.exe",
      "status": "avc_blocked",
      "last_blocked": "2017-09-14T07:56:33.000Z",
      "count": 1,
      "module": "avc"
    }
  ],
  "id": 1505375801845
}

```

Data Protection

This event is generated each time the data traffic is blocked on an endpoint, according to data protection rules.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: dp
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
target_type	string	yes	Malware type: mail, http

Name	Type	Mandatory	Description
blocking_rule_name	string	yes	Data protection rule name
url	string	yes	Url
status	string	yes	Always "data_protection_blocked"
last_blocked	timestamp	yes	Last timestamp this email/url was blocked
count	integer	yes	How many times this malware was detected

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-WIN7-X64-01",
        "computer_fqdn": "fc-win7-x64-01",
        "computer_ip": "192.168.0.1",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "target_type": "http",
        "blocking_rule_name": "dv",
        "url": "http://example.com/",
        "status": "data_protection_blocked",
        "last_blocked": "2017-09-11T10:23:43.000Z",
        "count": 1,
        "module": "dp"
      }
    ]
  },
  "id": 1505125464691
}
```

Exchange Malware Detection

This event is created when Bitdefender detects malware on an Exchange server in your network.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: exchange-malware
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
serverName	string	yes	Server name
sender	string	yes	Email sender
recipients	array	yes	List of email recipients (array of strings)
subject	string	yes	Email subject
detectionTime	timestamp	yes	Detection time
malware	array	yes	List of detected malware (array of {"malwareName": string, "malwareType": string, "actionTaken": string, "infectedObject": string})

Example:

```
{  
  "jsonrpc": "2.0",
```

```
"method": "addEvents",
"params": {
  "events": [
    {
      "companyId": "59a14b271da197c6108b4567",
      "computer_name": "FC- EXCHANGE - 01",
      "computer_fqdn": "fc- exchange - 01.fc.dom",
      "computer_ip": "192.168.0.1",
      "computer_id": "59b7d9bfa849af3a1465b7e4",
      "product_installed": "BEST",
      "endpointId": "59b7d9bfa849af3a1465b7e3",
      "serverName": "FC- EXCHANGE - 01",
      "sender": "fc_test01@fc.dom",
      "recipients": [
        "fc_test02@fc.dom"
      ],
      "subject": "Emailing Sending.. WL - cbe100c9f42a
20ef9a4b1c20ed1a59f9 - 0",
      "detectionTime": "2017- 09 - 13T14: 20:37.000Z",
      "malware": [
        {
          "malwareName": "Trojan.Generic.KD.874127",
          "malwareType": "virus",
          "actionTaken": "quarantine",
          "infectedObject": "WL- cbe100c9f42a20ef9
a4b1c20ed1a59f9 - 0"
        }
      ],
      "module": "exchange-malware"
    }
  ],
  "id": 1505312459584
}
```

Exchange License Usage Limit Has Been Reached

This event is generated when Exchange License limit has been reached

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: exchange-organization-info
companyId	string	yes	Company identifier

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "endpointId": "59b7d9bfa849af3a1465b7e3",
        "module": "exchange-organization-info",
        "mailboxes": 8,
        "license_limit": 5,
        "license_key": "5IMI111"
      }
    ]
  },
  "id": 1505387661508
}
```

Exchange User Credentials

This event is generated when an on-demand scan task could not start on the target Exchange server due to invalid user credentials. To complete the task, you need to change your Exchange credentials.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: exchange-user-credentials
companyId	string	yes	Company identifier

Name	Type	Mandatory	Description
endpointId	string	yes	Managed endpoint identifier in the GravityZone database

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "endpointId": "59b7d9bfa849af3a1465b7e3",
        "module": "exchange-user-credentials"
      }
    ]
  },
  "id": 1505387661508
}
```

Firewall

This event is generated when the endpoint agent blocks a port scan or an application from accessing the network, according to the applied policy.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier . Value: fw
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address

Name	Type	Mandatory	Description
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
status	string	yes	Status
local_port	string	no	Local port
protocol_id	string	no	Protocol identifier
application_path	string	no	Application path
source_ip	string	no	Source IP address
last_blocked	timestamp	yes	Last timestamp this connection was blocked
count	integer	yes	How many times this connection was detected

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-WIN7-X64-01",
        "computer_fqdn": "fc-win7-x64-01",
        "computer_ip": "192.168.0.1",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "status": "portscan_blocked",
        "protocol_id": "6",
        "source_ip": "192.168.0.2",
        "last_blocked": "2017-09-08T12:52:03.000Z",
        "count": 1,
        "module": "fw"
      }
    ]
  },
}
```

```
"id": 1504875129648
}
```

Hyper Detect event

Event generated when a malware is detected by the Hyper Detect module.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: hd
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
malware_type	string	yes	Type of the detected malware: file, http, cookie, pop3, smtp, process, boot, registry, stream
malware_name	string	yes	Malware name
hash	string	no	Malware file sha256 hash
final_status	string	yes	Final status of the action taken on the file: ignored, still present, deleted, blocked, quarantined, disinfected, restored
container_id	string	no	The identifier of the container entity

Name	Type	Mandatory	Description
container_host	string	no	The name of the host that manages the container entity
file_path	string	yes	Malware file path
attack_type	string	no	Values: targeted attack, grayware, exploits, ransomware, suspicious files and network traffic
detection_level	string	no	Values: permissive, normal, aggressive
is_fileless_attack	boolean	no	True for fileless attack
command_line_parameters	string	no	Command line parameters
process_info_path	string	no	Process path
process_info_command_line	string	no	Process command line parameters
parent_process_id	integer	no	Parent process ID
parent_process_path	string	no	Parent process path
hwid	string	yes	Hardware identifier
date	timestamp	yes	Timestamp when the malware was detected

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "module": "hd",
        "product_installed": "EPS",
        "user": {
          "name": "admin",
          "sid": "BF410F3B-5F3A-41E1-BF8F-28DE6948A355"
        }
      }
    ]
  }
}
```

```

"
    },
    "computer_name": "DHMSI",
    "computer_fqdn": "dhmsi",
    "computer_ip": "10.10.18.226",
    "computer_id": "5c4999491ddfad7177316f80",
    "malware_type": "file",
    "malware_name": "",
    "hash": "hash_3",
    "final_status": "quarantined",
    "file_path": "44e695d9ed259aea10e5b57145d0d0dc.b
ender",
    "attack_type": "suspicious files and network tra
ffic",
    "detection_level": "normal",
    "is_fileless_attack": 1,
    "command_line_parameters": "a b c",
    "hwid": "00000000-0000-0000-0000-406186b5bdbd",
    "companyId": "5c497704f9bf8d0b1b4df494",
    "date": "2019-01-24T11:13:04.000Z"
  }
]
},
" id": 1547719287349
}

```

Product Modules Status

This event is generated when a security module of the installed agent gets enabled or disabled.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: modules
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name



Name	Type	Mandatory	Description
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
container_id	string	no	The identifier of the container entity
container_host	string	no	The name of the host that manages the container entity
is_container_host	boolean	no	Whether the machine is container host or not
malware_status	boolean	no	Antimalware module
aph_status	boolean	no	Antiphishing module
firewall_status	boolean	no	Firewall module
avc_status	boolean	no	Active Threat Control module
ids_status	boolean	no	Intrusion detection system module
uc_web_filtering	boolean	no	Content Control Web Access Control module
uc_categ_filtering	boolean	no	Content Control Web Categories Filtering module
uc_application_status	boolean	no	Content Control Application Blacklisting module
dp_status	boolean	no	Content Control Data Protection module
pu_status	boolean	no	Power User module
dlp_status	boolean	no	Device Control module
exchange_av_status	boolean	no	Exchange Protection Antimalware module
exchange_as_status	boolean	no	Exchange Protection Antispam module

Name	Type	Mandatory	Description
exchange_at_status	boolean	no	Exchange Protection Attachment filtering module
exchange_cf_status	boolean	no	Exchange Protection Content filtering module
exchange_od_status	boolean	no	Exchange Protection On demand scan module
volume_encryption	boolean	no	Encryption module
patch_management	boolean	no	Patch management module
container_protection_status	boolean	no	Container Protection module

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC- WIN7 - X64 - 01",
        "computer_fqdn": "fc- win7 - x64 - 01",
        "computer_ip": "192.168.0.1",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "malware_status": 1,
        "aph_status": 1,
        "firewall_status": 1,
        "avc_status": 1,
        "uc_web_filtering": 0,
        "uc_categ_filtering": 0,
        "uc_application_status": 0,
        "dp_status": 0,
        "pu_status": 1,
        "dlp_status": 0,
        "module": "modules"
      }
    ]
  }
}
```

```
},
  "id": 1504871857671
}
```

Sandbox Analyzer Detection

This event is generated each time Sandbox Analyzer detects a new threat among the submitted files.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: network-sandboxing
companyId	string	yes	Company identifier
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
computerName	string	yes	Computer name
computerIp	string	yes	Computer IP address
detectionTime	integer	yes	Detection time
threatType	string	yes	Threat type
filePaths	array	yes	File paths (array of strings)
fileSizes	array	yes	File sizes (array of strings)
remediationActions	array	yes	Remediation actions (array of strings)

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "endpointId": "59a1604e60369e06733f8aba",
        "computerName": "FC-WIN7-X64-01",
```

```
    "computerIp": "192.168.0.1",
    "detectionTime": 1505386969,
    "threatType": "RANSOMWARE",
    "filePaths": [
      "C:\\Users\\Administrator\\Documents\\instal
ler.xml",
      "D:\\opt\\bitdefender\\installer2.xml",
      "D:\\sources\\console\\CommonConsole\\app\\m
odules\\policies\\view\\endpoints\\networkSandboxing\\installer3
.xml"
    ],
    "fileSizes": [
      "2614",
      "2615",
      "2616"
    ],
    "remediationActions": [
      "1",
      "",
      "1"
    ],
    "module": "network-sandboxing"
  }
}
},
" id": 1505386971126
}
```

Product Registration

This event is generated when the registration status of an agent installed in your network has changed.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: registration
product_installed	string	yes	Identifier for the installed GravityZone component

Name	Type	Mandatory	Description
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
container_id	string	no	The identifier of the container entity
container_host	string	no	The name of the host that manages the container entity
is_container_host	boolean	no	Whether the machine is container host or not
product_registration	string	yes	Values: registered, unregistered

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-EXCHANGE-01",
        "computer_fqdn": "fc-exchange-01.fc.dom",
        "computer_ip": "192.168.0.1",
        "computer_id": "59b7d9bfa849af3a1465b7e4",
        "product_installed": "BEST",
        "product_registration": "registered",
        "module": "registration"
      }
    ]
  },
  "id": 1505221060168
}
```

Outdated Update Server

This event is generated when an update server has outdated malware signatures.

Parameters:

Name	Type	Mandatory	Description
fromSupa	boolean	yes	Identifies events sent from Relays (always true)
module	string	yes	Event type identifier. Value: <code>supa-update-status</code>
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
status	boolean	yes	Update status

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-WIN7-X64-01",
        "computer_fqdn": "fc-win7-x64-01",
        "computer_ip": "192.168.0.1",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "status": 0,
        "fromSupa": 1,

```

```

        "module": "supa-update-status"
    }
  ],
  "id": 1505379714808
}

```

Overloaded Security Server

This event is generated when the scan load on a Security Server in your network exceeds the defined threshold.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: sva-load
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
loadAverage	integer	yes	Load average
cpuUsage	integer	yes	Cpu usage
memoryUsage	integer	yes	Memory usage
networkUsage	integer	yes	Network usage
overallUsage	integer	yes	Overall usage
svaLoad	string	no	SVA load

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "bitdefender-sva",
        "computer_fqdn": "bitdefender-sva",
        "computer_ip": "192.168.0.1",
        "computer_id": "59b8f3aba849af3a1465b81e",
        "product_installed": "SVA",
        "loadAverage": 1,
        "cpuUsage": 48,
        "memoryUsage": 32,
        "networkUsage": 0,
        "overallUsage": 48,
        "svaLoad": "Normal",
        "module": "sva-load"
      }
    ]
  },
  "id": 1505293227782
}
```

Security Server Status

This event is created when the status of a certain Security Server changes. The status refers to power (powered on/powered off), product update, signatures update and reboot required.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: sva
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier

Name	Type	Mandatory	Description
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
powered_off	boolean	yes	Powered off
product_update_available	boolean	no	Product update available
signature_update	timestamp	no	Last signatures update timestamp
product_reboot_required	boolean	no	True if a reboot is required
lastupdate	string	no	Last update
lastupdateerror	string	no	Last update error
updatesigam	string	no	Security Server engines version

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "bitdefender-sva",
        "computer_fqdn": "bitdefender-sva",
        "computer_ip": "192.168.0.1",
        "computer_id": "59b8f3aba849af3a1465b81e",
        "product_installed": "SVA",
        "powered_off": 0,
        "product_update_available": 1,
        "product_reboot_required": 0,
        "lastupdate": "0",
        "updatesigam": "7.72479",
        "module": "sva"
      }
    ]
  }
}
```

```

    }
  ],
  "id": 1505293227782
}

```

Antiexploit Event

This event is generated when Advanced Anti-Exploit triggers a detection.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: <code>antiexploit</code>
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
container_id	string	no	The identifier of the container entity
container_host	string	no	The name of the host that manages the container entity
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
detection_action	string	yes	The action that was taken upon the detection
detection_threatName	string	no	Threat type
detection_pid	string	yes	The pid of the detection

Name	Type	Mandatory	Description
detection_exploitTechnique	string	yes	The technique employed in the detection
detection_parentPid	string	no	The pid of the parent of the detected process
detection_path	string	yes	The path of the detection
detection_parentPath	string	no	The path of the parent process of the detection
detection_cve	string	no	Detection CVE
detection_payload	string	no	Detection payload
detection_username	string	no	The user that was logged when the detection was found
detection_time	timestamp	yes	Time of the event as reported by the product, already formatted in a string representation

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "module": "antiexploit",
        "product_installed": "BEST",
        "companyId": "5cf10c8af23f73097377c924",
        "computer_name": "TEST_ENDPOINT",
        "computer_fqdn": "test-endpoint.dsd.ro",
        "computer_ip": "10.10.18.226",
        "computer_id": "5cf51ba5e8ee8c5b1852a9d7",
        "endpointId": "5cf51ba5e8ee8c5b1852a9d6",
        "detection_action": "kill",
        "detection_threatName": "EICAR-Test-File (not a
```

```

virus)",
      "detection_pid": "2000",
      "detection_exploitTechnique": "Flash/Generic",
      "detection_parentPid": "4000",
      "detection_path": "C:\\file15c8ba8b90ea1de127962
f464.exe",
      "detection_parentPath": "C:\\file25c8ba8b90ea1de
127962f464.exe",
      "detection_username": "user@domain.com",
      "detection_time": "2019-06-03T13:58:30.000Z"
    }
  ],
},
  "id": 1547719287349
}

```

Network Attack Defense Event

This event is generated when the Network Attack Defense module triggers a detection.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: network-monitor
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
endpointId	string	yes	Endpoint identifier
label	string	no	The label set in the Network grid by the Admin

Name	Type	Mandatory	Description
actionTaken	string	yes	The action that was taken upon the detection
detection_name	string	yes	The name of the detection as received from BEST
detection_attackTechnique	string	yes	Name of the attack technique as set in the Network Attack Defense policy
source_ip	string	yes	IP of the attack source
victim_ip	string	yes	IP of the victim's endpoint
local_port	string	yes	The port on which the attack occurred
timestamp	timestamp	yes	Time of the event as reported by the product, already formatted in a string representation

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "module": "network-monitor",
        "product_installed": "BEST",
        "user": {
          "userName": "user1@domain.com",
          "userSid": "S-1-2-3-4"
        },
        "computer_name": "TEST_ENDPOINT",
        "computer_fqdn": "test-endpoint.dsd.ro",
        "computer_ip": "10.10.18.226",
        "computer_id": "5d639e8f48ac2f04f6e00b1c",
        "actionTaken": "reportOnly",
        "detection_name": "PrivacyThreat.PasswordStealer"
      }
    ]
  }
}
```

```
.HTTP",
    "detection_attackTechnique": "discovery",
    "source_ip": "10.17.134.4",
    "victim_ip": "213.211.198.58",
    "local_port": "80",
    "timestamp": "2019-01-24T11:13:04.000Z"
  }
]
},
"id": 1547719287349
}
```

Task Status

This event is generated each time a task status changes.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: task-status
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
userId	string	yes	User identifier
taskId	string	yes	Task identifier
taskName	string	yes	Task name
taskType	integer	yes	Task type
targetName	string	yes	Task name
isSuccessful	boolean	yes	True if the task was executed successfully
status	integer	yes	Task status

Name	Type	Mandatory	Description
errorMessage	string	yes	Error message
errorCode	integer	yes	Error code

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-WIN7-X64-01",
        "computer_fqdn": "fc-win7-x64-01",
        "computer_ip": "192.168.0.1",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "userId": "59a14b2b1da197c6108b4568",
        "taskId": "59b28dc81da19711058b4568",
        "taskName": "Quick Scan 2017-09-08 (sub-task)",
        "taskType": 272,
        "targetName": "FC-WIN7-X64-01",
        "isSuccessful": 1,
        "status": 3,
        "errorMessage": "",
        "errorCode": 0,
        "module": "task-status"
      }
    ]
  },
  "id": 1504874269032
}
```

User Control/Content Control

This event is generated when a user activity such as web browsing of software application is blocked on the endpoint according to the applied policy.

Parameters:



Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: uc
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
uc_type	string	no	Values: application, http
url	string	no	Url
block_type	string	no	Values: application, http_timelimiter, http_blacklist, http_categories, http_bogus, http_antimalware
categories	string	no	Values: WebProxy, Games, Tabloids, Hate, Gambling, Drugs, Illegal, Shopping, OnlinePay, Video, SocialNetwork, OnlineDating, IM, SearchEngines, RegionalTLDS, News, Pornography, MatureContent, Blog, FileSharing, Narcotics, VideoOnline, Religious, Suicide, Health, ViolentCartoons, Weapons, Hacking, Scams, CasualGames, OnlineGames, ComputerGames, PhotosOnline, Ads, Advice, Bank, Business, ComputerAndSoftware, Education, Entertainment, Government, Hobbies, Hosting, JobSearch, Portals, RadioMusic, Sports, TimeWasters, Travel, WebMail
application_path	string	no	Application path

Name	Type	Mandatory	Description
status	string	no	Values: uc_application_blocked, uc_site_blocked
last_blocked	timestamp	no	Last timestamp this malware was blocked
count	integer	no	How many times this malware was detected

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "FC-WIN7-X64-01",
        "computer_fqdn": "fc-win7-x64-01",
        "computer_ip": "192.168.0.1",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "uc_type": "http",
        "url": "http://192.168.0.1:2869/upnphost/udhisap
i.dll",
        "block_type": "http_timelimiter",
        "categories": "",
        "status": "uc_site_blocked",
        "last_blocked": "2017-09-08T12:46:30.000Z",
        "count": 1,
        "module": "uc"
      }
    ]
  },
  "id": 1504874799367
}
```

Storage Antimalware Event

This event is generated each time SVA detects a new threat among the protected storage (NAS).

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: storage-antimalware
companyId	string	yes	Company identifier
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
computer_name	string	yes	Computer name
storage_name	string	yes	The name of the storage unit
storage_ip	string	yes	The IP address of the storage unit
storage_type	string	yes	The type of the storage unit.(E.g., Nutanix, Citrix etc.)
file_path	string	yes	File path
file_hash	string	yes	File hash
malware_type	string	yes	Describes the type of malware as defined by Bitdefender. Possible values are: 'file', 'http', 'cookie', 'pop3', 'smtp', 'process', 'boot', 'registry' and 'stream'
malware_name	string	yes	Name of the malware as defined by Bitdefender
status	string	yes	Status
detection_time	timestamp	yes	Time of the event as reported by the product, already formatted in a string representation

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "companyId": "59a14b271da197c6108b4567",
        "endpointId": "59a1604e60369e06733f8aba",
        "computerName": "SVA_WITH_ICAP",
        "storage_name": "fileserver001",
        "storage_ip": "192.168.0.1",
        "storage_type": "Nutanix",
        "file_path": "C:\\Users\\Administrator\\Document
s\\installer.xml",
        "file_hash": "04d7cff845e23111633cc0a268634f5e6c
18145d0a9b5a38dedd8a58a422001c",
        "malware_type": "1",
        "malware_name": "BAT.Trojan.FormatC.Z",
        "status": "5",
        "detection_time": "2018-05-07T10:23:43.000Z",
        "module": "storage-antimalware"
      }
    ]
  },
  "id": 1505386971126
}
```

Install Agent

This event is generated when the agent is installed on endpoints.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: <code>install</code>
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name

Name	Type	Mandatory	Description
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
hwid	string	yes	Hardware identifier

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "product_installed": "BEST",
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "TEST_ENDPOINT",
        "computer_fqdn": "test-endpoint.dsd.ro",
        "computer_ip": "10.10.18.226",
        "computer_id": "5cf51ba5e8ee8c5b1852a9d7",
        "module": "install",
        "endpointId": "5e2085febf255a545e52276b",
        "hwid": "00000000-0000-0000-0000-406186b5bdbd50"
      }
    ]
  },
  "id": 1547719287350
}
```

Uninstall Agent

This event is generated when an agent is uninstalled from an endpoint.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: <code>uninstall</code>
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
reason	integer	yes	Uninstalling method. Available options: <ul style="list-style-type: none">• 1 - local uninstall• 2 - deleted from the network inventory in GravityZone Control Center• 3 - uninstall task from GravityZone Control Center

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "product_installed": "BEST",
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "TEST_ENDPOINT",
        "computer_fqdn": "test-endpoint.dsd.ro",
        "computer_ip": "10.10.18.226",
        "computer_id": "59b7d9bfa849af3a1465b7e4",
        "endpointId": "5e2085feb255a545e52276b",
        "reason": 1,
      }
    ]
  }
}
```

```
        "module": "uninstall"
      }
    ]
  },
  "id": 1505221060168
}
```

Hardware ID Change

This event is generated when the hardware ID of an endpoint from your network is changed

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: hwid-change
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
old_hwid	string	yes	The old hardware ID of the machine
new_hwid	string	yes	The new hardware ID of the machine
endpointId	string	yes	Managed endpoint identifier in the GravityZone database

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
```

```
    {
      "module": "hwid-change",
      "product_installed": "BEST",
      "companyId": "5e207bc354060806ed24a132",
      "computer_name": "A",
      "computer_fqdn": "test-endpoint.dsd.ro",
      "computer_ip": "10.10.18.526",
      "computer_id": "5e284ff5b7e43d387ba54a96",
      "old_hwid": "00000000-0000-0000-0000-406186b5bde
7",
      "new_hwid": "00000000-0000-0000-0000-406186b5bde
6",
      "endpointId": "5e284ff5b7e43d387ba54a95"
    }
  ],
  "id": 1547719287349
}
```

Endpoint moved in

This event is generated when endpoints are moved in Network Inventory from one company to another. The event is received by the destination company.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: endpoint-moved-in
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database

Name	Type	Mandatory	Description
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
hwid	string	yes	Hardware identifier

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "product_installed": "BEST",
        "companyId": "59a14b271da197c6108b4568",
        "computer_name": "TEST_ENDPOINT",
        "computer_fqdn": "test-endpoint.dsd.ro",
        "computer_ip": "10.10.18.226",
        "computer_id": "59b7d9bfa849af3a1465b7e3",
        "endpointId": "5e2085febf255a545e52276a",
        "module": "endpoint-moved-in",
        "hwid": "5e284ff-5b7e43d387ba-54a95"
      }
    ]
  },
  "id": 1505221060169
}
```

Endpoint moved out

This event is generated when endpoints are moved in Network Inventory from one company to another. The event is received by the source company.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: endpoint-moved-out

Name	Type	Mandatory	Description
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
endpointId	string	yes	Managed endpoint identifier in the GravityZone database
hwid	string	yes	Hardware identifier

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "product_installed": "BEST",
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "TEST_ENDPOINT",
        "computer_fqdn": "test-endpoint.dsd.ro",
        "computer_ip": "10.10.18.226",
        "computer_id": "59b7d9bfa849af3a1465b7e4",
        "endpointId": "5e2085feb255a545e52276b",
        "module": "endpoint-moved-out",
        "hwid": "5e284ff-5b7e43d387ba-54a95"
      }
    ]
  },
  "id": 1505221060170
}
```

Troubleshooting activity

The event is generated when a troubleshooting task ends, and it informs you of its status. If successful, it provides you with the logs.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: troubleshooting-activity
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
taskId	string	yes	The ID of the current Troubleshooting task.
taskType	string	yes	The type of the task
errorCode	integer	yes	Integer representing the error code if the task has failed
username	string	no	Name of the user account who started the Troubleshooting task
localPath	string	no	The path on the target machine where the Troubleshooting archive is placed
networkSharePath	string	no	The path on network share where the Troubleshooting archive is placed
saveToBitdefenderCloud	boolean	no	The option to also upload to Bitdefender Cloud the Troubleshooting archive

Name	Type	Mandatory	Description
status	integer	yes	The status with which the task has finished
stopReason	integer	no	The reason for which the Troubleshooting activity was stopped
failedStorageType	integer	no	In case some delivery methods succeeded and some not, which one has failed
startDate	timestamp	no	Timestamp of when the event has started
endDate	timestamp	no	Time of the event as reported by the product, already formatted in a string representation

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "product_installed": "BEST",
        "companyId": "59a14b271da197c6108b4567",
        "computer_name": "TEST_ENDPOINT_WINDOWS_10",
        "computer_fqdn": "test-endpoint.dsd.ro",
        "computer_ip": "10.10.0.101",
        "computer_id": "5ee30e2b29a4e218489442b6",
        "module": "troubleshooting-activity",
        "taskId": "5eea0105f23f731302405833",
        "taskType": "Debug Session",
        "errorCode": 3,
        "username": "test@test.com",
        "localPath": "/test/dir",
        "networkSharePath": "//1.2.3.4/dir",
        "saveToBitdefenderCloud": 0,
        "status": 3,
      }
    ]
  }
}
```

```
        "stopReason": 2,  
        "failedStorageType": 1,  
        "startDate": "2020-06-24T06:06:48.000Z",  
        "endDate": "2020-06-24T06:09:28.000Z"  
    }  
  ],  
  },  
  "id": 1505221060169  
}
```

Device Control

Every time the Device Control module detects a device inserted into a client system, an event is generated.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: <code>device-control</code>
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
username	string	no	The user that was logged in when the incident was found
silentAgentVersion	string	no	Agent version
action	string	yes	Action taken on the device: allowed, blocked, readonly. Present only when the state of the device is added.
deviceName	string	no	A descriptive name for the device

Name	Type	Mandatory	Description
deviceClass	integer	yes	Device class
deviceId	string	no	Device ID
productId	integer	no	Product ID of the device
vendorId	integer	no	ID of the vendor
date	timestamp	yes	The date when the device was blocked

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "module": "device-control",
        "product_installed": "BEST",
        "computer_name": "FC-WIN7-X64-01",
        "computer_fqdn": "fc-win7-x64-01",
        "computer_ip": "10.17.46.207",
        "computer_id": "5d529fb7008739443adb4003",
        "username": "Admin",
        "action": "blocked",
        "deviceName": "CD-ROM Drive",
        "deviceClass": 2,
        "deviceId": "IDE\\CDROMNECVMMWAR_VMWARE_IDE_CDR10
1.00____\\5&3A794E10&0&1.0.0",
        "productId": 0,
        "vendorId": 0,
        "date": "2019-08-13T11:33:18.000Z"
      }
    ]
  },
  "id": 1565697106257
}
```

Ransomware activity detection

This event occurs when the endpoint agent blocks ransomware attack.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: ransomware-mitigation
product_installed	string	yes	Identifier for the installed GravityZone component
companyId	string	yes	Company identifier
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN
computer_ip	string	yes	IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
company_name	string	yes	The company in which the attack was detected.
endpoint_id	string	yes	Managed endpoint identifier in the GravityZone database
attack_type	string	yes	Ransomware attack type
item_count	string	yes	The number of files encrypted during the attack
detected_on	integer	yes	The date and time when the attack was detected
attack_source	string	yes	The remote IP in case of a remote attack respectively the process path in case of a local attack

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
```

```
"params": {
  "events": [
    {
      "module": "ransomware-mitigation",
      "companyId": "5dad6f685f627d42cb3cd434",
      "product_installed": "SVA",
      "user": {
        "name": "user",
        "sid": "S-11-22-33"
      },
      "company_name": "Bitdefender",
      "computer_name": "DC-Nebula",
      "computer_fqdn": "dc-nebula.nebula.local",
      "computer_ip": "10.17.16.10",
      "computer_id": "5ed4d2fef23f7325715dbb22",
      "attack_type": "remote",
      "item_count": "23",
      "detected_on": 1591007594,
      "attack_source": "10.10.20.120"
    }
  ],
  "id": 1505221060169
}
```

New Incident

This event is generated every time a new Root Cause Analysis (RCA) is displayed under the Incidents section of Control Center. The event contains a list of relevant items extracted from the RCA JSON, which you can use to enrich SIEM driven correlations with EDR specific data.

Parameters:

Name	Type	Mandatory	Description
module	string	yes	Event type identifier. Value: new-incident
computer_name	string	yes	Computer name
computer_fqdn	string	yes	FQDN



Name	Type	Mandatory	Description
computer_ip	string	yes	Computer IP address
computer_id	string	yes	Unique endpoint identifier in the GravityZone database
incident_id	string	yes	Incident identifier
severity_score	integer	yes	Severity score
attack_entry	integer	yes	Attack entry
main_action	string	yes	Main action
detection_name	string	no	Detection name
file_name	string	no	File name
file_path	string	no	File path
file_hash_md5	string	no	MD5 file hash
file_hash_sha256	string	no	SHA-256 file hash
url	string	no	Domain URL
port	integer	no	Domain port
protocol	string	no	Application protocol
source_ip	string	no	Source IP address
process_pid	integer	no	Process pid
process_path	string	no	Process path
parent_process_pid	integer	no	Parent process PID
parent_process_path	string	no	Parent process path
attack_types	array	no	Attack types
att_ck_id	array	no	The IDs of MITRE ATT&CK
process_command_line	string	no	Process parameters in command line
severity	string	yes	The severity of the produced event
companyid	string	yes	Company identifier
endpointid	string	yes	Endpoint identifier
username	string	no	The user that was logged in when the incident was found

Name	Type	Mandatory	Description
user_sid	string	no	The SID of the user involved with the event source

Example:

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "module": "new-incident",
        "created": "2020-07-20T09:36:23.485Z",
        "computer_id": "5efb3a520075db7384dfa286",
        "computer_fqdn": "desktop-jac14gs",
        "computer_name": "DESKTOP-JAC14GS",
        "detection_name": "ATC.Malicious",
        "attack_types": [
          "Other"
        ],
        "computer_ip": "10.17.23.30",
        "severityScore": 90,
        "incident_id": "5f1557cbe7b2584f3959ee19",
        "attack_entry": 1688239188,
        "parent_process_path": "c:\\windows\\system32\\c
md.exe",
        "parent_process_pid": 9636,
        "process_path": "c:\\users\\bdadmin\\desktop\\at
csim\\atcsim32.exe",
        "process_pid": 10324,
        "username": "DESKTOP-JAC14GS\\bdadmin",
        "user_sid": "S-1-5-21-3349207704-443292085-22376
56896-1003",
        "process_command_line": "detect",
        "file_hash_md5": "ccb1b07bdf330627f02b3c832663a4
89",
        "file_hash_sha256": "d5adc6a65a57d30d3ae70d19598
3d155e7cd24f26e1bebe9b92655251ec55",
        "att_ck_id": [
          "T1036",

```

```
        "T1059",
        "T1002",
        "T1012"
    ],
    "severity": "high",
    "main_action": "no action",
    "endpointId": "5efb3a520075db7384dfa285",
    "companyId": "5efb2f7154060876cb4a13d2"
}
]
},
"id": 1505221060171
}
```

2.10. Incidents

The Incidents API includes the following methods allowing the management of Endpoint and Detection (EDR) features:

- `addToBlocklist` : adds a new hash to the Blocklist.
- `getBlocklistItems` : lists existing Blocklist items.
- `removeFromBlocklist` : removes a specific entry from the Blocklist.
- `createIsolateEndpointTask` : creates a task to isolate an endpoint.
- `createRestoreEndpointFromIsolationTask` : creates a task to restore an isolated endpoint.

API url: CONTROL_CENTER_APIs_ACCESS_URL/v1.0/jsonrpc/incidents

2.10.1. addToBlocklist

Use this method to add one or more file hashes to the Blocklist.

Parameters

Parameter	Type	Optional	Description
hashType	Number	No	the algorithm used to obtain the hash. Possible values: 1 - SHA256, 2 - MD5

Parameter	Type	Optional	Description
hashList	Array	No	An array containing several hashes. All hashes must be of the type specified by the <code>hashType</code> parameter.
sourceInfo	String	No	A description for the hashes.

Return value

This method returns a Boolean which is True if the operation was successful.

Example

Request :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810"
  "jsonrpc": "2.0",
  "method": "addToBlocklist",
  "params": {
    "hashType" : 2,
    "hashList": ["5b7ac19bb1a43dfb107b23c6",
                 "f696282aa4cd4f614aa995190cf442fe"],
    "sourceInfo": "Added from public API"
  }
}
```

Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": true
}
```

2.10.2. getBlocklistItems

This method lists all the hashes that are present in the blocklist.

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 on the blocked items. 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 blocklist items. Each entry in the list has the following fields:
 - `id`, the ID of the hash item in the Blocklist.
 - `hashType`, the algorithm used to obtain the hash. Possible values: 1 - SHA256, 2 - MD5
 - `hash`, the hash value for a specific file.
 - `source`, the source from where the hash entry hash originated. Possible values: 1 - Incident, 2 - Import, 3 - Manual.
 - `sourceInfo`, the description of the item, as the user provided when adding the item to the Blocklist.
 - `filename`, the name of file corresponding to the hash. This field is only displayed if this information exists.
 - `companyId`, the ID of your company associated with this item in the Blocklist.
- `total` - the total number of items

Example

Request :


```
{
  "params": {},
  "jsonrpc": "2.0",
  "method": "getBlocklistItems",
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810"
}
```

Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": {
    "items": [
      {
        "companyId": "5b680f6fb1a43d860a7b23c8",
        "hash": "098f6bcd4621d373cade4e832627b4f6",
        "hashType": 2,
        "id": "5b7ac19bb1a43dfb107b23c6",
        "source": 3,
        "sourceInfo": "Added from public API"
      },
      {
        "companyId": "5b680f6fb1a43d860a7b23c8",
        "filename": "file.txt",
        "hash": "f696282aa4cd4f614aa995190cf442fe",
        "hashType": 2,
        "id": "5b7ac19bb1a43dfb107b23c7",
        "source": 1,
        "sourceInfo": "Added from incident 1"
      }
    ],
    "page": 1,
    "pagesCount": 1,
    "perPage": 30,
    "total": 2
  }
}
```

2.10.3. removeFromBlocklist

This method removes an item from the Blocklist, identified by its ID.

Parameters

Parameter	Type	Optional	Description
hashItemId	String	No	the ID of the item in the Blocklist to be deleted

Return value

This method returns a Boolean which is True if the operation was successful.

Example

Request :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "method": "removeFromBlocklist",
  "params": {
    "hashItemId" : "5b680f6fb1a43d860a7b23c1"
  }
}
```

Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": true
}
```

2.10.4. createIsolateEndpointTask

This method creates a task to isolate the specified endpoint.

Parameters

Parameter	Type	Optional	Description
endpointId	String	No	the ID of the endpoint to be isolated

Return value

This method returns a Boolean which is True if the operation was successful.

Example

Request :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "method": "createIsolateEndpointTask",
  "params": {
    "endpointId" : "5b680f6fb1a43d860a7b23c1"
  }
}
```

Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": true
}
```

2.10.5. createRestoreEndpointFromIsolationTask

This method creates a task to restore the specified endpoint from isolation.

Parameters

Parameter	Type	Optional	Description
endpointId	String	No	the ID of the endpoint to be restored

Return value

This method returns a Boolean which is True if the operation was successful.

Example

Request :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "method": "createRestoreEndpointFromIsolationTask",
  "params": {
    "endpointId" : "5b680f6fb1a43d860a7b23c1"
  }
}
```

Response :

```
{
  "id": "0df7568c-59c1-48e0-a31b-18d83e6d9810",
  "jsonrpc": "2.0",
  "result": true
}
```

2.11. Quarantine

The Quarantine API contains the following methods allowing the management of quarantined 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.
- `createAddFileToQuarantineTask` : creates a task to quarantine a file based on its path.

API url: [CONTROL_CENTER_APIS_ACCESS_URL/v1.0/jsonrpc/quarantine](#)

2.11.1. `getQuarantinedItemsList`

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
<code>endpointId</code>	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.

Parameter	Type	Optional	Description
<code>page</code>	Number	Yes	The results page. The default value is 1.
<code>perPage</code>	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.
<code>filters</code>	Object	Yes	The filters to be used when querying the quarantine items list. For information regarding the available filters and how to use them, refer to “Available Filters” (p. 194).

Available Filters

You can use the `filters` parameter to query the quarantine by certain properties. The query result is a list of quarantine items that match ALL selected filters. These are the available filtering options:

Field	Type	Description
<code>threatName</code>	String	Filters the quarantined items by threat name. This filter is available for <code>computers</code> and <code>exchange services</code> .
<code>startDate</code>	String	Filters the items that were quarantined after the specified date. The format for <code>startDate</code> is in ISO 8601. This filter is available for <code>computers</code> and <code>exchange services</code> .
<code>endDate</code>	String	Filters the items that were quarantined before the specified date. The format for <code>endDate</code> is in ISO 8601. This filter is available for <code>computers</code> and <code>exchange services</code> .
<code>filePath</code>	String	Filters the quarantined items by file path. This filter is available for <code>computers</code> service.

Field	Type	Description
<code>ip</code>	String	Filters the quarantine items by IP address. This filter is available for <code>computers</code> service.
<code>actionStatus</code>	Integer	Filters the quarantine items by action status. The available values for <code>actionStatus</code> are: <ul style="list-style-type: none">● 0 - None● 1 - Pending remove● 2 - Pending restore● 3 - Remove failed● 4 - Restore failed If the service is <code>exchange</code> , then the following will also be valid action statuses: <ul style="list-style-type: none">● 16 - Pending Save● 17 - Failed Save This filter is available for <code>computers</code> and <code>exchange</code> services.



Important

- The fields `threatName`, `filePath` and `ip` work with partial matching.
The filter returns the items which are exact match or start with the specified value. To use the specified value as a suffix, use the asterisk symbol (*).
For example:
If `filePath` is `C:\temp`, the API returns all items originating from this folder, including sub-folders.
If `filePath` is `*myfile.exe`, then the API returns a list of all `myfile.exe` files from anywhere on the system.
- The `Exchange` filters require a valid license key for Security for Exchange.

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” \(p. 196\)](#).

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
detectionPoint	Integer	The level where the detection took place. Possible values: <ul style="list-style-type: none">● 0 - transport● 1 - mailbox● 2 - folder● 3 - on demand
itemType	Integer	The quarantined object type. Possible values: <ul style="list-style-type: none">● 0 - attachment● 1 - email
threatStatus	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">● 0 - spam● 1 - suspected● 2 - infected● 3 - attachment detection● 4 - content detection● 5 - unscannable
email	Object	<ul style="list-style-type: none">● senderIP, a String containing the sender's IP address● senderEmail, a String consisting in the sender's email address, as it appears in the email header fieldFrom● subject, a String with the subject of the quarantined email

Field name	Data type	Description
		<ul style="list-style-type: none">recipients, an Array with the recipients, as they appear in the email header fields To and CcrealRecipients, an Array containing the email addresses of the intended recipients

Example

Request :

```
{
  "params": {
    "endpointId": "5d36c255f23f730fa91944e2",
    "page": 2,
    "perPage": 1,
    "filters": {
      "threatName": "Virus 0",
      "actionStatus": 1,
      "startDate": "2019-07-28T11:31:28",
      "endDate": "2019-08-16T11:31:16",
      "filePath": "c:\\\\Virus0\\virus0.exe"
    }
  },
  "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": {
    "total": 2,
    "page": 2,
  }
}
```

```
"perPage": 1,
"pagesCount": 2,
"items": [
  {
    "id": "5d3968e0f23f730ecb0f68c2",
    "quarantinedOn": "2019-07-28T11:31:28",
    "actionStatus": 1,
    "companyId": "55896b87b7894d0f367b23c6",
    "endpointId": "5d36c255f23f730fa91944e2",
    "endpointName": "Computer 1",
    "endpointIP": "156.133.37.181",
    "canBeRestored": false,
    "canBeRemoved": false,
    "threatName": "Virus 0",
    "details": {
      "filePath": "c:\\Virus0\\virus0.exe"
    }
  }
]
}
```

This response example is for exchange service:

```
{
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86",
  "jsonrpc": "2.0",
  "result": {
    page: 2,
    pagesCount: 10,
    perPage: 1,
    total: 10,
    items[0]: {
      "id": "5b7d219bb1a43d170b7b23ee",
      "quarantinedOn": "2019-08-01T07:15:20",
      "actionStatus": 1,
      "endpointId": "5d36c255f23f730fa91944e2",
      "endpointName": "Computer 1",
      "endpointIP": "57.238.160.118",
      "endpointAvailable": true,
      "threatName": "Virus 0",
      "companyId": "55896b87b7894d0f367b23c6",
      "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"
  ]
}
}
}]
}
```

2.11.2. 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. The maximum number of items that can be removed once is 100.

Return value

This method returns a Boolean which is 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
}
```

2.11.3. 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 which is 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
}
```

2.11.4. 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 Default Policy assigned. The default value for this parameter is <code>False</code> .

Return value

This method returns a Boolean which is `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
}
```

2.11.5. 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 which is 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
}
```

2.11.6. createAddFileToQuarantineTask

This method creates a new task to add a file to quarantine.

Parameters

Parameter	Type	Optional	Description
endpointIds	Array	No	A list with the IDs of target endpoints. You can specify maximum 100 targets at once. Only endpoints with security agents in Detection and prevention mode and active EDR Sensor module are valid targets.
filePath	String	No	The absolute file path on disk. This path can be at most 4096 characters in length and should have the format suitable to the target endpoint's operating system.

Return value

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

Example

Request :

```
{
  "params": {
    "endpointIds": [
      "63896b87b7894d0f367b23c6",
      "65896b87b7894d0f367b23c6"
    ],
    "filePath": "Z:\\path\\to\\file"
  },
  "jsonrpc": "2.0",
  "method": "createAddFileToQuarantineTask",
  "id": "5399c9b5-0b46-45e4-81aa-889952433d86"
}
```

Response :

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

2.12. General

The General API includes methods for general use without the need to enable a specific API to call any of these methods.

- [getApiKeyDetails](#) : provides details about the API key used.

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

2.12.1. getApiKeyDetails

This method returns details about the API key used.

Parameters

No input parameters are required.

Return value

This method returns an Object containing the details of the API key:

- `enabledApis` - an Array containing the list of enabled APIs
- `createdAt` - a String representing the UTC date and time when the API key was generated

Example

Request :

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

Response :

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    "enabledApis": [
      "packages",
      "network",
      "policies",
      "reports"
    ],
    "createdAt": "2019-04-11T12:00:54"
  }
}
```

3. API USAGE EXAMPLES

The following API usage examples make use of the following generated API key: "UjlMS+0m1l9IUZjpyWjG8gbnv2Mta4T".

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");

String apiKey = "UjlMS+0m1l9IUZjpyWjG8gbnv2Mta4T";
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 custom groups using the Network API.

```
curl -i \
-H "Authorization: \
Basic VWpsTVMrMG0xbDlJVVpqcGpXeUpHOGdibnYyTXRhNFQ6" \
-H "Content-Type: application/json" \
-d '{"id": "123456789", "jsonrpc": "2.0",
"method": "getCustomGroupsList", "params": \
{"parentId" : "5582c0acb1a43d9f7f7b23c6"}}' \
-X POST \
https://{domain}/api/v1.0/jsonrpc/network

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": "5582c385b1a43deb7f7b23c6", "name": "my group 1"},
  {"id": "5582d3b3b1a43d897f7b23c8", "name": "my group 2"}]}
```

3.3. Python Example

Now, we will query the list of available packages.

```
import base64
import requests
# Generate Authorization header from API key
apiKey = "UjlMS+0m1l9IUZjppjWyJG8gbnv2Mta4T"
auth = base64.b64encode((apiKey + ":").encode("UTF-8"))\
    .decode("UTF-8")
authorizationHeader = "Basic " + auth
json = {
    "method": "getPackagesList",
    "params": {},
    "jsonrpc": "2.0",
    "id": 123
}
result = requests.post(
    "https://{domain}/api/v1.0/jsonrpc/packages",
    json=json,
    verify=False,
    headers = {
        "Content-Type": "application/json",
        "Authorization": authorizationHeader
    }).json()

print(result)
```

Output:

```
{'jsonrpc': '2.0',
 'id': '61f4dadcd-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 VWp5TVMrMG0xbDlJVVpqcGpXeUpHOGdibnYyTXRhNFQ6"
  },
  json: {
    "id": "123456789",
    "jsonrpc": "2.0",
    "method": "getPackagesList",
    "params": []
  }
}, function(response, body) {
  console.log(body);
});

// Output:

// {'jsonrpc': '2.0',
//  'id': '61f4dad9-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}  
// }
```

3.5. PowerShell Example

This is an example PowerShell script. It provides the basics to make an API call to a GravityZone API endpoint.



Note

We wrote the operations in this script explicitly for didactic purposes. Feel free to optimize them for your practical use cases, should you feel it necessary.

```
# Store the API token (change this to your API key)  
# For details, refer to the "API Keys" section of this guide.  
  
$api_key = 'UjlMS+0m1l9IUZjppjWyJG8gbnv2Mta4T'  
  
# build the login string (pass is an empty string)  
  
$user = $api_key  
$pass = ""  
$login = $user + ":" + $pass  
  
# encode the login string to base64  
  
$bytes= [System.Text.Encoding]::UTF8.GetBytes($login)  
$encodedlogin=[Convert]::ToBase64String($bytes)  
  
# prepend "Basic " to the encoded login string to obtain  
# the auth header
```

```
$authheader = "Basic " + $encodedlogin

# Replace the base_uri string with the correct one
# for your console

$base_uri = "https://cloud.gravityzone.bitdefender.com/api"

# Replace the api_endpoint string with the correct one for
# the method used in the request_data
# For details, defer to the "API Requests" section
# of this guide.

$api_endpoint = "/v1.0/jsonrpc/network"

# Build the request URI

$request_uri = $base_uri + $api_endpoint

# Store the request body in a JSON variable.
# Define the API call method and its parameters.
# For more details on each API method, refer to the "Reference"
# chapter of this guide.

$request_data = '{
  "id":"123456789",
  "jsonrpc":"2.0",
  "method":"getEndpointsList",
  "params":
  {
    "page":1,
    "perPage":3
  }
}'

# All required resources are now set.

# You have two options to make the API call.
```

```
# First option:
# Add all call parameters in one structure, then call
# Invoke-RestMethod with it.

$params = @{
    Uri          = $request_uri
    Headers      = @{
        'Authorization' = "$authheader"
        'Content-Type'  = "application/json"
    }
    Method       = 'POST'
    Body         = $request_data
    ContentType  = 'application/json'
}

$response = Invoke-RestMethod @params

# Second option:
# Build the headers structure, but specify the
# Invoke-RestMethod parameters inline.

$headers = New-Object `
[System.Collections.Generic.Dictionary[[String],[String]]
$headers.Add("Authorization",$authheader)
$headers.Add("Content-Type","application/json")

$response2 = Invoke-RestMethod -Uri $request_uri `
-Headers $headers -ContentType 'application/json' `
-Method Post -Body $request_data

# Random examples of how to address/display the obtained
# call results from the $response and $response2 variables

Write-Output '$response'
Write-Output "~~~~~"
$response
Write-Output '$response |ConvertTo-Json'
Write-Output "~~~~~"
$response |ConvertTo-Json
Write-Output '$response.result | ConvertTo-Json'
```

```
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response.result | ConvertTo-Json
Write-Output '$response.result.items |ConvertTo-Json'
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response.result.items |ConvertTo-Json

Write-Output '$response2'
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response2
Write-Output '$response2.result'
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response2.result
Write-Output '$response2.result.items'
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response2.result.items
Write-Output '$response2.result.items.id[0]'
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response2.result.items.id[0]
Write-Output '$response2.result.items.name[1]'
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response2.result.items.name[1]
Write-Output '$response2.result.items[1] |ConvertTo-Json'
Write-Output "~~~~~~~~~~~~~~~~~~~~"
$response2.result.items[1] |ConvertTo-Json
```

3.6. VBScript Example

This is a VBScript example. It provides the basics to make an API call to a GravityZone API endpoint.



Note

We wrote the operations in this script explicitly for didactic purposes. Feel free to optimize them for your practical use cases, should you feel it necessary.

```
'These are for displaying the results of the call.

Set fso = CreateObject ("Scripting.FileSystemObject")
Set stdout = fso.GetStandardStream (1)
Set stderr = fso.GetStandardStream (2)
```

```
'These are some helping funtions used for base64 encoding  
'of the authorization header.
```

```
Private Function Stream_StringToBinary(Text)  
    Const adTypeText = 2  
    Const adTypeBinary = 1  
    Dim BinaryStream 'As New Stream  
    Set BinaryStream = CreateObject("ADODB.Stream")  
    BinaryStream.Type = adTypeText  
    BinaryStream.CharSet = "us-ascii"  
    BinaryStream.Open  
    BinaryStream.WriteText Text  
    BinaryStream.Position = 0  
    BinaryStream.Type = adTypeBinary  
    BinaryStream.Position = 0  
    Stream_StringToBinary = BinaryStream.Read  
    Set BinaryStream = Nothing  
End Function
```

```
Function Base64Encode(sText)  
    Dim oXML, oNode  
    Set oXML = CreateObject("Msxml2.DOMDocument.3.0")  
    Set oNode = oXML.CreateElement("base64")  
    oNode.dataType = "bin.base64"  
    oNode.nodeTypedValue = Stream_StringToBinary(sText)  
    Base64Encode = Replace(oNode.text, chr(10), "")  
    Set oNode = Nothing  
    Set oXML = Nothing  
End Function
```

```
'Store the API token.  
'Make sure to change the string with your actual API key.  
'For more information, refer to the "API Keys" section  
'of this guide.
```

```
api_key = "UjlMS+0ml19IUZjppjWyJG8gbnv2Mta4T"
```

```
'Build the login string.
```

```
'Note: pass is an empty string.

user = api_key
pass = ""
login = user & ":" & pass

'Encode the login string to base64.

encodedlogin = Base64Encode(login)

'Prepend "Basic " to the encoded login string to obtain
'the auth header.

authheader = "Basic " & encodedlogin

'Change the base_uri string with the correct one for your console.

base_uri = "https://cloud.gravityzone.bitdefender.com/api"

'Change the api_endpoint string with the correct one
'for the method used in the request_data.
'For details, refer to "API Requests" section of this guide.

api_endpoint = "/v1.0/jsonrpc/network"

'Build the request URI.

request_uri = base_uri & api_endpoint

'Create the body of the request.
'Define the API call method and its parameteres.
'For more information, refer to the "Reference" chapter
'of this guide.
'Note: Due to limited page width, the strJSONRequest string
'is on multiple lines. You need to put it on one line.
```

```
strJSONRequest = {"id":"123456789",  
  "jsonrpc":"2.0",  
  "method":"getEndpointsList",  
  "params":{"page":1,"perPage":3}}
```

```
'All required resources are set.
```

```
'Make the API call.
```

```
Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")  
objHTTP.Open "POST", request_uri, False  
objHTTP.setRequestHeader "Authorization", authheader  
objHTTP.setRequestHeader "Content-Type", "application/json"  
objHTTP.send (strJSONRequest)
```

```
'Examples of how to display call reponse:
```

```
stdout.WriteLine "Response Code: " & objHTTP.status  
stdout.WriteLine "Response Headers: " & objHTTP.getAllResponseHeaders  
stdout.WriteLine "Response Data: " & objHTTP.responseText
```

A. Appendices

A.1. API Error Codes

Code	Description
4030001	This error is thrown when operation is not permitted, because the feature is not available on this platform
4030003	This error is thrown on MOVE ENDPOINTS validation process because Only MSP users can move endpoints to other companies
4050001	This error is thrown on MOVE ENDPOINTS validation process when destination group is invalid
4050002	This error is thrown on MOVE ENDPOINTS validation process when destination group Id param is not a string
4050003	This error is thrown on MOVE ENDPOINTS validation process when endpointIds param is not a non-empty array
4050004	This error is thrown on MOVE ENDPOINTS validation process when target endpoint is unmanaged
4050005	This error is thrown on MOVE ENDPOINTS validation process when target endpoint is under same company as destination
4050006	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because it is not movable
4050007	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because it does not have unified client app id
4050008	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because it already has a Move task in progress
4050009	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because it has been already moved from this company
4050010	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because source company is not directly under current user's company

Code	Description
4050011	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because of MA issues
4050012	This error is thrown on MOVE ENDPOINTS validation process because target endpoint cannot be moved between companies with different BEST customizations
4050013	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because it has encrypted volumes
4050014	This error is thrown on MOVE ENDPOINTS validation process when target endpoint cannot be moved because source company doesn't have monthly license
4050015	This error is thrown on MOVE ENDPOINTS validation process when destination company license is not Monthly License or destination company is not a direct company
4050016	This error is thrown on MOVE ENDPOINTS validation process when the target endpoint cannot be moved because the source company has paid subscription and the destination company has trial subscription
4050017	This error is thrown on DELETE CUSTOM CONTAINER GROUP validation process when the target groupId cannot be removed because contains container hosts
4050018	This error is thrown on MOVE CUSTOM GROUP validation process when trying to move entity into Containers from outside source
4050019	This error is thrown on MOVE CUSTOM CONTAINER GROUP validation process when trying to move entity from Containers to outside source
4050020	This error is thrown on DELETE CUSTOM CONTAINER GROUP validation process when trying to delete a container host folder
4050021	This error is thrown on DELETE CUSTOM CONTAINER GROUP validation process when trying to delete a container
4050022	This error is thrown on MOVE CUSTOM GROUP validation process when trying to move container host while is synchronizing